มาตรฐานศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
มศอ. ๔๐๐๓.๑–๒๕๕๒
NECTEC STANDARD
NTS 4003.1 – 2552

ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์
เล่ม ๑ ข้อกำหนด

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
กระทรวงวิทยาศาสตร์และเทคโนโลยี

NECTEC
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

มาตรฐานศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

National Electronics and Computer Technology Center Standard

ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

เล่ม ๑ ข้อกำหนด

Computer Log Systems

Part 1 Requirements

มศอ. ๔๐๐๓.๑ - ๒๕๕๒

NTS 4003.1 – 2552

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
๒๕๕๒

NECTEC
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ประกาศศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
เรื่อง ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์
เล่ม 1 ข้อกำหนด

เพื่อให้การรับและเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ เป็นไปโดยชอบตามกฎหมายและหลักการที่ถูกต้อง ลดความเสี่ยงต่อการสูญเสียความถูกต้องสมบูรณ์ของข้อมูลจราจรทางคอมพิวเตอร์ที่จัดเก็บไว้ รวมถึงการให้หลักเกณฑ์ในการเลือกเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ที่เหมาะสมกับประเภทของบริการและเพียงพอสำหรับผู้ที่เกี่ยวข้องได้อย่างถูกต้องชัดเจนและเชื่อถือได้

ศูนย์เทคโนโลยีอิเล็กทรอนิส์และคอมพิวเตอร์แห่งชาติ จึงจัดทำมาตรฐานศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ระบบจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ เล่ม 1 ข้อกำหนด ดังรายละเอียดท้ายประกาศฉบับนี้

ประกาศ ณ วันที่ ๙ กันยายน พ.ศ. 2552

(นายขวัญชัย หล่าอุบล)
รองผู้อำนวยการ
รักษาการแทนผู้อำนวยการ
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

คณะกรรมการวิชาการ

ประธานกรรมการ

นายอาจิน จิรชีพพัฒนา	สำนักส่งเสริมอุตสาหกรรมเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

กรรมการ

นายถนัด มานะพันธุ์นิยม	สำนักงานคณะกรรมการคุ้มครองผู้บริโภค
พันตำรวจเอกกัลป์ ทังสุพานิช	ศูนย์ตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ
นายธงชัย แสงศิริ	สำนักกำกับการใช้เทคโนโลยีสารสนเทศ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
นายณัฐ สกลชัย	สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม
นายวิรัตน์ พึ่งสาระ	สำนักงานส่งเสริมอุตสาหกรรมซอฟต์แวร์แห่งชาติ
นายสมญา พัฒนวรพันธุ์	สำนักข่าวกรองแห่งชาติ สำนักนายกรัฐมนตรี
นายสว่างพงศ์ หมวดเพชร	สมาคมสมาพันธ์ซอฟต์แวร์โอเพนซอร์ส
นายราเมศวร์ ศิลปะพรหม	สมาคมสมาพันธ์เทคโนโลยสารสนเทศแห่งประเทศไทย
นายขจร สินอภิรมย์สราญ	บริษัท ไอที คอมพาเนี่ยน จำกัด
นายบรรจง ทะรังสี	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
นายกมล เอื้อชินกุล	

กรรมการและเลขานุการ

นายกริช นาสิงห์ขันธุ์	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ผู้ช่วยเลขานุการ

นางสาวพลอยรวี เกริกพันธ์กุล	กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
นายอรรถนิติ อัศวินนิมิตกุล	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

รายชื่อคณะทำงาน

ที่ปรึกษา

นายพันธ์ศักดิ์ ศิริรัชตพงษ์	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
นายกว้าน สีตะธนี	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
นายโกเมน พิบูลย์โรจน์	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
นายศิวรักษ์ ศิวโมกษธรรม	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

คณะทำงาน ด้านเทคนิค

นายกริช นาสิงห์ขันธุ์	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
นายกำธร ไกรรักษ์	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
นายถิรเจต พันพาไพร	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
นายพุธ นาทีสุวรรรณ	บริษัท ที-เน็ต จำกัด
นายปิยวัฒน์ เลื่อนสุคันธ์	บริษัท ที-เน็ต จำกัด

สารบัญ

บทนำ

0 หลักการของการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

หลักการต่อไปนี้ไม่ครอบคลุมถึงข้อกำหนดด้านความปลอดภัย ด้านความเข้ากันได้ทางแม่เหล็กไฟฟ้า ด้านสมรรถนะ และลักษณะเฉพาะของระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

0.1 หลักการทั่วไป

ผู้ออกแบบจำเป็นต้องเข้าใจหลักการที่สำคัญของระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์เพื่อให้สามารถออกแบบสร้างระบบที่เป็นไปตามข้อกำหนดที่ต้องการได้

หลักการนี้ไม่ได้เป็นทางเลือกเพิ่มเติมสำหรับข้อกำหนดในมาตรฐานนี้ แต่มีเจตนาให้ข้อมูลเพื่อให้ผู้ออกแบบเข้าใจหลักการพื้นฐานของข้อกำหนดเหล่านั้น ในกรณีที่ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์เกี่ยวข้องกับเทคโนโลยี หรือเทคนิค หรือการสร้างที่ไม่ได้ครอบคลุมไว้เฉพาะ การออกแบบระบบควรจัดให้มีระดับความสามารถไม่ด้อยกว่าที่ระบุไว้ในหลักการนี้

ผู้ออกแบบต้องไม่คำนึงแต่เฉพาะภาวะการทำงานปกติของระบบเท่านั้น แต่ต้องคำนึงถึงภาวะผิดปกติที่อาจเกิดขึ้น ผลสืบเนื่องของภาวะผิดปกติที่ตามมา การใช้งานผิดที่คาดหมายล่วงหน้าได้อย่างมีเหตุผล การบุกรุกจู่โจมโดยเจตนา และภัยคุกคามภายนอกอื่นๆ ที่อาจมีผลต่อความถูกต้องและสมบูรณ์ของข้อมูล อาทิ ไวรัสคอมพิวเตอร์ ความผิดปกติบนแหล่งจ่ายไฟฟ้าประธาน และความผิดปกติบนโครงข่ายสื่อสาร

ควรจัดลำดับความสำคัญต่อไปนี้ ในการพิจารณาหามาตรการในการออกแบบ

- ในกรณีที่เป็นไปได้ ให้ระบุเกณฑ์การออกแบบที่กำจัด ลด ป้องกัน ความเสียหายที่อาจเกิดขึ้นแก่ระบบ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่ระบบเก็บรักษาไว้
- หากกรณีข้างต้นเป็นไปไม่ได้ในทางปฏิบัติเนื่องจากทำให้ความสามารถของระบบด้อยลง ให้ระบุวิธีซึ่งไม่ขึ้นอยู่กับระบบ เช่น การกำหนดนโยบายควบคุมการเข้าถึงข้อมูล (ซึ่งไม่ได้ระบุไว้ในมาตรฐานศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาตินี้)
- หากทั้ง ๒ กรณีข้างต้นเป็นไปไม่ได้ในทางปฏิบัติ หรือเพื่อเป็นการเพิ่มเติมมาตรการข้างต้น ให้ระบุในการทำฉลากและข้อแนะนำ ถึงความเสี่ยงที่มีอยู่

จำเป็นต้องพิจารณาถึงผู้ที่เกี่ยวข้องกับการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ๓ ประเภทคือ "ผู้ดูแลระบบ (administrator) ผู้ดูแลข้อมูล และพนักงานเจ้าหน้าที่

"ผู้ดูแลระบบ" ในที่นี้จะหมายถึง บุคคล หรือกลุ่มบุคคล ที่มีหน้าที่ ดูแลรักษา ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ แต่จะไม่มีสิทธิ์ในการเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ และอาจรวมถึงข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นๆ ที่เกี่ยวข้อง

"ผู้ดูแลข้อมูล" หมายถึง ผู้ที่ได้รับมอบสิทธิ์จากองค์กร/หน่วยงานในการเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ และ

อาจรวมถึงข้อมูลคอมพิวเตอร์ และข้อมูลอื่นๆ ที่เกี่ยวข้อง สิทธิ์ในการเข้าถึงข้อมูลจะต้องไม่รวมถึงสิทธิ์ในการแก้ไข เปลี่ยนแปลง ลบ หรือ ทำลายข้อมูล

"พนักงานเจ้าหน้าที่" หมายถึง ผู้ที่ได้รับการแต่งตั้งตามกฎหมายให้มีหน้าที่ในการตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ ปกติพนักงานเจ้าหน้าที่จะติดต่อประสานงานกับผู้ดูแลข้อมูลขององค์กร เฉพาะเมื่อเกิดกรณีที่สงสัยว่ามีการกระทำผิดกฎหมายและเกี่ยวข้องกับองค์กรนั้นๆ

0.2 บูรณภาพ (Integrity) ของข้อมูล

ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ต้องสามารถรักษาบูรณภาพของข้อมูลจราจรทางคอมพิวเตอร์ที่จัดเก็บไว้ได้ตลอดช่วงเวลาที่กำหนดไว้ การกระทำหรือเหตุการณ์หรือสภาพใดๆ รวมถึงอันตรายและภัยคุกคาม ที่อาจเกิดขึ้นได้กับระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์และทำให้ความถูกต้องหรือความสมบูรณ์ของข้อมูลเสียไป ต้องได้รับการชี้บ่ง รวมถึงควรจัดให้มีการป้องกันเพื่อหลีกเลี่ยงหรือลดความเสี่ยงต่อการสูญเสียบูรณภาพของข้อมูลที่อาจเกิดขึ้นได้ หรือควรจัดให้มีฉลากหรือข้อแนะนำเพื่อเตือนถึงความเสี่ยงใดๆ ที่มีตกค้างอยู่

