Canon

2024年

Cyber Security NEWS 8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

業務委託先や子会社への不正アクセスによる被害が広がっています

出版会社、情報処理サービス、ガス会社、税理士・会計・・・ 業種問わず

業務委託先や、子会社などへのランサムウエア、不正アクセスによる情報漏えい被害広がる

大手メディア企業がランサムウェア攻撃にさらされた一件は、日本中にサイバーテロの脅威を改めて知らしめたと言えます。2024年6月、同企業へのランサムウェア攻撃が明らかになり、2か月近く経過した現在（編集時）でも、まだ完全復旧には至っていません。攻撃者は、子会社が運営する動画配信などのサービスを停止させ、データを暗号化しました。さらに、**盗んだデータを**ダークウェブ上に**公開**すると**脅迫**しています。このように被害企業の関係者のデータを公開して関心を高める**「劇場型」**と言われる手口が増えており、犯行の狡猾（こうかつ）さが増し、**被害金額も増加**しています。

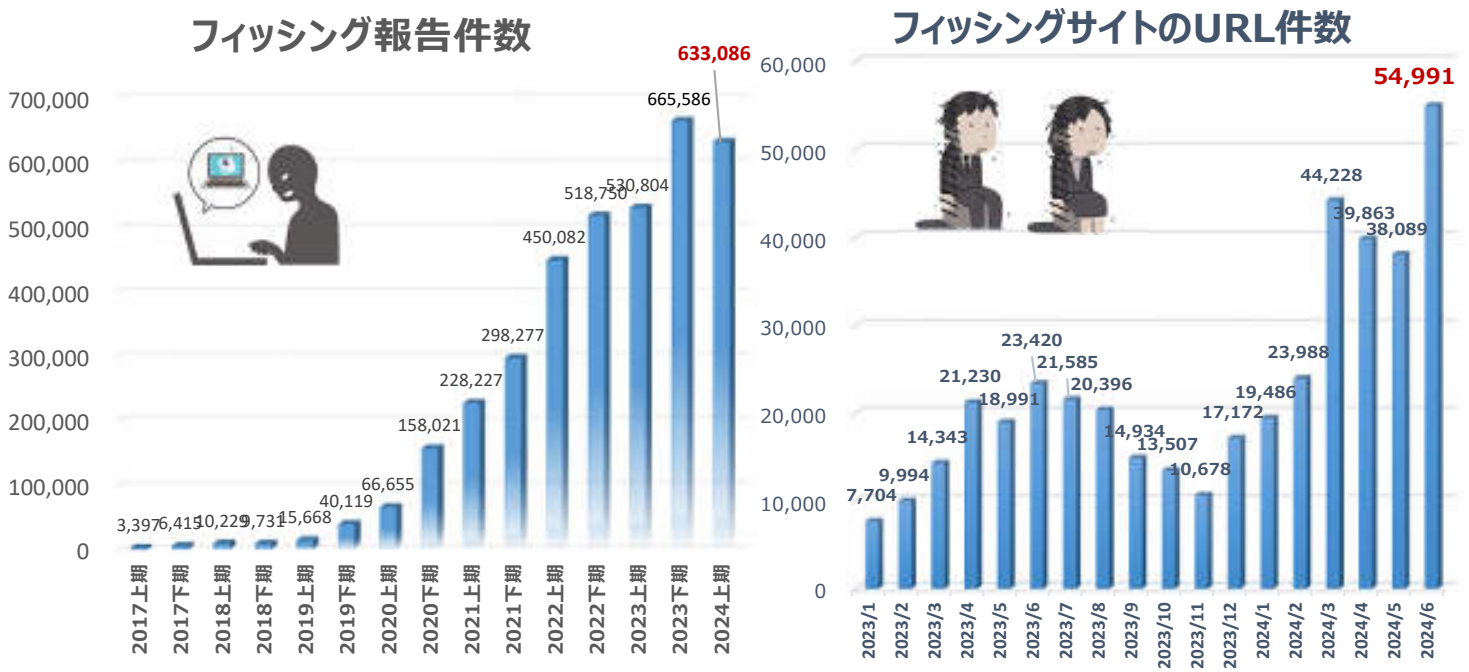
被害を受けた企業が加害者になるケースも・・・

ランサムウエア、不正アクセスを受けた情報漏えい元	漏えい元への業務委託などで情報漏えいの被害を受けた企業	漏えいの可能性が指摘される規模
税理士・会計法人	銀行×1、保険会社グループ×4、学会×1	約9万件以上の個人情報
大手ガスの子会社	奈良市、神奈川県、熊本市、福岡市、宇部市、都市づくり公社、由利本荘市、静岡、千葉など	416万人の個人情報
情報処理サービス会社	全国の銀行・信用金庫×16、生命保険会社×4 全国の府・県・市・区×19、その他教育機関他×7	約150万人の個人情報

上記のほか、**大阪**の理美容・医療機器メーカーの海外向けウェブサイトのサーバがフィッシングメール送信の踏み台になるケースも発生するなど、被害を受けた企業が逆に加害者となるケースも増えています。サプライチェーンのチェックも重要です。

※各種NEWS素材及び各企業のHP掲載内容から抜粋。公表された情報を基に掲載しており、特定の企業を誹謗中傷するものではありません。

6月のフィッシング、URL件数が過去最多を更新



※ グラフはフィッシング対策協議会統計データより作成 https://www.antiphishing.jp/report/monthly/202406.html

表紙のページで紹介した被害企業に追い打ちをかけるように、「漏えいした個人情報を削除したければ、カネ振り込め」とサイバー攻撃の被害者を狙う悪質メールが相次いでいるという記事もでています。また、企業へのサイバー攻撃によって大量の個人情報漏えい事件が相次ぐなか、被害者とみられる人に対し、弁護士を騙る悪質なメールを送る事例を複数確認したとして、警視庁生活安全部が、X（旧Twitter）で注意を呼び掛けています。

【注意！】
《企業へのサイバー攻撃で個人情報が流出したと思われる方々に対し、弁護士等になりすまし、「流出した情報を削除してほしい方は、口座に金を振り込んでください」という嘘のメールが送られている状況を複数把握しました。こういう悪質なかたりには、気をつけてください！》

