経済産業省

資料３

# 事務局説明資料

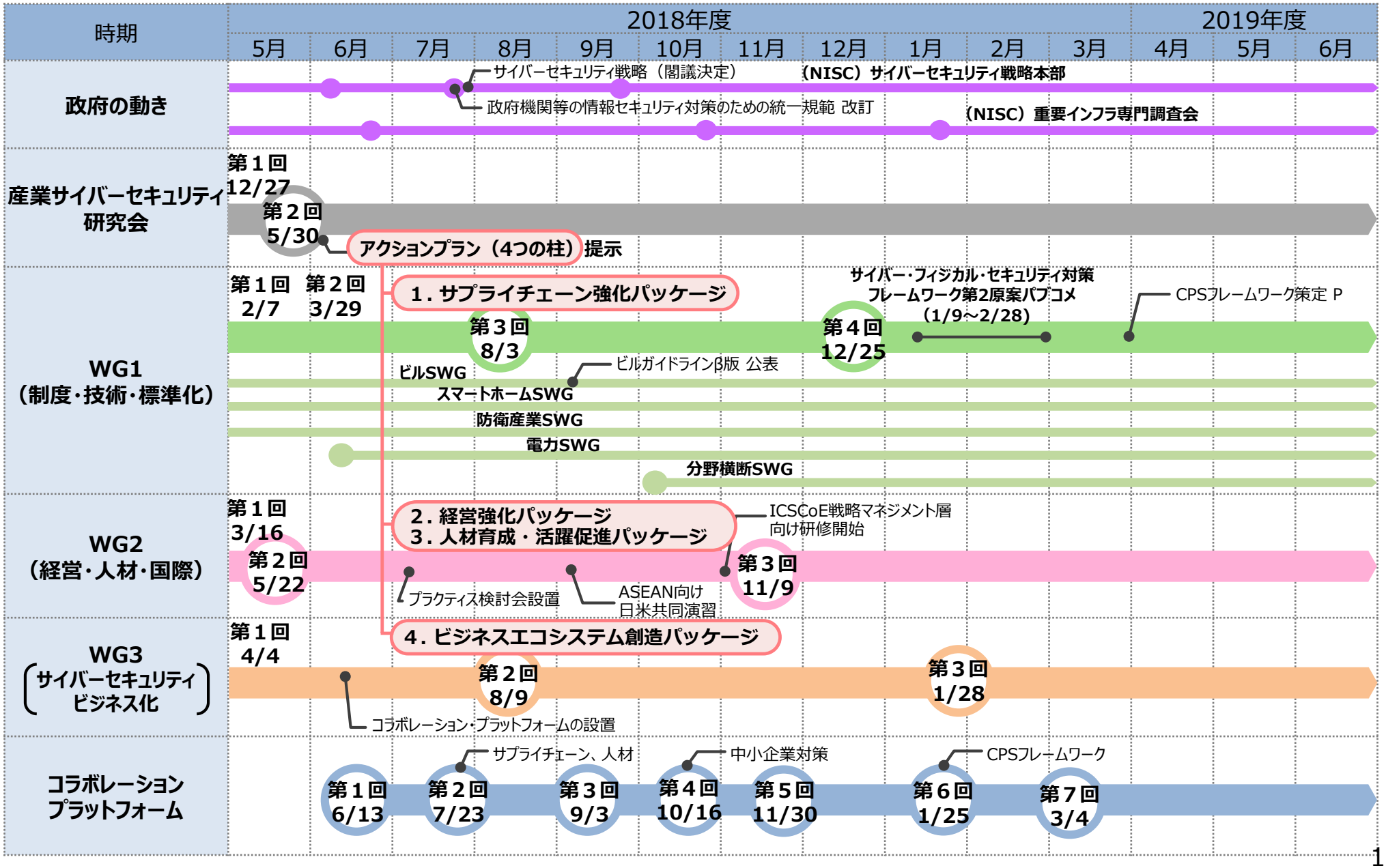
## （産業サイバーセキュリティ研究会WG3
## （サイバーセキュリティビジネス化）第3回）

平成31年1月28日

経済産業省　商務情報政策局

サイバーセキュリティ課

# 産業サイバーセキュリティ研究会関連の動き



# サイバーセキュリティビジネス化に関する政策の方向性

- ビジネス環境を整え、コラボレーション・プラットフォームを軸とした市場展開によりセキュリティ産業の振興・活性化を目指す

## 安心して製品・サービスを利用できる基盤を構築

- サイバーセキュリティ検証基盤
- 情報セキュリティサービス審査登録制度

&

## 隠れたニーズに対応したビジネスの創出

- サイバーセキュリティお助け隊

市場への展開

## ビジネスマッチング

- コラボレーション・プラットフォーム

**１．サイバーセキュリティ検証基盤の構築**
２．サイバーセキュリティお助け隊
３．情報セキュリティサービス審査登録制度
４．コラボレーション・プラットフォーム
５．委託時の責任範囲の明確化

# 包括的なサイバーセキュリティ検証基盤を構築し、『Checked by Japan』による競争力創出を促進

- 日本発のサイバーセキュリティ製品の有効性等を実機を通じて検証する等を目的として、**包括的なサイバーセキュリティ検証基盤を構築し、『Checked by Japan』による信頼できる製品の開発の普及促進を図るとともに、検証事業を活性化。**
- 来年度の予算事業を効果的に実施するために、今年度は事前調査を実施。

## 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、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、**実際の制御系システムのセキュリティを検証。**

セキュリティ製品のマーケットインの促進

検証ビジネスの活性化

# 【セキュリティ製品の有効性評価】
# 有識者との意見交換の結果

- セキュリティ製品の有効性評価の方向性について有識者との意見交換を実施。

## ＜検証に関する主なご意見＞

- セキュリティ製品の有効性判断は企業によって異なるため、一定の基準を設けることは困難。
- マーケットインの促進が目的であれば、製品カタログに書いてあることが確かに実装されているかという観点で、製品自体の品質を確認する方が有効。
- セキュリティ分野においては基準を設けて評価を行うことが困難なので、有識者が選定した製品を表彰するような方法も考えられる。
- 発展途上(今後の成長分野）については参入の余地はあるが、定量的な検証は困難。
- 今回のために新しい検証体制を整備するのではなく、IPA(ICSCoE)等の既存の組織との連携も考慮すべき。

## ＜導入に関する主なご意見＞

- ベンチャーは技術評価よりも商談につながるパスを探す方が困難なので、ビジネスの観点ではそちらのアプローチの検討も必要。 →（＜信頼性評価＞にて検討）
- 製品単体で優れた機能を持っていても、自社の環境の課題（他の製品との干渉等）をクリアできないと導入は困難。 →（＜信頼性評価＞にて検討）
- ベンチャー企業の場合、サポート体制の問題から導入に至らないケースも多い。

# 【セキュリティ製品の有効性評価】今後の方向性の案

## 案①：今後の成長分野の予測

- 今後成長すると思われる分野を予測し、セキュリティトレンド報告のような形で経済産業省等から公開する。成長分野を明確にすることで、新規参入企業が生まれることを期待。

## 案②：有識者等による製品評価の仕組みの構築

- 性能を定量的に測定するのは困難であるため、セキュリティ業界の著名な有識者等が製品を使ってみた感想を公表する仕組みを構築する。豊富な経験を持つ著名な有識者等の声は製品選定をする上でも参考になるとの声も。
- 有識者等が製品の相互接続検証（InteropのShowNet等）を行う場に、ベンチャー企業等が参入できるよう支援する。

## 案③：品質チェックの観点を強化

- セキュリティ機能の評価（優劣）ではなく、セキュリティ製品がカタログに書いてある機能を提供できているかといった品質チェックの第三者評価（PSQ認証(*1)等）を促進し、マーケットインを促す。

PSQ Certification
ISO/IEC 25051:2014

(*1)CSAJが、ISO/IEC25051:2014を評価基準として参照して構築した品質認証制度。カタログやマニュアル等とソフトウェアの機能が一致していることを確認。 ＜ http://www.csaj.jp/activity/project/psq/index.html ＞

# 【セキュリティ製品の有効性評価】今後の方向性の案
# 案①：今後の成長分野の予測

## ＜アウトプットのイメージ＞

- 市場動向や脅威情報等の様々な状況を踏まえて、今後の成長分野を予測して公開する。
- いち早く将来の成長予測を行うことで、早い段階で当該分野への参入企業の増加を期待。
- 当該分野に対応する技術・製品を持っている企業をコラボレーション・プラットフォーム等を通じて調査することも検討。

