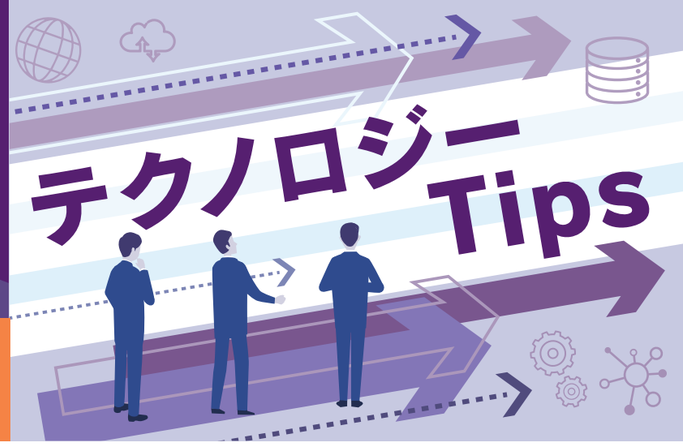
今こそ知りたい Tech Tips!
vol.15
(Ver2.0)

セキュリティインシデント…いろいろな企業が被害を受けていますよね…

最近のセキュリティインシデントを整理しながら、最新のソリューションを知り、対策を打ちましょう!

Windows11やMicrosoft365もセキュリティを大幅に強化していますよ。
2025年10月のWindows10サポート終了に向けて、セキュリティ強化も検討していきましょう。



2024年3月14日、警察庁より2023年版の国内サイバー犯罪レポート（「令和5年におけるサイバー空間をめぐる脅威の情勢等について」）が公開されました。

（2024年3月14日）

参考元URL：https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf 詳細はこちらから

＼ 残念ながら、サイバー攻撃に対する被害、インシデントは減ることはなく、増加傾向であることは間違いありません。整理しておきます。 ／

事例1 フィッシング報告・不正送金の被害が過去最悪

2023年は、インターネット関連のフィッシングと不正送金の被害が過去最悪となりました。
不正送金の発生件数は5,578件で、前年比391%の増加が見られ、被害総額は約87.3億円に達し、前年比474.6%の増加となりました。
フィッシング報告件数も約119万件で過去最悪を記録しています。また、セキュリティ対策ソフトウェア開発企業の調査によると、詐欺サイトへの誘導件数は2021年下半期以降、高水準を維持しています。

事例2 高い水準にとどまる国内組織へのランサムウェア攻撃

2023年のランサムウェア攻撃は197件報告され、高い水準が続いています。
セキュリティ企業の調査によるインシデント公表件数も同様の傾向を示しています。2023年には、名古屋港のコンテナターミナルがランサムウェア攻撃を受け、搬入出作業が3日間停止するという大きな影響がありました。
2024年に入っても、日本国内の病院や小売企業が攻撃を受け、業務停止や売上公表の延期につながるなど、事業継続に深刻な影響が出ています。

事例3 情報窃取を企図した不正アクセス

2023年には、電子部品関連企業、行政機関、学術機関、航空宇宙分野の研究開発機関から、不正アクセスの被害が公表されました。
これらの攻撃は、情報窃取を目的とした標的型攻撃で、重要産業や公的機関だけでなく、それらと取引のあるサプライチェーン内の企業や組織も標的にされる可能性があります。
そのため、どのような攻撃手口があるかを定期的に把握することが重要です。

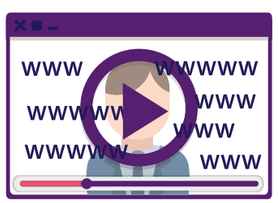
事例4 IoT機器を対象とした脆弱性探索行為

警察庁の「センサーにおいて検知したアクセス概況」によると、2023年の検知件数は1日9,000件以上と増加傾向にあります。調査目的とするIPアドレスからの通信が増加している一方で、IoT機器の普及により攻撃対象が増えていると分析されています。個人向けのIoT関連サービスを提供する企業・組織は、提供する機器の脆弱性をメンテナンスすることが重要です。
産業用IoT機器も探索行為の対象となり得るため、自組織への侵入経路となるIoT機器がないか確認する必要があります。

大きな企業のセキュリティインシデントも話題になりました。
被害を受けた企業も大変ですが、その企業の提供するサービスを利用するたくさんの人々も大きな影響を受けます。
ただ、中小企業のみなさまも他人事ではありませんよね…
こんな大きな企業でセキュリティ対策に大きな投資をしても、被害を受けてしまうのですから。
「対岸の火事」、「大企業だから狙われる」ではなく、できることからしっかり対策しましょう。

事例1 モバイル「Suica」、「えきねっと」などの交通系決済システムに障害が発生。
5月10日、サイバー攻撃に起因するシステム障害によりJR東日本が運用しているモバイル「Suica」や「えきねっと」などが一時的につながりにくい状態となりました。

