別紙1

情報開示分科会
報告書

2018 年6月

サイバーセキュリティタスクフォース

情報開示分科会

目 次

はじめに

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適切に評価される仕組みを構築していくことが求められている。

こうした状況を踏まえ、情報開示分科会は、あくまで任意の取組であることを前提としつつ、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、その普及に必要な方策について検討を行うことを目的として、2017 年 12 月、サイバーセキュリティタスクフォースの下に設置された。

検討の結果、セキュリティ対策の情報開示については、開示の対象者によって目的、方法、項目、その粒度等に違いがあることから、「社内の情報共有（第一者開示）」、「契約者間等の情報開示（第二者開示）」、「社会に対する情報開示（第三者開示）」の3つの側面に分けて議論を整理することとされた。

このうち、社内の情報共有（第一者開示）については、引き続き、経営層の理解を深め、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」等の育成に向けた取組を進める必要があるとされた。

また、契約者間等の情報開示（第二者開示）については、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とされた。さらに、サイバーセキュリティ保険の活用に向けて、セキュリティ対策及びその開示のインセンティブとなるような割引制度の普及や、グループ全体または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こととされた。

加えて、社会に対する情報開示（第三者開示）については、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とされた。

本報告書を踏まえ、民間企業におけるセキュリティ対策の情報開示を推進するため、今後の取組として、本年秋を目途に「セキュリティ対策情報開示ガイドライン」（仮称）を策定することとし、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を通じて、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等が期待される。

第１章　民間企業におけるセキュリティ対策の情報開示の現状

１．１　情報開示の基本的考え方

IoT 化が進んだ社会において、企業がセキュリティ対策に取り組むことは面的防御によるサイバー攻撃への耐性を強化するための社会的な責務であるとともに、企業自身にとっても事業継続のために必要不可欠である。その際、企業においてセキュリティ対策を進めるには、特に経営層においてセキュリティ対策が企業経営において重要な課題であるとの認識が深まることが重要である。

そのため、企業の経営層が自社のセキュリティ対策の現状を正しく認識し、また、他社の状況と比較することを通じて、さらに必要な具体的な対策を検討・導入できるような環境の実現という「セキュリティ対策の好循環」を創出することが必要である。加えて、こうした取組を積極的に進めている企業が、市場を含む第三者から適切に評価されることが必要である。こうした環境を実現するためには、自社のセキュリティ対策に係る情報について、経営層に限らず、社内全体で共有するとともに、関係企業及び社会全体に対して適切な方法・範囲で開示（共有）されることが必要であると考えられる。

情報開示については、これまで社会の幅広い対象に向けた「第三者開示」として捉えられていたが、本分科会での議論により、情報開示（共有）の対象者によってその考え方、取組が異なることが明らかになった。すなわち、社内における情報共有である「第一者開示」、契約の相手方や、グループ企業またはサプライチェーンを構成する企業、保険会社等、対象を限定した情報開示である「第二者開示」、さらに従来からの「第三者開示」である。

また、情報開示（共有）の内容については、平時のセキュリティ対策に関するものと、有事のセキュリティインシデントに関するものの２種類が考えられるが、今回の本分科会のとりまとめにおいては前者を主な検討の対象とした。

なお、セキュリティ対策に関する情報を開示するにあたっては、情報セキュリティ監査などを通じてその内容の正確性・客観性が担保されることが望ましい。開示する媒体によっては、監査役・監査等委員・監査委員による監査の対象となると考えられる。また、情報の開示によってサイバー攻撃を誘発することのないよう適切性を確保することも求められる。

（１）　社内の情報共有（第一者開示）

企業においてセキュリティ対策を進めるためには、その必要性・重要性・緊急性について、

セキュリティ対策の担当部署だけでなく、社内全体で理解されることが必要となる。特にセキュリティ対策について情報開示を行う際には、取締役会において検討される等により経営層としても責任を自覚すること（気づき）となり、セキュリティ対策の担当部署と経営層との間で情報共有が適切になされることから、セキュリティ対策が担当部署のみの問題ではなく、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自社の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新たな設備投資や、組織・人員の拡充、残存リスクに対応するためのサイバーセキュリティ保険への加入といった経営判断に資することが期待される。また、その実施にあたっては、経営層のみならず、社内の各担当部署においても、その必要性等について理解されていることが求められる。

（２） 契約者間等の情報開示（第二者開示）

企業においては、１社がサイバー攻撃を受けた場合に、被害が当事者だけでなく、サプライチェーン全体またはグループ全体に広がる懸念がある。また、今後 IoT 化によって領域を超えたシステム連携が進むことから、システミックリスクを回避するための仕組み作りが求められる。

このため、企業間取引においても、取引条件としてセキュリティ確保に関する要求がなされつつある状況にある。契約の相手方に自社のセキュリティ対策に係る情報を適切に共有することで両者の間で信頼を醸成するとともに、サイバー攻撃によるリスクを低減することが可能になる。このように、契約者間のセキュリティ対策に係る適切な情報の共有・開示により、サプライチェーン全体のセキュリティが向上することが期待される[1]。

また、同様のシステムを利用していることが多い業界内の企業が参画し、発生した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・開示することは、当該範囲の中での企業の枠を越えた信頼の醸成やセキュリティ対策の向上に資すると考えられる。

こうした取組は ISAC[2]の枠組みとして重要インフラ分野を中心に進んでいる。情報通信分野における ICT-ISAC はその先導的なモデルであり、この他、金融、電力、自動車等の分野で ISAC 組織が設立・運用されている[3]。

---

[1] 企業グループにおいて、親会社による企業集団内部統制の構築・運用の過程において親子会社間で情報のやり取りがなされることがあり、これは第二者開示の一種といえる。

[2] Information Sharing and Analysis Center の略。
サイバーセキュリティに関する情報収集や、収集した情報の分析等を行う組織。分析した情報は ISAC に参加する会員間で共有され、各々のセキュリティ対策等に役立てられる。（「サイバーセキュリティ 2017」（2017 年８月　サイバーセキュリティ戦略本部）　参考　用語解説）

[3] 国土交通省においては、所管する重要インフラ事業者（航空、鉄道、物流）が情報の共有・分

加えて、自社のセキュリティ対策で防ぐことができる範囲を超えて生じた損害を補償する手段として、サイバーセキュリティ保険を活用することが考えられるが、保険料の算定にあたっては損害保険会社に対して自社のセキュリティ対策について適切に開示し、評価を受けることが必要となる。また、その評価を踏まえて、追加的なセキュリティ対策を検討する機会となることも考えられる。

（３） 社会に対する情報開示（第三者開示）

事業者が自社のセキュリティ対策に係る情報を社会に向けて開示する「セキュリティ対策の見える化」を行うにあたっては、その前提として経営層の判断が求められることに加え、社会全体で「セキュリティの見える化」が進むことによって、自社と同業種・同規模の他社で取られているセキュリティ対策の状況を知り、自社の対策と比較することができる環境となることで、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ことが期待される。

また、自社のセキュリティ対策を開示した事業者が、経営上の重要課題としてセキュリティ対策に積極的に取り組んでいることが市場から正当に評価されて企業価値の向上に寄与することにより、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ことも期待される。

析や対策を連携して行う体制として「交通 ISAC」（仮称）の創設に向けた検討を支援することとしている。

１．２ 情報開示に関するこれまでの経緯

サイバー攻撃が近年急増するとともに、急速に複雑・巧妙化してきている。こうした中、企業等におけるサイバーセキュリティ対策は重要な経営課題の一つとして位置づけられるべきものとなっている。

個人情報保護委員会によると、個人情報漏えい事案の件数は近年減少傾向にあるものの、漏えい人数の多い事案が増加している傾向にある。平成 28 年度中に事業者が公表した個人情報漏えい事案（所管府省において把握したものに限る）のうち、漏えいした個人情報が5万件超の事案 22 件のうち 19 件が不正アクセス等によるサイバー攻撃事案となっている[4]。また、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）等の調査によるとサイバー攻撃事案の一件あたりの個人情報漏えい事案の被害規模の拡大（2016 年時点で 1 件あたり 6 億 28 百万円と推計）は企業経営に与える損失額を増加させ、企業経営にとって極めて重要な課題であることを示している。【資料１～３】

こうした中、企業等がサイバー攻撃対策を講じていることを企業内、サプライチェーン等の関係企業間、株主等の市場関係者と的確に共有する（情報開示を行う）ことは当該企業等の価値を高める上でますます重要なものになってきている。現時点において、我が国ではセキュリティ対策に特化した情報開示に関する法的な根拠や具体的な指針は存在しないものの、企業経営におけるサイバーセキュリティ対策の重要性について、企業等の情報開示のあり方を含め、様々な議論が始まっている状況にあり、今後その具体化を図っていくことが求められる。

民間企業におけるセキュリティ対策の情報開示に関する議論としては、例えば以下のようなものが挙げられる。

（１） サイバーセキュリティ戦略（2015 年９月　閣議決定）

「サイバーセキュリティ基本法」（平成 26 年法律第 104 号）の規定に基づき、政府はサイバーセキュリティに関する施策の基本的な方向性を示した国家戦略として「サイバーセキュティ戦略」を 2015 年９月に閣議決定した。【資料４】

本戦略においては、「セキュリティ対策はやむを得ない『費用』ではなく、より積極的な経営への『投資』であるとの認識を醸成していくことは、我が国の経済社会の活力の向上及び

[4] 「平成 28 年度個人情報の保護に関する法律施行状況の概要」（平成 29 年 11 月　個人情報保護委員会）
https://www.ppc.go.jp/files/pdf/personal_sekougaiyou_28ppc.pdf

持続的発展のために必要である」とし、このために「サイバーセキュリティ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仕組みや資金調達等の財務面で有利となる仕組みの構築、認識醸成のための官民が一体となった啓発活動を実施する」としている。

（２） 企業経営のためのサイバーセキュリティの考え方（2016 年8月　内閣サイバーセキュリティセンター）

内閣サイバーセキュリティセンター（以下「NISC」という。）においては、2015 年 12 月、普及啓発・人材育成専門調査会の下に「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」を設置し、サイバーセキュリティを事業戦略の一つとした企業経営の在り方について検討を行い、企業の自発的な取組を促進するため、サイバーセキュリティの基本的な考え方と企業の視点別の取組方法についてのガイドを示した、「企業経営のためのサイバーセキュリティの考え方」（2016 年８月）を策定・公表[5]している。【資料5】

セキュリティ対策の情報開示については、「（セキュリティ対策に関する）取組に係る姿勢や方針について情報発信していくことで、関係者の理解が深まり、社会的評価を高めることとなる」としており、「情報発信の方法として、一般に認知されている情報セキュリティ報告書、CSR 報告書、サステナビリティレポート、有価証券報告書やコーポレート・ガバナンス報告書等の活用が挙げられる」としている。

（３） サイバーセキュリティ経営ガイドライン Ver.2.0（2017 年 11 月 16 日　経済産業省・独立行政法人情報処理推進機構）

経済産業省及び独立行政法人情報処理推進機構（以下「IPA」という。）は、企業のセキュリティ対策に関して、経営者による判断の重要性が高まっているとの認識の下、2015 年 12 月、「サイバーセキュリティ経営ガイドライン」を策定、公表[6]した。その後、2017 年 11 月、サプライチェーンリスクへの対処等を追記した「サイバーセキュリティ経営ガイドライン Ver2.0」として更新・公開[7]されている。【資料6】

本ガイドラインにおいては、セキュリティ対策の情報開示について、「万一サイバー攻撃による被害が発生した場合、関係者と、平時から適切なセキュリティリスクのコミュニケーシ

---

[5] 「企業経営のためのサイバーセキュリティの考え方」（2016 年８月　NISC）
https://www.nisc.go.jp/active/kihon/pdf/keiei.pdf

[6] 「サイバーセキュリティ経営ガイドライン Ver1.0」（2015 年 12 月　経済産業省・ＩＰＡ）
http://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v1.0.pdf

[7] 「サイバーセキュリティ経営ガイドライン Ver2.0」（2017 年 11 月　経済産業省・ＩＰＡ）
http://www.meti.go.jp/press/2017/11/20171116003/20171116003-1.pdf

ョンができていれば，関係者の不信感の高まりを抑えることができる」ことから、「平時から実施すべきサイバーセキュリティ対策を行っていることを明らかにするなどのコミュニケーションを積極的に行うことが必要である」としている。

また、「サイバーセキュリティ経営の重要１０項目」[8]のうち、「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」の項目において、「ステークホルダーからの信頼性を高めるため、対策状況を開示させる」としており、「サイバーセキュリティ対策の状況について、サイバーセキュリティリスクの性質・度合いに応じて、情報セキュリティ報告書、CSR 報告書、サステナビリティレポートや有価証券報告書等への記載を通じて開示を検討する」としている。

（４） 民間団体における検討

一般社団法人日本経済団体連合会においては、2015 年２月と 2016 年１月の２度にわたり、「サイバーセキュリティ対策の強化に向けた提言」を公表[9]し、重要インフラ等におけるサイバーセキュリティ対策として、情報共有や人材育成等の重要性を指摘している。また、2017 年 11 月には「企業行動憲章」[10]を改訂し、持続可能な社会の実現に向けた企業の社会的責任としてサイバーセキュリティ対策を行うことを打ち出しており、同年 12 月には「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」と題した提言を公表[11]している。【資料７～10】

同提言においては、サイバーセキュリティを技術的なものとして情報システム部門等に一

---

[8] 以下の 10 項目を掲げている。
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
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
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
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
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

[9] 「サイバーセキュリティ対策の強化に向けた提言」（2015 年２月　日本経済団体連合会）
http://www.keidanren.or.jp/policy/2015/017_honbun.pdf
「サイバーセキュリティ対策の強化に向けた第二次提言」（2016 年１月　日本経済団体連合会）
http://www.keidanren.or.jp/policy/2016/006_honbun.pdf

[10] 「企業行動憲章」（2017 年 11 月　日本経済団体連合会）
http://www.keidanren.or.jp/policy/cgcb/charter2017.pdf

[11] 「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」（2017 年　日本経済団体連合会）
http://www.keidanren.or.jp/policy/2017/103_honbun.pdf

方的に任せるのではなく、経営層がサイバーセキュリティリスクを経営に大きな影響を与える最重要課題と捉えることが必要であり、経営会議や取締役会で定期的に報告・討議を行い、経営者の責任でリスクの低減・回避・共有・受容を判断しなければならないとしている。

また、サイバー攻撃に関する情報開示について、被害の他社等への拡大の防止の観点から、迅速かつ適切な情報公開が求められるとしているとともに、サイバー被害は誰にも生じうるものであるという認識を社会全体で広めることで、ベースラインの対策をとっていた企業をいたずらに責めることなく、むしろ積極的な情報公開を促す社会風土を醸成することも必要であるとしている。

さらに、各企業はサイバーセキュリティ確保が成長と事業継続の基盤であるとともに、社会的責任であるとの視点を持ちつつ、リスクを総合的に勘案の上、人材や技術、社内体制整備に十分な費用をかけて対策強化に努めなければならないとしている。一方で、サイバー攻撃は完全に防ぐことは困難であることから、そのリスクをカバーする手法の一つとしてサイバーセキュリティ保険を挙げている。また、サプライチェーン全体のサイバーセキュリティ管理の観点から、企業には国内外のグループ子会社や取引先等に対するセキュリティ状況のヒアリングや対応・対策支援も求められるとしている。

