サイバー安全保障分野での対応能力の向上に向けた有識者会議
官民連携に関するテーマ別会合　第2回
参考資料

令和６年７月23日

内閣官房
サイバー安全保障体制整備準備室

ソフトウェア等の脆弱性対応 ～安全な製品開発～

※前回資料（再掲）

- ✓ 各国では、これまで、安全な製品開発を促すため、**国際標準や認証制度の整備**を促進
- ✓ 一方、海外では、安全な製品開発に関する**製品ベンダの責務の明確化や法的義務の導入**も顕在化

【ソフトウェア等の脆弱性対応の流れ】

安全な製品開発 → 脆弱性認知 → 解消手段開発（製品開発者） → 注意喚起（公的機関） → 解消手段適用（利用者）

【国内外におけるこれまでの取組】

国際標準や認証制度の整備

- ✓ 情報技術に関連した製品及びシステムの評価に関するコモンクライテリア(ISO/IEC 15408, 1999年)を皮切りに国際標準の整備が進捗
- ✓ 制御システムに係る同様の国際標準として、IEC62443において、製品開発ライフサイクルや、技術的セキュリティの要件が定められている

国際標準等に即した国内の動き

- ✓ 上記国際標準に基づき、例えば、情報処理推進機構がISO/IEC15408の認証制度を運営
- ✓ 最近では、各国でIoT機器の枠組み整備が進められており、国内でも「IoT製品に対するセキュリティ適合性評価制度」が2025年3月から一部開始予定

＋

【海外における更なる取組】

サイバー空間を守る責任のリバランス (2023年)

- ✓ 「国家サイバーセキュリティ戦略」(2023年3月)において米国政府が提唱。現在、サイバーリスクを低減する責任が利用者に過度に偏っているとの現状認識の下、**システムの提供者や政府の役割拡大**を謳う

セキュアバイデザイン・セキュアバイデフォルト原則(2023年 日米欧等の18組織が共同署名)

- ✓ **ソフトウェア提供者に係る三原則**として、①顧客のセキュリティの結果に責任を持つ、②徹底した透明性と説明責任を負う、③トップ主導での実施、を具体的に説明。

製品セキュリティ及び通信インフラ法 (2024年施行)

- ✓ ネットワーク製品提供者に対し、脆弱な初期パスワード設定の禁止、**セキュリティ対応体制の構築を求める**

サイバーレジリエンス法草案 (2022年提出)

- ✓ デジタル製品のメーカに対し、上市前の適合性評価、**脆弱性悪用が発見された場合の当局(ENISA※)への報告等**を規定

※ENISA（欧州連合サイバーセキュリティ機関）：The European Union Agency for Cybersecurity

ソフトウェア等の脆弱性対応 ～脆弱性の早期対応～

※前回資料（再掲）

- ✓ 開発段階でいかに注意しても、システムへの不正侵入等に悪用し得るバグ（＝脆弱性）は発生
- ✓ 製品開発者による解消手段の開発と、利用者による適用を促すため、米国MITRE社等が脆弱性管理に係る国際枠組みを運営。**同国際枠組みと連携しながら、日本国内でも同様の制度を整備**
- ✓ 一方、海外では、解消手段の開発前に悪用が先行する「ゼロデイ脆弱性」も念頭に、**脆弱性悪用状況や、重要インフラにおける機器利用状況等を踏まえた、踏み込んだリスク情報も提供**

安全な製品開発 → **脆弱性認知** → **解消手段開発**（製品開発者） → **注意喚起**（公的機関） → **解消手段適用**（利用者）

【国内外におけるこれまでの取組】

脆弱性管理に係る国際枠組み（1999年）

- ✓ ソフトウェア等の脆弱性に係る情報を国際的に一元管理するため、米国非営利団体MITRE社が、年間3万件弱発見される個々の脆弱性を採番管理（例.CVE-2024-0000など）
- ✓ 米国国立標準技術研究所(NIST)が技術的な悪用可能性を「CVSS値」として算出・公表※

早期警戒パートナーシップ制度（2004年）

- ✓ 「情報処理の促進に関する法律」の告示に基づき、情報処理推進機構及びJPCERT/CCが運営。上記国際枠組みとも連携
- ✓ このほか、国内悪用実績などリスクが高い脆弱性は、JPCERT/CCやNISC等が注意喚起

＋

【海外における更なる取組】

悪用された脆弱性のデータベース化（2021年）

- ✓ 国土安全保障省のサイバーセキュリティ・インフラ保安庁(CISA)が、米国内で悪用された脆弱性について、**「既知の悪用された脆弱性(KEV)カタログ」として一覧化した上で公表**
- ✓ 政府機関は、カタログに記載された脆弱性について、**原則2週間以内に対策を講じる**ことが必要（期間は脆弱性の影響度により変わり得る）

重要インフラ保安法(SOCI法、2022年改正)

