セキュリティ関連技術ガイドライン群

令和4年6月24日
セキュリティTF

デジタル庁

セキュリティ関連技術ガイドライン群と各ドキュメントにおける概要

統一基準群で示されるセキュリティ対策に係る基本的な考え方と実践のポイントをふまえ、下記の4テーマについて統一基準群を具体化した技術ガイダンスを作成。今回は、Informativeな文書として位置づける。なお、将来的には内容を改訂し、各府省庁への適用することを視野にいれている。

統一基準群

informative

ゼロトラストアーキテクチャ適用方針

概要

政府機関では業務環境の変化に伴い、**イントラネットの外側で情報システムを利用するケースが増大**している。このような**従来の境界型のセキュリティモデルとは前提が異なる環境**で、情報セキュリティを確保するためには、境界型のセキュリティから大幅に拡張した考え方が求められる。本書は拡張の実態となる「ゼロトラストアーキテクチャ」の適用方針を説明する。

informative

常時リスク診断・対処（CRSA）システムアーキテクチャ

テキストを入力

概要

ゼロトラスト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。本書は、この活動を**継続的に実施するための、情報収集・分析**を目的としたプラットフォームのアーキテクチャについて説明する。

informative

政府情報システムのセキュリティ・バイ・デザインガイドライン

概要

情報システムに対し効率的にセキュリティを確保するため、**企画から運用まで一貫したセキュリティ対策**を実施する「**セキュリティ・バイ・デザイン**」の必要性が高まっている。本書では**システムライフサイクルにおけるセキュリティ対策**を俯瞰的に捉えるため、**各工程での実施内容**を記載すると共に**関係者の役割**についても定義する。

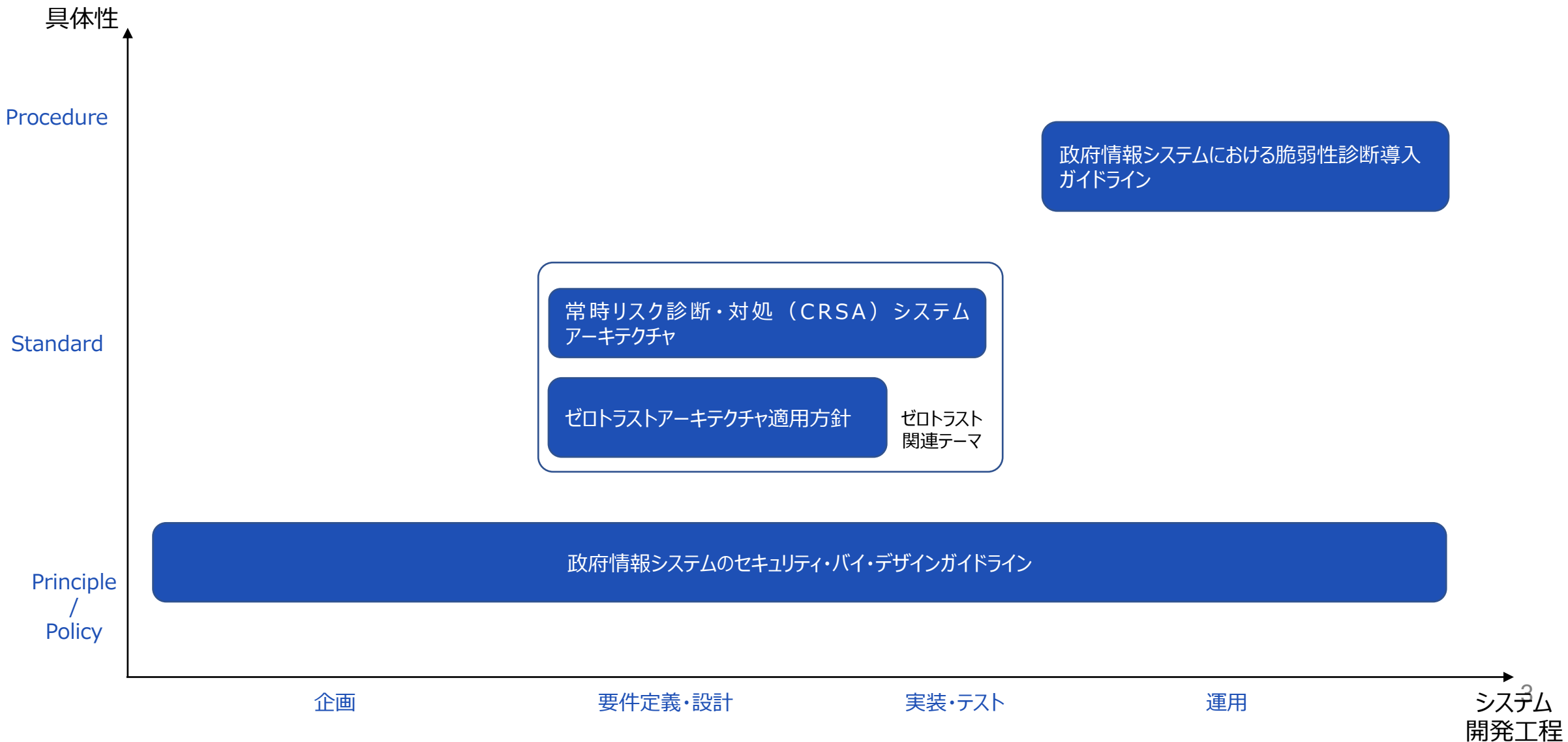
informa

政府情報システムにおける脆弱性診断ガイドライン

概要

政府機関では従来においても情報セキュリティリスクの低減を目的として**脆弱性診断を活用してきたが、導入方法に係る明確な基準や指針は十分整備されていない。**本書は、政府情報システムの関係者が**最適な脆弱性診断を選定、調達**できるようにするための基準及び指針を提供する。

ガイドライン全体の構造整理



政府情報システムのための
ゼロトラストアーキテクチャ
適用方針

本文書の背景となる課題感

- クラウド・バイ・デフォルト原則に従い、クラウドサービスの利活用が推進されている他、テレワークの利用等により、**イントラネット外の業務を前提**としたサイバーセキュリティ対策が必要。
- 近年の高度化した**サイバー攻撃を完全に予防・防御することは、従来の考え方と対策では難しい**。そのため、従来のネットワーク防御を中心にした**境界型セキュリティから考え方を拡張すること**が必要。
- 変革の実態である「**ゼロトラストアーキテクチャ」を適用するための基本的な方針および留意事項**を提供。

