ระบบบริหารจัดการและควบคุมการเข้าถึงอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์แบบอัตโนมัติตามมาตรฐาน ISO/IEC 27001 : 2013

Configuration and Access Control Automating Systems for Computer Network Switches Based on ISO/IEC 27001:2013 Standard

ธนากร สิทธิพล[1] ขจิตพรรณ กฤตพลวิมาน[1] และเตชค์ฐสิณป์ เพียซ้าย[1]*

Thanakorn Sittipol[1] , Khajitpan Kritpolviman[1] and Tejtasin Phiasai[1]*

รับบทความ 27 มกราคม 2565/ ปรับแก้ไข 17 มีนาคม 2565/ ตอบรับบทความ 21 เมษายน 2565

Received: January 27, 2022/ Revised: March 17, 2022/ Accepted: April 21, 2022

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์เพื่อ 1) พัฒนาระบบบริหารจัดการและควบคุมการเข้าถึงอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์แบบอัตโนมัติตามมาตรฐาน ISO/IEC 27001:2013 2) ประเมินประสิทธิภาพระบบบริหารจัดการและควบคุมการเข้าถึงอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์แบบอัตโนมัติ การวิจัยดำเนินการโดยวิเคราะห์และประเมินความเสี่ยงด้านความมั่นคงปลอดภัยระบบเครือข่ายคอมพิวเตอร์ตามมาตรฐาน ISO/IEC 27001:2013 จากนั้นทำการออกแบบและพัฒนาระบบบริหารจัดการและควบคุมการเข้าถึงอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ที่มีฟังก์ชันการทำงานแบบอัตโนมัติได้แก่ ฟังก์ชันการบริหารจัดการ ฟังก์ชันการตรวจสอบสถานะ และฟังก์ชันการแจ้งเตือน โดยพัฒนาระบบให้มีกระบวนทำงานแบบอัตโนมัติ ด้วยมายเอสคิวแอล ภาษาพีเอชพีและภาษาไพธอนในรูปแบบเจสันที่สามารถทำงานร่วมกับโพรโทคอลเอสเอ็นเอ็มพี ระบบที่พัฒนาถูกนำไปติดตั้งและทดสอบการใช้งานจำนวน 5 สถานการณ์ เพื่อประเมินประสิทธิภาพด้านการทำงานแบบอัตโนมัติและเป็นไปตามมาตรฐาน ISO/IEC 27001:2013 ผลการวิจัยพบว่าผลการประเมินประสิทธิภาพการทำงานแบบอัตโนมัติโดยรวมอยู่ในระดับมากที่สุด ($\bar{X}$ = 4.51, S.D. = 0.49) และระบบที่พัฒนาสามารถลดระดับความเสี่ยงด้านความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27001:2013 หมวด A.9.4 การควบคุมการเข้าถึงระบบและแอปพลิเคชันอยู่ในระดับต่ำมากในทุกๆ ประเด็นความเสี่ยง

คำสำคัญ: อุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ ระบบอัตโนมัติ ISO/IEC 27001:2013

[1]แขนงวิชาเทคโนโลยีสารสนเทศและการสื่อสาร สาขาวิชาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช จังหวัดนนทบุรี 11120

[1]Information and Communication Technology, School of Science and Technology, Sukhothai Thammathirat Open University, Nonthaburi 11120

*Corresponding author email: Khajitpan.Mak@stou.ac.th

Abstract

The purposes of this research were to 1) develop the configuration and access control automating systems for computer network switches based on ISO/IEC 27001:2013 standard, and 2) evaluate the performance of the configuration and access control automating systems for computer network switches. The research was conducted by analysis and security risk assessment of computer networks based on ISO/IEC 27001:2013 standard. Then the configuration and access control systems for computer network switches were designed and developed comprising automating functions such as configuration, status monitoring, and notification. Such automating procedures were generated by MySQL, PHP and Python programming in JSON format and operated with SNMP protocol. The developed configuration and access control automating systems were installed and implemented in 5 test cases to evaluate automating performance regarding ISO/IEC 27001:2013 standard. Consequently, the results showed that the overall performance of the developed systems in automation aspects was at the highest level ($\overline{x}$ = 4.51, S.D. = 0.49), and security risk assessment level corresponding to ISO 27001: 2013 Annex A.9.4 System and Application Access Control was degraded to the very low level (VL) in all risk aspects.

Keywords: Network switches, Automating systems, ISO/IEC 27001:2013

บทนำ

ในปัจจุบันองค์กรต่างๆ ทั้งภาครัฐ ภาคเอกชน และสถาบันการศึกษาต่างๆ ได้มีการสำรวจ วิเคราะห์และปรับปรุงระบบนิเวศน์เชิงดิจิทัลและโครงสร้างพื้นฐาน (Digital Eco-Systems and Infrastructure) ขององค์กรให้พร้อมสำหรับการปรับเปลี่ยนทางดิจิทัล (Digital Transformation) โดยเฉพาะอย่างยิ่งระบบเครือข่ายคอมพิวเตอร์ซึ่งเป็นโครงข่ายสื่อสารพื้นฐานที่ถูกวิเคราะห์ออกแบบ และขยายระบบเครือข่ายคอมพิวเตอร์ให้มีขนาดใหญ่ขึ้นหรือมีความเหมาะสมต่อการปรับเปลี่ยนและลักษณะการให้บริการแพลตฟอร์มดิจิทัลของแต่ละองค์กร ทำให้เกิดการใช้อุปกรณ์ต่างๆ ในระบบเครือข่ายคอมพิวเตอร์ร่วมกัน เช่น ฮับ เราท์เตอร์ อุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์หรือสวิตช์ เป็นต้น ส่วนใหญ่อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์ที่พบเห็นในแต่ละองค์กรมีการใช้อุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่ในการเชื่อมต่อระบบต่างๆ ภายในระบบเครือข่ายคอมพิวเตอร์ซึ่งอาจประสบปัญหาเกี่ยวกับการชนกันของข้อมูลในระบบเครือข่ายคอมพิวเตอร์ได้หากไม่มีระบบบริหารจัดการเครือข่ายคอมพิวเตอร์ โดยเฉพาะอย่างยิ่งองค์กรในหน่วยงานภาครัฐที่มีการติดต่อสื่อสารแลกเปลี่ยนข้อมูลความลับทางราชการระดับชั้นต่างๆ มีการปรับปรุงระบบนิเวศน์เชิงดิจิทัลและโครงสร้างพื้นฐานขององค์กร ควรมีระบบบริหารจัดการเครือข่ายคอมพิวเตอร์ที่มีความมั่นคงปลอดภัยจากการเข้าถึงโดยบุคคลภายนอกโดยไม่ได้รับอนุญาต สามารถกำหนดตรวจสอบผู้ที่มีสิทธิ์เข้าถึงอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ได้ เพื่อป้องกันการโจรกรรมข้อมูลขององค์กร ข้อมูลส่วนบุคคล และป้องกันการเข้าถึงและเปลี่ยนแปลงข้อมูลของเครือข่ายคอมพิวเตอร์ เช่น IP Address MAC Address และ IP Gateway เป็นต้น

