セキュリティマインドを持った企業経営ワーキンググループ

報告書

～事業継続と価値創出を支えるサイバーセキュリティ～

平成 30 年 5 月 31 日

セキュリティマインドを持った企業経営ワーキンググループ

目次

1　はじめに

（1）経緯

これまで、内閣サイバーセキュリティセンター（NISC）では、「サイバーセキュリティ戦略」（平成 27 年 9 月閣議決定）を踏まえ、関係省庁との連携の下、セキュリティ対策は「費用」ではなく「投資」であるとの認識を醸成するための経営層の意識改革や経営層のリーダーシップの下での組織能力の向上など、セキュリティマインドを持った企業経営を推進してきている。

具体的には、同戦略を踏まえ、NISC では、経営層に期待される認識等を示した「企業経営のためのサイバーセキュリティの考え方」（平成 28 年 8 月）を策定した。また、「サイバーセキュリティ人材育成プログラム」（平成 29 年 4 月、サイバーセキュリティ戦略本部決定）においては、本ワーキンググループを通じ、産業界と連携しつつ、経営層のサイバーセキュリティに関する認識や課題の把握と、その解決に向けた取組の検討を行うことが示された。

さらに、サイバーセキュリティ戦略本部が決定した「サイバーセキュリティ戦略中間レビュー」（平成 29 年 7 月決定）においては、経営層の意識改革を促すための取組や、中小企業のセキュリティを効率的に高めるための方策の検討・取組を進めていくことが示された。

こうした経緯を踏まえ、昨年 10 月、今夏に予定されている次期の「サイバーセキュリティ戦略」の策定を見据え、企業経営とサイバーセキュリティに関する現状や関連する官民の取組、諸外国の動向を把握するとともに、経営層の意識改革を促進するための方策や中小企業のセキュリティ対策、産学官の取組の方向性等について検討を行うとともに、「企業経営のためのサイバーセキュリティの考え方」の内容を充実するため、本ワーキンググループでの検討を開始した。

（2）本報告書の趣旨・位置づけ

本報告書は、本ワーキンググループで 3 回（平成 29 年 10 月、平成 30 年 2 月、平成 30 年 4 月）にわたり、以下の 5 つの内容を中心に検討を行った内容を取りまとめたものである。

① 「企業経営のためのサイバーセキュリティの考え方」（平成 28 年 8 月）策定後の企業経営に関するサイバーセキュリティを取り巻く動向（経営者の意識、情報開示の状況、米国における動向等）やこれまでの官民の取組を把握すること

② リスクマネジメントの一つの要素としてサイバーセキュリティを位置付け、その確保のために組織全体で進めるべき取組について、各企業の事業規模・内容や IT 利活用の度合い、サイバーセキュリティに対する認識の違いなどを意識しつつ、検討すること

③ サイバーセキュリティに関する経営層の意識改革促進の方策を検討すること
④ 中小企業におけるセキュリティ確保の方策、とりわけセキュアなクラウドの利用について検討すること
⑤ セキュリティマインドを持った企業経営を推進できるような産学官連携による取組の方向性について検討すること

なお、議論の過程においては、企業法制を反映した内容の整理をすべきとの意見もあったが、企業の機関設計や機能分担は多様で変化しつつあり、サイバーセキュリティとの関連づけはなお考察を要することから、本報告書の記載においては、現時点での企業経営におけるサイバーセキュリティの一般的な内容について論じるものとする。

また、本報告書で取りまとめた内容は、サイバーセキュリティと経営の問題に関する現状と課題及び今後の取組についての認識を、広く、経営層を含め共有するとともに、本報告書の内容を踏まえ、「次期サイバーセキュリティ戦略」の関係する部分についての検討を深めていくこととする。

２　企業経営とサイバーセキュリティの現状

(１) 経営層の意識・関与、組織体制

ａ．サイバーセキュリティ対策を進めるためには、経営層の意識改革が重要

サイバーセキュリティ対策は、それ自体が利益を生まない一方で、サイバー攻撃の被害が発生したときに初めて対策が不十分であったことに対する損失が明確になる。このため、自社においてサイバーセキュリティ対策の必要性について明確な位置付けがなされていないと取組が進みにくい。実際に、企業がサイバーセキュリティ対策を実施するきっかけの上位には、経営層のトップダウンによる指示、自社・他社のインシデントの発生が挙げられている。

経営層のトップダウンによる指示はもちろんのこと、インシデントの発生は、金銭的損害だけでなく企業の信用に多大な影響を与える可能性があり、経営層が問題意識をもつ契機になることに鑑みれば、サイバーセキュリティ対策を進めるためには、経営層のサイバーセキュリティに対する意識向上や経営層の関与が不可欠である。

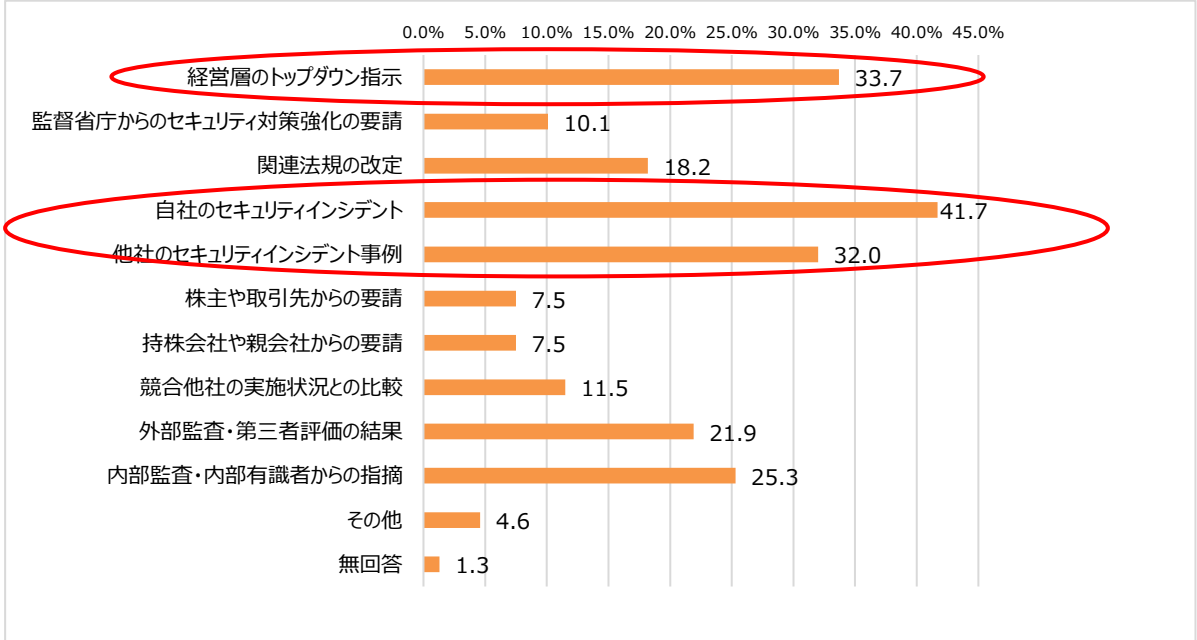


図１：情報セキュリティ対策の実施にいたった理由

出典：企業における情報セキュリティ実態調査 2017（NRI セキュアテクノロジーズ）

ｂ．業種によって経営層の関与度合いは異なる

経営層の情報セキュリティに対する関与の度合いは業種によって大きく異なる。具体的には、金融業界は突出して関与の度合いが高い一方、金融以外の業種は概ね６～７割が

IT 部門などの担当部門任せか、経営幹部の話題にならないものとなっている。

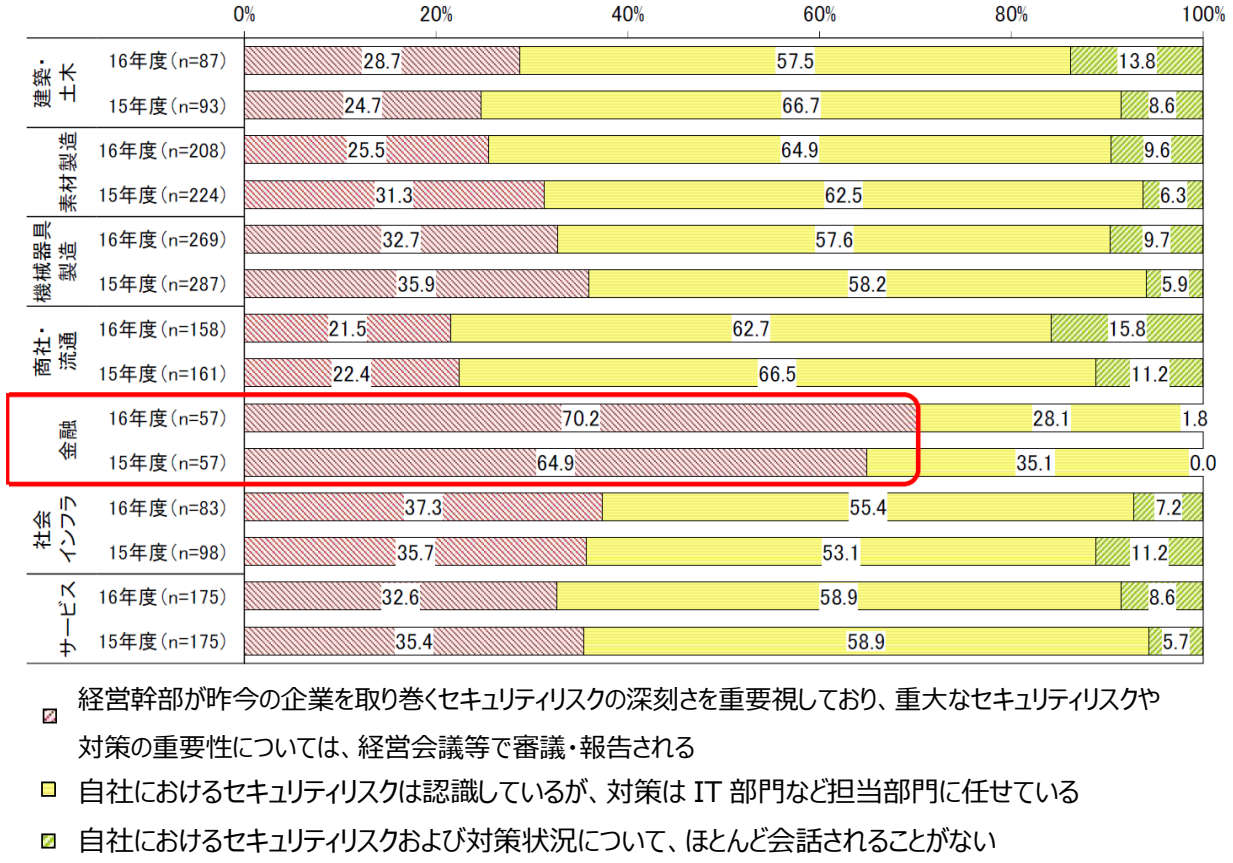


図 2：業種グループ別　経営幹部の情報セキュリティへの関与度合い　※n：母数

出典：企業 IT 動向調査 2017（JUAS）

c．セキュリティを将来に向けた「投資」と捉えている企業は、経営層が積極的に関与

NISC が日経 225 の企業を対象に実施した調査（「平成 28 年度企業のサイバーセキュリティ対策に関する調査」）によれば、サイバーセキュリティを、将来に向けた積極的な投資と捉えている、あるいは、自社のブランド価値として捉えている企業はいまだ少数派であり、一般的には、社会的責任や自社のリスク管理の一環として捉えられている。そのような状況において、サイバーセキュリティの取組を将来に向けた積極的な投資や自社のブランド価値として位置付けている企業は、そのように位置付けていない企業と比較して、経営層が日ごろから特に重要な問題としてサイバーセキュリティに取り組んでいる割合が多いことが明らかになっている。

