政府のサイバーセキュリティに関する予算

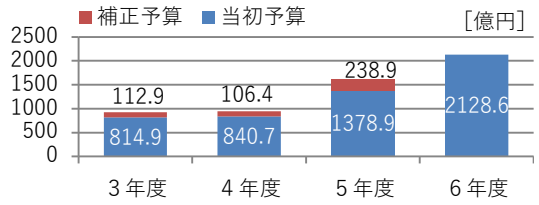
資料3

令和６年度予算額

２，１２８．６億円

（令和５年度当初予算額 １，３７８．９億円）

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



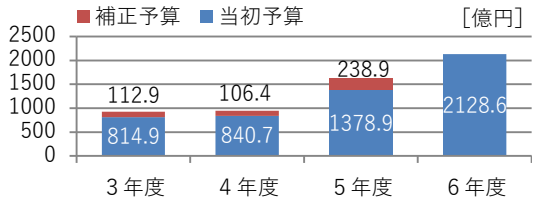
サイバーセキュリティ戦略における各分野ごとの主な施策例及び予算額

	令和６年度当初予算	令和５年度補正予算	令和５年度当初予算
（１）経済社会の活力の向上及び持続的発展	(63.2億円)	(9.8億円)	(49.1億円)
【経済産業省】産業サイバーセキュリティ強靭化事業	23.4億円	ー	23.5億円
【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	ー	12.0億円
【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	10.0億円	ー	ー
【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	8.5億円	ー	8.5億円
【経済産業省】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	0.7億円	ー	ー
【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	ー	5.1億円	ー
（２）国民が安全で安心して暮らせるデジタル社会の実現	(385.4億円)	(186.3億円)	(264.7億円)
【経済産業省】独法等の監視に係る次期システム構築事業	57.2億円	ー	ー
【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	30.4億円	53.3億円	27.1億円
【経済産業省】サイバーセキュリティ経済基盤構築事業	20.2億円	ー	19.6億円
【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	17.4億円	ー	12.7億円
【外務省】情報セキュリティ対策の強化	11.2億円	7.0億円	6.9億円
【警察庁】サイバー捜査用資機材の増強等	3.6億円	2.3億円	3.2億円
【警察庁】違法・有害情報対策に伴う経費	2.6億円	ー	2.0億円
【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	ー	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	1.5億円	0.9億円
【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	ー	0.7億円
【内閣官房】サイバーセキュリティ協議会の運用	0.6億円	ー	0.8億円
【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	0.4億円	4.7億円	0.5億円
【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	0.4億円	4.4億円	0.3億円
【内閣官房】サイバーセキュリティインシデントに係る調査	0.3億円	0.5億円	0.8億円
【国土交通省】国土交通省所管事業者等への情報セキュリティ対策経費	0.2億円	ー	0.2億円

政府のサイバーセキュリティに関する予算

令和６年度予算額

２，１２８．６億円　（令和５年度当初予算額　１，３７８．９億円）



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６年度当初予算	令和５年度補正予算	令和５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	(1,522.1億円)	(3.1億円)	(878.0億円)
【防衛省】情報システムの防護	1,064.0億円	ー	477.4億円
【防衛省】リスク管理枠組み（RMF）の導入	290.8億円	ー	301.1億円
【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	119.8億円	ー	68.5億円
【防衛省】サイバー分野における研究機能の強化	20.9億円	ー	14.6億円
【警察庁】サイバーテロ対策用資機材の増強等	11.7億円	0.4億円	4.3億円
【外務省】サイバー空間に関する外交及び国際連携	0.7億円	2.0億円	0.5億円
（４）横断的施策（人材育成等）	(128.4億円)	(37.3億円)	(150.3億円)
【防衛省】サイバー分野における教育機能の強化	25.5億円	ー	20.1億円
【文部科学省】GIGAスクールにおける学びの充実	3.2億円	2.1億円	2.8億円
【国土交通省】情報システムセキュリティ強化経費	0.3億円	ー	0.3億円
【内閣官房】サプライチェーンリスク対応のための技術検証体制構築に関する調査費	0.1億円	3.2億円	0.2億円

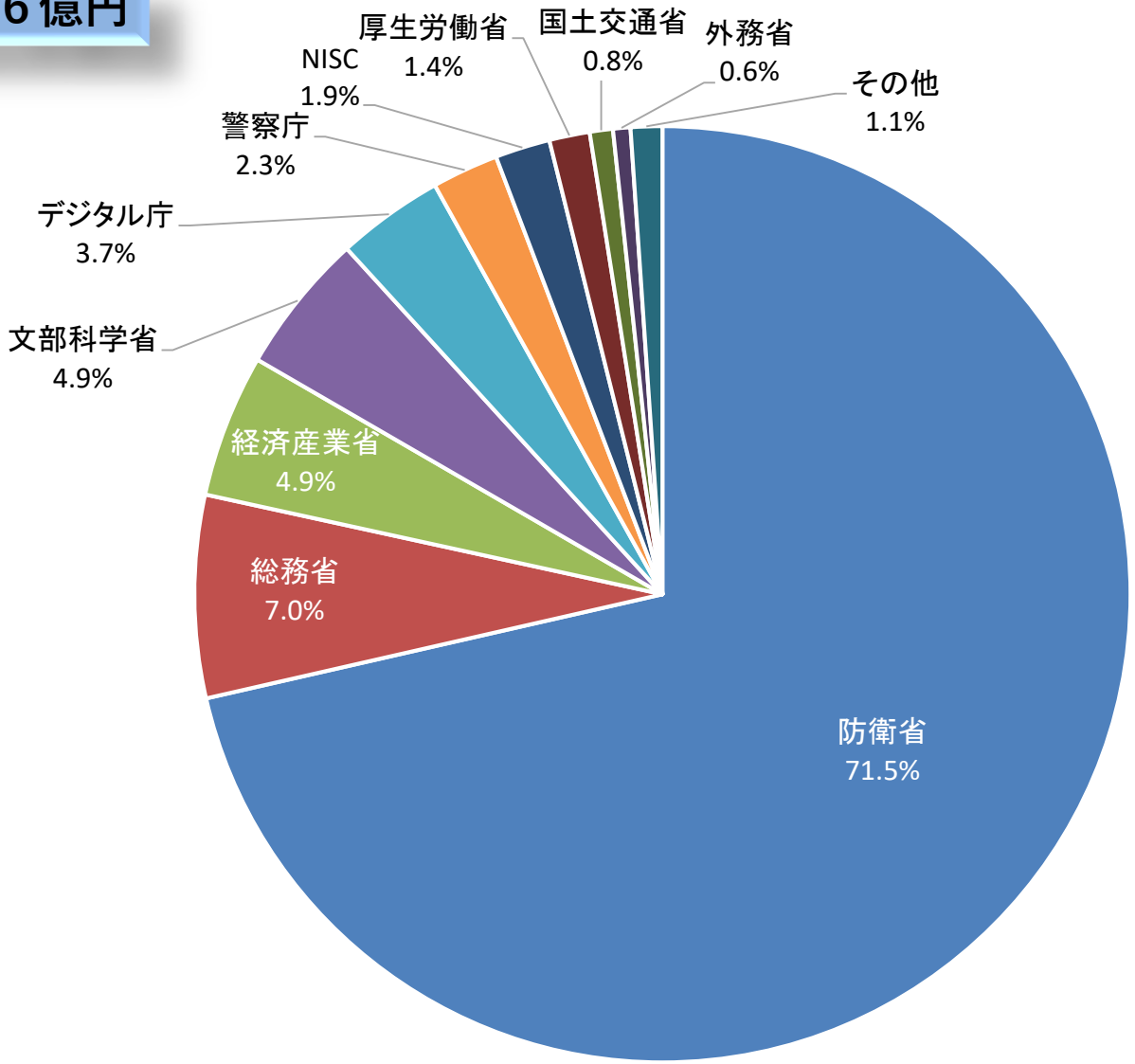
注１）サイバーセキュリティに関する予算として切り分けられない場合には計上していない。
注２）（　）内の数字は記載の主な施策例以外も含めたそれぞれの項目の総計

令和５年度補正予算　２３８．９億円

各府省庁等のサイバーセキュリティに関する予算

令和６年度予算額

２，１２８．６億円



※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。

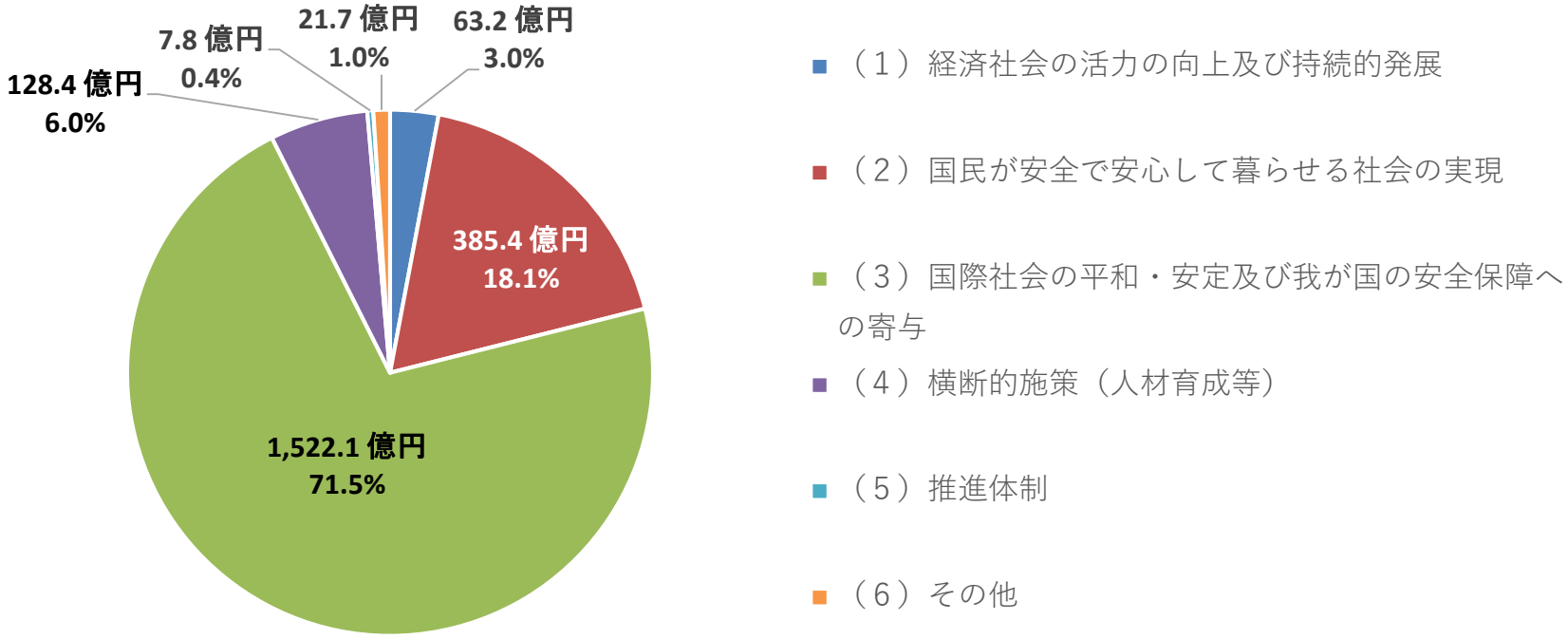
サイバーセキュリティ戦略　分野別内訳

令和６年度予算額

２，１２８．６億円

○　令和６年度予算におけるサイバーセキュリティ関連予算は、令和５年度当初予算額に対し約749.7億円の増額となる、2,128.6億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社会の実現」が約２割を占めている。



