政府のサイバーセキュリティに関する予算

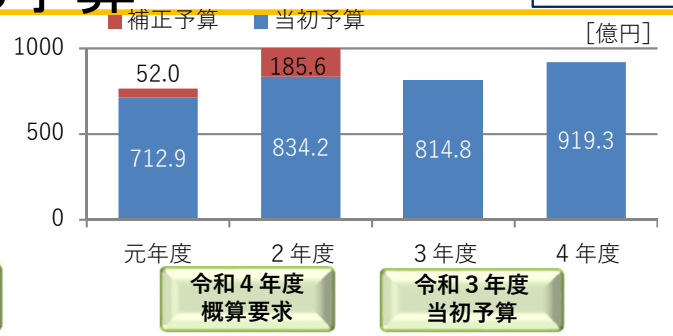
資料５

令和４年度予算概算要求額

９１９．３億円

令和３年度当初予算額
（８１４．８億円）

※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。



次期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４年度概算要求	令和３年度当初予算
(1)経済社会の活力の向上及び持続的発展	（30.8億円）	
【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	7.0 億円	7.0 億円
【経済産業省】サプライチェーン・サイバーセキュリティ対策促進事業	5.6 億円	－
【経済産業省】中小企業サイバーセキュリティ対策促進事業	3.4 億円	2.0 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	（304.8億円）	
【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	21.0 億円	22.0 億円
【経済産業省】産業系サイバーセキュリティ推進事業	21.0 億円	19.4 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	20.5 億円	19.3 億円
【総務省】サイバー攻撃インフラ検知等積極的セキュリティ対策総合実証	18.0 億円	－
【警察庁】　サイバー空間の脅威への対処能力の強化	14.9億円	－
【警察庁】　サイバー隊の設置	7.8億円	－
【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	4.3 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	4.1 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	1.8 億円	－
【内閣官房】サイバーセキュリティ対処調整センター及び情報共有システムの運用	1.0 億円	2.9 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	1.0 億円	0.8 億円
【内閣官房】サイバーセキュリティ協議会の運用	0.9 億円	0.8 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	0.8 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	0.8 億円	0.4 億円

※(　)内の数字は記載の主要事業以外も含めたそれぞれの項目の総計

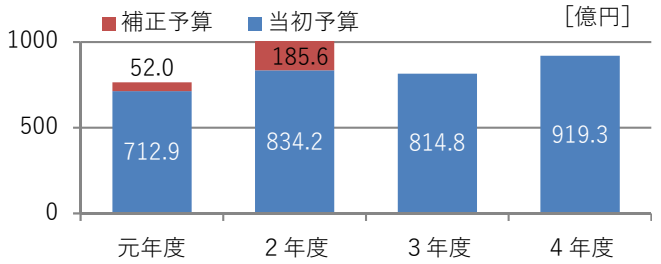
政府のサイバーセキュリティに関する予算

令和４年度予算概算要求額

９１９．３億円

令和３年度当初予算額
（８１４．８億円）

※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。



次期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

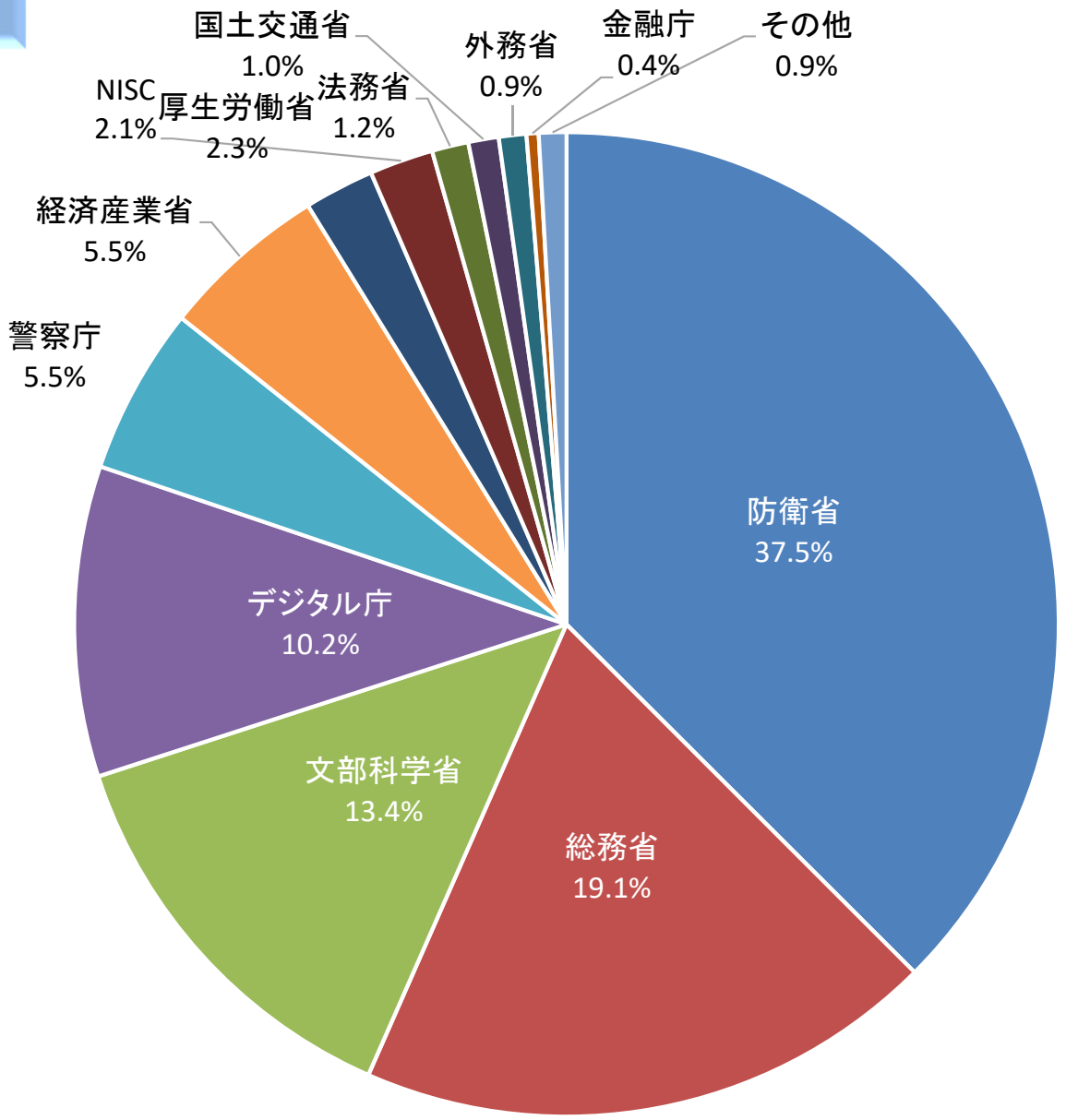
	令和４年度概算要求	令和３年度当初予算
(3)国際社会の平和・安定及び我が国の安全保障への寄与	（354.7億円）	
【防衛省】防護システムの整備	217.8 億円	202.1 億円
【防衛省】情報通信システムの安全性向上	82.9 億円	80.9 億円
【防衛省】サイバーに関する最新技術の活用	25.3 億円	10.9 億円
【外務省】サイバー空間に関する外交及び国際連携	0.6 億円	0.5 億円
(4)横断的施策（人材育成等）	（171.2億円）	
【総務省】ナショナルサイバートレーニングセンターの強化	14.0 億円	12.0 億円
【総務省】IoTの安心・安全かつ適正な利用環境の構築	11.5 億円	12.8 億円
【防衛省】サイバー人材の確保・育成	9.5 億円	6.1 億円
【文部科学省】GIGAスクールにおける学びの充実	4.6 億円	4.2 億円
【文部科学省】国立高専における情報セキュリティ人材の育成	3.3 億円	3.7 億円

※(　)内の数字は記載の主要事業以外も含めたそれぞれの項目の総計

各府省庁等のサイバーセキュリティに関する予算

令和４年度予算概算要求額

９１９．３億円



※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。

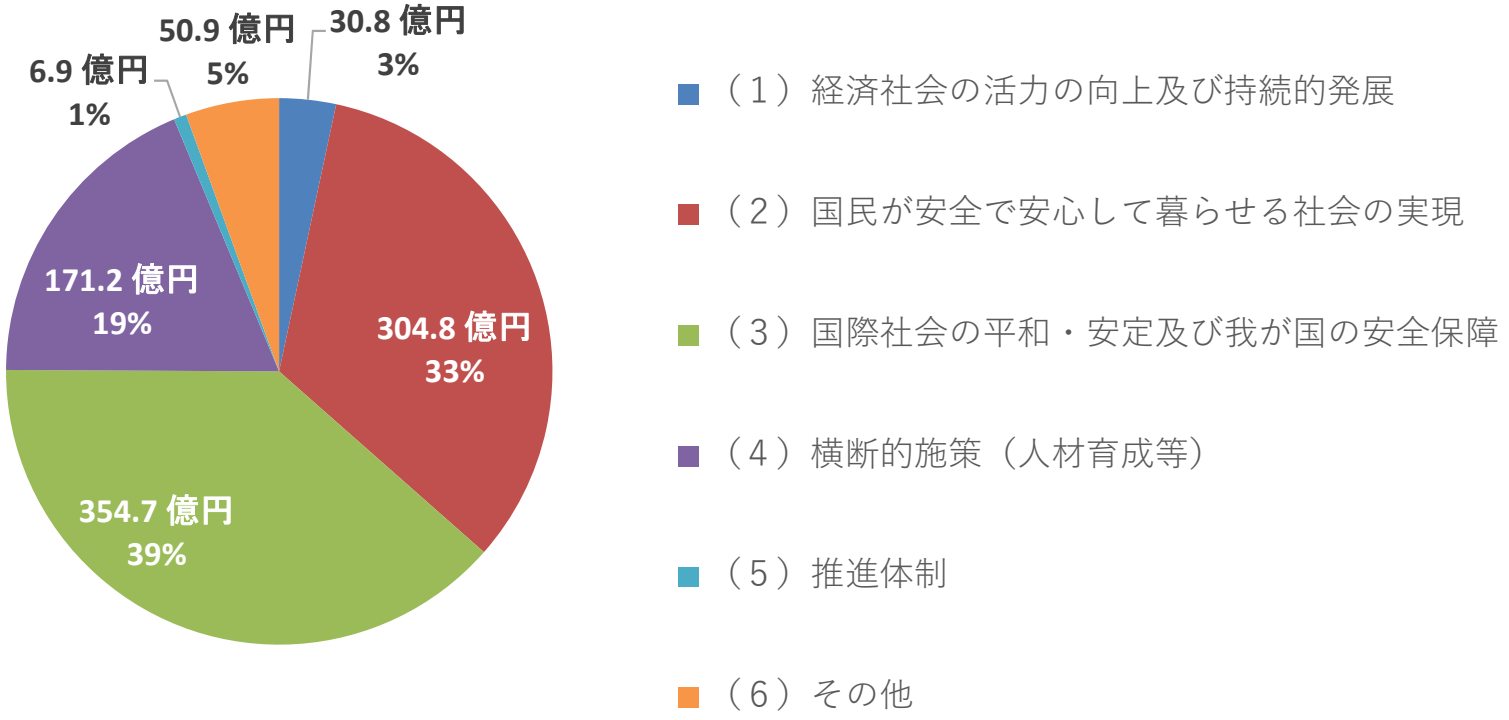
次期サイバーセキュリティ戦略　分野別内訳

令和４年度予算概算要求額

９１９．３億円

○　令和４年度予算概算要求におけるサイバーセキュリティ関連予算は、令和３年度当初予算額に比べ104.5億円増加し、919.3億円となっている。

○　次期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」が約４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３割を占めている。



