情報セキュリティにおけるインシデントマネジメントの必要性

企業の情報セキュリティに関するテーマは、依然として注目度が高い。特に近年では、標的型諜報攻撃[1]、スマートデバイスを狙った攻撃[2]、ウェブサイトを狙った攻撃[3]といった、外部からの悪意のある攻撃について、官民の様々な組織が活発に注意喚起を行っている。また、内部犯行やオペレーションミスによる情報漏えいについても、度々マスメディアで報道されている。

情報セキュリティに関するリスクが顕在化しないための取組みはもちろん重要であるが、悪意やミスによる情報漏えいは、従来の取組みを徹底したとしても完全に防ぐことは難しい。そこで本稿では、情報セキュリティに関するトラブルが発生した際に適切な対処が行えるよう、インシデントマネジメント強化の必要性やポイントについて解説する。

1. 情報セキュリティインシデントについて

情報セキュリティといっても、情報の種類（機密情報、個人情報等）や、対策の観点（IT、法律、従業員の意識、不正防止等）が多岐にわたるため、情報セキュリティインシデント[4]の発生状況を網羅的に把握することは難しい。ここでは、独立行政法人情報処理推進機構（IPA）による「2013 年度情報セキュリティ事象被害状況調査」、NPO 日本ネットワークセキュリティ協会（JNSA）による「2013 年 情報セキュリティインシデントに関する調査報告書［上半期 速報版］Ver.1.1」から、情報セキュリティインシデントの発生状況に関するデータを紹介する。

（1）コンピュータウイルスやサイバー攻撃による被害の状況

2013 年に IPA が企業を対象に実施した「2013 年度 情報セキュリティ事象被害状況調査」（調査期間：2012 年 4 月～2013 年 3 月）の結果は図 1 の通りである。同調査によると、67.1%[5]に上る企業がコンピュータウイルスに遭遇し、13.8%[6]がサイバー攻撃に遭っており、内部による不正の被害は 2.1%の企業で確認された。

---

[1] 特定のターゲットから情報を盗み出すことを意図した、様々な手法によるサイバー攻撃等を指す。「やりとり型」と呼ばれる、何気ないやりとりでターゲットを信用させてからウイルスメールを送るケース等、手口の巧妙化が見られる。

[2] 急激に普及しているスマートフォンやタブレット機器の脆弱性をついたサイバー攻撃等を指す。その普及が非常に速いため、セキュリティ対策が進んでいないことに付け込んだ攻撃が増加している。

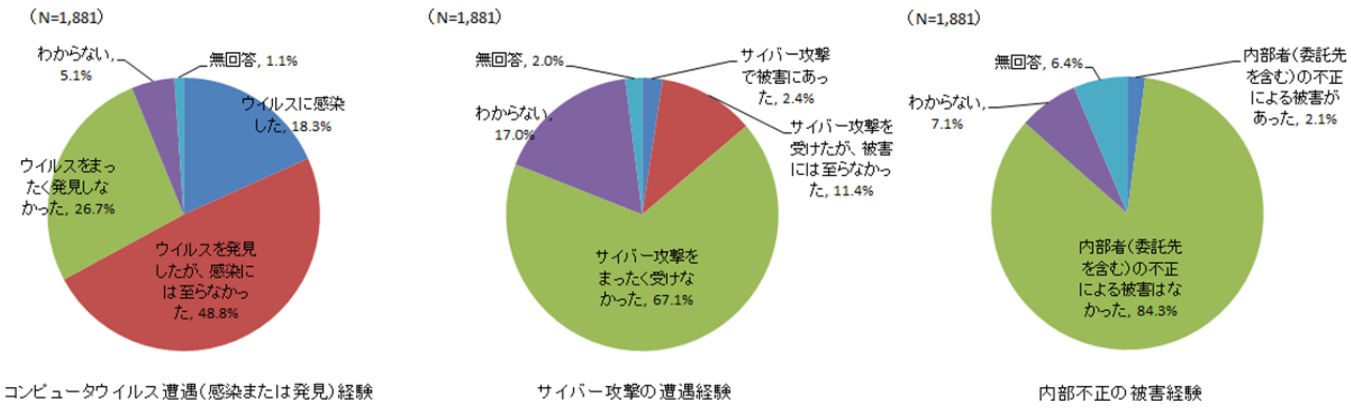
[3] 政治的な意図をもって政府機関のウェブサイトが狙われることがある他、金銭詐取を目的として金融機関のウェブサイトが狙われていることが確認されている。

[4] 本稿で記載する「情報セキュリティインシデント」は、JIS Q 27001:2006 における「望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの」を定義する。

