2025年

Cyber Security News

7 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

止まらぬランサムウェア被害、情報漏洩の危機！

次の標的は、ウチは関係ないという御社かも？

近畿限定

不正アクセス/ランサム攻撃の猛威が継続・・・近畿地区での被害報告多数

■2025年5-6月でのサイバー攻撃被害報告（近畿地区）を一部抜粋

日本各地、近畿地区でもランサムウェア攻撃を含む多くのサイバー攻撃被害報告が相次いでいます。
影響は企業だけでなく、警察や学校にも及んでおり、業界を問わず警戒が必要な状況です。
過去のIPAの調査では、**約60%の企業が被害を公表しない**とも回答しており、更に潜在している被害もあると思われます。

CAUTION

各種NEWS素材及び各企業のHP掲載内容から抜粋。公表された情報のみを掲載しています。

業種概要	都道府県	今年5－6月の公表被害内容
産業機器製造	大阪	ランサムウェア感染、情報漏洩の可能性
空港運営	大阪	法人向けサービス不正アクセス、1万件情報漏洩
鉄鋼製造	大阪	ランサムウェア感染、ファイル暗号化
学校	大阪	ランサムウェア感染、個人情報漏洩
警察	大阪	偽装サイト複数見つかる
医療機器卸	京都	ランサムウェア感染
医療用品卸	京都	ランサムウェア感染
建材製造卸	兵庫	ランサムウェア感染、ファイル暗号化
建設	兵庫	ランサムウェア感染、顧客情報漏洩
福祉用品レンタル	兵庫	ランサムウェア感染
県関連施設	滋賀	不正アクセス、ネットワークサービス停止
家具製造小売	和歌山	ECサイトに不正アクセス

委託先リスク管理の実態調査【2025年度版】

委託先リスク管理の担当者300名を対象として、委託先リスク管理の実態調査（株式会社アトミテック）が発表されました。

SUMMARY

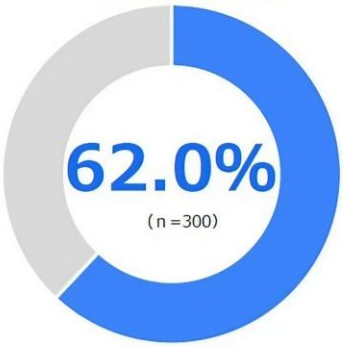
「株式会社アトミテック　委託先リスク管理の実態調査」
URL: https://atomitech.jp/vendortrustlink/vendormaterial/vendor_risk_management_research/

- 5年以内の委託先でのインシデント発生率は、**62.0%と昨年（66.0%）同様、6割越え**
- 2024年に中小企業へのランサムウェア攻撃が増加したことを受け、委託先のリスク評価の見直しを行ったのは7割弱。**31.3%**の企業が見直しを行っていない結果に

5年以内のインシデント発生率

5年以内の委託先におけるインシデント発生率は62.0%となっており、多くの企業が何かしらの委託先にまつわるインシデントを経験しています。内容としては納期遅れが最も多くなっていますが、**個人情報の漏洩・機密情報の漏洩もそれぞれ20%弱**となっており、対策が必要なことがわかります。

5年以内に委託先で何らかのインシデントを経験



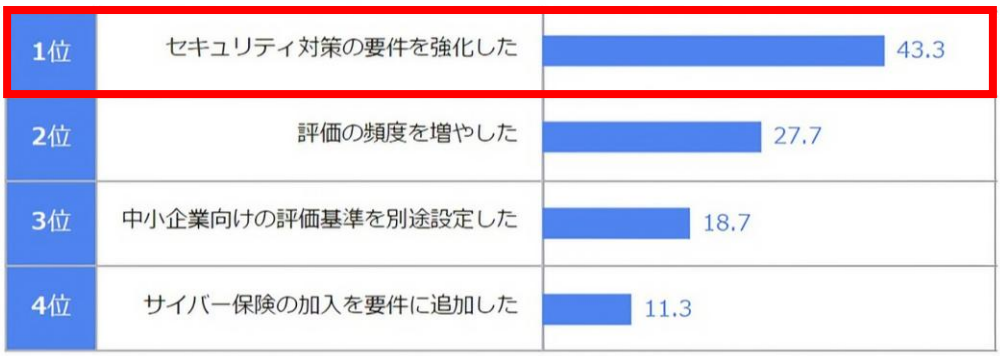
インシデントの内容

ランサムウェア攻撃増加の影響

2024年には**中小企業を標的としたランサムウェア攻撃が増加し、委託元企業にも影響**が及んでいます。それを受けて**委託先のリスク評価の見直しを行ったのは7割弱**。見直した点としては、**セキュリティ対策要件の強化（43.3%）**、評価の頻度増加（27.7%）が多かったようです。反面、31.3%は特に見直しを行っていないという結果になっています。