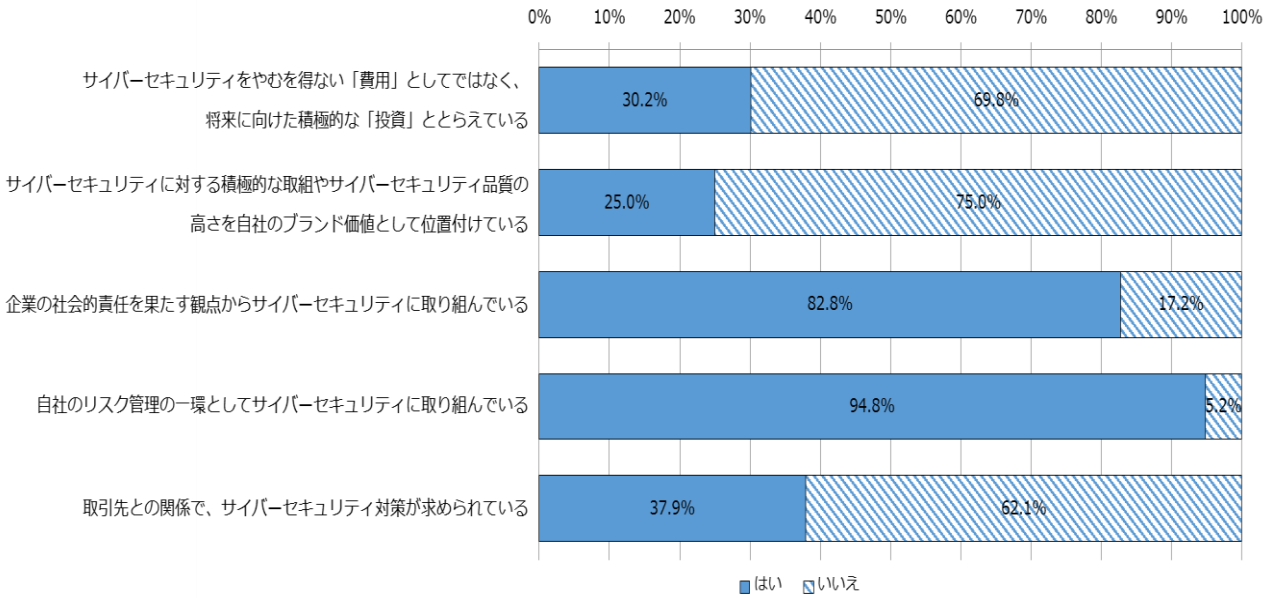


図 3：企業がサイバーセキュリティに取り組む姿勢

出典：平成 28 年度企業のサイバーセキュリティ対策に関する調査報告書

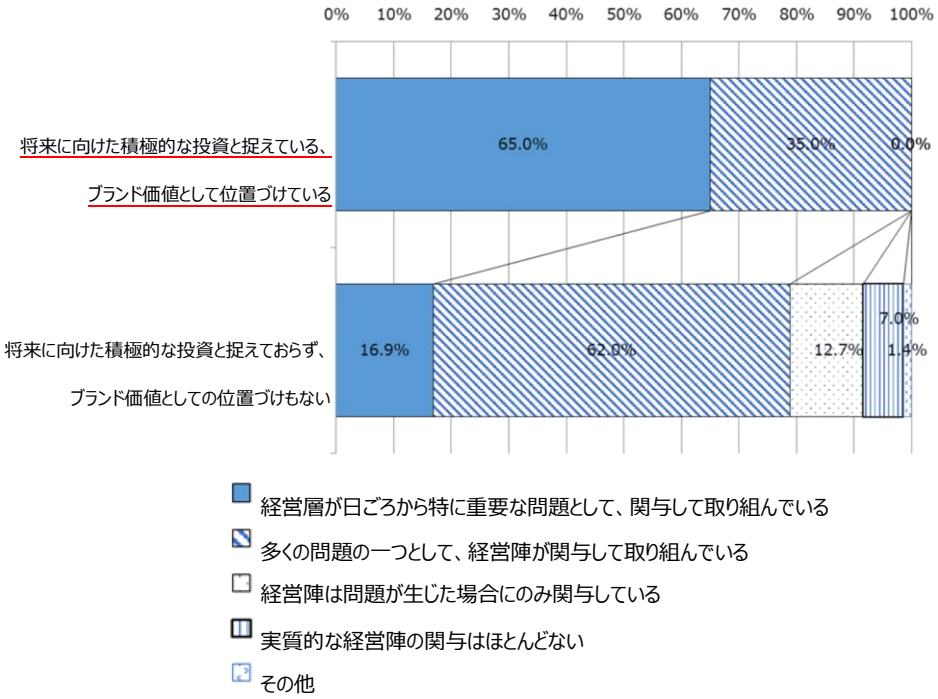


図 4：サイバーセキュリティの取組と経営層の関与

出典：平成 28 年度企業のサイバーセキュリティ対策に関する調査報告書

(2) 情報開示・発信

投資家への情報開示等を目的として作成される各種報告書（有価証券報告書、コーポレートガバナンス報告書、CSR 報告書など）は、企業の経営層によってその内容が決議されることが一般的であり、当該企業の経営層が自社のリスクをどのように認識し、対応をしているのかについて示唆を与えるものである。

ａ．有価証券報告書における記載は増加、ただし業界による差異が大きい

有価証券報告書の「事業等のリスク」において、サイバーセキュリティに関する記載を行っている企業は増加傾向にある。NISC が実施した調査では、平成 21 年の記載率が 52.6%に対し、平成 27 年には 67.1%（15%の伸び）となっている。

ただし、業界による記載率の差は大きく、「金融」は全ての企業が記載しているのに対し、「素材」（化学、鉄鋼、繊維等）は、約 4 割にとどまっている。

また、有価証券報告書の具体的な記載内容についても、企業によって差異がある。具体的には、「事業等リスク」において一般的な記載が見られる場合、「事業等リスク」のみならず、経営環境や内部統制に関連してセキュリティを位置づけている場合、さらには、リスクの記載や事業・財務状況への影響、過去に発生した具体的なインシデントへの言及など多角的な視点でサイバーセキュリティリスクを捉えている場合などがある。

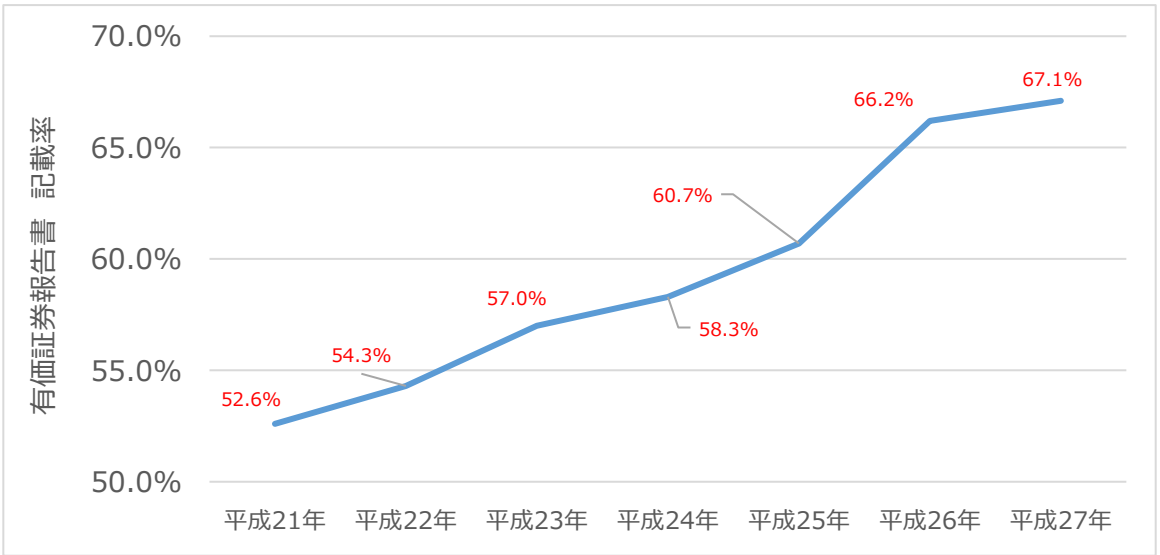


図 5：サイバーセキュリティに関して有価証券報告書に記載をしている企業の割合の推移

出典：平成 28 年度 企業のサイバーセキュリティ対策に関する調査

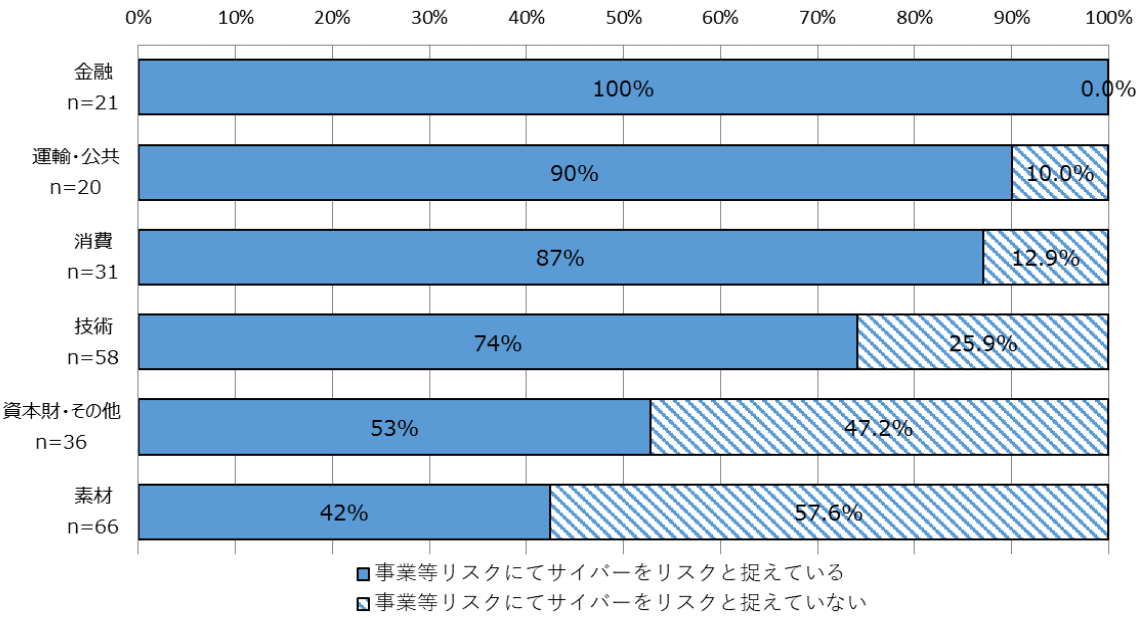


図 6：分野別サイバーセキュリティに関する記載状況

出典：平成 28 年度 企業のサイバーセキュリティ対策に関する調査

b．コーポレートガバナンス報告書よりも CSR 報告書に記載している企業が多い

NISC が実施した調査では、コーポレートガバナンス報告書にサイバーセキュリティを記載している企業は、当該報告書を作成している企業の約 2 割に留まっており、CSR 報告書に記載している企業の方が多い（約 6 割）。これは、サイバーセキュリティをコーポレートガバナンスの一環として捉えるよりも、社会的責任の一環として捉える傾向にあることを示している。

