仕様書

ＩｏＴ推進部

1. 件名

Connected Industries 推進のための協調領域データ共有・AI システム開発促進事業／
米国政府の CDM Program を参考にした常時診断システムの実現性調査

2. 目的

近年、サイバー攻撃が高度化・巧妙化する一方で、クラウドサービスの利用拡大やリモートワークの普及などにより標的となるシステム環境も大きく変化してきている。このような状況下において、従来のオンプレミス型を前提とした境界監視やインシデントレスポンス体制といった現状のセキュリティ対策についても見直しの必要が出てきている。また、デジタル時代における新たなセキュリティ対策の在り方として、ゼロトラストアーキテクチャの検討も進められており、新たなシステム環境やアーキテクチャに有効かつ整合性の取れたセキュリティ対策を検討する必要性が高まってきている。

このような背景を踏まえて、昨年度、米国の連邦政府機関にて導入されている、Continuous Diagnostics and Mitigation (CDM)プログラムの基礎調査を実施した。本年度は、この調査結果を元に、日本の政府機関への導入を想定した適合性の確認、課題・改善点の抽出を行うための調査事業を委託する。

本調査事業では、米国 CDM プログラムをベースに検証環境を準備し、既存ツールや各種資産管理システムからのデータ収集、ダッシュボード上でのリスク可視化・診断、是正・緩和等の常時診断に関する機能面及び運用面での実現性の検証を行い、日本の政府機関で導入する際の課題や留意事項、運用方法等についての考察を行うことを目的とする。

3. 内容

3.1. 概要

3.1.1. 調査事業の概要

本調査事業では、米国 CDM の事例を参考に、「Federal Dashboard 機能」、「Agency Dashboard 機能」、「CMaaS 機能」、「Sensor 等機能」を実環境上に準備し、「検証準備」、「検証項目の確定」、「検証環境の準備」、「検証実施」、「検証結果考察」、「検証結果報告」を実施する。

なお、CDM プログラムは次の①から④のアプローチで実施されるものであるが、本検証では③を検証のメイン項目と位置づけ、①から③は実機検証、④は机上検証を行うものとする。

① Policy Definition
- Desired State (理想状態)の定義

② Data Collection
- Actual State (現状)のデータ収集

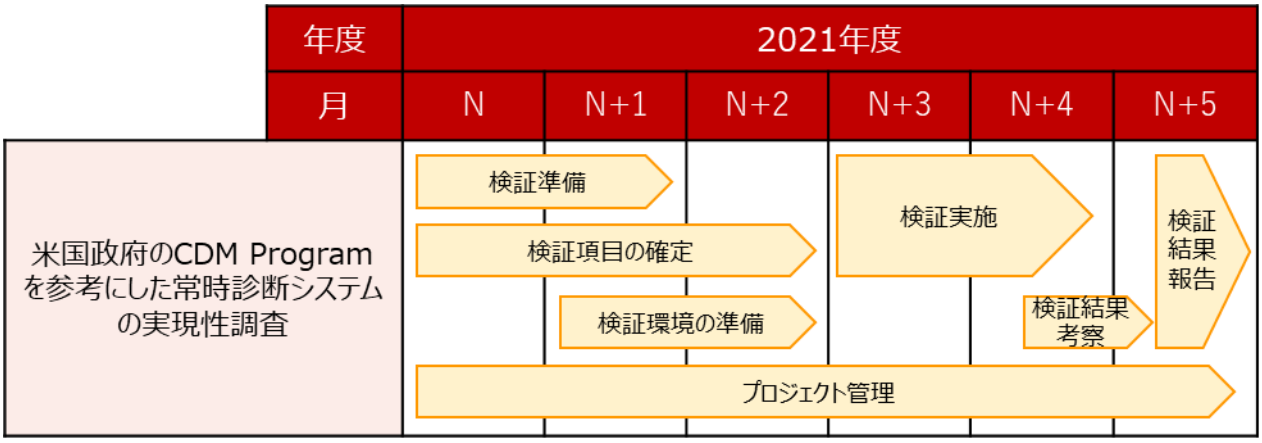
③ Diagnose (Find/Prioritize Defects)
- Desired State と Actual State のギャップの可視化
- リスクスコアリング(AWARE: Agency-Wide Adaptive Risk Enumeration)の算出

④ Mitigate Defects
- “Worst Problems First”の考え方に基づくギャップやリスクへの対応
- セキュリティ対策、Desired State の見直し

3.1.2. 想定スケジュール

本調査事業の想定スケジュール案を「図表 1　想定スケジュール」に示す。なお、本仕様書の要件を満たす範囲内で、より合理的なスケジュールが提案できる場合、このスケジュール案の変更は可とする。

図表 1　想定スケジュール



3.2. 委託作業の内容

3.2.1.検証準備

3.2.1.1. 統一基準に基づき自組織の情報を活用し検証する場合のルールの整理

今回の調査事業では、自組織で実際に利用している基盤システム等のデータを活用した検証を行うことが想定されている。検証を実施するにあたっては、政府機関や独立行政法人等が参照すべき「政府機関等の情報セキュリティ対策のための統一基準」準拠に必要となる対応、及びその手順化方針を検討すること。

「政府機関等の情報セキュリティ対策のための統一基準」で想定される関連部分は、「3.1.1 情報の取扱い」（情報の取扱いに係る規定の整備、情報の目的外での利用等の禁止、情報の格付け及び取扱い制限の決定・明示等、情報の利用・保存、情報の提供・公表、情報の運搬・送信、情報の消去、情報のバックアップ等）と考える。

なお、これ以下の内容に関しては、ここで整理したルールに基づき検証作業を進めること。

3.2.1.2. データ項目の確定

収集するデータ項目及び各 Dashboard に表示する項目を確定すること。

実機検証に関しては、「図表 2　検証優先度」に記載している、優先度「高」の Capability を必須としており、「別紙 1.　データ項目案」及び「図表 12 Federal Dashboard 表示項目例」、「図表 10 Agency Dashboard 表示項目例」を参考として、環境や選定したツールの機能や特性を踏まえ、本検証環境において収集・保管等の取扱いを行うデータ項目及び各 Dashboard に表示する項目を確定させること。

なお、優先度「低」の Capability を実機検証する場合も、同様に収集するデータ項目及び各 Dashboard に表示する項目を設計・確定すること。

データ項目の確定に際しては、データ定義書を作成し、NEDO の承認を得た上で提出すること。

3.2.1.3. リスクスコアリング方法の確定

リスクスコアリング方法に関しては、AWARE の考え方をもとに、インプットとする Metric および算出式を見直し・検討し検証用に定義すること。

原則として、「別添.　米国 CDM 事例」に記載している、米国の AWARE を踏襲することを想定しているが、選定した CDM ツールの機能や、日本へ導入する際の考慮点があれば反映すること。リスクスコアリング方法の確定に際しては、AWARE を踏襲する場合でも、リスクスコアリング定義書を作成し、NEDO の承認を得た上で提出すること。

3.2.2.検証項目の確定

3.2.2.1. 実機検証

本検証作業で実施する検証項目を作成すること。

本検証では、限られた時間・環境の中で効果的な検証を実施するために、「図表 2　検証優先度」のとおり、各 Capability に関して検証優先度を設定している。実機検証に関しては、優先度「高」の Capability を必須としており、「別紙 2.　検証項目案」を参考として、環境や選定したツールの機

能や特性を踏まえ、検証項目を確定すること。

実機検証項目の確定に際しては、NEDO の承認を得た上で、実機検証仕様書を作成し提出すること。なお、実機検証を対象外とした Capability に関しても、机上検証または考察は行うものとする。

優先度　高：実機検証は必須、収集範囲や収集方法については提案・協議可能

優先度　低：実機検証は提案・協議可能。

図表 2　検証優先度

#	Phase	Capability	優先度	備考
1	Asset Management	HWAM	高	
2		SWAM	高	
3		CSM	高	
4		VUL	高	
5		EMM	高	
6	Identity and Access Management	TRUST	高	
7		BEHAVE	低	Learning Management System が導入されている場合は、CMaaS とのデータ連携を検証する。
8		CRED	高	
9		PRIV	高	
10	Network Security Management	BOUND	低	SIEM 製品で統合管理され、#11,12 で BOUND の情報も連携される想定のため、個別の検証要件無し。
11		MNGEVT	高	
12		OMI	高	
13		DBS	低	設計・開発中の Capability であるため、個別の検証要件無し。
14	Data Protection Management	DISCOV	低	Data Protection Management System が導入されている場合は、CMaaS とのデータ連携を検証する。
15		PROT	低	
16		DLP	低	
17		SPIL	低	
18		IRM	低	

