開会ごあいさつ

2025年2月

商務情報政策局サイバーセキュリティ課

サイバー攻撃の現状

- 企業等の情報を暗号化して金銭をゆすり取る「**ランサムウェア攻撃**」やセキュリティ対策に弱点のある取引先等が攻撃経路として狙われ、被害が拡大する「**サプライチェーンの弱点を悪用した攻撃**」により、甚大な影響が生じている。また国家支援型の攻撃集団等が特定の企業を執拗に狙う「**標的型攻撃**」も大きな課題。
- 社会のデジタル化は進展する一方、AI等のデジタル技術の発展や地政学情勢の不安定化の影響もあり、**サイバー攻撃は今後ますます増加するとともに高度化・複雑化していく**おそれがある。
- 相対的にセキュリティの弱い**中小企業の対策強化**を我が国全体で進める必要がある。

情報セキュリティ10大脅威 2024	
順　位	組織向け脅威
1位	ランサムウェアによる被害
2位	サプライチェーンの弱点を悪用した攻撃
3位	内部不正による情報漏えい等の被害
4位	標的型攻撃による機密情報の窃取
5位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
6位	不注意による情報漏えい等の被害
7位	脆弱性対策情報の公開に伴う悪用増加
8位	ビジネスメール詐欺による金銭被害
9位	テレワーク等のニューノーマルな働き方を狙った攻撃
10位	犯罪のビジネス化（アンダーグラウンドサービス）

中小企業の被害が全体の約5割を占める

相対的にセキュリティ対策の弱い中小企業を起点に、大企業含むサプライチェーンを共有する企業を攻撃

<出典：(独)情報処理推進機構(IPA)、2024.1.24>

政府全体における検討と経済産業省における取組

- 内閣官房では国家安全保障戦略（2022年12月決定）に基づき、**能動的サイバー防御の導入に向けた制度整備の検討**を実施中。11月末に**有識者会議の提言を公表**し、必要な法制度の整備を準備中。
- 経済産業省においては、NISC等の関係省庁と連携しつつ、**産業界のサイバーセキュリティ強化に向けた各種施策を企画・実行中。**

サイバー安全保障分野での対応能力の向上に向けた提言

Ⅰ 官民連携の強化

➢ 基幹インフラ事業者がサイバー攻撃を受けた場合等の政府への情報共有や、政府から民間事業者等への対処に必要な情報の提供、情報共有会議の新設等

Ⅱ 通信情報の利用

➢ 一定の条件下での通信情報の利用を検討。特に国内の通信の分析が必要。独立機関によるプロセスの監視。コミュニケーションの本質的内容に関わる情報は分析せず。

Ⅲ アクセス・無害化

➢ サイバー攻撃元のコンピュータにアクセス・無害化等できる権限を整備。まずは警察が実施し、特別の必要がある場合に自衛隊と共同で対処。

Ⅳ 横断的課題

➢ NISCの発展的改組、重要インフラのレジリエンス強化、人材の定義の可視化、国産技術の活用推進、中小企業対策　等

経済産業省における主な取組

サプライチェーン全体での対策強化

- 経営者向けのガイドライン等の各種ガイドラインの公表
- 中小企業向けの支援（サイバーセキュリティお助け隊サービス等）
- **サプライチェーン企業のセキュリティ対策レベル可視化の仕組みの検討**

国際連携を意識した認証・評価制度

- 一定のセキュリティ基準を満たす**IoT製品を認証する制度の構築**・国際調和
- ソフトウェアのセキュリティ向上のための**ソフトウェア部品構成表（SBOM ）の活用促進**（手引き公表等）・国際連携
  ⇒上記制度は**政府調達等の要件**に

