資料3

Digital Architecture
Design Center

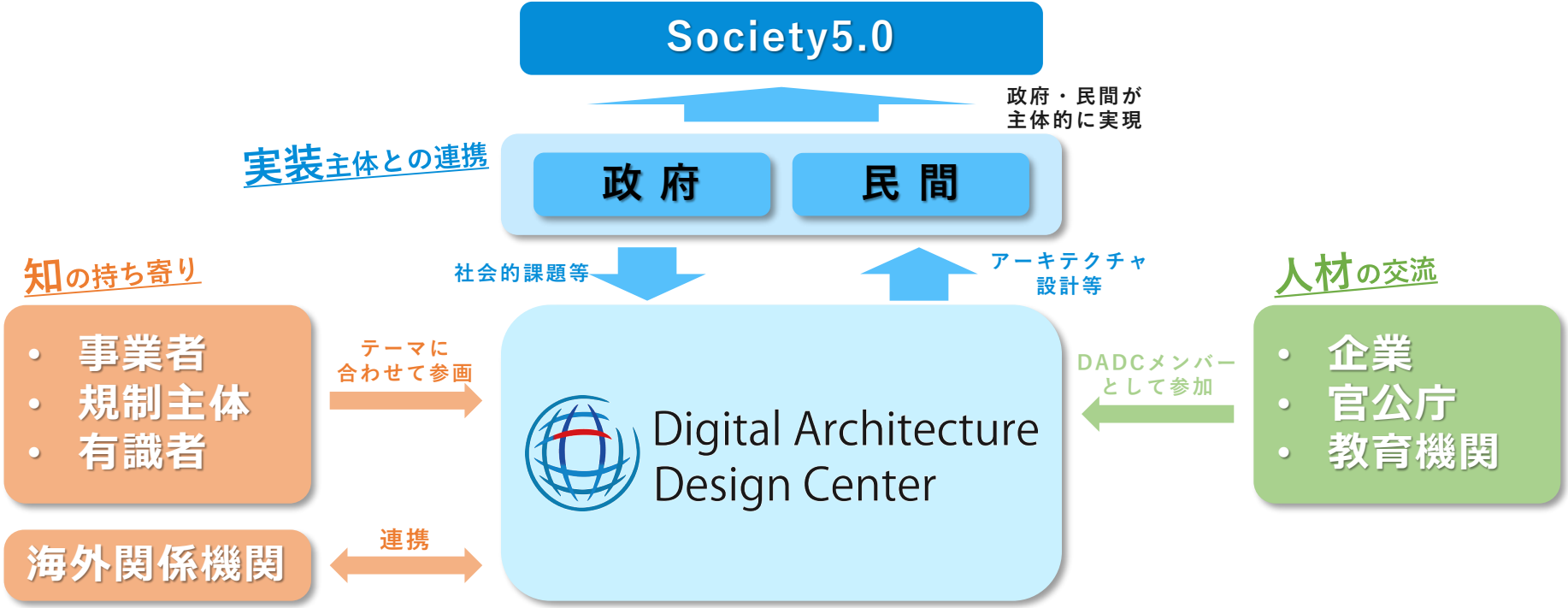
IPA Better Life with IT

DADCにおける
次世代型セキュリティアーキテクチャの
検討について

2022年2月24日
独立行政法人情報処理推進機構（IPA）
デジタルアーキテクチャ・デザインセンター（DADC）

デジタルアーキテクチャ・デザインセンター（DADC）について

Society5.0の実現に向けて社会実装を行う政府・民間からの依頼を受けて、グローバルな動向を踏まえがら、産学官の卓越したリーダーシップ・専門性を有する人材が一堂に会し、Society5.0の実現に必要な社会全体のアーキテクチャを設計する組織



