

CODEBLUE2023 OpenTalks

ファストフォレンジックにおける マルウェア解析の活用

2023/11/9

NEC サイバーセキュリティ戦略統括部
リスクハンティング・アナリシスグループ
竹内俊輝、松本隆志

\Orchestrating a brighter world

NECは、安全・安心・公平・効率という社会価値を創造し、
誰もが人間性を十分に発揮できる持続可能な社会の実現を目指します。

About Us



竹内 俊輝

NEC サイバーセキュリティ戦略統括部
リスクハンティング・アナリシスグループ
フォレンジック・アナリスト



松本 隆志

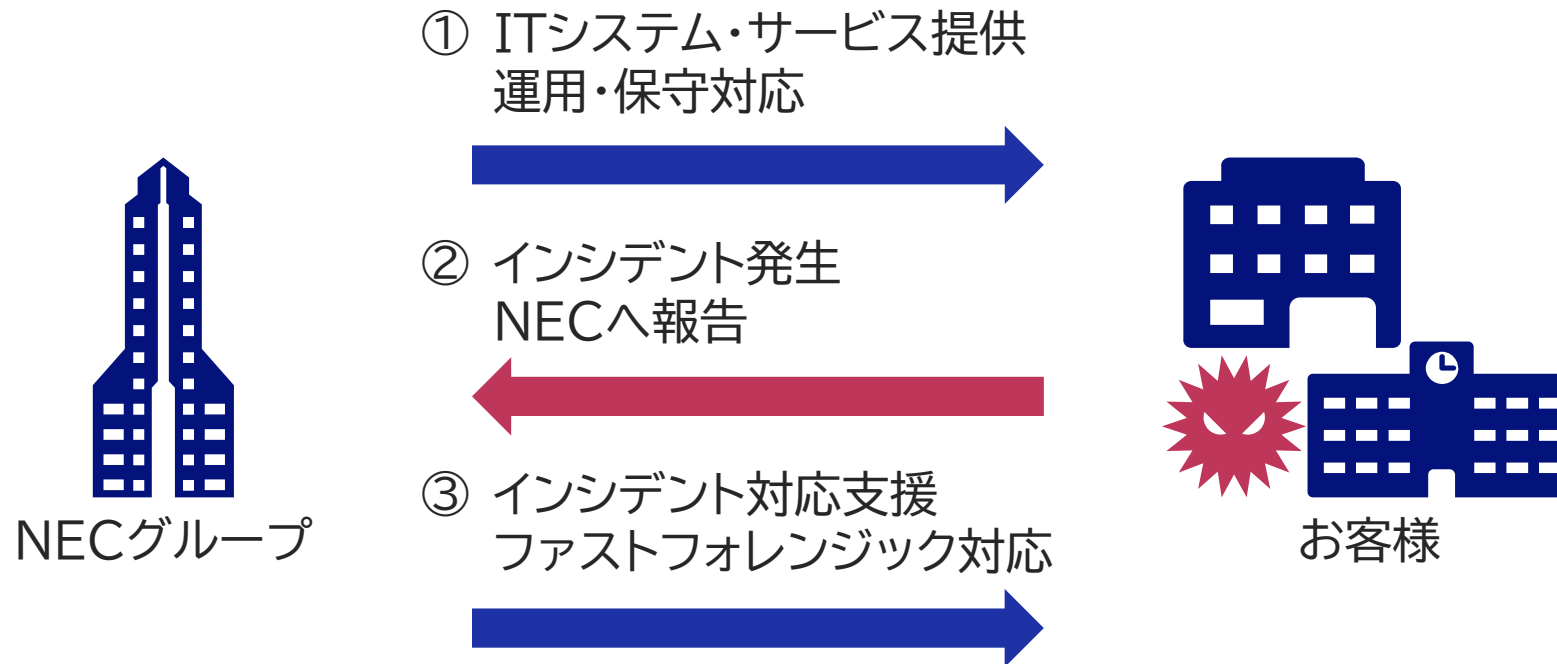
NEC サイバーセキュリティ戦略統括部
リスクハンティング・アナリシスグループ
フォレンジック・アナリスト

