報道発表
内閣官房 ンター(NI
活動内容
基本戦
国際戦
政府機 ーム
事案対
重要イ
会議
調査研究
関連サイ
関連法令

第1次情報セキュリティ基本計画

第3章　今後3年間に取り組む重点政策－「新しい官民連携モデル」の構築－

IT社会を構成するあらゆる主体が、前章に示した適切な役割分担の下で、「ITを安心して利用可能な環境」を構築するため、政府は、今後3年間、以下の重点政策に総合的に取組み、「新しい官民連携モデル」を構築する。

また、ここで示した政策の方向性に従い、政府は、毎年度、より具体的な施策の実施プログラムを「年度計画」として策定し、本基本計画の実現を図る。

第1節　対策実施4領域における情報セキュリティ対策の強化

第2章第1節で示したように、本基本計画においては、我が国全般の情報セキュリティ基盤の強化策を総合的に講じていくにあたり、対策を実際に適用し実施する主体の領域を、(1)政府機関・地方公共団体、(2)重要インフラ、(3)企業、(4)個人の4領域に分け、その対策のあり方を検討することが有効であるとの立場に立っている。政府は、この対策実施4領域について、前章第1節で示したそれぞれの役割に応じた対策を促進するための政策に、総合的に取り組んでいくことが必要である。

(1)政府機関・地方公共団体

政府機関においては、第2章第1節で示したように、国内外及び官民における「ベストプラクティス(模範例)」を積極活用した対策を実行し、常に最高水準の情報セキュリティ対策レベルを維持していくことが必要であり、また、地方公共団体においては、政府機関の取組みも踏まえながら情報セキュリティ対策の強化を図ることが必要である。

しかしながら、現在の状況を見ると、政府機関においては、情報セキュリティ水準に格差がある、特に内部からの脅威に対して脆弱である、緊急対応及び事業継続の観点からの取組みが不足している、年々複雑化する情報セキュリティ問題に対応するための高度な専門知識を有する人材が不足しているという問題を抱えている。また、地方公共団体においては、IT障害や情報漏洩などへの対策が徹底されておらず、また、地方公共団体間の情報共有体制が十分に構築されていないという問題を抱えている。

したがって、政府は、1)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2)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し、地方公共団体については、1)2006年9月を目処に地方公共団体における情報セキュリティ確保に係るガイドラインの見直しを行うとともに、情報セキュリティ監査や研修等の対策を推進すること、また、2)2006年度末までに地方公共団体間の情報共有体制が整備されることを目指し、今後3年間に、主に以下の政策に重点的に取り組んでいくこととする。

ア　政府機関

[1]政府機関統一基準とそれに基づく評価・勧告によるPDCAサイクルの構築

政府機関の情報セキュリティ対策の水準を世界最高のものとするため、政府機関統一基準について、技術や環境の変化を踏まえ、毎年その見直しを行うものとする。

また、各政府機関の情報セキュリティ対策の実施状況を、政府機関統一基準に基づき、必要な範囲で検査・評価し、勧告を通じた各政府機関の対策の改善と政府機関統一基準等の改善に結びつけることで、政府全体としてのPDCAサイクル(Plan・Do・Check・Actサイクル)を確立する。なお、評価の結果については、情報セキュリティの維持・確保にも配慮しつつ公表することとする。

さらに、政府機関の対策の内容・経験及びその他の知識は、民間企業、地方公共団体、独立行政法人等にとっても参照すべき価値のあるものであることが望まれるため、「ベストプラクティス(模範例)」として、これらの知識を分かりやすい形で公開し、その普及に努める。また、外部委託先の情報セキュリティ対策の水準の確保の観点についても十分に留意する必要がある。

[2]独立行政法人等のセキュリティ対策の改善

政府機関統一基準を踏まえ、独立行政法人等の情報セキュリティ水準の向上を促進する。特に、これまで情報セキュリティポリシーを策定していない独立行政法人等については、情報資産及びリスクの状況等、各法人の実情を踏まえつつ、情報セキュリティポリシーの策定を行い、また策定されている独立行政法人等については、ポリシーの見直しを行う等の改善を図る。

