デジタル社会推進実践ガイドブック　DS-211

常時リスク診断・対処（CRSA）の
エンタープライズアーキテクチャ（EA）

2024 年（令和 6 年）1 月 31 日

デジタル庁

〔ドキュメントの位置付け〕
Informative
参考とするドキュメント

〔キーワード〕
ゼロトラストアーキテクチャ、システムアーキテクチャ、資産管理、プラットフォーム

〔概要〕
ゼロトラストアーキテクチャの環境下において、安定かつ安全なサービス提供を実現するためには、政府全体のサイバーセキュリティリスクを早期に検知し、これを低減することが必要となる。本文書は、各府省庁の政府情報システムにおけるサイバーセキュリティリスクについて常時かつ継続的に状況を把握するとともに、必要に応じて各府省庁と連携してリスク低減活動を実施するための、情報収集・分析を目的としたシステム（以下、「常時リスク診断・対処（CRSA）システム」という。）のアーキテクチャについて解説している。

改定履歴

改定年月日	改定箇所	改定内容
2022年6月30日	―	初版決定
2024年1月31日	2.1、2.2 3	● CRSA の概要および目的と効果について明示 ● エンタープライズアーキテクチャ(EA)に関する説明であることを明示して、本文およびアーキテクチャ全体図を修正 ● 各政府機関の情報システムから統計情報を収集することについて言及 ● 診断対象領域と診断対象について明示

目次

１　はじめに

１．１　背景と目的

社会全体のデジタルトランスフォーメーションが加速し、我々を取り巻く様々な分野において ICT の利活用が進んでいる。他方、サイバー攻撃はその発生頻度の増加と高度化が続く状況下にあり、サイバーセキュリティ対策のさらなる強化が不可欠となってきている。こうした中で、政府情報システムに対しても、今後、サイバー攻撃の脅威は高まっていくことが予想される。

政府情報システムは国民生活や行政の活動の根幹を支える基盤であり、これらのシステムにおけるインシデントは社会基盤の機能停止に直結するリスクがある。このため、令和 3 年度に閣議決定されたサイバーセキュリティ戦略に基づき、従来の「境界型セキュリティ」にとどまらない、常時診断・対応型のセキュリティアーキテクチャの実装に向けた技術検討を進めていく必要がある。

従来型のセキュリティ監視・運用体制においては、政府として統一的なセキュリティポリシーの適切な運用、迅速なリスク検知・低減活動が困難となることが予想され、資産管理、構成管理、脆弱性管理等の拡充・レベルアップが求められている。このため、政府全体のサイバーセキュリティリスクを早期に検知し、これを低減することを目的とし、常時リスク診断・対処（CRSA: Continuous Risk Scoring and Action）システム（以下、「CRSA システム」という。）の導入を検討することになった。具体的には、令和 5 年度版の「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」（以下、「統一基準群」という。）に基づき、各府省庁システムにおけるサイバーセキュリティリスクについて常時かつ継続的に状況を把握し、必要に応じて各府省庁と連携してリスク低減活動を実施するための、情報収集・分析システムを構築することが求められている。

本文書は、「デジタル社会の実現に向けた重点計画」、「サイバーセキュリティ戦略」及び「情報システムの整備及び管理の基本的な方針」を踏まえ、CRSA のエンタープライズアーキテクチャを解説したものである。

１．２　適用範囲

本文書は、政府情報システムを適用対象として想定している。なお、本文書は CRSA システムへの理解を深める参考文書であり、適用の遵守を求めるものではない。

１．３　位置づけ

本文書は、標準ガイドライン群の Informative（情報提供）のレベルの参考文書である。

１．４　用語

本文書において使用する用語は、表１-1 及び本文書に別段の定めがある場合を除くほか、標準ガイドライン群用語集の例による。その他専門的な用語については、民間の用語定義を参照していただきたい。

表　1-1　用語の定義

項番	用語	定義
1	NIST	アメリカ国立標準技術研究所 National Institute of Standards and Technology
2	CISA	国土安全保障省サイバーセキュリティー・インフラセキュリティー庁 Cybersecurity & Infrastructure Security Agency
3	常時リスク診断・対処（CRSA）プログラム	システムの挙動やソフトウェアの状況をリアルタイムに監視し対処する取組 CRSA: Continuous Risk Scoring and Action
4	CRSA システム	常時リスク診断・対処（CRSA）プログラムを実現するためのシステムのこと
5	統一基準群	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
6	サイバーセキュリティ担当組織等担当者	常時リスク診断・対処（CRSA）プログラムにおけるサイバーセキュリティ担当組織及びデジタル化推進組織の担当者
7	府省庁担当者	常時リスク診断・対処（CRSA）プログラムにおける各府省庁の担当者
8	政府横断 GSO システム	CRSA システムにおけるサイバーセキュリティ担当組織及びデジタル化推進組織のシステム
9	GSO ダッシュボード	Government SecOps Dashboard

項番	用語	定義
		政府機関横断 SecOps ダッシュボード
10	GSO リポジトリ	Government SecOps Repository 政府機関横断 SecOps リポジトリ
11	ASO ダッシュボード	Agency SecOps Dashboard 府省庁 SecOps ダッシュボード
12	ASO リポジトリ	Agency SecOps Repository 府省庁 SecOps リポジトリ