3.2.2.2. 机上検証

「3.1.1 調査事業の概要」で記載したとおり、ダッシュボードで特定したリスクの是正処置について机上検証を実施すること。

机上検証とは、予め是正処置の運用フロー(案)を整備した上で、複数人の机上検証実施者が実際の Dashboard の表示内容と運用フロー(案)を見ながら、是正処置運用のウォークスルーを行い、問題なく運用可能か検証し、課題・問題点を抽出した上で、運用フロー(案)の修正や検証結果の考察を行

うことを想定する。

なお、Federal Dashboard と Agency Dashboard では表示項目や是正処置の運用・対応が異なることに留意し、各運用フロー(案)を事前に作成した上で実施すること。

机上検証項目の確定、各運用フロー(案)の作成に際しては、NEDO の承認を得た上で、机上検証仕様書を作成し提出すること。

なお、他に机上検証対象とした項目・Capability があれば、同様に机上検証仕様書に記載すること。

3.2.3. 検証環境の準備

本検証作業を実施する検証環境を準備すること。検証環境の要件は「3.3 検証作業の要件」を参照し、検証環境の構成を決定すること。また、本検証作業で使用するソフトウェア・ハードウェア等は新規に準備するものか、既存のものかを問わず、検証環境に関しての情報をまとめた検証環境定義書を作成し、NEDO の承認を得た上で提出すること。

なお、本検証作業は CDM プログラムの実運用を通して検証・課題抽出を行うことを目的としているため、提案者が業務で利用している実環境に検証環境を準備すること。

3.2.4. 検証実施

「3.2.2 検証項目の確定」で作成した検証項目を実施すること。

3.2.5. 検証結果考察

本検証結果および日本の政府機関で導入する際の課題や留意事項等について考察を行うこと。考察内容は主に以下を想定するが、NEDO と調整の上で確定すること。また、必要に応じて検証中のデータを用いて改善策の検証を行うこと。

- Federal Dashboard の表示項目
- Agency Dashboard の表示項目
- 各ダッシュボードを利用した是正処置の運用フロー、運用頻度
- ダッシュボード間のデータ連携
- リスクスコアリング方法
- その他、NEDO から依頼された事項

3.3. 検証作業の要件

3.3.1. 検証環境概要

3.3.1.1. 検証に必要な機能

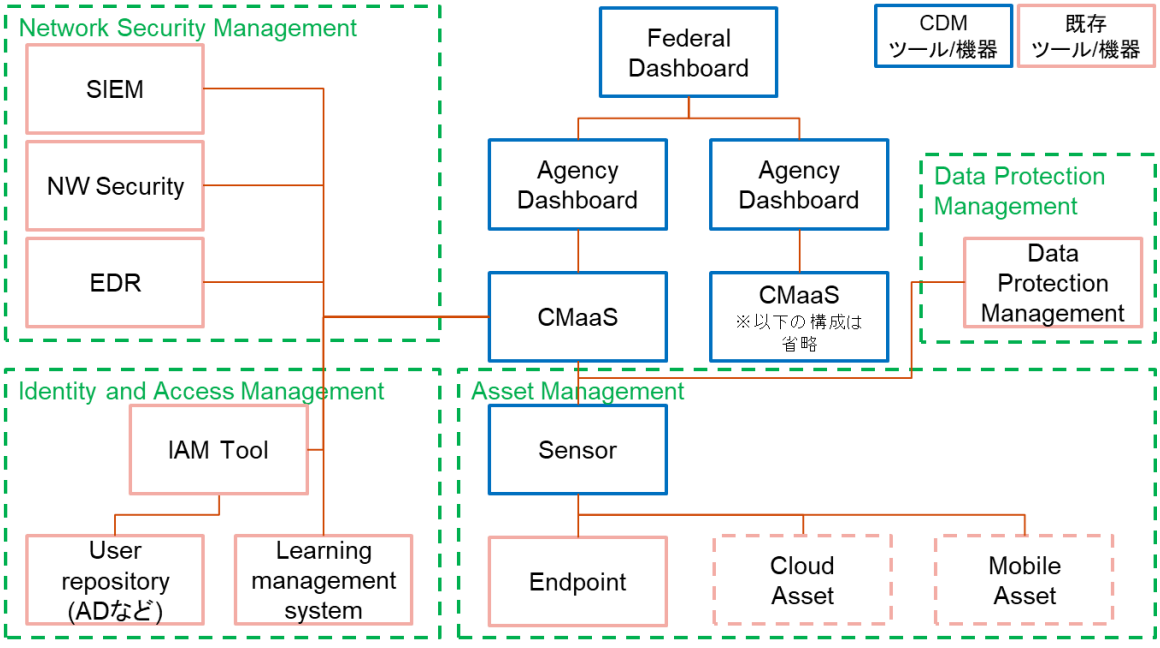
実環境（提案者が実際に業務に利用している環境）に本検証作業を実施可能な CDM の管理・運用に必要となるハードウェア・ソフトウェアの検証環境を準備する。

本検証環境は、「図表 3　検証環境全体構成図」のとおり、CDM ツール/機器とそれに接続する既存ツール/機器で構成される。「Federal Dashboard 機能」、「Agency Dashboard 機能」、「CMaaS 機能」、「Sensor 等機能」の各機能に対して、要件に沿った製品を導入・設定を行うことで、機能を実現すること。

既存ツール/機器に関しては、既に構築されている場合は、新規導入は行わず、構築済みのツール/機器で代替することを原則とする。

なお、米国の CDM プログラムでは、General Services Administration(GSA)が、「参考文献 3. Tools Special Item Number(Tools SIN)」及び「参考文献 4. Approved Products List(APL)」として Department of Homeland Security(DHS)が承認したソフトウェアを公開しており、DHS が「参考文献 7. Privacy Impact Assessment for the Continuous Monitoring as a Service (CMaaS)」に整理しており、これらを検証環境準備の参考とすること。

図表 3　検証環境全体構成図



3.3.1.2. データ収集対象

データ収集対象とする Endpoint に関しては、「図表 4 Endpoint の種類」のとおり想定している。具体的な対象は、提案者の提案を元に、NEDO と協議の上決定すること。

図表 4 Endpoint の種類

No	種別	概要	想定する条件
1	職員端末	職員が日常業務で使用している端末	・数十から数百台 ・Windows 10 環境を検証可能なこと
2	システムサーバ(オンプレ)	文書管理、経理処理　等の個別システムであり、オンプレミス環境で構成されているシステム	・主な OS のバリエーションを検証可能なこと (Windows Server、Linux など)
3	システムサーバ(クラウド)	文書管理、経理処理　等の個別システムであり、クラウド環境で構成されているシステム	・主なクラウドサービスを 1 つ以上検証可能なこと (AWS、Azure など)
4	モバイル端末(公用、BYOD)	携帯端末、タブレット端末等の政府機関から配布されたモバイル端末	・主な OS のバリエーションを検証可能なこと (iOS、Android など) ・主な MDM ソフトウェア(Mobile Device Management)を 1 つ以上検証可能なこと
5	複合機	コピー、FAX 等	・主な複合機を 1 つ以上検証可能なこと
6	NW 機器	FW、NW スイッチ、ルータ等	・特になし (特殊な NW 構成でないこと)

3.3.2. CmaaS の要件

3.3.2.1. 概要

CMaaS は、Sensor 等から収集した Endpoint のデータを集約・統合・正規化するデータプラットフォームである。様々なエンドポイントとのデータ連携が必要となるため、様々な製品・ツールとの相互運用性が必要である。各製品と接続する構成例を以下に示すため、これらを参考に最適な構成を検討すること。

3.3.2.2. ハードウェア要件

検証作業中に想定される収集データ量を、検証実施に支障をきたさず円滑に処理可能できるようハードウェアを構成すること。オンプレミス、クラウドは問わないものとする。

3.3.2.3. ソフトウェア要件

CMaaS 製品に必要な要件は、「図表 5 CMaaS 製品要件」のとおりであるが、本検証環境において実現する機能は、提案者の環境や選定したツールの機能や特性を踏まえ、提案すること。ただし、最終的な構成については、事業開始後に、NEDO と協議し決定すること。また、以下に記載する構成例を実現可能な製品を選定すること。

