経済産業省

資料３

事務局説明資料

平成30年8月９日

経済産業省　商務情報政策局

サイバーセキュリティ課

１．前回の議論のまとめと今後の方向性
２．コラボレーション・プラットフォーム
３．情報セキュリティサービス審査登録制度
４．検証基盤の構築
５．委託時の責任範囲の明確化
６．セキュリティ産業における法的課題への対策

前回の主なご意見と今後の方向性

前回WGでの主なご意見	今後の方向性
ユーザーに対するサイバーセキュリティの情報発信が上手くできると、セキュリティ産業の成長にも繋がるのではないか	WG2（投資家に対するセキュリティの啓発） **WG3（コラボレーション・プラットフォーム）**
セキュリティ製品やサービスの契約時に、責任範囲についてしっかりと合意形成をすることが重要ではないか	**WG3（委託時の責任範囲の明確化）**
事業者側のサイバーセキュリティに関する組織力をレーティングできる仕組みがあるとよいのではないか	WG2（可視化ツール）
ベンチャー企業に導入実績の課題を乗り越えさせ、マーケットインを支援する施策が必要ではないか	**WG3（コラボレーション・プラットフォームの活用）** **WG3（検証基盤の構築）**
ベンチャー企業の視点で見ると、実環境で評価できる環境を提供すべきではないか	
セキュリティビジネスの海外展開に向けて他分野との連携を図るべきではないか	
海外展開において、注意すべき海外の法規制が整理されているとよいのではないか	**WG3（セキュリティ産業における法的課題への対策）**
サイバーセキュリティは全産業に寄与する課題であり、法規制と運用を整理する取組を、関係省庁と協力して具体的に行っていくことが大切ではないか	

企業との意見交換の整理

- 第一回WG3（平成30年4月4日）以降、一部の企業とサイバーセキュリティビジネスの成長や今後の戦略等について意見交換を実施。期待される政策の方向性としては、産業サイバーセキュリティ研究会各WGにおける政策的出口とも一致。

事業としての課題

- 社内対応と経営者の理解獲得に時間とリソースが割かれている。
- セキュリティを独立の事業として捉えておらず、人材獲得や体制が整備できない。（目立つと標的になるリスクがある）

潜在リスク

- IoTの進展により、全ての製品、サービスがサイバーセキュリティリスクに晒されている。特にソフトウェアの脆弱性がリスク脅威となっている。
- 日本製品であれば安全という神話が崩壊する恐れ。

解決策

＜人材＞

- 三段階に分けた対応
  - ①経営人材：海外からのヘッドハンテイング
  - ②トップレベルのハッカー：シェアリングモデル
  - ③ボトムライン：韓国、インドなどの海外勢の動員
- 必要な人材モデルの可視化

