参考資料2

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

2021 年 3 月

国立研究開発法人新エネルギー・産業技術総合開発機構

委託先　　ＰｗＣコンサルティング合同会社

目次

1. 研究開発の成果と達成状況

1.1. 和文要約

近年、サイバー攻撃が多発しており、情報資産の適切なマネジメントが必要となっている。従前から検討されてきた危機管理体制下の事業継続や働き方改革に加え、コロナウイルス感染症の影響もあり、クラウドサービスの利用やリモートワークが急速に普及する中で、従来型のオンプレミス型を前提とした情報システムの境界監視及びインシデントレスポンス体制では、セキュリティポリシーの適切な運用及びアップグレード、迅速なサイバーインシデント発生時の対応が極めて困難となることが予想される。

このような状況において、情報資産を確実にサイバー攻撃から守り、着実に事業を継続していく観点から、常時アクセス判断・許可（通称：ゼロトラスト）のコンセプトに基づいた、常時診断システムを構築する重要性が高まっている。また、従来の枠を超えて各企業の連携が進む Connected Industries の実現に向けても、各企業においてこのようなシステムの構築を進めることは連携を更に促進する上で重要であり、加えて、企業横断的なプラットフォーム開発を行う上でも、その前提として今後どのようなシステム構成になるか、その潮流を把握しておくことは、拡張性・対応性を担保する上で重要である。

このような背景から、本事業では政府システムに対して常時診断システムを導入することを目的に、米国政府の常時診断・リスク緩和プログラム（Continuous Diagnostics & Mitigation (CDM) Program）についての基礎的な内容調査及び常時診断システムの試験研究を行うための事前準備の検討を行った。

1.1.1. 米国 CDM プログラムについての内容調査

常時診断システムのアーキテクチャ及びシステム仕様についての検討項目を整理すべく、文献調査を実施し、組織・体制、システム構成、各種要求事項、関連ガイドライン・フレームワーク、進行状況・課題などについて整理した。加えて、有識者へのインタビューによる調査を実施し、文献調査で確認した内容の詳細や CDM プログラム運用の実態についてまとめた。

1.1.2. 常時診断システムの試験研究のための事前準備

上記の調査結果に基づき、政府システムに対しての常時診断システムの試験研究を実施するにあたり、試験目的、スコープ、試験項目、システム構成、ツールに求める機能などについての検討を行い、仕様としてとりまとめた。

1.2. Summary

In recent years, cyber-attacks have become more prevalent and appropriate management of information assets has become more needed. In addition to the business continuity under the crisis management system and work style reforms that have been considered for some time, the use of cloud services and remote work is rapidly spreading due to the influence of coronavirus infections. It is expected that it will become extremely difficult to properly operate and upgrade security policies and to respond quickly to cyber incidents with existing boundary monitoring and incident response specific for on-premise systems.

Under such circumstances, it is becoming more and more important to build continuous monitoring and diagnostic system based on the concept of ongoing assessment and authorization of access (zero trust) from the perspective of reliably protecting information assets from cyber-attacks and steadily continuing business operations. In addition, as we move toward the realization of Connected Industries, where companies will collaborate with each other beyond the conventional boundaries, it is important for each company to build such a system in order to further promote collaboration. In addition, when developing a cross-enterprise platform, it is important to understand what kind of system structure could be in the future in order to ensure scalability and responsiveness.

With this background, this project aims to implement a continuous diagnostic system to government systems. Then we conducted a research for Continuous Diagnostics & Mitigation (CDM) Program of the U.S. government and made preparation for the pilot study of the continuous diagnosis system.

1.2.1. Research of the CDM program in the U.S.

In order to consider the architecture and system specifications of the continuous diagnostic system, we conducted a literature research and summarized the organization and structure, system configuration, various requirements, related guidelines and frameworks, and progress and issues. In addition, interviews with experts were conducted to summarize the details of the literature review and the actual status of CDM program operation.

1.2.2. Preliminary preparations for the pilot study of the continuous diagnosis system

Based on the results of the above research, we discussed the purpose, scope, test items, system configuration, and required functions of the tool, and compiled the specifications for the test and research of continuous diagnostic system for government systems.

2. 調査概要

2.1. 調査目的

本調査では、米国で推進されている CDM プログラムに関する組織・体制、システム構成、各種要求事項、関連ガイドライン・フレームワーク、進行状況・課題などについて情報収集及び整理を行い、政府システムに対する常時診断システムのアーキテクチャ及びシステム仕様の検討及び試験研究の事前準備を進める行う上でのポイントや課題を把握する事を目的とする。

2.2. 調査内容

本調査では、政府システムに対する常時診断システムのアーキテクチャ及びシステム仕様の検討及び試験研究の事前準備を進める行う上で必要となる情報を調査項目とした。

#	調査項目	説明
1	プログラム概要	・ プログラムの目的・定義 ・ 各フェーズ/Capability のコンセプト・概要
2	ガバナンス体制	・ 組織的・人的な役割・責任範囲
3	関連する指令及びガイドライン・フレームワーク	・ CDM プログラムに関連する指令やガイドライン ・ CDM の要求事項と各種フレームワークのマッピングなど
4	システムアーキテクチャ	・ CDM を実現するシステム構成、連携方式
5	詳細要求	・ 各フェーズにおける機能面・運用面等における要求事項 ・ Federal と Agent の監視内容の棲み分けなど
6	調達戦略	・ CDM プログラムに準拠する製品を調達するための戦略
7	技術的実装	・ データ収集、センサー/ツール配置、監視ポイント、製品とダッシュボード連携などの実装方式 ・ 各フェーズにおける代表的製品やサービス
8	進行状況	・ 適用対象の政府機関の拡大やフェーズの進行状況 ・ 実施する中での課題や改善状況など

2.3. 調査方法

本調査は、以下の文献調査とインタビュー調査を実施する。

① 文献調査

文献調査については、以下のような媒体を対象に情報収集を実施した。

- 米国政府機関の公式 HP、公開文書
- 米国政府系メディアサイト
- 企業（主にセキュリティベンダー）の公式 HP、公開文書

② インタビュー調査

インタビュー調査については文献調査を踏まえた上で、文献調査で確認した内容の詳細及び文献調査では確認できなかった内容などをもとにインタビュー項目を作成し、米国政府機関向けの業務従事経験者をインタビュー対象の有識者として選定し、ビデオ会議形式によるインタビューを実施した。

2.4. 調査結果を踏まえた試験研究準備

本調査を踏まえ、政府システムに対しての「常時診断システム」の実装のために必要な試験研究の事前準備として、政府及び独立行政法人情報処理推進機構と議論・連携の上、以下の作業を実施し、常時診断システムの試験研究に係る検討を行った。

① スコープ定義

CDM のアプローチである「Policy Definition」、「Data Collection」、「Diagnose」、「Mitigate Defects」のうち試験のメイン項目とするアプローチを定義し、実機試験の対象を整理した。

② 計画の策定

試験研究で実施すべき作業内容を整理しスケジュール案を作成した。

③ システム仕様の作成

試験研究で必要となる環境の全体概要、Federal Dashboard、Agency Dashboard、CMaaS、Sensor 等の仕様を整理した。

④ 導入候補製品およびサービスのリストアップ

試験研究で必要となる Federal Dashboard、Agency Dashboard、CMaaS、Sensor 等の機能要件及び米国で導入されている製品事例を整理した。

⑤ 試験研究 サイトにおける必要な運用体制の提案

試験研究で必要となる各 Dashboard の表示項目に関して整理した。

3. CDM プログラム概要

3.1. 基本概念

3.1.1. 背景

- 2001 年 9 月 11 日のテロ以降、米国政府は様々なセキュリティ強化の取組を行う中で 2002 年に連邦情報セキュリティマネジメント法(FISMA : Federal Information Security Management Act of 2002)を策定し、連邦政府機関の情報セキュリティの強化を義務付け、アメリカ国立標準技術研究所(NIST : National Institute of Standards and Technology)に対してはそのための規格やガイドラインの開発を義務付けた。
- NIST では、FISMA の規定を受けて、FISMA 導入プロジェクトを立ち上げ、FISMA リスクマネジメントフレームワークという、情報セキュリティを継続的に改善・向上させる枠組みや多くの規格、ガイドラインを開発した。
- 一方、近年ではサイバーセキュリティへの脅威は日進月歩で進化しており、スナップショットアプローチによる年次ベースでの評価及び報告では不十分となってきている。
- 2013 年、日々進化する脅威に対するサイバーセキュリティへの対応策として、継続的かつ動的なアプローチを導入した CDM プログラムが設立された。

3.1.2. 目的

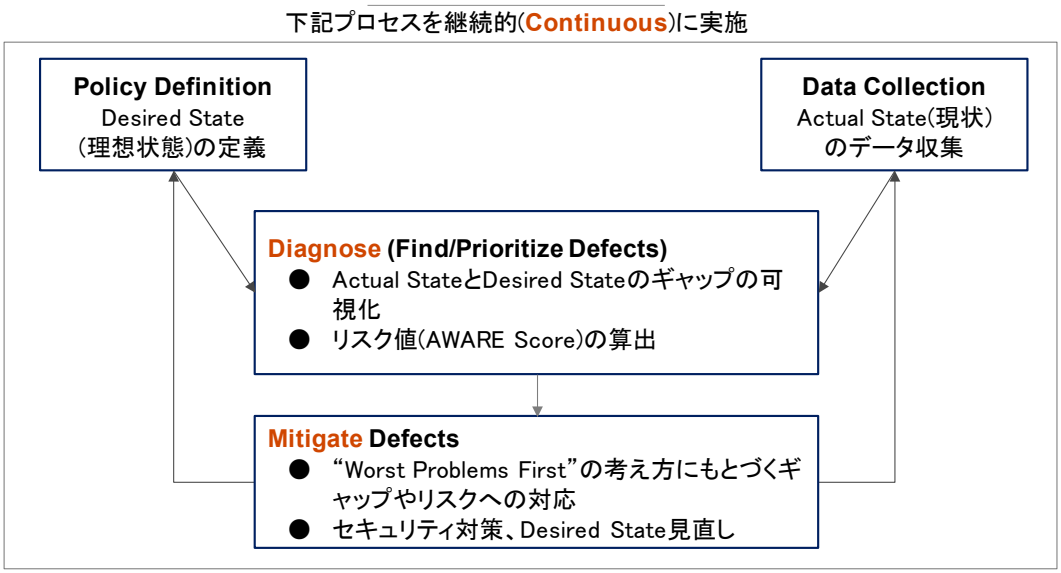
CDM プログラムでは、下記の 4 点を目的として、政府機関が継続的にサイバーセキュリティ態勢を強化・向上させる上で必要なツール、サービス及びダッシュボードの提供を行う。

Reduce	:	組織の攻撃対象領域の低減
Increase	:	連邦政府のサイバーセキュリティ態勢の可視性の向上
Improve	:	連邦サイバーセキュリティ対応力の向上
Streamline	:	FISMA 実施状況報告の効率化

3.1.3. アプローチ

CDM プログラムでは、継続的(Continuous)に政府機関のシステム及びネットワークに関するデータをよりリアルタイムに近い形で自動的に収集し、理想とする状態とのギャップやリスクを診断(Diagnostics)し、優先順位をつけて緩和(Mitigation)しリスクを軽減していくことを基本的なアプローチとしている。

図表 1 CDM プログラムのアプローチ



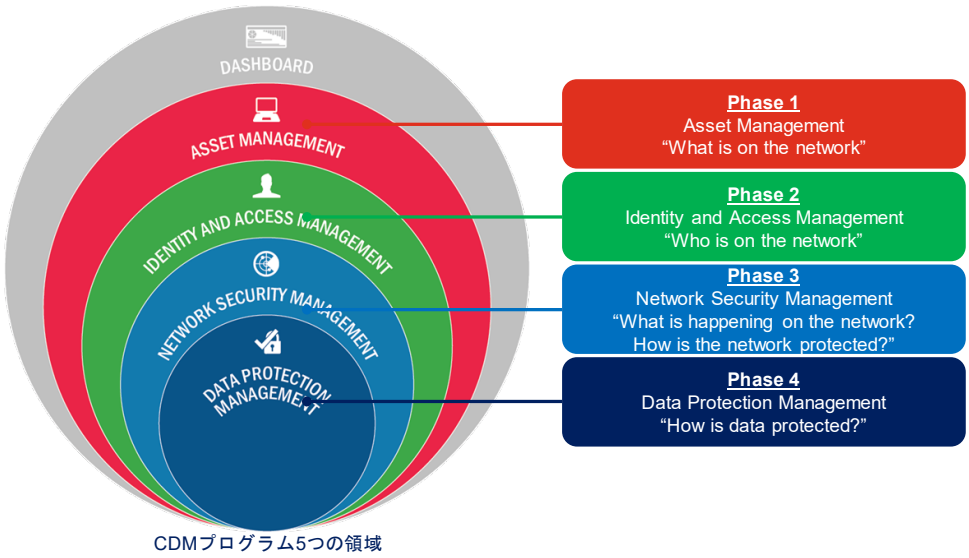
参考文献 7.HWAM Capability Description より転記

3.2. プログラム構成

CDM プログラムは、「図表 2 CDM プログラムの領域」のとおり、5 つの領域で構成されており、「ASSET MANAGEMENT」以下の 4 つが、順に実施すべき「Phase (フェーズ)※」として定義されている。

※参考文献 8 の最新の文書では、Phase が Capability Area に修正されている

図表 2 CDM プログラムの領域



参考文献 8.CDM Technical Capabilities Volume Two Requirements Catalog 2020 より転記

3.3. 各 Phase の概要

各 Phase の概要は「図表 3 各 Phase の概要」のとおり。

図表 3 各 Phase の概要

フェーズ		概要
Phase 1	Asset Management	**ネットワーク上に何があるのか？** デバイスの識別と監視に焦点を当て、デバイスが適切に構成され、脆弱性が識別されて修正されていることを確認する。
Phase 2	Identity And Access Management	**ネットワーク上に誰がいるのか？** ユーザーの識別に重点を置いており、ユーザーが適切に識別、精査、トレーニング、および認証されていることを確認する。
Phase 3	Network Security Management	**ネットワーク上で何が起こっているのか？ネットワークがどのように保護されているのか？** Phase1およびPhase2を土台に成り立っており、ネットワークや境界上のコンポーネント、ホストとデバイス、保存中と転送中のデータ、ユーザーの行動とアクティビティ等の領域を対象として、セキュリティの対策の広範囲かつ動的な監視を行う。また、インシデントへの備えや対応、ソフトウェアやシステム品質の確認、内部的な行動・振る舞い検知を通じて誰が何をしているのかを判断を行い、これらを通じてセキュリティインシデントを軽減してネットワーク/インフラストラクチャ全体への影響をを防止する。
Phase 4	Data Protection Management	**データがどのように保護されているのか？** 機密（特にプライバシー）データの保護に焦点を当てている。データ資産の機密性、整合性、および可用性を確保するため、許可されたアクセス権限及び目的のみに使用されるよう、保管中、使用中、および転送中のセキュリティとプライバシー両面でのデータ保護プロセスについてポリシーの確立や管理などを対象としている。

参考文献 1.Securing Federal Networks より転記

3.4. Capability 概要

各 Phase では、「図表 4 Capability 一覧」のとおり、実装すべき Capability が定義されている。

図表 4 Capability 一覧

フェーズ		Capability		
		略称	名称(EN)	名称(JP)
Phase 1	Asset Management	HWAM	Hardware Asset Management	ハードウェア資産管理
		SWAM	Software Asset Management	ソフトウェア資産管理
		CSM	Security Configuration Settings Management	構成・設定管理
		VUL	Vulnerability Management	脆弱性管理
		EMM	Enterprise Mobility Management	エンタープライズモバイル管理
Phase 2	Identity And Access Management	TRUST	-	アクセス権限・信頼レベル管理
		BEHAVE	-	ユーザ教育・行動管理
		CRED	-	資格情報・認証管理
		PRIV	-	特権管理
Phase 3	Network Security Management	BOUND	-	ネットワーク保護
		MNGEVT	Manage Events	セキュリティイベント管理
		OMI	Operate, Monitor and Improve	運用・監視・改善
		DBS	Design and Build in Security	セキュリティに配慮した設計・開発
Phase 4	Data Protection Management	DATA_DISCOV	Data Discovery/Classification	データ検出・分類
		DATA_PROT	Data Protection	データ保護
		DATA_DLP	Data Loss Prevention	データ漏えい防止
		DATA_SPIL	Data Breach/Spillage Mitigation	データ侵害・流出対応・緩和
		DATA_IRM	Information Rights Management	データ操作制御

参考文献 1.Securing Federal Networks より転記

3.4.1. Asset Management の Capability

Asset Management に必要な Capability は、「図表 5 Asset Management の Capability」のとおり。

図表 5 Asset Management の Capability

Capability		説明
Phase 1 Asset Management	HWAM (ハードウェア資産管理)	**ネットワーク上のIPアドレスを設定可能なデバイスを管理する** ・ ネットワークに接続する新しいデバイスを検出する ・ 実際に存在するすべてのデバイスを特定する ・ 許可されていないハードウェアがデータの漏えいに使用されるのを防ぐ など
	SWAM (ソフトウェア資産管理)	**ネットワーク上のデバイスにインストールされているソフトウェアを検出して管理する** ・ ネットワークに接続されたデバイス/システムにインストールされているソフトウェアを可視化する ・ ソフトウェア製品と実行可能ファイルに安全でない構成と古いパッチがあるか検出する ・ ソフトウェアのインストールを制限することにより、デバイスの侵害を停止または遅延させる など
	CSM (構成・設定管理)	**ネットワーク上のデバイス及びソフトウェアのセキュリティ構成・設定を識別して管理する** ・ 組織内の資産の構成や設定情報を追跡および管理する ・ ソフトウェアが悪意のある、または不正な形式の入力を実行または処理するのを防止または最小限に抑える ・ 設定ミスによるデバイスの侵害を停止または遅延させる など
	VUL (脆弱性管理)	**ネットワーク上のデバイスにインストールされているソフトウェアの脆弱性を検出して修正をサポートする** ・ 脆弱なソフトウェアが原因で、侵害されやすいデバイスの数を減らす ・ 脆弱なソフトウェアがネットワークの他の部分へのアクセス、特権の拡張や昇格、またはデータの漏えいに使用されるのを遅らせる、または防止する など
	EMM (エンタープライズモバイル管理)	**政府機関のポリシーに従って、モバイル端末の使用を保護する** ・ ソフトウェアのインストールと管理 ・ エンタープライズアクセスのデバイスコンプライアンス ・ センサー（カメラ、マイクなど）へのアクセス制御 ・ 暗号化と復号 など

参考文献 8.CDM Technical Capabilities Volume Two Requirements Catalog 2020

3.4.2. Identity and Access Management の Capability

Identity and Access Management に必要な Capability は、「図表 6 Identity and Access Management の Capability」のとおり。

図表 6 Identity and Access Management の Capability

Capability		説明
Phase 2 Identity And Access Management	TRUST (アクセス権限・信頼レベル管理)	**アクセスを許可された人の信頼を管理する** ユーザーに適切な、権限とセキュリティロールを設定することで、データの可用性、整合性、および機密性が損われるリスクを軽減する。これは、政府機関のポリシーおよび法令に従って、設定・更新及び監視されることが要件に含まれる。
	BEHAVE (ユーザ教育・行動管理)	**セキュリティ関連の行動を管理する** 全てのユーザーが設定されたロールにあったトレーニングや認定を受けているかを管理する。十分なトレーニングを受けていないユーザーは、システムの破壊や機密データの公開などのリスクがあるため、適切なトレーニングの受講及び受講完了の報告を行う。
	CRED (資格情報・認証管理)	**資格情報と認証を管理する** システム、情報、設備にアクセスするための資格情報の管理や認証が適切に行われていることを確認することで、データの可用性、整合性、および機密性が損われるリスクを軽減する。 資格情報の管理や認証における不備やリスクについて、ユーザの属性情報や承認ステータス等を収集することで自動的に監視、レポーティング、優先順位づけを行う。
	PRIV (特権管理)	**特権を管理する** 物理的、論理的な特権が許可された人・アカウントに確実に割り当てられるように管理する。特権アカウントのアクセスを監視および測定し、過剰な特権や不要なアカウントを識別し、不必要な特権が、割り当てられないようにする。

参考文献 8.CDM Technical Capabilities Volume Two Requirements Catalog 2020

3.4.3. Network Security Management の Capability

Network Security Management に必要な Capability は、「図表 7 Network Security Management の Capability」のとおり。

図表 7 Network Security Management の Capability

Capability		説明
Phase 3 Network Security Management	BOUND (ネットワーク保護)	**ネットワークの保護** ネットワーク保護に関する管理を行う。 **BOUND-F** :ネットワークフィルターと境界制御 **NAC** :ネットワークへのアクセス制御 **BOUND-E** :暗号化メカニズムの制御を監視 ※NAC : Network Access Control
	MNGEVT (セキュリティイベント管理)	**セキュリティイベントの管理** セキュリティ脅威ベクトルの識別、セキュリティ違反イベントの検出、およびイベントの影響の分類を行う。 インシデント対応、プライバシー、緊急時対応計画、監査と説明責任、継続的な評価を行う。
	OMI (運用・監視・改善)	**運用、監視、改善** セキュリティの根本原因の詳細な分析、セキュリティ緩和の対応/回復の優先順位付け、通知、およびインシデント後の振り返り等のアクティビティを行う。 継続的な承認、システムと情報の完全性、リスクアセスメント、セキュリティの評価と承認を行う。
	DBS (セキュリティに配慮した設計・開発)	**セキュリティの設計と構築** システム開発ライフサイクルの各領域でセキュリティとプライバシーが確実に組み込まれるようにする。 設計領域では、セキュリティとプライバシーのニーズに対する動機と目標を特定する。 開発領域では、セキュリティとプライバシーのニーズが効果的に実装されていることを開発とテストで確認する。 展開領域では、セキュリティとプライバシーのニーズが満たされていることを確認し、運用中のセキュリティ制御の更新を維持する。

参考文献 8.CDM Technical Capabilities Volume Two Requirements Catalog 2020

3.4.4. Data Protection Management の Capability

Data Protection Management に必要な Capability は、「図表 8 Data Protection Management の Capability」のとおり。

図表 8 Data Protection Management の Capability

Capability		説明
Phase 4 Data Protection Management	DATA_ DISCOV (データ検出・分類)	**データの識別、発見、および分類** 組織全体のデータ資産の識別するために、次の機能が含まれる。 **自動データ検出**:プライバシーの対象となるデータ(ユーザー名、社会保障番号、住所など)を含む分類された列を検出し、出力する。 **データ分類**:システムデータに割り当てられる複数レベルの分類を作成し、データの使用を追跡したり、データへのユーザーアクセスを監視したり、データマスキングなどの保護機能を割り当てる。 **データのタグ付け**:データの識別と適切なデータ保護メカニズムの適用をサポートする。
	DATA_ PROT (データ保護)	**データ保護** データ自体を保護するために、以下の2つの方法に対応する。 **暗号化方式**:機密データを適切な復号キーでのみアクセスできる形式に変換することにより、機密性を保護する。 **データマスキングまたは難読化方式**:アプリケーション経由やデータベースのクエリーをかけて一連のデータを表示する際に、特に機密性の高い特定のデータ項目に関しては、許可されていないユーザに必要以上に実データをを見せることがないよう、マスキングや難読化を施した上で表示上わからなくする。
	DATA_ DLP (データ漏えい防止)	**データの損失の最小化** 組織外への機密データ(特にプライシー)の漏洩を防止するため、以下の機能がある。また、PIIなどの機密情報の保護を強化することも可能で、権限のないデバイスやメディア上にデータをコピーすることを制限する。 **マルチプラットフォーム機能/マルチデータベース機能、役割/属性ベースのデータ保護、漏えいアラートと防止、保護オーケストレーション**
	DATA_ SPIL (データ侵害・流出対応・緩和)	**データ侵害/流出への対応** 組織データの不正な損失に対応して組織が開発するポリシー、プロセス、および手順を指します。データ侵害や流出緩和機能を活用して、PII などの機密情報の保護を強化することもできる。 ・ 機密情報の許可された使用に関連した報告要件の遵守を支援する。 ・ インシデントや違反の報告管理をインシデント対応に統合する。 ・ インシデントおよび違反対応プロセスの自動化を強化する。 ・ プライバシーデータなどの機密情報に関わる異常行動の監視、検出、報告を改善する。 ・ プライバシーデータなどの機密情報を含む異常行動への対応を支援する。
	DATA_ IRM (データ操作制御)	**情報権利管理と特有のデータ保護** 企業情報(ドキュメント、ファイルなど)へのアクセスを制御する。IRMソリューションは一般的に以下を採用している。 ・ 暗号化-機密データは暗号化されているため、転送中または保存中の場所に関係なく機密性が維持される。 ・ 粒度制御-エンティティには、データへのアクセス権が付与される。(表示、レビュー、編集、印刷、コピー/貼り付け、画面キャプチャなど) ・ 識別-エンティティは、役割やグループメンバーシップに基づくポリシーを使用してアクセスが許可される前に認証される。