[3]中長期的なセキュリティ対策の強化・検討

情報セキュリティに関する要求仕様の共通化、年度途中での緊急事態対応に向けた取組み等、以下のような、政府機関が全体として協力して行うべき情報セキュリティ対策の実施を図る。

(ア)最適化対象の府省共通業務・システム及び一部関係府省業務・システムの開発との連携

府省共通業務・システム及び一部関係府省業務・システムの最適化において、新たに開発(導入)するシステムについては、政府機関統一基準等との連携を図りつつ、情報セキュリティ機能の明確化等を通じて、情報セキュリティに関する要求仕様の共通化、信頼性の高い製品等の利用等を推進する。

(イ)セキュリティ強化に資する新規システム(機能)の導入検討とその実現

次世代の電子政府構築に向けて、政府全体の業務・システムの基盤となる共通的なプラットフォームの構築・整備について検討等を行うことが重要である。そのプラットフォームについてセキュリティ強化を図るため、IPv6、国家公務員身分証ICカード、暗号、電子署名、生体認証等の新規システム(機能)の導入について総合的な検討等を行い、その実現を推進す

る。
特に、今後、すべての政府機関の情報システムがIPv6を早期に利用できるようにするため、原則として2008年度までに、各府省の情報システムの新たな開発（導入）又は更改に合わせて、情報通信機器やソフトウェアのIPv6対応化を図る。

（ウ）政府機関への成りすましの防止
悪意の第三者が政府機関に成りすまし、一般国民や民間企業等に害を及ぼすことが無いよう、正統な政府機関であることを容易に確認可能とするため、電子証明書の広範な活用や、政府機関のドメインであることが保証されるドメイン名の利用を推進する。

（エ）政府機関における安全な暗号利用の促進
電子政府の安全性及び信頼性を確保するため、電子政府で使われている推奨暗号について、その安全性を継続的に監視・調査するとともに、技術動向及び国際的な取組みを踏まえ、暗号の適切な利用方策について検討を進める。

[4]サイバー攻撃等に対する政府機関における緊急対応能力の強化
サイバー攻撃等への迅速かつ適切な緊急時の対応及び技術や環境の変化への適応を実現するために、政府内において迅速に情報を共有し、統一的に情報を分析し、適切な対策を講ずることができる体制を構築するとともに、対処を行う関係機関の能力を向上させ体制を整備し、過去の緊急時等の対応から得られた知見を政府機関統一基準等の改善や政府における人材育成等に取り入れるなどにより、緊急対応能力を強化する。

[5]政府機関における人材育成
政府として情報セキュリティ対策を一体的に進めていくために、必要な知見や専門性を有する人材を育成・確保することが重要であることにかんがみ、政府機関における情報システム管理部門の担当職員の育成、情報セキュリティに関する専門性の高い人材の活用、教育機関と連携した人材育成の取組み、幹部職員・一般職員の意識の向上方策等を推進する。なお、政府機関の情報システム管理部門において、情報セキュリティ対策業務に携わる専門的職員については、全員が情報セキュリティに関する資格を保有することを目指す。

イ　地方公共団体

[1]情報セキュリティ確保に係るガイドラインの見直し等
地方公共団体における情報セキュリティ確保に係るガイドラインの見直し等を行うとともに、各地方公共団体における当該ガイドライン等を踏まえた対策の実施を推進する。

[2]情報セキュリティ監査実施の推進

各地方公共団体が講じる情報セキュリティ対策について、その実効性の評価・見直しによる継続的な対策レベルの向上に資するため、情報セキュリティ監査の実施を推進する。

[3]「自治体情報共有・分析センター」(仮称)の創設促進

地方公共団体におけるIT障害の未然防止、拡大防止・迅速な復旧及び再発防止に資するとともに、地方公共団体全体のセキュリティレベル向上を図るため、地方公共団体における情報セキュリティに関する情報の収集・分析・共有や政府等から提供される情報の共有等を行う機能を有する「自治体情報共有・分析センター」(仮称)の創設を促進する。

