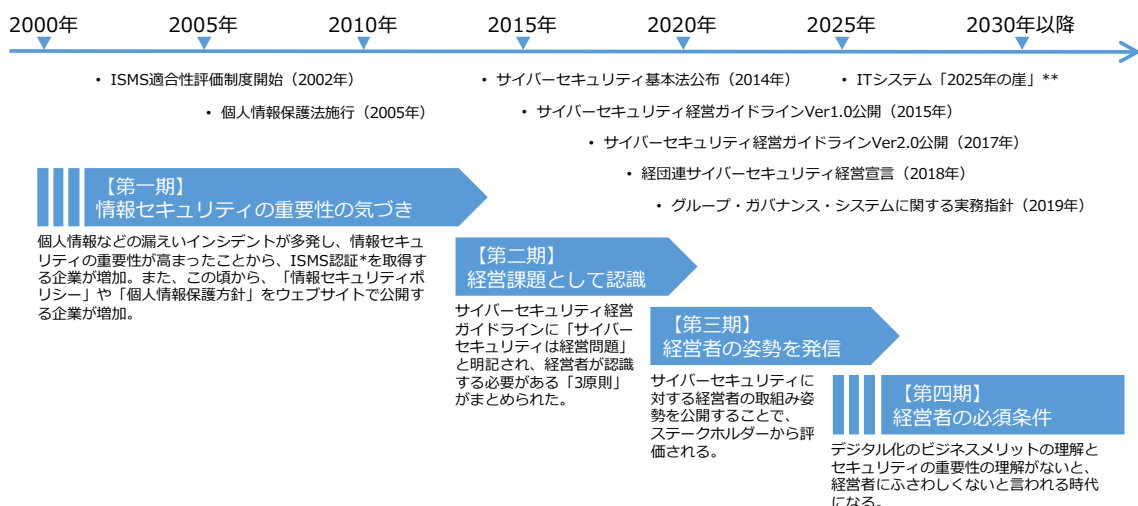


サイバーセキュリティ情報公開のポイント ～経営者の取組み姿勢が重要～

【要旨】

- 日本において「セキュリティ¹は経営問題」と言われて久しいが、多くの経営者に浸透しているとは言えない。新型コロナウイルスの影響により政府などからテレワークが要請された際、経営者は自社にとって何が合理的なセキュリティ対策なのかを正しく判断できただろうか。また、昨今のセキュリティ事象事例が示す通り、経営者のセキュリティの取組み不足により、企業経営を脅かす事態は後を絶たない。今後、ビジネスにおけるデジタル技術への依存度が増すにつれ、企業のセキュリティ対策も強化が不可欠になってくる。
- 「経営」と「セキュリティ」を結びつけるためには、国や団体が啓発を行い、現場から経営者に対してセキュリティ対策の必要性を訴えるだけでは十分ではない。経営者は自社のリスクを数値化することなどでセキュリティの重要性の理解を深め²、株主・顧客・取引先などのステークホルダーに対して、自ら率先してセキュリティへの取組み姿勢や体制などを情報公開していく必要がある。
- ステークホルダーに経営者の姿勢や平時のセキュリティ対策を公開することは、どのような意味があるだろうか。JCIC が公開討論やインタビュー調査を実施したところ、企業の情報公開のメリットは以下の通りであった。
 - 「顧客や取引先」に対して、安心して製品やサービスを利用してもらうことができる
 - 「株主」に対して、リスクマネジメントが合理的に機能していることの説明責任を果たすことができる
 - 「機関投資家」に対して、企業格付けなどにプラスの影響を与えることができる
- 2025 年以降、財務や労務の重要性理解と同様に、「デジタル化のビジネスメリットの理解」と「セキュリティの重要性の理解」がなければ経営者にふさわしくないとされる時代になるであろう（図表 1 の第四期）。このような動向を見据え、今から経営者がセキュリティ意識を高め、その取組み姿勢をステークホルダーへ発信することで競争優位性を確立し、先行者利益を得られるはずだ（図表 1 の第三期）。



