セキュリティに関連する標準ガイドラインの策定について

令和6年1月16日

セキュリティ危機管理チーム

デジタル庁

ガイドライン/技術レポート（セキュリティ）

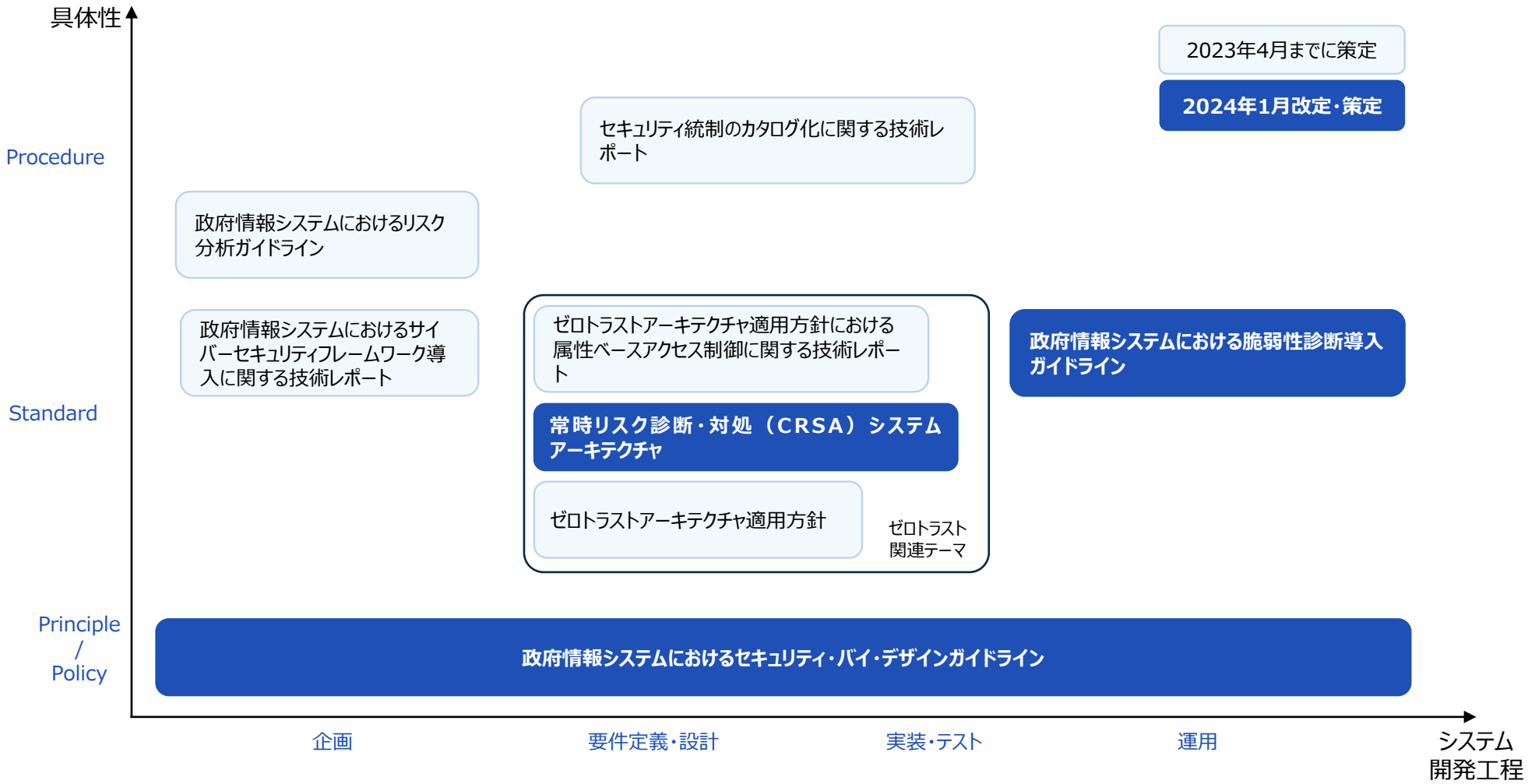
https://www.digital.go.jp/resources/standard_guidelines/#security

セキュリティ技術ガイドラインの公開

これまで8本のガイドライン・技術レポートを公開

- DS-200
  政府情報システムにおけるセキュリティ・バイ・デザインガイドライン
- DS-201
  政府情報システムにおけるセキュリティリスク分析ガイドライン～ベースラインと事業被害の組み合わせアプローチ～
- DS-210
  ゼロトラストアーキテクチャ適用方針
- DS-211
  常時リスク診断・対処（CRSA）アーキテクチャ
- DS-212
  ゼロトラストアーキテクチャ適用方針における属性ベースアクセス制御に関する技術レポート
- DS-220
  政府情報システムにおけるサイバーセキュリティフレームワーク導入に関する技術レポート
- DS-221
  政府情報システムにおける脆弱性診断導入ガイドライン
- DS-231
  セキュリティ統制のカタログ化に関する技術レポート

