常時リスク診断・対処（CRSA）システム

アーキテクチャ

2022（令和 4）年 6 月 30 日

デジタル庁

〔標準ガイドライン群 ID〕
DS-211

〔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

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[1]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３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[2]」（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 システムの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 システムのアーキテクチャ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] https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf

[2] https://www.nisc.go.jp/policy/group/general/kijun.html

１．３　位置づけ

本文書は、標準ガイドライン群の一つとして位置づけられる。

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

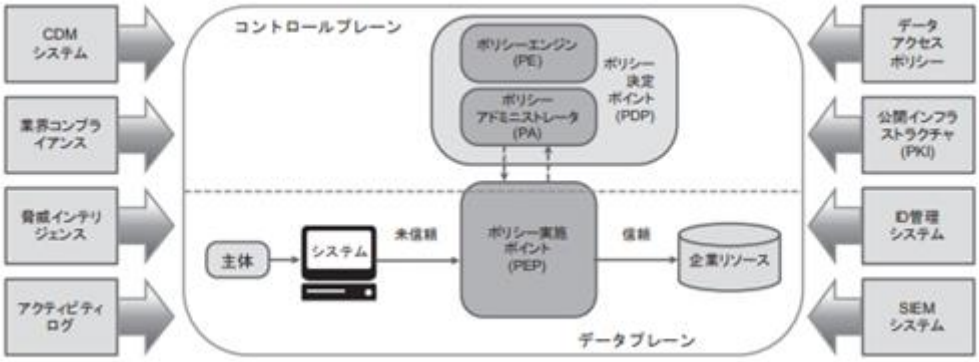
項番	用語	定義
1	常時リスク診断・対処（CRSA）プログラム	システムの挙動やソフトウェアの状況をリアルタイムに監視し対処するための取り組み CRSA: Continuous Risk Scoring and Action
2	CRSA システム	政府機関における常時リスク診断・対処（CRSA）プログラムを実現するためのシステム
3	統一基準群	政府機関等のサイバーセキュリティ対策のための統一基準群（令和３年度版）
4	NIST	アメリカ国立標準技術研究所 National Institute of Standards and Technology
5	CDM	Continuous Monitoring and Mitigation 継続的な診断及び軽減を意味する、米国連邦政府機関の情報セキュリティレベルを上げる取り組み
6	サイバーセキュリティ担当組織等担当者	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	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

項番	用語	定義
		テム
9	ASO システム	CRSA システムにおける府省庁のシステム
11	府省庁の政府情報システム	CRSA システムによるリアルタイム監視の対象となる府省庁のシステム
12	データ収集対象システム	ASO リポジトリの接続先として、府省庁システムにおけるセンサー／デバイス等により収集された診断データの収集対象となるシステム
13	GSO ダッシュボード	Government Security Operation Dashboard 政府機関横断セキュリティ運用ダッシュボード
14	GSO リポジトリ	Government Security Operation Repository 政府機関横断セキュリティ運用リポジトリ
15	ASO ダッシュボード	Agency Security Operation Dashboard 府省庁セキュリティ運用ダッシュボード
16	ASO リポジトリ	Agency Security Operation Repository 府省庁セキュリティ運用リポジトリ
17	レポート用リポジトリ	ASO リポジトリと GSO リポジトリとの間においてデータを連携するための仕組み
18	連携データ	GSO リポジトリと ASO リポジトリ間でやりとりされるデータ群
19	脅威ハンティング	セキュリティ対策製品等では検知が困難である潜在的な脅威を、様々な脅威情報を用いて能動的に探索、分析する活動
20	データストア	CRSA システムにおける各リポジトリで取り扱うデータを格納する領域

２　CRSAシステムの導入方針

２．１　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[3] 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 2-1　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）[4] 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

[3] https://csrc.nist.gov/publications/detail/sp/800-207/final

[4] https://www.gsa.gov/technology/technology-products-services/it-security/continuous-diagnostics-mitigation-cdm-program

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。

２.２　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？

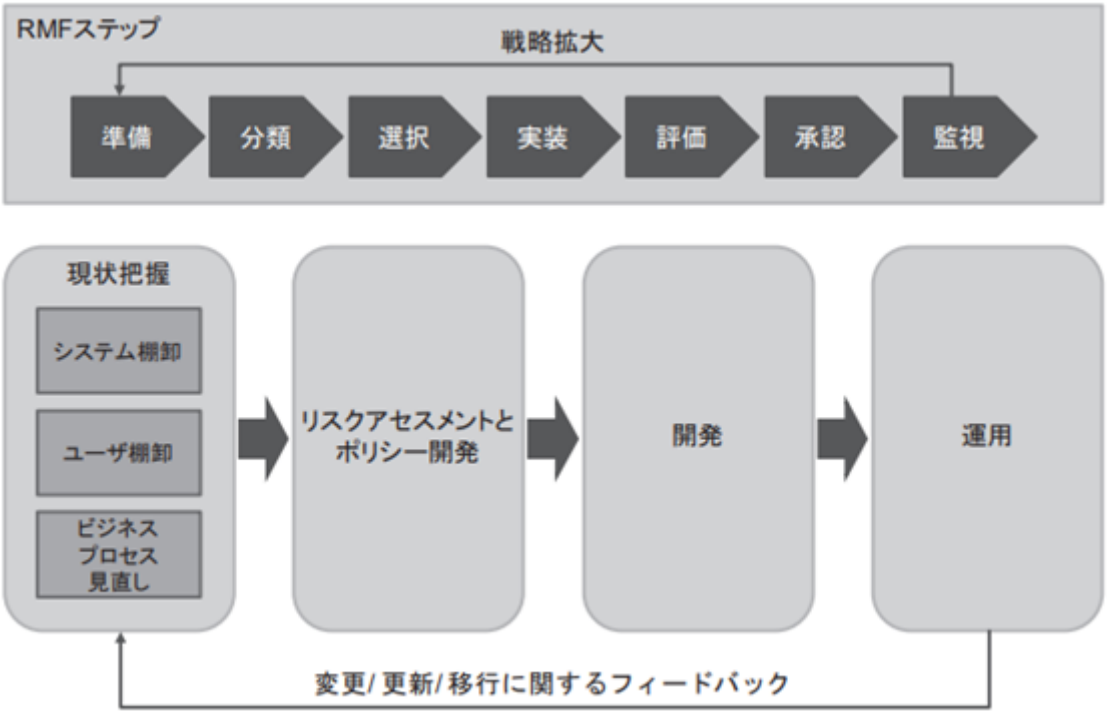
情報の保存時、転送時、及び利用時にどのように保護されるかについて、どのように保護されているかを把握する。

