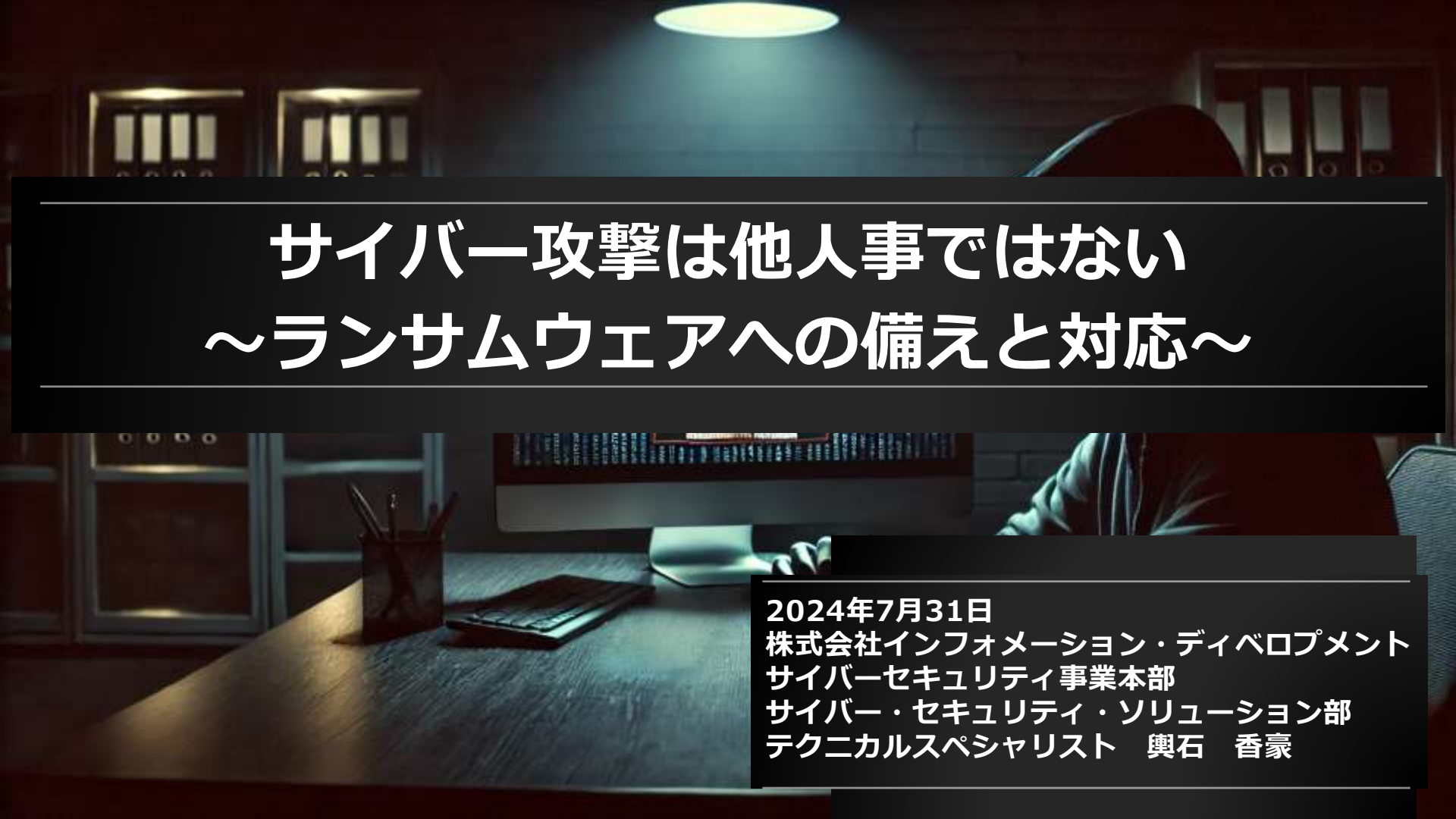


サイバー攻撃は他人事ではない
～ランサムウェアへの備えと対応～

2024年7月31日
株式会社インフォメーション・ディベロプメント
サイバーセキュリティ事業本部
サイバー・セキュリティ・ソリューション部
テクニカルスペシャリスト　輿石　香豪

本セッションのねらい

～ランサムウェアへの備えと対応～

ランサムウェアは、企業や個人のデータを暗号化し、その解除のために身代金を要求する非常に悪質な攻撃手法です。

ランサムウェアの脅威とトレンドを解説し、企業の規模や業種を問わず、情報システム部門や社内システムのセキュリティ管理部門の担当者が直面する、現実的な課題に対する解決策を考え、将来的なサイバー攻撃に対する備えを強化するための対応策を提供します。

講演者の紹介

名前：　輿石（コシイシ）　香豪（コウゴウ）

所属：株式会社インフォメーション・ディベロプメント
サイバーセキュリティ事業本部
サイバー・セキュリティ・ソリューション部
テクニカルスペシャリスト

略歴：

1996年、独立系ソフトウエア会社にてシステム開発、システム設計、導入等、システムエンジニアとして業務に従事
2011年、株式会社インフォメーション・ディベロプメント入社　システム開発、運用、保守、ヘルプデスク等幅広い業務に従事
2016年、セキュリティ部署に異動し、製品導入、組織立上げ支援、規程作成支援等、セキュリティに関する業務に従事
2024年現在、セキュリティに関する助言、支援等、お客様のセキュリティ向上に関わる業務を担当

主要な認定等：

情報処理安全確保支援士(経済産業省)第005524号、　応用情報処理技術者(経済産業省)、
情報セキュリティ管理士、　ファイナンシャルプランニング技能士3級(厚生労働省)