本文書の目的

- 課題への対応方針として、政府情報システムにおける**ゼロトラストアーキテクチャを適用する際の基本方針**を示すこと。
- ゼロトラストーアーキテクチャを適用する際の**実務的な留意事項**を示すこと。当該留意事項には運用時の留意事項も含まれる。

本文書の概要

1章 はじめに

1-1. 背景と目的

1-2. 適用対象

1-3. 位置づけ

1-4 用語

1-5. ゼロトラストアーキテクチャとは

- ゼロトラストアーキテクチャの概要

- 具体例

- 境界型セキュリティとの関係

2章 適用方針

1) リソースを識別し、特定できる状態にする

2) 主体の身元確認・当人認証を実施する

3) ネットワークを保護する

4) リソースの状態を確認する

5) アクセス制御ポリシーで評価し、アクセス管理をする

6) リソースとアクセスを観測する

3章 具体的な適用手順

3-1.適用プロセス

体制の構築

1) リソースや業務フローの識別・特定プロセス

2) スコープの決定プロセス

3) 実装・導入の推進プロセス

4) 観測プロセス

5) 評価及び改善プロセス

3-2. 適用における留意事項

1) 運用・保守体制を確保する

2)運用の設計と実装を初期段階から考慮した適用プロセスを進める

3) アクセス制御の評価タイミングをアクセス要求時に限定しない

4) 技術標準による相互互換性を確保する

5) 利用者の問い合わせ対応を強化する

1章 はじめに

1-1. 背景と目的

1-2. 適用対象

1-3. 位置づけ

1-4 用語

概念と対比されがちな境界型セキュリティとの関係

- 具体例

- 境界型セキュリティとの関係

コアとなる考え方と実例

2章 適用方針

1) リソースを識別し、特定できる状態にする

2) 主体の身元確認・当人認証を実施する

3) ネットワークを保護する

4) リソースの状態を確認する

5) アクセス制御ポリシーで評価し、アクセス管理をする

6) リソースとアクセスを観測する

ゼロトラスト・アーキテクチャを適用する際の留意事項について、適用後の運用を踏まえた方針

一過性のプロジェクトではなく、1つの適用サイクルを繰り返すことを前提に、そのサイクルの中で取りうるプロセスとその内容

3-1.適用プロセス

体制の構築

1) リソースや業務フローの識別・特定プロセス

2) スコープの決定プロセス

3) 実装・導入の推進プロセス

4) 観測プロセス

5) 評価及び改善プロセス

3-2. 適用における留意事項

1) 運用・保守体制を確保する

2)運用の設計と実装を初期段階から考慮した適用プロセスを進める

3) アクセス制御の評価タイミングをアクセス要求時に限定しない

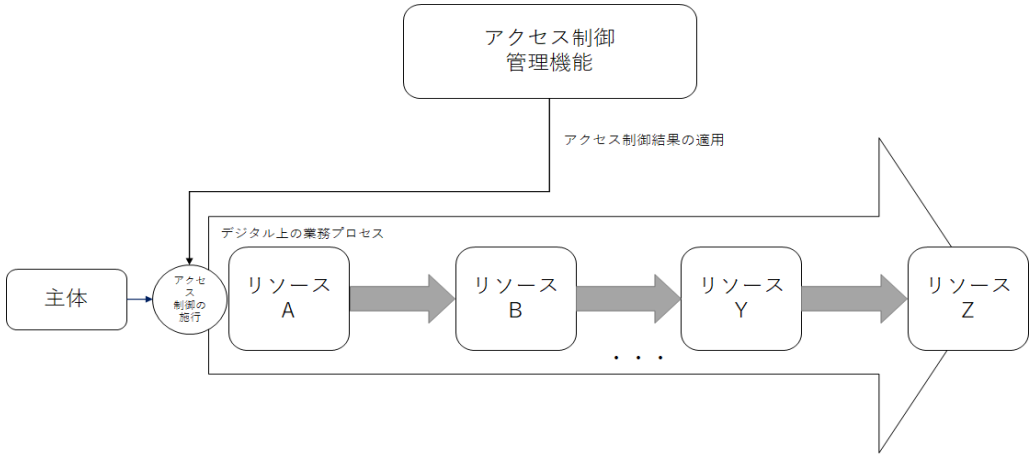
4) 技術標準による相互互換性を確保する

5) 利用者の問い合わせ対応を強化する

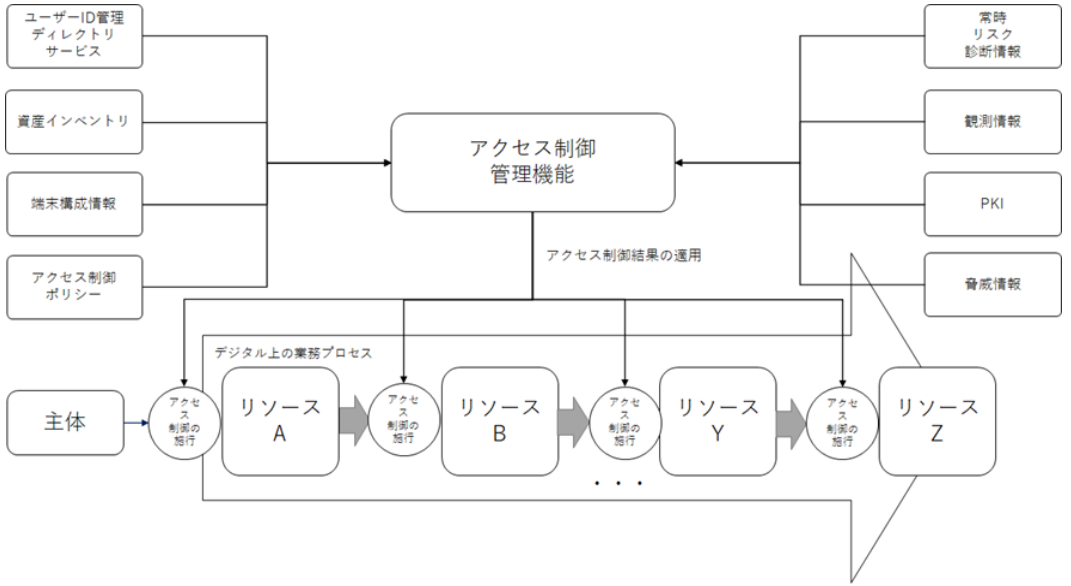
ゼロトラスト・アーキテクチャの概要の説明

ゼロトラスト・アーキテクチャに関する概念の説明

- **アクセスパターンが多様化（例: アプリケーション間など）**し、アクセスするリソースがアクセスされる側にもなりうる。
- **ゼロトラストアーキテクチャと境界型セキュリティは対立するものではない。**