ผู้วิจัยได้สำรวจหน่วยงานแห่งหนึ่งที่สังกัดกองบัญชาการกองทัพไทยที่มีแผนการปรับปรุงระบบนิเวศน์เชิงดิจิทัลขององค์กร หน่วยงานดังกล่าวได้อนุญาตให้บุคคลภายนอกที่ได้รับมอบหมายสามารถเข้าถึงระบบเครือข่ายภายในจากระยะไกล (Remote Access) ด้วยโปรแกรมสำเร็จรูปที่ไม่สามารถบันทึกรูปแบบคำสั่งสำหรับซ่อมบำรุงหรือดูแลรักษาระบบเครือข่ายคอมพิวเตอร์ขององค์กร สามารถตั้งค่าต่างๆ ของอุปกรณ์เครือข่ายคอมพิวเตอร์ เพิ่มอุปกรณ์ สามารถเข้าพื้นที่เพื่อ

ปฏิบัติการตามเวลาที่กำหนด และยังใช้ทรัพยากรสารสนเทศหรือไฟล์ข้อมูลร่วมกับบุคลากรภายใน ปัจจัยต่างๆ เหล่านี้เป็นความเสี่ยงด้านความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ อาจเกิดช่องโหว่ต่อระบบเครือข่ายคอมพิวเตอร์ส่งผลให้ถูกโจมตีหรือถูกขโมยข้อมูลสำคัญได้ ระบบเครือข่ายคอมพิวเตอร์องค์กรอาจเกิดความเสียหายหากผู้ดูแลระบบที่เป็นบุคลากรภายในไม่ได้ติดตามการเข้าถึงระบบและการปฏิบัติการซ่อมบำรุงต่างๆ ที่ดำเนินการโดยหน่วยงานซ่อมบำรุงจากภายนอก ความเสี่ยงดังกล่าวอาจส่งผลต่อการรักษาความลับ ความพร้อมใช้งาน และความสมบูรณ์ของสินทรัพย์ของหน่วยงาน ซึ่งการนำมาตรฐาน ISO/IEC 27001 : 2013 มาใช้เป็นข้อกำหนดสำหรับการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ส่งผลให้การรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กรมีประสิทธิผลและประสิทธิภาพมากขึ้น ทำให้องค์กรทราบสถานะปัจจุบันเกี่ยวกับความปลอดภัยของข้อมูล (Fonseca-Herrera, Rojas, & Florez, 2018) และสามารถดำเนินการควบคุมควบการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ขององค์กรได้อย่างเป็นระบบและมีประสิทธิภาพ

ดังนั้นคณะผู้วิจัยจึงมีแนวคิดในการพัฒนาระบบบริหารจัดการและควบคุมการเข้าถึงอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์แบบอัตโนมัติ (Automation) สำหรับใช้เป็นระบบต้นแบบติดตั้งภายในองค์กรให้มีการบริหารจัดการ ควบคุม และตรวจสอบการเข้าถึงอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ทั้งจากภายในองค์กรและเข้าถึงจากระยะไกลได้อย่างอัตโนมัติ โดยพัฒนาระบบด้วยภาษา PHP และ Python ทำงานร่วมกับ SNMP Protocol ในการบริหารจัดการ การตรวจสอบสถานะ และการแจ้งเตือนเกี่ยวกับสถานะอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ (Safrianti, Sari, & Sari, 2021) ให้มีความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27001 : 2013 มีการบริหารจัดการและการควบคุมการเข้าถึงอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์แบบอัตโนมัติ ประเมินประสิทธิภาพและวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยตามแนวทางการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของหน่วยงานที่สังกัดกองบัญชาการกองทัพไทยซึ่งเป็นไปตามกรอบมาตรฐาน ISO/IEC 27001:2013 (ณรงค์ฤทธิ์ วังคีรี, 2563)

วัตถุประสงค์การวิจัย

1. เพื่อพัฒนาระบบบริหารจัดการและควบคุมการเข้าถึงอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์แบบอัตโนมัติ ตามมาตรฐาน ISO/IEC 27001 : 2013
2. เพื่อประเมินประสิทธิภาพระบบบริหารจัดการและควบคุมการเข้าถึงอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์แบบอัตโนมัติ

เอกสารและงานวิจัยที่เกี่ยวข้อง

คณะผู้วิจัยได้ศึกษาเอกสารและงานวิจัยต่างๆ สำหรับแก้ปัญหาโจทย์วิจัยตามวัตถุประสงค์การวิจัยข้างต้น เช่น Khan and Khan (2017) ได้ออกแบบและใช้งานระบบตรวจสอบและการรายงานแบบเครือข่ายอัตโนมัติ โดยใช้ Universal Plug and Play (UPnP) Protocol บนอุปกรณ์ควบคุมที่สนับสนุน UPnP เช่น อุปกรณ์กระจายสัญญาณหรือสวิตช์เครือข่ายคอมพิวเตอร์หรืออุปกรณ์อื่นๆ ที่เข้าถึงได้โดยตรงจากผู้ให้บริการเครือข่าย (ISP) ด้วยการเปิดพอร์ตหรือกำหนดพารามิเตอร์ที่สามารถทำงานได้แบบอัตโนมัติ สำหรับตรวจสอบและรายงานสถานะเครือข่ายคอมพิวเตอร์แก่ผู้ดูแลระบบได้โดยอัตโนมัติผ่านข้อความแจ้งเตือน ทำให้ผู้ดูแลระบบทราบถึงประเภทและตำแหน่งข้อผิดพลาดที่เกิดขึ้นทันที

Safrianti, Sari, and Sari (2021) ได้พัฒนาระบบตรวจสอบอุปกรณ์เครือข่ายแบบเรียลไทม์ด้วย SNMP Protocol สำหรับการจัดการและตรวจสอบเครือข่ายในหน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ระบบที่พัฒนาขึ้นทำให้ผู้ดูแลระบบเครือข่ายสามารถตรวจสอบและควบคุมอุปกรณ์เครือข่าย โดยใช้ภาษา PHP และ MySQL ร่วมกับ SNMP Protocol สำหรับรวบรวมและจัดเรียงข้อมูลอุปกรณ์ในระบบเครือข่าย มีการแสดงผลข้อมูลการจัดการ

เครือข่ายในรูปแบบของสถานะ Up-Down และปริมาณการใช้ข้อมูลบนอุปกรณ์เครือข่าย ระบบสามารถแจ้งเตือนในรูปแบบเสียงเมื่ออุปกรณ์เครือข่ายไม่ทำงาน