2　CRSAシステムの導入方針

2.1　CRSA システムの概要

CRSA とは、サイバー攻撃等のリスクから情報システムを守るために導入された「必要なコントロール」（管理策）が、その目的とする機能を達成することを確実にするための仕組みである。すなわち、「必要なコントロール」と対象となる情報システムの「実際の状態」の差異を「ギャップやリスク」として「可視化」し、常時モニタリング（診断）を行い、必要に応じて「是正対応」を促す活動（対処）を継続することにより、「必要なコントロール」からの逸脱を防止するための仕組みである。

CRSA の概念図を以下に示す。

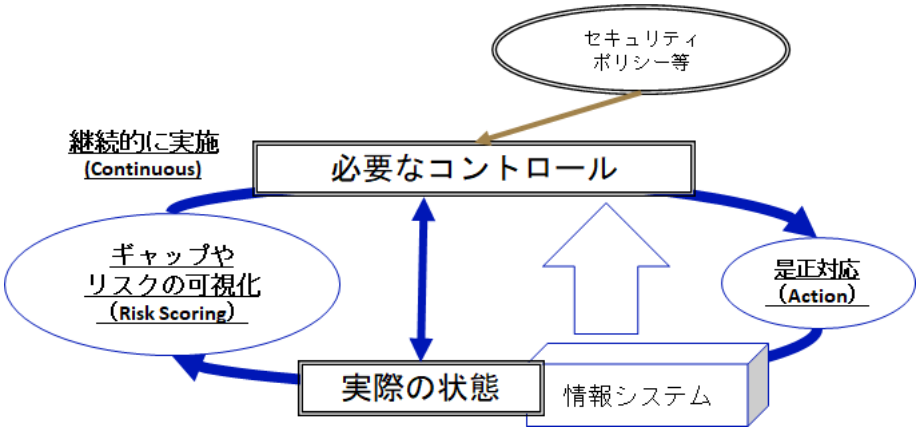


図　2-1　CRSA の概念図

CRSA は、組織のセキュリティポリシー等に準拠するために情報システムに導入された必要なコントロール（管理策）に関して、以下を実施する。

- リスク診断：必要なコントロールと実際の状態とのギャップやリスクを可視化
- 対処：可視化されたギャップやリスクの是正対応
- 常時：ギャップやリスクの可視化と是正対応を継続的に実施

CRSA は、ポリシーからの逸脱を発見し、迅速かつ計画的にその是正を図ることによって政府のシステムを予防的にセキュアにすることを目指している。CRSA は、資産管理や脆弱性のみならず、クレデンシャルの管理状況、ネットワーク内の監視体制の健全性、データの保護の状況（例えば、許可されていないところにデータが保存されていないことなどを含む。）なども常時診断の対象としていくものである。

CRSA システムの概要図を以下に示す。

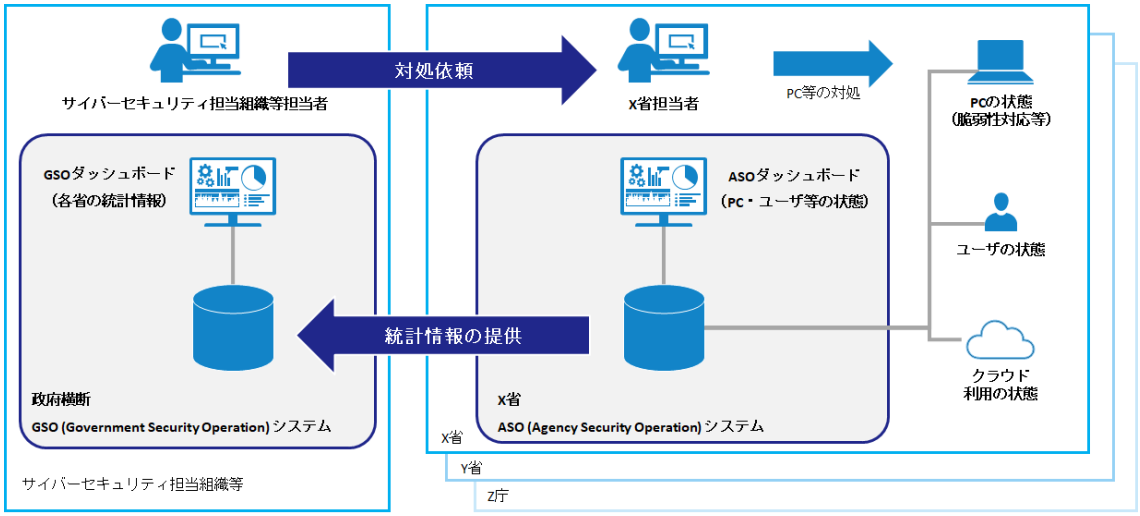


図 2-2 CRSA システムの概要図

CRSA システムは、政府横断 GSO システムと各府省の ASO システムに大別される。ASO システムは、PC、ユーザ、クラウドの状態等の組織の資産に関する情報を収集して ASO リポジトリに蓄積し、資産の構成及びソフトウェアコンポーネントに内在する潜在的リスクを可視化し、ASO ダッシュボードに表示することにより、各府省における是正活動を支援する。

