2020年12月21日

サイバー攻撃を受けた場合の対応シナリオと留意点

八雲法律事務所
代表弁護士　山岡裕明

1　はじめに

昨今サイバーリスクの内容が大きく変容している。企業が巻き込まれるサイバーリスクというと、2014年に発生した株式会社ベネッセコーポレーションにおける個人情報漏えい事件に代表されるように、内部者による個人情報の持ち出しが中心であったと思われる。

ところが、独立行政法人情報処理推進機構が発表している「情報セキュリティ10大脅威 2020」[1] を見ると、組織に対する脅威としては、「標的型攻撃による機密情報の窃取」が1位となっており、特定の企業の機密情報を標的と定めた外部からのサイバー攻撃がサイバーリスクの主流となりつつある。

2020年11月に公表された株式会社カプコンの被害事例は記憶に新しいが、公表文によると、「当社を標的とした」サイバー攻撃であり、個人情報最大35万件に加え「売上情報、取引先情報、営業資料、開発資料等」も流出した可能性があるとされており[2]、まさに「標的型攻撃による機密情報の窃取」の事例に他ならない。

こうした標的型攻撃によるサイバーリスクを被害の観点からみると、例えばコロナウイルスのワクチン情報など多額の開発費を投じた自社の機密情報が窃取された場合には競争力が大きく損なわれるし、取引先から受領した機密情報が窃取された場合には当該取引先から機密保持義務違反の責任を追及されることにもなる。会社が被る損害の内容は、個人情報の漏えい事案のそれとは大きく異なる。

また、セキュリティの難易度の観点からみると、標的型攻撃は、標的と定めた企業に対する入念な偵察行為と調査行為を前提とするいわばオーダーメイドな攻撃であるため、その対策は極めて困難となる。マルウェアを添付したメールを一例にとると、攻撃者は、標的となる担当者と取引先とのメールのやり取りを事前に取引先から窃取したうえで、取引先を装い、かつ、返信文の形でメールを送信する。この場合、社内でセキュリティ研修を入念に実施していたとしても、受信者が当該メールをサイバー攻撃であると気付かずに、添付されたファイルを開封してマルウェアに感染してしまうことは十分に想定されることである。

以上のとおり被害の深刻さ及びセキュリティの難易度を踏まえると、サイバーリスクは企業の継続的な事業活動にあたってもはや看過できないリスクとなっている。

---

[1] 独立行政法人情報処理推進機構「情報セキュリティ10大脅威2020」（2020年4月）
[2] https://www.capcom.co.jp/ir/news/html/201116.html

そして、リスクマネジメントの一環として、サイバーリスクが顕在化しないように事前に適切なサイバーセキュリティ体制を構築することの重要性は論を待たないが、それのみならず、完全に防御することの難易度を考慮すると、サイバーリスクが顕在化した場合の対策シナリオを事前に想定しておくことも重要である。

筆者は、サイバーセキュリティのインシデント対応を専門として、2020 年だけでも 60 件超の対応経験を持つ。

本稿においては、この対応経験に基づいて、標的型攻撃により機密情報が窃取された場合を想定した対応シナリオを調査フェーズ、対応フェーズ及び再発防止策構築フェーズの 3 段階に分けて、各フェーズの留意点を紹介する。

なお、想定シナリオにおいては、サイバー攻撃を受けた企業を X 社、X 社に機密情報を渡していた取引先を Y 社、サイバー攻撃を実施したものを単に攻撃者とする。

2　調査フェーズ

（1）発覚の経緯

発覚の経緯は大きく分けて 3 つある。

一つ目は、自社で検知する場合である。例えば、X 社のウイルスソフトがマルウェアの感染を検知したり、プロキシやファイアウォールが不審なトラフィックを検知したりした場合である。この場合、機密情報が窃取される前に検知できた可能性もあり、3 つの発覚経緯の中で最も望ましい経緯といえる。

二つ目は、外部の第三者から通知を受ける場合である。例えば、警察や当局から通知を受けたり、Y 社から「Y 社も攻撃を受けたが X 社が踏み台にされていた可能性がある」という通知を受けたり、後述のダークウェブモニタリングにおいて偶然発見した者から情報提供を受けたりする場合である。この場合は外部の当該第三者から詳細な情報提供を受けて、自社による調査に役立てることが重要である。

