第３節　セキュリティ管理の課題

日本大学危機管理学部　教授　美濃輪　正行

Ⅰ　組織におけるセキュリティ管理上の考慮点

前節通り年々巧妙化の一途を辿るサイバー攻撃の課題を考慮して、組織に求められる情報セキュリティ対策は次の点に考慮する必要がある。

①　サプライチェーン上関係する他組織を含めたセキュリティ管理の範囲の拡張
②　リスクが顕在化した場合の対応力
③　セキュリティに関する技術情報の取得

これらは、従来のイベント監視やセキュリティ教育等に追加して特に強調すべき点であり、技術動向や社会環境の変化を勘案したものである。

Ⅱ　セキュリティ管理の範囲の拡張

セキュリティ管理の範囲の拡張といっても自組織同様にセキュリティ管理を行うことは不可能である。具体的な活動例としては、自組織に関係する他組織とのセキュリティリスク及び責任範囲を明確にして問題発生時の対処法について合意しておくことが挙げられる。ここで想定されるサプライチェーンに関する対象としては､委託開発されたソフトウェア成果物、ベンダから購入する製品ソフトウェア、製品ハードウェア等も含まれる。マイクロソフト製品では定期的に更新版を提供している[1]が、常にサイバー攻撃の標的となっている。ネットワーク経由接続の監視カメラのパスワードが初期設定のままで盗み見や改竄される事案も発生している[2]。クラウドサービスでは、本年８月には米国のAWSで情報流出事件が発生している[3]。国内のクラウドサービスでもサイバー攻撃ではなかったもののシステムセンターの設備の制御機能が原因でサービス停止となる事案が発生している。これらは完成品として提供される製品またはサービスが原因となった事案である。事業運営に自組織外のサービスや製品を活用して事業効率化を図ることは、サプライチェーン攻撃に限らず外部の資源を活用する場合の組織が抱えるリスクの一部、更には経営戦略の一課題と捉えることもできよう。攻撃者は目的達成のため、あらゆる関連組織を標的にする可能性がある。中小企業等の組織も今後は攻撃の対象となる確率が高まるため、組織の規模にとらわれず各組織で堅実なセキュリティ対策を施すべきである。

Ⅲ　リスク顕在化時の対応力

サイバー攻撃によるリスクの顕在化は、如何なる対応をとったとしても確実に回避することは不可能である。それには二つの理由が挙げられる。

一つ目は、サイバー攻撃の被害を受けない確率が 0%でない限り、必ずその機会が訪れることにある。1 人の組織構成員がメールに添付されたマルウェアを開封する確率が 0.01%として同等の判断力を持つ構成員が 1000 人の組織を例に考える。完全確率を前提に計算すると被害を受けない確率は 90% に低下する。更に同程度の判断力を要するサイバー攻撃が 10 回発生した場合、この組織では同確率は 37% まで低下する。これは飽くまでも確率論上の計算であり、実際には構成員間の情報連携や組織内での注意喚起等が想定されるため、確率値は変動する。但し、メールに添付されたマルウェアを開封するリスクを考えただけでも、各構成員にセキュリティ教育の機会を与えることの重要性は理解できる。現実には人材の流動化や不正メール文章の巧妙さ等の条件を鑑みると、メールに添付されたマルウェアを開封しない判断力を習得することも困難になりつつある。

二つ目の理由は、訓練を積んだとしても極めて回避することが困難なサイバー攻撃が発生していることである。前節で取り上げたDNS環境改竄はその一例であるが、他にもフォームジャッキング[4]のような正規のサイトと識別が困難な手口が存在する。今後は日本国内でも本手口の攻撃が増加することも十分考えられる。

これらの理由により予防策の拡充に甘んじている状況は危険であり、被害に遭遇した際の具体的な体制や手続きについて事前に整えておく必要があることが分かる。重要な点は、次の 3 点である。

