JPCERT CC®

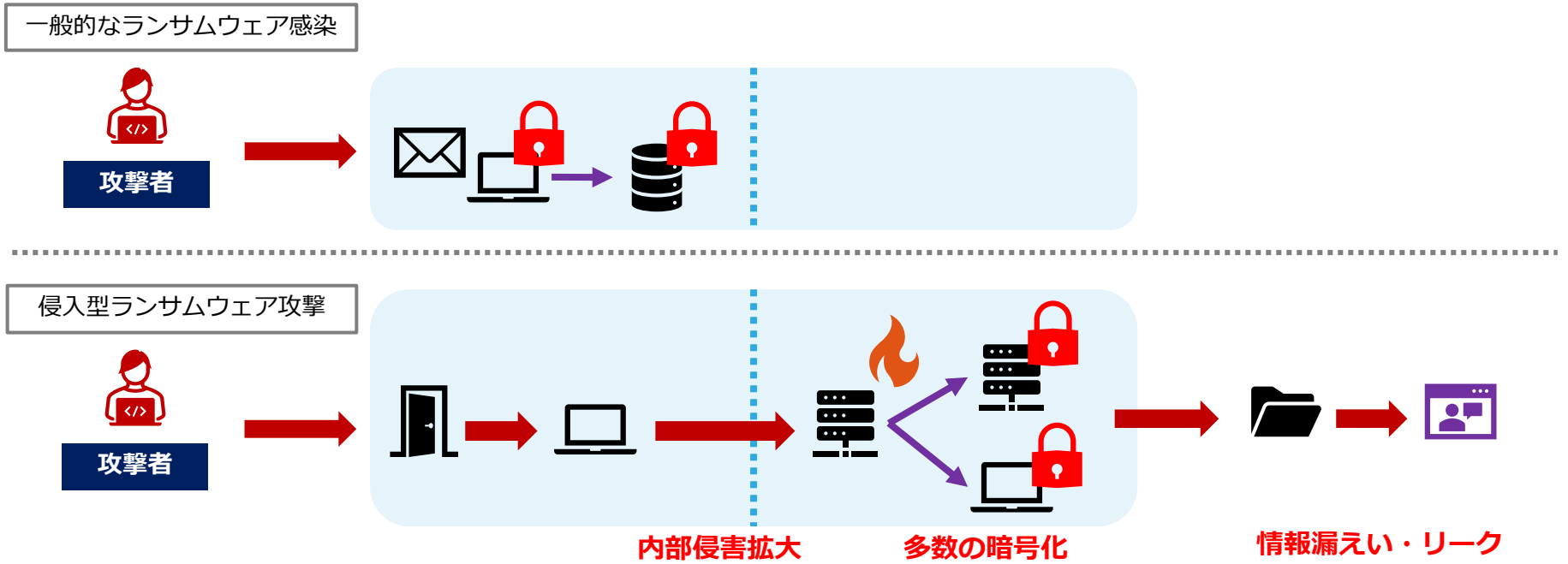
侵入型ランサムウェア攻撃の初動対応のポイント ～早期の業務復旧のために～

2022年3月

一般社団法人JPCERTコーディネーションセンター

侵入型ランサムウェア攻撃とは？

- “標的型～”と呼ばれることも ←特定組織／業界だけが狙われるわけではない
- 組織のNW**奥深くまで侵入**され、**情報が漏えい**／リークサイトに掲載される



どんな方法で侵入されるのか

- メール、改ざんサイト閲覧、別のマルウェア感染経由、SSL-VPN製品の脆弱性などさまざまな原因

⇒2020年以降の国内被害の多くでSSL-VPN経由での侵害

- 最近の海外事例から
  - SSL-VPN経由以外にも多くの侵入経路
  - Windows Exchange Serverの脆弱性
  - VMware HorizonのLog4j脆弱性
  - その他Webサーバーのさまざまな脆弱性