特に見直しはしていない

見直した点



日本のサイバー被害、半数が「取引先経由」という調査も・・・

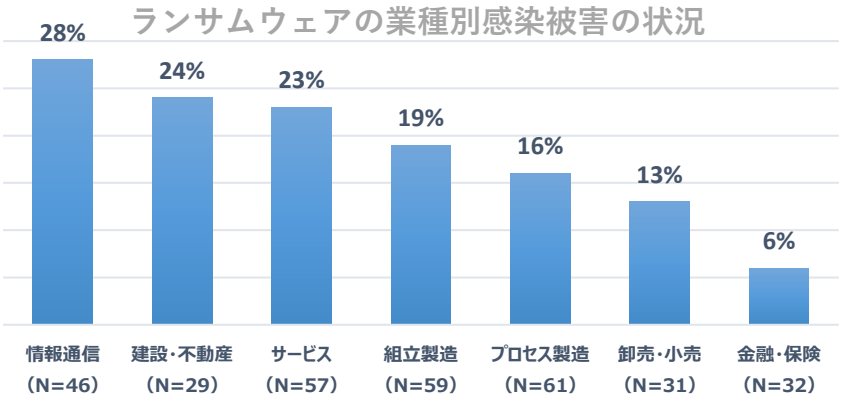
（米SecurityScorecard社調査）

ランサムウェア感染から完全復旧できない企業が7割に上る

サイバー攻撃を前提としたバックアップデータ保護と迅速な復旧の仕組みが重要に

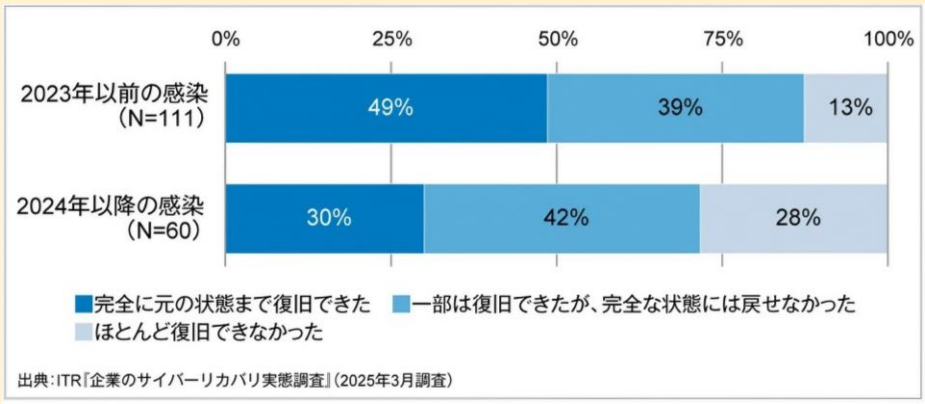
市場調査会社ITRが6月4日に発表した「企業のサイバーリカバリ実態調査」の結果、2024年以降の約1年の間でランサムウェアの被害に遭った国内企業のうち、**7割の企業**が完全にはシステムを**復旧できていない**ことが明らかになりました。

この調査で業種別の感染被害状況をみると、2024年以降は、情報通信の感染率が28%と最も高く、建設・不動産（24%）、サービス（23%）と続いています。2023年以前は、卸売・小売（52%）やプロセス製造（43%）の感染率が非常に高かったものの、被害は落ち着いています。これらの業種は特に攻撃への注意が必要と考えられます。



