資料２

関係省庁の取組状況について

【金　融　庁】

資料２－１　金融業界横断的なサイバーセキュリティ演習
（Delta Wall Ⅴ）について

【総　務　省】

資料２－２　IoT・5G セキュリティ総合対策 2020 等について

【経済産業省】

資料２－３　サイバーセキュリティ強化運動の全体像について

金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅴ）について

金融分野のサイバーセキュリティを巡る状況

- 資金移動業者の決済サービスを通じた不正出金等のインシデントが、複数の金融機関で発生
- また、新型コロナウイルス感染症に便乗したサイバー攻撃やテレワーク環境を狙ったサイバー攻撃が発生している状況
- こうしたサイバー攻撃の脅威は、金融システムの安定に影響を及ぼしかねない大きなリスクとなっており、金融業界全体のインシデント対応能力の更なる向上が不可欠

これまでの演習の概要

- ✓ 過去４回演習を実施。2016年度は77先・延べ約900人、2017年度は101先・延べ約1,400人、2018年度は105先・延べ約1,400人、2019年度は121先・延べ約2,000人が参加
- ✓ 参加金融機関の多くが規程類の見直しを実施・予定しているほか、社内及び外部組織との情報連携の強化に関する対応を実施・予定しており、本演習を通じて対応態勢の改善が図られている。

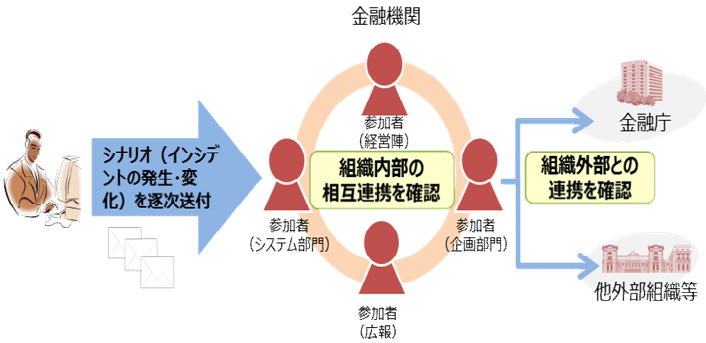
金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅴ）

- 2020年10月中旬、**金融庁主催による5回目の「金融業界横断的なサイバーセキュリティ演習」（Delta Wall Ⅴ（注））を実施し、約110先が参加。**
  最近の不正出金等においても重要性が認められた、**インシデント発生時の顧客対応や部門間及び組織外部との連携の実効性**を確認し、**業界全体のインシデント対応能力の底上げを図る。**　（注）Delta Wall: サイバーセキュリティ対策のカギとなる「自助」、「共助」、「公助」の３つの視点（Delta）＋防御（Wall）
- 昨年実施した演習の結果を踏まえ、銀行等については**今回新たに「インシデント対応能力のより一層の高度化を図ること」を目的に**、社内でのディスカッションを通じて**インシデント対応における社内エスカレーションから経営層の意思決定までの実効性を検証する演習**を実施
- テレワーク環境下でのインシデント対応能力の向上を図るため、**参加金融機関は実際のテレワーク環境下で演習に参加**

演習の特徴

- ✓ インシデント発生時における金融機関内外の情報連携に係る対応体制や手順の確認を目的とした演習
- ✓ 経営層や多くの関係部署（システム部門、広報、企画部門等）が参加できるよう、**自職場参加方式**で実施
- ✓ 民間の**専門家の知見や攻撃の実例分析等を参考**にしつつ、金融機関が陥りやすい弱点が浮き彫りとなり、**参加者が「気づき」を得る**ことができる内容
- ✓ 参加金融機関がPDCAサイクルを回しつつ、対応能力の向上を図れるよう、具体的な改善策や優良事例を示すなど、**事後評価に力点**
- ✓ 本演習の結果は、参加金融機関以外にも**業界全体にフィードバック**

