Canon

2025年 11 月号

Cyber Security News

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

大手飲料メーカーを襲ったランサムウエア攻撃の衝撃

大手飲料メーカーの社内システムが、2025年9月29日にサイバー攻撃を受け、10月3日にランサムウェア被害であることを公表しました。情報漏えいの可能性があり、内容や範囲は本文作成時点では調査中となっています。また、国内グループ各社の受注・出荷業務や電子メール受信に影響が出ており、徐々に出荷を再開しています。対応として、商品供給を最優先し、手作業で受注を進め、順次出荷を開始していますが、システム復旧時期は未定で、緊急対策本部を設置し外部専門家と連携中。業績への影響も精査中としてますが、その影響は業界全体に波及しています。

被害の全容

攻撃発生日時：2025年9月29日午前7時頃。
攻撃手法：ロシア系ランサムウェアグループ「Qilin（キリン）」による攻撃。
特徴：
・**二重脅迫（Double Extortion）**：システム暗号化＋盗んだデータ公開の脅し。
・**規制遵守の武器化**：マイナンバー等の個人情報流出を示唆し、法的リスクを利用して圧力を強化。
流出データ：約27GB（9,300件以上のファイル）
財務書類、契約書、従業員個人情報（マイナンバー含む）、開発計画など。

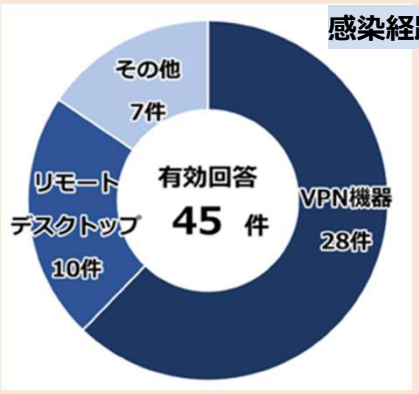
影響範囲：
・国内30工場の大半で生産停止。
・受注・出荷システム全面ダウン、コールセンター停止。
・コンビニ・飲食店で商品不足、サプライチェーン全体に波及。
経済的影響：株価約7%下落、損失は数百億円規模の可能性。
犯行声明：10月7日、Qilinがダークウェブで公開。サンプル画像にマイナンバーコピーなどを含む。

※参照元：該当企業からの正式発表ではなく、新聞各紙の情報を元に抜粋しており、一部専門家やハッカー集団が公表したデータなどからの予想値も含まれます。

オフィス用品通販大手、ランサムウェア被害で全サービス停止、サプライチェーン全体に波及

オフィス用品通販大手を襲ったランサムウェア攻撃の概要と影響

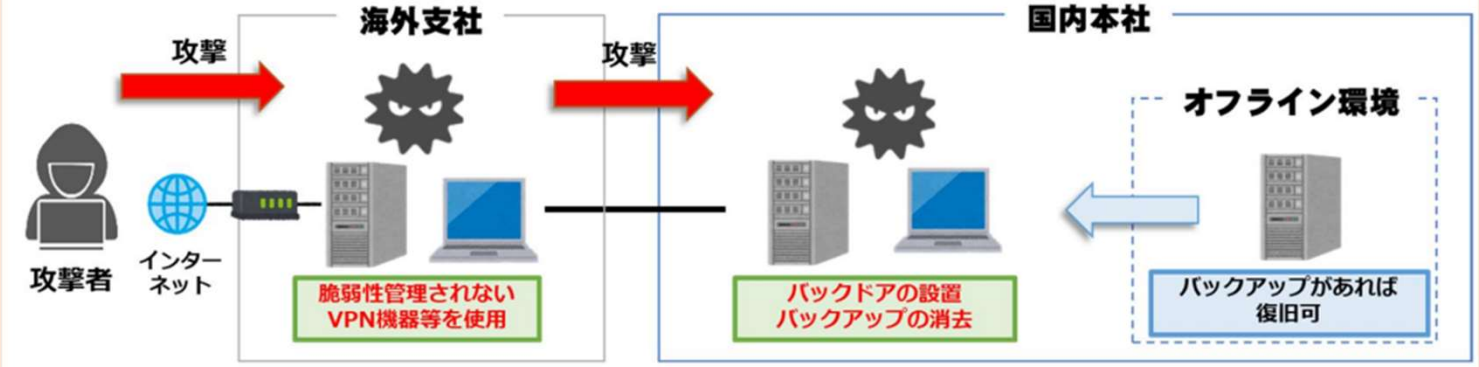
2025年10月19日、オフィス用品通販大手がランサムウェア攻撃を受け、法人向けシステムや個人向けシステムなどの全サービスが停止。注文・出荷業務が全面的に機能不全に陥り、同社の物流を利用していた大手小売企業にも影響が波及した。
攻撃はVPN機器の脆弱性を突いた可能性が高く、基幹システムが暗号化され、業務継続が不可能になった。同社は即座に警察へ通報し、全業務を停止。
復旧作業は続いているが、再開の目処は立っていない。



