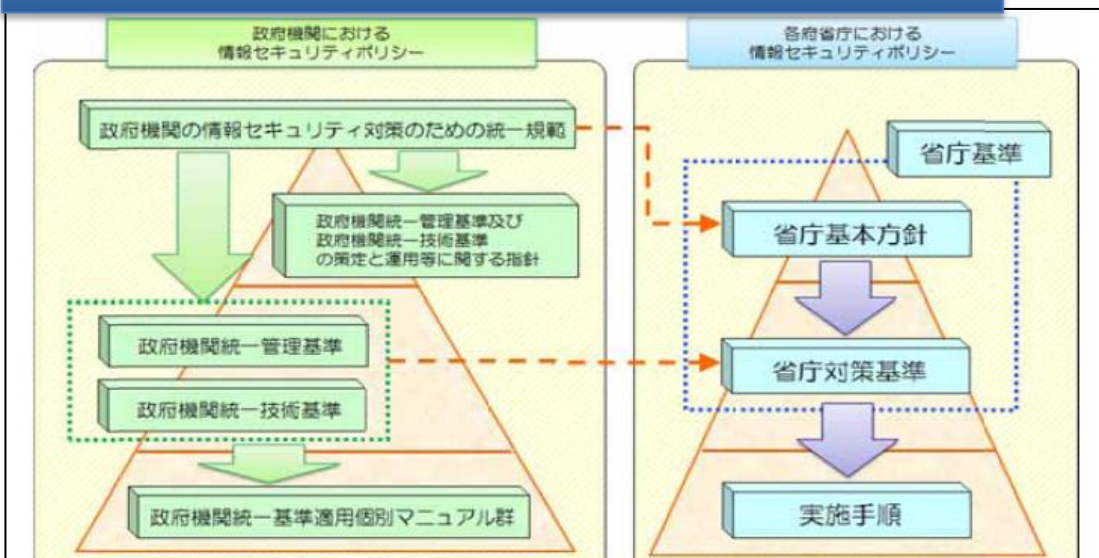


政府統一基準群の構成

文書名	概要
政府機関の情報セキュリティ対策のための 統一規範	最高情報セキュリティ責任者による情報セキュリティ対策の取組の理解及び把握に資する文書として、1.目的及び対象、2.政府機関の情報セキュリティ対策のための基本指針、3.政府機関の情報セキュリティ対策のための基本対策を示したもの。
政府機関の情報セキュリティ対策における政府機関統一管理基準及び政府機関統一技術基準の策定と 運用等 に関する 指針	下記の統一管理基準と統一技術基準の 運用の枠組み を示したもの。以下3つの骨格からなる。 1. 政府機関統一基準及び技術基準の策定と 各府省庁における情報セキュリティポリシーの見直し 2. 対策実施手順書の整備の支援 （各府省庁に対する草の根支援） 3. 対策実施状況の確認と評価に基づく P D C Aサイクルの確立
政府機関の情報セキュリティ対策のための 統一管理基準	政府機関統一規範に基づき、政府機関の情報セキュリティ対策の横断的な取組の一環として、情報セキュリティ対策の内容の整合化・共通化を促進するため、 それぞれの府省庁が最低限行うべき情報セキュリティ対策を定めた 政府の 統一な基準 。
政府機関の情報セキュリティ対策のための 統一技術基準	政府機関統一管理基準に記載された 情報セキュリティ対策を実施する上での具体的な技術的基準 。

各府省庁における情報セキュリティポリシーとの関係



「政府機関の情報セキュリティ対策における政府機関統一管理基準及び政府機関統一技術基準の策定と運用等に関する指針」より抜粋

「…府省庁においては、政府機関統一規範並びに政府機関統一管理基準及び政府機関統一技術基準で定められた以上の情報セキュリティの確保を目的として、**省庁基準及び実施手順**を策定するとともに、その後、**必要な見直し**を行うものとする。したがって、**府省庁において、政府機関統一管理基準及び政府機関統一技術基準で定められている内容を合理的な理由なく省庁対策基準に反映させない**ということはあってはならない。…」

（「政府機関の情報セキュリティ対策における政府機関統一管理基準及び政府機関統一技術基準の策定と運用等に関する指針」情報セキュリティ政策会議決定）

政府統一基準群について②

運用等指針における要求事項の概要

1. 計画

- (1) 組織・体制の確立
- (2) 省庁基本方針の策定
情報セキュリティ対策の目的、対象範囲等
- (3) リスク評価及びリスク対応
 - ① 情報資産の調査
 - ② 重要性の分類
 - ③ 脅威・脆弱性の調査
 - ④ 脅威の発生頻度、脆弱性の程度及び発生時の被害の大きさ
- (4) 省庁対策基準の策定
政府統一管理基準、政府統一技術基準に準拠
- (5) 省庁基準の決定
専門家、関係部局の意見を踏まえて、府省庁として意思決定

2. 実施

- (1) 実施手順の作成
- (2) 省庁基準及び実施手順の周知
- (3) 省庁基準及び実施手順の運用

3. 評価

情報セキュリティの状態を評価（内部点検、外部評価等）

4. 改善

省庁基準の改正、実施手順の改正等

ISMS適合性評価制度の認証基準である「ISO/IEC 27001:2005」で要求されている情報セキュリティマネジメントシステムに相当

統一管理基準における要求事項の概要

第1.1部 総則

本基準の位置づけと使い方、情報の格付け、用語定義など

第1.2部 組織と体制の整備

各種責任者の設置と役割の定義、教育、事故時の対応、自己点検や監査、外部委託、業務継続計画の策定などに係る遵守事項

第1.3部 情報についての対策

作成と入手、利用、保存、移送、提供、消去といった情報のライフサイクル全般に係る遵守事項

第1.4部 情報処理についての対策

情報システムの利用にあたっての認証とアクセス制御のあり方、府省庁外での情報処理などに係る遵守事項

第1.5部 情報システムについての基本的な対策

情報システムの計画時・構築及び運用時・移行及び廃棄・見直しの際に遵守すべき事項、文書及び台帳の整備、機器等の購入、ソフトウェア開発、主体認証・アクセス制御・権限管理・証跡管理・保証等の標準手順、暗号と電子署名の標準手順、ウイルス対策などに係る遵守事項

ISMS適合性評価制度の認証基準である「ISO/IEC 27001:2005」付属書Aで要求されている管理策に相当

統一技術基準における要求事項の概要

第2.1部 総則

本基準の位置づけと使い方、情報の格付け、用語定義など

第2.2部 情報セキュリティ要件の明確化に基づく対策

・主体認証機能、アクセス制御機能、権限管理機能、証跡管理機能、保証のための機能、暗号と電子署名に係る遵守事項
・情報システム構築時と運用時におけるセキュリティホール対策、不正プログラム対策、サービス不能攻撃対策、踏み台対策に係る遵守事項

第2.3部 情報システムの構成要素についての対策

コンピュータ機器を設置する施設・環境、サーバ・端末の設置・運用、電子メール・Web・DNSの導入・運用、府省庁内LAN・外部アクセス等に係る遵守事項

第2.4部 個別事項についての対策

IPv6技術の導入における対策

【統一基準群との差】

- ・統一基準群にのみ記載があるもの
→情報セキュリティ関係規定への違反に対する例外措置等
- ・付属書Aにのみ記載があるもの
→要員審査や雇用条件に関する対策等
※政府機関においては国家公務員法等により別途規定されているため。