最新の統計結果から見えてきた、今すべき対策とは

東京エレクトロン デバイス株式会社

CN BU CN営業本部
アカウント第一営業部
大澤 祐介

はじめに

ランサムウェアによる被害が、悪化の一途を辿っております。

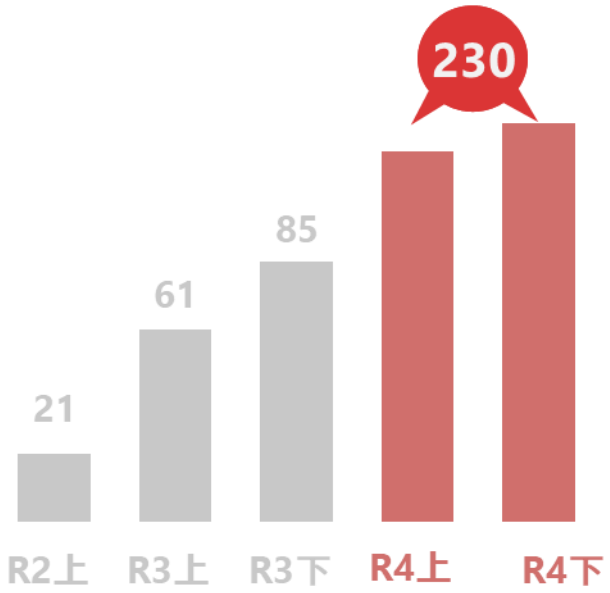
本セミナーでは、警察庁発表の

「令和４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」

の内容を紐解きながら、今行うべきランサムウェア対策についてご紹介させていただきます。

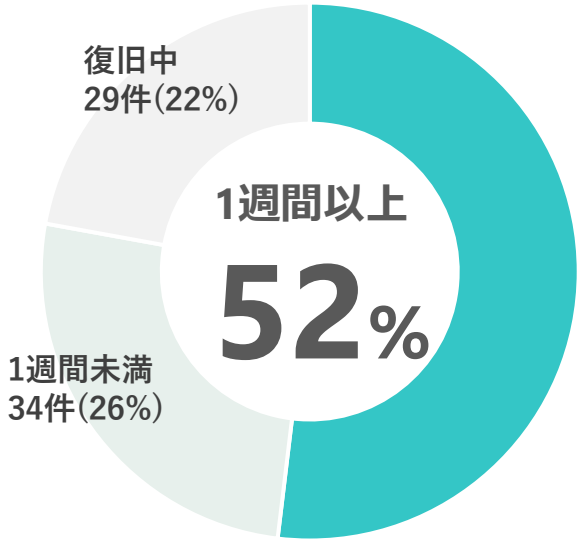
ランサムウェアの被害、急増中

被害報告件数の推移



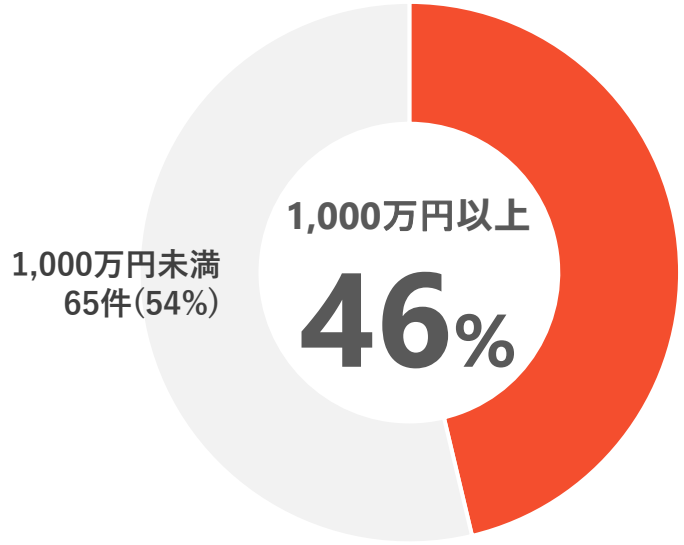
令和4年(2022年)通期の
被害報告件数は**230件**※
毎年右肩上がりで増加