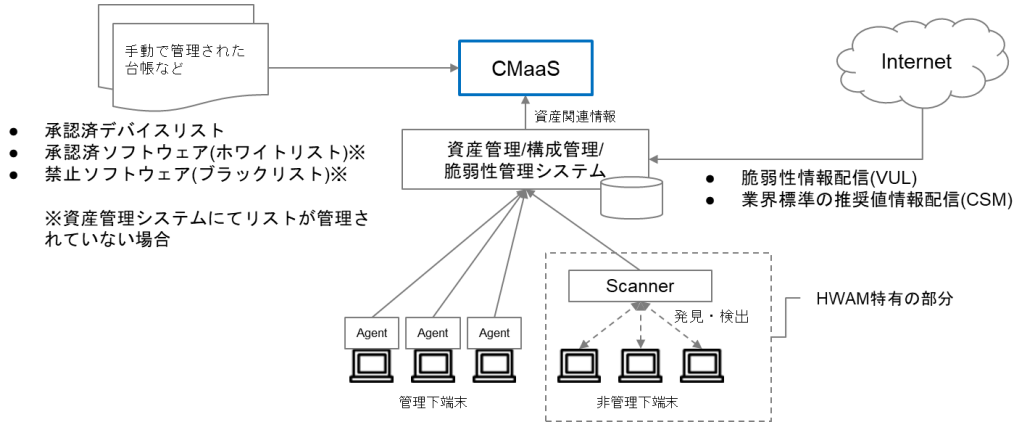
図表 5 CMaaS 製品要件

No	カテゴリ	要件
1	データ収集	・ テキストファイル形式のデータを収集できること ・ ログファイルなどの随時行が追加されるファイルについては、変更発生後に追加された差分のみを収集できること ・ RDBMS 上のデータに対してクエリを利用して収集できること ・ データを暗号化して転送できること
2	データ保管機能	・ 収集したデータは圧縮して保管できること ・ 収集したデータを保管するために RDBMS などのデータベースが不要であること ・ 収集したデータの改ざん防止機能を有すること ・ 収集したデータごとに、保持期間を指定できること

3.3.2.4. Asset Management 構成例

Asset Management で想定しているシステム構成の例は「図表 6 Asset Management 構成例」のとおり。

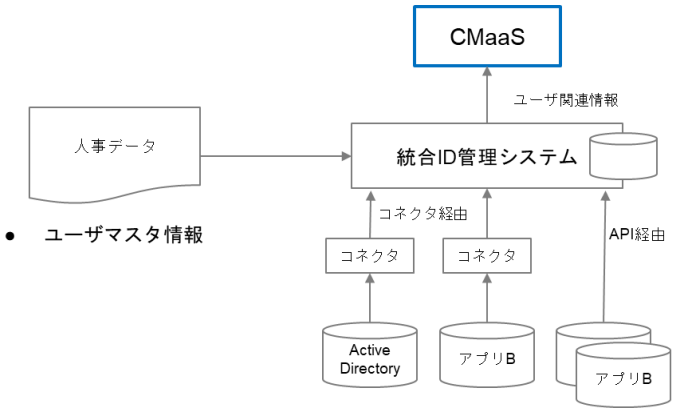
図表 6 Asset Management 構成例



3.3.2.5. Identity and Access Management 構成例

Identity and Access Management で想定しているシステム構成の例は「図表 7 Identity and Access Management 構成例」のとおり。

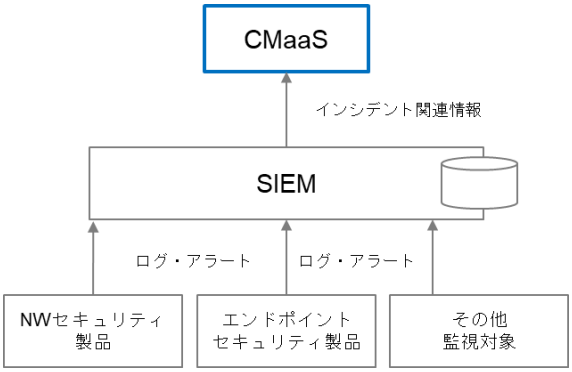
図表 7 Identity and Access Management 構成例



3.3.2.6. Network Security Management 構成例

Network Security Management で想定しているシステム構成の例は「図表 8 Network Security Management 構成例」のとおり。

図表 8 Network Security Management 構成例



3.3.3. Sensor 等の要件

3.3.3.1. 概要

Sensor 等は、CDM プログラムで監視する対象のエンドポイント及び監視対象の状態を収集するツールである。CDM では、ネットワーク上の IP アドレスが付与されている機器を監視対象として定義している。Endpoint の状態を収集する Sensor の種類は「図表 9 Sensor の種類」のとおりであるが、本検証環境において利用する Sensor の種類は、提案者の環境や選定したツールの機能や特性を踏まえ、提案すること。ただし、最終的な構成については、事業開始後に、NEDO と協議し決定すること。

図表 9 Sensor の種類

No	種別	概要
1	Active Network Sensor	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し収集するもの。
2	Passive Network Sensor	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収集するもの。
3	Asset Management Repository	組織内で、既に構築済みの他の目的の為に作成された、資産を管理し更新されるリポジトリ。
4	Network Event Sensor	特定の場所の特定のイベントを検出・収集する。Passive Network Sensor とは異なり、特定の条件を定義可能。
5	Endpoint-Based Sensor	デバイスに埋め込まれたソフトウェア・クライアント。

3.3.3.2. ハードウェア要件

検証作業中に想定される収集データ量を、検証実施に支障をきたさず円滑に処理可能できるようハードウェアを構成すること。オンプレミス、クラウドは問わないものとする。

3.3.3.3. ソフトウェア要件

「別紙 1. データ項目案」を参考に、必要なデータ項目が収集可能なソフトウェアを選定すること。

3.3.4. Agency Dashboard の要件

3.3.4.1. 概要

Agency Dashboard は、Agency のオブジェクトレベルのデータを収集し、Agency 全体のセキュリティリスクを可視化するダッシュボードである。

本検証では、CMaaS からオブジェクトレベルのデータを受領し、サマリデータや算出した AWARE スコアを表示し、問題が検出された際に対象の Endpoint を特定するなど、オブジェクトレベルのデータも保有する必要がある。

Agency Dashboard で表示する項目は「図表 10 Agency Dashboard 表示項目例」を参考として、提案者の環境や選定したツールの機能や特性を踏まえ、提案すること。ただし、最終的な構成については、事業開始後に、NEDO と協議し決定すること。

なお、本検証では、複数の Agency Dashboard と Federal Dashboard のデータ連携を検証項目とするため、2 つ以上の Agency Dashboard の準備が望ましい。また、1 つのレポジトリからビュー表示等で複数 Agency Dashboard を論理的に実現し、Federal Dashboard とデータ連携するのは 1 つであるといった構成は認められないことに留意する。

図表 10 Agency Dashboard 表示項目例

#	Capability	表示項目例	元データ (別紙 1 参照)
1	HWAM	総デバイス数	#1
2		サブシステム別デバイス数	#1,16
3		承認済デバイス数/割合	#1,17
4		未承認デバイス数/割合	#1,17,20
5		管理者割当済デバイスの数/割合	#1.18,20
6		利用 OS 別デバイス数/割合	#1,6,7,8
7		AWARE スコア(UAH)	#1,17,20
8	SWAM	総ソフトウェア数	#23
9		承認済ソフトウェアのみがインストールされているデバイス数/割合	#21,23,29
10		禁止ソフトウェアがインストールされているデバイス数/割合	#21,23,30
11	CSM	設定した推奨値を準拠しているデバイス数/割合	#38
12		AWARE スコア(CSM)	#38
13		AWARE スコア(CSM)の高いデバイス(TOP10)	#38
14	VUL	脆弱性毎の対応済デバイス数/割合	#41,45
15		脆弱性公開から対応完了までの平均日数	#41,43,45
16		重要度の高い脆弱性を指定期間(例:30 日間)以内に対応完了したデバイス数/割合	#41,43,45

