報道発表

平成18年4月28日
内閣官房情報セキュリティセンター（NISC）

第5回情報セキュリティ政策会議の開催について

－「セキュア・ジャパン2006」（案）等の策定－

1．　第5回情報セキュリティ政策会議での決定事項等

本日、「情報セキュリティ政策会議」（議長；内閣官房長官）の第5回会合が開催され、

（1）「第1次情報セキュリティ基本計画」（平成18年2月2日情報セキュリティ政策会議決定）の目的を実現するための、**2006年度におけるより具体的な施策の実施プログラム**である**「セキュア・ジャパン2006」**の案について、パブリックコメントを実施することで合意が得られました。

（2）また、**「省庁基準の策定状況と組織・体制の構築状況」**と、**「重要インフラの情報連絡・情報提供に関する実施細目」**について、報告がなされました。

2.「セキュア・ジャパン2006」（案）について

本日、パブリックコメントを実施することで合意が得られた「セキュア・ジャパン2006」（案）の概要は以下の通りです。

（1）ポイント

「セキュア・ジャパン2006」（案）は、我が国の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）である「第1次情報セキュリティ基本計画」を実現するための、**2006年度における実施プログラム**であり、

ア）基本計画を着実に実行に移す（「セキュア・ジャパンへの第一歩」）とともに、昨今新たに起こった問題（ウィニーを介した情報流出、政府機関を狙ったサイバー攻撃の多発等）に確実に対応し、情報管理のあり方も含めた総合的な対応策を盛り込んだ**「2006年度の実施計画」**

イ）2006年度の具体的施策を受け継ぎ、「第1次情報セキュリティ基本計画」の最終

年度である2008年度に向けての確かな道筋を確立するために2007年度に推進する施策の方向性を示した**「2007年度の重点施策の方向性」**

から構成されています（別紙1－1、1－2参照）。

※「第1次情報セキュリティ基本計画」は、第4回情報セキュリティ政策会議（平成18年2月2日）で決定されました。
→http://www.nisc.go.jp/conference/seisaku/index.html#seisaku04

①「2006年度の実施計画」（別紙2－1、2－2、2－3参照）

○基本計画に掲げた目的を達成するために、3か年計画の初年度である2006年度においては、**「官民における情報セキュリティ対策の体制の構築」を重点として**、**133の具体的施策**を推進。主な内容は別紙2－1、2－2、2－3をご参照下さい。

②「2007年度の重点施策の方向性」（別紙2－4参照）

○2006年度の施策を受け継ぎ、基本計画の最終年度である2008年度に向けての確かな道筋を確立すべく、**「官民における情報セキュリティ対策の底上げ」を重点として、2007年度に推進する施策の方向性**として、**26の施策**の方向性を提示。主な内容は別紙2－4をご参照下さい。

（2）今後の展開

本案について、**速やかにパブリックコメントを実施**し、広く意見を募集した上で、「セキュア・ジャパン2006」を確定する予定です。

※パブリックコメントの募集は、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/）において実施します。

3．省庁基準の策定状況と組織・体制の構築状況について

本日、政策会議に報告された**「省庁基準の策定状況」**の概要は以下の通りです。

（1）位置付けと主な内容（別紙3参照）

第3回情報セキュリティ政策会議（平成17年12月13日）において**「政府機関統一基準（2005年12月版（全体版初版））」**が策定されたことを受け、内閣官房情報セ

キュリティセンターが各府省庁に、政府機関統一基準に基づく省庁基準の見直しと組織・体制の構築を依頼したところ、3月までに14省庁、4月までに5省庁において、省庁基準の策定及び組織・体制の整備が行われ、**全府省庁において省庁基準の策定及び組織・体制の整備が完了**しました。

※「政府機関統一基準（2005年12月版（全体版初版））」の具体的な内容につきまして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のでご参照下さい。

（2）今後の展開

今後、各府省庁は、省庁基準に基づき、さらに具体的な実施手順を整備し、対策の徹底を図るとともに、対策の実施状況の自己点検及び監査等を通じて、見直しを行っていきます。

