資料47－１

「ICTサイバーセキュリティ政策の中期重点方針」に基づく取組状況

令和７年９月

サイバーセキュリティタスクフォース事務局

「ICTサイバーセキュリティ政策の中期重点方針」に基づく主な取組の概要

- 総務省では、2024年２月から「ICTサイバーセキュリティ政策分科会」（主査：後藤厚宏　情報セキュリティ大学院大学学長）を開催し、総務省が取り組むべきサイバーセキュリティ政策について、2030年頃も見据えた中長期的な方向性について検討。
- 2024年７月、今後重点的に取り組むべき施策として「ICTサイバーセキュリティ政策の中期重点方針」が取りまとめられた。当該方針に基づく主な取組は以下のとおり。

１．重要インフラ等におけるサイバーセキュリティの確保

- 通信分野（総合的なIoTボットネット対策の推進　等）
- 放送分野（安全・信頼性に関する技術基準に基づくサイバーセキュリティの確保　等）
- 自治体分野（ガイドラインを通じた地方公共団体におけるサイバーセキュリティの確保　等）
- クラウドセキュリティの確保やトラストサービス（eシールに係る認定制度等）の推進

２．サイバー攻撃対処能力の向上と新技術への対応

- 政府端末情報を活用したサイバーセキュリティ情報の収集・分析
- ナショナルサイバートレーニングセンターを通じた人材育成の推進
- 生成AI等の新技術への対応
- AIとサイバーセキュリティに係る取組の推進
- 耐量子計算機暗号（PQC）移行に係る取組の推進

３．地域をはじめとするサイバーセキュリティの底上げに向けた取組

- 地域に根付いたセキュリティコミュニティ（地域SECUNITY）の形成促進

４．国際連携の更なる推進（国際連携全般、人材育成支援）

- インド太平洋地域における開発途上国・地域に対する能力構築支援

1．重要インフラ等におけるサイバーセキュリティの確保

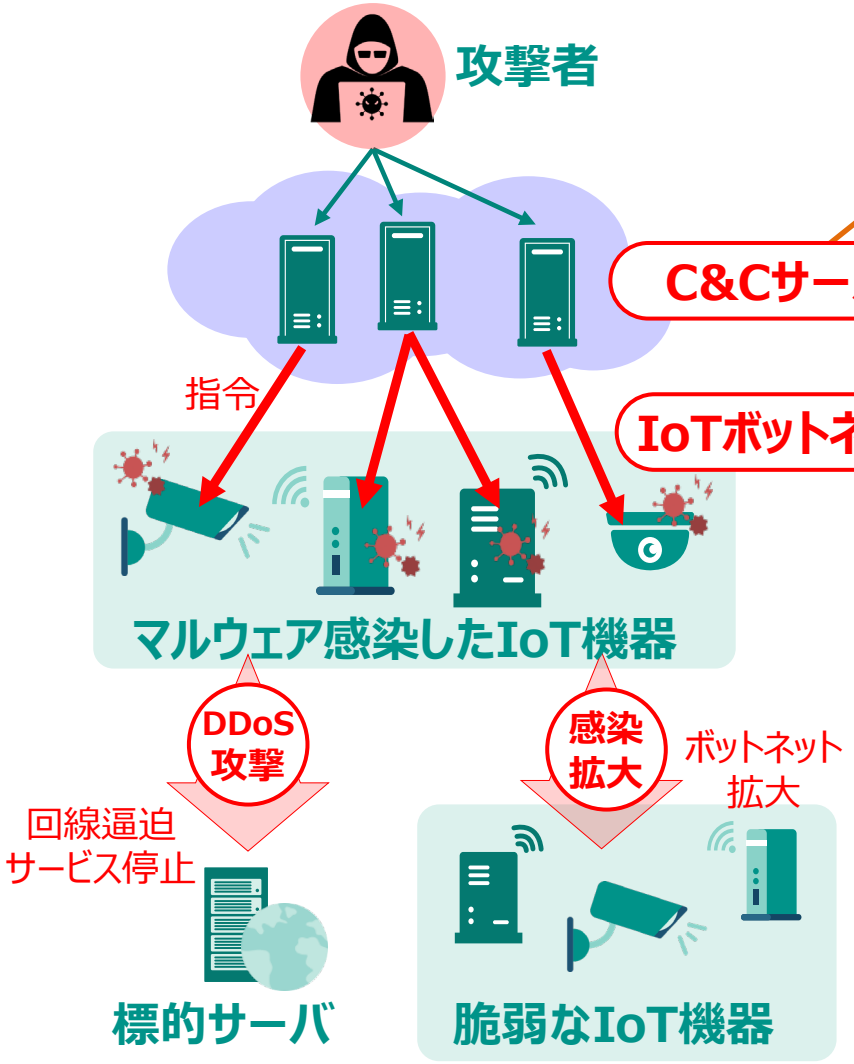
2．サイバー攻撃対処能力の向上と新技術への対応

3．地域をはじめとするサイバーセキュリティの底上げに向けた取組

4．国際連携の更なる推進
（国際連携全般、人材育成支援）

総合的なIoTボットネット対策

- IoT機器の急増に伴い、**IoT機器を悪用**した大規模なサイバー攻撃（**DDoS攻撃**等）が発生
- DDoS攻撃は**ネットワークの速度低下**を引き起こすほか、**標的側での対応が難しい**
- **電気通信事業者と総務省・NICTが協力**して、**C&Cサーバ**と、攻撃役となる**脆弱なIoT機器**の両面から対策



IoTボットネットに対して指令通信を出す C&Cサーバへの対処

電気通信事業者がネットワークの管理のために利用する「**フロー情報**※」を**分析**することで、**C&Cサーバを検知**
→ 対策に活用するための**実証事業を実施中**

※IPアドレス、ポート番号、プロトコル、パケット数などに関する情報
ヘッダー情報のみでペイロード（データの本体部分）は含まない

マルウェアに感染した/感染する危険性が高い 脆弱なIoT機器への対処

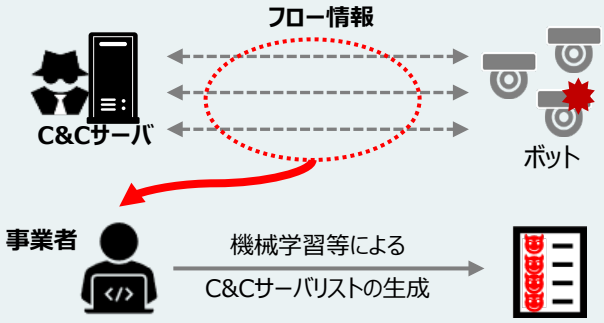
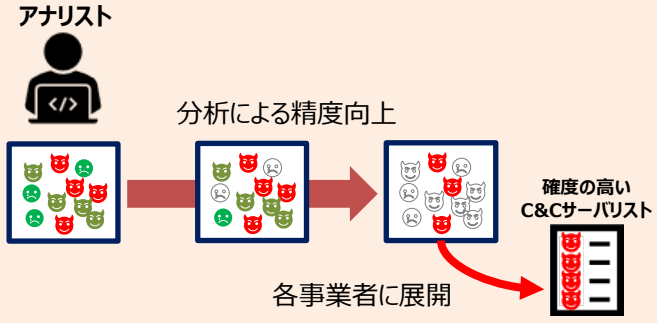
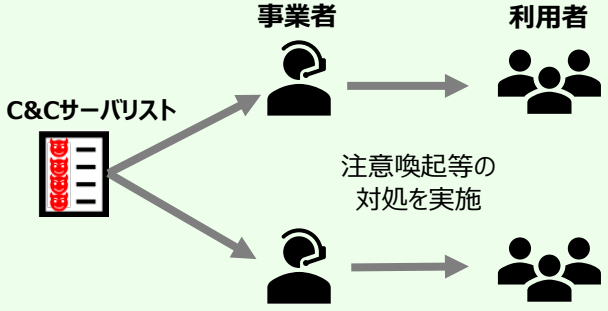
サイバー攻撃に悪用されるおそれのある**IoT機器を調査**し、
（サイバーセキュリティに知見のあるNICTにおいて調査を実施）
インターネットサービスプロバイダを通じ、**IoT機器の利用者に注意喚起**

