2021 年 9 月 9 日

コンサルティングレポート

# 中堅・中小企業[1]の情報セキュリティマネジメントの現状と今後の展望

業務ITコンサルティング部　アソシエイト　大道　裕江

## 1. はじめに

企業には多くの情報資産がさまざまな形（紙、記憶媒体、サーバー、クラウドサービスなど）で存在している。近年、情報資産の価値は高まってきており、それに伴い、情報セキュリティ対策の重要性はますます増している。情報セキュリティ対策が不十分なことが原因でセキュリティインシデント（事故）を起こした企業に対しては、年々厳しい目が社会から向けられるようになってきており、企業にとって情報セキュリティリスクに対するマネジメントは重要な経営課題のひとつと言える。

情報セキュリティに関するインシデントの代表としては、情報漏洩が挙げられる。企業の個人情報漏洩をはじめとするセキュリティインシデントは後を絶たず、連日のように公表され、一部は大きく取り上げられてニュースを賑わせている。情報漏洩と聞くと、企業がサイバー攻撃を受け個人情報や機密情報を盗まれたといったイメージを持つことが多いかもしれないが、原因として最も多いのは内部要因（ヒューマンエラー）によるものである。図表 1 の 2019 年 6 月に「特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）」が発表した「情報セキュリティインシデントに関する調査結果」によると、情報漏洩の原因は、第 1 位が「紛失・置き忘れ」（USB メモリや印刷した資料の紛失など）、第 2 位が「誤操作」（メールの誤送信など）となっており、このように組織内の人為的なミス（ヒューマンエラー）が原因の半数を占めている。続く第 3 位は「不正アクセス」であり、外部からの攻撃により情報資産が奪取されていることを示している。以上のことから、情報資産を適切に管理するためには、外部からの攻撃に対応するだけでなく、組織内のヒューマンエラーへの対応の両面からリスクマネジメントが必要であることが言える。

近年、企業を標的とするサイバー攻撃は増加の一途をたどっており、手法も高度化・巧妙化してきている。独立行政法人 情報処理推進機構（IPA）が公表した「情報セキュリティ 10 大脅威 2021」の組織に対する脅威（図表 2）では、1 位に「ランサムウェア [2]による被害」、2 位に「標的型攻撃 [3]による機密情報の窃取」がランクインし、企業の規模を問わず猛威を振るっている。「サプライチェーンの弱点を悪用した攻撃 」は 2019 年から 3 年連続で 4 位にランクインしており、サプライチェーンの中で情報セキュリティ対策が手薄な中堅・中小企業が攻撃され、大企業等に被害が波及する事案が顕在化してきていることを示している。

中小企業基本法の定義による中小企業は日本の企業数の 99%以上を占めており、サプライチェーンを形成しなが

---

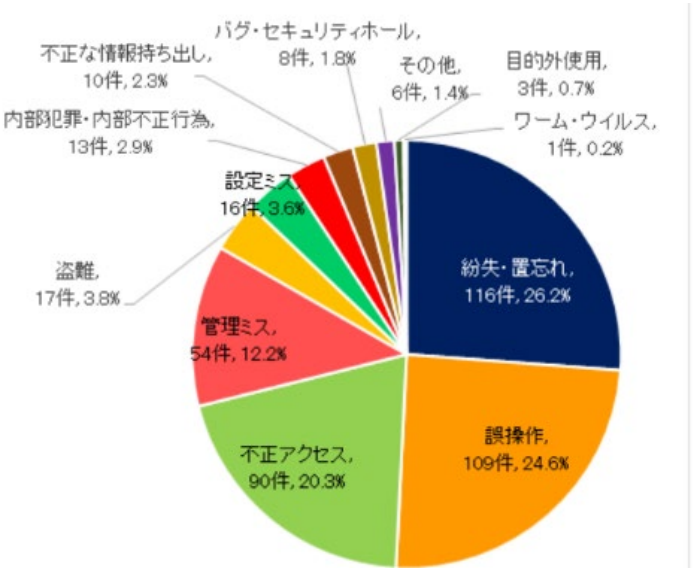
[1] 国内において、中小企業基本法における中小企業とは業種別に資本金と従業員の数によって定義されているが、本稿においては資本金 10 億以下の企業を想定し「中堅・中小企業」に表記を統一した。