境界型セキュリティ概念図



ゼロトラスト・アーキテクチャ概念図

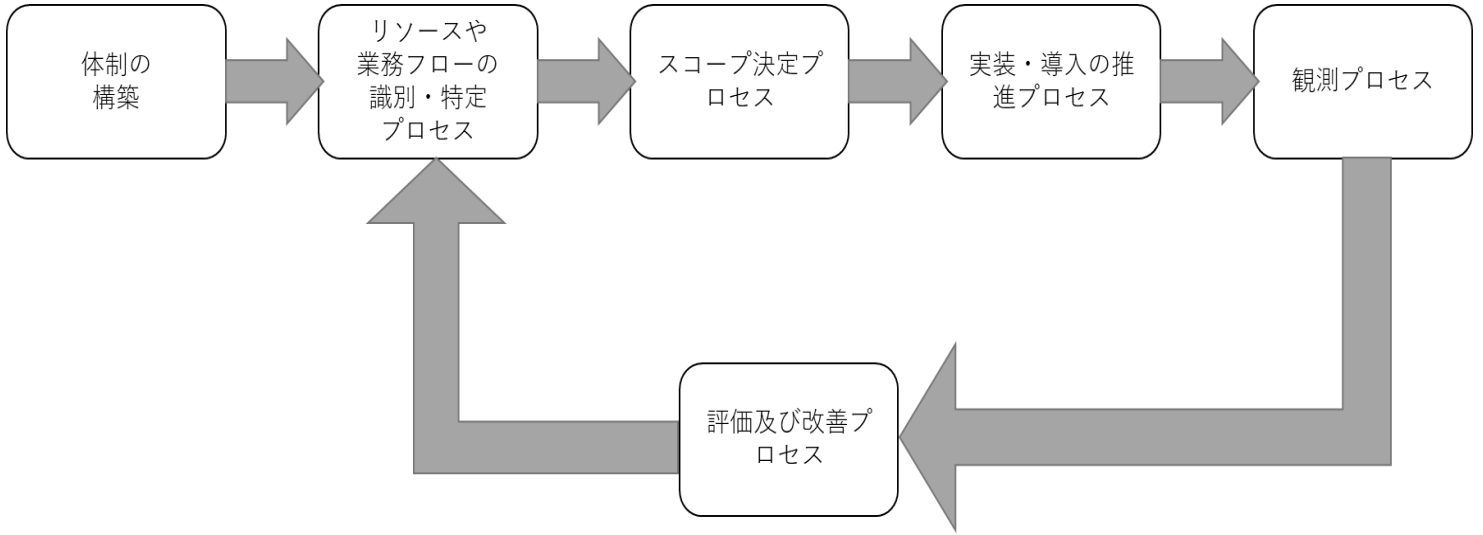
ゼロトラスト・アーキテクチャを適用する際の基本方針

1) リソースを識別し、特定できる状態にする
2) 主体の身元確認・当人認証を実施する
3) ネットワークを保護する
4) リソースの状態を確認する
5) アクセス制御ポリシーで評価し、アクセス管理をする
6) リソースとアクセスを観測する

（参考情報）
米国NIST SP800-207 Zero Trust Archite
米国政府 M-22-9 Moving the U.S. Government Toward Zero Trust Cybersecurity Principles
英国NCSC Zero Trust archtecture design principles

ゼロトラストアーキテクチャの適用プロセス

- ゼロトラストアーキテクチャは、**中長期的に運営する政府情報システムを堅牢にするためのアーキテクチャ。**
- 「ゼロトラストアーキテクチャの適用」は**一過性なプロジェクトではなく**、ましてや**単一のソリューションを導入したことで完了するものでもない。**
- プロジェクト・サイクルを**繰り返すことで成熟度をあげる行為**が、ゼロトラストアーキテクチャの適用。**プロセスはどこからでも開始可能。**



ゼロトラストアーキテクチャ適用プロセス

適用における留意事項

1)運用・保守体制を確保する
2)運用の設計と実装を、全体の設計段階から始める
3)アクセス制御の評価タイミングをアクセス要求時に限定しない
4)技術標準による相互互換性を確保する
5)利用者の問い合わせ対応を強化する

常時リスク診断・対処（CRSA）システム アーキテクチャ

本文書の背景となる課題感

- 従来型の**境界対策のみでは標的型攻撃等の高度サイバー攻撃への対応が困難**である
- 政府全体で**資産・ユーザ等の継続的な状態把握ができていない**
- 監視機能の性能が、**監視する専門家の能力に依存**している
- **統一基準群への準拠状況を常時的に把握する手段がない**
- 省庁内部での**インシデントの兆候把握ができない**

本文書の目的

- 課題への対応方針として、定常的に情報資産の状態を把握する仕組みとして**常時リスク診断・対処（CRSA）**の方針を示すこと
- CRSAを実現するためのシステムとして、**CRSAシステムのアーキテクチャ概要**を示すこと