セキュリティ技術ガイドライン全体の構造整理



改定

DS-200
政府情報システムにおける
セキュリティ・バイ・デザインガイドライン

デジタル庁

本ガイドラインの概要

政府情報システムでのセキュリティ・バイ・デザイン導入推進を目的とした、各工程での実施プロセスを定義した文書

デジタル庁内における各PJに対するセキュリティ支援やセキュリティ研修、システムリリース判定基準のベースとなる文書

目次

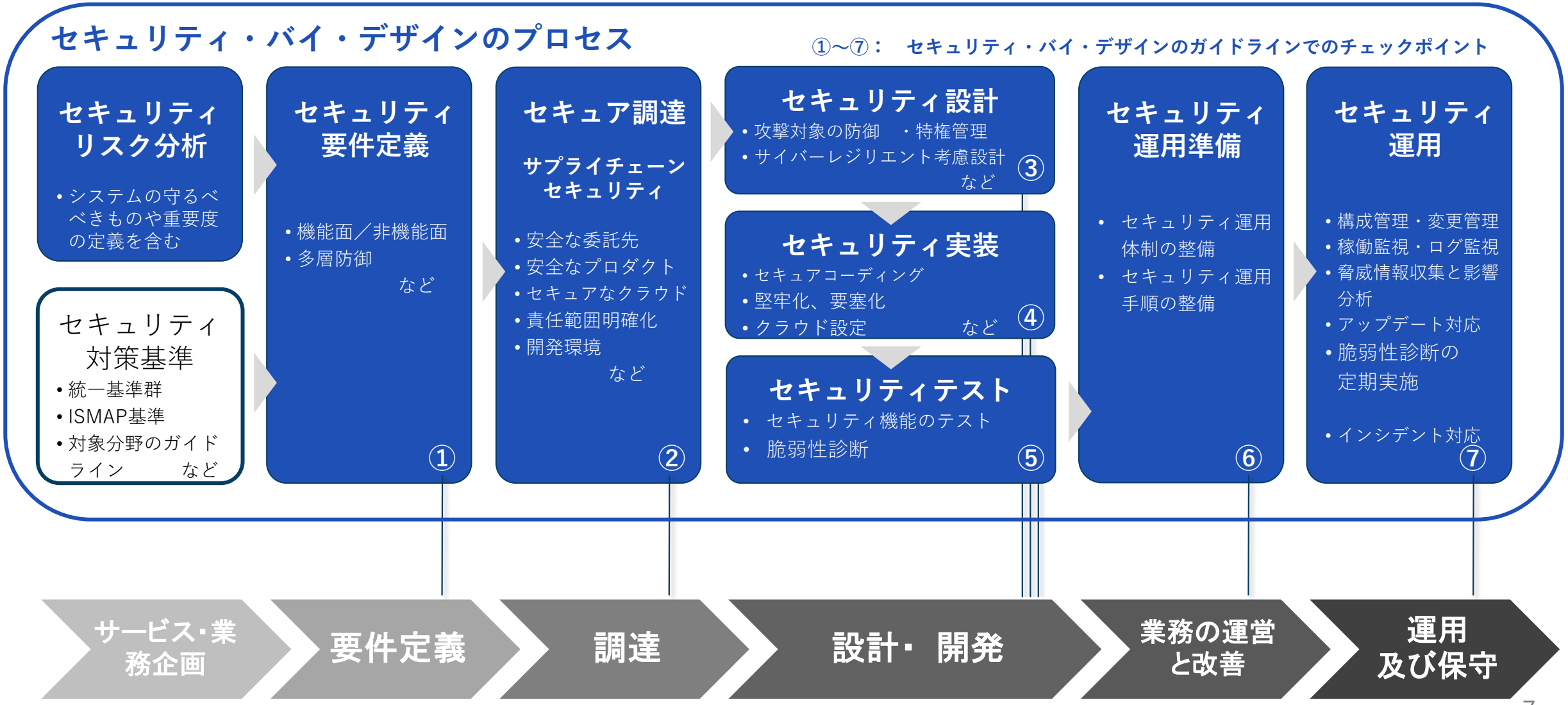
セキュリティバイデザインの基本を理解

各工程でセキュリティ要求事項、タスクを理解

各工程のセキュリティエッセンスを理解

セキュリティリスク管理に必要な役割を理解

セキュリティ･バイ･デザインの概要



デジタルガバメント推進標準ガイドラインのプロセス

本ガイドラインの修正方針

有識者からのFBや適用検証を行って文書品質を高めるとともに、環境の変化や世相を踏まえて内容を一部アップデートすることで、俯瞰的で、利用者にとってより使いやすい文書とすることを修正目的とする。

#	分類	修正方針	主な修正箇所
1	有識者や関連PJからフィードバックによる品質改善	各工程での実施内容や構成を見直して品質を強化、実用的なセキュリティtipsを拡充し、使いやすさを向上	4.セキュリティバイデザインの実施内容、別紙
2		リスク管理体制整備の重要性、具体的な体制整備イメージが持てるように内容を見直し	5.セキュリティバイデザインのリスク管理体制
3	世相や環境の変化を踏まえた内容のアップデート	システム利用者や開発/運用事業者等の「人に起因するセキュリティ脅威、対策の必要性、対策の考え方」を追記	文章全体
4		CISAのセキュアバイデザイン、セキュアバイデフォルト原則の内容を踏まえて更新	4.セキュリティバイデザインの実施内容
5		クラウド・バイ・デフォルトを前提としたクラウドベースの記載を拡充	4.セキュリティバイデザインの実施内容
6	その他	文章全体の誤記や不明瞭な表現の修正	文章全体
7		別紙各種のセキュリティ・バイ・デザイン導入をサポートする補助資料、ツールを改善	別紙2

本ガイドラインの修正方針

有識者からのFBや適用検証を行って文書品質を高めるとともに、環境の変化や世相を踏まえて内容を一部アップデートすることで、俯瞰的で、利用者にとってより使いやすい文書とすることを修正目的とする。

#	分類	修正方針	主な修正箇所
1	有識者や関連PJからフィードバックによる品質改善	各工程での実施内容や構成を見直して品質を強化、実用的なセキュリティtipsを拡充し、使いやすさを向上	4.セキュリティバイデザインの実施内容、別紙
2		リスク管理体制整備の重要性、具体的な体制整備イメージが持てるように内容を見直し	5.セキュリティバイデザインのリスク管理体制
3	世相や環境の変化を踏まえた内容のアップデート	システム利用者や開発/運用事業者等の「人に起因するセキュリティ脅威、対策の必要性、対策の考え方」を追記	文章全体
4		CISAのセキュアバイデザイン、セキュアバイデフォルト原則の内容を踏まえて更新	4.セキュリティバイデザインの実施内容
5		クラウド・バイ・デフォルトを前提としたクラウドベースの記載を拡充	4.セキュリティバイデザインの実施内容
6	その他	文章全体の誤記や不明瞭な表現の修正	文章全体
7		別紙各種のセキュリティ・バイ・デザイン導入をサポートする補助資料、ツールを改善	別紙2

［主な修正内容］

各工程での実施内容や構成を見直して品質を強化、実用的なセキュリティのtipsを拡充し、使いやすさを向上

実プロジェクトへの適用検証や有識者への確認で課題を導出

②セキュア調達のチェックリスト

#	確認項目	チェック
1	セキュリティ要件に基づき、調達におけるセキュリティ仕様（外部委託業務）を策定している	□
2	システムのセキュリティ対策、セキュリティ運用に抜け漏れが発生しないよう、自組織と委託先のセキュリティ対策に関する責任範囲を明確化している	□
3	セキュリティ仕様を実装できる能力を有し、セキュリティ管理基準を満たす安全な委託先を選定している	□
4	システムで利用する機器、ミドルウェア、ライブラリについて、不正侵入の経路となるバックドア等が含まれておらず、サポートを受けられる安全なプロダクトを選定している	□

③セキュリティ設計のチェックリスト

#	確認項目	チェック
1	セキュリティ設計の取りこぼしや属人化を避けるため、セキュリティベースラインやセキュリティフレームワークを導入して、セキュリティ設計を検証または実施している	□
2	外部からのアタックサーフェスを必要最小限に抑えるため、システムの操作に必要な外部インターフェースのみを公開する仕様としている	□
3	不要な機能、サービス、データはシステムから取り除いている	□
4	全ての外部入力は信頼せず、検証した上で、システムに被害が発生しないよう、安全に変換処理している	□
5	特定のセキュリティ対策が無効化された場合でも、システムに被害が発生しないように、多層/多重でのセキュリティ対策を実施している	□

□課題

- **確認項目が、何をどう確認すればよいか、分かり辛い（意図が不明瞭）**
- **本来確認すべき内容(セキュリティ対策)が不足している**
- **クラウドサービス前提とした記載とすべき、等**

改善

□アクション

- **分かりづらい記載について、確認目的や補足説明を追記**
- **抜漏れがないよう、必要なセキュリティ対策を再精査**
- **理解を補助するため、使用されるセキュリティ標準等の例示を記載**

②セキュア調達のチェックリスト

#	確認項目	チェック
1	【セキュリティ仕様の策定】 調達仕様書やそれに付随する文書の中に、システムに求めるセキュリティ要件に加えて、委託先に求めるセキュリティ（委託先での情報管理等）や機器/ソフトウェア/サービス選定時のセキュリティ要件等のサプライチェーンセキュリティに関する記載を含めている	□
2	【責任範囲の明確化】 システムのセキュリティ対策、セキュリティ運用に抜け漏れが発生しないよう、自組織と委託先のセキュリティ対策に関する責任範囲を明確化した上で調達仕様等におけるセキュリティ関連事項を記載している（クラウドサービスにおいては、クラウドサービスの特性（SaaS,IaaS,PaaS）等を踏まえて、責任範囲を明確化している）	□
3	【安全な委託先の選定】 セキュリティ仕様を実装できる能力を十分に有し、セキュリティ管理基準（委託元で提示したもの）を満たすことができる安全な委託先を選定している	□
4	【安全なプロダクトの選定】 システムで利用する機器、ミドルウェア、ライブラリについて、不正侵入の経路となるバックドア等が含まれておらず、サービスの提供期間中にサポートを受けられる安全なプロダクトを選定している	□

