攻撃被害を極小化するための インシデント対応支援ソリューション

大口 恭平　山崎 輝　山根 匡人

要 旨

どれだけサイバー攻撃対策を講じてもセキュリティインシデントをゼロにはできないと言われるなか、サイバー攻撃による被害を封じ込められるかどうかは、インシデント発覚直後から事態が一時的に鎮静化するまでの初動対応の質に大きく左右されます。本稿では、実例を踏まえ、適切な初動対応を実現するためのインシデント対応のあるべき姿と、初動対応をサポートするNECのサービスを紹介します。

KeyWords

サイバー攻撃／インシデントレスポンス／デジタル・フォレンジック／CSIRT／初動対応

1. はじめに

金銭や政治的な悪用を目的とし、企業や団体が持つ情報資産を窃取したり操業を妨害したりするサイバー攻撃が増加しています。機密情報の漏えいなど組織にとって深刻な被害を招くケースでは、マルウェア感染後、攻撃サーバへの通信や内部での権限奪取、機密情報の探索など、攻撃者はいくつかの手順を踏みます。そのため、サイバー攻撃による被害を封じ込められるかどうかは、攻撃をより早い段階で発見し、迅速にインシデント対応を行うことが鍵となります。

本稿では、迅速にインシデント対応を行うためにはどうすれば良いのか、現場の課題や実際の対応例を交えて紹介します（**図1**）。

2. インシデント対応の現状

2015年に経済産業省が、独立行政法人情報処理推進機構とともに「サイバーセキュリティ経営ガイドライン」[1)]を策定し、CISOに指示すべき重要10項目の1つとして「サイバー攻撃を受けた場合、迅速な初動対応により被害拡大を防ぐため、CSIRT（サイバー攻撃による情報漏えいや障害など、コンピュータセキュリティにかかるインシデントに対処するための組織）の整備や、初動対応マニュアルの策定など緊急時の対応体制を整備すること。」が盛り込まれました。

図1　本稿で紹介する対策の範囲

こういったガイドラインやサイバー攻撃の増加を受けて、インシデント対応強化を検討する組織は増えています。しかし、実際のインシデント対応において、多くの組織が以下3つの課題に直面しています。

2.1 不適切な初動対応による証拠消失

「ウイルス対策ソフトやゲートウェイ型の検知製品による発見」「不審なファイルを実行してしまった、ファイルが開けない、ログインできないなどの異常に気付いた利用者からの申告」「外部機関からの通知」などがきっかけとなり、インシデントを認識したセキュリティ担当者は事態を解決するためにさまざまなアクションを実行します。検知したファイルの駆除や隔離、ウイルス対策ソフトのフルスキャ

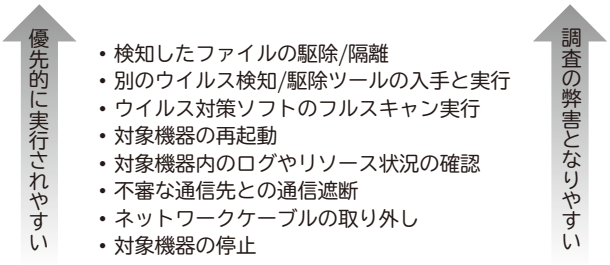


図２　優先的に実行されやすいアクションと調査への影響度

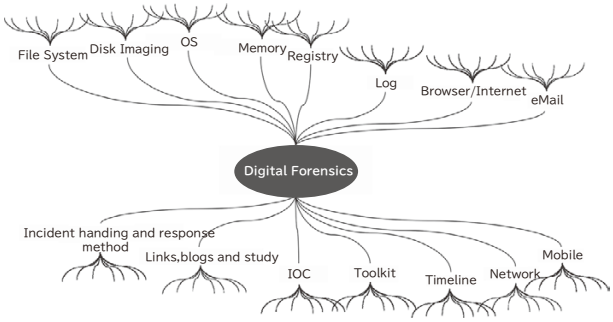


図３　フォレンジック[3]に必要な要素技術イメージ

ン、対象機器の再起動などのアクションは発生原因の把握や被害の拡大を止めるための試みであり、結果的に適切であることもあります。

しかし、事態が収束しなかった場合、つまり被害が深刻である可能性が判明した場合、それまでの調査や対処に伴うアクションによりコマンド・プログラムの実行履歴、ファイル・フォルダの変更履歴などが上書きされ、貴重な手がかりを消失させてしまうことがあります。また、セキュリティ担当者が行った調査や操作内容が記録されていない場合、残された履歴が調査対応時のものなのか攻撃者が実行したものなのか読み取ることは難しく、調査をより困難にしてしまいます（**図2**）。

