情報セキュリティ確保のための取組み

平成１２年１０月１６日
内閣安全保障・危機管理室
情報セキュリティ対策推進室

１．背　景

○インターネットの爆発的な普及、ＩＴ社会の急速な進展
－電子商取引・電子政府の進展　等

○サイバースペースにおける危険性の増大
－ネットワークを通じて世界中から２４時間攻撃される可能性、例えば我が国での中央省庁ホームページ改ざん事件　等

○米国においても情報セキュリティ対策を強化
・１９９８年５月　**大統領決定指令第６３号**
－情報セキュリティ確保のための官民の体制整備を指示
・２０００年１月　**情報システム防護のための国家計画**
－連邦政府機関における脆弱性の評価、侵入検知システムの整備、研究開発の推進等

２．我が国の取組み

（１）政府の体制整備

政府横断的な取組体制を整備

○**ＩＴ戦略本部**
－**情報セキュリティ部会**（民間有識者会合）
－**情報セキュリティ対策推進会議**（議長は内閣官房副長官、全省庁局長級）
（本年２月に高度情報通信社会推進本部の下に設置したものを改組）

○本年２月に内閣官房内閣安全保障・危機管理室に**情報セキュリティ対策推進室**を設置。

（２）これまでの取組み

○本年１月　ＩＴ社会の進展に見合った適切なセキュリティ水準を達成するため、**「ハッカー対策等の基盤整備に係る行動計画」**を策定。

○　　７月　全省庁のセキュリティ水準を向上させるため、**「情報セキュリティポリシーに関するガイドライン」**を整備。全省庁は年内を目途にそれぞれの情報セキュリティポリシーを策定。

○　　９月　「サイバーテロ対策ワーキンググループ」を設置し、いわゆるサイバーテロの被害を受けた場合に国民生活に大きな影響を及ぼす民間重要インフラの事業者も交え、年内を目途に**「サイバーテロ対策特別行動計画」**を策定中。

（３）今後の取組み

①　緊急対処能力の向上

ネットワークを通じてすべてのシステムが相互に接続されていることから、事案の拡散防止のため、政府を含めた早期対応能力の更なる向上を図る。

②　官民の連携の一層の強化

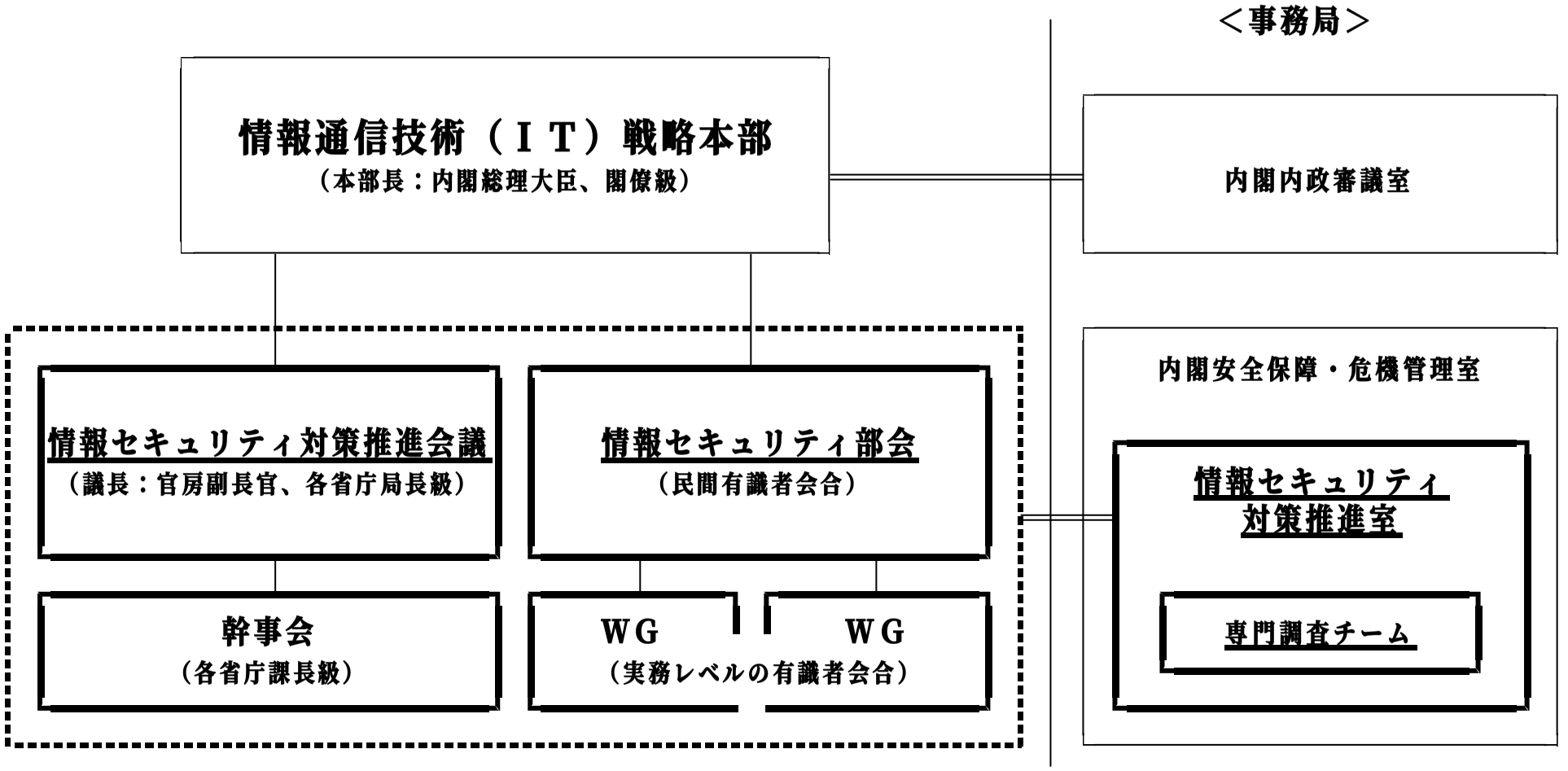
ＩＴ技術、国民生活に大きな影響を及ぼす重要インフラの多くが民間に存在することを踏まえ、官民の協力、連携を一層強化する。