２.３　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 2-2 のように表現できる。



NIST Special Publication 800-207 より引用

図 2-2　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システムのアーキテクチャ

3.1　アーキテクチャ全体

CRSA システムのアーキテクチャは、ガバナンスレイヤー、業務レイヤー、アプリケーションレイヤー、技術レイヤーの４つのレイヤーから構成される。CRSA システムが診断対象としている政府情報システムに影響を与える関係要素を含めた、CRSA システムのアーキテクチャ全体図を以下に示す。

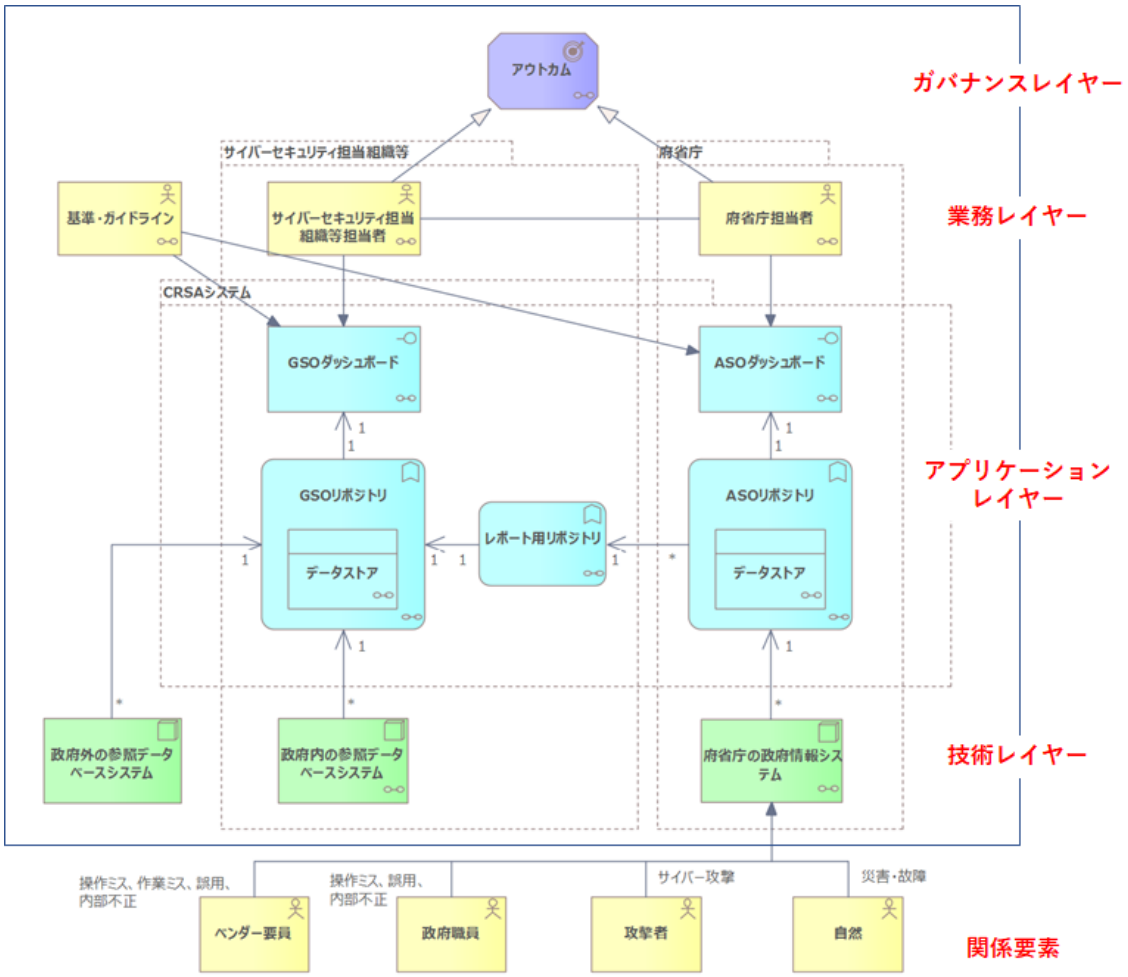


図 3-1　アーキテクチャ全体図

CRSA システムのアーキテクチャの構成について以下に解説する。

(1)ガバナンスレイヤー

ガバナンスレイヤーでは、CRSA システムが目指すべき方向性に関係する要素を記述する。ここでは、CRSA システムのアウトカム（結果要素）として、目的と対象領域を記述している。