アジェンダ

- ランサムウェアの現状と脅威
- 効果的な入口・出口対策
- バックアップの重要性
- まとめ
- 弊社サービス紹介

ランサムウェアの現状と脅威

ランサムウェアの現状と脅威

攻撃者への対応

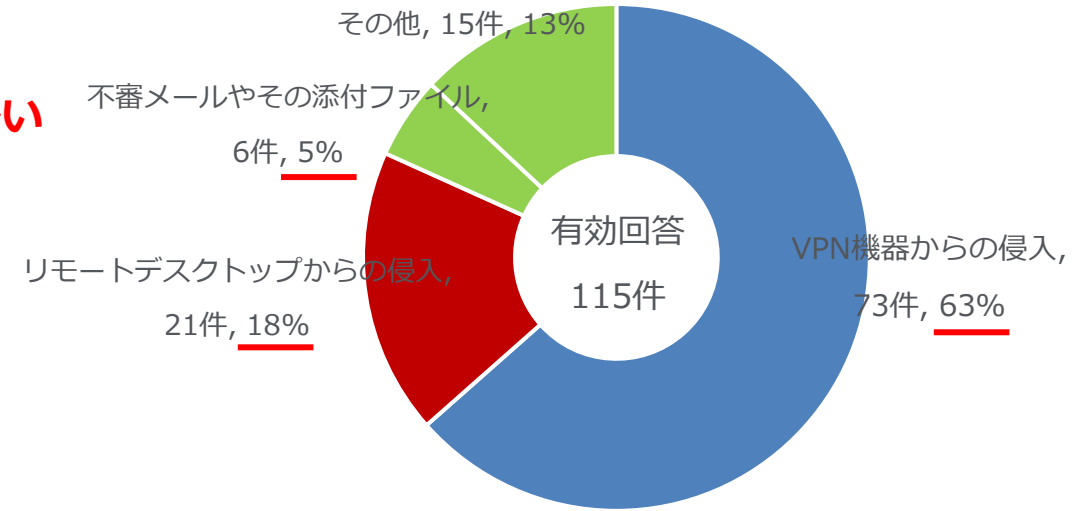
- 身代金支払の実態
- 身代金を支払うべきか？

ランサムウェアの現状と脅威

感染経路について

VPN機器から侵入が63%、リモートデスクトップからの侵入が18%。
外部ネットワークからの攻撃が8割を占めているが、不審メールや添付ファイルからも5%となっている。

⇒**VPN機器からの侵入が最も多い**



注：図中の割合は小数点第1位以下を四捨五入しているため、総計が必ずしも100にならない

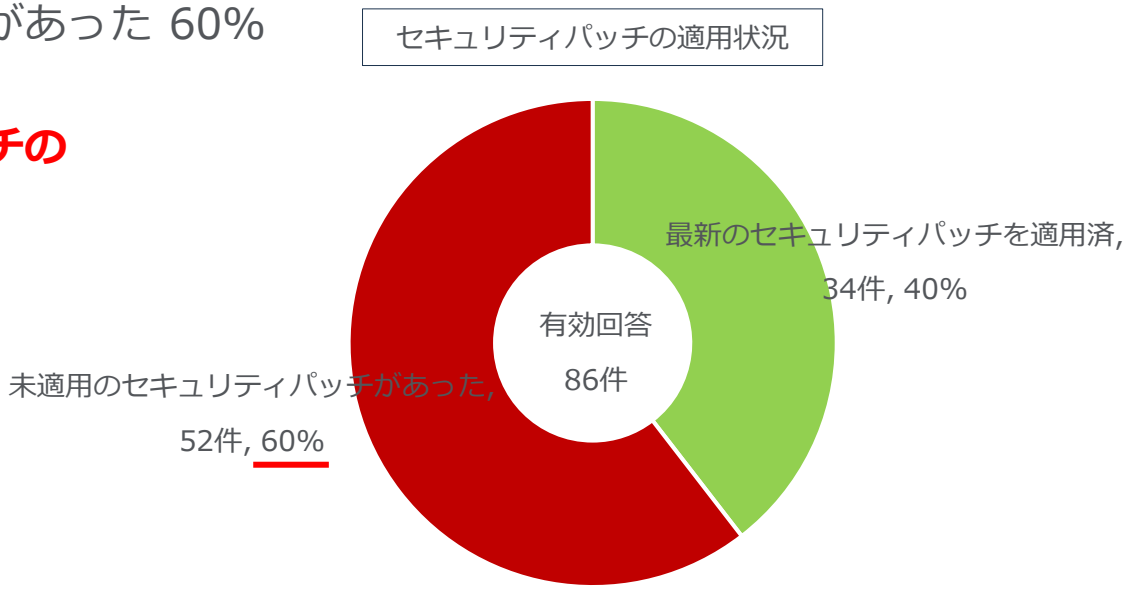
警察庁　令和５年におけるサイバー空間をめぐる脅威の情勢等について(令和6年3月14日) p26を元に作成
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

ランサムウェアの現状と脅威

感染経路について

侵入経路とされる機器のセキュリティパッチの適用状況について、
最新のセキュリティパッチを適用済 40%
未適用のセキュリティパッチがあった 60%

⇒**未適用のセキュリティパッチの機器が60%もある**



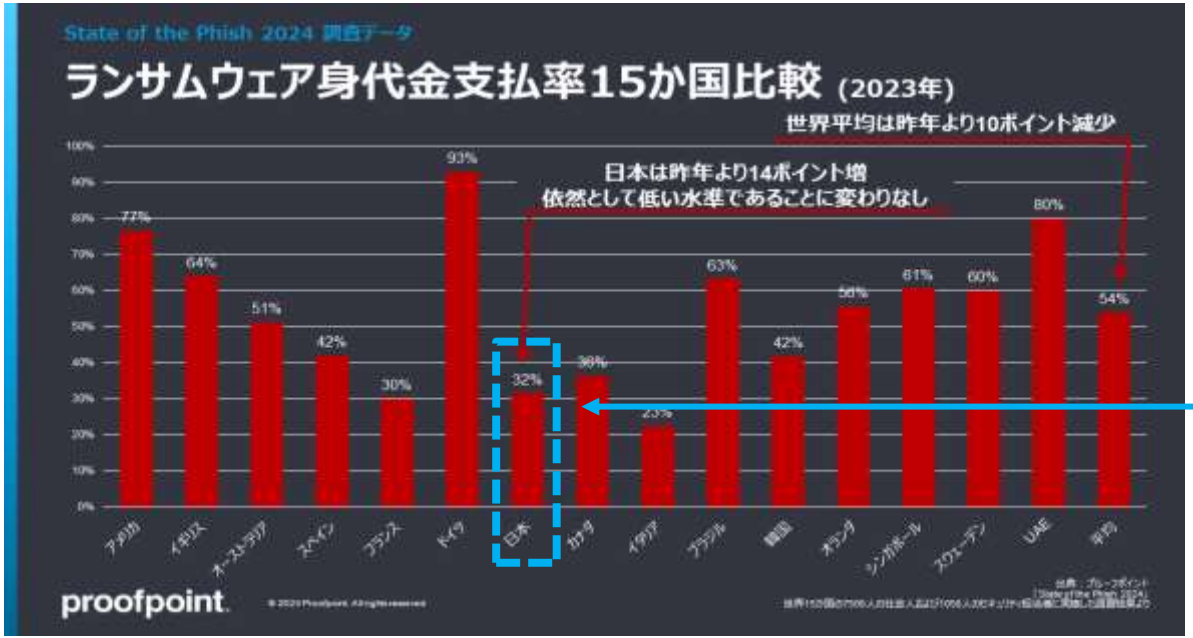
警察庁　令和５年におけるサイバー空間をめぐる脅威の情勢等について(令和6年3月14日) p48を元に作成
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