Moustasm, Alzahrani, Aljohani, Alshahrani, and Alharbi. (2019). นำเสนอผลการเปรียบเทียบการตรวจสอบความมั่นคงปลอดภัยตามมาตรฐาน ISO 27000/ ISO 27001/ ISO 27002 กับซอฟต์แวร์จัดการทรัพยากรความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อมที่ได้รับการพัฒนาขึ้นมาสำหรับใช้ผ่านเว็บไซต์องค์กร โดยผลการวิจัยพบว่าซอฟต์แวร์ที่พัฒนาขึ้นภายในองค์กรมีการรักษาความมั่นคงปลอดภัยที่แตกต่างจากการใช้มาตรฐาน ISO 27000/27001/27002 สำหรับบริหารจัดการความมั่นคงปลอดภัย ผลการวิเคราะห์ความเสี่ยงอยู่ในเกณฑ์ที่มีระดับความเสี่ยงมาก

Maingak, Candiwan, and Harsono (2018) ประเมินการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อตรวจสอบหาช่องโหว่ที่มีอยู่ก่อนการรับรองตามมาตรฐาน ISO/IEC 27001 : 2013 จำนวน 14 หมวด ของหน่วยงานภาครัฐ จากผลการสำรวจโดยการสัมภาษณ์ การสังเกต และเอกสารประกอบพบว่าความมั่นคงปลอดภัยสารสนเทศขององค์กรอยู่ในระดับ 1 (ระดับเบื้องต้น) นั่นคือองค์กรควรตระหนักและจัดการปัญหาที่ต้องแก้ไขหรือกระบวนการที่ไม่เป็นไปตามมาตรฐาน

วิธีการดำเนินการวิจัย

งานวิจัยนี้วิเคราะห์ ออกแบบ และพัฒนาระบบบริหารจัดการและควบคุมการเข้าถึงอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ให้มีกระบวนการทำงานแบบอัตโนมัติ เช่น การบริหารจัดการ การมอนิเตอร์หรือการตรวจสอบสถานะ และการแจ้งเตือนหรือรายงานการเข้าถึงอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ นอกจากนี้ได้มีการพัฒนาระบบให้สามารถบันทึกเหตุการณ์การป้อนข้อมูลคำสั่งในการบริหารจัดการอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ลงในระบบฐานข้อมูล (Database System) เพื่อเป็นการควบคุมและตรวจสอบการเข้าถึงอุปกรณ์กระจายสัญญาณระบบเครือข่ายคอมพิวเตอร์ให้สอดคล้องตามข้อกำหนดมาตรฐาน ISO/IEC 27001 : 2013 โดยมีกรอบการดำเนินการวิจัย ดังรูปที่ 1 ดังนี้

1. สำรวจและวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยระบบเครือข่ายคอมพิวเตอร์

1.1 สำรวจอุปกรณ์เทคโนโลยีสารสนเทศที่มีการใช้งานบนระบบเครือข่ายคอมพิวเตอร์ภายในองค์กร ประกอบด้วย เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย ระบบกล้องวงจรปิด ระบบลงบันทึกเวลาการทำงาน หรือการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ เป็นต้น เพื่อนำข้อมูลที่ได้จากการสำรวจมาจัดทำผังเครือข่าย การจัดสรรทรัพยากรและการออกแบบการเชื่อมโยงระบบเครือข่ายคอมพิวเตอร์เข้ากับระบบที่ต้องการ

1.2 วิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยระบบเครือข่ายคอมพิวเตอร์ ด้วยการนำหมวด A.9.4 การควบคุมการเข้าถึงระบบและแอปพลิเคชัน ตามมาตรฐาน ISO/IEC 27001:2013 มาใช้เป็นมาตรฐานในการประเมินความเสี่ยง ได้แก่ การจำกัดการเข้าถึงสารสนเทศ ความมั่นคงปลอดภัยในการเข้าถึงระบบ ระบบบริหารจัดการรหัสผ่าน การใช้โปรแกรมอรรถประโยชน์ และการควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม และนำเกณฑ์การประเมินความเสี่ยงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์

รูปที่ 1 กรอบการดำเนินการวิจัย

		Impact				
		ต่ำมาก	ต่ำ	ปานกลาง	สูง	สูงมาก
Likelihood	สูงมาก	VL15	L25	M35	H45	EH55
	สูง	VL14	L24	M34	H44	EH54
	ปานกลาง	VL13	L23	M33	M43	H53
	ต่ำ	VL12	L22	L32	L42	M52
	ต่ำมาก	VL11	VL21	VL31	L41	L51

รูปที่ 2 เกณฑ์การประเมินความเสี่ยงด้านความมั่นคงปลอดภัย (ณรงค์ฤทธิ์ วังคีรี, 2563)

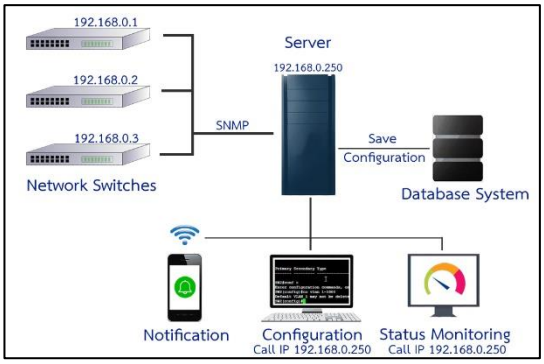
กองบัญชาการกองทัพไทย (ณรงค์ฤทธิ์ วังคีรี, 2563) แสดงดังรูปที่ 2 มาใช้เป็นเกณฑ์การประเมินความเสี่ยง ซึ่งมีการวิเคราะห์ข้อมูลและสถิติที่ใช้ ประกอบด้วย

1) โอกาสภัยคุกคามที่เริ่มเกิดขึ้นหรือเหตุการณ์ที่ได้เกิดขึ้น (Likelihood) คือ การประเมินโอกาสในการเกิดความเสี่ยงนั้นๆ ซึ่งระดับคะแนนในการเกิดความเสี่ยงแบ่งออกเป็น 5 ระดับ ได้แก่ สูงมาก สูง ปานกลาง ต่ำ และต่ำมาก

2) ระดับความรุนแรงของผลกระทบที่เกิดขึ้นจากเหตุการณ์ภัยคุกคาม (Impact) คือ การประเมินค่าความรุนแรงของผลกระทบของเหตุการณ์ภัยคุกคามโดยพิจารณาจากทรัพย์สินและประสิทธิภาพการทำงานของหน่วยงานแห่งหนึ่งที่สังกัดกองบัญชาการกองทัพไทย ซึ่งความรุนแรงของผลกระทบที่เกิดขึ้นจากเหตุการณ์ภัยคุกคามแบ่งออกเป็น 5 ระดับ ได้แก่ สูงมาก สูง ปานกลาง ต่ำ และต่ำมาก