(2)業務レイヤー

業務レイヤーでは、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する。ここでは、CRSA システムが対象とする業務として、サイバーセキュリティ担当組織等担当者が行う業務、府省庁担当者が行う業務及びこれらの業務に関係する基準・ガイドラインについて記述している。業務レイヤーの主たるアクターである担当組織等担当者と府省庁担当者は、ガバナンスレイヤーのアウトカムの実現を目指して業務を行う。

(3)アプリケーションレイヤー

アプリケーションレイヤーでは、CRSA システムを構成する機能に関係する要素を記述する。ここでは、CRSA システムにおけるデータ処理を担うリポジトリ機能とデータの可視化処理を担うダッシュボード機能について記述している。ダッシュボード機能は、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 ダッシュボードと府省庁担当者がアクセスする ASO ダッシュボードにより構成される。また、ダッシュボード機能には、CRSA システムに関係する基準・ガイドラインに準拠することが求められる。

(4)技術レイヤー

技術レイヤーでは、CRSA システムと連携する既存機能に関係する要素を記述する。ここでは、CRSA システムとのデータ連携の対象となるシステムについて記述している。CRSA システムは、政府情報システムの状態を把握することを目的としており、状態を把握する対象となる政府情報システムはこのレイヤーに位置付けられる。このため、アプリケーションレイヤーにおける ASO リポジトリは、政府情報システムからのデータ提供を受ける。また、ASO リポジトリは、複数の政府情報システムからデータ提供を受けることを想定しているため、両者間の多重度は１対多となっている。政府内の参照データベースシステムと政府外の参照データベースシステムは、政府情報システムの状態を把握するために参照すべき情報の取得対象となる。このため、アプリケーションレイヤーにおける GSO リポジトリは、これらの参照データベースシステムからのデータ提供

を受ける。GSO リポジトリは、政府内外とも複数の参照データベースシステムからデータ提供を受けることを想定しているため、両者間の多重度もそれぞれ１対多となっている。

(5)関係要素

関係要素は、政府情報システムに影響を与える外部要素を記述する。ここでは、CRSA システムが状態を把握する対象となる政府情報システムについて、セキュリティ侵害を引き起こす要素について記述している。

アーキテクチャ全体図は、縦方向に、サイバーセキュリティ担当組織等と府省庁に区分される。府省庁の政府情報システムにおいて収集された診断データの一部はレポート用リポジトリを介して GSO リポジトリに連携され、GSO ダッシュボードに表示される。

３.２　ガバナンスレイヤー

アーキテクチャ全体図で示したガバナンスレイヤーに関し、CRSA システムの導入目的と CRSA システムが状態を把握する対象とする政府情報システムの情報資産等の領域について記載する。

３．２．１　目的

CRSA システムのアーキテクチャは、下記の 4 点を目的として、政府組織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ツール、サービス及びダッシュボードの提供を行う。

(1)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。具体的には、ゼロトラストアーキテクチャの導入実現を目的として、政府内のデバイスや職員等の属性情報を収集し、アクセス制御のための認証・認可の判断に必要な情報を政府情報システムに提供する。

(2) 政府全体のサイバーセキュリティ体制の可視性の向上

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。

(3) 政府全体のセキュリティ運用機能の改善促進

政府全体で把握した参加組織の脆弱性対応及びインシデント対応について、脅威ハンティングを含むセキュリティ運用を支援するための仕組みを提供する。

(4) 統一基準群を踏まえた情報セキュリティ対策実効性確認の効率化

統一基準群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認知することができる仕組みを提供する。

３．２．２　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。

(1) デバイス等の監理

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、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の監理

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。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監理

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、情報システムやネットワークが適切に保護されており、理想的な状態を維持するための運用がされているかについて診断を行う。さらに、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。

(4) データ保護監理

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。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　業務レイヤー

アーキテクチャ全体図で示した業務レイヤーに関し、体制、業務、ユースケース、府省庁担当者の業務及びCRSAシステムに関係する基準・ガイドラインについて記載する。

３．３．１　サイバーセキュリティ担当組織等の体制

CRSA システムにおけるサイバーセキュリティ担当組織等担当者の役割分担は、以下の通り。

(1) 分析・評価担当者

CRSA システムから得られた各種の診断情報の分析と評価を行うとともに、各府省庁の担当者に改善策を助言する役割を担う。

(2) 基盤管理担当者

政府横断GSOシステムを管理するとともに、CRSAシステムが取り扱うデータや提供するサービス等の品質管理を行う役割を担う。

３．３．２　ユースケース

サイバーセキュリティ担当組織等担当者業務の主なユースケースを下記に示す。

(1) インシデント対応支援

分析・評価担当者は、府省庁におけるセキュリティインシデントの発生状況を随時把握し、同様のインシデントが他の政府情報システムにおいても発生する可能性を評価し、必要に応じて他の府省庁担当者に対して情報提供を行う等、政府横断的な対応支援を行う。例えば、発生したセキュリティインシデントの特徴として特定のオペレーティングシステムを標的とした攻撃であった場合に、CRSA システムを用いて同様のオペレーティングシステムを利用している政府情報システムを識別し、同システムを所管する府省庁担当者に対してセキュリティインシデントの発生状況に関する情報提供を行う。

(2) 脆弱性対応支援

分析・評価担当者は、新たな脆弱性情報を随時把握し、重要な脆弱性情報を追加・更新することにより、脆弱性マスターデータを維持管理する。また、分析・評価担当者は、新たな脆弱性情報を評価・分析し、特に重要と判断される脆弱性情報について、必要に応じて政府組織へ注意喚起を行う。