三つ目は、攻撃者からの通知で発覚する場合である。例えば、攻撃者から、窃取した機密情報を公開・流出されたくなければ、一定の時間内に“身代金”を支払うよう要求を受ける場合である。この場合は、限られた期限（例えば 72 時間）の中で事実関係の調査とともに身代金を支払うか否かの意思決定を迫られる点で、最も悩ましい発覚経緯である。

（2）原因調査

ア　デジタルフォレンジックとは

原因調査においては、いつ、どのような攻撃を受けたのかを調査項目として PC、サーバ、ネットワークについてデジタルフォレンジックを実施することになる。

ここで、デジタルフォレンジックとは、事故対応や法的紛争・訴訟に際し、デジ

タル機器の記録における証拠保全及びその調査・分析を行う科学的調査手法をいう。

デジタルフォレンジックは元々デジタルデータを法的紛争に備えて証拠化するためになされていたが、サイバー攻撃の文脈においては、それに加え、説明責任及び再発防止策の観点からも重要となる。

すなわち、サイバーインシデントが発生したことを外部に公表する場合や、取引先及び当局への説明（謝罪）をする場合に、事故の詳細を出来る限り把握したうえでこれを説明することが必要となる。

また、事故後の再発防止対策は、限られた予算内で効果的に策定する必要がある。例えば、パスワードが容易に推知できるもの（例えば「admin」）であったことが原因でサーバ内に不正アクセスされて機密情報が窃取された場合において、ウイルスソフトの強化に費用を掛けることは必ずしも効果的とはいえない。したがって、効果的な再発防止策を策定するうえでも、デジタルフォレンジックにより原因を可能な限り正確に確認する必要がある。

イ　デジタルフォレンジックの留意点

サイバーインシデントが発生した場合、デジタルフォレンジックの実施は法律上の義務ではないものの、上記の観点から、実務上はもはや必須のものといえる。

デジタルフォレンジックにあたっては、実務上以下の 2 つの点に留意が必要である。

一つ目は、サイバーインシデントの増加に伴い、デジタルフォレンジックサービスを提供する事業者も増えているものの、タイミングによっては、直ちに対応可能な事業者が見つからないことがあるという点である。特に攻撃者から一定の期限内に身代金を要求されている場合には、事業者の確保に時間を掛ける余裕はないことから、平時より事業者をリスト化しておくことが重要となる。

二つ目は、デジタルフォレンジックを実施したとしても、その技術上の限界から全ての原因が明らかになるとは限らない点に留意が必要である。例えば、攻撃者による不正アクセスの痕跡を残すアクセスログ（記録）が一定の時間の経過とともに自動的に削除される、マルウェアが自ら消去する機能を持っている等の理由で、サイバー攻撃の原因及び被害の範囲が明確にならないことが少なくない。したがって、デジタルフォレンジックは実務上必須になりつつあるものの、その調査結果に過度な期待を持つことは控えるべきであり、限られた調査結果のもとで意思決定を下さざるを得ないことも想定しておくべきである。

（3）被害範囲調査

上記の原因調査に加えて、どのサーバまで侵入されたか、どの電子ファイルが窃取されたか、PC 及びサーバが依然としてマルウェアに感染していないかといった被害

範囲の調査もデジタルフォレンジックの対象となる。

ただし上記のとおり、デジタルフォレンジックにも限界があることから、補助的な調査手法としてダークウェブのモニタリングが注目を集めている。

ここで、ダークウェブとは、特殊なブラウザによってのみ閲覧及び利用できる Web サイトをいう。特殊なブラウザを利用することで、自らの発信元 IP アドレスを隠して（匿名化して）通信することが可能となる。

図 1 は Tor (The Onion Router) ブラウザと呼ばれるダークウェブを閲覧する際に利用される代表的なブラウザである。

〈図 1〉

Tor ブラウザを利用することにより、自らの発信元 IP アドレスを隠して（匿名化して）通信することが可能となる結果、ダークウェブ上では素性を隠した者同士によって違法な商品・サービスが取引されている。

例えば、図 2 のようにサイバー攻撃を請け負うサービスも存在し、昨今では CaaS（Cyber-crime as a Service。サービスとしてのサイバー犯罪）という呼称も登場している。技術力の低い者でも CaaS を利用することで容易にサイバー攻撃を実行できることも、サイバー攻撃が増加している一因といえる。