＜With Securityにおける市場＞

- 製品・システムに対する**政策的なリスク評価スキームを構築**

＜For Securityにおける市場＞

- 中小企業向けセキュリティ市場の活性化
- 我が国発の製品・サービスの創出

＜WG２＞セキュリティ人材活用モデルの構築

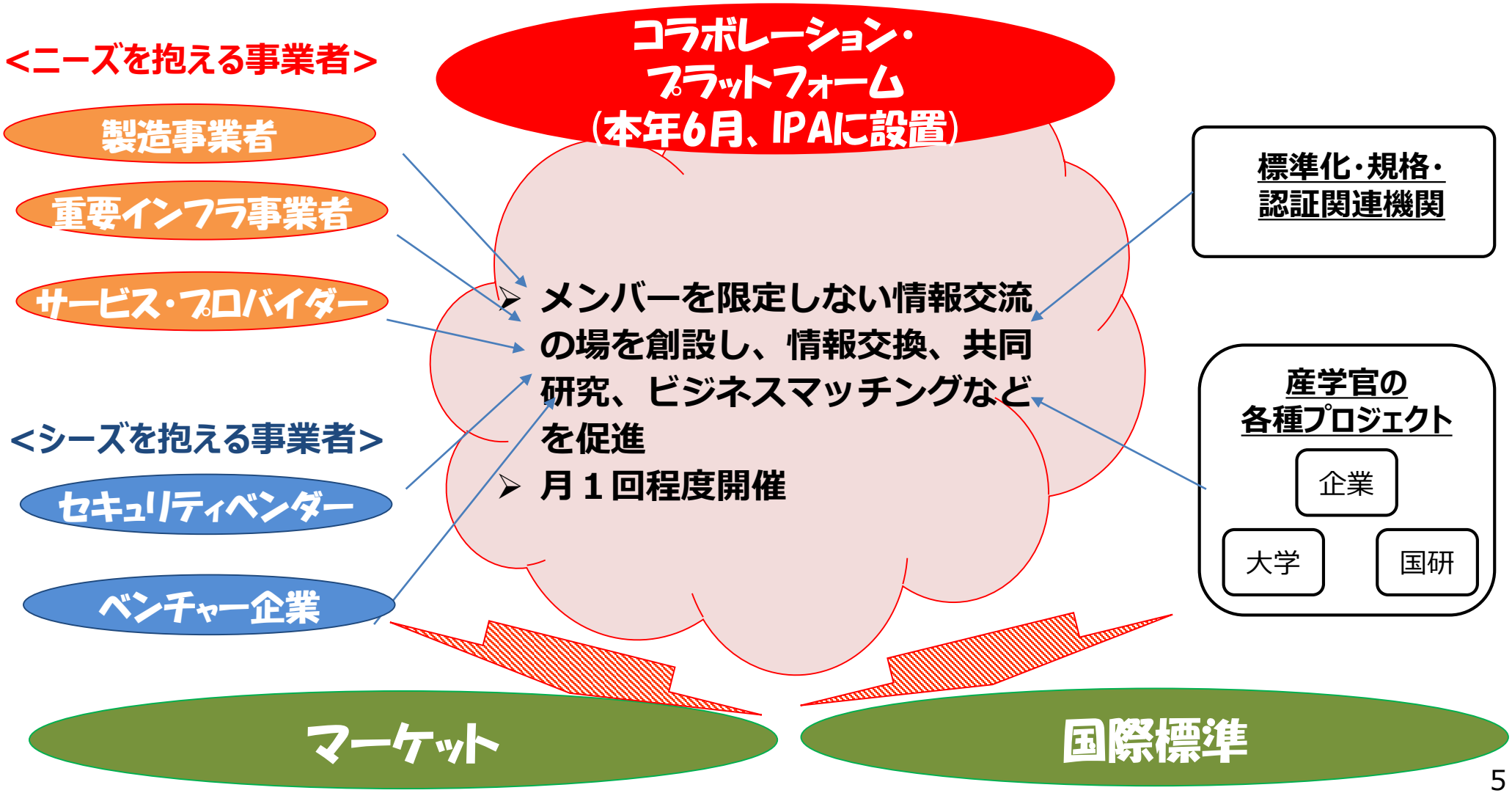
＜WG３＞コラボレーションプラットフォーム

＜WG３＞検証基盤の構築

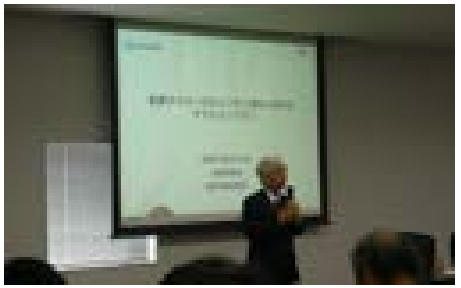
１．前回の議論のまとめと今後の方向性
２．コラボレーション・プラットフォーム
３．情報セキュリティサービス審査登録制度
４．検証基盤の構築
５．委託時の責任範囲の明確化
６．セキュリティ産業における法的課題への対策

ニーズとシーズをマッチングする『コラボレーション・プラットフォーム』の設置

- 各WGの活動などを通じて顕在化したニーズとシーズをマッチングする“場”となる『**コラボレーション・プラットフォーム**』を**IPAに設置し、6月から活動を開始。**



コラボレーション・プラットフォームの開催状況


富田理事長(IPA)ご挨拶


前田審議官(経済産業省)ご挨拶

第一回

日時：6月13日（14:00～17:00）
参加人数：179名（情報交換会：99名）
主なテーマ：経済産業省の政策動向、
パネルディスカッション（ビジネス、サプライチェーン）


パネルディスカッション(第一回)

第二回

日時：7月23日（14:00～17:00）
参加人数：104名（情報交換会：74名）
主なテーマ：IoTの発展に潜むリスクと対策、
グループディスカッション
（サプライチェーン、人材、つながる世界の脅威と対策）


グループディスカッション(第二回)

第一回、第二回共に、当初予定していた定員以上の参加申込みがあった。
参加者からは政府との意見交換、最新動向の情報収集、人脈形成等、
様々な視点で有益であったとの声も。

(*)第二回はグループディスカッション実施のため、第一回よりも定員を少なく設定。

コラボレーション・プラットフォームの今後の進め方

- 第一回はパネルディスカッション、第二回はグループディスディスカッションを実施。
- 次回以降も参加者からより多くの意見を引出し、ビジネスマッチングの場として有効活用できるよう、テーマ、実施方法等について検討を重ねていく。

参加目的※

- ビジネスマッチング
- 人脈形成
- 最近のサイバーセキュリティ動向の把握
- 自社のセキュリティ対策の向上
- 政策に対する意見表明　など

議論したい内容※

- 産業IoT(Connected Industries)
- サプライチェーン
- データ利活用・流通
- 人材/教育
- 保険(サイバー保険、契約書保険条項)　など

※第2回コラボレーション・プラットフォーム
アンケートより抜粋

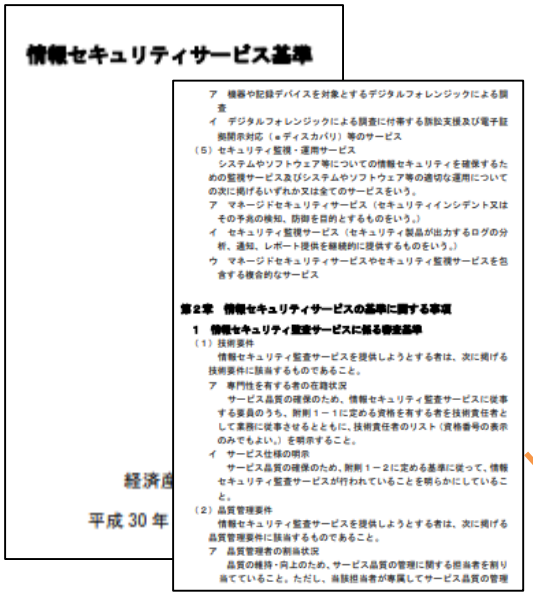
結果をもとに今後の進め方を検討

開催頻度、参加人数
講演やディスカッションのテーマ
業種や参加目的を絞って開催を検討
地方開催も必要か

１．前回の議論のまとめと今後の方向性
２．コラボレーション・プラットフォーム
３．情報セキュリティサービス審査登録制度
４．検証基盤の構築
５．委託時の責任範囲の明確化
６．セキュリティ産業における法的課題への対策