加えて、同提言を踏まえ、2018 年3月には「経団連サイバーセキュリティ経営宣言」を公表[12]しており、サイバー攻撃の激化が予想される 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定め、取り組むべき項目を、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・対策の実施、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及び⑤安心・安全なエコシステムの構築への貢献の5つに分けて示している。【資料 11】

[12] 「経団連サイバーセキュリティ経営宣言」（2018 年３月　日本経済団体連合会）
http://www.keidanren.or.jp/policy/2018/018.pdf

１．３ 情報開示の現状

（１）現状の情報開示手段

現在、我が国の企業の情報開示の手段に関しては、会社法[13]、金融商品取引法、有価証券上場規定等に基づく制度開示が存在する。また、企業は、これらの制度開示のほか、CSR 報告書、サステナビリティ報告書、情報セキュリティ基本方針、情報セキュリティ報告書等を通じた任意の情報開示も行うことにより、多様な情報開示に取り組んでいるところである。

以下、企業の情報開示の手段について概観する。

ア） 事業報告【制度開示】

会社法（昭和 17 年法律第 86 号）第 435 条第2項に基づき、株式会社は事業報告を作成することが義務づけられている。事業報告には、当該株式会社の状況に関する重要な事項等を記載することとされており、特に公開会社については、株式会社の現況に関する事項として、主要な事業内容、主要な営業所及び工場並びに使用人の状況、主要な借入先及び借入額、事業の経過及びその成果、資金調達や設備投資等の状況、直前三事業年度の財産及び損益の状況、重要な親会社及び子会社の状況、対処すべき課題等を記載することとされている。【資料 12】

---

[13] 「情報セキュリティ関連法令の要求事項集」（平成 23 年４月　経済産業省）においては、「会社法は、大会社と委員会設置会社について、内部統制システムの構築の基本方針を取締役会で決定すべきことを明文の義務としている（会社法第 348 条第３項第４号、第 362 条第４項第６号、第 416 条第１項第１号ホ）。これらの規定は、善管注意義務から要求される内部統制システム構築の基本方針決定義務を念のために明文にしたものである。決定すべき内部統制は、類型に分けて列挙されている。その中には、①法令等遵守体制、②損失危険管理体制、③情報保存管理体制、④効率性確保体制、⑤企業集団内部統制が含まれる（前記引用の会社法各条及び会社法施行規則第９　条第１項、第２項、第 100 条第１項、第 112 条第１項、第２項。なお、会社法の平成 26 年改正により企業集団内部統制が決定事項に含まれることが法本体で強調されるようになった。）。情報セキュリティに関するリスクが、会社に重大な損失をもたらす危険のある場合には、②の損失危険管理体制（損失の危険の管理に関する規程その他の体制をいう）に含まれる」ことを指摘している。このような基本方針の決定の概要は事業報告に記載しなければならない（会社法施行規則第 118 条２号）とされているが、これは株主にとって重要事項であるため、事業報告への記載によって株主に開示することにしたものである。事業報告は、監査役（会）（委員会設置会社では監査委員会）の監査を受ける（同法第 436 条）こととされており、その結果、決定の内容が「相当でないと認めるときは、その旨及びその理由」が、事業報告の監査に係る監査役（会）監査報告の必要的記載事項となる（同規則第 129 条第１項第５号・第 130 条第２項第２号・第 131 条第１項第２号）。
http://www.meti.go.jp/policy/netsecurity/docs/secgov/2010_JohoSecurityKanrenHoreiRequirements.pdf

イ） 有価証券報告書【制度開示】

金融商品取引法（昭和 23 年法律第 25 号）第 24 条に基づき、有価証券の発行者である会社は、事業年度ごとに、当該会社の商号、当該会社の属する企業集団及び当該会社の経理の状況その他事業の内容に関する重要な事項等について、内閣総理大臣に提出することが義務づけられている。【資料 13】

ウ） コーポレート・ガバナンス報告書【制度開示】

有価証券上場規程（平成 19 年 11 月 1 日　東京証券取引所）第 204 条第 12 項第1号等に基づき、新規上場申請者は、コーポレート・ガバナンスに関する事項について記載した報告書（コーポレート・ガバナンス報告書）を提出することとされている。また、上場後、その内容に変更があった場合は、遅滞なく変更後の報告書を提出することとされている。コーポレート・ガバナンス報告書については、コーポレート・ガバナンスに関する基本的な考え方及び資本構成、企業属性その他の基本情報等を記載することとされている。【資料 14】

エ） 適時開示【制度開示】

有価証券上場規程第 402 条等に基づき、上場会社は、剰余金の配当、株式移転、合併の決定を行った場合や災害に起因する損害又は業務遂行の過程で生じた損害が発生した場合等においては、直ちにその内容を開示することとされている。【資料 15】

オ） CSR 報告書、サステナビリティ報告書【任意開示】

CSR（企業の社会的責任）報告書は、環境や社会問題などに対して企業は倫理的な責任を果たすべきであるとするCSRの考え方に基づいて行う企業の社会的な取組をまとめた報告書であり、サステナビリティ（持続可能性）報告書とも呼ばれている。環境、労働、社会貢献などに関する情報や、事業活動に伴う環境負荷などが幅広く公表されている。

カ） 情報セキュリティ基本方針【任意開示】

情報セキュリティ基本方針は、企業や組織において実施する情報セキュリティ対策の方針や行動指針であり、社内規定といった組織全体のルールから、どのような情報資産を、どのような脅威から、どのように守るのかといった基本的な考え方、情報セキュリティを確保するための体制、運用規定、基本方針、対策基準などを具体的に記載するものである。

キ） 情報セキュリティ報告書【任意開示】

2007 年９月に経済産業省が「情報セキュリティ報告書モデル」を公表[14]しており、企業の情報セキュリティの取組の中でも社会的関心の高いものについて情報開示することにより、当該企業の取組が顧客や投資家などのステークホルダーから適正に評価されることを目指している。同モデルにおいては、①報告書の発行目的といった基礎情報、②経営者の情報セキュリティに関する考え方、③情報セキュリティガバナンス、④情報セキュリティ対策の計画・目標、⑤情報セキュリティ対策の実績・評価、⑥情報セキュリティに係る主要注力テーマ、⑦（取得している場合の）第三者評価・認証等を基本構成としている。【資料 16】

（２） 平成 28 年度 NISC 調査

NISC では、サイバーセキュリティに対する企業の意識や人材育成等について実態を把握する目的で、平成 28 年度に企業のサイバーセキュリティに関する調査を実施し、2017 年３月、その成果報告書を公表[15]している。

上場企業 225 社等[16]を対象にしたアンケート調査「サイバーセキュリティに関する情報発信の考え方について」によれば、企業の情報発信の姿勢について、「他の企業と同じレベルでできていればよい」と回答した企業が 74.1%であり、「他企業よりも積極的に情報発信する必要がある」と回答した企業は 18.1%であった。【資料 17】

また、「他企業よりも積極的に情報発信をする必要がある」と回答した企業のうち、その理由として、71.4%が「ブランド価値向上に資する」と回答しており、CSR 広報（66.7%）やリスク対応（61.9%）の一つとして実施しているとの回答が続く結果となった。

---

[14] 「情報セキュリティ報告書モデル」（2007 年９月　経済産業省）
http://www.meti.go.jp/policy/netsecurity/docs/secgov/2007_JohoSecurityReportModelRevised.pdf

[15] 「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」（2017 年　NISC）
https://www.nisc.go.jp/inquiry/pdf/kigyoutaisaku_honbun.pdf

[16] 対象企業については、2016 年 11 月１日現在の日経平均株価指数銘柄の 225 社に、調査期間中に入れ替えがあった１社を加え、226 社としている。また、有価証券報告書についての調査のみ、2016 年 11 月１日現在の日経平均株価指数銘柄の 225 社に、2013 年以降に同銘柄から外れた社を加えるとともに、2013 年度から３年間の推移を継続的に比較することができない社を除いた、計 232 社を対象としている。

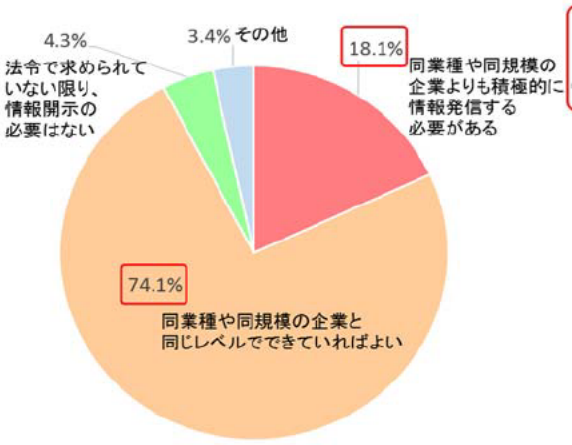


図1　サイバーセキュリティに関する情報発信の姿勢

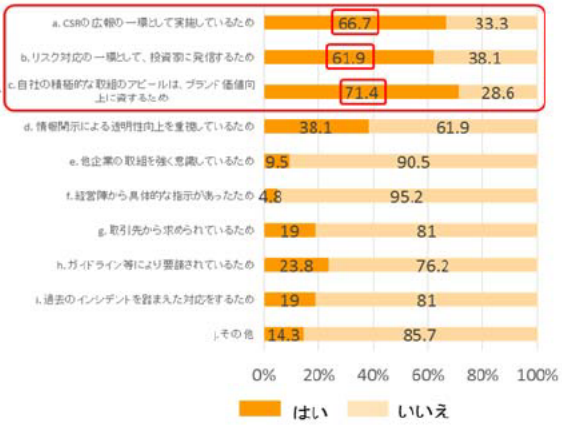


図2　積極的に情報発信を行う理由

また、同調査においては、上場企業 225 社等が平成 27 年度に発行した各種報告書の開示状況及び各種報告書におけるサイバーセキュリティに関する記述の有無について調査している。【資料 18】

本調査結果によると、サイバーセキュリティに関する記述が含まれる比率は、情報セキュリティ基本方針及び情報セキュリティ報告書（100%）を除くと、サステナビリティレポート（88%）、有価証券報告書（67%）、CSR 報告書（63%）と続いている。

一方、サイバーセキュリティに関する記述が含まれる比率が高い（a）情報セキュリティ基本方針、（b）情報セキュリティ報告書及び（c）サステナビリティレポートについては、そもそも開示している企業が少ない（226 社中開示している企業は（a）82 社、（b）5社及び（c）34 社）という結果が示された。

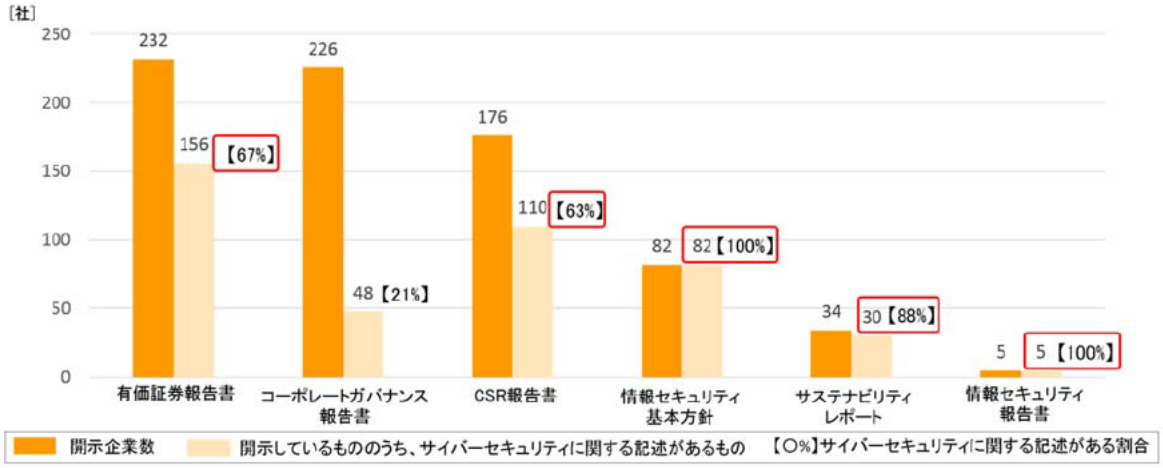


図3　各種報告書の開示状況及びそれぞれにおけるサイバーセキュリティに関する記述の有無

（3）平成 29 年度総務省調査結果

総務省では、平成 29 年度に、国内における情報開示の事例調査、情報開示に関する海外の取組の調査等を実施した。このうち、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、情報セキュリティ報告書における情報セキュリティ対策に係る記載状況（記載項目や粒度等）について調査した結果は以下のとおりである。

表1　各種報告書における情報セキュリティ対策に係る記載状況

報告書	記載状況
有価証券報告書	主に「事業等のリスク」の項目で記載されており、記載される内容は、システムの停止や機密データの漏洩等に関する概略であり、詳細な対策の内容については記載されない傾向がある。
コーポレート・ガバナンス報告書	「内部統制システム等に関する事項」の項目において、セキュリティに関するグローバルな推進体制や情報セキュリティ及び個人情報保護に関する体制を整備する等、情報セキュリティへの対策に関する管理体制の整備について記載される傾向がある。
CSR 報告書、サステナビリティ報告書	多くの企業が情報セキュリティに係る内容を報告書に記載している傾向にあり、情報セキュリティに係るリスクだけでなく、特に「セキュリティに関する基本方針等の策定状況」、「セキュリティに関する管理体制」、「社員に対する教育・人材育成」、「社外との情報共有体制」、「第三者評価・認証の取得状況」の5項目について記載される傾向がある。
情報セキュリティ報告書	経済産業省の「情報セキュリティ報告書モデル」を参考に、技術面の取組、体制の構築、マネジメントシステムについて詳細に記載されている傾向がある。

また、情報開示に関する海外の制度については、米国及び EU に共通して、投資家等が十分な情報に基づく投資判断を行うことを保証するために、事業に影響を及ぼしうるリスクについて公開することを求めている。

米国では、米国証券取引委員会（SEC：Securities and Exchange Commission）が、米国企業に対して日本の有価証券報告書にあたる Form 10-K による年次報告書の提出を求めており、Form 10-K に記載すべき Risk Factors（リスク要因）については連邦規則である Regulation S-K　Item 503(c)において、どの企業にもあてはまるような一般的な記述ではなく、リスクが当該企業あるいは投資家が取得・保有する有価証券にどのような影響を及ぼすかについて、具体的に分かり易く説明するよう求めている。

また、2011 年 10 月、米国証券取引委員会企業財務局（Division of Corporate Finance）は、サイバーインシデントに関するリスクやこれに伴う事業への影響に関する情報開示の

あり方に係るガイダンス（CF Disclosure Guidance）を策定・公表している。企業が自社特有の事実と状況を考慮しつつ、サイバーセキュリティについて何をどのような場合に開示すべきかを判断する上での手助けとなる内容となっており、Risk Factors の項について Regulation S-K の Item 503(c)に従うべきことが明記されている。

また、本ガイダンスは 2018 年2月に改訂[17]が行われたが、本改訂においては①インシデントが発生した際に正確かつ即時的に適切で有効な開示を行うため、サイバーセキュリティのリスクやインシデントに関する包括的なポリシー及び手続を確立し、維持することの重要性及び②サイバーセキュリティのリスクやインシデントに関する重要な非公開情報に基づくインサイダー取引の禁止の2点について盛り込まれている。