＜図２＞

ダークウェブ上では、サイバー攻撃によって窃取された機密情報が公開されたり取引されたりする。

そのため、ダークウェブ上をモニタリングすることで窃取された機密情報が見つかることがあり、それにより被害範囲を把握することも可能となる。

３　対応フェーズ

（１）公表

まず公表の要否について、個人情報保護法に規律される個人情報の漏えい事案は別段として、技術情報のような機密情報の流出について公表すべき法律上の義務はない。

ただし、X 社と Y 社との間の機密保持契約において、機密情報の漏えい時に報告すべき義務が明記されている場合には、X 社は Y 社に対して契約上の報告義務を負う。

また、Y 社への報告にとどまらず、説明責任の観点から、自主的に一般公開することも少なくない。

次に公表の範囲であるが、ここは慎重な判断が求められる。すなわち、上述のとおり、デジタルフォレンジックを実施したとしても、その技術上の限界から全ての原因が明らかになるとは限らず、調査結果においては可能性の摘示に留まる場合が少なくない。例えば調査報告書において「調査の結果、攻撃者により一部のログが削除されていたため流出した機密情報の範囲は判然としないものの、少なくともサーバ内への不正アクセスはあったことから、当該サーバ内に蔵置された機密情報全てが流出した可能性は否定できないところである。」という表現がなされることがある。この場合にどこまで公表するかについて、機密情報の性質、Y 社との関係、無用な混乱を招くリスクといった諸般の事情を考慮のうえ決定することになるが、留意すべきは事後的に隠蔽したと捉えられるリスクが存在することである。

なぜなら、標的型のサイバー攻撃においては、攻撃者が上述のダークウェブ上でサイバー攻撃の事実及び窃取した機密情報を公開することがあり、攻撃者により詳細な被害の内容が事後的に明らかにされるリスクが存在するからである。上記の調査報告書の例でいえば、流出の確度が高い機密情報のみを流出対象として公表したが、それ以外の機密情報も攻撃者により公開された場合に、当該機密情報の流出を隠蔽したという非難を受ける可能性があることに留意が必要となる。

なお、図3は、ハッカー集団「RAGNAR_LOCKER」が運営するダークウェブ上のサイトであり、同サイトには機密情報を窃取した企業名及びその情報が公開されている。

〈図 3〉

（2）当局対応

当局への届け出の要否についても、個人情報保護法に規律される個人情報の漏えい事案は別として、技術情報のような機密情報について届け出をすべき一般的な法律上の義務はない。

ただし、公表をきっかけにサイバーインシデントを覚知した監督官庁から情報提供を求められることもある。この場合も、攻撃者がダークウェブ上でサイバー攻撃の事実及び窃取した機密情報を公開することがあるリスクを念頭に、情報提供の範囲を決定することが重要である。

（３）攻撃者への対応

攻撃者から身代金の支払いを求められた場合、その支払いの可否について定める法律は存在しない。

ただし、攻撃者への身代金の支払いは、将来の犯罪行為の助長につながりかねないことに加え、身代金を支払ったとしても窃取された機密情報が攻撃者の手元において削除される保証はない点に留意が必要である。

この点について、国内での参考事例は乏しいものの、参考までに米国における事例を以下のとおり紹介する。

ア　FBI のスタンス

FBI が公表している「2019 Internet Crime Report」[3]によると、「FBI としては、身代金の支払いを支持しないものの、ビジネスが機能障害に陥った場合に、経営陣が利害関係人、従業員、消費者を守るためにあらゆる選択肢を評価することについて理解するところである。」という考えを示している。

この考えを踏まえると、米国においても、攻撃者への身代金の支払いが直ちに違法の評価を受けるものではないことが分かる。

イ　財務省外国資産管理室による 2020 年 10 月 1 日付勧告

2020 年 10 月 1 日、財務省外国資産管理室（The U.S. Department of the Treasury's Office of Foreign Assets Control。以下「OFAC」という）は、「ランサムウェアの支払いを助長することに関する潜在的制裁リスクについての勧告」（Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments）を公表した[4]。

攻撃者への身代金の支払いに言及する初めての公式な文書と言われている。

OFAC は、外国資産管理法（Foreign Assets Control Regulations）に基づいて情報の提供、処罰の設定、違反者への制裁等を所管する組織で、同法に基づいて制定される各種規制が OFAC 規制と言われる。