③セキュリティ設計のチェックリスト

#	確認項目	チェック
1	【セキュリティベースライン、フレームワークの導入】 セキュリティ設計の取りこぼしや属人化を避けるため、セキュリティベースラインやセキュリティフレームワークを参照して、網羅的なセキュリティ設計を実施している 例：CIS control（ver8）をベースラインとして用い、具体的な設計（設定）は CIS ベンチマークを用いてシステムにおけるセキュリティ設計を実施している　等	□
2	【アタックサーフェスの最小化】	□

［主な修正内容］

システム利用者や開発運用事業者等の「人に起因するセキュリティ脅威、対策の必要性、対策の考え方」を追記

主な想定脅威（従来）

〇システムの設定不備、脆弱性等に起因
・サイバー攻撃
・サプライチェーン攻撃、事故
・内部不正

想定脅威（今回）

〇システム面の不備、脆弱性等に起因
・サイバー攻撃
・サプライチェーン攻撃、事故
・内部不正

〇人の脆弱性に起因
・システム利用者によるオペレーション誤り
・システム開発/運用者によるオペレーション誤り

〇そのほか
・サービス仕様の不備（軽く触れる）

公金受け取り口座システムの利用者の作業ミスによる個人情報漏洩事故等が社会的に大きな話題になっており、対応が急務

［主な修正内容］

システム利用者や開発運用事業者等の「人に起因するセキュリティ脅威、対策の必要性、対策の考え方」を追記

2セキュリティ・バイ・デザインの概要

2.1　セキュリティ・バイ・デザインの概要

サイバー攻撃の大規模化/高度化に伴い、情報システムに対して確実にかつ効率的にセキュリティを確保するため、システム開発の企画工程からセキュリティを実装する「セキュリティ・バイ・デザイン」の必要性が高まっている。

また近年の情報システムは、絶え間なく、多種多様なセキュリティ脅威にさらされるため、システムの開発工程だけでなく、システムの運用工程のセキュリティ確保も同様に重要となり、開発工程と運用工程の双方において、シームレスで一貫性のあるセキュリティ対策が求められる。またサービス仕様や人的ミスに起因するセキュリティ事故についても大きな社会問題となっていることから、システムセキュリティの確保だけでなく、「サービス」や「人（開発者/運用者、サービス利用者）」も含めた総合的なセキュリティ対策が求められることも認識する必要がある。

一般的に、開発から運用まで含めたシステムライフサイクル全体でセキュリティ確保する方策を（とりわけソフトウェア開発においては）DevSecOpsと呼ぶが、本書では政府情報システムの企画工程から設計工程、開発工程、運用工程まで含めた全てのシステムライフサイクルにおいて、一貫したセキュリティを確保する方策のことを「セキュリティ・バイ・デザイン」と定義する。

人に起因するセキュリティ脅威の動向、対策の必要性を追記

2.3　セキュリティ・バイ・デザインの基本方針

セキュリティ・バイ・デザイン実施にあたっては、表層的で効果の薄いセキュリティ対策の実施に終始することを避けるため、セキュリティ・バイ・デザインの根底にある考え方（原則）を理解することが肝要となる。

本項では政府情報システムにおけるセキュリティ・バイ・デザインの原則となる基本方針を示す。政府情報システムにおけるセキュリティ・バイ・デザインは、下記基本方針に則ってシステムの開発工程、運用工程におけるセキュリティ対策を実施することが求められる。

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
   - セキュリティ・バイ・デザインは、インシデント等の発生を契機に取組むのではなく、予防的にセキュリティ・バイ・デザインを実施することが求められる。
2. 全てのシステムライフサイクルを保護すること
   - セキュリティ・バイ・デザインは特定工程においてのみ実施するのではなく、全てのシステムライフサイクルを通して、一貫したセキュリティ対策を実施することが求められる。
   - 委託先等の関係者間でセキュリティ対策の責任範囲を明確にし、抜け漏れなくセキュリティ対策を実施することが求められる。
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
   - システムの初期設定値としてセキュリティが担保された状態を実現し、システム運用者や利用者による設定ミスを極力少なくすることが求められる。
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実施すること
   - 全てのシステムに画一的なセキュリティ対策を講じるのではなく、システム特性や重要度等に応じて過不足なくセキュリティ対策を実施することが求められる。
   - セキュリティ対策を検討する際は、システム仕様におけるセキュリティ対策だけでなく、サービス仕様や人的ミスに起因するセキュリティ事故の発生も考慮した上で、多角的にセキュリティ対策を検討する必要がある。

4.2　セキュリティ・バイ・デザインの実施内容

- 人的ミスへの対応策の検討
  - サービス利用者やシステム管理者、運用者等の人的ミスにつながる可能性のあるシステム仕様については、デザインの改善や多重の技術的対策等を導入することで、発生防止につとめる。
  - システム仕様の改善だけで十分なリスク低減ができない場合は、ワークフロー（ダブルチェックや承認フローを設定等）や作業者のリテラシーを高めるための取組みとして必要な教育コンテンツを事前に提供する等の対策を講じることで、人による不確定性を極力排除する。
  - 人的セキュリティの対応については、システム開発部門や運用部門だけでなく、システムの利用者となる国民や自治体等多くのステークホルダを事前に巻きこみ、過去のインシデント事例等に基づいて事故発生防止に向けた議論や検討を重ねるとともに、被害発生時のダメージを極小化するための対応準備を事前に講じることが重要となる。

人に起因するセキュリティ脅威への対策の考え方を追記

［主な修正内容］

CISAの「セキュアバイデザイン、セキュアバイデフォルト原則」の内容を踏まえて更新

RECOMMENDATIONS FOR CUSTOMERS

The authoring organizations recommend organizations hold their supplying software manufacturers accountable for the security outcomes of their products. As part of this, the authoring organizations recommend that executives prioritize the importance of purchasing secure by design and secure by default products. This can manifest through establishing policies requiring that IT departments assess the security of software before it is purchased, as well as empowering IT departments to push back if necessary. IT departments should be empowered to develop purchasing criteria that emphasize the importance of secure by design and secure by default practices (both those outlined in this document and others developed by the organization). Furthermore, IT departments should be supported by executive management when enforcing these criteria in purchasing decisions. Organizational decisions to accept the risks associated with specific technology products should be formally documented, approved by a senior business executive, and regularly presented to the board of directors.

Key enterprise IT services that support the organization's security posture, such as the enterprise network, enterprise identity and access management, and security operations and response capabilities, should be seen as critical business functions that are funded to align with their importance to the organization's mission success. Organizations should develop a plan to upgrade these capabilities to leverage manufacturers that embrace secure by design and secure by default practices.

Where possible, organizations should strive to forge strategic relationships with their key IT suppliers. Such relationships include trust at multiple levels of the organization and provide vehicles to resolve issues and identify shared priorities. Security should be a critical element of such relationships and organizations should strive to reinforce the importance of secure by design and secure by default practices in both the formal (e.g., contracts or vendor agreements) and informal dimensions of the relationship. Organizations should expect transparency from their technology suppliers about their internal control posture as well as their roadmap towards adopting secure by design and secure by default practices.