- ✓ 重要インフラ事業者に対して、データ、コンピュータ等を含めた**資産登録義務付け**
- ✓ 登録された資産情報については、迅速な助言やリスク情報提供等に活用

※CVE（共通脆弱性識別子）：Common Vulnerabilities and Exposures ※CVSS（共通脆弱性評価システム）：Common Vulnerability Scoring System

脆弱性ハンドリングの類型

安全な製品開発 → **脆弱性認知** → **解消手段開発**（製品開発者） → **注意喚起**（公的機関） → **解消手段適用**（利用者）

【発見時において、未だ悪用されていない場合：約29,000件/年(MITRE,2023年)】

① 製品開発者が自ら脆弱性・対応策を公表する場合
（主要ベンダによる脆弱性公表、機器メーカーの「プロダクト・サート」）
※IEC62443等で標準化・普及
製品開発者

② 製品開発者が、外部発見者の協力を得て脆弱性を発見、対応策を公表する場合
（例：ベンダによる外部発見者への報奨金支払い）
発見者 ⟷ 製品開発者

③ バグバウンティ・プラットフォームが、製品開発者と外部発見者を仲介する場合
発見者 → バグバウンティプラットフォーム ⟷ 製品開発者

④ 専門機関が、製品開発者と外部発見者を仲介する場合
（例：MITRE, JPCERT/CC など）
発見者 → 調整機関 ⟷ 製品開発者

【発見時において、ゼロデイ脆弱性として既に悪用されている場合：約60-100件/年※】

⑤ ゼロデイ脆弱性の悪用が起点となり、脆弱性対応が行われる場合
被害組織 セキュリティベンダ → 対処機関 → 調整機関 ⟷ 製品開発者

※https://cloud.google.com/blog/topics/threat-intelligence/2023-zero-day-trends?hl=en

