資料３－２

「情報開示分科会」論点整理

平成30年2月

情報開示分科会の検討事項

検討事項

【検討事項１】情報開示する具体的な項目やその方法について

○　社会全体のセキュリティ対策を促進する観点や、個別の民間企業におけるＣＳＲの観点、株主の観点、情報開示にインセンティブを与える側の観点、情報開示する民間企業の負担の観点などから、新たなサイバー攻撃を誘発しないように配慮しつつ、中小企業を含めた民間企業がセキュリティ対策について適切に情報開示を行うためには、どのような項目を、どのような粒度で公表するべきか。

○　情報開示の媒体としては、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が考えられるが、上記と同様の観点からどのような媒体で、どのようなフォーマットで公表するのが望ましいか。

【検討事項２】情報開示の普及の方策について

○　セキュリティ対策の情報開示は各民間企業が任意で行うことを前提としているが、こうした取組を普及させるためにはどのような方策が有効か。

○　特に、セキュリティ対策の情報開示によるインセンティブとなりうるサイバーセキュリティ保険について、民間企業においてこのような保険商品の利用を普及させるには、どのような方策が有効か。

論点整理における基本的考え方

基本的考え方

○　サイバー空間のセキュリティ強化に向けて、民間企業におけるセキュリティ対策を促進する必要がある。そのためには、セキュリティ対策が企業経営において最も重要な課題であるとの認識が深まることが重要である。

○　民間企業においてセキュリティ対策が重要課題と位置づけられるためには、経営層がセキュリティ投資に係るグループ企業やサプライチェーンを含む自社の現状を認識し、また、他社の状況と比較し、さらに必要な具体的な対策を検討できるような環境の実現が必要となる。

○　そのような環境を実現するためには、民間企業におけるセキュリティ対策の情報開示の促進が必要である。情報開示の促進は、以下の「社内の情報共有」、「契約者間の情報開示（第二者開示）」、「社会に対する情報開示（第三者開示）」の3つの側面に分けて検討する必要がある。

①社内の情報共有

セキュリティに関する情報を外部に開示するにあたっては、セキュリティ対策の担当部署と経営層の間で情報共有が適切になされていることが前提とある。情報を社内で共有する中で、自社のセキュリティ対策が経営層の目に触れることになり、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り、セキュリティ対策の強化が期待される。

②契約者間の情報開示（第二者開示）

事業経営を適切に進めるにあたっては、自社のみならず、下請会社を含むサプライチェーン全体、または子会社を含むグループ全体のセキュリティが確保されている必要があり、そのためには各主体間におけるセキュリティ対策の情報開示が必要である。また、事業者が講じていた対策を超えたセキュリティインシデントが発生した場合に、その被害を軽減するためにはサイバーセキュリティ保険に加入することが有効であるが、その適切な料率算定のためにも、自社のセキュリティ対策を適切に認識し、損害保険会社に開示することが必要である。

③社会に対する情報開示（第三者開示）

セキュリティ対策に関する情報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ることにより、取引先候補として認識されるとともに、市場全体でさらなるセキュリティ対策の拡大が期待される。また、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ることで、さらにセキュリティ投資が拡大することが期待される。

①社内の情報共有について

考え方

○　企業の経営層におけるセキュリティ対策への理解を進めるため、「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）や「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）の内容を広く普及させていく取組や、現場と経営層の間の「橋渡し人材」の育成に向けた取組を進める必要があるのではないか。

現状・課題

○　社内におけるセキュリティ対策の情報共有を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、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」や「サイバーセキュリティ経営ガイドライン　Ver.2.0」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、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」（平成29年4月18日　サイバーセキュリティ戦略本部決定）においても示されてきたところであり、引き続き、その人材の育成に向けた取組を進める必要がある。

（参考）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）

2　現状と課題

（2）ITの利活用による新しい価値の創造への対応

⑥　経営層と実務者層の橋渡し役に関する課題

経営層が、新しいITを利活用する「挑戦」とそれに付随する「責任」として、サイバーセキュリティを経営戦略の一環として認識し、位置づけたとしても、具体的にどのようにサイバーセキュリティをビジネスに位置づけ、取り組んでいけばよいかについて、経営層自らが企画・立案し、実務者層を動かすことは困難である。むしろ、経営層の補佐的な役割を担う人材が、サイバーセキュリティの素養を持ち、経営戦略だけでなく、サイバーセキュリティの関係する業務課題を十分に理解した上で、経営層に対しセキュリティに関する課題と対応を経営層に進言するとともに、技術者をはじめとする様々な役割を持った実務者層を指揮することができるいわゆる「橋渡し人材層」が必要であり、その確保が課題である。加えて、「橋渡し人材層」がその役割を十分に遂行できるよう、「権限」と「責任を明示する必要がある。