復旧に要した期間



復旧に要した期間について、
1週間以上要したとの回答が
68件（有効回答131件）

調査・復旧費用



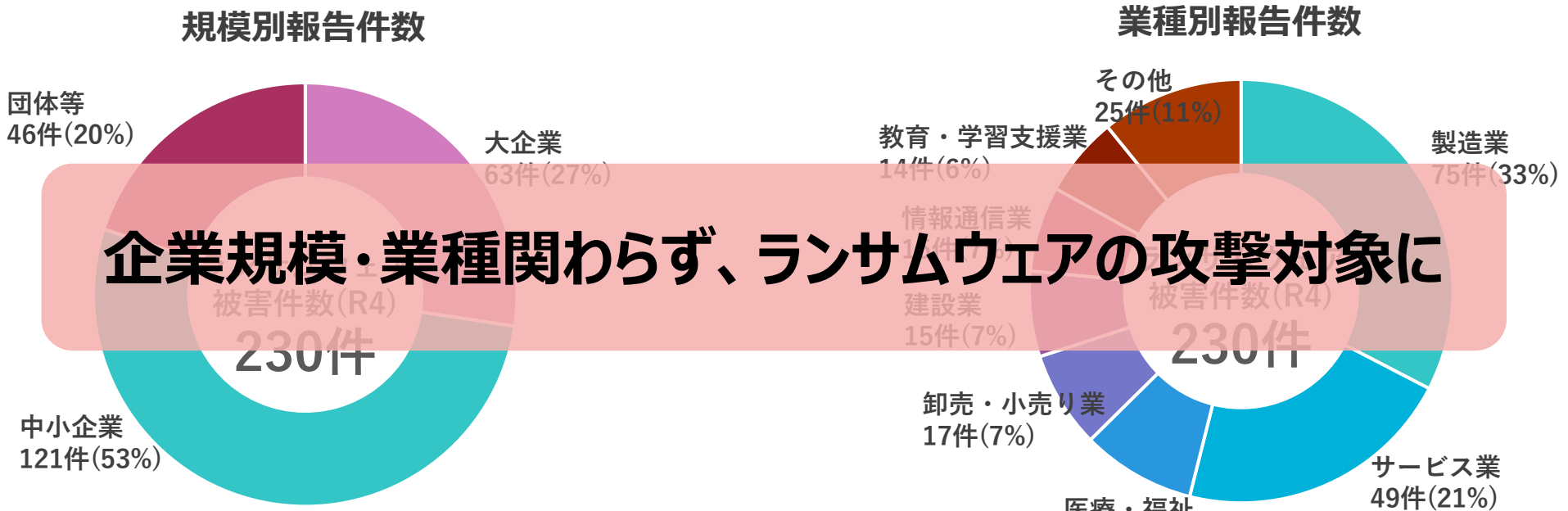
被害に関連して要した
調査・復旧費用の総額について、
1,000万円以上を要したとの回答が
56件（有効回答121件）