* ISMS認証：情報セキュリティマネジメントシステム（日本は6,000件の登録数があり、中国に次いで世界2位。2019年時点）
 **2025年の崖：経済産業省DXレポートによると、2025年までに既存システムの複雑化を解消しなければ、データ流出リスクが高まるとした。

図表 1 日本における「経営」と「セキュリティ」の過去動向と将来予測

¹ 本レポートの「セキュリティ」は、情報セキュリティ、サイバーセキュリティ、個人情報保護などの情報保護活動を意味する。

² JCIC レポート「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」参照

1. はじめに

JCIC では、「経営」と「セキュリティ」を結びつけるための研究や議論を重ねてきた。本レポートは、企業の平時のセキュリティ対策の情報公開に焦点を当て、なぜ広く発信する必要があるのか、誰に/どのように/どこまで公開すべきか、発信する際の留意点などをまとめ、今後の論点を提示するものである。なお、取引先に対する秘密保持契約書（NDA）ベースの機密情報開示³、セキュリティ事故発生時の当局通知や情報開示などは本レポートの範囲外とし、平時のセキュリティ対策の公開を対象とした。

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/広報・IR/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。ぜひ、このレポートを企業セキュリティの情報公開のヒントとして活用していただきたい。

2. 日本企業の平時のセキュリティ情報公開動向

業種 (全体社数)	有価証券報告書		コーポレートガバナンス報告書	
	記載社数	記載率	記載社数	記載率
保険業 (n=9)	9	100%	7	78%
銀行業 (n=82)	82	100%	27	33%
空運業 (n=3)	3	100%	1	33%
その他金融業 (n=27)	26	96%	21	78%
証券・商品先物取引業 (n=24)	23	96%	11	46%
情報・通信業 (n=210)	195	93%	130	62%
サービス業 (n=210)	179	85%	100	48%
小売業 (n=198)	158	80%	80	40%
不動産業 (n=71)	52	73%	26	37%
陸運業 (n=43)	31	72%	19	44%
電気・ガス業 (n=22)	14	64%	9	41%
倉庫・運輸関連業 (n=24)	15	63%	9	38%
その他製品 (n=54)	33	61%	30	56%
食料品 (n=82)	46	56%	35	43%
海運業 (n=8)	4	50%	5	63%
電気機器 (n=159)	72	45%	68	43%
石油・石炭製品 (n=9)	4	44%	3	33%
医薬品 (n=39)	16	41%	22	56%
繊維製品 (n=41)	17	41%	11	27%
卸売業 (n=176)	70	40%	77	44%
輸送用機器 (n=62)	24	39%	22	35%
精密機器 (n=32)	11	34%	13	41%
鉱業 (n=6)	2	33%	2	33%
機械 (n=141)	44	31%	50	35%
水産・農林業 (n=7)	2	29%	4	57%
建設業 (n=101)	29	29%	37	37%
非鉄金属 (n=24)	7	29%	8	33%
ゴム製品 (n=11)	3	27%	3	27%
化学 (n=146)	38	26%	51	35%
金属製品 (n=42)	9	21%	13	31%
ガラス・土石製品 (n=33)	7	21%	9	27%
鉄鋼 (n=31)	5	16%	11	35%
パルプ・紙 (n=12)	1	8%	4	33%
合計 (n=2,139)	1,231	58%	918	43%

多くの日本企業が、平時のセキュリティの取り組みやリスク認識を情報公開している。JCIC が東証一部上場企業の制度公開報告書を調査したところ、有価証券報告書でセキュリティに関するリスク事項を公開している企業は 58%、コーポレートガバナンス報告書では 43%であった。

業種別に見ると、保険・銀行などの金融業、空輸業、情報・通信業、サービス業、小売業などでセキュリティに関する記載率が高いことが分かる。一方、記載率が低い業界は、製造、化学、建設業などであった。

