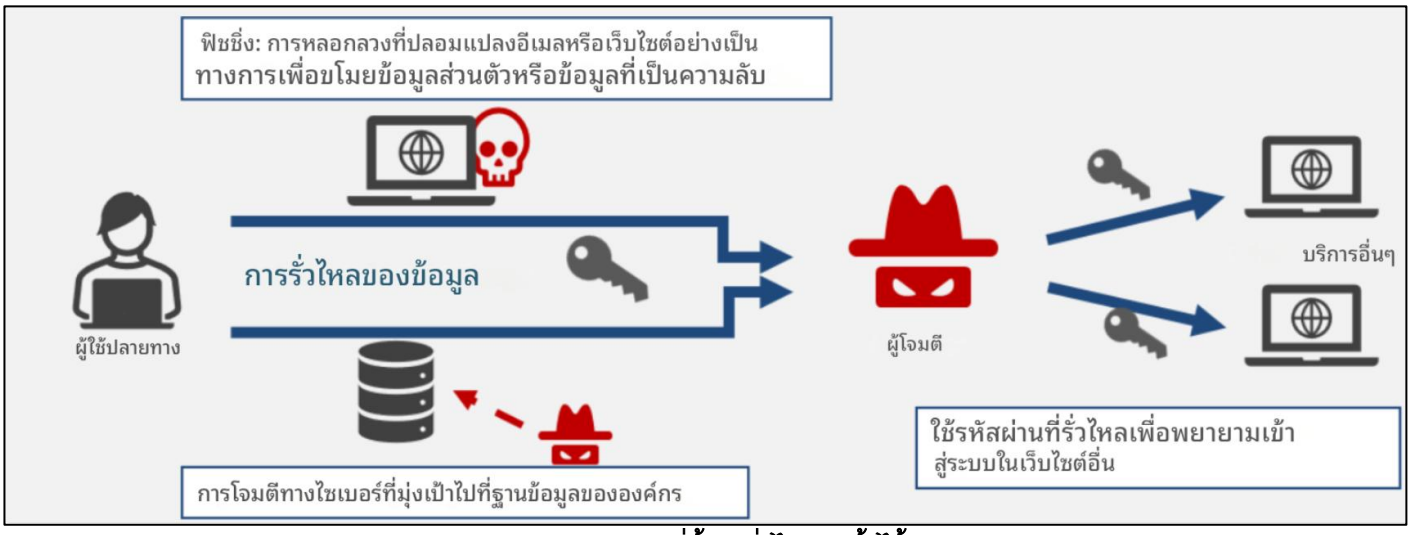
จดหมายข่าวความปลอดภัยของข้อมูล

ฉบับที่ 3 การจัดการรหัสผ่าน

การรั่วไหลของข้อมูลเกิดขึ้นได้อย่างไร

เมื่อคุณใช้งานบริการอินเทอร์เน็ต รหัสบัญชีและรหัสผ่านของคุณอาจรั่วไหลและถูกนำไปใช้ในทางที่ผิดได้ หากคุณใช้รหัสผ่านเดียวกันซ้ำกันในหลาย ๆ บริการ เมื่อบริการใดบริการหนึ่งถูกโจมตี **ผู้บุกรุกก็อาจเข้าถึงบัญชีอื่น ๆ ของคุณได้โดยไม่ได้รับอนุญาตเช่นกัน**



ภาพประกอบ: วิธีที่ข้อมูลรั่วไหลเกิดขึ้นได้

นอกจากนี้ รหัสผ่านที่อ่อนแอยังมีความเสี่ยงต่อการถูกโจมตีแบบ brute force **(คือการที่ผู้โจมตีพยายามสุ่มรหัสผ่านทุกความเป็นไปได้จนกว่าจะสำเร็จ)**. การรั่วไหลเช่นนี้ไม่เพียงแต่ส่งผลกระทบต่อบุคคลเท่านั้น **แต่ยังอาจสร้างความเสียหายต่อชื่อเสียงและผลประกอบการของบริษัทด้วย** เพื่อป้องกันความเสี่ยงเหล่านี้ ควรหลีกเลี่ยงการใช้รหัสผ่านที่ง่ายและสามารถคาดเดาได้ และจัดการรหัสผ่านอย่างเหมาะสม