3) ระดับของความเสี่ยงโดยรวม (Risk Exposure) คือ ผลลัพธ์ที่ได้จากการพิจารณาความสัมพันธ์ระหว่างโอกาสภัยคุกคามที่เริ่มเกิดขึ้นหรือเหตุการณ์ที่ได้เกิดขึ้น และระดับความรุนแรงของผลกระทบที่เกิดขึ้นจากเหตุการณ์ภัยคุกคาม และ

4) ผังประเมินระดับความเสี่ยงโดยรวม (Risk Assessment Matrix) โดยนำรายการความเสี่ยงของแต่ละระดับความเสี่ยงมาจัดเรียงลำดับ (Risk Ranking) แล้วนำมาวิเคราะห์เปรียบเทียบเกณฑ์ความสามารถในการยอมรับความเสี่ยง สำหรับนำมาเลือกวิธีตอบสนองความเสี่ยง (Risk Response) ได้แก่ ลดความเสี่ยง (Risk Reduction) ถ่ายโอนความเสี่ยง (Risk Transfer) หลีกเลี่ยงความเสี่ยง (Risk Avoidance) และ ยอมรับความเสี่ยง (Risk Acceptance) เพื่อนำมาจัดทำแนวทางการจัดการความเสี่ยง



รูปที่ 3 สถาปัตยกรรมการทำงานแบบอัตโนมัติของระบบ

2. 2. ออกแบบและพัฒนาระบบบริหารจัดการและควบคุมการเข้าถึงอุปกรณ์กระจายสัญญาณเครือข่าย

คอมพิวเตอร์แบบอัตโนมัติ ตามมาตรฐาน ISO/IEC 27001:2013 ด้วยโปรแกรม APPSERV ประกอบด้วย การใช้ Apache สำหรับพัฒนา Web Server การใช้ MySQL สำหรับพัฒนาระบบจัดการฐานข้อมูลที่ใช้บนเซิร์ฟเวอร์ การใช้ phpMyAdmin สำหรับจัดการฐานข้อมูล MySQL และมีการพัฒนาเว็บไซต์ด้วยภาษา PHP และใช้ Python สำหรับพัฒนาโปรแกรมติดต่อและดึงข้อมูลจากอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์มาแสดงผลในรูปแบบ JSON โดยทำงานร่วมกับ SNMP Protocol GetRequest และ GetResponse สำหรับติดต่อสื่อสารกับอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ จากรูปที่ 3 แสดงสถาปัตยกรรมการทำงานแบบอัตโนมัติของระบบบริหารจัดการและควบคุมการเข้าถึงอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ที่พัฒนาประกอบด้วย 3 ฟังก์ชันหลัก ได้แก่ 1) ฟังก์ชันการบริหารจัดการ (Configuration) 2) ฟังก์ชันการมอนิเตอร์หรือตรวจสอบสถานะ (Status Monitoring) และ 3) ฟังก์ชันการแจ้งเตือน (Notification) โดยระบบที่พัฒนาจะมีการปิด Service ต่างๆ ของอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ทั้งหมด ให้ตอบสนองต่อคำสั่งการควบคุมและบริหารจัดการจากเครื่องคอมพิวเตอร์แม่ข่ายที่กำหนดเท่านั้น

3. ทดสอบระบบที่พัฒนา โดยติดตั้งและทดสอบการใช้งานใน 5 สถานการณ์ ได้แก่ 1) การนำอุปกรณ์เทคโนโลยีสารสนเทศมาเชื่อมต่ออุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ 2) การป้อนรูปแบบคำสั่งเพื่อบริหารจัดการอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ 3) การพยายามเข้าสู่ระบบเพื่อใช้งาน 4) เหตุการณ์ผิดปกติเนื่องจากไฟฟ้าดับ และ 5) เหตุการณ์ผิดปกติเนื่องจากอุณหภูมิภายในอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์สูงมากกว่า 65 องศาเซลเซียส

4. ประเมินประสิทธิภาพระบบที่พัฒนา โดยประเมินระบบบริหารจัดการและควบคุมการเข้าถึงอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ด้านความสามารถในการทำงานได้โดยอัตโนมัติและสามารถตอบสนองต่อการปฏิบัติงานของกลุ่มผู้บริหารและผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ขององค์กร และมีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยในการควบคุมการเข้าถึงอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ตามมาตรฐาน ISO/IEC 27001:2013 หมวด A.9.4

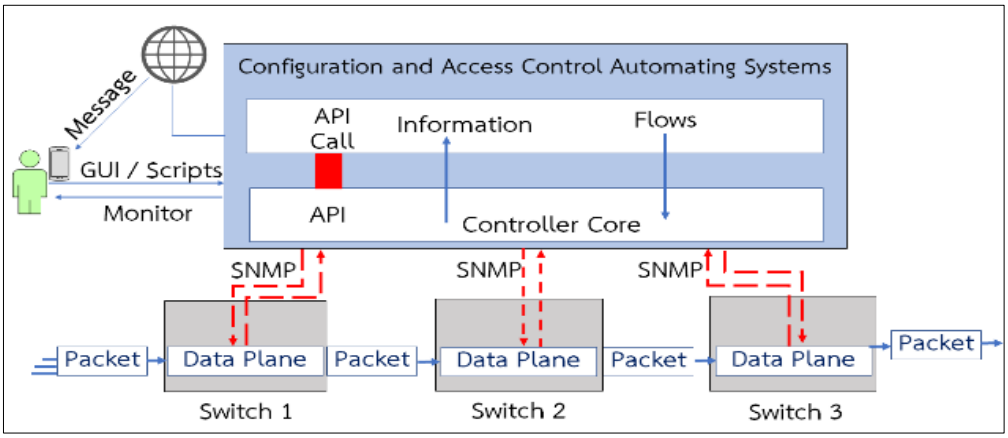
ผลการวิจัย

1. ผลการพัฒนาระบบบริหารจัดการและควบคุมการเข้าถึงอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์แบบอัตโนมัติ ตามมาตรฐาน ISO/IEC 27001: 2013 ผู้วิจัยดำเนินการออกแบบและพัฒนาฟังก์ชันต่างๆ ของระบบที่พัฒนาขึ้น โดยโครงสร้างการทำงานของระบบแสดงดังรูปที่ 4

