2025年

Cyber Security News

8 月号

先月の報道を中心に、サイバーセキュリティに関してのニュースを抜粋してお届けしています

大手ハンバーガーチェーン店が使う求人サイトのパスワードが「123456」で応募者情報6,400万件が流出の可能性

すで犯罪者に知られている、「最も危険なパスワード」 今すぐ変更を！

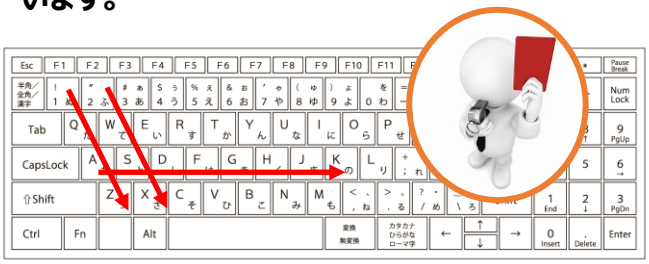
最も危険なパスワードのトップ10 日本版（個人：2025年7月12日現在）

日本のユーザー（個人）に関する最も危険なパスワードのトップ20のうち、上位10位までのリストが右記の通り。これらは、順番は異なりますが、**世界で最も使用されているパスワード（個人）の8つと一致**しており、**日本に関するユニークなパスワードは「aa123456」、「asdfghjk」「asdf12345」の3つとなっています。**

「asdfghjk」などは一見、ランダムな文字のようにみえますが、**キーボードの配列を左から右に順番に並べた**ままなので、**危険な（推測されやすい）パスワードとなっています。**

CAUTION

1. 123456789
2. password
3. 12345678
4. 1qaz2wsx
5. asdfghjk
6. asdf12345
7. aa123456
8. asdf1234
9. 123456
10. 1234567890



上記イラストはCopilotで作成

NordPassとNordStellarによって共同で作成されたリストより

今月の注目セキュリティトピックス

【事例紹介】奈良市立中学校でファイル共有設定ミス
～PTA議決資料が生徒・教職員等に誤って閲覧可能な状態に～

上記イラストはCopilotで作成

奈良市教育委員会は2025年7月18日、市立中学校においてGoogleドライブの共有設定ミスにより、個人情報を含むPTA議決資料が誤って奈良県内の教職員や児童生徒を含む他者に閲覧可能な状態で公開されていたことを公表しました。
　アクセス履歴の調査により、5名の閲覧が確認されましたが、ダウンロードなどの外部持ち出しの痕跡はなく、現時点で二次被害は報告されていないとのことです。
　今回の情報漏えいは、人的ミスが直接の原因ですが、背景には以下のような課題が潜んでいます。

クラウドストレージに対するリテラシー不足
Googleドライブ等のクラウドサービスの共有設定は多様であり、誤操作による情報公開が容易に発生します。利用者が幅広く、設定の複雑さに対する理解が浸透していない可能性があります。

システム上の自動チェック機能の不在
意図しない「広範囲への共有」設定を防ぐためのシステム的な制御がなかったことも問題です。

参照元：https://www.city.nara.lg.jp/site/press-release/243529.html

【事例紹介】建設会社の社有iPhoneがスミッシング攻撃被害

上記イラストはCopilotで作成

ある建設会社に所属する職員がショートメッセージを利用したサイバー攻撃「スミッシング」の被害に遭い、社有iPhoneに紐づけられていた個人情報にアクセス可能なAppleアカウントに対する不正アクセスが発生したそうです。同社によると、運送会社を装ったショートメッセージが届き、業務上の荷物を待っていた職員がメッセージリンクを開き、フィッシングサイトに誘導される事態となったそうです。その後、iPhoneは使用不能となり、Appleアカウントへの不正アクセスが確認されたとのことです。
不正アクセスを受けたAppleアカウントはiCloud上に同期されている電話帳にアクセス可能でした。電話帳には1,238件数の会社名・氏名・電話番号が記載されていたことがわかっています。