公表登録 →

IPA / MITRE / NIST National Institute of Standards and Technology

管理簿掲載内容分析

CVE番号付与
MITREが一括管理

CVSS値付与
NISTが技術面から悪用可能性を評価

ウェブサイト公表
NISTやIPAが管理

公開 →

NISC / CISA

影響評価 注意喚起 → 利用者

普及状況・悪用動向を含めた評価

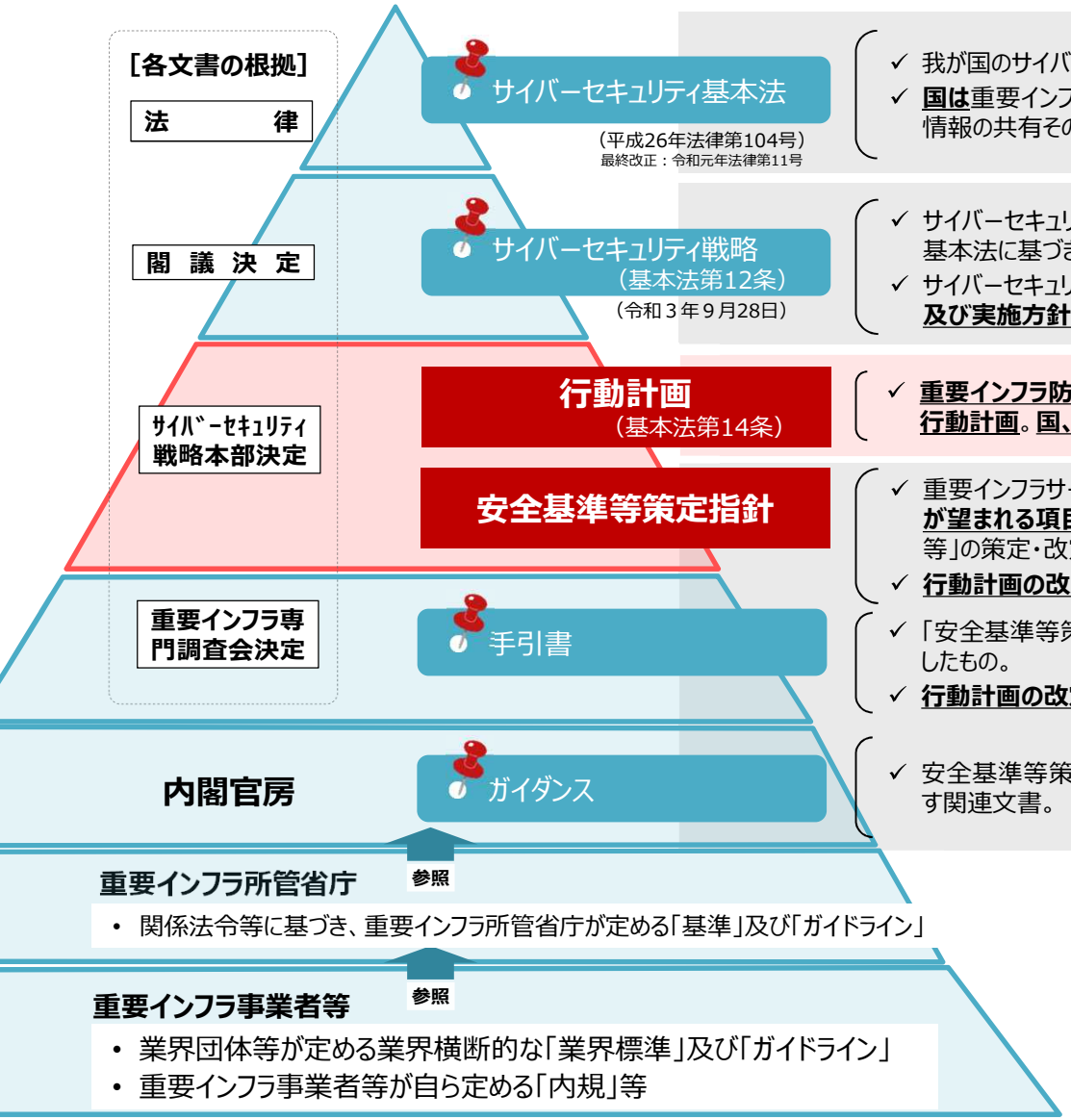
- 米国ではCISAが「既知の悪用された脆弱性(KEV)」を公表

商流を踏まえた利用者への周知

重要インフラ防護に関する戦略・指針等

■ 重要インフラ分野の防護範囲は、サイバーセキュリティ戦略本部が「行動計画」により決定。

■ また、同本部は「安全基準等策定指針」を策定している一方、遵守の実効性を確保する仕組みがあるわけではない。



- ✓ 我が国のサイバーセキュリティ政策に関し、基本理念、**国、事業者等の責務を定める**。
- ✓ **国は**重要インフラ事業者等におけるサイバーセキュリティに関し、**基準の策定**、演習及び訓練、情報の共有その他の自主的な取組の促進その他の**必要な施策を講ずるもの**とされている。

- ✓ サイバーセキュリティに関する施策の総合的かつ効果的な推進を図るため、サイバーセキュリティ基本法に基づき策定される**サイバーセキュリティに関する基本的な計画**。
- ✓ サイバーセキュリティに係る我が国としての基本的な立場を明らかにするとともに、**諸施策の目標及び実施方針を国内外に示す**ことを目的とする。３年ごとに改定。

- ✓ **重要インフラ防護に係る基本的な枠組み**を定めた政府と重要インフラ事業者との**官民共通の行動計画**。**国、重要インフラ事業者等が取り組むべき事項が規定**。

- ✓ 重要インフラサービスの安全かつ持続的な提供を図る観点から、**「安全基準等」において規定が望まれる項目を整理・記載**し、重要インフラ事業者や重要インフラ所管省庁の「安全基準等」の策定・改定を支援することを目的とするもの。
- ✓ **行動計画の改定、サイバーセキュリティを取り巻く環境の変化等を踏まえて見直し**を実施。

- ✓ 「安全基準等策定指針」で定めたリスクアセスメントや情報共有を行う際の手順を具体的に示したもの。
- ✓ **行動計画の改定、サイバーセキュリティを取り巻く環境の変化を踏まえて見直し**を実施。

- ✓ 安全基準等策定指針及び手引書に付随する文書として、個別の対処方法、留意点等を示す関連文書。

国際標準、他国の基準等

ISO/IEC　NIST　…

我が国と諸外国における重要インフラの対象分野

- 重要インフラ分野の範囲は、サイバーセキュリティ戦略本部による行動計画の改定により随時追加。
- 諸外国では、幅広く重要インフラとして指定しているが、必ずしも重要インフラ間の優先順位付けは見られない。
- なお、重要インフラ分野の防護範囲を決定する戦略本部の構成として、我が国や諸外国で重要インフラとなっている分野を所管する大臣が全て入っているわけではない。

	第１次行動計画 （2005年12月 ～ 2009年2月）	第２次行動計画 （2009年2月 ～ 2014年5月）	第３次行動計画 （2014年5月 ～ 2017年4月）	第４次行動計画 （2017年4月 ～ 2022年6月）	現 行動計画 （2022年6月 ～ ）
重要インフラ	**10分野**（情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流） 10分野	**＋3分野**（化学、クレジット、石油） 13分野	**＋1分野**（空港） 14分野	**＋1分野**（港湾）（2024年～） 15分野	

