報道資料

平成 22 年 5 月 11 日
内閣官房情報セキュリティセンター（NISC）

情報セキュリティ政策会議第 23 回会合の開催について

－「国民を守る情報セキュリティ戦略」の決定等－

本日、「情報セキュリティ政策会議」（議長：内閣官房長官）の第 23 回会合が開催され、その概要は以下のとおり。

1.「国民を守る情報セキュリティ戦略」決定

本日、我が国の情報セキュリティ政策に係る基本戦略である「国民を守る情報セキュリティ戦略」が決定された。

昨年7月、米韓において大規模なサイバー攻撃が発生するなど、最近、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している。また、諸外国においても情報セキュリティに関し戦略的な取組が行われているところである。

このような新たな環境変化に的確に対応し、安全・安心な国民生活を実現するため、今後4年間を対象として、既存の「第2次情報セキュリティ基本計画」を包む、包括的な新たな情報セキュリティ戦略を策定することとしたもの。

（資料1－1及び資料1－2参照）

2. 第2次情報セキュリティ基本計画の進捗状況について

第2次情報セキュリティ基本計画の進捗状況について報告された。

（資料2参照）

※ 本日の会議資料は、内閣官房情報セキュリティセンターのホームページにおいて公表する。
（http://www.nisc.go.jp/conference/seisaku/index.html#seisaku23）

国民を守る情報セキュリティ戦略の概要

資料1－1

現状の課題

大規模なサイバー攻撃事案等の脅威の増大

✓重要インフラ等、国民生活に直結するサービスの情報通信技術への依存による脅威の増大
✓国境を越えたサイバー攻撃が現実化（米韓大規模サイバー攻撃（昨年7月））
✓ガンブラーウイルス等、年々新たなウイルスが出現。攻撃手法も高度化・多様化

社会経済活動の情報通信技術への依存度の増大

✓情報家電、電子タグなどあらゆる機器がネットワークに接続
✓ 約8割の国民が情報セキュリティに不安感

急速な技術革新の進展

✓ クラウド・コンピューティング技術、IPv6への移行
✓ 暗号の危殆化につながるコンピュータの能力向上

グローバル化の進展

✓ 国境を越えた瞬時の情報流通
✓ 各国の個人情報保護・情報セキュリティ制度の調和

- *重要インフラ等の国民生活に直結するサービスの情報通信技術への依存の高まりにより、脅威（ITリスク）は着実に増大*
- *情報セキュリティ上の攻撃手法が多様化・高度化・複雑化しており、従来の取り組みでは対応が困難*
- *各国でも戦略的な取り組み（＊）を実施*

（＊）米国
・サイバースペース政策レビュー（60日レビュー）
・「サイバーセキュリティ調整官」を設置し、国家的取組みを強化
・「2010 Cybersecurity Enhancement Act 」（2010年2月）

課題に対応する
新戦略の必要性

「国民を守る情報セキュリティ戦略」

国民を守る情報セキュリティ戦略（2010～2013）

第2次基本計画（2009～2011）

（＊）第2次情報セキュリティ基本計画を包含し、今後4年間の重点的な取組み

基本的な考え方（取組みの重点化）

① サイバー攻撃の発生を念頭に置いた政策強化・対処体制整備
② 新たな環境変化に対応した政策の確立
③ 受動的な対策から能動的な対策へ

⇒

➢ ITリスクを克服し、安全・安心な国民生活を実現
➢サイバー空間の安全保障・危機管理政策の強化と情報通信技術政策の連携
➢安全保障・危機管理及び経済の観点に国民・利用者保護の観点を加えた3軸構造の総合的な政策（特に、国民・利用者の視点を重視した政策の推進）
➢ 国際連携の強化

安全・安心な国民生活を実現

サイバー空間上の我が国の安全保障・危機管理の確保

情報通信技術の利活用を促進し、我が国の経済成長に寄与

実現すべき成果目標

2020年までに、インターネットや情報システム等の情報通信技術を利用者が活用するにあたっての脆弱性を克服し、全ての国民が情報通信技術を安心して利用できる環境 （高品質、高信頼性、安全・安心を兼ね備えた環境）を整備し、世界最先端の「情報セキュリティ先進国」を実現

具体的な取組

● *強力なリーダシップの下、総合的な政策推進体制を確立し、官民の役割の明確化、官民連携を強化*

1　大規模サイバー攻撃事態への対処態勢の整備等

サイバー攻撃事態への対処態勢の整備

・平時からの対策と事案対処の連携強化

➢対処態勢の整備
- ・初動対処態勢の整備
- ・初動対処訓練の実施
- ・官民連携の推進
- ・サイバー攻撃に対する防衛分野での体制強化
- ・サイバー犯罪の取締り　等

➢平素からの情報収集・共有体制の構築・強化
- ・対処に資する情報収集・分析・共有体制の強化
- ・諸外国等との情報共有体制の構築・強化

2　新たな環境変化に対応した情報セキュリティ政策の強化

国民生活を守る情報セキュリティ基盤の強化

➢政府機関等の基盤強化
- ・各府省の最高情報セキュリティ責任者（CISO）の強化
- ・政府横断的な情報収集・分析システム（GSOC）の強化
- ・政府統一基準の見直し、政府機関情報システムの対策強化
- ・共通番号制に対応した情報セキュリティ対策の検討　等

➢重要インフラの基盤強化
- ・分野横断的な官民連携体制の強化
- ・情報共有体制の強化、サービス提供が確保できるシステム等の検討
- ・事業継続計画（BCP）の充実　等

➢その他の基盤強化
- ・マルウェア対策の充実・強化
- ・クラウド化、IPv6に対応した情報セキュリティ確保方策
- ・中小企業に対する情報セキュリティ対策支援
- ・医療、教育分野等における情報セキュリティ確保方策　等