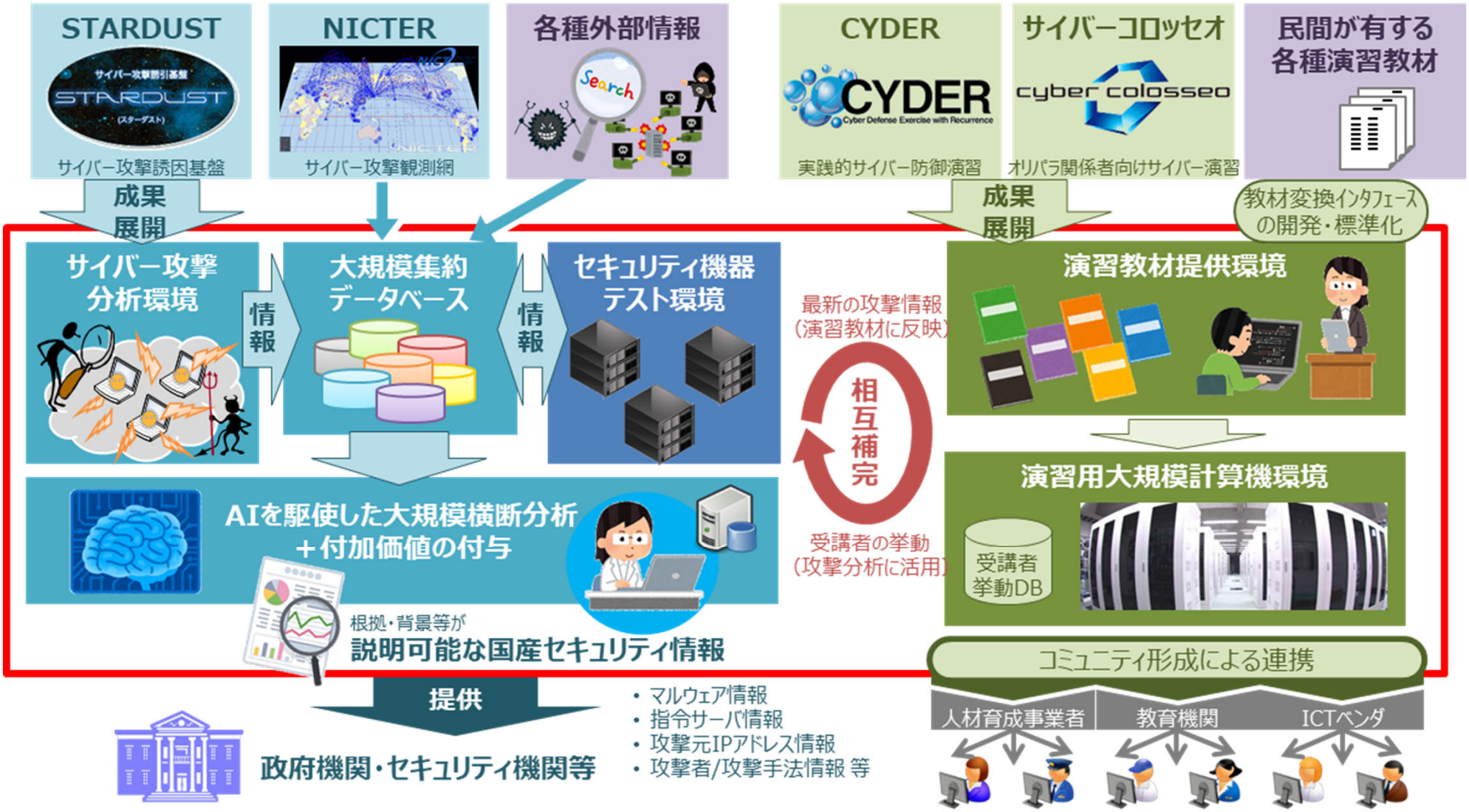
※サイバーセキュリティに関する予算として切り分けられない場合には計上していない。

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を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の向上を図る。

令和4年度要求額 7.0億円（令和3年度予算額 7.0億円）



経済産業省

サプライチェーン・サイバーセキュリティ対策促進事業

令和４年度概算要求額 5.6 億円（新規）

事業の内容

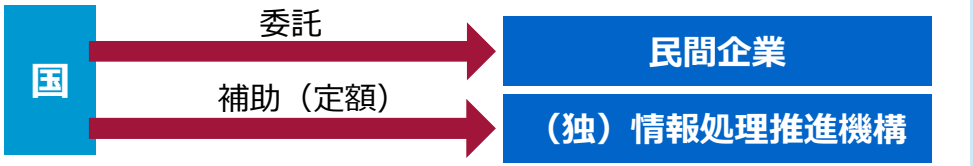
事業目的・概要

- 産業分野におけるサイバーセキュリティ確保に関して、サイバー空間とフィジカル空間の融合が進むSociety 5.0 においては、サイバー空間で流通するデータの増加による流出リスクの拡大や、サイバー攻撃起点の増大、フィジカル空間への影響の拡大が見られ、国際的にもルール形成が進んでいます。また、昨今では、セキュリティとセーフティの融合が一層進むとともに、クラウドやオープンAPIの活用により、システム等を所有するオーナー企業がシステムの全体像を把握できない課題が生じています。
- 本事業では、サプライチェーン全体でのセキュリティ確保のための産業界一丸となった対応に向けて、ガイドライン策定やソフトウェアサプライチェーン管理の高度化のための実証のほか、「開発のための投資」から「検証のための投資」へのシフトのためのセキュリティ検証事業者の育成や利用促進のための環境整備を実施します。

成果目標

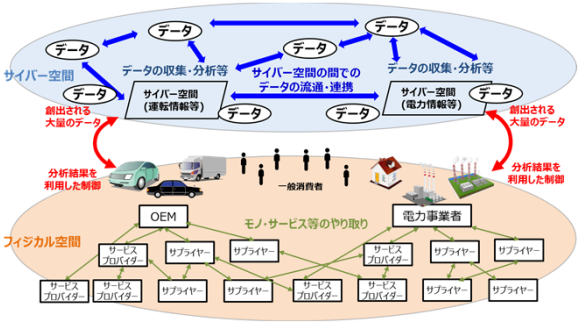
- 令和４年から令和６年まで３年間の事業であり、ガイドラインの整備等を進めることにより、7以上の産業分野でサプライチェーン全体でのサイバーセキュリティ対策が実施されることを目指します。
- ３年間の事業で、セキュリティ製品の有効性検証やセキュリティ検証ビジネスの信頼性の可視化等を実施することにより、有効性・信頼性が確認されたセキュリティ製品・サービスの数を10以上とすることを目指します。

条件（対象者、対象行為、補助率等）



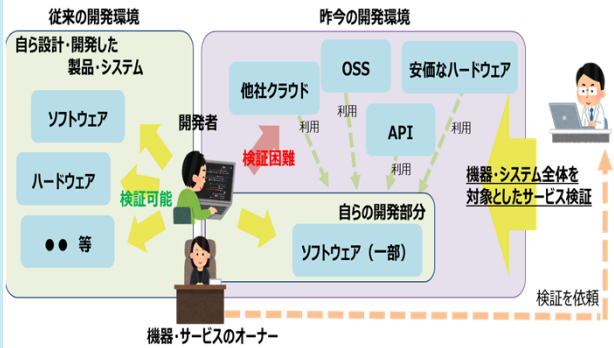
事業イメージ

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】



- サイバー空間とフィジカル空間の融合が進み、サプライチェーンが動的に構成される状況下におけるサプライチェーン全体での対策を進める必要があります。
- 業界横断的な課題や業界別の課題に対して、ガイドラインを整備することで、個々の企業による対策を超えて一体的な取組を促進する枠組みを整備します。

「開発のための投資」から「検証のための投資」への重点化促進【委託】



- OSSやオープンAPIの普及で飛躍的に改善した開発環境を支えるため、「開発」中心の投資から、「検証」中心の投資行動へのシフトが求められます。
- ソフトウェアの部品構成表であるSBOM活用の促進や、高度な検証能力を持った国内の検証事業者の育成や信頼の置ける検証事業者の可視化を実施します。

我が国のサイバーセキュリティビジネスのエコシステム構築【委託・補助】

- 日本発のセキュリティ製品・サービスが次々と創出され、ユーザ企業に採用されるエコシステムを確立する必要があります。
- そこで、セキュリティ製品の有効性を検証し、それを市場に発信していく枠組みを運用するとともに、各企業のサイバーセキュリティの担当者同士の交流の機会を創出する「コラボレーション・プラットフォーム」を運用します。

経済産業省

中小企業サイバーセキュリティ対策促進事業

令和４年度概算要求額 3.4億円（２.0億円）

事業の内容

事業目的・概要

- サイバー攻撃が高度化・巧妙化する中、中小企業を含むサプライチェーンリスクが高まり、世界的にサプライチェーンサイバーセキュリティ対策の強化へ向けた取組が進む中で、我が国中小企業のサイバーセキュリティ対策の強化を促進することを目的とします。
- 本事業では、中小企業を含むサプライチェーン全体のサイバーセキュリティ強化のため、主要産業のサプライチェーン上の中小企業に対するサイバー攻撃の実態調査等を実施することにより、必要な対策の検討や中小企業のサイバーセキュリティ対策の普及啓発を行うとともに、中小企業向けセキュリティサービスの普及を図ります。

成果目標

- 平成30年度から令和5年度までの6年間の事業であり、最終的には、令和6年度までに、中小企業のセキュリティ対策機器と事後支援がセットになったサービスの利用者数を３万者以上にすることを目指します。

条件（対象者、対象行為、補助率等）

国 → 補助（定額） → （独）情報処理推進機構

事業イメージ

（１）中小企業サイバー攻撃実態把握調査

- 中小企業を含むサプライチェーン全体のサイバーセキュリティ強化のため、経済安全保障の観点から重要となるサプライチェーン上の中小企業に対するサイバー攻撃の実態調査を行うことにより、攻撃手口を踏まえた必要な対策の検討や、中小企業のサイバーセキュリティ対策の普及啓発を図ります。
- 調査で得られた結果等も踏まえた、中小企業向けのセキュリティ監視・簡易保険サービス（「サイバーセキュリティお助け隊サービス」）の審査登録制度の運用を含め、中小企業向けの安価・効果的なセキュリティサービスの普及を行います。

（２）サプライチェーン全体でのサイバーセキュリティ推進

- 産業界が一丸となった中小企業を含むサプライチェーン全体でのサイバーセキュリティ強化の取組とも連携し、
  - 中小企業のサイバーセキュリティ強化に向けた各支援機関等の連携による普及啓発、
  - 地域企業のセキュリティ意識向上・情報共有を促進するためのコミュニティ形成・活動促進、
  - 産学官連携によるセキュリティ人材の育成・活躍促進、
  - インシデント対応等に関する経営層向けの情報発信等

  を行います。

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4年度予算概算要求額：21．0億円
（令和3年度当初予算：22．0億円）