＜調査＆注意喚起の対象＞
① ID・パスワードの設定に脆弱性がある機器
② ファームウェアの脆弱性等がある機器
③ 既にマルウェアに感染している機器

→「**NOTICE**」プロジェクト NOTiCE

C&Cサーバへの対処

- 電気通信事業者（ISP）は通信を安定的に流すため、普段から自社のネットワーク上を流れるフロー情報を観測しており、このフロー情報を分析すると、IoTボットネットと通信するC＆Cサーバを事前に検知できることがある。
- 攻撃の標的となる企業等の側からは根本的な対策が難しいDDoS攻撃に対し、**電気通信事業者がフロー情報を分析**することで、攻撃の指示を行う可能性のある**C＆Cサーバを事前に検知**し、**対策に活用**するための実証事業を実施している。

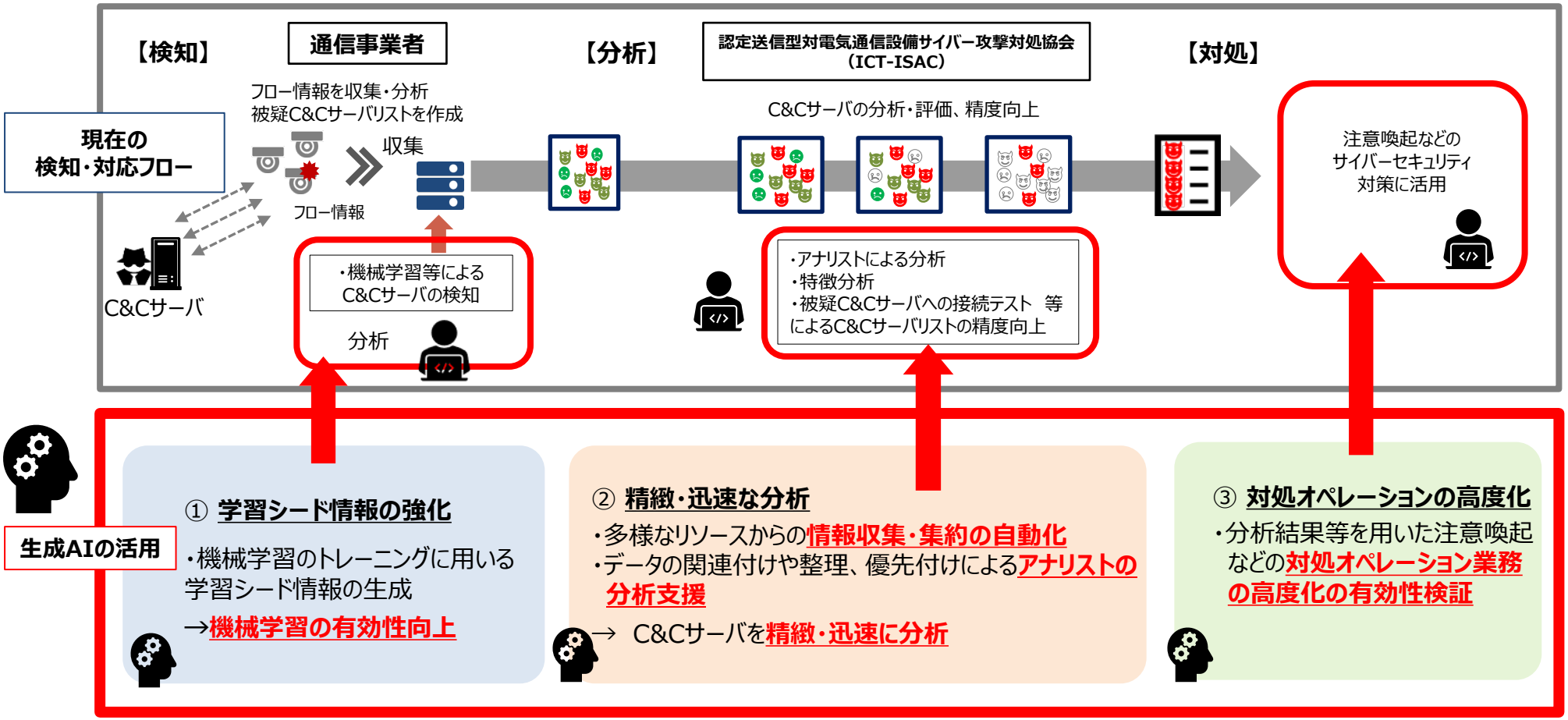
検知（電気通信事業者）	共有･分析（適切な事業者団体等）	対処（電気通信事業者）
機械学習等を用いたフロー情報分析によるC&Cサーバの検知	事業者団体（ICT-ISAC）による、共有されたC&Cサーバリストの分析及び事業者へのリストの展開	各事業者による注意喚起等のサイバー攻撃対処を実施 ※試行中
		

主な実績

- 平均して**月に数十件程度**の現に悪用継続中のC2サーバのIPアドレスを定常的に取得
- 検知したC&Cサーバのうち、**約30%**は公開情報よりも早く検知