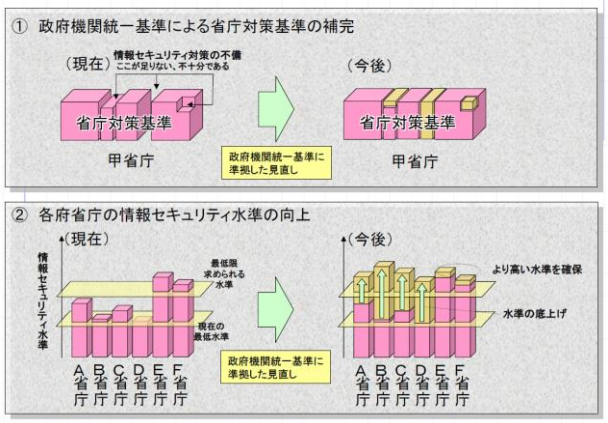
2020年5月15日、改正情報処理促進法の施行日に創設

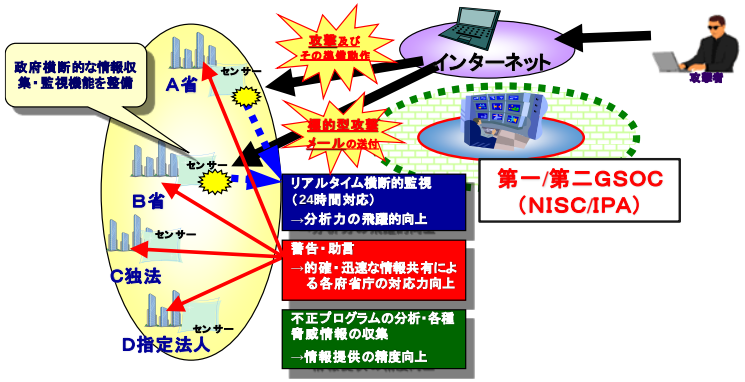
次世代型セキュリティアーキテクチャ設計に至る経緯

日本政府のサイバーセキュリティに係る現状認識

- 政府統一基準群の制定によって各府省庁の情報セキュリティの水準はあがったものの、IT資産の管理やセキュリティ監視・運用は、各省内での対応に限定されている
- 政府横断的な対策はGSOCセンサによる境界監視のみであり、守るべきIT資産に対する攻撃検知時/インシデント発生時の被害状況をリアルタイムに把握する仕組みがない

このような課題意識の下、今回の内閣官房からIPA（DADC）への、次世代型セキュリティアーキテクチャ設計の検討依頼に至った。





次世代型セキュリティアーキテクチャ設計に至る経緯

政府情報システムにおける課題と対応の方向性

課題

●境界型アーキテクチャの限界
- 境界対策を重厚にすることにより、利用者の利便性が低下し、結果としてシャドーIT化を助長しかねない
- 長期かつ多段的な標的型攻撃への対応が困難である。入口対策から出口・内部対策への転換が必要である

●マネジメントによるセキュリティ対応の限界
- 資産・ユーザ・インシデント等のリアルタイムな把握ができていない
- 監視機能の能力が、監視する専門家の能力に依存している

●各省庁での対応の限界
- 政府全体として報告書以外で対応状況を把握する手段がない
- 省庁横断的なサイバー攻撃の把握ができない。特に、インシデントの省庁内部での兆候の把握ができない

対応の方向性

●ゼロトラストアーキテクチャ導入の検討
- デバイス・ユーザの状態を把握し、動的にリソースへのアクセス制御を行う
- 府省庁のデバイスの状況を把握するソフトウェア（EDR、資産管理ツール等）を活用する

●府省間の管理データの連携
- 資産・ユーザ・インシデントの管理データの統合により傾向や予兆を把握する
- 全体の管理データを数10時間内に把握する

●組織に応じた役割分担
- 府省庁：個々の職員や個別のPCの直接的な管理を行う
- デジタル庁・NISC：政府全体の状況を把握し、改善策を検討する

米国CDM（Continuous Diagnostics & Mitigation）プログラムを参考にしつつ、検討中

日本版CDMの導入について

日本版CDMを導入することによるアウトカム

Drivers（駆動要素）

●サイバー攻撃の変化
- サイバー攻撃の高度化・多様化
- サイバー攻撃被害の甚大化
- 影響範囲拡大の迅速化

●政府横断的対応に係る課題
- システム侵害事案の増加
- 統一基準に基づくセキュリティ対策の徹底
- サイバー攻撃対策のための人的負荷の増大
- サイバー人材の不足
- 働き方の変化によるリスクの分散
- システム化予算の圧縮要求
- セキュリティ対策費用の圧縮要求

●その他
- 過度のベンダー依存からの脱却
- 安心・安全の確保
- DX、クラウドバイデフォルトの推進
- ZTAへの期待

Enterprise State

日本版CDM
常時診断・対応型
セキュリティ
アーキテクチャ

Work Processes

GSOC
CYMAT
CSIRT
等

Outcomes（アウトカム、結果要素）

●未然対応能力の向上
- 攻撃対象領域の極小化
- サイバーセキュリティ態勢の可視性の向上
- 情報セキュリティ対策実効性確認の効率化
- セキュリティリスクの低減
- セキュリティインシデントの抑止
- 迅速な脆弱性対応プロセスの提供
- 持続的な改善

●事故対応能力の向上
- サイバーセキュリティ対応機能の改善促進
- セキュリティ対策の負荷低減
- サイバー人材の育成と有効活用
- リスク検知の迅速化

●その他
- セキュリティ対策費用の圧縮
- ZTA導入に必要なコンポーネントの構築

米国CDMプログラムの概要

●CDM（Continuous Diagnostics and Mitigation）

- **Diagnostics**
  理想状態と現状状態の**ギャップやリスクを可視化**
- **Mitigation**
  可視化された**ギャップやリスクへ対応**
- **Continuous**
  ギャップやリスクを可視化し、対応を**継続的に実施**

