セキュリティー・インシデント発生時に企業は捜査機関といかに連携すべきか

はじめに

私は、2013年に日本IBMに入社以来、社内インシデント対応やISMS認証維持などの情報セキュリティー推進活動に従事しています。日本IBM入社以前は、約18年にわたり、神奈川県警察本部の刑事部および生活安全部において、捜査官としてサイバー犯罪の捜査や防犯活動に従事してきました。

近年、内部犯行による大規模情報流出事案や、標的型攻撃メールによるウイルス感染に起因した情報窃取事案などが社会問題化しており、官公庁や企業が内外から攻撃を受けるリスクが増大しています。それに伴って、業務への影響を最小化するための適切なインシデント対応のあり方について、多角的観点から議論されています。

本稿では、捜査官としての企業インシデントの捜査と、企業人としての社内インシデント対応の双方に従事した立場から、セキュリティー・インシデント対応における企業と捜査機関（本稿では警察に限定）との関わりあい方を考察します。

警察のスタンス

お客様とインシデント対応について意見交換をしていると、インシデント発生時に、主体的に警察に相談したり被害申告したりするという発想があまりないことに気が付きます。警察庁は、2012年に「サイバー犯罪に対する警察と民間事業者の共同対処の推進について[1]」、2013年に「サイバー犯罪対処能力の強化等に向けた緊急プログラム[2][3]」を発表し、その中で「民間事業者からの積極的な事件の通報の促進」「民間事業者の知見を活用した犯罪抑止と捜査活動」など、民間事業者との連携・協力の姿勢を強く発信しています。また、産学官の協働と国際連携によりサイバー犯罪に立ち向かう、という趣旨で設立された「一般財団法人日本サイバー犯罪対策センター」（通称JC3）が2014年秋より活動を開始するなど、国をあげてのサイバー犯罪防止の機運が高まっている状況です。このような警察側のスタンスを鑑みると、事業者は、安全安心な社会実現のため、良き企業市民として、サイバー犯罪の被害について警察と情報共有することをインシデント対応の中で検討するべきではないでしょうか。

警察との関わりあい方

警察の活動は、行政警察活動と司法警察活動に二分されています。行政警察活動とは、生命・身体の保護、犯罪の予防・鎮圧、公安の維持という行政目的を達成するための活動であり、分かりやすく言うと犯罪防止のための活動全般を指します。一方、司法警察活動とは、刑法や特別刑法で規定されている犯罪の捜査活動です。ここでは、サイバー・セキュリティーの観点から、この2つの活動の具体的な事例を紹介し、事業者と警察との関わりあい方を考えます。

①行政警察活動

警察は、サイバー犯罪防止のための情報提供を積極的に行っています。インターネットでの情報発信はもちろん、管轄内の企業、学校、地域コミュニティーなどに講師を派遣し、サイバー犯罪の傾向や手口、防犯対策に関する講演（サイバーセキュリティ・カレッジ）を実施しています[4]。

また、不正アクセス禁止法第９条により、不正アクセスの被害にあった事業者は、被害サーバーの分析を警察（厳密には、被害サーバーの所在地を管轄する都道府県公安委員会）に依頼し、再発防止策策定の援助を申し出ることができます[5]。これは、サイバー犯罪の再発防止措置が迅速・的確に講じられることを目的としています[6]。ただし、申し出はすべてが受理されるわけではなく、事業者側に専門知識や技術が不足している場合など、援助が行われる要件を満たす必要があります。

②司法警察活動

捜査機関が、事業者からの申告や相談を受けて「犯罪があると思料するとき（刑事訴訟法第189条2項）」、すなわち、刑法や特別刑法で規定されている犯罪の構成要件に該当する可能性があると判断した場合、捜査に着手することになります。事業者は、以下のような類型において、警察に相談ないし被害申告することを検討すべきであると考えます。

(a)外部からの攻撃

例えば攻撃の発信元のIPアドレスが社外のものである場合など、社内の調査では実行行為者を特定することがほぼ困難なインシデントが発生した場合、IPアドレスがインターネット・サービス・プロバイダー（以下、ISP）管理下のものであれば、ISPに対する差し押さえという強制処分を行わない限り、IPアドレスの利用者を特定することはほぼ不可能です（民事的手続きにより特定することも可能ですが、裁判所からの決定や判決を待たなければならず、時間を要します）。IPアドレス以外の要素でも、明らかに外部からの攻撃を示す兆候があれば、警察に相談ないし情報提供すべきであると考えます。同様の手口が相次いでいる場合などは、個々の事業者がインシデントを通じて入手している以上の情報を警察が持っていることも予想され、捜査により事件解決につながる可能性があるためです。

