2024年

Cyber Security NEWS 12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

【パスワードランキング2024発表】来年に向けて見直してみては？

日本人が使いがちな危険な組み合わせ、簡単にできる対策を！

	1位	2位	3位	4位	5位
2024（今回）	123456	password	123123	qwerty	111111
2021（前回）	123456	password	000000	1qaz2wsx	12345678

安全性を考える上で最も重要視して欲しい要素は文字数です。多いほど安全と言われ、総務省も10文字以上を推奨しています。ぜひ検討してほしいポイントですが、考えるのが難しい場合は単語ではなく文章を使う「パスフレーズ」を試してみてはいかがでしょうか？例えば「Osaka」では単語になってしまいますが、「Osakaga1banda!（大阪が一番だ!）」とすれば14文字になり、数字も記号も入ります。覚えやすく、強力なパスワードを簡単に作れるのでおすすめです。

推測されやすい駄目なパスワード

1. IDと同じ文字列を使っている
2. 名前や電話番号、誕生日などを含む
3. 「123456･･･」など単純な文字列
4. 辞書に載っている単語
5. 複数のサービスで使い回している
6. 他人に一度でも教えたことがある

※参照元：株式会社ソリトンシステムズ「日本人のパスワードランキング 2024最新版」 https://www.soliton.co.jp/products/csa/pw2410.html

生命保険会社の情報漏えい 18社で計42万2000件余 生命保険協会

生命保険会社で代理店に出向する社員による顧客情報の漏えいが相次いでいる問題で、生命保険協会は、10月末の時点で18の会社で合わせて42万件余りの情報漏えいが確認されたことを明らかにし、各社に対し再発防止を要請しています。

生命保険業界では、代理店に出向していた保険会社の社員が同業他社の顧客情報を出向元の会社にメールで送るなどの情報漏えいが相次いで確認されています。

生命保険協会は、金融庁と連携して各社に報告を求めたところ、10月末の時点で18の保険会社で合わせておよそ42万2000件の情報漏えいが確認されたと明らかにしました。

大手損害保険4社に2度目の報告徴求命令

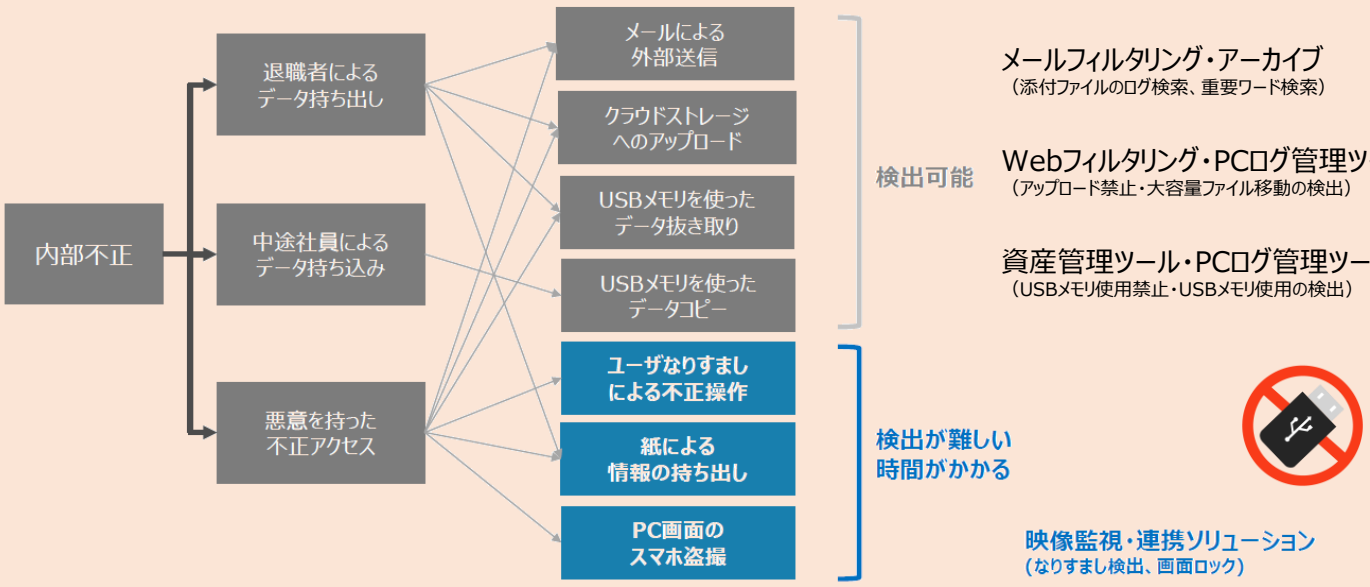
保険代理店から契約者の個人情報漏洩した問題で、金融庁が大手損害保険4社に2度目の報告徴求命令を出していたことがわかりました。