ランサムウェアの現状と脅威

身代金支払の実態

State of the Phish 2024レポート

Proofpointが2023年の現状について、世界15か国の7500人の社会人および1050人のセキュリティ担当者に調査を実施した結果



国別で比較すると日本は**32**%
身代金支払率は低い方に入る

出典：Proofpoint、State of the Phish 2024レポートより図引用
https://www.proofpoint.com/jp/blog/threat-insight/japan-ransomware-payment-result-2024

ランサムウェアの現状と脅威

身代金支払の実態

State of the Phish 2024レポート

Proofpointが2023年の現状について、世界15か国の7500人の社会人および1050人のセキュリティ担当者に調査を実施した結果

「1回目の身代金支払いで、データ復旧」**17**%

「2回目の身代金支払いで、データ復旧」**50**%

3割～4割はデータ復旧出来ていない

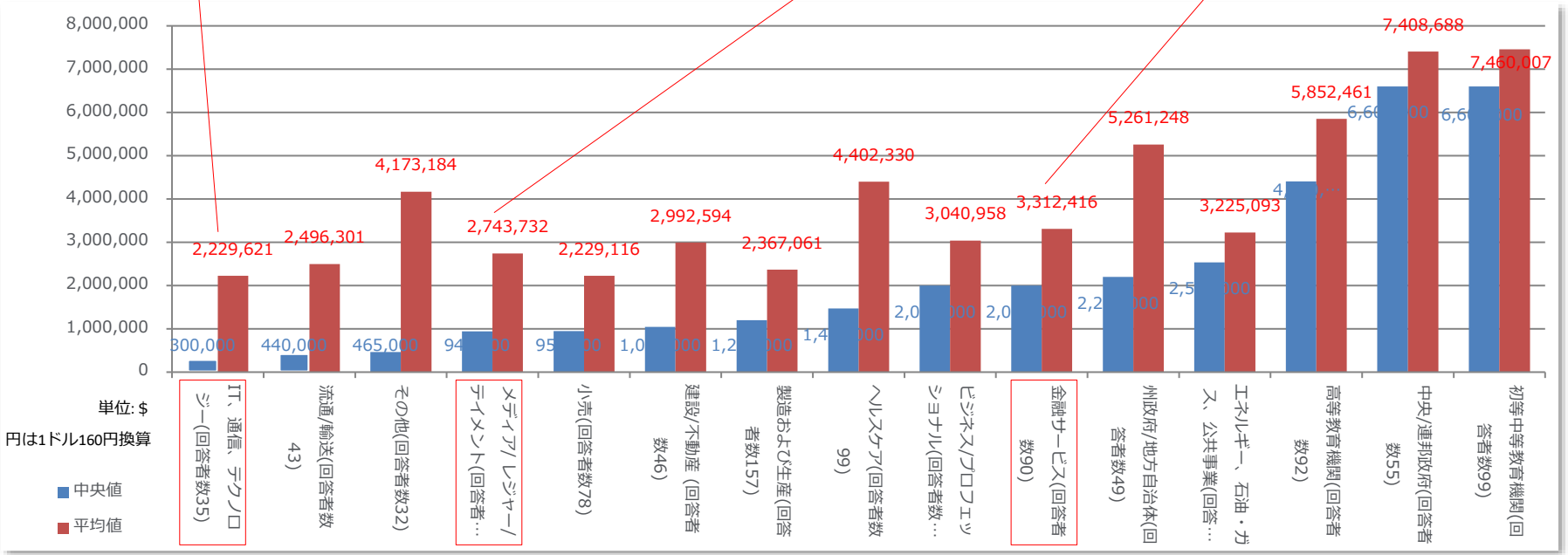
身代金を支払えば
データを復旧できるわけではない

出典：Proofpoint、State of the Phish 2024レポートより図引用
https://www.proofpoint.com/jp/blog/threat-insight/japan-ransomware-payment-result-2024

ランサムウェアの現状と脅威

身代金の支払額について(業界別)

