



พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับ คอมพิวเตอร์ พ.ศ. 2550

“จากพ.ร.บ. สู่การปฏิบัติ
การเก็บข้อมูลจราจรคอมพิวเตอร์ “

ชยา ลิ้มจิตติ

สำนักเทคโนโลยีสารสนเทศ จุฬาลงกรณ์มหาวิทยาลัย

26 กุมภาพันธ์ 2551



- ความเป็นมา
- สรุปสาระสำคัญของ พ.ร.บ.ฯ
- สรุปสาระสำคัญของประกาศกฎกระทรวง
- ผลกระทบต่อมหาวิทยาลัย/สถาบันการศึกษา
- แนวปฏิบัติตามพ.ร.บ.ฯ และ ประกาศกฎกระทรวง
- ตัวอย่างแนวปฏิบัติเพื่อเก็บข้อมูลจรรยาบรรณคอมพิวเตอร์



- พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มีผลบังคับใช้แล้วตั้งแต่วันที่ ๑๘ กรกฎาคม ๒๕๕๐ โดย มาตรา ๒๖ ของพ.ร.บ. ดังกล่าว มีข้อความส่วนหนึ่งว่า “ผู้ให้บริการต้องเก็บข้อมูลจราจรคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับตั้งแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ ผู้ให้บริการจะต้องเก็บรักษาข้อมูลผู้ให้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ให้บริการนับตั้งแต่เริ่มให้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การให้บริการสิ้นสุดลง”
- กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้ประกาศ หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐ ซึ่งมีผลบังคับใช้วันศุกร์ที่ ๒๓ สิงหาคม ๒๕๕๐ โดยในประกาศนี้ จัดให้สถาบันการศึกษาเป็นผู้ให้บริการประเภท ข ซึ่งต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. ๒ โดยต้องเริ่มเก็บข้อมูลจราจรทางคอมพิวเตอร์ตั้งแต่วันที่ วันอาทิตย์ที่ ๒๓ สิงหาคม ๒๕๕๑



สรุปสาระสำคัญของ พ.ร.บ.ฯ

- ส่วนทั่วไป (มาตรา ๑- ๔)
- ความผิดเกี่ยวกับคอมพิวเตอร์และบทลงโทษ (มาตรา ๕ - ๑๗)
- พนักงานเจ้าหน้าที่ (คุณสมบัติ อำนาจหน้าที่ และความผิด) (มาตรา ๑๘ – ๒๕ และ ๒๘ – ๒๙)
- ผู้ให้บริการ(หน้าที่ ความผิดและบทลงโทษ) (มาตรา ๒๖ – ๒๗)



สรุปสาระสำคัญของประกาศกฎกระทรวง

- เก็บข้อมูลจราจรคอมพิวเตอร์ที่สามารถรักษาความถี่ที่แท้จริง (ข้อ ๘(๑))
- กำหนดชั้นความลับของข้อมูลและต้องระบุตัวบุคคลที่สามารถเข้าถึงข้อมูลจราจรคอมพิวเตอร์ได้ (ข้อ ๘(๒))
- ไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลจราจรคอมพิวเตอร์ได้ (ข้อ ๘(๒))
- ให้มีผู้ประสานงานและให้ข้อมูลกับพนักงาน (ข้อ ๘(๓))
- ต้องระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้ (ข้อ ๘(๔))
- ต้องตั้งนาฬิกาให้ตรงกับเวลาอ้างอิงสากล (ข้อ ๙)



ผลกระทบต่อมหาวิทยาลัย/สถาบันการศึกษา

- ผลกระทบต่อบุคลากร และนิสิต นักศึกษา
 - บุคลากรและนิสิตอาจจะต้องรับโทษหากกระทำผิด ตามมาตรา ๕ - ๑๗
- ผลกระทบต่อคณะ/สถาบัน/หน่วยงานต่างๆในมหาวิทยาลัย
 - อาจจะต้องระวางโทษเช่นเดียวกับผู้กระทำผิด หากพิสูจน์ได้ว่า จงใจสนับสนุนหรือยินยอมให้มีการกระทำผิดตามมาตรา ๑๔ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของหน่วยงาน (มาตรา ๑๕)
 - ต้องจัดเก็บข้อมูลจราจรคอมพิวเตอร์ หากหน่วยงานนั้นมีบริการต่างๆที่ระบุไว้ในภาคผนวก ข.ของ ประกาศกระทรวงฯ เช่นมี e-mail servers หรือมี web servers เป็นต้น (ประกาศกระทรวงฯ ข้อ ๗)