目次

1. RIHTにおけるインシデント対応・統計
2. ファストフォレンジックの課題
3. マルウェア解析の活用事例
4. 現状の課題と今後の展望

RIHTで対応するサイバーインシデント

リスクハンティンググループ(RIHT)では
NECグループのお客様先で発生したインシデントを対応



RIHTが行うインシデント対応

ファストフォレンジック[†]を基本とした対応を実施

[†] 早急な原因究明、侵入経路や不正な挙動を把握するため、必要最低限のデータを抽出及びコピーし、解析すること^{*1}

Windows端末で解析するデータの例

- イベントログ
- ジャーナル
- レジストリ
- プリフェッチ など

Linux端末で解析する対象の例

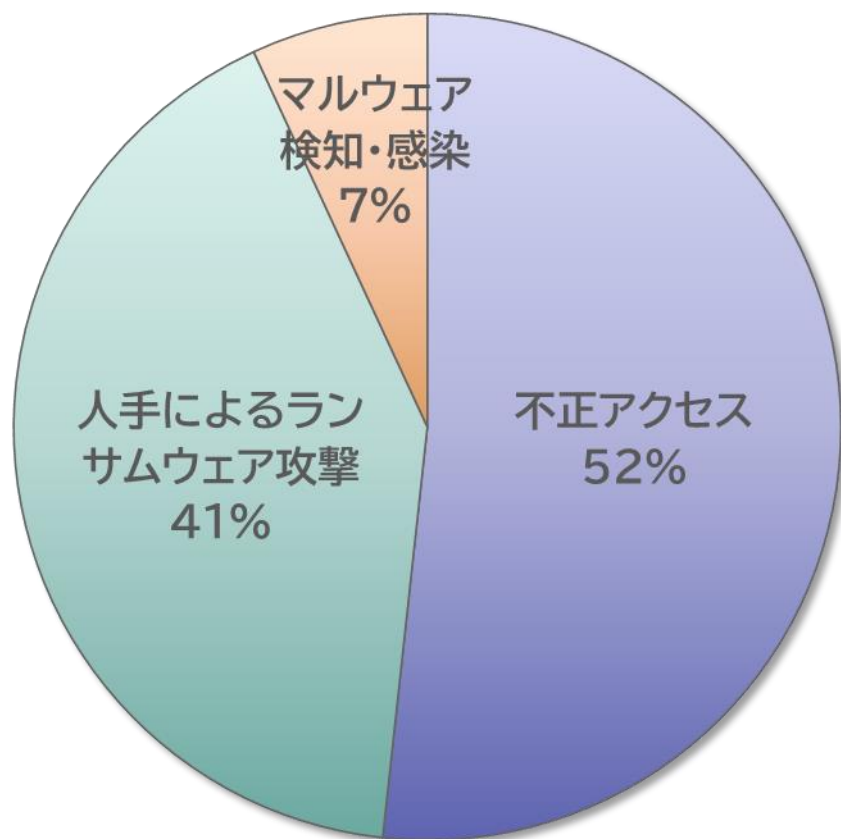
- ログ(SSH、HTTPなど)
- cron
- サービスの設定ファイル
など

早急な実態解明/ビジネスの早期復旧を目的とする事案へ対応
必要最低限のデータを解析するファストフォレンジックを実施

(^{*1}) デジタル・フォレンジック研究会 | 証拠保全ガイドライン第8版: <https://digitalforensic.jp/wp-content/uploads/2021/05/gl8-20210520.pdf>

