# 危機管理の観点でのサイバー侵害対応とデジタルフォレンジックの活用

Forensics事業部　Privacy & Cyber Responseチーム　五十嵐良一

▸ Yoshikazu Igarashi

事業会社で企業グループの情報セキュリティマネジメント推進およびサイバー侵害対応等に従事した後、2020年に当法人に入所。デジタルフォレンジックを活用したサイバー侵害の対応支援業務やサイバーインシデント対応態勢の評価・改善支援業務に従事。情報処理安全確保支援士。

## Ⅰ　はじめに

近年、DXによるビジネス変革や新型コロナウイルス感染症（COVID-19）に伴うリモートワークの拡大などにより、新しいテクノロジーの導入が急速に拡大していく中で、ランサムウエア攻撃など、サイバー侵害による基幹システムの停止や機密情報の破壊・漏洩（えい）などの被害が急増しています。

サイバー侵害への対応は、技術課題に加えて事業継続に係る危機管理上の課題もあるとの認識が浸透しつつある一方で、当法人が支援した事案において、サイバー侵害発生時に、経営層の判断に必要な情報を適時に把握することができず対応に苦慮した事例や、復旧優先で対応したため、財務諸表監査においてサイバー侵害の影響確認に苦慮した事例も確認しています。

本シリーズでは、ファイナンス部門のDX／ファイナンス領域におけるデジタルの活用ポイントについて包括的に論述しています。本稿では、不正調査を主たる業務としているEY Forensicsによる後編として、危機管理の観点でのサイバー侵害対応の課題とデジタルフォレンジックの活用について紹介します。

## Ⅱ　サイバー侵害対応における危機管理の課題

サイバー侵害は目に見えず、急速に進行する特性があり、さらにサイバー犯罪者は、調査を妨害するために侵害したシステムのログ等を消去することもあり、いつ、何が起きたのかを正しく把握することは容易ではありません。

企業の事業形態や保有するデータ、サイバー侵害の態様により、危機管理の観点での課題は異なりますが、ここでは＜図1＞に示す一般的なランサムウエア攻撃のプロセス例を題材に論じます。

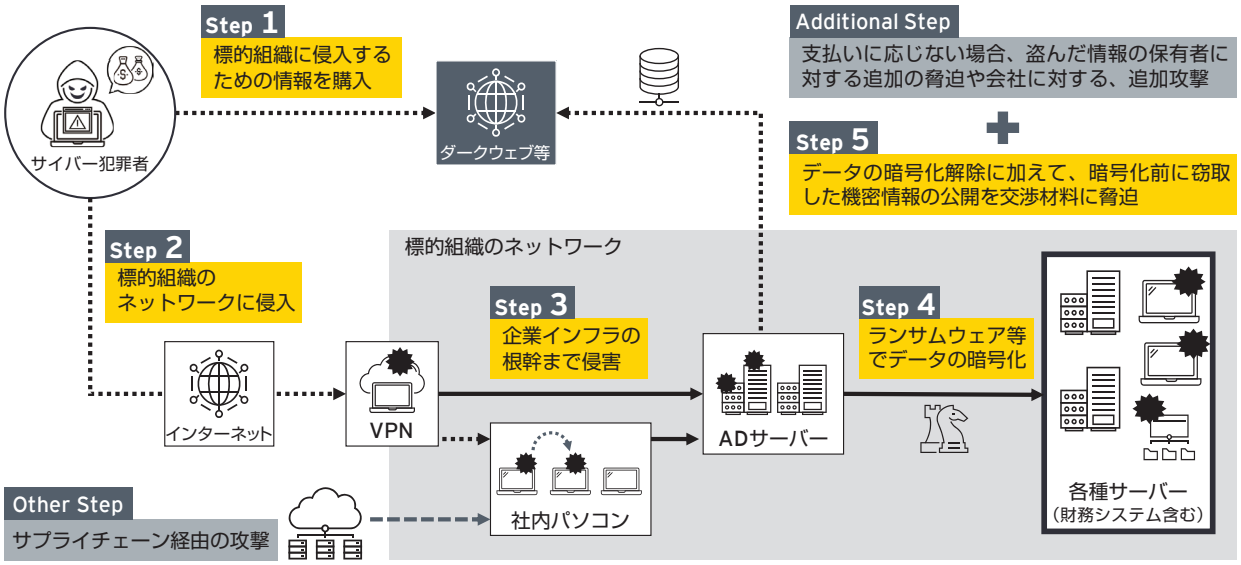
ランサムウエア攻撃を行うサイバー犯罪者は、何らかの方法で組織の内部ネットワークに侵入し、ファイルサーバーや基幹システム等をランサムウエアに感染させ、格納されているデータを暗号化し利用できなくした上で、データの暗号化解除と引き換えに身代金を要求してきます。さらに、暗号化前にデータを窃取し、身代金の要求に応じない場合、インターネット上でのデータ公開などを交渉材料として、追加の脅迫行為を行う場合もあります。このようなサイバー侵害における危機管理対応の観点での課題の一例を次に示します。