国民・利用者保護の強化

➢普及啓発活動の充実・強化
- ・情報セキュリティ月間による普及啓発の強化
- ・包括的な普及啓発プログラムの策定

➢情報セキュリティ安心窓口（仮称）の検討
- ・地域NPO法人等の支援
- ・国民・利用者からの相談受付窓口の検討

➢個人情報保護の推進
- ・プライバシー保護技術の適切な利用促進
- ・個人情報保護に関するガイドラインの見直し
- ・国際的なフレームワークへの対応　等

➢サイバー犯罪に対する態勢の強化
- ・犯罪取締りのための基盤整備の推進　等

国際連携の強化

➢米国、ASEAN、欧州等との連携強化
- ・日米サイバーセキュリティ会合、日ASEAN情報セキュリティ政策会議等を通じた戦略的連携強化
- ・海外CSIRTの構築支援
- ・新たな二国間関係の構築

➢APEC、ARF、ITU、MERIDIAN、IWWN等の国際会合を活用した情報共有体制等の強化
- ・国際会議への積極的な参加を通じた情報共有体制の強化

➢NISCの窓口機能の強化
- ・情報セキュリティに関するベストプラクティスの共有等
- ・情報セキュリティ政策について諸外国等と連携強化　等

技術戦略の推進等

➢情報セキュリティ関連の研究開発の戦略的推進等
- ・新たな情報セキュリティ研究開発戦略の策定
- ・高度化・多様化する攻撃等に対応できる技術の実現・普及（「グランドチャレンジ型」研究開発の推進）

➢情報セキュリティ人材の育成
- ・政府、大学、企業等における高度な情報セキュリティ人材の育成

➢情報セキュリティガバナンスの確立
- ・情報セキュリティガバナンスの経営としての位置付け
- ・事業継続計画（BCP）の策定、情報セキュリティ監査　等

制度整備

➢サイバー空間の安全性・信頼性を向上させる制度の検討等
- ・コンピュータウイルス関連の法改正等サイバー犯罪条約の早期締結に向けた検討
- ・機微な情報へのアクセス権限の明確化の検討　等

➢各国の情報セキュリティ制度の比較検討
- ・各国間の法制度等の相違について分析し、情報セキュリティ関連の国際連携のための課題抽出・連携方策の検討を実施

資料1-2

国民を守る情報セキュリティ戦略

2010 年 5 月 11 日
情報セキュリティ政策会議

Ⅰ．はじめに

これまで、我が国の情報セキュリティ対策については、情報セキュリティ政策会議（議長：内閣官房長官）において決定された「第２次情報セキュリティ基本計画」（2009 年 2 月 3 日）に基づき、官民の各主体によって取組が推進されてきたところである。

他方で、「第２次情報セキュリティ基本計画」策定後、2009 年 7 月に米韓における大規模サイバー攻撃事態が発生したほか、大規模な個人情報漏えい事案の発生も後を絶たない。

特に、米韓における大規模サイバー攻撃事態は、経済活動や社会生活の多くの面において情報通信技術への依存が進む我が国にとって、情報セキュリティ上の脅威が安全保障・危機管理上の問題になり得ることを示す契機となった。

また、最近、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している。更に、米国では、サイバーセキュリティ調整官を設置し国家的な取組を強化するなど、諸外国においても情報セキュリティに関し戦略的な取組が行われているところである。

こうした情報セキュリティを巡る環境の変化に的確に対応するため、「第２次情報セキュリティ基本計画」に基づく官民の各主体による取組を継続しつつ、新たな環境変化に対応した政府の取組を進める必要がある。特に、国民の日常生活に関わりの深い社会経済活動を支える重要インフラ防護の強化等により、情報通信技術の利用に係るリスク（ＩＴリスク）を克服する。また、安全保障・危機管理の観点から速やかに実施すべき取組について、これを強力に推進することとする。

本戦略は、「第２次情報セキュリティ基本計画」を包含する、今後 4 年間（2010 年度から 2013 年度）を対象とした包括的な戦略であり、本戦略に基づき、毎年度の年度計画である「セキュア・ジャパン 20XX」を推進する。また、本戦略の評価を定期的に行い、必要に応じて本戦略の取組内容の見直しを行う。

Ⅱ．基本的な考え方

（１）基本方針

情報セキュリティ政策については、「第２次情報セキュリティ基本計画」に基づく従来からの官民の取組を継続しつつ、以下の基本方針に基づき、政府による新たな取組の着手・実行や取組の重点化を行うとともに、安全保障・危機管理の観点からも速やかに実施すべき取組の強力な推進を図る。

① サイバー攻撃事態の発生を念頭に置いた政策の強化及び対処体制の整備

大規模サイバー攻撃等、我が国の安全保障・危機管理に影響を及ぼしうるサイバー攻撃から国民を守るための、平素からの取組を強化するとともに、サイバー攻撃事態が発生した際に有効に対処できる体制を整備する。

② 新たな環境変化に対応した情報セキュリティ政策の確立

社会経済活動が情報通信技術への依存度を高める中、あらゆる機器がネットワークに繋がり、情報が国境を越えて自由に流通することなどから、従来以上に情報セキュリティ上のリスクが増大しており、これらの新たに顕在化しつつある情報セキュリティ上のリスク・脅威等の環境変化に対し柔軟に対応可能な、国民生活を守る情報セキュリティ政策を確立する。