[2] コンピュータを強制的にロックし、データを暗号化した後に、元の状態に戻すことを条件として身代金を要求する不正プログラムの一種。

[3] 特定の個人や組織を狙ったサイバー攻撃のこと。業務関連のメールを装ったウイルスや不正サイトのリンクを含んだメール（標的型攻撃メール）を、組織の担当者に送付するケースが多い。

ら日本の産業を支えているが、サイバー攻撃対象の例外では決してなく、むしろ標的となっているのである。この状態を看過することはサプライチェーン全体として見た場合に大きなセキュリティリスクを抱えている状態と言える。サプライチェーン攻撃への対策は個別企業レベルで実施しても不十分であり、構成する企業群が連携して取り組む必要がある。そのため、近年、サプライチェーンというコンテキストの中での中堅・中小企業の情報セキュリティマネジメントは注目されつつある。本稿では中堅・中小企業における情報セキュリティマネジメントに着目して、現状と今後の展望を述べる。

【図表 1】 漏洩原因:2018 年単年データ(件数)




(出典)JNSA「情報セキュリティインシデントに関する調査結果」(2019 年 6 月発表)
https://www.jnsa.org/result/incident/data/2018incident_survey_sokuhou.pdf

【図表 2】 情報セキュリティ 10 大脅威 2021

| 順位 | 内容 | 昨年順位 |
|---|---|---|
| 1位 | ランサムウェアによる被害 | 5位 |
| 2位 | 標的型攻撃による機密情報の窃取 | 1位 |
| 3位 | テレワーク等のニューノーマルな働き方を狙った攻撃 | NEW |
| 4位 | サプライチェーンの弱点を悪用した攻撃 | 4位 |
| 5位 | ビジネスメール詐欺による金銭被害 | 3位 |
| 6位 | 内部不正による情報漏えい | 2位 |
| 7位 | 予期せぬIT基盤の障害に伴う業務停止 | 6位 |
| 8位 | インターネット上のサービスへの不正ログイン | 16位 |
| 9位 | 不注意による情報漏えい等の被害 | 7位 |
| 10位 | 脆弱性対策情報の公開に伴う悪用増加 | 14位 |

(出典)IPA「情報セキュリティ 10 大脅威 2021」より当社作成
https://www.ipa.go.jp/security/vuln/10threats2021.html

## 2. 中堅・中小企業にとって他人事ではない情報セキュリティ対策

中堅・中小企業の中には、自社で個人情報を扱っておらず、狙われるような価値ある情報も持っていないと考えている企業も多く存在する。しかし情報資産とは、企業活動によって収集した「ヒト・モノ・カネ」に関する情報のことであり、消失・漏洩が発生した場合、事業に多大な影響を与え社会的信用を失う情報全てを指す。たとえば、「顧客の個人情報」「従業員の人事情報」「会社の財務情報」「製品技術情報」「取引先の情報」等が情報資産に該当する。よって、情報資産のない企業は存在しない。普段耳にする企業のセキュリティインシデントのニュースは大企業のものが大半であるが、中堅・中小企業も実際は情報窃取・流出を目的とした外部からの攻撃の脅威にさらされている。

### (1) サイバー攻撃の標的となっている中堅・中小企業

#### ① 中堅・中小企業の 5 社に 1 社がサイバー攻撃の被害に遭っている

2019 年 1 月に一般社団法人日本損害保険協会が公表した「中小企業の経営者のサイバーリスク意識調査 2019[4]」において、825 人の中堅・中小企業経営者のうち、約 2 割にあたる 155 人が何らかのサイバー攻撃の被害に遭ったことがあると回答している。