※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。

経済産業省

商務情報政策局サイバーセキュリティ課

産業サイバーセキュリティ強靱化事業

令和6年度予算額 23億円（24億円）

事業の内容

事業目的

サイバー空間とフィジカル空間の融合が進む中、サイバー攻撃の高度化・巧妙化に伴い、サイバー空間でのデータ流出リスクの拡大や、サイバー攻撃起点の増加、フィジカル空間への影響の拡大といったリスクの増大が見られる。

本事業では、ソフトウェア管理の高度化やガイドライン等の導入促進、サイバーセキュリティ対策の中核を担う人材の育成等を通じて、産業界のサイバーセキュリティ強靱化を目指す。

事業概要

産業界のサイバーセキュリティ強靱化に向けて、以下の取組を行う。

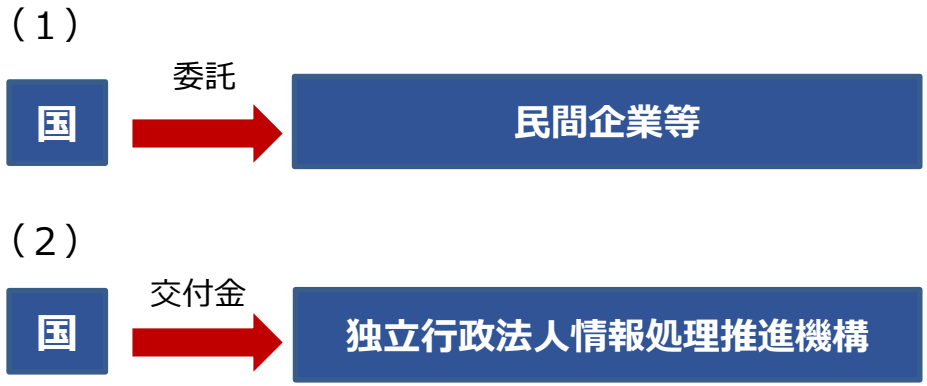
（１）サプライチェーン・サイバーセキュリティ対策基盤構築(委託)

- ✓ 国際連携の推進やガイドライン等の導入促進
- ✓ ソフトウェアの部品構成表であるSBOMの活用をはじめとしたソフトウエア・セキュリティの推進

（２）人材育成と実際のシステムの安全性・信頼性検証等(交付金)

- ✓ 模擬プラントを用いたセキュリティ演習
- ✓ 攻撃情報の調査・分析結果に応じた演習のアップデート
- ✓ 重要インフラ等の実際の制御システムの安全性・信頼性の検証

事業スキーム（対象者、対象行為、補助率等）



成果目標

産業界で策定されたガイドラインの数を15個以上にすることや、人材育成を通じて、産業界のセキュリティ対策を推進する。

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）

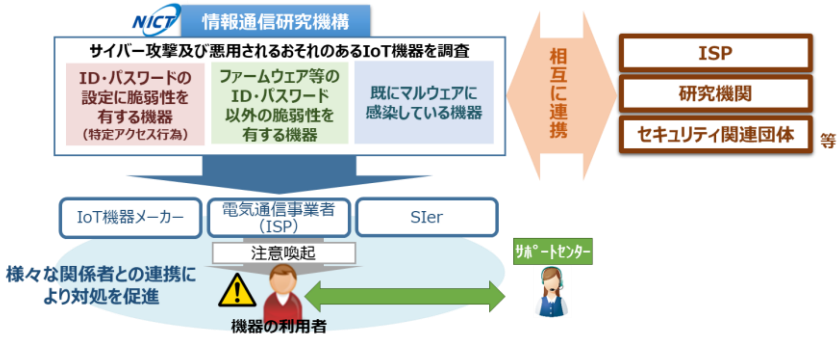
総務省

● 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）が、サイバー攻撃に悪用されうるIoT機器を調査し、利用者への注意喚起等の対処を行う取組（NOTICE）を、ISP等との連携により強化する。

①IoTセキュリティ対策の強化



② 5Gネットワークのセキュリティ確保に向けた体制整備と周知・啓発

5Gネットワークにおけるユースケースを考慮したセキュリティを担保するため、ユースケースに特徴的な構成要素及びネットワーク構成の汎用的なモデルを作成する。作成したモデルに対してリスク評価とサイバー攻撃の実行可能性について調査を行う。

③ 地域におけるIoTセキュリティ対策の強化

地域におけるIoTを活用したスマートシティのセキュリティ確保に向けて、改定したスマートシティセキュリティガイドラインや付随するガイドブック、及びチェックシートなどの文書の普及啓発の活動を行う。さらに、スマートシティセキュリティガイドラインへの各自治体の対応状況や事例を調査する。

④ 無線LANのセキュリティ対策の強化

無線LANを安心・安全に利用するため、利用者・提供者双方におけるセキュリティ対策状況調査やガイドライン策定を行うとともに、周知・啓発活動を推進する。

（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6年度予算額1,584百万円
（令和5年度当初予算 1,202百万円）

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開発し政府端末に導入することで、海外製品に頼らずに端末情報を収集し、得られた情報を国立研究開発法人情報通信研究機構（NICT）のCYNEX（サイバーセキュリティ統合知的・人材育成基盤）に集約して分析する取り組みを試行的に実施。
- 国産技術により端末情報を収集・分析する仕組みの実現性・有効性を検証する。

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

CYNEX CYBERSECURITY NEXUS

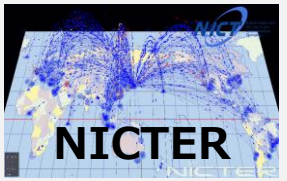
サイバーセキュリティ統合知的・人材育成基盤

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

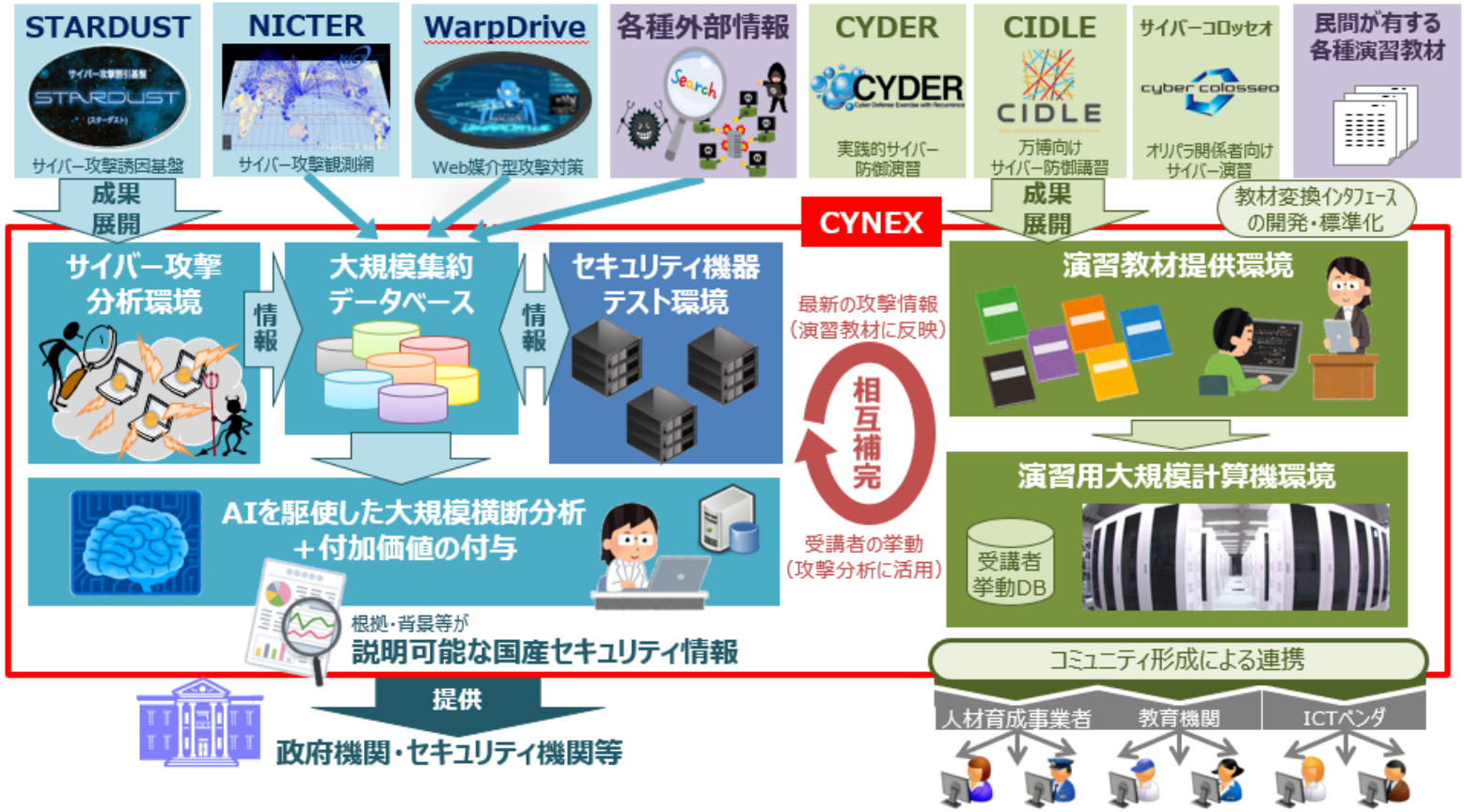
（事業主体）　国立研究開発法人情報通信研究機構（NICT）
（事業スキーム）　補助事業
（補助対象）　機器購入費、環境構築費、運営費
（補助率）　定額補助
（計画年度）　令和4年度～令和7年度