[5] 図 1「ウイルスに感染した」「ウイルスを発見したが、感染には至らなかった」の合計値。

[6] 図 1「サイバー攻撃の被害にあった」「サイバー攻撃を受けたが、被害には至らなかった」の合計値。

■図１ 企業の情報セキュリティに関するインシデント遭遇経験



出典：IPA「2013 年度 情報セキュリティ事象被害状況調査」より弊社作成

（２）個人情報漏えいの発覚件数、および、想定被害額

漏えいが発覚した情報の中でも、特に個人情報については、被害の拡大防止等の観点から積極的に公表するという対応が企業に根付いてきている。JNSA が報道情報やプレスリリース等をもとにまとめた 2012 年上半期の個人情報漏えいインシデントの調査結果は図２の通りである。個人情報漏えいは、公表されているだけでも 1 日に平均 5 件以上発生しており、個人情報漏えいインシデントの「一件当たりの平均損害賠償額[7]」は 3,787 万円にも上る。

■図２ 2012 年上半期 個人情報漏えいインシデント 概要データ

漏えい人数	123万9,626人
インシデント件数	954件
想定損害賠償総額	347億9,865万円
一件あたりの平均漏えい人数 ※1	1,349人
一件あたり平均損害賠償額 ※1	3,787万円
一人あたり平均損害賠償額 ※2	5万7,710円

※1：平均値は、被害者数が不明のインシデントを除いて算出している。

※2：この平均値は、一件当たりのばらつきを吸収するため、まず、各インシデントの一人あたりの想定損害賠償額を算出し、そこから全てのインシデントの一人あたりの想定損害賠償額の平均額を算出している。よって、想定損害賠償総額を漏えい人数で割った値ではないことに注意されたい。

出典：JNSA「2013 年 情報セキュリティインシデントに関する調査報告書［上半期 速報版］Ver.1.1」より弊社作成

[7] 同調査では、JNSA が「JNSA Damage Operation Model for Individual Information Leak」として定めた基準により、個人情報が漏えいした個人全員から損害賠償請求がなされた場合、最大でどの程度の損害賠償額となるかを計算している。

なお、ここでの損害賠償額は、「漏えい個人情報価値（機微情報の度合い等を踏まえて算定）」×「情報漏えい元組織の社会的責任度」×「事後対応評価」の式で計算されている。この式に表されているように、「事後対応評価」すなわち「事後対応の内容の優劣」は、最終的に企業に与える損害の大きさを左右する重要な要素となっている。

2. インシデントマネジメントの基本原則

情報セキュリティインシデントは、企業において顕在化する可能性が高いリスクであり、かつ、顕在化した際には社内外に大きな被害を及ぼす可能性がある。そのため企業は、「インシデント発生の防止策」を講じた上で、日頃から「インシデントの発生に備えた対応体制を構築」し、「万が一インシデントが発生した際には、早急に被害の最小化を図る対策をとれる」ようにしなければならない。

このように、情報セキュリティインシデントへの備えは、企業の危機管理（クライシスマネジメント）におけるインシデントマネジメント体制の整備・強化の観点を踏まえて実施することが重要である。ここではまず、危機管理におけるインシデントマネジメントの基本原則をまとめる。

（１）被害拡大防止・信頼回復

インシデントが発生した場合の企業の危機管理においては、ステークホルダーの被害を最小限に抑えることが、最大の目的となる。企業側の都合で事実を公表しないといった対応は、もはや世の中には受け入れられ難い。例えば、個人情報が漏えいした場合は「振り込め詐欺」等に悪用される可能性もあり、漏えいの可能性が判明した時点で注意喚起を行わなければ、被害の拡大を招きかねない。特に近年では、公益通報者保護制度の充実や、ソーシャルメディアの発達等により、不祥事の隠ぺい等の企業の望ましくない行為が世の中に暴露されるケースが増えている。漏えいしたことの事実を公表することより、隠ぺいとみなされるような対応を行う方が、企業にとっては多大なリスクを伴うことを念頭に置く必要がある。

インシデントマネジメントにおいては、ステークホルダーの被害拡大防止・信頼回復に最優先に取組むことが、企業に与える被害の極小化に繋がることを強く認識するべきである。

（２）スピード・透明性

ステークホルダーの被害拡大防止・信頼回復のためには、スピードと透明性が極めて重要となる。特に対応のスピードについては、ステークホルダーへの連絡・公表が遅れたために被害が拡大した場合、損害額が膨らむことはもとより、「隠ぺい体質」といった批判にも繋がりかねない。