インプット情報の例

セキュリティの市場動向

市場をとりまく脅威

実際に発生しているインシデント情報

海外動向

成長分野の予測

数年後の予測の例
- どのような技術・製品が成長するか
- どのような技術・製品が衰退するか

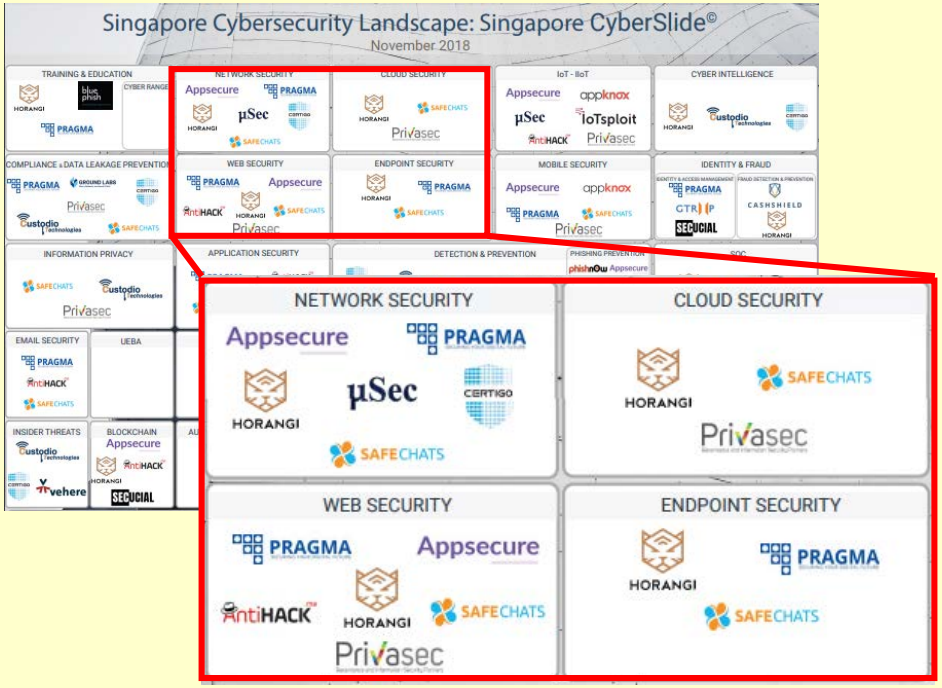
案②により検証
（次スライド参照）

# 【セキュリティ製品の有効性評価】今後の方向性の案
# 案②：有識者等による製品評価の仕組みの構築

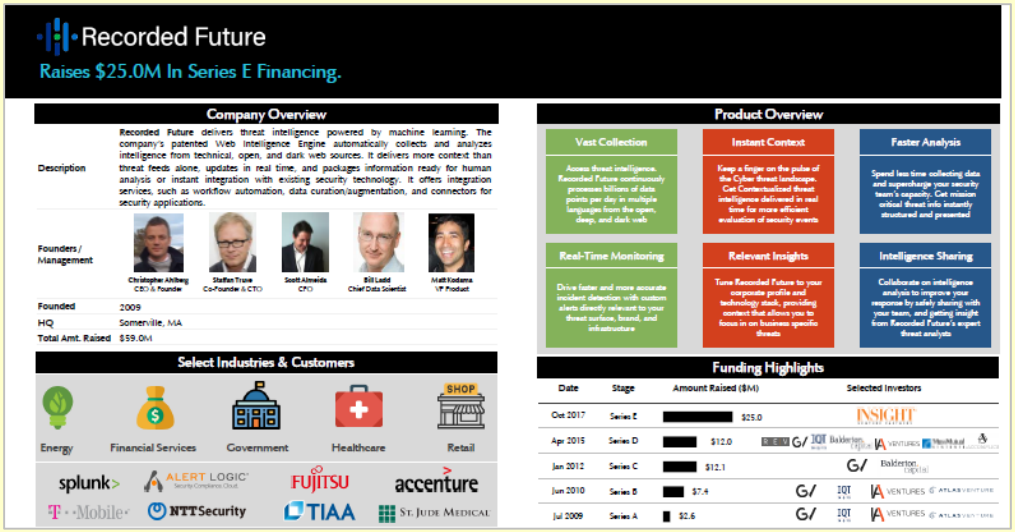
## ＜アウトプットのイメージ＞

- 前スライドで出てきた分野について、技術・製品の評価を希望する者を募集し、その技術・製品の業界の有識者等によるコメントを掲載するシステムを設置。
- 個社の情報や製品について率直な感想を掲載してもらう（良いことを書いてもらえるとは限らない）。
- 情報がたくさん集まるのであれば、国内の製品マップまで作成することを目指す。

海外の事例




国毎のセキュリティベンダーのマップを掲載(Cyberslide)




セキュリティ関連企業の個社毎の紹介等を掲載
(MomentumCYBER)

# 【セキュリティ製品の有効性評価】今後の方向性の案
# 案③：品質チェックの観点を強化

## ＜アウトプットのイメージ＞

- PSQ認証（第三者評価）の活用を促進する。

PSQ認証の概要

### PSQ認証制度は、ソフトウェア製品の安全性・信頼性を評価

- 申請者：利用者にソフトウェア製品を提供する事業者
- 対象ソフトウェア：企業向け業務パッケージソフトウェア及びクラウド提供製品

### 国際標準規格ISO/IEC25051(*1)に準拠

- 購入予定者にとって必要なことが、製品説明に矛盾なくきちんと記載されていること。
- 利用者用文書類に利用者にとって必要な情報が正しく記載され、かつ製品説明と矛盾がないこと。
- ソフトウェアに実装されている機能が実機テスト、もしくは試験文書類のいずれかで確認できること。

### ソフトウェア及び３種類の文書類による評価（国際相互承認の場合は実機テストも実施）

- 評価対象文書類は、製品説明（カタログ、製品の外装表示等）、利用者用文書類（インストールマニュアル、操作マニュアル等）、試験文書類（試験計画書、試験手順書等）

(*1)ソフトウェア製品の品質要求・評価に関する国際標準規格

# 【セキュリティ製品の有効性評価】
# （参考） 民間企業による有効性評価手法

- 海外では、第三者による検証事業も多く存在し、セキュリティ機能の品質評価も実施している。一方で、国内では、市場シェアや顧客度満足度、知名度などで評価しており、品質で評価する仕組みがない。

| 民間企業による製品テストの例（海外） | |
|---|---|
| AV-TEST | ドイツにあるセキュリティ製品の評価を行うテスト機関。実環境でのゼロデイ攻撃の検知テストや検知性能とパフォーマンスの相関テスト、感染システムの復旧テスト等を実施し、基準を満たした製品には合格マークを付与。 |
| AV-Comparative | オーストラリアにあるテスト機関。セキュリティソフトを選ぶ上で多くの個人・企業がその情報を参考にしている。PC/Macベースのウイルス対策製品やモバイルセキュリティソリューション等のセキュリティソフトをチェックする体系的な評価を実施。 |
| NSS Labs | アメリカにある世界を代表する情報セキュリティ調査とアドバイザリーの独立機関。実環境に近い形での性能評価にこだわっており、業界で最も包括的な第三者テストを実施。 |

| 市場調査、顧客満足度調査（国内） | |
|---|---|
| 富士キメラ | ネットワークセキュリティビジネス総覧を発刊（年１回）。 |
| アイ・ティ・アール | ITR Market View：サイバーセキュリティ対策市場を発刊（年１回）。 |
| イードアワード | ネット上で顧客満足度調査を実施し、様々な満足度での１位を発表。 |

# 【実環境における試行検証】セキュリティ製品導入組織との意見交換

- 自組織へのセキュリティ製品導入を事例として公表している組織と、製品導入における課題等について意見交換を実施中（～2019年2月まで）。
- セキュリティ製品については導入事例の公表を認めない組織が多い中、公表を認めている理由についても確認。

製品導入

導入実績の公表

ベンダー視点

製品が実環境でも問題なく動作することを検証

導入実績の公表により次のビジネスへつなげる

ユーザーとの意見交換

ユーザー視点での課題抽出

**政策的な方向性の明確化**

コラボレーション・プラットフォームを軸としたベンダーとユーザーのマッチング促進

ベンダー　　ユーザー（企業、大学等）

# 【ホワイトハッカーの実攻撃検証】検証の目的と枠組みの考え方

- Society5.0の進展に伴い、サイバー攻撃の影響範囲は末端のIoT機器まで及ぶことになった。これに伴い、影響が大きなIoT機器等についてはセキュリティの検証を行うことが必要。
- このため、製造者の過失によるIoT機器等の脆弱性に加え、製造者による意図的な脅威（機器が収集した個人情報等の外部への漏洩やバックドアの埋込など）が含まれていないかについて検証を行うための基盤を構築する。

