今後の検討の方向性について

平成27年2月25日
事務局

本研究会での検討スケジュール（案）

【 検討スケジュール 】

【第１回】 ・ 国内外におけるセキュリティリスクの状況

【第２回】 ・ 対策の方向案・各論の深掘り
【各論に係るプレゼン】
セキュリティマネジメントの評価のあり方について（横河電気）

【第３回】 ・ 対策の方向案・各論の深掘り
【各論に係るプレゼン】
・ 海外におけるセキュリティ政策及び重要インフラ対策の動向について（IPA／ジェトロNY）
・ セキュリティリスク情報の共有のあり方について

【第４回】 ・ 具体策検討
【各論に係るプレゼン】
・ 我が国におけるセキュリティ経営のあり方について（P)

【第５回】 ・ 具体策検討
【各論に係るプレゼン】
・ セキュリティリスクの市場化の方策について（P)

【第６回】 ・ 取りまとめ

（参考） 第１回研究会で提示した論点

（参考）本研究会での論点（案）（１／２） 【第１回資料３より抜粋】

１．セキュリティ経営の方法論

- 我が国企業の経営でのセキュリティのプライオリティを高めるためにどのような対応があるか。
- 企業のセキュリティ対策への支出の効果をどのように見える化をするべきか。
- 情報システムの外部委託について、どのように適切に管理するべきか。
- 企業の経営者やセキュリティ担当者が最新の情報を共有するため、どのような社外とのネットワーキングが必要か。

２．セキュリティ経営を評価する仕組み

- 企業のセキュリティに関する情報開示において、どのような枠組みの下、どのような情報を開示することが適切か。
- 企業のセキュリティ経営について、第三者による認証制度をどのように活用すべきか。

（参考）本研究会での論点（案）（2／2） 【第1回資料3より抜粋】

3. 情報共有のあり方

- 報告義務が無い一般的な情報漏洩事案について、どのように情報収集し、他の企業のセキュリティ対策促進に結びつけるか。

4. セキュリティリスクの市場化

- 企業に「合理的なセキュリティ投資」を促していくため、どのような情報提供が必要か。
- セキュリティ経営を促すインセンティブとして、サイバー保険の普及等を含めた環境整備をどのように進めるか。

5. 2020年東京オリンピックパラリンピックに向けた対応

- 重要インフラ事業者その他経済社会に影響を与える事業者等について、どのように対策を促進していくべきか。

  ※重要インフラは、「情報通信」、「金融」、「航空」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」、「化学」、「クレジット」及び「石油」の13分野（重要インフラの情報セキュリティ対策に係る第3次行動計画（平成26年5月19日情報セキュリティ政策会議決定））

- オリンピックを契機として、セキュリティ関連の成長産業をどのように発展させていくか。

（参考） サイバーセキュリティを巡る直近の動き

（参考）

Keidanren
Policy & Action

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17日
一般社団法人 日本経済団体連合会

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。

（参考） 民間部門のセキュリティ対策を促す諸外国の取組み

米国

政府主導で自主的取組み促進

○ 民間部門によるサイバーセキュリティ対策の義務付けを行う関連法案の不成立

民間部門の自主的な取組を促進する枠組み

① 重要インフラのサイバーセキュリティ強化のためのフレームワーク（2014年2月）

- 国立標準技術研究所（NIST）が対策基準として策定。
- 消費者保護などのテーマ別に官民フォーラムを開催し、対策状況等を共有し、フレームワーク採用を促進。
- 国土安全保障省等がサイバー保険の活用等のインセンティブ策を検討のほか、フレームワーク導入に向けた評価ツールなどの支援プログラムを用意。

② 民間部門によるサイバーセキュリティ情報の共有強化（2015年2月）

- サイバー攻撃情報と脆弱性情報を共有する業種別の官民情報共有網の構築促進に関する大統領令を発出。
- 国土安全保障省が、当該官民情報共有網の構築を支援する予定。

ドイツ

対策を法定化

○ IT戦略「デジタル・アジェンダ2014-2017」に基づき、重要インフラ事業者に対して、基準に基づく対策を**義務づける法案を内務省が提案**

（2014年8月）

【その他の主な施策】

- 評価・認証の推進
- 信頼性のあるITセキュリティ製品使用の拡充
- 重要インフラへのサイバー攻撃を分析・情報共有する市民保護庁の専門性強化

英国

政府主導で自主的取組み促進

○ ロンドンオリンピック開催にあたって、重点的に対策を講じるべき重要インフラ8分野を特定。

○ 官民のCIOグループと実務者グループを大会4年前に構成し、官民における対策の進捗管理。

○ 大会直前には、官民合同のサイバー演習等を実施。

事務局からの問題提起

民間部門におけるセキュリティ対策の促進に向けた重点的取組み案

○国がイニシアティブを取った、指針策定、ベストプラクティスの共有等による対策

【施策例】

- IoT時代に必要なセキュリティに係るガイドラインの策定。
- IoTのユースケースを業種毎別等に議論し、それに応じたセキュリティ対策を検討等するための官民フォーラムの設置。