การสร้างรหัสผ่านที่ปลอดภัย

เพื่อป้องกันการนำรหัสผ่านไปใช้ในทางที่ผิด ควรปฏิบัติตามแนวทางเหล่านี้เมื่อกำหนดรหัสผ่าน:

รหัสผ่านที่คาดเดาได้ง่าย

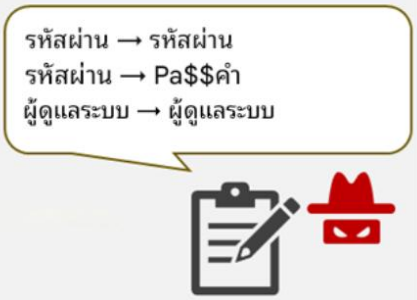
- รหัสผ่านที่มีข้อมูลส่วนบุคคล เช่น ชื่อ วันเกิด หรือหมายเลขโทรศัพท์
- สตริงอักขระแบบง่าย (เช่น 12345, 11111, abcde)
- คำทั่วไปหรือวลีง่ายๆ (เช่น รหัสผ่าน iloveyou)
- สตริงอักขระตามรูปแบบแป้นพิมพ์ (เช่น qwerty, 1qaz)
- มีความยาวสั้นเกินไป
- ประเภทอักขระที่จำกัด (เช่น เฉพาะตัวอักษร เฉพาะตัวเลข)

เงื่อนไขสำหรับรหัสผ่านที่ปลอดภัย

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

เหตุใดจึงแนะนำให้ใช้รหัสผ่านที่ยาวขึ้น

ในอดีต แนะนำให้ใส่ตัวอักษรพิมพ์ใหญ่ ตัวอักษรพิมพ์เล็ก ตัวเลข และสัญลักษณ์ในรหัสผ่าน อย่างไรก็ตาม วิธีการเช่น "การแทนที่ตัวอักษรด้วยตัวเลขหรือสัญลักษณ์" ไม่เพียงพออีกต่อไป ผู้โจมตีคาดการณ์เทคนิคดังกล่าวและบันทึกการแทนที่เหล่านี้ไว้ในพจนานุกรม ดังนั้น การแทนที่แบบง่าย ๆ เพียงอย่างเดียวจึงไม่เพียงพอ ปัจจุบัน การใช้รหัสผ่านที่ยาวขึ้นและมีอักขระมากขึ้นถือว่าปลอดภัยกว่าเมื่อเทียบกับรหัสผ่านสั้น ๆ แต่ซับซ้อน การใช้รหัสผ่านที่ยาวกว่าโดยมีเพียงตัวอักษรและตัวเลขจะปลอดภัยกว่าเพราะต้องใช้ต้นทุนการคำนวณที่สูงกว่ามากในการแคร็ก



จัดการรหัสผ่านอย่างปลอดภัย

เพื่อช่วยให้คุณสามารถจดจำรหัสผ่านได้ ขอแนะนำแนวทางการจัดการรหัสผ่านอย่างปลอดภัยดังนี้

เขียนลงบนกระดาษและเก็บไว้ในที่ปลอดภัย

วิธีหนึ่งคือเขียนรหัสผ่านของคุณลงบนกระดาษและเก็บไว้ในที่ที่ไม่สามารถมองเห็นได้ง่าย
อย่างไรก็ตาม หากทั้ง ID และรหัสผ่านของคุณเขียนไว้ในกระดาษเดียวกัน และถูกขโมยหรือสูญหาย ก็อาจถูกนำไปใช้ในทางที่ผิดได้ง่าย
ควรเขียน ID และรหัสผ่านของคุณลงในกระดาษแยกกันและเก็บไว้แยกกัน

เก็บไว้ในไฟล์อิเล็กทรอนิกส์ที่มีการป้องกันด้วยรหัสผ่าน

หากคุณเก็บรหัสผ่านไว้ในคอมพิวเตอร์ ควรป้องกันไฟล์ด้วยรหัสผ่านเสมอ เช่นเดียวกับบันทึกย่อบนกระดาษ สิ่งสำคัญคืออย่าบันทึกทั้ง ID และรหัสผ่านไว้ในไฟล์เดียวกัน