ผลกระทบต่อมหาวิทยาลัย/สถาบันการศึกษา(ต่อ)

- ผลกระทบต่อคณะ/สถาบัน/หน่วยงานต่างๆในมหาวิทยาลัย
 - ต้องจัดให้มีระบบเก็บรักษาความลับของข้อมูลจราจรคอมพิวเตอร์ที่จัดเก็บ (ประกาศกระทรวงฯ ข้อ ๘ (๒))
 - ต้องแต่งตั้งผู้มีหน้าที่เกี่ยวข้องที่สามารถเข้าถึงข้อมูลจราจรคอมพิวเตอร์ที่จัดเก็บ (ประกาศกระทรวงฯ ข้อ ๘ (๒))



- บุคลากรและนิสิต
 - ไม่กระทำความผิดเกี่ยวกับคอมพิวเตอร์
- คณะ/สถาบัน/หน่วยงานต่างๆในมหาวิทยาลัย/สถาบันการศึกษา
 - ประชาสัมพันธ์ให้บุคลากรและนิสิตในสังกัดทราบถึงความผิดและแนวปฏิบัติตามพ.ร.บฯ นี้
 - กำหนดมาตรการเพื่อลดความเสี่ยงที่จะเป็นการจูงใจสนับสนุนหรือยินยอมให้มีการกระทำผิดตามมาตรา ๑๔ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุม
 - จัดทำระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (หากมีบริการต่างๆตามประกาศกระทรวงฯ หรือมีการใช้ NAT)



● มหาวิทยาลัย

- ❑ ประชาสัมพันธ์ให้บุคลากรและนิสิตในสังกัดทราบถึงความผิดตามพ.ร.บฯ นี้
- ❑ กำหนดมาตรการเพื่อลดความเสี่ยงที่จะเป็นการจูงใจสนับสนุนหรือยินยอมให้มีการกระทำผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุม
- ❑ จัดทำระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์
- ❑ แต่งตั้งผู้มีหน้าที่ประสานงานและให้ข้อมูลกับพนักงานเจ้าหน้าที่ เพื่อการส่งมอบข้อมูลจราจรคอมพิวเตอร์ (ประกาศกระทรวงฯ ข้อ ๘ (๓))



การตั้งนาฬิกาของอุปกรณ์บริการ

- ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
 - เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ของผู้ให้บริการ

ข้อ ๘ เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริงผู้ให้บริการต้องตั้งนาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