	アメリカ（16分野）	イギリス（13分野）	オーストラリア（11分野）	EU NIS2指令（11＋7分野）※基幹事業体＋重要事業体	
重要インフラ対象分野	＜重要インフラ分野＞ ①通信 ②情報技術（IT） ③金融 ④輸送システム ⑤エネルギー ⑥化学 ⑦政府施設 ⑧上下水道 ⑨公衆衛生・医療 ⑩緊急サービス ⑪食糧・農業 ⑫商業施設 ⑬重要製造業 ⑭ダム ⑮防衛産業基盤 ⑯原子力(炉・部材・廃棄物)	＜国家重要インフラ分野＞ ①通信 ②金融 ③輸送 ④エネルギー ⑤政府 ⑥水道 ⑦保健 ⑧緊急サービス ⑨化学 ⑩食糧 ⑪防衛 ⑫民生用原子力 ⑬宇宙	＜重要インフラ分野＞ ①情報通信 ②金融 ③交通 ④エネルギー ⑤医療 ⑥水道 ⑦食料・農業 ⑧防衛産業 ⑨データ・クラウドサービス ⑩教育・研究機関 ⑪宇宙	＜基幹事業体＞ ①エネルギー（電力、地域冷暖房、石油、ガス、水素） ②輸送（航空、鉄道、水上、道路） ③銀行 ④金融市場インフラ ⑤医療 ⑥飲料水 ⑦廃水 ⑧デジタルインフラ ⑨ICTサービス ⑩行政 ⑪宇宙	＜重要事業体＞ ①郵便・宅配便 ②廃棄物処理 ③化学品 ④食糧 ⑤製造（医療機器、コンピュータ・電子光学機器、電気設備、機械設備、自動車・トレーラー、その他輸送機械） ⑥デジタルプロバイダー ⑦研究

諸外国における取り組むべき事項の明確化の取組

■ 諸外国では、分野横断的なサイバーセキュリティ対策のベースラインを明示。

■ 各国で共通する事項としては、「リスク管理（資産管理と脆弱性対策）」、「事業継続と復旧の計画」のほか、「サプライチェーン対策」などが規定されている。

※赤字は、各国で特に共通する事項

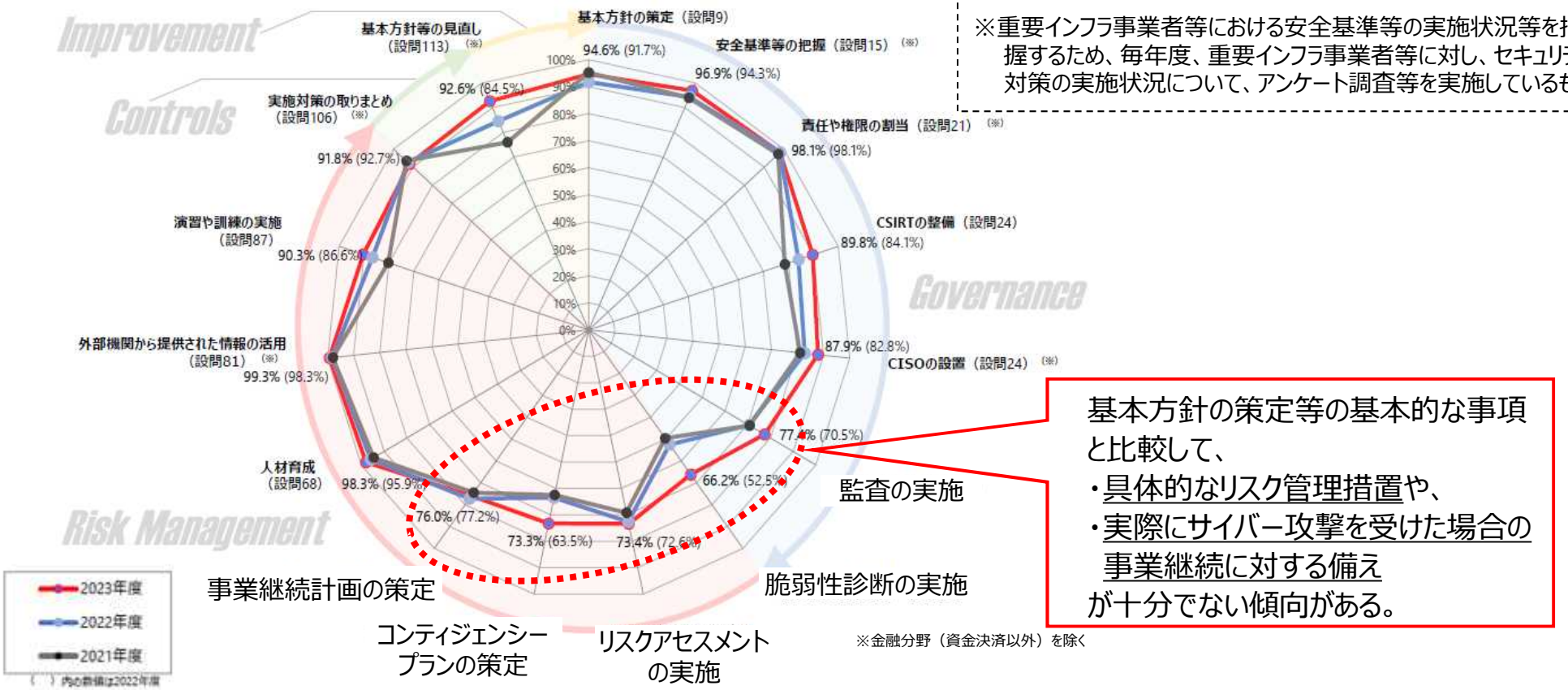
	アメリカ	イギリス	オーストラリア	EU
基準名	Cross-Sector Cybersecurity Performance Goals (CPGs)	Cyber Assessment Framework (CAF)	Essential Eight Maturity Model	NIS2指令 （うちリスク管理措置）