※あくまでも報告件数。実際の被害件数ははるかに多いと言われている

出典：警視庁：令和4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

国内ランサムウェア攻撃事例

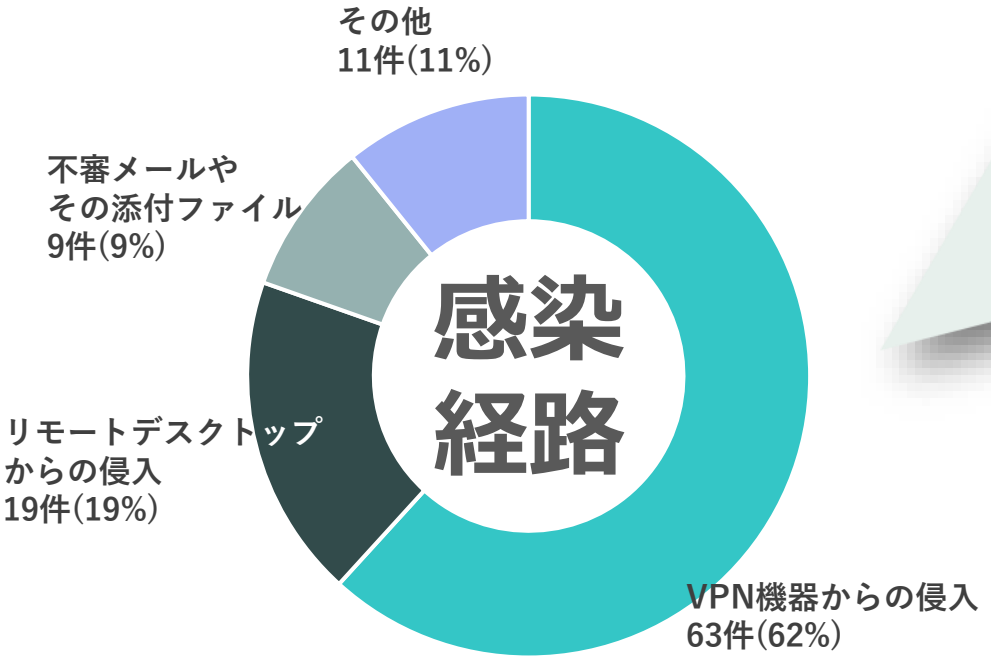
発 生 日	内 容
2022/03	トヨタ自動車は28日、3月1日に国内全工場（14工場28ライン）の稼働を停止すると発表した。トヨタ車の部品をつくるサプライヤーがサイバー攻撃を受け、部品供給を管理するトヨタのシステムが影響を受けたため。2日以降に通常稼働に戻せるかどうかは精査中。日野自動車とダイハツ工業も同日、同じ理由で1日に国内工場を止めると明らかにした。
2022/09	大潟村農業協同組合がサイバー攻撃を受け、組合員などおよそ5000人分の個人情報が流出した可能性があると発表した。流出した可能性がある個人情報には、組合員や利用者の名簿、マイナンバー、口座、貯金、年金、出資金、貸出金、確定申告に関する情報などが含まれる。
2022/10	大阪急性期・総合医療センターが、ランサムウェアによるサイバー攻撃を受け、電子カルテシステムが停止した。同院では約100台のサーバーを運用しているが、被害を受けたサーバーは、バックアップサーバーを含む基幹系サーバー、電子カルテの各システムがある仮想統合サーバー、部門系のバックアップサーバーなど31台にのぼるという。
2023/03	オーディオ機器メーカーのオーディオテクニカは3月7日、外部からランサムウェアによる不正アクセスを受け、社内の機密情報の一部が不正に閲覧された可能性があると発表した。



企業規模・業種関わらず、ランサムウェアの攻撃対象に

出典：警視庁：令和4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

感染経路



◆侵入経路を意識したランサムウェア対策

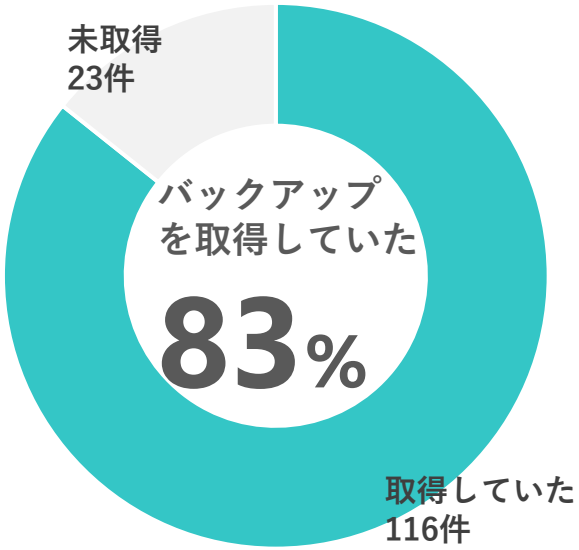
① 脆弱性対策
- 定期的なパッチ適用作業
  （更新プログラム適用作業）
- 重要なデータがバックアップが出来ているか
  定期的な実施・点検