ใช้เครื่องมือจัดการรหัสผ่าน

ในเครื่องมือจัดการรหัสผ่านหลายๆ ตัว เมื่อคุณลงทะเบียน ID บัญชีและรหัสผ่านสำหรับบริการอินเทอร์เน็ตแต่ละรายการ เครื่องมือจะดึงข้อมูลและป้อนข้อมูลดังกล่าวโดยอัตโนมัติเมื่อจำเป็น
เมื่อใช้เครื่องมือดังกล่าว โปรดแน่ใจว่าเลือกบริการที่เชื่อถือได้

นอกจากนี้ โปรดระมัดระวังสถานการณ์ต่อไปนี้เพื่อป้องกันไม่ให้รหัสผ่านของคุณถูกเปิดเผย

เอ็กซ์ ป้องกันไม่ให้ผู้อื่นเห็นรหัสผ่าน

หากคุณเขียนรหัสผ่านของคุณลงบนกระดาษและติดไว้ใกล้กับคอมพิวเตอร์ หรือป้อนรหัสผ่านในที่ที่ผู้อื่นมองเห็นได้ง่าย อาจมีความเสี่ยงที่รหัสผ่านของคุณจะถูกเปิดเผย
หลีกเลี่ยงการกรอกรหัสผ่านในที่สาธารณะหรือระหว่างการเดินทางให้มากที่สุด

เอ็กซ์ หลีกเลี่ยงการแชร์รหัสผ่าน

เมื่อใช้บริการคลาวด์เพื่อการทำงาน บางครั้งคุณอาจจำเป็นต้องแชร์ ID และรหัสผ่านภายในองค์กรของคุณ
หากไม่สามารถหลีกเลี่ยงการแบ่งปันรหัสผ่านได้ ให้ตั้งรหัสผ่านที่ไม่ซ้ำใครและไม่นำไปใช้ซ้ำที่อื่น และแบ่งปันผ่านวิธีการที่ปลอดภัยเท่านั้น

ข้อแนะนำเพิ่มเติม

นอกเหนือจากการใช้รหัสผ่านที่รัดกุมแล้ว โปรดพิจารณาการตั้งค่าต่อไปนี้เพื่อเพิ่มความปลอดภัยให้กับบัญชีของคุณ

การใช้การยืนยันตัวตนแบบสองปัจจัย (2FA)

วิธีที่นิยมใช้กันคือการป้อนรหัสผ่านครั้งเดียว (OTP) ที่ส่ง
ผ่าน SMS ไปยังหมายเลขโทรศัพท์ของคุณหรือผ่านการแจ้งเตือนใน
แอปพลิเคชัน 2FA ช่วยให้การเข้าสู่ระบบทำได้มากกว่าแค่การกรอก ID และรหัส
ผ่าน ซึ่งทำให้เป็นมาตรการรักษาความปลอดภัยที่แข็งแกร่งขึ้น ปัจจุบันหลาย
บริการได้นำฟีเจอร์นี้มาใช้แล้ว

การใช้ประวัติการเข้าสู่ระบบและฟังก์ชั่นการแจ้งเตือนการเข้าสู่ระบบ

บริการบางอย่างอนุญาตให้คุณตรวจสอบความพยายามเข้าสู่ระบบในอดีต รวมถึงวันที่
เวลา และแหล่งที่มาของการเข้าถึง
นอกจากนี้ บริการบางอย่างจะแจ้งให้คุณทราบหากมีการเข้าสู่ระบบจากตำแหน่งหรือ
อุปกรณ์ที่ผิดปกติ
ใช้ประโยชน์จากฟังก์ชั่นเหล่านี้เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตล่วงหน้า
หากคุณสังเกตเห็นความพยายามในการเข้าถึงที่น่าสงสัย ให้เปลี่ยนรหัสผ่าน
ของคุณทันที
ตรวจสอบว่ามีการใช้รหัสผ่านเดียวกันซ้ำกับบริการอื่นหรือไม่ และหากเป็น
เช่นนั้น ให้เปลี่ยนรหัสผ่านเหล่านั้นด้วย