③　国際連携の推進

情報セキュリティ確保のために、Ｇ８間の協力を始めとする国際協力の強化が不可欠。

④　研究・開発、人材の確保

情報セキュリティ関連の体制整備



参考1

情報セキュリティ関係省庁局長等会議

「行動計画」の概要
(「ハッカー対策等の基盤整備に係る行動計画」)

平成１２年１月

Ⅰ　背景

○　政府や民間における加速的な情報化・ネットワーク化の進展。
○　一方で、**ハッカーやウィルス**による問題発生の懸念。
　　↓
○　官民を含め我が国全体において、**情報化・ネットワーク化の進展に見合った、適切な情報セキュリティ水準を確保**していくことが必要。

↓

○　**昨年９月、情報セキュリティ局長等会議を設置**。

○　局長等会議における課題は、
　①法制度の検討
　②ハッカー対策等の基盤整備
　③サイバーテロ対策

○　今回の行動計画は、このうち、②の「**ハッカー対策等の基盤整備**」に係るもの。
　　↓
・「法制度の検討」については、引き続き検討。
・「**サイバーテロ対策**」については、今回の行動計画を基礎として、更に検討し、**本年１２月を目途**に「特別行動計画」をとりまとめる予定。

II　これまでの取組

○　**政府部内における取組**
　これまでも、各省庁の**情報システム部門を中心として**、技術的対策（パスワード管理、不正アクセス防止機能の導入、ウィルス検査等）を実施。

○　**民間に対する普及啓蒙等**（各種の基準・指針の提示等）
○　**技術開発の推進**
○　**法制度の整備と捜査体制の充実**
○　**国際的連携**（ＯＥＣＤ、Ｇ８その他）

III　取組強化に関する基本的考え方

1　政府部内における取組
○　電子政府の基盤構築を見据え、**平成１５年度を当面の目標年限**として設定。
○　各省庁の**情報システム部門のレベルに止まらず、政府全体として**取り組むべき課題との位置づけ（技術開発やセキュリティ評価といった政策ツールの有機的な活用等）。

2　民間等における取組
○　**政府部内における取組をモデル**として提示。
○　サイバーテロの危険性に鑑み、**民間重要インフラ等について**、特に取組を強化。

Ⅳ　具体的措置

1　政府部内における取組の強化

①システムの構築における対策

・製品等の**調達プロセスに、セキュリティ評価を導入**。

・セキュリティ関連の**技術開発**を推進し、成果を活用。

②システムの運用における対策

・**監視・緊急対処体制**の整備・強化。

（年末年始にＹ２Ｋ関連で設けた情報連絡体制も参考に）

③その他

・**総合的・体系的な情報セキュリティ対策**を引き続き検討。

・各省庁の対策を継続的に**評価・検証する体制**を検討。

2　民間等における取組の推進

①民間等一般への情報提供

・政府部門における取組強化等を踏まえ、**参考となる事項**を公開。

②民間重要インフラ等に係る取組の推進

・重要分野を選定し、**官民の連絡会議**を開催。

・本年１２月を目途に、サイバーテロ対策の「特別行動計画」をとりまとめ。

3　国際的連携の強化

上記対策の推進に伴い、**米国等の関係部局と**連携強化。

4　フォローアップ

以上の実施状況につき、**本年１２月**を目途にフォローアップ。

情報セキュリティポリシーに関するガイドラインの概要

平　成　１２　年　７　月
内閣安全保障・危機管理室
情報セキュリティ対策推進室

１．情報セキュリティポリシーに関するガイドライン

各省庁の情報システムにおけるセキュリティ対策をとりまとめる情報セキュリティポリシー策定のためのガイドラインであり、政府のセキュリティ対策の基本的な考え方、ポリシー策定の手順を示したガイドライン及び各省庁の情報システムにおける必須対策をとりまとめたポリシーの例等の付録から構成される。

