การสร้างภาพนามธรรมความต้องการความมั่นคง โดยใช้แบบจำลองเชิงโครงสร้างความมั่นคง

นางสาววิริยา สุภาณิชย์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2551

VISUALIZING SECURITY REQUIREMENTS USING SECURITY STRUCTURAL MODEL

Miss Weeriya Supanich

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science Program in Computer Science

Department of Computer Engineering

Faculty of Engineering

Chulalongkorn University

Academic Year 2008

หัวข้อวิทยานิพนธ์	การสร้างภาพนามธรรมความต้องการความมั่นคง โดยใช้แบบจำลองเชิงโครงสร้างความมั่นคง
โดย	นางสาววิริยา สุภาณิชย์
สาขาวิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	ผู้ช่วยศาสตราจารย์นครทิพย์ พร้อมพูล

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะวิศวกรรมศาสตร์
(รองศาสตราจารย์ ดร.บุญสม เลิศหิรัญวงศ์)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(รองศาสตราจารย์ ดร.วันชัย ริ้วไพบูลย์)

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(ผู้ช่วยศาสตราจารย์ นครทิพย์ พร้อมพูล)

..... กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.พิษณุ คนองชัยยศ)

..... กรรมการ
(อาจารย์ ดร.ยรรยง เต็งอำนวย)

..... กรรมการภายนอกมหาวิทยาลัย
(ผู้ช่วยศาสตราจารย์ ดร.ศรัณย์ อินทโกสุม)

วีริยา สุภาณิชย์ : การสร้างภาพนามธรรมความต้องการความมั่นคง โดยใช้แบบจำลองเชิงโครงสร้างความมั่นคง. (VISUALIZING SECURITY REQUIREMENTS USING SECURITY STRUCTURAL MODEL) อ. ที่ปรึกษาวิทยานิพนธ์หลัก : ผศ.นครทิพย์ พร้อมพูล, 193 หน้า.

วิทยานิพนธ์นี้มีวัตถุประสงค์เพื่อนำเสนอแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคง โดยใช้แผนภาพคลาสของยูเอ็มแอล และสร้างภาพนามธรรมความต้องการความมั่นคง โดยมีขอบเขตสนับสนุนแบบรูปความมั่นคงจำนวน 20 แบบรูป ซึ่งครอบคลุม 4 กลุ่มแบบรูปความมั่นคง ได้แก่ การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง การระบุตัวตนและการพิสูจน์ตัวจริง แบบจำลองการควบคุมการเข้าถึง และสถาปัตยกรรมไฟล์วอลล์ ทั้งนี้แบบจำลองเชิงโครงสร้างที่สร้างขึ้นได้ตรวจสอบกับผู้มีความรู้พื้นฐานด้านความมั่นคง เพื่อปรับปรุงแบบจำลองให้มีความสอดคล้องกับบริบทของแบบรูปความมั่นคง ด้านความสมบูรณ์ต่อการนำไปประยุกต์ใช้งาน และด้านความครบถ้วนของความสัมพันธ์ระหว่างแบบรูปความมั่นคง

ผู้วิจัยได้พัฒนาเครื่องมือต้นแบบสำหรับการสร้างภาพนามธรรมความต้องการความมั่นคงจากแบบจำลองเชิงโครงสร้าง ผู้ใช้งานสามารถเลือกประเภทของภาพนามธรรมได้โดยอยู่ในรูปแบบของแผนภูมิต่างๆ จากนั้นผู้วิจัยได้ทดสอบเครื่องมือต้นแบบใน 3 ปัจจัยจากหน่วยตัวอย่าง 12 หน่วย ในการประเมินความมั่นคงระบบของระบบจัดการห้องสมุด ผลจากการทดสอบสรุปได้ว่า 1) คุณภาพผลลัพธ์ภาพนามธรรมมีความชัดเจน ถูกต้อง และแปลความหมายจากความต้องการความมั่นคงได้ง่ายขึ้น 2) คุณสมบัติของเครื่องมือต้นแบบมีการออกแบบส่วนต่อประสานที่ง่าย และครอบคลุมต่อการใช้งาน และ 3) เครื่องมือต้นแบบสามารถนำไปประยุกต์ใช้ในองค์กรได้และเป็นการสนับสนุนให้เกิดองค์ความรู้ด้านแบบรูปความมั่นคง

เครื่องมือต้นแบบการสร้างภาพนามธรรมช่วยให้เกิดความเข้าใจที่ตรงกันอย่างชัดเจนระหว่างผู้ออกแบบระบบความมั่นคงและผู้ใช้งาน และสามารถวิเคราะห์ความต้องการในลักษณะของข้อมูลสรุปที่สำคัญ ที่สอดคล้องกับแบบรูปความมั่นคง

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต วีริยา สุภาณิชย์

สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์ ลายมือชื่ออ.ที่ปรึกษาวิทยานิพนธ์หลัก นครทิพย์ พร้อมพูล

ปีการศึกษา 2551

4970584621 : MAJOR COMPUTER SCIENCE

KEYWORDS: SECURITY PATTERNS / VISUALIZATION / SECURITY / SECURITY REQUIREMENTS / SECURITY GRAMMARS / STRUCTURAL MODEL / CLASS DIAGRAM

WEERIYA SUPANICH : VISUALIZING SECURITY REQUIREMENTS USING SECURITY STRUCTURAL MODEL. ADVISOR : ASST.PROF.NAKORNTHIP PROMPOON, 193 pp.

The objective of this thesis is to propose a structural model using UML class diagram and create a security requirements visualization based on the proposed structural model. It covers 20 security patterns from which 4 security patterns types; Enterprise Security and Risk Management, Identification and Authentication, Access Control Model and Firewall Architecture. Security domain persons who have a security fundamental knowledge help validate the proposed structural model to improve the consistency between the structural model and security patterns contexts, the completeness for applying the model and the completeness of model based on relations among security patterns.

A visualization supporting tool is also developed based on the proposed structural models. The results obtained from using the tool are graphical representations in terms of many chart types. To test the quality of visualization supporting tool in 3 main factors; the quality of chart representation, the user interface design and the tool capability for applying in organization, 12 persons are selected as sample units to evaluate the tool from a security system case study, the library management system. After using the tool, the sample units evaluate the level of satisfaction in various factors and also identify problems and recommendations. The experimental results are that the quality of chart representation is clear and correct. Users can interpret system security requirements easily. Also, the user interface design is simple to users and covers the usage aspects. The prototype tool can be applied to the organization and can directly support the construction of security patterns knowledge to organization.

The tool helps security system designer and user understand the security requirements clearly and analyze security requirements in terms of summarized data related to security patterns.

Department : Computer Engineering ..... Student's Signature : Weeriya Supanich .....

Field of Study : Computer Science ..... Advisor's Signature : Nakornthip Prompoon .....

Academic Year : 2008 .....

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้ได้สำเร็จลุล่วงด้วยความเมตตาและความช่วยเหลืออย่างยิ่งจากผู้ช่วยศาสตราจารย์นครทิพย์ พร้อมพูล อาจารย์ที่ปรึกษา ที่เสียสละเวลาช่วยให้คำปรึกษา ข้อคิดและคำแนะนำที่มีประโยชน์ต่องานวิจัย ตลอดจนความเอาใจใส่และความเชื่อมั่นที่อาจารย์มีให้ผู้วิจัย ซึ่งเป็นกำลังใจและเป็นแรงส่งเสริมให้ผู้วิจัยสามารถพัฒนางานวิจัยที่มีคุณภาพและมีคุณค่า

ขอขอบพระคุณ รองศาสตราจารย์ ดร.วันชัย ริ้วไพบูลย์ ประธานกรรมการสอบวิทยานิพนธ์ อาจารย์ ดร.ยรรยง เต็งอำนวย ผู้ช่วยศาสตราจารย์ ดร.พิษณุ คนองชัยยศ และผู้ช่วยศาสตราจารย์ ดร.ศรัณย์ อินทโกสุม กรรมการสอบวิทยานิพนธ์ ที่ได้กรุณาสละเวลาให้คำแนะนำสำหรับโครงร่างวิทยานิพนธ์และวิทยานิพนธ์ให้มีคุณภาพยิ่งขึ้น

ขอขอบพระคุณคณาจารย์ในภาควิชาวิศวกรรมคอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัยทุกท่าน ที่ประสิทธิ์ประสาทความรู้อันมีค่ายิ่งแก่ผู้วิจัย

ขอขอบคุณบุคลากรในภาควิชาวิศวกรรมคอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัยทุกท่าน ที่ให้ข้อมูล คำแนะนำและความช่วยเหลือในการดำเนินการทั้งในเรื่องการศึกษาและการสอบวิทยานิพนธ์ได้สำเร็จลุล่วง

ขอขอบคุณ เพื่อนๆ พี่ๆ และน้องๆ ทุกคนที่ผ่านเข้ามาในชีวิตของผู้วิจัย ที่ห่วงใยและให้ความช่วยเหลือในทุกๆ ด้านจนผู้วิจัยสามารถทำวิทยานิพนธ์ฉบับนี้สำเร็จลุล่วง

ขอบคุณสมาชิกในห้องปฏิบัติการวิศวกรรมซอฟต์แวร์ สำหรับน้ำใจ ความห่วงใย ความช่วยเหลือและคำแนะนำที่มีประโยชน์แต่ผู้วิจัย

ท้ายที่สุด ขอกราบขอบพระคุณบิดา มารดาและสมาชิกในครอบครัวทุกท่าน ที่ให้การสนับสนุน และให้กำลังใจแก่ผู้วิจัย เสมอมา

สารบัญ

หน้า

หน้า

สารบัญตาราง

หน้า

หน้า

หน้า

สารบัญภาพ

หน้า

หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในการพัฒนาระบบความมั่นคง มักเกิดช่องว่างระหว่างผู้เชี่ยวชาญทางด้านความมั่นคงกับผู้พัฒนาระบบ โดยผู้เชี่ยวชาญทางด้านความมั่นคงมักจะมุ่งเน้นเป้าหมายไปที่การสร้างความมั่นคงของระบบ ในขณะที่ผู้พัฒนามักจะมุ่งเน้นเป้าหมายไปที่การสร้างซอฟต์แวร์ที่สามารถนำไปใช้งานในความเป็นจริงได้ตามความต้องการของระบบ

แบบรูปความมั่นคง (Security Patterns) [1-5] ได้นำเสนอขึ้น เพื่อเชื่อมช่องว่างระหว่างผู้พัฒนากับผู้เชี่ยวชาญทางด้านความมั่นคง โดยนำเสนอแนวทาง หรือผลเฉลยของปัญหาด้านความมั่นคงต่างๆ ที่ถูกแก้ปัญหาไว้ก่อนหน้านี้แล้ว และสนับสนุนการนำกลับมาใช้ใหม่ (Reuse) อย่างไรก็ตามการศึกษาและวิเคราะห์แบบรูปความมั่นคงเพื่อนำมาประยุกต์ใช้ในการพัฒนาซอฟต์แวร์ทางด้านความมั่นคงนั้นทำได้ยาก เนื่องจากผู้พัฒนาจะต้องศึกษา และทำความเข้าใจโครงสร้างคุณสมบัติและเงื่อนไขบังคับของแบบรูปความมั่นคงก่อน จึงจะสามารถนำแบบรูปความมั่นคงเหล่านั้นมาประยุกต์ใช้ในการพัฒนาซอฟต์แวร์ได้ ไม่เช่นนั้นอาจเกิดผลเสียที่ตามมาต่อระบบ เช่น อาจทำให้ระบบมีจุดอ่อน ผู้บุกรุกหรือผู้ที่ไม่ประสงค์ดีสามารถเข้ามาโจมตีต่อระบบได้ง่าย

ในกระบวนการการออกแบบและพัฒนาระบบความมั่นคงนั้น ผู้วิเคราะห์และออกแบบระบบมักจะสร้างแบบจำลอง หรือโมเดล (Model) ขึ้นมา เพื่ออธิบายกลไกการทำงานของระบบ และเป็นเครื่องมือสื่อความหมายที่ตรงกันภายในทีมงานนักพัฒนา การสร้างแบบจำลองนี้จะช่วยจัดการกับความซับซ้อนของงานในระบบ โดยอาศัยยูเอ็มแอล (UML: Unified Modeling Language) ซึ่งเป็นภาษาสำหรับการสร้างแบบจำลองที่ได้รับความนิยม [5] ทั้งนี้การสร้างแบบจำลองเพื่ออธิบายกลไกการทำงานของระบบนั้นจำเป็นต้องมีแผนภาพหลายชนิดเพื่อแสดงรายละเอียดที่แตกต่างกันออกไปในการพัฒนาระบบ เช่น ในการแสดงแบบจำลองเชิงโครงสร้างของระบบ มักอาศัยแผนภาพคลาส (Class Diagram) เพื่ออธิบายส่วนประกอบต่างๆ ภายในระบบ ตลอดจนความสัมพันธ์ของแต่ละส่วนประกอบ ที่มีหน้าที่การทำงานสอดคล้องกัน

นอกจากกระบวนการการออกแบบและพัฒนาระบบความมั่นคงแล้ว ยังมีกระบวนการสำคัญ ที่มีความสัมพันธ์กัน คือ กระบวนการการกำหนดความต้องการด้านความมั่นคง ซึ่งจัดเป็นความต้องการที่ไม่ใช่หน้าที่ (non-Functional Requirements) หากแต่มีความสำคัญ เพราะเป็นการรวบรวมข้อกำหนดความต้องการต่างๆ จากผู้ที่เกี่ยวข้อง มาวิเคราะห์เพื่อออกแบบระบบให้ตอบสนองตามความต้องการของผู้ใช้งาน และเพิ่มความสามารถของระบบ [6] ความต้องการ

เหล่านี้เป็นความต้องการที่เกี่ยวข้องกับการตรวจหาจุดอ่อนที่อาจปรากฏได้ในระบบ ความเสี่ยงที่อาจจะเกิดขึ้น รวมถึงผลกระทบที่อาจตามมาหากถูกโจมตีในจุดดังกล่าว ซึ่งถือว่าเป็นความต้องการที่จำเป็นในการพัฒนาระบบ ในความเป็นจริงพบว่าการกำหนดความต้องการดังกล่าวต้องอาศัยผู้เชี่ยวชาญ และมีประสบการณ์ทางด้านความมั่นคง แต่เนื่องจากปัญหาของผู้ใช้งานหรือผู้พัฒนาอาจมีความรู้และประสบการณ์ทางด้านความมั่นคงไม่เพียงพอ อีกทั้งความต้องการด้านความมั่นคงนั้นมีความสำคัญ และมีผลกระทบโดยตรงต่อความมั่นคงของระบบ จึงควรอย่างยิ่งที่จะต้องให้ความสำคัญกับความต้องการด้านความมั่นคงอยู่ในลำดับต้น

มีงานวิจัยหลายงานวิจัยที่เกี่ยวข้องกับกระบวนการการกำหนดความต้องการด้านความมั่นคง เช่น A.V. Lamsweerde และคณะ [7] ได้นำเสนอการพิจารณาองค์ประกอบด้านความมั่นคงต่างๆ เพื่อเป็นแนวทางในการรวบรวมความต้องการด้านความมั่นคง และกวิน สุภาพร และคณะ [8] [9] ได้สร้างไวยากรณ์และเครื่องมือสำหรับสร้างข้อกำหนดความต้องการทางด้านความมั่นคงจากแบบรูปความมั่นคงของ M.Schumacher et al. [4] ผลลัพธ์ที่ได้จากงานวิจัยนี้คือ ความต้องการด้านความมั่นคงที่สอดคล้องกับแบบรูปความมั่นคง แต่หากพิจารณาถึงความต้องการด้านความมั่นคงนั้น พบว่าความต้องการดังกล่าวมีความซับซ้อนเป็นผลให้ผู้ใช้งานหรือผู้พัฒนาระบบนั้นอาจจะทำความเข้าใจได้ยาก ซึ่งอาจจะส่งผลถึงการวิเคราะห์ความต้องการ การออกแบบระบบที่ผิดพลาด หากว่า มีการพัฒนาเครื่องมือที่ช่วยในการแสดงความต้องการด้านความมั่นคงออกมาเป็นภาพแล้ว จะสามารถช่วยให้การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงทำได้อย่างเหมาะสม ตรงกับความต้องการของผู้ใช้งานมากขึ้น

จากความสำคัญของการรักษาความมั่นคงของระบบ ผู้วิจัยได้ตระหนักถึงบทบาทและประโยชน์ของการนำแบบรูปความมั่นคงมาประยุกต์ใช้ในการพัฒนาระบบความมั่นคงภายในองค์กร ทั้งนี้การนำแบบรูปความมั่นคงมาประยุกต์ใช้งานนั้น ในขั้นตอนของการออกแบบและพัฒนาระบบความมั่นคง ผู้วิจัยเล็งเห็นถึงประโยชน์ในการเลือกใช้แผนภาพคลาสเพื่อเป็นตัวแทนในการแสดงส่วนประกอบเชิงโครงสร้างของการนำแบบรูปความมั่นคง เนื่องจากแผนภาพคลาสมีความเหมาะสมในการแสดงแบบจำลองเชิงโครงสร้าง มีกฎเกณฑ์ และโครงสร้างของภาษาสำหรับการพัฒนาระบบ และสามารถใช้สื่อสารภายในทีมงาน และระหว่างทีมงานกับผู้ใช้ระบบ แต่เนื่องจากแบบจำลองเชิงโครงสร้างโดยใช้แผนภาพคลาสนั้นสามารถระบุข้อมูลภายในได้เพียงแค่ลักษณะประจำ การดำเนินการ และความสัมพันธ์ระหว่างคลาสเท่านั้น แต่อย่างไรก็ตามยังมีข้อจำกัดคือ ไม่สามารถระบุกรณีตัวอย่าง ของข้อมูลความต้องการด้านความมั่นคงได้ แต่ไวยากรณ์ความมั่นคงนั้นสามารถสร้างเป็นข้อมูลความต้องการความมั่นคงได้ แต่ทั้งนี้ยังไม่สามารถแสดงความสัมพันธ์ระหว่างองค์ประกอบต่างๆ ภายในแบบรูปความมั่นคง

ดังนั้นผู้วิจัยจึงมีแนวคิดในการพัฒนาเครื่องมือต้นแบบสำหรับการสร้างภาพนามธรรมโดยนำวิธีการสร้างภาพนามธรรม (Visualization) ซึ่งเป็นวิธีการหนึ่งสำหรับการสร้างภาพ แผนภาพ หรือ ภาพเคลื่อนไหว เพื่อใช้ในการสื่อสารข้อความเพื่อทำให้เกิดความเข้าใจที่ชัดเจน มีความเข้าใจตรงกันทั้งผู้ส่งสารและผู้รับสาร การสร้างภาพนามธรรมนั้นจัดได้ว่าเป็นวิธีการที่มีประสิทธิภาพในการสื่อสารถึงสิ่งที่เป็นนามธรรม มองเห็นภาพได้ยาก นำมาสร้างเป็นภาพเพื่อการติดต่อสื่อสารที่ทำความเข้าใจได้ง่ายและชัดเจนมากยิ่งขึ้น [10] ทั้งนี้เพื่อแสดงให้เห็นถึงความสัมพันธ์ของข้อมูลความต้องการด้านความมั่นคง ซึ่งผู้ใช้งานสามารถเลือกดูความสัมพันธ์ของข้อมูลความต้องการ ที่สอดคล้องกับแต่ละแบบรูปความมั่นคง และแบบรูปความมั่นคงแบบบูรณาการได้ เพื่อช่วยให้ผู้ออกแบบระบบความมั่นคงสามารถทำความเข้าใจกับความต้องการได้อย่างชัดเจน ทำให้เกิดความเข้าใจที่ตรงกันระหว่างผู้ออกแบบระบบความมั่นคง และผู้ใช้งาน

งานวิทยานิพนธ์นี้ จะนำเสนอแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคง โดยใช้แผนภาพคลาส และสร้างภาพนามธรรมความสัมพันธ์ของความต้องการด้านความมั่นคงของกวิน สุภาพร และคณะ [8] ซึ่งสนับสนุนแบบรูปความมั่นคงของ M.schumacher [4] เพื่อช่วยให้ผู้ออกแบบระบบความมั่นคงสามารถวิเคราะห์ความต้องการในมุมมองของแต่ละแบบรูปความมั่นคง และในมุมมองความสัมพันธ์ระหว่างแบบรูปความมั่นคงได้ และสามารถทำความเข้าใจกับความต้องการด้านความมั่นคงได้อย่างชัดเจน ทำให้มีความเข้าใจที่ตรงกันระหว่างผู้ออกแบบระบบความมั่นคง และผู้ใช้งาน

1.2 วัตถุประสงค์ของการวิจัย

1) สร้างแบบจำลองเชิงโครงสร้างของส่วนประกอบของแบบรูปความมั่นคง และความสัมพันธ์ภายในแต่ละแบบรูป ที่สอดคล้องกับแบบรูปความมั่นคง [10] และไวยากรณ์ความมั่นคง [1] โดยใช้แผนภาพคลาส

2) สร้างแบบจำลองเชิงโครงสร้างโดยบูรณาการแบบจำลองทั้งหมดที่ได้จาก 1) และสร้างความสัมพันธ์ที่เกิดขึ้น โดยใช้แผนภาพคลาส

3) สร้างเครื่องมืออัตโนมัติโดยนำความต้องการด้านความมั่นคงมาสร้างภาพนามธรรมความสัมพันธ์ โดยแสดงผลในรูปของกราฟ

1.3 ขอบเขตของการวิจัย

1) นำเสนอแบบจำลองเชิงโครงสร้างของส่วนประกอบของแบบรูปความมั่นคง ความสัมพันธ์ภายในแต่ละแบบรูป และความสัมพันธ์แบบบูรณาการ ที่สอดคล้องกับไวยากรณ์

ความมั่นคง [1] และแบบรูปความมั่นคงของ M. Schumacher [10] ที่ได้รับการออกแบบและตรวจสอบความถูกต้องแล้ว 4 กลุ่มแบบรูปดังต่อไปนี้

1.1) การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง

กลุ่มแบบรูปนี้จะเกี่ยวข้องกับการจัดการในเรื่องต่างๆ พื้นฐาน เช่น การระบุความจำเป็นพื้นฐาน การประเมินความเสี่ยง แนวคิดและการบริหารความมั่นคง และการให้ความสำคัญกับการติดต่อภายนอกองค์กร ซึ่งแบบรูปความมั่นคงในกลุ่มนี้ประกอบไปด้วย

(1) การระบุความต้องการด้านความมั่นคงสำหรับสินทรัพย์ขององค์กร

(2) การประเมินมูลค่าสินทรัพย์

(3) การประเมินภัยคุกคาม

(4) การประเมินภาวะเสี่ยง

(5) การกำหนดความเสี่ยง

(6) แนวคิดความมั่นคงขององค์กร

(7) บริการความมั่นคงขององค์กร

(8) การสื่อสารของผู้มีหุ้นส่วนในองค์กร

1.2) การระบุตัวตนและการพิสูจน์ตัวจริง

กลุ่มแบบรูปนี้จะเกี่ยวข้องกับการตรวจสอบปฏิสัมพันธ์ในเรื่องต่างๆ ระหว่างผู้ใช้งานกับระบบ ซึ่งรองรับการบริการด้านการระบุและยืนยันตัวตนแบบต่างๆ ตามความต้องการที่ระบุไว้ในกลุ่มแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง แบบรูปความมั่นคงในกลุ่มนี้ประกอบไปด้วย

(1) ความต้องการด้านการระบุและการพิสูจน์ตัวตน

(2) ทางเลือกการออกแบบสำหรับการระบุและการพิสูจน์ตัวตนแบบอัตโนมัติ

(3) การออกแบบและใช้รหัสผ่าน

(4) ทางเลือกการออกแบบสำหรับแบบชีวมิติ

1.3) แบบจำลองควบคุมการเข้าถึง

กลุ่มแบบรูปนี้จะเกี่ยวข้องกับการกำหนดเงื่อนไขบังคับ (Constraints) การเข้าถึงข้อมูลในระดับต่างๆ ไม่ว่าจะเป็นสถาปัตยกรรม โปรแกรมประยุกต์ และข้อบังคับของการปฏิบัติงาน แบบรูปความมั่นคงในกลุ่มนี้ประกอบด้วย

(1) การให้อำนาจ

(2) การควบคุมการเข้าถึงเชิงบทบาท

(3) ความมั่นคงหลายระดับ

(4) การตรวจสอบการเข้าถึงทรัพยากร

(5) การกำหนดสิทธิ์ให้กับบทบาท

1.4) สถาปัตยกรรมไฟร์วอลล์

กลุ่มแบบรูปนี้เกี่ยวข้องกับการการกำหนดเงื่อนไขบังคับ สำหรับการติดต่อสื่อสารผ่านทางระบบเครือข่าย (Network) ทั้งนี้เพื่อป้องกันการโจมตีหรือปลอมปนทั้งจากภายนอกและภายในองค์กร ซึ่งแบบรูปความมั่นคงในกลุ่มนี้ประกอบด้วย

(1) ไฟร์วอลล์สำหรับการกรองแพ็คเกจ

(2) ไฟร์วอลล์เชิงตัวแทน

(3) ไฟร์วอลล์เชิงสถานะ

2) สร้างเครื่องมือเพื่อนำความสัมพันธ์ของแต่ละความต้องการด้านความมั่นคงที่ได้จากข้อ 1) โดยแสดงผลในรูปของกราฟสองมิติ และสามมิติ

3) ทดสอบเครื่องมือ โดยใช้ผู้ร่วมทดลองที่มีประสบการณ์และมีความชำนาญด้านความต้องการด้านความมั่นคงมาทดลองใช้เครื่องมือการสร้างภาพนามธรรมของความต้องการด้านความมั่นคงจากสถานการณ์จำลองการกำหนดความต้องการด้านความมั่นคง เพื่อวัดระดับความพึงพอใจ และการการปรับปรุงเครื่องมือในการแสดงนามธรรมต่อไป

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1) ได้แบบจำลองเชิงโครงสร้างของส่วนประกอบของแบบรูปความมั่นคง ความสัมพันธ์ภายในแต่ละแบบรูป และความสัมพันธ์แบบบูรณาการของแบบรูปทั้งหมด

2) ได้เครื่องมือต้นแบบในการสร้างภาพนามธรรมที่แสดงความความสัมพันธ์ของความต้องการทางด้านความมั่นคง เพื่อใช้สนับสนุนการกำหนดความต้องการด้านความมั่นคงได้อย่างสะดวก ตรงกับความต้องการของผู้ใช้งาน

3) ได้ภาพนามธรรมในรูปแบบของแผนภูมิประเภทต่างๆ ที่แสดงให้เห็นความสัมพันธ์ของความต้องการด้านความมั่นคงจากการพิจารณาแบบรูปความมั่นคง สามารถทำความเข้าใจได้ง่ายขึ้น ซึ่งจะส่งผลทำให้การวิเคราะห์ความต้องการของระบบความมั่นคงทำได้อย่างเหมาะสมและมีประสิทธิภาพมากยิ่งขึ้น

1.5 วิธีดำเนินการวิจัย

1) ศึกษารายละเอียดของการกำหนดความต้องการทางด้านความมั่นคงของกวิน สุภาพร และคณะ [8] [9] และแบบรูปความมั่นคงของ M.Schumacher และคณะ [4]

2) วิเคราะห์การกำหนดความต้องการทางด้านความมั่นคง แบบรูปความมั่นคง เพื่อนำมาสร้างเป็นแบบจำลองเชิงโครงสร้าง โดยใช้แผนภาพคลาส ซึ่งสอดคล้องกับการกำหนดความต้องการทางด้านความมั่นคง โดยมีรายละเอียดตรงตามบริบทที่กล่าวถึงไว้ในแต่ละแบบรูป

3) วิเคราะห์ความสัมพันธ์ที่เชื่อมโยงกันระหว่างแบบรูปความมั่นคง เพื่อนำมาสร้างเป็นแผนภาพคลาสที่แสดงความสัมพันธ์แบบบูรณาการระหว่างแบบรูปทั้งหมด โดยมีรายละเอียดความสัมพันธ์ที่เชื่อมโยงระหว่างกันตรงตามบริบทที่กล่าวถึงไว้แบบรูป

4) สร้างเครื่องมือต้นแบบเพื่อนำความสัมพันธ์ของความต้องการทางด้านความมั่นคงทั้งหมด แสดงผลออกมาในรูปของแผนภูมิสองมิติ และสามมิติ

5) ทดสอบและปรับปรุงเครื่องมือต้นแบบ จากข้อเสนอแนะต่างๆ ของผู้ใช้งาน

6) จัดทำวิทยานิพนธ์

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ในบทนี้จะกล่าวถึงทฤษฎีที่นำมาใช้ในวิทยานิพนธ์ซึ่งได้แก่ แบบรูปความมั่นคง แผนภาพคลาส อีบีเอ็นเอฟ (EBNF) และการสร้างภาพนามธรรม นอกจากนี้จะกล่าวถึงงานวิจัยที่เกี่ยวข้องได้แก่ การกำหนดความต้องการด้านความมั่นคงโดยใช้ไวยากรณ์ของแบบรูปความมั่นคง เมทาดาตา และแบบรูปการให้อำนาจ แบบรูปการออกแบบความมั่นคง และมุมมองการสร้างภาพนามธรรม ซึ่งมีรายละเอียดดังต่อไปนี้

2.1 แนวคิดและทฤษฎี

2.1.1 แบบรูปความมั่นคง (Security Patterns)

แบบรูปความมั่นคง [1-5] คือ แบบแผน หรือแนวทางในการแก้ไขปัญหาทางด้านความมั่นคงต่างๆ ที่พบได้เป็นประจำในการออกแบบซอฟต์แวร์เกี่ยวกับความมั่นคง โดยแผนภาพที่นิยมนำมาใช้อธิบายความสัมพันธ์ต่างๆ ในแบบรูปความมั่นคง คือ แผนภาพยูเอ็มแอล ซึ่งนิยมใช้ในการอธิบายความสัมพันธ์ระหว่างวัตถุต่างๆ ในทางการเขียนโปรแกรมเชิงวัตถุ

แบบรูปความมั่นคงสามารถแบ่งได้เป็น 3 ประเภทคือ

1) *แบบรูปการวิเคราะห์ความมั่นคง* (Security Analysis Patterns) เป็นแบบรูปที่แก้ปัญหาการวิเคราะห์ความมั่นคงของระบบ

2) *แบบรูปการออกแบบความมั่นคง* (Security Design Patterns) เป็นแบบรูปที่แก้ปัญหาการออกแบบโครงสร้างความมั่นคงของระบบ

3) *แบบรูปกระบวนการความมั่นคง* (Security Process Patterns) เป็นแบบรูปที่แก้ปัญหาการออกแบบความมั่นคงให้กับกระบวนการของระบบ

แนวคิดในการพัฒนาแบบรูปความมั่นคงนั้นมีแนวคิดมาจากแบบรูปการออกแบบ [12] โดยแบบรูปความมั่นคงในระยะแรกๆ นั้น Yoder and Barcalow [3] ได้นำเสนอแบบรูปเกี่ยวกับแง่มุมทางด้านความมั่นคงไว้หลายแบบรูป ต่อจากนั้นมาได้มีผู้เสนอแบบรูปความมั่นคงต่างๆ ออกมาอย่างต่อเนื่อง เช่น Kienzle and Elder [2] นำเสนอแบบรูปความมั่นคงที่เกี่ยวกับการพัฒนาโปรแกรมประยุกต์บนเว็บไซต์จำนวน 2 กลุ่ม 29 แบบรูป B. Blakley [1] ได้นำเสนอแบบรูปความมั่นคงจำนวน 2 กลุ่ม 13 แบบรูป และ M.Schumacher et al. [4] ได้นำเสนอแบบรูปความมั่นคงจำนวน 8 กลุ่ม 46 แบบรูป

แบบรูปความมั่นคงที่จะนำมาใช้ในงานวิจัยฉบับนี้คือ แบบรูปของ M.Schumacher et al. [4] ที่นำเสนอในหนังสือแบบรูปความมั่นคง การบูรณาการความมั่นคงและวิศวกรรมระบบ (Security Patterns: Integrating Security and Systems Engineering) เนื่องจากเป็นแบบรูปที่ได้รับความนิยม และแบบรูปที่สร้างขึ้นนั้นสามารถนำไปประยุกต์ใช้กับการพัฒนาซอฟต์แวร์ได้

องค์ประกอบของแบบรูปความมั่นคงของ M.Schumacher et al. [4] ประกอบด้วยองค์ประกอบต่างๆ ดังนี้

1) ชื่อ (Name) เป็น ชื่อของแบบรูปความมั่นคง

2) ชื่อที่รู้จัก (Also Known As) เป็น ชื่ออื่นของแบบรูปความมั่นคง

3) ตัวอย่าง (Example) เป็นตัวอย่างที่แสดงถึงปัญหาและความต้องการของแบบรูปความมั่นคง

4) บริบท (Context) เป็น สถานการณ์ที่ควรใช้แบบรูปความมั่นคง

5) ปัญหา (Problem) เป็น ปัญหาที่แบบรูปความมั่นคงต้องแก้ไข

6) ผลเฉลย (Solution) เป็น คำตอบภายใต้แบบรูปความมั่นคง

7) โครงสร้าง (Structure) เป็น รายละเอียดโครงสร้างของแบบรูปความมั่นคง

8) ไดนามิก (Dynamics) เป็น เหตุการณ์ที่อธิบายถึงการทำงานของแบบรูปความมั่นคง

9) การทำให้เกิดผล (Implementation) เป็น การแนะนำในการทำให้เกิดผล

10) ตัวอย่างการแก้ไข (Example Resolved) เป็น ตัวอย่างการแก้ไขปัญหาด้วยแบบรูปความมั่นคง

11) รูปแปร (Variants) เป็น คำอธิบายของแบบรูปความมั่นคงที่มีลักษณะแตกต่างหรือพิเศษออกไป

12) การนำไปใช้ที่ทราบ (Know Uses) เป็น ตัวอย่างของการใช้แบบรูปความมั่นคงในระบบความเป็นจริง

13) ผลที่ได้ (Consequence) เป็น ประโยชน์ที่ได้จากแบบรูปความมั่นคง

14) เห็นได้จาก (See Also) เป็น การอ้างถึงแบบรูปความมั่นคงอื่นที่แก้ไขปัญหาเดียวกัน

2.1.2 แผนภาพคลาส

แผนภาพคลาส (Class Diagram) [13] [14] คือ แผนภาพที่แสดงกลุ่มของคลาส และความสัมพันธ์ต่างๆ ระหว่างกัน หรือกล่าวอีกนัยหนึ่งได้ว่า แผนภาพคลาส คือ กลุ่มของจุดยอด (Vertices) และเส้นเชื่อม (Arcs) โดยมักใช้แผนภาพคลาสนี้ในการวิเคราะห์ระบบ เป็นการอธิบายว่าในระบบงานหนึ่งๆ นั้นประกอบไปด้วยคลาสอะไรบ้าง แต่ละคลาสมีความสัมพันธ์กันอย่างไร มีลักษณะประจำ และการดำเนินการอะไรบ้าง

องค์ประกอบของแผนภาพคลาส จะประกอบไปด้วยส่วนสำคัญต่างๆ ดังต่อไปนี้

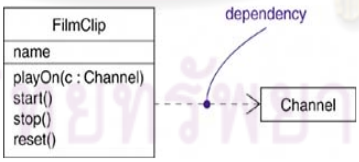
1) *คลาส* ถือเป็นองค์ประกอบที่สำคัญที่สุดในแผนภาพคลาส โดย คลาส คือ กลุ่มของวัตถุที่มีลักษณะประจำ (Attributes) การดำเนินการ (Methods) ร่วมกัน โดยคลาส ประกอบไปด้วยส่วนสำคัญต่างๆ ดังต่อไปนี้

(1) ลักษณะประจำ คือ คุณสมบัติของคลาส

(2) การดำเนินการ คือ บริการที่ถูกระบุไว้สำหรับวัตถุของคลาส

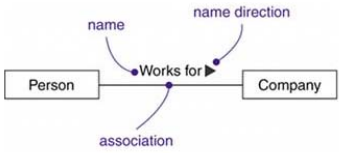
2) *ความสัมพันธ์* (Relationships) มีความสัมพันธ์ที่สำคัญต่างๆ ดังนี้

(1) ความสัมพันธ์แบบดีเพนเดนซี (Dependency) คือ ความสัมพันธ์แบบขึ้นต่อกัน การเปลี่ยนแปลงต่างๆ ที่เกิดขึ้นกับคลาสที่หนึ่ง จะมีผลกระทบต่อคลาสที่สอง มีการใช้สัญลักษณ์ลูกศร โดยให้หัวลูกศรชี้ไปยังคลาสที่มีอิทธิพลกับคลาสอื่น ดังรูปที่ 2.1



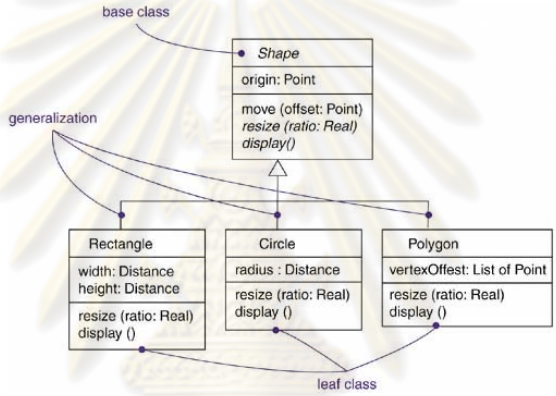
รูปที่ 2.1 ตัวอย่างการใช้ความสัมพันธ์แบบดีเพนเดนซี [13]

(2) ความสัมพันธ์แบบแอซโซซิเอชัน (Association) ใช้เพื่อแสดงการจำลองความสัมพันธ์ระหว่างคลาสที่มีความสัมพันธ์อยู่ในระนาบความสัมพันธ์เดียวกัน ในภาษายูเอ็มแอล จะใช้เส้นตรงที่มีชื่อ และตัวเลขแสดงความสัมพันธ์ (Multiplicity) กำกับเพื่ออธิบายถึงความสัมพันธ์แบบแอซโซซิเอชัน ตัวอย่างแสดงได้ดังรูปที่ 2.2



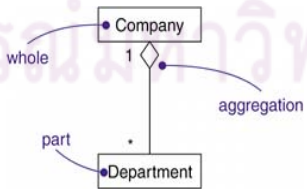
รูปที่ 2.2 ตัวอย่างการใช้ความสัมพันธ์แบบแอซโซซิเอชัน [13]

(3) ความสัมพันธ์แบบเยนเนอร์ไรเซชัน (Generalization) ใช้เพื่ออธิบายความสัมพันธ์ระหว่างคลาสในลักษณะของการจำแนกชนิด การจำเพาะเจาะจงรายละเอียด หรือการหาลักษณะร่วมกันของคลาสที่ต่างชนิดกัน เพื่อสร้างคลาสที่เป็นตัวแทนกลุ่มของคลาสเหล่านั้น ตัวอย่างแสดงได้ดังรูปที่ 2.3



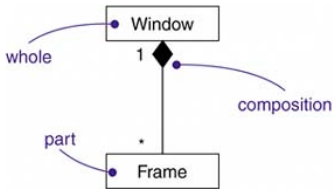
รูปที่ 2.3 ตัวอย่างการใช้ความสัมพันธ์แบบเยนเนอร์ไรเซชัน [13]

(4) ความสัมพันธ์แบบแอกริเกชัน (Aggregation) เป็นการกำหนดความสัมพันธ์ระหว่างคลาส ในลักษณะของการเป็นองค์ประกอบ โดยคลาสที่เป็นองค์ประกอบ เรียกว่า พาร์ทคลาส (Part Class) ส่วนคลาสที่เกิดจากการรวมกันขององค์ประกอบต่างๆ เรียกว่า โฮลคลาส (Whole Class) ตัวอย่างแสดงได้ดังรูปที่ 2.4



รูปที่ 2.4 ตัวอย่างการใช้ความสัมพันธ์แบบแอกริเกชัน [13]

(5) ความสัมพันธ์แบบคอมโพซิชัน (Composition) จะมีลักษณะคล้ายกับความสัมพันธ์แบบแอริเกชัน แต่มีข้อแตกต่างกันอยู่ กล่าวคือ การดำรงอยู่ของโฮลคลาส จะมีผลโดยตรงต่อการมีอยู่ของพาร์ทคลาส ตัวอย่างแสดงได้ดังรูปที่ 2.5



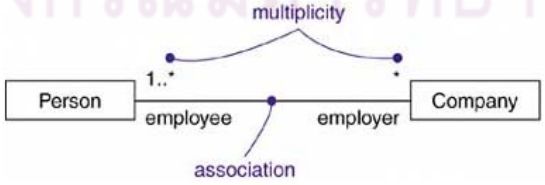
รูปที่ 2.5 ตัวอย่างการใช้ความสัมพันธ์แบบคอมโพซิชัน [13]

3) *ตัวเลขแสดงความสัมพันธ์* (Multiplicity)

ในการพิจารณาความสัมพันธ์ระหว่างคลาส สิ่งที่ควรคำนึงถึงคือ ค่าที่เป็นไปได้ของจำนวนสมาชิกในคลาสหนึ่งๆ ที่มีความสัมพันธ์กันนั้นเป็นเท่าใด โดยตัวเลขแสดงความสัมพันธ์นี้คือ ค่าของจำนวนสมาชิกของคลาสที่เป็นไปได้ในความสัมพันธ์นั้นๆ ซึ่งทำให้ความสัมพันธ์ระหว่างคลาสมีความชัดเจนมากยิ่งขึ้น โดยใช้ตัวเลขแสดงความสัมพันธ์ต่างๆ ดังตารางที่ 2.1 และมีวิธีการเขียนดังรูปที่ 2.6

ตารางที่ 2.1 ความหมายของตัวเลขแสดงความสัมพันธ์

ตัวเลขแสดงความสัมพันธ์	ความหมาย
-	ไม่ระบุ (Unspecified)
1	เพียงหนึ่ง (One)
0..1	ศูนย์หรือหนึ่ง (Zero or One)
0..*	ศูนย์หรือมากกว่า (Zero or More)
1..*	หนึ่งหรือมากกว่า (One or More)
2..4	กำหนดเป็นช่วง 2 ถึง 4 (Specified Range)
2,4..10	กำหนด 2, 4 ถึง 10 (Specified Range)



รูปที่ 2.6 ตัวอย่างการใช้ตัวเลขแสดงความสัมพันธ์ [13]

2.1.3 **บีเอ็นเอฟ** (Backus-Naur Form: BNF) **และอีบีเอ็นเอฟ** (Extended Backus-Naur Form: EBNF)

บีเอ็นเอฟ [15] [16] คือ สัญลักษณ์ที่ใช้ในการอธิบายไวยากรณ์ไม่พึ่งบริบท (Context-free Grammar) ถูกนำเสนอขึ้นโดย John Backus และ Peter Naur บีเอ็นเอฟถูกใช้ในวงกว้าง เช่น ในการระบุไวยากรณ์ของการโปรแกรมคอมพิวเตอร์ ชุดคำสั่ง ตลอดจนโปรโตคอลการติดต่อสื่อสาร

ต่อมา Niklaus Wirth ได้นำเสนอ extended Backus–Naur form (EBNF) [15] ขึ้นมา ซึ่งใช้งานได้ง่ายกว่า และไม่กำกวมเมื่อเปรียบเทียบกับบีเอ็นเอฟแบบเดิม เนื่องจากปัญหาในเรื่องของการใช้สัญลักษณ์ ‘<’ ‘>’ ‘|’ ‘::=’ และการวนซ้ำ (Repetition) ในประโยคยาวๆ ที่ค่อนข้างวกวน [8]

อีบีเอ็นเอฟ เป็นข้อมูลอธิบายภาษาที่กำหนดโดยองค์กรมาตรฐานสากลไอเอสโอ 14977 [17] (International ISO) ในปี1977 โดยพัฒนาต่อยอดมาจากบีเอ็นเอฟเดิม โดยมีกฎทั่วไปดังนี้

1) เทอร์มินอลซิมโบล (Terminal Symbol) จะถูกกำหนดอยู่ภายใต้เครื่องหมายอัญประกาศ (“…”) เสมอ

2) เครื่องหมาย ‘[’ และ ‘]’ เป็นสัญลักษณ์ทางเลือก หมายความว่าสัญลักษณ์ภายในอาจปรากฏหรือไม่ก็ได้

3) เครื่องหมาย ‘{’ และ ‘}’ เป็นสัญลักษณ์การวนซ้ำ หมายความว่า สัญลักษณ์ภายในจะปรากฏได้มากกว่า 1 ครั้ง

4) สามารถใช้เครื่องหมาย ‘(’ และ ‘)’ เพื่อจัดกลุ่มของสัญลักษณ์ได้ ซึ่งมีความหมายเหมือนแนวคิดทางคณิตศาสตร์

5) กรณีที่ต้องใช้สัญลักษณ์พิเศษนอกข้อมูลอื่นๆ จะต้องใช้ภายใต้เครื่องหมาย‘?...?’ เพื่อแสดงสัญลักษณ์พิเศษ

6) กรณีที่ต้องการใส่ข้อคิดเห็น (Comment) จะต้องใช้ภายใต้เครื่องหมาย ‘(*’ และ‘*)’ เท่านั้น ซึ่งจะไม่ถูกนำไปแปลงเป็นผลลัพธ์ภายหลัง

7) ทุกกฎที่ถูกนำเสนอจะต้องแสดงโดยใช้เครื่องหมายมหัพภาค (.) เพื่อแสดงการสิ้นสุดของกฎเสมอ

8) กรณีที่ต้องการยกเว้น (Except) ใช้เครื่องหมาย ‘-’

2.1.4 **การสร้างภาพนามธรรม และ การสร้างภาพนามธรรมของข้อมูล** (Data Visualization)

การสร้างภาพนามธรรม คือ วิธีการหนึ่งสำหรับการสร้างภาพ แผนภาพ หรือภาพเคลื่อนไหว เพื่อใช้ในการสื่อสารข้อความเพื่อทำให้เกิดความเข้าใจที่ชัดเจน มีความเข้าใจตรงกันทั้งผู้ส่งสารและผู้รับสาร การสร้างภาพนามธรรมนั้นจัดได้ว่าเป็นวิธีการที่มีประสิทธิภาพในการสื่อสารถึงสิ่งที่เป็นนามธรรม มองเห็นภาพได้ยาก นำมาสร้างเป็นภาพเพื่อการติดต่อสื่อสารที่ทำความเข้าใจได้ง่ายและชัดเจนมากยิ่งขึ้น ในปัจจุบันการสร้างภาพนามธรรมนั้นได้ถูกนำไปใช้อย่างแพร่หลายในวงกว้าง ไม่ว่าจะเป็น การศึกษา, วิทยาศาสตร์, วิศวกรรม และการแพทย์ [10]

วิธีการสร้างภาพนามธรรมในทางวิทยาศาสตร์นั้นหากแบ่งตามลักษณะของข้อมูลที่นำเสนอแล้วนั้น สามารถแบ่งออกได้เป็น 4 ประเภท [10] ดังนี้

1) ขั้นตอนวิธีแบบสเกลาร์ (Scalar Algorithm) มักใช้ขั้นตอนวิธีนี้กับข้อมูลประเภทตัวเลข

2) ขั้นตอนวิธีแบบเวกเตอร์ (Vector Algorithm) มักใช้ขั้นตอนวิธีนี้กับข้อมูลแบบเวกเตอร์ซึ่งประกอบด้วยตัวเลขและทิศทาง

3) ขั้นตอนวิธีแบบเทนเซอร์ (Tensor Algorithm) มักใช้ขั้นตอนวิธีนี้กับข้อมูลประเภทเมทริกซ์แบบสามมิติ

4) ขั้นตอนวิธีแบบการสร้างตัวแบบ (Modeling Algorithm) มักใช้ขั้นตอนวิธีนี้กับข้อมูลที่ต้องการจะสร้างเป็นตัวแบบ เช่น ข้อมูลเรขาคณิต ข้อมูลพื้นผิวต่างๆ

สำหรับประเภทของการสร้างภาพนามธรรมนั้นสามารถแบ่งออกได้หลายประเภท ตามจุดประสงค์ของการสร้างภาพนามธรรมและประเภทของการนำเสนอ [16] ดังนี้

1) การสร้างภาพนามธรรมของข้อมูล (Data Visualization)

2) การสร้างภาพนามธรรมของสารสนเทศ (Information Visualization)

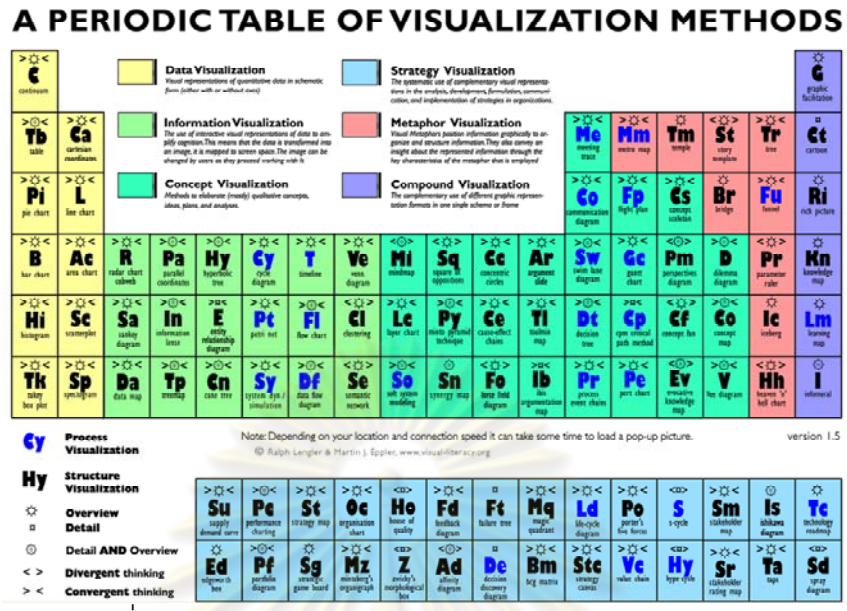
3) การสร้างภาพนามธรรมของแนวคิด (Concept Visualization)

4) การสร้างภาพนามธรรมของกลยุทธ์ (Strategy Visualization)

5) การสร้างภาพนามธรรมของการอุปมาน (Metaphor Visualization)

6) การสร้างภาพนามธรรมของการประกอบ (Compound Visualization)

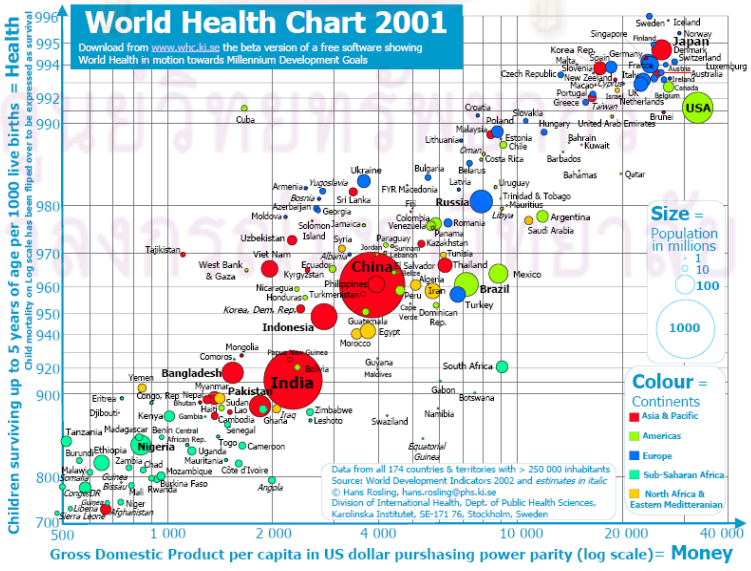
สามารถแสดงได้ดังรูปที่ 2.7 แสดงให้เห็นถึงตารางพีริออดิกของวิธีการสร้างภาพนามธรรม



รูปที่ 2.7 ตารางพีริออดิกของวิธีการสร้างภาพนามธรรม [16]

การสร้างภาพนามธรรมของข้อมูล เป็นวิธีการในการนำเสนอข้อมูลประเภทหนึ่งโดยการใช้แผนภูมิ, กราฟ, เส้นจำนวน, และตาราง เป็นต้น ซึ่งเป็นวิธีการพื้นฐานในการสร้างภาพนามธรรมของข้อมูล นอกจากนี้ยังสามารถเพิ่มเติมการใช้ขนาดของตัวอักษร สีสัน รูปทรง ตลอดจนภาพเคลื่อนไหวต่างๆ เข้ามาประกอบการสร้างภาพได้ด้วย

ตัวอย่างการสร้างภาพนามธรรมของข้อมูลแสดงได้ดังรูปที่ 2.8 โดยในตัวอย่างนี้เป็นการใช้แผนภูมิแบบฟอง (Bubble Chart) แสดงข้อมูลสุขภาพของประชากรโลก [18]



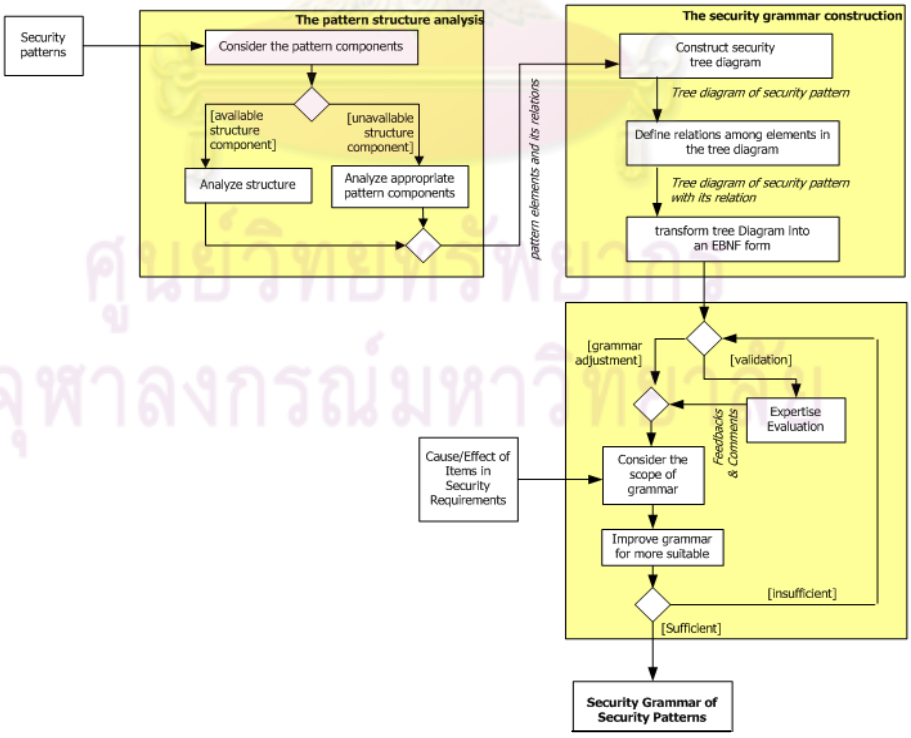
รูปที่ 2.8 แผนภูมิแบบฟอง แสดงข้อมูลสุขภาพของประชากรโลก [18]

2.2 งานวิจัยที่เกี่ยวข้อง

2.2.1 การกำหนดความต้องการด้านความมั่นคงโดยใช้ไวยากรณ์ของแบบรูปความมั่นคง

งานวิจัยนี้ [8] [9] มีวัตถุประสงค์เพื่อสร้างไวยากรณ์ความมั่นคงจากแบบรูปความมั่นคง โดยไวยากรณ์ที่ใช้ในงานวิจัยนี้เป็นไวยากรณ์อีบีเอ็นเอฟ [15] [16] และเครื่องมือที่นำไวยากรณ์ที่ได้มาประยุกต์ใช้ เพื่อใช้กำหนดความต้องการด้านความมั่นคง โดยแบบรูปความมั่นคงที่ใช้นั้นมาจากแบบรูปความมั่นคงของ M.schumacher [4] โดยนำเอาแบบรูปดังกล่าวมาประยุกต์ใช้จำนวนทั้งสิ้น 20 แบบรูป จาก 4 กลุ่ม ได้แก่ การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง การระบุตัวตนและการพิสูจน์ตัวจริง แบบจำลองควบคุมการเข้าถึง และสถาปัตยกรรมไฟล์วอลล์ แล้วสร้างเป็นแผนภาพต้นไม้ความมั่นคง เพื่อแสดงความสัมพันธ์ระหว่างองค์ประกอบของแบบรูปความมั่นคงและแปลงไปเป็นไวยากรณ์ความมั่นคงในรูปอีบีเอ็นเอฟ

กรอบงานของการสร้างไวยากรณ์ความมั่นคงที่ใช้แบบรูปความมั่นคงเป็นพื้นฐานนั้นแสดงได้ดังรูปที่ 2.9 โดยสิ่งที่นำมาพิจารณาใช้ในวิทยานิพนธ์ฉบับนี้ คือ การวิเคราะห์โครงสร้างของแบบรูปความมั่นคง และแบบรูปความมั่นคงที่สัมพันธ์กัน ซึ่งช่วยในการพิจารณาสร้างเป็นแบบจำลองเชิงโครงสร้าง โดยใช้แผนภาพคลาสที่รองรับไวยากรณ์ที่ถูกสร้างขึ้นมาสำหรับแบบรูปความมั่นคง



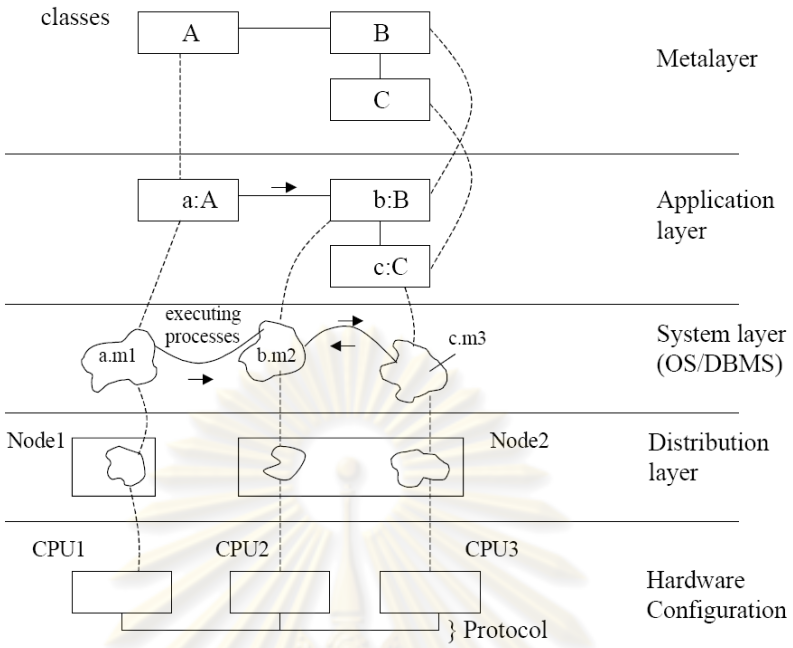
รูปที่ 2.9 กรอบงานของการสร้างไวยากรณ์ความมั่นคงจากแบบรูปความมั่นคง [8]

ไวยากรณ์ความมั่นคงนี้สามารถก่อกำเนิด (generate) เป็นความต้องการด้านความมั่นคงที่สอดคล้องกับแต่ละแบบรูปความมั่นคง [4] โดยอยู่ในรูปแบบของข้อความ (text) แต่อย่างไรก็ตามในการแสดงความสัมพันธ์ความต้องการด้านความมั่นคงระหว่างแบบรูปนั้นยังเป็นข้อจำกัดของงานวิจัยนี้อยู่ ดังนั้นผู้วิจัยจึงได้นำเสนอการสร้างแบบจำลองเชิงโครงสร้างแบบบูรณาการแบบรูปความมั่นคงทั้งหมด และการสร้างภาพนามธรรม เพื่อใช้ในการแสดงความสัมพันธ์ความต้องการด้านความมั่นคงระหว่างแบบรูปความมั่นคง

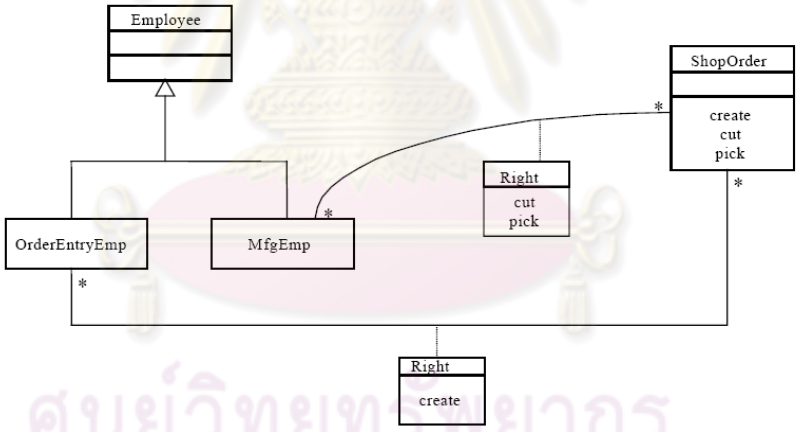
2.2.2 **เมทาดาตาและแบบรูปการให้อำนาจ** (Metadata and authorization patterns)

งานวิจัยนี้ได้นำเสนอแบบรูปการให้อำนาจ [19] ในมุมมองของสถาปัตยกรรมชั้นเมทาดาตาของการโปรแกรมเชิงวัตถุ โดยมีการยกตัวอย่างให้เห็นถึงการประยุกต์ใช้มุมมองของสถาปัตยกรรมชั้นเมทาดาตาของแบบรูปการให้อำนาจนี้ โดยมุมมองสถาปัตยกรรมชั้นเมทาดาตานี้จะช่วยในการควบคุมพฤติกรรม และทิศทางในระดับโปรแกรมประยุกต์ต่อไป

รูปที่ 2.10 แสดงถึงระดับสถาปัตยกรรมในชั้นต่างๆ จะเห็นได้ว่าในชั้นบนสุด คือ ชั้นของเมทาดาตานั้น จะระบุถึงคลาสต่างๆ ที่มีความสัมพันธ์กัน ต่อมาในชั้นของโปรแกรมประยุกต์นั้นก็จะนำคลาสเหล่านั้นมาใช้ โดยทำการสร้างเป็นวัตถุขึ้นมาสำหรับแต่ละคลาส ต่อมาในชั้นของระบบ เป็นการบริการให้การประมวลต่างๆ สามารถกระทำการได้ ต่อมาในชั้นของการกระจาย จะทำการแยกการประมวลผล และวัตถุต่างๆ ออกไปเป็นโหนด (node) ซึ่งแต่ละโหนดอาจจะต้องการใช้หน่วยประมวลผลกลางหนึ่งหน่วย หรือมากกว่าก็ได้ อีกทั้งยังมีการเชื่อมโยงกันในระหว่างเครือข่ายโดยการใช้งานโพรโทคอลต่างๆ ในชั้นของโครงแบบฮาร์ดแวร์ ส่วนในรูปที่ 2.11 แสดงให้เห็นถึงแบบจำลองเชิงโครงสร้างของแบบรูปการให้อำนาจโดยใช้แผนภาพคลาส



รูปที่ 2.10 ระดับสถาปัตยกรรมในชั้นต่างๆ [19]



รูปที่ 2.11 ตัวอย่างแผนภาพคลาสของแบบรูปการให้อำนาจ (Authorization) [19]

สิ่งที่นำมาพิจารณาใช้ในวิทยานิพนธ์นี้ คือ การสร้างแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคงนั้นสามารถกระทำได้ในรูปแบบของการใช้แผนภาพคลาส โดยควรมีการพิจารณาถึงสถาปัตยกรรมในชั้นเมทาดาตา คือ ขั้นตอนในการสร้างคลาสต่างๆ และความสัมพันธ์ระหว่างคลาส และสถาปัตยกรรมในชั้นโปรแกรมประยุกต์ คือ การนำคลาสเหล่านั้นไปสร้างเป็นวัตถุ เพื่อใช้ในการพัฒนาโปรแกรมประยุกต์ต่อไป แต่อย่างไรก็ตามแบบจำลองเชิงโครงสร้างของงานวิจัยนี้ยังไม่มีการระบุลักษณะประจำ และการดำเนินลงไป ซึ่งอาจจะทำให้ผู้พัฒนาระบบยังไม่สามารถใช้ประโยชน์จากแบบจำลองเชิงโครงสร้างได้อย่างมีประสิทธิภาพเท่าที่ควร ดังนั้นผู้วิจัยจึงได้

นำเสนอแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคง โดยระบุลักษณะประจำ และการดำเนินการ เพื่อทำให้ผู้พัฒนาระบบสามารถใช้ประโยชน์จากแบบจำลองได้อย่างสะดวก

2.2.3 **แบบรูปการออกแบบความมั่นคง** (Security Design Patterns)

งานวิจัยแบบรูปการออกแบบความมั่นคง [1] นำเสนอกลวิธีในการออกแบบแบบรูปความมั่นคง และตัวอย่างแบบรูปความมั่นคง โดยมีวัตถุประสงค์เพื่อนำเสนอแนวทางในการออกแบบแบบรูปความมั่นคงให้อยู่ในแบบแผนเดียวกัน ซึ่งกลวิธีเหล่านี้จะทำให้การออกแบบแบบรูปความมั่นคงทำได้อย่างมีประสิทธิภาพ สอดคล้องกับความต้องการของผู้พัฒนาระบบและผู้เชี่ยวชาญทางด้านความมั่นคง

กลวิธีในการออกแบบแบบรูปความมั่นคงที่ดีนั้น ประกอบไปด้วย

1) แบบรูปความมั่นคงที่ดีจะต้องอธิบายปัญหาใด เพียงปัญหาหนึ่งเท่านั้น

2) แบบรูปความมั่นคงที่ดีจะต้องอธิบายรายละเอียดเนื้อหาเมื่อปัญหานั้นๆ เกิดขึ้น

3) แบบรูปความมั่นคงที่ดีจะต้องอธิบายผลเฉลย ในรูปแบบของเอนติตีในการสร้างซอฟต์แวร์

4) แบบรูปความมั่นคงที่ดีจะต้องอธิบายขั้นตอนการออกแบบ หรือกฎของการสร้างผลเฉลย

5) แบบรูปความมั่นคงที่ดีจะต้องเป็นแรงผลักดันเพื่อนำไปสู่ผลเฉลยของปัญหา

6) แบบรูปความมั่นคงที่ดีจะอธิบายให้เห็นถึงตัวอย่างที่ผลเฉลยสามารถแก้ปัญหาได้

7) แบบรูปความมั่นคงที่ดีจะต้องอธิบายรายละเอียดในแง่มุมต่างๆ ที่หลากหลาย

8) แบบรูปความมั่นคงที่ดีจะต้องอธิบายให้เห็นถึงตัวอย่างการใช้งานของแบบรูปอย่างน้อย 1 ตัวอย่าง

9) แบบรูปความมั่นคงที่ดีจะต้องอธิบายให้เห็นถึงตัวอย่างการใช้งานระหว่างแบบรูปต่างๆ

10) แบบรูปความมั่นคงที่ดีจะต้องอธิบาย หรืออ้างอิงรูปแปรของแบบรูปย่อยๆ ได้

11) แบบรูปความมั่นคงที่ดีจะต้องอธิบาย หรืออ้างอิงไปยังแบบรูปอื่นๆ ที่สัมพันธ์กันได้

12) แบบรูปความมั่นคงที่ดีจะต้องอธิบาย หรืออ้างอิงไปยังแบบรูปอื่นๆ ที่ขึ้นต่อแบบรูปนี้ได้

งานวิทยานิพนธ์จะนำกลวิธีในการออกแบบแบบรูปความมั่นคงรวมถึงแนวทาง และข้อแนะนำต่างๆ ในการออกแบบแบบรูปความมั่นคงให้มีประสิทธิภาพ นำมาประยุกต์ใช้ในการออกแบบแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคง โดยใช้แผนภาพคลาส

2.2.4 **มุมมองของการสร้างภาพนามธรรม** (Views on Visualization)

งานวิจัยนี้ [11] ได้อธิบายถึง ในการพิจารณาประโยชน์และคุณค่าของการสร้างภาพนามธรรมที่ดีนั้น ควรจะต้องพิจารณาออกเป็นหลายมุมมองด้วยกัน ซึ่งประกอบไปด้วย มุมมองทางด้านเทคโนโลยี ซึ่งในปัจจุบันมีการพัฒนาไปอย่างรวดเร็ว ซึ่งคุณค่าของการสร้างภาพนามธรรมนั้นจะถูกวัดจากประโยชน์ และประสิทธิภาพที่ได้ มุมมองทางด้านเศรษฐกิจนั้นสามารถประเมินได้จากผลประโยชน์ที่ได้ และค่าใช้จ่ายที่ต้องเสียไป มุมมองทางด้านผลกระทบและข้อจำกัด เช่น ค่าใช้จ่ายที่สิ้นเปลืองต่างๆ และบทบาทของการปฏิสัมพันธ์ระหว่างผู้ใช้งาน นอกจากนี้ยังนำเสนอมุมมองทางเลือกใหม่ ของการสร้างภาพนามธรรม ประกอบด้วย ศิลปะของการสร้างภาพนามธรรม, การออกแบบภาพนามธรรม และการสร้างภาพนามธรรมในมุมมองทางวิทยาศาสตร์ ดังรูปที่ 2.12