●米国におけるCDMプログラムの位置づけ

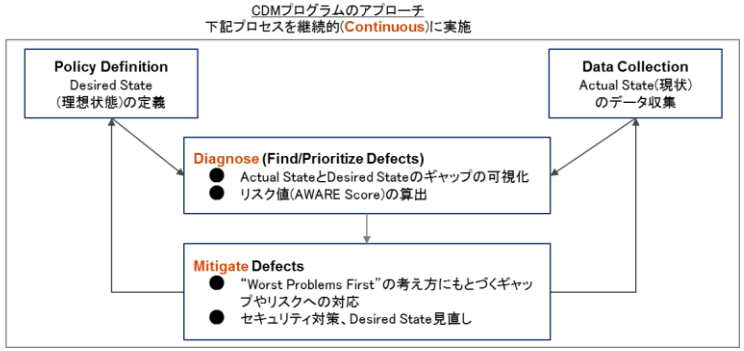
- 連邦政府機関の情報システムに関する**管理状況をほぼリアルタイムに報告**する仕組み
- 従来から各機関は、FISMA（連邦情報セキュリティ管理法）に基づき定期的に報告書を提出している
- DHS（Department of Homeland Security）及びOMB（Office of Management and Budget）がプログラムを推進。なお、小規模組織向けのCDMのシェアサービスは、GSA（General Services Administration）で提供
- **ゼロトラストの導入を促進するプロジェクト**と位置付けられており、2022年1月26日にOMBから発出された覚書においても、各機関に対してCDMプログラムに参加するための計画を立てることが指示されている

●CDMの管理対象

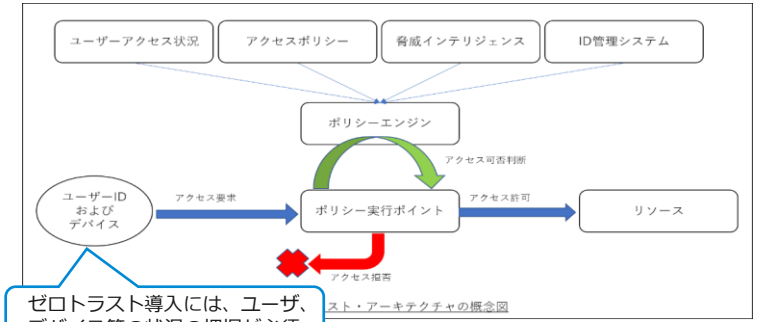
- **IT資産（デバイス、ソフトウェア等）**、**ユーザ**、ネットワークセキュリティ、データ保護を管理対象としている

※2020年時点では、主に資産管理、ユーザ管理が行われている。ネットワークセキュリティ、データ保護管理は順次構築中

CDMの基本概念



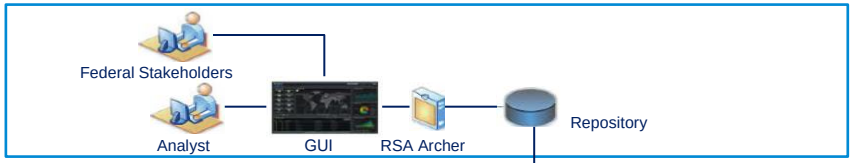
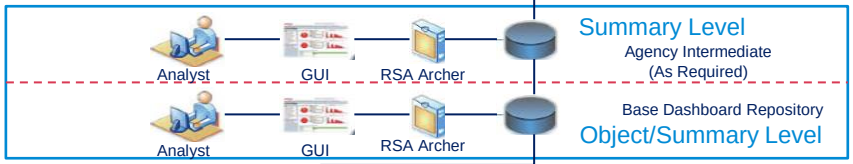
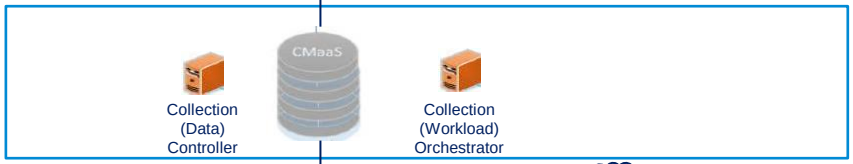
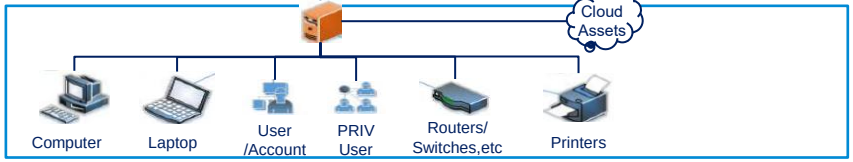
（参考）ゼロトラスト・アーキテクチャーの概念図



米国CDMについて

米国CDMの全体アーキテクチャ

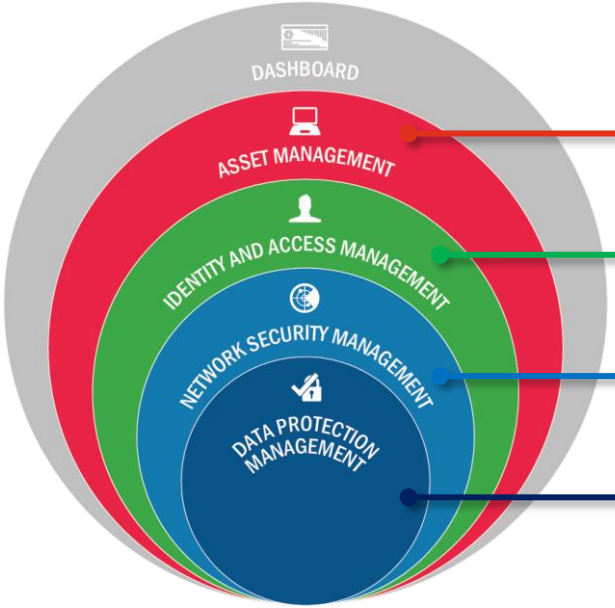
米国CDMのアーキテクチャは、下図のLayer A-Dの4つのレイヤーから構成される。

