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８回

令和６年４月３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とWGの設置による検討体制

産業サイバーセキュリティ研究会

第１回：平成29年12月27日　開催
第２回：平成30年　5月30日　開催
　アクションプラン（４つの柱）を提示
第３回：平成31年　4月19日　開催
　アクションプランを加速化する３つの指針を提示
第４回：令和2年　　4月17日　開催（電話開催）
　産業界へのメッセージを発信
第５回：令和2年　　6月30日　開催
　サイバーセキュリティ強化運動の展開
第６回：令和３年　　４月２日　開催
　アクションプランの持続的発展と、新たな課題へのチャレンジへ
第７回：令和４年　　4月11日　開催
　産業界へのメッセージを発信

構成員

※　2022年4月開催時の構成員・役職

泉澤　清次	三菱重工業株式会社取締役社長
遠藤　信博	日本経済団体連合会サイバーセキュリティ委員長、日本電気株式会社取締役会長等
大林　剛郎	日本情報ｼｽﾃﾑ･ﾕｰｻﾞｰ協会会長、株式会社大林組代表取締役会長
櫻田　謙悟	経済同友会代表幹事、ＳＯＭＰＯホールディングスグループＣＥＯ取締役　代表執行役社長
篠原　弘道	日本電信電話株式会社取締役会長
東原　敏昭	株式会社日立製作所取締役会長　代表執行役
船橋　洋一	一般財団法人アジア・パシフィック・イニシアティブ理事長
村井　純(座長)	慶應義塾大学教授
渡辺　佳英	日本商工会議所特別顧問、大崎電気工業株式会社取締役会長

ｵﾌﾞｻﾞｰﾊﾞｰ　NISC、警察庁、金融庁、総務省、外務省、文部科学省、厚生労働省、農林水産省、国土交通省、防衛省、デジタル庁

WG１（制度・技術・標準化）

第１回　平成30年2月7日
第２回　平成30年3月29日
第３回　平成30年8月3日
第４回　平成30年12月25日
第５回　平成31年4月4日
第６回　令和2年3月（書面開催）
第７回　令和2年10月（書面開催）
第８回　令和3年３月15日
第９回　令和4年4月4日
第10回　令和6年3月14日

１．サプライチェーン強化パッケージ

WG２（経営・人材・国際）

第１回　平成30年3月16日
第２回　平成30年5月22日
第３回　平成30年11月9日
第４回　平成31年3月29日
第５回　令和2年1月15日
第６回　令和2年8月25日
第７回　令和3年2月18日
第８回　令和4年3月23日
第９回　令和5年3月27日
第10回　令和6年3月25日

２．経営強化パッケージ
３．人材育成・活躍促進パッケージ

WG３（サイバーセキュリティビジネス化）

第１回　平成30年4月4日
第２回　平成30年8月9日
第３回　平成31年1月28日
第４回　令和元年8月2日
第５回　令和2年3月(書面開催)
第６回　令和3年3月10日
第７回　令和4年4月6日
第８回　令和6年4月3日

４．ビジネスエコシステム創造パッケージ

産業サイバーセキュリティの加速化指針

１．『グローバル』をリードする
２．『信頼の価値』を創出する～Proven in Japan～
３．『中小企業・地域』まで展開する

前回のWG3における主なご指摘

- WG3 は「ビジネス」に関して議論する場になるので、**資金の流れや資金を捻出する意思という観点で調査を進めるべき**。
- 検証サービスを展開している側の意見として、検証ビジネスの市場規模はまだ小さく、相場観も定まっていないため、**価格は固定せずに市場価格に任せたほうがよい**。
- **経済安全保障の観点も踏まえて整理**してみてはどうか。
- サイバーセキュリティを考える上では明確な基準を定めることが重要である。例えば、最低限実施すべき検証を行っていればリスク値がわかる、となれば保険も適用できるのではないかと思うものの、そのような最低ラインの実施基準を準備できるのか、準備できた場合に損害保険業界の協力を得られるのか、など引き続き検討が必要である。
- **隠れたニーズの掘り起こしは実施しなくてよいのではないか**。**検証サービスを必要とする人に提供することが重要**である。
- **海外のセキュリティラベリング制度のような制度を日本でも構築できると良く**、検証しないと取引できない、サプライチェーンにはいれない、製品が売れないといった状況になり、結果として検証ビジネスのニーズの掘り起こしにつながる。日本だけが厳しい基準を示すのではなく、国際的な動向に合わせ、各国とスピード感を合わせていけるとよい。
- サイバーセキュリティお助け隊について、実際にサービス提供企業へ連絡するユーザ企業は少ないのが現状。サービスを買わされるイメージであるため、コンシュルジュの様な相談サービスがあるとよい。

