2024年

Cyber Security NEWS 11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

日本へのサイバー攻撃が急増し、被害が拡大！

ロシア系のハッカー集団が日本の自治体や交通機関などのウェブサイトに大量の通信を送りつけるサイバー攻撃を行ったとSNS上で主張

10/23には首相官邸の偽サイトを確認、青木官房副長官が注意喚起

青木官房長官は衆院選が公示された10月15日に自民党のホームページがダウンしたことについてサイバー攻撃の可能性を示唆しています。「ハッカー集団によるサイバー攻撃に関する動向は政府として承知している」と明かしました。また、政府の有識者会議は相手の攻撃を未然に防ぐ**「能動的サイバー防御」の導入**に向けた法整備の議論を進め、「可能な限り早期に法案をお示しできるよう検討をさらに加速していく予定だ」と言及しています。

さらに、10月23日の記者会見では、同じく官房長官が首相官邸ホームページの偽サイトを確認したと明らかにしています。「国民が誤ってアクセスし、個人情報を盗まれることがないよう、官邸のホームページやSNSで注意喚起を行った」と説明しました。

※イラスト参照元：産経新聞社 https://www.sankei.com/article/20241025-4JVJMMXADNIMLPVWE3X4NV5VYI/?outputType=theme_election2024

ロシア系ハッカーが犯行声明

過去には世界で選挙前後にサイバー攻撃の被害が発生

ウクライナ支援国に対するサイバー攻撃を行う親ロシア派の「ハクティビスト」が、日本への攻撃も活発化させました。衆院選公示日に、自民党公式ホームページ（HP）が閲覧できなくなり、グループが攻撃したとの声明を出しています。過去に世界では、選挙の前後で混乱を狙うかのようにサイバー攻撃が確認されたケースがあり、日本でも多くの被害が確認されており、これまで以上に注意が必要だといいます。

山梨県や名古屋市などの全国自治体や福岡空港、とかち帯広空港、複数の造船所や第2地方銀行、日本証券業協会などの金融業界団体などにもDDoS攻撃による被害は広がっており、ロシア系ハッカー集団がサイバー攻撃を行ったとSNS上で主張しています。

能動的サイバー防御

➢能動的サイバー防御については、政府が平時からサイバー攻撃の兆候を監視し、必要に応じて攻撃元のサーバーに侵入して無力化することを目指しています。すでに、自民党が法整備の議論を開始し、政府も有識者会合を開催しています。今後、法案が成立すれば、企業や公共機関がサイバー攻撃に対して積極的な防御策を講じることができるようになります。

企業のセキュリティ対策の格付け基準

➢企業のセキュリティ対策の格付け基準については、経済産業省が2025年度に企業のサイバー攻撃対応力を5段階で格付けする制度を導入する予定です。この制度は、企業のセキュリティ対策の質を可視化し、取引先やビジネスパートナーの選定基準として重要な指標となります。特に、サプライチェーンに関わる企業には高いセキュリティ対応力が求められることになります。

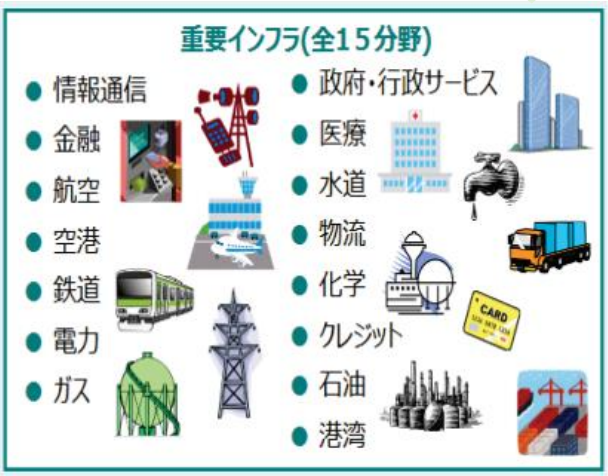
企業のサイバー攻撃対策の格付けイメージ

← 自己宣言型 →			←第3者機関の認定→	
1つ星 ★	2つ星 ★★	3つ星 ★★★	4つ星 ★★★★	5つ星 ★★★★★
← 中小企業 →			重要インフラ関連企業↑	
		←サプライチェーン形成企業→		

法改正も含めた検討

政府の主な政策目標と課題

目 標	課 題
サイバー空間の怪しい動きを平時から監視	「通信の秘密」などを規定する憲法との整合性
サイバー攻撃前に相手サーバーを無害化	サーバーが置かれた国との摩擦を生まないか
民間通信事業者が保有する通信情報を活用	政府が正しく活用していることをどう担保するのか