CRSA: Continues Risk Scoring & Action

本文書の概要

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

CRSAシステムの位置づけと基本的な考え方を解説

2.　常時リスク診断・対処（CRSA）システムの導入方針

2.1. CRSAシステムの位置付け

2.2. CRSAシステムの考え方

2.3. CRSAシステムの導入

アーキテクチャの構造と要素を概説

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

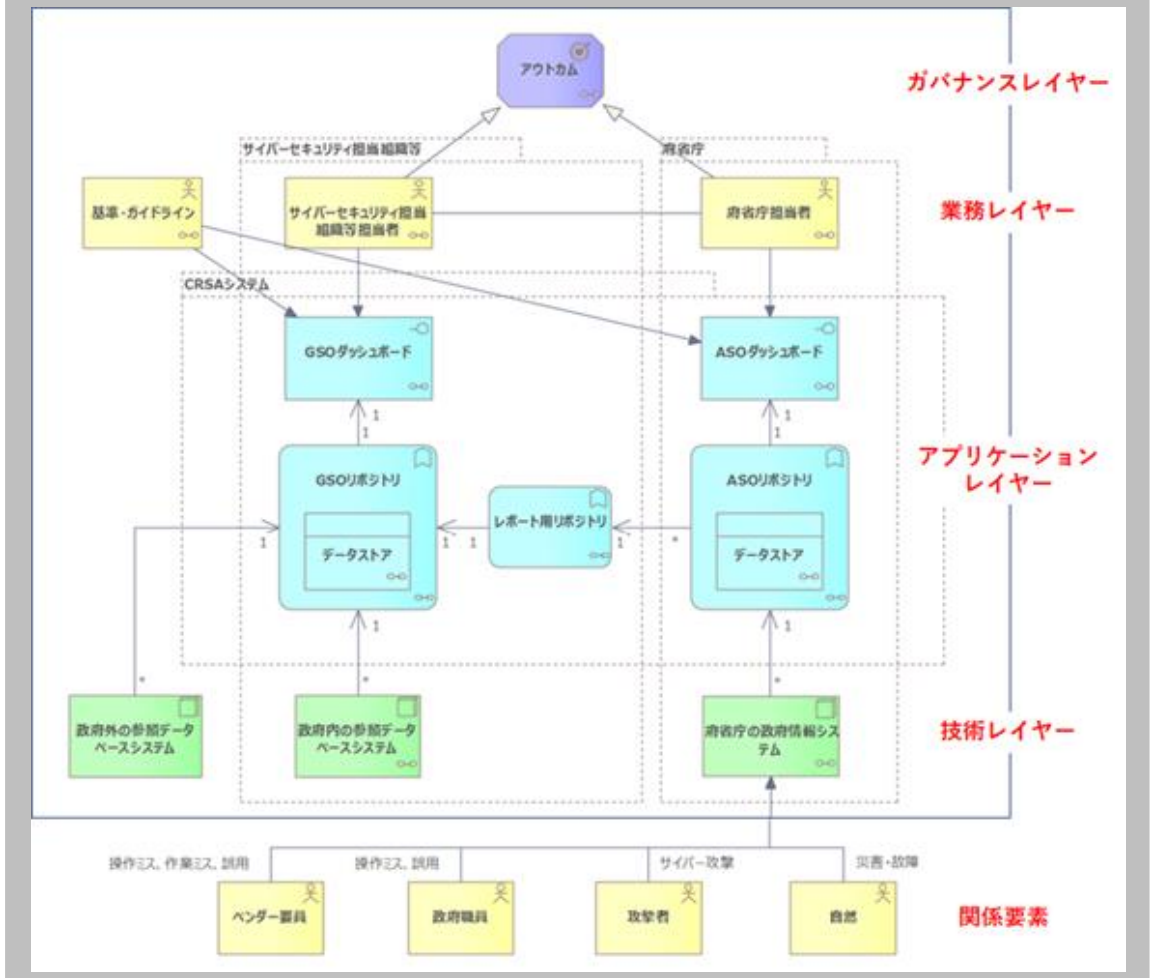
4.　参考文献

常時リスク診断・対処（CRSA）の方針

- CRSAとは、**政府情報システムにおいて常時的に情報資産の状態を把握し必要に応じて対処を実施**するものである
- 政府のゼロトラストアーキテクチャの実現に向けたシステムコンポーネントの一つとして、CRSAシステムを位置づけている
- CRSAシステムは、政府情報システムにおける**デバイス、ユーザー、システムおよびネットワーク、データについて、常時的に状態を把握・可視化し、不適切な状態を是正するための継続的な活動を支援**するシステムである
- CRSAシステムが提供する機能によって、政府全体のサイバーセキュリティの可視性を向上し、セキュリティ運用機能の改善を促進する

CRSAシステムアーキテクチャの概説

3.1.アーキテクチャ全体



(1)ガバナンスレイヤー
CRSAシステムアーキテクチャのアウトカム（結果要素）として、全体の目的とCRSAシステムの診断対象となる4つの対象領域を記述している。

(2)業務レイヤー
CRSAシステムアーキテクチャに係る利害関係者の業務と関係要素（基準・ガイドライン等）について記述している。

(3)アプリケーションレイヤー
CRSAシステムのデータ処理を行う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。

(4)技術レイヤー
CRSAシステムと連携する既存機能に関係する要素として、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

(5)関係要素
CRSAシステムの診断対象である府省庁の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。

政府情報システムのための
セキュリティ・バイ・デザインガイドライン

デジタル庁

本ガイドラインの背景（課題）、目的

【課題】

- デジタル庁のシステム開発におけるセキュリティ対策に関して、統制が働いていない
  - デジタル庁の各開発/運用工程で**どのようなセキュリティ対策をすべきか、PJMO（システムオーナー）任せ**になっている
  - 組織の品質管理部門も、**各システムのセキュリティリスクを把握、管理できていない状況**

本ガイドラインの目的

- 上記課題解決のため、政府情報システムにおける**セキュリティ・バイ・デザインの実施内容を定義**すること
- セキュリティ・バイ・デザインの実効性担保に不可欠な、**セキュリティリスク管理に関わる関係者の役割を定義**すること