## 検証基盤構築へ向けた考え方

1．IoT機器・システム等の重要性等を考慮した**検証対象の特定**

＋

2．対象機器のライフサイクルへの対応も考慮した**検証手法の選定**

＋

3．技術的・組織的な観点から信頼できる**検証主体の確保**

平成30年度予算を活用し、事前調査を実施

平成31年度予算を活用して、考え方を整理し、検証基盤を構築

# 【ホワイトハッカーの実攻撃検証】

## １．IoT機器・システム等の重要性等を考慮した検証対象の特定

- 検証対象については、そのIoT機器等がサイバー攻撃を受けた場合の影響の大きさや、どの程度の被害を受けやすいか、といった観点を考慮して特定していく必要がある。

### IoT機器等の特定にあたっての観点

**（１）攻撃されたときの影響の大きさ**

①IoT機器等が扱う情報の量と質

－カメラや、位置情報などの各種センサーを備えて情報を収集するIoT機器　等

②フィジカル空間への影響の大きさ

－電力や通信など重要インフラにおいて活用されるIoT機器　等

**（２）攻撃対象になりやすさ**

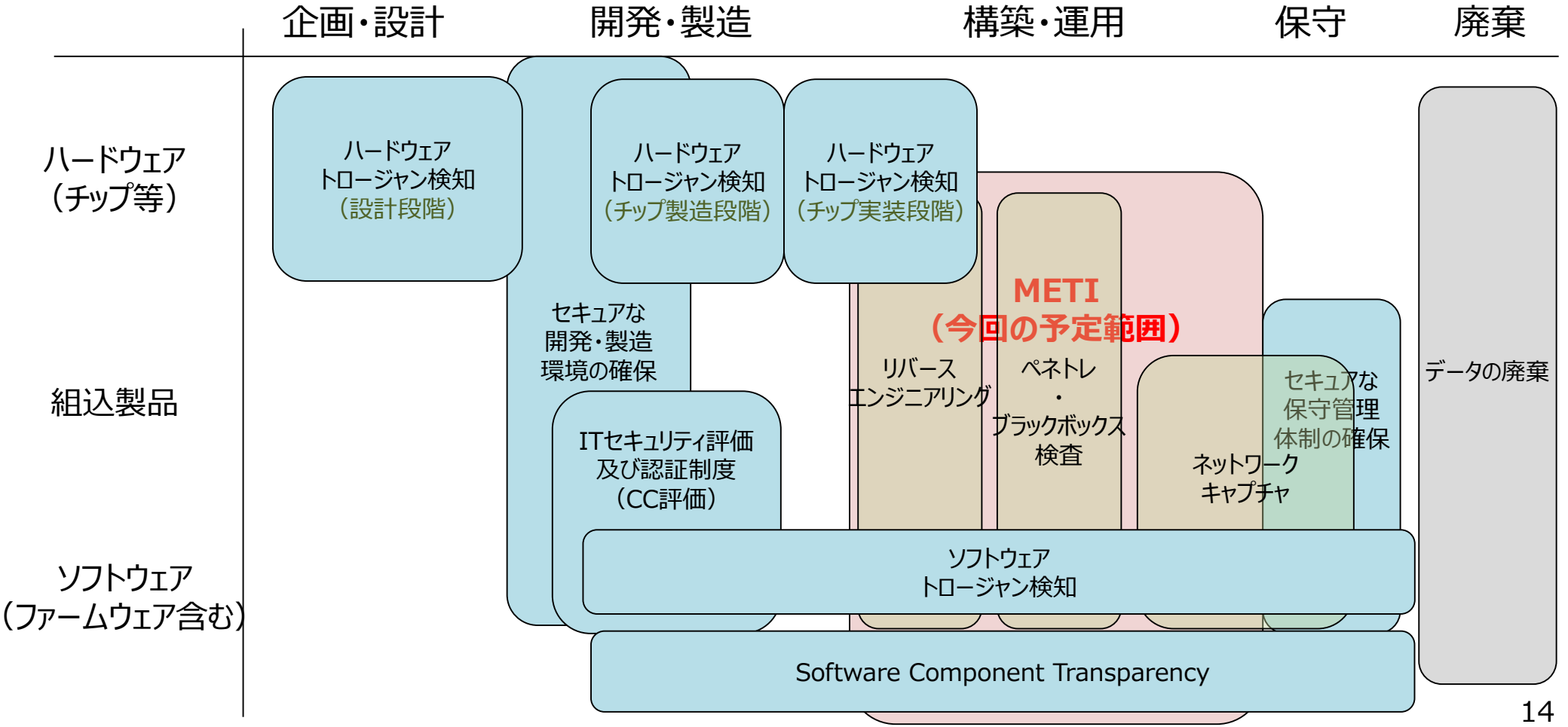
①インターネットへの接続の仕方

－インターネットや携帯網に常時・直接接続しているIoT機器　等

②セキュリティにかけられるコスト

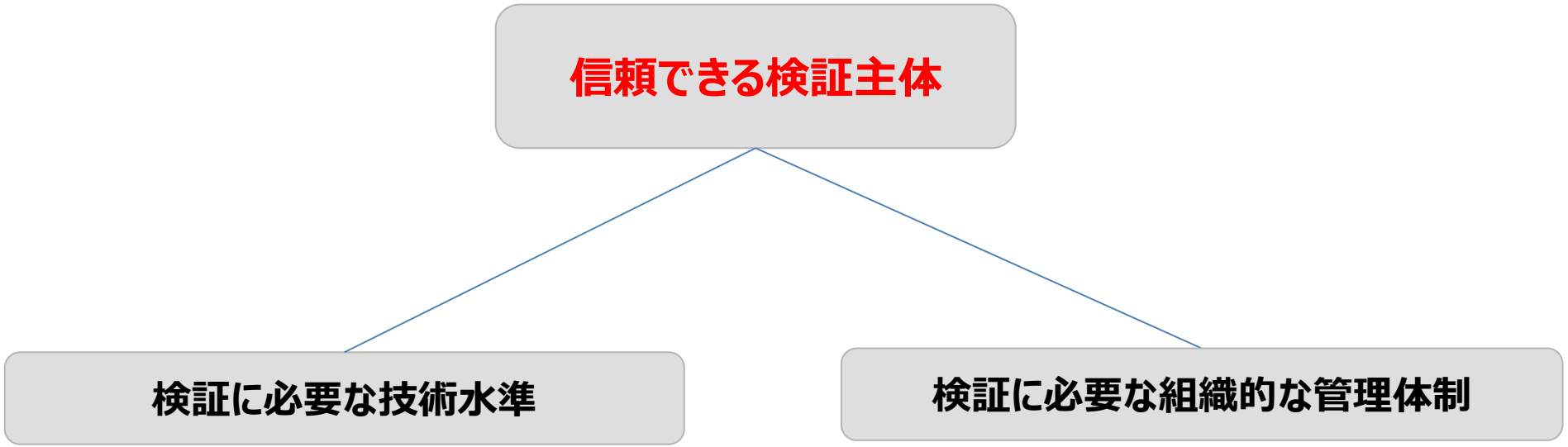
# 2．対象機器のライフサイクルへの対応も考慮した検証手法の選定

- 製品のセキュリティ検証の実施に当たっては、製品のライフサイクルも考慮し、検証方法を選択する必要がある。
- IoT機器等を対象とした本検証では、構築・運用段階における検証手法について、その有効性等について確認するとともに、その他の検証手法との関係も整理する。



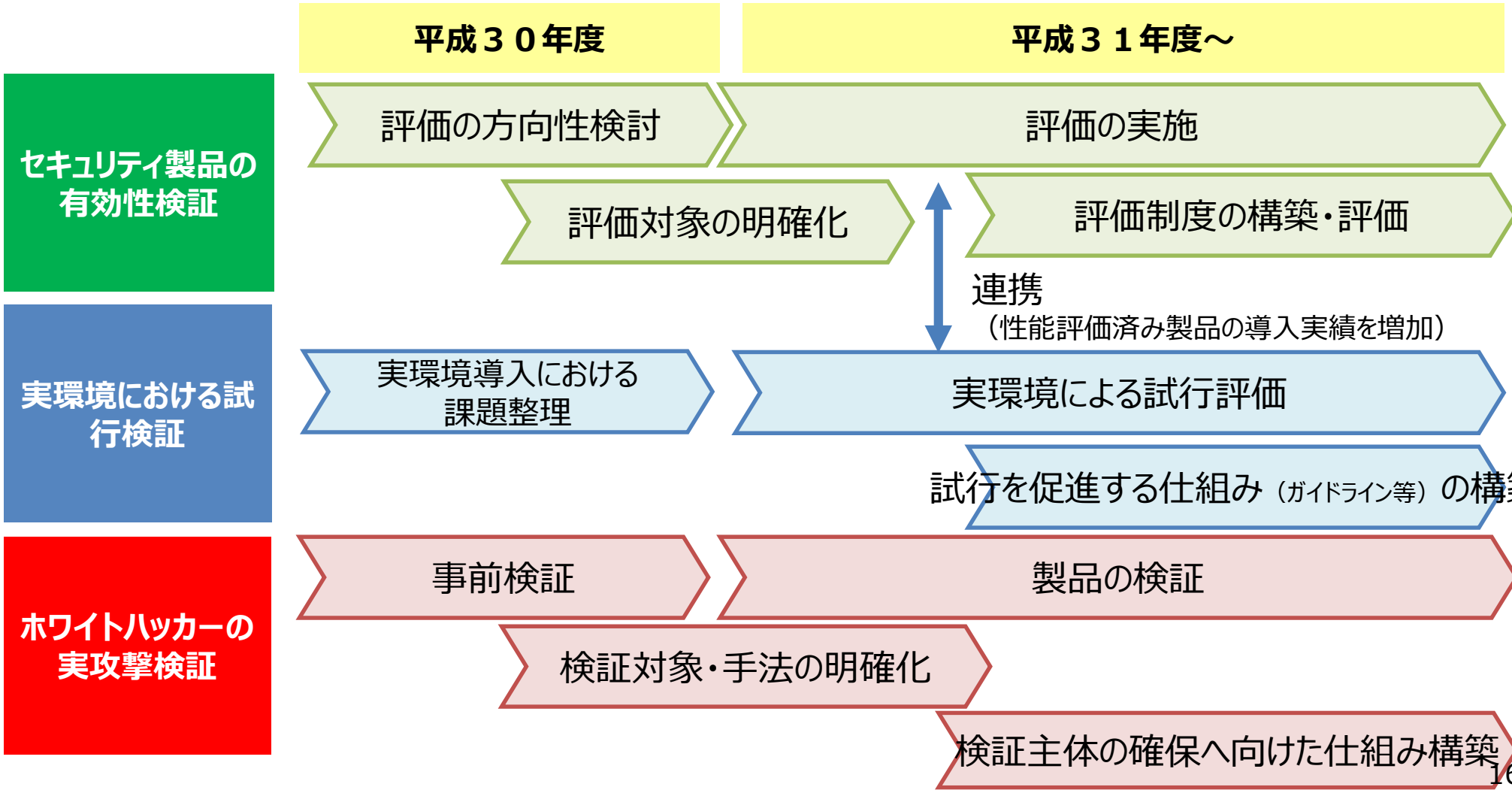
# 【ホワイトハッカーの実攻撃検証】
# ３．技術的・組織的な観点から信頼できる検証主体の確保

