2022 年 3 月

社内のセキュリティリソースは「0.5%以上」を確保せよ

～DX with Security を実現するためのサイバーリスク数値化モデル～

【要旨】

- 国内上場企業の約 9 割が DX（Digital Transformation）に取り組んでいるが 、DX の効果を持続的に得るためには、サイバーセキュリティを同時に推進しなければならない。**セキュリティ対策を怠ると、システム停止や情報流出のリスクが顕在化するだけではなく、多額の金銭的損失が発生する可能性がある**からだ。

- JCIC が不正アクセス等の適時開示を行った企業の株価を調査したところ、**50 日後の株価が平均 6.3%下落することがわかった。**また、セキュリティ対策の未整備は、損害賠償や善管注意義務違反に問われる恐れもある。もはや、DX 推進のためのサイバーセキュリティ「DX with Security」は、IT・セキュリティ部門だけの問題ではなく、**取締役や経営者等の役員を巻き込み、全社一丸で取り組むべき経営課題**となったといえる。

- DX を推進し、企業の生産性向上や効率化を実現するため、また金銭的損失を回避するためには「DX with Security 戦略」が不可欠である。この DX with Security 戦略の策定や実現のために、JCIC では以下のアプローチを推奨する。

DX with Security 先進企業のための戦略策定の推奨アプローチ

- サイバーリスク数値化モデルを用いリスクを可視化せよ
- DX with Security 戦略を策定せよ
  - ○ ストーリーとして戦略を語るためのフレームワークを活用すべき
  - ○ セキュリティ投資額は、連結売上高の**「0.5%以上」**を投資すべき
  - ○ セキュリティ人材は、全従業員数の**「0.5%以上」**を確保すべき
- セキュリティ KPI を設定し、定期的にモニタリングせよ

- DX 推進部門は、ビジネス変革のためのトライ＆エラーを日々繰り返し、少しでも早く成果を出そうとする。この段階で、セキュリティ部門が強い統制を効かせることは DX の足かせになるため望ましくない。セキュリティ責任者は、セキュアな PoC 環境の整備やガイドラインを策定することで、DX をアシストしていくという考え方になるべきであり、**商用サービスを具体的に検討する段階で、セキュリティ責任者が積極的に関与していくことが望ましい。**

1. はじめに

JCIC は、サイバーセキュリティのシンクタンクとして、「経営とサイバーセキュリティ」の研究を行ってきた。本レポートは、JCIC が 2018 年に公開した「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」を全面改訂したものである。コロナ禍においてデジタル化やリモートワークが浸透したこと、DX に取り組む企業が激増したことを受け、DX におけるセキュリティの位置付けを再考し、今回、DX with Security 推進のアプローチを整理した。

本レポートでは、DX を**「デジタル技術を活用し、画期的な新規ビジネスを展開することや、業務プロセスを抜本的に変革すること」**という意味で用いている。人手や紙で行っていたアナログ業務を単にデジタル化するという意味ではない。新規ビジネスや業務プロセス変革には、財務リスクや法的リスク等、様々なリスクが潜在している。その中でも、**サイバーリスクは、全ての DX で共通して考慮すべき事項であり、リスクが顕在化した場合のビジネス影響が大きく、脅威が日々変化していることから、喫緊の課題であると言えよう。**

本レポートの対象読者は、主にセキュリティ責任者（CISO、部門長など）を想定しているが、取締役/監査役/経営層/経営企画/総務/リスク管理/人事/財務/情報システム・DX 推進/広報・IR・サスティナビリティ/購買・調達などのマネジメント層も読んでいただきたい内容になっている。

また、本レポートのメインの対象企業は、IT 企業並みに人材と予算を DX に投資し、ビジネスモデルや業務プロセスを変革する「DX with Security 先進企業」である。先進企業とは、利便性とセキュリティ管理を全社的に高い次元で実現しようとする企業（利便性重視・モニタリング型 [1]）であるとも言える。また、既存のビジネスや業務を維持しつつ、DX を部分的に試行する「DX with Security フォロワー企業」も参考になる内容になっている。

ぜひ、このレポートを DX with Security 推進のヒントとして活用していただきたい。

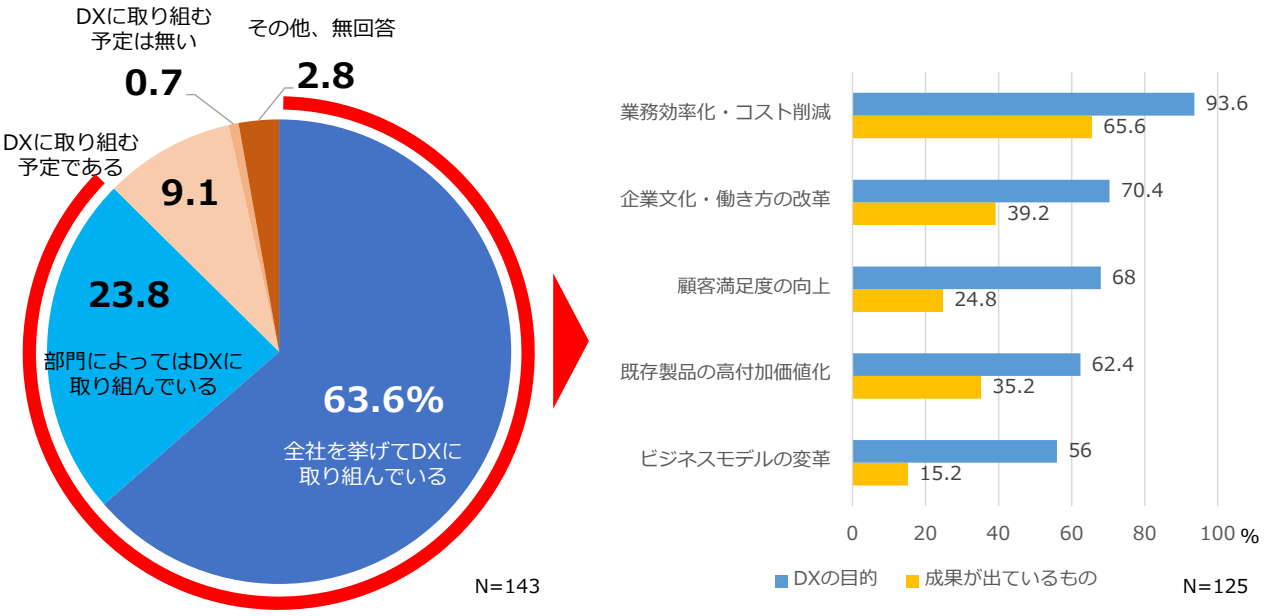
[1] JCIC「2025 年に向けた利便性とセキュリティのリバランス」では、①利便性重視・モニタリング型の他、②裁量主義・現場責任型、③場当たり型／フレキシブル型、④セキュリティ原理主義型の 4 つのタイプに企業が分類できるとした。https://www.j-cic.com/pdf/report/Rebalancing.pdf

2. DX with Security の重要性

公益財団法人 日本生産性本部イノベーション会議の調査によると[2]、上場企業の経営者の約 9 割が DX に取り組んでいると回答している。9 割の内訳は、全社的に取り組んでいる企業が 64%、部門で取り組んでいる企業が 24%であった。

また、DX の目的のトップは、「業務効率化・コスト削減」であり、2/3 の企業は既に効果が出ていると回答している。目的の 2 番目以降は、「企業文化・働き方の改革」、「顧客満足度の向上」、「既存製品の高付加価値化」と続く。

コロナ禍において、リモートワークでも十分にビジネスがまわり、リモートの方が業務効率の良い場面が多いことが社会的に証明された。また、リアル社会からデジタル社会への変化は、「モノ消費」から「コト消費」への価値観の変化を促進した。アフターコロナ時代に世の中が大きく変わる中で、企業が DX に取り組むことは、企業価値を維持向上するために不可避であると言えよう。