【ข้อมูลติดต่อสอบถาม】

ฝ่ายเลขานุการคณะกรรมการความปลอดภัยสารสนเทศ (กองเทคโนโลยีสารสนเทศ แผนกระบบสารสนเทศ ส่วนที่ 2)
อีเมล์ securitylearning@fanuc.co.jp

Information Security Newsletter

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.**

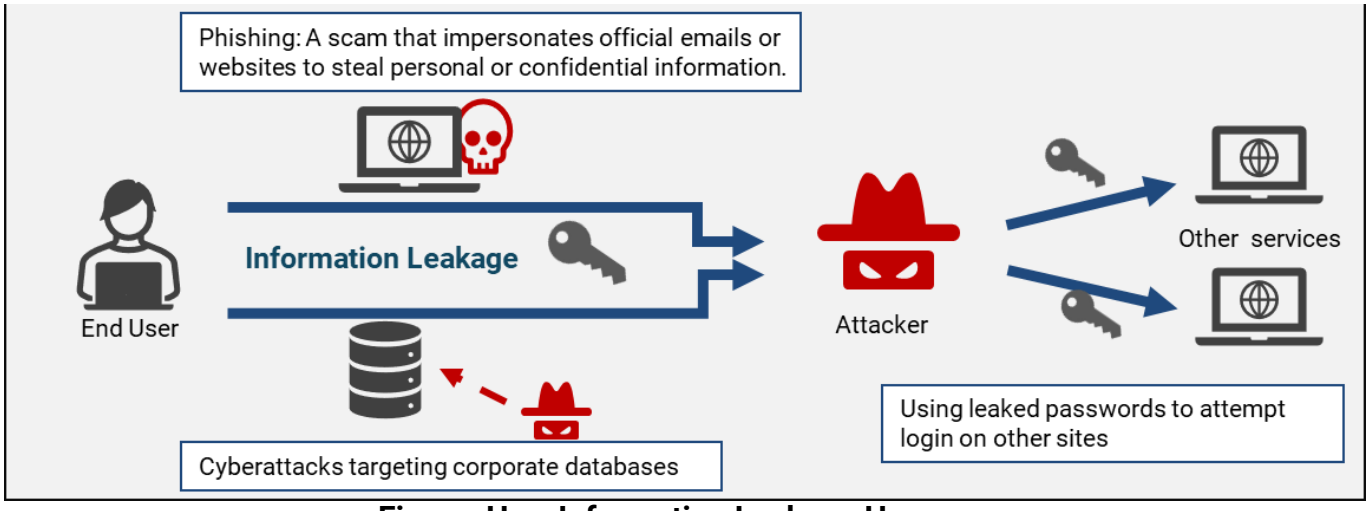


Figure: How Information Leakage Happens

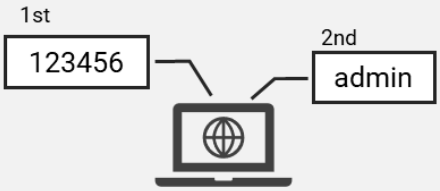
In addition, weak passwords are vulnerable to **brute force attacks (where attackers try all possible combinations until they succeed).**
Such leaks not only harm individuals **but may also damage the company's reputation and business performance**. To reduce these risks, avoid simple and predictable 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