官民の状況把握力・対処能力向上

- JPCERTによる事案対処支援
- IPAをハブとした**サイバー情勢分析能力強化と専門チーム（J-CRAT）の強化**

研究開発・産業振興

- **サイバー防御等のための研究開発プロジェクトの実施（300億円／5年間）**
- セキュリティ産業の振興と高度人材の育成・確保に向けた検討

工場システムにおけるセキュリティ対策ガイドライン

- 2022年11月に本編、 2024年4月にスマート化を進める上でのポイント（別冊）を公表。

ガイドラインの背景・目的

● 本編　★ 別冊

- 業界団体や個社が自ら対策を企画・実行するに当たり、参照すべき考え方やステップを示した「手引き」 →**工場セキュリティの底上げが目的。**
- ★ 工場がサイバー空間に密接につながっていく世界、サプライチェーンにおいて取引先に対するセキュリティ対策が要請されている →**先進的な企業が臆することなく工場のスマート化を進め、工場の価値創造を促進する。**

想定する読者の方

- IT関係部門、生産関係部門、監査部門
- 戦略マネジメント部門（経営企画等）
- ★ リスク管理部門、DX担当部門
- 機器システム提供ベンダ、機器メーカ
  （サプライチェーンを構成する調達先を含む）

※想定読者が経営層（CTO、CIO、CISO）をはじめとした意思決定層と適切なコミュニケーションを行うことが重要。

対策に取り組む効果・読み方

- **工場のBC／SQDCの価値がサイバー攻撃により毀損されることを防止**し、セキュリティが担保されることでIoT化や自動化が進み、多くの工場から新たな付加価値が生み出されていくことを期待。
- ★ **スマート工場の概要を示すとともに、ガイドライン本編3章に示した各ステップの対策におけるスマート化を進めるに当たっての留意点や具体例を提示。**

セキュリティ対策企画・導入の進め方

ステップ1　内外要件（経営層の取組や法令等）や業務、保護対象等の整理

- **ステップ1-1**　セキュリティ対策検討・企画に必要な要件の整理
  (1)経営目標等の整理
  (2)外部要件の整理
  (3)内部要件／状況の把握
- **ステップ1-2**　業務の整理
  ★ スマート化の目的に照らした業務の広がり
  ★ 業務の広がりに応じたシステム範囲の拡大
- **ステップ1-3**　業務の重要度の設定
- **ステップ1-4**　保護対象の整理
- **ステップ1-5**　保護対象の重要度の設定
- **ステップ1-6**　ゾーンの整理とゾーンと業務、保護対象の結びつけ
- **ステップ1-7**　ゾーンと、セキュリティ脅威の影響の整理
  ★ スマート化におけるゾーンごとのセキュリティ要件の考え方
  ★ スマート化により考慮すべき脅威と影響の考え方

ステップ2　セキュリティ対策の立案

- **ステップ2-1**　セキュリティ対策方針の策定
- **ステップ2-2**
  想定脅威に対するセキュリティ対策の対応づけ

(1)システム構成面での対策

①ネットワークにおけるセキュリティ対策
  ★ ネットワーク接続における対策
  ★ クラウド利用時の対策
②機器におけるセキュリティ対策
  ★ 汎用品のセキュリティ対策
③業務プログラム・利用サービスにおけるセキュリティ対策
  ★ データ活用・連携における対策

(2)物理面での対策

①建屋にかかわる対策、②電源／電気設備にかかわる対策、③環境(空調など)にかかわる対策、④水道設備にかかわる対策、⑤機器にかかわる対策、⑥物理アクセス制御にかかわる対策

ステップ3　セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施）

- **ライフサイクルとサプライチェーンを考慮した対策**

(1)ライフサイクルでの対策

①運用・管理面のセキュリティ対策
  A) サイバー攻撃の早期認識と対処(OODAプロセス)
  B) セキュリティ対策管理(ID/PW管理、機器の設定変更など)
  C) 情報共有
  ★ スマート化におけるサイバー攻撃の早期認識と対処プロセスの実現
②維持・改善面のセキュリティ対策
  ・セキュリティ対策状況と効果の確認・評価、環境変化に関する情報収集、対策の見直し・更新
  ・組織　・人材のスキル向上（教育、模擬訓練等）
  ★ スマート化においてPDCAサイクルを実現する上で有効な考え方