【設問】御社ではDXを実施していますか（単一選択）

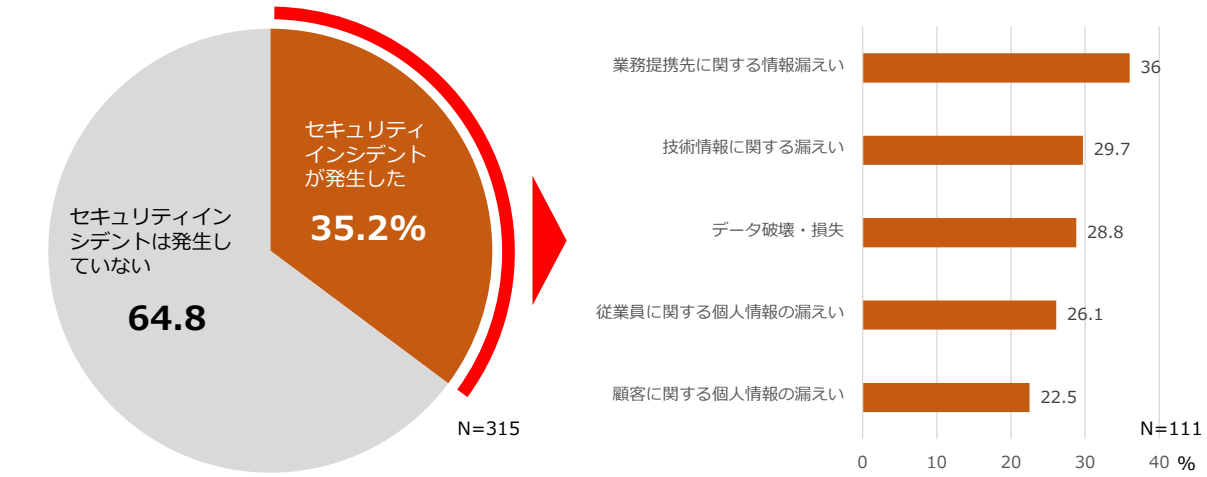
【設問】御社におけるDXの目的は何ですか。その目的に対して成果が出ていますか（複数選択）

図表 1 DX 実施状況と DX の目的

[2] 公益財団法人 日本生産性本部「新政権への期待と DX に関する緊急アンケート」（2022 年 12 月）, https://www.jpc-net.jp/research/detail/005615.html

このように上場企業のほとんどが DX に取り組んでいる状況ではあるが、DX の持続的な効果を得るためにサイバーセキュリティを同時に推進しなければならない。セキュリティ対策を怠ると、システム停止や情報流出のリスクが顕在化するだけではなく、数百億円もの金銭的損失が発生する可能性があるからだ。

トレンドマイクロの調査[3]によると、DX を推進する担当者のうち約 35%がセキュリティインシデントを経験している。インシデントの被害内容は「情報漏えい」に関するものが比較的多く、DX を推進する上で、新たなシステムを導入した際にデータの保護が十分に徹底できていないとのことだ。

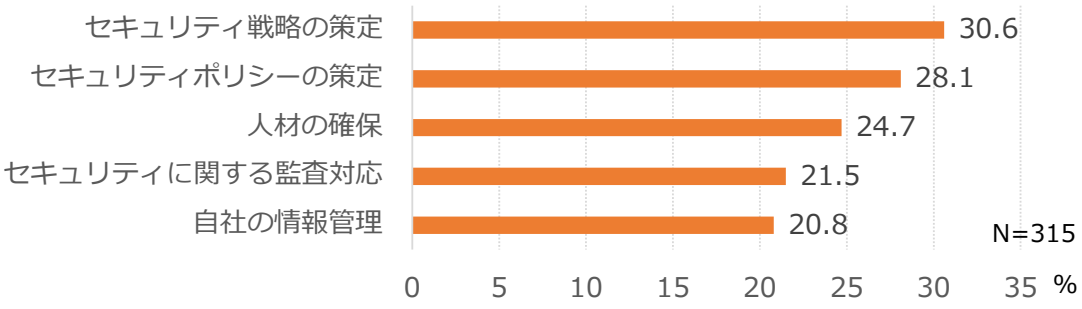


DX推進のために活用したシステムにおいて、何かしらのサイバーセキュリティインシデントは発生しましたか。（単一回答）

セキュリティインシデントによって、どのような被害がもたらされましたか。(複数回答)

図表 2 DX におけるセキュリティインシデント発生状況

また、自社の DX 推進におけるサイバーセキュリティ対策について懸念があるかを聞いたところ、懸念材料としては、「セキュリティ戦略の策定」が約 31%、「セキュリティポリシーの策定」が約 28%と、組織のセキュリティ対策の軸である戦略やポリシーの策定に懸念を持っている企業が多い。



自社のDX推進におけるサイバーセキュリティ対策について懸念はありますか。あなたが最も関わりが深い自社のDX推進について、あてはまるものを全て選択してください。（複数回答）

図表 3 DX 推進におけるサイバーセキュリティ対策の懸念

[3] トレンドマイクロ「DX 推進における法人組織のセキュリティ動向調査」（2021 年 11 月），https://www.trendmicro.com/ja_jp/about/press-release/2021/pr-20211130-01.html

ここで、実際にセキュリティが原因で DX が失敗した例を見ていきたい。

図表 4 は、セキュリティ不備が原因で DX サービス（新しいデジタル技術を活用した新規ビジネス）が廃止となった主な国内事例である。大手通信事業者と大手小売業の例は、いずれも不十分な認証機能が原因で、日本全国の利用者等が金銭的な被害を被ったものだ。また、大手人材サービス業の例では、学生に同意なく個人データを企業等に提供したことで、社会的に大きな問題となり、サービス廃止に至った。

このように、DX におけるセキュリティ対策を怠ると、不正アクセス等により機密情報が流出してしまうだけではなく、サービス自体が廃止になってしまうこともあるのだ。

一方で、セキュリティ統制を効かせるタイミングは重要である。一般的な DX 推進部門は、短期間でプロトタイプ（試作品）を多数開発し、PoC（Proof of Concept：仮説の証明）を繰り返してシステムを開発する傾向がある。このトライ＆エラーの段階で、セキュリティ部門が強い統制を効かせることは望ましくない。セキュリティが DX の足かせになってはいけないからだ。セキュリティ責任者は、DX にブレーキをかけるのではなく、セキュアな PoC 環境の整備やガイドラインを策定することで、DX をアシストしていくという考え方になるべきである。PoC が承認され、商用サービスを具体的に検討する段階で、セキュリティ責任者が積極的に関与していくことが望ましい。

一般に公開されている情報ではないが、企業内のセキュリティ管理体制を強固にしすぎたため、DX のためのシステムリリースが大幅に遅延したり、セキュリティ対応で疲弊したりしたためプロジェクトメンバーの意識が低下し、多くの退職者が出たという話も耳にするようになった。DX 推進とセキュリティ管理のバランスが今後増々重要になっていくだろう。

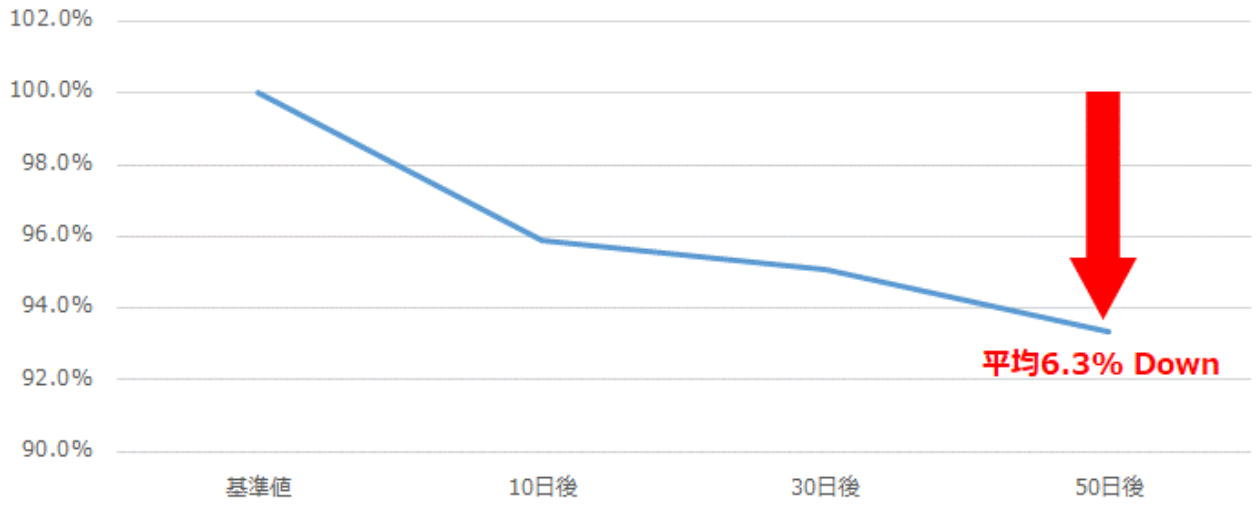
企業種別	時期	DXの取り組み	セキュリティ不備事項	結果
大手通信事業	2019年	スマートフォンを用いた電子決済サービス	不十分な認証機能が原因で不正引出しが発生	単体でのサービス提供終了（別アプリへ一部機能を統合）
大手小売業	2019年	スマートフォンを用いたバーコード決済サービス	不十分な認証機能が原因で不正チャージや不正利用が発生	サービス廃止
大手人材サービス業	2019年	学生の個人情報をAI（人工知能）で分析し、内定辞退率を予測するサービス	個人データの第三者提供に関する同意取得を行っていなかった	サービス廃止
ネットサービス業	2018年	デジタルコンテンツに特化したダウンロード販売専門のマーケットプレイス	不正アクセスによりクレジットカード情報が流出	サービス廃止（後日、マーケットプレイス事業を他社へ譲渡）

