# 政府のサイバーセキュリティに関する予算

資料３

## 令和５年度予算政府案

**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要事業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５年度予算政府案 |
|---|---|
| (1)経済社会の活力の向上及び持続的発展 | （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 | 23.5 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 | 8.5 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 | 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 | （264.7 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 | 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 | 19.6 億円 |
| 【外務省】情報セキュリティ対策の強化 | 6.6 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 | 0.5 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 | 0.3 億円 |
| 【警察庁】違法・有害情報対策に伴う経費 | 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 |
| 【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 | 0.8 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 |
| 【内閣官房】サイバーセキュリティ協議会の運用 | 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 | 0.7 億円 |

# 政府のサイバーセキュリティに関する予算

## 令和５年度予算政府案

**１，３７８．９億円**

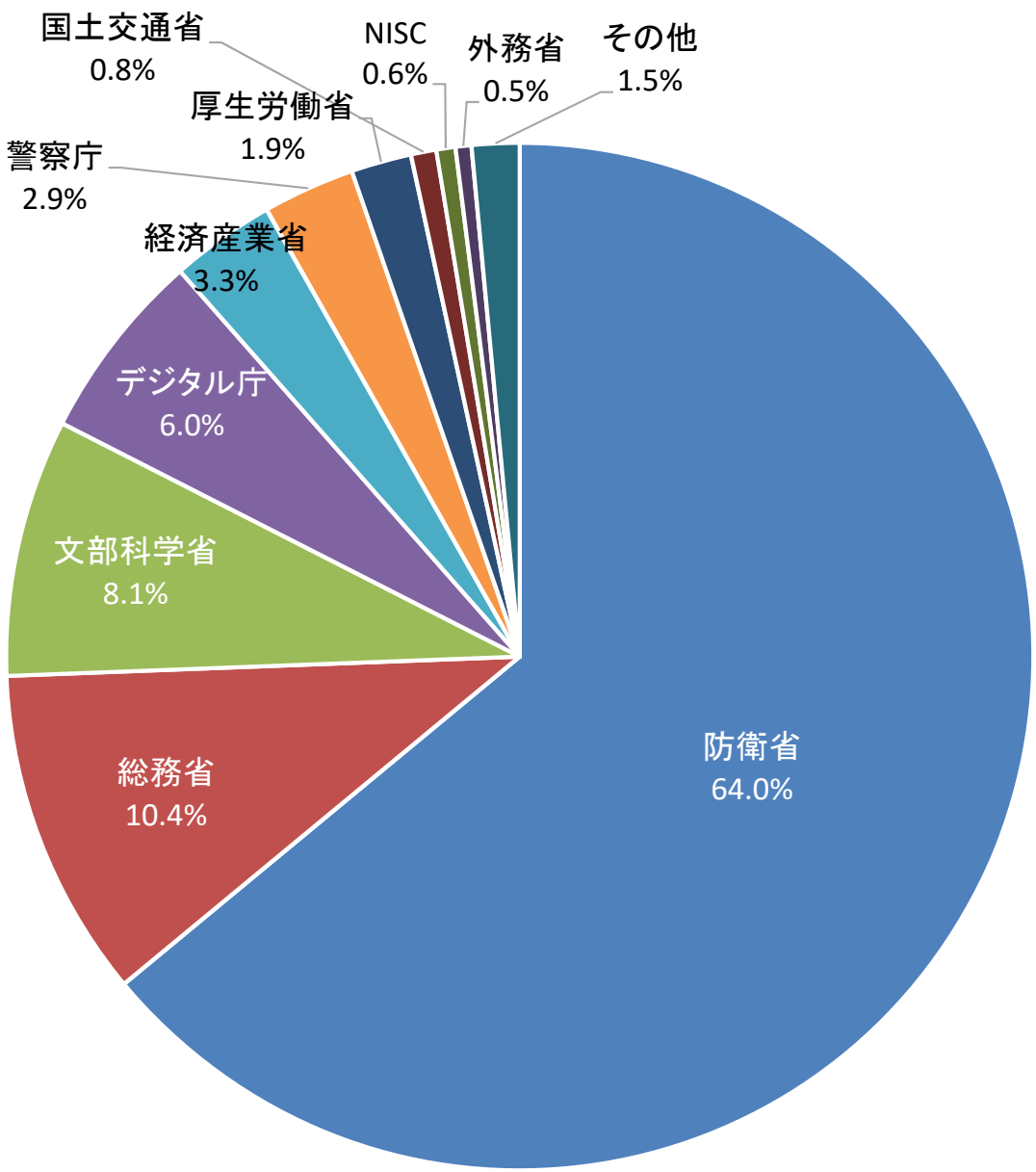
注１）サイバーセキュリティに関する予算として切り分けられない場合には計上していない。
注２）（　）内の数字は記載の主要事業以外も含めたそれぞれの項目の総計

| 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５年度予算政府案 |
|---|---|
| (3)国際社会の平和・安定及び我が国の安全保障への寄与 | （ 878.0 億円） |
| 【防衛省】情報システムの防護 | 477.4 億円 |
| 【防衛省】リスク管理枠組み（RMF）の導入 | 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 | 68.5 億円 |
| 【防衛省】サイバー分野における研究機能の強化 | 14.6 億円 |
| 【警察庁】サイバーテロ対策用資機材の増強等 | 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 | 0.6 億円 |
| (4)横断的施策（人材育成等） | （150.3 億円） |
| 【防衛省】サイバー分野における教育機能の強化 | 20.1 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 | 12.7 億円 |
| 【総務省】 IoTの安心・安全かつ適正な利用環境の構築 | 12.0 億円 |
| 【文部科学省】GIGAスクールにおける学びの充実 | 2.8 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 | 0.2 億円 |
| 【国土交通省】情報システムセキュリティ強化経費 | 0.6 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５年度予算政府案**