検証基盤の構築（「Proven in Japan」）に向けたこれまでの取組

	主な内容	これまでの取組・成果
緑 セキュリティ製品の 有効性検証	サイバー攻撃に対応するセキュリティ製品分野を公表し、その分野に該当する我が国発の製品について、専門家による有効性確認を実施し、その内容を発信することで、ユーザーが我が国発の製品を選定しやすい環境を構築。	• 試行導入・導入実績公表の手引き（2021年4月公開）やセキュリティ製品・サービス重要分野マップ（2022年3月改訂）等を公開。
青 実環境における 試行検証	実環境への試行導入・実績公表を行う企業向けの手引きを作成するとともに、試行導入に関心があるユーザーとベンダーをマッチングし、我が国発のセキュリティ製品の試行導入・実績公表を促進。	
赤 攻撃型を含めた ハイレベルな検証	機器のハイレベル検証(ペネトレーションテスト)の方法や人材育成の方法を整理・公開。産業機器等を対象に検証も実施し、その方法の有効性を確認。	• サービス事業者と検証依頼者が実施すべき事項等を整理した手引きを公開（2023年6月改訂）。 • 機器検証サービスの運営開始（2023年3月から審査登録制度に追加、現状登録されているサービスは8件）
開発 セキュリティ・バイ・デザインを 実現する開発段階検証	開発段階から、設計書とソースコード、実装したプロトタイプで検証を行い、脆弱性を排除した開発を実施することにより、効果的な検証の進め方を整理するとともに、開発段階からの検証の効果を可視化。これにより、設計段階からセキュリティを意識する「セキュリティ・バイ・デザイン」の考え方を採り入れ、コスト低減を図りつつ、中小企業に検証の必要性を認知してもらうことを目指す。	・検証事業者や製品ベンダが参照するための手引きを公開（2023年9月公開）。 ・ものづくり補助金において、当該補助金を活用して開発・導入した製品やサービス、システムに対するペネトレーションテスト・脆弱性診断も支援対象として追加（第15次公募（2023年4月）から開始）。

IoT製品に対するセキュリティ適合性評価制度の構築

- 欧米諸国を中心に、**IoT製品に対するセキュリティ対策強化に向けた議論が加速**。
- 諸外国との制度調和も図りつつ、**IoT製品のセキュリティ対策を適切に評価し、適切な対策が講じられているIoT製品が広まる仕組みの検討を実施**（2022年11月～2024年3月に「IoT機器に対するセキュリティ適合性評価制度構築に向けた検討会」を開催）。**2024年3月15日、最終とりまとめを公表し、制度構築方針（案）のパブコメを開始**（１か月間）。
- **インターネットに直接接続されない製品も含め、幅広いIoT製品を対象**としつつ、製品ごとの特性に応じた基準を既存の制度を活かしながら設けられるよう、**複数のレベル（☆１～☆４）を用いた制度**を想定。
- 検討会の最終とりまとめを踏まえ、**☆１については2024年度中の制度開始**を予定。**政府調達等の要件等とすべく関係省庁と議論中**。併せて、**米欧等の諸外国との制度調和を図るため議論中**。

欧米の動向

サイバーレジリエンス法案
（Cyber Resilience Act）

- **デジタル要素を備えた全ての製品（ソフトウエア含む）の製造者に対し、**セキュリティ特性要件に従った**上市前の設計製造等を義務付け。**
- 2023年11月に暫定政治合意。**インシデント等報告義務の運用開始は2025年秋～冬、その他は2027年夏頃運用開始を想定。**

米国サイバー・トラスト・マーク
（U.S. Cyber Trust Mark）

- **消費者向け無線IoT製品を対象とした、任意のラベリング制度。**消費者向けルータ、スマートメーター等**一部製品については、個別のセキュリティ要件が定義される見込み。**
- **2024年中に制度運用開始**を予定。

