

Ⅲ 信頼できる情報通信環境の整備

Ⅱ. サイバーセキュリティ対策の強力な推進

(1) 生成AI等を活用したセキュリティの確保

生成AI等を活用したサイバーセキュリティ対策強化

- サイバー攻撃対処能力の向上に向け、サイバー脅威情報の収集・分析や生成AI等を活用した攻撃インフラの検知の精緻化・迅速化を行うとともに、セキュリティ分野におけるAIの安全かつ効果的な開発・提供に向けたガイドラインの策定等のほか、NICTと米国等の様々な専門機関との連携によるAI安全性の研究開発を実施する。

【予算】 生成AI等を活用したサイバーセキュリティ対策強化
6年度補正 21.5億円（新規）

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、垂種の大量生産

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
- LLMの学習データの汚染
- 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

- 生成AIがサイバーセキュリティに与える負の影響の検証・評価
- 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MITRE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>

Ⅲ 信頼できる情報通信環境の整備

Ⅱ. サイバーセキュリティ対策の強力な推進

(2) 国や自治体、医療分野等でのセキュリティ人材育成

ナショナルサイバートレーニングセンターにおける人材育成

- ・ 巧妙化・複雑化するサイバー攻撃に対応できるサイバーセキュリティ人材を育成するため、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」において、以下の事業を実施。
 - － 国や地方公共団体、独立行政法人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実践的サイバー防御演習（CYDER）を実施。
 - － 25歳以下の若手ICT人材を対象として、新たなセキュリティ対処技術を生み出しうる最先端のセキュリティ人材であるセキュリティイノベーターを育成（SecHack365）。

【予算】 ナショナルサイバートレーニングセンターの強化
12.0億円（6年度 17.4億円）



Ⅲ 信頼できる情報通信環境の整備

11. サイバーセキュリティ対策の強力な推進

(2) 国や自治体、医療分野等でのセキュリティ人材育成

サイバーセキュリティ統合知的・人材育成基盤の構築

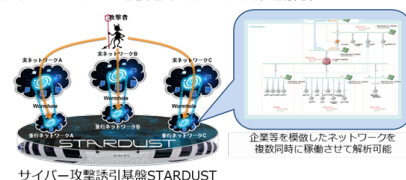
- 国立研究開発法人情報通信研究機構 (NICT) を中核として、サイバーセキュリティ情報を国内で収集・蓄積・分析・提供するとともに、社会全体でサイバーセキュリティ人材を育成するための共通基盤 CYNEX を産学官の結節点として開放することで、我が国全体のサイバーセキュリティ対応能力の向上を図る。



【予算】 サイバーセキュリティ統合知的・人材育成基盤の構築
9.0億円（6年度 8.5億円）

Co-Nexus A (Accumulation & Analysis)

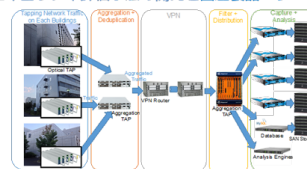
- 目的: STARDUSTを核としたデータ収集と解析



サイバー攻撃誘引基盤STARDUST

Co-Nexus E (Evaluation)

- 目的: セキュリティ評価手法の開発と国産製品・サービスの評価



国産セキュリティ製品テスト環境 (例: 機内ネットワーク観測システム)

Co-Nexus S (Security Operation & Sharing)

- 目的: SOC人材の育成とCYNEX独自の脅威情報の生成・発信



オンライン研修によるSOC人材育成 OJTによるSOC人材育成 国産脅威情報の生成・発信 ※SOC(Security Operation Center): 企業等に設置されたセキュリティ部門やチーム

Co-Nexus C (CYROP)

