資料３

関係省庁の取組状況について

【総　務　省】

資料３－１　総務省におけるサイバーセキュリティ施策の
取組状況について

【経済産業省】

資料３－２　経済産業省におけるサイバーセキュリティ施策の
取組状況について

資料３－１

総務省におけるサイバーセキュリティ施策の取組状況について

2022年1月

総務省サイバーセキュリティ統括官室

（1）実践的サイバー防御演習（CYDER）

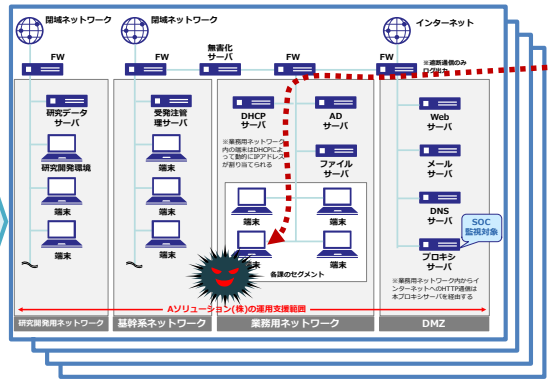
CYDER：CYber Defense Exercise with Recurrence

- 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。 参加申込 → https://cyder.nict.go.jp
  ※2017年度：100回・3,009名／2018年度：107回・2,666名／2019年度：105回・3,090名／2020年度：106回・2,648名

演習のイメージ

我が国唯一の情報通信に関する公的研究機関である**NICTが有する最新のサイバー攻撃情報を活用**し、実際に起こりうるサイバー攻撃事例を再現した**最新の演習シナリオ**を用意。

北陸StarBED技術センターの大規模高性能サーバ群を活用



擬似攻撃者

企業・自治体の**社内LANや端末を再現**した環境で演習を実施

受講チームごとに独立した演習環境を**構築**

演習模様 **専門指導員**による補助

チーム内での議論を通じた相互理解

本番同様のデータを使用した演習

インシデント（事案）対処能力の向上

令和３年度の実施計画

コース名	演習方法	レベル	受講想定者（習得内容）	受講想定組織	開催地	開催回数	実施時期
A	集合演習	初級	システムに携わり始めた者 (事案発生時の対応の流れ)	全組織共通	４７都道府県	６９回	７月～翌年２月
B-1		中級	システム管理者・運用者 (主体的な事案対応・ｾｷｭﾘﾃｨ管理)	地方公共団体	全国１１地域	２１回	10月～翌年２月
B-2				地方公共団体以外	東京・大阪・名古屋・福岡	１３回	翌年１月～２月
C		準上級	セキュリティ専門担当者 (高度なセキュリティ技術)	全組織共通	東京	３回	翌年１月～２月
オンラインA	ｵﾝﾗｲﾝ演習	初級	システムに携わり始めた者 (事案発生時の対応の流れ)	全組織共通	（受講者職場等）	随時	11月～翌年３月 （６～８月に試験提供）

令和３年度から**新規**開設

（2）電気通信事業者による積極的セキュリティ対策

➢ 大規模化・巧妙化・複雑化するサイバー攻撃・脅威に、電気通信事業者が積極的に対処できるようにするため、フロー情報(注1)の分析を通じて、サイバー攻撃の指令元であるC&Cサーバ(注2)を検知する技術の実証等を行う。