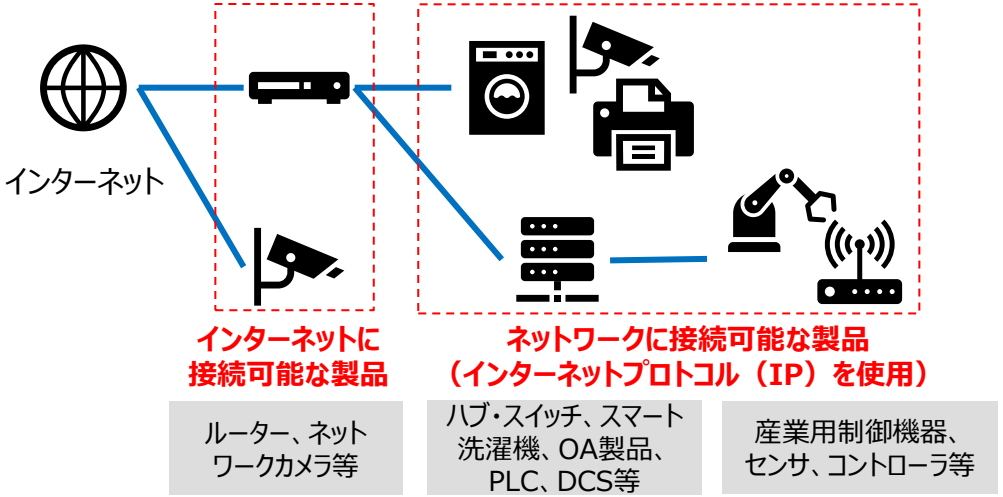
IoT機器に対するセキュリティ適合性評価制度構築に向けた検討会 委員・オブザーバー

（委員）
猪俣 敦夫 大阪大学 情報セキュリティ本部 教授
稲垣 隆一 稲垣隆一法律事務所 弁護士
岩﨑 章彦 一般社団法人電子情報技術産業協会 セキュリティ専任部長
江崎 浩 デジタル庁 シニアエキスパート
高倉 弘喜 国立情報学研究所 アーキテクチャ科学研究系 教授
高橋 範 株式会社ソラコム 事業開発ディレクター
中尾 康二 国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所 主管研究員
中野 学 パナソニックホールディングス株式会社 技術部門 テクノロジー本部 製品セキュリティセンター 製品セキュリティグローバル戦略部 部長
花見 英樹 株式会社日立製作所 インダストリアルデジタルビジネスユニット CTO
広瀬 良太 ヤマハ株式会社 音響事業本部 基盤技術開発部 部長
松浦 芳樹 GROOVE X株式会社 Softwareチーム エリアプロダクトオーナー
唯根 妙子 消費生活アドバイザー

（オブザーバー）
内閣官房内閣サイバーセキュリティセンター
総務省 サイバーセキュリティ統括官室
経済産業省 情報産業課、製品安全課、産業機械課、航空機武器宇宙産業課、国際電気標準課、 通商機構部
（独）情報処理推進機構（IPA）
（独）製品評価技術基盤機構（NITE）
（国研）新エネルギー・産業技術総合開発機構（NEDO）
（公社）日本通信販売協会（JADMA）
（公社）日本防犯設備協会（SSAJ）
（一社）重要生活機器連携セキュリティ協議会（CCDS）
（一社）情報通信ネットワーク産業協会（CIAJ）
（一財）電気安全環境研究所（JET）
（一社）日本電機工業会（JEMA）
（一財）日本品質保証機構（JQA）
（一社）ビジネス機械・情報システム産業協会（JBMIA）
（一社）セキュアIoTプラットフォーム協議会
（一社）組込みシステム技術協会（JASA）
（技組）制御システムセキュリティセンター（CSSC）
電気製品認証協議会（SCEA）
ロボット革命・産業IoTイニシアティブ協議会（RRI）