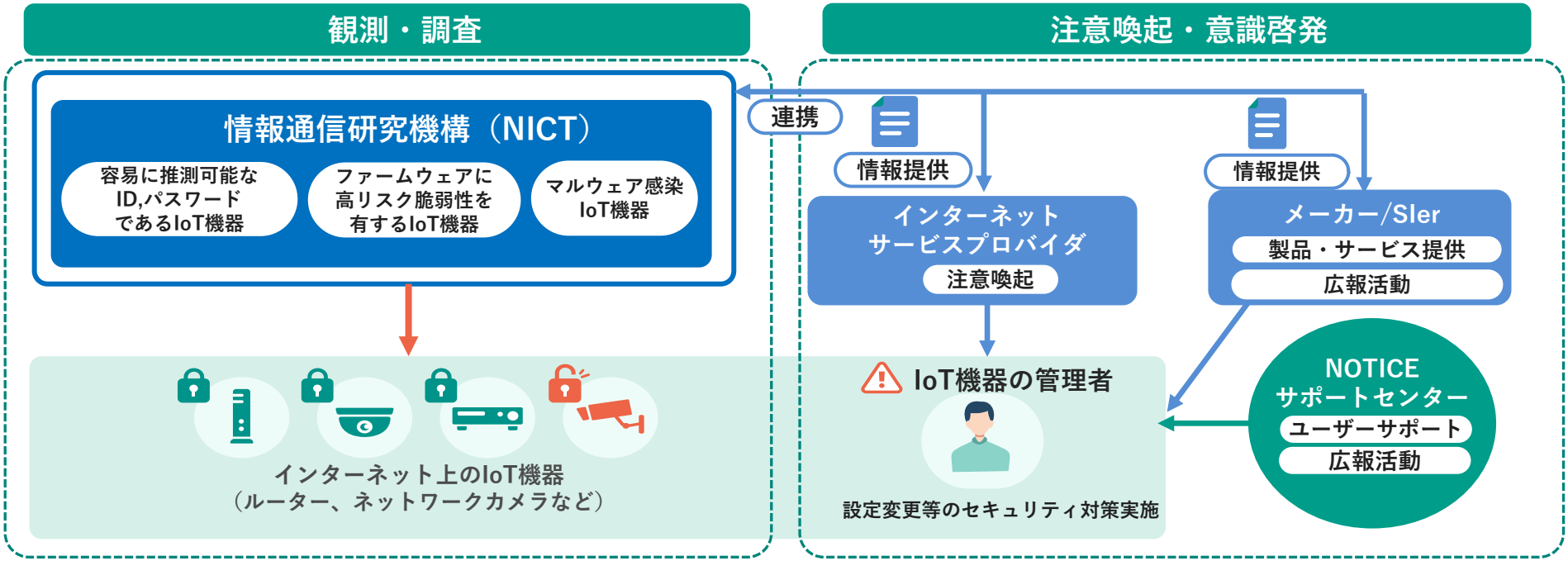
生成AIを活用したC＆Cサーバ検知の高度化

➢ **生成AIを効果的に活用**し、**攻撃インフラ分析の精緻化・迅速化を図る**とともに、**当該分析結果等を踏まえた対処オペレーション業務の高度化を図る**ための技術的な検証を実施



脆弱なIoT機器への対処（NOTICE）

➢ マルウェアに感染したIoT機器は新たな機器に感染を広げ規模を拡大するため感染拡大通信を行う。この感染拡大通信等をNICTが観測・調査し、**既に感染しているIoT機器や、今後感染する危険性が高い脆弱なIoT機器を発見**する。**それらのIoT機器を使用している管理者**に対し、インターネットサービスプロバイダと連携して**注意喚起・周知啓発等**を行うことで、IoTボットネットによる**サイバー攻撃（DDoS攻撃）の発生と被害を軽減**する。（NOTICE事業）



2025年7月観測結果

容易に推測可能なID,パスワードである IoT機器	ファームウェアに高リスク脆弱性を有するIoT機器	マルウェア感染IoT機器
月 14,370 件	月 2,865 件	最大 1,024 件/日

放送分野におけるサイバーセキュリティの取組について

放送設備の安全・信頼性確保に関する規定

・特定地上基幹放送事業者においては、法第112条
・基幹放送局提供事業者においては、法第121条
・登録一般放送事業者においては、法第136条
に、技術基準への適合維持義務を規定。

○放送法に規定する技術基準適合維持義務

（設備の維持）

第111条　認定基幹放送事業者は、基幹放送設備を総務省令で定める技術基準に適合するように維持しなければならない。

2　前項の技術基準は、これにより次に掲げる事項が確保されるものとして定められなければならない。

一　基幹放送設備の損壊又は故障により、基幹放送の業務に著しい支障を及ぼさないようにすること。

二　基幹放送設備を用いて行われる基幹放送の品質が適正であるようにすること。

◆ **放送法施行規則（省令）に安全・信頼性に関する技術基準を規定**

- 予備機器等
- 故障検出
- 試験機器及び応急復旧機材の配備
- 耐震対策
- 機能確認
- 停電対策
- 送信空中線に起因する誘導対策
- 防火対策
- 屋外設備
- 放送設備を収容する建物
- 耐雷対策
- 宇宙線対策
- **サイバーセキュリティの確保※**

※2020年に「サイバーセキュリティの確保」を技術基準に追加、2024年にはさらにIP化に対応したサイバーセキュリティ対策を追加している。

措置項目	措置内容
サイバーセキュリティの確保	• 放送設備及び当該放送設備を維持又は運用するために必要な設備は、放送の業務に著しい支障を及ぼすおそれがないよう、サイバーセキュリティの確保のために必要な措置。

【参考】番組送出設備（マスター設備）に関する動向

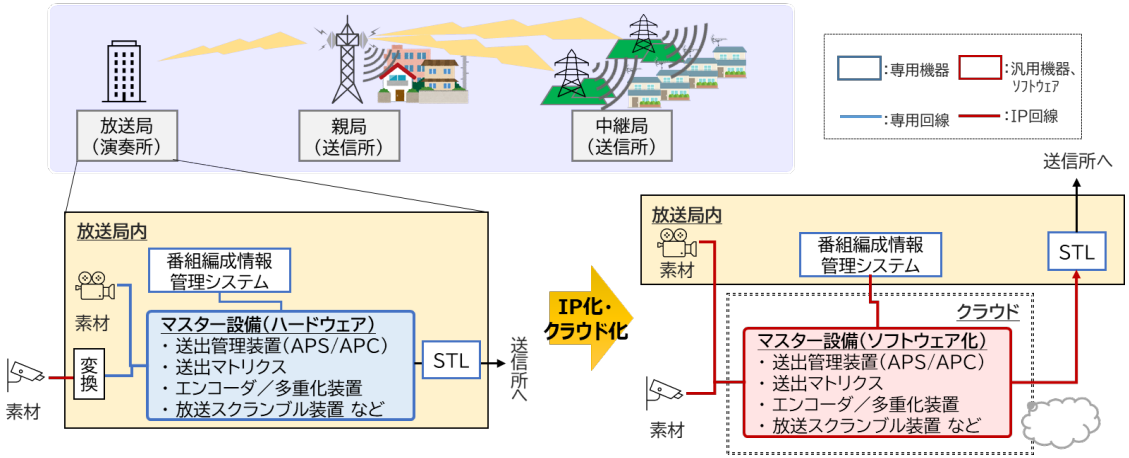
今後の方向性

- 地上デジタルテレビジョン放送のマスター設備について、2028年～2030年頃（令和10年～令和12年頃）に想定される在京キー局での設備更新を見据え、効率化を図る観点から、マスター設備の集約化・IP化・クラウド化は経営の選択肢となり得る。
- 集約化に当たっては、放送番組のやり取りが行われており、設備仕様がある程度共通化されている系列局の単位で集約化を図ることが現実的である。例えば衛星放送のプラットフォーム事業者のように、マスター設備を特定の場所に設置し、その運用・維持管理を地上基幹放送事業者以外の事業者が担うことや、クラウドサービスとして提供を受けることが考えられる。
- 集約化の対象エリアは、系列局単位での集約化を前提に、地域ブロックに加え、全国単位も視野に入ると考えられる。
- 集約化・クラウド化に当たっては、**サイバーセキュリティ対策等、安全・信頼性をどのように確保可能かについて検討すべき**である。追加的なコストが発生することとなるが、持続可能な放送の実現のためのコスト削減とサイバーセキュリティ対策等の安全・信頼性確保の両立に向けた道筋を描くことは可能と考えられる。
- 我が国におけるクラウド化の実現に向けて、**どの程度の可用性を確保すべきかといった検討が必要**と考えられる。
- マスター設備の集約化・IP化・クラウド化は、放送事業者の経営の選択肢であることに留意しつつ、その要求条件を総務省において検討・整理すべきである。その際、放送に求められる可用性を確保するためには、**不測の事態における対処をクラウド側に委ねるのではなく、マスター設備の利用者である放送事業者自らがリスクをグリップ（把握）し、コントロール（制御）できることが重要であることにも留意すべき**である。

