政府のサイバーセキュリティに関する予算

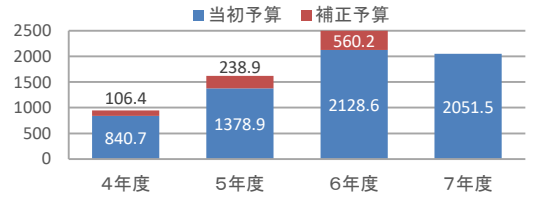
資料６

令和7年度当初予算額

2，０５１．５億円

（令和6年度当初予算額　２,１２８．６億円）

注１）サイバーセキュリティに関する予算として切り分けられない場合には計上していない。
注２）（　）内の数字は記載の主な施策例以外も含めたそれぞれの項目の総計



サイバーセキュリティ戦略における各分野ごとの主な施策例及び予算額

	令和7年度当初予算	令和6年度補正予算	令和6年度当初予算
（１）経済社会の活力の向上及び持続的発展	(97.3億円)	(27.7億円)	(63.2億円)
【経済産業省】産業サイバーセキュリティ対策の強化に向けた環境整備事業	54.1億円	―	44.0億円
【総務省】IoTの安心・安全かつ適正な利用環境の構築	15.8億円	―	15.8億円
【総務省】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	―	10.0億円
【総務省】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	―	8.5億円
（２）国民が安全で安心して暮らせるデジタル社会の実現	(363.3億円)	(283.0億円)	(385.4億円)
【厚生労働省】厚生労働省及び関係機関等における情報セキュリティ対策推進費	32.2億円	90.4億円	19.5億円
【外務省】情報セキュリティ対策の強化	15.0億円	2.2億円	11.2億円
【内閣官房】政府機関情報セキュリティ横断監視・即応調整チームの運用	16.0億円	―	9.8億円
【総務省】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	―	17.4億円
【国土交通省】航空管制セキュリティシステム	11.6億円	―	14.0億円
【内閣官房】各府省庁等の情報システムに対するマネジメント監査及びペネトレーションテスト	5.7億円	―	0.4億円
【内閣官房】独立行政法人及び指定法人におけるサイバーセキュリティ施策の評価委託	5.1億円	―	0.4億円
【内閣官房】政府機関等に対するサイバーセキュリティの実践的検証	5.0億円	19.7億円	―
【警察庁】サイバー捜査用資機材の増強等	2.8億円	6.9億円	3.1億円
【経済産業省】政府情報システムのためのセキュリティ評価事業	2.8億円	―	2.8億円
【内閣官房】重要インフラ分野の演習等企画実施	2.4億円	―	0.4億円
【こども家庭庁】こども家庭庁におけるセキュリティ対策体制強化費	0.8億円	―	0.3億円
【デジタル庁】サイバーセキュリティ確保環境整備費	1.3億円	―	1.3億円
【金融庁】金融業界横断的なサイバーセキュリティ演習の実施	0.9億円	0.2億円	0.8億円
【警察庁】生成ＡＩ等を活用したフィッシングサイト判定の高度化・効率化	0.3億円	―	―
【総務省】地方公共団体の情報セキュリティ対策の強化	―	3.0億円	―
【総務省】地方公共団体の情報セキュリティ対策の見直し	―	1.9億円	―
【総務省】地方公共団体の情報セキュリティ対策の推進	0.7億円	―	0.7億円
【国土交通省】国土交通省（CSIRT等）や所管事業者における情報セキュリティ対策の強化	0.6億円	5.0億円	0.6億円

政府のサイバーセキュリティに関する予算

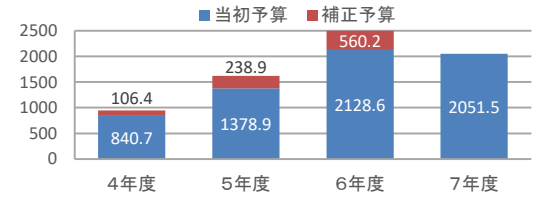
表紙

令和7年度当初予算額

2，０５１．５億円

（令和6年度当初予算額　２,１２８．６億円）

注１）サイバーセキュリティに関する予算として切り分けられない場合には計上していない。
注２）（　）内の数字は記載の主な施策例以外も含めたそれぞれの項目の総計



サイバーセキュリティ戦略における各分野ごとの主な施策例及び予算額

	令和7年度当初予算	令和6年度補正予算	令和6年度当初予算
（３）国際社会の平和・安定及び我が国の安全保障への寄与	(1388.3億円)	(0.6億円)	(1,522.1億円)
【防衛省】情報システムの防護	876.3億円	—	1064.0億円
【防衛省】リスク管理枠組み（RMF）の導入	340.8億円	—	290.8億円
【防衛省】防衛産業におけるサイバーセキュリティ対策の強化	134.2億円	—	119.8億円
【外務省】サイバー空間に関する外交及び国際連携	0.3億円	—	0.7億円
（４）横断的施策（人材育成等）	(168.7億円)	(38.6億円)	(128.4億円)
【防衛省】サイバー分野における教育機能の強化	25.4億円	—	25.5億円
【文部科学省】GIGAスクールにおける学びの充実	1.6億円	2億円	3.2億円
【総務省】生成ＡＩ等を活用したサイバーセキュリティ対策強化	—	21.5億円	—

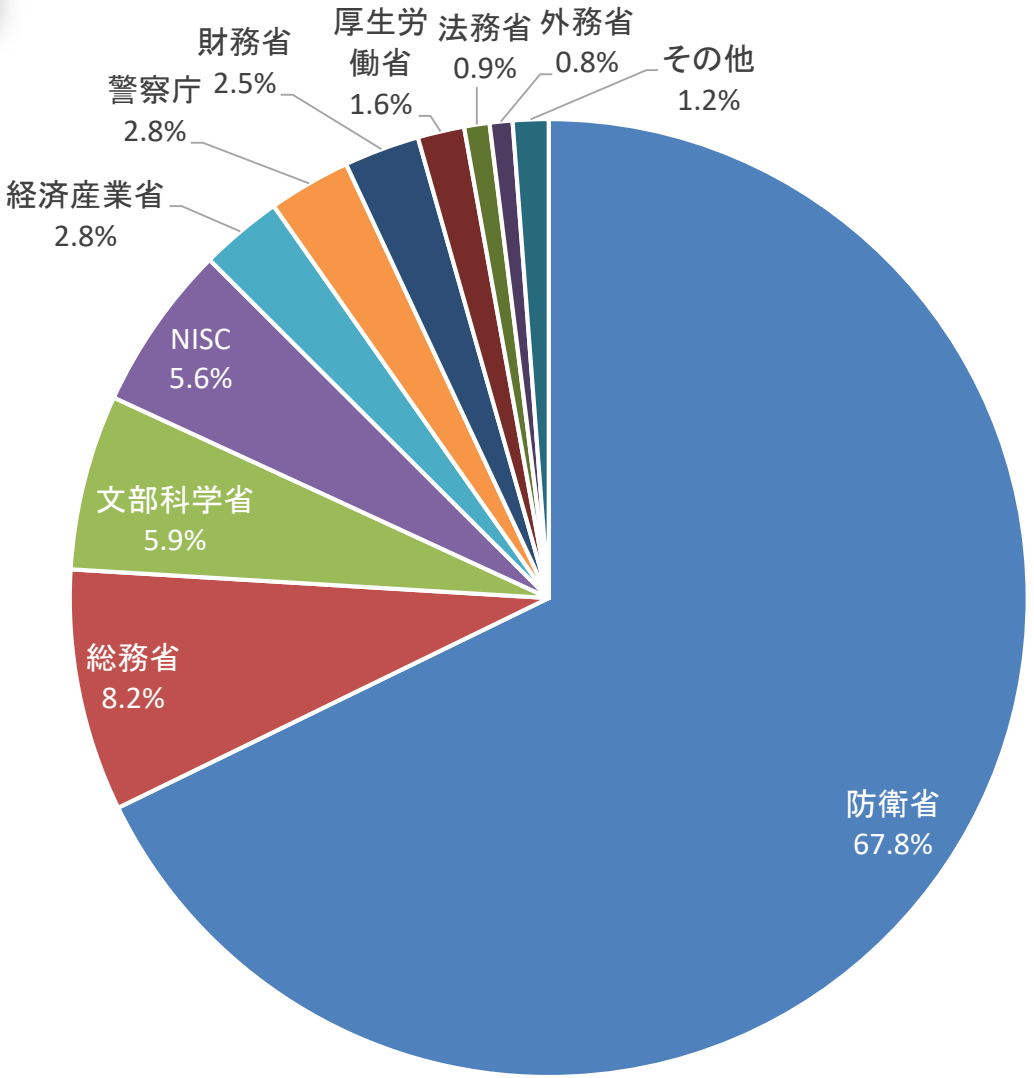
令和６年度補正予算

５６０．２億円

各府省庁等のサイバーセキュリティに関する予算

令和7年度当初予算額

2，０５１．５億円



※サイバーセキュリティに関する予算として切り分けられない場合には計上していない。

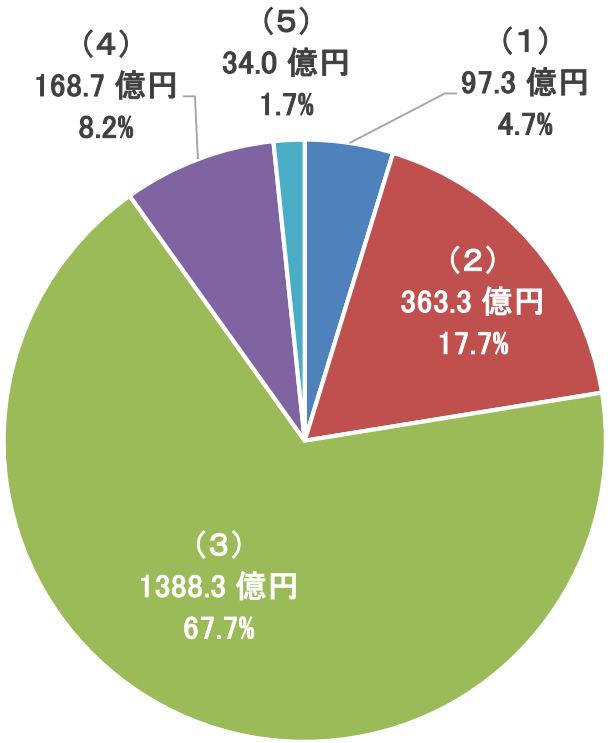
サイバーセキュリティ戦略　分野別内訳

令和7年度当初予算額

2，０５１．５億円

○　令和７年度当初予算におけるサイバーセキュリティ関連予算は、令和６年度当初予算額に対し約７７．１億円の減額となる、２,０５１.５億円が措置されている。

○　サイバーセキュリティ戦略における分野別の内訳について、「（３）国際社会の平和・安定及び我が国の安全保障への寄与」が約７割を占め、「（２）国民が安全で安心して暮らせるデジタル社会の実現」が約２割を占めている。



