政府機関・重要インフラの情報セキュリティ対策の強化に向けて
－第2回情報セキュリティ政策会議での決定事項－

平成17年9月22日

内閣官房情報セキュリティセンター（NISC）

1．情報セキュリティ政策会議において検討中の課題

政府機関
情報セキュリティ基本問題委員会
第1次提言
(平成16年11月16日)

重要インフラ
情報セキュリティ基本問題委員会
第2次提言
(平成17年4月22日)

早期に着手すべき政府統一的・横断的課題
＜当面の課題への対応＞
政策会議決定 (平成17年7月14日)

第1回
(7/14)

政府機関
- ◆ 総合的な監視・警戒態勢の構築　等
- ◆ **情報セキュリティ対策の統一的な基準を示し、ガイドライン群を作成**

企業・個人
- ◆ 「インターネット安全教室」等、国民のリテラシー向上等への取組み
- ◆ フィッシング、ボットネットなど新たに登場してきた脅威への対策　等

重要インフラ
- ◆「安全基準・ガイドライン」の指針を9月までに策定
- ◆重要インフラごとの「安全基準・ガイドライン」策定
- ◆自治体ISAC (仮称) の創設支援　等
- ◆ **「重要インフラのサイバーテロ対策に係る特別行動計画」の改定に向けての検討**

＜政策会議決定＞　＜自由討議＞　＜政策会議決定＞

第2回
(9/15)

政府機関統一基準
(2005年項目限定版)
- ・情報セキュリティ対策の強化に関する政府基本方針
- ・統一基準運用指針 (スキームの提示)
- ・政府機関の統一基準

基本計画の方向性
- ・「第1次情報セキュリティ基本計画 (仮称)」の骨子と方向性

重要インフラの情報セキュリティ対策に係る基本的考え方
- ・重要インフラの対象範囲等の見直し
- ・情報セキュリティ水準向上のための具体的対策
- ・官民の連絡・連携、情報共有体制の強化

セキュリティ文化専門委員会等での検討

項目の追加充実

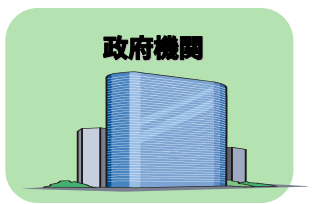
基本的考え方に基づいた具体的な行動計画の策定

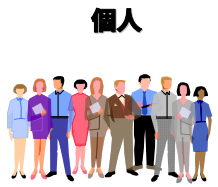
第3回
(12月)

「第1次情報セキュリティ基本計画(仮称)」
情報セキュリティ問題を俯瞰した中長期の戦略
(平成17年12月中 (予定))

政府機関統一基準
(2005年12月版(全体版初版))

重要インフラの情報セキュリティ対策に係る行動計画





2．「政府機関の情報セキュリティ対策のための統一基準（2005年項目限定版）」について

●各府省庁の情報セキュリティ対策の整合化・共通化を促進し、**政府機関全体としての情報セキュリティ水準の向上を図るべく、「政府機関の情報セキュリティ対策のための統一基準」とその運用枠組みを政策会議決定**（平成17年9月15日）。

●今後、各府省庁は本基準を踏まえて対策を実施し、**内閣官房情報セキュリティセンター（NISC）が対策実施状況を検査・評価。**

ポイント

1．政府機関統一基準の策定と省庁対策基準の見直し（水準の底上げ）
　各府省庁の情報セキュリティ対策の整合化・統一化と、その水準の斉一的な引き上げ

2．各府省庁の対策実施状況の検査と評価に基づくＰＤＣＡサイクルを確立
　第三者の視点で内閣官房情報セキュリティセンター（NISC）が検査・評価し、当該評価結果を基に情報セキュリティ政策会議が勧告→見直し

3．政府機関統一基準の対策項目の具体化（個別ガイドライン群の策定）
　各府省庁における具体的なレベルでの対策実施を支援するための個別ガイドライン群の策定
（例：webサーバ設置、モバイルPC管理等）

今回策定した文書

政府機関統一基準（2005年項目限定版）
「政府機関の情報セキュリティ対策のための統一基準」

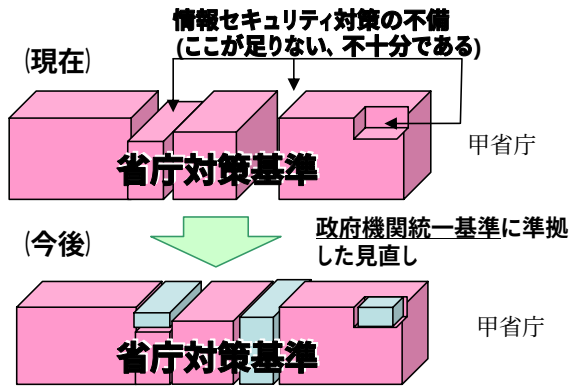
各府省庁の情報セキュリティ対策内容の整合化・共通化を促進するために、各府省庁が採るべき情報セキュリティ対策を定めたもので、緊急性の高いものを中心に取りまとめ

＜盛り込まれた内容の例＞
- ●情報の格付け及び取扱制限に関する基準を明示する手順の整備
- ●情報の持ち出し等の制限事項の強化
- ●一定の情報システムに対するアクセス制御・ログ管理機能の導入
- ●サービス不能攻撃（DoS攻撃）対策の実施
- ●省庁ネットワークに対する不用意な接続の禁止
- ●外部委託先が遵守すべき事項等を含めた契約書の取り交わし