1　厚生労働省（日本年金機構を含む）における情報セキュリティ対策の推進

20．0億円（20．8億円）

○ 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

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

1．0億円（ 1．0億円）

○ リスクに基づく実践的訓練
・サイバー攻撃を検知した際の国への報告及び事業者内の対応について、リスク分析・評価に基づく実践的な訓練の実施

○ その他重要インフラ防護の取組
・医療分野におけるサイバーセキュリティ対策の実態調査等の実施

産業系サイバーセキュリティ推進事業

経済産業省

令和４年度概算要求額　21.0億円（19.4億円）

事業の内容

事業目的・概要

- 近年、企業や個人の情報を狙ったサイバー攻撃にとどまらず、プラントやインフラそのものの停止を狙い、制御系システムまで含めた社会システム全体を標的とするサイバー攻撃のリスクが高まっており、海外では攻撃事例も出てきています。

  ※制御系システム：工場やプラントの機械や設備などのコントロールを行うために用いられるシステムのこと

- こうした状況の中で安全・安心な社会を築くためには、重要インフラや我が国経済・社会の基盤を支える産業のサイバーセキュリティに関する人材・技術・ノウハウを結集することで、サイバー攻撃への防護力を強化することが不可欠です。
- このため、（独）情報処理推進機構（IPA）に平成29年4月に設立した「産業サイバーセキュリティセンター（Industrial Cyber Security Center of Excellence）」において、模擬プラントを用いた演習等を通じて、官民の共同によりサイバーセキュリティ対策の中核となる人材を育成します。また、サイバーインシデントの観点から、インフラ等における事故の原因究明を行う機能の整備に係る検討を含め、実際の制御系システム等の安全性検証等により、産業分野におけるサイバーセキュリティ対策のノウハウを創出します。

成果目標

- センターのプログラム提供により、100人以上の人材を育成します。良質なプログラムの提供により、これらの受講者による、人材育成プログラムに対する上位の回答割合が80%以上となることを目指します。

条件（対象者、対象行為、補助率等）

国 → 交付金 → （独）情報処理推進機構

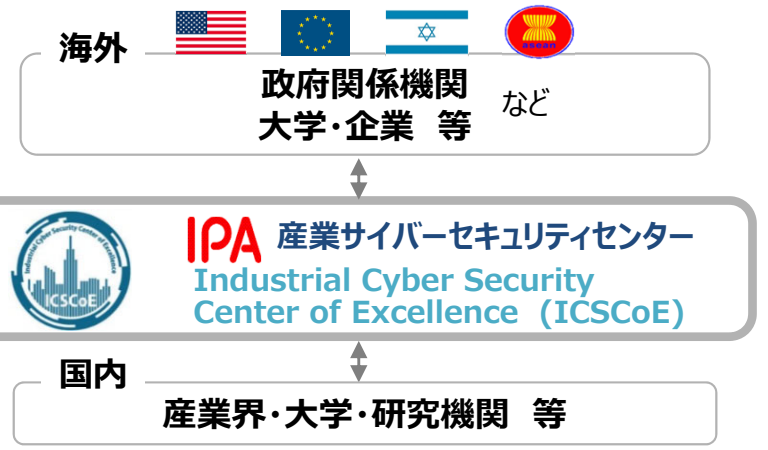
事業イメージ

模擬プラントを用いた演習等を通じた人材育成

- 情報系システムから制御系システムまでを想定した模擬プラントを設置。専門家と共に安全性・信頼性の検証や早期復旧の演習を行う。修了後も中核人材としての活動を支援。
- 最新の攻撃情報の調査・分析結果に応じてプログラムのアップデート等を実施。
- 海外との連携も積極的に実施。

実際のシステムの安全性・信頼性検証等

- 社会インフラ等で活用されている実際の制御システムやIoT機器の安全性・信頼性を検証。
- サイバーインシデントの観点から事故原因の究明を行う機能（いわゆる「サイバー事故調」機能）の整備に向けた検討を実施。
- あらゆる攻撃可能性を検証し、必要な対策立案を行うことで、業界全体で活用可能なサイバーセキュリティ対策のノウハウを創出・蓄積。



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4年度概算要求額　20.5億円（19.3億円）

※うち6.7億円は独立行政法人情報処理推進機構（IPA）運営費交付金要求分

事業の内容

事業目的・概要

- 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、共同対処等を行います。【委託】
- 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)情報処理推進機構(IPA）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ります。【交付金】

※1　Computer Security Incident Response Teamの略。日本の窓口CSIRTは、一般社団法人JPCERTコーディネーションセンター。
※2　Cyber Rescue and Advice Team against target attacked of japan

成果目標

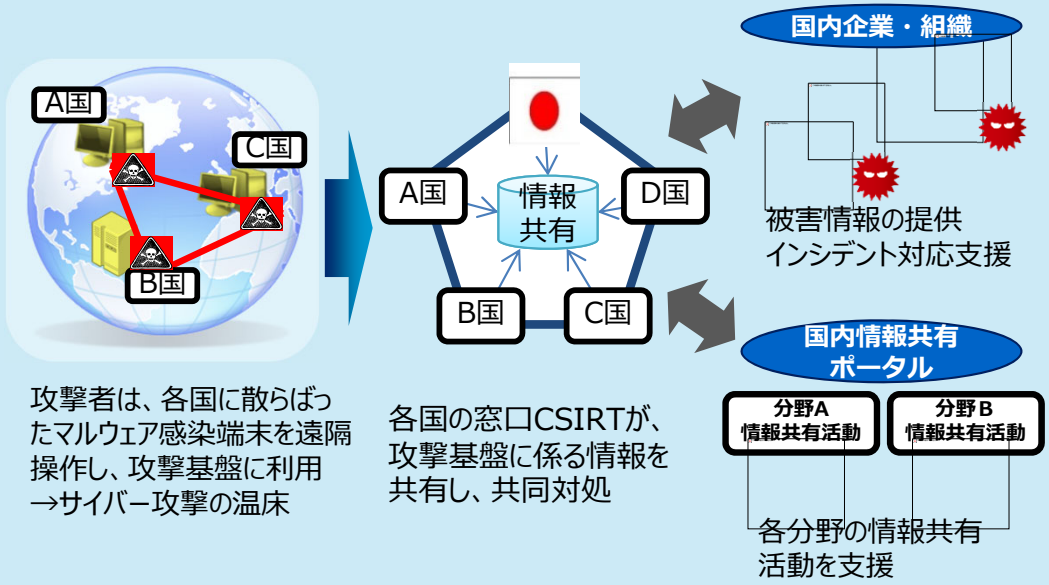
- 本事業の目標は、日々発生し続けるサイバー攻撃から我が国企業等を守る体制を構築し、維持し続けることです。サイバー攻撃の手口は高度化・巧妙化を続けており、政府・公的機関や重要インフラ分野等を狙った攻撃が発生しているところ、インシデントの支援要請や国際連携対応に確実に対応します。こうした対応により、社会に広く影響を与える大規模なサイバー攻撃事態の発生を０件に抑えることを目指します。

条件（対象者、対象行為、補助率等）

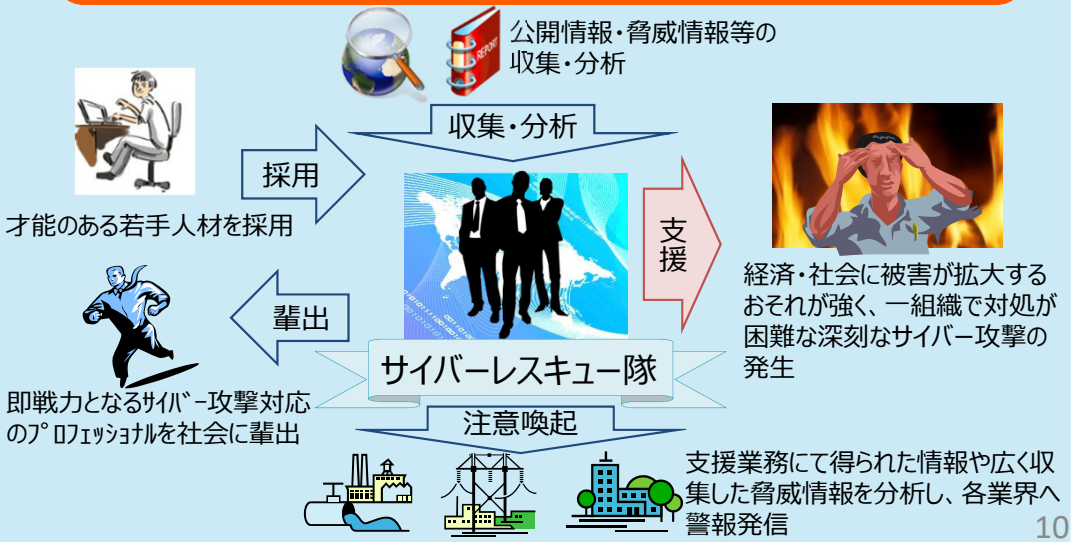
国 → 委託 → 民間専門機関
国 → 交付金 → （独）情報処理推進機構

事業イメージ

各国窓口CSIRT間の連携（情報共有・共同対処）【委託】



サイバーレスキュー隊による支援業務【交付金】



サイバー攻撃インフラ検知等の積極的セキュリティ対策総合実証

総務省

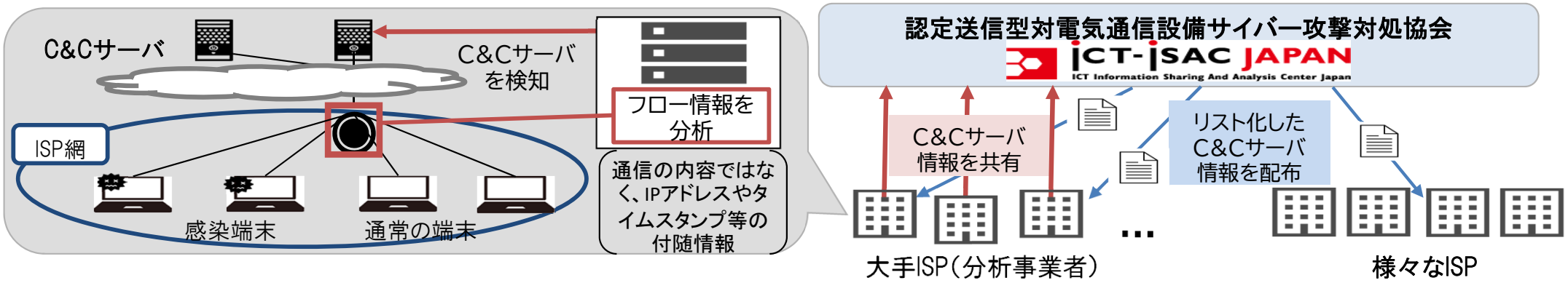
● 大規模化が懸念されるサイバー攻撃に、電気通信事業者側において効率的・積極的に対処できるようにするため、①フロー情報分析によるC&Cサーバ検知技術の実証、②悪性Webサイトの検知技術・共有手法の実証、③ネットワークセキュリティ対策技術の円滑な導入のための実証を実施。