しかしながら、掲載されている内容は形式的なものも多く、誰に何を伝えたいのかが明確でない記載もあった。また、個社毎に記載のばらつきがあり、客観的に比較や評価することが難しい。

図表 2 制度公開報告書のセキュリティ関連記載状況⁴

³ 本レポートでは、「開示」は特定の組織にのみ情報を伝えること、「公開」は広く一般に情報を発信することとした。

⁴ 検索条件：〔上場市場：東証一部〕、〔キーワード：「システムリスク OR 情報セキュリティ OR サイバーセキュリティ OR 個人情報 OR プライバシー OR サイバー攻撃 OR 不正アクセス」を含む〕、〔日付/期間：決算日 2018/11/01～2019/10/31〕

3. 情報公開のメリット

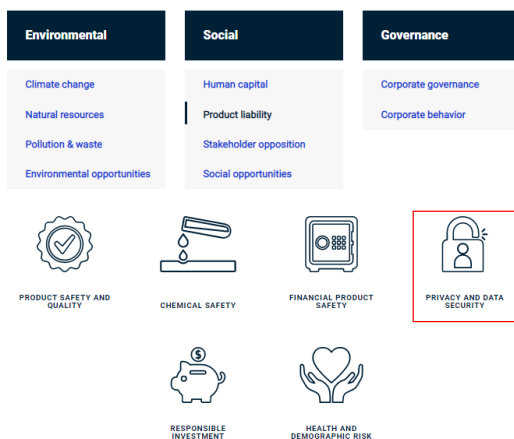
なぜ、企業は平時のセキュリティ対策について広く発信する必要があるのだろうか。また、誰に対して、どこまで公表すべきであろうか。JCIC は、会員企業とのワーキンググループ、国際シンポジウムでの公開討論⁵、個別インタビューにより情報公開のメリットに関する調査を実施した。

情報公開のメリット		対象者
①	安心して製品やサービスを利用してもらえることができる	顧客や取引先
②	リスクマネジメントが合理的に機能していることの説明責任を果たすことができる	株主
③	非財務情報の開示により格付けなどにプラスの影響を与えることができる	機関投資家

図表 3 企業のセキュリティ情報公開のメリット

まず、1 つ目のメリットは、顧客や取引先に対して、安心して製品やサービスを利用してもらえることである。ネットショッピングなどのインターネットを経由して個人情報を取り扱うサービスはもちろんのこと、小売業や交通業などでもデジタル技術を使った行動分析が行われているためセキュリティの重要性は高まっている。また、企業間取引においても、機密情報を安心して共有できる相手であることを示すことは、ビジネスにおける信頼関係を構築するために必要である。

2 つ目の株主に対しては、リスクマネジメントが合理的に機能していることの説明責任を果たすことが挙げられる。企業経営の持続的成長が株主から求められる昨今、リスクマネジメントやコーポレートガバナンスの一環として、セキュリティリスクに対する経営者の考え、守るべき資産に対する対策の合理性を公開することは、経営者の説明責任を果たすことにつながる。



図表 4 ESG 評価指標

3 つ目のメリットは、セキュリティ対策といった非財務情報の公開によって、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挙げられる。例えば、MSCI（モルガン・スタンレー・キャピタル・インターナショナル）の ESG 指数では、「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いる。ESG 機関投資家は、公開情報の調査、アンケートやインタビューから「プライバシー & データセキュリティ」を 10 段階で評価し、全体の ESG 評価に反映する。企業からの情報が得られない場合、評価は最低スコアになることもあるという。

（コラム「ESG 指数の考え方」を参照）

上記以外のメリットとしては、他社の取組みと比較した結果を自社の活動に活かせること、経営者の対外メッセージを通じて自社の社員の間でセキュリティの重要度合いが共通化できること、メディアを通じて一般消費者に対してブランドイメージを向上できることなどの意見も挙がった。

