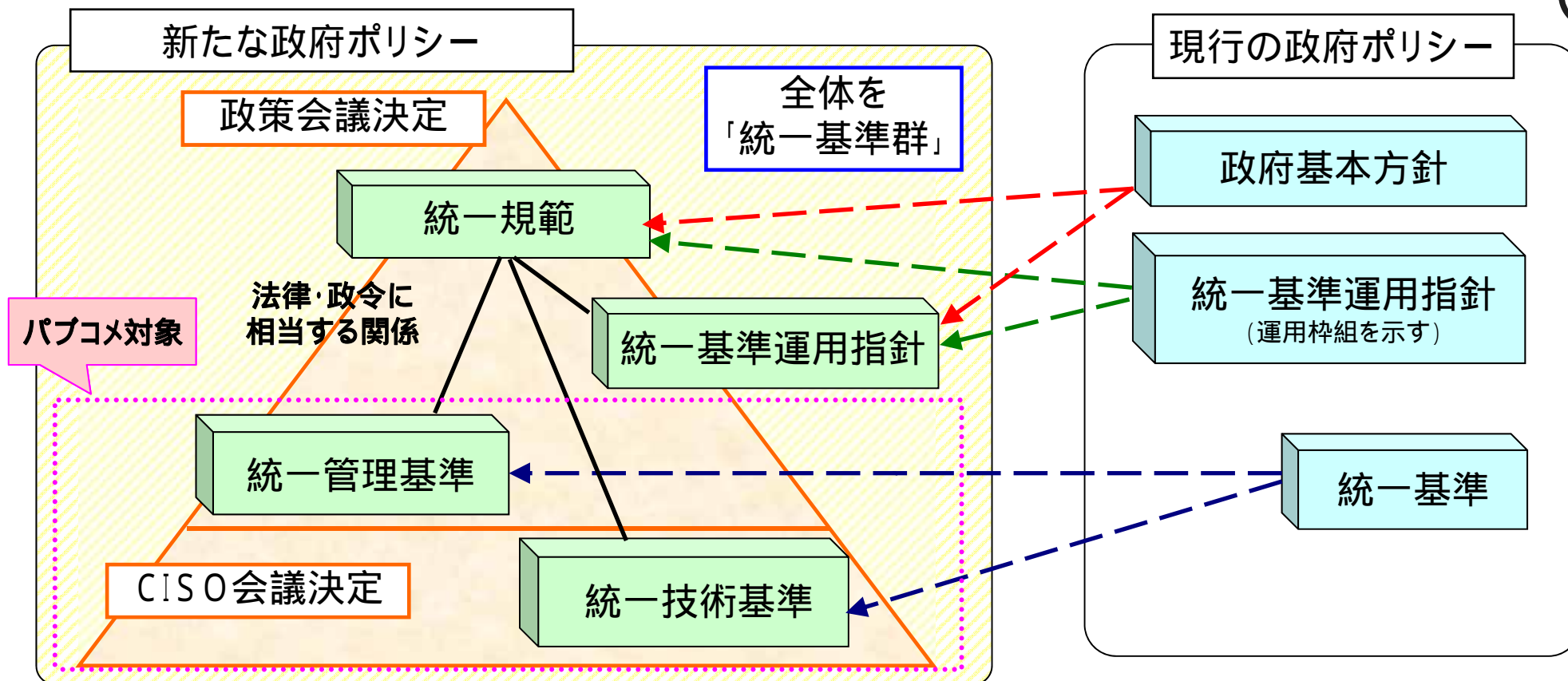


政府機関の情報セキュリティ対策のための統一基準群 の概要について

2010年12月
内閣官房情報セキュリティセンター

1. 新たな政府統一基準群の体制について(基本方針の廃止と統一規範の策定)

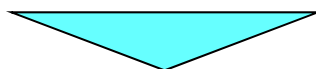


	文書	現行	新体制	決定
1	情報セキュリティ基本方針	政府基本方針	統一規範	政策会議
2	情報セキュリティマネジメントの指針	統一基準運用指針	統一基準運用指針	政策会議
3	情報セキュリティポリシー (基本編)	統一基準	統一管理基準	政策会議
4	情報セキュリティポリシー (技術編)	統一基準	統一技術基準	CISO等連絡会議