・組織における意思決定工程
・技術的な支援の拡充
・構成情報と問題発生時のサービスへの影響の把握

有事の際の対応の基本は意思決定であり、被害発生時から適切な判断が求められる。その影響度によって上層部の担当者を含めた判断が必要になることもあるが、軽微な被害であれば定型化された手続きでも対応可能である。影響の大小を判断する意味では、初期段階の判断が重要であり、初動の起点となる SoC(Security Operation Center)[5] の初期対応手順に大きく依存する。当該のサイバー攻撃が新種の手口または対応が非常に困難なものであれば、一層意思決定工程の重要度は増す。サイバー攻撃の発生から問題解決までの意思決定工程が事前に定められていることが望まれるところである。

サイバー攻撃に遭遇した場合の対応の問題の一つに技術力の不足がある。適切な技術情報が提供されなければ対応判断はできないし、問題解決に取り組むこともできない。更には一般的な組織では、サイバー攻撃の検知ですら困難である。サイバー攻撃の技術は日々進化しており、それらに精通している組織構成員が常に存在するとは限らない。そのような場合は自前の人員やサービスに拘らず、積極的に外部の資源を利用することが合理的で

ある。サイバー攻撃の検知は複数のイベントから特定の条件に絞り込む必要があることがあり、大量のトランザクションが発生している状況では、高い技術力と専門性が求められる。複数のサービスベンダーからセキュリティ監視・運用サービスは提供されており[6]、その中でもMSS(Managed Security Service)はセキュリティ監視のための複数の専用機器の統合的な監視を代行するものであり、一定精度のインシデント判定に有効である。

Ⅳ　技術情報の取得

技術情報は、攻撃に関する情報とユーザ側の情報に大別される。リスクが顕在化するには、脅威となる手口がユーザ側の脆弱性に合致して攻撃が実行されることが条件である。攻撃の手口の知識に加えて、自組織は攻撃に対してどの程度の耐性を持っているのか、についても知っておく必要がある。

攻撃に関する情報とは主に脅威つまり手口に関する情報であるが、手口を可能とする適用技術も含む。手口の理解だけでは十分でなく、手口に関連する技術要素を精通していないと攻撃の検知や防御、回復には効果がない。ユーザ側の情報とは、自社情報システムの脆弱性及びそれに関連する情報である。その組織の脆弱性は、情報システムのOSの修正モジュールのレベルやハードウェアのマイクロコードのレベル、アプリケーション・プログラムの構造、更にはシステムの管理や運用の品質やユーザの教育の程度等々から表出する状態である。情報システムの構成が複雑かつ膨大になってきたとしても、常に最新のシステム構成の状態を把握することがセキュリティ管理上、重要である。この情報が不足すると、攻撃の検知や状況の分析、回復措置に支障が発生する。更に被害箇所と状況に応じて組織に与える影響を事前に想定して、業務的な対策を検討しておくことが賢明である。

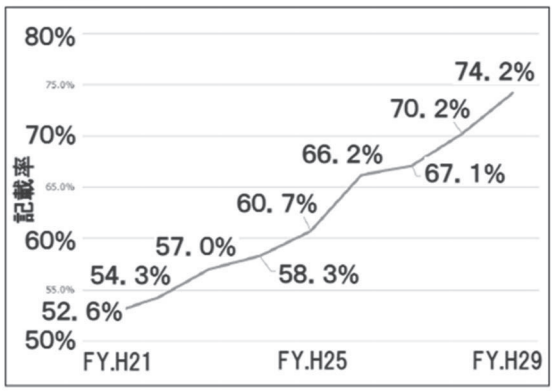
これらの情報は常に最新化を図るべきである。攻撃の観点からは手口の種類の数は常に増えており、常に新しい技術情報の獲得が望まれる。IPAが毎年公開しているその年々に社会的に影響が大きかった脅威のランキング[7]を見ても、サイバー攻撃の手口が流動的であることが分かる。ユーザ側が保有する技術情報も常に最新化して対応能力を備えておくことが必要である。組織の対応領域は変動し、情報システムはそれに応じて機能の追加や改変が発生する。これらの開発後には新たな脅威の可能性が想定されるため、技術情報を習得して対応策を講じておく必要がある。対応が不十分であった例としては、新たに決済サービスを開始することにより第三者のカード情報が悪用された事案[8]、河川監視システムで河川の状況を公開するホームページが改竄された事案[9]等がある。新しい領域の情報システムは認識が不十分な脆弱性が懸念される。人工知能の分野においては、画像認識機能を持つ機械学習システムに特定のノイズを与えると認識率が極端に低下することを利用したAdversarial Example[10]が指摘されており、新たな領域でもシステムの信頼性を大きく損なう脆弱性が危惧されるところである。