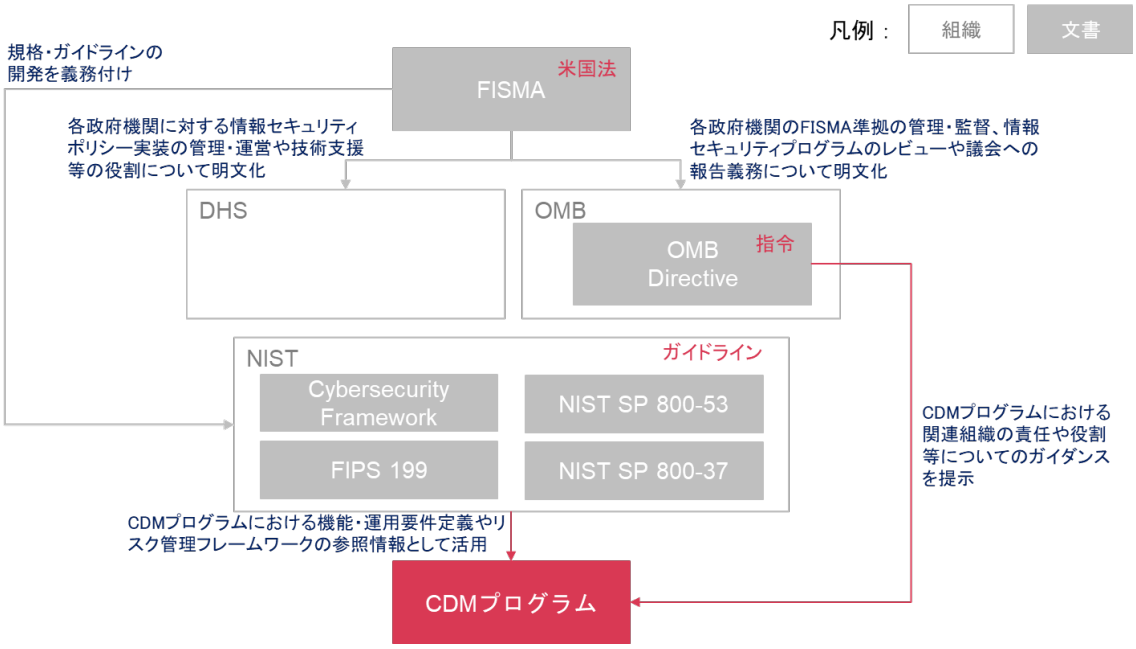
参考文献 8.CDM Technical Capabilities Volume Two Requirements Catalog 2020

4. ポリシー・ガイドライン

4.1. 関連するポリシー・ガイドラインとの関連性

CDM プログラムに関連する、ポリシー・ガイドラインとの関連性は「図表 9 ポリシー・ガイドラインとの関連性」のとおり。

図表 9 ポリシー・ガイドラインとの関連性



4.2. 関連するポリシー・ガイドラインの概要

関連するポリシー・ガイドラインの概要は「図表 10 関連するポリシー・ガイドラインの概要」のとおり。

図表 10 関連するポリシー・ガイドラインの概要

文書名	概要
FISMA	**連邦情報セキュリティマネジメント法** 連邦政府機関が情報セキュリティの強化および対策状況の報告を行うことを義務付け、NISTに対してはそのための規格やガイドラインの開発を義務付けた法律
OMB Directive	**アメリカ合衆国行政管理予算局からの指令** CDMに関しては、Federalダッシュボードの展開と運用、各Capability実現のためのツールやサービスの調達、リソースの割り当て(予算化、費用負担)などについて、DHSや各政府機関に対する責任範囲、役割、期待について記載
Cybersecurity Framework	**重要インフラのサイバーセキュリティを改善するためのフレームワーク** 重要インフラのサイバーセキュリティリスクマネジメントを改善することを目的として作成されたフレームワーク
SP 800-53	**連邦政府情報システムおよび連邦組織のためのセキュリティ管理策とプライバシー管理策** 組織全体の情報セキュリティをプライバシーリスクとともに管理する管理策。CDMプログラムにおける"Desired State"を定義する上で参照
SP 800-37	**連邦政府情報システムに対するリスクマネジメントフレームワーク適用ガイド：セキュリティライフサイクルによるアプローチ** セキュリティ分類、セキュリティ管理策の選択および実施、セキュリティ管理策のアセスメントなどの、リスクマネジメントフレームワークを連邦政府の情報システムに適用するためのガイドライン。CDMにおいても当フレームワークのリスクマネジメントのプロセスの考え方を参照
FIPS 199	**連邦政府の情報および情報システムに対するセキュリティ分類規格** 連邦政府の情報および情報システムの影響レベルを適切に分類し、影響レベルに応じたセキュリティ要求事項について記載した文書。CDMプログラムにて収集した資産の分類や重みづけを行う上で参照

4.3. Risk Management Framework との対応

Risk Management Framework (RMF)と CDM の対応は、「図表 11 RMF との対応」のとおり。

図表 11 RMF との対応

RMF Steps	Definition	CDM Defined Activity	CDM Capability
Step1	情報システムの分類 FIPS 199 / SP 800-60	CDM Agencyダッシュボード内の資産およびポリシーとの関係を含めるために、独自のFISMAコンテナ内に各Agency情報システムを確立する	-
Step2	セキュリティ管理策の選択 FIPS 200 / SP 800-53	FIPS 199 レーティングおよび機関ポリシーに基づく各 FISMA システムについて、NIST SP 800-53 コントロールを調整し、運用可能な CDM 機能に合わせて調整する	-
Step3	セキュリティ管理策の実装 SP 800-160	有効性の評価を自動化できるコントロールには、CDMが提供する機能を利用する	Ongoing Assessment (Phase3:MNGEVT)
Step4	セキュリティ管理策の評価 SP 800-53A	CDM統合システムの機能を活用して、影響を受ける各NIST SP 800-53コントロールに固有のDesiredStateに対して、ActualStateデータを集約して相関させることで、継続的に実施する	
Step5	情報システムの認可 SP 800-37	標準化された測定値を提供し、リスクアセスメントと承認事項を変更せざるを得ない事項を可視化する	Ongoing Authorization (Phase3:OMI)
Step6	セキュリティ管理策のモニタリング SP 800-137	リスクスコアリングによるシステムの状態の自動化と継続的な状況認識を、権限を持つ関係者やその他の関係者に提供する	-

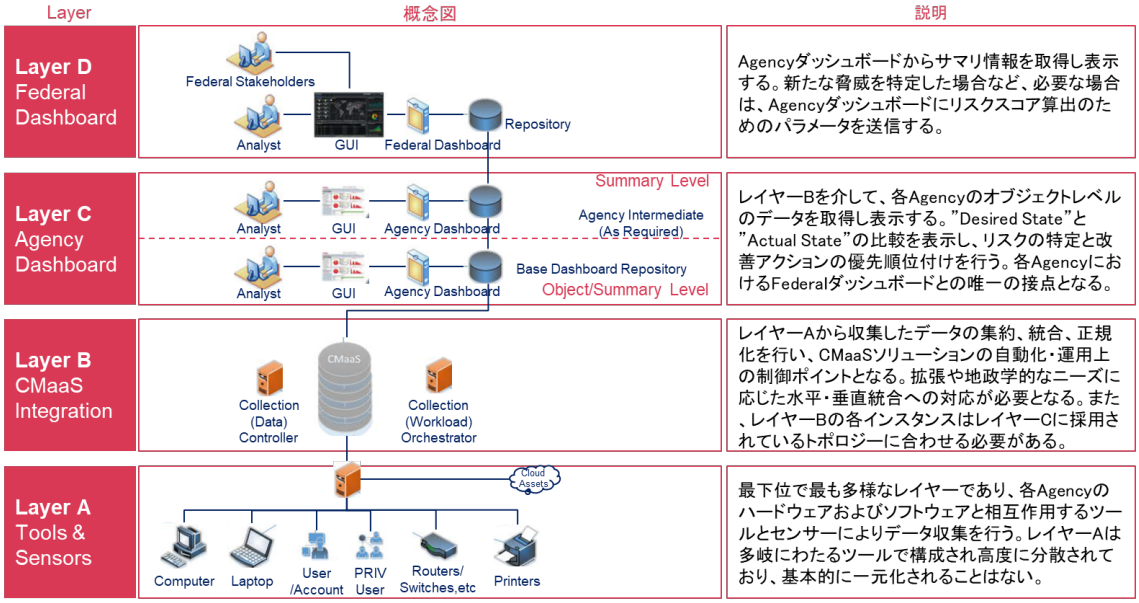
参考文献 8.CDM Technical Capabilities Volume Two Requirements Catalog 2020 より転記

5. システム

5.1. 全体アーキテクチャ

CDM プログラムは、Layer A-D の 4 レイヤーから構成される。各レイヤーの概念図と概要は「図表 12 CDM 全体アーキテクチャ」のとおり。

図表 12 CDM 全体アーキテクチャ

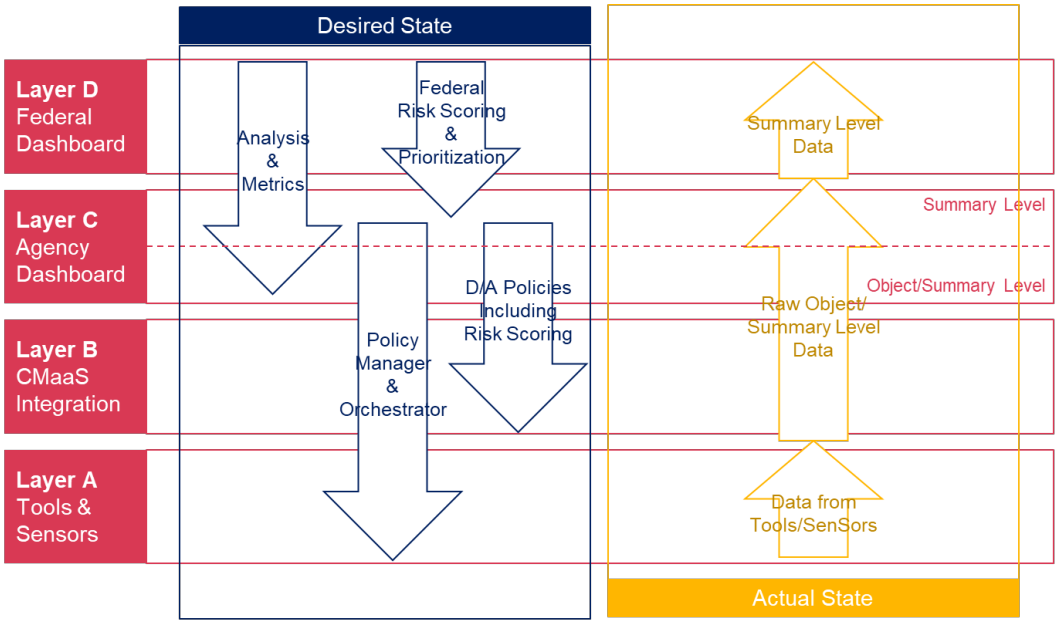


参考文献 9.CDM Technical Capabilities Volume One Actual Desired States より転記

5.2. データフロー

CDM では、政府機関内で定められた"Desired State"(理想状態)と、実際に収集した"Actual State"(現状)を動的に比較することでリスクを特定し、緩和する。それぞれのデータフローは「図表 13 データフロー概要図」のとおり。

図表 13 データフロー概要図



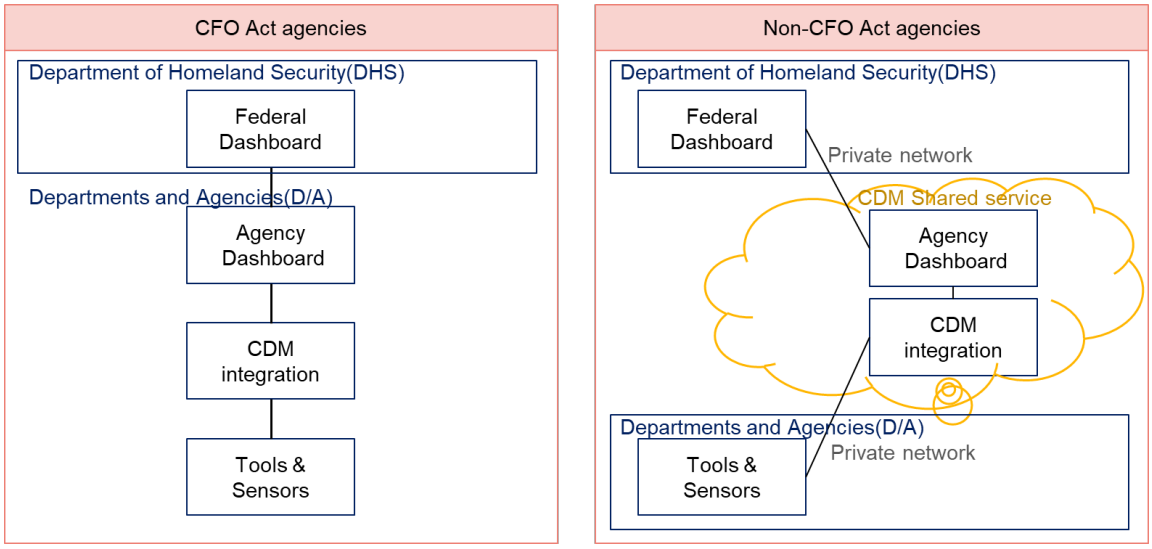
参考文献 9.CDM Technical Capabilities Volume One Actual Desired States より転記

5.3. シェアードサービス

5.3.1. シェアードサービス構成

CFO Act(首席財務官法)の影響を受ける政府機関(CFO Act agencies)とそれ以外の政府機関(Non-CFO Act agencies)とで CDM の提供形態が分かれており、CFO Act agencies よりも組織規模が小さくセキュリティ対応人員も少ない Non-CFO Act agencies に対しては、「図表 14 シェアードサービス構成図」のとおり、Layer B(CDM Integration)及び Layer C(Agency Dashboard)がシェアードサービスとして提供され、CDM への対応コストやリソース負担を軽減するよう配慮されている。

図表 14 シェアードサービス構成図

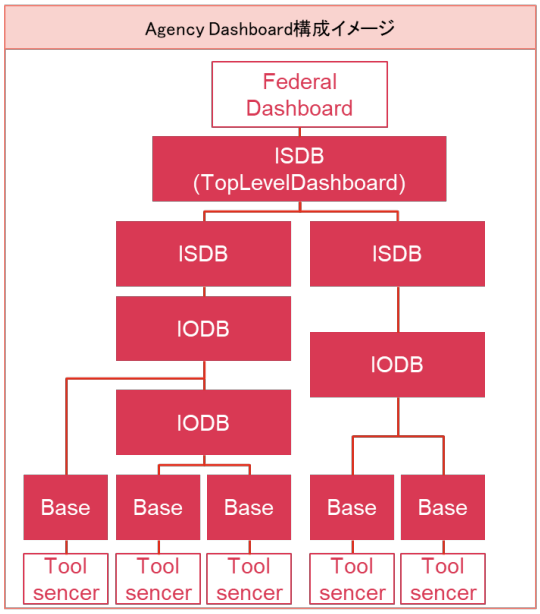


参考文献 10.CDM PROGRAM SHARED SERVICES PLATFORM FACT SHEET より転記

5.4. ダッシュボード構成

Agency Dashboard の種類に関しては、「図表 15 Agency Dashboard の種類」のとおり複数定義されており、大規模な組織は必要に応じて中間サマリー情報を扱う Dashboard を構築する必要がある。

図表 15 Agency Dashboard の種類



1.Base CDM Dashboard(Base)
- CMaaSツールとセンサーからすべてのデータをオブジェクトレベルで取得する
- 独自の範囲を超えてデータまたはダッシュボード構成に影響を与える権限はない

2.Intermediate Object-Level CDM Agency Dashboard(IODB)
- このダッシュボードの下には、Base及び、IODBが存在し、各ダッシュボードからオブジェクトレベルのデータを取得する
- 複数のBaseダッシュボードが必要で、Agencyレベルでの詳細データを希望する場合に使用する
- センサーへの接続を必要とする部分を除いて、Agencyダッシュボードのすべての機能を持つことができる
- 一般的に、中間Agencyダッシュボードは、エージェンシーおよび/またはそのサブコンポーネントが、組織の範囲に関連するリスクを監視するために使用するもの
- Agencyダッシュボードがオブジェクトレベルであれば、特定のオブジェクト上の特定の欠陥の識別と除去も容易になる

3.Intermediate Summary CDM Agency Dashboard(ISDB)
- 他のAgencyダッシュボードからすべてのサマリレベルデータを取得する（オブジェクトレベルデータは取得しない）
- 他のISDBが上の階層に存在する場合がある
- オブジェクトレベルのデータが要求/許可されていない大規模な機関（国防総省（DoD）など）のデータを要約するために使用される

4.Top Level Dashboard
- FederalDashboardに報告する唯一のダッシュボード
- Agencyにダッシュボードが1つしかない場合はそれが該当する

参考文献 5.CONTINUOUS DIAGNOSTICS AND MITIGATION TRAINING

5.5. データ収集方式

5.5.1. Actual State データ収集のセンサータイプ

Actual State に関するデータ収集には、「図表 16 Actual State のセンサータイプ」のとおり 5 つのセンサータイプがある。

図表 16 Actual State のセンサータイプ

センサータイプ	概要
Active Network Sensor	• アクティブネットワークセンサーは、ネットワークまたはネットワーク上のデバイスをアクティブに探査する。センサによって収集されたデータがソース・デバイスから発信されている（つまり、データがプロキシされていない）ため、誤検知の報告が少なくなる。
Passive Network Sensor	• パッシブ・ネットワーク・センサは、特定のネットワーク・セグメントを通過する通信を収集・検査して、ネットワーク接続や接続に関する情報を提供するように構成されている。パッシブな性質のため、これらのセンサは、十分な情報を常に収集できるわけではない。
Asset Management Repository	• 資産管理リポジトリとは、組織のためにその資産を管理するプロセスや活動の一環として作成され、更新されるリポジトリである。また、企業が収集のプロセスを管理していないが、その結果を利用できるようにしている場合には、独自の手段や外部の手段で取得した資産データを収集することも可能である。
Network Event Sensor	• ネットワークイベントセンサは、特定の場所の特定のイベントを検出して報告するように設計されてる。特定の条件を定義可能な点でパッシブ・ネットワーク・センサとは異なる。また、人に警告したり、イベントを集約してサーバーに送信したり、ネットワーク通信の一部を変更/ブロックしたりすることもある。
Endpoint-Based Sensors	• エンドポイント・ベース・センサは、デバイスのOSにインストールまたはネイティブに埋め込まれたソフトウェア・クライアントである。センサがデバイスに直接インストールまたは、埋め込まれているため、誤検知率が最も低くなる。誤検出は、報告の頻度が十分でない場合や、エンドポイント・デバイスが危殆化してセンサに誤ったデータを提供した場合に発生する可能性がある。

参考文献 11.Description of Generic Sensor Types for the Continuous Diagnostic and Mitigation (CDM) Collection System より転記

5.5.2. Actual State の各センサーの特徴

各センサータイプの特徴は、「図表 17 各センサータイプの特徴」のとおり。

図表 17 各センサータイプの特徴

Type	Weaknesses and Limitations	False Positives	False Negatives	Bandwidth Considerations
Active Network Sensor	大規模なIP範囲を能動的に感知するには、長時間（数年の可能性もあります）が必要である。	エンドポイントデバイスから直接センサによって受信されるため、クレデンシャル・センサでは誤検出は少ないが、非クレデンシャル・センサを使用すると、誤検出率が高くなる。また、センサに応答するデバイスやソフトウェアが侵害、偽装、変更されたりした場合にも、誤検出率が高くなる	未検出は、デバイスを探査できないことが、直接的な原因である。実装上の問題（NW接続ポリシーなど）や過度に大きなスキャン範囲（IPv6ブロックなど）を設定している場合がある。デフォルトで「パス」に設定されている非クレデンシャルセンサを使用すると、発生する場合もある。	ネットワーク上のデバイスを積極的に調査したり、デバイスから受信した応答の量が多いため、帯域幅のオーバーヘッドが増加する可能性がある。
Passive Network Sensor	ネットワークのサブネット化やセグメント化により、ネットワークの可視性が制限される。必要なレベルの忠実度が一般的なネットワーク通信の一部として提供されていないため、デバイスの状態情報が不正確になる可能性がある。	誤検出は、一般的なネットワーク通信に含まれるデータから、センサがデバイスに関する特定の十分な情報（例えば、ソフトウェアのバージョンやパッチレベル）を判断できないことに関連している。	未検出は、同じセグメントを横断しているトラフィックしか見ることができず、特別に設定されたデータしか収集できないため、センサーの実装上の問題が原因であることがほとんどである。	分析のために大量のデータをサーバーに戻す必要がある場合、帯域幅の増加が発生することがある。
Asset Management Repository	そのツールやメカニズムによって管理のために識別されたデバイスのみに限定される。利用可能な情報は、別の目的のために収集され、使用されているため、すでに使用しているフォーマットで提供されているデータに限定される。	誤検出は、リポジトリが情報をフォーマットや忠実度のレベルで保存していたり、必要とされるコンテキストとは異なるコンテキストで保存していることが原因である。	未検出は、ほとんどの場合、より大きなケイパビリティの一部として管理されていないデバイスが原因であり、リポジトリにそれらに関するデータがない。	帯域幅の増加は、CDMが使用するためのこの格納情報の更新またはアクセスを行う「バックエンド」のみである。
Network Event Sensor	必要なレベルの忠実度が一般的なネットワーク通信の一部として提供されていないため、関連するデバイス情報が不正確になる可能性がある。しきい値やトリガの適切な設定が簡単に定義されていないか、または決定されていないため、イベントの識別が不正確になる可能性がある。	誤検出の多くは、イベントのしきい値やトリガーの不適切な調整から発生し、通常の活動が誤検出される。また、イベントを検出するためのデータが十分に特定されていないか、または正確でない場合も誤検出される。	未検出は、しきい値とトリガーが広い/狭い場合発生する。また、スコープが広すぎる場合は、重要なイベントの見落としや、未分析が発生し、スコープが狭すぎる場合、チューニングによってイベントの識別ができなくなる。	しきい値やトリガーが大量のイベントを識別するレベルに設定されていたり、識別されたイベントに対して大量のデータを受け渡す必要がある場合、帯域幅の増加が発生する可能性がある。
Endpoint-Based Sensors	プロセッサの負荷が増加するため、デバイスに悪影響を及ぼす可能性がある。	誤検知が発生するのは、報告の頻度が十分でない場合や、デバイスが侵害されている場合のみである。報告頻度は、エージェントの構成によって直接影響を受けるか、ネットワーク接続の問題によって間接的に影響を受ける可能性がある。	未検出は、エージェントがインストールされていない、またはソフトウェアが埋め込まれていないデバイスに直接関連している。	デバイスエージェントとコレクションマネージャ間の帯域幅オーバーヘッドが増加する。オーバーヘッドの量は、情報の種類（例：ハートビート、変更のみ、フルコレクション）と、頻度（例：毎日、変更が検出されたときのみ）に影響される。

参考文献 11.Description of Generic Sensor Types for the Continuous Diagnostic and Mitigation (CDM) Collection System より転記

5.5.3. Desired State データ収集のセンサータイプ

Desired State に関するデータ収集には、「図表 18 Desired State のセンサータイプ」のとおり、3 つのセンタータイプがある。

図表 18 Desired State のセンサータイプ

センサータイプ	概要
Desired State Manager	• DesiredStateManagerは、DesiredStateのセンサーデータの権威あるソースとして機能する信頼された個人である。CDM 内のDesiredStateデータを直接入力、修正、および更新することができる。報告されたデータまたは収集されたデータに矛盾がある場合、矛盾を解消するための権威ある回答をどこで得て、適切な変更を行うかを知る必要がある。
Human Agent	• Human Agentは、必要な状態情報を収集し、CDMに直接入力する信頼された人物である。専門知識や経験が異なるため、収集して入力するデータの品質も異なる。データの品質に関する問題は、通常、収集プロセスに関連しており、収集が完了するまでに時間がかかりすぎたり、エラーが発生しやすい場合（すなわち、プロセスが複雑であるため）、Desired Stateデータの不正確さに基づいて、欠陥が誤って検出されたり、見落とされたりする可能性がある。
Management Repository	• Management Repositoryは、そのデータを管理する責任のあるプロセスまたは活動によって作成され、更新されたデータの集合体であり、CDMに直接データを提供するためにCDM収集システムに組み込まれている必要はない。これらのリポジトリは、CDM の外部にある組織内のツールやプロセスによって管理されているため、一部の情報が誤っている場合や、CDM に必要なものとは異なる形式の場合もある。

参考文献 11.Description of Generic Sensor Types for the Continuous Diagnostic and Mitigation (CDM) Collection System より転記

5.6. ツール

5.6.1. 主な APL 登録ベンダー

Approved Product List (APL)に登録されている、各 Phase に対応している主なベンダーは、「図表 19 主な APL 登録ベンダー」のとおり。

図表 19 主な APL 登録ベンダー

Phase	Vendors		
Phase1. Asset Management	• BeyondTrust • CA Technologies • Check Point • Cisco Systems, Inc. • Crowdstrike • Digital Guardian • Elasticsearch Federal, Inc. • ForeScout Technologies, Inc. • HCL Technologies, Inc. • Hewlett Packard Enterprise • IBM		• McAfee • Microsoft • MobileIron, Inc. • Netskope, Inc. • Palo Alto Networks • RSA Security • Splunk • Tanium, Inc. • Tenable • Tripwire
Phase2. Identity and Access Management	• BeyondTrust • Broadcom • CA Technologies • Check Point • CyberArk • Forcepoint, LLC • Hewlett Packard Enterprise • McAfee • MobileIron, Inc. • Okta		• One Identity • RSA Security • SailPoint Technologies • Splunk
Phase3. Network Security Management	• A10 Networks, Inc. • Akamai • BeyondTrust • Broadcom • CA Technologies • Check Point • Cisco Systems, Inc. • Core Security • Crowdstrike • CyberArk	• Digital Guardian • Elasticsearch Federal, Inc. • F5 Networks, Inc. • FireEye, Inc. • Forcepoint, LLC • ForeScout Technologies, Inc. • HCL Technologies, Inc. • Hewlett Packard Enterprise • McAfee • Micro Focus	• MicroSoft • MobileIron, Inc. • Netskope, Inc. • Palo Alto Networks • Proofpoint • RSA Security • Splunk • Tanium, Inc. • Tripwire • Zscaler Inc.
Phase4. Data Protection Management	• Broadcom • CA Technologies • Crowdstrike • FireEye, Inc. • Forcepoint, LLC • INFORMATICA • McAfee • Micro Focus • MobileIron, Inc. • Netskope, Inc.	• Splunk • Zscaler Inc.	