ลักษณะทางกายภาพ รูปแบบการติดตั้งของสื่อที่ใช้บันทึกข้อมูลจราจรทางคอมพิวเตอร์ รวมถึงรูปแบบการติดตั้งระบบและการเลือกใช้ส่วนประกอบต่างๆ ของระบบ ล้วนมีผลต่อบูรณภาพของข้อมูล

0.3 ความเชื่อถือได้ของข้อมูล

ความเชื่อถือได้ของข้อมูลขึ้นอยู่กับปัจจัยสองส่วน ส่วนแรกคือความสามารถในการรักษาบูรณภาพของข้อมูล ส่วนที่สองคือความไม่ขัดแย้งกับกฎหมายอื่นๆ ที่จะทำให้ข้อมูลจราจรทางคอมพิวเตอร์ไม่สามารถนำมาใช้อ้างอิงในทางศาลได้ ความขัดแย้งกับกฎหมายอื่นๆ ได้แก่ การเก็บข้อมูลส่วนบุคคลในลักษณะของการละเมิดสิทธิส่วนบุคคลโดยกฎหมายไม่ได้อนุญาตไว้ เป็นต้น

0.4 อันตรายและภัยคุกคาม

การนำมาตรฐานฉบับนี้ไปใช้มีเจตนาเพื่อลดความเสี่ยงจากการสูญเสียบูรณภาพของข้อมูล เนื่องจากสาเหตุต่อไปนี้

- อันตรายจากภาวะแวดล้อม
- ภัยคุกคาม

0.4.1 อันตรายจากภาวะแวดล้อม

อันตรายจากภาวะแวดล้อม ปกติจะหมายถึงอันตรายต่อระบบเก็บรักษาข้อมูลจราจรคอมพิวเตอร์หรือข้อมูลจราจรคอมพิวเตอร์ ซึ่งปกติเกิดขึ้นได้เอง โดยไม่มีเจตนาของบุคคลเข้ามาเกี่ยวข้อง อาทิ

- ความผิดปกติของระบบแหล่งจ่ายไฟฟ้าประธาน
- ความผิดปกติของโครงข่ายสื่อสาร โทรคมนาคม
- ความเสื่อมสภาพของสื่อบันทึกข้อมูล

- ความไม่เสถียรของระบบ อันเนื่องมาจากสภาพแวดล้อม อาทิ อุณหภูมิ ความชื้น ฝุ่น สัญญาณรบกวนแม่เหล็กไฟฟ้า

- ภัยธรรมชาติ

- ความไม่เสถียรของระบบช่วยหรือระบบสนับสนุนหรือส่วนประกอบ อันเนื่องมาจากสาเหตุข้างต้น

ตัวอย่างมาตรการที่ลดความเสี่ยงและความรุนแรงของอันตรายดังกล่าว ได้แก่

- การเลือกส่วนประกอบของระบบที่ได้รับการรับรองว่ามีความคงทนหรือมีภูมิคุ้มกันต่อภาวะแวดล้อมในระดับสูงและเชื่อถือได้ตลอดอายุการใช้งานที่คาดการณ์หรือออกแบบไว้

- การติดตั้งส่วนประกอบเชิงหน้าที่สำรอง หรือเพิ่มเติม

- การติดตั้งระบบในพื้นที่ที่สามารถควบคุมสภาพแวดล้อม ให้อยู่ในพิสัยที่ต้องการได้อย่างน่าเชื่อถือ

0.4.2 ภัยคุกคาม

เจตนาของบุคคล เป็นสิ่งที่แยกภัยคุกคามออกจากอันตรายจากสภาพแวดล้อม ภัยคุกคามอาจเกิดขึ้นได้ทั้งในลักษณะเฉพาะเจาะจงเป้าหมายและในลักษณะไม่เฉพาะเจาะจงเป้าหมาย

ภัยคุกคามอาจเกิดขึ้นได้จาก

- โปรแกรมไม่พึงประสงค์ที่กระจายอยู่ในเครือข่ายคอมพิวเตอร์ อาทิ หนอนคอมพิวเตอร์ ไวรัสคอมพิวเตอร์ โทรจัน เป็นต้น

- การดัดแปลง แก้ไข สร้างสภาพแวดล้อมที่ผิดปกติโดยเจตนาให้เกิดความล้มเหลวแก่ระบบ หรือความเสียหายแก่ข้อมูล

- การบุกรุก เข้าถึงพื้นที่หรือระบบหรือข้อมูล ที่จำกัดการเข้าถึง โดยไม่ได้รับอนุญาต หรือโดยไม่มีการป้องกันหรือแจ้งเตือน ทั้งทางกายภาพหรือทางอิเล็กทรอนิกส์ (ทางตรรก) หรือทั้งสองทาง

ตัวอย่างของมาตรการที่ลดความเสี่ยงดังกล่าว ได้แก่

- การติดตั้งโปรแกรมควบคุมโปรแกรมไม่พึงประสงค์ที่เชื่อถือได้ และจัดให้มีการปรับปรุงฐานข้อมูลให้ทันสมัยเสมอ

- การจัดให้มีการป้องกันการตั้งค่า แก้ไข เปลี่ยนแปลงค่าที่ตั้งไว้ของระบบช่วยหรือระบบสนับสนุน รวมถึงการจัดการให้มีแผนการซ่อมบำรุงที่เหมาะสม

- การจัดให้มีการกำหนดสิทธิและระดับการเข้าถึง รวมถึงการควบคุมการใช้ที่เหมาะสม

- จัดให้มีมาตรการเฝ้าระวังที่เหมาะสม

- จัดให้มีขั้นตอน หรือนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบและข้อมูลเพิ่มเติมตามความเหมาะสม

มาตรฐานศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

เล่ม ๑ ข้อกำหนด

1 ขอบข่าย

1.1 ทั่วไป

มาตรฐานศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ฉบับนี้ กำหนดคุณลักษณะที่ต้องการ การแสดงเครื่องหมายและฉลาก วิธีการรับและเก็บรักษาข้อมูล ของระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ โดยมีวัตถุประสงค์เพื่อให้วิธีการรับข้อมูลจราจรทางคอมพิวเตอร์เป็นไปโดยชอบตามกฎหมายและหลักการที่ถูกต้อง ลดความเสี่ยงต่อการสูญเสียความถูกต้องสมบูรณ์ของข้อมูลจราจรทางคอมพิวเตอร์ที่จัดเก็บไว้ รวมถึงประสงค์จะให้หลักเกณฑ์ในการเลือกเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่เหมาะสมกับประเภทของบริการ และเพียงพอสำหรับชี้บ่งผู้เกี่ยวข้องได้อย่างน่าเชื่อถือ

มาตรฐานฉบับนี้ใช้ได้กับทั้งระบบซึ่งอาจหมายถึงหลายหน่วยต่อเชื่อมกันหรือหน่วยเดี่ยว รวมถึงซอฟต์แวร์ประยุกต์ที่ออกแบบมาโดยประสงค์ให้ติดตั้งในระบบคอมพิวเตอร์ เพื่อให้ระบบคอมพิวเตอร์นั้นทำหน้าที่เป็นระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

มาตรฐานศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ แบ่งออกได้เป็น 2 เล่ม ดังนี้

เล่ม ๑ ข้อกำหนด

เล่ม ๒ แนวทางในการจัดทำและตรวจสอบระบบ

1.2 ข้อกำหนดเพิ่มเติม

ข้อกำหนดเพิ่มเติมนอกเหนือไปจากที่กำหนดไว้ในมาตรฐานฉบับนี้ อาจมีความจำเป็นสำหรับ

- ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ที่ออกแบบสำหรับผู้ให้บริการที่ประสงค์ให้บริการแก่บุคคลภายนอกที่มาใช้บริการแบบชั่วคราวหรือระยะสั้นๆ
- ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ที่ออกแบบสำหรับผู้ให้บริการที่ประสงค์ให้บริการเป็นการชั่วคราวหรือระยะสั้นๆ
- ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ที่ความเสี่ยงต่อการถูกคุกคามมากกว่าปกติ อาทิ ติดตั้งในสภาพแวดล้อมที่มีระดับการป้องกันการเข้าถึงต่ำกว่าที่แนะนำ

– ผู้ประกอบกิจการโทรคมนาคมและผู้ประกอบกิจการกระจายภาพและเสียง

1.3 ข้อยกเว้น

มาตรฐานฉบับนี้ไม่ครอบคลุมถึงการทำงานของ โปรแกรม ซอฟต์แวร์ประยุกต์ อุปกรณ์เครือข่าย เครื่องและระบบคอมพิวเตอร์ อื่นซึ่งทำหน้าที่ให้บริการใดๆ ในระบบคอมพิวเตอร์ที่ต่อเชื่อมถึงกัน และมีหน้าที่ต้องส่งข้อมูลจราจรทางคอมพิวเตอร์ที่กำหนด ให้ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

หมายเหตุ ผู้ประกอบกิจการโทรคมนาคม และผู้ประกอบกิจการกระจายภาพและเสียง ที่ให้บริการอื่นๆ นอกเหนือจากการให้บริการโครงข่ายโทรคมนาคม และการกระจายภาพและเสียง ถูกพิจารณาว่าอยู่ในขอบข่ายของมาตรฐานฉบับนี้

2 บทนิยาม

ความหมายของคำที่ใช้ในมาตรฐานศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ฉบับนี้มีดังต่อไปนี้

2.1 **ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์** ซึ่งต่อไปในมาตรฐานฉบับนี้จะเรียกว่า “ระบบ” หมายถึง คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่ทำหน้าที่เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ทั้งนี้หมายรวมถึงซอฟต์แวร์ที่จะติดตั้งในระบบคอมพิวเตอร์เพื่อให้ทำหน้าที่ดังกล่าวข้างต้น

2.2 **ระบบคอมพิวเตอร์** หมายถึง คอมพิวเตอร์ หรืออุปกรณ์ หรือชุดอุปกรณ์ของคอมพิวเตอร์ ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