図表 4 セキュリティ不備が原因で DX サービスが廃止となった主な国内事例

3. サイバーリスクの金銭的影響

日本国内で情報流出等の適時開示を行った企業 47 社を JCIC が調査したところ、適時開示後 50 日後には株価が平均 6.3%下落したことがわかった。2018 年の調査では、平均 10%の下落率であったため、若干の改善は見られたものの、依然として株価影響は避けられない状況である。株価が下落する理由としては、インシデント対応の金銭的影響に加え、システムの停止や新規営業活動の停滞が懸念され、企業価値が低下したことが考えられる。

なお、適時開示を行った企業の売上高と純利益の変動についても今回調査したが、コロナ禍による業績影響が大きく、精緻な数値が得られなかったため、本レポートでの調査データの公開は見送った。



図表 5 不正アクセス等の適時開示後の株価推移（n=47）

調査手法
- 証券取引所へ不正アクセス等の「適時開示」を行った 47 社
- 2014 年 7 月以降の適時開示企業を対象
- 開示日より 10 日前を 100%（基準値）とした
- 日経平均株価の変動値は調整済み

図表 6 は、近年サイバー攻撃によって発生したセキュリティインシデントの例である。1 回のサイバー攻撃によって大規模な金銭的損害が発生しているケースが世界で発生していることがわかる。もはや、DX 推進のためのサイバーセキュリティ「DX with Security」は、IT 担当役員や CISO、セキュリティ部門だけの問題ではなく、取締役や経営者等の役員が一丸で取り組むべき経営課題となったといえる。

#	時期（降順）	国・地域	組織	影響種別	金銭影響	概要
1	2021年11月	日本	病院	改修費用	2億円	新電子カルテシステム構築費用
2	2021年8月	日本	建設	特別損失	7.5億円	ランサムウェア感染の調査復旧費用
3	2021年5月	ブラジル	食肉加工	身代金	12億円	ランサムウェアに感染し身代金を支払った
4	2020年10月	英国	航空	制裁金	27億円	個人情報漏えいによるGDRP違反
5	2020年10月	英国	ホテル	制裁金	25億円	個人情報漏えいによるGDRP違反
6	2019年3月	ノルウェー	製造業	営業停止	45億円	ランサムウェア感染により生産量減少
7	2018年10月	香港	航空	時価総額	226億円	不正アクセスにより株価3.8%安
8	2018年8月	台湾	半導体	営業停止	275億円	ランサムウェア感染により製造が3日停止
9	2018年1月	日本	暗号資産	金銭被害	580億円	不正アクセスにより暗号資産が流出
10	2017年12月	米国	運輸	営業停止	440億円	ランサムウェア感染による大規模な影響
11	2017年8月	デンマーク	運輸	営業停止	330億円	ランサムウェア感染により輸送が遅延し混乱
12	2017年6月	ドイツ	製薬	営業停止	360億円	ランサムウェア感染によりネットワーク停止
13	2016年2月	バングラデシュ	銀行	金銭被害	1080億円	不正アクセスにより海外口座に不正送金
14	2014年7月	日本	教育	特別損失	260億円	内部犯行による情報漏えい後、対策費に投資

図表 6 金銭的被害が発生したセキュリティインシデント事例

4. 役員の責任

企業が DX with Security を推進する際、技術的な側面がクローズアップされることが多いが、役員・従業員の法的な責任、損害賠償責任といった法的な視点からの検討も欠かすことはできない。セキュリティ対策は DX を推進するための経営上極めて重要な意義を有するものであることから、会社法上の内部統制システムの構築にあたって検討すべき主要な要素の一つだと考えられる。つまり、セキュリティ対策の未整備は、自社が被害を受けるだけでなく、他者に被害を与えたことによる損害賠償や善管注意義務違反に問われる恐れもあるのだ。

また、株主や機関投資家等からは DX 推進を停滞させ企業価値を低下させたとして、集団訴訟を起こされたり、取締役会で報酬返上や退任を求められたりする場合がある。特に米国では、個人情報漏えいに関する集団訴訟が活発であり、多額の和解金を勝ち取った事例が多数存在する。日本国内では、集団訴訟事例は数少ないが、経営者の退任や報酬返上の事例は多数存在している。

企業種別	概要	和解金等
保険会社	米国約8000万人の顧客データが流出	和解金127億円
小売業	米国7000件のクレジットカード情報が流出	和解金31億円
小売業	米国5600件のクレジットカード情報が流出	和解金28億円
ネットサービス業	カナダのマッチングサイトで3600万件のデータが流出	和解金14億円
製造業	不正アクセスにより公開前のコンテンツや従業員情報等が流出	和解金9億円
ネットサービス業	米国の大量のユーザー情報が流出	和解金55億円
自動車配車業	米国5700万人の個人情報がサイバー攻撃によって流出	和解金170億円
小売業	米国200万人の情報漏えいがCCPA違反として、集団訴訟を実施	係争中
通信事業業	営業機密を持ち出し協業に転職した件で、1000億円の損害賠償を請求	1000億円の損害賠償請求権を主張
教育業	お詫びの500円の金券が不十分だとして集団訴訟を実施	係争中

図表 7 情報セキュリティに関する訴訟の事例

企業種別	時期	概要	影響
ネットサービス業	2021年	不正アクセスによる会員情報流出	CEO役員報酬3か月30%減
証券取引所	2020年	システム障害によるサービス停止	CEO辞任
小売業	2019年	認証機能不備によるサービス廃止	CEO退任
ゲーム業	2018年	不正アクセスによるサービス停止	代表取締役社長1年間無報酬
地方自治体	2019年	職員による個人情報の持ち出し	市長給与2か月減給10%

図表 8 経営者の退任や報酬返上の事例

更に、プライバシー・データセキュリティは、企業の ESG 等のサスティナビリティ格付けにも影響することにも留意が必要だ。セキュリティ対策といった非財務情報の開示によって、機関投資家の各種企業格付けにプラスの影響を与えることがある。逆に、格付け会社が該当企業からの情報が得られない場合、評価が低くなることもある。企業の ESG 評価が格下げとなった場合、資金調達コスト増や取引先減少のリスクも生じるため、重大な経営ダメージになる恐れがある。

説明責任を果たすためには、平時から自社のセキュリティの取り組み状況を自社サイトや株主向けサイト等で広く情報公開し、顧客やステークホルダーの信頼向上につなげることが重要である。なお、情報発信する際は、サイバー攻撃のヒントになるような情報などは公開する必要はなく、経営者の取組み姿勢を広く発信すべきである。詳しくは、損失額を減らすための「サイバーセキュリティ情報公開のポイント[4]」を参照されたい。

格付け機関	Dow Jones Sustainability Indices（DJSI）	MSCI（モルガン・スタンレー・キャピタル・インターナショナル）
概要	専門家アンケートで、「品質が高い ESG 格付機関」の 1 位に選定された代表的な格付け評価	世界最大のインデックスプロバイダの一つであり、MSCI ESG Research 部門がおよそ 7,500 の発行体の ESG 評価を実施
情報源	・質問票による調査 ・企業の公開情報	・企業の公開情報
評価方法	各企業（約 5000 社）の ESG データに基づきスコアを算出の上、評価の高い銘柄をインデックスに選定	スコアリングの上、AAA/AA/A/BBB/BB/B/CCC の 7 段階で評価
プライバシー・データセキュリティ評価の位置づけ	業種によって「Cybersecurity & System Availability」や「Privacy Protection」が 100 点満点で評価される	「社会」スコアの中に、「製品サービスの安全」－「プライバシー＆データセキュリティ」という評価項目が設定されており、10 段階で評価

図表 9 主な ESG 格付け機関のプライバシー・データセキュリティ評価の位置づけ

[4] JCIC「サイバーセキュリティ情報公開のポイント ～経営者の取組み姿勢が重要～」, https://www.j-cic.com/pdf/report/Disclosure-Report.pdf

5. DX with Security 戦略実現のための推奨アプローチ

DX を推進し、企業の生産性向上や効率化を実現するため、また甚大な金銭的損失を回避するためには、「DX with Security 戦略」が不可欠である。DX with Security 戦略とは、「DX の目的を達成するためのセキュリティ方針」を意味する。また、中長期的なセキュリティリソース（予算、人材等）計画を検討し、取締役会等で承認されることも求められる。

DX with Security 先進企業が戦略を策定するために、JCIC では以下のアプローチを推奨する。

DX with Security 先進企業のための戦略策定の推奨アプローチ

①サイバーリスク数値化モデルを用いリスクを可視化せよ

②DX with Security 戦略を策定せよ

- **ストーリーとして戦略を語るためのフレームワークを活用すべき**
- **セキュリティ投資額は、連結売上高の 0.5%以上を投資すべき**
- **セキュリティ人材は、全従業員数の 0.5%以上を確保すべき**