③ 受動的な情報セキュリティ対策から能動的な情報セキュリティ対策へ

従来の情報セキュリティ対策は、リスクが発生した時点でその都度対応するといった対症療法的な対策に流れる傾向にあり、本質的な対策に至らない場合が多かった。情報通信技術の進歩が著しい中、問題の根本的な解決をもたらす情報セキュリティ対策の検討等に戦略的に取り組むとともに、ＰＤＣＡサイクルを活用するなど、受動的な情報セキュリティ対策から、各主体が能動的に取組を進められる体制の実現を目指す。

（２）背景

基本方針を定めるにあたり、考慮した最近の環境変化は以下のとおりである。

① 大規模なサイバー攻撃事案等の脅威の増大

2009 年 7 月に、韓国内を中心とする極めて多数のボットに感染した PC（ボット感染 PC）から米国・韓国の政府機関等に対して大規模な DDoS 攻撃（分散サービス不能攻撃）がなされた。当該 DDoS 攻撃は我が国の情報システム等を直接の対象としたものではなかったが、同様の手法を用いて大規模なボット感染 PC のネットワークが構築され、我が国の情報システム等に対し大規模なサイバー攻撃が行われる可能性は否定できない。また、国内の多数のウェブサイトが改ざんされた、いわゆる「ガンブラー」型攻撃等、攻撃手法は年を追うごとに高度化・複雑化している状況にある。重要インフラ等の多くが情報通信技術を用いたシステムによって制御されるようになったことを踏まえると、国民生活の安全等のための情報セキュリティを確保する必要性が増大している。

他方で、クレジットカード情報や銀行口座情報等を売買するアンダーグラウンド市場の存在が指摘されており、経済的利得を誘因としてインターネット上の犯罪行為が発生する傾向にある。また、企業による個人情報等の漏えい事故は引き続き多発しており、漏えいした情報が悪用されることにより、消費者等が被害を受けるケースも発生している。

② 新たな環境変化

（ｉ）社会経済活動の情報通信技術への依存度の増大

（社会経済活動との関係）

社会経済活動における「情報」の役割が増大し、我が国の社会経済活動が情報通信技術への依存度を高める中で、情報セキュリティは社会基盤の一つになっている。経済成長や少子高齢化、地球環境問題への対応等、我が国が有する課題の解決に情報通信技術を活用していくためには、近年のあらゆる機器がネットワークに接続される環境を踏まえ、情報通信技術の利用環境を安全・安心な形で構築することが不可欠となっている。また、海外での事業活動や生産・開発委託の拡大等の経済活動のグローバル化が進む中で、我が国企業が自ら保有する情報資産の価値を保護しつつ情報通信技術を活用したグローバルな企業活動や生産・品質管理（サプライチェーンマネジメント）を推進していくためには、我が国のみならず海外においても安全・安心な情報通信技術の利用環境を整備し、海外の情報セキュリティレベルを向上させていくことが重要となっている。さらに、各企業の知的財産、音楽・映像コンテンツ等の知的財産がインターネットを通じて流通する現在、「知識情報社会」を支える情報通信技術基盤の安全・安心が確保され、情報資産が適切に保護され

ていく必要がある。

（国民・利用者保護）

国民生活における「情報」の役割が増大し、情報通信技術への依存度が高まる中で、従来以上に情報通信技術の利用者としての国民の権利・利益を保護する視点を重視し、国民の情報資産の保護や情報セキュリティの確保等に取り組んでいく必要がある。同時に、ＩＴリスクを認識する国民が主体的に情報セキュリティ対策に取り組むことができる環境を醸成することが重要である。現状では、情報セキュリティの確保に関して、約８割の国民が不安感を持っており、情報通信技術の活用を促進するためには、その早期解消が課題となっている。

（ⅱ）新たな技術革新への対応

情報通信技術の技術革新と情報セキュリティの確保は軌を一にして推進される必要がある。クラウドコンピューティング技術の発達、IPv6等新たなインターネット技術、情報家電、携帯端末、電子タグの普及及び暗号の危殆化にもつながるコンピュータの演算能力向上等、情報通信技術の技術革新や情報技術を活用したビジネス革新は留まることなく進展していることから、これら情報通信技術の技術革新や技術の普及に的確に対応した情報セキュリティ政策を推進する必要がある。

（ⅲ）グローバル化等

グローバルな経済活動や、インターネットを経由して国境を越えたサービスの提供が行われる中、国境を超えて流通する情報が増大している。これに伴い、個人情報保護や情報セキュリティに関する各国間の法制度等の相違が、情報が国境を越えて自由に流通する際の課題として顕在化しつつある。

（３）重点的な取組

今後、情報セキュリティに係る政府の取組を推進するにあたっては、上記（１）の基本方針等を踏まえ、具体的に以下の事項に重点的に取り組むこととする。

①　ＩＴリスクを克服し、安全・安心な国民生活を実現

社会経済活動の情報通信技術への依存度が高まり、情報セキュリティ上の脅威が増大している中、特に、国民の日常生活に関わりの深い

社会経済活動を支える重要インフラ防護の強化等により、ＩＴリスクを克服し、安全・安心な国民生活を実現する。また、大規模なサイバー攻撃等の脅威の増大等を踏まえ、近年、サイバー空間が我が国の安全保障・危機管理上重要な活動空間となっていることから、サイバー空間の安全保障や危機管理を高める政策を強力に推進する。

② サイバー空間の安全保障・危機管理に係る政策の強化と社会経済活動の基盤としての情報通信技術政策との連携

サイバー空間の安全保障や危機管理を高める政策の強化にあたっては、社会経済活動の基盤としての情報通信技術の利活用を推進するというＩＴ基本法等の理念に沿って行われている政策との十分な連携を図る。