よく見られる初動対応上の問題点

- ランサムウェアの種別特定がされていない
- 侵入原因箇所の調査・対処がされていない

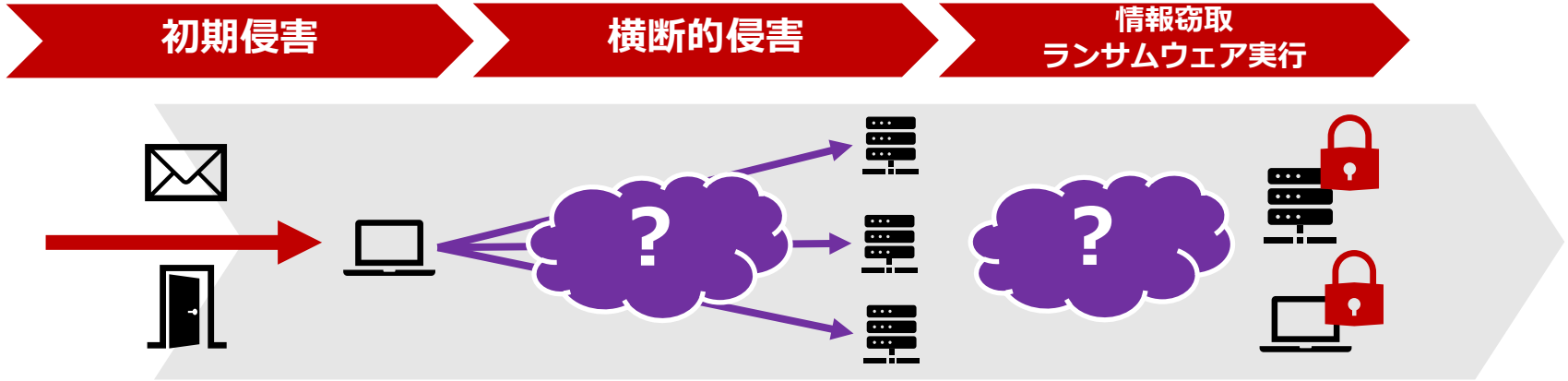
「復旧優先」のため、後回しにされるか、そもそも着手されていない対応事例が見られる

システム停止／NW停止の期間を長引かせてしまっている恐れ

攻撃の流れと調査の流れ

- 一般的な不正アクセス調査の手順では時間がかかるため、速やかな復旧に影響が出るケースも
- ログを保存したサーバーも被害を受けるなど、通常の調査が困難なケースも