RIHTで対応したインシデントの統計

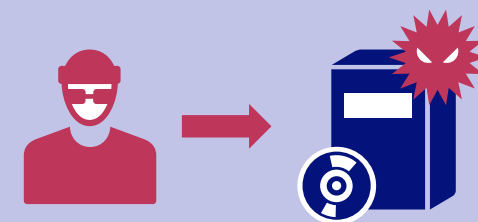
RIHTで対応したインシデントの発生原因を大きく3つに分類



RIHTで対応した事案の分類結果

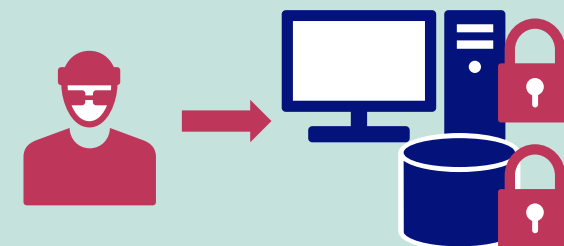
不正アクセス

既知の脆弱性や自作したアプリケーションの脆弱性を悪用された事案



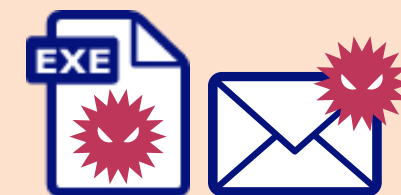
人手によるランサムウェア攻撃

組織内ネットワーク(NW)に侵入し、ランサムウェアを実行された事案



マルウェア検知・感染

メールに添付されていたマルウェアを開いた/セキュリティソフトにより、マルウェアを検知した事案



マルウェアが関連するインシデント対応件数の推移

	RIHTへのマルウェアが関連する インシデント報告件数 (検知・感染未遂含む)	RIHTでの ファストフォレンジック 実施件数
FY2020	2件	1件
FY2021	8件	4件
FY2022	9件	6件

