「期待した結果につながった対応」と「改善を要する対応」事例に見る背景および外的要因

2021 年 1 月

日々、報道や SNS を通じて、サイバー攻撃や不正アクセスの被害を受けた日本企業に関する情報が伝えられており、その頻度と数は増加している。

ところが、テレビの全国放送や大手新聞で伝えられるサイバー事案は、社会的影響の大きいものに限られているため、国内の有名企業や政府機関に関するものがほとんどである。それも全て伝えられているわけではなく、担当記者の努力により「運良く」掲載が実現したもののみである。

そのため、公にされないサイバー事案は非常に多い。特に、有名企業の海外拠点のみで閉じた事案や国内の中堅以下の企業における事案は、インターネットで探しても、実際の状況を理解するために必要な情報を得ることが困難となっている。

そのような中でも、企業におけるサイバーセキュリティ対策部門（あるいはその担当者）は、さまざまなコミュニティやセキュリティ専門会社が提供するサービスを利用することで、サイバー攻撃に関するデータや分析情報を獲得することができるようになってきており、予算や人的リソースの制約を受けながらも、「技術的対策」を立案および計画して自社の対策の適正化と改善につなげようとしている。

しかし、IT やインターネットに依存した業務の効率や生産性の向上に対して、一定の制約を与える「運用的対策」については、発生し得るサイバー事案が業務に及ぼすリスクを導出することを前提としたものとなるため、サイバーセキュリティ部門が主体的に立案および計画することはできない。たとえ、策定したとしても、業務を推進する部門が受け入れなければ、その意味はなくなる。

したがって、「運用的対策」は、営業や生産などの「事業部門」が行うべきものとなる。ただし、業務に及ぼすリスクを過小評価しては、対策効果が著しく低下する。そのため、発生し得るサイバー事案を十分に「理解」していただき、業務に及ぼす影響を「導出」した上で、バランスの取れた運用的対策を立案することが重要となる。この「事業部門」が行う「理解」と「導出」は、短期的に業務の効率を下げることになるが、近い将来に発生する、「業務を完全に止める可能性の高い甚大なサイバー事案」を回避あるいは（発生したとしても）被害拡大の抑制につなげることができる。

筆者や同様な活動をしているサイバーセキュリティ専門家などは、被害を受けた組織や団体に対する観察や分析を重ねながら、昨今のサイバー脅威に適合した対策を実現いただくべく、次のようなメッセージを相手の状況に応じたさまざまな表現で発信している。

- 【ネガティブ表現】従来の情報セキュリティ対策（ルール徹底や技術的措置）に基づく強化」だけでは、サイバーリスクの高まりを軽減することはできない。

- 【ポジティブ表現】関係先（サプライチェーン）を含めた形で「サイバーセキュリティ対策（強化されたセキュリティ運用）の維持」を組み込んでいくことで、サイバーリスクをコントロールすることができる。

残念ながら、これらのメッセージは、すべての企業や団体には届いていない。一部届いたとしても、十分な理解と行動変容に結びついている事例はほんの僅かである。この要因として、筆者は次の 2 つがあると考えている。

- 送り側である（筆者を含めた）サイバーセキュリティ専門家が、テクニカルに偏重したことを話し、受け側の業務の見識や実情理解を怠っている。（受け側に十分に寄り添った姿勢が見られない）
- 受け側である企業や団体が、サイバーリスクに対する「想像力」を未だ有していない。

この「想像力」の定義は、「感覚（視覚、聴覚など）で得ることなく、心的な像、感情、アイディアを作り出す能力のこと」あるいは「知識を問題解決に応用することができる、経験と学習を統合させた基本的要素のこと」である。そして、この「想像力」の基本的訓練は、「ストーリーテリング」（伝えたい思いやコンセプトを、それを想起させる印象的な体験談やエピソードなどの“物語”を引用することによって、聞き手に強く印象付ける手法）であるとされている。

企業や団体が自社のサイバーリスクを理解し「運用的対策」を導出するためには、彼らが想起できる物語としてインシデントの事例や対応の結果を語ることが有効と考える。

ただし、サイバーセキュリティ専門家が観察した事例を、大まかに「期待した結果につながった対応」と「改善を要する対応」に分けた上で、それらを注意深くレビューおよび分析したところ、対応者の知見や能力だけではなく、発生したインシデントの「種類」、「場」そして「タイミング」などの外的要因が、結果に大きな影響を与えていた。そのため、第三者による主観的な評価による良い／悪いという判断を画一的にすることは難しい。基準となる大まかな指標や目安としての「最善策（ベストプラクティス）」を提供することはできるが、それぞれの組織に応じた適正性を確保したインシデント対応のあり方は、その背景や外的要因に依拠している。また背景や外的要因の情報を伝えることで、聞き手が事例と比較して自社のサイバーリスクを想像しやすくなるといえる。

そこで、筆者の活動におけるインシデント対応支援やその助言の中で、直接把握することができた事象を、背景や外的要因を補ってストーリーテリングのような形で紹介したい。

●「期待した結果につながった対応」の背景と外的要因

A 社. 採用した CISO やサイバーセキュリティ人材に必要な権限と責任を与え、改善を積み重ねていた

社長が、何度もセキュリティ対策強化を社内に指示していたが、さまざまな規模のセキュリティインシデントの発生頻度が高まり、営業や事業推進に影響が出てきた。そこで、社長は役員待遇のセキュリティ人材（CISO）を探しはじめ、数カ月後にようやく採用することに成功した。

会社から、一定の責任と権限を与えられた CISO は、まず、会社全体の包括的なセキュリティ戦略を立案するために必要な情報収集に着手し、社内全体の徹底的な観察を行った。この努力により得られた「サイバー攻撃の発生が考えられるセキュリティ上の弱点」をリストアップし、社内関係部門への説明と理解を獲得した上で、短期および中長期的なセキュリティ運用の強化に着手した。