攻撃の流れ⇒



←（一般的な）調査の流れ

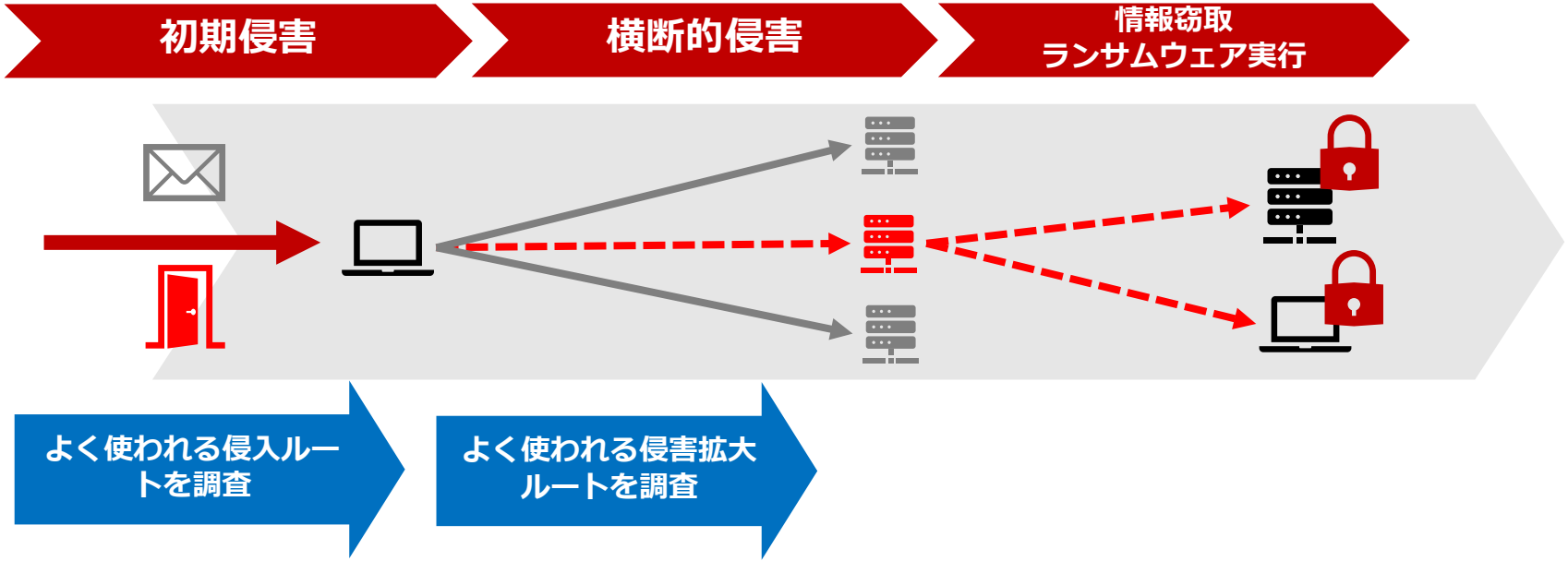
侵害経路・範囲の特定

調査対象端末のフォレンジック

各種ログ調査

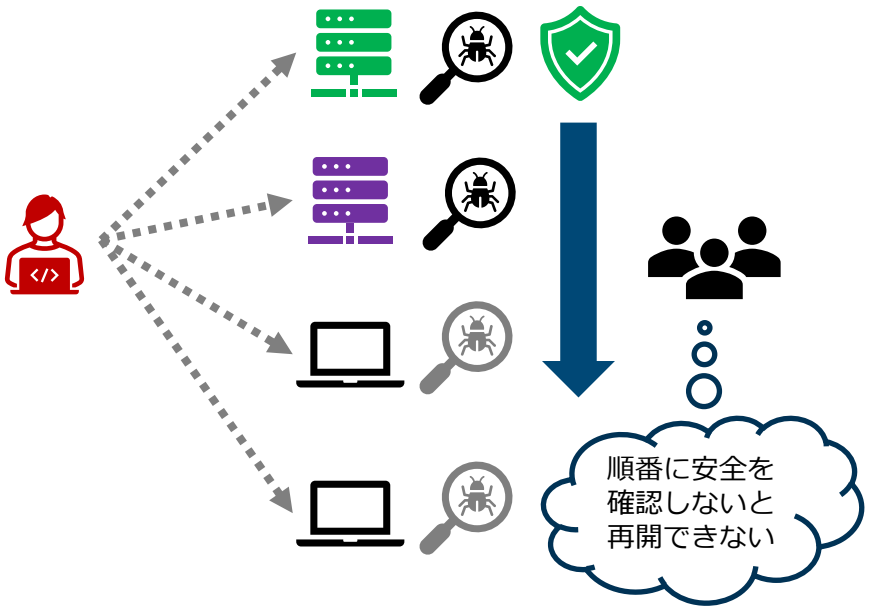
侵入原因の候補を絞り込んだ調査アプローチ

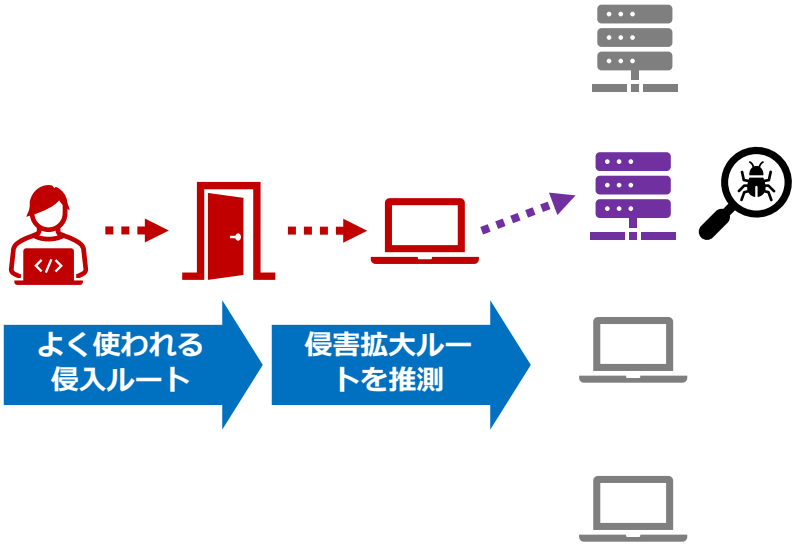
- ある程度、侵入経路の候補を絞り込み、調査範囲を狭める



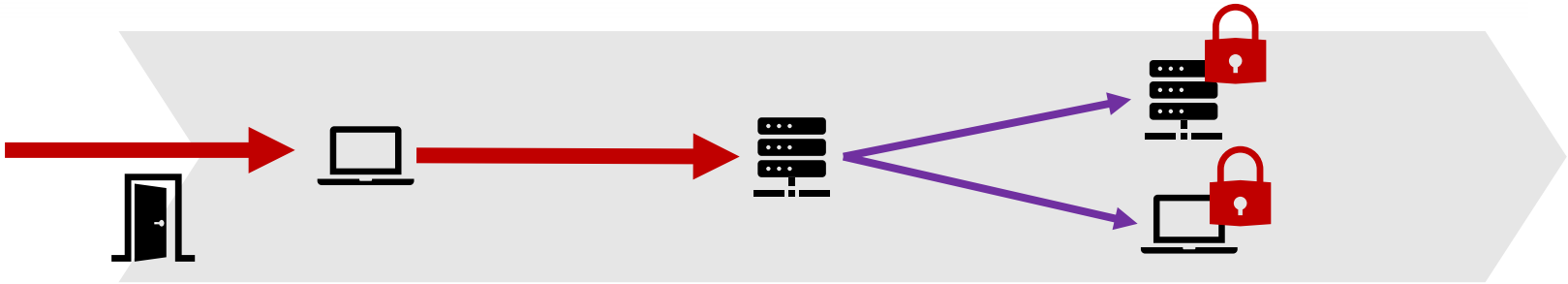
復旧までの時間短縮のための原因調査

- 侵害された可能性がほぼないサーバー／端末の調査を待たずにある程度復旧させることが可能





調査対象の絞込み



よく使われる侵入ルートを調査

- SSL-VPN接続のログに不審なログイン履歴がないか
- 不審なログインでどのアカウントが使われたのか
- 不審なログインでどの端末にアクセスがされたのか

例）SSL-VPN製品のログ調査

よく使われる侵害拡大ルートを調査

- 侵入された可能性のある端末から他の端末やサーバーに対して不審なアクセスをしていないか
- ADサーバーのログ上で特定のアカウントの不審な動きがないか
- ADサーバー自体が侵害されていないか