※NISC（内閣サイバーセキュリティセンター）に代わる独立した第三者機関を検討

（出所）有識者会議通信情報の利用に関するテーマ別会合（第１回）資料より一部抜粋

10/27 衆院選の結果を受け、法改正時期に不透明な部分は残りますが・・・

「サイバー安全保障分野での対応能力の向上に向けた有識者会議」のこれまでの議論の整理（論点整理）が8月7日に公表されました。また9月10日、自民党は「能動的サイバー防御」に関する提言を首相へ提出。岸田首相（当時）は、「能動的サイバー防御」の法制化に向け、「できるだけ迅速に対応できるよう取り組みたい」と述べています。同席した安全保障調査会長は記者団に、「日本の安全保障上、↗速やかに法整備に移ることが極めて重要だ」と強調している様に、憲法が保障する「通信の秘密」とどう整合性を取るかなどの法整備に向けた議論を進め、第三者機関と重要インフラ関連企業への対応指針を検討して、企業のセキュリティ対策格付け基準の内容が決まってくるのでは？と思われます。現在、秋の臨時国会への提出を目指していると報道されていましたが、時期は不透明な状況です。

経済同友会　インフラ企業のサイバー被害、報告義務化を提起

経済同友会は、サイバー攻撃への一層の対策を促す政策提言を発表。重要なインフラを担う事業者には攻撃の被害などについて政府への報告を義務付けるよう提起しました。攻撃を未然に防ぐ「能動的サイバー防御」を早期に導入すべきだとも訴えています。 民間企業はレピュテーション（評判）リスクの不安から、情報を出さない場合があり、官民で新たな組織体を立ち上げて政府との情報交換や対応支援などに取り組み、「ギブ・アンド・テイク」の概念を念頭に信頼関係を築くよう同友会として提唱しました。
企業経営者に向けてはサイバー攻撃のリスクを重要な経営課題だと認識し、取締役会の議題に設定する必要があると記しています。 参照元：https://www.doyukai.or.jp/policyproposals/2024/241023.html

頻発するランサムウェア事件に見る委託先セキュリティ対策の重要性

物流代行事業（大阪市）

物流代行事業社のサーバーにおいてランサムウェアの感染が確認された事件では、同社のサービスで保有していた情報が流出した可能性もあることから、同社サービスを利用する約50社の企業から被害の可能性が発表されました。
さらに埼玉県の同業社でも同様にランサムウェアの被害が発生し、各企業に影響がでています。

保育園、学童サービス

ランサムウェアによるサーバへの外部からの不正アクセスの形跡を検出。
具体的な情報漏洩の事実は確認できていないものの、保有する企業情報や個人情報の一部が漏洩もしくは閲覧された可能性があり、東京都や千葉県、神奈川県の複数の市区や、愛知県、関西でも大手私鉄系で保育園事業を委託していた企業にも影響がでています。

健康組合向けソフト開発

サーバの脆弱性およびVPNルータの設定不備から、攻撃者が社内ネットワークに不正侵入し、ランサムウェアにより、複数のサーバに対してデータの暗号化、サーバのイベントログの消去、バックドア設置の痕跡が確認されています。
この事件では関西系企業を中心に、複数の企業の健康保険組合で情報漏えいの可能性が公表されています。

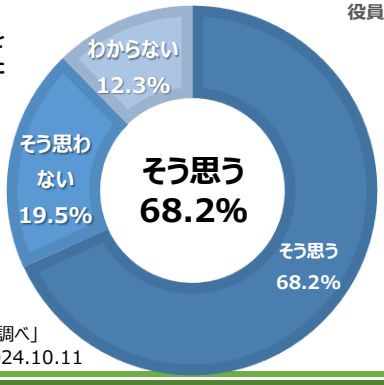
これらの事件は、企業が自社だけでなく委託先にもサイバーセキュリティ対策を強化する必要性を強く示唆しています。

これらはサイバー攻撃が単に企業単体に対して行われるものではなく、取引先や委託先を通じて広がるリスクがあることを示しています。企業が取るべき対策として、委託先のセキュリティ評価は重要です。業務を委託する際、その企業のセキュリティレベルを事前に評価し、不十分な場合には契約を見直す必要があります。
また、問題が発生した際の迅速な情報共有と対応も重要です。このようなインシデントでは、問題が発生してから対応までのスピードが被害拡大を防ぐ鍵となります。さらに、従業員に対するサイバーセキュリティ教育も不可欠であり、定期的な訓練によって従業員の意識を高め、サイバー攻撃への初期対応能力を強化する必要があります。

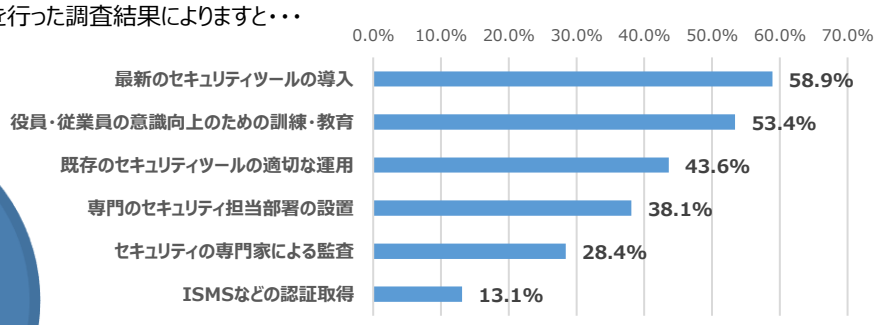
236名のインシデント経験者の回答から明らかになった「過去に戻れるならやりたい6つのサイバー防衛強化策」とは？