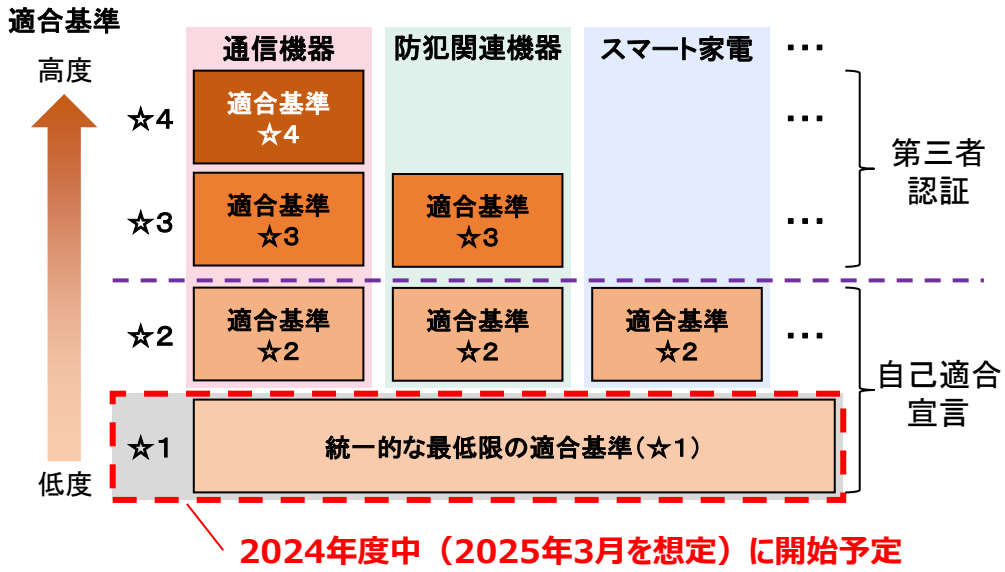
制度構築方針（案）の概要：対象製品、☆１～４の考え方

対象製品の概要



※ 国内外の一部の既存制度と同様に、利用者がソフトウェア製品等により容易にセキュリティ対策を追加することができる汎用的なIT製品（パソコン、タブレット端末、スマートフォン等）は対象外とする。

各レベル（☆１～☆４）のイメージ



レベル	位置付け	適合基準	評価方式
☆３以上	**政府機関等や重要インフラ事業者、大企業の重要なシステムでの利用を想定**したIoT製品類型ごとの汎用的なセキュリティ要件を定め、それを満たすことを**独立した第三者が評価して示す**もの	製品類型別	第三者認証
☆２	**IoT製品類型ごとの特徴を考慮**し、☆1に追加すべき基本的なセキュリティ要件を定め、それを満たすことを**IoT製品ベンダーが自ら宣言**するもの		自己適合宣言
☆１	IoT製品として共通して求められる**最低限のセキュリティ要件**を定め、それを満たすことを**IoT製品ベンダーが自ら宣言**するもの	製品類型共通	

（参考）☆１（IoT製品類型に共通する最低限のレベル）の基準等

- 国際的な基準・ガイドライン（ETSI、NIST）において**一般的にIoT製品類型に共通する最低限のレベルとして求められている事項**を包含する形で、「容易に推測可能なデフォルトパスワードの禁止」、「適切な認証に基づくアクセス制御」、「総当たり攻撃からの保護」、「容易かつ分かりやすいアップデート手順」等、**16の評価項目を設定**。
- 製品類型毎（当面はカメラ、ドローン、NW機器の３類型を想定）に作成する☆２以上では、より具体的なユースケースから脅威を設定し、適合基準を定める。（例：関連サービスとの間の接続認証、データの流れに関する対策）

