2020.03.02

情報セキュリティニュース ＜2019 No.4＞

デジタル・フォレンジックの概要

【要旨】
■デジタル・フォレンジックとは、情報セキュリティ事故や内部不正等の原因調査・分析のプロセスで活用する手法のひとつである。その調査・分析の結果は、その後の対応の品質に影響を与える重要な意味を持つ。
■デジタル・フォレンジックにはさまざまな手法がある。発生した事象の種類によって最適な手法を選択して対応することにより、被害が発生した原因や、影響範囲を特定することができる。
■企業は、デジタル・フォレンジックの概要を理解したうえで、適切な手法を選択することにより、発生した事実・事象を究明し、適切な事後対応を取ることでインシデント発生時の被害を最小限に抑えることが望まれる。

1．デジタル・フォレンジックとは

フォレンジック（Forensics）とは「科学捜査」、「法医学」、「鑑識」という意味を持つ言葉であり、デジタル・フォレンジックとは、「デジタルの領域における鑑識」と表現すると理解がしやすい。

刑事ドラマに出てくる鑑識は、事件が発生すると現場へ赴き、靴あとや指紋、血痕等を、特殊なスキル・ツールを利用し調査し、犯行の手口や犯人特定につながる証拠を検出する。

一方、デジタル・フォレンジックは、例えば、サーバへの不正アクセスを検知した企業の拠点等（現場）へ赴き、パソコン（PC）、ハードディスクドライブ（HDD）、サーバ、スマートフォン、USB メモリ等から、特殊なスキル・ツールを利用して調査・分析し、サイバー攻撃等の犯行の手口や影響等の特定につながる証拠を検出する。すなわち、デジタル・フォレンジックとは、「コンピュータやネットワーク上の情報を保全し、調査し、解析をして証拠を確保するための手法」である。

また、デジタル・フォレンジックは、不正アクセス等のサイバー攻撃の検知時だけでなく、談合や機密情報の不正な持ち出し等の不正や、ハラスメント等に関するインシデント[1]が発生した場合の緊急時対応においても活用される。

表１　「鑑識」と「デジタル鑑識」の対比

刑事ドラマの鑑識			デジタル鑑識	
犯行現場 ● 靴あと ● 指紋 ● 血痕 …	● 鑑定 ● 照合 ● 試験		インシデント発生企業 ● PC ● サーバ ● スマホ ● USB メモリ …	● データ復元 ● 侵入有無 ● メール証跡
	● 犯人像 ● 犯行手口 など			● 攻撃の実態 ● 被害の影響 など

[1] インシデント
重大な事件や事故に発展する可能性を持つ事象のこと。

２．緊急時対応のフローにおけるデジタル・フォレンジックの位置づけ

デジタル・フォレンジックは、インシデント発生時の緊急時対応のフロー上の「分析」において被害の発生の有無を判断するために、また、被害の発生の可能性が高い場合はインシデントの影響範囲の特定や、発生原因の調査・分析をするために行われる。