AironWorks株式会社が、現在情報セキュリティ関連業務に従事し、実際にセキュリティインシデントを経験したことがあるセキュリティ担当者236人を対象にインシデント発生後の対応に関する実態調査を行った調査結果によりますと・・・

質問：あなたが現在勤務する会社で経験したセキュリティインシデントは、しっかりとしたセキュリティ対策を行っていれば防げたものだったと思いますか？



n=236



「AironWorks株式会社調べ」
配信元：PRTIMES　2024.10.11

「セキュリティインシデントを未然に防ぐための有効な対策」

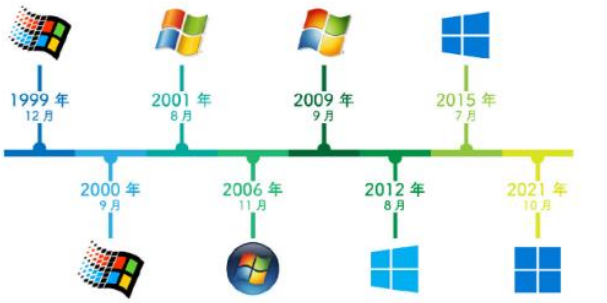
「最新のセキュリティツールの導入」が58.9%で最多となり、「役員・従業員の意識向上のための訓練・教育」が53.4%で続きました。
過半数の担当者の回答が集中していることからも、サイバー攻撃対策として新しいセキュリティ製品の活用と、役員・社員への啓発活動が重要であると言えます。

Windows 10の終了まであと1年！ 計画的な入替を！
でも「22H2」にアップデートしていないとすでに危険だとご存じですか？

「Windowsの仕様」でWindows 10の「バージョン」や「OSビルド」を確認。
少なくともバージョンが22H2でないと危険です。

■Windows　10のバージョン

【21H1】2021年5月18日提供→2022年12月13日サポート終了
【21H2】2021年11月16日提供→2023年6月13日サポート終了
【22H2】2022年10月18日提供→2025年10月14日サポート終了



Windowsのバージョンの歴史

- **Windows XP：2001年**
- **Windows Vista：2006年**
- **Windows 7：2009年**
- **Windows 8：2012年**
- **Windows 10：2015年**
- **Windows 11：2021年**

Windows7のサポート終了時には深刻なPC不足も発生しています。

自分のWindows 10パソコンのバージョンが「22H2」になっているかを確認しましょう。その方法は簡単です。設定の「システム」→「詳細情報」を開き、「Windowsの仕様」で現在のバージョンを確認できます。

開催概要

お申込み：https://v2.nex-pro.com/campaign/72045/apply?np_source=C301

会 期 ：2024年11月20日（水）13:00~2024年11月22日（金）16:30
形 式 ：ライブ配信セミナー
参加費：無料
主 催 ：キヤノンマーケティングジャパン株式会社
企画協力：アイティメディア株式会社 ITmedia エンタープライズ編集部

詳しくは・・・

招待コード：BP01

こんな課題を抱える方におすすめ

- ランサムウェアをはじめとしたサイバー攻撃の最新動向や攻撃手法を知りたい
- サイバーや物理で生じるセキュリティリスクを知り、効果的な対策を講じたい
- 予算やリソースの兼ね合いから自社でできるセキュリティ対策には限界がある
- セキュリティの保守・運用についても課題を抱えている

■本イベントは事前申し込み制です
(申込締切：2024年11月22日(金)16:05まで)

■お問い合わせ
Canon Security Days 2024 事務局：
ssinfo@canon-mj.co.jp

ECサイトにおける脆弱性診断が義務化へ

オンラインショッピングが日常の一部となった今、ECサイトの安全性確保は喫緊の課題となっています。

そんな中、急増するサイバー攻撃からECサイトを守り、私たち消費者の個人情報やクレジットカード情報を保護するため、経済産業省は2024年度末を目処にすべてのECサイトに対して、脆弱性診断の実施を義務化する方針を発表しています。
定期的な脆弱性診断の実施が、今後ますます重要になると考えられます。

2023年のカード不正利用被害額は、前年比2割増の541億円に。そのうち93%がクレジットカード番号の盗用による被害。総務省の調査結果でも、不正アクセス件数が急増しており、その大半が全国の中小企業で発生しています。

まずは、自社のセキュリティポリシーを作ることから始めましょう。経済産業省が公開している「ECサイト構築・運用セキュリティガイドライン」を参考にしてはいかがでしょうか？

「ECサイト構築・運用セキュリティガイドライン」
https://www.ipa.go.jp/security/guide/vuln/guideforecsite.html