2.2 **ข้อมูลจราจรทางคอมพิวเตอร์** หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรือข้อมูลอื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

2.3 **ผู้ให้บริการ** หมายถึง ผู้ซึ่งมีเจตนา

2.3.1 ให้บริการแก่ บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือเพื่อประโยชน์ของบุคคลอื่น

2.3.2 ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

2.4 **ผู้ดูแลระบบ** หมายถึง บุคคล หรือกลุ่มบุคคล ที่มีหน้าที่ ดูแลรักษา ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ แต่จะไม่มีสิทธิ์ในการเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ และอาจรวมถึงข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นๆ ที่เกี่ยวข้อง

2.5 **ผู้ดูแลข้อมูล** หมายถึง ผู้ที่ได้รับมอบสิทธิ์จากองค์กร/หน่วยงานในการเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ และอาจรวมถึงข้อมูลคอมพิวเตอร์ และข้อมูลอื่นๆ ที่เกี่ยวข้อง สิทธิ์ในการเข้าถึงข้อมูลจะต้องไม่รวมถึงสิทธิ์ในการ

แก้ไข เปลี่ยนแปลง ลบ หรือ ทำลายข้อมูล

2.6 **ผู้ใช้** หมายถึง **ผู้ดูแลระบบ หรือ ผู้ดูแลข้อมูล**

2.7 **การยืนยันตัวบุคคล** หมายถึง ขั้นตอนการชี้บ่ง เพื่อยืนยันความถูกต้องของหลักฐานที่ใช้ระบุ (Identity) แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง สามารถแบ่งออกได้เป็น 2 ขั้นตอน คือ การระบุตัวตน และการพิสูจน์ตัวตน

2.8 **การระบุตัวตน** (Identification) หมายถึง ขั้นตอนหรือวิธี ที่ผู้ใช้แสดงเป็นหลักฐานชี้บ่งตนเอง เช่น ชื่อผู้ใช้ (username) เป็นต้น

2.9 **การพิสูจน์ตัวตน** (Authentication) หมายถึง ขั้นหรือวิธี การตรวจสอบหลักฐานแวดล้อมเพื่อยืนยันว่าเป็นบุคคลที่กล่าวอ้างจริง

2.10 **การล็อกอิน** หมายถึง การเข้าใช้งานระบบคอมพิวเตอร์ โดยต้องทำการพิสูจน์ตัวตนก่อนเข้าใช้งาน

2.11 **ข้อมูลการล็อกอิน** หมายถึง ข้อมูลที่ใช้ในการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบคอมพิวเตอร์

2.12 **บูรณภาพของข้อมูล** (Integrity) หมายถึง ความถูกต้อง เที่ยงตรง และความสมบูรณ์ของข้อมูล

3 ข้อมูลและเอกสารอ้างอิง

3.1 ประกาศราชกิจจานุเบกษา, "พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550", วันที่ 18 มิถุนายน 2550

3.2 ประกาศราชกิจจานุเบกษา, "ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550", วันที่ 23 สิงหาคม 2550

3.3 หน่วยปฏิบัติการ วิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศ และคณะอนุกรรมการด้านความมั่นคง ภายใต้ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ในคณะอนุกรรมการธุรกรรมทางอิเล็กทรอนิกส์, "มาตรฐานการรักษาความมั่นคงปลอดภัย ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2.5) ประจำปี 2550", ISBN: 978-974-229-584-4, พิมพ์ครั้งที่ 1, ธันวาคม 2550

3.4 SN ISO/IEC 17799:2005, "Information technology – Security Technique – Code of practice for information security management (ISO/IEC 17799:2005)", Second Edition, 2005-06-15

3.5 Chaiyakorn Apiwathanokul, "Computer Time Synchronization Scheme" , http://www.etcommission.go.th/documents/standard/time_sync_server_v1_0.pdf, 3 October 2007

3.6 ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย ภายใต้ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, "แนวทางการจัดเก็บข้อมูลล็อกสำหรับองค์กรเพื่อให้สอดคล้องตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550" , http://www.thaicert.org/paper/auditing/LogImplementationandAuditingGuideline_r2.pdf , 23 สิงหาคม

2550

3.7 อสมาภรณ์ ฉัตรัตติกรณ์ และ ชวลิต ทินกรสูติบุตร, "การเทียบเวลาด้วย Network Time Protocol ให้สอดคล้องกับ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550" http://www.thaicert.org/paper/basic/NTPandLAW.php, 27 กุมภาพันธ์ 2551
อสมาภรณ์ ฉัตรัตติกรณ์ และ ชวลิต ทินกรสูติบุตร, "คู่มือการใช้บริการ Time Server [ฉบับปรับปรุง]", http://www.thaicert.org/paper/basic/manualTimeServer.php, 27 กุมภาพันธ์ 2551

3.8 W3C, "Extended Log File Format", http://www.w3.org/pub/WWW/TR/WD-logfile-960221.html, 19 May 2009

3.9 IETF Working Groups, "RFC1738 - Uniform Resource Locators (URL)", http://www.ietf.org/rfc/rfc1738.txt, December 1994

3.10 IETF Working Groups, "RFC1321 - The MD5 Message-Digest Algorithm", http://www.ietf.org/rfc/rfc1321.txt, April 1992

3.11 IETF Working Groups, "US Secure Hash Algorithm 1 (SHA1)", http://www.ietf.org/rfc/rfc3164.txt, September 2001

3.12 IETF Working Groups, "The BSD syslog Protocol", http://www.ietf.org/rfc/rfc3174.txt, August 2001

3.13 Federal Information Processing Standards (FIPS), "FIPS-180-1 SECURE HASH STANDARD", http://www.itl.nist.gov/fipspubs/fip180-1.htm, 1995 April 17

3.14 Wikipedia, "Cryptographic hash function", http://en.wikipedia.org/wiki/Cryptographic_hash_function, 19 May 2009

3.15 Karen Kent and Murugiah Souppaya, NIST, Special Publication 800-92, "Guide to Computer Security Log Management", September 2006

3.16 Roger Meyer, "Auditing a Corporate Log Server" GAIC Gold Certification, GIAC Systems and Network Auditor (GSNA), SANS Institute 2006 Reading Room, 17 September 2006

4 คุณลักษณะทั่วไป

4.1 ทั่วไป

ปกติระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ จะทำงานเกี่ยวข้องกับผู้ใช้สองประเภทที่แตกต่างกันคือ ผู้ดูแลระบบ ซึ่งทำหน้าที่ติดตั้ง ตั้งค่าและดูแลการทำงานของระบบ แต่จะไม่มีสิทธิเข้าถึงข้อมูลที่จัดเก็บไว้ และผู้ดูแลข้อมูล ซึ่งจะสามารถเข้าถึงข้อมูลได้ แต่จะไม่มีสิทธิ์แก้ไข ดัดแปลง หรือลบ ทำลายข้อมูลจราจรทางคอมพิวเตอร์

และไม่มีสิทธิ์ในการเปลี่ยนแปลงการตั้งค่าใดๆ ของระบบ

ระบบควรจำกัดจำนวนผู้ใช้ที่อนุญาตหรือยอมให้สร้างบัญชีผู้ใช้ขึ้นบนระบบ โดยทั่วไปจำนวนผู้ดูแลข้อมูล ไม่ควรจะมีเกิน 1 บัญชี และผู้ดูแลระบบควรมีจำนวนน้อยที่สุดเท่าที่เป็นไปได้ตามความจำเป็น และต้องไม่สามารถกำหนดให้มีบัญชีผู้ใช้ใดๆ มีสิทธิเป็นผู้ดูแลระบบและผู้ดูแลข้อมูลพร้อมกันได้

หมายเหตุ การเพิ่มจำนวนบัญชีผู้ใช้ จะทำให้ความเสี่ยงต่ออันตรายและภัยคุกคามเพิ่มมากขึ้น ดังนั้นผู้ออกแบบควรจัดให้มีมาตรการควบคุมเพิ่มเติมตามระดับความเสี่ยงที่เพิ่มขึ้น เช่นการกำหนดจำนวนผู้ใช้งานได้พร้อมกัน การควบคุมบัญชีและรหัสผ่าน หรือการให้ข้อแนะนำเกี่ยวกับนโยบายด้านความมั่นคงปลอดภัยเสริมอื่น เช่น นโยบายเกี่ยวกับการตั้งรหัส การกำหนดอายุใช้งานของรหัส นโยบายการเข้าถึงและใช้งานของผู้ใช้สำรอง เป็นต้น

4.2 คู่มือและข้อแนะนำ

ระบบ ต้องให้ข้อแนะนำวิธีการติดตั้ง การตั้งค่าและการเตรียมการต่างๆ อย่างเพียงพอสำหรับผู้ดูแลระบบ ทั้งนี้หมายรวมถึงข้อแนะนำในการปรับปรุง เลือกและกำหนดพื้นที่ติดตั้ง สภาพแวดล้อมที่เหมาะสม รูปแบบและวิธีการต่อเชื่อมเข้ากับระบบคอมพิวเตอร์อื่น การประเมินปัจจัยและความเสี่ยงและการตรวจสอบขั้นต้น เพื่อให้แน่ใจว่าผู้ดูแลระบบจะสามารถปฏิบัติตามได้อย่างถูกต้องตามวัตถุประสงค์ที่ตั้งไว้

ระบบ ต้องมีข้อแนะนำการใช้งานที่จำเป็น สำหรับผู้ดูแลข้อมูล อาทิ วิธีการเรียกดูข้อมูล การตั้งรหัส การแก้ไขปัญหาขั้นต้น

คู่มือและข้อแนะนำการใช้ ต้องจัดทำเป็นภาษาไทย สำหรับคู่มือหรือข้อแนะนำเพิ่มเติมอื่น ที่ใช้ประกอบเพื่อเป็นข้อมูล อนุญาตให้ใช้ภาษาอื่นได้หากไม่เป็นการเพิ่มความเสี่ยงในการใช้งานปกติ