**１，３７８．９億円**




※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。

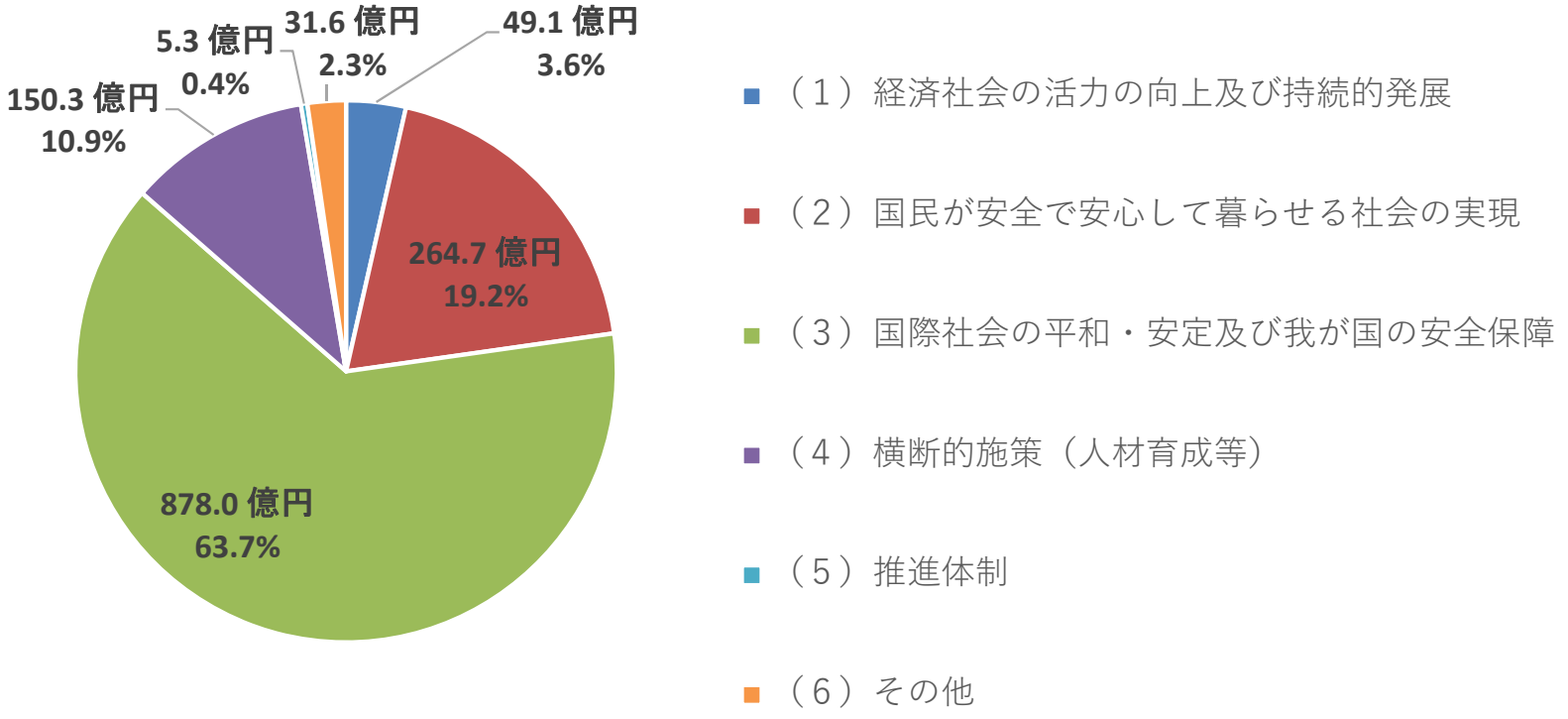
# サイバーセキュリティ戦略　分野別内訳

## 令和５年度予算政府案

**１，３７８．９億円**

○　令和５年度予算政府案におけるサイバーセキュリティ関連予算は、1,378.9億円となっている。

○　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」が約６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

# 産業サイバーセキュリティ強靭化事業

商務情報政策局
サイバーセキュリティ課

**令和５年度予算案額　23.5　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ます。本事業では、ガイドライン等の策定や、ソフトウェア管理の高度化、IoT製品の信頼性確保を進めるとともに、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靭化を目指します。

### 事業概要

産業界のサイバーセキュリティ強靭化に向けて、以下の取組を行います。
（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）
・ガイドライン等の策定や国際連携・活用促進
・ソフトウェアの部品構成表であるSBOMの活用を通じたソフトウエア管理の高度化
・IoT製品の信頼性を確保するための環境整備
（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
・制御システムの事故原因の究明を行うための体制整備

## 事業スキーム（対象者、対象行為、補助率等）


## 成果目標

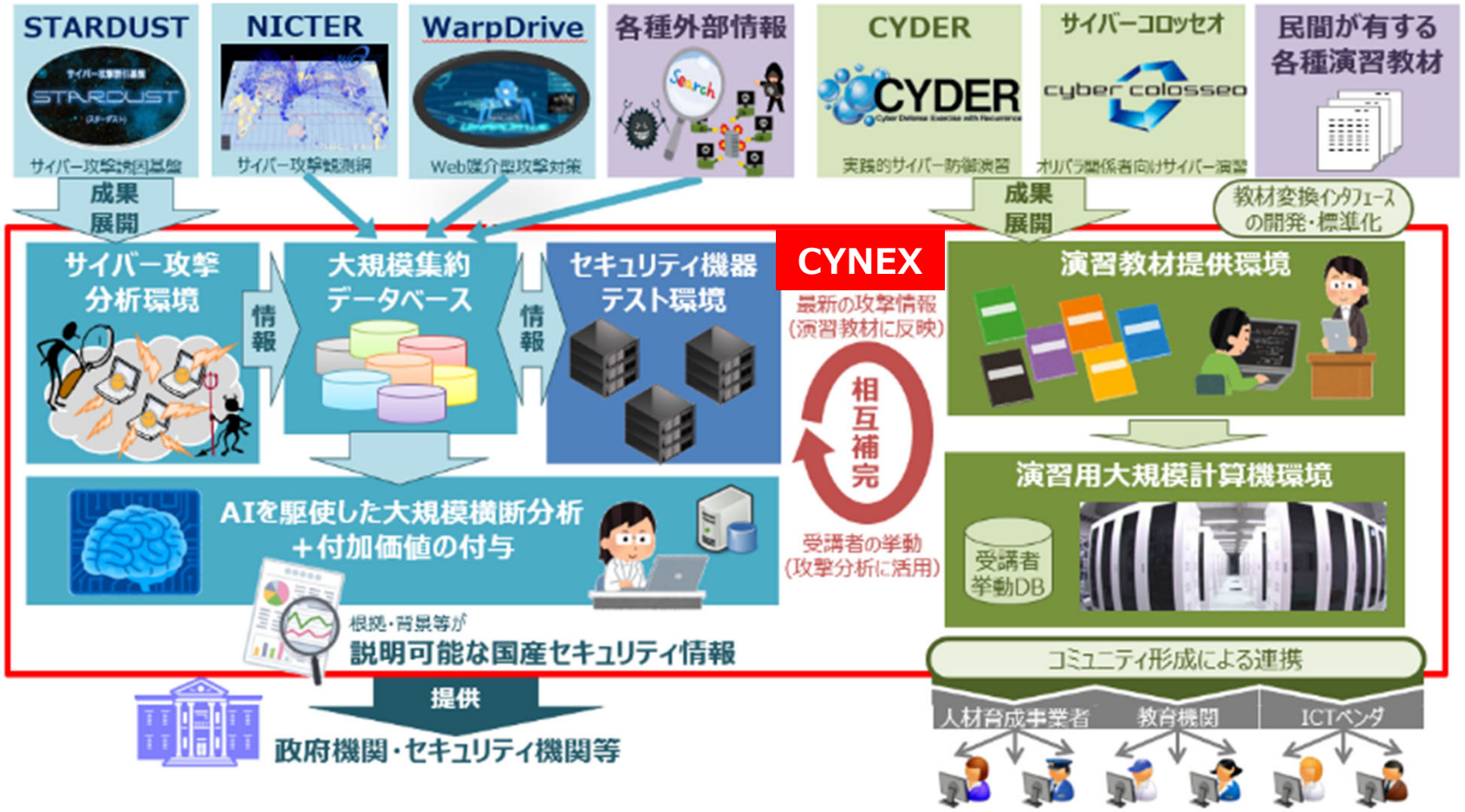
産業界で策定されたガイドラインの数を15個以上にすることや人材育成を通じて、産業界のセキュリティ対策を推進します。

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。

**令和5年度予算政府案 8.5億円**




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。

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

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

**令和５年度予算案額　　2.0　億円**

## 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ます。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、サイバーセキュリティお助け隊サービス等のセキュリティ対策の普及を行うとともに、経営層も含めた中小企業の人材の「プラス・セキュリティ」（※）を推進し、我が国の中小企業のサイバーセキュリティ対策の強化を目指します。

（※）自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につけること

**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(IPA)において、以下の取組を行います。（補助）

・産業界の取組と連携し、産学官連携による人材育成等を進めます。
・経営層も含めた中小企業の人材の「プラス・セキュリティ」を推進するため、サイバー脅威の机上演習（経営者向け）や自社の情報資産のリスク分析（担当者向け）を専門家が伴走して行います。
・中小企業にとって身近な支援機関とも連携し、セキュリティ対策の重要性を喚起します。
・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（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行います。

