



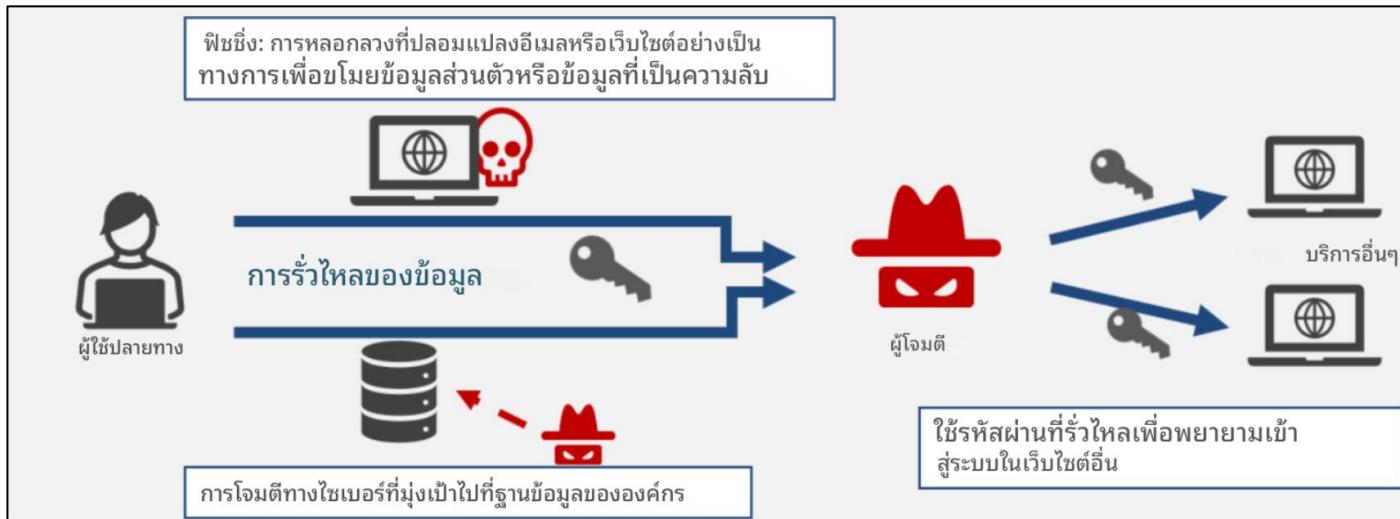
จดหมายข่าวความปลอดภัยของข้อมูล



ฉบับที่ 3 การจัดการรหัสผ่าน

การรั่วไหลของข้อมูลเกิดขึ้นได้อย่างไร

เมื่อคุณใช้งานบริการอินเทอร์เน็ต รหัสบัญชีและรหัสผ่านของคุณอาจรั่วไหลและถูกนำไปใช้ในทางที่ผิดได้ หากคุณใช้รหัสผ่านเดียวกันซ้ำกันในหลาย ๆ บริการ เมื่อบริการใดบริการหนึ่งถูกโจมตี ผู้บุกรุกอาจเข้าถึงบัญชีอื่น ๆ ของคุณได้โดยไม่ได้รับอนุญาตเช่นกัน



ภาพประกอบ: วิธีที่ข้อมูลรั่วไหลเกิดขึ้นได้

นอกจากนี้ รหัสผ่านที่อ่อนแอก็ยังมีความเสี่ยงต่อการถูกโจมตีแบบ brute force (คือการที่ผู้โจมตีพยายามสุมรวมรหัสผ่านทุกความเป็นไปได้จนกว่าจะสำเร็จ). การรั่วไหลเช่นนี้ไม่เพียงแต่ส่งผลกระทบต่อบุคคลเท่านั้น แต่ยังอาจสร้างความเสียหายต่อชีวิตระบบทั่วโลก ประจำการของบริษัทด้วย เพื่อป้องกันความเสี่ยงเหล่านี้ ควรหลีกเลี่ยงการใช้รหัสผ่านที่ง่ายและสามารถคาดเดาได้ และจัดการรหัสผ่านอย่างเหมาะสม

การสร้างรหัสผ่านที่ปลอดภัย

เพื่อป้องกันการนำรหัสผ่านไปใช้ในทางที่ผิด ควรปฏิบัติตามแนวทางเหล่านี้เมื่อกำหนดรหัสผ่าน:

รหัสผ่านที่คาดเดาได้ยาก

- รหัสผ่านที่มีข้อมูลส่วนบุคคล เช่น ชื่อ วันเกิด หรือ หมายเลขโทรศัพท์
- สตริงอักขระแบบง่าย (เช่น 12345, 11111, abcde)
- คำท้าไปหรือลิ้งค์ๆ (เช่น รหัสผ่าน iloveyou)
- สตริงอักขระตามรูปแบบแป้นพิมพ์ (เช่น qwerty, 1qaz)
- มีความยาวสั้นเกินไป
- ประเภทอักขระที่จำกัด (เช่น เฉพาะตัวอักษร เฉพาะตัวเลข)