- 目的: 教材開発とCYROP提供によるセキュリティ人材育成促進



サイバーセキュリティ演習基盤CYROP

CYNEXオリジナル演習教材

Ⅲ 信頼できる情報通信環境の整備

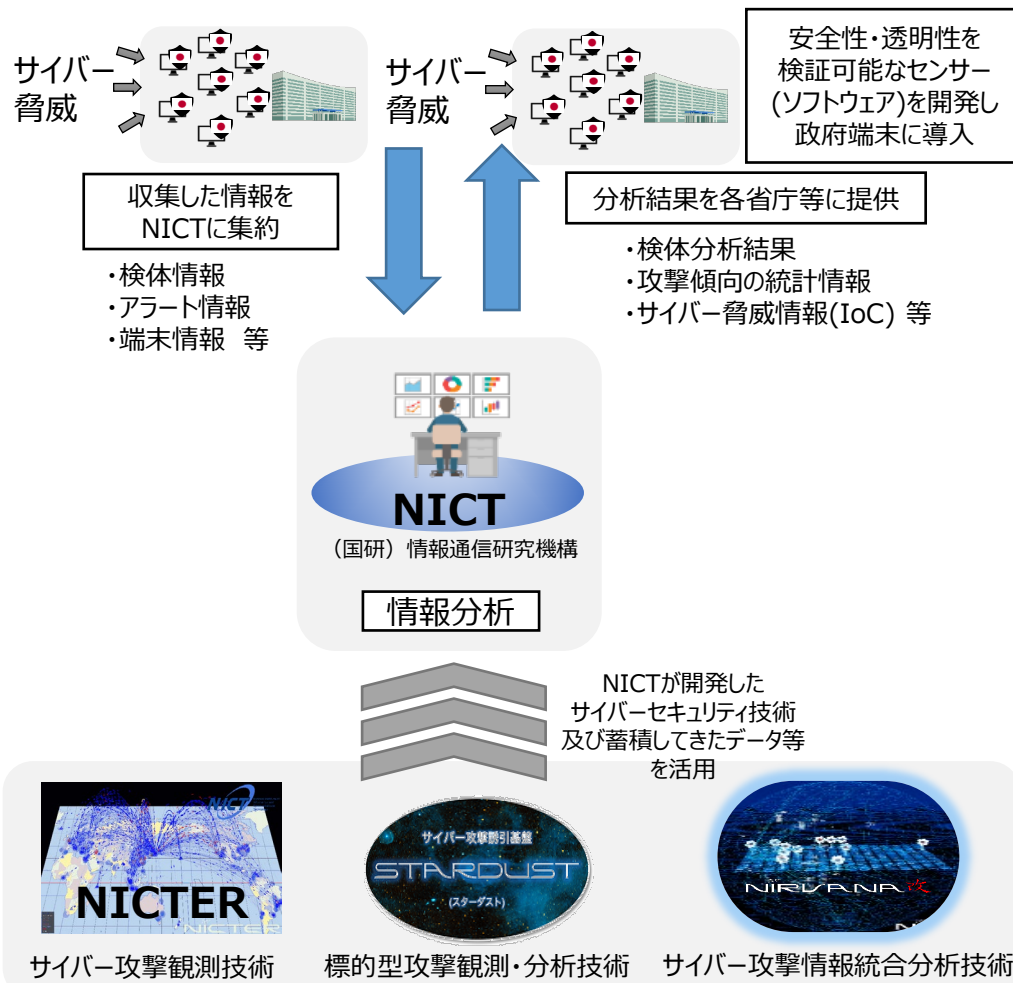
Ⅱ. サイバーセキュリティ対策の強力な推進

(3) 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

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・分析に係る実証事業

- 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、国立研究開発法人情報通信研究機構（NICT）の能力を活用して分析する実証事業を実施。
- 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。

【予算】 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・分析に係る実証事業
13.0億円（6年度 10.0億円）



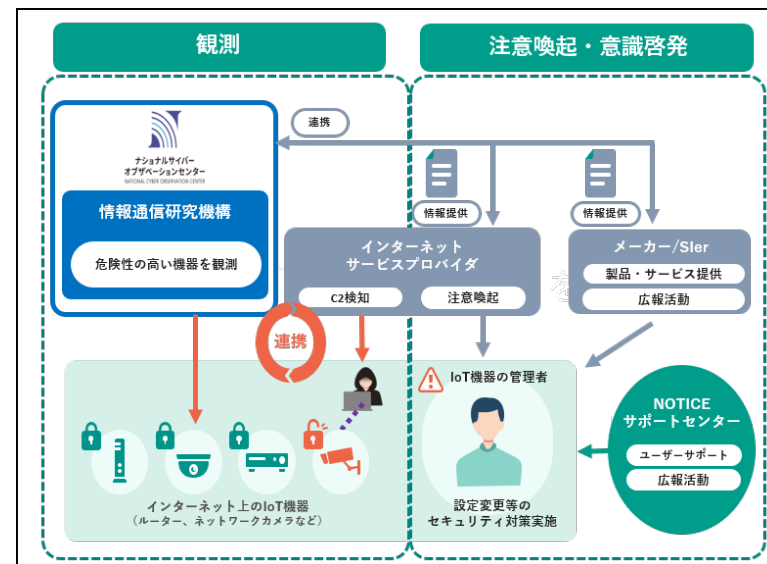
Ⅲ 信頼できる情報通信環境の整備

Ⅱ. サイバーセキュリティ対策の強力な推進

(4) 総合的なIoTセキュリティ対策の強化 / (5) 諸外国のサイバーセキュリティ関連制度等の調査研究

IoTセキュリティ対策の強化

- 国立研究開発法人情報通信研究機構（NICT）によるサイバー攻撃及びサイバー攻撃に悪用されうる様々な脆弱性を有するIoT機器の調査、並びにインターネットサービスプロバイダ（ISP）等によるIoTボットネットの観測を踏まえ、IoT機器管理者への注意喚起、様々な関係者との連携による対処の促進及びIoT機器のセキュリティ対策の周知啓発を行うNOTICE等の取組を実施する。また、サイバー攻撃の脅威の高まりに対応するため、更なる調査・観測能力、相互連携の強化を図ることで、IoTの安心・安全かつ適正な利用環境を整備する。



