資料４

関係省庁の取組状況について

【金　融　庁】

資料４－１　金融業界横断的なサイバーセキュリティ演習
（Delta Wall VI）について

【総　務　省】

資料４－２　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４－３　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４－１

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

令和3年10月

金融庁総合政策局リスク分析総括課サイバーセキュリティ対策企画調整室

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

金融分野のサイバーセキュリティを巡る状況

- 世界各国において、大規模なサイバー攻撃が発生しており、攻撃手法は一層高度化・複雑化
- 我が国においても、サイバー攻撃による業務妨害、重要情報の窃取、金銭被害等の被害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5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、2020年度は114先・延べ約1,700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 Ⅵ）

- 2021年10月、**金融庁主催による6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 Ⅵ（注））を実施。**

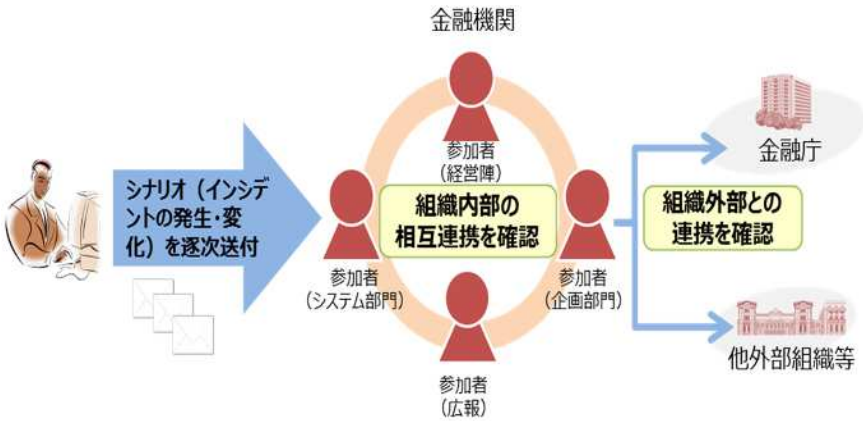
（注）Delta Wall: サイバーセキュリティ対策のカギとなる「自助」、「共助」、「公助」の3つの視点（Delta）＋防御（Wall）

- **中小金融機関のカバレッジ拡大**の観点から、信金・信組及び顧客に影響を及ぼすインシデントが発生した資金移動業者の参加先数を拡大し、**約150先が参加**。
- 対応できなかった項目の自己分析結果（例：コンチプラン（Plan）の課題か対応（Do）の課題か）を提出することとし、**評価の要因を明確化**することで、演習効果を高める。
- 昨年度に引き続き、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**初動対応、攻撃内容の調査等の技術的対応、情報連携、業務継続**等を確認
- ✓ 銀行では、インシデント対応時における**議論の内容や意思決定過程**を検証
- ✓ 経営層や多くの関係部署（システム部門、広報、営業部門等）が参加できるよう、**自職場参加方式**で実施
- ✓ 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**
  - ✓（ブラインド方式のため非開示）
- **信金・信組**
  - ✓ 重要システムの異常による顧客影響が発生
- **証券・FX・資金移動業者・暗号資産交換業者等**
  - ✓ 取引システムへの不正アクセスにより、顧客資産の流出が発生
- **生命保険・損害保険・保険代理店・監査法人**
  - ✓ 顧客情報の漏えいが発生