参考文献 12.CDM Approved Products List より転記

5.6.2. Asset Management の代表的ツール

米国で導入されている、Asset Management の代表的なツールは、「図表 20 Asset Management の代表的ツール」のとおり。

図表 20 Asset Management の代表的ツール

Capability	Baseline and Current Tools	Tool Alternates (Component Choice)
HWAM	• **Forescout** – ForeScout アプライアンスは、ネットワーク上のハードウェア資産（物理および仮想の両方）のハードウェア資産管理（HWAM）データを提供するためのネットワークディスカバリとハードウェアスキャンを行うために使用され、このアセット情報は、マスターデバイスレコードを作成するために使用される。	• **Cisco ISE** • **ServiceNow** • **Tenable**
SWAM	• **McAfee Application Control (AC)** – McAfee Application Controlは、エンドポイント、サーバー、および固定デバイスを制御する不正なアプリケーションによるリスクを低減する。動的な信頼モデルと、ローカルおよびグローバルなレピュテーション インテリジェンス、リアルタイムの行動分析、エンドポイントの自動免疫化などの革新的なセキュリティ機能を使用し、手間のかかるリスト管理や署名の更新を必要とせずに、APT を即座に阻止する。	• **Tanium** • **App Locker** • **Tenable**
CSM	• **McAfee Policy Auditor (PA)** – McAfee Policy Auditor は、Security Content Automation Protocol (SCAP) を活用して、内部および外部の IT およびセキュリティ監査に必要なプロセスを自動化するエージェントベースの IT 評価ソリューションである。	• **Tenable** • **Qualys**
VUL	• **Retina** – BeyondTrust Retina Network Security Scanner は、企業の脆弱性評価ソリューションであり、IT エクスポージャを効率的に特定し、企業全体の改善策に優先順位をつけることを可能にする。	• **Tenable** • **Qualys**

参考文献 13.Privacy Impact Assessment for the Continuous Monitoring as a Service (CMaaS)より転記

5.6.3. Identity and Access Management の代表的ツール

米国で導入されている、Identity and Access Management の代表的なツールは、「図表 21 Identity and Access Management の代表的ツール」のとおり。

図表 21 Identity and Access Management の代表的ツール

Capability	Baseline and Current Tools	Tool Alternates (Component Choice)
Identity and Access Management	• **CyberArk** – **CyberArk**は、特権ユーザの二要素認証を実施するために使用されるCOTS製品である。	–
	• **PAM** – **PAM** は、許可されたユーザに DHS サーバへのセキュアなアクセスを提供し、監査/コンプライアンス機能のためのツールを備えた、企業全体のソフトウェアプラットフォームである。このセキュリティメカニズムは、特権アカウントへのリンクを通じて、DHS 企業全体のすべてのアクセスとクレデンシャル管理を処理する。	• **Xceedium**
	• **SailPoint** – SailPoint Identity IQ ID 管理ソリューションは、規制への準拠とユーザーへのアクセスの提供の両方にかかるコストと複雑さを軽減する。SailPoint を使用すると、デジタル ID を効率的に安全かつ自信を持って管理することができる。	–

参考文献 13.Privacy Impact Assessment for the Continuous Monitoring as a Service (CMaaS)より転記

6. ダッシュボード

6.1. 概要

ダッシュボードの種類と概要は、「図表 22 ダッシュボードの種類と概要」のとおり。

図表 22 ダッシュボードの種類と概要

種類	概要
ダッシュボード	各政府機関のセンサーやツールから収集した情報をもとに、サイバーセキュリティリスクを可視化し、各政府機関毎および政府横断的な**状況認識**を可能にする。それに加えて以下のような利点をもたらす。 • **スケーラビリティ** 政府機関内で収集された大規模なデータセットを効果的かつスケーラブルに処理が可能 • **パフォーマンス** クエリ処理と計算をスピード重視で処理することが可能 • **柔軟性と革新性** 様々な種類の製品と統合できる柔軟性を持ち合わせており、革新的で最先端のテクノロジーを常に利用可能
Agency ダッシュボード	Agencyダッシュボードは、各政府機関毎に配備され、デバイス、ユーザー、権限、および脆弱性に関するデータを表示する。このダッシュボードは、収集した脆弱性の詳細情報を収集・整理し、政府機関のサイバーセキュリティ態勢のオブジェクトレベルのビューを提供する。
Federal ダッシュボード	FederalダッシュボードはCISAとOMBに対して、すべての政府機関のサイバーリスク管理状況を横断的に可視化し、連邦政府としてのサイバーセキュリティ向上を支援する。また、Agencyレベルでのリスク管理を改善するために追加のリソース、ガイダンス、ポリシー、または指示が必要かどうかを判断するのに使用する。

参考文献 1.Securing Federal Networks より転記

6.2. 主な提供機能と表示内容

各ダッシュボードの主な提供機能と表示内容は「図表 23 主な提供機能と表示内容」のとおり。Agency Dashboard では、各政府機関単位で収集された個々のデバイス、ユーザーなどの詳細情報及びサマリーデータ(統計情報など)を確認することができ、リスクスコアが算出される。Federal Dashboard では、各政府機関の Agency Dashboard から連携されたサマリーデータやリスクスコアが横断的に表示される。

図表 23 主な提供機能と表示内容

種類	主な提供機能	主な表示内容
Federal ダッシュボード	• 政府全体のデータ正規化 • 政府全体の状況可視化・レポーティング	• Agency毎の端末数 • 重要度の高い脆弱性の未対応端末数 • 搭載OS毎の端末数 • 各AgencyのAWAREスコア • スコア傾向分析データ (改善数、悪化数 など)
Agency ダッシュボード	• 政府機関内のデータの正規化 • 政府機関内の状況可視化、レポーティング • 収集データの詳細検索 • リスクスコアリング(AWAREスコア算出) • アラートと通知	• 端末毎の、脆弱性の対応有無リスト • 端末毎の、設定ミスのリスト • AWAREの端末スコア • ユーザー毎の資格情報ステータス • インシデント数、インシデント対応時間、侵入から被害発生までの時間(※)

※Phase3のインシデント対応は、Agencyダッシュボードでサマリー確認し、SIEM/EDR等の各ツール管理画面で詳細調査・分析・対応実施と使い分けをしている

6.3. ダッシュボードベースでの運用

ダッシュボードをベースにした運用について有識者より確認した実態は、「図表 24 ダッシュボードの運用実態」のとおり。

プライバシーリスクについて配慮し、基本的には外部委託は行わず政府職員がダッシュボードの確認を行う。外部委託を行う場合は、通常より高い要求事項による調達、要員のバックグラウンドチェックを実施し、ルール違反等の問題発生時には厳しいペナルティが課せられる。

図表 24 ダッシュボードの運用実態

区分	運用実態
Federal Dashboard	• 定期的に、可視化された各Agencyのリスクの状況を確認・比較し、リスクの高いAgencyに対して詳細な状況確認や対応・改善の依頼を行う。 ✓ 確認内容の例：Windowsに最新のパッチが適用されていないデバイスがどの程度あるか、など • 対応に関してAAR(After Action Review)を行い、実施したアクションの効果を確認する。 • 非常にリスクが高いAgencyに対しては、週次で対応状況のレビューを行うケースもある。 • Agency側に予算や人員の不足等があり、対応が困難な場合はAgencyがDHSに対して追加予算の要求を行い、DHSがOMB/GSAと調整を行う。 • AWAREスコアは、各政府機関ごとに、トータルスコアを端末数で割った平均スコアで比較する
Agency Dashboard	• ダッシュボードは日次、場合によっては毎時確認を行う。 • ダッシュボードの確認とギャップ把握専任のチームを設定しているケースもある。 • DHSに対しては月次にて報告を実施。 • DesiredStateとActualStateにギャップが発見された場合、基本的には即座に対応が必要となり、対応が完了するとレビューが行われる。 • AWARE スコアのベースラインはDHS から示される。年度初めに設定され、社会的・経済的条件（例：大統領選挙など）に応じて月次で見直し、全体的にリスクが上昇傾向にある場合は週次で見直される。 • Desired Stateポリシーの見直し・変更は年次もしくは組織のポリシーの変更状況に応じて適宜行われる。

6.4. 進行状況

ダッシュボードは、「図表 25 進行状況」のとおり、四半期ごとのリリースサイクルで継続してデータ品質の向上や機能拡張を実施している。

また、FY2021 中にプラットフォームの変更を予定している。これは、Phase3 以降で収集するデータ量の増大が見込まれ、拡張性や柔軟性のあるプラットフォームを実現するため、ダッシュボードツールを RSA 社の Archer から Elastic 社の Elasticsearch、Kibana に移行する方向で進んでいる。

図表 25 進行状況

	FY2020 Q4	FY2021 Q1	FY2021 Q2	FY2021 Q3	FY2021 Q4
運用上の優先事項	• Agencyダッシュボードのパイロット開始（5以上のAgency） • フィードバックメカニズムの確立	• Agencyダッシュボードの完全展開 • 旧ダッシュボードの維持	• 新しいFederalダッシュボードへの情報交換を確立する	• 新しいFederalダッシュボードへの情報交換を継続する	• 移行完了
サポートするプラットフォーム	+ RSA Archer	+ RSA Archer	OR RSA Archer	OR RSA Archer	
リリース目標	• Agencyダッシュボードの強化 • Federalダッシュボードの最小構成の開発	• ダッシュボードの相互運用性コンポーネントの開発	• 自動レポートでのダッシュボードの状態と移行ステータスの通知	• 新しいプラットフォームで拡張機能を開始（ネットワークアクセス制御）	• 未定
リリース機能	• Agencyヘルスモニタリング（データ品質） • Kibanaのカスタマイズ（パート1）カスタムログインページとロゴ • 要約データの集約と視覚化（AgencyとFederal）	• AgencyとFederalの相互運用性の実装 • FederalからAgencyへのデータ配布と表示（VUL,CSM,SWAM）	• Federalダッシュボードのデータ品質の可視化 • アプリケーションのエラー管理 • システムヘルス-リソース使用量/接続ステータス • モバイル資産の可視化	• AWARE 2.0 • ネットワークアクセスコントロール（NAC） • 機能強化（機能未定）	• 機能強化（機能未定）

※図中のFYは米国の会計年度(fiscal year)を指す。

参考文献 4.OMB sets new CDM data standards deadline for agencies より転記

6.5. 新ダッシュボードの利点

新ダッシュボードを開発している ECS 社と、新ダッシュボードツールの製造元である Elastic 社が挙げている新ダッシュボードの利点は、「図表 26 新ダッシュボードの利点」のとおり。

図表 26 新ダッシュボードの利点

項目	利点
Scalability and Performance	• 大量のデータを即時に取り込み可能(現状は、収集した全データの取り込みができず、可視化できる範囲が限定的 • データの取り込み時にインデックス化することで、即座にデータを分析に活用することが可能
Data Quality	• Elastic Common Schemaを活用することで、多様なソースから収集したデータ項目の正規化が容易となる • データのリアルタイム性が向上(現状のダッシュボード表示は静的なものでリアルタイム性が低く、表示された内容の元となるデータへのアクセスがしづらい)
Connectivity	• RESTful APIをサポートしており、レガシーツールや他のデータ分析プラットフォームとの連携が可能
Removal of State Data	• 一定期間(72時間)更新のないデータを自動的に消去でき、よりリアルタイムに近い状態を把握可能(現状は、ハードウェア資産情報に関する古いデータが残ったままなってしまい消去できない)

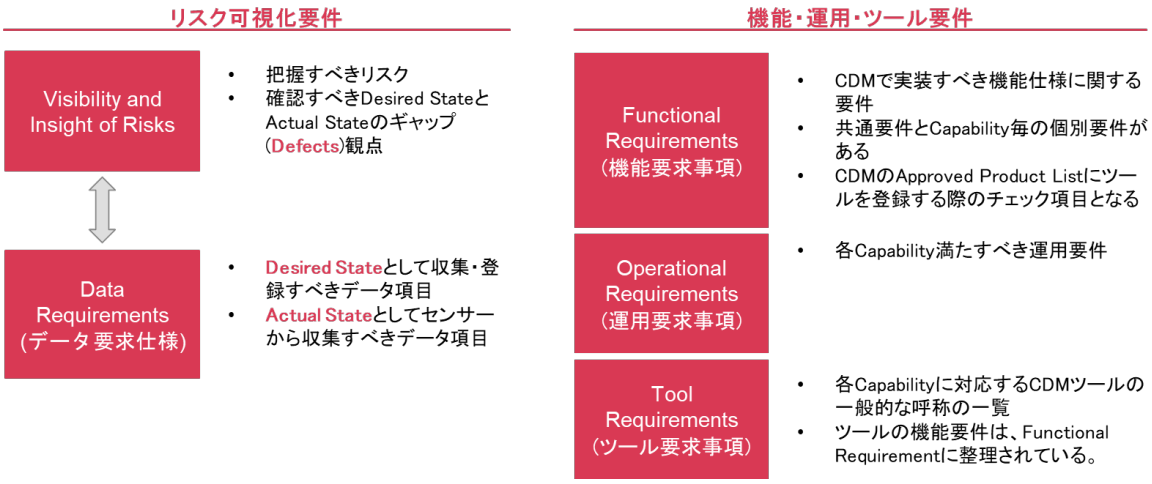
参考文献 14.Elastic for CDM Overview より転記

7. 要求仕様

7.1. 要求仕様全体像

CDM プログラムでは、「図表 27 要求仕様全体像」のとおり、可視化・確認すべきリスクや、そのために収集すべきデータ項目を整理したリスク可視化要件と、データの収集や管理を行うためのツールの機能や運用についての要件を整理した機能・運用・ツール要件を、Capability ごとに定めている。

図表 27 要求仕様全体像



7.2. データ要求仕様(Phase1)

7.2.1. HWAM

7.2.1.1. データ定義

HWAM における、Desired State、Actual State、Defects の定義は、「図表 28 HWAM のデータ定義」のとおり。

図表 28 HWAM のデータ定義

Desired State	• 承認されたハードウェアインベントリ内のデバイスのみがネットワーク上にある。 • 承認されたすべてのデバイスは、承認されたハードウェアインベントリにある。 • 承認されたすべてのデバイスが管理者に割り当てられている。
Actual State	• ネットワークに接続されていると識別されたデバイス • 実際のインベントリに検出、記録、報告するセンサーおよび/またはプロセス ※すべてのActual Stateデータ要素には、その要素の各コレクションインスタンスに関連付けられた日付/時刻が必要
Defects	認可されたハードウェア・インベントリの情報と、認可されたインベントリにあるべき情報、または、実際のインベントリにある情報との間にある違いである。これはダッシュボードに送信され、スコア化されます。

参考文献 15.HWAM Capability Data Sheet より転記

7.2.1.2. Desired State のデータ要求仕様

HWAM における、Desired State のデータ要求仕様は、「図表 29 Desired State データ要求仕様(HWAM)」のとおり。

図表 29 Desired State データ要求仕様(HWAM)

#	目的	データ項目
1	• デバイスを一意に識別する • ネットワーク上のデバイスが承認されたデバイスであり、「偽物」ではないことを検証する	デバイスを正確に識別するために必要なデータ • シリアル番号 • ハードウェアまたは同等のものに期待されるCPE(ベンダー、製品、モデル番号) • 静的IPアドレス(該当する場合) • MACアドレス • プロパティ番号 Local enhancements※には、サブコンポーネントを正確に識別するために必要なデータが含まれる場合がある
2	• デバイスのすべての適切な欠陥が定義され、実行され、報告されていること • デバイスの欠陥を探す他の機能に関連する非レポートを特定する	他の機能がそのデバイスで実行する適切な欠陥チェックを決定できるように、デバイスを記述するために必要なデータ • デバイスまたは同等のオペレーティングシステムに期待されるCPE (ベンダー、製品、バージョン、リリースレベル)
3	• 発見されたリスク状態の修正を指示する人 • リスク管理における各人のパフォーマンスを評価する	デバイスの管理を担当する個人または組織。Local enhancementsには次のものが含まれる。 • 割り当てられている承認者 • 承認されているマネージャー • 受領を確認するマネージャー
4	• 許可されていないデバイスを識別する • どのデバイスに欠陥があるかを知る	ネットワーク上で検出されたデバイスを承認されたハードウェアインベントリと比較するために必要なデータ サイト固有の例は次の通り • IPアドレス • MACアドレス • ホストベースの証明書またはエージェントID • デバイスのドメイン名
5	管理者がデバイスを見つけられるようにする • サプライチェーンのリスク管理のために再検証する • 許可されていない場合は削除する	物理デバイスを見つけるために必要なデータ
6	以前に認可されたデバイスが認可されたハードウェアのインベントリに残っていても、認可されていないことを知る	デバイスが許可されている期間 local enhancementsには次のものが含まれる。 • サプライチェーンのリスク管理のためにデバイスを物理的に検査/検証する必要がある場合
7	許可されたハードウェアインベントリ内のどのデバイスが実際の状態のインベントリで見つからない可能性が高いかを判断する	デバイスの予想されるステータス(承認済み、期限切れ、承認待ち、欠落など)には、次のものが含まれる • 最初に承認された日付 • 最新の承認日 • 承認が取り消された日付 local enhancementsには次のものが含まれる • リスクの高い場所から戻ってきた • 保留中の再承認を削除しました • 最後のステータス変更の日付

※local enhancements:
各政府機関は、ローカル環境のデータ要件と関連する欠陥を定義でき、これはCMaaS請負業者と調整して行われ、これらのローカルの欠陥は連邦ダッシュボードに報告されない。

参考文献 15.HWAM Capability Data Sheet より転記

7.2.1.3. Actual State のデータ要求仕様

HWAM における、Actual State のデータ要求仕様は「図表 30 Actual State データ要求仕様(HWAM)」のとおり。

図表 30 Actual State データ要求仕様(HWAM)

#	目的	データ項目
1	許可されていないデバイス、または、欠陥のあるデバイスを特定する	デバイスを正確に識別するために必要なデータ サイト固有の 例は 次のとおり • IPアドレス • MACアドレス • ホストベースの 証明書またはエージェントID • デバイスのドメイン名
2	これらのデバイスのすべての 適切な欠陥が 定義され、実行され、報告されていることを確認する	他の 機能がそのデバイスで実行する 適切な欠陥チェックを決定できるように、デバイスの 属性を記述するために 必要なデータ • デバイスまたは 同等のオペレーティングシステムに 期待されるCPE ✓ ベンダー、製品、バージョン、リリースレベル
3	許可されていないデバイスを識別する	ネットワークに接続されているデバイスを承認されたハードウェアインベントリと比較するために必要なデータ • IPアドレスと関連ログ • MACアドレス • ホストベースの 証明書またはエージェントID • デバイスのドメイン名
4	管理者がデバイスを見つけて修正、検証、または 削除できるようにする	運用環境で収集された情報に基づいて物理的資産を特定するために必要なデータ サイト固有の 例は 次の 通り • デバイスを検出したエッジスイッチ • USBドライブが 接続されているホスト
5	デバイスが 存在していた期間と、企業内で最後に検出された時刻を確認する	デバイスが 環境内に 存在していた期間を判別するために必要なデータ 最低でも必要なデータは 次の 通り • 最初に発見された 日時 • 最後に検出された 日時

参考文献 15.HWAM Capability Data Sheet より転記

7.2.1.4. Defect

HWAM における、想定される Defect 及び内在するリスクと緩和策は「図表 31 想定される Defect(HWAM)」のとおり。

図表 31 想定される Defect(HWAM)