○セキュリティ対策企業を評価・支援し、自主的取組みを促進

【施策例】

- 官民のサイバー攻撃情報共有網の拡充。
- 企業のセキュリティ対策に関する情報開示のあり方の検討。
- セキュリティ対策状況の第三者評価制度の確立。

○人材育成・研究開発による底上げ

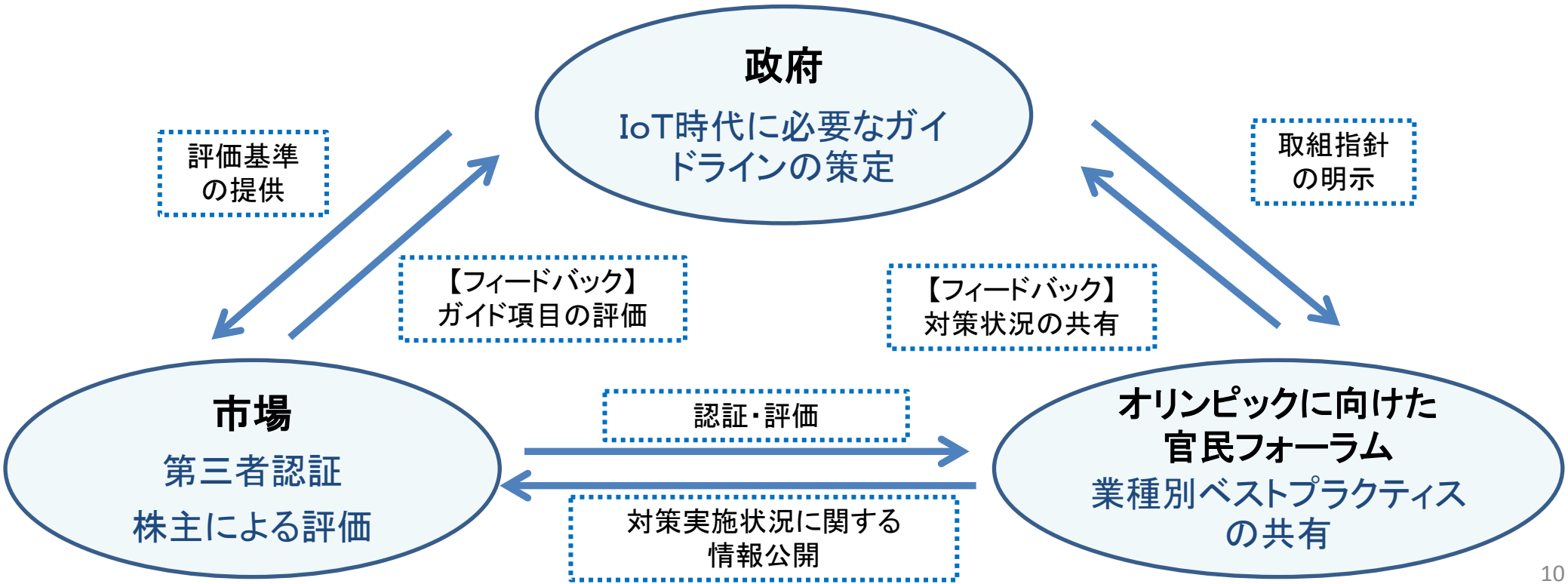
【施策例】

- 大学教育・初等中等教育からのセキュリティ教育の拡充。
- ユーザー企業向けのセキュリティマネイジメント人材試験の創設。
- 低コストで効果の高いセキュリティソリューションを提供するための技術開発、抜本的な対策を講じるための研究開発。

IoT社会に向けたセキュリティ対策の強化（案）

○ IoTの広まりとそれへのサイバー攻撃の経済・社会への影響及び諸外国における取組みを踏まえれば、政府がイニシアティブを取って、
- IoT時代に対応した業種横断的共通ガイドライン及び個別の主要ユースケースに応じたガイドラインの策定。
- 2020年に向けた、官民フォーラム等による業種横断的、あるいは業種別ベストプラクティスの共有等が必要ではないか。

