経済産業省

産業分野におけるサイバーセキュリティ政策

（Proven in Japan -検証基盤構築事業-）

経済産業省　商務情報政策局

サイバーセキュリティ課長

奥家 敏和

１．はじめに
～最近の攻撃事例と注意喚起

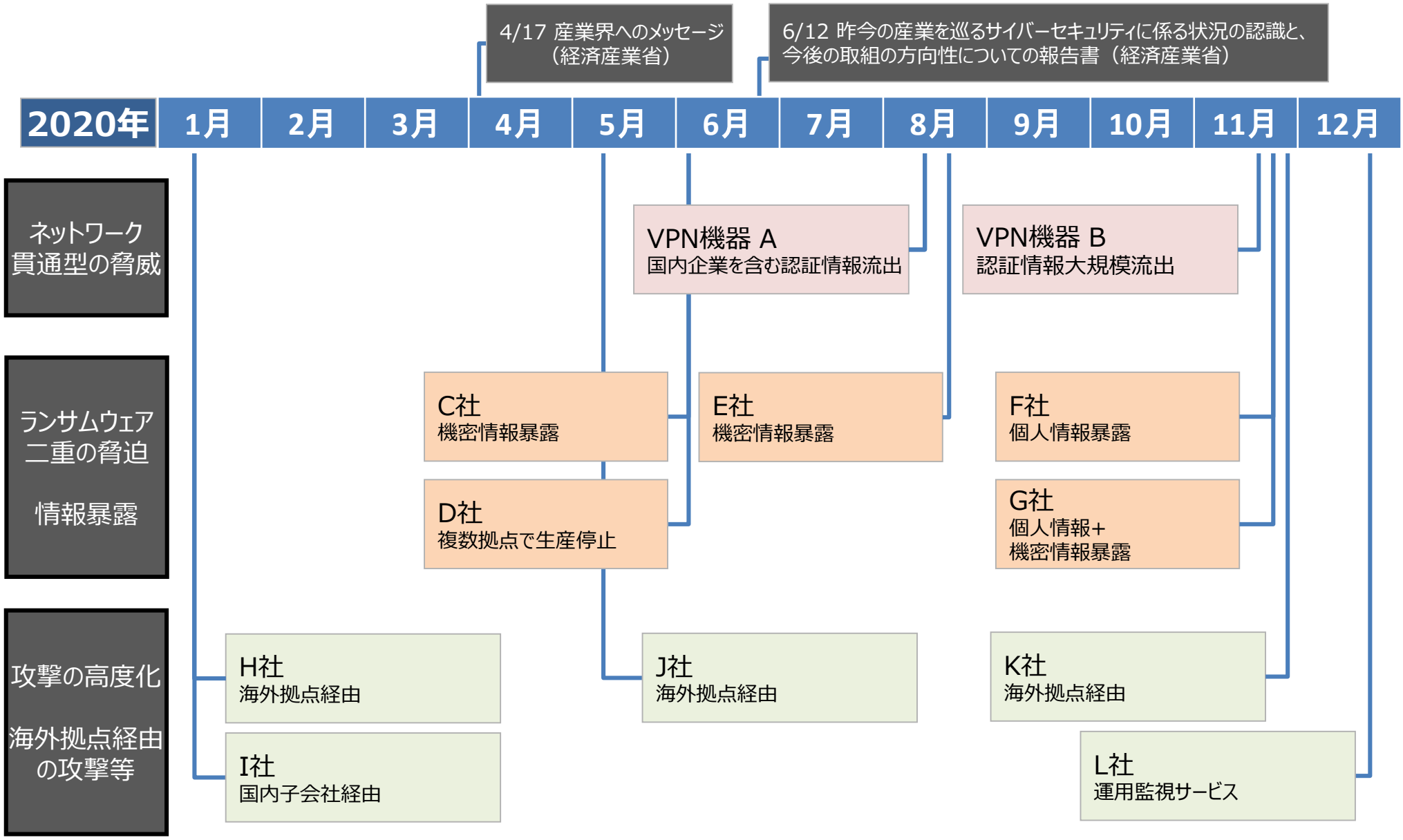
２．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

３．サイバーセキュリティビジネスの創出
～エコシステムの構築　Proven in Japan（検証基盤）

（参考）その他のセキュリティビジネス創出に向けた取組
～情報セキュリティサービス審査登録制度、コラボレーションプラットフォーム

2020年の主なサイバー攻撃事案

2020年12月18日公開資料



※攻撃開始時期ではなく、報道・公表された時期等でマッピング

「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」

2020年12月18日公開資料

- サイバー攻撃は規模や烈度の増大とともに多様化する傾向にあり、実務者がこれまでの取組を継続するだけでは対応困難になっている。
- アップデート等の基本的な対策の徹底とともに、**改めて経営者のリーダーシップが必要に**。

① 攻撃は格段に高度化し、被害の形態も様々な関係者を巻き込む複雑なものになり、技術的な対策だけではなく関係者との調整や事業継続等の判断が必要に。改めて経営者がリーダーシップを。

② ランサムウェア攻撃による被害への対応は企業の信頼に直結。経営者でなければ判断できない問題。

- 「二重の脅迫※」によって、顧客等の情報を露出させることになるリスクに直面。日常的業務の見直しを含む事前対策から情報露出に対応する事後対応まで、経営者でなければ対応の判断が困難。
- 金銭支払いは犯罪組織への資金提供とみなされ、制裁を受ける可能性のあるコンプライアンスの問題。

③ 海外拠点とのシステム統合を進める際、サイバーセキュリティを踏まえたグローバルガバナンスの確立を。

- 国・地域によってインターネット環境やIT産業の状況、データ管理に係るルール等が異なっており、海外拠点とのシステム統合を通じてセキュリティ上の脆弱性を持ち込んでしまう可能性も。
- 拠点のある国・地域の環境をしっかりと評価し、リスクに対応したセグメンテーション等を施したシステム・アーキテクチャの導入や拠点間の情報共有ルールの整備等、グローバルガバナンスの確立が必要。

