2025年

Cyber Security News

4 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

警察庁発表：サイバー空間をめぐる脅威の情勢等

BCP「ランサム想定」 途上
被害企業5割「復旧に1カ月超」 事前策定で早期回復も

警察庁は3月13日、24年のサイバー空間をめぐる脅威情勢を公表しました。

【概要】

■2024年にランサムウェア被害を受けた企業・団体のうち、約50%が復旧に1カ月以上。
■特に、1カ月以上かつ1千万円以上の費用がかかったケースが多い。
■サイバー攻撃を想定した事業継続計画（BCP）を策定していない企業ほど影響が長期化する傾向。

【事業継続計画（BCP）の策定状況】

■サイバー攻撃を想定したBCPを策定していた企業・団体は全体の約31%。
■BCPを策定していた企業は早期復旧に成功する傾向がある。

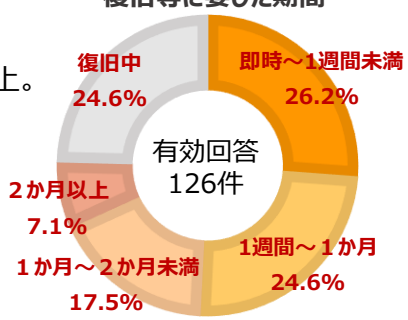
【費用と影響】

■復旧にかかった費用が1億円以上のケースもあり、事業への影響が大きい。
■早期復旧が事業への影響を最小限に抑えるために重要であることが強調されています。

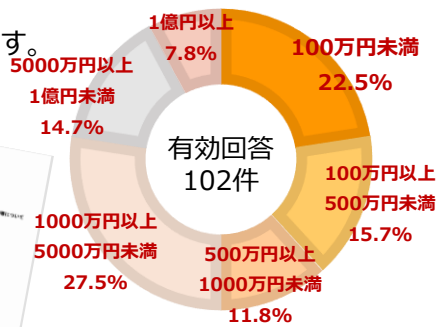
【対策と教訓】

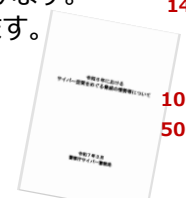
■事前にBCPを策定し、サイバー攻撃に備えることの重要性が指摘されています。
■警察庁は企業に対し、サイバー攻撃を想定したBCPの策定を促しています。

復旧等に要した期間



調査費用の総額





参照元：日本経済新聞2025年3月14日朝刊043P より抜粋
警察庁発表資料より、グラフ作図

参照元 警察庁：https://www.npa.go.jp/publications/statistics/cybersecurity/

改めて問われるIT-BCP

IT-BCP（IT事業継続計画）とは、災害や予期せぬ事態が発生した場合に、重要なITサービスや業務を中断させずに継続するための計画で、BCP対策の重要な一つとなっています。

中小企業庁「事業継続力強化計画」認定制度の中でも重要項目

中小企業庁「事業継続力強化計画」とは？

中小企業が自社の災害リスクを認識し、防災・減災対策の第一歩として取り組むために、必要な項目を盛り込んでおり、将来的に行う災害対策などを記載するものです。認定を受けた中小企業は、金融支援や、税制支援などの様々な支援策が受けられます。

53,053件の計画が認定取得　（2023年3月末時点）

参照元：独立行政法人 中小企業基盤整備機構
https://kyoujinnka.smrj.go.jp/

初めてのサイバーセキュリティ対策はここから

■情報セキュリティ５か条
■5分でできる！情報セキュリティ自社診断
■セキュリティインシデント対応の手引き　　等

参照元：独立行政法人情報処理推進機構（IPA）

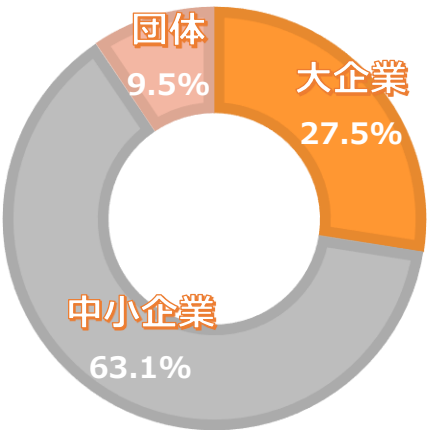
警察庁が2024年のサイバー犯罪統計を発表
中小企業のランサム被害件数は37%増