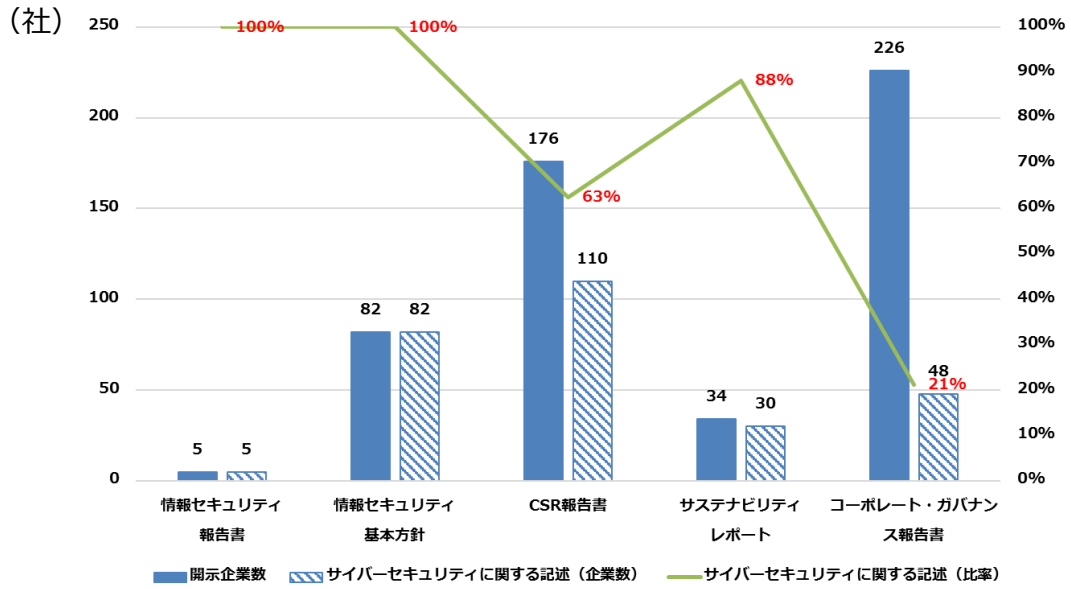


図 7：各種報告書等におけるサイバーセキュリティに関する記載の状況

出典：平成 28 年度　企業のサイバーセキュリティ対策に関する調査

c．多くの企業が、サイバーセキュリティ対策について横並びで足りると考えている

NISC が実施した調査では、7 割を超える企業が、同業種や同規模の企業と同じレベルで情報開示が出来ていれば足りるという意識を持っていることが明らかになっている。

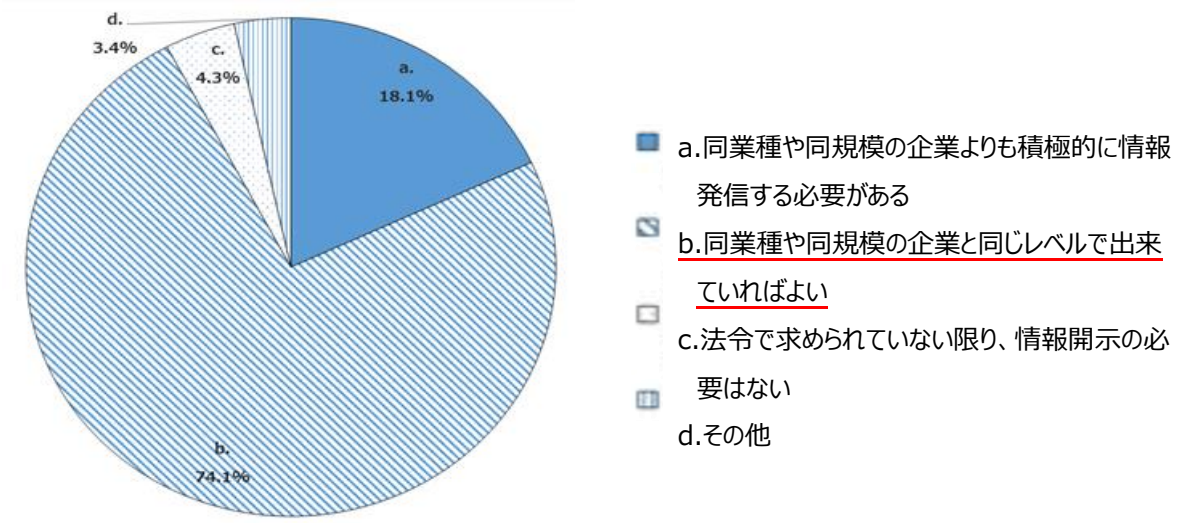


図 8：日経 225 等の企業におけるサイバーセキュリティに関する情報発信の情勢

出典：平成 28 年度　企業のサイバーセキュリティ対策に関する調査

（３）企業の取組の「見える化」

企業のサイバーセキュリティリスクを明確化し、それに対する対策を「見える化」することは、自社の経営層に対し、サイバーセキュリティ対策の強化に向けた意識改革を促すのみならず、投資家等に対して自社の取組を示し、それに対して市場からの評価を得ることで、サイバーセキュリティ対策を進めるための環境づくりにつながるものである。

これまで、企業の取組を見える化するための様々なツールが整備されてきており、それらのツールの活用が進んでいる。

ａ．情報セキュリティマネジメントシステム（ISMS）認証制度

日本情報経済社会推進協会（JIPDEC）が認定した民間の認証組織がISO27001 に基づいて組織の情報資産のセキュリティ管理について適合性評価を実施する仕組みとして広く活用されている。

2002 年以降増加、認証取得組織数は継続的に増加している[1]。

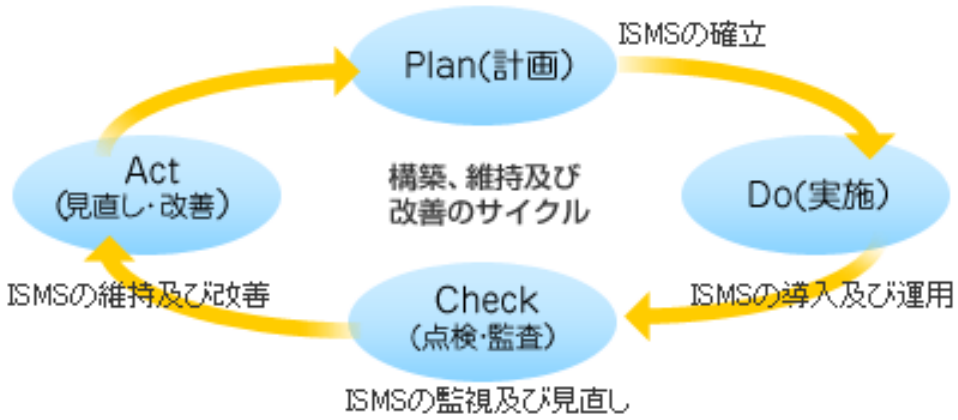


図 9:情報セキュリティマネジメントシステム（ISMS）の概要
出典：IPA 「情報セキュリティマネジメントと PDCA サイクル」
https://www.ipa.go.jp/security/manager/protect/pdca/index.html

ｂ．情報セキュリティ格付制度

株式会社アイ・エス・レーティングが実施。情報セキュリティに関するマネジメントの成熟度や情報漏えい防止策の強度、コンプライアンスへの取組などの視点から審査し、取組のレベルを 17 段階で評価しており[2]、企業の取組の見える化に貢献している。

---

[1] 2018 年４月時点で 5,501 組織が取得。一部の企業、学校、自治体等における調達要件に採用されている。

[2] 2018 年４月時点で 18 組織を対象に格付を行っている。

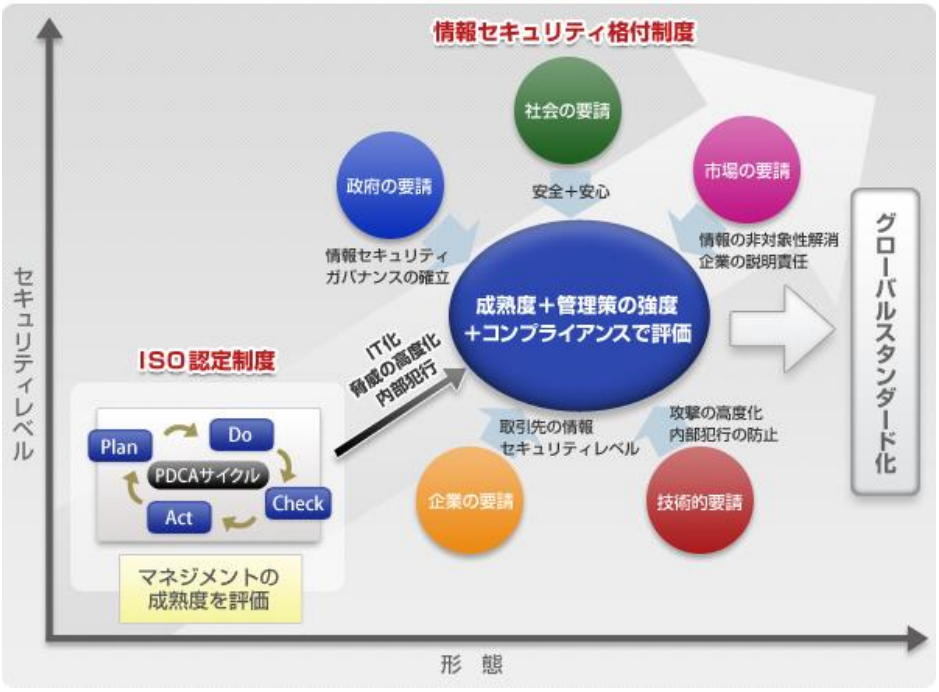


図 10：情報セキュリティ格付について

出典：株式会社アイ・エス・レーティング：http://www.israting.com/background/index.html

c．情報セキュリティ監査制度

経済産業省策定の「情報セキュリティ監査制度」に基づき、日本セキュリティ監査協会が監査人の資格制度を運用している。現在、情報セキュリティ監査は、大企業の約 2 割（N=541 社）が実施しており、同協会がイベント・セミナー等を通じて監査制度の普及に取り組んでいる。