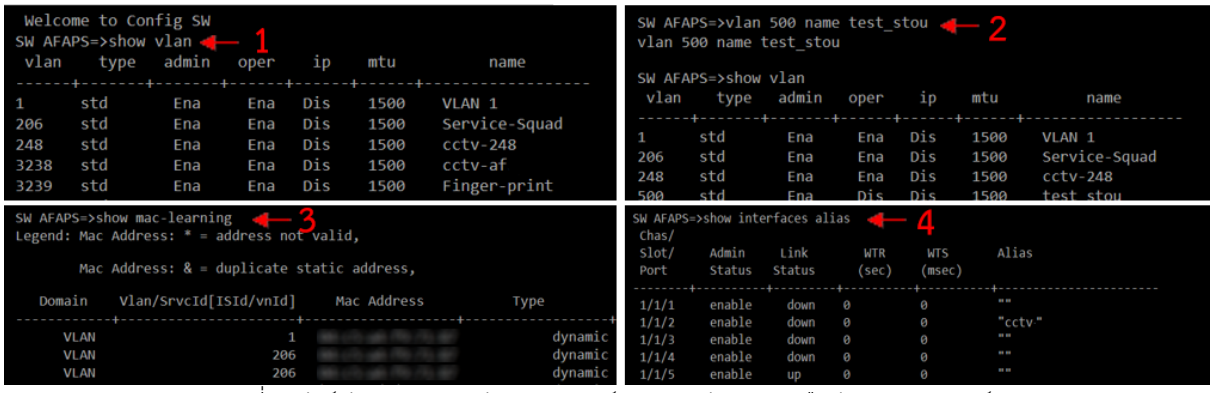
จากรูปผู้ใช้งานสามารถควบคุมระบบผ่าน GUI หรือ Scripts สำหรับบริหารจัดการและตรวจสอบสถานะอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์แบบอัตโนมัติ โดยระบบจะทำหน้าที่เป็น Software Defined Network (SDN) ในการบริหารจัดการอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ให้สามารถเชื่อมโยงกันได้ ส่วนของการส่ง Packet ข้อมูลคำสั่งทำหน้าที่เป็น Data Plane ทำให้อุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ที่เปิด Secure Shell (SSH) แต่ละอุปกรณ์สามารถเชื่อมต่อหรือใช้งานร่วมกันได้ การติดต่อสื่อสารระหว่างระบบบริหารจัดการที่พัฒนากับอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ถูกเข้ารหัสข้อมูลโดย SNMP Protocol โดยที่โปรแกรมต่อประสาน (API) รับคำสั่งต่างๆ มาประมวลผลแล้วส่งกลับคืนไปยังผู้ใช้งานที่ป้อนคำสั่งต่างๆ นอกจากนี้ส่วนของฟังก์ชันของระบบที่ทำหน้าที่บริหารจัดการอยู่ในส่วนของ Configuration Plane ซึ่งมีกระบวนการทำงานเป็นแบบอัตโนมัติ และมีผลการพัฒนาฟังก์ชันการทำงานดังนี้

1.1 ฟังก์ชันการบริหารจัดการ (Configuration) เป็นฟังก์ชันบริหารจัดการอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์สำหรับเชื่อมต่อไปยังคอมพิวเตอร์หรืออุปกรณ์เทคโนโลยีสารสนเทศอื่นๆ ภายในระบบเครือข่ายคอมพิวเตอร์ซึ่งมีการเข้ารหัสข้อมูลในระหว่างการสื่อสารด้วย SNMP Protocol โดยป้อนรูปแบบคำสั่งจำนวน 4 คำสั่ง ดังรูปที่ 5 ดังนี้

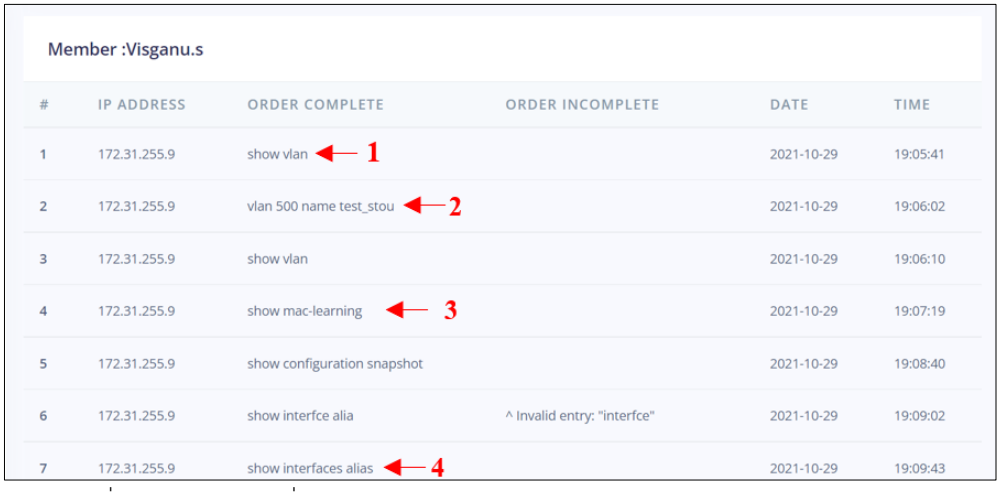
หมายเลข 1 show vlan เป็นคำสั่งใช้สำหรับตรวจสอบค่า หมายเลข 2 vlan 500 name test_stou เป็นคำสั่งสำหรับสร้าง vlan หมายเลข 3 show mac-learning เป็นคำสั่งสำหรับตรวจสอบMac-address และหมายเลข 4 show interfaces alias สำหรับตรวจสอบสถานะการเชื่อมต่ออุปกรณ์ ซึ่งคำสั่งที่ใช้บริหารจัดการทั้งหมดจะถูกบันทึกผลลงระบบฐานข้อมูล หลังจากที่มีการป้อนรูปแบบคำสั่งดังกล่าวแล้ว โดยผู้ดูแลระบบสามารถรายงานผลคำสั่งในการบริหารจัดการของแต่ละคำสั่งได้ดังรูปที่ 6 แล้วนำรูปแบบคำสั่งที่ถูกต้องมาวิเคราะห์ผลและตรวจสอบกระบวนการทำงานที่เกี่ยวข้องกับความมั่นคง



รูปที่ 4 โครงสร้างการทำงานของระบบ



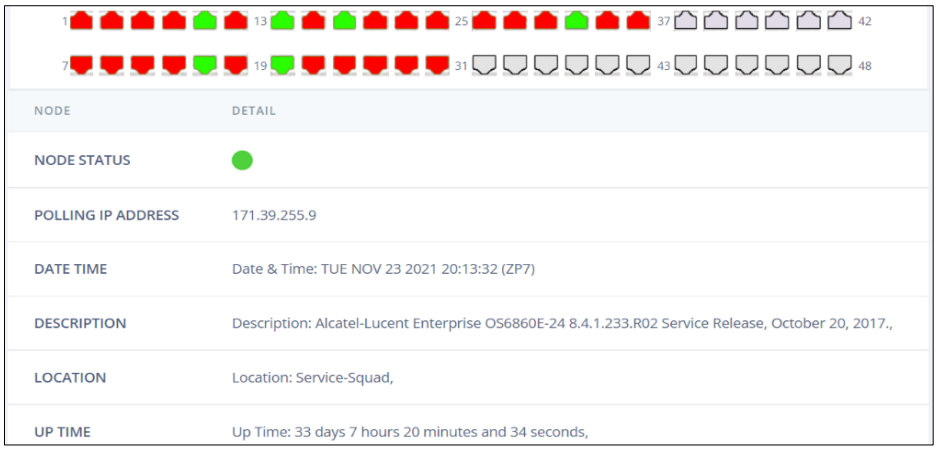
รูปที่ 5 ฟังก์ชันการบริหารจัดการอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์