このような努力により、委託先のシステムがマルウェア感染した際、A 社に対して正規な経路で仕掛けられたサイバー侵害を早期に検知および対処することに成功し、被害を発生させずに済んだ。ちなみに、同じ委託先に接続していた他の委託元は、一部で深刻な被害が発生した。

B 社. 社内の中核人材に対して、さまざまな形態の教育や演習に参加させていた

サイバーセキュリティ強化を推進している業界団体に参加している B 社は、業界団体からの推奨に基づいて、社内でサイバーセキュリティの中核となる人材を、外部の教育プログラム（1 年間）に差し出した。

その後、外部の教育プログラムを終了した人材を、サイバーセキュリティ対策部門（CSIRT）に配置し、関係部門の管理者やキーパーソンに対するセキュリティの教育・訓練、会社全体のセキュリティ運用を強化するための業務を与えた。また、当該人材のつながりを通じて、サイバーセキュリティの国内コミュニティや関連団体で開催されるサイバー演習に人材を継続的に参加させ、そのフィードバックとして社内の関係部門に対する情報共有や勉強会などを実施した。

このような取り組みにより、それぞれの部門で恒常的に発生していたセキュリティインシデントによる被害が縮小し、その発生頻度も低下した。

●「改善を要する対応」の背景と外的要因

C 社. 事業部門の役員や部長クラスが非協力的な姿勢あるいは逃げ腰で、IT 部門に責任を押し付ける

事業部門において発生した原因不明のセキュリティインシデントへの対処に追われていた IT 部門は、その事業部門の責任者（役員や部長クラス）から厳しい叱責を受けた。このインシデントは、導入していたセキュリティ検知システムにより検知されたものであり、業務への影響はなかった。

その IT 部門は、対処に加えて原因調査を行った結果、業務部門の社員によるセキュリティ違反が原因であることを突き止めたが、当該社員は、重要プロジェクトの推進を担当していたため、事業部門の責任者は、IT 部門に対してこれ以上の調査をしないことを命じた。

その後、事業部門がランサムウェア攻撃を受けて、大半のプロジェクトが停止してしまった。

D 社. 発生したインシデント対応にかかる労力の大半が「部門間調整」に費やされた

CSIRT が、外部拠点において発生したセキュリティインシデントへの対応に追われていた。

その拠点は遠方にあるため、CSIRT が現状を把握するための手段が限られているのに加え、窓口担当者が、拠点責任者の業務復旧（暗に調査を拒否）の強い意向に沿うような対応姿勢を貫いていた。

そのため、CSIRT を所管する部門と外部拠点を所管する事業部門の間での調整（都度の役員報告を含む）に、数週間の時間を費やし、十分な原因究明の調査を行うことができなかった。

E 社. セキュリティ対策の立案と計画を IT 部門だけに任せていた

昨今のサイバー脅威の高まりを受けて、役員会議でサイバーセキュリティ対策を強化することで一致した。

社内の事業部門は、一様にセキュリティ強化の必要性に懐疑的であったため、IT 部門のみで立案と計画を立てることになった。その後、外部のサイバーセキュリティ専門家の助言など利用しながら、数週間ほどでドラフトを作成した。

そのドラフトは、そのまま役員会議に付議され、事業部門でレビューおよび修正した上で確定することになった。しかし、およそ 1 ヶ月後に事業部門から戻ってきた「修正されたドラフト」は、ほとんどの強化項目が骨抜きとなり、ほぼ実効性のないものとなってしまった。（この強化策の事実上の失敗の責任を負わされた IT 部門から、離職者が出た。）

上記以外にも、特に「改善を要する対応」の背景と外的要因については相当数の事例があるが、保秘の都合上、次のような概要に留めて紹介する。

F 社. ファイアウォールや VPN のみに依存した境界防御を継続していた。（契約相手とのやり取りで利用せざるを得なかった外部ファイル共有サービス経由でマルウェア感染した）

G 社. 固有 ID や MAC アドレスのフィルタリングだけで、デバイスのネットワーク接続を許可していた。（退職予定社員が MAC アドレス変更ツールで、業務ネットワークに許可されていないデバイスを接続した。）

H 社. ペネトレーションテストや脆弱性診断を実施していない、あるいは部分的な実施であった。（事業部門の統廃合などを繰り返したために残存していたネットワーク設定の不備が、マルウェア感染の拡大につながった。）

I 社. 社員のセキュリティ教育が、Web ラーニングや文書配布などの形式的なものだった。（社内全体で軽微なセキュリティ違反が常態化していたため、複数の Emotet 感染が発生し、契約相手に被害を与えた）

現在、コロナ禍で大きな打撃を受けた経済を立て直す取り組みが始まっている。DX（デジタルトランスフォーメーション）というキーワードを使用せずとも、高付加価値や生産性の向上が期待できる「パブリック・クラウド」のビジネス利用や、さまざまなパートナー制度を提供することで戦略的な事業拡大を図る仕組み「パートナーシップエコサイクル」の進展などが目覚ましい。

このような変化の中で、サイバー脅威に適合したセキュリティを確保するためには、ネットワーク・データ・アプリケーションを保護するための取り組みや適切なソリューションの利用が必要となる。

これは、情報資産の保護を目的とした情報セキュリティと類似しているところもあるが、1 回限りの対策で十分な実効性を維持することはできないものであることに留意する必要がある。サイバーセキュテリィは「実践」であり、それを実現するために「強化されたセキュテリィ運用の維持」が前提となる。

本コラムで紹介した事例などを通じて、皆さんのサイバーリスクに対する「想像力」を少しでも高めていただけることを期待している。
（了）