令和6年度予算額 1,000百万円
（令和4年度二次補正 2,000百万円）

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6年度予算額 850百万円
（令和5年度予算額 850百万円）

経済産業省

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

令和6年度予算額 0.7億円（新規）

商務情報政策局サイバーセキュリティ課
中小企業庁経営支援部経営支援課

事業の内容

事業目的

近年、サプライチェーン全体の中で対策が相対的に遅れている中小企業を対象とするサイバー攻撃により、中小企業自身及びその取引先である大企業等への被害が顕在化している。

本事業では、サプライチェーン全体での対策を推進するため、産業界の取組と連携し、中小企業の効果的なサイバーセキュリティ対策に向けた環境整備等を実施し、我が国の中小企業のサイバーセキュリティ対策の強化及びサプライチェーン全体のセキュリティの確保を図る。

事業概要

中小企業のサイバーセキュリティ対策を強化するため、独立行政法人情報処理推進機構において、以下の取組を行う。

- サイバーセキュリティお助け隊サービス審査事業
- 身近に相談等できる関連団体等の形成支援

事業スキーム（対象者、対象行為、補助率等）

成果目標

・セキュリティに関する関係団体数50団体を目指す。

・SECURITY ACTION制度において、自己宣言をした事業者数40万者を目指す。

経済産業省
商務情報政策局
サイバーセキュリティ課

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5年度補正予算額 5.1億円

事業の内容

事業目的

本事業は、中小企業等のサイバーセキュリティ対策を促進するための環境整備や、サイバーインシデント事故調査の実施に向けた環境整備を通じて、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）中小企業におけるサイバーセキュリティ対策の強化

中小企業のサイバーセキュリティ対策を強化するため、独立行政法人情報処理推進機構において、企業規模等に応じて求められる効果的なセキュリティ対策・手法の提示等を行う。

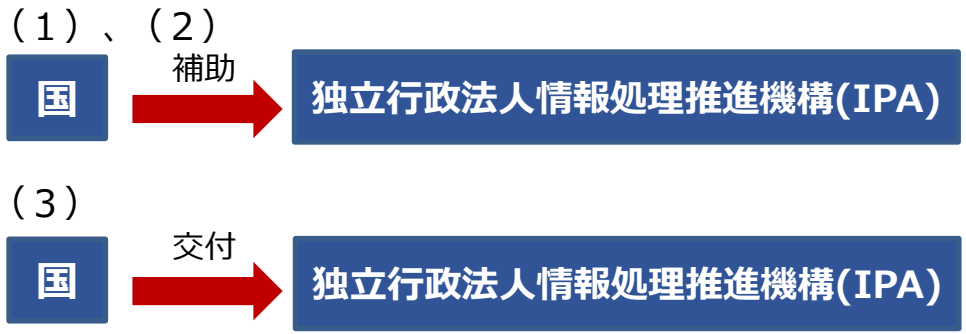
（２）IoT機器のセキュリティ対策向上

IoT機器の信頼性を確保するため、独立行政法人情報処理推進機構において、サイバーセキュリティ対策を講じているIoT機器の評価・導入促進等を行う。

（３）サイバーインシデント事故調査の実施に向けた環境整備

高圧ガス保安法等の一部を改正する法律（令和四年法律第七十四号）の施行に向け、独立行政法人情報処理推進機構において、サイバーインシデント事故調査の実施に向けた環境整備を行う。

事業スキーム（対象者、対象行為、補助率等）



成果目標

情報セキュリティ対策に取り組むことを自己宣言する事業者の拡大や、評価制度のスキームの構築、サイバーインシデント事故調査の実施のための環境整備等を通じて、産業界のサイバーセキュリティ対策を強化する。

経済産業省

独法等の監視に係る次期システム構築事業

商務情報政策局 サイバーセキュリティ課
商務情報政策局 総務課

令和6年度予算額 57億円（新規）

事業の内容

事業目的

政府機関等におけるサイバーセキュリティ対策について政府横断的な立場から推進するために、2017年４月から独立行政法人情報処理推進機構(独立行政法人等を監視対象)に第二GSOC※が設置され、NISCの監督の下、24時間365日体制でサイバー攻撃等の不審な活動の横断的な監視、不正プログラムの分析、脅威情報の収集等を実施している。

サイバー攻撃が複雑化・巧妙化している中、新たな技術の活用等によりGSOCシステムを強化し、サイバー攻撃を早期に検知することで、これに起因する被害の発生・拡大を防止することを目的とする。

※Government Security Operation Coordination team：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）

事業概要

独法等の監視に係る現第二GSOCシステムの更改時期を捉え、最新の技術を活用した次期システムを令和７年度から運用開始するため、必要となる詳細設計や構築などを行う。

事業スキーム（対象者、対象行為、補助率等）

成果目標

政府機関・独立行政法人等における横断的な監視等を通じ、サイバー攻撃に対する対処・警戒態勢の強化を図る。

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6年度予算　：30．4億円
令和5年度補正予算　：53．3億円
令和5年度当初予算　：27．1億円

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

令和6年度予算　：29．0億円（25．7億円）

○ 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

令和6年度予算　：　1．4億円（ 1．4億円）
令和5年度補正予算　：53．3億円

○ 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
・診療録等の電子的記録やネットワーク利用が進展する中、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5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の支援
○ 医療機器サイバーセキュリティ対策に係る支援事業
・令和5年改正の基本要件基準に基づく医療機器サイバーセキュリティ対策への理解・対応を促すため医療機器製造販売業者に講習会等を実施
・国内の医療機器製造販売業者に対し、ソフトウェア部品表の導入やサポート期間終了が近い医療機器への対応状況等の調査を行い、その結果に基づき医療機器サイバーセキュリティ対策に係る手引書の更新等を実施
○ 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

経済産業省

サイバーセキュリティ経済基盤構築事業

令和6年度予算額 20億円（20億円）

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

企業等の経済活動におけるサイバーセキュリティ確保に向けた取組を実施し、深刻化が進むサイバー攻撃が国民生活や経済活動に大きな影響を及ぼすことのないように備えるとともに、企業における深刻な事業リスクであるサイバー攻撃等の事象への対応能力の向上等を目的とする。

事業概要

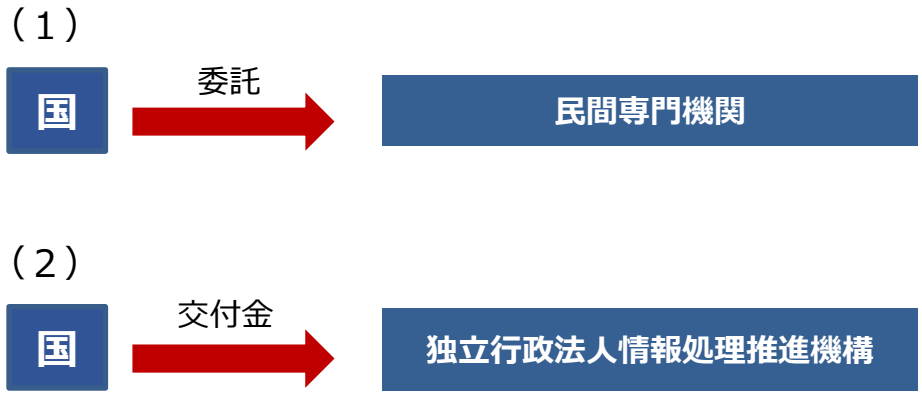
（１）日々高度化が進み、国境を越えて行われるサイバー攻撃に対処するため、先進国をはじめとして100か国以上の国に設置されているサイバー攻撃対応連絡調整窓口（窓口CSIRT※１）の間で情報共有を行うとともに、共同対処等を行う。（委託）

（２）サイバー攻撃被害の経済全体への連鎖を抑制し被害低減を図るため、経済社会に被害が拡大するおそれが強く、個々の能力では対処が困難な深刻なサイバー攻撃を受けた組織に対し、独立行政法人情報処理推進機構のサイバーレスキュー隊（J-CRAT※2）により、被害状況を把握し、再発防止の対処方針を立てる等の初動対応支援を行うことで、深刻化するサイバー攻撃から重要インフラ事業者等を守る。（交付金）

※1 Computer Security Incident Response Teamの略。

※2 Cyber Rescue and Advice Team against target attacked of Japan

事業スキーム（対象者、対象行為、補助率等）



成果目標

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。

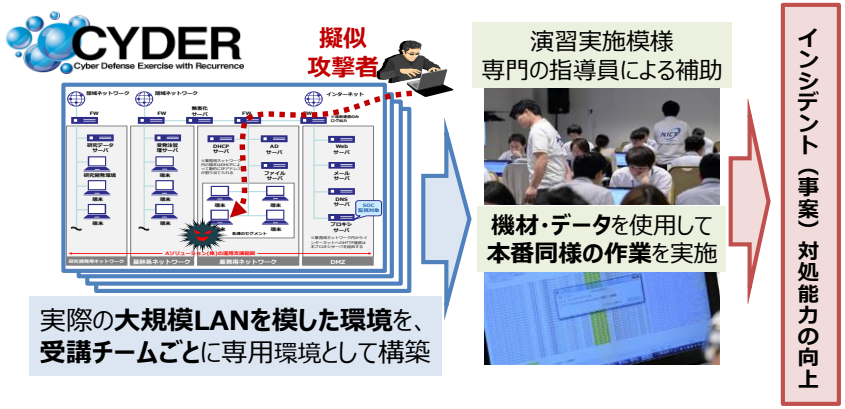
総務省

ナショナルサイバートレーニングセンターの強化

● 巧妙化・複雑化するサイバー攻撃に対し、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し、我が国のサイバーセキュリティを強化。

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た実践的サイバー防御演習（CYDER）を実施。



②CIDLE（万博向けサイバー防御講習）

2025年日本国際博覧会（大阪・関西万博）開催に向けて、万博関連組織の情報システム担当者等を対象として、CYDERの知見を活用した人材育成の演習等プログラムである万博向けサイバー防御講習（CIDLE）を実施。 **0.4**

③SecHack365（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。

（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6年度予算額 1,742百万円（令和5年度予算額 1,270百万円）