- 信頼性が高い検証を実施できる組織には、技術的な能力や、組織的な管理体制の整備等が求められる。



# 包括的なサイバーセキュリティ検証基盤の構築へ向けた今後の取組

- 今年度中に事前調査を行い、評価の方向性や対象等を明確化。
- 来年度、検証を実施し、対象製品の決定、構築し、評価を開始予定。



１．サイバーセキュリティ検証基盤の構築
**２．サイバーセキュリティお助け隊**
３．情報セキュリティサービス審査登録制度
４．コラボレーション・プラットフォーム
５．委託時の責任範囲の明確化

# サイバーセキュリティお助け隊

- 平成30年度第二次補正予算、中小企業強靭化対策事業の中の１事業として「サイバーセキュリティお助け隊」の実証事業を全国8地域程度で実施。
- IPAが事業実施主体となり、2月より公募開始予定。

## 中小企業等強靭化対策事業

**平成30年度第2次補正予算案額 15.0億円**

中小企業庁 経営安定対策室
03-3501-0459
中小企業庁 技術・経営革新課
03-3501-1816
商務情報政策局 サイバーセキュリティ課
03-3501-1253

### 事業の内容

**事業目的・概要**

- BCP（Business Continuity Plan：事業継続計画）の取組事例や早期復旧事例などを広く紹介するとともに、サプライチェーンに位置づけられる中小企業等のBCPの策定を支援し、そうした取組を横展開することによって、中小企業の防災意識の啓発、強靭化に向けた取組の促進を図ります。
- サイバー攻撃に備えて、中小企業等のセキュリティ対策の普及啓発、マネジメント指導のほか、トラブル時の相談対応・現場派遣体制構築等の実証事業を行います。

**成果目標**

- 延べ2万者の中小企業者に対し、BCPの重要性等について啓発を行います。
- BCPのモデルとなる取組（例：サプライチェーン、地域の中核企業）を支援し、これら支援成果をとりまとめて事例集として公表し、BCP策定を促進します。
- 8地域で、サイバーセキュリティ対策の啓発を行うとともに、トラブル時の相談体制等の実証を行い、必要な人材、体制等を明らかにすることを目指します。

（１）BCP等普及啓発事業

国 → 民間団体等 → 中小企業・小規模事業者

委託・補助（10/10）　説明会・訪問・相談会、指導等

（２）BCP策定・対策支援事業

国 → 民間団体等 → 中小企業・小規模事業者

委託・補助（10/10）　支援・実証

### 事業イメージ

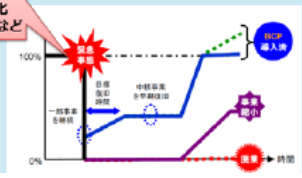
**１．BCP等普及啓発事業**

- 中小企業に、自社の災害リスクやサプライチェーンに対するサイバー攻撃のリスクを認識してもらうとともに、BCPの策定・取引先も含めた対策状況の点検や保険を含めた対応等について、啓発を図ります。
- 具体的には、商工団体等を通じて、会員企業等への周知を行うとともに、全国各地において、シンポジウム等を開催します。

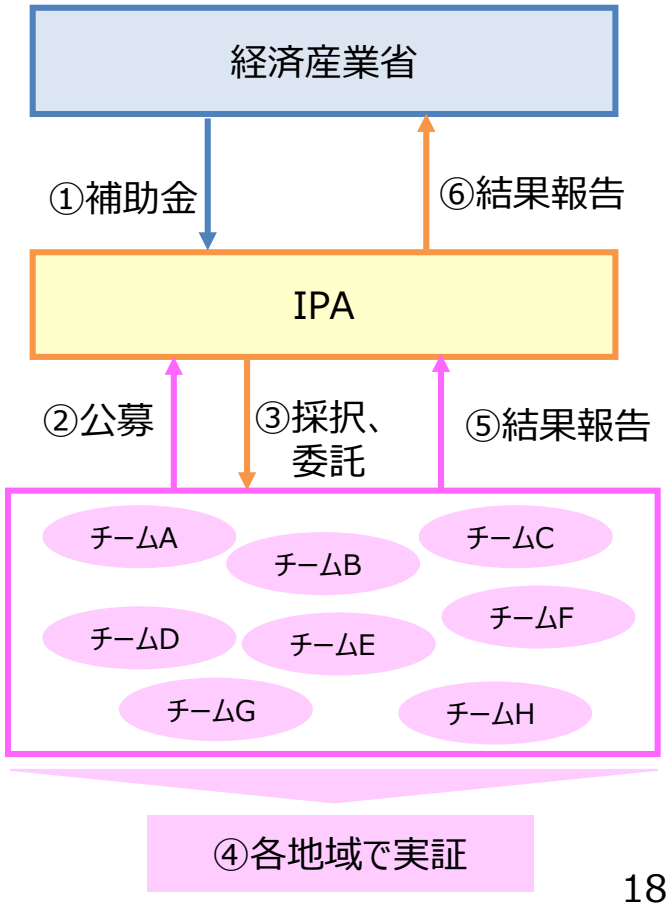
**２．BCP策定・対策支援事業**

- サプライチェーンに位置づけられる中小企業等について、各企業が直面するリスクに応じたBCPの策定をハンズオンで支援します。
- 全国各地において、ワークショップを開催し、参加する中小企業に対し、BCPの必要性について啓発を図るとともに、その策定に向けた試行的取組を支援します。
- サプライチェーン全体のサイバーセキュリティ対策の普及啓発に取り組むとともに、サイバー攻撃によるトラブル時の相談対応・現場派遣などの支援サービス提供体制を整備するなど、中小企業のニーズに沿ったセキュリティ技術・サービスの実証事業を地域単位で実施します。