2.2 デジタル・フォレンジック技術者のリソース不足

PCやサーバ、ネットワークを解析し、インシデントの発生原因や被害の詳細を特定する技術をデジタル・フォレンジック（以下、フォレンジック）と呼びます。フォレンジック技術者は市場全体で不足しており、ユーザー企業や組織の体制構築はもとよりインシデントが発生し支援を必要とする組織に対しても、インシデント対応事業者の手が行き届かない状況です。

背景としては、フォレンジック技術者は高度な知識が要求されることが挙げられます。コンピュータに残された微かな痕跡を探すためには、ファイルシステムやメモリの構造など、本来人間が読み取ることが難しいコンピュータの内部動作や原理に関する知識が必要となります。一方、IT業界の開発全般は比較的人間に理解しやすい高級言語を用いた環境に変わっており、コンピュータ原理的な技術を習得する機会が非常に少なくなっています。このような背景から、インシデント対応を担える人材はますます希少化しており、需要に対して供給が足りない状況が続いています（**図3**）。

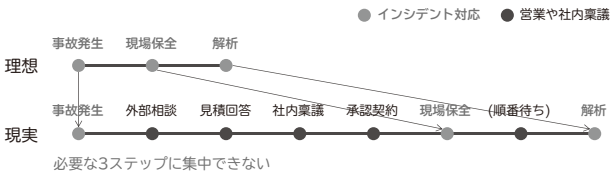


図４　担当者に課せられる間接業務例

2.3 担当者がインシデント対応に集中できない環境

社内にフォレンジック技術者がいない場合、速やかに社外の専門家に支援を依頼することが必要です。しかし、前述のとおり、市場全体でリソースが枯渇しているため、緊急で支援を受けるためには複数社に連絡を取り、最も早く駆けつけることのできる事業者を探す必要があります。また、いつ発生するか分からないインシデントのためにまとまった対策予算を準備している組織は多くありません。そのため、現場の担当者はインシデント対応と並行して、見積依頼、見積の精査、特別予算の社内稟議などの業務を行う必要があります（**図4**）。

実際には、深刻な事態だと理解を得られるケースばかりではなく、一般的には、可能性を示す痕跡だけでセキュリティの専門家ではない経営層に理解、納得をさせることは困難を極めます（**図5**）。その結果、担当者にとって必要なタイミングで必要な支援を得られず、対応に時間がかかってしまうことが多いと言えます。通常、攻撃者に時間を与えると攻撃の痕跡を隠ぺいしながら侵害を拡大することが可能になり、調査が難しくなります。また、サイバー攻撃のなかには感染させる端末ごとに使用するマルウェアのハッシュ値や通信先を細かく変えるものもあり、初動対応を誤り、マルウェアが蔓延してしまうと個々のマルウェアごとに感染を特定する条件が異なるため、根絶することは非常に困難になります。

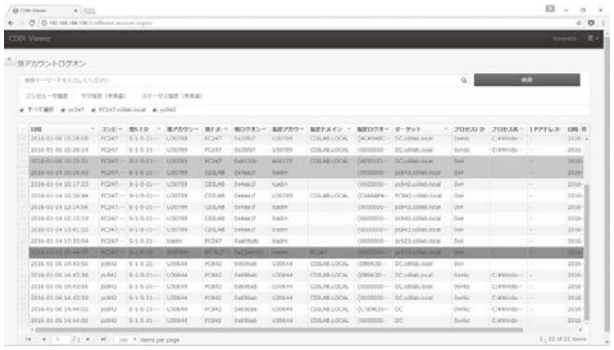


図５　初動対応で得られるサイバー攻撃の痕跡例
（攻撃者にアカウントを取得された可能性を示す痕跡）

3. 課題解決の方法

第２章にて、インシデント対応における３つの課題を挙げさせていただきました。

（1）不適切な初動対応により証拠が消失すること
（2）フォレンジック技術者の確保が難しいこと
（3）担当者がインシデント対応に集中できないこと

以降にて、これらの課題に対する解決方法について説明します。

3.1 適切かつスピーディーな保全

深刻な被害を防ぐためには、サイバー攻撃の初動対応で「攻撃された可能性のある端末のデータ保全」[2]というアクションを早い段階で実施しておくことが有効です。必要なデータを保全しておくことで、詳細な調査が必要な状況になったとしても実態が明らかになる可能性が高くなるからです。

しかし、インシデント発覚直後は情報が少ないため、何をどれだけ保全すれば良いか判断することも難しく、それなりに手間のかかる保全作業を後回しにしてしまうことがよくあります。そのため、証拠が消失している事例が多い現状の課題解決として、NECグループのセキュリティ専門会社であるサイバーディフェンス研究所（以下、CDI）では、CDIR Collectorという、簡単な手順でインシデント対応に有用なデータを保全することが可能なツールを開発しました。CDIR Collectorは、揮発性と情報価値の兼ね合いから保全対象を選定しています（表）。