事例2 動画サイト「ニコニコ動画」などを運営する株式会社KADOKAWAは6月8日、ニコニコを中心としたサービス群を標的としたサーバがランサムウェアを含む大規模なサイバー攻撃を受けたことを発表。
サイバー攻撃に関しては「BlackSuit」と名乗るサイバー犯罪グループが闇サイトに声明を発表。身代金の支払いに応じなければ7月1日には奪取した個人情報を全て公開すると主張していました…



来年、2025年10月14日にWindows 10のサポートが終了します。

Microsoft社は、Windows 11を過去最高のOSとして推奨しており、特に「セキュリティ」が20%向上しているとしています。具体的にどのような部分が強化されているのか、一緒に整理してみましょう。詳細については、ぜひ当社の担当者にお問い合わせください。

Windows 11のセキュリティが強化された理由は、いくつかの重要な機能と技術が導入されたためです。以下が主なポイントです。

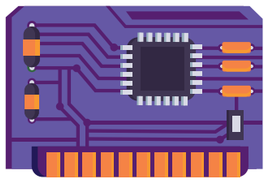
❶ コア分離とメモリ整合性

Windows11は、コンピュータの安全を守るために「仮想化ベースのセキュリティ(VBS)」という技術を使用しています。
この技術は、システムの重要な部分を仮想的に隔離された安全な領域で動かす仕組みです。
これにより、ウイルスやマルウェアがコンピュータの重要な部分に侵入しようとしても、直接触れないように防ぐことができます。
これを使うことで、システムが壊されるリスクが大幅に減ります。

例え　大切な書類を頑丈な金庫に入れておくようなものです。金庫の外で何が起こっても、中の書類はしっかり守られています。

❷ TPM(トラステッド プラットフォーム モジュール)2.0

TPM 2.0は、コンピュータに内蔵された特別なチップです。このチップは、パスワードや暗号化キーなど、非常に大切なデータを安全に保存します。Windows 11では、このTPM 2.0が必須になっており、これによってパソコンのセキュリティが大幅に強化されます。
たとえ悪意のあるプログラムが侵入しようとしても、このチップが大切な情報をしっかり守ってくれます。



例え　家の鍵を安全な金庫に入れておくようなものです。鍵が金庫で守られているので、家全体が安全です。

❸ セキュアブート

セキュアブートは、コンピュータを起動するときにすべてのプログラムが安全で正当なものであるかを確認する機能です。
もし不正なプログラムがあった場合、起動を防ぎます。
これにより、悪意のあるプログラムが勝手に動き出すことを防ぎます。

例え　車を運転する前にエンジンやタイヤをチェックするようなものです。問題があれば、車は出発しません。

❹ Windows Hello

Windows Helloは、生体認証を使ってデバイスにアクセスする機能です。顔認証や指紋認証を利用することで、パスワードを入力する必要がなくなります。
これにより、パスワードを盗まれる心配がなくなり、セキュリティが向上します。
また、パスワードを覚える手間も省けます。

例え　家の鍵を使わずに、顔認証でドアを開けるようなものです。鍵を持ち歩く必要もなく、安心して家に入れます。

❺ 強化されたWindows Defender

Windows Defenderは、リアルタイムでウイルスやマルウェアを見張り、すぐに取り除く機能を持っています。Windows11では、この機能がさらに強化され、常に最新の脅威からコンピュータを守ります。
これにより、デバイスが安心して使える環境が提供されます。

例え　家の中を常に見回って、不審者がいないかチェックする警備員のようなものです。何か怪しい動きがあれば、すぐに対応してくれます。

まとめ　Windows 11は、貴社のビジネスを強力に守るための最新セキュリティ機能を備えています。

- ☑ 「コア分離」により、重要なシステムを安全に保ち、マルウェアの攻撃を防ぎます。
- ☑ TPM 2.0チップでパスワードや重要なデータをしっかり保護。
- ☑ セキュアブート機能で、不正なプログラムの起動も阻止します。
- ☑ Windows Helloで顔認証や指紋認証を使い、パスワード不要で簡単に安全にアクセスできます。
- ☑ Windows Defenderも強化され、最新の脅威に迅速に対応します。

Windows 11への移行で、ビジネスの未来を切り開きましょう！
この新しいOSは、強力なセキュリティ機能で安心を提供し、AIアシスタントがあなたの生産性を最大化します。
今こそ、ICTへの投資で企業のデジタル変革(DX)を加速させる時です。パソコンの入れ替えからICTインフラ全体の見直しまで、私たちが未来を見据えたトータルソリューションをご提案します。

Windows 11で、もっと効率的に、もっと安全に、そしてもっとスマートに働きませんか？一緒に新しい時代の扉を開きましょう！

当社がしっかりご提案、導入サポートいたします！

まるっと当社にご相談ください！