#	Defect Type	内在するリスク	リスク緩和策①	リスク緩和策②
1	デバイスがActualStateインベントリにあるが、承認されたハードウェアインベントリにない。	そのデバイスが 承認されていない、または 承認されているか 判断できない。	そのデバイスを環境で 動作させる 必要がある 場合は、デバイスを承認し、承認されたハードウェアインベントリに 追加して、管理用に 割り当てる。	その 他の 場合は、デバイスを環境から 削除する。
2	デバイスが 承認されたハードウェアのインベントリとActualStateのインベントリにあるが、そのデバイスの 管理者が 割り当てられていない Local enhancementsには、以下が 含まれている。 • 管理者が 責任を認めていない • 管理者が 承認されていない	その 資産の 管理者が 不明である。	すでに管理者が 割り当てられている 場合は、管理者を特定し、その 結果を許可されたハードウェアのインベントリに 記録する。	そうでなければ、デバイスを適切な管理者に 割り当て、これを承認されたハードウェアインベントリに 記録する。 (その 結果、この 管理者には、デバイス上の 他のリスク状況が 通知され、それらに 対処できるようになります)
3	• デバイスが 承認されたハードウェア・インベントリにあるが、Actual Stateのインベントリにない。 • 承認されたハードウェア・インベントリのステータスは、Actual Stateのインベントリにない 理由を提供しない。	• デバイスがレポートしていない 可能性があり、他の 領域でデバイスを監視する 能力が 低下する。 • デバイスが 誤って、または 悪意を持って 動作環境から 取り外された 可能性がある。(紛失など) • セキュリティ上の 理由から、デバイスが 意図的に 環境から 削除されている 可能性がある。	• デバイスが 実際に 動作しているにもかかわらず 報告しない 場合は、センサーの 問題の 可能性がある。 • センサーマネージャーと 協力して 問題をトラブルシューティングをする。	そうでない場合は、意図的、偶発的、または 悪意を持って 除去された 可能性があるため、原因を調査します。 除去がセキュリティ違反を引き起こした 場合は、インシデントとして 記録し、許可されたハードウェアインベントリでデバイスのステータスを更新します。 除去がセキュリティ目的であった 場合は、デバイスを承認されたハードウェアインベントリから削除するか、不正な(再) 使用を検出できるように、未承認のステータスに 変更します。
4	デバイスが 承認されたハードウェアとActual Stateのインベントリの 両方にあるが、承認が 失効している。	承認の 決定に 関連したリスクは、時間の 経過とともに 増加する。 過去に 許容されていた 判断が、今ではリスクが 高すぎると 考えられる。	環境で 動作するためにデバイスを再認証する 必要がある 場合は、ステータスが 承認に 設定されていることを確認し、承認されたハードウェアインベントリで 有効期限をリセットする。	それ 以外の 場合は、承認されたハードウェアのインベントリおよび 環境からデバイスを削除する。
5	認可されたハードウェアインベントリの 重要なデータ要素が 欠落している。 • CPEまたはそれに 相当するもの	リスクのスコア 付けや 割り当てに 使用される 情報の 重要な 部分が 不明である。	データ要素が 判明している 場合は、その 情報を許可されたハードウェアインベントリに 記録する。	そうでなければ、データ要素を決定または 定義し、これを認可されたハードウェアのインベントリに 記録します。
6	デバイスが 必要とされる 状態にあるかどうかを、設定された 期間内にチェックしていない 例: • 承認済デバイスの 物理的な 再検証を、定義された 期間内に 行っていない。 • 報告のないデバイスについて、物理的な 場所の 特定を決められた 期間内に 行っていない。	特定の 脆弱な 状態に 関する 可視性が 限定的となる。	デバイスが 実際に 利用され、認知されているにも 関わらず 特定の 状態について 報告がなされていない 場合は、承認済ハードウェアインベントリのデータが 不正確である 可能性があるため、これを更新する。	自動的なチェックのための 情報収集や 手動チェックのプロセスに 問題が 発生している 可能性があるため、センサーや 情報収集の 管理者やプロセスオーナーとともに、問題についてトラブルシュートを行う。

参考文献 15.HWAM Capability Data Sheet より転記

7.2.2. SWAM

7.2.2.1. データ定義

SWAM における、Desired State、Actual State、Defects の定義は、「図表 32 SWAM のデータ定義」のとおり。

図表 32 SWAM のデータ定義

Desired State	• スコープデバイスには、承認されたソフトウェア製品と実行可能ファイルのみがインストールされる • すべてのデバイスは、一連のデバイス属性に対して割り当てまたは承認され、承認は定期的に再検証される • すべてのソフトウェアのインストールと実行の制限メカニズムが正しく展開および構成される • すべてのブラックリストは最新である • ホワイトリストまたはブラックリストで明示的に識別されていないすべてのソフトウェアは、グレーリストに含まれる • すべてのグレーリストソフトウェアが調査され、特定の期間内に許可または無許可であると判断され、適切なホワイトリストまたはブラックリストに追加される
Actual State	• すべてのデバイスにインストールされているすべての列挙型ソフトウェア • デプロイされたすべての既知の悪質なソフトウェアのブラックリストと最終更新の日付/時刻 • 実際の状態情報を検出および記録/報告するための収集メカニズムおよび/またはプロセス ※すべてのActual Stateデータ要素には、その要素の各コレクションインスタンスに関連付けられた日付/時刻が必要
Defects	許可されたソフトウェアインベントリとデバイスに存在するソフトウェアとの間の不一致として定義されます。また、デバイスの役割、ソフトウェア製品、ブラックリスト、またはソフトウェアプロファイルに関連するポリシーまたは承認の間の不整合である可能性もあります。

参考文献 16.SWAM Capability Data Sheet より転記

7.2.2.2. Desired State のデータ要求仕様

SWAM における、Desired State のデータ要求仕様は「図表 33 Desired State データ要求仕様(SWAM)」のとおり。

図表 33 Desired State データ要求仕様(SWAM)

#	目的	データ項目
1	• どのデバイスをどの欠陥チェックに対してチェックするかを特定するため	割り当てられ承認されたデバイス属性を含む承認済みハードウェアインベントリ
2	• デバイスに関連する欠陥に優先順位を付ける	属性に関連付けられた値
3	• デバイスに割り当てられた属性のセットと比較するため	D/Aのポリシーに従って相互に排他的に指定された属性のセット
4	• 承認されたソフトウェアの有効期限を計算する • 欠陥ではない差異の自動削除を可能にする • ソフトウェアを一意に識別できるようにする • デバイス上のソフトウェアが本当に承認されたソフトウェアであることを検証できるようにする • 見つかった特定のリスク状態を修正するように指示する人を知る • リスク管理におけるそのような各人のパフォーマンスを評価する	D/Aに含まれるすべての承認済みソフトウェアのリスト: • ソフトウェア製品を正確に識別し、収集された実際の状態データと比較するために必要なデータ(ベンダー、製品、バージョン/リリースレベル/パッチレベル、ソフトウェア識別タグ(SWID)、CPE) • 製品に関連付けられている実行可能ファイルの信頼できるリスト • ソフトウェアマネージャー • 有効期限ポリシー • ソフトウェア認証ステータス • 最初に承認された日付 • 最終承認日 • 取り消された日付
5	• ライセンス、パッチ適用、および構成の標準が最新であることを確認するための管理責任を特定する • 明示的に指定されていない場合は、デバイスマネージャと見なされる • 見つかった特定のリスク状態を修正するように指示する人を知るため • リスク管理におけるそのような各人のパフォーマンスを評価する	承認された各ソフトウェア製品の各ソフトウェア管理機能の管理責任 ローカル拡張機能2には次のものが含まれます。 • 割り当てられている承認者 • 承認されているマネージャー • 受領を確認するマネージャー
6	• デバイスに存在するソフトウェアと比較して欠陥を特定する • デバイスごとにソフトウェアの許可/禁止を定義する • 環境に対して許可されなくなったソフトウェアがベースラインに使用されている時期を判断する • 既知の悪質なソフトウェアのブラックリストが古くなっているかどうかを判断する	D / Aに含まれるソフトウェアプロファイルのセット: • 関連する属性 • 許可されたソフトウェア • 必須のソフトウェア • 禁止されているソフトウェア製品のブラックリスト • 既知の悪質なソフトウェアのブラックリスト • 既知の悪質なソフトウェアのブラックリストの更新頻度
7	• 属性のセットが割り当てられているデバイス(データベースサーバーやデータベース認証サーバーなど)に、より制限的なポリシーを適用する	同じデバイスに割り当てられたときに一意のソフトウェアプロファイルを必要とするデバイス属性のセットには、次のものが含まれます。 • 置き換えられたソフトウェアプロファイル • 使用されるソフトウェアプロファイル

参考文献 16.SWAM Capability Data Sheet より転記

7.2.2.3. Actual State のデータ要求仕様

SWAM における、Actual State のデータ要求仕様は「図表 34 Actual State データ要求仕様(SWAM)」のとおり。

図表 34 Actual State データ要求仕様(SWAM)

#	目的	データ項目
1	• 許可されていないソフトウェアがデバイスにインストールされていることを特定する	すべてのデバイスにインストールされているソフトウェア。このデータは、承認されたソフトウェアインベントリと比較できる形式に変換する必要があります。例は次のとおりです。 • SWID • CPE
2	• 許可されていないソフトウェアがデバイスに存在していた期間を確認する	許可されていないソフトウェアがデバイスに存在していた期間を特定するために必要なデータ。最低でも: • 最初に発見された日時 • 最後に検出された日時
3	• デバイスに不正なソフトウェアがないかどうかを確認する • 既知の悪質なソフトウェアのブラックリストがポリシーごとに最新であるかどうかを判断する	デバイスのチェックに使用される既知の悪質なソフトウェアのブラックリストには、バージョン番号や最終更新日が含まれています。

参考文献 16.SWAM Capability Data Sheet より転記

7.2.2.4. Defect

SWAM における、想定される Defect 及び内在するリスクと緩和策は「図表 35 想定される Defect(SWAM)」のとおり。

図表 35 想定される Defect(SWAM)

#	Defect Type	内在するリスク	リスク緩和策①	リスク緩和策②
1	ソフトウェアの承認が失効している。	承認の決定に関連したリスクは、時間の経過とともに増加する。過去には受け入れられていた判断が、今ではリスクが高すぎるとみなされることがある。	ソフトウェアを再承認する。	そうでなければ、ソフトウェアの承認を取り消したり、一時停止する。
2	ソフトウェアはグレーリスト上にあり、承認されたものとして表示されている。	デバイスに悪意のあるソフトウェアのインストールが許可される。	ソフトウェアを承認する。	そうでなければ、グレーリスト上で、承認されていないものとして扱う。
3	承認されたデバイスに割り当てられたロールが収集されていない、または定義されていない (デバイスロールの非報告)	デバイスに、過剰、無承認、または時代遅れのソフトウェアが許可される。	必要なデータを提供するために開発したプロセスを修正する 機器の役割がわかっている場合は、その役割を記録する。	そうでなければ、プロセスが適切に機能している場合は、コレクションの問題を修正する。 それ以外の場合は、適切なデバイスの役割を決定して記録する。
4	D/Aのデバイスロールポリシーに違反している。 (例:ポリシーによって互換性がないと判断されたデバイスロールが1つのデバイスに割り当てられている)	デバイスのロールポリシーは、1つのデバイスが過剰なアクセスや特権によって組織に過度な影響を与えないようにするために設計されている。	相互に排他的と考えられるデバイスロールからデバイスを削除する。	それ以外の場合は、デバイスロールポリシーを更新する。
5	既知の悪質なソフトウェアのブラックリストがデバイスに定義されていない。	危殆化したデバイスはネットワーク上で動作し続ける。	デバイスに使用する既知の悪質なソフトウェアのブラックリストが判明している場合は、認可されたソフトウェアのインベントリに記録する。	それ以外の場合は、どの既知の悪質なソフトウェアのブラックリストを使用するかを決定し、認可されたソフトウェアのインベントリに記録する。
6	既知の悪質なソフトウェアのブラックリストがデバイスに展開されていない、または実装されていない。	前回のチェックで危うくなったデバイスが、ネットワーク上で動作し続けている。	デバイスに対して既知の悪質なソフトウェアのブラックリストを実行し、タイムリーな自動チェックを実行する機能を配備する。	それ以外の場合は、既存のケイパビリティで実装の問題を修正する。
7	既知の悪質なソフトウェアのブラックリストが期限切れである。	デバイスは既知の攻撃によって侵害され、ブラックリストが更新されるまでネットワーク上で動作し続ける可能性がある。	デバイスのブラックリストを更新し、タイムリーな自動チェックを実行する機能を配備する。	それ以外の場合は、既存のケイパビリティで実装の問題を修正します。
8	実際は未承認であるものの、ブラックリストもしくは(未承認扱いで)グレーリストに登録されていないソフトウェアが存在する。	未承認のソフトウェアは、承認されたソフトウェアに比べて、信頼性が低く、脆弱性が高く、組織の攻撃対象領域が増加する。	ソフトウェアがデバイスで必要な場合は、それを承認し、承認されたソフトウェアインベントリに記録する。	それ以外の場合は、デバイスからソフトウェアを削除する。
9	デバイスに、ブラックリストに登録されている、またはグレーリストで未承認のソフトウェアがインストールされている。	ブラックリストに登録されているソフトウェア(マルウェアなど)は、既に侵害された痕跡もしくは侵害される上での初期条件がそろっていることを示す。	デバイスからソフトウェアを削除する。	調査の結果、ソフトウェアがブラックリストやグレーリストに載るべきではないことが判明した場合は、適切なプロファイルのためにソフトウェアを承認する。
10	ソフトウェアのインストール制限機能が正しく展開されていない、または設定されていない。	許可されていない、または悪意のあるソフトウェアをデバイスにインストールすることが許可されている。	メカニズムをデプロイするか、ポリシーごとに設定する。	それ以外の場合は、既存のメカニズムで実装の問題を修正する。
11	ソフトウェアのインストール制限機能が正しく展開されていない、または設定されていない。	脆弱性や欠陥のあるソフトウェアを悪用した攻撃は、デバイスを侵害することに成功する可能性がある。	メカニズムをデプロイするか、ポリシーごとに設定する。	それ以外の場合は、既存のメカニズムで実装の問題を修正する。
12	認可されたソフトウェアインベントリの重要なデータ要素が欠落している。	リスクのスコア付けや割り当てに使用される重要な情報が不明である。	データ要素が判明している場合は、その情報を認可されたソフトウェアのインベントリに記録する。	そうでなければ、データ要素を決定または定義し、これを認可されたソフトウェアインベントリに記録する。
13	インストールされたソフトウェアが、デバイスの設定された時間枠内に報告されていない。 (ソフトウェアの非報告)	脆弱な状態を監視するための省庁(D/A)の能力が限られている。	センサー/コレクションマネージャーまたはプロセスオーナーと協力して、問題のトラブルシューティング/解決を行う。	そうでなければ、デバイスの認可を取り消すか、または一時停止する。

参考文献 16.SWAM Capability Data Sheet より転記

7.2.3. CSM

7.2.3.1. データ定義

CSM における、Desired State、Actual State、Defects の定義は、「図表 36 CSM のデータ定義」のとおり。

図表 36 CSM のデータ定義

Desired State	• すべてのハードウェアおよびソフトウェア資産が、すべてのインスコープデバイスのポリシーに従って構成されている。 • セキュリティ関連の構成設定を持つすべての認可されたハードウェアおよびソフトウェアには、そのアセットタイプのポリシーを定義する構成設定仕様がある。
Actual State	• ハードウェアやソフトウェアの資産ごとにセキュリティ関連の設定を行うことができる。 • Actual State情報を検出し、記録・報告するための収集機構及び／又はプロセス。 ※すべてのActual Stateデータ要素には、その要素の各コレクションインスタンスに関連付けられた日付/時刻が必要
Defects	実際のハードウェアまたはソフトウェアの構成設定と、D / Aのポリシーで定義されているスコープ内の各デバイスの仕様との不一致として定義される。

参考文献 17.CSM Capability Data Sheet より転記

7.2.3.2. Desired State のデータ要求仕様

CSM における、Desired State のデータ要求仕様は「図表 37 Desired State データ要求仕様(CSM)」のとおり。

図表 37 Desired State データ要求仕様(CSM)

#	目的	データ項目
1	• チェックすべきデバイスおよび適用すべき仕様を特定する • セキュリティ関連の設定を持つが、既存の設定仕様が存在しない、認可されたハードウェアを特定する	すべてのデバイスに含める認定ハードウェアインベントリ • セキュリティ関連の設定フラグ • 適用するコンフィグレーション設定仕様（名前、バージョン、要件オプション）
2	• デバイスに関連する欠陥の優先順位をつける	各デバイス属性の関連する値
3	• チェックすべきデバイスおよび適用すべき仕様を特定する • セキュリティ関連の設定を持つが、既存の設定仕様が存在しない、認可されたソフトウェア製品を識別するため	認可されたすべてのソフトウェア製品に含める組織のホワイトリスト • セキュリティ関連設定フラグ • 適用するコンフィグレーション設定仕様（名前、バージョン、要件オプション） 同じソフトウェア製品に対して、デバイスの属性によって異なる構成ポリシーがある場合は、すべてのソフトウェアプロファイルに、そのソフトウェア製品に対して以下を含める。 • 適用する構成設定の仕様（名前、バージョン、要件オプション）

参考文献 17.CSM Capability Data Sheet より転記

7.2.3.3. Actual State のデータ要求仕様

CSM における、Actual State のデータ要求仕様は「図表 38 Actual State データ要求仕様(CSM)」のとおり。

図表 38 Actual State データ要求仕様(CSM)

#	目的	データ項目
1	• チェックすべきデバイスおよび適用すべき仕様を特定する • セキュリティ関連の設定を持つが、既存の設定仕様が存在しない、認可されたハードウェアを特定する	すべてのデバイスに含める認定ハードウェアインベントリ • セキュリティ関連の設定フラグ • 適用するコンフィグレーション設定仕様(名前、バージョン、要件オプション)
2	• デバイスに関連する欠陥の優先順位をつける	各デバイス属性の関連する値
3	• チェックすべきデバイスおよび適用すべき仕様を特定する • セキュリティ関連の設定を持つが、既存の設定仕様が存在しない、認可されたソフトウェア製品を識別するため	認可されたすべてのソフトウェア製品に含める組織のホワイトリスト • セキュリティ関連設定フラグ • 適用するコンフィグレーション設定仕様(名前、バージョン、要件オプション) 同じソフトウェア製品に対して、デバイスの属性によって異なる構成ポリシーがある場合は、すべてのソフトウェアプロファイルに、そのソフトウェア製品に対して以下を含める。 • 適用する構成設定の仕様(名前、バージョン、要件オプション)
4	• 許可されていない、準拠していない、または古くなった設定を検出する • 見つかった具体的なリスク状況を修正するために、誰に指示すればよいかを知る。 • リスク管理の各人のパフォーマンスを評価する • 必要な頻度でチェックが行われていることを確認する	セキュリティ関連の設定が含まれるすべての認可されたハードウェアまたはソフトウェア製品のための構成設定の仕様 • バージョン • 日付 • 仕様管理者 • 認可状況 • 最初に承認された日付 • 最後に承認された日付 • 取り消された日 • 有効期限について • 対象となる資産の種類・属性 • 仕様周波数 • コンフィグレーション設定チェック識別子(CCE または同等のもの すべての構成設定のチェックインクルードについて • チェック周波数 • 関連するシステム属性 • 要求値/許容値 • コンプライアンスの定義 • 結果の定義

参考文献 17.CSM Capability Data Sheet より転記

7.2.3.4. Defect

CSM における、想定される Defect 及び内在するリスクと緩和策は「図表 39 想定される Defect(CSM)」のとおり。

図表 39 想定される Defect(CSM)

#	Defect Type	内在するリスク	リスク緩和策①	リスク緩和策②
1	認可されたハードウェアまたはソフトウェアにセキュリティ関連の設定がない場合は、フラグが設定されている。	組織のセキュリティ関連の要件が文書化されていないか、または配備されていないため、リスクのあるデバイスが情報やシステムに継続的にアクセスできるようになっている。	すでにセキュリティ関連の設定が決定されている場合は、その結果を記録する。	それ以外の場合、製品を調査し、セキュリティ関連の設定があるかどうかを判断し、結果を記録する。
2	認定されたハードウェアまたはソフトウェアにはセキュリティ関連の設定がありますが、仕様は開発されていない。	組織のセキュリティ関連の要件が実施されておらず、リスクのあるデバイスが情報やシステムに継続的にアクセスできるようになっていない。	認定製品の構成設定仕様書を作成する。	さらに解析して、セキュリティ関連の設定がないと判断された場合は、セキュリティ関連の設定フラグを "No "にリセットする。
3	認定されたハードウェアまたはソフトウェアは、期限切れの仕様でチェックされている。	承認の決定に関連したリスクは、時間の経過とともに増加します。過去には受け入れられていた判断が、今ではリスクが高すぎるとみなされることがある。	コンフィグレーション設定の仕様を再設定する。	それ以外の場合は、製品を適切な認定仕様に関連付ける。
4	サスペンド、リポーク、不適切な設定設定仕様でデバイスチェックを実施した。	既知の安全でない構成設定は、コンプライアンスに準拠しているか、組織のセキュリティ関連の要件を満たしていると考えられますが、リスクのあるデバイスが情報やシステムに継続的にアクセスできるようにするための要件は実施されていない。	承認されたハードウェアまたはソフトウェアのインベントリを更新して、デバイスの正しい製品またはデバイスの役割を反映する。	そうでなければ、認可装置を一時停止するか、または取り消す。
5	デバイスに不正な設定がある。	ハードウェアの設定ミスやインストールされているソフトウェアの設定ミスにより、デバイスは攻撃を受けやすい状態になっている。	コンフィグレーション設定を修正する。	そうでなければ、仕様を更新するか、デバイスの認可を一時停止/取り消しする。
6	Desired State仕様の重要なデータ要素が欠落している。	リスクのスコア付けや割り当てに使用される重要な情報が不明である。	データ要素が既知の場合は、その情報を記録する。	そうでなければ、データ要素を決定または定義し、情報を記録する。
7	設定した時間内に運用設定情報が提供されていない、または更新されていない。 (構成設定は非報告)	脆弱な状態(欠陥など)を監視する能力は限られている。	センサー/コレクションマネージャーまたはプロセスオーナーと協力して、問題のトラブルシューティング/解決を行う。	そうでなければ、デバイスの認可を取り消すか、または一時停止する。

参考文献 17.CSM Capability Data Sheet より転記

7.2.4. VUL

7.2.4.1. データ定義

VUL における、Desired State、Actual State、Defects の定義は、「図表 40 VUL のデータ定義」のとおり。

図表 40 VUL のデータ定義

Desired State	• すべてのデバイスにインストールされているソフトウェア製品には、既知の脆弱性がない • 既知の脆弱性のリストは最新である
Actual State	• すべてのデバイスにインストールされているすべての列挙された脆弱なソフトウェアのリスト • 代替方法によって適切に軽減されたすべてのデバイス上のすべてのCVE • 実際の状態情報を検出および記録/報告するための収集メカニズムおよび/またはプロセス ※すべてのActual Stateデータ要素には、その要素の各コレクションインスタンスに関連付けられた日付/時刻が必要
Defects	少なくとも1つの既知の脆弱性を含む、または古い/不完全なCVEデータを使用しているインストール済みソフトウェア製品の存在です。

参考文献 18.VULN Capability Data Sheet より転記

7.2.4.2. Desired State のデータ要求仕様

VUL における、Desired State のデータ要求仕様は「図表 41 Desired State データ要求仕様(VUL)」のとおり。

図表 41 Desired State データ要求仕様(VUL)

#	目的	データ項目
1	• チェックするデバイスを特定する	許可されたハードウェアインベントリ
2	• デバイスに関連する欠陥に優先順位を付ける	すべてのデバイス属性に関連付けられた値
3	• システムに存在する既知の脆弱性を検出する	以下を含む既知の脆弱性が少なくとも1つあるすべてのソフトウェア製品のバージョン管理された日付付きリスト。 • 認定ソフトウェアインベントリと同じ形式の脆弱なソフトウェア製品(CPEまたはSWIDと同等) • そのソフトウェア製品に関連付けられているすべてのCVE 局所的に定義された既知の脆弱性ごとに、以下を含むバージョン管理された日付のリストを維持する。 • 認定ソフトウェアインベントリと同じ形式の脆弱なソフトウェア製品(CPEまたはSWIDと同等) • そのソフトウェア製品に関連するすべてのローカル脆弱性の識別子 • 各ローカル脆弱性の重大度(CVSSスコア相当)
4	• スコアから自動的にチェックできる代替方法によって軽減された脆弱性を除外する • それぞれの特定のチェックへの準拠を判断する	既知の脆弱性に対する代替の緩和仕様で、ソースベンダーが、ソフトウェアにパッチを適用/復帰させて以下を含める代わりに実装できる緩和オプションを提供します。 • CVEまたはローカル識別子 • 関連するシステム属性 • 必須/許容値 • コンプライアンスの定義

参考文献 18.VULN Capability Data Sheet より転記

7.2.4.3. Actual State のデータ要求仕様

VUL における、Actual State のデータ要求仕様は「図表 42 Actual State データ要求仕様(VUL)」のとおり。

図表 42 Actual State データ要求仕様(VUL)

#	目的	データ項目
1	• 欠陥を特定する	すべてのデバイスにインストールされている脆弱なソフトウェア
2	• スコアからこれらの脆弱性を排除する	適切に軽減されたCVEまたはローカル識別子を含む代替の軽減仕様に準拠しているデバイス
3	• デバイスに脆弱性が存在していた期間を確認する	脆弱なソフトウェアがデバイスに存在していた期間を特定するために必要なデータ 最低でも必要なデータは次の通り • 最初に発見された日時 • 最後に検出された日時