### 1. 業務の再開・継続に関する課題

暗号化により実質的に破壊されたデータをバックアップから復旧できない場合、システムを利用せず手作業による暫定的な業務継続や、紙の帳票から破壊されたデータを再入力するなどの対応を検討する必要があります。

データをバックアップから復旧できる場合は、ランサムウエアやサイバー犯罪者が遠隔操作に利用したツール等の除去、システムの再構築、バックアップデータの完全性の検証を実施した上で、データ復旧を進める必要があります。侵入された原因の特定・除去を行わずに復旧作業を進めた場合、復旧途中または復旧後に再びシステムが侵害される可能性があるため、復旧作業の準備と並行し、侵害原因の特定・除去も進める必要があります。

▶図1　一般的なランサムウエア攻撃プロセスの例




### 2. ステークホルダー対応の課題

個人情報や取引先の機密情報等が漏洩した場合、適切なタイミングで被害者や関係者へ通知する必要があります。

しかし実際のサイバー侵害事案では、情報漏洩の明確な痕跡が残されていないことも多く、情報漏洩の有無の判断に苦慮することがあります。なお、「情報漏洩していないことを確認した」とプレス発表した当日に、サイバー犯罪者のウェブサイト上に窃取された情報が公開された事案も発生しています。

また、サイバー侵害により発生した資産の減損に対して、株主等から経営者の善管注意義務違反を指摘される可能性もあり、説明責任を果たすためには、サイバー侵害が発生した原因や、侵害による影響の把握が必要となります。

### 3. 規制当局対応の課題

日本においては、2022年4月の改正個人情報保護法により、ランサムウエア感染等で個人データが暗号化され復元できなくなった時点で、個人データの漏洩が発生したおそれがある事態と見なし、概ね3～5日以内に個人情報保護委員会へ報告する必要があります。

また、欧州連合（EU）域内の子会社でのサイバー侵害など、GDPR（EU一般データ保護規則）の保護対象となる個人データが漏洩した場合は、72時間以内に監督機関へ報告する必要があります。

このように、各国におけるサイバーセキュリティやプライバシーに係る規制等に基づく対応も考慮する必要があります。

### 4. 財務諸表監査対応の課題

ランサムウエア攻撃により、財務諸表に係るシステムに格納されたデータやプログラム・設定情報が破壊された場合、財務諸表数値の完全性が損なわれる可能性があります。また、サイバー犯罪者に内部ネットワークのシステム特権を取得された場合、財務諸表に係るシステムが不正に操作された可能性等も考慮した調査が必要となります。

影響調査を十分に実施せずにシステム復旧を進めた場合、財務諸表監査において虚偽表示や潜在的な減損のリスクに関する指摘を受け、対応に苦慮する可能性もあります。

## Ⅲ　サイバー侵害におけるデジタルフォレンジック

サイバー侵害対応では、目に見えないサイバー侵害の全容を可能な限り早く把握し、速やかに業務を再開することが求められますが、やみくもに復旧作業や調査を進めても、調査に必要な証跡を消してしまうなど、かえって判断に必要な情報の把握に時間がかかる可能性があります。

デジタルフォレンジックによる調査手順の概要や留意事項を理解しておくことは、サイバー侵害発生時の適切な対応に役立ちます。

サイバー侵害におけるデジタルフォレンジックの調査手順の例として、証拠保全、初期侵入経路の調査、侵害範囲の調査、侵害による影響の調査の概要と留意事項を以下に示します。

### 1. 証拠保全

サイバー侵害の調査において、最も慎重に対応すべきことの1つが、調査に必要な証跡を確保する証拠保全と呼ばれる作業です。

侵害されたパソコン・サーバー等を復旧するために、機器の初期化・再インストールを行うと、機器に残された侵害の痕跡なども消去され、調査が困難となる場

合があります。また、デジタルフォレンジックの観点を意識せず、むやみに侵害されたパソコン・サーバー等の機器にログインして調査することにより、例えると事件現場に土足で踏み込み、犯人が残した痕跡を消してしまうような結果となる可能性があります。