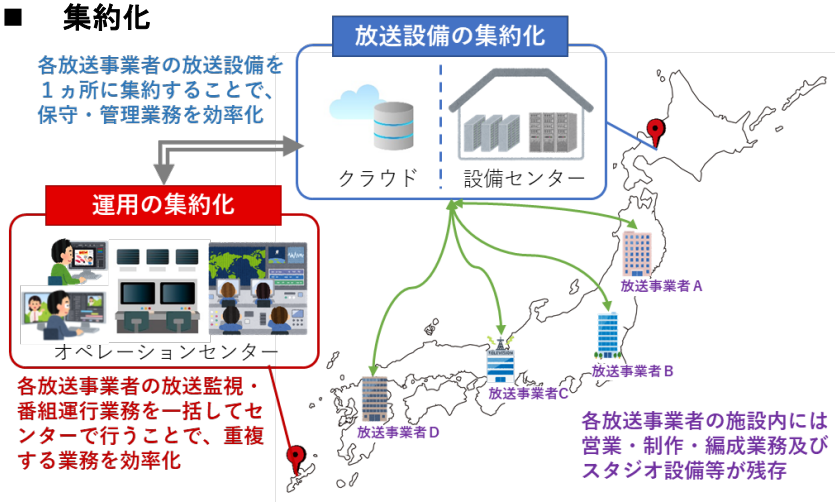
出典：「デジタル時代における放送の将来像と制度の在り方に関する取りまとめ」（デジタル時代における放送制度の在り方に関する検討会　令和４年８月５日公表）より事務局作成

将来のマスター設備のイメージ

■ IP化・クラウド化



■ 集約化

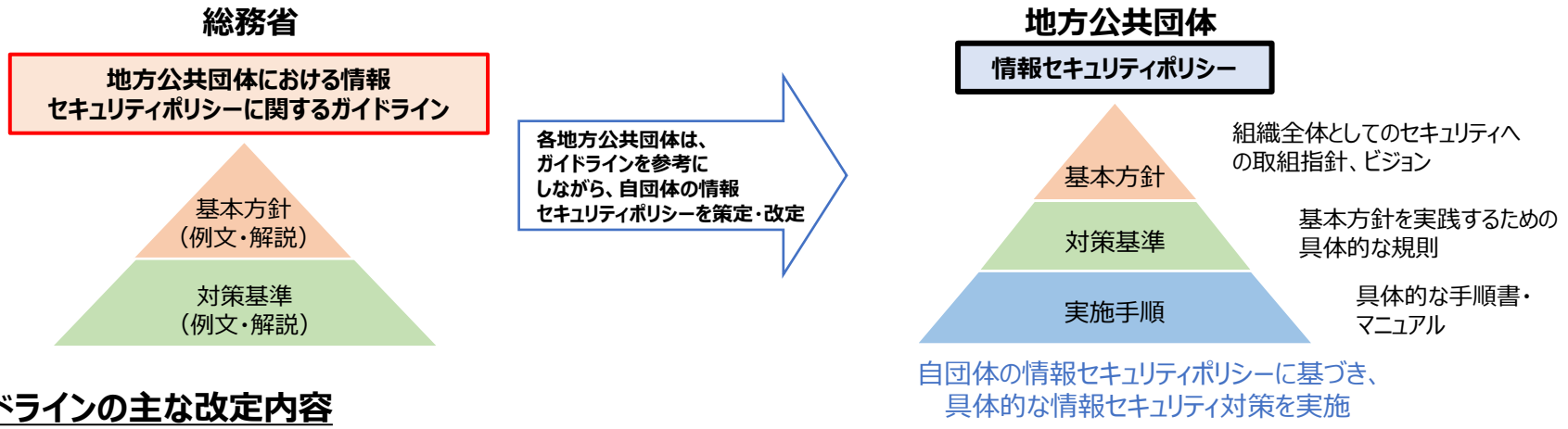


「地方公共団体における情報セキュリティポリシーに関するガイドライン」について

地方公共団体の業務システムの標準化・共通化やサイバー攻撃の高度化・巧妙化を踏まえ、**新たな自治体情報セキュリティ対策の在り方について調査研究**を行い、**「地方公共団体における情報セキュリティポリシーに関するガイドライン」に反映**する。

１．概要

各自治体のセキュリティ対策の指針として総務省が策定し助言。国における情報セキュリティ対策の動向やデジタル化の動向等を踏まえながら、有識者検討会での議論を経て、**年度ごとに改定を実施**。令和６年に改正された地方自治法等を踏まえ、最新のセキュリティ動向に合わせた技術的な知見に加え、自治体の業務に即した対策を検討することが重要。



２．ガイドラインの主な改定内容

改定時期	改定内容
2018年９月	平成27年の日本年金機構における情報流出事案を受け、総務省から地方公共団体へ要請を行った「三層の対策」等の情報セキュリティの抜本的強化策の内容を反映
2020年12月	「三層の対策」の効果や課題、新たな時代の要請を踏まえ、セキュリティの確保と効率性・利便性向上の両立の観点から、高度なセキュリティ対策を実施することを条件に、インターネット接続系に業務端末を配置するモデルを提示するなど新たな対応策を追加
2022年３月	令和３年７月の「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」の改定や、地方公共団体のデジタル化の動向を踏まえた内容を反映
2023年3月	標準準拠システム等のクラウドサービスの利用を想定し、クラウドサービスを利用する際の具体的な情報セキュリティ対策の内容を第4編（特則）に反映
2024年10月	Web会議等の目的で、業務端末からインターネット経由で、特定のクラウドサービスを安全に利用するための対策や、政府統一基準の改定内容に沿った業務委託時における対策、地方公共団体が取り扱う個人情報の重要性を鑑みて、個人情報を自治体機密性３分類に分類することを追加
2025年３月	令和６年６月の「国・地方ネットワークの将来像及び実現シナリオに関する検討会報告書」を踏まえたマイナンバー利用事務系に係る画面転送の方式やLGWAN接続系・マイナンバー利用事務系における無線LAN利用の要件等について新たに規定

クラウドサービス等に係るガイドラインの策定

- 総務省は、下記に示すとおり、**クラウドサービスのセキュリティに関するガイドライン**等を策定・公表
- これらのガイドラインの一部は、**地方自治体が情報セキュリティポリシーの策定や見直しを行う際の参考とする「地方公共団体における情報セキュリティポリシーに関するガイドライン(令和７年３月版)」（2025年3月28日公表）において、引用**

  引用されているガイドライン例： クラウドサービス提供における情報セキュリティ対策ガイドライン
  クラウドサービス利用・提供における適切な設定のためのガイドライン

① 2021年９月「クラウドサービス提供における情報セキュリティ対策ガイドライン」（第３版）

IoT技術の急速な進展や、IoT機器ベンダーが提供する付加価値サービスの急増に伴い、利用者に対して提供されるサービスのサプライチェーンや契約構造にも明確な変革が見られるようになったことを踏まえて改定