品表（SBOM）の採用、④脆弱性の報告を奨励する開示プログラムの導入、⑤侵害をシステム全体に広げないための多層防御の導入など。

- セキュアバイデフォルト手法の導入：①デフォルトパスワードを排除する、②多要素認証を導入する、③高品質の監査ログの追加料金なしでの提供、④シングルサインオン（SSO）を実装する、⑤古いシステムとの互換性よりもセキュリティを優先、⑥「セキュリティ強化ガイド」の簡素化など。
- ①顧客のセキュリティの結果の責任を持つ、②徹底した透明性と説明責任を負う、③トップ主導での実施、という3つの基本原則を遵守する。

（3）ユーザ組織（顧客）への提言

- セキュリティ結果の責任をソフトウェア作成業者に問うよう推奨する。
- セキュリティバイデザインやセキュリティバイデフォルトの製品の購入を優先する。
- ソフトウェア作成業者と戦略的な連携関係を構築。ソフトウェア作成業者への要望を調整し、セキュリティを優先させる。
- クラウド利用の場合、責任分担を明確し透明性の高い企業を優先する。

今回のスコープでは
ソフトウェアを利用するユーザ組織の立場で留意点を追記
（調達、サプライチェーンセキュリティ関連）

［主な修正内容］

CISAの「セキュアバイデザイン、セキュアバイデフォルト原則」の内容を踏まえて更新

品表（SBOM）の採用、④脆弱性の報告を奨励する開示プログラムの導入、⑤侵害をシステム全体に広げないための多層防御の導入など。
- セキュアバイデフォルト手法の導入：①デフォルトパスワードを排除する、②多要素認証を導入する、③高品質の監査ログの追加料金なしでの提供、④シングルサインオン（SSO）を実装する、⑤古いシステムとの互換性よりもセキュリティを優先、⑥「セキュリティ強化ガイド」の簡素化など。
- ①顧客のセキュリティの結果の責任を持つ、②徹底した透明性と説明責任を負う、③トップ主導での実施、という3つの基本原則を遵守する。

（3）ユーザ組織（顧客）への提言
- セキュリティ結果の責任をソフトウェア作成業者に問うよう推奨する。
- セキュリティバイデザインやセキュリティバイデフォルトの製品の購入を優先する。
- ソフトウェア作成業者と戦略的な連携関係を構築。ソフトウェア作成業者への要望を調整し、セキュリティを優先させる。
- クラウド利用の場合、責任分担を明確し透明性の高い企業を優先する。

今回のスコープでは
ソフトウェアを利用するユーザ組織の立場で留意点を追記（調達、サプライチェーンセキュリティ関連）

修正内容(ｲﾒｰｼﾞ)

3)セキュア調達

ア 要求事項
- セキュリティ要件に基づいて、システム調達におけるセキュリティ仕様が策定され、委託先との責任範囲が明確になっていること
- クラウドサービスを利用する際はサービス形態（SaaS、IaaS、PaaS 等）を踏まえて自組織の責任範囲を特定し、責任共有モデルに基づく義務を果たす能力と内部統制について透明性の高いサービスを選定すること
- システムのセキュリティ仕様を実装できる能力を有し、求めるセキュリティ管理基準を満たし、セキュリティリテラシーおよび意識が高い、安全な委託先が選定されていること
- システムで利用する機器、ミドルウェア、ライブラリ等について、セキュリティ・バイ・デザインやセキュリティ・バイ・デフォルトを取り入れ、不正侵入の経路となるバックドア等が含まれていない、サポートを受けられる安全なプロダクトを選定すること

イ 実施内容
セキュリティ要件に基づき、調達仕様におけるセキュリティ仕様策定
セキュリティ仕様に関する、委託先との責任範囲の明確化
委託先に求めるセキュリティ管理基準の策定
セキュリティ仕様を満たす能力を有した安全な委託先の選定
不正侵入の経路となるバックドア等が含まれていない、サポートを受けられる安全なプロダクトの選定

ウ 重要なセキュリティ対策の考え方
セキュリティ仕様を満たす能力を有した委託先の選定、管理
- 委託先の能力不足、管理不足が原因によるセキュリティインシデントが多発しているため、セキュリティリテラシーおよび意識が高い十分な安全な委託先を選定し、適切な管理を行うことが肝要である。
- システムのセキュリティ要件に基づくセキュリティ仕様を策定した上で、当該仕様を実装可能な能力を有した委託先を選定する。
- システム基盤にクラウドサービスを使用する場合は、ISMAP の運用フローに従ってクラウドサービスを選定する。
- 委託先のセキュリティ管理の不備によるインシデント等を防止するため、委託先に求めるセキュリティ管理基準を策定し、委託先を管理、監督する。

バックドア等が含まれていない安全なプロダクトの選定
- サプライチェーンの多様化、グローバル化に伴い、調達したソフトウェアや機器が原因による、セキュリティインシデントが多発している。
- システムで利用するサードパーティのライブラリやミドルウェア、機器については、セキュリティ・バイ・デザインやセキュリティ・バイ・デフォルトを取り入れている事業者から提供されており、不正侵入の経路となるバックドア等が含まれていない安全なプロダクトを選定する。
- システムの稼働期間中、脆弱性が検出された場合にセキュリティパッチ提供等のサポートが受けられる、プロダクトを選定する。

改定

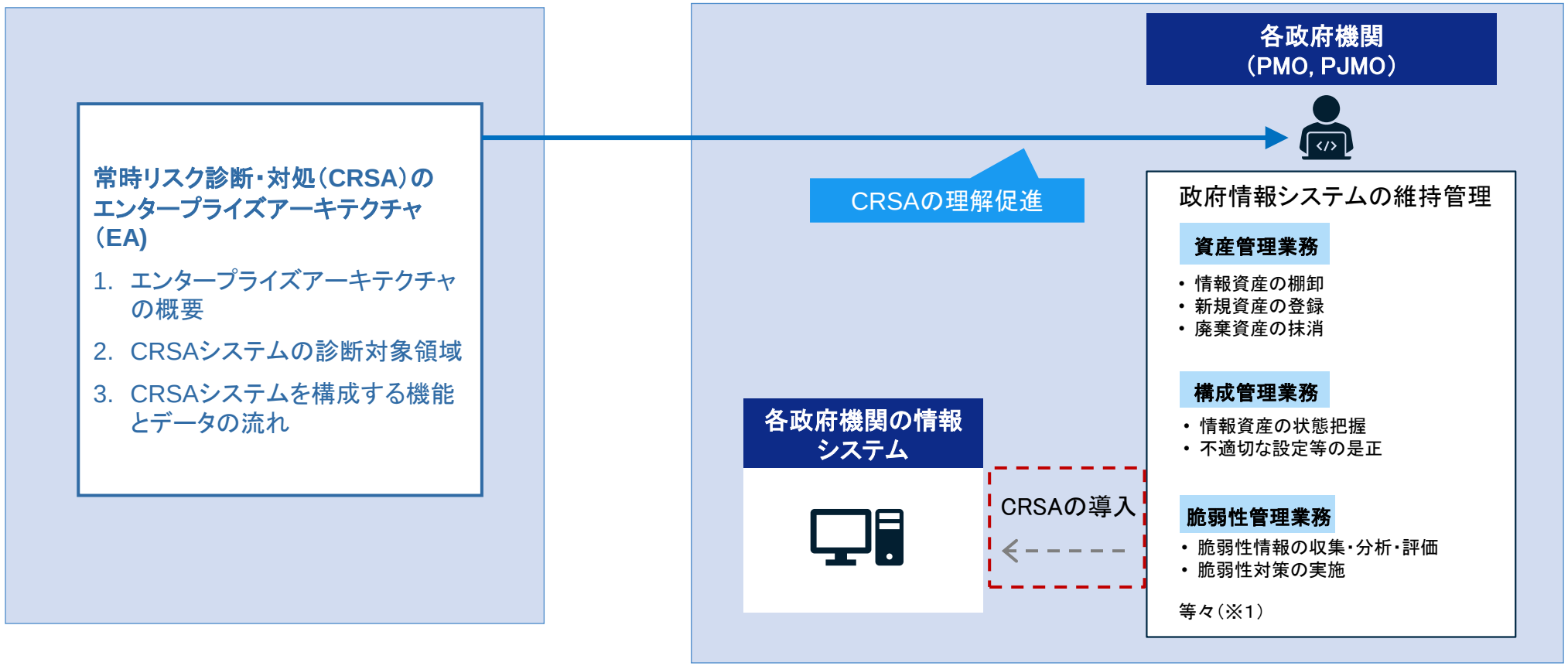
DS-211
常時リスク診断・対処（CRSA）の
エンタープライズアーキテクチャ（EA）