○ 第三者認証制度の活用や、企業における対策実施状況に関する情報開示の促進により、対策実施企業が評価される環境づくりが必要ではないか。



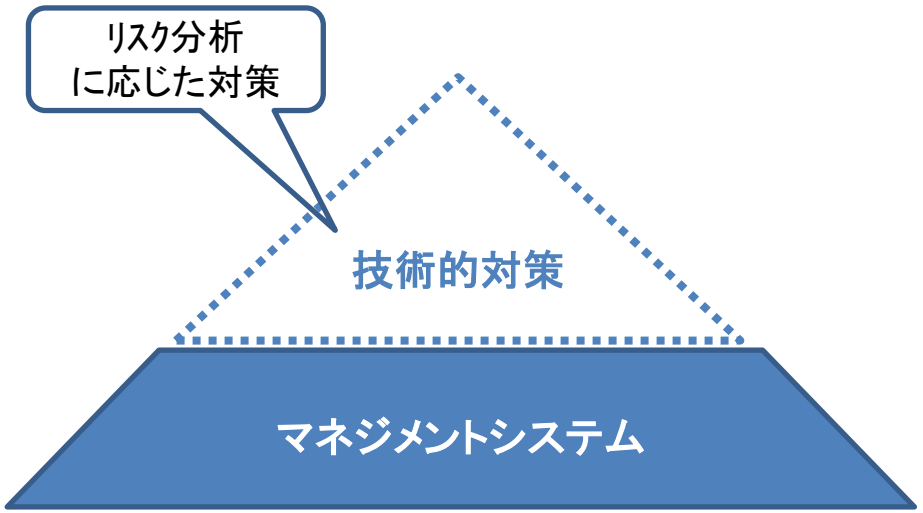
第三者認証制度のあり方（案）

○　従来のISMSやCSMSの第三者認証では、セキュリティ対策実施に係るPDCAをマネジメントとして回しているかについて認証を実施。

○　他方、例えば、ウイルスソフトで検知できない新型マルウェアなど高度化したサイバー攻撃に対応した対策を未実施でも認証可能。

○　こうした中、対策実施企業を市場等が評価するためには、PDCA対策に加えて、一定の技術的対策基準も加味した認証制度により、セキュリティ強度を測ることが必要ではないか。

マネイジメントシステムに基づく技術的対策の実施



第三者認証の対象分野

	情報システム	制御システム
マネジメントシステム	Pマーク（更新2年） ISMS認証（更新3年） CSMS認証（更新3年）	
技術的対策		EDSA認証（期限なし） SSA認証（期限なし）

人材育成のあり方について

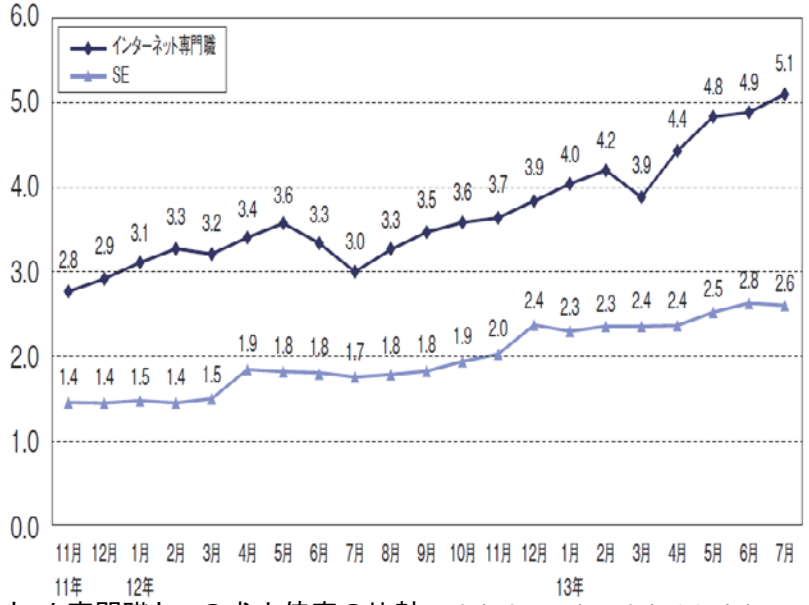
○　IT人材市場については、インターネットビジネスにおける求人が盛んな傾向。セキュリティ人材については、現状、ベンダーにおいて不足しているという声がある一方、求人が多くは出ていないとも言われている。