③セキュリティ KPI を設定し、定期的にモニタリングせよ

①サイバーリスク数値化モデルを用いリスクを可視化せよ

サイバーセキュリティを議論する場合、技術的な観点での議論に終始しがちである。しかし、セキュリティ責任者が経営者に説明する際は、ビジネス視点で報告すべきである。最も効果的にビジネス視点でサイバーセキュリティを説明する方法は、経営の共通言語である「お金」を用いることである。経営者は、IT 用語には詳しくないかもしれないが、お金のことを理解しない経営者は存在しないからだ。

サイバーリスクの定量化については、様々な研究が世界で行われているが、攻撃自体が進化しているため、未だ確立されたリスク定量化手法は存在していない。近年、海外ではサイバーリスクの数値化の研究に取り組んでいるが、データ収集や複雑な計算処理に社内リソースを要するため、必ずしも日本企業に適しているとは言えない（参考資料を参照）。

そこで、JCIC が 2018 年に発表した「サイバーリスク数値化モデル」を最新版に更新し、日本企業が最大損失額（PML、Probable Maximum Loss）を簡易に算出できるようにした。このモデルは、最大損失額の目安を算出するものであり、JCIC のウェブサイトで簡易シミュレーションの Excel ツールを公開している。

この数値化モデルを用いることで、サイバーセキュリティを技術的な議論にせず、経営の共通言語である「お金」でリスクを議論することができる。損失額を議論のスタート地点にすれば、経営と現場の課題の理解を共通化することができ、経営者がサイバーリスクを自分事として捉えてもらうことの契機になるはずだ。

		最大損失額の目安	算出根拠
直接被害	個人情報漏えいによる金銭被害	▲12億円	1人あたり推定損害賠償額は、JNSAによるJOモデルを参考に算出（10万件流出の場合：12億円の損害賠償額）
	ビジネス停止による機会損失	5営業日あたり ▲20億円	ランサムウェア感染により大規模システム停止が発生した際の最大業務影響
	法令違反による制裁金	▲1億円	日本の改正個人情報保護法の罰金額（EUや中国の個人情報を有する場合、別途制裁金が科せられる恐れあり）
	事故対応費用	▲0.6億円	フォレンジック調査、コールセンター費用、ダークウェブ調査、再発防止費用等
間接被害	時価総額への影響	▲63億円	JCIC調査実績より算出 （時価総額1000億円×6.3%=63億円）

図表 10 サイバーリスク数値化モデル（年商 1000 億円の製造販売業の場合）

②DX with Security 戦略を策定せよ

- **ストーリーとして戦略を語るためのフレームワークを活用すべき**

DX の目的を達成するためのセキュリティ方針（DX with Security 戦略）は、誰が聞いても同じ理解になるよう、シンプルなものが求められる。技術用語は用いず、課題と解決策がストーリーになっている必要がある（参考資料を参照）。ストーリーとして戦略を語るためには、フレームワークを用いることが有効である。以下に、参考となる DX with Security 戦略のためのフレームワークを示す。

項目	説明
DX の目的	DX を実施するための目的やゴールを記載
セキュリティ課題	DX を推進する上でのセキュリティやプライバシー保護の課題を記載
解決策と効果	課題を解決するための打ち手と、それを実現した時のメリットを記載
投資計画	売上高に占めるセキュリティ投資の割合は、連結売上高の「0.5%」以上を推奨
人員計画	総従業員数に占めるセキュリティスタッフ比率は「0.5%」以上を推奨

図表 11 DX with Security 戦略のためのフレームワーク

【モデルケース A】年商 5000 億円、従業員数 5000 人の製薬業

項目	DX の目的を達成するためのセキュリティ方針（DX with Security 戦略）
DX の目的	最先端の創薬技術力を築くため、国内外の大学や病院と連携し、AI やヘルステック等のデジタル技術を活用した革新的な新薬創出プロセスを 3 年以内に構築する。
セキュリティ課題	医療研究データは、サイバー攻撃の標的になっているため、厳格なセキュリティ対策が求められる。情報漏えいが発生した場合、直接被害が 370 億円、間接被害が 330 億円も発生する恐れがある。
解決策と効果	セキュアなクラウドサービス、ゼロトラストアーキテクチャ実装、協力パートナーのアクセス管理の強化等を実施する。AI 創薬、ウェアラブル端末による治験等、新たな創薬プロセスを社外パートナーとセキュアに構築できるため、新薬開発を短縮化できる。
投資計画	年 25 億円
人員計画	25 名　（正社員 20 名、外部委託 5 名）

【モデルケース B】年商 1000 億円、従業員数 2000 人の製造販売業

項目	DX の目的を達成するためのセキュリティ方針（DX with Security 戦略）
DX の目的	顧客への付加価値向上のため、オンライン会員登録を増加させ、年額サブスクリプション型のサービスを新規展開する。3 年以内に売上 20%増を実現する。
セキュリティ課題	個人情報を大量に扱うことになるため、情報盗難が発生すると、直接被害が 34 億円、間接被害が 66 億円も発生する恐れがあり、当社経営戦略に対する大きなインパクトとなる。
解決策と効果	セキュアシステム開発導入、従業員教育、セキュリティ人員増加等により開発利便性とセキュリティ管理を高い次元で実現する。この結果、付加価値と安心のブランドを確立し、他社との差別化を図る。
投資計画	年 5 億円
人員計画	10 名　（正社員 7 名、外部委託 3 名）

【モデルケース C】年商 300 億円、従業員数 1000 人の教育塾

項目	DX の目的を達成するためのセキュリティ方針（DX with Security 戦略）
DX の目的	授業サービス品質向上のため、データ活用型のオンライン授業やコンテンツを 2 年以内に新規開発する。またオンライン専門校を設立することで遠隔地の生徒を取り込む。
セキュリティ課題	IT に詳しくない学生でも使いやすいサービスにしつつ、成績や進路といった機微な情報を厳格に守る必要がある。大規模な事故が発生した場合、直接被害が 17 億円、間接被害が 10 億円も発生する恐れがある。
解決策と効果	ユーザーアカウントの多要素認証の実装、不正アクセス対策、従業員教育、生徒への啓発を実施する。セキュアなデジタルツール提供により、既存生徒の単価向上、遠隔地の新規生徒の取り込みを実現する。
投資計画	年 1.5 億円
人員計画	5 名　（正社員 4 名、外部委託 1 名）

● **セキュリティ投資額は、連結売上高の「0.5%以上」を投資すべき**

DX with Security 戦略が経営者等から承認されるためには、中長期的なセキュリティリソース（投資予算、人員等）計画も策定しなければならない。

まず、DX with Security 先進企業のセキュリティ投資額は、連結売上高の「0.5%以上」を目安に計画することを推奨する。「0.5%以上」という目安は、金融機関の調査データから設定した[5]。DX with Security をリードする企業は、IT システムを用いて付加価値を生み出している金融機関並みに投資を強化すべきという考えが背景にある。この投資額には、人件費、アウトソース費用、セキュリティシステム購入費や利用費等が含まれる。例えば、年商 10 億円企業の場合、セキュリティ投資額は年 500 万円、また年商 1000 億円企業の場合、セキュリティ投資額は年 5 億円が目安となる。

現段階では、「0.5%以上」を参考にすべき企業対象は、IT 企業並みに人材と予算を DX に投資し、ビジネスモデルや業務プロセスを変革する「DX with Security 先進企業」である。つまり、利便性とセキュリティ管理を全社的に高い次元で実現しようとする企業（利便性重視・モニタリング型）が、セキュリティ投資額の目安として活用していただきたい。その後、DX with Security のフォロワー企業も将来の目標値として活用することを想定している。

連結売上高	セキュリティ投資額の目安（連結売上高の0.5%）
1兆円～	50億円～
5000億円	25億円
1000億円	5億円
500億円	2.5億円
100億円	5000万円
50億円	2500万円
10億円	500万円

なお、セキュリティ投資額については、IT 予算に占める割合から算出する方法、従業員 1 人あたりの支出額から算出する方法もある。前者の目安としては、IT 予算の 5%～9.99%をセキュリティに投資している日本企業が多い[6]。後者の目安としては、フルタイム従業員 1 人あたり約 31 万円（2,691 米ドル）のセキュリティ投資額を金融機関では行っているという調査データがある[7]。

[5] FS-ISAC（金融サービス情報共有分析センター）とデロイトが実施した金融機関に対する調査によると、総収益に占めるサイバーセキュリティ支出は、2019 年の 0.34%から 2020 年には「0.48%」に増加している。
https://www2.deloitte.com/content/dam/Deloitte/jp/Documents/risk/cr/jp-cr-reshaping-the-cybersecurity.pdf
また、JP モルガンは、年間約 660 億円以上をサイバーセキュリティに投資しており、このセキュリティ投資額は同社営業収益の「0.5%」に相当する。https://reports.jpmorganchase.com/investor-relations/2018/ar-ceo-letters.htm
サイバーセキュリティ支出の割合が増加していること、また DX with Security を目指す企業は金融機関並みに投資を強化すべきという理由から「0.5%」を目安の数値とした。