②契約者間の情報開示（第二者開示）について

考え方

○ サプライチェーン全体やグループ全体で、複数の組織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を構築する取組をモデル事業の実施等を通じて促してはどうか。

現状・課題

○ 現状、業種毎の情報共有としては、ISAC（Information Sharing and Analysis Center）、CEPTOAR（Capability for Engineering of Protection, Technical Operation, Analysis and Response）がある。

○ また、業界横断的、又は地域的な情報共有としてC4TAP（Ceptoar Councils Capability for Cyber Targeted Attack Protection）、J-CSIP（Initiative for Cyber Security Information sharing Partnership of Japan）が存在しており、米国ではAIS（Automated Indicator Sharing）やISAO（Information Sharing and Analysis Organization）がある。

○ サプライチェーンは特定の業種に閉じたものではないため、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、上記のような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の取組が発展する中、グル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の構築をすすめることも必要であると考えられる。

○ 一方で、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形態も含む。）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められることは難しいと考えられ、モデル事業の実施等を通じた促進策が考えられる。

○ また、様々な主体間の効果的かつ効率的な情報共有の実現にあたっては、AIの活用についても検討するべきではないか。

②契約者間の情報開示（第二者開示）について

考え方

○ サイバーセキュリティに配慮したサプライチェーンを構築するため、契約者間で確認するべき事項や、必要な対策について整理する必要があるのではないか。

現状・課題

○ 経済産業省においては、我が国の産業界が直面するサイバーセキュリティの課題を洗い出し、関連政策を推進していくため、平成29年12月から「産業サイバーセキュリティ研究会」を開催している。

○ また、平成30年2月には同研究会のもとでワーキンググループ1（制度・技術・標準化）を開催しており、産業活動において必要なセキュリティ対策を示す「サイバー・フィジカル・セキュリティ対策フレームワーク」の策定に向けて議論しているところである。

○ 「サイバー・フィジカル・セキュリティ対策フレームワーク」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。

②契約者間の情報開示（第二者開示）について

考え方

○　サプライチェーン参加企業全体が一括して加入するサイバーセキュリティ保険や、セキュリティインシデント発生時にその対策に必要となる費用を保険金として支払うほか、付随して必要となるサービスを一括して提供するような保険商品について、その普及に向けた啓発活動が必要ではないか。

現状・課題

○　現状、提供されているサイバーセキュリティ保険においては、損害賠償請求を受けた額や、外部調査機関への調査依頼費用といった被保険者の被害の補填に加え、調査・応急対応支援や、広報対応、コールセンターの設置など、付随して必要となるサービスを併せて提供している。

○　そのようなサイバーセキュリティ保険は、セキュリティ対策が必ずしも十分に進んでいない中小企業にとって有用なものであるが、経済的な理由等から利用が進んでいない状況にある。一方で、親会社が子会社もまとめてグループで包括的に損害保険に加入しようという動きはある。

◆　構成員のご意見

・　子会社や関連会社について、親会社がまとめて一本でグループ包括ということで保険に入り、そのグループの中で効率的に保険を掛けていこうという動きはある。一方で、資本が入っていない下請会社のような場合は、川上の会社がまとめて保険を掛けるほど、そんなに優しいことはない。保険がないと取引しないというような慣習がもしあれば、保険があるとすぐに調査ができたり、止血ができたり、原因究明、責任関係が明らかになるようなサポートができるようになるので、サプライチェーンに何かあってもすぐに初動対応でリカバリーが効くという体制ができるとは思う。そこにどう保険を、誰がつけるのか、誰が保険料を負担するのかみたいなところの現実問題がまだ不明確な部分がありますので、こういうのが徐々になくなってくると、保険の面でサプライチェーンにいろいろな貢献ができるのではないかなというふうに考えております。（第2回・教学構成員代理）

③社会に対する情報開示（第三者開示）について

考え方

○　特に中小企業に対しては、最終的に取組を高度化していく観点から、まずは独立行政法人情報処理推進機構（IPA）におけるセキュリティ対策自己宣言制度（SECURITY　ACTION）の活用を促進するとともに、その二つ星の要件としている「5分でできる！情報セキュリティ自社診断シート」の項目または合計得点数について、何らかの方法（HP掲載等も含む）で開示するよう促してはどうか。