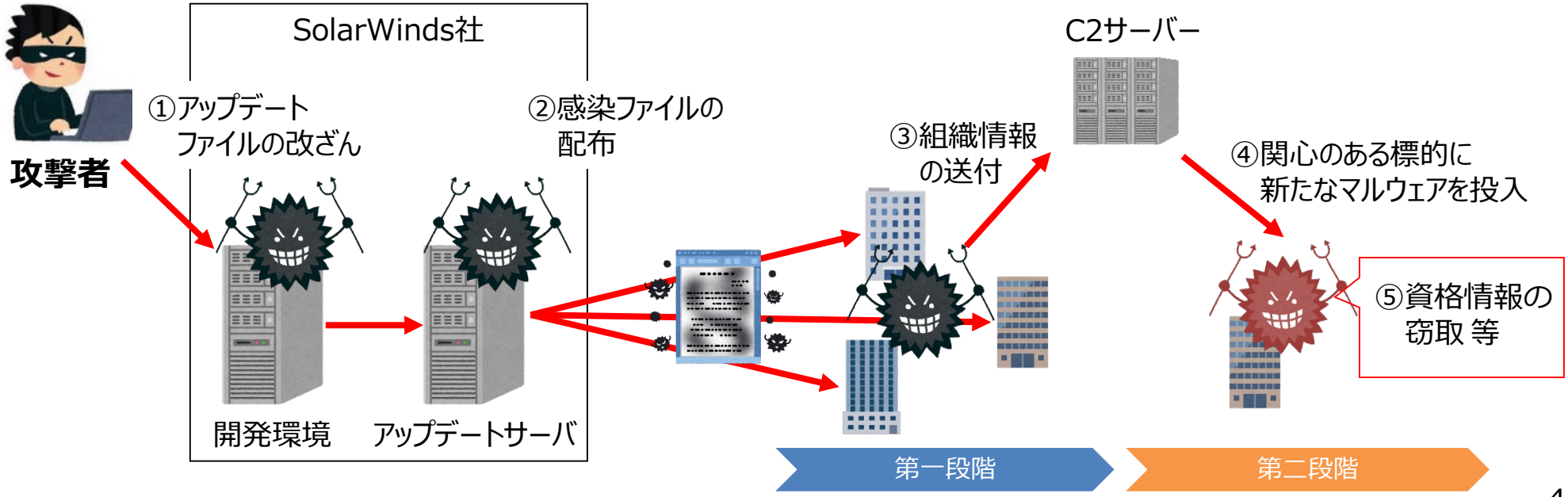
④ 基本行動指針（高密度な情報共有、機微技術情報の流出懸念時の報告、適切な場合の公表）**の徹底を。**

※攻撃者が、被攻撃企業が保有するデータ等を暗号化して事業妨害をするだけではなく、暗号化する前にあらかじめデータを窃取しておいて支払いに応じない場合には当該データを公開することで、被攻撃企業を金銭の支払いに応じざるをえない状況に追い込む攻撃形態。

SolarWinds Orion Platformのアップデートを悪用した攻撃

- 2020年12月13日、SolarWinds社は同社のネットワーク監視ソフトウェア「Orion Platform」に、**正規のアップデートを通じてマルウェアが仕込まれた**ことを公表。
- 攻撃は2019年9月には始まっていたとみられ、2020年3月～6月のアップデートファイルが侵害されたことで、米政府機関等を含む**最大約18,000組織が影響**を受けたとされる。
- 初期段階のマルウェアは、セキュリティサービスの検知を回避しつつ被害組織の情報をC2サーバーへ送信。**攻撃者が関心のある標的に対しては第２段階のマルウェアが投入**され、資格情報を窃取した上で、**米国政府内、政府間のやり取りを傍受していた可能性が指摘されている。**

◆攻撃イメージ

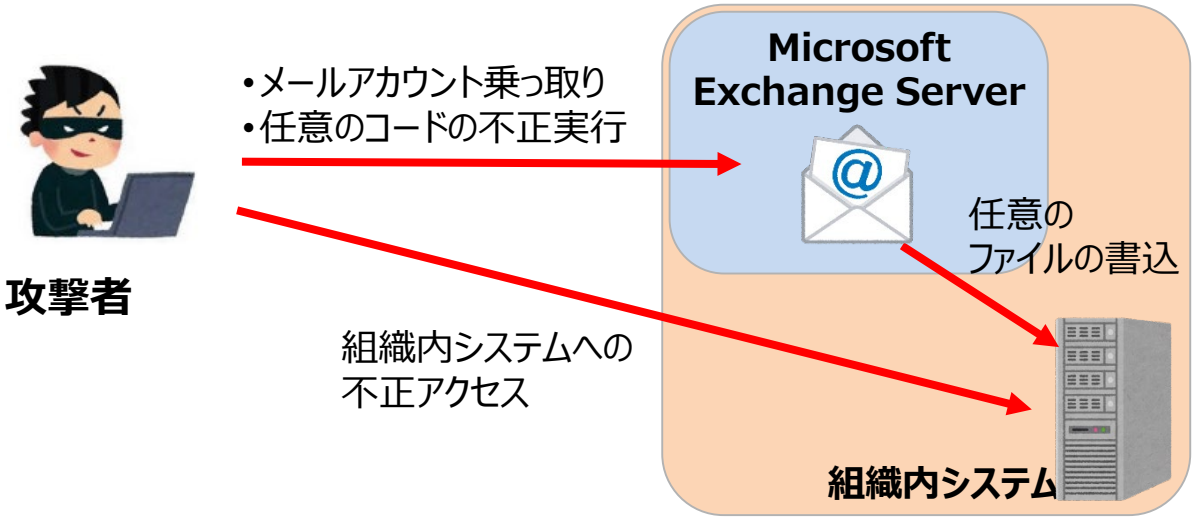


（出典）各種公開情報に基づき経済産業省作成

Microsoft Exchange Serverを狙った国家支援型サイバー攻撃

- 2021年3月2日、Microsoft社は**Microsoft Exchange Serverのゼロデイ脆弱性を悪用**した不正アクセス事案の発生及び当該脆弱性のセキュリティパッチを公表した。
- 本脆弱性を悪用することで、**Eメールアカウントの乗っ取りの他、攻撃者がさらなるシステム侵害を行うためのバックドアが設置**されるおそれがある。そのため、パッチの適用のみならず、侵害の有無の確認及び影響の排除を行う必要がある。
- 本事案が判明した時点で、**全世界で数十万にのぼる組織が攻撃を受けた**とされている。
- Microsoft社は、**中国の支援を受けた攻撃グループによる犯行**の可能性が高いとしている。

◆攻撃イメージ



2020年12月18日発出「注意喚起」のUpdate　～最新事例から得られる教訓

- 2020年12月18日発出の「注意喚起」以降に発生したサイバー攻撃の動向等を踏まえ、ソフトウェア・システム開発ベンダ、ユーザー企業が留意すべき点をまとめる。

ソフトウェア・システム開発ベンダが留意するべき事項

- **ソフトウェア開発工程のセキュア化**
  - ➡ 開発環境への侵入を前提に、ゼロトラスト等の仕組みを導入し、ソフトウェア開発工程全体をセキュア化する。
- **ソフトウェア構成情報(SBOM）や、緊急的な攻撃回避策等の迅速・確実な提供**
  - ➡ 提供するソフトウェア・サービスに関して、顧客自らが正確にリスクを把握できるように、SBOM等を提供する。
  - ➡ 情報漏えいにつながりうる機能追加を実施したり、新たな脆弱性等が発見された場合には、被害を最小限に留めるための攻撃回避策や対応策について、迅速かつ確実に提供し、顧客を丁寧にサポートする。
  - ➡ 上記の問題が発生し、全ての顧客と相対で速やかに対応することが難しい場合、問題と対処法を速やかに公表する。

ユーザ企業が留意するべき事項

- **海外拠点（海外に業務委託している場合を含む）のセキュリティ対策の一層の強化**
  - ➡ 海外拠点経由のサイバー攻撃が急増していることや、海外の事業者に業務委託する中で情報流出が発生する懸念が明らかになってきていることを踏まえ、攻撃の起点となる脆弱なサーバ（野良サーバ等）が放置されていないか、サーバ上でWebshell等の危険度の高いツールが悪用される可能性がないか、業務委託している場合のアクセス範囲の設定などが適切になっているかなど、改めて総点検する。
- **利用中のシステム/クラウドサービスに関するリスクの永続的な見直しの実施**
  - ➡ システムを構築したまま放置したり、管理を委託先任せにしたりせずに、SBOM等を活用して関連する脆弱性情報を自ら積極的に把握し、迅速に対応できるようにする。
  - ➡ クラウドサービス利用時には、不都合な仕様変更がありうることを前提に、定期的な検証を実施する。