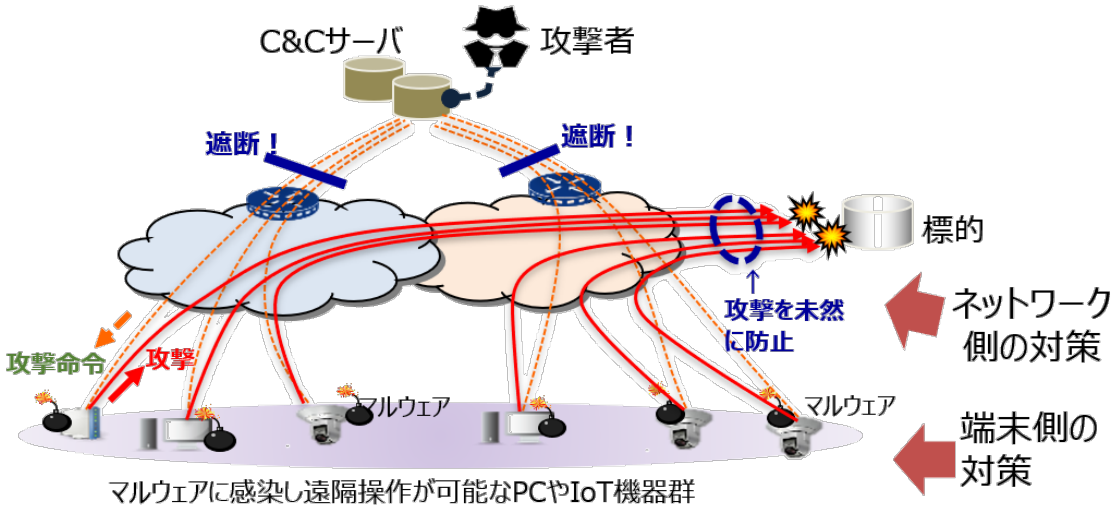
（1）通信の秘密に係る法的整理

有識者による研究会において、電気通信事業者における、インターネット利用者のトラヒックのうち必要最小限の範囲で収集するフロー情報の統計的・相関的な分析によるC&Cサーバである可能性が高い機器の検知について、通信の秘密に係る法的整理を実施。

※「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」（座長：鎮目征樹学習院大学法学部教授）の第四次とりまとめ（令和3年11月24日公表）において、正当業務行為（通信の秘密の侵害に該当しない）として整理。

（2）実証事業（令和3年度補正予算）　※「サイバー攻撃インフラ検知等の積極的セキュリティ対策総合実証」（18.0億円）

令和3年度補正予算により、電気通信事業者におけるフロー情報分析によるC&Cサーバ検知技術の有効性の検証や、事業者間の共有に当たっての運用面の課題整理のための実証事業を推進。



注１　フロー情報
　通信トラフィックに係るデータのうち、IPアドレス及びポート番号等のヘッダ情報並びにルータでヘッダ情報を抽出する際に付与されるタイムスタンプ等の情報（通信の内容は含まない）

注２　C&Cサーバ
　Command and Controlサーバの略で、外部から侵入して乗っ取ったコンピュータを多数利用したサイバー攻撃において、コンピュータ群に対して攻撃者から指令を送り、制御を行うサーバコンピュータのこと

（3）電気通信事業ガバナンス検討会（概要）

1．背景・目的

- **「デジタル社会」の実現**のためには、その中枢基盤として、サイバー空間とフィジカル空間を繋ぐ神経網である**通信サービス・ネットワークが安心・安全で信頼され、継続的・安定的かつ確実に提供されることが不可欠**。
- 最近、通信サービス・ネットワークを司る電気通信事業者において、利用者の個人情報や通信の秘密の漏えい事案が発生し、海外の委託先等を通じ、これらのデータにアクセス可能な状態にあることに関する**リスク等が顕在化**。
- 更に、電気通信事業者に対するサイバー攻撃により、通信サービスの提供の停止に至る事案や、通信設備に関するデータが外部に漏えいした恐れのある事案など、サイバー攻撃の**リスク等が深刻化**。
- デジタル時代における安心・安全で信頼できる通信サービス・ネットワークの確保を図るため、**電気通信事業者における**サイバーセキュリティ対策と**データの取扱い等に係るガバナンス確保の在り方を検証し、今後の対策を検討**。