③ 安全保障・危機管理及び経済の観点に、国民・利用者保護の観点を加えた3軸構造の総合的な政策の確立。特に、国民・利用者の視点を重視した情報セキュリティ政策を推進

サイバー空間における安全保障・危機管理の向上や経済社会活動の基盤としての情報通信技術の利活用促進といった観点からの情報セキュリティ政策のみならず、情報通信技術革命の恩恵は国民一人一人が享受すべきであるとの基本理念に立ち返り、特に、国民・利用者の視点を重視した情報セキュリティ政策を推進する。

④ 経済成長戦略に寄与する情報セキュリティ政策の確立

情報通信技術の利活用を図っていく上で不可欠となる、安全・安心で高い信頼性のある情報通信技術環境が経済社会活動の基盤として提供されることは、情報通信技術の戦略的投資や利活用が促進され、我が国の経済成長や我が国が有する課題の解決に資する。このような経済成長戦略に寄与する情報セキュリティ政策を推進・確立する。

⑤ 国際連携の強化

情報が国境を越えて自由に流通することによりグローバルな観点での利便性等が向上する一方、グローバルな観点での各国間制度の相互の調和等、人類が今まで直面しなかった新たな課題も発生しており、情報セキュリティ政策に関して国際連携・協調を強化する必要がある。特に、データプライバシー保護等を含む広義の情報セキュリティ政策に関する国際連携を強化する。

Ⅲ. 実現すべき成果目標

○ 2020 年までに、インターネットや情報システム等の情報通信技術を利用者が活用するにあたっての脆弱性を克服し、すべての国民が情報通信技術を安心して利用できる環境（高品質、高信頼性、安全・安心を兼ね備えた環境）を整備し、世界最先端の「情報セキュリティ先進国」を実現する。

　具体的には、サイバー攻撃等、情報通信技術に係る全ての脅威に対する対応力を世界最高水準に高めるとともに、政府の事案対処能力を充実・強化することにより、国民の安全・安心を確保する。また、すべての国民が、情報セキュリティに対する不安を感じずに情報通信技術を積極的に活用できる環境を構築する。

○ 今後 4 年間は、「第 2 次情報セキュリティ基本計画(2009 年度-2011 年度)」に規定された施策の推進に加え、以下に述べる具体的な取組を重点的に推進し、情報セキュリティに対する国民の不安を解消する。

Ⅳ. 具体的な取組

　情報セキュリティ政策の推進にあたっては、情報セキュリティ事案発生時に的確な対応を行い、国民の安全・安心を確保することは言うまでもないが、今後、益々高度化・多様化する情報セキュリティ事案に的確に対応するためには、我が国全体の「基礎対応力」を常に向上させておくことが不可欠である。そのためには、強力なリーダーシップの下、内閣官房が中心となり関係省庁が連携した総合的な政策推進体制を確立することが重要である。特に、国境を越えて様々な事態が発生する可能性が高まることから、国際的な連携を強化する必要がある。

　また、情報システムの構築や通信サービスの提供や利用等、情報通信技術基盤の構築・提供・利用が民間分野において行われていることから、情報セキュリティ政策の推進にあたっては、官民それぞれの役割分担を明確にしつつ、官民連携の強化を図っていく必要がある。

　さらに、「事故前提社会」であるとの認識を共有するとともに、そのような社会に対する対応力を強化するため、持続的に情報セキュリティ対策の取

組を改善していく必要がある。そのためには、政府の取組の成果を可視化し評価した上で、継続的に取組を改善・向上させていく仕組みを確立していくことが重要である。

１　大規模サイバー攻撃事態への対処態勢の整備等

2009 年 7 月に米韓において発生したような大規模なサイバー攻撃事態が、今後我が国においても発生する可能性があること等を踏まえ、国民の生命、身体、財産又は国土に重大な被害が生じ、又は生じるおそれのあるサイバー攻撃事態（大規模サイバー攻撃事態）の発生時における対処態勢の整備、及び「重要インフラの情報セキュリティ対策に係る第２次行動計画」等に基づく官民情報共有体制を活用した平素からの情報収集・共有体制の強化を図る。

取組の推進に当たっては、未然防止等の観点から平素からの取組を行う部局と、大規模サイバー攻撃事態発生時の対処を行う部局との十分な連携を図り、総合的な対処に努める。

（１）対処態勢の整備

・　大規模サイバー攻撃事態における政府の初動対処態勢の整備

「緊急事態に対する政府の初動対処体制について（平成１５年１１月２１日閣議決定）」等に基づき、大規模サイバー攻撃事態が発生した際に政府及び関係機関が迅速かつ適切な初動対処をとるための態勢を整備する。併せて、大規模サイバー攻撃事態が発生した際の初動対処に係る訓練を実施する。

・　官民連携の推進

大規模サイバー攻撃事態における対処においては、重要インフラ事業者等からの協力が不可欠であることにかんがみ、官民が緊密に連携できるよう、重要インフラ事業者等の理解と協力の促進に努める。

・　サイバー攻撃に対する防衛分野での体制の強化

諸外国において戦力強化が必要とされる分野としてサイバー空間が取り上げられていること等を踏まえ、防衛分野におけるサイバー攻撃対処能力の強化を図る。

・ サイバー犯罪の取締り

デジタルフォレンジックの活用や国際的な捜査機関協力の推進を通じ、サイバー犯罪の取締りを推進する。

・ サイバー攻撃への対処に係る国際連携の強化

サイバー攻撃等に係る情報交換、国際会議等への積極的な参加を通じ、国際連携の強化を図る。

（２）平素からの情報収集・共有体制の構築・強化

・ 対処に資する情報の収集・分析・共有体制の強化

内閣官房と各省庁との間において、サイバー攻撃事態への対処に資する情報の収集・分析・共有体制を強化する。

・ サイバー攻撃等に関する諸外国等との情報共有体制の構築･強化

諸外国の関係機関･国際組織と内閣官房及び関係省庁との間において、サイバー攻撃事態への対処に資する情報の共有体制の構築･強化を図る。

２　新たな環境変化に対応した情報セキュリティ政策の強化

（１）国民生活を守る情報セキュリティ基盤の強化

①　政府機関等の基盤強化

・ 最高情報セキュリティ責任者（ＣＩＳＯ）の機能強化

最高情報セキュリティ責任者（ＣＩＳＯ）連絡会議の設置や最高情報セキュリティ・アドバイザー連絡会議の設置等を通じて、各省庁のＣＩＳＯの機能強化を図る。また、各府省庁のＣＩＳＯが情報セキュリティ報告書を作成し、公表を行うことにより、自ら問題意識を持って情報セキュリティ対策の改善を図る。