เงื่อนไขสำหรับรหัสผ่านที่ปลอดภัย

- ตั้งรหัสผ่านให้ยาวขึ้น (แนะนำ 12 ตัวอักษรขึ้นไป)
- รวมอักขระประเภทต่างๆ เช่น ตัวพิมพ์ใหญ่ ตัวพิมพ์เล็ก ตัวเลข และสัญลักษณ์
- หลีกเลี่ยงการใช้ชื่อ วันเกิด คำท้าไป ตัวเลข หรือ ID การเข้าสู่ระบบเป็นรหัสผ่าน
- อย่าใช้รหัสผ่านซ้ำในบริการที่แตกต่างกัน



เหตุใดจึงแนะนำให้ใช้รหัสผ่านที่ยาบี้

ในอดีต แนะนำให้ใช้ตัวอักษรพิมพ์ใหญ่ ตัวอักษรพิมพ์เล็ก ตัวเลข และสัญลักษณ์ในรหัสผ่าน อย่างไรก็ตาม วิธีการ เช่น "การแทนที่ตัวอักษรด้วยตัวเลขหรือสัญลักษณ์" ไม่เพียงพออีก ต่อไป ผู้โจมตีคาดการณ์เทคนิคดังกล่าวและบันทึกการแทนที่ เหล่านี้ไว้ในพจนานุกรม ดังนั้น การแทนที่แบบง่าย ๆ เพียงอย่างเดียวจึงไม่เพียงพอ ปัจจุบัน การใช้รหัสผ่านที่ยาบี้นั้นมีอัตราหายใจที่สูงกว่า เมื่อเทียบกับรหัสผ่านสันسورฟ์ แต่ข้อดีของการใช้รหัสผ่านที่ยาบี้คือโดยมีเพียงตัวอักษรและตัวเลขจะปลอดภัยกว่า เพราะต้องใช้ต้นทุนการคำนวณที่สูงกว่ามากในการแครก

รหัสผ่าน → รหัสผ่าน
รหัสผ่าน → Pa\$\$%
ผู้ดูแลระบบ → ผู้ดูแลระบบ



จัดการรหัสผ่านอย่างปลอดภัย

เพื่อช่วยให้คุณสามารถจำรหัสผ่านได้ ขอแนะนำแนวทางการจัดการรหัสผ่านอย่างปลอดภัยดังนี้



เขียนลงบนกระดาษและเก็บไว้ในที่ปลอดภัย



วิธีหนึ่งคือเขียนรหัสผ่านของคุณลงบนกระดาษและเก็บไว้ในที่ที่ไม่สามารถมองเห็นได้ง่าย อย่างไรก็ตาม หากทั้ง ID และรหัสผ่านของคุณเขียนไว้ในกระดาษเดียวกัน และถูกหักโหมหรือสูญหาย ก็อาจถูกนำไปใช้ในการที่ผิดได้ง่าย ควรเขียน ID และรหัสผ่านของคุณลงในกระดาษแยกกันและเก็บไว้แยกกัน



เก็บไว้ในไฟล์อิเล็กทรอนิกส์ที่มีการป้องกันด้วยรหัสผ่าน



หากคุณเก็บรหัสผ่านไว้ในคอมพิวเตอร์ ควรป้องกันไฟล์ด้วยรหัสผ่านเสมอ เช่นเดียวกับบันทึกย่อในกระดาษ สิ่งสำคัญคืออย่าบันทึกทั้ง ID และรหัสผ่านไว้ในไฟล์เดียวกัน



ใช้เครื่องมือจัดการรหัสผ่าน

ในเครื่องมือจัดการรหัสผ่านหลายตัว เมื่อคุณลงทะเบียน ID บัญชีและรหัสผ่านสำหรับบริการอินเทอร์เน็ตแต่ละรายการ เครื่องมือจะดึงข้อมูลและป้อนข้อมูลดังกล่าวโดยอัตโนมัติ เมื่อจำเป็น

เมื่อใช้เครื่องมือดังกล่าว โปรดแน่ใจว่าเลือกบริการที่เชื่อถือได้

นอกจากนี้ โปรดระมัดระวังสถานการณ์ดังไปนี้เพื่อป้องกันไม่ให้รหัสผ่านของคุณถูกเปิดเผย

เลือกช่องกันไม่ให้ผู้อื่นเห็นรหัสผ่าน

หากคุณเขียนรหัสผ่านของคุณลงบนกระดาษและติดไว้ใกล้กับคอมพิวเตอร์ หรือป้อนรหัสผ่านในที่ที่ผู้อื่นมองเห็นได้ง่าย อาจมีความเสี่ยงที่รหัสผ่านของคุณจะถูกเปิดเผย หลีกเลี่ยงการกรอกรหัสผ่านในที่สาธารณะหรือระหว่างการเดินทางให้มากที่สุด