情報セキュリティサービス基準等の策定

- 経済産業省にて、情報セキュリティサービス基準、及び情報セキュリティサービスに関する審査登録機関基準を策定（平成30年2月28日）。
- IPAより情報セキュリティサービス基準に適合するサービスのリストを公開。



情報セキュリティサービス基準

以下の4サービスに関する基準を定める
- 情報セキュリティ監査サービス
- 脆弱性診断サービス
- デジタルフォレンジックサービス
- セキュリティ監視・運用サービス

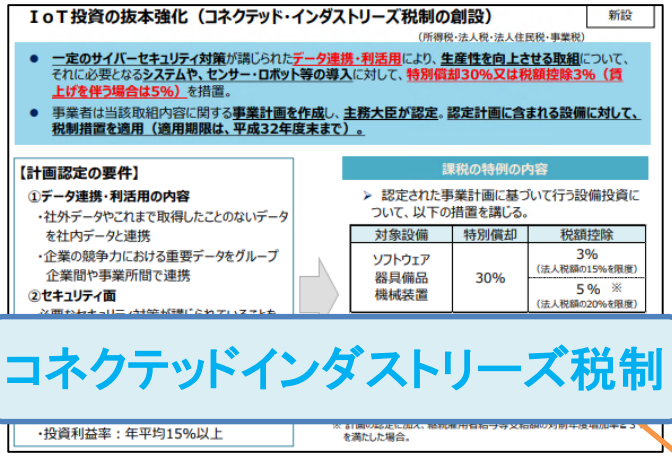
情報セキュリティ監査サービス　　掲載日：2018年7月5日

サービス名称	事業者 ①名称 ②所在地	登録年月日	リスト掲載期限	審査登録機関名
監査およびアシュアランス	①PwCあらた有限責任監査法人 ②東京都千代田区大手町1-1-1 大手町パークビルディング	2018/6/12	2020/6/11	日本セキュリティ監査協会(JASA)
情報セキュリティ監査サービス	①エヌ・ティ・ティ・データ先端技術株式会社 ②東京都中央区月島１－１５－７	2018/6/12	2020/6/11	日本セキュリティ監査協会(JASA)
情報セキュリティプランニング	①株式会社ラック ②東京都千代田区平河町２丁目16番1号平河町森タワー	2018/6/12	2020/6/11	日本セキュリティ監査協会(JASA)
	①株式会社ディアイティ			日本セキュリティ監査協会

47サービスが掲載（7/5時点）
- 情報セキュリティ監査（12サービス）
- 脆弱性診断（14サービス）
- デジタルフォレンジック（10サービス）
- セキュリティ監視・運用（11サービス）

情報セキュリティサービスの利用促進

- 情報セキュリティサービスの利用を促進する措置として、政府調達での活用、税制・補助金における要件化を実施。

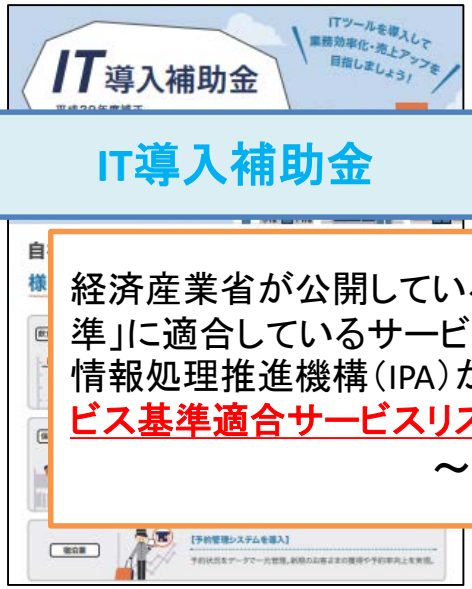


コネクテッドインダストリーズ税制

セキュリティ監視・運用サービスを利用する場合、経済産業省が定める「情報セキュリティサービス基準」及び当該基準を満たすと認められた企業を記載した**「情報セキュリティサービス基準適合サービスリスト」に記載があるサービスを利用している**。

～「認定申請書記入方法」より抜粋

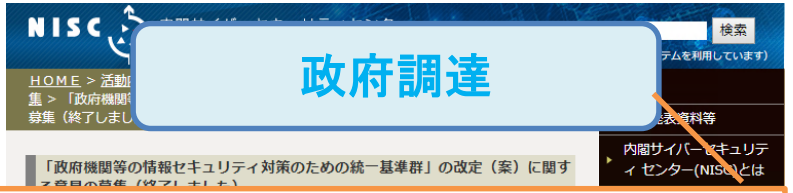
※情報セキュリティ監査、脆弱性診断についても同様に記載。



IT導入補助金

経済産業省が公開している「情報セキュリティサービス基準」に適合しているサービスのリストとして、独立行政法人情報処理推進機構（IPA）が公表する**「情報セキュリティサービス基準適合サービスリスト」を参照することが望ましい。**