○　経産省では、セキュリティキャンプなどの若手人材育成の取組みの他、以下を実施。今後、どのような取組みが必要か。

① 技能の見える化のため、脆弱性診断に必要な技能を評価する試験を今年度試作
② 情報処理技術者試験におけるセキュリティマネイジメント人材の試験区分の検討

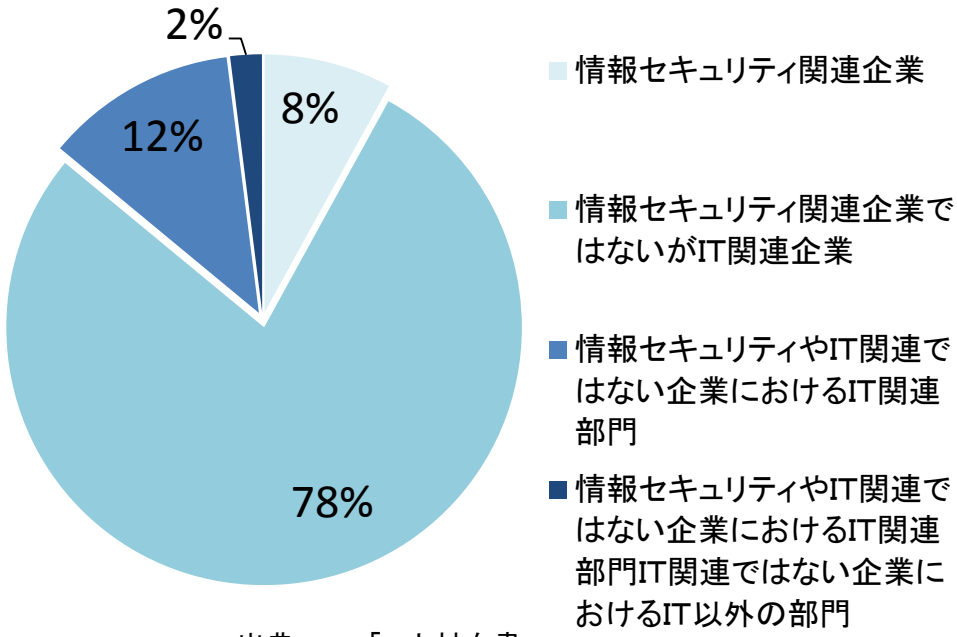
○　また、大学におけるセキュリティ専門教育の取組みも行われているが、どのように促進されるべきか。

（参考）インターネットビジネスの求人倍率が高い



インターネット専門職とSEの求人倍率の比較　（有効求人人数÷有効登録者数／2013年7月現在）／株式会社リクルートキャリア社内調べ

（参考）セキュリティキャンプ卒業生の就職先



出典：IPA「IT人材白書2014」

研究開発のあり方について

○ セキュリティソリューションにおける海外ベンダのシェアは、検知の段階におけるソリューションで高くなっており、サイバー攻撃情報の収集能力の面で、国内ベンダよりも海外ベンダが優位になっている可能性。
○ サイバー攻撃が高度化する中、例えば、不正通信の検出においては、人海戦術の要素が高まっているとも言われているが、R&Dや研究開発が対応できる要素もあるのか。
○ さらに、（下図の「実施すべき機能」には項目は無いが）攻撃者優位の状況を変え得るような（Game Change）、攻撃の抑止に、研究開発は寄与し得るのか。

サイバーセキュリティリスク管理で実施すべき機能※1		主な製品・技術	技術開発動向	海外ベンダ製品シェア※2
特定	リスクアセスメント	検査ツール	検出率の向上、Webアプリ技術の発展への対応	52.8%
防御	アクセス制御	認証技術	リモートアクセス認証強化	40.0%
		統合ID管理	外部IDとの連携	36.5%
	データセキュリティ	データベース、メールセキュリティ	DLP等、機能の統合	45.1%
	保護技術	デバイス・端末管理	運用面での機能向上	7.0%
検知	異常・イベント継続的モニタリング	ログ管理・分析	SIEM等、複数機器のログ分析による相関分析	77.8%
			制御システムのログ蓄積・管理・分析	
		DDoS対策	バックボーン上の制御、クラウドによるネット最適化	76.5%
		Webセキュリティ	CDN,DDoS等への総合的Webセキュリティ対策	74.1%
		標的型対策	振る舞い検知（カーネル/BIOSレイヤ）・インディケータ等、	73.1%
			ログ分析による検知技術、サンドボックス、インテリジェンス等	
		ファイアウォール/VPN/UTM	次世代ファイアウォールによるアプリケーション可視化	62.3%
			制御システムのハードレベルでの片方向通信許可	
		監視ツール	おとりサーバによるマルウェアの捕獲・分析	42.0%
			高検知、高スループット	
		ウイルス対策	ホワイトリストによるマルウェア実行抑止	24.9%
			マルウェアの静的解析（コード解析）	
			レピュテーションを用いた未知ウイルスへの対応	
		メールフィルタリング	レピュテーションを用いたフィルタリング精度向上	20.1%
		Webフィルタリング、セキュリティ	レピュテーション、Web改ざん検知・防止・自動修復	0.0%
対応	対応計画分析、改善	フォレンジック	予兆の検知	30.1%
復旧	復旧計画、改善	－	（組織的対策が中心）	－

※1 「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」（NIST、2014年）に基づく分類
※2 「2014 ネットワークセキュリティビジネス調査総覧」（富士キメラ総研、2014年）よりシェアが特定されたベンダのみを対象として算出