資料３

技術検討会議

2022年3月15日（火）

デジタル庁

常時リスク診断・対処（**CRSA**）について

常時リスク診断・対処（CRSA）の導入に関する技術レポート（仮）

常時診断・対応型セキュリティアーキテクチャ技術レポート(仮)はCDMアーキテクチャの要約で構成する予定です

目次･構成案

目次（案）
1はじめに
1背景と目的
2適用対象
3位置づけ
4用語
2基本方針
1ゼロトラストにおけるCDM
2米国版CDMプログラム
3CDMの詳細項目
1CDMの概要とアーキテクチャ
2事例

その他の技術レポートと同様の構成と内容を想定

ゼロトラストアーキテクチャとの関連性

IPA「次世代政府セキュリティアーキテクチャの検討」より「2.アーキテクチャの概要」の要約

以下の内容のうちどこを対象とするか
- ✓ 概要図はIPAを流用
- ✓ 各レイヤごとの説明（ガバナンスレイヤ、業務レイヤ、アプリケーションレイヤ、技術レイヤ）をどこまで詳細に記載する必要があるか

関連性に関するイメージ図（From NIST）

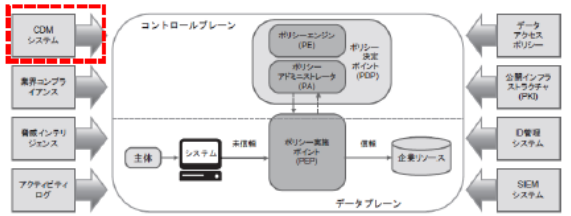
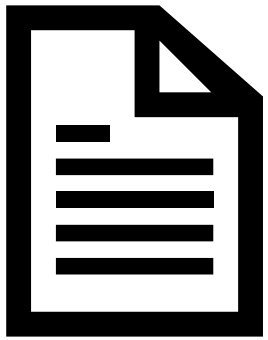


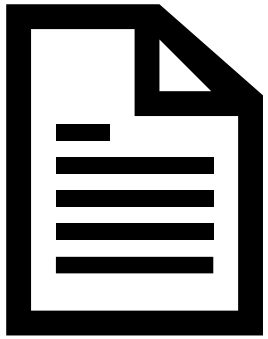
図 2: ゼロトラストの中核となる論理コンポーネント

作成成果物の構成



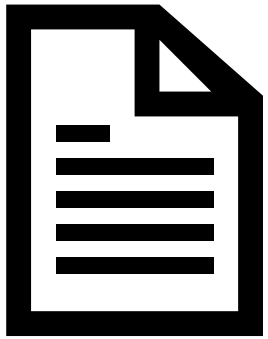
NIST SP 800-207

1. 序章
2. セロトラストの基本
3. **ZTAの論理的構成要素**
4. 導入シナリオ/ユースケース
5. **ZTAと既存の連邦ガイダンスとの連携の可能性**
6. **ZTAへの移行**



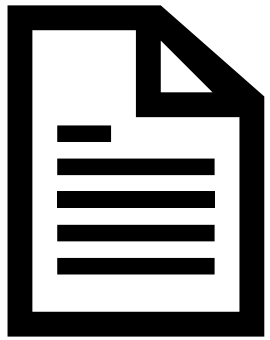
ゼロトラストアーキテクチャ適用方針ガイドライン

1. はじめに
2. **基本方針**
3. **具体方針**
4. 付属文書
5. 参照文書



アーキテクチャ設計書

1. はじめに
2. **アーキテクチャの概要**
3. 定量化指標とモニタリング指標
4. スコアリング
5. ダッシュボードの表示項目
6. データモデル



常時リスク診断・対処（CRSA）の導入に関する技術レポート（仮）

1. はじめに
1.1. 背景と目的
1.2. 適用範囲
1.3. 位置づけ
1.4. 用語
2. 基本方針
2.1. 常時リスク診断・対処（CRSA）の位置づけ
2.2. 基本方針
2.3. 常時リスク診断・対処（CRSA）の導入
2.4. ゼロトラストアーキテクチャの適用方針との関係
3. 常時リスク診断・対処（CRSA）アーキテクチャ
3.1. アーキテクチャ全体
3.2. ガバナンスレイヤー
3.3. 業務レイヤー
3.4. アプリケーションレイヤー
3.5. 技術レイヤー
3.6. 関係要素
4. 付属文書
5. 参照文書

目次（案）

CDM技術レポート目次案

1 はじめに
- 1 背景と目的
- 2 適用範囲
- 3 位置づけ
- 4 用語

2 基本方針
- 1 常時リスク診断・対処（CRSA）の位置づけ
- 2 基本方針
- 3 常時リスク診断・対処（CRSA）の導入
- 4 ゼロトラストアーキテクチャの適用方針との関係