(3) スコア変動対応

分析・評価担当者は、GSO ダッシュボードに表示されるリスクスコア情報を定期的に確認し、スコアの変動に対応する。変動の大きなリスクスコアの変動要因について、政府横断的な分析を行い、状況を把握する。具体的には、デバイス管理リスクスコア等のリスクスコア毎に政府横断的な状況把握を継続的に行い、政府横断的に状況の変化を把握する。また、スコア変動の大きな情報システムを識別し、各リスクスコアの変動要因について分析を行い、当該情報システムの状況を把握する。分析の結果、対応が必要と判断される場合には、分析・評価担当者は当該システムを所管する府省庁担当者への問い合わせや改善のための助言を行う。

(4) 進捗管理

分析・評価担当者は、サイバーセキュリティ担当組織等担当者の業務に係る府省庁担当者とのやり取りについて、進捗管理を行う。スコア変動対応において府省庁担当者への改善のための助言等が発生した場合には、作業内容について起票を行い、府省庁担当者の対応状況を逐次把握することにより、作業進捗の管理を行う。

(5) 運用改善施策の検討

分析・評価担当者は、インシデント対応支援、脆弱性対応支援、スコア変動対応において得られた分析結果や知見をもとに、政府横断でのセキュリティ運用の改善施策を検討する。

(6) CRSA システムの維持管理

基盤管理担当者は、CRSA システムの維持管理の一環として、政府横断 GSO システムに係る保守・運用ベンダーを監督するとともに、ASO システムに係る保守・運用について府省庁担当者の支援を行う。基盤管理担当者は、CRSA システムが取り扱うデータについての品質を監視し、問題等が発生した場合には対応を行う。

(7) 接続システムライフサイクル管理

基盤管理担当者は、CRSA システムが診断する府省庁の政府情報システムの新規接続、変更、診断終了までの対応を行う。新規接続においては、政府情報システムへの ASO システムの導入支援を行うともに、政府横断 GSO システムとの接続試験を行い、接続確認を行う。また、府省庁が提示する資産等の申請情報をもとに、接続開始時において初期診断を行い、リスクスコア算出のための基準データを収集する。政府情報システムに変更が発生した場合には、府省庁担当者からの変更情報をもとに変更時診断を行い、リスクスコア算出のための基準データを修正する。診断終了時は、当該システムに係るデータの抹消処理を行う。

(8) CRSA プログラムの効果測定

分析・評価担当者及び基盤管理担当者は、期初において CRSA プログラムの効果指標と目標値を定め、期末において CRSA プログラムの効果測定の結果を評価し、課題となる項目について改善計画等を立案する。