☆1で考慮する主な脅威			脅威に対抗するために☆1で求める適合基準 ※先頭の"(N)"は対応する☆1評価項目番号を示す			
			IoT製品に対する適合基準		IoT製品ベンダーに対する適合基準	
1.	①弱い認証機能により、	外部からの不正アクセスの対象となり、マルウェア感染や踏み台となる攻撃等を受けることで、情報漏えい、改ざん、機能異常の発生につながる脅威	識別・認証、アクセス制御	(1)適切な認証に基づく**アクセス制御** (2)**容易に推測可能なデフォルトパスワードの禁止** (3)パスワード等の認証値の変更機能 (4)ネットワーク経由のユーザ認証に対する**総当たり攻撃からの保護**	情報提供	(16)ユーザへの**セキュアな利用・廃棄方法に関する情報提供**(初期設定手順、セキュリティ更新、サポート期限、安全な廃棄手順等)
	②脆弱性の放置により、		脆弱性対策、ソフトウェア更新	(6)ソフトウェアコンポーネントのアップデート機能 (7)**容易かつ分かりやすいアップデート手順** (8)アップデート前のソフトウェアの完全性の確認機能 (10)ユーザが型式番号を認識可能とする記載・機能	情報・問い合わせの受付、情報提供	(5)連絡先・手続き等の**脆弱性開示ポリシーの公開** (9)セキュリティアップデートの優先度決定方針の文書化
	③未使用インタフェースの有効化により、		インターフェイスへの論理アクセス	(13)**不要かつリスクの高いインタフェースの無効化**(物理的・論理的な通信ポート等)	－	－
	①～③共通		データ保護	(11)製品に保存される守るべき情報の保護(**保存データの暗号化、匿名化**等)	－	－
2. 機器の通信が盗聴され、守るべき情報が漏えいする脅威			データ保護	(12)ネットワーク経由で伝送される守るべき情報の保護(**通信の暗号化、保護された通信環境の利用**等)	－	－
3. 廃棄・転売等された機器から、守るべき情報が漏えいする脅威			データ保護	(15)**製品内に保存される守るべき情報の削除機能**	情報提供	※(16)に含む
4. ネットワーク切断や停電等の事象が発生した際に、セキュリティ機能に異常が発生する脅威			レジリエンス向上	(14) 停電・ネットワーク停止等からの復旧時の**認証情報やソフトウェア設定の維持**(初期状態に戻らないこと)	－	－

情報セキュリティサービス審査登録制度の概要

- 経済産業省は、**情報セキュリティサービス業の普及を促進し、国民が情報セキュリティサービスを安心して活用することができる環境を醸成することを目的**に、以下の基準を策定。
  - ① **情報セキュリティサービスが満たすべき最低限の技術要件及び品質管理要件を示し、品質の維持・向上に努めている情報セキュリティサービスを明らかにするための基準**（「情報セキュリティサービス基準」）（2018年2月、2023年3月第3版改訂）
  - ② 同基準への適合を審査する機関（以下、審査登録機関）が満たさなければならない基準（「情報セキュリティサービスに関する審査登録機関基準」）（2018年2月、2022年3月第2版改訂）
- これらの基準を踏まえ、登録申請のあったサービスが情報セキュリティサービス基準に適合するかを**審査登録機関が審査の上、「情報セキュリティサービス基準適合サービスリスト」に掲載。**
- 2024年4月現在、**５区分のサービス**を対象として**年4回**の審査を行っており、**合計約300サービスが登録**されている。

＜情報セキュリティサービスにおける課題＞

どの事業者のサービスを選べば良いかわからない

信頼できるサービス事業者にお願いしたい

ユーザ
（企業、政府機関等）

選定時に活用

○情報セキュリティサービス基準適合サービスリスト（IPA）

審査登録機関による審査で基準を満たすと認められたサービスをリストとして公開

基準を満たした約300サービスを掲載（2024年4月時点）

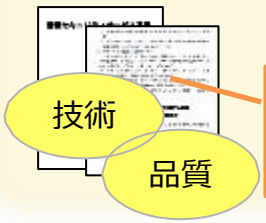
- 情報セキュリティ監査サービス
- 脆弱性診断サービス
- デジタルフォレンジックサービス
- セキュリティ監視・運用サービス
- 機器検証サービス
- **ペネトレーションテスト（侵入試験）サービス（現在検討中）**

審査を受けリストに掲載

我が社のサービスを もっと見つけて欲しい

我が社の技術力、サービス品質をアピールしたい

ベンダー
（サービス提供事業者）



○情報セキュリティサービス基準（経済産業省）

上記６サービスに関して技術要件・品質管理要件を定めた基準

本制度を通じて目指す社会

専門知識を持たないユーザでも、自社に最適かつ品質を備えたサービスを選択できる

技術と品質を備えた情報セキュリティサービスの普及・発展

制度の普及・浸透

情報セキュリティサービス審査登録制度の改訂

- 「政府機関等のサイバーセキュリティ対策のための統一基準群」「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」等でペネトレーションテストが追加セキュリティ対策及び要求事項として記載されていることや、ペネトレーションテストの一般化による**事業者からの追加リクエストがあることを受け**、2022年度より「ペネトレーションテストサービス」の区分追加を検討。
- 既存のサービス区分である**「脆弱性診断サービス」のオプションサービスとして「ペネトレーションテスト（侵入試験）サービス」を追加**した**「情報セキュリティサービス基準第４版」を、今後策定する予定**。