演習スキーム



【演習シナリオの概要】

銀行等

（ブラインド方式のため非開示）

信金・信組等

- ✓ ホームページ異常による顧客影響が発生
- ✓ 社内端末のマルウェア感染とその拡大

証券・FX・生損保・資金移動業者・監査法人等

- ✓ 顧客情報の漏えいが発生
- ✓ 外部からのマルウェア侵入・社内感染

暗号資産交換業者

- ✓ 顧客資産の流出
- ✓ 社内システムへの不正侵入・外部への不正通信

IoT・5Gセキュリティ総合対策2020について

資料２－２

■ サイバーセキュリティタスクフォースにおけるこれまでの短期的・中長期的な観点の議論、「我が国のサイバーセキュリティ強化に向け速やかに取り組むべき事項 [緊急提言]」※１の内容、さらには新型コロナウイルス感染症への対応等を踏まえつつ、「IoT・5Gセキュリティ総合対策」※２について、必要な改定を行い、「IoT・5Gセキュリティ総合対策2020」として2020年７月に公表。

https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00126.html

● 改定に当たっての主要な政策課題

1 COVID-19 への対応を受けたセキュリティ対策の推進

① テレワークシステムのセキュリティに関するチェックリストの作成や相談対応体制の拡充など、特に中小企業を念頭においたテレワークセキュリティの確保のための実践的な対策を推進する。

② ネット上で業務・手続を完結可能とするため、電子署名やeシールなどのトラストサービスの制度化や普及促進を図るとともに、制度・手続・慣習の見直しを進める。

2 5G の本格開始に伴うセキュリティ対策の強化

① 5Gネットワークの脆弱性及び脅威の検証・分析のための手法や体制の確立

② 関係者間のリスク・脅威情報の共有の促進

③ 規制・振興両面でのセキュリティ対策の実装の促進など

セキュリティ・バイ・デザインの観点で推進

3 サイバー攻撃に対する電気通信事業者のアクティブな対策の実現

巧妙化・多様化するサイバー攻撃に対処するため、電気通信事業者における積極的なサイバーセキュリティ対策（C&Cサーバの能動的な検知や攻撃指令通信の遮断等）を迅速かつ効果的に実施可能とするため、通信の秘密の保護を図りつつ、一層のサイバーセキュリティを確保する方策について検討を行う。

4 我が国のサイバーセキュリティ情報の収集・分析能力の向上に向けた産学官連携の加速

我が国におけるセキュリティ製品・サービスの海外依存や慢性的な人材不足から脱却するため、サイバーセキュリティ情報を国内で収集・蓄積(生成)・提供するとともに、社会全体でサイバーセキュリティ人材を育成するための共通基盤を構築し、産学官連携の結節点とするための体制の構築を図る。

● IoT・5Gセキュリティ総合対策2020の枠組み

重点的に対応すべき情報通信サービス・ネットワークの個別分野等に関する具体的施策

- ✓ IoT、5G、クラウドサービス、スマートシティ、テレワークシステムのセキュリティ
- ✓ トラストサービスの制度化と普及促進　など

具体的施策間でも連携

連携　連携　連携

研究開発	人材育成 普及啓発	情報共有 情報開示
✓ 統合知的基盤 ✓ ハードウェア脆弱性 ✓ AI ✓ 暗号 など	✓ 人材育成基盤 ✓ サイバー演習 ✓ 地域の人材育成 など	✓ 情報共有基盤 ✓ 情報開示の促進 など

連携

国際連携

- ✓ ASEAN各国や欧米諸国等との連携
- ✓ 国際標準化　など

※１　2020年東京大会に向けた対処として短期的な観点から早急に取り組むべき事項を整理した結果を「我が国のサイバーセキュリティ強化に向け速やかに取り組むべき事項 [緊急提言]」として 2020年１月に公表。
※２　IoT・5G時代にふさわしいサイバーセキュリティ政策の在り方について検討した結果を「IoT・5Gセキュリティ総合対策」として2019年8月に公表。

テレワークセキュリティに関する手引き（チェックリスト）

- 総務省では従来より**「テレワークセキュリティガイドライン」**を策定し、セキュリティ対策の考え方を示している。
- 新型コロナウイルスの影響により、これまで未導入だった中小企業等においてもテレワークの導入が広まる中で、**実践的かつ具体的で分かりやすい内容**の資料が求められている。
  → テレワークにおける**最低限のセキュリティを確実に確保**してもらうための**手引き（チェックリスト）**を作成。

  【手引き(チェックリスト)の想定読者像】
  - ✓ セキュリティの**専任担当がいない**ような中小企業等における、**システム管理担当者**
  - ✓ 専門的なIT用語（例：VPN）は聞いたことがあるが、**仕組みを理解できていない**レベル