～「ITツール登録要領」より抜粋



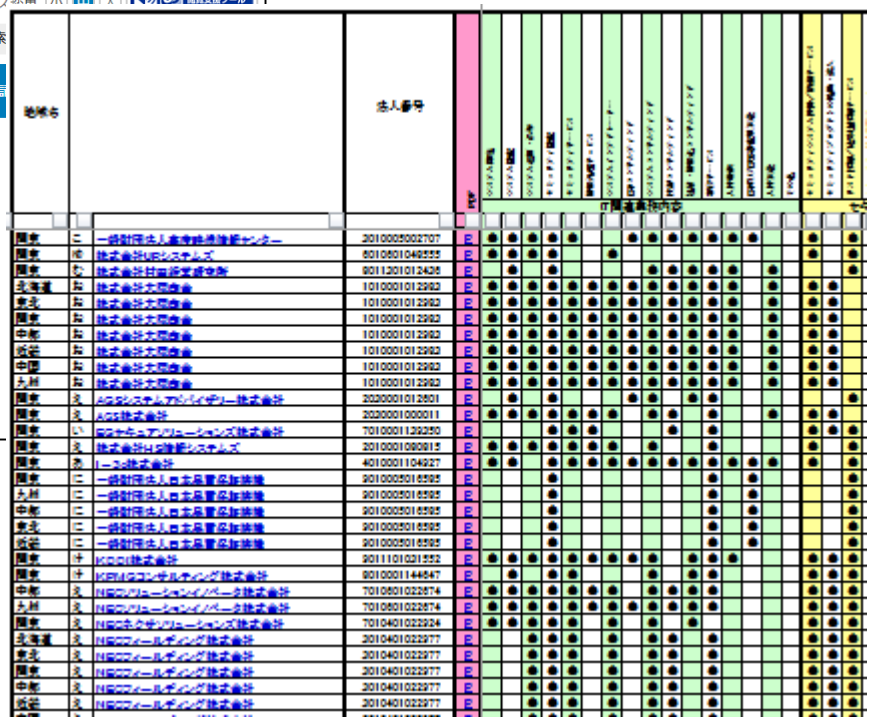
政府調達

経済 産業省が定める「情報セキュリティサービス基準」及び当該基準を満たすと認められた 企業を記載した**「情報セキュリティサービス基準適合サービスリスト」（うちセキュリ ティ監査サービスに係る部分）を活用**するほか、（中略）～参照することも考えられる。

～「政府機関等の対策基準策定のためのガイドライン」より抜粋

監査企業台帳制度

- 自治体等の調達要件でも参照されている監査企業台帳制度 (*)があるが、当該台帳は原則として自己申告であり、申告書の提出があった組織をすべて登録。
- 監査企業台帳については、将来的に登録内容の信憑性がより高い情報セキュリティサービス基準適合サービスリストへ移行し、廃止することを検討。



情報セキュリティ監査企業台帳

(*)情報セキュリティ監査企業台帳とシステム監査企業台帳があり、それぞれ情報セキュリティ監査、システム監査を行う主体を登録する台帳。システム監査企業台帳も調達時にセキュリティ監査目的で使用されているケースもある。

１．前回の議論のまとめと今後の方向性
２．コラボレーション・プラットフォーム
３．情報セキュリティサービス審査登録制度
４．検証基盤の構築
５．委託時の責任範囲の明確化
６．セキュリティ産業における法的課題への対策

検証基盤の構築等によるマーケットインの促進

1. 実戦的サイバーセキュリティ検証基盤の構築：有効性の評価

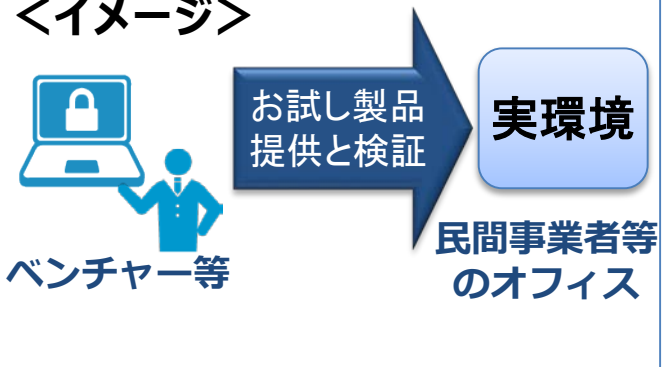
1．セキュリティ製品の有効性検証 ＜性能評価＞

＜イメージ＞

・検証機関が、**セキュリティ製品の有効性を検証し、お墨付きを与えることで、マーケットインを促進。**

2．実環境における試行検証 ＜信頼性評価＞

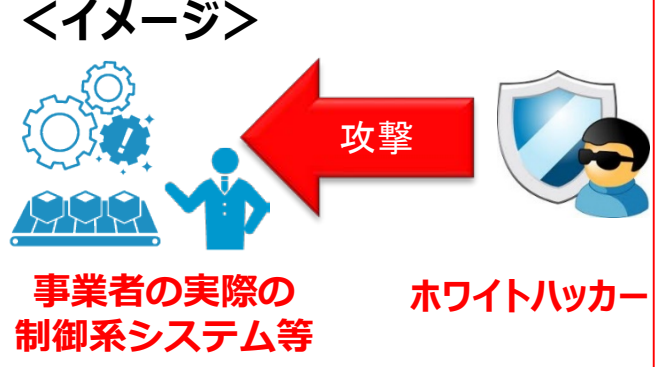
＜イメージ＞



・ベンチャー等が、**製品の信頼性等を検証するために、製品を民間事業者等へ提供し、実績を作る。**

3．ホワイトハッカーの実攻撃検証 ＜ハイレベルなリスク評価＞

＜イメージ＞



・**ホワイトハッカーによる自由な攻撃**を通じて、**重要産業の製品・システムのセキュリティを検証。**

2. 製品・サービスのレーティング制度：選定時の判断指標の整理

エンドユーザが利用している製品・サービスの評価（レーティング）を実施し、常に最新の評価を確認できる仕組みを構築

セキュリティ製品の有効性検証基盤の構築

**１．セキュリティ製品の有効性検証
＜性能評価＞**

- セキュリティ製品について、実績不足をカバーできるよう、国が製品の有効性評価基準を策定し、民間企業がそれに基づく評価の実施を検討。

＜検証のイメージ＞

検証の利用者

・セキュリティベンダー　等

検証の対象

・セキュリティ製品　等

検証環境

・制御系システム(実機)
・パソコン環境(実機)
・仮想環境

検証の実施者

過去のウイルス検体等を活用し、
セキュリティ製品の**有効性を検証**

＜検証により得られる成果＞

有効性検証の基準を
クリアした製品のリスト

我が国発製品の
マーケットイン

検証の実施にあたり必要な仕組み等
(**実証を通じて基準等を整備**)