また、判明した事実をすべて公表し、透明性の高い対応を行うことも不可欠である。一度事実を公表した後に、その事実とは異なった情報（漏えい原因が異なる、漏えい件数が極端に増える等）が出てくると、信頼の回復が非常に困難となる。顧客やマスメディアから、「まだ情報を隠しているのでは」という疑いの目を向けられると、それを払拭することは難しく、長期に渡って企業イメー

ジが毀損することは避けられない。

（３）社内外との効率的な連携

インシデント発生時の対応に際しては、平常時とは異なった多くの対応を、様々な関係者と連携しながら、短時間で行う必要がある。そのため、事態に応じた招集体制や連絡先を整備し、事態解決に必要な連携を効率的に図れるようにしておくことが重要である（図３）。

なお、招集の要否についてインシデントが発生してから検討するルールでは、必要な体制を即座に構築することができず、初動が遅れる要因の一つとなる。少なくとも社内の関係者については、一定のインシデントが発生した際にはトリガー（招集基準）に従って自ら参集するよう徹底することが、効果的である。

■図３　インシデント対応組織が連携する可能性のある関係者の例　（弊社作成）

事実確認：セキュリティ担当部門、IT 部門、内部統制担当部門、財務部門
対外対応：広報部門、IR 部門、監督官庁との渉外担当部門
意思決定：経営者
その他：経緯等の記録を行う補助要員、外部の各種専門家

3. 情報セキュリティインシデント発生時の対応における基本的な流れ

次に、情報セキュリティにおけるインシデント発生時の対応の基本的な流れについて解説する。

（１）発見・発覚

組織や個人がインシデントの発生に気づいた際は、その後の対応がスムーズに行えるように、適切な情報（発生時の状況、漏えいした情報の内容・件数、想定される原因、現状の対応状況等）の収集を行うとともに、あらかじめ定められた関係者に速やかに周知・連絡を行う。

（２）事実確認・トリアージ

連絡等を受けた緊急時の対応組織（例：リスクマネジメント事務局等）は、可能な範囲で早急に事実確認を行う。

また、組織のリソース（人員体制等）には限りがあるため、事態の重大性を踏まえて対応の必要性に関する優先順位づけ（トリアージ）を行い、招集する関係者の範囲等を決定の上対応を進める。

（3）応急措置

被害拡大防止のために、とり得る応急措置を早急に講じる。

例えば、Web サイトからの情報漏えいであればそのサービスを停止する、情報の誤発送であれば可能な限り回収する等、ある程度の頻度で発生が想定される事態については、応急措置の内容を決めておくことも重要である。

（4）調査・重要度の判定

事実確認、影響範囲、原因等の調査を進め、漏えいした情報の種類ごとに今後想定される事態を整理し、重要度を判定する。

（5）通知・届出・公表等の検討

事態の重要度については、漏えいした情報の内容、影響範囲、漏えい原因、二次被害防止の観点を踏まえて総合的に判断し、顧客、監督官庁、報道機関等への連絡・公表の必要性について検討する。また検討の結果、外部への公表等の必要性が高いと判断された場合には、可能な限り迅速に対応を行う。

（6）二次被害防止措置・顧客対応の検討

原因や事象によっては、被害の拡大防止に向けた更なる対応を講じる。顧客へのお詫びや補償を検討する等の対応を実施して、事態の収束を図る。

4. 情報セキュリティインシデントへの対応における CSIRT の重要性

情報セキュリティインシデントへの対応に際しては、発見、事実確認、応急措置等に関して非常に高度な専門知識を要する場合があるため、社内外の専門家と連携を図りながら事態の解決にあたる必要がある。また、適切に連携を図り、必要な情報を集めて対策を検討するためにも、一定以上の専門的知見が必要となる。そのため、CSIRT[8]という組織を設置し、情報、ノウハウ、人的リソース等の集約・確保を行っている企業もある。

CSIRT 設置のメリットとしては、その企業の情報セキュリティインシデントへの対応レベルが向上することに加え、様々な企業の CSIRT 同士が情報共有を行うネットワークに参加することで、新たな脅威の発生状況や、他企業の対策状況等に関する情報収集の幅が広がることが挙げられる。

利用価値の高い情報を多く持っている企業等については、それだけ情報漏えいの発生頻度や影響度も大きいことが想定されるため、CSIRT を設置する等により、さらに専門的な知見を踏まえたインシデント対応を実行できる体制の整備を検討することも重要である。