３．３．３　サイバーセキュリティ担当組織等担当者の業務

サイバーセキュリティ担当組織等担当者の業務機能を以下に示す。

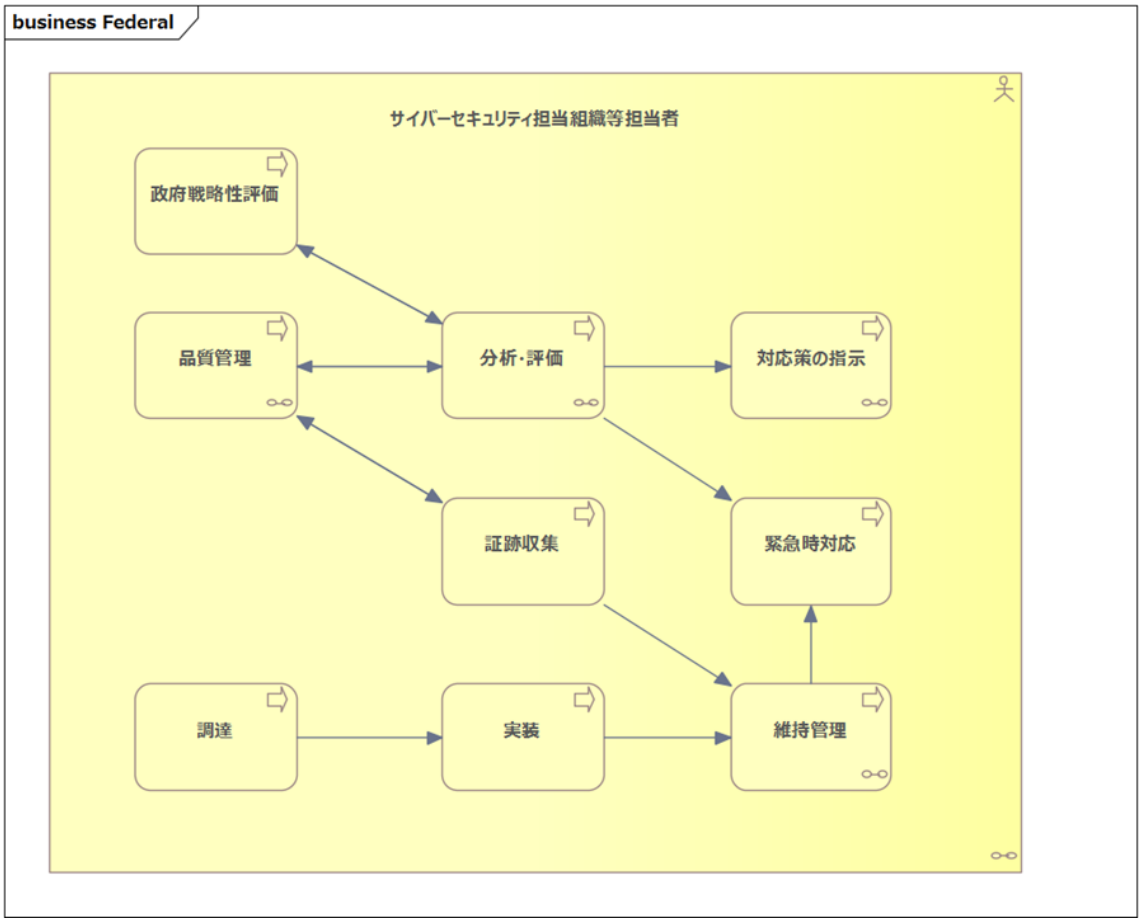


図 3-2　サイバーセキュリティ担当組織等担当者の業務機能

(1) 政府戦略性評価

分析・評価業務からのインプットを基に以下を実施する。

- 政府戦略に基づき、政府情報システムが目標とする状態を設定する。
- 分析・評価から得られた結果をもとに、政府戦略の実現状況を評価する。
- 評価結果に基づき改善計画を立案し、実行する。
- 政府情報システムに係る IT 資産の状態（デバイス数等の変動）を把握する。
- CRSA システムのパフォーマンスを評価するための効果指標（KPI）を設定する。
- 評価指標（KPI）に基づき CRSA システムのパフォーマンスを評価する。
- 評価結果に基づき改善計画を立案し、実行する。

(2) 品質管理

主として基盤管理担当者が行う業務で、分析・評価業務及び証跡収集業務からのインプットを基に以下を実施する。

- 府省庁の政府情報システムから提供されるデータ等、政府横断 GSO システムで取り扱うデータの品質管理を行う。
- GSO ダッシュボードの表示項目や画面イメージ等、政府横断 GSO システムが提供するサービスの品質管理を行う。
- GSO ダッシュボードの応答時間や政府横断 GSO システムの稼働時間等、政府横断 GSO システムにおけるシステムの品質管理を行う。

(3) 分析・評価

主として分析・評価担当者が行う業務で、政府戦略性評価業務及び品質管理業務からのインプットを基に以下を実施する。

- GSO ダッシュボードの表示データを基に分析・評価を行う。
- 各府省庁のデータに基づき、優先して実行すべき施策を検討する。
- CRSA システムの稼働に必要なマスター情報（情報システム一覧、脆弱性辞書、等）の管理を行う。

(4) 対応策の助言等

主として分析・評価担当者が行う業務で、府省庁担当者に対して以下の対応策について助言等を行い、進捗状況を把握する。

- 分析・評価の結果を基に、府省庁に対して対応策を助言する。
- サイバーセキュリティ担当組織等担当者から助言や照会を行った事案のうち、長期間状況変化が見られない事案について府省庁担当者に状況を確認する。
- 府省庁担当者からの報告をもとに今後の対応方針を府省庁担当者と協議する。
- 府省庁の対応を支援する。

(5) 証跡収集

主として分析・評価担当者が行う業務で、CRSA システムに係る以下の証跡収集を行う。

- CRSA システムを維持するための各種の証跡収集を行う。
- CRSA システムが取り扱うデータについてのプライバシー影響評価 (PIA) の実施を支援する。

(6) 緊急時対応

CRSA システムに係る緊急事態の発生時において、以下を実施する。

- 府省庁の政府情報システムにおけるインシデント発生状況を随時把握し、システム関連の情報提供等により、インシデント対応の支援を行う。
- CRSA システムのセキュリティインシデント発生時に対処する。
- CRSA システムの障害発生時に対処する。
- 災害発生に対処する。

(7) 調達

主として基盤管理担当者が行う業務で、CRSA システムに係る計画に基づきサービス等の調達を行う。

(8) 実装

主として基盤管理担当者が行う業務で、調達業務からのインプットを基に以下を実施する。

- 府省庁の政府情報システムを CRSA システムの対象として登録する。
- 政府横断 GSO システムの機能拡張等、各種の改善措置の実施を行う。

(9) 維持管理

主として基盤管理担当者が行う業務で、実装及び証跡収集業務からのインプットを基に以下を実施する。

- CRSA システムの保守・運用を実施する。
- 収集した証跡に基づく改善を実施する。
- 関係者に対して教育・訓練を行う。

３．３．４　府省庁の体制

府省庁においては、デジタル統括責任者及び最高情報セキュリティ責任者の下、CRSA システムから得られた分析の結果をもとに現状評価を行い、施策の見直しを検討するとともに、府省庁の政府情報システムの改善等を行う。CRSA システムにおける府省庁担当者の役割分担は、以下の通り。

(1) 分析・評価担当者

CRSA システムから得られた各種の診断情報の分析と評価を行い、改善策を立案するとともに、サイバーセキュリティ担当組織等担当者からの助言に基づき改善策を検討し、基盤管理担当者とともに対策を実施する役割を担う。関係する

担当者の例は、以下の通り。(統一基準群より抜粋)

- CSIRT 責任者
- CYMAT に属する職員
- 情報システムセキュリティ責任者

(2) 基盤管理担当者

ASO システムを管理するとともに、CRSA システムが取り扱うデータや提供するサービス等の品質管理を行う役割を担う。また、分析・評価担当者とともに改善策を実行する役割を担う。

