Soliton®

MWS2023 Pre Meeting
研究テーマのアイデアを求めて
我々は現場の奥地へ向かった

インシデントレポートから見えてくること

2023年6月29日

株式会社ソリトンシステムズ
荒木 粧子

インシデントレポート例

全体傾向の分析レポート

- ベライゾン：DBIR2023（2023年データ漏えい/侵害調査報告書）
  - https://www.verizon.com/business/resources/reports/dbir/
- 警察庁：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
  - https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

業界団体・コミュニティでの事例紹介

- サイバー情報共有イニシアティブ J-CSIP（ジェイシップ）
  - https://www.ipa.go.jp/security/j-csip/about.html

被害組織からの調査報告

- 大阪急性期・総合医療センター： 情報セキュリティインシデント調査委員会報告書
  - https://www.gh.opho.jp/important/785.html

DBIR2023: データ漏えい/侵害トレンド

DBIR2023では、2021/11/1～2022/10/31に発生した16,312件のセキュリティインシデントを分析、
そのうち 5,199件でデータ侵害を確認

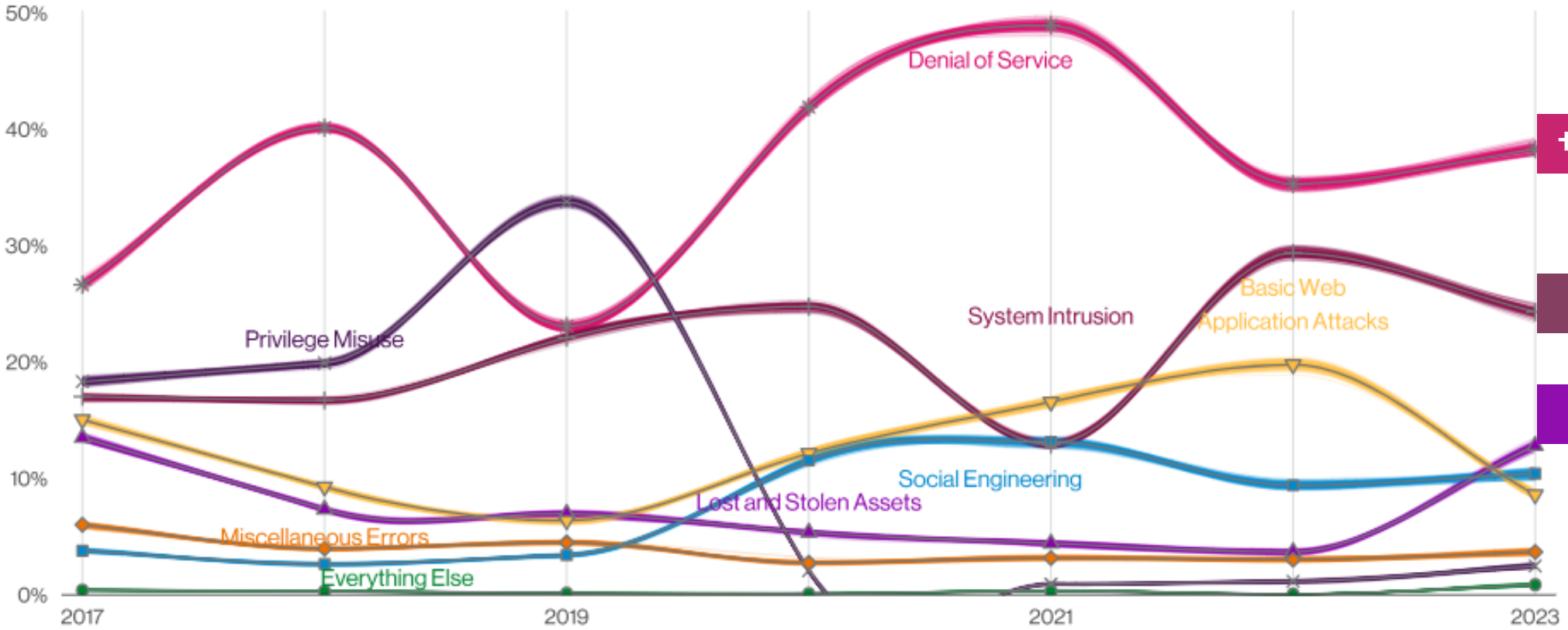


Figure 25. Patterns over time in incidents

サービス拒否（DoS）

システム侵入

資産の紛失・盗難

2023年データ漏洩/侵害調査報告書(Verizon, 2023)
https://www.verizon.com/business/resources/reports/dbir/2023/incident-classification-patterns-intro/

DBIR2023: 主なデータ漏えい/侵害要因

- 主なデータ漏えい/侵害
  - 侵害の83%が外部アクター
  - 侵害の74%が人的要因
    - エラー、誤使用、盗まれた認証情報の利用、ソーシャルエンジニアリング
  - 侵害の49%が認証情報の利用
  - 侵害の24%がランサムウェア

- 外部要因(エラー・誤使用除く)
  - 認証情報の利用: 約50%
  - フィッシング: 約15%
  - 脆弱性:約5%

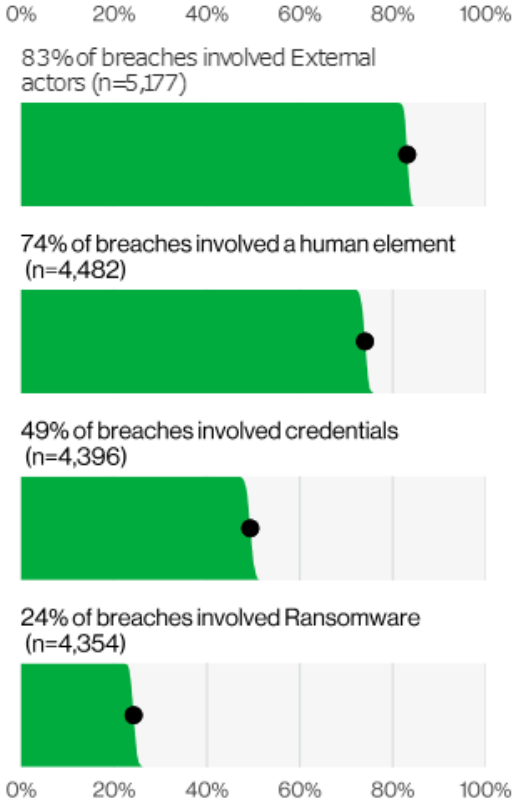


Figure 6. Select key enumerations

主なデータ漏えい/侵害の件数

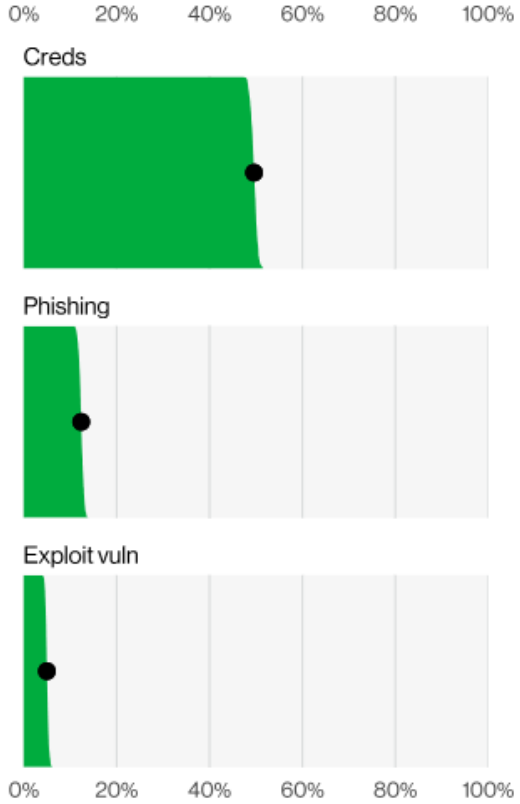


Figure 7. Select enumerations in non-Error, non-Misuse breaches (n=4,291)