2. 新たな政府統一基準群に向けた改訂(案)の背景とポイント

背景

- ・ウェブ改ざん型攻撃や標的型メール攻撃など、外部からの不正アクセスを招く脅威が増加しており、そのような脅威への迅速な対応が必要。
- ・政府内において政府共通プラットフォームの検討が進められるなど、いわゆるクラウド技術を利用する機会が拡大しており、そのセキュリティ面での技術的対応が必要。



統一基準(第4版)(平成21年度修正)では、統一基準(第4版)及びそれを踏まえた省庁対策基準の定着に重点を置くこととしたことから、必要最小限の修正を行ったところ。

一方、**新たな政府統一基準群では、環境の変化へ適切に対応することを想定し、改訂を実施。**

統一管理基準及び統一技術基準への改訂(案)のポイント

1. 統一管理基準と統一技術基準への再編
2. クラウド技術への対応
3. ウェブ等の外部からの不正アクセスに係る対応
4. 教育・人材育成の充実

()その他、解説書の記述の明確化等も実施。

3. 新たな政府統一基準群に向けた改訂(案)の概要



1. 統一管理基準と統一技術基準への再編

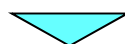
経緯

- ・最近の情報セキュリティ上のリスクが多様化・高度化・複雑化しており、従来の取組では情報セキュリティの確保が困難な状況が発生。
- ・各府省庁において、情報セキュリティ上のリスクへの対応を迅速化することは喫緊の課題。

方針案

現状 ■ 現行の統一基準は、基本的基準(基本編)と技術的基準(技術編)の双方を記載。

- ・現行の統一基準は、政府機関内の一般職員と情報システムを扱う技術的専門職員の双方を対象としており、統一基準の浸透を図る上で課題があった。



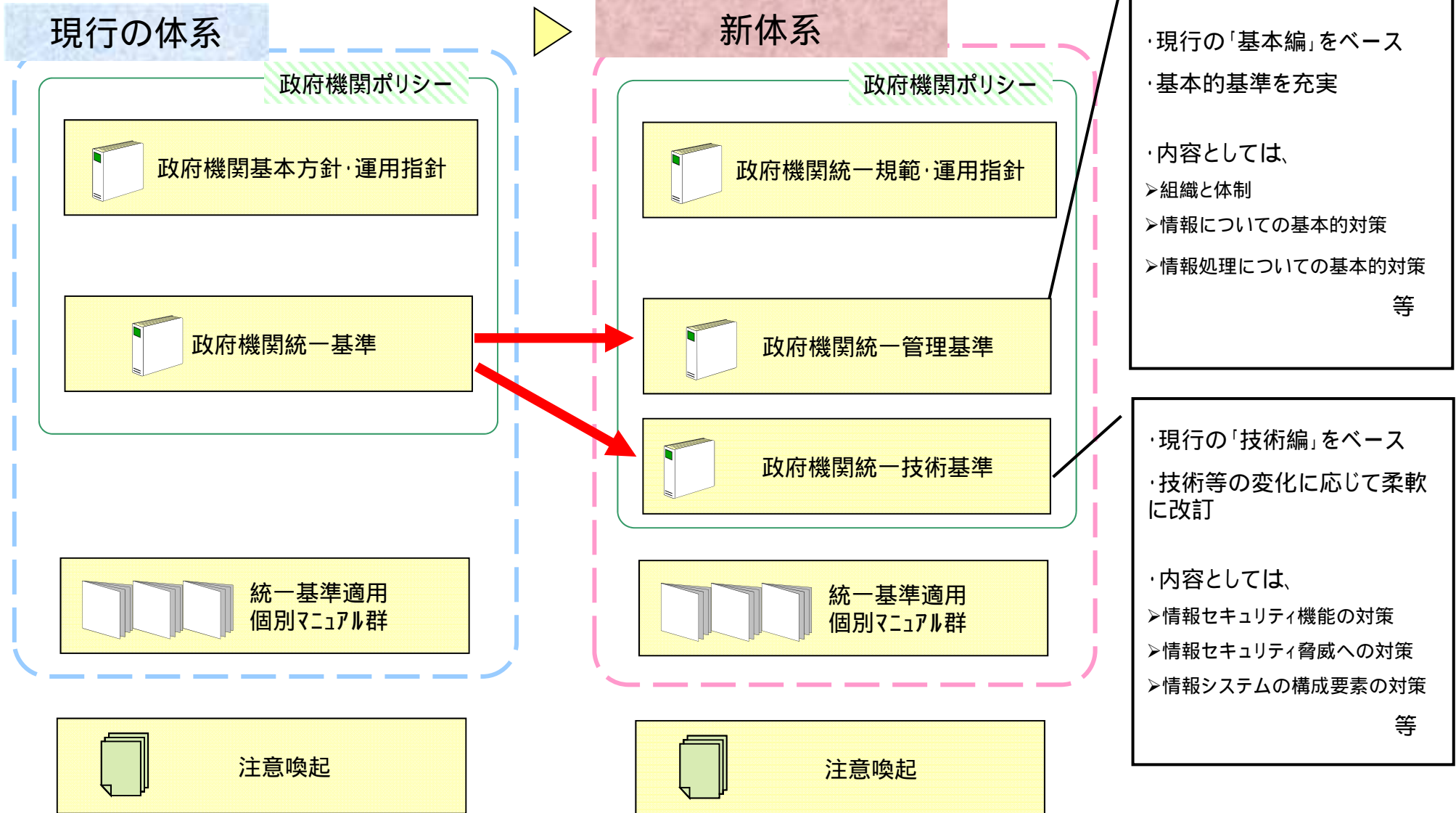
改定案 ■ 統一管理基準(基本的基準)と統一技術基準(技術的基準)を分離し、策定者を独立。