ตัวอย่างแนวปฏิบัติเพื่อเก็บข้อมูลจราจรคอมพิวเตอร์

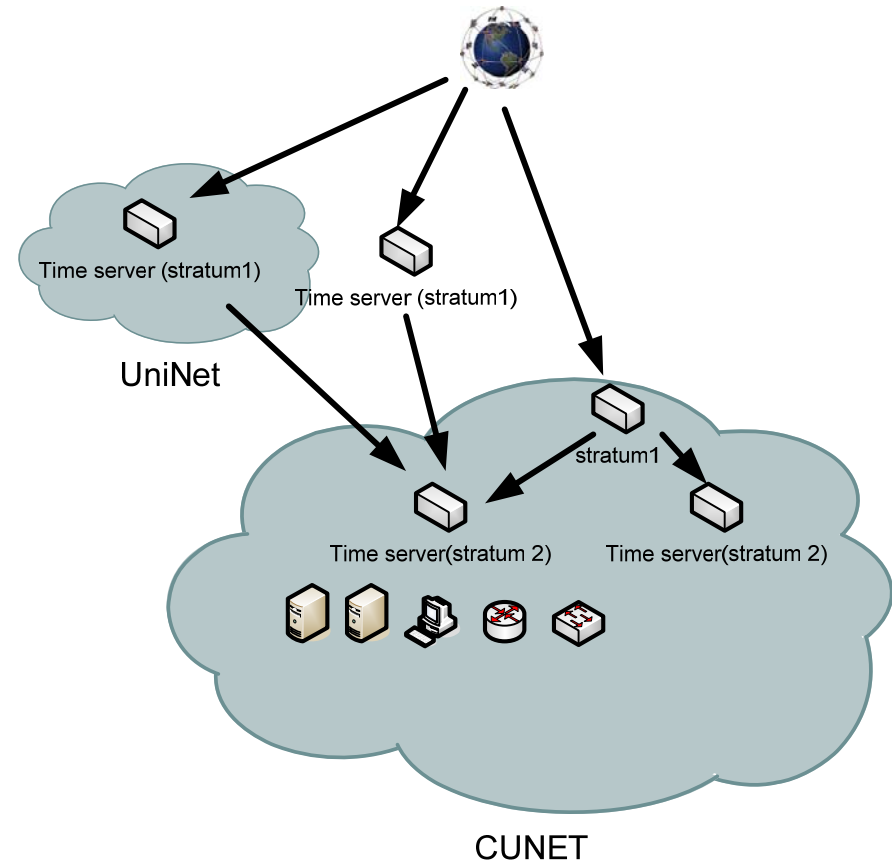


- การตั้งเวลาอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล
- การปรับเวลาให้ตรงกันให้ทำได้โดยใช้โปรโตคอล NTP ซึ่งเป็นโปรโตคอลมาตรฐานที่มีในอุปกรณ์เครือข่ายๆและเครื่องคอมพิวเตอร์ เป็นส่วนใหญ่
 - NTP server
 - ntp.chula.ac.th
 - NTP client
 - UNIX (/etc/ntp.conf)
 - Windows (ควรตั้งผ่าน GPO)

ตัวอย่างแนวปฏิบัติเพื่อเก็บข้อมูลจราจรคอมพิวเตอร์



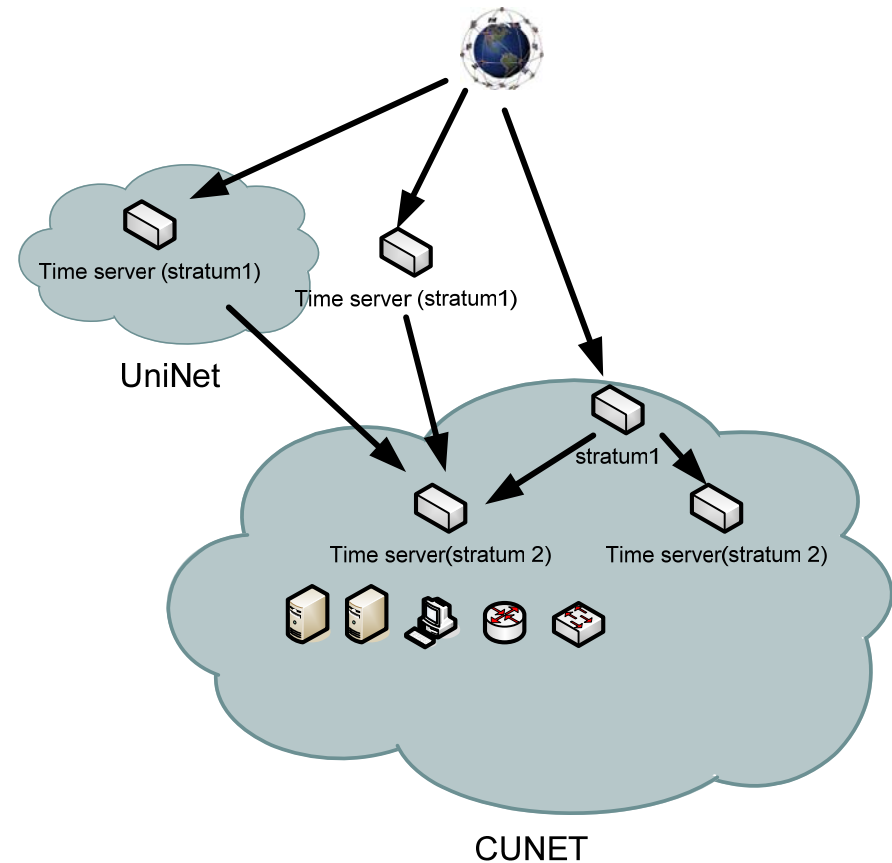
- การตั้งเวลาอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล
- ตัวอย่างไฟล์ ntp.conf
- ตัวอย่างการใช้ GPO
- ข้อมูลเพิ่มเติมที่ <http://www.ntp.org>