この事件は、単一企業への攻撃がサプライチェーン全体に波及する**「連鎖的リスク」**の深刻さを浮き彫りにした。特に同社は、複数企業の物流を担う「ハブ」としての役割を果たして、その停止は広範な混乱を招いた。

背景には、**日本企業のセキュリティ体制の脆弱性**や、**VPN機器の管理不備、DX投資の遅れ**などがある。
今後は、**ゼロトラストの導入**、**バックアップ体制の強化**、**サプライチェーン全体のセキュリティ評価**など、包括的な対策が求められる。この事件は、企業が「自社も攻撃される」という前提で備えるべき時代に突入したことを示しており、経営層を含めた全社的なセキュリティ意識の改革が急務である。

VPN やリモートデスクトップ用の機器からの侵入イメージ（例）



参照元：警察庁　令和７年上半期におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/index.html

ランサムウエアはどんなウイルス？　企業で相次ぐ被害

Q　ランサムウエアってどんなウイルスなの？

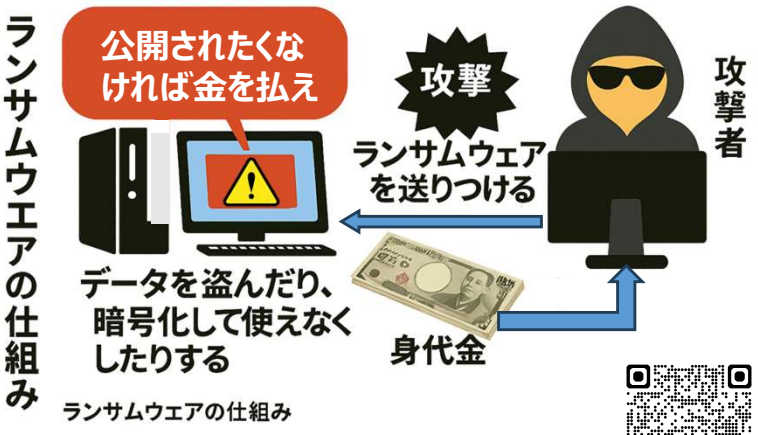
A　ランサムウエアは、パソコンやサーバーに侵入してデータを勝手に暗号化してデータを使えなくし「元に戻したければお金を払え」と脅す、身代金要求型ウイルスのことです。最近は顧客情報などの大事なデータを盗み取ることもあります。

Q　どうして被害が増えているの？

A　生成AI（人工知能）の発展で、それほど専門知識がなくてもサイバー攻撃ができるようになり、手口もどんどん巧妙になっているからです。

Q　復旧にはどれくらい時間がかかるの？

A　東京の調査会社の調べでは、最近は7割の企業が復旧に1週間以上かかっています。1カ月以上かかった会社も12%あり、被害が長引く傾向です。



Q　対策はできないの？

A　「対策を講じても、高度化するサイバー攻撃を完全に防ぐことは困難だ」と専門家は話しています。そのため、バックアップデータを安全に保管したり、初動対応のマニュアルを作ったりして、被害を最小限にすることが大切です。