[6] PwC「Digital Trust Insights レジリエンス指数を高めるために」,
https://www.pwc.com/jp/ja/knowledge/thoughtleadership/2020/assets/pdf/resiliency-quotient2002-02.pdf

[7] FS-ISAC・デロイト「サイバーセキュリティ展望を再構築」,
https://www2.deloitte.com/jp/ja/pages/risk/articles/cr/reshaping-the-cybersecurity.html

セキュリティ投資額に含めるべき投資項目を以下に示す。投資の区分は、「人件費」、「教育費」、「システム費[8]」、「アウトソース費」、「評価・監査費」に分けられる。企業によって、予算の組み方は異なるため、あくまでも参考情報として活用していただきたい。

区分	主なセキュリティ投資項目
人件費	専任のセキュリティ人員の人件費
教育費	セキュリティ研修費用
システム費	セキュリティシステム購入・保守費用
	セキュリティサービス利用費用
	コンサルティング費用
	アウトソース費用
アウトソース費	派遣社員の人件費
	コンサルティング費用
	業務委託・アウトソース費用
評価・監査費	認証制度の新規取得・更新費用
	外部監査費用

図表 12　主なセキュリティ投資項目

なお、IT 費用とセキュリティ費用の区分けが難しいケースがある。例えば、クラウドサービスに含まれるセキュリティオプション機能等は費用の区分けが難しい。このようなケースでは、厳密に費用配賦を管理するよりも、主要な機能を提供している項目に計上すること、つまりクラウドサービスであれば IT 費用として計上するほうが現実的であると考えられる。同様に、本業に加えてセキュリティ業務を兼務している人材の人件費は、本業の部門に計上したほうが現実的である。

適切な社内セキュリティリソースを確保し、主要施策を遂行することにより、前述のセキュリティ課題が解決され、DX の目的を達成できるメリットがある。また、各種セキュリティアセスメントの評価や成熟度が向上することも期待できる。どこからセキュリティ対策を行うべきか悩んでいる企業には、情報処理推進機構（IPA）の情報セキュリティ診断[9]を実施することを推奨する。セキュリティ診断の流れは以下の通りであり、推奨される取り組みが可視化されるため、次のアクションに繋げやすくなる。

1. 「サイバーセキュリティ経営可視化ツール」の設問に回答
2. 診断結果が表示され、ベンチマーク比較や推奨される取り組みを確認
3. 関連するプラクティス（施策事例）を確認

[8] 企業によっては、SOC やデータセンター等の賃料を含める場合がある

[9] 情報処理推進機構（IPA）「情報セキュリティ診断」, https://security-shien.ipa.go.jp/diagnosis/

セキュリティリソース「0.5%以上」に関する留意事項

- 「0.5%以上」という数値は、あくまでも目安である。連結売上高や従業員数の変動に関わらず、複数の情報源から自社にとって適切な目標を掲げる必要がある
- 新規システム導入やインシデント対応等の状況によりセキュリティリソースが 0.5%よりも必要になる場合、または投資が落ち着いたため 0.5%未満になっても問題がない場合がある
- セキュリティ投資額、専任セキュリティ人材数は、全社のリソース総計である。一部のシステムや部門だけの数値ではない
- 現段階では、0.5%以上を参考にすべき企業対象は、DX with Security 先進企業である。DX with Security のフォロワー企業も将来の目標値として活用できる
- IT 費用とセキュリティ費用の区分けが難しい場合、主要な機能を提供している項目に計上することが望ましい

【コラム】新規 DX システムにかけるべきセキュリティリソース

今回の連結売上高の「0.5%以上」というのは、1 企業が確保すべきセキュリティ投資額の目安である。一方、新規 DX システム開発において、どの程度セキュリティリソースが必要であるかという質問も多くいただいている。

新規開発するシステムの特性によって、適切なセキュリティ投資額の割合は変わるが、新規 DX システム投資額の内、「10%」をセキュリティ投資に割り当てることが目安になると考えられる。

この「10%」の理由は、前出の FS-ISAC・デロイトが実施した金融機関に対する調査によると、IT 支出に占めるセキュリティ投資額の割合は「8.2%～11.9%」であるためだ。新たな DX にチャレンジするにあたり、金融機関並みのセキュリティ投資が求められるという考えから 10%が目安になるであろう。

- **セキュリティ人材は、全従業員数の 0.5%以上を確保すべき**

DX with Security 先進企業が専任のセキュリティ人員数を検討する場合、全従業員の「0.5%以上」を目安に計画することを推奨する。0.5%の数値は、各種レポートや JCIC 調査によって設定した[10]。このセキュリティ人員数には、専任でセキュリティ業務に従事する正社員、IT 子会社社員、アウトソースを含む総人数が含まれる。海外の現地法人や子会社でセキュリティ業務に従事している人材がいる場合、その人員数もカウントする。なお、プラス・セキュリティ人材（本来の業務を担いながら IT を利活用する中でセキュリティスキルも必要となる人材）は、この専任セキュリティ人員数に含めない。

例えば、全従業員が 500 人の場合、セキュリティ人員数は 3 人、また全従業員が 3000 人の場合、セキュリティ人員数は 15 人が目安となる。なお、全従業員が 1 万人の大企業の場合は、業種業態によって変動要素が大きいため 50 人～とした。また、従業員数 100 名以下の場合、バックアップ体制を考慮し、セキュリティ人員数の目安を 1 名ではなく 2 名とした。

人員数も同様に、「0.5%以上」という目安は、現段階では DX with Security 先進企業が対象となり、今後 DX with Security のフォロワー企業も将来の目標値として活用することを想定している。

総従業員数	専任セキュリティ人員数の目安（総従業員数の0.5%）
10,000人～	50人～
5,000	25
3,000	15
1,000	5
750	4
500	3
250	2
100	2

[10] (a)ITR「国内 IT 投資動向調査報告書 2021」によると、総従業員数に占める IT スタッフ比率は、「平均 7.2%」であり、その比率は年々増加している https://enterprisezine.jp/article/detail/12656
(b)カーネギーメロン大学が年商 60 億円以上、4 ヵ国の 555 組織を調査したところ、IT 部門社員数の割合に対するセキュリティ社員は「平均 5.2%」であった https://resources.sei.cmu.edu/asset_files/TechnicalNote/2015_004_001_446198.pdf
上記(a)、(b)より、総従業員数に占めるセキュリティスタッフ比率 = 総従業員数 x (a) 7.2% x (b) 5.2% = 0.37%
また、「韓国の電子金融監督規定」では、全社員数に対するセキュリティ社員は「0.25%以上」、セキュリティ予算は、IT 予算総額のうち「7%以上」という数値を規定している。 http://www.law.go.kr/행정규칙/전자금융감독규정 （第 8 条）
IT スタッフ比率が年々増加していること、また DX with Security を目指す企業は業界平均より人員強化すべきという理由から「0.5%」を目安の数値とした。なお、「0.5%」の妥当性を検証するために、JNSA「セキュリティ業務を担う人材の現状調査報告書」や JCIC 内のナレッジを活用して検証した。

専任セキュリティ人材の主なタスク（業務内容）を以下に示す。タスク区分は、セキュリティ統括部門や CISO オフィスが担う「ガバナンス（方針策定や内部統制）」や「アセスメント（評価や監査）」、SOC や CSIRT が担う「オペレーション（運用やインシデント対応）」に分けられる。セキュリティ体制検討や人材確保を計画する際は、どのタスクに何名のセキュリティ人材を割り当てるか、どの部分をアウトソースするかを検討する必要がある。

区分	タスク名
ガバナンス	セキュリティ戦略策定（予算、体制含む）
	セキュリティポリシー策定・改訂
	セキュリティ教育・普及啓発
	コンプライアンス・プライバシー対応
アセスメント	リスクアセスメント
	脆弱性診断、ペネトレーションテスト
	セキュリティ監査
オペレーション	セキュリティサービスの導入・運用
	セキュリティ監視・検知・対応
	インシデントレスポンス
	フォレンジック、マルウェア解析
	脅威・脆弱性情報の収集・分析・活用

図表 13　専任セキュリティ人材の主なタスク [11]