・ 政府横断的な情報収集・分析システム（ＧＳＯＣ）の充実・強化

2008 年度に本格運用を開始し政府機関情報システムの２４時間監視を行っているＧＳＯＣについて、緊急時における連絡体制や関係連携機関との連携強化等による情報収集能力、攻撃等の分析・解析能力強化等により、政府全体としてサイバー攻撃等に対する緊急対応能力を向上させる。

（注） GSOC: Government Security Operation Coordination team

・　政府機関情報システムの効率的・継続的な情報セキュリティ対策の向上

　政府機関のサーバ集約化等を通じて、情報システムのスリム化や運用効率化を一層推進し、情報セキュリティ対策の向上・効率化を図る。また、各省庁の情報セキュリティ対策の評価を通じて、取組の持続的な改善を図る。

・　政府機関における安全な暗号利用の推進

　政府機関で使われている電子政府推奨暗号について、移行指針に従って暗号の着実な移行を進める。また、電子政府推奨暗号の安全性を継続的に監視・調査し、安全性が低下した暗号については速やかに代替となる暗号への移行を進めるための計画を策定するとともに、急激な安全性の低下に備え、あらかじめ緊急避難的な対応（コンティンジェンシープラン）を検討する。

・　クラウドコンピューティング技術における情報セキュリティの確保等

　情報システムの統合・集約化等を可能とするクラウドコンピューティング技術について、電子行政へ効率的に活用するため必要となる情報セキュリティ確保方策を検討する。

　また、先進的なセキュリティ対策事例を踏まえ、政府機関においてもテレワークの環境整備を推進する。

・　政府機関の情報セキュリティ対策のための統一基準の見直し

　現行の政府機関統一基準の定着を図るとともに、情報通信技術や環境の変化を踏まえ、政府機関統一基準の見直しを適時に行い、新たな情報セキュリティ上の脅威に対応する。

・　政府機関情報システムに情報セキュリティ対策が適切に組み込まれる仕組みの構築

　情報システムに係る政府調達について、企画段階から情報セキュリティ対策を適切に組み込む方策を検討し、情報システムに組み込むべき情報セキュリティ要件を定める。

　また、情報セキュリティに係る評価・認証取得が必要となる情報セキュリティ要件の明確化を図ること等により、当該評価・認証を受けた製品の活用が促進されるよう取り組む。

・　社会保障・税の共通番号制に対応した情報セキュリティ対策の検討

　社会保障・税の共通番号制の検討に際し、プライバシーポリシーの下で適切な情報セキュリティ対策が講じられるよう、課題の抽出及び解決方策の検討を行う。

・　地方公共団体、独立行政法人等における情報セキュリティ対策の促進

　政府機関統一基準等の見直し等を行うとともに、地方公共団体、独立行政法人等における情報セキュリティ対策の一層の推進を図る。

②　重要インフラの基盤強化

　重要インフラの関係主体は、「重要インフラの情報セキュリティ対策に係る第２次行動計画」に基づいて、重要インフラサービスの維持に努め、また、ＩＴ障害発生時の迅速な復旧等を確保することに努めることとする。これに加え、最近の環境変化を踏まえ、国民生活に重大な影響を及ぼすおそれのある重要インフラに対する情報セキュリティ上の脅威に的確に対応する。

（「分野横断的な官民連携体制」の強化）

　各重要インフラサービスの情報通信技術に対する依存性が高まり、重要インフラサービスにおける情報セキュリティ上の脅威も高度化、多様化していること等を踏まえ、官民の役割分担を明確にした上で、官民の緊密な連携の下、重要インフラ分野の情報セキュリティ対策を強化するため、以下の事項に重点的に取り組む。

・　情報共有体制の強化

　重要インフラにおける情報セキュリティ対策に資する情報共有体制を強化するため、これまでに整備された官民の役割分担に基づき、情報提供、情報連絡等に必要な環境整備等を実施する。

・　「セプターカウンシル」の活動促進

　各重要インフラ事業分野における横断的な情報セキュリティに関する情報共有、分析体制の充実・強化に向けて、「セプターカウンシル」の活動を促進する。

・　「安全基準等」の整備浸透

　社会経済動向の変化等に対応し、また新たな知見を適時反映していくとともに、重要インフラ分野及び重要インフラ事業者等の「安全基

準等」整備浸透を推進するため、「安全基準等」策定指針の分析・検証を行い、継続的な改善を図る。

・　重要インフラ防護対策の向上

　重要インフラ各分野における脅威の分析や分野横断的演習の継続的な実施を通じて、重要インフラ事業者等の情報セキュリティ対策を向上させ、重大なＩＴ障害等が発生した場合においても、その被害が局所化・最小化されるよう促す。