参照元：https://www.kumagaigumi.co.jp/news/2025/nw-20250704-003894.html

【大阪府警からの警告】サイバー犯罪は“今そこにある脅威”
～企業が今すぐ取り組むべき対策とは～

大阪・関西万博の開催に便乗した偽サイトの急増、公共機関やインフラを狙う標的型攻撃など、サイバー犯罪は日々進化しています。大阪府警では、セミナーなどで特に以下の点に注意を促しています。

企業がもっとも注意すべきランサムウェアで、中小企業の被害件数が増えている
攻撃ツールがサービス化され、実行者のすそ野が広がり、対策が手薄なことが多い中小企業が狙われているとも考えられ、BCP（事業継続計画）対策が重要。

VPN機器の脆弱性が最大の侵入口
強固なパスワード、多要素認証の導入、IPアドレスの接続制限の設定が必須。

なりすましメール・DDoS攻撃への備え
DMARC、WAFやIDS/IPSなどの対策機器やサービスの導入、海外IPからの通信の遮断などの多層防御が求められる。

フィッシング・サポート詐欺・SNS乗っ取りなど多様な手口
SIMスワップやリアルタイム型フィッシングなど、巧妙な手法が次々登場。

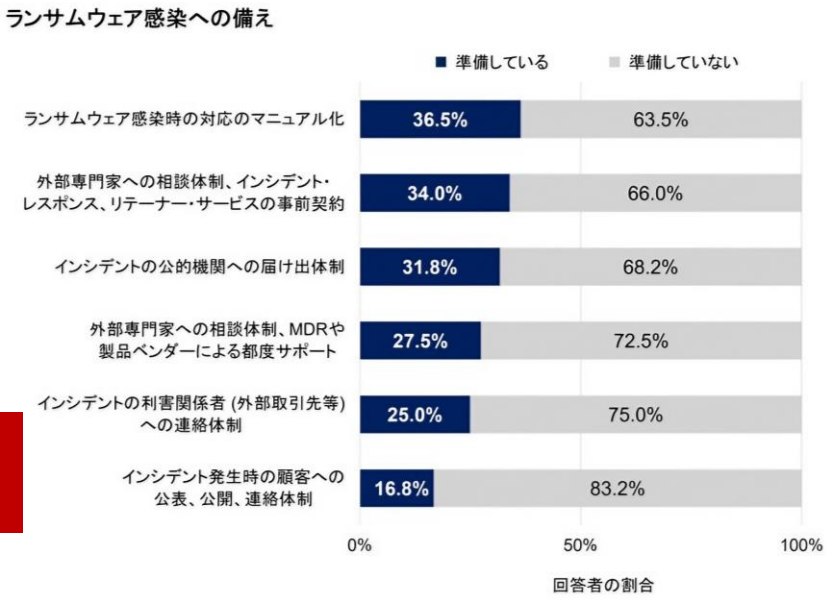
上記イラストはCopilotで作成

大阪府警は「セキュリティ対策は利益を生まないが、損失を防ぐ“経営の盾”」と強調。
万が一被害に遭った場合は、最寄りの警察署またはサイバーセキュリティ対策課へ通報して欲しいということです。

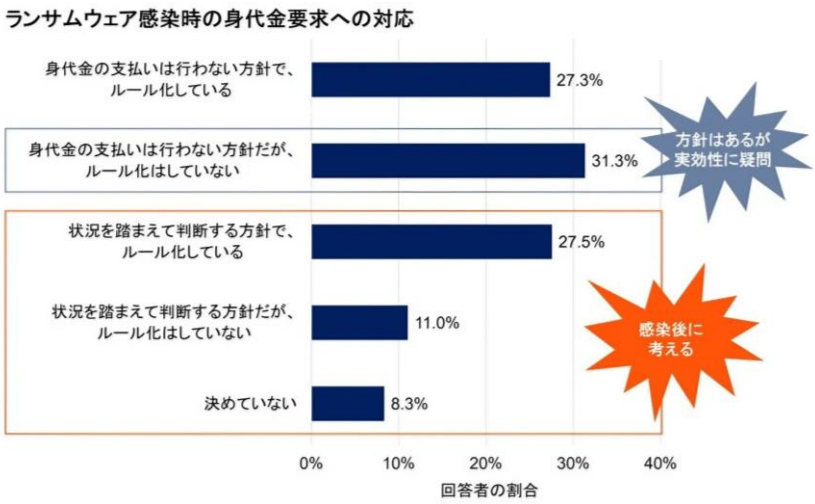
参照元：https://news.mynavi.jp/techplus/article/20250707-3368050/
参照元：https://www.police.pref.osaka.lg.jp/seikatsu/saiba/chuikanki/index.html