外務省の施策例

外務省

外務省サイバーセキュリティ施策

令和５年度当初予算額　：　７．５億円
令和６年度予算額　：　１１．９億円

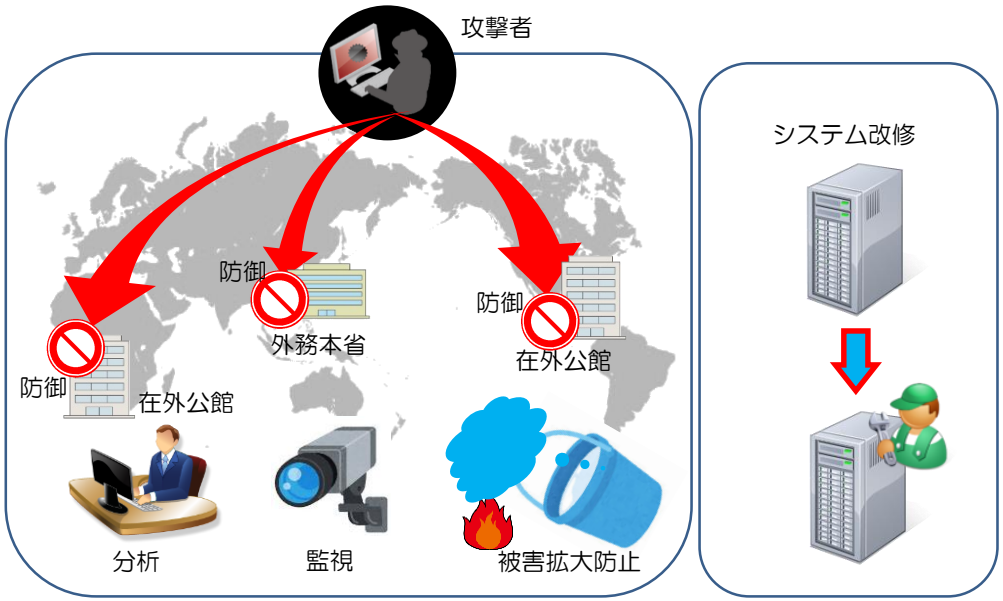
情報セキュリティ対策の強化

令和６年度予算額：１１．２億円

事業目的･概要

○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。

○事業概要
・不正通信の監視、同監視装置の更改及び新規配備。
・セキュリティインシデント対応チームによるログ分析、フォレンジック等の事案解明及び対処。
・ペネトレーションテストやセキュリティ監査の実施。



サイバー空間に関する外交及び国際連携

令和６年度予算額：０．７億円

事業目的･概要

○目的
　近年のサイバー空間における脅威の増大を背景に、一昨年閣議決定した「国家安全保障戦略」も踏まえて、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。

○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

サイバー捜査用資機材の増強等

警察庁

概要

サイバー特別捜査隊（現在はサイバー特別捜査部）等にサイバー捜査に必要な資機材の増強・整備等を行う。

令和６年度予算額　：　３．６億円
令和５年度補正予算額：　２．３億円
令和５年度当初予算額：　３．２億円

現状

○令和４年４月に設置したサイバー特別捜査隊は、重大サイバー事案について、部門を越えた捜査を展開し、確実に成果を上げつつある。
○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

強化

公開情報捜査、犯罪収益捜査を通じて取得した重大サイバー事案の捜査に必要な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

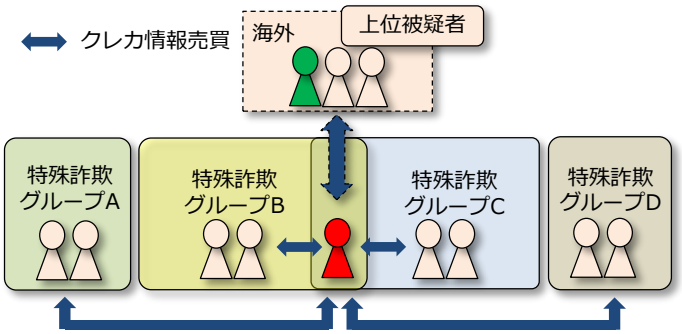
サイバー捜査分析用資機材
（令和６年度予算）

全国的・部門横断的な情報の分析

報告 ⇑⇓ 指示

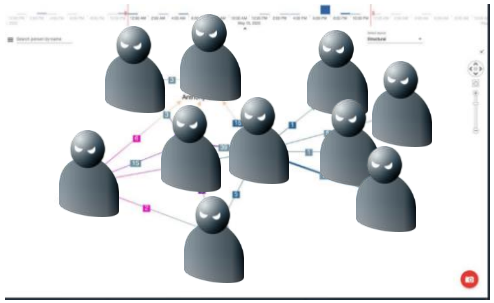
サイバー特別捜査隊（現在はサイバー特別捜査部）

公開情報捜査



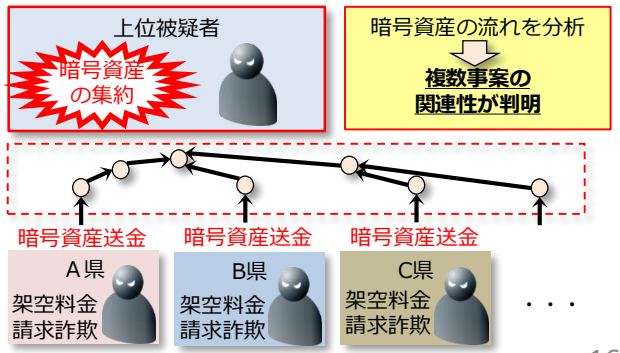
犯罪収益等捜査情報分析用資機材

（令和５年度補正予算）



関係者間の関連性分析の自動化

犯罪収益捜査



違法・有害情報対策に伴う経費

警察庁

概要

警察庁では、インターネット利用者等から、違法情報等に関する通報を受理し、警察への通報やサイト管理者等への削除依頼を行うインターネット・ホットラインセンター（ＩＨＣ）と重要犯罪密接関連情報及び自殺誘引等情報を収集し、ＩＨＣに通報するサイバーパトロールセンター（ＣＰＣ）を事業委託しているところ、犯罪実行者募集情報をＩＨＣやＣＰＣの取扱情報の範囲に追加するため、体制を強化する。

令和６年度予算額　　：２．６億円
令和５年度当初予算額：２．０億円

① IHCにおける取扱情報の範囲の拡充

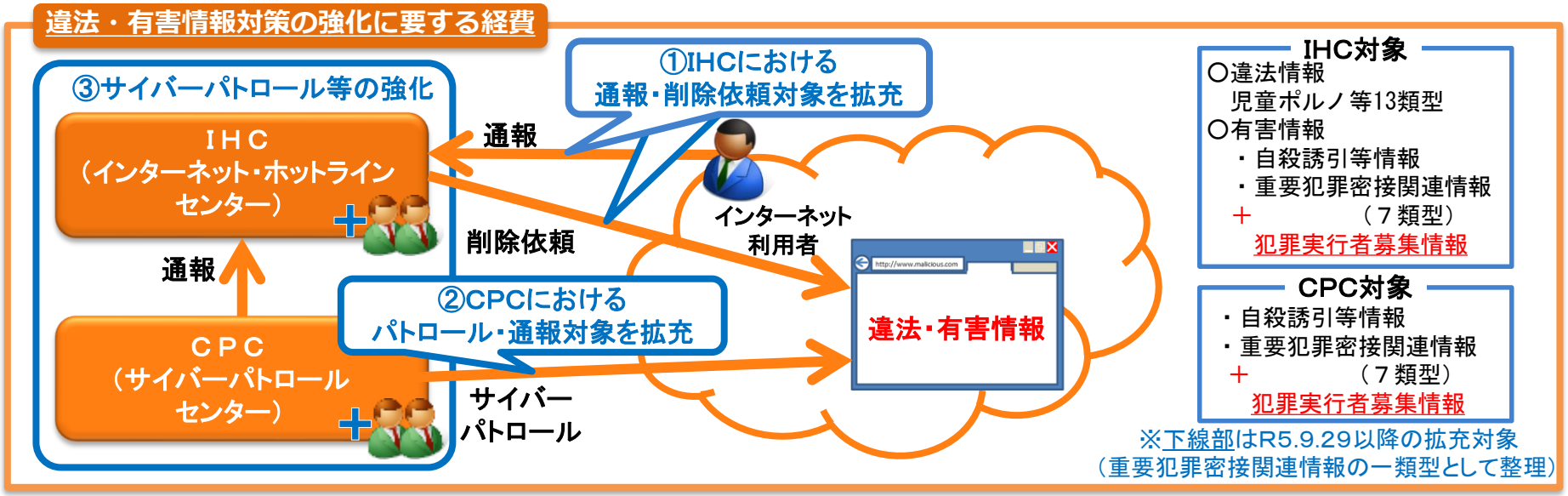
IHCにおける取扱情報の範囲（現行は、違法情報、自殺誘引等情報及び重要犯罪密接関連情報）に、著しく高額な報酬の支払を示唆して行う犯罪の実行者を直接的かつ明示的に誘引等（募集）する情報（以下「犯罪実行者募集情報」という。）を追加することにより、違法・有害情報対策の強化を図る。

② CPCにおける取扱情報の範囲の拡充

CPCにおける取扱情報の範囲（現行は自殺誘引等情報及び重要犯罪密接関連情報）に、犯罪実行者募集情報を追加することにより、有害情報対策の強化を図る。

③ サイバーパトロール等の強化

爆発物・銃砲等の製造等に関する重要犯罪密接関連情報や犯罪実行者募集情報の排除等に向け、CPCにAI検索システムを運用し、当該情報の収集を行うなど、運用体制を強化する。



デジタル庁

サイバーセキュリティ確保環境整備費（セキュリティ班）

６年度予算額　１．３億円
（５年度予算額　１．３億円）

事業概要・目的

○ 近年、システムの脆弱性やバックドア等を利用した攻撃を含むセキュリティインシデントが深刻化する中、デジタル庁においても、情報システムの設計・開発段階を含め、セキュリティ対策の強化を図ることが重要です。

○ 特に、新たなセキュリティ脅威や攻撃手法を踏まえてサイバー攻撃に強いシステムを企画段階から設計（セキュリティ・バイ・デザイン）するほか、運用・保守段階を含め検証・監査等を実施し、システムの脆弱性を未然に発見・防止することで、システムライフサイクル全体で対策を確実に実行します。

○ 加えて、デジタル庁の情報システムに関与するシステム管理者からビジネス/リスクオーナーが、セキュリティ・バイ・デザインの考えに基づき、政府情報システムのセキュリティ確保のための対策を実施できる環境を整えるとともに、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、職員の情報セキュリティに係る意識の向上及び知見の習得を図ります。