## 事業スキーム（対象者、対象行為、補助率等）

国 → 補助（定額） → 独立行政法人情報処理推進機構(IPA)

## 成果目標

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6.8万者以上にすることを目指します。

# 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5年度予算政府案：27．1億円

## 1　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の推進　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

## 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　1．4億円

○ 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

経済産業省

商務情報政策局
サイバーセキュリティ課

# サイバーセキュリティ経済基盤構築事業

**令和５年度予算案額　19.6　億円**

## 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指します。

### 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、共同対処等を行います。（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(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。
※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

迅速な初動対応や適切な情報共有・注意喚起により、サイバー攻撃が社会に広く影響を与える大規模なサイバー攻撃事態へ発展するケースを０件に抑えることを目指します。

# 外務省の施策例



## 外務省サイバーセキュリティ施策

令和５年度予算政府案額　：７．２億円

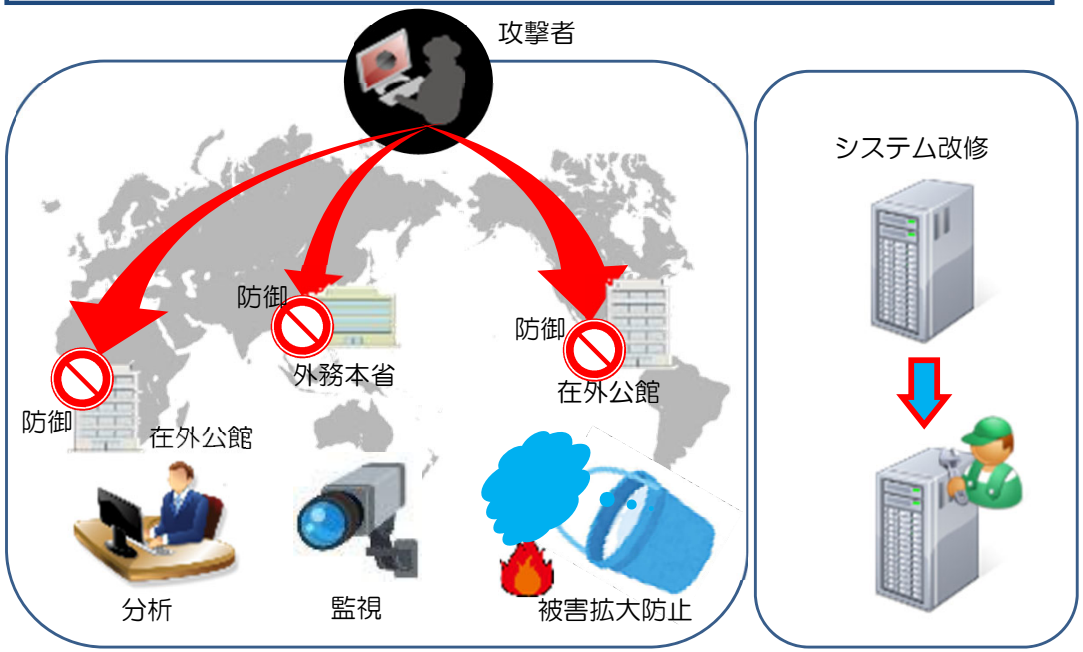
### 情報セキュリティ対策の強化

令和５年度予算政府案額：６．６億円

**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。



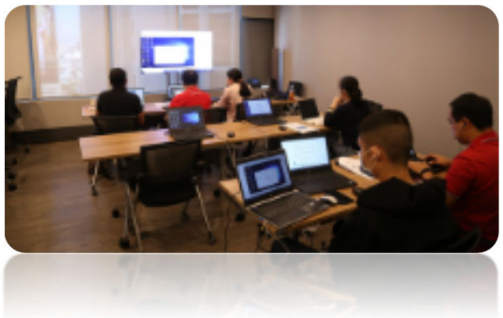

### サイバー空間に関する外交及び国際連携

令和５年度予算政府案額：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
　･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）

# 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５年度予算政府案額　０．５億円

## 事業概要・目的

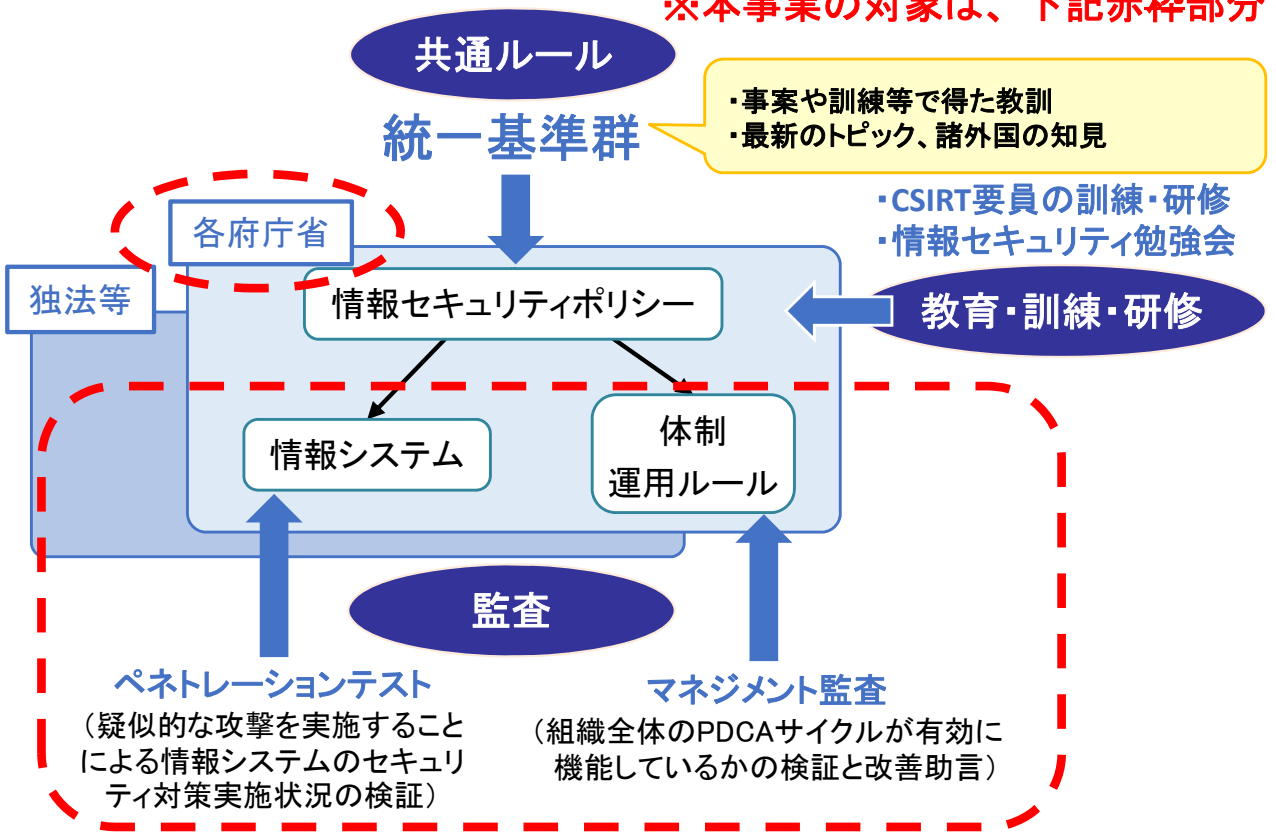
戦略本部がサイバーセキュリティに関する施策を総合的かつ効果的に推進するため、府省庁等のサイバーセキュリティ対策に関する現状を、情報システムに対する「マネジメント監査」と「ペネトレーションテスト（侵入試験）」を行うことにより評価し、NISCからの助言を通して、府省庁等におけるサイバーセキュリティ対策を強化します。

