SECURITY TREND NEWS

Vol.04
2026

Hot Topics 2026 Apr.

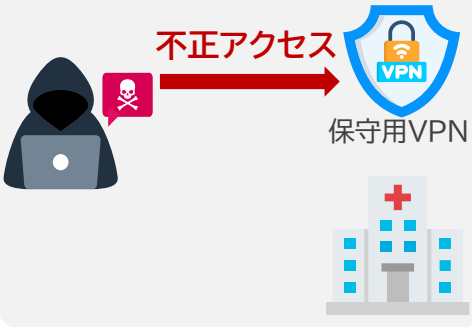
- 武蔵小杉病院　ランサムウェア被害 ― VPN／リモート保守の盲点―
- 最新パスワード指針 ― “長さ”が安全という新常識 ―
- 退職者アカウントのリスク ― 新年度に注意すべき内部不正 ―

Topic 01

武蔵小杉病院のランサムウェア被害

2026年2月、武蔵小杉病院は**医療機器保守用VPNの脆弱性を突かれ、ランサムウェア被害に遭いました。**漏えい規模は当初の1万人から、最終的に13万人へと拡大しています

保守用VPN装置から侵入



二重脅迫型ランサムウェア

被害が拡大しやすい構造

- ■ **VPN／リモート保守経路は最重要リスク**：型落ち機器、初期パスワード、接続制限なしなど
- ■ **狙われる「本番システム」以外**：FAXサーバー、監視カメラ、複合機、ベンダー保守PCなど
- ■ **被害は後から拡大する**：早期検知・遮断ができないと、影響範囲と損害は急速に広がる

Topic 02

＼“長さ”が安全という新常識／

最新パスワード指針

NIST（米国国立標準技術研究所）は2025年以降、「パスワード指針」を改訂し、**複雑さよりも「人が守りやすく、攻撃に強いパスワード」を重視**する方針へ転換しました