② 弱い認証情報の対策
- パスワードの複雑さを求めるパスワードポリシーを適用
- 多要素認証を採用

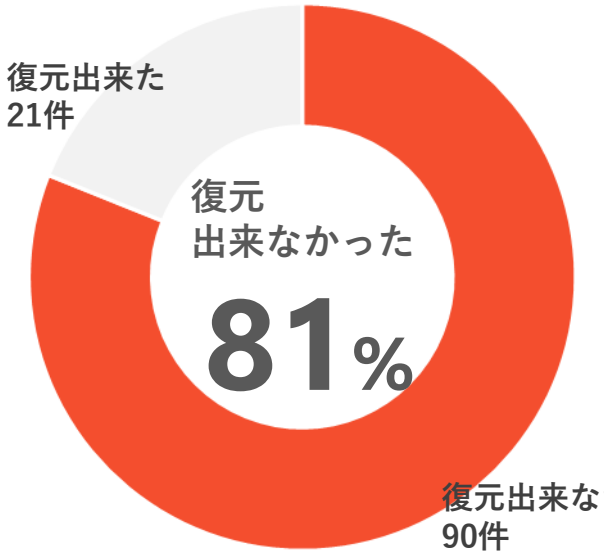
出典：NISC(内閣サイバーセキュリティセンター) 2022年9月27日

今やバックアップデータも攻撃対象に

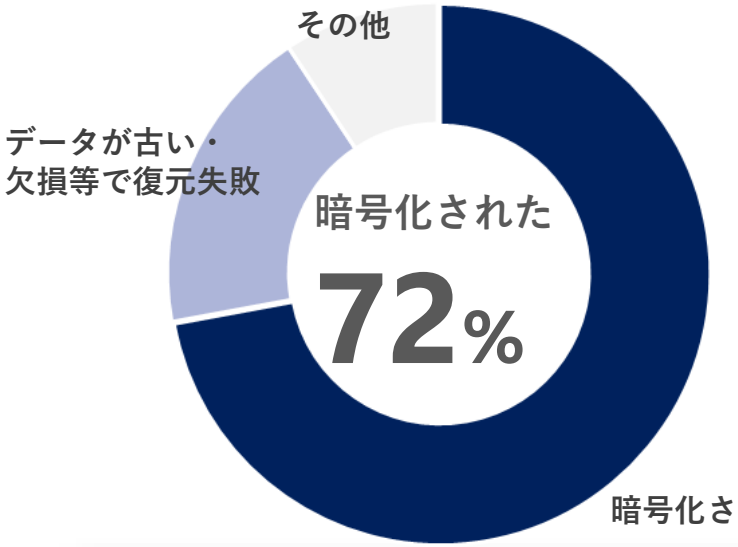
バックアップ取得の有無



復元結果



バックアップを利用して復元できなかった理由



出典：警視庁：令和4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

グループ会社を含むサーバの大半が同時攻撃を受け、バックアップを含む大量のデータが暗号化されて復旧不能に。外部専門家に「前例のない規模」と報告を受け

日本の製粉大手に「前例ない」大規模攻撃　大量データ暗号化　起動不能、バックアップもダメで「復旧困難」

2021年08月17日 16時46分 公開　[松浦立樹，ITmedia]

印刷　見る　Share　B!　1026　0

PR Reactの状態管理|HooksやServer Componentsの登場による変化

PR 「セキュリティに不安」「作業効率に課題」を一挙に解決！

「システムの起動そのものが不可能で、データ復旧の手段はない」――製粉大手のニップン（東証一部上場）は8月16日、7月7日に受けたサイバー攻撃の詳細と影響を明らかにした。