事業イメージ・具体例

○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・調査等を実施します。

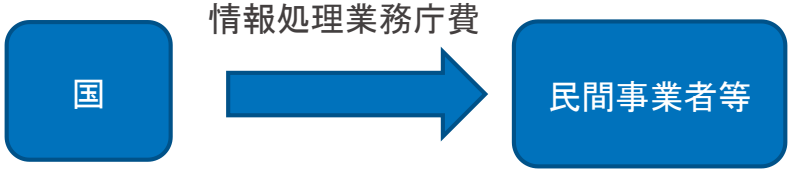
○バックドア等検証
デジタル庁内のシステムの提供に際して、安全性を確保するため、ソフトウェア構成管理を活用した脆弱性・バックドアへの対策を実施します。

○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
デジタル庁の情報システムの企画・開発・整備・運用に携わる職員が各工程で把握し、実務で活かす事を目的としたセキュリティ評価等のスキル形成等を実施します。

○CSIRT要員の研修の実施
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す。

○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します。

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（企画設計時のセキュリティ・バイ・デザイン、検証・監査）、②問題が発生した際には被害を最小限にする（インシデント対応時）を実現することで、システムのセキュリティを確保します。

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

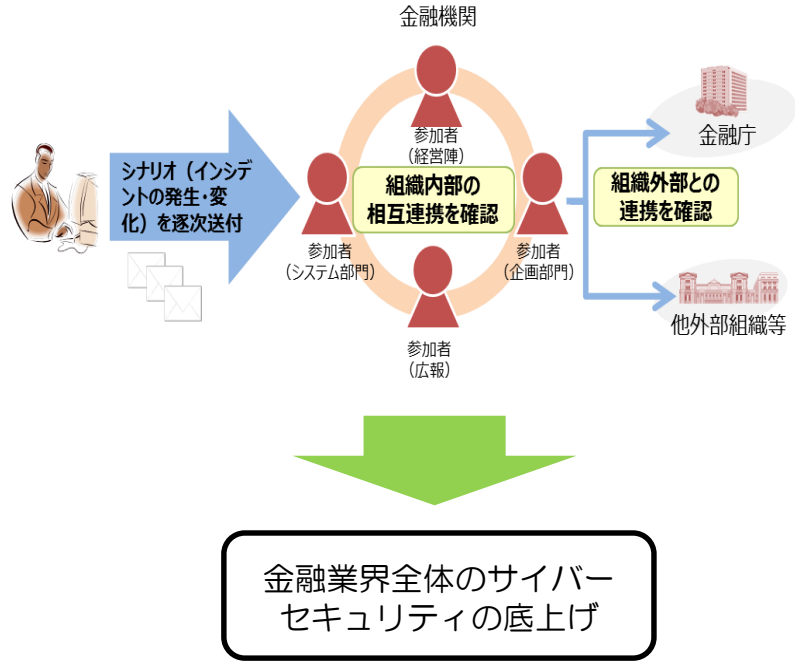
令和６年度予算額：0.9億円
（令和５年度当初予算：0.9億円,令和５年度補正予算：1.5億円）

事業概要

- 金融分野に対するサイバー攻撃の複雑化・巧妙化が進む中、サイバーセキュリティにかかる態勢の整備は、金融システム全体の安定のため喫緊の課題。
- サイバーセキュリティにかかる態勢整備のためには、演習を通じて、現在の対応態勢が十分であるか、何が不足しているのかを確認し、必要なリソースを割り当てるなどのPDCAサイクルを回していくことが有効。
- 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６年度も、９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



総務省

地方公共団体の情報セキュリティ対策の推進

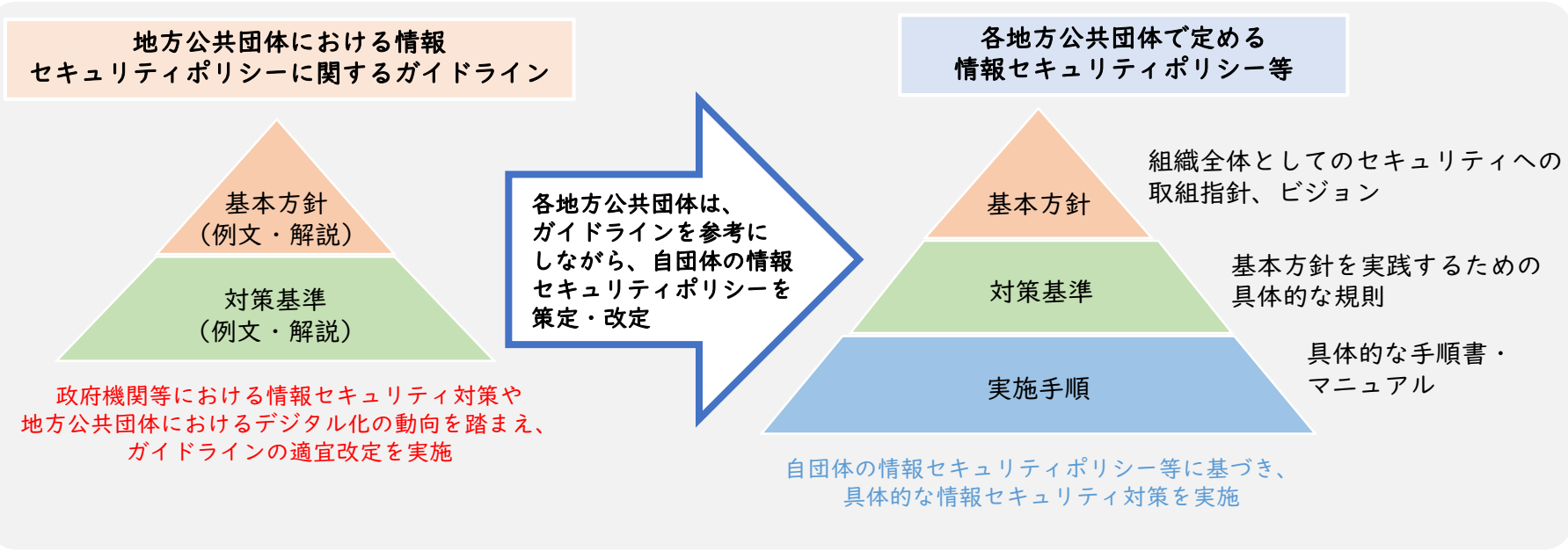
【主な経費】 地方公共団体の情報セキュリティ対策の強化に要する経費　令和6年度予算額 74百万円
（令和5年度予算額 74百万円）

施策概要

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検討を行う。

総務省は、地方公共団体の情報セキュリティ対策を支援するため、平成13年度に自治体情報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、その後も、政府機関等における情報セキュリティ対策や地方公共団体におけるデジタル化の動向等を踏まえながら適宜ガイドラインの改定を実施してきた。

地方公共団体の業務システムの標準化・共通化を踏まえたガバメントクラウドの利活用や、新しい住民サービスの提供、高度化・巧妙化しているサイバー攻撃への対応を可能とするため、最新のセキュリティ関連技術の動向や地方公共団体の実態の調査を行い、最適なネットワーク構成となるような自治体情報セキュリティ対策の在り方について検討を実施する。



内閣官房

（内閣サイバーセキュリティセンター）

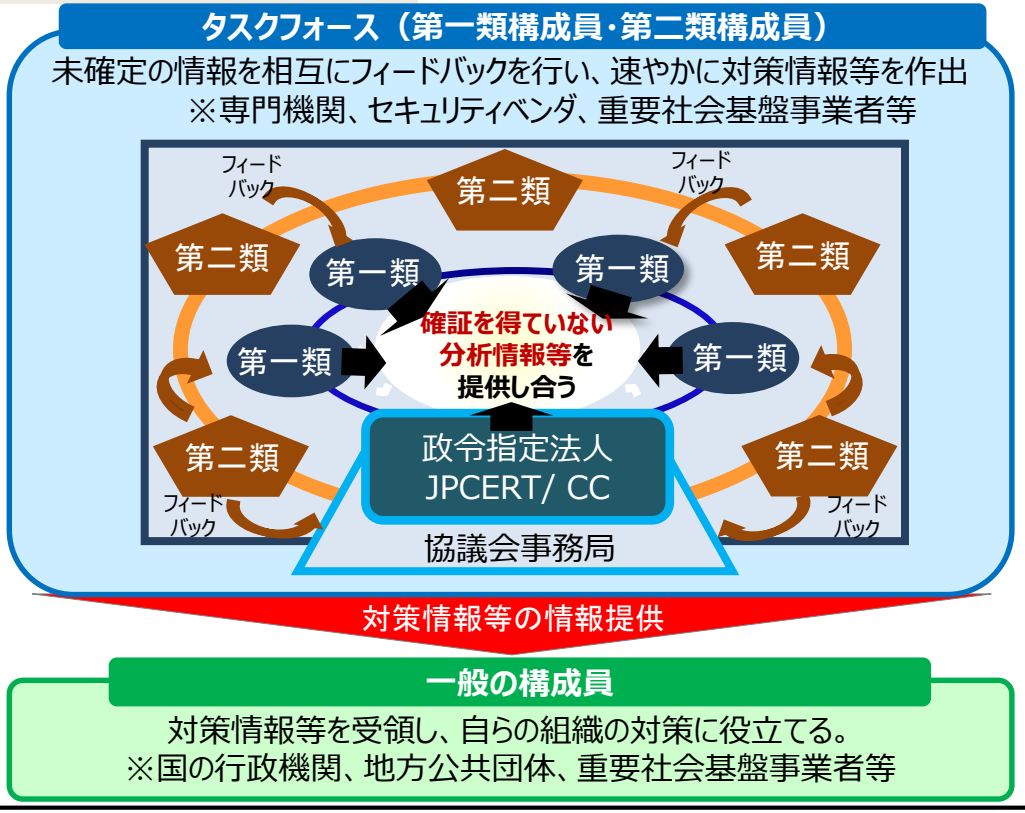
サイバーセキュリティ協議会の運用

令和６年度当初予算額　　０．６億円
（令和５年度当初予算額　０．８億円）

事業概要・目的

○平成30年12月に成立したサイバーセキュリティ基本法の一部を改正する法律に基づき、平成31年４月、国の行政機関、重要社会基盤事業者、サイバー関連事業者等、官民の多様な主体が相互に連携し、より早期の段階で、サイバーセキュリティの確保に資する情報を迅速に共有することにより、サイバー攻撃による被害を予防し、また、被害の拡大を防ぐことなどを目的とする「サイバーセキュリティ協議会（以下「協議会」という。）」が組織されました。
○協議会の情報共有活動の核となる連絡調整業務は、政令で指定されたJPCERTコーディネーションセンターに委託して実施しています。
○デジタル改革の進展やコロナ禍の影響も踏まえた「ニューノーマル」と呼ばれる生活様式が浸透する中、サイバーセキュリティに関する脅威は複雑化・巧妙化しており、協議会においては、引き続きサイバーセキュリティの確保に資する情報を協議会構成員等に対して迅速かつ確実に共有するとともに、より多くの主体が参加する重厚な体制を構築していくことが今まで以上に求められています。