３．３．５　府省庁担当者の業務

府省庁担当者の業務機能を以下に示す。

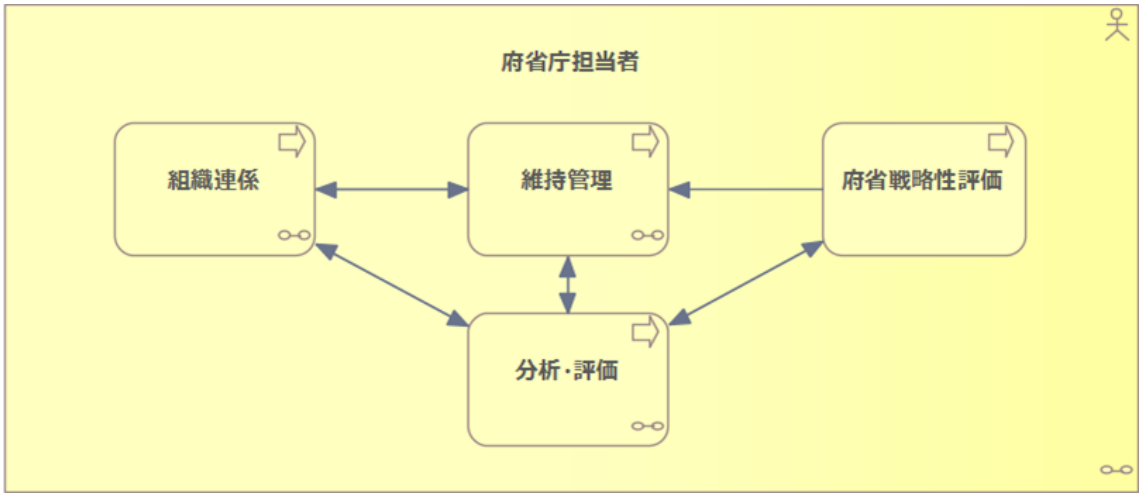


図 3-3　府省庁担当者の業務

(1) 府省庁戦略性評価

分析・評価業務からのインプットを基に以下を実施する。

- 府省庁戦略に基づき、府省庁の情報システムについて、目標とする状態を設定する。
- 分析・評価から得られた結果をもとに、府省庁の現状を評価する。

(2) 組織連携

主としてサイバーセキュリティ担当組織等との連携を行う。サイバーセキュリティ担当組織等からの依頼作業に関する進捗報告等の業務が含まれる。

(3) 維持管理

主として基盤管理担当者が行う業務で、以下を実施する。

- 政府情報システム及びASOシステムの保守・運用を行う。
- 分析・評価担当者及びサイバーセキュリティ担当組織等担当者からの指示を基に、サイバーセキュリティ対応策を行う。

(4) 分析・評価

主として分析・評価担当者が行う業務で、以下を実施する。

- ASOダッシュボードの表示データの分析を行う。
- 府省庁の方針に基づき、分析結果を評価する。

３．３．６　基準・ガイドライン

CRSA システムを設計・構築・運用する際に前提あるいは参考とした主な基準・ガイドラインを下記に示す。

(1) 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（令和３年度版）

CRSA システムは、以下に示す統一基準群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することを目的としている。

- 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
- 政府機関等のサイバーセキュリティ対策の運用等に関する指針
- 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３年度版）
- 政府機関等の対策基準策定のためのガイドライン（令和３年度版）

(2) 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1.1版

重要インフラのサイバーセキュリティを改善するために米国国立標準研究所（NIST）によって策定されたフレームワークであり、CRSA システムのアーキテクチャを作成する際に参考にした。

(3) 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（NIST SP800-37）

リスクマネジメントの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に米国国立標準研究所（NIST）によって策定されたガイドラインであり、

CRSA システムのアーキテクチャを作成する際に参考にした。

(4) 連邦政府の情報及び情報システムに対するセキュリティ分類規格（FIPS 199）

連邦政府が使用する情報システムのセキュリティカテゴリを確立するための米国連邦政府の標準であり、CRSA システムにおける情報システムのセキュリティ分類を定義する際に参考にした。

(5) The CIS Critical Security Controls v8

技術的なセキュリティ対策を整理するために米国 CIS(Center for Internet Security)によって策定されたガイドラインであり、リスクスコアを定義する際に参考にした。

(6) CIS Benchmarks

システムを安全に構成するための構成基準及びベストプラクティスを提供するために米国 CIS(Center for Internet Security)によって策定されたガイドラインであり、リスクスコアを定義する際に参考にした。