「IT、通信、テクノロジー」は平均**3億5千万円**、「メディア」は**4億円強**、「金融」は **5億円強**

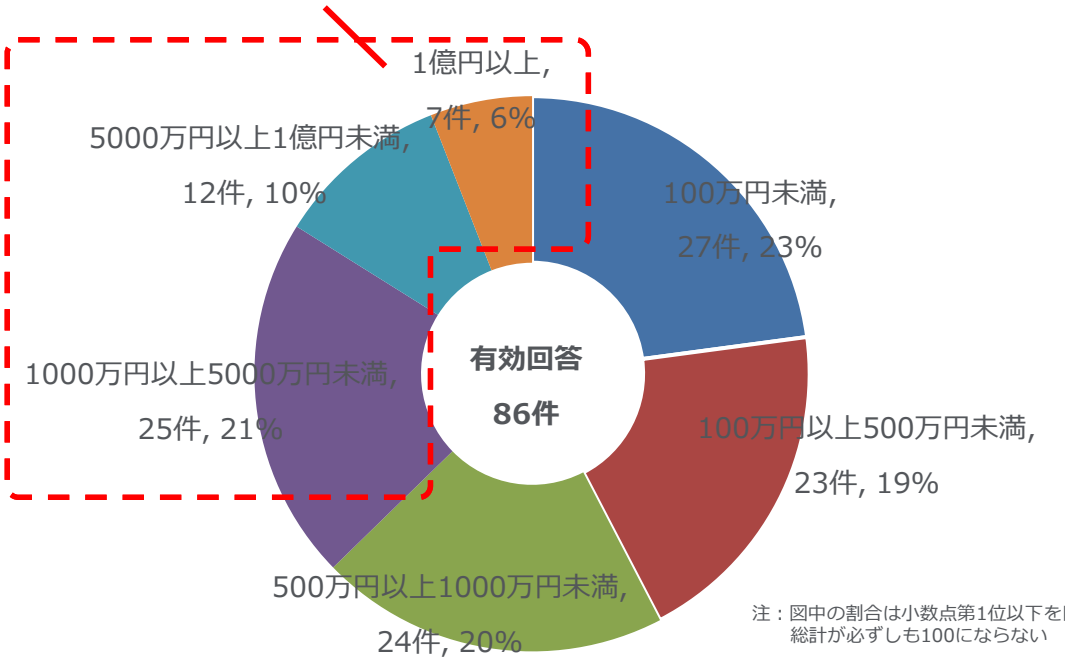


ソフォス ホワイトペーパー ランサムウェアの現状2024年版の「要求された身代金額 (業界別)」を元に作成
https://assets.sophos.com/X24WTUEQ/at/f7pxb9f8ws4fqzx78rv9g5p7/sophos-state-of-ransomware-2024-wpja.pdf

ランサムウェアの現状と脅威

調査・復旧費用について

1000万円以上が37%、そのうち1億円以上が6%
⇒4割弱が1000万円以上



注：図中の割合は小数点第1位以下を四捨五入しているため、総計が必ずしも100にならない

警察庁　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(令和6年3月14日) p26を元に作成
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

ランサムウェアの現状と脅威

ランサムウェア不払いに関する声明

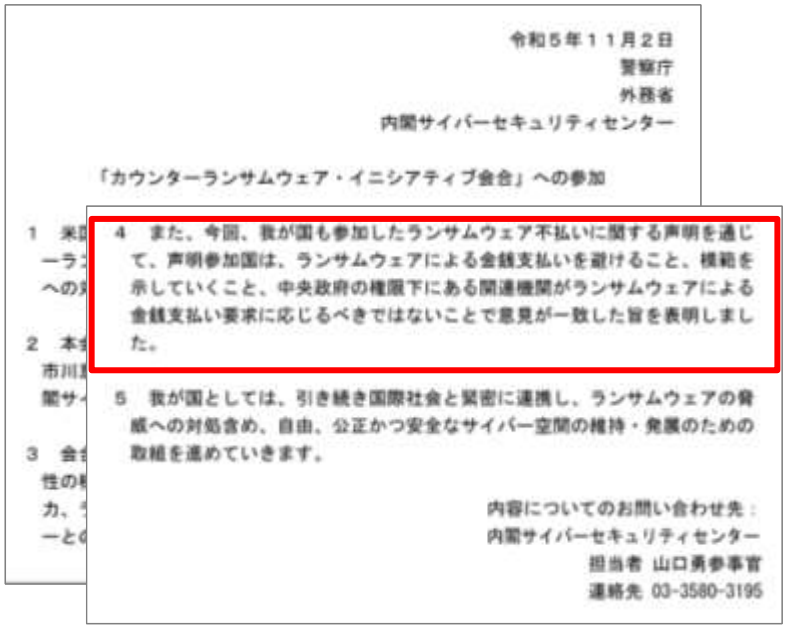
令和5年11月、政府等関係機関が「カウンターランサムウェア・イニシアティブ会合」へ参加し、ランサムウェア不払いに関する声明を発表

計５０か国・機関：アルバニア、オーストラリア、オーストリア、ベルギー、ブラジル、ブルガリア、コロンビア、コスタリカ、クロアチア、チェコ共和国、ドミニカ共和国、エジプト、エストニア、ＥＵ、ドイツ、ギリシャ、インド、インターポール、アイルランド、イスラエル、日本、ヨルダン、ケニア、リトアニア、メキシコ、オランダ、ニュージーランド、ナイジェリア、ノルウェー、パプアニューギニア、ポーランド、ポルトガル、ルーマニア、ルワンダ、シエラレオネ、シンガポール、スロバキア、南アフリカ、スウェーデン、スイス、アラブ首長国連邦、ウクライナ、ウルグアイ

内閣官房副長官補ほか、警察庁、外務省、内閣サイバーセキュリティセンターなどが参加。
今回、我が国もランサムウェア不払いに関する声明を通じて、

- ✓ **ランサムウェアによる金銭支払いを避けること**
- ✓ 模範を示していくこと
- ✓ **中央政府の権限下にある関連機関がランサムウェアによる金銭支払い要求に応じるべきではないこと**

上記で意見が一致した旨を表明



令和５年１１月２日
警察庁
外務省
内閣サイバーセキュリティセンター

「カウンターランサムウェア・イニシアティブ会合」への参加

４　また、今回、我が国も参加したランサムウェア不払いに関する声明を通じて、声明参加国は、ランサムウェアによる金銭支払いを避けること、模範を示していくこと、中央政府の権限下にある関連機関がランサムウェアによる金銭支払い要求に応じるべきではないことで意見が一致した旨を表明しました。

５　我が国としては、引き続き国際社会と緊密に連携し、ランサムウェアの脅威への対処含め、自由、公正かつ安全なサイバー空間の維持・発展のための取組を進めていきます。

内容についてのお問い合わせ先：
内閣サイバーセキュリティセンター
担当者 山口勇参事官
連絡先 03-3580-3195

ランサムウェアの現状と脅威

身代金を支払うべきか？

攻撃者への対応

- 身代金を支払えばデータが必ず復旧できるわけではない
- 被害原因の調査を行わないと被害の原因が解決されない
- 「ランサムウェア不払いに関する声明」に反する
- 法律面でのリスクとして、
  - ➢支払先が経済制裁者の場合、外為法違反のリスク
  - ➢アメリカのOFAC(Office of Foreign Assets Control)規制違反のリスク

⇒米国財務省外国資産管理局(OFAC)は、ランサムウェア攻撃の被害者と関わる企業に、
ランサムウェアの支払いを容易にするための潜在的な制裁リスクについて警告する勧告を発行

・身代金を支払うということは犯罪組織に金銭的支援を行っているということ
・安易に身代金を支払うべきではない

OFAC(Office of Foreign Assets Control) Ransomware Advisory
https://ofac.treasury.gov/recent-actions/20201001
https://ofac.treasury.gov/media/48301/download?inline