17		AWARE スコア(VUL)	#42,44
18		AWARE スコア(VUL)の高いデバイス(TOP10)	#42,44
19	EMM	総モバイルデバイス数	#46
20		承認済モバイルデバイス数/割合	#46,62
21		管理者割当済モバイルデバイス数/割合	#46,63
22		利用 OS 別モバイルデバイス数/割合	#46,50,51
23		総ソフトウェア数	#55
24		承認済ソフトウェアのみがインストールされているモバイルデバイス数/割合	#29,55
25		禁止ソフトウェアがインストールされているモバイルソフトウェア数/割合	#30,55
26		ポリシー適用率	#58
27		パッチ適用率	#59
28	TRUST/	総ユーザ数	#66
29	CRED/	総アカウント数	#66,71
30	PRIV	未許可アカウント数/割合	#71,73
31		無効化未実施アカウント数/割合	#71,73
32		未許可のアクセス権限があったアカウント数/割合	#71,72
33		一定期間利用のないアカウント数/割合	#71,75
34	MNGEVT/	インシデント総数	#77
35	OMI	緊急度別インシデント発生件数	#77,79
36		インシデント検知から対応着手までの平均所要時間	#77,80,81
37		インシデント検知から対応完了までの平均所要時間	#77,80,82

3.3.4.2. ハードウェア要件

検証作業中に想定される収集データ量を、検証実施に支障をきたさず円滑に処理可能できるようハードウェアを構成すること。オンプレミス、クラウドは問わないものとする。

3.3.4.3. ソフトウェア要件

Agency Dashboard の製品に求められる要件は「図表 11 Agency Dashboard 製品要件」のとおりであるが、本検証環境において実現する機能は、提案者の環境や選定したツールの機能や特性を踏まえ、提案すること。ただし、最終的な構成については、事業開始後に、NEDO と協議し決定すること。なお、Federal Dashboard と同製品を採用することも可能とする。

図表 11 Agency Dashboard 製品要件

No	カテゴリ	要件
1	検索機能	・ 各センサーにより収集したデータを対象とした検索ができること ・ 収集したデータに含まれるタイムスタンプを指定して、任意の期間のデータを対象とした検索ができること ・ 収集したデータフォーマットを認識し、フィールドとして認識できること ・ 特定のフィールドを指定した検索ができること ・ 複数のデータフォーマットを対象とした横断的な検索ができること ・ 検索条件として正規表現、論理演算子を利用できること ・ 収集したデータの特定項目を、事前に定義した一覧情報(リスト)と照合し、ヒット結果を表示できること ・ 検索条件を保存でき、再利用できること ・ 検索結果を保存し、他のユーザを共有できること
2	統計・グラフ機能	・ 収集したデータの特定項目のカウント数・合計値・平均・割合・標準偏差などの統計処理ができること ・ 収集したデータの特定項目もしくは、統計処理により算出した数値(指標)を、時系列で表示できること ・ 収集したデータの特定項目もしくは、統計処理により算出した結果の並び替えができること ・ 検索結果や統計処理によって抽出された数値や項目を棒グラフや線グラフにより表示できること。 ・ 検索結果や統計処理によって抽出された数値や項目を表形式により表示できること。 ・ 複数の図表を 1 つのダッシュボード画面上で表示できること
3	データ出力・外部システム連携機能	・ 収集データの検索結果を REST API により外部システムに連携が可能であること ・ グラフ機能によって作成された図表を PDF 等のファイル形式で出力できること
4	認証・アクセス制御機能	・ Active Directory や SAML などの外部認証方式と連携した認証ができること ・ Active Directory や LDAP など既存のユーザレポジトリを活用し、ユーザのロールや権限管理ができること ・ ユーザのロールや権限にもとづくダッシュボード・収集データへのアクセス制御ができること

3.3.5. Federal Dashboard の要件

3.3.5.1. 概要

Federal Dashboard は、Agency のサマリレベルのデータを収集し、政府機関全体のセキュリティリスクを可視化するダッシュボードである。

本検証では、複数の Agency Dashboard からデータを受領し、サマリデータや AWARE スコアを横断的に比較・確認する機能を準備する。Federal Dashboard で表示する項目は「図表 12 Federal Dashboard 表示項目例」及び「別紙 2. 検証項目案」を参考として、提案者の環境や選定したツールの機能や特性を踏まえ、提案すること。ただし、最終的な構成については、事業開始後に、NEDO と協議し決定すること。

なお、米国 CDM では、Federal と Agency が異なる政府機関で構築されるものであるため、本検証では、複数 Agency Dashboard とのデータ連携を検証項目とし、Federal Dashboard と Agency Dashboard が同じレポジトリを参照し、データ連携が不要になる等の構成は認められないことに留意する。

図表 12 Federal Dashboard 表示項目例

#	表示項目例
1	Agency 毎の端末数
2	重要度の高い脆弱性の未対応端末数
3	搭載 OS 毎の端末数
4	各 Agency の AWARE スコア
5	スコア傾向分析データ(改善数、悪化数 など)

3.3.5.2. ハードウェア要件

検証作業中に想定される収集データ量を、検証実施に支障をきたさず円滑に処理可能できるようハードウェアを構成すること。オンプレミス、クラウドは問わないものとする。

3.3.5.3. ソフトウェア要件

Federal Dashboard の製品に求められる要件は「図表 13 Federal Dashboard 製品要件」のとおりであるが、本検証環境において実現する機能は、提案者の環境や選定したツールの機能や特性を踏まえ、提案すること。ただし、最終的な構成については、事業開始後に、NEDO と協議し決定すること。なお、Agency Dashboard と同製品を採用することも可能とする。

図表 13 Federal Dashboard 製品要件

No	カテゴリ	要件
1	検索機能	・ 各センサーにより収集したデータを対象とした検索ができること ・ 収集したデータに含まれるタイムスタンプを指定して、任意の期間のデータを対象とした検索ができること ・ 収集したデータフォーマットを認識し、フィールドとして認識できること ・ 特定のフィールドを指定した検索ができること ・ 複数のデータフォーマットを対象とした横断的な検索ができること ・ 検索条件として正規表現、論理演算子を利用できること ・ 収集したデータの特定項目を、事前に定義した一覧情報(リスト)と照合し、ヒット結果を表示できること ・ 検索条件を保存でき、再利用できること ・ 検索結果を保存し、他のユーザを共有できること
2	統計・グラフ機能	・ 収集したデータの特定項目のカウント数・合計値・平均・割合・標準偏差などの統計処理ができること ・ 収集したデータの特定項目もしくは、統計処理により算出した数値(指標)を、時系列で表示できること ・ 収集したデータの特定項目もしくは、統計処理により算出した結果の並び替えができること ・ 検索結果や統計処理によって抽出された数値や項目を棒グラフや線グラフにより表示できること。 ・ 検索結果や統計処理によって抽出された数値や項目を表形式により表示できること。 ・ 複数の図表を 1 つのダッシュボード画面上で表示できること
3	データ出力・外部システム連携機能	・ 収集データの検索結果を REST API により外部システムに連携が可能であること ・ グラフ機能によって作成された図表を PDF 等のファイル形式で出力できること
4	認証・アクセス制御機能	・ Active Directory や SAML などの外部認証方式と連携した認証ができること ・ Active Directory や LDAP など既存のユーザレポジトリを活用し、ユーザのロールや権限管理ができること ・ ユーザのロールや権限にもとづくダッシュボード・収集データへのアクセス制御ができること

3.3.6.その他の要件

3.3.6.1. 外部接続要件

「図表 14 必要な外部データ」のとおり、CDM を運用する上で必要なデータを、外部環境から取得すること。該当データを取集する方法についても提案に含めることこと。