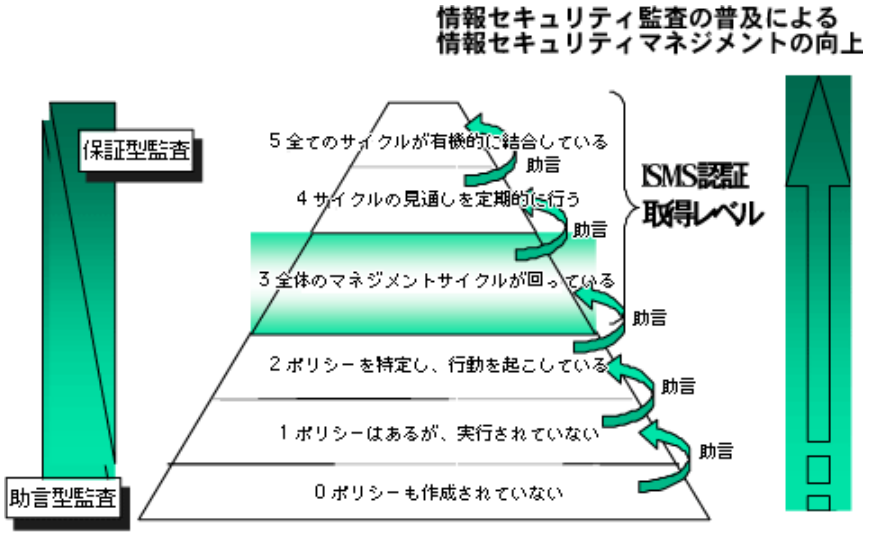


図 11：情報セキュリティ監査制度について

出典：日本セキュリティ監査協会　http://www.jasa.jp/audit/audit.html

(4) サイバーセキュリティ保険の状況

サイバーセキュリティ保険は、セキュリティ事故に起因して発生した損害賠償責任や、事故対応費用（不正アクセス等の発見時の各種対応費用など）を補償するものである。不正アクセスが確定する前の「不正アクセス等のおそれ」が発見された場合においても補償の対象となることが一般的であり、サイバーセキュリティ保険によって早期の事故調査の着手がしやすくなることで、被害の広がりを防ぐ効果もある。また、一般的にサイバーセキュリティ対策を支援するためのサービスが付帯されている。サイバーセキュリティ保険については、近年、企業のサイバーセキュリティリスクのマネジメントツールとして企業において活用が進んできており、我が国のセキュリティ保険市場は成長傾向にあり、2017 年度には 156 億円の市場となっている。

保険料は、売上高を基準に算出され、業種、支払限度額などによって決定されている。また、セキュリティ対策の取組の状況により保険料を割り引くケースもある。なお、支払限度額については、最大で 1 ～10 億円程度が一般的であり、サイバー攻撃によるリスクの広がりに対して十分ではないとの指摘もある。

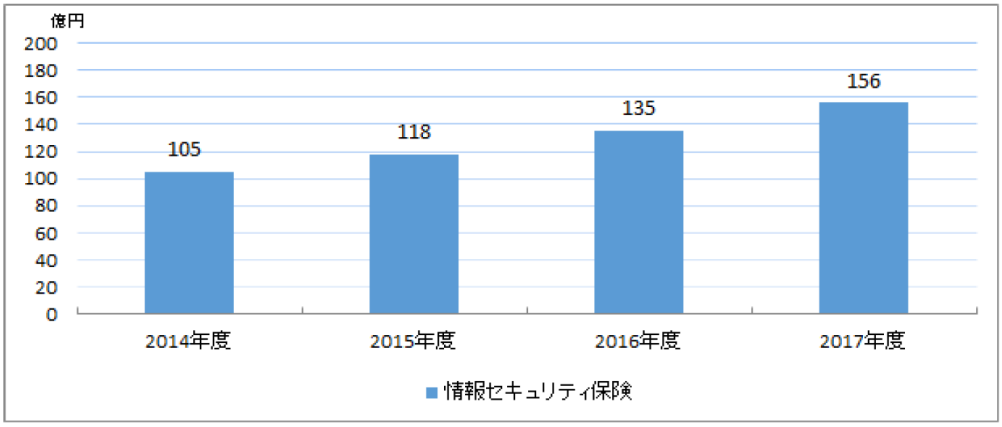


図 12：国内情報セキュリティ保険市場の推移

出典：2016 年度情報セキュリティ市場調査報告書（JNSA）

(5) 米国における取組

米国では次に示すような産学官の連携による経営層の意識改革・啓発、情報開示、見える化等の取組が進められている。

a．全米取締役協会「サイバーリスクハンドブック」[3]（Cyber-Risk Oversight Handbook）

全米取締役協会サイバーリスクハンドブックは、2017 年 1 月に全米取締役協会（NACD）[4]が発行（第 2 版）した指南書であり、取締役がサイバーセキュリティに関して実施すべき 5 つの原則及び具体的な取組を紹介している。主なポイントについては以下のとおり。

１．背景・考え方

①サイバー攻撃の脅威の潜伏と拡大、②つながりの拡大に伴うリスクの増加、③収益性とサイバーセキュリティ対策のバランス

２．５つの原則

（１）全社リスクの一環としてサイバーセキュリティリスクを認識

取締役は、サイバーセキュリティについて、単に IT の問題としてではなく、全社リスク管理の一環として捉え、それを理解し取り組む必要がある。

（２）サイバーセキュリティリスクの法的側面の理解

取締役は、企業を取り巻く環境に応じてサイバーセキュリティリスクがもたらす法的責任について理解しなければならない。

※情報開示に関する要求事項（証券取引委員会（ＳＥＣ）のガイダンス等）の理解を含む。

（３）サイバーセキュリティ専門知識の適切な習得

取締役会は、サイバーセキュリティの専門知識を適切に習得しなければならない。また、サイバーセキュリティ管理について取締役会の議題として定期的に適切な時間をかけて議論を行わなければならない。

（４）サイバーセキュリティ管理フレームワークの整備

取締役は、適切な人材と予算を確保し、セキュリティ管理者が全社にわたるサイバーセキュリティ管理フレームワークを整備できるようにしなければならない。

（５）サイバーセキュリティ対策について具体的な議論を実施

取締役会は、サイバーセキュリティリスクの識別、低減、回避、転嫁（保険）に関して、具体的な方法論や計画について議論を行わなければならない。

---

[3] https://www.nacdonline.org/files/FileDownloads/NACD%20Cyber-Risk%20Oversight%20Handbook%202017.pdf

[4] 全米取締役協会（National Association of Corporate Directors (NACD)）

全米の上場企業、非上場企業の取締役 17,000 人以上の会員が参加する団体。コーポレートガバナンス、内部統制、リスクマネジメント等の助言を行っており、米国 SEC（証券取引委員会）と連携し、企業統治に貢献している。

b．企業金融開示指針 第２号－サイバーセキュリティ（2011 年 10 月発行、2018 年 2 月改訂）[5]

企業金融開示指針は、2011 年 10 月に米国証券取引委員会（Securities and Exchange Commission：SEC）が発行したガイドラインである。同指針においては、企業が、任意で、サイバーセキュリティリスクと事業への影響について示すことを求めている。主なポイントについては以下のとおり。

１．目的
連邦証券法が要求する情報開示（リスク、財務状況、事業内容等）において、サイバーセキュリティリスクとその事業への影響について実質的な情報を開示するための指針（任意）を示すこと。
２．サイバー攻撃により想定される悪影響
・修復費用（例：システム損傷の修復、窃取された情報に対する賠償責任）、是正費用（例：攻撃後、顧客に提供する取引継続のためのインセンティブの支払い）、追加対策費用（例：追加の人員やセキュリティ技術の導入に要する費用）の発生
・窃取された情報の不正使用や、顧客離れ等による収入の損失
・訴訟、風評被害
３．サイバーセキュリティリスクとインシデントに係る開示の内容
サイバーセキュリティリスクとインシデントは、明示的な開示対象ではないが、他のリスク同様、開示の妥当性を検討すべきである。
①リスク要因
リスクを評価し、重要なリスクの性質や、各リスクが企業に与える影響を明記すべき。具体的には、リスクや潜在的なコスト、リスクを伴う機能、インシデントの内容と対処コスト、検知が出来ないインシデントに関連するリスク、保険によるカバー範囲が含まれる。
※サイバーセキュリティを脅かす内容の開示を避けつつ、定型的な内容にならないようにすること。

②財務状況
インシデント（潜在的なものも含む）が財務状況に与える影響、利益減少のおそれへの対処（訴訟対策、防御等）コストの予測が必要。
③事業内容
インシデントが製品、サービスや、競争環境に影響を及ぼす場合、「事業内容」の項目における開示が必要。
④法的手続
インシデントが関連する係争案件がある場合、「法的手続」の項目における開示が必要。
⑤財務諸表
インシデント発生前：インシデントの予防のための費用の考慮が必要。
インシデント発生中・発生後：顧客に提供する取引継続のためのインセンティブ費用、保証・契約違反の損害賠償など偶発的な損失、キャッシュフローの悪化に伴う資産の減損等の考慮が必要。

４．開示管理及び手続の妥当性
情報開示に関する管理及び手続の妥当性についての開示が必要である。

また、2018 年 2 月 21 日、SEC は、当該指針について、重要なサイバーセキュリティのリスクとインシデントを開示する際、インシデント等が企業の事業や財政状態に与える影響を

[5] https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.html

適切に識別できるようにするとともに、企業の取締役・役員及びその他の企業内部関係者等、重要な非公開情報を知りえる立場の者が有価証券の取引をしないようにするため、①インシデントが発生した際にはタイムリーにユーザと投資家へ報告すること、②インシデント発生時のインサイダー取引防止に努めることの 2 点について、更新を行った。

c．セキュリティ格付に関する取組（全米商工会議所）[6]

セキュリティ格付に関する取組は、2017 年 6 月に全米商工会議所が発行。セキュリティ格付に当たって、評価のための 6 つの原則を紹介している。

公平かつ正確なセキュリティ格付を行う原則（2017 年 6 月 20 日）
（1）策定の目的
セキュリティ格付は、組織のサイバーリスクを評価することにより、リスクに関するコミュニケーションを組織間で行う際に有用である。
業界全体で、①格付の品質と正確性の促進、②報告の公平性の促進、③報告された内容の誤り又は正確性を判断するためのプロセスの整備、④格付の適切な使用と開示のガイドラインの確立、によって格付の価値を高めるべきであり、そのための原則を示すこととする。

（2）評価のための 6 つの原則
①透明性
格付機関は、格付の方法論、評価するデータの種別・出所に関する情報を透明性をもって提供すること
被格付組織は、格付に影響を与えるデータへのアクセスが許可されること
②修正
格付機関は、格付の修正を要求する権利を有し、それに関する紛争解決プロセスを保有すること
③正確性と妥当性
格付は実証的であること。格付機関は、格付手法と過去の実績を検証すること
④ガバナンス
格付機関は、評価方法等を変更する場合、事前に通知方法を提供し、変更による影響を伝えること
⑤独立性
格付機関と被格付組織間の商業契約の有無が格付に影響を与えないこと
被格付組織は、格付機関の顧客かどうかにかかわらず、格付の確認と修正の要求ができること
⑥守秘義務
格付・紛争の過程で格付機関が被格付組織から提供された情報は適切な保護をすること

d. ニューヨーク証券取引所（NYSE）による取組

ニューヨーク証券取引所においては、サイバーセキュリティ侵害の説明責任やサイバー攻撃による影響、CISO に求められる素養などについてのアンケート調査等を通じた調査

[6]https://www.uschamber.com/sites/default/files/principles_for_fair_and_accurate_security_ratings.finallist_1.pdf

（2015 年）、M&A におけるサイバーセキュリティ上の課題、買収の適正評価手続におけるサイバーセキュリティの検討要素等についての調査（2016 年）といったサイバーセキュリティと企業経営に関する調査を実施している。