例）ADサーバーのログ調査

【留意点】

- ランサムウェアの種類によっては感染拡大するケースも
- 攻撃者によっては、NW内部に侵入したままのケースも

侵入方法をどうやって推測するか

被害現場ですぐに見つかる情報

拡張子

脅迫文

検知名

専門的知見から得られる情報

ランサムウェア種別の特定

攻撃グループ推定

初動対応判断に資する情報

・何らかの対処をしないとNW上で感染拡大するタイプかどうか

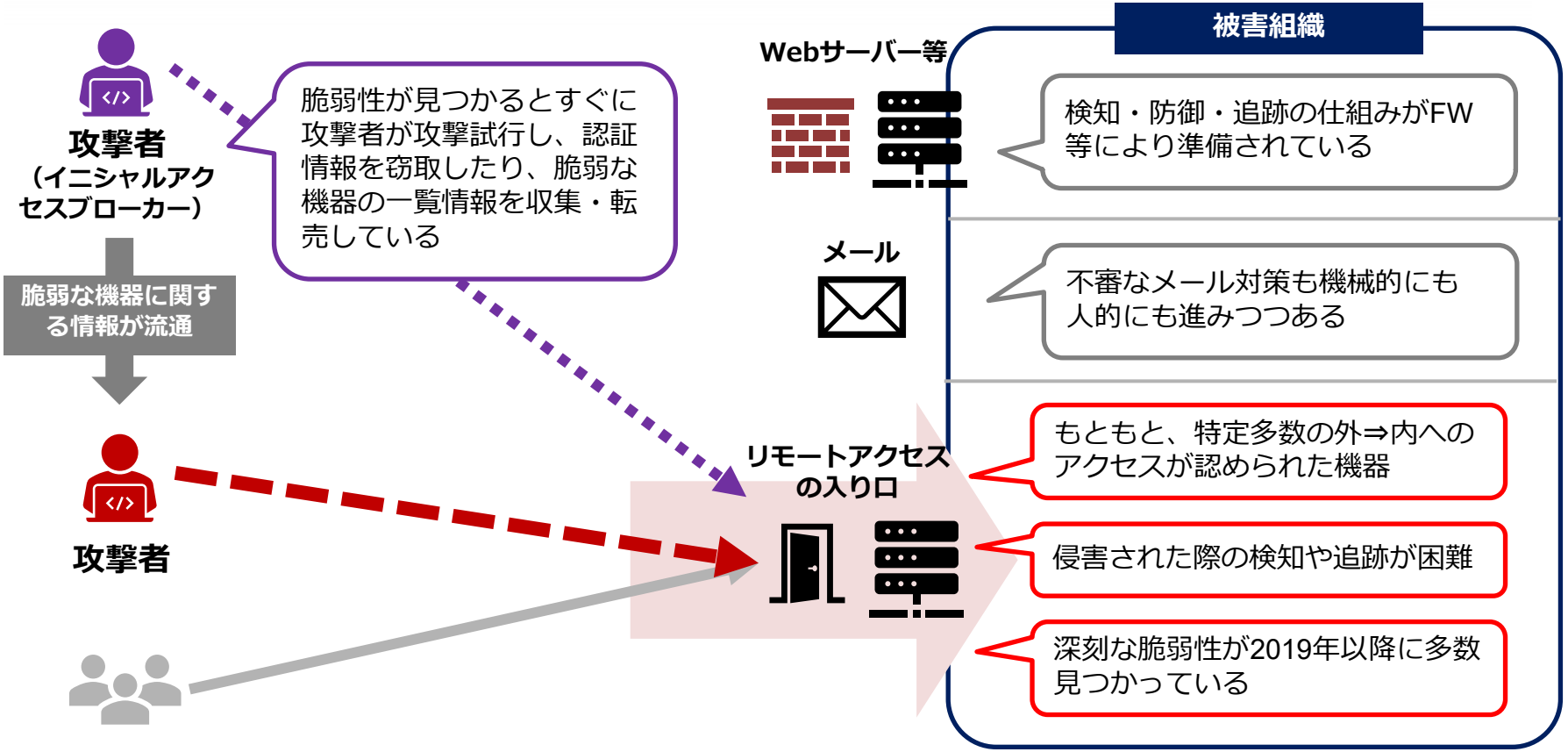
・**どのような初期侵入方法を用いることが多いか**

・侵入後にどのように横断的侵害をしていくか