② 2022年10月「クラウドサービス利用・提供における適切な設定のためのガイドライン」

設定不備を原因とする不正アクセスが多く見られる中で、利用者の理解不足や、提供事業者側の情報提供不足など、利用側・提供側双方において設定不備を発生させない対策の推進が必要であることから、クラウドサービスの「設定」に特化したガイドラインを策定

③ 2024年４月「クラウドの設定ミス対策ガイドブック」

「クラウドサービス利用・提供における適切な設定のためのガイドライン」を平易に解説するガイドブックを策定

④ 2024年６月「スマートシティセキュリティガイドライン（第 3.0 版）」

スマートシティの推進のための指針として、多様な関係主体が講じるべきセキュリティ対策や留意事項等を示し、スマートシティのセキュリティの考え方やスマートシティを実現する上で実施することが推奨されるセキュリティ対策等について整理。内閣府が示すスマートシティリファレンスアーキテクチャの改定に対応するために改定

eシールの検討状況

- ✓ 2019年から、総務省で、トラストサービスなどデータ信頼性の確保等に関する検討を開始。

□ 2021年６月、総務省で、「**eシールに係る指針**」策定。
- ｅシールに係る技術や運用等に関する一定の基準を示す

- ✓ 2023年9月、総務省がeシールに係る認定（大臣認定）制度の創設に向けた検討を開始。

□ 2024年４月、総務省で、「**ｅシールに係る指針（第２版）**」を公表。
- ｅシールの定義･ユースケースの明確化等や保証レベルの区分等を追記

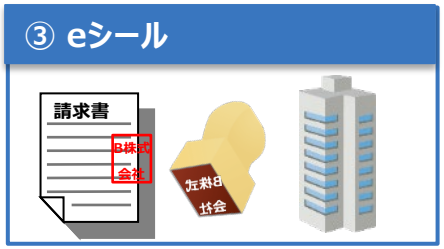
- ✓ 2024年６月公表の政府戦略において、「電子データの発行元組織を示すｅシールの認定制度を本年度中に創設」することとされた。
（「新しい資本主義のグランドデザイン及び実行計画 2024改訂版」 2024年6月21日閣議決定）
- ✓ 2024年６月より、総務省で、「eシールに係る認定制度の関係規程策定のための有識者会議」を開催。

□ **2025年3月**に、総務省で、**ｅシール認定制度の告示、実施要項及びガイドラインを制定。**
- ✓ **2025年度内に指定調査機関を指定し、制度運用を開始するとともに、順次認定申請の受け入れを開始予定。**

・署名者の意思を確認できる仕組み

・データの存在証明の仕組み

・文書の発行元を確認できる仕組み



<eシールのユースケース例※１>

	企業間取引関係	組織等が公開する情報	組織等が発出する証明書	官民間のやりとり	監査関係	その他
高 ↕ 保証レベル２ ※２			• 資格証明書（排他的独占業務とされている士業等）等 • 商工会議所が発行する貿易関係書類	• 公的機関が発行する書類のうち、特になりすましや改ざんを防止する必要のある書類 • 国への各種申請書類等	• 財務状況を示す資料（財務諸表等） • 残高証明書	
	• 領収書 • 請求書	• 気象データ • IR関連資料 • 広報資料	• 健康診断結果証明書	• 請負、委託業務の成果物		• 情報連携基盤・クラウド環境等でやり取りされるデータ
↕ 保証レベル１ ※３	• 見積書 • 納品書 • 受領書 • デジタル名刺 • 企業間でやりとりされる一般的なデータ		• 生産者証明書 • 在学、卒業証明書 • 加工証明書 • 機器の保証書、その他証明書 • ライセンス証書			• 機器測定ﾃﾞｰﾀ

※１　本ユースケース例については現時点での目安であり、今後、各種法令や制度の改正等に伴って変更の可能性あり。
※２　総務大臣の認定を経たeシール認証業務によって保証されるeシール。
※３　総務大臣による認定を経ずに、より低コスト･簡易な手続で大量発行されるeシール。

1．重要インフラ等におけるサイバーセキュリティの確保

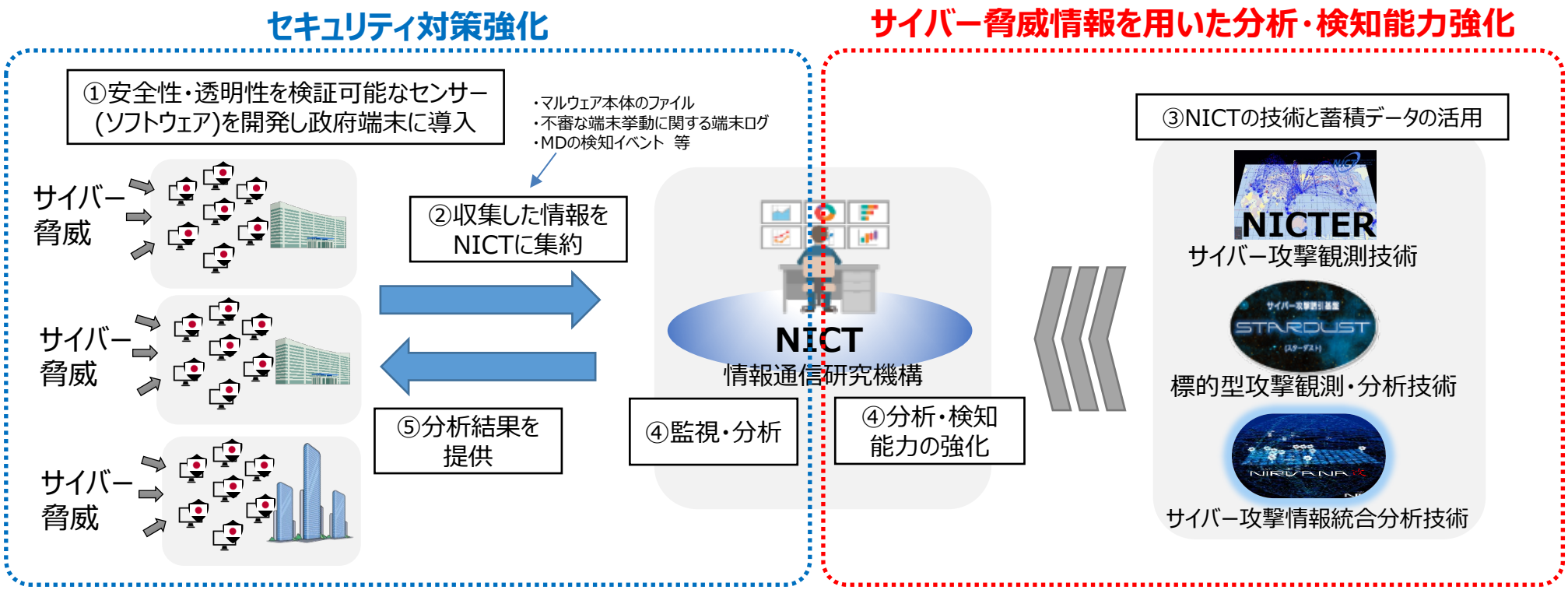
2．**サイバー攻撃対処能力の向上と新技術への対応**

3．地域をはじめとするサイバーセキュリティの底上げに向けた取組

4．国際連携の更なる推進
（国際連携全般、人材育成支援）

政府端末情報を活用したサイバーセキュリティ情報の収集・分析

- 総務省では、2022年度から、安全性や透明性の検証が可能なセンサーを政府端末に導入してサイバーセキュリティ情報を収集し、NICTの能力を活用して分析する実証事業である“CYXROSSプロジェクト”を開始。センサー導入先の府省庁のサイバーセキュリティを強化しつつ、NICTが開発した様々な技術や観測等で蓄積したデータも活用し、我が国独自のサイバーセキュリティに関する情報を生成。
- サイバーセキュリティ基本法の改正を踏まえ、今後は、監視・分析等の各省のセキュリティ対策強化部分をサイバーセキュリティ戦略本部委託事業として、大局的なサイバー脅威情勢分析や検知能力強化などの研究開発・技術開発部分を総務省補助事業として実施