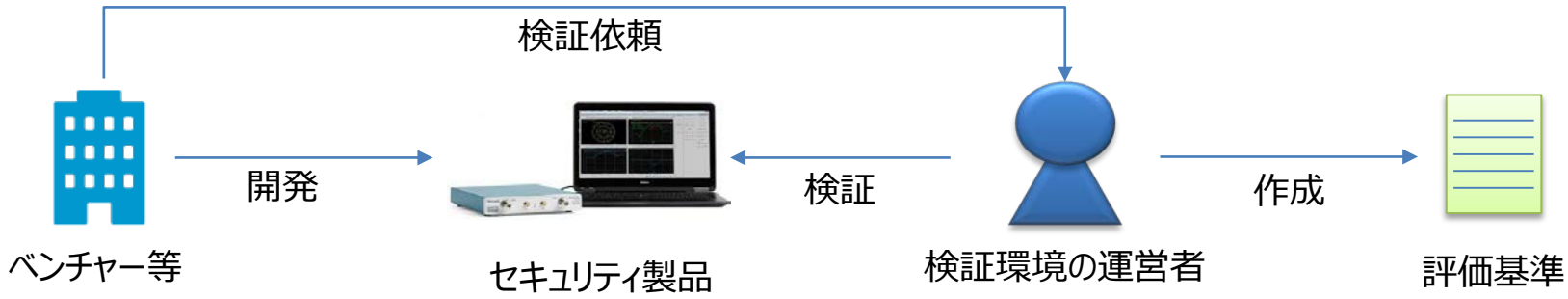
- **有効性の検証手法**
- **検証に使う
攻撃手法、脆弱性情報等**
- **検証実施者の管理能力**
- **有効性の評価基準**

有効性検証基盤の構築へ向けて整理すべき事項

**１．セキュリティ製品の有効性検証
＜性能評価＞**

整理すべき事項	イメージ
検証対象製品	システム環境への依存が低い製品を中心に選定（例：アンチウィルス、秘密分散ソフトウェア等）
利用者	ベンチャー企業やキャピタルなど
検証の軸	セキュリティ検証　（対象製品に既知の脆弱性が存在していなかという観点での評価） 性能検証　（対象製品のセキュリティ機能が一定の水準を満たしていることの評価）
検証に必要な環境	クライアントPC、サーバ、ネットワーク環境、脆弱性診断ツール、その他検証に必要なツール
検証に必要なツール	検証対象の製品分野毎に求められる水準（評価基準）
検証に必要な脆弱性情報等	IPA、JPCERTの保有する情報等を利用
検証環境の運営者	
成果物	評価手法、評価基準、検証実施者の管理能力

＜検証体制のイメージ＞



検証対象製品について

- 情報セキュリティ市場分類区分定義表2012年度版（JNSA、http://www.jnsa.org/result/2013/surv_mrk/2012fymarketresearchreport_apx.pdfを参照すると、セキュリティ製品について以下のように分類できる。
- **これらの中から、特に有効性評価の実施が求められる製品を選定**していく。

ネットワーク系	コンテンツ系
・ファイヤーウォール ・VPN ・IDS/IPS ・WAF ・ペネトレーション ・ネットワーク可視化 ・データダイオード	・ブラックリスト型ウィルス対策 ・サンドボックス型ウィルス対策 ・スパムメール対策 ・URLフィルタリング ・ウェブサニタライジング ・EDR
アイデンティティ管理系	**システムセキュリティ管理系**
・個人認証デバイス ・生体認証デバイス ・ID管理 ・ログオン管理 ・PKI関連	・ログ管理 ・脆弱性検証関連 ・ポリシー管理 ・暗号化 ・ホワイトリスト ・フォレンジック

実環境の提供者と製品提供者のマッチングの促進

**2．実環境における試行検証
＜信頼性評価＞**

- 信頼性が確認されていない製品の採用に、ユーザーは躊躇する傾向あり。このため、ベンチャー企業等による新たな製品が採用されにくい。
- 一方で、ユーザー事業者の中には、有効性が確認できたものを、セキュリティ製品の導入前に、自社等の実環境で信頼性の評価をしたいという意向はあるのではないか。
- こうした状況を踏まえ、実環境における試行検証を促進するため、ユーザー事業者が試行を行う上で注意すべき点の洗い出しと、ユーザー事業者と製品の提供事業者のマッチングを行うこと等を検討。

＜検証のイメージ＞

検証の利用者
・セキュリティベンダー　等

検証環境の提供者
・民間事業者、大学等

検証の対象
・セキュリティ製品　等

検証環境
・オフィス環境　等

実環境に導入し、
セキュリティ製品の信頼性を検証

＜検証により得られる成果＞

導入実績

我が国発製品の
マーケットイン

ホワイトハッカー等による製品等に対する実試験

**3．ホワイトハッカーの実攻撃検証
＜ハイレベルなリスク評価＞**

- サイバー攻撃の影響範囲が拡大する中で、末端のIoT機器まで含めた検証の必要性は増大。
- 検証ビジネスには信頼性が求められる。検証を実施する者に必要な管理能力の整理や、検証手法の整備等の実施を検討。