- 平行して実施した実態調査※の結果を踏まえて**年内に改定版（第２版）を作成・公表**予定。

※ 全国の３万事業者に対して本年８月に調査を実施。テレワークを導入している約1,500社から回答。

	平成30年４月策定 **ガイドラインの想定読者像**	**手引き（初版）の想定読者像**
対象属性	システム管理者のほか 経営層や利用者を幅広く対象	システム管理担当者
セキュリティ予算	外部委託コストは必要に 応じて捻出しうるレベル	外部委託コストの捻出は難しいレベル
セキュリティ推進体制	**専任**の担当・担当部門**が存在する**	**専任は存在しない**
セキュリティリテラシ	「適切に…」「レベルに応じて…」等の読者に解釈をゆだねるような**抽象的な要求に対して、対応内容を検討・判断し、対策を実行できる**	「適切に…」「レベルに応じて…」等の読者に解釈をゆだねるような**抽象的な要求だけでは、対応すべき内容がわからない**
ITリテラシ	VPN・フィルタリング・アンチウイルス等の基本的な**IT用語は仕組みとして理解している**レベル	VPN・フィルタリング・アンチウイルス等の基本的な**IT用語は聞いたことがあり、利用シーンがイメージできる**レベル
	システム設定作業は、基本的な内容であれば、**無理なく行うことができる**	**システム設定作業は**、基本的な内容であれば、**インターネット検索によって調べながら行うことができる**

手引きの構成とチェックリスト作成に当たっての考え方

- 手引きは、主に第１部・第２部から構成。
  - ✓ **第１部**で、本手引きの読者は自分の組織が採用する**テレワーク方式を確認・特定**
  - ✓ **第２部**では、第１部で特定した**テレワーク方式に対応するチェックリストを確認**
- チェックリストについては、セキュリティ確保を図る上で**優先対応**すべきものが**わかりやすいよう配慮**
  - ✓ セキュリティ**重要度**が**高**く、対策**実施**が**易**しいものは「◎」、**それ以外**を「○」として、優先順位をつけて整理
  - ✓ セキュリティ**重要度**が**低**いものや、対策**実施**が**難**しいものは、チェックリスト**対象外**として整理
- テレワークで**広く使われているソフトウェア**については、具体的な設定例として、**設定解説資料を作成**※
  - ※ 手引きの初版では、オンライン会議システムとして、Microsoft Teams、Cisco WebEx Meeting、Zoomの３製品分の解説資料を作成（第２版に向けて、順次拡張していく予定）

	第１部	第２部	参考
手引きの構成	1 はじめに 2 テレワーク方式の確認 3 テレワーク方式の解説 4 テレワーク環境で想定される脅威の解説	1 テレワーク方式ごとの**セキュリティ対策チェックリスト** 2 セキュリティ対策チェックリストの設定例一覧 →**補足文書として設定解説資料を用意** 3 テレワーク環境のセキュリティ対策と想定脅威一覧	• 用語集 • テレワークセキュリティに関する参考情報
読者の行動	• 自社に適合しているテレワーク方式の確認・特定 • 自社のテレワーク環境において想定される脅威の理解	• 第１部で特定したテレワーク方式に対応したチェックリストの特定 • 当該チェックリスト記載のセキュリティ対策実施 • 各セキュリティ対策に紐づく脅威の確認	(下記を必要に応じて実施) • 本書記載の用語の理解 • 参考文献等の閲覧 • 困った場合の問合せ先

テレワークのセキュリティに関する相談対応

- 総務省では従来から、**テレワークに関する幅広い相談**について、**テレワークマネージャー**相談事業により対応。
- 今般、中小企業等においてもテレワーク利用が急速に広まっており、適切かつ十分なセキュリティ対策がとられていない可能性もあることから、**セキュリティに関する不安**、具体的な**セキュリティ対策方法**、ルール作りや自社の実施状況の適切性の**コンサルティング**などを**相談できる窓口を開設**しています。
- **セキュリティの専門家**に対して、**無料**で気軽に相談可能ですので、是非ご利用を検討ください。