令和4年度要求額 18.0億円（新規）

① フロー情報分析によるC&Cサーバ検知技術の実証

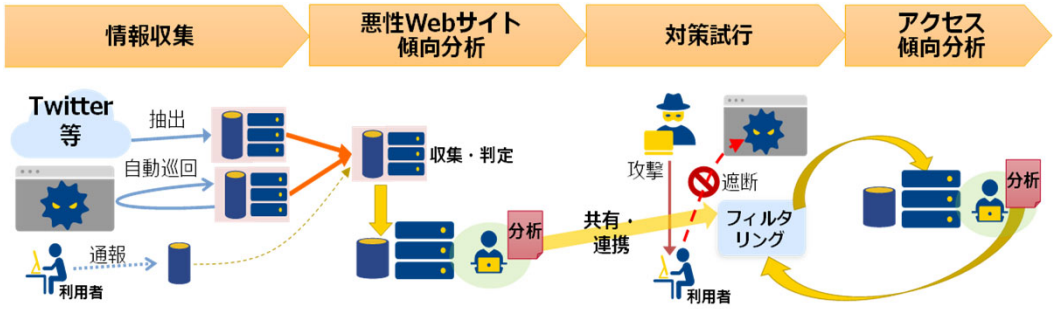
※C&C(Command and Control)サーバ：各感染端末（ボット）にサイバー攻撃の指示を出す管理サーバ

インターネット利用者のトラヒックのうちフロー情報を大規模かつ統計的・相関的に分析し、C&Cサーバを検知する手法の有効性や、C&Cサーバの検知・共有に当たっての技術・運用面の課題を整理。



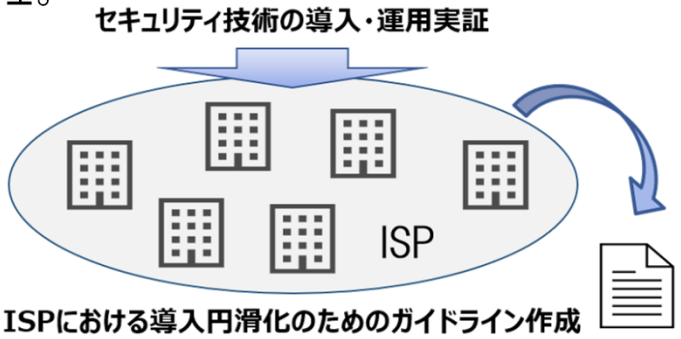
② 悪性Webサイトの検知技術・共有手法の実証

SNSや利用者による通報、自動巡回の仕組みにより収集した、悪性Webサイト（フィッシングサイト等）を分析し、検知する技術の有効性や検知結果の共有手法の課題を整理。



③ ネットワークセキュリティ対策技術の導入実証

ISPにおけるセキュリティ対策を強化するため、ネットワークセキュリティ対策技術の円滑な導入、実装及び運用に係る技術的な諸課題を整理。



警察庁の施策例

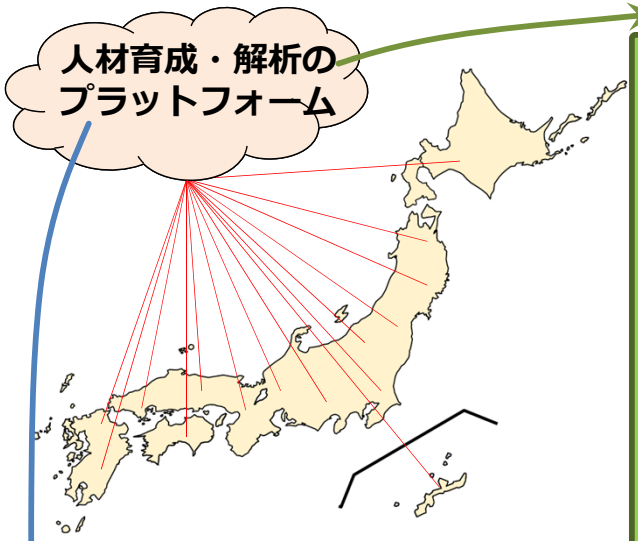
警察庁

サイバー空間の脅威への対処能力の強化

令和４年度概算要求：１４．９億円

概要

職員が実戦的な捜査演習等を遠隔で受講できる人材育成基盤、全国の高度専門人材が協働して解析等を行う解析基盤を整備。



解析基盤機能

遠隔解析

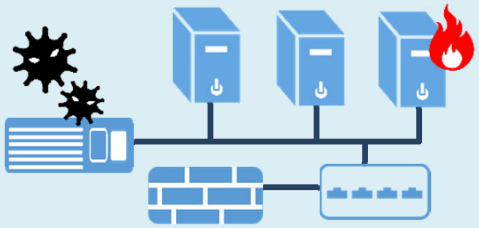
警察庁と地方機関を遠隔接続し、地方機関で対応困難な解析対象物のデータを警察庁において解析

検証部

・大規模産業型制御システムを対象とした不正プログラムの動作や痕跡を検証
・アプリの解析手法の検証・解析ツールの作成　等

人材育成基盤機能

事案対処訓練環境



サイバー犯罪等被害を受けた企業ネットワークを再現

解析訓練環境

遠隔での訓練環境を提供

県情報通信部

技能競技会

競技形式の演習環境を提供

県警察本部

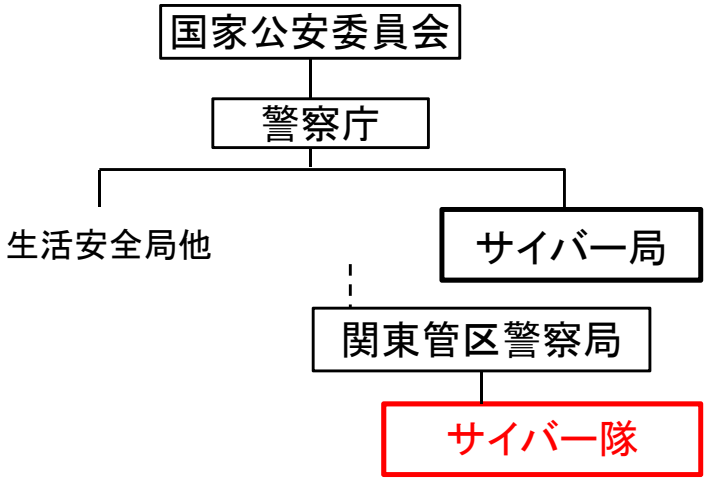
サイバー隊の設置

（※各種維持費を含む）
令和４年度概算要求：７．８億円

概要

国として対応が必要なサイバー事案等への対処のため、全ての都道府県を管轄区域とするサイバー隊を設置。

○　警察庁組織図（改正後イメージ）



サイバー隊の設置、活動等に必要となる主要な経費

○　**捜査・解析用資機材**

各種サイバー捜査や証拠品の解析等を行うために必要となる捜査用資機材、解析用資機材の整備

○　**装備資機材**

車両等のサイバー隊の活動に必要となる装備資機材の整備

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

４年度概算要求額　４．３億円
（３年度予算額　０．５億円）

事業概要・目的

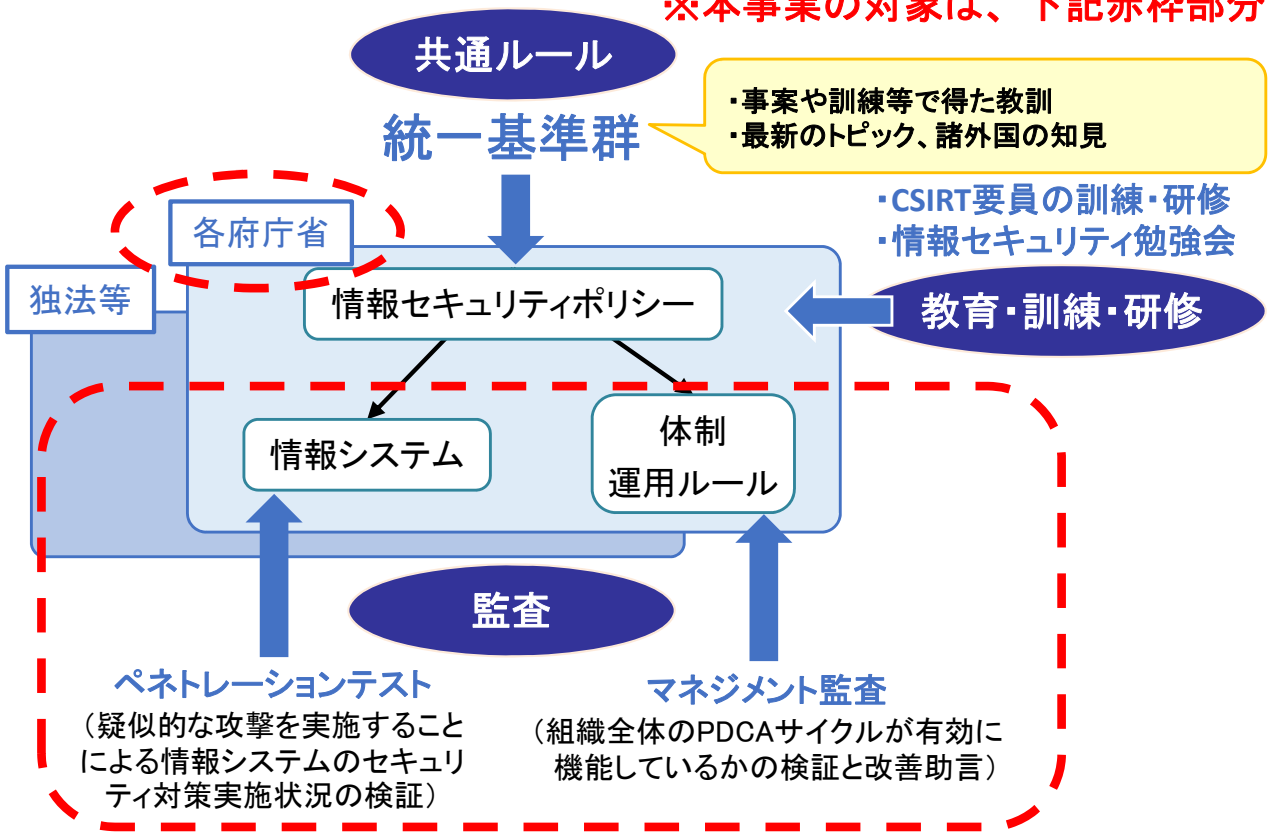
戦略本部がサイバーセキュリティに関する施策を総合的かつ効果的に推進するため、府省庁等のサイバーセキュリティ対策に関する現状を、情報システムに対する「マネジメント監査」と「ペネトレーションテスト（侵入試験）」を行うことにより評価し、NISCからの助言を通して、府省庁等におけるサイバーセキュリティ対策を強化します。

また、これまでの監査を踏まえ、引き続き、中央組織に比べセキュリティ対策水準が低いことが把握されている地方組織が管理する情報システムも含めて監査候補とするとともに、新たに発足するデジタル庁を対象として監査を行うことで、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

