2. パスワード漏洩に関する考察

要約

- 多くの日本人が安全なパスワードを利用していない実態が浮き彫りに。
- インターネットサービスの利活用増加により、ますますサイバーセキュリティリスクが増加。
- パスワード要件の見直しに対応するため、ID 管理ソリューション、認証管理ソリューションの導入を推奨。

国内の状況

企業からの大規模なアカウント情報の漏洩事案(※1)や個人を狙ったフィッシング攻撃によるパスワード漏洩事案が後を絶ちません。「情報セキュリティ 10 大脅威 2024 [個人]」(※2)では「インターネット上のサービスからの個人情報の窃取」が 5 年連続で 1 位になっており、窃取した情報を用いることにより、アカウントの乗っ取りやクレデンシャルスタッフィング(攻撃者が、漏洩したパスワードを使って他のサービスにもログインを試行すること)等の犯罪に利用される可能性があります。

まずパスワードに関する 2 本の調査レポートを確認してみます。

『パスワードの利用実態調査 2023』(※3)では、調査対象ユーザーの 8 割以上がパスワードを使い回し、約 2 割が不正アクセスや情報流出の被害に遭っている実態が報告されました。パスワードを使い回す理由としては、「異なるパスワードを設定すると忘れてしまう」「異なるパスワードを考えるのが面倒」という声が多くあげられています。

また『日本人のパスワードランキング 2024 最新版』(※4)では、2024 年 1 月から 8 月にかけて発見された 276 件の情報漏洩事件を基に、日本人が利用するパスワードを分析した結果がまとめられていますが、上位が「123456」「password」「123123」となっており、パスワード長も短く、かつ容易に推測できるものでした。

次にパスワードに関する安全な設定・管理については、総務省が運用している「国民のためのサイバーセキュリティサイト」(※5)にて、以下の 3 点で説明されています。

- 安全なパスワードの設定

  安全なパスワードとは、他人に推測されにくく、ツールなどの機械的な処理(辞書に掲載されているような単語の組み合わせ)で割り出しにくいものをいいます。
- パスワードの保管方法

  せっかく安全なパスワードを設定しても、パスワードが他人に漏れてしまえば意味がないため、同僚等の第三者に教えずに秘密にすること、電子メールでやりとりしないこと、パスワードのメモをディスプレイなど他人の目に触れる場所に貼ったりしないことに留意しましょう。
- パスワードを複数のサービスで使い回さない(定期的な変更は不要)

(*1) 不正アクセスによる、情報漏えいに関するお知らせとお詫び | LINE ヤフー株式会社

(*2) 情報セキュリティ 10 大脅威 2024 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構

(*3) パスワードの利用実態調査 2023| トレンドマイクロ | トレンドマイクロ (JP)

(*4) 「日本人のパスワードランキング 2024 最新版」公開 | ニュース | 株式会社ソリトンシステムズ

(*5) 安全なパスワードの設定・管理 | 国民のためのサイバーセキュリティサイト

パスワードの歴史

コンピュータシステムの黎明期は、ATM の暗証番号のように、比較的短くて覚えやすいパスワードのみで事足りていましたが、インターネットの普及とともに、複数のサービスで異なるパスワードを設定し管理する必要に迫られました。

時期	説明
2000年代初頭	• 多くのユーザーは短くて簡単なパスワード（例：12345、password）を使用していました。 • セキュリティのためにパスワードを定期的に変更することが推奨されていました。
2000年代中盤	• 大文字、小文字、数字、特殊文字を組み合わせた複雑なパスワードが推奨されるようになりました。 • 1つのIDとパスワードで複数のサービスにログインできる仕組み（シングルサインオン（SSO））が普及し始めました。
2010年代	• パスワード管理ツールが普及し、複雑なパスワードの生成と管理が容易になりました。これらのツールは、複雑なパスワードを自動生成し、安全に保存する機能を提供します。 • パスワードの弱点を補完するスマートフォンや生体認証を用いた多要素認証（MFA）が一般的になりました。
2020年代	• 生体認証やパスキー、FIDO2（※1）などの技術により、パスワードを使用しない認証方法が増えてきました。 • 米国のNIST（※2）やCISA（※3）の最新のドキュメントでは、「パスワードの使い回しは絶対にしない」「パスワードマネージャーを使用する」等のパスワードに関するルールが紹介されています。

今後の見通し

認証に関するガイドラインである「NIST SP 800-63B」(※4)について、2024 年 8 月より改訂（NIST SP 800-63B-4 2pd）に向けた意見募集を実施しています。主な変更点の内、パスワード要件の見直しとして、パスワードの長さや複雑性ルールおよびパスワードの定期変更等に関する事項が変更されています。

- ✓ パスワードの長さ： 15 文字以上を求めることを推奨
- ✓ 複雑性ルール： パスワードに対して、特殊文字の使用や大文字小文字の混在等の追加の複雑なルールを強制することは禁止
- ✓ パスワードの定期的な変更： 要求することは禁止

これに伴い今後、NISC（内閣サイバーセキュリティセンター）が発行する「インターネットの安全・安心ハンドブック Ver5.00」や総務省の「国民のためのサイバーセキュリティサイト」に記載されている要件も見直される可能性があります。

なお、見直しに伴うセキュリティ強化の達成や運用効率化等を実現するため、組織内外のユーザーのデジタルアイデンティティを一元管理するための ID 管理ソリューション、またユーザーがシステムやサービスにアクセスする際の本人確認プロセスを管理・強化するための認証管理ソリューションの導入・更改も視野に入れる必要があるでしょう。

（水谷　浩樹）

(*1) パスキーとは　FIDO 認証との違い、3 つのメリットと課題 - WOR(L)D ワード｜大和総研の用語解説サイト

(*2) NIST Special Publication 800-63B

(*3) Secure Our World｜CISA

(*4) 「NIST SP800-63」は、デジタル空間上の本人（デジタルアイデンティティ）確認のための登録や認証に関するガイドラインのこと