(b)行為態様が悪質／社会的影響の大きい内部犯行事案

内部犯行の場合は、行為者が特定されているか否か、行為態様の悪質性、損害や影響の大きさなどの点を総合的に勘案する必要があります。損害や影響が比較的軽微な事案で、社内調査で実行行為者が特定でき、行為者が改悛の情、および、損害補填の意思を示している場合などは、内部の懲戒処分のみで済まされるケースが多いように見受けられます。

一方、内部犯行であることまでは判明しているものの、具体的な行為者の特定に至っていない事案で、行為態様が悪質（過失では起こりえない態様）であり、事業者の信頼失墜や損害が多大な場合は、警察に相談することをお勧めします。警察という「公権力」かつ「捜査のプロ」が関わることで行為者が特定され、事案の全容解明につながることが期待できるためです。実際に、私が捜査官として携わった企業インシデントで、社内調査では行為者特定に至らなかったものの、警察が捜査着手したことで実行行為者が特定され、行為者自身から詳細な供述が得られて全容解明につながったという事案がありました（もちろん、そのように好転しない場合もあります）。行為者自身により犯行に至った経緯が明らかにされれば、事業者は、いわゆる不正のトライアングル（機会、動機、正当化）を分析し、再発防止策に盛り込むことが可能となります。

なお、司法警察活動に関して留意していただきたいのは、公権力という言葉のとおり、捜査の目的は、「国家及び社会の秩序維持という公益を図るため」であり、「被害者の被侵害利益ないし損害の回復を目的とするものではない」ということです[7]。すなわち、警察は無料の公営探偵事務所ではなく、あくまでも捜査は、「事案の真相を明らかにし、刑罰法令を適正且つ迅速に適用実現する」ことが最終目的です。従って、ひとたび警察が捜査に着手した場合は、警察は刑事訴訟法や犯罪捜査規範等に基づき、検察に送致するために必要な活動を行うという流れになります。

また、事業者にとって気になるのが、犯罪の発生事実や検挙が広く報道されることによるビジネスへの悪影響です。前述の「サイバー犯罪に対する警察と民間事業者の共同対処の推進について」の中で、「民間事業の運営に影響を及ぼすことに鑑み、事業者の意見を聴いて、公表のもつ社会的意義を総合的に勘案して当否を判断する」と述べられており、事業者側の意向も組み入れられることになっています。

終わりに

現在、いずれの都道府県警でも、サイバー犯罪に特化した部署があり、専門的知識・技術に精通した捜査員が配置されています。捜査は公益のためとはいっても、私自身の経験からも、事件が無事解決し、被害事業者から感謝されたときの喜びはひとしおです。「検挙に勝る防犯なし」の言葉どおり、事件解決がもたらす犯罪抑止効果は多大なものです。

本稿が、インシデント対応のみならず、平時におけるセキュリティー啓発活動においても、警察との連携について検討する際の一助となれば幸甚です。

[参考文献]
[1] 警察庁：サイバー犯罪に対する警察と民間事業者の共同対処の推進について，http://www.npa.go.jp/pdc/notification/seian/jyohotaisaku/jyohotaisaku20120712.pdf
[2] 警察庁：「平成25年版　警察白書」特集I サイバー空間の脅威への対処　第3節　今後の取組，https://www.npa.go.jp/hakusyo/h25/honbun/html/pf130000.html
[3] 警察庁：「サイバー犯罪対処能力の強化等に向けた緊急プログラム」に係る各施策の主な取組状況，https://www.npa.go.jp/kanbou/cybersecurity/H2607_kinkyuprogramFU.pdf
[4] 静岡県警察：サイバーセキュリティ・カレッジ，http://www.pref.shizuoka.jp/police/kurashi/higai/cyber/security.html
一例として、静岡県警では情報漏洩対策も含めた講演を企業からの要請に基づき実施している。
[5] 警察庁：不正アクセス行為の再発を防止するための都道府県公安委員会による援助に関する規則，https://www.npa.go.jp/cyber/legislation/kitei/enjyo_kitei.htm
ここに申出時の書式が規定されている。
[6] 不正アクセス対策法制研究会（編）：逐条　不正アクセス行為の禁止等に関する法律　第2版，立花書房（2012）
[7] 最高裁平成2年2月20日第三小法廷判決、最高裁平成17年4月21日第一小法廷判決

日本アイ・ビー・エム株式会社
セキュリティー事業本部
情報セキュリティー推進

松井 育子
Ikuko Matsui

2013年入社。社内のインシデント対応、ISMS認証維持、セキュリティー啓発活動などに従事。1994年から2012年まで、神奈川県警察本部においてサイバー犯罪特別捜査官として捜査・防犯活動に従事。元神奈川県警部。CISSP（情報セキュリティ・プロフェッショナル）。CFE（公認不正検査士）。