Solarwinds事案：米･英当局による対ロシア共同キャンペーン

- 2021年4月15日、米NSA･CISA･FBIは、SolarWinds Orion Platformのアップデートを悪用した攻撃がロシア対外諜報庁（SVR）によるものと特定し、早急な対策を推奨。
- 同日、バイデン大統領は、ロシアの悪質な対外活動に対し制裁を課す大統領令に署名。米政府は、露外交官10名の国外退去、国債取引の禁止等、包括的な対ロシア制裁を発表。
- 同日、英外務省･NCSCは、米の懸念を共有し、攻撃の背後にSVRがいるとの評価を初めて公表。

●米NSA・CISA・FBIによる共同アドバイザリー

・露SVRは、5つの既知の脆弱性を悪用し、米国及び同盟国のネットワークを攻撃。
・全ての関係者に対し、5つの脆弱性による侵入の痕跡チェックと早急な対策を強く推奨。

●米政府による露政府の有害な対外活動に関する包括的制裁、国際協調のイニシアティブ

・バイデン大統領は、ロシア政府の有害な外国活動を対象とした制裁発動に係る大統領令に署名。
・米財務省は、2021年6月14日以降、ロシア国債の米国金融機関による取扱を禁止する指令を発令。
・米財務省は、ロシア諜報機関によるサイバープログラムを支援しているとされる6社（Positive Technologies、AST、Neobit、Pasit、SVA、ERA Technopolis）を制裁対象に指定。
・米財務省は、ロシア政府による米国大統領選挙への干渉に関係した32の団体・個人を制裁対象に指定。
・諜報機関要員を含むロシアの外交使節団10名を国外退去。
・①独ジョージマーシャルセンターでのパブリック・アトリビューション・コースの開設、②DODによる防衛演習“CYBER FLAG 21-1”の英、仏、デンマーク、エストニアとの共同開催等、同盟国との協力強化を発表。

●英NCSCプレスリリース、英外務省プレスリリース

・英NCSCは、SolarWindsの侵害を含む一連のサイバー攻撃の背後に露SVRがいるとの評価を、初めて公表。
・英外務省は、ロシアの悪意ある行動に対する米国の懸念を共有。ロシアを依然として安全保障上の最も深刻な脅威と表明し、社会を不安定化させようとするロシアの試みを引き続き防ぐ。

サイバー攻撃による米国石油パイプラインの操業停止について

- 5月7日、米石油パイプライン最大手のコロニアル・パイプラインがランサムウェアによるサイバー攻撃を受け、全ての業務を停止したと発表。直接の影響を受けたのはITシステムだが、脅威を封じ込めるためにOTシステムをオフラインにし、全てのパイプラインの運用を停止した。小規模ラインの一部は復旧し始めているものの、全体の復旧時期は不明。
- 米運輸省は9日、燃料の輸送に関して緊急措置の導入を宣言。また、CISAのサイバーセキュリティ部門トップも声明を公表。
- FBIはロシア系攻撃集団「ダークサイド」の関与を断定、同グループは「目的は金銭であり社会に影響を与えることは意図していない」と表明（※）。

※：同グループは略取した身代金の一部を対価に開発したランサムウェアをグループ外の実行犯に提供するスキームを運用しており、実行犯がもたらした影響に同グループは関知しない、とのスタンス

コロニアル・パイプライン

メキシコ湾岸の製油所と米東部・南部を結ぶ全長8,850kmのパイプライン。
東海岸の需要の約半分にあたる１日約１億ガロンを輸送。

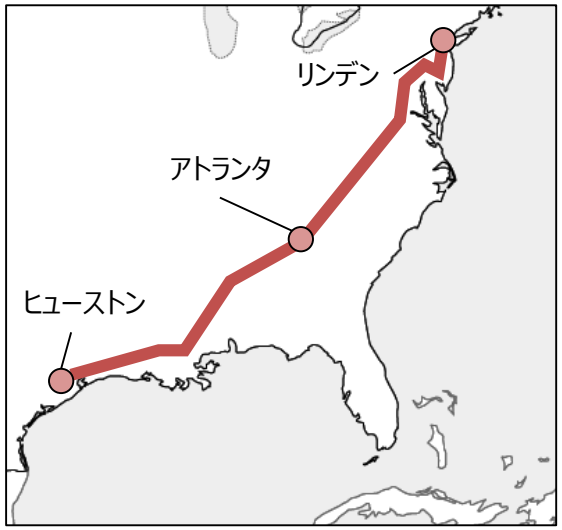
米運輸省による緊急措置の内容

影響を受ける１７州と首都ワシントン向けに
燃料を輸送する運転手の労働時間規制を一時的に緩和。

米CISAによる声明のポイント

CISAは、サイバーセキュリティ部門トップのGoldstein氏名で声明を公表。

・被害企業と関係官庁とともに本事案に対処中。
・ランサムウェアは組織の規模、セクターに関係なく直面する脅威。
・この種の脅威に晒されるリスクを減らすためサイバーセキュリティ体制を強化する措置を講じることを各組織に推奨。



コロニアル・パイプラインの
主要パイプライン（イメージ）

食肉加工事業者へのランサムウェア攻撃事案

- 2021年5月30日(日)、ブラジルにある食肉加工世界最大手JBSがランサムウェアによるサイバー攻撃を受け、アメリカ、カナダ、オーストラリアにおける操業を一時停止。この影響で米国の牛肉生産が1/5減少し、オーストラリアの食肉処理場で非正規雇用者を最高7,000人一時解雇。
- 北米、オーストラリアの情報システムが被害を受けるも、バックアップサーバーから復旧を行い6月3日中に全ての施設で業務を再開。
- FBIは声明で、ロシアを拠点とするサイバー攻撃集団「REvil(Sodinokibi)」による攻撃と発表。

■JBSの概要
- JBSは世界に300以上の生産工場を持ち、150カ国以上に食肉を輸出。
- 牛肉とラムでは世界最大の加工業者。

■攻撃の概要
- 北米とオーストラリアのデータサーバの一部に影響があり、影響を受けたすべてのシステムを一時停止したことに伴い、一部の加工工場の操業も停止。
- 影響がなかったバックアップサーバーからシステムを復旧。
- 顧客、サプライヤー、従業員のデータが侵害された形跡はないと発表。
- 犯罪組織から身代金を要求されたとのことだが、支払いの有無は不明。
- 同社は、「本事案による生産量の減少は１日分にも満たず、向こう１週間で取り戻せる」と発表。

出典：https://www.nikkei.com/article/DGXZQOGN03EHL0T00C21A6000000/
https://www.itmedia.co.jp/news/articles/2106/02/news067.html

１．はじめに
～最近の攻撃事例と注意喚起

２．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

３．サイバーセキュリティビジネスの創出
～エコシステムの構築　Proven in Japan（検証基盤）

（参考）その他のセキュリティビジネス創出に向けた取組
～情報セキュリティサービス審査登録制度、コラボレーションプラットフォーム

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

※2021年4月開催時点

構成員

- **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
- **中西　宏明**　株式会社日立製作所取締役会長
- **船橋　洋一**　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