他方、EU では 2013 年の「EU 会計指令(2013/34/EU)」[18]、2014 年の「EU 非財務報告指令(2014/95/EU)」[19]によって、EU 加盟各国に企業の保有するリスクの情報開示を義務付けるよう求めている。指令を受けたEU加盟各国は、リスク開示に向けた国内法の制定等を行ったが、開示情報に含めるべきリスクの種類、手順等の具体的な内容等は未だ指定されていない状況である。しかし、英国財務報告評議会（FRC : Financial Reporting Council）が 2014 年6月に公表した「戦略報告書に関するガイダンス」[20]の改定案が 2017 年8月に公表[21]されており、その中で戦略報告書に記載すべきリスクとしてサイバーリスクを挙げているこ

---

17 「Commission Statement and Guidance on Public Company Cybersecurity Disclosures」（2018 年２月　米国証券取引委員会）
https://www.sec.gov/rules/interp/2018/33-10459.pdf

18 「特定種の事業の年次財務諸表、年次連結財務諸表および関連報告書に関する 2013 年 6 月 26 日付欧州議会・理事会指令 2013/34/EU (Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC Text with EEA relevance)」（2016 年６月　欧州議会・理事会）
http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32013L0034

19 「特定の大規模事業・グループの非財務情報開示に関する 2014 年 10 月 22 日付欧州議会・理事会指令 2014/95/EU (Directive 2014/95/EU of the European Parliament and of the Council of 22 October 2014 amending Directive 2013/34/EU as regards disclosure of non-financial and diversity information by certain large undertakings and groups Text with EEA relevance)」（2014 年 10 月　欧州議会・理事会）
http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32014L0095

20 「戦略報告書に関するガイダンス (Guidance on the Strategic Report)」（2014 年６月　英国財務報告評議会）
https://www.frc.org.uk/getattachment/2168919d-398a-41f1-b493-0749cf6f63e8/Guidance-on-the-Strategic-Report.pdf

21 「戦略報告書に関するガイダンス改定案 (Draft amendments to Guidance on the Strategic Report)」（2017 年８月　英国財務報告評議会）
https://www.frc.org.uk/getattachment/9e05c133-500c-4b98-9d76-497172387bea/;.aspx

とや、フランス金融市場庁（AMF：Autorité des Marchés Financiers）の報告書「2017 年リスク見通し」[22]において金融業界が重点的に取り組むべきリスクとしてサイバーリスクが掲げられる等、サイバーセキュリティに関する情報を開示する方向で、EU 加盟各国の議論が進んでいることが推察される内容となっている。

https://www.frc.org.uk/accountants/accounting-and-reporting-policy/clear-and-concise-and-wider-corporate-reporting/narrative-reporting/guidance-on-the-strategic-report

[22] 「2017 年リスクの見通し（2017 RISK OUTLOOK）」（2017 年７月　フランス金融市場庁）
http://www.amf-france.org/en_US/Publications/Lettres-et-cahiers/Risques-et-tendances/Archives?docId=workspace%3A%2F%2FSpacesStore%2F50b71ad3-51f9-403e-b884-c92ac8b4b040

第２章　民間企業におけるセキュリティ対策の情報開示のあり方

民間企業におけるセキュリティ対策の情報開示のあり方については、１．１で述べたとおり、「社内の情報共有（第一者開示）」、「契約者間等の情報開示（第二者開示）」、「社会に対する情報開示（第三者開示）」の３つの類型に分けて検討を行う。

２．１　社内の情報共有（第一者開示）のあり方

（１）経営層の理解促進

社内におけるセキュリティ対策等に係る情報共有を進め、セキュリティ対策の強化に繋げるためには、企業の経営層におけるセキュリティ対策への理解が必要不可欠である。その必要性については、前述のとおり、これまで「企業経営のためのサイバーセキュリティの考え方」（2016 年８月　NISC）や「サイバーセキュリティ経営ガイドライン　Ver.2.0」（2017 年 11 月　経済産業省・IPA）において示されてきたところであり、これらの内容を広く普及させていく取組が必要となる。

また、各企業において、CISO（最高情報セキュリティ責任者）の統括の下、セキュリティ対策の担当部署としても、経営層に気づきを与えるよう、積極的に情報開示（共有）を行うべく社内的な取組を進めることが求められる[23]。

（２）橋渡し人材等の育成の促進

より効率的に新たなセキュリティ対策の導入に繋げるためには、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」が必要となる。その必要性については、「サイバーセキュリティ人材育成プログラム」（2017 年４月 18 日 サイバーセキュリティ戦略本部決定）[24]においても示されてきたところである。また、「サイバーセキュリティ人材の育成に関する施策間ワーキンググループ報告書　～「戦略マネジメント層」の育成・定着に向けて～」（2018 年５月 31 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）[25]においては、サイバーセキュリティリスクを認識し、そのリスクに対し、

---

[23] 「上場企業における不祥事予防のプリンシプル」（2018 年　日本取引所自主規制法人）も参考になる。
http://www.jpx.co.jp/rules-participants/public-comment/detail/d10/nlsgeu000002xw82-att/preventive-principles.pdf

[24] 「サイバーセキュリティ人材育成プログラム」（2017 年　NISC）
https://www.nisc.go.jp/active/kihon/pdf/jinzai2017.pdf

[25] 「サイバーセキュリティ人材の育成に関する施策間ワーキンググループ報告書　～「戦略マ

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、経営者に報告する役割等を担う「戦略マネジメント層」について、経営層の理解の促進を含め、産業界と連携しつつ、その定着を図るとともに、カリキュラム・教材開発や学び直しプログラムを推進することとしており、引き続き、これらの人材の育成に向けた取組を進める必要がある。【資料 19】

具体的には、これらの人材に求められるスキルを具体化するとともに、こうしたスキルを取得するための教育コンテンツの開発・普及を進める他、必要に応じ、スキル認定を行う仕組みを産学官の連携により構築する方向で検討を進める必要がある。その際、社会人のリカレント教育（学び直し）の意義や重要性に関する関係者の理解を深めていく必要がある。また、各企業におけるセキュリティ人材のキャリアパスの明確化やスキルに対する評価が行われるような体制の整備が進むことが期待される。

ネジメント層」の育成・定着に向けて～」（2018 年 5 月 31 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）
http://www.nisc.go.jp/conference/cs/pdf/jinzai-sesaku2018set.pdf

２．２ 契約者間等の情報開示（第二者開示）のあり方

（１） セキュリティに配慮したサプライチェーン構築のための情報共有

サプライチェーン全体のセキュリティ対策を確保するためには、サプライチェーンを構成する契約者間において、相手方がどのようなセキュリティ対策を取っているかを確認できることが望ましい。セキュリティ対策について、自社のどういった事項を相手方に示し、また相手方に確認を求めるべきかが具体化されることによって、このような確認が円滑になされ、サプライチェーン全体のセキュリティが強化されることが望ましい。

セキュリティに配慮したサプライチェーン構築のための、契約者間で確認すべき事項や必要な対策の整理については、経済産業省の「産業サイバーセキュリティ研究会」に置かれたワーキンググループ１（制度・技術・標準化）[26]において、産業活動において必要なセキュリティ対策を示すこととしている「サイバー・フィジカル・セキュリティ対策フレームワーク」の中で、2018 年２月から議論されているところである。【資料 20】

「サイバー・フィジカル・セキュリティ対策フレームワーク」においては、「企業と企業の繋がり」、「フィジカル空間とサイバー空間の繋がり」及び「サイバー空間とサイバー空間の繋がり」の３つの切り口から、「セキュアなサプライチェーン構築のために取引先に確認すべき項目」、「セキュアなサイバー・フィジカル・セキュリティ構築に向けて必要な対策の項目」及び「セキュアなデータ連携・活用に必要な対策の項目」といった具体的な対応策を示すこととしている。

今後、「サイバー・フィジカル・セキュリティ対策フレームワーク」の策定により、企業の取組が進展し、サプライチェーン全体のセキュリティの強化に繋がることが期待される。

（２） 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

業界単位または業界横断的な枠組の中で、発生したインシデントや、その対策等について情報を共有または開示することは、当該枠組の中でのセキュリティ対策の向上に資すると考えられる。特に、サプライチェーンは様々な業種の企業によって構成されていることを踏まえると、サプライチェーン全体のサイバーセキュリティを確保するためには、業種横断的な情報共有の仕組みが必要である。また、企業毎の CSIRT[27]の取組が発展する中、グル

[26] 「産業サイバーセキュリティ研究会「ワーキンググループ１（制度、技術、標準化）」を開催します」（2018 年　経済産業省）
http://www.meti.go.jp/press/2017/02/20180202003/20180202003.html

[27] Computer Security Incident Response Team の略（シーサート）。

ープ企業間でのインシデント対応を高度化するよう、共同 CSIRT の構築を進めることも有用であると考えられる。現状では、業種毎の情報共有体制として ISAC や CEPTOAR[28]、業界横断的または地域的な情報共有体制として C4TAP[29]、J-CSIP[30]が存在しており、米国においては、ISAC 間の連携を促進するための組織として NCI（National Council of ISACs）[31]が設置されている他、情報共有の自動化を図るための AIS[32]が一部で稼働している。

こうした中、サプライチェーン全体またはグループ全体（スマートシティのような地域単位の事業者の集まりを含む。）においては、規模や業種、地域等が異なる事業者が混在しており、また費用負担等の観点から、民間の中で自発的にそのような取組が進むことは難しい面がある。このため、サプライチェーン全体やグループ全体で、様々な業種の事業者がサイバー攻撃やサイバーセキュリティに関する情報を共有する仕組みを構築する観点から、米国において取組が始まっている ISAO[33]の構築について、我が国においてもモデル事業

企業や行政機関等において、情報システム等にセキュリティ上の問題が発生していないか監視するとともに、万が一問題が発生した場合にその原因解析や影響範囲の調査等を行う体制のこと。（「サイバーセキュリティ 2017」（2017 年８月　サイバーセキュリティ戦略本部）　参考　用語解説）

[28] Capability for Engineering of Protection, Technical Operation, Analysis and Response の略（セプター）。
重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。2005 年以降順次構築が進められ、2017 年３月末現在、13 分野で 18 セプターが活動。（「サイバーセキュリティ 2017」（2017 年８月　サイバーセキュリティ戦略本部）　参考　用語解説）

[29] Ceptoar Councils Capability for Cyber Targeted Attack Protection の略。
重要インフラ事業者において、標的型攻撃が疑われるメールについての一定情報を共有することで、より多くの標的型攻撃に関する情報を収集・共有し、重要インフラサービスへの標的型攻撃の未然防止、もしくは被害軽減、サービスの維持、早期復旧を容易にすることを目指す取組み。（ＮＩＳＣ資料「標的型攻撃に関する情報共有体制（C4TAP）」
https://www.nisc.go.jp/active/infra/pdf/cc_c4tap.pdf）

[30] Initiative for Cyber Security Information sharing Partnership of Japan の略。
サイバー情報共有イニシアティブ。IPA を情報ハブ（集約点）の役割として、参加組織間で情報共有を行い、高度なサイバー攻撃対策に繋げていく取組。（「サイバーセキュリティ 2017」（2017 年８月　サイバーセキュリティ戦略本部）　参考　用語解説）

[31] 2018 年４月現在、①Automotive ISAC（自動車）、②Aviation ISAC（航空）、③Communications ISAC（通信）、④Defense Industrial Base ISAC（防衛産業）、⑤Downstream Natural Gas ISAC（天然ガス供給事業）、⑥Electricity ISAC（電力）、⑦Emergency Management And Response ISAC（危機管理）、⑧Financial Services ISAC（金融）、⑨Healthcare Ready（健康管理）、⑩Information Technology ISAC（情報技術）、⑪Maritime ISAC（海運）、⑫Multi-State ISAC（自治体）、⑬National Defense ISAC（国家防衛）、⑭National Health ISAC（国民健康）、⑮Oil & Natural Gas ISAC（石油・天然ガス）、⑯Real Estate ISAC（不動産）、⑰Research And Education Network ISAC（研究・教育）、⑱Retail Cyber Intelligence Sharing Center（陸上輸送）、⑲Surface Transportation, Public Transportation And Over-The-Road Bus ISACS（陸上輸送・公共交通・高速道路運行バス）及び⑳Water ISAC（水）の 20 の ISAC がメンバーとなっている。（https://www.nationalisacs.org/member-isacs）

[32] Automated Indicator Sharing の略。自動情報共有システム。

[33] Information Sharing and Analysis Organization の略。2015 年２月 13 日の「民間部門にお

の実施等を公的支援によって促す必要がある。

（３） サイバーセキュリティ保険の活用

「IoT セキュリティ総合対策」（2017 年 10 月）において、「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」とされていることを踏まえ、第二者開示に係る検討の一環として、サイバーセキュリティ保険についても検討を行った。

ア） サイバーセキュリティ保険の概要

サイバーセキュリティ保険は、サイバーセキュリティに起因して発生する損害（例：顧客の個人情報の漏えいに係る損害賠償、争訟費用、復旧費用、調査費用　等）の補填に加え、損害保険会社が提携している各種事業者による調査・応急対応支援、広報対応、コールセンターの設置等のセキュリティインシデント発生時に付随して必要となるサービスを提供している。各企業において、自らセキュリティ対策に適切に取り組むことを前提としつつ、それでも防ぎきれないセキュリティインシデントによって生じる損害を補償する手段として、サイバーセキュリティ保険を活用することは有用であると考えられる。【資料 21】

セキュリティ対策の情報開示（共有）とサイバーセキュリティ保険の関係について、第二者開示の観点からは、企業は損害保険会社に対して、その保険料の算定のため、告知書を通じて自社のセキュリティ対策について開示することが求められる。保険料の算定においては、被保険者となる企業においてどのくらいセキュリティ対策が実施されているかが影響することから、損害保険会社に対して自社のセキュリティ対策について適切に開示し、評価を受けることが必要となる。また、適切な開示によって、セキュリティインシデントによって生じるリスクの移転に要するコストを抑えることが可能となると同時に、定期的に損害保険会社によるリスクアセスメントを受けることになるため、自社のセキュリティ対策を見直す機会となり得る。

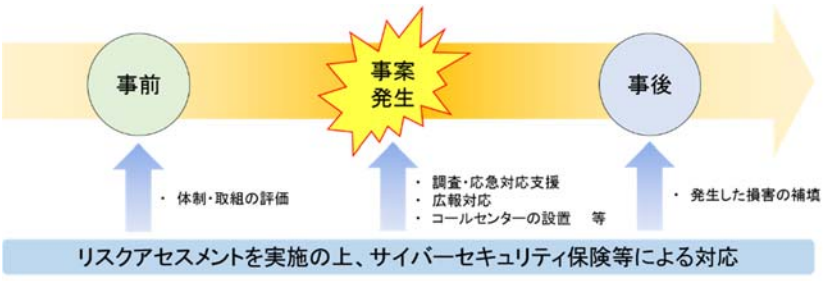


図４　サイバーセキュリティ保険の活用

けるサイバーセキュリティに係る情報共有の促進に関する大統領令」（Executive Order – Promoting Private Sector Cybersecurity Information Sharing）において、ISAO は、特定の新たな脅威や脆弱性に対応するために、セクター、サブセクター、地域、または他の一体性に基づいて組織されるとしている。

なお、第三者開示の観点からは、IPA が実施しているセキュリティ対策の自己宣言制度（SECURITY ACTION、p.24～25 参照）において、「二つ星」を宣言した企業については保険料を割り引く運用が一部の損害保険会社において既になされており、適切な開示がコストの抑制等に繋がることが考えられる。