・情報を外部に持ち出すか

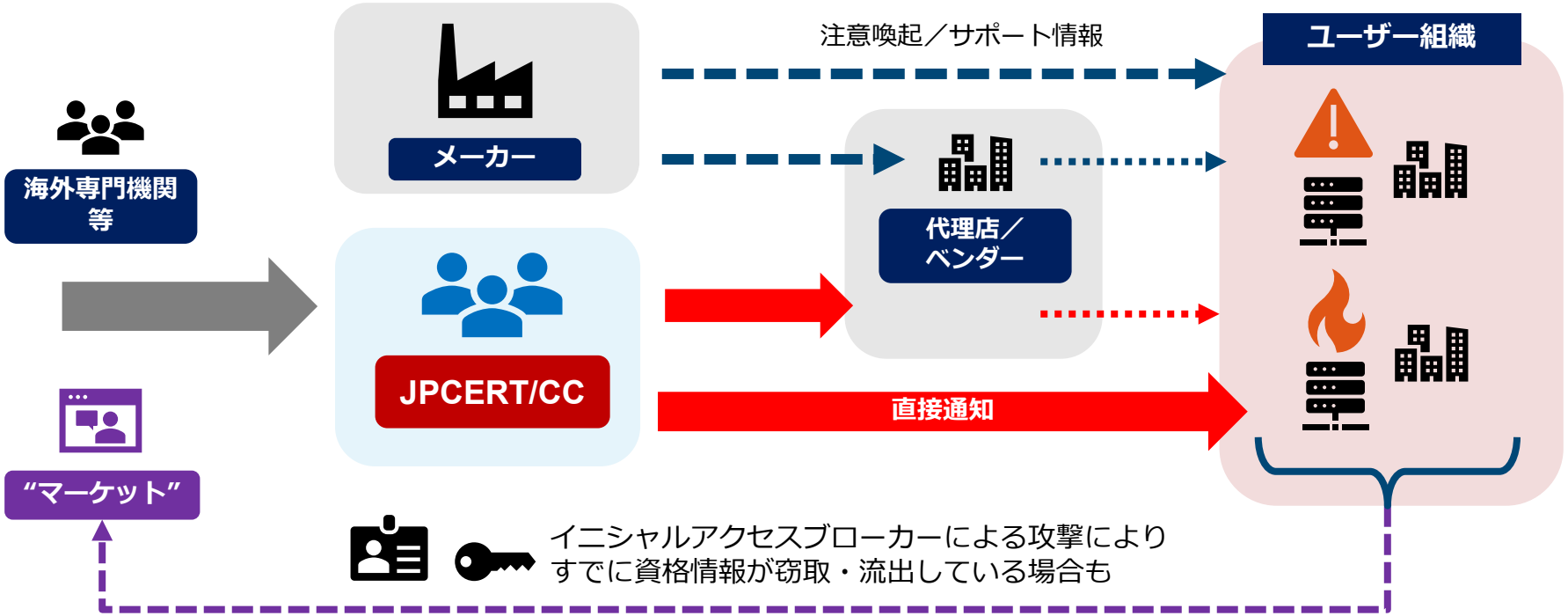
・ランサムウェア実行後もNW内に残留し続けるか

なぜSSL-VPN製品から侵入されるケースが多いのか



SSL-VPN製品利用組織へのJPCERT/CCからの通知

- 海外からの情報提供や調査により、脆弱なままの機器や、すでに脆弱性の悪用により認証情報が窃取された機器の利用組織に対して通知オペレーションを実施



どうやって「備える」か

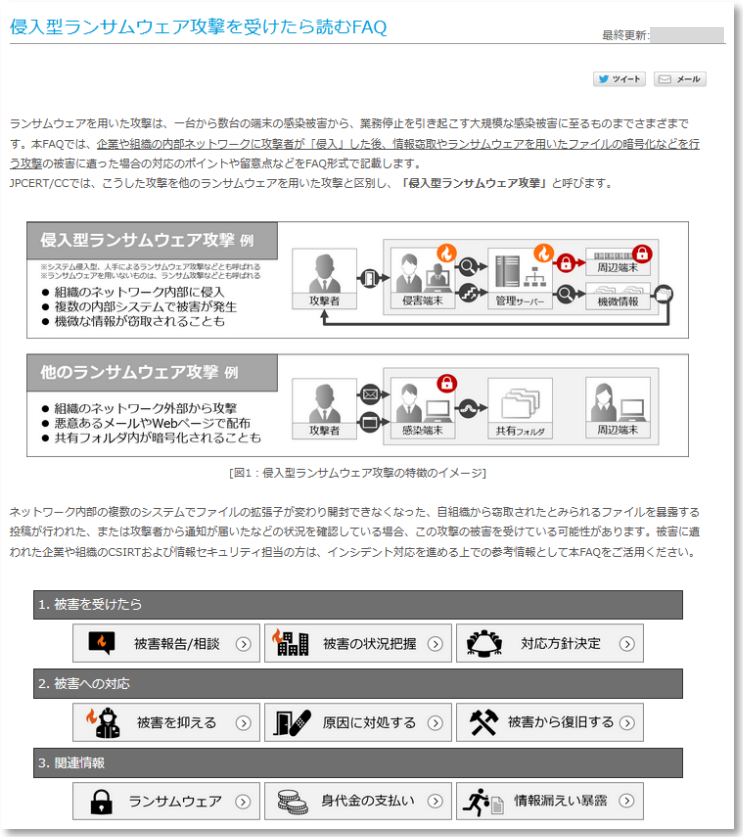
- **SSL-VPN製品の点検**
  - 最新版のアップデートに対応済みか確認