警察庁
National Police Agency

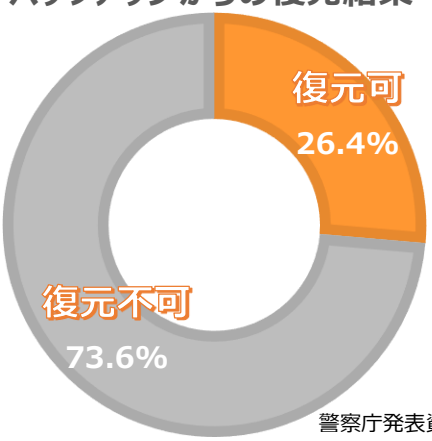
警察庁は2025年3月13日、2024年のサイバー犯罪に関する被害状況などをまとめたリポート「令和6年におけるサイバー空間をめぐる脅威の情勢等について」を発表しました。リポートでは、2024年におけるランサムウエア被害件数が222件と2023年に続き高水準で推移していると報告。また**2024年の特徴として、大企業のランサムウエア被害件数は2023年より減少した一方、中小企業のランサムウエア被害件数は37%増加**したという。

警察庁は原因として、ランサムウエア攻撃用のクラウドサービスであるRaaS（ランサムウエア・アズ・ア・サービス）が普及したためと推定しています。技術的な知識が少なくてもランサムウエアを手に入れて攻撃しやすくなったことで、結果的に攻撃の裾野が広がり、対策が比較的手薄な中小企業で被害が特に増加したとの見方を示しています。

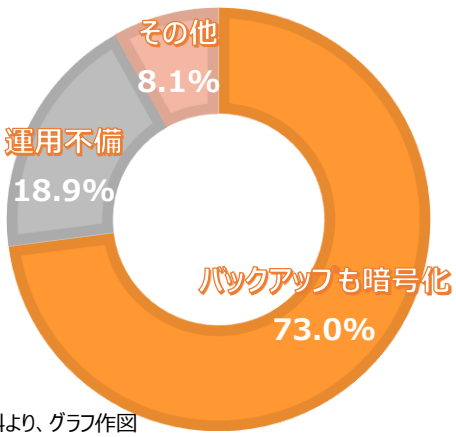
被害企業の規模別割合



バックアップからの復元結果



バックアップから復元できなかった理由



警察庁発表資料より、グラフ作図

参照元　警察庁：https://www.npa.go.jp/publications/statistics/cybersecurity/

警察庁発表：地政学的リスクについても具体例が掲載

国家の関与が疑われるサイバー攻撃には、軍事技術や国の機密情報の搾取を狙ったものが挙げられます。これは企業の競争力を損ない、経済安全保障に重大な影響を与える可能性があります。例えば、令和元年頃から日本国内のシンクタンクや政府関係者に対し、MirrorFaceというグループが情報窃取を目的とした攻撃を行っており、中国の関与が疑われています。

また、暗号資産の窃取を目的とする攻撃もあります。令和6年3月、国連の専門家パネルは北朝鮮が関与する暗号資産関連事業者への攻撃を調査し、北朝鮮の外貨収入の約半数がサイバー攻撃によるものであると公表しました。日本でも、令和6年5月にTraderTraitorというグループが約482億円相当の暗号資産を窃取しました。

さらに、重要インフラの機能停止を狙った攻撃もあります。令和4年5月には、ロシアがウクライナ侵略の際に国際衛星通信への攻撃を行い、欧州全域に影響を与えました。令和6年2月には、米国の重要インフラ事業者への侵害が確認され、中国のVolt Typhoonというグループによる攻撃が指摘されています。このグループは高度な検知回避能力を持ち、正規の管理ツールを用いるため検知が難しいとされています。