現状・課題

○　中小企業においては、開示するほどのセキュリティ対策がまだできていないという意識が強く、また、開示するのに十分な人員や予算が確保できないことが考えられる。

○　独立行政法人情報処理推進機構（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）の取組を平成29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」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、「二つ星」を使用するためには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」で自社の状況を把握した上で、情報セキュリティポリシーを定め、外部に公開することが必要となる。

○　当該制度は中小企業を対象としたものであり、比較的負担が軽く、簡便であるため、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り得るものであると考えられる。

③社会に対する情報開示（第三者開示）について

考え方

○　現在、セキュリティ対策を開示していない又は十分でない事業者に対しては、「CSR報告書」や「サステナビリティレポート」で記載例が見られる以下の5項目について、開示するように促してはどうか。

・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（研修の実施　等）

・社外との情報共有体制（日本シーサート協議会に加盟　等）

・第三者評価・認証の取得状況

現状・課題

○情報セキュリティ報告書について

- サイバーセキュリティに関する記載は100％なされているが、作成している事業者が極めて少ない（上場企業226社においても5社）。

○有価証券報告書について

- 「事業等のリスク」の観点から記載はされているが、詳細な対策について記載されている事例が少なく、また、対象が上場企業のみであるため、事業者の範囲が狭められてしまう。

◆　構成員のご意見

- 有価証券報告書で開示している企業もあるが、内容が形骸化して、コピーペーストのようなものが多い印象。（第1回・鵜飼構成員）
- 有価証券報告書については、上場企業にとっては非常に大きな責任を伴うものなので非常に効果があるかもしれないが、基本的に上場企業のみが対象であるため、企業の範囲が非常に狭められてしまうという懸念がある。（第1回・鵜飼構成員）
- セキュリティリスクであれば有価証券報告書、セキュリティ対策であればコーポレートガバナンス報告書で開示する事になると思うが、有価証券報告書に全てを書くことが適当かどうかは自明ではない。（第1回・大杉構成員）

③社会に対する情報開示（第三者開示）について

現状・課題

○CSR報告書及びサステナビリティレポート

- 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、そのうち110社（63％）にサイバーセキュリティに関する記載があり、サステナビリティレポートについては34社が作成しており、そのうち30社（88％）にサイバーセキュリティに関する記載がある。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210社がいずれかの報告書を作成しており、140社（67％）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レポートにおけるサイバーセキュリティに関する具体的な記載内容について分析すると、「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（研修の実施　等）」、「社外との情報共有体制（日本シーサート協議会に加盟　等）」及び「第三者評価・認証の取得状況」の5項目に分類されると考えられる。
- これらの項目については、以下の観点から開示する項目として望ましいと考えられる。
  - 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
  - 開示することによって、セキュリティ対策の穴が見えるということが少ない
  - 対外的にセキュリティ対策をきちんと行っている姿勢が見せられる
  - 適度に同業他社との比較・競争が期待できる

◆　構成員のご意見

- 開示内容が正しいかどうか、十分に網羅的なものか、更にそれがわかりやすく開示されているかについては、技術的、専門的な知識がないと難しく、これらをどう担保するかも検討する必要がある。（第1回・鵜飼構成員）
- 簡単な方法で、その時代に即し、かつ誰が行ってもある程度正確性を持って開示できるような仕組みが必要。（第1回・鵜飼構成員）
- 正確性の担保については、客観的にかつ独立性を持ってチェックを行うための経験や専門性、能力を有する人材を育成しなければ、なかなか難しいのではないか。誰かが内容をチェックしたというだけでは恐らく情報開示に対する期待には応えられないのではないか。（第1回・加藤構成員）
- 開示されている情報を見たときに、各企業の違いやどちらが良いのかを広くあまねく分かるということは難しいのではないかと思う。その点での簡素化、見える化が必要。見る側も開示された情報を理解して、お互いに相互作用し合うスキームにする必要がある。（第2回・源田構成員）

③社会に対する情報開示（第三者開示）について

考え方

○　現在、既に何らかの方法でセキュリティ対策を開示している事業者に対しては、「情報セキュリティ報告書」を作成・公表するように促してはどうか。

現状・課題

○　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と考えられるが、サイバーセキュリティに特化した単体の報告書であり、当該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開示する媒体として理想的なものであると考えられる。