適用対象	重要インフラ全体	国家重要インフラを含む民間事業者	重要インフラを含む様々な組織	基幹事業者及び重要事業者
主な内容	1．識別 資産インベントリ、ITとOTのサイバーセキュリティ関係の改善、既知の脆弱性の緩和、サプライチェーンでのインシデントの報告　等 2．防御 デフォルトパスワードの変更、ネットワークセグメンテーション、多要素認証、OTサイバーセキュリティトレーニング、協力でアジャイルな暗号化、マクロの無効化、システムのバックアップ、ログの収集、公衆インターネットへのOT接続の制限　等 3．検知 関連する脅威及びTPPの検知 4．対応 インシデント報告、脆弱性報告　等 5．復旧 インシデント計画及び準備	1．ガバナンス 2．リスク管理 3．資産管理 4．サプライチェーン 5．サービス保護の方針とプロセス 6．IDとアクセス制御 7．データ・セキュリティ 8．システム・セキュリティ（脆弱性管理等） 9．レジリエントなネットワークとシステム（バックアップ等） 10．スタッフの意識向上と研修 11．セキュリティ監視 12．プロアクティブなセキュリティ・イベントの発見 13．対応と復旧計画 14．教訓からの学習	1．資産管理と脆弱性スキャン 2．OSへのパッチ適用 3．多要素認証 4．特権アカウントの管理 5．アプリケーション制御 6．MS officeのマクロ制御 7．ウェブブラウザの制御 8．定期的なバックアップ	・リスク分析及び情報セキュリティに関する方針 ・インシデント対応 ・事業継続（バックアップ管理等） ・サプライチェーンセキュリティ ・ネットワークやシステムのセキュリティ（脆弱性対処等） ・リスク管理措置の有効性評価 ・サイバー衛生の実施及びサイバーセキュリティ研修 ・暗号の使用 ・人的セキュリティ（アクセス管理等）及び資産管理 ・多要素認証等の活用