例えば、
・大地震等の自然災害
・テロ等の事件、大事故
・突発的な経営環境の変化
など




＜事業実施体制＞

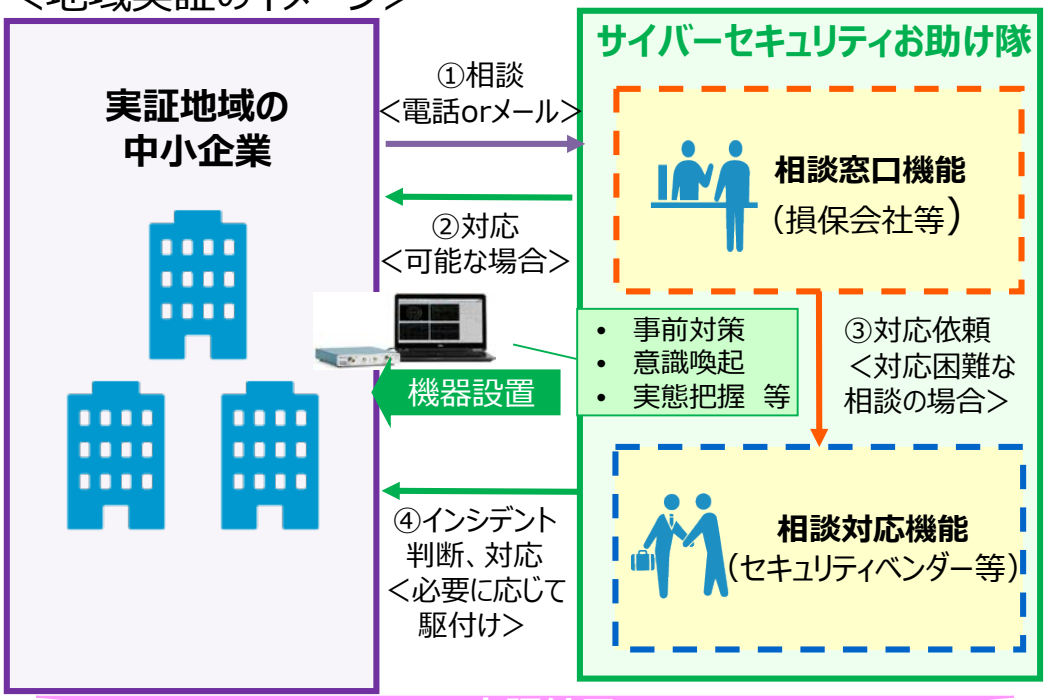



経済産業省　平成30年度第２次補正予算案の概要（ＰＲ資料）

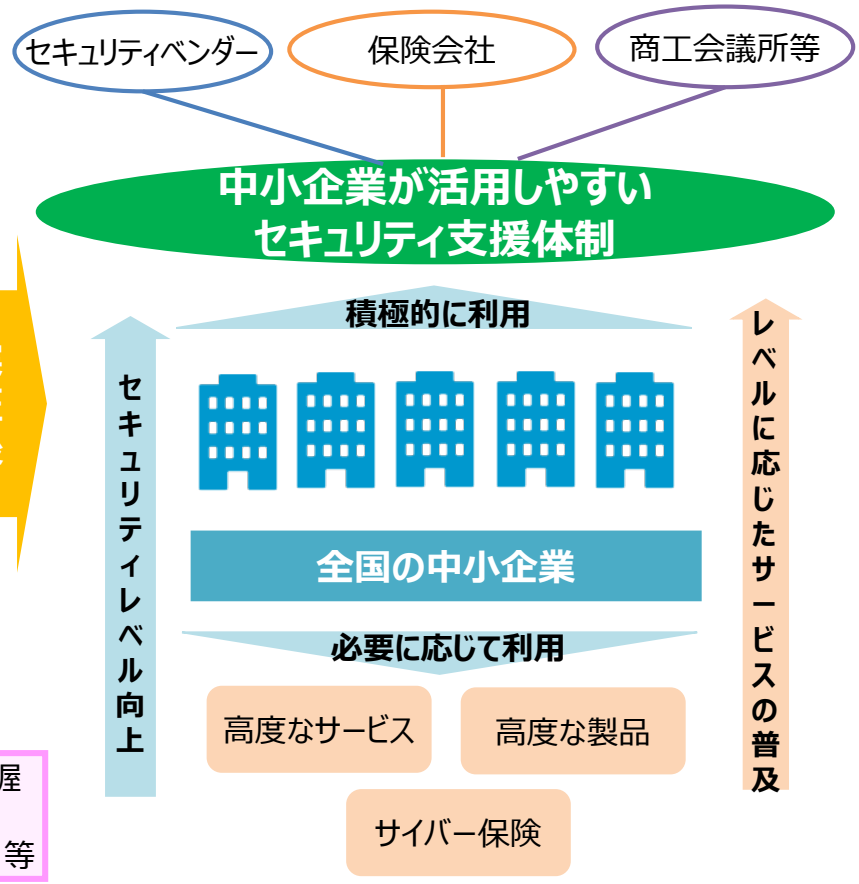
# サイバーセキュリティお助け隊の実証

- 中小企業向けにサイバーセキュリティに関する支援の仕組みを新たに構築し、全国最大8地域を対象に地域の団体、企業等と連携した実証を行い、サイバー攻撃の実態や対策のニーズを把握するとともに、中小企業の事前対策の促進、意識喚起を図る。
- 実証後は、保険機能とも連動した中小企業が利用しやすい支援体制の構築を目指す。

＜地域実証のイメージ＞




実証後




実証結果

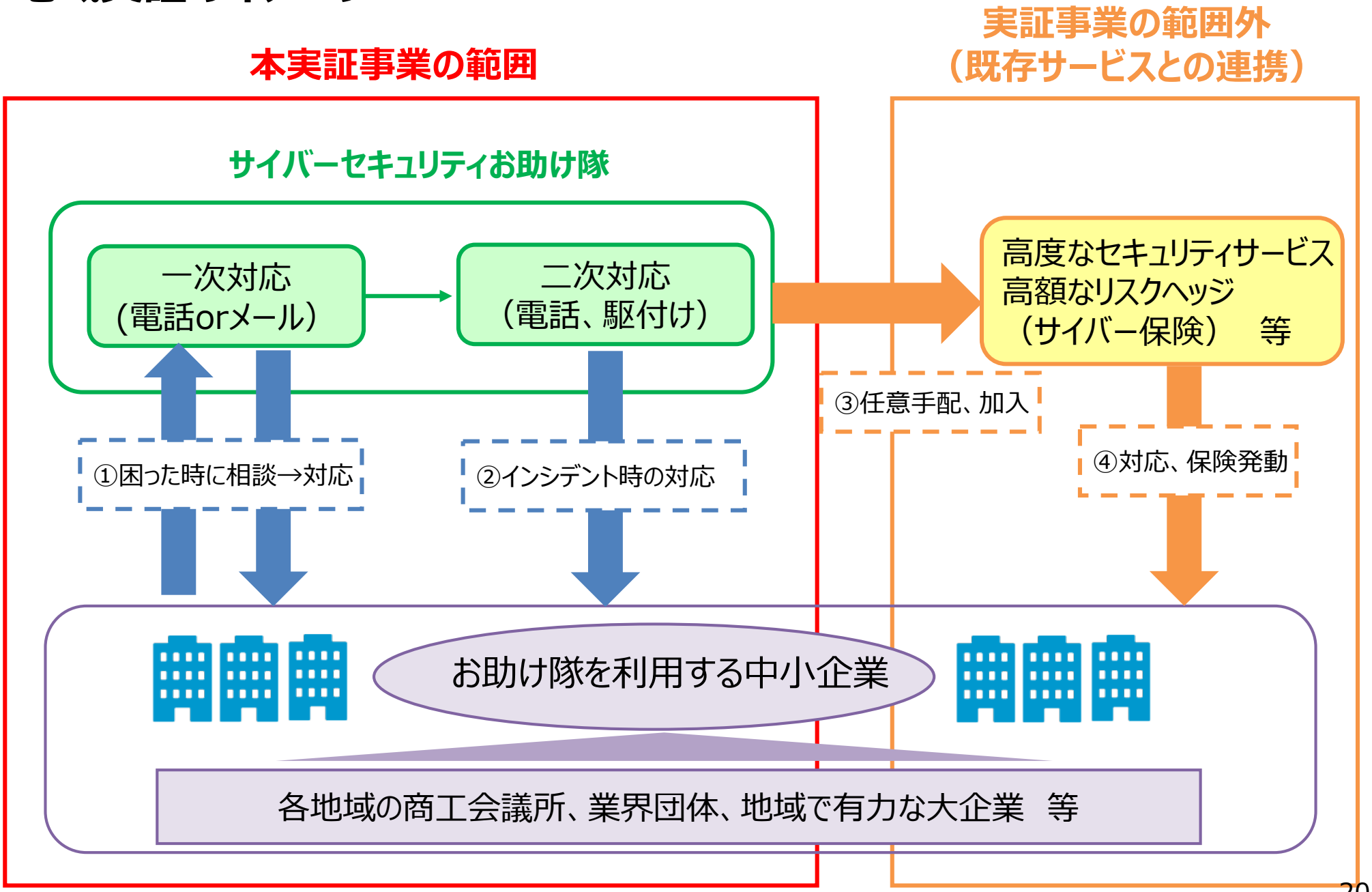
**中小企業　側**

- 自社の攻撃実態等への気付き
- セキュリティ事前対策の促進
- 事後対応への意識向上　　等

**保険会社、セキュリティベンダー　側**

- 中小企業のセキュリティ対策状況の把握
- 中小企業の被害実態の把握
- 中小企業が求めるサービスの把握　　等

# 地域実証のイメージ


本実証事業の範囲
実証事業の範囲外
（既存サービスとの連携）
サイバーセキュリティお助け隊
一次対応
(電話orメール)
二次対応
（電話、駆付け）
高度なセキュリティサービス
高額なリスクヘッジ
（サイバー保険）　等
③任意手配、加入
④対応、保険発動
①困った時に相談→対応
②インシデント時の対応
お助け隊を利用する中小企業
各地域の商工会議所、業界団体、地域で有力な大企業　等

１．サイバーセキュリティ検証基盤の構築
２．サイバーセキュリティお助け隊
**３．情報セキュリティサービス審査登録制度**
４．コラボレーション・プラットフォーム
５．委託時の責任範囲の明確化