- （１）経済社会の活力の向上及び持続的発展
- （２）国民が安全で安心して暮らせるデジタル社会の実現
- （３）国際社会の平和･安定及び我が国の安全保障への寄与
- （４）横断的施策（人材育成等）
- （５）その他

※サイバーセキュリティに関する予算として切り分けられない場合には計上していない。

産業サイバーセキュリティ対策の強化に向けた環境整備事業

令和7年度予算額 54億円（44億円）

経済産業省
商務情報政策局
サイバーセキュリティ課

事業の内容

事業目的

本事業は、サイバー攻撃被害に対する対処支援や中小企業等によるサイバーセキュリティ対策の促進、サイバーセキュリティ人材の育成等を通じて、産業界のサイバーセキュリティ対策を強化することを目的とする。

事業概要

(1)サイバーセキュリティ経済基盤構築事業

①国際的なサイバー被害に関する対応支援等を実施。

②高度標的型サイバー攻撃を受けた組織に対して初動対応支援を実施。攻撃者の意図把握に資するサイバー情勢に関する研究機能を強化。

(2)サプライチェーン・中小企業サイバーセキュリティ対策促進事業

セキュリティ意識向上やサイバーセキュリティ人材の確保等を通じて中小企業によるセキュリティ対策強化を支援。

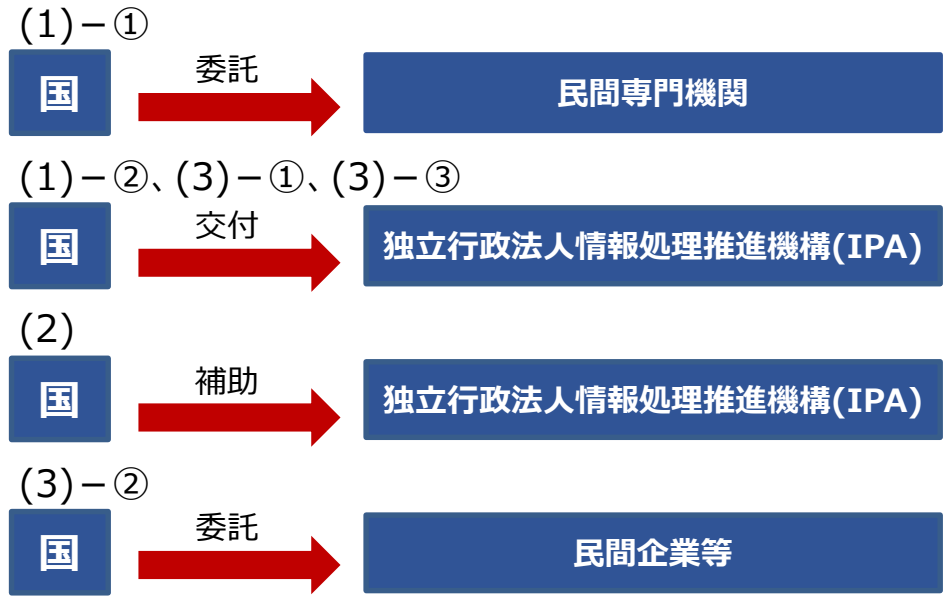
(3)産業サイバーセキュリティ強靭化事業

①重要インフラ等におけるサイバーセキュリティ人材の育成やサイバーインシデント事故調査に向けた体制整備等を実施。

②セキュアなソフトウェアの市場流通促進に向けた実証事業等を実施。制度詳細を具体化。

③IoTセキュリティ適合性評価制度（JC-STAR）や企業のセキュリティ対策水準を評価・可視化する制度の整備・運営等。

事業スキーム（対象者、対象行為、補助率等）



成果目標

(1)サイバー攻撃によって、官邸危機管理センターに官邸連絡室が設置される件数を0件にする。

(2)SECURITY ACTION制度において、自己宣言をした事業者数47万者を目指す。

(3)第５期中核人材育成プログラム以降の修了者の活動数を令和９年度までに1,000件以上とする。　等

総務省

IoTの安心・安全かつ適正な利用環境の構築（電波法第103条の2第4項第12号に規定する事務）

● 電波を使用するIoT機器が急増し多様化するとともに、それらに対するサイバー攻撃の脅威が増大していることから、IoTに係る様々なセキュリティ対策の強化やIoTの適正な利用環境の構築に向けたリテラシーの向上を図ることで、国民生活や社会経済活動の安心・安全の確保等を実現する。

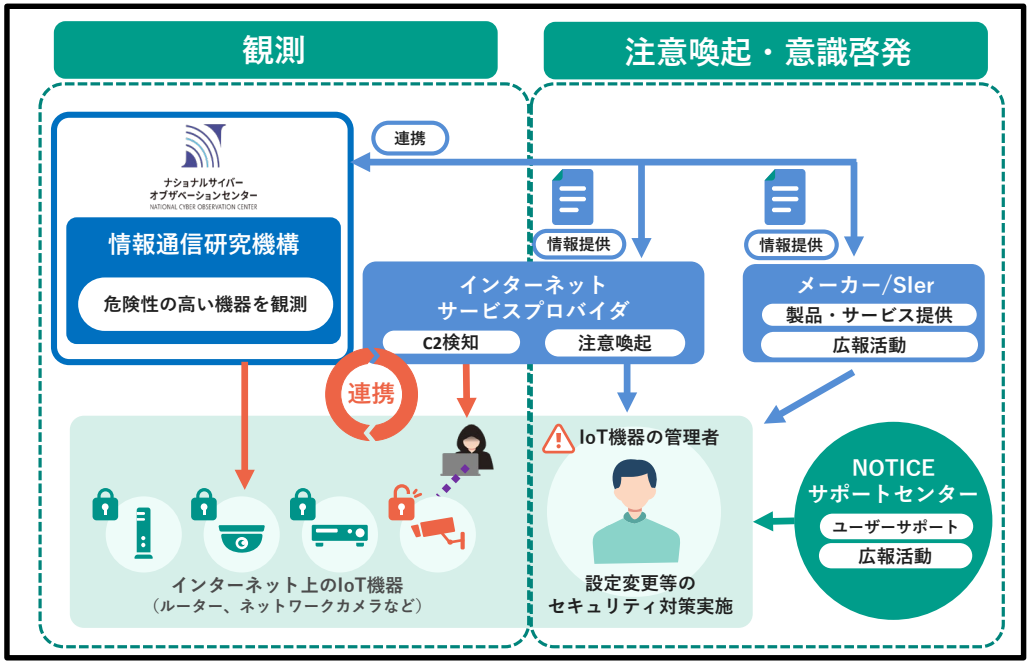
① IoTセキュリティ対策の強化

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脆弱な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。

② IoTの安心・安全かつ適正な利用環境の構築にむけた情報提供の充実

Society5.0の基盤であるIoT機器の安心・安全かつ適正な利用環境の確保に向け、利用実態の調査を行うとともに、必要となるセキュリティ要件や対策を、ガイドライン等の文書にとりまとめ周知広報に取り組むことにより、IoT機器利用に関するリテラシーの向上を目指す。

①IoTセキュリティ対策の強化



（事業主体）　国立研究開発法人情報通信研究機構（①の一部）、民間企業（通信事業者、ベンダ　等）
（事業スキーム）　補助事業（①の一部）、実証事業（請負）、調査研究（請負）　等
（補助対象）　人件費、機器費　等
（補助率）　定額
（計画年度）　令和元年度～令和7年度

令和7年度当初予算　1,584百万円
（令和6年度当初予算 1,584百万円）

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

総務省

- 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（CYXROSSプロジェクト）。
- 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。

安全性・透明性を検証可能なセンサー(ソフトウェア)を開発し政府端末に導入

サイバー脅威

サイバー脅威

サイバー脅威

収集した情報をCYNEXに集約

・検体情報
・アラート情報
・端末情報　等

（国研）情報通信研究機構

NICT

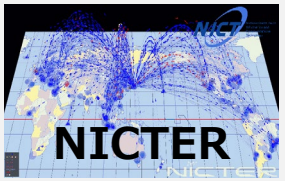
サイバーセキュリティ統合知的・人材育成基盤

情報分析

分析結果を各省庁等に提供

・検体分析結果
・攻撃傾向の統計情報
・サイバー脅威情報(IoC) 等

NICTが開発したサイバーセキュリティ技術及び蓄積してきたデータ等を活用



サイバー攻撃観測技術

標的型攻撃観測・分析技術

サイバー攻撃情報統合分析技術

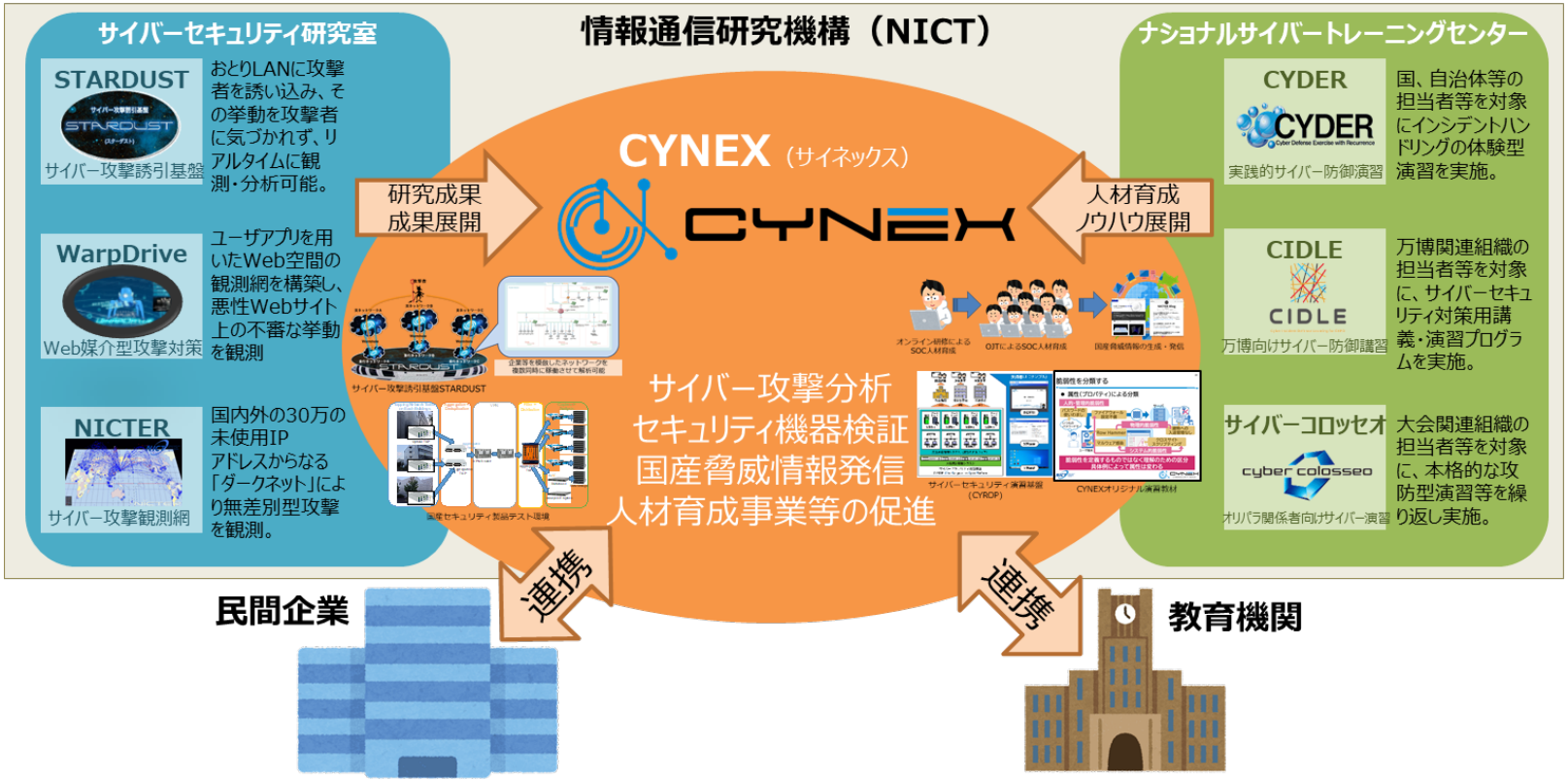
（事業主体）　国立研究開発法人情報通信研究機構（NICT）
（事業スキーム）　補助事業
（補助対象）　機器購入費、環境構築費、運営費
（補助率）　定額補助
（計画年度）　令和4年度～令和7年度