調査に必要な証跡を消してしまった場合、危機管理対応において判断に必要な情報が不足するなど、対応に苦慮する可能性があるため、調査に必要なデータを適切な手順で保全し、保全したデータに対して調査を実施することが望ましいです。

適切に証拠保全を実施しておくことで、例えば財務諸表監査において、財務システムへの影響などの確認を求められた場合にも、必要に応じて追加調査が可能となります。

証拠保全の一例としては、保管期間を超過すると消去されてしまうシステムの操作ログを別の媒体へ複製したり、侵害された機器に接続されたハードディスク等のストレージの削除済み領域も含む全領域、または調査に必要なデータをフォレンジック用ツールで複製したりすることが考えられます。また、保全したデータの妥当性に疑義を生じさせないためには、証拠保全を実施した日時、作業者、作業手順などを記録しておくことも必要です。

しかし、サイバー侵害対応においては、一刻も早い復旧が求められ、証拠保全にかけることができる時間は限られています。事前にデジタルフォレンジック専門家なども交え、サイバー侵害時に保全すべきデータを取捨選択し、保全手順を整備しておくことが有効です。

さらに、事前にパソコン・サーバー等にEDR（Endpoint Detection and Response）と呼ばれる、機器の詳細な動作状況をログに記録し監視できるセキュリティ対策製品を導入しておくことで、サイバー侵害発生時にEDRログを活用した調査を迅速に実施することが可能となります。

なお、内部統制の観点で記録している財務システムに係る操作ログ等も調査に有用ですが、サイバー侵害においては、システムの脆弱性を突いてデータベースに記録されたデータを直接削除・改変するなど、財務システムの操作ログ等に記録されない形で攻撃される可能性もあります。サイバー侵害の財務システムへの影響調査の観点からは、財務システムの操作ログ等だけでなく、追加の証拠保全が必要となる可能性がある点に留意する必要があります。

### 2. 初期侵入経路の調査

ランサムウエア攻撃を認知した後、何も対策を講じなければ、サイバー犯罪者が再び組織の内部ネットワークへアクセスしてくる可能性があるため、初動対応として、サイバー犯罪者が侵入のために利用した経路の遮断や侵害されたパソコン・サーバー等をネットワークから切り離す等の「封じ込め」と呼ばれる対応を実施し、侵害が拡大することを止めた上で、初期侵入経路および侵入された原因を特定し除去する必要があります。

初期侵入経路の特定を効果的に進めるためには、システム構成やセキュリティの更新プログラムの適用状況、ランサムウエアの脅迫メッセージから推測されるサイバー犯罪者の特徴などを踏まえ、初期侵入経路となる可能性が高い機器等の仮説を設定し、調査を行うことが有効です。例えば、近年、企業においてインターネットVPNなど、リモートワーク環境の整備が急速に進みましたが、セキュリティ対策が不十分な状態で運用されているVPN装置を通じて組織の内部ネットワークへ侵入される事案が散見されます。当法人が支援した企業においても、インターネットVPNを利用しており、かつセキュリティの更新プログラムを適用していなかったため、VPN装置が初期侵入経路となった可能性が高いとの仮説を設定し、優先的にVPN装置のログや設定情報の調査を進めたところ、外部の第三者が内部ネットワークへアクセスした痕跡を確認し、初期侵入経路を速やかに特定できた事例もあります。

デジタルフォレンジックの調査では、ネットワーク機器が記録する通信履歴など、機器が記録したログだけでなく、機器の仕様に基づき、機器のメモリやハードディスク等に残される動作の痕跡も解析対象とします。例えば、EDR等が導入されていないパソコンにおいても、デジタルフォレンジックによりハードディスク等を解析することにより、＜表1＞のように、限定的ではありますが、ファイルの作成・削除・編集された日時を解析し、サイバー犯罪者による操作の痕跡を確認できることがあります。ただし、デジタルフォレンジックの手法では、パソコン・サーバー等の操作・動作により痕跡が上書き消去される可能性もあるため、さまざまな観点で複合的に分析を行います。

### 3. 侵害範囲の調査

ランサムウエア感染など明確な侵害の痕跡が無いパソコン・サーバー等も、サイバー犯罪者に侵入された可能性が否定できない場合、侵害された痕跡の有無を調査し、侵害された機器をリスト化します。