金融庁は大手損保に対して7月に最初の報告徴求命令を出していますが、実態をさらに詳しく調べるため追加で報告徴求命令を出したとみられます。

金融庁は11月15日に命令を出していて、12月13日までに結果を報告するよう求めています。

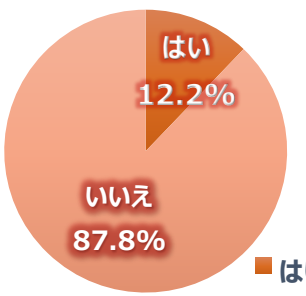
大手損保4社で判明した情報漏えい件数は約250万件

内部不正の種類と課題



内部不正・過失による情報漏えい対策の実態

12.1%が持ち運び可能な外部記憶媒体（USB等）を利用

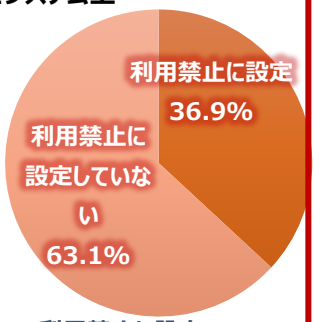


持ち運び可能な外部記憶媒体（USB等）を利用していますか？

USB等の持ち運び可能な外部記憶媒体を利用するのは、情報管理の観点で非常にリスクのある状態です。しかしながら12.1%で利用されていることが分かりました。容易に外部に持ち出しができてしまい、不正利用や、紛失・盗難による情報漏えいリスクが高まります。　※「Assured調べ」：https://assured.jp/20231027-01

持ち運び可能な外部記憶媒体をシステム上利用禁止にしている割合

持ち運び可能な外部記憶媒体は、利用禁止のルールを定めるだけでなく、システム上接続不可にすることが推奨されますが、設定できているのは36.9%にとどまりました。
ルールの策定や教育を行うことは有効ですが、外部記録媒体の利用を不可とするならば、システム上利用禁止に設定することが実効性のある対策になります。



63.1%が持ち運び可能な外部記憶媒体（USB等）の利用を、システム上制御できていない

大阪・関西万博に向けテロ対策協議 官民一体で連携を強化

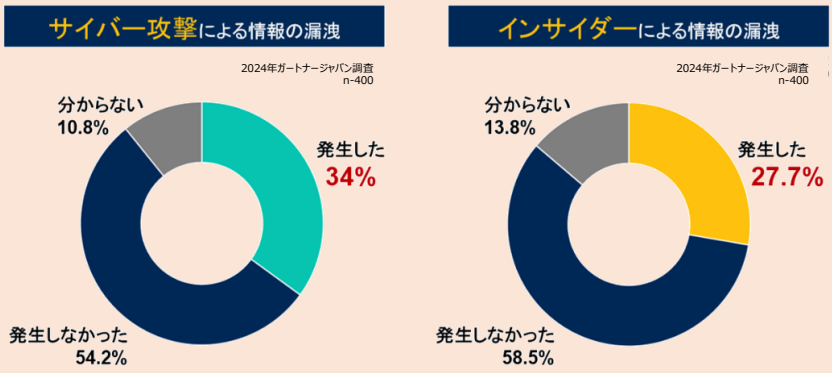
来年の大阪・関西万博に向け、警察や行政、企業の関係者が集まりテロ対策を協議する会合が大阪市で開かれ、官民一体となって連携を強化していくことが確認されました。