令和7年度当初予算 1,300百万円
（令和6年度当初予算 1,000百万円）

総務省

サイバーセキュリティ統合知的・人材育成基盤の構築

● サイバーセキュリティ情報を国内において収集・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）を国立研究開発法人情報通信研究機構（NICT）に構築し、産学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を強化。



次のとおり活用可能な基盤をNICTに構築。

- **国産セキュリティ情報の収集・蓄積・分析・提供**
  幅広くサイバーセキュリティ情報を収集・蓄積し、AIを駆使して横断的に分析することで、高信頼で即時的なセキュリティ情報を生成し、政府・セキュリティ機関等に提供。
- **セキュリティ機器テスト環境**
  国産のセキュリティ機器・サービスの開発を推進するため、最新のサイバー攻撃情報を活用し、その対応状況をセキュリティ事業者がテストできる環境を提供。
- **高度解析人材の育成**
  収集したセキュリティ情報を活用し高度なサイバー攻撃を迅速に検知・分析できる卓越した人材を育成。
- **人材育成のための基盤提供**
  NICTが有する人材育成に関する環境・知見を民間・教育機関等に開放し、自立的な人材育成を推進。

（事業主体）　国立研究開発法人情報通信研究機構（NICT）
（事業スキーム）　補助事業
（補助対象）　機器購入費、環境構築費、運営費
（補助率）　定額補助
（計画年度）　令和3年度～令和7年度

令和7年度当初予算 899百万円
（令和6年度当初予算 850百万円、令和5年度補正 1,254百万円の内数）

厚生労働省の施策例

厚生労働省

厚生労働省及び関係機関等における情報セキュリティ対策推進費

令和7年度予算　：32．2億円
令和6年度補正予算　：90．4億円
令和6年度当初予算　：19．5億円

1　厚生労働省及び関係機関における情報セキュリティ対策の推進　19．7億円（18．1億円）

○ CSIRT支援
・外部事業者を活用した情報セキュリティコンサルティング業務（情報セキュリティインシデント対処等）の実施
○ 情報セキュリティ監査
・情報セキュリティ対策にかかる実効性の向上を図るための外部事業者を活用した監査遂行能力の拡充
○ サイバーセキュリティ対策
・情報システムにおける情報セキュリティ対策の強化に必要な機能の導入・運用等の実施

2　重要インフラの情報セキュリティに関する取組の強化　12．5億円（ 1．4億円）

○ 医療分野におけるサイバーセキュリティ対策調査事業
・医療機関向けセキュリティ研修に加え、インシデントが発生した医療機関への原因究明や対応指示など初動支援体制を強化
○ 保健医療福祉分野の公開鍵基盤（HPKI）普及啓発等事業
・医師のなりすましや診療データの改ざんといったリスクを防止するため、保健医療福祉分野の公開鍵基盤（HPKI）の普及・啓発等を実施

（令和6年度補正予算）
○ 医療機関におけるサイバーセキュリティ確保事業
・外部ネットワークとの接続の安全性の検証・検査や、オフライン・バックアップ体制の整備を支援する。
○ 医療機器サイバーセキュリティ対応の推進事業
・医療機関と医療機器製造販売業者での連携や共有されたSBOMの分析手法、得られた脆弱性情報に基づくフィードバック等、SBOMから得られる情報の活用方法について検討を行い、医療機器製造販売業者が医療機関に対してSBOMの適切な活用手法を示すための指針を作成する。
○ 医療扶助におけるオンライン資格確認の導入
・生活保護の医療扶助にマイナンバーカードによるオンライン資格確認を導入し、 マイナンバーカードによる確実な資格・本人確認を実現

外務省の施策例

外務省サイバーセキュリティ施策

令和７年度当初予算額　：　１５．３億円
令和６年度補正予算額　：　　２．２億円

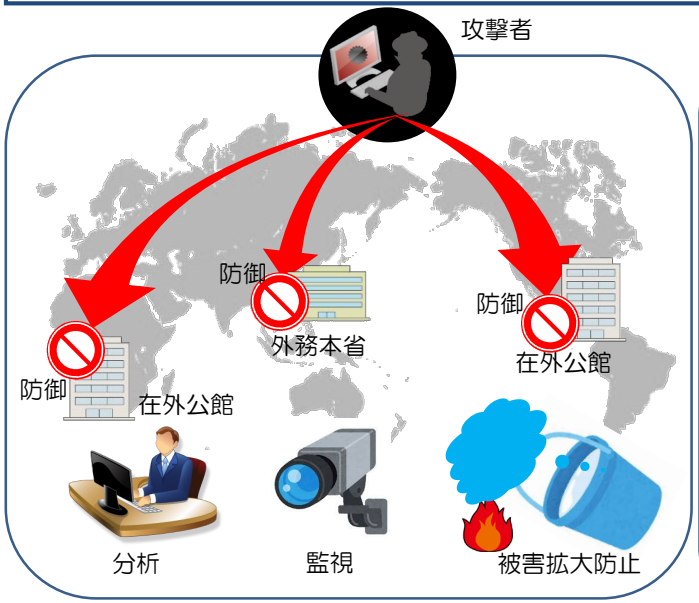
情報セキュリティ対策の強化

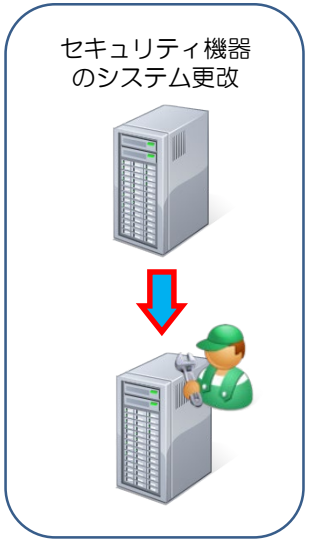
令和７年度当初予算額：　１５．０億円（１１．２億円）
令和６年度補正予算額：　　２．２億円

事業目的･概要

〇目的
　脅威やインシデントの予兆を早期に検知・対応し、被害の回避・最小化を図るとともに、不正アクセス対策を強化する。

〇事業概要
・不正通信の監視、遮断、及びメールフィルタやエンドポイントでの未知の不正プログラム対策。
・ログ分析、フォレンジック等による事案解明及び対処。
・サイバーセキュリティ監査の実施。
・次期情報ネットワークLANシステムへの刷新に伴うセキュリティ機器のシステム更改。





サイバー空間に関する外交及び国際連携

令和７年度当初予算額：０．３億円（０．７億円）

事業目的･概要

〇目的
　近年のサイバー空間における脅威の増大を背景に、令和４年に閣議決定した「国家安全保障戦略」を踏まえて、国際的なルール形成・深化、同盟国・同志国との連携、信頼醸成、開発途上国における能力構築支援等に取り組んでいく。

〇事業概要
　･サイバーセキュリティに関する関連会議
　･開発途上国におけるサイバーセキュリティに関する能力構築支援

サイバーセキュリティに関する協議等

内閣官房

（内閣サイバーセキュリティセンター）

政府機関情報セキュリティ横断監視・即応調整チームの運用

７年度予算額１６．０億円　（６年度予算額　９．８億円）

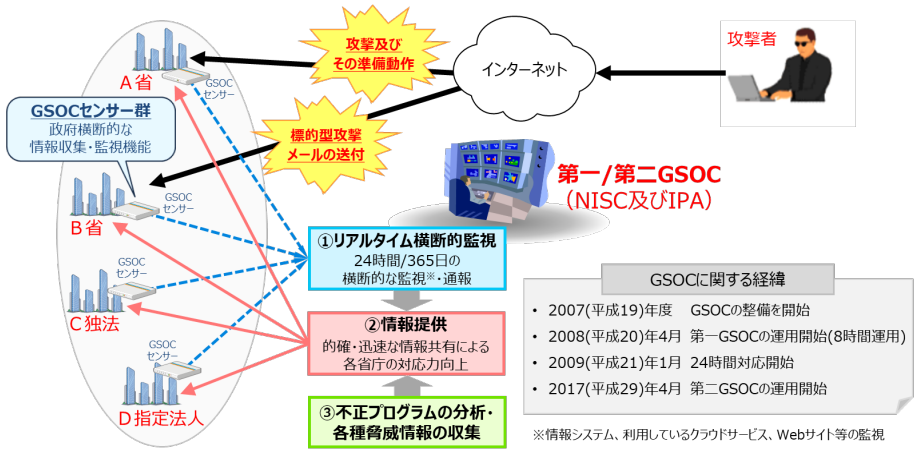
事業概要・目的

① 内閣サイバーセキュリティセンター（NISC）は、サイバーセキュリティ基本法第13条に基づき、政府関係機関情報セキュリティ横断監視・即応調整チーム(GSOC)を設け、24時間365日体制でサイバー攻撃等の不審な通信の横断的な監視、不正プログラムの分析や脅威情報の収集を実施している。