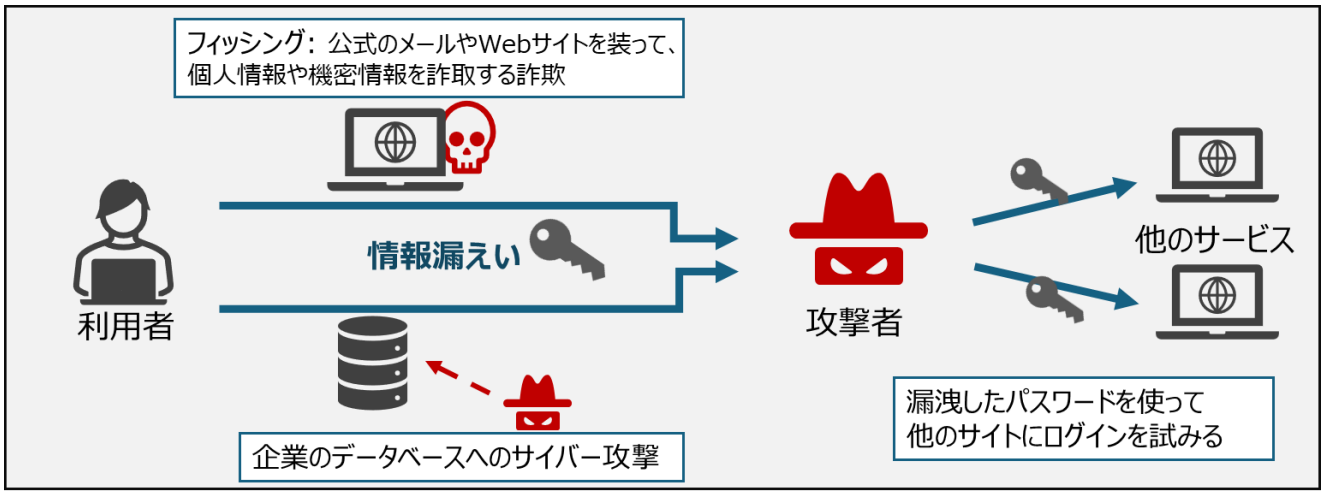
情報セキュリティ定期注意喚起

第３回 パスワード管理

情報漏えいが起こるしくみ

インターネット上のサービスを利用する際に入力するアカウント情報（ID やパスワードなど）が漏えいし、悪用されるといった事件が多く発生しています。

特に、同一のパスワードを複数のサービスで使い回していると、どれか 1 つのサービスから情報が漏えいした際に、**他のサービスにも不正にアクセスされ、被害に遭う恐れがあります。**



情報漏えいのサイクル

また、強度の弱いパスワードを使っている場合は、**ブルートフォース攻撃（総当たりでパスワードを試行する攻撃）**の被害にあう場合もあります。

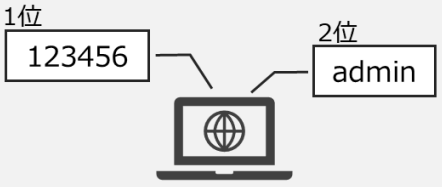
情報漏えいは個人の被害だけでなく、場合によっては**会社の信用が低下し、収益に影響を及ぼす可能性もあります。**このようなリスクを減らすために、単純で推測されやすいパスワード設定を避け、パスワードは適切に管理してください。

安全なパスワードの設定

悪用を防ぐために、安全なパスワードの設定方法をご紹介します。

推測されやすいパスワード

- 氏名や生年月日、電話番号などの個人情報を含んだもの
- 単純な文字列（ex. 12345、11111、abcde）
- 単語や簡単な文章（ex. password、iloveyou）
- キーボードの配列に沿った文字列 (ex. qwerty、1qaz)
- 文字数が少ない
- ローマ字だけ、数字だけなど文字の種類が少ない



世界で最も使われているパスワード (2023)
NordPass社の調査による

安全なパスワードの条件

- パスワードの文字列は長めにする（**12文字以上**を推奨）
- 大文字、記号、数字など様々な文字の種類を組み合わせる
- 氏名や生年月日、推測されやすい単語、数字、ログインIDと同じパスワードにすることは避ける
- **他のサービスで利用しているパスワードは使いまわさない**

より長いパスワードが望ましい理由

これまでは、英大文字・小文字、数字に加えて記号を混ぜ込むことが推奨されてきました。
しかし、「アルファベットを数字や記号に置き換える」等の方法では、攻撃者はこうした対策を見越して、置き換えたものを辞書に登録する恐れがあるため、**簡単な置き換えだけでは不十分**と言われています。
そのため、現在では、**多くの文字数を使うことが望ましい**と考えられています。短くて複雑なパスワードを使うよりも、英数字のみでも長いパスワードを使うほうが、**解読の時間がかかる**ためです。

パスワードの適切な管理

パスワードを忘れないために、安全なパスワードの管理方法をご紹介します。

紙にメモして、安全な場所で保管する

紙に書いて人目につかない場所で保管する方法です。
ただし、1枚の紙にIDとパスワードの両方をメモすると、万が一盗み見られたり紛失したときに容易に不正アクセスされてしまう可能性があります。
IDとパスワードは別の紙にメモして、別々に保管するようにしましょう。