参考文献 18.VULN Capability Data Sheet より転記

7.2.4.4. Defect

VUL における、想定される Defect 及び内在するリスクと緩和策は「図表 43 想定される Defect(VUL)」のとおり。

図表 43 想定される Defect(VUL)

#	Defect Type	内在するリスク	リスク緩和策①	リスク緩和策②
1	デバイスに脆弱性のあるソフトウェア製品がインストールされている。	デバイスが悪用される可能性がある。	パッチを適用するか、またはソフトウェア製品をアップグレードする。	それ以外の場合は、デバイスからソフトウェア製品を削除する。
2	脆弱性のあるソフトウェアのリストには、最新のCVEまたはローカルの脆弱性データが含まれていない。	デバイスが攻撃に対して脆弱性な状態にあるものの、各スコアが適切にリスクを反映した状態で報告されない。	リストを更新し、タイムリーな更新を実行するプロセスを実装する。	それ以外の場合は、既存のプロセスで実装の問題を修正する。
3	脆弱なソフトウェアリストまたは代替の緩和仕様の重要なデータ要素が欠落している。	リスクのスコアリングに使用される重要な情報がない。	データ要素がわかっている場合は、情報を記録する。	それ以外の場合は、データ要素を決定または定義し、情報を記録する。
4	脆弱なソフトウェアが、デバイスの設定された時間枠内に報告できていない。 (脆弱性の非報告)	脆弱性を監視する部門または機関(D/A)の機能が制限される。	センサー/コレクションマネージャーまたはプロセス所有者と協力して、問題のトラブルシューティング/解決を行う。	それ以外の場合は、デバイスの認証を取り消すか一時停止する。

参考文献 18.VULN Capability Data Sheet より転記

7.3. データ要求仕様(Phase2)

7.3.1. MUR

7.3.1.1. データ項目

Phase2 にて、使用する共通データは「図表 44 MUR データ項目」のとおり、Master User Record (MUR)として管理している。各 Capability にて独自に扱うデータ項目は各 Capability の項目を参照。

図表 44 MUR データ項目

#	Data Element	Description
1	Unique Identifier	コンポーネント名とユーザーID で構成され、ユーザーを一意に識別する属性
2	Account ID	物理システムまたは論理システム上で特定のアカウントを一意に識別する属性
3	Full Name	フルネーム
4	First Name	ファーストネーム
5	Last Name	ラストネーム ※Agency のポリシーで必要な場合
6	Middle Name	ミドルネーム
7	Email	電子メールアドレス
8	Job Title	役職名
9	Department	所属する組織名
10	Component	所属する組織名
11	User Status	ユーザーのステータス情報。以下から 1 つ選択される ・SEPARATED - 組織には既に存在しない。 ・ACTIVE - 組織内に在籍し、活動している。 ・SERVICE - 個人ではないエンティティに予約されており、このエンティティに関連付けられた特権/アカウントがまだ使用中であることを示す。 ・INACTIVE - 一時的に組織から離れている。 (サバティカル休暇 など) ・PENDING - まだ活動していない可能性がある。 (手続き中、トレーニング中 など)
12	User Type	ユーザーのタイプ情報。以下から 1 つ選択される ・GOVERNMENT ・CONTRACTOR ・NONPERSON ・OTHER GOVT AGENCY
13	Manager	管理者・監督者

参考文献 13.Privacy Impact Assessment for the Continuous Monitoring as a Service (CMaaS)より転記

7.3.1.2. リスクシナリオと操作

MUR に関する、リスクチェックのシナリオと操作方法の手順は「図表 45 MUR リスクシナリオ」のとおり。

図表 45 MUR リスクシナリオ

シナリオ

DHS-CBPの新しいディレクターが、DHS-CBPネットワーク上のすべての有効で特権的なネットワークアカウントのリストを要求している。

操作

- CDMAgencyダッシュボードの「マスターユーザーレコード」ドキュメントに移動し検索ツールを選択する
- 日付範囲を適切に指定し、現在の状況が表示されるようにする
- インデックスパターンで「cdm_mur_current」を指定する
- レポートに含めるレコード(「organizational.id」、「user.first_name」、「user.last_name」)を選択する
- 組織情報(DHS-CBP)、アカウントタイプ(PRIVILEGED_NETWORK)、アカウントステータス(ENABLED)でフィルタする

リスクチェック

Actual StateとDesired Stateを比較し、調査結果を報告する。

Actual State

- CDMAgencyダッシュボードから取得したデータ

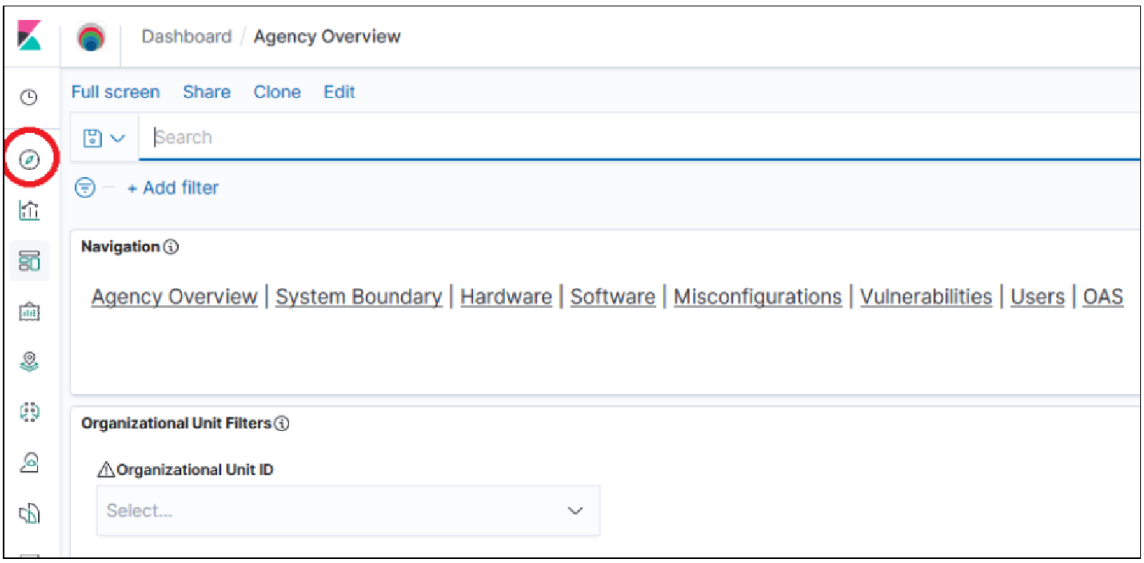
Desired State

- 局長、人事担当者、システム管理者等から取得したデータ

参考文献 5.CONTINUOUS DIAGNOSTICS AND MITIGATION TRAINING より転記

7.3.1.3. ダッシュボードの操作イメージ

(1) Agency ダッシュボードの「マスターユーザーレコード」ドキュメントに移動し検索ツールを選択する

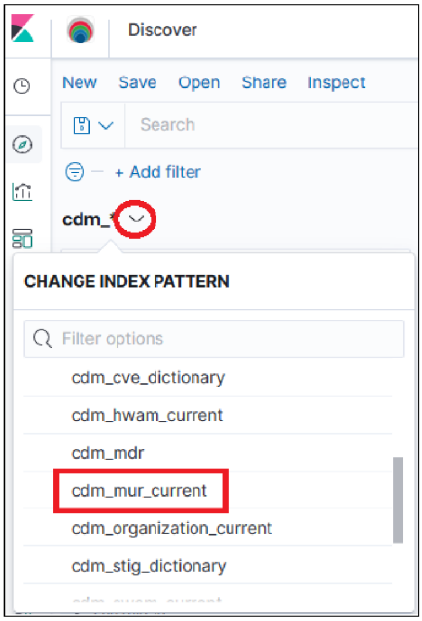


参考文献 5.CONTINUOUS DIAGNOSTICS AND MITIGATION TRAINING より転記

(2) 日付範囲を適切に指定し、現在の状況が表示されるようにする

参考文献 5.CONTINUOUS DIAGNOSTICS AND MITIGATION TRAINING より転記

(3) インデックスパターンで「cdm_mur_current」を指定する



参考文献 5.CONTINUOUS DIAGNOSTICS AND MITIGATION TRAINING より転記

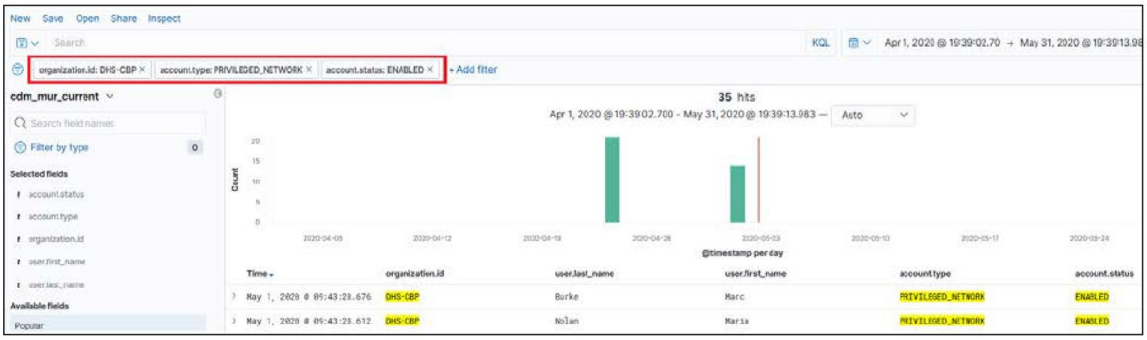
(4) レポートに含めるレコードを選択する

参考文献 5.CONTINUOUS DIAGNOSTICS AND MITIGATION TRAINING より転記

Time	organization.id	user.last_name	user.first_name	account.type	account.status
May 1, 2020 @ 09:43:28.986	DHS-CBP	Barnes	Christopher	-	-
May 1, 2020 @ 09:43:28.986	DHS-CBP	Barnes	Christopher	-	-

参考文献 5.CONTINUOUS DIAGNOSTICS AND MITIGATION TRAINING より転記

(5) 組織情報(DHS-CBP)、アカウントタイプ(PRIVILEGED_NETWORK)、アカウントステータス(ENABLED)でフィルタする



参考文献 5.CONTINUOUS DIAGNOSTICS AND MITIGATION TRAINING より転記

7.3.2. TRUST

7.3.2.1. TRUST Requirements

TRUST の要求事項は以下のとおり。

- 必要な信頼レベルを持つ認可されたユーザーだけが情報やネットワークにアクセスしている
- すべての認可されたユーザーは、定期的に信頼レベルの再検証を受けている

7.3.2.2. データ項目

TRUST で独自に収集するデータ項目は、「図表 46 TRUST データ項目」のとおり。

図表 46 TRUST データ項目

#	Data Element	Description
1	Trust Identifier	特定の TRUST インスタンスを参照する一意な識別子
2	Trust Status	TRUST 認証の現在の状態。以下から 1 つ選択される ・PENDING ・AUTHORIZED ・SUSPENDED ・EXPIRED ・REVOKED
3	Trust Type	スクリーニング/審査のタイプ分類。以下から選択される ・INVESTIGATIVE - バックグラウンドチェックなどの身元調査 ・SUITABILITY - 業務遂行能力や適合性の確認 ・ROB - 行動規約のルールによる承認 ・NDA - 秘密保持契約による承認 ・FDA - 財務状況開示同意書による承認 ・AGENCYOTHER - その他、組織独自のプロセス

参考文献 13.Privacy Impact Assessment for the Continuous Monitoring as a Service (CMaaS)より転記

7.3.2.3. リスクシナリオと操作

TRUST に関する、リスクチェックのシナリオと操作方法の手順は「図表 47 TRUST リスクシナリオ」のとおり。

図表 47 TRUST リスクシナリオ

シナリオ

GAO報告書は、DHS-OIGオフィスのユーザークリアランスの再調査プロセスに弱点があることを明らかにしたばかりです。あなたの機関では、すべてのユーザーに、公的信頼、秘密など、ある種のクリアランスを持つことを要求しています。あなたの上司は、現在INVESTIGATIVE TRUSTのステータスを持っており、今年の年末までに期限が切れるか、すでに期限が切れている権限のあるすべてのユーザーを特定するように依頼することで、この問題の是正を開始することを決定しました。

操作

- CDMAgencyダッシュボードの「マスターユーザーレコード」ドキュメントに移動し検索ツールを選択する
- 日付範囲を適切に指定し、現在の状況が表示されるようにする
- インデックスパターンで「cdm_mur_current」を指定する
- レポートに含めるレコード(「organizational.id」、「user.first_name」、「user.last_name」、「trust.expiration_date」、「trust.status」、「trust.type」)を選択する
- 組織情報(DHS-OIG)、trust.status(AUTHORIZED)、trust.type(INVESTIGATIVE)でフィルタする

リスクチェック

取得した、既に有効期限が切れているまたは、年末までに有効期限が切れるユーザーリストを報告する

参考文献 5.CONTINUOUS DIAGNOSTICS AND MITIGATION TRAINING より転記

7.3.3. CRED

7.3.3.1. CRED Requirements

CRED の要求事項は以下のとおり。

- 正しいタイプの認証情報を持つ認可されたユーザーのみが、施設、情報、及びネットワークにアクセスする
- すべての認可されたユーザーは、定期的に資格情報の再発行またはリセットを受ける

7.3.3.2. データ項目

CRED で独自に収集するデータ項目は、「図表 48 CRED データ項目」のとおり。

図表 48 CRED データ項目

#	Data Element	Description
1	CRED Identifier	特定の CRED インスタンスを参照する一意な識別子
2	CRED Status	CRED の現在の状態。以下から 1 つ選択される ・PENDING ・ISSUED ・SUSPENDED ・EXPIRED ・REVOKED
3	CRED Type	システムで判別された CRED のクラス属性。以下から 1 つ選択される ・USERID PASSWORD ・PIV CARD ・BIOMETRIC ・CAC CARD(防衛省版 PIV CARD) ・Level of Assurance 4 CREDENTIAL ・AGENCYOTHER

参考文献 13.Privacy Impact Assessment for the Continuous Monitoring as a Service (CMaaS)より転記

7.3.3.3. リスクシナリオと操作

CRED に関する、リスクチェックのシナリオと操作方法の手順は「図表 49 CRED リスクシナリオ」のとおり。

図表 49 CRED リスクシナリオ

シナリオ

“フィッシング攻撃により、エージェンシーXXXのユーザーアカウントのUSERIDとパスワードが危険にさらされる！”と今朝のヘッドラインニュースがありました。その結果、DHS本部（DHS）は、全機関に対し、ユーザー名とパスワードを使用してログオンできるアカウントを特定するよう指示を出しました。また、すべてのユーザー認証ポリシーと手順の見直しも求めている。

操作

- CDMAgencyダッシュボードの「マスターユーザーレコード」ドキュメントに移動し検索ツールを選択する
- 日付範囲を適切に指定し、現在の状況が表示されるようにする
- インデックスパターンで「cdm_mur_current」を指定する
- レポートに含めるレコード（「organizational.id」、「user.first_name」、「user.last_name」、[cred.expiration_date」、「cred..status」、「cred.type」）を選択する
- 組織情報（DHS）、cred.type（USERID_PASSWORD）でフィルタする

リスクチェック

取得した、ユーザー名とパスワードでログインしているアカウントリストを報告する

参考文献 5.CONTINUOUS DIAGNOSTICS AND MITIGATION TRAINING より転記

7.3.4. BEHAVE

7.3.4.1. BEHAVE Requirements

BEHAVE の要求事項は以下のとおり。

- 施設、システム、情報にアクセスしているのは、必須トレーニングを受けた権限のある利用者のみ
- すべての権限を持つ利用者が定期的にトレーニングを受けていることを確認する

7.3.4.2. データ項目

BEHAVE で独自に収集するデータ項目は、「図表 50 BEHAVE データ項目」のとおり。

図表 50 BEHAVE データ項目

#	Data Element	Description
1	Training Identifier	適切なセキュリティ関連の BEHAVE 要素を参照する一意な識別子
2	Training Status	セキュリティ関連の BEHAVE 要素の現在の状態。以下から 1 つ選択される ・COMPLETED - BEHAVE が完了している。 ・PENDING - BEHAVE が猶予期間内、または進行中である。 ・INCOMPLETE - BEHAVE が完了していない。 ・EXPIRED - BEHAVE が期限切れである。
3	Training Type	セキュリティ関連の BEHAVE のクラス属性。以下から 1 つ選択される ・CSAT - Cyber Security Awareness Training、FISMA 規定されているサイバーセキュリティ意識向上訓練 ・PHISHING - FISMA に規定されているフィッシング演習 ・ROLE TRAINING - FISMA に規定された要件を満たすために組織内で定義された役割毎のセキュリティ訓練 ・KNOWLEDGE - 研修など、スキルアップ、知識構築を目的としたイベント ・CERTIFICATION ・AGENCYOTHER

参考文献 13.Privacy Impact Assessment for the Continuous Monitoring as a Service (CMaaS)より転記

7.3.4.3. リスクシナリオと操作

BEHAVE に関する、リスクチェックのシナリオと操作方法の手順は「図表 51 BEHAVE リスクシナリオ」のとおり。

図表 51 BEHAVE リスクシナリオ

シナリオ

あなたの組織であるDHS-FEMAは、最初のフィッシング対策キャンペーンを完了し、ユーザーを対象にテストを実施しました。最初のテストでは、約27%のユーザーがテスト用のフィッシングメールに埋め込まれたリンクをクリックしたことが判明しました。CISOは、フィッシング対策トレーニングを完了していないすべてのユーザーの月次報告を求めている。さらに、CISOは、機関内のすべてのフィッシング対策の方針と手順の見直しを要求しています。

操作

- CDMAgencyダッシュボードの「マスターユーザーレコード」ドキュメントに移動し検索ツールを選択する
- 日付範囲を適切に指定し、現在の状況が表示されるようにする
- インデックスパターンで「cdm_mur_current」を指定する
- レポートに含めるレコード(「organizational.id」、「user.first_name」、「user.last_name」、[cred.expiration_date」、「cred..status」、「cred.type」)を選択する
- 組織情報(DHS)、cred.type(USERID_PASSWORD)でフィルタする

リスクチェック

取得した、ユーザー名とパスワードでログインしているアカウントリストを報告する

参考文献 5.CONTINUOUS DIAGNOSTICS AND MITIGATION TRAINING より転記

7.3.5. PRIV

7.3.5.1. PRIV Requirements

PRIV の要求事項は以下のとおり。

- システムにアクセスしているのは、正しいタイプのアカウントを持つ認可されたユーザーのみ
- すべての従業員は、仕事をするために必要な権限のみを持っている

7.3.5.2. **データ項目**

PRIV で独自に収集するデータ項目は、「図表 52 PRIV データ項目」のとおり。

図表 52 PRIV データ項目

#	Data Element	Description
1	PRIV ID	特定の PRIV インスタンスを参照する一意な識別子
2	PRIV Type	アカウントに付与されたシステム特権のタイプと範囲によって決定される PRIV インスタンス分類。以下から 1 つ選択される ・SYSADMIN - ネットワーク上のサーバーで管理者レベル、または root レベルのアクセス権を持つシステム管理者 ・SECADMIN - ネットワーク上の任意のターゲットデバイスの管理者または、root レベルのアクセス権を持つセキュリティ管理者 ・WINENTADMIN - Windows Enterprise Administrator、ネットワーク上のすべての Active Directory ドメインコントローラに対して権限のある管理者 ・WINDOMAINADMIN - Windows Domain Administrator、ネットワーク上の Active Directory ドメインコントローラの管理者権限を持つ Windows ドメイン管理者 ・WINWKSADMIN - Windows Workstation Administrator、ネットワーク上の Active Directory に接続されたワークステーションの管理機能にアクセスできる Windows ワークステーションの管理者 ・MFADMIN - Main Frame Administrator、ネットワーク上のメインフレーム管理機能に管理者アクセス権を持つメインフレーム管理者 ・ENTLDAPADMIN - LDAP Server Administrator、LDAP サー

		バーの管理者 ・ MDMADMIN - Mobile Device Manager (MDM) Administrator、ネットワーク上のモバイル デバイスを制御する MDM システム上の管理アクセス権を持つモバイル デバイス マネージャ (MDM) 管理者 ・NETADMIN - Network Device Administrator、ネットワーク上のネットワーク デバイス管理コントロール コンソールへの管理者アクセス権を持つネットワーク デバイス管理者 ・AGENCYDEFINED - その他、各組織で固有の情報を設定
3	PRIV Status	PRIV 要素の現在の状態。以下から 1 つ選択される ・PENDING ・ISSUED ・SUSPEND ・EXPIRED ・REVOKED
4	Account ID	物理システムまたは論理システム上で特定のアカウントを一意に識別する属性
5	System Boundary ID	特定のシステム境界を識別する一意の識別子
6	Entitlement ID	特定のエンタイトルメントのための一意の識別子
7	Entitlement Type	特定の特権に定められた資格名 (FIREWALL, ROUTER, CORESWITCH)

参考文献 13.Privacy Impact Assessment for the Continuous Monitoring as a Service (CMaaS)より転記

7.3.5.3. リスクシナリオと操作

PRIV に関する、リスクチェックのシナリオと操作方法の手順は「図表 53 PRIV リスクシナリオ」のとおり。

図表 53 PRIV リスクシナリオ

シナリオ

失効したDHS請負業者の管理者アカウントがあなたの機関のシステムにアクセスするために使用されていたことが明らかになったというニュースが発表されました。長官は、保留中、失効、期限切れまたは一時停止されているすべてのDHS請負業者の管理者アカウントのリストを要求しています。また、管理者アカウントの取り扱いに関する方針と手順の更新も求めています。最後に、この問題が解決されるまで、保留、失効、期限切れ、または一時停止されているすべての管理者アカウントについて、週次レポートを作成しなければなりません。

操作

- CDMAgencyダッシュボードの「ユーザー」を選択する
- 日付範囲を適切に指定し、現在の状況が表示されるようにする
- 「User PRIV Details」パネルの「Type」列に各管理者がシステム上で持っている特権のレベルが表示され、[status]列には、各アカウントの状態が表示される
- CDMAgencyダッシュボードの「マスターユーザーレコード」ドキュメントに移動し検索ツールを選択する
- 日付範囲を適切に指定し、現在の状況が表示されるようにする
- インデックスパターンで「cdm_mur_current」を指定する
- レポートに含めるレコード(「organizational.id」、「user.first_name」、「user.last_name」、[priv.expiration_date」、「priv.status」、「priv.type」)を選択する
- 組織情報(DHS-Contractor)、priv.type(exists)、priv.status(pending、revoked、expired、suspended)でフィルタする

リスクチェック

取得した、保留中、失効、期限切れ、一時停止されているDHS請負業者の管理アカウントリストを報告する

参考文献 5.CONTINUOUS DIAGNOSTICS AND MITIGATION TRAINING より転記

7.4. データ要求仕様(Phase3)

7.4.1. BOUND

BOUND で収集するデータ項目は以下のとおり。

- ネットワーク境界線のフィルタリングポリシーに関連するデータ
- NAC(ネットワークアクセス制御)のポリシーに関連するデータ(パッチ適用のベースライン、ウイルス対策ソフトの更新状況などデバイスの状態に関する要件や、ブロックや検疫など非準拠デバイスへのアクション)
- NAC ポリシー施行に関連するイベントやログ
  - ✓ 対象デバイスのメタデータ：ホスト名、OS、IP アドレス
  - ✓ NAC ポリシー施行結果：ブロック、許可、隔離
  - ✓ NAC ポリシー施行結果の理由：ポリシー遵守/非遵守
  - ✓ 検疫デバイス/非準拠デバイスへのポリシー強制状況
- 暗号化ポリシーに関するデータ