ランサムウェアの動向（ガートナージャパン調査）

ランサムウェア感染のインシデントは、企業が対処すべきセキュリティ脅威の重要事項です。Gartnerは2025年2月に、日本国内の従業員500人以上の組織のセキュリティ・リーダーを対象に実施した調査で、ランサムウェア感染への企業の準備状況を尋ねました。準備していると回答した割合が最も多かった項目は「ランサムウェア感染時の対応のマニュアル化」(36.5%)で、次が「外部専門家への相談体制、インシデント・レスポンス、リテーナー・サービスの事前契約」(34.0%) でした。



身代金、払う？払わない？企業の半数が「感染後に考える」



本調査で、ランサムウェア感染時の身代金への対応について尋ねたところ、「身代金の支払いは行わない方針だが、ルール化していない」が最も多く、31.3%の回答者に選択されました。「状況を踏まえてから判断する方針だが、ルール化はしていない」(11.0%)、「決めていない」(8.3%) などの回答を含めると、相当数の企業が、具体的な対応方法はランサムウェアの感染後に検討する予定であることが明らかになりました 。

ランサムウェア対策は事前の準備が重要だが、日本企業の準備は依然として不十分な状況

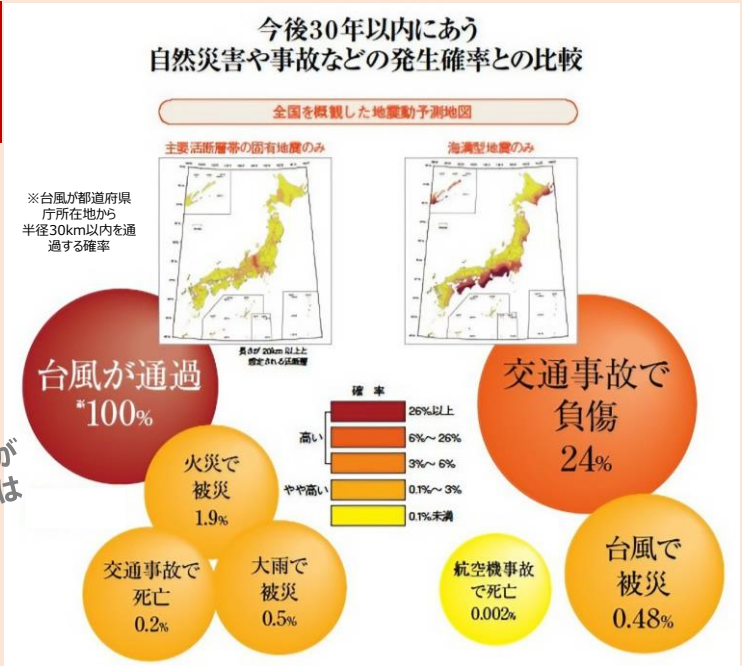
出典：2025年7月7日発表
ガートナージャパン株式会社国内のランサムウェア対策状況に関する最新の調査結果より
https://www.gartner.co.jp/ja/newsroom/press-releases/pr-20250707-ransomware