さらに、ASO リポジトリに蓄積された情報は、統計処理を実施したうえで政府横断 GSO システムと連携する。GSO リポジトリでは、各府省から送付された各省の統計情報をもとに、政府横断での潜在的リスクを可視化し、GSO ダッシュボードに表示することにより、政府横断での是正活動を支援する。GSO ダッシュボードにおいて検知された問題点については、GSO 担当者から各府省の ASO 担当者に対処が依頼され、ASO 担当者において対処が成される。

政府横断 GSO システムは、情報システムの運用等におけるセキュリティポリシー等からの逸脱を発見することなどを目指している。例えば、端末で適切なパッチが適用済みのオペレーティングシステムが実行されているか、組織が承認したソフトウェアコンポーネントの完全性が保たれているか、承認されていないコンポーネントが存在していないか、資産に既知の脆弱性がないか等、リソースへの接続要求を行う資産に関する情報などを包括的に監理する。将来的にはゼロトラストアーキテクチャにおけるポリシーエンジン（ポリシーに違反した情報を発見し、事前に定義されたアクションを実行する機構）にそれらの情報を提供する役割を担っていくことを想定している。

２.２　CRSA システム導入の目的と効果

CRSA システム導入の目的と効果を以下に示す。

1. 統一基準群等に準拠したコントロール（管理策）からの逸脱の迅速な把握と是正対応

   ●CRSA システムは、サイバーセキュリティ対策に必要なコントロールの実施状況を継続的にモニタリングできるため、どこが不適切な状態になっているかを迅速に把握し、是正対応を実施することができる。

   ●

2. インシデント発生時のトリアージ等の効果的な対応

   ●CRSA システムは、リアルタイムに自組織の資産状況、脆弱性対応状況等を把握できるため、インシデント発生時の資産等への影響規模や対応の優先度について迅速に判断できるようになる。

   ●

3. リアルタイムデータによるセキュリティ対策実施状況の効率的な報告

   ●CRSA システムを導入した組織は、リアルタイムな資産状態、アカウントの利用状況、インシデントの発生状況などを把握できる。これにより、サイバーセキュリティ対策状況を客観的かつ効率的に報告できるようになる。政府全体としては、各組織のサイバーセキュリティ対策状況を各組織に負担をかけることなく効率的に把握できるようになる。

   ●

4. 脅威やインシデントに対する政府横断的な脆弱箇所の迅速な発見と是正対応

   ●CRSA システムは、特定の脅威情報やインシデントに関する情報をもとに、影響のある箇所やインシデントの発生する可能性のある箇所を政府横断的に特定できるため、迅速かつ効果的に対処できるようになる。

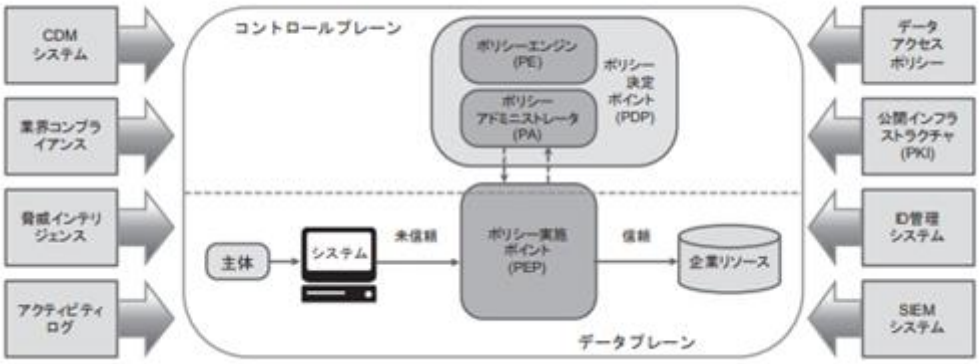
   ●

5. ゼロトラストアーキテクチャの運用環境を適切に維持

   ●ゼロトラストアーキテクチャの具体的な実装・運用においては、ネットワーク上の各デバイスでの脆弱性対応状況等を把握することにより、システム全体の健全性を把握し、維持していく必要がある。CRSA システムにおける診断結果は、ゼロトラストアーキテクチャにおけるポリシーエンジンのインプット情報としても活用できる。

２．３　CRSA システムの位置づけ

CRSA システムは、政府機関が継続的にサイバーセキュリティ体制を強化・向上させる上で必要な仕組みを提供することを目的としたシステムである。次の図は、NIST SP800-207 に掲載された、ゼロトラストアーキテクチャの論理的構成要素を示している。



. NIST Special Publication 800-207 より転記

図　2-3　ゼロトラストアーキテクチャの論理的構成要素

この図は、ゼロトラストアーキテクチャを構成している論理コンポーネント間の関係を示した概念図であり、米国連邦政府機関における CDM（Continuous Diagnostic and Mitigation）システムが、ゼロトラストアーキテクチャにおける参照リソースとして位置づけられている。CRSA システムは、この図における CDM システムに相当する。