※本事業の対象は、下記赤枠部分



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

４年度概算要求額　４．１億円
（３年度予算額　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。

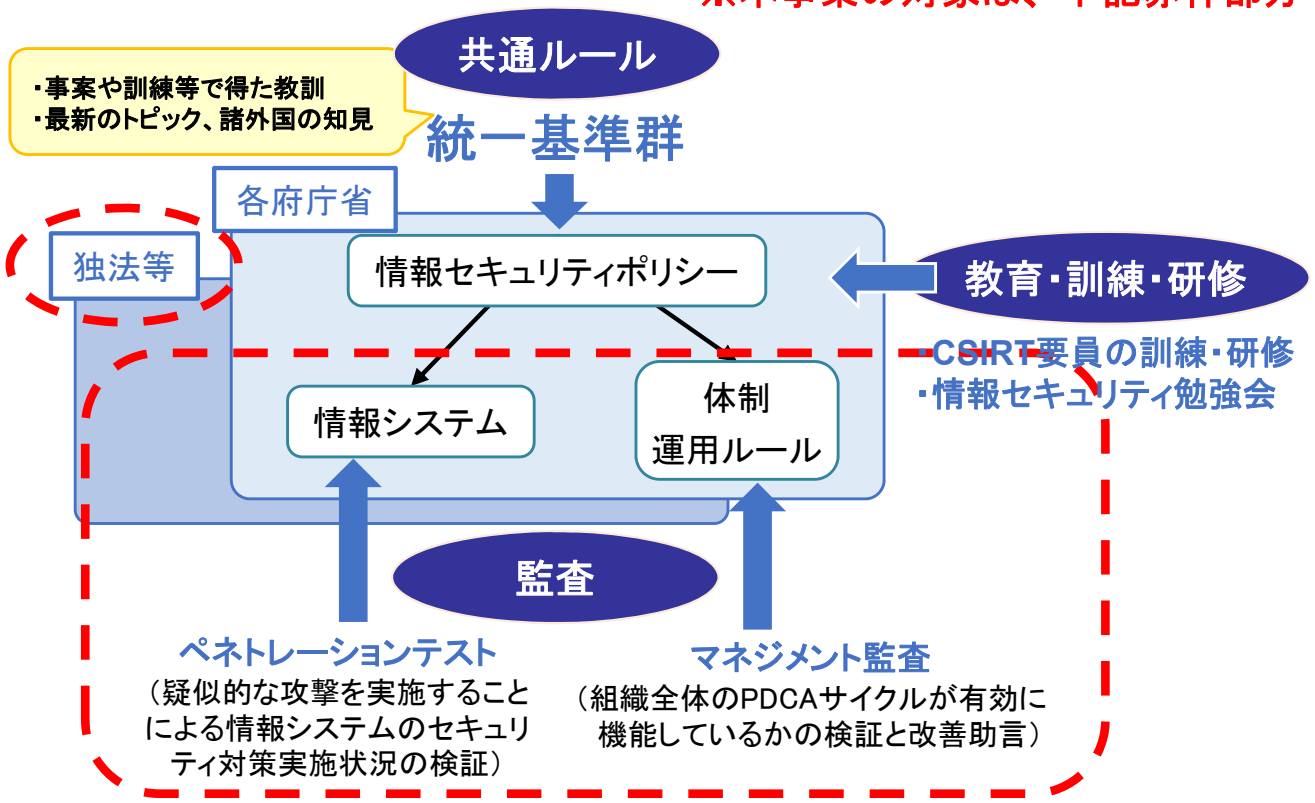
令和４年度においても、各独法等が自律的な情報セキュリティ対策への取組を促進し、情報セキュリティ水準の向上を図ることを目的として監査を実施します。

※（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。

デジタル庁

サイバーセキュリティ確保環境整備費

４年度概算要求額　１．８億円（新規）

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・開発段階を含めてセキュリティの強化を図ることは重要。

○特に、刻々と進化するハッカーの手法に対抗するため、ハッカーの思想を踏まえて攻撃に強いシステムを企画設計するほか（セキュリティ・バイ・デザイン）、運用・保守段階含め検証・監査等を実施しシステムの脆弱性を未然に発見・防止するなど、プロセス全体で対策を確実に実行することが重要。

○デジタル庁のセキュリティ専門チームおよび各システム調達担当が、外部専門機関も活用しながら対策を実施できる環境を整えるため、実務的に準拠可能な技術ガイダンス策定や事業者の信頼性評価調査、セキュリティ研修等を実施する。

事業イメージ・具体例

○監査等業務企画支援委託費

デジタル庁内のシステム開発工程におけるセキュリティ・バイ・デザインの実装および運用工程におけるセキュリティを確保する等のために、各調達担当者が実務的に準拠可能な技術ガイダンス等を企画・策定する。

○セキュリティ・開発ベンダー等の信頼性調査

システム検証等を外部事業者に委託する際に、専門性等の観点から当該事業者の信頼性を評価・可視化し、適切な事業者選定を行えるようにするための調査を実施する。

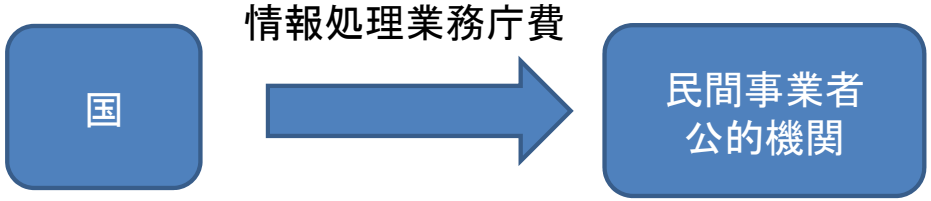
○バックドア等検証

デジタル庁が調達する機器やソフトウエア等のうち主要なものの安全性を確保するため、バックドアが仕掛けられていないかの検証等を実施する。

○システム調達担当者等をターゲットとした研修の実施

デジタル庁内部でシステムの整備・運用に携わる職員がシステム調達時に把握しておくべきセキュリティ要件等のスキル形成等を実施する。

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（企画設計時のセキュリティ・バイ・デザイン、監査・検証）、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対処調整センター及び情報共有システムの運用

４年度概算要求額　１．０億円
（デジタル庁への別途計上額２．６億円）

（３年度予算額　２．９億円）

事業概要・目的・必要性

○　東京2020大会を支える重要サービス事業者等におけるサイバー攻撃対策に万全を期すため、サイバーセキュリティ対処調整センター（以下、「対処調整センター」という。）を設置し、関係する組織間の情報共有と対処調整を行ってきました。

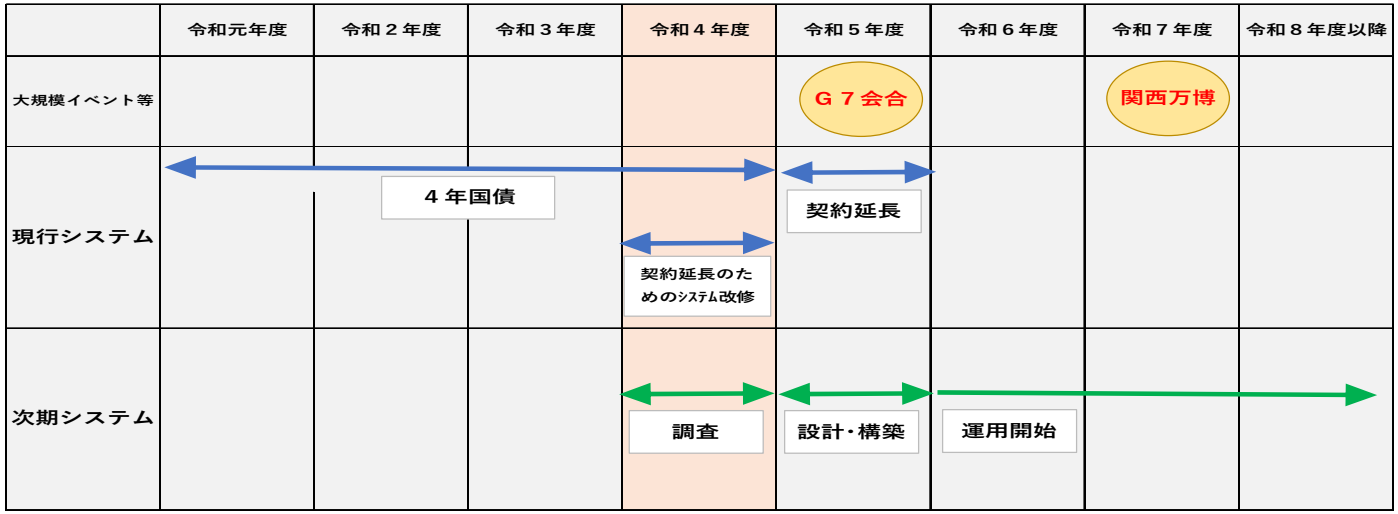
○　東京2020大会後は、サイバーセキュリティに対する脅威が高度化、巧妙化する中、大会で培った経験やノウハウを活用し、対処調整センターを我が国の持続的なサイバーセキュリティ強化に活用する予定です。

○　これに伴い、対処調整センターにおける情報共有、対処調整に欠かせない情報共有システムについても、引き続き活用していく必要があります。

事業イメージ・具体例

現行の情報共有システムの保守・運用等

○現行の情報共有システムのハードウエア・ソフトウエアの保守、クラウドサービス・回線の利用、セキュリティ運用監視、システム運用監視等によるシステムの保守・運用
○対処調整センターの執務室借り上げ等
○現行の情報共有システムの運用期間延長に伴う対応の実施、サポート切れ製品の入替等



期待される効果

東京２０２０大会に引き続き、我が国の持続的なサイバーセキュリティの強化のための活動拠点及び中核システムとして活用することが可能となる。

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インシデントに係る調査

４年度概算要求額　１．０億円
（３年度予算額　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。

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

４年度概算要求額　　０．９億円
（３年度予算額　０．８億円）

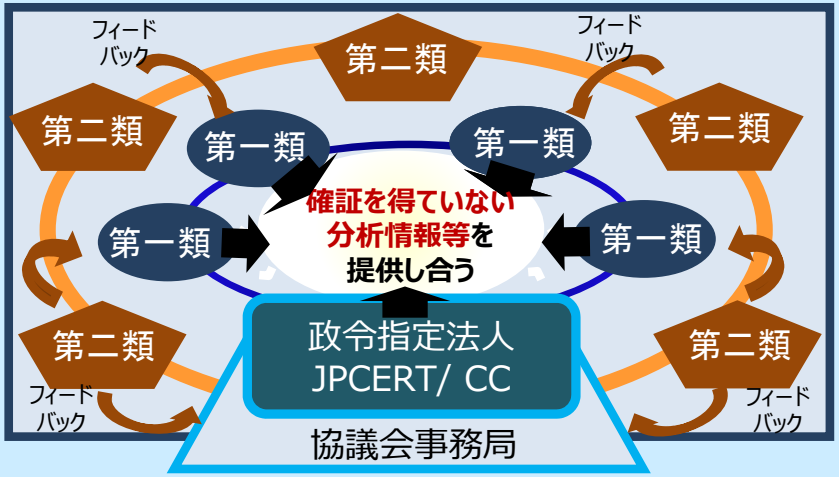
事業概要・目的

○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

タスクフォース（第一類構成員・第二類構成員）

未確定の情報を相互にフィードバックを行い、速やかに対策情報等を作出
※専門機関、セキュリティベンダ、重要社会基盤事業者等



対策情報等の情報提供

一般の構成員

対策情報等を受領し、自らの組織の対策に役立てる。
※国の行政機関、地方公共団体、重要社会基盤事業者等

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。

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４年度予算政府案：0.9億円（令和３年度当初予算：0.８億円）