7.4.2. OMI

OMI で収集するデータ項目は以下のとおり。

- システム及び情報の完全性を維持するためのポリシー施行に関連する情報
  - ✓ システム及び情報の完全性に関するコンポーネントの脆弱性を緩和するための NIST SP 800-53 セキュリティ管理策の有効性に影響を与えるセキュリティ態勢の変更内容
  - ✓ 自動化された対応や復旧作業を通じた脆弱性及び脅威の是正状況
  - ✓ 悪意のあるコード、行動、脅威からの保護と、脅威や悪意のある活動が脆弱な状態を悪用した場合の緩和策の実施状況
- リスクアセスメントの実施に関連する情報
  - ✓ システム、アプリケーションの分類や、データの機密性、政府機関における業務への影響を踏まえた、継続的なインシデント監視状況
  - ✓ 脆弱性スキャンの結果
  - ✓ リスクアセスメントに沿ったインシデント情報（分析及びアラートを含む）

7.4.3. MNGEVT

MNGEVT で収集するデータ項目は以下のとおり。

- インシデント対応に関連する情報
  - ✓ 悪意あるもしくは異常な活動に関するイベントやインシデント情報
  - ✓ イベントタイプ、脅威発生源、シグネチャ、影響を受けたシステムなどにもとづくインシデントの緊急度に関する分析情報
  - ✓ インシデントの記録、ステータス管理、報告に関するワークフロー
  - ✓ 大量のデータを活用した相関分析アルゴリズム
  - ✓ 深刻度や緊急度にもとづく自動化されたインシデント対応についての情報
- コンティンジェンシープラン実施に関連する情報
  - ✓ コンティンジェンシープランニングにおけるバックアップ運用に関連する情報

- ✓ コンティンジェンシープランに従った事象への対応と復旧のためのアクション

・ 監査データ収集に関連する情報
  - ✓ レビュー、分析及び報告を支援する監査ログ情報
  - ✓ 複数のログソースにまたがって評価と相関関係を実行できるように、標準フォーマット（例： syslog や Common Event Format）での監査ログ情報
  - ✓ 監査と説明責任に沿ったセキュリティポリシーの分析とアラート
  - ✓ 運用ログベースのソースとネットフローソースの統合

7.4.4. DBS

DBS で収集するデータ項目は以下のとおり。

・ 情報システムに対する脅威のモデリング、脆弱性の特定や対策の実施や以下の活動に関連する情報
  - ✓ 情報システムの攻撃対象領域の特定
  - ✓ システムやソフトウェアの設計や開発要件の管理

・ 情報システムのセキュアな開発に関連する以下の活動に関連する情報
  - ✓ 構成管理、変更管理、バージョン管理
  - ✓ 脆弱性検査

・ 情報システムのセキュアなデプロイに関連する以下の活動に関連する情報
  - ✓ リリース管理、パッチ管理
  - ✓ セキュアな設定情報のベースラインの整備と維持
  - ✓ 実行中の情報システムの監視
  - ✓ 実行中の情報システムの問題の追跡
  - ✓ デジタル署名

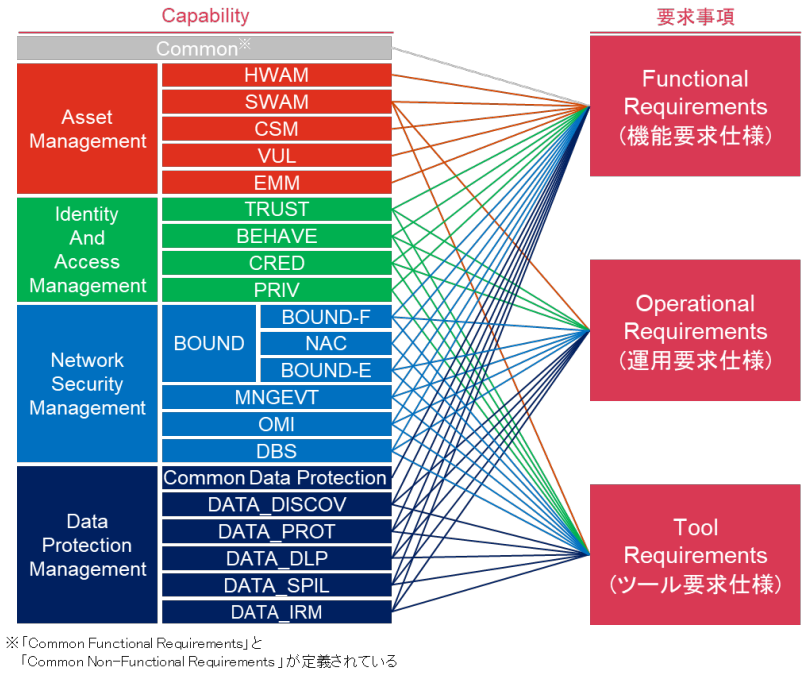
7.5. データ要求仕様(Phase4)

Phase4 にて使用するデータは現時点では詳細に定義されていない。

7.6. 機能・運用・ツール要求仕様

CDM では、「図表 54 各 Capability の要求仕様」のとおり、Capability 毎に機能要求仕様、運用要求仕様、ツール要求仕様が定義されている。要求仕様の詳細は「参考文献 8.CDM Technical Capabilities Volume Two Requirements Catalog 2020」を参照。

図表 54 各 Capability の要求仕様



参考文献 9.CDM Technical Capabilities Volume One Actual Desired States

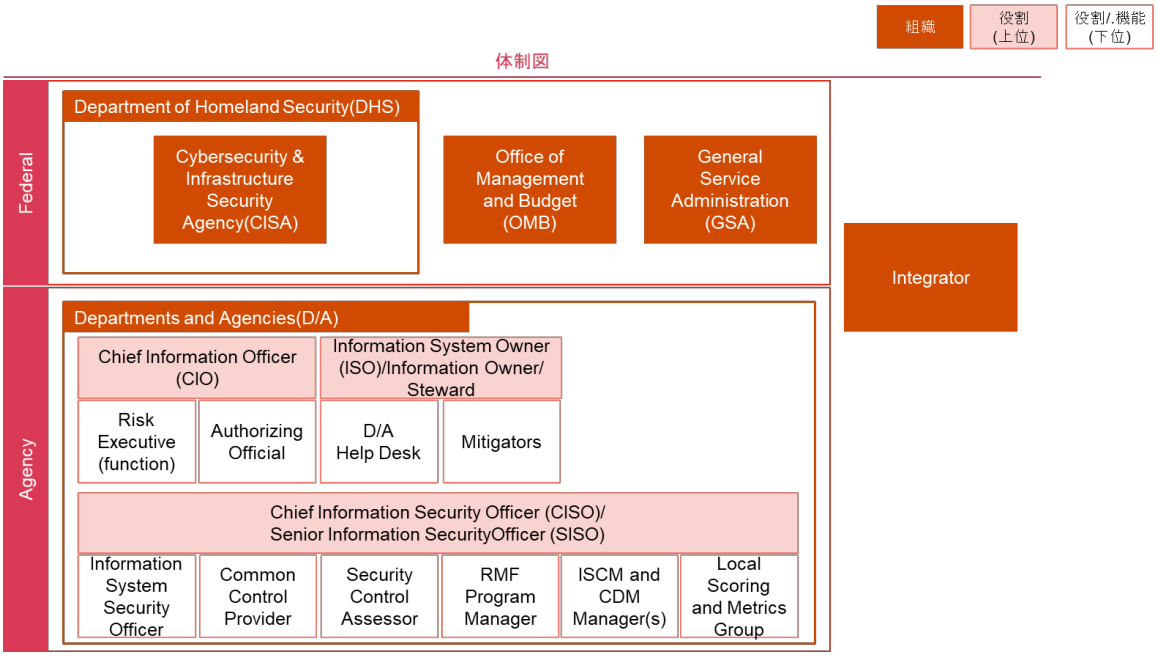
8. 体制

8.1. 関連組織と役割及び責任範囲

8.1.1. 全体体制

CDM プログラムの全体体制は「図表 55 CDM 全体体制図」のとおり。

図表 55 CDM 全体体制図



参考文献 19.CDM Roles & Responsibilities Guide

8.1.2. 各組織の役割

各組織の役割分担は「図表 56 役割分担」のとおり。

図表 56 役割分担

#	組織	役割および責任範囲
1	DHS （国土安全保障省）	D/A(各政府機関)が情報システムのセキュリティを向上させる上での技術的、運用的な支援や、情報セキュリティポリシーの整備およびそれにもとづく対策の実施状況のモニタリングを行う。CDMの各Capabilityの実装を行う上での共通的な機能要件、運用要件を提供する。 Federalダッシュボードの維持・運用を行い、連邦政府全体でのサイバーセキュリティ態勢の状況認識ができるようにする。D/Aに対してFederal Dashboardへの供給を求めるデータ属性について、OMBと協議の上でCDMの技術要求文書にて定義する。 CDMのPMOとしては、CDMツールに関してD/Aの代わりに調達を行い、初期費用（ライセンスおよび初年度保守費用など）の負担を行う。また、CDMの実装に関してD/Aからのフィードバックを求めたり、GSAにより選定されたIntegratorがD/Aのネットワークに対してCDMのツールを一定レベルの質で導入・構成することを確実なものにする。
2	OMB （行政管理予算局）	2002年に制定された電子政府法により、電子政府局が設置され、省庁間の協力体制や統合プロジェクトの調整や監視を行い、D/Aの情報やサービスの利便性向上に努める。また、該当局は、革新的な政府機関プロジェクトをサポートすることを目的とした電子政府ファンドや、委託業者の革新的システム開発を支援するプログラムの運用を行っている。 DHSと共にCIO FISMAメトリクス(D/Aにおけるサイバーセキュリティ対策実施の進捗状況を確認するための指標)を開発している。また、FISMAにより、DHSと協議の上でD/Aの情報セキュリティポリシーおよび対策実施の有効性について毎年報告するよう求められている。
3	GSA （政府一般調達局）	政府全体のCDMのツールやサービスの調達を管理している。ツールとサービスのセットをD/Aに低コストで提供することを目的とした契約手段を導入した。
4	D/A (Departments and Agencies, 各政府機関)	Integratorによる実装計画を評価し、実装後のCDMツールの運用、維持の実施および費用負担（初期費用除く）を行う。 議会での予算説明文書を含む年次の予算文書において、CDM特有の独立した項目を設けて記載することを求められる。加えて、OMBのRMO(資源管理局)と連携して、CDM専用のリソース(人員等)の詳細が記載された費用計画を準備し、将来的な予算計画にCDMの要件を組み込む。 また、FISMAにより、毎年情報セキュリ ティポリシーおよび手順の妥当性と有効性についてDHS、OMB、議会委員会、会計検査院長に報告するよう求められている。
5	Integrator	CDMツール・システムを構築するために、GSAに選定された民間組織。DHSをはじめとする関連組織と連携して、CDMの機能要件と運用要件をサポートするソリューションを開発する必要があり、各ツール・システムの運用と保守を行うことが求められています。 ※Agencyを6つのグループに分け、各グループごとにインテグレーターが割り当てられている。

参考文献 20.DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program

8.1.3. 調達に関する DHS と GSA の役割分担

CDM の調達に関する役割分担は、「図表 57 調達関連の役割分担」のとおり。

図表 57 調達関連の役割分担

	TaskOrder	ツール調達	インテグレータ調達	実行フェーズ
DHS	• 要件の取りまとめ・策定 （TableTop形式※により、各政府機関を集め要件のレビューやステータス収集等を行う）	• APL登録申請のあった製品の審査	• 予算の見積もり、要求、執行	• プロジェクト管理
GSA	• 発行 （Issued by）	• APLの更新・掲載	• 予算の承認 • TaskOrderに基づくインテグレータの選定	• プロジェクト管理
OMB	–	–	• 予算の承認	–

※TableTop形式: 要件策定の際に、各政府機関の担当者やPMOを集め、DHSから提示するスコープ・要件に対するレビューと各政府機関のCDM整備ステータス収集を行い、必要なツールの過不足や必要条件について調整を行う。

8.1.4. Integrator 向けのコミュニティ

CDM に関して、「図表 58 CDM の情報発信・コミュニティ」のとおり、トレーニング資料の公開や各種イベントを開催し、Integrator 向けの情報発信や啓蒙活動が行われている。

図表 58 CDM の情報発信・コミュニティ

媒体	主催	概要
Training 資料	CISA(DHS)	CDMの概要やTraining資料・Webinerの公開
Industry Day	DHS	CDMプログラムに関する、概要、連絡事項、進捗状況、質疑応答などの情報提供
	GSA	CDMツールの特別品目番号（SIN）や調達方式(DEFEND Task Orderなど)に関する情報の業界パートナーへの提供
CDM Central	MeriTalk社	政府機関および民間企業のCDM関係者向けのカンファレンス（有識者・専門家による講演、パネルディスカッションで構成）

8.2. 要員の役割と業務内容

CDM では、要員の役割と業務内容が参考情報として定義されている。これは、各 D/A に強制するものではなく、役割の兼務など各 D/A の状況に合わせて適切に検討することが推奨されている。

8.2.1. Chief Information Officer (CIO)

CIO に関連する役割に推奨される業務内容は「図表 59 CIO に関連する業務内容」のとおり。

図表 59 CIO に関連する業務内容

Chief Information Officer (CIO)	• D/A内でISCMプログラムを主催し、推進する • 各ワーキンググループの代表者のアサインや、スタッフへのトレーニング・リソースを確認する • CDMガイダンス資料と組織内のセキュリティポリシー等を統合する • Agencyダッシュボードに表示する項目の要件設定や、ダッシュボードの結果分析後の改善のプロセスや情報セキュリティへの投資を決定する • 初期のスコアリング及び評価フェーズを障害なく実施し、また、各フェーズの完了時に、障害がないことを公平かつ客観的に確認する
Risk Executive (function)	• レポートカテゴリが、NIST SP 800-39のリスクレベルおよびリスクスコアをカバーしていることを確認する • CDMダッシュボードデータの使用方法を調整し状況把握とリスク管理を行い、許容できないリスク、(暗黙的に)許容できるリスクを確立する
Authorizing Official	• Agencyダッシュボードに表示されるシステムレベルのレポートカテゴリを確立し、継続的にリスクを評価する

参考文献 19.CDM Roles & Responsibilities Guide より転記

8.2.2. Information System Owner (ISO) / Information Owner / Steward

ISO に関連する役割に推奨される業務内容は「図表 60 ISO に関連する業務内容」のとおり。

図表 60 ISO に関連する業務内容

Information System Owner (ISO)/ Information Owner/Steward	• 適切なセキュリティ担当者(システム所有者、情報システムセキュリティ管理者、情報システムセキュリティ担当者など)と協力して、システムレベルで適切なレポート要件を確立する • Agencyダッシュボードのデータを使用して、継続的にリスクを評価する • Agencyダッシュボードのデータを使用して、永続的な問題に対処する情報セキュリティ投資を決定する • CDMプログラムのスタッフが、割り当てられた職務を遂行するために必要なトレーニングとリソース(スタッフや予算など)を持っていることを確認する
D/A Help Desk	• CDMの問題に対応、エスカレーション及び調整を行う
Mitigators	• 不具合確認を見直し、タイムリーにリスク軽減を行う

参考文献 19.CDM Roles & Responsibilities Guide より転記

8.2.3. Chief Information Security Officer (CISO) / Senior Information Security Officer (SISO)

CISO に関連する役割に推奨される業務内容は「図表 61 CISO に関連する」のとおり。

図表 61 CISO に関連する業務内容

Chief Information Security Officer (CISO)/ Senior Information SecurityOfficer (SISO)	• CDMプログラムの管理者と実装者をアサインや、スタッフのトレーニング・リソースを確認する • CDMプログラムの利害関係者を特定し、プログラムについて常に情報を提供するためのプロセスを確立する • CDMプログラムによって満たされるFISMAおよびCISOレベルのレポート要件を特定する • Agencyダッシュボードのデータを使用して、許容できないリスク状況の検知方法や、情報セキュリティへの投資を決定する
Information System Security Officer	• 適切なセキュリティ担当者と協力して、システムレベルで適切なレポート要件を確立する • Agencyダッシュボードのデータを使用して、継続的にリスクを評価し、情報セキュリティ投資の推奨事項を作成する
Common Control Provider	• 適切なセキュリティ担当者と協力して、共通の管理レベルでCDMプログラムによって満たされる適切なレポート要件を確立する • Agencyダッシュボードのデータを使用して、継続的にリスクを評価する
Security Control Assessor	• 自動制御評価で使用するために、NIST SP 800-37RMFプログラムに準拠した適切なレポート要件を確立する • CDMデータがまだ十分または品質に達していない場合は、自動化されていない評価方法を引き続き使用する
RMF Program Manager	• CDMとそのセキュリティ管理評価への影響に関する情報を共有するためのプロセスを監察官事務所（OIG）と開発する • 自動制御評価で使用するためのレポート要件を策定する • CDMの結果を継続的な承認でどのように使用するかを決定する • （継続的な承認に関するNIST補足ガイダンス：ほぼリアルタイムのリスク管理への移行、2014年6月を参照）
ISCM and CDM Manager(s)	• CMaaSプロバイダーと調整して、下記の通りセンサーパフォーマンスを管理する ✓ センサーアクセス認証（ファイアウォール経由を含む）、データの完全性（可用性を含む）、データの適時性、エラー率（誤検知および誤検知） • ダッシュボードのアクセス制御プロセスと手順を確立し、適切に管理されていること確認する • D/Aヘルプデスクと調整し、問題に対する事前に記述された解決策及びエスカレーションのルールと手順等を確立する • 緩和策に技術的な支援を提供するプロセスを確立する • さまざまなユーザー間でレポート要件を調整する • CDMの監視項目を実装するための業務を確立し、スタッフがトレーニングを受けるようにする（少なくとも、DHS CDMが提供するトレーニングを利用する） • CDMプログラムのスタッフが、必要なトレーニングとリソースを持っていることを確認する • 契約担当官と連携して、契約後のCDMおよびCMaaSの有効性を継続的に確認する
Local Scoring and Metrics Group	• Federalのスコアリングワーキンググループおよびメトリクスワーキンググループとの連絡係を設置する • 新たなリスクの導入を管理するためのプロセスを確立し、運用する • 構成設定の問題点と調整サブグループを確立する • センサー性能の測定と管理のための要件を確立する • リスク移転サブグループの作成など、リスク移転を実施するためのプロセスを確立し、運用する • 以下を含むリスクスコアリングを管理する ✓ リスクスコアの管理方法と、ベースライン設定から逸脱した場合の対処方法を決定する ✓ 連邦政府や地方のスコア算出の調整方法を決定する ✓ スコアの公正性、透明性、信頼性、客観性の検証と維持を行う ✓ 懸念事項に対処しながら、モチベーションを高め、パフォーマンスを評価するために、スコアと成績を使用する

参考文献 19.CDM Roles & Responsibilities Guide より転記

9. 各種評価指標

9.1. リスクスコアリング

9.1.1. AWARE の概要

Agency-wide Adaptive Risk Enumeration (AWARE)は、CDM におけるリスクスコアリングの方法論であり、”Worst Problem First”の考え方に基づき、サイバーリスクについての状況認識と脅威と脆弱性のタイムリーな緩和を可能にする。

AWARE スコアは、「図表 62 AWARE の概要」のとおり、主に Phase1 の各 Capability にて収集するデータにもとづき算出され、VUL、CSM、UAH の 3 種類がある。

図表 62 AWARE の概要

Agency-wide Adaptive Risk Enumeration (AWARE)	CDM用に開発された、スコアリングシステムです。 「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し、セキュリ ティ態勢の状況を表します。 算出されたスコアから優先順位を付けを行い、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します。
ソフトウェア脆弱性 (VUL)	アセット管理中に VUL 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とエクスポージャー (CVE) から構成されます。
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ます。
未承認機器管理 (UAH)	UAHは、ダッシュボード・コンテナ内で所有権が割り当てられていないハードウェア・デバイスを表します。所有権が割り当てられていない資産は、資産管理の発見時にハードウェア資産管理ツールを使用して発見されます。

参考文献 21.CDM PROGRAM AWARE SCORING より転記

9.1.2. AWARE スコア算出方法

AWARE スコアは、「図表 63 AWARE 算出方法」のとおり、「Base Metric」、「Age Metric」、「Weight Metric」、「Allowable Tolerance Metric」 の 4 要素から算出される。また、各スコア種類によって算出に使用される Metric の値が異なる。

図表 63 AWARE 算出方法

算出に使用する値

	Base Metric	Age Metric	Weight Metric	Allowable Tolerance Metric
VUL	CVSSに応じた値	経過日数に応じた値	影響度に応じた値	30 days
CSM	STIGに応じた値	1	影響度に応じた値	30 days
UAH	10	1	1	7 days

参考文献 5.CONTINUOUS DIAGNOSTICS AND MITIGATION TRAINING より転記

9.1.2.1. Base Metric

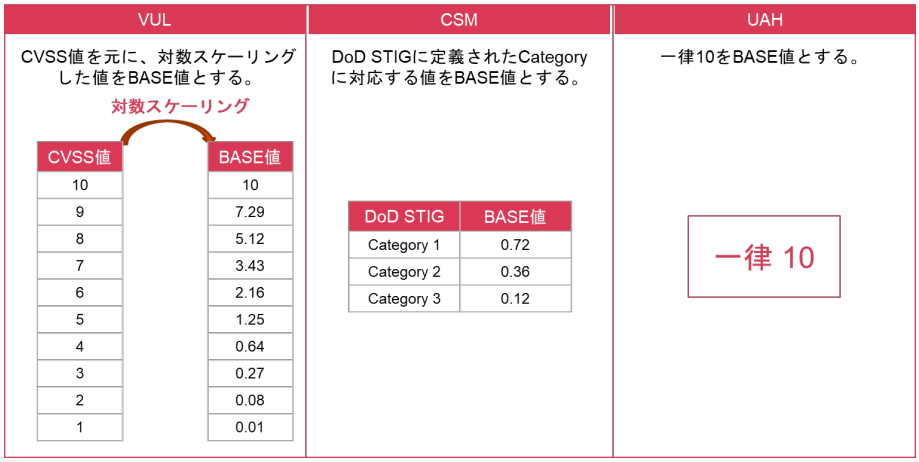
Base Metric は、「図表 64 Base Metric」のとおり、各スコア種類によって使用する値が異なる。

VUL に関しては、共通脆弱性評価システム(CVSS：Common Vulnerability Scoring System)によって算出された脆弱性の評価値(CVSS 値)の値を対数スケーリングした値を使用する。

CSM に関しては、米国の国防総省(DoD：Department of Defense)の国防情報システム局(DISA：Defense Information Systems Agency)が提供するセキュリティ技術ガイドライン(STIG：Security Technical Implementation Guide)に定義されている、リスクの重大度を示すカテゴリ(Category 1- 3)に対応する値を使用する。

UAH では、一律 10 を使用する。

図表 64 Base Metric

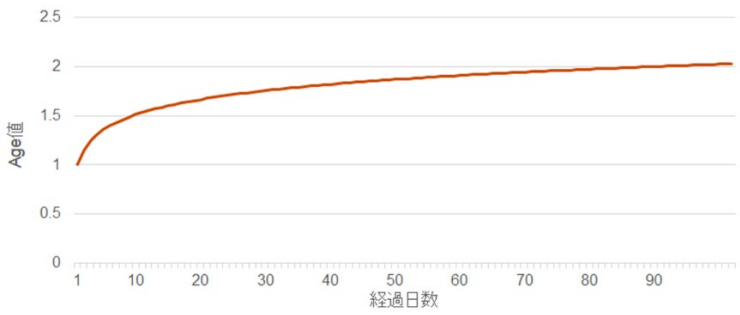


参考文献 5.CONTINUOUS DIAGNOSTICS AND MITIGATION TRAINING より転記

9.1.2.2. Age Metric

Age Metric は、「図表 65 Age Metric」のとおり、共通脆弱性識別子(CVE：Common Vulnerabilities and Exposures)が公開されてからの経過日数を対数スケーリングした値を使用する。脆弱性は、更改されてからの時間経過と共に攻撃を受ける可能性が増えるため、リスクが増加するという考え方である。