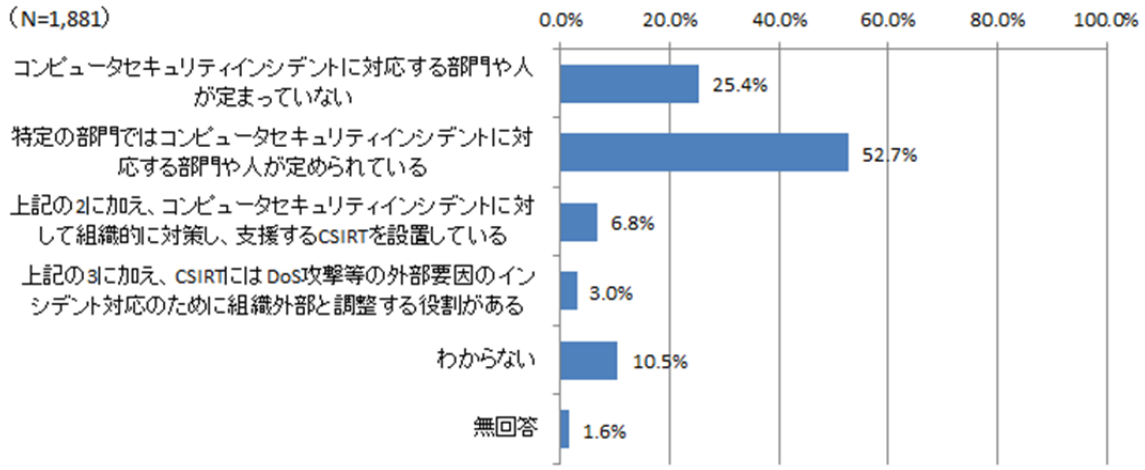
[8] Computer Security Incident Response Team：コンピュータセキュリティに関するインシデント対応組織を指す。CSIRT の詳細については、一般社団法人 JPCERT コーディネーションセンターが提供している CSIRT マテリアル（https://www.jpcert.or.jp/csirt_material/）にも詳しい情報がまとめられている。

5. 企業の現状

情報セキュリティに関するインシデントマネジメント体制構築や、CSIRT の設置については、その重要性が指摘されている一方、企業の体制整備は途上にある。

2013 年に IPA が企業に向けて実施した調査では、52.7%の企業が「特定の部門ではコンピュータセキュリティインシデントに対応する部門や人が定められている」と回答した一方で、「コンピュータセキュリティインシデントに対応する部門や人が定まっていない」もしくは「わからない」と回答した企業が 35.9%あり、今後さらに対策を進めていく必要がある（図４）。

■図４ 情報セキュリティに関する事故や異常事態への対応体制



出典：IPA「2013 年度 情報セキュリティ事象被害状況調査」より弊社作成

6. 平時からの備え

情報セキュリティにおけるインシデントマネジメントを適切に行うためには、体制整備、対応レベルの維持・向上について、平時から組織的に取組むことが重要であり、以下にそのポイントをまとめる。

（１）インシデントマネジメント体制の整備

対応体制やルールの整備が行われていなければ、インシデント発生時の対応を適切に行うことは困難である。まずは、人的リソースの確保、社内外の連携体制の整備、緊急時の対応ルールの整備等を行い、万が一の際の備えを進める。

（２）対応レベルの維持・向上

インシデントマネジメントを、リスクマネジメントの一環として位置づけ、組織的に対応レベルの維持・向上を図ることが、活動を定着させる上で必要となる。具体的には、次のような取組みを計画的・継続的に実施していくことがポイントとなる。

a.リスクの洗い出し

インシデント発生に気づくためには、そもそもそのようなリスクがあることについて、組織として把握し、組織内に周知することが重要である。リスクマップ等を活用し、リスクの洗い出しを行い、関係者に情報共有を図る。

b.情報の収集と分析

日々発生する大小様々なインシデントについて、情報を蓄積するとともに、定期的にその情報を分析し、対応レベルの向上に活用する。

c.教育・訓練

インシデント発生時に招集する対策本部要員に対して実働訓練を実施し対応力の向上を図る、全社員に向けて E ラーニングや標的型攻撃メール訓練（偽のウイルスメールを特定の対象に送り、開封しないか等を確認する訓練）等を行うことで意識啓発を図る、といった対策を継続し、担当者及び従業員の知識・意識の継続的な向上を図る。

情報セキュリティインシデント対応の成否は、「事後対応の内容の優劣」にかかっているといっても過言ではない。いざという際に、ステークホルダーの信頼回復に向けて素早く・適切な対応を取るため、平時より危機管理の観点からの準備を行うことが求められる。

［2014 年 4 月 7 日発行］

東京海上日動リスクコンサルティング株式会社
ビジネスリスク事業部 グローバルリスクグループ
〒100-0005 東京都千代田区丸の内 1-2-1 東京海上日動ビル新館 8 階
Tel.03-5288-6556 Fax.03-5288-6625
http://www.tokiorisk.co.jp/