オブザーバー　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

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

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

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

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

１．はじめに
～最近の攻撃事例と注意喚起

２．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

３．サイバーセキュリティビジネスの創出
～エコシステムの構築　Proven in Japan（検証基盤）

（参考）その他のセキュリティビジネス創出に向けた取組
～情報セキュリティサービス審査登録制度、コラボレーションプラットフォーム

セキュリティのエコシステムを実現するための課題全体像

- 信頼できる製品・サービスと隠れたニーズを掘り起こし、ビジネスマッチングの場を提供することにより、セキュリティ産業の発展を目指す。

安心して製品・サービスを利用できる基盤を構築

1．Proven in Japan（検証基盤）

2．情報セキュリティサービス審査登録制度

3．セキュリティに関する契約の在り方の検討

&

隠れたニーズに対応したビジネスの創出

4．サイバーセキュリティお助け隊

5．中小企業向け製品・サービスの検証

市場への展開

ビジネスマッチング

6．コラボレーション・プラットフォーム

包括的なサイバーセキュリティ検証基盤を構築し、『Proven in Japan』を促進

- 「**Proven in Japan**」では、2つの方向を追求し、**セキュリティビジネスの成長を促進**。

① 有効性確認等を通じ、日本発のサイバーセキュリティ製品のマーケット・インを促進

② IoT機器等の信頼性を高度に検証するハイレベル検証サービスの拡大

1．セキュリティ製品の有効性検証

2．実環境における試行検証

3．攻撃型を含めたハイレベルな検証サービス

信頼できる
セキュリティ製品・サービス

世界に貢献する
高水準・高信頼の検証サービス

セキュリティ製品の有効性検証・実環境における試行検証実施

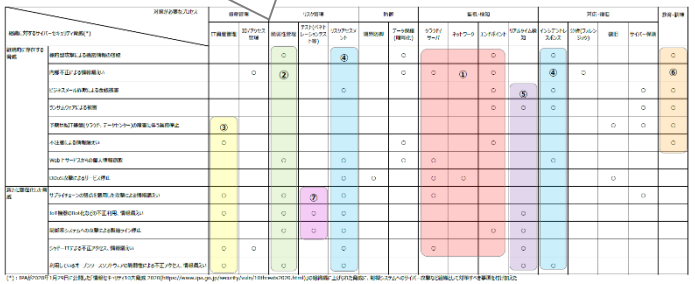
緑 青

- 有識者会議を開催し、重要分野の選定、該当分野の製品の公募、検証作業を実施。
- 有効性検証、実環境における試行検証それぞれのアウトプットを取りまとめ、コラボレーション・プラットフォームで発表。

累計2,101DL
（2020/4/10～2021/3/31）

有識者会議でセキュリティ領域の全体マップを作成し、**重要分野**を選定（市場性、日本発の製品が強味を発揮可能か等の観点から）

① 脅威の可視化
② 脆弱性の可視化
③ IT資産管理
④ 脅威インテリジェンスの整理・管理
⑤ マルウェア感染/は省の重篤度判定
⑥ 教育・トレーニング
⑦ ハイレベルセキュリティ検証



重要分野に該当する**製品を公募で選定**
有効性評価、実環境における試行**評価を実施**

有効性検証 → **検証環境**

yamory
（OSSの脆弱性可視化）
VISIONAL

お試し製品提供と検証 → **実環境**

AX-Network Visualization
（ネットワーク脅威可視化）
AlaxalA

結果をIPAから公表した他、第13回コラボレーション・プラットフォーム（2020年9月）で発表、**ビジネスマッチング**を実施

日本発製品・サービスのプロモーションに資するため、主に以下の内容を公表

有効性検証結果
製品のストロングポイント

実環境における試行検証結果
『試行導入・導入実績公表の手引き』
- 公表のメリット／デメリット
- 公表可否判断のポイント
- 公表内容
- ステークホルダーとの調整 等

セキュリティ製品の有効性検証・実環境における試行検証実施

緑 青

- コラボレーション・プラットフォームで成果発表とビジネスマッチングを実施、90名が参加
- ベンダー各社は有効性検証に参加したことを自社の宣伝活動に活用

コラボレーション・プラットフォームでビジネスマッチングを実施

（第13回、2020年9月28日）

- 「課題解決に役立つ対策技術のご紹介」と題し、検証に参加いただいたベンダーの製品紹介と、個別相談会を実施
- 90名参加

ベンダー各社が有効性検証の成果を自社製品の宣伝に活用

- **Visional社ブログ**
  - 「yamory」が IPA のセキュリティ製品の有効性検証の試行対象として選定
  - 「yamory」の終わりなき技術的挑戦。Visionalの仲間とともに、サイバーセキュリティの未来を創る。
- **アラクサラネットワークス社広報**
  - 「IPAがアラクサラのネットワーク可視化・異常検知ソリューション(AX-NV)の検証結果を公表」
  - 日刊工業新聞、日経新聞、日経産業新聞がアラクサラの広報を転載して紹介


yamory Blog

2020/4/13 お知らせ

「yamory」が IPA のセキュリティ製品の有効性検証の試行対象として選定

編集チーム

オープンソース脆弱性管理ツール「yamory」は、この度、独立行政法人情報処理推進機構（IPA）の「セキュリティ製品の有効性検証の試行」において対象製品に選ばれ、その結果が公表されました。

1. オープンソース脆弱性管理ツール「yamory（ヤモリー）」について
2. 「セキュリティ製品の有効性検証の試行」について
3. 有効性検証の試行結果

オープンソース脆弱性管理ツール「yamory（ヤモリー）」について

yamoryは、オープンソースの利用状況を自動で把握し、脆弱性を検出、管理・対策できるサービスです。

オープンソースに関する最新の脆弱性情報を用いて、yamory 独自の脆弱性データベースを構築しています。


AlaxalA お問い合わせ

ホーム > 会社情報 > プレスリリース >
IPAがアラクサラのネットワーク可視化・異常検知ソリューション(AX-NV)の検証結果を公表

IPAがアラクサラのネットワーク可視化・異常検知ソリューション(AX-NV)の検証結果を公表

2020年5月25日
アラクサラネットワークス株式会社

アラクサラネットワークス株式会社（本社：神奈川県川崎市　代表取締役社長兼CEO 中川 勝博 ／ 以下、アラクサラ）のネットワーク可視化・異常検知ソリューションAX-Network-Visualization（AX-NV）は、独立行政法人情報処理推進機構（IPA）が行った「セキュリティ製品の有効性検証の試行」において「利用者の実環境における試行検証」の対象製品として選定され、その結果が公表されました。

https://www.ipa.go.jp/security/economics/shikoukekka2019.html

経済産業省の産業サイバーセキュリティ研究会の下に設置したWG3は、日本発の新たなセキュリティ製品の市場参入を促進するために、有効性検証および実環境における試行導入検証を実施し、その内容を発信することで、ユーザが日本発の製品を選定しやすい環境の構築を進めています。

これを受けて「サイバーセキュリティ検証基盤構築に向けた有識者会議(以下、有識者会議)」をIPA内に2019年9月に立ち上げました。そして有識者会議が、日本のユーザ企業の重要課題に対応可能な日本発のセキュリティ製品として、AX-NVを対象にユーザの実環境における試行検証を行いました。

