報道発表

平成 18 年2月3日
内閣官房情報セキュリティセンター（NISC）

「第1次情報セキュリティ基本計画」等の政策会議決定について

― 「セキュア・ジャパン」の実現に向けて ―

1． 第4回情報セキュリティ政策会議での決定事項等

「情報セキュリティ政策会議」（議長；内閣官房長官）の第4回会合が持ち回り開催され、昨日、我が国の情報セキュリティ問題全般についての中長期計画である**「第1次情報セキュリティ基本計画」**と、**「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針」**について、政策会議決定がなされ、政府としての正式決定となりました。

※「情報セキュリティ政策会議」は、平成17年5月30日のIT戦略本部決定によって設置されました（http://www.nisc.go.jp/press/pdf/050530seisaku-press.pdf）。
※「第1次情報セキュリティ基本計画」及び「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針」は、内閣官房情報セキュリティセンター（NISC）ホームページ（http://www.nisc.go.jp/）において公表しています。

2．「第1次情報セキュリティ基本計画」について

昨日、政策会議決定された「第1次情報セキュリティ基本計画」の概要は以下の通りです。本基本計画の決定にあたっては、平成17年12月13日から本年1月13日までの間、パブリックコメントを実施し、21の個人・団体から76件のご意見を頂き、それらを踏まえ策定されたものです。

(1) 位置付けと主な内容（別紙1－1、1－2参照）

昨今、行政機関からの情報漏洩、国民生活・社会経済活動の基盤となる重要インフラの情報システムの停止、企業からの個人情報の漏洩等、**情報セキュリティを巡る問題が多発し複雑化**しています。こうした中、従来からの、個別縦割り的対応、対症療法的対応に問題があり、**我が国全体としての戦略的な取組みが必要**であることが指摘されてきました。これを受け、今般、**情報セキュリティ問題全般についての**

3年間の計画（2006年度～2008年度）としての「第1次情報セキュリティ基本計画」を策定することとしたものです。主な内容は以下の通りです。

①我が国が情報セキュリティ問題に取り組む上での基本理念を提示（別紙1－1参照）

○以下の3つの基本理念の下、今後3年間で、官民の全主体が適切な役割分担を果たす**「新しい官民連携モデル」を構築**し、その結果、我が国が「**情報セキュリティ先進国」へ進展**することを目指す。

＜3つの基本理念＞

1）経済国家日本の持続的発展を支える情報セキュリティ
2）安全・安心で、より良い国民生活を実現するための情報セキュリティ
3）我が国の安全保障における IT に起因する新たな脅威に対応するための情報セキュリティ

②今後3年間に取り組む重点政策の方向性を提示（別紙1－2参照）

○全主体が適切な役割分担を果たす**「新しい官民連携モデル」の構築に向けて**、今後3年間、政府は以下のような多面的な取組みを実施。

- 「政府機関統一基準」に基づいた各省庁の検査・評価、そして勧告を通じた改善プロセスの確立
- 地方公共団体における情報セキュリティ監査実施の推進
- 各重要インフラ分野における情報共有・分析機能（CEPTOAR）の整備と重要インフラ横断的な「重要インフラ連絡協議会（CEPTOAR-Council）」（仮称）の創設促進
- 企業の情報セキュリティ対策レベルの評価を政府調達の入札条件等へ盛り込み
- 情報セキュリティ教育の推進、「情報セキュリティの日」の創設等広報啓発の推進による個人の意識向上
- 成果を政府が活用することを前提とした情報セキュリティ関連の新たな研究開発・技術開発の推進
- 情報セキュリティに関する資格制度の体系化等を通した情報セキュリティ人材の育成
- 国際的な安全・安心の基盤作り等への貢献
- サイバー犯罪の取締り強化及び権利利益の保護・救済　　等