新しいパスワードの方針

複雑性の強制は不要

✖ P@ssw0rd!（大文字・小文字・数字・記号）

○ long-horse-battery-staple

長さが最重要

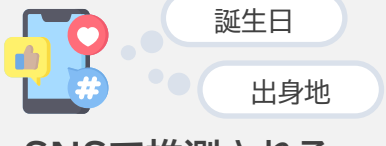
○ パスワード単体：15文字以上

○ MFA（多要素認証）併用：8文字以上

定期変更は不要

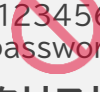
規則性が生まれる

秘密の質問は禁止



SNSで推測される

弱いパスワードを登録させない



ブロックリストで防ぐ

Topic 03

内部不正の実態と退職者アカウントのリスク

内部不正は長年にわたり深刻な脅威とされています。また、上場企業における個人情報漏えい・紛失事故も増加傾向が続いています

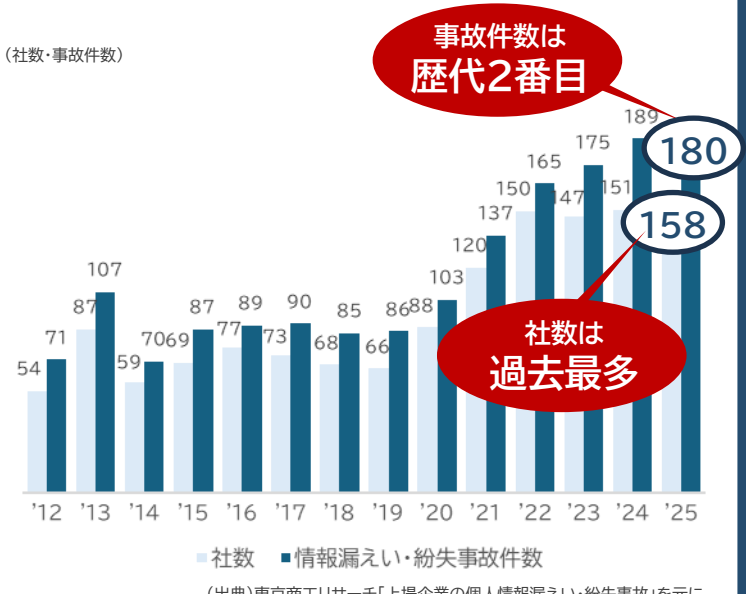
情報セキュリティ10大脅威 2026［組織］

1	ランサム攻撃による被害
2	サプライチェーンや委託先を狙った攻撃
3	AIの利用をめぐるサイバーリスク
4	システムの脆弱性を悪用した攻撃
5	機密情報を狙った標的型攻撃
6	地政学的リスクに起因するサイバー攻撃（情報戦を含む）
7	**内部不正による情報漏えい等**
8	リモートワーク等の環境や仕組みを狙った攻撃
9	DDoS攻撃（分散型サービス妨害攻撃）
10	ビジネスメール詐欺

（出典）独立行政法人情報処理推進機構「情報セキュリティ10大脅威 2026」

11年連続で組織向け脅威にランクイン

上場企業の個人情報漏えい・紛失事故件数



（出典）東京商工リサーチ「上場企業の個人情報漏えい・紛失事故」を元にキヤノンマーケティングジャパン（株）で作成

新年度に増える「退職者アカウントのリスク」

アカウント管理のリスクは、最新の調査でも明らかです。人事異動が集中する**新年度は、異動者・退職者のアカウント管理がより重要になります**

37.3% の企業で退職者アカウントが放置されている（出典1）

88.0% のIT管理者がアカウント管理不備リスクを実感（出典2）

攻撃者に放置アカウントが狙われる理由は…

- パスワード変更が停止
- MFA（多要素認証）が未設定
- 未使用よる発見遅延
- SaaS・クラウドの権限が残存
- 退職者による不正持ち出し

事例1　元従業員による不正アクセス

元従業員 → 顧客リストへ不正アクセス → 競合他社へ持ち出し

事例2　削除漏れアカウントが突破口

攻撃者 → 削除漏れアカウント → 内部システムへ不正侵入

（出典1）㈱アクト「企業セキュリティ国勢調査2025」　（出典2）ソニービズネットワークス㈱「SaaS管理不備によるセキュリティリスクに関する実態調査」

無料オンラインセミナー開催のご案内

サプライチェーンの関係者はどう見ている？

リサーチで読み解く「セキュリティ対策評価制度」と現実的な備え方

参加無料
事前登録制

日時
2026年
5月27日(水)
14:00-15:00

●定員：300名
●対象：経営層・ご担当者様
●申込締切：2026年5月22日(金)
■インターネット環境があれば自席で受講いただけます

セミナー概要

セキュリティ対策評価制度は、サプライチェーンに関わる多くの発注企業・受注企業に影響を与える重要な制度です。本ウェビナーでは、制度の基本的な考え方を分かりやすく整理するとともに、サプライチェーン企業が抱える制度への不安や課題について、最新のリサーチ結果をもとに読み解きます。あわせて、今後の制度活用の方向性を見据えながら、企業として今から準備すべきポイントや、現実的かつ実践的な対応策をご紹介します。

講師

キヤノンITソリューションズ株式会社
先進セキュリティ技術部 アセスメント課

中濱 禎夫

＜講師　プロフィール＞
アンチウイルスソフトウェアの製品開発を起点に、長年にわたり情報セキュリティ分野に従事。セキュリティ製品開発の経験を基盤に、近年はWebメディアを通じた情報発信や、社内外に向けたセキュリティ教育・啓発活動にも取り組む。2025年より、これまでの知見を活かし、セキュリティ診断業務に参画。
情報処理安全確保支援士

■セミナー申込サイト

キヤノンMJ　セミナー　検索

WEBサイト：https://canon.jp/biz/event

※お申込みの際に
【会社コード】の入力が必要です。
【会社コード】G03867

■セミナー紹介動画

セミナーの概要を3分でご紹介しています！