OFAC は、サイバー関連制裁プログラム（cyber-related sanctions program）を設け、同プログラムの下で、悪意あるサイバー行為者を指定し、その中には、ランサムウェア[5]を用いた攻撃者やランサムウェア関連の取引を助長した者を含めている。そして、この指定された者と取引を行うことを禁じている。

---

[3] https://www.ipa.go.jp/security/announce/2020-ransom.html ↩

[4] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf ↩

[5] ランサムウェアとは、ランサム（身代金）＋マルウェアの造語であり、従来はデータを暗号化し、復旧の対価として身代金を要求する攻撃手法が一般的であった。しかし、近年、暗号化のみならず情報の窃取も行うという攻撃手法を取るランサムウェアが現れている（二重の脅迫）。

OFAC は、同勧告において、「被害企業に代わってランサムウェアの支払いを助長する金融機関、保険会社、デジタルフォレンジック企業及び危機対応企業といった企業は、将来のランサムウェアの支払い要求を促進させるだけでなく、OFAC 規制に違反するリスクがある」ことを示した。

4　再発防止策構築フェーズ

サイバー攻撃を受けた場合の最後のフェーズとして再発防止策を構築することとなる。

再発防止策においては、当然のことながら原因調査に係るデジタルフォレンジック報告書を参考にして同種の原因による再発を防止する内容とすることが重要である。なぜなら、X 社を標的として成功した攻撃手法は、ダークウェブ上の攻撃者のコミュニティで共有されていると考えるのが自然であり、別の攻撃者が同じ内容の攻撃を試行する可能性が極めて高いからである。

また、既に発生した標的型攻撃において、社内ネットワークの構成に係る情報であったり、各端末へアクセスするための認証情報も窃取された可能性もあるため、ネットワークの構成の変更や、認証情報の変更など、直接の原因への対策に留まらない抜本的な防止策が必要となる。

5　おわりに

本稿で述べたとおり、標的型攻撃による機密情報の窃取というサイバーリスクは、業種や規模を問わずあらゆる企業が直面する深刻なリスクとなりつつある。

テレワークや DX の普及により企業活動のあらゆる部分でデジタル化が進む昨今の流れにおいて、上記のサイバーリスクは増大することはあっても減ることはないと思われる。

サイバーセキュリティの重要性は浸透しつつあるものの、どちらかというと事前の技術的なアプローチに重きが置かれており、サイバー攻撃を実際に受けた場合の対応ノウハウはあまり共有されていない印象である。

本稿で紹介した内容が、サイバーリスクが顕在化した場合の対応シナリオ策定にあたって一助となれば幸いである。

以上

著者略歴

2007 年 3 月	東京大学法学部卒業
2009 年 3 月	中央大学法科大学院卒業
2010 年 12 月	司法修習修了（63 期）・弁護士登録（第一東京弁護士会）
2018 年 10 月	八雲法律事務所設立
2019 年 7 月	カリフォルニア大学バークレー校 School of Law 客員研究員
2019 年 7 月	内閣サイバーセキュリティセンター サイバーセキュリティ戦略本部 SWG タスクフォース 構成員

なお、「米国のサイバーセキュリティ法制と訴訟リスクの検討」、「経営者のための 情報セキュリティ Q&A45」、「IT 関連の最新動向と法務リスク」、「情報漏えいと取締役の情報セキュリティ体制整備義務」、「サイバーセキュリティと企業法務」等の論稿多数。

また、「サイバーセキュリティ」、「データ管理」、「個人情報保護法」等に関する企業向けセミナー実績多数。特にハッキングの実演も交えたサイバーセキュリティに関するセミナーについては好評を博している。

主要取扱分野

サイバーセキュリティ、システム紛争、知財紛争。
なお、サイバーインシデントの増加に伴い、2020 年 10 月から米国の調査機関と提携のうえ、脅威インテリジェンスサービス（ダークウェブモニタリング）事業を始め、企業が直面するサイバーリスクについて法律面のみならず技術面からもサポートを行っている。

筆者への連絡先

〒101-0047 東京都千代田区内神田 1-2-2 小川ビル 9 階
電話：03-5843-8190　Fax：03-5843-8191
ホームページ：https://www.ykm-law.jp（お問い合わせフォーム有り）

掲載日：2021 年 1 月 8 日