レイヤー	概念図	説明
Layer D Federal Dashboard		Agencyダッシュボードからサマリ情報を取得し表示する。 新たな脅威を特定した場合など、必要な場合はAgencyダッシュボードにリスクスコア算出のためのパラメータを送信する。
Layer C Agency Dashboard		レイヤーBを介して、各Agencyのオブジェクトレベルのデータを取得し表示する。”Desired State”と”Actual State”の比較を表示し、リスクの特定と改善アクションの優先順位付けを行う。 各AgencyにおけるFederal ダッシュボードとの唯一の接点となる。
Layer B CMaaS Integration		レイヤーAから収集したデータの集約、統合、正規化を行い、CMaaSソリューションの自動化・運用上の制御ポイントとなる。 拡張や地政学的なニーズに応じた水平・垂直統合への対応が必要となる。また、レイヤーBの各インスタンスはレイヤーCに採用されているトポロジーに合わせる必要がある。
Layer A Tools & Sensors		最下位で最も多様なレイヤーであり、各Agencyのハードウェアおよびソフトウェアと相互作用するツールとセンサーによりデータ収集を行う。レイヤーAは多岐にわたるツールで構成され高度に分散されており、基本的に一元化されることはない。

※CMaaS : Continuous Monitoring as a Service

米国CDMについて

米国CDMプログラムの管理領域



CDMプログラムの管理領域

領域 1
資産管理
ネットワークに繋がっているものは何か？

- ハードウェア資産管理
- ソフトウェア資産管理
- 構成・設定管理
- 脆弱性管理
- エンタープライズモバイル管理

領域 2
アイデンティティとアクセス管理
ネットワークを利用しているのは誰か？

- アクセス権限・信頼レベル管理
- ユーザ教育・行動管理
- 資格情報・認証管理
- 特権管理

領域 3
ネットワークセキュリティ管理
ネットワーク上で何が起きているか？
ネットワークは守られているか？

- ネットワーク保護
- セキュリティイベント管理
- 運用・監視・改善
- セキュリティに配慮した設計・開発

領域 4
データ保護管理
データは守られているか？

- データ検出・分類
- データ保護
- データ漏えい防止
- データ侵害・流出対応・緩和
- データ操作制御

領域１より順次、診断領域を深化させ、
脆弱な領域を極小化するための能力向上を図る。

米国CDMについて

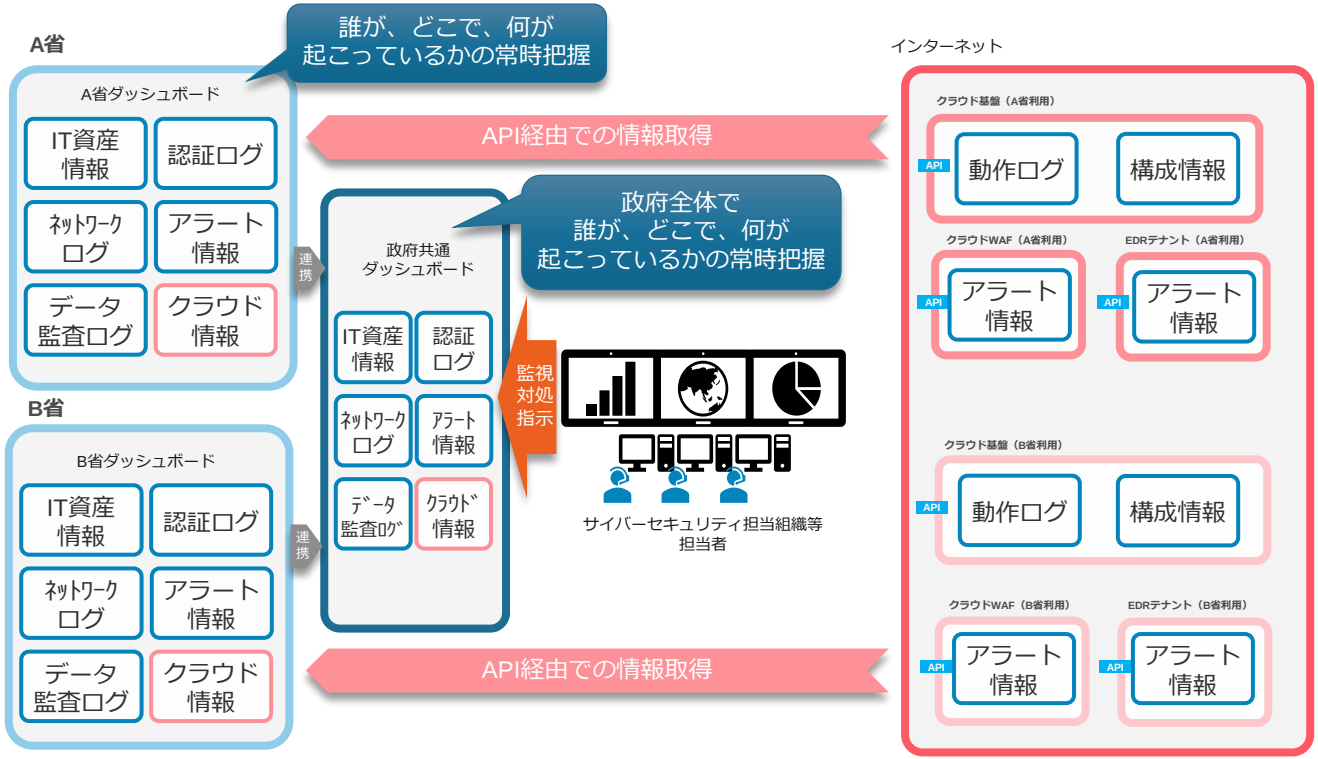
リスクスコア（AWARE）について

- AWARE（Agency-wide Adaptive Risk Enumeration）は、米国CDMにおけるリスクスコアリングの方法論であり、”Worst Problem First” の考え方にもとづき、サイバーリスクについての状況認識や脅威と脆弱性のタイムリーな緩和を可能にする。
- AWAREの各リスクスコアは、主に資産管理領域にて収集するデータにもとづき算出される。

Agency-wide Adaptive Risk Enumeration (AWARE)	「欠陥の種類」、「欠陥の内在期間」、「欠陥が発見されたシステムの重要度」、「その他の重要な要因」を考慮し、リスクスコアを算出することでセキュリティ態勢の状況を表す。算出されたスコアから優先順位付けを行い、セキュリティ上の問題をタイムリーに解決することを可能にする。
ソフトウェア脆弱性（VUL）	アセット管理中に脆弱性スキャンツールによってネットワークエンドポイント上で識別された個々の共通脆弱性識別子（CVE）に基づいて算出されるスコア。
構成設定管理（CSM）	CSMツールによって実施されるCSMチェックに失敗した欠陥は、深刻度に基づいて、共通脆弱性スコアリングシステム（CVSS）スケール内のスケーリングされた値を割り当てることによってスコア化される。
未承認機器管理（UAH）	UAHは、所有権が割り当てられていないハードウェア・デバイスを表す。所有権が割り当てられていない資産は、ハードウェア資産管理ツールを使用して発見される。