ตัวอย่างแนวปฏิบัติเพื่อเก็บข้อมูลจราจรคอมพิวเตอร์



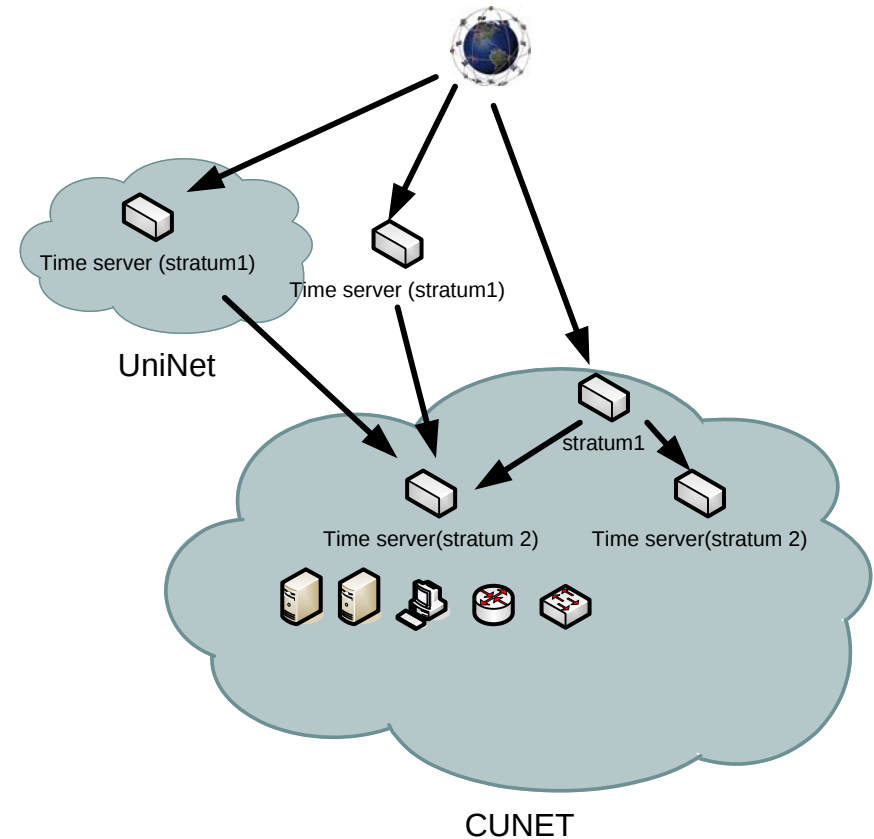
- การตั้งเวลาอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล
- ตัวอย่างไฟล์ ntp.conf
- ตัวอย่างการใช้ GPO
- ข้อมูลเพิ่มเติมที่ <http://www.ntp.org>



ตัวอย่างแนวปฏิบัติเพื่อเก็บข้อมูลจราจรคอมพิวเตอร์



- สำนักเทคโนโลยีสารสนเทศอยู่ระหว่างจัดหา time server (stratum 1)
- ให้บริการ stratum 1 กับคอมพิวเตอร์แม่ข่ายของคณะ/สถาบัน/หน่วยงานต่างๆ
- เครื่องลูกข่ายใช้บริการ ntp จากคอมพิวเตอร์แม่ข่ายของคณะ/สถาบัน/หน่วยงานนั้นๆ





การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์

● ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

□ เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ของผู้ให้บริการ

ข้อ ๘ การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ผู้ให้บริการต้องใช้วิธีการที่มั่นคงปลอดภัย ดังต่อไปนี้

(๑) เก็บในสื่อ (Media) ที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง (Integrity) และระบุตัวบุคคล (Identification) ที่เข้าถึงสื่อดังกล่าวได้

(๒) มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เช่น การเก็บไว้ใน Centralized Log Server หรือการทำ Data Archiving หรือทำ Data Hashing เป็นต้น เว้นแต่ ผู้มีหน้าที่เกี่ยวข้องที่เจ้าของหรือผู้บริหารองค์กร กำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ เช่น ผู้ตรวจสอบระบบสารสนเทศขององค์กร (IT Auditor) หรือบุคคลที่องค์กรมอบหมาย เป็นต้น รวมทั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้

