本当に”効く”インシデントマネジメント体制構築のポイント

一般社団法人 JPCERT コーディネーションセンター
早期警戒グループ 兼 情報流通対策グループ　リーダー
情報セキュリティアナリスト　佐々木　勇人氏

現在、企業活動を行う上で、インシデントを前提としたセキュリティ対策が求められている。今日は、自社でインシデントが発生してしまった場合の全社的な対応ポイントを紹介したい。

■JPCERT/CC とは

JPCERT/CC は、国内におけるサイバーセキュリティ上の問題の特定、そしてそれによる被害の拡大を防止するための活動を、主要各国の CERT や国内外のセキュリティ専門企業、ISP 事業者、IT ベンダーと連携を取りながら行っている。

- 脆弱性情報ハンドリング
  ソフトウェアの脆弱性が出た場合の調整。
- 情報収集・分析・発信
  インターネット上に分散配置された観測用のセンサーをはじめ、多方面から得られた情報から、大規模攻撃の兆候や新種の攻撃の兆候をとらえる活動
- インシデントハンドリング
  サイバー攻撃被害を受けた企業・組織の被害復旧、原因究明に向けた調査を支援している。

また、企業にサイバー攻撃が行われた場合、企業と攻撃元の間に入って攻撃遮断等を行うには、様々な専門機関、政府機関との連携が必要となる。この時に、コーディネーションセンターとして、省庁や業界の枠を超えた調整活動を行っている。

■サイバー攻撃により想定される被害は？

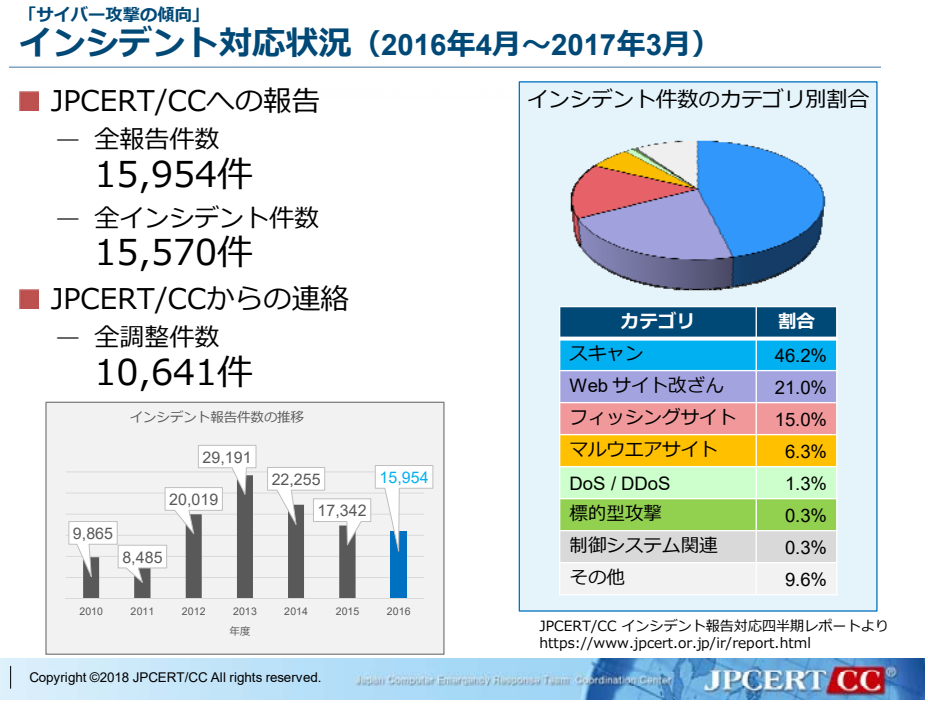
サイバー攻撃による被害としては、情報漏えい、特に個人情報の漏えいが社会的にも注目され、甚大な被害になると想定される。また、インシデント発生後の原因調査や被害復旧のための対応コストも、ある程度の企業規模になると数千万から億単位になる場合がある。

JNSA の調査では、2016 年の個人情報漏えいインシデント概要では、全体で漏えい件数は 1500 万件以上、賠償コストは 3000 億円以上、１社あたりにすると漏えい件数が約 3 万件、賠償コストは 6 億円という結果が出ている。

また、金銭的コスト以外にも、インフラの乗っ取り（いわゆる踏み台）も想定される。自

社の管理が甘かったことで他社に被害が及び、公表段階で自社名が出た場合や自社製品・サービスが踏み台となった場合のレピュテーションリスク、自社ブランドへの影響が想定される。