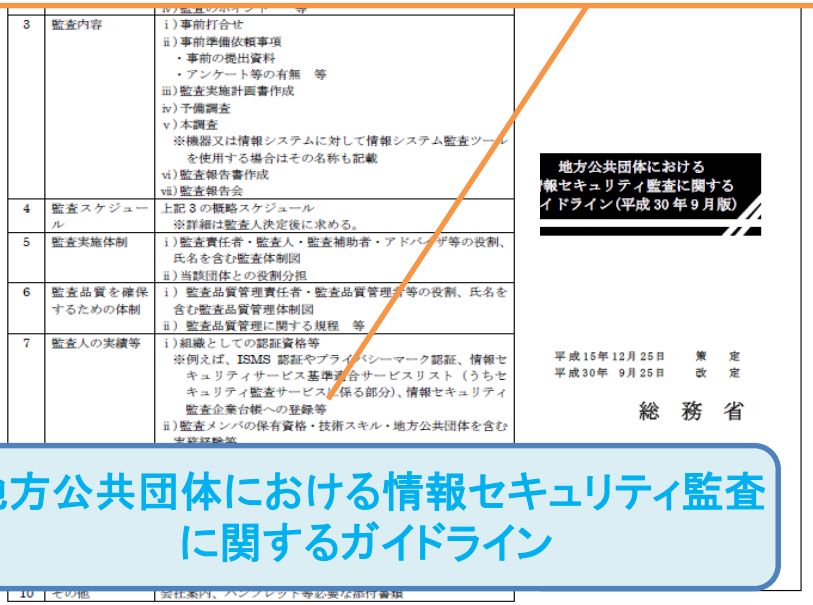
# 情報セキュリティサービス基準適合サービスリスト

- 6月にパイロット審査、7月より本審査を開始し、1月末時点で90サービスを登録。今年度末には登録サービス数が100サービスを超える見込み。
- 政府調達での活用、税制・補助金における要件化に加え、地方公共団体における情報セキュリティ監査に関するガイドライン（総務省）へも記載。


**90サービスが掲載（1月末時点）**
- 情報セキュリティ監査（21サービス）
- 脆弱性診断（31サービス）
- デジタルフォレンジック（16サービス）
- セキュリティ監視・運用（22サービス）

https://www.ipa.go.jp/security/it-service/service_list.html

ⅰ)組織としての認証資格等
※例えば、ISMS 認証やプライバシーマーク認証、**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）**、情報セキュリティ監査企業台帳への登録等
～地方公共団体における情報セキュリティ監査に関するガイドラインより抜粋




**地方公共団体における情報セキュリティ監査に関するガイドライン**

http://www.soumu.go.jp/denshijiti/jyouhou_kansa/

# IT導入補助金＆コネクテッドインダストリー税制

- IT導入補助金及びコネクテッドインダストリー税制において情報セキュリティサービス基準適合サービスリストを推奨。

## IT導入補助金

- 平成２９年度補正１次～３次（第４期まで）の採択件数は**合計41,026件**
- ５名以下の小規模事業者の採択が５割以上を占める。
- ５０万円（補助金上限）の交付が５割以上を占める。

<ご参考>
SECURITY ACTIONの取得が、IT導入補助金申請時の必須要件となっている。
SECURITY ACTIONの取得企業数は、合計61,411件（12月末現在）

## コネクテッドインダストリー税制

| No. | 事業者の氏名又は名称 | 事業分野 | 認定日 |
|---|---|---|---|
| 1 | 株式会社ジェーシービー | 貸金業，クレジットカード業等非預金信用機関 | 平成30年7月13日 |
| 2 | 株式会社アルファパーチェス | 各種商品卸売業 | 平成30年7月19日 |
| 3 | 株式会社日伝 | 機械器具卸売業 | 平成30年7月27日 |
| 4 | キヤノン株式会社 | 業務用機械器具製造業 | 平成30年9月20日 |
| 5 | 株式会社ユニクロ | 繊維・衣服等卸業 | 平成30年9月28日 |
| 6 | 株式会社プレステージ・インターナショナル | その他の事業サービス業 | 平成30年9月28日 |
| 7 | 富士電機株式会社 | 電気機械器具製造業 | 平成30年10月12日 |
| 8 | 日本食研ホールディングス株式会社 | 食料品製造業 | 平成30年10月30日 |
| 9 | 株式会社ヨロズ大分 | 輸送用機械器具製 | |
| 10 | 昭栄化学工業株式会社 | 化学工業 | |
| 11 | 東ソー・クォーツ株式会社 | 窯業・土石製品製 | |
| 12 | 東京インキ株式会社 | 化学工業 | 平成30年12月7日 |

**20事業者が認定（12月末現在）**

経済産業省　コネクテッド・インダストリーズ税制（IoT税制）HPより抜粋
http://www.meti.go.jp/policy/it_policy/data-katsuyo/iot-zeisei/iot-zeisei.html

# サーベイランスWG及び高度化方策検討会の設置

- 情報セキュリティサービス基準適合サービスリスト掲載事業者を対象とし、サーベイランスの内容等を検討するWG及び、より良い情報セキュリティサービスを普及させる方策について議論する検討会を設置。

**サーベイランスWG**

＜実施目的＞
制度の信頼性を担保するために、リストに掲載されたサービスを対象に実施するサーベイランスに関する事項について専門的見地から検討することを目的とする。
＜議論内容＞
サーベイランス内容、サーベイランス実施方法　等

**高度化方策検討会**

＜実施目的＞
より良い情報セキュリティサービスの情報を伝えるために開示すべき情報等、情報セキュリティサービスを普及させる方策について検討することを目的とする。
＜議論内容＞
情報セキュリティサービスの評価の在り方、情報セキュリティサービスの評価方法　等
＜第一回検討会（12/7開催）の検討状況＞
- 情報セキュリティサービスの用途や対象に応じたカテゴリを定義すると、ユーザ企業が利用時に選択し易くなる。
- カテゴリはレベルとは異なる概念であり、サービスの優劣を示すものとすべきではない。
- ユーザーが利用し易い制度にすべきである。
- 地方で情報セキュリティサービスを提供する企業や、ベンチャー企業による登録にも配慮すべきである。

# カテゴリーのイメージ(情報セキュリティ監査サービスの例)

| サービス分野 | カテゴリー分類（案） | カテゴリーの定義（案） | カテゴリーに求める要件（案） | 特徴 |
|---|---|---|---|---|
| 情報セキュリティ監査サービス | 助言型監査サービス（改善提言型） | 監査の対象となる組織体の情報セキュリティに関するマネジメントやマネジメントにおけるコントロールについて、リスク分析に基づくその有効性に関する判断結果をもとに、改善を目的とする助言を行うもの | ・技術要件（専門性を備えた技術者が実施）<br>・品質管理要件（属人的でなく、品質管理体制に基づいたマネジメントを実施） | サービスに関し、強み（特定業種に強い等）、オプションとして提供可能なサービス等を記載。 |
| | 保証型監査サービス | 監査の対象となる組織体の情報セキュリティに関するマネジメントやマネジメントにおけるコントロールが、満たすべき水準に照らして適切であることの保証を行うもの | ・技術要件（専門性を備えた技術者が実施）<br>・品質管理要件（属人的でなく、品質管理体制に基づいたマネジメントを実施）<br>・業務経験 | |

# 監査企業台帳制度の見直しについて

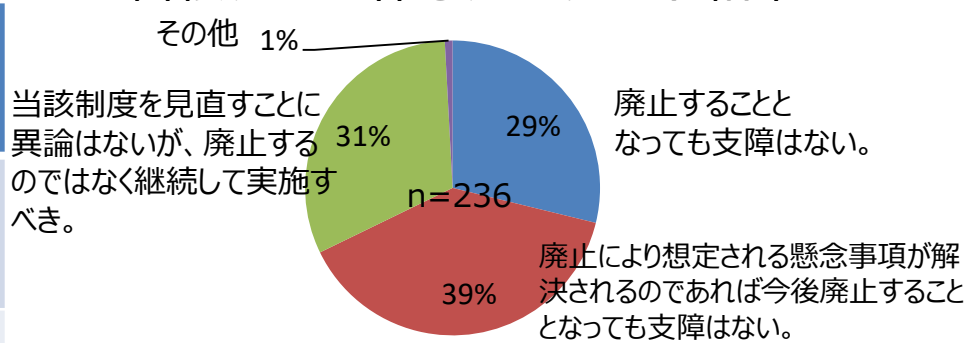
- 情報セキュリティ監査企業台帳制度については、以下の理由を踏まえ、廃止としたい。
  ① より信頼性の高い情報を提供する情報セキュリティサービス審査登録制度（情報セキュリティ監査サービス）が創設されたこと。
  ② 平成28、29年度に実施した登録事業者へ実施した台帳制度見直しに係るアンケート結果においても、廃止しても支障なしとの意見（条件付きを含む。）が約７割を占めたこと。
- 廃止時期は、周知・準備等の期間を考慮し、平成３１年度末を検討。
- なお、システム監査企業台帳制度は、現在同様の制度が存在しないことなどを踏まえ、今般の対応とは別とし、その在り方の検討を今後の課題とする。