資料４－２

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

2021年10月

総務省サイバーセキュリティ統括官室

「ICTサイバーセキュリティ総合対策2021」（2021年7月　総務省「サイバーセキュリティタスクフォース」策定）の概要

＜政策課題に対処するための主な施策＞

＜電気通信事業者における安全かつ信頼性の高いネットワークの確保＞

5Gを含めて、電気通信事業者のネットワークや電気通信サービスにおけるリスクの高まりに応じた適切なセキュリティ対策を講じる必要

＜COVID-19への対応を受けたセキュリティ対策の推進＞

COVID-19感染拡大が続く中、中小企業等におけるテレワーク推進のためセキュリティ対策が急務。コロナ後も視野に、トラストサービスの推進も重要。

＜デジタル改革・DX推進の基盤となるサービス等のセキュリティ対策＞

IoT、クラウド、スマートシティについて、それぞれの課題に応じた適切な対策を推進していくことが必要。

＜サイバーセキュリティ情報に関する産学官での連携・共有等の促進＞

有効な技術や知見の共有による社会全体での対策の底上げ等が重要。

「ICTサイバーセキュリティ総合対策2021」の構成

Ⅰ　改定に当たっての主要な政策課題

Ⅱ　情報通信サービス・ネットワークの個別分野に関する具体的施策

1. 電気通信事業者における安全かつ信頼性の高いネットワークの確保のためのセキュリティ対策の推進

（1）安全かつ信頼性の高いネットワークの確保
（2）サイバー攻撃に対する電気通信事業者の積極的な対策の実現
（3）5Gの本格的な普及に向けたセキュリティ対策の強化

2. COVID-19への対応を受けたセキュリティ対策の推進

（1）テレワークセキュリティの確保
（2）トラストサービスの制度化と普及促進

3. デジタル改革・DX推進の基盤となるサービス等のセキュリティ対策の推進

（1）IoTのセキュリティ対策
（2）クラウドサービスの利用の進展を踏まえた対応
（3）スマートシティのセキュリティ対策

4. 分野別の具体的施策

（1）無線LANのセキュリティ対策
（2）放送分野のセキュリティ対策
（3）地域の情報通信サービスのセキュリティの確保

Ⅲ　横断的施策

1. サイバーセキュリティ情報に関する産学官での連携・共有等の促進

（1）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
（2）サイバー攻撃被害情報の適切な共有及び公表の促進
（3）その他の情報共有・情報開示の促進

2. ICTサイバーセキュリティに係る横断的施策

（1）国際連携の推進
（2）研究開発の推進
（3）人材育成・普及啓発の推進

別添：プログレスレポート2021（総合対策2020の各施策の進捗状況）

＜施策の推進・実施に当たっての基本的考え方・主な留意点＞

①サイバーセキュリティ戦略に定める5原則を踏まえた施策展開

情報の自由な流通、法の支配、開放性、自律性、多様な主体の連携の5原則を確保。

②サービス・製品の提供側と利用側の双方の観点からの施策展開

③各施策の粒度やタイムスパン等の違いに応じた施策展開

具体的・政策的施策の双方、短期的・中長期的施策の双方を総合的・有機的に推進。

実践的サイバー防御演習（CYDER）

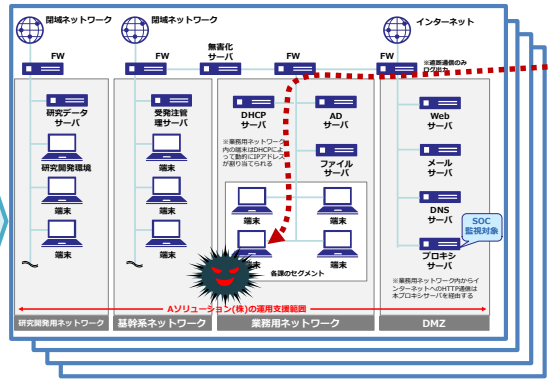
CYDER：CYber Defense Exercise with Recurrence

- 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

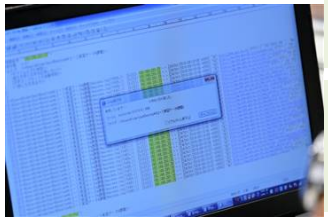


擬似攻撃者

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	６５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	２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２月 (6~8月に試験提供予定)

令和３年度から**新規**開設

電気通信事業者の積極的な対策（ネットワーク側での機動的な対処）の実現

- IoTの進展に伴い、脆弱でセキュリティ対策が困難な端末機器も増加する中、**端末側とネットワーク側の双方から、総合的なセキュリティ対策を実施**することが求められている。
- 端末側の対策としては、電気通信事業法における端末設備等規則へのセキュリティ要件の追加や、脆弱な状態にある機器の利用者への注意喚起等の取組みを実施。
- **ネットワーク側の対策**として、**電気通信事業者が個々の感染端末に指示を出すC&Cサーバ※に直接対処**するなど、**より効率的・機動的にセキュリティ対策を実施**することが重要。