V　統計情報の考察

情報セキュリティを巡る状況を考察するに当たって、いくつかの企業を対象とした統計情報を取り上げる。マスコミ報道やセキュリティ・ベンダの脅威レポート等を参照するに、事件への興味からか、サイバー攻撃の手口ごとの発生件数やその推移等に偏重している状況が窺われる。情報セキュリティを管理サイクル全体で考えると、事前策つまり情報セキュリティ対策はインシデント発生後の事後策と同様に重要である。大規模な被害に及ぶサイバー犯罪は報道されるが、企業がどの程度の情報セキュリティへの意識を持っているか、どの程度情報セキュリティ対策に関心を払っているか、数値として把握することは困難である。

但し、「有価証券報告書」「コーポレートガバナンス報告書」へのサイバーセキュリティに関する記載の割合からその概況を伺い知ることができる。この記載は法律上の義務ではなく[11]、各企業の判断に委ねられている。NISC が日経 225 等の企業を対象に調査・分析した「有価証券報告書」へのサイバーセキュリティに関する記載率は図表 1[12] の通り年々増加している。平成 21 年から 28 年の会計年度で全体として約 50% の増加である。日経 225 の業種別に分析したものが図表 2 である。金融は 100%、次点で消費（水産、食品、小

図表 1　有価証券報告書にサイバーセキュリティに関する記載を行っている企業の割合の推移
（NISC「企業のサイバーセキュリティ対策に関する調査」より引用）



図表 2　サイバーセキュリティに関する分野別の記載状況
（NISC「企業のサイバーセキュリティ対策に関する調査」より引用）

業種分類	平成28年度		平成29年度	
	該当企業数	開示企業%	該当企業数	開示企業%
技術	44	77. 2%	47	82. 5%
金融	21	100. 0%	21	100. 0%
消費	27	90. 0%	29	90. 6%
素材	27	45. 0%	32	54. 2%
資本財・その他	22	59. 5%	21	58. 3%
運輸・公共	17	85. 0%	17	85. 0%
計	158	70. 2%	167	74. 2%

図表 3　組織長からみた業務遂行の評価
（データは情報処理推進機構「情報処理安全確保士の活動に関する実態調査調査書」から引用）

評価	課題が多くほとんど成果を上げていない		成果は上がっているが期待するレベルには達していない		期待されるレベルの成果を上げている		期待以上の成果を上げている		何ともいえない		回答しない	
経営判断 (n=24)	3件	13%	5件	21%	11件	46%	0件	0%	5件	21%	0件	0%
管理体制の構築 (n=57)	0件	0%	20件	35%	28件	49%	0件	0%	8件	14%	1件	2%
マネジメント (n=26)	2件	3%	20件	34%	29件	49%	0件	0%	6件	10%	2件	3%
セキュア設計 (n=59)	0件	0%	25件	33%	38件	51%	2件	3%	7件	9%	3件	4%
システム運用 (n=96)	2件	2%	23件	24%	51件	53%	6件	6%	10件	10%	4件	4%
機器運用保守 (n=65)	2件	3%	14件	22%	38件	58%	3件	5%	7件	11%	1件	2%
監視・情報収集 (n=62)	1件	2%	15件	24%	33件	53%	3件	5%	7件	11%	3件	5%
監査/脆弱性 (n=50)	3件	6%	12件	24%	30件	60%	3件	6%	2件	4%	0件	0%
インシデント (n=72)	4件	6%	16件	22%	39件	54%	3件	4%	7件	10%	3件	4%
調査研究 (n=50)	7件	14%	14件	28%	19件	38%	2件	4%	7件	14%	1件	2%
教育育成 (n=33)	6件	11%	22件	41%	19件	35%	3件	6%	4件	7%	0件	0%