参照元：毎日新聞 https://mainichi.jp/articles/20251020/k00/00m/040/135000c

令和７年上半期における
サイバー空間をめぐる脅威の情勢等について

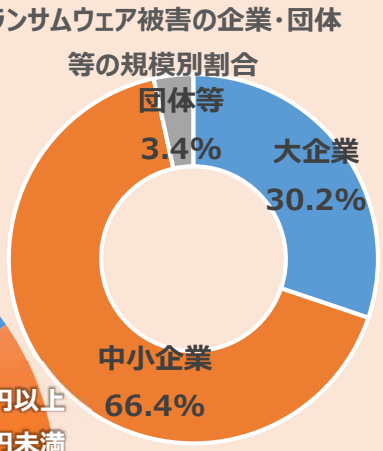
サイバー攻撃は過去最多の水準　復旧費用は被害企業の5割以上で1千万円超え　警察庁調査

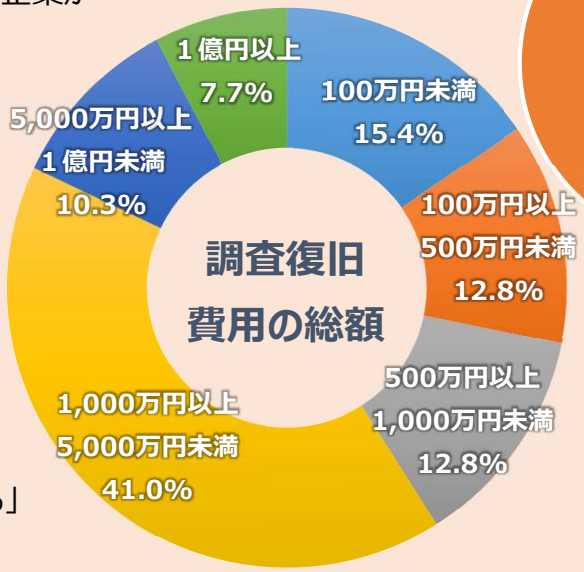
警察庁のまとめでは、復旧費用に1千万円以上を要した企業などの割合が、約59%にのぼることが分かりました。復旧には1週間以上かかるケースが多く、長期化する傾向にあるという。

同庁が今年9月に公表した「令和7年上半期におけるサイバー空間をめぐる脅威の情勢等について」のまとめによると、令和7年上半期の被害報告は116件で、4年下半期と並び最多水準となっています。
ランサムウエアの被害件数は、昨年同様に、中小企業が狙われる状況が続いているということです。

被害に遭った企業・団体等に実施したアンケートでは、昨年と比較してランサムウエアの被害による調査、復旧費用は高額化しています。被害に対して復旧などにかかった期間を尋ねた結果では、「1週間以上」または「復旧中」と回答した企業などが約79%となっています。
復旧費用に関しては、「1千万円以上」と回答した企業などが約59%にのぼっています。

警察庁は「中小企業の被害が増える中で費用負担が増加しており、被害組織の経営に与える影響は決して小さくないと考えられる」ということです。





参照元　https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf

NISTが改定したパスワード新基準
複雑性より長さ、定期変更より侵害時対応へ

新ガイドラインが定めるパスワード要件の概要

新しいガイドラインが定めるパスワード要件の概要は次のとおり。

・パスワードに「複雑さ」(特殊文字、数字など)を強制してはならない
・パスワードの長さは15文字以上とする。ただし、多要素認証(MFA: Multi-Factor Authentication)を併用する場合は8文字以上を許容する。最大長は少なくとも64文字をサポートする
・定期的なパスワードの変更を要求してはならない。ただし、侵害された証拠があれば変更を強制できる
・知識ベース認証(最初のペットの名前は何ですか?など)の使用を求めてはならない
・アカウント回復手段を提供する。具体的には「保存された回復コード」、「発行されたリカバリコード」、「回復連絡先の使用」、「繰り返しの身元確認」のうち1つ以上を提供する。