○　情報セキュリティ報告書の記載事項については、経済産業省が平成19年に「情報セキュリティ報告書モデル」を公表しており、基本構成として以下のとおり示している。

（参考）情報セキュリティ報告書モデル（平成19年　経済産業省）

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
　情報セキュリティに関する取組方針、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等

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等

④情報セキュリティ対策の計画、目標
　アクションプラン、数値目標等

⑤情報セキュリティ対策の実績、評価
　実績、評価、情報セキュリティの品質改善活動、海外拠点の統制、外部委託、情報セキュリティに関する社会貢献活動、事故報告等

⑥情報セキュリティに係る主要注力テーマ
　内部統制や個人情報保護、事業継続計画など特に強調したい取組、テーマの紹介、工夫した点等

⑦（取得している場合の）第三者評価・認証等
　ISMS 適合性評価制度、情報セキュリティ監査、プライバシーマーク制度、情報セキュリティ関連資格者数、格付け／ランキング等

※　下線がついている項目は、記載することが望ましい基本的な要素。

開示事項について

考え方

○ これまで事業者が経験したセキュリティインシデント及びそれを踏まえた対策の実施状況について開示するように促してはどうか。

現状・課題

○ 事業者が経験したセキュリティインシデントについては、「情報セキュリティ報告書モデル」においても「⑤情報セキュリティ対策の実績、評価」の項目の中で「事故報告」として掲げられており、「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）が平成23年10月に公表している開示ガイドライン（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。

（参考）CF Disclosure Guidance: Topic No. 2(Division of Corporation Finance Securities and Exchange Commission (October 13, 2011))

Risk Factors

Depending on the registrant's particular facts and circumstances, and to the extent material, appropriate disclosures may include:

・Description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences;

◆ 構成員のご意見

・ 保険会社としては、過去にセキュリティインシデントがあったことについては、再発防止をしっかり行っているのだろうと考え、リスクは低減されているのではないかと考える。そのような観点で過去のインシデントの情報を積極的に企業に開示できる状況になると、評価されるのではないかと思う。（第2回・教学構成員代理）

・ 上場企業については、上場契約の中でインシデント発生時の開示が義務づけられている。原因の探求や改善に結びつける大きな誘因になっているが、第三者調査委員会の活動や調査報告書については、評価が定まっていない。（第1回・大杉構成員）

・ コーポレートガバナンスの観点からすると、会社自体の損害よりもインシデントによる影響の大きさ、影響の種類の開示が強く望まれていると考える。（第2回・野口構成員）

開示事項について

考え方

○ 万が一、セキュリティインシデントが発生した場合の被害の軽減策として、サイバーセキュリティ保険に加入している旨を開示するように促してはどうか。

現状・課題

○ サイバーセキュリティ保険は、事業者が取っていたセキュリティ対策を超えるセキュリティインシデントが発生した際の被害を軽減するだけではなく、損害保険会社による審査を経ることで一定のセキュリティ対策が担保されるとともに、当該事業者がセキュリティリスクを重要な経営リスクとして認識しており、対策をとっていることを対外的に示すことなるものである。

○ また、米国の証券取引委員会(SEC)が平成23年10月に公表している開示ガイドライン(CF Disclosure Guidance)においても、関連する保険の適用範囲に係る解説が適切な情報開示に含まれるとしている。

(参考)CF Disclosure Guidance: Topic No. 2(Division of Corporation Finance Securities and Exchange Commission (October 13, 2011))

Risk Factors

Depending on the registrant's particular facts and circumstances, and to the extent material, appropriate disclosures may include:

・Description of relevant insurance coverage.

◆ 構成員のご意見

・ サイバーセキュリティ保険の加入している旨を開示の1つの項目としてもいいのではないか。(第2回・鵜飼構成員)

開示事項について

考え方

○　自社だけでなく、子会社を含むグループ全体、また下請会社を含むサプライチェーン全体のセキュリティ対策の状況について、開示するように促してはどうか。

現状・課題

○　中小企業においては、開示するほどのセキュリティ対策がまだできていないという意識が強く、また、開示するのに十分な人員や予算が確保できないことが考えられる。

○　ついては、まずは情報開示に取り組んでいる事業者が、その子会社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のセキュリティ対策について開示するように促してはどうか。

◆　構成員のご意見

・　中小企業においては、開示するほどのセキュリティ対策がまだできていないという意識が強いと思われるが、そのような中では、サプライチェーンの川上にある発注元から実質的に求められるような動きがないと開示しようというモチベーションにつながらないのではないか。（第1回・教学構成員代理）