図表 65 Age Metric



参考文献 5.CONTINUOUS DIAGNOSTICS AND MITIGATION TRAINING より転記

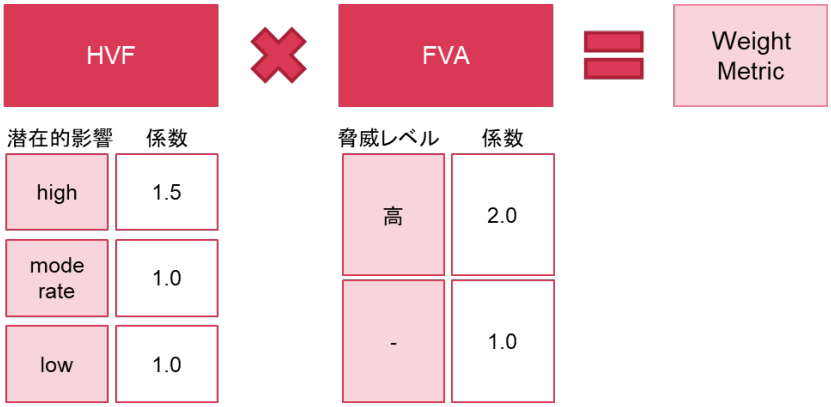
9.1.2.3. Weight Metric

Weight Metric は、「図表 66 Weight Metric」のとおり、High Value Factor (HVF)と Federal Vulnerability Action (FVA)のから算出される。対象のシステムの重要度が高いほど、脆弱性の脅威レベルが高いほどリスクが高くなるという考え方である。

HVF に関しては、Federal Information Processing Standard Publication 199 (FIPS 199)によって算出された潜在的影響の段階に応じて値が決まる。

FVA に関しては、threat intelligence によって CVE の脅威レベルが「高」と判断された場合は 2.0、それ以外の場合は 1.0 となる。

図表 66 Weight Metric

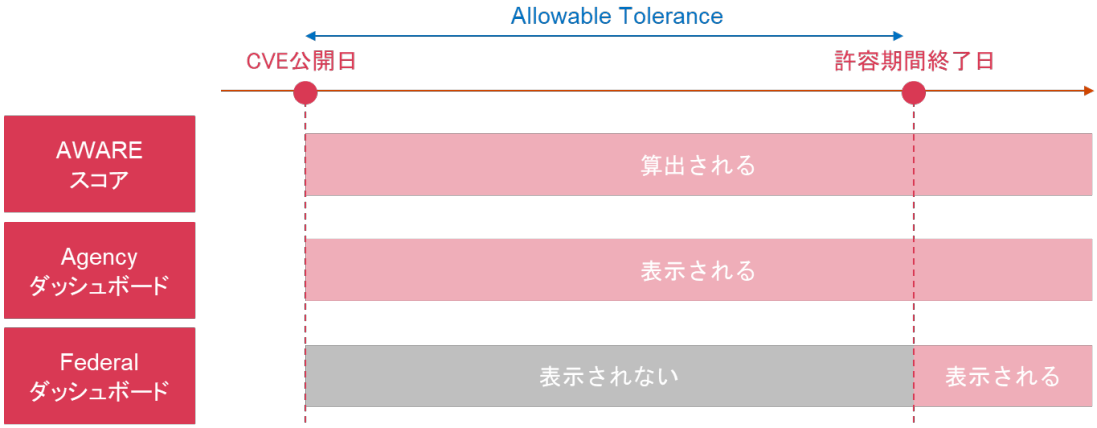


9.1.2.4. Allowable Tolerance Metric

Allowable Tolerance Metric は、CVE 公開日から対応完了までの間に必要となる、パッチ適用テストや動作確認等のための期間を、「パッチが適用されていない状態を許容する猶予期間」として定めたものである。

「図表 67 Allowable Tolerance Metric」のとおり、定義された許容期間の間は、AWARE の算出及び Agency Dashboard への表示は行われるが、Federal Dashboard へのデータ連携は行われない。

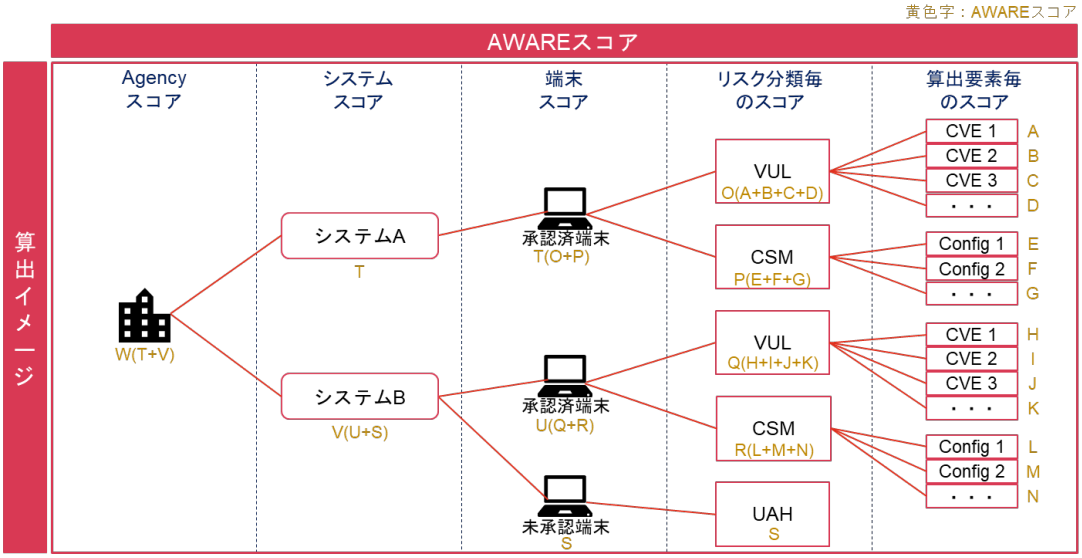
図表 67 Allowable Tolerance Metric



9.1.3. AWARE スコア集計方法

AWARE スコアは、まずは端末に対する各スコア(VUL,CSM,UAH)の合計値を端末スコアとして算出する。その上で、「図表 68 スコア集計イメージ」のとおり、端末スコアを、システム単位、Agency 単位で集計することで、システムスコア、Agency スコアが算出される。

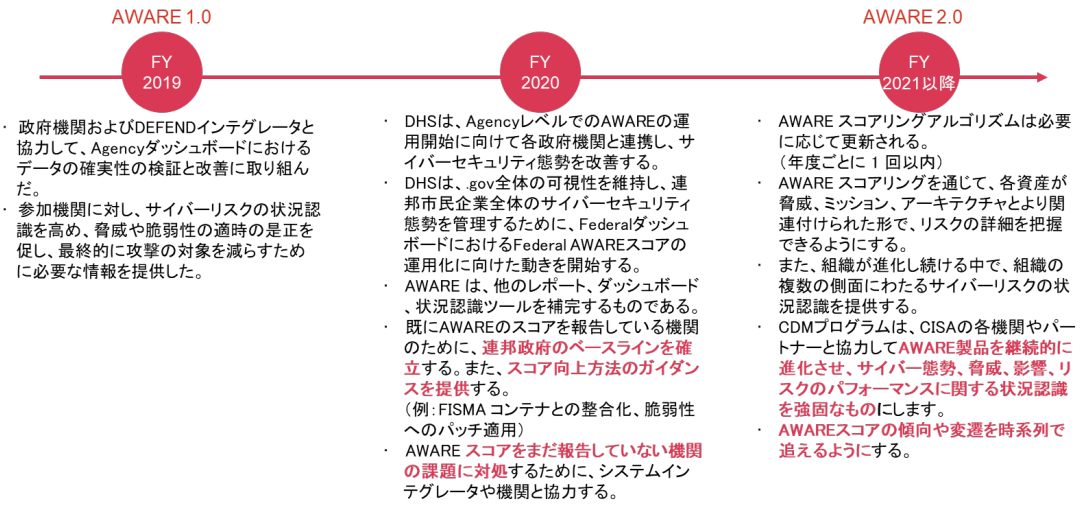
図表 68 スコア集計イメージ



9.1.4. AWARE の進行状況

「図表 69 AWARE の進行状況」のとおり、政府機関全体で AWARE スコアの算出・報告するための取り組みを進めるとともに、スコアリングアルゴリズムを継続的に更新し、より詳細なサイバーリスクの状況認識を提供することを目指している。

図表 69 AWARE の進行状況



参考文献 21.CDM PROGRAM AWARE SCORING より転記

9.2. CDM の効果測定指標

DHS は毎年度、連邦政府のサイバーセキュリティ強化のゴールプランの策定と進捗状況の公開を行っている。「図表 70 CDM の効果測定指標」のとおり、その中で 3 つの Strategy と共に効果測定指標を設けており、CDM プログラムに関連する目標と結果が記載されている。

図表 70 CDM の効果測定指標

Strategy	効果測定指標(Key Indicator/Measure)	FY20目標	FY20結果
エンタープライズリスクに対する認識向上	• 信頼性の高い、資産AWAREスコアをFederalに報告したAgencyの割合	0%	100%
	• Federalダッシュボードへのユーザーアクセスデータの提供を開始したAgencyの割合	25%	100%
	• FISMAのデバイスについて、Federalダッシュボードで報告されたITハードウェアデバイスが自己申告した数値の10%以内に収まっているAgencyの割合	FY21から報告開始予定	
	• Federalダッシュボードのアクティブユーザー数が、FISMAユーザーの自己申告数の10%以内に収まっているAgencyの割合	FY21から報告開始予定	
既知の脆弱性の軽減	• cyber hygieneスキャンによって特定された重要または高い脆弱性のうち、指定された期限内に緩和されたものの割合	70%	75%
	• 重要かつ構造的に高い脆弱性に対する緩和活動のうち、スケジュール通りに実施されている割合	60%	32%
	• 重要かつ高度な構成ベースの脆弱性のうち、30日以内に緩和された割合	70%	30%
悪意のあるインシデントの管理	• 影響を受けるAgencyが指定された時間内に警告を受けた潜在的な悪意のあるサイバー活動の通知の割合	75%	93%
	• 通知されたAgencyが受信を確認した潜在的な悪意のあるサイバー活動の通知の割合	75%	93%
	• Agencyが悪質ではないと確認した潜在的な悪質なサイバー活動の通知の割合	15% 以上	55%

※灰色箇所は、National Cybersecurity Protection System (NCPS)からの通知に対する管理を指しており、CDMの範囲外

参考文献 22.Strengthen Federal Cybersecurity January 2021 より転記

10. 調達戦略

10.1. 調達方式

10.1.1. CDM の調達方式

CDM のサービス調達は、「図表 71 CDM の調達方式」のとおり、GSA の政府横断型調達契約、Alliant 2 Government Wide Acquisition Contract (GWAC)に基づき、Dynamic and Evolving Federal Enterprise Network Defense (DEFEND)という一連の Task Order (TO)を通じて行わる。

従来の包括購買協定、Black Purchase Agreement (BPA)方式から DEFEND Task Order への移行により、CDM の全ての Phase、Capability 及びライフサイクル全体を一括で調達することが可能となり、政府機関の調達に関する負担が軽減された。

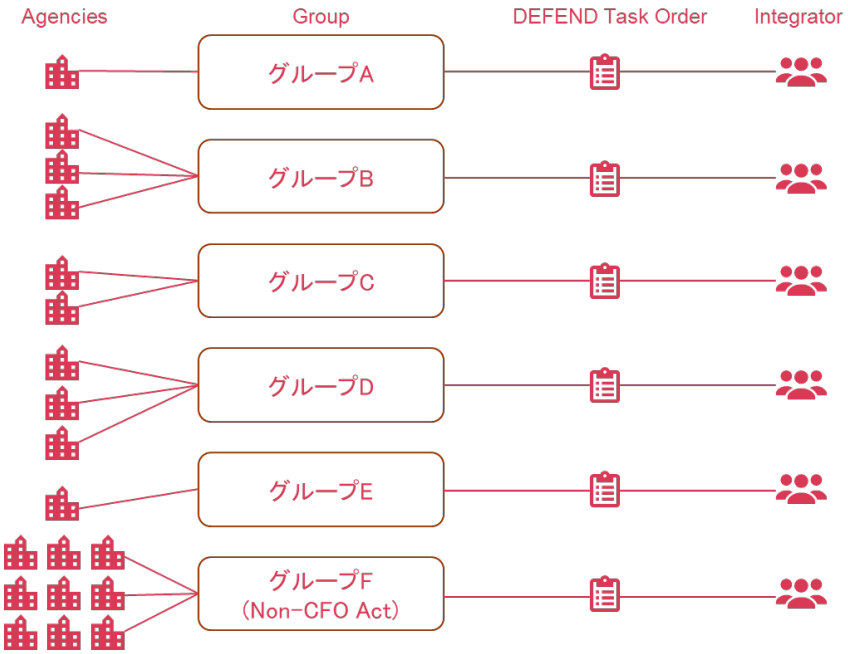
図表 71 CDM の調達方式

従来の方式	Blanket Purchase Agreements (BPA)	• 消耗品やサービスのための反復的なニーズを満たすために設立された契約 • 定期的なニーズを満たすことが容易になり、同時に、数量割引を利用して買い手の購買力をフルに活用し、管理時間を節約し、事務処理を削減することができる • 個々の政府機関のレベルで交渉が行われる
新しい方式	DEFEND Task Order	• CDMのための新しい調達方式であり、ツール単品の購入ではなく、導入・サービスも含めたライフサイクル全体をカバーする調達方式である • CDMプログラムの全フェーズ・Capabilityを対象としており、既存で導入済のPhase1,2のCDMソリューションのサポートと、Phase3,4,の機能追加がスコープとして含まれる • 5～6年の長期契約期間 • (DEFEND TOの前身である)BPAベースでの調達(Task Order 2(TO2)シリーズもしくはPRIVMGMT、CRED MGM)に参加していない機関に対する、CDM全ソリューションの提供 • 複数の政府機関のニーズに対して一括で対応が可能

10.1.2. DEFEND Task Order の範囲

DEFNED Task Order は、「図表 72 DEFEND の調達イメージ」のとおり、6 つに分割された Agency のグループ単位で作成され、グループ毎に Integrator 及びツールを調達している。

図表 72 DEFEND の調達イメージ



10.1.3. Agency のグループ構成

Agency の 6 グループの構成及び Task Order を受注した Integrator 及び受注金額は、「図表 73 Agency のグループ構成(A-E)」と「図表 75 Agency のグループ構成(F)」のとおりである。A-E のグルーピングは、Agency の規模(ネットワーク上の endpoint 数)を一つの目安として行われている。

なお、グループ F(Non-CFO Agencies)の場合は、CDM の費用支払いが出来ない場合は、OMB、CISA に申請することで CDM PMO に費用負担をしてもらえる等の違いがある。

図表 73 Agency のグループ構成(A-E)

Group	Agency	Integrator	金額
A	• Department of Homeland Security	CACI International	$407M six-year
B	• Executive Office of the President (EOP) of the United States (Office of Management and Budget (OMB) MAX) • Department of Energy (DOE) • Department of Interior (DOI) • Department of Transportation (DOT) • Office of Personnel Management (OPM) • Department of Agriculture (USDA) • Department of Veteran Affairs (VA)	Booz Allen Hamilton	$621M six-year
C	• Departments of Commerce • Departments of Justice • Departments of Labor • Departments of State • the U.S. Agency for International Development.	CGI Federal	$530M six-year
D	• GSA • Department of Health and Human Services (HHS) • National Aeronautics and Space Administration (NASA) • Social Security Administration (SSA) • Department of the Treasury (Treasury) • the United States Postal Service (USPS)	Booz Allen Hamilton	$1.03 billion six-year
E	• Department of Education (ED) • Department of Housing and Urban Development (HUD) • HUD Office of Inspector General (HUD OIG) • Environmental Protection Agency (EPA) • Federal Deposit Insurance Corporation (FDIC) • Nuclear Regulatory Commission (NRC) • National Science Foundation (NSF) • Securities and Exchange Commission (SEC) • Small Business Administration (SBA)	ManTech	$668M six year

図表 74 Agency のグループ構成(F)

Group	Agency	Integrator	金額
F	• American Battle Monuments Commission (ABMC) • Broadcasting Board of Governors (BBG) • Consumer Financial Protection Bureau (CFPB) • Commodity Futures Trading Commission (CFTC) • Council of the Inspectors General on Integrity and Efficiency (CIGIE) • Corporation for National and Community Service (CNCS) • Consumer Product Safety Commission (CPSC) • Court Services and Offender Supervision Agency for DC (CSOSA) • Defense Nuclear Facilities Safety Board (DNFSB) • Department of State Office of the Inspector General (DOS OIG) • Equal Employment Opportunity Commission (EEOC) • Farm Credit Administration (FCA) • Federal Elections Commission (FEC) • Federal Energy Regulatory Commission (FERC) • Federal Housing Finance Agency (FHFA) • Federal Maritime Commission (FMC) • Federal Trade Commission (FTC) • International Boundary and Water Commission • Millennium Challenge Corporation • Merit Systems Protection Board (MSPB) • National Archives and Records Administration (NARA) • National Capital Planning Commission (NCPC) • National Endowment for the Arts (NEA) • National Endowment for the Humanities (NEH) • National Labor Relations Board (NLRB) • National Transportation Safety Board (NTSB) • Office of Government Ethics (OGE) • Overseas Private Investment Corporation (OPIC) • United States Office of Special Counsel (OSC) • Occupational Safety and Health Review Commission (OSHRC) • Pension Benefit Guaranty Corporation (PBGC) • Privacy and Civil Liberties Oversight Board (PCLOB) • Peace Corps Peace Corps • Postal Regulatory Commission (PRC) • Railroad Retirement Board (RRB) • U.S. Securities and Exchange Commission (SEC) • Selective Service System (SSS) • Tennessee Valley Authority (TVA) • United States Access Board (USAB) • U.S. African Development Foundation (USADF) • United States International Trade Commission (USITC) • USPS Office of Inspector General	CGI	$276M six year

10.2. 調達関連ツール

GSA は、「図表 75 調達関連ツール」のとおり、CDM を実現するために DHS が承認した利用可能な製品リストを CDM Approved Product List (APL)として、各政府機関が認定済製品及び付帯サービスを調達・購入する仕組みとして CDM Tools Special Item Number (SIN)を整備している。Tools SIN は、DEFEND Task Order の枠組みの範囲以外で製品を調達する際に活用可能である。

図表 75 調達関連ツール

CDM Approved Product List(APL)	• DHSが承認した、CDM要件を満たす製品のカタログである。 • 承認されるためには、各CapabilityのFunctional Requirementsを満たしている必要がある。 • CDM Tools SINに製品を追加する前に、CDM APL として承認される必要がある。
CDM Tools Special Item Number(SIN)	• 連邦政府機関が利用可能な、DHS(CISA)が認定したCDM製品への直接アクセスを提供する。 • CDM Tools SINの全機能には、関連するメンテナンスやトレーニングなどの関連サービスが含まれている。

11. 実行上の課題

11.1. 課題サマリー

CDM 実行に関する課題を「図表 76 課題サマリー」のとおり、主に 6 つの項目に整理・要約した。詳細は「11.2 課題に関する各情報源の記載詳細」に記載する。

図表 76 課題サマリー

項目	概要
戦略	• より価値の高い資産や特定のシステム環境にフォーカスするのか、全てのシステム環境に全てのCapabilityを導入するのか、といった方向性の整理が必要である
導入スピード	• CDMの導入や展開のスピードが遅く、サイバー攻撃の進化に追いついていない
データ品質	• データ品質が悪く、ダッシュボードを用いた意思決定が困難である • データ形式や収集方式の標準化が必要である
リソース配分（金・人）	• 現在の予算の割り当てではCDMの導入・維持が困難 • Agency側の人的リソースも厳しい状態である • より長期的にサポートを得られるようなリソース計画が必要である
スキル・能力	• 政府横断的な、ITおよびセキュリティに関する概念的およびハンズオンのトレーニングがより必要である • Agency側のCDMに対する知識やインテグレータの管理能力が不足している • インテグレータ側のCDMに精通しているスタッフが不足している
新技術領域への対応	• 今後政府機関のクラウドサービスの利用が増えると想定され、クラウドサービスへのプログラム提供が必要である • モバイルデバイスへのプログラム適用が必要である • 人工知能/機会学習、SOAR、RPAなどの技術を利用し、分析や対応の高度化・自動化を進めることが必要である

11.2. 課題に関する各情報源の記載詳細

11.2.1. CDM Referendum (Meri Talk)

Meri Talk が 2019 年に作成した CDM Referendum では、160 人以上の連邦政府及び業界関係者への調査にもとづき CDM プログラムに対する評価や課題が整理されている。

以下、主な記載内容を抜粋。

- CDM プログラムは、連邦政府のサイバーセキュリティを改善しているが、スピード、予算、文化的課題等の問題がある。
- 85%のステークホルダーは CDM によって連邦政府のサイバーセキュリティが改善されたと答えているが、大きな影響があったと答えたのはわずか 22%に過ぎない。
- 連邦政府と業界は、文化とトレーニングが CDM 成功の最大の障害であることに同意している。
- 連邦政府機関のわずか 27%しか、現在の予算配分で CDM の進捗を維持できると答えていない。DEFEND Task Order がプログラムに影響を与えるのに十分な時間があると確信している産業界の利害関係者は、15%とさらに少数である。
- 連邦政府は業界よりも寛容だが、CDM はペースを上げなければならないという点では両者とも一致している。
- DHS の CDM 管理の格付けを求められた際、連邦政府の A 評価と業界の D 評価が同数であった。
- 今後、DHS と業界は、DHS が CDM の早期採用とクラウド環境を再検討する必要があることに同意する。
- ステークホルダーは、CDM を進めるため、専門的なトレーニング、合理化されたプロセス、及び予算の詳細を推奨する。
- ステークホルダーは、Agency での成功は、反復的な採用、適応性、トレーニング、及びクラウド統合にかかっていると述べている。

11.2.2. Government Accountability Office (GAO) Report

GAO が 2020 年に CDM に関する課題を調査し、「図表 77 Asset Management の課題」のとおり報告している。現時点では、収集したデータ品質が低く、意思決定のためにダッシュボードを利用することが難しい点などが挙げられている。

また、「図表 79 その他の課題」のとおり、データ品質以外でもリソースやスキル等の課題があり、DHS を中心に対応している状況となっている。

図表 77 Asset Management の課題

Capability	概要	対応状況
HAWM	• ハードウェアインベントリに必要な情報が不足していた。 • 重複するハードウェア情報が含まれていた（約40%のハードウェアが重複した識別子を持っていた）	• DHSは2019年3月に、Agencyとインテグレーターがこの問題を解決するためのガイダンスを発行したが、2020年4月の時点では、解決されていない。
SWAM	• デバイスの誤作動やクラッシュの原因となったため、SWAMのツールを導入していないかった。	• CDM PMOは、2020年5月の時点で、Agency及びインテグレータと協力して、SWAMの要件をサポートする代替ソリューションの実装に取り組んでいた。
CSM	• 一部のシステムに導入されているOSのみ対応していた。 • 構成設定を連邦のコアベンチマークとAgency固有のバリエーションの両方と比較するときに、一貫性のないCDMツールを使用していた。	-（記載なし）
VUL	• 脆弱性が修正された時間は収集していなかった。 • ライセンス切れのため、CDMツールをタイムリーに更新していなかった。	• DHSはインテグレーターと協力して、脆弱性が修正された時間が含まれるようにしている。 • ツールのライセンスを取得、更新し、スキャンを実施しました。

参考文献 20.DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program より転記

図表 78 その他の課題

分類	課題	解決策
人員と資金	• CDMを実施するための、Agency側の人的リソースを過小評価または全く見積もりしていなかった。	• 人員と資金に関するリスクと解決するための手順を定義した。 • CDM ツールを継続的に資料するためのライセンス費用を賄う十分な資金が無い場合は、OMBと調整する。
インテグレータとの調整	• ネットワーク上のインテグレーターのインストールとCDMツールの構成をAgencyが直接監督できておらず、問題を解決するためにDHSのCDM PMOに依存する必要があった。 • PMOスタッフとインテグレーターとの会議の調整と出席にかなりの時間が必要であった。	• インテグレーターとの問題を解決するための、DHSからプログラムマネージャーを配置し、AgencyのCDMスタッフと定期的に連絡し、CDMを実施する際の問題を理解する役割を持たせた。
ソリューション	• ソフトウェア管理のツールを導入できず、SWAMの要件を満たしていなかった。	• インテグレータと協力し、Agencyの環境に合わせた代替ソリューションをみつけた。 • CDMの契約により、初期ソリューションに加え、カスタマイズされた追加のサービスをインテグレータに依頼することが可能となった。
スタッフ	• インテグレータの後続スタッフの専門知識が不足しており、期限超過や実施が進まない原因となっている。	• インテグレータがどれだけ迅速に適切なスキルを持った人材を調達・雇用し、重要な人材を保持していたか等の指標を毎月参加機関から収集した。 • インテグレータのスタッフに関連する問題をエスカレーションするための追加の手段を機関に提供した。