รูปที่ 2.12 มุมมองของการสร้างภาพนามธรรม [11]

สิ่งที่นำมาพิจารณาใช้ในวิทยานิพนธ์นี้ คือ การพิจารณาประโยชน์และคุณค่าของการสร้างภาพนามธรรมที่ดีนั้นประกอบไปด้วยสิ่งใดบ้าง เพื่อเป็นแนวทางในการออกแบบการสร้างเครื่องมือเพื่อแสดงผลภาพนามธรรม เพื่อให้ภาพนามธรรมที่ได้มีประโยชน์ และประสิทธิภาพที่ดี

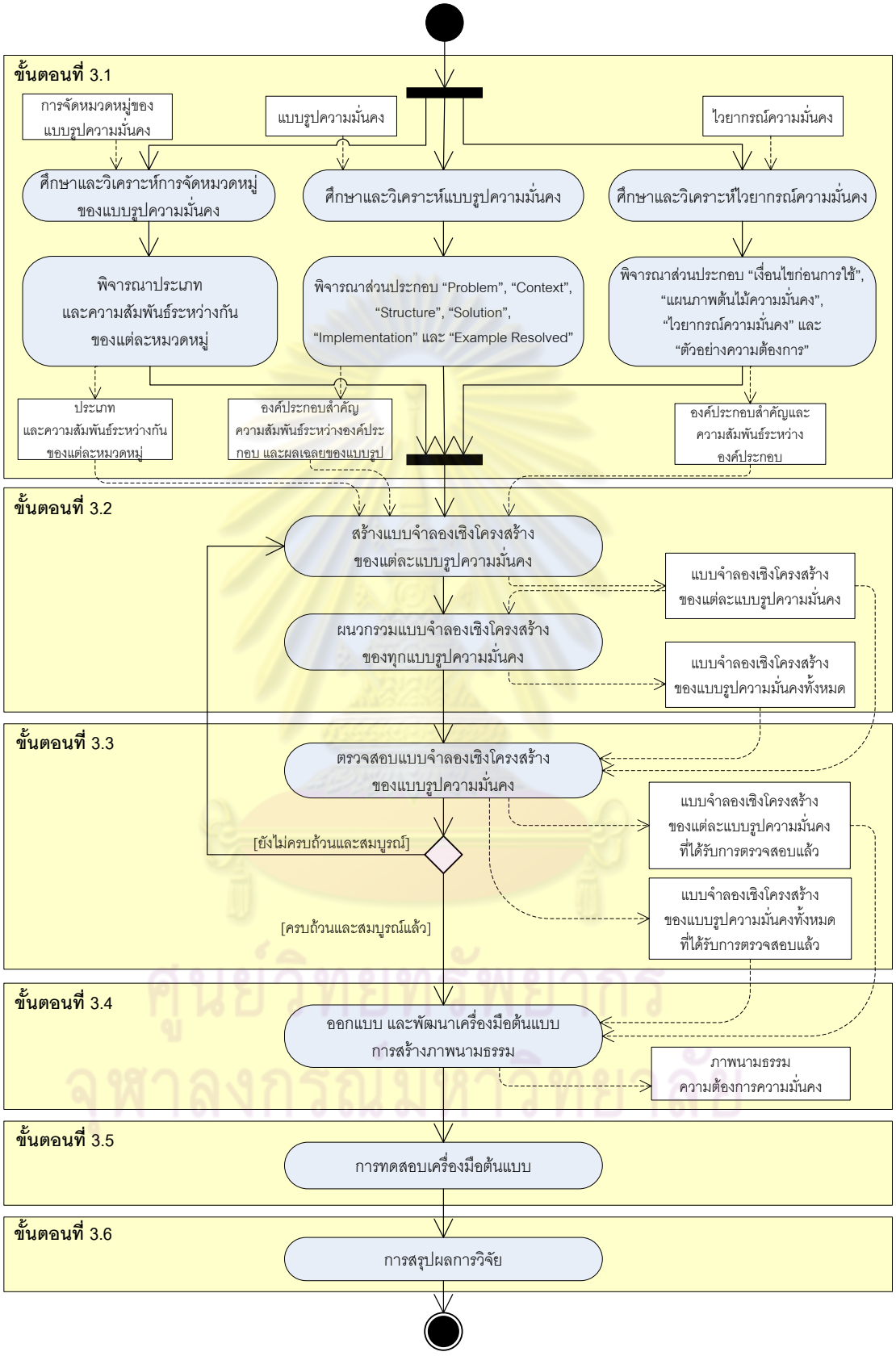
บทที่ 3
การวิเคราะห์แบบรูปความมั่นคง ไวยากรณ์ความมั่นคง และการออกแบบแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคง

งานวิจัยนี้แบ่งขั้นตอนการดำเนินงานออกเป็น 6 ส่วนหลัก สามารถแสดงได้ดังแผนภาพกิจกรรมดังรูปที่ 3.1

พิจารณารูปที่ 3.1 ในขั้นตอนที่ 3.1 การศึกษาและวิเคราะห์การจัดหมวดหมู่ของแบบรูปความมั่นคง แบบรูปความมั่นคง และไวยากรณ์ความมั่นคงเป็นขั้นตอนเริ่มต้นของการดำเนินงาน โดยแบ่งออกเป็น 3 ขั้นตอนย่อย คือ ขั้นตอนที่ 3.1.1 คือ การศึกษาและวิเคราะห์การจัดหมวดหมู่ของแบบรูปความมั่นคง เพื่อหาหมวดหมู่และประเภทของแบบรูปความมั่นคง และความสัมพันธ์ในแต่ละหมวดหมู่ ขั้นตอน 3.1.2 การศึกษาและวิเคราะห์แบบรูปความมั่นคง เพื่อหาองค์ประกอบสำคัญและผลเฉลยภายในแบบรูปความมั่นคง และขั้นตอน 3.1.3 คือ การศึกษาและวิเคราะห์ไวยากรณ์ความมั่นคง เพื่อหาส่วนประกอบสำคัญและความสัมพันธ์ระหว่างแบบรูปความมั่นคง โดยแบบรูปความมั่นคงที่นำมาใช้ในงานวิจัยนี้รวมทั้งสิ้น 20 แบบรูป ครอบคลุม 4 กลุ่มความมั่นคง ได้แก่ การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง การระบุตัวตนและการพิสูจน์ตัวจริง แบบจำลองควบคุมการเข้าถึง และสถาปัตยกรรมไฟล์วอลล์ ซึ่งผลลัพธ์จากขั้นตอนนี้คือ รายการประเภท หมวดหมู่ความสัมพันธ์ระหว่างกันในแต่ละหมวดหมู่ และองค์ประกอบสำคัญของแบบรูปความมั่นคง

ขั้นตอนที่ 3.2 แสดงขั้นตอนการสร้างแบบจำลองเชิงโครงสร้างที่สอดคล้องกับแบบรูปความมั่นคงและไวยากรณ์ความมั่นคง ซึ่งต้องใช้ผลลัพธ์รายการประเภท หมวดหมู่ความสัมพันธ์ระหว่างกันในแต่ละหมวดหมู่ และองค์ประกอบสำคัญของแบบรูปความมั่นคงของขั้นตอน 3.1 มาใช้ ส่วนขั้นตอน 3.2.1 เป็นการสร้างเป็นแบบจำลองเชิงโครงสร้างของแต่ละแบบรูปโดยใช้แผนภาพคลาส และในขั้นตอน 3.2.2 เป็นการผนวกรวมแบบจำลองเชิงโครงสร้างของแต่ละแบบรูป ให้ได้เป็นแผนภาพคลาสแบบบูรณาการของแบบรูปความมั่นคงทั้งหมด

ขั้นตอนที่ 3.3 แสดงการตรวจสอบแบบจำลองเชิงโครงสร้างที่ได้ถูกสร้างขึ้นไว้ในขั้นตอน 3.2.1 และ 3.2.2 เพื่อทำให้การบูรณาการแบบจำลองมีความสมบูรณ์และถูกต้องมากยิ่งขึ้น โดยรายละเอียดของแต่ละขั้นตอนจะกล่าวถึงในหัวข้อ 3.1 3.2 และ 3.3 ตามลำดับ สำหรับรายละเอียดในขั้นตอน 3.4 3.5 และ 3.6 ที่เกี่ยวข้องกับการสร้างเครื่องมือต้นแบบ การทดสอบเครื่องมือ และการสรุปผลการวิจัย จะกล่าวถึงต่อไปในบทที่ 4 บทที่ 5 และ บทที่ 6 ตามลำดับ

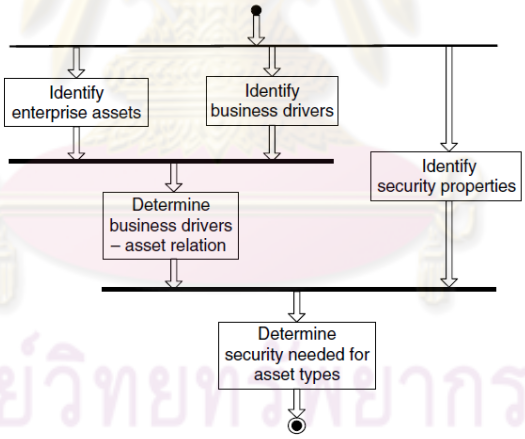


รูปที่ 3.1 แผนภาพขั้นตอนการดำเนินการวิจัย

เพื่อความสะดวกในการทำความเข้าใจในการสร้างแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคงในบทนี้ ผู้วิจัยได้ใช้แบบรูปการระบุความต้องการด้านความมั่นคงสำหรับสินทรัพย์องค์กรมาเป็นกรณีศึกษา ซึ่งเป็นแบบรูปความมั่นคงในกลุ่มการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง เป็นแบบรูปเริ่มต้นสำหรับการพิจารณาความมั่นคงองค์กร มีวัตถุประสงค์เพื่อการกำหนดความต้องการด้านความมั่นคงที่จำเป็นต้องมีในองค์กร เพื่อนำคุณสมบัติด้านความมั่นคง (การรักษาความลับ ความบูรณภาพ สภาพพร้อมใช้งาน และภาระรับผิดชอบ) มาประยุกต์ใช้ ทั้งนี้จะมีการพิจารณาจากตัวขับเคลื่อนทางธุรกิจเป็นหลัก ลำดับขั้นตอนการทำงานของแบบรูป มีขั้นตอนดังนี้

1) ระบุสินทรัพย์
2) ระบุตัวขับเคลื่อนทางธุรกิจ
3) ระบุความสัมพันธ์ระหว่างสินทรัพย์และตัวขับเคลื่อนทางธุรกิจ
4) กำหนดคุณสมบัติด้านความมั่นคง
5) ระบุคุณสมบัติด้านความมั่นคงให้กับสินทรัพย์โดยพิจารณาจากตัวขับเคลื่อนทางธุรกิจ

สามารถแสดงภาพขั้นตอนการทำงานได้ดังรูปที่ 3.2



รูปที่ 3.2 ลำดับขั้นตอนการทำงานของแบบรูปการระบุความต้องการด้านความมั่นคงสำหรับสินทรัพย์องค์กร [4]

3.1 การศึกษาและวิเคราะห์การจัดหมวดหมู่ของแบบรูปความมั่นคง แบบรูปความมั่นคงและไวยากรณ์ความมั่นคง

การศึกษาและวิเคราะห์การจัดหมวดหมู่ของแบบรูปความมั่นคง แบบรูปความมั่นคงและไวยากรณ์ความมั่นคง เพื่อให้ได้รายการองค์ประกอบสำคัญในการสร้างแบบจำลองเชิงโครงสร้าง แบ่งออกเป็น 3 ขั้นตอนย่อย คือ การศึกษาและวิเคราะห์การจัดหมวดหมู่แบบรูปความ

มั่นคง การศึกษาและวิเคราะห์โครงสร้างแบบรูปความมั่นคง และการศึกษาและวิเคราะห์ไวยากรณ์ความมั่นคง

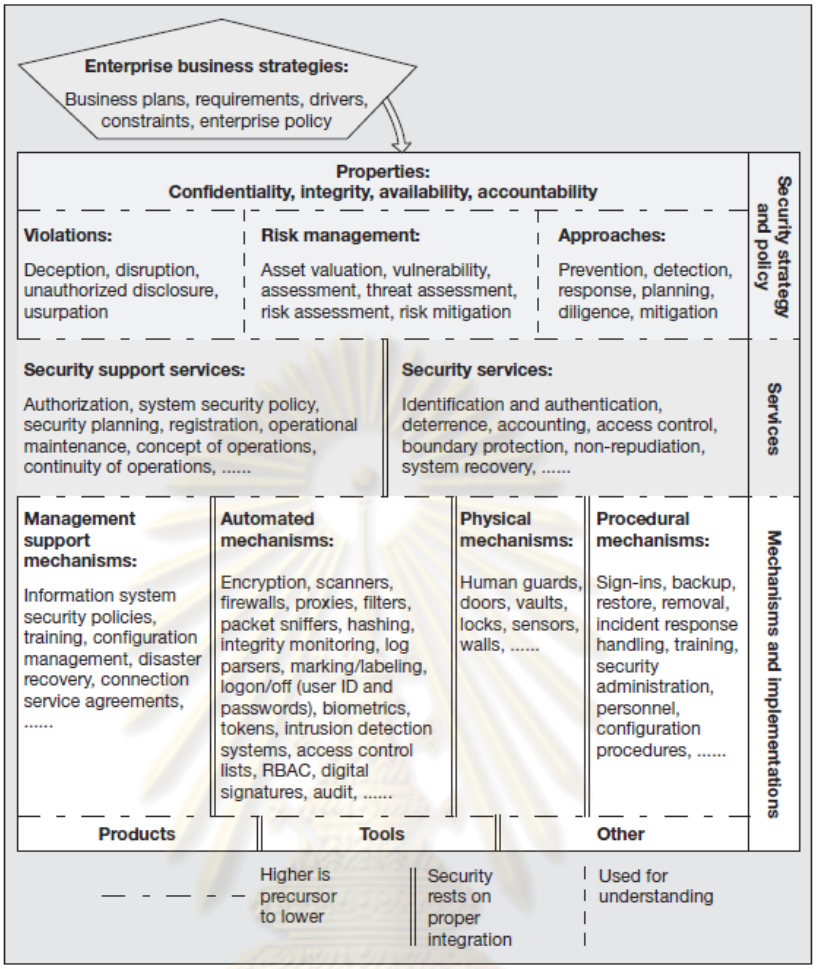
3.1.1 การศึกษาและวิเคราะห์การจัดหมวดหมู่แบบรูปความมั่นคง

การศึกษาและวิเคราะห์การจัดหมวดหมู่แบบรูปความมั่นคงเป็นการพิจารณาถึงประเภทและความสัมพันธ์ของแต่ละหมวดหมู่ โดยในขั้นตอนนี้จะเป็นการวิเคราะห์ส่วนประกอบสำคัญที่จะช่วยให้ผู้วิจัยสามารถทราบถึงความสัมพันธ์ของแบบรูปความมั่นคงในแต่ละหมวดหมู่ ว่ามีความเกี่ยวข้อง และแบบรูปสามารถสนับสนุนกันได้อย่างไร เพื่อจะนำข้อมูลที่ได้จากการวิเคราะห์นี้ไปวิเคราะห์และออกแบบการสร้างภาพนามธรรมของแบบรูปความมั่นคงต่อไป

พิจารณารูปที่ 3.3 การจัดหมวดหมู่ของแบบรูปความมั่นคง [4] แบ่งออกเป็น 3 ชั้น คือ กลยุทธ์และนโยบายความมั่นคง (Security Strategy and Policy) การบริการ (Service) และ กลไกและการนำไปปฏิบัติ (Mechanisms and Implementations) ซึ่งมีข้อมูลกลยุทธ์ทางธุรกิจขององค์กรเป็นข้อมูลนำเข้าเริ่มต้น ข้อมูลเหล่านี้มีความสำคัญแต่ก็ถูกจัดให้อยู่นอกหมวดหมู่ของแบบรูปความมั่นคง

พิจารณาหมวดหมู่แรก คือ กลยุทธ์และนโยบายความมั่นคง ซึ่งจัดอยู่ในชั้นบนสุด โดยทั่วไปแล้วผู้บริหารต้องการให้กิจกรรม การดำเนินงานต่างๆ ขององค์กรบรรลุเป้าหมายขององค์กรที่ได้วางเอาไว้ วิธีการหนึ่งที่จำเป็น และมีความสำคัญคือ การวางแผนนโยบายทางด้านความมั่นคง ซึ่งประกอบไปด้วย 4 กลุ่มย่อย คือ การกำหนดคุณสมบัติทางด้านความมั่นคง (Properties) การฝ่าฝืนทางด้านความมั่นคง (Violations) การจัดการความเสี่ยง (Risk Management) และแนวคิดความมั่นคง (Approaches)

พิจารณาหมวดหมู่ที่สอง คือ การบริการ โดยการบริการนี้จะเป็นตัวช่วยให้กิจกรรมขององค์กร และนโยบายความมั่นคงองค์กรที่ระบุไว้ในหมวดหมู่แรกสามารถบรรลุเป้าหมายได้ การบริการสามารถแบ่งออกเป็น 2 กลุ่มย่อย คือ การบริการสนับสนุนความมั่นคง (Security Support Services) และ การบริการความมั่นคง (Security Services) ตัวอย่างเช่น หากพิจารณาตัวอย่างของการลงทะเบียน (Registration) ซึ่งจัดอยู่ในกลุ่มย่อยการบริการสนับสนุนความมั่นคง โดยเก็บรวมรวมข้อมูลที่จำเป็นต่างๆ เช่น ข้อมูลประจำตัวนิสิต ข้อมูลรายวิชา เพื่อสนับสนุนกลุ่มแบบรูปการระบุและพิสูจน์ตัวตน (Identification and Authentication) ซึ่งจัดอยู่ในกลุ่มย่อยการบริการความมั่นคง เป็นต้น



รูปที่ 3.3 การจัดหมวดหมู่ของแบบรูปความมั่นคง [4]

พิจารณาหมวดหมู่ที่สาม คือ กลไกและการนำไปปฏิบัติ ซึ่งการนำเอาการบริการความมั่นคงจากหมวดหมู่ที่สองไปปฏิบัติใช้จริงได้นั้น ย่อมต้องการการสนับสนุนการทำให้เกิดผลจากหมวดหมู่ที่สามนี้ โดยการบริการความมั่นคงสามารถเลือกใช้ได้หลายๆ กลไก ในขณะเดียวกันในแต่ละกลไกก็สามารถช่วยสนับสนุนได้หลายๆ บริการความมั่นคงเช่นกัน หมวดหมู่กลไกและการนำไปปฏิบัตินี้สามารถแบ่งออกเป็น กลไกการสนับสนุนการจัดการ (Management Support Mechanisms) จะเป็นกลไกที่คอยควบคุมกลไกสนับสนุนตัวอื่นๆ กลไกอัตโนมัติ (Automated Mechanisms) เป็นกลไกที่สนับสนุนบริการความมั่นคงอย่างอัตโนมัติ โดยอาศัยวิธีการทางด้านเทคโนโลยีสารสนเทศ กลไกทางกายภาพ (Physical Mechanisms) เป็นกลไกตอบสนองบริการความมั่นคงทางกายภาพ ยกตัวอย่างเช่น ตึก อาคารที่มีระบบรักษาความปลอดภัย รวมถึงเจ้าหน้าที่รักษาความปลอดภัย และกลไกกระบวนการ (Procedural Mechanisms) เป็นกลไกตอบสนอง และสนับสนุนการบริการความมั่นคงที่เกิดขึ้น ยกตัวอย่างเช่น การกำหนดให้มีการ

เปลี่ยนรหัสผ่านสำหรับการลงทะเบียนเข้าสู่ระบบ (Sign In) เป็นประจำ หรือการกำหนดให้มีการสำรองข้อมูลไว้ทุกๆ 1 เดือน เป็นต้น

หากพิจารณากรณีตัวอย่างแบบรูปการระบุความต้องการด้านความมั่นคงสำหรับสินทรัพย์องค์กร จากข้อมูลการศึกษาและวิเคราะห์การจัดหมวดหมู่ของแบบรูปความมั่นคงแล้วนั้น ทำให้ทราบว่าแบบรูปนี้จัดอยู่ในหมวดหมู่กลยุทธ์และนโยบายความมั่นคง ซึ่งควรมีการกำหนดความต้องการด้านความมั่นคง ซึ่งในที่นี้คือ คุณสมบัติความมั่นคง อันประกอบไปด้วย การรักษาความลับ (Confidentiality) ความบูรณภาพ (Integrity) สภาพพร้อมใช้งาน (Availability) และสภาวะรับผิดชอบ (Accountability) โดยพิจารณาจากข้อมูลนำเข้า คือ ข้อมูลกลยุทธ์ทางธุรกิจขององค์กร มาเป็นหลักในการพิจารณา โดยหลังจากการกำหนดคุณสมบัติความมั่นคงแล้ว หากพิจารณาจากการจัดหมวดหมู่ของแบบรูปความมั่นคงข้างต้น จะเห็นได้ว่าแบบรูปความมั่นคงที่นำมาเป็นกรณีศึกษานี้ จะมีความสัมพันธ์กับแบบรูปการจัดการความเสี่ยง และแบบรูปการกำหนดแนวคิดความมั่นคง เป็นต้น

3.1.2 การศึกษาและวิเคราะห์โครงสร้างแบบรูปความมั่นคง

การศึกษาและวิเคราะห์โครงสร้างแบบรูปความมั่นคงเป็นการพิจารณาโครงสร้างหรือส่วนประกอบของเอกสารแบบรูปความมั่นคงที่ได้นำเสนอไว้ใน [4] โดยในขั้นตอนนี้จะเป็นการวิเคราะห์ส่วนประกอบสำคัญที่จะช่วยให้ผู้วิจัยสามารถทราบถึงองค์ประกอบสำคัญภายในแบบรูปความมั่นคง เพื่อนำองค์ประกอบ และความสัมพันธ์ระหว่างแบบรูปความมั่นคงที่ได้จากการวิเคราะห์ นำมาสร้างเป็นแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคง โดยมีรายละเอียดการวิเคราะห์ดังต่อไปนี้

3.1.2.1 การวิเคราะห์โครงสร้างแบบรูปความมั่นคงจากส่วนประกอบ “Problem” “Context” และ “Structure”

ส่วนประกอบ “Problem” เป็นส่วนประกอบที่แสดงถึงปัญหาของแบบรูปความมั่นคงที่ต้องแก้ไข ผลลัพธ์จากการวิเคราะห์ส่วนประกอบนี้คือ การทราบถึงเป้าหมายหลักของแบบรูปความมั่นคงนี้มุ่งเน้นแก้ไข เพื่อใช้เป็นข้อมูลในการพิจารณาสร้างแบบจำลองเชิงโครงสร้าง ส่วนประกอบ “Context” เป็นส่วนประกอบที่แสดงถึงสถานการณ์ที่เหมาะสมในการประยุกต์ใช้แบบรูปความมั่นคง ผลลัพธ์จากการวิเคราะห์ส่วนประกอบนี้คือ การทราบถึงแบบรูปความมั่นคงที่เกี่ยวข้อง และขึ้นต่อกัน และส่วนประกอบ “Structure” เป็นส่วนประกอบที่แสดงถึงรายละเอียดและข้อกำหนดของคุณลักษณะเชิงโครงสร้างของแบบรูปความมั่นคง ผลลัพธ์จากการวิเคราะห์

ส่วนประกอบนี้คือ การทราบถึงโครงสร้างของแบบรูปความมั่นคงเพื่อใช้เป็นแนวทางในการพิจารณาในการสร้างแบบจำลองเชิงโครงสร้าง

จากการพิจารณาทั้ง 3 ส่วนประกอบของแบบรูปการระบุความต้องการด้านความมั่นคงสำหรับสินทรัพย์องค์กร จะได้รายการองค์ประกอบสำคัญ ที่นำมาพิจารณาในการสร้างแบบจำลองเชิงโครงสร้างของแบบรูปการกำหนดค่าความเสี่ยงดังนี้

1) Asset คือ สินทรัพย์ขององค์กร โดยจะต้องมีการกำหนดคุณสมบัติความมั่นคงให้แก่สินทรัพย์นั้นๆ และจะถูกกำหนดให้เป็นชื่อคลาส

2) SecurityProperty คือ คุณสมบัติความมั่นคง ซึ่งสามารถมีค่าที่เป็นไปได้คือ การรักษาความลับ ความบูรณภาพ สภาพพร้อมใช้งาน และภาระรับผิดชอบ และต่อมาจะถูกกำหนดให้เป็นชื่อคลาส

3) BusinessDriver คือ ตัวขับเคลื่อนทางธุรกิจ ซึ่งเป็นสิ่งที่แต่ละองค์กรระบุไว้ ซึ่งต่อมาจะถูกกำหนดให้เป็นชื่อคลาส

4) AssetType คือ ประเภทของสินทรัพย์ สามารถมีค่าที่เป็นไปได้คือ ประเภทข้อมูล และประเภทกายภาพ ต่อมาจะถูกกำหนดให้เป็นลักษณะประจำภายในคลาส Asset

3.1.2.2 การวิเคราะห์โครงสร้างแบบรูปความมั่นคงจากส่วนประกอบ “Solution” และ “Implementation”

ส่วนประกอบ “Solution” เป็นส่วนประกอบที่แสดงถึงแนวทาง หรือผลเฉลยในการแก้ไขปัญหา (ซึ่งส่วนประกอบ “Problem” ได้กล่าวถึงปัญหาของแบบรูปไว้) ส่วนประกอบ “Implementation” เป็นส่วนประกอบที่แสดงถึงการนำเสนอวิธีการในทางปฏิบัติเพื่อแก้ไขปัญหา (ซึ่งส่วนประกอบ “Solution” ได้นำเสนอแนวทางเอาไว้) ผลลัพธ์จากการวิเคราะห์ทั้ง 2 ส่วนประกอบนี้คือ ทำให้ทราบถึงเซตขององค์ประกอบที่จำเป็นที่ใช้ในการพิจารณาสร้างแบบจำลองเชิงโครงสร้าง กล่าวคือ นำมาพิจารณาเป็นชื่อคลาส ชื่อลักษณะประจำ หรือชื่อของการดำเนินการ

จากการพิจารณาทั้ง 2 ส่วนประกอบของแบบรูปการกำหนดค่าความเสี่ยง จะได้รายการองค์ประกอบสำคัญนอกเหนือจากส่วนประกอบที่ได้จากหัวข้อ 3.1.2.1 ซึ่งจะนำมาพิจารณาในการสร้างแบบจำลองเชิงโครงสร้างของแบบรูปการกำหนดค่าความเสี่ยงดังนี้

1) Asset-Security Property คือ รหัสของสินทรัพย์ และ รหัสของคุณสมบัติความมั่นคง ซึ่งจะถูกกำหนดให้เป็นชื่อคลาสเชื่อมโยง (Association Class)

2) SetSecurityProperty คือ วิธีการในการกำหนดคุณสมบัติความมั่นคงซึ่งจะถูกกำหนดให้เป็นการดำเนินการภายในคลาส SecurityProperty

3) SetBusinessDriver คือ วิธีการในการกำหนดตัวขับเคลื่อนทางธุรกิจให้กับสินทรัพย์ ซึ่งจะถูกกำหนดให้เป็นการดำเนินการภายในคลาส BusinessDriver

3.1.2.3 การวิเคราะห์โครงสร้างแบบรูปความมั่นคงจากส่วนประกอบ “Example Resolved”

ส่วนประกอบ “Example Resolved” เป็นการพิจารณาคุณลักษณะสำคัญ หรือตัวอย่างผลลัพธ์ที่ได้จากการแก้ปัญหา ผลลัพธ์จากการวิเคราะห์ส่วนประกอบนี้คือ ทำให้ทราบถึงตัวอย่างที่ชัดเจนของค่าที่เป็นไปได้ในแต่ละเซตขององค์ประกอบที่ได้จากขั้นตอน 3.1.2.1 และ 3.1.2.2

จากการพิจารณาส่วนประกอบ “Example Resolved” ทำให้ทราบถึงค่าที่เป็นไปได้ของ AssetType ซึ่งจะประกอบด้วย Information Type ตัวอย่างเช่น Employee Data, Financial/Insurance Data, Contractual Data and Business Planning Advertisements and Other Public Data และ Physical Type ยกตัวอย่างเช่น Building Staff Collections and Exhibits Transport Vehicles เป็นต้น

3.1.3 การศึกษาและวิเคราะห์โครงสร้างไวยากรณ์ความมั่นคง

การศึกษาและวิเคราะห์โครงสร้างไวยากรณ์ความมั่นคงเป็นการพิจารณาโครงสร้างหรือส่วนประกอบของไวยากรณ์ความมั่นคงที่ได้นำเสนอไว้ใน [8] โดยในขั้นตอนนี้จะเป็นการวิเคราะห์ส่วนประกอบสำคัญที่จะช่วยให้ผู้วิจัยสามารถทราบถึงองค์ประกอบสำคัญภายในไวยากรณ์ความมั่นคง ซึ่งประกอบไปด้วย ความสัมพันธ์ระหว่างแบบรูป ชื่อคลาส และลักษณะประจำ รวมถึงตัวอย่างค่าที่เป็นไปได้ เพื่อนำองค์ประกอบ และความสัมพันธ์ระหว่างแบบรูปความมั่นคงที่ได้จากการวิเคราะห์ นำมาสร้างเป็นแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคง โดยมีรายละเอียดการวิเคราะห์ดังต่อไปนี้

3.1.3.1 การวิเคราะห์โครงสร้างไวยากรณ์ความมั่นคงจากส่วนประกอบ “เงื่อนไขก่อนการใช้”

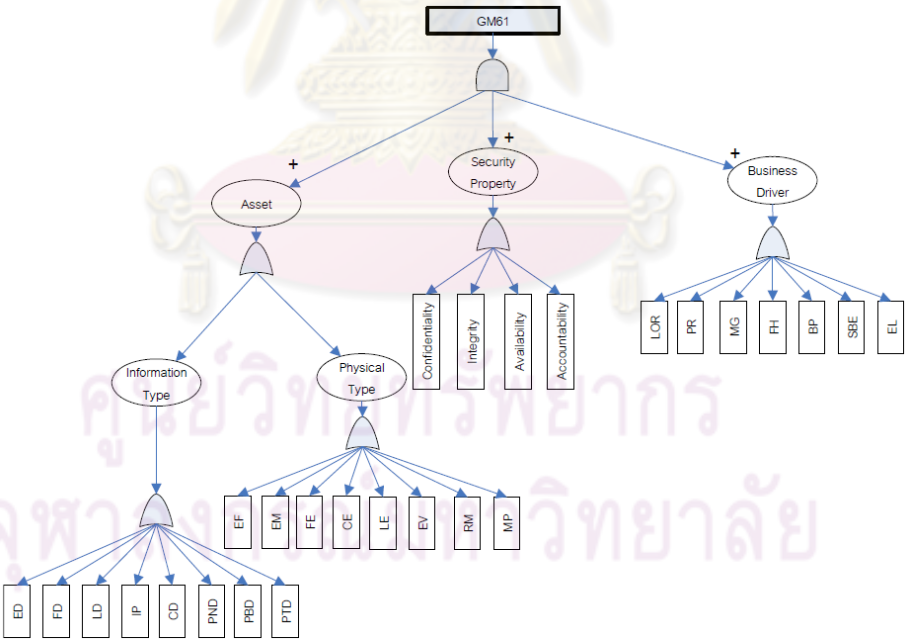
ส่วนประกอบ “เงื่อนไขก่อนการใช้” เป็นส่วนประกอบที่ใช้แสดงเงื่อนไขที่จำเป็นต้องมี หรือควรมี ก่อนจะใช้ไวยากรณ์แบบรูปความมั่นคงนั้นๆ ผลลัพธ์จากการวิเคราะห์ส่วนประกอบนี้คือ ทำให้ทราบถึงความสัมพันธ์ระหว่างแบบรูปความมั่นคงที่เกี่ยวข้อง และขึ้นต่อ

กัน ตัวอย่างเช่น จากแบบรูปการกำหนดมูลค่าสินทรัพย์ จะต้องมีการประยุกต์ใช้แบบรูปการระบุความต้องการด้านความมั่นคงสำหรับสินทรัพย์องค์กรก่อน

เนื่องจากการพิจารณาส่วนประกอบ “เงื่อนไขก่อนการใช้” ของแบบรูปการระบุความต้องการด้านความมั่นคงสำหรับสินทรัพย์องค์กรนั้นพบว่า เงื่อนไขก่อนการใช้แบบรูปนี้ไม่ต้องการการประยุกต์ใช้แบบรูปใดๆ มาก่อนหน้านี้ ดังนั้นจึงไม่ได้รายการองค์ประกอบสำคัญเพิ่มเติม

3.1.3.2 การวิเคราะห์โครงสร้างไวยากรณ์ความมั่นคงจากส่วนประกอบ “แผนภาพต้นไม้ความมั่นคง”

ส่วนประกอบ “แผนภาพต้นไม้ความมั่นคง” แสดงให้เห็นถึงส่วนประกอบและความสัมพันธ์ระหว่างส่วนประกอบภายในแบบรูป ผลลัพธ์จากการวิเคราะห์ส่วนประกอบนี้คือ ทำให้ทราบถึงเซตขององค์ประกอบที่จำเป็นที่จะใช้ในการพิจารณาสร้างแบบจำลองเชิงโครงสร้าง กล่าวคือ นำมาพิจารณาเป็นชื่อคลาส ชื่อลักษณะประจำ หรือชื่อของการดำเนินการ



รูปที่ 3.4 แผนภาพต้นไม้ความมั่นคง ของแบบรูปการระบุความต้องการด้านความมั่นคงสำหรับสินทรัพย์องค์กร [8]

พิจารณารูปที่ 3.4 แสดงส่วนประกอบ “แผนภาพต้นไม้ความมั่นคง” ของแบบรูปการกำหนดค่าความเสี่ยง จะได้รายการองค์ประกอบสำคัญดังนี้

1) Asset คือ สินทรัพย์ขององค์กร โดยจะต้องมีการกำหนดคุณสมบัติความมั่นคงให้แก่สินทรัพย์นั้นๆ โดยสามารถแบ่งประเภทของสินทรัพย์ออกได้ 2 ประเภท คือ สินทรัพย์ประเภทข้อมูล และประเภทกายภาพ ซึ่งถูกกำหนดให้เป็นชื่อคลาส

2) SecurityProperty คือ คุณสมบัติความมั่นคง ซึ่งสามารถมีค่าที่เป็นไปได้คือ การรักษาความลับ ความบูรณภาพ สภาพพร้อมใช้งาน และภาระรับผิดชอบ และต่อมาจะถูกกำหนดให้เป็นชื่อคลาส

3) BusinessDriver คือ ตัวขับเคลื่อนทางธุรกิจ ซึ่งเป็นสิ่งที่แต่ละองค์กรระบุไว้ ซึ่งต่อมาจะถูกกำหนดให้เป็นชื่อคลาส

4) AssetType คือ ประเภทของสินทรัพย์ สามารถมีค่าที่เป็นไปได้คือ ประเภทข้อมูล และประเภทกายภาพ ซึ่งในแผนภาพต้นไม้ความมั่นคงนี้จะทำให้ทราบตัวอย่างค่าที่เป็นไปได้ของแต่ละประเภทของสินทรัพย์ ซึ่งต่อมาจะถูกกำหนดให้เป็นลักษณะประจำภายในคลาส Asset

จากการพิจารณาส่วนประกอบ “แผนภาพต้นไม้ความมั่นคง” ของแบบรูปนี้จะเห็นได้ว่ารายการองค์ประกอบสำคัญมีความคล้ายคลึงกันกับรายการองค์ประกอบสำคัญที่ได้จากการพิจารณาส่วนประกอบ “Problem” “Context” และ “Structure” ของแบบรูปความมั่นคง

3.1.3.3 การวิเคราะห์โครงสร้างไวยากรณ์ความมั่นคงจากส่วนประกอบ “ไวยากรณ์ความมั่นคง” และ “ตัวอย่างความต้องการด้านความมั่นคง”

ส่วนประกอบ “ไวยากรณ์ความมั่นคง” ระบุถึงไวยากรณ์ที่ถูกสร้างขึ้นมาเพื่อใช้สำหรับการระบุความต้องการของแบบรูปความมั่นคงนั้นๆ โดยอยู่ในรูปแบบไวยากรณ์ไม่พึ่งบริบท ส่วนประกอบ “ตัวอย่างความต้องการด้านความมั่นคง” แสดงตัวอย่างความต้องการที่ได้จากไวยากรณ์ความมั่นคง ผลลัพธ์จากการวิเคราะห์ 2 ส่วนประกอบนี้ ทำให้ทราบถึงเซตขององค์ประกอบที่จำเป็นที่ใช้ในการพิจารณาสร้างแบบจำลองเชิงโครงสร้าง กล่าวคือ นำมาพิจารณาเป็นชื่อคลาส ชื่อลักษณะประจำ หรือชื่อของการดำเนินการ และทำให้ทราบค่าที่เป็นไปได้ของลักษณะประจำ

พิจารณารูปที่ 3.5 แสดงส่วนประกอบ “ไวยากรณ์ความมั่นคง” และ “ตัวอย่างความต้องการด้านความมั่นคง” ของแบบรูปการระบุความต้องการด้านความมั่นคงสำหรับสินทรัพย์องค์กร จะได้รายการเซตขององค์ประกอบที่จำเป็นต้องใช้ในการพิจารณาสร้างแบบจำลองเชิงโครงสร้าง ดังนี้

1) Asset คือ สินทรัพย์ขององค์กร โดยจะต้องมีการกำหนดคุณสมบัติความมั่นคงให้แก่สินทรัพย์ โดยผู้ใช้งานสามารถระบุชื่อและประเภทของสินทรัพย์ได้ ซึ่งต่อมาจะถูกกำหนดให้เป็นชื่อคลาส

2) SecurityProperty คือ คุณสมบัติความมั่นคง ซึ่งสามารถมีค่าที่เป็นไปได้คือ การรักษาความลับ ความบูรณภาพ สภาพพร้อมใช้งาน และภาระรับผิดชอบ โดยสินทรัพย์สามารถกำหนดคุณสมบัติความมั่นคงได้มากกว่า 1 ค่า ซึ่งต่อมาจะถูกกำหนดให้เป็นชื่อคลาส

3) BusinessDriver คือ ตัวขับเคลื่อนทางธุรกิจ ซึ่งเป็นสิ่งที่แต่ละองค์กรระบุไว้ ซึ่งต่อมาจะถูกกำหนดให้เป็นชื่อคลาส

4) AssetType คือ ประเภทของสินทรัพย์ สามารถมีค่าที่เป็นไปได้คือ ประเภทข้อมูล และประเภทกายภาพ ซึ่งในแผนภาพต้นไม้ความมั่นคงนี้จะทำให้ทราบตัวอย่างค่าที่เป็นไปได้ของแต่ละประเภทของสินทรัพย์ ซึ่งต่อมาจะถูกกำหนดให้เป็นลักษณะประจำภายในคลาส Asset

ไวยากรณ์ความมั่นคง			
(1)	**Risk-Determination**	=	"The qualitative risk for" , **Asset-Name** , "is", **Qualitative-Risk** , "." ;
(2)	**Asset-Name**	=	? The asset name from GM61 ? ;
(3)	**Qualitative-Risk**	=	["negligible" | "low" | "medium" | "high" | "very high" | "extreme"] ;
ตัวอย่างความต้องการ			
The qualitative risk for **museum collections and exhibits** are **extreme**.			

รูปที่ 3.5 ไวยากรณ์ความมั่นคงและตัวอย่างความต้องการ
ของแบบรูปการระบุความต้องการด้านความมั่นคงสำหรับสินทรัพย์องค์กร [8]

3.2 การสร้างแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคง

ภายหลังจากการศึกษาและวิเคราะห์แบบรูปความมั่นคง และไวยากรณ์ของแบบรูปความมั่นคง ขั้นตอนต่อมา คือ การสร้างแบบจำลองเชิงโครงสร้างโดยใช้แผนภาพคลาส เนื่องจากแผนภาพคลาสเป็นแผนภาพมาตรฐานหนึ่งของยูเอ็มแอลซึ่งได้รับความนิยม และง่ายต่อการนำไปประยุกต์ใช้ ในขั้นตอนนี้มีเป้าหมายเพื่อให้ได้แผนภาพคลาสที่สอดคล้องกับแบบรูปความมั่นคง [4] และไวยากรณ์ความมั่นคง [8] เพื่อใช้ในการแสดงความสัมพันธ์ภายในของแต่ละคลาส และความสัมพันธ์แบบบูรณาการของทุกแบบรูปความมั่นคงสำหรับนำไปใช้ในขั้นตอนการสร้างภาพนามธรรมความมั่นคงต่อไป การสร้างแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคงประกอบด้วย 2 ขั้นตอนย่อย คือ การสร้างแบบจำลองเชิงโครงสร้างของแต่ละแบบรูปความมั่นคง และการสร้างแบบจำลองเชิงโครงสร้างแบบบูรณาการของแบบรูปความมั่นคงทั้งหมด

3.2.1 การสร้างแบบจำลองเชิงโครงสร้างของแต่ละแบบรูปความมั่นคง

ในขั้นตอนนี้เป็นการสร้างแผนภาพคลาสของแต่ละแบบรูปความมั่นคง โดยนำเอาเซตขององค์ประกอบที่วิเคราะห์ได้ทั้งหมดจากขั้นตอน 3.1.1, 3.1.2 และ 3.1.3 นำมาสร้างเป็นแผนภาพคลาส โดยมีขั้นตอนวิธีการสร้างแผนภาพคลาสของแต่ละแบบรูปความมั่นคงดังรูปที่ 3.6

ข้อมูลนำเข้า เซตขององค์ประกอบที่วิเคราะห์ได้ทั้งหมดจากขั้นตอน 3.1.1, 3.1.2 และ 3.1.3
ข้อมูลออก แผนภาพคลาสของแต่ละแบบรูปความมั่นคง
เริ่มต้น
นำเข้าเซตขององค์ประกอบที่วิเคราะห์ได้ทั้งหมดจากขั้นตอน 3.1.1, 3.1.2 และ 3.1.3
สำหรับ แต่ละคลาสจากขั้นตอน 3.1.1, 3.1.2 และ 3.1.3
จนกระทั่ง สิ้นสุดคลาสที่นำมาพิจารณา
ดำเนินการ
1. ระบุชื่อคลาส
2. ระบุลักษณะประจำภายในคลาส
3. ระบุการดำเนินการภายในคลาส

จนกระทั่ง สิ้นสุดเซตขององค์ประกอบของแต่ละคลาส
ระบุความสัมพันธ์ระหว่างคลาส
หยุดการทำงาน

รูปที่ 3.6 ขั้นตอนวิธีการสร้างแผนภาพคลาสของแต่ละแบบรูปความมั่นคง

พิจารณาตามขั้นตอนวิธีข้างต้น จะได้รายละเอียดของคลาส ลักษณะประจำ และการดำเนินการดังแสดงในรูปที่ 3.7 ซึ่งมีรายละเอียดดังต่อไปนี้

1) คลาส Asset คือ คลาสสินทรัพย์ขององค์กร โดยจะต้องมีการกำหนดคุณสมบัติความมั่นคงให้แก่สินทรัพย์นั้นๆ

1.1) assetID คือ รหัสประจำตัวสินทรัพย์

1.2) assetName คือ ชื่อของสินทรัพย์

1.3) assetType คือ ประเภทของสินทรัพย์ โดยสามารถแบ่งประเภทของสินทรัพย์ออกได้ 2 ประเภท คือ สินทรัพย์ประเภทข้อมูล และประเภทกายภาพ

2) คลาส SecurityProperty คือ คลาสคุณสมบัติความมั่นคง ซึ่งสามารถมีค่าที่เป็นไปได้คือ การรักษาความลับ ความบูรณภาพ สภาพพร้อมใช้งาน และภาระรับผิดชอบ

2.1) propertyID คือ รหัสคุณสมบัติความมั่นคง

2.2) propertyName คือ ชื่อของคุณสมบัติความมั่นคง โดยสามารถมีค่าที่เป็นไปได้คือ การรักษาความลับ ความบูรณภาพ สภาพพร้อมใช้งาน และภาระรับผิดชอบ [4]

3) BusinessDriver คือ ตัวขับเคลื่อนทางธุรกิจ ซึ่งเป็นสิ่งที่แต่ละองค์กรระบุไว้

3.1) driverID คือ รหัสตัวขับเคลื่อนทางธุรกิจ

3.2) driverName คือ ชื่อตัวขับเคลื่อนทางธุรกิจ

3.3) driverDescription คือ รายละเอียดคำอธิบายตัวขับเคลื่อนทางธุรกิจนั้น

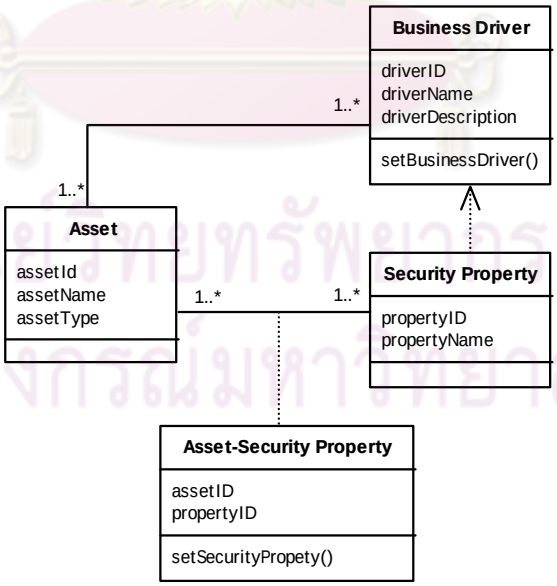
3.4) setBusinessDriver() คือ วิธีการกำหนดตัวขับเคลื่อนทางธุรกิจแก่สินทรัพย์

4) คลาส Asset-SecurityProperty คือ คลาสที่แสดงค่ารหัสของสินทรัพย์ และ รหัสของคุณสมบัติความมั่นคง ซึ่งถูกกำหนดให้เป็นชื่อคลาสเชื่อมโยง

4.1) assetID คือ รหัสของสินทรัพย์

4.2) propertyID คือ รหัสของคุณสมบัติความมั่นคง

4.3) setSecurityPropety() คือ วิธีการในการกำหนดคุณสมบัติความมั่นคงให้กับแต่ละสินทรัพย์

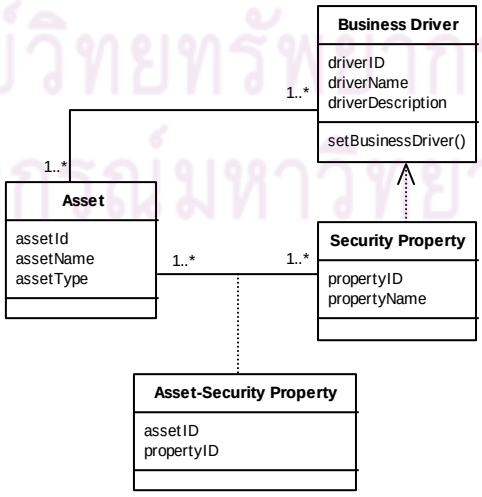


รูปที่ 3.7 แผนภาพคลาสของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร

หลังจากพิจารณาตามขั้นตอนวิธีในรูป 3.6 แล้วจะได้แผนภาพคลาสที่สอดคล้องกับทุกแบบรูปความมั่นคง และเพื่อให้ง่ายต่อการทำความเข้าใจ ในที่นี้จะยกตัวอย่างแผนภาพคลาสที่สอดคล้องกับแบบรูปความมั่นคงในกลุ่มแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยงในตารางที่ 3.1-3.8 โดยรวบรวมคำอธิบายองค์ประกอบต่างๆ ของแบบรูปความมั่นคงประกอบไปด้วย ชื่อแบบรูป รหัสแบบรูป ชื่อกลุ่มของแบบรูป เงื่อนไขก่อนการใช้ คำอธิบายแบบรูป ปัญหา ผลเฉลย และแผนภาพคลาส

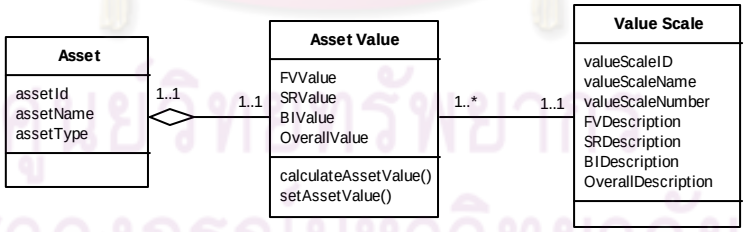
ตารางที่ 3.1 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปการระบุความต้องการด้านความมั่นคงสำหรับสินทรัพย์องค์กร

ชื่อแบบรูป	การระบุความต้องการด้านความมั่นคงสำหรับสินทรัพย์องค์กร
รหัสแบบรูป	P61
ชื่อกลุ่มของแบบรูป	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
เงื่อนไขก่อนการใช้	ไม่มี
คำอธิบาย	เป็นแบบรูปเริ่มต้นสำหรับการพิจารณาความมั่นคงองค์กร ซึ่งจะช่วยให้เข้าใจถึงความต้องการด้านความมั่นคงที่จำเป็นต้องมีในองค์กร เพื่อนำคุณสมบัติด้านความมั่นคง (Confidentiality : การรักษาความลับ, Integrity : ความบูรณภาพ, Availability : สภาพพร้อมใช้งาน, และ Accountability : ภาระรับผิดชอบ) มาประยุกต์ใช้
ปัญหา	องค์กรต้องการกำหนดความมั่นคงให้กับสินทรัพย์
ผลเฉลย	1. ระบุสินทรัพย์ 2. ระบุตัวขับเคลื่อนทางธุรกิจ 3. ระบุความสัมพันธ์ระหว่างสินทรัพย์และตัวขับเคลื่อนทางธุรกิจ 4. กำหนดคุณสมบัติด้านความมั่นคง 5. ระบุคุณสมบัติด้านความมั่นคงให้กับสินทรัพย์โดยพิจารณาจากตัวขับเคลื่อนทางธุรกิจ
แผนภาพคลาส	



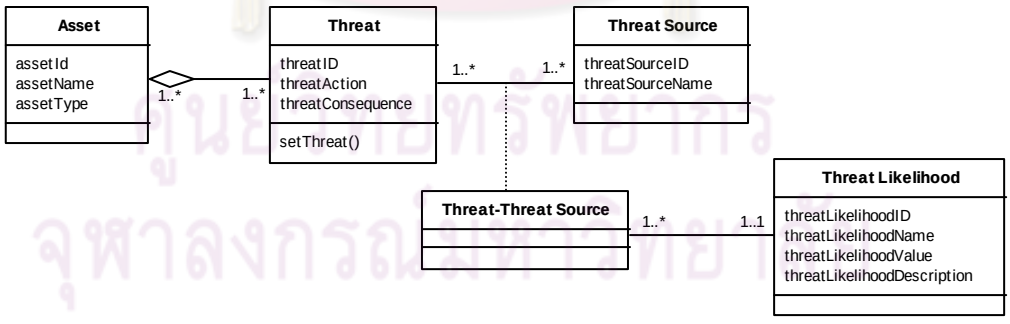
ตารางที่ 3.2 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปการกำหนดมูลค่าสินทรัพย์

ชื่อแบบรูป	การกำหนดมูลค่าสินทรัพย์
รหัสแบบรูป	P62
ชื่อกลุ่มของแบบรูป	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
เงื่อนไขก่อนการใช้	1. ชื่อสินทรัพย์ จาก GM61
คำอธิบาย	การกำหนดมูลค่าสินทรัพย์จะช่วยให้สามารถกำหนดความสำคัญของสินทรัพย์ขององค์กรที่เป็นเจ้าของหรือควบคุมอยู่ เพื่อระบุว่าเมื่อเกิดความสูญเสียของสินทรัพย์จะกระทบต่อองค์กรในด้านใดบ้างและมีผลกระทบในระดับใด โดยมูลค่าสินทรัพย์จะได้จากการพิจารณาผลกระทบในด้านต่างๆ ต่อไปนี้ ได้แก่ ด้านความต้องการด้านความมั่นคง ด้านเศรษฐกิจ และทางด้านธุรกิจ
ปัญหา	การกำหนดค่าความสำคัญของสินทรัพย์ทำอย่างไร
ผลเฉลย	1. ระบุ security value ของสินทรัพย์ 2. ระบุ financial value ของสินทรัพย์ 3. ระบุ business impact value ของสินทรัพย์ 4. สร้างตารางรวมค่าสินทรัพย์ ทั้งหมดโดยกำหนดให้ ค่ามากที่สุดกลายเป็น overall value ของสินทรัพย์นั้น
แผนภาพคลาส	



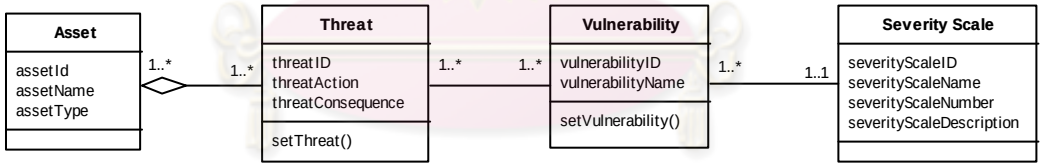
ตารางที่ 3.3 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปการประเมินภัยคุกคาม

ชื่อแบบรูป	การประเมินภัยคุกคาม
รหัสแบบรูป	P63
ชื่อกลุ่มของแบบรูป	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
เงื่อนไขก่อนการใช้	1. ชื่อสินทรัพย์ จาก GM61
คำอธิบาย	ภัยคุกคามเป็นโอกาสของอันตรายต่างๆ ที่อาจเกิดขึ้นและมีกระทบต่อสินทรัพย์องค์แบบรูปนี้จึงมีวัตถุประสงค์เพื่อกำหนดภัยคุกคาม ความถี่ของภัยคุกคามที่จะเกิดต่อสินทรัพย์ (Threat likelihood) และผลกระทบเมื่อสินทรัพย์ถูกคุกคาม (Threat consequence)
ปัญหา	จะระบุภัยคุกคามที่เกิดขึ้นกับสินทรัพย์ได้อย่างไร
ผลเฉลย	1. การระบุภัยคุกคาม ประกอบด้วย 1) ต้นเหตุที่ทำให้เกิดภัยคุกคาม 2) ภัยคุกคามที่เกิดขึ้น 3) ผลของภัยคุกคามนั้น 2. สร้างตารางภัยคุกคาม แยกตามชนิดของสินทรัพย์ 3. ระบุระดับความถี่ที่เกิดขึ้นของภัยคุกคาม 4. ระบุระดับความถี่ที่เกิดขึ้นในแต่ละภัยคุกคาม
แผนภาพคลาส	



ตารางที่ 3.4 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปการประเมินภาวะเสี่ยง

ชื่อแบบรูป	การประเมินภาวะเสี่ยง
รหัสแบบรูป	P64
ชื่อกลุ่มของแบบรูป	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
เงื่อนไขก่อนการใช้	1. ชื่อสินทรัพย์ จาก GM61 2. ชื่อภัยคุกคามสำหรับสินทรัพย์ในข้อ 1 ที่กำหนดไว้แล้วจาก GM63
คำอธิบาย	จุดอ่อน (ภาวะไม่มั่นคง) เป็นจุดที่จะถูกใช้โดยภัยคุกคาม การประเมินภาวะจุดอ่อน คือ การระบุจุดอ่อนของสินทรัพย์ในองค์กร และระดับความรุนแรงเมื่อถูกภัยคุกคามโจมตีจุดอ่อนดังกล่าว (Severity scale)
ปัญหา	ทำอย่างไรจึงจะกำหนดจุดอ่อนของสินทรัพย์ และระดับความรุนแรงเมื่อเกิดภัยคุกคามโจมตี
ผลเฉลย	1. รวบรวมข้อมูลของภัยคุกคาม 2. ระบุจุดอ่อนที่อาจเกิดขึ้น 3. สร้างตารางความสัมพันธ์ระหว่างจุดอ่อนและภัยคุกคาม 4. กำหนดระดับความรุนแรง
แผนภาพคลาส	

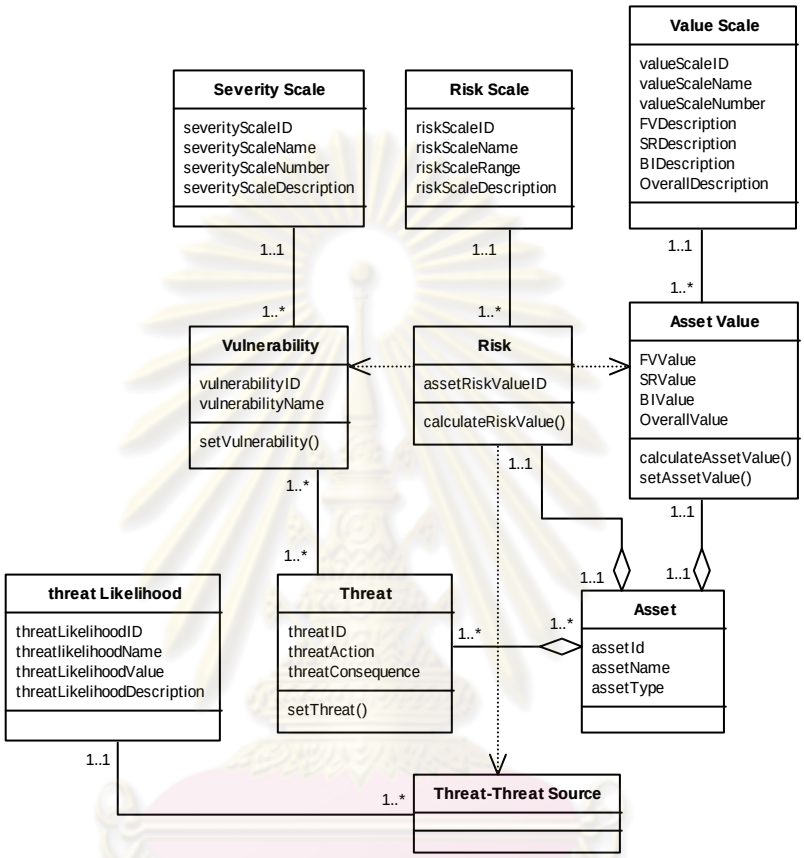


ตารางที่ 3.5 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปการกำหนดค่าความเสี่ยง

ชื่อแบบรูป	การกำหนดค่าความเสี่ยง
รหัสแบบรูป	P65
ชื่อกลุ่มของแบบรูป	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
เงื่อนไขก่อนการใช้	1. ชื่อสินทรัพย์ จาก GM61 (เฉพาะที่ตัวที่กำหนดมูลค่าสินทรัพย์ ประเมินภัยคุกคาม และภาวะเสี่ยงแล้วเท่านั้น) 2. ความถี่ของการเกิดภัยคุกคามทุกตัวสำหรับสินทรัพย์ในข้อ 1 จาก GM63 3. ระดับความรุนแรงของภาวะเสี่ยงทุกตัวสำหรับภัยคุกคามในข้อ 2 จาก GM64 4. มูลค่าสินทรัพย์ในข้อ 1 จาก GM62
คำอธิบาย	การกำหนดค่าความเสี่ยงเป็นขั้นตอนสุดท้ายของกระบวนการประเมินความเสี่ยง โดยการใช้ข้อมูลการประเมินมูลค่าสินทรัพย์ ภัยคุกคามและความถี่ที่เกิด ภาวะจุดอ่อนและระดับความรุนแรงมาใช้เป็นข้อมูลนำเข้าเพื่อนำมาคำนวณและแสดงผลเป็นระดับความเสี่ยงที่เหมาะสม ช่วยให้สามารถทราบความเสี่ยงของสินทรัพย์และจัดลำดับความสำคัญของสินทรัพย์ได้
ปัญหา	จะกำหนดค่าความเสี่ยงให้กับสินทรัพย์ได้อย่างไร
ผลเฉลย	1. รวบรวมผลลัพท์จาก 6.2, 6.3, 6.4 2. เชื่อมโยงภัยคุกคาม จุดอ่อน และสินทรัพย์เข้าด้วยกัน 3. คำนวนค่าความเสี่ยงตามสูตร ค่าความเสี่ยง = $\sum_{i=1}^{n}(ThreatLikelihood_i \times VulnerbilitySeverityScale_i) \times AssetValue$

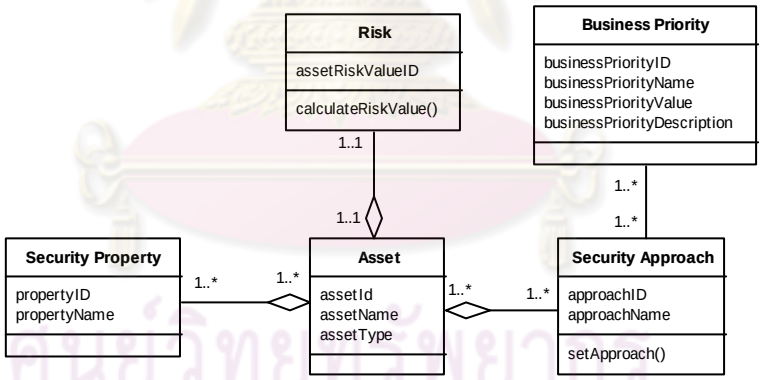
ตารางที่ 3.5 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปการกำหนดค่าความเสี่ยง (ต่อ)

แผนภาพคลาส



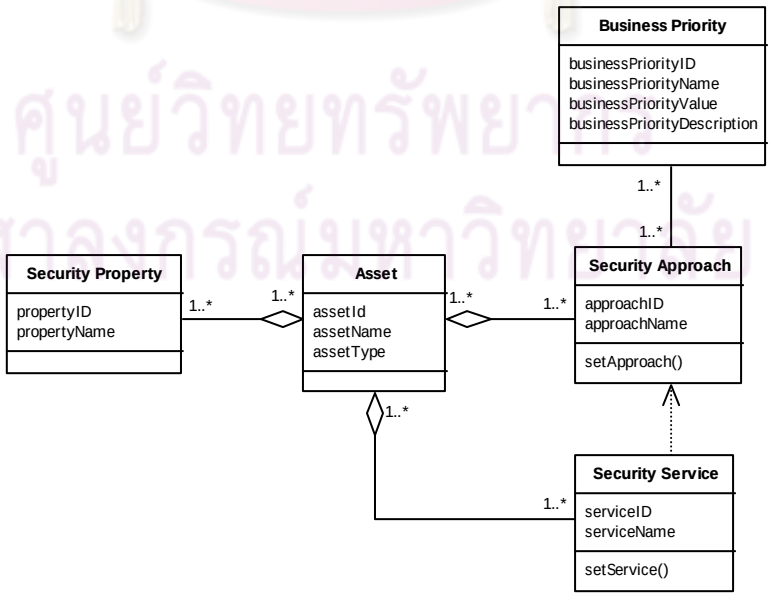
ตารางที่ 3.6 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปแนวคิดความมั่นคงองค์กร

ชื่อแบบรูป	แนวคิดความมั่นคงองค์กร
รหัสแบบรูป	P66
ชื่อกลุ่มของแบบรูป	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
เงื่อนไขก่อนการใช้	1. ชื่อสินทรัพย์ จาก GM61
คำอธิบาย	แบบรูปนี้จะช่วยเป็นตัวแนะนำในการเลือกแนวคิดความมั่นคง (Prevention : การป้องกัน Detection : การตรวจหา และ Response : การตอบสนอง) ตามคุณสมบัติความมั่นคงที่เหมาะสม และระดับความเสี่ยงของสินทรัพย์ที่พิจารณา
ปัญหา	จะกำหนดแนวคิดความมั่นคงให้แก่สินทรัพย์ได้อย่างไร
ผลเฉลย	1. รวบรวมข้อมูลที่จำเป็น คือ ชนิดของสินทรัพย์ 2. รวบรวมข้อมูลค่าความเสี่ยงของสินทรัพย์ 3. เลือกแนวคิดความมั่นคงให้เหมาะสมกับสินทรัพย์
แผนภาพคลาส	



ตารางที่ 3.7 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปบริการความมั่นคงองค์กร

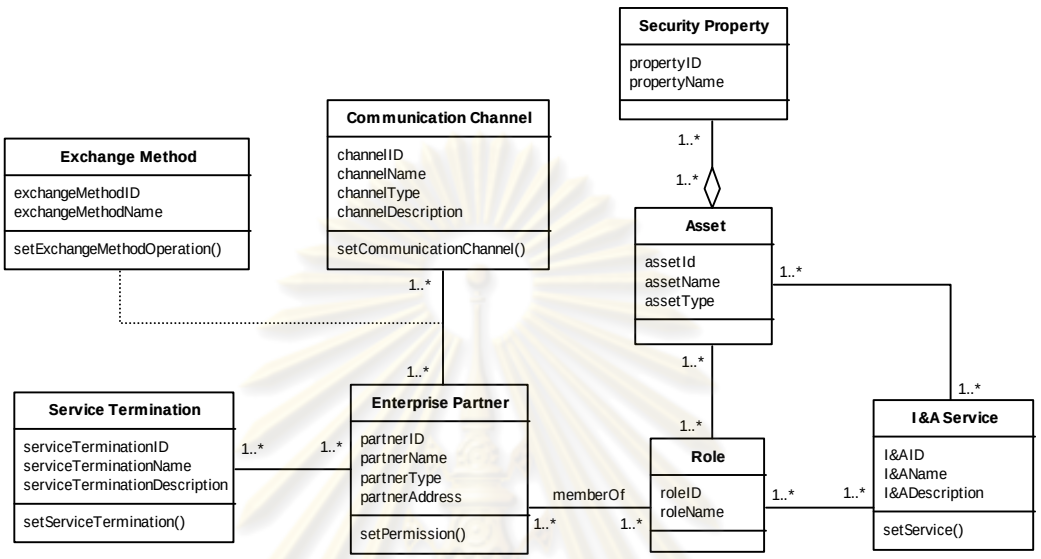
ชื่อแบบรูป	บริการความมั่นคงองค์กร
รหัสแบบรูป	P67
ชื่อกลุ่มของแบบรูป	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
เงื่อนไขก่อนการใช้	1. ชื่อสินทรัพย์ จาก GM61 (ในการพัฒนาจริงจะถูกผนวกรวมเข้ากับ GM66)
คำอธิบาย	แบบรูปนี้ต่อเนื่องจากแบบรูป GM66 โดยแบบรูปนี้เป็นการแนะนำในการเลือกตัวบริการความมั่นคงที่จะใช้ในการป้องกันสินทรัพย์ภายหลังที่ได้กำหนดแนวคิดความมั่นคงสำหรับสินทรัพย์ดังกล่าวแล้ว ตัวอย่างบริการด้านความมั่นคง เช่น การระบุและยืนยันตัวตน (GM71) การควบคุมการเข้าถึง (GM82) เป็นต้น
ปัญหา	จะกำหนดบริการความมั่นคงของสินทรัพย์ในองค์กรได้อย่างไร
ผลเฉลย	1. รวบรวมข้อมูลที่จำเป็น(ประเภทของสินทรัพย์ คุณสมบัติความมั่นคง แนวคิดความมั่นคงองค์กร) 2. ระบุบริการความมั่นคงสำหรับสินทรัพย์และแนวคิดความมั่นคง 3. ทวนสอบบริการความมั่นคงอย่างสม่ำเสมอ เมื่อมีสถานการณ์เปลี่ยนแปลง
แผนภาพคลาส	



ตารางที่ 3.8 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปการสื่อสารของผู้มีหุ้นส่วนองค์กร

ชื่อแบบรูป	การสื่อสารของผู้มีหุ้นส่วนองค์กร
รหัสแบบรูป	P68
ชื่อกลุ่มของแบบรูป	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
เงื่อนไขก่อนการใช้	1. ชื่อสินทรัพย์ จาก GM61 2. ชื่อบริการสำหรับระบุและยืนยันตัวตนจาก GM72
คำอธิบาย	เมื่อองค์กรมีการติดต่อกับองค์กรภายนอก จะต้องมีการเตรียมเครื่องมือและบริการต่างๆ ไว้อำนวยความสะดวกและควบคุมการติดต่อและการแลกเปลี่ยนข้อมูล แต่การดำเนินการดังกล่าวจะต้องเลือกบริการความมั่นคงที่เหมาะสม ในการจัดการสิทธิ์การเข้าถึง รวมถึงการป้องกันข้อมูลมิให้ถูกเข้าถึงโดยผู้ที่ไม่มีสิทธิ์
ปัญหา	เมื่อมีการติดต่อของหุ้นส่วนกับองค์กร จะปกป้องระบบและข้อมูลขององค์กรได้อย่างไร
ผลเฉลย	1. ระบุข้อมูล และapplication services ที่ต้องมีการแลกเปลี่ยนระหว่างองค์กร จากนั้นให้ระบุความต้องการด้านความมั่นคงของข้อมูลดังกล่าว 2. กำหนดความมั่นคงด้านการตรวจสอบ การเข้าใช้งานของหุ้นส่วน โดยพิจารณาจากความต้องการด้านความมั่นคงของข้อมูลและนโยบายขององค์กร 3. ระบุและป้องกันช่องทางการติดต่อ 1) ระบุช่องทางการติดต่อ 2) แยกช่องทางของหุ้นส่วนออกจากช่องทางหลัก 3) กำหนดการจัดการด้าน Port's และ Portals 4) กำหนดการจัดการด้านการควบคุมการเข้าถึง 4. กำหนดวิธีดำเนินการที่ใช้ในช่องทางการติดต่อ 5. กำหนดกิจกรรมการสิ้นสุดของหุ้นส่วน ตามข้อตกลงก่อนหน้า