イ） 米国におけるサイバーセキュリティ保険市場

米国におけるサイバーセキュリティ保険市場は 2002 年ころから拡大を始めている。その背景には、各州においてデータ侵害通知法（Data Breach Notification Law）が制定・施行され、企業が保有する個人情報漏えい事案に対する迅速な対応が求められるとともに、漏えいした個人情報に係る損害賠償請求等のリスクが高まったこと等があると指摘されている。また、前述の米国証券取引委員会（SEC）の情報開示のあり方に係るガイダンスが 2011 年に策定・公表されたことも、保険ニーズの更なる高まりをもたらしている。その結果、米国のサイバーセキュリティ保険市場は 2011～2015 年の間に年間約 30%の成長を遂げており、市場規模は 2015 年時点で約 15 億ドルに達している[34]。【資料 22】

これに対し、日本のサイバーセキュリティ保険市場は 2017 年度で約 156 億円にとどまっており、米国の 10 分の1程度の市場規模となっている[35]。今後、企業の情報共有や情報開示の促進とともに、サイバーセキュリティ対策を講じてもなお残存するリスクを共有し、面的な防御能力を向上させていくためにも、多様なサイバーセキュリティ保険が提供される環境整備を進めていく必要がある。

ウ） サイバーセキュリティ保険の活用の推進

サイバーセキュリティ保険は自社のセキュリティ対策で防ぐことができる範囲を超えて生じた損害を補償し、当該企業の営業活動の継続に資するものであり、セキュリティに係るリスクマネジメントの一環として、その活用について検討することは有益である。

また、高度なセキュリティ対策を短期間で導入することが難しい中小企業にとって、セキュリティインシデントによって生じうる損害を補填しつつ、可能な範囲でセキュリティ対策を進めていくために、サイバーセキュリティ保険は有用であると考えられるが、費用等の観点からその普及が進んでいない状況にある。「二つ星」を宣言した企業の事例のように、各企業のセキュリティ対策及びその開示のレベルに応じた割引制度の普及や、例えば、子会社

---

[34] 「米国におけるサイバー保険の現状」（2017 年 11 月　ジェトロ・ニューヨーク事務所）
https://www.jetro.go.jp/ext_images/_Reports/02/2017/92c65a1f1a9f3ddc/ny11201711.pdf

[35] 「2016 年度情報セキュリティ市場調査報告書　V1.1」（2017 年６月　NPO 日本ネットワークセキュリティ協会）
http://www.jnsa.org/result/2017/surv_mrk/data/2016_mrk-report_v1.1.pdf

を含むグループ全体や、下請会社を含むサプライチェーン全体で一括して加入することにより保険料の負担軽減が図られるような保険商品の展開が期待される。

エ） 中小企業等を対象とするサイバーセキュリティ保険の可能性

中小企業の場合、個社単位でサイバーセキュリティ対策を講じることは資金的・技術的に困難な場合が多い。そこでサプライチェーンを構成する企業群や同一地域に根ざした同業他社などを対象として、リスク評価サービス、セキュリティ対策に関する助言、インシデントが発生した場合の対応支援等を行うとともに、事案発生時のフォレンジック調査や顧客対応等のためのコストを損害保険によってまかなう仕組みの構築が考えられる。

また、こうした仕組みを今後各地で構築されるスマートシティの取組に活かしていくことも考えられる。スマートシティの場合、地方自治体を中心に、通信、交通、エネルギー、健康・医療・介護など様々な分野の主体がデータの収集や利用の面で協働することとなる。スマートシティによって得られるデータを窃取されたり、改ざんされたりすることがないよう、地域の関係者が一体となったサイバーセキュリティ対策を講じる上で、サイバーセキュリティ保険の枠組を活用することが考えられる。また、こうした地域における取組を ISAO の設立に繋げていくことも考えられる。

こうした取組を通じ、地域におけるサイバーセキュリティ分野への投資の拡大、情報共有体制の強化を進め、サイバーセキュリティと地域の活性化を繋ぐ取組を強化していくことが考えられる。このため、政府においては、こうした取組を地域において実現するための実証事業を今後展開し、PoC（Proof of Concept）を通じて標準仕様化を進めていくことを検討する必要がある。

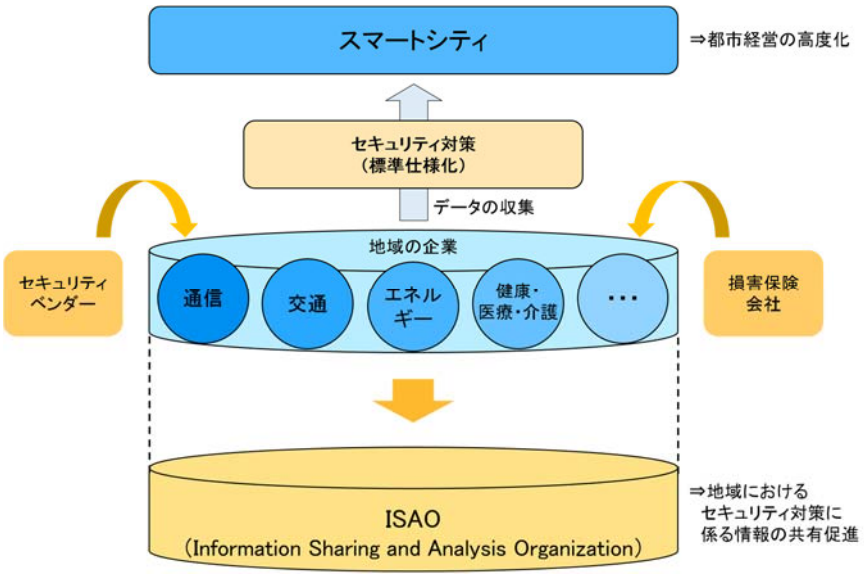


図5　地域単位の情報共有体制（ISAO）の構築の推進

オ） 今後の検討課題

こうした取組を進めるとともに、サイバーセキュリティ保険の魅力を高めるためには、サイバー攻撃事案の態様や損害額等のデータについて匿名化の上で集約する仕組みを構築し、保険料率の設定やニーズに即した商品開発が行えるような体制を構築していくことも将来の課題として今後検討していく必要があろう。サイバーセキュリティ保険の普及に向けて協調領域と競争領域を踏まえた検討を行うとともに、サイバーセキュリティ保険の前提となる各主体の対策の強化（セキュリティ対策のための投資の促進）、情報開示や情報共有の促進などを総合的な視点から進めていくことが望まれる。

２．３ 社会に対する情報開示（第三者開示）のあり方

社会に対する情報開示（第三者開示）については、事業者の規模や取組状況によって求められる対応が異なることから、「中小企業における情報開示に向けた取組」、「セキュリティ対策が非開示または限定的である事業者における情報開示」及び「既に情報開示に取り組んでいる事業者における情報開示」に分けて対策を検討する。事業の規模や取組の進展に応じて、段階的に更なる対応を講じていくこと（進捗ステージごとのマチュリティ（成熟）モデルの具体化）が望ましい。

（１） 中小企業におけるセキュリティ対策に係る情報開示に向けた取組

我が国企業の大宗を占める中小企業においては、セキュリティ対策が十分に進んでいない事業者が多いと考えられる。また、一定のセキュリティ対策を講じている事業者であっても、情報を開示するのに必要な作業に要する人員や予算が十分に確保できない状況にある。

一方で、契約の条件として一定のセキュリティ対策を講じていることが求められることが増えた場合、セキュリティ対策の不備によって契約の相手方から除外されてしまう可能性がある。また、社会全体で考えた場合、サプライチェーンを支える中小企業のセキュリティ対策に不備があると、当該事業者の被害がサプライチェーン全体に拡大することも考えられる。

したがって、引き続き、中小企業の情報システムのクラウド化を進めるとともに、実効性のあるセキュリティ対策を促進する必要があるが、セキュリティ対策に係る情報の開示にあたっては、できるだけ負担が少ない方法で行われることが望ましい。

中小企業におけるセキュリティ対策に関する取組として、IPA においては、中小企業にサイバーセキュリティ対策に係るリスクに対する意識を向上させるために、セキュリティ対策の自己宣言制度（SECURITY ACTION）の取組を 2017 年４月から開始している。IPA が公開している「中小企業の情報セキュリティ対策ガイドライン」[36]に基づき、「情報セキュリティ５か条」[37]に取り組んだ企業については「一つ星」、25 問の診断項目で構成される「５分でできる！情報セキュリティ自社診断シート」[38]で自社の状況を把握した上で、情報セキュリティポリシ

[36] 「中小企業の情報セキュリティ対策ガイドライン」（2017 年　IPA）
https://www.ipa.go.jp/files/000055520.pdf
[37] 「情報セキュリティ５か条」（2017 年　IPA）
https://www.ipa.go.jp/files/000055516.pdf
[38] 「５分でできる！情報セキュリティ自社診断シート」（2017 年　IPA）
https://www.ipa.go.jp/files/000055517.pdf

一を定め、外部に公開した企業については「二つ星」を使用することができることとされている。【資料 23、24】

当該制度は中小企業を対象としたものであり、その実施は比較的負担が軽く、簡便であることから、中小企業がセキュリティ対策の取組を始めるための端緒となるものであると考えられる。「情報セキュリティ5か条」や「5分でできる！情報セキュリティ自社診断シート」を使用することにより、必要とされているセキュリティ対策の中でまだ十分でないものが明確になり、更に必要な対策について具体的に検討することができるようになる。また、「一つ星」または「二つ星」を用いてセキュリティ対策に積極的に取り組んでいる旨を対外的に示すことにより、社会的な信用を得ることができ、契約の条件として一定のセキュリティ対策を講じていることが求められる中で、前向きな評価に繋がることが考えられる。

このため、セキュリティ対策の自己宣言制度（SECURITY ACTION）による「一つ星」や「二つ星」といったセキュリティ対策の取組状況に関する対外的な開示を引き続き促していくとともに、開示を通じてさらにセキュリティ対策が強化されることが期待される。

また、民間部門においてもセキュリティ対策の強度を簡易に判断できる評価ツールキットの開発等が進んでいるところであり、これらのツールキットを第三者が評価する仕組み等についても検討していく必要がある。

（２） セキュリティ対策が非開示または限定的である事業者における情報開示

既に一定のセキュリティ対策には取り組んでいるものの、対外的にその情報を開示していないまたは開示が限定的である企業については、セキュリティ対策に積極的に取り組んでいることが対外的にわかるような情報開示を促進することが望ましい。

セキュリティ対策を開示する媒体については、「企業経営のためのサイバーセキュリティの考え方」（2016 年８月　NISC）や「サイバーセキュリティ経営ガイドライン Ver.2.0」（2017 年 11 月　経済産業省・IPA）において、情報セキュリティ報告書、CSR報告書、サステナビリティ報告書、有価証券報告書などが挙げられている。

情報セキュリティ報告書については、図３（P12）によれば作成している企業が調査時点で 226 社中5社にとどまっており、普及していない。また、有価証券報告書については、作成する主体が上場企業のみであるため、媒体として使用する企業の範囲が限定的であり、また、「事業等のリスク」の観点からセキュリティ対策に関する記載は見受けられるが、詳細な対策について記載されている事例が少ない。

一方、CSR 報告書及びサステナビリティ報告書については、法的に策定・公表が義務づ

けられているものではないにもかかわらず、図3によれば上場企業 226 社中、CSR 報告書については 176 社が作成しており、サステナビリティ報告書については 34 社が作成している。また、それぞれの報告書においてセキュリティ対策に関する記載があるものは、CSR 報告書については 176 社中 110 社（63%）、サステナビリティレポートについては 34 社中 30 社（88%）となっている。なお、両者は各事業者においてどちらかを作成しているという実態にあるが、単純に計算すれば 226 社中 210 社がいずれかの報告書を作成しており、そのうち 140 社（67%）の報告書にサイバーセキュリティに関する記載がある。

CSR 報告書及びサステナビリティ報告書におけるセキュリティ対策に係る記載については、有価証券報告書と比較して、より具体的な記述が見られた。記載内容を分析すると、「セキュリティに関する基本方針等の策定状況」、「セキュリティに関する管理体制」、「社員に対する教育・人材育成」、「社外との情報共有体制」及び「第三者評価・認証の取得状況」の5項目に分類できる。

開示されている例が見られたセキュリティ対策主要5項目

①セキュリティに関する基本方針等の策定状況
記載例：情報セキュリティ基本方針、情報セキュリティポリシーの策定

②セキュリティに関する管理体制
記載例：情報セキュリティマネジメント体制、CSIRT の設置

③社員に対する教育・人材育成
記載例：従業員に対する研修の実施

④社外との情報共有体制
記載例：ISACや日本シーサート協議会への加盟

⑤第三者評価・認証の取得状況
記載例：情報セキュリティマネジメントシステム（ISMS）の国際規格「ISO/IEC27001:2005」及び「JISQ27001:2006」の認証を取得

上記5項目については、

- 一定程度、セキュリティ対策に積極的に取り組んでいる姿勢を示すことができる項目であること。
- 開示内容は各事項の有無や定量的な情報（例：研修の開催回数、受講者数等）であり、対外的に開示する事業者側にとっても、開示情報を見る側にとっても、技術的・専門的な知識をあまり要しないこと。
- 具体的なシステム構成、使用している機器やサービスを明示する必要がないため、

これらの情報を開示することによって生じうるシステム上の弱点が露見するおそれがなく、新たな攻撃を誘発するリスクが低いこと。

・ 他社と比較した際に自社で不足している部分が明確になり、また今後の自社の取組の参考にしやすく、他社との比較・競争による社会全体のセキュリティ対策の向上が期待できること。

等を勘案すると、セキュリティ対策を対外的に開示する項目として適切であり、現在セキュリティ対策が非開示または限定的である事業者に対して、まずは上記5項目について開示するように促すことが有効であると考えられる。

（３） 既に情報開示に取り組んでいる事業者における情報開示

ア）「情報セキュリティ報告書」の作成

先述のとおり、「情報セキュリティ報告書」は上場企業 226 社において5社しか作っておらず、普及が進んでいない状況にある。一方で、「情報セキュリティ報告書」はサイバーセキュリティに特化した単体の報告書であり、作成した事業者のセキュリティに対する考え方や体制、計画、対策等について総覧できることから、事業者がセキュリティ対策を対外的に開示する媒体として理想的なものであると考えられる。他方、こうした報告書を策定・公表することに見合うメリットが見出せないとの指摘もある。

情報開示を行う媒体については、各企業の事業規模や取組状況に応じて検討されるべきものであるが、最終的に目指すべき開示媒体の一つとして、引き続き、任意開示としての「情報セキュリティ報告書」の策定・公表を推進していくことが適当であると考えられる。その際、新たな攻撃を誘発しないように十分に配慮することも併せて求められる。

イ） セキュリティインシデントに係る情報開示

事業者が経験したセキュリティインシデントに関する情報については、その共有によって新たな被害の拡大の防止が期待されるとともに、当該インシデントを踏まえた対策の実施状況を示すことにより、株主等の関係者に対して説明責任を果たすことに繋がる。

「情報セキュリティ報告書モデル」（2007 年　経済産業省）においても、記載事項に「事故報告」が挙げられており、「IT事故に至る経緯」、「被害状況」、「影響範囲・規模（取引先、顧客、売上、企業価値、信用・評判等）」、「対応状況」、「事故原因」、「再発防止に向けた取組」を記載することとしている。また、米国の証券取引委員会（SEC）が 2011 年 10 月に公表している情報開示のあり方に係るガイダンス（CF Disclosure Guidance）においても、事業者が経験したサイバーインシデントに係る解説が適切な情報開示に含まれるとしている。