USBメモリやネットワークドライブに本ツールを格納し、対象端末を接続・実行することで、数分から十数分でデータを保全することができます（**図６**）。

3.2 自組織で保有する役割とアウトソースの整理

フォレンジックなど自組織で行うには技術的なハードルの高い対応については、外部から協力を得ることも事前に視野にいれておく必要があります。自組織にセキュリティ担当者がいるか、システムの維持管理をしているかなど保有する業務や人材を分析し、組織内でどこまでの対応を行い、何をアウトソースするか役割を整理し、必要なときに調査・解析のリソースを確保できるようにしておくことが重要です[4) 5)]。

3.3 事前の準備と周知

サイバー攻撃が疑われる状況になった際には、誰が何をするのか、誰に連絡するのかなどインシデントの対応計画、意思決定プロセスを事前に準備し、経営層も含め理解

表　CDIR Collectorの保全データと得られる情報

取得データ	得られる情報（例）	解析における利用（例）
メモリ	直近のアクティビティ、ファイルキャッシュ、通信先情報	・不審な通信先 ・（動作中の）プログラムの発見 ・関連ファイルの調査
メタデータ	ファイルパス、ファイル名、ファイルのタイムスタンプ	・ファイル作成（設置）日時の特定 ・不審ファイルに関する付属情報
ジャーナル	ファイル及びフォルダの変更ログ	・マルウェアの発見 ・情報窃取の有無
イベントログ	ローカルアカウントのログオン / オフ、 サービス / タスクスケジュール処理、システム稼働状況	・被害発生範囲の調査 ・不審なサービス / タスクの有無
プリフェッチ	プログラム実行日時、回数、ファイルパス、関連ファイル	・マルウェアの発見、格納場所の調査 ・関連ファイルの調査
レジストリ	プログラム実行履歴、自動実行設定、ハッシュ値	・マルウェアの発見 （もしくはマルウェアの判定） ・不審な自動実行設定の有無
ブラウザ履歴	アクセスした Web サイト	・感染源、感染日時の特定

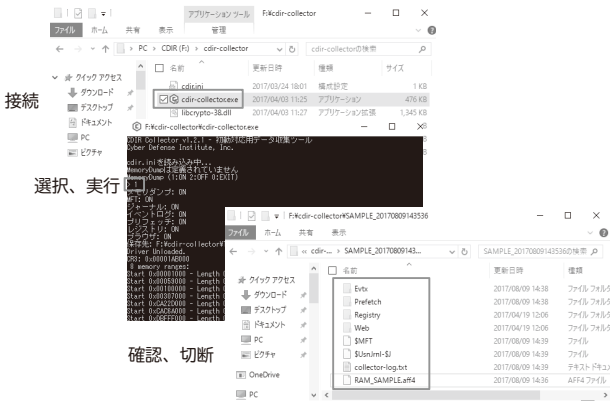


図６　CDIR Collectorの実行例

を深めておくことで、万が一インシデントが起きたとしてもスムーズに対応することができます。

4. インシデント対応を支援するサービス

NECでは、CDIR Collectorを活用することで簡単に保全が行えるようになることを受け、CDIR Collectorで保全したデータを解析するリモート支援サービスを提供します（**図7**）。

端末に残るサイバー攻撃の痕跡をNEC専門部隊が解析するサービスで、従来のフォレンジックサービスとは異なり、サービスレベル目標を設定し迅速に初動対応の支援を行います。具体的には、お客様より保全データを受け取ったのち、1営業日以内に判明した内容を速報としてレポートすることを目標としています。

また、万が一、情報漏えいや深刻な侵害が判明した際は、CDIと連携し徹底的な対応にあたります。更に、本サービスは、月額契約のため、インシデント対応において余計に時間を要する見積や社内稟議などの事務的業務を省略することができます。本サービスによって、お客様が迅速かつ集中してインシデント対応を行うためのスキームを提供します。