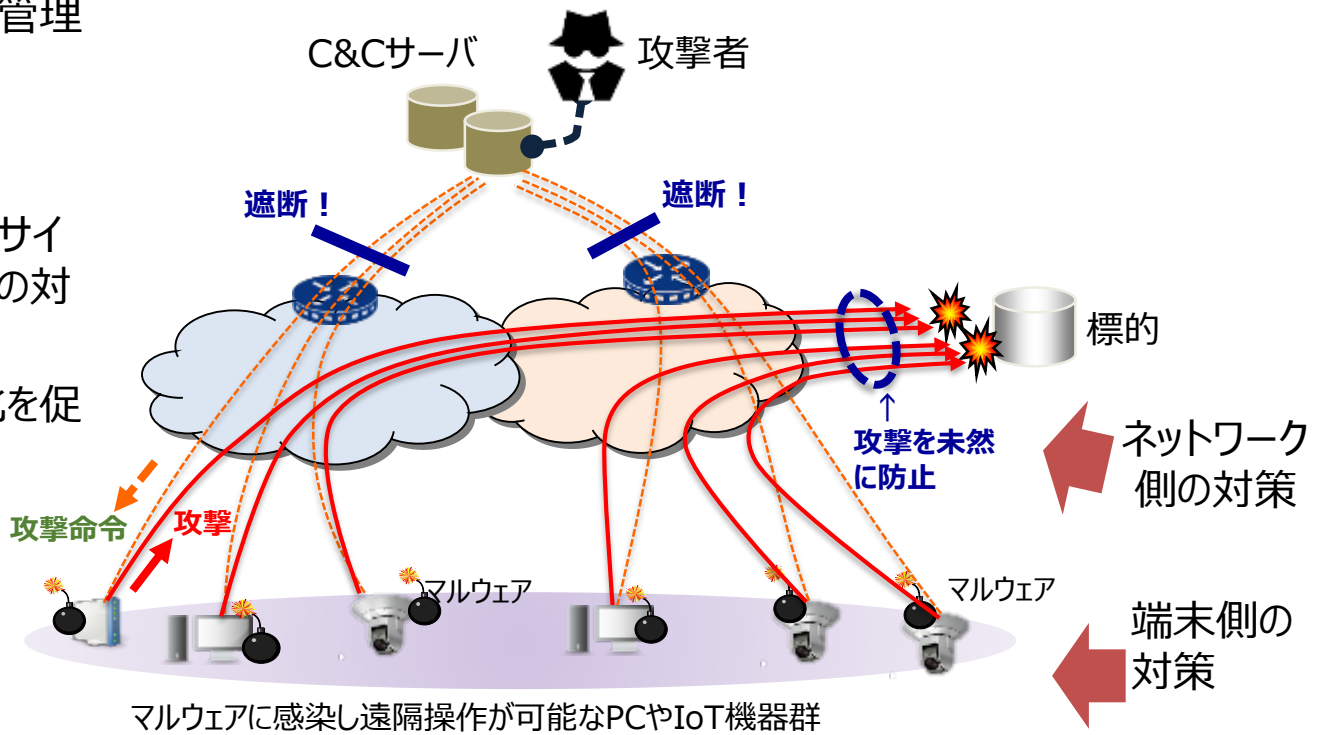
  ⇒ サイバー攻撃が通過する**ネットワーク側で機動的な対処を行う環境整備**が必要。

※Command and Controlサーバの略であり、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