パスワード付きの電子ファイルで保管する

パソコンの中で保管したい場合は、必ずファイルにパスワードをかけて保管しましょう。
また、これも紙の時と同様にIDとパスワードを同じファイル内にメモしないようにすることが重要です。

また、パスワードの漏えいを防ぐために、以下のような状況にも注意してください。

パスワードが覗き見られないようにする

パソコンの近くにパスワードをメモした紙を貼ったり、人目につきやすい場所でパスワードを入力すると、**パスワードが覗き見られてしまう可能性があります。**
公共の場所や移動中にパスワードを入力することは極力避けるようにしてください。

パスワードの共有を避ける

業務でクラウドなどを利用している場合は特に、IDとパスワードを社内で共有することがあるかもしれません。
IDとパスワードの共有が必要な場合は、**使いまわしていないユニークなパスワード設定し、安全な方法で共有するようにしてください。**

不正アクセスを防ぐために

強固なパスワードの設定以外にも、以下のような設定を行っておくとさらにアカウントのセキュリティが強化されます。

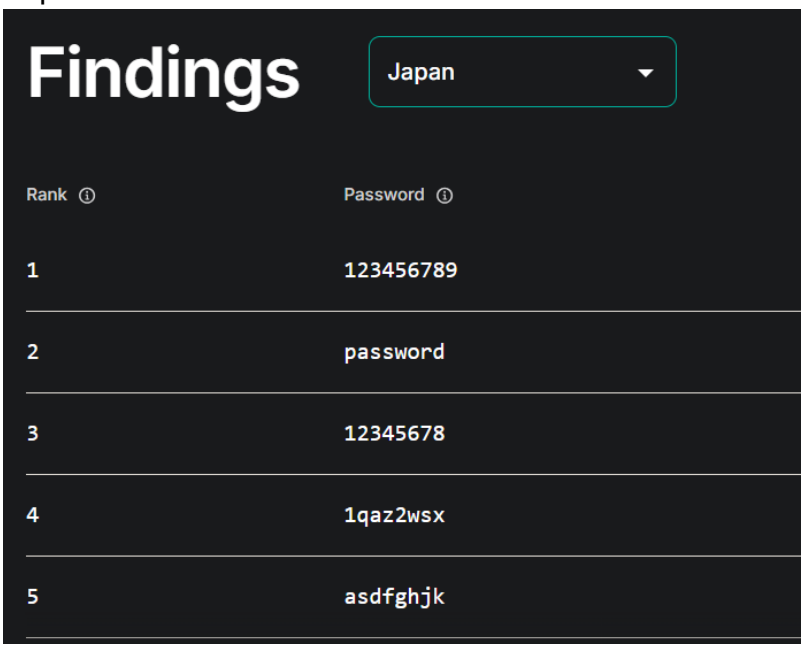
二段階認証の活用

代表的なものが、電話番号へのショートメッセージ（SMS）や、アプリに通知されるワンタイムパスワードを入力して**二段階認証**を行う方法です。IDとパスワードを入力しただけではログインできないため、より強固なセキュリティ対策として多くのサービスで導入されています。

ログイン履歴機能、ログインアラート機能の活用

サービスによっては、過去にログインが試みられた日時やアクセス元などを確認することができます。また、通常とは異なる場所やデバイスからログインされた場合に通知を受け取れるサービスもあります。**こうした機能を活用して不正アクセスを未然に防ぎましょう。**
もしも不正なアクセスが試みられた場合は、**早急にパスワードを変更してください**。また、ほかのサービスで同じパスワードを使いまわしていないか確認し、**もしも同じパスワードを使用している場合はそちらも変更するようにしましょう。**

【参考情報】
NordPass 社が公開した、2024 年において日本でよく使われているパスワードランキングを公表しました。
Top5 は以下の通りです。



引用：Top 200 Most Common Passwords | NordPass

【お問い合わせ先】
IT 本部　情報システム部　二課
情報セキュリティ委員会事務局
事務局へのお問合せ