重要インフラにおける安全基準等の浸透状況

■ サイバーセキュリティ戦略本部が定める安全基準等策定指針については、重要インフラ事業者への実施状況を毎年度調査。項目等によるばらつきが見られ、例えば、「監査／脆弱性診断の実施」、「リスクアセスメントの実施」、「コンティジェンシープラン／事業継続計画の策定」は、他の項目として相対的に低くなっていることが伺われる。

■ なお、各分野における基準・ガイドライン等は、業法等に基づき所管省庁が定めるもののほか、業界独自に策定するものなど様々となっており、必ずしも遵守の実効性を確保する仕組みがあるわけではない。

安全基準等の浸透状況に関する調査結果（※）
［2021～2023年度］



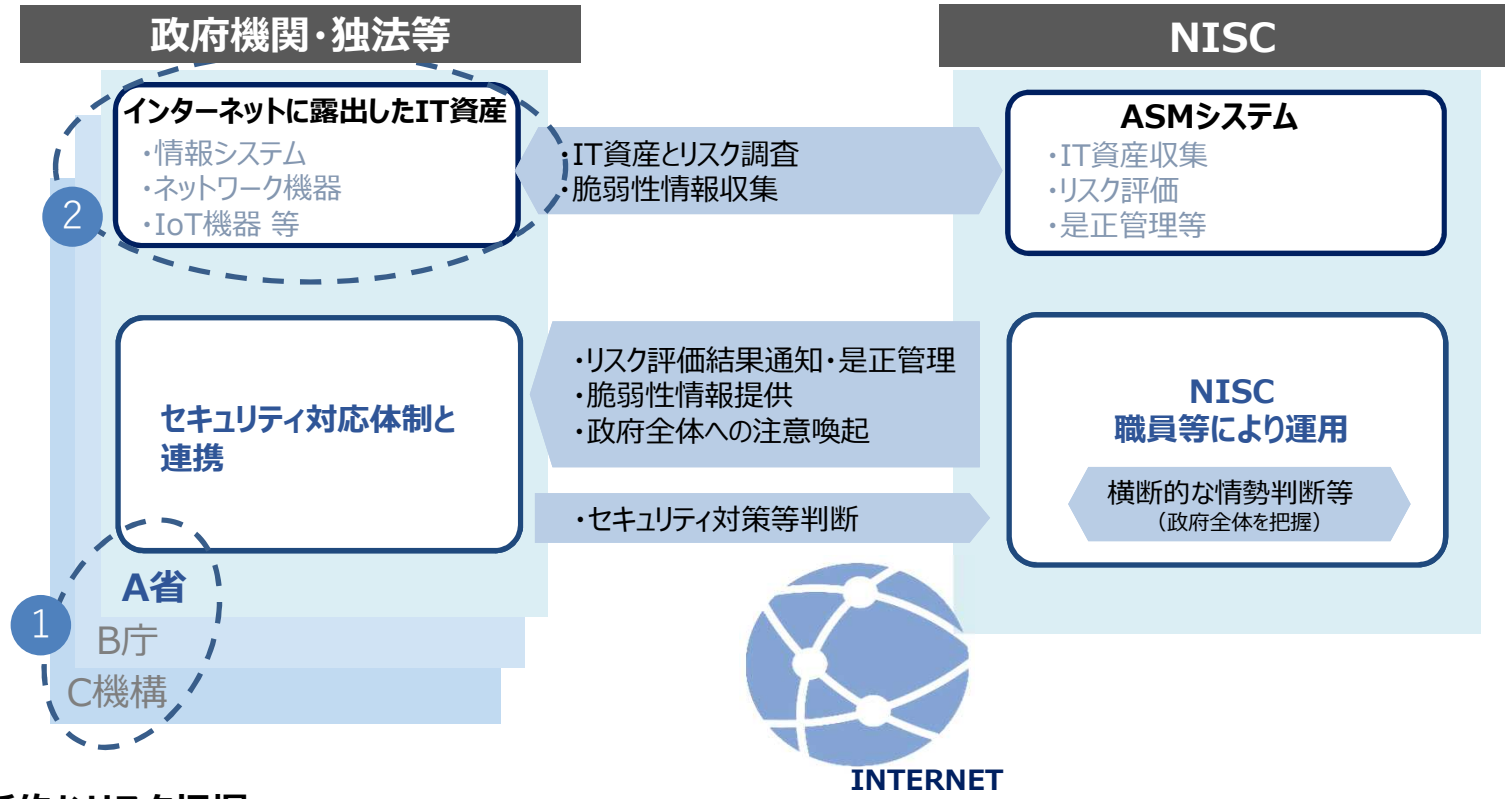
※金融分野（資金決済以外）を除く

※重要インフラ事業者等における安全基準等の実施状況等を把握するため、毎年度、重要インフラ事業者等に対し、セキュリティ対策の実施状況について、アンケート調査等を実施しているもの。

基本方針の策定等の基本的な事項と比較して、
・具体的なリスク管理措置や、
・実際にサイバー攻撃を受けた場合の事業継続に対する備え
が十分でない傾向がある。

政府機関等の対策強化に向けた取組例①（横断的ASM事業）

- NISCにおいて、インターネットに露出した政府機関等のIT資産を対象に、常時評価し、脆弱性等を随時是正する事業として、令和６年度から横断的アタックサーフェスマネジメント事業（横断的ASM事業）を開始。
- なお、政府機関等に提供するリスク評価結果や注意喚起について、その対応は各政府機関等に委ねられており、対応の実効性を確保する仕組みがあるわけではない。



1 横断的なリスク把握

サイバーセキュリティの司令塔として、 NISCにはASM情報の他、各組織で発生したインシデント情報や各種の脅威情報も集約される。
これらの情報とともに政府全体にかかるリスク影響を的確に把握し、政府組織全体のセキュリティ対策を牽引する。

