

「情報開示分科会」における検討について

情報開示分科会

平成30年4月

- 民間企業におけるセキュリティ対策の情報開示による「セキュリティ対策の見える化」を通じて、民間企業の経営層が自社のセキュリティ対策の現状を認識し、また、他社の状況と比較することにより、さらに必要な具体的な対策を検討し、導入する「セキュリティ対策の好循環」が起こる環境の実現が期待される。
- 情報を開示するにあたっては、開示の対象者によってその考え方、取組が異なることから、報告書(案)においては、①社内の情報共有(第一者開示)、②契約者間等の情報開示(第二者開示)、③社会に対する情報開示(第三者開示)の3つの側面に分けて整理している。

これまでの開示の考え方

⇒ 社会に対する情報開示(第三者開示)

↓
本分科会での整理

セキュリティ対策の開示(共有)の3つの側面

社内の情報共有(第一者開示)

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

【意義】

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

契約者間等の情報開示(第二者開示)

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

【意義】

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

社会に対する情報開示(第三者開示)

社会の幅広い対象に向けて、自社のセキュリティ対策を開示すること。

【意義】

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

検討結果

社内の情報共有(第一者開示)

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

契約者間等の情報開示(第二者開示)

- ・ 契約者間等で確認すべき事項や必要な対策の整理、サプライチェーン全体またはグループ全体における情報共有体制の構築の促進が必要である。
- ・ サイバーセキュリティ保険について、対策の実施及び開示のインセンティブとなるような割引制度の普及や、グループ全体・サプライチェーン全体で一括して加入するような保険商品の展開が期待される。

社会に対する情報開示(第三者開示)

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

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

今後の取組

(社内の情報共有に向けた橋渡し人材の育成)

1. 人材のスキルの具体化、スキル取得のための教育コンテンツの開発・普及、スキル認定を行う仕組みを産学官により構築するための検討。

【平成30年度中を目途に方向性を整理】

(関係者間の情報共有促進のための仕組みづくりの検討)

2. 米国等におけるISAO(※)等の動向等について調査するとともに、**公的支援のあり方について検討。**

【平成30年度中を目途に検討結果を取りまとめ】

(※)ISAO:Information Sharing and Analysis Organization

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

【モデル事業については平成30年度に検討】

(第三者開示の促進に向けたガイドラインの策定)

4. 「**セキュリティ対策情報開示ガイドライン(仮称)を策定・公表。**

【平成30年秋を目途にガイドラインを策定】

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

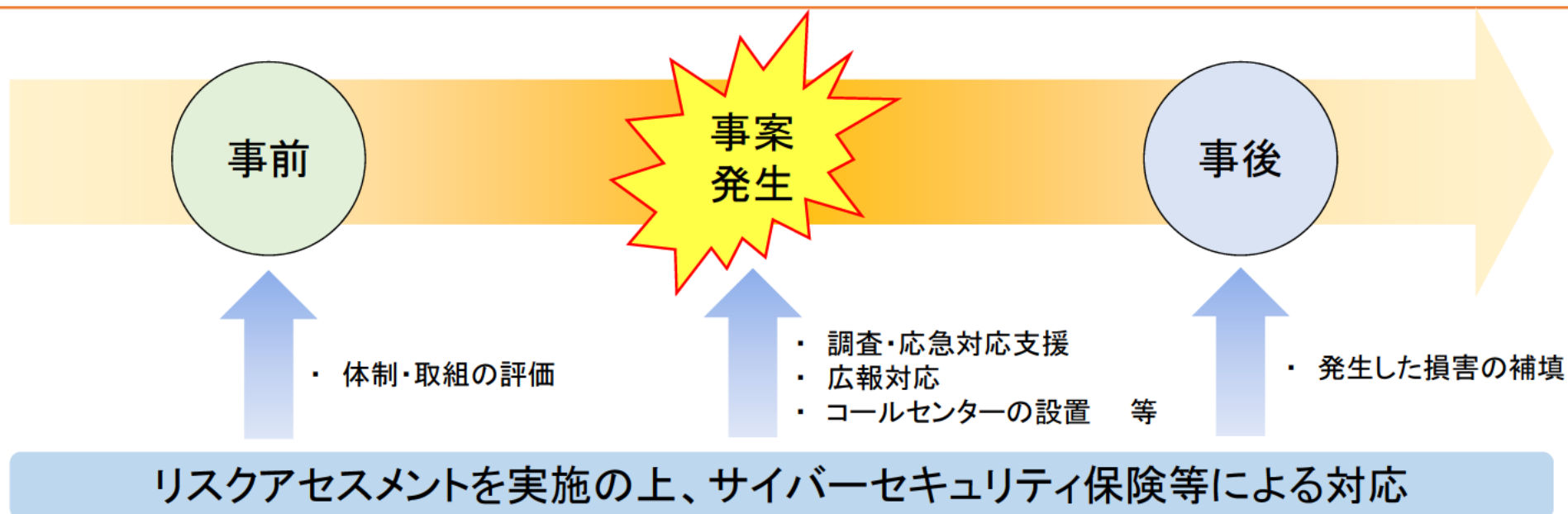
【支援税制の運用にあわせて適宜実施】

サイバーセキュリティ保険による取組の推進

- 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

- 第三者開示 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

今後のスケジュール

- 第4回の議論を踏まえ、報告書(案)を調整した後、意見募集(パブリックコメント)(20日間)を実施。
- 第5回(5月中下旬開催予定)において、報告書(案)に対する意見募集の結果を報告するとともに、報告書を取りまとめ。
- とりまとめた報告書をもとに「セキュリティ対策情報開示ガイドライン」(仮称)の案を作成し、第6回(6月開催予定)において議論することを予定。

平成29年	平成30年						
12月	1月	2月		3月	4月	5月	6月
● 第1回 (12/13)		● 第2回 (2/1)	● 第3回 (2/27)		● 第4回 (4/6)	● 第5回	● 第6回
<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 		<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 	<ul style="list-style-type: none"> ・調査報告 ・論点整理 ・意見交換 		<ul style="list-style-type: none"> ・報告書(案) ・意見交換 	<ul style="list-style-type: none"> ・意見募集の結果 ・報告書 とりまとめ 	<ul style="list-style-type: none"> ・ガイドライン(案) ・意見交換
							
					<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)(20日間) 		

	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・アシュアランス部 パートナー
	野口 和彦	横浜国立大学 大学院 環境情報研究院 教授
	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
	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