緑 青

2020年度の取組（1/2）

有識者会議を６回開催。昨年度成果を踏まえ、検証基盤の構築・運用に関するより踏み込んだ検討を実施。公募を経て２製品を選定し、検証を実施。（緑検証）

緑
サイバーセキュリティ検証基盤の構築
・製品選定～有効性検証の仕組みの構築
・有効な検証結果公表の仕組みの構築

緑
サイバーセキュリティ検証基盤の運用
・製品選定～有効性検証の実施

緑
市場参入支援の仕組み検討
・日本発セキュリティ製品の市場参入を支援する、業界横断の仕組み検討（調査、課題分析、全体図）

青
2019年度成果「試行導入の手引き」改良
・セキュリティ製品のPOCに積極的に取組んでいるユーザ企業にヒアリング等実施

検証基盤運用のプロセス	実施概要
1. 重要分野選定	• 重要分野マップについて、セキュリティ脅威の状況、ユーザ企業の状況、セキュリティ技術の変化等を踏まえて必要な見直しを行う。
2. 製品公募	• 製品公募に際しての公募要領・応募用紙を作成し、公募を行う。 • 幅広い製品・ベンダーに応募頂くために、公募の周知を行う。
3. 製品選定	• 応募された製品・ベンダーの中から、有効性検証の対象となる製品を選定する。 • 製品選定を効率化するために、事前に審査基準を定める。
4. 有効性検証	• 選定された製品の検証を実施する。そのために、製品に対する検証項目、検証環境、検証方法を決定する。 • 製品の特徴的な機能や強み、差別化ポイント（ストロングポイント）を調査する。
5. 検証結果公表	• 検証結果を文書化し、公表する。 • 検証結果に基づき、当該製品・ベンダーのプロモーションを行う。

公募の結果、独自性、重要分野への該当度合等の観点から以下の２製品を検証対象に選定し、検証を実施：

・GUARDIAX（グレスアベイル社）
SaaS型のWAF（Webアプリケーション・ファイアウォール）

・WiSAS（スプライン・ネットワーク社）
WiFi環境の可視化、最適化、不正利用の防止等

緑 青

2020年度の取組（2/2）

- 来年度以降を見据えてスタートアップ等ベンダーの市場参入支援の仕組みの検討も実施（緑検証）
- ユーザ企業の声等から「試行導入の手引き」の改良も実施（青検証）

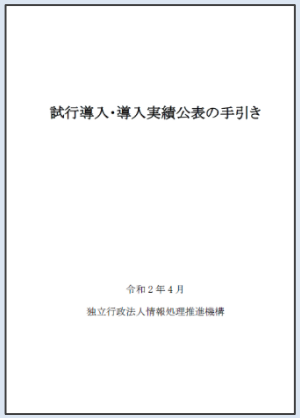
緑
サイバーセキュリティ検証基盤の構築
・製品選定～有効性検証の仕組みの構築
・有効な検証結果公表の仕組みの構築

緑
サイバーセキュリティ検証基盤の運用
・製品選定～有効性検証の実施

緑
市場参入支援の仕組み検討
・日本発セキュリティ製品の市場参入を支援する、業界横断の仕組み検討（調査、課題分析、全体図）

青
2019年度成果「試行導入の手引き」改良
・セキュリティ製品のPOCに積極的に取組んでいるユーザ企業にヒアリング等実施

主な論点：
- **ベンチャー成長の各フェーズにおける課題と解決の方向性**
- **関係するプレイヤーと役割の整理**
- **本基盤の目指す所と提供すべき機能**
- **プロモーションの方式・場**
- **投資家による企業評価との連携**
- **公的機関の役割　他**

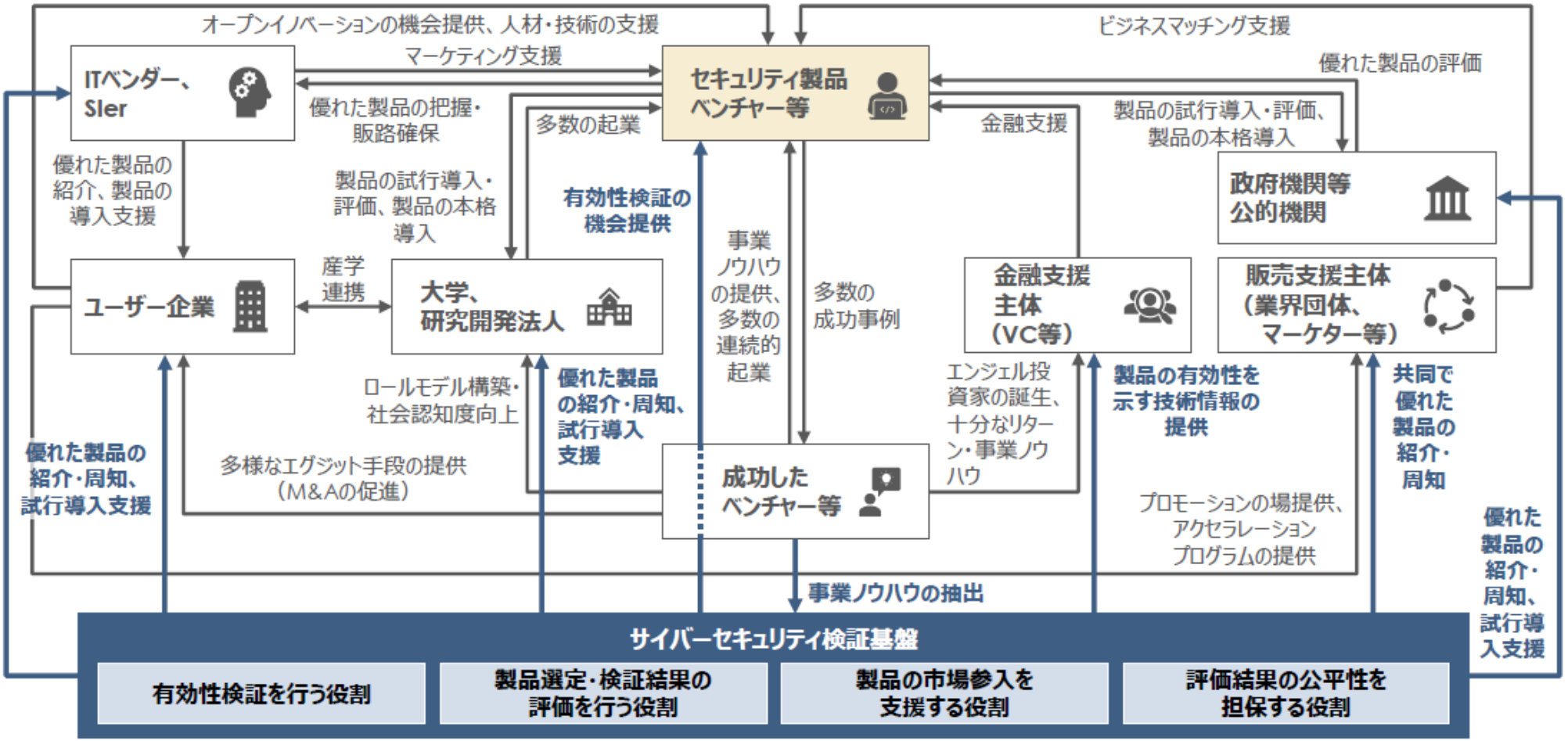

試行導入・導入実績公表の手引き

令和２年４月
独立行政法人情報処理推進機構

ユーザ企業２社へのインタビュー調査等実施、以下の記述を強化：
- 試行導入結果の公表可否判断のポイント（メリット・デメリット）
- 試行導入をした上で実導入することのメリット（コスト最適化、運用の早期安定化等）
- ベンダー側が準備し、ユーザに提供すべき情報　等