■ 端末側の対策とも連携しつつ、ISPが管理するネットワーク側においても高度かつ機動的な対処を実現するための方策の検討が必要。

- ISPが自らC&Cサーバを検知し、サイバー攻撃の指令通信の遮断などの対策を実施するための方策
- 新技術を活用した対策の高度化を促進するための方策　等

⇒ **制度的・技術的な観点から検討**を推進



電気通信事業者におけるガバナンス確保の在り方の検討

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

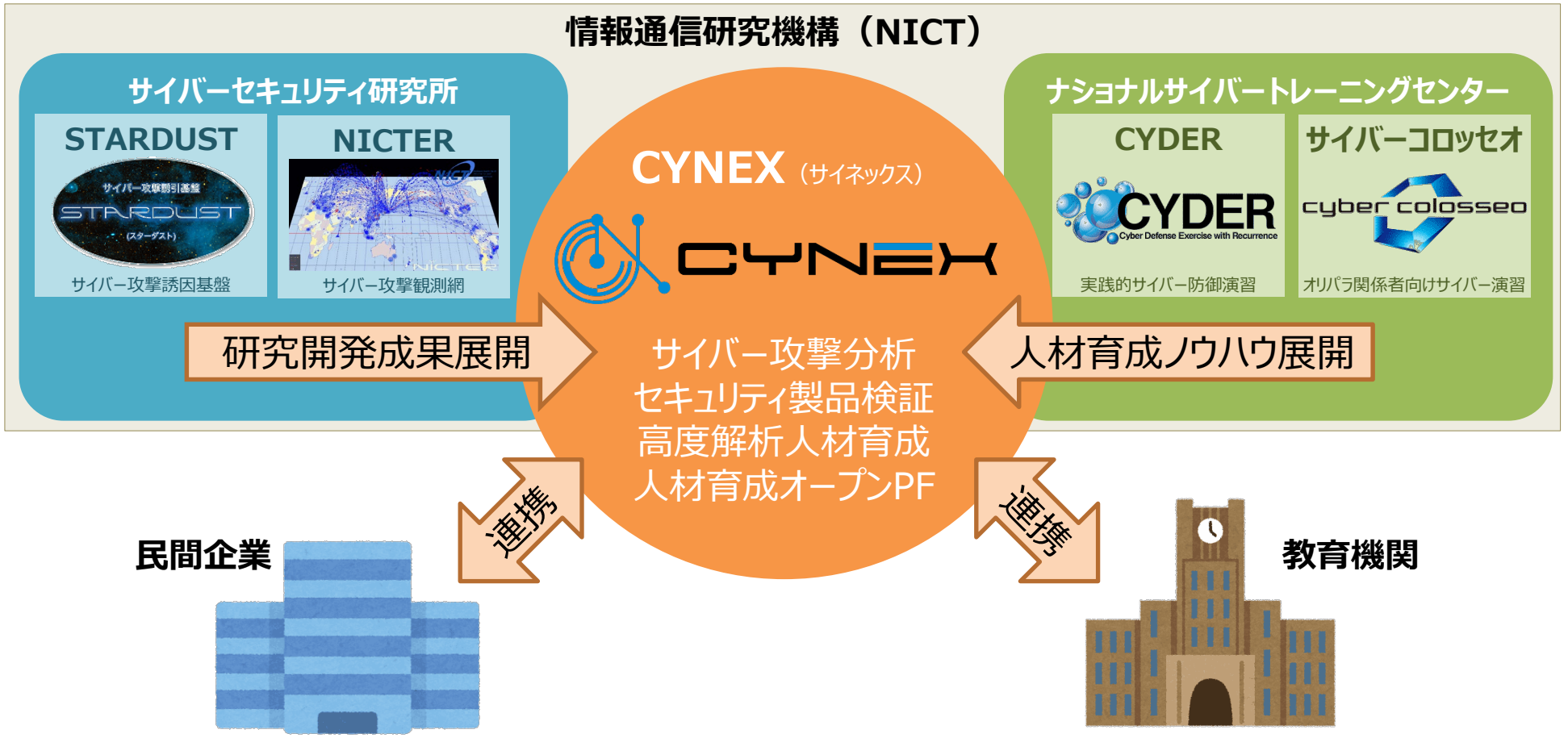
3．体制・スケジュール

- 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。
- 本年5月12日に第1回会合を開催。会議は非公開（議事概要・資料等は公開）。

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
大橋　弘（座長）	東京大学公共政策大学院院長
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