ตารางที่ 3.8 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปการสื่อสารของผู้มีหุ้นส่วนองค์กร (ต่อ)

แผนภาพคลาส


3.2.2 การสร้างแบบจำลองเชิงโครงสร้างแบบบูรณาการของแบบรูปความมั่นคงทั้งหมด

ในขั้นตอนนี้เป็นการสร้างแผนภาพคลาสแบบบูรณาการความสัมพันธ์ ของแบบรูปความมั่นคงทั้งหมด เพื่อสร้างความสัมพันธ์ที่เกิดขึ้นระหว่างแบบรูปความมั่นคง และจัดโครงสร้างของแบบรูปความมั่นคงเพื่อเตรียมพร้อมสำหรับการสร้างความสัมพันธ์ในตารางฐานข้อมูล (ในบทที่ 4 การพัฒนาเครื่องมือการสร้างภาพนามธรรม) ที่จะกล่าวถึงต่อไป

ขั้นตอนวิธีในการสร้างแผนภาพคลาสแบบบูรณาการแบบรูปความมั่นคงนั้นสามารถแสดงได้ดังรูปที่ 3.8 โดยมีวิธีดำเนินการคือ นำเข้าแผนภาพคลาสของแต่ละแบบรูปความมั่นคงที่ได้สร้างจากหัวข้อ 3.2.1 จำนวน 20 แบบรูป ต่อมาระบุแผนภาพคลาสที่ต้องการจะบูรณาการความสัมพันธ์ 2 แบบรูป แล้วค้นหาคลาสที่มีชื่อเหมือนกันจากแผนภาพคลาสของในแต่ละแบบรูป โดยการพิจารณาจากตารางความสัมพันธ์ระหว่างแบบรูปความมั่นคง [8] ซึ่งตารางความสัมพันธ์นี้แสดงไว้ในภาคผนวก ญ ในตาราง ญ. 1 ถัดมาพิจารณาชื่อคลาส หากมีชื่อคลาสเหมือนกันแล้วให้บูรณาการความสัมพันธ์โดยใช้คลาสนั้นเป็นตัวเชื่อมความสัมพันธ์ระหว่าง 2 แบบรูปความมั่นคง ทำซ้ำเช่นนี้จนกระทั่งสิ้นสุดแผนภาพคลาสทั้ง 20 แบบรูป

เพื่อความสะดวกในการทำความเข้าใจ ในที่นี้จะขอยกตัวอย่างแผนภาพคลาสของแบบรูปการระบุความต้องการด้านความมั่นคงสำหรับสินทรัพย์องค์กรดังแสดงในรูปที่ 3.7 และแผนภาพคลาสของแบบรูปการกำหนดมูลค่าสินทรัพย์ ดังแสดงในรูปที่ 3.9 มาเป็นกรณีศึกษาในการสร้างแผนภาพคลาสแบบบูรณาการ

ข้อมูลนำเข้า แผนภาพคลาสของแต่ละแบบรูปความมั่นคงที่สร้างได้จาก 3.2.1 จำนวน 20 แบบรูป

ข้อมูลออก แผนภาพคลาสแบบบูรณาการความสัมพันธ์ของแบบรูปทั้งหมด

เริ่มต้น

นำเข้าแผนภาพคลาสของแบบรูปความมั่นคงที่สร้างได้จาก 3.2.1 จำนวน 20 แบบรูป

ดำเนินการ

1. ระบุแผนภาพคลาสที่ต้องการจะบูรณาการความสัมพันธ์ 2 แบบรูป
2. ค้นหาคลาสที่มีชื่อเหมือนกันจากแผนภาพคลาสของในแต่ละแบบรูป โดยการพิจารณาจากตารางความสัมพันธ์ระหว่างแบบรูปความมั่นคง [8]

ถ้า คลาสมีชื่อเหมือนกัน

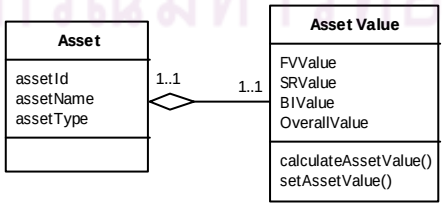
ดำเนินการ

บูรณาการความสัมพันธ์โดยใช้คลาสนั้นเป็นตัวเชื่อมความสัมพันธ์ระหว่าง 2 แบบรูปความมั่นคง

จนกระทั่ง สิ้นสุดแผนภาพคลาสทั้ง 20 แบบรูป

หยุดการทำงาน

รูปที่ 3.8 ขั้นตอนวิธีการสร้างแผนภาพคลาสแบบบูรณาการของแบบรูปความมั่นคงทั้งหมด



รูปที่ 3.9 แผนภาพคลาสของแบบรูปการกำหนดมูลค่าสินทรัพย์

แบบรูปการกำหนดมูลค่าสินทรัพย์ มีวัตถุประสงค์เพื่อให้สามารถกำหนดความสำคัญของสินทรัพย์ขององค์กรที่เป็นเจ้าของหรือควบคุมอยู่ เพื่อระบุว่าเมื่อเกิดความสูญเสียของสินทรัพย์จะกระทบต่อองค์กรในด้านใดบ้างและมีผลกระทบในระดับใด โดยมูลค่าสินทรัพย์สามารถคำนวณได้จากการพิจารณาผลกระทบในด้านต่างๆ ต่อไปนี้ ได้แก่ ด้านความความต้องการด้านความมั่นคง ด้านเศรษฐกิจ และทางด้านธุรกิจ

จากความสัมพันธ์ของทั้ง 2 แบบรูปข้างต้นสามารถนำมาสร้างเป็นแผนภาพคลาสได้ดังรูปที่ 3.10 โดยสามารถอธิบายความสัมพันธ์ของทั้ง 2 แบบรูปได้ คือ สินทรัพย์จะต้องมีการกำหนดค่าคุณสมบัติความมั่นคงโดยยึดหลักการขับเคลื่อนทางธุรกิจ และสินทรัพย์ยังต้องมีการกำหนดค่าเพื่อระบุความสำคัญของสินทรัพย์ต่อองค์กร โดยรายละเอียดแผนภาพคลาสแบบบูรณาการของ 2 แบบรูป ประกอบด้วยคลาสต่างๆ ดังรายละเอียดต่อไปนี้

1) แบบรูปการระบุความต้องการด้านความมั่นคงสำหรับสินทรัพย์องค์กร

รายละเอียดคลาสของไวยากรณ์นี้ถูกอธิบายไว้แล้วในหัวข้อ 3.2.1

2) แบบรูปการกำหนดมูลค่าสินทรัพย์

2.1) คลาส Asset คือ คลาสสินทรัพย์ขององค์กร โดยต้องมีการกำหนดมูลค่าของแต่ละสินทรัพย์ขององค์กรเพื่อระบุถึงความสำคัญของสินทรัพย์นั้นๆ ต่อองค์กร ภายในจะประกอบไปด้วยลักษณะประจำ และการดำเนินการต่างๆ ดังนี้

(1) assetID คือ รหัสประจำตัวสินทรัพย์

(2) assetName คือ ชื่อของสินทรัพย์

(3) assetType คือ ประเภทของสินทรัพย์ โดยสามารถแบ่งประเภทของสินทรัพย์ออกได้ 2 ประเภท คือ สินทรัพย์ประเภทข้อมูล และประเภทกายภาพ

2.2) คลาส AssetValue คือ คลาสมูลค่าสินทรัพย์ โดยจะมีการคำนวณมูลค่าสินทรัพย์ในหลายมุมมอง ประกอบด้วยมุมมองด้านเศรษฐกิจ มุมมองด้านธุรกิจ มุมมองด้านความมั่นคง และนอกจากนี้ยังมีการคำนวณมูลค่าสินทรัพย์โดยรวมอีกด้วย ภายในประกอบไปด้วยลักษณะประจำ และการดำเนินการต่างๆ ดังนี้

(1) OverallRating คือ มูลค่าของสินทรัพย์โดยรวม

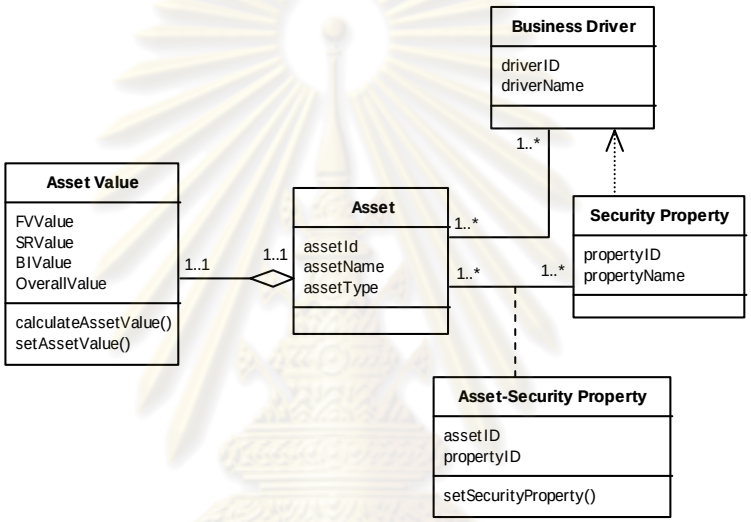
(2) FVRating คือ มูลค่าของสินทรัพย์โดยพิจารณาจากความต้องการทางด้านเศรษฐกิจ

(3) BIRating คือ มูลค่าของสินทรัพย์โดยพิจารณาจากความต้องการทางด้านธุรกิจ

(4) SRRating คือ มูลค่าของสินทรัพย์โดยพิจารณาจากความต้องการทางด้านความมั่นคง

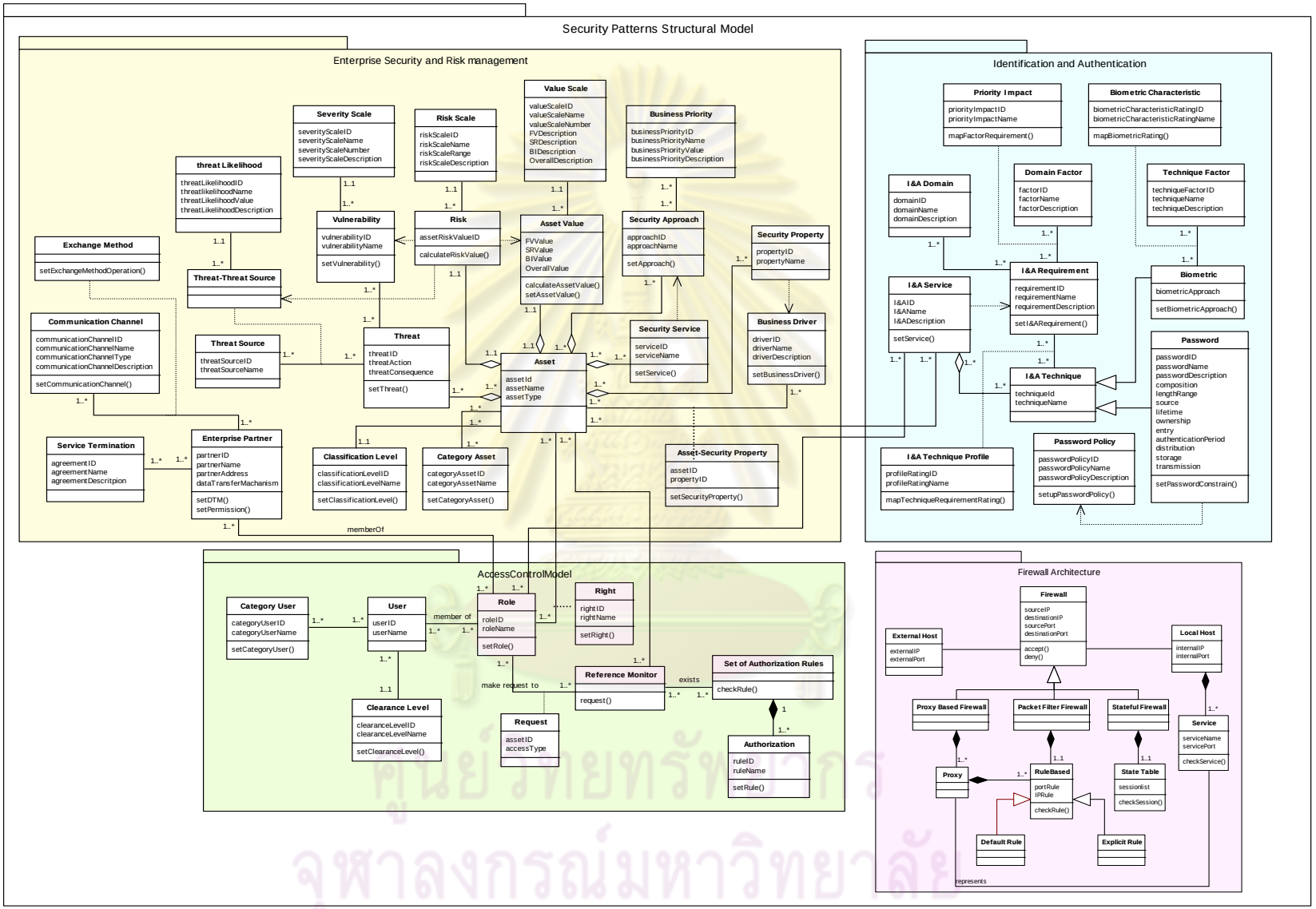
(5) calculateAssetValue() คือ วิธีการในการคำนวณมูลค่าของสินทรัพย์โดยรวม โดยพิจารณาจากความต้องการทางด้านธุรกิจ ความต้องการทางด้านเศรษฐกิจ และความต้องการทางด้านความมั่นคง

(6) setAssetValue() คือ วิธีการในการกำหนดมูลค่าให้กับแต่ละสินทรัพย์ โดยแต่ละสินทรัพย์จะมีมูลค่าโดยรวมของสินทรัพย์ได้เพียง 1 ค่า



รูปที่ 3.10 แผนภาพคลาสแบบบูรณาการของแบบรูปการระบุความต้องการด้านความมั่นคงสำหรับสินทรัพย์องค์กร และแบบรูปการกำหนดมูลค่าสินทรัพย์

ทั้งนี้เมื่อได้บูรณาการแบบรูปความมั่นคงครบทั้ง 20 แบบรูปความมั่นคงเรียบร้อยแล้วจะได้แผนภาพคลาสแบบบูรณาการแบบรูปความมั่นคงดังรูปที่ 3.11



รูปที่ 3.11 แผนภาพคลาสแบบบูรณาการ 20 แบบรูปความมั่นคง

3.3 การตรวจสอบแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคง

การตรวจสอบแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคง ประกอบด้วย 3 ขั้นตอน ดังนี้

3.3.1 การตรวจสอบความสอดคล้องตามบริบทของแบบรูปความมั่นคง

การตรวจสอบความสอดคล้องตามบริบทของแบบรูปความมั่นคง มีวัตถุประสงค์เพื่อตรวจสอบความสอดคล้องของแบบจำลองเชิงโครงสร้างที่ได้ว่ามีความสอดคล้องตามบริบทที่ได้กล่าวถึงไว้ในแบบรูปความมั่นคงของ [4] หรือไม่ โดยการพิจารณาร่วมกันกับผู้มีความรู้พื้นฐานด้านความมั่นคง เพื่อรับข้อเสนอแนะและความคิดเห็นเพื่อใช้ปรับปรุงแบบจำลองเชิงโครงสร้างให้มีความสอดคล้องตามบริบทของแบบรูปความมั่นคงมากขึ้น โดยพิจารณาในทุกๆ ส่วนประกอบย่อยของแต่ละแบบรูปความมั่นคงและไวยากรณ์ความมั่นคง โดยส่วนประกอบนั้นๆ อาจถูกพิจารณากลายมาเป็นคลาส ลักษณะประจำภายในคลาส หรือการดำเนินการ ซึ่งขึ้นอยู่กับหน้าที่และความสำคัญของส่วนประกอบนั้นๆ

รายละเอียดในการตรวจสอบความครบถ้วนของแบบจำลองเชิงโครงสร้างสามารถพิจารณาได้ดังรายการต่อไปนี้

1) มีคุณลักษณะเชิงโครงสร้างสอดคล้องกับส่วนประกอบโครงสร้าง (Structure) ของแบบรูปความมั่นคง

2) สามารถนำไปประยุกต์ใช้ได้ในสถานการณ์ตามที่อ้างอิงในองค์ประกอบไดนามิก (Dynamic) ของแบบรูปความมั่นคง

3) สามารถนำไปสู่ผลเฉลยแบบรูป ตามที่กล่าวไว้ในส่วนประกอบผลเฉลย (Solution) และ ตัวอย่างการแก้ไข (Example Resolved) ของแบบรูปความมั่นคง

4) มีคุณลักษณะเชิงโครงสร้างสอดคล้องกับส่วนประกอบแผนภาพต้นไม้ความมั่นคง ของไวยากรณ์ความมั่นคง

3.3.2 การตรวจสอบความสมบูรณ์เพื่อการนำไปประยุกต์ใช้งาน

การตรวจสอบความสมบูรณ์เพื่อการนำไปประยุกต์ใช้งานของแบบจำลองเชิงโครงสร้าง มีวัตถุประสงค์เพื่อพิจารณาองค์ประกอบในแบบจำลองเชิงโครงสร้างให้มีความสมบูรณ์และสามารถตอบสนองต่อความต้องการในการนำไปประยุกต์ใช้งานได้ โดยในการปรับปรุงแบบจำลองเชิงโครงสร้างนี้เกิดจากการวิเคราะห์และพิจารณาองค์ประกอบของแต่ละแบบรูปความ

มั่นคง ว่ามีองค์ประกอบใดที่ต้องเพิ่มเติมบ้าง ทั้งนี้การเพิ่มเติมอาจเกิดจากการเพิ่มเติมองค์ประกอบให้มีความครบถ้วน และสมบูรณ์มากยิ่งขึ้น เพื่อทำให้แบบจำลองเชิงโครงสร้างสามารถตอบสนองต่อความต้องการในการใช้งาน เช่น การเพิ่มเติมลักษณะประจำ partnerType ภายในคลาส Partner ใช้ระบุถึงประเภทของหุ้นส่วนที่ติดต่อกับองค์กร เพื่อความสะดวกในการจัดการ ติดต่อสื่อสาร กับหุ้นส่วนประเภทต่างๆ กัน

3.3.3 การตรวจสอบความครบถ้วนของความสัมพันธ์

ในขั้นตอนนี้มีวัตถุประสงค์เพื่อตรวจสอบความครบถ้วนของความสัมพันธ์ระหว่างแบบรูปความมั่นคง ว่ามีการระบุไว้อย่างครบถ้วนและถูกต้องหรือไม่ ซึ่งแต่ละแบบรูปความมั่นคงนั้นอาจมีความขึ้นต่อกัน ยกตัวอย่างเช่น ในการประยุกต์ใช้แบบรูปการกำหนดค่าความเสี่ยงในทางปฏิบัติได้นั้น จะต้องกำหนดค่าของมูลค่าสินทรัพย์ จากแบบรูปการกำหนดมูลค่าสินทรัพย์ ค่าของภัยคุกคามและความถี่ที่เกิดขึ้น จากแบบรูปการประเมินภัยคุกคาม และค่าภาวะจุดอ่อนและระดับความรุนแรง จากแบบรูปการประเมินภาวะเสี่ยงก่อน จึงจะสามารถประยุกต์ใช้แบบรูปการกำหนดค่าความเสี่ยงได้

บทที่ 4

การออกแบบวิธีการสร้างภาพนามธรรม และการพัฒนาเครื่องมือต้นแบบสำหรับการสร้างภาพนามธรรมความต้องการด้านความมั่นคง

ภายหลังจากการออกแบบแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคง และการกำหนดความต้องการด้านความมั่นคงแล้ว ขั้นตอนต่อไปคือ การออกแบบวิธีการสร้างภาพนามธรรมของความต้องการด้านความมั่นคง โดยการนำข้อมูลความสัมพันธ์ และองค์ประกอบที่สำคัญต่างๆ ของแบบจำลองเชิงโครงสร้างที่ได้สร้างขึ้นในบทที่ 3 มาร่วมพิจารณาประกอบ ทั้งนี้เพื่อประโยชน์ในการช่วยเหลือให้ผู้ใช้งานมีความสะดวก มองเห็นภาพของความต้องการด้านความมั่นคงที่ถูกกำหนดขึ้นได้อย่างชัดเจน และใช้ประกอบการพิจารณาในการกำหนดนโยบายความมั่นคงขององค์กรต่อไป

ในบทนี้จะกล่าวถึงการออกแบบวิธีการสร้างภาพนามธรรมและการพัฒนาเครื่องมือต้นแบบสำหรับการสร้างภาพนามธรรมของความต้องการด้านความมั่นคง ประกอบด้วย การออกแบบวิธีการสร้างภาพนามธรรม การออกแบบหน้าที่การทำงานของเครื่องมือ การออกแบบส่วนต่อประสานผู้ใช้ และสภาพแวดล้อมในการพัฒนาเครื่องมือ โดยมีรายละเอียดดังนี้

4.1 การออกแบบวิธีการสร้างภาพนามธรรม

จากการวิเคราะห์และศึกษาการจัดหมวดหมู่ของแบบรูปความมั่นคง แบบรูปความมั่นคงและไวยากรณ์ความมั่นคง ตลอดจนผลลัพธ์แผนภาพคลาสแบบบูรณาการความสัมพันธ์ของแบบรูปความมั่นคงทั้งหมดที่ได้จากบทที่ 3 ในหัวข้อนี้จะพิจารณาข้อมูลความสัมพันธ์ และองค์ประกอบที่สำคัญต่างๆ ที่ได้จากการสร้างแผนภาพคลาส โดยในการออกแบบวิธีการสร้างภาพนามธรรมนี้แบ่งออกได้ 3 วิธี คือ

4.1.1 การสร้างภาพนามธรรมจากแบบรูปความมั่นคง

ในการออกแบบการสร้างภาพนามธรรมจากแบบรูปความมั่นคง ผู้วิจัยได้ศึกษาและวิเคราะห์ข้อมูลแบบรูปความมั่นคงทำให้ทราบถึงความหมาย ผลเฉลย ส่วนประกอบสำคัญของแบบรูปความมั่นคง และไวยากรณ์ความมั่นคงทำให้ทราบถึงส่วนประกอบสำคัญ และความสัมพันธ์ระหว่างไวยากรณ์แบบรูปความมั่นคง ตลอดจนผลลัพธ์แผนภาพคลาสแบบบูรณาการความสัมพันธ์ของแบบรูปความมั่นคงทั้งหมดที่ได้จากบทที่ 3 แล้วนำมาวิเคราะห์เป็น

ข้อมูลสรุปที่เหมาะสมที่ผู้ใช้งานต้องการทราบในแต่ละแบบรูปความมั่นคง ทั้งนี้รายการการสร้างภาพนามธรรมจากแบบรูปความมั่นคงทั้ง 20 แบบรูปได้แสดงไว้ในตาราง 4.1

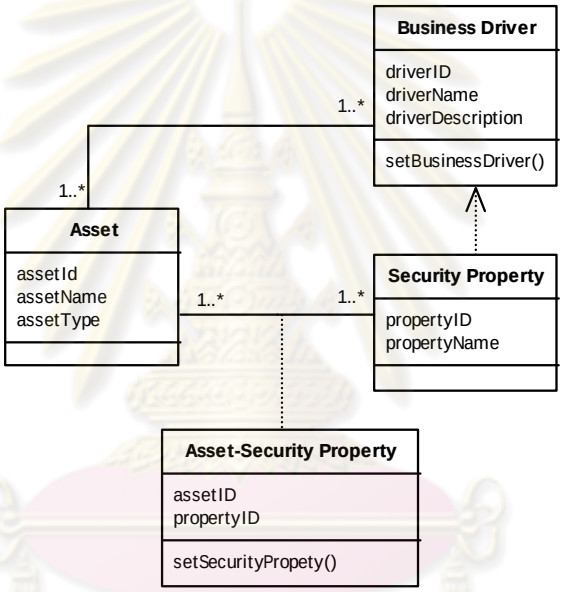
ตารางที่ 4.1 รายการตัวเลือกการสร้างภาพนามธรรมจากแบบรูปความมั่นคง

แบบรูปความมั่นคง	ชนิดของแผนภูมิ	ข้อมูลลักษณะประจำที่ใช้
กลุ่มการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง		
การระบุความต้องการความมั่นคงสำหรับสินทรัพย์ขององค์กร	แผนภูมิแบบจุดสองมิติ	Asset, Security Property
	แผนภูมิแบบจุดสองมิติ	Asset, Asset Type
	แผนภูมิแบบจุดสามมิติ	Asset, Security Property, Business Driver
	แผนภูมิรูปวงกลม	Business Driver
การประเมินมูลค่าสินทรัพย์	แผนภูมิแบบจุดสองมิติ	Asset, Asset Value
	แผนภูมิเรดาร์	Asset Value
การประเมินภัยคุกคาม	แผนภูมิแบบจุดสองมิติ	Asset, Threat Action
	แผนภูมิแบบจุดสองมิติ	Threat Action, Threat Source
	แผนภูมิแบบจุดสามมิติ	Asset, Threat Action, Threat Likelihood
การประเมินภาวะเสี่ยง	แผนภูมิแบบจุดสองมิติ	Threat Action, Vulnerability
	แผนภูมิแบบจุดสามมิติ	Asset, Vulnerability, Threat
การกำหนดความเสี่ยง	แผนภูมิแบบจุดสองมิติ	Asset, Risk Value
	แผนภูมิแบบฟอง	Asset Name, Asset Type, Risk Value
แนวคิดความมั่นคงขององค์กร	แผนภูมิแบบจุดสองมิติ	Asset, Security Approach
	แผนภูมิแบบจุดสามมิติ	Asset, Security Approach, Business Priority
บริการความมั่นคงขององค์กร	แผนภูมิแบบจุดสองมิติ	Asset, Security Service
	แผนภูมิแบบจุดสามมิติ	Asset, Security Service, Security Approach
การสื่อสารของผู้มีหุ้นส่วนในองค์กร	แผนภูมิแบบจุดสองมิติ	Partner, Communication Channel
	แผนภูมิแบบจุดสามมิติ	Asset, Partner, Communication Channel
กลุ่มการระบุตัวตนและการพิสูจน์ตัวจริง		
ความต้องการด้านการระบุและการพิสูจน์ตัวตน	แผนภูมิแบบจุดสองมิติ	I&A Service, I&A Requirement

ตารางที่ 4.1 รายการตัวเลือกการสร้างภาพนามธรรมจากแบบรูปความมั่นคง (ต่อ)

แบบรูปความมั่นคง	ชนิดของแผนภูมิ	ข้อมูลลักษณะประจำที่ใช้
กลุ่มการระบุตัวตนและการพิสูจน์ตัวจริง		
ทางเลือกการออกแบบสำหรับการระบุและการพิสูจน์ตัวตนแบบอัตโนมัติ	แผนภูมิแบบจุดสองมิติ	I&A Service, I&A Technique
	แผนภูมิเรดาร์	I&A Requirements and Technique Profile
การออกแบบและใช้รหัสผ่าน	แผนภูมิแบบจุดสองมิติ	Password, PasswordPolicy
ทางเลือกการออกแบบสำหรับแบบชีวมิติ	แผนภูมิแบบฟอง	Biometrics and Technique Factors Scale
กลุ่มแบบจำลองควบคุมการเข้าถึง		
การให้อำนาจ	แผนภูมิแบบจุดสองมิติ	User, Asset
	แผนภูมิแบบจุดสามมิติ	User, Asset, Right
การควบคุมการเข้าถึงเชิงบทบาท	แผนภูมิแบบจุดสองมิติ	Role, Asset
	แผนภูมิแบบจุดสามมิติ	Role, Asset, Right
	แผนภูมิแบบแท่ง	Student Role, Asset, Right
	แผนภูมิเส้น	Teacher Role, Asset, Right
ความมั่นคงหลายระดับ	แผนภูมิแบบจุดสองมิติ	Asset, Category Asset
	แผนภูมิแบบฟอง	Asset, Category, Classification Level
การตรวจสอบการเข้าถึงทรัพยากร	แผนภูมิแบบแท่ง	Student Role, Asset, Right
	แผนภูมิเส้น	Teacher Role, Asset, Right
การกำหนดสิทธิ์ให้กับบทบาท	แผนภูมิแบบแท่ง	Student Role, Asset, Right
	แผนภูมิเส้น	Teacher Role, Asset, Right
กลุ่มสถาปัตยกรรมไฟล์วอลล์		
ไฟร์วอลล์สำหรับการกรองแพ็คเกจ	แผนภูมิแบบจุดสองมิติ	internalIP,externalIP
		internalHostName, externalHostName
ไฟร์วอลล์เชิงตัวแทน	แผนภูมิแบบจุดสองมิติ	externalIP, appServiceName
		externalHostName, appServiceName
ไฟร์วอลล์เชิงสถานะ	แผนภูมิแบบจุดสองมิติ	externalIP, stateSessionName
		externalHostName, stateSessionName

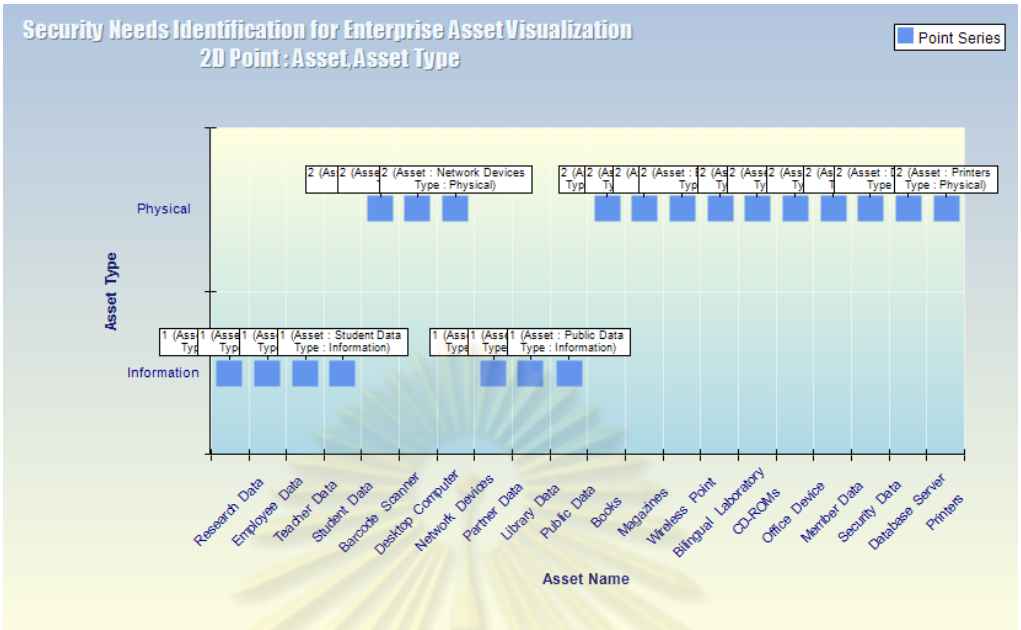
เพื่อความเข้าใจที่ชัดเจนมากยิ่งขึ้น ในที่นี้จะขอตัวอย่างการวิเคราะห์การสร้างภาพนามธรรมจากแบบรูปความมั่นคงการระบุความต้องการด้านความมั่นคงสำหรับสินทรัพย์องค์กร โดยจะขอยกตัวอย่างรูปที่ 3.7 ซึ่งแสดงในบทที่ 3 นำมาแสดงเป็นรูปที่ 4.1 ซึ่งแสดงให้เห็นถึงแผนภาพคลาสของแบบรูปการระบุความต้องการด้านความมั่นคงสำหรับสินทรัพย์องค์กร จะเห็นได้ว่ามี 4 คลาสที่เกี่ยวข้อง คือ Asset, Business Driver, Security Property และ Asset-Security Property ในที่นี้ผู้วิจัยขอยกตัวอย่างการสร้างภาพนามธรรมภายในคลาสเดียวกัน (ในที่นี้คือคลาส Asset) และตัวอย่างการสร้างภาพนามธรรมระหว่างคลาส (ในที่นี้คือคลาส Asset และ Business Driver) โดยมีรายละเอียดดังนี้



รูปที่ 4.1 แผนภาพคลาสของแบบรูปความมั่นคงการระบุความต้องการด้านความมั่นคงสำหรับสินทรัพย์องค์กร

1) การสร้างภาพนามธรรมภายในคลาสเดียวกัน

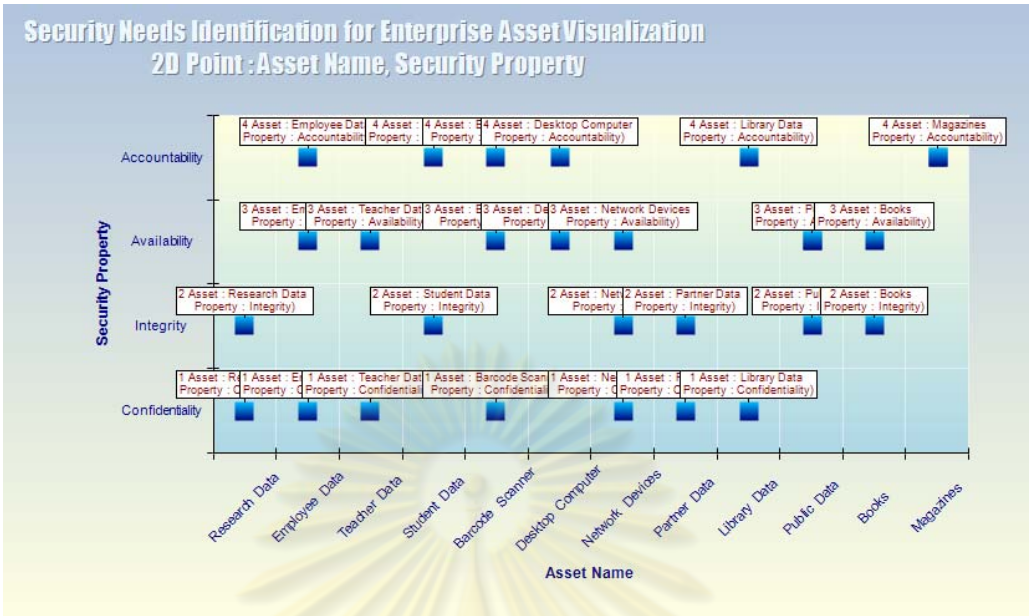
พิจารณาคลาส Asset ในกรณีนี้ผู้วิจัยนำลักษณะประจำ assetName และ assetType มาสร้างเป็นภาพนามธรรม โดยใช้แผนภูมิแบบจุดสองมิติ ดังแสดงในรูป 4.2 โดยกำหนดให้แกนนอน (แกน x) แทนค่าของลักษณะประจำ assetName และแกนตั้ง (แกน y) แทนค่าลักษณะประจำ assetType ซึ่งสอดคล้องกับผลเฉลยของแบบรูปความมั่นคง คือ สินทรัพย์ขององค์กรสามารถแบ่งออกได้เป็นสองประเภท คือ ประเภทกายภาพ และประเภทข้อมูล



รูปที่ 4.2 การสร้างภาพนามธรรมจากแบบรูปความมั่นคงภายในคลาสเดียวกัน

2) การสร้างภาพนามธรรมระหว่างคลาส

พิจารณาคลาส Asset และคลาส Security Property ในกรณีนี้ผู้วิจัยนำลักษณะประจำ assetName จากคลาส Asset และนำลักษณะประจำ propertyName จากคลาส Security Property มาสร้างเป็นภาพนามธรรม โดยใช้แผนภูมิแบบจุดสองมิติ ดังแสดงในรูป 4.3 โดยกำหนดให้แกนนอน (แกน x) แทนค่าของลักษณะประจำ assetName และแกนตั้ง (แกน y) แทนค่าลักษณะประจำ propertyName ซึ่งสอดคล้องกับผลเฉลยของแบบรูปความมั่นคง คือ องค์กรควรมีการกำหนดค่าคุณสมบัติความมั่นคงให้กับสินทรัพย์ โดยคุณสมบัติความมั่นคงประกอบไปด้วย การรักษาความลับ (Confidentiality) ความบูรณภาพ (Integrity) สภาพพร้อมใช้งาน (Availability) และภาวะรับผิดชอบ (Accountability)



รูปที่ 4.3 การสร้างภาพนามธรรมจากแบบรูปความมั่นคงระหว่างคลาส

4.1.2 การสร้างภาพนามธรรมจากรายการที่มีไว้ให้

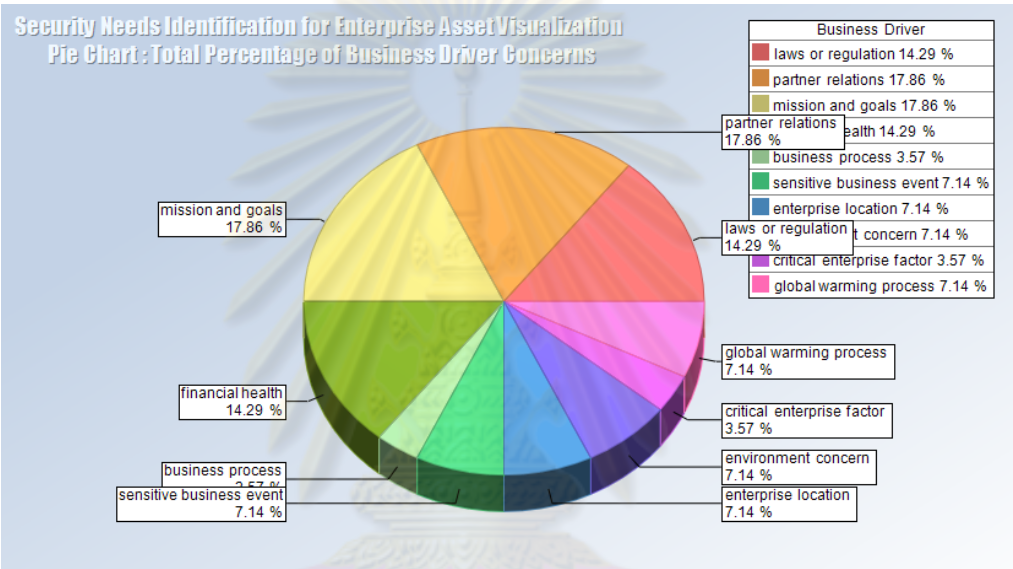
ในการออกแบบการสร้างภาพนามธรรมจากรายการที่มีไว้ให้ ผู้วิจัยได้ศึกษาและวิเคราะห์ข้อมูลการจัดหมวดหมู่ของแบบรูปความมั่นคงทำให้ทราบถึงหมวดหมู่และประเภทของแบบรูปความมั่นคงและความสัมพันธ์ในแต่ละหมวดหมู่ แบบรูปความมั่นคงทำให้ทราบถึงความหมายผลเฉลย ส่วนประกอบสำคัญของแบบรูปความมั่นคง และไวยากรณ์ความมั่นคงทำให้ทราบถึงส่วนประกอบสำคัญ และความสัมพันธ์ระหว่างไวยากรณ์แบบรูปความมั่นคง ตลอดจนผลลัพธ์แผนภาพคลาสแบบบูรณาการความสัมพันธ์ของแบบรูปความมั่นคงทั้งหมดที่ได้จากบทที่ 3 แล้วนำมาวิเคราะห์เป็นข้อมูลสรุปที่เหมาะสมที่ผู้ใช้งานต้องการทราบ ทั้งนี้รายการการสร้างภาพนามธรรมจากรายการที่มีไว้ให้ทั้งหมดได้แสดงไว้ในตาราง 4.2

ตารางที่ 4.2 ตารางรายการตัวเลือกการสร้างภาพนามธรรมจากรายการที่มีไว้ให้

กลุ่มของแบบรูปความมั่นคง	ชนิดของแผนภูมิ	ตัวอย่างที่กำหนดให้
กลุ่มการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง	แผนภูมิเรดาร์	Top 5 highest asset risk values using radar chart
	แผนภูมิแท่งแบบเรียงซ้อน	Top 5 highest asset risk values using stack bar chart
	แผนภูมิแบบจุดสองมิติ	Relationships of asset, threat action and threat likelihood
	แผนภูมิจุดแบบสามมิติ	Relationships of asset, threat action and vulnerability
	แผนภูมิรูปวงกลม	Total percentage of business driver concern
กลุ่มการระบุตัวตนและการพิสูจน์ตัวจริง	แผนภูมิเรดาร์	Summary of I&A requirements with I&A technique profile
	แผนภูมิแบบจุดสองมิติ	Relationships of Passwords and Password Policy
	แผนภูมิเรดาร์	Classifying biometrics with technique factor
กลุ่มแบบจำลองควบคุมการเข้าถึง	แผนภูมิเรดาร์	Student Role associates with assets and rights
	แผนภูมิเรดาร์	Teacher Role associates with assets and rights
	แผนภูมิแบบฟอง	The multilevel of asset classification and category
กลุ่มสถาปัตยกรรมไฟร์วอลล์	แผนภูมิแบบจุดสองมิติ	Relationships of external host and internal host
	แผนภูมิแบบจุดสองมิติ	Relationships of external host and application service
	แผนภูมิแบบจุดสองมิติ	Relationships of external host and state session

เพื่อความเข้าใจที่ชัดเจนมากยิ่งขึ้น ในที่นี้จะขอยกตัวอย่างของแบบรูปความมั่นคงการระบุความต้องการด้านความมั่นคงสำหรับสินทรัพย์องค์กร โดยยกตัวอย่างรายการตัวขับเคลื่อนทางธุรกิจใดที่นำมาใช้พิจารณาในการกำหนดคุณสมบัติความมั่นคงให้แก่สินทรัพย์มากที่สุด โดย

ใช้แผนภูมิรูปวงกลม ดังแสดงผลในรูป 4.4 ซึ่งหากพิจารณาในรูป 4.1 แล้วจะพบว่าภาพนามธรรมนี้เป็นการพิจารณาคลาส Business Driver โดยเลือกลักษณะประจำ driverName นำแต่ละรายการข้อมูลตัวขับเคลื่อนทางธุรกิจมาคำนวณค่าร้อยละ แล้วเปรียบเทียบกับผลรวมรายการข้อมูลตัวขับเคลื่อนทางธุรกิจทั้งหมด ในการแปลความหมายจะสอดคล้องกับผลเฉลยของแบบรูปความมั่นคงที่ว่า ในการกำหนดคุณสมบัติความมั่นคงให้แก่สินทรัพย์ขององค์กรนั้นจะต้องมีการระบุคุณสมบัติด้านความมั่นคงให้กับสินทรัพย์โดยพิจารณาจากตัวขับเคลื่อนทางธุรกิจ



รูปที่ 4.4 การสร้างภาพนามธรรมจากรายการที่มีไว้ให้

4.1.3 การสร้างภาพนามธรรมจากลักษณะประจำใด ๆ

ในการออกแบบการสร้างภาพนามธรรมจากลักษณะประจำใดๆ ผู้วิจัยได้ศึกษาและวิเคราะห์ข้อมูลแบบรูปความมั่นคงทำให้ทราบถึงความหมาย ผลเฉลย ส่วนประกอบสำคัญของแบบรูปความมั่นคง และไวยากรณ์ความมั่นคงทำให้ทราบถึงส่วนประกอบสำคัญ และความสัมพันธ์ระหว่างไวยากรณ์แบบรูปความมั่นคง ตลอดจนผลลัพธ์แผนภาพคลาสแบบบูรณาการความสัมพันธ์ของแบบรูปความมั่นคงทั้งหมดที่ได้จากบทที่ 3 แล้วนำมาวิเคราะห์เพื่อสร้างเป็นความสัมพันธ์ระหว่างลักษณะประจำใดๆ ที่ผู้ใช้งานสามารถเลือกได้ การแสดงผลการสร้างภาพนามธรรมในหัวข้อนี้จะใช้แผนภูมิจุดแบบสองมิติ และสามมิติ โดยขั้นตอนวิธีในการสร้างความสัมพันธ์ระหว่าง 2 และ 3 ลักษณะประจำใดๆ สามารถแสดงได้ดังรูปที่ 4.5 และรูปที่ 4.7 ตามลำดับ ทั้งนี้รายการลักษณะประจำที่ผู้ใช้งานสามารถเลือกได้แบบ 2 ลักษณะประจำแสดงได้

ดังตารางที่ 4.3 และรายการลักษณะประจำที่ผู้ใช้งานสามารถเลือกได้แบบ 3 ลักษณะประจำแสดงไว้ในภาคผนวก ก

ข้อมูลนำเข้า แผนภาพคลาสแบบบูรณาการแบบรูปความมั่นคงที่ได้จากบทที่ 3
ข้อมูลออก ความสัมพันธ์ของลักษณะประจำใดๆ 2 ลักษณะประจำ
เริ่มต้น
นำเข้าแผนภาพคลาสแบบบูรณาการแบบรูปความมั่นคง
สำหรับ คลาส$_i$ ใดๆ จากแผนภาพคลาส **จนกระทั่ง** สิ้นสุดคลาสที่นำมาพิจารณา
สำหรับ คลาส$_j$ ใดๆ จากแผนภาพคลาส **จนกระทั่ง** สิ้นสุดคลาสที่นำมาพิจารณา
ถ้า คลาส$_i$ และ คลาส$_j$ มีเส้นเชื่อมความสัมพันธ์ระหว่างคลาส < 4
ดำเนินการ
ถ้า คลาส$_i$ และ คลาส$_j$ มีความสัมพันธ์กัน ตามข้อมูลการวิเคราะห์จากการจัดหมวดหมู่ของแบบรูปความมั่นคง แบบรูปความมั่นคงและไวยากรณ์ความมั่นคง
ดำเนินการ
เลือกลักษณะประจำที่มีความสัมพันธ์ระหว่าง คลาส$_i$ และ คลาส$_j$ (แต่ละคลาสอาจมีตัวแทนลักษณะประจำมากกว่า 1 ก็ได้)
หยุดการทำงาน

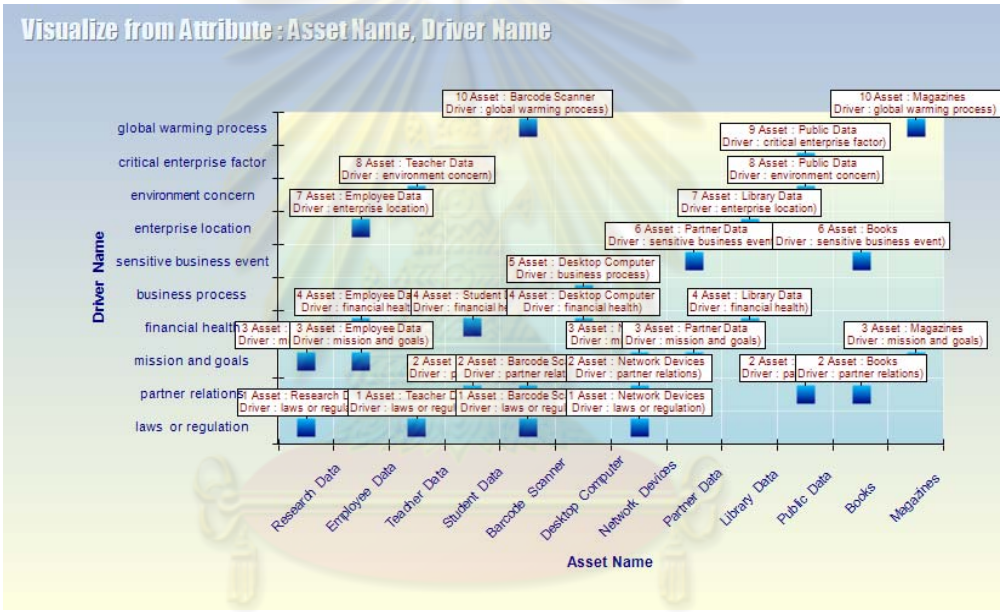
รูปที่ 4.5 ขั้นตอนวิธีในการสร้างความสัมพันธ์ระหว่าง 2 ลักษณะประจำใดๆ

จากรูปที่ 4.5 เมื่อพิจารณาคลาส$_i$ และ คลาส$_j$ ใดๆ แล้ว หากว่าเส้นความสัมพันธ์ระหว่างสองคลาสนี้มีระยะห่างมากกว่า 4 เส้นแล้ว ทั้งสองคลาสจะไม่สามารถเชื่อมความสัมพันธ์กันได้ เนื่องจากผู้วิจัยได้วิเคราะห์และพิจารณาจากแบบจำลองเชิงโครงสร้าง และความหมายในแต่ละคลาสเมื่ออ้างอิงตามบริบทของของแบบรูปความมั่นคงแล้ว พบว่าหากสองคลาสใดๆ มีเส้นความสัมพันธ์มากกว่า 4 เส้นแล้วจะส่งผลกระทบต่อการแปลความหมายระหว่างคลาส กล่าวคือ การแปลความหมายจะทำความเข้าใจได้ยาก เนื่องจากต้องแปลความระหว่างสองคลาสที่มีเส้นเชื่อมความสัมพันธ์ก่อน แล้วจึงค่อยแปลความคลาสอื่นๆ ที่อยู่ถัดไป ทำให้มีคลาสที่ต้องแปลความหมายเพิ่มมากขึ้น และความหมายตามบริบทของแบบรูปความมั่นคงจะค่อยๆ ลดลง โดยแปรผกผันกับระยะห่างระหว่างคลาส

ตาราง 4.3 รายการข้อมูลลักษณะประจำ โดยแสดงผลในรูปแผนภูมิแบบจุดสองมิติ

	assetName	assetType	propertyName	driverName	overallValue	threatAction	threatConsequence	threatSourceName	threatLikelihoodName	vulnerabilityName	assetRiskValue	approachName	severityScaleName	businessPriorityName	serviceName	partnerName	partnerType	communicationChannel	exchangeMethodName	serviceTermination	I&AServiceName	I&ARequirementName	factorName	domainName	priorityImpactName	techniqueName	profileRatingName	passwordName	passwordPolicyName	biometricMechanism	techniqueFactorName	biometricCharacteristic	userName	rightName	roleName	categoryUserName	clearanceLevelName	categoryAssetName	classificationLevel	externalIP	externalHostName	internalIP	internalHostName	appSerViceName	sessionName
assetName		✓	✓	✓	✓	✓				✓	✓	✓			✓	✓					✓					✓									✓				✓	✓						
assetType	✓																																												
propertyName	✓			✓																																									
driverName	✓		✓																																										
overallValue	✓																																												
threatAction	✓						✓	✓																																					
threatConsequence						✓																																							
threatSourceName						✓																																							
threatLikelihoodName																																													
vulnerabilityName	✓												✓																																
assetRiskValue	✓																																											
approachName	✓																																											
severityScaleName										✓																																		
businessPriorityName																																												
serviceName	✓																																								✓	✓				
partnerName	✓																✓	✓			✓															✓										
partnerType																✓																														
communicationChannel																✓			✓																											
exchangeMethodName																		✓																											
serviceTermination																																													
I&AServiceName	✓																					✓				✓									✓										
I&ARequirementName																					✓			✓																					
factorName																																													
domainName																						✓																						
priorityImpactName																																													
techniqueName	✓																																												
profileRatingName																																													
passwordName																												✓																	
passwordPolicyName																											✓																		
biometricMechanism																																													
techniqueFactorName																																													
biometricCharacteristic																																													
userName																																					✓	✓	✓							
rightName																																													
roleName	✓															✓					✓													✓										
categoryUserName																																		✓										
clearanceLevelName																																		✓										
categoryAssetName	✓																																											
classificationLevel	✓																																											
externalIP															✓																										✓				✓
externalHostName															✓																											✓			✓
internalIP																																								✓					
internalHostName																																									✓				
appSerViceName																																													
sessionName																																									✓	✓				

เพื่อความเข้าใจที่ชัดเจนมากยิ่งขึ้น ในที่นี้จะยกตัวอย่างการพิจารณารูปแผนภาพคลาสที่ 4.1 ของแบบรูปความมั่นคงการระบุความต้องการด้านความมั่นคงสำหรับสินทรัพย์องค์กรโดยการเลือกลักษณะประจำ assetName จากคลาส Asset และเลือกลักษณะประจำ driverName จากคลาส Business Driver โดยกำหนดให้แกนนอน (แกน x) แทนค่าของลักษณะประจำ assetName และแกนตั้ง (แกน y) แทนค่าลักษณะประจำ driverName ซึ่งสอดคล้องกับผลเฉลยของแบบรูปความมั่นคงที่ว่า ในการกำหนดคุณสมบัติความมั่นคงให้แก่สินทรัพย์ขององค์กรนั้นจะต้องมีการระบุคุณสมบัติด้านความมั่นคงให้กับสินทรัพย์โดยพิจารณาจากตัวขับเคลื่อนทางธุรกิจ โดยตัวอย่างภาพนามธรรมที่สร้างได้สามารถแสดงได้ดังรูปที่ 4.6



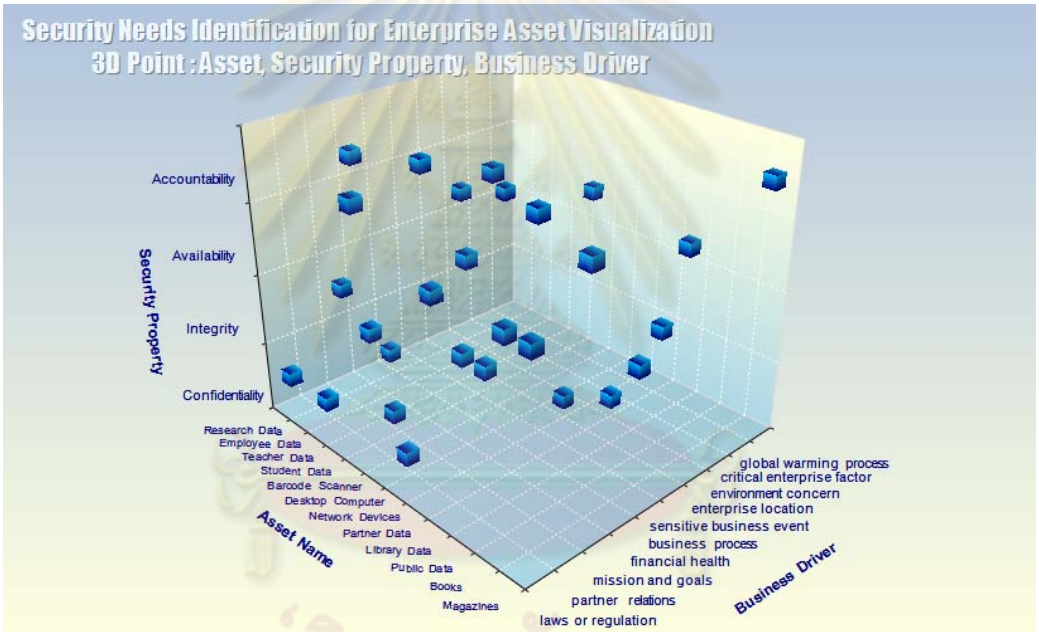
รูปที่ 4.6 การสร้างภาพนามธรรมจากการเลือก 2 ลักษณะประจำ

ข้อมูลนำเข้า แผนภาพคลาสแบบบูรณาการแบบรูปความมั่นคงที่ได้จากบทที่ 3
ข้อมูลออก ความสัมพันธ์ของลักษณะประจำใดๆ 3 ลักษณะประจำ
เริ่มต้น
นำเข้าแผนภาพคลาสแบบบูรณาการแบบรูปความมั่นคง
สำหรับ คลาส$_i$ ใดๆ จากแผนภาพคลาส **จนกระทั่ง** สิ้นสุดคลาสที่นำมาพิจารณา
FOR คลาส$_j$ ใดๆ จากแผนภาพคลาส **จนกระทั่ง** สิ้นสุดคลาสที่นำมาพิจารณา
FOR คลาส$_k$ ใดๆ จากแผนภาพคลาส **จนกระทั่ง** สิ้นสุดคลาสที่นำมาพิจารณา
ถ้า คลาส$_i$, คลาส$_j$ และคลาส$_k$ มีเส้นเชื่อมความสัมพันธ์ระหว่างคลาส < 4 **ดำเนินการ**
ถ้า คลาส$_i$, คลาส$_j$ และคลาส$_k$ มีความสัมพันธ์กัน ตามข้อมูลการวิเคราะห์จากการจัดหมวดหมู่ของแบบรูปความมั่นคง แบบรูปความมั่นคง และไวยากรณ์ความมั่นคง
ดำเนินการ
เลือกลักษณะประจำที่มีความสัมพันธ์กันทั้ง 3 คลาส
(แต่ละคลาสอาจมีตัวแทนลักษณะประจำมากกว่า 1 ก็ได้)
สิ้นสุดการทำงาน

รูปที่ 4.7 ขั้นตอนวิธีในการสร้างความสัมพันธ์ระหว่าง3 ลักษณะประจำใดๆ

จากรูปที่ 4.7 เมื่อพิจารณาคลาส$_i$ คลาส$_j$ และ คลาส$_k$ ใดๆ แล้ว หากว่าเส้นความสัมพันธ์ระหว่างสองคลาสใดๆ นี้มีระยะห่างมากกว่า 4 เส้นแล้ว ทั้งสองคลาสจะไม่สามารถเชื่อมความสัมพันธ์กันได้ เนื่องจากผู้วิจัยได้วิเคราะห์และพิจารณาจากแบบจำลองเชิงโครงสร้าง และความหมายในแต่ละคลาสเมื่ออ้างอิงตามบริบทของของแบบรูปความมั่นคงแล้ว พบว่าหากสองคลาสใดๆ มีเส้นความสัมพันธ์มากกว่า 4 เส้นแล้วจะส่งผลกระทบต่อการแปลความหมายระหว่างคลาส กล่าวคือ การแปลความหมายจะทำความเข้าใจได้ยาก เนื่องจากต้องแปลความระหว่างสองคลาสที่มีเส้นเชื่อมความสัมพันธ์ก่อน แล้วจึงค่อยแปลความคลาสอื่นๆ ที่อยู่ถัดไป ทำให้มีคลาสที่ต้องแปลความหมายเพิ่มมากขึ้น และความหมายตามบริบทของแบบรูปความมั่นคงจะค่อยๆ ลดลง โดยแปรผกผันกับระยะห่างระหว่างคลาส

เพื่อความเข้าใจที่ชัดเจนมากยิ่งขึ้น ในที่นี้จะยกตัวอย่างการพิจารณารูปแผนภาพคลาสที่ 4.1 ของแบบรูปความมั่นคงการระบุความต้องการด้านความมั่นคงสำหรับสินทรัพย์องค์กรโดยการเลือกลักษณะประจำ assetName จากคลาส Asset เลือกลักษณะประจำ propertyName จากคลาส Security Property และเลือกลักษณะประจำ driverName จากคลาส Business Driver โดยกำหนดให้แกนนอน (แกน x) แทนค่าของลักษณะประจำ assetName แกนตั้ง (แกน y) แทนค่าลักษณะประจำ propertyName และแกนลึก (แกน z) แทนค่าลักษณะประจำ driverName ซึ่งสอดคล้องกับผลเฉลยของแบบรูปความมั่นคงที่ว่า ในการกำหนดคุณสมบัติความมั่นคงให้แก่สินทรัพย์ขององค์กรนั้นจะต้องมีการระบุคุณสมบัติด้านความมั่นคงให้กับสินทรัพย์โดยพิจารณาจากตัวขับเคลื่อนทางธุรกิจ โดยตัวอย่างภาพนามธรรมที่สร้างได้สามารถแสดงได้ดังรูปที่ 4.8

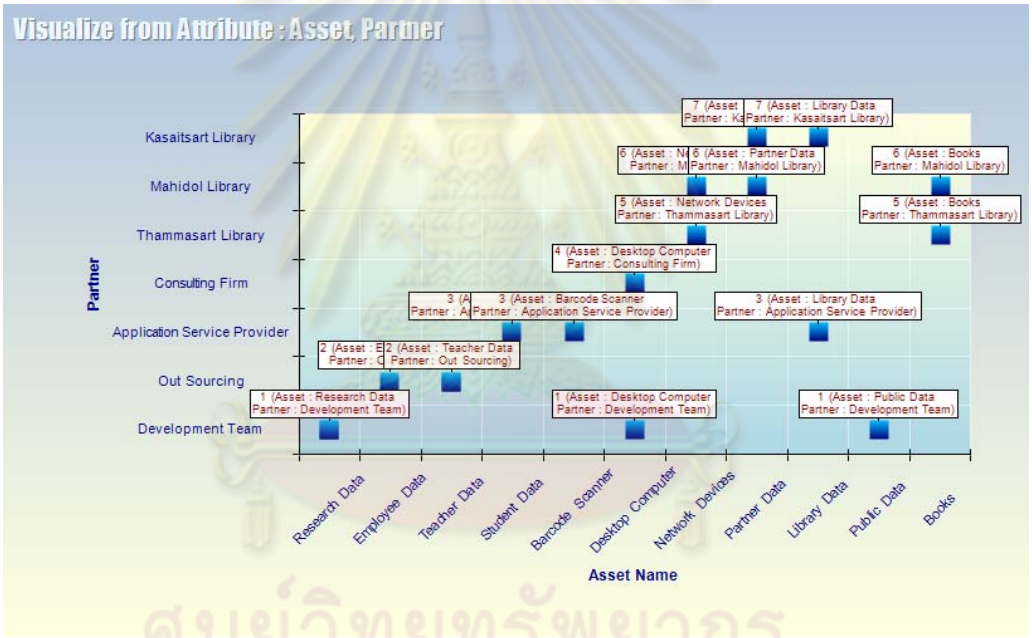


รูปที่ 4.8 การสร้างภาพนามธรรมจากการเลือก 3 ลักษณะประจำ

ทั้งนี้ความหมายในแต่ละประเภทของแผนภูมิที่เครื่องมือต้นแบบสามารถสร้างได้ พร้อมกับรูปภาพตัวอย่างของแต่ละแผนภูมิแสดงได้ดังตารางที่ 4.4 – 4.11

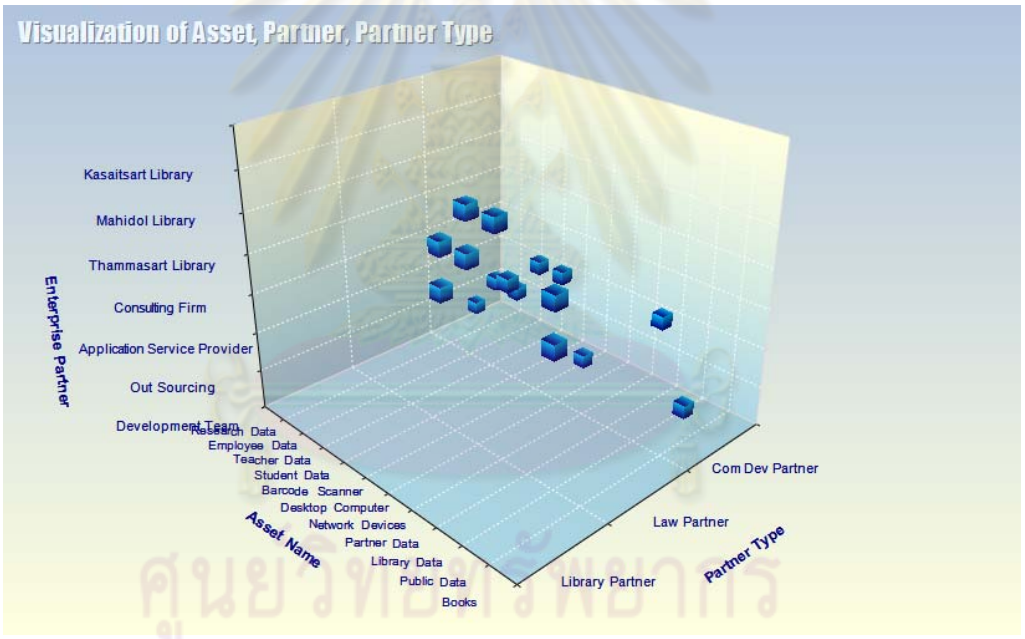
ตารางที่ 4.4 ความหมายของแผนภูมิแบบจุดสองมิติ

ชื่อแผนภูมิ	แผนภูมิแบบจุดสองมิติ
ความหมาย	แผนภูมิแบบจุดสองมิติ เป็นแผนภูมิที่ใช้สำหรับแสดงความสัมพันธ์ระหว่างข้อมูล 2 ชุดข้อมูล โดยอาศัยการแสดง หรือการลงจุดกลุ่มของสองข้อมูลให้เสมือนเป็นหนึ่งชุดข้อมูล แผนภูมิแบบจุดสองมิตินี้มีแกนค่าสองแกน ซึ่งแสดงชุดของข้อมูลตัวเลขชุดหนึ่งตามแกนนอน (แกน x) และแสดงข้อมูลอีกชุดหนึ่งตามแกนตั้ง (แกน y) แผนภูมินี้มักใช้เพื่อแสดงและเปรียบเทียบข้อมูลทางวิทยาศาสตร์ ข้อมูลทางสถิติ และข้อมูลทางวิศวกรรม
ตัวอย่างภาพนามธรรมที่สร้างได้จากเครื่องมือ	



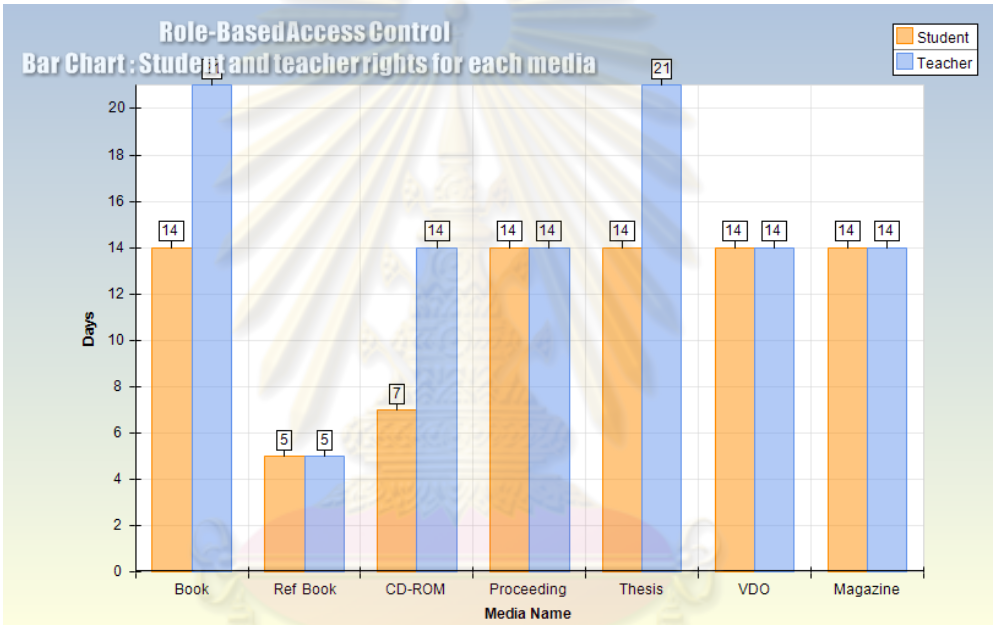
ตารางที่ 4.5 ความหมายของแผนภูมิแบบจุดสามมิติ

ชื่อแผนภูมิ	แผนภูมิแบบจุดสามมิติ
ความหมาย	แผนภูมิแบบจุดสามมิติ เป็นแผนภูมิที่ใช้สำหรับแสดงความสัมพันธ์ระหว่างข้อมูล 3 ชุดข้อมูล โดยอาศัยการแสดง หรือการลงจุดกลุ่มของสามข้อมูลให้เสมือนเป็นหนึ่งชุดข้อมูล แผนภูมิแบบจุดสามมิตินี้มีแกนค่าสามแกน ซึ่งแสดงชุดของข้อมูลตัวเลขชุดหนึ่งตามแกนนอน (แกน x) แสดงข้อมูลอีกชุดหนึ่งตามแกนตั้ง (แกน y) และแสดงข้อมูลอีกชุดหนึ่งตามแกนลึก (แกน z) แผนภูมินี้มักใช้เพื่อแสดงและเปรียบเทียบข้อมูลทางวิทยาศาสตร์ ข้อมูลทางสถิติ และข้อมูลทางวิศวกรรม
ตัวอย่างภาพนามธรรมที่สร้างได้จากเครื่องมือ	