デジタル庁

本ガイドラインの概要

常時リスク診断・対処（CRSA）の理解促進を進め、各政府機関の情報システムへのCRSA導入を円滑にすることを目的として、CRSAのエンタープライズアーキテクチャ（EA)について説明する。

本ガイドラインが提供するもの



（※１）対象とする個別の管理業務については本プロジェクト内において、機器等の管理からアイデンティティ情報管理、システムとネットワークの状態管理、データ保護管理へ段階的に拡張していく予定です。

本ガイドラインの修正方針

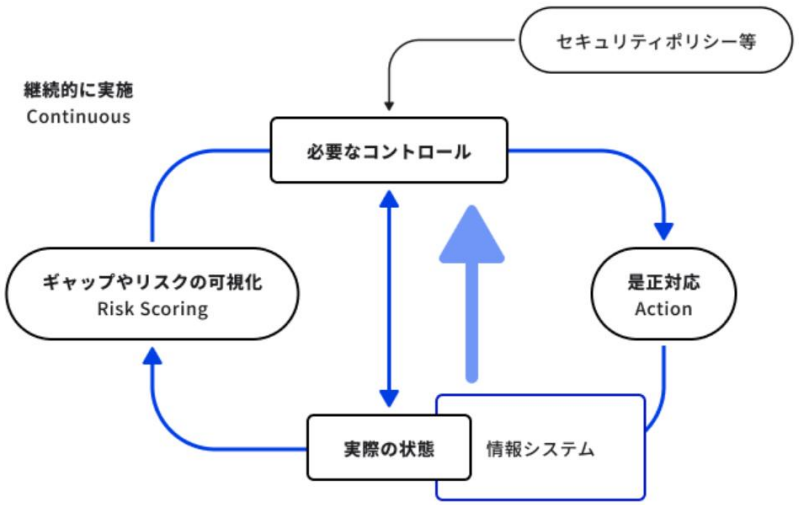
本版では、以下の分類における修正を行いました。

#	分類	修正方針	主な修正箇所
1	関連ドキュメントの更改に伴う改定	①「サイバーセキュリティに関するデジタル庁の取組」の記載内容に合わせて修正	①CRSAの概要および目的と効果について第1章において明示
2	初版に対して寄せられた質問や意見への対応	②アーキテクチャに関する記述の見直し ③収集情報についての説明追加	②エンタープライズアーキテクチャ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 ③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第2章において言及
3	CRSAシステムの実装に向けた検討結果の反映	④診断対象領域の明示	④診断対象領域と診断対象について第2章において明示

[修正内容①CRSAの概要および目的と効果の明示]

「サイバーセキュリティに関するデジタル庁の取組」（デジタル庁ホームページ）における
「常時リスク診断・対処（CRSA）の詳細」の記載に合わせて、CRSAの概要および目的と効果を明示。

CRSAの概念図



デジタル庁　ホーム　一般の方　行政・事業者の方　報道関係者の方　検索　Global Site　メニュー

CRSAシステム導入の目的と効果

1. 政府機関統一基準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、是正対応を実施できます。

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ります。

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ます。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ります。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ります。

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ります。

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

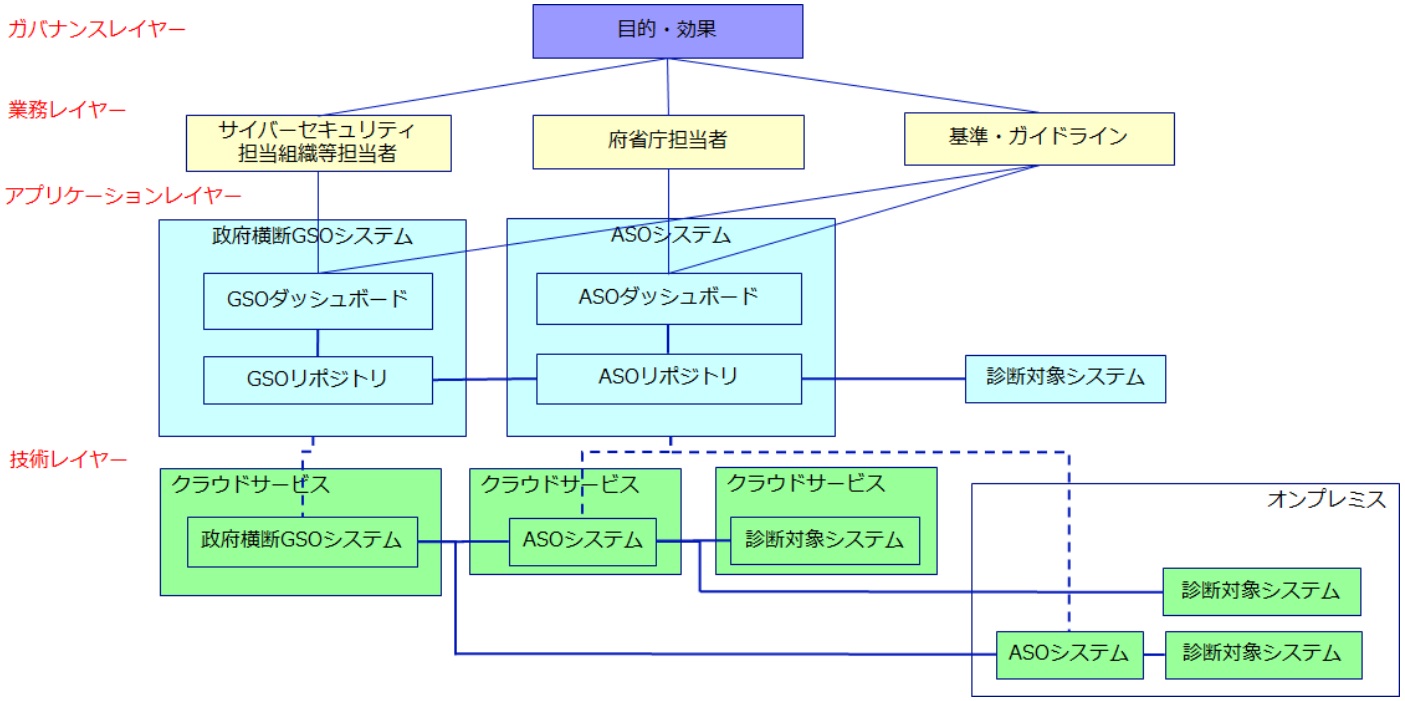
ゼロトラストアーキテクチャの具体的な実装・運用においては、ネットワーク上の各デバイスでの脆弱性対応状況等を把握することにより、システム全体の健全性を把握し、維持していく必要があります。CRSAシステムにおける診断結果は、ゼロトラストアーキテクチャにおけるポリシーエンジンのインプット情報としても活用していきます。

- 参考資料：常時リスク診断・対処（CRSA）（PDF／711KB）

「サイバーセキュリティに関するデジタル庁の取組」の抜粋
https://www.digital.go.jp/policies/security/crsa/

[修正内容②アーキテクチャに関する記述の見直し]

本文書が常時リスク診断・対処（CRSA）のエンタープライズアーキテクチャ（EA）について解説していることをを明示して、アーキテクチャ全体図および関連する本文の記載内容を修正。