事業内容 | ニュース
パスワードにはそれほど多くの面倒な文字は必要ない、とNISTは言います

	NIST これまでのパスワードガイドライン	NIST 新しいパスワードガイドライン
パスワードの長さ	8 文字から 16 文字に制限	最大64文字までの長いパスワード
文字の複雑さ	奨励	不要
パスワードの変更が必須	毎月必須	侵害された場合のみ
パスワードブロックリスト	基本用語	侵害されたパスワード、パターン、および一般的なバリエーション
回復方法	セキュリティの質問	リンクと確認コード

※　米国国立標準技術研究所(NIST: National Institute of Standards and Technology)

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年制度開始予定！
経産省のセキュリティ対策評価制度の概要と重要性

- **開催月日 ： 2025年11月19日（水）** （申込締切：11月14日（金）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。

セミナー紹介動画！
https://youtu.be/yaW6yL5oOt8

【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

キヤノンMJ　セミナー　検索

もはや企業の価値は製品やサービスの利便性だけで測られる時代ではありません。
「あの会社は、本当に信頼できるのか？」その問いに客観的な指標で答える新基準、それが経済産業省の『セキュリティ対策評価制度』です。この制度は、自社のセキュリティ対策レベルを客観的に証明し、取引先との信頼関係を円滑にする強力なツールであり、ビジネスの機会損失を防ぐだけではなく、新たな取引を呼び込むきっかけにもなります。５段階の格付けによる証明がサプライチェーンにおける「信頼の証」となり、取引先から選ばれるための条件の一つとなるかもしれません。
本セミナーでは、経済産業省が打ち出す新たなセキュリティ制度『セキュリティ対策評価制度』の本質を読み解き、来年の施行に向けて、必要となる具体的なアクションについて徹底解説します。

＜講師プロフィール＞

**IT・サイバーセキュリティ領域を中心にサイバー演習やIT - BCPに関わるコンサルティング支援に参画。特にサイバーセキュリティ成熟度評価支援やサイバーセキュリティ認証取得支援において多くの実績を持つ。
お客様の課題解決を第一とし、総論ではなく、お客様の実状や組織風土に合った具体的なアクションプランの提示を大切にしている。**

＜講師紹介＞

**ニュートン・コンサルティング株式会社
山中 祥央 氏**

評価制度の開始前から取り組める「SECURITY ACTION宣言」

サプライチェーン強化に向けたセキュリティ対策評価制度が本格的にスタートするのは2026年ですが、外部に向けてセキュリティ基準を示すために、2026年までに取り組み始めることができる「SECURITY ACTION セキュリティ対策自己宣言（以降、SECURITY ACTION宣言）」というものがすでに2017年からスタートしています。

SECURITY ACTION宣言とは？背景や目的

この制度は、経済産業省所管の「IPA（独立行政法人 情報処理推進機構）」が設けた自己宣言制度です。

IPAがセキュリティ基準を認定するものではなく、中小企業自らがセキュリティ対策に取り組むことを宣言することで、国内におけるセキュリティ対策の普及・啓発を図ることが主な目的です。
企業が自社のセキュリティ対策を段階的に向上させるための入口として位置づけられ、セキュリティ対策評価制度は三つ星～五つ星を認定の対象としますが、SECURITY ACTION宣言はその前段階である一つ星～二つ星を補完するもので、三つ星以上と比べて初歩的なもので取り組みやすくなっています。

参照元　https://canon.jp/biz/trend/securityaction