หมายเหตุ การใช้ภาษาอื่นนอกเหนือจากภาษาไทย อาจเพิ่มความเสี่ยงต่อการตีความข้อมูล และสารสนเทศผิดไปจากความหมายที่ตั้งไว้

4.3 สภาพแวดล้อมสำหรับติดตั้งระบบ

โดยปกติ สภาพแวดล้อมสำหรับติดตั้งระบบต้องสามารถป้องกันการเข้าถึงระบบหรือข้อมูล โดยไม่เจตนาของบุคคลอื่นซึ่งไม่ใช่ผู้ใช้ได้ รวมถึงต้องมีคุณสมบัติเหมาะสม สำหรับการทำงานอย่างถูกต้องเชื่อถือได้ของระบบ ในกรณีที่สภาพแวดล้อมที่ติดตั้งระบบ มีผลอย่างสำคัญต่อการทำงานของระบบหรือการป้องกันการเข้าถึงระบบและข้อมูลจราจรทางคอมพิวเตอร์ ผู้ออกแบบควรให้ข้อแนะนำในการเลือก ดัดแปลงและปรับปรุงที่เพียงพอ เพื่อให้มีคุณลักษณะตามที่ต้องการ และต้องทำเครื่องหมายหรือแสดงข้อมูลให้เห็นได้อย่างชัดเจนถึงความต้องการดังกล่าว

5 การแสดงเครื่องหมายและฉลาก

5.1 ระบบ ต้องแสดงเครื่องหมายหรือข้อความบนเปลือกหุ้มด้านนอกของบรรจุภัณฑ์ และบนเปลือกหุ้มของบริภัณฑ์หรือระบบ ในลักษณะที่สามารถเห็นได้ง่ายและชัดเจน ที่ให้ข้อมูลอย่างน้อยดังนี้

- ชื่อแบบรุ่น และชื่อผู้ทำ

- ประเภทของข้อมูลจราจรทางคอมพิวเตอร์ ที่สามารถเก็บได้
- คุณลักษณะพื้นฐานที่มีให้ หรือคุณลักษณะพื้นฐานที่ต้องการ ด้านการประมวลผลของระบบ ได้แก่ แบบ รุ่นของหน่วยประมวลผล ขนาดหน่วยความจำ
- ความสามารถในการจัดเก็บข้อมูล หรือขนาดความจุของฮาร์ดดิสก์หรือสื่ออื่นๆ ที่ต้องการ

เครื่องหมายและข้อความ ต้องมีความคงทนต่อการใช้งานตามปกติ และอ่านเข้าใจได้ง่าย

การตรวจความเป็นไปตามข้อกำหนดให้ทำโดยการตรวจพินิจทั้งขนาด รูปแบบ การสะกดและเนื้อหา สำหรับความคงทนให้ทำโดยการถูเครื่องหมายและข้อความด้วยผ้าชุ่มน้ำเป็นเวลา ๑๕ วินาทีและด้วยผ้าชุ่มปิโตรเลียมสปิริต (petroleum spirit) เป็นเวลา ๑๕ วินาที หลังการทดสอบนี้เครื่องหมายและข้อความต้องอ่านได้ง่าย ไม่เลอะเลือน ต้องไม่สามารถแกะหรือถอดแผ่นเครื่องหมายและข้อความออกได้โดยง่าย และแผ่นเครื่องหมายและข้อความต้องไม่ม้วน หรือโก่งงอ

5.2 ระบบต้องแสดงข้อมูลต่อไปนี้ในเอกสารข้อแนะนำการติดตั้งระบบ ในตำแหน่งที่สามารถเข้าถึงได้โดยง่าย

- ประเภท ของข้อมูลจราจรที่จัดสามารถจัดเก็บได้ รวมถึงรายละเอียดที่เกี่ยวข้องกัน อาทิ ชื่อและรุ่นของซอฟต์แวร์ประยุกต์ ชื่อและรุ่นของอุปกรณ์หรือบริการหรือระบบต้นทางใดๆ ที่เป็นแหล่งกำเนิดข้อมูลจราจรทางคอมพิวเตอร์ เป็นต้น
- คุณลักษณะพื้นฐานที่มีให้ หรือคุณลักษณะพื้นฐานที่ต้องการ ด้านการประมวลผลของระบบ ได้แก่ แบบ รุ่นของหน่วยประมวลผล ขนาดหน่วยความจำ
- ความสามารถในการจัดเก็บข้อมูลที่มีให้ หรือวิธีการคำนวณความสามารถในการจัดเก็บ
- จำนวนผู้ใช้งานสูงสุด และจำนวนเหตุการณ์สูงสุดต่อหน่วยเวลา ที่สามารถรองรับได้
- ความสามารถสูงสุด ที่สามารถขยาย หรือเพิ่มเติมได้ (ถ้ามี)

การตรวจความเป็นไปตามข้อกำหนดให้ทำโดยการตรวจพินิจ

6 ข้อกำหนดของระบบ

6.1 ระบบ ต้องสามารถเก็บข้อมูลจราจรทางคอมพิวเตอร์ ตามประเภทและความสามารถที่ระบุไว้ และต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ได้ต่อเนื่องเป็นเวลาไม่น้อยกว่า ๙๐ วัน

การตรวจความเป็นไปตามข้อกำหนด ให้ทำโดยการประเมินข้อมูลจากฉลากและเอกสารที่เกี่ยวข้อง การประเมินทรัพยากรและค่าที่ตั้งไว้หรือโดยการทดสอบกับระบบจำลองสภาพการทำงานที่เกี่ยวข้องตามข้อ 7.2

6.2 ระบบต้องสามารถปรับตั้งนาฬิกาภายใน ให้ตรงกับเวลาอ้างอิงมาตรฐานระดับชาติ ได้โดยอัตโนมัติ

ความถี่ในการปรับตั้งค่าอัตโนมัติ ให้พิจารณาจากข้อมูลแวดล้อมที่เกี่ยวข้อง อาทิ ความเสถียรของระบบ

การตรวจความเป็นไปตามข้อกำหนด ให้ทำโดยการประเมินค่าที่ตั้งไว้และข้อมูลแวดล้อมที่เกี่ยวข้อง

หมายเหตุ รายชื่อหน่วยงานและเครื่องแม่ข่ายที่ให้บริการปรับเทียบเวลาอ้างอิงมาตรฐานระดับชาติ ได้แก่

1. สถาบันมาตรวิทยาแห่งชาติ ได้แก่ time1.nimt.or.th(203.185.69.60) time2.nimt.or.th(203.185.69.59) และ time3.nimt.or.th(203.185.69.56)
2. กรมอุทกศาสตร์ กองทัพเรือ ได้แก่ time.navy.mi.th(118.175.67.83)
3. ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย(ThaiCERT) ได้แก่ clock1.thaicert.org (203.185.129.186) และ clock2.thaicert.org (203.185.129.187)

6.3 ระบบต้องมีการกำหนดการป้องกันการเข้าถึงระบบโดยผู้ไม่ได้รับอนุญาต ทั้งทางกายภาพและทางอิเล็กทรอนิกส์อย่างเหมาะสม ทั้งนี้อาจหมายรวมถึงข้อแนะนำต่างๆ ที่เกี่ยวข้อง โดยอย่างน้อยวิธีใดวิธีหนึ่ง หรือรวมกันต่อไปนี้

- การใช้รหัสผ่านหรือการยืนยันตัวบุคคลหรือวิธีการอื่นที่คล้ายกัน
- การจำกัดรูปแบบและวิธีการเข้าถึง
- การจำกัดจำนวนผู้ใช้
- การจำกัดเวลาการใช้
- การกำหนดช่วงเวลาที่อนุญาต
- การกำหนดใช้นโยบายและเทคนิคด้านความมั่นคงปลอดภัยอื่น

หากระบบอนุญาตให้เข้าถึงระยะไกลได้ โดยผ่านระบบคอมพิวเตอร์ที่ต่อเชื่อมถึงกันโดยโครงข่ายภายในองค์กรหรือโครงข่ายสาธารณะ อาจจำเป็นต้องมีมาตรการด้านความมั่นคงปลอดภัยเพิ่มเติมจากที่ระบุไว้ข้างต้น อาทิ

- การใช้เทคนิคการเข้ารหัสข้อมูล
- การจำกัดสิทธิ หรือยกเลิกสิทธิบางประการ
- การกำหนดรูปแบบ หรือเทคนิคการเข้าถึงแบบเฉพาะ

6.4 ระบบต้องสามารถควบคุมและป้องกันการเปลี่ยนแปลงการตั้งค่าต่างๆ ของระบบโดยผู้ใช้ได้ สำหรับการตั้งค่าที่อนุญาตให้เปลี่ยนแปลงได้ ต้องสามารถควบคุมและป้องกันการเปลี่ยนแปลงการตั้งค่า โดยผู้ใช้ที่ไม่เกี่ยวข้องได้ การเปลี่ยนแปลงการตั้งค่าใดๆ ของระบบ และบัญชีผู้ใช้ ต้องไม่ทำให้คุณสมบัติตามข้อกำหนดที่ต้องการของมาตรฐานฉบับนี้ ด้อยลง หรือเสียสภาพ หรือเกิดความผิดพร่องขึ้น

6.5 ระบบต้องสามารถระบุและจำแนกตัวบุคคล และบันทึกประวัติการเข้าถึงและใช้งานระบบได้ รวมถึงต้องสามารถป้องกันการแก้ไข เปลี่ยนแปลง การปลอมแปลงข้อมูลที่เกี่ยวข้องเพื่อการเข้าถึงระบบหรือข้อมูลโดยไม่ได้รับอนุญาตได้ เทคนิคและวิธีที่ใช้ในการระบุตัวบุคคลและป้องกันการเปลี่ยนแปลง ควรเป็นเทคนิคที่ถูกตรวจสอบ