RIHTでファストフォレンジックを実施するインシデントのうち
マルウェアが関連する事案が年々増加している

インシデント対応におけるファストフォレンジックの課題

情報漏えいの可能性に関する見解提示

- ・ 情報漏えいの可能性を複数の観点から説明する必要がある
- ・ マルウェアに情報を持ち出す機能が存在するか説明を求められる

侵害端末上のファイル再利用の可否判断

侵害された端末上のファイルを再利用したいと要望があるときに安全であるか、使用しても問題ないかの説明を要求される

公開情報に存在しないマルウェアの動作説明

公開情報からマルウェアのハッシュ値を使った情報収集ができない場合、マルウェアの動作は検知名等による推定での説明となる。

マルウェア解析による課題の解決

課題

情報漏えいの可能性に関する見解提示

対策

マルウェアを解析し、外部への通信の有無・情報漏えいに関する機能を明らかにする

フォレンジック調査以外の観点の説明材料を増やす

侵害端末上のファイル再利用の可否判断

再利用の
要望のあるファイルを調査

マルウェアを解析し、
寄生する動作がないか確認

マルウェアによって改ざんされていないか、バックドア等が仕込まれていないかの確認

公開情報に存在しないマルウェアの動作説明

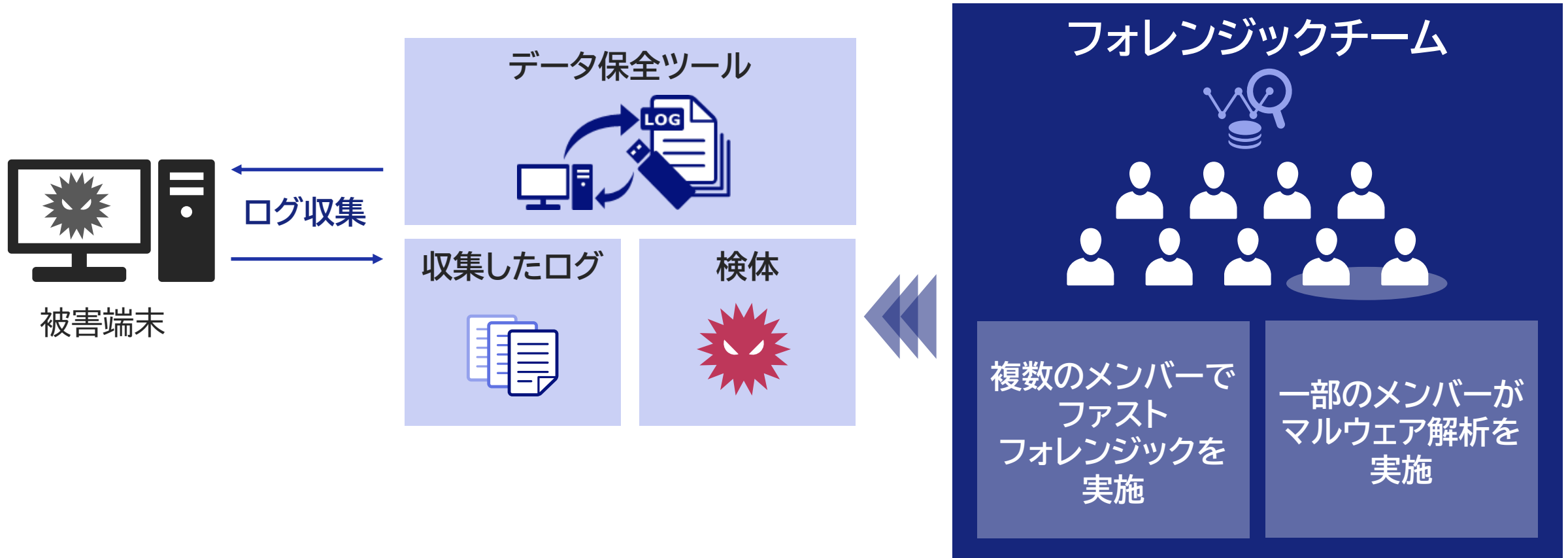
解析結果から
マルウェアの
ファミリを特定

類似の
インシデント/検体の
公開情報を調査

フォレンジックの
調査へ反映

フォレンジックチームの体制

調査に必要なデータを収集し、インシデント対応チームが解析
検体の解析も行い、解析結果をチームに還元



マルウェア解析対応者の作業

ファストフォレンジックだけでは調査が困難な領域をマルウェア解析でサポート

実際の作業の流れ

1. フォレンジックチームによるログ分析で見つかった不審な検体を収集する。
2. 収集した検体の表層解析・動的解析を行う(時間をかけた深い解析は行わない)。
3. 見つかった痕跡をフォレンジックチームメンバーに共有する。

解析中に重点的に見るポイント

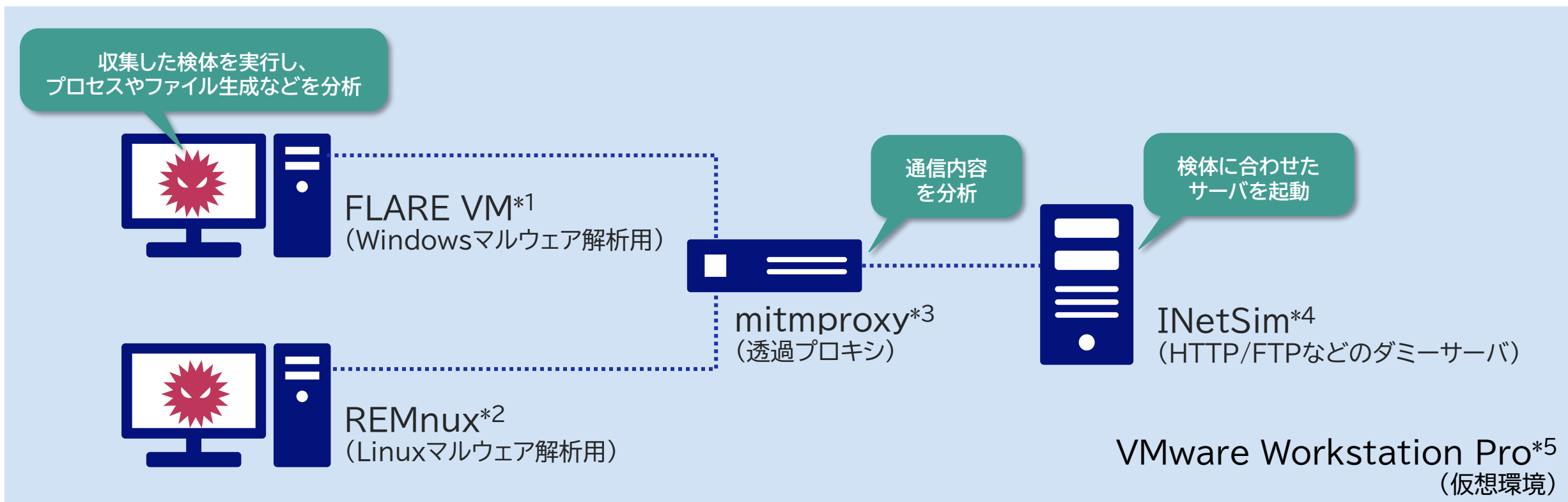
- 通信先
- 生成するファイル
- 永続化の設定 など

解析中にあまり見ないポイント

- RATによって実行されるコマンドの洗い出し
- 既知マルウェアとの差分
- 耐解析技術の詳細な解析

(参考)マルウェア解析環境

マルウェアに感染させない・影響を発生させない構成環境を事前に構築
チームメンバーに共通の解析環境を用意



(*1) <https://github.com/Mandiant/flare-vm>

(*2) <https://remnux.org/>

(*3) <https://mitmproxy.org/>

(*4) <https://www.inetsim.org/>

(*5) <https://www.vmware.com/jp/products/workstation-pro.html>

具体例1:ファストフォレンジックのログとの突合(1)