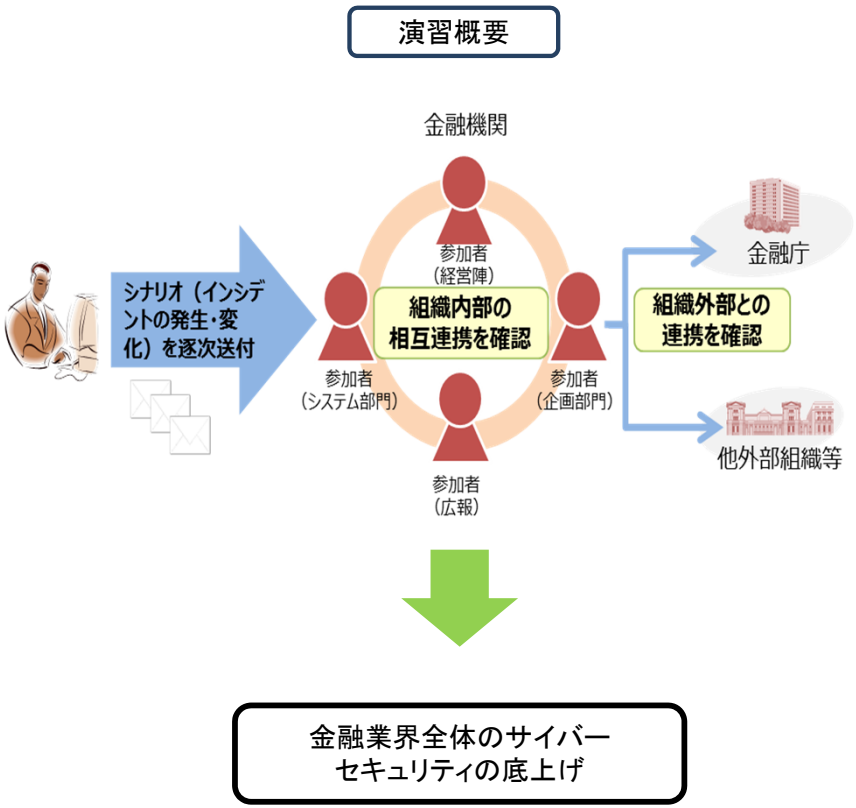
事業概要

- 金融分野におけ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の確保は、金融システム全体の安定のため喫緊の課題。
- 「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」（27年７月公表、30年10月アップデート）に基づき、金融業界全体のインシデント対応能力の更なる向上を図るため、令和３年度、６回目の「金融業界横断的な演習」（Delta Wall Ⅵ）を実施。

  （参考）令和３年度演習は、対象業態を拡充のうえ、約１５０先が参加予定（前回は約114先）。

- サイバー攻撃へ的確に対応するためには、演習を通じて、現在の対応態勢が十分であるかを確認するなど、PDCAサイクルを回しつつ、対応能力を向上させることが有効。
- 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４年度も、引き続き演習を実施予定。

  （注）本演習は、金融庁と参加金融機関の双方で負担



総務省の施策例

地方公共団体の情報セキュリティ対策の推進

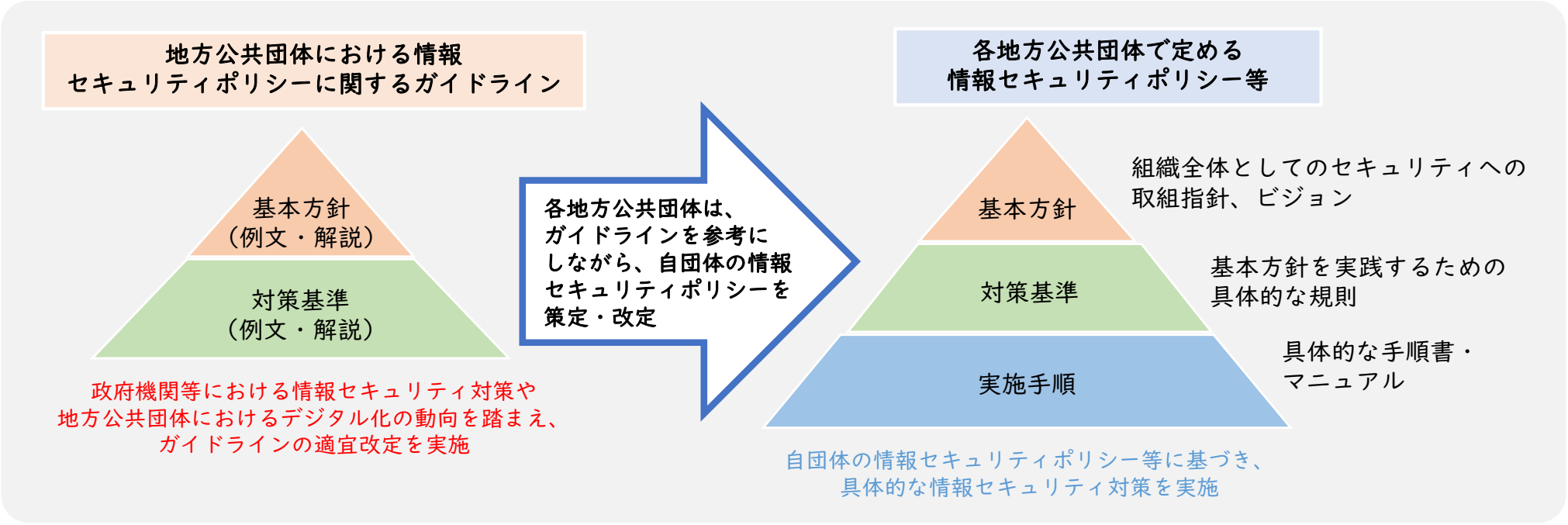
【主な経費】 地方公共団体の情報セキュリティ対策の強化に要する経費　０．８億円〈令和4年度予算政府案〉

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。

令和４年度においても、今後の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・巧妙化を踏まえた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い、引き続き地方公共団体の情報セキュリティ対策を支援する。



防衛省の施策例

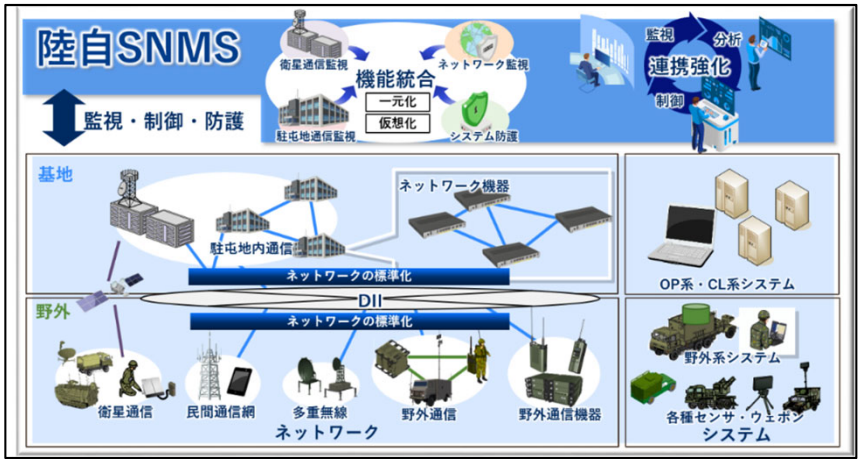
防護システムの整備　令和4年度予算概算要求額：217．8億円（令和3年度当初予算額：202．1億円）

（令和4年度予算概算要求事業の具体例）

◆ 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

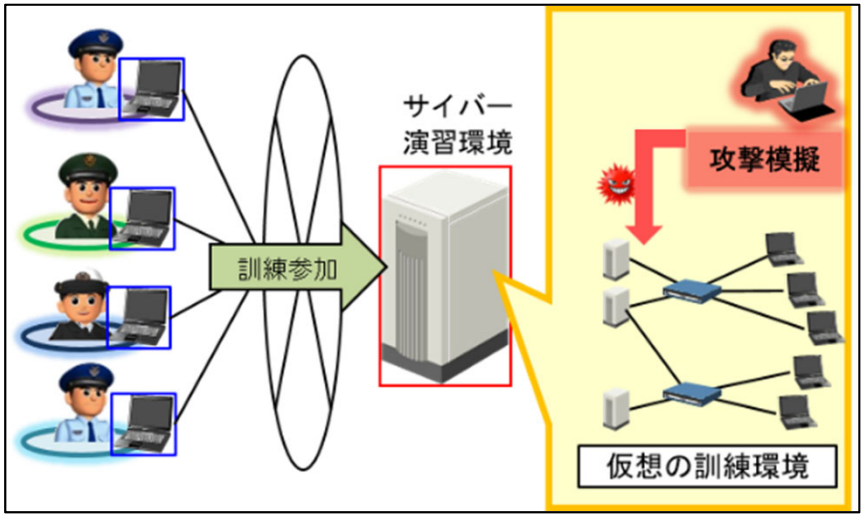
※　SNMS：システム・ネットワークマネージメントシステム



システムネットワーク管理機能の整備（イメージ）

◆ サイバー演習環境の整備

自衛隊の全てのサイバー関連部隊が利用できるサイバー攻撃等への実戦的な訓練を行うための装置を増強



サイバー演習環境の運用（イメージ）

◆ 制御システムのサイバーセキュリティに関する調査・研究

海上自衛隊の艦艇及び航空機で運用する制御システムに対する脆弱性調査手法及びサイバー攻撃への対応策を改善するため、制御システムのサイバーセキュリティに関する調査・研究を実施