  <2019年以降にJPCERT/CC等から注意喚起のあった製品（抜粋）>
    - PulseSecure製品
    - Fortinet製品
    - SonicWall製品
  - 過去にJPCERT/CCから通知が来ていないか確認
  - すでにイニシャルアクセスブローカーによって認証情報が窃取されている可能性があるため認証情報のリセットなどの対応が必要
- **これまでに注意喚起があった脆弱性の対応**
  - Microsoft Exchange Server
  - Log4j脆弱性
  - その他
- **バックアップの取得**
  - ランサムウェア被害を受けないように、オフラインでのバックアップが重要
  - こまめなバックップが早期復旧につながる

まとめ

- 再発防止のためだけでなく、早期復旧のためにも侵入原因の早期特定が重要
- 侵入原因を早期に特定するためには、ランサムウェアの種別を特定して、攻撃グループがよく用いる侵害方法に関する情報を得ることが必要
- （上記情報を得るために）専門的知見を持つセキュリティ専門企業、専門機関、ITベンダー、警察への早期の相談が重要
- 今一度、SSL-VPN製品の点検を！！

侵入型ランサムウェア攻撃被害の初動対応FAQ



(1) コンテンツ内容

- 攻撃を受けた場合の対応のポイントや留意点、よくある質問をFAQ形式を掲載（html形式）
- 攻撃を受けた後の対応に特化したコンテンツ

(2) コンテンツ想定読者

- 被害組織のCSIRT／情報セキュリティ担当
- 被害組織を支援するセキュリティベンダー会社
- 被害組織の支援や捜査にあたる都道府県警　　など

(3) コンテンツ構成

1. 被害を受けたら：被害報告/相談、状況把握、対応方針決定
2. 被害への対応　：被害最小化、原因対処、被害復旧
3. 関連情報　　：ランサムウェア、身代金支払い、情報漏えい調査

(4) コンテンツの期待効果

- 攻撃の全体像や侵害原因を速やかに特定
- 不必要なNW停止などを最小限に留めて対応
- 専門機関等へ速やかに報告・連絡

JPCERT/CC 「侵入型ランサムウェア攻撃を受けたら読むFAQ」より
https://www.jpcert.or.jp/magazine/security/ransom-faq.html

参考資料

【初動対応／調査の参考資料】

- 侵入型ランサムウェア攻撃を受けたら読むFAQ
  https://www.jpcert.or.jp/magazine/security/ransom-faq.html
- ログを活用したActive Directoryに対する攻撃の検知と対策
  https://www.jpcert.or.jp/research/AD.html

【SSL-VPN製品の脆弱性情報】

※下記は主要な注意喚起を抜粋したものです。他の製品や、SSL-VPN製品以外の重要な脆弱性に関する注意喚起情報もJPCERT/CCのWebサイトからご参考ください。

- 複数の SSL VPN 製品の脆弱性に関する注意喚起
  https://www.jpcert.or.jp/at/2019/at190033.html
- Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性 (CVE-2018-13379) の影響を受けるホストに関する情報の公開について
  https://www.jpcert.or.jp/newsflash/2020112701.html
- SonicWall SMA100シリーズの複数の脆弱性に関する注意喚起
  https://www.jpcert.or.jp/at/2022/at220004.html
- SonicWall製SMA100シリーズの脆弱性（CVE-2021-20016）に関する注意喚起
  https://www.jpcert.or.jp/at/2021/at210006.html
- SonicWall製のSMA100シリーズの脆弱性（CVE-2021-20034）に関する注意喚起
  https://www.jpcert.or.jp/at/2021/at210042.html

お問い合わせ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

- Email：ew-info@jpcert.or.jp
- https://www.jpcert.or.jp/

インシデント対応相談

- Email：info@jpcert.or.jp
- https://www.jpcert.or.jp/form/

制御システムインシデントの報告

- Email：icsr-ir@jpcert.or.jp
- https://www.jpcert.or.jp/ics/ics-form.html

脆弱性に関するお問い合わせ

- Email：vultures@jpcert.or.jp
- https://jvn.jp/