　また、被害があった場合でもサービス提供が維持できるよう、制御システムを含め、システムの堅ろう化等について検討する。

・　事業継続計画（ＢＣＰ）の充実

　重要インフラ事業者等において作成されつつある事業継続計画に関し、想定される情報セキュリティ上の脅威（大規模なサイバー攻撃、地震、疾病等）を踏まえ、災害対策等と調和する情報セキュリティ対策の在り方について、関係機関等と連携し検討する。

・　重要インフラ分野における国際連携の推進

　ＭＥＲＩＤＩＡＮ（重要情報インフラに関する国際会合）等の国際会合を利用して、各国のベストプラクティスに関する情報の共有や活用、国際的な演習への参加等を通じた、重要インフラ分野における国際連携を促進する。

③　<u>その他の基盤強化</u>

・　マルウェア対策等の充実・強化等

　マルウェアへの感染対策等を強化するため、情報セキュリティインシデントへの対応能力の維持・向上や利用者への普及・啓発といったコンピュータ等の情報セキュリティ対策を強化するとともに、情報セキュリティ脅威の収集解析システム等の充実や、利用者・ＩＳＰ等への情報提供を通じたネットワーク等の情報セキュリティ対策を強化する。加えて、国際的な連携を推進する。

　また、マルウェア対策としての検体解析等を行う際のリバースエンジニアリングやダウンロードの適法性を明確化するための措置を速やかに講じる。さらに、脆弱性関連情報の速やかな流通により、不正アクセス等の未然防止に引き続き取り組む。

・　クラウドコンピューティング化に対応した情報セキュリティ確保方策、標準化

　クラウドコンピューティングを利用したサービスを構築・運用・利用するための情報セキュリティ要件に関するガイドライン、クラウドコンピューティング技術の適用が見込まれる分野毎の情報の取扱い等に関するガイドライン等を検討、策定する。

・　IPv6 対応に関する情報セキュリティ確保方策

　IPv6 対応における情報セキュリティ上の課題に適切に対応するため、検証環境の活用等により、具体的な情報セキュリティ課題の抽出や人材育成等を実施し、円滑な移行を図る。

・　情報家電、モバイル端末、電子タグ、センサーネットワークの情報セキュリティ確保方策

　情報家電、モバイル端末、電子タグ、センサー等あらゆるものがネットワークに繋がった場合の情報セキュリティの確保方策として、開発者に対する検証ツールや安全性評価体制の整備等の環境整備・技術課題の解決を図るとともに新たな利用指針等を検討する。

・　医療、教育分野等における情報セキュリティ確保方策

　医療、教育分野等において、医療・教育機関、国民等が安全・安心に情報通信技術を活用するためのガイドラインの充実等情報セキュリティ対策の推進方策について検討する。

・　中小企業に対する情報セキュリティ対策支援

　中小企業に対し、高度な情報セキュリティが確保された戦略的な情報通信技術投資を促進するための環境整備や、独立行政法人や関係機関等を活用し、情報セキュリティに係る情報提供、相談窓口の提供等の支援を行う。

・　安全な電子商取引の推進

　クレジットカード情報等の保護のため、国際標準を踏まえた情報セキュリティ対策を推進し、電子商取引を行うウェブサイトについて、情報セキュリティ基準の策定やその準拠を推進するとともに、新たな情報漏えい防止対策等を検討する。

・　知的財産保護の推進

企業等の知的財産を適切に保護するため、「知的財産推進計画 2010」（2010 年 5 月策定予定）に基づき、インターネット上の著作権侵害コンテンツ対策の推進、模倣品・海賊版拡散防止条約（ＡＣＴＡ）交渉の妥結を通じ、世界に知的財産保護の輪を広げる。

④　内閣官房情報セキュリティセンター（ＮＩＳＣ：National Information Security Center）の機能強化

・　ＮＩＳＣの総合調整機能の強化

ＮＩＳＣにおいて、情報セキュリティに関する高度な情報収集や分析機能の強化を実施し、専門性の向上を図るとともに、官民連携を強化する。

（２）国民・利用者保護の強化

①　普及・啓発活動の充実・強化

国民・利用者がＩＴリスクを認識し、自ら情報セキュリティ対策を実施することを促すため、普及・啓発活動を強力に推進する。2010 年 2 月から、新たに２月を「情報セキュリティ月間」として定め、普及・啓発を強化したところであるが、更なる充実強化を図るため、「包括的な普及・啓発プログラム」を策定する。

②　情報セキュリティ安心窓口（仮称）の検討

国民・利用者の情報セキュリティ水準を向上させるための活動を行う地域 NPO 法人等の支援を行うとともに、国民・利用者からの情報セキュリティに関する相談を受け付けるため、既存の枠組みも活用しつつ、「情報セキュリティ安心窓口（仮称）」の設置を検討する。

③　個人情報保護の推進

・　プライバシー保護技術の適切な利用促進

大規模な個人情報漏えいを防止する観点から、アクセス権の設定、認証情報の管理、暗号化、匿名化等のプライバシー保護技術の適切な利用を促進する。

・　各事業分野ごとの個人情報保護に関するガイドラインの見直し

企業から個人情報等の情報の漏えいを防止する観点から、情報の適切な暗号化等を促進するため、漏えいした個人情報に適切な技術的安

全管理措置が施されていた場合の手続の簡略化等、各事業分野の特性を踏まえつつ、事業者に暗号化等を行うインセンティブを付与するための見直しを行う。

・　国際的なフレームワークへの対応

　個人情報の国際的な流通が適切かつ安全な形で行われることを促進するため、ＯＥＣＤ（The Organizations for Economic Cooperation and Development）をはじめとして、ＡＰＥＣ（Asia-Pacific Economic Cooperation)、ＥＵ（European Union）等様々な場で進められている国際的な取組を踏まえ、プライバシー保護に関する越境執行協力等、国際的な協調を図っていくとともに、我が国の法制度についても国際的な理解を求め、データプライバシー保護に係る諸外国の制度と我が国の法制度との整合性に留意しつつ、我が国として必要な対応を検討する。