#### ② 中堅・中小企業は業種や規模を問わずサイバー攻撃の脅威にさらされている

2019 年度、2020 年度に、中堅・中小企業のサイバーセキュリティ対策を支援する仕組みの構築を目的として、独立行政法人 情報処理推進機構(IPA)が実施した実証事業 [5](サイバーセキュリティお助け隊。2019 年度は全国 8 地域で計 1,064 社、2020 年度は全国 13 地域・2 産業分野で計 1,117 社の中堅・中小企業が参加。)では、内外に向けた不正通信等を数多く検知した。導入したほとんどの中堅・中小企業で何らかのサイバー攻撃またはその予兆が検知されており、被害の発生にまでは至っていなくとも、常にインシデントは起こり得る状態にあると言える。中堅・中小企業においても、業種や規模を問わずサイバー攻撃の脅威にさらされており、ウイルス対策ソフト等の既存対策だけでは防ぎきれていない実態が明らかとなった。

### (2) 中堅・中小企業における情報セキュリティ対策の現状

中堅・中小企業は実際にサイバー攻撃の標的になっている一方で、大企業と比較して十分な対策が取られているとは言えないのが現状である。原因としては中堅・中小企業においては、自社が攻撃対象となり得ること、インシデントが発生した場合にビジネスに甚大な影響を与えることへの実感が乏しいことが指摘されている。

#### ① 中堅・中小企業は情報セキュリティ対策が手薄となっている

前述の「中小企業の経営者のサイバーリスク意識調査 2019」では、中堅・中小企業の 4 社に 1 社は、今もなおサイバー攻撃への対策をしておらず、情報セキュリティ対策のうち、最も優先度が高い対策と言える「OS やソフトウェアの最新化、ウイルス対策ソフトの導入実施率」でさえ 52.4%にとどまっていることが明ら