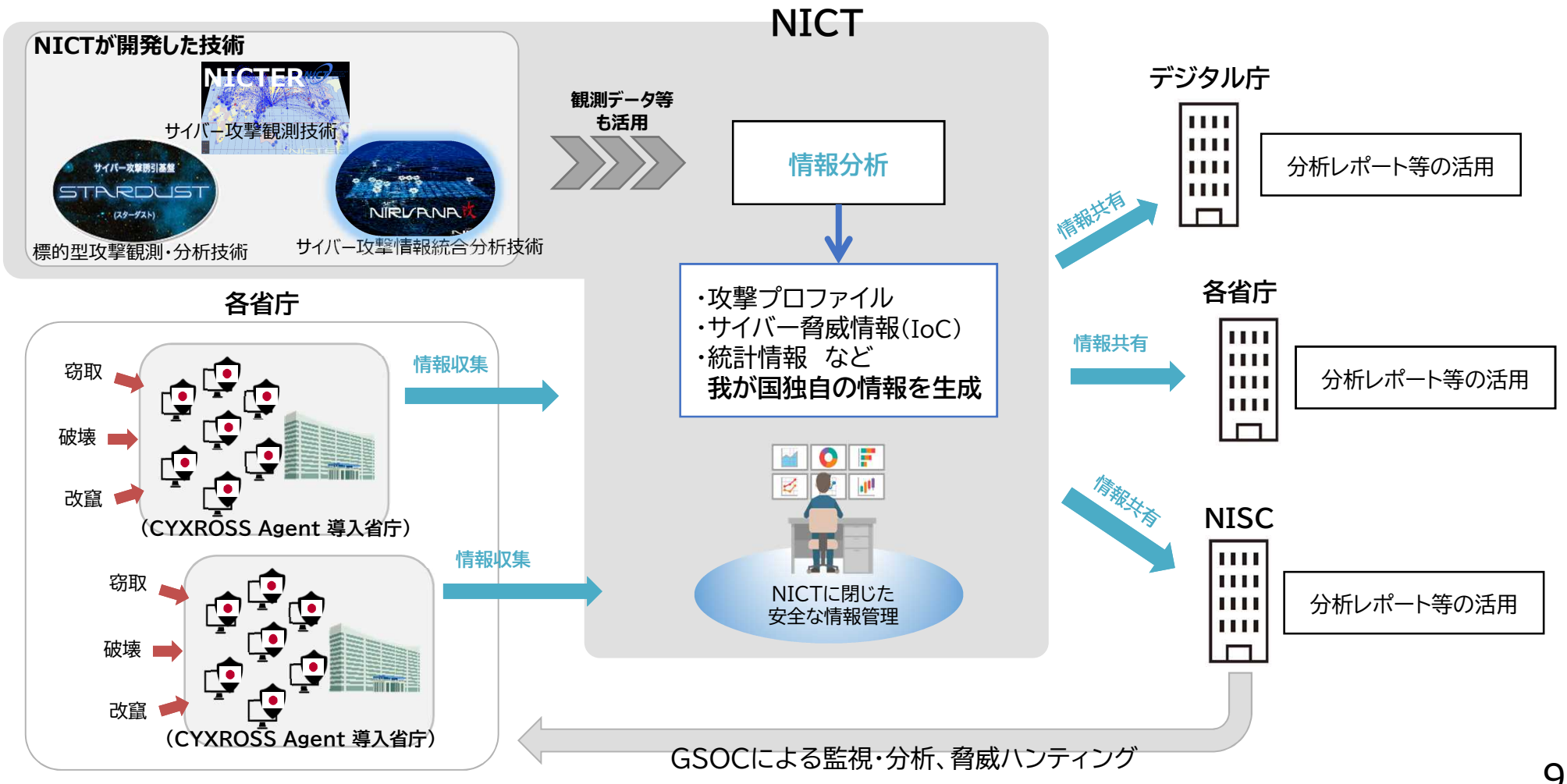
2 攻撃者目線での施策立案

NISCにはセキュリティに精通した人材や機材が集中しており、 攻撃者目線でのリスク評価・是正管理を効果的・効率的に推進することができる。

政府機関等の対策強化に向けた取組例②（CYXROSSプロジェクト）

CYXROSSプロジェクト：CYNEX XROSS-organ observatory Project

- 総務省では、国立研究開発法人情報通信研究機構（NICT）を通じ、安全性や透明性の検証が可能な国産センサー『CYXROSS Agent』を開発し、政府端末に導入することで情報収集や分析を行う事業を実施。NICTが開発した様々な技術や観測等で蓄積したデータも活用し、我が国独自のサイバーセキュリティに関する情報を生成。
- NISCでは、サイバーセキュリティ運用の枠組み（GSOC）による従来の政府機関等全体の監視・分析等に加え、脅威ハンティングのためにも、同事業による組織横断的な情報分析の結果を活用する方向で検討中。



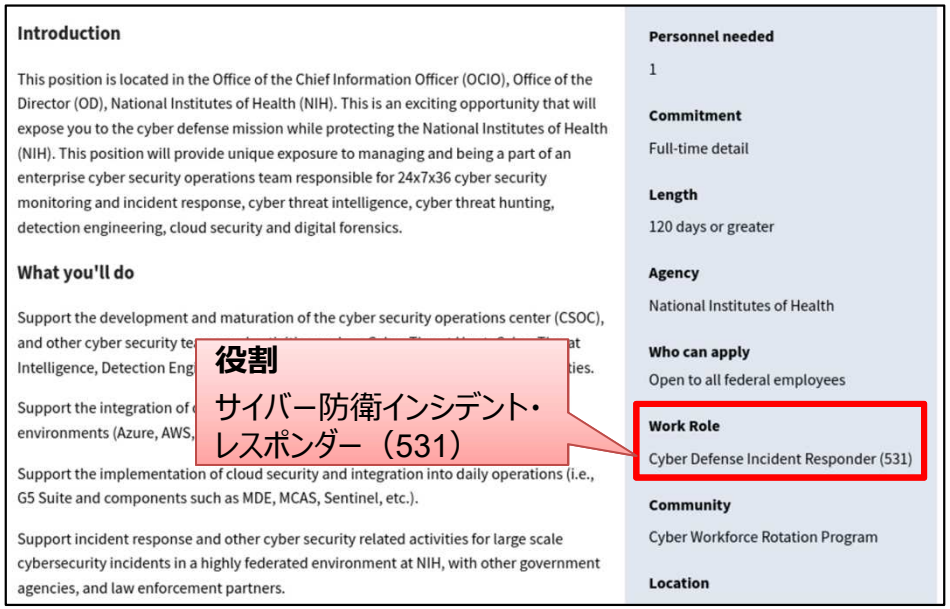
米国におけるNICEフレームワークの人材育成・確保への活用例

■ 米国では、NICEフレームワークを活用し、同フレームワークで定義された職種を軸にして検索できるサイトが提供されているほか、役割に応じた教育コースの提供などがされている。