③政策の推進体制を提示

○政府全体の推進体制を有効に機能させるため、**内閣官房情報セキュリティセンター（NISC）を強化**。

○**「年度計画」の策定とその評価を実施**し、評価結果を公表、基本計画については3年ごとに見直しを実施。

(2) 今後の展開

本基本計画に基づき、2006年度から毎年度ごとの推進計画(「年度計画」)を策定していく予定です。

3. 重要インフラの情報セキュリティ対策について

昨日、政策会議決定された**「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針」**の概要は以下の通りです。本指針の決定にあたっては、平成17年12月13日から本年1月13日までの間、パブリックコメントを実施し、10の個人・団体から31件のご意見を頂き、それらを踏まえ策定されたものです。

(1) 位置付けと主な内容

「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針」は、重要インフラの情報セキュリティ対策のうち、まず喫緊に対応すべきものとして、重要インフラ分野ごとに対策の規範になる「安全基準等」を策定するにあたり、規定が望まれる事項(対策を行うべき事項)を横断的に提示するものです。

本指針は、従来から対策の中心に据えていた「サイバー攻撃等に起因する IT 障害」に加えて、昨今の証券取引所のシステム障害等でも問題となっている「システムの仕様やプログラム上の欠陥等に起因する IT 障害」も対象に含めて、対策の具体化を推進するものとなっています。位置付け及び内容は、別紙2をご参照下さい。

(2) 今後の展開

今後は、本指針に基づき、各重要インフラ分野ごとに、本年9月を目途に「安全基準等」の策定・見直しが推進される予定です。

【本件に関する問い合わせ先】

内閣官房情報セキュリティセンター

山口補佐官、大矢参事官、山崎参事官補佐

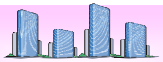
電話　03-3581-3768(センター代表)

第１次情報セキュリティ基本計画

－「セキュア・ジャパン」の実現に向けて－（２００６年２月２日　情報セキュリティ政策会議決定）

○行政機関からの情報漏洩、国民生活・社会経済活動の基盤となる重要インフラの情報システムの停止等、情報セキュリティ問題は多発し複雑化する一途。
○情報セキュリティ問題全般に関する中長期計画として、「第１次情報セキュリティ基本計画」（２００６年度から２００８年度までの３ヵ年計画）を策定。

現状



政府機関・地方公共団体
◆行政機関からの情報漏洩（複数　　等

重要インフラ
◆航空関連システムの停止、証券取引システムの停止 等

企業
◆企業からの個人情報の漏洩（複数）　等

個人
◆インターネットバンキング情報の窃取（複数）　　等

第１次情報セキュリティ基本計画
－「セキュア・ジャパン」の実現に向けて－

＜捉えるべき視点＞

基本理念

1. 経済国家日本の基盤としての情報セキュリティ
2. 安全・安心を求める、より良い国民生活実現のための情報セキュリティ
3. 新たな安全保障確保の観点からの情報セキュリティ

◆我が国の経済基盤（商取引）の１／４はITに依存

◆世界最大のブロードバンド大国
◆災害対策等安全・安心に対する国民ニーズの高まり

◆ITに起因する新しい安全保障への脅威と、我が国の「強み」の再認識

今後３年間の取組み

官民の各主体が適切な役割分担を果たす「新しい官民連携モデル」の構築
～ 内閣官房情報セキュリティセンター（NISC）を中心に、全主体が参加して実行 ～

目指すべき姿

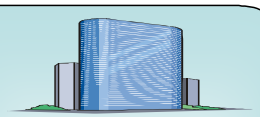
「情報セキュリティ先進国」への進展

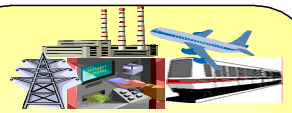
【政府機関】：**すべての政府機関**が「政府機関統一基準」が求める水準の対策を実施。【重要インフラ】：IT障害の発生を**限りなくゼロ**に。
【企業】：企業における情報セキュリティ対策の実施状況を**世界トップクラスの水準**に。【個人】：「IT利用に不安を感じる」とする個人を**限りなくゼロ**に。