本ガイドラインの記載方針

□**ガイドラインの記載方針：**

①本ガイドは**デジタル・ガバメント推進標準ガイドラインのセキュリティに係る参考資料**

②開発～運用工程まで含め、**システムライフサイクル全体をスコープ**に各工程の実施内容を記載、読み手はPJMOの担当者

③本ガイドラインに含める内容（読み手に理解頂く内容）は以下のとおり

a.セキュリティ・バイ・デザインの**必要性**

b.セキュリティ・バイ・デザインの**原理原則（考え方）**

本書の標準化スコープ

c.（**全体俯瞰的視点**で）各工程における**一般的なセキュリティ対策の実施内容、要求事項**

d.各工程において特に**重要となるセキュリティ対策の考え方**

e.セキュリティ・バイ・デザイン**実現に必要な関係者の役割・責任定義**

④本ガイドラインの本紙には、**以下の内容は含めない**

- **特定システムや特定脅威を対象にした具体的なセキュリティ対策**
- **特定のセキュリティフレームワーク、ベースラインをベースにした内容**

⑤本ガイドラインの別紙では各種ベストプラクティスや事例含め、具体的な内容を記載する予定（下記）

- 開発、運用工程で参照可能なセキュリティ標準、チェックリスト、実施イメージ（運用フロー）

⑥主な参照ガイドラインは下記の通り

- NCSC（security design principle）、NIST(CSF)、その他NISC関連基準

目次

目次

セキュリティバイデザインの基本を理解

セキュリティバイデザインの実施内容、要求事項を理解

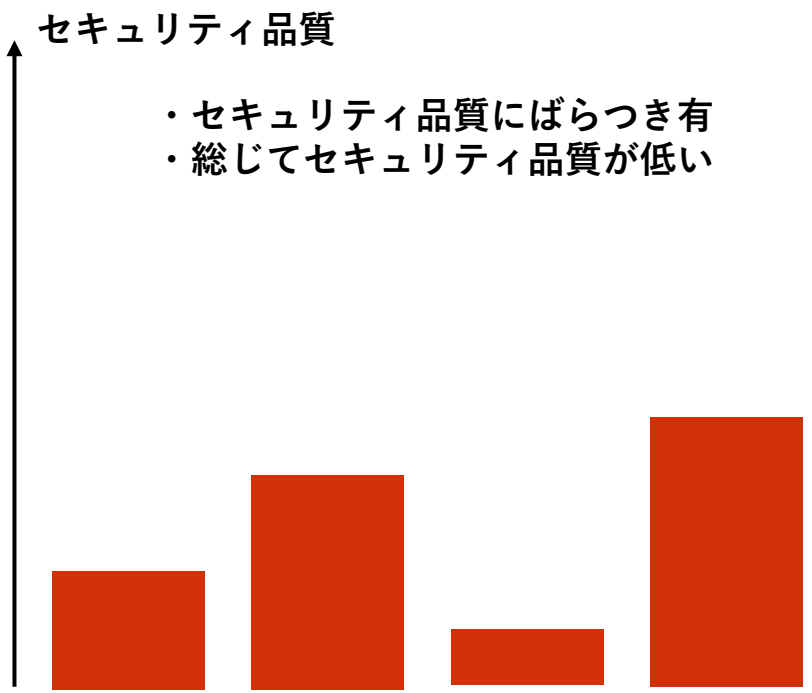
各工程の重要なセキュリティ対策の考え方を理解

セキュリティリスク管理に必要な役割を理解

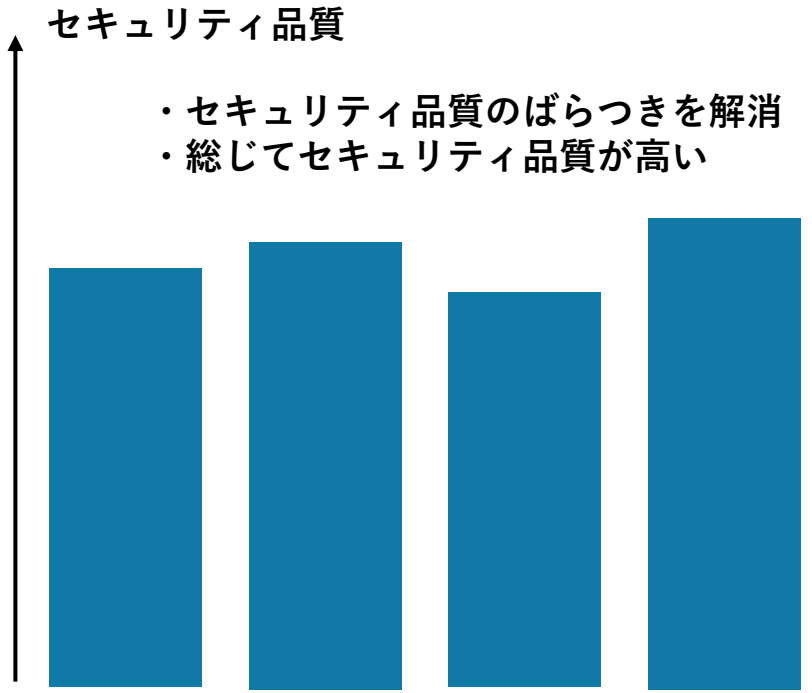
2-2.セキュリティ・バイ・デザインのメリット

セキュリティ・バイ・デザインの導入メリットを明記

□セキュリティバイデザインが導入されていない組織



□セキュリティバイデザインを導入している組織



2-3.セキュリティ・バイ・デザインの 原理原則

セキュリテイ・バイ・デザインの原理原則を定義

1. **事後的ではなく、予防的にセキュリティ対策を組み込むこと**
2. **全てのシステムライフサイクルを保護すること**
3. **初期設定値においてセキュリティが担保された状態を実現すること**
4. **システム特性に応じて過不足ないセキュリティ対策を施すこと**
5. **セキュリティリスクの評価、管理を実施すること**
6. **利便性を損なわないように、セキュリティを確保すること**

4. セキュリティ・バイ・デザインの実施内容

項番	デジタル・ガバメント推進標準ガイドラインおける工程名	セキュリティバイデザインの工程名	概要
1	サービス・業務企画	セキュリティリスク分析	•想定脅威にかかるセキュリティリスク分析の実施 •セキュリティ対応方針の決定
2	要件定義	セキュリティ要件定義	•システムにおける機能面、非機能面でのセキュリティ要件の定義
3	調達	セキュア調達	•セキュリティ調達仕様の策定、責任範囲の明確化 •安全な委託先、安全なプロダクトの選定
4	設計・開発	セキュリティ設計	•機能面と非機能面でのセキュリティ設計
5		セキュリティ実装	•セキュリティ機能の実装 •アプリケーションのセキュアコーディング •プラットフォームのセキュリティ設定の実施(堅牢化)
6		セキュリティテスト	•セキュリティ機能のテスト •脆弱性診断
7	サービス・業務の運営と改善	セキュリティ運用準備	•セキュリティ運用体制の確立 •セキュリティ運用手順の整備
8	運用及び保守	セキュリティ運用	•平時のセキュリティ運用 •有事のセキュリティ運用