ตัวอย่างแนวปฏิบัติเพื่อเก็บข้อมูลจราจรคอมพิวเตอร์



- การทำ Centralized log server โดยใช้เทคโนโลยี syslog
- syslog คือมาตรฐานในการรับส่งเหตุการณ์ต่างๆที่เกิดขึ้นกับระบบ
- มาตรฐานของระบบ syslog แบ่งเหตุต่างๆเป็นประเภท (Facility) และ ระดับของเหตุการณ์นั้นๆ (level)
 - Facility: mail, kern, daemon, user, local1, local2 เป็นต้น
 - Level: debug, info, notice, warning เป็นต้น
 - Facility จะช่วยแยกประเภทเหตุการณ์ที่เกิดขึ้นกับระบบ
 - Level จะเป็นตัวกำหนดว่า ต้องการข้อมูลละเอียดระดับใด



- โปรแกรม syslog client

- ☐ Network devices
- ☐ UNIX (เขียนโปรแกรมให้ส่งข้อมูลไปยัง syslog, Snare Agent)
- ☐ Windows (Snare Agent)

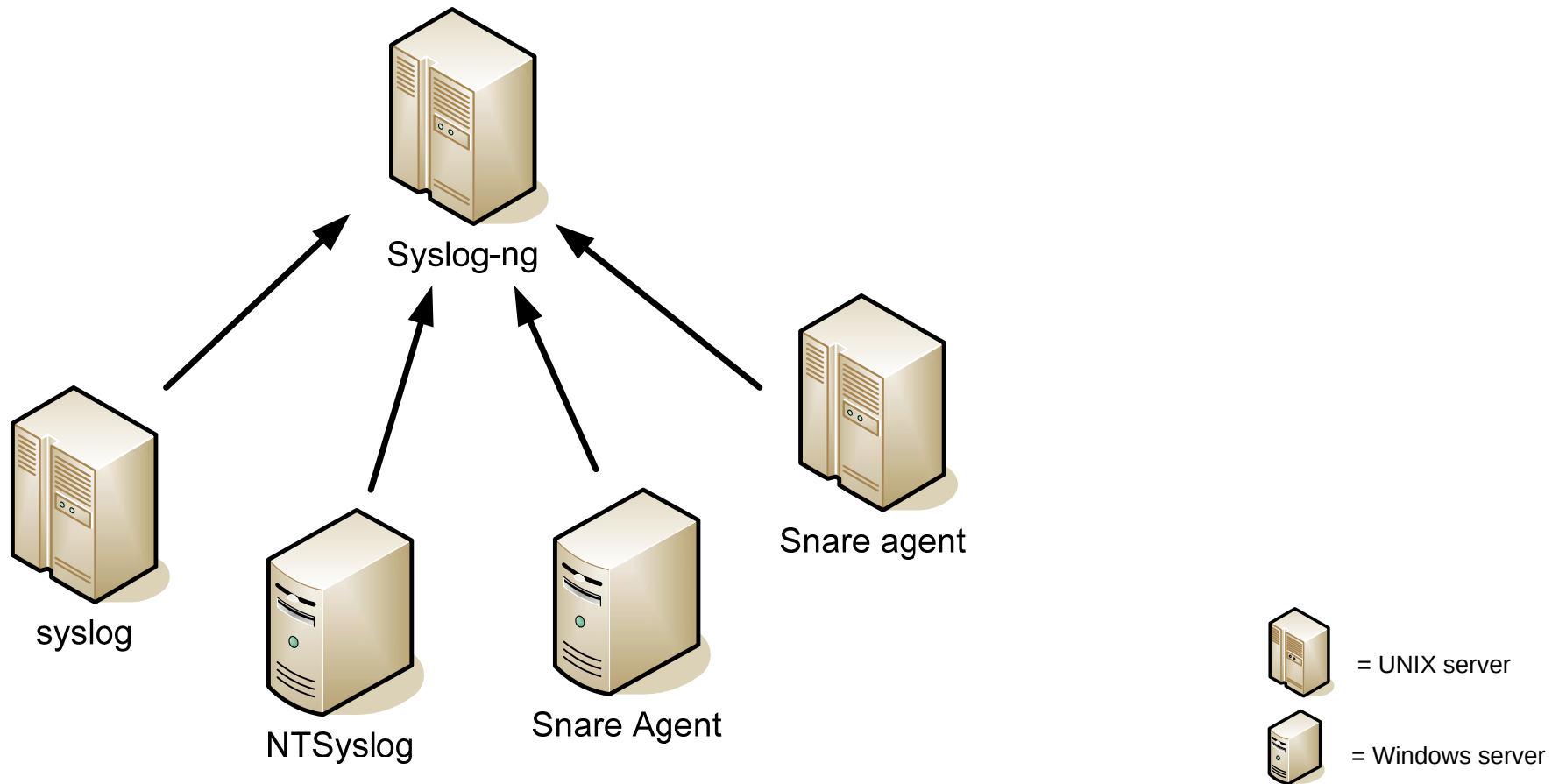
- โปรแกรม syslog server

- ☐ UNIX (Syslogd, syslog-ng)
- ☐ Windows (Snare BackLog, WinSyslog, KiWi Syslog)