緑 青

（参考）市場参入支援の仕組みを構成するプレイヤー・役割の関係図（現状案）

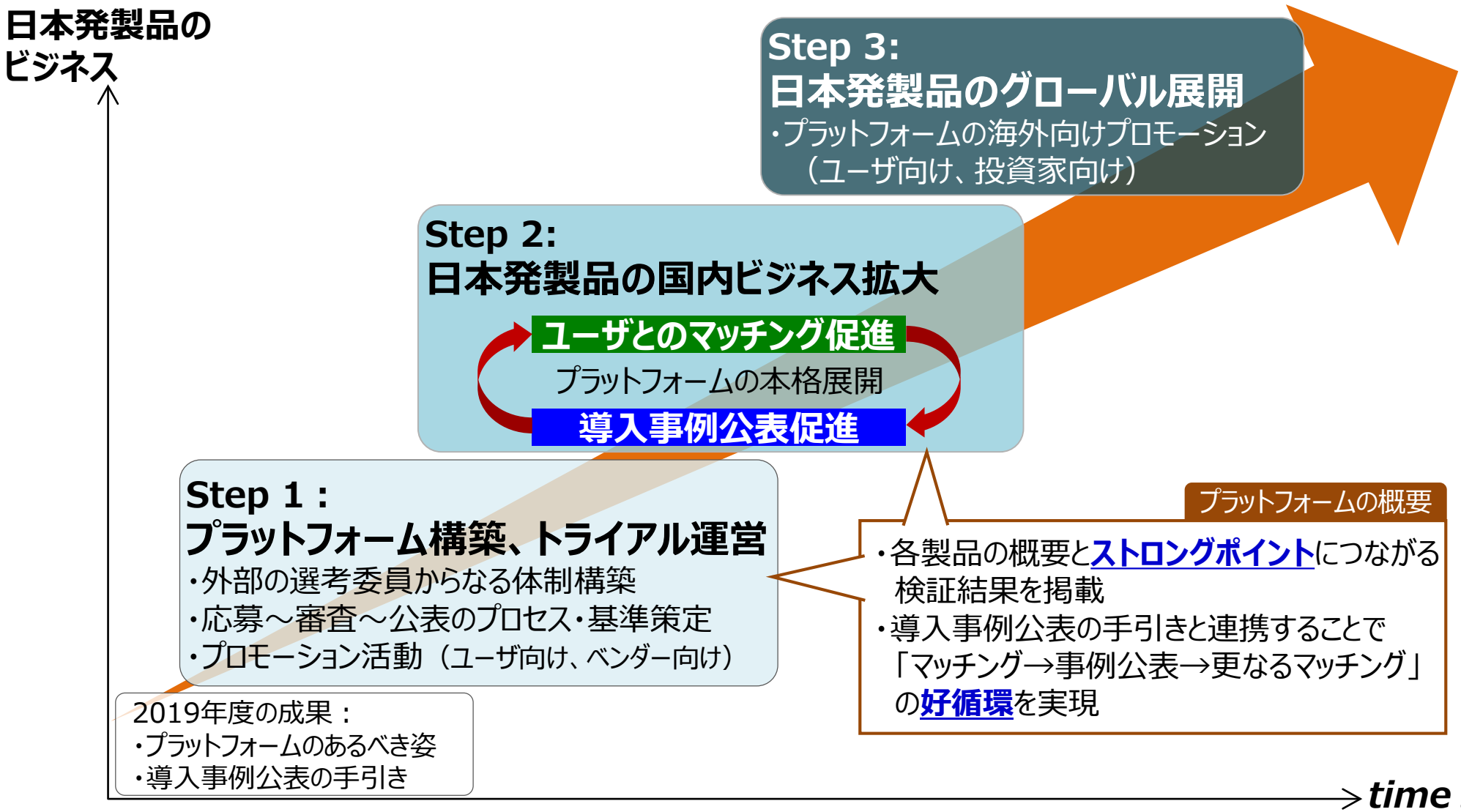


出所）経済産業省「イノベーション・ベンチャー政策について」に基づき三菱総合研究所作成
http://www.kantei.go.jp/jp/singi/keizaisaisei/miraitoshikaigi/innovation_dai3/siryou4.pdf

セキュリティ製品の有効性検証・実環境における試行検証実施

緑 青

２年間に渡る本事業の成果を基に、マッチングプラットフォーム構築、日本発セキュリティ製品の国内ビジネス拡大、更に海外展開を目指す。



赤

（参考）Society5.0時代の信頼性確保のために必要となる攻撃型手法を含むハイレベルな検証サービスの普及展開へ向けた実証

- 検証サービスの信頼性向上及び検証ビジネスの活性化のために、2019年度に作成した手引きについて、2020年度は**本編を拡充するとともに、検証サービス事業者・検証依頼者それぞれを対象とし、より具体的な記載を行った別冊を作成**。2021年４月に公開。

実証

検証事業者

検証

・IoT機器等
＜2019年度＞
ルータ、UTM、タブレット、スマートロック
＜2020年度＞
ドローン、スイッチ、ロボット掃除機、ノートPC

実証の成果と活用のイメージ

機器のサイバーセキュリティ確保のための セキュリティ検証手引き

検証サービス事業者、検証依頼者の双方が、検証における各フェーズにおいて留意すべき事項等を記載

別冊1：検証サービス事業者向け

本編の記載を検証サービス事業者向けに深掘り
・脅威分析の手法　・実施すべき検証項目　・検証の流れ　等

別冊2：検証依頼者（特に機器メーカ）向け

本編の記載を主な検証依頼者である機器メーカ向けに深掘り
・機器開発における検証の重要
・検証を依頼する際に必要な事項　等

別冊3：検証人材の育成について

検証人材の育成について深掘り
・検証人材に求められるスキル・知識、キャリアデザイン　等

期待される効果

検証サービスの効果・信頼性向上

検証ビジネスの普及展開

『Proven in Japan』の促進

https://www.meti.go.jp/press/2021/04/20210419003/20210419003.html

（参考）ハイレベル検証：機器のサイバーセキュリティ確保のための検証の手引き策定

赤

- 検証サービスの信頼性向上及び検証ビジネスの活性化のために、2019年度に作成した手引きについて、2020年度は**本編を拡充するとともに、検証サービス事業者・検証依頼者それぞれを対象とし、より具体的な記載を行った別冊を作成、2021年4月に公開。**

機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き （2019年度作成、2020年度拡充）

- 検証スキルの向上や検証サービスの高度化を目的とし、検証サービス事業者が実施すべき事項や、検証依頼者が実施すべき事項や用意すべき情報、二者間のコミュニケーションにおいて留意すべき事項等を記載。
- 信頼できる検証サービス事業者を判断・選択するための基準を記載。