導入前のお悩み

私物のパソコンを従業員に
使わせても問題ないの？

これからテレワークの
仕組みを作りたいけど、
セキュリティは何をすればいいの？

アクセス制限が必要と聞いたけど、
何をどう設定すればいいの？

導入後のお悩み

とりあえずテレワークの
仕組みは作ったけれど、
セキュリティ的に大丈夫なの？

情報漏えいが心配だけど、
従業員への教育は必要？
何をすればいいの？

情報セキュリティのルールづくりで
考慮すべきポイントは何？

相談費用

無料

相談対応期間

2021年３月まで

相談対応方法

申込の後、相談者の希望に応じて、電話・メール・Web会議により対応します。

相談の申込先

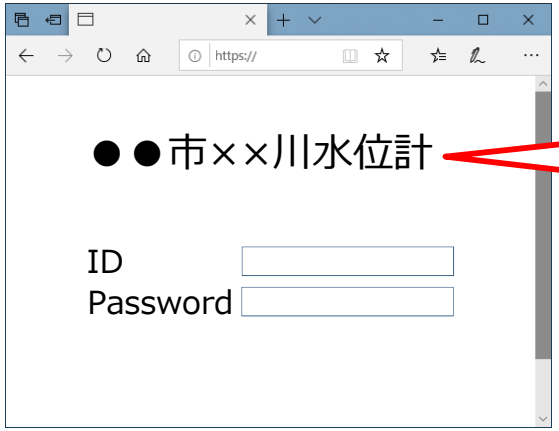
https://www.lac.co.jp/telework/security.html

※本事業は、総務省が株式会社ラックに委託し、実施しています。
セキュリティ専門企業の同社の専門家が相談対応に当たります。

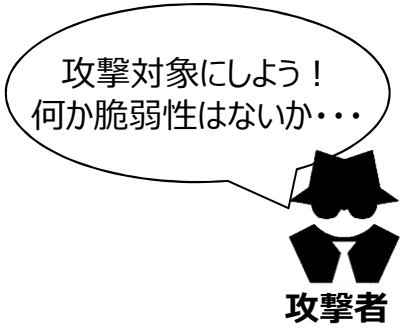
重要IoT機器のセキュリティ対策

- 重要インフラ等の社会的に影響を及ぼすリスクを伴った使用をしているIoT機器（**重要IoT機器**）について、**公開する必要のない情報が公開されている**など、攻撃を受けやすい**脆弱な状態**にあるものを**検出**する。
- 検出した重要IoT機器について、利用事業者に対して**設定状況等のヒアリング**を行った上で、脆弱な状態を解消するための**注意喚起**や**対策手法の提示**を行い、**対策の完了までのトレース**を行う。

脆弱な状態の例

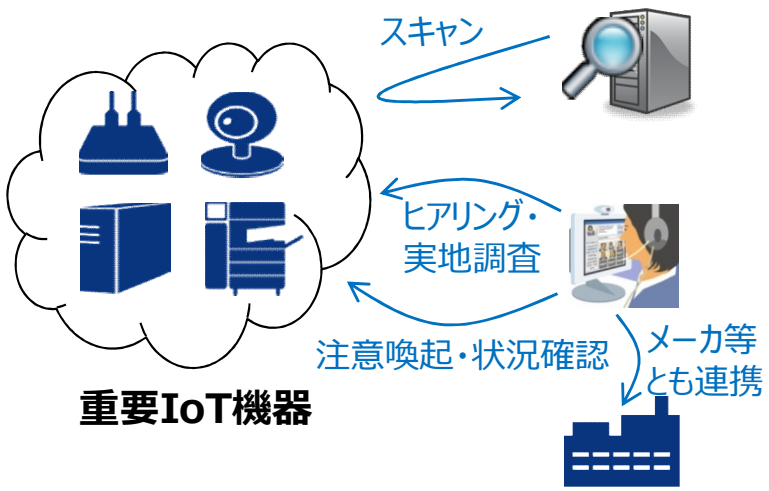


利用事業者や設置場所が推測可能な情報が表示されている



※脆弱な状態かどうかは、想定されるリスクをもとに利用事業者自身が判断する必要はあるが、利用事業者が認識していない場合もあるため、見つけた場合に 注意喚起 することは有効！

対策スキーム



重要IoT機器探索	重要IoT機器？ Web画面が見える？
利用者特定	画面の事業者名は？
利用環境調査	どのような用途か？ どのような設定・管理をしているか？ どのようなネットワーク環境で使っているか？
注意喚起実施	想定されるリスクはどのようなものか 対策にはどのようなものが有効か
対策状況確認	対策の実施に当たり問題はないか？