◆ セキュリティソフトで検知されたファイルを動的解析した事例

- マルウェアの感染経路の特定が目標の一つであった
- ファストフォレンジックの調査で、PsExec*¹実行後に大量のファイル書込みが行われたことを発見



ファストフォレンジックの結果からは2つの可能性が考えられた

- ① PsExecで何らかのマルウェアを実行(ログからPsExecで実行されたコマンドは不明)
- ② フォレンジックから把握できない、ログが残っていない経路からの感染

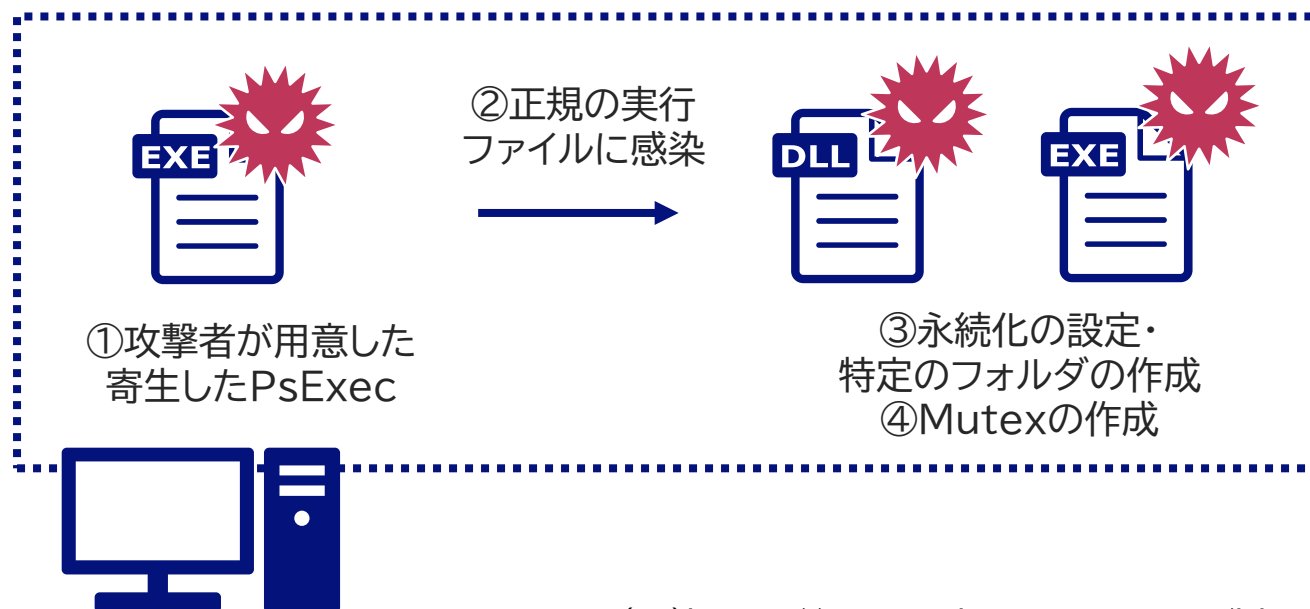
(*1)<https://learn.microsoft.com/ja-jp/sysinternals/downloads/psexec>

具体例1:ファストフォレンジックのログとの突合(2)

◆ 解析の結果、攻撃者が使用したPsExecの実行ファイルが既にマルウェアに寄生されていたファイルの可能性が高いことを説明

- 解析結果を元に公開情報を調査したところ、類似の事例*1を発見
- ログとの突合を行い、ファイルへの書き込み時間から、PsExecによる実行が最も疑いの高い記録