また、「2.脅威情報」に関しては、自動または手動で収集・反映するかも含め検討し、考察に含めること。

図表 14 必要な外部データ

#	データ名	用途
1	脆弱性情報	AWARE の VUL の算出に使用する。
2	脅威情報 (スレッドインテリジェンス)	AWARE の Weight Metric の算出に使用する。

4. 付属文書

別紙 1. データ項目案

別紙 2. 検証項目案

5. 事業期間

ＮＥＤＯが指定する日から 2022 年 2 月 28 日まで

6. 予算額

5,000万円以内

7. 報告書

提出期限：2022 年 2 月 28 日

提出方法：NEDO プロジェクトマネジメントシステムによる提出

記載内容：「成果報告書・中間年報の電子ファイル提出の手引き」に従って、作成の上、提出のこと。

https://www.nedo.go.jp/itaku-gyomu/manual.html

8. 報告会等の開催

調査期間中又は調査期間終了後に、成果報告会における報告を依頼することがある。

9. その他

実施事項の内容や進め方、及び本仕様書に定めなき事項等については、NEDO と実施事業者が協議の上で決定するものとする。

以上

＜参考＞

別添. 米国 CDM 事例

参考文献 1. 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 2. CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, CONTINUOUS DIAGNOSTICS AND MITIGATION (CDM),
https://www.cisa.gov/cdm

参考文献 3. Tools Special Item Number,
https://www.gsaelibrary.gsa.gov/ElibMain/home.do

参考文献 4. 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 5. 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 6. 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 7. 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

別紙 1. データ項目案

別紙１．　データ項目案

#	Phase	Capability	区分	データ項目	備考
1	Asset Management	HWAM	必須	シリアルNo.	
2	Asset Management	HWAM	必須	HWベンダー名	
3	Asset Management	HWAM	必須	HW製品名	
4	Asset Management	HWAM	必須	HWモデル名/番号	
5	Asset Management	HWAM	必須	ホスト名/コンピュータ名	
6	Asset Management	HWAM	必須	OS種別	Windows,Linux,macOSなど
7	Asset Management	HWAM	必須	OSエディション	Windows 10,WIndows 2016など
8	Asset Management	HWAM	必須	OSバージョン	
9	Asset Management	HWAM	必須	MACアドレス	
10	Asset Management	HWAM	必須	IPアドレス	
11	Asset Management	HWAM	任意	ネットワーク関連情報(ネットワークアダプタ、サブネット、デフォルトGW、DHCPサーバなど)	
12	Asset Management	HWAM	任意	レジストリ情報(キー、値)	
13	Asset Management	HWAM	任意	CPU情報	
14	Asset Management	HWAM	任意	メモリ情報	
15	Asset Management	HWAM	任意	ディスク情報	
16	Asset Management	HWAM	任意	AD上のデバイス情報(所属ドメイン名、DN、OUなど)	
17	Asset Management	HWAM	任意	承認者	
18	Asset Management	HWAM	任意	管理者	
19	Asset Management	HWAM	任意	利用者	
20	Asset Management	HWAM	任意	承認日	
21	Asset Management	SWAM	必須	ホスト名	収集対象のデバイスを識別するための情報
22	Asset Management	SWAM	必須	インストール済ソフトウェアのベンダー名	資産管理ツールより収集
23	Asset Management	SWAM	必須	インストール済ソフトウェアの製品名	資産管理ツールより収集
24	Asset Management	SWAM	必須	SWバージョン/リリースレベル/パッチレベル	資産管理ツールより収集
25	Asset Management	SWAM	任意	サービス詳細	
26	Asset Management	SWAM	任意	稼働中・停止中サービス	
27	Asset Management	SWAM	任意	稼働中プロセス	
28	Asset Management	SWAM	任意	デフォルトブラウザの設定	
29	Asset Management	SWAM	任意	ホワイトリスト(承認済ソフトウェア一覧)	資産管理ツールとして管理していない場合は、手動でCMaaS/ダッシュボードに投入することを想定
30	Asset Management	SWAM	任意	ブラックリスト(インストール・実行禁止ソフトウェア一覧)	同上
31	Asset Management	SWAM	任意	承認ステータス	
32	Asset Management	SWAM	任意	承認者	
33	Asset Management	CSM	必須	デバイス識別情報(ホスト名など)	収集対象のデバイスを識別するための情報
34	Asset Management	CSM	必須	製品識別情報(製品名、CPEなど)	設定項目がどの製品に関するものなのかを識別するための情報
35	Asset Management	CSM	必須	検査ポリシー名	
36	Asset Management	CSM	必須	設定項目名	
37	Asset Management	CSM	必須	設定値(実際の設定値)	

別紙１．　データ項目案

#	Phase	Capability	区分	データ項目	備考
38	Asset Management	CSM	必須	ベンチマークとの照合結果(準拠/非準拠)	
39	Asset Management	VUL	必須	ホスト名	収集対象のデバイスを識別するための情報
40	Asset Management	VUL	必須	製品識別情報(製品名,CPEなど)	検出された脆弱性がどの製品・バージョンに関するものなのかを識別するための情報
41	Asset Management	VUL	必須	CVE識別番号(CVE-ID)	脆弱性を一意に識別するための番号
42	Asset Management	VUL	必須	CVSSスコア	
43	Asset Management	VUL	必須	脆弱性公開日	
44	Asset Management	VUL	任意	パッチ適用状況	
45	Asset Management	VUL	任意	例外フラグ/対応済情報	パッチ適用など正規の手段ではないものの、代替的対策により当該脆弱性が緩和されている事を識別するための情報
46	Asset Management	EMM	必須	シリアルNo.	
47	Asset Management	EMM	必須	製造元	
48	Asset Management	EMM	必須	モデル名/番号	
49	Asset Management	EMM	必須	デバイス名	
50	Asset Management	EMM	必須	OS種別	
51	Asset Management	EMM	必須	OSバージョン	
52	Asset Management	EMM	必須	IMEI	
53	Asset Management	EMM	必須	Wi-Fi Macアドレス	
54	Asset Management	EMM	必須	IPアドレス	
55	Asset Management	EMM	必須	アプリ名	
56	Asset Management	EMM	必須	アプリバージョン	
57	Asset Management	EMM	必須	プロファイル名	
58	Asset Management	EMM	必須	ポリシー準拠状況(準拠/非準拠)	
59	Asset Management	EMM	必須	パッチ適用状況	
60	Asset Management	EMM	任意	電話番号	
61	Asset Management	EMM	任意	サード パーティのユーザー識別子(Apple IDなど)	
62	Asset Management	EMM	任意	承認者	
63	Asset Management	EMM	任意	管理者	
64	Asset Management	EMM	任意	利用者	
65	Asset Management	EMM	任意	承認日	
66	Identity and Access Management	TRUST/CRED/PRIV	必須	ユーザ識別子	職員番号、ユーザIDなど、湯ユーザを一意的に識別するための情報
67	Identity and Access Management	TRUST/CRED/PRIV	必須	姓	
68	Identity and Access Management	TRUST/CRED/PRIV	必須	名	
69	Identity and Access Management	TRUST/CRED/PRIV	必須	所属組織	
70	Identity and Access Management	TRUST/CRED/PRIV	必須	役職	
71	Identity and Access Management	TRUST/CRED/PRIV	必須	アカウントID	各アカウント毎
72	Identity and Access Management	TRUST/CRED/PRIV	必須	アクセス権(グループなど)	各アカウント毎
73	Identity and Access Management	TRUST/CRED/PRIV	必須	ステータス(有効、無効、承認済など)	各アカウント毎

#	Phase	Capability	区分	データ項目	備考
74	Identity and Access Management	TRUST/CRED/PRIV	任意	Eメールアドレス	
75	Identity and Access Management	TRUST/CRED/PRIV	任意	最終ログイン日時	各アカウント毎
76	Identity and Access Management	TRUST/CRED/PRIV	任意	有効期限	各アカウント毎
77	Network Security Management	MNGEVT/OMI	必須	インシデントID	インシデントを一意に識別する情報
78	Network Security Management	MNGEVT/OMI	必須	インシデント件名	
79	Network Security Management	MNGEVT/OMI	必須	インシデントの緊急度	
80	Network Security Management	MNGEVT/OMI	必須	インシデント検知日時	SIEMによる相関分析園児により自動的にインシデントと判定、もしくはSOCアナリストがインシデントと判断した日時(インシデントチケットオープン日時)
81	Network Security Management	MNGEVT/OMI	必須	インシデント対応開始日時	
82	Network Security Management	MNGEVT/OMI	必須	インシデント対応完了日時	
83	Network Security Management	MNGEVT/OMI	必須	インシデント対応ステータス	
84	Network Security Management	MNGEVT/OMI	任意	インシデントカテゴリ	攻撃手法・タイプ
85	Network Security Management	MNGEVT/OMI	任意	対象デバイス名	インシデントが発生したデバイス