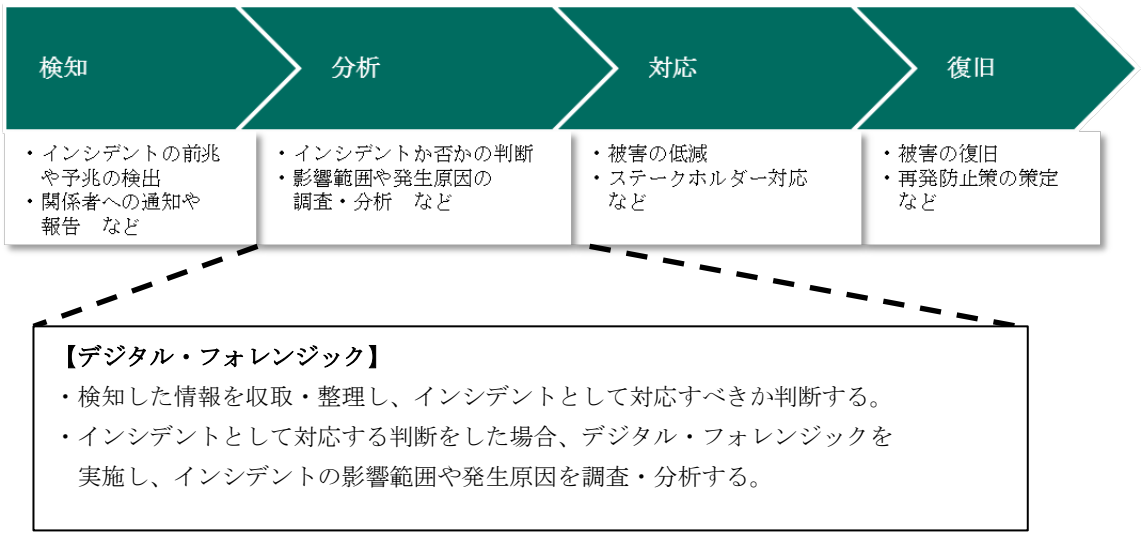

図１　緊急時対応フローにおけるデジタル・フォレンジックの位置づけ

３．デジタル・フォレンジックの主な手法

デジタル・フォレンジックは、発生した事象の種類によって最適な手法を選択して対応する。主な手法を以下に示す。

表２　デジタル・フォレンジックの主な手法

名称	調査・分析の対象	得られる情報	備考
コンピュータ・フォレンジック	● コンピュータの記憶媒体 HDD、ソリッドステートドライブ（SSD）等の固定媒体の他、USB メモリ等の可搬媒体も含む。	● コンピュータに格納されている情報そのもの ● コンピュータでどのような操作がされたか （例） ・どのファイルに誰がいつアクセスしたか ・web ブラウザでどのようなページを閲覧したか 等	削除されたデータの復元や、拡張子の偽装の確認等も行う。
メモリ・フォレンジック	● コンピュータのメモリ[2]上のデータ	● コンピュータ上でどのプログラムが動いているか ● コンピュータがどこと通信しているか　等	HDD や SSD に痕跡を残さないタイプのマルウェアでも、メモリには痕跡を残すことがあり、このような場合に有効な手法となる。 メモリは揮発性（電源を切るとデータが消える性質）のため、コンピュータを起動させたまま実施する必要がある。

[2] RAM（Ramdom Access Memory）のこと。データやプログラムを一時的に記憶する作業場所であり、コンピュータの電源を切るとメモリ上からデータは削除される。

モバイル・フォレンジック	● スマートフォン等のモバイルデバイス上の情報	● 発信・着信履歴 ● メール・SMS のメッセージ ● モバイルデバイスに保存された動画、写真、電話帳 ● SNS 内のメッセージ　等	モバイル・フォレンジック専用のツールを用いる。
ネットワーク・フォレンジック	● ネットワーク上の情報の動き	● どのコンピュータが／いつ／どのような経路で／何を送信したか	外部サーバとの通信や、インターネットの閲覧履歴等を調査する。

4．デジタル・フォレンジックの実施手順と活用事例

一般的なデジタル・フォレンジックの実施手順を以下に示す。デジタル・フォレンジックを実施するにあたり、平時の準備として、ログを収集する仕組みの導入、インシデント対応体制の整備、エスカレーションルートの構築等をしておく必要がある。

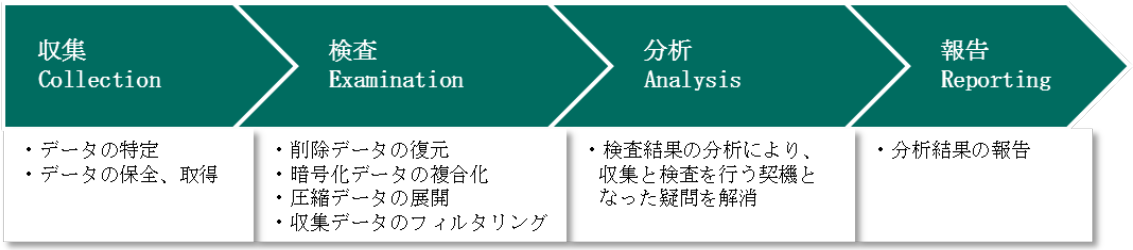

図２　デジタル・フォレンジックの実施手順

また、以下にてデジタル・フォレンジックをどのように活用するか、事例を用いて解説する。

【事例】

複数の社員から、「PC がおかしな挙動をしたため、マルウェア感染したのではないか」との報告があった。事象から、マルウェア感染の可能性があるものの、現時点で具体的な被害は明らかになっていない。調査・分析のため、フォレンジック業者へ依頼した。

（１）収集

ネットワーク・フォレンジックにより、危険と認識されている外部サーバとの不審な通信が発生していることが判明したため、同サーバと通信している PC を洗い出し、当該 PC についてデータ保全[3]を行った。

（２）検査

保全したデータから削除データを復元したうえで、調査対象をマルウェア感染の疑いがあるとの報告があった日時以降の作成・更新・参照日時となっているファイルに絞り込んだ。