セキュリティインシデントの開示にあたっては、第二者に対するものと第三者に対するものについて、その粒度や機微情報の記載方法に留意することで、より多くの情報を開示することが可能となる。

ウ） グループ全体・サプライチェーン全体のセキュリティ対策の情報開示

既に情報開示に取り組んでいる事業者において、当該事業者自身だけではなく、グループまたはサプライチェーンを構成する上記のような中小企業のセキュリティ対策を開示することにより、当該事業者に関わる全体のセキュリティ対策に関する市場の評価が高まるとともに、グループ全体またはサプライチェーン全体のセキュリティ対策の現状を定期的に確認し、必要に応じて更なるセキュリティ対策を子会社や請負事業者に求める機会となることが考えられる。

（４） 今後の取組の方向性

以上を踏まえ、民間企業におけるセキュリティ対策の情報開示を促進するためには、「情報セキュリティ報告書」の策定・公表を最終的なゴールと位置づけつつ、企業の判断を尊重しながら、その他の情報開示のための報告書にも参照可能であり、また企業の対策における成熟度に応じた開示項目やその粒度を見据えた「セキュリティ対策情報開示ガイドライン」（仮称）を本年秋を目途に策定することが適当である。なお、本ガイドラインにおいては優良事例を盛り込み、企業が参照しやすい実践的なものとなることが期待される。

また、企業における情報開示を推進するためには、その前提として、セキュリティ関連投資を促進するための政策支援のあり方について引き続き検討していく必要がある。この点、一定のセキュリティ対策が講じられたデータ連携・利活用により生産性を向上させる投資について税額控除や特別償却を認める「コネクティッド・インダストリー税制」（平成 30 年度～平成 32 年度）が導入されることとなっており、当該税制の活用動向や企業ニーズ等を踏まえつつ、一層の投資促進のあり方について検討することが求められる。

第3章　今後の取組

本報告書を踏まえ、今後は以下の5項目の取組を中心に産学官が連携しつつ進めていくこととする。各施策の進捗状況については本分科会において定期的に検証し、追加的な課題の洗い出しを行うとともに、サイバーセキュリティタスクフォースにおける「IoT セキュリティ総合対策」のプログレスレポートに含めて公表する。

（社内の情報共有に資する橋渡し人材等の育成）

1. 企業において経営層と現場をつなぐ「橋渡し人材」等の育成に向け、これらの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・普及の他、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を進める（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. サプライチェーン全体やスマートシティ等の地域の情報共有のための情報共有体制として ISAO の構築を支援する観点から、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を行う（平成 30 年度中を目途に検討結果を取りまとめ）。

3. 上記2に関連して、サプライチェーン全体やスマートシティ等に関連する事業者はもとより、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 PoC を実施するためのモデル事業を推進し、考慮すべき事項の整理を踏まえ、標準仕様化に向けた検討を進める。また、これに関連して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についても検討を進める（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）

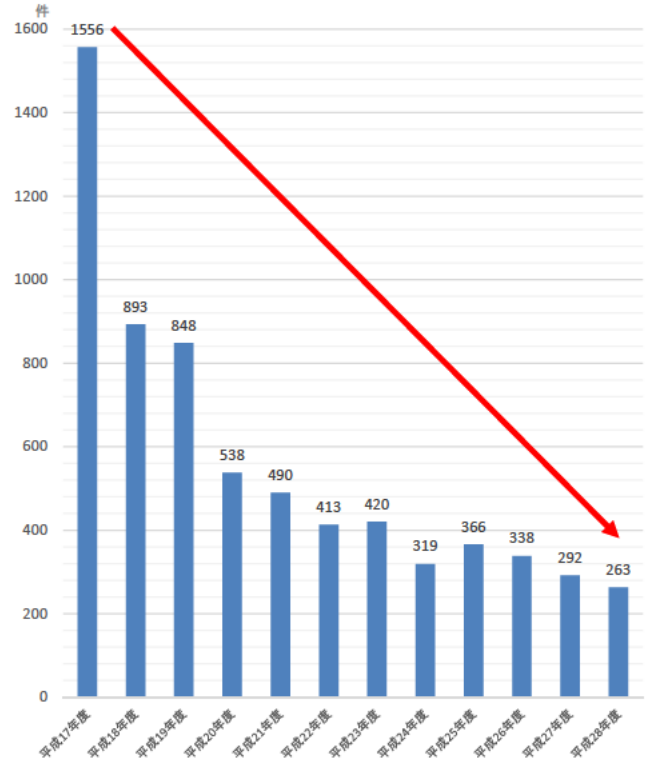
4. 民間企業におけるセキュリティ対策の情報開示を促進する観点から、「セキュリティ対策情報開示ガイドライン」（仮称）を策定・公表する。その際、企業における対策の成熟度に応じた取組ができるように配慮するとともに、優良事例を盛り込むなど、企業が参照しやすい実践的なものとなるよう検討する（平成 30 年秋を目途にガイドラインを策定）。

5. 企業におけるセキュリティ対策に係る情報開示を推進するためには、まずはセキュリティ対策そのものが促進されるような環境整備が求められることから、導入予定の「コネク

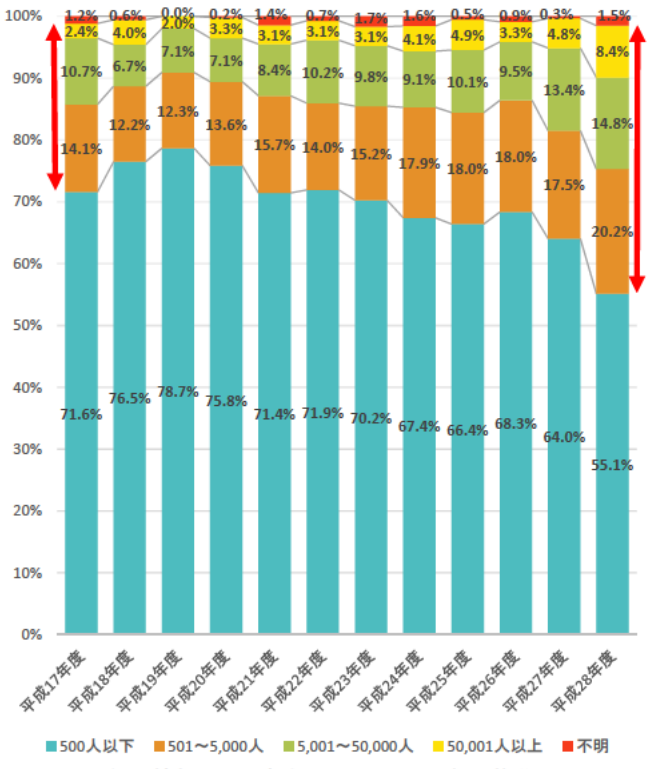
ティッド・インダストリー税制」の活用状況を分析するとともに、企業のニーズ等を反映した投資促進のための政策支援のあり方について検討する（支援税制の運用にあわせて適宜実施）。【資料 25】

参考資料

個人情報漏えい事案の発生件数及び漏えい人数の推移　【資料1】



個人情報漏えい事案の発生件数の推移



個人情報漏えい事案の漏えいした人数の推移

（出典）いずれも、毎年度個人情報保護委員会が公表している「個人情報の保護に関する法律施行状況の概要」を参考に作成。
「平成28年度個人情報の保護に関する法律施行状況の概要」（平成29年11月　個人情報保護委員会）　https://www.ppc.go.jp/files/pdf/personal_sekougaiyou_28ppc.pdf

平成28年度における主な個人情報漏えい事案　【資料2】

事業者名	所轄府省	公表日	漏えい人数（最大）	漏えいの原因
A社	経済産業省	平成28年４月11日	約20万件	不正アクセス
B社	総務省	平成28年４月21日	約43万件	不正アクセス（OSコマンドインジェクション）
C社	総務省	平成28年４月22日	約64万件	不正アクセス（OSコマンドインジェクション）
D社	経済産業省	平成28年４月27日	約13万件	不正アクセス
E社	経済産業省	平成28年４月28日	約64万件	不正アクセス
F社	経済産業省 総務省	平成28年５月11日	約5万件	不正ログイン（リスト型攻撃）
G社	総務省	平成28年６月14日	約33万件	不正アクセス
H社	国土交通省 （観光庁）	平成28年６月14日	約678万件	外部からの不正アクセス
I社	総務省	平成28年６月21日	約62万件	不正アクセス
J社	総務省	平成28年６月22日	約98万件	不正アクセス
K社	総務省	平成28年７月25日	約12万件	不正アクセス（SQLインジェクション）
L社	経済産業省	平成28年８月23日	約21万件	外付けハードディスクの紛失
M社	経済産業省 総務省	平成28年８月26日	約11万件	不正アクセス
N社	経済産業省 総務省	平成28年11月29日	約58万件	不正アクセス
O社	経済産業省	平成28年12月２日	約42万件	不正アクセス
P社	経済産業省	平成29年１月１日	約5万9千件	不正アクセス
Q社	厚生労働省	平成29年２月17日	約19万人分	紛失（誤廃棄の可能性）
R社	経済産業省	平成29年２月27日	約120万件	バックアップストレージの盗難
S社	経済産業省 総務省	平成29年３月10日	約40万件	不正アクセス
T社	経済産業省	平成29年３月10日	36万件	不正アクセス（Apache Struts2 ぜい弱性）
U社	経済産業省	平成29年３月23日	約118万件	不正アクセス
V社	経済産業省	平成29年４月25日	約15万件	不正アクセス

※平成28年度中に事業者が公表した個人情報漏えい事案（所管府省において把握したものに限る）のうち、漏えいした個人情報が50,001件以上の事案を掲載。

（出典）「平成28年度個人情報の保護に関する法律施行状況の概要」（平成29年11月　個人情報保護委員会）を参考に作成。
https://www.ppc.go.jp/files/pdf/personal_sekougaiyou_28ppc.pdf

個人情報漏えい事案の一件あたりの平均損害賠償額の経年変化　【資料3】

	一件あたりの 平均想定損害賠償額	（参考） 想定損害賠償総額
2005年	5億3,935万円	約5,329億円
2006年	4億8,156万円	約4,570億円
2007年	27億9,347万円	約2兆2,711億円
2008年	1億,8552万円	約2,367億円
2009年	2億6,683万円	約3,890億円
2010年	7,551万円	約1,215億円
2011年	1億2,810万円	約1,900億円
2012年	9,313万円	約2,133億円
2013年	1億6,575万円	約1,439億円
2014年	10億8,561万円	約1兆6,642億円
2015年	3億2,192万円	約2,527億円
2016年	6億2,811万円	約2,789億円

（出典）「情報セキュリティインシデントに関する調査報告書　第1.2版」（2017年6月14日　JNSA＆長崎県立大学）　http://www.jnsa.org/result/incident/data/2016incident_survey_ver1.2.pdf

「サイバーセキュリティ戦略」（平成27年9月4日 閣議決定）について　【資料4】

1 サイバー空間に係る認識

- サイバー空間は、「**無限の価値を産むフロンティア**」である人工空間であり、人々の経済社会の活動基盤
- あらゆるモノがネットワークに連接され、実空間とサイバー空間との融合が高度に深化した「**連接融合情報社会（連融情報社会）**」が到来
  同時に、サイバー攻撃の被害規模や社会的影響が年々拡大、脅威の更なる深刻化が予想

2 目的

- 「自由、公正かつ安全なサイバー空間」を創出・発展させ、もって「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせる社会の実現」、「国際社会の平和・安定及び我が国の安全保障」に寄与する。

3 基本原則

① 情報の自由な流通の確保　② 法の支配　③ 開放性　④ 自律性　⑤ 多様な主体の連携

4 目的達成のための施策

①後手から**先手**へ　／　②受動から**主導**へ　／　③サイバー空間から**融合**空間へ

経済社会の活力の向上及び持続的発展	国民が安全で安心して暮らせる社会の実現	国際社会の平和・安定及び我が国の安全保障
～ 費用から投資へ ～	～ 2020年・その後に向けた基盤形成 ～	～ サイバー空間における積極的平和主義 ～
■安全なIoTシステムの創出 安全なIoT活用による新産業創出	■国民・社会を守るための取組 事業者の取組促進、普及啓発、サイバー犯罪対策	■我が国の安全の確保 警察・自衛隊等のサイバー対処能力強化
■セキュリティマインドを持った企業経営の推進 経営層の意識改革、組織内体制の整備	■重要インフラを守るための取組 防護対象の継続的見直し、情報共有の活性化	■国際社会の平和・安定 国際的な「法の支配」確立、信頼醸成推進
■セキュリティに係るビジネス環境の整備 ファンドによるセキュリティ産業の振興	■政府機関を守るための取組 攻撃を前提とした防御力強化、監査を通じた徹底	■世界各国との協力・連携 米国・ASEANを始めとする諸国との協力・連携

横断的施策

- ■研究開発の推進
  攻撃検知 防御能力向上(分析手法 法制度を含む)のための研究開発
- ■人材の育成・確保
  ハイブリッド型人材の育成、実践的演習、突出人材の発掘 確保、キャリアパス構築

5 推進体制

- 官民及び関係省庁間の連携強化、オリンピック・パラリンピック東京大会等に向けた対応

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2日 内閣サイバーセキュリティセンター）①【資料5】

企業が自発的に行うサイバーセキュリティの取組が促進されるよう、企業経営のためのサイバーセキュリティに係る基本的考え方とともに、経営層に期待される"認識"や経営戦略を企画する人材層に向けた実装のためのツールを示す。
※普及啓発・人材育成専門調査会の下に設置された、「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」（主査：林紘一郎 情報セキュリティ大学院大学教授）を通じ、検討を実施。

基本方針　ーサイバーセキュリティは、より積極的な経営への「投資」へー

グローバルな競争環境の変化
- ITの発展によるビジネスの変革が、消費者向けのビジネスから企業間取引へと拡大
- サイバー空間と実空間の融合がさらに進み、チャンスもリスクも一層増大

サイバーセキュリティをやむを得ない「費用」でなく、積極的な経営への「投資」と位置づけ、企業としての「挑戦」と、それに付随する「責任」として取り組むことが期待される

I.基本的考え方

二つの基本的認識

<①挑戦>
サイバーセキュリティは、利益を生み出し、ビジネスモデルを革新するものであり、新しい製品やサービスを創造するための戦略の一環として考えていく必要がある。

<②責任>
全てがつながる社会において、サイバーセキュリティに取り組むことは社会的な要求・要請であり、自社のみならず社会全体の発展にも寄与することとなる。

三つの留意事項

<①情報発信による社会的評価の向上>
- 「セキュリティ品質」を高め、品質向上に有効な経営基盤の一つとしてセキュリティ対策を位置付けることで企業価値を高めることが必要。
- そのような取組に係る姿勢や方針を情報発信することが重要。

<②リスクの一項目としてのサイバーセキュリティ>
- 提供する機能やサービスを全うする（機能保証）という観点から、リスクの一項目としてのサイバーセキュリティの視点も踏まえ、リスクを分析し、総合的に判断。
- 経営層のリーダーシップが必要。

<③サプライチェーン全体でのサイバーセキュリティの確保>
- サプライチェーンの一部の対策が不十分な場合でも、自社の重要情報が流出するおそれあり。
- 一企業のみでの対策には限界があるため、関係者間での情報共有活動への参加等が必要。

（参考）「企業経営のためのサイバーセキュリティの考え方」（2016年8月 NISC）　https://www.nisc.go.jp/active/kihon/pdf/keiei.pdf