CRSA システムは、組織の資産に関する情報を収集し、デバイスやソフトウェア等のセキュリティ構成や脆弱性対応の適正化を支援することにより、組織のネットワークとシステムのサイバーセキュリティを強化するための仕組みを提供する。また CRSA システムは、使用しているオペレーティングシステムにおいて適切な修正プログラムが適用されているかどうか、組織が承認したソフトウェアの完全性や承認されていないソフトウェアの存在、資産に既知の脆弱性があるかどうか等、接続要求を行う資産に関する情報をアクセス制御に適用する役割を担っている。

２．４　CRSA システムの考え方

情報システムを保護するために、組織は、情報システムに係わる様々な事象を

検知し、把握するためのプロセスを構築し、情報システムに潜在している脆弱なポイントを診断し、これに対処する能力を有する必要がある。CRSA システムはこの内、情報システムに係わる事象を検知、把握することにより、情報システムに係わる脆弱なポイントを診断する役割を担う。以下、CRSA システムの導入において、情報システムを保護するために検知、把握すべき事象についての考え方を示す。

(1)何がつながっているのか？

情報システムにおいて、どのようなデバイス、ソフトウェア、及びクラウドサービス等の外部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。

(2)誰がネットワークを使用しているか？

ネットワークの利用者がどのような組織に所属しているか、または利用者がどのような権限を持っているか等、利用者の属性を把握する。

(3)システムやネットワークで何が起こっているのか？

システムやネットワークにおいてどのような通信が発生しているかを把握する。これには、リスクのある通信が発見された際に、必要に応じて改善策を講ずることが含まれる。

(4)データはどのように保護されているか？

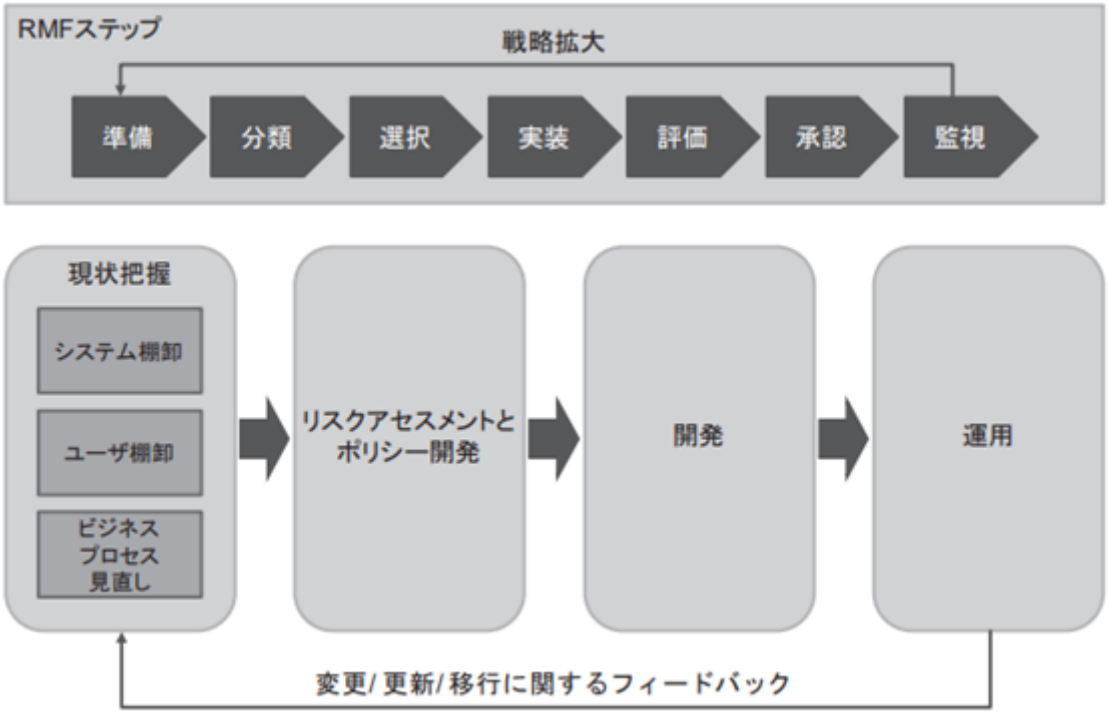
情報の保存時、転送時、及び利用時にどのように保護されるかについて、どのように保護されているかを把握する。

２.５　CRSA システムの導入

ゼロトラストアーキテクチャの環境下においては、組織がその資産（物理的及び仮想的）、主体（ユーザ権限を含む）、業務プロセスに関する詳細な情報を保持している必要がある。この情報は、各種の資産及び主体からのアクセス要求を制御する際に必要となるものであり、この情報が不十分であれば、適切なアクセス制御を実施することが困難になる。このため CRSA システムは、この情報が十分なものであるかを評価するための仕組みと捉えることができる。また、組織にゼロトラストアーキテクチャを導入する際には、事前準備として、資産、主体、データフロー、業務フローの調査を行う必要がある。ここでのデータフローとは、