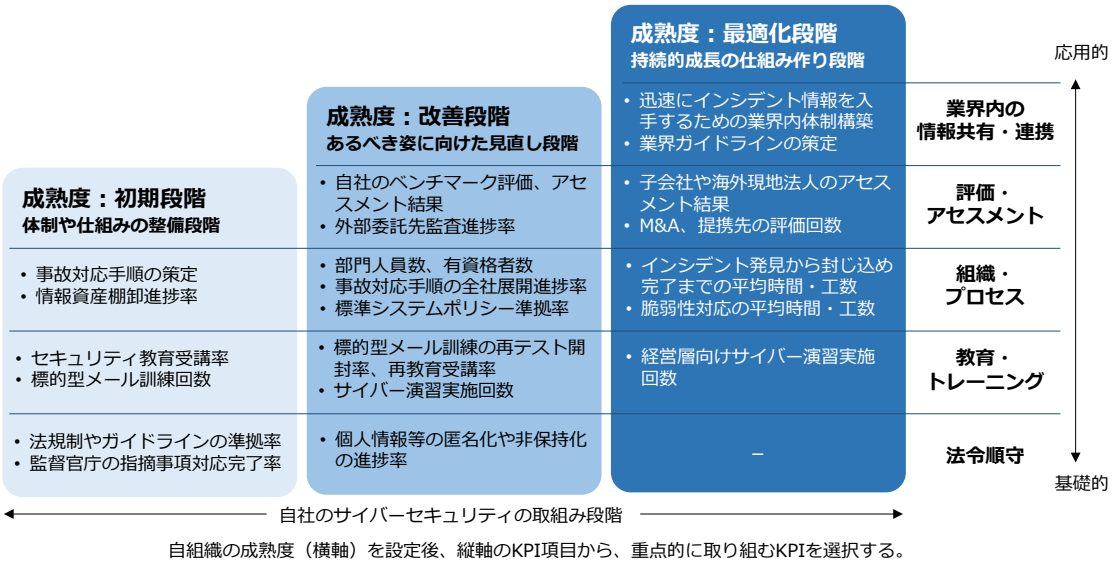
セキュリティ人材確保や育成は多くの企業で課題になっており、国内外で様々な研究調査が行われている。体制検討や育成に関して、特に参考になる情報を以下に示す。

- **セキュリティ体制検討に役立つ情報**
  - 経済産業省「サイバーセキュリティ体制構築・人材確保の手引き」
  - JNSA「セキュリティ業務を担う人材の現状調査報告書」
  - CRIC CSF「ユーザー企業のためのセキュリティ統括室構築・運用キット（統括室キット）」
- **人材育成に役立つ情報**
  - NISC「サイバーセキュリティ・ポータルサイト」
  - JCIC「攻めのプラス・セキュリティ人材で DX with Security の実現を」
  - 日本サイバーセキュリティ人材キャリア支援協会（JTAG 財団）「VisuMe」
  - 米国 NIST「NICE Framework」

[11] 経済産業省「サイバーセキュリティ体制構築・人材確保の手引き」を参考に JCIC が作成

③セキュリティ KPI を設定し、定期的にモニタリングせよ

サイバーセキュリティ施策が有効に機能しているかをモニタリングするためには、サイバーセキュリティの KPI を用いることが有効である。JCIC では、セキュリティ責任者が自組織の取組み段階（成熟度）に応じた 47 種類の KPI をモデルから選択し、目標設定やパフォーマンス評価に活用することを提案している。詳しくは、損失額を減らすための「サイバーセキュリティの KPI モデル[12]」を参照されたい。



図表 14 サイバーセキュリティの KPI モデル

KPI によるモニタリング状況は、定期的に取締役会等に報告すべきである。この KPI に加え、サイバー空間で起きている攻撃の傾向、他社の取り組み、関連する法規制の動向も取締役にとって有益である。

2022年度　セキュリティ投資額

計画	実績	昨年比
¥200 M	¥195 M	18% ↑

施策導入状況

セキュリティ施策		KPI	実績
リスク管理体制	サイバーセキュリティ関連人員の増員	CSIRT 7名→10名	社員 +1名
			外注 +2名
		運用要員 3名→5名	外注 +2名
サプライチェーン	系列企業・ビジネスパートナーの対策実施状況確認	+5社（68%→82%）	4社へ実施（76%）
業界内情報共有	情報提供の仕組み構築	完了	完了
	情報取得の仕組み構築	完了	遅延 2023年3月予定

運用状況

管理項目		実績	昨年比
セキュリティ事故	発生件数	124件	-5%
	想定損失	¥20 M	-6%
	復旧費用	¥1 M	+5%
リスク特定	リスク分析対象システム	231	+1%
	指摘事項数 High	53	+2%
	指摘事項数 Medium	230	-3%
	指摘事項数 Low	78	-4%
	対応進捗率	43%	+6%pt
教育	セキュリティ教育対象者	1,936名	+1%
	セキュリティ研修実施回数	36回	±0%
	研修受講率	85%	+2%

図表 15 経営陣への定期報告例

[12] JCIC「損失額を減らすためのサイバーセキュリティの KPI モデル（試論）」,https://www.j-cic.com/pdf/report/KPI-Report-JA.pdf

6. まとめ

本レポートでは、DX を推進し、企業の生産性向上や効率化を実現するため、また甚大な金銭的損失を回避するためには、「DX with Security 戦略」が必要であることを説明した。デジタル技術を活用し、画期的な新規ビジネスを展開したり、業務プロセスを抜本的に改革したりする DX においては、サイバーリスクは全ての DX で共通して考慮すべき事項であり、喫緊の課題である。コロナ禍においてデジタル化やリモートワークが浸透したこと、DX に取り組む企業が激増したことから、多くの企業で DX とセキュリティのバランスに頭を悩ませているが、皆様の組織における DX with Security 推進のヒントとして本レポートを活用していただきたい。

数年前までは、IT 部門とセキュリティ部門を自動車に例えて、IT 部門がエンジン役、セキュリティ部門がブレーキ役と表現されることがあった。時速 100km の速度で高速移動するためには、高性能なブレーキが必要というロジックである。しかし、DX with Security で求められるのは、DX 推進部門を適切な方向へ導いて成果をアシストする役割、電気自動車で例えると電子制御ユニット（ECU）の役割がセキュリティ部門に求められるのだ。つまり、セキュリティ部門の役割は、今までの守りの役割だけではなく、今後は事業部門と密接に連携して DX を伴走しながらアシストしていく役割も担う必要があるのだ。そのために、DX 検証環境やガイドラインの整備、積極的な DX プロジェクトへの関与とレビューの迅速化等、セキュリティ部門の方針やリソースを抜本的に見直すことも求められる。

最後に、本レポートで提示した重要ポイントのチェックリストを掲載する。このチェックリストは先述したアプローチに加え、姿勢や心構えも示した。ぜひとも、今後の参考にしていただきたい。

本レポートの主なポイント

- ✓ サイバーリスク数値化モデルを用いリスクを可視化すること
- ✓ ストーリーとして戦略を語るためのフレームワークを活用し、DX with Security 戦略を策定すること
- ✓ セキュリティ投資額は、連結売上高の 0.5%以上を目安とすること
- ✓ 専任のセキュリティ人材は、全従業員数の 0.5%以上を目安とすること
- ✓ セキュリティ KPI を設定し、定期的にモニタリングすること
- ✓ セキュリティの取り組み状況を、広く情報公開すること
- ✓ プロトタイプや PoC の段階では、強い統制を効かせないこと
- ✓ 商用サービスを具体的に検討する段階で、セキュリティ責任者が関与していくこと

以上

参考資料①　サイバーリスク指標モデル「想定損失額の目安」の解説

JCJC では、日本企業が最大損失額（PML、Probable Maximum Loss）を簡易に算出できるように簡易シミュレーションの Excel ツールを公開している。黄色セルの入力項目をすべて選択・入力すると、組織におけるサイバーリスクにおける潜在損失額が算定される。

項目	入力項目	説明
①-1～①-3 個人情報漏えいによる金銭被害	• 機微情報度 • 本人特定容易度 • 個人情報数	セキュリティ事故によって個人情報が漏えいした場合の想定損害額。JNSA が公開している「JO モデル」を用いた損害賠償額算定式より算出。 なお、入力者の負担を軽減するため、「社会的責任度」は年商 1000 億円以上の場合「高」とし、年商 1000 億円未満は「その他」とした。また、事後対応評価は、いずれの場合も「不明」とした。
②-1～②-2 ビジネス停止による機会損失	• 1 日あたりの売上 • 事業中断期間	ランサムウェア感染による社内システムや EC サイトの停止によって、業務が停止し、本来得られるはずだった売上機会の損失額。このシートでは簡易的に算出するため、「1 日の売上×事業中断期間」によって算出。
③法令違反による制裁金	• 全世界の売上高 • EU 個人情報有無 • 中国個人情報有無 • 日本個人情報有無	EU の一般データ保護規則（GDPR）、中国の個人情報保護法、日本の改正個人情報保護法による制裁金を想定。
④事故対応費用	• フォレンジック調査有無 • コールセンター費用有無 • ダークウェブ調査有無 • 再発防止費用有無	サイバー攻撃を受けたかどうかや攻撃を受けた場合の影響範囲や原因を調査するための費用（フォレンジック費用）、データの復旧費用、応急処置や再発防止のためのセキュリティ強化費用。JNSA「インシデント損害額調査レポート 2021 年版」を参考に想定金額を設定。なお、各企業でセキュリティ業者等にヒアリングを行い算出することが望ましい。
⑤株価下落による時価総額減少額	時価総額	JCIC の調査実績より算出。47 社を調査した結果、セキュリティ事故の適時開示 50 日後に株価が 6.3%減少。