日本版CDM（CRSAアーキテクチャ）の導入について

常時診断を実現する日本ToBeモデル概要（現状案）

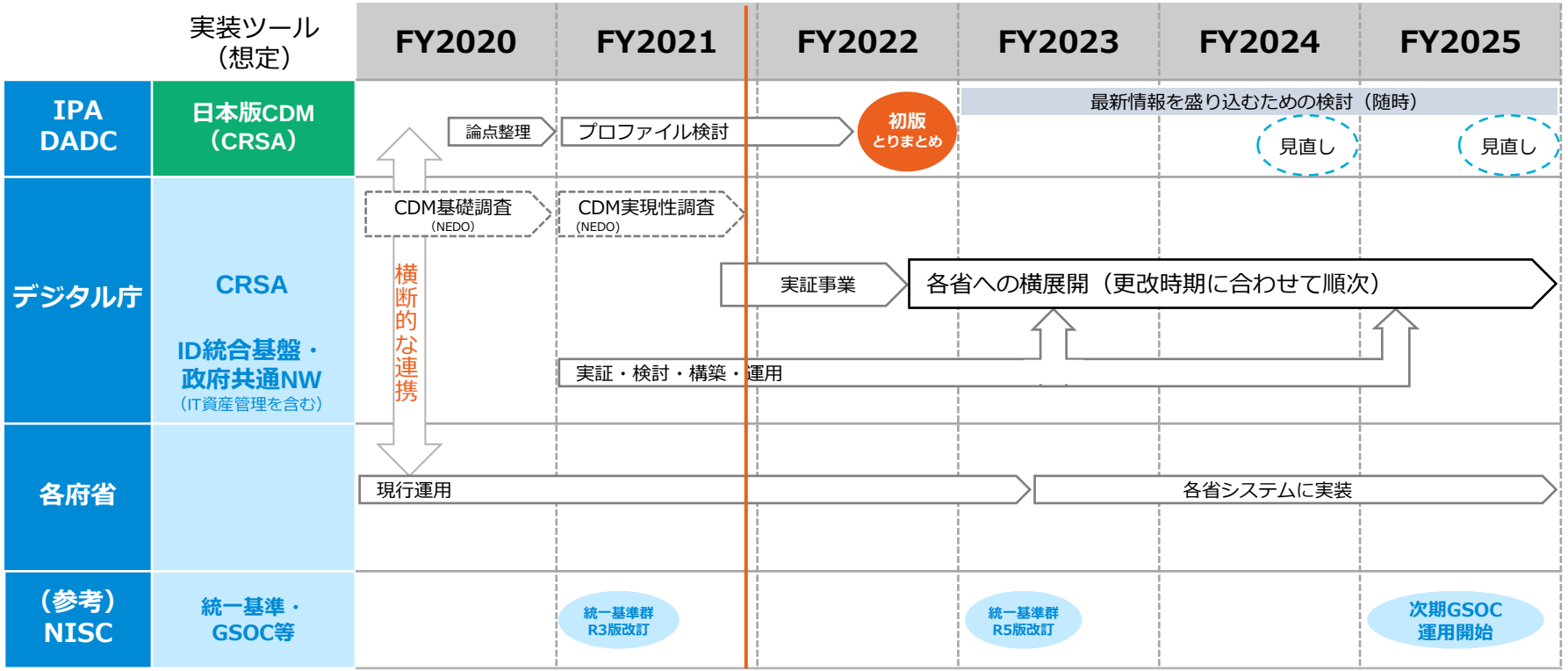


Continuous Risk Scoring and Action（CRSA）アーキテクチャ

政府全体で各種データを収集することにより
継続的にリスクを可視化し、その変化に対処する

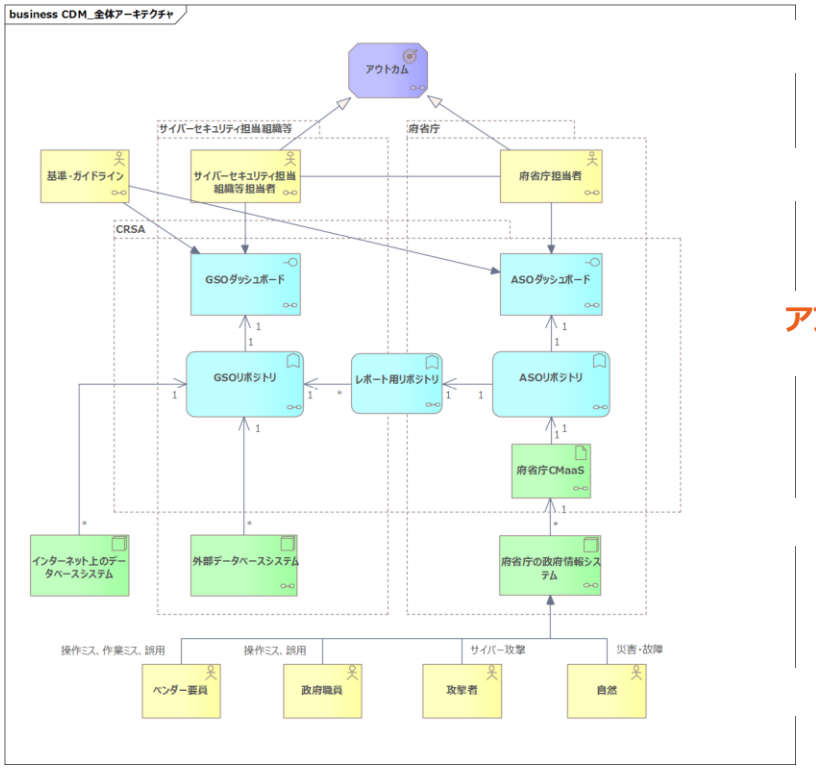
日本版CDM（CRSAアーキテクチャ）の導入について

検討プロジェクトの全体スケジュール（想定）



日本版CDM（CRSAアーキテクチャ）の導入について

CRSAアーキテクチャ全体概要図



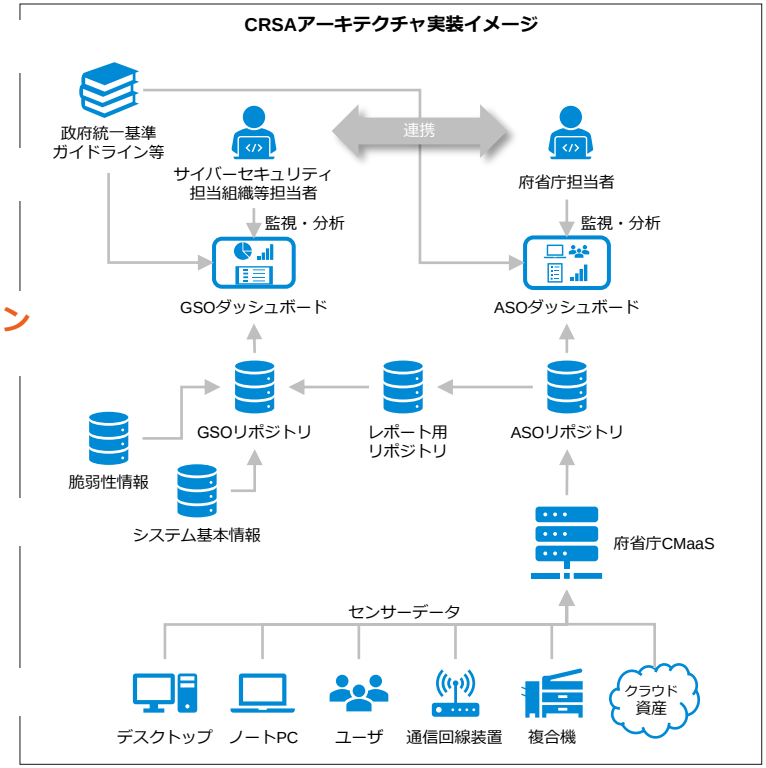
ガバナンスレイヤ

業務レイヤ

アプリケーションレイヤ

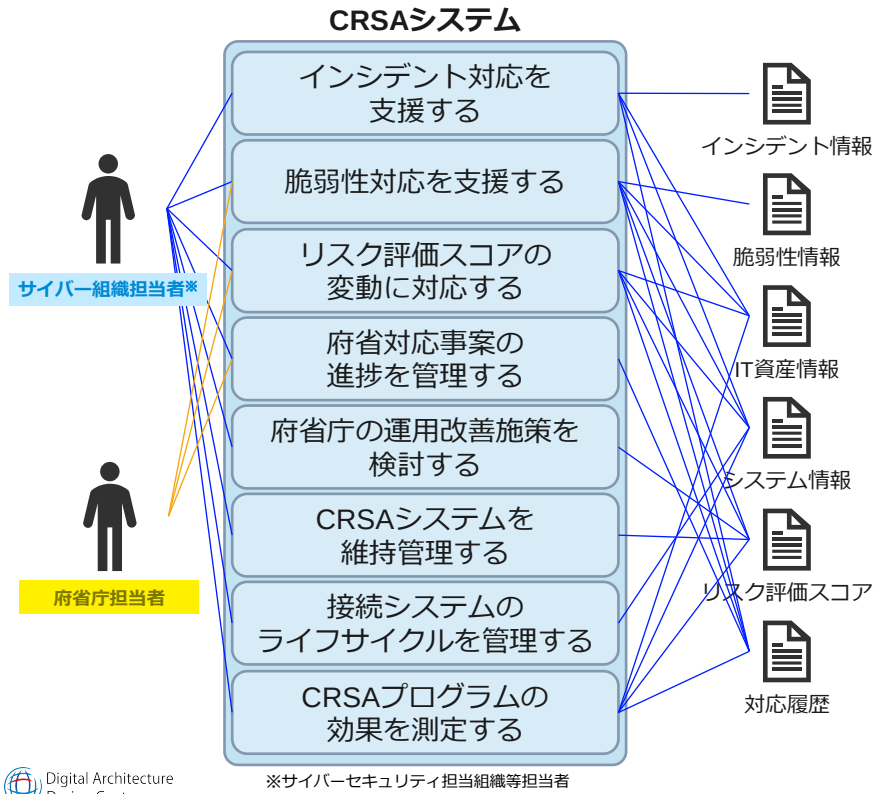
技術レイヤ

関係要素



日本版CDM（CRSAアーキテクチャ）の導入について

CRSAシステムのユースケース（案）



- **インシデント対応支援** サイバー組織担当者
  府省庁におけるインシデント発生状況を随時把握し、インシデントに係るソフトウェアやデバイスの情報をサイバーセキュリティ担当組織等に提供することにより、政府横断的なインシデント対応の支援を行う