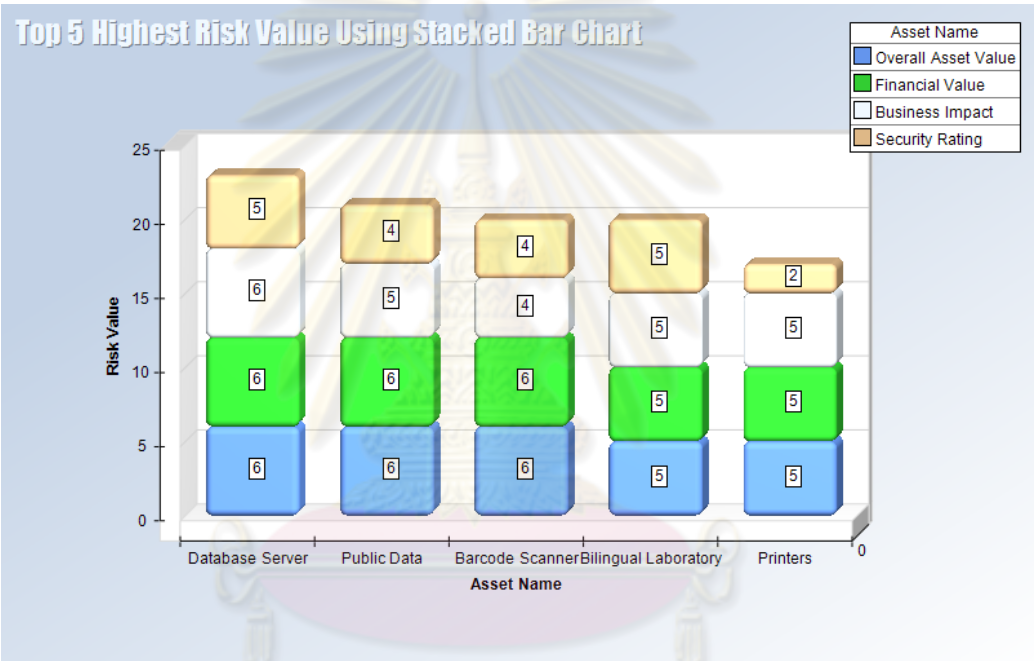
ตารางที่ 4.6 ความหมายของแผนภูมิแท่ง

ชื่อแผนภูมิ	แผนภูมิแท่ง
ความหมาย	แผนภูมิแท่ง เป็นแผนภูมิที่ใช้สำหรับแสดงภาพประกอบการเปรียบเทียบระหว่างรายการ โดยจะแสดงค่าในสี่เหลี่ยมผืนผ้าแนวตั้งแบบสองมิติ แต่แผนภูมิแท่งแบบสามมิติ จะแสดงข้อมูลโดยการใช้ทัศนมิติ (Perspective) แบบสามมิติเท่านั้น และจะไม่ใช้แกนลึก
ตัวอย่างภาพนามธรรมที่สร้างได้จากเครื่องมือ	



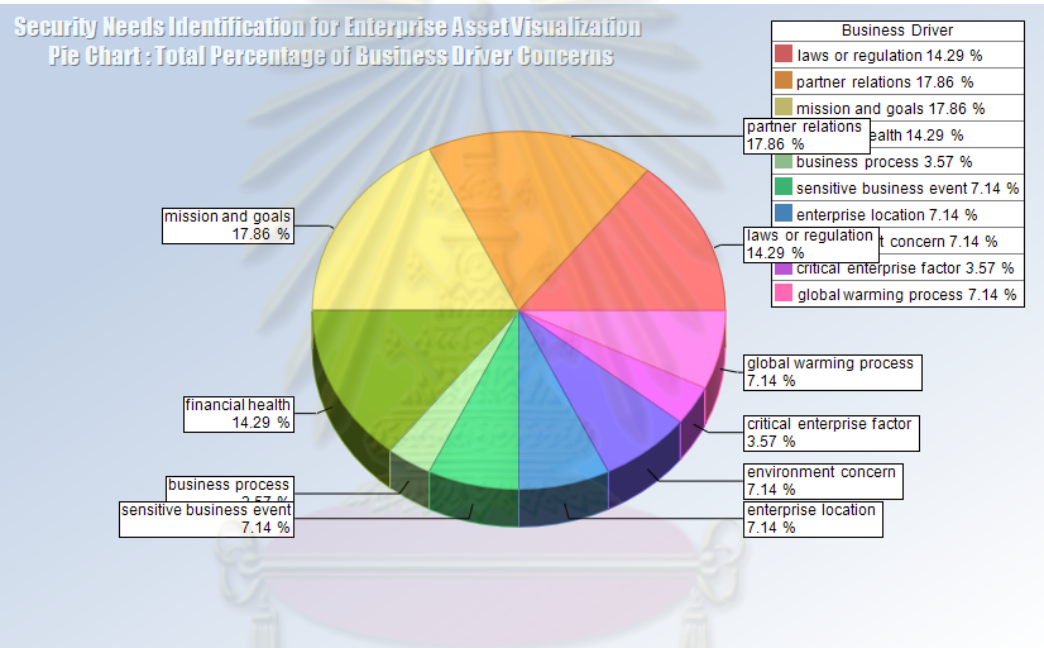
ตารางที่ 4.7 ความหมายของแผนภูมิแท่งแบบเรียงซ้อน

ชื่อแผนภูมิ	แผนภูมิแท่งแบบเรียงซ้อน
ความหมาย	แผนภูมิแท่งแบบเรียงซ้อน เป็นแผนภูมิที่ใช้สำหรับแสดงความสัมพันธ์ของรายการข้อมูลแต่ละรายการเปรียบเทียบกับรายการข้อมูลทั้งหมด โดยการแสดงผลแต่ละรายการข้อมูล สามารถใช้สี่เหลี่ยมผืนผ้าแนวตั้งทั้งแบบสองมิติและสามมิติ
ตัวอย่างภาพนามธรรมที่สร้างได้จากเครื่องมือ	



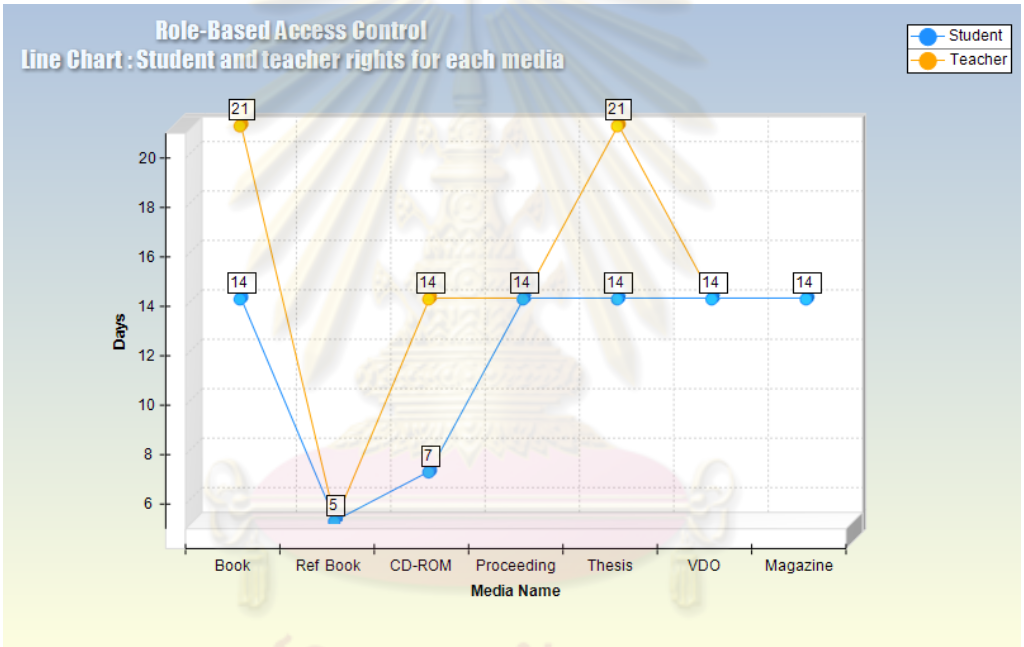
ตารางที่ 4.8 ความหมายของแผนภูมิรูปวงกลม

ชื่อแผนภูมิ	แผนภูมิรูปวงกลม
ความหมาย	แผนภูมิรูปวงกลม เป็นแผนภูมิที่ใช้สำหรับแสดงขนาดของหนึ่งรายการข้อมูลเป็นสัดส่วนกับผลรวมของรายการข้อมูลทั้งหมดในแผนภูมิรูปวงกลม โดยในการแสดงผลแต่ละรายการข้อมูลจะถูกแสดงผลโดยคิดเป็นร้อยละของวงกลมทั้งวง
ตัวอย่างภาพนามธรรมที่สร้างได้จากเครื่องมือ	



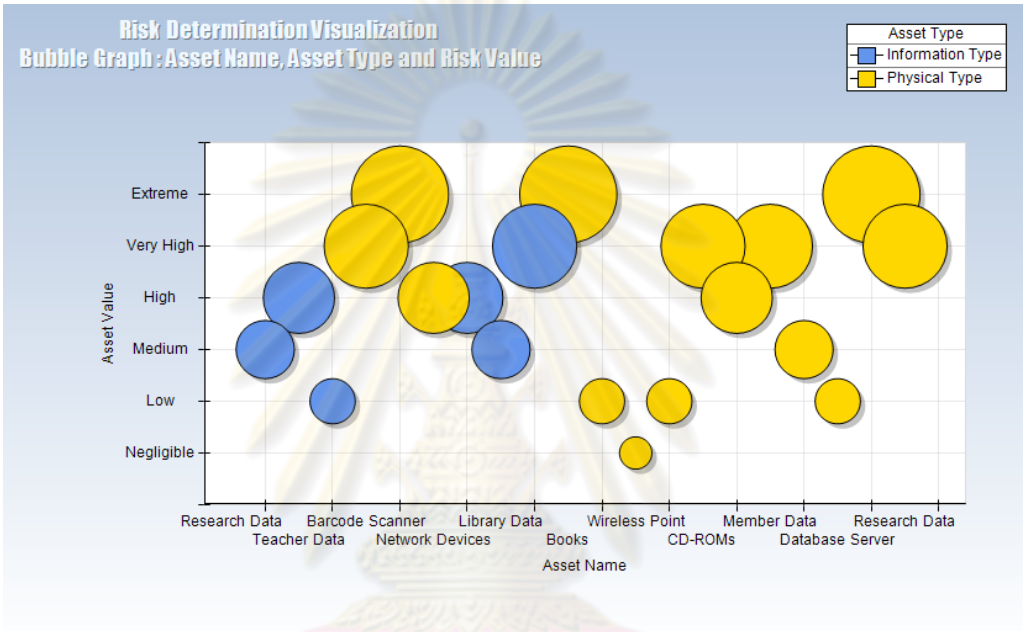
ตารางที่ 4.9 ความหมายของแผนภูมิเส้น

ชื่อแผนภูมิ	แผนภูมิแบบเส้น
ความหมาย	แผนภูมิแบบเส้น เป็นแผนภูมิที่ใช้สำหรับแสดงข้อมูลที่มีความต่อเนื่องกันในช่วงระยะเวลาหนึ่งตามมาตราส่วนทั่วไป จึงเป็นแผนภูมิที่เหมาะสำหรับนำไปใช้แสดงแนวโน้มของข้อมูลที่มีระยะห่างเวลา เท่ากัน ในแผนภูมิเส้นข้อมูลประเภทจะกระจายเท่ากันตามแกนนอน และข้อมูลค่าทั้งหมดจะกระจายเท่ากันตามแกนตั้ง
ตัวอย่างภาพนามธรรมที่สร้างได้จากเครื่องมือ	



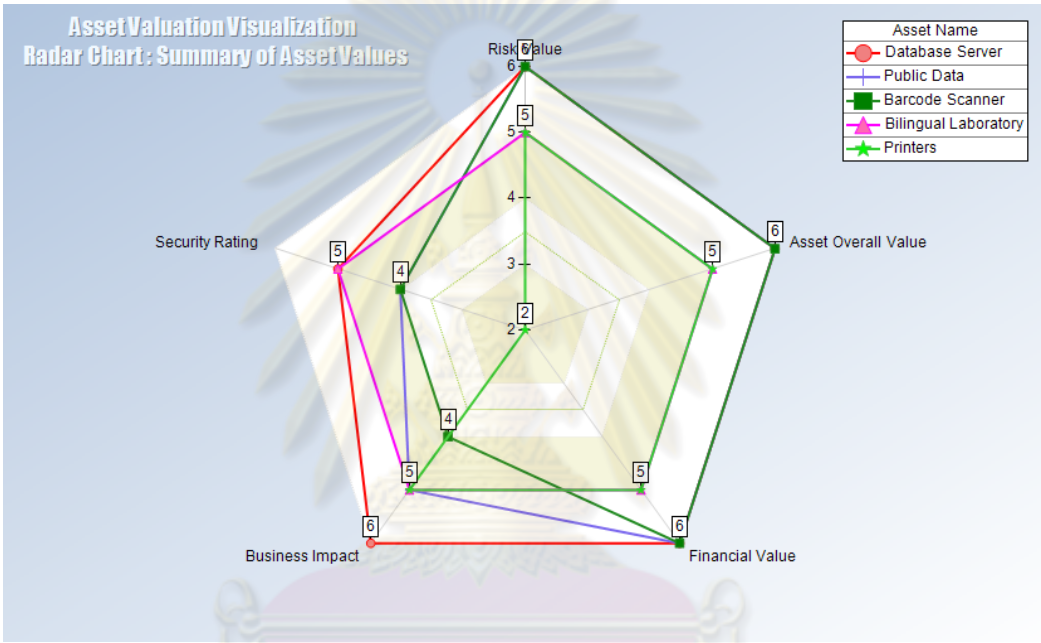
ตารางที่ 4.10 ความหมายของแผนภูมิแบบฟอง

ชื่อแผนภูมิ	แผนภูมิแบบฟอง
ความหมาย	แผนภูมิแบบฟอง เป็นแผนภูมิที่ใช้สำหรับแสดงเปรียบเทียบชุดของค่าสามค่า จากแกนนอน แกนตั้ง ส่วนค่าที่สามจะเป็นตัวกำหนดขนาดของฟอง
ตัวอย่างภาพนามธรรมที่สร้างได้จากเครื่องมือ	



ตารางที่ 4.11 ความหมายของแผนภูมิเรดาร์

ชื่อแผนภูมิ	แผนภูมิเรดาร์
ความหมาย	แผนภูมิเรดาร์ เป็นแผนภูมิที่ใช้สำหรับแสดงการเปรียบเทียบของค่าสะสมของชุดข้อมูลหลายชุด จะแสดงการเปลี่ยนแปลงของค่าเมื่อเทียบกับจุดศูนย์กลางจุดหนึ่ง
ตัวอย่างภาพนามธรรมที่สร้างได้จากเครื่องมือ	



4.2 การออกแบบหน้าที่การทำงานของเครื่องมือต้นแบบ

เครื่องมือต้นแบบสำหรับสร้างภาพนามธรรมของความต้องการด้านความมั่นคงนั้น เป็นเครื่องมือที่สนับสนุนการดำเนินการและการจัดการความต้องการด้านความมั่นคง ทำให้ผู้ใช้งานมีความสะดวก มองเห็นภาพของความต้องการด้านความมั่นคงที่ถูกกำหนดขึ้นได้อย่างชัดเจน โดยหน้าที่การทำงานของเครื่องมือต้นแบบนี้สามารถนำเสนอด้วยแผนภาพยูสเคส (Use Case Diagram) ซึ่งเป็นแผนภาพที่อธิบายการติดต่อกันระหว่างผู้ใช้ระบบ (Actors) กับฟังก์ชันงานต่างๆ ที่ปรากฏในระบบ ดังนั้นในการพัฒนาเครื่องมือต้นแบบนี้ สามารถนำเสนอฟังก์ชันงานต่างๆ และการติดต่อระหว่างฟังก์ชันงาน หรือฟังก์ชันงานกับผู้ใช้ ดังรูปที่ 4.9 โดยมีรายละเอียดดังนี้

4.2.1 **ส่วนการลงทะเบียนเข้าใช้ระบบ**

สำหรับให้ผู้ใช้ทำการป้อนชื่อและรหัสผ่านเพื่อเข้าใช้งานเครื่องมือ ซึ่งข้อมูลและความต้องการด้านความมั่นคงที่เกิดขึ้นนั้นจะจำแนกตามแต่ละบัญชีผู้ใช้ ในส่วนการลงทะเบียนเข้าใช้ระบบแบ่งออกเป็น 2 ส่วนย่อย คือ

1) *การตรวจสอบรหัสผู้ใช้งาน และรหัสผ่าน* เป็นการตรวจสอบว่ามีรหัสผู้ใช้งานนี้ในฐานข้อมูลหรือไม่ และการตรวจสอบการยืนยันตัวตนของรหัสผู้ใช้งานนี้

2) *การอนุญาตให้เข้าสู่ระบบ* หากผู้ใช้งานสามารถผ่านการตรวจสอบในข้อ 1) แล้วจะสามารถเข้าใช้งานเครื่องมือต้นแบบได้

4.2.2 **ส่วนการกำหนดความต้องการด้านความมั่นคง**

ส่วนนี้จะให้ผู้ใช้เลือกแบบรูปความมั่นคงที่ต้องการมากำหนดความต้องการด้านความมั่นคง ทั้งนี้การเข้าใช้งานบางไวยากรณ์จะต้องมีการตรวจสอบความถูกต้องของข้อมูล และมีการตรวจสอบเงื่อนไขก่อนการใช้ไวยากรณ์ก่อน ซึ่งหากไม่ผ่านเงื่อนไขใดเงื่อนไขหนึ่งก็จะไม่สามารถใช้ไวยากรณ์ดังกล่าวได้

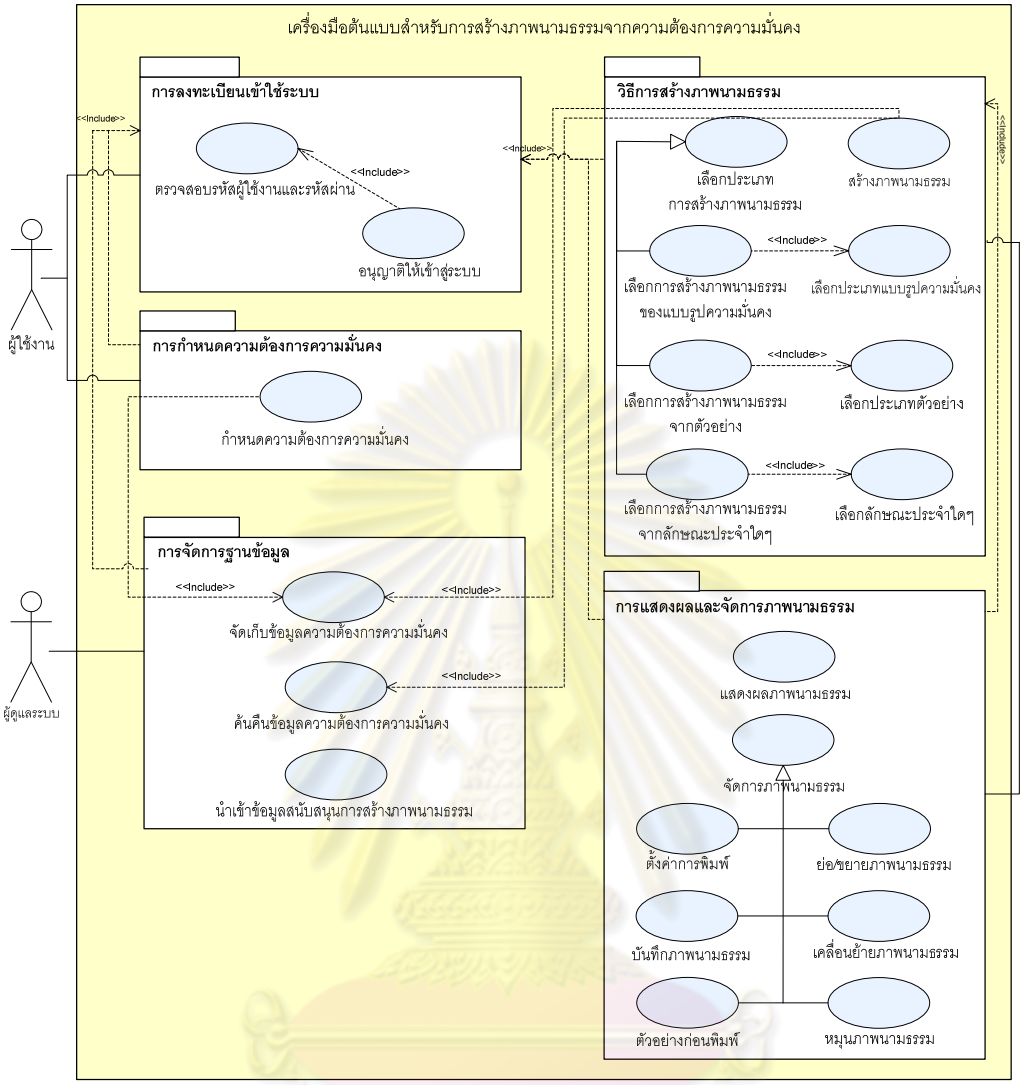
4.2.3 **ส่วนการจัดการฐานข้อมูล**

ในส่วนของการจัดการฐานข้อมูลนี้ จะแบ่งออกเป็น 3 ส่วนย่อย คือ

1) *การจัดเก็บข้อมูลความต้องการด้านความมั่นคง* ในส่วนนี้จะมีการทำงานร่วมกันกับส่วนการกำหนดความต้องการด้านความมั่นคง

2) *การค้นคืนข้อมูลความต้องการด้านความมั่นคง* ในส่วนนี้จะมีการทำงานร่วมกันกับส่วนการกำหนดความต้องการด้านความมั่นคง ส่วนการสร้างรายงานความต้องการด้านความมั่นคง และส่วนการคำนวณค่าความเสี่ยง

3) *การนำเข้าข้อมูลสนับสนุนการสร้างภาพนามธรรม* ในส่วนนี้ผู้ดูแลระบบจะเป็นผู้นำเข้าข้อมูลสนับสนุนการสร้างภาพนามธรรมลงในฐานข้อมูลโดยผ่านทางส่วนต่อประสาน



รูปที่ 4.9 แผนภาพยูสเคสของเครื่องมือต้นแบบการสร้างภาพนามธรรม
ของความต้องการด้านความมั่นคง

4.2.4 ส่วนวิธีการสร้างภาพนามธรรม

ส่วนนี้จะเป็นวิธีการสร้างภาพนามธรรมของข้อกำหนดความต้องการด้านความมั่นคงที่ได้ระบุไว้จากในส่วนที่ 4.2.2 หากยังไม่มีการระบุข้อกำหนดความต้องการด้านความมั่นคงจะไม่สามารถสร้างภาพนามธรรมได้ ในส่วนวิธีการสร้างภาพนามธรรมนี้ เครื่องมือต้นแบบสามารถสร้างภาพนามธรรมโดยอยู่ในรูปของแผนภูมิต่างๆ ทั้งแบบ 2 มิติ และ 3 มิติ เช่น แผนภูมิแท่ง (Bar Chart) แผนภูมิแท่งแบบเรียงซ้อน (Stack Bar Chart) แผนภูมิรูปวงกลม (Pie Chart) แผนภูมิเส้น

(Line Chart) แผนภูมิจุด (Point Chart) แผนภูมิแบบฟอง (Bubble Chart) และแผนภูมิเรดาร์ (Radar Chart) เป็นต้น

ผู้ใช้งานสามารถเลือกประเภทการสร้างภาพนามธรรมได้ โดยแบ่งประเภทการสร้างภาพนามธรรมออกเป็น 3 ประเภท ดังนี้

1) *การสร้างภาพนามธรรมจากแบบรูปความมั่นคง*

เป็นการสร้างภาพนามธรรมจากแบบรูปความมั่นคง โดยสามารถเลือกรายการแบบรูปความมั่นคงได้ 20 แบบรูป และสามารถเลือกรูปแบบแผนภูมิสำหรับการแสดงผลแต่ละแบบรูปความมั่นคงได้ รายการแบบรูปความมั่นคง ชนิดของแผนภูมิ และข้อมูลลักษณะประจำที่ใช้ที่ผู้ใช้งานสามารถเลือกได้ ปรากฏดังตาราง 4.1

2) *การสร้างภาพนามธรรมจากรายการที่มีไว้ให้*

ผู้ใช้งานสามารถเลือกการสร้างภาพนามธรรมจากรายการที่มีไว้ให้ได้ ซึ่งอยู่ในรูปแบบของข้อมูลสรุปต่างๆ โดยสามารถเลือกรายการได้จากแต่ละกลุ่มของแบบรูปความมั่นคง โดยรายการตัวอย่างภาพนามธรรมที่มีไว้ให้และชนิดของแผนภูมิสามารถแสดงได้ ดังตาราง 4.2

3) *การสร้างภาพนามธรรมจากข้อมูลลักษณะประจำใดๆ*

ผู้ใช้งานสามารถเลือกข้อมูลลักษณะประจำที่ต้องการนำมาสร้างภาพนามธรรมได้ โดยสามารถเลือกแผนภูมิประเภทแผนภูมิจุดแบบสองมิติ และสามมิติได้ ทั้งนี้การเลือกข้อมูลลักษณะประจำใดๆ ผู้ใช้จะสามารถเลือกได้จากแต่ละกลุ่มของแบบรูปความมั่นคง รายการข้อมูลลักษณะประจำที่ผู้ใช้สามารถเลือกได้โดยแสดงผลในรูปแผนภูมิแบบจุดสองมิติ (เลือกข้อมูลลักษณะประจำได้ 2 ข้อมูล) และสามมิติ (เลือกข้อมูลลักษณะประจำได้ 3 ข้อมูล) แสดงดังตารางที่ 4.3 และ ภาคผนวก ก ตามลำดับ

4.2.5 ส่วนการแสดงผลและจัดการภาพนามธรรม

ในส่วนนี้จะแบ่งออกเป็น 2 ส่วนย่อยดังนี้

1) *การแสดงผลภาพนามธรรม* ในส่วนนี้ใช้สำหรับแสดงผลภาพนามธรรมโดยอยู่ในรูปของแผนภูมิต่างๆ ทั้งแบบ 2 มิติ และ 3 มิติ เช่น แผนภูมิแท่ง (Bar Chart) แผนภูมิแท่งแบบเรียงซ้อน (Stack Bar Chart) แผนภูมิรูปวงกลม (Pie Chart) แผนภูมิเส้น (Line Chart) แผนภูมิจุด (Point Chart) แผนภูมิแบบฟอง (Bubble Chart) และแผนภูมิเรดาร์ (Radar Chart) เป็นต้น

2) *การจัดการภาพนามธรรม* เครื่องมือต้นแบบมีเมนูการจัดการภาพนามธรรมเพื่อให้ผู้ใช้งานสามารถจัดการภาพนามธรรมได้ โดยมีรายการเมนูดังนี้

2.1) การย่อ/ขยายภาพนามธรรม

2.2) การย้ายภาพนามธรรม

2.3) การหมุนภาพนามธรรม

2.4) การตั้งค่าการพิมพ์

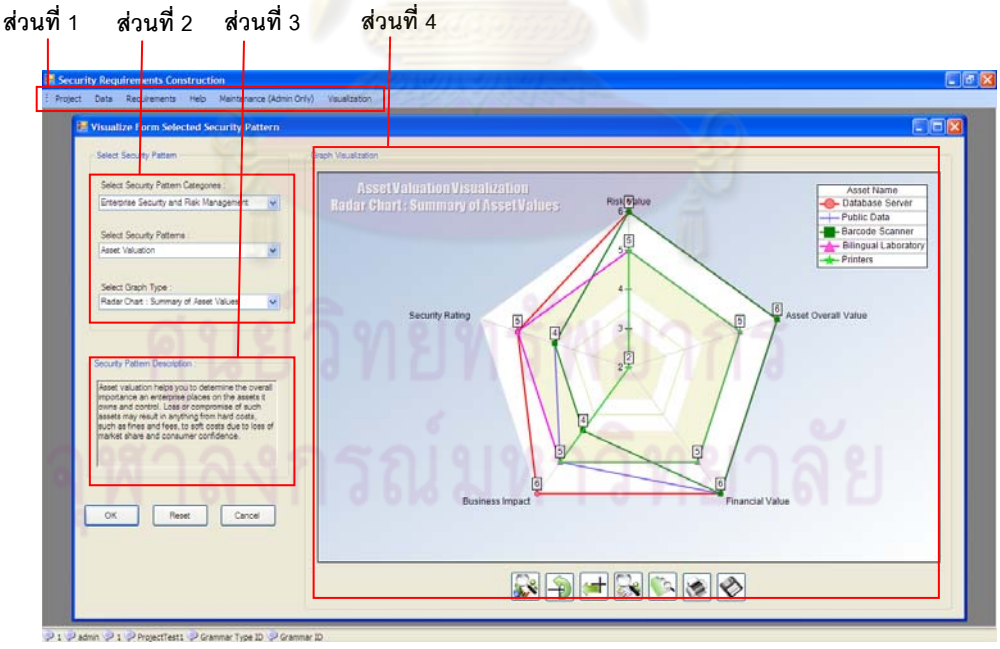
2.5) การดูภาพตัวอย่างก่อนพิมพ์

2.6) การบันทึกภาพนามธรรม

อนึ่งในงานวิทยานิพนธ์นี้ผู้วิจัยได้พัฒนาเครื่องมือต้นแบบการสร้างภาพนามธรรมจากความต้องการด้านความมั่นคงต่อจากเครื่องมือต้นแบบของ [8]

4.3 การออกแบบส่วนต่อประสานผู้ใช้

ในการออกแบบส่วนต่อประสานผู้ใช้ สามารถแบ่งออกได้เป็น 4 ส่วน ดังแสดงในรูป 4.10 โดยมีรายละเอียดในแต่ละส่วนดังต่อไปนี้



รูปที่ 4.10 โครงสร้างส่วนต่อประสานกับผู้ใช้

1) *ส่วนที่ 1 คือ ส่วนแถบเครื่องมือ* อยู่บริเวณบนด้านบนของหน้าจอ รวบรวมเมนูใช้งานต่างๆ ของเครื่องมือต้นแบบ ดังต่อไปนี้

(1) เมนู Project ผู้ใช้งานสามารถลงทะเบียนเข้าสู่ระบบ และออกจากโปรแกรมต้นแบบ

(2) เมนู Data ผู้ใช้งานสามารถสร้างสินทรัพย์องค์กร โครงงาน และกำหนดตัวขับเคลื่อนทางธุรกิจใหม่

(3) เมนู Requirements ผู้ใช้งานสามารถกำหนด แก้ไข และลบความต้องการด้านความมั่นคงได้

(4) เมนู Help เป็นเมนูช่วยเหลือผู้ใช้งาน

(5) เมนู Maintenance (Admin Only) เป็นเมนูการจัดการเกี่ยวกับผู้ใช้งานเครื่องมือต้นแบบ

(6) เมนู Visualization ผู้ใช้งานสามารถสร้างภาพนามธรรมโดยอยู่ในรูปแบบของแผนภูมิต่างๆ ทั้งแบบ 2 มิติ และ 3 มิติ เช่น แผนภูมิแท่ง (Bar Chart) แผนภูมิแท่งแบบเรียงซ้อน (Stack Bar Chart) แผนภูมิรูปวงกลม (Pie Chart) แผนภูมิเส้น (Line Chart) แผนภูมิจุด (Point Chart) แผนภูมิแบบฟอง (Bubble Chart) และแผนภูมิใยแมงมุม (Radar Chart) เป็นต้น โดยภายในเมนู Visualization ประกอบด้วยเมนูย่อยต่างๆ ดังนี้

- Visualize from Security Patterns ภายในเมนูนี้ผู้ใช้งานสามารถสร้างภาพนามธรรมจากการเลือกแบบรูปความมั่นคง และสามารถเลือกประเภทของแผนภูมิที่ต้องการได้
- Visualize from Samples ภายในเมนูนี้ผู้ใช้งานสามารถสร้างภาพนามธรรมจากรายการที่มีไว้ให้ และสามารถเลือกประเภทของแผนภูมิที่ต้องการได้
- Visualize from User Selection ภายในเมนูนี้ผู้ใช้งานสามารถสร้างภาพนามธรรมจากการเลือกข้อมูลลักษณะประจำใดๆ และสามารถเลือกประเภทของแผนภูมิที่ต้องการได้ทั้งแบบแผนภูมิแบบจุดสองมิติ และสามมิติ

2) *ส่วนที่ 2 คือ ส่วนการเลือกแบบรูปความมั่นคง* และประเภทของแผนภูมิที่ต้องการสร้างภาพนามธรรม โดยผู้ใช้สามารถเลือกแบบรูป และประเภทของแผนภูมิผ่านทาง คอมโบ-บอกซ์ (Combo Box) ซึ่งอยู่บริเวณด้านซ้ายของหน้าจอเครื่องมือต้นแบบ

3) *ส่วนที่ 3 คือ ส่วนแสดงคำอธิบาย* ซึ่งเป็นรายละเอียดของรูปแบบแผนภูมิที่ผู้ใช้งานเลือกจากส่วนที่ 2 โดยแสดงผลผ่านทางกล่องข้อความ (Text Box)

4) ส่วนที่ 4 คือ *ส่วนแสดงผล และการจัดการแผนภูมิ* อยู่บริเวณด้านขวาของหน้าจอเครื่องมือต้นแบบ โดยมีเมนูให้ผู้ใช้สามารถจัดการกับแผนภูมิได้อยู่บริเวณด้านล่างขวา ซึ่งมีรายการเมนูเครื่องมือต่างๆ ดังต่อไปนี้

(1) การย่อ/ขยายภาพนามธรรม

(2) การย้ายภาพนามธรรม

(3) การหมุนภาพนามธรรม

(4) การตั้งค่าการพิมพ์

(5) การดูภาพตัวอย่างก่อนพิมพ์

(6) การบันทึกภาพนามธรรม

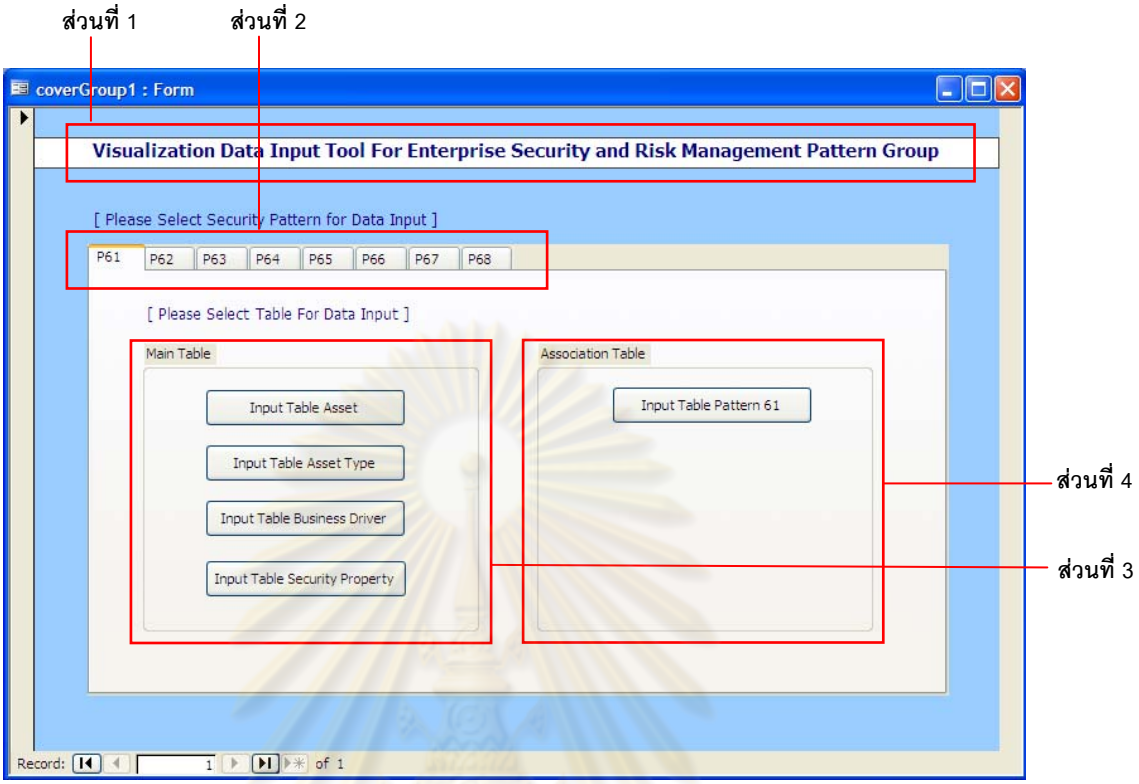
การออกแบบส่วนต่อประสานผู้ใช้ สำหรับส่วนในการนำเข้าข้อมูลสนับสนุนการสร้างภาพนามธรรม สามารถแสดงได้ดังรูป 4.11 โดยแบ่งออกเป็น 4 ส่วน ดังนี้

1) ส่วนที่ 1 เป็นส่วนแสดงชื่อของกลุ่มแบบรูปความมั่นคง ที่ต้องการจะนำเข้าข้อมูลสนับสนุนการสร้างภาพนามธรรม

2) ส่วนที่ 2 เป็นส่วนการเลือกแบบรูปความมั่นคง โดยใช้รหัสของแบบรูปความมั่นคง ซึ่งขึ้นต้นด้วยตัวอักษร P แล้วตามด้วยตัวเลขตัวแรกแสดงหมายเลขบทของแบบรูปความมั่นคงในหนังสือแบบรูปความมั่นคง การบูรณาการความมั่นคงและวิศวกรรมระบบ [4] และ ตัวเลขที่สองแสดงลำดับที่ของแบบรูปความมั่นคงในบทนั้น

3) ส่วนที่ 3 เป็นส่วนการเลือกตารางข้อมูลหลักสำหรับการนำข้อมูลเข้า

4) ส่วนที่ 4 เป็นส่วนการเลือกตารางข้อมูลความสัมพันธ์สำหรับการนำข้อมูลเข้า



รูปที่ 4.11 โครงสร้างส่วนต่อประสานข้อมูลนำเข้า

4.4 สภาพแวดล้อมในการพัฒนาเครื่องมือ

สภาพแวดล้อมในการพัฒนาเครื่องมือต้นแบบ จำแนกได้เป็น 2 ประเภท คือ ฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) โดยมีรายละเอียดดังนี้

4.4.1 สภาพแวดล้อมในการพัฒนาเครื่องมือด้านฮาร์ดแวร์

เครื่องคอมพิวเตอร์พกพา (Notebook) 1 เครื่อง

- หน่วยประมวลผล Intel Core Duo Processor T2300 ความเร็ว 1.66 GHz
- หน่วยความจำหลัก DDR2 ขนาด 512 เมกกะไบต์ (MB)
- ฮาร์ดดิสก์ความเร็ว 4,200 รอบ/วินาที ขนาด 80 กิกะไบต์ (GB)

4.4.2 สภาพแวดล้อมในการพัฒนาเครื่องมือด้านซอฟต์แวร์

1) ระบบปฏิบัติการวินโดส์เอ็กซ์พี (Microsoft Windows XP)

2) ไมโครซอฟท์วิสชวลซีชาร์บ 2008 (Microsoft Visual C# 2008) สำหรับพัฒนาเครื่องมือในส่วนที่เป็นส่วนต่อประสานผู้ใช้ (Interface)

3) ไมโครซอฟท์วิสชวลซีชาร์บ 2008 (Microsoft Visual C# 2008) เป็นภาษาสำหรับพัฒนาเครื่องมือต้นแบบส่วนที่เป็นโปรแกรมทั้งหมด

4) ไมโครซอฟท์ดอทเน็ตเฟรมเวิร์ก (Microsoft .NET Framework) รุ่น 3.5 ขึ้นไป เพื่อใช้สำหรับการทำงานของวิสชวลสตูดิโอ และ การทำงาน (Run) ของเครื่องมือต้นแบบ

5) ไมโครซอฟท์แอกเซส 2003 (Microsoft Access 2003) สำหรับโปรแกรมและจัดการข้อมูลในฐานข้อมูล

6) เนฟรอน ดอทเน็ตวิชชัน 2008 [20] (Nevron .Net Vision Q1 2008) สำหรับโปรแกรมการแสดงผล และการจัดการแผนภูมิ

บทที่ 5
การทดสอบเครื่องมือต้นแบบสำหรับการสร้างภาพนามธรรม จากแบบรูปความมั่นคง

การทดสอบการพัฒนาเครื่องมือต้นแบบการสร้างภาพนามธรรมความต้องการด้านความมั่นคงนี้ ผู้วิจัยมีเป้าหมายเพื่อต้องการทราบว่าในการพัฒนาเครื่องมือต้นแบบ และภาพนามธรรมความต้องการด้านความมั่นคงที่ได้สร้างขึ้นมานั้นมีฟังก์ชันการทำงานถูกต้อง ครบถ้วนที่ได้ระบุไว้ในการออกแบบเครื่องมือต้นแบบในบทที่ 4 หรือไม่ โดยใช้การทดสอบจากฟังก์ชันที่ระบุไว้ในแผนภาพยูสเคส ในรูปที่ 4.4 และการทดสอบความพึงพอใจ ตลอดจนประโยชน์ต่อผู้ใช้เป็นอย่างไร (การทดสอบเชิงคุณภาพการทำงาน) โดยการให้ผู้ร่วมทดลองได้ทดลองใช้เครื่องมือต้นแบบนี้ และทดสอบการทดลองใช้เครื่องมือต้นแบบจากสถานการณ์จำลอง (Scenario) ที่กำหนดให้ ซึ่งครอบคลุมแบบรูปทั้งหมดในขอบเขตงานวิจัยนี้ และผู้วิจัยได้วิเคราะห์ผลการทดสอบ เพื่อสรุปผลการทดสอบ เพื่อใช้เป็นแนวทางในการปรับปรุงการพัฒนาเครื่องมือต้นแบบการสร้างภาพนามธรรมความความมั่นคงต่อไป

5.1 การทดสอบเชิงฟังก์ชันการทำงานของเครื่องมือต้นแบบ

การทดสอบนี้มีวัตถุประสงค์เพื่อตรวจสอบเครื่องมือต้นแบบว่ามีฟังก์ชันการทำงานถูกต้องและครบถ้วนตามที่ได้ระบุไว้ในหัวข้อ 4.2 หรือไม่ โดยทดสอบกับสถานการณ์จำลองระบบการจัดการห้องสมุด ซึ่งหัวข้อที่ใช้ในการทดสอบมีดังนี้ การลงทะเบียนเข้าใช้ระบบ การกำหนดความต้องการด้านความมั่นคง การคำนวณค่าความเสี่ยง การสร้างรายการความต้องการด้านความมั่นคง การจัดการฐานข้อมูล การสร้างภาพนามธรรม และการแสดงผลและจัดการภาพนามธรรม สามารถแสดงตารางรายการการทดสอบได้ดังตารางที่ 5.1

ตารางที่ 5.1 การทดสอบเชิงฟังก์ชันการทำงานของเครื่องมือต้นแบบ

ลำดับที่	รายการการทดสอบ	ผลการทดสอบ	หมายเหตุ
การลงทะเบียนเข้าใช้ระบบ			
1	การตรวจสอบผู้ใช้งานและรหัสผ่าน	ผ่าน	มีข้อความเตือนผู้ใช้งานหากไม่ได้กรอกรหัส
2	การอนุญาติให้เข้าสู่ระบบ	ผ่าน	-

ตารางที่ 5.1 การทดสอบเชิงฟังก์ชันการทำงานของเครื่องมือต้นแบบ (ต่อ)

ลำดับที่	รายการการทดสอบ	ผลการทดสอบ	หมายเหตุ
การกำหนดความต้องการด้านความมั่นคง			
3	การกำหนดความต้องการด้านความมั่นคง	ผ่าน	-
4	การตรวจสอบเงื่อนไขก่อนการใช้	ผ่าน	มีข้อความแจ้งเตือนหากผู้ใช้งานไม่ได้ตรวจสอบเงื่อนไขก่อนการใช้
5	การตรวจสอบความถูกต้องของข้อมูล	ผ่าน	มีข้อความแจ้งเตือนหากผู้ใช้งานกรอกข้อมูลผิด
การจัดการฐานข้อมูล			
6	จัดเก็บข้อมูลความต้องการด้านความมั่นคง	ผ่าน	-
7	ค้นคืนข้อมูลความต้องการด้านความมั่นคง	ผ่าน	-
8	นำเข้าข้อมูลสนับสนุนการสร้างภาพนามธรรม	ผ่าน	เฉพาะผู้ดูแลระบบ
วิธีการสร้างภาพนามธรรม			
9	การสร้างภาพนามธรรมจากแบบรูปความมั่นคง	ผ่าน	มีข้อความแจ้งเตือนหากผู้ใช้งานไม่ได้เลือกประเภทแบบรูปความมั่นคง และรูปแบบของแผนภูมิ
10	การสร้างภาพนามธรรมจากรายการที่มีไว้ให้	ผ่าน	มีข้อความแจ้งเตือนหากผู้ใช้งานไม่ได้เลือกรายการที่มีไว้ให้
11	การสร้างภาพนามธรรมจากลักษณะประจำใดๆ	ผ่าน	มีข้อความแจ้งเตือนหากผู้ใช้งานไม่ได้เลือกประเภทการแสดงผลลักษณะประจำ
การแสดงผลและการจัดการภาพนามธรรม			
12	การย่อ/ขยายภาพนามธรรม	ผ่าน	-
13	การย้ายภาพนามธรรม	ผ่าน	-
14	การหมุนภาพนามธรรม	ผ่าน	-
15	การตั้งค่าการพิมพ์	ผ่าน	-
16	การดูตัวอย่างก่อนพิมพ์ภาพนามธรรม	ผ่าน	-
17	การบันทึกภาพนามธรรม	ผ่าน	-

จากผลการทดสอบเชิงฟังก์ชันการทำงานในตารางที่ 5.1 พิจารณาได้ข้อสรุปว่าเครื่องมือต้นแบบการสร้างภาพนามธรรมมีฟังก์ชันการทำงานที่ถูกต้อง และครบถ้วนตามที่ได้ระบุไว้ในหัวข้อการออกแบบหน้าที่การทำงานของเครื่องมือต้นแบบ (หัวข้อที่ 4.2)

5.2 การทดสอบเชิงคุณภาพการทำงานของเครื่องมือต้นแบบ

การทดสอบนี้มีวัตถุประสงค์เพื่อวัดระดับความพึงพอใจของหน่วยทดลองใช้เครื่องมือต้นแบบในการสร้างภาพนามธรรมความต้องการด้านความมั่นคงจากแบบรูปความมั่นคง ใน 3 กลุ่มปัจจัย ได้แก่ คุณภาพของภาพนามธรรมความต้องการด้านความมั่นคงที่ได้ คุณสมบัติของเครื่องมือต้นแบบ และการนำเครื่องมือต้นแบบไปประยุกต์ใช้ รูปแบบและวิธีการทดสอบของงานวิจัยนี้ จะใช้ผู้ร่วมทดลอง 12 คนที่มีผู้มีความรู้พื้นฐานด้านความมั่นคงเป็นหน่วยทดลอง มาทดลองใช้เครื่องมือในการสร้างภาพนามธรรมความต้องการด้านความมั่นคง แล้วให้หน่วยทดลองประเมินระดับความพึงพอใจในประเด็นต่างๆ ที่กล่าวมาข้างต้น รวมถึงให้หน่วยทดลองแสดงความคิดเห็นต่อภาพนามธรรมความต้องการด้านความมั่นคง และเพื่อใช้ในการปรับปรุงภาพนามธรรมความต้องการด้านความมั่นคงต่อไปในอนาคต

ผลลัพธ์ที่ได้จากการทดลองจะเป็นระดับความพึงพอใจในแต่ละประเด็น ที่ได้กำหนดไว้ข้างต้น และข้อคิดเห็นหรือข้อเสนอแนะที่มีต่อเครื่องมือ แล้วนำมาวิเคราะห์เพื่อหาข้อสรุปเพื่อปรับปรุงเครื่องมือ

5.2.1 วัตถุประสงค์ของการทดสอบ

เพื่อให้ผู้วิจัยสามารถทราบถึงประสิทธิภาพและประโยชน์ของภาพนามธรรมว่าเป็นไปตามเป้าหมายที่ตั้งไว้หรือไม่ ระดับความพึงพอใจของหน่วยทดลองนั้นเป็นอย่างไร อยู่ในระดับใดบ้าง พร้อมทั้งข้อคิดเห็นและข้อเสนอแนะจากหน่วยทดลอง เพื่อใช้ในการปรับปรุงเครื่องมือการสร้างภาพนามธรรมความต้องการด้านความมั่นคงที่ได้ต่อไป

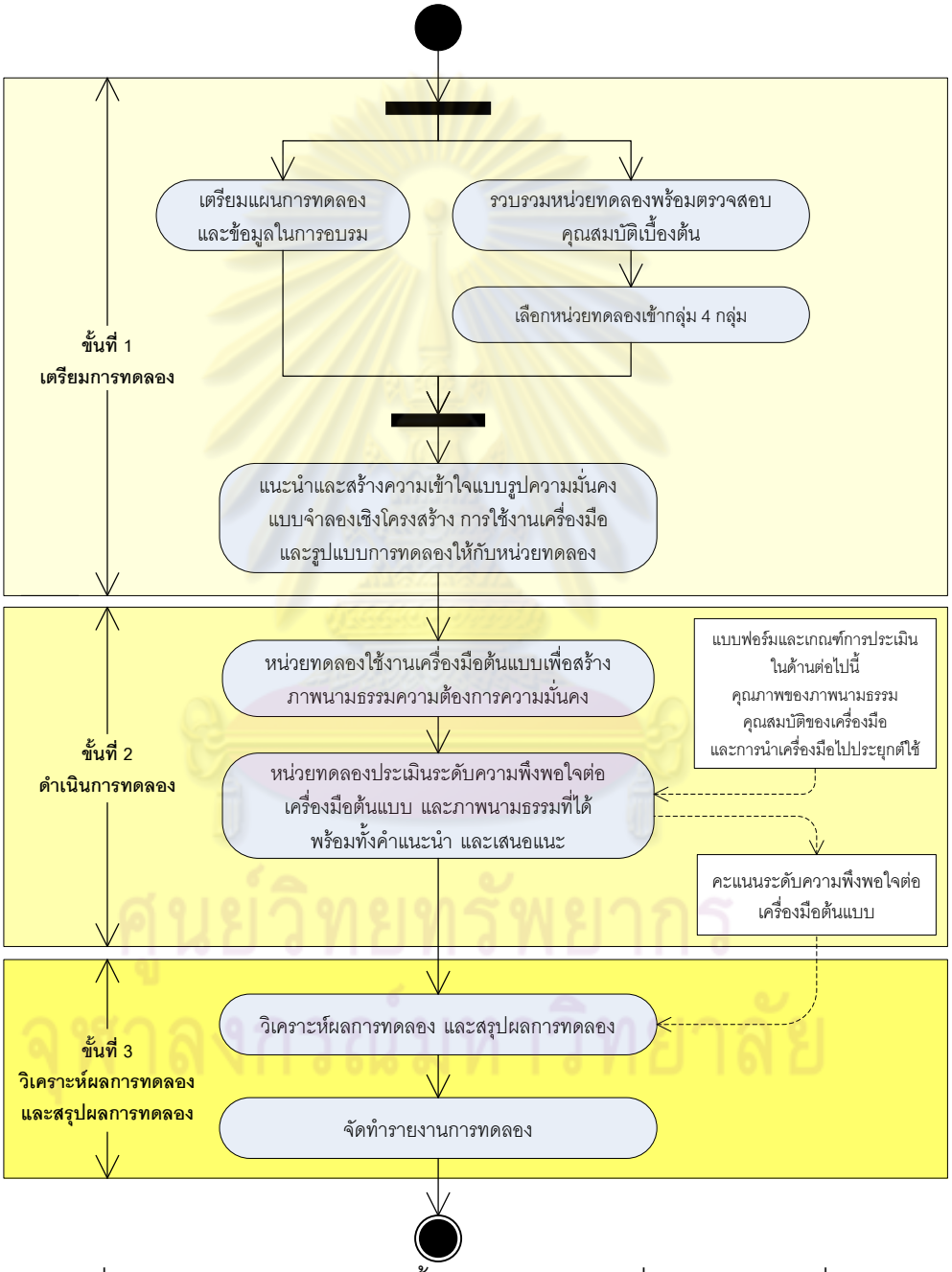
วัตถุประสงค์การทดสอบ แบ่งออกเป็น 2 ประเด็น ดังนี้

1) วิเคราะห์ระดับความพึงพอใจของผู้ใช้ในกลุ่มปัจจัยต่างๆ ได้แก่ คุณภาพของภาพนามธรรมความต้องการด้านความมั่นคงที่ได้ คุณสมบัติของเครื่องมือต้นแบบ และการนำเครื่องมือต้นแบบไปประยุกต์ใช้

2) รวบรวมและวิเคราะห์ความคิดเห็นและข้อเสนอแนะจากหน่วยทดลอง เพื่อนำมาสรุปและพิจารณาในการปรับปรุงการสร้างภาพนามธรรมจากเครื่องมือต้นแบบ

5.2.2 ขั้นตอนการทดสอบ

จากภาพรวมการทดลองที่กล่าวมาข้างต้นสามารถแสดงขั้นตอนการทดลองเป็น 3 ขั้นตอน ดังแสดงด้วยแผนภาพกิจกรรมได้ดังรูปที่ 5.1 ซึ่งประกอบด้วย ขั้นตอนการเตรียมการทดลอง ขั้นตอนการดำเนินการทดลอง และขั้นตอนวิเคราะห์และสรุปผลการทดลอง



รูปที่ 5.1 แผนภาพกิจกรรมแสดงขั้นตอนการทดลองเพื่อการทดสอบเครื่องมือการสร้างภาพนามธรรมความมั่นคง

5.2.3 **การวางแผนการทดลอง** (Experimental Planning)

5.2.3.1 **หน่วยทดลอง** (Experimental Unit)

หน่วยทดลองในการทดลองนี้ มีจำนวน 12 คน ซึ่งจะแบ่งออกเป็น 4 กลุ่ม กลุ่มละ 3 คน ดังรายละเอียดต่อไปนี้

กลุ่มที่ 1

สำหรับหน่วยทดลองในกลุ่มที่ 1 นี้ จะต้องเป็นนิสิตระดับบัณฑิตศึกษาขึ้นไป ที่มีความรู้พื้นฐานด้านความมั่นคงหรือ ผ่านการเรียนวิชาความมั่นคงสำหรับระบบคอมพิวเตอร์ (Computer System Security) และ/หรือ วิชาวิศวกรรมความต้องการซอฟต์แวร์ (Software Requirements Engineering) ของภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย หรือสาขาวิชาที่เกี่ยวข้อง และมีระดับผลการเรียนในรายวิชาดังกล่าวไม่ต่ำกว่า B หรือ เป็นบุคลากรที่มีความเชี่ยวชาญและมีประสบการณ์ในระบบด้านความมั่นคง ที่กำลังปฏิบัติงานและมีความเชี่ยวชาญในกรอบงานของความมั่นคงที่เหมาะสม

นอกจากนี้ในหน่วยทดลองกลุ่มที่ 1 นี้ ก่อนการทดลองผู้วิจัยจะให้ความรู้แก่หน่วยทดลองก่อนการทดลองจริง เพื่อเป็นการปรับพื้นฐานความรู้ด้านความมั่นคง แบบรูปความมั่นคง ไวยากรณ์ความมั่นคง แบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคง และเครื่องมือต้นแบบ

กลุ่มที่ 2

สำหรับหน่วยทดลองในกลุ่มที่ 2 นี้ จะต้องเป็นนิสิตระดับบัณฑิตศึกษาขึ้นไป ที่มีความรู้พื้นฐานด้านความมั่นคง หรือ ผ่านการเรียนวิชาความมั่นคงสำหรับระบบคอมพิวเตอร์ และ/หรือ วิชาวิศวกรรมความต้องการซอฟต์แวร์ ของภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย หรือสาขาวิชาที่เกี่ยวข้อง และมีระดับผลการเรียนในรายวิชาดังกล่าวไม่ต่ำกว่า B หรือ เป็นบุคลากรที่มีความเชี่ยวชาญและมีประสบการณ์ในระบบด้านความมั่นคง ที่กำลังปฏิบัติงานและมีความเชี่ยวชาญในกรอบงานของความมั่นคงที่เหมาะสม

แต่สำหรับหน่วยทดลองในกลุ่มที่ 2 นี้ ก่อนการทดลองจะไม่มีการให้ความรู้ทางด้านแบบรูปความมั่นคง ไวยากรณ์ความมั่นคง แบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคง และเครื่องมือต้นแบบใดๆ เลย

กลุ่มที่ 3

สำหรับหน่วยทดลองในกลุ่มที่ 3 นี้ จะต้องเป็นนิสิตระดับบัณฑิตศึกษาขึ้นไป และไม่เคยผ่านการเรียนวิชาความมั่นคงสำหรับระบบคอมพิวเตอร์ และ/หรือ วิชาวิศวกรรมความต้องการซอฟต์แวร์มาก่อน และไม่เป็นบุคลากรที่มีความเชี่ยวชาญและมีประสบการณ์ในระบบด้านความมั่นคงมาก่อน

แต่สำหรับหน่วยทดลองในกลุ่มที่ 3 นี้ ก่อนการทดลองผู้วิจัยจะให้ความรู้แก่หน่วยทดลองก่อนการทดลองจริง เพื่อเป็นการปรับพื้นฐานความรู้ด้านความมั่นคง แบบรูปความมั่นคง ไวยากรณ์ความมั่นคง แบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคง และเครื่องมือต้นแบบ

กลุ่มที่ 4

สำหรับหน่วยทดลองในกลุ่มที่ 4 นี้ จะต้องเป็นนิสิตระดับบัณฑิตศึกษาขึ้นไป และไม่เคยผ่านการเรียนวิชาความมั่นคงสำหรับระบบคอมพิวเตอร์ และ/หรือ วิชาวิศวกรรมความต้องการซอฟต์แวร์มาก่อน และไม่เป็นบุคลากรที่มีความเชี่ยวชาญและมีประสบการณ์ในระบบด้านความมั่นคงมาก่อน

อีกทั้งหน่วยทดลองในกลุ่มที่ 4 นี้ ก่อนการทดลองจะไม่มีการให้ความรู้ทางด้านแบบรูปความมั่นคง ไวยากรณ์ความมั่นคง แบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคง และเครื่องมือต้นแบบใดๆ เลย

ตารางที่ 5.2 สรุปคุณสมบัติเบื้องต้นของแต่ละหน่วยทดลอง

	เป็นผู้ที่มีความรู้พื้นฐานด้านความมั่นคง	**ให้ความรู้แบบรูปความมั่นคงก่อนการทดลอง**
กลุ่มที่ 1	✓	✓
กลุ่มที่ 2	✓	✗
กลุ่มที่ 3	✗	✓
กลุ่มที่ 4	✗	✗

5.2.3.2 **สิ่งทดลอง** (Treatment)

สิ่งทดลองในการทดลองนี้ คือ สถานการณ์จำลองซึ่งเป็นระบบที่ถูกกำหนดขึ้นโดยผู้วิจัย ซึ่งครอบคลุมเกี่ยวข้องกับความมั่นคง เพื่อให้หน่วยทดลองทำการใช้เครื่องมือการสร้างภาพนามธรรมความต้องการของระบบดังกล่าว ในการทดลองจะกำหนด 1 สถานการณ์ ซึ่งถูก

กำหนดให้ครอบคลุมแบบรูปความมั่นคงทั้ง 4 กลุ่มที่ได้นำเสนอไว้ในขอบเขตงานวิจัย ได้แก่ การจัดการสินทรัพย์องค์กรและความเสี่ยง การระบุตัวตนและการยืนยันตน การตรวจสอบการเข้าถึง และสถาปัตยกรรมไฟล์วอลล์ รายละเอียดของสถานการณ์จำลองในการทดลองมีดังนี้

สถานการณ์จำลองระบบห้องสมุด (Library Management)

เป็นระบบที่มุ่งเน้นการดูแลและควบคุมการใช้สินทรัพย์ต่างๆ ที่มีในห้องสมุด โดยประเภททรัพยากรที่ปรากฏ เป็นได้ทั้งทรัพยากรประเภทข้อมูล (Information Asset) ได้แก่ แฟ้มข้อมูลวิทยานิพนธ์ออนไลน์ แฟ้มข้อมูลนิสิต แฟ้มข้อมูลพนักงาน เป็นต้น และทรัพยากรประเภทกายภาพ (Physical Asset) เช่น หนังสือ ซีดีรอม วิทยานิพนธ์ วารสาร โต๊ะ เก้าอี้ เครื่องปรับอากาศ คอมพิวเตอร์ เป็นต้น ซึ่งมีความจำเป็นต้องกำหนดคุณสมบัติความมั่นคง และนโยบายของห้องสมุด (Library Policy) อย่างไรก็ตามผู้ที่สามารถเข้าออกห้องสมุดได้อาจเป็นได้ทั้งสมาชิกห้องสมุด และบุคคลภายนอก แต่การยืมหนังสือ เรื่องสื่อประเภทต่างๆ ได้นั้นควรเป็นสมาชิกของห้องสมุดเท่านั้น จึงมีความจำเป็นต้องมีการตรวจสอบและระบุตัวตนก่อนการยืมหนังสือ หรือสื่อประเภทต่างๆ และจะต้องมีการกำหนดสิทธิ์ให้เฉพาะบุคคล หรือบทบาทที่บุคคลดังกล่าวจะได้รับ เช่น นิสิต สามารถยืมหนังสือได้ 7 วัน ส่วนอาจารย์หรือพนักงาน สามารถยืมหนังสือได้ 14 วัน เป็นต้น สำหรับระบบเครือข่ายที่ได้ทำการติดตั้งไว้ในห้องสมุดจะต้องมีการควบคุมการใช้งานเช่นกัน เช่น การกรองแพ็คเกจการเชื่อมต่อระหว่างภายในห้องสมุดกับภายนอก เป็นต้น

5.2.3.3 การให้ความรู้แก่หน่วยทดลอง

ในการทดลองเพื่อการทดสอบเครื่องมือการสร้างภาพนามธรรมความมั่นคงนี้ได้กำหนดให้หน่วยทดลองในกลุ่ม 1 และกลุ่มที่ 3 ได้รับความรู้เบื้องต้นก่อนการทดลองจริง เพื่อเป็นการปรับพื้นฐานความรู้ด้านความมั่นคง แบบรูปความมั่นคง ไวยากรณ์ความมั่นคง แบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคง และเครื่องมือต้นแบบ โดยดำเนินการตามลำดับดังต่อไปนี้

1) แนะนำแบบรูปความมั่นคงในภาพรวม และอธิบายแบบรูปที่อยู่ในขอบเขตงานวิจัย และเป้าหมายของการทดลอง

2) แนะนำแบบรูปความมั่นคงแต่ละแบบรูป โดยอธิบายความหมาย วัตถุประสงค์ ขอบเขต ผลเฉลย พร้อมตัวอย่างประกอบ

3) แนะนำความสัมพันธ์ระหว่างแบบรูป เงื่อนไขก่อนการใช้แบบรูป

4) แนะนำแบบจำลองเชิงโครงสร้างที่ได้สร้างขึ้นในงานวิจัยนี้ เพื่อประโยชน์ในการช่วยให้เห็นความสัมพันธ์ของภาพนามธรรมความต้องการด้านความมั่นคงในมุมมองระหว่างแบบรูปต่างๆ

5) แนะนำเครื่องมือการใช้งาน และข้อจำกัดของเครื่องมือที่พัฒนาขึ้น

6) แนะนำรูปแบบ สถานการณ์จำลอง และความหมายของการประเมินผลการทดลองตามปัจจัยที่กำหนด

5.2.3.4 ปัจจัยที่ใช้ในการประเมินเครื่องมือ

ในการทดลองนี้ จะพิจารณาจากกลุ่มปัจจัยต่อไปนี้ ได้แก่ คุณภาพของภาพนามธรรมความต้องการด้านความมั่นคงที่ได้ คุณสมบัติของเครื่องมือต้นแบบ และการนำเครื่องมือต้นแบบไปประยุกต์ใช้ โดยจำแนกปัจจัยในแต่ละกลุ่มดังนี้

1) กลุ่มปัจจัยด้านคุณภาพของภาพนามธรรมความต้องการด้านความมั่นคง

(1) ความชัดเจน

(2) ความถูกต้อง

(3) การแปลความหมายของภาพ

2) กลุ่มปัจจัยด้านคุณสมบัติของเครื่องมือต้นแบบ

(1) ส่วนต่อประสานง่ายต่อการใช้งาน

(2) เมนูการแสดงภาพนามธรรมมีความครอบคลุมการใช้งาน

(3) มีเครื่องมือการจัดการแผนภูมิที่ครอบคลุมการใช้งาน

3) กลุ่มปัจจัยด้านการนำเครื่องมือต้นแบบไปประยุกต์ใช้

(1) ความเหมาะสมในการนำไปใช้งานในองค์กร

(2) ช่วยสร้างองค์ความรู้ความมั่นคงให้กับองค์กร

ในการประเมินจะวิเคราะห์จากระดับความคิดเห็นว่าเห็นด้วยกับปัจจัยต่างๆ (เอกสารการประเมินหน่วยทดลองเครื่องมือแสดงดัง ภาคผนวก ฌ) ในระดับใด โดยในที่นี้กำหนดให้มีระดับดังต่อไปนี้

5 หมายถึง หน่วยทดลองเห็นด้วยมากที่สุด

4 หมายถึง หน่วยทดลองเห็นด้วยมาก

3 หมายถึง หน่วยทดลองเห็นด้วยปานกลาง

2 หมายถึง หน่วยทดลองเห็นด้วยน้อย

1 หมายถึง หน่วยทดลองเห็นด้วยน้อยมาก

5.2.4 **การดำเนินการทดลอง**

รูปแบบการทดลองในงานวิจัยนี้ ให้หน่วยทดลองสร้างภาพนามธรรมความต้องการด้านความมั่นคง และประเมินระดับความพึงพอใจการใช้งานเครื่องมือต้นแบบและภาพนามธรรมที่ได้ โดยขั้นตอนการดำเนินการทดลองมีรายละเอียดดังต่อไปนี้

1) แบ่งหน่วยทดลองจำนวน 12 คน ออกเป็น 4 กลุ่ม กลุ่มละ 3 คน ตามรายละเอียดในหัวข้อ 5.2.3.1

2) ผู้วิจัยให้ความรู้เบื้องต้นก่อนการทดลองจริง ให้แก่กลุ่มที่ 1 และ 3 เพื่อเป็นการปรับพื้นฐานความรู้ด้านความมั่นคง แบบรูปความมั่นคง ไวยากรณ์ความมั่นคง แบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคง และเครื่องมือต้นแบบ

3) ผู้วิจัยแนะนำ และอธิบายสถานการณ์จำลองให้แก่ทุกกลุ่มทดลอง

4) ผู้ทดลองทั้ง 4 กลุ่ม ทดลองใช้เครื่องมือต้นแบบการสร้างภาพนามธรรมความต้องการด้านความมั่นคง

5) เมื่อผู้ทดลองทั้ง 4 กลุ่ม ทดลองใช้เครื่องมือต้นแบบการสร้างภาพนามธรรมเสร็จเรียบร้อยแล้ว ให้ผู้ทดลองทำแบบประเมินความพึงพอใจในการใช้งานเครื่องมือต้นแบบ และภาพนามธรรมที่ได้ พร้อมทั้งให้ข้อคิดเห็น และข้อเสนอแนะ

5.2.5 **ผลการทดลอง** (Experiment Results)

ผลการทดลองในการทดสอบเครื่องมือต้นแบบในงานวิจัยนี้จะเป็นการวัดระดับความเห็นของหน่วยทดลองมีต่อเครื่องมือต้นแบบ และภาพนามธรรมที่ได้ในปัจจัยด้านต่างๆ เช่น คุณภาพของภาพนามธรรมความต้องการด้านความมั่นคงที่ได้ คุณสมบัติของเครื่องมือต้นแบบ และการนำเครื่องมือต้นแบบไปประยุกต์ใช้ โดยผลสรุปความคิดเห็นของหน่วยทดลองจำนวน 12 คนโดยแสดงความถี่ของความคิดเห็นของผู้ใช้จำแนกตามระดับความคิดเห็นในปัจจัยที่พิจารณาต่างๆ แสดงดังตารางที่ 5.3

ตารางที่ 5.3 การแจกแจงความคิดเห็นของหน่วยทดลองจำแนกตามระดับความคิดเห็นจากหน่วยทดลอง 12 คน