別冊1：脅威分析及びセキュリティ検証の詳細解説書（2020年度作成）

- 検証ビジネス全体の底上げのために、検証サービス事業者が実施すべき脅威分析の手法や実施すべき検証項目、検証の流れを詳細に示す。
- 機器全般に汎用的に活用できる整理を目標とするが、対象の例としてIoT機器を例示し具体的な記載も行う。

別冊3：検証人材の育成に向けた手引き（2020年度作成）

- 検証人材に求められるスキル・知識を示し、それらのスキル・知識を獲得するために望まれる取組を示す。
- 検証人材のキャリアを構想・設計する上で考慮すべき観点を示し、検証人材のキャリアの可能性を示す。

別冊2：機器メーカに向けた脅威分析及びセキュリティ検証の解説書（2020年度作成）

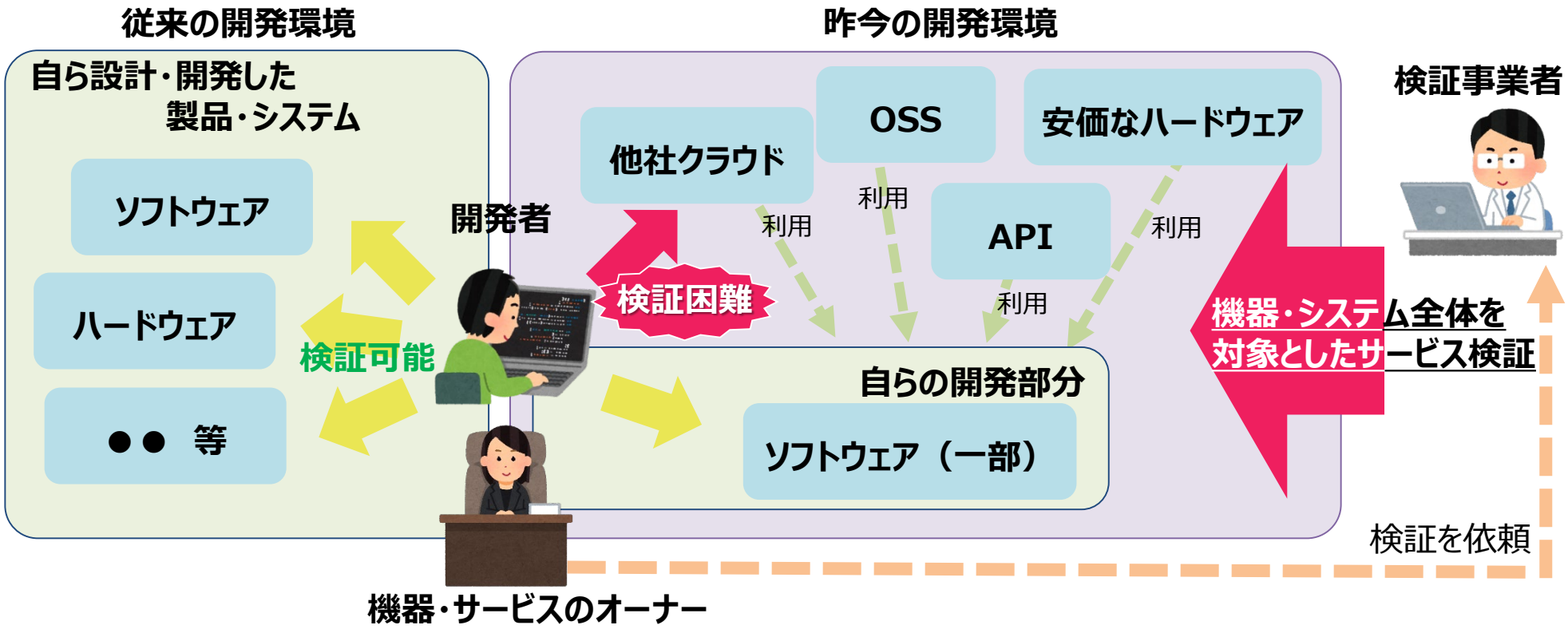
- 機器メーカが実施すべき事項や用意すべき情報等、意図した検証を依頼するために必要な事項を詳細に示す。
- 攻撃手法への対策例や、検証結果を踏まえたリスク評価等の対応方針を示す。
- 機器開発におけるセキュリティ検証の重要性を示す。

https://www.meti.go.jp/press/2021/04/20210419003/20210419003.html

赤

（参考）「開発のための投資」から「検証のための投資」へのシフト

- 近年では**クラウドやIoTなどの新しい技術の活用が進み、またオープンAPIやOSSが充実したことで、必要な“機能”を容易に調達してシステム構築できる環境**になっており、**開発者自身がシステム全体を把握・検証することが困難**になりつつある。
- こうした環境の変化で、**官民において第三者によるセキュリティ検証の必要性が増大**し、**検証ビジネスの需要が拡大し、産業として重要になっていく**と考えられる。



１．はじめに
～最近の攻撃事例と注意喚起

２．産学官の検討体制の構築
～産業サイバーセキュリティ研究会

３．サイバーセキュリティビジネスの創出
～エコシステムの構築　Proven in Japan（検証基盤）

（参考）その他のセキュリティビジネス創出に向けた取組
～情報セキュリティサービス審査登録制度、コラボレーションプラットフォーム

情報セキュリティサービス審査登録制度の概要

- **一定の技術・品質管理要件を定めた「情報セキュリティサービス基準」**を策定し、基準に適合するサービスのリストを2018年6月よりIPAが公開。

＜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分からない

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

審査を受けてリストに掲載

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

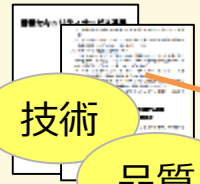
○情報セキュリティサービス基準適合サービスリスト（IPA）

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234サービスが掲載

- 情報セキュリティ監査（64サービス）
- 脆弱性診断（96サービス）
- デジタルフォレンジック（30サービス）
- セキュリティ監視・運用（44サービス）

2021年３月現在



○情報セキュリティサービス基準（METI）

上記４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

専門的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

（参考）登録サービス事業者の所在地の内訳

- **情報セキュリティ監査**（64サービス）　東京49、神奈川6、埼玉2、兵庫2、千葉1、新潟1、京都1、大阪1、広島1
- **脆弱性診断**（96サービス）　東京75、神奈川7、大阪3、兵庫3、新潟2、宮城1、茨城1、千葉1、大分1、福岡1、沖縄1
- **デジタルフォレンジック**（30サービス）　東京25、神奈川3、兵庫1、熊本1
- **セキュリティ監視・運用**（44サービス）　東京34、神奈川6、大阪1、兵庫1、福岡1、大分1

2020年度に実施したアンケート・ヒアリング結果のまとめ

制度の更なる改善を図るため、ユーザ・ベンダ双方への**本制度の活用状況・ニーズ調査**を実施した。

＜制度の認知度・効果＞

- ユーザー企業の半数超が本制度を認知。
- 登録メリットを感じる事業者が存在するほか、登録サービスの利用者による品質評価で「期待未満」が皆無であるなど、制度の目的が満たされていることが観察される。

＜セキュリティサービスの利用動向＞

- **ユーザー企業の約３割がセキュリティサービスを外部に委託**している実態。
- 外部委託における課題として、多くの企業が「サービスが自社の求めている条件を満たしているかどうかの判断ができない」「サービス品質が適切かどうか、使ってみるまで判断できない」と回答。