売業、サービス）、運輸・公共が続く。54% の素材（化学、非鉄・金属、窯業、商社等）が最低である。サイバーセキュリティへの関心や監督省庁の影響度によって、業界レベルで記載率に差が出ている。

では、実際の現場で組織の管理者が自らのサイバーセキュリティに関する業務遂行をどのように評価しているか、情報処理推進機構が登録セキュリティスペシャリストが所属する組織の組織長に実施したアンケート結果[13]により確認できる（図表 3)。アンケートの質問は「サイバーセキュリティ対策関連業務は、期待されている成果を上げていますか」というものであるが、複数の項目への評価となっている。割合でみた時に最も評価が低いのは教育育成の項目である。組織構成員の判断力への信頼が懸念される。次点で低い項目は、「調査研究」、「マネジメント」、「管理体制の構築」と続く。調査研究については、技術情報の取得に不満があること、または技術要員の手薄さの原因が想定されるが、この調査はセキュリティスペシャリストが所属する組織で実施されているので、別の原因が考えられるであろう。相対して、評価がやや高いのが、システム運用、機器運用保守、監視情報収集等、定型的な要素が濃い業務に関する項目である。

国立研究開発法人情報通信研究機構の調査[14]によると、セキュリティ人材を育成している組織と人材の受け入れ先となる企業の間で重視する人材の特性が異なるとの結果が出ている。実践の場となる企業では、経営寄りでかつジェネラリストの人材を求める一方、育成する組織の側では経営寄りではなく現場寄りのジェネラリスト及びスペシャリストを指向する傾向が見られた。これは図 3 の「経営判断」と「管理体制の構築」の評価が低いことが関係していること、及びシステム運用、機器運用保守、監視情報収集等のスペシャリストは既に充足していることが推測される。

Ⅵ　経営上の課題

セキュリティ管理をいかに実現するかということは組織全体に影響を与える経営上の課題であるが、インターネット上にいくつかの経営者向けセキュリティ関連コンテンツが提

供されている。経産省が公開している「サイバーセキュリティ経営ガイドライン」[15] は経営上重要な 10 項目が「指示」という表現で記載されており、怠った場合のシナリオと現実に即した具体例が参考になる。日本ネットワークセキュリティ協会が提供する「経営者のための情報セキュリティ対策　―ISO31000 から組織状況の確定の事例―」[16] は、リスクマネジメントの国際規格「ISO31000」を基準として組織の情報セキュリティに対する必要性の認識の醸成を狙ったものである。ISO31000 はリスクマネジメントを対象とする規格であるため ISO2700X の規格と比較すると抽象度は上がる。一方、JCIC(Japan Cybersecurity Innovation Committee)[17] からは「取締役会で議論するためのサイバーリスクの数値化モデル」[18] が提供されている。このモデルを元に開発された「サイバーリスク指標モデル『想定損失額の目安」簡易シミュレーション』では、その組織が保有する個人情報の内容と件数、組織の売上、利益、想定事後対策費用を入力すると潜在的な損失額が試算される。自組織でサイバー犯罪の被害が発生した場合の概算レベルでの影響度を把握することに役立つ。これらの情報は飽くまでも全組織共通のものであるが、自組織固有の情報システム環境やビジネスへの依存度を勘案することによって、より精緻なセキュリティ対策が可能となる。