ยืนยันความใช้ได้แล้ว

6.6 ระบบ ควรมีการตรวจสอบความใช้ได้ของข้อมูลอื่น ที่ไม่ใช่ข้อมูลจราจรทางคอมพิวเตอร์ ที่รับเข้าสู่ระบบ (Input Validation)

ในกรณีที่เหมาะสม ควรจัดให้มีการเฝ้าระวังอันตรายและภัยคุกคาม พร้อมทั้งระบบแจ้งเตือนผู้เกี่ยวข้อง รวมถึงจัดให้มีข้อแนะนำเกี่ยวกับมาตรการตรวจสอบและแก้ไข หากสงสัยหรือพบว่ามีอันตรายหรือภัยคุกคามเกิดขึ้น

6.7 ระบบ ควรจัดให้มีคำอธิบายเพื่อให้ความช่วยเหลือ (Help) ในการแก้ไขปัญหาและข้อบกพร่องต่างๆ ที่มักเกิดขึ้น อย่างเหมาะสมและเพียงพอ

7 การรับและการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

7.1 การรับข้อมูลจราจรทางคอมพิวเตอร์

ระบบต้องสามารถรับข้อมูลจราจรทางคอมพิวเตอร์ จากอุปกรณ์ บริการหรือระบบต้นทาง ตามที่ระบุได้ อย่างครบถ้วน ถูกต้อง และหากเป็นไปได้ระบบควรมีระบบตรวจสอบและปฏิเสธข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลอื่นที่ส่งมาจากระบบต้นทาง ที่ไม่ถูกต้องหรือผิดปกติ

7.2 การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

ข้อมูลจราจรทางคอมพิวเตอร์ ที่รับเข้ามาในระบบต้อง

- เก็บในสื่อ (Media) ที่สามารถรักษาบูรณภาพของข้อมูลได้อย่างเหมาะสมและป้องกันการสูญหาย เสียหาย ถูกลบ ทำลาย แก้ไข ดัดแปลง ทั้งโดยเจตนาและไม่เจตนา
- เข้าถึงได้เฉพาะผู้ดูแลข้อมูล และไม่สามารถเข้าถึงได้โดยผู้ไม่เกี่ยวข้องหรือผู้ไม่ได้รับอนุญาต
- ถูกเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าที่ได้ระบุไว้ และต้องไม่น้อยกว่า ๙๐ วัน

7.3 ระบบต้องสามารถป้องกันการแก้ไข เปลี่ยนแปลง ลบ ทำลายข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลการใช้งานระบบ และข้อมูลคอมพิวเตอร์อื่นๆ ที่เกี่ยวข้อง โดยผู้ดูแลข้อมูล และผู้อื่นที่ไม่เกี่ยวข้องได้ ทั้งโดยเจตนาและไม่เจตนา เว้นแต่เป็นการลบหรือทำลายข้อมูลส่วนที่เกินและไม่มีความจำเป็นต้องจัดเก็บแล้ว

7.4 ระบบต้องสามารถตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ที่จัดเก็บไว้ได้ รวมถึงควรจัดให้มีการเฝ้าระวังบูรณภาพของข้อมูลอย่างเหมาะสม

ภาคผนวก ก
การตรวจสอบความถูกต้องสมบูรณ์ของข้อมูล

ก.1 วิธีแฮช (hash)

การตรวจสอบความสมบูรณ์และความถูกต้องของข้อมูลโดยวิธีแฮช หมายถึง กรรมวิธีตรวจสอบความสมบูรณ์และความถูกต้องของข้อมูล โดยอาศัยหลักการของการเข้ารหัสลับ (Cryptography) ที่ใช้ฟังก์ชันแฮช (hash function) ที่ถูกออกแบบมาโดยเฉพาะสำหรับใช้ในด้านการรักษาความปลอดภัยของสารสนเทศ เช่น SHA-1, MD5 หรือ CRC32 ซึ่งคุณสมบัติของฟังก์ชันแฮชเหล่านี้คือ เมื่อนำข้อมูลนำเข้า (input data) มาคำนวณค่ากับฟังก์ชันแฮช จะได้ผลลัพท์เป็นค่าเฉพาะตัวค่าหนึ่งหรือที่เรียกว่าค่าแฮช ซึ่งเป็นค่าที่แตกต่างในทุกๆข้อมูลนำเข้า และค่าเฉพาะตัวนี้ได้รับการรับรองการจัดการข้อมูลที่จะไม่มีโอกาสซ้ำกันได้ในระดับการใช้งาน ที่ได้รับการยอมรับเป็นสากล จากคุณสมบัติดังกล่าว ฟังก์ชันแฮช จึงถูกนำมาใช้ในการตรวจสอบความถูกต้องของข้อมูลได้ โดยการคำนวณค่าแฮชแล้วนำค่ามาเก็บไว้ก่อน ที่จะนำข้อมูลไปใช้งานและเมื่อต้องการการตรวจสอบความถูกต้องให้นำข้อมูลนั้น กลับมาคำนวณค่าแฮช อีกครั้ง ถ้าพบว่าค่าแฮช มีค่าเดิมจะถือว่าข้อมูลมีความถูกต้องและสมบรูณ์ แต่หากค่าแฮช มีค่าเปลี่ยนไปไม่เหมือนเดิม แสดงว่าเกิดการเปลี่ยนแปลงของข้อมูลเกิดขึ้น

ภาคผนวก ข
ตัวอย่างข้อมูลจราจรทางคอมพิวเตอร์

ข.1 ข้อมูลจราจรทางคอมพิวเตอร์ จากการต่อเชื่อมเข้าถึงระบบเครือข่าย

รายการข้อมูลที่ต้องจัดเก็บ

- ข้อมูลจราจรทางคอมพิวเตอร์ที่มีการบันทึกไว้เมื่อมีการเข้าถึงระบบเครือข่าย (Access Logs)
- ข้อมูลเกี่ยวกับวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and Time of Connection of Client to Server)
- ข้อมูลเกี่ยวกับชื่อที่ระบุตัวตนผู้ใช้ (User ID)
- ข้อมูลหมายเลขชุดอินเทอร์เน็ตที่ถูกกำหนดโดยระบบผู้ให้บริการ (Assigned IP Address)
- ข้อมูลที่บอกถึงหมายเลขสายที่เรียกเข้ามา (Calling Line Identification)

```
Radius Log
Sun Mar 18 04:35:24 2008 localhost@server radiusd[2305]: Login OK:
[8uJY5653/<CHAP-Password>] (from client APP2 port 7 cli 00-1B-77-
F3-18-C3)

Squid Log
192.168.99.7 - lersak [18/Aug/2008:21:06:48 +0700] "GET
/images/bgON.gif HTTP/1.1" 304 -
"http://virus.thaicert.org/stylesheets/_menu.css?1213106214"
"Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.8.0.4)
Gecko/20060602 Firefox/1.5.0.4"

Chillispot Log
Aug 13 20:34:05 192.168.1.21  chillispot[1099]: chilli.c: 3200:
Client MAC=00-1B-77-0A-F8-20 assigned IP 192.168.1.122

Aug 13 20:34:10 192.168.1.21 chillispot[1102]: chilli.c: 3502:
Successful UAM login from username=56F7hesa IP=192.168.1.122
```

รูปที่ ข.1 ตัวอย่างข้อมูลจราจรทางคอมพิวเตอร์ จากการต่อเชื่อมเข้าถึงระบบเครือข่าย

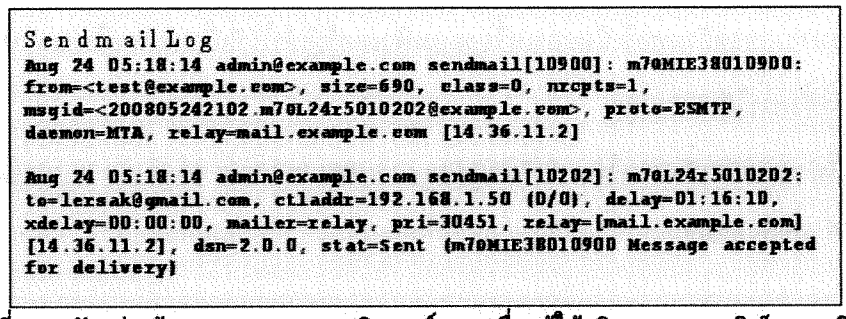
ข.2 ข้อมูลจราจรทางคอมพิวเตอร์ จากเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (e-mail servers)

รายการข้อมูลที่ต้องจัดเก็บ

- ข้อมูลจราจรทางคอมพิวเตอร์ที่บันทึกไว้เมื่อเข้าถึงเครื่องให้บริการไปรษณีย์อิเล็กทรอนิกส์ (SMTP) ซึ่งได้แก่
  - * ข้อมูลชื่อที่อยู่อิเล็กทรอนิกส์ของผู้ส่ง (Sender E-mail Address)
  - * ข้อมูลหมายเลขของข้อความที่ระบุในจดหมายอิเล็กทรอนิกส์ (Message ID)
  - * ข้อมูลชื่อที่อยู่อิเล็กทรอนิกส์ของผู้รับ (Receiver E-mail Address)

* ข้อมูลที่บอกถึงสถานะในการตรวจสอบ (Status Indicator) ซึ่งได้แก่ จดหมายอิเล็กทรอนิกส์ที่ส่งสำเร็จ จดหมายอิเล็กทรอนิกส์ที่ส่งคืน จดหมายอิเล็กทรอนิกส์ที่มีการส่งล่าช้า เป็นต้น

- ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้ใช้บริการที่เชื่อมต่ออยู่ขณะเข้ามาใช้บริการ (IP Address of Client Connected to Server)
- ข้อมูลวันและเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and time of connection of Client Connected to server)
- ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องบริการจดหมายอิเล็กทรอนิกส์ที่ถูกเชื่อมต่ออยู่ใน ขณะนั้น (IP Address of Sending Computer)
- ชื่อผู้ใช้งาน (User ID) (ถ้ามี)
- ข้อมูลที่บันทึก การเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ ผ่านโปรแกรมจัดการจากเครื่องของสมาชิก หรือเข้าถึงเพื่อเรียกข้อมูลจดหมายอิเล็กทรอนิกส์ไปยังเครื่องสมาชิก โดยยังคงจัดเก็บข้อมูลที่บันทึกการเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ที่ดึง ไปนั้น ไว้ที่เครื่องให้บริการ หรือ POP3 Log หรือ IMAP4 Log


Sendmail Log

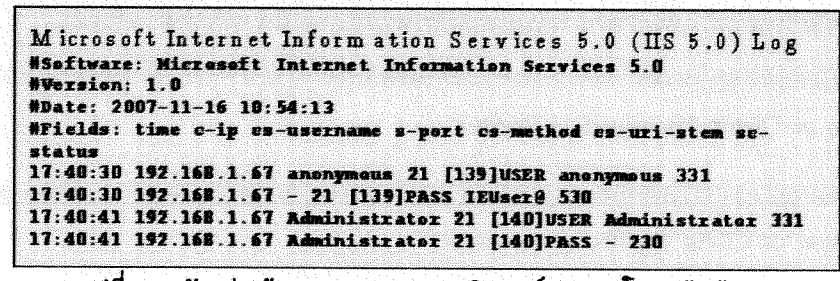
```
Aug 24 05:18:14 admin@example.com sendmail[10900]: m70MIE3B010900:
from=<test@example.com>, size=690, class=0, nrcpts=1,
msgid=<200805242102.m70L24x5010202@example.com>, proto=ESMTP,
daemon=MTA, relay=mail.example.com [14.36.11.2]

Aug 24 05:18:14 admin@example.com sendmail[10202]: m70L24x5010202:
to=lersak@gmail.com, ctladdr=192.168.1.50 (0/0), delay=01:16:10,
xdelay=00:00:00, mailer=relay, pri=30451, relay=[mail.example.com]
[14.36.11.2], dsn=2.0.0, stat=Sent (m70MIE3B010900 Message accepted
for delivery)
```

รูปที่ ข.2 ตัวอย่างข้อมูลจราจรทางคอมพิวเตอร์จากเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์

ข.3 ข้อมูลจราจรทางคอมพิวเตอร์ จากการโอนแฟ้มข้อมูลบนเครื่องให้บริการโอนแฟ้มข้อมูล

รายการข้อมูลที่ต้องจัดเก็บ

- ข้อมูลจราจรทางคอมพิวเตอร์ที่บันทึกเมื่อมีการเข้าถึงเครื่องให้บริการโอนแฟ้มข้อมูล
- ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and Time of Connection of Client to Server)
- ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้เข้าใช้ที่เชื่อมต่ออยู่ในขณะนั้น (IP Source Address)
- ข้อมูลชื่อผู้ใช้งาน (User ID) (ถ้ามี)
- ข้อมูลเส้นทาง (Path) และชื่อไฟล์ที่อยู่บนเครื่องให้บริการโอนถ่ายข้อมูลที่มีการส่งขึ้นมาบันทึก หรือดึงให้ข้อมูลออกไป (Path and Filename of Data Object Uploaded or Downloaded)



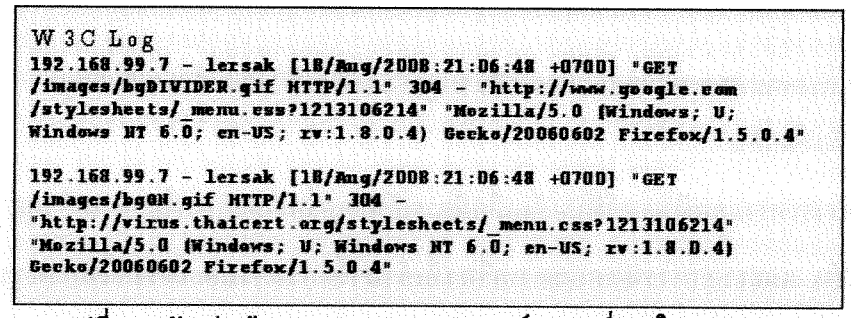
```
Microsoft Internet Information Services 5.0 (IIS 5.0) Log
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2007-11-16 10:54:13
#Fields: time c-ip cs-username s-port cs-method cs-uri-stem sc-
status
17:40:30 192.168.1.67 anonymous 21 [139]USER anonymous 331
17:40:30 192.168.1.67 - 21 [139]PASS IEUser@ 530
17:40:41 192.168.1.67 Administrator 21 [140]USER Administrator 331
17:40:41 192.168.1.67 Administrator 21 [140]PASS - 230
```

รูปที่ ข.3 ตัวอย่างข้อมูลจราจรทางคอมพิวเตอร์จากการโอนแฟ้มข้อมูล บนเครื่องให้บริการโอนแฟ้มข้อมูล

ข.4 ข้อมูลจราจรทางคอมพิวเตอร์ จากเครื่องผู้ให้บริการเว็บ

รายการข้อมูลที่ต้องจัดเก็บ

- ข้อมูลจราจรทางคอมพิวเตอร์ที่บันทึกเมื่อมีการเข้าถึงเครื่องผู้ให้บริการเว็บ
- ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ
- ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้เข้าใช้ที่เชื่อมต่ออยู่ในขณะนั้น
- ข้อมูลคำสั่งการใช้งานระบบ
- ข้อมูลที่บ่งบอกถึงเส้นทางในการเรียกดูข้อมูล (URI: Uniform Resource Identifier) เช่น ตำแหน่งของหน้าเว็บ (web page)



```
W3C Log
192.168.99.7 - lersak [18/Aug/2008:21:06:48 +0700] "GET
/images/bgDIVIDER.gif HTTP/1.1" 304 - "http://www.google.com
/stylesheets/_menu.css?1213106214" "Mozilla/5.0 (Windows; U;
Windows NT 6.0; en-US; rv:1.8.0.4) Gecko/20060602 Firefox/1.5.0.4"

192.168.99.7 - lersak [18/Aug/2008:21:06:48 +0700] "GET
/images/bgON.gif HTTP/1.1" 304 -
"http://virus.thaicert.org/stylesheets/_menu.css?1213106214"
"Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.8.0.4)
Gecko/20060602 Firefox/1.5.0.4"
```

รูปที่ ข.4 ตัวอย่างข้อมูลจราจรทางคอมพิวเตอร์ จากเครื่องผู้ให้บริการเว็บ

ข.5. ข้อมูลจราจรทางคอมพิวเตอร์ จากเครือข่ายคอมพิวเตอร์ขนาดใหญ่ (Usenet)

รายการข้อมูลที่ต้องจัดเก็บ

- ข้อมูลประวัติที่บันทึกเมื่อมีการเข้าถึงเครือข่าย (NNTP หรือ Network News Transfer Protocol Log)

- ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and Time of Connection of Client to Server)
- ข้อมูลหมายเลข Port ในการใช้งาน (Protocol Process ID)
- ข้อมูลชื่อเครื่องให้บริการ (Host Name)
- ข้อมูลหมายเลขลำดับข้อความที่ได้ถูกส่งไปแล้ว (Posted Message ID)

```
187.58.96.87, user, 12/1/2007, 14:37:37, NNTPSVC1, NEWS_Server,
134.56.87.11, 2814, 11, 513, 220, 0, article, 6
arlql#SHHGA.425@serve, microsoft.public.ins

207.46.248.16, <feed>, 4/29/2007, 11:49:10, NNTPSVC1, NEWS_Server,
134.56.87.11, 890, 0, 61, 502, 0, newnews, Access Denied.,
microsoft.public.windows.server.sbs 060101 080000 GMT,
```

รูปที่ ข.5 ตัวอย่างข้อมูลจราจรทางคอมพิวเตอร์ จากเครือข่ายคอมพิวเตอร์ขนาดใหญ่ (Usenet)

ข 6. ข้อมูลจราจรทางคอมพิวเตอร์ จากการโต้ตอบกันบนเครือข่ายคอมพิวเตอร์

รายการข้อมูลที่ต้องจัดเก็บ

- ข้อมูลเกี่ยวกับวัน เวลาการติดต่อของผู้ใช้บริการ (Date and Time of Connection of Client to Server)
- ข้อมูลชื่อเครื่องบนเครือข่าย (Client Hostname and/or IP Address)ข้อมูลหมายเลข Port ในการใช้งาน (Protocol Process ID)
- หมายเลขเครื่องของผู้ให้บริการที่เครื่องคอมพิวเตอร์เชื่อมต่ออยู่ในขณะนั้น (Destination Hostname and/or IP Address)

หมายเหตุ ตัวอย่างการโต้ตอบกันบนเครือข่ายคอมพิวเตอร์ ได้แก่ Internet Relay Chat (IRC) หรือ Instance Messaging (IM) เป็นต้น

```
1205326745.661 1912 192.168.42.165 TCP_MISS/200 8460 CONNECT
login.live.com:443/ - DIRECT/login.live.com - CMF:40 DCF:20 ERR:0
DEFAULT_CASE-DefaultGroup
```