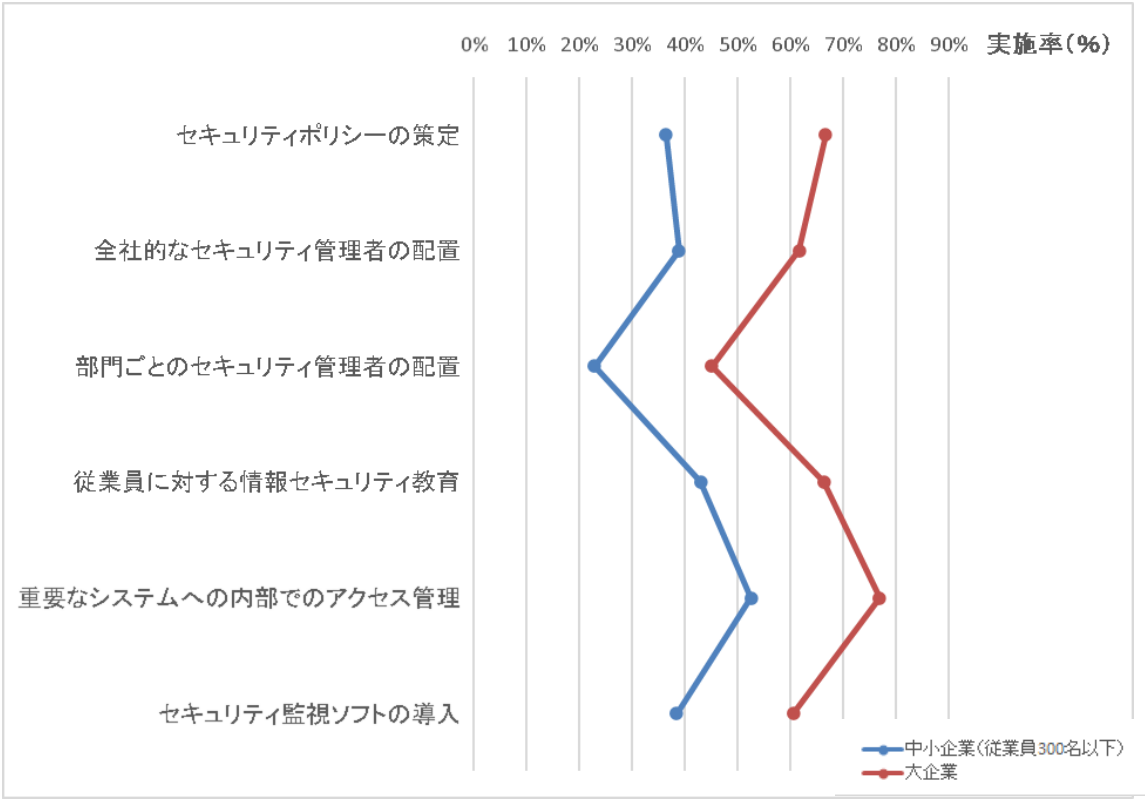
---

[4] 一般社団法人日本損害保険協会「中小企業の経営者のサイバーリスク意識調査 2019」(2019 年 1 月発表)
https://www.sonpo.or.jp/news/release/2019/2001_02.html

[5] IPA サイバーセキュリティお助け隊
(2019 年度)https://www.ipa.go.jp/security/fy2019/reports/sme/otasuketai_houkoku.html
(2020 年度)https://www.ipa.go.jp/security/fy2020/reports/sme/otasuketai_houkoku.html

かとなった。特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）が経済産業省 「平成 23 年度情報処理実態調査」データより作成した、情報セキュリティ対策実施率を比較したグラフ（図表 3）からも、大企業と比較して中堅・中小企業（従業員 300 人以下）の情報セキュリティ対策（後述する人的対策）の実施率は軒並み低いことは明らかである。この傾向は 2015 年、2016 年に情報処理推進機構（IPA）が実施した「中小企業における 情報セキュリティ対策の実態調査 [6]」においても変わりはなかった。

**【図表 3】 大企業と中堅・中小企業の対策実施率の差**




（出典）経済産業省 「平成 26 年度情報処理実態調査」データより当社作成
https://www.meti.go.jp/statistics/zyo/zyouhou/result-2/h26jyojitsu.html

### ② 中堅・中小企業はサイバー攻撃に対する危機意識が希薄

前述の「中小企業の経営者のサイバーリスク意識調査 2019」では、自社がサイバー攻撃の対象となることを認識している中堅・中小企業は 1 割未満にすぎず、中堅・中小企業の経営者の約半数がサイバー攻撃をイメージできていないことが明らかとなった。また、優先度の高い経営課題を選択する設問では、サイバー攻撃への対策は、12 項目中最下位となっている。中堅・中小企業ではそもそも予算が潤沢でなく、情報セキュリティ対策への投資は直接利益を生むわけではないため投資の対象となりにくいことは想像に難くない。情報セキュリティ対策の必要性への認識が低く、結果として対策が後回しにされていると考えられる。

---

6 IPA 中小企業における 情報セキュリティ対策の実態調査
（2015 年度）https://www.ipa.go.jp/files/000051252.pdf
（2016 年度）https://www.ipa.go.jp/files/000058502.pdf

サイバー攻撃を含むセキュリティリスクに対して危機意識が醸成されない大きな要因としては、情報セキュリティ分野での技術や知識がある人材の不足や、人員に余裕がなくセキュリティ担当者が定められていないことが考えられる。その結果、情報セキュリティに関する情報を収集できておらず、また、自社が受けている外部からのサイバー攻撃の実態についても把握できていないことが推測される。

### (3) 中堅・中小企業においても、情報セキュリティ対策は喫緊の経営課題である

情報資産管理が不適切なことによりセキュリティインシデントが発生した場合、下記に示すようにビジネスに甚大な影響を与える。セキュリティインシデントとは、情報資産が損なわれてしまった状態を指し、インシデントの例としては情報の消失・破壊、不正アクセス、情報漏洩、業務停止などが挙げられる。