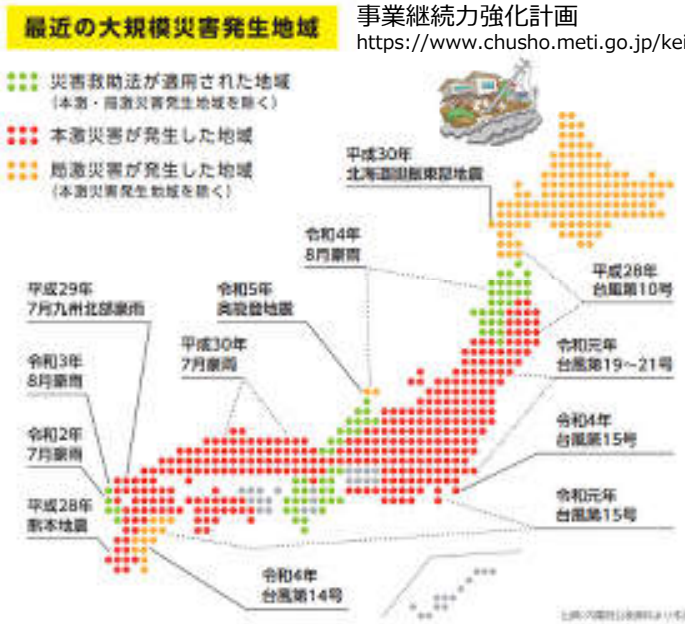
※警視庁生活安全部の「X」より、文面を抜粋

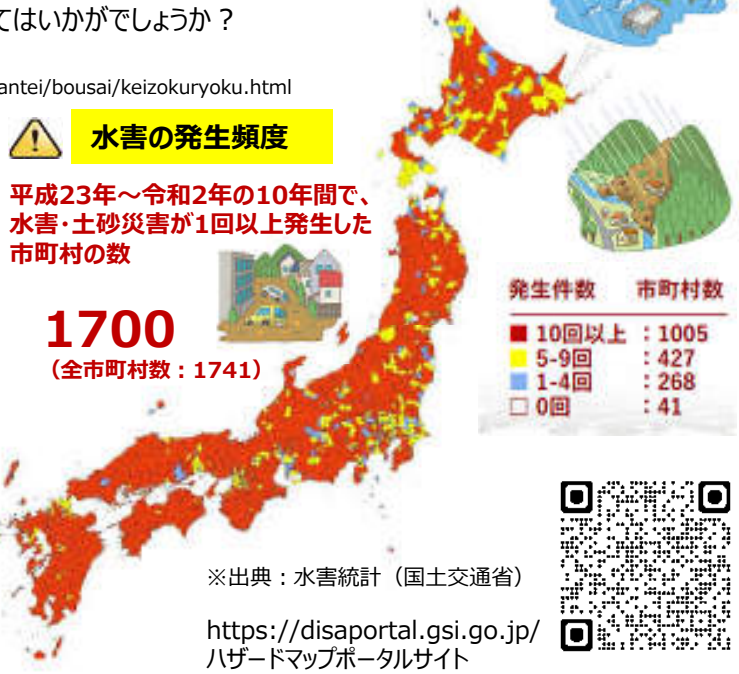
事業継続リスクに備える国の認定制度 ご存じですか？事業継続力強化計画

事業継続力強化計画
https://www.chusho.meti.go.jp/keiei/antei/bousai/keizokuryoku.html

最近の10年間で約97%の市区町村で水害が発生しています

私たちの住んでいる日本は、国土面積に占める可住地の割合が27.3%と小さく、海沿いや山あいをはじめ、平地においても河川沿いを住居や勤務地とする地域が多く存在します。