資料１－２

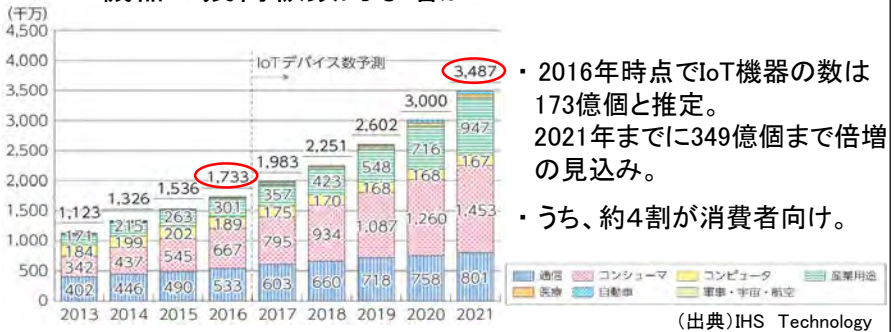
民間企業におけるセキュリティ対策に関する情報開示の現状について

平成29年12月

IoTセキュリティ総合対策（2017年10月）

現状

○IoT機器の幾何級数的な増加

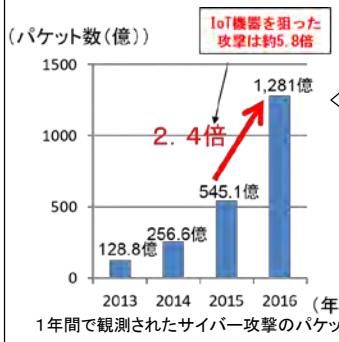


・2016年時点でIoT機器の数は173億個と推定。
2021年までに349億個まで倍増の見込み。

・うち、約4割が消費者向け。

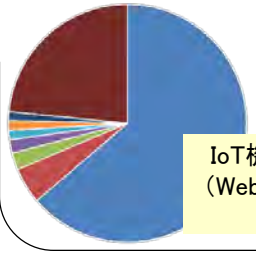
（出典）IHS Technology

○IoT機器を狙った攻撃が急増



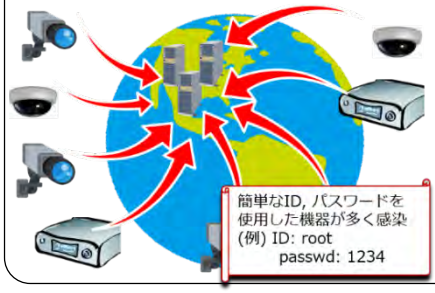
1年間で観測されたサイバー攻撃のパケット数

観測された全サイバー攻撃
1,281億パケットのうち、 2/3 がIoTを狙っている！



IoT機器を狙った攻撃
（Webカメラ、ルータ等）
64%

○IoT機器を踏み台にした大規模攻撃が発生



・2016年10月21日米国のDyn社のDNSサーバーに対し、大規模なDDoS攻撃が2回発生。

・同社からDNSサービスの提供を受けていた企業のサービスにアクセスしにくくなる等の障害が発生。

・サイバー攻撃の元は、「Mirai」というマルウェアに感染した大量のIoT機器。

対策

IoTセキュリティ総合対策

脆弱性対策に係る体制の整備

・IoT機器の脆弱性についてライフサイクル全体（設計・製造、販売、設置、運用・保守、利用）を見通した対策が必要。

・脆弱性調査の実施等のための体制整備が必要。

研究開発の推進

・セキュリティ運用の知見を情報共有し、ニーズにあった研究開発を促進。

民間企業等におけるセキュリティ対策の促進

・民間企業等のサイバーセキュリティに係る投資を促進。

・サイバー攻撃の被害及びその拡大防止のための、攻撃・脅威情報の共有の促進。

人材育成の強化

・圧倒的にセキュリティ人材が不足する中、実践的サイバー防御演習等を推進。

国際連携の推進

・二国間及び多国間の枠組みの中での情報共有やルール作り、人材育成、研究開発を推進。

半年に1度を目途としつつ、必要に応じて検証
（関係府省と連携）

「IoTセキュリティ総合対策」における情報開示に係る記載

○「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）（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。