サイバーリスク指標モデル「想定損失額の目安」

一般社団法人　日本サイバーセキュリティ・イノベーション委員会

version 2.0

あなたの組織について、回答欄に入力してください。

項番	大項目	中項目	設問	回答欄	
①-1	個人情報漏えいによる金銭被害	機微情報度	あなたの組織が保有する個人情報の種別を選んでください	1-1_氏名、住所、生年月日、メールアドレス、性別等_1	
①-2		本人特定容易度	あなたの組織が保有する個人情報は個人の特定が容易ですか	6_個人を簡単に特定可能（氏名、住所が含まれる）	
①-3		個人情報数	あなたの組織が保有する個人情報の数を入力してください	100,000	件
②-1	ビジネス停止による機会損失	1日あたりの売上	あなたの組織における1日あたりの売上総額を入力してください	400,000,000	円
②-2		事業中断期間	ランサムウェア感染により大規模システム停止が発生した際の最大業務影響日数を記載してください。（不明な場合、5日とします）	5.0	日
③	法令違反による制裁金	全世界の売上高	全世界の年間売上高（前年度）を入力してください	¥100,000,000,000	円
③-1		EU GDPR	EUの個人情報を保有していますか	No	
③-2		中国 個人情報保護法	中国の個人情報を保有していますか	No	
③-3		日本 個人情報保護法	日本の個人情報を保有していますか	Yes	
④-1	事故対応費用	フォレンジック調査	フォレンジック調査（10台）をアウトソースしますか	Yes	
④-2		コールセンター費用	コールセンター費用（3か月）をアウトソースしますか	Yes	
④-3		ダークウェブ調査	ダークウェブ調査（3か月）をアウトソースしますか	No	
④-4		再発防止費用	再発防止費用（ツール導入、組織編制、教育等）を想定しますか	Yes	
⑥	時価総額への影響	時価総額	上場企業の場合、現在の時価総額を入力してください	¥100,000,000,000	円

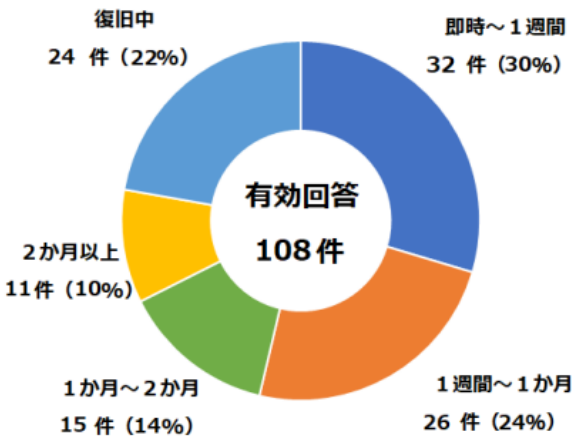
あなたの組織におけるサイバーリスクにおける潜在損失額

				（参考）	
直接被害	①個人情報漏えいによる金銭被害	-¥1,200,000,000		▲ 12.0	億円
	②ビジネス停止による機会損失	-¥2,000,000,000		▲ 20.0	億円
	③法令違反による制裁金	-¥100,000,000		▲ 1.0	億円
	④事故対応費用	-¥55,000,000		▲ 0.6	億円
間接被害	⑤時価総額への影響	-¥6,300,000,000		▲ 63.0	億円

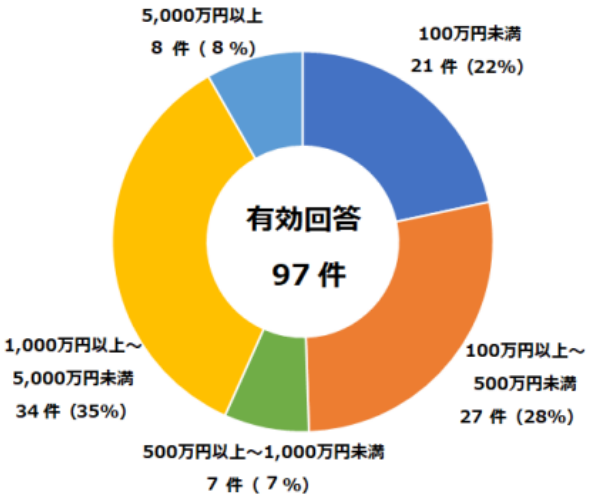
参考資料②　ランサムウェアに関する数値データ

項目	内容	補足
平均身代金支払い額 *1	322,168 ドル （約 3700 万円相当）	前四半期より 130%増加。大企業を目立つことなく標的にしたため。
身代金支払い額の中央値 *1	117,116 ドル （約 1350 万円相当）	前四半期より 63%増。
平均ダウンタイム *1	20 日	前四半期より 9%減。バックアップから回復できた企業が増加したため。
ランサムウェア修復コスト *2	1.85 百万ドル （約 2.1 億円相当）	前年より約 2 倍増加
身代金支払い割合 *2	32%	前年より 6 ポイント増加
年間ランサムウェア被害の報告件数（国内） *3	146 件	中小企業：54%、大企業：34%
被害からの復旧に要した期間（国内） *3	即時～一週間が最多	下のグラフ参照
被害の調査・復旧に要した総額（国内） *3	1000 万円以上～500 万円未満が最多	下のグラフ参照

被害からの復旧に要した期間



被害の調査・復旧に要した総額



*1 Coveware「Quartely Ransamware Report」, https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021
*2 Sophos「The state of ransomware - 2021」,
https://secure2.sophos.com/ja-jp/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf
*3 警察庁「令和３年におけるサイバー空間をめぐる脅威の情勢等について」,
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei_sokuhou.pdf

参考資料③　サイバーリスク定量化の国内外動向

前出の FS-ISAC・デロイトが実施した金融機関に対する調査によると、サイバーセキュリティ支出は金融セクターによって違いが生じている。2020 年の総収入に占めるサイバーセキュリティ支出は、消費者/金融サービス（ノンバンク）や保険では 0.3%であるのに対して、金融ユーティリティは 0.8%であった。また、IT 支出に占める割合は、8.2%～11.9%であった。従業員あたりの支出額は、1,984 米ドル～4,375 米ドルであり、日本円では従業員あたり 22.8 万円～50.3 万円の年間セキュリティ支出を行っている。

セクター別のサイバーセキュリティ支出

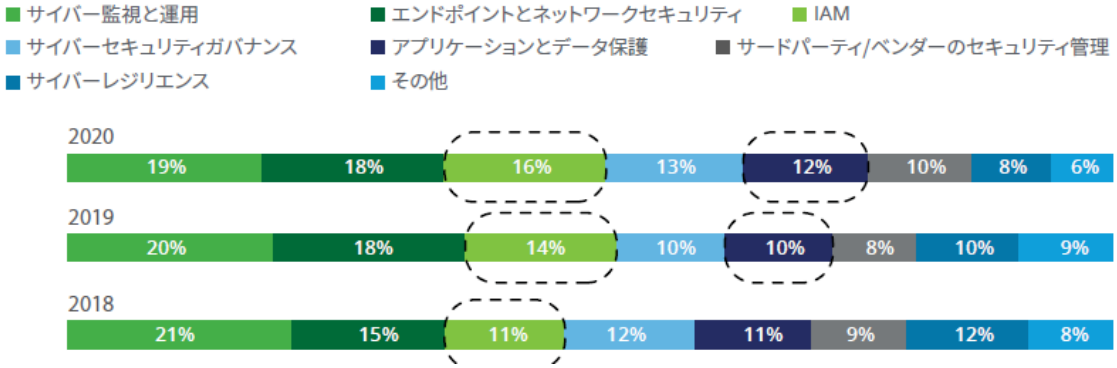
■総収益に占める割合　■IT支出に占める割合　■従業員あたりの支出額

	2019	2020
リテール/コーポレートバンキング	0.3% 10.1% 2,074米ドル	0.6% 9.4% 2,688米ドル
消費者/金融サービス (ノンバンク)	0.3% 9.7% 2,817米ドル	0.4% 10.5% 2,348米ドル
保険	0.3% 9.3% 2,245米ドル	0.4% 11.9% 1,984米ドル
サービスプロバイダー	0.6% 8.9% 1,956米ドル	0.6% 7.2% 3,226米ドル
金融ユーティリティ	0.8% 15.2% 3,630米ドル	0.8% 8.2% 4,375米ドル
全体	0.3% 10.1% 2,337米ドル	0.5% 10.9% 2,691米ドル