グループ会社を含むサーバの大半が同時攻撃を受け、バックアップを含む大量のデータが暗号化されて復旧不能に。外部専門家に「前例のない規模」と報告を受けたという。

出典：ITmediaNEWS（2021年8月17日）

東京エレクトロン デバイス

「バックアップを取っているから大丈夫」

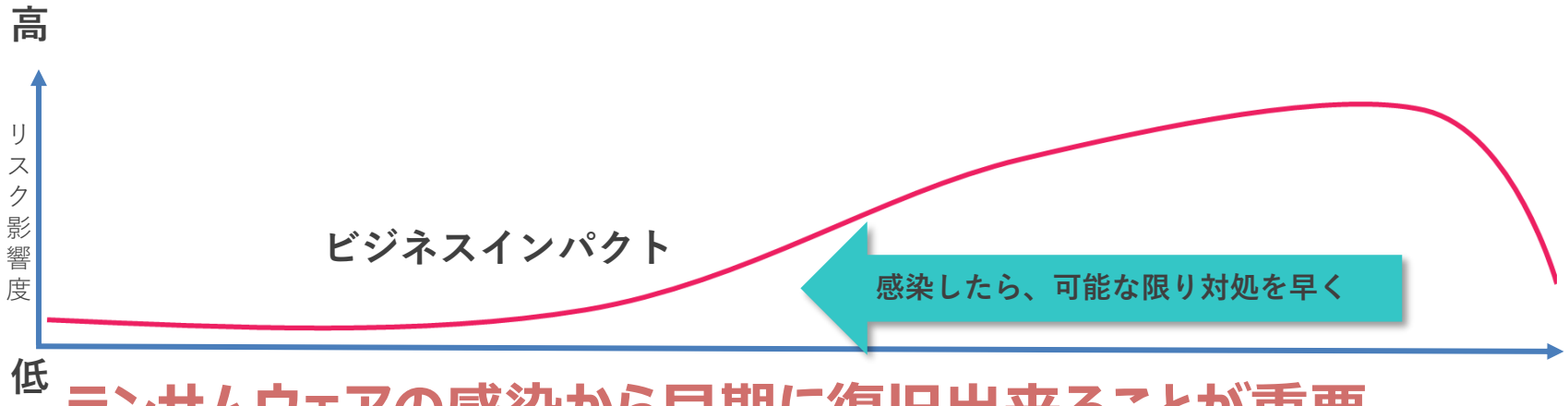
では不十分です

これからのセキュリティ対策ではバックアップが重要に

- あらゆるセキュリティ対策を実施しつつ、ランサムウェアに感染される前提での、ポストインシデント対策の強化へ

NIST：サイバーセキュリティフレームワーク(CSF)

特定	防御	検知	対応	復旧
ネットワーク/データセキュリティなど		EDRなど		バックアップなど
ITリソースの把握 最低限のアクセス、通信のみ許可 ネットワーク/データセキュリティ対策		エンドポイントにおける検知と抑制 原因と影響範囲の分析 隔離などにより被害を最小化		サービスや データの復旧
プリインシデント		ポストインシデント		



バックアップの重要性の高まり

- 防御を突破され、検知を免れ、ランサムウェアに感染される前提において、復旧のためのバックアップは不可欠
- 各ベンダー/機関がバックアップを確実に取得することを推奨

Sophos
ランサムウェアはバックアップによって決まる。身代金を支払うのではなくバックアップからの復元により、存続可能な、管理可能な損失のみに抑制される

Fortinet
重要なシステムやデータをバックアップする。データのバックアップがビジネス要件を満たすこと、迅速に復元できるようにしておくことが重要

ランサムウェアの感染から早期に復旧出来ることが重要
バックアップは言わばその”最後の砦”