ガイドライン本紙では工程ごとに下記を定義

実施内容

＋

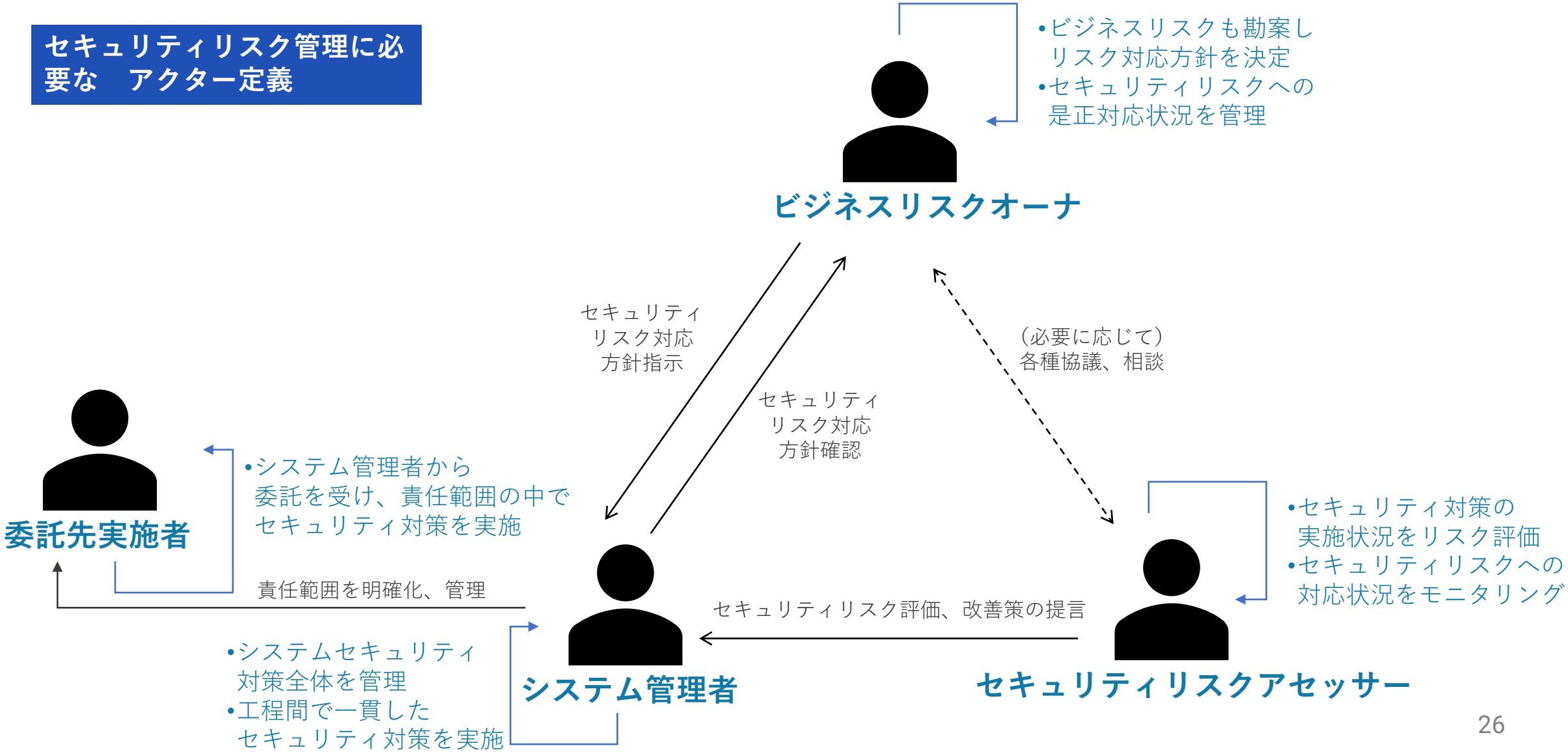
要求事項

＋

重要なセキュリティ対策の考え方

2-3. 関係者の役割

セキュリティリスク管理に必要な　アクター定義

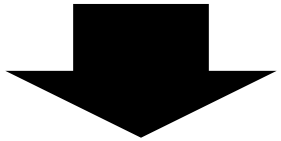


政府情報システムのための
脆弱性診断導入ガイドライン

背景となる課題感

政府情報システムに対する脆弱性診断の実施基準の不在

（各システム担当者の調達能力に依拠）



結果として顕在化している事象

- 自動スキャナをかけただけのWebアプリケーション診断結果
- 診断済みサイトの脆弱性（見落とし）を職員が複数検出
- 診断対象に含まれていないサブドメイン　等

本ガイドラインの目的

各機関のシステムにおいて、適切な脆弱性診断が実施される状態とすること
（結果として、政府情報システムの安全性向上に寄与すること）

目的の実現に際して必要となること

- 脆弱性診断の**調達能力の向上**
- システムの特性に応じた診断**調達基準の策定**

目次

1 章 はじめに

1-1. 目的とスコープ

1-2.