เลือกช่องเลี่ยงการแชร์รหัสผ่าน

เมื่อใช้บริการคลาวด์เพื่อการทำงาน บางครั้งคุณอาจจำเป็นต้องแชร์ ID และรหัสผ่านภายในองค์กรของคุณ หากไม่สามารถหลีกเลี่ยงการแบ่งปันรหัสผ่านได้ ให้ตั้งรหัสผ่านที่ไม่ซ้ำใครและไม่นำไปใช้ซ้ำที่อื่น และแบ่งปันวิธีการที่ปลอดภัยเท่านั้น



ข้อแนะนำเพิ่มเติม

นอกเหนือจากการใช้รหัสผ่านที่รัดกุมแล้ว โปรดพิจารณาการตั้งค่าต่อไปนี้เพื่อเพิ่มความปลอดภัยให้กับบัญชีของคุณ

การใช้การยืนยันตัวตนแบบสองปัจจัย (2FA)

วิธีที่นิยมใช้กันคือการป้อนรหัสผ่านครั้งเดียว (OTP) ที่ส่งผ่าน SMS ไปยังหมายเลขโทรศัพท์ของคุณหรือผ่านการแจ้งเตือนในแอปพลิเคชัน 2FA ช่วยให้การเข้าสู่ระบบทำได้มากกว่าแค่การกรอก ID และรหัสผ่าน ซึ่งทำให้เป็นมาตรฐานการรักษาความปลอดภัยที่แข็งแกร่งขึ้น ปัจจุบันหลายบริการได้นำฟีเจอร์นี้มาใช้แล้ว



การใช้ประวัติการเข้าสู่ระบบและฟังก์ชันการแจ้งเตือนการเข้าสู่ระบบ

บริการบางอย่างอนุญาตให้คุณตรวจสอบความพยายามเข้าสู่ระบบในอดีต รวมถึงวันที่เวลา และแหล่งที่มาของ การเข้าถึง นอกเหนือจากนี้ บริการบางอย่างจะแจ้งให้คุณทราบหากมีการเข้าสู่ระบบจากตำแหน่งหรืออุปกรณ์ที่ผิดปกติ ใช้ประโยชน์จากฟังก์ชันเหล่านี้เพื่อบังคับการเข้าถึงโดยไม่ได้รับอนุญาตล่วงหน้า หากคุณสังเกตเห็นความพยายามในการเข้าถึงที่น่าสงสัย ให้เปลี่ยนรหัสผ่านของคุณทันที ตรวจสอบว่ามีการใช้รหัสผ่านเดียวกันซ้ำกับบริการอื่นหรือไม่ และหากเป็นเช่นนั้น ให้เปลี่ยนรหัสผ่านเหล่านั้นด้วย



วันที่และเวลาเข้า
ระบบ แหล่งการเข้าถึง
การเข้าถึงที่
น่าสงสัย

【 ข้อมูลติดต่อสอบถาม】

ฝ่ายเลขานุการคณะกรรมการความปลอดภัยสารสนเทศ (กองเทคโนโลยีสารสนเทศ แผนกระบบสารสนเทศ สำนักที่ 2)

อีเมล securitylearning@fanuc.co.jp



Vol3 Password Management

How Information Leakage Happens

When using internet services, your account IDs and passwords may be leaked and misused. If you reuse the same password across multiple services, once one of them is compromised, **attackers may gain unauthorized access to your other accounts as well.**