また、政府は、2025年大阪・関西万博へのサイバー攻撃対策の強化に向け、内閣サイバーセキュリティセンター（NISC）や重要インフラ事業者など官民による大規模演習を年明けにも実施する方針を固めており、国際イベントは大規模な攻撃を受けやすいため、専門職員の派遣や民間事業者への講習なども行い、安全対策に万全を期す考えです。

万博を巡っては、ウクライナ侵略を巡る日本の制裁に反発するロシアが昨秋、参加取りやめを表明しています。政府は、ロシアによる報復的な行動を含め、様々な主体によるサイバー攻撃への警戒を強めています。

サイバー攻撃・インサイダーが原因の情報漏えいを経験した国内企業が各々約3割

情報漏洩の発生状況



ガートナージャパンは、日本国内のセキュリティリーダーを対象にした情報漏えいの発生状況に関する調査結果を発表しています。同社は、AIや生成AIの利用がビジネス環境で身近になるにつれ、企業における情報漏えいのリスクへの懸念も高まっており、セキュリティと企業競争力強化を目指すためにデータセキュリティの刷新が重要だとしています。

また同調査によると、サイバー攻撃が原因の情報漏えいを経験した企業の割合は34.0%、インサイダーが原因の情報漏えいを経験した企業は27.7%だった。さらに情報漏えい対策が十分でないため、AIなどによるデータ活用の拡大について不安に感じていると回答した企業は57.2%だったとしています。

出典元：Gartner(2024年10月) https://www.gartner.co.jp/ja/newsroom/press-releases/pr-20241030-datasecurity

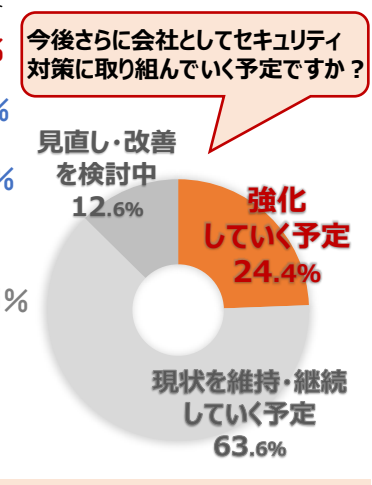
情報漏洩が問題になっているなか、他の会社ではどのような対策を行っているのでしょう？

IT企業以外の会社ではセキュリティ対策が十分に実施されていないケースも多く、対策を講じれば本当に情報漏洩を防げるのか、そもそもなぜ情報漏洩が発生するのかなど、疑問に思う方も少なくないでしょう。

また現在セキュリティ対策を行っていない場合、実際に情報漏洩をした会社はどれくらいあるのか・またなぜ情報漏洩したのか、今後さらに会社として情報漏洩対策強化を行う目的など、気になりますね。

調査概要：「情報セキュリティ投資」に関する調査

【調査方法】PRIZMAによるインターネット調査
【調査人数】1,016人
【調査対象】調査回答時にIT企業以外の経営者と回答したモニター
※NSSスマートコンサルティング株式会社「情報セキュリティ投資」に関する調査結果
https://prtimes.jp/main/html/rd/p/000000021.000055385.html



永続版Microsoft Officeのサポート終了日に注意

永続版のOfficeは、これまで5年間のメインストリームサポート、5年間の延長サポートが提供されてきました。しかし、段階的に延長サポートが短くなってきており、Office 2021からはメインストリームサポートの5年間のみとなり、大幅にサポート期間が短くなっています。

2025年にサポートが終了する主なMicrosoft製品

この他、Azureの幾つかのサービスやMicrosoft SQL Server 2012（拡張セキュリティ更新プログラム3年目）、SQL Server 2014（拡張セキュリティ更新プログラム1年目）、Exchange Server 2016／2019などのサーバ製品のサポートも終了予定なので、利用していないかどうかを確認することをおすすめします。