2．主な検討事項

① 電気通信事業者におけるサイバーセキュリティ対策とデータの取扱い等に係るガバナンス確保の今後の在り方

② 上記①を踏まえた、政策的な対応の在り方

③ その他

3．体制

- データ、サイバーセキュリティ及びガバナンスに関する有識者から構成される検討会（座長：大橋教授）を設置。
- 構成員及びオブザーバーは右のとおり。

4．開催状況

- 令和3年5月12日に第1回会合を開催し、令和4年1月14日までに16回の会合を開催。**報告書案について、パブコメを実施中（1月15日～2月4日）**

大橋　弘	東京大学公共政策大学院院長
相田　仁	東京大学大学院工学系研究科教授
石井　夏生利	中央大学国際情報学部教授
上沼　紫野	虎ノ門南法律事務所弁護士
後藤　厚宏	情報セキュリティ大学院大学学長
中尾　康二	（一社）ICT-ISAC顧問 （国研）NICTサイバーセキュリティ研究所主管研究員
中村　修	慶應義塾大学環境情報学部教授
古谷　由紀子	（公社）日本消費生活アドバイザー・コンサルタント・相談員協会監事
森　亮二	英知法律事務所弁護士
山本　龍彦	慶應義塾大学大学院法務研究科教授

※　内閣官房国家安全保障局、デジタル庁、NISC、個人情報保護委員会事務局がオブザーバー参加

（3）電気通信事業ガバナンス検討会（報告書案）

- **利用者が安心して利用できる電気通信サービスの提供を確保し通信の信頼性を保持する観点**から、**①電気通信事業に係る情報の漏えい・不適正な取扱い等に対するリスク対策**や、**②ネットワークの多様化等を踏まえた電気通信サービスの停止に対するリスク対策**を行っていくことが必要。
- あわせて、リスク対策を講じていく際には、**③情報の適正な取扱いや電気通信サービス提供等に関する利用者への情報提供**が重要な観点となることに留意が必要。

① 電気通信事業に係る情報の漏えい・不適正な取扱い等に対するリスク対策

- ✓ 大量の情報を取得・管理等する者による電気通信事業に係る情報の漏えい・不適正な取扱い等のリスクに対応するため、利用者情報の適正な取扱いを促進するための規律を措置。
- ✓ 利用者の情報が外部送信される際、電気通信事業を営む者を対象として、利用者に確認の機会を適切な方法で与える規律を措置。

② ネットワークの多様化等を踏まえた電気通信サービスの停止に対するリスク対策

- ✓ 電気通信設備の損壊・故障対策等の適用対象について、仮想化技術等の進展を踏まえた見直しを実施。
- ✓ ISP間の情報共有や分析をサイバー攻撃の発生前にも実施できるようにするための環境を整備。
- ✓ 電気通信事故等の未然防止や被害軽減に向けて、重大事故等のおそれのある事態の報告制度を措置。

③情報の適正な取扱いや通信サービスの提供等に関する利用者等への情報提供

- ✓ 平常時から、情報の適正な取扱いや通信サービスの提供に関する情報、情報の漏えい・不適正な取扱い等や事故が生じた際の対処方策等について利用者に理解しやすい形での周知広報に努める。
- ✓ 非常時にも、適時に適切な方法で情報提供を行い、利用者が適切な対応ができるような方策を検討。