3 常時リスク診断・対処（CRSA）アーキテクチャ
- 1 アーキテクチャ全体
- 2 ガバナンスレイヤー
  - 1 目的
  - 2 対象領域
- 3 業務レイヤー
  - 1 基準・ガイドライン
  - 2 体制
  - 3 業務
  - 4 ユースケース
  - 5 府省庁担当者の業務
- 4 アプリケーションレイヤー
  - 1 GSOダッシュボード
  - 2 ASOダッシュボード
  - 3 GSOリポジトリ
  - 4 ASOリポジトリ
  - 5 レポート用リポジトリ
- 5 技術レイヤー
  - 1 政府内の参照データベースシステム
  - 2 政府外の参照データベースシステム
  - 3 府省庁の政府情報システム
- 6 関係要素

4 付属文書

5 参照文書

常時リスク診断・対処（CRSA）の位置づけ、診断と対応における基本方針を記載

IPA「次世代政府セキュリティアーキテクチャの検討」より「2．アーキテクチャの概要」の要約

２章　基本方針

2.1. 常時リスク診断・対処（CRSA）の位置づけ

常時リスク診断・対処（CRSA）システムは、接続要求を行う資産に関する情報をポリシーエンジンに提供する役割を担う

2.2. 基本方針

常時リスク診断・対処（CRSA）アーキテクチャの基本方針

2.3. 常時リスク診断・対処（CRSA）の導入

常時リスク診断・対処（CRSA）アーキテクチャの導入による、ゼロトラストアーキテクチャ展開サイクルの実現

2.4. ゼロトラストアーキテクチャの適用方針との関係

「資産の把握」、「資産の状態確認」、「監視強化と可視化」と常時リスク診断・対処（CRSA）アーキテクチャとの関係

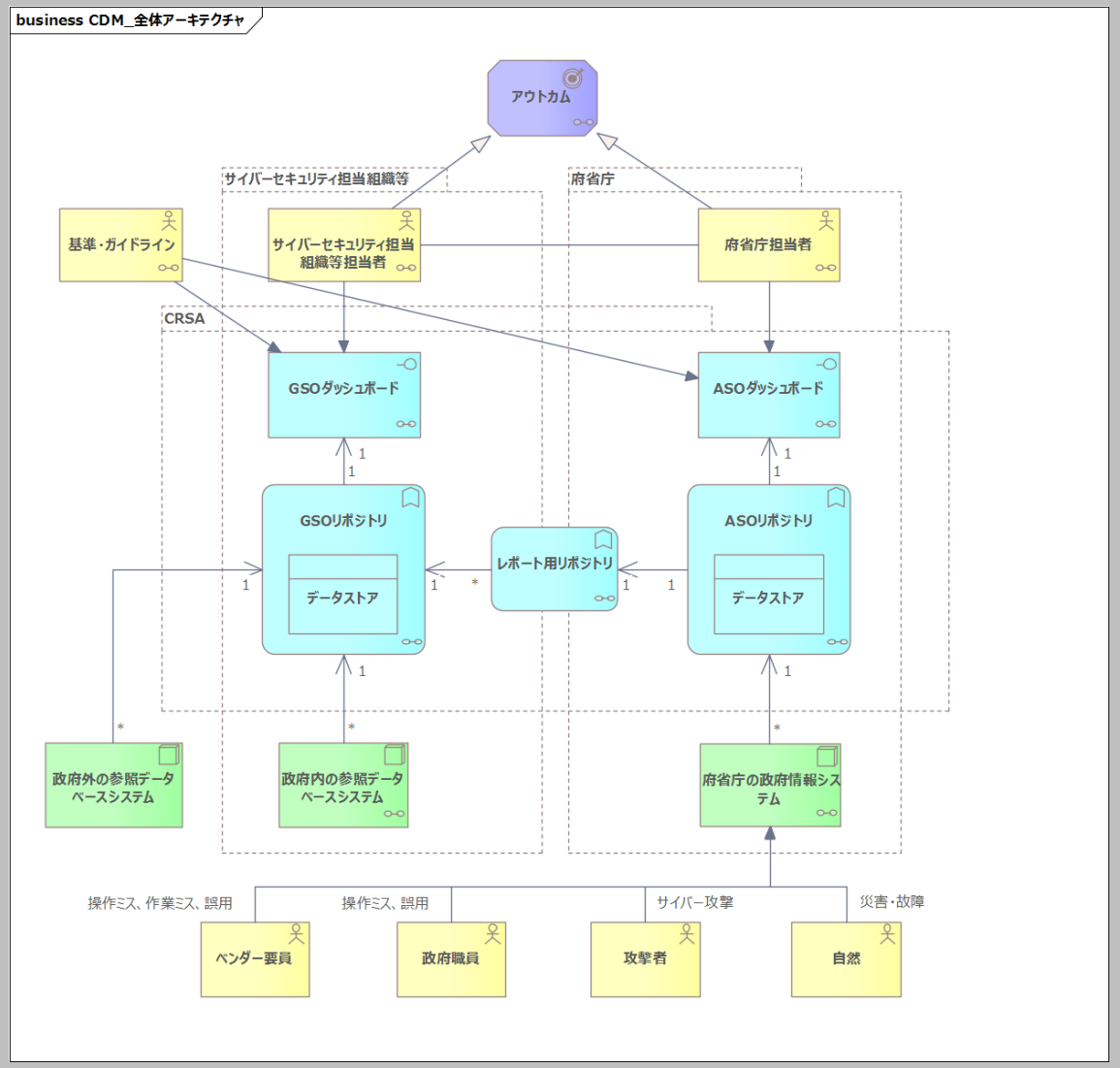
概要

記載方針

- ゼロトラストアーキテクチャを構成する論理コンポーネントにおける、CRSAシステムの位置付けを記載する。
- 基本方針
  - **何がつながっているのか？**
    組織において、どのようなデバイス、アプリケーション、およびサービスが利用されているかを把握する。これには、脆弱性や脅威が発見された際に、これらのセキュリティ対策の実行状況を確認し、必要に応じて改善策を講ずることが含まれる。
  - **誰がネットワークを使用しているか？**
    どのような利用者が組織に所属しているか、またはどのような外部の利用者が組織の資産へのアクセスを許可されているかを把握する。
  - **ネットワークで何が起こっているのか？**
    どのようなシステム間のトラフィックパターンやメッセージが発生しているのかを把握する。