＜検証のイメージ＞

検証の利用者
・制御メーカー
・機器メーカー
・セキュリティベンダー　等

検証の対象
・制御システム
・セキュリティ製品
・IoT機器　等

検証環境
・制御系システム(実機)
・パソコン環境(実機)
・仮想環境

検証の実施者

ホワイトハッカー等による攻撃を実施し、
対象となる**システム等の脆弱性等を検証**

検証の実施にあたり必要な仕組み等
(**実証を通じて基準等を整備**)

- **AI等を活用した攻撃ツール**
- **検証に使う攻撃手法、脆弱性情報等**
- **検証実施者の管理能力**
(情報の取扱い、脆弱性が見つかったときの対応　等)

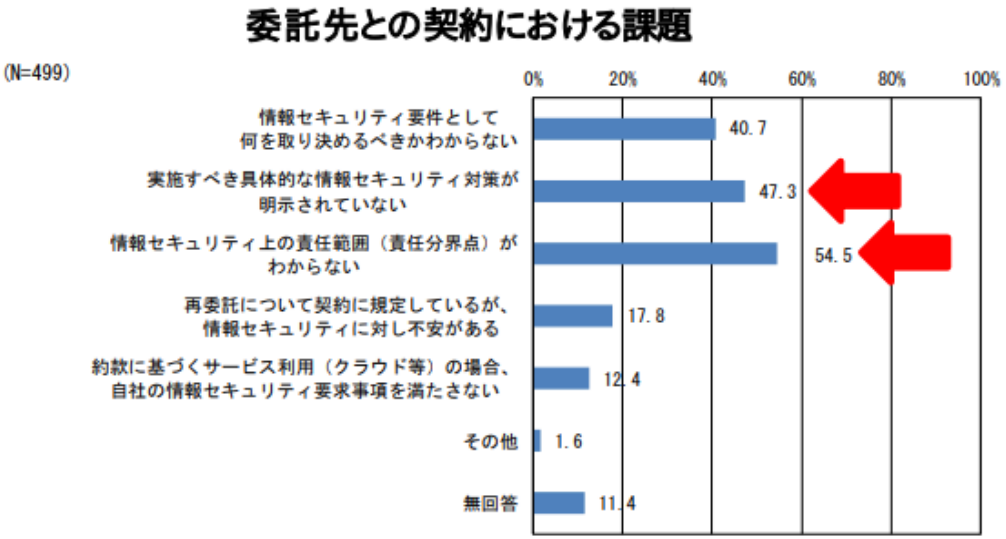
＜検証により得られる成果＞

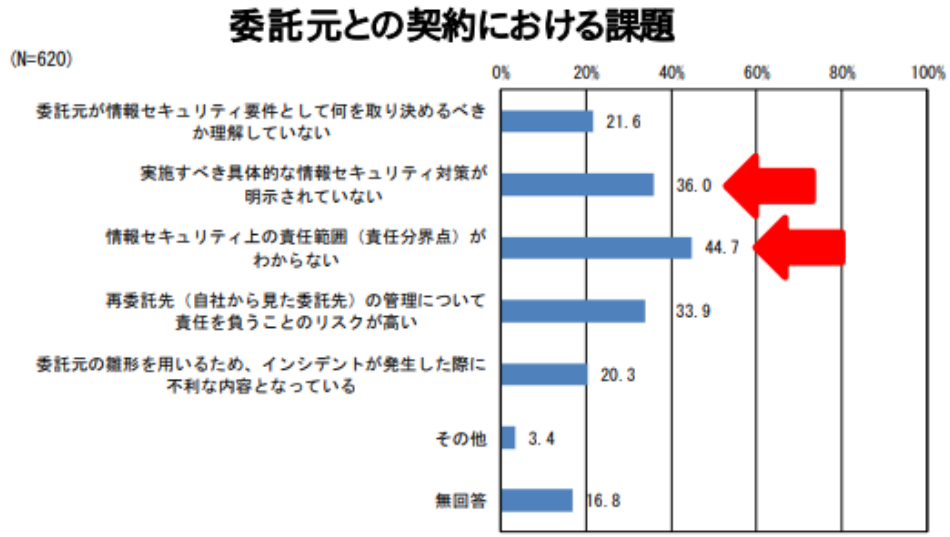
攻撃的検証によりあぶりだされた脆弱性に対する対策	攻撃的検証をクリアしたIoT機器・セキュリティ製品リスト	検証基盤(能力のある検証実施者、検証の仕組み　等)の政府調達への活用
社会全体のセキュリティ向上	我が国発製品のマーケットイン	政府のセキュリティ向上

１．前回の議論のまとめと今後の方向性
２．コラボレーション・プラットフォーム
３．情報セキュリティサービス審査登録制度
４．検証基盤の構築
５．委託時の責任範囲の明確化
６．セキュリティ産業における法的課題への対策

サプライチェーン上の責任分界点における課題

- （独）情報処理推進機構（IPA）にて、サプライチェーンにおいて委託元、委託先がそれぞれ行っているリスクマネジメントの実態を調査（平成30年3月）。
- 課題の一つとして委託契約時における情報セキュリティ上の責任範囲（責任分界点）が明確になっていないことも挙げられており、トラブル発生時の弊害になる可能性。





（出典）ITサプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査（IPA）

契約時の課題として「実施すべき具体的なセキュリティ対策が明示されていない」、「情報セキュリティ上の責任範囲がわからない」の2点が多い

サプライチェーン上のセキュリティに係る責任範囲に関する調査

- IPAにて「サプライチェーン上のセキュリティに係る責任範囲の明確化と合意形成に関する調査を実施予定（平成３０年度）

＜調査内容の案＞

- 責任範囲の明確化に関する実態調査
  - セキュリティの責任範囲として何を、どのような手段で取り決めているのか
  - 海外企業との取引において、セキュリティの責任範囲をどのように取り決めているのか
- 調達仕様や委託契約におけるセキュリティ対策や責任範囲の記載について示された国内外の文献調査