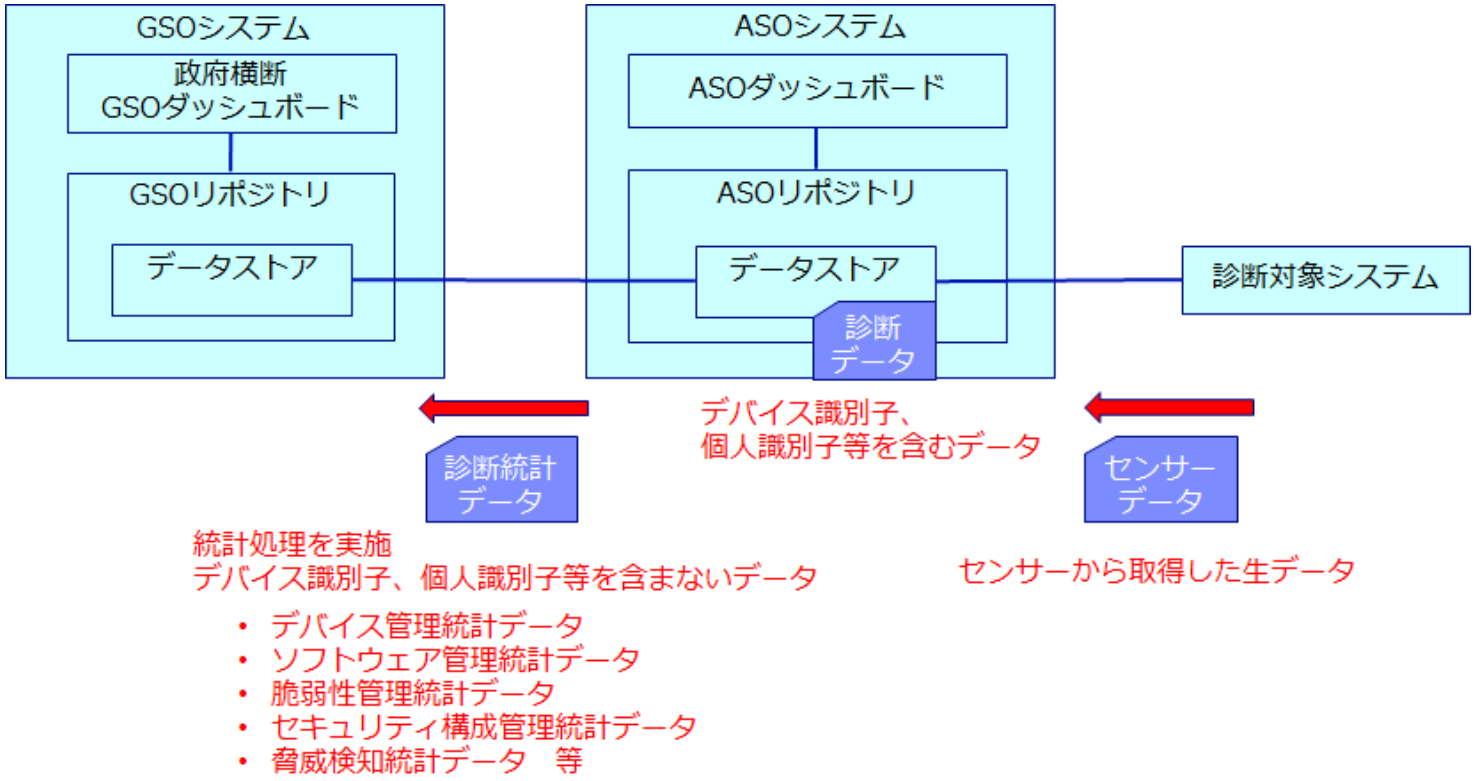


CRSAのエンタープライズアーキテクチャ（EA)の概要

エンタープライズアーキテクチャ（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。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。

[修正内容③収集情報についての説明追加]

CRSAシステムの機能とデータの流れについて説明し、CRSAシステムにおいて各政府機関の情報システムから収集する情報が統計情報であることを明示。統計情報とは、デバイス識別情報や個人識別情報を含まないよう統計処理を実施したものである。



アプリケーションレイヤーでのデータの流れ

[修正内容③収集情報についての説明追加]

診断統計データを用いて、必要なコントロールと実際の状態のギャップを可視化する。

診断対象のコントロール（政府統一基準）

- 6.1.1 (1) (e) 情報システムセキュリティ責任者は、**端末において利用するソフトウェアに関連する公開された脆弱性について対策を実施する**こと。

ギャップ

情報システムの実際の状態（例）

- 公開された脆弱性について対策が実施されていない

システム的に収集したデータでギャップやリスクを可視化

CRSAシステム

脆弱性管理統計データ（実際の状態を示すデータ）

デバイス上で検出されたソフトウェア脆弱性について
- 脆弱性識別子（CVE）
- 検出されたデバイス台数（DeviceCount）

参照

照合するデータ（理想的な状態を示すデータ）

検出されたソフトウェア脆弱性の属性情報
- 脆弱性識別子（CVE）
- CVSS値（CVSS）
- 脆弱性公開日（PublishedDate）
- 悪用事実の有無（FVA）
- システムの重要度（HVF）

可視化されるギャップ

- 脆弱性が検出されたデバイス台数 ＞ 0（未対応脆弱性が残っていることを示すデータ）
- 脆弱性検出日時 – 脆弱性公開日 ＞ 30日（脆弱性が長期間未対応であることを示すデータ）

可視化されるリスク

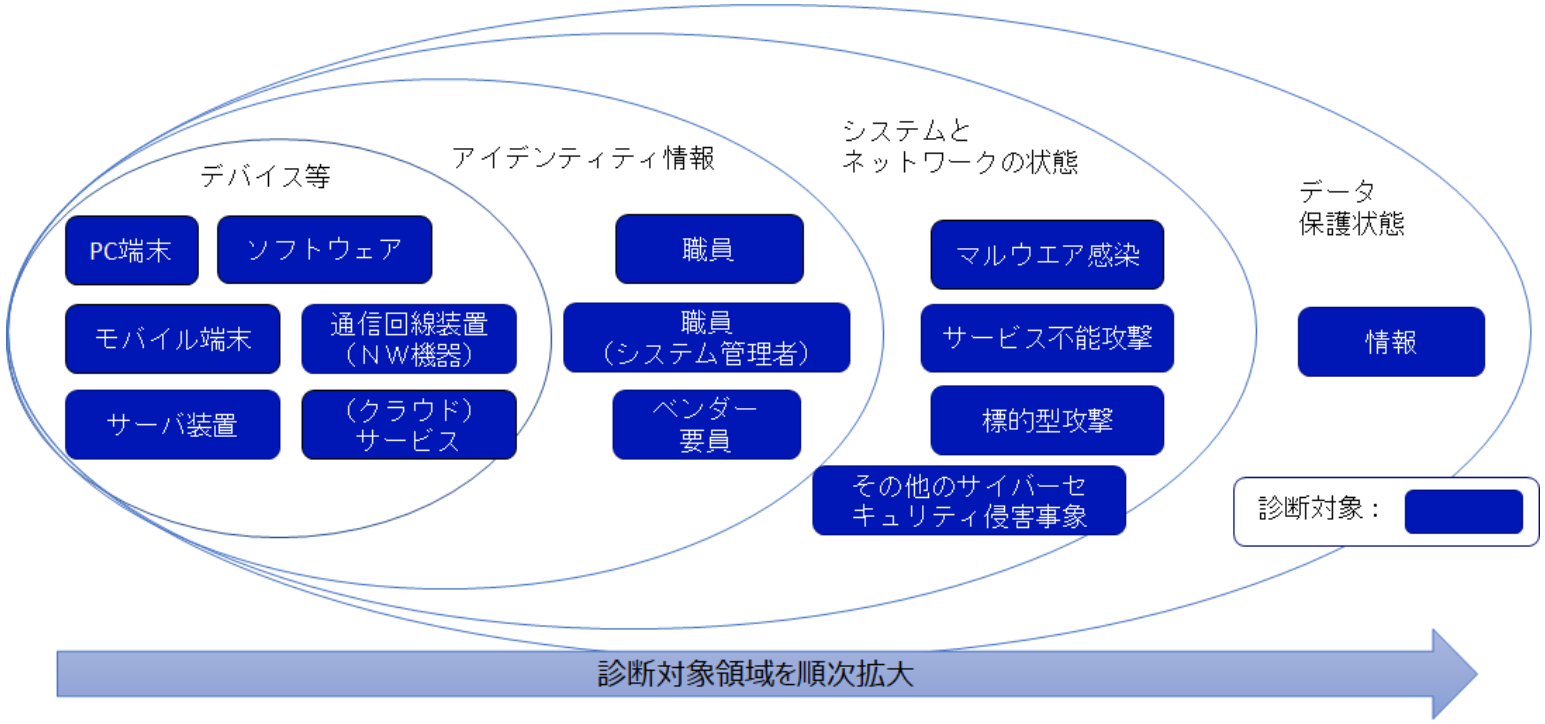
- 未対応脆弱性が残存していることによるリスク（VUL）
  リスクスコア計算式：