4．重要インフラの情報連絡・情報提供に関する実施細目について

本日、政策会議に報告された**「『重要インフラの情報セキュリティ対策に係る行動計画』の情報連絡・情報提供に関する実施細目」**の概要は以下の通りです。

（1）位置付けと主な内容

「『重要インフラの情報セキュリティ対策に係る行動計画』の情報連絡・情報提供に関する実施細目」は、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のIT障害が昨今多発したことを受け、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、第3回情報セキュリティ政策会議（平成17年12月13日）において策定された、**「重要インフラの情報セキュリティ対策に係る行動計画」のうち、官民の協力の下、情報の円滑な共有を推進すべく、情報連絡の方法、情報の取り扱いに関する取り決めなど、内閣官房を中心とした体制における具体的な実施事項について規定した**ものです。主な内容は、別紙4をご参照下さい。

※「重要インフラの情報セキュリティ対策に係る行動計画」の具体的な内容につきまして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のでご参照下さい。

（2）今後の展開

今後は、これを受け、**各重要インフラ分野におけるIT障害に関する内閣官房と重要インフラ所管省庁等との間の情報連絡・情報提供を実施していく**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、小林参事官、佐藤（隆）参事官補佐

電話　03-3581-3768（センター代表）

※「情報セキュリティ政策会議」は、2005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）。

※本日の会議資料は、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。また本日の議事要旨は、後日、同ホームページにて公表いたします。

「第1次情報セキュリティ基本計画」の概要と「セキュア・ジャパン2006」（案）の位置づけ

「第1次情報セキュリティ基本計画」（2006年2月2日　情報セキュリティ政策会議）

2006～08年度の3ヵ年計画。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」の構築を目指す。

	政府機関・地方公共団体	重要インフラ	企　業	個　人
目標	2009年度初めには すべての政府機関が 「政府機関統一基準」が 求める水準に	2009年度初めには IT障害を限りなくゼロに	2009年度初めには 対策の実施状況を 世界トップクラスの水準に	2009年度初めには 「IT利用に不安を感じる」 個人を限りなくゼロに
各実施領域の重要政策	◆ 政府機関統一基準に基づく各省庁の評価 ◆ 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 ◆ 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 ◆ 第三者評価制度の活用 ◆ ウィルス等への体制強化	◆ セキュリティ教育の推進 ◆ 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

横断的な重要政策

- 情報セキュリティ技術戦略の推進
- 情報セキュリティ人材の育成確保
- 国際連携・協調の推進
- 犯罪の取締り、権利利益の保護救済

2005年度 → 2006年度 → 2007年度 → 2008年度 → 2009年度

「セキュア・ジャパン2006」（案）

① 2006年度の実施計画
～「官民におけるセキュリティ対策の体制の構築」

② 2007年度の重点施策の方向性
～「官民におけるセキュリティ対策の底上げ」

セキュア・ジャパン2007

セキュア・ジャパン2008

別紙１－１

「セキュア・ジャパン2006」（案）のポイント

○「第１次情報セキュリティ基本計画」（2006年２月２日）を着実に実行に移す（「セキュア・ジャパンへの第一歩」）とともに、昨今新たに起こった問題（ウィニーを介した情報流出等）に確実に対応し、情報管理のあり方も含めた総合的な対応策を盛り込み。

○2006年度に実施する具体的行動計画と、2007年度の重点施策の方向性を示す。

＜基本計画を着実に実行に移す必要性＞

－「第1次情報セキュリティ基本計画」（2006年度～2008年度）の実現に向けての初年度（「セキュア・ジャパンへの第一歩」）

＜基本計画策定(2006.2.2)後に起こった主な問題への対応＞

➢Winny（ウイニー）を介した情報流出の多発

最近の情報流出（報道ベース）	
2月13日	鹿児島刑務所・福岡拘置所の受刑者情報等
2月21日	宮崎地検に係る被疑者情報等
2月22日	栃木県警の捜査資料等
2月23日	海上自衛隊の通信に関する情報等
3月 2日	陸上自衛隊及び航空自衛隊の訓練計画等
3月 3日	岡山県警の捜査資料等
3月 7日	愛媛県警の捜査資料等