総務省実証事業として実施

サイバーセキュリティ戦略本部委託事業として実施

総務省研究開発事業として実施

ナショナルサイバートレーニングセンターを通じた人材育成の推進

- 高度化するサイバー攻撃に対して我が国のサイバー対処能力を強化するため、国立研究開発法人情報通信研究機構（NICT）の「ナショナルサイバートレーニングセンター」を通じて、NICTの有する知見を活用した、実践的なセキュリティ人材の育成を推進。

① 実践的サイバー防御演習「CYDER」

- 国や地方公共団体、独立行政法人、重要インフラ事業者等の情報システム担当者等を対象に、実践的サイバー防御演習（CYDER）を実施。2024年度は4,225名が集合演習を受講。

※CSIRT 担当者が知っておくべき基礎的な事項を短時間で習得できる「プレCYDER」についても2023年度より本格実施。2024年度は4,058名が受講。

② 万博向けサイバー防御演習「CIDLE」

- 2025年大阪・関西万博に向け、 2023年度から万博関連組織の情報システム担当者等を対象として万博向けサイバー防御講習「CIDLE（シードル）」を実施。

③ 分野別演習開発プラットフォーム「CYROP」

- サイバーセキュリティ演習に必要となる基盤（仮想環境、演習教材等）を大学、民間企業等へ開放。2024年度までに66組織が参画、利用。

④ 若手セキュリティ人材育成プログラム「SecHack365」

- 若手ICT人材を対象とした通年の研究指導プログラム（SecHack365）を通じて、革新的な国産セキュリティ技術の開発を担う人材の育成を推進。2024年度は39名が修了。

実践的サイバー防御演習
CYDER

万博向け
サイバー防御演習
CIDLE

分野別演習開発
プラットフォーム
CYROP

演習基盤を産学官に開放、分野別演習を開発

若手セキュリティ人材
育成プログラム
SecHack365

AIとサイバーセキュリティに係る取組

➢ 生成AI等のAI技術を巡る最新動向を把握しつつ、**AIに起因するセキュリティリスクを可能な限り回避・低減するための「Security for AI」**に取り組むとともに、**AIをセキュリティ対策に効果的に活用するための「AI for Security」**に取り組むことが重要

生成AIの負の影響

サイバー攻撃に悪用される可能性

（例）
- 生成AI利用によるフィッシングメールの巧妙化
- マルウェアの生成、亜種の大量生産

生成AIへのサイバー攻撃・脆弱性内包

（例）
- リスクにつながる悪意のある入力
- 事業者設定ミスによる安全ではない出力処理

Security for AI
安心安全な利用の促進

① **生成AIの進展によるサイバーセキュリティへの影響に係る調査・検証**
- AIの安心・安全な開発・提供に向けたセキュリティのガイドラインの策定

＜実例検証＞

② **米国専門機関とのAI安全性に関する共同研究事業**
- AIの安全性に係る分野の研究開発を推進するため、北米にNICTの研究拠点を構築し、米国等の様々な専門機関との共同研究事業を実施

＜理論研究＞

生成AIの正の影響

サイバー攻撃対策への活用の可能性

（例）
- サイバー防御の自動化
- セキュリティレポート作成の自動化
- 脅威インテリジェンスの精度向上
- 脆弱性のない安全なコード開発の支援
- サイバー攻撃の予見
- インシデント対応の支援

AI for Security
サイバーセキュリティ対策への活用

③ **AIを用いたサイバー脅威情報収集・分析の高度化**
- 世界中の様々な機関等から発信されるサイバー脅威情報をAIを活用して収集・分析するための技術を開発及び展開

＜平時の分析活動＞

④ **生成AI等を活用した重要インフラ分野におけるサイバーセキュリティ対策強化**
- 生成AI等を活用した攻撃インフラ分析の精緻化・迅速化の検証
- 当該情報等を用いた対処オペレーション業務の効率化・迅速化の検証とノウハウの展開