アクセス制御に必要となる資産や主体に係る属性データの流れのことであり、業務フローとは、資産や主体がアクセスの対象とするリソースに到達するまでに経由する業務機能の流れのことである。この事前準備は、ゼロトラストアーキテクチャを導入するうえで非常に重要なプロセスである。組織は、現在の運用状況を把握していなければ、どのような新しいプロセスやシステムを導入する必要があるのかを判断することはできない。CRSA システムは、この調査プロセスを継続的に実施する機能を担っている。このため、CRSA システムの導入は、ゼロトラストアーキテクチャの維持において不可欠のものであると言うことができる。

ゼロトラストアーキテクチャを実現するための道筋は、図 2-4 のように表現できる。



NIST Special Publication 800-207 より転記

RMF: Risk Management Framework

図 2-4 ゼロトラストアーキテクチャの展開サイクル

CRSA システムは、この図に示された一連の展開サイクルにおいて、現状把握を支援するものと位置づけられる。すなわち、ゼロトラストアーキテクチャの展開サイクルにおいて、CRSA システムは、情報システムの運用におけるフィード

バックを基に、常時かつ継続的に情報システムを構成するデバイスとその利用者の状態を把握するためのものであり、リスクアセスメントに基づくポリシー開発を促すための仕組みを提供する。

3　CRSAのエンタープライズアーキテクチャ

3.1　エンタープライズアーキテクチャの概要

CRSA のエンタープライズアーキテクチャ（以下、「EA」という。）および EA を構成する各レイヤーの概要を以下に示す。EA とは、企業の事業を構成する要素（組織や人的資源等）の構造を整理して、構造化する方法論、またはその取り組みを指すものであり、業務プロセスや情報システム等の最適化・効率化を図るために導入・推進される。

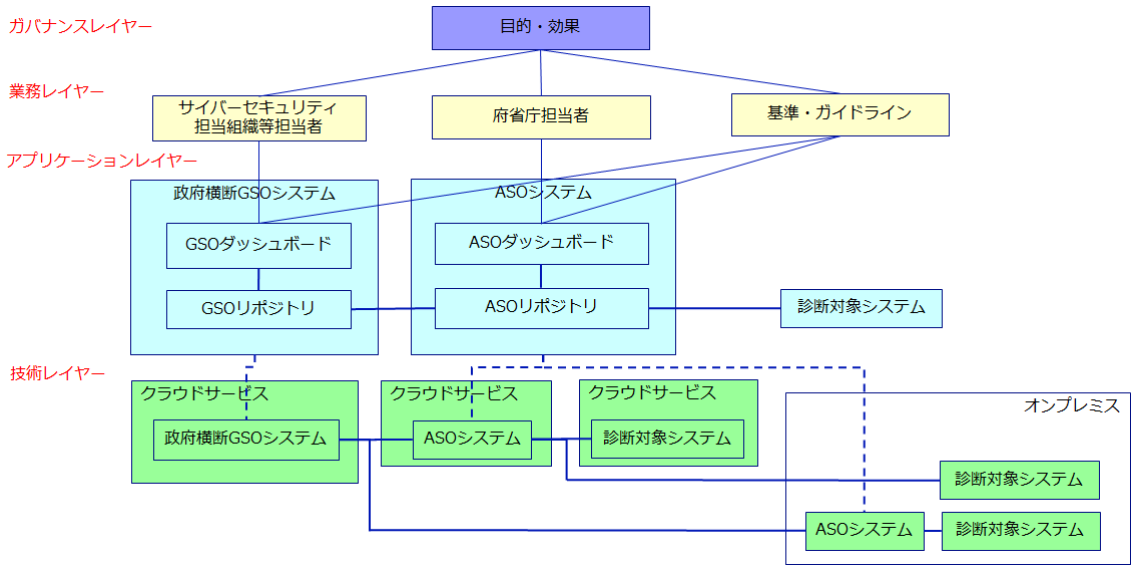


図　3-1　CRSA の EA の概要

- ガバナンスレイヤー：
  CRSA が目指すべき方向性に関係する要素として目的・効果を記述している。
- 業務レイヤー：
  CRSA システムが対象とする業務に関係する要素について記述している。
- アプリケーションレイヤー：
  CRSA システムを構成する機能に関係する要素を記述している。
- 技術レイヤー：
  アプリケーションレイヤーで記述した機能要素を実装するための技術に関係する要素を記述する。

図 3-2 EA を構成する各レイヤーの概要

CRSA の EA の構成について以下に解説する。

(1)ガバナンスレイヤー

CRSA が目指すべき方向性は、サイバーセキュリティ戦略（令和 3 年 9 月 28 日閣議決定）において以下とされている。

> **4.2. 国民が安全で安心して暮らせるデジタル社会の実現**
>
> サイバー空間の公共空間化とサイバー・フィジカルの垣根を越えた相互連関・連鎖の深化を踏まえ、あらゆるサービスの提供主体には、これまでの「任務保証」という考え方を深め、サイバー空間のこのような変容に適合したリスクマネジメントを講ずることが求められる。国は、サイバー空間の安全を確保することによって、サイバー空間に関わるあらゆる国民や主体が、安心してサイバー空間に参画できるよう、サイバー空間全体を俯瞰しつつ、関係主体との連携を通じて、自助・共助による自律的なリスクマネジメントが講じられる環境づくりに努める。また、国民の安全・安心の根幹に関わる経済社会基盤については、国は、防御すべき対象を不断に検証しつつ、関係主体と連携を図りながら、持ち得る全ての手段を活用して包括的なサイバー防御を講ずるとともに、先進的な取組の導入を率先して進めることで社会全体の実装を牽引し、サイバー空間の安全性・信頼性の確保を図る。
>
> これらの取組を通じて、サイバー空間に係るあらゆる主体の自助・共助・公助からなる多層的なサイバー防御体制を構築し、もって国全体のリスクの低減とレジリエンスの向上を図る。