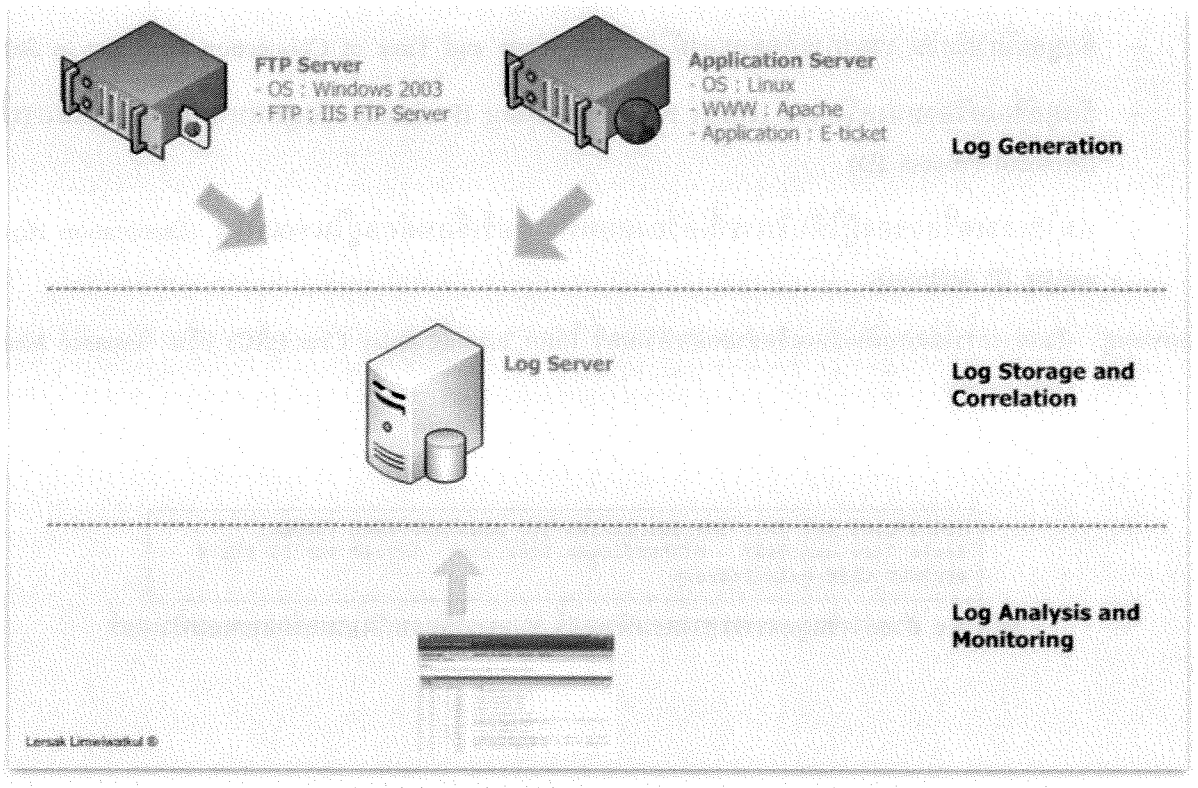
รูปที่ ข.6 ตัวอย่างข้อมูลจราจรทางคอมพิวเตอร์ จากการโต้ตอบกันบนเครือข่ายคอมพิวเตอร์

ภาคผนวก ค
กระบวนการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์เป็นส่วนหนึ่งของกระบวนการจัดเก็บข้อมูลจราจราทางคอมพิวเตอร์ ซึ่งจะทำงานเกี่ยวข้องเชื่อมโยงกันทั้งฮาร์ดแวร์ ซอฟต์แวร์ ระบบและอุปกรณ์เครือข่ายต่างๆ รวมถึงสื่อบันทึกข้อมูลที่เลือกใช้ เพื่อให้ได้ข้อมูลจราจรทางคอมพิวเตอร์ มาเก็บรักษาไว้ตามวัตถุประสงค์ที่ต้องการ

ค.1 ส่วนประกอบในกระบวนการจัด เก็บข้อมูลจราจรทางคอมพิวเตอร์

สำหรับองค์กรทั่วไป กระบวนการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (ดูเอกสารอ้างอิง 3.15) จะสามารถแบ่งส่วนประกอบหลักได้เป็น 3 ส่วน คือ ส่วนของการสร้างข้อมูลจราจรทางคอมพิวเตอร์และการส่งผ่านข้อมูลจราจรทางคอมพิวเตอร์(ซึ่งปกติจะส่งผ่านเครือข่ายท้องถิ่นหรือเครือข่ายส่วนบุคคล) ส่วนของการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (รวมถึงส่วนของการตัดสินอนุญาตให้ลบข้อมูลจราจรทางคอมพิวเตอร์ หากพิจารณาแล้วว่าไม่มีความจำเป็นต้องเก็บในระบบแล้ว) และส่วนของการวิเคราะห์และเฝ้าระวังข้อมูลจราจรทางคอมพิวเตอร์ ดังได้แสดงไว้ในรูป ค.1



รูปที่ ค.1 ตัวอย่างกระบวนการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

- **ส่วนสร้างข้อมูลจราจรทางคอมพิวเตอร์** ทำหน้าที่เป็นแหล่งกำเนิดหรือสร้างข้อมูลจราจรทางคอมพิวเตอร์ (Log Generation) ปกติข้อมูลจราจรทางคอมพิวเตอร์จะสร้างขึ้นบนเครื่องให้บริการ(เครื่องเซิร์ฟเวอร์) หรือ Log Source ที่ให้บริการอย่างใดอย่างหนึ่ง หรืออุปกรณ์บนระบบเครือข่ายที่มีข้อมูลจราจรทางคอมพิวเตอร์จากระบบปฏิบัติการและซอฟต์แวร์ประยุกต์

การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้บนเครื่องให้บริการที่สร้างข้อมูลนั้นขึ้นมา หรือในอุปกรณ์ที่เครื่องนั้นควบคุมโดยตรงได้ เรียกว่าการจัดเก็บแบบปฐมภูมิ (Primary Logging) ในกรณีที่มีการส่งผ่านข้อมูลจราจรทางคอมพิวเตอร์ไปเก็บรักษาที่เครื่องหรือระบบอื่นซึ่งไม่ใช่เครื่องที่สร้างข้อมูลขึ้นมา อาทิ เครื่องให้บริการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log server) เรียกว่า การจัดเก็บแบบทุติยภูมิ (Secondary Logging)

- **ส่วนของการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์** ทำหน้าที่รับข้อมูลจราจรทางเคอมพิวเตอร์ที่ได้จากแหล่งกำเนิด (Log Storage and Correlation) และจัดเก็บตามรูปแบบ วิธี และระยะเวลาที่กำหนดไว้ ทั้งนี้อาจรวมถึงการแปลงหรือเข้ารหัสข้อมูลจราจรทางคอมพิวเตอร์ ให้อยู่ในรูปแบบที่เหมาะสมกับการจัดเก็บด้วย ส่วนนี้จะหมายรวมถึงสื่อที่ใช้ในการบันทึกข้อมูลที่จัดเก็บด้วย

ในบางกรณี ส่วนนี้อาจทำหน้าที่เสริมในการเปลี่ยนการจัดรูปแบบข้อมูลจราจรทางคอมพิวเตอร์ให้อยู่ในรูปแบบที่พร้อมสำหรับการนำไปใช้วิเคราะห์ต่อได้

สำหรับเครื่องให้บริการที่มีความสามารถในการรับข้อมูลจราจรทางคอมพิวเตอร์จากแหล่งกำเนิดข้อมูลจราจรทางคอมพิวเตอร์จำนวนมาก อาจถูกเรียกว่า Collectors หรือ Aggregators

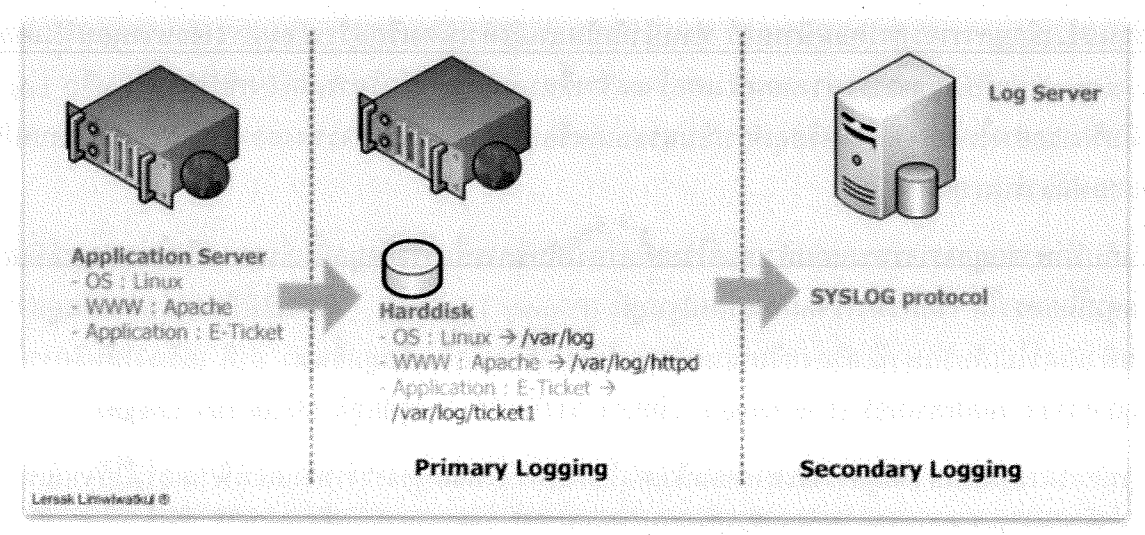
- **ส่วนของการวิเคราะห์และเฝ้าระวังข้อมูลจราจรทางคอมพิวเตอร์** ทำหน้าที่เป็นส่วนติดต่อกับผู้ดูแลระบบหรือผู้ดูแลข้อมูลแล้วแต่กรณี (Log Analysis and Monitoring) โดยจะทำหน้าที่วิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ที่เก็บรักษาไว้ เฝ้าระวังบูรณภาพของข้อมูล และช่วยในการตรวจสอบค่าที่ตั้งไว้ โดยทั่วไปส่วนนี้มักติดตั้งหรือทำงานอยู่บนเครื่องหรือระบบเดียวกันกับส่วนของการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

