การพัฒนาความรู้ความเข้าใจด้านความปลอดภัย

การศึกษาด้านความปลอดภัยประจำปี 2025

2025-10

YRC-CSIRT

INDEX

1. บทนำ

ทุกคนทราบถึงความเสี่ยงที่อาจเกิดขึ้นเมื่ออุปกรณ์ที่ใช้ในการดำเนินการทางธุรกิจติดไวรัสหรือไม่
อาจนำไปสู่ไม่เพียงแต่การรั่วไหลของข้อมูลส่วนบุคคลและความเสียหายทางการเงินเท่านั้น แต่ยังทำให้สูญเสียความน่าเชื่อถือของบริษัทอีกด้วย
เอกสารฉบับนี้จะอธิบายโดยเฉพาะถึงความเสี่ยงเหล่านี้ มาตรการป้องกันการติดไวรัส และแนวทางการปฏิบัติเมื่อสงสัยว่าอุปกรณ์อาจติดไวรัส

2. ความเสี่ยงจากการติดไวรัส

ความเสี่ยงจากการติดไวรัสมีอะไรบ้าง?

การเข้าถึงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต

หากอุปกรณ์ติดไวรัส ข้อมูลส่วนบุคคลและข้อมูลสำคัญที่จัดเก็บอยู่ในอุปกรณ์อาจถูกโจรกรรมหรือเข้าถึงโดยไม่ได้รับอนุญาต

■ ข้อมูลที่เป็นเป้าหมายหลักของการโจมตีทางไซเบอร์

- ข้อมูลส่วนบุคคล: ชื่อ ที่อยู่ หมายเลขโทรศัพท์ ที่อยู่อีเมล เป็นต้น
- ข้อมูลสำหรับการยืนยันตัวตน เช่น รหัสผู้ใช้ รหัสผ่าน ข้อมูลบัตรเครดิต และข้อมูลบัญชีธนาคาร เป็นต้น
- ข้อมูลที่มีความลับสูง เช่น เอกสารทางธุรกิจ รูปภาพ วิดีโอ และข้อมูลอื่น ๆ ที่เกี่ยวข้องกับการดำเนินงานขององค์กร ซึ่งหากรั่วไหลอาจส่งผลกระทบอย่างร้ายแรงต่อบริษัท

ความเสียหายทางการเงิน

สถานการณ์ดังกล่าวอาจก่อให้เกิดความเสียหายทางการเงินโดยตรงต่อองค์กร

- การใช้งานโดยไม่ได้รับอนุญาต ข้อมูลบัตรเครดิตหรือบัญชีธนาคารที่ถูกขโมยอาจถูกนำไปใช้ในการทำธุรกรรมออนไลน์ เช่น การซื้อสินค้า หรือการโอนเงิน โดยไม่ได้รับอนุญาตจากเจ้าของบัญชี
- การเรียกค่าไถ่ นี่เป็นกรณีของการติดไวรัส ransomware (ไวรัสเรียกค่าไถ่) ซึ่งจะทำการเข้ารหัสข้อมูลและเรียกร้องเงินเพื่อแลกกับการกู้คืนข้อมูลนั้น.

การเข้าควบคุมและใช้งานอุปกรณ์โดยบุคคลที่ไม่มีสิทธิ์

อุปกรณ์ที่ติดไวรัสอาจถูกควบคุมจากระยะไกล ทำให้เกิดการทำงานที่ไม่ได้ตั้งใจ

- **การส่งอีเมลสแปม** อุปกรณ์ที่ติดไวรัสอาจถูกนำไปใช้โดยไม่รู้ตัวเป็นฐานส่งอีเมลสแปมจำนวนมากไปยังผู้อื่น
- การมีส่วนร่วมในการโจมตีทางไซเบอร์: มีความเสี่ยงที่อุปกรณ์จะถูกนำไปใช้ในกิจกรรมที่ผิดกฎหมาย เช่น การถูกใช้เพื่อโจมตีคอมพิวเตอร์เครื่องอื่น

การสูญเสียความน่าเชื่อถือ

หากอุปกรณ์ที่ใช้ในการทำงานติดไวรัสและเกิดการรั่วไหลของข้อมูลลูกค้า อาจส่งผลให้ความน่าเชื่อถือของบริษัทหรือองค์กรลดลง