＜攻撃インフラ特定＞

NICTにおけるAI×サイバーセキュリティ推進体制（CREATE）

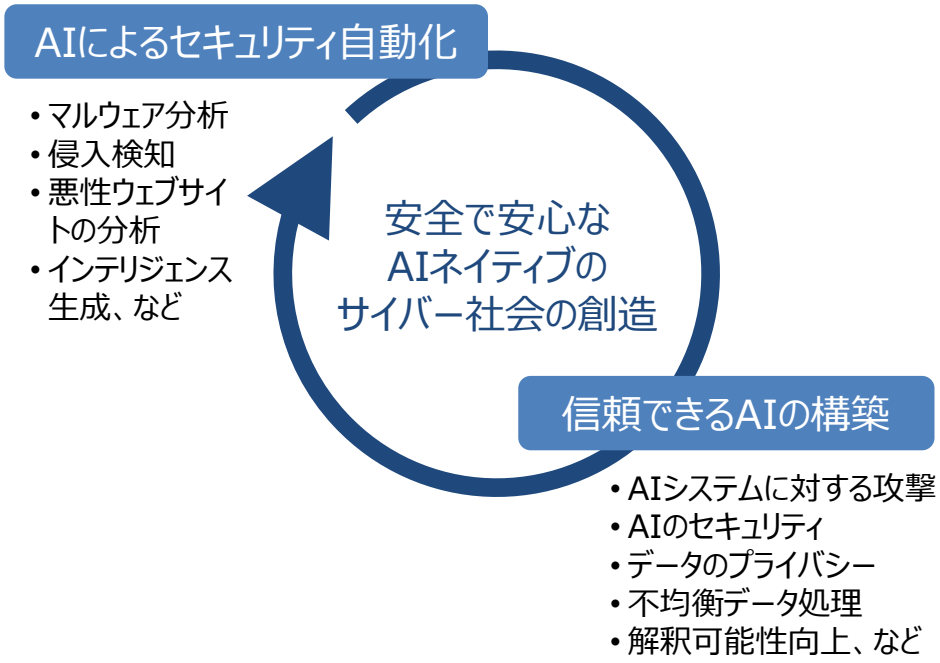
CREATE設立の背景

- AIセキュリティは国の重要課題。NICTは研究開発と国際連携の両面で貢献を求められる
- この分野における戦略的な技術力強化が必要不可欠

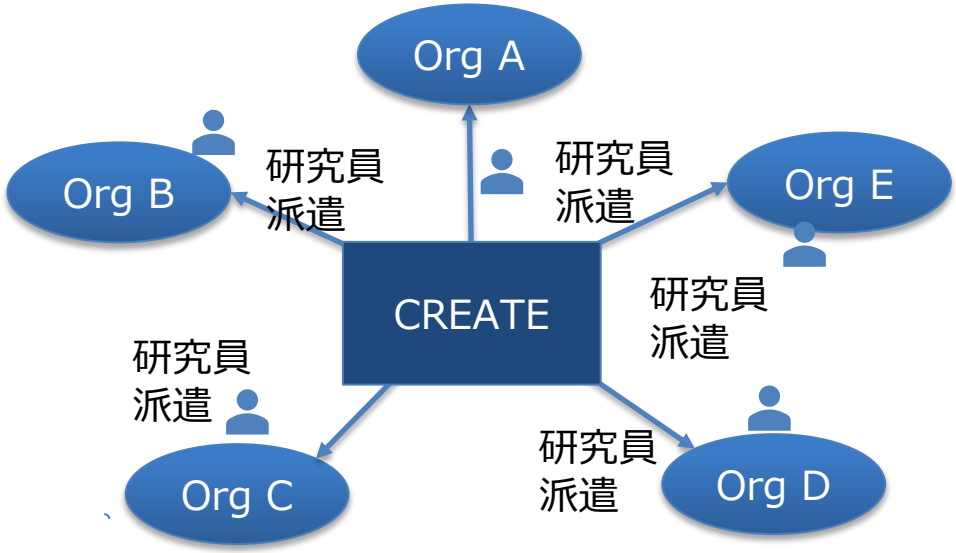
AIセキュリティ研究開発力を強化すべく、2025年2月1日サイバーセキュリティ研究所内にAIセキュリティ研究センター（CREATE）を設立

CREATEの3つの業務領域

1 AIセキュリティに関する研究開発



2 AIセキュリティの研究開発を加速する国際的なコミュニティの形成（研究開発を通じてAIセキュリティ分野における強固な北米連携を実現）



3 AIセキュリティに関する情報収集と情報発信

耐量子計算機暗号(PQC)に係る検討状況

- 米国NIST(国立標準技術研究所)は、2024年８月にPQCの暗号アルゴリズム３方式（FIPS203,204,205）を公開。
- 一方、我が国において、CRYPTREC※が2025年３月にPQCの安全性評価・実装性能評価に関する活動を開始。
- また、政府は、**政府機関等におけるPQC利用**に関し、関係府省庁の緊密な連携のもと、必要な施策を検討・推進するため、**関係府省庁連絡会議**を2025年６月30日に立ち上げ。

※ CRYPTREC（クリプトレック）はデジタル庁・総務省・経済産業省が共同運営する、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト。

○米国NISTの標準化済（予定含む）のPQC暗号アルゴリズム

暗号アルゴリズム	改称前	暗号ベース	用途
FIPS 203 (ML-KEM)	CRYSTALS-Kyber	格子暗号ベース	暗号化・鍵交換用途
FIPS 204 (ML-DSA)	CRYSTALS-Dilithium	格子暗号ベース	署名用途
FIPS 205 (SLH-DSA)	SPHINCS+	ハッシュ関数ベース	署名用途
FIPS 206 (FN-DSA) ※標準化予定	FALCON	格子暗号ベース	署名用途

○サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項 令和７年５月29日 サイバーセキュリティ戦略本部

量子技術については、その進展に伴い、現在広く使われている公開鍵暗号の危殆化が懸念されているところ。そのため、諸外国や暗号技術検討会（CRYPTREC）における検討状況を踏まえ、多岐にわたる課題に対応するための関係省庁による検討体制を立ち上げ、**政府機関等における耐量子計算機暗号（PQC）への移行の方向性について、次期サイバーセキュリティ戦略**に盛り込む。

○耐量子計算機暗号(PQC)利用に関する関係府省庁連絡会議

＜参加者＞

議長　内閣官房副長官補（内政担当）
副議長　内閣官房内閣審議官（国家安全保障局）
　内閣官房内閣審議官（NCO）
主査　デジタル庁統括官（デジタル社会共通機能担当）
　総務省サイバーセキュリティ統括官
　経済産業省商務情報政策局長
構成員　内閣官房内閣審議官（内閣官房副長官補付）
　内閣府科学技術・イノベーション推進事務局統括官
　警察庁長官官房技術総括審議官
　デジタル庁統括官（戦略・組織担当）
　外務省大臣官房サイバーセキュリティ・情報化参事官
　文部科学省研究振興局長
　経済産業省イノベーション・環境局長
　防衛省大臣安房サイバーセキュリティ・情報化審議官
※会議は非公開（議事要旨及び配付資料は原則公開）

＜スケジュール＞

令和７年６月30日
　第１回関係府省庁連絡会議
　○検討開始

令和７年７～11月
　○課長級会合による検討

令和７年11月頃
　第２回関係府省庁連絡会議
　○工程表(ロードマップ)の骨子

令和８年度中
　第３回関係府省庁連絡会議
　○工程表(ロードマップ)の策定

＜検討すべき論点＞

○量子計算機の開発・普及状況、危殆化する公開鍵暗号等の特定とその時期
○諸外国の動向の把握
○PQCの安全性等の評価・確認とその時期
○PQCへの移行期限及び危殆化した公開鍵暗号等の利用に係る停止の時期
○政府機関等の移行への対応に必要な支援策等
○政府機関等の移行にむけた工程表（ロードマップ）の策定　など

1．重要インフラ等におけるサイバーセキュリティの確保

2．サイバー攻撃対処能力の向上と新技術への対応

3．地域をはじめとするサイバーセキュリティの底上げに向けた取組

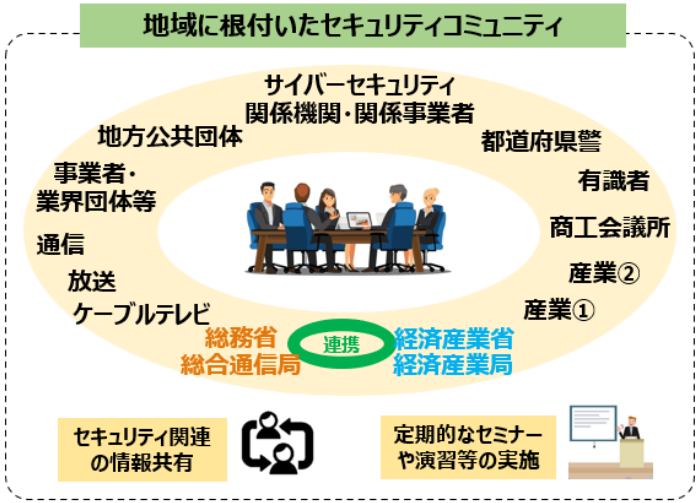
4．国際連携の更なる推進
（国際連携全般、人材育成支援）

地域に根付いたセキュリティコミュニティ（地域SECUNITY）の形成促進

➢ 総務省、経済産業省が互いに連携しつつ、**地域単位の事業者のセキュリティ対策の強化のため、地域に根付いたセキュリティコミュニティ（地域SECUNITY（セキュニティ））の形成を促進**

※ 2024度は、サイバーセキュリティに関するセミナー（20回、受講者1407名）、インシデント演習（14回、受講者389名）、地域型CTF（３回、受講者58名）、全国型CTF（７会場、受講者406名）の開催を支援