➢政府機関を狙ったサイバー攻撃の多発

－DoS攻撃（サービス妨害攻撃）に加え、政府機関向けに新種のコンピュータウイルスを送り込む攻撃が発生

全体対策

対策の方向性

＜「セキュア・ジャパン2006」（案）のポイント＞

政府機関の情報セキュリティ対策の徹底

→2006年度中に対策の徹底を図る

【主な具体策】

- 「政府機関統一基準」に基づき各政府機関が対策を徹底し（情報の外部持ち出し及び私物パソコンの業務使用の管理も含んだ全体対策）、内閣官房がその対策を評価し、結果を公表
- 内閣官房を中心として、高セキュリティ機能を実現する次世代OS環境を開発
- 内閣官房を中心としたサイバー攻撃等に関する情報収集、分析・解析機能の強化

広く国民も含めた全主体への対策の普及

→2006年度中に「官民における体制の構築」を図る

【主な具体策】

- 小中学校からの情報セキュリティ教育を実施
- 「インターネット安全教室」等による普及啓発を実施
- 企業が政府調達に参加する際の入札条件の整備を検討
- 重要インフラ分野ごとに「安全基準等」を策定し、それを評価

対策が遅れがちな主体の底上げ

→2006年度に着手し、2007年度に「官民における対策の底上げ」を図る

【主な具体策】

- 分かりやすく実用的な教育コンテンツを作成・配布
- 情報セキュリティ教育者、専門家の育成・訓練とキャリアパスの構築

別紙１－２

「セキュア・ジャパン2006」（案）に盛り込む具体的施策①　～2006年度の実施計画～

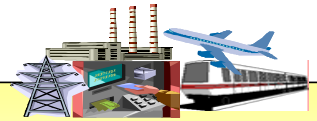
対策実施4領域における情報セキュリティ対策の強化

1　政府機関・地方公共団体

【　目　標　】 政府機関について、2008年度までに政府機関統一基準のレベルを世界最高水準のものとし、かつ、2009年度初めにはすべての政府機関において政府機関統一基準が求める水準の対策を実施していることを目指す。

【主な施策】
- ○ 「政府機関統一基準」に基づくPDCAサイクルの確立・試行的評価の実施及び結果の公表（内閣官房及び全府省庁）
- ○ 各府省庁における情報の外部持ち出し及び私物パソコンの業務使用に関する厳格な管理（全府省庁）
- ○ 高セキュリティ機能を実現する次世代OS環境の開発（内閣官房、内閣府、総務省及び経済産業省）
- ○ 政府機関に対するサイバー攻撃等に関する情報収集、分析・解析機能の強化（内閣官房）
- ○ 地方公共団体における情報セキュリティポリシーの策定・見直しの促進（総務省）　等

2　重要インフラ



【　目　標　】 2009年度初めには、重要インフラにおけるIT障害の発生を限りなくゼロにすることを目指す。

【主な施策】
- ○ 各重要インフラ分野における情報セキュリティ確保に係る「安全基準等」の策定・見直し（重要インフラ所管省庁）
- ○ 「安全基準等」の策定状況の把握及び評価（内閣官房）
- ○ 情報共有体制整備と機能強化（内閣官房及び重要インフラ所管省庁）
- ○ 各重要インフラ分野の依存関係を可視化できる仕組みの構築及びこれに基づく相互依存性解析の試行的実施（内閣官房）
- ○ 重要インフラ横断的な研究的演習及び机上演習の実施・各分野サイバー演習間の連携（内閣官房及び重要インフラ所管省庁）　等