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

※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

令和５年度予算政府案額　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。

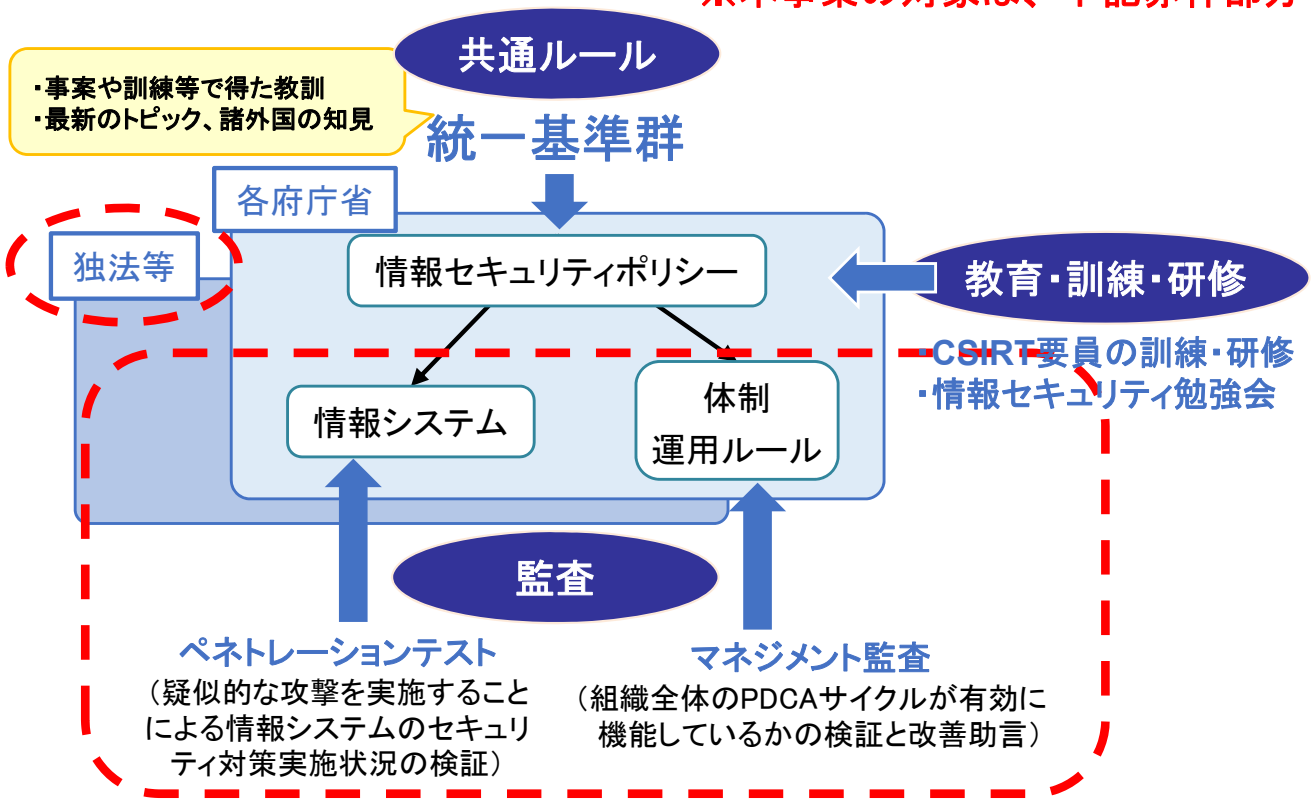
令和５年度においても、各独法等が自律的な情報セキュリティ対策への取組を促進し、情報セキュリティ水準の向上を図ることを目的として監査を実施します。

※（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。

# 違法・有害情報対策に伴う経費

警察庁

**概要**

インターネット・ホットライン事業やサイバーパトロール事業の対象に爆発物・銃砲等の製造、殺人や強盗等の請負・誘引等に関する情報等追加するため、インターネット・ホットラインセンター及びサイバーパトロールセンターの運用体制を強化するとともに、違法・有害情報の把握の高度化を図るため、サイバーパトロール事業におけるＡＩを活用した検索システムの導入等を行う。

令和５年度政府予算案：約２．０億円

## ① ホットライン業務の外部委託に要する経費

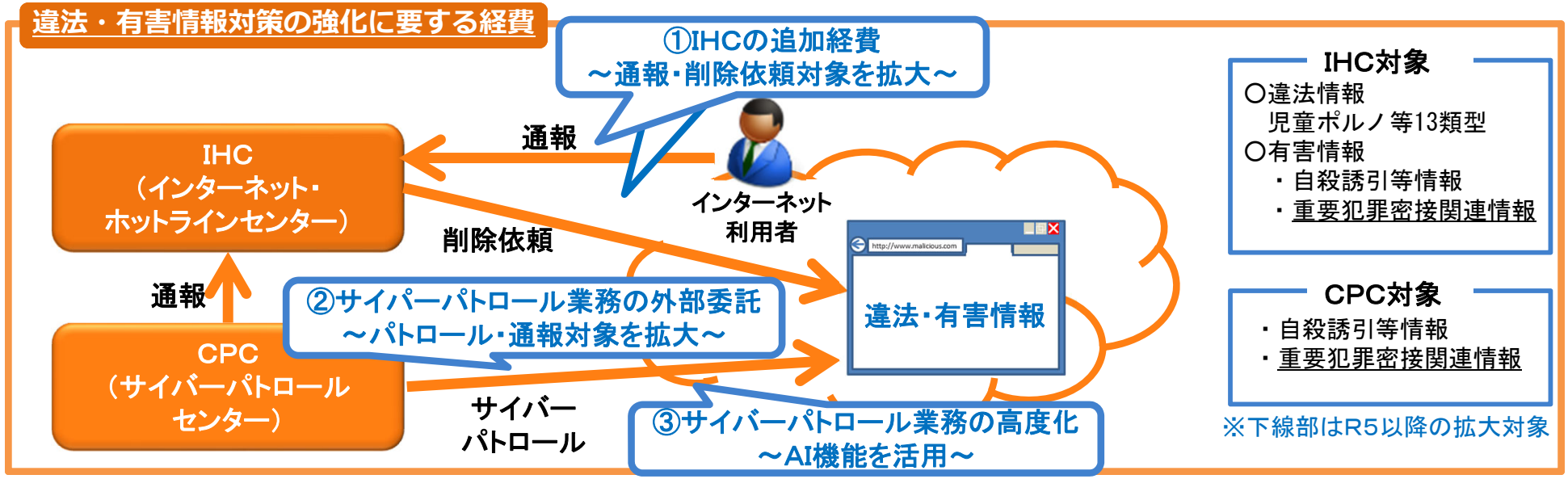
インターネット・ホットラインセンター（IHC）における取扱情報の対象（現行は、違法情報及び自殺誘引等情報）に、個人の生命・身体に危害を加えるおそれが高い重要犯罪等と密接に関連する情報（以下「重要犯罪密接関連情報」という。）を追加することにより、違法・有害情報対策の強化を図るための経費。