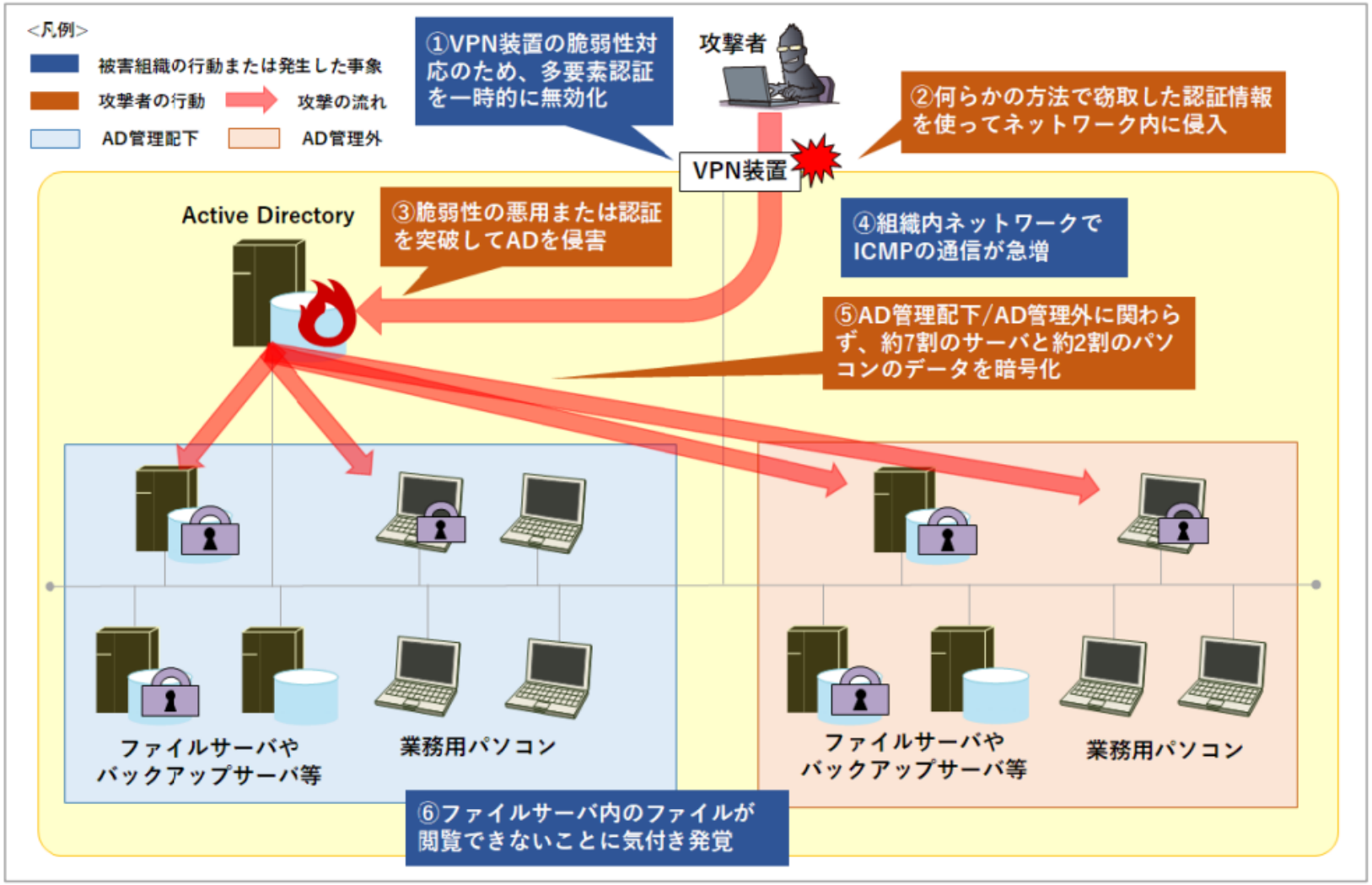
エラーや誤使用ではない
データ漏えい/侵害の件数

2023年データ漏洩/侵害調査報告書(Verizon, 2023)
https://www.verizon.com/business/resources/reports/dbir/2023/summary-of-findings/