ここでリスト化した機器を対象に、後述する侵害による影響の調査を実施するため、侵害された機器への個人情報など機密情報の格納有無や、財務システムま

▶表1　解析により特定したファイル操作履歴の例

| Time Stamp (UTC+9) | USN | File/Directory Name | Full Path | Event Info |
|---|---|---|---|---|
| 2020/11/15 14:00 | 9818200 | ransom.exe | ¥Share¥ransom.exe | File_Created |
| 2020/11/15 14:00 | 9818280 | ransom.exe | ¥Share¥ransom.exe | File_Created / Data_Added |
| 2020/11/15 14:00 | 9818360 | ransom.exe | ¥Share¥ransom.exe | File_Created / Data_Added / Data_Overwritten |
| 2020/11/15 14:00 | 9818440 | ransom.exe | ¥Share¥ransom.exe | File_Created / Attr_Changed / Data_Added / Data_Overwritten |
| 2020/11/15 14:00 | 9818520 | ransom.exe | ¥Share¥ransom.exe | File_Created / Attr_Changed / Data_Added / Data_Overwritten / File_Closed |

たは財務諸表に係るデータの取扱い有無などについても整理します。

なお、侵害範囲の調査は、侵害されたネットワークに接続された多数の機器を対象に実施するため、EDRなどによりパソコン・サーバー等のログを一元管理していない場合、調査に時間がかかる可能性があります。調査期間を少しでも短縮するため、システム構成などを踏まえ、効率的に調査する手法を検討する必要があります。例えば、調査対象のパソコン・サーバーから侵害範囲の調査に必要な最小限のデータのみ取得し、取得した全データに対して簡易解析を実施することで侵害された可能性がある機器を絞り込む手法も考えられます。

### 4. 侵害による影響の調査

ランサムウエア攻撃によるサイバー侵害においては、多数のパソコン・サーバー等から侵害の痕跡が確認されることがあり、重要なシステム、または重要な情報が格納されているシステムから優先的に侵害による影響の調査を実施します。

財務システムなどの業務システムが記録する操作ログ等から不正アクセスの痕跡有無を確認するとともに、システムが稼働するための基盤として利用しているデータベースやオペレーティングシステムにおける不審な操作の痕跡有無も確認し、サイバー侵害によるシステムへの影響を調査します。

なお、現時点で当法人が把握している範囲においては、ランサムウエア感染事案において、サイバー犯罪者が財務諸表数値の改変を目的に活動した痕跡は確認されていませんが、ランサムウエア感染などにより、財務諸表に係るデータの欠損やシステムの異常動作など、財務諸表監査への影響が発生する可能性もあることに留意が必要です。

重要な情報が格納されているシステムにおいては、情報漏洩の可能性を調査しますが、パソコン・サーバーにEDRが導入されていないなど、詳細な動作ログを記録していない場合、不審なファイルアクセスの痕跡や、不審な通信履歴の痕跡などを横断的に分析し、情報漏洩の可能性を推測します。

また、サイバー犯罪者は、ダークウェブと呼ばれる、特殊なツールを利用しないとアクセスできないネットワーク上に窃取した情報を公開したり、売買したりすることがあるため、必要に応じてダークウェブのモニタリングも実施します。

サイバー侵害の調査においては、侵害による影響を断定できる痕跡までは発見されず、調査により把握した情報に基づき判断せざるを得ない場合もありますが、そのような場合においても、適切にデジタルフォレンジックを実施することにより、判断が合理的であることを説明しやすくなります。

## Ⅳ　おわりに

近年、サイバー侵害を完全に防止することは技術的に困難であり、サイバー侵害の発生を前提とした対策を講じることが必要となっています。

危機管理対応の観点でサイバー侵害に適切に対応するためには、デジタルフォレンジックを活用し、目に見えないサイバー侵害の全容を速やかに把握することが必要となります。

そのためには、サイバー侵害の発生する前の平常時から、危機管理対応を意識した調査手順を整理し訓練を実施する、サイバー侵害発生時に速やかにデジタルフォレンジック専門家の支援を受けることができるよう契約条件を事前に調整する、サイバー侵害の対応費用を補填するためにサイバー保険に加入するなど、さまざまな準備をしておくことが重要です。

**お問い合わせ先**
EY新日本有限責任監査法人
Forensics事業部
E-mail：yoshikazu.igarashi@jp.ey.com