Canon

2025年

Cyber Security News

12

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

月号

2025年の傾向から、来年に備えるべきことは？

2024年末から2025年始にかけて、DDoS攻撃が相次いで発生し、46の組織が標的になったと報告されるなど、日本国内がサイバー攻撃による混乱から始まった今年も残すところわずかとなりましたが、現在も大手飲料メーカーやオフィス用品の通販サービスを展開する大手企業などへのランサムウエア攻撃による混乱が続いています。

これまで以上にランサムウェアやサプライチェーン攻撃の脅威が増す状況のなか、中小企業は2026年度開始予定の経済産業省の**「セキュリティ対策評価制度」**を見据えた対策が急務と言えます。

取り組むべき対策は、主に以下の通りです。

「SECURITY ACTION」の自己宣言: まずはIPAが定める「中小企業の情報セキュリティ対策ガイドライン」に基づき、基本的な対策を実施し「SECURITY ACTION」を自己宣言することが、新制度対応への第一歩となります。

サプライチェーン対策: 自社だけでなく取引先も含めたサプライチェーン全体のリスクを認識し、対策を講じることが評価基準に含まれるため、関連企業と連携したセキュリティ水準の底上げが必要です。

事業継続性の確保: 攻撃による事業停止リスクに備え、製品・サービスの提供途絶を防ぐための事業継続計画（BCP）の策定が重要です。

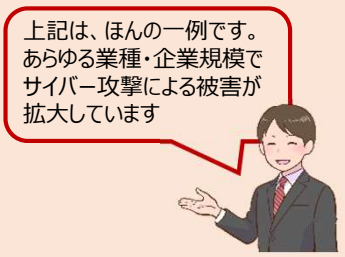
可視化と証明: 実施したセキュリティ対策を文書化・可視化し、客観的に証明できるようにしておくことが求められます。

これらの取り組みにより、取引先からの信頼獲得と経営リスクの低減を目指しましょう。

2025年日本国内のサイバー攻撃を振り返る

	業種	被害規模	概要
2024年末～2025年1月	航空事業者、金融機関、通信事業者、日本気象協会 他	欠航や遅延、インターネットがつながりにくいなど	警察庁が「MirrorFace」によるサイバー攻撃に注意喚起、DDoS攻撃
2025年1月	インターネットカフェ、フィットネスジム運営	約729万件の顧客情報が漏えいした可能性	システムへの不正アクセス（DDoS攻撃）
2025年1月	専門小売チェーン	約12万件情報漏えい	公式アプリへの不正アクセス
2025年2月	テーマパーク運営会社	最大200万件情報漏えいの可能性＋予約停止	ネットワークに不正アクセス（ランサムウエア攻撃）
2025年2月	医療法人	30万人の患者情報漏えい	ランサムウェア感染
2025年2月	保険サービス事業	約510万件情報漏えい	ランサムウェア感染
2025年3月	地域密着型百貨店・スーパー	全23店舗臨時休業	ランサムウェア感染
2025年4月	大手損害保険会社	最大で約1750万件の顧客情報が漏洩	Webサブシステムの脆弱性悪用
2025年4月	インターネット、通信大手	複数企業に二次被害、顧客情報407万件漏えいの可能性	メールサービス不正アクセス
2025年4月	情報・プラットフォーム企業	約90万件の情報漏えい	不正アクセス
2025年4月	複数の大手証券会社	犯罪集団「フィッシング」急増	口座乗っ取り、株売買
2025年4月	物流大手	基幹システム停止	ランサムウェア感染
2025年4月	学校法人：大学	全国7キャンパスで休講	ランサムウェア感染
2025年5月	鞄・バッグ類、小物類卸売業	個人情報 9万件とカード情報3万件超	ECサイトへの不正アクセス
2025年6月	学習教材出版	個人情報約33万件	SQLインジェクション攻撃
2025年6月	紳士服販売業	約1万8,000件	ランサムウェア感染
2025年7月	調査・情報サービス業務	30社以上の委託元保険会社	ランサムウェア感染
2025年7月	イベント会社	約91万人の個人情報漏洩	イベントサイトへの不正アクセス
2025年9月	コーヒー チェーン店	約3万1,500件	委託先がランサムウェア感染
2025年9月	大手飲料メーカー	全国出荷・工場一時停止	ランサムウェア攻撃
2025年10月	オフィス用品通販	業務システム停止	ランサムウェア感染
2025年10月	全国スーパー	約3万人の従業員の個人情報	委託先がランサムウェア感染
2025年11月	新聞社	1.7万人の社員・取引先情報	ビジネスチャット「Slack」への不正ログイン
2025年11月	国立国会図書館	コピーサービス利用情報4万件	再委託先事業者へのサイバー攻撃