このほか、経営層向けに、コーポレートガバナンスにおけるサイバーセキュリティについて、ベストプラクティスを含むトレーニングコンテンツの提供などを行っている。

(6) 英国における取組

英国国家サイバーセキュリティセンター（NCSC）は、サイバーセキュリティに関わる用語についての理解を促すため、次に示すような用語集を発表しており、経営層の理解促進においても活用が可能と考えられる。

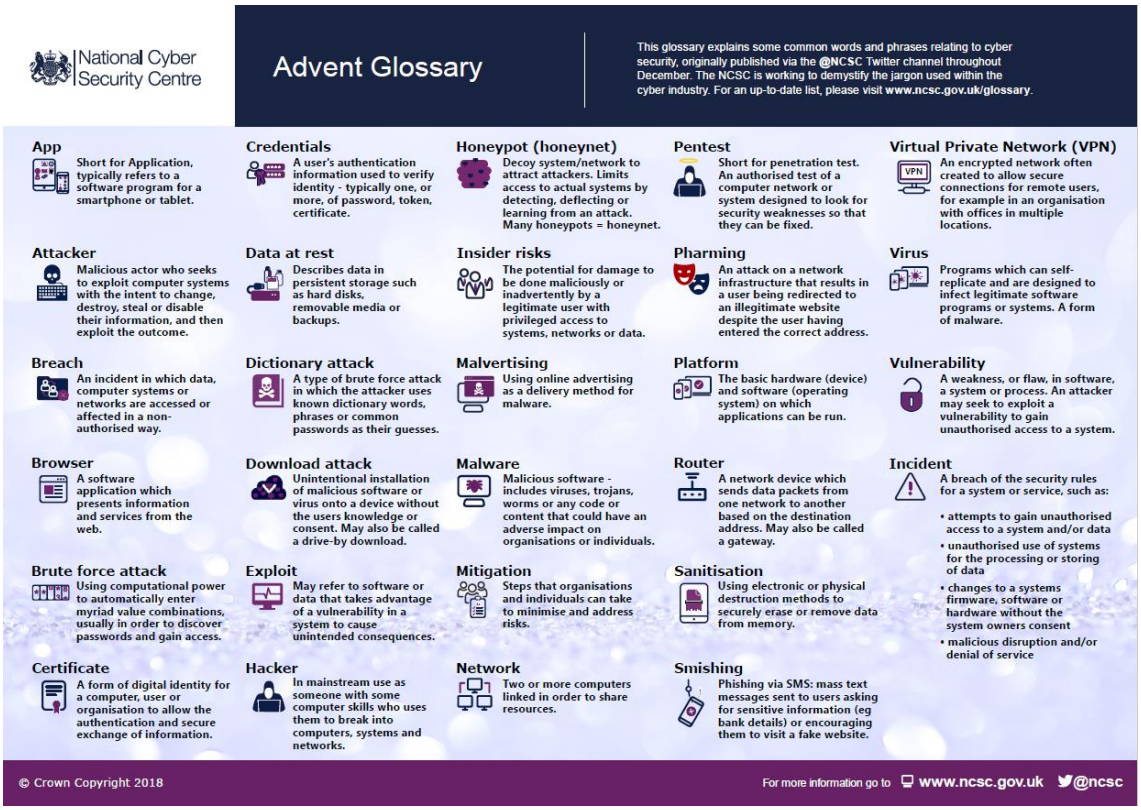


図 13：NCSC 作成のサイバーセキュリティ用語集

出典：https://www.ncsc.gov.uk/information/infographics-ncsc

(7) 経済界の取組

a．日本経済団体連合会による取組

平成 29 年 12 月、一般社団法人日本経済団体連合会は、「Society5.0 実現に向

けたサイバーセキュリティの強化を求める」と題した提言を取りまとめた。[7]その中で、IV.経団連アクションプランにおいては、サイバーセキュリティ対策の強化を Society5.0 の実現に向けた最重要課題と捉え、経営層の理解促進及び広報・周知活動について、自ら次のような取組を進めていくとしている。

１．　経営層の理解促進
・「経団連サイバーセキュリティ経営宣言」を策定
・経営者向けセミナー・研修・合宿を実施

２．　広報・周知活動
・各社のサイバーセキュリティ対策の実態調査の実施および事例集等の公開
・機関誌や説明会・講師派遣等を通じた広報・周知
・政府・各団体におけるイベントへの協力
・国内外のステークホルダーへの情報発信

その後、平成 30 年３月、同連合会においては、経営層としてのリーダーシップを発揮しつつサイバーセキュリティに取り組むこと等を内容とする「経団連サイバーセキュリティ経営宣言[8]」を発表した。

ｂ．日本商工会議所による取組

平成 29 年年６月、日本商工会議所では、図 14 に示すように、地域における商工会議所のサイバーセキュリティ対策を体系化し、日本商工会議所及び各地の商工会議所が実施するサイバーセキュリティ対策支援の取組だけでなく、それ以外の支援情報等を含め、一元的な情報提供を開始した。あわせて、各地の商工会議所自身のサイバーセキュリティ対策を推進すべく支援を行っている。

各地の商工会議所及び日本商工会議所が実施している中小企業向けのサイバーセキュリティ対策について、参考４に取組事例を示す。

[7] 提言の概要については、参考 2 を参照。
[8] 詳細については参考３を参照。

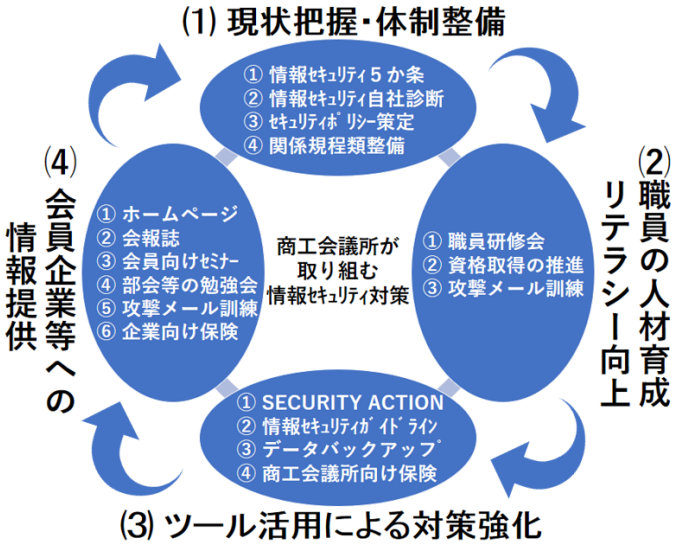


図 14：地域における商工会議所のセキュリティ対策の体系図

※日本商工会議所提供

３　企業経営とサイバーセキュリティをめぐる課題

(1) 基本的考え方

様々なリスクが企業を取り巻く中、企業においては、自らが提供するビジネスやサービスを着実に遂行するために必要となる能力及び資産の確保（任務保証）が最重要の課題である。このような観点から、サイバーセキュリティについても、リスクマネジメントの一環としてとらえ、具体的な対策を講じていくことが重要である。ここでいうリスクマネジメントとは、企業が提供するビジネスやサービスの内容に応じて、リスクを特定・分析・評価し、リスクを許容し得る程度まで低減する対応を指す。

各企業における具体的なサイバーセキュリティ対策については、その企業の業種・業態や規模、ビジネスモデルやその中での IT 利活用の状況等によって、リスクの捉え方や内容、その許容レベルが異なってくるため、一概に規定することはできない。また、サイバー攻撃が、企業にとって新しい脅威の場合、経営層の理解には、時間がかかる可能性もある。

このため、各組織において、それぞれの業種・業態や規模等の状況に応じて、自らのビジネスにおけるサイバーセキュリティの位置付けを可能な限り明確にし、経営層にとって他のリスク要因と同様に、サイバーセキュリティのリスクを「想定内」のリスクにしていくための試行錯誤を行いつつ、自然な形で組織体制やガバナンス等のメカニズムに浸透していくようにすることが重要であり、産学官が連携してそのための環境整備を進める必要がある。

このような観点から、企業の社会的責任としてサイバーセキュリティに取り組む必要性を経営層が認識することは当然のことながら、経営層がサイバーセキュリティ対策を継続的に推進するためには、何らかの経営上のインセンティブが付与されることが重要である。その一つの方策として、サイバーセキュリティ対策を経営上の重要課題として取り組んでいることが、市場や出資者といったステークホルダーから正当に評価されるような仕組みが挙げられる。このような仕組みにより、サイバーセキュリティ対策の取組に対して市場からポジティブな評価を得て、さらなるサイバーセキュリティ投資のインセンティブを生み、安全・安心なビジネスの実現によって企業価値が高まっていく好循環を形成することが期待される。

(2) 企業の IT 利活用の形態による取組の方向性

ａ．リスクマネジメントによる事業継続（危機管理）

今や、IT 企業に限らず、いわゆるものづくりの企業や重要インフラを担う企業、小売り等の消費者向けサービスを提供する企業等、大半の企業が、自らの事業や業務を遂行するための基盤として IT を利活用している。そのような場合、当該事業や業務を円滑に実施するために、そのセキュリティを確保することは重要な課題である。例えば、サイバー攻撃は、個人情報、事業にとって重要な知的財産、金融資産等の窃取、システム停止による事業の

中断など、事業の円滑な実施の妨げになるものである。また、サイバー攻撃への備えが不十分であった場合には、取引先に悪影響が及ぶことや、サイバー攻撃の踏み台になることも想定され、サイバー攻撃に対する備えは自社のビジネスを守るのみならず、企業の社会的責任を果たす上で不可欠なものとなっている。このため、企業の経営者においては、企業活動全体に対する様々なリスクマネジメントの事項の一つとして、サイバーセキュリティを意識して取り組み、そのための戦略と具体的対策を策定することが必要である。

また、その際のリスクの想定においては、既に知られた、あるいは発生する確率が高いと思われる一般的な脅威だけでなく、確率的には低いが発生すると事業継続に極めて大きな影響を及ぶことが想定される事象も含めて、その対応への判断が行われることが必要である。

サイバーセキュリティのリスクマネジメントの実践において、経営層は、サイバー攻撃に対する備えの体制を整備するとともに、対策のための枠組み（例えば、PDCA サイクルに関する枠組みの導入）を組織に組み込み、着実に実施されるよう指示・監督をすることが求められる。これらの体制構築や枠組みの選択においては、その企業の事業や業務手順に合ったものを採用できるよう、自由度を持たせる形にしておくことが必要である。

その上で、リスクマネジメントを実施していくためには、以下の３点に留意する必要がある。

① 経営層がリスクマネジメントを全うするためには、経営層には、リスクマネジメントのために必要な一定の IT やサイバーセキュリティに関する知識・能力が求められる。例えば、IT 利活用の恩恵（ベネフィット）と脅威（リスク）を理解し、株主等に対して説明できることが求められる。その際、経営層は、様々な経営課題に直面しており、極めて多忙であることが想定されるため、分かりやすく経営層が理解できるようにしておくことが必要である。

② 経営層は、上記のサイバーセキュリティに関する知識・能力を身につける仕組みをつくるとともに、個々のリスクへの対応を行う技術者等の取組に対して判断が求められるが、経営層に深い技術的知識やスキルを期待することは必ずしも現実的ではない。このため、企業組織において、経営戦略等におけるサイバーセキュリティリスクを認識した上で、事業継続と価値創出に係るリスクマネジメントを中心となって支えるとともに、経営層の方針を踏まえた対策を立案、様々な役割を担う実務者・技術者を指揮し、経営層に報告する役割を担う人材（いわゆる「戦略マネジメント層」[9]）を確保することが重要であること。