出典：ITR「企業のサイバーリカバリ実態調査」（2025年3月調査）より

ランサムウェア感染からのシステム復旧状況

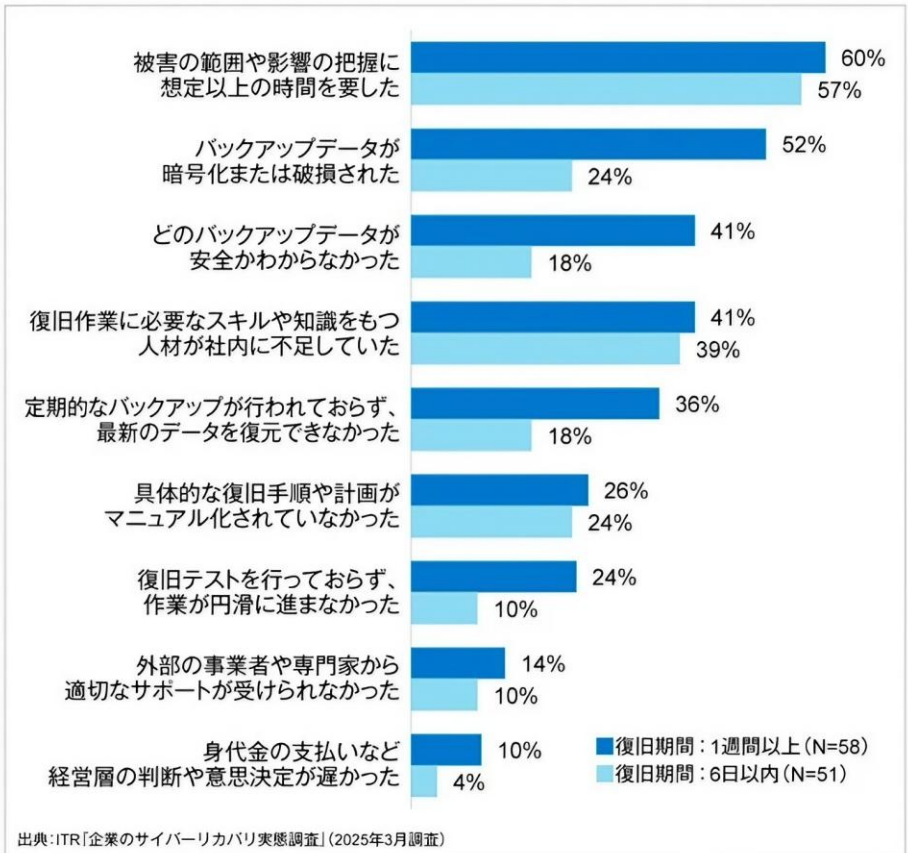


出典：ITR『企業のサイバーリカバリ実態調査』（2025年3月調査）

ランサムウェアの感染経験がある企業に対し、システムの復旧状態を調査したところ、2023年以前は49%とほぼ半数の企業が完全復旧できたのに対し、2024年以降は30%にまで減少しています。一方、「ほとんど復旧できなかった」企業は、2023年以前の13%から、2024年以降は28%に倍増しました。「一部は復旧できたが、完全な状態には戻せなかった」企業を含めると、**2024年以降は完全復旧できなかった企業が70%に上ります。**

ランサムウェア感染からシステムの復旧までに生じた問題

復旧に1週間以上を要した企業が7割、迅速な被害把握と初動対応が重要な課題



出典：ITR「企業のサイバーリカバリ実態調査」（2025年3月調査）

復旧までの過程で企業が直面した問題としては、「被害の範囲や影響の把握に**想定以上の時間を要した**」が最も多く、復旧に1週間以上かかった企業の60%、6日以内の企業でも57%がこれをあげています。また、「**どのバックアップデータが安全かわからなかった**」との回答も、特に復旧に1週間以上かかった企業に多くみられました。ランサムウェア感染時には、まずデータの被害範囲と感染していない安全なデータを早急に把握することが重要ですが、多くの企業はその初動対応に時間を要していることがわかりました。さらに、「復旧作業に必要なスキルや知識をもつ人材が社内に不足していた」との回答も多く、専門スキルをもつ人材の不足も課題となっています。

出典元　株式会社アイ・ティ・アール（ITR）
：「企業のサイバーリカバリ実態調査」
https://www.itr.co.jp/topics/pr-20250604-1

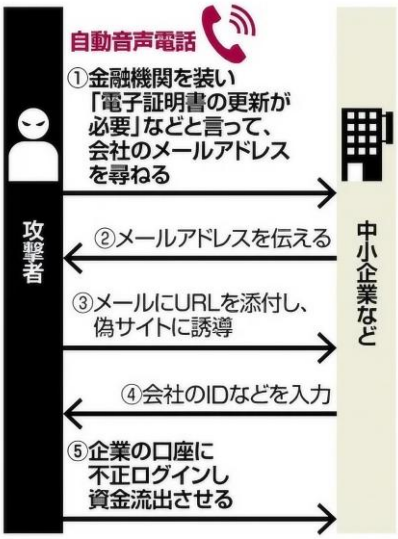
中小企業狙う「ボイスフィッシング」、金融機関装う電話で「偽サイト」誘導…不正送金被害２８億円

金融機関を装って企業に電話をかけて偽サイトに誘導し、法人口座の情報を盗み取る「ボイスフィッシング」の被害が昨年11月以降、４月末までに**国内約80社**に上り、**計約28億円が不正送金されていた**ことが、警察庁の調べで明らかになりました。個人口座に比べ、１日の**送金限度額が高く設定されている法人口座が狙われている**とみられ、各地の警察が捜査しているということです。

ボイスフィッシング（ビッシング）は、電話をかけて音声（ボイス）で偽サイトに誘導し、ＩＤやパスワードを入力させて盗み取る「フィッシング詐欺」の一種ですが、警察庁によると**主に中小企業が狙われており**、タクシーや不動産、食品、電子機器メーカーなど業種は様々。