J-CSIP運用状況[2022年10-12月]より

- 初期侵入
  - 多要素認証を一時的に無効化したVPN経由での侵入
    - 脆弱性対応のための一時措置※（1週間程度の間）
    - 窃取済み認証情報が悪用
- 侵害範囲拡大と暗号化
  - AD侵害
    - Zerologon(CVE-2020-1472)あるいは、脆弱なパスワードの突破
  - ランサム配布
    - PsExecでランサム配布・実行
    - サーバーの70%、PCの20%のデータが暗号化
    - クラウドは無事(分離されていた)
    - バックアップサーバーも暗号化され復旧に利用できず

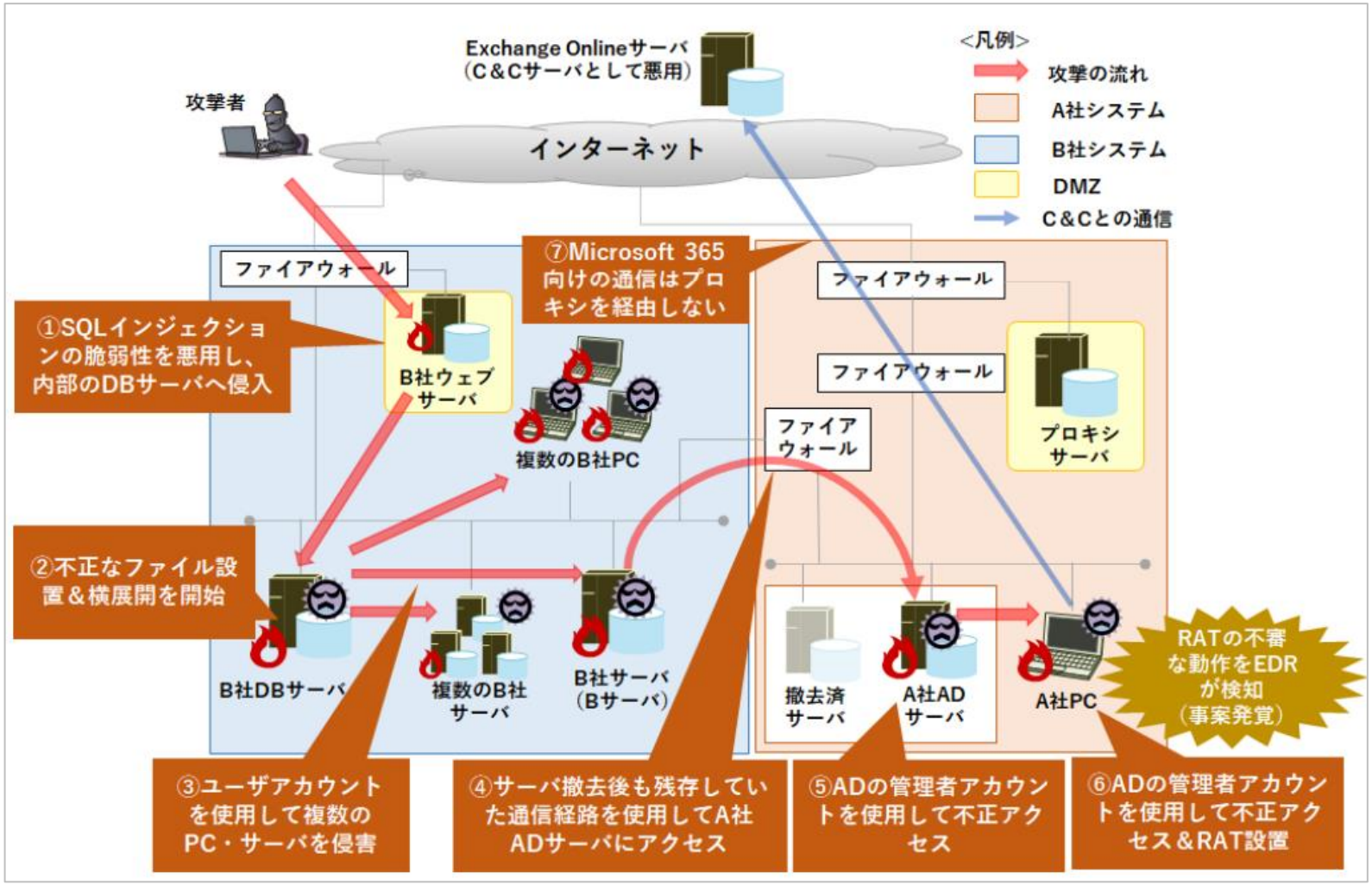
※なお、多要素認証を無効化しないと脆弱性対応ができなかった要因については情報提供外のため不明