セキュリティ対策に関する情報開示により期待される効果

情報開示を行った企業自身

・ 説明責任の遂行

サイバーインシデントが事業の存続すら脅かすリスクとなりつつある中、セキュリティリスクに一層高い関心を示すと見込まれるステークホルダーに対する説明責任の遂行に資することになる。

・ 経営層に対する意識付け

情報開示するための報告書を準備・作成し、対外的に説明する作業を通じて、経営層が自社のセキュリティ対策について認識し、更なる検討を促す効果が期待される。

・ 新たな事業価値の創出

自社のセキュリティ向上に関する取組を対外的に公表することで、取引先、顧客、投資家等からの支持を得て、企業価値の向上、競争優位の確保を狙うことが可能となる。

各ステークホルダー

取引先

・ 取引相手の信頼性の把握

調達等における相手企業の安定的な事業継続や情報管理の状況に対して高い関心を寄せる取引先にとって、有益な情報となる。

従業員、グループ会社、外部委託先

・ 意識の共通化、理解の向上

従業員のセキュリティ意識・理解を高め、対外的な説明を共通化・統一する等の効果が期待される。

顧客、消費者

・ マーケティング効果、ブランドイメージの向上

「顧客情報・個人情報の保護」に関心を持つ顧客、消費者に対し、そのような問題に誠意をもって取り組んでいることを訴求することができる。

投資家、アナリスト

・ 投資対象の評価

対象企業の業績や将来成長性を評価する上で、リスク情報やその対策に関する情報を活用することが可能となる。

格付け機関、メディア、関連団体

・ 分析材料の充実

セキュリティリスクが経営に及ぼす影響が今以上に大きくなれば、リスクマネジメントの視点から、格付け機関が開示情報を積極的に活用することが考えられる。

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

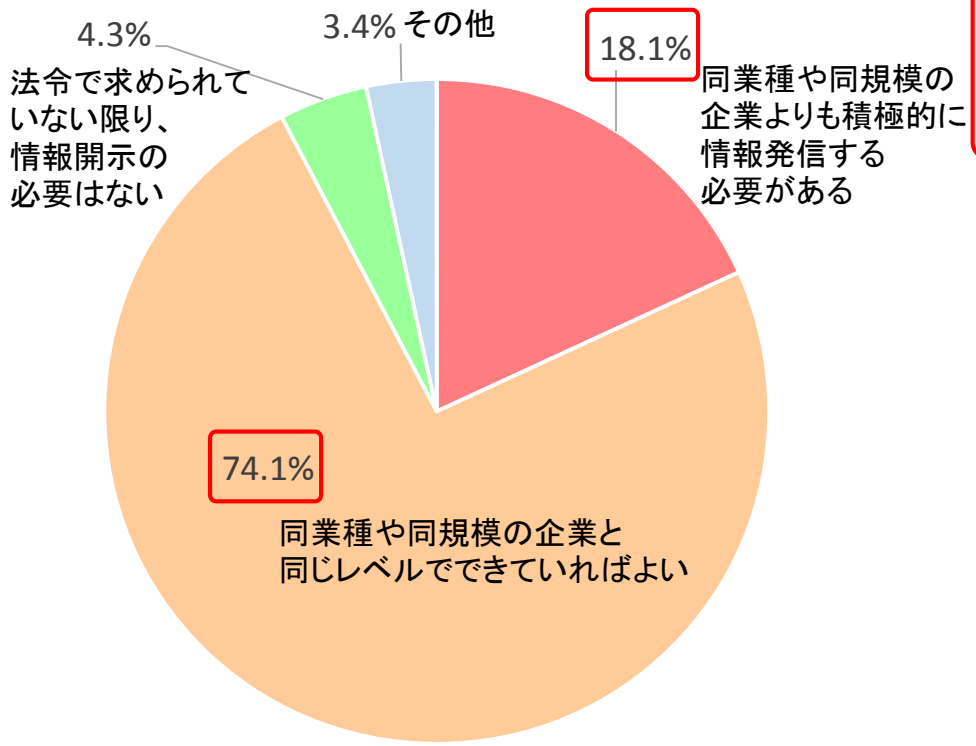
民間企業におけるサイバーセキュリティに関する情報発信に対する認識

○ 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。

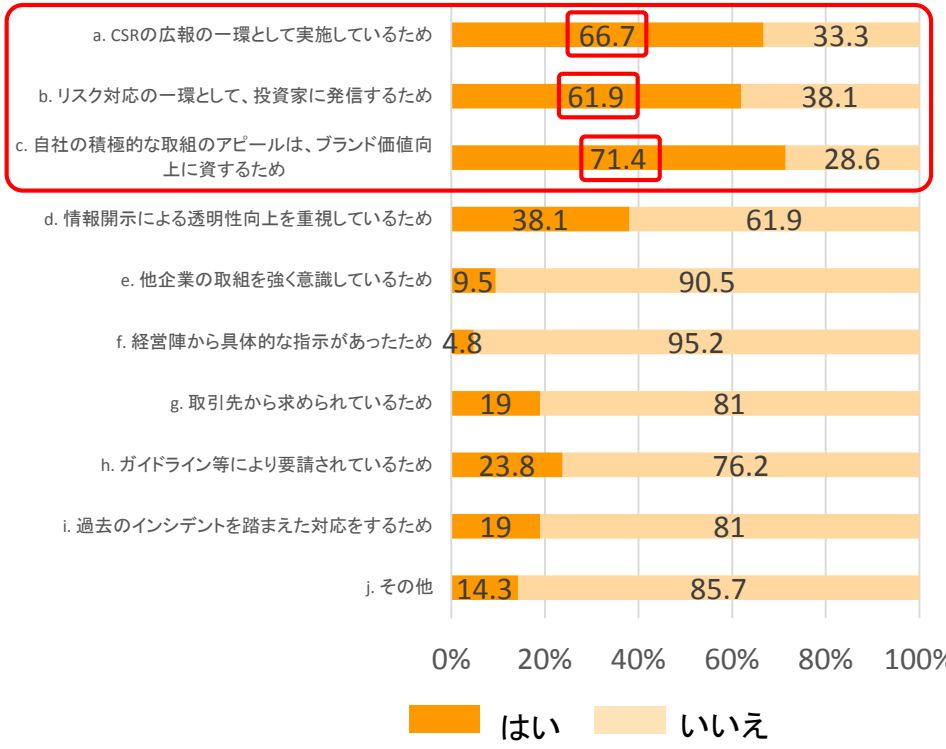
○ 情報発信の姿勢について、他の企業と同じレベルでできていればよいと回答した企業が74.1%であり、他企業よりも積極的に情報発信をする必要があると回答した企業は18.1%となっている。