(2) サプライチェーン対策

・取引先や調達先に対するセキュリティ対策の要請、対策状況の確認
★ クラウド/汎用品/ソフトウェア 利用時の留意事項

事業や環境、技術の変化に応じて各ステップについて不断の見直しを行いながらステップのサイクルを回す

※「ゾーン」とは、業務の重要度が同等であり、同等の水準のセキュリティ対策が求められる領域

サイバーセキュリティ政策に関する国際的な動向

- **セキュア・バイ・デザイン**＊1**の概念が国際的に支持を集める**など、企業は自社をサイバー攻撃から守ることのみならず、**自社が提供する製品のサイバーセキュリティ対策についても問われる時代に**なりつつある。

＊1 IT 製品（特にソフトウェア）が、設計段階から安全性を確保されていることを指す。

セキュア・バイ・デザインの要請

サイバーレジリエンス法案（Cyber Resilience Act）

- 2023年4月に**米CISAが一部有志国と共にセキュアバイデザイン、セキュアバイデフォルトの実践に向けた推奨事項をまとめたガイダンスを作成**。
- ソフトウェア開発者に対し、安全な製品を出荷するために必要な措置を講じるよう促した（法的拘束力なし）。同年10月に本文書が改訂され、日本含む13か国が共同署名。

PSTI法（Product Security and Telecommunication Infrastructure Act）

- **消費者向けIoT機器の製造者に対し**、デフォルトパスワードを使用しない等の**最低セキュリティ基準への自己適合宣言を義務化**。
- 2022年12月に国王裁可し、下位法制定を経て**2024年4月29日より施行予定**。

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、**①セキュリティ特性要件に従った**上市前の設計製造**、② **上市後に積極的に悪用された脆弱性、インシデント**について**認識後24時間以内の早期警告通知**、**72時間以内の通知をCSIRTに報告すること等を義務付け。**
- 2023年11月に暫定合意。**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。**

（出典）各種公開情報に基づき経済産業省作成

IoT製品に対するセキュリティ適合性評価制度の概要

- 2022年11月より検討会(※1)を開催し、2024年3～4月のパブコメを経て、8月に制度構築方針を公表。**9月30日にIPAから「JC-STAR」という制度名にて制度開始の案内**(※2)を実施。
- **★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。**米欧等の諸外国との制度調和**を図るため議論中。

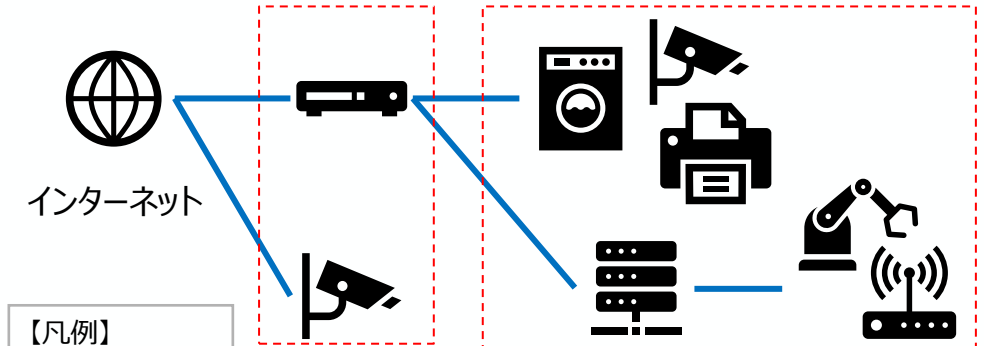
制度名称・ロゴ・ラベル

セキュリティ要件適合評価
及びラベリング制度
JC-STAR
(Labeling Scheme based on
Japan Cyber-Security Technical
Assessment Requirements)