参考文献 20.DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program より転記

11.2.3. Meri Talk Web Site

Meri Talk は、CDM 業界関係に対して CDM の 7 年後の想定に関してヒアリングを行い、それに対して 10 社が回答している。以下、回答全体の要約と各社コメントを抜粋して記載。

① 回答全体の要約

- CDM プログラムのミッションである連邦政府機関のサイバーセキュリティの向上は変わらないが、その目標を達成するためのツールやアプローチは急速に進化している可能性があるという点で大方の意見が一致している。
- 技術面では、多くの業界関係者が、CDM のミッションを支援するための人工知能（AI）やロボティック・プロセス・オートメーション（RPA）技術の重要性が高まっていることを指摘した。また、インフラの面では、連邦政府機関によるクラウドサービスの採用が増えることで、より良いセキュリティの目標に近づけるマネージドセキュリティサービスの利用が増えることに多くの関係者が同意した。

② Red Seal 社(Christine Carberry, Vice President-Federal Business Unit at Red Seal)

- クラウドベースの製品の採用が増え、セキュアな必要があるアプリケーションをクラウドに置くことが増えると想定している。
- Software-Defined Networking (SDN)、クラウド環境、物理環境を可視化して、全てがどのように接続されているかを認識できるようにすることが重要になってくる。
- それら全てのクラウドコンポーネントがどのように接続されているかを可視化することは数年前よりも重要になってきている。
- 2012 年にプログラムが始まった時にはクラウドと SDN へのシフトは実際には進んでいなかったが、6 年後にはユビキタスになっているだろう。

③ Splunk 社 (Adilson Jardim, AVP of Sales Engineering, Public Sector, at Splunk)

- 1 つ目は、既存の資産、インベントリ、体制を理解することに焦点を当てている。機関がアプリケーション、ハードウェア、インフラストラクチャをアップグレードすると、その内部の仕組みは徐々に、ほとんどの場合は段階的に変化していくだろう。
- 2 つ目は、IT の近代化とクラウドサービスの採用ペースの加速に焦点を当てている。これまで以上に多くのイノベーションを顧客に提供できるようになる。このイノベーションの恩恵を受けるためには、機関は CDM プラットフォームのデータがどのようにアプリケーションやパターンを特定し、最適な移行先を見極めることができるかを検討する必要がある。
- 例えば、どのようなアプリケーションが古くなっているか、あるいは利用されていないのか、また、混乱を最小限に抑えながら、どのようなミッション・サービスがクラウドベースのサービスの恩恵を受けられるだろうか等を検討する必要がある。

- Federal Risk and Authorization Management Program (FEDRAMP)の成功により、検討すべきクラウドサービスプロバイダの数が増え続けており、これが続けば、CDM のキャパシティは、オンプレミス、クラウドベース、ハイブリッドの機能を含む、はるかに多様なセットを含むように進化していくだろう。

④ Broadcom 社 (Jodi Kohut, Director of Partners and Programs at Broadcom)

- 政府はセキュリティ態勢を継続的に監視したいと考えているため、ミッションはおそらく変わらないだろう。
- テクノロジーが進化するにつれ、政府は人工知能、機械学習及び基礎となるネットワーク コンポーネントを最大限に活用して、予測可能で応答性が高く、自動化されたコンテキストを意識したセキュリティ境界を実現することができるようになると期待している。

⑤ Elastic 社(George Young, Vice President of U.S. Public Sector at Elastic)

- 新たなリスクに対処するために、新しいツールやより洗練されたセンサーが開発されると想定するが、変わらないのは、スケーラブルな検索技術の必要性である。
- このプログラムでは、脅威検出のためのより積極的な姿勢を継続し、膨大なデータセットの中から異常を特定し、攻撃を修正するためのターゲット検索を行う能力を優先していく。
- これは、敵対者の一歩先を行くためには非常に重要なことである。検索技術と急速に進化する機械学習ツールを組み合わせることで、自動化を引き続き合理化し、セキュリティチームは人間のインテリジェンスを最も差し迫ったリスクに集中できるようになる。また、サイバーセキュリティソリューションのコードベースの透明性が標準となり、個々のツールを排除し、より複数の分野にまたがるプラットフォームに移行することで攻撃の表面を減らすことに焦点が当てられるようになると予測している。

⑥ Forescout 社 (Erik Floden, Director of Global Strategic Alliances at Forescout)

- CDM のミッションは、リスクを特定して軽減するための連邦政府の要件と密接に連携しており、その結果、時間の経過とともに一貫性を保つことになるだろう。
- しかし、このプログラムが将来的にどのようにツールやサービスを機関に提供するかという点については、あまり一定ではなく、将来的には 2 つの大きな変動要因がある。
- 1 つ目は、機関が CDM のサービスをマネージドサービスとして、特に中規模・大規模の機関が、どれぐらい早い期間で CDM のサービスを利用するかということである。
- 2 つ目は、プログラムの成功にとって基本的なことであり、機関がリスクの特定と軽減のために DHS が提供する CDM ツールとサービスをうまく利用できるかどうかである。識別されたリスクを軽減し、企業のセキュリティを向上させるためには、機関がどの程度のペースで取り組むかが重要になる。

⑦ Forcepoint 社 (Eric Trexler, Vice President, Global Governments and Critical Infrastructure, at Forcepoint)

- CDM の状況に関する 2018 年のフォースポイントの調査では、多くの根本的な課題が、CDM 目標の達成に向けた省庁の進捗を遅らせていることが明らかになり、CDM プログラムが最善の努力をしているにもかかわらず、これらの課題は現在も当てはまっている。
- 進展があり、グループ F の機関がプログラムに参入し、CDM への資金提供要請が増加し続けている一方で、多くの機関は、機関の次のステップを計画的に計画しているにもかかわらず、あまりにも遅々として進んでいる。
- 敵対勢力は、機関の最善の努力を追い越しており、新たなセキュリティアプローチが必要とされている。

⑧ Tenable 社 (Chris Jensen, Public Sector Business Development Manager at Tenable)

- 確かに、プログラムの寿命は、現在のタスクオーダーのパフォーマンス期間を超えても、ずっと続くように思える。下院と上院の両方で、CDM プログラムを成文化して拡大するための法案が提出された。
- さらに、CISA は、ホワイトハウスからサイバーに関する連邦政府の「品質サービス管理局」としての役割を果たす追加権限を与えられており、今後も必要に応じて CDM プログラムを適応させ、進化させていくことを可能にする「拘束力のある運用指令」を発行している。
- 主なテーマは、共有サービスと一般的な統合である。
- 初日から、CDM は、すべての連邦政府機関をサイバーセキュリティの一貫した基準に引き上げる努力をしてきた。 将来的にその一貫した基準を達成するためには、CISA によって定義され、実施されているように、連邦企業の統合、統合、集中化をさらに進める必要がある。 CISA の影響力はまた、産業制御システム（ICS）などの運用技術を含むわが国の重要インフラ全体を CDM の傘の下に置くことで、CDM プログラムの範囲を拡大することにもなる。

⑨ Zscaler 社 (Stephen Kovac, Vice President of Global Government and Compliance at Zscaler)

- 1 つの可能性としては、CDM が脅威データの SaaS ベースのリポジトリになり、ツールやダッシュボードを提供しながら、収集したデータから得られるインサイトをリアルタイムで機関に共有することが考えられる。
- CDM プログラムは、自社のインフラストラクチャを展開してデータを収集するのではなく、将来的には、CDM が所有するハードウェアやシステムを展開しなければならないというコストや課題を抱えることなく、クラウドサービスプロバイダから収集されたデータに依存するようになるかもしれない。

- このモデルにおける CDM プログラムの主な役割は、大規模なセキュリティデータウェアハウスと脅威分析・警告システムとしての役割を果たすことであり、リアルタイムでのセキュリティ状況認識を提供する多機能なベンダーに依存しないダッシュボードに統合されている。

⑩ ManTech 社 (Seana McMoil, Senior Executive Director & Branch Manager, National Cybersecurity Programs, at ManTech)

- ManTech は、CDM の導入を最初に選択した企業の 1 つであり、当社のサイバーチームは、連邦政府の現場での広範な CDM の経験を持っている。私たちは、テクノロジーが変化し、セキュリティリスクも変化することを知っている。
- ロボティック・プロセス・オートメーションのような新しい技術やイノベーションは、セキュリティリスクに対処し、サイバーチームを強化するために開発または成熟し続けている。
- 当社は、変化する脅威の状況の中で存在するリスクを軽減するために、機関が適切な立場にあることを保証するために投資を行っている。
- 当社のツールにとらわれないアプローチは、進化するサイバー脅威から連邦政府機関を守るために、関係者に革新的なソリューションを継続的に評価し、導入していることを保証している。

⑪ Trustwave Government Solutions (Bill Rucker, President of Trustwave Government Solutions)

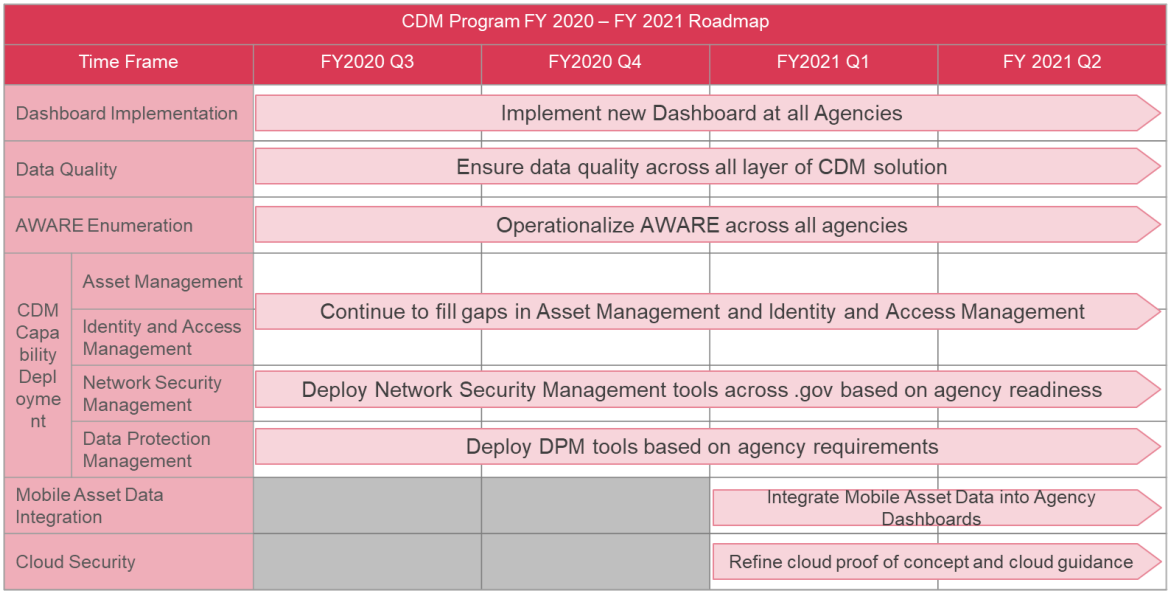
- プレーヤーは変わるかもしれないが、ゲームは変わりません。機関のミッションを守るためにリスクとなるのはデータである。これまで進化している脅威から守るための技術がなければならない。
- 私たちは、サイバー犯罪者や国家からの攻撃に常に直面しており、特に検知を回避したり、初歩的なソーシャルエンジニアリングで防御を迂回したりする能力が高度化している。
- データが指数関数的な速度で増加し続け、Internet of Things や環境に新たなアプリケーションが追加されることで攻撃のベクトルが作られるようになると、より迅速な検知能力が重要になってくる。
- Trustwave の継続的モニタリングソリューションにおける AI、機械学習、Security Orchestration, Automation, and Response (SOAR)への投資は、当社のイノベーションと先を行くために非常に重要なものとなっている。

12. ロードマップ

12.1. ロードマップ

CDM の FY2020 から FY2021 のロードマップは、「図表 79 CDM ロードマップ」のとおり。

図表 79 CDM ロードマップ



参考文献 6.CDM CENTRAL TALES FROM THE FRONTLINES より転記

12.2. 優先項目

FY2020 と FY2021 に優先する項目は、「図表 80 CDM の優先事項」のとおり。これらの優先事項に加えて、継続してデータ品質向上に取り組んでいる。

図表 80 CDM の優先事項

項目	概要
Enterprise Mobility Management	モバイルディスカバリーの完了後、モバイル資産データを介してエージェンシーエンタープライズモビリティ管理をエージェンシーダッシュボードに統合する作業を開始する。
Proof of Concept CDM Dashboard	新しいCDM Dashboardのコンセプトを、最初はラボ環境で、次に参加機関と共同で実証する。
Proof of Concept Cloud Security	クラウドディスカバリーが完了した後、DHSチーム、機関、システムインテグレータ、DHSサイバーセキュリティ部門のパートナーと協力して、クラウドセキュリティの概念実証のための適切なアプローチと範囲を決定する。
High Value Assets	HVAに対するデータ保護(Phase4)のパイロット／概念実証の参加機関を拡大する (DEFENDグループごとに少なくとも1つのパイロットを持つ)
Asset Management and Identity and Access Management Gap Fills	既存の作業を継続し、Asset ManaementおよびIdentity and Access Managementのイニシアチブに関するギャップを埋める。

参考文献 6.CDM CENTRAL TALES FROM THE FRONTLINES より転記

12.3. モバイル、クラウド、データ品質

モバイル管理とクラウドセキュリティ、データ品質に関する進捗状況は、「図表 81 モバイル・クラウド・データ品質の進捗状況」のとおり。

また、クラウドに関しては、Amazon Web Service 社、Microsoft 社ともに、CDM の Capability に対応するために対協可能な自社のサービスの情報について自社サイト等に掲載している。

図表 81 モバイル・クラウド・データ品質の進捗状況

Enterprise Mobility Management		• エンタープライズ・モビリティ管理業務の開始が間近に迫っている • モバイル資産の可視性、保護、管理を強化し、Agencyを支援する • モバイル脅威防御（MTD）、モバイル・アプリケーション・ベッチン グ（MAV）など、新たなモバイル能力に焦点を当てた国家サイバーセキュリティ・センター・オブ・エクセレンス（NCCoE）のラボ・インスタンスとの協働 • 連邦モビリティグループ（FMG）およびFISMAモビリティメトリクス作業部会との緊密な連携
Cloud Security		• 中小企業庁と共同でCDMクラウド移行パイロットを実施中 • CISAのチーフテクノロジーオフィスとスレットハンティングは、Amazon Web ServicesやMicrosoft Azureと連携して、Agency顧客のサイバーセキュリティ意識をサポートしています。 • ネイティブツールとサードパーティツールを使用したAgencyとのクラウドディスカバリーのパイロット • クラウドにおけるアイデンティティとアクセス管理に焦点を当てたNCCoE Labインスタンス • CDM は CISA Trusted Internet Connections（TIC）3.0 チームと密接に連携している
データ品質	CDMデータ管理チーム（DMT）	• CDMソリューションの完全性、正確性、タイムラインなど、強化されたデータの「要件」を定義するタスクを持つチームを結成した • DMTは6月にこれらの要件を運用し、2020年度の残りの期間に学んだベストプラクティスと教訓を特定する
	CDMデータ品質管理計画（DQMP）	• 最近、DMTの調査結果の概要を説明する機関およびシステムインテグレーターに配布された • 要約データを認証するために定量的および定性的基準の組み合わせを使用するCDMデータ認証ルーブリックが含まれている • FY21第4四半期末までに、すべてのCFO Act AgencyがDQMPを利用して、認証を取得できない場合は、OMBとCISAに書面による正当な理由を提出しなければならない。(OMB Directiveより)

参考文献 6.CDM CENTRAL TALES FROM THE FRONTLINES より転記

13. 常時診断システム導入に向けた検討項目

13.1. 検討項目一覧

本調査を踏まえ、常時診断システムを日本に導入するためには、「図表 82 検討事項一覧」のとおり、様々な課題があると考えられる。これらは、米国政府と比べた場合に、導入の前提となる、法令(FISMA)が無いことや、政府機関内の役割分担が明確ではないことが起因して発生しているものが主であると考えられる。

図表 82 検討事項一覧

カテゴリ	検討事項
対象	**1. CDMプログラムの対象範囲** 中央省庁、地方公共団体、独立行政法人など、どの範囲までを対象とするのかを検討する
組織	**2. DHS相当の管理組織はどこが担うのか** Federalダッシュボードの管理・運用、機能要件・運用要件等の整備、予算管理 などの管理組織を検討する **3. GSA相当の管理組織はどこが担うのか** ツールの選定・インテグレーターの選定、調達管理 などの管理組織を検討する **4. OMB相当の管理組織はどこが担うのか** セキュリティ対策状況の報告先 などの管理組織を検討する **5. ツール・インテグレーターの選定方法** 前例のない日本内で、どのツール・インテグレーターを選定するのか検討する必要がある。インテグレーターへの教育・共同研究なども必要となる場合がある。
技術	**6. システム統一・標準化への対応方針への検討** CFO Act agenciesにおいて、全て別々の仕組みを導入するのか、統一・標準化を行うのか検討する **7. シェアードサービスの構築** Non-CFO Act agenciesに提供する、シェアードサービスを誰がどのように構築するか検討する **8. クラウドバイデフォルトへの対応** CDMプログラムを実施する際に、クラウドサービスの利用可否を検討する
運用	**9. 各ダッシュボードの可視化内容及び分析内容** ダッシュボードを利用した運用の詳細(または管理組織)を検討する **10. リスク可視化方式** スコアリングの方式や優先順位の考え方、算出方式(または管理組織)を検討する **11. 運用サイクルの検討** データ収集、可視化、対応、見直しの一連のサイクルや運用フロー(または管理組織)を検討する

13.2. CDM 構築の前提に関する米国・日本の状況・相違点整理

「13.1 検討項目一覧」の記載事項の検討を行うにあたり、法令・制度など CDM プログラムを構築する上での前提として米国で整備されている各種事項に関する日本の状況・相違点(検討時の留意点)は、「図表 83 米国・日本の状況及び相違点整理」のとおり。

図表 83 米国・日本の状況及び相違点整理

項目	米国の状況	日本の状況・米国との相違点 (検討時の留意点)	関連する検討事項(前頁)
関連法令・制度の整備	FISMAにもとづき、関係省庁の役割・責任範囲を定義し、CDM関連ツールの導入、常時診断・緩和、報告を義務付けている	CDMの導入や政府機関の役割・責任範囲について定義し、省庁横断的なデータ収集やリスク対応状況の閲覧の権威付けや報告を義務化するための法令・制度や仕組みの整備が必要	1.CDMプログラムの対象範囲 2.DHS相当の管理組織はどこが担うのか 3.GSA相当の管理組織はどこが担うのか 4.OMB相当の管理組織はどこが担うのか 11. 運用サイクルの検討
費用負担、シェアードサービス提供基準	CFO Act(首席財務官法)上のCFO Act AgencyとNon-CFO Act Agencyに分類し、費用負担の方針やシェアードサービスを提供有無を分けている	CFO Actと同等の基準がないため、独自の基準整理が必要	7. シェアードサービスの構築
製品・ツール調達方針	APL(承認済製品リスト)を整備し、リスト中の製品・ツールから選定して導入する仕組みになっている	製品候補からの選択式での調達や、ツールが満たすべき要件を省庁横断的に共通要件として定義し調達仕様上に反映させるための制度や仕組みの整備が必要	5. ツール・インテグレーターの選定方法 6. システム統一・標準化への対応方針への検討

14. 参考文献

14.1. WEB ページ

参考文献1. Securing Federal Networks
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, Securing Federal Networks, https://www.cisa.gov/cdm

参考文献2. Continuous Diagnostics and Mitigation (CDM)
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, Continuous Diagnostics and Mitigation (CDM), https://us-cert.cisa.gov/cdm/home

参考文献3. Continuous Diagnostics & Mitigation (CDM) Program
U.S General Services Administration, Continuous Diagnostics & Mitigation (CDM) Program, https://www.gsa.gov/technology/technology-products-services/it-security/continuous-diagnostics-mitigation-cdm-program

参考文献4. OMB sets new CDM data standards deadline for agencies
FEDERAL NEWS NETWORK, OMB sets new CDM data standards deadline for agencies, https://federalnewsnetwork.com/reporters-notebook-jason-miller/2020/11/omb-sets-new-cdm-data-standards-deadline-for-agencies/

参考文献5. CONTINUOUS DIAGNOSTICS AND MITIGATION TRAINING
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, CONTINUOUS DIAGNOSTICS AND MITIGATION TRAINING, https://www.cisa.gov/cdm-training

参考文献6. CDM CENTRAL TALES FROM THE FRONTLINES
Meri Talk, https://www.meritalk.com/event/cdm-central-may-2020/faqs/, CDM Keynote with Kevin Cox, CDM Program Manager, CISA Presentation

14.2. 文書

参考文献7. HWAM Capability Description
https://us-cert.cisa.gov/cdm/resources, HWAM_CapabilityDescription.pdf

参考文献8. CDM Technical Capabilities Volume Two Requirements Catalog 2020
https://www.gsa.gov/technology/technology-products-services/it-security/continuous-diagnostics-mitigation-cdm-program, CDM Technical Capabilities Volume Two Requirements Catalog 2020 [PDF - 2 MB]

参考文献9. CDM Technical Capabilities Volume One Actual Desired States
https://www.gsa.gov/technology/technology-products-services/it-security/continuous-diagnostics-mitigation-cdm-program, CDM Technical Capabilities Volume One Actual Desired States [PDF - 652 KB]

参考文献10. CDM PROGRAM SHARED SERVICES PLATFORM FACT SHEET
https://www.cisa.gov/publication/cdm-program-shared-services-platform, CDM Program Shared Services Platform Fact Sheet

参考文献11. Description of Generic Sensor Types for the Continuous Diagnostic and Mitigation (CDM) Collection System
https://us-cert.cisa.gov/sites/default/files/cdm_files/DescriptionofGenericSensorTypesfortheCDMCollectionSystem.pdf
参考文献12. CDM Approved Products List
https://www.gsa.gov/technology/technology-products-services/it-security/continuous-diagnostics-mitigation-cdm-program, CDM Approved Products List (APL) [XLSX - 15 MB]
参考文献13. Privacy Impact Assessment for the Continuous Monitoring as a Service (CMaaS)
https://www.dhs.gov/publication/dhsallpia-082-continuous-monitoring-service-cmaas, DHS/ALL/PIA-082 Continuous Monitoring as a Service (CMaaS) - February 2020
参考文献14. Elastic for CDM Overview
https://www.elastic.co/jp/videos/cdm-dashboard-2-with-elastic-ecs, elastic-for-cdm.pdf
参考文献15. HWAM Capability Data Sheet
https://us-cert.cisa.gov/cdm/resources, HWAM_CapabilityDataSheet.pdf
参考文献16. SWAM Capability Data Sheet
https://us-cert.cisa.gov/cdm/resources, SWAM_DataSheet.pdf
参考文献17. CSM Capability Data Sheet
https://us-cert.cisa.gov/cdm/resources, CSM_DataSheet.pdf
参考文献18. VULN Capability Data Sheet
https://us-cert.cisa.gov/cdm/resources, VUL_DataSheet.pdf
参考文献19. CDM Roles & Responsibilities Guide
https://us-cert.cisa.gov/cdm/guides, FNR_CPM_GDE_CDMRRGuide.PDF
参考文献20. DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program
https://www.gao.gov/products/gao-20-598, 708885.pdf
参考文献21. CDM PROGRAM AWARE SCORING
https://www.cisa.gov/publication/cdm-program-aware-scoring-fact-sheet, CDM Program AWARE Scoring Fact Sheet
参考文献22. Strengthen Federal Cybersecurity January 2021
https://trumpadministration.archives.performance.gov/homeland_security/APG_dhs_2.html, FY2021_january_Strengthen_Federal_Cybersecurity.pdf

契約管理番号： 20002062-0