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2日　内閣サイバーセキュリティセンター）②

II.企業の視点別の取組

企業が投資すべき対象や経営リスクは様々であり、各企業の人的・金銭的資源にも限りがあることから、ITの利活用やサイバーセキュリティへの取組において、各企業の事業規模のみならず、その認識の違いなどを踏まえて取り組んでいく必要がある。

ITの利活用を事業戦略上に位置づけ、サイバーセキュリティを強く意識し、積極的に競争力強化に活用しようとしている企業 （積極的にITによる革新と高いレベルのセキュリティに挑戦するあらゆる企業）	【経営者に期待される認識】 • 積極的なITの利活用を推進する中で、製品やサービスの「セキュリティ品質」を一層高め、自社のブランド価値の向上につなげるべく、システムの基盤におけるセキュリティの向上、情報・データの保護、製品等の安全品質向上に取り組む。 • 様々な関係者との協働が重要であるため、情報提供に主体的に取り組む。 • 決して現存する標準や取り組みなどに満足することなく、実空間とサイバー空間の融合が高度に深化した明日の世界をリードし、変革していく存在となることが期待される。 【実装に向けたツール】 • IoTセキュリティに関するガイドライン（「IoTセキュリティのための一般的枠組」等） • 自社のブランド価値としてのサイバーセキュリティに係る積極的な情報発信
IT・セキュリティをビジネスの基盤として捉えている企業 （IT・サイバーセキュリティの重要性は理解しているものの、積極的な事業戦略に組み込むところまでは位置づけていない企業）	【経営者に期待される認識】 • 経営者のリーダーシップによって、社会的責任としてのサイバーセキュリティ対策に取り組む。 • サプライチェーンやビジネスパートナー、委託先を含めた対策を行う。 • 平時・緊急時のいずれにおいても、情報開示などの適切なコミュニケーションを行う。 【実装に向けたツール】 • サイバーセキュリティ経営ガイドライン • 企業等がセキュリティ対策に取り組む上での保険等のリスク管理手法の活用 • サイバーセキュリティを経営上の重要課題として取り組んでいることの情報発信
自らセキュリティ対策を行う上で、事業上のリソースの制約が大きい企業 （主に中小企業等でセキュリティの専門組織を保持することが困難な企業）	【経営者に期待される認識】 • サプライチェーンを通じて中小企業等の役割はますます重要となる中、消費者や取引先との信頼関係醸成の観点から経営者自らサイバーセキュリティ対策に関心を持ち、取り組む。 • 外部の能力や知見を活用しつつ、効率的に進める方策を検討する。 【実装に向けたツール】 • 効率的なセキュリティ対策のためのサービスの利用（中小企業向けクラウドサービス等） • サイバーセキュリティに関する相談窓口やセミナー、地域の相談員等の活用

サイバーセキュリティ経営ガイドライン　Ver.2.0（平成29年11月16日　経済産業省、独立行政法人　情報処理推進機構）【資料6】

- 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）経営者が、**リーダーシップを取って対策**を進めることが必要
（２）自社のみならず、**ビジネスパートナーを含めた対策**が必要
（３）平時及び緊急時のいずれにおいても、**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
（１）組織全体での対策方針の策定
（２）方針を実装するための体制の構築
（３）予算・人材等のリソース確保

インシデントに備えた体制構築
（７）緊急対応体制の構築
（８）復旧体制の構築

リスクの特定と対策の実装
（４）リスクを洗い出し、計画の策定
（５）リスクへの対応
（６）PDCAの実施

サプライチェーンセキュリティ
（９）サプライチェーンセキュリティの確保

関係者とのコミュニケーション
（10）情報共有活動への参加

（参考）「サイバーセキュリティ経営ガイドラインVer2.0」（2017年11月　経済産業省・IPA）　http://www.meti.go.jp/press/2017/11/20171116003/20171116003-1.pdf

サイバーセキュリティ対策の強化に向けた提言（概要）（2015年2月　日本経済団体連合）【資料7】

世界中でサイバー攻撃による被害が深刻化、わが国では対策を強化。国民生活や経済活動に支障が生じるおそれがある重要インフラ等のサイバーセキュリティ対策の強化に向けて提言。

1. 国内外の情勢

(1)**国際情勢**
2012年にイギリスのロンドンオリンピック、昨年末に米国でサイバー攻撃が発生。
(2)**国内情勢**
サイバー攻撃の件数は増加傾向。サイバーセキュリティ基本法の成立やサイバーセキュリティ戦略本部の設置。2020年の東京オリンピック・パラリンピックにおける対策が急務。

2. サイバー攻撃の脅威

情報通信、金融、鉄道、電力、ガスなどが停止すれば、国家の機能維持が困難。
（1）**サイバー攻撃の特徴**　　攻撃者の特定が困難。攻撃者が常に優位な立場。
（2）**サイバー攻撃への対処**　　全ての攻撃を防ぐことは困難で、被害の極小化が重要。
（3）**攻撃対象の拡大**　　情報システムに加え制御システム、スマートフォンなども攻撃対象。

3. 重要インフラ等に対するサイバーセキュリティ対策

政府は重要インフラ等をサイバー攻撃から守ることを明確にし、抑止力を向上させる必要。
（1）**具体的施策**
①**情報共有の強化**
サイバー攻撃に関する多数の会議体の情報共有体制の強化。被害、対応、予防等に関する官民の具体的な情報共有方法の検討。
②**演習の実施等**
大規模なサイバー攻撃に対する判断基準や指針の整備、官民合同の訓練・演習の実施。
③**技術開発とシステム運用**
事前探知と攻撃の無効化、探知と追跡、情報共有などの技術開発。第5期科学技術基本計画への盛り込み。優れた防御システムの継続的運用と能力向上。
④**人材育成の強化**
トップ人材やホワイトハッカーなどの育成、産学官連携によるセキュリティ人材の質と量の充足。
⑤**国際連携の推進**
海外との情報共有。攻撃者を追跡、特定し、対処する国際的な仕組みの検討。国際会議の開催。
⑥**重要インフラ分野の見直し**
現在の13分野の見直し。スマートシティやITSなど新たなネットワーク系サービスの追加の検討。
⑦**インターネットの安全性の向上**
インターネットの利用者の知見の向上。
(2)**政府の体制整備**
内閣官房に情報集約機能を一元化。サイバーセキュリティ戦略本部のリーダーシップの発揮。

4. 産業界の取組み

産業界は、サイバーセキュリティを経営上の重要課題として、経営層の意識改革、組織改革や人材育成、業種間の情報交流や意見交換を促進。
大学・大学院のセキュリティ講座を企業が支援。こうした取組みにより国家のサイバーセキュリティが向上。

（出典）「サイバーセキュリティ対策の強化に向けた提言」（2015年2月　日本経済団体連合会）を参考に作成。　http://www.keidanren.or.jp/policy/2015/017_honbun.pdf

サイバーセキュリティ対策の強化に向けた第二次提言（概要）（2016年1月　日本経済団体連合）【資料8】

1. はじめに

■わが国では、昨年1月にサイバーセキュリティ基本法の施行やサイバーセキュリティ戦略本部の発足など政府の推進体制が強化。
■一方、政府機関や企業に対するサイバー攻撃が増加。昨年5月に日本年金機構から個人情報が流出。
■サイバー空間はイノベーション創出により成長戦略を実現する重要な場。2020年の東京オリンピック・パラリンピックに向け重大な局面。
昨年9月に政府はサイバーセキュリティ戦略を閣議決定。
■産学官の連携強化と経済界の具体的な取り組みについて、経団連として第二次提言をとりまとめ。

2. サイバーセキュリティの意義

■公的機関（中央省庁、独立行政法人、特殊法人等）における総合的な対策の強化。マイナンバー制度の導入により、地方公共団体を含めた対策の充実。
■インターネットに接続するIoT（Internet of Things）の安全な利用。
■サイバー攻撃により企業の事業活動への支障や、情報漏洩による信用の毀損等のリスクへの対応。
■サイバー空間における国際的に自由な情報の流通の確保。

3. サイバーセキュリティ対策

(1)**情報共有**
政府機関と企業による双方向の情報共有。ISAC(情報共有・分析機関）やCSIRT（セキュリティ事案対処チーム）などの業界や企業における設置。
機密情報を保全した情報提供。
(2)**人材育成**
人材の要件の明確化。大学等における人材レベルに応じた教育。
企業における評価や処遇の見直し。産学官による人材育成と維持のシステムの構築。
(3)**セキュリティレベルの高いシステムの構築**
①**社会システム**
重要インフラの重点的な防護、範囲の見直し。高度人材が産学官で柔軟に動ける仕組みの構築。
②**技術開発とシステム運用**
通信検知や攻撃解析などの技術開発。システムの安定的な稼働。内閣府の戦略的イノベーション創造プログラムやIoT推進コンソーシアムの活動への期待。
(4)**国際連携の推進**
国際的な議論への積極的な参画。米国、欧州、ASEANなどとの連携。
(5)**東京オリンピック・パラリンピックへの対応**
大会会場に加えて周辺施設等を含めた総合的な対策の実施。中核となるCSIRTの早期設置。演習・訓練の実施。既存の人材の能力向上。
NISC（内閣サイバーセキュリティセンター）を中心とした体制整備や対策のロードマップの策定と実行。

4. 産業界の取組み

サイバーセキュリティの確保を経営上の重要項目として位置づけ、経営層の意識を改革。組織・体制の整備、情報共有、人材育成を自主的かつ迅速に推進。
ステークホルダーへの自主的な情報開示。セキュリティが確保されたシステムの開発や製品の提供。サイバーセキュリティ保険の提供。

（出典）「サイバーセキュリティ対策の強化に向けた第二次提言」（2016年1月　日本経済団体連合会）を参考に作成。　http://www.keidanren.or.jp/policy/2016/006_honbun.pdf

企業行動憲章　―持続可能な社会の実現のために―

（1991年9月制定、2017年11月　第5回改定　日本経済団体連合会）　【資料9】

企業は、公正かつ自由な競争の下、社会に有用な付加価値および雇用の創出と自律的で責任ある行動を通じて、持続可能な社会の実現を牽引する役割を担う。そのため企業は、国の内外において次の10原則に基づき、関係法令、国際ルールおよびその精神を遵守しつつ、高い倫理観をもって社会的責任を果たしていく。

（持続可能な経済成長と社会的課題の解決）
1. イノベーションを通じて社会に有用で安全な商品・サービスを開発、提供し、持続可能な経済成長と社会的課題の解決を図る。

（公正な事業慣行）
2. 公正かつ自由な競争ならびに適正な取引、責任ある調達を行う。また、政治、行政との健全な関係を保つ。

（公正な情報開示、ステークホルダーとの建設的対話）
3. 企業情報を積極的、効果的かつ公正に開示し、企業をとりまく幅広いステークホルダーと建設的な対話を行い、企業価値の向上を図る。

（人権の尊重）
4. すべての人々の人権を尊重する経営を行う。

（消費者・顧客との信頼関係）
5. 消費者・顧客に対して、商品・サービスに関する適切な情報提供、誠実なコミュニケーションを行い、満足と信頼を獲得する。

（働き方の改革、職場環境の充実）
6. 従業員の能力を高め、多様性、人格、個性を尊重する働き方を実現する。また、健康と安全に配慮した働きやすい職場環境を整備する。

（環境問題への取り組み）
7. 環境問題への取り組みは人類共通の課題であり、企業の存在と活動に必須の要件として、主体的に行動する。

（社会参画と発展への貢献）
8.「良き企業市民」として、積極的に社会に参画し、その発展に貢献する。

（危機管理の徹底）
9. 市民生活や企業活動に脅威を与える反社会的勢力の行動やテロ、サイバー攻撃、自然災害等に備え、組織的な危機管理を徹底する。

（経営トップの役割と本憲章の徹底）
10. 経営トップは、本憲章の精神の実現が自らの役割であることを認識して経営にあたり、実効あるガバナンスを構築して社内、グループ企業に周知徹底を図る。あわせてサプライチェーンにも本憲章の精神に基づく行動を促す。また、本憲章の精神に反し社会からの信頼を失うような事態が発生した時には、経営トップが率先して問題解決、原因究明、再発防止等に努め、その責任を果たす。

（出典）「企業行動憲章」（2017年11月　日本経済団体連合会）を参考に作成。 http://www.keidanren.or.jp/policy/cgcb/charter2017.pdf

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（2017年　日本経済団体連合）【資料10】

＜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「Society5.0」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
- Society5.0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を推進～

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

（出典）「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」（2017年　日本経済団体連合会）を参考に作成。 http://www.keidanren.or.jp/policy/2017/103_honbun.pdf

経団連サイバーセキュリティ経営宣言（2018年3月　日本経済団体連合）　【資料11】

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。

（参考）「経団連サイバーセキュリティ経営宣言」（2018年3月　日本経済団体連合会）を参考に作成。 http://www.keidanren.or.jp/policy/2018/018.pdf

情報開示手段に係る関連条文抜粋①　【資料12】

1．事業報告関連

○会社法（昭和17年法律第86号）
第四百三十五条　（略）
２　株式会社は、法務省令で定めるところにより、各事業年度に係る計算書類（貸借対照表、損益計算書その他株式会社の財産及び損益の状況を示すために必要かつ適当なものとして法務省令で定めるものをいう。以下この章において同じ。）及び事業報告並びにこれらの附属明細書を作成しなければならない。
３及び４　（略）

○会社法施行規則（平成18年法務省令第12号）
第百十八条　事業報告は、次に掲げる事項をその内容としなければならない。
一　当該株式会社の状況に関する重要な事項（計算書類及びその附属明細書並びに連結計算書類の内容となる事項を除く。）
二～五　（略）

（公開会社の特則）
第百十九条　株式会社が当該事業年度の末日において公開会社である場合には、次に掲げる事項を事業報告の内容に含めなければならない。
一　株式会社の現況に関する事項
二～四　（略）

（株式会社の現況に関する事項）
第百二十条　前条第一号に規定する「株式会社の現況に関する事項」とは、次に掲げる事項（当該株式会社の事業が二以上の部門に分かれている場合にあっては、部門別に区別することが困難である場合を除き、その部門別に区別された事項）とする。
一　当該事業年度の末日における主要な事業内容
二　当該事業年度の末日における主要な営業所及び工場並びに使用人の状況
三　当該事業年度の末日において主要な借入先があるときは、その借入先及び借入額
四　当該事業年度における事業の経過及びその成果
五　当該事業年度における次に掲げる事項についての状況（重要なものに限る。）
　イ　資金調達
　ロ　設備投資
　ハ～ヘ　（略）
六　直前三事業年度（当該事業年度の末日において三事業年度が終了していない株式会社にあっては、成立後の各事業年度）の財産及び損益の状況
七　重要な親会社及び子会社の状況
八　対処すべき課題
九　前各号に掲げるもののほか、当該株式会社の現況に関する重要な事項
２及び３　（略）

情報開示手段に係る関連条文抜粋②

【資料13】

2. 有価証券報告書関連

○金融商品取引法（昭和23年法律第25号）

第二十四条　有価証券の発行者である会社は、その会社が発行者である有価証券（特定有価証券を除く。次の各号を除き、以下この条において同じ。）が次に掲げる有価証券のいずれかに該当する場合には、内閣府令で定めるところにより、事業年度ごとに、当該会社の商号、当該会社の属する企業集団及び当該会社の経理の状況その他事業の内容に関する重要な事項その他の公益又は投資者保護のため必要かつ適当なものとして内閣府令で定める事項を記載した報告書（以下「有価証券報告書」という。）を、内国会社にあつては当該事業年度経過後三月以内（やむを得ない理由により当該期間内に提出できないと認められる場合には、内閣府令で定めるところにより、あらかじめ内閣総理大臣の承認を受けた期間内）、外国会社にあつては公益又は投資者保護のため必要かつ適当なものとして政令で定める期間内に、内閣総理大臣に提出しなければならない。（略）