⁵ サイバーセキュリティ国際シンポジウム（慶應義塾大学三田キャンパス）レポート（2019/12/12）, <https://www.jcic.com/news/event20191212-2.html>

4. 情報公開の留意事項

一方、JCIC の調査では、企業セキュリティの情報公開に関する懸念材料として、情報を公開しすぎるとサイバー攻撃の増加につながる、事業戦略を無視したセキュリティ強度の競争につながる、といった懸念点が挙げた。

【企業のセキュリティ情報公開に関する主な留意事項】

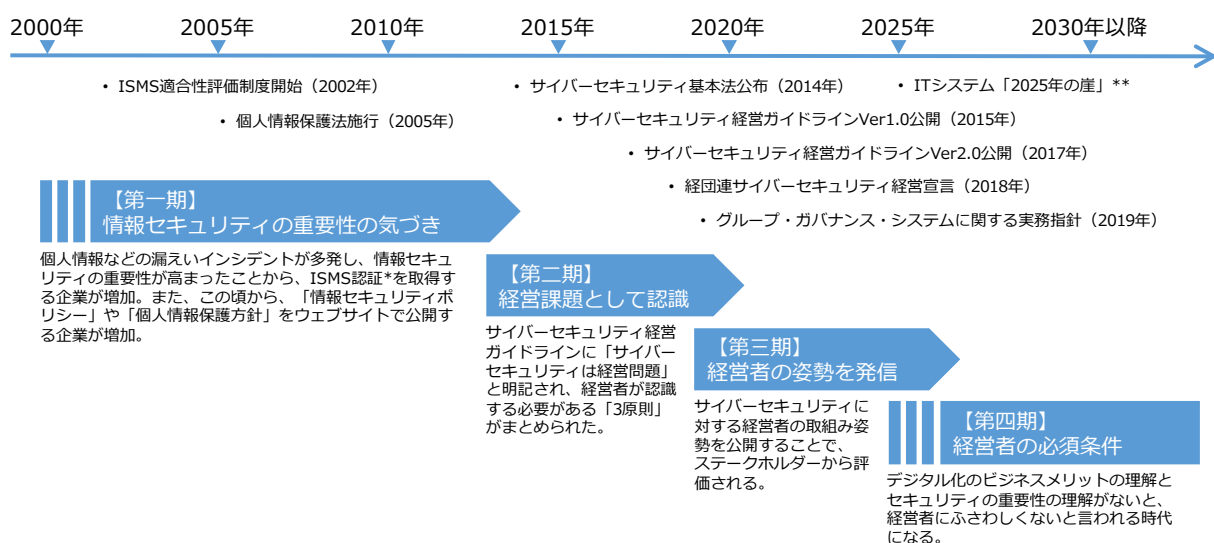
- **サイバー攻撃のヒントになるような情報などは公開する必要はなく、公開/非公開の線引きが必要**
 - － 技術的な対策手法などを公開する場合、サイバー攻撃のヒントになる恐れがある。具体的なセキュリティ対策手法は一般に公開する必要はなく、経営者の姿勢やリスク認識、管理体制を公開すべきである。
- **どれだけセキュリティが厳しいかの競争にならないようにする必要がある**
 - － 企業毎に事業戦略が異なり、デジタル技術への依存度が異なる。そのため、セキュリティ強度が強ければ良いというわけではない。自社の事業戦略やデジタル化に沿って、セキュリティ強度のバランスを取る必要があり、その考え方を公開すべきである。
- **情報公開することは手段であり、目的化しないこと**
 - － 前述の通り、企業のセキュリティ情報公開は、ステークホルダーへの説明責任を果たすことが目的の一つである。情報を公開すること自体を目的化しないよう心掛ける必要がある。