事業イメージ・具体例



期待される効果

○政令指定法人であるJPCERT/CCと連携して、自組織単独ではまだ確証を得るに至っていない早期の段階で、脅威情報等を共有・分析するとともに、確度の高い対策情報等を作出し、国の行政機関、地方公共団体や重要社会基盤事業者等に対し迅速に共有することで、サイバー攻撃による被害を予防し、また、被害の拡大を防ぐことが可能となります。

内閣官房

（内閣サイバーセキュリティセンター）

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

令和６年度当初予算額　　０．４億円
令和５年度補正予算額　　４．７億円
（令和５年度当初予算額　０．５億円）

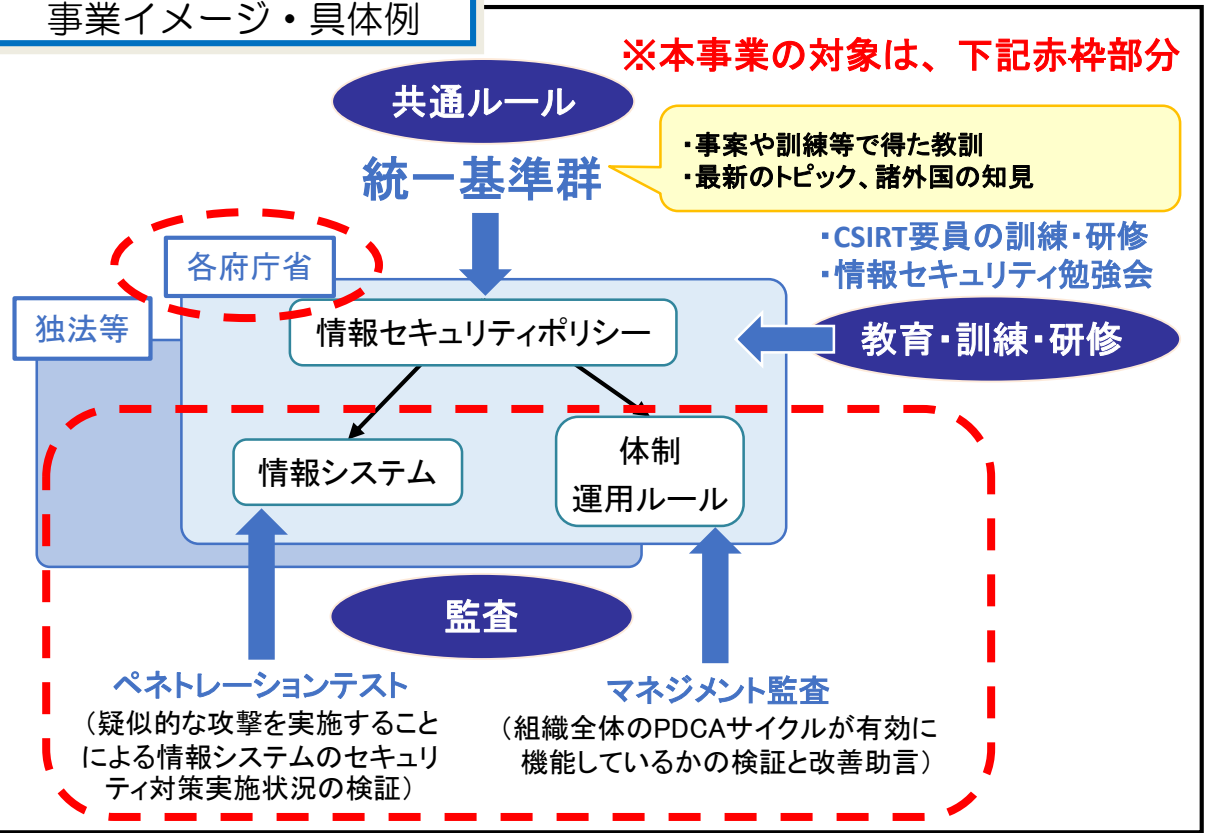
事業概要・目的

戦略本部がサイバーセキュリティに関する施策を総合的かつ効果的に推進するため、府省庁等のサイバーセキュリティ対策に関する現状を、情報システムに対する「マネジメント監査」と「ペネトレーションテスト（侵入試験）」を行うことにより評価し、NISCからの助言を通して、府省庁等におけるサイバーセキュリティ対策を強化します。

また、これまでの監査を踏まえ、引き続き、外局や地方組織等が管理する情報システムも含めて監査対象として検討するとともに、近年の脅威動向・状況変化を踏まえたリスク対応が行われているか等について確認を強化すること等により、監査の充実を図り、ひいては政府全体としてセキュリティ対策の底上げを進めていく必要性があります。

※（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）。

事業イメージ・具体例



期待される効果

府省庁等は、監査を通じて情報システムの個別具体的な脆弱性や体制不備等を把握し、対策を講じることによって、情報漏えいリスクやサイバー攻撃リスクを適時に低減し、行政サービスの信頼性や安定性の向上が期待できます。さらに、投資計画の策定に当たり、総花的な対策ではなく重点的な対策や予算が措置できます。

内閣官房

（内閣サイバーセキュリティセンター）

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

令和６年度当初予算額　　０．４億円
令和５年度補正予算額　　４．４億円
（令和５年度当初予算額　０．３億円）

事業概要・目的

サイバーセキュリティ基本法第31条第1項※の規定（事務の委託）に基づき、ＮＩＳＣが実施する「施策の評価（監査）事務」のうち「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に基づく評価（監査）」について、（独）情報処理推進機構（ＩＰＡ）に委託して実施します。

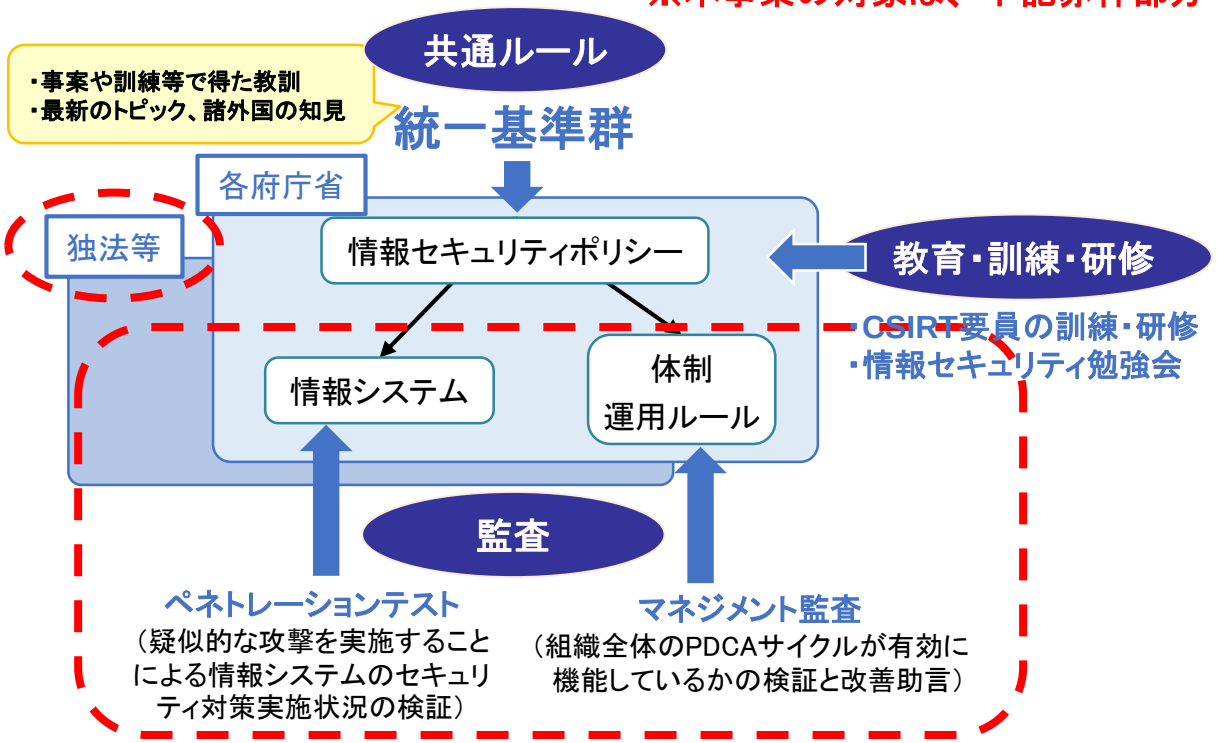
令和６年度においても、各独法等が自律的な情報セキュリティ対策への取組を促進し、情報セキュリティ水準の向上を図ることを目的として監査を実施します。

※（事務の委託）
第三十一条　本部は、次の各号に掲げる事務の区分に応じて、当該事務の一部を当該各号に定める者に委託することができる。

一　第二十六条第一項第二号に掲げる事務（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に基づく監査に係るものに限る。）又は同項第三号に掲げる事務（独立行政法人又は指定法人で発生したサイバーセキュリティに関する重大な事象の原因究明のための調査に係るものに限る。）　独立行政法人情報処理推進機構その他サイバーセキュリティに関する対策について十分な技術的能力及び専門的な知識経験を有するとともに、当該事務を確実に実施することができるものとして政令で定める法人

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

独立行政法人・指定法人は、監査を通じて情報システムの個別具体的な脆弱性や体制不備等を把握し、対策を講じることによって、情報漏えいリスクやサイバー攻撃リスクを適時に低減し、法人が提供するサービス等の信頼性や安定性の向上が期待できます。さらに、投資計画の策定に当たり、総花的な対策ではなく重点的な対策や予算が措置できます。

内閣官房

（内閣サイバーセキュリティセンター）

サイバーセキュリティインシデントに係る調査

令和６年度当初予算額　　０．３億円
令和５年度補正予算額　　０．５億円
（令和５年度当初予算額　０．８億円）

事業概要・目的

○「サイバーセキュリティ基本法」※では、国の行政機関等において発生したサイバーセキュリティに関する重大な事象（以下、「特定重大事象」という。）に対して、原因究明のための調査を含む施策の評価を行うこととされています。

○技術的知見等を蓄積している民間企業等を活用して特定重大事象に対する調査等を行い、その結果を国の行政機関等で適切に共有することにより被害の拡大防止を行うことを目的としています。

※（所掌事務等）
第26条①３　国の行政機関、独立行政法人又は指定法人で発生したサイバーセキュリティに関する重大な事象に対する施策の評価（原因究明のための調査を含む。）（略）。