Member :Visganu.s

#	IP ADDRESS	ORDER COMPLETE	ORDER INCOMPLETE	DATE	TIME
1	172.31.255.9	show vlan ← 1		2021-10-29	19:05:41
2	172.31.255.9	vlan 500 name test_stou ← 2		2021-10-29	19:06:02
3	172.31.255.9	show vlan		2021-10-29	19:06:10
4	172.31.255.9	show mac-learning ← 3		2021-10-29	19:07:19
5	172.31.255.9	show configuration snapshot		2021-10-29	19:08:40
6	172.31.255.9	show interfce alia	^ Invalid entry: "interfce"	2021-10-29	19:09:02
7	172.31.255.9	show interfaces alias ← 4		2021-10-29	19:09:43

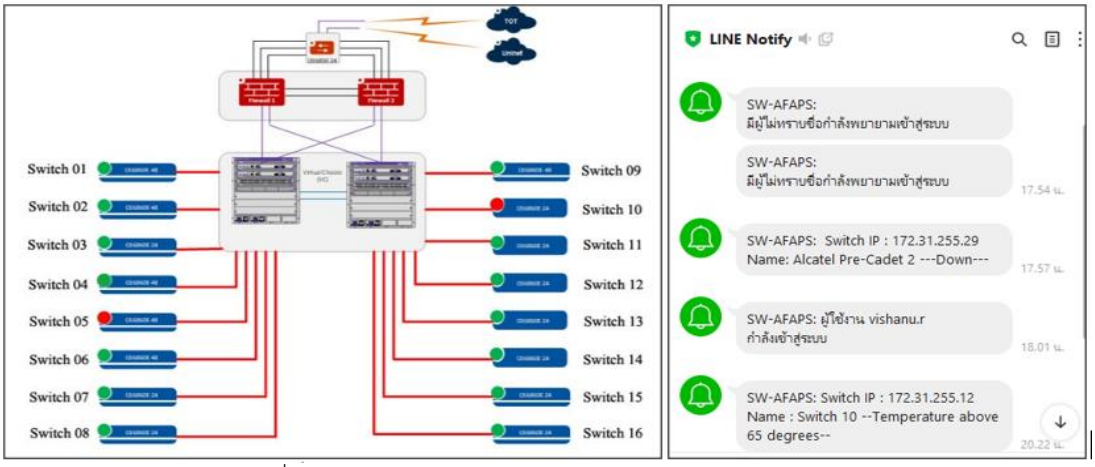
รูปที่ 6 รายงานผลคำสั่งการบริหารจัดการอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์



รูปที่ 7 ฟังก์ชันการตรวจสอบสถานะการใช้งานอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์

ปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ได้ และคำสั่งที่ไม่ถูกต้องถูกนำมาใช้เป็นข้อมูลสำหรับปรับปรุงให้ระบบสามารถใช้งานได้มีประสิทธิภาพยิ่งขึ้น

1.2 ฟังก์ชันการตรวจสอบสถานะ (Status Monitoring) แสดงในรูปที่ 7 เป็นฟังก์ชันตรวจสอบและแสดงสถานะความพร้อมของอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์แบบเรียลไทม์ เช่น แสดงสถานะปกติและไม่ปกติ สถานะการใช้งานพอร์ตต่างๆ สถานะหน่วยประมวลผล และสถานะหน่วยความจำของทรัพยากรที่เกี่ยวข้องกับการบริหารจัดการอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ โดยสีเขียวแสดงการเชื่อมต่อเข้ากับอุปกรณ์ สีแดงแสดงการไม่เชื่อมต่อและได้ทดสอบฟังก์ชันการทำงาน โดยเชื่อมต่อเครื่องคอมพิวเตอร์ 6 เครื่องเข้ากับอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ พบว่า



รูปที่ 8 ฟังก์ชันการแจ้งเตือนเหตุการณ์ผ่าน Line Application

สถานะพอร์ตการเชื่อมต่อแสดงสถานะสีเขียวจำนวน 6 พอร์ต

1.3 ฟังก์ชันการแจ้งเตือน (Notification) จากรูปที่ 8 เป็นการแจ้งเตือนเหตุการณ์ต่างๆ ของระบบด้วยการส่งข้อความให้กับผู้ดูแลระบบผ่าน Line Application เพื่อแจ้งสถานะการแสดงผลแบบเรียลไทม์ เช่น การเปิด-ปิด (Up-Down) การเข้าระบบปกติ การพยายามเข้าระบบแบบไม่ปกติ และสภาวะทางกายภาพผิดปกติ เช่น ระดับอุณหภูมิอุปกรณ์สูงกว่าที่กำหนด

2. ผลการประเมินประสิทธิภาพการพัฒนาระบบบริหารจัดการและควบคุมการเข้าถึงอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์แบบอัตโนมัติ ตามมาตรฐาน ISO/IEC 27001 : 2013 โดยประเมินด้านประสิทธิภาพการทำงานแบบอัตโนมัติ และประเมินความเสี่ยงด้านความมั่นคงปลอดภัย ผลการวิจัยเป็นดังนี้

2.1 ผลการประเมินประสิทธิภาพการทำงานแบบอัตโนมัติ โดยประเมินประสิทธิภาพจากการใช้งาน 5 สถานการณ์ ในแต่ละสถานการณ์มีการประเมินประสิทธิภาพจำนวน 5 รายการโดยกลุ่มผู้บริหารและผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ขององค์กรจำนวน 7 คน ตารางที่ 1 แสดงผลการประเมินประสิทธิภาพการทำงานของระบบที่มีการทำงานแบบอัตโนมัติ โดยรวมอยู่ในระดับมากที่สุด ($\overline{x}$ = 4.51, S.D. = 0.49) และเมื่อพิจารณาเป็นรายกรณีทดสอบความเป็นอัตโนมัติ พบว่ารายการประเมินที่มีระดับคะแนนประเมินประสิทธิภาพเฉลี่ยสูงที่สุด คือ มีการแสดงสถานะการทำงานของอุปกรณ์กระจายสัญญาณทั้งหมดแบบเรียลไทม์ การแก้ปัญหาต่างๆ เป็นแบบอัตโนมัติ ทำได้เร็วขึ้น โดยมีค่าเฉลี่ย $\overline{x}$ = 4.86 และค่าเบี่ยงเบนมาตรฐาน S.D. = 0.38