２．情報セキュリティポリシーの概要

このガイドラインに従い策定される情報セキュリティポリシーの主な概要は次のとおり。

(1) **策定～導入～運用～評価・見直しを繰り返し高いセキュリティ水準を実現**

高いセキュリティ水準を確保するためには、単にポリシーを策定するだけではなく、適切な導入及び継続的な運用を行い、更には評価・見直しを繰り返し、ポリシーを発展させていく。

(2) **最高情報セキュリティ責任者及び情報セキュリティ対策委員会の設置により情報セキュリティ確保のための体制を確立**

情報セキュリティについて、組織幹部の関与を明確にするとともに、関係者の責任の所在を明確にするため、情報セキュリティに関する最高責任者定め、その下に情報セキュリティ委員会を設ける。

(3) **情報セキュリティ確保に必要な対策について、物理的セキュリティ、人的セキュリティ、技術的セキュリティ、運用の観点から包括的な対策を実施**

①	物理的セキュリティ	施設・設備を保護する出入り管理等
②	人的セキュリティ	職員に対する教育・訓練、パスワード管理等
③	技術的セキュリティ	ネットワーク管理、ウィルス対策等
④	運用	システムの監視、緊急時対応計画の策定

(4) **ポリシーに定められた情報セキュリティ対策の実施を徹底するため、各々の部局において実施手順を策定**

ポリシーに定められた情報セキュリティ対策の実施に必要な手順については、実施手順として文書化して定める。

３．今後の予定

各省庁においては、このガイドラインを踏まえ、平成１２年１２月までに情報セキュリティポリシーを策定する。

ポリシーの例については、セキュリティ対策ＷＧ委員及び各省庁の意見を踏まえ、内閣情報セキュリティ対策推進室において策定する。

情報セキュリティポリシーの概要

平成12年7月
内閣安全保障・危機管理室
情報セキュリティ対策推進室

Ⅱ革命による高速な情報の流通　電子政府への取組み　・・・　政府システムへのアクセスの増加

個人情報等の情報が漏洩する脅威　情報が改ざんされる脅威　・・・　情報が利用不可能になる脅威

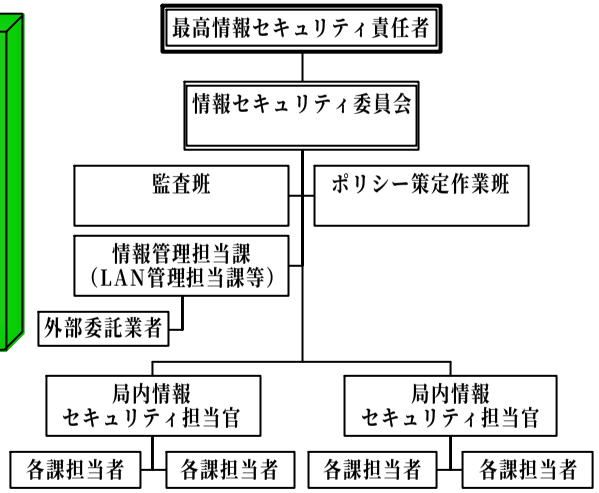
情報セキュリティ確保のため、明文化された情報セキュリティポリシーの策定が急務

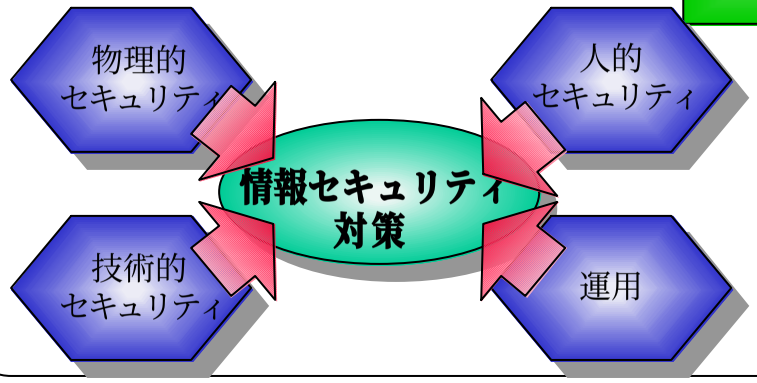
策定 → 導入 → 運用 → 評価・見直し → 策定

策定～導入～運用～評価・見直しを繰り返し高いセキュリティ水準を実現

情報セキュリティポリシーに関するガイドライン

最高情報セキュリティ責任者及び情報セキュリティ対策委員会の設置により情報セキュリティ確保のための体制を確立





物理的セキュリティ、人的セキュリティ、技術的セキュリティ、運用の観点から包括的な対策を実施

アメリカの情報セキュリティ体制

（PDD63のﾌﾚｰﾑﾜｰｸ）