（３）分析

危険と認識されている外部サーバとの不審な通信が発生している PC へのコンピュータ・フォレンジックにより、当該 PC が外部サーバと通信している時間帯付近に、当該 PC がアクセスしたファイルを特定した。特定したファイルには顧客の氏名、会社名等の個人情報が約 1 万件含まれていた。再びネットワーク・フォレンジックを実施した結果、同ファイルを外部サーバへ送信した履歴が発見された。

[3] 調査・分析用に、収集した機器のデータと全く同一のものを作成すること。

（4）報告

フォレンジック業者が（3）分析フェーズで得られた情報を整理し、発注者へ報告した。

（5）報告を受けた企業の対応

外部へ流出したファイルとその内容が判明したことにより、個人情報の漏えいが発生したことの確定および個人情報が漏えいした顧客を特定できた。この事実に基づき、対象の顧客へお詫び対応をするとともに、漏えいした件数を勘案して、自社ＨＰを通じてサイバー攻撃による不正アクセスにあい、顧客情報が流出した事実を公表した。

５．インシデントに応じたデジタル・フォレンジック手法の選択

インシデントの発生を検知した際には、各種ステークホルダーへの報告や情報開示のために「早くて、正確で、抜け漏れのない」情報の収集が求められる。一方で、ストレージの大容量化や調査対象機器台数の増加、フォレンジック人材の不足等により、従来のデジタル・フォレンジック手法では調査・分析に多大な時間やコストがかかる場面が増えている。

そのため、近年では初動対応の「早さ」を重視した手法であるファスト・フォレンジックが広がっている。ファスト・フォレンジックは、インシデント発生による被害範囲および深刻度の早期判断を目的とし、インシデントの発生を検知した後、速やかに最小限のデータ（レジストリ、メモリ、イベントログ等、サイバー攻撃の痕跡を発見できる期待があるもの）を取得し、一定の推測も交えて調査することで、サイバー攻撃にあった企業は調査・分析にかかる時間やコストを短縮することができる。EDR（Endpoint Detection and Response）製品が平常時よりネットワークで収集するデータをファスト・フォレンジックに利用することも有効な手法である。

６．インシデント発生時のフォレンジック業者選定

実際にインシデントが発生した際は、速やかにフォレンジック業者へ依頼をするべきだが、日常的に業者と付き合いのある企業は決して多くはない。そのため、特定非営利活動法人　日本ネットワークセキュリティ協会で公開している「サイバーインシデント緊急対応企業一覧」や、デジタル・フォレンジック研究会の団体会員一覧などから、フォレンジック業者を予め把握しておくことを推奨する。（相談や見積は無償の企業も多い。）

また、フォレンジック業者は法律事務所、会計事務所等と連携するケースが多いので、顧問弁護士、監査法人等に相談することも有効である。

費用については、本格的なデジタル・フォレンジックは多額の費用がかかることが多いものの、前述のファスト・フォレンジックのように、調査対象範囲を限定することにより、数万円単位から実施可能な場合もある。

企業は、自社で起こりうるインシデントがどのようなものか、その場合に依頼できるフォレンジック業者はどこか、費用はどの程度なのか等を、予め把握することで、インシデント発生時に迅速な対応を行うことができる。

サイバー攻撃の目的や手法は多様化・高度化しており、その攻撃の被害は国内外問わず多数発生、企業は専守防衛とならざるを得ない圧倒的に不利な状況にある。企業は、万が一サイバー攻撃にあった際には、デジタル・フォレンジックの手法を理解したうえで、発生したインシデントの種類や深刻度等に応じた有効な手法を選択し、発生した事実・事象を究明し、適切な事後対応を取ることで被害を最小限に抑えることが望まれる。

ＭＳ＆ＡＤインターリスク総研㈱　リスクマネジメント第四部
上席コンサルタント　　五十嵐　大

ＭＳ＆ＡＤインターリスク総研株式会社は、ＭＳ＆ＡＤインシュアランス グループのリスク関連サービス事業会社として、リスクマネジメントに関するコンサルティングおよび広範な分野での調査研究を行っています。
情報セキュリティに関するコンサルティング・セミナー等を実施しております。
コンサルティングに関するお問い合わせ・お申込み等は、下記の弊社お問合せ先、またはあいおいニッセイ同和損保、三井住友海上の各社営業担当までお気軽にお寄せ下さい。

お問い合せ先
ＭＳ＆ＡＤインターリスク総研㈱
リスクマネジメント第四部　事業継続マネジメント第一グループ
千代田区神田淡路町2-105 TEL:03-5296-8918／FAX:03-5296-8941
https://www.irric.co.jp/