第一回コラボレーション・プラットフォームにおいて、責任範囲としてグレーゾーンは必ず残るため、米国では契約時にサイバー保険に加入することを条件としている事例もあるとの発言があった。本調査では保険の在り方についても検討予定。

１．前回の議論のまとめと今後の方向性
２．コラボレーション・プラットフォーム
３．情報セキュリティサービス審査登録制度
４．検証基盤の構築
５．委託時の責任範囲の明確化
６．セキュリティ産業における法的課題への対策

サイバーセキュリティに関するビジネスを行う際に注意すべき法規制の整理

- **サイバーセキュリティに関するサービスを提供する事業者が業務を行うに当たり、「不正指令電磁的記録（コンピュータ・ウイルス）に関する罪」に問われないよう、業務上の留意事項を整理する必要がある。**また、海外へのビジネス展開の際には、現地の法律などの制度を理解した対応が求められる。
- こうした状況を踏まえ、民間事業者が**セキュリティビジネスを実施するうえで注意すべき事項について論点を整理**する。

前回WG3における指摘

- 企業が海外展開する際にGDPRの関係等、**海外の法制度を意識する必要があるため、海外の法律において気を付ける点が整理されているとよい。**
- サイバーセキュリティは全産業に寄与する課題であるため、各省庁横断で取組んでいくことが重要である。国家全体の価値序列をきちんと定め、それに従って、**法による支えとともに、法規制と運用を序列づける取組みを、関係省庁と協力して具体的に行っていくことが大切ではないか。**

今後の対応案

様々な事案のケーススタディを元に、セキュリティビジネスを実施する上で注意すべき事項等について、**WG3の事務局が、JPCERTの協力を得ながら、事業者や関係省庁へのヒアリングを実施し、論点を整理。**

－セキュリティビジネスに関わる法律の洗い出し

－最新のセキュリティビジネスの実態と法律の関係の整理　等

参考資料

第二回産業サイバーセキュリティ研究会
（平成30年5月30日）資料を一部加工

経営層向け：
経営者にサイバーセキュリティ経営を促す仕組み『３STEPアプローチ』

1st Step

サイバーセキュリティ経営の在り方の明確化

- サイバーセキュリティ経営ガイドラインの普及・定着

2nd Step

サイバーセキュリティ経営を求める仕組みの構築

- **コーポレート・ガバナンス・システム（CGS)に関するガイドライン**のとりまとめに向け、**サイバーセキュリティを位置付け**
- **『取締役会実効性評価』の項目**にサイバーリスクを組み込むことを促進
- **サイバーセキュリティが経営リスクであることの投資家に対する啓発**

3rd Step

市場（投資家）に対するサイバーセキュリティ経営の可視化

- セキュリティの高い企業であることを投資家が評価できるようにするための、**サイバーセキュリティ経営に関する情報の開示の在り方**の検討

サイバーセキュリティ経営を求める仕組みの構築

第二回産業サイバーセキュリティ研究会
（平成30年5月30日）資料を再掲

1．CGSに関するガイドラインのとりまとめに向け、サイバーセキュリティを位置付け

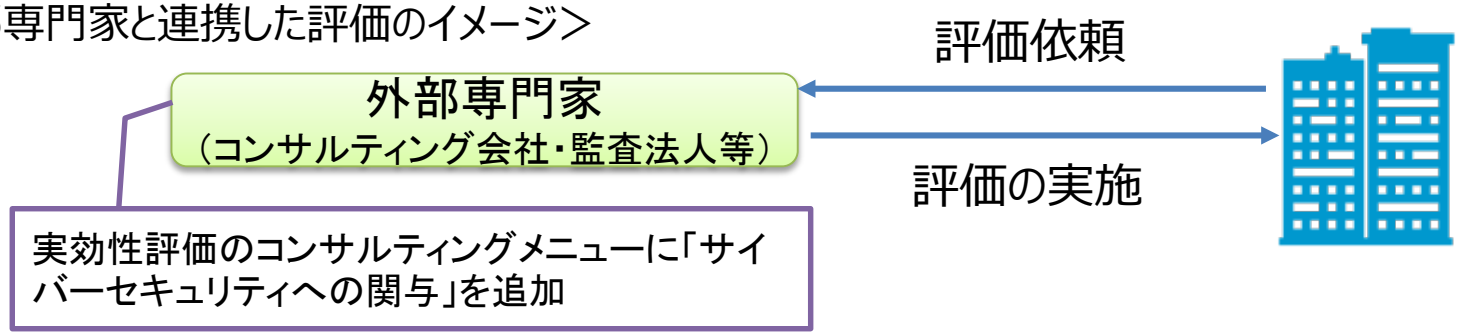
・コーポレート・ガバナンス・システムに関する議論の中で、「守り」のリスク管理の一環として、 サイバーセキュリティ対策を位置付け、コーポレート・ガバナンス・システム（CGS）に関する ガイドラインのとりまとめに向け、サイバーセキュリティを位置付けることを検討。