5. 今後の情報公開の在り方 ～経営者の取組み姿勢を示すべき～

日本における「経営」と「セキュリティ」の動向を整理したものを図表 1 に示す。

【第一期】情報セキュリティの重要性の気づき

1990 年代から、オフィスで 1 人 1 台のパソコンが支給され、パソコンの中で機密情報や個人情報を取り扱うようになった。2000 年代には、企業の個人情報漏えい事故が多発し、情報セキュリティの必要性が高まったことから、ISMS 認証を取得する企業が増加。個人情報保護法の施行もセキュリティ機運を高めた。各社で「情報セキュリティポリシー」や「個人情報保護方針」を策定し、ISMS や P マークを取得する企業が増えた時期を【第一期】情報セキュリティの重要性の気づきとした。



* ISMS認証：情報セキュリティマネジメントシステム（日本は6,000件の登録数があり、中国に次いで世界2位。2019年時点）

**2025年の崖：経済産業省DXレポートによると、2025年までに既存システムの複雑化を解消しなければ、データ流出リスクが高まるとした。

図表 1 日本における「経営」と「セキュリティ」の過去動向と将来予測（再掲）

【第二期】経営課題として認識

「セキュリティは経営問題」という考え方が徐々に浸透した時期を「【第二期】経営課題として認識」とした。特に、経済産業省と独立行政法人情報処理推進機構（IPA）が 2015 年に公開したサイバーセキュリティ経営ガイドラインは多くの企業に影響を与え、ガイドライン発行 1 年後の利用率は 54.8%となった⁶。また、2018 年には経団連が「サイバーセキュリティ経営宣言」を呼びかけ、経営方針の策定と意思表明を促進した。2019 年には、経済産業省が「グループ・ガバナンス・システムに関する実務指針」を発行し、親会社の取締役会レベルでセキュリティ対策の在り方について検討されるべきであると明記された。

【第三期】経営者の姿勢を発信

JCIC では、2020 年以降は経営者が積極的にセキュリティへの取組み姿勢を公開する新たな時代に入ると見ている（この時代を「【第三期】経営者の姿勢を発信」とした）。今までは、国や団体が「セキュリティは経営問題」という啓発を行ってきたが、全ての経営者が理解し実践しているわけではなかった。これからは、株主・顧客・取引先などのステークホルダーに対して、経営者の姿勢や管理体制を公開することで企業が評価される時代になるであろう。その理由としては、2020 年の世界経済フォーラムの年次総会（ダボス会議）でもテーマになったように、企業は収益至上主義を見直し、ESG（環境・社会・企業統治）への対応が求められていることが挙げられる。ESG 活動に積極的な経営者が、セキュリティ活動を含めた取組みを広く発信することにより、評価がプラスされることが期待できる。また、この時代は、経営者のビジネススキル移行期とも捉えることができる。現在、全ての経営者が財務や労務の重要性を理解しているように、今後はデジタル化のビジネスメリットの理解とセキュリティの重要性の理解がなければ経営者にふさわしくないとされる時代になるであろう。今から経営者がセキュリティ意識を高め、その取組み姿勢をステークホルダーへ発信することで競争優位性を確立し、先行者利益を得られるはずだ。

【第四期】経営者の必須条件

将来に目を向けると、デジタル技術をビジネスに利活用するデジタル・トランスフォーメーション（DX）を推進し、「2025 年の崖」と呼ばれる既存システムの複雑化を解消する現在のリーダークラスが経営を担うであろう。この頃の経営者は、新入社員の頃から 1 人 1 台のパソコンが支給された世代に代わるため、デジタル化のメリットやセキュリティリスクを自分事として捉えやすく、「セキュリティは経営問題」という認識が全業界で浸透しやすくなっているはずだ。この時代を「【第四期】経営者の必須条件」とした。

6. 今後の論点

これまで、企業が平時のセキュリティ対策として、経営者の取組み姿勢を広く発信する必要性について述べてきた。今後の論点として、誰に/どのように/どこまで公開すべきかについて、議論を重ねる必要がある。