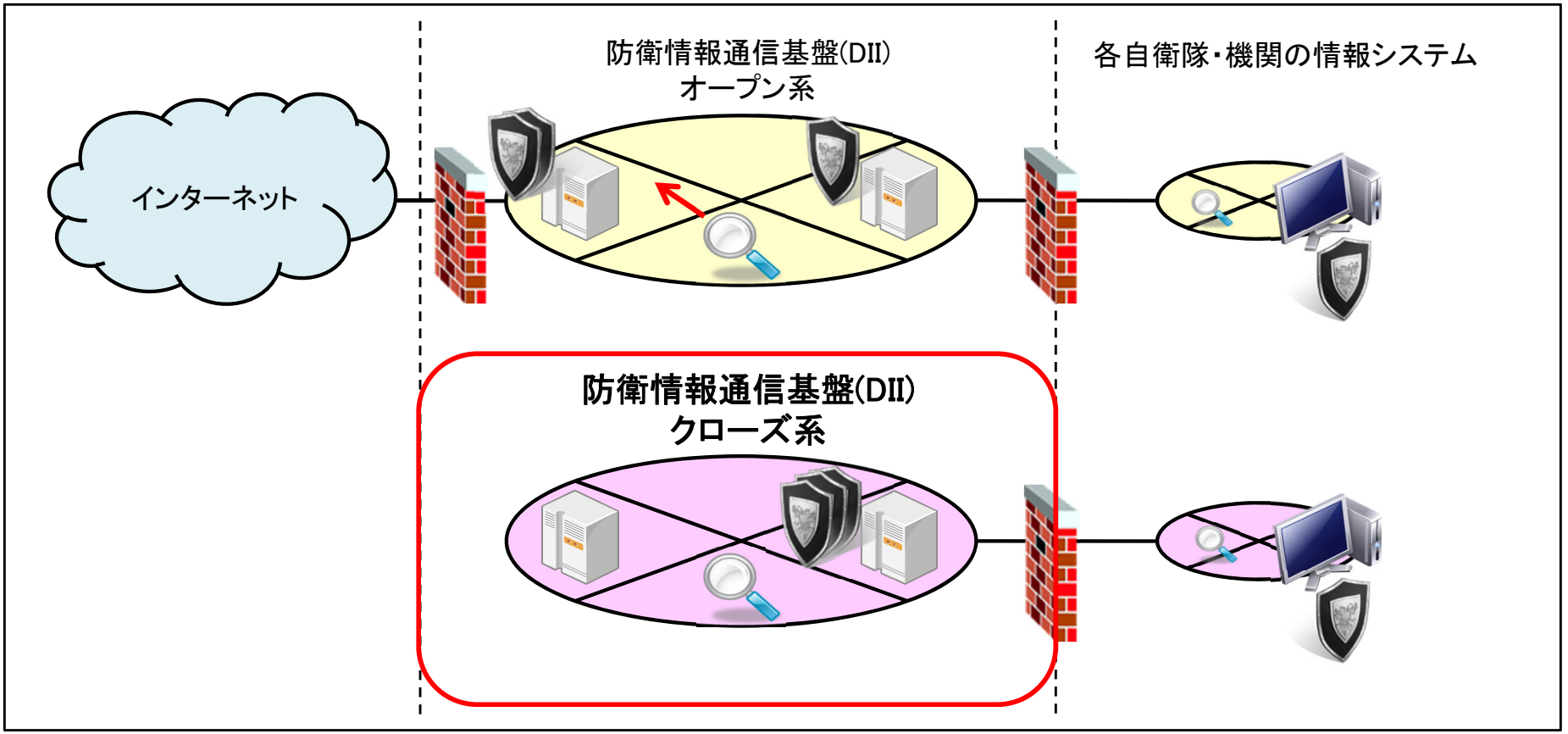
防衛省の施策例

情報通信システムの安全性向上　令和4年度予算概算要求額：82．9億円（令和3年度当初予算額：80．9億円）

（令和4年度予算概算要求事業の具体例）

◆ 防衛情報通信基盤（DII）の整備（クローズ系）

防衛省・自衛隊の共通通信インフラである防衛情報通信基盤（DII）における防護機能を強化



防衛情報通信基盤（DII）の整備（イメージ）

防衛省の施策例

サイバーに関する最新技術の活用　令和4年度予算概算要求額：25．3億円（令和3年度当初予算額：10．9億円）

（令和4年度予算概算要求事業の具体例）

◆ サイバー攻撃へ対処する技術の研究

装備品等に対するサイバー攻撃発生時における被害拡大防止やシステムの運用継続を図るため、対処能力向上に資する技術の研究を実施

サイバー攻撃へ対処する技術の研究（イメージ）

外務省

外務省の施策例

外務省サイバーセキュリティ施策

令和３年度当初予算額　　：４．５億円
令和４年度予算概算要求額：８．３億円

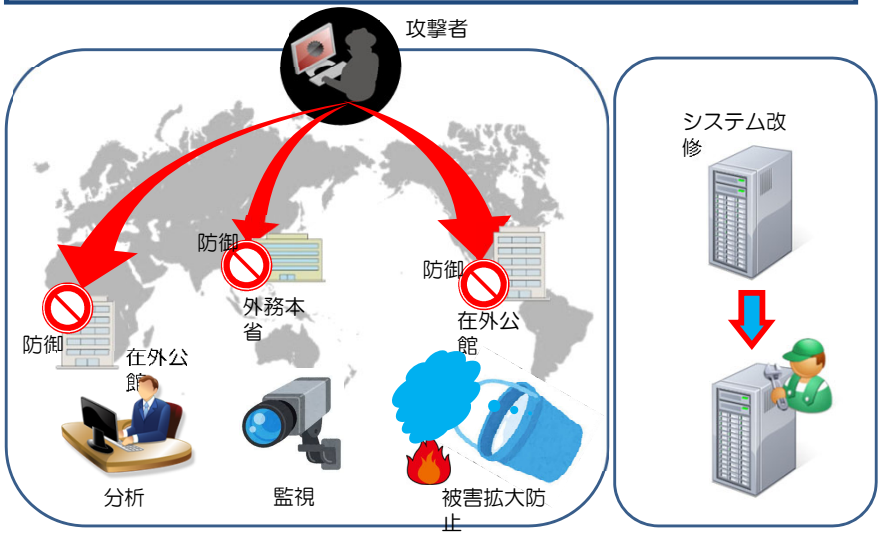
情報セキュリティ対策の強化

令和４年度予算概算要求額：７．７億円

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。
・サーバ、ネットワーク機器入替等に伴う一部システムの改修。



サイバー空間に関する外交及び国際連携

令和４年度予算概算要求額：０．６億円

事業目的･概要

○目的
　近年増大するサイバー空間における脅威及びサイバー問題の重要性を背景に、国際的なルール作り、安全保障面での課題の検討、各国との連携、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係者会議／関連会議
　･サイバー犯罪条約締約国会議／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

ナショナルサイバートレーニングセンターの強化

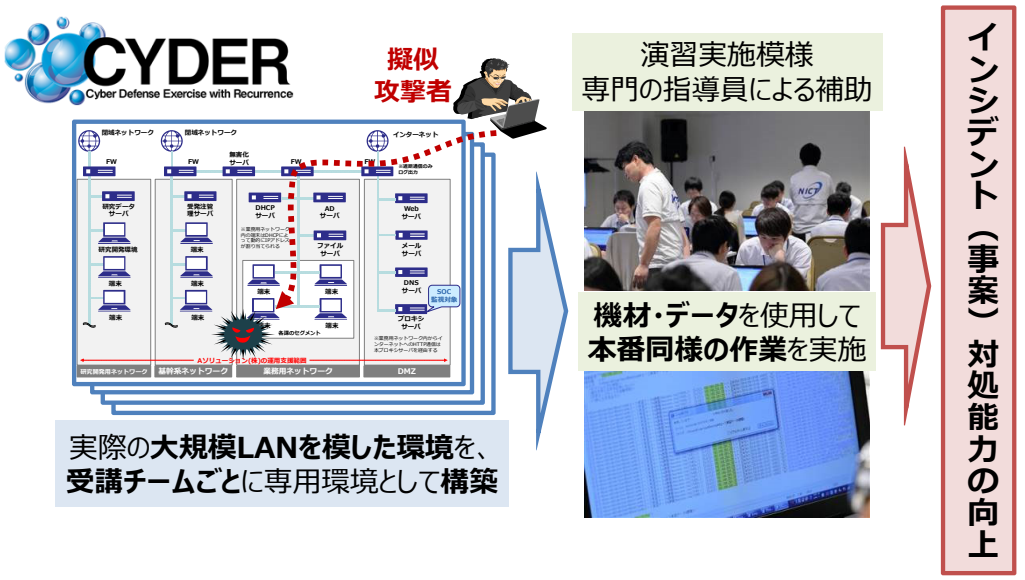
総務省

● 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する。 **令和4年度要求額 14.0億円（令和3年度予算額 12.0億円）**

①CYDER（実践的サイバー防御演習）

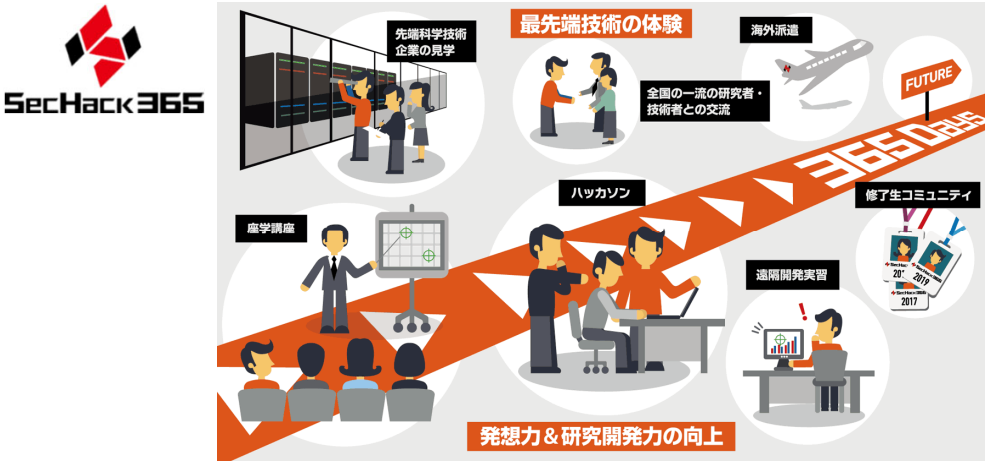
国の行政機関、地方公共団体、独立行政法人及び重要インフラ事業者等の情報システム担当者等を対象とした実践的サイバー防御演習（CYDER）を実施。

※オンライン受講環境を令和３年度より本格稼働。



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うる最先端のセキュリティ人材を育成。



IoTの安心・安全かつ適正な利用環境の構築

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。

令和4年度要求額 11.5億円（令和3年度予算額 12.8億円の内数）

① IoTセキュリティ対策の推進

国立研究開発法人情報通信研究機構法に基づき国内のインターネットに接続されたIoT機器のうちサイバー攻撃に悪用されうる脆弱なIoT機器を調査し、当該機器の利用者に個別に注意喚起を行うプロジェクト「NOTICE」を実施する。

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ネットワークやその構成要素及びサービスについて、ソフトウェア及びハードウェア両面の技術的検証を通じ、各構成要素におけるサプライチェーンリスク対策を含むセキュリティを総合的かつ継続的に担保する仕組みを整備する。