- **脆弱性対応支援** サイバー組織担当者 府省庁担当者
  脆弱性情報の政府マスター情報（脆弱性辞書）を維持管理するとともに、新たな脆弱性情報や政府組織における脆弱性対応状況を随時把握し、府省庁担当者への情報提供等により脆弱性対応を支援する
- **リスク評価スコア変動対応** サイバー組織担当者 府省庁担当者
  リスク評価スコア変動の原因を分析し、必要に応じて各組織への状況確認や対応支援を行う
- **進捗管理** サイバー組織担当者 府省庁担当者
  サイバーセキュリティ担当組織等担当者の業務に係る府省庁担当者とのやり取りについて、進捗管理を行う
- **運用改善施策の検討**
  リスクスコア変動や対応状況の傾向から、府省庁におけるセキュリティ運用の状況、改善施策の効果等を分析・評価し、政府横断的な対応施策を検討する

- **CRSAシステムの維持管理**
- **接続システムのライフサイクル管理**
- **CRSAプログラムの効果測定**

サイバー組織担当者

日本版CDM（CRSAアーキテクチャ）の導入について

CRSAダッシュボードのトップ画面イメージ

GSOダッシュボードトップ画面の表示項目（概要）

- **脆弱性に関する情報**
  - 脆弱性件数（緊急・新規・更新）
  - 長期間未対応の脆弱性件数
- **リスク評価スコア変動に関する情報**
  - スコア変動のあった件数
  - 政府全体のリスク評価スコアの最新値