効果的な入口・出口対策

効果的な入口・出口対策

ランサムウェアの被害に遭わないために以下のような被害防止対策、被害軽減対策について見直しを行うとともに、従業員・役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実施する

カテゴリ	被害防止策	対策区分
事前対策	**VPN機器等のぜい弱性を塞ぐ** 必須!	入口対策 出口対策
	認証情報の適切な管理	入口対策
	アクセス権等権限の最小化	内部対策
	EDR等ウイルス対策ソフトの導入	内部対策
	電子メール等の警戒	入口対策 出口対策
	NDR、SIEM等を導入しネットワークの監視	内部対策
	脆弱性診断やASM※1の活用	入口対策
事後対策	**データ等のバックアップの取得** 重要!	被害軽減
	サイバー保険への加入 (**身代金は補償外**(日本損害保険協会より))	被害軽減

※1 ASM(Attack Surface Management)：外部(インターネット)からアクセス可能な IT 資産の情報を調査し、それらに存在する脆弱性を継続的に評価する取り組みで、専用のツールやサービスを活用して実施することが一般的

警察庁　ランサムウェア被害防止対策を参考
https://www.npa.go.jp/bureau/cyber/countermeasures/ransom.html

効果的な入口・出口対策

技術的対策以外にも以下のような「人的対策」、「組織的対策」を計画し、実行することを強く推奨します

実施区分	被害防止策	対策区分
組織的対策	社内ルール(情報共有、プレスリリース、連絡体制等)の整備	内部対策 外部対策
	最終的な意思決定者と決定内容の基本方針確認、フロー準備	内部対策 外部対策
	インシデント発生時の迅速な対応フローの確立	内部対策
	インシデント後のフォローアップと改善策の実施	内部対策
人的対策	**標的型攻撃メール訓練の実施** ネットワーク外部と接点がある部分の対策として	内部対策
	インシデント訓練・演習の実施	内部対策
	セキュリティ意識向上を目的としたサイバー攻撃教育の実施	内部対策

事前対策として
計画・実施

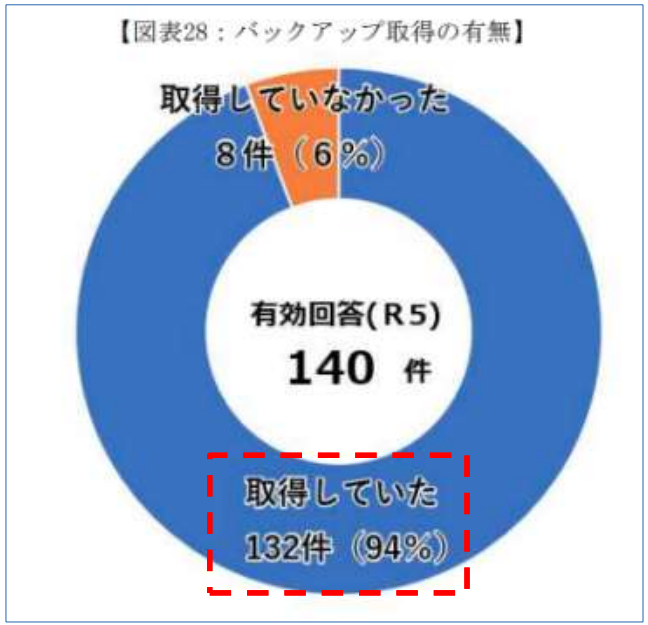
バックアップの重要性

バックアップの重要性

バックアップの重要性

被害に遭ったシステム又は機器のバックアップの取得状況

バックアップを取得していた・・・94%



⇒では被害直前の水準まで

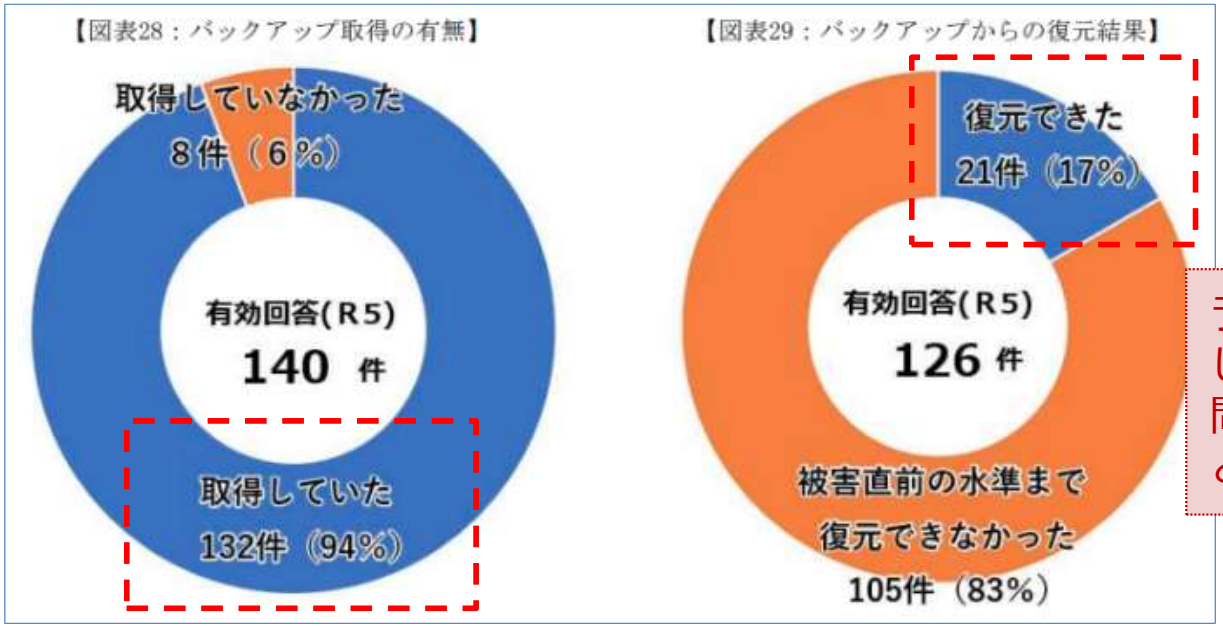
復元できた割合は？？？％？

警察庁　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(令和6年3月14日) p27,図引用
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

バックアップの重要性

被害に遭ったシステム又は機器のバックアップの取得状況

⇒被害直前の水準まで復元できた・・・**17**%



ランサムウェア対策を考慮したバックアップを実施、問題なくリストア出来ることが重要

警察庁　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(令和6年3月14日) p27,図引用
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