２～１５　（略）

情報開示手段に係る関連条文抜粋③

【資料14】

3. コーポレート・ガバナンス報告書関連

○有価証券上場規程（平成19年11月１日　東京証券取引所）

（新規上場申請に係る提出書類等）

第２０４条　（略）

２～１０　（略）

１１　本則市場へ新規上場申請を行う新規上場申請者は、当取引所が新規上場申請に係る株券等の上場を承認した場合には、次の各号に掲げる書類を提出し、第２号に掲げる書類を上場前及び上場後において当取引所が公衆の縦覧に供することに同意するものとする。

（１）及び（２）　（略）

１２　前項に規定する場合において、次の各号に掲げる新規上場申請者は、当該各号に定める書類を提出し、当該書類を上場前及び上場後において当取引所が公衆の縦覧に供することに同意するものとする。

（１）内国株券等及び当取引所を主たる市場とする外国株券等の新規上場申請を行う新規上場申請者
　　施行規則で定めるコーポレート・ガバナンスに関する事項について記載した報告書

（２）（略）

（コーポレート・ガバナンスに関する報告書）

第４１９条　上場会社（その発行する上場外国株券等が当取引所以外を主たる市場とする上場外国会社を除く。）は、施行規則で定めるコーポレート・ガバナンスに関する事項について記載した報告書の内容に変更が生じた場合には、遅滞なく変更後の報告書を提出するものとする。この場合において、当該上場会社は、当該変更後の報告書を当取引所が公衆の縦覧に供することに同意するものとする。

２　（略）

○有価証券上場規程施行規則（平成19年11月１日　東京証券取引所）

（上場承認時の提出書類）

第２１１条　（略）

２及び３　（略）

４　規程第２０４条第１２項第１号に規定する施行規則で定めるコーポレート・ガバナンスに関する事項とは、次の各号に掲げる事項をいう。ただし、第２号及び第６号にあっては、新規上場申請者が内国株券の発行者である場合に限る。

（１）コーポレート・ガバナンスに関する基本的な考え方及び資本構成、企業属性その他の新規上場申請者に関する基本情報（支配株主を有する場合は、当該支配株主との取引等を行う際における少数株主の保護の方策に関する指針を含む。）

（２）～（７）　（略）

情報開示手段に係る関連条文抜粋④

【資料15】

4. 適時開示関連

○有価証券上場規程（平成19年11月１日　東京証券取引所）
（会社情報の開示）
第４０２条　上場会社は、次の各号のいずれかに該当する場合（施行規則で定める基準に該当するものその他の投資者の投資判断に及ぼす影響が軽微なものと当取引所が認めるものを除く。）は、施行規則で定めるところにより、直ちにその内容を開示しなければならない。
（１）上場会社の業務執行を決定する機関が、次のａからａｒまでに掲げる事項のいずれかを行うことについての決定をした場合
（当該決定に係る事項を行わないことを決定した場合を含む。）
ａ～ｇ　（略）
ｈ　剰余金の配当
ｉ　（略）
ｊ　株式移転
ｋ　合併
ｌ～ａｒ　（略）
（２）次のａからｘまでに掲げる事実のいずれかが発生した場合
ａ　災害に起因する損害又は業務遂行の過程で生じた損害
ｂ～ｘ（略）

情報セキュリティ報告書モデル（平成19年　経済産業省）

【資料16】

》企業の情報セキュリティの取組みの中でも社会的関心の高いものについて情報開示することにより、当該企業の取組みが顧客や投資家などのステークホルダーから適正に評価されることを目指す。
》不要な情報まで開示してしまうことがないよう若干の配慮が必要。

情報セキュリティ報告書の記載項目（フルセット）

①基礎情報
- 報告書の発行目的
- 利用上の注意
- 対象期間、責任部署等

②経営者の情報セキュリティに関する考え方
- 企業の情報セキュリティに関する取り組み方針
- 対象範囲対象範囲
- 報告書におけるステークホルダーの位置付け、ステークホルダーに対するメッセージ

③情報セキュリティガバナンス
- 情報セキュリティマネジメント体制（責任の所在、組織体制、コンプライアンス等）
- 情報セキュリティに関わるリスク
- 情報セキュリティ戦略

④情報セキュリティ対策の計画、目標
- アクションプラン
- 数値目標（対策ベンチマークのスコア等）

⑤情報セキュリティ対策の実績、評価
- 計画に対する実績、評価
- 事故報告

⑥情報セキュリティに係る主要注力テーマ
- ✓ 特に強調したい取組み、テーマを選択し、その状況を紹介（例：個人情報保護、事業継続計画等）

⑦第三者評価・認証
- ✓ 第三者評価・認証に係る取り組み
  - 認証の取得状況(ISMS、プライバシーマーク)
  - 情報セキュリティ監査の実施状況　等

- ✓ 記載項目の選択や記載内容のレベルは企業が自社の事情に応じて選択可能
- ✓ 他の報告書の一部として組み込む形もありうるし、単体の報告書という形もありうる

情報セキュリティ報告書（参考）「情報セキュリティ報告書モデル」（2007年９月　経済産業省）　http://www.meti.go.jp/policy/netsecurity/docs/secgov/2007_JohoSecurityReportModelRevised.pdf

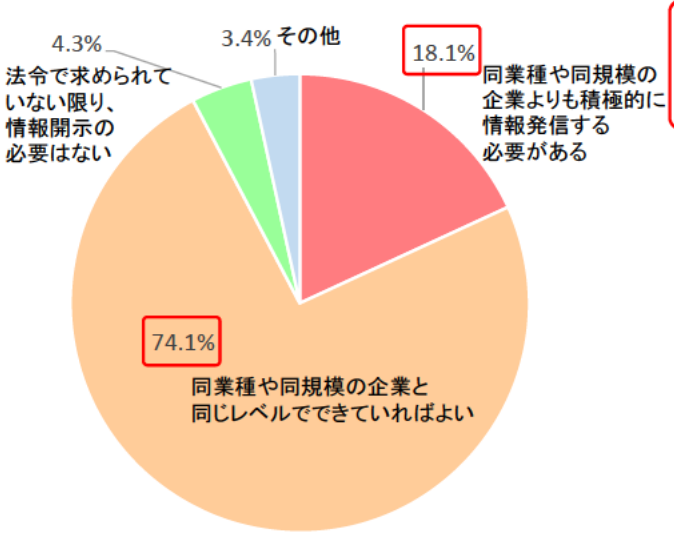
民間企業におけるサイバーセキュリティに関する情報発信に対する認識【資料17】

○ 内閣サイバーセキュリティセンターにおいては、上場企業225社等を対象にサイバーセキュリティに関する情報発信の考え方について、アンケート調査を実施している。

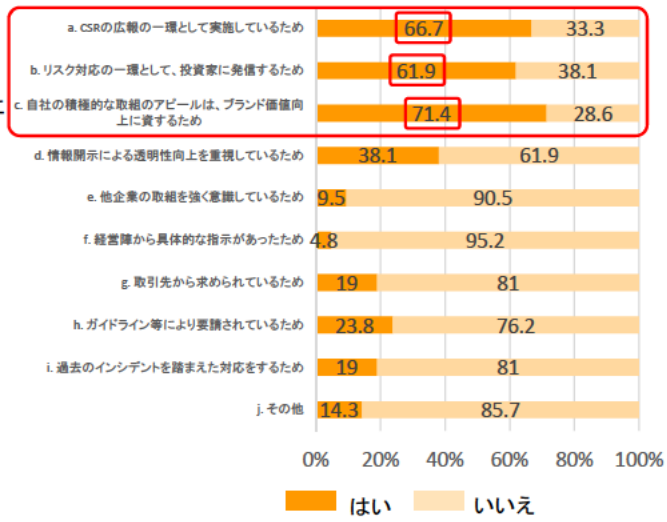
○ 情報発信の姿勢について、他の企業と同じレベルでできていればよいと回答した企業が74.1%であり、他企業よりも積極的に情報発信をする必要があると回答した企業は18.1%となっている。

○ 他企業よりも積極的に情報発信をする必要があると回答した企業のうち、その理由として、71.4%がブランド価値向上に資すると回答しており、CSR広報の一つやリスク対応の一つとして実施しているとの回答が続いている（それぞれ66.7%、61.9%）。

サイバーセキュリティに関する情報発信の姿勢



積極的に情報発信を行う理由



（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」（NISC）を参考に作成　https://www.nisc.go.jp/inquiry/pdf/kaiji_honbun.pdf

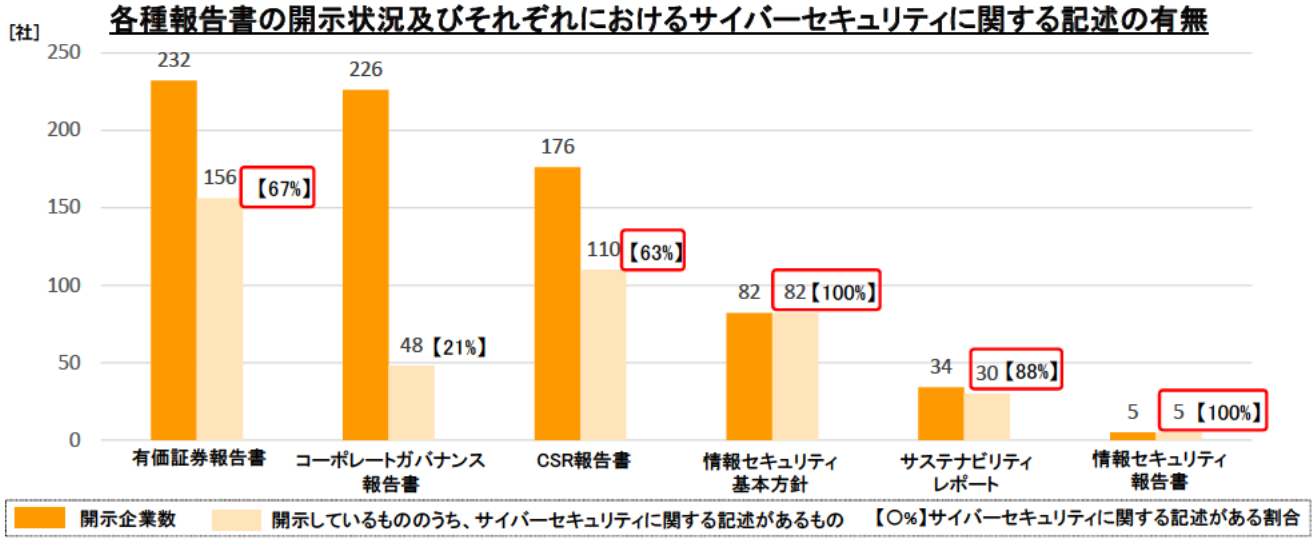
民間企業におけるセキュリティ対策に関する情報開示の実態【資料18】

○ 同調査においては、上場企業226社が平成27年度に発行した各種報告書の開示状況及びそれぞれにおけるサイバーセキュリティに関する記述の有無についても調査している。

○ サイバーセキュリティに関する記述が含まれる比率は、100%となっている情報セキュリティ基本方針及び情報セキュリティ報告書を除くと、サステナビリティレポート（88%）、有価証券報告書（67%）、CSR報告書（63%）と続いている。

○ 一方で、サイバーセキュリティに関する記述が含まれる比率が高い情報セキュリティ基本方針、情報セキュリティ報告書及びサステナビリティレポートについては、そもそも開示している企業が少ない（226社中、開示している社数はそれぞれ82社、5社、34社）。

各種報告書の開示状況及びそれぞれにおけるサイバーセキュリティに関する記述の有無



（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」（NISC）を参考に作成　https://www.nisc.go.jp/inquiry/pdf/kaiji_honbun.pdf

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18日 サイバーセキュリティ戦略本部決定）【資料19】

現状と課題

○脅威は更に深刻化、これまでの人材育成の取組は一定の成果を得つつも専門性を高める取組等一層の充実が必要。
○ ITの利活用により、新しい価値を創造するビジネスイノベーションと一体となったサイバーセキュリティへの取組が必要。
→ビジネスにおけるそれぞれの役割の中で、サイバーセキュリティ全体を俯瞰でき、関連するサイバーセキュリティを実践できる人材の育成が必要。
○ビジネスイノベーションを生み出せるサイバーセキュリティ人材の育成が必要。また、将来的な社会変化に対応するため、セキュリティに対する意識を若年層から高めることが必要。

今後の取組方針

【基本方針】　需要（雇用）と供給（教育）の好循環の形成

○これまでの取組に加え、ITの利活用により新たな価値を創造するためのサイバーセキュリティ人材育成が必要。
・経営層：サイバーセキュリティを実務者層だけの問題ではなく経営問題としてとらえるとともに、新たな価値の創造という「挑戦」に付随する「責任」としてサイバーセキュリティに取り組むという意識改革を図る。
・橋渡し人材層：経営層・実務者層のコーディネーターにとどまらず、ビジネス戦略と一体となってサイバーセキュリティの企画・立案を行い、実務者層を指揮できる橋渡し人材層の育成に取り組む。
・実務者層：情報セキュリティ技術に関する知識・能力の向上だけでなく、チームとなってサイバーセキュリティを推進するための人材育成に取り組む。
・高度人材（高等教育段階を含む）：高度なセキュリティ技術の専門性を持ちつつ、ビジネスイノベーションを創出する高度人材の育成に取り組む。
・初等中等教育段階：児童生徒の情報活用能力（プログラミング的思考や情報セキュリティ、情報モラルを含む）を培う。