別紙 2.　検証項目案

別紙２．　検証項目案

#	Phase	Capability	試験項目	確認方法(例)
1	Asset Management	HWAM	資産管理ツールなどによりデバイス情報を収集する	・資産管理ツールから、デバイスに関するデータ項目を収集し、CMaaS/ダッシュボードに連携する ・未承認デバイスもスコープとする場合は、デバイス探索ツールにより、ネットワーク上に接続されたデバイスを検出する
2	Asset Management	HWAM	資産管理インベントリ(IT資産管理ツールのレポジトリ)上のデバイスは全て承認済であることを確認する	・収集した資産管理インベントリのデータ項目に承認者に関する項目が存在する場合、この項目がメンテナンスされていることを確認する ・収集した資産管理インベントリのデータ項目に承認者に関する項目は存在しない場合、手動で管理された台帳や帳票などの承認エビデンスをもとに各デバイスが承認済であることを確認する
3	Asset Management	HWAM	承認済のデバイスは、全て資産管理インベントリに存在することを確認する	・デバイス探索ツールにより発見されたデバイスのうち、資産管理インベントリには存在しない且つ承認済のデバイスがないかどうかを確認する
4	Asset Management	HWAM	資産管理インベントリ上のデバイスには、管理者が割り当てられている事を確認する	・収集した資産管理インベントリのデータ項目に管理者に関する項目が存在する場合、この項目がメンテナンスされていること ・収集した資産管理インベントリのデータ項目に管理者に関する項目は存在しない場合、帳票などの承認エビデンスをもとに各デバイスが特定の管理者の管理下であることを確認する
5	Asset Management	SWAM	資産管理ツールなどにより承認済デバイス上にインストールされたソフトウェア情報を収集する	・資産管理ツールから、デバイス上にインストールされたソフトウェア情報を収集し、CMaaS/ダッシュボードに連携する
6	Asset Management	SWAM	承認済ソフトウェアのみがインストールされていることを確認する	・収集した資産管理インベントリ上のインストール済ソフトウェア一覧は、全て承認・許可済である事を、利用申請・承認履歴などと照合し確認する
7	Asset Management	SWAM	禁止ソフトウェアがインストールされていないことを確認する	・収集した資産管理インベントリ上のインストール済ソフトウェア一覧に、禁止ソフトウェアが含まれていない事を確認
8	Asset Management	SWAM	禁止ソフトウェアのインストールや実行を制限するための機能が、導入されてないもしくはポリシーが適用されていないデバイスがあるかどうかを確認する	・インストール・実行制限するためのモジュール(エージェントなど)の導入状況やポリシーの提供状況を、承認済デバイス一覧と照合する。
9	Asset Management	CSM	承認済デバイス上の設定情報を収集する	・構成管理ツールから、デバイス上の設定情報を収集し、CMaaS/ダッシュボードに連携する
10	Asset Management	CSM	ハードウェア、ソフトウェアが事前に定義されたポリシーに従って構成・設定されていることを確認する	・ハードウェアやソフトウェアの設定に関する、業界標準のベンチマーク(STIG,CIS Benchmarkなど)をベースに組織としてのポリシー(推奨値)を定義し、実際の設定値と照合する
11	Asset Management	CSM	非準拠項目が確認されてから対応完了するまでに要した期間を確認する	・ツールにより非準拠状態を初めて確認した日と、是正実施後に是正されたことを確認した日の差分を計算する
12	Asset Management	VUL	承認済デバイスから、インストールされているソフトウェア情報を収集する	・資産管理ツール(もしくは脆弱性管理ツール)から、デバイス上にインストールされたソフトウェア情報を収集し、CMaaS/ダッシュボードに連携する
13	Asset Management	VUL	既知の脆弱性が対応済であることを確認する	・収集した資産管理インベントリ上のソフトウェア情報や適用済パッチ情報と、最新の「既知の脆弱性情報」を照合する
14	Asset Management	VUL	脆弱性が確認されてから対応完了するまでに要した期間を確認する	・脆弱性の公表日(もしくはツールによりデバイス上に脆弱性があることを確認した日)と、是正実施後に是正されたことを確認した日の差分を計算する
15	Asset Management	EMM	MDM/MAMツールによりデバイス情報を収集する	・MDM/MAMツールから、デバイスに関するデータ項目を収集し、CMaaS/ダッシュボードに連携する
16	Asset Management	EMM	MDM/MAMツールで管理されているデバイスは全て承認済であることを確認する	・収集したデータ項目に承認者に関する項目が存在する場合、この項目がメンテナンスされていることを確認する ・収集したデータ項目に承認者に関する項目は存在しない場合、手動で管理された台帳や帳票などの承認エビデンスをもとに各デバイスが承認済であることを確認する
17	Asset Management	EMM	MDM/MAMのインベントリ上のデバイスには、管理者が割り当てられている事を確認する	・収集したデータ項目に管理者に関する項目が存在する場合、この項目がメンテナンスされていること ・収集したデータ項目に管理者に関する項目は存在しない場合、帳票などの承認エビデンスをもとに各デバイスが特定の管理者の管理下であることを確認する
18	Asset Management	EMM	MDM/MAMツールなどにより承認済デバイス上にインストールされたアプリ情報を収集する	・MDM/MAMツールから、デバイス上にインストールされたアプリ情報を収集し、CMaaS/ダッシュボードに連携する
19	Asset Management	EMM	承認済アプリのみがインストールされていることを確認する	・収集したインストール済アプリは、全て承認・許可済である事を、利用申請・承認履歴などと照合し確認

別紙２．　検証項目案

#	Phase	Capability	試験項目	確認方法(例)
20	Asset Management	EMM	禁止アプリがインストールされていないことを確認する	・収集したインストール済アプリに、禁止アプリが含まれていない事を確認
21	Asset Management	EMM	承認済デバイス上の設定情報を収集する	・構成管理ツールから、デバイス上の設定情報を収集し、CMaaS/ダッシュボードに連携する
22	Asset Management	EMM	デバイスが事前に定義されたポリシーに従って構成・設定されていることを確認する	・MDM/MAMのポリシーが適用されている事を確認する
23	Asset Management	EMM	デバイス上のポリシー違反を確認する	・MDM/MAMのポリシー上、違反とされている設定や行為がないかを確認する
24	Asset Management	EMM	既知の脆弱性が対応済であることを確認する	・OSやアプリのバージョン情報等をもとに、パッチが最新の状態になっているかを確認する
25	Identity and Access Management	TRUST/CRED/PRIV	各アカウント情報を収集する	・統合ID管理製品により、各アカウント情報を収集する
26	Identity and Access Management	TRUST/CRED/PRIV	ユーザ(職員)と各アカウントの関連付けを行う	・統合ID管理製品により、ユーザとアカウントの関連付けを行う
27	Identity and Access Management	TRUST/CRED/PRIV	未許可アカウントの存在を確認する	・収集したアカウントのうち、システム管理者が認識していない/作成そのものを承認していないアカウントがいないかを確認する
28	Identity and Access Management	TRUST/CRED/PRIV	無効化されているべきアカウントが有効になっていないかを確認する (例：退職者、休職者、期限満了した委託先ユーザ)	・収集したアカウントのステータスと、退職者、休職者などのリストを照合し、無効化されていないアカウントがないかを確認する
29	Identity and Access Management	TRUST/CRED/PRIV	許可されていない管理者権限が付与されていないかを確認する	・収集したアカウントの管理者権限と、管理者権限の付与申請・承認履歴などを照合し、未許可の管理者権限がないかを確認する
30	Identity and Access Management	TRUST/CRED/PRIV	許可されていないアクセス権限(管理者権限以外)が付与されていないかを確認する	・収集したアカウントのアクセス権限と、アカウント権限の付与申請・承認履歴や所属組織・役職にもとづいて付与される権限情報などを照合し、未許可の管理者権限がないかを確認する
31	Identity and Access Management	TRUST/CRED/PRIV	一定期間利用されていないアカウントを確認する	・最終ログイン日からの経過期間を確認する
32	Network Security Management	MNGEVT/OMI	インシデント関連情報を収集する	・SIEM/EDR製品から、インシデントに関する情報を収集し、CMaaS/ダッシュボードに連携する
33	Network Security Management	MNGEVT/OMI	インシデントを検知してから対応着手するまでに要した時間を確認する	・インシデントを検知したに日時と対応着手日時の差分を確認する
34	Network Security Management	MNGEVT/OMI	インシデントの対応着手してから対応完了するまでに要した時間を確認する	・インシデントの対応着手日時と対応完了日時の差分を確認する
35	Network Security Management	MNGEVT/OMI	緊急度別の発生状況を確認する	・インシデントの緊急度(Severity)/優先度毎に、一定期間内での発生件数や対応中(未クローズ)の件数を確認する