ปัจจัยที่ใช้ในการพิจารณา	ระดับความคิดเห็น				
	5	4	3	2	1
1. ความคิดเห็นต่อคุณภาพผลลัพธ์ภาพนามธรรมความต้องการด้านความมั่นคง					
1.1 ภาพนามธรรมที่ได้มีความชัดเจนทำให้เข้าใจความต้องการความมั่นคงได้ชัดเจนมากขึ้น	2	6	4	0	0
1.2 ภาพนามธรรมที่ได้มีความถูกต้องตรงกับความต้องการด้านความมั่นคงที่ผู้ใช้งานกำหนด	6	6	0	0	0
1.3 ภาพนามธรรมที่ได้สามารถแปลความหมายได้ง่ายทำให้เข้าใจความต้องการด้านความมั่นคงได้ง่ายดายมากขึ้น	1	5	5	1	0
2. ความคิดเห็นต่อคุณสมบัติเครื่องมือต้นแบบ					
2.1 เครื่องมือต้นแบบมีการออกแบบส่วนต่อประสานที่ง่ายต่อการใช้งาน	7	5	0	0	0
2.2 เครื่องมือต้นแบบมีการออกแบบเมนูการแสดงภาพนามธรรมซึ่งมีความครอบคลุมการใช้งาน	9	3	0	0	0
2.3 เครื่องมือต้นแบบมีเครื่องมือจัดการแผนภูมิที่ครอบคลุมการใช้งาน	6	6	0	0	0
3. ความคิดเห็นต่อการนำเครื่องมือต้นแบบไปประยุกต์ใช้ในองค์กรด้านความมั่นคง					
3.1 องค์กรควรนำเครื่องมือไปประยุกต์ใช้เพื่อกำหนดความต้องการด้านความมั่นคงและนโยบายความมั่นคงสำหรับองค์กรได้	2	6	4	0	0
3.2 องค์กรสามารถนำความต้องการด้านความมั่นคงจากเครื่องมือมาจัดเก็บเป็นข้อมูลเพื่อสร้างเป็นองค์ความรู้สำหรับองค์กรได้	4	6	2	0	0

5.2.6 วิเคราะห์ผลการทดลอง

จากข้อคำถามเกี่ยวกับระดับความความคิดเห็นที่มีต่อการกำหนดความต้องการด้านความมั่นคงตั้งแต่ข้อที่ 1.1 จนถึงข้อ 3.2 โดยมีเกณฑ์การให้คะแนนระดับความเห็นที่กำหนดในข้อ 5.2.3.4 สามารถนำมาเขียนเป็นตารางคะแนนความคิดเห็นแบบรายปัจจัยได้ดังตารางที่ 5.4

ตารางที่ 5.4 คะแนนความคิดเห็นต่อเครื่องมือที่ใช้ในการกำหนดความมั่นคงเป็นรายปัจจัย

กลุ่มปัจจัย	ปัจจัย	หน่วยทดลองที่												S.D.	ค่าเฉลี่ยปัจจัย	ค่าเฉลี่ยกลุ่มปัจจัย
		1	2	3	4	5	6	7	8	9	10	11	12			
คุณภาพของภาพนามธรรมความต้องการด้านความมั่นคง	ความชัดเจน	3	4	3	4	4	4	3	4	3	4	5	5	0.71	3.83	3.94
	ความถูกต้อง	5	5	4	4	5	4	5	4	4	5	4	5	0.52	4.5	
	การแปลความหมาย	2	3	4	4	4	4	5	3	4	3	3	3	0.79	3.5	
คุณสมบัติของเครื่องมือต้นแบบ	ส่วนต่อประสานง่ายต่อการใช้	5	5	5	4	4	4	5	5	4	4	5	5	0.51	4.58	4.61
	เมนูภาพนามธรรมครอบคลุมการใช้	5	5	5	5	5	5	4	4	4	5	5	5	0.45	4.75	
	เครื่องมือจัดการแผนภูมิครอบคลุมการใช้งาน	4	4	5	5	4	5	4	5	4	4	5	5	0.52	4.5	
การนำเครื่องมือต้นแบบไปประยุกต์ใช้	มีความเหมาะสม	3	4	4	4	3	3	3	4	4	4	4	4	0.49	3.66	3.91
	สร้างองค์ความรู้ความมั่นคงแก่องค์กร	5	5	4	4	4	5	5	4	4	3	3	4	0.71	4.16	

จากตารางที่ 5.4 สามารถสรุปได้ดังนี้

1) ความเห็นของหน่วยทดลองที่มีต่อคุณภาพของภาพนามธรรมความต้องการด้านความมั่นคงพบว่า หน่วยทดลองส่วนใหญ่มีความเห็นในระดับดีต่อคุณภาพของภาพนามธรรมในมุมมองความชัดเจน ถูกต้อง และการแปลความหมาย ซึ่งมีระดับความพึงพอใจเฉลี่ยที่ 3.94

2) ความเห็นของหน่วยทดลองต่อคุณสมบัติของเครื่องมือต้นแบบพบว่าเครื่องมือต้นแบบมีส่วนต่อประสานที่ง่ายต่อการใช้งาน มีเมนูการสร้างภาพนามธรรม และเมนูเครื่องมือการจัดการแผนภูมิที่ครอบคลุมการใช้งาน ช่วยให้หน่วยทดลองสามารถจัดการกับภาพนามธรรมได้อย่างสะดวก และรวดเร็ว โดยดูจากระดับความพึงพอใจที่ 4.61

3) ความเห็นของหน่วยทดลองต่อการนำเครื่องมือไปประยุกต์ใช้พบว่าเครื่องมือช่วยให้หน่วยทดลองเกิดการเรียนรู้เกี่ยวกับแบบรูปความมั่นคงมากขึ้น และการนำเครื่องมือไปประยุกต์ใช้ในองค์กรมีความเหมาะสม โดยพิจารณาจากระดับความพึงพอใจที่ 3.91

5.2.7 **สรุปและอภิปรายผลการทดลอง**

จากผลการทดลองในการทดสอบเครื่องมือต้นแบบการสร้างภาพนามธรรมความต้องการด้านความมั่นคงสามารถสรุปเป็น 3 กลุ่มปัจจัยได้ดังนี้

1) คุณภาพของภาพนามธรรมความต้องการด้านความมั่นคงที่ได้มีความชัดเจน ถูกต้องและมีการแปลความหมายที่ตรงกัน

2) เครื่องมือต้นแบบช่วยให้ผู้ใช้งานสามารถจัดการกับภาพนามธรรมที่ได้อย่างสะดวกและรวดเร็ว ด้วยการออกแบบส่วนต่อประสานที่ไม่ซับซ้อน

3) เครื่องมือต้นแบบการสร้างภาพนามธรรมความต้องการด้านความมั่นคงที่พัฒนาบนพื้นฐานของแบบรูปความมั่นคงมีความเหมาะสมที่จะนำไปประยุกต์ใช้ในองค์กร เนื่องจากสามารถนำเครื่องมือต้นแบบนี้ดูข้อมูลสรุปต่างๆ เพื่อใช้พิจารณาในการกำหนดนโยบายความมั่นคงขององค์กร หรือสร้างเป็นองค์ความรู้ความมั่นคงสำหรับองค์กรได้

5.2.8 **ปัญหาและแนวทางแก้ไข**

ปัญหาบางประการที่ปรากฏในการทดลอง จะสอดคล้องกับข้อเสนอแนะของหน่วยทดลอง 12 คน สามารถจำแนกเป็นรายข้อได้ดังนี้

1) ปัญหาที่เกิดจากความสับสนในแนวคิดความมั่นคงและคำศัพท์ทางด้านความมั่นคง

หน่วยทดลองบางคนมีความสับสนระหว่างการกำหนดแนวคิดความมั่นคง (Security Approach) และการบริการความมั่นคง (Security Service) ภายหลังทำการทดลองผู้วิจัยได้สอบถามพบว่าหน่วยทดลองบางคนไม่เข้าใจความหมายของคำศัพท์ด้านความมั่นคง ทำให้เกิดความเข้าใจที่ผิดพลาดในการแปลความหมายของภาพนามธรรม

แนวทางการแก้ไข ผู้วิจัยสามารถให้ความรู้เพิ่มเติมแก่หน่วยทดลองให้มีความเข้าใจมากยิ่งขึ้น หรือแนะนำแหล่งข้อมูลความมั่นคงที่หน่วยทดลองสามารถศึกษาด้วยตนเอง ซึ่งจะช่วยหลีกเลี่ยงปัญหาความสับสนที่เกี่ยวข้องกับความมั่นคง

2) ปัญหาที่เกิดจากความไม่เข้าใจในแบบรูปความมั่นคง

หน่วยทดลองบางคนยังไม่มีความเข้าใจที่เพียงพอเกี่ยวกับแบบรูปความมั่นคง เช่น ยังไม่เข้าใจว่าแบบรูปความมั่นคงการประเมินภาวะเสี่ยงนั้น จะต้องทราบค่าภัยคุกคามก่อน ถึงจะสามารถทำการประเมินภาวะเสี่ยง (หรือภาวะไม่มั่นคง) ได้

แนวทางการแก้ไข ผู้วิจัยได้สร้างเอกสารสรุปการสร้างแบบจำลองเชิงโครงสร้างจากแบบรูปความมั่นคง ซึ่งภายในมีหัวข้อสรุปต่างๆ สามารถให้หน่วยทดลองศึกษาเพิ่มเติมได้ เพื่อลดความสับสนในการใช้งานแบบรูปความมั่นคง

บทที่ 6
บทสรุปงานวิจัยและแนวทางการวิจัยต่อ

ในบทนี้จะกล่าวสรุปผลการวิจัยที่ได้ดำเนินการ และเสนอแนวทางในการทำวิจัยที่สามารถต่อยอดจากงานวิจัยนี้ได้ โดยมีรายละเอียดดังนี้

6.1 บทสรุปงานวิจัย

งานวิจัยนี้ได้นำเสนอแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคง โดยใช้แผนภาพคลาส และสร้างภาพนามธรรมความสัมพันธ์ของความต้องการด้านความมั่นคงของกวิน สุภาพร และคณะ [8] ซึ่งสนับสนุนแบบรูปความมั่นคงของ M.Schumacher [4] โดยแบบรูปความมั่นคงที่นำมาใช้ในงานวิจัยนี้มีจำนวน 20 แบบรูป ซึ่งครอบคลุม 4 กลุ่มแบบรูปความมั่นคง ได้แก่ การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง การระบุตัวตนและการพิสูจน์ตัวจริง แบบจำลองการควบคุมการเข้าถึง และสถาปัตยกรรมไฟล์วอลล์ เนื่องจากแบบรูปดังกล่าวมีการนำไปประยุกต์ใช้ได้อย่างกว้างขวาง มีความจำเป็นต่อการกำหนดความต้องการด้านความมั่นคงพื้นฐานที่ทุกระบบหรือทุกองค์กรต้องพิจารณาเป็นลำดับต้นๆ

หลังจากได้ทำการสร้างแบบจำลองเชิงโครงสร้างแล้วนั้น ได้มีการพัฒนาเครื่องมือต้นแบบสำหรับการสร้างภาพนามธรรมความต้องการด้านความมั่นคงจากแบบรูปความมั่นคง โดยในการออกแบบวิธีการสร้างภาพนามธรรมนั้น ผู้วิจัยได้ใช้หลักในการพิจารณาจากความสัมพันธ์ และองค์ประกอบสำคัญของแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคงที่ได้สร้างไว้ก่อนหน้านี้ และเลือกประเภทของภาพนามธรรมที่จะนำเสนอให้เหมาะสม โดยนำเสนอโดยอยู่ในรูปแบบของแผนภูมิหลายๆ ประเภท ประกอบไปด้วย แผนภูมิแท่ง (Bar Chart) แผนภูมิแท่งแบบเรียงซ้อน (Stack Bar Chart) แผนภูมิรูปวงกลม (Pie Chart) แผนภูมิเส้น (Line Chart) แผนภูมิจุด (Point Chart) แผนภูมิแบบฟอง (Bubble Chart) และแผนภูมิเรดาร์ (Radar Chart) เป็นต้น โดยภาพนามธรรมความต้องการด้านความมั่นคงนั้นจะแสดงให้เห็นถึงความสัมพันธ์ระหว่างความต้องการด้านความมั่นคงที่ระบุมาได้อย่างชัดเจน และสามารถทำความเข้าใจได้ง่ายขึ้น ซึ่งจะส่งผลทำให้การวิเคราะห์ความต้องการของระบบความมั่นคงทำได้อย่างเหมาะสม ตรงกับความต้องการของผู้ใช้งาน และมีประสิทธิภาพมากยิ่งขึ้น

เมื่อเครื่องมือต้นแบบการสร้างภาพนามธรรมได้ถูกพัฒนาขึ้นแล้วนั้น ย่อมต้องมีการทดสอบเครื่องมือต้นแบบใน 3 ปัจจัยคือ คุณภาพผลลัพธ์ภาพนามธรรม คุณสมบัติเครื่องมือ

ต้นแบบ และการนำเครื่องมือต้นแบบไปประยุกต์ใช้ในองค์กร ผลจากการทดสอบสรุปได้ว่า คุณภาพผลลัพธ์ภาพนามธรรมมีความชัดเจน ถูกต้อง และแปลความหมายจากความต้องการด้านความมั่นคงได้ง่ายขึ้น คุณสมบัติของเครื่องมือต้นแบบมีการออกแบบส่วนต่อประสานที่ง่ายและครอบคลุมต่อการใช้งาน และสามารถนำเครื่องมือต้นแบบไปประยุกต์ใช้ในองค์กรได้

6.2 แนวทางการวิจัยต่อ

งานวิจัยนี้ได้แบบจำลองเชิงโครงสร้างและการสร้างภาพนามธรรมของแบบรูปความมั่นคงจาก 20 แบบรูป ซึ่งจัดเป็น 4 กลุ่ม จากทั้งหมด 8 กลุ่มแบบรูปความมั่นคงที่นำเสนอไว้โดย Schumacher และคณะ ซึ่งเป็นแบบรูปที่ได้จากการประชุมวิชาการโดยผู้เชี่ยวชาญด้านความมั่นคง และแบบรูปความมั่นคง ดังนั้นการขยายขอบเขต งานให้ครอบคลุมทั้ง 8 กลุ่มแบบรูปความมั่นคง ถือเป็นสิ่งที่มีความท้าทาย และช่วยให้แบบจำลองเชิงโครงสร้างและการสร้างภาพนามธรรมของแบบรูปความมั่นคงมีความสมบูรณ์แบบมากขึ้น ซึ่งมีประโยชน์อย่างมากต่อกระบวนการวิศวกรรมความต้องการ

รายการอ้างอิง

[1] Blakley, B., and others. Security design patterns. United Kingdom: The Open Group U.K., 2004.

[2] Drrell, M. K., and Matthew, C. E. Security patterns for web application development. DARPA Contract # F30602-01-C-0164, 2002.

[3] Yoder, J., and Bacalow, J. Architectureal patterns for enabling applications security: Proceedings of PLoP. 1997.

[4] Schumacher, M., Fernandez, E. B., Hybertson, D., Buschmann, F., and Sommerlad, P. Security patterns integrating security and systems engineering. England: John Wiley & Sons, 2006.

[5] Jurjens, J. Secure systems development with UML. Springer-Verlag Berlin Heidelberg, 2005.

[6] Schumacher, M. Security Engineering with Patterns. Spinger-Verlag Berlin HeidelBerg, 2002.

[7] Lamsweerde, A. V. Elaborating security requirements by construction of intentional anti-models: Proceedings of the 26th international conference on software engineering. Edinburgh, 2004.

[8] กวิน สุภาพร. การกำหนดความต้องการความมั่นคงโดยใช้ไวยากรณ์ของแบบรูปความมั่นคง. วิทยานิพนธ์ ปริญญามหาบัณฑิต, ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2550.

[9] Supaporn, K., Prompoon, N., and Rojkangsadan, T. Enterprise assets security requirements construction from ESRMG grammar based on security patterns: Proceeding of the 14th asia-pacific software engineering conference. Nagoya, 2007.

[10] Johnson, C. R., and Hansen, C. D. Visualization handbook. New York: Elsevier Butterworth-Heinemann, 2004.

[11] Jarke, J., and Wijk, V. Views on visualization: Proceeding of IEEE transactions on visualization and computer graphics. 2006.

[12] Gamma, E., Helm, Richard., Johnson, R., and Vlissides, J. M. Design patterns elements of reusable object-oriented software. Addison-Wesley Professional, 1995.

[13] Larman, C. Applying UML and patterns: An introduction to object-oriented analysis and design and iterative development. Massachusetts: Pearson Education, 2004.

[14] Rumbaugh, J., Jacobson, I., and Booch, G. The unified modeling language reference manual second edition. Addison Wesley Professional, 2005.

[15] Naur, P. Revised report on the algorithmic language ALgoL 60: Proceeding of Communications of the ACM. 1963.

[16] Lengler, R., and Eppler, M. J. Towards a periodic table of visualization methods for management: Proceedings of graphics and visualization in engineering. Florida, 2007.

[17] ISO/IEC14977. Information technology-syntactic metalanguage-extended BNF, 1996.

[18] World health chart 2001 [Online]. Available from: http://www.whc.ki.se [2008, March 19]

[19] Fernandez, E. B. Metadata and authorization patterns. Florida: Florida Atlantic University, Report TR-CSE-00-16, 2000.

[20] Nevron .Net Vision Q1 2008 [Online]. Available from: http://www.nevron.com [2008, August 2]

ภาคผนวก

ภาคผนวก ก

ตารางรายการตัวเลือกการสร้างภาพนามธรรมจากลักษณะประจำใด ๆ โดยแสดงผลในรูปแผนภูมิจุดแบบสามมิติ

ตาราง ก.1 รายการข้อมูลลักษณะประจำ โดยแสดงผลในรูปแผนภูมิแบบจุดสามมิติ

ที่	ข้อมูล ลักษณะประจำที่ 1	ข้อมูล ลักษณะประจำที่ 2	ข้อมูล ลักษณะประจำที่ 3	รหัสแบบรูป ความมั่นคง ของลักษณะ ประจำที่ 1	รหัสแบบรูป ความมั่นคง ของลักษณะ ประจำที่ 2	รหัสแบบรูป ความมั่นคง ของลักษณะ ประจำที่ 3
1	assetName	propertyName	driverName	1	1	1
2	assetName	driverName	propertyName	1	1	1
3	assetName	threatAction	threatLikelihoodName	1	3	3
4	assetName	threatAction	vulnerabilityName	1	3	4
5	assetName	threatLikelihoodName	threatAction	1	3	3
6	assetName	vulnerabilityName	threatAction	1	4	3
7	assetName	vulnerabilityName	severityScaleName	1	4	4
8	assetName	severityScaleName	vulnerabilityName	1	4	4
9	assetName	approachName	businessPriorityName	1	6	6
10	assetName	approachName	serviceName	1	6	7
11	assetName	businessPriorityName	approachName	1	6	6
12	assetName	serviceName	approachName	1	7	6
13	assetName	partnerName	partnerType	1	8	8
14	assetName	partnerName	communicationChannelName	1	8	8
15	assetName	partnerType	partnerName	1	8	8
16	assetName	communicationChannelName	partnerName	1	8	8
17	assetName	communicationChannelName	exchangeMethodName	1	8	8
18	assetName	exchangeMethodName	communicationChannelName	1	8	8
19	assetName	userName	rightName	1	13	13
20	assetName	userName	roleName	1	13	14
21	assetName	rightName	userName	1	13	13
22	assetName	rightName	roleName	1	13	14
23	assetName	roleName	userName	1	14	13

ตาราง ก.1 รายการข้อมูลลักษณะประจำ โดยแสดงผลในรูปแผนภูมิแบบจุดสามมิติ (ต่อ)

ที่	ข้อมูล ลักษณะประจำที่ 1	ข้อมูล ลักษณะประจำที่ 2	ข้อมูล ลักษณะประจำที่ 3	รหัสแบบรูปความมั่นคงของลักษณะประจำที่ 1	รหัสแบบรูปความมั่นคงของลักษณะประจำที่ 2	รหัสแบบรูปความมั่นคงของลักษณะประจำที่ 3
24	assetName	roleName	rightName	1	14	13
25	assetName	categoryAssetName	classificationLevelName	1	15	15
26	assetName	classificationLevelName	categoryAssetName	1	15	15
27	propertyName	assetName	driverName	1	1	1
28	propertyName	driverName	assetName	1	1	1
29	driverName	assetName	propertyName	1	1	1
30	driverName	propertyName	assetName	1	1	1
31	threatAction	assetName	threatLikelihoodName	3	1	3
32	threatAction	assetName	vulnerabilityName	3	1	4
33	threatAction	threatConsequence	threatLikelihoodName	3	3	3
34	threatAction	threatSourceName	threatLikelihoodName	3	3	3
35	threatAction	threatLikelihoodName	assetName	3	3	1
36	threatAction	threatLikelihoodName	threatConsequence	3	3	3
37	threatAction	threatLikelihoodName	threatSourceName	3	3	3
38	threatAction	vulnerabilityName	assetName	3	4	1
39	threatAction	vulnerabilityName	severityScaleName	3	4	4
40	threatAction	severityScaleName	vulnerabilityName	3	4	4
41	threatConsequence	threatAction	threatLikelihoodName	3	3	3
42	threatConsequence	threatLikelihoodName	threatAction	3	3	3
43	threatSourceName	threatAction	threatLikelihoodName	3	3	3
44	threatSourceName	threatLikelihoodName	threatAction	3	3	3
45	threatLikelihoodName	assetName	threatAction	3	1	3

ตาราง ก.1 รายการข้อมูลลักษณะประจำ โดยแสดงผลในรูปแผนภูมิแบบจุดสามมิติ (ต่อ)

ที่	ข้อมูล ลักษณะประจำที่ 1	ข้อมูล ลักษณะประจำที่ 2	ข้อมูล ลักษณะประจำที่ 3	รหัสแบบรูปความมั่นคงของลักษณะประจำที่ 1	รหัสแบบรูปความมั่นคงของลักษณะประจำที่ 2	รหัสแบบรูปความมั่นคงของลักษณะประจำที่ 3
46	threatLikelihoodName	threatAction	assetName	3	3	1
47	threatLikelihoodName	threatAction	threatConsequence	3	3	3
48	threatLikelihoodName	threatAction	threatSourceName	3	3	3
49	threatLikelihoodName	threatConsequence	threatAction	3	3	3
50	threatLikelihoodName	threatSourceName	threatAction	3	3	3
51	vulnerabilityName	assetName	threatAction	4	1	3
52	vulnerabilityName	assetName	severityScaleName	4	1	4
53	vulnerabilityName	threatAction	assetName	4	3	1
54	vulnerabilityName	threatAction	severityScaleName	4	3	4
55	vulnerabilityName	severityScaleName	assetName	4	4	1
56	vulnerabilityName	severityScaleName	threatAction	4	4	3
57	severityScaleName	assetName	vulnerabilityName	4	1	4
58	severityScaleName	threatAction	vulnerabilityName	4	3	4
59	severityScaleName	vulnerabilityName	assetName	4	4	1
60	severityScaleName	vulnerabilityName	threatAction	4	4	3
61	approachName	assetName	businessPriorityName	6	1	6
62	approachName	assetName	serviceName	6	1	7
63	approachName	businessPriorityName	assetName	6	6	1
64	approachName	serviceName	assetName	6	7	1
65	businessPriorityName	assetName	approachName	6	1	6
66	businessPriorityName	approachName	assetName	6	6	1
67	serviceName	assetName	approachName	7	1	6
68	serviceName	approachName	assetName	7	6	1

ตาราง ก.1 รายการข้อมูลลักษณะประจำ โดยแสดงผลในรูปแผนภูมิแบบจุดสามมิติ (ต่อ)

ที่	ข้อมูล ลักษณะประจำที่ 1	ข้อมูล ลักษณะประจำที่ 2	ข้อมูล ลักษณะประจำที่ 3	รหัสแบบรูปความมั่นคงของลักษณะประจำที่ 1	รหัสแบบรูปความมั่นคงของลักษณะประจำที่ 2	รหัสแบบรูปความมั่นคงของลักษณะประจำที่ 3
69	partnerName	assetName	partnerType	8	1	8
70	partnerName	assetName	communicationChannelName	8	1	8
71	partnerName	partnerType	assetName	8	8	1
72	partnerName	communicationChannelName	assetName	8	8	1
73	partnerName	communicationChannelName	serviceTerminationName	8	8	8
74	partnerName	serviceTerminationName	communicationChannelName	8	8	8
75	partnerType	assetName	partnerName	8	1	8
76	partnerType	partnerName	assetName	8	8	1
77	communicationChannelName	assetName	partnerName	8	1	8
78	communicationChannelName	assetName	exchangeMethodName	8	1	8
79	communicationChannelName	partnerName	assetName	8	8	1
80	communicationChannelName	partnerName	serviceTerminationName	8	8	8
81	communicationChannelName	exchangeMethodName	assetName	8	8	1
82	communicationChannelName	serviceTerminationName	partnerName	8	8	8
83	exchangeMethodName	assetName	communicationChannelName	8	1	8
84	exchangeMethodName	communicationChannelName	assetName	8	8	1
85	serviceTerminationName	partnerName	communicationChannelName	8	8	8
86	serviceTerminationName	communicationChannelName	partnerName	8	8	8
87	I&ARequirementName	techniqueName	profileRatingName	9	10	10
88	I&ARequirementName	profileRatingName	techniqueName	9	10	10

ตาราง ก.1 รายการข้อมูลลักษณะประจำ โดยแสดงผลในรูปแผนภูมิแบบจุดสามมิติ (ต่อ)

ที่	ข้อมูล ลักษณะประจำที่ 1	ข้อมูล ลักษณะประจำที่ 2	ข้อมูล ลักษณะประจำที่ 3	รหัสแบบรูปความมั่นคงของลักษณะประจำที่ 1	รหัสแบบรูปความมั่นคงของลักษณะประจำที่ 2	รหัสแบบรูปความมั่นคงของลักษณะประจำที่ 3
89	techniqueName	I&ARequirementName	profileRatingName	10	9	10
90	techniqueName	profileRatingName	I&ARequirementName	10	10	9
91	techniqueFactorName	biometricMechanismName	biometricCharacteristicRatingName	12	12	12
92	techniqueFactorName	biometricCharacteristicRatingName	biometricMechanismName	12	12	12
93	biometricMechanismName	techniqueFactorName	biometricCharacteristicRatingName	12	12	12
94	biometricMechanismName	biometricCharacteristicRatingName	techniqueFactorName	12	12	12
95	userName	assetName	rightName	13	1	13
96	userName	assetName	roleName	13	1	14
97	userName	rightName	assetName	13	13	1
98	userName	roleName	assetName	13	14	1
99	rightName	assetName	userName	13	1	13
100	rightName	assetName	roleName	13	1	14
101	rightName	userName	assetName	13	13	1
102	rightName	roleName	assetName	13	14	1
103	roleName	assetName	userName	14	1	13
104	roleName	assetName	rightName	14	1	13
105	roleName	userName	assetName	14	13	1
106	roleName	rightName	assetName	14	13	1
107	categoryAssetName	assetName	classificationLevelName	15	1	15
108	categoryAssetName	classificationLevelName	assetName	15	15	1
109	classificationLevelName	assetName	categoryAssetName	15	1	15
110	classificationLevelName	categoryAssetName	assetName	15	15	1

ตาราง ก.1 รายการข้อมูลลักษณะประจำ โดยแสดงผลในรูปแผนภูมิแบบจุดสามมิติ (ต่อ)

ที่	ข้อมูล ลักษณะประจำที่ 1	ข้อมูล ลักษณะประจำที่ 2	ข้อมูล ลักษณะประจำที่ 3	รหัสแบบรูปความมั่นคงของลักษณะประจำที่ 1	รหัสแบบรูปความมั่นคงของลักษณะประจำที่ 2	รหัสแบบรูปความมั่นคงของลักษณะประจำที่ 3
111	profileRatingName	I&ARequirementName	techniqueName	10	9	10
112	profileRatingName	techniqueName	I&ARequirementName	10	10	9
113	biometricCharacteristicRatingName	techniqueFactorName	biometricMechanismName	12	12	12
114	biometricCharacteristicRatingName	biometricMechanismName	techniqueFactorName	12	12	12
115	externalIP	internalIP	appSerViceName	18	18	19
116	externalIP	internalIP	sessionName	18	18	20
117	externalIP	appSerViceName	internalIP	18	19	18
118	externalIP	sessionName	internalIP	18	20	18
119	externalHostName	internalHostName	appSerViceName	18	18	19
120	externalHostName	internalHostName	sessionName	18	18	20
121	externalHostName	appSerViceName	internalHostName	18	19	18
122	externalHostName	sessionName	internalHostName	18	20	18
123	internalIP	externalIP	appSerViceName	18	18	19
124	internalIP	externalIP	sessionName	18	18	20
125	internalIP	appSerViceName	externalIP	18	19	18
126	internalIP	sessionName	externalIP	18	20	18
127	internalHostName	externalHostName	appSerViceName	18	18	19
128	internalHostName	externalHostName	sessionName	18	18	20
129	internalHostName	appSerViceName	externalHostName	18	19	18
130	internalHostName	sessionName	externalHostName	18	20	18
131	appSerViceName	externalIP	internalIP	19	18	18
132	appSerViceName	externalHostName	internalHostName	19	18	18
133	appSerViceName	internalIP	externalIP	19	18	18
134	appSerViceName	internalHostName	externalHostName	19	18	18
135	sessionName	externalIP	internalIP	20	18	18
136	sessionName	externalHostName	internalHostName	20	18	18
137	sessionName	internalIP	externalIP	20	18	18
138	sessionName	internalHostName	externalHostName	20	18	18

ภาคผนวก ข

แบบสอบถาม

แบบฟอร์มการประเมินการทดสอบเครื่องมือสำหรับกำหนดความต้องการความมั่นคงจากไวยากรณ์ความมั่นคงที่สร้างจากแบบรูปความมั่นคง

ให้ท่านทำเครื่องหมาย ✓ลงในช่องว่างทางขวามือ ตรงกับความคิดเห็นของท่าน ในการใช้เครื่องมือที่สร้างบนพื้นฐานของไวยากรณ์ความมั่นคงเพื่อกำหนดความต้องการด้านความมั่นคง ซึ่งมี 5 ระดับ

5 หมายถึง เห็นด้วยมากที่สุด

4 หมายถึง เห็นด้วยมาก

3 หมายถึง เห็นด้วยปานกลาง

2 หมายถึง เห็นด้วยน้อย

1 หมายถึง เห็นด้วยน้อยที่สุด

ปัจจัยที่ใช้ในการพิจารณา	ระดับความคิดเห็น				
	5	4	3	2	1
1. ความคิดเห็นต่อคุณภาพผลลัพธ์ภาพนามธรรมความต้องการความมั่นคง 1.1 ภาพนามธรรมที่ได้มีความชัดเจนทำให้เข้าใจความต้องการความมั่นคงได้ชัดเจนมากขึ้น 1.2 ภาพนามธรรมที่ได้มีความถูกต้องตรงกับความต้องการความมั่นคงที่ผู้ใช้งานกำหนด 1.3 ภาพนามธรรมที่ได้สามารถแปลความหมายได้ง่ายทำให้เข้าใจความต้องการความมั่นคงได้ง่ายดายมากขึ้น					

ปัจจัยที่ใช้ในการพิจารณา	ระดับความคิดเห็น				
	5	4	3	2	1
2. ความคิดเห็นต่อคุณสมบัติเครื่องมือต้นแบบ 2.1 เครื่องมือต้นแบบมีการออกแบบส่วนต่อประสานที่ง่ายต่อการใช้งาน 2.2 เครื่องมือต้นแบบมีการออกแบบเมนูการแสดงภาพนามธรรมซึ่งมีความครอบคลุมการใช้งาน 2.3 เครื่องมือต้นแบบมีเครื่องมือจัดการแผนภูมิที่ครอบคลุมการใช้งาน					
3. ความคิดเห็นต่อการนำเครื่องมือต้นแบบไปประยุกต์ใช้ในองค์กรด้านความมั่นคง 3.1 องค์กรควรนำเครื่องมือไปประยุกต์ใช้เพื่อกำหนดความต้องการความมั่นคงและนโยบายความมั่นคงสำหรับองค์กรได้ 3.2 องค์กรสามารถนำความต้องการความมั่นคงจากเครื่องมือมาจัดเก็บเป็นข้อมูลเพื่อสร้างเป็นองค์ความรู้สำหรับองค์กรได้					

ความคิดเห็นและข้อเสนอแนะ

……..

……..

……..

……..

……..

ภาคผนวก ค

ผลงานตีพิมพ์

ระหว่างดำเนินงานวิจัย ผู้วิจัยได้เขียนบทความเพื่อตีพิมพ์ผลงานในวารสารวิชาการและการประชุมวิชาการระดับชาติ ดังนี้

W.Supanich, N. Prompoon and T. Rojkangsadan, Applying and Visualizing Risk Determination Pattern. Proceeding of the 12th National Computer Science and Engineering Conference (NCSEC2008), King Mongkut's University of Technology North Bangkok, Thailand, November 20-21, 2008.

การประยุกต์และการสร้างภาพนามธรรมจากแบบรูปการกำหนดค่าความเสี่ยง

Applying and Visualizing Risk Determination Pattern

วีริยา สุภาณิชย์ ธงชัย โรจน์กังสดาล นครทิพย์ พร้อมพูล
ห้องปฏิบัติการวิศวกรรมซอฟต์แวร์ ศูนย์เชี่ยวชาญเฉพาะทางด้านวิศวกรรมซอฟต์แวร์
ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
เขตปทุมวัน กรุงเทพมหานคร 10330
Email : weeriya.s@student.chula.ac.th thongchai.r@chula.ac.th nakornthip.s@chula.ac.th

บทคัดย่อ

การพัฒนาระบบความมั่นคงที่มีประสิทธิภาพเป็นสิ่งที่หลายองค์กรให้ความสำคัญ ทั้งนี้เพื่อใช้ปกป้อง รักษาสินทรัพย์ขององค์กร ซึ่งรวมถึงข้อมูลเชิงวิกฤต ให้ปลอดภัยจากผู้บุกรุก ดังนั้นข้อมูลที่เกี่ยวข้องกับมูลค่าและความเสี่ยงของสินทรัพย์ต่างๆ ขององค์กรจึงเป็นสิ่งที่สำคัญ และมักใช้ในการประมาณการเพื่อการประเมินความเสี่ยงของสินทรัพย์ แบบรูปความมั่นคงถูกนำเสนอขึ้นเพื่อใช้เป็นแนวทางในการแก้ไขปัญหาต่างๆ ในขั้นตอนของการออกแบบระบบความมั่นคง ในงานวิจัยนี้นำเสนอการนำแบบรูปความมั่นคงมาประยุกต์ใช้งานในสถานการณ์จริง การประเมินค่าความเสี่ยงของสินทรัพย์ต่างๆ ภายในองค์กร โดยนำเสนอการวิเคราะห์และออกแบบระบบใน 4 มุมมอง ประกอบด้วยมุมมองเชิงฟังก์ชันการทำงาน (อธิบายบริการของระบบ), มุมมองเชิงโครงสร้าง (อธิบายการจัดเก็บข้อมูลที่จำเป็นและความสัมพันธ์ระหว่างข้อมูล), มุมมองเชิงพฤติกรรม (อธิบายการโต้ตอบกันระหว่างส่วนประกอบของระบบ) และมุมมองเชิงสถาปัตยกรรม (อธิบายสถาปัตยกรรมเชิงตรรกะของระบบ) อีกทั้งยังนำเสนอการสร้างภาพนามธรรม เพื่อแสดงรายงานความเสี่ยงต่างๆ ที่เกิดขึ้น เพื่อให้ผู้บริหาร ผู้พัฒนาระบบ หรือผู้ใช้งานตระหนักถึงความสำคัญของสินทรัพย์นั้นๆ ต่อองค์กร เพื่อที่จะมีการวางแผน การจัดการทางด้านความมั่นคง ตลอดจนการออกนโยบายระเบียบข้อปฏิบัติต่างๆ เกี่ยวกับสินทรัพย์ได้อย่างเหมาะสม และมีประสิทธิภาพ

คำสำคัญ : แบบรูปความมั่นคง แบบรูปการกำหนดค่าความเสี่ยง การสร้างภาพนามธรรม

Abstract

Developing an efficiency security system is usually an important concern of many organizations since it helps organization protect and control organizational assets including critical data from intruder. Data related to the asset value and asset risk is important because it is basically used to estimate asset risk evaluation. Security patterns may be used as a solution or guidelines for solving particular recurring security problems. In this paper, we present a methodology for applying and visualizing risk determination pattern for an enterprise. Our methodology are proposed in 4 views, functional modeling view (describing system services), structural modeling view (describing necessary data stored and their relationships), behavioral modeling view (describing interactive between components of the designed system), and architectural view (describing the logical system architecture). We also represent the visualization method for reporting risk determination of asset. It may help developer through manager visualize the risk of asset explicitly to realize the importance of each asset in order to plan and manage security policy and rule efficiently.

Keywords: Security Patterns Risk Determination Pattern Data Visualization

1. บทนำ

กลยุทธ์ทางด้านความมั่นคงขององค์กรต่างๆ ในปัจจุบันเป็นสิ่งที่แต่ละองค์กรควรพิจารณา กำหนด และให้ความสำคัญในลำดับต้น เพราะองค์กรจำเป็นต้องมีการติดต่อสื่อสารกับบุคคลต่างๆ ทั้งภายในเครือข่ายขององค์กร เครือข่ายภายนอกองค์กร และเครือข่ายอินเทอร์เน็ต ดังนั้นองค์กรควรมีระบบที่มีความมั่นคง ปลอดภัยเพียงพอในการดูแลรักษาข้อมูลสำคัญขององค์กรต่างๆ ไม่ให้ถูกทำลาย หรือดัดแปลงจากผู้บุกรุกที่ไม่ประสงค์ดี องค์กรควรมีการกำหนดนโยบายทางด้านความมั่นคง ซึ่งรวมถึงสิทธิในการเข้าถึงข้อมูล ทรัพยากรต่างๆ ภายในองค์กร มีการประเมินมูลค่าสินทรัพย์ที่สำคัญ การประเมินค่าความเสี่ยง การระบุถึงภัยคุกคามที่อาจจะเกิดขึ้นต่อสินทรัพย์นั้นๆ ขององค์กร ตลอดจนแผนปฏิบัติต่อเหตุการณ์เมื่อภัยคุกคามนั้นๆ เกิดขึ้น

แบบรูปความมั่นคง (Security pattern) [1,6,7,12,15] นำเสนอแนวทาง หรือผลเฉลยของปัญหาทางด้านความมั่นคงต่างๆ ที่ได้ถูกแก้ปัญหาไว้ก่อนหน้านี้แล้ว และสนับสนุนการนำกลับมาใช้ใหม่ แต่อย่างไรก็ตามในการศึกษาและวิเคราะห์แบบรูปความมั่นคงเพื่อนำมาประยุกต์ใช้ในการพัฒนาระบบความมั่นคงขององค์กรนั้นทำได้ยาก เนื่องจากผู้พัฒนาระบบจะต้องศึกษา และทำความเข้าใจโครงสร้าง คุณสมบัติและเงื่อนไขบังคับของแบบรูปความมั่นคงก่อน จึงจะสามารถนำแบบรูปความมั่นคงเหล่านั้นมาประยุกต์ใช้ในการพัฒนาระบบความมั่นคงได้ ไม่เช่นนั้นอาจเกิดผลเสียที่ตามมาต่อระบบ เช่น อาจทำให้ระบบมีจุดอ่อน ผู้บุกรุกหรือผู้ที่ไม่ประสงค์ดีสามารถเข้ามาโจมตีต่อระบบได้ง่าย

ในขั้นตอนของการพัฒนาระบบความความมั่นคงนั้น ต้องเริ่มจากการออกแบบระบบความมั่นคง โดยทั่วไปนิยมใช้ยูเอ็มแอล (UML: Unified Modeling Language) [3,9] ซึ่งเปรียบเสมือนสัญลักษณ์มาตรฐานเข้ามาช่วยในการอธิบาย แสดงรายละเอียด จำลองโครงสร้างการทำงานจริงของระบบ เช่น แผนภาพยูสเคสใช้อธิบายแบบจำลองเชิงพฤติกรรมของระบบ, แผนภาพคลาสใช้อธิบายแบบจำลองเชิงโครงสร้างของระบบ, แผนภาพซีเควนซ์ใช้อธิบายแบบจำลองเชิงปฏิสัมพันธ์ของระบบ และแผนภาพดีพลอยเมนต์ใช้อธิบายแบบจำลองเชิงสถาปัตยกรรมของระบบ เป็นต้น

ในงานวิจัยนี้นำเสนอการนำแบบรูปความมั่นคง [12] มาประยุกต์ใช้งานในสถานการณ์จริง การประเมินค่าความเสี่ยงของสินทรัพย์ต่างๆ ภายในองค์กร โดยนำเสนอการวิเคราะห์และออกแบบระบบใน 4 มุมมอง ประกอบด้วยมุมมองเชิงฟังก์ชันการทำงาน อธิบายบริการของระบบโดยใช้แผนภาพยูสเคส มุมมองเชิงโครงสร้าง อธิบายการจัดเก็บข้อมูลที่จำเป็นและความสัมพันธ์ระหว่างข้อมูลโดยใช้แผนภาพคลาส มุมมองเชิงพฤติกรรม อธิบายการโต้ตอบกันระหว่างส่วนประกอบต่างๆ ของระบบโดยใช้แผนภาพซีเควนซ์ และมุมมองเชิงสถาปัตยกรรม อธิบายสถาปัตยกรรมเชิงตรรกะของระบบโดยใช้แผนภาพดีพลอยเมนต์ อีกทั้งยังนำเสนอการสร้างภาพนามธรรม (Visualization) เพื่อแสดงรายงานความเสี่ยงต่างๆ ที่เกิดขึ้นในรูปของกราฟ เพื่อให้ผู้พัฒนาระบบ หรือผู้ใช้งานตระหนักถึงความสำคัญในการวางแผน และการจัดการทางด้านความมั่นคงที่ดีสำหรับสินทรัพย์ขององค์กร โดยการใช้การบริหารจัดการ ออกระเบียบปฏิบัติ ตลอดจนการนโยบายทางด้านความมั่นคงต่างๆ ที่เหมาะสม เพื่อที่จะสามารถดูแลรักษาสินทรัพย์ ข้อมูลสำคัญต่างๆ ขององค์กร ได้อย่างมีประสิทธิภาพ

2. ทฤษฎีที่เกี่ยวข้อง

2.1 แบบรูปความมั่นคง

แบบรูปความมั่นคง [1,6,7,12,15] เป็นแบบแผน หรือแนวทางในการแก้ไขปัญหาทางด้านความมั่นคงต่างๆ ที่พบได้เป็นประจำในการออกแบบระบบความมั่นคง โดยแผนภาพที่นิยมนำมาใช้อธิบายความสัมพันธ์ต่างๆ ในแบบรูปความมั่นคง คือ แผนภาพยูเอ็มแอลซึ่งนิยมใช้ในการอธิบายความสัมพันธ์ระหว่างวัตถุต่างๆ ในทางการเขียนโปรแกรมเชิงวัตถุ

แบบรูปความมั่นคงสามารถแบ่งได้เป็น 3 ประเภทคือ (1) แบบรูปการวิเคราะห์ความมั่นคง (Security Analysis Patterns) คือแบบรูปที่แก้ปัญหาการวิเคราะห์ความมั่นคงของระบบ (2) แบบรูปการออกแบบความมั่นคง (Security Design Patterns) คือแบบรูปที่แก้ปัญหาการออกแบบโครงสร้างความมั่นคงของระบบ และ (3) แบบรูปกระบวนการความมั่นคง (Security Process Patterns) คือแบบรูปที่แก้ปัญหาการออกแบบความมั่นคงให้กับกระบวนการของระบบ

แนวคิดในการพัฒนาแบบรูปความมั่นคงนั้นมีแนวคิดมาจากแบบรูปการออกแบบ แบบรูปความมั่นคงในระยะแรกๆ นั้น Yoder และ Barcalow [15] ได้นำเสนอแบบรูปเกี่ยวกับการพัฒนา ออกแบบระบบความมั่นคงไว้หลายแบบรูป ต่อจากนั้นมาได้มีผู้เสนอแบบรูปความมั่นคงต่างๆ ออกมาอย่างต่อเนื่อง เช่น Drrell M. Kienzle และ Matthew C. Elder [7] ได้นำเสนอแบบรูปความมั่นคงที่เกี่ยวกับการพัฒนาโปรแกรมประยุกต์บนเว็บไซต์จำนวน 2 กลุ่ม 29 แบบรูป B.Blakley และคณะ [1] ได้นำเสนอแบบรูปความมั่นคงจำนวน 2 กลุ่ม 13 แบบรูป M.schumacher และคณะ [12] ได้นำเสนอแบบรูปการออกแบบความมั่นคงจำนวน 8 กลุ่ม 46 แบบรูป

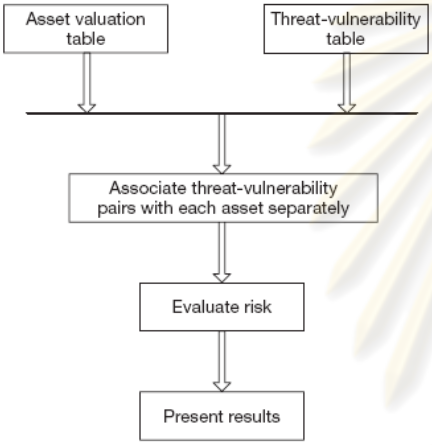
แบบรูปความมั่นคงที่จะนำมาใช้ในงานวิจัยฉบับนี้คือ แบบรูปของ M.schumacher และคณะ [12] ที่นำเสนอในหนังสือแบบรูปความมั่นคง การบูรณาการความมั่นคงและวิศวกรรมระบบ (Security Patterns: Integrating Security and Systems Engineering) เนื่องจากเป็นแบบรูปที่ได้รับความนิยม และแบบรูปที่สร้างขึ้นนั้นสามารถนำไปประยุกต์ใช้กับการพัฒนาซอฟต์แวร์ได้

องค์ประกอบของแบบรูปความมั่นคงของ M.schumacher และคณะ [12] ประกอบด้วยองค์ประกอบต่างๆ ดังนี้ (1) *ชื่อ (Name)* เป็นชื่อของแบบรูปความมั่นคง (2) *ชื่อที่รู้จัก (Also Known As)* เป็น ชื่ออื่นของแบบรูปความมั่นคง (3) *ตัวอย่าง (Example)* เป็น ตัวอย่างที่แสดงถึงปัญหาและความต้องการของแบบรูปความมั่นคง (4) *บริบท (Context)* เป็น สถานการณ์ที่ควรใช้แบบรูปความมั่นคง (5) *ปัญหา (Problem)* เป็นปัญหาที่แบบรูปความมั่นคงต้องแก้ไข (6) *ผลเฉลย (Solution)* เป็นคำตอบภายใต้แบบรูปความมั่นคง (7) *โครงสร้าง (Structure)* เป็นรายละเอียดโครงสร้างของแบบรูปความมั่นคง (8) *ไดนามิก (Dynamics)* เป็น เหตุการณ์ที่อธิบายถึงการทำงานของแบบรูปความมั่นคง (9) *การทำให้เกิดผล (Implementation)* เป็นการแนะนำในการทำให้เกิดผล (10) *ตัวอย่างการแก้ไข (Example Resolved)* เป็น ตัวอย่างการแก้ไขปัญหาด้วยแบบรูปความมั่นคง (11) *รูปแปร (Variants)* เป็น คำอธิบายของแบบรูปความมั่นคงที่มีลักษณะแตกต่างหรือพิเศษออกไป (12) *การนำไปใช้ที่ทราบ (Known Uses)* เป็น ตัวอย่างของการใช้แบบรูปความมั่นคงใน

ระบบความเป็นจริง (13) *ผลที่ได้ (Consequence)* เป็น ประโยชน์ที่ได้จากแบบรูปความมั่นคง (14) *เห็นได้จาก (See Also)* เป็น การอ้างถึงแบบรูปความมั่นคงอื่นที่แก้ไขปัญหาเดียวกัน

2.2 แบบรูปการกำหนดค่าความเสี่ยง

แบบรูปการกำหนดค่าความเสี่ยง (Risk Determination Patterns) [12] จัดอยู่ในกลุ่มของแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง เป็นขั้นตอนสุดท้ายของกระบวนการประเมินความเสี่ยง โดยการใช้ข้อมูลของมูลค่าสินทรัพย์ ภัยคุกคามและความถี่ที่เกิด ภาวะจุดอ่อนและระดับความรุนแรงมาใช้เป็นข้อมูลนำเข้า เพื่อนำมาคำนวณและแสดงผลเป็นระดับความเสี่ยงที่เหมาะสม ช่วยให้สามารถทราบความเสี่ยงของสินทรัพย์และจัดลำดับความสำคัญของสินทรัพย์ได้ ลำดับขั้นตอนการทำงานของแบบรูปนี้สามารถแสดงได้ดังรูปที่ 1



รูปที่ 1 ลำดับขั้นตอนการทำงานของแบบรูปการคำนวนค่าความเสี่ยง

การคำนวนค่าความเสี่ยงของสินทรัพย์สามารถคำนวนได้จากสูตรที่ (1)

$$Risk(A) = AssetValue(A) \times \sum_{i=1}^{n} Threat_i(A) \times vu\ln erability_i(A) \quad (1)$$

Risk(A) แทนค่าความเสี่ยงของสินทรัพย์ *AssetValue(A)* แทนมูลค่าของสินทรัพย์นั้น ๆ (จากแบบรูปการกำหนดมูลค่าสินทรัพย์) *Threat(A)* แทนอัตราการเกิดขึ้นของภัยคุกคามต่อสินทรัพย์ (จากแบบรูปการประเมินภัยคุกคาม) และ *Vulnerability(A)* แทนระดับความรุนแรงของจุดอ่อน (จากแบบรูปการประเมินภาวะเสี่ยง)

จากสูตรที่ (1) ค่าความเสี่ยงของสินทรัพย์ *A* มีค่าเท่ากับมูลค่าของสินทรัพย์นั้นๆ คูณกับผลรวมของผลคูณระหว่างอัตราการเกิดขึ้นของภัยคุกคามต่อสินทรัพย์ และ ระดับความรุนแรงของจุดอ่อน ในการกำหนดค่าความเสี่ยงเชิงคุณภาพนั้น จะนำค่าความเสี่ยงของแต่ละสินทรัพย์ที่คำนวนได้มาเรียงลำดับแล้วแบ่งเป็น 6 ชั้น โดยมีช่วงความกว้างของค่าความเสี่ยงในแต่ละชั้นเท่าๆ กัน ดังแสดงในตารางที่ 1

ตารางที่ 1 ตารางระดับความเสี่ยงเชิงคุณภาพ และค่าตัวอย่างความเสี่ยง

Level/Qualitative Name	Level/Qualitative value	Example of Risk Value
Extreme	6	200-239
Very high	5	160-199
High	4	120-159
Medium	3	80-119
Low	2	40-79
Negligible	1	1-39

2.3 การสร้างภาพนามธรรม

การสร้างภาพนามธรรม [5,8] เป็นวิธีการหนึ่งสำหรับการสร้างภาพ แผนภาพ หรือ ภาพเคลื่อนไหว เพื่อใช้ในการสื่อสารข้อความเพื่อทำให้เกิดความเข้าใจที่ชัดเจน มีความเข้าใจตรงกันทั้งผู้ส่งสารและผู้รับสาร การสร้างภาพนามธรรมนั้นจัดได้ว่าเป็นวิธีการที่มีประสิทธิภาพในการสื่อสารถึงสิ่งที่เป็นนามธรรม มองเห็นภาพได้ยาก นำมาสร้างเป็นภาพเพื่อการติดต่อสื่อสารที่ทำความเข้าใจได้ง่ายและชัดเจนมากยิ่งขึ้น

การสร้างภาพนามธรรมนั้นสามารถแบ่งออกได้หลายประเภทตามจุดประสงค์ของการสร้างภาพนามธรรมและประเภทของการนำเสนอ [8] ดังนี้ *การสร้างภาพนามธรรมของข้อมูล (Data Visualization) การสร้างภาพนามธรรมของสารสนเทศ (Information Visualization) การสร้างภาพนามธรรมของแนวคิด (Concept Visualization) การสร้างภาพนามธรรมของกลยุทธ์ (Strategy Visualization) การสร้างภาพนามธรรมของการอุปมาน (Metaphor Visualization)* และ *การสร้างภาพนามธรรมของการประกอบ (Compound Visualization)*

การสร้างภาพนามธรรมของข้อมูล เป็นวิธีการในการนำเสนอข้อมูลประเภทหนึ่งโดยการใช้แผนภูมิ กราฟ เส้นจำนวน และตาราง เป็นต้น ซึ่งเป็นวิธีการพื้นฐานในการสร้างภาพนามธรรมของข้อมูล นอกจากนี้ยังสามารถเพิ่มเติมการใช้ขนาดของตัวอักษร สีสัน รูปทรงตลอดจนภาพเคลื่อนไหวต่างๆ เข้ามาประกอบการสร้างภาพได้ด้วย

3. งานวิจัยที่เกี่ยวข้อง

กวิน และคณะ [14] เสนอการสร้างไวยากรณ์ความมั่นคงจากแบบรูปความมั่นคงโดยไวยากรณ์ที่ใช้ในงานวิจัยนี้เป็นไวยากรณ์อีบีเอ็นเอฟ [2,11] และเครื่องมือที่นำไวยากรณ์ที่ได้มาประยุกต์ใช้ เพื่อใช้กำหนดความต้องการความมั่นคง โดยแบบรูปความมั่นคงที่ใช้นั้นมาจากแบบรูปความมั่นคงของ M.schumacher และคณะ [12] โดยนำเอาแบบรูปดังกล่าวมาประยุกต์ใช้จำนวนทั้งสิ้น 20 แบบรูป จาก 4 กลุ่ม ได้แก่ การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง การระบุตัวตนและการพิสูจน์ตัวจริง แบบจำลองควบคุมการเข้าถึง และสถาปัตยกรรมไฟล์วอลล์ แล้วสร้างเป็นแผนภาพต้นไม้ความมั่นคง เพื่อแสดงความสัมพันธ์ระหว่างองค์ประกอบของแบบรูปความมั่นคงและแปลงไปเป็นไวยากรณ์ความมั่นคงในรูปอีบีเอ็นเอฟ จากงานวิจัยนี้เราได้นำวิธีการวิเคราะห์โครงสร้างของแบบรูปความมั่นคง และแบบรูปความมั่นคงที่สัมพันธ์กัน ซึ่งช่วยใน

การพิจารณาสร้างเป็นแบบจำลองเชิงโครงสร้าง โดยใช้แผนภาพคลาสที่รองรับไวยากรณ์ที่ถูกสร้างขึ้นมาจากแบบรูปความมั่นคง

งานวิจัยที่เกี่ยวกับการประเมินค่าความเสี่ยง Meier และคณะ [10] นำเสนอวิธีการในการคำนวณค่าความเสี่ยงของภัยคุกคามสำหรับโปรแกรมประยุกต์บนเว็บ ซึ่งมีค่าเท่ากับความน่าจะเป็นของภัยคุกคามที่อาจเกิดขึ้นคูณกับระดับความรุนแรงของเหตุการณ์นั้น ผลลัพธ์ที่ได้มีค่าตั้งแต่ 1 ถึง 100 โดยแทนค่าความเสี่ยงน้อยที่สุดและมากที่สุดตามลำดับ ดังแสดงในสูตรที่ (2)

$$Risk = Probability \times Damage\ Potential \quad (2)$$

Risk แทนค่าความเสี่ยงของภัยคุกคาม *Probability* แทนความน่าจะเป็นของภัยคุกคามที่อาจเกิดขึ้น และ *Damage Potential* แทนระดับความรุนแรงของเหตุการณ์นั้น

สำหรับการประเมินค่าความเสี่ยงเชิงคุณภาพนั้น ความเสี่ยง “ต่ำ” จะแทนค่าความเสี่ยงตั้งแต่ 1 ถึง 33, ความเสี่ยง “ปานกลาง” จะแทนค่าความเสี่ยง 34 ถึง 66 และความเสี่ยง “สูง” จะแทนค่าความเสี่ยงตั้งแต่ 67 ถึง 100 Stoneburner และคณะ [13]ใช้วิธีการคำนวณค่าความเสี่ยงแบบเมตริกซ์ 3x3 โดยพิจารณาค่าความน่าจะเป็นของการเกิดภัยคุกคามซึ่งมีค่า“สูง”, “กลาง” และ “ต่ำ” โดยมีค่าเท่ากับ 1.0, 0.5 และ 0.1 ตามลำดับ และ ค่าผลกระทบของภัยคุกคามนั้นๆ ซึ่งมีค่า“สูง”, “กลาง” และ “ต่ำ” โดยมีค่าเท่ากับ 100, 50 และ 10 ตามลำดับ มาคำนวณหาค่าความเสี่ยงโดยการคูณ จากการศึกษางานวิจัยการคำนวณค่าความเสี่ยงทั้งสามของ M.schumacher [12] Meier [10] และ Stoneburner [13] พบว่ามีรายการแตกต่างบางประการ สามารถสรุปได้ดังตารางที่ 2

ตารางที่ 2 สรุปข้อแตกต่างงานวิจัยการคำนวณค่าความเสี่ยง

รายการข้อแตกต่าง	M.schumacher [12]	Meier [10]	Stoneburner [13]
ระบบอ้างอิง	Enterprise Asset	Web application	IT system
การออกแบบ	Pattern	Document	Document
จำนวนระดับความเสี่ยง	6	3	3-5
ตัวแปรในการคำนวน	มูลค่าสินทรัพย์, อัตราการเกิดขึ้นของภัยคุกคาม, ความรุนแรงของจุดอ่อน	ความน่าจะเป็นของภัยคุกคาม, ระดับความรุนแรงของเหตุการณ์	ความน่าจะเป็นของภัยคุกคาม, ผลกระทบของภัยคุกคาม

จากตารางที่ 2 ผู้วิจัยได้เลือกใช้แบบรูปการคำนวณค่าความเสี่ยงของ M.schumacher [12] เนื่องจากเป็นการนำเสนอการคำนวณค่าความเสี่ยงสินทรัพย์ขององค์กร มีจำนวนระดับความเสี่ยง 6 ขั้น และมีการนำมูลค่าของสินทรัพย์มาใช้ในการคำนวณด้วย

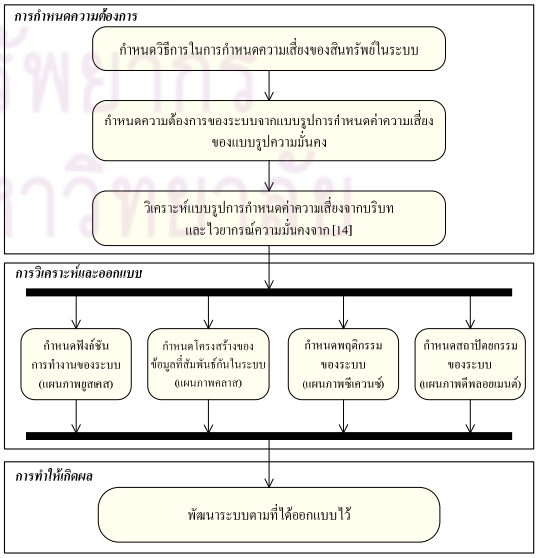
4. การประยุกต์ใช้แบบรูปเพื่อการกำหนดค่าความเสี่ยง

ในขั้นตอนนี้จะเป็นการนำเสนอวิธีการประยุกต์ใช้แบบรูปการกำหนดค่าความเสี่ยงในการใช้งานจริงขององค์กร โดยแบบรูปการกำหนดค่าความเสี่ยงนั้นเป็นขั้นตอนสุดท้ายของกระบวนการประเมินความเสี่ยง โดยการใช้ข้อมูลการประเมินมูลค่าสินทรัพย์ ภัยคุกคามและความถี่ที่เกิด ภาวะจุดอ่อนและระดับความรุนแรงมาใช้เป็นข้อมูลนำเข้าเพื่อนำมาคำนวณและแสดงผลเป็นระดับความเสี่ยงที่เหมาะสม ช่วยให้สามารถทราบความเสี่ยงของสินทรัพย์และจัดลำดับความสำคัญของสินทรัพย์ได้

โดยการประยุกต์ใช้แบบรูปการกำหนดค่าความเสี่ยงนั้นจะต้องมีการระบุชื่อของสินทรัพย์ (จากแบบรูป การระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร : Security Needs Identification for Enterprise Asset : SNIEA) ระบุมูลค่าของสินทรัพย์ (จากแบบรูปการกำหนดมูลค่าสินทรัพย์ : Asset Valuation : AV) ระบุภัยคุกคาม (จากแบบรูปการประเมินภัยคุกคาม : Threat Assessment : TA) และภาวะเสี่ยง (จากแบบรูปการประเมินภาวะเสี่ยง : Vulnerability Assessment : VA) สำหรับสินทรัพย์นั้นๆ ก่อน จึงจะสามารถประยุกต์ใช้แบบรูปการกำหนดค่าความเสี่ยงนี้ได้

ภายในหัวข้อนี้จะกล่าวถึงรายละเอียดของการประยุกต์ใช้แบบรูปการกำหนดค่าความเสี่ยง โดยนำเสนอการวิเคราะห์และออกแบบระบบใน 4 มุมมอง ประกอบด้วยมุมมองเชิงฟังก์ชันการทำงาน อธิบายบริการของระบบโดยใช้แผนภาพยูสเคส มุมมองเชิงโครงสร้าง อธิบายการจัดเก็บข้อมูลที่จำเป็นและความสัมพันธ์ระหว่างข้อมูลโดยใช้แผนภาพคลาส มุมมองเชิงพฤติกรรม อธิบายการโต้ตอบกันระหว่างส่วนประกอบต่างๆ ของระบบโดยใช้แผนภาพซีเควนซ์ และมุมมองเชิงสถาปัตยกรรม อธิบายสถาปัตยกรรมเชิงตรรกะของระบบโดยใช้แผนภาพดีพลอยเมนต์

กรอบงานการประยุกต์ใช้แบบรูปการกำหนดค่าความเสี่ยงสามารถแสดงได้ดังรูปที่ 2 ประกอบด้วย 3 ขั้นตอน คือ (1) การกำหนดความต้องการ เพื่อให้ได้ความต้องการที่ตรงกับวัตถุประสงค์ของผู้ใช้งานและแบบรูป (2) การวิเคราะห์และออกแบบ เป็นการวิเคราะห์และสร้างแบบจำลองต่างๆ เพื่อใช้ในขั้นตอนของการออกแบบ และ (3) การทำให้เกิดผล โดยพัฒนาและทดสอบตามที่ออกแบบไว้ในขั้นตอนที่ (2)

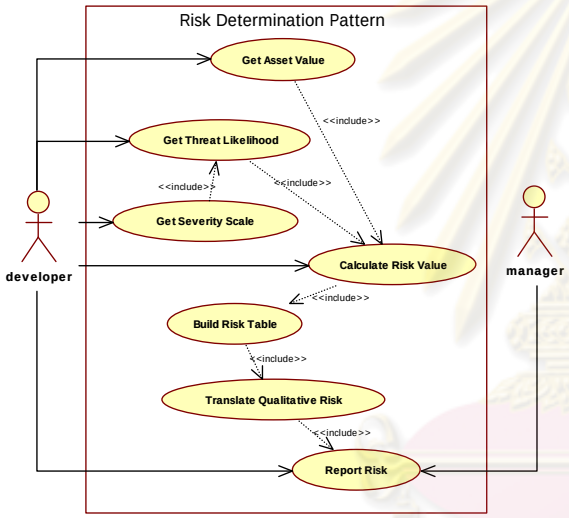


รูปที่ 2 กรอบงานการประยุกต์ใช้แบบรูปเพื่อการกำหนดค่าความเสี่ยง

4.1 การสร้างแบบจำลองเชิงฟังก์ชันของแบบรูป

ขั้นตอนแรกนี้เป็นการอธิบายฟังก์ชันการทำงาน และบริการต่างๆ ของระบบโดยใช้แผนภาพยูสเคส ใช้สำหรับสื่อสารระหว่างผู้พัฒนาระบบกับผู้ใช้ระบบงาน เพื่อให้ได้ความต้องการที่แท้จริง

แผนภาพยูสเคสของแบบรูปการกำหนดค่าความเสี่ยงสามารถเขียนได้ดังรูปที่ 3 ภายในประกอบไปด้วยยูสเคส *Get Asset Value, Get Threat Likelihood, Get Severity Scale, Calculate Risk Value, Build Risk Table, Translate Qualitative Risk* และ *Report Risk* โดยผู้พัฒนาระบบจะสามารถดูข้อมูลมูลค่าของสินทรัพย์ ค่าอัตราการเกิดขึ้นของภัยคุกคาม ค่าระดับความรุนแรงของจุดอ่อน และสามารถคำนวนหาค่าความเสี่ยงของสินทรัพย์นั้นๆ ได้ ตลอดจนการสร้างรายงานสรุปค่าความเสี่ยง ในส่วนของผู้บริหารนั้นจะสามารถเรียกดูข้อมูลรายงานสรุปค่าความเสี่ยงของสินทรัพย์ต่างๆ ได้

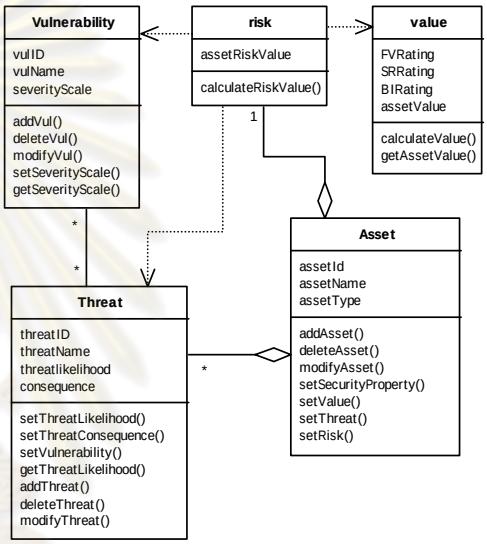


รูปที่ 3 แผนภาพยูสเคสของแบบรูปการกำหนดค่าความเสี่ยง

4.2 การสร้างแบบจำลองเชิงโครงสร้างของแบบรูป

ในการสร้างแบบจำลองเชิงโครงสร้างของระบบนี้จะใช้แผนภาพคลาสช่วยในการออกแบบ อธิบายการจัดเก็บข้อมูลที่จำเป็นและความสัมพันธ์ระหว่างข้อมูล เนื่องจากแผนภาพคลาสเป็นแผนภาพมาตรฐานหนึ่งของยูเอ็มแอลซึ่งได้รับความนิยมในการแสดงแบบจำลองโครงสร้างของระบบ ทำให้เข้าใจได้ง่ายขึ้น และง่ายต่อการนำไปประยุกต์ใช้ การสร้างแผนภาพคลาสนี้มีเป้าหมายเพื่อให้ได้แผนภาพคลาสที่สอดคล้องกับแบบรูปการกำหนดค่าความเสี่ยง [12] และไวยากรณ์ความมั่นคง [14] เพื่อแสดงให้เห็นความสัมพันธ์ภายในแต่ละคลาสของแบบรูปการกำหนดค่าความเสี่ยง

แผนภาพคลาสของแบบรูปการกำหนดค่าความเสี่ยงสามารถแสดงได้ดังรูปที่ 4 ประกอบไปด้วย 5 คลาส ดังนี้ (1) *คลาส Asset* เป็นคลาสสินทรัพย์ขององค์กร (2) *คลาส Value* เป็นคลาสมูลค่าสินทรัพย์โดยต้องมีการกำหนดมูลค่าในแต่ละสินทรัพย์ขององค์กรเพื่อระบุถึงความสำคัญของสินทรัพย์นั้นๆ ต่อองค์กร (3) *คลาส Threat* เป็นคลาสภัยคุกคามต่อสินทรัพย์ โดยต้องมีการประเมินภัยคุกคามที่อาจเกิดขึ้น (4) *คลาส Vulnerability* เป็นคลาสภาวะเสี่ยงของภัยคุกคามที่อาจจะเกิดขึ้นกับสินทรัพย์ (5) *คลาส Risk* เป็นคลาสความเสี่ยง โดยแต่ละสินทรัพย์จะต้องมีการประเมินค่าความเสี่ยงซึ่งจะขึ้นกับค่าของมูลค่าสินทรัพย์(ค่า *assetValue* จากคลาส *Value*) ค่าอัตราการเกิดขึ้นของภัยคุกคามต่อสินทรัพย์(ค่า *threatlikelihood* จากคลาส *Threat*) ค่าระดับความรุนแรงของภาวะเสี่ยงของภัยคุกคามนั้นๆ (ค่า *severityScale* จากคลาส *Vulnerability*)