しかし、仔細に亘って情報システムやビジネスモデルへの影響度を経営層が把握することは困難であるが、組織内の技術者や担当者がそれらを推定して適正なセキュリティ施策を発案することが組織の理想である。組織にとって必要となるセキュリティ対応力を備えた体制やセキュリティ活動に順応した組織風土を作り上げることは経営層に課せられた大きな責務である。

Ⅶ　セキュリティ管理上の課題

サイバー攻撃の被害は脅威と脆弱性の関係性から生まれ、ICT が進化すればそれによってビジネスモデルも変化し、その脆弱性を突く脅威が登場する。当面の間、ICT は停滞することなく進化が続く。また大半のビジネスモデルは時流に合わせて変化しないと衰退する [19]。技術の進化以外にも人口構成の変動 [20] や法制度の変化 [21] も新たなリスクを生む要因となり得る。

人材の流動化が激しくなれば、新たに組織に加入した構成員にセキュリティ教育を実施する機会も増えよう。この観点からは、セキュリティ管理に関する目的意識を如何に共有するかが問題となる。これは下位組織をどのように構成するか、具体的には下位組織の構成人数 [22] 等も影響する。巨大な組織においては、下位組織の人数が少ないほど意思疎通は確実になり目標意識の共有が可能となるが、管理職の人数を考えると人件費の増加にもなりかねない。

定型業務としてのセキュリティ対策の拡充のためには人材の獲得ではなく、外部資源の活用の手段をとることも可能である。但し、コスト・バランスを考慮して、かつ責任範囲

を明確にしてサービスを受けることが前提となる。一つの問題は、新たな技術革新や法制度に対応する要件が発生した場合である。RPA(Robotic Process Automation)、AI(Artificial intelligence) をビジネスに適用する動きは顕著であるし、GAFA を規制する法案によって国内のサービス事業者が影響を受けないとも限らない。ビジネスコンサルタントの助言を受け入れる選択もあるが、本質的には成果物が自組織にとって適正なものか判断する能力も必要となる。

現代のセキュリティ管理に模範解答は存在しない。歴史学者のユヴァル・ノア・ハラリ (Yuval Noah Harari) は「ホモデウス (Homo Deus)」で次のように語っている。

「現在のシステムを理解している人はもう一人もいないので、誰もそれを止められないのだ。」[23]

私たちに求められているものは、画一的な発想に囚われることなく、自らの問題を探索して対策を講じ、あらゆる問題に真摯に取り組む姿勢である。

◆さらに学ぶための参考文献

- 矢田篤史・粕谷真紀子・西村忠興（2012 年）『実例 情報セキュリティマネジメントシステムの本質化・効率化』（日本規格協会）
- 横浜信一（2018 年）『経営とサイバーセキュリティ　デジタルレジリエンシー』（日経 BP 社）

---

[1] Microsoft Security Response Center「セキュリティ更新プログラム リリース スケジュール (2019 年)」https://msrc-blog.microsoft.com/2018/10/24/securityupdatereleaseschedule2019/ (2019 年 10 月 27 日アクセス)

[2]「監視カメラに不正アクセス　キヤノン製、60 台以上被害　セキュリティに弱点」産経新聞 2018/5/7

[3] Department of Justice U.S. Attorney’s Office Western District of Washington (2019/07/29) “*Seattle Tech Worker Arrested for Data Theft Involving Large Financial Services Company*”

[4] Symantec “*Internet Security Thread Report Volume 24|February 2019*” P.14 “*FORMJACKING*”

[5] JPNIC「SoC とは」 https://www.nic.ad.jp/ja/basics/terms/soc.html (2019 年 10 月 27 日アクセス)

[6] IPA(2019 年 10 月 17 日)「セキュリティ監視・運用サービス」https://www.ipa.go.jp/files/000067320.pdf (2019 年 10 月 27 日アクセス)