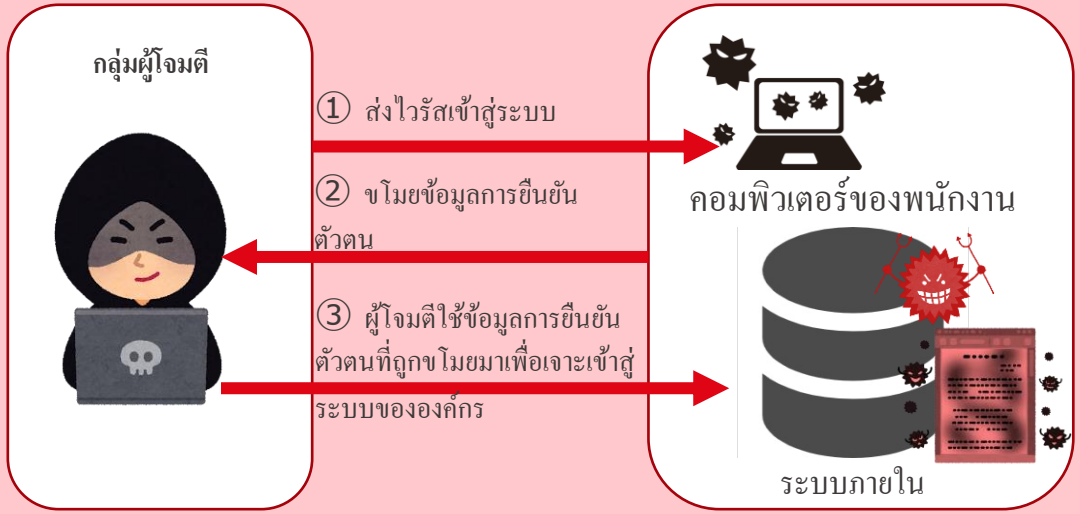
3. บทนำเกี่ยวกับเหตุการณ์ที่เกิดขึ้นในปี 2025

กลุ่มบริษัท YRC ยังไม่เคยได้รับความเสียหายจากการโจมตีทางไซเบอร์ เช่น Ransomware หรือการโจมตีแบบเจาะจงเป้าหมาย (Targeted Attack)อย่างไรก็ตาม มีกรณีที่บริษัทญี่ปุ่นหลายแห่งได้รับผลกระทบจากการโจมตีทางไซเบอร์ ซึ่งจะได้นำเสนอเป็นตัวอย่างในที่นี้

ความเสียหายจากการโจมตีทางไซเบอร์ของบริษัทญี่ปุ่น

*เนื้อหานี้เป็นข้อมูล ณ วันที่หนึ่งในเดือนตุลาคม ปี 2025
*ทางเราจะดำเนินการอัปเดตข้อมูลนี้ทันที หากมีข้อมูลใหม่เพิ่มเติมในอนาคต

ภาพการโจมตี



เมื่อวันที่ 29 กันยายน บริษัทญี่ปุ่นแห่งหนึ่งได้ประกาศว่าเป็นเหยื่อของการโจมตีทางไซเบอร์ต่อมาเมื่อวันที่ 3 ตุลาคม มีการประกาศต่อสาธารณะว่า การโจมตีดังกล่าวเกิดจากไวรัสเรียกค่าไถ่ (Ransomware)

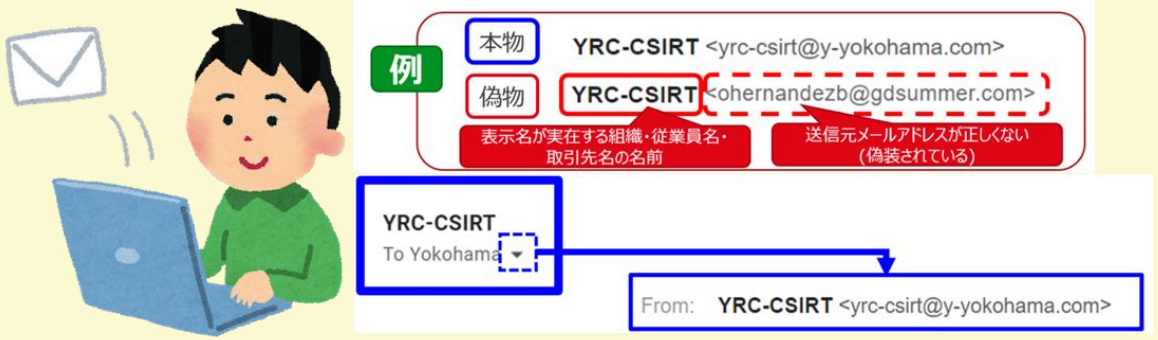
เกิดความขัดข้องของระบบ ทำให้ไม่สามารถดำเนินการสั่งซื้อและจัดส่งสินค้าได้ ส่งผลให้โรงงานภายในประเทศต้องหยุดการดำเนินงานชั่วคราว เกิดภาวะสินค้าขาดสต็อกในบางร้านค้า และต้องเลื่อนการเปิดตัวผลิตภัณฑ์ใหม่ออกไป ต่อมาได้มีการประกาศว่า สาเหตุของความขัดข้องของระบบดังกล่าวเกิดจากการโจมตีทางไซเบอร์ด้วยไวรัสคอมพิวเตอร์ที่เรียกค่าไถ่ หรือ Ransomware ความเสียหายจากการโจมตีครั้งนี้มีความรุนแรง โดยมีการรั่วไหลของข้อมูลคู่ค้าทางธุรกิจและข้อมูลภายในของบริษัทด้วย