（CTF：Capture The Flagの略で、ゲーム形式でセキュリティの実践的技能を競うコンテストを行う）



インシデント演習の開催例

- 昨今話題となっているインシデント事例への対応について講師から解説があった後、疑似的なインシデント対応を机上演習として体験
- インシデント発生時からの一時対応の検討、情報連携、評価までのサイクルを、参加者が互いにディスカッション・意思決定しながらグループワーク形式で進めていく

「サイバーインシデント演習 in 大阪」（2025.3.6開催）

出典：近畿総合通信局ウェブサイト

【各地域の連絡会】

名称	事務局
北海道地域情報セキュリティ連絡会	北海道総合通信局、北海道経済産業局、北海道警察本部
東北地域サイバーセキュリティ連絡会	東北総合通信局、東北経済産業局
関東サイバーセキュリティ連絡会	関東総合通信局、関東経済産業局
信越サイバーセキュリティ連絡会	信越総合通信局、関東経済産業局
北陸サイバーセキュリティ連絡会	北陸総合通信局
東海サイバーセキュリティ連絡会	東海総合通信局、中部経済産業局

名称	事務局
関西サイバーセキュリティ・ネットワーク	近畿総合通信局、近畿経済産業局、(一財)関西情報センター
中国地域サイバーセキュリティ連絡会	中国総合通信局、中国経済産業局
四国サイバーセキュリティネットワーク	四国総合通信局、四国経済産業局
九州・沖縄地域情報セキュリティ推進連絡会議	九州総合通信局、九州経済産業局
沖縄サイバーセキュリティネットワーク	内閣府沖縄総合事務局、沖縄総合通信事務所、沖縄県警察本部

1. 重要インフラ等におけるサイバーセキュリティの確保

2. サイバー攻撃対処能力の向上と新技術への対応

3. 地域をはじめとするサイバーセキュリティの底上げに向けた取組

4. 国際連携の更なる推進
（国際連携全般、人材育成支援）

インド太平洋地域における開発途上国・地域に対する能力構築支援

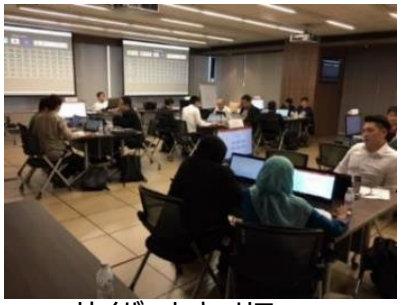
➢ 地理的に重要な**ASEAN地域や大洋州島しょ国・地域**に向けて**サイバーセキュリティ能力構築支援**を実施し、地域内のサイバーセキュリティ能力を底上げすることで、**自由で開かれたインド太平洋（FOIP）の実現に貢献**

＜ASEANにおけるサイバーセキュリティ能力構築支援＞

- 我が国がASEANと共同で、2018年に**日ASEANサイバーセキュリティ能力構築センター(AJCCBC)**をタイに設置。以来、ASEAN10カ国の政府機関・重要インフラ事業者等に対し、**実践的サイバー防御演習「CYDER」（NICTが開発）**等を実施（JICA技術協力支援）。
- 2025年5月時点で**約2,700名が受講**。
- AJCCBCでは、同志国によるサイバーセキュリティ演習も実施しており、米国・欧州各国が協力。
- 2025年度からは、ランサムウェア※によるサイバー攻撃に対応した演習を提供予定。

※サーバーや端末などに保存されているデータを暗号化して使用できない状態にして、そのデータを復号する鍵と引き換えに金銭を要求する攻撃

AJCCBC
ASEAN JAPAN CYBERSECURITY CAPACITY BUILDING CENTRE



サイバーセキュリティ演習模様

Cyber SEA Game模様

＜大洋州島しょ国・地域におけるサイバーセキュリティ能力構築支援＞

- 2024年２月、**AJCCBCの運用で培ったスキルやノウハウを活用**して立ち上げた**大洋州島しょ国を対象としたサイバーセキュリティ能力構築支援（演習事業）**を実施。
  （パラオ、ミクロネシア、マーシャル諸島、ナウル、キリバスの5カ国が参加）
- 2024年度は**対象国・地域を拡大**し、2024年10月にフィジー、2025年2月にグアムで演習実施。

2024年度第1回演習参加者集合写真

2024年度演習参加国・地域:パプアニューギニア、フィジー、サモア、ソロモン諸島、バヌアツ、トンガ、ナウル、ツバル、ミクロネシア連邦、パラオ、マーシャル諸島、キリバス、クック諸島、仏領ポリネシア

【参考】「ICTサイバーセキュリティ政策の中期重点方針」（2024年7月31日公表）

➢ 総務省では、2024年２月から「ICTサイバーセキュリティ政策分科会」（主査：後藤厚宏　情報セキュリティ大学院大学学長）を開催し、総務省が取り組むべきサイバーセキュリティ政策について、2030年頃も見据えた中長期的な方向性について検討。

【政府の主な動き】

- **国家安全保障戦略**
- **経済安全保障推進法の施行（特定社会基盤事業者の指定等）　等**

【サイバーセキュリティを巡る主な課題】

- **厳しさを増す国際情勢とサイバー攻撃リスクの高まり**
- **多様化・複雑化するサプライチェーンとアタックサーフェス（攻撃対象領域）の増加**
- **セキュリティ人材の確保**
- **生成AI等の新たな技術への対応**

１．重要インフラ等におけるサイバーセキュリティの確保

- 通信分野（総合的なIoTボットネット対策（新NOTICEの推進やC&Cサーバの検知・対処能力の向上）、スマートフォンアプリのセキュリティ対策やサプライチェーン対策の推進等）
- 放送分野（安全・信頼性に関する新たな技術基準に基づくセキュリティ対策の着実な推進等）
- 自治体分野（クラウド化・標準化等の環境変化を見据えた人材育成やCSIRT能力向上の取組等）
- クラウドセキュリティの確保やトラストサービス（eシールの認定制度を2024年度中に創設等）の推進

２．サイバー攻撃対処能力の向上と新技術への対応

- CYNEX・CYXROSSを強力に推進し、国産のサイバーセキュリティ情報・技術による自律的なサイバーセキュリティ対処能力を抜本的に強化
- CYXROSSとGSOCとの連携により政府システムの一元的な監視体制の構築に貢献
- CYDER等を通じた国や地方公共団体等におけるCSIRT対処能力の抜本的強化
- サイバーセキュリティ研究分野の国際競争力向上を図るため、NICT内に米国との連携を強化するための結節点を形成
- 生成AI等の新技術への対応（AIを起因とするセキュリティリスクの回避・低減に向けた取組、AIを活用したサイバーセキュリティ対策の促進、耐量子計算機暗号技術（PQC）等の研究開発等の推進）

３．地域をはじめとするサイバーセキュリティの底上げに向けた取組

- 地域SECUNITYの活動強化（他機関との更なる連携、持続的な推進体制の整備等）
- 各種ガイドラインの周知啓発等

４．国際連携の更なる推進（国際連携全般、人材育成支援）

- 日ASEANサイバーセキュリティ能力構築センター（AJCCBC）の活動強化（プログラムの拡充、有志国との連携強化等）
- 大洋州島しょ国向け人材育成支援プロジェクトの2025年度以降の本格的な実施