(2)業務レイヤー

業務に関係する要素を以下に示す。

- サイバーセキュリティ担当組織等担当者
- 府省庁担当者
- 基準・ガイドライン（統一基準群及び各府省セキュリティポリシー等）

CRSA システムが対象となる可能性がある業務を以下に例示する。

- 統一基準群等に準拠したコントロール（管理策）からの逸脱の把握と是正等に係る業務

  府省庁担当者が行う内部監査、サイバーセキュリティ担当組織等担当者が行う監査等の現状把握と是正又は助言に係る業務。管理策の実施

状況が継続的にモニタリングできるため、より精度の高い状況把握に基づく監査等が可能になることが期待できる。

- インシデント発生時の対応に係る業務
  インシデント発生時の資産等への影響規模や対応の優先度を評価するための情報収集および分析等業務。
- セキュリティ対策実施状況の報告に係る業務
  府省庁担当者が行うセキュリティ対策の実施状況に係る報告業務。管理策の実施状況が継続的にモニタリングできるため、より精度の高い状況報告が可能になることが期待できる。
- 政府横断的な脆弱箇所の発見と是正対応に係る業務
  サイバーセキュリティ担当組織において実施する、政府横断的な脆弱箇所の調査・分析および検知した脆弱箇所の是正対応業務。
- ゼロトラストアーキテクチャの運用環境維持に係る業務
  パッチ適用の徹底等、ゼロトラストアーキテクチャの考え方に基づき運用環境を維持するための業務。

(3)アプリケーションレイヤー

CRSA システムの機能に関係する要素を以下に示す。

- 政府横断 GSO システム
  GSO ダッシュボードと GSO リポジトリにより構成される。GSO ダッシュボードは、データの可視化処理を担っており、サイバーセキュリティ担当組織等担当者がアクセスする。GSO リポジトリは、ASO リポジトリとのデータの授受および GSO ダッシュボードに表示するためのデータ処理を担う。
- ASO システム
  ASO ダッシュボードとASO リポジトリにより構成される。ASO ダッシュボードは、データの可視化処理を担っており、府省庁担当者がアクセスする。ASO リポジトリは、診断対象システムからのデータの収集、GSO リポジトリとのデータの授受およびASO ダッシュボードに表示するためのデータ処理を担う。ASO リポジトリは、診断対象システムからの収集したデータを GSO リポジトリに転送するためのデータの統計処理も担っている。
- 診断対象システム
  CRSA における診断対象となる情報システム。

(4)技術レイヤー

CRSA システムの実装に大きく影響する技術に関係する要素としては、クラウドサービスとオンプレミスの別が挙げられる。診断対象システムは、クラウドサービス上に構築されたものとオンプレミスとして構築されたものがあり、CRSA システムは双方に対応する必要がある。政府横断 GSO システムは、クラウドサービス上において実装する方針である。一方で、ASO システムは、診断対象システムを所管する各府省庁の判断により、クラウドサービス上に実装する場合とオンプレミスのシステムとして実装する場合がある。

３．２　CRSA システムの診断対象領域

CRSA システムは、下記の 4 つの領域を対象として診断を行う。

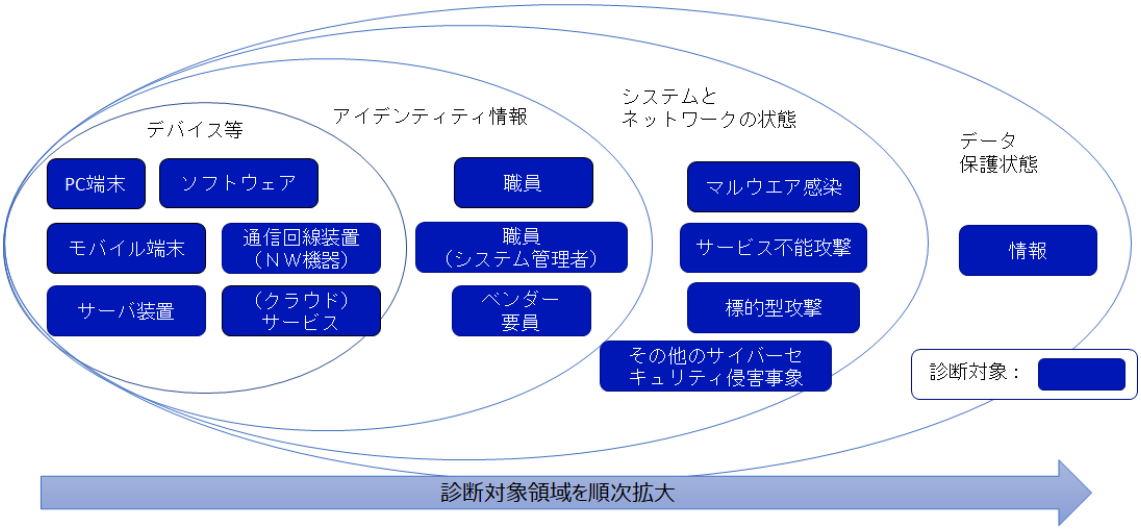


図　3-3　診断対象領域と診断対象

(1) デバイス等

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、端末やサーバ等の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かについて診断を行う。今後、監視対象を通信回線装置、その他デバイス（複合機や IoT デバイス等）、クラウド環境に拡張することが必要となる。