การฟื้นฟูระบบหลังการโจมตีทางไซเบอร์ต้องใช้เวลา

การดำเนินมาตรการป้องกันในระดับบุคคลเป็นสิ่งจำเป็น เพื่อป้องกันไม่ให้การโจมตีทางไซเบอร์ส่งผลกระทบหรือทำให้การดำเนินธุรกิจหยุดชะงัก

4. มาตรการป้องกันการติดไวรัสคอมพิวเตอร์

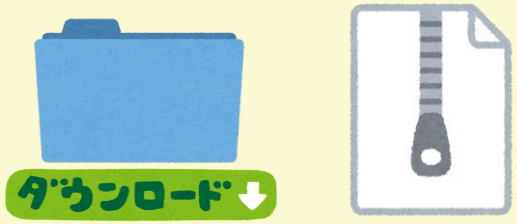
การดำเนินมาตรการในระดับบุคคลสามารถช่วยป้องกันการติดไวรัสได้ขอให้ทุกคนปฏิบัติตามมาตรการต่อไปนี้เพื่อหลีกเลี่ยงความเสี่ยงจากการติดไวรัสหรือมัลแวร์ในระบบ



ตรวจสอบที่อยู่อีเมลและเนื้อหาอีเมลเมื่อได้รับข้อความโปรดตรวจสอบชื่อที่แสดง (Display Name) และที่อยู่อีเมลให้รอบคอบก่อนเปิดอ่านหรือคลิกลิงก์ใด ๆ

ตรวจสอบว่าโปรแกรมป้องกันไวรัสออนไลน์อยู่หรือไม่

งดเข้าชมเว็บไซต์ที่ไม่เกี่ยวข้องกับงาน



ดาวน์โหลดไฟล์แนบด้วยความระมัดระวัง (รวมถึงไฟล์ที่มีมาโครและไฟล์บีบอัด)

4. มาตรการป้องกันการติดไวรัสคอมพิวเตอร์

ภัยคุกคามจากไวรัสมีอยู่เสมอในการใช้งานคอมพิวเตอร์และสมาร์ตโฟนในชีวิตการทำงานประจำวัน
การมีความตระหนักด้านความปลอดภัยของแต่ละบุคคล เป็นส่วนสำคัญที่ช่วยในการปกป้องทั้งองค์กรโดยรวม
เพื่อรักษาสภาพแวดล้อมในการทำงานให้ปลอดภัย ขอให้ทุกคนระมัดระวังในการใช้งานในแต่ละวัน และปฏิบัติตามมาตรการป้องกันไวรัสอย่างเคร่งครัด

■ โปรดปฏิบัติตามแนวทางต่อไปนี้อย่างเคร่งครัดเมื่อใช้งานอินเทอร์เน็ต เพื่อป้องกันความเสี่ยงจากไวรัสและการโจมตีทางไซเบอร์

*โปรดหลีกเลี่ยงการใช้งานอินเทอร์เน็ตโดยไม่จำเป็น หรือเข้าชมเว็บไซต์ที่ไม่เกี่ยวข้องกับงาน

*โปรดหลีกเลี่ยงการเข้าชมเว็บไซต์ที่ไม่น่าเชื่อถือหรือมีความเสี่ยงสูง

*โปรดหลีกเลี่ยงการคลิกที่หน้าต่างป๊อปอัป ทันทีเมื่อปรากฏขึ้นบนหน้าจอ

■ โปรดตระหนักและเฝ้าระวังอีเมลที่มีความน่าสงสัย

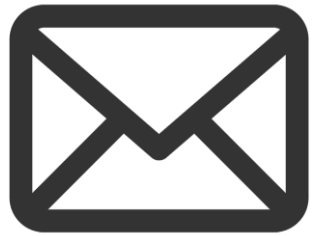
*โปรดหลีกเลี่ยงการเปิดอีเมลที่มีความน่าสงสัย