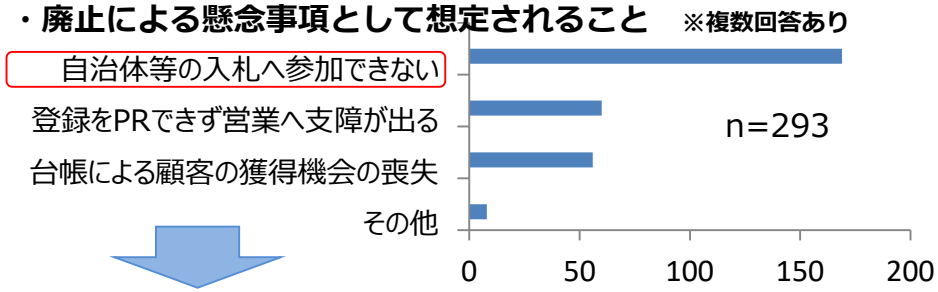
## ＜両制度の概要＞

| | 情報セキュリティ監査企業台帳制度 | 情報セキュリティサービス審査登録制度（情報セキュリティ監査サービス） |
|---|---|---|
| 根拠 | 情報セキュリティ監査企業台帳に関する規則（告示） | 情報セキュリティサービス基準<br>情報セキュリティサービスに関する審査登録機関基準 |
| 目的 | 情報セキュリティ監査の普及 | 情報セキュリティサービス業の普及促進等 |
| 登録方法 | 申告書の提出（申告があれば原則掲載） | 審査登録機関による情報サービス基準への適合審査 |

審査登録制度は、審査登録機関による審査が実施されるため、企業台帳制度よりも信頼性が高い。

## ＜台帳廃止に係るアンケート結果＞




調達参加の要件は、登録審査制度を参照

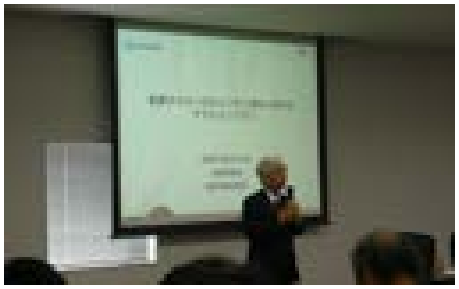
１．サイバーセキュリティ検証基盤の構築
２．サイバーセキュリティお助け隊
３．情報セキュリティサービス審査登録制度
**４．コラボレーション・プラットフォーム**
５．委託時の責任範囲の明確化

# コラボレーション・プラットフォームの開催状況

- 各回、予定定員以上の申込みがあり、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、様々な視点で有益との声も。

| | 日にち | 参加人数(*) | 主なテーマ |
|---|---|---|---|
| 第一回 | 6月13日 | 179名（99名） | 経済産業省の政策動向 |
| 第二回 | 7月23日 | 104名（74名） | サプライチェーン対策、人材育成、つながる世界の脅威と対策 |
| 第三回 | 9月3日 | 132名（69名） | 業界別のセキュリティ対策、セキュリティ検証基盤、サイバーセキュリティ経営 |
| 第四回 | 10月16日 | 151名（56名） | 中小企業のセキュリティ対策 |
| 第五回 | 11月30日 | 98名（40名） | IoTの技術・標準化動向 |
| 第六回 | 1月25日 | 約100名予定 | サイバー・フィジカル・セキュリティ対策フレームワーク |

(*)括弧内の人数はコラボレーション・プラットフォーム後に開催した情報交換会の出席者数


富田理事長(IPA)ご挨拶

三角審議官(経済産業省)ご挨拶

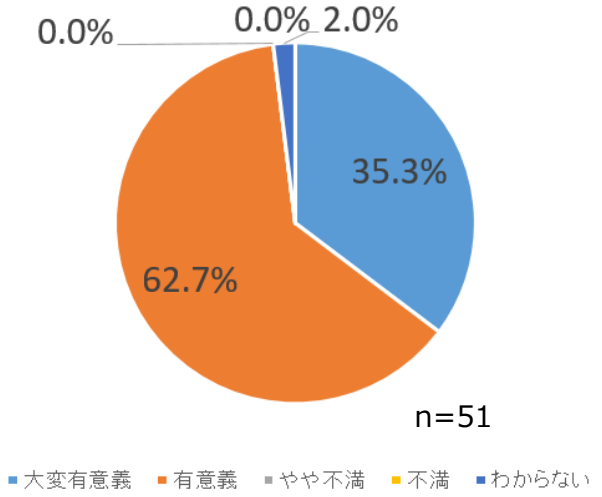

パネルディスカッション(第一回)


グループディスカッション(第二回)

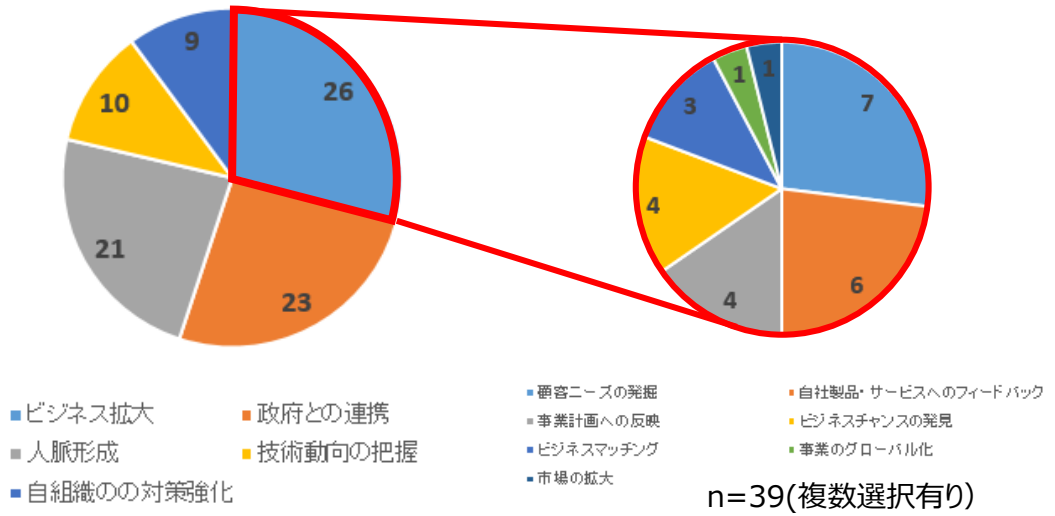
# コラボレーション・プラットフォーム参加者の声

- 「ビジネス拡大」、「政府との連携」の観点で実際にメリットがあった参加者が多数。
- アンケートでは「他業界とのコラボができて有意義だった」、「ユーザーの立場として有益な情報を入手できた」、「貴重な機会である」等、満足度の高いご意見も多数寄せられた。

Q.コラプラの満足度についてお聞かせください




Q.過去にコラボレーション・プラットフォームにご参加いただいたことで、良かったこと・役に立ったことはありますか？




※第五回コラボレーション・プラットフォームアンケートより。
アンケート回答者56名のうち、39名（約70%）が参加して良かったこと・役に立ったことがあったと回答

## <コラボレーション・プラットフォームのマッチング事例>

- コラボレーション・プラットフォームで名刺交換をした企業のソリューションと連携できないかについて、後日具体的なディスカッションを実施。現在も継続して調整している。