② 国家安全保障戦略において**「最新のサイバー脅威に常に対応できるようにするため、政府機関のシステムを常時評価し、政府機関等の脅威対策やシステムの脆弱性等を随時是正するための仕組みを構築する。その一環として、サイバーセキュリティに関する世界最先端の概念・技術等を常に積極的に活用する。」**と書かれた取組とも連携し、GSOCの運用を更に強化する。

事業イメージ・具体例

■サイバーセキュリティ基本法第十三条に基づき、「(前略)国の行政機関、独立行政法人又は指定法人の情報システムに対する不正な活動の監視及び分析(後略)」を実施



ナショナルサイバートレーニングセンターの強化

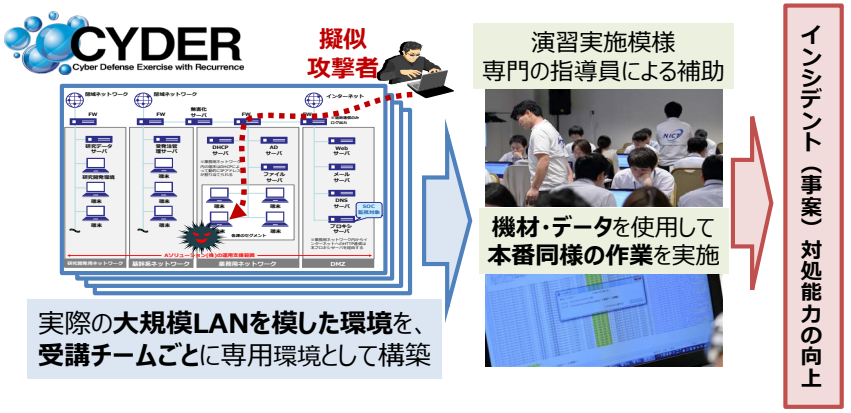
● 巧妙化・複雑化するサイバー攻撃に対して我が国のサイバーセキュリティを強化するため、国立研究開発法人　情報通信研究機構（NICT）に設置した「ナショナルサイバートレーニングセンター」において、実践的な対処能力を持つセキュリティ人材等を育成。

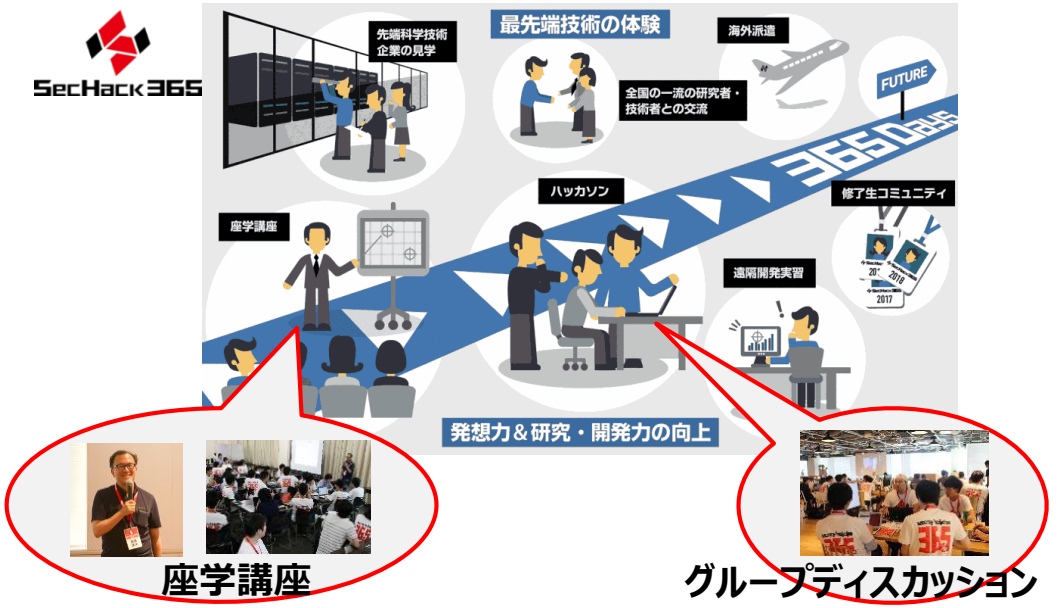
①CYDER（実践的サイバー防御演習）

国の行政機関、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て実践的サイバー防御演習（CYDER）を実施。
全国の会場で年間100回、3,000名規模で運営。

②SecHack365（若手セキュリティイノベータの育成）

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得る最先端のセキュリティ人材を育成。
毎年40名程の受講者を選抜し、1年間トレーニング。





（事業主体）　国立研究開発法人情報通信研究機構（NICT）
（事業スキーム）　補助事業
（補助対象）　機器購入費、環境構築費、運営費
（補助率）　定額補助
（計画年度）　平成26年度～令和7年度

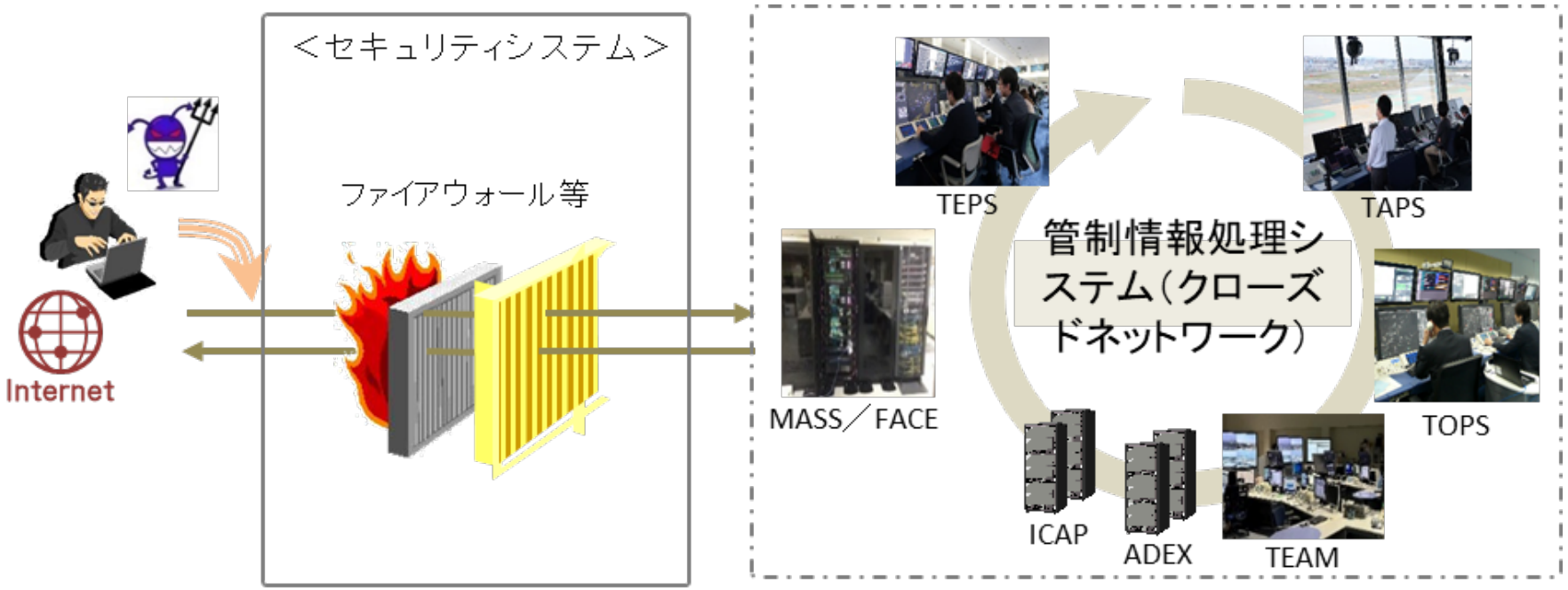
令和7年度当初予算 1,195百万円
（令和6年度当初予算 1,742百万円、令和5年度補正 1,254百万円の内数）

国土交通省

航空管制セキュリティシステム

【令和7年度予算額　：　11．6億円】（14．0億円）

　管制情報処理システムは、航空機の安全な運航を支える航空管制に必要不可欠なシステムである。本システムは、エアラインや海外管制機関等の関係各所と接続し、飛行計画など航空管制に必要な情報のやり取りを行っており、外部との接続に対しては、セキュリティシステムを介して、コンピュータウイルス等のサイバー攻撃に対する防御を行っている。
　昨今のサイバー攻撃の手口は、高度かつ複雑化しており、日々洗練・巧妙化している状況であることから、セキュリティの対策強化を実施する。



内閣官房

（内閣サイバーセキュリティセンター）政府機関等への監査関連事業

各府省庁等の情報システムに対するマネジメント監査及びペネトレーションテスト　７年度予算額　５．７億円（６年度予算額　０．４億円）
独立行政法人及び指定法人におけるサイバーセキュリティ施策の評価委託　７年度予算額　５．１億円（６年度予算額　０．４億円）

事業概要・目的

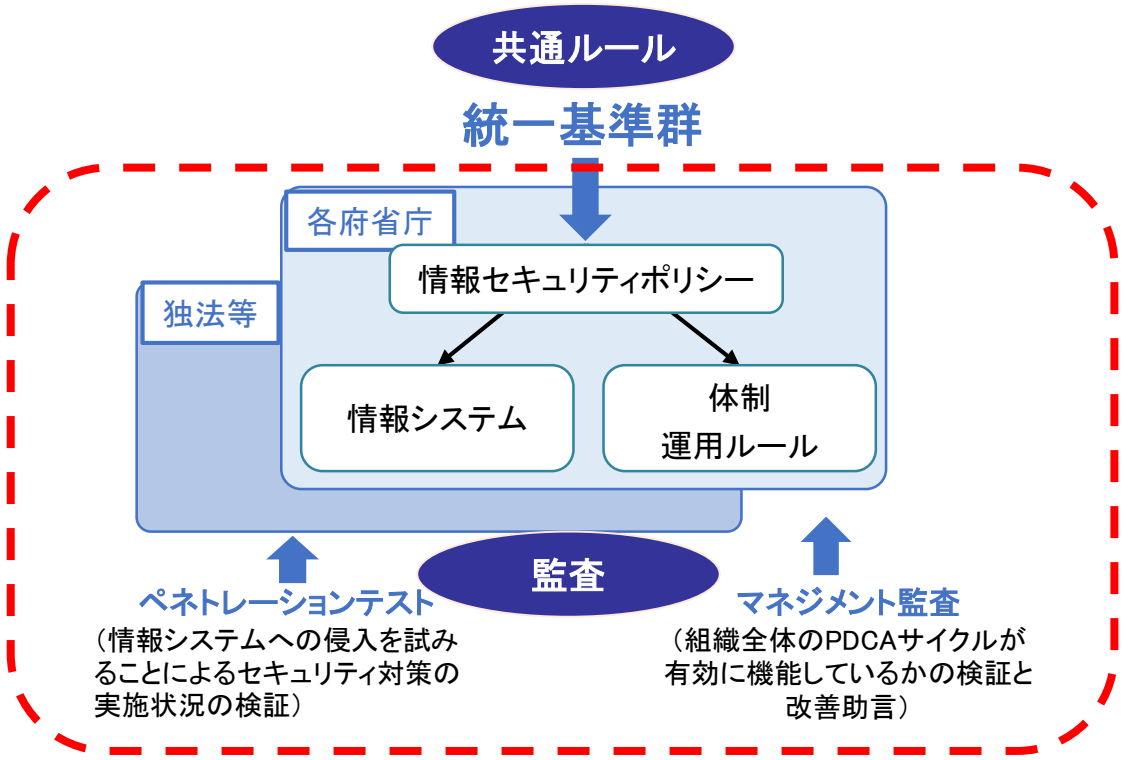
政府機関等のサイバーセキュリティ対策等に関する現状を、「マネジメント監査」及び「ペネトレーションテスト（侵入検査）」を行うことにより評価し、政府機関等におけるサイバーセキュリティ対策を強化します。