従来型のバックアップシステムが抱える課題

01 **ランサムウェアはバックアップも攻撃対象**

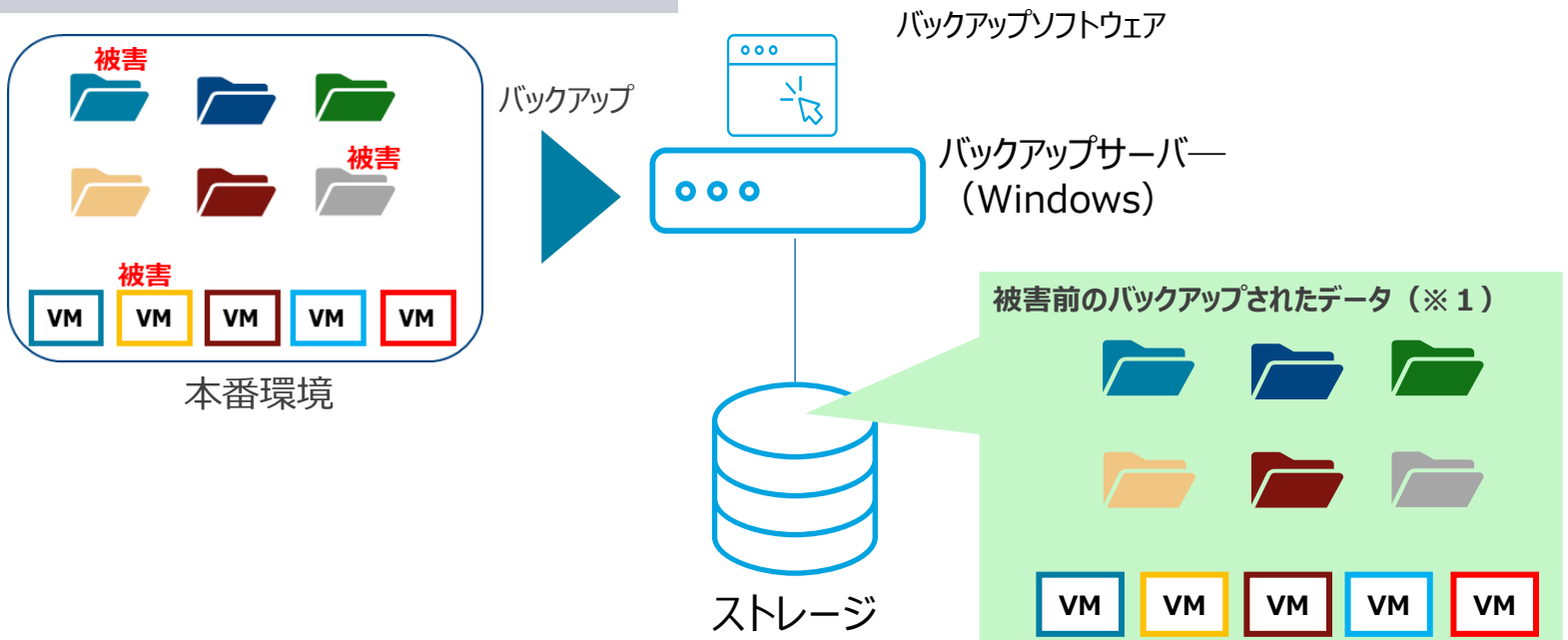
- 本番データも、バックアップデータ（※１）も、両方暗号化されたら対処できない

02 **Windowsは一番攻撃されやすいOS**

- シェア率の高い、WindowsやLinuxが狙われる危険性
- 管理者権限の奪取によるソフトウェアのアンインストール、なりすましによる設定変更

03 **被害箇所特定・どの時点のバックアップをリストアするかをすぐに決断できるか？**

- 緊急事態下で、基幹システムのディスクを、高負荷にしてデータ調査しますか？



データセキュリティにおける新しいアプローチが必要

バックアップデータを
サイバーアタックから
保護する

リスクを監視し
脅威を迅速に
調査できる

必要なデータだけを
安全、かつ迅速に
復旧できる

ランサムウェアなどの攻撃からの防御、調査、復旧ができれば、
ランサムウェア攻撃への身代金を支払う必要はない

まとめ

- ランサムウェアの被害件数は、毎年増加の一途をたどっている
- 企業規模・業種に関わらず、ランサムウェアの攻撃対象となっている
- バックアップを取っているから大丈夫、では不十分。**有事の際に“使える”バックアップが必要**
- **Windowsは一番狙われやすいOS。**管理者権限を奪取される可能性
- データセキュリティにおける**新しいアプローチが必要**

onnect Beyond

共に創る　新たな価値を

東京エレクトロン デバイス