---

9 詳細は、「サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ報告書」を参照のこと。

③ サイバーセキュリティ事案は、企業グループの端で発生したものが全体に波及し、風評被害も含めて親会社が被るような問題に発展する可能性がある。このため、自社のサイバーセキュリティ対策だけでなく、外部委託先やサプライチェーン全体を視野に入れたガバナンス（統制）の検討が必要であること。

b．新たな技術等の利活用による価値創出（Society5.0）

Society5.0 の実現に向けて、IoT や AI など新しい技術を含めた IT を利活用し、ビジネスイノベーションを進めていく中で、それに伴ってサイバーセキュリティリスクに直面することになる。経営層の関心は、そのリスクを上回るリターンとして、ビジネスの価値創出ができるかどうかである。さらに言えば、経営層が、高いリターンを追求し、より大きな価値の創造を実現するためには、サイバー空間の不確実性というリスクに積極的に向き合い、サイバー空間をいかに積極的に活用していくかという意識を持つ必要がでてくる。その中で、サイバー空間から得られる恩恵や利益（ベネフィット）と比較して、リスク（ネガティブなリスクだけでなく、ポジティブなリスク[10]も含む）を適切にコントロールしていく意識を持ち、サイバーセキュリティを含めたビジネスに対する投資の判断をすることが必要である。

こうした視点の下では、サイバー空間のポジティブな面、ネガティブな面を俯瞰的にみていくことになる。また、セキュリティ・バイ・デザインによって予めセキュリティを製品やサービスに組み込むことによって、後からセキュリティに多大なコストをかけることなく、一定のサイバーセキュリティが確保された安全・安心な製品やサービスを提供できることは競争力の強化にもつながる。このため、この局面においては、サイバーセキュリティは、単なる事業継続のためのリスクマネジメントだけの問題ではなく、ビジネス戦略そのものの問題として捉えることが必要である。

また、価値創出を目指したサイバーセキュリティに取り組む上では、上記 a. 事業継続（危機管理）のリスクマネジメントの PDCA サイクルの中で実施される過去の事故事例をもとにした再発防止的な対応だけでなく、ビジネス戦略の企画と一体となって、将来起こりうるベネフィットやリスクについて、イメージを膨らませながら、対応することが必要となる可能性がある。

なお、イノベーションによって新たな価値が創出された後は、その成果が定着し、いかに安定的にその価値を活かした事業を継続させるかというステージに移る。すなわち、企業の創造した価値は、次々に b.のフェーズから a.のフェーズに移っていき、IT 分野においては、その

[10] ISO31000 で”It can be positive,negative,or both”と定義されている

スピードが極めて速い傾向にある。経営層はこのような認識の下で、サイバーセキュリティ対策を捉えるべきである。

（３）中小企業をはじめとする事業上のリソースの制約が大きい企業の対策

中小企業は、大企業に比べて経営基盤が必ずしも盤石ではないため、サイバー攻撃により、金銭的な損害や信用の低下を招いてしまった場合、経営に与えるインパクトが極めて大きい。また、中小企業であることを理由に、その企業へのサイバー攻撃が社会に与えるインパクトが必ずしも小さいとはいえず、中小企業が踏み台となって自社のみならず取引先までサイバー攻撃の影響が拡大することも想定される。一方、中小企業は、IT 機器（PC や複合機等）の利活用において、必ずしも高いセキュリティに関する知識やスキルを有しているとはいえず、セキュリティのための追加投資を理解することが難しいという事情を踏まえた上で、セキュリティ対策の検討を進めることが必要である。

このため、中小企業に対するセキュリティ対策のインセンティブを与えるための中小企業へのリーチの仕方については、中小企業をカテゴライズした上で検討することが有効であると考えられる。具体的には、中小企業全般については、社会全体に悪影響を与えないよう普及啓発を図るとともに、セキュリティ対策を導入するための資金的インセンティブを検討することが必要である。

その上で、例えば、グループ企業はホールディングスでガバナンスを効かせる、大企業と取引のある中小企業はサプライチェーン管理の一環として大企業の方が取引先としての中小企業を指導する、業種によっては類似の業務を抱えている場合があるので、そのような場合には共同してクラウドサービスを利用するといった対応が挙げられる。

その上で、情報システムの導入・運用において、追加的に過度なセキュリティ対策のコストや日常的な作業負担が生じないようなシステムモデルの検討が必要である。

（４）産学官連携の推進

企業の経営層がリスクマネジメントと価値創出の両面からサイバーセキュリティに取り組めるよう、各主体がそれぞれの役割を明確化しつつ、コミュニケーションを密に図りながら連携し、社会全体で取組を推進し、産学官連携のエコシステムを構築していく必要がある。

４　具体的方策

我が国企業の円滑なビジネスの遂行に向けて、事業継続（危機管理）としてのサイバーセキュリティを着実に遂行するとともに、イノベーションによる価値創出を実現するため、今後、以下に掲げる具体的方策について、産学官連携の下、検討をすべきである。

なお、これらの項目については、内閣サイバーセキュリティセンター（NISC）が全て実施することを企図したものではない。むしろ、NISC が必要に応じて関係者の調整・合意を図りつつ、関係省庁間、さらには、産学官の適切な役割分担の下、各主体が自発的・自律的に実施することを想定している。

(１) 経営層の理解と意識改革の推進

①　経営層の理解促進

- サイバーセキュリティ対策について経営層が果たすべき役割や持つべき認識について、引き続き検討を深め、「企業経営のためのサイバーセキュリティの考え方」の見直し、共有を図る。
- サイバーセキュリティを経営層による理解の下で取り組むためには、その取組の基本方針や内容について、経営層も含めた理解の促進と認識の共有ができるよう、マークやスローガンなど分かりやすい形でサイバーセキュリティの取組を表現し、普及するためのツールの整備を行うことが有効である[11]。
- 経営層の目線で、サイバーセキュリティ対策について議論が出来る人材が、経営層の理解を促していくことが期待される。このため、サイバー攻撃の脅威やその対応について、経営層にとって分かりやすく、納得感を持って説明や議論ができる人材（伝道師）の発掘・派遣を行う仕組みについて、既に取組が行われているオープンデータやシェアリングエコノミー等の分野の例を参考にしつつ検討を行う。
- 経営層がサイバーセキュリティの動向や対策について知ることが出来るよう、官民が連携して、経団連が策定した「サイバーセキュリティ経営宣言」[12]の普及や経営層向けのサイバーセキュリティに関するセミナー等を開催することが必要である。

---

11 海外の事例としては２（６）を参照

12 サイバーセキュリティ経営宣言（参考３）は、2020 年までを重点取り組み期間として、①経営課題としての認識、②経営方針の策定と意思表明、③社内外体制の構築・体制の実施、④対策を講じた製品・システムやサービスの社会への普及、⑤安心・安全なエコシステムの構築への貢献、の実践に努めることを宣言している。

(2) 業種・業態別の差異を踏まえた基盤の整備

① 体制整備の推進

- 経営層が、価値創出と事業継続（危機管理）のための取組を進めていく上で、サイバーセキュリティに関して、経営層に求められる役割を明確化することが必要である。併せて、経営層が、サイバーセキュリティリスクに関する経営判断を行う際、それを支援し、経営層と個々のリスク対応を行う実務者・技術者の間で調整が出来る人材としての「戦略マネジメント層」の育成・確保が必要である。その上で、実務者・技術者が担う役割を明確化し、内部で育成するのか、外部の事業者に委託するのかを含め、体制整備が必要である。
- 類似の企業の対策状況を見ながら自社の対策を考える企業が一般的であることから、自社にとって望ましい対策の理解を促すアプローチとして、（例えば、業種・業態毎の）平均的なセキュリティ対策のレベル感と望ましい対策のレベルを示せるよう、そのための基準（例：サイバーセキュリティ経営ガイドライン）と経営層に分かりやすく提示するための可視化ツールの整備を検討することが必要である。

② 制度整備の推進

- サイバーセキュリティ対策を進めていく際、ハイレベルのポリシーのレベルだけでは動きづらい場合がある。このため、経営層の示す方針に対応した望ましい具体的対策について業界、規模毎についてベストプラクティスとして広く共有し、経営層に対策の納得感を得ていくことが有益である。
- IT を利活用したビジネスにおいては、サイバーセキュリティに関連した法制度が密接に関わるため、企業が参照すべき法制度についての整理に向けた検討を行うことが有用であると考えられる。なお、法制度に関しては、法規制の下でのコンプライアンスに訴える強制的なアプローチは、経営の自由度を失う可能性があるため、特色あるリスクテイクによる新しい価値・イノベーションの創出に向けた阻害要因となる可能性があるため、慎重な検討が必要である。

(3) サイバーセキュリティ投資のためのインセンティブ

① 情報開示の促進に関する取組の推進

- サイバーセキュリティ対策について、企業が社会的責任を果たす観点から、それに取り組むとともに、市場や出資者といったステークホルダーからの評価を得て、経営上のインセンティブとしていくため、情報開示による企業のサイバーセキュリティの取組の見える化

を促すことが必要である。このため、例えば、ベストプラクティスやガイドラインの策定に向けた検討を行うことが必要である。[13]

② サイバーセキュリティ保険の普及に関する取組の推進

- 企業がサイバーセキュリティ対策を行うインセンティブが与えられるような仕組み（例：税制優遇の執行やサイバー保険）について、その効果も含めて今後のインセンティブ策の充実に向けた検討が必要である。
- サイバーセキュリティ対策のリスクマネジメント手段の一つとして、保険の活用が広がっているが、サイバーセキュリティ対策の実施状況に応じて、適切に保険料が算定される仕組みにより、リスクへの備えに対するコストが明確になっていくため、投資が進めやすくなる可能性がある。こうした点を踏まえ、官民が連携してサイバーセキュリティにおける保険の活用を推進するための方策について検討が行われることが期待される。

(4) 中小企業の関心や実態を踏まえたサイバーセキュリティ対策

- 中小企業に期待されるサイバーセキュリティ対策の基本的な項目について、中小企業の IT 利活用に対する関心や、セキュリティに対して必ずしも十分なコストや作業負担をかけることは出来ないとの実態を踏まえつつ、IT やセキュリティの知識がなくとも理解できるような対策集（「中小企業向け「情報セキュリティハンドブック（仮称）」の作成）が必要である。
- 上記項目の中でも特に優先して取り組むべき内容として、中小企業向けのセキュアな情報システムの利活用モデルの提示を検討すべきである。例えば、一社では十分なセキュリティ対策が難しいことが想定されるため、クラウドを活用することが有効である可能性がある。具体的には、アプリケーションとデータをサーバ上にあげて、マルチテナントでの運用を行う事業者の傘に入り、クライアント端末の自由度を下げることにより、セキュリティを高めるモデルなど、生産性・利便性向上やコストを考慮した中小企業向けのセキュリティレベルの高いシステムモデルが挙げられる。
- 中小企業におけるサイバーセキュリティ対策のインセンティブの仕組み（税制優遇など）については、引き続き検討を行う。
- 近年、イノベーションを目指したベンチャー企業は、例えば、IoT や AI、ブロックチェーンといった新技術をアグレッシブに利用し、開発と運用を繰り返してサービスを連続的に見直しつつ改善を図って品質を徐々に高めていくシステム構築のモデルが広がりはじめてい