## ② サイバーパトロール業務の外部委託に要する経費

サイバーパトロールセンター（CPC）における取扱情報の対象（現行は自殺誘引等情報）に、重要犯罪密接関連情報を追加することにより、有害情報対策の強化を図るための経費。

## ③ サイバーパトロール業務の高度化等に要する経費

サイバーパトロールセンター（CPC）におけるサイバーパトロールの高度化のため、AI（自然言語処理）を活用したシステムを導入することにより、有害情報対策の強化を図るための経費。



デジタル庁

# サイバーセキュリティ確保環境整備費

５年度予算政府案額　１．３億円【うち重要政策推進枠０．４億円】

## 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サイバー攻撃に強いシステムを企画設計（セキュリティ・バイ・デザイン）するほか、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、システムライフサイクル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、監査・検証の実施、セキュリティ研修、脆弱性診断等を実施する。

○デジタル庁システムの情報セキュリティ確保のため、各種研修を実施・受講することによりセキュリティ人材の育成を図る。

## 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り組みの検証・監査・調査等を実施する。

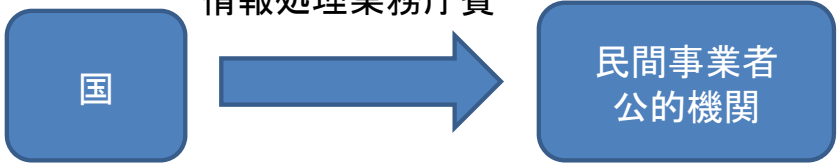
○バックドア等検証
デジタル庁内のシステムや調達する機器・ソフトウェア等のうち、重要なものの安全性を確保するため、バックドアが仕掛けられていないかの検証等を行う。

○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。

○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外部研修により習得する。

○脆弱性診断等の実施
統一基準における「自己点検」や「情報セキュリティ監査」の位置付けで行うこととし、各システムの脆弱性対策が適切に実施されているか庁内のシステム全体を視野に実施する。

## 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・検証等）、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インシデントに係る調査

令和５年度予算政府案額　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。

# 金融庁の施策例

金融庁

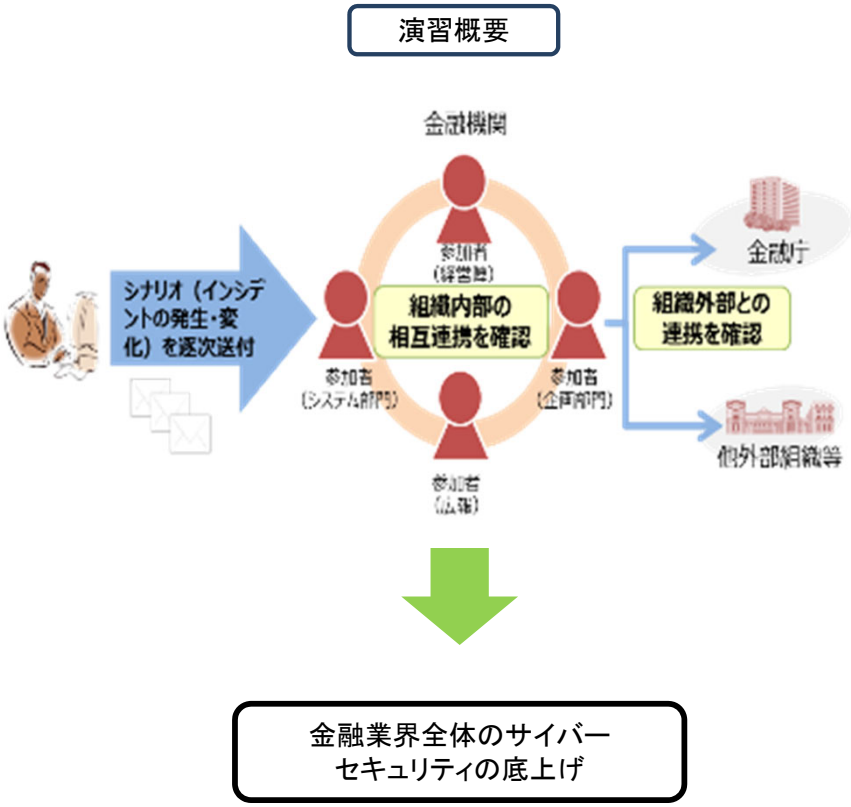
## 金融分野のサイバーセキュリティ対策強化

### ○ 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５年度予算政府案：0.9億円

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」（平成27年７月策定、30年10月、令和4年2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4年度、7回目の「金融業界横断的な演習」（Delta Wall Ⅶ）を実施。
  （参考）令和4年度演習は約160先が参加（前回は150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5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



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５年度予算政府案額　０．８億円

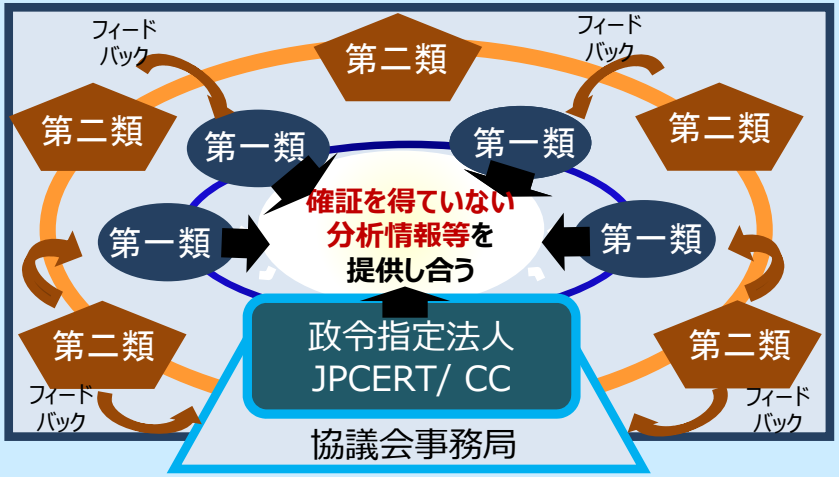
## 事業概要・目的

○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。

# 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

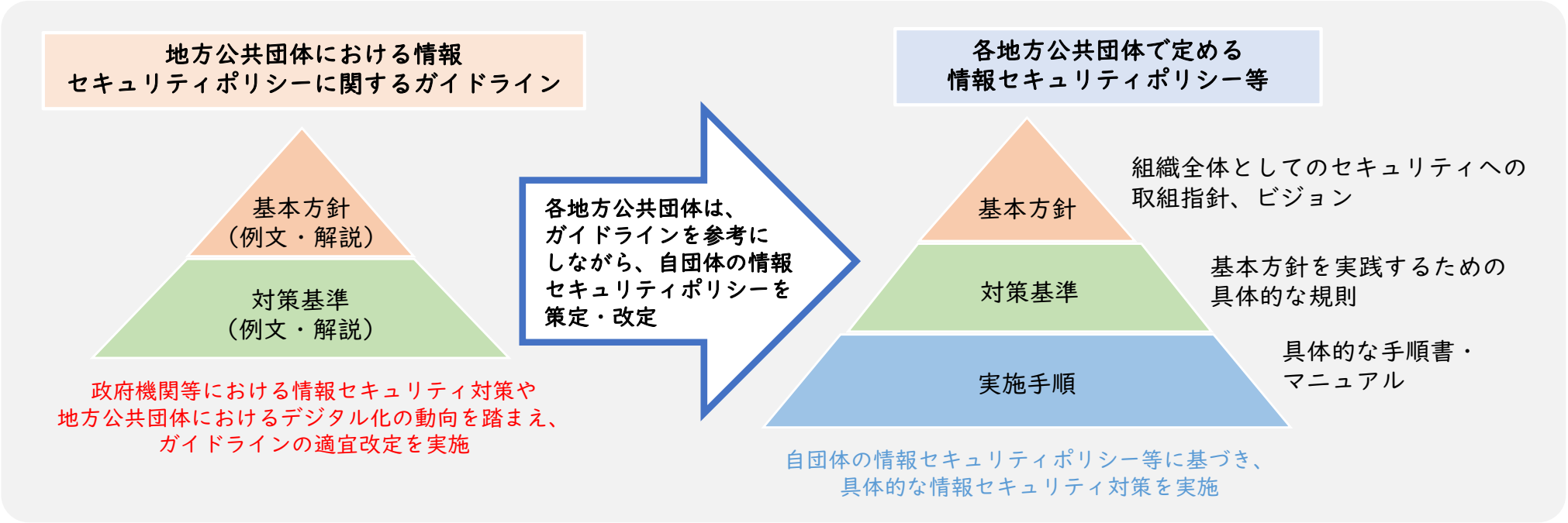
【主な経費】 地方公共団体の情報セキュリティ対策の強化に要する経費　０．７億円〈令和5年度予算政府案〉