- 業務継続が困難となり、業務を一時停止せざるを得なくなり、復旧コストがかかる
- 社会的信用の低下を招き、将来的な事業の機会も失う
- 影響が取引先に及んだ場合は、損害賠償請求や取引停止等の厳しい措置がとられる可能性がある

2019 年 5 月に大阪商工会議所が公表した「サプライチェーンにおける取引先のサイバーセキュリティ対策等に関する調査 7」では、「取引先がサイバー攻撃を受け、それが自社に及んだ経験」がある企業は 4 社に 1 社に上り、取引先がサイバー攻撃被害を受け、その被害が自社に及んだ場合に採り得る対処(複数回答可)として、47%が損害賠償請求、29%が取引停止という厳しい措置を取り得ると回答した。

## 3. 中堅・中小企業が実施すべき情報セキュリティ対策

### (1) 情報セキュリティ対策の概要

#### ① 情報セキュリティ対策の 3 分類

情報セキュリティ対策は一般的に「技術的対策」、「物理的対策」、「人的対策」の 3 つに分類される。着眼点が異なる他の分類法もあるが、いずれの分類にせよ、組織がとらなければならない対策であることには変わりはない。

- 技術的対策の例:OS やソフトウェアの最新化、ウイルス対策ソフトの導入
- 物理的対策の例:入退室管理
- 人的対策の例:セキュリティポリシーの策定、教育、PDCA サイクル

#### ② 情報セキュリティ対策の 3 つの機能

情報セキュリティ対策の 3 つの機能は以下の通りである。

- セキュリティインシデントの発生を抑止・防止すること
- セキュリティインシデントの発生や予兆を検知すること
- セキュリティインシデントが発生した場合に早期復旧し、被害を最小化すること

情報セキュリティ対策は、実施手段の 3 分類(技術・物理・人)と、目的別の 3 機能(抑止・検知・被害の最

7 大阪商工会議所「サプライチェーンにおける取引先のサイバーセキュリティ対策等に関する調査」(2019 年 5 月公表)
https://www.osaka.cci.or.jp/Chousa_Kenkyuu_Iken/press/190510sc.pdf

小化）の組み合わせでまずは大きく分類できる。技術的対策については、想定する脅威やリスクの種類によって、対応策がさらに細分化される。

### ③ 目指すべき情報セキュリティ対策

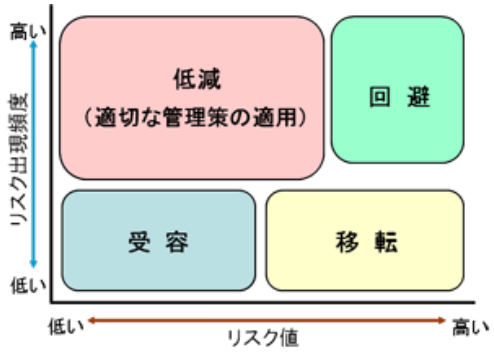
情報セキュリティ対策のポイントとして、「①情報資産の使い手（＝人）のリテラシー向上が必要」、「②組織的で継続的な取り組みが重要」、「③リスクアセスメント（図表 4）を行い、対応方針を決定する」の 3 点をここでは強調したい。

まず 1 点目の「情報資産の使い手のリテラシー向上が必要」であるが、情報資産を取り扱うのも、「情報セキュリティ対策を行う」という意思決定を行うのも、自社の情報資産を守る仕組みを作り運用するのも人である。情報資産の重要性やリスクを認識することが情報セキュリティ取り組みのきっかけや原動力となることから、情報資産の使い手のリテラシー向上は必須と言える。情報資産の使い手と意思決定者のリテラシーが不十分な場合、情報セキュリティ対策に資源（人・予算）が割り当てられず、情報資産や情報システム、機器の管理ルールが策定されない。その結果、情報漏洩につながるヒューマンエラーを誘発し、標的型攻撃をはじめとしたサイバー攻撃を成功させてしまう。例えば、USB を紛失したり、推測しやすいパスワードを使い回しで設定したり、不審なメールのリンクや添付ファイルを開いてしまっては、他に情報セキュリティ対策を行っていたとしても全体として見るとそれが抜け穴となる。情報セキュリティ対策というと、インシデントの発生を予防する技術的対策ばかりに目が行きがちであるが、情報資産の使い手のリテラシーを高め、特に人的対策、そして物理的対策にも目を向けて複数の対策を組み合わせながら、バランスの取れた対策を実施すべきである。