  - **データはどのように保護されているか？**
    情報の保存時、転送時、および利用時にどのように保護されるかについて、ポリシーを定める。
- 常時リスク診断・対処（CRSA）システムが担う、フィードバックループの重要性について言及する。
- 適用方針のうち、関係性の高い項目について記載する。

3章　常時リスク診断・対処（CRSA）アーキテクチャ

3.1.アーキテクチャ全体



3.2. ガバナンスレイヤー
- 目的
- 対象領域

3.3. 業務レイヤー
- 基準・ガイドライン
- 職員

3.4. アプリケーションレイヤー
- ダッシュボード（可視化機能）
- リポジトリ（データ処理機能）

3.5. 技術レイヤー
- 連携する他システム

3.6. 関係要素
- 診断対象システムに影響を与える要素

３章　常時リスク診断・対処（CRSA）アーキテクチャ

3.2. ガバナンスレイヤー

3.2.1.目的

記載方針

➢ ４つの**目的**

- **政府組織の攻撃対象領域の極小化**
  リスクベースの考え方に基づき、政府組織においてサイバー攻撃の対象となりうる脆弱な領域を極小化するための仕組みを提供する。

- **政府全体のサイバーセキュリティ態勢の可視性の向上**
  複雑化する情報システムにおける脆弱性の所在を確認し、優先順位を定めて対応するために、ダッシュボードとスコアを定義して可視性を高める仕組みを提供する。

- **政府全体のサイバーセキュリティ対応機能の改善促進**
  政府全体で把握した参加組織の脆弱性対策について、 Threat Hunting を含むサイバーセキュリティ対応機能の改善を促進するための仕組みを提供する。

- **統一基準を踏まえた情報セキュリティ対策実効性確認の効率化**
  統一基準に準拠した定量化指標に基づき政府組織の情報セキュリティ対策状況をスコアリングし、その実効性の確認を効率化することで、政府組織において情報セキュリティリスクを早期に探知することができる仕組みを提供する。

3章　常時リスク診断・対処（CRSA）アーキテクチャ

3.2. ガバナンスレイヤー

3.2.2.対象領域

対象領域については、まず「端末とサーバ装置等の管理」から着手し、順次領域を拡大する予定

記載方針

➢ 4つの**対象領域**

- **端末とサーバ装置等の管理**
  府省庁の政府情報システムにおけるデバイスについて、識別と状態の監視が適切に行われているかについて診断を行う。デバイスが適切に構成され、脆弱性が識別されて対応が実施されていることを確認する。