○情報セキュリティ審査登録制度における基準等、文書の関係性

情報セキュリティ審査登録制度

- **情報セキュリティサービス基準** ― （附則） ― **情報セキュリティサービスにおける技術及び品質の確保に資する取組みの例示**

  （情報セキュリティサービスおよびそれぞれが満たすべき基準を定義）

  - 情報セキュリティ監査サービス
  - 脆弱性診断サービス
    - ペネトレーションテスト（侵入試験）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
  - 機器検証サービス

- **情報セキュリティサービスに関する審査登録機関基準**

- 「脆弱性診断サービス」のオプションサービスとして「ペネトレーションテスト（侵入試験）サービス」を追加。
- 既存の「脆弱性診断サービス」は、その対象としてプラットフォーム診断、ウェブアプリケーション診断といった分類を持っているが、この分類に追加した場合、追加の要件を定義することができないため、「ペネトレーションテスト（侵入試験）サービス」はここへの追加を選択せず。
- 「ペネトレーションテスト（侵入試験）サービス」は高度な脆弱性診断サービスとの位置付けで、脆弱性診断サービスに係る基準を包含。満たさなければならない基準も既存の「脆弱性診断サービス」の基準を満たしたうえで、さらに追加の基準を満たす必要がある。

（※）「政府機関等のサイバーセキュリティ対策のための統一基準群」や「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」等で**ペネトレーションテストは高度な脆弱性診断として位置付けられており、それらとの整合性を図る**ため、他のサービスとは別の区分の位置付け。

サイバーセキュリティお助け隊サービス

- 2019年度・2020年度実証事業で得られた知見に基づき、実証参加事業者がサービスを開発。
- サービス普及に向け、2021年度よりサービスブランドを設立。現時点で**42事業者**がサービスを提供。
- 中小企業の意識啓発・サプライチェーンによる普及などの施策と一体となった普及施策の展開を開始。IT導入補助金による支援を拡充。

中小企業のサイバーセキュリティ対策に不可欠な各種サービス

- EDR・UTM等による異常監視
- 緊急時の対応支援・駆付けサービス
- 相談窓口
- 簡易サイバー保険
- 簡単な導入・運用

中小企業でも導入・維持できる価格でワンパッケージで提供

サイバーセキュリティお助け隊サービスウェブページ
https://www.ipa.go.jp/security/otasuketai-pr/

お助け隊サービス審査登録制度：
一定の基準を満たすサービスにお助け隊マークの商標利用権を付与

お助け隊サービスA
お助け隊サービスB
お助け隊サービスC

サービス提供 → 中小企業 → 自社の信頼性をアピール → 取引先（大企業等）

お助け隊サービス利用の推奨等の中小企業の取組支援

サイバーセキュリティお助け隊

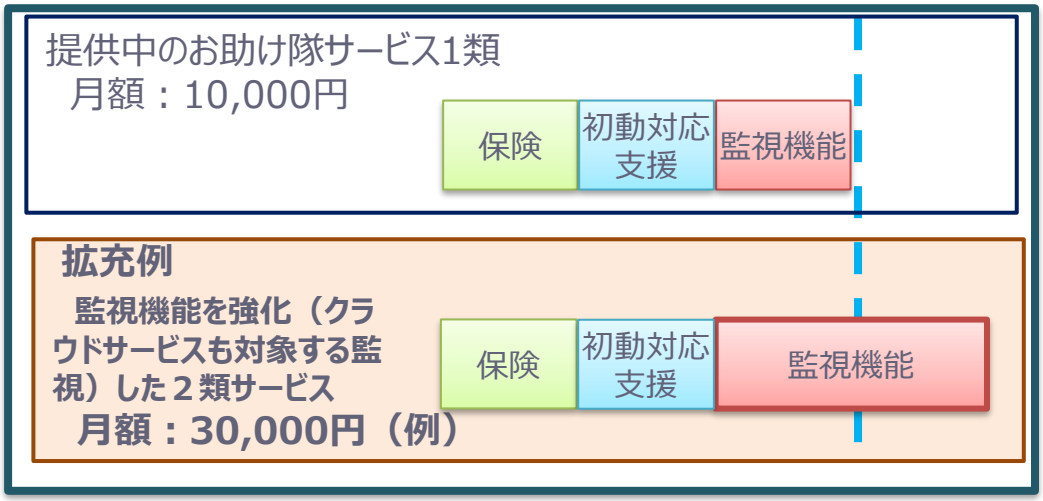
SC3(サプライチェーン・サイバーセキュリティ・コンソーシアム)