48. サイバー情報共有イニシアティブ(J-CSIP) 運用状況 [2022年10月～12月] (IPA、2023年2月9日)
https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/000107999.pdf

J-CSIP運用状況[2023年1-3月]より①

- 初期侵入
  - 海外グループ企業(B社)のサーバ
    - SQLインジェクションでDBサーバに侵入
    - リモートコード実行可能な脆弱性あり
    - 匿名アカウントが有効
    - ADユーザーはDBサーバのCドライブ書き込み権限あり
- 侵害範囲拡大
  - B社複数端末に侵害拡大
    - Cobalt Strike利用
  - A社ADサーバに不正アクセス
    - A社のサーバー撤去後にも残存していた通信経路が悪用された
    - 退職済みの外部業者に付与していたID とパスワードが悪用されAD侵害 ※
  - A社ADから複数のA社端末を侵害
    - Microsoft社のExchange Onlineサーバを C2サーバとして悪用する遠隔操作プログラム (RAT)がEDRで検知されて発覚



※当該ID/パスワードが悪用された原因は不明

49. サイバー情報共有イニシアティブ(J-CSIP) 運用状況 [2023年1月～3月](IPA、2023年5月11日)
https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/fy22-q4-report.pdf

J-CSIP運用状況[2023年1-3月]より②

- 命令方法
  - 攻撃者が作成したメールアカウントでExchange Onlineに接続
  - 特定件名のメール添付ファイルの暗号化命令を復号して実行
  - 命令実行結果を暗号化して、特定件名のメール添付ファイルに格納
- Exchange OnlineがC2となることの課題
  - 正規通信とみなされ攻撃検知は一般的には困難
  - Microsoft 365通信はプロキシをバイパスすることが負荷の観点から推奨されている
    - プロキシに痕跡が残らない