診断を実施する際の留意点を概説
⇒調達能力の向上

2 章 脆弱性診断の概要

2-1. 脆弱性対策における脆弱性診断の位置付け

2-2. 一般的な脆弱性診断の種別

- プラットフォーム脆弱性診断
- Webアプリケーション脆弱性診断
- スマートフォンアプリケーション脆弱性診断

2-3. 脆弱性診断を行うにあたっての留意事項

- 脆弱性診断サービスの選定
- 検出された脆弱性の深刻度評価
- 脆弱性診断に伴うリスクの管理

各機関で診断を行う際の実施基準
⇒ 調達基準の策定

3 章 政府情報システムにおける脆弱性診断の実施基準

3-1. 実施基準

- 構築時診断
- 定期診断

3-2. 診断技術要件

- プラットフォーム脆弱性診断要件
- Webアプリケーション脆弱性診断要件
- スマートフォンアプリケーション脆弱性診断要件

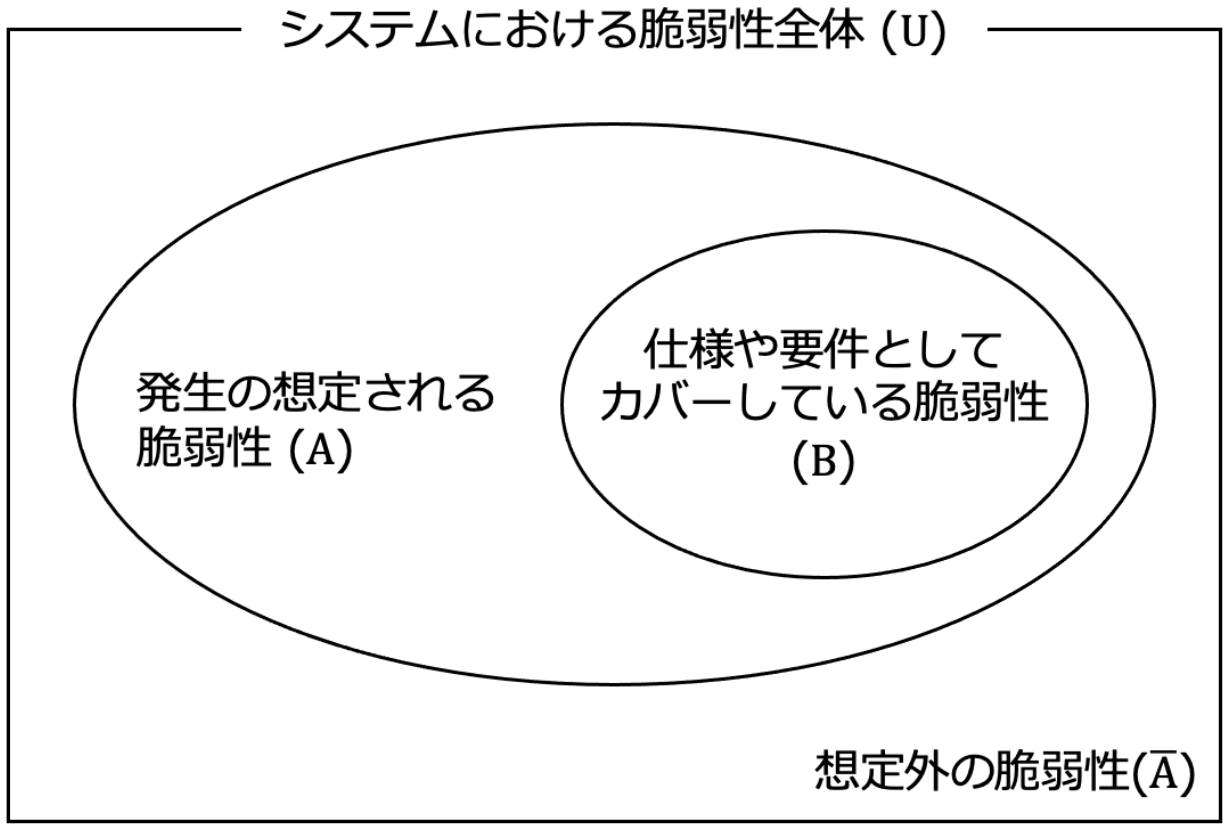
3-3. 脆弱性の対応基準

付録

各種テンプレート等

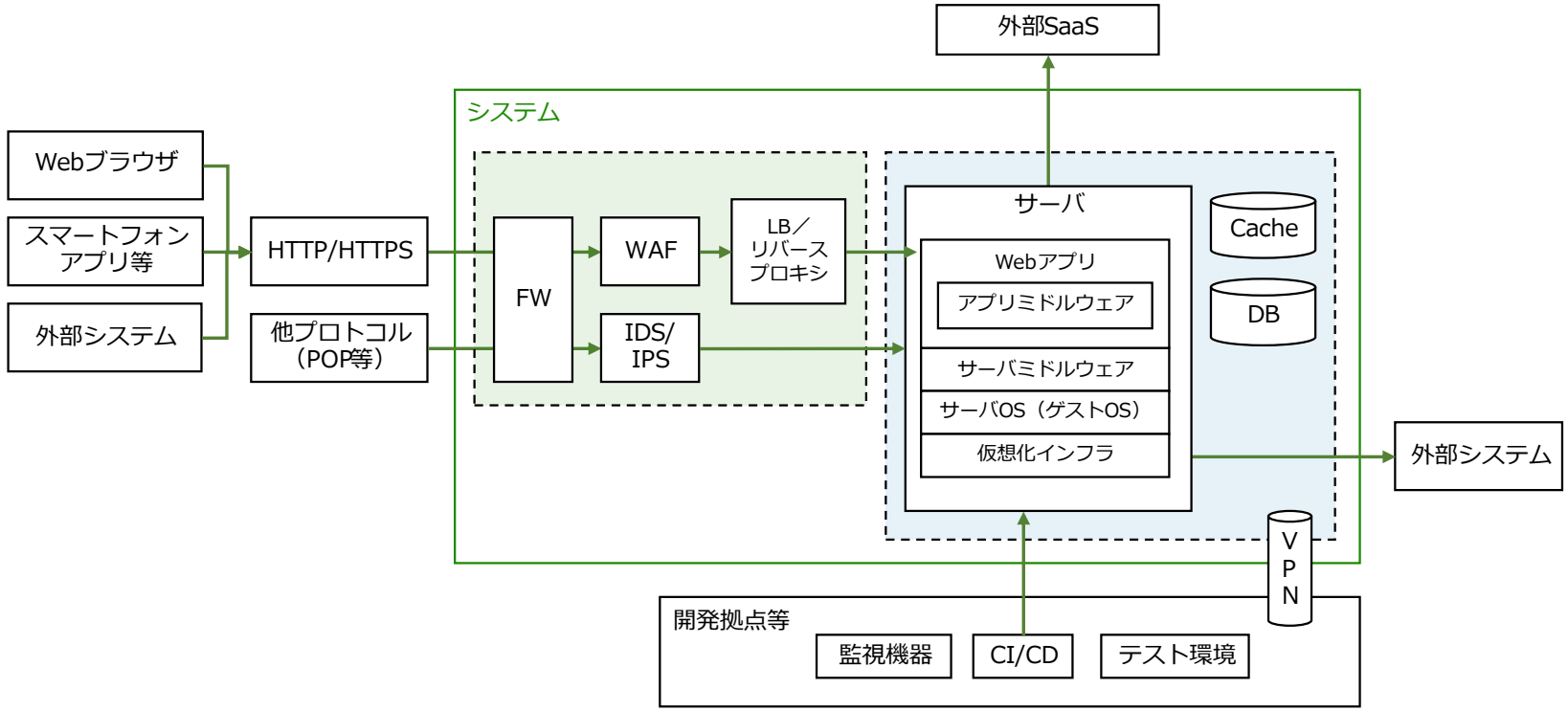
2-1. 脆弱性対策における脆弱性診断の位置付け

我々が対処しなければいけないシステムの脆弱性を説明した上で、
脆弱性対策の全体像における脆弱性診断の位置付けを解説



2-2. 一般的な脆弱性診断の種別

脆弱性の発生部位を説明した後、これらを網羅的に防ぐためには
様々な診断メニューを組み合わせる必要がある旨を解説



情報システムにおける脆弱性の発生部位

2-2-1. プラットフォーム脆弱性診断

プラットフォーム脆弱性診断で検出すべき脆弱性の全体像を解説

脆弱性の種別	概要
不要ポートの開放	ポートスキャンにより通信可能なポートを確認する。結果として、外部からの接続を意図していないオープンポートや、第三者に仕掛けられたバックドア等の不審なサービスが検出される。
脆弱なソフトウェアの利用	上記で検知したオープンポートに接続を試み、サーバから取得したバナー情報に基づき、ポートを待ち受けているOSやミドルウェアの情報を推定する。結果として、既知の脆弱性を含むバージョンのソフトウェアの利用等が検出される。
設定の不備	主にツールに搭載されたシグネチャに基づき、サーバの設定不備を確認する。結果として、推測可能なパスワード（システムの初期パスワード等）や意図しない情報の公開等の問題が検出される。
プロトコル固有の脆弱性	主にツールに搭載されたシグネチャに基づき、プロトコル固有の脆弱性を確認する。結果として、DNS、FTP、SSH、POP、SMTP、TELNET、SSL/TLS等のプロトコルを扱うソフトウェアの脆弱性や、脆弱なアルゴリズムの利用等が検出される。

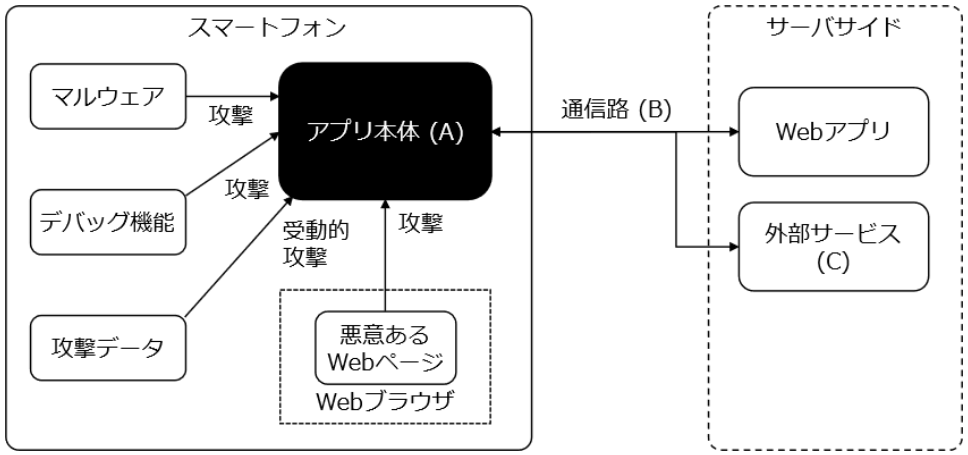
2-2-2. Webアプリケーション脆弱性診断

Webアプリ脆弱性診断で検出すべき脆弱性の全体像を解説