**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５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



## 情報システムの防護

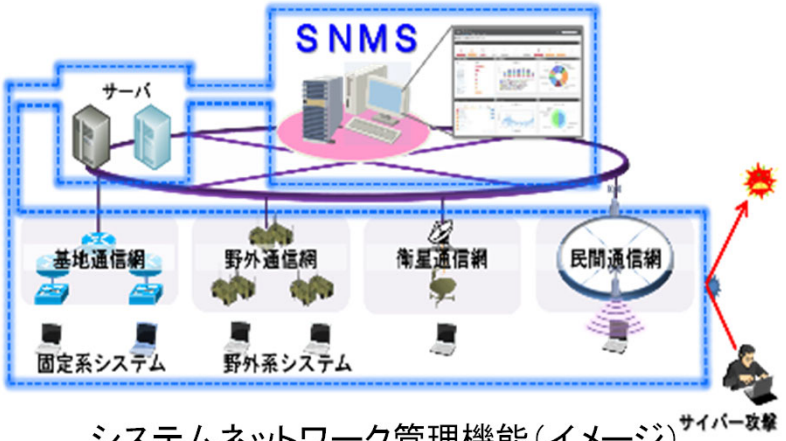
令和5年度予算政府案：477．4億円

（令和5年度予算政府案の具体例）

### ◆ 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



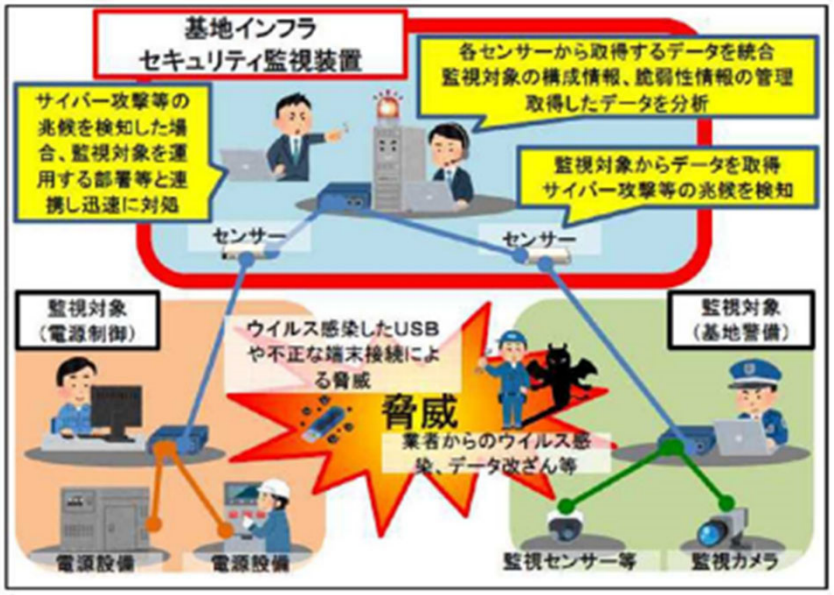

システムネットワーク管理機能（イメージ）

### ◆ 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

### ◆ 施設インフラにおけるサイバーセキュリティ対策

施設インフラにおける物理的対策や可搬記憶媒体及びプログラムへの不正接続を感知・通報・遮断するシステムの導入




基地インフラセキュリティ監視装置（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5年度予算政府案：301．1億円

（令和5年度予算政府案の具体例）

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」**

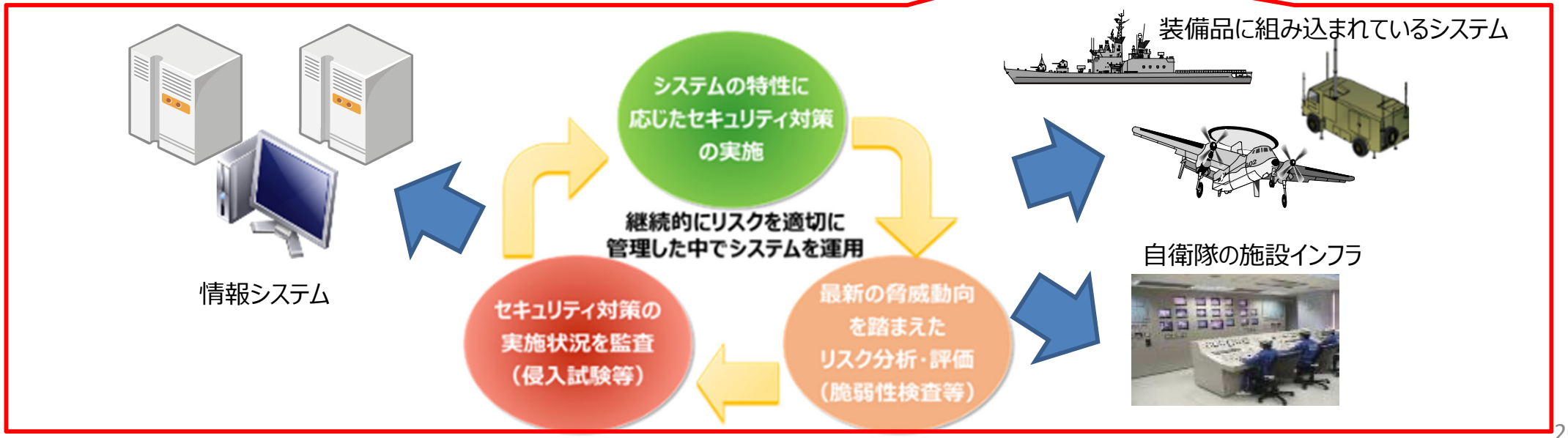
**ＮＩＳＴ　ＳＰ８００－３７**
**（リスク管理枠組み（Risk Management Framework：RMF））**