(2) アイデンティティ情報

府省庁の政府情報システムを利用するユーザのアイデンティティ情報について、管理が適切に行われているかについて診断を行う。今後、ユーザ

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な権限が付与されていることを確認する。

(3) システムとネットワークの状態

IP アドレスを持つデバイス間でどのようなトラフィックパターンやメッセージが発生しているかについて、特にマルウェア感染等のサイバーセキュリティ侵害事象に係るものについて診断を行う。将来的には、システムやアプリケーションのライフサイクル管理等（適切な管理策が導入されているか、定期的な脆弱性診断が実施されているか等）も診断対象とする。

(4) データ保護

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。機密データについて、その識別やアクセス制限、暗号化等の措置が適切に実施されていることを確認する。

３．３　CRSA システムを構成する機能とデータの流れ

アプリケーションレイヤーの概要を以下に示す。

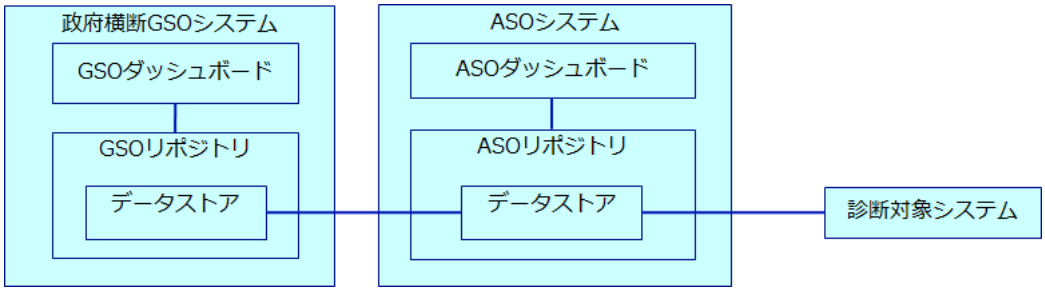


図　3-4　アプリケーションレイヤーの概要

３．３．１　GSO ダッシュボード

各システムの状況を含む、政府全体のシステムの状況について表示する。主な表示項目は、以下の通り。

- PC 端末の数
- モバイル端末の数

- 端末にインストールされているソフトウェアの数
- 検出されたソフトウェアの脆弱性の数
- 端末の設定違反（推奨していない設定）の数
- 端末の利用違反（未承認の利用者による利用）の数
- マルウェア等の検知数
- リスクスコアの値

３．３．２　ASO ダッシュボード

府省庁の政府情報システムの状況について表示する。主な表示項目は、以下の通り。

- PC 端末の内訳
- モバイル端末の内訳
- 端末にインストールされているソフトウェアの内訳
- 検出されたソフトウェアの脆弱性の内訳
- 端末の設定違反（推奨していない設定）の内訳
- 端末等の利用違反（未承認の利用者による利用）の内訳
- マルウェア等の検知の内訳
- リスクスコアの値

３．３．３　GSO リポジトリ

GSO リポジトリの機能は以下の通り。

- ASO リポジトリからの連携データの集約・統合
- インターネット上のデータベースからの脆弱性情報等のデータ収集
- 外部システムからの政府情報システムに係る情報等のデータ収集
- リスクスコア算出等の各種のデータ処理
- ダッシュボード表示データの編成

データストアに格納されるデータの構成は以下の通り。

表 3-1　GSO のデータストアの構成

No	データ名	説明
1	マスターデータ	各府省庁の政府情報システムに関する基礎情報や脆弱性に関する基礎情報等のマスターデータ

		群
2	連携データ	各府省庁の政府情報システムから収集された診断統計情報等、ASO システムから政府横断 GSO システムへ受け渡される連携データ群
3	スコアデータ	組織スコアやシステムスコア等のスコアデータ群
4	外部データ	セキュリティインシデントに係るデータや脆弱性に関する情報等の外部から取り込まれたデータ群
5	ログデータ	CRSA システムが記録するログデータ群

３．３．４　ASO リポジトリ

ダッシュボード表示データの編成 ASO リポジトリの機能は以下の通り。

- 府省庁の政府情報システムから取得した診断データの集約・統合
- リスクスコア算出等の各種のデータ処理
- ダッシュボード表示データの編成
- GSO リポジトリへ連携する統計情報の作成