・　サイバーリスクは、複数の企業がつながっている場合、つながっている全ての企業に影響する。つながっている企業が同質でないという点や、それらのつながっている同質でない企業が1つのリスクを受容しているという点がポイントとなる。（第1回・源田構成員）

・　保険に関しては、親会社が子会社分もまとめて保険に加入するという動きはある。（第2回・教学構成員代理）

普及策について

考え方

○ 各開示媒体に応じたベストプラクティス集を公表してはどうか。

現状・課題

○ 事業者のサイバーセキュリティに関する情報発信の姿勢については、調査対象の74.1%の事業者が「同業者や同規模の企業と同じレベルでできていればよい」と考えており、横並びを意識して情報開示している実態がみえる。

○ 現状において、有価証券報告書におけるサイバーセキュリティに関する記載は定型句のように似通ったものとなっており、事業者固有の状況に応じた記載となっておらず、具体的なセキュリティ対策が把握できない状況にある。

○ 一方で、セキュリティ対策を記載しているCSR報告書及びサステナビリティレポートにおいては、各事業者が策定しているセキュリティに関する基本方針や、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・認証の取得状況など、具体的な記載がなされている。

○ 米国の証券取引委員会(SEC)が平成23年10月に公表している開示ガイドライン(CF Disclosure Guidance)においては、情報を開示するにあたっては事業者の個別の事実や状況に応じて行うべきあるとしている。

(参考)CF Disclosure Guidance: Topic No. 2(Division of Corporation Finance Securities and Exchange Commission (October 13, 2011))

Risk Factors

Depending on the registrant's particular facts and circumstances, and to the extent material, appropriate disclosures may include …

◆ 構成員のご意見

- 企業が情報開示するに当たって、ベストプラクティスや、ガイドラインのようなものがあると、参照頻度が過度に高くなることで、内容が横並びであっても全体の水準が上がることに資するのではないか。(第1回・加藤構成員)
- 情報開示のベストプラクティスの提示や、表彰制度等により、サイバーセキュリティの普及や保険への関心が進むのではないか。また、どの程度対策を取れば良いかが不明瞭であることが投資を妨げる要因となっており、ベストプラクティスの提示等により、セキュリティ対策のベンチマークを示すことで、それが基準となり対策が進むのではないか。(第2回・秋保構成員)

普及策について

考え方

○　平成30年度からセキュリティに関する税制として、「コネクテッド・インダストリーズ税制」が創設されることとなっているが、同様に税制の側面から情報開示を促進するためのインセンティブを設けることは可能か。

現状・課題

○　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％）を措置することとしている。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、税制措置が適用される（平成30～32年度）。

○　今後、同税制の活用状況のなどを分析し、その結果を踏まえつつ、情報開示を促進するインセンティブとして税制を活用することは可能か。

考え方

○　以上のような方策や、共有すべき情報、粒度等についてガイドラインを策定することで、各社の取組の推進に資することができるのではないか。

（参考資料）

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

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。

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

- 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

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

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

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

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）

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。

『サイバー・フィジカル・セキュリティ対策フレームワーク』のイメージ

WG1にて検討を進め、年度内に大枠を整理することを目指す

来年度以降 SWGにて 具体を検討

（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）（第１回）
「資料６　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向けて」より抜粋）

セキュリティ認証制度の活用事例

○　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、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が一部の損保会社から提供されている。

★　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、外部に公開した企業

25の診断項目により、自社の対策状況を把握

宣言により、一部のサイバー保険の保険料が割引

5分でできる自社診断シート

入門レベルとして最初に取り組むべき
情報セキュリティ対策の自社診断シート

IPA

●診断の前に、まず裏面の 1 をご覧ください。
●下記の診断内容を読み、チェック欄の該当するするもの1つに○を付けてください。
●「実施している」はすべての従業者が実施している場合に選んでください。
●シートは、経営者または管理者の方がご記入ください。
●チェックが終了したら最下段に合計を記入して、裏面の 2 をご覧ください。