**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

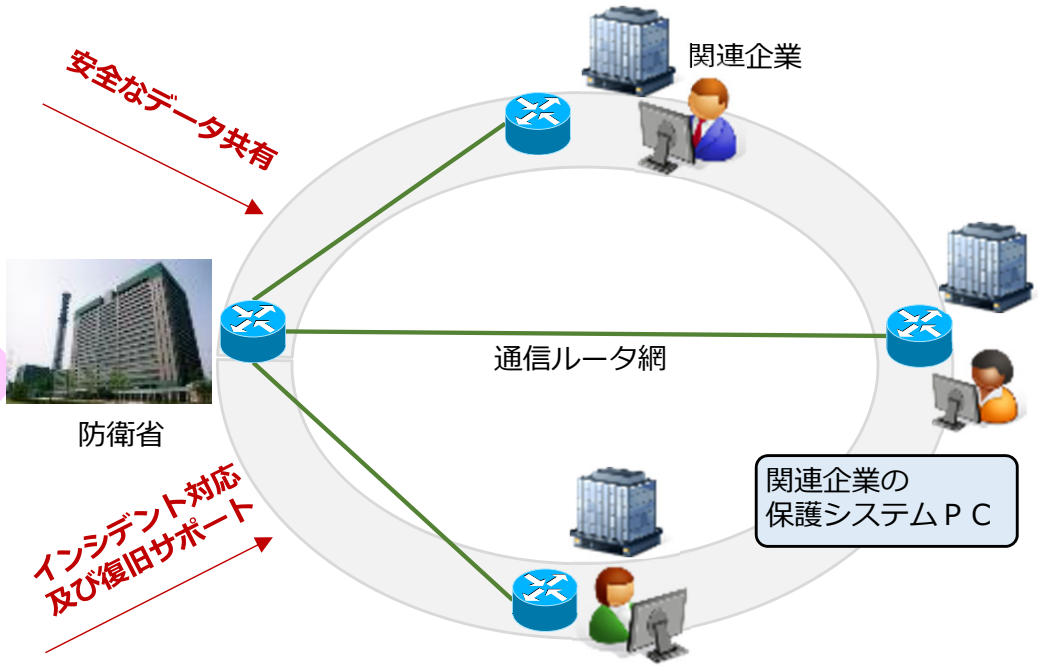
**令和5年度予算政府案：68．5億円**

（令和5年度予算政府案の具体例）

### ◆ 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、防衛関連企業に対して「防衛産業サイバーセキュリティ基準」に適合するセキュリティ機能を供用

| | |
|---|---|
| 保管・管理機能 | ➢ データ保管・管理機能 |
| **セキュリティ機能** | ➢ アクセス制御、識別・認証機能<br>➢ 構成管理・資産管理<br>➢ システム監視・ログ取得機能<br>➢ 脆弱性スキャン機能<br>➢ デプロイメント管理機能<br>➢ バックアップ機能 |
| **ＳＯＣ**<br>（セキュリティオペレーションセンター） | ➢ 脆弱性対応管理<br>➢ 変更管理<br>➢ インシデントレスポンス<br>➢ 点検・監視<br>➢ 構成・資産管理 |




※防衛省が整備するクラウド型セキュリティゲートウェイ機能を利用して、プライム・ベンダー間や企業・防衛省で情報のやり取りをできるようにする。

# 防衛省の施策例



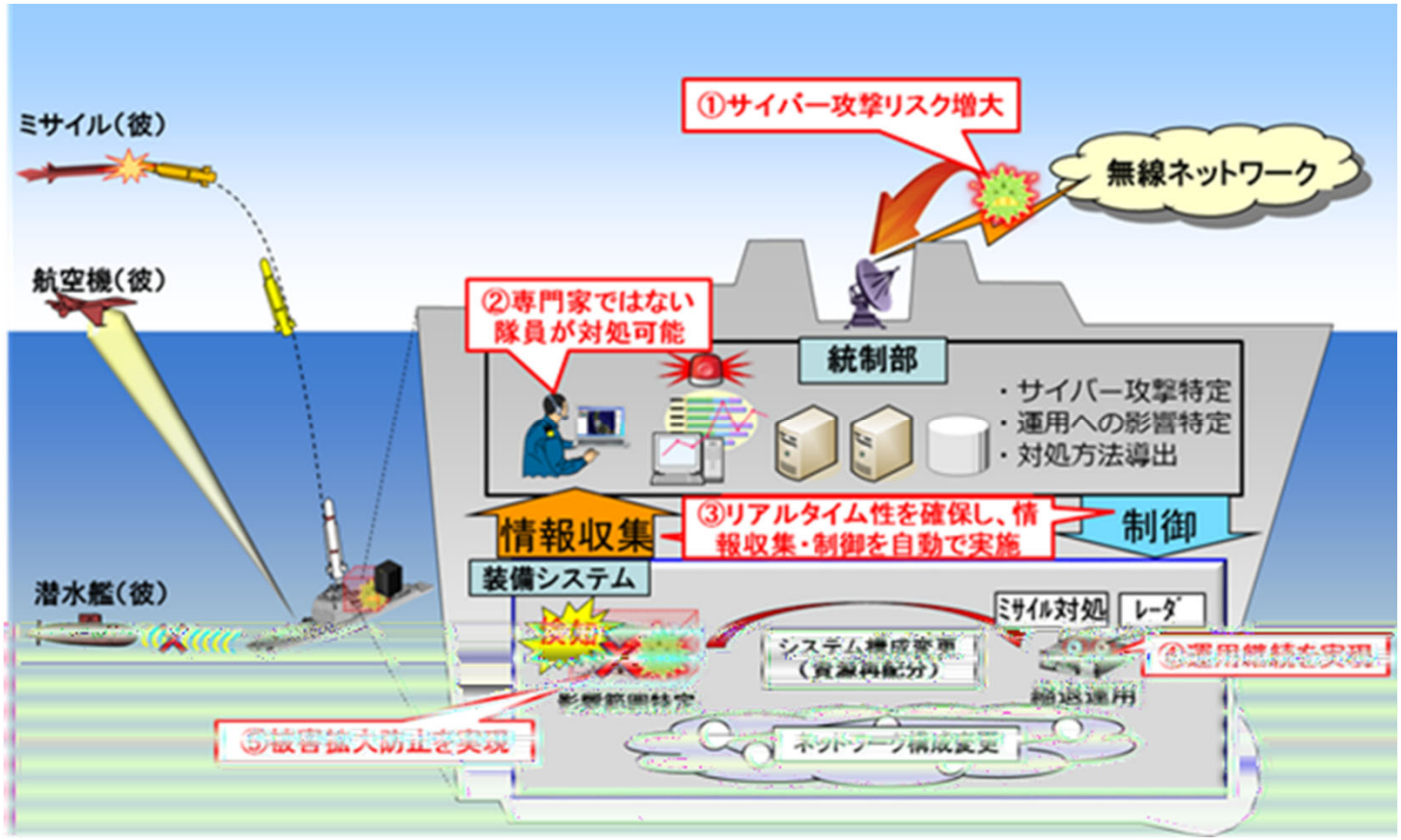
## サイバー分野における研究機能の強化

令和5年度予算政府案：14．6億円

（令和5年度予算政府案の具体例）

◆ **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の装備システム用サイバー防護技術の研究を実施し、護衛艦等の装備システムに研究成果を反映




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テロの被害の未然防止・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５年度政府予算案：　４．３億円

**目的**

○高度化・複雑化が進むサイバー攻撃等の被疑者の検挙・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

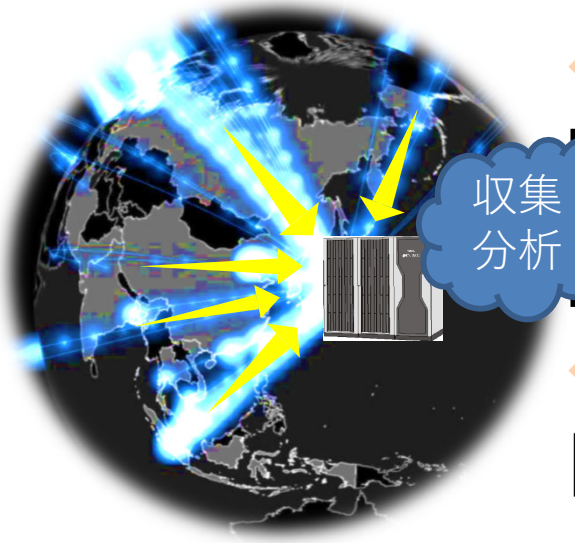
**現状**

○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センサーの機能を強化
○オープンソース情報等を活用した、多角的な分析を実施