注）従業員とはフルタイムまたはフルタイムと同等の従業員を指します。

また、予算配分は 3 年間でほとんど変化していない。サイバー監視と運用、エンドポイントとネットワークセキュリティ、ID およびアクセス管理（IAM）の 3 分野で予算配分の 50%以上を占めていることが明らかになっている。

サイバーセキュリティ領域全体における予算配分



参考資料④　サイバーリスク定量化の国内外動向

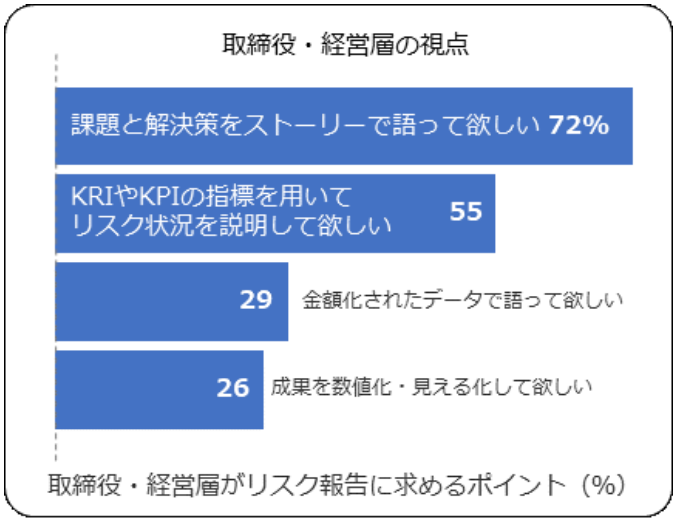
サイバーリスクの定量化については、様々な研究が国内外で行われている。しかし、日々攻撃が進化していることから、未だ確立されたリスク定量化手法は存在していない。

タイトル	組織名	発表時期	概要
Cost of a Data Breach Report	Ponemon Institute	2021年9月	データ侵害にかかる平均総コスト等、データ侵害の動向、それらの要因やコストの変動を把握すること目的とした調査。
予想損失額シミュレーション	東京海上日動	2020年3月	サイバー攻撃による被害が生じた場合の「予想損失額」を一定の計算ロジックから算出
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	JCIC	2018年9月	サイバーリスクを金額換算した「サイバーリスク指標モデル」
A Framework for Quantitative Assessment	IMF（国際通貨基金）	2018年6月	バリューアットリスク（VaR、最大損失額）によるサイバーリスクの定量的分析を実施。50か国の最新の被害事例を分析に用いた。
THE IMPACT OF DATA BREACHES ON REPUTATION & SHARE VALUE	Ponemon, Centrify	2017年5月	セキュリティ事故が発生した世界113社の株価を調査。113社の株価は平均5%下落した。
The Cyber-Value Connection	CGI IT UK	2017年4月	セキュリティ事故発生後の株価を調査。インシデント後、恒久的に株価が1.5%低下した。
FAIR（情報リスクの要因分析）モデル	FAIR INSTITUTE	2016年2月	定量的リスク分析モデル。潜在的な将来の損失（リスク）を、1つ以上のリスクシナリオの評価を通じ、金銭的価値として算出する。
A Framework for Categorizing Disruptive Cyber Activity and Assessing its Impact	University of Maryland	2015年7月	Cyber Disruption Index（CDI、サイバー破壊指数）という計算手法によりサイバー攻撃の影響を分析。

参考資料⑤　米国の取締役・経営層がサイバーリスクの報告時に求めるポイント

米国民間企業の調査によると、取締役・経営層は、サイバーリスク報告に求めるポイントとして、「課題と解決策をストーリーで語って欲しい」という回答が最も多く、次いで「KRI*や KPI を用いてリスク状況を説明して欲しい」という回答があった。

* KRI（Key Risk Indicators；企業のリスク度合いを測るリスク指標）

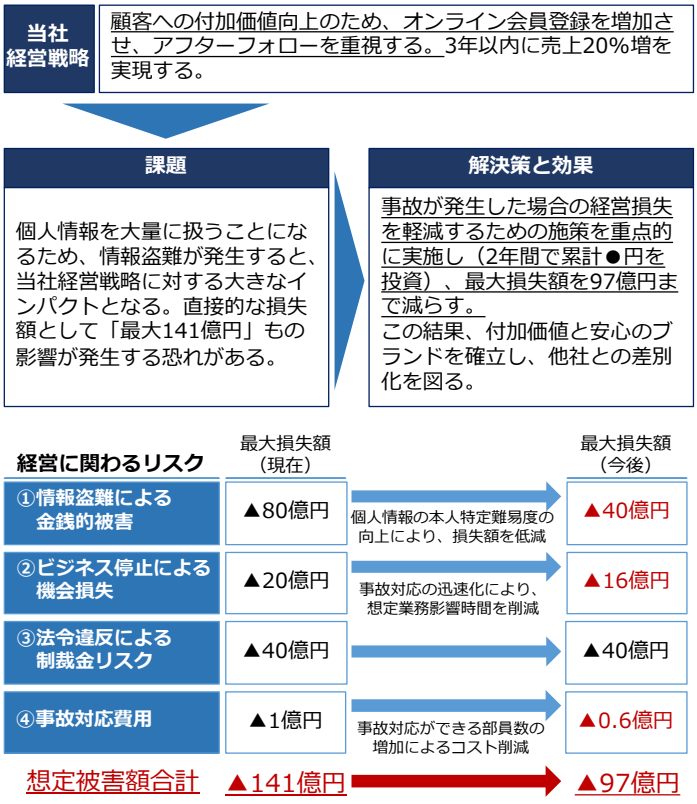


出所：Cyber Balance Sheet 2017 Report（Cyentia Institute 調査、n=85）

参考資料⑥　経営層への説明例

セキュリティ責任者が経営者に説明する際は、技術用語は用いずに、ビジネス視点で報告すべきである。最も効果的にビジネス視点でサイバーセキュリティを説明する方法は、経営の共通言語である「お金」を用いることである。

以下の説明資料は、業務用・家庭用の空調設備を取り扱う年商 1000 億円の製造業の例である。空調設備は成熟した市場であり、海外メーカーとの競合が厳しい状況になっている。そこで、中期経営計画として「顧客の声を重視した付加価値向上」を掲げ、製品購入時のオンライン会員登録を必須にし、消耗品の交換時期の通知などのアフターフォローを重視する戦略とした。

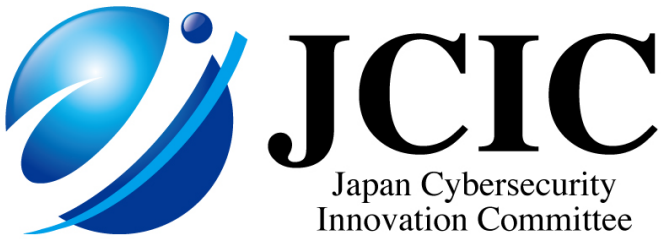


まず、自社の経営戦略におけるサイバーセキュリティの目的や重要性をストーリーで説明する。同社では、「付加価値向上のためオンライン会員を増加させる」という経営戦略を掲げているが、情報盗難が発生すると経営戦略に対する大きな影響となり、会員数増加という戦略実現の障壁になる。

事故が発生した場合の損失額を軽減するためのセキュリティ施策を重点的に実施することで、最大損失額を「141 億円」から「97 億円」までに減らす効果があることをセキュリティ責任者が経営層に示している。また、最大損失額は、JCIC の「サイバーリスクの数値化モデル」を用いて金額換算した。

参考文献

- 公益財団法人 日本生産性本部「新政権への期待と DX に関する緊急アンケート」（2022 年 12 月）, https://www.jpc-net.jp/research/detail/005615.html
- トレンドマイクロ「DX 推進における法人組織のセキュリティ動向調査」（2021 年 11 月）, https://www.trendmicro.com/ja_jp/about/press-release/2021/pr-20211130-01.html
- PwC「Digital Trust Insights レジリエンス指数を高めるために」, https://www.pwc.com/jp/ja/knowledge/thoughtleadership/2020/assets/pdf/resiliency-quotient2002-02.pdf
- FS-ISAC・デロイト「サイバーセキュリティ展望を再構築」, https://www2.deloitte.com/jp/ja/pages/risk/articles/cr/reshaping-the-cybersecurity.html
- ITR「国内 IT 投資動向調査報告書 2021」, https://enterprisezine.jp/article/detail/12656
- カーネギーメロン大学「Structuring the Chief Information Security Officer Organization」, https://resources.sei.cmu.edu/asset_files/TechnicalNote/2015_004_001_446198.pdf



[本調査に関する照会先]

主任研究員　上杉謙二　uesugi@j-cic.com