※ ソフトウェアに関する技術的検証については、令和３年度で終了。

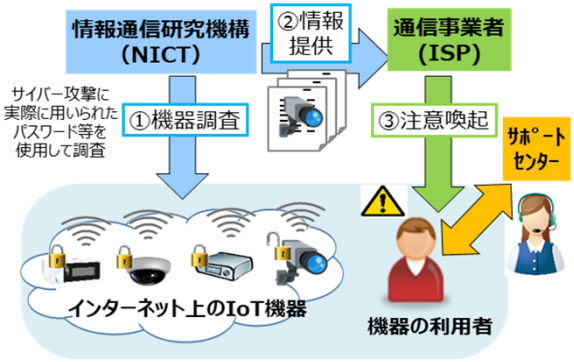
③ 地域におけるIoTセキュリティ対策の強化

地域のコミュニティや企業、教育機関等と連携して、IoTセキュリティに関して活躍可能な人材を自立的に育成していくためのエコシステムの確立に向けた実証を行う。

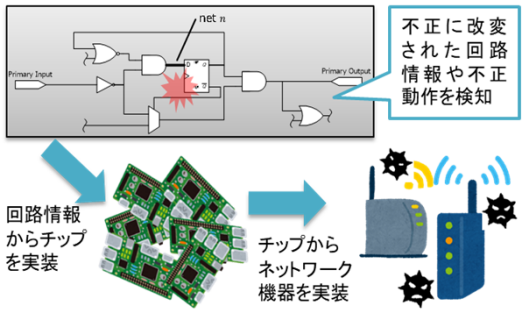
④ 無線LANのセキュリティ対策の強化

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。

①IoTセキュリティ対策の推進



②5G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



防衛省の施策例

防衛省

サイバー人材の確保・育成　令和4年度予算概算要求額：９．５億円（令和3年度当初予算額：６．１億円）

（令和4年度予算概算要求事業の具体例）

◆ サイバー人材共通のスキル評価指標作成のための調査・研究

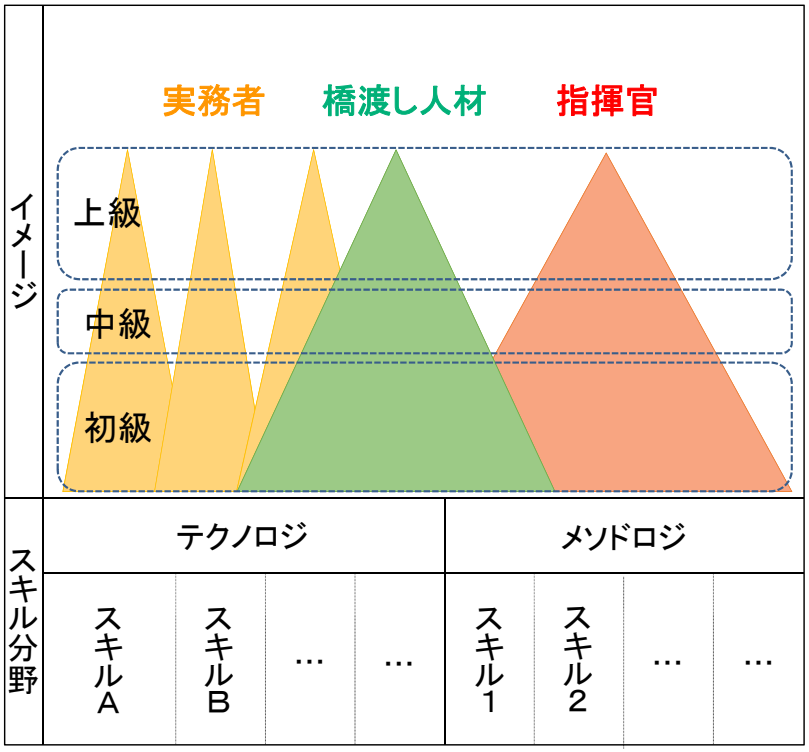
防衛省・自衛隊において、効果的・効率的にサイバー人材の確保・育成を行うためのスキル評価指標を確立するため、民間や諸外国におけるサイバー人材のスキル評価手法について調査・研究を実施

◆ サイバーセキュリティ統括アドバイザーの採用

部内教育では育成困難な高度サイバー人材を非常勤の国家公務員として雇用し、サイバー分野の能力を強化

◆ サイバー分野における部外力の活用に関する調査・研究

部外人材の安定的かつ効果的な活用のための新たな制度設計の資とするため、諸外国の軍及び防衛当局でのサイバー分野における予備役や非常勤職員等の部外力活用の実態について調査・研究を実施



サイバー人材共通のスキル評価指標（イメージ）

GIGAスクールにおける学びの充実

令和4年度要求・要望額　5億円
（前年度予算額　4億円）

文部科学省

事業内容

1人1台端末環境の本格運用を踏まえ、その効果的な活用を通じた児童生徒の学びの充実に向けて、**自治体への指導支援、教師の指導力向上支援の更なる強化**を図るとともに、**児童・生徒の情報モラルを含めた情報活用能力の育成及びその把握を踏まえた指導内容の改善**等を一体的に行う。

①　アドバイザー等による自治体支援事業

・文部科学省が委嘱した教育課程の専門家とGIGA StuDX推進チームが連携した指導内容の助言・支援 **<新規>**
・ICT活用指導力向上やICTを効果的に活用した指導の実施に関する助言・支援
・学校の持続可能なICT環境に関する助言・支援

委託先	民間企業等	委託対象経費	人件費・諸謝金等必要な経費

②　ICTを活用した指導力向上支援事業 <新規>

・各教科等・各OSごとに1人1台端末の効果的な活用方法をまとめた動画を作成・提供
・新学習指導要領に基づく高等学校の教科「情報」の効果的な実施に向けた全国での実践、ノウハウの普及・展開

委託先	自治体、民間企業等	委託対象経費	人件費・諸謝金等必要な経費

③　情報モラル教育推進事業

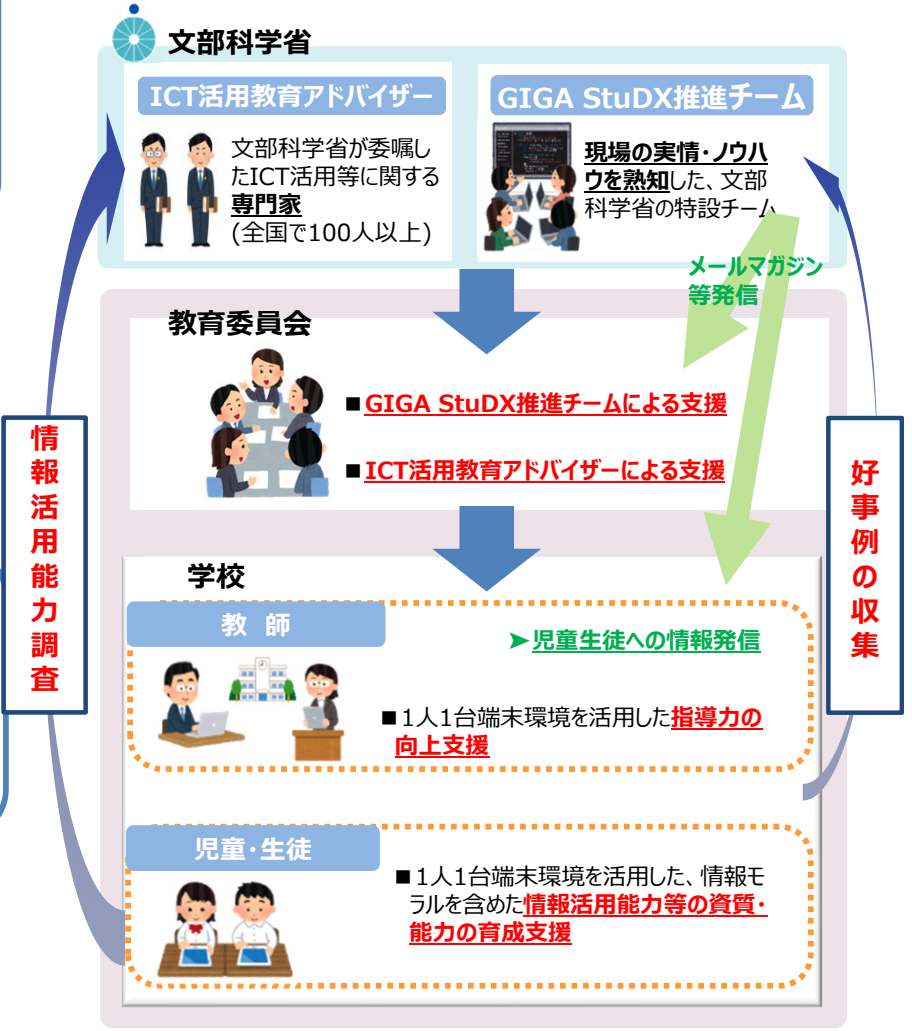
・１人１台端末環境下における情報モラル教育の推進
・情報モラル教育の推進に係るコンテンツの充実　・情報モラル教育指導者セミナーの実施
・都道府県と市区町村が連携したモデル事業の実施による好事例の発信や授業公開の実施**<新規>**
・児童生徒に対する啓発資料等による情報発信

委託先	自治体、民間企業等	委託対象経費	人件費・諸謝金等必要な経費

④　児童生徒の情報活用能力の把握に関する調査研究

・R3年度に実施した本調査の結果分析
・調査結果の分析を踏まえた、情報活用能力育成のための指導内容の整理・周知

委託先	民間企業等	委託対象経費	人件費・諸謝金等必要な経費



文部科学省

サイバーセキュリティ人材育成の高度化

令和4年度概算要求額　3.3億円
(前年度予算額　3.7億円)

背景

○Society5.0時代を迎えるに当たって、**特にDX時代に必要なリアルとサイバーの両方の空間を意識した教育の強化を図りつつ**、AIやIoTを使いこなせる**先端IT人材の育成が急務**となっている。また、あらゆるものがインターネットに接続され、ITを活用したサービスが拡大する中、**あらかじめセキュリティを考慮したセキュリティ・バイ・デザインができる人材**の育成が必要である。
○これらを実現するため、**成長戦略**に記されている産学官協働による需要（企業等）と供給（教育機関）の好循環にむけて**2020年度にサプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）**が発足され、そこでの**産学官連携人材育成WGにおいて高専への期待が高い。**
○**内閣サイバーセキュリティセンター（NISC）の報告書等において、若年層向けのサイバーセキュリティ教育において高専への期待が高い。**

これまで

＜第１フェーズ＞
○2016度に整備した**先行５拠点**（一関、木更津、石川、高知、佐世保）において、「情報セキュリティ人材」の育成に必要な**教育を実践・検証**

＜第２フェーズ＞
○**後発５拠点**（旭川、小山、岐阜、松江、熊本）の**環境整備を実施**し、**全国10ヶ所で「サイバーセキュリティ人材」の発掘・育成を実施**。
○サイバーセキュリティに係る教育プログラムや、専門学科毎のケーススタディを学ぶ**分野別教材を開発**

＜第3フェーズ＞
○**サイバーセキュリティ教育の徹底**
○IPA等の**外部機関との連携により**、セキュリティ教育を実践できる**教員の高度化を図り、サイバーセキュリティ教育の高度化**。
○日々進化するサイバーセキュリティ技術の高度化に対応するため、**演習拠点環境を更新**

＜成果＞
○サイバーセキュリティ教育の実践と教材開発（モデルコアカリキュラム（MCC）への導入）
○10拠点の演習拠点整備
○高専教員のサイバーセキュリティ教育の高度化

事業内容

＜第４フェーズ＞
継続可能で高度化に繋げる2つの柱を実施

＜柱１＞サイバーセキュリティ人材育成のエコシステム構築のために、**高専と産業界（大企業・団体等）との強固な連携したKOSENサイバーセキュリティセンター（K-CSC）機能**を構築する。

（主な実施事項）
- サイバーセキュリティ教育の情報集約・発信（柱２のハブ機能含む）
- 教材・環境UPDATE、高度教員育成
- セキュリティの教育プログラム認定等の検討等

＜柱２＞地域中小企業との連携および貢献のために、**地域のサイバーセキュリティコミュニティ等と高専の連携**を進める。

（主な実施事項）
- サイバーセキュリティに特化した地域連携の機能整備
- 地域中小企業との連携
- 地域の中小企業におけるサイバーセキュリティの理解・対策等の支援（社会実装教育としての高専生の教育およびキャリア教育も含む）

目標とする姿

＜高専生の輩出（継続）＞
✓**サイバーセキュリティのトップ人材育成**
✓各専門分野において「守るべきものは何か？」を知った**セキュリティスキルを持った高専生の育成（プラス・セキュリティ人材の輩出）**

＜高度化（特に注力する事項）＞
✓**KOSENサイバーセキュリティセンター機能**
✓**サイバーセキュリティを軸とした地域連携**

サイバーセキュリティ人材育成の高度化
サイバーセキュリティを軸とした高専×産業界×地域
⇒継続的なサイバーセキュリティ人財教育、地域のサイバーセキュリティレベル向上、地域へ高専生を輩出