○ 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

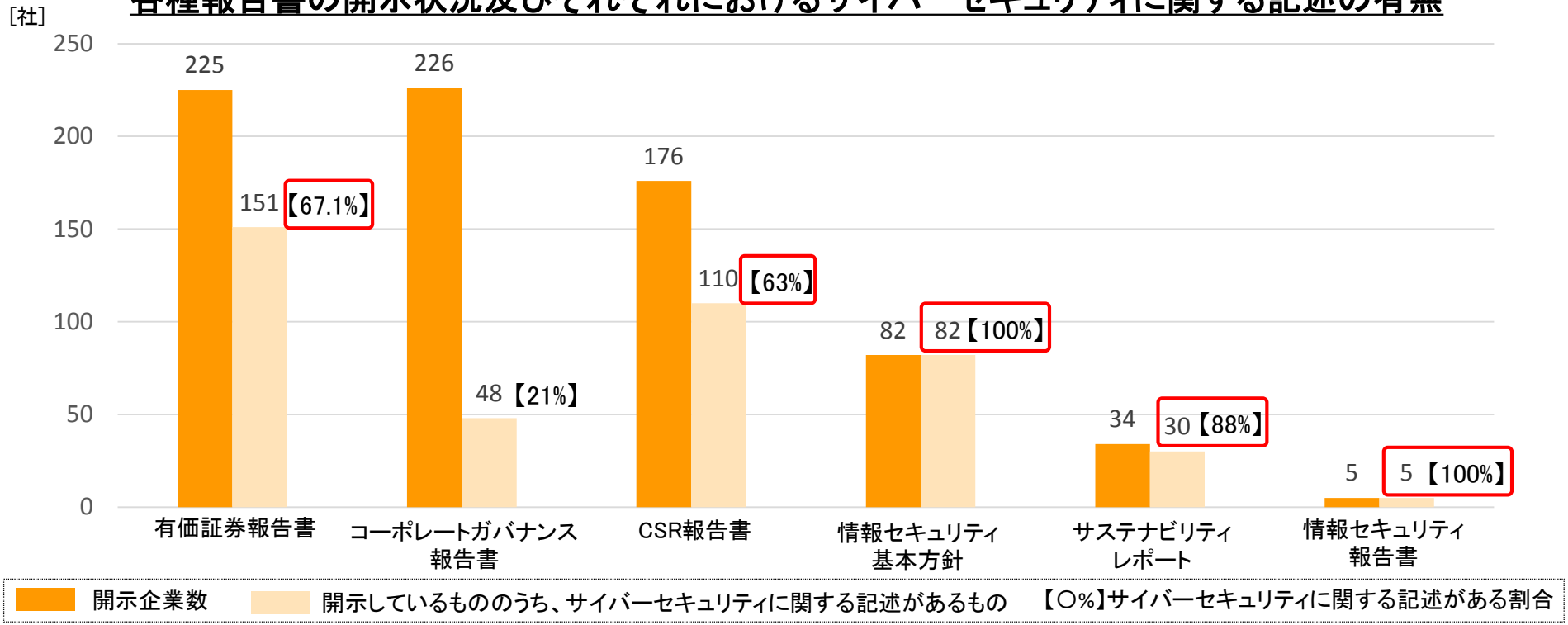
民間企業におけるセキュリティ対策に関する情報開示の実態

○ 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

（参考）各種報告書におけるセキュリティ対策に関する情報開示の例

○有価証券報告書の記載例

○　情報システム及び情報セキュリティに関するリスク

当社グループは、 すべての役員及び従業員に対し、情報の取扱に関する行動規範を定め、**高い情報セキュリティレベルを確保することを重要事項と認識**しております。当社グループは、情報共有や業務の効率化のため、情報システムを構築・運用するとともに、情報システム運営上の安全性確保のため、**サイバーセキュリティリスクも考慮し、セキュリティガイドラインの設定、危機管理対応の徹底に取組んでおります**。

しかしながら、こうした対策を行ったとしても、**外部からの予期せぬ不正アクセス、コンピューターウィルス侵入等による機密情報・個人情報の漏洩、設備の損壊・通信回線のトラブル等による情報システムの停止等のリスク**を完全に回避できるものではなく、被害の規模によっては将来の当社グループの**財政状態や業績に重要な影響**を及ぼす可能性があります。

○　情報セキュリティに関するリスク

当社グループが顧客に対して商品販売やサービス提供を行うに際しては、**顧客の情報管理に最大限に注意を払い漏えいしないための情報システム防御を実行**しております。しかしながら、**第三者等による情報システムへの意図的な進入が行われたり、様々な原因や理由によって情報システムが停止するなどの問題が予想され、それによって個人を含む顧客情報の漏えいや流出が発生するリスクが存在**いたします。万一、このような自体が発生した場合には**顧客からの損害賠償請求や信用の失墜により、当社グループの業績等に影響**を及ぼす可能性があります。