บางระบบสนับสนุนการสร้างรายงานการวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ รวมถึงสามารถตั้งค่าการแจ้งเตือนผู้เกี่ยวข้องโดยอัตโนมัติได้ ทั้งนี้เพื่อให้ข้อมูลเร็วและตรงกับความเป็นจริงในปัจจุบันที่สุด

ค.2 การจัดเก็บแบบปฐมภูมิ (Primary Logging) และการจัดเก็บแบบทุติยภูมิ (Secondary Logging)

โดยปกติแล้วเครื่องให้บริการหรืออุปกรณ์เครือข่าย มักจะสามารถสร้างและจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ได้ในตัว รวมถึงสามารถตั้งค่าให้มีการส่งผ่านข้อมูลจราจรทางคอมพิวเตอร์ไปยังระบบหรือเครื่องให้บริการอื่นได้ ทั้งนี้การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ สามารถแยกได้เป็น 2 แบบคือ

- การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์บนตัวระบบที่สร้างข้อมูลนั้นขึ้นมาเอง เรียกว่า การจัดเก็บแบบปฐมภูมิ (Primary Logging)
- การจัดส่งข้อมูลจราจรทางคอมพิวเตอร์ไปบันทึกหรือจัดเก็บที่เครื่องหรือระบบอื่น เรียกว่า การจัดเก็บแบบทุติยภูมิ (Secondary Logging)



รูปที่ ค.2 การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์แบบปฐมภูมิ (Primary Logging) และแบบทุติยภูมิ (Secondary Logging)

การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์แบบปฐมภูมิ ปกติจะเป็นการจัดเก็บข้อมูลบนฮาร์ดดิสก์หรือสื่อบันทึกข้อมูลบนตัวอุปกรณ์หรือระบบที่กำเนิดข้อมูลจราจรทางคอมพิวเตอร์เอง ในรูปที่ ค.2 เป็นตัวอย่างการเก็บข้อมูลทางคอมพิวเตอร์ แยกตามข้อมูลทางคอมพิวเตอร์ของระบบปฏิบัติการ ในตัวอย่างนี้ใช้เป็นระบบปฏิบัติการลีนุกซ์ ข้อมูลจราจรทางคอมพิวเตอร์ของเว็บเซิร์ฟเวอร์และข้อมูลจราจรทางคอมพิวเตอร์ของระบบแอพพลิเคชัน ในที่นี้เป็นระบบ E-ticket ระบบปฏิบัติการลีนุกซ์จะบันทึกข้อมูลจราจรทางคอมพิวเตอร์ไว้ในไดเรกทอรี /var/log/httpd และ /var/log/ticket1 เป็นต้น

การจัดส่งข้อมูลจราจรทางคอมพิวเตอร์ไปบันทึกหรือเก็บรักษาไว้ที่เครื่องให้บริการจัดเก็บล็อก (ล็อกเซิร์ฟเวอร์) ตามที่แสดงไว้ในรูปนั้น สามารถส่งผ่านระบบเครือข่ายได้อีกหลายรูปแบบ ตัวอย่างเช่น

- ส่งข้อมูลตามรูปแบบของไฟล์ไบนารีหรือการเรียกใช้ Application Programming Interface หรือ API ของล็อกเซิร์ฟเวอร์เพื่อส่งข้อมูลจราจรทางคอมพิวเตอร์
- ส่งข้อมูลในรูปแบบของไฟล์ เช่นส่งไฟล์เป็น TEXT หรือรูปแบบไฟล์ CSV (Comma-Separated) ผ่านโปรโตคอล รับ-ส่งไฟล์ (File Transfer Protocol หรือ FTP)
- ส่งข้อมูลในรูปแบบมาตรฐาน SYSLOG เป็นโพรโตคอล UDP ใช้หมายเลขพอร์ตเป็น 514 นิยมใช้กับระบบปฏิบัติตระกูลยูนิกซ์และลีนุกซ์ ซึ่งใช้เป็นตัวอย่าง ตามรูปที่ ค.2
- ส่งข้อมูลในรูปแบบมาตรฐาน EVENTLOG ซึ่งเป็นรูปแบบของไฟล์หรือผ่านสคริปต์การส่งข้อมูล EVENTLOG นิยมใช้บนระบบปฏิบัติการตระกูลไมโครซอฟต์วินโดวส์
- ส่งข้อมูลในรูปแบบของระบบฐานข้อมูลด้วยโครงสร้างภาษา SQL หรือ Structure Query Language เพื่อส่งข้อมูลจราจรทางคอมพิวเตอร์ไปเก็บที่ระบบบริหารจัดการฐานข้อมูลหรือ Database Management

System บนล็อกเซิร์ฟเวอร์โดยตรง

- ใช้การส่งข้อมูลผ่านโพรโตคอล Simple Network Management Protocol หรือ SNMP
- ส่งข้อมูลในรูปแบบ XML หรือ XHTML ผ่านโพรโตคอล SOAP

เครื่องให้บริการจัดเก็บล็อกหรือล็อกเซิร์ฟเวอร์ ซึ่งทำหน้าที่จัดเก็บข้อมูลแบบทุติยภูมิ นอกจากทำหน้าที่หลักในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์แล้ว ยังมีความสามารถอื่นเพิ่มเติมได้อีก อาทิ การเก็บสำรองข้อมูลจราจรทางคอมพิวเตอร์ การเพิ่มเติมระบบป้องกันการเข้าถึงหรือควบคุมการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต การช่วยวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ รวมถึงบริหารจัดการข้อมูลจราจรทางคอมพิวเตอร์ชั้นสูง เป็นต้น รวมถึงอาจทำงานเป็นส่วนหนึ่งของเครื่องให้บริการ (ที่ไม่ได้สร้างข้อมูลจราจรทางคอมพิวเตอร์) หรือประกอบรวมกันด้วยวิธีใดวิธีหนึ่งจากหลายเครื่องรวมกันเป็นระบบก็ได้

ชื่อเรียกต่อไปนี้ เป็นตัวอย่างของเครื่องหรือระบบที่จัดเก็บข้อมูลแบบทุติยภูมิ

- เครื่องให้บริการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์แบบศูนย์กลาง (Centralized Log Server)
- เครื่องให้บริการบริหารจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์แบบศูนย์กลาง(Centralized Log Management Server)
- ระบบบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Event Manager System / SEM) ทำหน้าที่เก็บบันทึกข้อมูลเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้นภายในระบบสารสนเทศ
- ระบบบริหารจัดการข้อมูลเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Information Management System / SIM) ทำหน้าที่เก็บบันทึกข้อมูลเหตุการณ์ ตอบสนองผ่านการวิเคราะห์และสรุป เพื่อให้ผู้เชี่ยวชาญระบบความมั่นคงปลอดภัยนำไปวิเคราะห์ต่อได้อย่างแม่นยำ มักมีการนำไปใช้ในระบบวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ระดับสูง เพื่อติดตามปัญหา วิเคราะห์ปัญหา และหาสาเหตุของปัญหาทางด้านความมั่นคงปลอดภัยอย่างเป็นระบบ

ค.3 บูรณภาพและความมั่นคงปลอดภัยของการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

ในทางปฏิบัติแล้ว การจัดเก็บแบบทุติยภูมินั้น มีระดับความเสี่ยงต่ออันตรายและภัยคุกคามน้อยกว่า การจัดเก็บแบบปฐมภูมิ เนื่องจาก

- สามารถควบคุมและบริหารจัดการความมั่นคงปลอดภัยของข้อมูลจราจรทางคอมพิวเตอร์ ผ่านการควบคุมและจำกัดการเข้าถึง การป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต การสำรองข้อมูลจราจรทางคอมพิวเตอร์ ดำเนินการผ่านศูนย์กลางหรือล็อกเซิร์ฟเวอร์เพียงจุดเดียว
- เพิ่มระดับความมั่นคงปลอดภัยให้กับข้อมูลจราจรทางคอมพิวเตอร์ ในกรณีที่ผู้บุกรุกเข้าถึงระบบโดยไม่ได้รับอนุญาตนั้น ข้อมูลจราจรทางคอมพิวเตอร์ที่เครื่องที่สร้างข้อมูล (Primary Logging) มักจะถูกแก้ไขหรือ

ถูกลบข้อมูลการเข้ามาในระบบ หรือโดยมากมักจะพิจารณาได้โดยทันทีว่าในกรณีที่ระบบถูกบุกรุกโดยไม่ได้รับอนุญาตนั้น ข้อมูลจราจรทางคอมพิวเตอร์ที่บันทึกและเก็บไว้แบบปฐมภูมินั้น จะมีความน่าเชื่อถือและความถูกต้องน้อยมากจนไม่สามารถนำมาพิจารณาได้ทั้งหมด

- สามารถประเมินระดับความต้องการและขีดความสามารถในการรองรับการเก็บข้อมูลจราจรทางคอมพิวเตอร์ได้อย่างมีประสิทธิภาพ เช่น การติดตามปริมาณของการเก็บข้อมูลจราจรทางคอมพิวเตอร์บนสื่อบันทึกข้อมูลหรือฮาร์ดดิสก์เฉพาะที่ล็อกเซิร์ฟเวอร์ เพื่อประเมินแนวโน้มอัตราการเติบโตของข้อมูลจราจรทางคอมพิวเตอร์เป็นต้น
- สามารถนำข้อมูลจราจรทางคอมพิวเตอร์ที่ศูนย์กลางไปใช้วิเคราะห์ได้อย่างรวดเร็วและมีประสิทธิภาพ รวมถึงการเพิ่มเติมความสามารถอื่นๆ สามารถทำได้โดยไม่มีผลกระทบต่อสมรรถนะของเครื่องให้บริการ อาทิ การตั้งให้แจ้งเตือนเป็นแบบทันที (Real-time) หรือ การเพิ่มส่วนสนับสนุนการวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์แบบ Off-line ก็ย่อมได้โดยง่าย