[13] 総務省 情報開示分科会報告書（案）においては、平成 30 年秋を目途にガイドラインを策定とされている。

る。こうしたモデルにおいては、セキュリティをこれらのシステム開発・運用者が同時に組み込みながら進めていく必要があるため、そういった新たなモデルの中でのセキュリティの在り方について検討し、機動的にガイドラインの策定等を行うことが必要である。

５　今後の取組とまとめ

本取りまとめの内容を踏まえ、次期サイバーセキュリティ戦略の検討を進めるとともに、「企業経営のためのサイバーセキュリティの考え方」について必要な見直しを図るものとする。また、引き続き、産業界との緊密な連携の下、人材育成施策の検討を進めるとともに、本報告書の示した具体的方策の実施状況については、サイバーセキュリティ戦略の年次報告等を通じてフォローアップを行う。

（別紙１）参考資料

参考１　各省庁の主な取組[14]

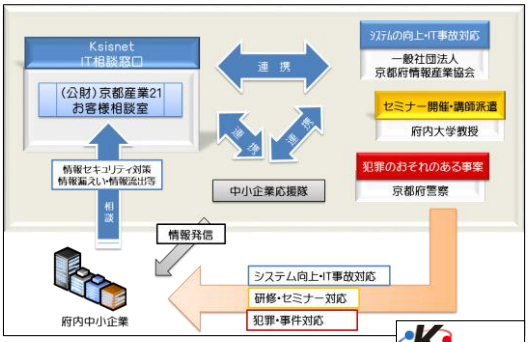
（１）警察庁の取組

中小企業におけるサイバーセキュリティ向上のための取組

警察では、中小事業者が有する先端技術に関する情報の窃取や、中小事業者の保有するサーバ等がサイバー攻撃の踏み台として悪用されることなどを防止するため、商工会議所、学術機関、地方公共団体等と連携し、中小事業者における適切な対策を促すための広報啓発活動等を実施している。

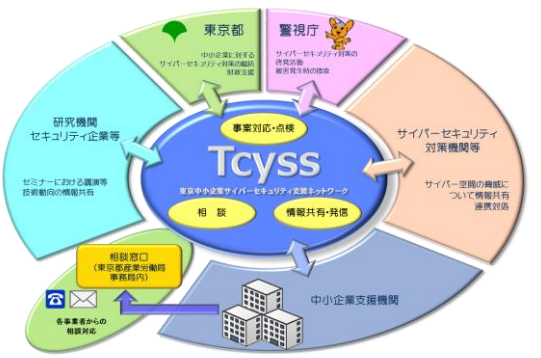
主な産学官連携の枠組み

京都中小企業情報セキュリティ支援ネットワーク（Ksisnet）



※　平成30年４月時点で24の関係機関・団体等が参加

東京中小企業サイバーセキュリティ支援ネットワーク（Tcyss）



※　平成29年４月時点で21の関係機関・団体等が参加

産学官が連携し、サイバーセキュリティに関する相談窓口の設置、セミナーの開催等
中小企業におけるサイバーセキュリティ対策への支援を実施

14　関係省庁より提供

（２）総務省の取組

※総務省　サイバーセキュリティタスクフォース第９回会合（平成 30 年４月 11 日）資料より抜粋

情報開示分科会の設置

検討の背景・目的

○　民間企業におけるセキュリティ対策の情報開示については、「サイバーセキュリティ戦略」（平成27年９月４日閣議決定）等で触れられているほか、「IoTセキュリティ総合対策」（平成29年10月　サイバーセキュリティタスクフォース）において、民間企業におけるセキュリティ対策を促進するために、「企業のセキュリティ対策に係る情報開示に関するガイドラインの策定について、関係府省と連携しつつ、年度内を目途に一定の結論が得られるよう検討する必要がある」とされているところ。

○　このため、サイバーセキュリティタスクフォースの下に「情報開示分科会」を設置し、民間企業のセキュリティ対策の情報開示に関する課題を整理し、必要な方策について検討を行う。

（参考）「IoTセキュリティ総合対策」（平成29年10月　サイバーセキュリティタスクフォース）より抜粋

Ⅱ　具体的施策
（３）民間企業等におけるセキュリティ対策の促進
②　セキュリティ対策に係る情報開示の促進

民間企業においては、複雑・巧妙化するサイバー攻撃に対する対策強化を進める動きが見られるようになってきており、こうした取組をさらに促進するためには、セキュリティ対策を講じている企業が市場を含む第三者から評価される仕組みを構築していくことが求められる。

米国においては、日本の有価証券報告書にあたる10－K報告書において記載することが推奨されるセキュリティ対策について証券取引委員会（SEC）がガイドラインを策定・公表している 。こうした情報開示はあくまで任意のものであるが、企業の対策促進の観点からみて有益な取組であると考えられる。

このため、我が国においても、あくまで任意の情報開示であることを前提としつつ、企業のセキュリティ対策に係る情報開示に関するガイドラインの策定について、関係府省と連携しつつ、年度内を目途に一定の結論が得られるよう検討する必要がある。その際、開示する情報の粒度については情報開示が新たな攻撃を誘発しないよう十分に配慮するとともに、こうした情報開示とサイバーセキュリティ保険の普及の在り方について併せて検討する必要がある。

情報開示分科会報告書（案）概要

○　民間企業における**セキュリティ対策の情報開示による「セキュリティ対策の見える化」を通じて、**民間企業の経営層が自社のセキュリティ対策の現状を認識し、また、他社の状況と比較することにより、さらに必要な具体的な対策を検討し、導入する**「セキュリティ対策の好循環」が起こる環境の実現**が期待される。

○　情報を開示するにあたっては、開示の対象者によってその考え方、取組が異なることから、報告書（案）においては、**①社内の情報共有（第一者開示）**、**②契約者間等の情報開示（第二者開示）**、**③社会に対する情報開示（第三者開示）**の3つの側面に分けて整理している。

これまでの開示の考え方

⇒　社会に対する情報開示（第三者開示）

本分科会での整理

セキュリティ対策の開示（共有）の3つの側面

社内の情報共有（第一者開示）

自社のセキュリティ対策について、その必要性・重要性・緊急性をセキュリティ対策の担当部署だけでなく、社内全体で共有すること。

【意義】
・　取締役会における検討等を通じて、経営層としても責任を自覚すること（気づき）となり、セキュリティ対策が経営課題として扱われることになる。
・　経営層がセキュリティ面におけるリスク及びその対策の状況を適切に認識することにより、セキュリティ対策を強化するための経営判断に資する。

契約者間等の情報開示（第二者開示）

契約の相手方や、グループ企業やサプライチェーンを構成する企業、保険会社等、対象を限定して自社のセキュリティ対策を開示すること。

【意義】
・　契約の相手方との間で信頼を醸成するとともに、サプライチェーン全体のセキュリティが向上する 。
・　セキュリティインシデントや、その対策等について情報を共有・開示することにより、共有範囲の中で信頼の醸成やセキュリティ対策の向上に資する。
・　サイバーセキュリティ保険について、保険会社に対して適切にセキュリティ対策を開示し、定期的に評価を受けることにより、追加的なセキュリティ対策を検討する機会となる。

社会に対する情報開示（第三者開示）

社会の幅広い対象に向けて、自社のセキュリティ対策を開示すること。

【意義】
・　経営層が自社のセキュリティ対策を認識するきっかけとなる。
・　他社のセキュリティ対策の状況を知り、自社と比較することができる環境となり、さらに社会全体でセキュリティ対策が競争的に拡大する。
・　開示した企業が、適切かつ優良な取引先として認識されることを通じて、サプライチェーン全体のセキュリティの確保に資する。

情報開示分科会報告書（案）概要

検討結果

社内の情報共有（第一者開示）

・ 経営層の理解を深め、気づきを与えるとともに、セキュリティ対策の担当部署の現場と経営層の間を繋ぐ、いわゆる「橋渡し人材」の育成に向けた取組を進める必要がある。

契約者間等の情報開示（第二者開示）

・ 契約者間等で確認すべき事項や必要な対策の整理、サプライチェーン全体またはグループ全体における情報共有体制の構築の促進が必要である。

・ サイバーセキュリティ保険について、対策の実施及び開示のインセンティブとなるような割引制度の普及や、グループ全体・サプライチェーン全体で一括して加入するような保険商品の展開が期待される。

社会に対する情報開示（第三者開示）

・ 事業者の規模や取組状況に応じて、セキュリティ対策の自己宣言制度や主要5項目（※）の開示、「情報セキュリティ報告書」の作成など、段階的に対策を講じていくことが望ましい。

※ ①基本方針等の策定状況 ②管理体制 ③教育・人材育成
④社外との情報共有体制 ⑤第三者評価・認証

今後の取組

（社内の情報共有に向けた橋渡し人材の育成）

1. **人材のスキルの具体化**、スキル取得のための**教育コンテンツの開発・普及**、**スキル認定を行う仕組みを産学官により構築するための検討**。
【平成30年度中を目途に方向性を整理】

（関係者間の情報共有促進のための仕組みづくりの検討）

2. **米国等におけるISAO(※)等の動向等について調査**するとともに、**公的支援のあり方について検討**。
【平成30年度中を目途に検討結果を取りまとめ】
（※）ISAO：Information Sharing and Analysis Organization

3. **セキュリティベンダー、損害保険会社、その他の関連する企業によるサイバーセキュリティ保険を含む総合サービスの開発に向けたモデル事業を推進**し、標準仕様化に向けて検討。また、**企業のセキュリティ対策の強度を簡易に診断できるツールキットを評価する仕組みづくりを検討**。
【モデル事業については平成30年度に検討】

（第三者開示の促進に向けたガイドラインの策定）

4. **「セキュリティ対策情報開示ガイドライン」（仮称）を策定・公表**。
【平成30年秋を目途にガイドラインを策定】

5. 導入予定の「コネクティッド・インダストリー税制」の活用状況を分析するとともに、**企業のニーズ等を反映した投資促進のための政策支援のあり方について検討**。
【支援税制の運用にあわせて適宜実施】

（３）経済産業省の取組

サイバーセキュリティ経営ガイドライン（平成27年12月28日公開、平成29年11月16日改訂）

- 経済産業省と（独）情報処理推進機構（IPA）にて策定。
- 経営者のリーダーシップによってサイバーセキュリティ対策を推進するため、**経営者が認識すべき3原則**と、**経営者がセキュリティの担当幹部（CISO等）に指示すべき重要10項目**を提示。

１．経営者が認識すべき３原則

（１）経営者は、サイバーセキュリティリスクを認識し、**リーダーシップによって対策を進める**ことが必要

（２）自社は勿論のこと、ビジネスパートナーや委託先も含めた**サプライチェーンに対するセキュリティ対策が必要**

（３）平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、**関係者との適切なコミュニケーションが必要**

２．経営者がCISO等に指示すべき１０の重要事項

リスク管理体制の構築

（指示１）サイバーセキュリティリスクの認識、組織全体での対応方針の策定
（指示２）サイバーセキュリティリスク管理体制の構築
（指示３）サイバーセキュリティ対策のための資源（予算、人材等）確保