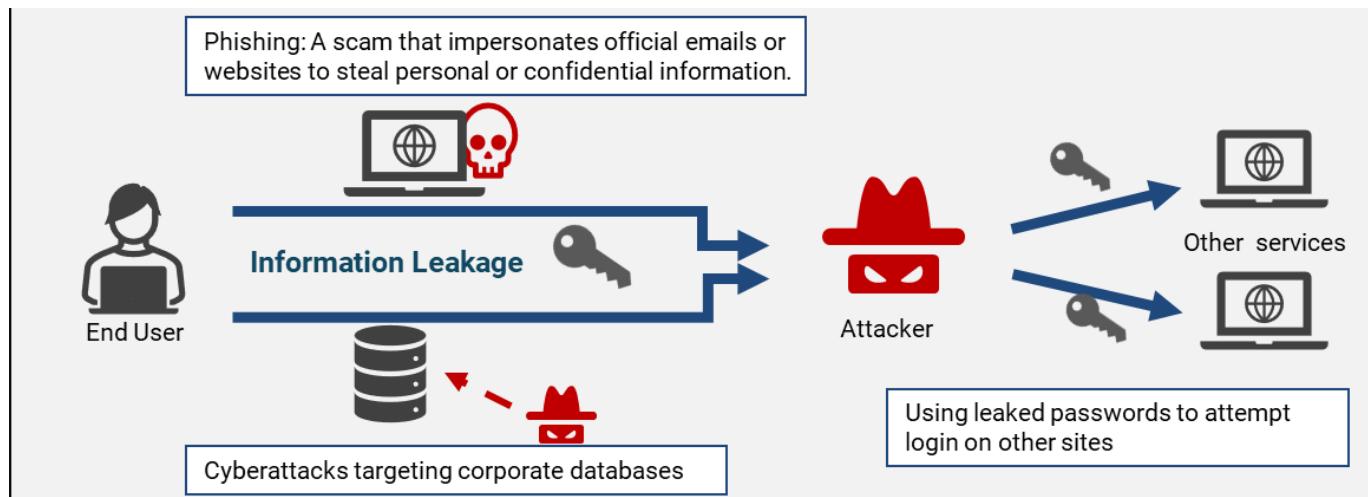


Figure: How Information Leakage Happens

In addition, weak passwords are vulnerable to **brute force attacks** (where attackers try all possible combinations until they succeed).

Such leaks not only harm individuals **but may also damage the company's reputation and business performance**. To reduce these risks, avoid simple and predictable passwords, and manage them appropriately.

Creating a Secure Password

To prevent misuse, follow these guidelines when setting passwords:

Easily Guessable Passwords

- Passwords containing personal information such as name, date of birth, or phone number
- Simple character strings (e.g., 12345, 11111, abcde)
- Common words or simple phrases (e.g., password, iloveyou)
- Character strings based on keyboard patterns (e.g., qwerty, 1qaz)
- Too short in length
- Limited character types (e.g., only letters, only numbers)



The most commonly used passwords worldwide (2023), according to NordPass

Conditions for a Secure Password

- Make passwords longer (**12 characters or more recommended**)
- Combine various character types: uppercase letters, lowercase letters, numbers, and symbols
- Avoid using names, birthdays, common words, numbers, or login IDs as passwords
- **Do not reuse passwords across different services**



Why Longer Passwords Are Recommended

In the past, it was recommended to include uppercase letters, lowercase letters, numbers, and symbols in passwords. However, methods such as "replacing letters with numbers or symbols" are no longer sufficient. Attackers anticipate such techniques and register these replacements in their dictionaries. Therefore, **simple substitutions alone are not enough**. Today, it is considered more secure to **use longer passwords with more characters**. Compared to short but complex passwords, using a longer password with only letters and numbers is safer because it **requires significantly more computational cost to crack**.

**Password → P@ssword
Password → Pa\$\$word
Admin → Adm1n**



How to Manage Passwords Safely

To help you remember your passwords, here are some secure management practices.



Write it down on paper and store it in a safe place

One way is to write down your password on paper and keep it in a place where it cannot be easily seen.



However, if both your ID and password are written on the same paper and it is stolen or lost, it may be easily misused.

Always write your ID and password on separate papers and store them separately.



Store it in a password-protected electronic file

If you store passwords on your computer, always protect the file with a password. As with paper notes, it is important **not to record both your ID and password in the same file**.



Use a password manager

In many password management tools, once you register your account ID and password for each internet service, the tool can automatically retrieve and enter them when needed.



When using such tools, be sure to choose a trusted service.

In addition, be mindful of the following situations to prevent your passwords from being exposed.



Prevent Passwords from Being Seen by Others

If you write down your password on paper and stick it near your computer, or enter it in a place where others can easily see, **there is a risk that your password may be exposed**.



Avoid entering passwords in public places or while in transit as much as possible.



Avoid Sharing Passwords

When using cloud services for work, you may sometimes need to share IDs and passwords within your organization.



If password sharing is unavoidable, **set a unique password that is not reused elsewhere, and share it only through secure methods**.

Additional Recommendations

Beyond using strong passwords, consider the following settings to further protect your accounts.

Use of Two-Factor Authentication (2FA)

A common method is to enter a one-time password (OTP) sent via SMS to your phone number or through an app notification.

With 2FA, logging in requires more than just entering your ID and password, making it a stronger security measure. Many services have already adopted this feature.



Use of Login History and Login Alert Functions

Some services allow you to check past login attempts, including date, time, and source of access.

In addition, some services notify you if a login occurs from an unusual location or device.

Leverage these functions to prevent unauthorized access in advance.

If you notice any suspicious access attempts, **change your password immediately.**

Also, check if the same password is being reused on other services, and **if so, make sure to change those as well.**



[Inquiry]

Information Security Committee Secretariat
(IT Division information System Department Section 2)
securitylearning@fanuc.co.jp