5. むすび

インシデントにおける初動対応の重要性とフォレンジック技術を用いたサービスによる対応の迅速化について、述べました。

NECが責任を持って提供させていただくインシデント対応支援サービスは、サイバー攻撃によるインシデントを深刻化させないためのソリューションです。サービス提供

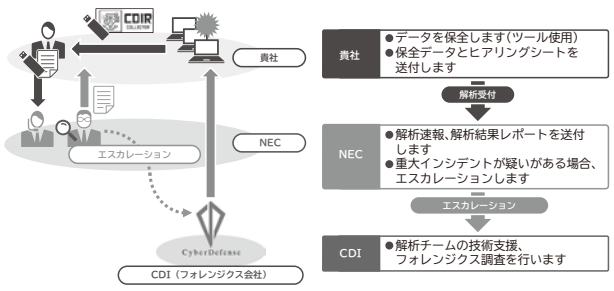


図7　サービスの概要

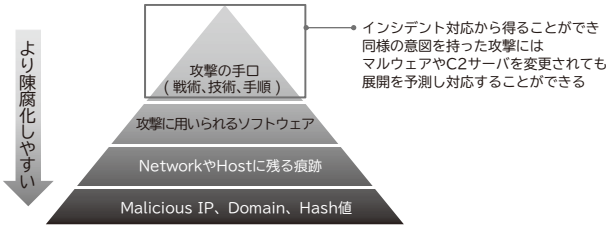


図8　サービスによって得られるノウハウイメージ

によって得られる最新の攻撃手口などのノウハウ[6]（**図8**）やお客様のセキュリティ業務における課題をNECのサイバーセキュリティサービス群へ迅速に反映することで、すべてのお客様へのより良いサービス提供に貢献できればと考えます。

参考文献

1）経済産業省：サイバーセキュリティ経営ガイドライン
http://www.meti.go.jp/policy/netsecurity/mng_guide.html
2）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6版
https://digitalforensic.jp/home/act/products/df-guideline-6th/
3）Aman Hardikar：Forensics, Mind Maps
http://www.amanhardikar.com/mindmaps/Forensics.html
4）@IT:初動対応用データ保全ツール「CDIR Collector」解説（前編）
http://www.atmarkit.co.jp/ait/articles/1609/15/news006.html
5）@IT:初動対応用データ保全ツール「CDIR Collector」解説（後編）
http://www.atmarkit.co.jp/ait/articles/1609/30/news005.html
6）Use of the term "Intelligence" in the RSA 2014 Expo
http://detect-respond.blogspot.com/2014/03/use-of-term-intelligence-at-rsa.html

執筆者プロフィール

大口 恭平
セキュリティ事業推進室
主任

山崎 輝
株式会社サイバーディフェンス研究所
上級分析官

山根 匡人
ナショナルセキュリティ・ソリューション事業部
主任

関連URL

CDIR-ファストインシデントレスポンスツール
https://www.cyberdefense.jp/products/cdir.html

NEC 技報のご案内

NEC 技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報（日本語）　NEC Technical Journal（英語）

Vol.70 No.2　ビジネスの安全・安心を支えるサイバーセキュリティ特集
～Futureproof Security　安心の先へ。～

ビジネスの安全・安心を支えるサイバーセキュリティ特集によせて
増大するサイバー犯罪の根源的な解決へ～“産学官”のオールジャパンで立ち向かう第三者機関の姿とは？～
サイバーセキュリティを取り巻く社会動向とNECの取り組み

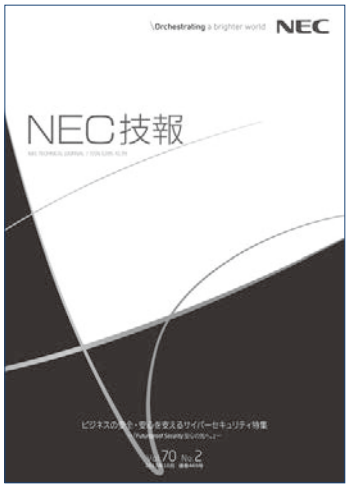
◇ 特集論文

社会の動向とNECの取り組み
重要インフラに対するサイバー攻撃の実態と分析
2017 サイバー攻撃最新動向 NEC Cyber Threat Intelligence活用モデル
サイバーセキュリティ対策の社内事例

サイバーセキュリティソリューション
複雑化 / 高度化するサイバー脅威に対抗するSOCとセキュリティ監視サービス
攻撃被害を極小化するためのインシデント対応支援ソリューション
サイバー演習によるインシデントハンドリング能力の強化
セキュリティ統合管理・対処ソリューション「NEC Cyber Security Platform」
クラウド型ファイル暗号化サービス －ActSecureクラウドセキュアファイルサービス－
セキュリティLCMサービス
EMMを活用したセキュアなモバイルワークソリューション
IoT 時代の経営を支援するサイバーセキュリティコンサルティング

サイバーセキュリティへのAI技術の活用
AI（人工知能）を活用した未知のサイバー攻撃対策
採るべき対策の「なぜ？」に答えるAIの可能性
オープンソースインテリジェンスを活用したサイバー脅威の検出と自動分析
犯罪捜査支援のためのサイバー・フィジカル統合分析技術

お客様に安全・安心を届けるための社内の取り組み
安全・安心な製品・サービスをご提供するための取り組み ～セキュア開発・運用～
サイバーセキュリティ人材のタレントマネジメント



Vol.70 No.2
（2017年10月）

特集TOP