・　個人情報保護法の見直し

　個人情報保護法について、法改正も視野に入れた問題点についての審議を踏まえ検討を行う。

④　<u>サイバー犯罪に対する態勢の強化</u>

・　犯罪取締りのための基盤整備の推進

　サイバー犯罪の取締り体制の強化を図るとともに、デジタルフォレンジックを活用したサイバー犯罪の取締り、国際協調の推進等の基盤強化を推進する。

　さらに、原因特定や犯行過程解明に不可欠な情報提供がなされ、被疑者の検挙や被害の拡大防止につなげられるよう、法執行機関と被害者等との間の良好な協力関係の構築を一層推進するなど、犯罪に強い社会構築のための官民連携に向けた取組を推進する。

・　犯罪抑止のための広報啓発の推進

　サイバー犯罪抑止を図るため、国民一人一人が自らサイバー犯罪から身を守るという意識を高めるための、情報セキュリティに関する講習等の啓発活動を強力に推進する。

（３）国際連携の強化

① 米国、ＡＳＥＡＮ(Association of South East Asian Nations)、欧州等との連携強化（二国間、ＡＳＥＡＮとの関係強化）

日米サイバーセキュリティ会合や日ＡＳＥＡＮ情報セキュリティ政策会議等の開催を通じ、政策面における海外との連携を戦略的に強化するとともに、情報セキュリティ対策セミナーの開催等の海外ＣＳＩＲＴ(コンピュータセキュリティ緊急対応チーム)の構築支援等、実務面におけるネットワークの構築を図る。

また、従来の取組に加え、インターネットが急速に普及している国々の状況も踏まえつつ、新たな二国間関係の構築等に努める。

② ＡＰＥＣ、ＡＲＦ(ASEAN Regional Forum)、ＩＴＵ(International Telecommunications Union)、ＭＥＲＩＤＩＡＮ、ＩWWN (International Watch and Warning Network)等国際会合を活用した情報共有体制等 の強化

ＡＰＥＣ、ＡＲＦ、ＩＴＵ、ＭＥＲＩＤＩＡＮ、ＩWWN、ＦＩＲＳＴ(Forum for Incident Response and Security Teams)、ＡＰＣＥＲＴ(Asia Pacific Computer Emergency Response Teams)等、様々な分野の国際会議に積極的に参加し、外国機関等との情報共有体制を強化する。

③ ＮＩＳＣの窓口機能の強化

ＮＩＳＣは、横断的な情報セキュリティ問題に関する国際ＰＯＣ(Point of Contact)として、各国の情報セキュリティに関するベストプラクティスの共有､各国の重要インフラの情報セキュリティ対策等を含む情報セキュリティ政策全般について､諸外国等の関係機関との連携を強化する。

（４）技術戦略の推進等

① 情報セキュリティ関連の研究開発の戦略的推進等

米国等の動向も踏まえ、情報セキュリティに係る研究開発を戦略的に推進するため、新たな情報セキュリティ研究開発戦略を策定する。

インターネットを始めとする情報通信技術を利用者が活用するにあたっての脆弱性の克服や、IPv6 や、クラウドコンピューティング、情報家電、携帯端末、センサーネットワーク等の情報通信技術の環境の変化に対応した情報セキュリティ技術の開発、高度化・多様化する攻撃等に対応できる情報セキュリティ技術（「グランドチャレンジ型」研究開発・

技術開発）の実現・普及の実現を目指す。また、情報セキュリティ脅威の実態を踏まえた、システム設計管理対策の強化・普及を図る。

② 情報セキュリティ人材の育成

一般利用者の情報セキュリティ水準を底上げするため、利用者の身近で情報セキュリティ対策をサポートできる人材を育成する。

また、共通的な人材評価・育成ツールを活用して、産学連携による実践的な人材育成手法等に基づく高度な情報セキュリティ人材を育成するとともに、このような人材を育成するためのモデル的なキャリアパスを策定、可視化し、普及等を図る。

また、情報セキュリティ人材の中長期的な確保メカニズムの確立も視野に入れつつ、幅広い分野における情報セキュリティ人材育成に係る工程表を策定する。

③ 情報セキュリティガバナンスの確立

事業継続計画（ＢＣＰ）の策定、情報セキュリティ監査の実施や財務システム等の業務システムの入れ替え時における情報セキュリティ確保を図るため、普及・啓発活動を通じ、情報セキュリティガバナンスが経営課題として位置付けられ、経営者の意識改革が行われることを促すとともに、新たなリスクマネジメント等に関する手法の導入において情報セキュリティが明確に位置づけられるような方策を推進する。

（５）情報セキュリティに関する制度整備

① サイバー空間の安全性・信頼性を向上させる制度の検討等

サイバー犯罪条約の早期締結に向けて必要な検討を進め、また、コンピュータウイルス関連の法改正等の法整備を推進するとともに、機微な情報へのアクセス権限を明確化するための方策や情報漏えい等を防止するための方策の検討等サイバー空間の安全性・信頼性を向上させる制度について積極的な検討を行う。