＜制度において改善すべき事項＞

- ユーザー企業からは登録サービス数の増加を求める意見が最多であるほか、**基準適合サービスリストの改善を求める声**（条件に見合った検索が出来るようリストの記載項目をもっと充実させて欲しい等）があった。
- **地域のベンダーはもっと存在しているはずなのに、登録数としては少ない**印象を受ける。

＜セキュリティサービスの普及方策への期待＞

- ベンダーの自己負担で営業活動で認知向上に取り組むには限界があり、**本制度の普及を通じてユーザーへの認知度向上を期待**する意見あり。

※ 全国のユーザー企業でサイバーセキュリティ対策関連業務に従事している方411名を対象にアンケート調査を実施。ユーザー（企業や自治体）、セキュリティサービスベンダー各15社程度を対象にヒアリング調査を実施。

基準適合サービスリストの改善（2021年2月）

- 制度ユーザーからの要望を踏まえ、利用者にとってより分かりやすいものにすべく、基準適合サービスリストを改善。（2021年2月1日公開）
- 官側の利用促進が必要との意見もあるところ、政府統一基準群等への引用も検討中。

ユーザーからの要望

- リストから条件に合った事業者を検索するのが不便である
- リストに掲載されているサービス名称からサービスの内容が把握できない
- 条件に見合った検索ができるよう、検索機能をもっと充実させるべき　等

サービスの概要欄を追加
（どのようなサービスで、どのような手法で行っているか等）

主な顧客の分野・業種欄を追加

事業者のHPへのリンクを追加

サービス提供地域欄を追加

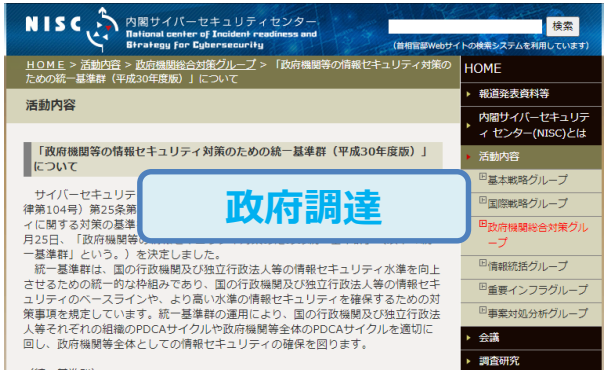
【基準適合サービスリスト（IPA公開）の改善】

サービス名称	事業者名称	事業者所在地	サービスの概要	主たる顧客対象の分野・業種	対象とする地域	登録年月日	有効期限	審査登録機関名
セコムプロフェッショナルサポート	セコムトラストシステムズ株式会社	東京都渋谷区神宮前一丁目5番1号 セコム本社ビル	主にPCのウイルス感染・不正アクセス・情報漏えい等のセキュリティ事案が発生した際の原因調査と早期復旧を目的としたサービスです。本サービスでは、デジタルフォレンジック技術を活用して対象データの保全・解析等を行います。2008年のサービス開始以来、2020年末までに480回のセキュリティ事案対応を行っています。情報セキュリティ担当者がいない中小企業への対応実績もあります。	建設業　化学　機械・電機・精密機器　医薬品・医療関連・化粧品　電気・ガス・熱供給・水道業　マスコミ・出版・印刷・広告　情報処理・ソフトウェア・ＳＩ　運輸・倉庫　商社・流通・卸売・小売業　銀行・証券・保険業　官公庁（宮公庁・自治体　等）　その他サービス業　旅行業　銀行・証券・保険業　商社・流通・卸売・小売業　鉄鋼・金属　機械・電機・精密機器　自動車・輸送機器　繊維・アパレル　職業紹介・人材派遣	日本全国	2020/12/20	2022/12/19	日本セキュリティ監査協会（JASA）
インシデントレスポンス	PwCコンサルティング合同会社	東京都 千代田区丸の内2-6-1	企業を脅かすサイバー活動に対応するべく、PwCは専門知識と経験を持つ専門家からなるサイバーセキュリティインシデント対応チームを有しています。PwCのグローバルネットワークを活用し、世界中でインシデント対応アドバイザリーデジタルフォレンジック、ステークホルダーマネジメントといった支援を行います。	公務（宮公庁・自治体　等）　その他サービス業　旅行業　銀行・証券・保険業　商社・流通・卸売・小売業　鉄鋼・金属　機械・電機・精密機器　自動車・輸送機器　繊維・アパレル　職業紹介・人材派遣	日本全国	2020/9/23	2022/9/22	日本セキュリティ監査協会（JASA）

有識者からの意見

- 政府調達で本制度が使われる等、官側の利用促進も図っていくべき　等

「政府機関等の情報セキュリティ対策のための統一基準群」等での引用も検討中。



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。

	開催日		参加人数(*)	テーマ
2018年	6月13日	第一回	179名（99名）	経済産業省の政策動向
		～		
2019年	1月25日	第六回	108名（48名）	サイバー・フィジカル・セキュリティ対策フレームワーク
	3月4日	第七回	114名（42名）	IoTの製造現場のセキュリティ対策
	4月23日	第八回	97名（51名）	サイバーセキュリティ経営、検証基盤
	6月12日	第九回	133名（34名）	データ利活用
	7月29日	第十回	112名（42名）	クラウド
	9月12日	第十一回	98名（42名）	経済産業省の来年度政策
	11月25日	第十二回	127名（49名）	中小企業
2020年	9月28日	第十三回	90名	課題解決に役立つ対策技術のご紹介
	10月30日	第十四回	91名	テレワークとセキュリティ
2021年	1月29日	第十五回	123名	中小企業との情報共有のあり方
	2月25日	第十六回	172名	クラウドシフトのセキュリティ

(*)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

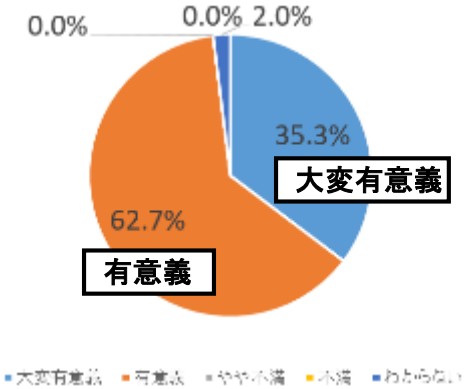
富田理事長(IPA)ご挨拶

三角審議官(経済産業省)ご挨拶

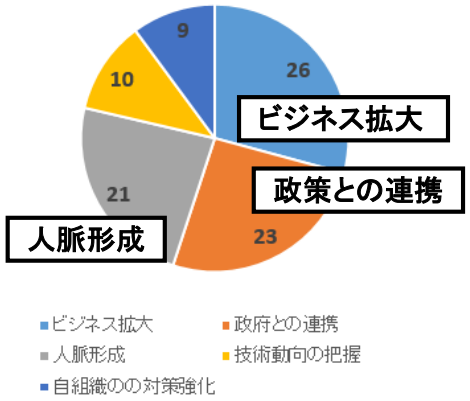
グループディスカッション(第二回)

（詳細はIPAのサイトを参照） https://www.ipa.go.jp/security/announce/collapla_index.html

Q.コラプラの満足度は？



Q.コラプラに参加して良かったことは？



※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


METI
Ministry of Economy, Trade and Industry