【企業のセキュリティ情報公開に関する今後の論点】

- 伝えたい対象は誰か
経営者のセキュリティへの取組み姿勢を伝えたい対象を整理する必要がある。
 - － 顧客：安心して製品やサービスを利用してもらうため
 - － 取引先：ビジネスにおける信頼関係を構築するため

⁶ IPA「企業の CISO や CSIRT に関する実態調査 2017」, <https://www.ipa.go.jp/files/000058850.pdf>

- 株主：リスクマネジメントが合理的に機能していることの説明責任を果たすため
 - 機関投資家や証券会社：非財務情報の公開により企業価値を正しく理解してもらうため
 - 社員：セキュリティ対策の立ち位置（重要度合い）を共通化するため
 - メディア：一般消費者へのブランドイメージ向上のため
- どのように伝えるか
伝えたい対象に最も効果的かつ効率的な伝達方法を検討する必要がある。
 - 有価証券報告書
 - コーポレートガバナンス報告書
 - CSR 報告書
 - サステナビリティ報告書
 - 統合報告書
 - アニュアルレポート
 - 情報セキュリティ報告書
 - 自社ウェブサイト、SNS、広告
 - どこまで公開すべきか
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、公開/非公開の線引きが必要
 - 経営者のセキュリティへの取組み姿勢
 - 経営者のリスク認識
 - 守るべき情報資産
 - セキュリティ対策の合理性
 - セキュリティ管理体制（責任者、組織体制、子会社を含むガバナンス）

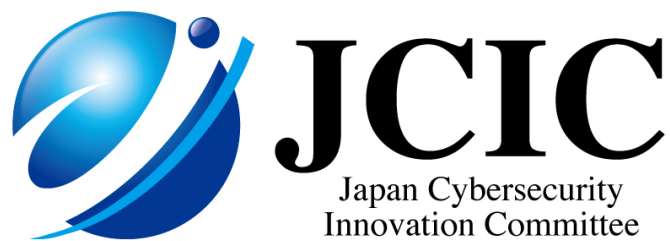
7. まとめ

「経営」と「セキュリティ」を結びつけるためには、国や団体が啓発を行い、現場から経営者に対してセキュリティ対策の必要性を訴えるだけでは十分ではない。経営者は自ら率先して、株主・顧客・取引先などのステークホルダーに対して、セキュリティへの取組み姿勢や体制などを情報公開していく必要がある。そこで、本レポートでは、企業の平時のセキュリティ対策の情報公開に焦点を当て、広く発信するメリットや今後の論点を提示した。

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。自社の事業戦略やデジタル技術の利活用方針を説明する中で、リスクをどのように経営者が捉えているのかを説明する必要がある。また、守るべき重要情報資産を定義し、リスクを低減するための合理的なセキュリティ対策を説明し、経営者が適切だと考える攻めと守りのバランスを示すべきである。このような考え方を社内外に示すことで、経営者はセキュリティをストーリーとして語るできるようになり、ステークホルダーへの説明責任に繋がる。

今後、経営者のセキュリティ取組み姿勢が広く公開されていくために、誰に/どのように/どこまで公開すべきかについて、議論を重ねる必要がある。

以 上



[本調査に関する照会先]

主任研究員 上杉謙二 uesugi@j-cic.com

客員研究員 山中樹八 yamanaka@j-cic.com

－ ご利用に際して －

- 本資料は、JCIC の会員の協力により、作成しております。本資料は、作成時点での信頼できるとされる各種データに基づいて作成されていますが、JCIC はその正確性、完全性を保証するものではありません。
- 本資料は著作権法により保護されており、これに係る一切の権利は特に記載のない限り JCIC に帰属します。引用する際は、必ず「出典：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（JCIC）」と明記してください。
- [お問い合わせ先] info@j-cic.com