サイバーセキュリティに関する産学官の結節点『CYNEX』

- 情報通信研究機構（NICT）では、これまでも次のような取組を実施
  サイバーセキュリティ研究所・・・最先端のサイバーセキュリティ関連技術の研究開発を実施
  ナショナルサイバートレーニングセンター・・・実践的サイバー防御演習等による人材育成を実施
- これらの知見を活用し、サイバーセキュリティに関する産学官の巨大な結節点となる先端的基盤として
  ＣＹＮＥＸ（CYbersecurity NEXus：サイネックス） を構築



テレワークセキュリティガイドラインの改定

- 総務省では従来から「**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**を示してきた。
  → テレワークを取り巻く環境やセキュリティ動向の変化に対応するため**2021年５月**に**全面的に改定**
- ガイドラインを補完するものとして、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いても、テレワークを実施する際に**最低限のセキュリティ**を**確実に確保**してもらうための**チェックリスト**についても策定。

公表URL　https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

テレワークセキュリティガイドライン
（2021年５月　第５版）

2004年12月初版
2006年４月第２版
2013年３月第３版
2018年４月第４版

- ✓ テレワークを業務に活用する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するための指針
- ✓ 中小企業を含む全企業を対象
- ✓ システム管理者のほか経営層や利用者(勤務者)を幅広く対象

ガイドラインに記載の内容について、理解や検討が難しい場合

中小企業等担当者向けテレワークセキュリティの手引き(チェックリスト)
（2021年５月　第２版）　2020年９月初版

中小企業等に向け**最低限のセキュリティを確実に確保**してもらうためのものに限定

【想定読者像】
- ✓ システム管理担当者向け
- ✓ 専任の担当・部門は存在しない
- ✓ 基本IT用語は聞いたことがあるレベル
- ✓ 設定作業は検索しながら実施可能

テレワークで活用される代表的なソフトについて、**設定解説資料**を作成し、具体的な設定を解説

【設定解説資料の対象】
CiscoWebexMeetings ／ Microsoft Teams／Zoom／Windows／Mac／iOS ／ Android ／ LanScope An ／ Exchange Online ／ Gmail ／ Teams_chat ／ LINE ／ OneDrive ／ Googleドライブ／Dropbox／YAMAHA VPNルータ／CiscoASA／Windowsリモートデスクトップ接続／Chromeリモートデスクトップ／Microsoft Defender／ウイルスバスター ビジネスセキュリティサービス

テレワークセキュリティガイドラインの改定（2021年５月）

【テレワーク環境・セキュリティ動向の変化】
- ✓ テレワークは「一部の従業員」が利用するものから、Web会議を含め、一般的な業務・勤務形態に
- ✓ クラウドサービスの普及やスマートフォン等の活用が進むなど、システム構成や利用形態が多様化
- ✓ 標的型攻撃等の高度な攻撃が増え、従来型のセキュリティ対策では十分対応できない状況も発生

【ガイドライン改定の主要なポイント】
- ✓ テレワーク方式を再整理し、適した方式を選定するフローチャートや特性比較を掲載
- ✓ クラウドやゼロトラスト等のセキュリティ上のトピックについても記載
- ✓ 経営者・システム管理者・勤務者の立場それぞれにおける役割を明確化
- ✓ 実施すべきセキュリティ対策の分類や内容を全面的に見直し
- ✓ テレワークセキュリティに関連するトラブルについて、具体的事例を含め全面見直し
  （事例紹介のほか、セキュリティ上留意すべき点や、採るべき対策についても明示）

資料４－３

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

2021年10月

経済産業省サイバーセキュリティ課

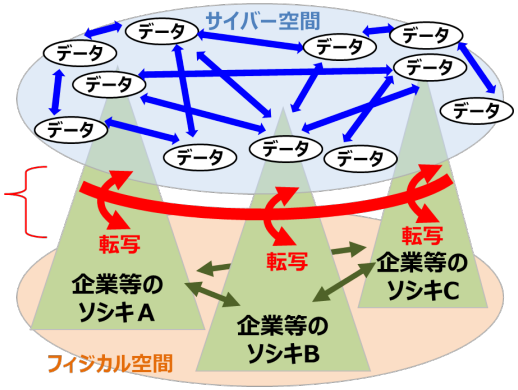
サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）
～ Society5.0 における新たなサプライチェーン（バリュークリエイションプロセス）の信頼性の確保に向けて ～