[7] IPA(2019/08/07) “情報セキュリティ 10 大脅威 2019” https://www.ipa.go.jp/security/vuln/10threats2019.html (2019 年 10 月 25 日アクセス)

[8] PayPay (2018/12/14) “身に覚えのないクレジットカードの請求がきたら” https://paypay.ne.jp/notice/20181214/01/ (2019 年 10 月 25 日アクセス)

[9] Scan Net Security(2018/05/01)「河川監視カメラへ不正アクセス、『I'm hacked.bye2』のメッ

セージ残す（上尾市）」 https://scan.netsecurity.ne.jp/article/2018/05/01/40886.html (2019 年 10 月 25 日アクセス)

[10] 林瑛晟，服部隆志，萩野達也 (2019-02-28)「複数モデルの出力を用いた Adversarial Examples」情報処理学会第 81 回全国大会

[11] 大杉 謙一（2017）「会社法・金商法上のリスク情報の開示の現状と課題」 総務省　サイバーセキュリティタスクフォース情報開示分科会　P.1「1. 会社法」

[12] NISC(2019/05/17)「企業のサイバーセキュリティ対策に関する調査（概要）」 P.3「1. サイバーセキュリティ対策に係る情報発信内容の調査」より引用

[13] 情報処理推進機構 (2019/07)「情報処理安全確保支援士の活動に関する実態調査 調査書」P.52「2.6.2 組織長から見た業務遂行の評価」

[14] 衛藤将史　神薗雅紀「セキュリティ人材育成の現状と実践 : 1. セキュリティ人材育成の現状と今後の展望 - 持続的なセキュリティ人材の供給に向けて -」「情報処理」 Vol.60 No.10　P.973「セキュリティ人材の需要と供給の対応状況」

[15] 情報処理推進機構 (2017/11/16)「サイバーセキュリティ経営ガイドライン Ver 2.0」https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf（2019 年 10 月 20 日アクセス)

[16] 日本ネットワークセキュリティ協会 (2018/06/11)「経営者のための情報セキュリティ対策―ISO31000 から組織状況の確定の事例―」 https://www.jnsa.org/result/2018/west_tebiki/ (2019 年 10 月 25 日アクセス)

[17] JCIC(Japan Cybersecurity Innovation Committee) は一般社団法人　非営利・独立の民間シンクタンク　サイバーセキュリティの強化に貢献することを目的とする組織。

[18] JCIC(2018/09/19)「取締役会で議論するためのサイバーリスクの数値化モデル」https://www.j-cic.com/pdf/report/QuantifyingCyberRiskSurvey-20180919(JP).pdf ；サイバーリスク指標モデル「想定損失額の目安」簡易シミュレーション（Excel）https://www.j-cic.com/pdf/report/CyberRiskEstimationModel-20180919.xls　(2019 年 10 月 25 日アクセス)

[19] 一般財団法人技術同友会 (2017/05)「新たな事業環境変化に対応する日本の新産業の創造に関する提言」P.3「Ⅱ . 本提言における問題認識・背景」

[20] e-Stat(2017/06/28)「年齢 (5 歳階級及び 3 区分)，男女別人口（各年 10 月 1 日現在）－総人口，日本人人口（平成 12 年～ 27 年)」 https://www.e-stat.go.jp/stat-search/files?page=1&layout=datalist&toukei=00200524&tstat=000000090001&cycle=0&tclass1=000000090004&tclass2=000001051180 (2019 年 10 月 25 日アクセス)

[21] 大和総研 (2019/01/04)「2019 年以降の制度改正予定（企業法務編）」

[22] OrgChart(2015/12/02) "*Importance Of Span of Control & Organizational Structure*" https://www.orgchartpro.com/span-of-control-and-organizational-structure/ (2019 年 10 月 29 日アクセス)

[23] Yuval Noah Harari(2015)「ホモデウス（上）」河出書房新社　P.70「第 1 章人類が新たに取り組むべきこと」