JC-STAR

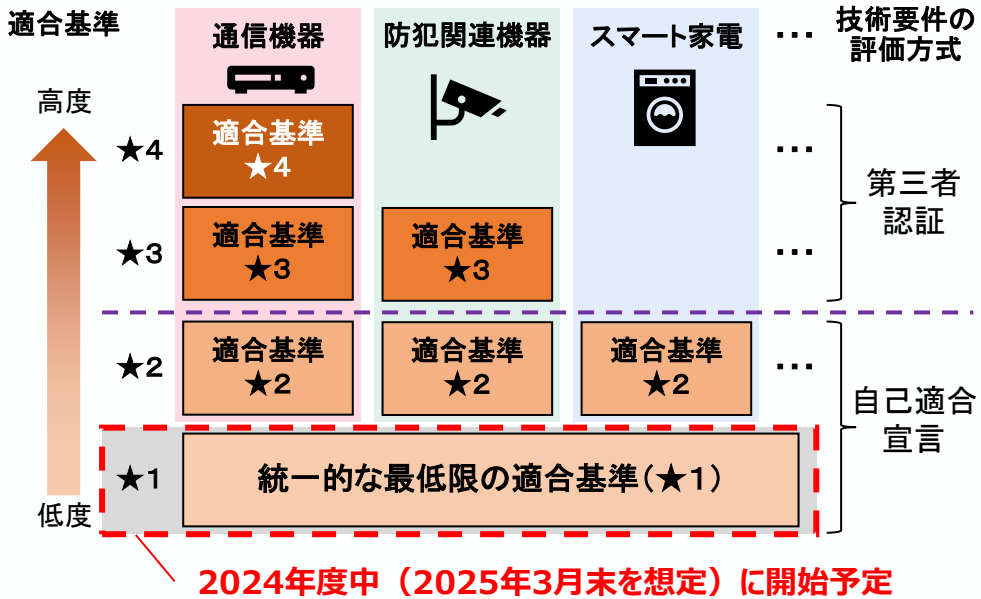
JAPAN CYBERSECURITY LABEL
ジャパン・サイバーセキュリティ・ラベル
★★★★
JC-STAR
Registered ID: 0123456789012345
Information-technology Promotion Agency, JAPAN (IPA)

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。

制度の概要（イメージ）

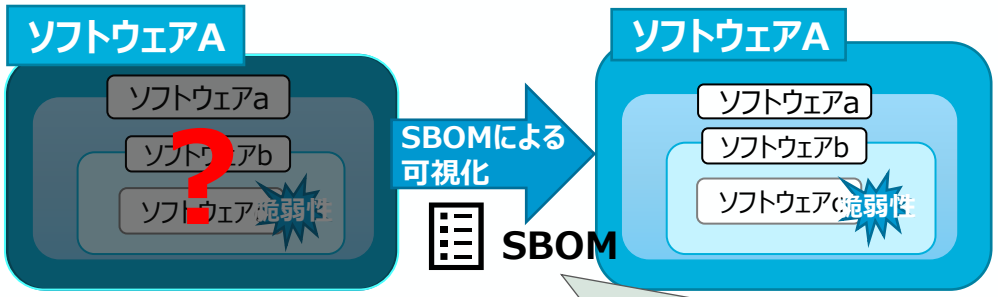


(※1)経済産業省「ワーキンググループ3（IoT製品に対するセキュリティ適合性評価制度構築に向けた検討会）」https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/index.html
(※2)IPA「IoT製品に対するセキュリティ要件適合評価・ラベリング制度を開始します」https://www.ipa.go.jp/pressrelease/2024/press20240930.html