*โปรดหลีกเลี่ยงการดาวน์โหลดไฟล์แนบ เว้นแต่จะตรวจสอบได้ว่าผู้ส่งเป็นบุคคลหรือแหล่งที่มาที่เชื่อถือได้

*โปรดหลีกเลี่ยงการคลิกลิงก์ในเนื้อหาอีเมล เว้นแต่จะตรวจสอบได้แน่ชัดว่าผู้ส่งเป็นบุคคลหรือแหล่งที่มาที่เชื่อถือได้

*โปรดตรวจสอบที่อยู่อีเมลของผู้ส่งทุกครั้งก่อนเปิดอ่าน คลิกลิงก์ หรือดาวน์โหลดไฟล์แนบ (**example@rnicrosoft.com**)

*โปรดหลีกเลี่ยงการกดปุ่ม **“Enable Editing”** หรือ **“Enable Content”** เมื่อเปิดไฟล์เอกสารของ **Microsoft Office** เว้นแต่จะตรวจสอบได้แน่ชัดว่าไฟล์นั้นมาจากแหล่งที่เชื่อถือได้



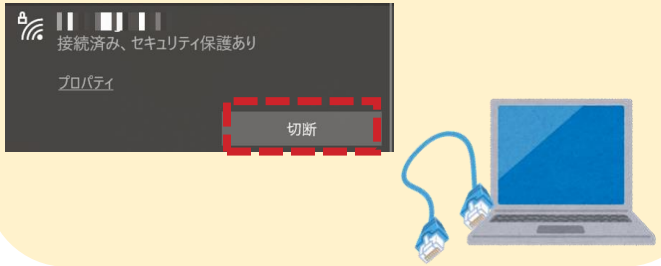
*โปรดอัปเดตโปรแกรมป้องกันไวรัสและไฟล์รูปแบบการตรวจจับไวรัส ให้เป็นเวอร์ชันล่าสุดอยู่เสมอ

5. ในกรณีฉุกเฉิน

หากคุณสงสัยว่ามีการติดไวรัส โปรดปฏิบัติตามขั้นตอนทั้งสามข้อต่อไปนี้โดยเคร่งครัด

Action ยกเลิกการเชื่อมต่อเครือข่าย

- โปรดตัดการเชื่อมต่อคอมพิวเตอร์ออกจากทั้งเครือข่ายแบบสายและไร้สายเมื่อไม่ได้ใช้งาน



Action ให้คงสภาพหน้าจอและเครื่องตามเดิม

- คงหน้าจอที่แสดงอยู่ไว้ อย่าปิด
- ห้ามรีสตาร์ทหรือปิดเครื่องคอมพิวเตอร์

คงหน้าจอที่แสดงอยู่ไว้!

Action การรายงานเหตุ

ติดต่อ YRC-CSIRT และผู้จัดการฝ่ายบริหารข้อมูล (Information Management Manager) และรายงานเหตุการณ์ที่เกิดขึ้นทันที

Information

รายงานถึง

โปรดรายงานเหตุการณ์ด้านความปลอดภัยของข้อมูล (Information Security Incidents) ให้ผู้จัดการฝ่ายบริหารข้อมูลของแผนก/บริษัท และ YRC-CSIRT ทราบทันที

Mail Address **yrc-csirt@y-yokohama.com**

6.สรุป

ครั้งนี้คุณได้เรียนรู้เกี่ยวกับ **การติดไวรัสคอมพิวเตอร์**
โดยความเสียหายที่เกิดจากการติดไวรัสอาจทำให้ **การดำเนินธุรกิจหรือกระบวนการผลิตต้องหยุดชะงัก** และอาจรุนแรงได้
โปรดปฏิบัติตามมาตรการต่อไปนี้เพื่อป้องกันความเสียหาย

✓	**อัปเดตระบบปฏิบัติการ ซอฟต์แวร์ และโปรแกรมสแกนไวรัสให้เป็นเวอร์ชันล่าสุดอยู่เสมอ**
✓	**ห้ามใช้อินเทอร์เน็ตเพื่อวัตถุประสงค์ที่ไม่เกี่ยวข้องกับงาน**
✓	**โปรดหลีกเลี่ยงการเปิดไฟล์แนบจากอีเมลที่มีความน่าสงสัย**
✓	**โปรดแบ่งปันข้อมูลด้านความปลอดภัยภายในองค์กร และตระหนักว่า “ทุกคนสามารถเป็นเป้าหมายของการโจมตีทางไซเบอร์ได้”**


YOKOHAMA