組織名

記入者名

実施年月日　　年　　月　　日

No	診断項目	診断内容	チェック 実施している	一部実施している	実施していない	わからない	自社診断 パンフレットと対応しています。
1	保管について	重要情報※1を机の上に放置せず鍵付き書庫に保管し施錠するなどのように、重要情報がみだりに扱われないようにしていますか？	4	2	0	0	P1 No.1 保管についてを参照
2	持ち出しについて	重要情報を社外へ持ち出す時はパスワードロックをかけるなどのように、盗難・紛失対策をしていますか？	4	2	0	0	P1 No.2 持ち出しについてを参照
3	廃棄について	重要な書類やCDなどを廃棄する場合は、シュレッダーで裁断するなどのように、重要情報が読めなくなるような処分をしていますか？	4	2	0	0	P1 No.3 廃棄についてを参照
4		重要情報の入ったパソコン・記憶媒体を廃棄する場合は、消去ソフトを利用したり、業者に消去を依頼するなどのように、電子データが読めなくなるような処理をしていますか？	4	2	0	0	P1 No.4 廃棄についてを参照
5	事務所について	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？	4	2	0	0	P2 No.5 事務所についてを参照
6		退社時に、机の上の備品やノートパソコンを引き出しに片付けるなどのように、盗難防止対策をしていますか？	4	2	0	0	P2 No.6 事務所についてを参照
7		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？	4	2	0	0	P2 No.7 事務所についてを参照
8	パソコンについて	Windows Update※2を行うなどのように、常にソフトウェアを安全な状態にしていますか？	4	2	0	0	P3 No.8 パソコンについてを参照
9		ファイル交換ソフト※3を入れないようにするなどのように、ファイルが流出する危険性が高いソフトウェアの使用を禁止していますか？	4	2	0	0	P3 No.9 パソコンについてを参照
10		社内外での個人パソコンの業務使用を許可制にするなどのように、業務で個人パソコンを使用することの是非を明確にしていますか？	4	2	0	0	P3 No.10 パソコンについてを参照
11		退社時にパソコンの電源を落とすなどのように、他人に使われないようにしていますか？	4	2	0	0	P3 No.11 パソコンについてを参照
12	パスワードについて	パスワードは自分の名前を避けるなどのように、他人に推測されにくいものに設定していますか？	4	2	0	0	P4 No.12,13,14 パスワードについてを参照
13		パスワードを他人が見えるような場所に貼らないなどのように、他人にわからないように管理していますか？	4	2	0	0	P4 No.12,13,14 パスワードについてを参照
14		ログイン用のパスワードを定期的に変更するなどのように、他人に見破られにくくしていますか？	4	2	0	0	P4 No.12,13,14 パスワードについてを参照
15	ウイルス対策について	パソコンにはウイルス対策ソフトを入れるなどのように、怪しいWebサイトや不審なメールを介したウイルスから、パソコンを守るための対策をおこなっていますか？	4	2	0	0	P4 No.15 ウイルス対策についてを参照
16		ウイルス対策ソフトのウイルス定義ファイル※4を自動更新するなどのように、常に最新のウイルス定義ファイルになるようにしていますか？	4	2	0	0	P4 No.16 ウイルス対策についてを参照
17	メールについて	電子メールを送る前に、目視にて送信先アドレスの確認をするなどのように、宛先の送信ミスを防ぐ仕組みを徹底していますか？	4	2	0	0	P5 No.17 メールについてを参照
18		お互いのメールアドレスを知らない複数人にメールを送る場合は、Bcc※5機能を活用するなどのように、メールアドレスを誤って他人に伝えてしまわないようにしていますか？	4	2	0	0	P5 No.18 メールについてを参照
19		重要情報をメールで送る場合は、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？	4	2	0	0	P5 No.19 メールについてを参照
20	バックアップについて	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？	4	2	0	0	P5 No.20 バックアップについてを参照
21	従業者について	採用の際に守秘義務があることを知らせるなどのように、従業者に秘密を守らせていますか？	4	2	0	0	P6 No.21 従業者についてを参照
22		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、従業者に意識付けを行っていますか？	4	2	0	0	P6 No.22 従業者についてを参照
23	取引先について	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、取引先に機密を守ることを求めていますか？	4	2	0	0	P6 No.23 取引先についてを参照
24	事故対応について	重要情報の流出や紛失、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？	4	2	0	0	P6 No.24 事故対応についてを参照
25	ルールについて	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？	4	2	0	0	P6 No.25 ルールについてを参照

A 実施している の合計点	B 一部実施している の合計点	A+B 合計点
点	点	点

※1 重要情報とは、その情報が失われたことによりビジネスに打撃を与えたり、組織の信頼失墜につながる情報
全ての顧客情報、販売名簿、設計図面、開発スケジュール、仕入単価、取引関係など