令和7年1月、警察庁は、MirrorFace と呼称されるサイバー攻撃グループが、令和元年頃から国内の組織、事業者及び個人に対して、マルウェアを添付したメールの送信や、ソフトウェアのぜい弱性を悪用した標的ネットワーク内への侵入により、情報窃取を目的としたサイバー攻撃を行っていることを確認。さらに、これら攻撃が、中国の関与が疑われる組織的なサイバー攻撃活動であると評価し、同グループの手口や未然防止対策等に関する注意喚起を実施しています。

令和6年12月、警察庁は、米国連邦捜査局（FBI）及び米国国防省サイバー犯罪センター（DC3）とともに、北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」が暗号資産関連事業者から暗号資産を窃取したことを特定し、合同で文書を発出。

また、関係省庁との連名でTrader Traitor の手口等に関する注意喚起を実施しています。

参照元　警察庁：https://www.npa.go.jp/publications/statistics/cybersecurity/

企業の45%が生成AIを利用、日常業務では80%超の企業が利用成果を認識

現在、生成AIへの関心が非常に高まっています。生成AIの利用状況について質問したところ、「全社的に利用が推奨され、幅広い業務で利用されている」が15.9%、「必要性の高い特定部門での利用に限定されている」が29.1%となり、合わせて45.0%の企業がすでに生成AIを利用している状況にあります。また、「一部のプロジェクトやチームで試験的に利用され、効果を検証している」は26.3%となり、生成AIを利用する企業がさらに増えていくとみられます。

参照：一般財団法人日本情報経済社会推進協会/株式会社アイ・ティ・アール『企業IT利活用動向調査2025』

1. 45%の企業が生成AIを利用。電子メールや資料作成など、日常業務の利用では80%超が効果を認識している。

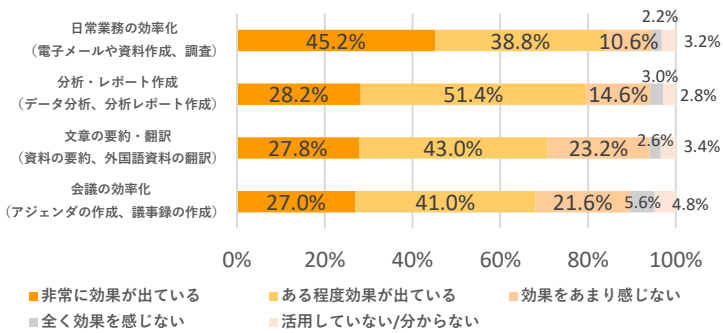


図1.業務における生成AIの活用効果より抜粋/グラフ作図

2. 生成AI利用のリスクとして、機密情報の漏えいとハルシネーション倫理的問題が懸念されている

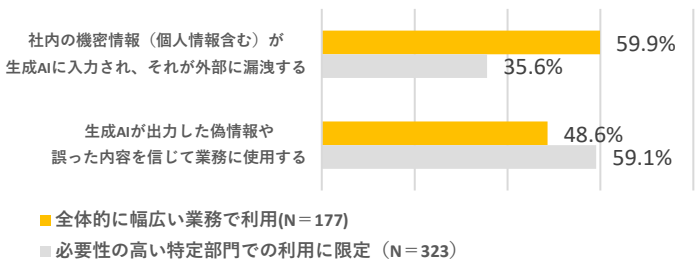
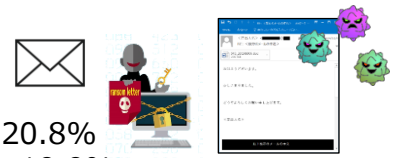


図2．生成AIの利用におけるセキュリティ／プライバシー上の懸念点より抜粋/グラフ作図

3. ランサムウェア感染経験は48%、メールによる攻撃とリモートアクセスの脆弱性が主な侵入経路

国内で拡大しているランサムウェア攻撃による感染被害の経験について、**48.0%がランサムウェアの感染経験がある**ことが分かりました。うち**約半数が身代金を支払った**としており、全体の23.8%となりました。また、**システムやデータを復旧できなかった企業は25.9%**となり、**半数以上が復旧できておらず、ランサムウェアに感染してしまうと、システムの復旧が難しい**ことが分かりました。