令和７年度においても、政府機関等が自律的な情報セキュリティ対策への取組を促進し、情報セキュリティ水準の向上を図ることを目的として監査等を実施します。

※（所掌事務等）
第26条①２　国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する対策の基準の作成及び当該基準に基づく施策の評価（監査を含む。）（略）
※（事務の委託）
第31条①により、独立行政法人及び指定法人における監査を情報処理推進機構に委託します。

事業イメージ・具体例

※本事業の対象は、下記赤枠部分



期待される効果

マネジメント監査やペネトレーションテストを通じて情報システムの脆弱性や体制不備等を把握し、各機関の改善を促すことにより、情報漏えいやサイバー攻撃リスクを低減することが期待できます。これらの取組みで得られた知見等を政府機関等全体のセキュリティ施策等へ反映することで、政府機関等全体におけるサイバーレジリエンスの自律的・継続的強化につながります。

内閣官房

（内閣サイバーセキュリティセンター）

政府機関等に対するサイバーセキュリティの実践的検証

７年度予算額５．０億円　（６年度補正予算額１９．７億円）

事業概要・目的

○ 「国家安全保障戦略」では「サイバー安全保障での対応能力を欧米主要国と同等以上に向上させる」とした上で「内閣サイバーセキュリティセンター（NISC）を発展的に改組する」こととしている。新組織でこうした対応能力向上を実現していくには、政府機関等において、LOTL攻撃（システム内寄生攻撃）などの高度サイバー攻撃を検知するための能力向上の実現、国家安全保障に影響の大きい政府機関等への対策の重点化、高度サイバー攻撃の検知に関するノウハウの広範な共有等に向けた対策を実施する必要がある。

○ 具体的には、仮想的な環境での検証による検知手法・ルールの構築、リスクシナリオ等に基づく現状のシステムを対象とした脅威ベースのリスク評価、実践的な疑似的なサイバー攻撃を実施する脅威ベースの侵入試験、先述の検知手法・ルールや、検知ログ分析ツールを活用した脅威探索を通じて、高度サイバー攻撃の検知手法・ルールの確立と精緻化を進めていくことが必要である。

事業イメージ・具体例

○ 仮想的な環境での検証による検知手法・ルールの構築
　仮想環境上で擬似的なサイバー攻撃を実行することで、当該検知手法等の検証・評価・改善を行う。

○ 政府機関等向け実践的検証の実施
　政府機関等を対象に、実践的検証に当たる、脅威ベースのリスク評価、脅威ベースの侵入試験、脅威探索を実施する。
- ✓ 脅威ベースのリスク評価：多種多様なリスクシナリオに基づき、システムにおける脅威の検知・防御の可否を確認・評価。
- ✓ 脅威ベースの侵入試験：検知手法・ルールを適用した上で、有効性を検証するため疑似的なサイバー攻撃を実施。
- ✓ 脅威探索：検知ログ分析ツールによる分析等を通じて脅威の有無を確認するもの。

⇒実践的検証を通じ、サイバーセキュリティ対応能力の強化と共に、上記の検知手法・ルール及び検知ログ分析ツールを精緻化

○ 政府機関等向け実践的検証要員の育成
　実践的検証の可能な体制を恒常的なものとするため、実践的検証を実施するために必要な能力等を備えた職員を育成する。

期待される効果

○ サイバーセキュリティに関する実践的検証の実施が政府機関等を対象に広く普及することで、政府機関等におけるサイバーセキュリティ体制の恒常的に強化につながり、我が国のサイバーセキュリティの抜本的強化に資する。

警察庁

サイバー捜査用資機材の増強等

令和７年度予算額　：　２．８億円
令和６年度補正予算：　６．９億円

概要

○　サイバー特別捜査部は、部門を越えた捜査を展開。
○　これまでの捜査から、①ＳＮＳ等の公開情報の捜査、②暗号資産等の犯罪収益の捜査、③重大サイバー事案の情報の集約が重要であることが判明。
○　公開情報捜査、犯罪収益捜査を通じて取得した情報を横断的に分析するための資機材整備を推進。

サイバー警察局

サイバー捜査分析用資機材
※令和６年度補正予算事業

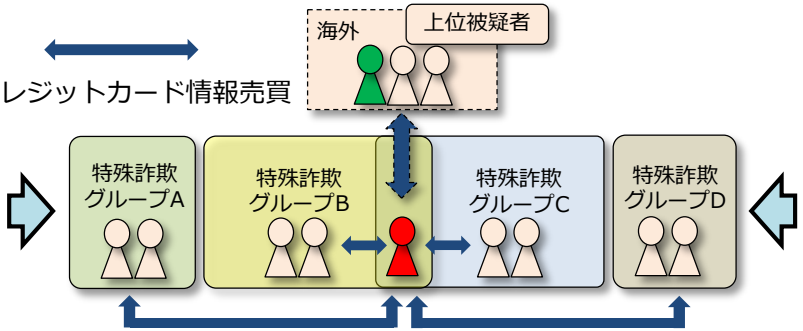
全国的・部門横断的な情報の集約・分析

報告　指示

サイバー特別捜査部

ダークウェブ調査ツール

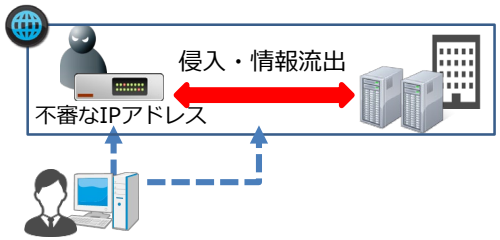
薬物及びクレジットカード情報等の販売、ランサムウェア被害の状況等



事案の全体像の解明
関連被疑者や上位被疑者の検挙

公開情報調査ツール

※令和７年度予算事業



インターネット上の不審な通信の調査

政府情報システムのためのセキュリティ評価事業

令和7年度予算額 2.8億円（2.8億円）

経済産業省
商務情報政策局情報産業課
情報処理基盤産業室

事業目的・概要

事業目的

政府調達におけるクラウド利用の拡大に向けて、セキュリティを確保する観点から、クラウドサービスをはじめとする政府情報システムの安全性評価を行い、基準を満たすサービスを登録する制度を実施することで、安全・安心にクラウドサービスを採用・継続的に利用する環境を整備し、クラウド・バイ・デフォルト原則の実現を目的とする。

事業概要

クラウドサービスに対して要求すべき情報セキュリティ管理・運用の基準（ISMAP管理基準）に基づき、セキュリティ対策を実施していることが確認されたクラウドサービスを、「ISMAP等クラウドサービスリスト」に登録し、各政府機関等がクラウドサービスを調達する際には、原則として、「ISMAP等クラウドサービスリスト」に掲載されたサービスから調達を行う。

具体的には、

（１）管理基準等の基準を策定・更新するとともに、クラウドサービス及び監査機関について、以下のように、登録基準を満たしているか審査を実施する。

・基準策定・改善：クラウドサービス事業者が登録申請を行う上で実施すべきセキュリティ対策基準や、監査機関を登録する際の基準等を策定・改善する。

・監査機関の選定：クラウドサービスの監査を行う監査機関を審査・登録し、監督する。

・サービスの登録：クラウドサービス事業者による申請を受けて、登録基準に基づいて登録簿への登録可否を審査する。

（２）制度の運用に必要となるシステムの管理や、関連する海外動向の調査を実施する。

事業スキーム（対象者、対象行為、補助率等）

（１）サービス登録・更新の審査等に係る事務対応

サービスの登録・更新の審査業務等を情報処理推進機構にて実施。

（２）関連システム運用・調査等

登録済サービスの公開や問い合わせ窓口等の機能を持つサイト運用や、海外を中心とした類似制度等の調査については、専門性を有する民間事業者等に委託。

成果目標・事業期間

令和3年度からの継続事業であり、最終的にはクラウド・バイ・デフォルト原則に基づく、デジタルガバメントの実現に貢献するとともに、我が国のクラウドサービス活用の基盤となることを目指す。