バックアップの重要性

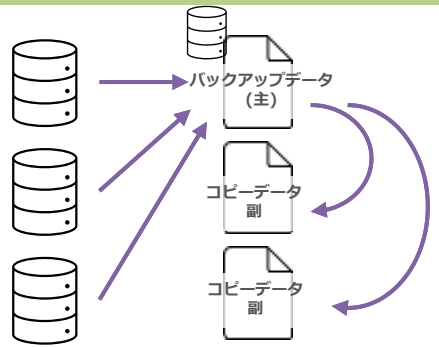
バックアップの321ルール

アメリカのCISA(サイバーセキュリティ・インフラセキュリティ庁)が推奨するベストプラクティス。データバックアップには損失や破損から保護する必要があり損失または破損したデータを回復できる可能性を高めるための施策

重要！

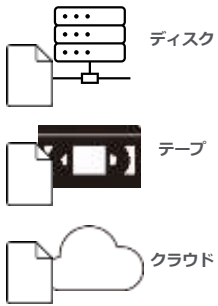
バックアップを3つ保存

Keep 3 copies of any important file: 1 primary and 2 backups.



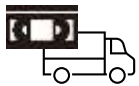
バックアップファイルを異なる2種類の媒体に保存

Keep the files on 2 different media types to protect against different types of hazards.



1つをオフラインに保管

Store 1 copy offsite (e.g., outside your home or business facility).



東京から大阪へ
移送

バックアップサーバシャットダウン
LANケーブル抜線

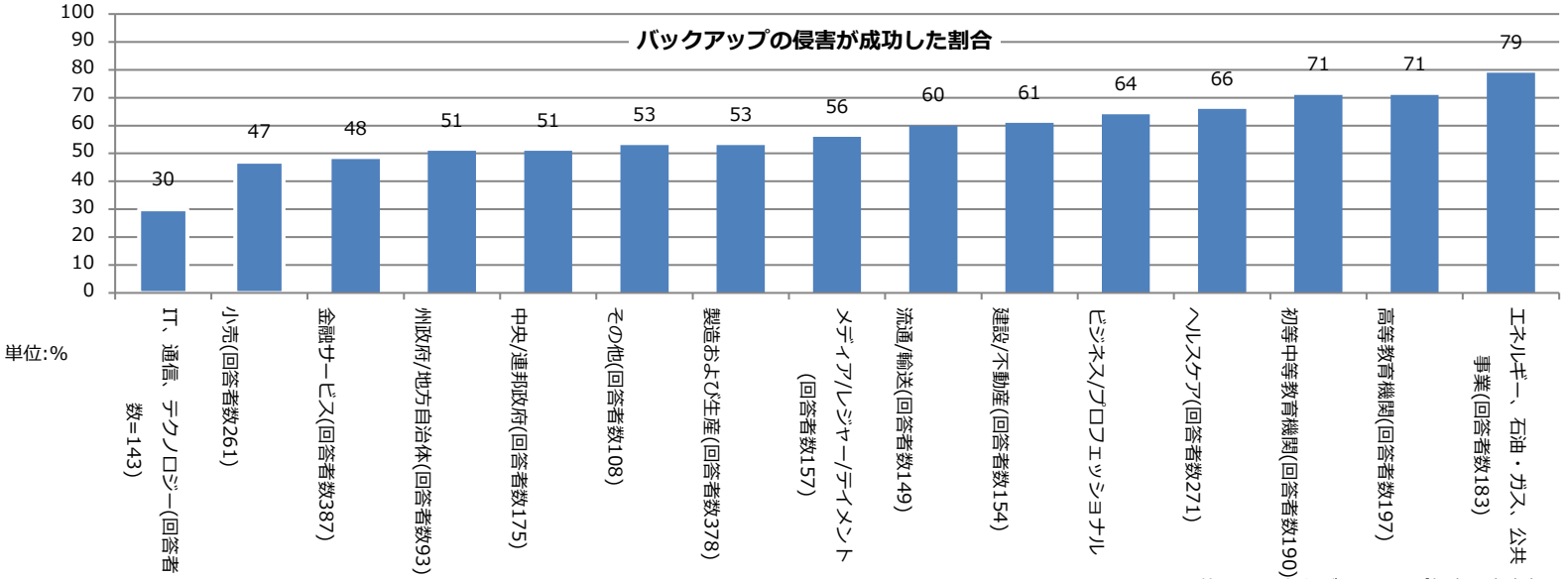
論理的ネットワーク隔離、
書換不可のストレージへ保存

CISA（Cybersecurity and Infrastructure Security Agency） Data Backup Optionsより作成
https://www.cisa.gov/sites/default/files/publications/data_backup_options.pdf

バックアップの重要性

- 過去ランサムウェア被害にあった組織のうち、サイバー攻撃者はバックアップに対しての侵害について試行された割合・・・94%、
- バックアップ侵害の成功率は平均57%
  「IT、通信、テクノロジー」30%、「メディア」56%、「金融」48%

⇒バックアップデータが信用できないor復旧出来ない状態もありえる！



ソフォス　ランサムウェアの現状　2024年版バックアップ侵害の成功率より作成
https://www.cisa.gov/sites/default/files/publications/data_backup_options.pdf

バックアップのベストプラクティス

①イミュータブルストレージの考え方を持つサービス・ソリューションの利用

イミュータブルストレージとは・・・

保存したデータを改変出来ない（書込みのみや削除出来ない設定が出来る）

バックアップの重要性

- **Cloud（イミュータブルストレージの考え方を持つサービスで計画・実施）**
  - Microsoft Azure　・・・　BLOB（Binary Large OBject）
  - Amazon Web Services（AWS）　・・・　Amazon S3オブジェクトロック
  - Google Cloud Platform(GCP)

- **バックアップソリューション（<u>イミュータブルストレージ機能があるかを製品選定時に追加</u>）**
  - Arcserve ：OneXafe(ワンセーフ)
  - Rubrik　：Rubrik　Zero Trust Data Security、Rubrik Cloud Vault
  - Veeam　：Veeam Data Platform
  - Veritas　：Veritas NetBackup Flex Appliance