2．サイバーセキュリティを考慮した取締役会の実効性評価の促進

・サイバーセキュリティへの経営層の関与を、上場企業で行われている『取締役会の実効性評価』の評価項目へ組み込むことを促進。

・投資家に対するサイバーセキュリティの啓発を実施。

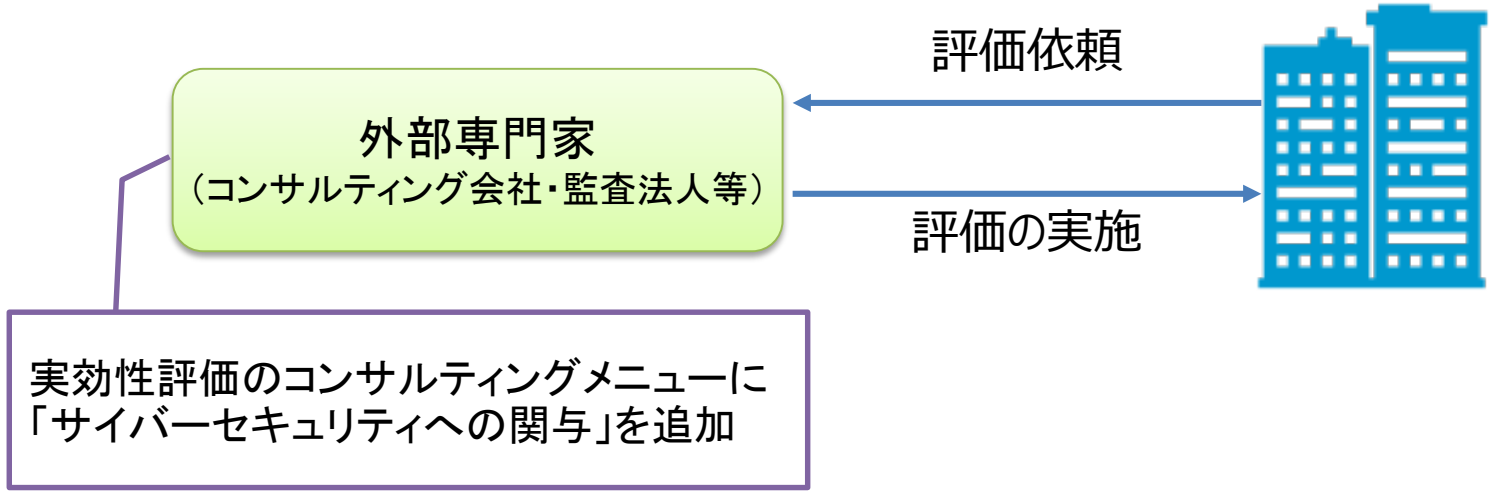
<外部専門家と連携した評価のイメージ>



（参考）投資家に対するセキュリティの啓発

第二回WG2（経営・人材・国際）
（平成30年5月22日）資料より再掲

- 実効性評価の実施方法や評価項目は各企業の目指す姿によってそれぞれ定められるものの、外部の専門家による評価を実施することで、評価結果の信頼性が向上。
- **外部専門家と連携し、サイバーセキュリティへの関与状況も考慮した実効性評価を促進**するとともに、**投資家に対するサイバーセキュリティの教育を実施**。



（参考） 英国における実効性評価の位置づけ
2010年に制定された英国コーポレートガバナンス・コードにおいて、主要な上場企業（FTSE350企業）には**外部の専門家を関与させた評価を少なくとも3年ごとに実施することを要求**。

B.6.2. Evaluation of the board of FTSE 350 companies should be externally facilitated at least every three years. The external facilitator should be identified in the annual report and a statement made as to whether they have any other connection with the company.

（The UK Corporate Governance Code（Financial Reporting Council）より抜粋）

（参考）可視化ツール

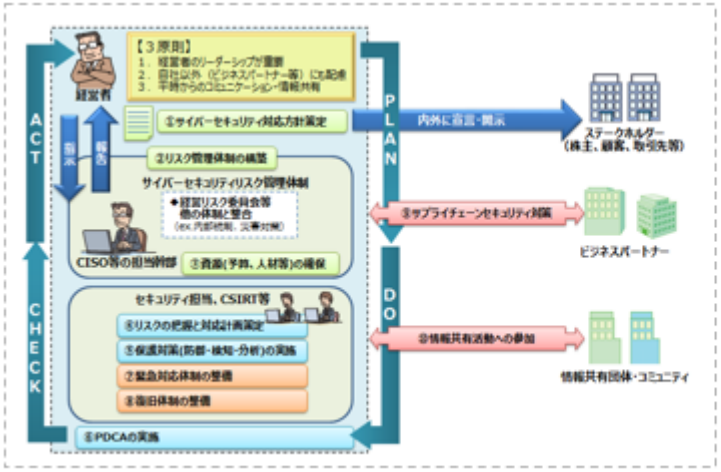
第二回産業サイバーセキュリティ研究会
（平成30年5月30日）資料より再掲(日時のみ更新)

- 企業現場での対策導入を促すべく、**具体的な対策の参考となる『対策事例集』**と**自社の状況（成熟度）を把握するための『可視化ツール』**の整備に着手。
- ツール整備・活用推進のため、**『サイバーセキュリティ経営プラクティス検討会』を発足。**

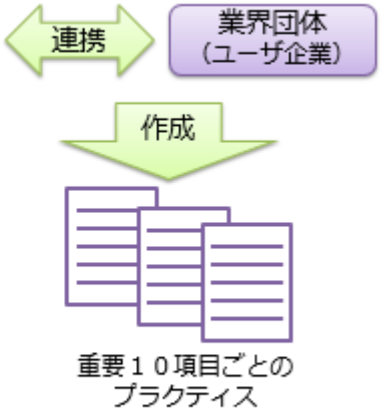
サイバーセキュリティ経営プラクティス検討会(本年7月設置)
(事務局：IPA、経産省)

損保会社 | 産業横断サイバーセキュリティ人材育成検討会 | JUAS | 日本商工会議所

「対策事例集」の作成



サイバーセキュリティ経営ガイドライン



『可視化ツール』のイメージ
(米国NPOとも協力)