資料３－２

経済産業省における
サイバーセキュリティ施策の取組状況について

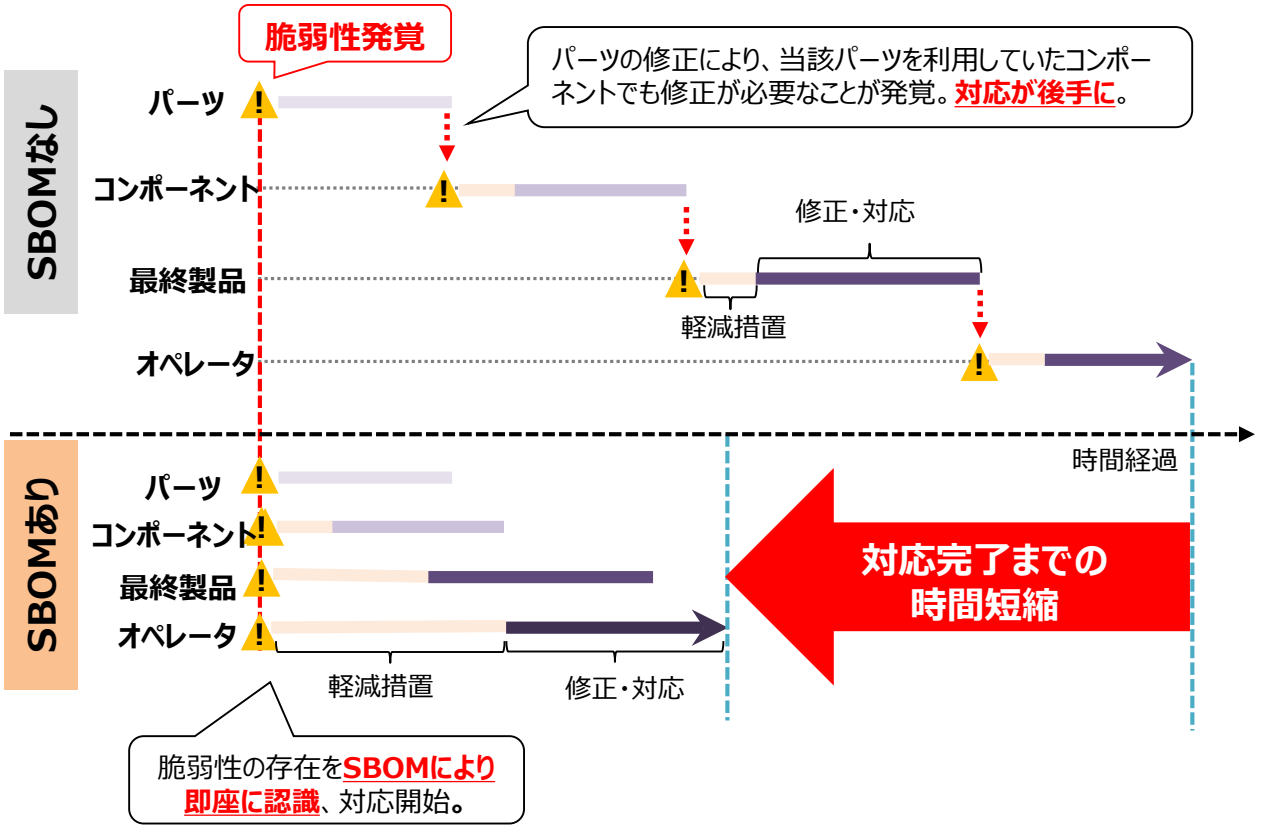
2022年1月

経済産業省サイバーセキュリティ課

SBOMに係る取組の進展

- 米国NTIAが2018年から主導するSoftware Component Transparencyでは、ヘルスケア分野における実証事業（PoC）に続いて、自動車分野・電力分野にも取組が拡大。
- 米国では、2021年5月に発令された大統領令においてもSBOM提供について言及されており、今後、政府調達要件として整備が進むものと想定。
- 米国の動向も踏まえ、日本においても、業界構造や商習慣を考慮しつつSBOMの導入効果やコスト等を明らかにすべく、SBOM活用に向けた実証事業を実施。

SBOMの導入効果：脆弱性発覚から復旧までの時間を短縮



米国NTIAにおけるSBOMのPoC

ヘルスケア分野（病院、医療機器）

病院、医療機器メーカー、ベンダーが参加。2回のPoCを経てSBOM活用の手法、課題等を公開。4/29のNITA会合にて、医療機器メーカーにおけるSBOM活用に向けたガイドラインを取りまとめる予定と発表。

自動車産業分野

Auto-ISACを中心としたサプライヤー中心のプロジェクト。ヘルスケア分野のPoCを参考にしつつ、自動車産業分野でのSBOMの普及促進を目的として、SBOM構築方法や得られた教訓・課題等を確認する。12ヶ月ほどかけてサプライヤー向けの推奨事項がとりまとめられる予定。

電力分野

INL主導で、電力会社、電力機器ベンダー、ソフトウェアベンダー、電気協会等が参加。米国エネルギー省からもプレゼンターとして参加。2021年中のPoC実施完了に向け、目的、実施内容、スケジュールに関する議論を経て、9/1からPoCを実施中。

SBOM導入・活用の障害・課題に関する整理

- SBOM活用による効果が想定される一方で、**SBOM導入にかかるコスト等が障壁となり、日本全体としてSBOMの導入・活用が進んでいない**。
- 本実証事業においては、どのようにSBOMを活用すれば、**SBOM導入によって得られる効果が大きくなり、普及に繋がるかを確認したい**。