2025年のサイバー攻撃は高度化と多様化が顕著であり、特にAIの悪用が急増しました。生成AIを利用したフィッシングや偽情報拡散は精巧化し、従来の防御策では見抜きにくくなっています。ランサムウェア攻撃は依然として圧倒的な脅威であり、製造業・物流・医療・教育機関が主要な標的となりました。また、委託先を経由するサプライチェーン攻撃が増加し、取引先や外部サービスの脆弱性が深刻なリスクとなっています。さらに、航空業界やネットサービスを狙ったDDoS攻撃によるサービス停止も目立ちました。2026年に向けて中小企業が注意すべきは、①AIを悪用したフィッシング対策の強化、②ランサムウェア防御とバックアップ体制の整備、③委託先を含むサプライチェーンのセキュリティ確認、④多層防御による不正アクセス防止、⑤DDoS対策と可用性確保です。また、人的教育も非常に重要な要素です。サイバー訓練など、ぜひご相談ください！



参照元：各メディア掲載NEWSより、抜粋

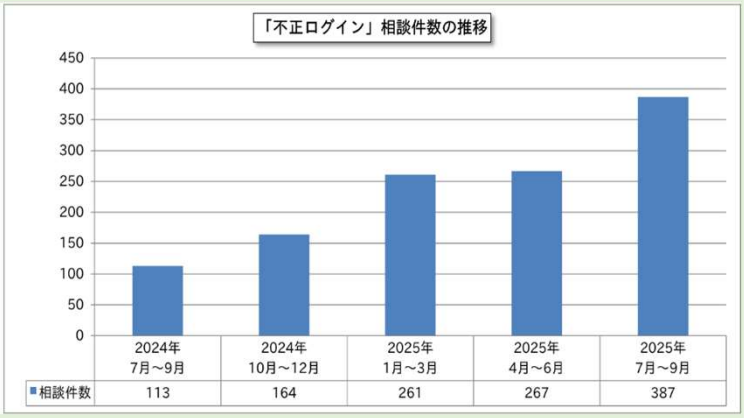
IPA報告 「不正ログイン」相談が約1.5倍 –「偽警告」は関係者逮捕で減少するも限定的

2025年第3四半期に個人から寄せられたセキュリティの相談件数は、前四半期比4.0%減となり、2,824件だった一方、「不正ログイン」に関する相談については約1.5倍に増加しているそうです。

情報処理推進機構（IPA）が、第３四半期に同機構の「情報セキュリティ安心相談窓口」で対応した個人からの相談状況について取りまとめたレポートによると・・・

同四半期に寄せられた相談件数は2,824件。前四半期の2,941件から約4.0%減少し、2期連続で減少しています。

相談内容を見ると、「マルウェアを検出した」などと偽の警告画面で不安を煽り、「サポート窓口」を装って金銭をだまし取ったり、端末を侵害する「偽警告」が647件で、912件だった前四半期から約29.1%減と目立って減少しています。
5月にサポート詐欺に関与したとされる6人が逮捕され、一時的に相談件数の減少が見られたものの、その後増加しているとし、予断を許さない状況となっています。