中小企業向けBCP対策の重要性「“備え”が、あなたの会社を守る」

近年、ランサムウェア攻撃の標的が中小企業にシフトしており、BCP（事業継続計画）未整備の企業が特に狙われやすい傾向にあると言われています。被害を受けた企業の多くが復旧に時間を要し、業務停止や信頼失墜などに直結するケースも発生しています。BCPの整備は、災害やサイバー攻撃などの緊急事態に備える「企業の生命線」となっています。今こそ、業務の優先順位や復旧手順を明確にし、実効性のあるBCPを構築しませんか？

今後30年以内に南海トラフ地震が発生する確率80%以上

サイバー攻撃を受けたことがあると回答した中小企業は30%以上



出典：文部科学省地震調査研究推進本部地震調査委員会「地震の将来予測への取組」「全国を概観した地震動予測地図」2008年版

「うちは小規模だから狙われない」―それはもう過去の話です。ランサムウェアは、セキュリティの弱い企業を狙います。BCPの整備は、企業規模に関係なく「生き残るための準備」です。また自然災害時の備えとしても、BCPの見直しを始めましょう。

オンラインセミナーのご案内　　インターネット環境があれば自席で受講できます。

災害大国日本における実効力のあるBCPの重要性

- **開催日　：　8月20日（水）（申込締切日：8月18日（月）まで）**
- **開催時間　：　14：00～15：00**
- **会場　：　オンラインセミナー会場**
  開催日前日にZoom視聴用URLをご案内いたします。
- **お申込み　：　下記URLより事前登録願います**
  https://canon.jp/biz/event
  お申し込み時には招待会社コードが必要です。担当セールスにご確認をお願い致します。

セミナー紹介動画！
https://youtu.be/_5DKCoBen2w

【セミナー概要】
近年、南海トラフ地震臨時情報の発令など、わが国の災害リスクは一層の高まりを見せています。
このような状況下で、企業にとって実効力のあるBCP（事業継続計画）の策定・運用は、事業の継続性と企業価値を守る上で、喫緊の課題として重要性が高まっています。
本セミナーでは、災害大国日本の現状と、近年多様化・激甚化する災害リスクを踏まえ、なぜ「今」BCP 対策が企業にとって不可欠なのかを解説させていただきます。
そして、有事の際に事業を継続させるために企業が BCPを策定する上で押さえるべき要素、さらに、絵に描いた餅で終わらせない「実効力を持つBCP」とするための具体的な勘どころについてご案内致します。

＜講師紹介＞

ニュートン・コンサルティング株式会社　　中村 大七 氏

キヤノンMJ　セミナー　検索

【講師プロフィール】
BCPコンサルタントとして製造業を中心に情報通信業やサービス業、大学法人等における事業継続計画（BCP）の策定・改善・訓練支援に注力。BCPに限らずERM（全社的リスクマネジメント）に携わり、形式的な支援ではなく、各社の事情に沿った本質的なリスクマネジメント支援を信条としています。
プライベートでは、洋酒、特にカクテルを好み、カクテルシェイカーを購入するほどとの事。

IPAによると長期休暇の時期は、システム管理者が長期間不在になりいつもとは違う状況になりやすく、もしウイルス感染や不正アクセス等の被害に遭っても対処が遅れる可能性が高くなります。このような事態にならないためにも、以下の対策の実施をオススメします！

長期休暇前

1．緊急連絡体制の確認

2．社内ネットワークへの機器接続ルールの確認と遵守
ウイルス感染した端末を社内ネットワークに接続し、拡散する事例が多発しています。
長期休暇中に社内ネットワークへ機器を接続する予定がある場合は、社内の機器接続ルールを事前に確認し遵守してください。

3．使用しない機器の電源OFF

長期休暇明け

1．修正プログラムの適用

2．定義ファイルの更新
長期休暇中に電源を切っていたパソコンは、セキュリティソフトの定義ファイルが古いままになっています。
パソコンを立ち上げたら、まずは定義ファイルを更新し最新の状態にして下さい

3．サーバ等における各種ログの確認

※参照元：IPA「長期休暇における情報セキュリティ対策」　https://www.ipa.go.jp/security/anshin/measures/vacation.html