SBOM導入・活用の障害・課題

● SBOM導入にかかるコスト

– SBOMの導入・管理にかかるコストが新たに発生。

– 効果に対してどの程度のコストをかけるべきか判断に必要な情報が少ない。

– 多数のSBOMを手動で管理するとコストが膨大になるためツールによる自動化が考えられるが、下記のような課題が存在。

- ツールの導入コスト・ランニングコストが発生。
- ソフトウェアIDやSBOM形式が統一されていないなど、自動化の障害が存在。

● SBOM情報開示に対するサプライヤーの抵抗感

– サプライヤーによるSBOM生成・情報開示に関する抵抗感が強い。

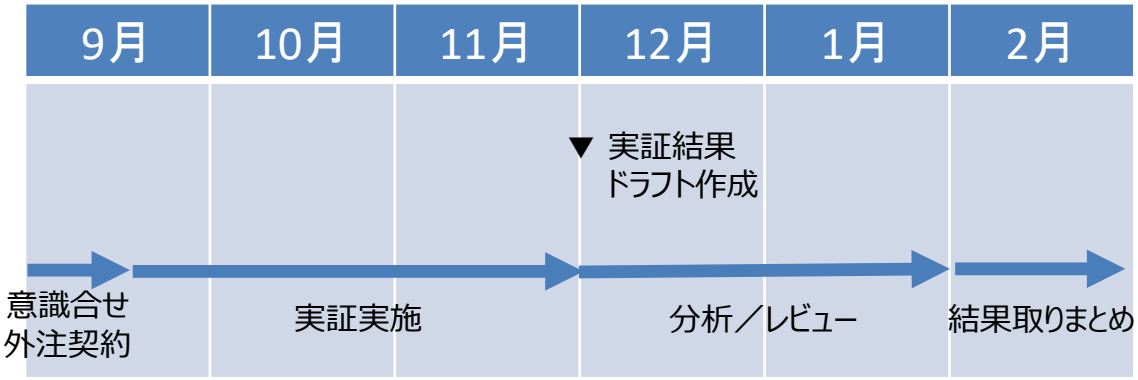
SBOM実証の対象ソフトウェア・体制・スケジュール

- ユーザー企業や製品ベンダーからのご協力が見込まれることから、**自動運転システム検証基盤ソフトウェア「GARDEN」を実証の対象ソフトウェアに選定**。

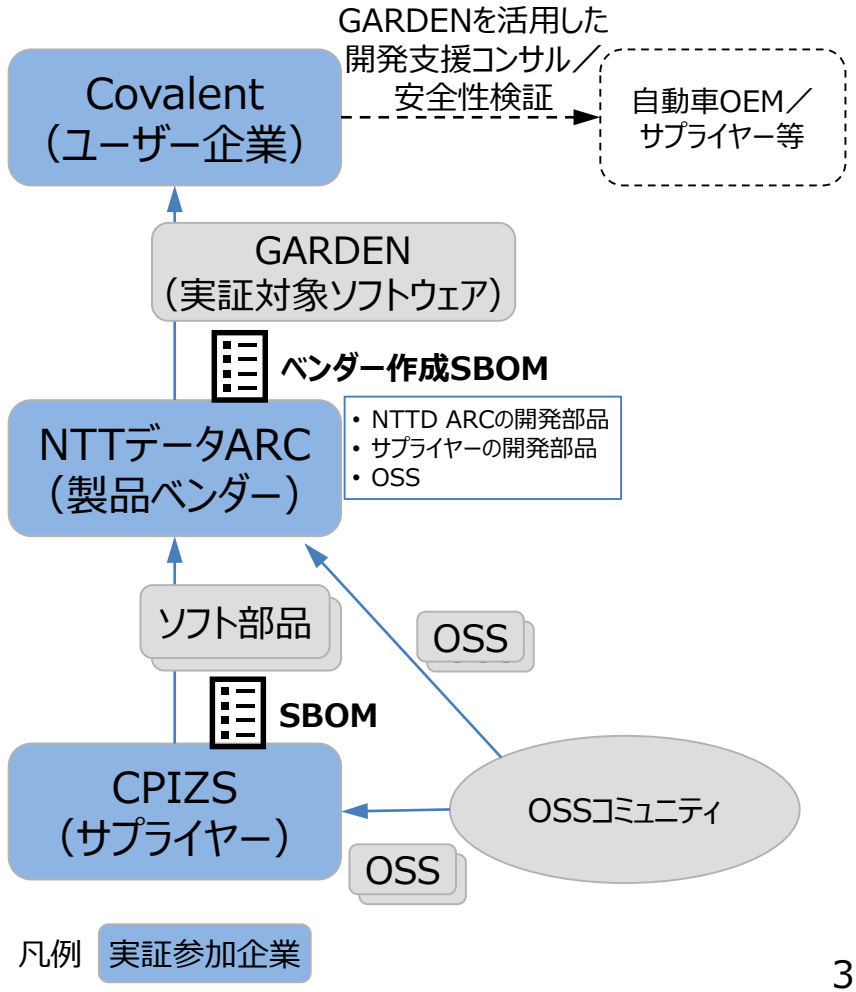
実証対象ソフトウェア 「GARDEN」

名称	GARDEN Scenario Platform
製品ベンダー	株式会社NTTデータ オートモビリジェンス研究所 （NTTデータARC）
概要	• 自動運転システム開発向け検証基盤ソフトウェア。 • 自動運転ソフトウェアの安全性評価のための機能動作シミュレーションのシナリオ生成機能を提供。 ➢ モデリング、走行データ分類、軌跡抽出道路編集、シナリオ組合せテスト、シナリオ実行 • オープンソースとして、ソースコードを公開。

想定スケジュール



実証体制（GARDENのサプライチェーン）



SBOM実証の内容（案）

- 実証においては、作成手段や作成者等の条件を設定して、SBOMの実際の効果やコストを比較し、今後の検討事項を整理。

比較項目

- **SBOMの効果**
  - 脆弱性管理　　脆弱性特定工数、脆弱性修正までの期間、脆弱性残留リスク等の低減