ตัวอย่างแนวปฏิบัติเพื่อเก็บข้อมูลจราจรคอมพิวเตอร์



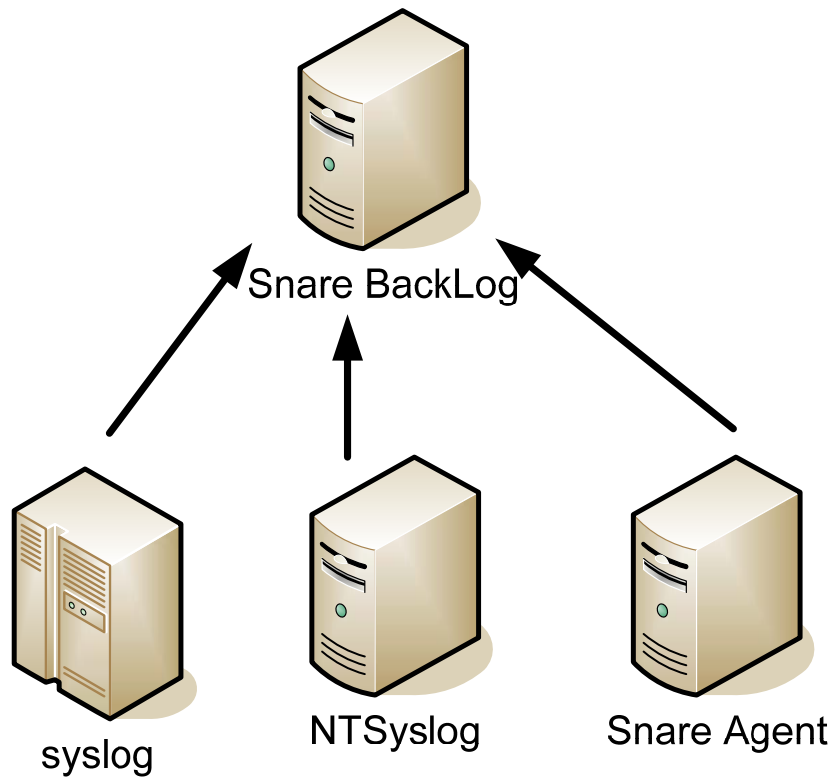
- ใช้ UNIX เป็น Centralized log server



ตัวอย่างแนวปฏิบัติเพื่อเก็บข้อมูลจราจรคอมพิวเตอร์



- ใช้ Windows เป็น Centralized log server



= UNIX server



= Windows server



นิยามประเภทของผู้ให้บริการ

- ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
 - เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ของผู้ให้บริการ

ภาคผนวก ก

แนบท้ายประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ
พ.ศ. ๒๕๕๐

ประเภท	ตัวอย่างของผู้ให้บริการ
ข.ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider)	๑) ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ทั้งมีสายและไร้สาย ๒) ผู้ประกอบการซึ่งให้บริการในการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ในห้องพัก ห้องเช่า โรงแรม หรือร้านอาหารและเครื่องดื่ม ในแต่ละกลุ่มอย่างหนึ่งอย่างใด ๓) ผู้ให้บริการเข้าถึงระบบเครือข่ายคอมพิวเตอร์สำหรับองค์กร เช่น หน่วยงานราชการ บริษัทหรือ สถาบันการศึกษา



- ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
 - เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ของผู้ให้บริการ

ภาคผนวก ข

แนบท้ายประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ

พ.ศ. ๒๕๕๐

๒. ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผู้ให้บริการตามประกาศข้อ ๕ (๑) ข. ถึง ค. มีหน้าที่ต้องเก็บรักษา มีดังต่อไปนี้

ตัวอย่างแนวปฏิบัติเพื่อเก็บข้อมูลจราจรคอมพิวเตอร์



- ข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย
- ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์
- ข้อมูลอินเทอร์เน็ตจากการโอนแฟ้มข้อมูลบนเครื่องให้บริการโอนแฟ้มข้อมูล
- ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บ