※2 マイクロソフト社が提供しているウインドウズパソコンの不具合を修正するプログラム

※3 WinnyやShareなど、インターネット上で不特定多数のコンピュータ間でファイル（データ）をやり取りできるソフトウェア

※4 コンピュータウイルスを検出するための データベースファイル「パターンファイル」とも呼ばれる

※5 Blind Carbon Copyの略で、他の受信者にメールアドレスを伏せて送信する機能

★この自社診断シートで例示している対策方法については、これらだけで十分ということを保証するものではありません。

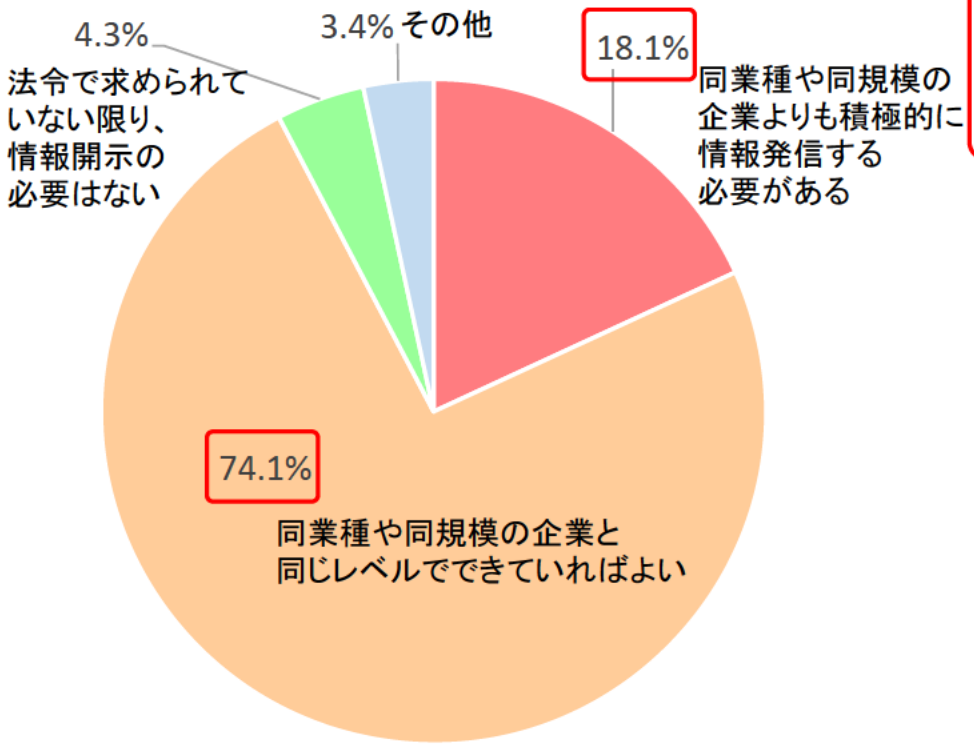
民間企業におけるサイバーセキュリティに関する情報発信に対する認識

○ 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。

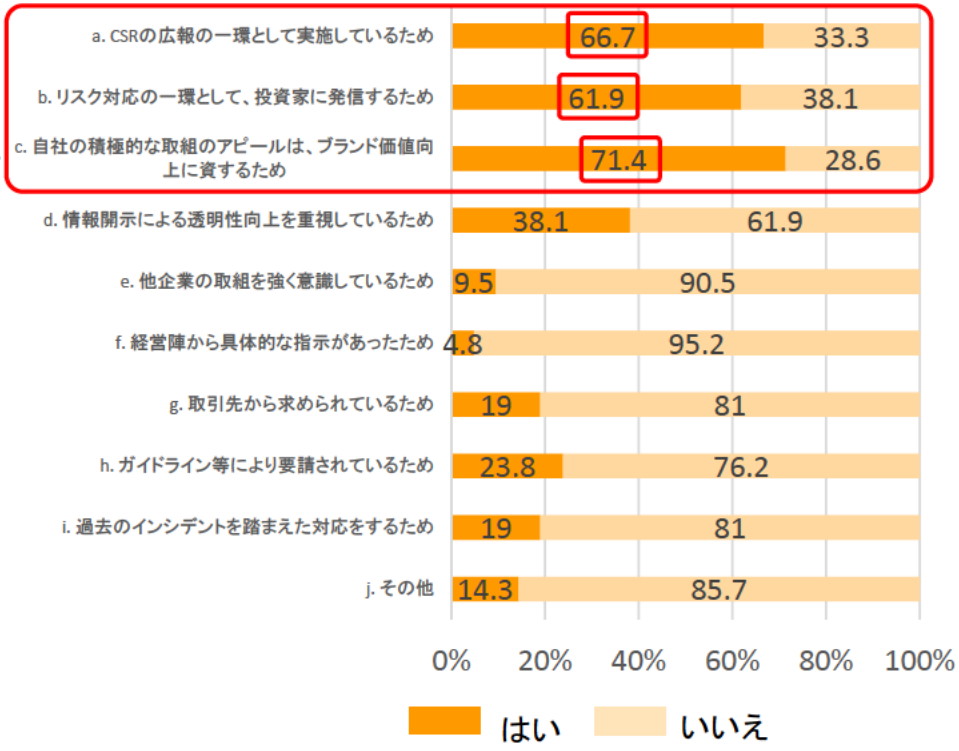
○ 情報発信の姿勢について、他の企業と同じレベルでできていればよいと回答した企業が74.1%であり、他企業よりも積極的に情報発信をする必要があると回答した企業は18.1%となっている。