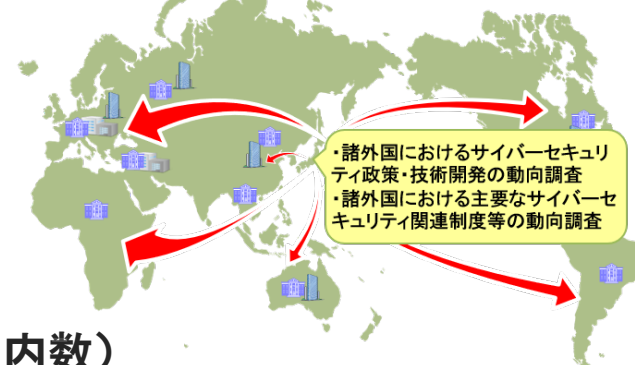
【予算】IoTの安心・安全かつ適正な利用環境の構築
15.8億円の内数 （6年度 15.8億円の内数）

諸外国のサイバーセキュリティ関連制度等の調査研究

- サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるため、サイバーセキュリティに関する新たな脅威とその対策等に関して、諸外国における関連制度等に係る調査・研究を行う。

【予算】サイバーセキュリティ政策に関する調査研究

6年度補正 0.8億円 7年度 2.5億円（6年度 2.5億円の内数）



Ⅲ 信頼できる情報通信環境の整備

Ⅱ. サイバーセキュリティ対策の強力な推進

(6) 自治体の情報セキュリティ向上

自治体の情報セキュリティ向上

- 今年6月に成立した改正地方自治法に新たに位置づけられた、総務大臣の責務を果たすことと、「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」報告書で提示された令和12年頃の将来像への円滑な移行のため、以下を実施。
 - セキュリティインシデントを早期発見する仕組み（自治体情報セキュリティクラウド）の構築
 - 自治体システムの脆弱性を検証するための実証事業（ペネトレーションテスト）等
 - 将来像の実現に向けた調査研究

【予算】

自治体の情報セキュリティ向上に係る経費
6年度補正 ①3.0億円 ②1.9億円（新規）

【再掲】

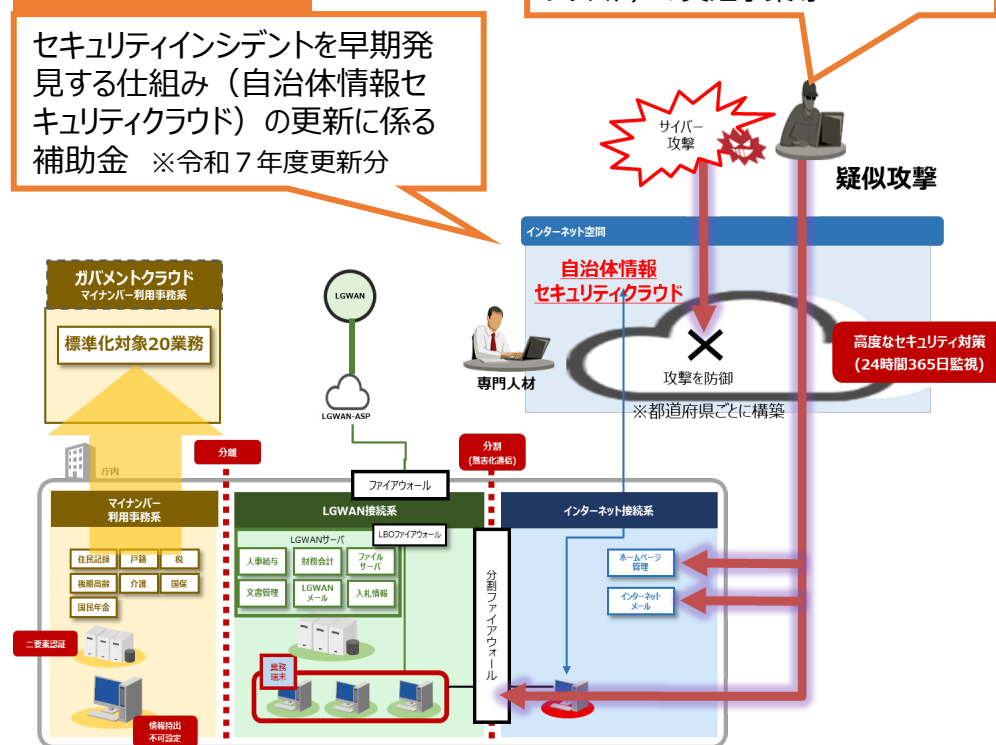
自治体の情報セキュリティ対策の
強化に対する調査研究費
0.7億円（6年度 0.7億円）【再掲】

令和6年度補正①

セキュリティインシデントを早期発見する仕組み（自治体情報セキュリティクラウド）の更新に係る補助金 ※令和7年度更新分

令和6年度補正②

実際にネットワークへの攻撃を試み、脆弱性を検証するテスト（ペネトレーションテスト）の実証事業等



令和7年度当初

- ✓総務省は、各自治体のセキュリティ対策の指針として、「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」を策定し、助言。
- ✓「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」報告書で将来像として示された、ゼロトラストアーキテクチャの考え方の導入のため、調査・分析・検証を行った上でガイドラインについて検討を実施。