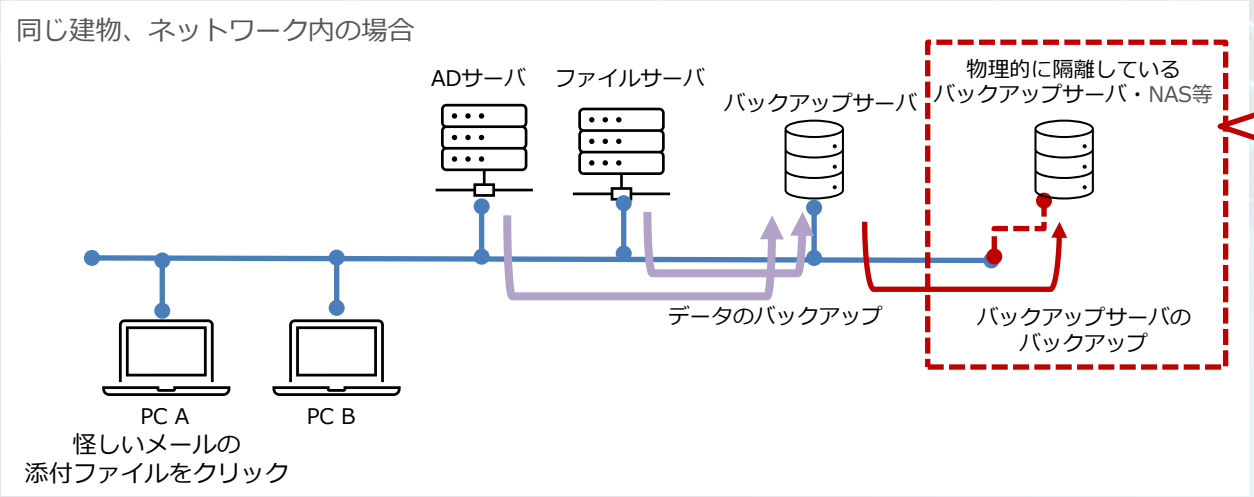
  等

既にサービス・ソリューション導入済みの場合、
機能を調査し、有効に活用しているか確認する

バックアップのベストプラクティス

② エアギャップバックアップを考慮する

システムのネットワークから分離し、物理的に隔離したバックアップの仕組みを構築



一例：

- 対応策として、バックアップ時にLANケーブル接続、バックアップ終了後抜線
- 途中にスイッチングHUBを挟み、バックアップするときだけHUBの電源ON、バックアップ終了後電源OFFする

⇒バックアップ処理していない時はネットワークから遮断

まとめ

まとめ

① 身代金を支払っても確実にファイルが復号出来るわけではない

② VPN機器等の脆弱性対策、標的型攻撃メール対策、
インシデントに関わる社内ルール・体制整備
} 必須事項

③ どの媒体にどのような方法でバックアップを取得しているのか確認
⇒ キーワードは、イミュータブルストレージ、エアギャップバックアップ

④ バックアップ・リストアが正しく行えているか。手順として確立しているか
⇒ 調査し問題があるなら直ちに改善策を実施(経営層のトップ指示の下)

サイバーインシデントは自然界でいう地震などの重要災害と捉え、
ランサムウェア対策を含めた企業継続計画(BCP)という目線で対策を
行うことが大変重要

参考資料

警察庁　ランサムウェア被害防止対策
https://www.npa.go.jp/bureau/cyber/countermeasures/ransom.html

プルーフポイント　State of the Phish 2024レポート
https://www.proofpoint.com/jp/blog/threat-insight/japan-ransomware-payment-result-2024

内閣サイバーセキュリティセンター(NISC)　サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会
https://www.nisc.go.jp/council/cs/kyogikai/guidancekentoukai.html

ソフォス　ランサムウェアの現状　2024年版
https://www.sophos.com/ja-jp/press/press-releases/2024/04/ransomware-payments-increase-500-last-year-finds-sophos-state
https://assets.sophos.com/X24WTUEQ/at/f7pxb9f8ws4fqzx78rv9g5p7/sophos-state-of-ransomware-2024-wpja.pdf

(株)インフォメーション・ディベロプメント　サイバーセキュリティ関連
https://www.idnet.co.jp/service?category[]=%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3