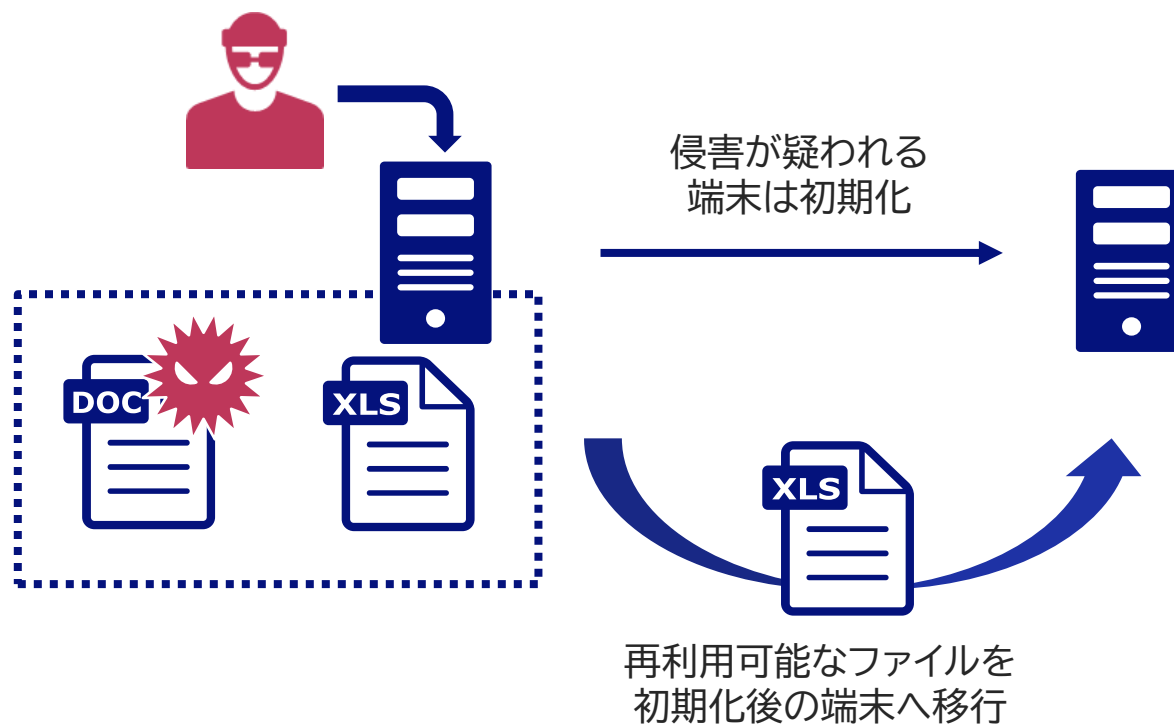
インシデントにおける動作



(*1)<https://www.cybereason.co.jp/blog/threat-analysis-report/8411/>

具体例2：侵害が疑われる端末上のファイルの安全性確認

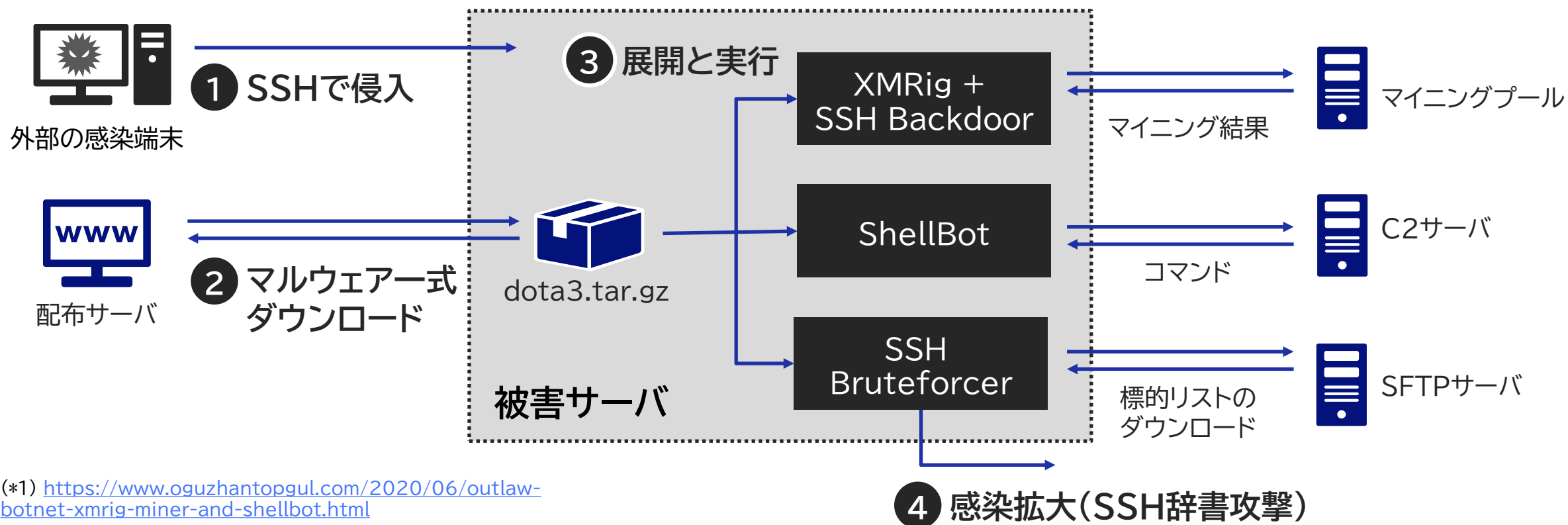
- ◆ 侵害が疑われる端末上で使用していた業務用ファイルを再利用するため、そのファイルの安全性を確認
 - 動的解析を行い不審な動作の有無/マクロの内容を確認
 - 各ファイルについてのリスクを説明し、再利用にあたっての注意点を展開