参照元
https://atmarkit.itmedia.co.jp/ait/articles/2411/18/news016.html

主なOffice製品	サポート終了日
Microsoft Office 2016	2025年10月14日
Access 2016	2025年10月14日
Excel 2016	2025年10月14日
OneNote 2016	2025年10月14日
Outlook 2016	2025年10月14日
PowerPoint 2016	2025年10月14日
Project 2016	2025年10月14日
Publisher 2016	2025年10月14日
Visio 2016	2025年10月14日
Word 2016	2025年10月14日
Microsoft Office 2019	2025年10月14日
Access 2019	2025年10月14日
Excel 2019	2025年10月14日
Outlook 2019	2025年10月14日
PowerPoint 2019	2025年10月14日
Project 2019	2025年10月14日
Publisher 2019	2025年10月14日
Visio 2019	2025年10月14日
Word 2019	2025年10月14日

2025年にサポートが終了する主なOffice製品

主なMicrosoft製品	サポート終了日
Azure Database for MariaDB	2025年9月19日
Azure Basic Load Balancer	2025年9月30日
Azure HPC Cache	2025年9月30日
Azure Service Map	2025年9月30日
Azureアンマネージドディスク	2025年9月30日
Azure vFXT	2025年9月30日
SQL Server 2012（拡張セキュリティ更新プログラム3年目）	2025年7月8日
SQL Server 2014（拡張セキュリティ更新プログラム1年目）	2025年7月8日
Visual Studio 2022、バージョン17.8（LTSCチャネル）	2025年7月8日
Exchange Server 2016	2025年10月14日
Exchange Server 2019	2025年10月14日
Skype for Business 2016	2025年10月14日
Skype for Business 2019	2025年10月14日
Skype for Business Server 2015	2025年10月14日
Skype for Business Server 2019	2025年10月14日
Visual Studio 2015	2025年10月14日
Visual Studio Team Foundation Server 2015	2025年10月14日
Windows Server 2012（拡張セキュリティ更新プログラム2年目）	2025年10月14日
Windows Server 2012 R2（拡張セキュリティ更新プログラム2年目）	2025年10月14日
Windows Server 半期チャネル、バージョン23H2	2025年10月24日

2025年にサポートが終了する主なMicrosoft製品

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。

販促物で売上・企業価値拡大！
事例で学ぶ販促デザインセミナー

- **開催日　：　12月17日（火）（12月12日 17:30申込締切）**
- **開催時間　：　14：00～15：00**
- **定　員　：　300名**
- **対　象　：　企画・広告・広報を担当する皆さま、営業推進を担当する皆さま**
- **お申込み：下記URLより事前登録願います**
  URL：https://canon.jp/business/event

セミナー紹介動画！
https://youtu.be/nqLIQ63vEwU

キヤノンMJ　セミナー　検索

今回のセミナーでは、実店舗での実績豊富な講師が、集客力や販促力を発揮するＰＯＰやチラシの作成方法のコツを解説します。
また、実際の現場で、この作成方法を使って、どのように販売力・集客力アップにつながったか、事例も豊富にお伝えしますのでよりご理解しやすい内容となっております。
新たに作成されるPOPやチラシなど販促物をより良いものにするためのヒントをたくさんご紹介しますので、是非、この機会にご参加ください。

≪講師紹介≫

Nasunoデザインワークス　代表　那須野　雄一郎　氏

（グラフィックデザイナー・販促物コンサルタント）

某チェーンストアにて全社向けのPOP・チラシ等の販促物の制作を担当後、現在独立。チェーンストアにおいてオリジナルのPOP作成と展開によって医薬品・サプリメントなど担当部門の利益を大幅に改善する。業務の傍らデザインスクールにても学び、2011年度二科展デザイン部入選。現在は、飲食店や美容室、他様々な分野の販促物も手がける。

セキュリティ対策の準備は万全ですか？　ーお正月休暇に向けてー

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！

仕事納め　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

仕事始め　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