事業継続性を確保するためのインシデント・レスポンス

2020 年 11 月

名和 利男

はじめに

「事業継続性の確保」は、企業経営者に共通する課題である。そのため、これまでの多くの企業が、2005 年 3 月に経産省から公表された「企業における情報セキュリティガバナンスのあり方に関する研究会」参考資料の「事業継続計画策定ガイドライン」[1] を参照しながら、事業継続計画（BCP）の策定に努力してきた。

この事業継続計画のガイドラインは、誰が事業継続計画を構築すべきかについて、次のように示している。

> "企業経営者は、個々の事業形態・特性などを考えた上で、企業存続の生命線である「事業継続」を死守するための行動計画である「BCP（Business Continuity Plan）」及び、その運用、見直しまでのマネジメントシステム全体である「BCM（Business Continuity Management）」を構築することが望まれる。"

そして、2017 年 11 月に経産省から公表された「サイバーセキュリティ経営ガイドライン Ver 2.0」[2] では、次の重要なメッセージが示された。

- セキュリティ対策の実施を「コスト」と捉えるのではなく、将来の事業活動・成長に必須なものと位置づけて「投資」と捉えることが重要
- セキュリティ投資は必要不可欠かつ経営者としての責務である

さらに、このサイバーセキュリティ経営ガイドラインは、「サイバー攻撃によって純利益の半分以上を失う企業が出るなど、深刻な影響を引き起こす事件が発生している」という危機感を示した上で、「経営者が適切なセキュリティ投資を行わずに社会に対して損害を与えてしまった場合、社会からリスク対応の是非、さらには経営責任や法的責任が問われる可能性がある」と警告に近い表現で、強いメッセージを伝えている。

このように、国が経営者に対して、企業存続の生命線である「事業継続」を死守するよう促し、セキュリティ投資をするよう強く要請しているにも関わらず、多くの現場において、いまだに「従来の発想とやり方」で対策強化をしている状況が見られる。

---

[1] https://www.meti.go.jp/policy/netsecurity/downloadfiles/6_bcpguide.pdf

[2] https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide2.0.pdf

「従来の発想とやり方」とは

日本企業の経営者が陥りやすい「従来の発想とやり方」とは、端的に表現すると、「安全な領域を確保するために必要最小限のセキュリティ環境の整備」である。これは、一般的な人間の認知能力や推論能力で把握できる「物理的な安全策（セキュリティ）」を、自組織のコンピューター空間およびネットワーク空間に適用したものと言える。つまり、不安全な（自組織でコントロールできない）「インターネット」と安全な（自組織でコントールできる）「組織内ネッワーク」の間に境界線（エッジ）を設けて、ファイアウォールや侵入検知システムなどの技術を使いながら、防御を行うことである。そして、ユーザーが PC を操作して境界線を跨いで「インターネット」にアクセスするため、ウィルス対策ソフトを利用して「組織内ネットワーク」への侵入を防ぐようにした。

ここで重要なポイントがある。「従来の発想とやり方」で有効性が発揮された場（あるいは領域）は、自組織が保有し運用していたシステムおよびネットワークである。つまり、業務で利用するコンピューターシステム（PC、サーバーなど）およびネットワーク（内部通信網で接続されたコンピューターシステム全体）が、すべてオンプレミスで運用されていることを前提としたのである。

この概念は、昔のお城を守る仕組みに類似する。つまり、「点で守る」ような努力を積み重ねていたのである。これが、「従来の発想とやり方」である。

「点で守る」vs「面で守る」

近年、多くの日本企業が、「IT 費用の削減」と「利便性・生産性の向上」という相反する二つの課題を同時に解決させるべく、無線 LAN（Wi-Fi）への移行、クラウドサービスの積極的利用、IoT の導入、MSP[3] への委託などを進めている。特に最近では、コロナ禍の影響により VPN や DaaS[4] の利用が拡大している。各種サービスが無線信号や社外を経由するものに置き変わったことで、視覚的に分かりづらくなっているが、守るべき対象は自組織を一気に飛び越えて、他組織が保有および運用するコンピューターおよびネットワークに急激に拡大してしまったのである。