→SC3（業種別業界団体が参加）で利用推奨を行うことで、より多くの中小企業がお助け隊サービスを活用し、万が一の際に早急に正しい対処が行える状態を目指す。

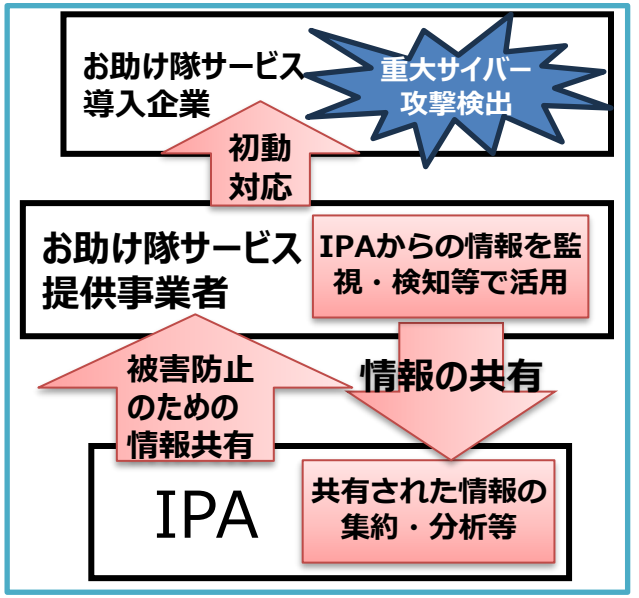
サイバーセキュリティお助け隊サービスの新たな類型（２類）について

- 経済産業省では、ＩＰＡを通じて、システムの異常監視やサイバー攻撃時の初動対応支援、復旧費用の簡易保険など**中小企業のセキュリティ対策に必要となる各種サービスをまとめて提供する民間のセキュリティサービスを登録し公表する「サイバーセキュリティお助け隊サービス」制度を運用（2021年度開始）**。
- 現行のお助け隊サービス（１類）は価格上限があるため実態上、従業員10人前後の中小企業への提供がメインであるところ、**中規模以上の中小企業のニーズにも応えるサービスとなるよう、お助け隊サービスの新たな類型（２類）の検討を実施**。
- 具体的には、現行のお助け隊サービスのコンセプトは維持しながら、**価格要件を緩和しつつ、提供中のお助け隊サービス１類をベースに監視機能の強化や定期的なコンサル実施などの拡充、IPAへの重大サイバー攻撃に関する情報の共有等を要件として、基準の改定を実施**（2024年３月15日に公開）。**お助け隊サービス提供事業者から共有された情報は、IPA内で集約・分析等し、お助け隊サービス提供事業者へ情報共有する**。
- **令和６年度以降、２類サービスの基準への適合性審査を開始し、適合した２類サービスを登録、公表予定**。厚生労働省等の**関係機関や業界団体とも連携しながら**、**お助け隊サービスの更なる普及、促進を図る**。