- サイバーとフィジカルが高度に融合する**「Society5.0」**では、**より柔軟で動的なサプライチェーンの構成が可能**になる一方、**サイバー攻撃の起点の拡散、フィジカル空間への影響の増大という新たなリスク**に直面。
- そのため、Society5.0における**新たなリスクに対応するセキュリティ対策の全体像を整理した『サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）Ver1.0』を2019年4月18日に公表**。
- 2度にわたるパブコメ（日本語、英語）に対して**国内外から多数のコメント**（合計：約800件、国内51・海外22の個人・組織）が寄せられ、**国際的認知も進展**。

CPSFが示した『3層構造』

サイバー空間におけるつながり
【第３層】
自由に流通し、加工・創造されるサービスを創造するための**データの信頼性**を確保

フィジカル空間とサイバー空間のつながり
【第２層】
フィジカル・サイバー間を正確に**“転写”する機能の信頼性**を確保



企業間のつながり
【第１層】
適切な**マネジメントを基盤に各主体の信頼性**を確保

CPSFが示した『6つの構成要素』

- **リスクベースの対策**につなげるため、動的に構成されるサプライチェーンの**構成要素を6つに整理**

ソシキ	ヒト	モノ	データ	プロシージャ	システム

CPSFにおけるリスクマネジメントの考え方

（各層の）機能 → セキュリティインシデント → リスク源（構成要素ごとに整理） → 対策要件 → 対策例（3つにレベル分け）
- High-Advanced
- Advanced
- Basic

CPSFと国際規格等との整合性確保

- **国際規格等との対応関係を記載**（第Ⅲ部、添付C及び添付Ｄ）
- **以下3つの主要な国際規格等から見た対応表も整理**（添付D）
  - NIST Cybersecurity Framework
  - NIST SP800-171
  - ISO/IEC 27001付属書A

分野別SWGにおけるサイバー・フィジカルセキュリティ対策フレームワーク（CPSF）の具体化 とテーマ別TFにおける検討

- **6つの産業分野別サブワーキンググループ(SWG)**を設置し、CPSFに基づくセキュリティ対策の具体化・実装を推進
- 分野横断の共通課題を検討するために、3つの**タスクフォース（TF）を設置**

産業サイバーセキュリティ研究会ＷＧ１（制度・技術・標準化）

標準モデル（CPSF）

Industry by Industryで検討
(分野ごとに検討するためのSWGを設置)

- **ビルSWG**
  - ガイドライン第1版の策定(2019.6)
- **電力SWG**
  - 小売電気事業者ガイドライン策定(2021.2)
- **防衛産業SWG**
- **自動車産業SWG**
  - ガイドライン1.0版を公表(2020.12)
- **スマートホームSWG**
  - ガイドライン1.0版を公表(2021.4)
- **宇宙産業SWG**
  - 2021年1月に第1回を開催
- ・・・

分野横断SWG

『第3層』TF：『サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース

検討事項：
データの信頼性確保に向け「データによる価値創造（Value Creation）を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク（仮）」骨子案のパブリックコメントを実施。

ソフトウェアTF：サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース

検討事項：
OSSの管理手法に関するプラクティス集の策定、SBOM活用促進に向けた実証事業（PoC）を検討。

『第2層』TF：『フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース

検討事項：
フィジカル空間とサイバー空間のつながりの信頼性の確保するための「IoTセキュリティ・セーフティ・フレームワーク(IoT-SSF)」を公開。

第3層TF：サイバー空間における価値創造を支えるデータマネジメントの枠組みの策定

- データマネジメントに関する定義を明確化し、フレームを設定することで、主体間を転々流通するデータに関する**リスクポイントの洗い出しを可能に**する。
- また、本枠組みを**共通の定規として利用**することで、各国・地域などの**主体間のデータに関するルールのギャップ/データの流通プロトコルの問題を可視化、データの囲い込みを回避する**取組につなげる。
- 「データによる価値創造（Value Creation）を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク（仮）」の**骨子案を取り纏め、パブリックコメントを実施**。（2021/7/15～10/11）