別紙2－1

「セキュア・ジャパン2006」（案）に盛り込む具体的施策②　～2006年度の実施計画～

対策実施4領域における情報セキュリティ対策の強化（続き）

3 企 業

【 目 標 】2009年度初めには、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することを目指す。

【主な施策】
- ○ 企業における情報セキュリティガバナンスの確立促進（経済産業省）
- ○ 政府調達において競争参加者に入札条件等として求めるセキュリティ対策レベルの検討（内閣官房、総務省、財務省及び全府省庁）
- ○ 情報セキュリティ関連制度と内部統制制度等との整合性確保（内閣官房、金融庁及び経済産業省）
- ○ 情報セキュリティ関連リスクに対する定量的評価手法の検討（経済産業省）
- ○ 情報通信セキュリティ人材を育成するための研修事業への支援（総務省）　等

4 個 人

【 目 標 】2009年度初めには、「IT利用に不安を感じる」とする個人を限りなくゼロにすることを目指す。

【主な施策】
- ○ 小中学校における情報セキュリティ教育の推進（文部科学省）
- ○ 「インターネット安全教室」の充実・強化と全国での継続的開催（経済産業省及び警察庁）
- ○ 保護者・教職員向け啓発講座（e－ネットキャラバン）の全国規模での実施（総務省及び文部科学省）
- ○ 「情報セキュリティの日」の創設（内閣官房、警察庁、総務省、文部科学省及び経済産業省）
- ○ IPv6によるユビキタス環境構築に向けたセキュリティの確保（総務省）　等

別紙2－2

「セキュア・ジャパン2006」（案）に盛り込む具体的施策③ ～2006年度の実施計画～

横断的な情報セキュリティ基盤の形成

1 情報セキュリティ技術戦略の推進

【主な施策】
- ○ 高い情報セキュリティ保証レベル（EAL6）を満足する情報システムの試作（防衛庁）
- ○ 長期的な視野で抜本的な技術革新等の実現を目指す「グランドチャレンジ型」のテーマ検討（内閣官房及び内閣府） 等

2 情報セキュリティ人材の育成・確保

【主な施策】
- ○ 情報セキュリティ関連の高等教育機関における多面的・総合的能力を有する人材の育成（文部科学省）
- ○ 情報セキュリティに関する資格制度の体系化等のための検討（内閣官房、総務省、文部科学省及び経済産業省） 等

3 国際連携・協調の推進

【主な施策】
- ○ 多国間の枠組み等における国際連携・協力の推進（内閣官房及び全府省庁）
- ○ ベストプラクティスの国際的な発信・普及（内閣官房及び全府省庁） 等

4 犯罪の取締り及び権利利益の保護・救済

【主な施策】
- ○ サイバー犯罪の取締り強化のための技能水準の向上、体制の強化・整備、捜査・解析用資機材の充実・強化（警察庁）
- ○ 高度なネットワーク認証基盤実現のための技術開発（内閣官房） 等

政策の推進体制等

1 政策の推進体制、他の関係機関等との連携

【主な施策】
- ○ 内閣官房情報セキュリティセンター（NISC）の強化（内閣官房）
- ○ 情報セキュリティ対策の体制の強化及び府省庁横断的な取組みの実施（全府省庁）
- ○ 関係機関等（IT戦略本部、経済財政諮問会議、総合科学技術会議等）との連携強化（内閣官房及び内閣府） 等

2 持続的改善構造の構築

【主な施策】
- ○ 「セキュア・ジャパン2006」の評価の実施及び公表（内閣官房）
- ○ 政府機関の情報セキュリティ対策強化に向けたマイルストーンの検討等（内閣官房）
- ○ 情報セキュリティ対策に関する評価指標の確立（内閣官房、総務省及び経済産業省） 等

別紙2－3

「セキュア・ジャパン2006」（案）に盛り込む具体的施策④～2007年度の重点施策の方向性～

○2006年度の体制の構築を受け継ぎ、2008年度に向けての確かな道筋を確立すべく、「官民における情報セキュリティ対策の底上げ」を重点として、2007年度に推進する施策の方向性を提示。