ตารางที่ 1 ผลการประเมินประสิทธิภาพการทำงานแบบอัตโนมัติ

ข้อที่	รายการประเมิน	$\overline{x}$	S.D.	ระดับความคิดเห็น
1	มีการทำงานได้ตามขั้นตอนที่กำหนดและเพิ่มประสิทธิภาพการทำงานจากการทำงานแบบแมนวลรูปแบบเดิม	4.43	0.54	มาก
2	มีการแสดงสถานะการทำงานของอุปกรณ์กระจายสัญญาณทั้งหมดแบบเรียลไทม์ การแก้ปัญหาต่างๆ เป็นแบบอัตโนมัติ ทำได้เร็วขึ้น	4.86	0.38	มากที่สุด
3	ลดระยะเวลาในขั้นตอนการทำงานเมื่อนำไปใช้งานจริง	4.29	0.49	มาก
4	มีการใช้ GUI เชื่อมต่อประสานกับผู้ใช้งานทำให้การใช้ฟังก์ชันการทำงานต่างๆ ของระบบเข้าใจง่ายขึ้น	4.43	0.54	มาก
5	สามารถนำไปประยุกต์ร่วมกับระบบนิเวศน์เชิงดิจิทัลและโครงสร้างพื้นฐานขององค์กรได้	4.57	0.54	มากที่สุด
	โดยรวม	4.51	0.49	มากที่สุด

ตารางที่ 2 ผลการประเมินความเสี่ยงด้านการควบคุมการเข้าถึงระบบและแอปพลิเคชัน

A.9 การควบคุมการเข้าถึง (Access control)				
ข้อ	ประเด็นความเสี่ยง	ลักษณะความเสี่ยง	ค่าความเสี่ยงก่อนพัฒนาระบบ	ค่าความเสี่ยงหลังพัฒนาระบบ
A.9.4 การควบคุมการเข้าถึงระบบและแอปพลิเคชัน				
A.9.4.1	การจำกัดการเข้าถึงสารสนเทศ	มีการควบคุมและให้สิทธิ์การเข้าถึงระบบบริหารจัดการอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ แทนการควบคุมและให้สิทธิ์แบบแมนวลหรือการยื่นเอกสารขออนุมัติ	M35	VL12
A.9.4.2	ความมั่นคงปลอดภัยในการเข้าถึงระบบ	ขั้นตอนการเข้าถึงระบบและอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์มีความมั่นคงปลอดภัย รหัสผ่านคาดเดายากและจำกัดจำนวนครั้งของการพยายามเข้าใช้ระบบ	H44	VL11
A.9.4.3	ระบบบริหารจัดการรหัสผ่าน	มีการบริหารจัดการรหัสผ่านที่เป็นไปตามนโยบายการควบคุมการเข้าถึงที่สามารถสร้าง ลบ แก้ไข ชื่อผู้ใช้และรหัสผ่าน	H45	VL12

A.9.4.4	การใช้โปรแกรมอรรถประโยชน์	อุปกรณ์มีการจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ โดยมีการเปิดเฉพาะการบริการ (Service) ที่จำเป็นและมีความมั่นคงปลอดภัย	L23	VL13
A.9.4.5	การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม	มีการจำกัดจำนวนสิทธิ์และควบคุมการเข้าถึงซอร์สโค้ดโปรแกรมการตั้งค่าและโปรแกรมคำสั่งต่างๆ สำหรับบริหารจัดการระบบ	H44	VL12

2.2 ผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยเมื่อมีการนำระบบที่พัฒนานำไปใช้จริง โดยประเมินความเสี่ยงตามมาตรฐาน ISO 27001: 2013 หมวด A.9.4 การควบคุมการเข้าถึงระบบและแอปพลิเคชัน โดยเปรียบเทียบระดับค่าความเสี่ยงเมื่อใช้กระบวนการทำงานแบบแมนวลเดิม (ก่อนพัฒนาระบบ) กับเมื่อใช้งานระบบที่พัฒนาให้มีการบริหารจัดการแบบอัตโนมัติ (หลังพัฒนาระบบ) แสดงดังตารางที่ 2 พบว่ารายการความเสี่ยงลดลงอยู่ที่ระดับต่ำมาก (VL)ในทุกประเด็นความเสี่ยงโดยเฉพาะอย่างยิ่งหมวด A.9.4.2 A.9.4.3 และ A.9.4.5 การใช้งานระบบที่พัฒนาซึ่งมีความเป็นอัตโนมัติมากขึ้นสามารถลดความเสี่ยงลงอยู่ในระดับที่องค์กรยอมรับได้ (ณรงค์ฤทธิ์ วังคีรี, 2563) และบรรลุตามวัตถุประสงค์ที่กำหนดไว้

อภิปรายผลการวิจัย

งานวิจัยนี้ได้พัฒนากระบวนการทำงานของระบบให้สามารถทำงานได้อัตโนมัติประกอบด้วยฟังก์ชันการบริหารจัดการ การตรวจสอบสถานะ และการแจ้งเตือน นับเป็นจุดเด่นของงานวิจัยนี้ที่สามารถลดขั้นตอนการเข้าถึงระบบได้ สามารถบันทึกเหตุการณ์การป้อนข้อมูลคำสั่งในการบริหารจัดการระบบแบบอัตโนมัติลงระบบฐานข้อมูลและมีการรายงานสถานะการเข้าถึง การตั้งค่า สถานะอุปกรณ์กระจายสัญญาณไปยังผู้ดูแลระบบทันที โดยใช้ SNMP Protocol สำหรับติดต่อสื่อสารกับอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ ซึ่งสอดคล้องกับงานวิจัย (Safrianti et al., 2021) ที่พัฒนาระบบตรวจสอบอุปกรณ์เครือข่ายแบบเรียลไทม์ด้วย SNMP Protocol ทำให้ระบบสามารถบริหารจัดการและแสดงผลได้อย่างมีประสิทธิภาพ

ผลการประเมินประสิทธิภาพการทำงานของระบบที่พัฒนาโดยกลุ่มผู้บริหารและผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ขององค์กรจำนวน 7 คน ดำเนินการประเมินประสิทธิภาพจากการใช้งานในสถานการณ์ 5 สถานการณ์ พบว่ากระบวนการบริหารจัดการและควบคุมการเข้าถึงสามารถทำงานได้แบบอัตโนมัติ ช่วยลดขั้นตอนการเข้าถึงถึงระบบ และเห็นภาพรวมของสถานะการทำงานของระบบได้อย่างรวดเร็ว มีการแสดงสถานะการทำงานของอุปกรณ์กระจายสัญญาณทั้งหมดแบบเรียลไทม์ การแก้ปัญหาต่างๆ เป็นแบบอัตโนมัติ ทำได้เร็วขึ้น ซึ่งสอดคล้องกับงานวิจัยของ Khan & Khan (2017) ที่แสดงถึงการทำงานแบบอัตโนมัติ ช่วยแก้ปัญหาด้านระยะเวลาการเข้าถึงการตรวจสอบอุปกรณ์จากระบบเดิมที่ต้องมีการป้อนคำสั่งแสดงผลเสมอ