ここ数年においては、台風やゲリラ豪雨による浸水被害や崖崩れなどで建物だけでなく、人命に関わる被害も増えてきました。災害に備えて住んでいる地域、働いている地域で、どのような災害が起きやすいかを事前に「ハザードマップ」で確認してみてください。また、これを機に事業継続力強化計画を策定してみてはいかがでしょうか？





※出典：水害統計（国土交通省）

https://disaportal.gsi.go.jp/
ハザードマップポータルサイト

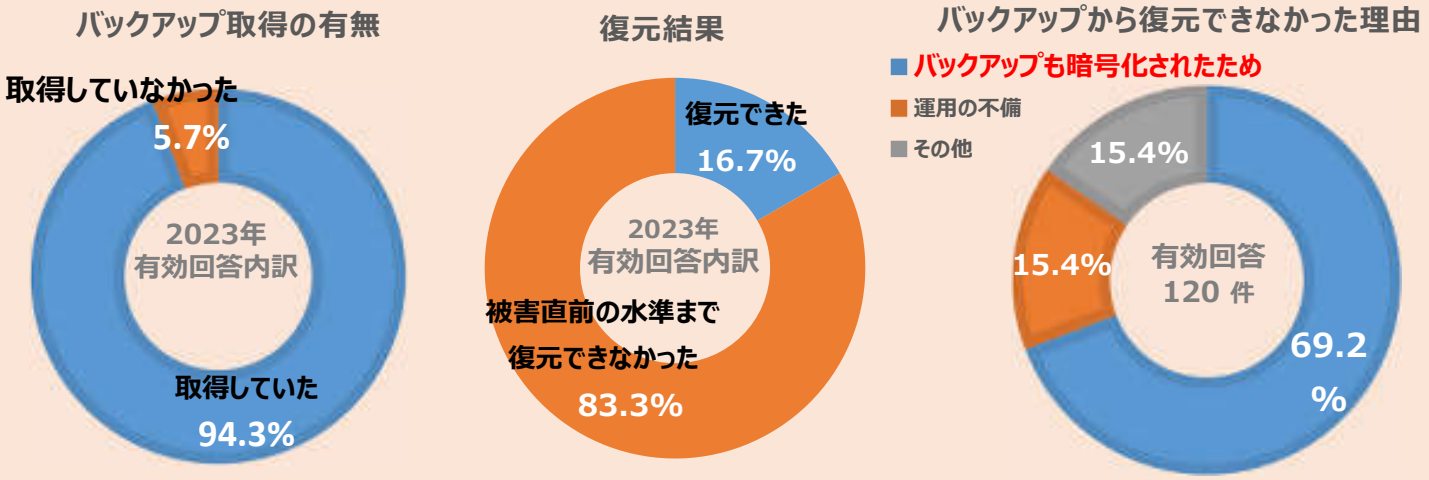
警察庁サイバー警察局　ランサムウェア被害防止対策抜粋

ランサムウェアの被害に遭わないために、被害防止対策、被害軽減対策等について見直しを行うとともに、社員に対して適切なセキュリティ教育を行うなど、総合的な対策強化を図ってください。