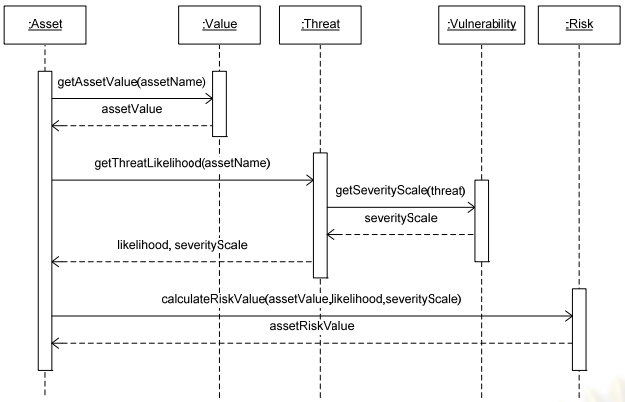


รูปที่ 4 แผนภาพคลาสของแบบรูปการกำหนดค่าความเสี่ยง

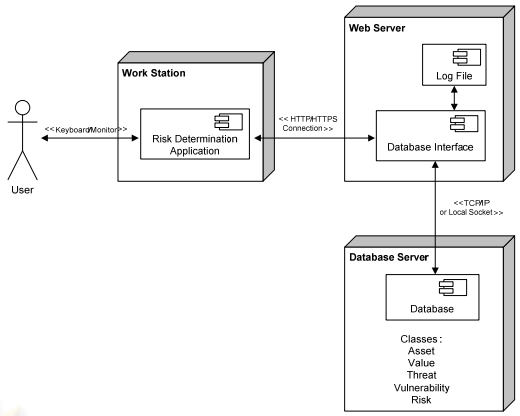
4.3 การสร้างแบบจำลองเชิงพฤติกรรมของแบบรูป

หลังจากได้ออกแบบแผนภาพยูสเคสเพื่อใช้อธิบายแบบจำลองเชิงฟังก์ชันการทำงานของระบบ และแผนภาพคลาสเพื่อใช้แสดงแบบจำลองเชิงโครงสร้างของระบบแล้ว ขั้นตอนต่อไปคือการสร้างแบบจำลองเชิงพฤติกรรมของระบบ โดยจะใช้แผนภาพซีเควนซ์เพื่อใช้แสดงการโต้ตอบกันระหว่างวัตถุ ณ เวลาต่างๆ และลำดับของการส่งสารระหว่างคลาสต่างๆ ของแบบรูปการกำหนดค่าความเสี่ยง

แผนภาพซีเควนซ์ของแบบรูปการกำหนดค่าความเสี่ยงสามารถเขียนได้ดังรูปที่ 5 โดยเป็นการแสดงการส่งสารระหว่าง 5 คลาส เริ่มจาก คลาส *Asset* จะส่งสาร *getAssetValue()* และ *getThreatLikelihood()* ไปยังคลาส *Value* และ *Threat* เพื่อรับค่ามูลค่าสินทรัพย์ ค่าอัตราการเกิดขึ้นของภัยคุกคาม และค่าระดับความรุนแรงของจุดอ่อน เพื่อนำมาใช้เป็นค่านำเข้าในการคำนวณค่าความเสี่ยงในคลาส *Risk* โดยเมดธอด *CalculateRiskValue()*



รูปที่ 5 แผนภาพซีเควนซ์ของแบบรูปการกำหนดค่าความเสี่ยง



รูปที่ 6 แผนภาพดีพลอยเมนต์ของแบบรูปการกำหนดค่าความเสี่ยง

ตารางที่ 3 ตัวอย่างข้อมูลลักษณะประจำภายในแต่ละคลาส

SNIEA Patterns		AV Patterns	TA Patterns		VA Patterns		RD Patterns
Asset class		Value class	Threat class		Vulnerability class		Risk class
Asset Name	Asset Type	Asset Value	ThreatName	Threat likelihood	Vulnerability Name	Severity Scale	Risk Value
Computer (or server)	Physical	Very high	Hacked (in case of server) for computer	High	Inadequate security control	High	Very high
			ID and password was take over	High	Encryption devices do not used	High	
			Data entry error	Low	Lack of data validation from input process	Low	
Network device	Physical	Very high	Network down	High	Lack of monitoring devices to detect unauthorized intrusions	High	Very high
					Inadequate audit trail review of system activity	Medium	
			Data entry error	Low	Lack of data validation from input process	Low	
Critical lab data	Information	Extreme	Lost of critical lab data	Very high	Lack of proper physical controls	Medium	Extreme
			Unauthorized access for critical lab data	high	Full audit trail is not implemented	Medium	
					Poor password management program	Medium	
SE lab member	Physical	Medium	Unauthorized modification for SE lab member	Medium	Inadequate program control	Very high	Low
Personal data	Information	low	Unauthorized modification for personal data	Medium	Inadequate program control	Very high	Low

4.4 การสร้างแบบจำลองเชิงสถาปัตยกรรมของแบบรูป

ขั้นตอนนี้เป็นการสร้างแผนภาพดีพลอยเมนต์เพื่อใช้อธิบายแบบจำลองเชิงสถาปัตยกรรมของแบบรูปการกำหนดค่าความเสี่ยง โดยสามารถแสดงได้ดังรูปที่ 6 ประกอบไปด้วย 3 โหนดหลักคือ *Work Station, Web Server* และ *Database Server* โดยผู้ใช้งานจะติดต่อกับส่วนประกอบ *Risk Determination Application* ซึ่งเป็นโปรแกรมในการกำหนดค่าความเสี่ยง โดยผ่านทางแป้นพิมพ์หรือหน้าจอ จากนั้นโปรแกรมจะติดต่อไปยังส่วนประกอบ *Database Interface* ของเว็บเซิฟเวอร์โดยผ่านทางการเชื่อมต่อ *HTTP/HTTPS* และเชื่อมต่อไปยังฐานข้อมูลโดยผ่านทางการเชื่อมต่อ *TCP/IP* หรือ *Local Socket* อนึ่งคลาส *Asset, Value, Threat, Vulnerability* และ *Risk* จะอยู่ในส่วนของโหนด *Database Server* ซึ่งภายในจะเก็บข้อมูลอยู่ในรูปแบบของตาราง

5. การสร้างภาพนามธรรมของแบบรูปการกำหนดค่าความเสี่ยง

ในหัวข้อนี้แบ่งออกเป็น 3 หัวข้อย่อย ประกอบด้วย การคำนวนค่าความเสี่ยง, การกำหนดค่าความเสี่ยงเชิงคุณภาพ และการสร้างภาพนามธรรมของการกำหนดค่าความเสี่ยง

5.1 การคำนวนค่าความเสี่ยง

ค่าความเสี่ยงนั้นสามารถคำนวนได้จากสูตรที่ (1) ค่าของสินทรัพย์คูณกับค่าผลรวมของผลคูณระหว่างอัตราการเกิดขึ้นของภัยคุกคามต่อสินทรัพย์ และ ระดับความรุนแรงของจุดอ่อน ตารางแสดงระดับความเสี่ยงเชิงคุณภาพ และค่าตัวอย่างความเสี่ยงที่สามารถคำนวนได้ แสดงในตารางที่ 1

ในกรณีนี้เราจะยกตัวอย่างการประเมินค่าความเสี่ยงของสินทรัพย์ภายในห้องปฏิบัติการ โดยสินทรัพย์ภายในห้องปฏิบัติการอาจจะประกอบไปด้วย คอมพิวเตอร์(หรือเซิฟเวอร์), อุปกรณ์เครือข่าย, ข้อมูลสำคัญต่างๆ ของห้องปฏิบัติการ, สมาชิกภายในห้องปฏิบัติการ

และข้อมูลสมาชิก เป็นต้น ตารางที่ 3 แสดงตัวอย่างข้อมูลลักษณะประจำภายในแต่ละคลาส ที่สอดคล้องกับแผนภาพคลาสที่ 3 โดยประกอบด้วย 5 แบบรูป จำนวน 5 คลาส ภายในแสดงค่าตัวอย่างลักษณะประจำที่เป็นไปได้

ข้อมูลจากตารางที่ 3 เราสามารถคำนวนค่าความเสี่ยงของแต่ละสินทรัพย์โดยการใช้สูตรที่ (1) เช่น ค่าความเสี่ยงของคอมพิวเตอร์ (หรือเซิฟเวอร์) สามารถคำนวนได้ดังนี้

$$Risk(computer\ or\ server) = AssetValue(computer\ or\ server) \times \sum_{i=1}^{n} Threatlikelihood_i(computer\ or\ server) \times SeverityScale_i(computer\ or\ server)$$

$$Risk(computer\ or\ server) = 5 \times ((4x4)+(4x4)+(4x2))$$
$$Risk(computer\ or\ server) = 180$$

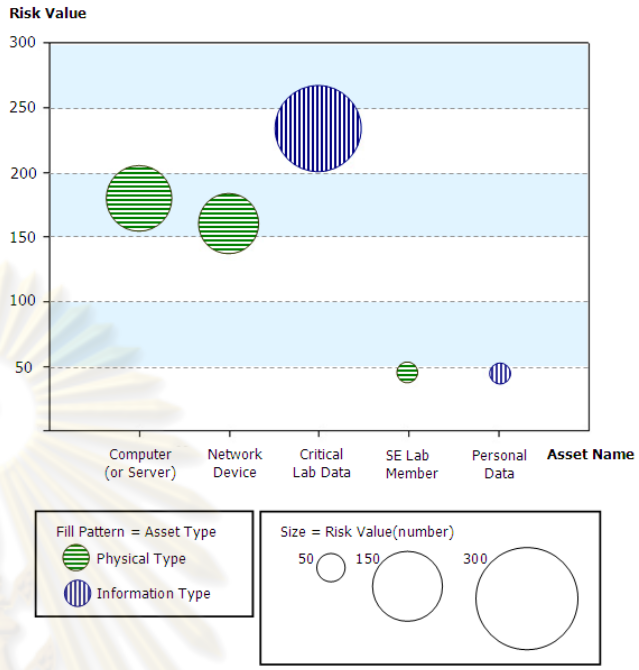
ใช้การคำนวนในลักษณะเดียวกันกับสินทรัพย์ต่างๆ จะได้ค่าความเสี่ยง 160, 234, 45 และ 45 สำหรับสินทรัพย์อุปกรณ์เครือข่าย, ข้อมูลสำคัญต่างๆ ของห้องปฏิบัติการ, สมาชิกภายในห้องปฏิบัติการ และข้อมูลสมาชิก ตามลำดับ

5.2 การกำหนดค่าความเสี่ยงเชิงคุณภาพ

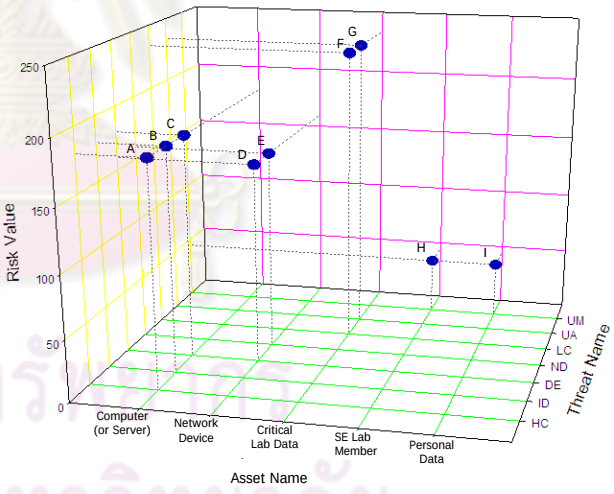
เมื่อนำค่าความเสี่ยงของสินทรัพย์ต่างๆ ที่ได้จากข้อ 5.1 มาเรียงลำดับโดยแบ่งช่วงชั้นให้เท่าๆ กัน ตามตารางที่ 1 แล้วจะได้ระดับค่าความเสี่ยงเชิงคุณภาพของแต่ละสินทรัพย์ดังแสดงในสดมภ์สุดท้ายของตารางที่ 2 กล่าวคือ คอมพิวเตอร์(หรือเซิฟเวอร์) และอุปกรณ์เครือข่าย มีระดับค่าความเสี่ยงเชิงคุณภาพเป็น *Very high,* ข้อมูลสำคัญต่างๆ ของห้องปฏิบัติการมีระดับค่าความเสี่ยงเชิงคุณภาพเป็น *Extreme,* สมาชิกภายในห้องปฏิบัติการ และข้อมูลสมาชิกมีระดับค่าความเสี่ยงเชิงคุณภาพเป็น *Low* ซึ่งระดับค่าความเสี่ยงเชิงคุณภาพของแต่ละสินทรัพย์นี้จะช่วยให้ผู้พัฒนาระบบ หรือผู้ใช้งานตระหนักถึงความสำคัญในการวางแผนและการจัดการทางด้านความมั่นคงสำหรับสินทรัพย์ขององค์กร โดยการใช้การบริหารจัดการ ระเบียบปฏิบัติ ตลอดจนการออกนโยบายทางด้านความมั่นคงต่างๆ ที่เหมาะสมสำหรับแต่ละสินทรัพย์ที่มีระดับความสำคัญต่างๆ ขององค์กร

5.3 การสร้างภาพนามธรรมของการกำหนดค่าความเสี่ยง

เมื่อนำข้อมูลที่ได้จากตารางที่ 2 มาสร้างภาพนามธรรมของข้อมูลในรูปแบบของกราฟสองมิติ และสามมิตินั้นสามารถแสดงได้ดังรูปที่ 7 และ 8 โดยรูปที่ 7 นั้นแสดงแผนภูมิแบบฟอง (Bubble Graph) ระหว่างค่าของ *AssetName* ในแกน x และค่าความเสี่ยงของ *RiskValue* ในแกน y ส่วนขนาดและสีของฟอง (Bubble) จะแทนด้วยค่าความเสี่ยงและประเภทของสินทรัพย์ ตามลำดับ ในรูปที่ 8 นั้นแสดงกราฟแบบสามมิติ ระหว่างค่าของ *AssetName, ThreatName* และ *RiskValue* ในแนวแกน x, y และ z ตามลำดับ ตัวอย่างเช่น จุด *A* แทนค่าคอมพิวเตอร์ (หรือเซิฟเวอร์) อาจเกิดภัยคุกคาม *Hack (in case of server) for computer* โดยมีค่าความเสี่ยงเท่ากับ 180 เป็นต้น



รูปที่ 7 แผนภูมิแบบฟองระหว่าง AssetName และ RiskValue



รูปที่ 8 กราฟแบบสามมิติ ระหว่าง AssetName, RiskValue และ ThreatName

ในการสร้างภาพนามธรรมของข้อมูล เพื่อแสดงรายงานความเสี่ยงต่างๆ ที่เกิดขึ้นในรูปของกราฟนี้จะทำให้ผู้บริหาร หรือผู้พัฒนาระบบความมั่นคงนั้น สามารถตระหนักถึงความสำคัญ และมูลค่าของสินทรัพย์นั้นๆ ต่อองค์กรได้อย่างชัดเจน สามารถออกนโยบาย ระเบียบปฏิบัติทางด้านความมั่นคงต่างๆ ที่เหมาะสม เพื่อที่จะสามารถดูแลรักษาสินทรัพย์ ข้อมูลสำคัญต่างๆ ขององค์กร ได้อย่างมีประสิทธิภาพมากที่สุด

6. สรุปและงานที่จะทำในอนาคต

ทุกๆ องค์กรต้องการที่จะปกป้อง รักษาสินทรัพย์ ตลอดจนข้อมูลสำคัญต่างๆ ขององค์กรไว้ ดังนั้นข้อมูลเกี่ยวกับมูลค่าของสินทรัพย์ ตลอดจนมูลค่าความเสี่ยงของสินทรัพย์ต่างๆ ขององค์กรจึงเป็นสิ่งสำคัญที่ควรต้องมีการพิจารณาและให้ลำดับความสำคัญ ในงานวิจัยนี้นำเสนอการนำแบบรูปความมั่นคงมาประยุกต์ใช้งานในสถานการณ์จริง การประเมินค่าความเสี่ยงของสินทรัพย์ต่างๆ ภายในองค์กร อีกทั้งยังนำเสนอการสร้างภาพนามธรรม เพื่อแสดงรายงานความเสี่ยงต่างๆ ที่เกิดขึ้นในรูปของกราฟ เพื่อให้ผู้บริหาร ผู้พัฒนาระบบ หรือผู้ใช้งานตระหนักถึงความสำคัญของสินทรัพย์นั้นๆ ต่อองค์กร เพื่อที่จะมีการวางแผน การจัดการทางด้านความมั่นคง ตลอดจนการออกนโยบาย ระเบียบข้อปฏิบัติต่างๆ เกี่ยวกับสินทรัพย์ได้อย่างเหมาะสม และมีประสิทธิภาพ

ในขั้นตอนต่อไปของการประยุกต์ใช้แบบรูปการกำหนดค่าความเสี่ยงนั้นคือการเขียน และการทดสอบโปรแกรม งานวิจัยในอนาคตควรจะสามารถทำการสร้างและตรวจสอบโปรแกรมจากแผนภาพยูเอ็มแอลที่ได้นำเสนอไว้ในงานวิจัยนี้ โดยจะต้องมีความสอดคล้องกันกับแบบรูปการกำหนดค่าความเสี่ยง และข้อมูลความต้องการต่างๆ ของผู้ใช้งาน

7. รายการอ้างอิง

[1] B. Blakley, C. Heath and members of The Open Group Security Forum, “Security Design Patterns”, *The Open Group U.K.*, April, 2004.

[2] EBNF language construct and some results, http://en.wikipedia.org/wiki/EBNF, 2008

[3] G. Booch, J. Rumbaugh, I. Jacobson, *The Unified Modeling Language User Guide SECOND EDITION*, Addison Wesley Professional, 2005.

[4] Gramma, E., et al., “Design Patterns Elements of Reusable Object-Oriented Software”, 1995.

[5] C. R. Johnson, C. D. Hansen. *Visualization Handbook*, Acadamic Press, 2004.

[6] J. Jurjens, *Secure Systems Development with UML*, Springer-Verlag Berlin Heidelberg 2005.

[7] D. M. Kienzle, M. C. Elder, “Security Patterns for Web Application Development”, *DARPA Contract # F30602-01-C-0164*, 2002.

[8] R. Lengler and M. J. Eppler. “Towards A Periodic Table of Visualization Methods for Management”, *In Proceedings of Graphics and Visualization in Engineering (GVE 2007)*, Clearwater, Florida, USA, ACTA Press. pp. 2007

[9] C. Larman, *Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and Iterative Development*, Addison Wesley Professional, 2004.

[10] J. D. Meier et al, “Improving Web Application Security: Threats and Countermeasures”, *Microsoft*, 2003

[11] N. Peter (ed.), “Revised Report on the Algorithmic Language ALGOL 60”, *Communications of the ACM*. 299-314.3-5, May 1960.

[12] M. Schumacher, E. Fernandez-Buglioni, D. Hybertson, F.Buschmann and P. Sommerlad, *Security Patterns: Integrating Security and Systems Engineering*, John Wiley & Son Ltd, England, 2005.

[13] G. Stoneburner, A. Goguen, A. Feringa, “Risk Management Guide for Information Technology Systems”, *NIST Special Publication SP800-30*, *National Institute of Standards and Technology (NIST)*, 2001

[14] K. Supaporn, *Defining Security Requirement Using Grammar of Security Patterns*, Master Thesis, Computer Engineering Department, Engineering Faculty, Chulalongkorn University, 2007.

[15] J. Yoder and J. Barcalow, “Architectureal Patterns for Enabling Applications Security”, *in Proceedings of PLoP*, 1997.

นางสาววีริยา สุภาณิชย์ สำเร็จการศึกษาในระดับปริญญาตรีสาขาวิทยาการคอมพิวเตอร์จากมหาวิทยาลัยบูรพา ปัจจุบันกำลังศึกษาต่อในระดับปริญญาโท สาขาวิทยาศาตร์คอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัย มีความสนใจทางด้าน Security patterns Data Visualization และ Software Engineering

อ.ธงชัย โรจน์กังสดาล สำเร็จการศึกษาM.Sc. (U. of Delaware) ปัจจุบันเป็นอาจารย์สอนที่จุฬาลงกรณ์มหาวิทยาลัย มีความสนใจทางด้าน Computer Security Creativity Support Tools Operating System และ Networking

ผศ.นครทิพย์ พร้อมพูล สำเร็จการศึกษา M.S. (George Washington U.) ปัจจุบันเป็นอาจารย์สอนที่จุฬาลงกรณ์มหาวิทยาลัย มีความสนใจทางด้าน Software Engineering และRequirements Engineering

ภาคผนวก ง
คำอธิบายและแผนภาพเชิงโครงสร้างของแบบรูปความมั่นคง

แผนภาพเชิงโครงสร้างของแบบรูปความมั่นคงในขอบเขตงานวิจัยนี้ ประกอบด้วย 20 แผนภาพ จาก 20 แบบรูปความมั่นคง จาก 4 กลุ่มแบบรูปความมั่นคง ซึ่งสามารถจำแนกตามกลุ่มของแบบรูปความมั่นคงได้ดังนี้

กลุ่มที่ 1 การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง ประกอบด้วย

1) การระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร

2) การกำหนดมูลค่าสินทรัพย์

3) การประเมินภัยคุกคาม

4) การประเมินภาวะเสี่ยง

5) การกำหนดความค่าความเสี่ยง

6) แนวคิดความมั่นคงองค์กร

7) บริการความมั่นคงองค์กร

8) การสื่อสารของผู้มีหุ้นส่วนองค์กร

กลุ่มที่ 2 การระบุและการพิสูจน์ตัวตน ประกอบด้วย

1) ความต้องการการระบุและการพิสูจน์ตัวตน

2) ทางเลือกการออกแบบการระบุและการพิสูจน์ตัวตน

3) การออกแบบและใช้รหัสผ่าน

4) ทางเลือกการออกแบบชีวมิติ

กลุ่มที่ 3 การควบคุมการเข้าถึง ประกอบด้วย

1) การให้อำนาจ

2) การควบคุมการเข้าถึงเชิงบทบาท

3) ความมั่นคงหลายระดับ

4) การตรวจสอบการเข้าถึงทรัพยากร

5) การกำหนดสิทธิ์ให้กับบทบาท

กลุ่มที่ 4 สถาปัตยกรรมไฟล์วอลล์ ประกอบด้วย

1) ไฟล์วอลล์กรองแพ็คเกจ

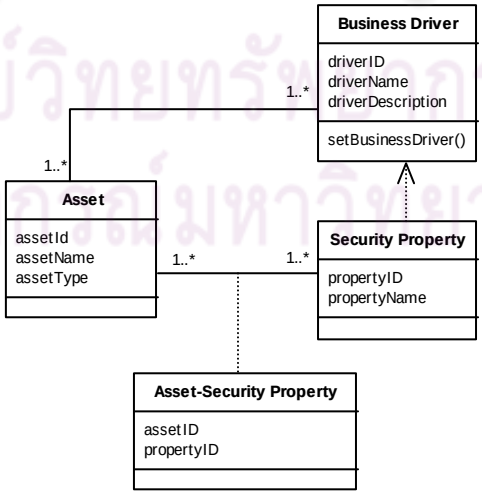
2) ไฟล์วอลล์เชิงตัวแทน

3) ไฟล์วอลล์เชิงสถานะ

งานวิจัยนี้ใช้แผนภาพคลาสในการแสดงแบบจำลองเชิงโครงสร้าง โดยมีรายละเอียดดังนี้

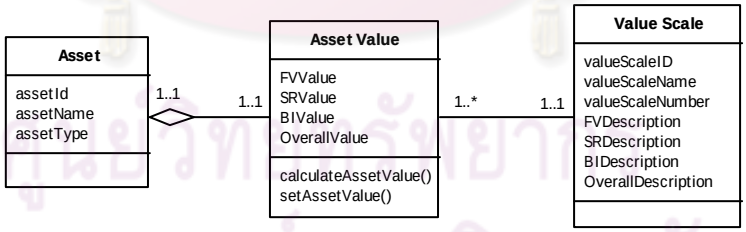
ตารางที่ ง.1 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร

ชื่อแบบรูป	การระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร
รหัสแบบรูป	P61
ชื่อกลุ่มของแบบรูป	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
เงื่อนไขก่อนการใช้	ไม่มี
คำอธิบาย	เป็นแบบรูปเริ่มต้นสำหรับการพิจารณาความมั่นคงองค์กร ซึ่งจะช่วยให้เข้าใจถึงความต้องการด้านความมั่นคงที่จำเป็นต้องมีในองค์กร เพื่อนำคุณสมบัติด้านความมั่นคง (Confidentiality : การรักษาความลับ, Integrity : ความบูรณภาพ, Availability : สภาพพร้อมใช้งาน, และ Accountability : ภาระรับผิดชอบ) มาประยุกต์ใช้
ปัญหา	องค์กรต้องการกำหนดความมั่นคงให้กับสินทรัพย์
ผลเฉลย	1. ระบุสินทรัพย์ 2. ระบุตัวขับเคลื่อนทางธุรกิจ 3. ระบุความสัมพันธ์ระหว่างสินทรัพย์และตัวขับเคลื่อนทางธุรกิจ 4. กำหนดคุณสมบัติด้านความมั่นคง 5. ระบุคุณสมบัติด้านความมั่นคงให้กับสินทรัพย์โดยพิจารณาจากตัวขับเคลื่อนทางธุรกิจ
แผนภาพคลาส	



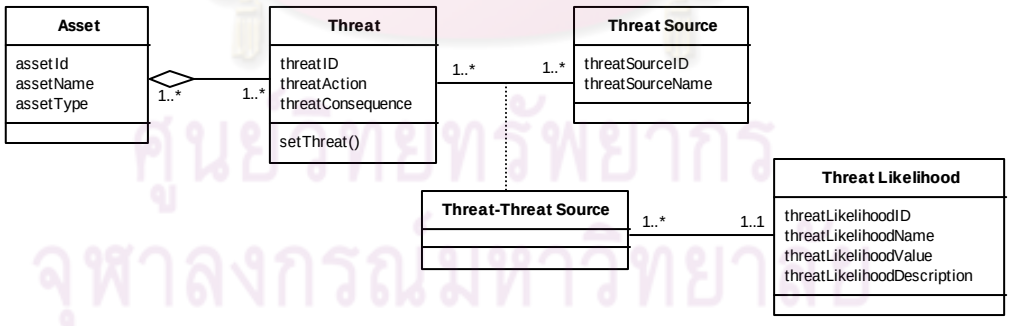
ตารางที่ ง.2 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปการกำหนดมูลค่าสินทรัพย์

ชื่อแบบรูป	การกำหนดมูลค่าสินทรัพย์
รหัสแบบรูป	P62
ชื่อกลุ่มของแบบรูป	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
เงื่อนไขก่อนการใช้	1. ชื่อสินทรัพย์ จาก GM61
คำอธิบาย	การกำหนดมูลค่าสินทรัพย์จะช่วยให้สามารถกำหนดความสำคัญของสินทรัพย์ขององค์กรที่เป็นเจ้าของหรือควบคุมอยู่ เพื่อระบุว่าเมื่อเกิดความสูญเสียของสินทรัพย์จะกระทบต่อองค์กรในด้านใดบ้างและมีผลกระทบในระดับใด โดยมูลค่าสินทรัพย์จะได้จากการพิจารณาผลกระทบในด้านต่างๆ ต่อไปนี้ ได้แก่ ด้านความต้องการความมั่นคง ด้านเศรษฐกิจ และทางด้านธุรกิจ
ปัญหา	การกำหนดค่าความสำคัญของสินทรัพย์ทำอย่างไร
ผลเฉลย	1. ระบุ security value ของสินทรัพย์ 2. ระบุ financial value ของสินทรัพย์ 3. ระบุ business impact value ของสินทรัพย์ 4. สร้างตารางรวมค่าสินทรัพย์ ทั้งหมดโดยกำหนดให้ ค่ามากที่สุดกลายเป็น overall value ของสินทรัพย์นั้น
แผนภาพคลาส	



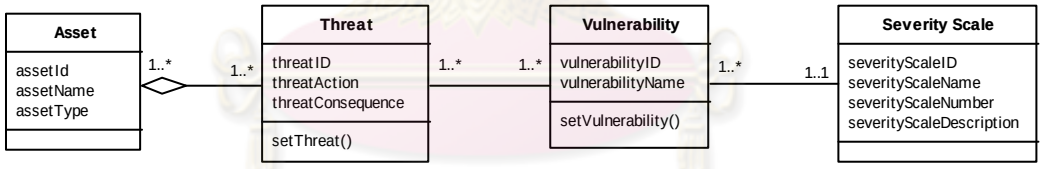
ตารางที่ ง.3 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปการประเมินภัยคุกคาม

ชื่อแบบรูป	การประเมินภัยคุกคาม
รหัสแบบรูป	P63
ชื่อกลุ่มของแบบรูป	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
เงื่อนไขก่อนการใช้	1. ชื่อสินทรัพย์ จาก GM61
คำอธิบาย	ภัยคุกคามเป็นโอกาสของอันตรายต่างๆ ที่อาจเกิดขึ้นและมีกระทบต่อสินทรัพย์องค์แบบรูปนี้จึงมีวัตถุประสงค์เพื่อกำหนดภัยคุกคาม ความถี่ของภัยคุกคามที่จะเกิดต่อสินทรัพย์ (Threat likelihood) และผลกระทบเมื่อสินทรัพย์ถูกคุกคาม (Threat consequence)
ปัญหา	จะระบุภัยคุกคามที่เกิดขึ้นกับสินทรัพย์ได้อย่างไร
ผลเฉลย	1. การระบุภัยคุกคาม ประกอบด้วย 1) ต้นเหตุที่ทำให้เกิดภัยคุกคาม 2) ภัยคุกคามที่เกิดขึ้น 3) ผลของภัยคุกคามนั้น 2. สร้างตารางภัยคุกคาม แยกตามชนิดของสินทรัพย์ 3. ระบุระดับความถี่ที่เกิดขึ้นของภัยคุกคาม 4. ระบุระดับความถี่ที่เกิดขึ้นในแต่ละภัยคุกคาม
แผนภาพคลาส	



ตารางที่ ง.4 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปการประเมินภาวะเสี่ยง

ชื่อแบบรูป	การประเมินภาวะเสี่ยง
รหัสแบบรูป	P64
ชื่อกลุ่มของแบบรูป	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
เงื่อนไขก่อนการใช้	1. ซื้อสินทรัพย์ จาก GM61 2. ซื้อภัยคุกคามสำหรับสินทรัพย์ในข้อ 1 ที่กำหนดไว้แล้วจาก GM63
คำอธิบาย	จุดอ่อน (ภาวะไม่มั่นคง) เป็นจุดที่จะถูกใช้โดยภัยคุกคาม การประเมินภาวะจุดอ่อน คือ การระบุจุดอ่อนของสินทรัพย์ในองค์กร และระดับความรุนแรงเมื่อถูกภัยคุกคามโจมตีจุดอ่อนดังกล่าว (Severity scale)
ปัญหา	ทำอย่างไรจึงจะกำหนดจุดอ่อนของสินทรัพย์ และระดับความรุนแรงเมื่อเกิดภัยคุกคามโจมตี
ผลเฉลย	1. รวบรวมข้อมูลของภัยคุกคาม 2. ระบุจุดอ่อนที่อาจเกิดขึ้น 3. สร้างตารางความสัมพันธ์ระหว่างจุดอ่อนและภัยคุกคาม 4. กำหนดระดับความรุนแรง
แผนภาพคลาส	

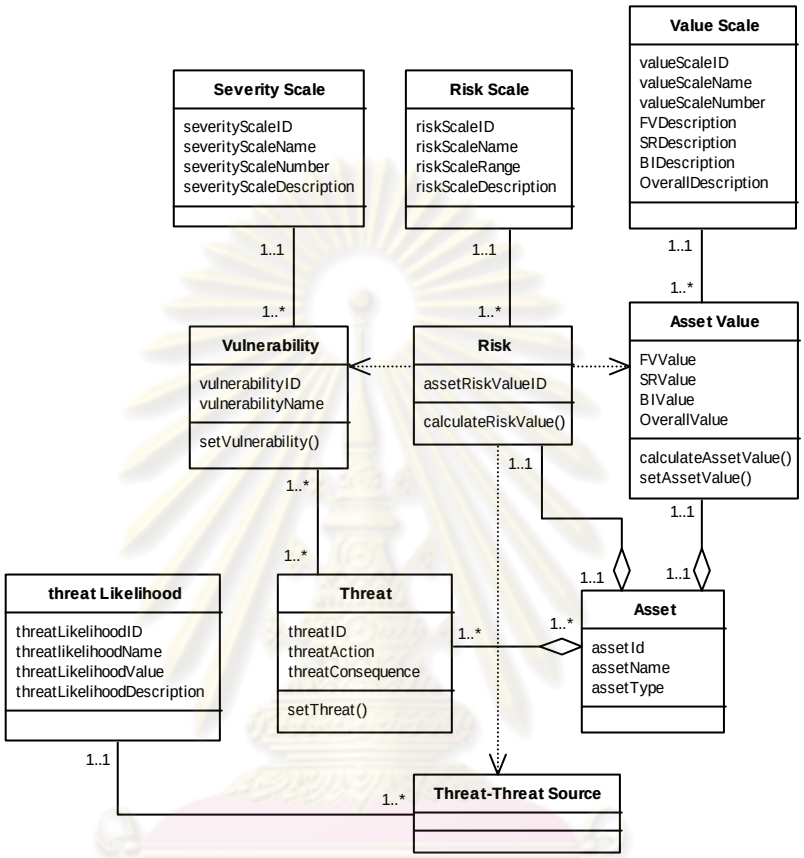


ตารางที่ ง.5 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปการกำหนดค่าความเสี่ยง

ชื่อแบบรูป	การกำหนดค่าความเสี่ยง
รหัสแบบรูป	P65
ชื่อกลุ่มของแบบรูป	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
เงื่อนไขก่อนการใช้	1. ชื่อสินทรัพย์ จาก GM61 (เฉพาะที่ตัวที่กำหนดมูลค่าสินทรัพย์ ประเมินภัยคุกคาม และภาวะเสี่ยงแล้วเท่านั้น) 2. ความถี่ของการเกิดภัยคุกคามทุกตัวสำหรับสินทรัพย์ในข้อ 1 จาก GM63 3. ระดับความรุนแรงของภาวะเสี่ยงทุกตัวสำหรับภัยคุกคามในข้อ 2 จาก GM64 4. มูลค่าสินทรัพย์ในข้อ 1 จาก GM62
คำอธิบาย	การกำหนดค่าความเสี่ยงเป็นขั้นตอนสุดท้ายของกระบวนการประเมินความเสี่ยง โดยการใช้ข้อมูลการประเมินมูลค่าสินทรัพย์ ภัยคุกคามและความถี่ที่เกิด ภาวะจุดอ่อนและระดับความรุนแรงมาใช้เป็นข้อมูลนำเข้าเพื่อนำมาคำนวณและแสดงผลเป็นระดับความเสี่ยงที่เหมาะสม ช่วยให้สามารถทราบความเสี่ยงของสินทรัพย์และจัดลำดับความสำคัญของสินทรัพย์ได้
ปัญหา	จะกำหนดค่าความเสี่ยงให้กับสินทรัพย์ได้อย่างไร
ผลเฉลย	1. รวบรวมผลลัพท์จาก 6.2, 6.3, 6.4 2. เชื่อมโยงภัยคุกคาม จุดอ่อน และสินทรัพย์เข้าด้วยกัน 3. คำนวนค่าความเสี่ยงตามสูตร ค่าความเสี่ยง = $\sum_{i=1}^{n}(ThreatLikelihood_i \times VulnerbilitySeverityScale_i) \times AssetValue$ 4. แสดงผลลัพท์ความเสี่ยง

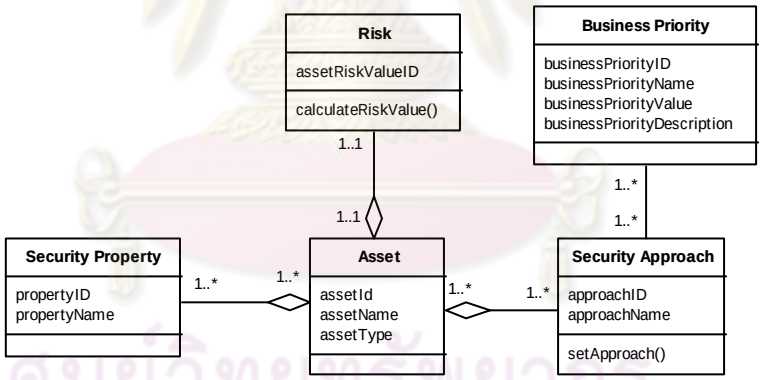
ตารางที่ ง.5 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปการกำหนดค่าความเสี่ยง (ต่อ)

แผนภาพคลาส



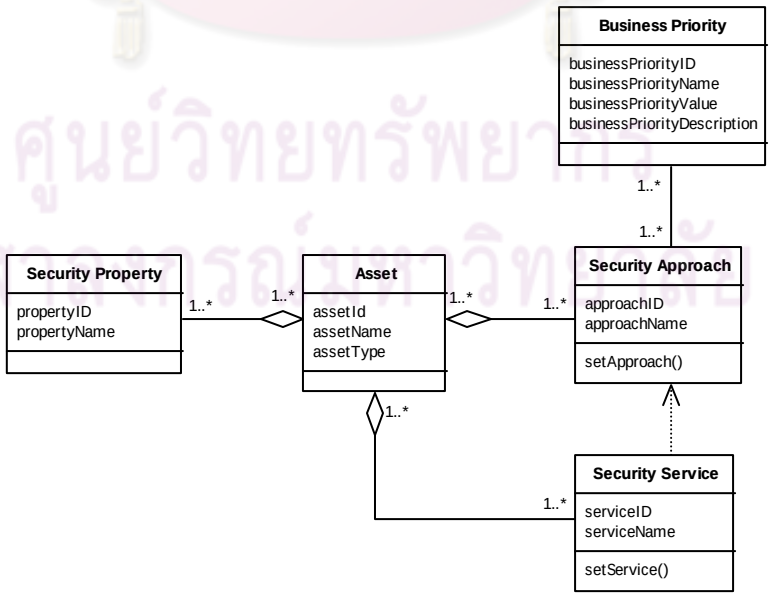
ตารางที่ ง.6 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปแนวคิดความมั่นคงองค์กร

ชื่อแบบรูป	แนวคิดความมั่นคงองค์กร
รหัสแบบรูป	P66
ชื่อกลุ่มของแบบรูป	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
เงื่อนไขก่อนการใช้	1. ชื่อสินทรัพย์ จาก GM61
คำอธิบาย	แบบรูปนี้จะช่วยเป็นตัวแนะนำในการเลือกแนวคิดความมั่นคง (Prevention : การป้องกัน, Detection : การตรวจหา และ Response : การตอบสนอง) ตามคุณสมบัติความมั่นคงที่เหมาะสม และระดับความเสี่ยงของสินทรัพย์ที่พิจารณา
ปัญหา	จะกำหนดแนวคิดความมั่นคงให้แก่สินทรัพย์ได้อย่างไร
ผลเฉลย	1. รวบรวมข้อมูลที่จำเป็น คือ ชนิดของสินทรัพย์ 2. รวบรวมข้อมูลค่าความเสี่ยงของสินทรัพย์ 3. เลือกแนวคิดความมั่นคงให้เหมาะสมกับสินทรัพย์
แผนภาพคลาส	



ตารางที่ ง.7 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปบริการความมั่นคงองค์กร

ชื่อแบบรูป	บริการความมั่นคงองค์กร
รหัสแบบรูป	P67
ชื่อกลุ่มของแบบรูป	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
เงื่อนไขก่อนการใช้	1. ชื่อสินทรัพย์ จาก GM61 (ในการพัฒนาจริงจะถูกผนวกรวมเข้ากับ GM66)
คำอธิบาย	แบบรูปนี้ต่อเนื่องจากแบบรูป GM66 โดยแบบรูปนี้เป็นการแนะนำในการเลือกตัวบริการความมั่นคงที่จะใช้ในการป้องกันสินทรัพย์ภายหลังที่ได้กำหนดแนวคิดความมั่นคงสำหรับสินทรัพย์ดังกล่าวแล้ว ตัวอย่างบริการด้านความมั่นคง เช่น การระบุและยืนยันตัวตน (GM71) การควบคุมการเข้าถึง (GM82) เป็นต้น
ปัญหา	จะกำหนดบริการความมั่นคงของสินทรัพย์ในองค์กรได้อย่างไร
ผลเฉลย	1. รวบรวมข้อมูลที่จำเป็น(ประเภทของสินทรัพย์, คุณสมบัติความมั่นคง , แนวคิดความมั่นคงองค์กร) 2. ระบุบริการความมั่นคงสำหรับสินทรัพย์และแนวคิดความมั่นคง 3. ทวนสอบบริการความมั่นคงอย่างสม่ำเสมอ เมื่อมีสถานการณ์เปลี่ยนแปลง
แผนภาพคลาส	

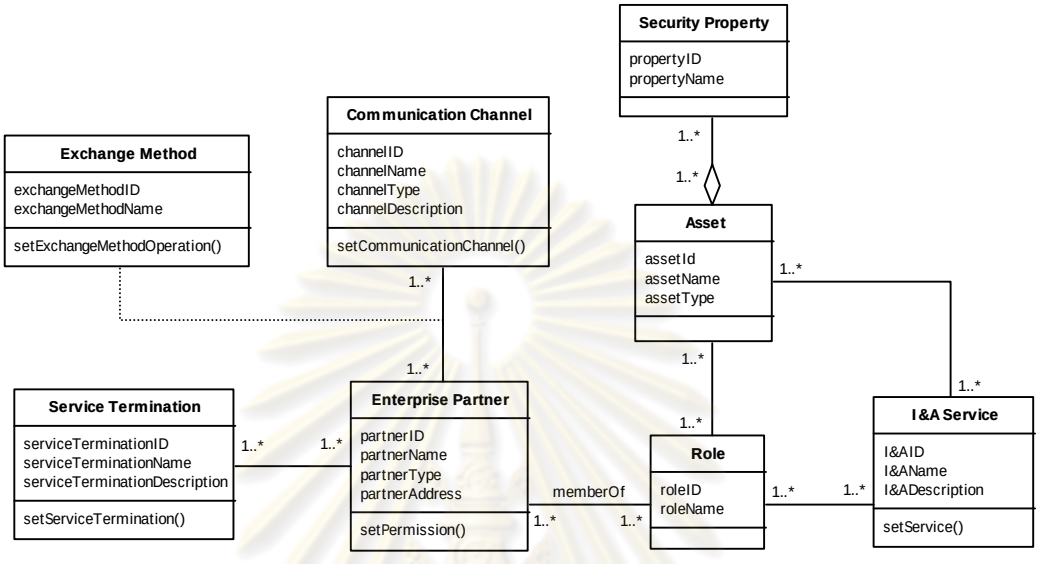


ตารางที่ ง.8 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปการสื่อสารของผู้มีหุ้นส่วนองค์กร

ชื่อแบบรูป	การสื่อสารของผู้มีหุ้นส่วนองค์กร
รหัสแบบรูป	P68
ชื่อกลุ่มของแบบรูป	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง
เงื่อนไขก่อนการใช้	1. ชื่อสินทรัพย์ จาก GM61 2. ชื่อบริการสำหรับระบุและยืนยันตัวตนจาก GM72
คำอธิบาย	เมื่อองค์กรมีการติดต่อกับองค์กรภายนอก จะต้องมีการเตรียมเครื่องมือและบริการต่างๆ ไว้อำนวยความสะดวกและควบคุมการติดต่อและการแลกเปลี่ยนข้อมูล แต่การดำเนินการดังกล่าวจะต้องเลือกบริการความมั่นคงที่เหมาะสม ในการจัดการสิทธิ์การเข้าถึง รวมถึงการป้องกันข้อมูลมิให้ถูกเข้าถึงโดยผู้ที่ไม่มีสิทธิ์
ปัญหา	เมื่อมีการติดต่อของหุ้นส่วนกับองค์กร จะปกป้องระบบและข้อมูลขององค์กรได้อย่างไร
ผลเฉลย	1. ระบุข้อมูล และapplication services ที่ต้องมีการแลกเปลี่ยนระหว่างองค์กร จากนั้นให้ระบุความต้องการความมั่นคงของข้อมูลดังกล่าว 2. กำหนดความมั่นคงด้านการตรวจสอบ การเข้าใช้งานของหุ้นส่วนโดยพิจารณาจากความต้องการความมั่นคงของข้อมูลและนโยบายขององค์กร 3. ระบุและป้องกันช่องทางการติดต่อ 1) ระบุช่องทางการติดต่อ 2) แยกช่องทางของหุ้นส่วนออกจากช่องทางหลัก 3) กำหนดการจัดการด้าน Port's และ Portals 4) กำหนดการจัดการด้านการควบคุมการเข้าถึง 4. กำหนดวิธีดำเนินการที่ใช้ในช่องทางการติดต่อ 5. กำหนดกิจกรรมการสิ้นสุดของหุ้นส่วน ตามข้อตกลงก่อนหน้า

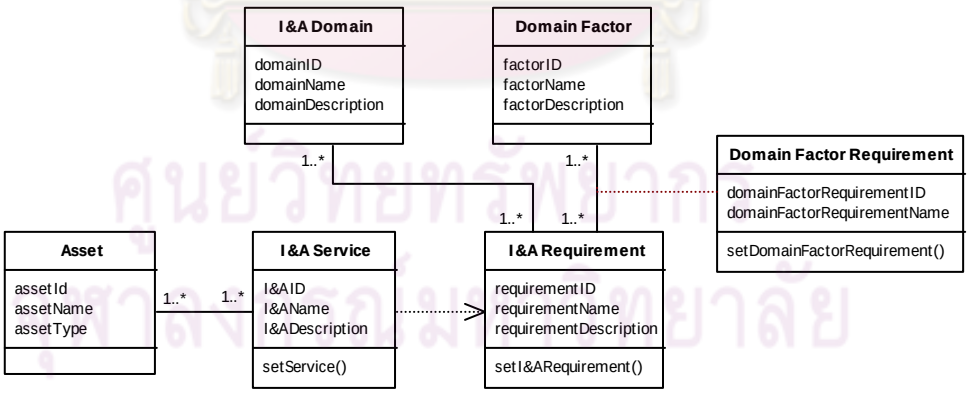
ตารางที่ ง.8 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปการสื่อสารของผู้มีหุ้นส่วนองค์กร (ต่อ)

แผนภาพคลาส



ตารางที่ ง.9 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปความต้องการการระบุและการพิสูจน์ตัวตน

ชื่อแบบรูป	ความต้องการการระบุและการพิสูจน์ตัวตน
รหัสแบบรูป	P71
ชื่อกลุ่มของแบบรูป	การระบุตัวตนและการพิสูจน์ตัวตน
เงื่อนไขก่อนการใช้	ไม่มี
คำอธิบาย	บริการด้านการระบุและพิสูจน์ตัวตนเป็นเซตของความต้องการสำหรับการบริการและคุณภาพของบริการ แบบรูปนี้นำเสนอและสร้างความต้องการพื้นฐานสำหรับการบริการด้านการระบุและพิสูจน์ตัวตน
ปัญหา	จะกำหนดความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตนได้อย่างไร
ผลเฉลย	1. ระบุขอบเขตในการใช้บริการการระบุและพิสูจน์ตัวตน 2. ระบุปัจจัยที่มีผลต่อการกำหนดความต้องการ 3. ระบุความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน ในแต่ละขอบเขต (แบบรูปได้กำหนดความต้องการเบื้องต้นไว้แล้ว) 4. ระบุความสัมพันธ์ระหว่างปัจจัยในข้อ 2 และความต้องการที่ระบุไว้ในข้อ 3 ที่สำคัญ
แผนภาพคลาส	

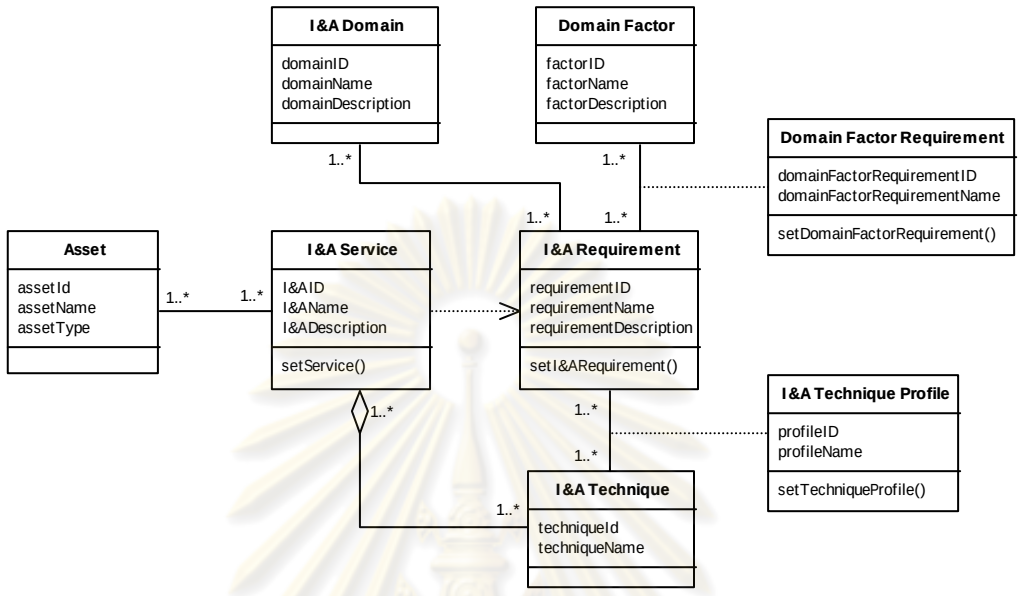


ตารางที่ ง.10 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปทางเลือกการออกแบบสำหรับการระบุตัวตนและการพิสูจน์ตัวตนอัตโนมัติ

ชื่อแบบรูป	ทางเลือกการออกแบบสำหรับการระบุตัวตนและการพิสูจน์ตัวตนอัตโนมัติ
รหัสแบบรูป	P72
ชื่อกลุ่มของแบบรูป	การระบุตัวตนและการพิสูจน์ตัวตน
เงื่อนไขก่อนการใช้	1. ชื่อตัวบริการที่กำหนดไว้แล้ว จาก GM71
คำอธิบาย	เป็นแบบรูปที่ช่วยในการกำหนดเทคนิคที่จะใช้กับบริการการระบุและพิสูจน์ตัวตนเพื่อช่วยเลือกกลยุทธ์ที่เหมาะสม ให้สอดคล้องกับความต้องการด้านการระบุและพิสูจน์ตัวตน
ปัญหา	จะเลือกใช้เทคนิคการระบุ และพิสูจน์ตัวตนให้เหมาะสมกับความต้องการจากแบบรูป 7.1 ได้อย่างไร
ผลเฉลย	1. รวบรวมข้อมูลที่จำเป็น ประกอบด้วย - ขอบเขตในการใช้บริการ - ความต้องการของการใช้บริการ - บริการการระบุและพิสูจน์ตัวตน 2. ระบุเทคนิคในการระบุ และพิสูจน์ตัวตน โดยพิจารณาถึงบริการการระบุและพิสูจน์ตัวตน 3. ระบุความเหมาะสมของแต่ละเทคนิคสำหรับความต้องการใช้บริการ 4. เปรียบเทียบในแต่ละเทคนิคที่เหมาะสมกับความต้องการ 5. ในแต่ละความต้องการ หากใช้เทคนิคเดียวไม่เพียงพอ สามารถใช้เทคนิคอื่นเข้ามาช่วยได้

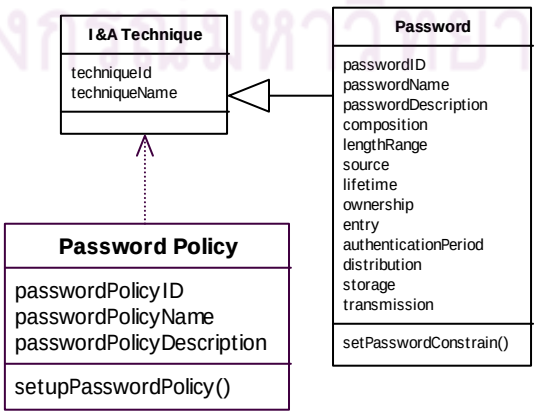
ตารางที่ ง.10 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปทางเลือกการออกแบบสำหรับการระบุตัวตนและการพิสูจน์ตัวตนอัตโนมัติ (ต่อ)

แผนภาพคลาส



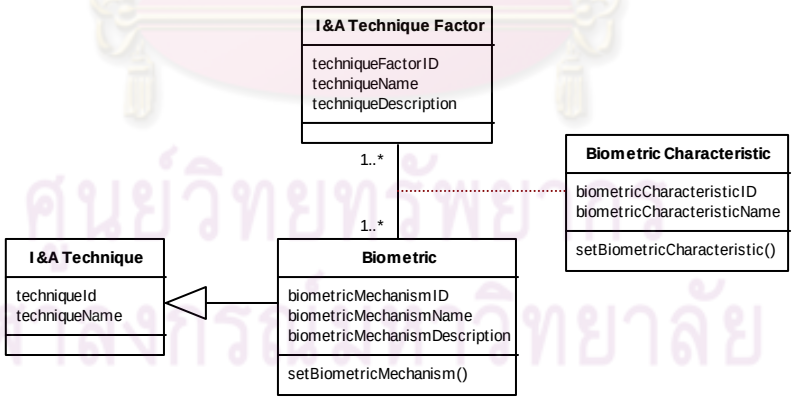
ตารางที่ ง.11 คำอธิบายแบบรูปและ แผนภาพเชิงโครงสร้างของแบบรูปการออกแบบและใช้รหัสผ่าน

ชื่อแบบรูป	การออกแบบและใช้รหัสผ่าน
รหัสแบบรูป	P73
ชื่อกลุ่มของแบบรูป	การระบุตัวตนและการพิสูจน์ตัวตน
เงื่อนไขก่อนการใช้	1. ชื่อตัวบริการที่กำหนดไว้แล้ว จาก GM71 2. ชื่อบริการที่ได้จากข้อ 1 จะต้องใช้ I&A Technique เป็น “Identifier and Password” ที่ถูกกำหนดโดย GM72
คำอธิบาย	แบบรูปนี้ใช้ในการออกแบบ การสร้าง และการจัดการการใช้รหัสผ่านสำหรับการบริการการระบุและพิสูจน์ตัวตน
ปัญหา	ทำอย่างไรจึงจะสร้าง จัดการ และใช้งานรหัสผ่านได้อย่างปลอดภัย
ผลเฉลย	1. กำหนดตัวอักษรที่จะใช้ในรหัสผ่าน 2. กำหนดความยาวของรหัสผ่าน 3. กำหนดที่มาของรหัสผ่าน 4. กำหนดอายุการใช้งานของรหัสผ่าน 5. กำหนดบุคคลที่มีสิทธิ์ในการใช้งานรหัสผ่าน 6. กำหนดวิธีการในการกรอกรหัสผ่าน 7. กำหนดระยะเวลาของการพิสูจน์ตัวตนโดยใช้รหัสผ่าน 8. กำหนดวิธีการในการส่งรหัสผ่านให้ผู้ใช้งาน 9. กำหนดวิธีการในการจัดเก็บรหัสผ่าน 10. กำหนดวิธีการในการถ่ายโอนรหัสผ่าน เพื่อใช้ในการตรวจสอบ
แผนภาพคลาส	



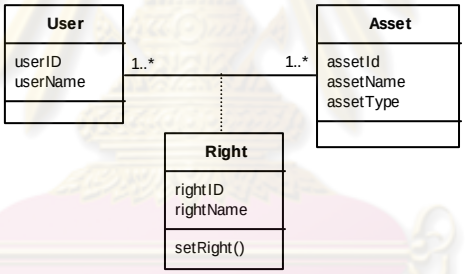
ตารางที่ ง.12 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปทางเลือกการออกแบบชีวมิติ

ชื่อแบบรูป	ทางเลือกการออกแบบชีวมิติ
รหัสแบบรูป	P74
ชื่อกลุ่มของแบบรูป	การระบุตัวตนและการพิสูจน์ตัวตน
เงื่อนไขก่อนการใช้	1. ชื่อตัวบริการที่กำหนดไว้แล้ว จาก GM71 2. ชื่อบริการที่ได้จากข้อ 1 จะต้องใช้ I&A Technique เป็น “Biometric” ที่ถูกกำหนดโดย GM72
คำอธิบาย	แบบรูปนี้ใช้ในการออกแบบ การสร้าง และการจัดการการใช้รหัสผ่านสำหรับการบริการการระบุและพิสูจน์ตัวตนโดยใช้วิธีการทางด้านชีวมิติ
ปัญหา	ทำอย่างไรจึงจะสามารถเลือกใช้ชีวมิติได้อย่างเหมาะสมกับความต้องการในการระบุและพิสูจน์ตัวตน
ผลเฉลย	1. ทบทวนการออกแบบทางชีวมิติที่เป็นไปได้ทั้งหมดตามแต่ปัจจัย (ความง่ายในการใช้งาน, ความปลอดภัย, ความสะดวก รวดเร็ว, ฯลฯ) 2. เลือกการออกแบบทางชีวมิติที่เหมาะสม (Face recognition, Finger image, Iris scan, ฯลฯ)
แผนภาพคลาส	



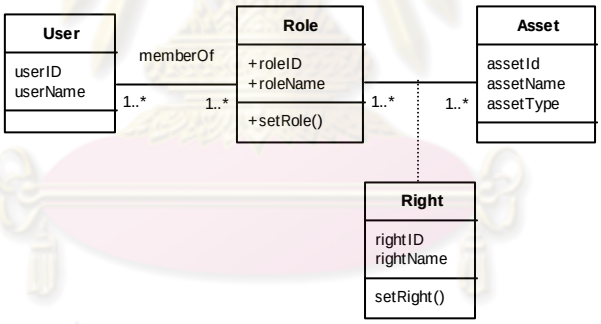
ตารางที่ ง.13 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปการให้อำนาจ

ชื่อแบบรูป	การให้อำนาจ
รหัสแบบรูป	P81
ชื่อกลุ่มของแบบรูป	การควบคุมการเข้าถึง
เงื่อนไขก่อนการใช้	1. ข้อมูลสินทรัพย์จาก GM61
คำอธิบาย	แบบรูปนี้ช่วยในการกำหนดว่า ใครบ้างมิสิทธิ์ที่จะเข้าถึงทรัพยากรของระบบ ในสภาพแวดล้อมที่มีการควบคุมการเข้าถึง เพื่อแสดงให้เห็นว่าทรัพยากรใดถูกเข้าถึงและเข้าถึงได้อย่างไร
ปัญหา	จะอธิบายว่า active entity สามารถเข้าใช้ทรัพยากรได้อย่างไร
ผลเฉลย	1. ระบุ active entity ที่เข้าใช้ทรัพยากร 2. ระบุทรัพยากรที่ถูกควบคุมการเข้าถึง 3. ระบุ entity ที่ควบคุมการเข้าใช้ทรัพยากร
แผนภาพคลาส	



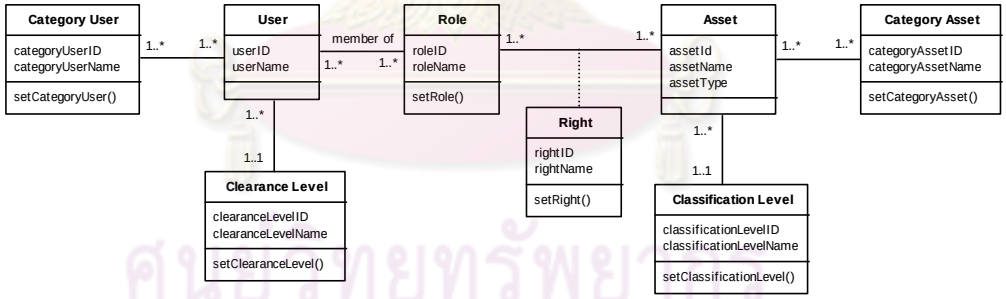
ตารางที่ ง.14 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปการควบคุมการเข้าถึงเชิงบทบาท

ชื่อแบบรูป	การควบคุมการเข้าถึงเชิงบทบาท
รหัสแบบรูป	P82
ชื่อกลุ่มของแบบรูป	การควบคุมการเข้าถึง
เงื่อนไขก่อนการใช้	1. ข้อมูลสินทรัพย์จาก GM61 คำแนะนำ : ไวยากรณ์นี้เป็นส่วนขยายของ GM81
คำอธิบาย	แบบรูปนี้ใช้ในการกำหนดสิทธิ์บนพื้นฐานของบทบาทที่บุคคลได้รับ เพื่อใช้ในการควบคุมการเข้าถึง ซึ่งเพิ่มจาก GM81 โดยมีการนำเสนอกลุ่มบุคคล ประเภทข้อมูลและการดำเนินการที่บุคคลสามารถทำได้กับทรัพยากรที่ต้องการเข้าถึง
ปัญหา	จะกำหนดสิทธิจากหน้าที่ของบุคคลได้อย่างไร
ผลเฉลย	กำหนดบทบาทของผู้ใช้งาน โดยพิจารณาจากหน้าที่การทำงาน
แผนภาพคลาส	



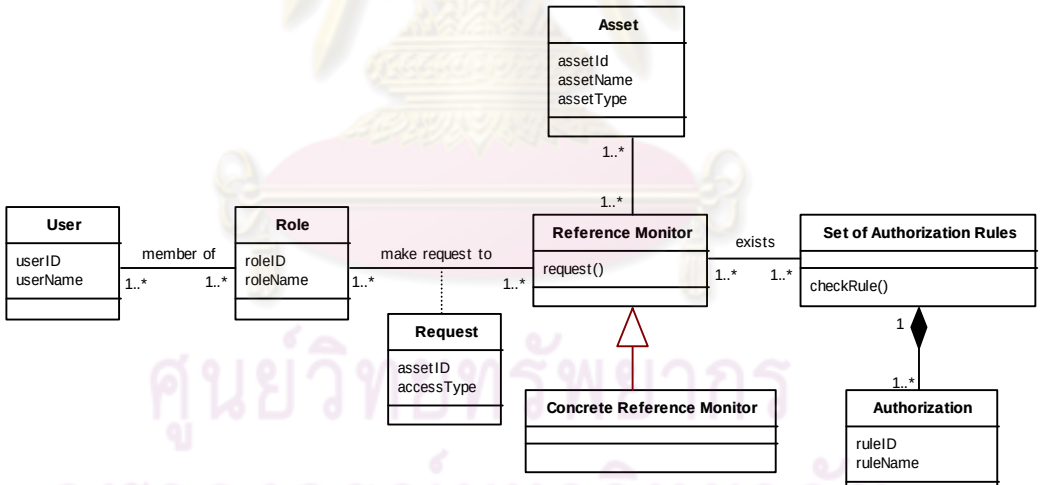
ตารางที่ ง.15 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปความมั่นคงหลายระดับ

ชื่อแบบรูป	ความมั่นคงหลายระดับ
รหัสแบบรูป	P83
ชื่อกลุ่มของแบบรูป	การควบคุมการเข้าถึง
เงื่อนไขก่อนการใช้	1. ข้อมูลสินทรัพย์จาก GM61
คำอธิบาย	ในบางกรณีที่ข้อมูลหรือเอกสารมีระดับความสำคัญที่แตกต่างกันออกไป แบบรูปนี้จะช่วยในการกำหนดระดับหรือกลุ่มของทรัพยากร และกำหนดระดับสิทธิ์ให้กับผู้ใช้ที่เข้ามาติดต่อทรัพยากรดังกล่าว เพื่อใช้ในการตรวจสอบการเข้าถึงว่าผู้ใช้มีระดับสิทธิ์มากพอที่จะเข้าถึงทรัพยากรดังกล่าวหรือไม่
ปัญหา	จะควบคุมการเข้าถึงของข้อมูลที่มีความสำคัญได้อย่างไร โดยยึดจากตำแหน่งในองค์กรและสามารถเพิ่มหรือลดสิทธิของผู้ใช้งานได้
ผลเฉลย	1. จัดเป็นหมวดหมู่ของผู้ใช้งานตามหน้าที่การทำงาน 2. จัดแบ่งหมวดหมู่ของเอกสารและข้อมูลตามระดับความสำคัญ เช่น ลับที่สุด, ลับ, เปิดเผย เป็นต้น
แผนภาพคลาส	



ตารางที่ ง.16 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปการตรวจสอบการเข้าถึงทรัพยากร

ชื่อแบบรูป	การตรวจสอบการเข้าถึงทรัพยากร
รหัสแบบรูป	P84
ชื่อกลุ่มของแบบรูป	การควบคุมการเข้าถึง
เงื่อนไขก่อนการใช้	1. ข้อมูลการดำเนินงาน (Task) สำหรับบทบาทจาก GM85
คำอธิบาย	แบบรูปนี้ใช้ในการกำหนดข้อบังคับในการใช้งานทรัพยากรเป้าหมาย ว่าคำร้องขอเข้าใช้ทรัพยากรนั้นสามารถทำได้หรือไม่ โดยการตรวจสอบกับเซตของบทบาทที่ได้รับอนุญาต และสิทธิ์สำหรับบทบาทดังกล่าว
ปัญหา	ทำอย่างไรจึงจะควบคุมคำร้องของผู้ใช้งานหรือ process ในทุกๆ ระดับของระบบ
ผลเฉลย	กำหนด abstract process ที่ควบคุมและตรวจสอบคำร้องขอใช้ทรัพยากร
แผนภาพคลาส	

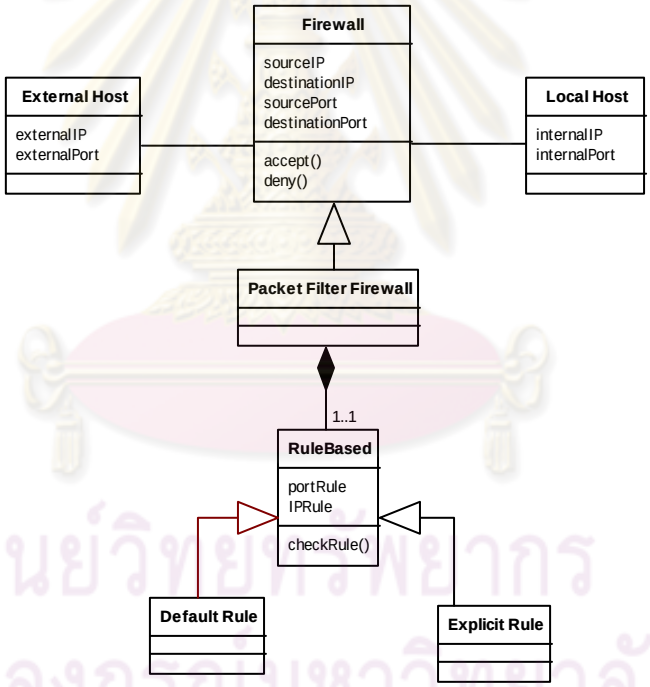


ตารางที่ ง.17 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปการตรวจสอบการเข้าถึงทรัพยากร

ชื่อแบบรูป	การกำหนดสิทธิ์ให้กับบทบาท
รหัสแบบรูป	P85
ชื่อกลุ่มของแบบรูป	การควบคุมการเข้าถึง
เงื่อนไขก่อนการใช้	ไม่มี
คำอธิบาย	แบบรูปนี้สนับสนุนแนวคิดการให้สิทธิ์ต่ำสุด เป็นหลักการพื้นฐานสำหรับระบบความมั่นคง แต่จะต้องมีการกำหนดสิทธ์ให้กับบทบาท เพื่อให้ทราบว่าบทบาทนี้มีสิทธิ์ในการดำเนินการอะไรกับทรัพยากรใดได้บ้าง
ปัญหา	เราจะกำหนดสิทธิให้กับบทบาทได้อย่างไร โดยคำนึงถึงสิทธิขั้นพื้นฐานของแต่ละบทบาท
ผลเฉลย	1. สร้างยูสเคสโดย actor จะถูกแทนที่ด้วยบทบาท 2. สร้าง sequence diagram สำหรับในแต่ละ use case 3. วิเคราะห์ sequence diagram เพื่อหา operation ในการกำหนดสิทธิ 4. หาข้อยกเว้นใน use case diagram เพื่อหาการกระทำที่ละเมิดความมั่นคง 5. การเพิ่มหรือลบกฎการให้อำนาจจะกระทำเมื่อเพิ่ม ลบ หรือมีการเปลี่ยนแปลง use case
แผนภาพคลาส	
ไม่มีแผนภาพคลาสสำหรับแบบรูปความมั่นคงนี้ เนื่องจากผลเฉลยภายในแบบรูปความมั่นคงนี้นำเสนอถึงขั้นตอนวิธีในการกำหนดสิทธิ์ให้กับบทบาท สำหรับแผนภาพคลาสที่ได้สร้างขึ้นจากวิธีการการกำหนดสิทธิ์ให้กับบทบาทนี้ คือแผนภาพคลาสในแบบรูปการควบคุมการเข้าถึงเชิงบทบาท (P82)	