https://www.meti.go.jp/press/2021/07/20210715005/20210715005.html

データマネジメントの新たな捉え方

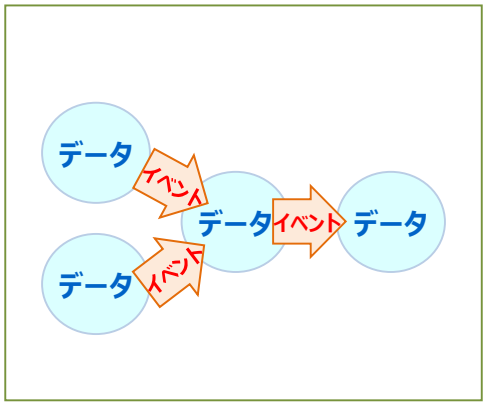
▶「データの "**属性**" が "**場**" における "**イベント**" により変化する過程をライフサイクル全体にわたって管理すること」

属性		場		イベント
データが有する性質	✖	特定の規範を共有する範囲	✖	データの属性を生成・変化させる処理

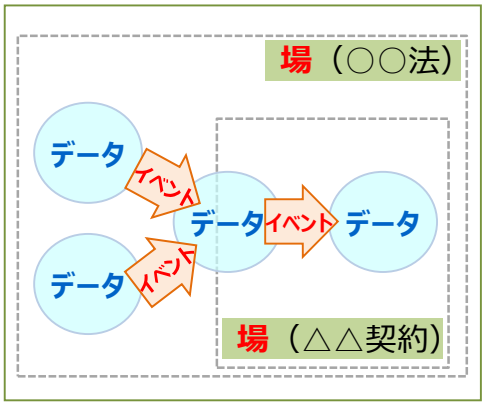
新たな捉え方への当てはめステップ

▶4つのステップに沿ってバリュークリエイションプロセスにおけるデータの状態を可視化しリスクを洗い出す。

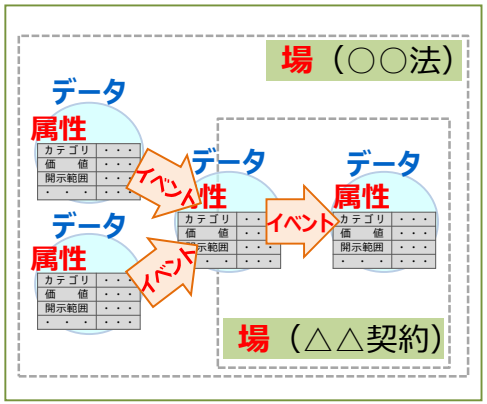
STEP 1
データ処理フロー（「イベント」）の可視化



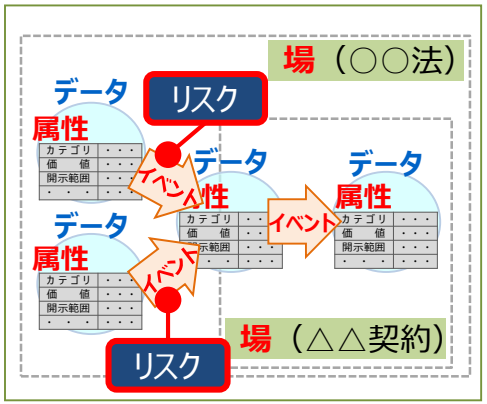
STEP 2
必要な制度的保護措置（「場」）の整理



STEP 3