○情報セキュリティ報告書の構成例

・グループにおける情報セキュリティへの取り組み
- 情報セキュリティガバナンスの基本的な考え方
- 情報セキュリティマネジメントシステム
  情報セキュリティ方針、情報セキュリティ推進体制、
  情報セキュリティ規則、情報セキュリティマネジメントサイクル、
  情報セキュリティ監査、情報セキュリティに関する教育
- 情報セキュリティに対する技術面での取り組み
  ネットワークセキュリティ、メールセキュリティ、
  エンドポイントセキュリティ、IDセキュリティ、
  ドキュメントセキュリティ
- クラウド活用におけるセキュリティへの取り組み
- 物理セキュリティに対する取り組み
- お取引先様と連携した取り組み
- サイバーセキュリティに対する脆弱性対策・インシデント・対応への取り組み
  インシデントレスポンスチーム
- グローバル情報セキュリティの取り組み
  グローバル情報セキュリティ管理規定
- 個人情報保護に対する取り組み
  個人情報保護推進体制、個人情報保護マネジメントシステム、
  委託先の管理強化

・製品・サービスの情報セキュリティ確保に向けた取り組み
・情報セキュリティに関する社外活動
・第三者評価・認証

セキュリティ対策に関する情報開示に係るこれまでの取組①

内閣サイバーセキュリティセンター(NISC)

○サイバーセキュリティ戦略（平成27年９月４日　閣議決定）

５．目的達成のための施策
５．１．経済社会の活力の向上及び持続的発展
５．１．２．セキュリティマインドを持った企業経営の推進
（１）経営層の意識改革

企業の経営層が、事業の基盤として用いるシステムや営業秘密の事業戦略上の価値・役割を認識して活用することは、企業経営において不可欠なものである。また、高いレベルのセキュリティ品質が確保された製品・サービスを市場に投入し、新たなビジネスを創出する経営判断に当たり、サイバーセキュリティに関する素養が企業経営層の必須能力となりつつある。こうした社会の変化をより多くの企業経営層が的確に認識し、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持続的発展のために必要である。このため、**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**。

○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）

Ⅰ　基本的考え方
２．三つの留意事項
２－① 情報発信による社会的評価の向上

競争力のある新たな製品やサービスを提供するに当たっては、高いレベルの「セキュリティ品質」を確保することが前提となる。このためには、セキュリティ対策を従来の問題解決策としてではなく、品質向上等に有効な経営基盤の一つとして位置づけて取り組むことが必要である。

そして、**自社のこうした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**。**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**。また、その過程を通じて自社のリスク認識を高めることにもつながるものと考えられる。

セキュリティ対策に関する情報開示に係るこれまでの取組②

経済産業省

○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）

２．経営者が認識すべき３原則

（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

（解説）

・　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。

・　このため、**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。

３．サイバーセキュリティ経営の重要１０項目

３．２．サイバーセキュリティリスクの特定と対策の実装

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

計画を確実に実施し、改善していくため、サイバーセキュリティ対策をPDCAサイクルとして実施させる。
その中で、定期的に経営者に対策状況を報告させた上で、問題が生じている場合は改善させる。
また、**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**。

対策例

・　**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**。

（参考）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。

SECURITY ACTION ★
セキュリティ対策自己宣言

★　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！

SECURITY ACTION ★★
セキュリティ対策自己宣言

★★　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

情報開示分科会の検討事項（案）

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。

情報開示分科会の今後のスケジュール（案）

○　平成29年12月中旬から5回程度分科会を開催し、平成30年３月下旬を目途に検討結果を取りまとめ。
○　議論に資するために、情報開示に係る制度や事例の調査を同時並行で行う（１月中旬～２月中旬を予定）。
○　民間企業のセキュリティ対策の情報開示に関するガイドラインを作成するとともに、分科会における検討の結果をサイバーセキュリティタスクフォースに報告。

12月	平成30年１月	２月	３月	
● 第１回（12/13） ・これまでの取組 ・構成員からのプレゼンテーション ・意見交換	● 第２回 ・構成員からのプレゼンテーション ・意見交換	● 第３回 ・調査報告 ・意見交換	● 第４回 ・論点整理	● 第５回 ・とりまとめ

〇調査研究の請負
契　約　日：１月中旬想定
調査期間：契約日～２月中旬
調査事項：
・情報開示に関する海外の制度の調査
・米国における情報開示の事例調査
・国内における情報開示の事例調査