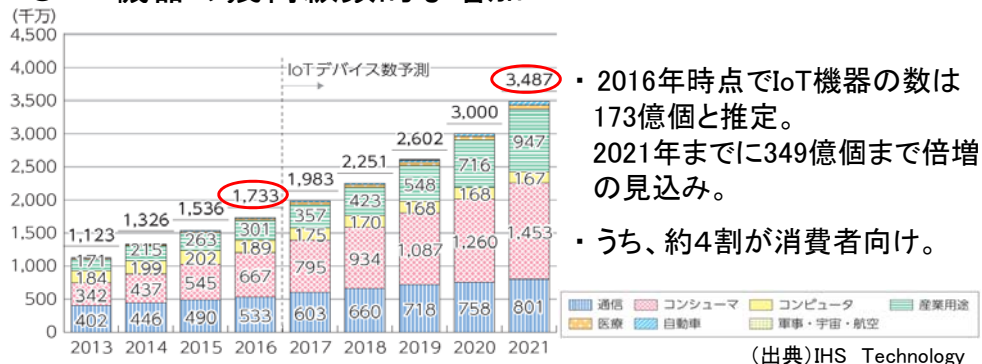


情報開示分科会における検討について

総 務 省
情報流通行政局
サイバーセキュリティ課

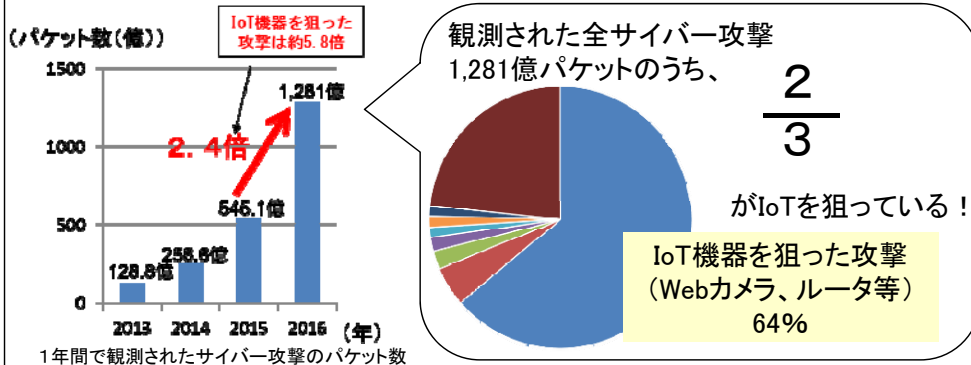
現状

○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。

○IoT機器を狙った攻撃が急増



○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。

簡単なID、パスワードを使用した機器が多く感染 (例) ID: root passwd: 1234

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)

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。

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。

構成員

秋保 宏之 損害保険ジャパン日本興亜株式会社 企画開発部長

石原 康史 東京海上日動火災保険株式会社 企業商品業務部 部長

鵜飼 裕司 株式会社FFRI 代表取締役社長

大杉 謙一 中央大学 法科大学院 教授

(主査) 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

梶浦 敏範 一般社団法人 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

加藤 俊直 PwCあらた有限責任監査法人
システム・プロセス・アシユアランス部 パートナー

源田 浩 三井住友海上火災保険株式会社 公務開発部 部長兼開発室長

野口 和彦 横浜国立大学 大学院 環境情報研究院 教授

【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

① 情報開示することが望ましい項目及びその粒度

(構成員の御意見)

- 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。(鵜飼構成員)
- 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。(鵜飼構成員)
- 有価証券報告書の記載について、詳細に記載すると営業秘密等々に触れることがあるため、一般論のような記載にならざるを得ないのではないか。(岡村主査)
- 情報開示すべき項目については、業種、業態等によって価値観が異なるので、ユースケースを示して議論する必要があるのではないか。(梶浦構成員)

② 情報開示するにあたって望ましい媒体及びフォーマット

(構成員の御意見)

- 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。(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。(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。また、対策についてステークホルダーに説得力を持って開示できれば良いが、その方法は簡単ではないと思う。(大杉構成員)
- 開示資料として誰でも見られるような書面を作成するという話では必ずしもなく、むしろ相対の中で取引相手に示していくということもあるのではないか。(大杉構成員)

【検討事項2】 情報開示の普及の方策について

① 情報開示の普及方策

(構成員の御意見)

- 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。(加藤構成員)
- 企業が情報を出すだけでなく、その情報がしかるべきところへ流れていくプロセスや、評価の基準が必要なのではないか。(梶浦構成員)
- 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。(教学構成員代理)

② 普及方策のうち、特に保険商品の利用の普及方策

(構成員の御意見)

(本日ご議論いただければと存じます。)

- 平成29年12月から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。
- 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。

平成29年12月	平成30年 1 月	2 月	3 月
<p>●</p> <p>第1回 (12/13)</p> <ul style="list-style-type: none"> ・ 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 		<p>●</p> <p>第2回 (2/1)</p> <ul style="list-style-type: none"> ・ 構成員からのプレゼンテーション ・ 意見交換 	<p>●</p> <p>第3回</p> <ul style="list-style-type: none"> ・ 調査報告 ・ 論点整理 ・ 意見交換
		<p>●</p> <p>第4回</p> <ul style="list-style-type: none"> ・ 報告書（案） ・ 意見交換 	<p>●</p> <p>第5回</p> <ul style="list-style-type: none"> ・ とりまとめ
	<p>○調査研究の請負 調査期間：1月中旬～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</p>		<ul style="list-style-type: none"> ・ 報告書（案）に対する意見募集（パブリックコメント）