短期的には、令和７年度までに、政府機関等に調達された登録クラウドサービス数を1,050件にすることを目指す。

内閣官房

（内閣サイバーセキュリティセンター）

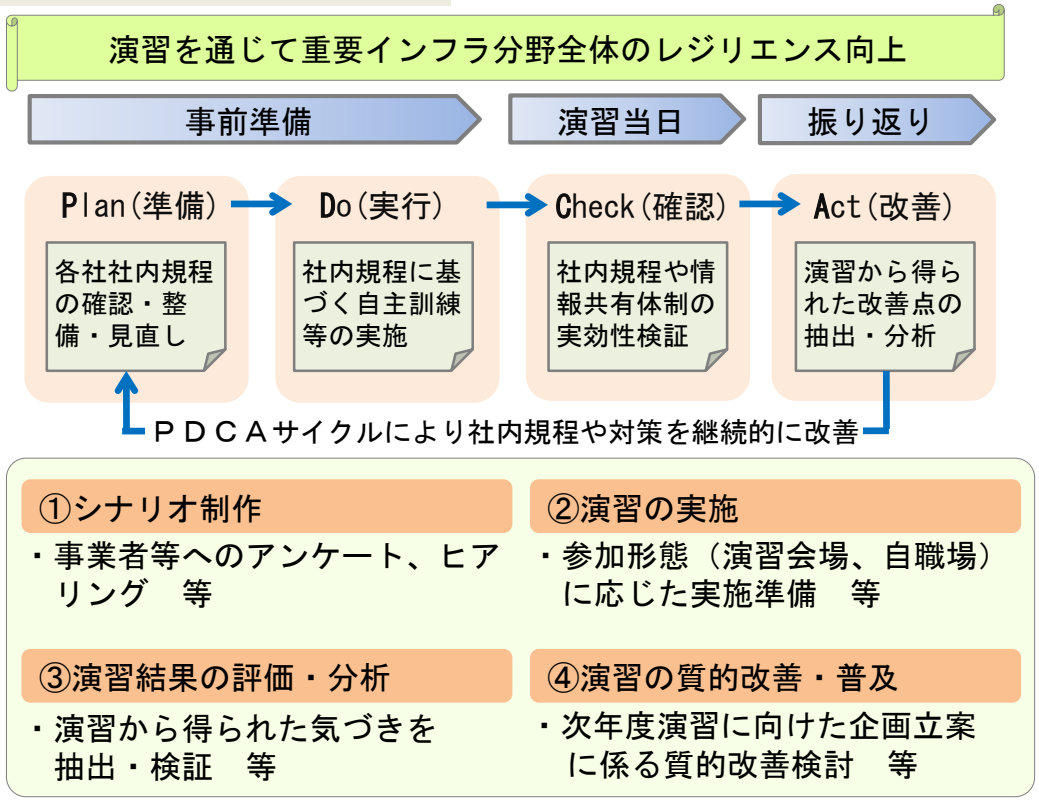
重要インフラ分野の演習等企画実施

７年度予算額：2．４億円　　（６年度予算額0．４億円）

事業概要・目的

- 内閣官房では、「重要インフラのサイバーセキュリティに係る行動計画」（令和６年３月８日サイバーセキュリティ戦略本部改定）に基づき、重要インフラサービスの継続的提供の強靭性の確保を念頭に、重要インフラ事業者等の障害対応体制の有効性を継続的に検証・改善する機会として、重要インフラ全15分野の事業者等が幅広く参加する分野横断的な演習（全分野一斉演習）を平成18年度より継続実施している。
- 全分野一斉演習は、重要インフラ事業者等の自組織の被害発生への対処の確認に重点を置いているため、大規模サイバー攻撃発生時等における複数組織での被害発生への対処や官民間での情報共有の実践・確認が課題となっている。
- そのため、大規模サイバー攻撃を想定し、重要インフラ分野間で発生し得る相互依存性のあるリスクを把握するため、重要インフラサービスの途絶等の状況を盛り込んだ官民間の連携の実践に重点を置いた演習（官民連携演習）を全分野一斉演習に加えて実施する。

事業イメージ・具体例



期待される効果

重要インフラ事業者等の自組織の障害対応体制の継続的改善を促すとともに、他の重要インフラ分野において発生した複数組織に影響を与えるインシデントへの対処能力の向上及び官民間の情報共有体制の強化、ひいては、重要インフラ分野全体のレジリエンス向上が見込まれる。

デジタル庁

サイバーセキュリティ確保環境整備費（セキュリティ・危機管理担当）

７年度予算額　１．３億円（６年度予算額　１．３億円）

事業概要・目的

○ 近年、国家を背景とするグループからの攻撃をはじめとするサイバー攻撃の深刻化や巧妙化が一層進展し、政府機関等への攻撃や、サプライチェーン・リスクを突いた攻撃、ランサムウェア等による被害が拡大するなど、サイバー脅威が高まっている。「デジタル社会の実現に向けた重点計画」（令和６年６月21日閣議決定）でも、デジタル庁はセキュリティ対策の強化を図るとともに、効率的にセキュリティを確保するため、セキュリティ・バイ・デザインを前提としたシステム構築等、セキュリティ対策の強化を図ることとされている。

○ このため、デジタル庁で整備・運用を行うシステムにおける脆弱性を未然に発見・修正し、システムライフサイクル全体でセキュリティ対策を確実に実施する必要がある。

○ このため、システムの企画から運用までの各段階において職員に求められる必要なセキュリティ知識等の習得機会の確保を行うとともに、設計の段階においてソフトウェア構成管理を活用した脆弱性対策を行う。また、運用段階におけるシステムに対して脆弱性の診断や運用自体への監査を行い、CSIRT要員に対して情報セキュリティインシデントへの的確な対応体制を整備するため、インシデント対応に必要な識能の取得を図る。

事業イメージ・具体例

○セキュリティバイデザインの浸透に向けたセキュリティ研修の構築・実施
企画から運用まで一貫したセキュリティ対策を実施する考え方（セキュリティ・バイ・デザイン）を実現するため、企画・開発・整備・運用に携わる職員が各工程の実務で必要となる知識や対策を学ぶ機会を確保を図る。

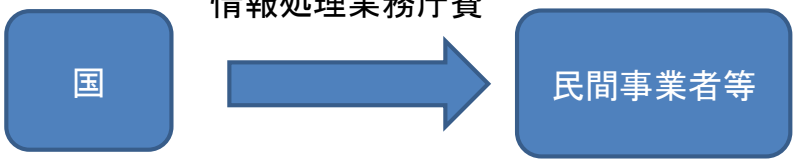
○バックドア等検証
デジタル庁が整備・運用するシステムについて、開発の段階からより安全性を確保するため、ソフトウェア構成管理を活用した脆弱性・バックドアへの対策の検証を実施する。

○監査等業務企画支援委託費
デジタル庁が整備・運用するシステムについて、セキュリティポリシーに準拠した運用管理規程が策定され、この規程に準拠した運用管理が行われているか等、セキュリティ確保に関する取組の検証・監査・調査等を実施する。また、デジタル庁が整備・運用するシステムへの疑似的なサイバー攻撃を通じて、サイバー攻撃への組織的な検知・対応を検証し、デジタル庁全体の組織的な対応能力の向上を図る。

○脆弱性診断等の実施
庁内システムに対し、各システムの脆弱性対策が適切に実施されているか等の診断を実施する。

○CSIRT要員等への研修の実施
デジタル庁CSIRT要員が、インシデント対応に必要な識能を部外研修により習得し、また、デジタル庁内のPJMOと実践的な演習を行うことで、サイバーセキュリティ対応態勢の高度化を図る。

資金の流れ



期待される効果

○ 企画設計から保守運用までの一連のプロセスを通じ、①問題を発生させない（監査、TLPT、バックドア検証、セキュリティ・バイ・デザイン研修、脆弱性診断）、②問題が発生した際には被害を最小限にする（ＣＳＩＲＴ研修）を実現することで、システムのセキュリティを確保する。

金融庁の施策例

金融庁

金融分野のサイバーセキュリティ対策強化

○ 金融業界横断的なサイバーセキュリティ演習の実施

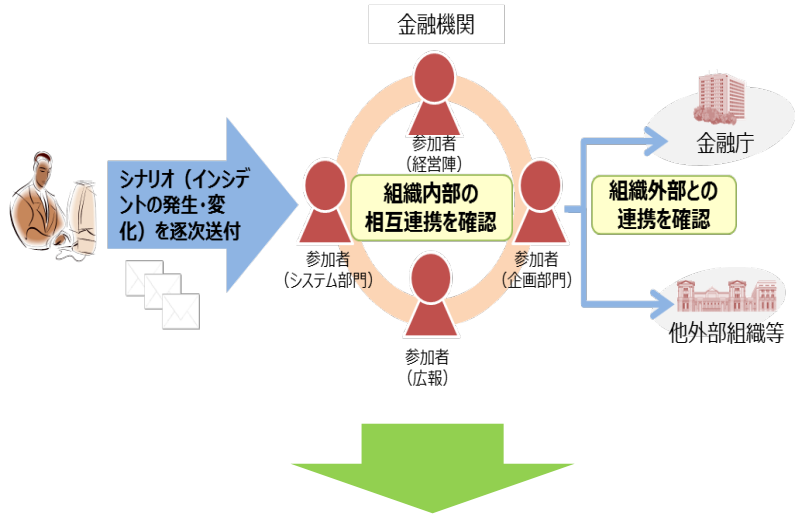
令和7年度予算額：0.9億円
（令和6年度当初予算額：0.8億円、令和6年度補正予算額：0.2億円）

事業概要

- 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、我が国においても、サイバー攻撃による重要情報の窃取、金銭被害等が発生。
- 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。
- このため、金融庁では、「金融分野におけるサイバーセキュリティ強化に向けた取組方針」（平成27年７月策定、令和4年2月改訂）に基づき、中小金融機関を含めた金融分野全体のサイバーセキュリティ態勢の底上げを目的とし、「金融業界横断的なサイバーセキュリティ演習」（Delta Wall）を継続的に実施。
- 金融分野のサイバーセキュリティ強化には、官民が一体になって取り組んでいくことが重要であり、令和7年度も、10回目となる演習を実施予定。

（注）本演習にかかる費用は、金融庁と参加金融機関の双方で負担。

演習概要



金融業界全体のサイバーセキュリティの底上げ

こども家庭庁

こども家庭庁

こども家庭庁におけるセキュリティ対策体制強化費

令和7年度予算額　　：0.8億円
令和6年度当初予算額：0.3億円

目的

・近年の高度情報通信ネットワーク社会においては、AI技術を活用した巧妙な攻撃型メールによる情報の搾取やシステムの脆弱性を狙ったゼロデイ攻撃など新たな脅威が日々出現しており、情報セキュリティインシデントの発生を前提とした体制と対策が必要な状況である。このような背景を踏まえ、情報セキュリティに関する専門的知見を有する外部の支援事業者を調達することにより、インシデント発生時における適切な対応できる体制及び手順を整えることにより、こども家庭庁＊ＣＳＩＲＴの効果的な業務の実施を図る。

要求概要

・主にインシデント対処のための準備（関係規程等の策定及び見直し、体制整備）やインシデント対処、フォレンジック調査検討、情報セキュリティ訓練等に関する支援を外部調達するものである。

ゴール

・こども家庭庁全職員が訓練を通して情報セキュリティ遵守の重要性を認識し、セキュリティリテラシーの向上を図ることでインシデントの発生を防止することで、国民に対する安定したサービスを提供する。
ＣＳＩＲＴについては、不測の事態に対する即応力を養うとともに関係府省庁との連携を密とした組織力を維持する。

セキュリティ対策体制強化の流れ

関連規程	庁内への周知	リテラシー向上	脆弱性対策	ＣＳＩＲＴ体制の強化	マネジメント監査支援	年間活動総括
●「政府機関等のサイバーセキュリティ対策のための統一基準」見直しに伴う、ポリシー改定に関する提案・助言など	●最新のインシデント傾向に関する情報提供	●全職員向け教育資料に関する評価と改善に関する助言など	●ペネトレーションテストの実施に関する評価と助言など ●攻撃型メール訓練の実施に関する助言	●専門的な知見の共有とメンバーの能力向上に関する助言など	●受査に向けたプロセス確認に関する助言など	●年間の活動に関する評価と次年度活動に関する助言など