インシデントに備えた体制構築

（指示７）**インシデント発生時の緊急対応体制の整備**
（指示８）**インシデントによる被害に備えた復旧体制の整備**

リスクの特定と対策の実装

（指示４）サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
（指示５）**サイバーセキュリティリスクに対応するための仕組みの構築**
（指示６）サイバーセキュリティ対策におけるPDCAサイクルの実施

サプライチェーンセキュリティ

（指示９）**ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握**

関係者とのコミュニケーション

（指示10）情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供

※赤字及び太字は平成29年度11月16日改訂部分

（参考）セキュリティ対策自己宣言「SECURITY ACTION」

- 中小企業自らが、セキュリティ対策に取り組むことを自己宣言する制度をIPAにて開始(*)。
- 二つ星を宣言した企業には、サイバー保険の保険料を割り引く制度も損保会社（損保ジャパン）より提供。

★ 一つ星

SECURITY ACTION ★
セキュリティ対策自己宣言

情報セキュリティ5か条に取り組む企業

① OS・ソフトウェアの最新化（パッチ適用、バージョンアップ）
② ウイルス対策ソフトの導入
③ 強固なパスワード設定
④ データ等は必要最低限の人のみに共有
⑤ 攻撃の手口の把握

★★ 二つ星

SECURITY ACTION ★★
セキュリティ対策自己宣言

情報セキュリティ自社診断により自社の状況を把握し、セキュリティポリシーを策定する企業

25の診断項目により自社の対策状況を把握

セキュリティポリシー策定のためのひな形も提供

(*) https://www.ipa.go.jp/security/security-action/

参考２ 「Society5.0 実現に向けたサイバーセキュリティの強化を求める」（要点）
（2017 年 12 月 12 日 一般社団法人日本経済団体連合会）

Keidanren
Policy & Action

2017年12月12日 公表

Society 5.0 実現に向けた
サイバーセキュリティの強化を求める

一般社団法人 日本経済団体連合会

<背景>
- サイバー攻撃による被害が世界中で拡大するなか、2020年の東京オリパラに向けて対策強化は喫緊の課題。
- サイバーセキュリティの強化は「Society 5.0」の基盤となりうる成長のための最重要分野でもある。
- 経団連は、2015年・2016年に提言を公表し、ある程度の対策は進んだが、まだ道半ばである。
- 2017年11月には経団連「企業行動憲章」を改定し、社会的責任としてサイバー対策に取り組むことを打ち出した。
- あらゆるステークホルダーの連携のもとでより具体的な対策を進めるために、改めて提言を行う。

サイバーセキュリティに関する基本的な視点

①価値創造
- Society 5.0時代には、IoTによりあらゆるモノがサイバー空間と結びつく。サイバーセキュリティ確保が競争力の源となる。
- 中小企業も含めたサプライチェーン全体のサイバーセキュリティ確保が重要。

②危機管理
- サイバー攻撃による情報漏えいやサービス停止など被害が拡大中。IoTなど攻撃の対象も増加。
- 対策を怠れば、関係者から信頼を失いかねない。
- 企業としては、事業継続を重視し、自主的に対策を行うことが必要。

具体的に取り組むべき事項 ～自助・共助・公助・国際連携の視点で取り組み推進を～

①意識改革
- 社会全体での意識向上、協調領域としての認識
- セキュリティ・バイ・デザインの実装
- 経営の最重要課題としての認識
- 被害を受けた企業を過度に責めない社会風土醸成

②リソース確保 ～ヒト・情報・技術・カネの好循環～

人材育成
- 国民全体のリテラシー向上
- 経営者の理解増進
- 人材育成・維持のエコシステム
- キャリアパス構築、見える化
- 高度人材の厚遇
- 資格普及
- 人材発掘

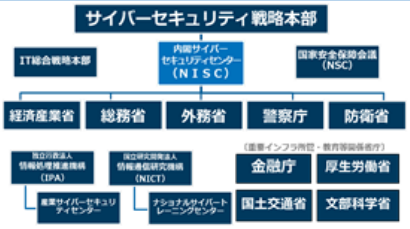
情報共有
- 情報の類型等の整理
- ISAC・ISAOの設立
- 政府支援・情報提供
- アクセス権限管理
- 活用・対応の仕組み
- 国際連携

投資促進
- 官民での積極投資
- サイバー保険の活用
- 共済や全国的組織、シンクタンクの設置
- 対策費への税制・補助金等の公的支援
- 政府予算の大幅拡充

技術対策
- OS等のアップデート
- 中小企業クラウド化
- 商品・サービスのセキュリティ強化
- OTとIT連携への対策
- 研究開発の推進
- 国際標準の先導

③推進体制の整備

政府関連組織の整備・連携



- 関係省庁の役割分担の明確化、施策の一体化、優先順位の共有
- NISCの総合調整機能の強化、予算・人員拡大
- 将来的には情報関連政策を一元的に所管する機関の創設
- 政治のリーダーシップへの期待

企業内外の体制整備
- CISOやCSIRTの設置及びスタッフの充実
- 従業員への継続的な研修や演習
- BCP(事業継続計画）の策定及び訓練
- サプライチェーン全体のサイバーセキュリティ管理
- SOCレポート、各種報告書の活用

④法制度・規範の整備
- 技術進歩に法制度が追いついていないことへの対応
- 不正アクセス禁止法や電気通信事業法の見直し
- 技術標準や対策ガイドラインの整備
- 国際規範の策定に向けた官民の協力・積極参加

経団連アクションプラン ～経団連自らも具体的な取り組みを推進～

①経営層の理解促進
- 「サイバーセキュリティ経営宣言」策定
- 経営者向けセミナー、研修、合宿

②広報・周知活動
- 実態調査、事例集の公開
- 機関紙や説明会を通じた周知

③国際連携
- 国際会合への参加
- 世界経済フォーラムとの連携

参考３ 「経団連サイバーセキュリティ経営宣言」（2018 年３月 16 日 一般社団法人日本経済団体連合会）

2018 年 3 月

一般社団法人 日本経済団体連合会

最新テクノロジーとデータを活用して社会全体の生産性向上と課題解決を図る「Society 5.0」に向け、あらゆる場面で IT との融合が進む一方、サイバー空間の秩序や安全に脅威を与える、著しい悪意を持った行為も多発している。いまやすべての企業にとって価値創造とリスクマネジメントの両面からサイバーセキュリティ対策に努めることが経営の重要課題となっている。

重要インフラの多くを担い、さまざまな製品やサービスを提供する経済界は、主体的に対策を講じる必要性を強く自覚する。

経済界は、全員参加でサイバーセキュリティ対策を推進し、安心・安全なサイバー空間の構築に貢献する。サイバー攻撃が激化する 2020 年の東京オリンピック・パラリンピック競技大会までを重点取り組み期間として、以下の事項の実践に努めることを宣言する。

1 経営課題としての認識

■経営者自らが最新情勢への理解を深めることを怠らず、サイバーセキュリティを投資と位置づけて積極的な経営に取り組む。
■経営者自らが現実を直視してリスクと向き合い、経営の重要課題として認識し、経営者としてのリーダーシップを発揮しつつ、自らの責任で対策に取り組む。

2 経営方針の策定と意思表明

■特定・防御だけでなく、検知・対応・復旧も重視した上で、経営方針やインシデントからの早期回復に向けた BCP(事業継続計画)の策定を行う。
■経営者が率先して社内外のステークホルダーに意思表明を行うとともに、認識するリスクとそれに応じた取り組みを各種報告書に自主的に記載するなど開示に努める。

3 社内外体制の構築・対策の実施

■予算・人員等のリソースを十分に確保するとともに、社内体制を整え、人的・技術的・物理的等の必要な対策を講じる。
■経営・企画管理・技術者・従業員の各層における人材育成と必要な教育を行う。
■取引先や委託先、海外も含めたサプライチェーン対策に努める。

4 対策を講じた製品・システムやサービスの社会への普及

■製品・システムやサービスの開発・設計・製造・提供をはじめとするさまざまな事業活動において、サイバーセキュリティ対策に努める。

5 安心・安全なエコシステムの構築への貢献

■関係官庁・組織・団体等との連携のもと、各自の積極的な情報提供による情報共有や国内外における対話、人的ネットワーク構築を図る。
■各種情報を踏まえた対策に関して注意喚起することによって、社会全体のサイバーセキュリティ強化に寄与する。

DECLARATION OF CYBER SECURITY MANAGEMENT

参考４　商工会議所における取組事例

◆東京商工会議所：警察機関との連携（2017 年 10 月～）

・ 東京商工会議所は、管内中小事業者におけるサイバーセキュリティの意識向上、サイバー犯罪・サイバー攻撃による被害の防止を目的として、警視庁、行政、支部(江東、中央、荒川、品川)、各区で、サイバーセキュリティに関する協定を締結。今後、他支部においても、順次、協定締結の予定。

◆大阪商工会議所：ホームページパトロールサービス（2017 年６月～）

・ 大阪商工会議所は、会員企業のホームページを１日２回巡回してサイバー攻撃を検知する月額 500 円のサービスを開始。

・ 現在は、関西の会員企業を対象とし、これまでに 80 企業・団体が利用。今後、サービス利用対象を全国に拡大する予定。

◆日本商工会議所：サイバーセキュリティ保険（2018 年３月～）

・ 日本商工会議所では、国内外でのサイバー攻撃が増加する中、IT 活用を進める中小企業経営者のサイバーリスクに対する備えを図るため、民間保険として、2018 年３月から従来の保険制度にサイバーリスクに対する補償を拡充。

（別紙２）セキュリティマインドを持った企業経営ワーキンググループ　委員等名簿及び開催実績

＜委員＞

主査	林　紘一郎	情報セキュリティ大学院大学　教授
委員	大杉　謙一	中央大学大学院　法務研究科　教授
委員	岡村　久道	英知法律事務所　弁護士 京都大学大学院　医学研究科　講師
委員	落合　正人	SOMPO リスクケアマネジメント株式会社 サイバーセキュリティ事業本部　サービス推進部長
委員	野口　和彦	横浜国立大学　大学院　環境情報研究院　教授 リスク共生社会創造センター長
委員	橋本　伊知郎	野村ホールディングス株式会社　参事　Co-CIO 野村證券株式会社　経営役　業務企画　兼　IT 担当
委員	丸山　満彦	デロイト トーマツ リスクサービス株式会社　代表取締役社長

＜オブザーバー＞

梶浦　敏範	日本経済団体連合会 情報通信委員会 企画部会長代行・サイバーセキュリティに関する懇談会座長
小松　靖直	日本商工会議所　情報化推進部　部長
上野　耕司	一般社団法人サイバーリスク情報センター 産業横断サイバーセキュリティ人材育成検討会 会長

関係省庁　（警察庁、金融庁、総務省、法務省、経済産業省）

（敬称略）

＜開催実績＞

第４回　平成 29 年 10 月 30 日

・企業経営のためのサイバーセキュリティについて

・関係省庁及び民間の取組について

第５回　平成 30 年２月９日

・前回提示した論点及びこれまでの議論の整理について

・中小企業のサイバーセキュリティについて

・関係省庁及び民間の取組について

第６回　平成 30 年４月 18 日

（サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループと合同開催）

・サイバーセキュリティ人材育成に関する方向性について

－セキュリティマインドを持った企業経営ワーキンググループ報告書

－サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ報告書