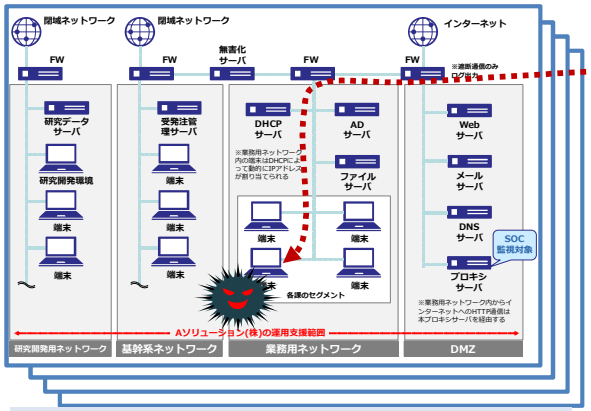
実践的サイバー防御演習（CYDER）

CYDER：CYber Defense Exercise with Recurrence

- 総務省は、情報通信研究機構(NICT)を通じ、**国の機関**、**指定法人**、**独立行政法人**、**地方公共団体**及び**重要インフラ事業者等**の情報システム担当者等を対象とした体験型の**実践的サイバー防御演習**(**CYDER**)を実施。
- 受講者は、**チーム単位で演習に参加。組織のネットワーク環境を模した大規模仮想LAN環境下で、実機の操作を伴って**サイバー攻撃によるインシデントの検知から対応、報告、回復までの**一連の対処方法を体験。**
- **全都道府県**において、年間**100回**・計**3,000名規模**で実施。
  ※平成29年度：年間100回・3,009名受講／平成30年度：年間107回・2,666名受講／令和元年度：年間105回・3,090名受講

演習のイメージ

NICTの有する技術的知見を活用し、サイバー攻撃に係る我が国固有の傾向等を徹底分析し、現実のサイバー攻撃事例を再現した**最新の演習シナリオ**をコースごとに用意。



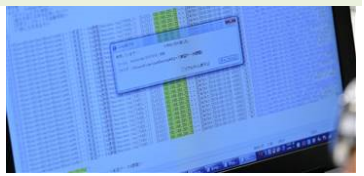
実際の**大規模LANを模した環境**を、**受講チームごと**に専用環境として**構築**

擬似攻撃者

NICT北陸StarBED技術センターに設置された大規模高性能サーバー群を活用

演習実施模様
専門の指導員による補助

機材・データを使用して**本番同様の作業**を実施



インシデント（事案）対処能力の向上

令和２年度の実施計画

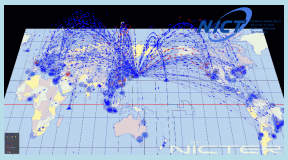
※このほか、令和３年１月頃から未受講の地方公共団体を対象としたオンライン演習を導入予定

コース	受講対象組織	対象者	開催地	開催回数	実施時期
Aコース（初級）	全組織共通	システムの運用担当者（システムの利用者レベルを含む）	４７都道府県	６５回	８月～翌年２月
B-1コース（中級）	地方公共団体	セキュリティ管理業務を主導する立場の者	全国１１地域	２０回	10月～翌年２月
B-2コース（中級）	国の機関等、重要インフラ事業者等		東京・大阪・名古屋・福岡	１５回	１月～翌年２月

サイバーセキュリティ統合知的・人材育成基盤

➢ サイバーセキュリティ情報を**国内で収集・蓄積・分析・提供**するとともに、**社会全体でサイバーセキュリティ人材を育成する**ための共通基盤をNICTに構築し、産学の結節点として開放することで、サイバーセキュリティ対応能力の向上を図る。