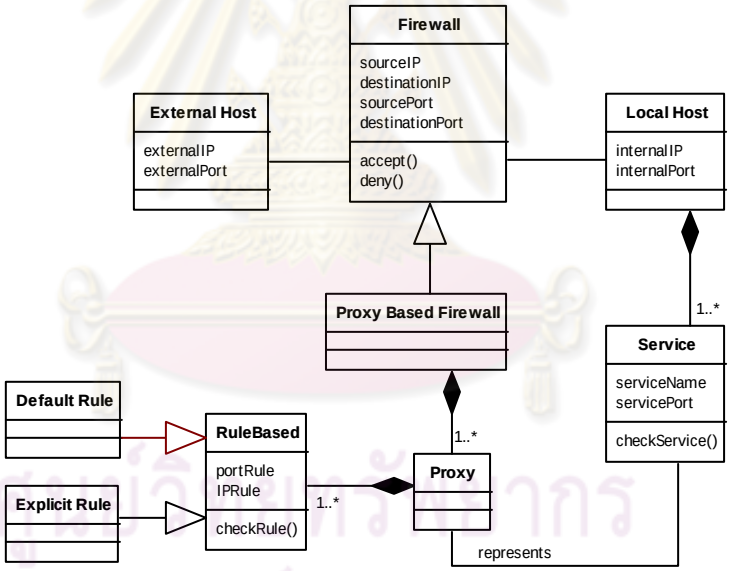
ตารางที่ ง.18 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปไฟล์วอลล์กรองแพ็คเกจ

ชื่อแบบรูป	ไฟล์วอลล์กรองแพ็คเกจ
ชื่อกลุ่มของแบบรูป	สถาปัตยกรรมไฟล์วอลล์
เงื่อนไขก่อนการใช้	ไม่มี
คำอธิบาย	ไวยากรณ์นี้ใช้ในการระบุโฮสต์ (Host) เพื่อทำการปิดกั้นหรืออนุญาตให้ผ่านไฟล์วอลล์ในระดับไอพี (IP Level)
ปัญหา	ทำอย่างไรจะระบุ และป้องกันการเข้าถึงจาก external host ในระดับ network layer
ผลเฉลย	กำหนด packet filter firewall ที่ควบคุมข้อมูลเข้าออกของเครือข่าย โดยมีการกำหนดกฎในการควบคุมข้อมูล
แผนภาพคลาส	



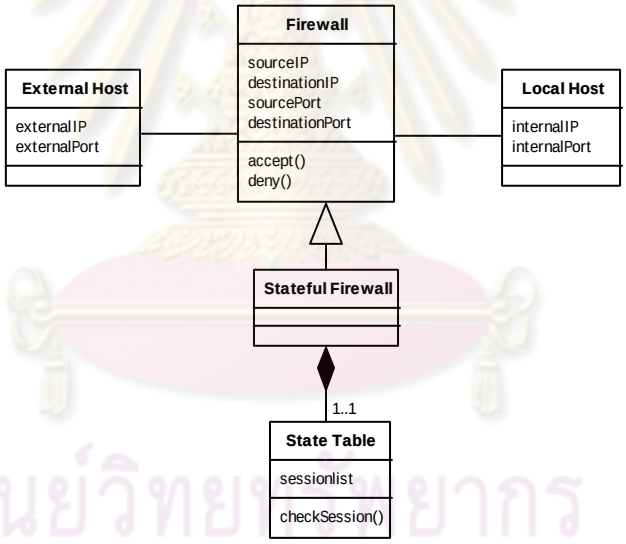
ตารางที่ ง.19 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปไฟล์วอลล์เชิงตัวแทน

ชื่อแบบรูป	ไฟล์วอลล์เชิงตัวแทน
ชื่อกลุ่มของแบบรูป	สถาปัตยกรรมไฟล์วอลล์
เงื่อนไขก่อนการใช้	ไม่มี
คำอธิบาย	ไวยากรณ์นี้ใช้ในการระบุโฮสต์ เพื่อทำการปิดกั้นหรืออนุญาตให้ผ่านไฟล์วอลล์ในระดับไอพี โดยพิจารณาชื่อบริการ (Service Name) และ พอร์ต (Port)โดยมีตรวจสอบร่วมกับกฎที่ถูกกำหนดไว้
ปัญหา	ทำอย่างไรจะระบุ และป้องกันการเข้าถึงจาก external host ในระดับ application layer
ผลเฉลย	กำหนด proxy firewall ที่ควบคุมคำร้องขอไปยังโปรแกรมประยุกต์ โดยมีการกำหนดกฎในการควบคุมคำร้องไปยังโปรแกรมประยุกต์
แผนภาพคลาส	



ตารางที่ ง.20 คำอธิบายแบบรูปและแผนภาพเชิงโครงสร้างของแบบรูปไฟล์วอลล์เชิงสถานะ

ชื่อแบบรูป	ไฟล์วอลล์เชิงสถานะ
ชื่อกลุ่มของแบบรูป	สถาปัตยกรรมไฟล์วอลล์
เงื่อนไขก่อนการใช้	ไม่มี
คำอธิบาย	ไวยากรณ์นี้ใช้ในการระบุโฮสต์ เพื่อทำการปิดกั้นหรืออนุญาตให้ผ่านไฟล์วอลล์ในระดับไอพี โดยพิจารณาชื่อบริการและ พอร์ต โดยมีตรวจสอบสถานะของการเข้าถึงและกฎที่กำหนดไว้ในไฟล์วอลล์
ปัญหา	ทำอย่างไรจึงจะเพิ่มประสิทธิภาพของการใช้ firewall ในการกรอก packet
ผลเฉลย	กำหนดตารางที่เก็บสถานะของการเชื่อมต่อของ packet เพื่อลดการตรวจสอบการเชื่อมต่อ
แผนภาพคลาส	



ภาคผนวก จ

ตารางรายละเอียดโครงสร้างคลาส

ตารางรายละเอียดโครงสร้างคลาสมีทั้งหมด 20 ตาราง โดยผู้วิจัยจะเรียงลำดับตามแผนภาพคลาสของแบบรูปความมั่นคง โดยตารางโครงสร้างคลาสมีรายละเอียดดังนี้

ตารางที่ จ.1 รายละเอียดโครงสร้างคลาสของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร

แบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร	
คลาส Asset	
ลักษณะประจำ	**คำอธิบาย**
assetId	รหัสสินทรัพย์
assetName	ชื่อสินทรัพย์
assetType	รหัสประเภทสินทรัพย์
คลาส Business Driver	
ลักษณะประจำ	**คำอธิบาย**
driverID	รหัสตัวขับเคลื่อนทางธุรกิจ
driverName	ชื่อตัวขับเคลื่อนทางธุรกิจ
driverDescription	คำอธิบายตัวขับเคลื่อนทางธุรกิจ
การดำเนินการ	**คำอธิบาย**
setBusinessDriver	การกำหนดค่าตัวขับเคลื่อนทางธุรกิจ
คลาส Security Property	
ลักษณะประจำ	**คำอธิบาย**
propertyID	รหัสคุณสมบัติความมั่นคง
propertyName	ชื่อคุณสมบัติความมั่นคง
คลาส Asset-Security Property	
ลักษณะประจำ	**คำอธิบาย**
asssetID	รหัสสินทรัพย์
propertyID	รหัสคุณสมบัติความมั่นคง

ตารางที่ จ.2 รายละเอียดโครงสร้างคลาสของแบบรูปการกำหนดมูลค่าสินทรัพย์

แบบรูปการกำหนดมูลค่าสินทรัพย์	
คลาส Asset	
ลักษณะประจำ	**คำอธิบาย**
assetId	รหัสสินทรัพย์
assetName	ชื่อสินทรัพย์
assetType	รหัสประเภทสินทรัพย์
คลาส Asset Value	
ลักษณะประจำ	**คำอธิบาย**
FVValue	มูลค่าของสินทรัพย์ในด้านการเงิน
SRValue	มูลค่าของสินทรัพย์ในด้านความมั่นคง
BIValue	มูลค่าของสินทรัพย์ในด้านธุรกิจ
OverallValue	มูลค่าเฉลี่ยรวมของสินทรัพย์
การดำเนินการ	**คำอธิบาย**
calculateAssetValue	การกำหนดค่าตัวขับเคลื่อนทางธุรกิจ
setAssetValue	การกำหนดมูลค่าสินทรัพย์
คลาส Value Scale	
ลักษณะประจำ	**คำอธิบาย**
valueScaleID	รหัสมูลค่าสินทรัพย์
valueScaleName	ชื่อมูลค่าสินทรัพย์
valueScaleNumber	ตัวเลขแสดงมูลค่าสินทรัพย์
FVDescription	คำอธิบายมูลค่าสินทรัพย์ในด้านการเงิน
SRDescription	คำอธิบายมูลค่าสินทรัพย์ในด้านความมั่นคง
BIDescriptipn	คำอธิบายมูลค่าสินทรัพย์ในด้านธุรกิจ
OverallDescription	คำอธิบายมูลค่าเฉลี่ยรวมของสินทรัพย์

ตารางที่ จ.3 รายละเอียดโครงสร้างคลาสของแบบรูปการประเมินภัยคุกคาม

แบบรูปการประเมินภัยคุกคาม	
คลาส Asset	
ลักษณะประจำ	**คำอธิบาย**
assetId	รหัสสินทรัพย์
assetName	ชื่อสินทรัพย์
assetType	รหัสประเภทสินทรัพย์
คลาส Threat	
ลักษณะประจำ	**คำอธิบาย**
threatID	รหัสภัยคุกคาม
threatAction	ชื่อภัยคุกคาม
threatConsequence	ผลกระทบจากภัยคุกคาม
การดำเนินการ	**คำอธิบาย**
setThreat	การกำหนดภัยคุกคาม
คลาส Threat Source	
ลักษณะประจำ	**คำอธิบาย**
threatSourceID	รหัสแหล่งที่มาของภัยคุกคาม
threatSourceName	ชื่อแหล่งที่มาของภัยคุกคาม
คลาส Threat-Threat Source	
ลักษณะประจำ	**คำอธิบาย**
threatID	รหัสภัยคุกคาม
threatSourceID	รหัสแหล่งที่มาของภัยคุกคาม
คลาส Threat Likelihood	
ลักษณะประจำ	**คำอธิบาย**
threatLikelihoodID	รหัสความถี่ของภัยคุกคาม
threatLikelihoodName	ชื่อความถี่ของภัยคุกคาม
threatLikelihoodValue	ค่าตัวเลขความถี่ของภัยคุกคาม
threatLikelihoodDescription	คำอธิบายความถี่ของภัยคุกคาม

ตารางที่ จ.4 รายละเอียดโครงสร้างคลาสของแบบรูปการประเมินภาวะเสี่ยง

แบบรูปการประเมินภาวะเสี่ยง	
คลาส Asset	
ลักษณะประจำ	**คำอธิบาย**
assetId	รหัสสินทรัพย์
assetName	ชื่อสินทรัพย์
assetType	รูปแบบสินทรัพย์
คลาส Threat	
ลักษณะประจำ	**คำอธิบาย**
threatID	รหัสภัยคุกคาม
threatAction	ชื่อภัยคุกคาม
threatConsequence	ผลจากภัยคุกคาม
การดำเนินการ	**คำอธิบาย**
setThreat	การกำหนดภัยคุกคาม
คลาส Vulnerability	
ลักษณะประจำ	**คำอธิบาย**
vulnerabilityID	รหัสจุดอ่อน
vulnerabilityName	ชื่อจุดอ่อน
การดำเนินการ	**คำอธิบาย**
setVulnerability	การกำหนดจุดอ่อน
คลาส Severity Scale	
ลักษณะประจำ	**คำอธิบาย**
severityScaleID	รหัสระดับความรุนแรงของจุดอ่อน
severityScaleName	ชื่อระดับความรุนแรงของจุดอ่อน
severityScaleNumber	เลขระดับความรุนแรงของจุดอ่อน
severityScaleDescription	คำอธิบายระดับความรุนแรงของจุดอ่อน

ตารางที่ จ.5 รายละเอียดโครงสร้างคลาสของแบบรูปการกำหนดค่าความเสี่ยง

แบบรูปการกำหนดค่าความเสี่ยง	
คลาส Asset	
ลักษณะประจำ	**คำอธิบาย**
assetId	รหัสสินทรัพย์
assetName	ชื่อสินทรัพย์
assetType	รูปแบบสินทรัพย์
คลาส Asset Value	
ลักษณะประจำ	**คำอธิบาย**
FVValue	มูลค่าของสินทรัพย์ในด้านการเงิน
SRValue	มูลค่าของสินทรัพย์ในด้านความมั่นคง
BIValue	มูลค่าของสินทรัพย์ในด้านธุรกิจ
OverallValue	มูลค่าเฉลี่ยรวมของสินทรัพย์
การดำเนินการ	**คำอธิบาย**
calculateAssetValue	ค่าตัวเลขการคำนวนสินทรัพย์
setAssetValue	ค่าตัวเลขการกำหนดสินทรัพย์
คลาส Value Scale	
ลักษณะประจำ	**คำอธิบาย**
valueScaleID	รหัสมูลค่าสินทรัพย์
valueScaleName	ชื่อมูลค่าสินทรัพย์
valueScaleNumber	ตัวเลขแสดงมูลค่าสินทรัพย์
FVDescription	คำอธิบายมูลค่าสินทรัพย์ในด้านการเงิน
SRDescription	คำอธิบายมูลค่าสินทรัพย์ในด้านความมั่นคง
BIDescription	คำอธิบายมูลค่าสินทรัพย์ในด้านธุรกิจ
OverallDescription	คำอธิบายมูลค่าเฉลี่ยรวมของสินทรัพย์

ตารางที่ จ.5 รายละเอียดโครงสร้างคลาสของแบบรูปการกำหนดค่าความเสี่ยง (ต่อ)

แบบรูปการกำหนดค่าความเสี่ยง	
คลาส Threat	
ลักษณะประจำ	**คำอธิบาย**
threatID	รหัสภัยคุกคาม
threatAction	ชื่อภัยคุกคาม
threatConsequence	ผลจากภัยคุกคาม
การดำเนินการ	**คำอธิบาย**
setThreat	การกำหนดภัยคุกคาม
คลาส threat Likelihood	
ลักษณะประจำ	**คำอธิบาย**
threatLikelihoodID	รหัสความถี่ของภัยคุกคาม
threatLikelihoodName	ชื่อความถี่ของภัยคุกคาม
threatLikelihoodValue	ค่าตัวเลขความถี่ของภัยคุกคาม
threatLikelihoodDescription	คำอธิบายความถี่ของภัยคุกคาม
คลาส Threat-Threat Source	
ลักษณะประจำ	**คำอธิบาย**
threatID	รหัสภัยคุกคาม
threatSourceID	รหัสแหล่งที่มาของภัยคุกคาม
คลาส Vulnerability	
ลักษณะประจำ	**คำอธิบาย**
vulnerabilityID	รหัสจุดอ่อน
vulnerabilityName	ชื่อจุดอ่อน
การดำเนินการ	**คำอธิบาย**
setVulnerability	การกำหนดจุดอ่อน
คลาส Severity Scale	
ลักษณะประจำ	**คำอธิบาย**
severityScaleID	รหัสระดับความรุนแรงของจุดอ่อน
severityScaleName	ชื่อระดับความรุนแรงของจุดอ่อน
severityScaleNumber	เลขระดับความรุนแรงของจุดอ่อน

ตารางที่ จ.5 รายละเอียดโครงสร้างคลาสของแบบรูปการกำหนดค่าความเสี่ยง (ต่อ)

แบบรูปการกำหนดค่าความเสี่ยง	
คลาส Risk	
ลักษณะประจำ	**คำอธิบาย**
assetRiskValueID	รหัสค่าความเสี่ยง
การดำเนินการ	**คำอธิบาย**
calculateRiskValue	การคำนวณค่าความเสี่ยง
คลาส Risk Scale	
ลักษณะประจำ	**คำอธิบาย**
riskScaleID	รหัสค่าความเสี่ยง
riskScaleName	ชื่อค่าความเสี่ยง
riskScaleRange	ขอบเขตค่าความเสี่ยง
riskScaleDescription	คำอธิบายค่าความเสี่ยง

ตารางที่ จ.6 รายละเอียดโครงสร้างคลาสของแบบรูปแนวคิดความมั่นคงองค์กร

แบบรูปแนวคิดความมั่นคงองค์กร	
คลาส Asset	
ลักษณะประจำ	**คำอธิบาย**
assetId	รหัสสินทรัพย์
assetName	ชื่อสินทรัพย์
assetType	รูปแบบสินทรัพย์
คลาส Business Priority	
ลักษณะประจำ	**คำอธิบาย**
businessPriorityID	รหัสลำดับความสำคัญของแนวคิดต่อองค์กร
businessPriorityName	ชื่อลำดับความสำคัญของแนวคิดต่อองค์กร
businessPriorityValue	ค่าลำดับความสำคัญของแนวคิดต่อองค์กร
businessPriorityDescription	คำอธิบายลำดับความสำคัญของแนวคิดต่อองค์กร
คลาส Risk	
ลักษณะประจำ	**คำอธิบาย**
assetRiskValueID	รหัสค่าความเสี่ยง
การดำเนินการ	**คำอธิบาย**
calculateRiskValueID	การคำนวณค่าความเสี่ยง
คลาส Security Approach	
ลักษณะประจำ	**คำอธิบาย**
approachID	รหัสแนวคิดความมั่นคง
approachName	ชื่อแนวคิดความมั่นคง
การดำเนินการ	**คำอธิบาย**
setApproach	การกำหนดแนวคิดความมั่นคง
คลาส Security Property	
ลักษณะประจำ	**คำอธิบาย**
propertyID	รหัสคุณสมบัติความมั่นคง
propertyName	ชื่อคุณสมบัติความมั่นคง

ตารางที่ จ.7 รายละเอียดโครงสร้างคลาสของแบบรูปบริการความมั่นคงองค์กร

แบบรูปบริการความมั่นคงองค์กร	
คลาส Asset	
ลักษณะประจำ	**คำอธิบาย**
assetId	รหัสสินทรัพย์
assetName	ชื่อสินทรัพย์
assetType	รูปแบบสินทรัพย์
คลาส Business Priority	
ลักษณะประจำ	**คำอธิบาย**
businessPriorityID	รหัสลำดับความสำคัญของแนวคิดต่อองค์กร
businessPriorityName	ชื่อลำดับความสำคัญของแนวคิดต่อองค์กร
businessPriorityValue	ค่าลำดับความสำคัญของแนวคิดต่อองค์กร
businessPriorityDescription	คำอธิบายลำดับความสำคัญของแนวคิดต่อองค์กร
คลาส Security Approach	
ลักษณะประจำ	**คำอธิบาย**
approachID	รหัสแนวคิดความมั่นคง
approachName	ชื่อแนวคิดความมั่นคง
การดำเนินการ	**คำอธิบาย**
setApproach	การกำหนดแนวคิดความมั่นคง
คลาส Security Property	
ลักษณะประจำ	**คำอธิบาย**
propertyID	รหัสคุณสมบัติความมั่นคง
propertyName	ชื่อคุณสมบัติความมั่นคง
คลาส Security Service	
ลักษณะประจำ	**คำอธิบาย**
serviceID	การบริการความมั่นคง
serviceName	ชื่อการบริการความมั่นคง
การดำเนินการ	**คำอธิบาย**
setService	การกำหนดบริการความมั่นคง

ตารางที่ จ.8 รายละเอียดโครงสร้างคลาสของแบบรูปการสื่อสารของผู้มีหุ้นส่วนองค์กร

แบบรูปการสื่อสารของผู้มีหุ้นส่วนองค์กร	
คลาส Asset	
ลักษณะประจำ	**คำอธิบาย**
assetId	รหัสสินทรัพย์
assetName	ชื่อสินทรัพย์
assetType	รูปแบบสินทรัพย์
คลาส Communication Channel	
ลักษณะประจำ	**คำอธิบาย**
channelID	รหัสช่องทางการติดต่อ
channelName	ชื่อช่องทางการติดต่อ
channelType	ประเภทช่องทางการติดต่อ
channelDescription	คำอธิบายช่องทางการติดต่อ
การดำเนินการ	**คำอธิบาย**
setCommunicationChannel	การกำหนดช่องทางการติดต่อ
คลาส Enterprise Partner	
ลักษณะประจำ	**คำอธิบาย**
partnerID	รหัสหุ้นส่วนขององค์กร
partnerName	ชื่อหุ้นส่วนองค์กร
partnerType	รูปแบบหุ้นส่วนองค์กร
partnerAddress	ที่อยู่หุ้นส่วนองค์กร
การดำเนินการ	**คำอธิบาย**
setPermission	การกำหนดสิทธิ์ให้แก่หุ้นส่วนขององค์กร
คลาส Exchange Method	
ลักษณะประจำ	**คำอธิบาย**
exchangeMethodID	รหัสวิธีดำเนินการที่ใช้ในช่องทางการติดต่อ
exchangeMethodName	ชื่อวิธีการดำเนินการที่ใช้ในช่องทางการติดต่อ
การดำเนินการ	**คำอธิบาย**
setExchangeMethodOperation	การกำหนดวิธีดำเนินการที่ใช้ในช่องทางการติดต่อ

ตารางที่ จ.8 รายละเอียดโครงสร้างคลาสของแบบรูปการสื่อสารของผู้มีหุ้นส่วนองค์กร (ต่อ)

แบบรูปการสื่อสารของผู้มีหุ้นส่วนองค์กร	
คลาส I&A Service	
ลักษณะประจำ	**คำอธิบาย**
I&AID	รหัสการระบุและพิสูจน์ตัวตน
I&AName	ชื่อการระบุและพิสูจน์ตัวตน
I&A Service	การบริการการระบุและพิสูจน์ตัวตน
การดำเนินการ	**คำอธิบาย**
setService	การกำหนดบริการ
คลาส Role	
ลักษณะประจำ	**คำอธิบาย**
roleID	รหัสบทบาท
roleName	ชื่อบทบาท
คลาส Security Property	
ลักษณะประจำ	**คำอธิบาย**
propertyID	รหัสคุณสมบัติความมั่นคง
propertyName	ชื่อคุณสมบัติความมั่นคง
คลาส Service Termination	
ลักษณะประจำ	**คำอธิบาย**
serviceTerminationID	รหัสกิจกรรมการสิ้นสุดของหุ้นส่วน
serviceTerminationName	ชื่อกิจกรรมการสิ้นสุดของหุ้นส่วน
serviceTerminationDescription	คำอธิบายกิจกรรมการสิ้นสุดของหุ้นส่วน
การดำเนินการ	**คำอธิบาย**
setServiceTermination	การกำหนดกิจกรรมการสิ้นสุดของหุ้นส่วน

ตารางที่ จ.9 รายละเอียดโครงสร้างคลาสของแบบรูปความต้องการระบุและการพิสูจน์ตัวตน

แบบรูปการการระบุและการพิสูจน์ตัวตน	
คลาส Asset	
ลักษณะประจำ	**คำอธิบาย**
assetId	รหัสสินทรัพย์
assetName	ชื่อสินทรัพย์
assetType	รูปแบบสินทรัพย์
คลาส Domain Factor	
ลักษณะประจำ	**คำอธิบาย**
factorID	รหัสปัจจัยที่มีผลต่อการกำหนดความต้องการ
factorName	ชื่อปัจจัยที่มีผลต่อการกำหนดความต้องการ
factorDescription	คำอธิบายปัจจัยที่มีผลต่อการกำหนดความต้องการ
คลาส Domain Factor Requirement	
ลักษณะประจำ	**คำอธิบาย**
domainFactorRequirementID	รหัสความสัมพันธ์ของปัจจัยและความต้องการ
domainFactorRequirementName	ชื่อความสัมพันธ์ของปัจจัยและความต้องการ
การดำเนินการ	**คำอธิบาย**
setDomainFactorRequirement	การกำหนดความสัมพันธ์ของปัจจัยและความต้องการ
คลาส I&A Domain	
ลักษณะประจำ	**คำอธิบาย**
domainID	รหัสขอบเขตในการใช้บริการการระบุและพิสูจน์ตัวตน
domainName	ชื่อขอบเขตในการใช้บริการการระบุและพิสูจน์ตัวตน
domainDescription	คำอธิบายขอบเขตในการใช้บริการการระบุและพิสูจน์ตัวตน
คลาส I&A Requirement	
ลักษณะประจำ	**คำอธิบาย**
requirementID	รหัสความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน
requirementName	ชื่อความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน
requirementDescription	คำอธิบายความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน
การดำเนินการ	**คำอธิบาย**
setI&ARequirement	ความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน

ตารางที่ จ.9 รายละเอียดโครงสร้างคลาสของแบบรูปความต้องการระบุและการพิสูจน์ตัวตน (ต่อ)

แบบรูปการการระบุและการพิสูจน์ตัวตน	
คลาส I&A Service	
ลักษณะประจำ	**คำอธิบาย**
I&AID	รหัสการระบุและพิสูจน์ตัวตน
I&AName	ชื่อการระบุและพิสูจน์ตัวตน
I&ADescription	คำอธิบายการระบุและพิสูจน์ตัวตน
การดำเนินการ	**คำอธิบาย**
setService	การบริการการระบุและพิสูจน์ตัวตน

ตารางที่ จ.10 รายละเอียดโครงสร้างคลาสของแบบรูปทางเลือกการออกแบบสำหรับการระบุตัวตนและการพิสูจน์ตัวตนอัตโนมัติ

แบบรูปทางเลือกการออกแบบสำหรับการระบุตัวตนและการพิสูจน์ตัวตนอัตโนมัติ	
คลาส Asset	
ลักษณะประจำ	**คำอธิบาย**
assetId	รหัสสินทรัพย์
assetName	ชื่อสินทรัพย์
assetType	รูปแบบสินทรัพย์
คลาส Domain Factor	
ลักษณะประจำ	**คำอธิบาย**
factorID	รหัสปัจจัยที่มีผลต่อการกำหนดความต้องการ
factorName	ชื่อปัจจัยที่มีผลต่อการกำหนดความต้องการ
factorDescription	คำอธิบายปัจจัยที่มีผลต่อการกำหนดความต้องการ
คลาส Domain Factor Requirement	
ลักษณะประจำ	**คำอธิบาย**
domainFactorRequirementID	รหัสความสัมพันธ์ของปัจจัยและความต้องการ
domainFactorRequirementName	ชื่อความสัมพันธ์ของปัจจัยและความต้องการ
การดำเนินการ	**คำอธิบาย**
setDomainFactorRequirement	การกำหนดความสัมพันธ์ของปัจจัยและความต้องการ
คลาส I&A Domain	
ลักษณะประจำ	**คำอธิบาย**
domainID	ขอบเขตในการใช้บริการ
domainName	ชื่อขอบเขตในการใช้บริการ
domainDescription	คำอธิบายขอบเขตในการใช้บริการ
คลาส I&A Requirement	
ลักษณะประจำ	**คำอธิบาย**
requirementID	รหัสความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน
requirementName	ชื่อความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน
requirementDescription	คำอธิบายความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน

ตารางที่ จ.10 รายละเอียดโครงสร้างคลาสของแบบรูปทางเลือกการออกแบบสำหรับการระบุตัวตนและการพิสูจน์ตัวตนอัตโนมัติ (ต่อ)

แบบรูปทางเลือกการออกแบบสำหรับการระบุตัวตนและการพิสูจน์ตัวตนอัตโนมัติ	
คลาส I&A Service	
ลักษณะประจำ	**คำอธิบาย**
I&AID	รหัสการระบุและพิสูจน์ตัวตน
I&AName	ชื่อการระบุและพิสูจน์ตัวตน
I&ADescription	คำอธิบายการระบุและพิสูจน์ตัวตน
การดำเนินการ	**คำอธิบาย**
setService	การกำหนดบริการ การระบุและพิสูจน์ตัวตน
คลาส I&A Technique	
ลักษณะประจำ	**คำอธิบาย**
techniqueId	รหัสเทคนิคการระบุและพิสูจน์ตัวตน
techniqueName	ชื่อเทคนิคการระบุและพิสูจน์ตัวตน
คลาส I&A Technique Profile	
ลักษณะประจำ	**คำอธิบาย**
profileID	รหัสโพรไฟล์สำหรับความต้องการใช้บริการ
profileName	ชื่อโพรไฟล์สำหรับความต้องการใช้บริการ
การดำเนินการ	**คำอธิบาย**
setTechniqueProfile	การกำหนดโพรไฟล์สำหรับความต้องการใช้บริการ

ตารางที่ จ.11 รายละเอียดโครงสร้างคลาสของแบบรูปการออกแบบและใช้รหัสผ่าน

แบบรูปการออกแบบและใช้รหัสผ่าน	
คลาส I&A Technique	
ลักษณะประจำ	**คำอธิบาย**
techniqueId	รหัสเทคนิคการระบุและพิสูจน์ตัวตน
techniqueName	ชื่อเทคนิคการระบุและพิสูจน์ตัวตน
คลาส Password	
ลักษณะประจำ	**คำอธิบาย**
passwordID	รหัสของรหัสผ่าน
passwordName	ชื่อของรหัสผ่าน
passwordDescription	คำอธิบายของรหัสผ่าน
composition	ตัวอักษรที่จะใช้ในรหัสผ่าน
lengthRange	ความยาวของรหัสผ่าน
source	แหล่งที่มาของรหัสผ่าน
lifetime	อายุการใช้งานของรหัสผ่าน
ownership	บุคคลที่มีสิทธิ์ในการใช้งานรหัสผ่าน
entry	วิธีการในการกรอกรหัสผ่าน
authenticationPeriod	ระยะเวลาของการพิสูจน์ตัวตนโดยใช้รหัสผ่าน
distribution	วิธีการในการจัดเก็บรหัสผ่าน
storage	การเก็บรักษารหัสผ่าน
transmission	วิธีการในการถ่ายโอนรหัสผ่าน เพื่อใช้ในการตรวจสอบ
การดำเนินการ	**คำอธิบาย**
setPasswordConstrain	การกำหนดเงื่อนไขการใช้งานรหัสผ่าน
คลาส Password Policy	
ลักษณะประจำ	**คำอธิบาย**
passwordPolicyID	รหัสของนโยบายการใช้รหัสผ่าน
passwordPolicyName	ชื่อของนโยบายการใช้รหัสผ่าน
passwordPolicyDescription	คำอธิบายของนโยบายการใช้รหัสผ่าน
การดำเนินการ	**คำอธิบาย**
setupPasswordPolicy	การกำหนดนโยบายการใช้รหัสผ่าน

ตารางที่ จ.12 รายละเอียดโครงสร้างคลาสของแบบรูปการออกแบบชีวมิติ

แบบรูปการออกแบบชีวมิติ	
คลาส Biometric	
ลักษณะประจำ	**คำอธิบาย**
biometricMechanismID	รหัสชีวมิติ
biometricMechanismName	ชื่อชีวมิติ
biometricMechanismDescription	คำอธิบายชีวมิติ
การดำเนินการ	**คำอธิบาย**
setBiometricMechanism	การกำหนดชีวมิติ
คลาส Biometric Characteristic	
ลักษณะประจำ	**คำอธิบาย**
biometricCharacteristicID	รหัสลักษณะชีวมิติ
biometricCharacteristicName	ชื่อลักษณะชีวมิติ
การดำเนินการ	**คำอธิบาย**
setBiometricCharacteristic	การกำหนดลักษณะชีวมิติ
คลาส I&A Technique	
ลักษณะประจำ	**คำอธิบาย**
techniqueId	รหัสเทคนิคการระบุและพิสูจน์ตัวตน
techniqueName	ชื่อเทคนิคการระบุและพิสูจน์ตัวตน
คลาส I&A Technique Factor	
ลักษณะประจำ	**คำอธิบาย**
techniqueFactorID	รหัสปัจจัยในการใช้งานชีวมิติ
techniqueFactorName	ชื่อปัจจัยในการใช้งานชีวมิติ
techniqueFactorDescription	คำอธิบายปัจจัยในการใช้งานชีวมิติ

ตารางที่ จ.13 รายละเอียดโครงสร้างคลาสของแบบรูปการให้อำนาจ

แบบรูปการให้อำนาจ	
คลาส Asset	
ลักษณะประจำ	**คำอธิบาย**
assetId	รหัสสินทรัพย์
assetName	ชื่อสินทรัพย์
assetType	รูปแบบสินทรัพย์
คลาส Right	
ลักษณะประจำ	**คำอธิบาย**
rightID	รหัสของสิทธิ์
rightName	ชื่อของสิทธิ์
การดำเนินการ	**คำอธิบาย**
setRight	การกำหนดสิทธิ์
คลาส User	
ลักษณะประจำ	**คำอธิบาย**
userID	รหัสผู้ใช้งาน
userName	ชื่อผู้ใช้งาน

ตารางที่ จ.14 รายละเอียดโครงสร้างคลาสของแบบรูปการควบคุมการเข้าถึงเชิงบทบาท

แบบรูปการเข้าถึงเชิงบทบาท	
คลาส Asset	
ลักษณะประจำ	**คำอธิบาย**
assetId	รหัสสินทรัพย์
assetName	ชื่อสินทรัพย์
assetType	รูปแบบสินทรัพย์
คลาส Right	
ลักษณะประจำ	**คำอธิบาย**
rightID	รหัสของสิทธิ์
rightName	ชื่อของสิทธิ์
การดำเนินการ	**คำอธิบาย**
setRight	การกำหนดสิทธิ์
คลาส Role	
ลักษณะประจำ	**คำอธิบาย**
roleID	รหัสบทบาท
roleName	ชื่อบทบาท
การดำเนินการ	**คำอธิบาย**
setRole	การกำหนดบทบาท
คลาส User	
ลักษณะประจำ	**คำอธิบาย**
userID	รหัสผู้ใช้
userName	ชื่อผู้ใช้

ตารางที่ จ.15 รายละเอียดโครงสร้างคลาสของแบบรูปความมั่นคงหลายระดับ

แบบรูปความมั่นคงหลายระดับ	
คลาส Asset	
ลักษณะประจำ	**คำอธิบาย**
assetId	รหัสสินทรัพย์
assetName	ชื่อสินทรัพย์
assetType	รูปแบบสินทรัพย์
คลาส Category Asset	
ลักษณะประจำ	**คำอธิบาย**
categoryAssetID	หมวดหมู่ของสินทรัพย์
categoryAssetName	ชื่อหมวดหมู่ของสินทรัพย์
การดำเนินการ	**คำอธิบาย**
setCategoryAsset	การกำหนดหมวดหมู่ของสินทรัพย์
คลาส Classification Level	
ลักษณะประจำ	**คำอธิบาย**
classificationLevelID	รหัสระดับความสำคัญของสินทรัพย์
classificationLevelName	ชื่อระดับความสำคัญของสินทรัพย์
การดำเนินการ	**คำอธิบาย**
setClassificationLevel	การกำหนดระดับความสำคัญของสินทรัพย์
คลาส Clearance Level	
ลักษณะประจำ	**คำอธิบาย**
clearanceLevelID	รหัสระดับความสำคัญของสิทธิ์
clearanceLevelName	ชื่อระดับความสำคัญของสิทธิ์
การดำเนินการ	**คำอธิบาย**
setClearanceLevel	การกำหนดระดับความสำคัญของสิทธิ์
คลาส Right	
ลักษณะประจำ	**คำอธิบาย**
rightID	รหัสสิทธิ์
rightName	ชื่อสิทธิ์
การดำเนินการ	**คำอธิบาย**

ตารางที่ จ.15 รายละเอียดโครงสร้างคลาสของแบบรูปความมั่นคงหลายระดับ (ต่อ)

แบบรูปความมั่นคงหลายระดับ	
คลาส Role	
ลักษณะประจำ	**คำอธิบาย**
roleID	รหัสบทบาท
roleName	ชื่อบทบาท
การดำเนินการ	**คำอธิบาย**
setRole	การกำหนดบทบาท
คลาส User	
ลักษณะประจำ	**คำอธิบาย**
userID	รหัสผู้ใช้
userName	ชื่อผู้ใช้

ตารางที่ จ.16 รายละเอียดโครงสร้างคลาสของแบบรูปการตรวจสอบการเข้าถึงทรัพยากร

แบบรูปการตรวจสอบการเข้าถึงทรัพยากร	
คลาส Asset	
ลักษณะประจำ	**คำอธิบาย**
assetId	รหัสสินทรัพย์
assetName	ชื่อสินทรัพย์
assetType	รูปแบบสินทรัพย์
คลาส Authorization	
ลักษณะประจำ	**คำอธิบาย**
ruleID	รหัสกฎการให้อำนาจ
ruleName	ชื่อกฎการให้อำนาจ
การดำเนินการ	**คำอธิบาย**
setRule	การกำหนดกฎการให้อำนาจ
คลาส Concrete Reference Monitor	
ลักษณะประจำ	**คำอธิบาย**
-	-
คลาส Request	
ลักษณะประจำ	**คำอธิบาย**
assetID	รหัสสินทรัพย์
accessType	ประเภทการเข้าถึง
คลาส Reference Monitor	
การดำเนินการ	**คำอธิบาย**
request	คำร้องขอ
คลาส Role	
ลักษณะประจำ	**คำอธิบาย**
roleID	รหัสของบทบาท
roleName	ชื่อของบทบาท
คลาส Set of Authorization Rules	
การดำเนินการ	**คำอธิบาย**
checkRule	ตรวจสอบการให้อำนาจ

ตารางที่ จ.16 รายละเอียดโครงสร้างคลาสของแบบรูปการตรวจสอบการเข้าถึงทรัพยากร (ต่อ)

แบบรูปการตรวจสอบการเข้าถึงทรัพยากร	
คลาส User	
ลักษณะประจำ	**คำอธิบาย**
userID	รหัสผู้ใช้
userName	ชื่อผู้ใช้

ตารางที่ จ.17 รายละเอียดโครงสร้างคลาสของแบบรูปไฟร์วอลล์กรองแพ็คเกจ

แบบรูปไฟร์วอลล์กรองแพ็คเกจ	
คลาส Default Rule	
ลักษณะประจำ	**คำอธิบาย**
-	-
คลาส Explicit Rule	
ลักษณะประจำ	**คำอธิบาย**
-	-
คลาส External Host	
ลักษณะประจำ	**คำอธิบาย**
externalIP	เลขที่อยู่ไอพีของโฮสต์ภายนอก
externalPort	พอร์ทของโฮสต์ภายนอก
คลาส Firewall	
ลักษณะประจำ	**คำอธิบาย**
sourceIP	เลขที่อยู่ไอพีแหล่งต้นทาง
destinationIP	เลขที่อยู่ไอพีแหล่งปลายทาง
sourcePort	พอร์ทต้นทาง
destinationPort	พอร์ทปลายทาง
การดำเนินการ	**คำอธิบาย**
accept	ยอมรับ
deny	ปฏิเสธ
คลาส Packet Filter Firewall	
ลักษณะประจำ	**คำอธิบาย**
-	-
คลาส Local Host	
ลักษณะประจำ	**คำอธิบาย**
internalIP	เลขที่อยู่ไอพีจากโฮสต์ภายใน
internalPort	พอร์ทภายใน

ตารางที่ จ.17 รายละเอียดโครงสร้างคลาสของแบบรูปไฟร์วอลล์กรองแพ็คเกจ (ต่อ)

แบบรูปไฟร์วอลล์กรองแพ็คเกจ	
คลาส RuleBased	
ลักษณะประจำ	**คำอธิบาย**
portRule	กฎของพอร์ท
IPRule	ไอพีของพอร์ท
การดำเนินการ	**คำอธิบาย**
checkRule	ตรวจสอบกฎของไฟร์วอลล์

ตารางที่ จ.18 รายละเอียดโครงสร้างคลาสของแบบรูปไฟร์วอลล์เชิงตัวแทน

แบบรูปไฟร์วอลล์เชิงตัวแทน	
คลาส Default Rule	
ลักษณะประจำ	**คำอธิบาย**
-	-
คลาส Explicit Rule	
ลักษณะประจำ	**คำอธิบาย**
-	-
คลาส External Host	
ลักษณะประจำ	**คำอธิบาย**
externalIP	เลขที่อยู่ไอพีของโฮสต์ภายนอก
externalPort	พอร์ทของโฮสต์ภายนอก
คลาส Firewall	
ลักษณะประจำ	**คำอธิบาย**
sourceIP	เลขที่อยู่ไอพีแหล่งต้นทาง
destinationIP	เลขที่อยู่ไอพีแหล่งปลายทาง
sourcePort	พอร์ทต้นทาง
destinationPort	พอร์ทปลายทาง
การดำเนินการ	**คำอธิบาย**
accept	ยอมรับ
deny	ปฏิเสธ
คลาส Proxy	
ลักษณะประจำ	**คำอธิบาย**
-	-
คลาส Proxy Based Firewall	
ลักษณะประจำ	**คำอธิบาย**
-	-
คลาส Local Host	
ลักษณะประจำ	**คำอธิบาย**
internalIP	เลขที่อยู่ไอพีจากโฮสต์ภายใน

ตารางที่ จ.18 รายละเอียดโครงสร้างคลาสของแบบรูปไฟร์วอลล์เชิงตัวแทน (ต่อ)

แบบรูปไฟร์วอลล์เชิงตัวแทน	
คลาส RuleBased	
ลักษณะประจำ	**คำอธิบาย**
portRule	กฎของพอร์ท
IPRule	กฎของไอพี
การดำเนินการ	**คำอธิบาย**
checkRule	การตรวจสอบกฎ
คลาส Service	
ลักษณะประจำ	**คำอธิบาย**
serviceName	ชื่อของบริการ
servicePort	พอร์ทที่ใช้บริการ
การดำเนินการ	**คำอธิบาย**
checkService	การตรวจสอบบริการ

ตารางที่ จ.19 รายละเอียดโครงสร้างคลาสของแบบรูปไฟร์วอลล์เชิงสถานะ

แบบรูปไฟร์วอลล์เชิงสถานะ	
คลาส External Host	
ลักษณะประจำ	**คำอธิบาย**
externalIP	เลขที่อยู่ไอพีของโฮสต์ภายนอก
externalPort	พอร์ทของโฮสต์ภายนอก
คลาส Firewall	
ลักษณะประจำ	**คำอธิบาย**
sourceIP	เลขที่อยู่ไอพีแหล่งต้นทาง
destinationIP	เลขที่อยู่ไอพีแหล่งปลายทาง
sourcePort	พอร์ทต้นทาง
destinationPort	พอร์ทปลายทาง
การดำเนินการ	**คำอธิบาย**
accept	ยอมรับ
deny	ปฏิเสธ
คลาส Local Host	
ลักษณะประจำ	**คำอธิบาย**
internalIP	เลขที่อยู่ไอพีจากโฮสต์ภายใน
internalPort	พอร์ทภายใน
คลาส Stateful Firewall	
ลักษณะประจำ	**คำอธิบาย**
-	-
คลาส State Table	
ลักษณะประจำ	**คำอธิบาย**
sessionlist	รายการช่วงเวลา
การดำเนินการ	**คำอธิบาย**
checkSession	ตรวจสอบช่วงเวลา

ภาคผนวก ฉ

ตัวอย่างการใช้งานเครื่องมือต้นแบบการสร้างภาพนามธรรมความต้องการความมั่นคงจากแบบรูปความมั่นคง

ภาคผนวก ฉ นำเสนอตัวอย่างการใช้งานเครื่องมือต้นแบบที่ได้พัฒนาบนพื้นฐานของแผนภาพเชิงโครงสร้างที่สร้างขึ้น โดยจะนำเสนอในหัวข้อต่อไปนี้

1) ประเภทของการสร้างภาพนามธรรมที่เครื่องมือสนับสนุน

2) ตัวอย่างการใช้งานการสร้างภาพนามธรรมจำแนกตามแต่ละประเภท

โดยมีรายละเอียดดังนี้

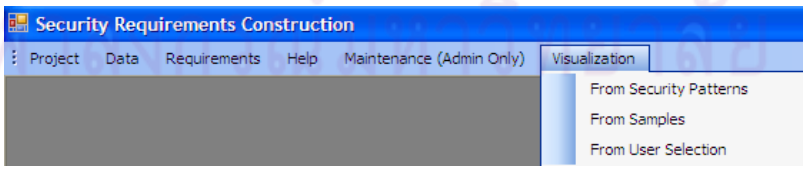
ฉ.1 ประเภทของการสร้างภาพนามธรรมที่เครื่องมือสนับสนุน

ประเภทการสร้างภาพนามธรรมที่เครื่องมือต้นแบบสนับสนุน สามารถแบ่งออกได้เป็น 3 ประเภท ซึ่งผู้ใช้งานสามารถเลือกประเภทการสร้างภาพนามธรรมได้จากเมนูแถบเครื่องมือด้านบน ดังรูป ฉ.1 โดยมีรายละเอียดของแต่ละเมนูดังนี้

1) *Visualize from Security Patterns* ภายในเมนูนี้ผู้ใช้งานสามารถสร้างภาพนามธรรมจากการเลือกแบบรูปความมั่นคง และสามารถเลือกประเภทของแผนภูมิที่ต้องการได้

2) *Visualize from Samples* ภายในเมนูนี้ผู้ใช้งานสามารถสร้างภาพนามธรรมจากตัวอย่างที่กำหนดให้ และสามารถเลือกประเภทของแผนภูมิที่ต้องการได้

3) *Visualize from User Selection* ภายในเมนูนี้ผู้ใช้งานสามารถสร้างภาพนามธรรมจากการเลือกข้อมูลลักษณะประจำใดๆ และสามารถเลือกประเภทของแผนภูมิที่ต้องการได้ทั้งแบบแผนภูมิแบบจุดสองมิติ และสามมิติ



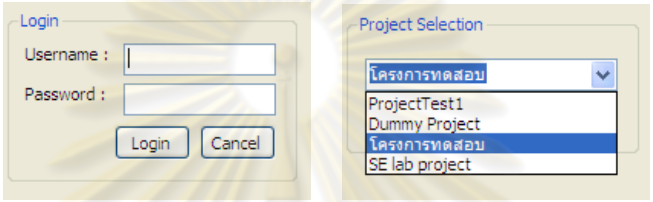
รูปที่ ฉ.1 เมนูการเลือกประเภทการสร้างภาพนามธรรม

ฉ.2 ตัวอย่างการใช้งานการสร้างภาพนามธรรมจำแนกตามแต่ละประเภท

ประเภทการสร้างภาพนามธรรมสามารถแบ่งออกได้เป็น 3 ประเภท โดยมีรายละเอียดตัวอย่างการใช้งานในแต่ละประเภทดังนี้

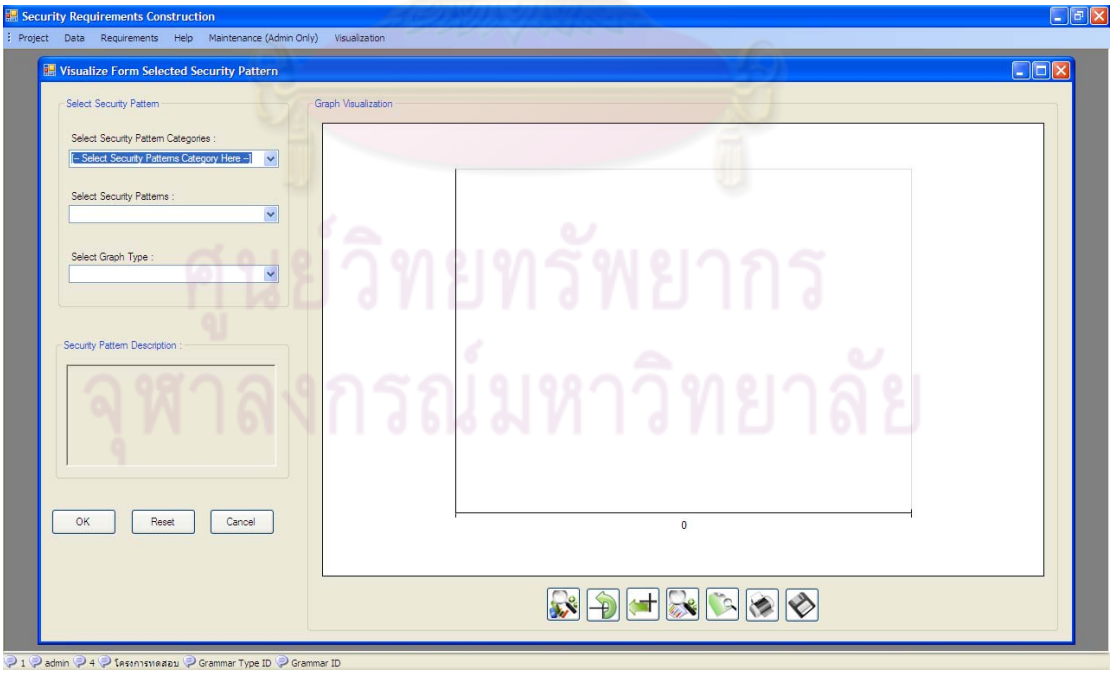
1) การสร้างภาพนามธรรมประเภทการเลือกจากแบบรูปความมั่นคง

เพื่อแสดงให้เห็นขั้นตอนการใช้งานที่แท้จริง ในที่นี้จะขอยกตัวอย่างการสร้างภาพนามธรรมจากแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร ซึ่งจัดอยู่ในกลุ่มของแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง โดยในการใช้งานเครื่องมือจะต้องทำการลงทะเบียนเพื่อเข้าระบบ และเลือกโครงการที่ต้องการสร้างภาพนามธรรม ดังรูปที่ ฉ.2



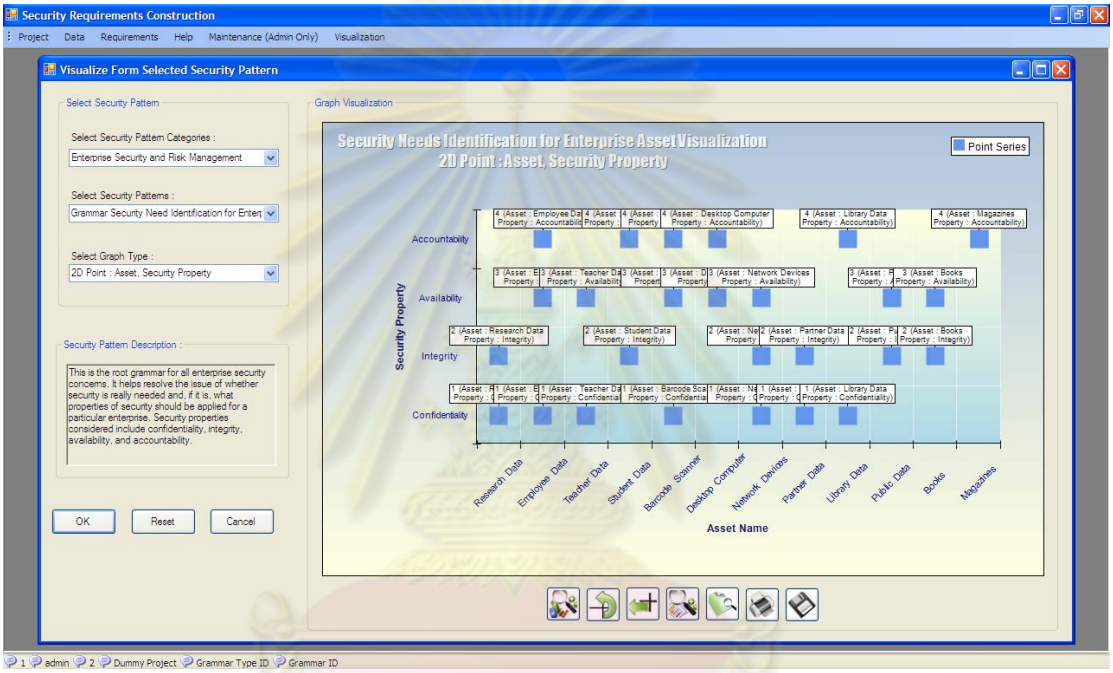
รูปที่ ฉ.2 เมนูการลงทะเบียนเพื่อเข้าระบบ และเลือกโครงการที่ต้องการสร้างภาพนามธรรม

ภายหลังขั้นตอนการลงทะเบียนเข้าใช้ระบบแล้ว ให้เลือก เลือกเมนู “Visualization” และ “Visualize from Security Patterns” จะได้หน้าจอหลักดังรูปที่ ฉ.3



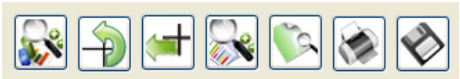
รูปที่ ฉ.3 หน้าจอหลักการสร้างภาพนามธรรมประเภทการเลือกจากแบบรูปความมั่นคง

เลือก “Security Pattern Categories” ในกลุ่ม “Enterprise Security and Risk Management” แล้วจึงเลือก “Security Needs Identification for Enterprise Assets” เพื่อสร้างภาพนามธรรมความต้องการความมั่นคงจากแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร จากนั้นเลือก “2D Point : Asset Name, Security Property” เครื่องมือจะแสดงคำอธิบายสำหรับแบบรูปความมั่นคงนั้นๆ และแสดงผลภาพนามธรรมในรูปแบบของแผนภูมิแบบจุดสองมิติที่ได้เลือกไว้ ทางด้านขวามือของหน้าจอดังรูปที่ ฉ.4



รูปที่ ฉ.4 การสร้างภาพนามธรรมจากแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร

ผู้ใช้งานสามารถจัดการกับแผนภูมิด้วยแถบเครื่องมือด้านล่างขวาของหน้าจอได้ ดังรูปที่ ฉ.5 โดยแถบเครื่องมือประกอบด้วยฟังก์ชันต่างๆ ที่จำเป็นต่อการควบคุมแผนภูมิ เช่น การย่อ/ขยาย การย้าย การหมุน การตั้งค่าการพิมพ์ การดูภาพตัวอย่างก่อนพิมพ์ และการบันทึกภาพแผนภูมิ

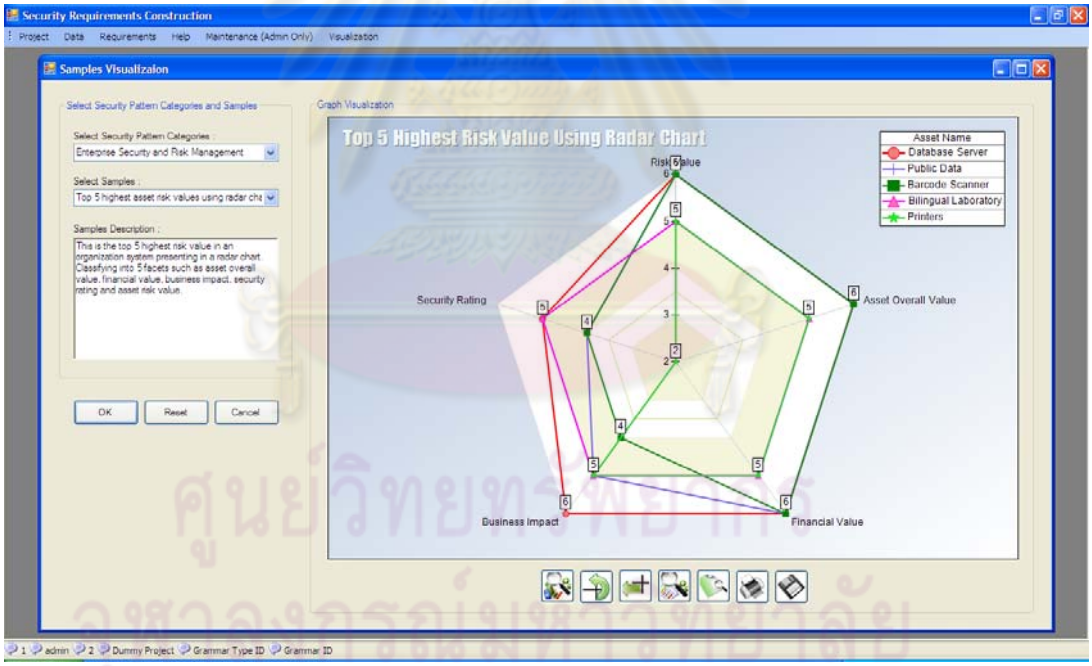


รูปที่ ฉ.5 เมนูแถบเครื่องมือการจัดการแผนภูมิ

2) การสร้างภาพนามธรรมประเภทการเลือกจากตัวอย่างที่กำหนดให้

เพื่อแสดงให้เห็นขั้นตอนการใช้งานที่แท้จริง ในที่นี้จะขอยกตัวอย่างการสร้างภาพนามธรรมจากการเลือกจากตัวอย่างที่กำหนดให้ “Top 5 highest asset risk value using radar chart” จากกลุ่มของแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง

โดยให้ผู้ใช้งานเลือกเลือกเมนู “Visualization” และ “Visualize from Samples” จากแถบเครื่องมือด้านบน จะเข้าสู่หน้าจอหลักของการสร้างภาพนามธรรมประเภทการเลือกจากตัวอย่างที่กำหนดให้ ต่อมาให้ผู้ใช้งานเลือก “Security Pattern Categories” ในกลุ่ม “Enterprise Security and Risk Management” แล้วจึงเลือก “Top 5 highest asset risk value using radar chart” เพื่อสร้างภาพนามธรรมสินทรัพย์ที่มีค่าความเสี่ยงสูงสุด 5 อันดับแรกโดยใช้แผนภูมิเรดาร์จากนั้นเครื่องมือจะแสดงคำอธิบายตัวอย่างที่กำหนดให้ และแสดงผลภาพนามธรรมในรูปแบบของแผนภูมิแท่งแบบเรียงซ้อนที่ได้เลือกไว้ ทางด้านขวามือของหน้าจอดังรูปที่ ฉ.6



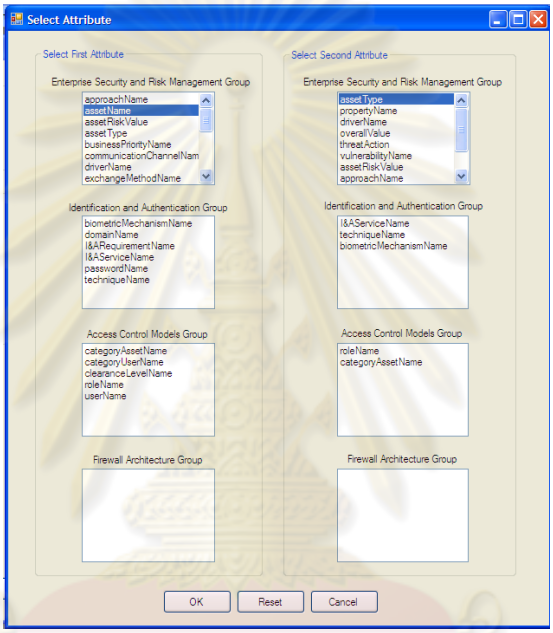
รูปที่ ฉ.6 การสร้างภาพนามธรรมจากตัวอย่างที่กำหนดให้ “สินทรัพย์ที่มีค่าความเสี่ยงสูงสุด 5 อันดับแรกโดยใช้แผนภูมิเรดาร์”

3) การสร้างภาพนามธรรมประเภทการเลือกจากข้อมูลลักษณะประจำ

เพื่อแสดงให้เห็นขั้นตอนการใช้งานที่แท้จริง ในที่นี้จะขอยกตัวอย่างการสร้างภาพนามธรรมจากการเลือกจากข้อมูลลักษณะประจำประเภทสองมิติ โดยเลือกค่า “Asset Name”

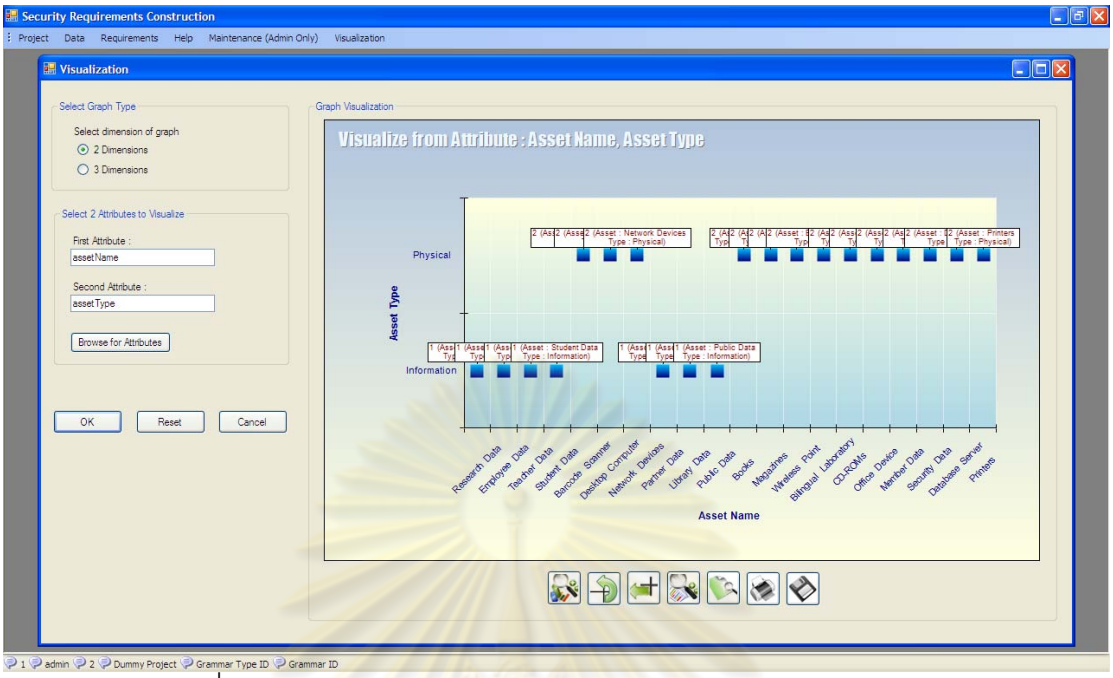
และ “Overall Value” จากแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร และแบบรูปการประเมินมูลค่าสินทรัพย์

โดยให้ผู้ใช้งานเลือกเลือกเมนู “Visualization” และ “Visualize from User Selection” จากแถบเครื่องมือด้านบน จะเข้าสู่หน้าจอหลักของการสร้างภาพนามธรรมประเภทการเลือกจากข้อมูลลักษณะประจำ ต่อมาให้ผู้ใช้งานเลือกรูปแบบแผนภูมิประเภทสองมิติ และเลือกปุ่ม “Browse for Attribute” จะได้หน้าจอการเลือกลักษณะประจำดังรูปที่ ฉ.7



รูปที่ ฉ.7 หน้าจอการเลือกข้อมูลลักษณะประจำแบบสองมิติ

จากนั้นให้ผู้ใช้งานเลือกข้อมูลลักษณะประจำตัวที่ 1 จากคอลัมน์แรก โดยเลือกข้อมูล “Asset Name” จากกลุ่มของแบบรูป “Enterprise Security and Risk Management” และเลือกข้อมูลลักษณะประจำตัวที่ 2 จากคอลัมน์ที่สอง โดยเลือกข้อมูล “Overall Value” จากกลุ่มของแบบรูป “Enterprise Security and Risk Management” จากนั้นเครื่องมือจะแสดงผลภาพนามธรรมในรูปแบบของแผนภูมิจุดแบบสองมิติที่ได้เลือกไว้ ทางด้านขวามือของหน้าจอดังรูปที่ ฉ.8



รูปที่ ฉ.8 การสร้างภาพนามธรรมจากการเลือกข้อมูลลักษณะประจำ “Asset Name” และ “AssetType”

ภาคผนวก ซ

ตัวอย่างผลลัพธ์ภาพนามธรรมความต้องการความมั่นคงจากแบบรูปความมั่นคง

ตัวอย่างผลลัพธ์ภาพนามธรรมความความต้องการความมั่นคงที่ได้จากเครื่องมือ จำแนกตามการสร้างภาพนามธรรมทั้ง 3 ประเภท มีรายละเอียดดังต่อไปนี้

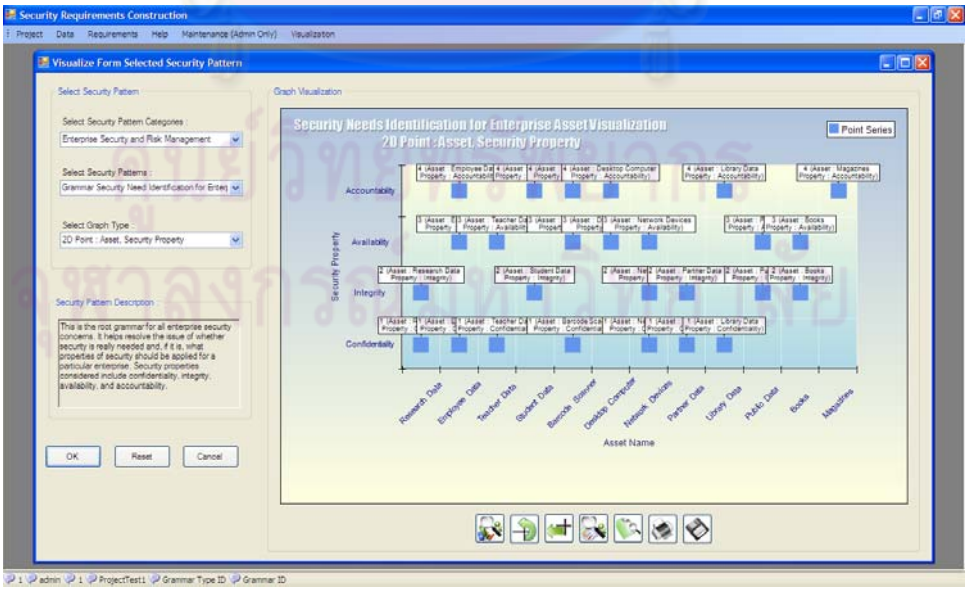
ซ.1 ตัวอย่างผลลัพธ์ภาพนามธรรมที่ได้จากการเลือกเมนูการสร้างภาพนามธรรมจากแบบรูปความมั่นคง

ผู้ใช้งานสามารถดูรายละเอียดรายการการสร้างภาพนามธรรมจากการเลือกแบบรูปความมั่นคงทั้งหมดได้จากตารางที่ 4.1 ในบทที่ 4 สำหรับตัวอย่างผลลัพธ์ในหัวข้อนี้จะจำแนกตามกลุ่มของแบบรูปความมั่นคง ดังรายละเอียดต่อไปนี้

1) กลุ่มการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง

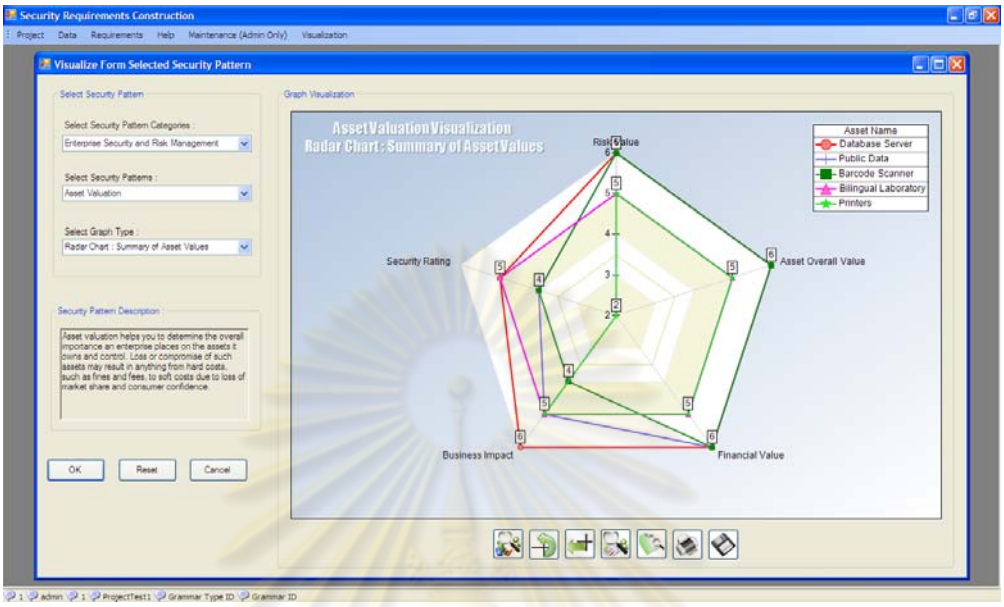
กลุ่มแบบรูปนี้จะเกี่ยวข้องกับการจัดการในเรื่องต่างๆ พื้นฐาน เช่น การระบุความจำเป็นพื้นฐาน การประเมินความเสี่ยง แนวคิดและการบริหารความมั่นคง และการให้ความสำคัญกับการติดต่อภายนอกองค์กร ซึ่งรายการตัวอย่างผลลัพธ์ตามแบบรูปความมั่นคงในกลุ่มนี้ประกอบไปด้วย