และผลจากการวิเคราะห์ข้อมูลประเมินความเสี่ยง แสดงให้ทราบระดับค่าความเสี่ยงก่อน – หลังพัฒนาระบบซึ่งสะท้อนให้เห็นค่าความเสี่ยงที่แตกต่างกันทำให้องค์กรสามารถวางแผนเพื่อกำหนดแนวทางปฏิบัติในการป้องกันและควบคุมความเสี่ยงในการบริหารจัดการการควบคุมการเข้าถึงระบบและแอปพลิเคชัน ตามมาตรฐาน ISO/IEC 27001 : 2013 ที่องค์กรใช้อ้างอิง อย่างไรก็ตามจากการทดสอบการใช้งานจริงพบว่างานวิจัยนี้มีข้อจำกัดคือเมื่อมีการนำอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์จากแหล่งผลิตอื่นๆ ติดตั้งเพิ่มเติม จะต้องมีการเขียนคำสั่งเพิ่มเพื่อให้ระบบแสดงผลคำสั่งให้สอดคล้องและตรงตามการตั้งค่าของแต่ละอุปกรณ์จึงจะสามารถติดต่ออุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ระหว่างกันได้

สรุปผลการวิจัย

จากการพัฒนา และประเมินประสิทธิภาพของระบบบริหารจัดการและควบคุมการเข้าถึงอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์แบบอัตโนมัติ ตามมาตรฐาน ISO/IEC 27001:2013 พบว่าระบบบริหารจัดการและควบคุมการเข้าถึงอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์แบบอัตโนมัติสามารถใช้งานได้ตรงตามวัตถุประสงค์ การทดสอบประสิทธิภาพการทำงานแบบอัตโนมัติในภาพรวมมีผลการประเมินอยู่ในระดับมากที่สุด ($\overline{x}$ = 4.51, S.D. = 0.49) และผลการวิจัยสามารถนำระบบดังกล่าวที่พัฒนาขึ้นไปใช้ในองค์กรสำหรับบริหารจัดการความเสี่ยงเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 หมวด A.9.4 การควบคุมการเข้าถึงระบบและแอปพลิเคชัน โดยค่าความเสี่ยงด้านการควบคุมการเข้าถึงระบบและแอปพลิเคชันลดลงอยู่ในระดับต่ำมาก

ข้อเสนอแนะ

งานวิจัยการพัฒนาระบบบริหารจัดการและควบคุมการเข้าถึงอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์แบบอัตโนมัติตามมาตรฐาน ISO/IEC 27001 : 2013 นี้ดำเนินการพัฒนาระบบโดยการโปรแกรมภาษาคอมพิวเตอร์ที่เป็นโอเพนซอร์สทำให้สามารถพัฒนาฟังก์ชันการทำงานต่างๆ เพิ่มเติมตามความต้องการของผู้ใช้งาน ผู้ดูแลระบบ หรือลักษณะการบริหารจัดการเครือข่ายคอมพิวเตอร์ของแต่ละองค์กรได้ เพื่ออำนวยความสะดวกในการบริหารจัดการ ตรวจสอบและควบคุมการเข้าถึงอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ได้อย่างมีประสิทธิภาพมากขึ้น ผู้ดูแลระบบสามารถพัฒนาโปรแกรมสนับสนุนกระบวนการทำงานให้เป็นอัตโนมัติและสามารถทำงานได้ครบถ้วนสมบูรณ์มากขึ้น เช่น

1. ปรับตั้งค่าระบบรับส่งข้อมูลในระยะเวลาที่เหมาะสมกับสภาพการทำงานของเครือข่ายคอมพิวเตอร์ของแต่ละองค์กร เพื่อให้อุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ทำงานได้เต็มประสิทธิภาพและไม่ทำงานหนักมากหากต้องมีการอ่านค่าข้อมูลเข้า-ออกปริมาณมากหรือตลอดเวลา

2. ปรับเลือกการป้อนคำสั่งหรือการตั้งค่าอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ได้อย่างถูกต้องตามรุ่นผลิตภัณฑ์ที่ใช้งาน สำหรับองค์กรที่ใช้งานอุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์หลากหลายผลิตภัณฑ์ร่วมกัน ซึ่งอุปกรณ์แต่ละผลิตภัณฑ์หรือแต่ละรุ่นมีรูปแบบการป้อนคำสั่ง หรือการตั้งค่าที่แตกต่างกัน

3. บริหารจัดการ ตรวจสอบและควบคุมความมั่นคงปลอดภัยระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศขององค์กรตามมาตรฐาน ISO/IEC 27001:2013 อย่างต่อเนื่อง และปรับเปลี่ยนแบบอัตโนมัติได้ เพื่อให้สอดคล้องกับสถานการณ์ สภาพการทำงานหรือการให้บริการขององค์กรในแต่ละช่วงเวลา เช่น การตั้งค่าไฟร์วอลล์ การกำหนดสิทธิ์ในการเข้าถึงระบบ การอนุญาตให้ผู้มีสิทธิ์เข้าถึงระบบสามารถเข้าใช้งานจากภายนอกได้ เป็นต้น

เอกสารอ้างอิง

ณรงค์ฤทธิ์ วังคีรี. (2563). คู่มือการรักษาความมั่นคงปลอดภัยไซเบอร์หน่วยขึ้นตรงกองบัญชาการกองทัพไทย. หลักสูตรการฝึกตามหน้าที่และหลักพื้นฐานการปฏิบัติการทางไซเบอร์ บก.ทท. พ.ศ.2564. กรุงเทพฯ : ศูนย์ไซเบอร์ทหาร.

Fonseca-Herrera, O. A., Rojas, A. E., and Florez, H. (2018). A model of an information security management system based on NTC-ISO/IEC 27001 standard. *IAENG International Journal of Computer Science*, *48*(2).

Khan, R. and Khan, S. (2017). Design and Implementation of an Automated Network Monitoring and Reporting Back System. *Journal of Industrial Information Integration*. DOI:10.1016/j.jii.2017.11.001

Maingak, A Z., Candiwan, C. and Harsono, L D. (2018). Information security assessment ISO/IEC 27001:2013 standard on government institution. *Trikonomika Journal*, *17*(1), 28-37.

Moustasm, T., Alzahrani, A., Aljohani, R., Alshahrani, M., & Alharbi, B. (2019). Security review based on ISO 27000/ ISO 27001/ ISO 27002 standards: A case study research. *International Journal of Management and Applied Science*. 120-123.

Safrianti, E., Sari, L. O. and Sari, N. A. (2021). *Real-time network device monitoring system with Simple Network Management Protocol (SNMP) model.* Paper presented at the 2021 3rd International Conference on Research and Academic Community Services. 122-127.