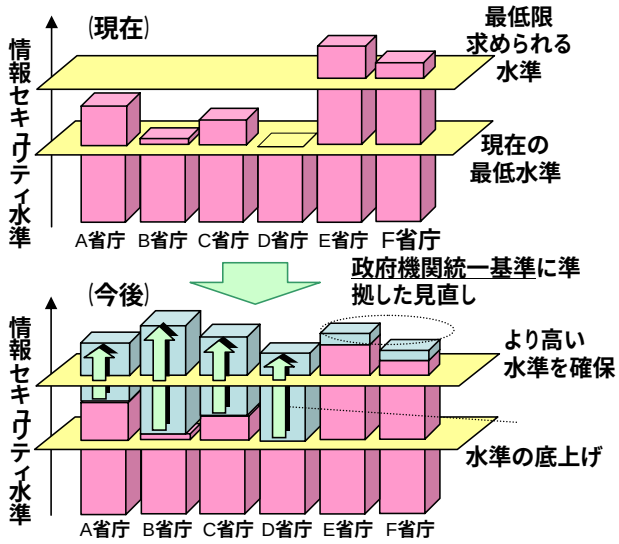
PDCAサイクルの確立
政府機関統一基準（2005年12月版(全体版初版)）の策定（年内目途）
→ 内閣官房情報セキュリティセンターによる検査・評価（本年度内目途）

対策の具体化
具体的対策基準として個別ガイドライン群を作成

① 政府機関統一基準による省庁対策基準の補完



② 各府省庁の情報セキュリティ水準の向上



3.「重要インフラの情報セキュリティ対策に係る基本的考え方」について

●情報セキュリティ基本問題委員会第2次提言を受け、**情報セキュリティ面からの新たな重要インフラ防護の基本理念として、「重要インフラの情報セキュリティ対策に係る基本的考え方」を政策会議決定**（平成17年9月15日）。

●「基本的考え方」に基づき、政策会議に設置した重要インフラ専門委員会の検討を経て、**本年12月を目処に「重要インフラの情報セキュリティ対策に係る行動計画（仮称）」を策定**する予定。

対象分野・脅威の見直し

➢重要インフラ分野として、情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービスに、**新たに、医療、水道、物流を加えた10分野**を設定
➢想定する脅威を、**「サイバー攻撃」に加えて、人為的ミス等の「非意図的要因」、「自然災害」へと拡大**

新たな体制の構築

1. 重要インフラ横断的機能の強化

➢内閣官房情報セキュリティセンターを中心に、**横断的な状況把握（相互依存性解析等）を実施**

2. 情報セキュリティ水準の向上

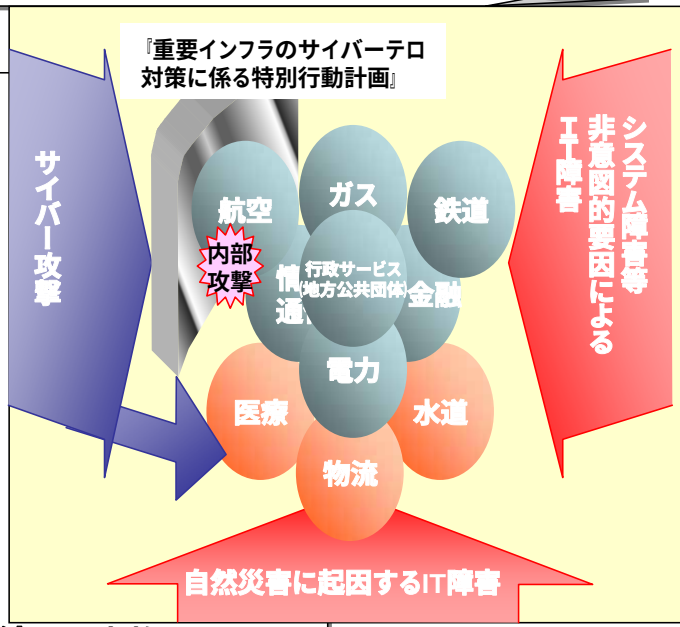
➢技術的基準及び運用基準についての**「安全基準・ガイドライン」の策定・見直し**等を実施

3. 情報共有・提供体制の強化

➢**「情報共有・分析センター」（仮称）等の各分野内情報共有機構の創設**
➢重要インフラ横断的な情報共有の推進（「重要インフラ連絡協議会」（仮称）の設立等）
➢情報提供体制の整理・強化、情報の充実・質の向上

4. 分野横断的演習の実施

➢想定脅威に対応した具体的脅威シナリオの類型を元に、毎年度、**重要インフラ分野横断的な演習**を実施



（5年経過）　（平成18年度）

重要インフラのサイバーテロ対策に係る特別行動計画 ・・・・・ 情報セキュリティ基本問題委員会 → 第2次提言 我が国の重要インフラにおける情報セキュリティ対策の強化に向けて → 重要インフラの情報セキュリティ対策に係る基本的考え方 → 重要インフラ専門委員会 → 重要インフラの情報セキュリティ対策に係る行動計画（仮称）

- 相互依存性解析の実施
- 「安全基準・ガイドライン」の策定・見直し
- 情報共有機構の創設
- 分野横断的演習の実施

平成12年12月　平成16年7月　平成17年4月　平成17年9月　平成17年12月