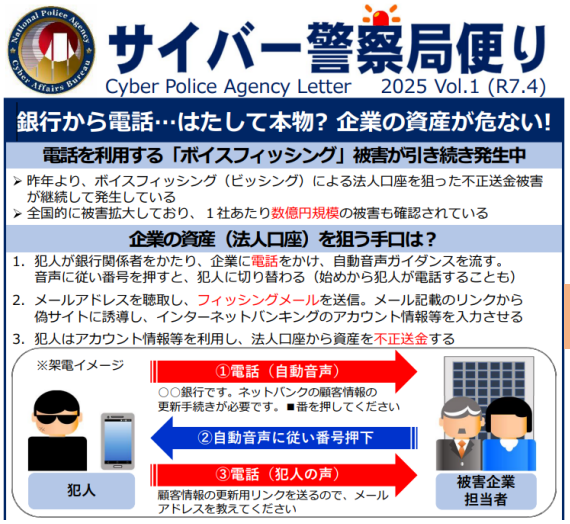
地方銀行や信用金庫、大手銀行を装い、「電子証明書の更新が必要」などと自動音声の電話をかけてくるのが特徴となっています。

国際電話番号からの着信が目立ち、警察当局は、海外の犯罪組織が**日本の中小企業を標的にしている**とみているそうです。



参照元：読売新聞オンライン
https://www.yomiuri.co.jp/national/20250531-OYT1T50100/

下図：サイバー警察局便り（警察庁から昨年末から2度も注意喚起）
https://www.npa.go.jp/bureau/cyber/index.html



相次ぐボイスフィッシング被害、AI利用で脅威が加速

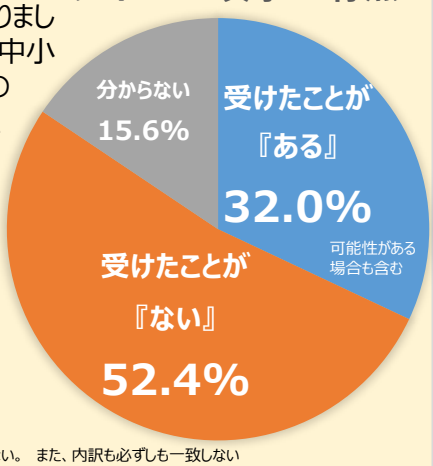
山形鉄道が山形銀行を装う偽の自動音声電話にだまされ、約1億円の不正送金被害を出した事件以外にも様々な金融機関を偽った被害報告が相次いでいます。**社長の声をAI（人工知能）に学習させた偽電話**など、新たな手法も登場しているということです。

サイバー攻撃に関する実態調査（2025年）帝国データバンク調べ

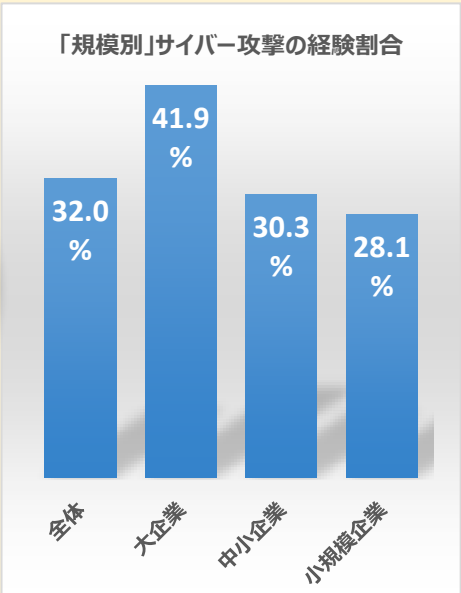
サイバー攻撃　企業の32.0%で経験あり　大企業への攻撃目立つ ～直近で中小企業の被害が急拡大～

帝国データバンクの調査によると、3割を超える企業がサイバー攻撃を受けたことがあると分かりました。最近では、大企業と比べて対策が手薄な中小企業での被害が増加しているという。警察庁の調査によると、2024年の中小企業のランサムウェア被害件数は2023年より37%増加。帝国データバンクは、サイバー攻撃を人ごとと捉えず、BCP（事業継続計画）の一環として対策を整備していくことが重要だとしています。

サイバー攻撃の有無



「規模別」サイバー攻撃の経験割合



※株式会社帝国データバンク、全国2万6,389社を対象にした「サイバー攻撃」に関するアンケート調査より
調査期間：2025年5月19日～5月31日（インターネット調査）
調査対象：全国2万6,389社、有効回答企業数は1万645社

注1：母数は、有効回答企業1万645社
注2：小数点以下第2位を四捨五入しているため、合計は必ずしも100とはならない。 また、内訳も必ずしも一致しない

参照元：株式会社帝国データバンク
https://www.tdb.co.jp/report/economic/20250619-2025cyber-attack/