＊CSIRT：Computer Security Incident Response Teamの略

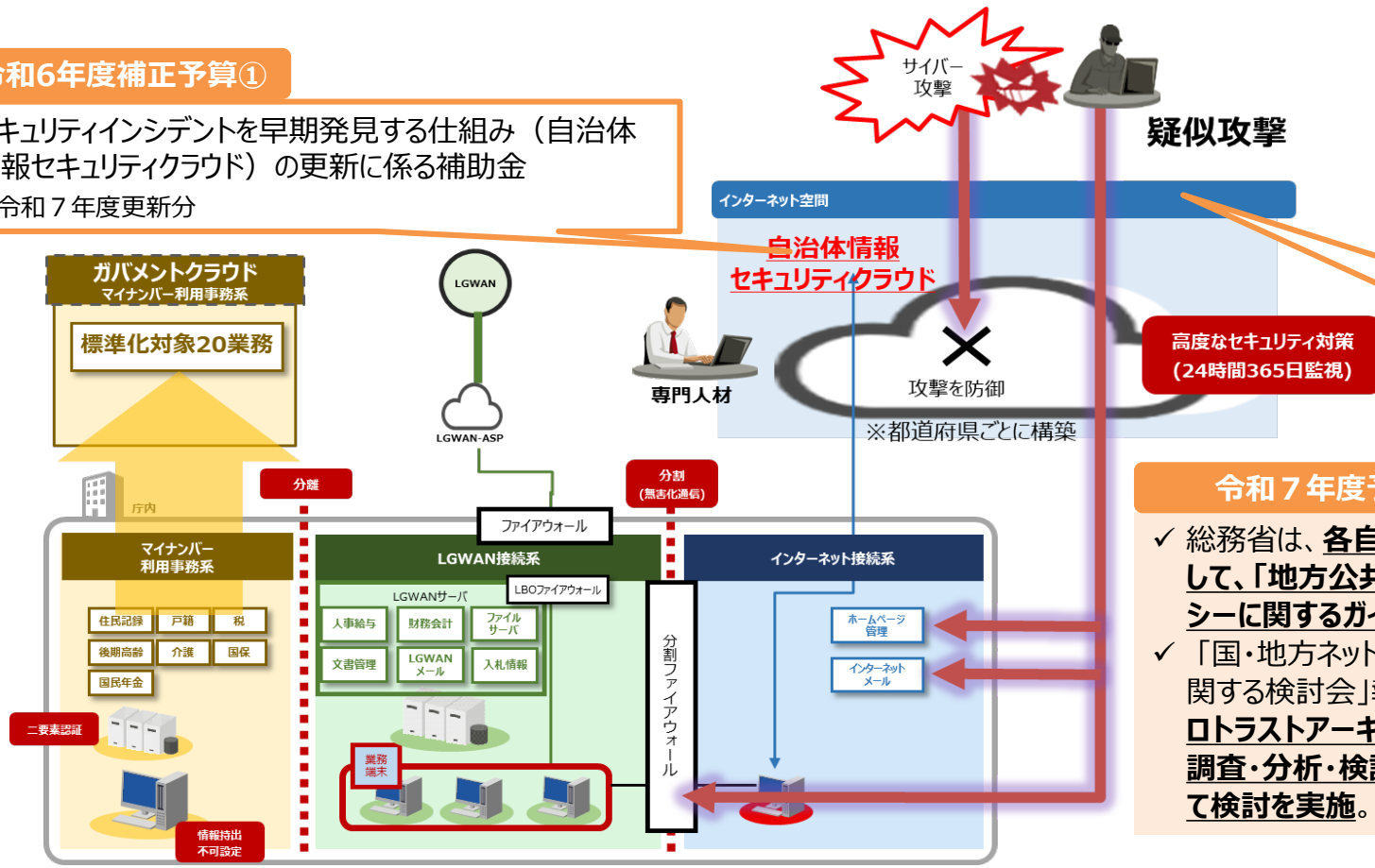
総務省

地方公共団体の情報セキュリティ対策の強化

■ 令和６年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）の更新
- 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

令和6年度補正予算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年度補正予算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

令和７年度予算

- ✓ 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**。

令和6年補正① 296百万円
令和6年補正② 193百万円

令和7年度予算額 74百万円
（令和6年度当初予算 74百万円

国土交通省の施策例

○国土交通省（CSIRT等）や所管事業者における情報セキュリティ対策の強化

令和7年度予算額：0.６億円
令和6年度補正予算額：5.0億円
（令和6年度当初予算額：0.6億円）

１．国土交通省CSIRT(注１) の強化等を行うことにより、当省における情報セキュリティインシデントへの対応能力の向上を図る

○ 情報セキュリティ体制強化支援業務　等
（外部専門家による国土交通省CSIRTの支援）

(注1) Computer Security Incident Response Teamの略。国土交通省における情報セキュリティインシデントに対処するための組織。

２.国土交通省所管事業者等への情報セキュリティ対策を実施するにあたり、外部専門家による支援を受け、サイバーセキュリティの強化・充実を図る

○ 国土交通省所管事業者等への情報セキュリティ対策支援業務
（外部専門家による国土交通省所管事業者等への支援）

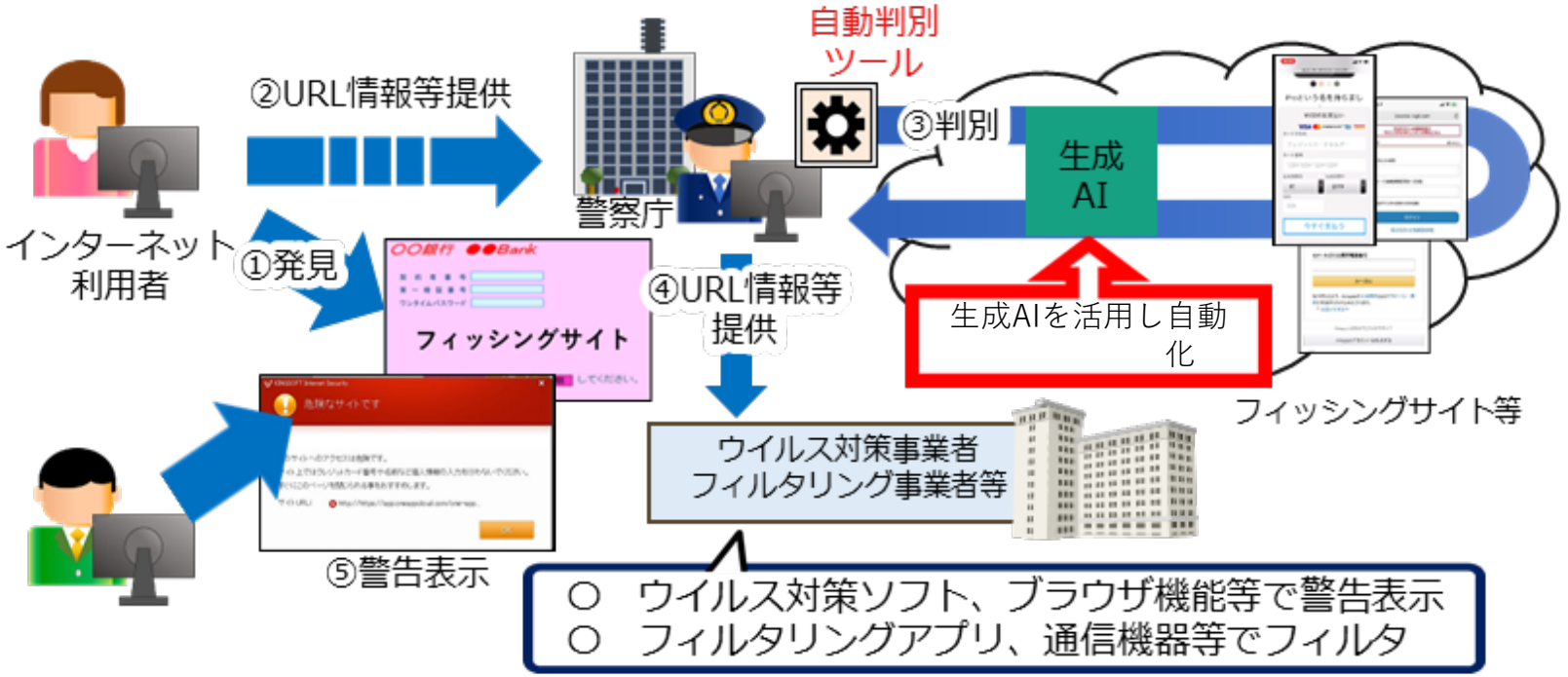
警察庁

生成ＡＩを活用したフィッシングサイト判定の高度化・効率化

令和７年度予算額 ： ０．３億円

概要

○　生成AIを活用し、都道府県警察やJC3等から提供されたURLがフィッシングサイトであるか判別。
○　フィッシングサイトであることが判明したURL情報については、ウイルス対策事業者、フィルタリング事業者等に提供。
　インターネット利用者に対して、アクセスしようとしているサイトがフィッシングサイトである旨の警告表示や、フィルタリングアプリのリストとして活用。



防衛省の施策例

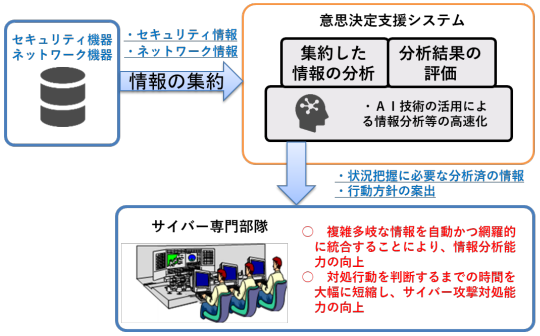
情報システムの防護

令和7年度予算額：876．3億円（令和6年度当初予算額：1064．0億円）

（令和7年度予算額の具体例）

◆ サイバー領域における意思決定支援システムの整備

サイバー攻撃等対処に係る状況把握・対処等をより迅速かつ的確に行うため、AIを活用した支援システムを整備



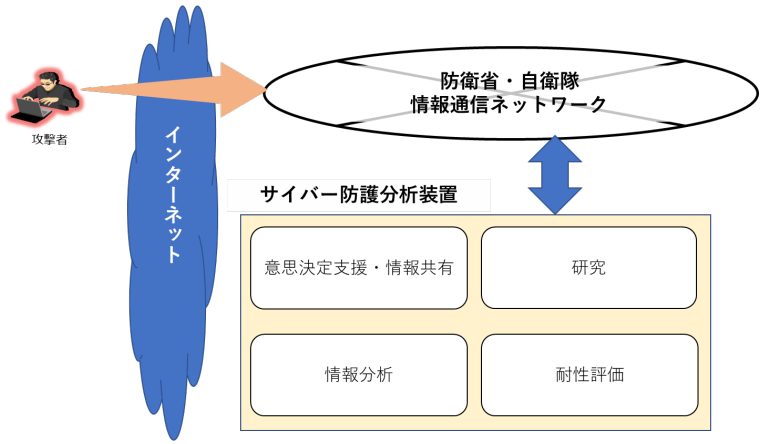
サイバー領域における意思決定支援システム（イメージ）

◆ サイバー防護分析装置の整備

防衛省に対するサイバー攻撃に関する手法の収集・分析等を行うサイバー攻撃対処のための装置の監視・評価機能等を強化

◆ スレットハンティング器材の整備

内部の潜在的脅威を継続的に探索・検出する器材を整備



サイバー防護分析装置（イメージ）

防衛省の施策例

リスク管理枠組み（RMF）の導入

令和7年度予算額：340．8億円（令和6年度当初予算額：290．8億円）

（令和7年度予算額の具体例）

常時継続的にリスクを管理する考え方を基礎に、運用開始後も継続的にリスクを分析・評価し、適切に管理する「リスク管理枠組み（RMF）」を導入。防衛省版RMFは、米政府で推奨されているセキュリティ基準と同等のもの。