2類のイメージ

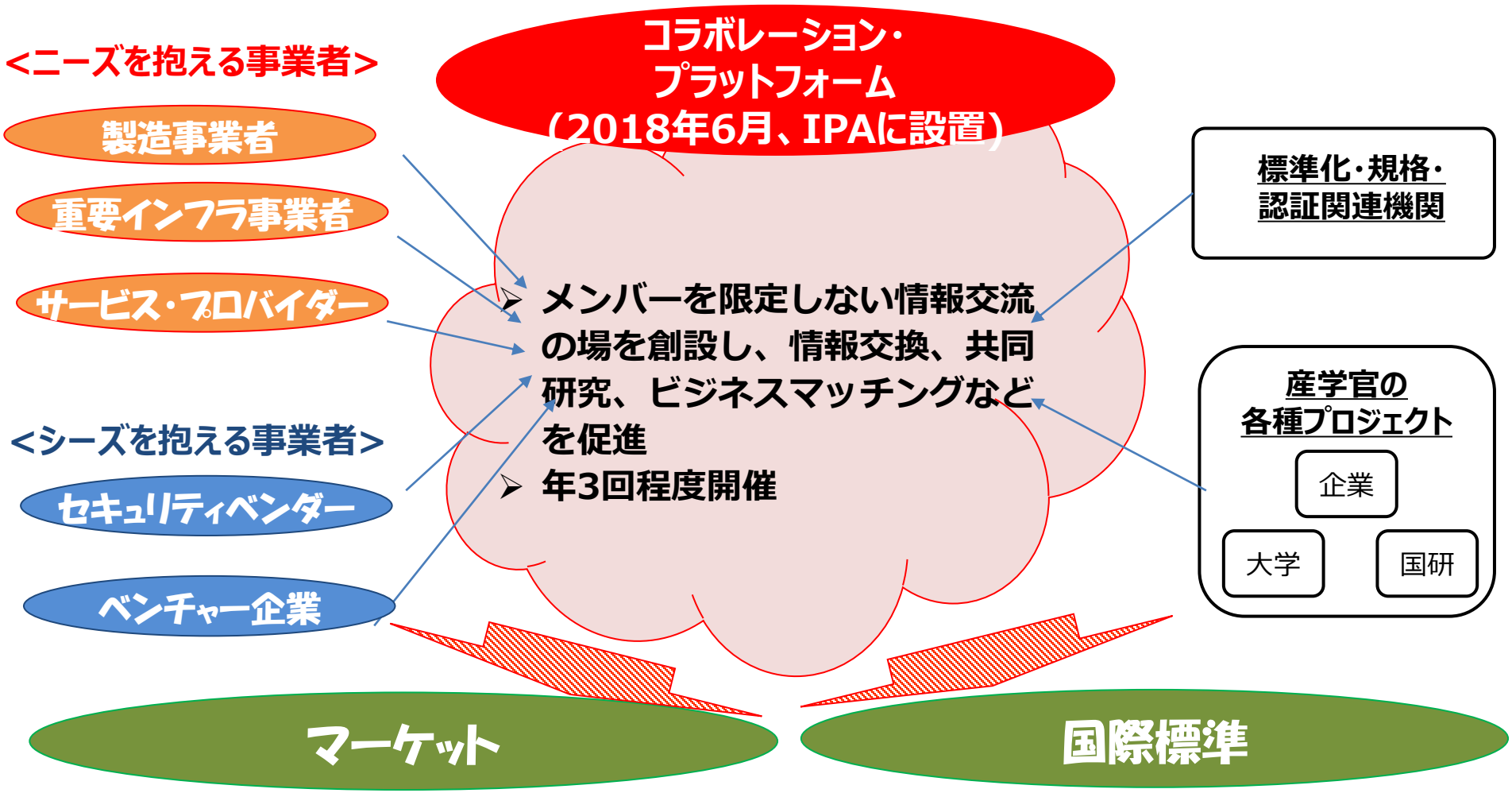


IPAとの情報共有イメージ



官民の対話の場としてのコラボレーション・プラットフォームの開催

- 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、2018年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直近の開催状況

- 令和５年度は３回開催（対面・オンライン併用のハイブリッド形式）。

	開催日	参加人数	テーマ
第25回	2023年9月22日	現地：42名 オンライン：128名	「ポストPPAPのメールセキュリティ」
	➢ 第1部は経済産業省の施策紹介。 ➢ 第2部はパネラーによるショートプレゼンテーションとポストPPAPに関するディスカッション及び質疑応答。		
第26回	2023年12月22日	現地：7名 オンライン：154名	「『サイバーセキュリティ経営ガイドライン』に基づく対策実施状況の可視化」
	➢ 第1部は全員を対象にサイバーセキュリティ経営ガイドラインのポイント解説及び支援ツールの紹介。 ➢ 第2部は現地参加者を対象にサイバーセキュリティ経営可視化ツールのワークショップを開催。		
第27回	2024年2月26日	現地：30名 オンライン：222名	「サイバー・フィジカル・セキュリティ：工場を守るセキュリティ対策とは」
	➢ 第1部は「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」のポイント解説、「スマート工場化でのシステムセキュリティ対策事例 調査報告書」の概説、および工場セキュリティガイドラインをもとに自社工場のセキュリティ対策を実施した企業の事例を紹介。 ➢ 第2部は「サイバー・フィジカル時代の工場セキュリティ対策に重要なものとは」をテーマにパネルディカッションを実施。		