別紙１－１

第1次情報セキュリティ基本計画－今後3年間の重点政策－

○全主体が適切な役割分担を果たす「新しい官民連携モデル」の構築に向けて、今後３年間、政府は「第１次情報セキュリティ基本計画」に基づき、各種対策を強化。





	政府機関・地方公共団体	重要インフラ	企業	個人
役割	情報セキュリティ対策の「ベストプラクティス」へ	国民生活・社会経済活動の基盤としての安定供給の確保	市場に評価される情報セキュリティ対策の実施	IT社会の担い手としての意識の向上
今後３年間の主な重点政策①（４領域）	◆政府機関統一基準に基づいた 各省庁の評価 ◆ サイバー攻撃等への緊急対応能力の強化	◆ 情報共有・分析機能の整備 ◆ 重要インフラ連絡協議会の設置 ◆ 分野横断的な演習、相互依存性解析の実施	◆政府調達における入札条件の整備 ◆ 情報セキュリティ監査等第三者評価制度の活用推進 ◆ コンピュータウィルス等への対応体制の強化	◆ 情報セキュリティ教育の推進 ◆「情報セキュリティの日」の創設等広報啓発の強化 ◆ ユーザーフレンドリーなサービスの提供等の環境整備
	政府機関統一基準	重要インフラ行動計画	各省庁による施策	各省庁による施策

今後３年間の主な重点政策②（横断的事項）

情報セキュリティ技術戦略の推進
- ◆政府が活用することを前提とした技術開発実施
- ◆「グランドチャレンジ型」技術開発の推進

国際連携・協調の推進
- ◆ 国際的な安全・安心の基盤づくりへの貢献
- ◆ 我が国発の国際貢献

情報セキュリティ人材の育成確保
- ◆ 多面的・総合的能力を有する実務家の育成
- ◆ 情報セキュリティの資格制度を体系化

犯罪の取締り、権利利益の保護救済
- ◆ サイバー犯罪の取締り強化及び関連基盤整備
- ◆ サイバー空間の安全性向上のための技術開発

別紙１－２

重要インフラの「安全基準等」の指針

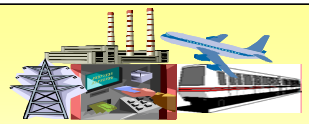
○証券取引や航空関連の情報システムの停止、重要情報の漏洩など、国民生活・社会経済活動の基盤となる重要インフラ(※1)のIT障害(※2)が昨今多発。

○IT障害から重要インフラを防護するための全体計画として「重要インフラの情報セキュリティ対策に係る行動計画」を策定(2005年12月13日情報セキュリティ政策会議決定)。

○このうち、まず喫緊に対応すべきものとして、重要インフラ分野ごとの規範となる「安全基準等」を策定するにあたり、規定が望まれる事項(対策を行うべき事項)について、横断的に示した「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針」を今般策定。

(※1) 重要インフラ10分野:情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流

(※2) 重要インフラの各事業において発生する障害(サービスの停止や機能の低下等)のうちITの機能不全が引き起こすものを「IT障害」という。



重要インフラの情報セキュリティ対策に係る行動計画

(2005年12月13日情報セキュリティ政策会議決定)

【4つの柱】

1.「安全基準等」の整備

2. 情報共有体制の構築(CEPTOAR)

3. 相互依存性解析の実施

4. 分野横断的演習の実施

重要インフラの「安全基準等」の指針

- 分野横断的視点から、情報セキュリティ対策の実施にあたり、対処がなされていることが望ましい項目を列記

<4つの柱>

1. 組織・体制及び資源の確保
2. 情報についての対策
3. 情報セキュリティ要件の明確化に基づく対策
4. 情報システムについての対策

<3つの重点項目>

1. IT障害の観点から見た事業継続性確保のための対策
2. 情報漏えい防止のための対策
3. 外部委託における情報セキュリティ確保のための対策

これを受け、各重要インフラ分野において、「安全基準等」の策定・見直し(2006年9月まで)

別紙2