○ 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



「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

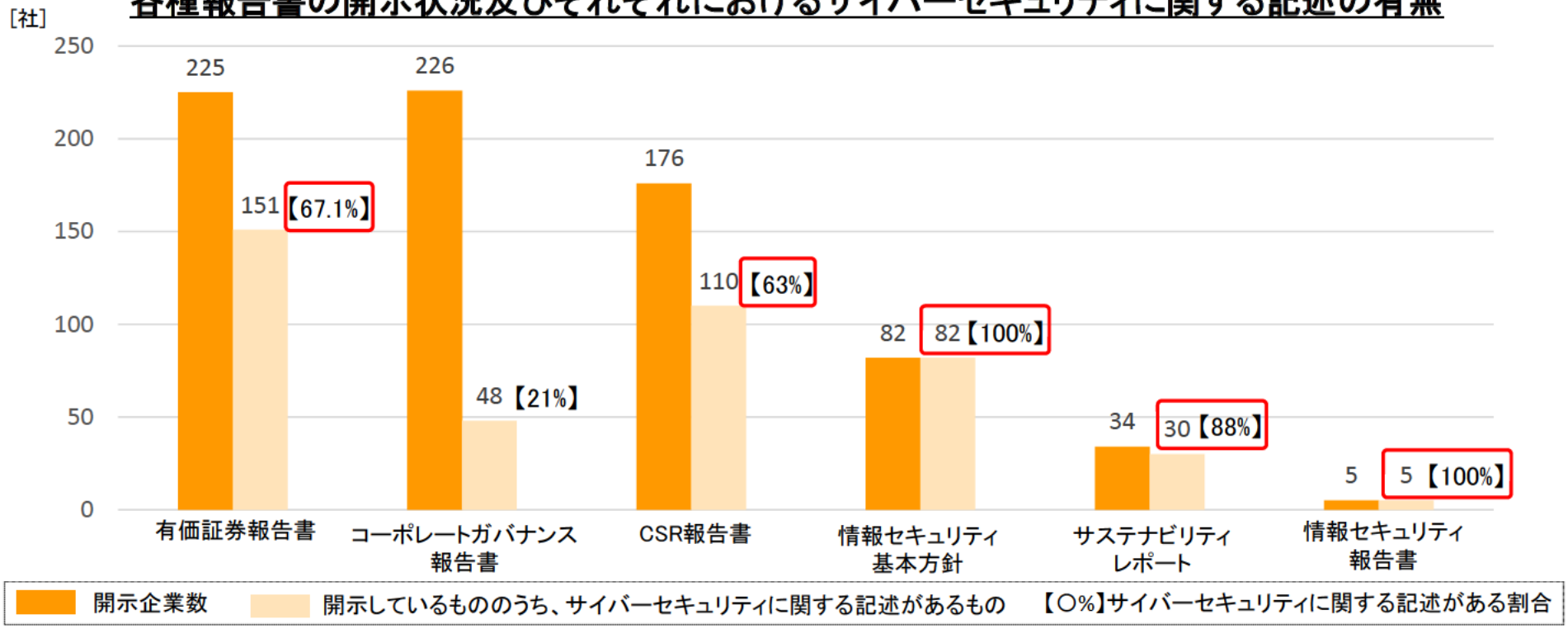
民間企業におけるセキュリティ対策に関する情報開示の実態

○ 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



「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

情報セキュリティ報告書モデル（平成19年　経済産業省）

》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

情報セキュリティ報告書

- ✓ 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

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）

○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

<u>最低投資合計額：5,000万円</u>

※ 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。