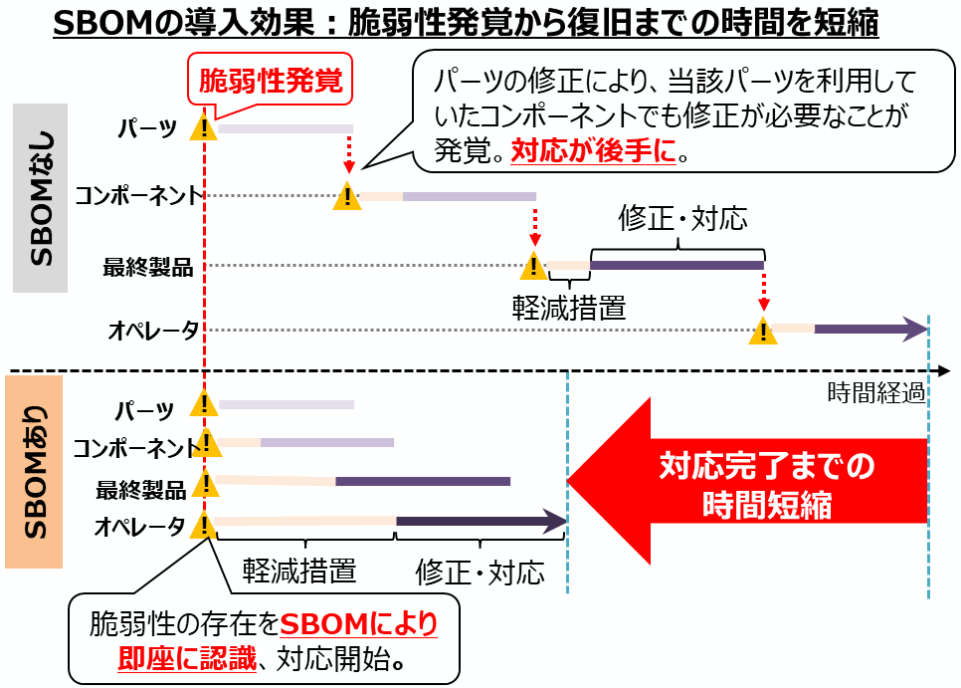
ソフトウェア・セキュリティ確保手段としてのSBOM

- SBOM （Software Bill of Materials）とは、**ソフトウェアの部品構成表**のこと。
- SBOMにより脆弱性情報の即時の特定が可能である一方、その作成効果やコストなどの課題が存在するため、実証による検証を実施。
- 2023年7月、SBOMに関する基本的な情報や導入に向けた実施事項のポイントを示した**「ソフトウェア管理に向けたSBOMの導入手引き」を公表。2024年８月に改訂版を公表。**

＜SBOMイメージ＞



サプライヤ名	コンポーネント名	バージョン	製品URLなど	…
A会社	ソフトウェアA	Ver1.0	……	…
A会社	|…ソフトウェアa	Ver2.1	……	…
B会社	|…ソフトウェアb	Ver5.3	……	…
C会社	|…ソフトウェアc	Ver1.2	……	…

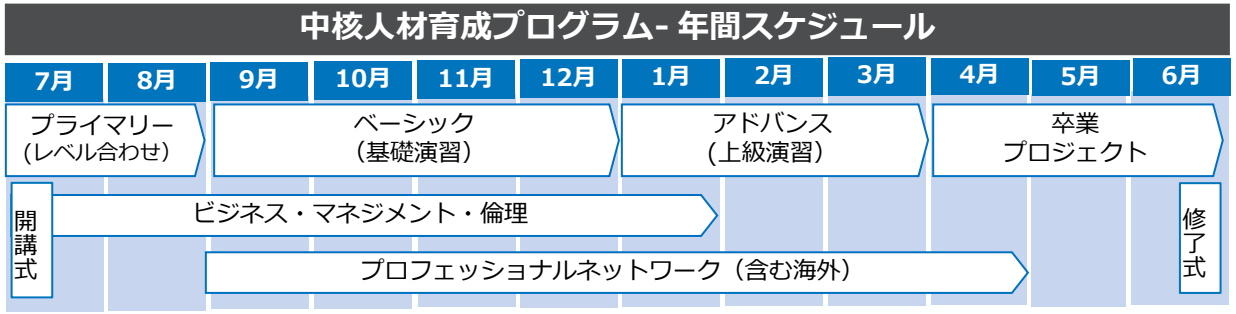


IPA産業サイバーセキュリティセンター（ICSCoE） ※2017年4月設置

- 社会インフラ・産業基盤における防護力の強化のため、OT(制御技術）とIT（情報技術）の知見を結集させた**世界レベルのサイバーセキュリティ対策の中核拠点**として、IPA内に発足。
- ICSCoEでは世界的にも限られている、制御系セキュリティにも精通する講師を招き、テクノロジー、マネジメント、ビジネス分野を総合的に学ぶ１年の集中トレーニング等を実施。

□　１年を通じた集中トレーニング

□　電力、石油、ガス、化学、自動車、鉄道分野等の企業から1年間派遣
（第1期：76人、第2期：83人、第3期：69人、第4期：46人、第5期：48人、第6期：48人、第7期：65人、第８期：57人）



- **IT系・制御系に精通した専門人材の育成**
- **模擬プラントを用いた対策立案**
- **実際の制御システムの安全性・信頼性検証等**
- **攻撃情報の調査・分析**