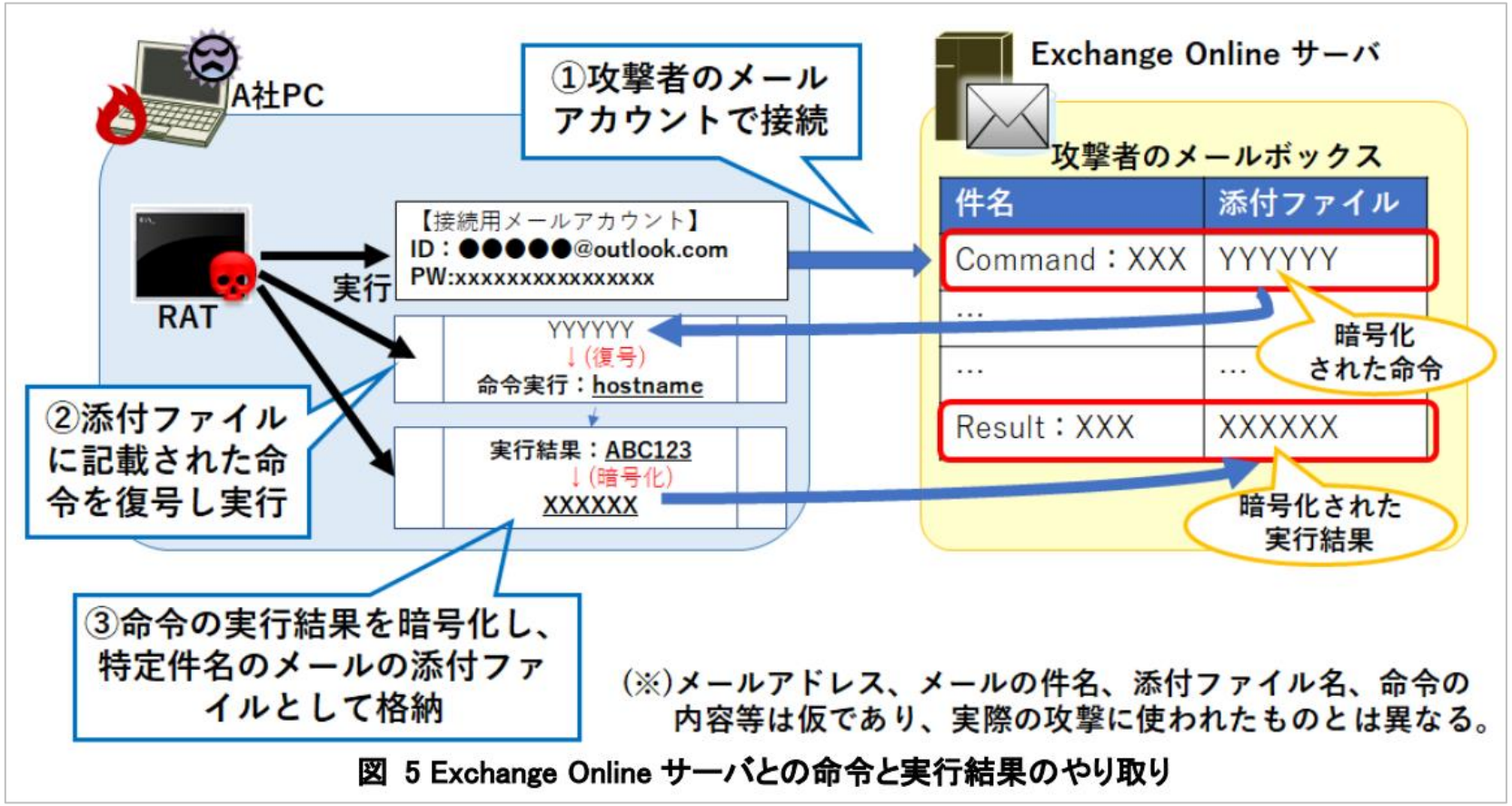


図 5 Exchange Online サーバとの命令と実行結果のやり取り

49. サイバー情報共有イニシアティブ(J-CSIP) 運用状況 [2023年1月～3月](IPA、2023年5月11日)
https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/fy22-q4-report.pdf

インシデントレポートから見えてくること

- 全体傾向の把握
  - 森を見ることも大事
    - 情報の切り出し方によっては、見え方が異なるかもしれないことに注意

- 個別事案からの共通点
  - Weakest Linkが狙われる
    - パッチ適用のため1週間だけMFAを無効化していた
    - 脆弱性が放置されていた
    - 匿名アカウント(Guest)が有効だった
    - 退職済み外部業者用ID/Passwordが利用された
    - 過去必要だった通信経路を放置していた　等

- その他
  - 情報共有は、被害予防に有効(公表組織・公表の取り組みに感謝！)