海外におけるインシデントの傾向では、データ窃取の 1 割が数秒以内、8 割が数分以内に行われる一方、自社への侵入被害に気付くまでは数週間かかっている。侵入原因はパスワードの悪用が半数を超え、攻撃手法は古い脆弱性の悪用が 8 割以上。対策していれば防げるものとなっている。



現在、サイバー攻撃はもはや前提条件であり、被害を受けた場合、組織のガバナンスが問われる風潮は高まっている。

■Connected Industries に向けたセキュリティ対策

インターネット接続製品が多くなる中、自組織の管理が及ばない機器類が増加している。持出機器がソフトウェアのアップデートやアンチウイルスソフトの更新がなされないまま使用されているケースが多く、狙われるポイントとなっている。また、セキュリティ対策のための資産管理システムが狙われるケースも増えてきている。

2017 年 5 月に大きく報道された WannaCry は、当初侵入経路がわからなかったが、その後、出張で持ち出した端末が外部のネットワークで感染し、自社内ネットワークにつないだ瞬間に爆発的に感染が広がったケースがあることがわかった。この WannaCry の感染はまだ収束せず、亜種の感染が増えている。出張先でのネット接続では、持出機器に直接 IP アドレスが振られネット上に見える形になるため、そこで感染してしまう。持出機器以外にも遠隔拠点の端末など社内管理が行き届かないまま直接 IP アドレスが振られて運用されてい

る端末は脆弱性が放置されるケースがあることから、点検が必要である。

また、自社の販売した IoT 製品が攻撃の踏み台になるケースでは、自社製品の脆弱性に対応したくても、様々な流通ルートや関係者が介在しておりメーカーが直接回収することが難しい。

IoT botnet は、2016 年に Mirai が、2017 年には Mirai の改良版である satori が爆発的に感染数を増やしている。乗っ取られた大量の機器は Dos 攻撃など様々なサイバー攻撃の踏み台に利用される可能性がある。従来は、機器の ID パスワードが悪用されたが、2017 年では製品の脆弱性を突いて侵入するケースが増えており、ユーザーが適切な ID 管理をしてもアップデートしない限り根治しない。JPCERT/CC では、被害組織からの連絡をもとに ISP 事業者、設置事業者・販売店、ベンダーとの連携を進め、JVN（脆弱性対策情報ポータルサイト）で情報共有・注意喚起を行っている。

■インシデント対応のポイント

漏えいの一報があった場合、何をしなければならないかすぐに思い浮かぶ人は少ないが、考えなければならないことは多く、段取りが整理されていないと担当者がパンクしてしまう。残念ながら、セキュリティに関するガイドラインは様々な機関から出されているが、インシデント対応についてまとまったものがない。

インシデント対応のポイントとしては、まずは何をしなければならないかゴールから考えるとよい。実際に攻撃による被害が発生した場合、フェーズとしては、被害把握・収束フェーズ、回復フェーズ、定常状態の 3 段階に分けることができる。本来のゴールは定常状態に戻すことであるが、発生初動時には、公表・プレスリリース等第一報を打つところまでをとりあえずのゴールと設定し、情報発信の観点からどのようなインシデント対応が必要か考えるとやるべきことが整理される。

実際に攻撃を受けた場合の報道例からみると、以下のような内容を社内で把握する必要があることがわかる。

① 被害把握（感染被害の範囲、業務停止の有無、個人情報漏えいの有無・件数・内容、金銭被害の有無、取引先への被害有無、二次被害の有無）
② 経緯（発覚の時期・経緯、対応状況、手口）
③ 対応（所管省庁等への届出の有無、顧客対応の状況、今後の対応方針等）