収集
分析

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

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

効果

被疑者の検挙
攻撃手法の特定
アトリビューション

分析結果等の照会

注意喚起

重要インフラ事業者等
一般インターネット利用者

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5年度予算政府案額：20．1億円

（令和5年度予算政府案事業の具体例）

◆ 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

◆ 自衛隊におけるサイバー教育基盤の拡充

サイバーセキュリティ態勢の強化のため、陸上自衛隊通信学校を「陸上自衛隊システム通信・サイバー学校（仮称）」に改編

◆ 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

◆ 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、諸外国との協議や訓練等を通じて、サイバー分野における連携を強化

陸自通信学校の教場（イメージ）

# 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

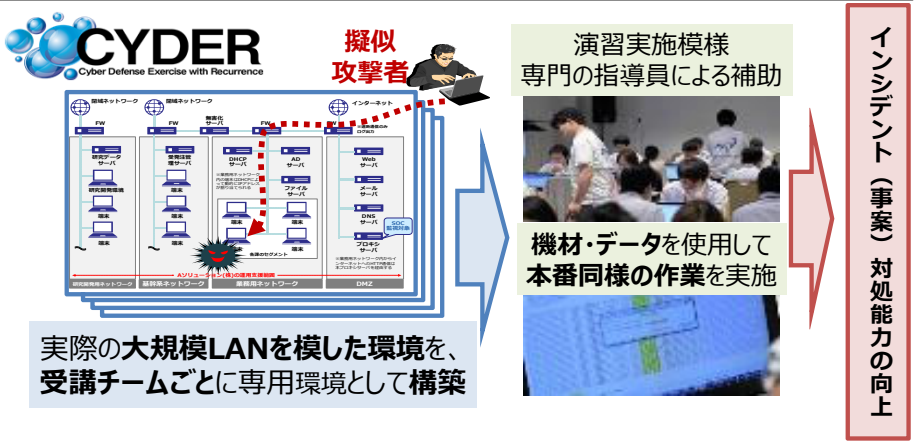
● 巧妙化・複雑化するサイバー攻撃に対し、国立研究開発法人情報通信研究機構（NICT）に設置した「ナショナルサイバートレーニングセンター」において、実践的な対処能力を持つセキュリティ人材等を育成し、我が国のサイバーセキュリティを強化。

令和5年度予算政府案　12.7億

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得る最先端のセキュリティ人材を育成。


③万博向け演習プログラムの提供

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に、CYDERを基にした人材育成の演習プログラムを提供。


サイバー攻撃に対処可能な万博関連組織の人材育成

**万博向け演習プログラムの提供**

# 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。

**令和5年度予算政府案 12.0億円**

## 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ネットワークの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担保するため、その構成要素及びサービスについて5Gユースケース毎に技術的検証を実施する。

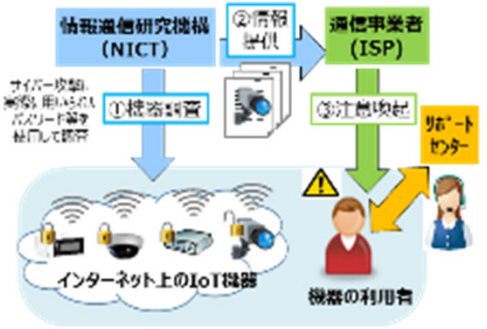
## ③ 地域におけるIoTセキュリティ対策の強化

地域のコミュニティや企業、教育機関等と連携して、IoTセキュリティ人材を自立的に育成していくためのエコシステムの横展開に向けた実証を行うとともに、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、ガイドラインの見直しや事例調査等を実施する。

## 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。

①IoTセキュリティ対策の推進



文部科学省

# GIGAスクールにおける学びの充実

令和5年度予算額（案）　3億円

## 背景・課題

「GIGAスクール構想」の下で１人１台端末の整備が概ね完了し、本格的な活用フェイズに入る中、優良事例の普及、自治体支援機能の強化、指導者の確保など課題も顕在化しており、地域間・学校間の格差も生じている。このため、これらの課題の解消に総合的に取り組む。

## 事業内容

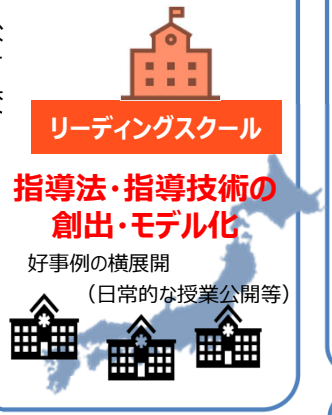
1人1台端末環境の本格運用を踏まえ、その効果的な活用を通じた児童生徒の学びの充実に向けて、実践例の創出・普及、要支援地域への指導支援、教師の指導力向上支援の更なる強化を図る。

### ○リーディングDXスクール事業

（令和4年度第2次補正予算）

１人１台端末の活用状況を把握・分析するとともに、効果的な実践例を創出・モデル化し、都道府県等の域内で校種を超えて横展開するとともに全国に広げていくことで、全国のすべての学校でICTの「普段使い」による教育活動の高度化を図る。

- 全国各地域における先進的な実践例の創出
- 好事例の動画等制作、全国展開
- 教科横断的プログラムの開発・展開支援
- GIGAスクール構想のための調査・分析




### ○学校DX戦略アドバイザー事業等による自治体支援事業

（一部、令和4年度第2次補正予算）

１人１台端末の日常的な活用について、課題を抱える自治体・学校に、集中的な伴走支援を実施。学識経験者、先進地域の教育委員会や指導主事、ネットワークや情報セキュリティの専門家など、国がアドバイザーとして任命した者が、地域・学校へ直接助言する。

<助言を必要とする主な課題やテーマ>

【指導面】
- GIGA端末を活用した効果的な指導方法
- GIGA端末を活用した働き方改革の推進
- 情報モラル教育の充実

【環境整備面】
- 域内のＤＸ推進計画の立案
- 運営支援体制の充実
- 校務のＤＸ、データ連携
- ネットワークの改善整備など
- 情報セキュリティポリシーの改訂

### ○高等学校情報科等強化によるデジタル人材の供給体制整備支援事業

（令和4年度第2次補正予算）

専門性の高い指導者が育成・確保されるエコシステム確立に向け、大学・専門学校・民間企業・NPO等と各都道府県教育委員会とのマッチングを図る協議会等により取組の格段の充実を図る。また、高度な内容を扱う新設科目「情報Ⅱ」（令和５年度～）の指導の充実に向けて、教材等を開発、作成する。

- 専門人材の育成・確保の仕組の確立
- 新学習指導要領に基づく「情報Ⅱ」の指導の充実に向けた教材等の開発
- 効果的な指導事例の開発、普及・展開

### ○情報モラル教育推進事業

- 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改訂
- 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

- 調査問題の妥当性等を検証するための予備調査実施など次回調査に向けた準備
- R4新規作成調査問題のシステム搭載

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

令和５年度予算政府案額　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。

# 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５年度予算政府案額：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）