[4]職員の研修等の支援

上記のほか、高度な技術の開発・導入や職員の研修等について支援を行い、地方公共団体のセキュリティ強化を図る。

(2)重要インフラ

重要インフラにおいては、第2章第1節で示したようにそのサービスの安定的供給が最優先課題であるという面から、各事業において発生するIT障害が国民生活・社会経済活動に重大な影響を及ぼさないよう対策を実施することが必要である。しかしながら、現在の状況を見ると、サイバー攻撃等意図的要因に起因する障害以外のIT障害への対策についての検討が不足しており、官民の情報共有体制が十分に構築されていない等の問題を抱えている。したがって、政府は、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し、今後3年間に、主に以下の政策に重点的に取り組んでいくこととする。なお、重要インフラの情報セキュリティ対策については、「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)が別途定められており、本行動計画に従って、より具体的な対策に取り組んでいくこととする。

[1]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」の整備

「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」を踏まえ、それぞれの重要インフラ事業分野ごとに、必要な又は望ましい情報セキュリティ対策の水準について、「安全基準等」に明示することを目標とする。さらに、指針については1年ごと及び必要に応じて適時見直すこととし、「安全基準等」については、情報セキュリティを取り巻く環境の変化に応じ、随時見直しを行う。

[2]情報共有体制の強化

IT障害に関する情報について、1)IT障害の未然防止、2)IT障害の拡大防止・迅速な復旧、3)IT障害の要因等の分析・検証による再発防止の3つの側面から、政府等は重要インフラ事業者等に対し適宜・適切に提供し、また重要インフラ事業者等間並びに相互依存性のある重要インフラ分野間においてはこれら情報を共有する体制を強化する。

(ア)官民の情報提供・連絡のための環境整備

関係機関と連携し、注意喚起等、各重要インフラ事業者等の対策に資するものとして、重要インフラ事業者等に提供する情報の収集を行い、CEPTOAR(後述)等を通じて、情報を提供する。

また、重要インフラ事業者等が、法令等で報告が義務づけられている事故、障害、業務遅延等のほか、特異重大なものとして重要インフラ事業者等が連絡を要すると判断した情報を政府に連絡するための環境の整備を促進する。

(イ)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

IT障害の未然防止、発生時の被害拡大防止・迅速な復旧及び再発防止のため、政府等から提供される情報について、適切に重要インフラ事業者等に提供し、関係重要インフラ事業者等間で共有することにより、各重要インフラ事業者等のサービスの維持・復旧能力の向上に資するため、各重要インフラ分野内に「情報共有・分析機能」(CEPTOAR: Capability for Engineering of Protection, Technical Operation, Analysis and Response)の整備を促進する。

(ウ)「重要インフラ連絡協議会(CEPTOAR－Council)」(仮称)の創設促進

重要インフラ事業者等において、分野横断的な情報共有の推進を図り、多様な知見をサービスの維持・復旧に活かしていくため、各CEPTOAR間での横断的な情報共有の場として「重要インフラ連絡協議会(CEPTOAR－Council)」(仮称)の創設を促進する。

[3]相互依存性解析の実施

我が国全体としての重要インフラ対策の向上に向けた、分野横断的な状況の把握のため、それぞれの重要インフラに起こりうる脅威が何であるかを把握するとともに、ある重要インフラにIT障害が生じた場合に、他の重要インフラに、いかなる影響が波及するかという相互依存性の把握を行う。

[4]分野横断的な演習の実施

想定される具体的な脅威シナリオの類型をもとに、各重要インフラ所管省庁、各重要インフラ事業者等、各重要インフラ分野のCEPTOAR等の協力の下に、重要インフラ横断的な演習を行う。演習を通じ、安全基準等、情報共有体制、情報共有・分析機能、相互依存性解析等の各施策の実効性・妥当性を定期的に、かつ、段階的に、検証する。また、この演習やその他の訓練、セミナー等を通じて、重要インフラ所管省庁及び重要インフラ事業者等を中心に、高度なITスキルを有する人材を育成し、確保する。

(3)企業

企業においては、第2章第1節で示したように、グローバル社会における経済発展の担い手であると同時に、ITの根幹を担う製品・サービス等を提供する主体でもあるという面から、対策を実施することが必要である。しかしながら、現在の状況を見ると、企業におけるセキュリティ対策が市場評価に十分に繋がっていない、企業における情報セキュリティ人材の確保・育成が十分でないという問題を抱えている。したがって、政府は、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し、今後3年間に、主に以下の政策に重点的に取り組んでいくこととする。