データストアに格納されるデータの構成は以下の通り。

表 3-2　ASO のデータストアの構成

No	データ名	説明
1	マスターデータ	各府省庁の政府情報システムに関する基礎情報や脆弱性に関する基礎情報等のマスターデータ群
2	連携データ	ASO システムから政府横断 GSO システムへ受け渡す連携データ群
3	スコアデータ	デバイススコアやシステムスコア等のスコアデータ群
4	診断データ	各府省庁の政府情報システムから収集した診断情報
5	ログデータ	CRSA システムが記録するログデータ群

３．３．５　診断対象システム

診断対象システムは、システムを構成するデバイス種別に違いにより基盤系システムとアプリ系システムに大別される。

基盤系システムは、主として端末およびネットワーク機器によって構成されている。端末は、職員に貸与されるＰＣ端末に加えて、ＢＹＯＤ端末やモバイル端末を含む場合がある。

アプリ系システムは、主としてサーバ機器によって構成されている。

３．３．６　データの流れ

アプリケーションレイヤーでのデータの流れを以下に示す。

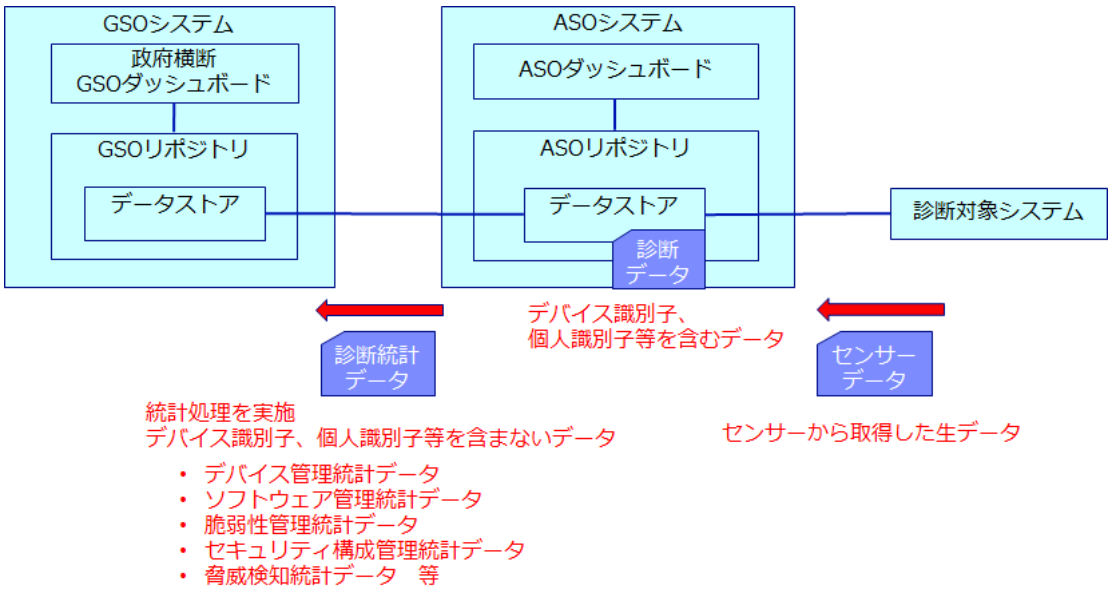


図　3-5　アプリケーションレイヤーでのデータの流れ

４　参照文書

1) サイバーセキュリティ戦略（令和３年９月 28 日　閣議決定）

サイバーセキュリティ 2021（2020 年度年次報告・2021 年度年次計画）、令和３年（2021 年）９月 27 日、サイバーセキュリティ戦略本部

デジタル社会の実現に向けた重点計画、令和３年 12 月 24 日，閣議決定

情報システムの整備及び管理の基本的な方針、令和３年 12 月 24 日，デジタル大臣決定

Zero Trust Architecture, NIST Special Publication 800-207

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（2020 年度 NEDO 事業 報告書管理番号：20220000000503）

2) 政府機関等の対策基準策定のためのガイドライン（令和５年度版）、令和５年７月４日、内閣官房 内閣サイバーセキュリティセンター

3) 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（令和５年度版）、令和５年７月４日、サイバーセキュリティ戦略本部

政府機関等のサイバーセキュリティ対策のための統一規範、令和５年７月４日改定、サイバーセキュリティ戦略本部決定

Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, April 16, 2018, National Institute of Standards and Technology

Security and Privacy Controls for Information Systems and Organizations, September 2020, NIST Special Publication 800-53 Revision 5

Risk Management Framework for Information Systems and Organizations /A System Life Cycle Approach for Security and Privacy, December 2018, NIST Special Publication 800-37 Revision 2

Standards for Security Categorization of Federal Information and Information Systems, February 2004, FIPS PUB 199

CIS Critical Security Controls® Version 8, Center for Internet Security

4) 政府情報システムに係る IT 資産管理の必要性について、2021 年５月、政府 CIO 補佐官等ディスカッションペーパー

5) 2021 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（2021 年度 NEDO 事業　報告書管理番号：20210000000194）

6) Continuous Diagnostics and Mitigation (CDM) Program (CISA), https://www.cisa.gov/resources-tools/programs/continuous-diagnostics-and-mitigation-cdm-program
7) Continuous Diagnostics and Mitigation (CDM) Training (CISA), https://www.cisa.gov/resources-tools/programs/continuous-diagnostics-and-mitigation-cdm-training