别添. 米国 CDM 事例

目次

1. 米国 CDM 事例

1.1. CDM 全体アーキテクチャ

CDM プログラムの全体アーキテクチャは、「図表 1 CDM 全体アーキテクチャ」のとおり、Layer A から Layer D の 4 階層で構成される。

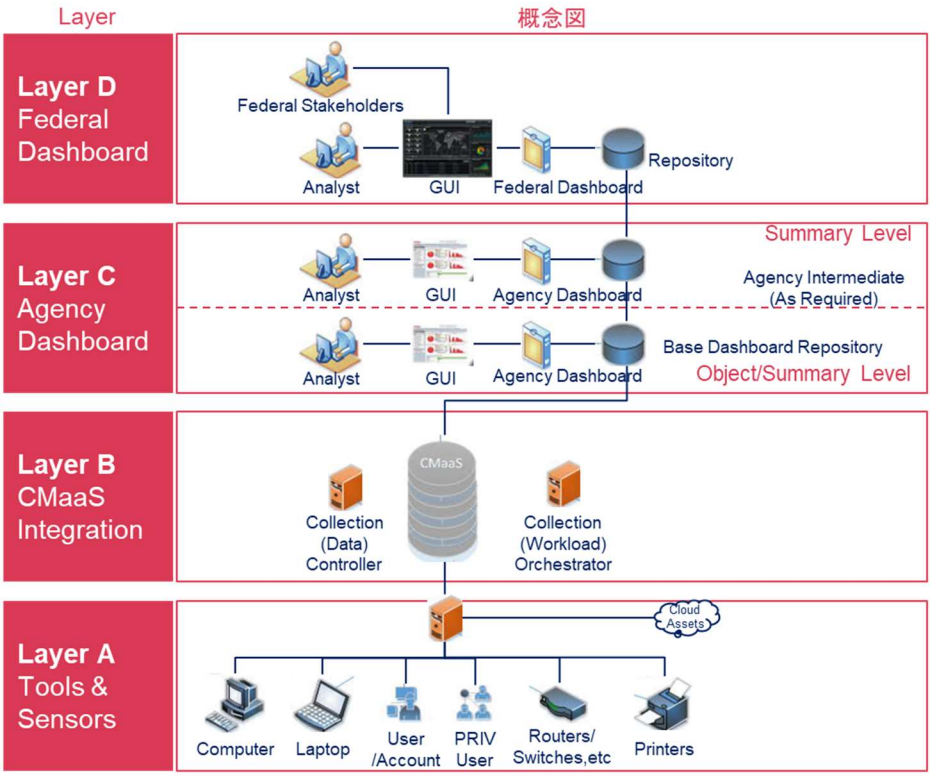
Layer A は、CDM プログラムで監視する対象のエンドポイントである。CDM プログラムでは、ネットワーク上の IP アドレスが付与されている機器を監視対象として定義し、監視対象機器の状態を収集するツール(Sensor)を導入する。

Layer B は、Layer A から収集した情報を集約・統合・正規化する CMaaS ツールである。様々なエンドポイントからの情報を収集し、Layer C へデータを連携する運用上の制御ポイントとなるため、Layer A 及び Layer C の製品・ツールとの相互運用性が必要である。

Layer C は、収集した情報を省庁レベルで可視化するダッシュボードである。サマリデータや算出した AWARE スコアを表示するだけでなく、問題が検出された際に対象端末を特定するなど、オブジェクトレベルのデータも保有する必要がある。

Layer D は、省庁レベルのサマリデータを収集し、政府機関全体のセキュリティリスクを可視化するダッシュボードである。サマリデータや AWARE スコアを横断的に確認することが用途のため、オブジェクトレベルのデータは保有しない。

図表 1 CDM 全体アーキテクチャ

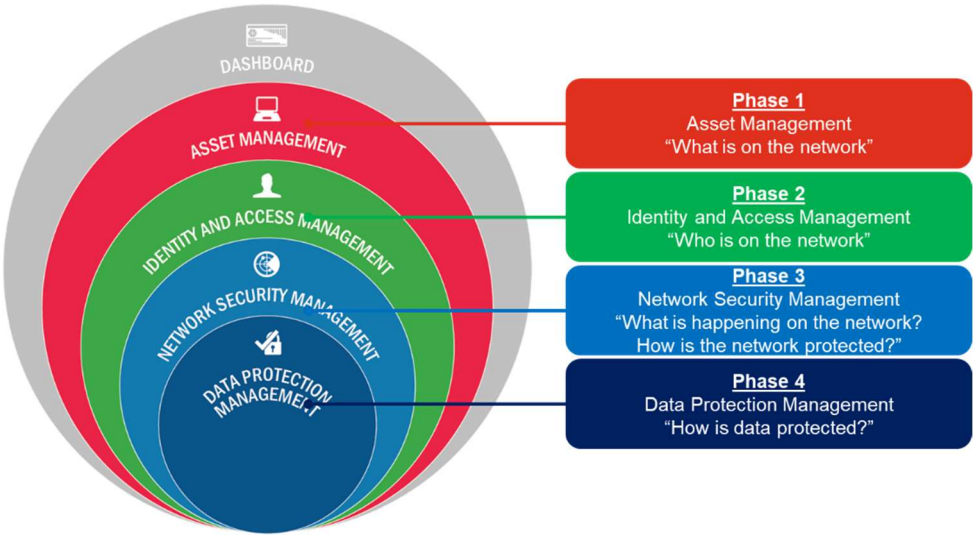


1.2. CDM の Capability

1.2.1. CDM のプログラム構成

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。

図表 2 CDM プログラムの領域



1.2.2. 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。

1.2.3. 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

1.2.4. Asset Management (Phase1)の Capability

Asset Management では、「図表 5 Asset Management の Capability」のとおり、HWAM(ハードウェア資産管理)、SWAM(ソフトウェア資産管理)、CSM(構成・設定管理)、VUL(脆弱性管理)、EMM(エンタープライズモバイル管理)の 5 つの Capability が必要である。

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

1.2.5. Identity and Access Management (Phase2)の Capability

Identity and Access Management では、「図表 6 Identity and Access Management の Capability」のとおり、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)の 4 つの Capability が必要である。

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。

1.2.6. Network Security Management (Phase3)の Capability

Network Security Management では、「図表 7 Network Security Management の Capability」のとおり、BOUND(ネットワーク保護)、MNGEVT(セキュリティイベント管理)、OMI(運用・監視・改善)、DBS(セキュリティに配慮した設計・開発)の 4 つの Capability が必要である。

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** ネットワーク保護を管理するには、下記次の3つを管理する。 BOUND-F　:ネットワークフィルターと境界制御の管理 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および管理 ※NAC : Network Access Control
	MNGEVT (セキュリティイベント管理)	**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提供し、次の領域をカバーする。 • 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
	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アクティビティに重点をおき、次の領域をカバーする。 • 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
	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。

1.2.7. Data Protection Management (Phase4)の Capability

Data Protection Management では、「図表 8 Data Protection Management の Capability」のとおり、DISCOV(データ検出・分類)、PROT(データ保護)、DLP(データ漏洩防止)、SPIL(データ侵害・流出対応・緩和)、IRM(データ操作制御)の 5 つの Capability が必要である。

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。

1.3. CDM のリスクスコアリング方法(AWARE)

AWARE とは、CDM 用に開発されたスコアリング方法論であり、Phase1 の Capability にて収集したデータに基づき、リスクスコアを算出する。算出された AWARE スコアから、”Worst Problem First”の考え方に基づき、サイバーリスクへの状況認識と、脅威と脆弱性へのタイムリーな緩和を可能にする。