ところが、「従来の発想とやり方」で守ることができる対象は、費用と人的リソースのかかる「オンプレミスで運用されている領域」のみである。それより遥かに広い領域となる「他組織が保有及び運用するコンピューターやネットワーク」の守りに対しては、契約あるいは身勝手な期待や思い込みで「大丈夫だろう」と信じることしかできない。これでは、事業継続の確保の観点で責任を放棄していると見なされても仕方ない。

近年、生産年齢人口の減少が強く懸念されている中で、コロナ禍による深刻な経済的影響を受けたことにより、ほとんどの企業は、投資を最小限にしつつ事業の生産性を一気に向上させ

---

[3] MSP（Managed Service Provider）とは、顧客の利用するコンピューターやネットワークなどの IT システムの運用や監視、保守などを行い、利用可能な状態に維持するサービスを提供する事業者のこと。

[4] DaaS（Desktop as a Service）とは、デスクトップ仮想化システムをクラウドサービスとして提供すること。

て、短期間で利益を生み出していかなければならない。そのため、AI（人工知能）、IoT、ビッグデータ等「他組織が保有および運用する資産」を積極的に活用せざるを得ず、かつ DX（デジタルトランスフォーメーション）や 5G による事業基盤の大きな変革を遂げていかなければならない状況になりつつある。したがって、日本企業は、費用と人的コストのかかる「オンプレミスで運用されている領域」を再構築することは不可能であるといえる。

そのため、今後のインシデント・レスポンスは、「面で守る」姿勢で臨まざるを得ないのである。

インシデント・レスポンスの現状

最近、マルウェア感染（特にランサムウェアや Emotet）や不正アクセスなどのサイバー攻撃により被害を受けた企業が、その後のお詫びのプレスリリースにおいて、「さらなるセキュリティ強化」を宣言するものを多く見かける。その前後の文脈を確認しても、「従来の発想とやり方」から脱却する姿勢を打ち出しているものをほとんど見かけず、同様な被害を繰り返す企業すら出てきている。

これは、事業継続性を確保することを目的としたインシデント・レスポンスに着手していない表れである。そして、いまだに、その実務を担う CSIRT 機能を事実上 IT 部門に押し付けている状況が見られ、セキュリティ人材を育成するのみで現状を乗り越えようとする、浅はかで短絡的な取り組みがまかり通っている。

そこで、筆者のインシデント・レスポンスの支援活動の中で、主に管理者層からの要請に対応する経験から整理した、「事業継続性を確保する」ための4つの「見出されたこと（Findings）」および4つの「得られた教訓（Lessons Learned）」を紹介させていただく。

●見出されたこと（Findings）

1. 整備された連絡体制がうまく機能しない
   - 異動で担当になっただけの窓口担当者が役割を認識していない（背景や文脈を知らない）
   - 受領した連絡内容のみでは判断できない（あるいは伝達相手へ配慮不足）
   - 受領した情報の伝達のみに徹する（すべて上司に判断を仰ぐ／責任を取れない）
   - 情報管理が厳しすぎて、機密性レベルが定義されていない情報を転送できない
   - 受信メールの内容が通常ではないため、不審メールとして処理（削除）した
2. メンバーが役職者ばかりで、実動要員が不在
   - インシデント（であるかどうか）の判断を現場任せにしている（自分たちで精査できない）
   - 情報通信技術(IT/ICT）の教養と経験が不足（適切な指示が出せない）
   - 部下からサポートを受けないと行動をとれない
   - 責任追及に偏重しがち（“責任者が責任者を探す“）
3. 適切な状況認識ができていない
   - 関連情報として入手するものが日本語のみ（英語による詳細情報をスルー）