○これまでの取組と新たな取組の質的向上を図るため、施策間連携の場をつくり、具体化（例：モデルとなるカリキュラムの策定）を図る。

まとめ（今後の検討）

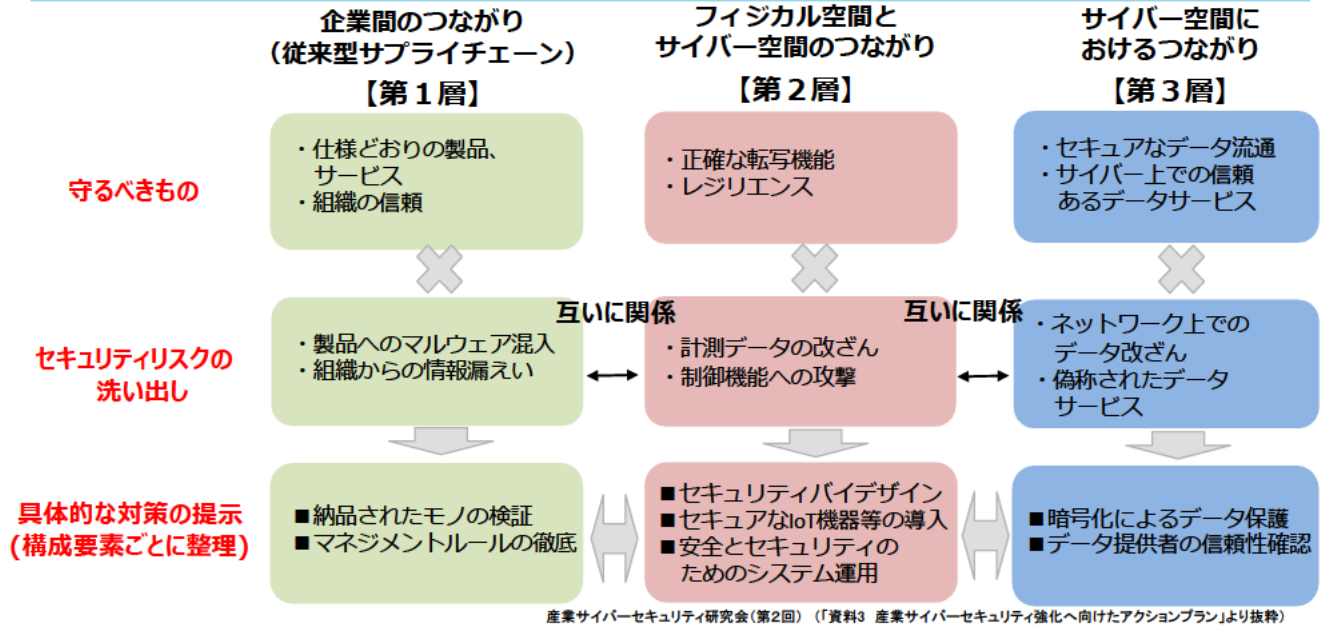
産学官の取組状況や施策間連携の検討状況、サイバーセキュリティ人材をとりまく課題について、フォローアップを行い、必要に応じて本プログラムの見直しを検討。

（参考）「サイバーセキュリティ人材育成プログラム」（2017年　NISC）　https://www.nisc.go.jp/active/kihon/pdf/jinzai2017.pdf

『サイバー・フィジカル・セキュリティ対策フレームワーク』　【資料20】

Society5.0/Connected Industriesの進展に対応した『サイバー・フィジカル・セキュリティ対策フレームワーク』の策定

- Society5.0、Connected Industriesの進展によって**複雑化していくサプライチェーンのサイバーリスクに対応する新たな対策フレームワーク**の原案を作成。
- IoTやビッグデータの活用などに伴う新たなリスクに対応するため、**産業社会を三層（企業間、フィジカル-サイバー、サイバー空間）に分類した新たなアプローチ**を提示。



産業サイバーセキュリティ研究会（第2回）（「資料3　産業サイバーセキュリティ強化へ向けたアクションプラン」より抜粋）
http://www.meti.go.jp/committee/kenkyukai/shoujo/sangyo_cyber/pdf/002_03_00.pdf

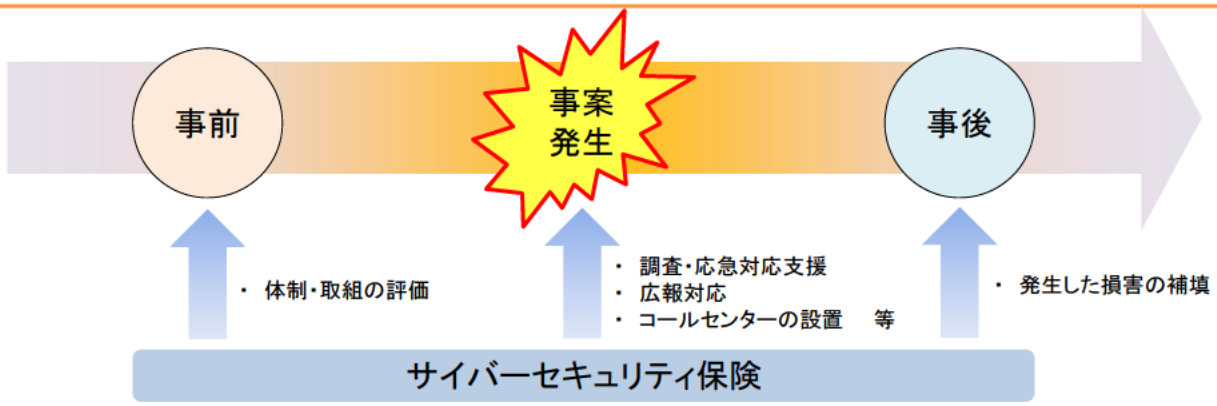
サイバーセキュリティ保険による取組の促進

【資料21】

○ サイバーセキュリティ保険は、**事前・事案発生時・事後と段階に応じて、セキュリティインシデントによって生じるリスクへの対応に資する**ものと考えられる。

事前	：	保険料算定のためのセキュリティに関する体制や取組の評価
事案発生時	：	損害保険会社が提携している各種事業者による調査・応急対応支援、広報対応、コールセンターの設置等
事後	：	事案によって生じる損害（例：顧客の個人情報の漏えいに係る損害賠償、争訟費用、復旧費用、調査費用　等）の補填

○ 特に、**個社単位でサイバーセキュリティ対策を講じることが資金的・技術的に困難な中小企業にとっては有効**であると考えられる。



情報開示によるインセンティブ

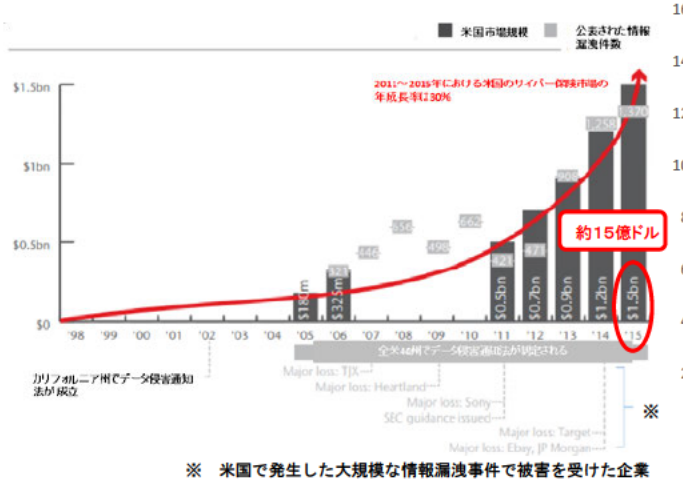
○第二者開示　しっかりと取り組んでいることを保険会社に示すことで保険料が低減

○第三者開示　独立行政法人情報処理推進機構（IPA）が実施しているセキュリティ対策の自己宣言制度（SECURITY ACTION）によって、「二つ星」を宣言した企業について、一部の保険会社において保険料が割引

日米サイバー保険市場比較

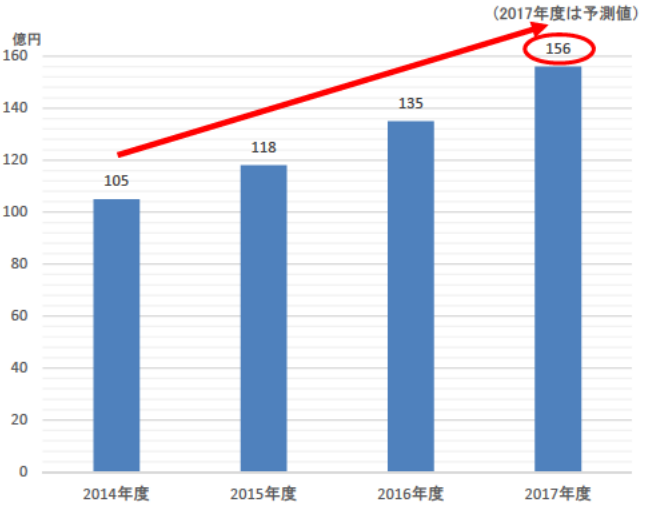
【資料22】

米国のサイバーセキュリティ保険市場は2011～2015年の間に年間約30%の成長を遂げており、市場規模は2015年時点で約15億ドルに達している一方で、日本のサイバーセキュリティ保険市場は2017年度で約156億円にとどまっており、米国の10分の1程度の市場規模となっている 。



※　米国で発生した大規模な情報漏洩事件で被害を受けた企業

米国におけるサイバー保険の推定市場規模推移



国内情報セキュリティ保険市場推移

（出典）左図表：「米国におけるサイバー保険の現状」（2017年11月　ジェトロ・ニューヨーク事務所）を参考に作成。
https://www.jetro.go.jp/ext_images/_Reports/02/2017/92c65a1f1a9f3ddc/ny11201711.pdf
右図表：「2016年度情報セキュリティ市場調査報告書　V1.1」（2017年6月　NPO日本ネットワークセキュリティ協会）を参考に作成。
http://www.jnsa.org/result/2017/surv_mrk/data/2016_mrk-report_v1.1.pdf

セキュリティ認証制度の活用事例

【資料23】

○ 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である「SECURITY ACTION」を、独立行政法人情報処理推進機構（IPA）が平成29年４月から開始。

○ IPAが公開している「中小企業の情報セキュリティ対策ガイドライン」の実践をベースに「一つ星」及び「二つ星」の２段階が用意されており、<u>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運用が一部の損保会社においてなされている</u>。

★ 一つ星…「情報セキュリティ5か条」に取り組む企業

①OSやソフトウェアは常に最新の状態にしよう！
②ウィルス対策ソフトを導入しよう！
③パスワードを強化しよう！
④共有設定を見直そう！
⑤脅威や攻撃の手口を知ろう！

★★ 二つ星…「5分でできる！情報セキュリティ自社診断」で自社の状況を把握したうえで、情報セキュリティポリシーを定め、<u>外部に公開した企業</u>

25の診断項目により、自社の対策状況を把握

➡ <u>宣言により、一部のサイバー保険の保険料が割引</u>

（参考）「情報セキュリティ5か条」（2017年 IPA） https://www.ipa.go.jp/files/000055516.pdf
「5分でできる！情報セキュリティ自社診断シート」（2017年 IPA） https://www.ipa.go.jp/files/000055517.pdf

5分でできる！情報セキュリティ自社診断（IPA）

【資料24】

5分でできる自社診断シート

組織で最低実施すべき情報セキュリティ対策を25項目に絞込み。
この項目の実施状況を点検し、未実施の対策を実施していくもの。

診断項目	No	診断内容
Part 1 基本的対策	1	Windows Updateを行うなどのように、常にOSやソフトウェアを安全な状態にしていますか？
	2	パソコンにはウイルス対策ソフトを入れてウイルス定義ファイルを自動更新するなどのように、パソコンをウイルスから守るための対策を行っていますか？
	3	パスワードは自分の名前、電話番号、誕生日など推測されやすいものを避けて複数のウエブサービスで使い回しをしないなどのように、強固なパスワードを設定していますか？
	4	ネットワーク接続の複合機やハードディスクの共有設定を必要な人だけに限定するなどのように、重要情報に対する適切なアクセス制限を行っていますか？
	5	利用中のウェブサービスや製品メーカーが発信するセキュリティ注意喚起を確認して社内共有するなどのように、新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？
Part 2 従業員としての対策	6	受信した不審な電子メールの添付ファイルを安易に開いたり本文中のリンクを安易に参照したりしないようにするなど、電子メールを介したウイルス感染に気をつけていますか？
	7	電子メールを送る前に目視にて送信アドレスを確認するなどのように、宛先の送信ミスを防ぐ仕組みを徹底していますか？
	8	重要情報をメールで送る時は重要情報を添付ファイルに書いてパスワード保護するなどのように、重要情報の保護をしていますか？
	9	無線LANを利用する時は強固な暗号化を必ず利用するなどのように、無線LANを安全に使うための対策をしていますか？
	10	業務端末でのウェブサイトの閲覧やSNSへの書き込みに関するルールを決めておくなどのように、インターネットを介したトラブルへの対策をしていますか？
	11	重要情報のバックアップを定期的に行うなどのように、故障や誤操作などに備えて重要情報が消失しないような対策をしていますか？
	12	重要情報を机の上に放置せず書庫に保管し施錠するなどのように、重要情報の紛失や漏えいを防止する対策をしていますか？
	13	重要情報を社外へ持ち出す時はパスワード保護や暗号化して肌身離さないなどのように、盗難や紛失の対策をしていますか？
	14	離席時にコンピュータのロック機能を利用するなどのように、他人に使われないようにしていますか？
	15	事務所で見知らぬ人を見かけたら声をかけるなどのように、無許可の人の立ち入りがないようにしていますか？
	16	退社時に机の上のノートパソコンや備品を引き出しに片付けて施錠するなどのように、盗難防止対策をしていますか？
	17	最終退出者は事務所を施錠し退出の記録（日時、退出者）を残すなどのように、事務所の施錠を管理していますか？
	18	重要情報を廃棄する場合は、書類は細断したり、データは消去ツールを使ったりするなどのように、重要情報が読めなくなるような処分をしていますか？
Part 3 組織としての対策	19	従業員を採用する際に守秘義務や罰則規定があることを知らせるなどのように、従業員に秘密を守らせていますか？
	20	情報管理の大切さなどを定期的に説明するなどのように、従業員に意識付けを行っていますか？
	21	社内外での個人所有のパソコンやスマートフォンの業務利用を許可制にするなどのように、業務で個人所有端末の利用の可否を明確にしていますか？
	22	契約書に秘密保持（守秘義務）の項目を盛り込むなどのように、取引先に秘密を守ることを求めていますか？
	23	クラウドサービスなど外部サービスを利用する時は利用規約やセキュリティ対策を確認するなどのように、サービスの安全・信頼性を把握して選定していますか？
	24	秘密情報の漏えいや紛失、盗難があった場合の対応手順書を作成するなどのように、事故が発生した場合に備えた準備をしていますか？
	25	情報セキュリティ対策（上記1 ～ 24など）を会社のルールにするなどのように、情報セキュリティ対策の内容を明確にしていますか？

（参考）「中小企業向け情報セキュリティ対策「5分でできる！情報セキュリティ自社診断」」（2017年 IPA ）を参考に作成。 https://www.ipa.go.jp/security/manager/know/sme-guide/index.html

IoT投資の抜本強化（コネクテッド・インダストリーズ税制の創設）　【資料25】

○一定のサイバーセキュリティ対策が講じられたデータ連携・利活用により、生産性を向上させる取組について、それに必要となるシステムや、センサー・ロボット等の導入に対して、特別償却30%又は税額控除3%（賃上げを伴う場合は5%）を措置。

○ 事業者は当該取組内容に関する事業計画を作成し、主務大臣が認定。認定計画に含まれる設備に対して、税制措置を適用（適用期限は、平成32年度末まで）。

※ 経済産業省との共管

【計画認定の要件】

①データ連携・利活用の内容

・社外データやこれまで取得したことのないデータを社内データと連携

・企業の競争力における重要データをグループ企業間や事業所間で連携

②セキュリティ面

必要なセキュリティ対策が講じられていることをセキュリティの専門家(登録セキスペ等)が担保

③生産性向上目標

投資年度から一定期間において、以下のいずれも達成見込みがあること

・労働生産性：年平均伸率２%以上

・投資利益率：年平均15%以上

課税の特例の内容

➢ 認定された事業計画に基づいて行う設備投資について、以下の措置を講じる。

対象設備	特別償却	税額控除
ソフトウェア 器具備品 機械装置	30%	3% （法人税額の15%を限度）
		５% ※ （法人税額の20%を限度）

【対象設備の例】
データ収集機器（センサー等）、データ分析により自動化するロボット・工作機械、データ連携・分析に必要なシステム（サーバ、ＡＩ、ソフトウェア等）、サイバーセキュリティ対策製品　等

最低投資合計額：5,000万円

※ 計画の認定に加え、平均給与等支給額の対前年度増加率≧３%を満たした場合。