2007年度：官民における情報セキュリティ対策の底上げ

模範となる領域の情報セキュリティ対策の底上げ

- ○ 政府機関でのPDCAサイクルの定着と本格的評価の推進
- ○ 政府機関に対するサイバー攻撃等に対する機能の強化
  （GSOC（Government Security Operation Coordination team）の本格稼動）
- ○ 重要インフラ分野間の動的依存性解析、機能的演習の推進　等

取組みが遅れがちな主体の対策の底上げ

- ○ 政府機関の情報に係るポータルサイトの充実・整備
- ○ 分かりやすく実用的な教育コンテンツの作成・配布
- ○ サイバー犯罪の情勢を反映した被害防止対策の推進　等

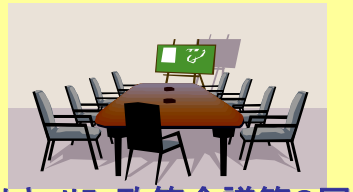
横断的な情報セキュリティ基盤の底上げ

- ○ 「情報セキュリティ対策白書（仮称）」の作成・発行
- ○ 情報セキュリティ教育者、専門家の育成・訓練とキャリアパスの構築に向けた戦略の検討
- ○ 高セキュリティ機能を実現する次世代OS環境の部分的成果の実証利用と機能拡大に向けた開発
- ○ サイバー犯罪に対する捜査能力の総合的底上げ　等

2008年度（基本計画の最終年）へ

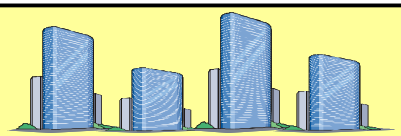
別紙２－４

省庁基準の策定状況と組織・体制の構築状況



情報セキュリティ政策会議第３回会合
（2005年12月13日）
政府機関統一基準（ 2005年12月版（全体版初版））策定

内閣官房情報セキュリティセンター
政府機関統一基準に基づく省庁基準の見直しと組織・体制の構築を依頼



各府省庁
省庁基準の策定及び組織・体制の整備について、
３月末までに完了１４省庁
４月中に完了５省庁

	省庁基準の策定	組織・体制の構築
内閣官房	３月	３月
内閣法制局	３月	３月
人事院	３月	３月
内閣府	３月	３月
宮内庁	３月	３月
公正取引委員会	３月	３月
警察庁	３月	３月
防衛庁	４月	４月
金融庁	３月	３月
総務省	２月	３月
外務省	４月	４月
法務省	４月	４月
財務省	３月	３月
文部科学省	３月	３月
厚生労働省	３月	３月
農林水産省	４月	４月
経済産業省	３月	３月
国土交通省	４月	４月
環境省	２月	３月

別紙３

「『重要インフラの情報セキュリティ対策に係る行動計画』の情報連絡・情報提供に関する実施細目」の概要について

○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、官民の協力の下、情報の円滑な共有を促進すべく、内閣官房を中心とした体制における具体的な実施事項について規定。

（※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
   - (1) 官民の情報提供・連絡
   - (2) CEPTOAR
   - (3) CEPTOAR-Council
3. 相互依存性解析の実施
4. 分野横断的演習の実施

情報連絡・情報提供に関する実施細目

- 重要インフラ事業者等がサービスを維持・復旧することがより容易になるように、官民の協力の下、情報の円滑な共有を促進
- 内閣官房情報セキュリティセンターと重要インフラ所管省庁等との間の情報連絡・情報提供について規定
  - ○ 情報共有レベルの設定（Traffic Light Protocol の採用）
  - ○ 情報連絡の手順の設定
    - ・情報連絡におけるIT障害に関する共通の分類・カテゴリの設定
    - ・統計的な発生状況の把握
  - ○ 情報提供の手順の設定

これを受け、各重要インフラ分野におけるIT障害に関する情報連絡・情報提供を実施

別紙4