

この10日間で、何が起きたか

2026年秋、国内で大規模インシデントの公表が立て続けに起きています

10日間で5件 – 2026年秋の公表

赤＝委託先・外部サービスが起点の事案



侵害はどこで起きたか – 6件中4件は従来の防御が見ていなかった場所

大和証券

侵害箇所 委託先のサーバー

補足情報 スカラコミュニケーションズ

大東ガス ほか8組織

侵害箇所 委託先のIT企業

補足情報 両毛システムズ / VPN悪用

日本経済新聞社

侵害箇所 業務用クラウド

補足情報 Microsoft 365アカウント

第一生命

侵害箇所 社内の人事システム

補足情報 顧客システムとは別系統

タイムズモビリティ

侵害箇所 調査中

補足情報 侵入経路は未公表

京王電鉄グループ

侵害箇所 調査中

補足情報 漏えいは未確認

赤＝自社が直接管理していない場所、または自社の防御の想定外にあった場所

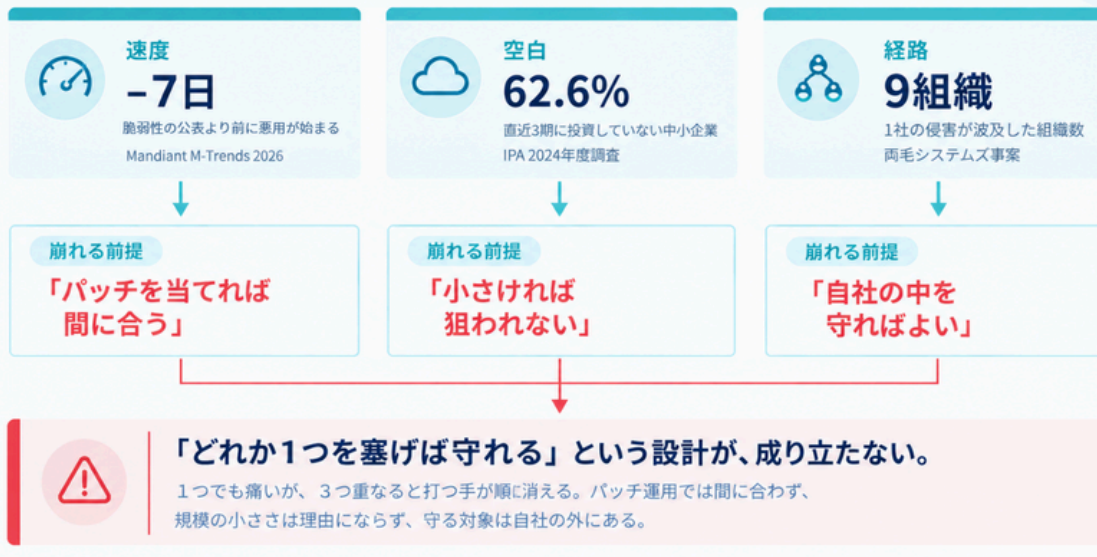
「自社が狙われているか」より、「自社が何とつながっているか」

2026年秋の6件のうち4件は、従来の防御が見ていなかった場所で起きています。御社の場合、どこまで把握できていますか。

一緒に確認したい、3つの問い

守り方の前提が、3つとも外れている

3つは独立に効く。掛け合わせるのではなく、別々の前提をひとつずつ崩している



Q1 公開資産・SaaS・委託先の一覧は、すぐ出せますか

「どこに、誰の、どんな個人情報があるか」が答えられない状態では、侵害が起きたときに公表することができません。2026年秋の事案の多くは、自社が直接管理していない場所で起きています。

Q2 VPN・管理画面の多要素認証は、は、すべて有効になっていますか

委託先IT企業の事案はVPNアカウントの悪用、新聞社の事案は業務用クラウドアカウントの乗っ取りが起点でした。退職者・不要アカウントの棚卸しもあわせて。

Q3 委託先との契約に、インシデント報告の義務と期限は書いてありますか

自社の防御水準は、自社の投資額だけでは決まりません。つながっている組織のうち最も弱いところの水準に引き下げられます。取引先への要請は、自社防御の一部です。

出典 各社公表資料（タイムズモビリティ／パーク24・京王電鉄・第一ライフグループ／第一生命保険・日本経済新聞社・大和証券・スカラコミュニケーションズ・シチズン時計・損害保険ジャパン・東武鉄道・両毛システムズ／長野都市ガス）／Mandiant「M-Trends 2026」／Google Threat Intelligence Group（2026/9/30）／Unit 42（2026/9/2）／Cisco Talos（2026/9/17）／IPA「2024年度 中小企業における情報セキュリティ対策に関する実態調査」／ESRB・英AI Security Institute。記載の数値は2026年10月時点のものです。

※ 本資料は公表済みの一次情報をもとに当社が作成したものです。当社はWAF（SiteGuardシリーズ）、脆弱性診断、セキュリティ監視等のサービスを提供しています。なお「AIが被害増の原因」であることを定量的に示した統計は現時点では存在せず、本資料は両者が同時進行していることを示すにとどめます。