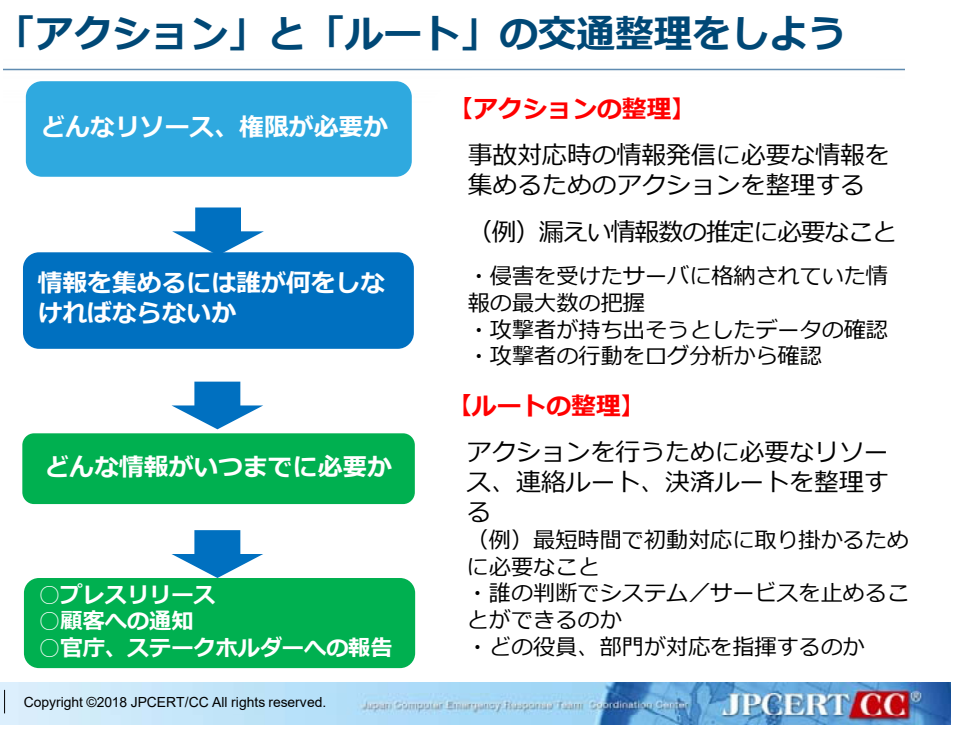
しかし、現実には、初動調査のための緊急調達やシステム停止の判断に時間がかかってしまう、情報が速やかに集まらない等の理由で公表が遅れ、対応の遅さを批判されてしまう等、残念なケースが少なくない。

- 外部からの指摘が所管部門に届かないケース
  標的型サイバー攻撃は外部からの連絡で気づくケースが 70%近い。しかし、報告窓口に通知できない場合、実際のセキュリティ担当部門に届くまで 60 日を要した事例がある。

- 想定外の仕様により被害が発生したケース
  設計・構築時や運用のミスにより、本来保存されていないはずのカード情報がシステムに保存され、それが漏えいしてしまったり、脆弱な設計や運用不備で既知の SQL インジェクション攻撃等古くからある攻撃手法で被害にあうケース、攻撃者にバックドアプログラムを設置され情報が抜かれてしまうケース等がある。
- 状況が一向に把握できないケース
  部署間で被害状況の共有がうまく進まず、対応が遅れるケースもあるが、攻撃者の意図が掴めずに被害の実態の把握が遅れるケースが
  ある。2017 年の台湾遠東商業銀行へのサイバー攻撃では、不正送金の発覚を遅らせるため、ランサムウェアがばら撒かれた。このケースでは不正送金にも気づき対応がなされたが、目の前の被害に気を取られて、隠された被害の発見が遅れることが懸念される。

■インシデント対応の体制強化に向けて

インシデント対応の体制を強化するにあたって、まずはアクションとルートの整理がポイントとなる。



整理に当たっては、2017 年 12 月のサイバーセキュリティ経営ガイドライン改訂時に追加された「付録 C インシデント発生時に組織内で整理しておくべき事項」が参考になる。

具体的なポイントとしては、以下が挙げられる。

- 自組織で管理するシステムに加え、外注で運用するシステムやデータ連携する外部シ

ステムの状況や管理情報の把握や契約・運用規約の点検

- 外部機関からの情報提供に速やかに対応するための社内連絡ルート点検、外部連携機関の連絡先等確認
- CSIRT の設置も含めた、部門を超えた対応体制の整備

CSIRT を設置することでインシデント発生時の初動時間が短縮するだけでなく、他社の CSIRT との情報交換等を自社の対策強化につなげていくことができる。また、体制作りは一から始めるのではなく、既存の災害時対応、BCP 対応等の体制を参考に体制構築のプランやマニュアル作りを進めていくと効率がよい。

脆弱性情報やその脆弱性を突く攻撃は次々に出てくるので、日頃から情報収集が必要となる。JPCERT/CC では、メールニュースや Web サイトで情報提供・注意喚起を行っているのでぜひ活用していただきたい。