STARDUST
サイバー攻撃誘因基盤

NICTER

サイバー攻撃観測網

各種外部情報

CYDER
実践的サイバー防御演習

サイバーコロッセオ
オリパラ関係者向けサイバー演習

民間が有する各種演習教材

成果展開

成果展開

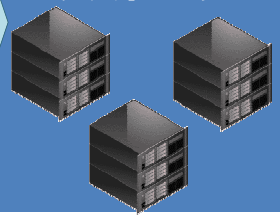
教材変換インタフェースの開発・標準化

サイバー攻撃分析環境

情報

大規模集約データベース

情報

セキュリティ機器テスト環境


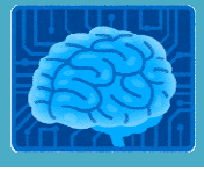
最新の攻撃情報（演習教材に反映）

相互補完

受講者の挙動（攻撃分析に活用）

演習教材提供環境

演習用大規模計算機環境
受講者挙動DB

AIを駆使した大規模横断分析＋付加価値の付与


根拠・背景等が
説明可能な国産セキュリティ情報

提供

政府機関・セキュリティ機関等

- マルウェア情報
- 指令サーバ情報
- 攻撃元IPアドレス情報
- 攻撃者/攻撃手法情報 等

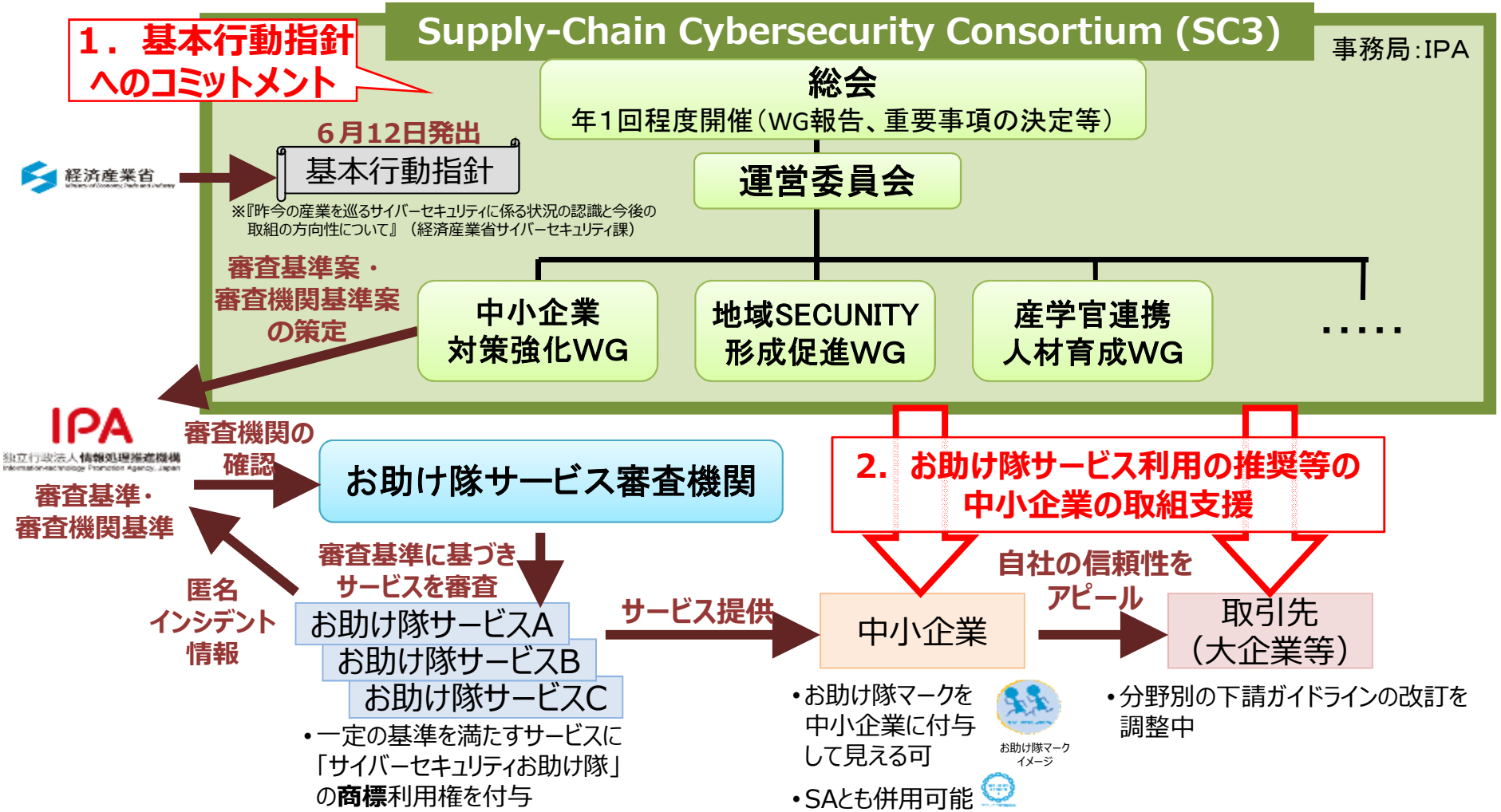
コミュニティ形成による連携

人材育成事業者 | 教育機関 | ICTベンダ

経済産業省

資料２－３

サイバーセキュリティ強化運動の全体像（コンソーシアムのイメージ）

- 大企業と中小企業がともにサイバーセキュリティ対策を推進するためのコンソーシアムを立ち上げ、基本行動指針の実践と中小企業・地域を含めたサプライチェーンのサイバーセキュリティ対策を産業界全体の活動として展開していく。

参加資格：コンソーシアムの取組方針や経産省の「基本行動指針」に賛同いただき、規約に同意いただける個人・法人