事業イメージ・具体例

○行政機関等において職員利用端末のマルウェア感染による情報漏えい等の特定重大事象が発生するなどした際に、専門的な知見による詳細な調査を実施します。

○主な調査内容は以下のとおりです。
・職員利用端末等の解析
・各種サーバ等の解析
・通信履歴等のログの解析　等

期待される効果

○民間企業等による調査の解析結果を適切に共有することで、国の行政機関等における被害の拡大防止や政府内部での技術的知見の蓄積、技術力の向上等に役立てます。また、調査により判明した攻撃手法及び最新の情報セキュリティ技術等の詳細情報は、政府機関の情報セキュリティ対策のための統一基準の作成等にフィードバックすることが可能になります。

国土交通省の施策例

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

令和６年度予算額：0.６億円
（令和５年度当初予算額：0.５億円）

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）

防衛省の施策例

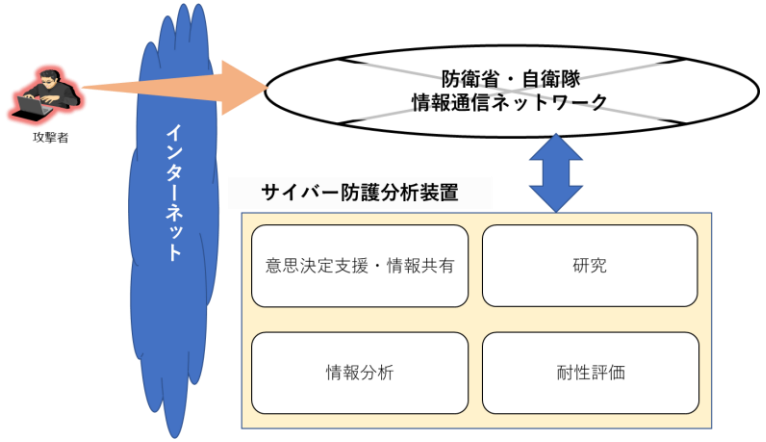
情報システムの防護

令和6年度当初予算額：1，064．0億円（令和5年度当初予算額：477．4億円）

（令和6年度当初予算額の具体例）

◆ **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

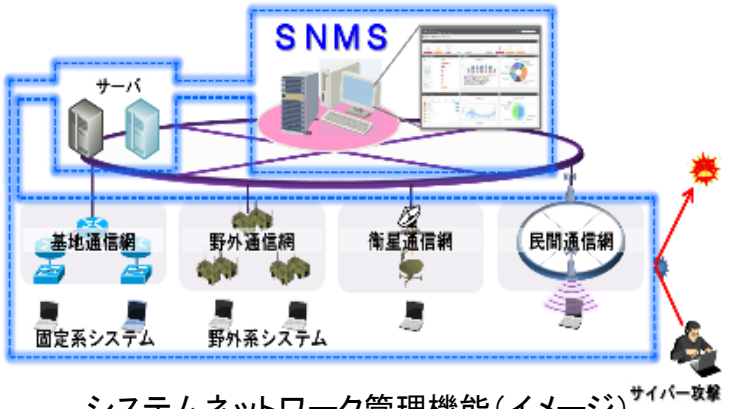


サイバー防護分析装置（イメージ）

◆ **システムネットワーク管理機能の整備**

陸上自衛隊の全システムの防護、監視、制御等を一元的に行うシステムを整備

※　SNMS：システム・ネットワークマネージメントシステム



システムネットワーク管理機能（イメージ）

◆ **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

防衛省の施策例

リスク管理枠組み（RMF）の導入

令和6年度当初予算額：290．8億円（令和5年度当初予算額：301．1億円）

（令和6年度当初予算額の具体例）

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」

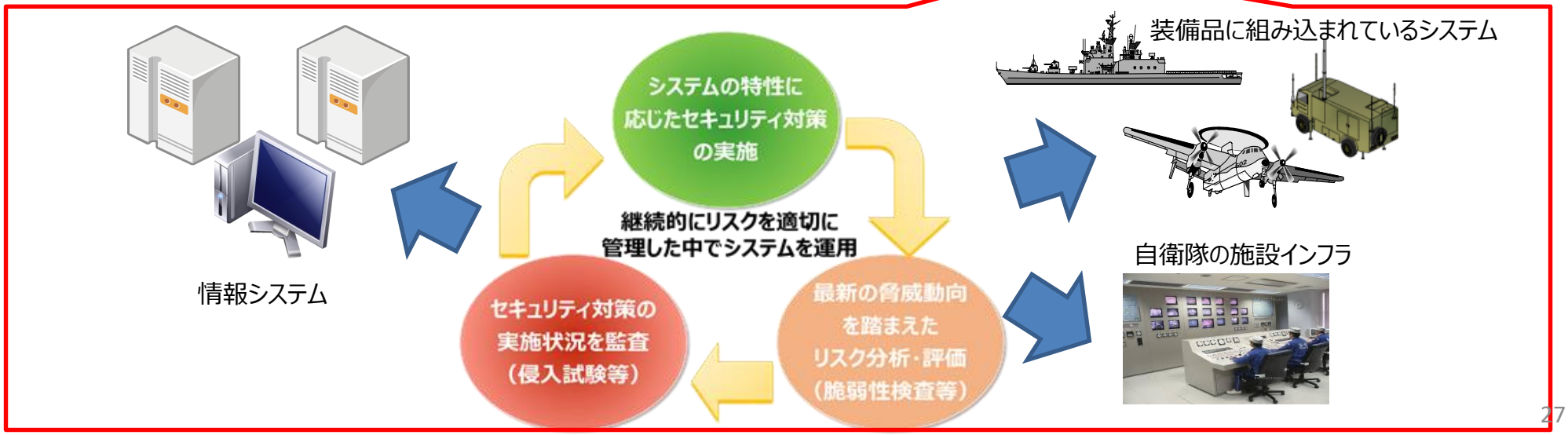
ＮＩＳＴ　ＳＰ８００－３７
（リスク管理枠組み（Risk Management Framework：RMF））