現場を指揮・指導するリーダーを育成

□　米・英・仏等の海外とも協調したトレーニングを実施

➢ DHSが開催する高度なサイバーセキュリティトレーニングである301演習への参加

➢ 政府機関、産業界等のセキュリティ専門家との意見交換や研究機関の施設見学等を実施

など

（参考）中核人材育成プログラムの成果と修了者の活動

- 中核人材育成プログラム受講者は、 1年間のプログラムで学んだ技術や人脈を業界の課題に当てはめていくことを主眼に、**プログラムの最後にチーム別の卒業プロジェクトに取り組む。**
- 修了者の知見をアップデートし、また、その知見やノウハウを産業界や社会へ還元していくため、**業種横断の修了者コミュニティ「叶会」を運営。**経済産業省やＩＰＡの取組に貢献。

最近の卒業プロジェクトの成果物

【第６期生　2023年８月公開】（一部紹介）

➢ **セキュリティ投資を得る方法**

セキュリティをネガティブに考える「コスト」としてではなく、自発的に行う「投資」にしていくべく、セキュリティ投資を得ている方々にヒアリングし、セキュリティ投資を得る方法を作成

➢ **攻撃者視点の獲得を目的としたボードゲーム：Cyber Attacker Placement**

サイバー攻撃の種類や、セキュリティ投資の重要性を学ぶことができる、ボードゲームを作成。

修了者コミュニティ　叶会（かなえかい）

【目的】
- 卒業後も知見をアップデート
- 卒業年次・業種を超えた人脈形成
- 修了者の知見の社会還元

【主な活動】
- 年１回年次総会（11月）で最新動向と修了者の近況の活躍を発表。
- サイバーセキュリティ情報提供活動：情報共有ツール「SIGNAL」を使い、ICSCoEが入手した脆弱性情報等を修了者に提供。
- 東京以外の地域（関西・中京等）でも修了者がコミュニティを形成、各地でセミナー等を開催、またセキュリティ対応等のノウハウをシェア。
- 商工会や地銀と連携、会報や業界紙にセキュリティの啓発記事を掲載。

●修了者の技術や知見の活用：「ビル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」作成への貢献

中核人材育成プログラムでビルが直面するセキュリティの課題と解決手法を学んだ受講者が、有志で経済産業省のビルSWGに参加。カリキュラムのアウトプットとして、経済産業省が2019年6月にリリースした「ビル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」をより分かりやすく理解できる“解説書”を作成するとともに、ビル関係者向けの脆弱性情報やその解説の配信にも協力。

（出典）IPA「中核人材育成プログラム 卒業プロジェクト」https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/index.html

インド太平洋地域向け産業制御システム・サイバーセキュリティ演習

- 経済産業省とIPA産業サイバーセキュリティセンター(ICSCoE)が、**米国・EU政府等と連携し、毎年開催するインド太平洋地域向けの1週間の研修プログラム**。これまで2018年度より毎年開催。
- 本演習では、**インド太平洋地域の重要インフラ事業者、製造業者等のICSセキュリティの向上を目的**に、**産業用制御システム（ICS）のサイバーセキュリティに焦点**を当て、IPA産業サイバーセキュリティセンターの施設を使用した**ハンズオン演習**や、**日米欧専門家による講演**、**参加者間のネットワーキング**を実施。

2024年演習の概要

- **日時**：2024年11月12日～15日
- **場所**：IPA文京キャンパス、IPA秋葉原キャンパス、EU代表部
- **主催**：経済産業省、IPA産業サイバーセキュリティセンター、米国政府（国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁、国務省）及びEU政府（通信ネットワーク・コンテンツ・技術総局）
- **参加者**：ASEAN加盟国、インド、バングラデシュ、スリランカ、モンゴル、台湾の重要インフラ事業者、製造業者、ナショナルCSIRT、政府機関等

ハンズオン演習

日米欧専門家による講演

インド太平洋地域参加者間のネットワーキング

METI
Ministry of Economy, Trade and Industry

経済産業省のサイバーセキュリティ政策ウェブページはこちら⇒
https://www.meti.go.jp/policy/netsecurity/index.html