NISC NEWS
第３１号（２０１０年５月１４日発行）

内閣官房情報セキュリティセンター
National Information Security Center (NISC)

★目次

１．国民を守る情報セキュリティ戦略について
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

１．国民を守る情報セキュリティ戦略について

去る５月11日（火）に情報セキュリティ政策会議が開催され、「国民を守る情報セキュリティ戦略」が決定されました。

近年、重要インフラ等の国民生活に直結するサービスの提供において、情報通信技術への依存が高まっています。また、昨年七月に米国・韓国の政府機関等に対して大規模なサイバー攻撃が行われたように、情報セキュリティ上の攻撃手法が多様化・高度化しています。このため、国民生活に与える脅威は増大しており、情報通信技術の利用に係るリスク（ＩＴリスク）を克服することが必要になってきております。

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、今後四年間を対象として、既存の「第二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です。

戦略の基本的な考え方としては、

・　サイバー攻撃の発生を念頭に置いた政策強化・対処態勢の整備、
・　新たな環境変化に対応した政策の確立、
・　能動的な情報セキュリティ対策の推進、

としております。

これらの取組を通じて、ＩＴリスクを克服し、安全・安心な国民生活を実現し、世界最先端の「情報セキュリティ先進国」を実現したいと考えております。

具体的な取組内容については、

・　大規模サイバー攻撃事態への対処態勢の整備等
・　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

を大きな柱としております。

「大規模サイバー攻撃事態への対処態勢の整備等」については、大規模サイバー攻撃事態等への初動対処態勢の整備等を行うとともに、平素からの情報収集・共有体制を構築・強化を図ります。

「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」については、次の５分野の取組みを推進することとしております。

・　重要インフラ、政府、その他の分野において、国民生活を守る情報セキュリティ基盤を強化
・　普及啓発活動の充実・強化、情報セキュリティ安心窓口（仮称）の検討、個人情報保護の推進、サイバー犯罪に対する態勢の強化を通じ、国民・利用者保護を強化、
・　米国、ASEAN、欧州等との連携強化、APEC、ARF、MERIDIAN、IWWN 等の国際会合を活用した情報共有体制等の強化、ＮＩＳＣの窓口強化を通じ、国際連携を強化、
・　研究開発の戦略的推進、情報セキュリティ人材の育成や情報セキュリティガバナンスの確立、
・　サイバー空間の安全性・信頼性を向上させる精度の検討や各国の情報セキュリティ制度の比較検討の実施

としております。

概要資料、本文については、ＮＩＳＣホームページに掲載されておりますのでご覧下さい。

【資料】 http://www.nisc.go.jp/active/kihon/pdf/senryaku.pdf
http://www.nisc.go.jp/conference/seisaku/dai23/pdf/23siryou01.pdf

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２３回情報セキュリティ政策会議において、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いたしました。

(1)「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

・ 「消費者庁」を適用対象範囲に追加するなどの修正を踏まえた、政府機関統一基準（第 4 版）（平成 21 年度修正）が決定されました。

・ また、2009 年度に実施した以下の調査等を報告いたしました。

ー対策実施状況報告

・ 2009 年度は、前年度より改善が見られるが、業務継続計画と情報セキュリティ関係規程の不整合などの課題も存在。

・ 2010 年度に向けた取組としては、情報セキュリティ教育、トップマネジメントの強化、対策実施状況報告の改善・効率化。

ー重点検査

・ 端末・公開ウェブサーバ・電子メールサーバの対策実施状況について、2009 年度末で全府省庁において改善。

ー政府機関のサーバ集約化計画

・ 2013 年度末までに概ね半減が達成できる見通し。

※各府省庁においては、今年度より、情報セキュリティ報告書を作成し、能動的に情報セキュリティ対策に取り組んでいくことも決定いたしました。

(2)「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

重要インフラにおけるＩＴ障害が国民生活、社会経済活動に重大な影響を及ぼすことがないようにするため、官民の緊密な連携の下、次に掲げる情報セキュリティ対策の向上に係る取組を実施しました。

・ 「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」の第３版を決定しました。主な改正点は次のとおり。

・ 従来からの情報セキュリティ対策について、利用者視点から、ＩＴ障害発生時におけるサービス状況等の利用者への情報提供、また新型インフルエンザ等の新たな脅威への対応を盛り込んだ。

・ 従来からの全分野に亘る情報セキュリティ対策の底上げの観点から必要な対策に加えて、新たに個別の先進的な対策を取り込めるような記載とし、発展性を持たせた。

・ また、「安全基準等の浸透状況等に関する調査」を実施し、9 割の事業者が内規を制定しているが、一方、演習・訓練の未実施が 3 割強であるとの結果を得た。

・ ＩＴ障害波及の最小化のための取組として、「共通脅威分析」と「分野横断的演習」を実施しました。

・ 「共通脅威分析」では、重要インフラ分野間で共通に存在する情報セキュリティ上の脅威を抽出し、５つの要素に分類・整理した。

・ 「分野横断的演習」では、広域停電を想定し、情報システムの稼動継続に関わる BCP（事業継続計画）における非常用発電機の燃料、機器の冷却水、要員の確保等の重要性を確認した。

・ 情報共有体制の強化のための取組として、官民における情報共有に必要な環境整備を進めるとともに２００９年２月に設立されたセプターカウンシル（重要インフラ各分野により構成される共助・互恵の活動の場）の活動を支援することにより、その充実を図りました。

(3) その他の報告事項

・企業・個人への普及啓発の推進

本年から、新たに２月を「情報セキュリティ月間」と制定し、期間中にセミナー等関連行事を開催しました。

・国際連携・協調

第２回 日・ASEAN 情報セキュリティ政策会議がタイ・バンコクで開催され、日本は共同議長国として参加し、連携枠組みでの一致に貢献しました。

・情報セキュリティ政策の評価

・第２次基本計画の内容に基づき、評価の方針、評価指標等をまとめた「評価の枠組み文書」の見直しを実施しました。

詳しくは次をご参照ください。

【資料】http://www.nisc.go.jp/conference/seisaku/dai23/pdf/23siryou02.pdf

＜バックナンバー・配信先変更・配信中止＞
本メールマガジンにおけるバックナンバーの取得及び配信先の変更、配信の中止等は下記のURLから可能です。
http://www.nisc.go.jp/nisc-news/

＜御意見、御感想＞
http://www.nisc.go.jp/mail.html