【ランサムウェアの侵入経路】
1位　メールやその添付ファイル：28.3%
2位　VPNやネットワーク機器の脆弱性：20.8%
3位　リモートデスクトッププロトコルの悪用：19.9%



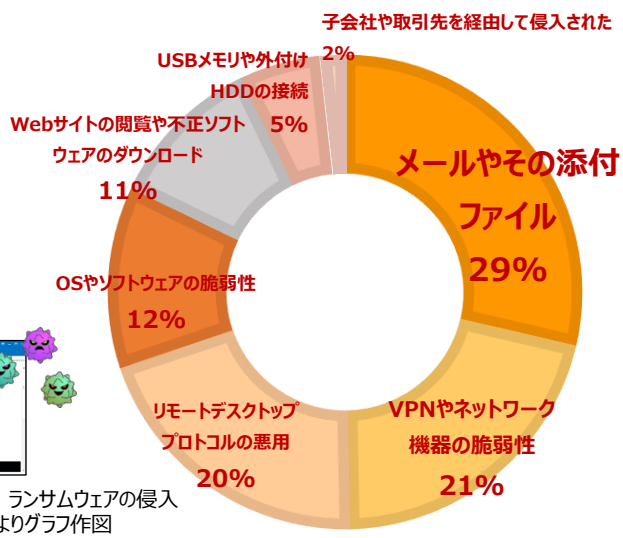


図3．ランサムウェアの侵入経路よりグラフ作図

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。

2025年 改正育児・介護休業法実務対応セミナー
～柔軟な働き方への対応～

- **開催日　：　5月27日（金）（申込締切日：5月22日（木）まで）**
- **開催時間　：　14：00～15：00**
- **会場　：　オンラインセミナー会場**
  開催日前日にZoom視聴用URLをご案内いたします。
- **お申込み　：　下記URLより事前登録願います**
  https://canon.jp/biz/event
  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/EzIDM0yRFs8

キヤノンMJ　セミナー　検索

【セミナー概要】
2025年4月及び10月の二段階で行われる改正育児・介護休業法ですが、
10月の改正は新たな制度設計が必要になり、4月に比べ、
より実務上の注意点や自社の状況を踏まえたうえでの検討が重要です。
しかし、人事部門はやるべきことが多岐にわたり、足元の業務で手一杯で、
情報収集にお困りの方も多いのではないでしょうか？
本セミナーでは、社会保険労務士による、10月改正に向けた実務上のポイントについてお話しします。

是非この機会にご参加ください。

講師紹介：　アクタス社会保険労務士法人　代表社員
特定社会保険労務士　　松澤　隆志 氏

【松澤　隆志 氏　略歴】
社労士事務所での勤務経験、東証プライム上場企業の人事部長職を経て現職。
社会保険労務士として多くの中小企業の労務管理に携わり、個社ごとの事情に応じた現実的なアドバイスに定評があります。

いよいよ開幕！　大阪・関西万博
EXPO2025
2025/4/13 - 2025/10/13

OSAKA, KANSAI, JAPAN EXPO 2025
ぜんぶのいのちと、ワクワクする未来へ。
Towards a brighter future for all
開催期間 2025年4月13日(日)－10月13日(月) Period Sunday, 13 April to Monday, 13 October 2025
開催場所 大阪　夢洲（ゆめしま） Venue Yumeshima Island, Osaka City

2025年は、**大阪・関西万博**が開かれ、関西や大阪が世界的に有名になり、名前を売ろうとするグループが、サイバー攻撃を仕掛ける可能性が高まると懸念されており、地政学的リスクの高まりからも注意が必要です。

【想定されるサイバー攻撃の脅威】
①DDos攻撃
②ランサムウェア
③偽情報（フィッシング、悪質ECサイト）
既に、万博の公式アカウントを装う偽アカウントが確認されたと発表されています。