  - 政府全体のリスク評価スコアの推移
- **進捗管理（チケット）に関する情報**
  - 新規・更新チケット件数
  - チケット一覧
- **政府内の資産管理情報**
  - 政府全体の情報システム数、デバイス数
  - デバイスのOSバージョン分布
- **インシデントに関する情報**
  - 新規に発生したインシデント件数
  - 対応状況が更新されたインシデント件数
  - 政府内で発生したインシデント一覧

※表示されている情報は実際のものではありません。

日本版CDM（CRSAアーキテクチャ）の導入について

ご意見をいただきたい論点

- **日本版CDMが担う役割について**
  日本版CDM導入によるアウトカム、ユースケースの過不足等
- **日本版CDMにおける管理対象について**
  ４つの管理領域についての妥当性、他に検討すべき領域や観点等
- **日本版CDMの導入について**
  導入にあたっての留意点、検討の方向性等

次回のテーマについて

アジェンダ（予定）

- **システムの実装や拡張に関する検討方針について**
  対象システムやデバイスの拡張等における課題等について
- **リスク評価スコアの拡張について**
  脆弱性、構成、デバイス管理以外のスコア化候補について
- **政府マスター情報の必要性について**
  脆弱性情報、システムやクラウドのセキュリティ構成等の
  マスター情報を政府として管理する必要性や課題について

