

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。まずはデジタル庁を適用範囲とする。6月末に策定予定。なお、将来的には各府省庁への適用する方向で改訂することを視野にしている。

統一基準群

ゼロトラスト・アーキテクチャ適用方針

informative

概要

政府機関ではクラウドサービスの利用や業務環境の変化が進んでいる。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、サイバーセキュリティ要件を満たすには、パラダイムシフトが求められる。本文書はゼロトラスト・アーキテクチャというパラダイムシフトの適用方針に関する原則を説明する。

常時リスク診断・対処(CRSA)システムアーキテクチャ

informative

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。本文書は、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している。

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

informative

概要

情報システムに対して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。本文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。併せてセキュリティバイデザインの実用性確保するための関係者の役割を定義する。

政府情報システムにおける脆弱性診断ガイドライン

informative

概要

政府機関では、これまでも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ているが、導入方法に明確な基準や指針があるとは言えない。本取り組みでは、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ガイダンスを提供する。

(参考) セキュリティ関連技術ガイドライン群の構造整理