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

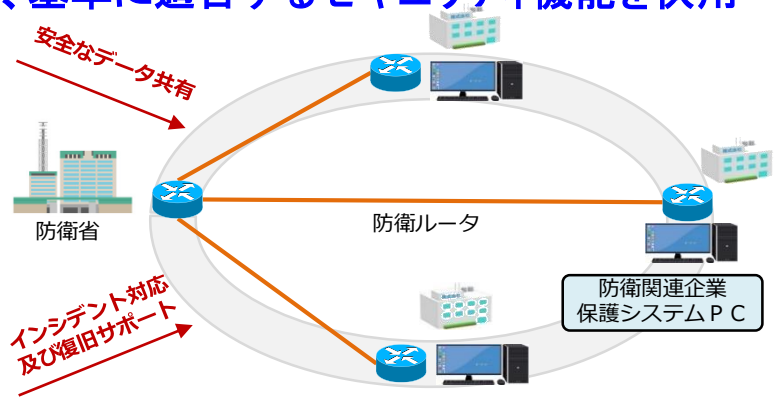
防衛産業におけるサイバーセキュリティ対策の強化

令和6年度当初予算額：119．8億円（令和5年度当初予算額：68．5億円）

（令和6年度当初予算額の具体例）

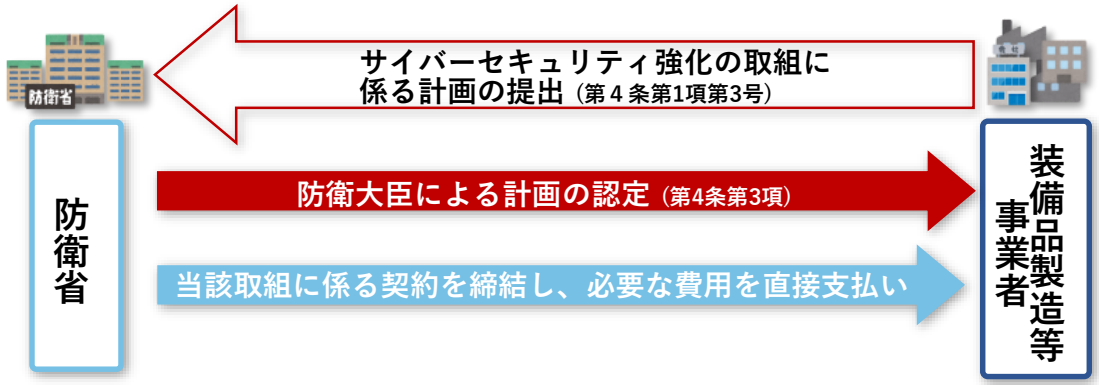
◆ 防衛セキュリティゲートウェイの整備

官民共用クラウドを導入し、基準に適合するセキュリティ機能を供用



◆ 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



防衛省の施策例

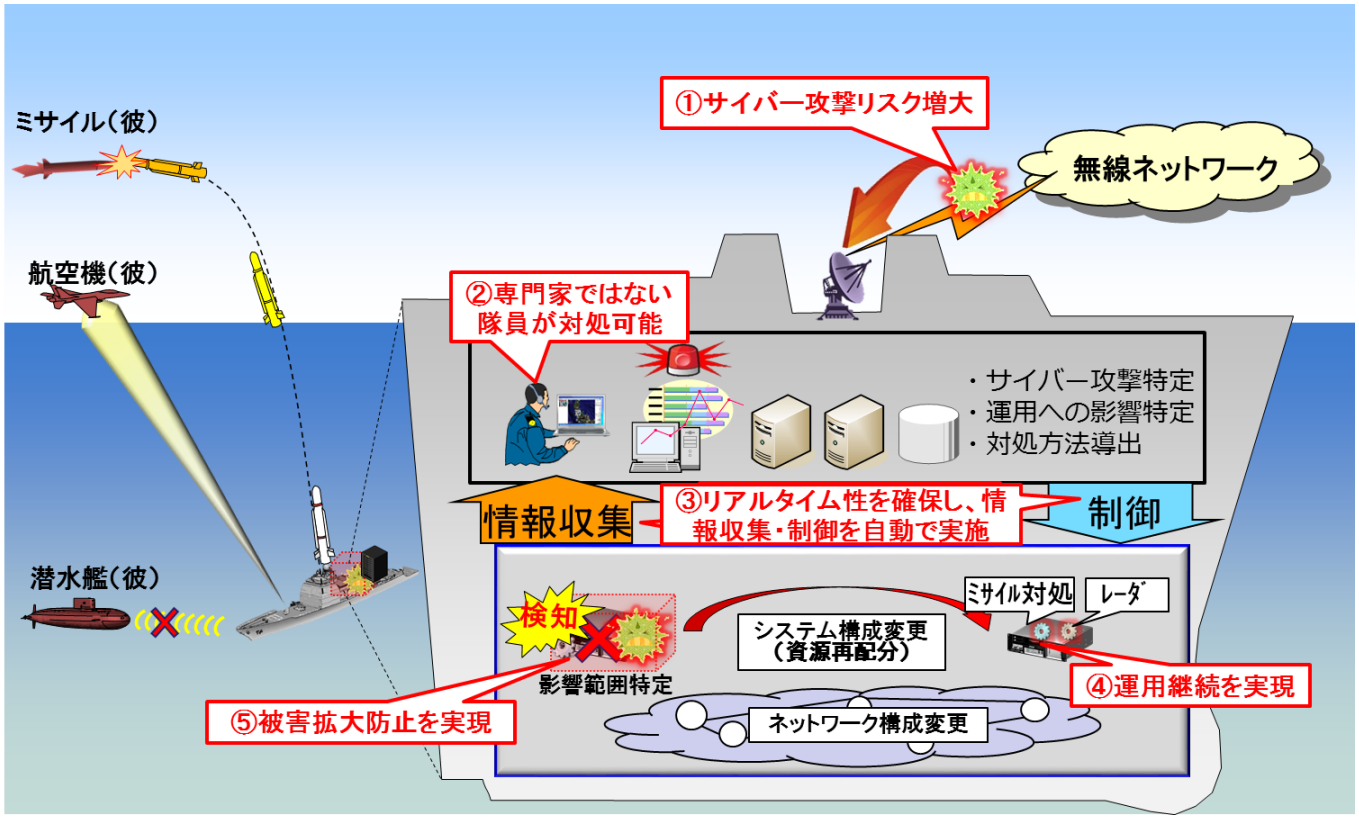
サイバー分野における研究機能の強化

令和6年度当初予算額：20．9億円（令和5年度当初予算額：14．6億円）

（令和6年度当初予算額の具体例）

◆ **装備システム用サイバー防護技術の研究**

サイバー攻撃による被害拡大の防止やシステムの運用継続を図るため、装備システム用サイバー防護技術を研究



装備システム用サイバー防護技術の研究（イメージ）

サイバーテロ対策用資機材の増強等

警察庁

概要

国境を越えて行われるサイバー攻撃の被害の未然防止・拡大防止に資するため、サイバー空間の観測・分析を行っている装置等の更新及び機能の強化。

令和６年度予算額　：１１．７億円
令和５年度補正予算額：　０．４億円
令和５年度当初予算額：　４．３億円

目的

○高度化・複雑化が進むサイバー攻撃の被疑者の検挙・攻撃手法の特定及びアトリビューション
○サイバー攻撃の未然防止・被害拡大防止

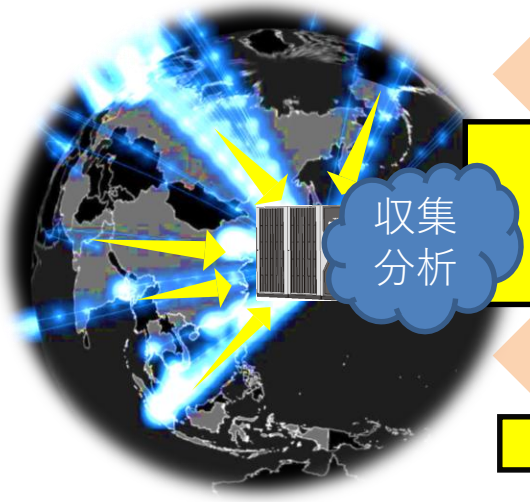
現状

○24時間体制でインターネット上に設置したセンサーに対するアクセス情報を集約・分析
○DoS攻撃の発生や不正プログラムに感染したコンピュータの動向を把握
○インターネット観測結果を重要インフラ事業者等に情報提供、ウェブサイト上に公開して注意喚起

機能を見直し

強化

○サイバー攻撃の最近の傾向を踏まえた機能を強化
○オープンソース情報等を活用した、多角的な分析を実施



最新の脅威情報の直接照会

・不審なアクティビティの分析
・脅威アクターの特定
・認知事案の通知
・脅威情勢の提供

分析結果等の照会

注意喚起

サイバー特別捜査隊
都道府県警察

管区・都道府県
情報技術解析課

重要インフラ事業者等
一般インターネット利用者

効果

被疑者の検挙
攻撃手法の特定
アトリビューション

効果

未然防止
被害拡大防止

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6年度当初予算額：25．5億円（令和5年度当初予算額：20．1億円）

（令和6年度当初予算額の具体例）

◆ **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

◆ **サイバー等安全保障研究体制の強化**

サイバーの領域を含め、戦略的・機動的な防衛政策の企画立案を支援するために防衛研究所の機能を強化

陸自システム通信・サイバー学校の教場（イメージ）

GIGAスクールにおける学びの充実

令和6年度予算額　3億円
（前年度予算額　3億円）
令和５年度補正予算額　2億円

文部科学省

現状・課題

個別最適な学びと協働的な学びの一体的な充実など、教育の質を向上させるために、「GIGAスクール構想」の下で児童生徒の１人１台端末及び通信ネットワーク等の学校ICT環境での新しい学びが本格的に開始されている。各学校において学習者用情報端末などを活用した学習活動が一層促進されるよう、ICT 環境を積極的に活用する中で一つ一つの課題の解決を図りながら、改善に取り組む必要がある。

事業内容

端末の活用状況を把握・分析するとともに、日常授業の改善を中心とする効果的な実践例（指導技術、指導プログラム）を創出・モデル化し、都道府県等の域内で校種を超えて横展開し全国展開することで、端末更新期を迎える前に、全国すべての学校でICTの「普段使い」による教育活動の高度化を実現する。

○GIGAスクール構想の加速化事業（伴走支援強化・先進事例創出）

GIGAスクール第１ステージ半ばで顕在化した自治体間格差を解消するため、令和５～６年を集中推進期間と位置づけており、効果的な実践事例を創出・横展開するとともに、伴走支援を徹底強化する必要がある。また、GIGAスクール構想第２ステージに向けては、準備が整った自治体・学校において生成AIの適切な活用や高度なプログラミング教育、デジタルものづくりなどの先進事例を創出する必要がある。

学校DX戦略アドバイザー

・課題を抱える自治体・学校にアドバイザーの国費派遣（ICT活用に関する学識経験者、先進地域関係者、ネットワークや情報セキュリティ、ICT支援、AI等の専門家）
・事前の調整により、年間を通じて計画的にオンライン/現地派遣を組み合わせて集中的な伴走支援を行うスタイルも新たに実施。

リーディングDXスクール　令和５年度補正予算額　２億円

実施内容①
・GIGA端末とクラウド環境の徹底活用による教育活動の高度化
・指定校が実施する様々な実践例から効果的な指導技術を創出・展開（都道府県・指定都市に1箇所以上設置）
・１人１台端末の活用状況の把握・分析

実施内容②
・生成AIを活用した授業実践研究 ※ガイドラインを遵守 ※効果的な取組実践を創出する観点から、学術的知見を有する研究者や優れた実践家等から伴走支援を受けること（学校DX戦略アドバイザーの支援含む）
・生成AI を用いた取組の成果に関し、年度末に実施する成果報告会で発表（予定）

○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、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。

- 情報モラル教育指導者セミナーの実施
- 情報モラル指導モデルカリキュラム表の再整理
- 情報モラルを含む情報活用能力ポータルサイトによる情報発信
- 情報モラル教育の推進に係るコンテンツ（動画教材等）の充実

○児童生徒の情報活用能力の把握に関する調査研究

令和５年度に予備調査を実施し令和６年度に本調査を実施予定
（前回調査令和３年度）
プログラミング教育によって育成される資質・能力も含め、「情報活用能力」を構成する要素を児童生徒がどの程度身に付けているかを測定し、それを踏まえて、今後の情報教育関係施策の改善等に活用。

- 調査問題の妥当性等を検証するための予備調査の検証など
- 次回本調査に向けた準備・実施

（担当：初等中等教育局修学支援・教材課）

内閣官房

（内閣サイバーセキュリティセンター）

サプライチェーンリスク対応のための技術検証体制構築に関する調査費

令和６年度当初予算額　　０．１億円
令和５年度補正予算額　　３．２億円
（令和５年度当初予算額　０．２億円）

事業概要・目的・必要性

〇サイバー空間と実空間の一体化の進展や、サプライチェーンのグローバル化により、サプライチェーンリスクの増大が大きな課題となっています。具体的には、製品やサービスを製造・流通する過程において、不正なプログラム等の組込み・改ざんが行われるリスクへの対応など、サプライチェーンにおけるサイバーセキュリティ対策の強化が求められます。
〇また、国内外の諸情勢や、新型コロナの影響により加速するグローバルサプライチェーンの見直しの中で、我が国としてサプライチェーンリスクを検証できる能力を「中長期的」な観点で国内に涵養・蓄積していくとともに、各省庁が調達する情報通信機器等に対する信頼性の評価をはじめ、リスクを検証できる体制を構築していくことが極めて重要です。
〇このため、グローバルな動向を十分に注視し、必要な連携も図った上で、ICT製品やサービスのセキュリティの検証・評価を行うための技術検証体制を、関係府省とも連携しつつ構築します。直近3年間に行ってきた、検証スキームの検討・策定、検証の実施手法・評価方法の検討、及びそれらを踏まえた試行運用の実績に基づき、多様な検証技術の活用等を含め、技術検証を実施します。

事業イメージ・具体例

〇技術検証体制構築にかかる事業のうち、緊急的かつ初期投資的に必要となる業務を実施。

（１）機器検証の実施（定常計画検証）
・安全保障等の観点から特に関心の高い機器等について、ハイレベルな検証技術等を活用し、一定期間（3-4ヶ月程度）で計画的に検証を実施。

（２）機器検証の実施（オンデマンド検証）
・政府で調達される情報通信機器等のうち、サプライチェーン・リスクの観点から助言を実施する緊要性の高い機器等について、自動化ツール等を活用し、短期間で検証を実施。

（３）関係機関の取組状況把握調査
・上記対象機器等のサプライチェーン調査や、諸外国の政府関係機関における検証能力に関する調査を実施。

期待される効果

〇我が国としてサプライチェーンリスクを検証できる能力を国内に涵養・蓄積していくとともに、各省庁が調達する情報通信機器等の評価する体制を構築していき、我が国のサイバーセキュリティのリスクを低減することが期待されます。