- **認証・認可・特権の管理**
  府省庁の政府情報システムを利用するユーザーについて、識別と認証が適切に行われているかについて診断を行う。ユーザーが適切に識別され、トレーニングを受けており、その役割に応じて適切に認証されていることを確認する。

- **ネットワークセキュリティ管理**
  府省庁の政府情報システムを構成する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、適切な監視が行われているかについて診断を行う。情報システムのライフサイクルを通して、脆弱な領域を増大させる可能性のある要因を確認する。

- **データ保護管理**
  府省庁の政府情報システムが保持する機密（特にプライバシー）データについて、適切な保護が実施されているかについて診断を行う。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等が適切に実施されていることを確認する。

３章　常時リスク診断・対処（CRSA）アーキテクチャ

3.3. 業務レイヤー

	概要
3.3.1. 基準・ガイドライン	政府機関等のサイバーセキュリティ対策のための統一基準群、ガイドライン群、フレームワーク、等
3.3.2. 体制	意思決定者、分析・評価担当者、品質管理担当者
3.3.3. 業務	政府戦略性評価、品質管理、分析・評価、対応策の指示、監査支援、緊急時対応、調達、実装、維持管理
3.3.4. ユースケース	セキュリティインシデント対応支援、脆弱性対応支援、スコア変動イベント対応、進捗管理、CRSAシステムの運用管理、等
3.3.5. 府省庁担当者の業務	府省戦略性評価、品質管理、分析・評価、対応策の実施、データメンテナンス

記載方針

- 業務レイヤーは、CRSAアーキテクチャに係る基準・ガイドラインの解説と職員別の業務機能について記載する。
- 基準・ガイドラインについては、既存のものに加えて、今後作成予定のもの（例：ゼロトラスト・アーキテクチャ適用方針ガイドライン）についても記載する。
- ユースケースは、代表的なケースについて一連の業務として記載する。
- 府省庁の体制は、統一基準に基づき記載する。

３章　常時リスク診断・対処（CRSA）アーキテクチャ

3.4. アプリケーションレイヤー

	概要
3.4.1. GSOダッシュボード	サイバーセキュリティ担当組織等担当者に対する可視化を実現する機能について
3.4.2. ASOダッシュボード	府省庁担当者に対する可視化を実現する機能について
3.4.3. GSOリポジトリ	GSOダッシュボードへの表示データを集約し統合する機能について データストア機能とデータ構造について
3.4.4. ASOリポジトリ	GSO/ASOダッシュボードへの表示データを集約し統合する機能について データストア機能とデータ構造について
3.4.5. レポート用リポジトリ	GSOリポジトリとASOリポジトリ間でのデータ連携機能とデータ構造について

記載方針

- アプリケーションレイヤーは、CRSAシステムを構成する５つの機能要素について記載する。
- ５つの機能要素は、ダッシュボード機能（可視化機能）とリポジトリ機能（データ処理機能）に大別される。
- GSOダッシュボードとASOダッシュボードについては、表示項目の概要について記載する。
- GSOリポジトリとASOリポジトリついては、データ処理機能に加えて、ダッシュボード機能および外部システムとの連携について記載する。
- レポート用リポジトリについては、主としてGSOリポジトリとASOリポジトリのデータ連携について記載する。

３章　常時リスク診断・対処（CRSA）アーキテクチャ

3.5. 技術レイヤー

	概要
3.5.1. 政府内の参照データベースシステム	政府内に所在する、各種の参照データベースシステムについて
3.5.2. 政府外の参照データベースシステム	インターネット上のデータベース等、政府外の参照データベースシステムについて
3.5.3. 府省庁の政府情報システム	診断の対象となる、府省庁の政府情報システムについて

3.6. 関係要素

府省庁の政府情報システムのセキュリティを阻害する要素、想定すべき代表的な脅威について

記載方針

- 技術レイヤーは、主としてCRSAシステムと連携する下記の他システムについて記載する。
  - 政府内の参照データベースシステム
  - 政府外の参照データベースシステム
  - 府省庁の政府情報システム

常時リスク診断・対処（CRSA）の導入に関する技術レポート（仮）

ご意見をいただきたい論点

- **技術レポートの構成について**

  「常時リスク診断・対処（CRSA）の導入に関する技術レポート」の構成、記載内容の妥当性、盛り込むべき要素、等

- **基本方針（2章）について**

  基本方針の妥当性、等

- **アーキテクチャ全体（3.1節）について**

  アーキテクチャ全体の構成要素の過不足、記載様式の修正方針、等

- **ガバナンスレイヤー（3.2節）について**

  目的の妥当性、対象領域の妥当性、等

デジタル庁