具体例3: クリプトマイナーを発見した事例

◆ ファストフォレンジック中に発見した実行ファイルを動的解析

- cronに登録されたファイルの特徴や通信先などから攻撃キャンペーン*1を特定
- 特定したキャンペーンの情報から芋づる式に痕跡を発見



(*1) <https://www.oguzhantopgul.com/2020/06/outlaw-botnet-xmrig-miner-and-shellbot.html>

マルウェア解析のフォレンジックへの貢献

1 インシデントの発生原因・影響に対する複数観点から見解の提示が可能

- 攻撃キャンペーンの特定/類似の攻撃事象と紐づけてお客様へ説明を行い、ファストフォレンジックの結果以上の説得力を持たせることが可能となった。
- 使用されたマルウェアや今後再利用したいファイルの解析から、ファイルの安全性やリスクの説明が可能となった。

2 ファストフォレンジック調査の効率化

- 「マルウェアの動作による痕跡」と「攻撃者の操作による痕跡」の識別がある程度可能となった。
- マルウェア解析で発見した動作を、ファストフォレンジックの調査に活用することができるようになった。

NECでのマルウェア解析における3つの課題と展望(1)

◆ 課題1: マルウェア解析者の不足

フォレンジックチーム内でマルウェア解析を行えるメンバーは、現状2～3名程度

ハンズオン形式のマルウェア解析勉強会を実施し、解析メンバーを育成/増強

◆ アクション1: マルウェア解析者の育成(今年度から実施中)

① 解析テーマの選定

育成対象者に解析してもらうマルウェアのテーマを選定する。

② マルウェアの収集

事前に決めたテーマに応じたマルウェアをVirusTotalなどから収集する。

③ マルウェアの解析

育成対象者に収集したマルウェアの解析を実施してもらう。

④ フィードバック

解析結果の報告会を行い、育成対象者にフィードバックする。

約1か月の
サイクル

NECでのマルウェア解析における3つの課題と展望(2)

◆ 課題2: ファストフォレンジック用のログ解析基盤との連携

解析結果をチャットベースでメンバーに共有し、手動でログと紐づけている状態

マルウェア解析を一部自動化し、ELKスタック上のログと紐づけ

◆ アクション2: マルウェア解析の自動化と収集したログとの紐づけ

現在のログ解析基盤



各種ログを
パースして投入



Elasticsearch*1

ログの可視化



Kibana*2



サンドボックス解析

解析結果の投入

(*1) <https://www.elastic.co/jp/elasticsearch>

(*2) <https://www.elastic.co/jp/kibana>

NECでのマルウェア解析における3つの課題と展望(3)

◆ 課題3: 脅威インテリジェンスの活用

インシデント発生時に関連する
攻撃事例等の情報収集を行っている状態

NECが収集した脅威インテリジェンスを
マルウェア解析の場面で活用

◆ アクション3: インテリジェンスグループとの連携



インシデントに関連する
情報を入手する



マルウェア解析者

マルウェアファミリーの早期特定
ログに残る痕跡の抽出の効率化

\Orchestrating a brighter world

NEC