1.3.1. AWARE スコアの分類

ソフトウェア脆弱性、構成設定管理上の不備、機器の未承認状況の 3 つの観点でのリスクを可視化するために、AWARE スコアは「図表 9 AWARE スコアの分類」のとおり VUL、CSM、UAH の 3 つに分類されている。

図表 9 AWARE スコアの分類

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。

1.3.2. AWARE スコア算出式

AWARE スコアは、「図表 10 AWARE 算出式」のとおり、「Base Metric」、「Age Metric」、「Weight Metric」、「Allowable Tolerance Metric」 の 4 つの Metric の積により算出される。

VUL、CSM、UAH の各スコアは、この算出式に対して 1.3.3 および 1.3.4 で示す分類毎の Metric 値を当てはめて算出する。

VUL は発見された脆弱性を対象に算出した値の積算値、CSM は不備があった設定項目を対象に算出した値の積算値、

端末毎に、発見された脆弱性毎の VUL の積算値、発見された設定不備毎の CSM の積算値、(未承認機器であった場合は)UAH を合計したものが端末自身の AWARE スコアとなる。

図表 10 AWARE 算出式

1.3.3. スコア分類毎の Metric 値

AWARE スコアの算出に使用する各 Metric の値は、「図表 11 スコア分類別の Metric 値」のとおり、スコア分類間で異なる。

図表 11 スコア分類別の Metric 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

1.3.4. 各 Metric 値算出の考え方

AWARE に使用する 4 つの Metric の値の算出に関する考え方は以下のとおり。

① Base Metric

VUL の場合は、「図表 12 Base Metric (VUL)」のとおり、CVSS 値を元に対数スケーリングした値を Base 値として使用する。

図表 12 Base Metric (VUL)

対数スケーリング

CVSS値	BASE値
10	10
9	7.29
8	5.12
7	3.43
6	2.16
5	1.25
4	0.64
3	0.27
2	0.08
1	0.01

CSM の場合は、「図表 13 Base Metric (CSM)」のとおり、DISA STIG に定義された Category に対応する値を Base 値として使用する。

図表 13 Base Metric (CSM)

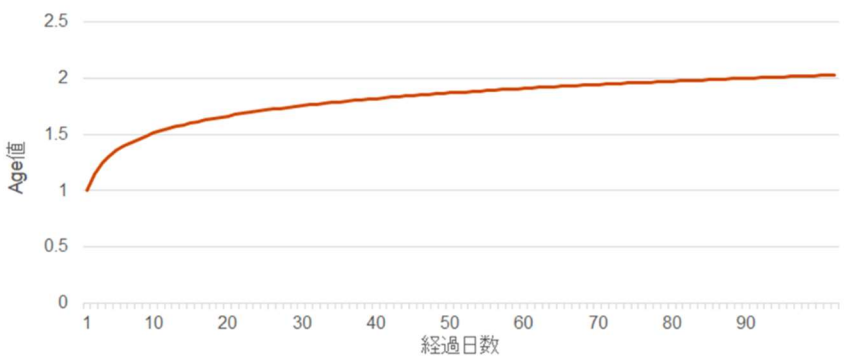
DoD STIG	BASE値
Category 1	0.72
Category 2	0.36
Category 3	0.12

UAH の場合は、一律「10」を Base 値として使用する。

② Age Metric

Age Metric とは、「図表 14 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。なお、経過日数 90 日で Age Metric は 2 倍となる。

図表 14 Age Metric



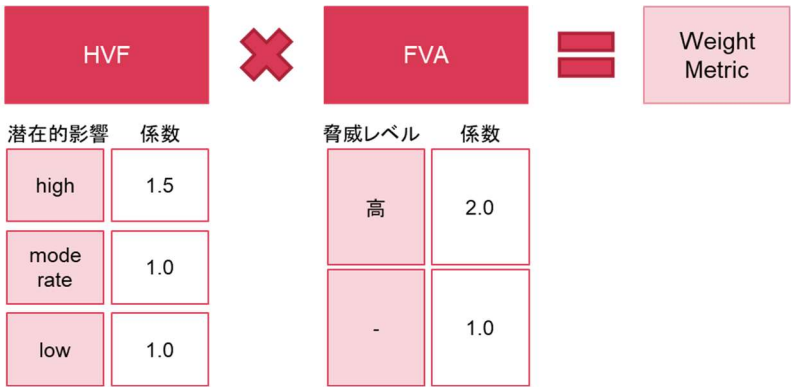
③ Weight Metric

Weight Metric は、「図表 15 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 15 Weight Metric



④ Allowable Tolerance

Allowable Tolerance は、CVE が公開されてから対応するまでに、適用テストの実施等、一定期間は必要であるという考え方である。「図表 16 Allowable Tolerance」のとおり、定義された許容期間内は AWARE スコアの算出や Agency ダッシュボードへの表示はされるが、Federal ダッシュボードへの連携はされない。

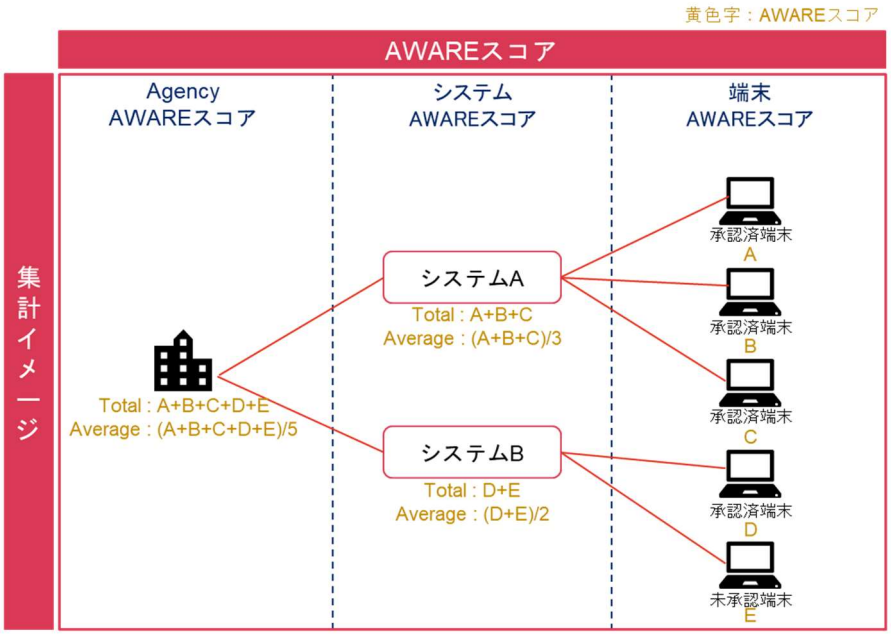
図表 16 Allowable Tolerance

1.3.5. システム単位および Agency 単位でのスコア集計方法

AWARE スコアの集計方法は、「図表 17 スコア集計イメージ」のとおり、各端末の AWARE スコアをシステム単位および Agency 単位で集計することで、それぞれシステム AWARE スコアと Agency AWARE スコアが算出される。

なお、集計にあたっては Total(合計値)と、端末数で割った Average(平均値)等の集計方法がある。

図表 17 スコア集計イメージ



1.4. 米国で採用されている製品

1.4.1. ダッシュボード

ダッシュボード製品は、「図表 18 ダッシュボードのロードマップ」のとおり、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 18 ダッシュボードのロードマップ

	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。

1.4.2. CMaaS

CMaaS 製品は、Splunk が使用されている。

1.4.3. 主な APL 登録ベンダー

仕様書本紙の参考文献 4.Approved Products List(APL)に登録されている、CDM の各 Phase に対応した製品を提供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 • Mobilelron, 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 • Mobilelron, 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 • Mobilelron, 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 • Mobilelron, Inc. • Netskope, Inc.	• Splunk • Zscaler Inc.	

1.4.4. Asset Management

仕様書本紙の参考文献 7. Privacy Impact Assessment for the Continuous Monitoring as a Service (CMaaS)にて示されている、Asset Management に関する Sensor 製品は、「図表 20 Asset Management の製品」のとおり。

図表 20 Asset Management の製品

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**

1.4.5. Identity and Access Management

仕様書本紙の参考文献 7. Privacy Impact Assessment for the Continuous Monitoring as a Service (CMaaS)にて示されている、Identity and Access Management に関する製品は、「図表 21 Identity and Access Management の製品」のとおり。

図表 21 Identity and Access Management の製品

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。	–