次に 2 点目の「組織的で継続的な取り組み」であるが、情報セキュリティ対策は、ある一時点で万全を期したとしても、最新化し続けなければ陳腐化する。時間の経過とともに脆弱性が発見され、新たな攻撃手法が生まれ、当初の設定と実態との間に乖離が発生するからである。定期的に実施すべき情報セキュリティ対策の具体例としては、OS・ソフトウェアとウイルス対策ソフトのウイルス定義ファイルの最新化、教育、各種アカウントや管理台帳の最新化などが挙げられる。これらの情報セキュリティ対策を確実に定期的に実施するために、ルール策定とルールを守るための仕組みの整備、PDCA サイクルの確立といった組織としての取り組みが必要である。

最後に 3 点目の「リスクアセスメントを行い、対応方針を決定する」であるが、全てのリスクに対してインシデントの発生を抑止する対策を行った場合、費用が莫大となり十分な費用対効果を得ることは難しい。そのためインシデントの予防ばかりに注力するのではなく、セキュリティインシデントの発生は完全になくすことはできないという前提のもとで、リスクの発生頻度と影響度合いによって対応方針を「低減」「移転」「受容」「回避」に分類するリスクアセスメントを行う。さらに「低減」の中でも、対策の優先順位をつけ、インシデントが発生した際の影響を小さくする、事後対応を適切に行う（そのための手順を事前に定めておく）といった管理策を組み合わせながら、大きな穴のない管理体制の構築を目指すことが重要である。

【図表 4】リスクへの対応




経営リスク管理の一環として、リスクの発生頻度と影響度合いによって対応方針を決定する。

・リスクの回避（頻度大、影響大）：リスクが発生する可能性をなくす
・リスクの低減（頻度大、影響小）：リスクの発生頻度を低減させる
・リスクの移転（頻度小、影響大）：保険など
・リスクの受容（頻度小、影響小）：対応を行わない

（出典）JNSA「リスクアセスメントとリスク対応」https://www.jnsa.org/ikusei/01/01-01.html

### （2）　何から着手すべきか分からない場合

#### ①　自社による状況把握

自社の現状の情報セキュリティの状態や実際に何から手を付けたらいいのかが分からない場合、独立行政法人情報処理推進機構（IPA）が提供する「SECURITY ACTION」[8]をまず参照することを推奨する。「SECURITY ACTION」とは中堅・中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度で、最優先で実施すべき情報セキュリティ対策を示した「情報セキュリティ 5 か条」と、自社の状況把握に活用できる「5 分でできる！情報セキュリティ自社診断」など非常に有益なコンテンツを利用することができる。

#### ②　社外リソースの活用

自社内の人材不足により情報セキュリティ診断の実施や方針策定が難しい場合、外部のサービスを活用する方法がある。一部の商工会議所などでも、サービス提供や支援を行っている。また、弊社でも情報セキュリティ診断サポートを提供しているため、相談先の候補に含めていただけると幸いである。

外部の診断サービスや伴走支援サービスを活用することで、情報セキュリティリスクに対する危機意識を高め、自社の情報セキュリティ対策の弱みととるべき対策を把握することができる。自社の情報セキュリティレベル向上に向けて一歩ずつ継続的に取り組みながら、取引先や顧客からの信頼を高めてほしい。



[8] IPA　SECURITY ACTION 自己宣言者サイト（https://www.ipa.go.jp/security/security-action/index.html）