# コラボレーション・プラットフォームの今後の方向性

- 新規参加企業の増加を促し、人脈形成の機会を強化するとともに４つの観点でのコラボレーションの実現を目指す。

## 【政策とのコラボレーション】

政策に関する意見交換の機会を増やし、**参加者からのご意見を着実に政策に反映**。

※ コラボレーション・プラットフォームだからこそ実現可能。

## 【シーズサイドのコラボレーション】

ベンダー企業間で連携を図り、**より大きなソリューションを市場に流通**。

※ ベンダー同士でチームを組むことにより、解決できる課題や販売網の拡大を期待。

## 【ニーズサイドのコラボレーション】

ユーザ企業や大学等の間で課題を共有し、**セキュリティに関するニーズを具体化**。

※ セキュリティ担当者が少ない企業からは、悩みを共有できる仲間がいなくて困っているとの声も。

## 【ニーズとシーズのコラボレーション】

ニーズサイドとシーズサイドの連携を図り、**ビジネスマッチング**につなげる。

※ 規模の小さな企業からはユーザ企業等とのパスがなく事業拡大が困難との声も。

# 政策とのコラボレーション

経済産業省の政策

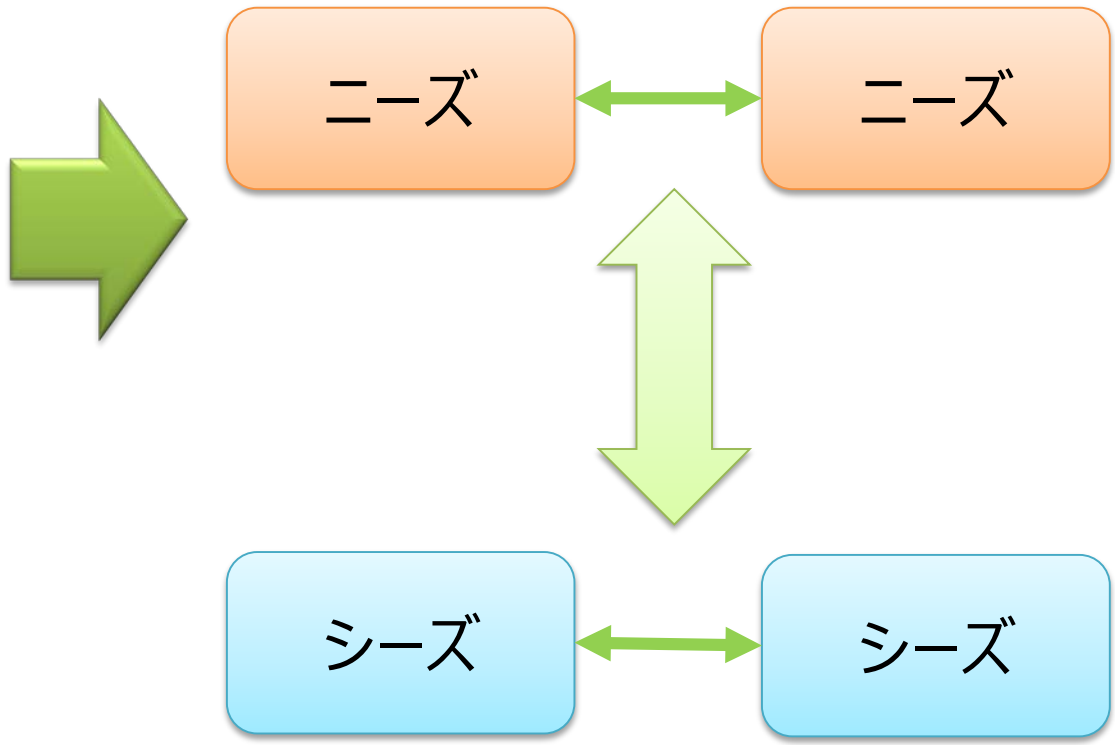
| | | これまでの内容と主なご意見 |
|---|---|---|
| ① **発起段階**<br>問題意識の共有 | 民間からの<br>幅広い意見交換 | **サイバーセキュリティ検証基盤**（第三回）<br>• 定量的な評価は難しいので表彰制度という考え方も有効だと思う。<br>• 製品そのものの信頼性だけではなく、実環境でいかに動くかという視点も考えないといけない。 |
| ② **立案段階** | 政策内容に関する<br>意見交換 | **サイバー・フィジカル・セキュリティ対策フレームワーク**（第一回、第六回）<br>• 要求事項が実装できるようにするために、松竹梅のレベル分けがあるとよい。<br>※ 第六回は1/25(金)に開催 |
| ③ **普及・実施段階** | 政策内容の<br>共有 | **中小企業向け政策**（第四回）<br>※ 第四回はディスカッションは未実施。SECURITY ACTIONやIT導入補助金等の中小企業向けに展開している政策を共有し、参加者からも好評の声が多数。 |

# 民間（学も含む）同士のコラボレーション

- 形成した人脈をつかい、コラボレーション・プラットフォーム内外で自由なマッチングの促進を期待。

コラボレーション・プラットフォーム

- 政策動向の共有
- 市場を取り巻く最新動向の共有
- 興味のあるテーマの紹介
- 企業の取り組み事例の紹介



１．サイバーセキュリティ検証基盤の構築
２．サイバーセキュリティお助け隊
３．情報セキュリティサービス審査登録制度
４．コラボレーション・プラットフォーム
**５．委託時の責任範囲の明確化**

# 委託範囲に関する調査

- 「ITシステム・サービスの業務委託におけるセキュリティに係る責任範囲に関する調査」を実施中（IPA、今年度中に調査結果を公開予定）

## ＜調査の背景＞

- 委託元、委託先それぞれにおいて、委託業務でのセキュリティ対策の責任範囲が明確にされていないケースが多いことが明らかになったところ（ 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報告書（IPA、2018年3月）） 。

  - 責任範囲の明確化に対する意見
    - 明確にすべき
      - インシデント発生時に迅速に対応できず被害拡大
      - 責任追及の時間と費用が大きな負担
      - ITベンダに責任が押し付けられる日本の慣例
    - 明確にすべきではない
      - 明確にすることが困難（IoTやAIなど新サービスは責任範囲が不明瞭。専門知識が無いユーザには判断が困難。）
      - 明確にすることがビジネスを阻害（明確化に時間がかかり機会損失。コスト高になり合意困難。）

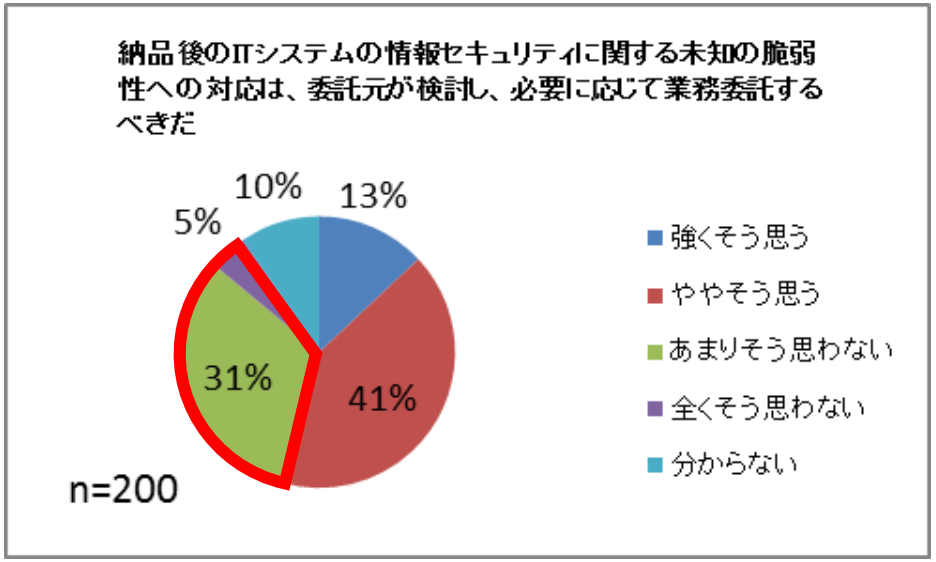
## ＜調査の目的＞

- 責任範囲を明確にする場合、明確にできない場合のリスクの実態把握と課題の認識及びその対策事例を調査。

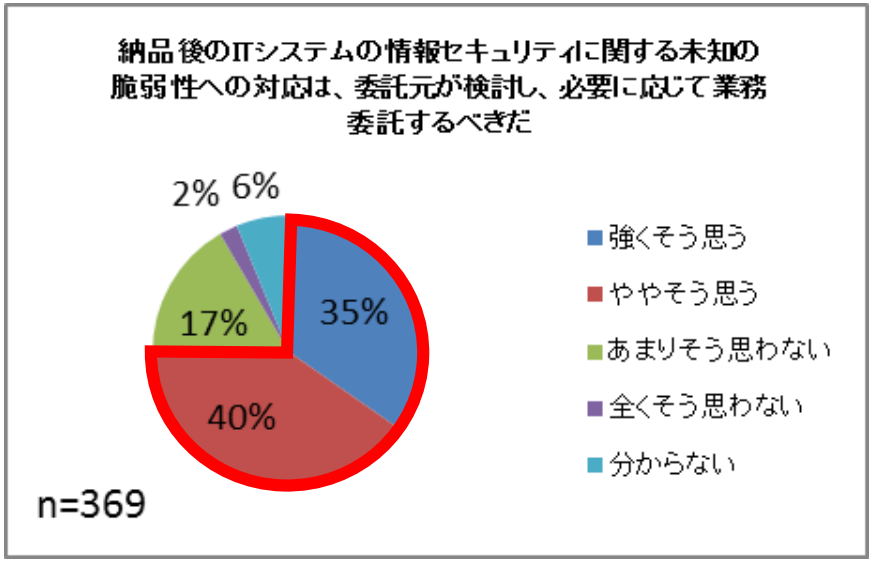
# 委託範囲に関する調査の中間報告

- 委託元、委託先の双方において責任範囲は明確にすべきと認識しているものの、委託先側は「コスト増」、「契約時点で要求自身が曖昧」、委託元側は「知識・スキル不足」等が原因で明確にはならないとのこと。
- 特に**納品後の未知の脆弱性対応については委託元、委託先の認識のギャップが大きく、トラブル要因の一つ**となっている。

**委託元の認識**




**委託先の認識**




- 多くの企業（委託元：36%、委託先：75%）が納品後の脆弱性対応は自分がやるべきと思っていない。取引相手がやるものと思い込み、脆弱性が放置されるリスクにも繋がる。