３．４　アプリケーションレイヤー

アーキテクチャ全体図で示したアプリケーションレイヤーに関し、各コンポーネントの概要について記載する。

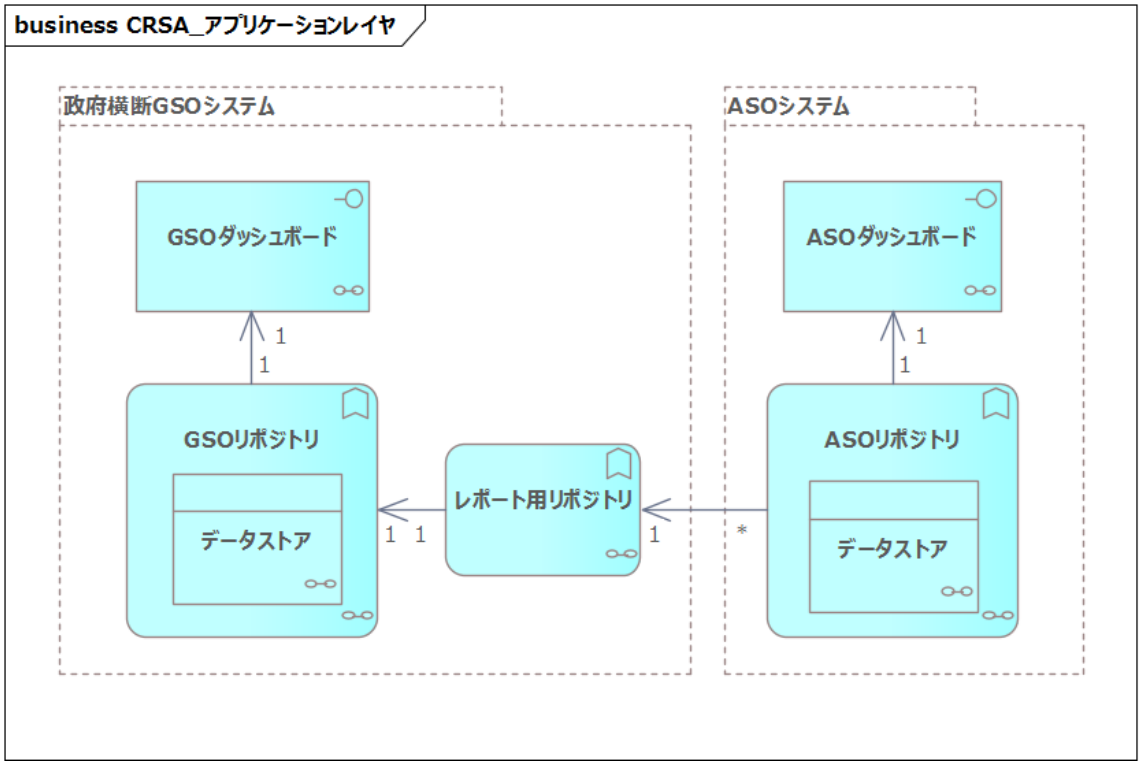


図 3-4　アプリケーションレイヤーの概要

CRSA システムは、政府横断 GSO システムと ASO システムにより構成される。政府横断 GSO システムは、GSO ダッシュボード、GSO リポジトリ及びレポート用リポジトリにより構成され、ASO システムは、ASO ダッシュボードと ASO リポジトリにより構成される。政府横断 GSO システムは複数の ASO システムからのデータを収集・統合するため、レポート用リポジトリは複数の ASO リポジトリからデータ提供を受けることを想定しているため、両者間の多重度は 1 対多となっている。

３．４．１　GSO ダッシュボード

各府省庁の政府情報システムの状況及び政府横断的な状況について表示する。主として、サイバーセキュリティ担当組織等の担当者が利用する。主な表示項目は、以下の通り。

- インシデント対応支援に関する項目
- 脆弱性対応支援に関に関する項目
- リスクスコアの変動に関する項目
- 各種作業の進捗状況に関する項目
- 政府内の資産や情報システムに関する項目

３．４．２　GSO リポジトリ

GSO リポジトリは、主にレポート用リポジトリを介して ASO リポジトリからのデータを取得する役割と GSO ダッシュボード機能に対して表示データを提供する役割を担う。GSO リポジトリの主な機能は以下の通り。

- 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
- GSO ダッシュボード表示データの編成

GSO リポジトリ内の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　データストアの構成

No	データ名	説明
1	診断統計データ	GSO リポジトリと ASO リポジトリ間でやりとりされる統計処理した診断データ
2	マスターデータ	リスクスコアデータの算出に使用する基準となるデータ群 例)各府省庁の政府情報システムに関する基礎情報、脆弱性に関する基礎情報
3	リスクスコアデータ	サイバー攻撃に関する攻撃対象領域の大きさを定量化したデータ群 例）府省庁スコア、情報システムリスクスコア
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	システムの動作に関するデータや業務の進捗に関するデータ等から構成されるデータ群

３．４．３　レポート用リポジトリ

レポート用リポジトリは、複数の ASO リポジトリからの連携データを受付けて、GSO リポジトリに転送する役割を担う。レポート用リポジトリの主な機能は以下の通り。

- 複数の ASO リポジトリからの連携データの収集
- 連携データの集約と GSO リポジトリへの転送
- 連携データ転送の正常性チェック

３．４．４　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。主として、府省庁担当者が利用する。主な表示項目は、以下の通り。

- 脆弱性対応に関に関する項目
- リスクスコアの変動に関する項目
- 資産や情報システムに関する項目
- 各種作業の進捗状況に関する項目

３．４．５　ASO リポジトリ

ASO リポジトリは、主にレポート用リポジトリを介して GSO リポジトリとデータ連携する役割と GSO ダッシュボード機能に対して表示データを提供する役割を担う。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
- ASO ダッシュボード表示データの編成
- 連携データの生成

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　データストアの構成

No	データ名	説明
1	診断データ	各府省庁の政府情報システムから収集したセンサーデータ及び、これらを加工したデータより構成されるデータ群
2	診断統計データ	GSO リポジトリと ASO リポジトリ間でやりとりされる統計処理した診断データ
3	マスターデータ	リスクスコアデータの算出に使用する基準となるデータ群

		例)各府省庁の政府情報システムに関する基礎情報、脆弱性に関する基礎情報
4	リスクスコアデータ	サイバー攻撃に関する攻撃対象領域の大きさを定量化したデータ群 例) デバイスリスクスコア、情報システムリスクスコア
5	ログデータ	システムの動作に関するデータや業務の進捗に関するデータ等から構成されるデータ群

３．５ 技術レイヤー

アーキテクチャ全体図で示した技術レイヤーに関し、CRSA システムと連携する主要な技術コンポーネントについて記載する。CRSA システムが必要とする外部データを提供する政府内の参照データベースシステムと政府外の参照データベースシステム及びCRSA システムが診断の対象とする府省庁の情報システムがある。

３．５．１　政府内の参照データベースシステム

政府内の参照データベースシステムの例として、下記のようなものがある。

(1) 政府システムの資産に係るデータベース

政府情報システムの情報資産に関するデータベースなど、政府情報システムに係る情報や政府職員に係る情報を格納しているデータベース等が該当する。

(2) 政府情報システムのインシデントに係るデータベース

政府情報システムへのサイバー攻撃等の分析・解析のためのデータベースなど、政府情報システムに発生したセキュリティインシデントに係る情報を格納しているデータベース等が該当する。