大分類	分類	脆弱性の例
(A)Webアプリの仕様に起因する脆弱性	(A-1)固有のビジネスロジックに依存するもの	ID連携の不備により他のユーザになりすましができる等
	(A-2)一般的な仕様上の不具合	他人のデータを読み書きできる、管理者権限の機能を誰でも利用できる、パスワードリセット機能の悪用、認証の回避等
(B)Webアプリの実装に起因する脆弱性	(B-1)実装のメカニズムに対する高度な理解が要求されるもの	レースコンディションによるデータの不整合、Officeファイルの投稿機能におけるXML外部エンティティ参照（XXE）、電子署名の迂回等
	(B-2)一般的な実装の不備	SQLインジェクション、ディレクトリトラバーサル、クロスサイトスクリプティング等
(C)利用するWebアプリミドルウェア固有の脆弱性		ログ出力や画像変換ライブラリ等における既知の脆弱性の悪用、CMS（Content Management System）やWebアプリフレームワークの誤用に起因する脆弱性等

2-2-3. スマホアプリ脆弱性診断

スマホアプリ脆弱性診断で検出すべき脆弱性の全体像を解説



脆弱性の発生部位	脆弱性の例
アプリ本体(A)	・ 他のアプリから機密情報を参照される ・ カスタムURLスキーム等のアプリ間連携機能により意図しない機能が実行される ・ WebView（アプリ上にWebページを表示する機能）上で悪意のあるWebページを開かされる
通信路(B)	・ サーバ証明書の検証不備 ・ 平文による機密情報の送受信
外部サービス(C)	・ アプリにハードコードされた認証情報を用いて外部サービスに不正アクセスされる ・ アプリにハードコードされたURLを通じて、脆弱な設定のクラウドストレージやMBaaS（Mobile Backend as a Service）の存在が特定される

左図は一般社団法人日本スマートフォンセキュリティ協会「Androidアプリのセキュア設計・セキュアコーディングガイド 」を基に作成

3. 診断の実施基準

脆弱性診断を行う目的の違いに応じて2つの診断種別を定義
また、各種別の対象と実施要件を設定

	対象システム	対象範囲	実施要件
構築時診断 各システムの構築時に行う診断で、脆弱性対策の実施内容の確認やセキュリティ品質の確保を目的として実施するもの	新規構築または機能追加等の改修を行ったシステム	外部から攻撃を受ける可能性のある箇所を中心に診断	**共通要件** ・診断品質に関わる要件 ・診断の管理要件 ・診断の成果物に関する要件 **診断種別ごとに個別の要件** ・プラットフォーム診断要件 ・Webアプリ診断要件 ・スマートフォンアプリ診断要件
定期診断 各システムの脆弱性対策が適切に実施されていることの自己点検や監査を目的として各機関で定期的に実施するもの	各機関の自己点検や監査計画に準ずる	各機関が保有するシステムのインベントリ情報（構成情報）に基づき総合的判断	

デジタル庁