(1) ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์ขององค์กร



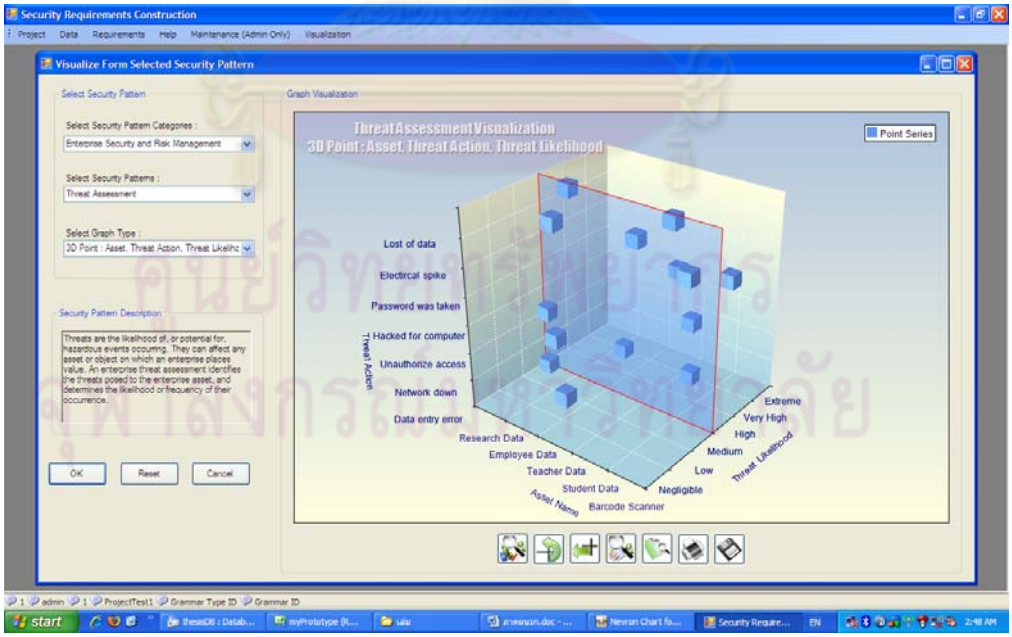
รูปที่ ซ.1 ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์ขององค์กร

(2) **ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปการประเมินมูลค่าสินทรัพย์**



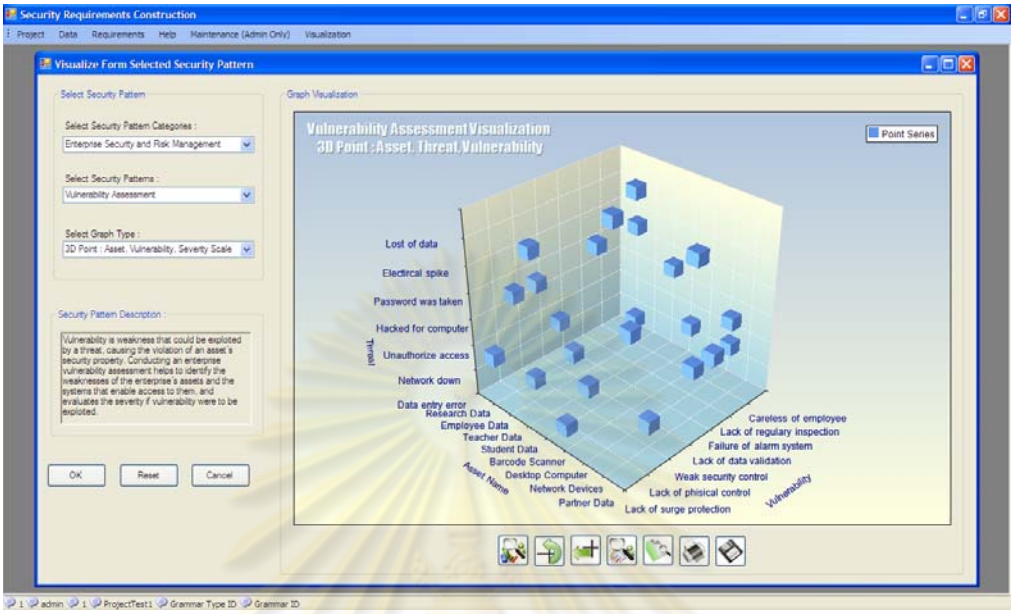
รูปที่ ช.2 ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปการประเมินมูลค่าสินทรัพย์

(3) **ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปการประเมินภัยคุกคาม**



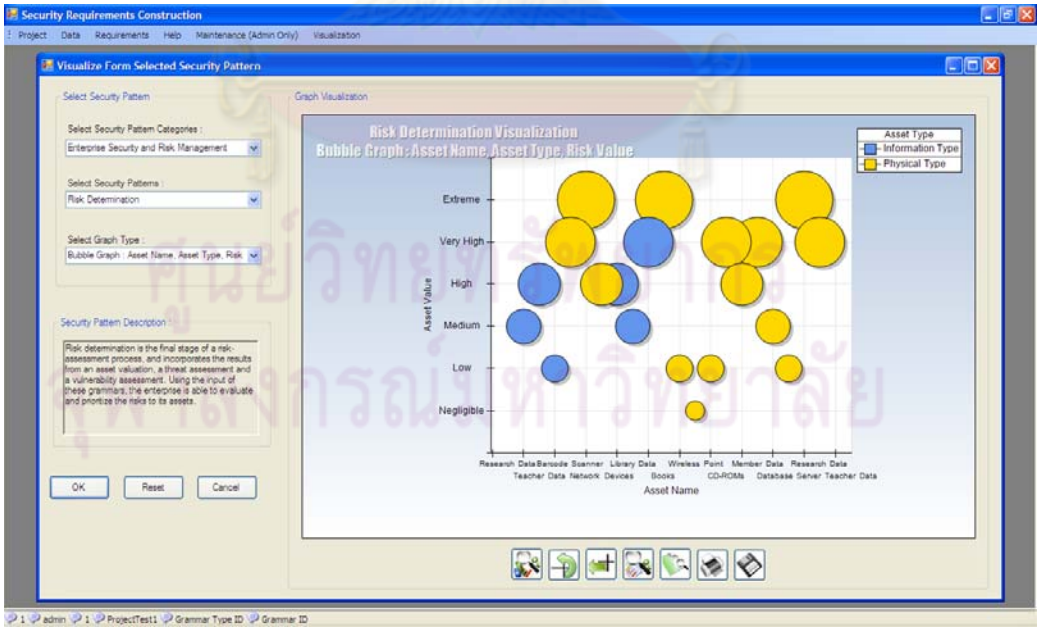
รูปที่ ช.3 ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปการประเมินภัยคุกคาม

(4) ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปการประเมินภาวะเสี่ยง



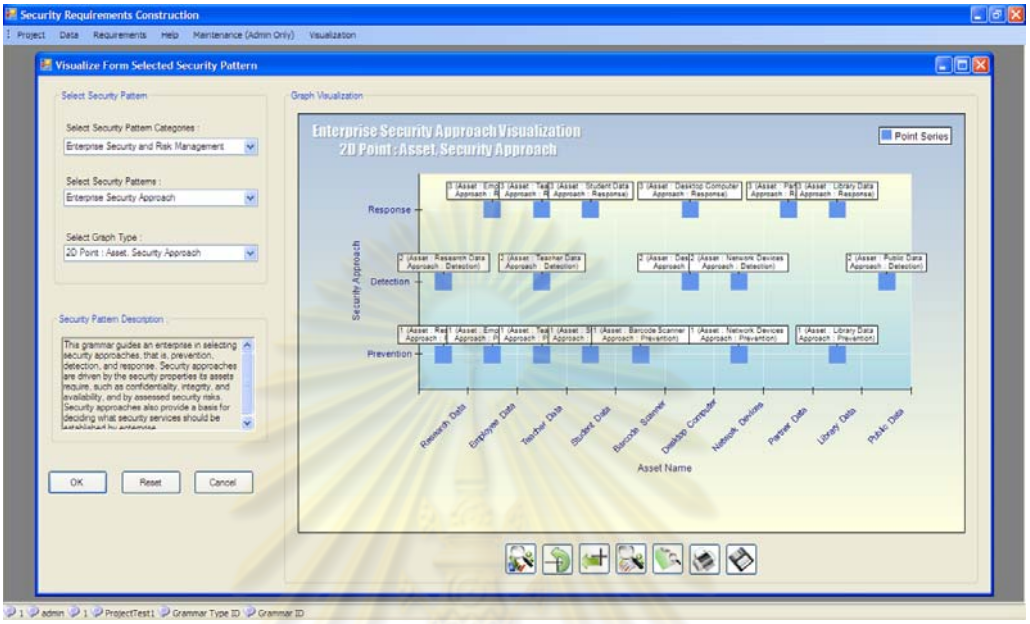
รูปที่ ช.4 ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปการประเมินภาวะเสี่ยง

(5) ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปการกำหนดค่าความเสี่ยง



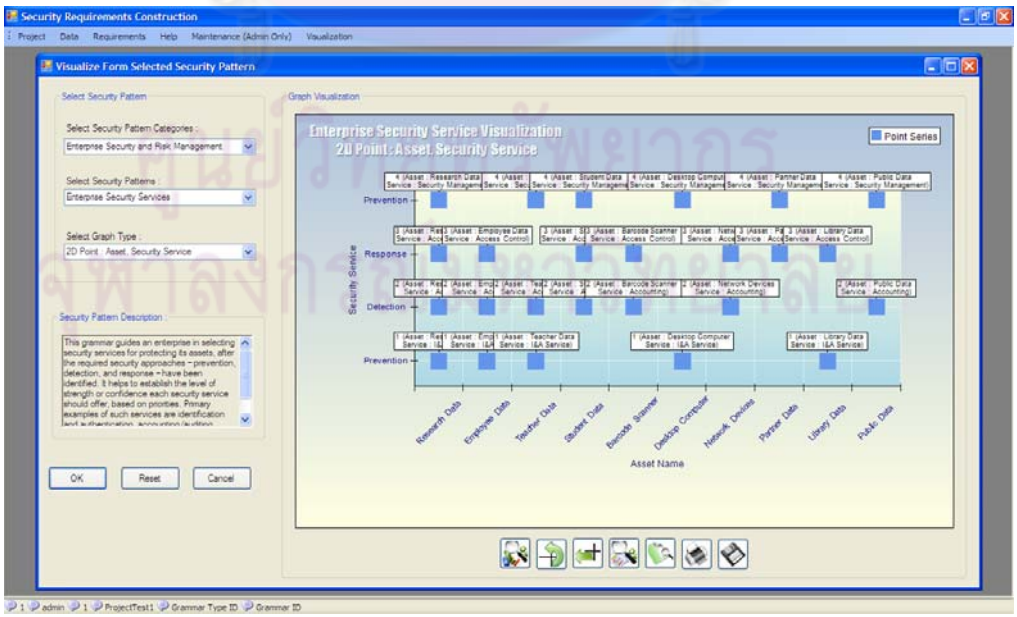
รูปที่ ช.5 ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปการกำหนดความเสี่ยง

(6) ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปแนวคิดความมั่นคงขององค์กร



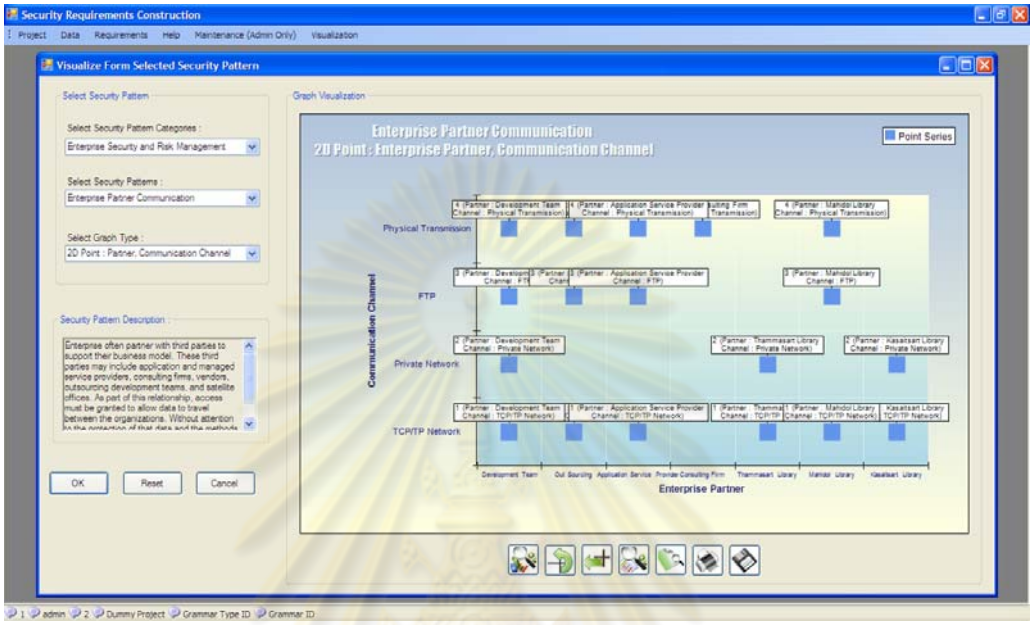
รูปที่ ช.6 ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปแนวคิดความมั่นคงขององค์กร

(7) ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปบริการความมั่นคงขององค์กร



รูปที่ ช.7 ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปบริการความมั่นคงขององค์กร

(8) ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปการสื่อสารของผู้มีหุ้นส่วนในองค์กร

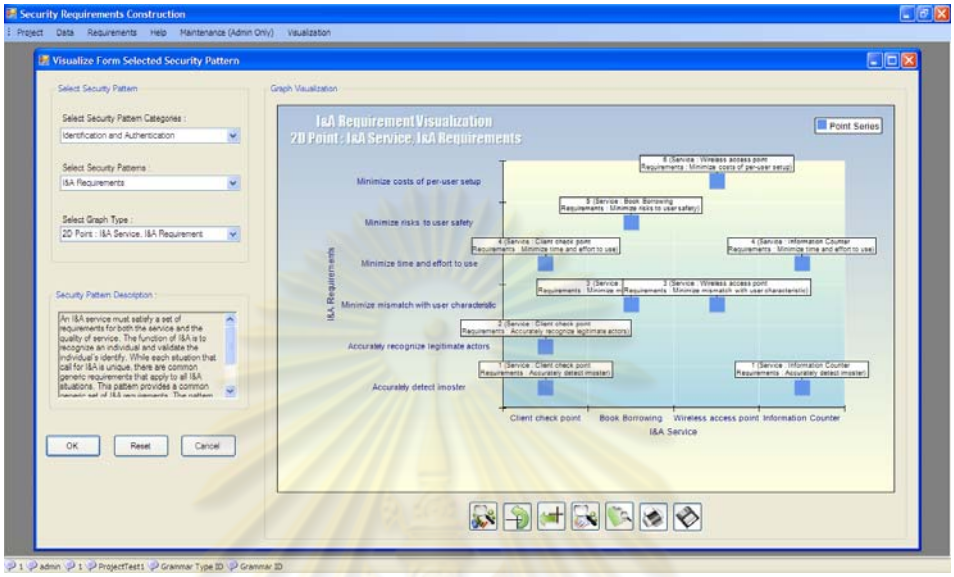


รูปที่ ช.8 ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปการสื่อสารของผู้มีหุ้นส่วนในองค์กร

2) กลุ่มการระบุตัวตนและการพิสูจน์ตัวจริง

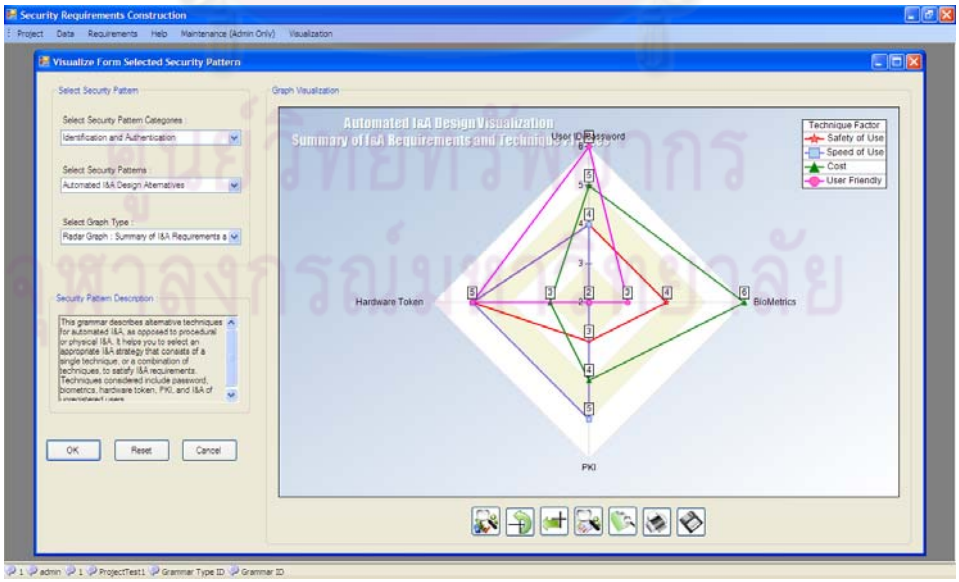
กลุ่มแบบรูปนี้จะเกี่ยวข้องกับการตรวจสอบปฏิสัมพันธ์ในเรื่องต่างๆ ระหว่างผู้ใช้งาน กับระบบ ซึ่งรองรับการบริการด้านการระบุและยืนยันตัวตนแบบต่างๆ ตามความต้องการที่ระบุไว้ในกลุ่มแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง ซึ่งรายการตัวอย่างผลลัพธ์ตามแบบรูปความมั่นคงในกลุ่มนี้ประกอบไปด้วย

(1) ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปความต้องการด้านการระบุและการพิสูจน์ตัวตน



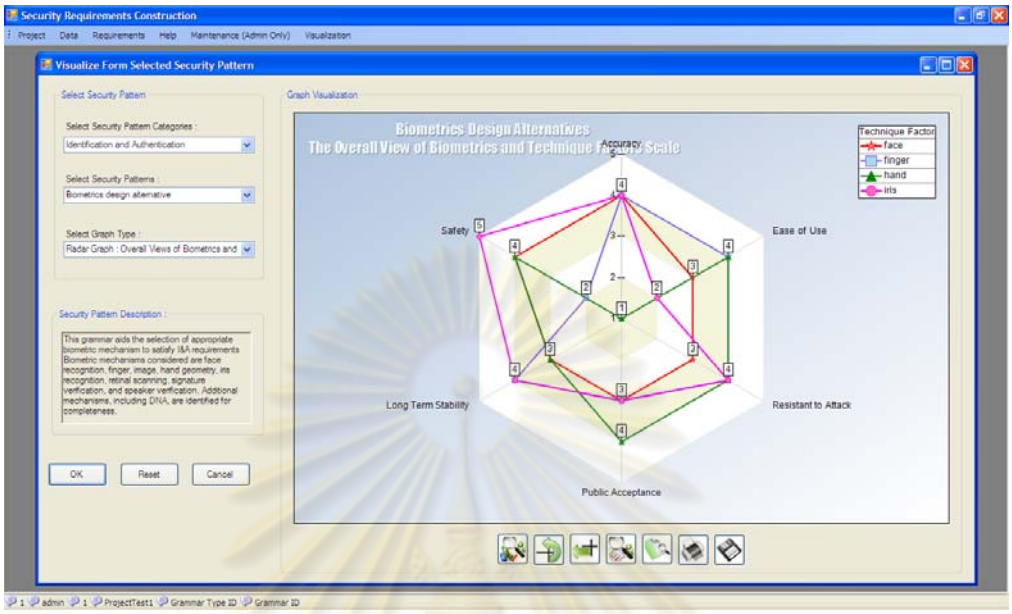
รูปที่ ช.9 ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปความต้องการด้านการระบุและการพิสูจน์ตัวตน

(2) ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปทางเลือกการออกแบบสำหรับการระบุและการพิสูจน์ตัวตนแบบอัตโนมัติ



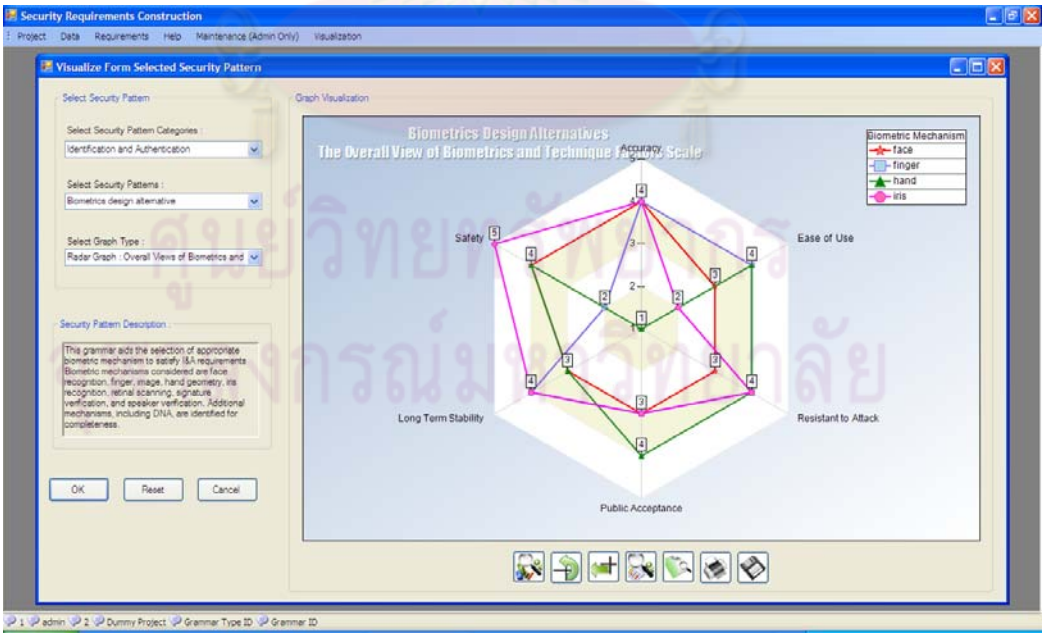
รูปที่ ช.10 ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปทางเลือกการออกแบบสำหรับการระบุและการพิสูจน์ตัวตนแบบอัตโนมัติ

(3) ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปการออกแบบและใช้รหัสผ่าน



รูปที่ ช.11 ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปการออกแบบและใช้รหัสผ่าน

(4) ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปทางเลือกการออกแบบสำหรับแบบชีวมิติ

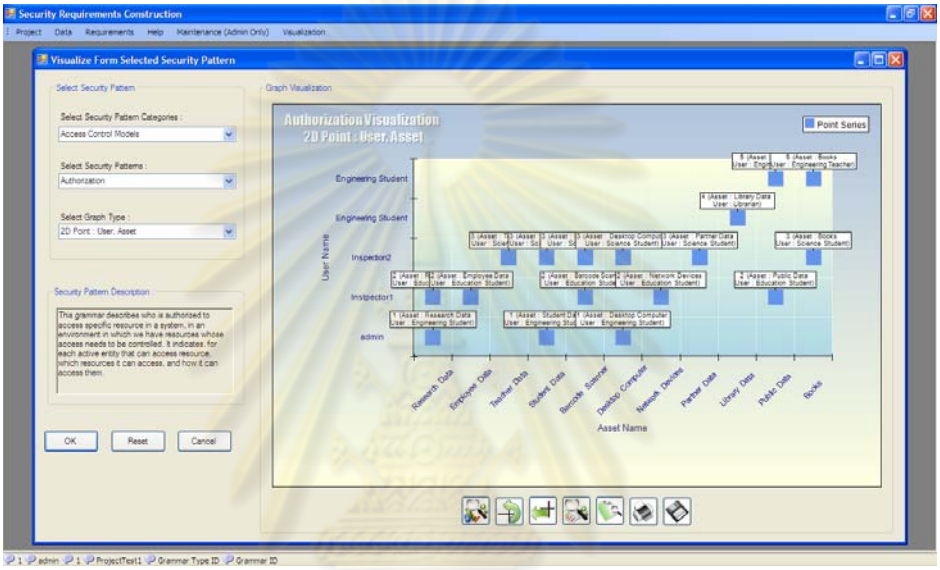


รูปที่ ช.12 ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปทางเลือกการออกแบบสำหรับแบบชีวมิติ

3) กลุ่มแบบจำลองควบคุมการเข้าถึง

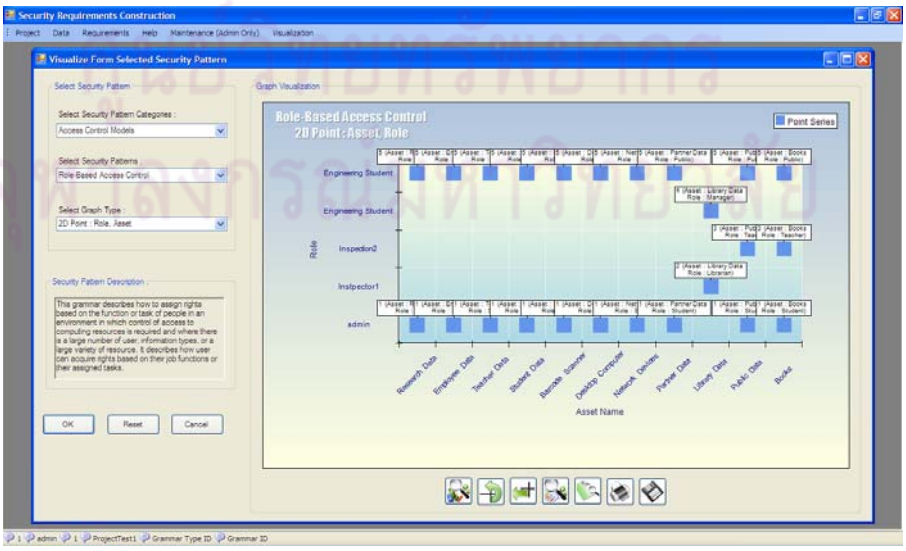
กลุ่มแบบรูปนี้จะเกี่ยวข้องกับการกำหนดเงื่อนไขบังคับ (Constraints) การเข้าถึงข้อมูลในระดับต่างๆ ไม่ว่าจะเป็นสถาปัตยกรรม โปรแกรมประยุกต์ และข้อบังคับของการปฏิบัติงาน ซึ่งรายการตัวอย่างผลลัพธ์ตามแบบรูปความมั่นคงในกลุ่มนี้ประกอบด้วย

(1) ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปการให้อำนาจ



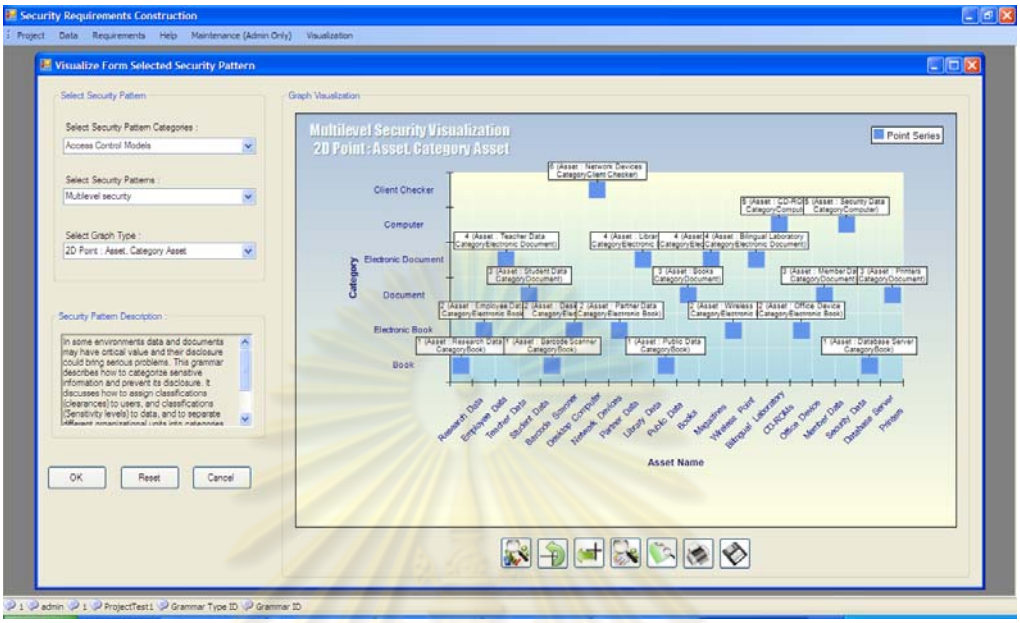
รูปที่ ช.13 ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปการให้อำนาจ

(2) ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปการควบคุมการเข้าถึงเชิงบทบาท



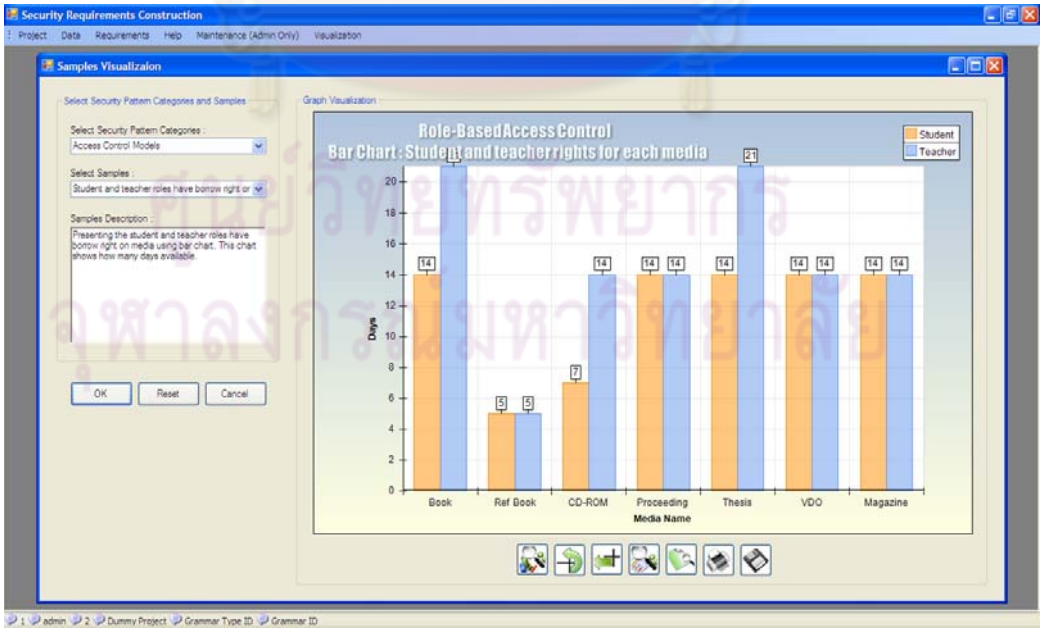
รูปที่ ช.14 ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปการควบคุมการเข้าถึงเชิงบทบาท

(3) ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปความมั่นคงหลายระดับ



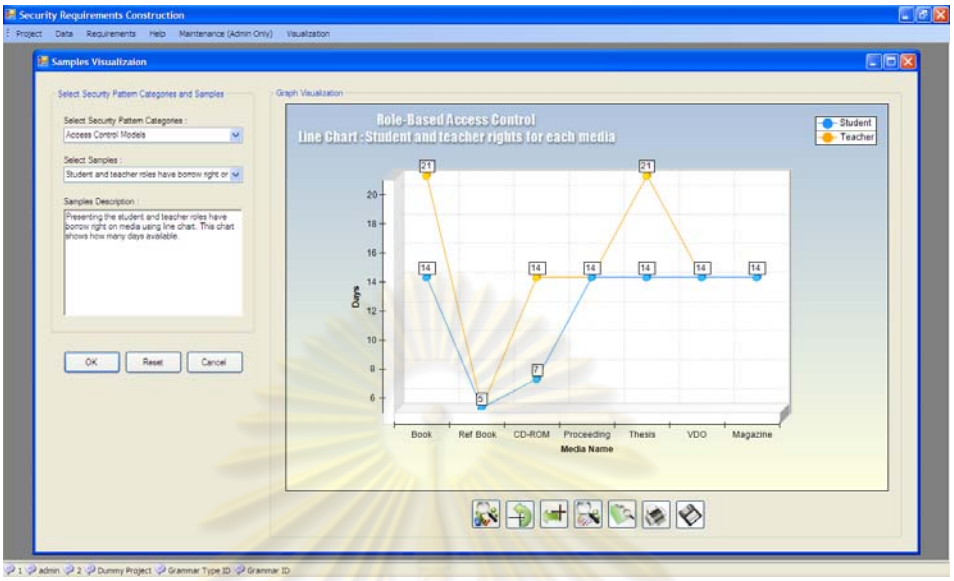
รูปที่ ช.15 ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปความมั่นคงหลายระดับ

(4) ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปการตรวจสอบการเข้าถึงทรัพยากร



รูปที่ ช.16 ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปการตรวจสอบการเข้าถึงทรัพยากร

(5) ตัวอย่างผลลัพธ์จากแบบรูปการกำหนดสิทธิ์ให้กับบทบาท

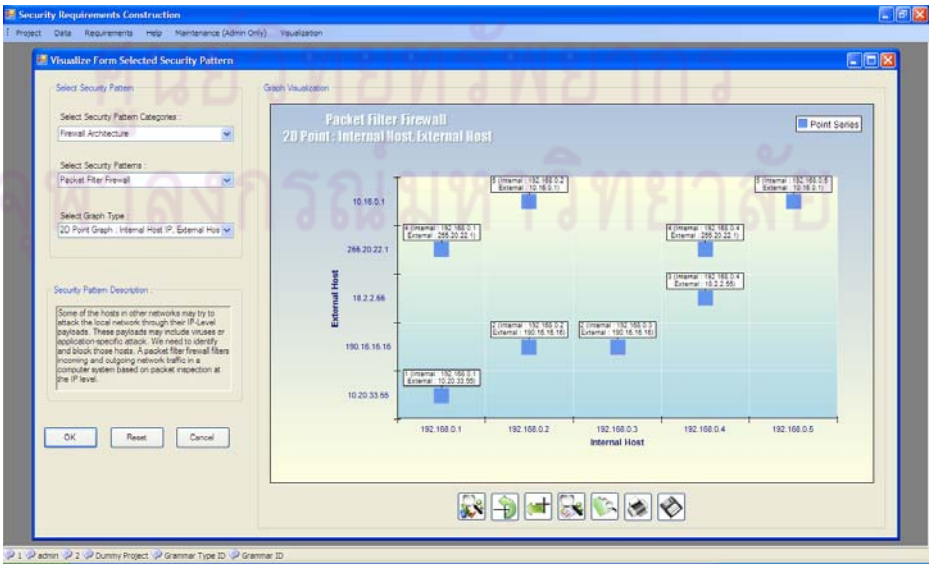


รูปที่ ช.17 ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปการกำหนดสิทธิ์ให้กับบทบาท

4) กลุ่มสถาปัตยกรรมไฟร์วอลล์

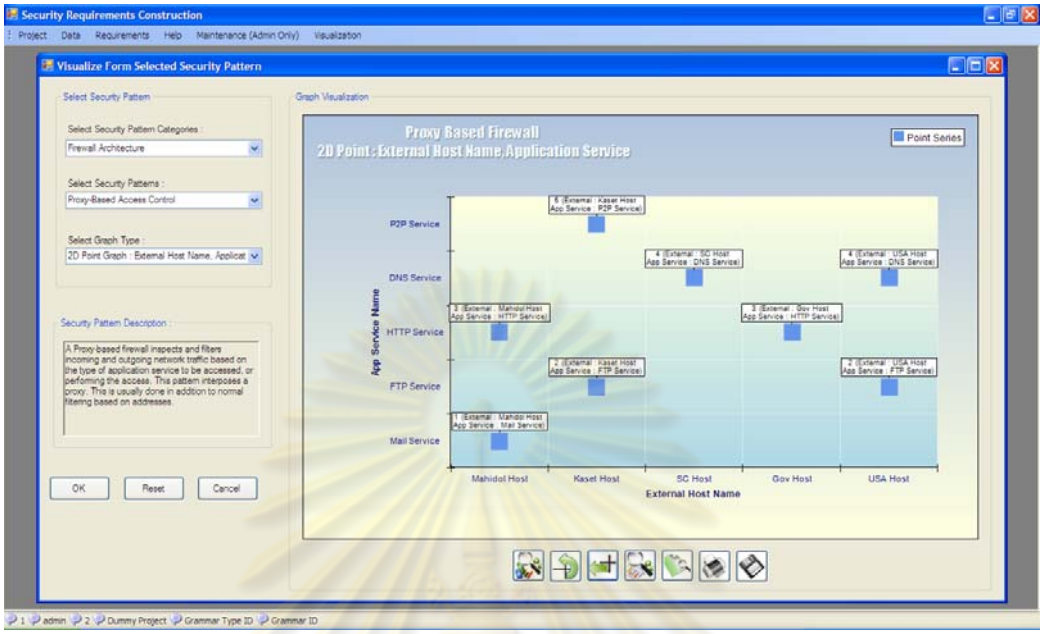
กลุ่มแบบรูปนี้เกี่ยวข้องกับการการกำหนดเงื่อนไขบังคับ สำหรับการติดต่อสื่อสารผ่านทางระบบเครือข่าย (Network) ทั้งนี้เพื่อป้องกันการโจมตีหรือปลอมปนทั้งจากภายนอกและภายในองค์กร ซึ่งรายการตัวอย่างผลลัพธ์ตามแบบรูปความมั่นคงในกลุ่มนี้ประกอบด้วย

(1) ตัวอย่างผลลัพธ์จากแบบรูปไฟร์วอลล์สำหรับการกรองแพ็คเกจ



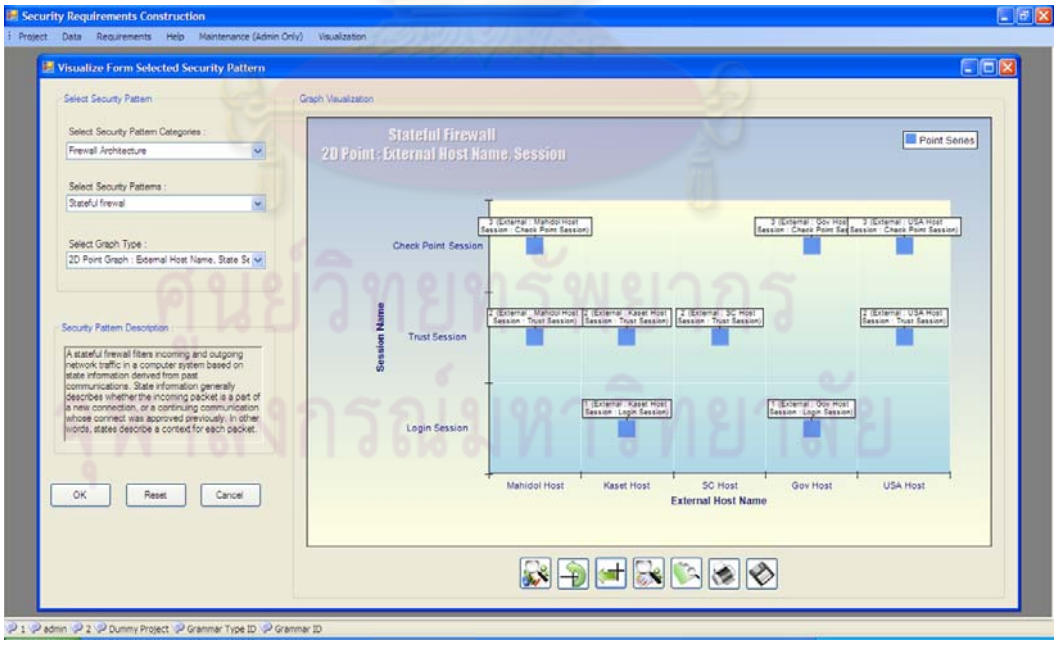
รูปที่ ช.18 ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปไฟร์วอลล์สำหรับการกรองแพ็คเกจ

(2) ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปไฟร์วอลล์เชิงตัวแทน



รูปที่ ช.19 ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปไฟร์วอลล์เชิงตัวแทน

(3) ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปไฟร์วอลล์เชิงสถานะ



รูปที่ ช.20 ตัวอย่างผลลัพธ์ภาพนามธรรมจากแบบรูปไฟร์วอลล์เชิงสถานะ

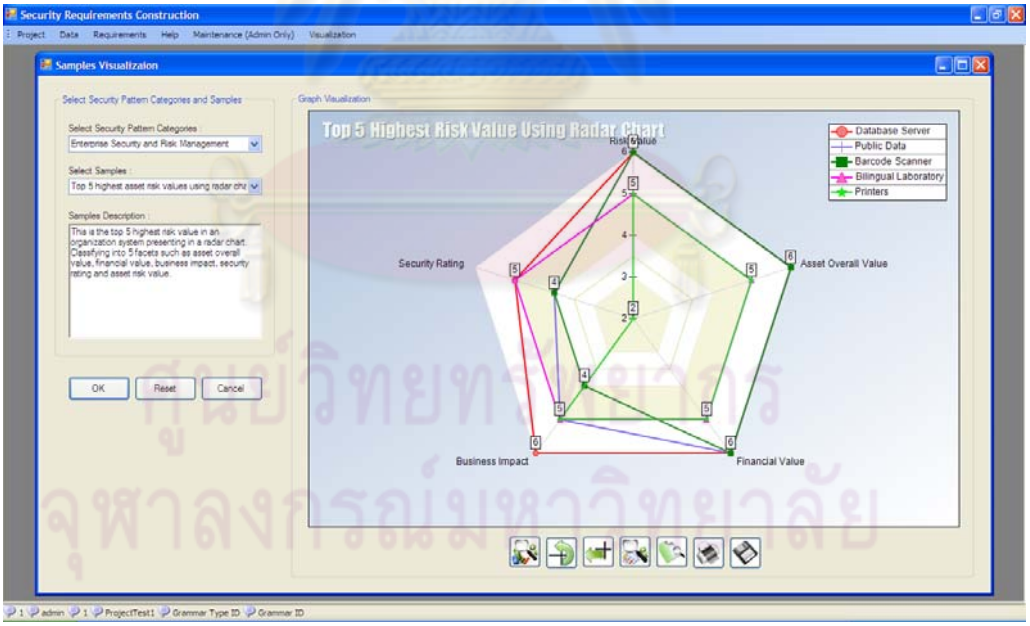
ช.2 ตัวอย่างผลลัพธ์ภาพนามธรรมที่ได้จากการเลือกจากตัวอย่างที่มีอยู่แล้ว

ผู้ใช้งานสามารถดูรายละเอียดรายการการสร้างภาพนามธรรมจากตัวอย่างที่มีอยู่แล้วได้ทั้งหมดจากตาราง 4.2 ในบทที่ 4 สำหรับการแสดงตัวอย่างผลลัพธ์ภาพนามธรรมในหัวข้อนี้ จะจำแนกตามกลุ่มของแบบรูปความมั่นคง มีรายละเอียดดังนี้

1) การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง

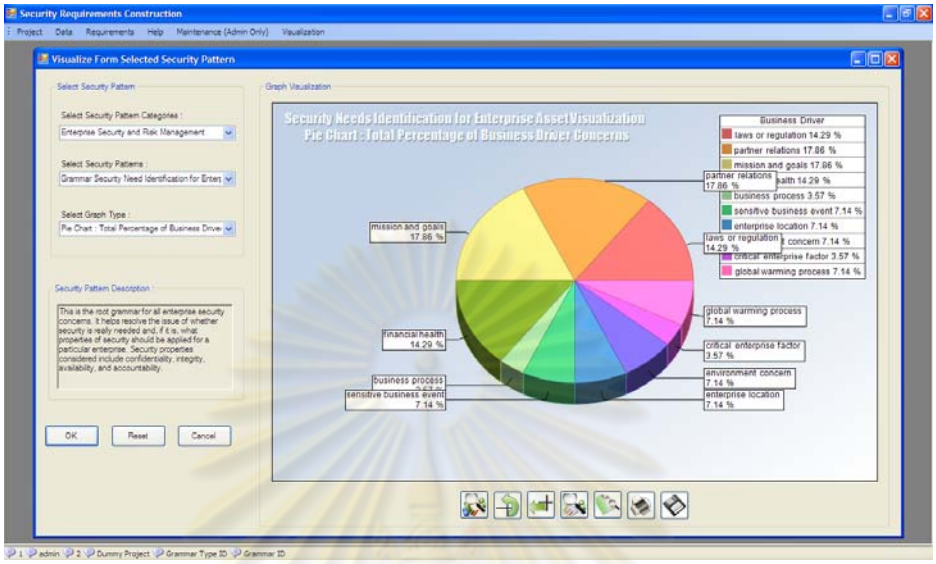
ในกลุ่มนี้จะยกตัวอย่างผลลัพธ์ภาพนามธรรมของตัวอย่าง “สินทรัพย์ที่มีความเสี่ยงสูงที่สุด 5 อันดับแรก โดยใช้แผนภูมิเรดาร์” (Top 5 highest asset risk value using radar chart) และ “การนำตัวขับเคลื่อนทางธุรกิจมากำหนดคุณสมบัติความมั่นคงองค์กร โดยจำแนกตามอัตราส่วนร้อยละ โดยใช้แผนภูมิรูปวงกลม” (Total percentage of business driver using pie chart)

(1) ตัวอย่างผลลัพธ์ภาพนามธรรมของตัวอย่างสินทรัพย์ที่มีความเสี่ยงสูงที่สุด 5 อันดับแรก โดยใช้แผนภูมิเรดาร์



รูปที่ ช.21 ตัวอย่างผลลัพธ์ภาพนามธรรมของตัวอย่างสินทรัพย์ที่มีความเสี่ยงสูงที่สุด 5 อันดับแรก โดยใช้แผนภูมิเรดาร์

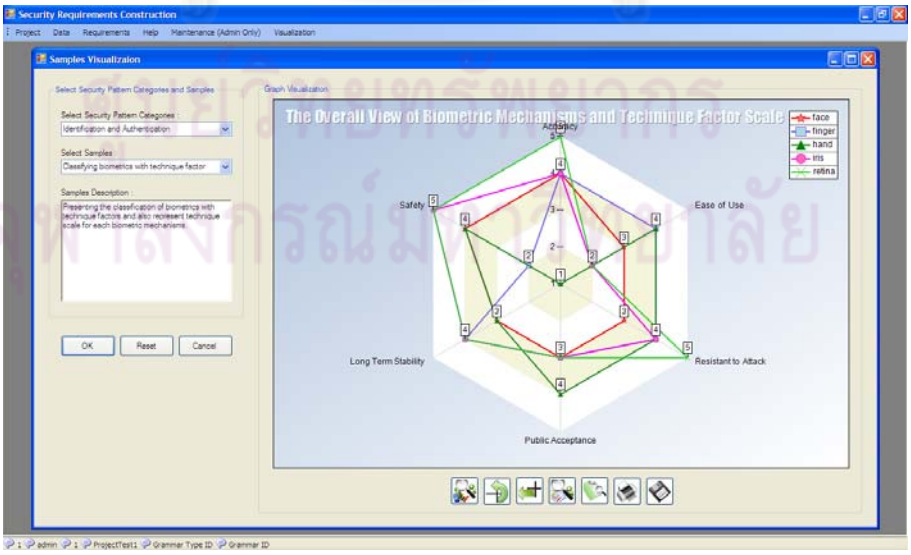
(2) ตัวอย่างผลลัพธ์ภาพนามธรรมของตัวอย่างการนำตัวขับเคลื่อนทางธุรกิจมากำหนดคุณสมบัติความมั่นคงองค์กร โดยใช้แผนภูมิรูปวงกลม



รูปที่ ช.22 ตัวอย่างผลลัพธ์ภาพนามธรรมของตัวอย่างการนำตัวขับเคลื่อนทางธุรกิจมากำหนดคุณสมบัติความมั่นคงองค์กร โดยใช้แผนภูมิรูปวงกลม

2) การระบุตัวตนและการพิสูจน์ตัวจริง

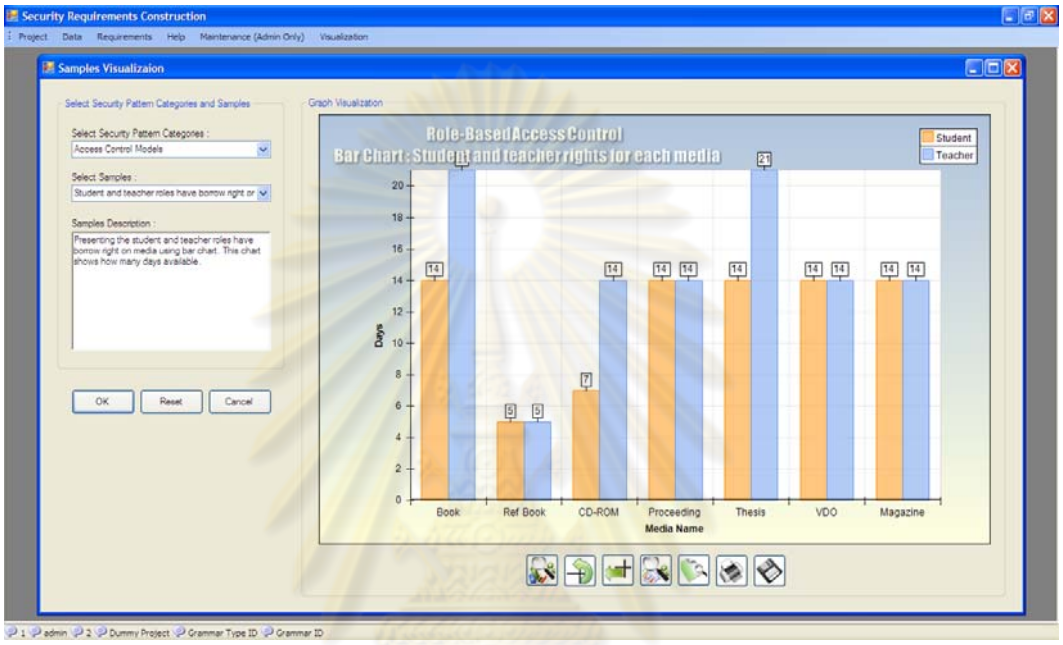
ในกลุ่มนี้จะยกตัวอย่างผลลัพธ์ภาพนามธรรมของตัวอย่างการจำแนกวิธีการระบุตัวตนและพิสูจน์ตัวจริงโดยใช้กลไกชีวมิติในปัจจัยต่างๆ (The overall view of biometric mechanisms and technique factor scale) โดยการใช้แผนภูมิเรดาร์



รูปที่ ช.23 ตัวอย่างผลลัพธ์ภาพนามธรรมของตัวอย่างการจำแนกวิธีการระบุตัวตนและพิสูจน์ตัวจริงโดยใช้กลไกชีวมิติในปัจจัยต่างๆ โดยใช้แผนภูมิเรดาร์

3) แบบจำลองควบคุมการเข้าถึง

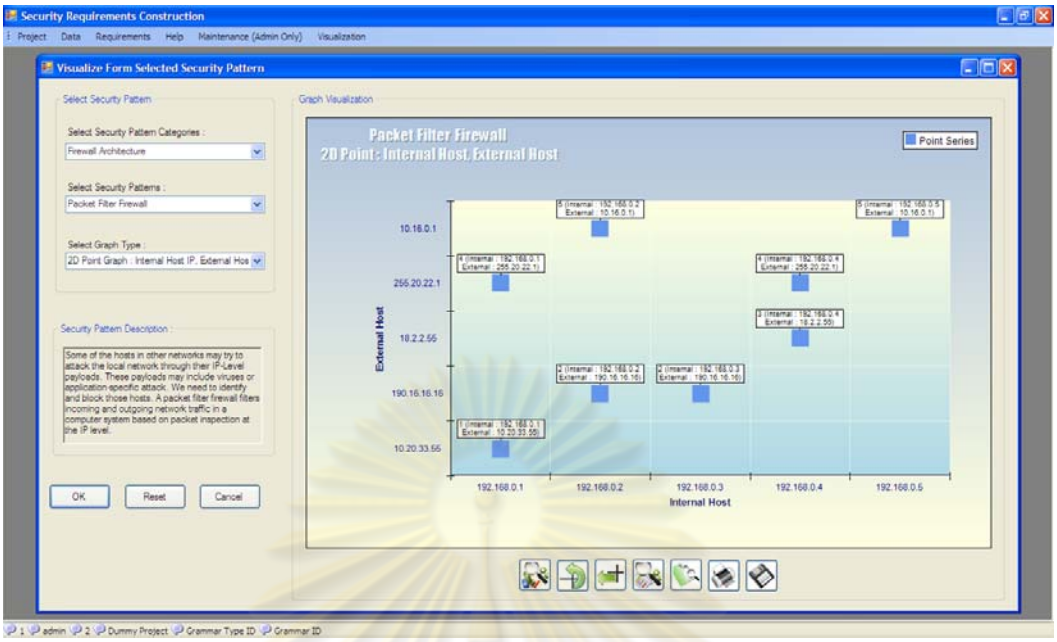
ในกลุ่มนี้จะยกตัวอย่างผลลัพธ์ภาพนามธรรมของตัวอย่างการกำหนดสิทธิการยืมสื่อประเภทต่างๆ ภายในห้องสมุดให้แก่บทบาทต่างๆ (Roles-based access control on for each media types)



รูปที่ ช.24 ตัวอย่างผลลัพธ์ภาพนามธรรมของตัวอย่างการกำหนดสิทธิการยืมสื่อประเภทต่างๆ ภายในห้องสมุดให้แก่บทบาทต่างๆ กัน

4) สถาปัตยกรรมไฟร์วอลล์

ในกลุ่มนี้จะยกตัวอย่างผลลัพธ์ภาพนามธรรมของตัวอย่างการติดต่อกันระหว่างองค์กรและโฮสภายนอกใดมีจำนวนมากที่สุด โดยใช้แผนภูมิแบบจุดสองมิติ (Summary of external host communicate with enterprise using pie chart)

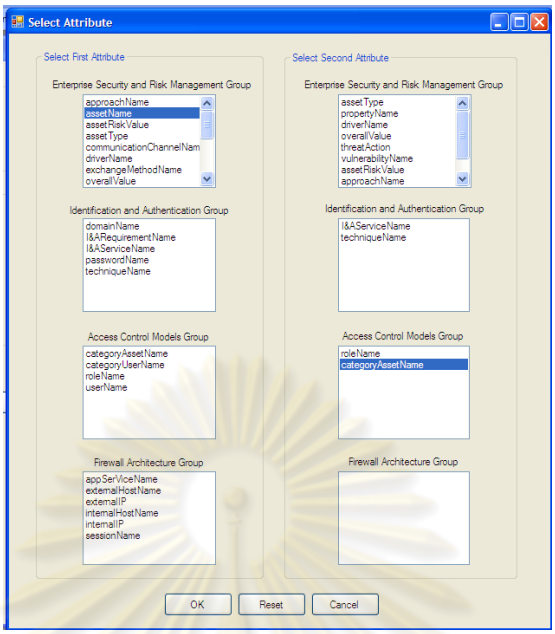


รูปที่ ช.25 ตัวอย่างผลลัพธ์ภาพนามธรรมของตัวอย่างการติดต่อกันระหว่างองค์กรและโฮสภายนอกใดมีจำนวนมากที่สุด โดยใช้แผนภูมิแบบจุดสองมิติ

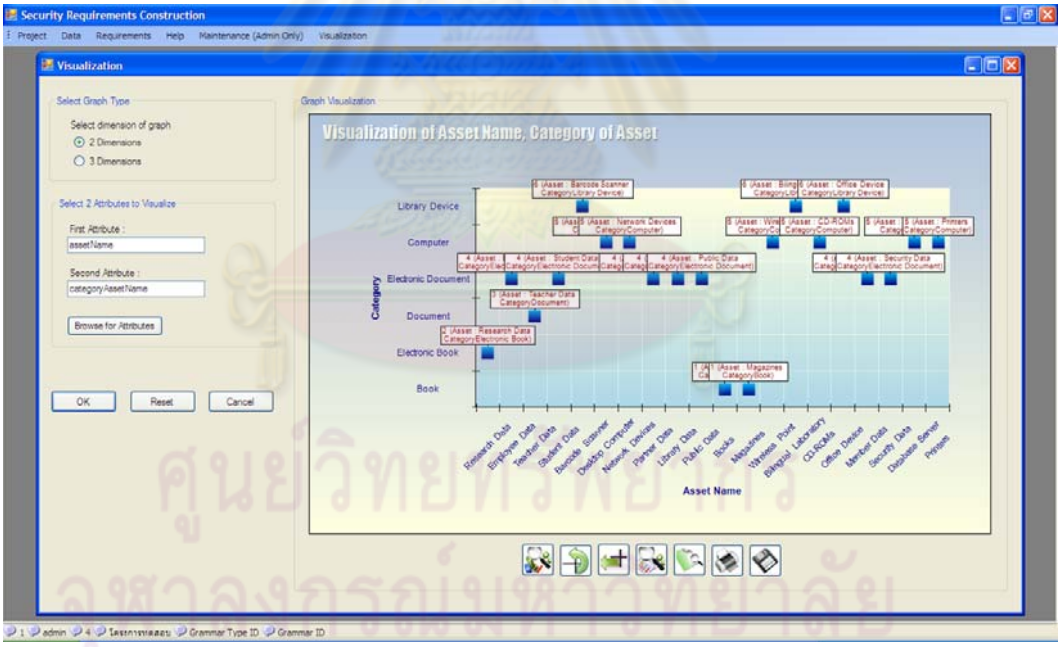
ช.3 ตัวอย่างผลลัพธ์ภาพนามธรรมที่ได้จากการเลือกจากข้อมูลลักษณะประจำ

ในการแสดงตัวอย่างผลลัพธ์ภาพนามธรรมที่ได้จากการเลือกจากข้อมูลลักษณะประจำจะจำแนกประเภทของแผนภูมิแบบสองมิติ และสามมิติ ซึ่งในแต่ละประเภทจะจำแนกตามกลุ่มของแบบรูปความมั่นคง ซึ่งมีรายละเอียดดังนี้

1) **ตัวอย่างผลลัพธ์ภาพนามธรรมแบบแผนภูมิแบบจุดสองมิติ** ที่ได้จากการเลือกจากข้อมูลลักษณะประจำใดๆ 2 ข้อมูล ทั้งนี้ผู้ใช้งานสามารถดูรายละเอียดรายการข้อมูลลักษณะประจำที่สามารถเลือกได้ทั้งหมดที่ภาคผนวก ค สำหรับการแสดงตัวอย่างผลลัพธ์ภาพนามธรรมในหัวข้อนี้จะยกตัวอย่างการเลือกข้อมูลลักษณะประจำ assetName จากกลุ่มของแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยงเป็นลักษณะประจำตัวแรก และเลือกข้อมูลลักษณะประจำ I&AServiceName เป็นลักษณะประจำตัวที่สอง จากกลุ่มของแบบรูปการระบุตัวตนและการพิสูจน์ตัวจริง โดยหน้าจอการเลือกลักษณะประจำแสดงได้ดังรูปที่ ช.26 และสามารถแสดงผลแผนภูมิแบบจุดสองมิติได้ในรูปที่ ช.27



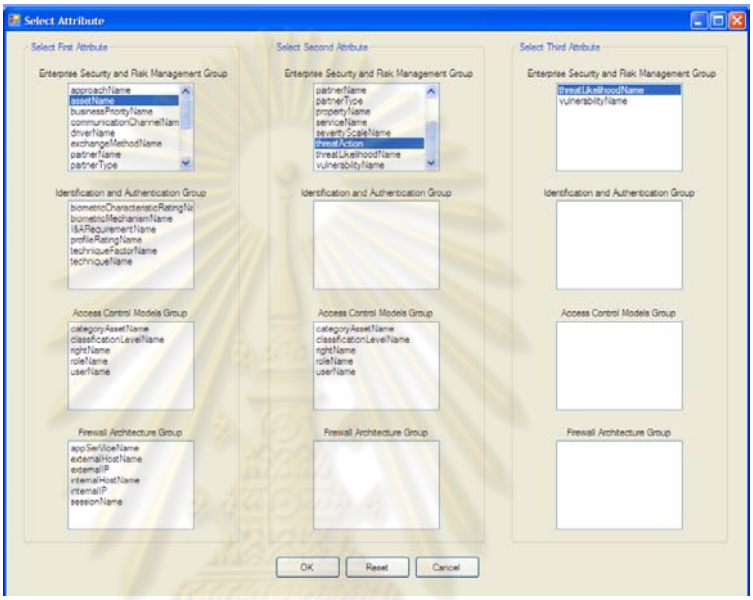
รูปที่ ช.26 หน้าจอการเลือกลักษณะประจำ assetName และ categoryAssetName



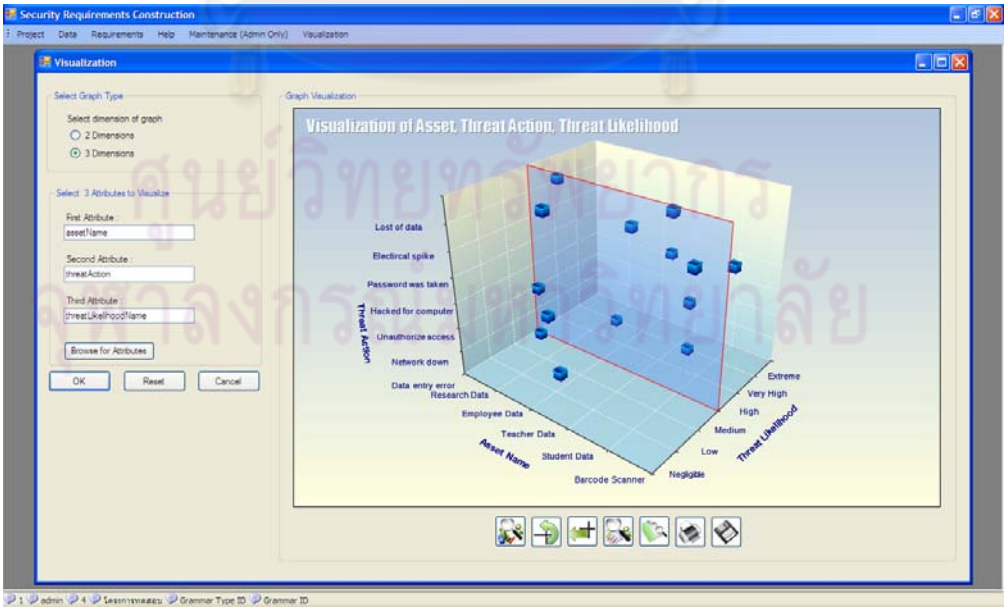
รูปที่ ช.27 ตัวอย่างผลลัพธ์แผนภูมิแบบจุดสองมิติของลักษณะประจำ assetName และ categoryAssetName

2) **ตัวอย่างผลลัพธ์ภาพนามธรรมแบบแผนภูมิแบบจุดสามมิติ** ที่ได้จากการเลือกจากข้อมูลลักษณะประจำใดๆ 3 ข้อมูล ทั้งนี้ผู้ใช้งานสามารถดูรายละเอียดรายการข้อมูลลักษณะประจำที่สามารถเลือกได้ทั้งหมดที่ภาคผนวก ง สำหรับการแสดงตัวอย่างผลลัพธ์ภาพนามธรรม

ในหัวข้อนี้จะยกตัวอย่างการเลือกข้อมูลลักษณะประจำ assetName เลือกข้อมูลลักษณะประจำ threatAction เป็นลักษณะประจำตัวที่สอง และเลือกข้อมูลลักษณะประจำ threatlikelihood จากกลุ่มของแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยงเป็นลักษณะประจำตัวที่สาม โดยหน้าจอการเลือกลักษณะประจำแสดงได้ดังรูปที่ ช.28 และสามารถแสดงผลแผนภูมิแบบจุดสามมิติได้ในรูปที่ ช.29



รูปที่ ช.28 หน้าจอการเลือกลักษณะประจำ assetName threatAction และ threatlikelihood



รูปที่ ช.29 ตัวอย่างผลลัพธ์แผนภูมิแบบจุดสามมิติของลักษณะประจำ assetName threatAction และ threatlikelihood

ภาคผนวก ญ

การนำข้อมูลเข้าสู่เครื่องมือต้นแบบการสร้างภาพนามธรรม

ในภาคผนวก ญ นี้ แสดงตารางสรุปตารางข้อมูลหลัก และตารางข้อมูลความสัมพันธ์ของแบบรูปความมั่นคง ดังปรากฏในตาราง ญ.1 และลำดับขั้นตอนการนำข้อมูลเข้าสู่เครื่องมือต้นแบบการสร้างภาพนามธรรมสามารถแสดงได้ดัง ตาราง ญ.2

ตารางที่ ญ.1 ความสัมพันธ์ของแบบรูปความมั่นคง [8]

	GM61	GM62	GM63	GM64	GM65	GM66	GM67	GM68	GM71	GM72	GM73	GM74	GM82	GM83	GM84	GM85	GM121	GM122	GM123
GM61																			
GM62	AssetName																		
GM63	AssetName																		
GM64			ThreatName																
GM65	AssetName	AssetValue	LikelihoodScale	SeverityScale															
GM66	AssetName				RiskValue		Included												
GM67	AssetName																		
GM68	AssetName								IAServivce										
GM71										Include	Include	Include							
GM72									IA Service										
GM73										IA Service + Password									
GM74										IA Service + Biometric									
GM81	AssetName																		
GM82	AssetName															AuthorizedRole			
GM83	AssetName																		
GM84	AssetName															Include			
GM85	AssetName																		
GM121	AssetName																	Include	Include
GM122	AssetName																		
GM123	AssetName																		

GM61 การระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร (Security Needs Identification for Enterprise Assets)

GM62 การกำหนดมูลค่าสินทรัพย์ (Asset Valuation)

GM63 การประเมินภัยคุกคาม (Threat Assessment)

GM64 การประเมินภาวะเสี่ยง (Vulnerability Assessment)

GM65 การกำหนดความค่าความเสี่ยง (Risk Determination)

GM66 แนวคิดความมั่นคงองค์กร (Enterprise Security Approaches)

GM67 บริการความมั่นคงองค์กร (Enterprise Security Services)

GM68 การสื่อสารของผู้มีหุ้นส่วนองค์กร (Enterprise Partner Communication)

GM71 ความต้องการการระบุและการพิสูจน์ตัวตน (I&A Requirements)

GM72 ทางเลือกการออกแบบการระบุและการพิสูจน์ตัวตน (Automated I&A Design Alternative)

GM73 การออกแบบและใช้งานรหัสผ่าน (Password Design and Use)

GM74 ทางเลือกการออกแบบชีวมิติ (Biometric Design Alternative)

GM81 การให้อำนาจ (Authorization)

GM82 การควบคุมการเข้าถึงเชิงบทบาท (Role-Based Access Control)

GM83 ความมั่นคงหลายระดับ (Multilevel Security)

GM84 การเฝ้าสังเกตเชิงอ้างอิง (Reference Monitor)

GM85 การนิยามสิทธิ์ให้กับบทบาท (Role Rights Definition)

GM121 ไฟล์วอลล์กรองแพ็คเกจ (Packet Filter Firewall)

GM122 ไฟล์วอลล์เชิงตัวแทน (Proxy-Based Firewall)

GM123 ไฟล์วอลล์เชิงสถานะ (Stateful Firewall)

ตารางที่ ญ.2 ลำดับขั้นตอนการนำข้อมูลเข้าสู่เครื่องมือต้นแบบการสร้างภาพนามธรรม

รหัสแบบรูปความมั่นคง	ตารางข้อมูลหลัก	ตารางข้อมูลความสัมพันธ์	หมายเหตุ
P61	tbAsset tbSecurityProperty tbBusinessDriver tbAssetType	tb61	เป็นแบบรูปพื้นฐาน ในการกำหนดความต้องการควรเริ่มต้นจากแบบรูปนี้
P62	-	tbGM62	
P63	tbThreat tbThreatSource	tb63Vis tbThreat_ThreatSource	
P64	tbVul	tbAsset_Threat_Vul	
P65	-	tbGM65	
P66	tbSecurityAppr	tb66Vis	
P67	tbService	tb66Vis	
P68	tbPartner tbPartnerType tbExchangeMethod tbServiceTermination tbCommunicationChannel	tbCommu_Exchange tbPartner_Commu	
P71	tbIADomain tbIAService tbIARequirement	tbAsset_IAService tbIAService_Req	
P72	tbIATechnique tbIAReqProfile tbDomainFactor	tbService_Technique tbIAReqProfileRelation	
P73	tbPassword		
P74	tbBiometric tbIATechniqueFactor	tbIATechnique_Bio	
P81	tbMemberUser tbRight	tbAsset_User_Right	

ตารางที่ ญ.2 ลำดับขั้นตอนการนำข้อมูลเข้าสู่เครื่องมือต้นแบบการสร้างภาพนามธรรม (ต่อ)

รหัสแบบรูปความมั่นคง	ตารางข้อมูลหลัก	ตารางข้อมูลความสัมพันธ์	หมายเหตุ
P82	tbRole	tbMemberUser_Role	
	tbMedia	tbBorrowMediaStudent	
	tbDay	tbBorrowMediaTeacher	
P83	tbCategoryAsset	tbAsset_Category	
	tbCategoryUser	tbMemberUserCategory	
	tbClassificationLevel		
P84	-	-	
P85	-	-	
P121	tbFirewallExternalHost	tbFirewall121	
	tbFirewallInternalHost		
P122	tbFirewallAppService	tbFirewall122	
P123	tbFirewallSession	tbFirewall123	

ประวัติผู้เขียนวิทยานิพนธ์

นางสาววีริยา สุภาณิชย์ เกิดเมื่อวันที่ 3 พฤศจิกายน พ.ศ. 2526 สำเร็จการศึกษาปริญญาบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์ จากคณะวิทยาศาสตร์ จากมหาวิทยาลัยบูรพา ในปีการศึกษา 2547 และเข้าศึกษาต่อระดับปริญญามหาบัณฑิต สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ในปีการศึกษา 2549