（参考）米政府で推奨されているセキュリティ基準「ＮＩＳＴ　ＳＰ８００」

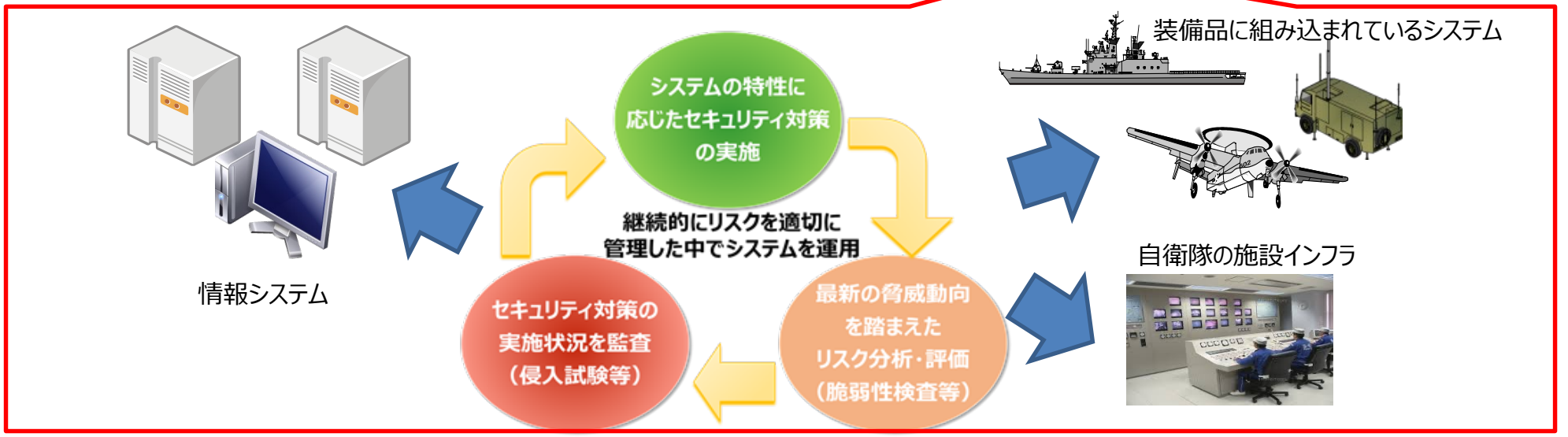
ＮＩＳＴ　ＳＰ８００－３７
（リスク管理枠組み（Risk Management Framework：RMF）－

ＮＩＳＴ　ＳＰ８００－５３
（連邦政府情報システムにおける推奨セキュリティ管理策）

・ 米政府機関向けの情報システムのセキュリティ標準

ＮＩＳＴ　ＳＰ８００：米国国立標準技術研究所（National Institute of Standards and Technology）が発行する一連の文書であり、ＳＰ（Special Publication）８００シリーズは、コンピュータ・セキュリティに関する基準。米政府機関は、同基準に準拠してシステムを運用。

防衛省版RMF



防衛省の施策例

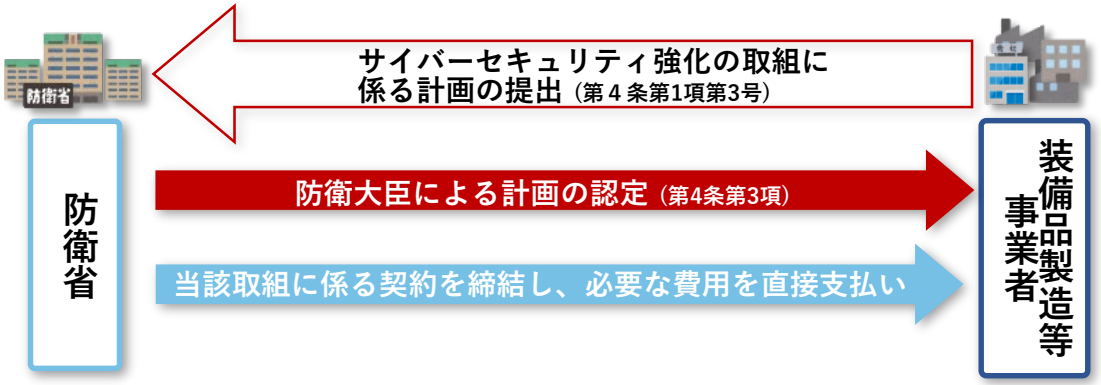
防衛産業におけるサイバーセキュリティ対策の強化

令和7年度予算額：134．2億円（令和6年度当初予算額：119．8億円）

（令和7年度予算額の具体例）

◆ 防衛装備品等の生産基盤強化のための体制整備事業

防衛省と契約関係にある企業の防衛部門のみならず、下請企業に対しても総合的・一体的なサイバーセキュリティ対策を実施



◆ 防衛産業サイバーセキュリティ基準への対応に係るシステムセキュリティ調査等

企業が保護システムに実装するセキュリティ機器等の脆弱性等を確認するための調査、企業にする管理策に係る説明会の実施や情報セキュリティ監査官に対する教育等を実施

防衛省の施策例

サイバー分野における教育機能の強化

令和7年度予算額：25．4億円（令和6年度当初予算額：25．5億円）

（令和7年度予算額の具体例）

◆ **各学校におけるサイバー教育基盤等の拡充**

サイバーセキュリティ態勢の強化のため、陸上自衛隊システム通信・サイバー学校を始め、防衛省・自衛隊の各学校におけるサイバー教育基盤を整備

◆ **部外力を活用したサイバー教育**

全隊員に対するITリテラシー教育やスキルを持つ隊員の国内外の大学への留学などを実施

◆ **諸外国とのサイバー分野における連携強化**

サイバー攻撃は国際社会共通の課題であるところ、諸外国との訓練等を通じて、サイバー分野における連携を強化

多国間サイバー防衛演習
ロックドシールズ2024の光景

文部科学省

GIGAスクールにおける学びの充実

令和7年度予算額　1.6億円
（令和6年度予算額　3.2億円）

令和6年度補正予算額　2.1億円

現状・課題

GIGAスクール構想の下、１人１台端末の更新やネットワークの高速化は各自治体において進められているが、その活用状況については自治体間で格差が生じつつある。今後、全ての学校においてICTを日常的に活用し、ICT環境を基盤として、個別最適な学びと協働的な学びの一体的な充実を進めることや新たな技術にも対応した情報モラルを含む情報活用能力を育成することが課題である。

事業内容

事業実施期間　平成２７年～

○GIGAスクール構想の加速化事業（伴走支援強化・事例創出）

学校DX戦略アドバイザー

・１人１台端末の利活用等の各種専門家による相談体制を構築
・自治体等の課題解決に向けて支援

＜課題例＞
・端末を活用した、新たな指導方法のあり方
・端末を活用した子供の学びのあり方
・先生にも保護者にも、安心できる持ち帰りのあり方
・学校での校務DXに向けた取組のあり方
・自治体におけるネットワーク構成のあり方
・生成AIを授業に活かす活用のあり方

※令和６年度学校DX戦略アドバイザー人数　163人
※相談に係る経費は、「GIGAスクール構想支援体制整備事業」において支援

リーディングDXスクール　令和６年度補正予算額　２億円

・指定校における１人１台端末及び高速ネットワーク（クラウド環境）を基盤とした個別最適な学びと協働的な学びの一体的な充実に資する好事例の創出
・様々な事例を全国の学校に普及・展開
・情報活用能力の育成等ICT活用の意義を伝える研修の実施
＜指定校＞　全国で100箇所程度

指定校の取組メニュー（例）
・「個別最適な学び」と「協働的な学び」の一体的な充実
・インターネット上の動画教材の活用、外部専門家によるオンライン授業の実施
・端末の日常的な持ち帰りによる家庭学習の充実等
・校務の徹底的な効率化や対話的・協働的な職員会議・教員研修

○情報モラル教育推進事業

普段から意識すべきことや直面する諸課題（生成AI、ファクトチェックなど）について、児童生徒が自分で考え、解決できる力を身に付けることを目指し、授業で活用できる情報モラルポータルサイトにおける各種コンテンツの充実や情報モラル教育指導者セミナーを開催。

○児童生徒の情報活用能力の把握に関する調査研究

情報及び情報技術を適切かつ効果的に活用して、問題を発見・解決したり自分の考えを形成したりしていくために必要な「情報活用能力」を児童生徒（小５、中２、高２）がどの程度身に付けているかを定期的に測定し、施策の改善等に活用。

令和５年度
●予備調査
▶
令和６年度
●本調査
▶
令和７年度
●調査報告書の作成と調査結果の公表
●次回の調査に向けた新規調査問題開発

（担当：初等中等教育局学校情報基盤・教材課）

生成AI等を活用したサイバーセキュリティ対策強化

- あらゆる分野において生成AIの実装が急速に進んでいる一方で、生成AIを巡るリスクとして、偽誤情報の拡散、プライバシーの侵害、知的財産権の侵害等に加えて、サイバー攻撃への悪用等によるサイバーセキュリティのリスクが新たに指摘されている。
- 他方、サイバー攻撃の大規模化・複雑化・巧妙化に伴い、サイバーセキュリティ対策の業務負荷が課題となっている中、サイバー攻撃対策への生成AI等の利活用が期待されている。
- こうした背景を踏まえ、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」に取り組むことが必要。

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
- 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＞

（事業主体）　国立研究開発法人情報通信研究機構（②、③）、民間企業（通信事業者、ベンダ　等）
（事業スキーム）　調査研究（請負①）、補助事業（②、③）、実証事業（請負④）
（補助対象）　機器購入費、環境構築費、人件費
（補助率）　定額補助
（計画年度）　令和6年度～令和7年度

令和6年度補正予算額 21.5億円（新規）