  - ライセンス管理　　ライセンス特定工数、ライセンス違反残留リスク等の低減
- **SBOMのコスト**
  - 初期コスト　　体制構築、環境整備
  - SBOM作成コスト　　作成工数、作成ツール費用
  - SBOM活用コスト　　部品管理工数（脆弱性の影響特定など）、管理ツール費用

比較条件

- そもそもソフトウェアの部品管理を行わない場合
- SBOMという形ではないが、何らか部品管理を実施する場合
- SBOMをユーザーが作成する場合
- SBOMをベンダーが作成する場合（手動で行う場合、ツールを利用する場合）

- **実証を通じてSBOMの実際の効果やコストを算出。**
- **国外の取組の進展も踏まえ、SBOMの効果的な活用方法を検討、今後の検討事項を整理。**

SBOMに関する施策の進め方（案）

- 国内施策および国際連携により、SBOMに係る対応を進める。
- 令和3年度の実証を通じてSBOMの効果的な活用方法を検討（STEP1）。
- STEP1の結果を踏まえて令和4年度以降、実証の対象を拡大し必要な制度、ツール整備を図る。

＜施策テーマ＞

	施策テーマ	施策
国内施策	(1) 国内産業のSBOM対応促進	**① 国内産業のSBOM普及啓発** • 実証やガイダンス等により国内産業へのSBOM普及促進を図る。
		②SBOM普及に向けた論点整理 ①で明らかにした論点を整理し、必要な制度・ツール等を整備する。 例：費用負担やリスク負担、知財権保護等の整理。自動化に向けたツール環境やソフトウェアID等の整備。
国際連携	(2) 日米の協力関係構築	**③SBOM検討に係る日米協力** OSS事例集や国内実証のコスト評価結果などを提供することにより、日米検討の協力関係を構築し、ツール等の整備における必要な調整を図る。

＜検討のステップ＞

STEP1：【R3年度実施】

実証を通じたSBOMの効果的な活用方法の検討

STEP2：【R4年度実施】

実証の対象拡大による課題整理（サプライチェーンにおける共有等）

STEP3：【R4年度～】

制度、ツールの検討・整備
国外との制度調和