参照元 https://www.ipa.go.jp/security/anshin/reports/2025q3outline.html

大手飲料メーカーのランサムウェア被害の続報
最大191万件の顧客情報漏洩の恐れあり 完全復旧は来年2月以降の見通し

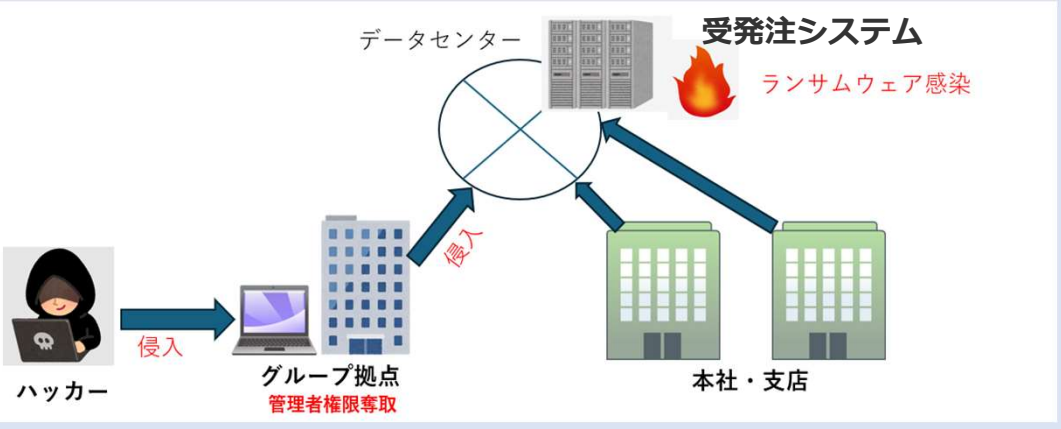
アサヒグループホールディングス（HD）は11月27日、サイバー攻撃で191万件の個人情報が流出した可能性があると発表

被害が発覚した9月29日から約2か月となるタイミングで勝木敦志社長など経営陣が記者会見を開き、攻撃を受けた原因や商品を受発注するシステム障害の状況などについて説明しました。
感染経路について**グループ内の拠点にあるネットワーク機器を経由**してデータセンターのネットワークに侵入され個人情報が盗み取られたとしています。同社は再発防止策として、通信経路やネットワークを再設計し、2026年2月までの復旧を目指すとの事です。
同社ではセキュリティ対策として**EDRは導入していたものの今回のサイバー攻撃には検知できなかった。**「一定の対策以上のことは実施していたが、攻撃者は想定を上回って巧妙かつ高度だった」とのコメントを残しています。
システムのバックアップは実施しており、「幸いなことに、そのバックアップが生きていた。それを活用し、自ら復旧を進めることができている。ただし、バックアップがあるからといって、一気にそのデータをシステムに戻せばよいといった単純なことではない。壊れた、触られた箇所がないのか、システムを確認し、リスクの点検を進めた上で、確認しながら修復していくことになるとの見解を示しました。

参照元：各メディア掲載ニュース

攻撃から復旧までの全体像　ハッカーは拠点のネットワークから侵入

[拠点ネットワーク機器]
↓（侵入）
[データセンター]
├─ 管理者権限奪取
├─ サーバー侵入・偵察
└─ ランサムウェア一斉実行]
↓（暗号化）
[ネットワーク遮断・隔離]
↓
[バックアップ活用]
↓
[慎重な検証・修復]
↓
[正常稼働へ]



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。

「2026年 セキュリティ対策評価制度」解説セミナー

～ 取引先から選ばれる企業へ！ SECURITY ACTIONで備えるセキュリティ強化 ～

- **開催月日 ： 2025年12月19日（金）** （申込締切：12月16日（火）まで）
- **開催時間 ： 14:00～15:00**
- **定員 ： 300名（参加費無料）**
  開催日前日にZoom視聴用URLをご案内いたします。
- **会場 ： オンラインセミナー会場**
  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。

キヤノンMJ　セミナー　検索

【セミナー申込】事前登録が必要です。※プロモーション動画サイトからも直接ページ移動できます。

WEBサイト:https://canon.jp/biz/event

■セミナー概要

2026年度から本格運用が予定されている「セキュリティ対策評価制度」は、
企業のセキュリティ対策レベルを可視化し、取引先との信頼構築に活用できる
新たな仕組みです。
本セミナーでは、制度の概要と評価基準をわかりやすく解説するとともに、
今から取り組むべき「SECURITY ACTION」の実践方法をご紹介します。

＜講師紹介＞

キヤノンマーケティングジャパン株式会社
ITSビジネス推進部　エリアＳＳ第二課
松永 皐希

＜講師プロフィール＞

2020年入社、セキュリティソリューションスペシャリストとして、
クラウド・ネットワーク領域における提案・導入支援を担当。
主な資格：基本情報処理技術者

セミナー紹介動画！
https://youtu.be/EwMF06JD-W0

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

出展：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