- 外部のチーム(組織)とのコミュニティケーションができていない
- 専門技術用語を伴う報告から全体像を把握することが難しい
- 顕在化した情報のみで認識しようとする傾向が強い
- 潜在化した可能性のある事実への追求姿勢を持たない

4. インシデントハンドリングの流れに一貫性がない

- 事前に取り決めたインシデント対応を推進するには高いレベルの教養や習熟が必要だった
- 兼務している業務の知識や経験から影響を受けた発言や判断がされ、衝突する
- 影響を受ける他部門の内情が分からないため、適切な判断ができない
- 上層部から、インシデント対応行動の方針や適正化に繋げる指示がまったくない
- インシデント対応の流れに手戻りが多い

●得られた教訓(Lessons Learned)

A. メンバー間の定例会(特に勉強会)を実施する

- インシデント発生時においてやり取りする相手の顔が見える
- やり取りにおいて必要となる認識・教養の統一化を図ることができる
- インシデントハンドリングの流れや規定等の改善を図ることができる
- 上層部の考え方を把握することができる
- 発生した事例を把握することができる

B. 継続的な情報共有を可能とする仕組みを構築および継続運用する

- 連絡先の疎通確認をすることができる(異動等による疎通不能の回避)
- サイバー脅威の変動状況に(ある程度)追いつくことができる
- メンバー間の一体感を感じることができる
- 潜在化した可能性のあるイベント(事象)を検知するトリガーとなる
- 教養不足を補うことができる

C. 定期的にサイバー演習を実施および評価を行い、その結果を次の演習につなげる

- メンバー間の関係性強化を図ることができる
- 教養に加え、(擬似)経験を積み上げることができる
- メンバー間で流通する情報に対する関心が向上する
- インシデントハンドリングや規定等の具体的な改善点を見出せる
- 全般的なインシデント対応に係る時間を短縮できる

D. 経験者(特に SME、内容領域専門家)を獲得(ヘッドハンティング)する

- 組織内で「育成を担当する者」を、適切に育成することはできない
- 候補者の信頼性確認の一つとしてソーシャル・ネットワーキング・サービスを利用できる
- 新人研修のブラザーシスター制度のような「教養と経験豊かな先輩」が必要である
- セキュリティ人材の育成は、持続的・倫理的・主体的・発展的であるべき

継続的な努力の必要性

日本の企業が、業務の効率化を目的にやや画一的なオンプレミスのコンピューターやネットワークを運用していた「昔の時代」は、インシデント・レスポンスのための知識体系を構築しやすかった。しかし、「今とこれからの時代」は、常に変動する顧客の関心や社会のニーズと同調するように事業基盤を変容していかざるを得ない。そのような環境におけるインシデント・レスポンスの知識体系は、構築したとしても、すぐに役に立たなくなる。非常に厄介な状況である。

そのため、経験に裏付けられた教訓をその後の改善策に確実に反映するというサイクルが必要となり、そのサイクルを確実に積み重ねていく覚悟が必要となる。これは、実務を担当する CSIRT でなく、責任を持つ上層部が主体的に行うべきである。この努力を怠り、自組織ばかりか顧客に被害を与えてしまった場合、謝罪するのは責任を持つ上層部である。ここ数年の間に発生した深刻なサイバーセキュリティ事案に関するお詫びを伴った記者会見で、多くの方が認識しているはずである。

これまでは、謝罪と金銭的な補償だけで済ませることができていたかもしれないが、今後、事業基盤に DX を浸透させなければ企業として生き残れない中で、想定外に発生したインシデントは、顧客の身体や命に深刻な影響を与える可能性が出てくることを見込まなければならない。今年 2020 年において、他国で発生した複数の産業制御システムへのサイバー攻撃が、その可能性を裏付けるものとなっている。

おわりに

事業継続性を確保するためのインシデント・レスポンスの能力獲得は、自組織の利益を守るだけではない。今後、他の組織の利益や人の身体を守ることにもつながっていくものになることを、私たちは強く認識し、行動に移していかなければならない。

（了）