[1]企業の情報セキュリティ対策が市場評価に繋がる環境の整備

社会的責任にも配慮したコーポレートガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用することを推進する。このため、情報セキュリティ対策ベンチマーク、情報セキュリティ報告書モデル及び事業継続計画策定ガイドラインの普及・改善を図るとともに、情報システム等の政府調達の競争参加者に対して、必要に応じて、これらの制度や第三者評価の結果等を活用した情報セキュリティ対策レベルの評価を入札条件等の一つとする。また、政府が推進する情報セキュリティに関する取組みについて、政府全体としての整合性を確保する。

[2]質の高い情報セキュリティ関連製品及びサービスの提供促進

情報セキュリティ対策は、本来業務を達成するために必要な機能とは異なる機能を、リスクに応じて講じていく性質のものであること、また、対策そのものを可視化しにくい特性等を持つことから、企業が情報セキュリティ対策を講ずる際には、理解のしやすい形で必要な対策を選択できる環境が整備される必要がある。このため、企業の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研究を推進するとともに、ITセキュリティ評価及び認証制度、情報セキュリティマネジメントシステム(ISMS)適合性評価制度、情報セキュリティ監査といった第三者評価の活用を推進することにより、質の高い情報セキュリティ関連製品及びサービスの提供が促進されることを図ることとする。

また、こうした第三者評価の審査等の効率化を図るとともに、質の高い情報セキュリティ関連製品等を活用する企業に対し、その投資を加速するためのインセンティブが与えられる環境の整備を促進する。

[3]企業における情報セキュリティ人材の確保・育成

企業においては、経営トップ等の情報セキュリティへの理解や企業内における情報セキュリティ人材が不足している。このため、企業の情報セキュリティ対策が市場評価に繋がる環境の整備を通じて経営トップ等の情報セキュリティへの理解を普及させるとともに、企業の情報システム担当者等に対する全国規模での広報啓発を推進する。また、各企業において情報セキュリティ対策を行っている担当者のモチベーションの維持のための取組みを促進する。

[4]コンピュータウイルスや脆弱性等に早期に対応するための体制

の強化

企業における情報セキュリティ問題に的確に対応するためには、情報関連事業者をはじめとする関係者間において、迅速な情報共有、対策の策定及び対策の普及を円滑に図る必要がある。このため、情報関連事業者等の自主的な協力を得ながら平時からの連絡体制を構築し、コンピュータウイルスや脆弱性等に早期に対応するための連携対応体制を強化する。

(4)個人

個人においては、第2章第1節で示したように、8000万人のインターネット利用者の情報セキュリティに対する理解が均一ではないという現状を認識し、老若男女を問わず各人がその状況に応じて情報セキュリティに関するリテラシーを向上させることを支援すべく、関係する各主体が様々な対策を実施することが必要である。しかしながら、現在の状況を見ると、個人が情報セキュリティを当たり前のこととして認識できる環境、また、一般個人にとってITの仕組みは理解しがたいにも関わらず、個人の自己責任の限界を補う環境が不足している、という問題を抱えている。したがって、政府は、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し、今後3年間に、主に以下の政策に重点的に取り組んでいくこととする。

[1]情報セキュリティ教育の強化・推進

初等中等教育からの情報セキュリティ教育や世代横断的な情報セキュリティ教育を推進する。

[2]広報啓発・情報発信の強化・推進

全国的規模での広報啓発・情報発信の継続的実施、ランドマーク的イベントの実施(「情報セキュリティの日」の創設等)、日常からの世論喚起・情報提供の仕組み(「情報セキュリティ天気予報」(仮称)の実施検討)の構築、我が国の情報セキュリティの基本戦略の国内外への発信を行う。

[3]個人が負担感なく情報関連製品・サービスを利用できる環境整備

情報関連事業者が、個人が高度な情報セキュリティ機能を享受しながら負担感なく利用できる製品やサービス(「情報セキュリティ・ユニバーサルデザイン」)を開発・供給する環境の整備を促進する。

- 第3章　第2節　横断的な情報セキュリティ基盤の形成
- 第1章　基本理念
- 第2章　「新しい官民連携モデル」の構築における各主体の役割と連携
- 第4章　政策の推進体制と持続的改善の構造