(3) 脆弱性情報に係るデータベース

脆弱性に係る情報を格納しているデータベース等が該当する。

３．５．２　政府外の参照データベースシステム

CRSA システムに関係する政府外の参照データベースシステムの例として、下記のようなものがある。

(1) 脆弱性情報に係るデータベース

脆弱性に係る情報を格納しているデータベース等が該当する。

(2) CRSA システムの維持管理に係るシステム

CRSA システムを構成するソフトウェアの更新ファイルの提供元等、CRSA システムの維持管理に係るシステムが該当する。

３．５．３　府省庁の政府情報システム

診断対象となる府省庁の政府情報システムには、下記のようなものがある。

(1) 基盤システム

政府情報システムのうち、行政端末機能、メールサーバ機能、ファイルサーバ機能、インターネット接続機能等を提供するシステム。代表的な府省庁の政府情報システムの例として、基盤システムの概要例を以下に示す。

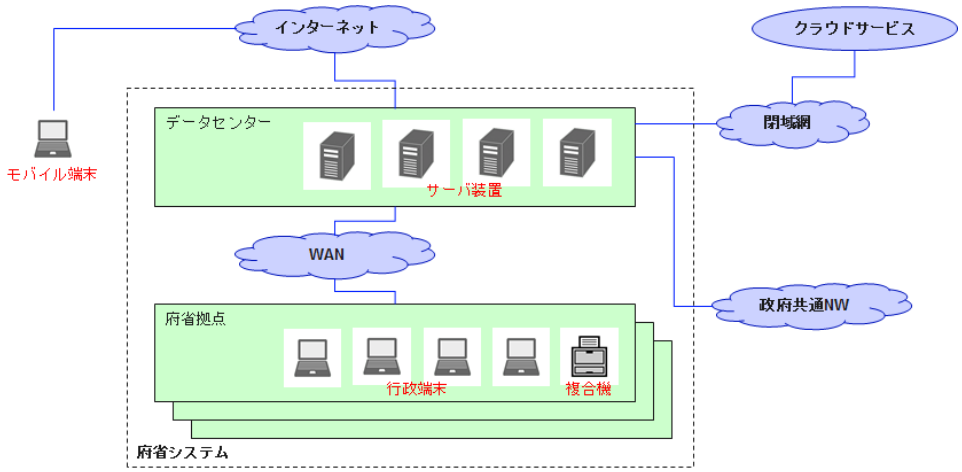


図 3-5　基盤システムの概要例

基盤システムは、行政端末や複合機等が設置された府省庁拠点とサーバ装置等が設置されたデータセンターから構成され、これらが WAN 回線で接続されている。外部接続先としてはインターネットと政府共通ネットワークがあり、データセンターから接続している。閉域網を介して各種のクラウドサービスと接続している場合がある。

各府省庁の情報システムは、それぞれのシステムを監視・管理するための管理

システムを有している場合が多い。診断情報は、府省庁の情報システムにおけるセンサー／デバイス等により収集され、各種の管理システム（以下、「データ収集対象システム」という。）に格納される。データ収集対象システムは、クラウドサービス上に構築されている場合もある。CRSA システムでは、これらのデータ収集対象システムに分散して格納される各種の情報を統合・集約するための機能が必要となる。

(2) その他の情報システム

その他の府省庁の政府情報システムとしては、府省庁のウェブサイトシステムや国民向けのサービスを提供する個別業務システムがある。

３．６　関係要素

アーキテクチャ全体図で示した技術レイヤーに関し、府省庁の政府情報システムに影響を与える関係要素について記載する。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として、以下が挙げられる。

- ベンダー要員（操作ミス、作業ミス、誤用、内部不正）
- 政府職員（操作ミス、誤用、内部不正）
- 攻撃者（サイバー攻撃）
- 自然（災害、故障）

上記の内、攻撃者（サイバー攻撃）に係る想定すべき代表的な脅威は以下のとおり。

- 脆弱性未対応デバイスへの攻撃
- ベンダー要員や政府職員による管理不備等に伴う設定誤りのあるデバイスへの攻撃
- 設定誤りのあるデバイスを踏み台にした攻撃
- 脆弱なアカウント設定による権限の不正利用（特に管理者アカウント）
- 事象発生の把握が遅延することによる対応の遅れ（このことによる被害の拡大）
- 外部設置サイトの不正利用によるネットワーク内部への攻撃（内部サーバの遠隔操作等）
- 保護対策が講じられていない重要情報の不正持ち出し

これらの想定すべき脅威は、これまでに政府システムにおいて発生したサイバーセキュリティ侵害事象に関する報告書を分析して抽出したものである。

4 参考文献

1) 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
2) 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
3) サイバーセキュリティ戦略、令和３年９月２８日、閣議決定
4) 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
5) Zero Trust Architecture, NIST Special Publication 800-207
6) 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）
7) 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３年７月７日改定、サイバーセキュリティ戦略本部決定
8) 政府機関等のサイバーセキュリティ対策の運用等に関する指針、令和３年７月７日改定、サイバーセキュリティ戦略本部決定
9) 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３年度版）、令和３年７月７日、サイバーセキュリティ戦略本部
10) 政府機関等の対策基準策定のためのガイドライン（令和３年度版）、令和３年７月７日、内閣官房 内閣サイバーセキュリティセンター
11) Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, April 16, 2018, National Institute of Standards and Technology
12) Security and Privacy Controls for Information Systems and Organizations, September 2020, NIST Special Publication 800-53 Revision 5
13) 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
14) Standards for Security Categorization of Federal Information and Information Systems, February 2004, FIPS PUB 199
15) CIS Critical Security Controls® Version 8, Center for Internet Security

16)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