$$0.01 \times (\mathrm{CVSS})^3 \times \left(1 + \frac{\log(Days)}{\log(DaysToDouble)}\right) \times (\mathrm{FVA} * \mathrm{HVF}) \times DeviceCount$$

※検出された全ての脆弱性について上記を算出して積算する
Days：PublishedDateからの経過日数
DaysToDouble：Age Metricが2になるまでの日数

[修正内容④診断対象領域の明示]

CRSAが対象とする診断対象領域と診断対象について明示。診断対象領域は順次拡大を予定している。



診断対象領域と診断対象

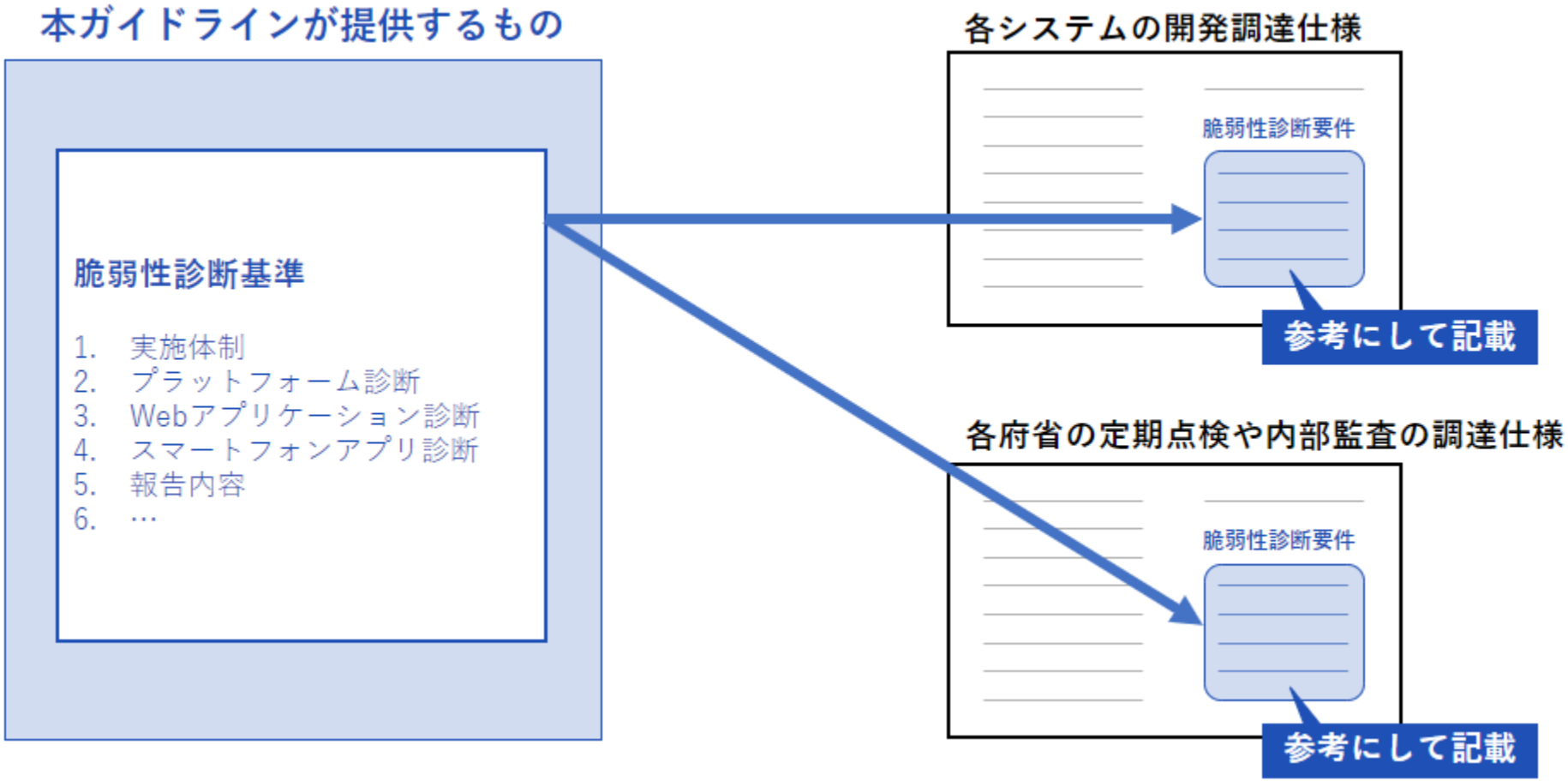
改定

DS-221
政府情報システムにおける脆弱性診断導入ガイドライン

デジタル庁

本ガイドラインの概要

各政府機関の情報システムにおいて、適切な脆弱性診断が実施されることを目的として、
診断の実施基準及びガイダンスを提供。



本ガイドラインの修正方針

本版では、主に以下2分類における記載の変更を行いました。

#	分類	修正方針	主な修正箇所
1	外部基準の変更に伴う改定	①　統一基準群（令和5年度版）に伴う改定 ②　CVSSのバージョン指定を廃止 ③　OWASP MASVSの改定に伴う修正	後述スライドにて説明
2	初版に対して寄せられた質問や意見への対応	各脆弱性を診断する際に留意すべき点を記載（例：WebSocketに関する脆弱性は、WebSocketプロトコルを利用している場合のみ診断対象とする等）	付録A（各種診断で検出対象とする脆弱性種別）等

[修正内容①] 統一基準群（令和5年度版）に伴う改定

統一基準群を参照する箇所の記載を全面的に変更しました。

本ガイドライン（改訂版）

1.1 目的とスコープ

本書で述べる基準は令和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」における「脆弱性検査を含む情報セキュリティの観点での試験を実施」（基本対策事項 5.2.2(1)-1 f））やウェブアプリケーションを運用段階へ移行する前の「脆弱性診断の実施」（基本対策事項 6.6.1(3)-2）、ソフトウェアに関する脆弱性対策を目的とした「脆弱性診断を実施」（基本対策事項 7.2.1(1)-1）における実施基準としての活用を想定する。また、「自己点検の実施」（遵守事項 2.3.1(2)(a)）を背景に点検の手段として脆弱性診断を行う際や、情報セキュリティ監査における「実際の運用が情報セキュリティ関連規定に準拠していること」（遵守事項 2.3.2(2)-2 c)）の確認手段として脆弱性診断を取り入れる際の実施基準としての活用も想定に含む。