② 各国の情報セキュリティ制度の比較検討

情報セキュリティに関する国際連携・協調を推進するため、各国間の法制度等の相違について分析し、課題の抽出と連携方策の検討を行う。

別添

○ 用語集

用語	用語解説
サイバー空間	情報通信技術を用いて情報がやりとりされる、インターネットその他の仮想的な空間。
サイバー犯罪	インターネット等の高度情報通信ネットワークを利用した犯罪やコンピュータ又は電磁的記録を対象とした犯罪等の情報技術を利用した犯罪。
重要インフラ、重要インフラ事業者等	「重要インフラの情報セキュリティ対策に係る第２次行動計画」（第２次行動計画）において、「重要インフラ」とは、「情報通信」、「金融」、「航空」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む。）」、「医療」、「水道」及び「物流」の１０分野とされ、「重要インフラ事業者等」とは、上記１０分野に属する事業を営む者のうち、第２次行動計画別紙１の「対象となる事業者」に指定された者及びこれらの者から構成される団体とされている。
デジタルフォレンジック	不正アクセスや機密情報漏えい等コンピュータに関する犯罪や法的紛争が生じた際に、原因究明や捜査に必要な機器やデータ、電子的記録を収集・分析し、その法的な証拠性を明らかにする手段や技術の総称。
ボット	コンピュータを外部から遠隔操作するため、悪意を持って作成されたプログラムのこと。悪意を持った攻撃者がボットに感染したコンピュータを遠隔操作することによって、「迷惑メールの大量配信」、「特定サイトの攻撃」等の迷惑行為や、情報窃取等の被害がもたらされる。
マルウェア	コンピュータウイルス、ワーム、スパイウェア等の計算機及び利用者に害を与える悪意あるソフトウェアのこと。

第２次情報セキュリティ基本計画の進捗状況について

資料2

※2009年度～2011年度の3ヶ年計画。ITを安心して利用できる環境の構築を目指す。

政府機関・地方公共団体

「政府機関統一基準」等による
情報セキュリティ水準の確保

①政府機関統一基準の見直し（※）

概要

各府省が守るべき最低限の対策水準※を定め、情報セキュリティ水準の向上を図る。

（※　情報（データ）、ハードウェア（端末）、ソフトウェア、マネジメント（組織、人）等。）

今回見直し

対象機関に「消費者庁」を追加。

②対策実施状況報告

概要

各府省における政府機関統一基準に基づく対策実施状況※を把握し、必要な改善を勧告。

（※適切な情報の取り扱い、IDとパスワードの適切な管理などが実施されているか。）

結果

年度	2007	2008	2009
全府省庁平均実施率	93.4%	96.9%	98.1%

③重点検査

概要

重点的にセキュリティ対策を図るべき事項について対策状況の検査※を実施。

（※対象数：　①端末約55万台　②公開ウェブサーバ約800台　③電子メールサーバ約1,300台
※主な検査項目：不正プログラム対策、不正アクセス対策、情報保護対策等）

結果

2006年度から実施し、2009年度末で100%に改善された。

④サーバ集約化

概要

管理するサーバの台数を削減することにより、セキュリティの向上及び行政コストの削減を目指す。

見通し

2013年度末までに概ね半減達成の見通し。
・公開ウェブサーバ（約1,000→約　550）
・電子メールサーバ（約1,900→約1,000）

⑤情報セキュリティ報告書（※）

概要

従来のNISC主導の情報セキュリティ対策から、各府省庁の自主的な対策改善に転換するためのガイドライン。

今後の取組

・2009年度　総務省、経済産業省で試行的に作成
・2011年度　全府省庁にて作成、公表（完全実施）

重要インフラ

「重要インフラ行動計画」に基づく
官民連携による重要インフラ防護

①安全基準等策定の「指針」改定（※）

概要

各重要インフラ事業は、国が定めた安全基準等に従って運用。本「指針」は、重要インフラ10分野横断的な情報セキュリティ対策の基準を定めたもの。

●情報通信　●金融　●航空　●鉄道
●電力　●ガス　●行政サービス
●医療　●水道　●物流

主な改正点

・利用者視点から、IT障害発生時における利用者への情報提供、新型インフルエンザ等の新たな脅威への対応を盛り込み。

安全基準等の浸透状況等に関する調査

重要インフラ事業者等を対象に、「内規」を含む情報セキュリティ対策の状況の客観的把握。

（2009年度調査）
内規の制定率は、約9割。一方、演習・訓練の未実施は3割強。

②IT障害波及の最小化

重要インフラ各分野に共通する脅威を分析するなど、IT障害波及の最小化を図る。

（1）共通脅威分析

概要

重要インフラ事業者に共通に存在する情報セキュリティの脅威を分析。

平成21年度の取組

重要インフラ分野間で共通に存在する脅威を抽出し、サイバー攻撃による脅威、運用・管理体制における脅威など5つの要素に分類・整理。

（2）分野横断的演習

概要

重要インフラ事業者のIT障害対策における課題を抽出するため、分野横断的な演習を実施。


平成21年度の取組

電力途絶に関する演習を実施し、情報システムの稼働継続に係わるBCPについて、非常用発電機等の燃料、機器の冷却水、要員の確保等の重要性を確認。

③情報共有体制の強化

関係者間での情報共有に必要な環境を整備するとともにセプターカウンシル（重要インフラの各分野により構成される共助活動の場）等の活動を充実。

企業・個人

普及啓発の推進

「情報セキュリティ月間」の実施

概要

本年から、新たに2月を「情報セキュリティ月間」と制定。

取組

① 官房長官からのメッセージの発信

②セミナー等関連行事の開催

③ NISCウェブサイトにおける情報提供

国際連携・協調

①日米サイバーセキュリティ会合

概要

2010年3月、日米における情報セキュリティに関する取組みについて実務者レベルで情報交換を実施。

②日・ASEAN情報セキュリティ政策会議

概要

日・ASEAN地域における情報セキュリティ水準の向上を図るため、第2回会合を2010年3月に実施。

情報セキュリティ政策の評価

評価の「枠組み文書」の見直し（※）

概要

第2次基本計画の内容に基づき、評価の方針、評価指標等の見直しを実施。

※は今回の決定・了解案件