「属性」の具体化



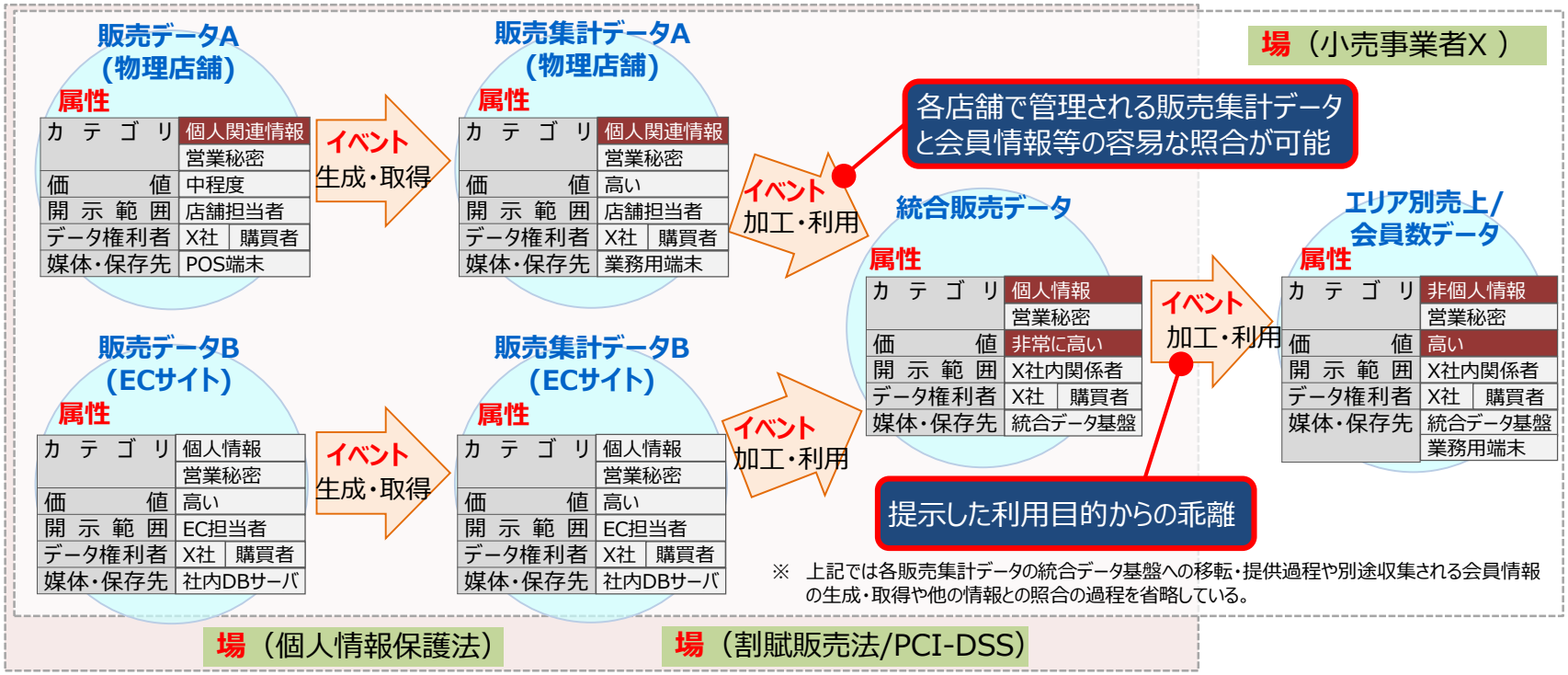
STEP 4
「イベント」ごとのリスクの洗い出し



第3層TF：フレームワークのユースケースに係る検討（POSデータ活用事例）

- ユースケースのひとつとして、小売業におけるPOSデータの活用事例にフレームワークを適用。
- 販売データの生成・取得からマーケティング目的での加工・利用に至るまでの一連の利活用プロセスを可視化するとともに、今後のセキュリティ水準等の向上のために必要なアクションを明確化。

新たな捉え方の適用（小売業におけるPOSデータの活用事例）



新たな捉え方の適用を通じてx社が導き得るアクション（例）

- 一律のデータ保護水準を確保することが難しい各物理店舗において、他データとの照合等を通じて個人情報に該当するデータが保有されないことを改めて確実なものとすべく、統合データ基盤で管理される会員情報に対する各店舗、支社によるアクセス状況のレビュー、アクセス制御ポリシーその他の運用規定の見直し等を行う
- 購買者に関するデータの利用実態を踏まえ、自社の個人情報保護方針や会員規約等の一部（利用目的に関する条項等）を改定する