3 政府情報システムにおける脆弱性診断の実施基準

・構築時診断
各システムの情報セキュリティ責任者やPJMO等が、統一基準群に従い自身のWebアプリを運用段階へ移行する前に脆弱性診断を実施する場合や、ソフトウェアに関する脆弱性対策の一環として自身の管理するシステムにおける脆弱性診断を実施する場合を想定する。
・定期診断
統一基準群の求める情報セキュリティ対策における自己点検や情報セキュリティ監査の一環として自組織のシステム全体を視野に実施することを想定する。

参照

統一基準群（令和５年度版）

2.3.1 自己点検

2.3.2 情報セキュリティ監査

5.2.2 情報システムの調達・構築

5.2.2(1)-1 f) 脆弱性診断を実施する際は、デジタル庁が公表している以下のガイドラインを参考にするとよい。

6.6.1 アプリケーション・コンテンツの作成・運用時の対策

6.6.1(3)-2 なお、脆弱性診断については、デジタル庁が公表している以下のガイドラインを参考にするとよい。

7.2.1 ソフトウェアに関する脆弱性対策

7.2.1(1)-1 また、脆弱性診断の種別や対象範囲、事業者が提供するサービス等の検討に当たっては「政府情報システムにおける脆弱性診断導入ガイドライン」を参考にするとよい。

［修正内容②］CVSSのバージョン指定を廃止

初版では脆弱性の深刻度評価にCVSS v3.1を用いることを指定しておりましたが、国内では未だv3.1に対応できないセキュリティ企業が存在する状況や、FIRSTより年内にCVSS v4.0が新たに公開される状況を受け、利用する基準を柔軟に選択できるようにするため、CVSSのバージョン指定を廃止しました。

また、CVSS v4.0ではv3.1までのTemporal MetricsやEnvironmental Metricsという指標が廃止されていることから、これら指標に関する記載も削除しました。

本ガイドライン（改訂版）

2.3 2) 2) 検出された脆弱性の深刻度評価

こうした脆弱性の評価において世界的に活用されているのはFIRST（Forum of Incident Response and Security Teams）が公開するCVSS（Common Vulnerability Scoring System）~~v3.1~~である。CVSS~~v3.1~~では、脆弱性そのものの技術的な深刻度を評価する基本評価基準（Base Metrics）に加え、攻撃コードの出現状況や~~等の現状のリスクを算定する現状評価基準（Temporal Metrics）、そして~~対象のシステム環境において想定される脅威~~に応じて最終的なリスクを算定する環境評価基準（Environmental Metrics）の3軸~~に基づき、0.0～10.0までのスコアで脆弱性の深刻度を評価する。また、このスコアに応じて、深刻度を以下の5段階で表現している。

［修正内容③］OWASP MASVSの改定に伴う修正 1/3

スマートフォンアプリ診断の基準に用いてきたOWASP MASVSがv2に改定され、従来のセキュリティレベルという概念は廃止、技術領域別の要件として再構成されました。当ガイドラインはMASVS-L1を実施基準としているため、基準の再定義が必要となります。

MASVS v1（従来）

MASVS-L1

標準セキュリティレベルであり、スマートフォンアプリにおけるセキュリティのベストプラクティスに準拠する。全てのスマートフォンアプリに適している。

MASVS-L2

多層防御に位置付けられ、標準的な要件を超える高度なセキュリティコントロールを導入する。モバイルバンキングアプリ等の機密性の高いデータを処理するアプリに適している。

MASVS-R

リバースエンジニアリングと改ざんへの耐性を有するレベルであり、アプリに対する様々な攻撃に対して耐性を有する。モバイルゲーム等のように知的財産の保護やアプリの改ざんを防止する必要のあるアプリに適している。

改定

MASVS v2（現在）

- MASVS-STORAGE
- MASVS-CRYPTO
- MASVS-AUTH
- MASVS-NETWORK
- MASVS-PLATFORM
- MASVS-CODE
- MASVS-RESILIENCE

[修正内容③] OWASP MASVSの改定に伴う修正 2/3

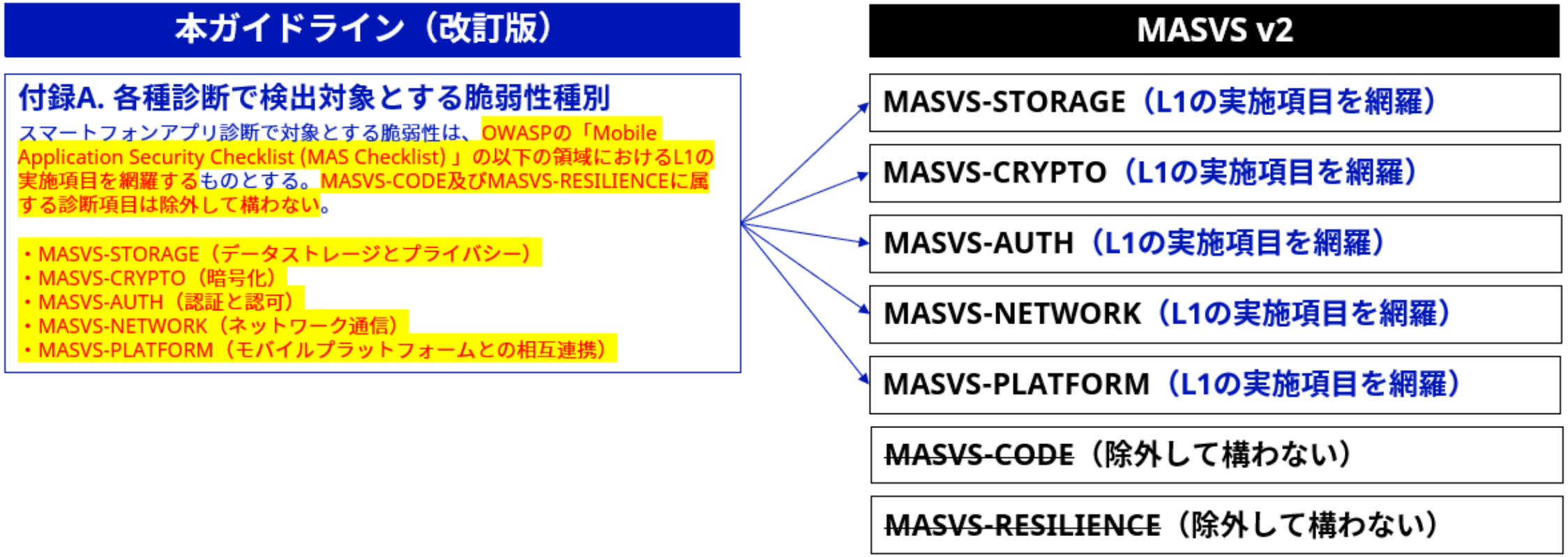
現時点では移行期間として、従来のセキュリティレベル（L1, L2, R）との対応関係が示されていることから、当ガイドラインでは引き続きセキュリティレベルの概念を取り入れた基準を定義します。

OWASP MASVS v2
における要件

OWASP MASVS v1の
セキュリティレベル
との対応関係

［修正内容③］OWASP MASVSの改定に伴う修正 3/3

具体的には、MASVS v2の各技術領域におけるL1の実施項目を診断対象と定めます。ただし、診断での検出が困難なMASVS-CODE（コード品質）と従来のMASVS-Rに相当するMASVS-RESILIENCE（リバースエンジニアリングと改竄に対する耐性）は除外します。



デジタル庁