- ・統一技術基準については、技術等の変化に応じて柔軟に改訂を実施し、各府省庁においても、それぞれの対策基準を適切な者が策定。
- ・両者を分離することで、一般職員及び技術的専門職員双方の使い勝手をよくし、脅威への対応の迅速化を図る。

()「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(平成21年2月3日改定))において、統一管理基準と統一技術基準の分離を明記。

3. 新たな政府統一基準群に向けた改訂(案)の概要

1. 統一管理基準と統一技術基準への再編



3. 新たな政府統一基準群に向けた改訂(案)の概要



2. クラウド技術への対応

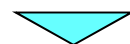
経緯

- ・政府内において、政府共通プラットフォームの検討が進められるなど、政府機関においていわゆるクラウド技術を利用する機会は今後拡大。
- ・そこで、各府省庁において具体的にクラウド技術(外部委託を含む)を活用するにあたってのセキュリティ上の配慮事項を示す必要がある。

方針案

現状 ■ 現行の統一基準は、クラウド技術を想定した基準となっていない。

- ・前回の内容改訂(第4版)より1年半以上経過しており、クラウドといった新たな技術やサービスを勘案したものとなっていない。



改定案 ■ 統一管理基準及び統一技術基準に、クラウド技術を活用するにあたってのセキュリティ上の配慮事項を追加。

- ・情報の保存場所に係る基準や外部委託における注意事項等、クラウド技術を活用するにあたっての配慮事項を新たに追加。

3. ウェブ等の外部からの不正アクセスに係る対応

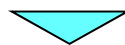
経緯

- ・昨今、ウェブ改ざん型攻撃や標的型メール攻撃など、外部からの不正アクセスを招く脅威が増加。
- ・ウェブサーバをはじめとする政府機関の情報システムにおいても、その対応が求められている。

方針案

現状 ■**現行の統一基準は、最近の新たな不正アクセスを勘案したものとなっていない。**

- ・前回の内容改訂(第4版)より1年半以上経過しており、昨今よく用いられている不正アクセスの手法を勘案したものとなっていない。



改定案 ■**統一管理基準及び統一技術基準に、新たな不正アクセス手法に対応するための基準等を追加。**

- ・ウェブやサービス不能攻撃対策に係る基準の改善を実施。
- ・また、ウェブの改ざんやメール送信者の偽装を判定する方法(電子証明書や送信ドメイン認証)に係る基準等を新たに追加。

3. 新たな政府統一基準群に向けた改訂(案)の概要



4. 教育・人材育成の充実

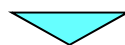
経緯

- ・各府省庁が能動的なPDCAサイクルを円滑に実施するためには、各府省庁の職員における情報セキュリティの知識向上が必要。
- ・一方で、定期的な人事異動のために職員の知識向上は容易ではなく、情報セキュリティに係る能力の強化が課題となっている。

方針案

現状 ■ 現行の統一基準では、職員に対して教育を受けさせる基準を記載。

- ・現行の統一基準では、職員に対して教育を受けさせる基準はあるが、教育の内容が画一的であるなど教育のあり方に改善の余地があった。



改定案 ■ 統一管理基準及び統一技術基準において、教育の種類を充実し、より実効性のあるものに改善。

- ・教育を役割者別に実施するよう改善し、そのための教材をNISCにて作成して政府機関内に配布。