弊社サービス紹介

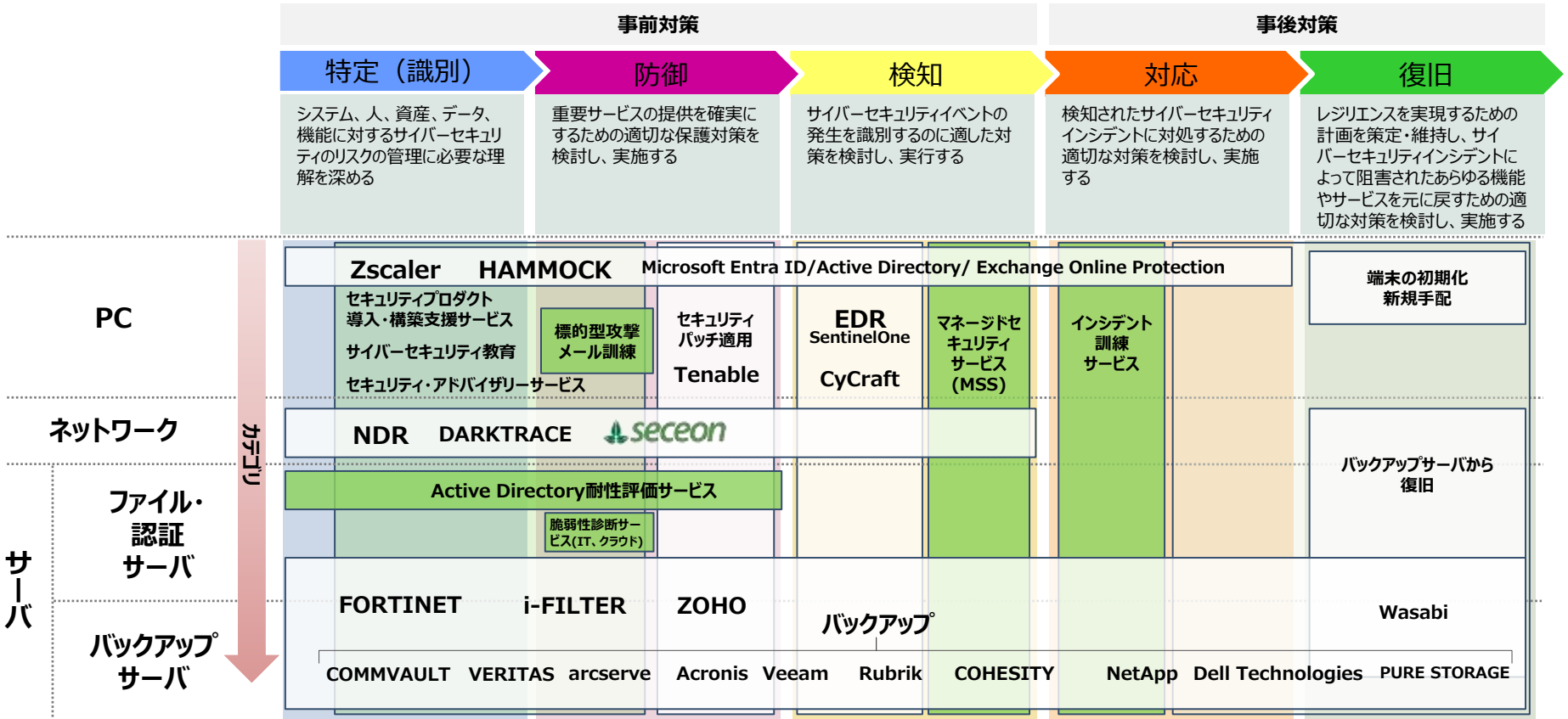
弊社サービス紹介

セキュリティサービスを幅広く提供しています

計画から改善までのトータルサービス	概要
セキュリティプロダクト導入・構築支援	ニーズに合わせたセキュリティ製品の選定や導入・セキュリティポリシーの設定なども行い総合的なセキュリティ製品導入の実現を支援します
サイバーセキュリティ訓練サービス （インシデント対応訓練、標的型攻撃メール訓練）	セキュリティインシデント対応の訓練や不審メールを模した訓練メールを送付し、社員が適切な対応ができるか確認する訓練をご提案します
サイバーセキュリティ教育サービス （セキュリティ教育、セキュリティコンテンツ提供）	経験豊富な講師による実践的な演習を通じてセキュリティ対策の本質を自ら試行できるセキュリティ人材の育成を支援します
マネージドセキュリティサービス (MSS)	お客様ご担当者様に代わり、24時間365日フルタイムで不正アクセス・攻撃を監視し、インシデント発生時には適切な対応を実施します
脆弱性診断サービス（IT系）	システムやWebアプリケーション、無線LANなどへの悪意ある攻撃を受ける前に、セキュリティリスクを検知し、防御する脆弱性対策を支援します
脆弱性診断サービス（クラウド）	AWS等のクラウドサービスを利用しているシステに対し、管理ルールの不備や権限設定ミスなど情報漏洩や内部統制強化の観点から診断を行います
セキュリティ・アドバイザリーサービス （アドバイス、サイバー保険）	日々行っているセキュリティ運用の中で疑問や確認したい状況が発生した場合に、セキュリティ専門チームがアドバイスを行います
セキュリティトピックス提供サービス	多岐にわたる情報源から最新かつ信頼性の高いセキュリティ情報を集約してお届けします

ランサムウェア対策ソリューションマップ

事前対策、事後対策別に
技術的対策と人的対策を組み合わせることがポイントです



サイバーセキュリティ訓練サービス

サイバー攻撃に見舞われた場合、いかに素早く初動対応ができるかが被害軽減の鍵となります。
有事の際に想定通りに行動できるか、実際の攻撃を想定した形式で確認する
「**サイバーセキュリティの避難訓練**」を実施いたします。

■ インシデント対応訓練サービス

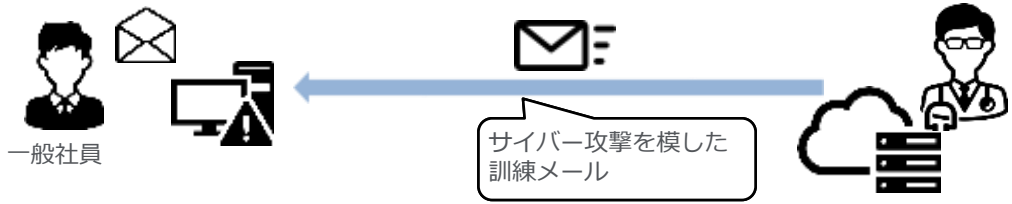
情報システム部・CSIRT向け

**セキュリティインシデント（不正アクセス、情報漏えい事件等）が発生したと想定し、
貴社の担当組織が適切な対応を施せるか確認する訓練をご提案します。**

■ 標的型攻撃メール訓練サービス

全社員向け

**サイバー攻撃に用いられる不審メールを模した訓練メールを送付し、
貴社の社員が不審メールに気づけるか、適切な対応ができるか確認する訓練をご提案します。**



■ ショートメール詐欺訓練サービス

**携帯端末でのショートメール利用についても
リテラシー向上が必要になっています。**

ショートメールは技術的対策が困難

セキュリティ・アドバイザリーサービス

サブスクリプションサービス：月40時間程度からのご契約（専任チームによるエスカレーション支援）
セキュリティ定例会等の参加・助言、サイバー攻撃・脆弱性への対応策等、セキュリティ全般の相談窓口

セキュリティ資格を有する専門家が技術的な
アドバイス対応策の策定を支援します

1 インシデント対応 業務支援

- ✓ 貴社インシデントフローに従って対応を行います。
- ✓ 侵入経路の特定は行わず、復旧優先で対応にあたります。

2 定例会議 運営支援

- ✓ 定例会議に出席します。
- ✓ 月次定例(1回/月)および週次定例(4回/月)の資料作成を支援します。

3 サイバーセキュリティ 演習支援

- ✓ NISC分野横断的演習(1回/年)の準備を支援します。
- ✓ 事前説明会および意見交換会に対する準備を行います。
- ✓ 演習当日サブコントローラーとして、演習をファシリテーションします。

4 ワークショップ その他

- ✓ セキュリティトピックスの作成、セキュリティ教育資料作成など、契約工数の中で対応を行います。

ご清聴有難うございました

サービスのお問い合わせ
株式会社インフォメーション・ディベロプメント
サイバーセキュリティ事業本部

marketing@idnet.co.jp
03-3262-9171