NICEフレームワークの職種
「サイバー防衛インシデント・レスポンダー」を軸として

①採用情報を検索

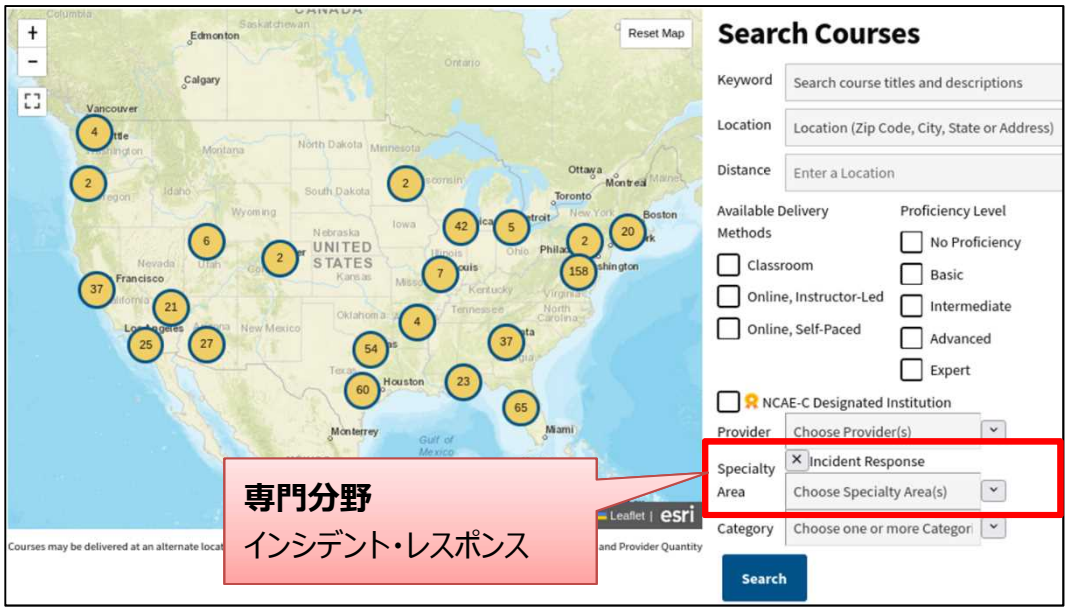
（例）インシデント・レスポンダーを求める連邦政府職員の募集要項



USAJOBSは、連邦政府機関の公務員の採用、ローテーションプログラム等の情報が掲載された米国政府のウェブサイト。NICEフレームワークの職種で求人情報検索ができる。

②教育情報を検索

（例）インシデント・レスポンダーを教育する機関・コースの検索結果



NICCS Education and Training Catalog は、米国各地における、あらゆるスキルレベルのサイバーセキュリティ人材向けの関連育成コースを検索できるサイト。

重要インフラ事業者におけるCISOの設置について

■ 2023年に改定された「重要インフラのサイバーセキュリティに係る安全基準等策定指針」（サイバーセキュリティ戦略本部決定）では、重要インフラ事業者に対し、 CISO等を任命することを求めるとともに、経営層クラスから任命することを推奨。

重要インフラにおける安全基準等策定指針 (2023)改定の背景とポイント

背景	旧指針
サイバー攻撃やシステム障害が重要インフラの**事業経営に影響を及ぼす**ものに変化。	経営層のコミットメント等を含めた情報セキュリティ方針を策定。

改訂のポイント

経営方針にセキュリティ担保を組み入れるとともに、**経営層に相当する者の中からCISO等を任命**することを推奨

重要インフラにおける安全基準等策定指針 （2023年7月4日サイバーセキュリティ戦略本部決定）

3．組織統治におけるサイバーセキュリティ

3.4. 責任及び権限の割当て

サイバーセキュリティリスクの管理について、サイバーセキュリティを担当する部署及び従業員を決定するとともに、責任及び権限を割り当てる。特に、**サイバーセキュリティに関する責任者（CISO等）を任命すべき**であり、その任命にあたっては、経営層の責任において実施する。当該責任者は、サイバーセキュリティに関する知見を有する者であるとともに、組織内の職階において、平時に、またとりわけ有事に、組織トップと直接コミュニケーションできる者として位置づけられるべきであり、**経営層に相当する者の中から任命されることが望ましい**。