（参考）今後のアーキテクチャ検討について

システムの拡張に関する検討方針（案）

No	検討項目	検討方針
1	**参加組織**	参加する府省庁、およびこれらの所管法人等への拡張を検討する
2	**対象システム種別**	府省庁の基盤システムをはじめとして、個別の業務システム等、システムの特性等に応じてシステムを分類し、常時診断の対象とするシステムの拡張を検討する
3	**対象デバイス種別**	常時診断の対象とするデバイスをPC端末から、サーバ機器、通信回線装置、その他機器（複合機やIoT機器等）への拡張を検討する
4	**システム構成**	大規模府省においては、部局組織等が独立してシステムを開発・運用している場合があるため、ダッシュボードやCMaaS等の多段構成について検討する
5	**ダッシュボード**	政府統一基準やガイドラインの更新等の外部環境の変化に応じて、ダッシュボードに表示する項目やスコア化項目の拡張を検討する
6	**業務内容**	ダッシュボードの拡張や外部環境の変化に応じて、当システムに係る担当者の業務拡張を検討する

（参考）今後のアーキテクチャ検討について

リスク評価スコアの拡張（案）

対象領域 CDM	対象領域 CRSA	基本スコア 名称	評価内容	基本値	経過時間に係る 係数	重み付けに係る 係数	スコア概要
領域 1	端末とサーバ装置等の管理	VUL	ソフトウェア脆弱性の対応状況	Scaled Base CVSS (0.0～10.0)	脆弱性公開日からの経過日数	・システムの重要度 ・脅威情報	デバイスにおける未対応の脆弱性をスコア化
		CSM	構成の規定準拠状況	Scaled STIG Cat. (0.12～0.72)	–	・システムの重要度	ソフトウェアにおける構成誤りについてスコア化
		UAH	デバイスの管理状況	10	–	–	未承認（非管理）デバイスの存在をスコア化
		UAS	ソフトウェアの管理状況	固定値	–	–	未承認ソフトウェアの存在をスコア化
		USS	ソフトウェアの署名状況	固定値	–	–	未署名ソフトウェアの存在をスコア化
領域 2	認証・認可・特権の管理	*UAU*	ユーザの管理状況	固定値	–	–	未承認（非管理）ユーザの存在をスコア化
		PPS	パスワードの管理状況	固定値	–	–	パスワード強度が低い特権アカウントの存在をスコア化
領域 3	情報システムのライフサイクル管理	*LSS*	ログ管理の状況	固定値	–	–	不適切なログの保管状況をスコア化
		EVT	不正アクセス等の発生状況	固定値	–	–	セキュリティアラートの発生状況の変化量をスコア化
領域 4	データの保全管理	*NPF*	情報の保護状況	固定値	–	–	要保護情報が適切に保護されていない状況をスコア化
		ETS	データ暗号化の状況	固定値	–	–	暗号化されていないデータ送信をスコア化

（参考）リファレンスURL一覧

●IPA - デジタルアーキテクチャ・デザインセンター
https://www.ipa.go.jp/dadc/

●CISA - CONTINUOUS DIAGNOSTICS AND MITIGATION (CDM)
https://www.cisa.gov/cdm

●CISA - CDM Program Overview fact sheet
https://www.cisa.gov/sites/default/files/publications/cdm-program-overview-fact-sheet-012022-508.pdf

●CISA - CDM Program‘s Dashboard Ecosystem fact sheet
https://www.cisa.gov/sites/default/files/publications/cdm-program-dashboard-ecosystem-fact-sheet-092020-508.pdf

●CISA - Agency-Wide Adaptive Risk Enumeration (AWARE)
https://www.cisa.gov/sites/default/files/publications/cdm-program-aware-scoring-fact-sheet-092020-508.pdf

●OFFICE OF MANAGEMENT AND BUDGET Memorandum (M-22-09)
https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

●NEDO - 2020年度成果報告書　Ｃｏｎｎｅｃｔｅｄ　Ｉｎｄｕｓｔｒｉｅｓ推進のための協調領域データ共有・ＡＩシステム開発促進事業/米国におけるＣＤＭ（Ｃｏｎｔｉｎｕｏｕｓ　Ｄｉａｇｎｏｓｔｉｃ　ａｎｄ　Ｍｉｔｉｇａｔｉｏｎ：継続的な診断とリスクの緩和）についての基礎調査（報告書番号：20210000000194）
https://www.nedo.go.jp/library/database_index.html

●NEDO - 「Connected Industries推進のための協調領域データ共有・AIシステム開発促進事業／米国政府のCDM Programを参考にした常時診断システムの実現性調査」に係る実施体制の決定について
https://www.nedo.go.jp/koubo/IT3_100190.html

●デジタル庁 - デジタル社会の実現に向けた重点計画
https://www.digital.go.jp/policies/priority-policy-program

●デジタル庁 - 国等の情報システムの統括・監理（情報システムの整備及び管理の基本的な方針）
https://www.digital.go.jp/policies/posts/development_management