- **VPN機器等の脆弱性を塞ぐ**
- **認証情報を適切に管理する（強力なパスワードを使用する）**
- **アクセス権等の権限を最小化する**
- **ウイルス対策ソフト等を導入する**
- **電子メール等を警戒する**
- **ネットワークを監視する：**ランサムウェアを含めたマルウェア等に感染したパソコンでは、外部のサーバーとの間で不審な通信を行う場合があります。ネットワークに侵入されてしまった場合にネットワーク内の不審な挙動を検知し感染拡大や外部からの侵入の範囲拡大を阻止するため、ＥＤＲ（Endpoint Detection and Response）の導入も検討してください。
- **データ等のバックアップを取得する：**ランサムウェアにより、バックアップデータやログも暗号化されてしまう事例が確認されています。

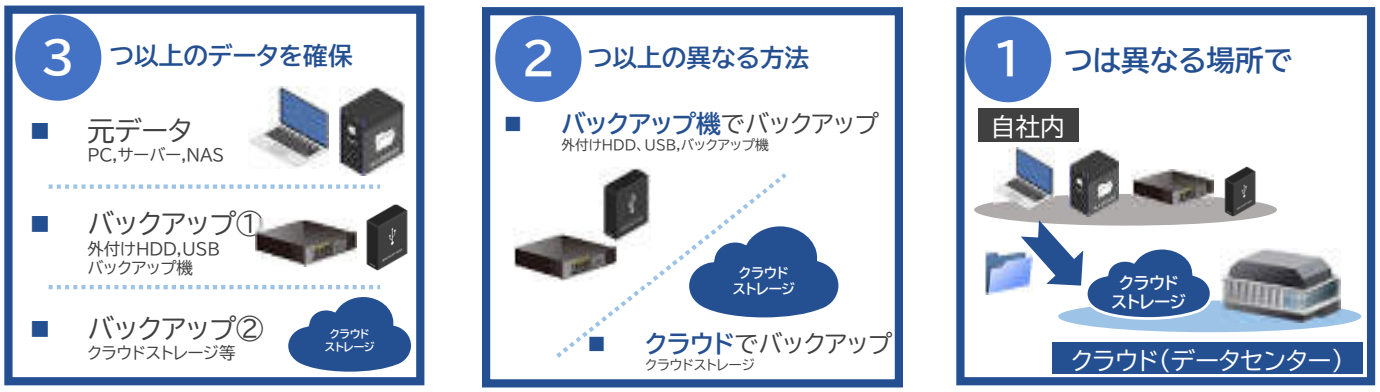
参照元：警察庁　https://www.npa.go.jp/bureau/cyber/countermeasures/ransom.html

ランサムウェアによる被害を受けた組織のアンケート回答より（警察庁）



出典元：【2024年3月警察庁広報資料】令和５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

定期的にバックアップを作成して、最新状態のシステムに復元できるよう備えましょう。また、マルウェア感染でバックアップにも影響が発生した場合のことも考慮して、感染していない期間を選べるよう、世代管理ができるバックアップを用意することをおすすめします。ランサムウェア攻撃の脅威から守るために、**バックアップの3-2-1** ルールが提唱されています。



一部のランサムウェアについては、「No More Ransom」プロジェクトのウェブサイトで復号ツールが公開されています。
「No More Ransom」 https://www.nomoreransom.org/ja/index.html

ところで、あなたの会社のサイバー攻撃対策は大丈夫？

「5分でできる!オンラインセキュリティ自社診断（IPA提供）」で、御社のセキュリティレベルを把握してみませんか？

入門編に設けられている25個の診断項目に答えると、御社の情報セキュリティのレベルを知ることができます。また、解説編もついているので、対応していない場合に生じるリスクと今後、必要な対策を学ぶことができます。

入門編　　基本編