報道資料

平成 24 年 5 月 30 日
内閣官房情報セキュリティセンター（NISC）

「政府機関における情報セキュリティに係る年次報告(平成 23 年度)」の決定等について

本日、第6回「情報セキュリティ対策推進会議（CISO 等連絡会議）」（議長：竹歳内閣官房副長官）が持ち回り開催され、以下のとおり報告・決定された。

各府省庁の平成 23 年度「情報セキュリティ報告書」の報告

各府省庁の「**情報セキュリティ報告書**」が、各府省庁の CISO から初めて**報告**された。

※本報告書は、各府省庁の最高情報セキュリティ責任者（CISO）が中心となって自ら取りまとめたものであり、今回、平成 23 年度版において初めて本格的に作成。

「政府機関における情報セキュリティに係る年次報告（平成 23 年度）」の決定

平成 23 年度の情報セキュリティに関する内外の動向、政府機関の取組、各府省庁の報告書の評価等について NISC が取りまとめ、本 CISO 等連絡会議において決定された。

（詳細については別添資料参照）

〔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（NISC）
内閣参事官　木本　裕司　電話　03－3581－3959

※　本会議の資料等は、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しております。
（各府省庁の情報セキュリティ報告書についても、一括して下記 URL によりご覧頂けます。）
http://www.nisc.go.jp/conference/suishin/index.html

情報セキュリティ報告書の概要

別添資料

■ **情報セキュリティ報告書の目的**

各府省庁の最高情報セキュリティ責任者が中心となり、自ら問題意識を持って、自組織の**情報セキュリティ対策の取組状況を国民へ公表**し、各府省庁の参考となる**ベストプラクティスを共有**するなどの取組を通じて、**能動的に情報セキュリティ対策の改善**を図る仕組みを各府省庁において実現する。

これまでの取組み

【平成21年度】

・ 情報セキュリティ報告書専門委員会において、情報セキュリティ報告書作成のためのガイドラインを策定。

・ 総務省及び経済産業省において、試行的に21年度の情報セキュリティ報告書を作成。

【平成22年度 】

・ 全府省庁において、情報セキュリティ報告書を**試行的に作成**。

平成23年度の取組状況

【主な取組】

・ 全ての府省庁において、情報セキュリティ報告書案を作成（復興庁を除く）

・ 最高情報セキュリティアドバイザー等連絡会議において、各府省庁が作成した報告書案に対する助言及び推奨事例候補を推薦

・ アドバイザー会議における意見等を踏まえ、各府省庁で必要な見直しを実施

・ 各府省庁で策定した報告書について、CISO等連絡会議に報告し、公表

情報セキュリティ報告書の基本構成

○ 最高情報セキュリティ責任者によるメッセージ及び23年度の総括	(1) 最高情報セキュリティ責任者によるメッセージ (2) 23年度の取組に対する評価及び24年度の目標
○ 23年度における重点的な取組	(1) 23年度の重点目標、取組実績及び評価 (2) 障害・事故等の再発防止状況
○ 情報セキュリティ対策の実施状況	(1) 自己点検結果（対策の実施率等） (2) 情報システムに関する技術的な対策状況 (3) 教育の企画、職員の受講状況、教育教材の整備等 (4) 外部委託の状況　等
○ 情報セキュリティに関する障害、事故等	(1) 事故等の概要及び対応状況 (2) 対応手順、訓練、職員向け注意喚起の状況等
○ 24年度の計画	(1) 24年度の実施計画

平成23年度における各府省庁の取組

体制の強化に関する取組

① CSIRT体制の充実と関係職員への研修・訓練の実施

② 首都直下型地震等の不測の事態に備えた情報システムに係る運用継続計画の策定

③ 重要業務の継続を確保する観点から、災害時対応情報システムの設置　等

教育・調達等に関する取組

①職員教育・意識啓発

・e-ラーニング研修における受講状況の確認、受講促進メールの送信
・知識、経験や役割に応じた教育教材の整備、理解度確認テストの実施
・情報セキュリティ関連資料をワンストップ化し、常に職員が閲覧できるようイントラネットに掲載

②調達・外部委託

・委託先における情報セキュリティ対策の実施を確保するための調達仕様書のひな形、手順書等の整備、対策の実施状況等の確認

③その他

・情報の格付及び取扱制限の表示フォームを自動付与する機能を導入
・全ての公開ウェブサーバについて脆弱性の有無に関する監査の実施及び対策のフォローアップ
・暗号化機能等を有するセキュアUSBメモリの導入、USBのデバイス管理の導入
・自己点検に関する監査対象の拡大、e-ラーニングシステム機能を活用した自己点検の自動化　等

政府機関における情報セキュリティに係る年次報告（平成23年度）の概要　1／2

「政府機関における情報セキュリティに係る年次報告（平成23年度）」：　各府省庁の情報セキュリティ報告書等を踏まえ、対策の実施状況等についてCISO等連絡会議で評価した報告書　　（CISO等連絡会議において決定後、公表）

国内外における情報セキュリティに関する動向

①巧妙化する攻撃手法

＊ 政府機関や民間企業への標的型攻撃の顕在化

＊ 内部ネットワークを経由した制御システム等への侵入

＊ 電子証明書の不正利用等、なりすましの高度化

＊ クラウドサービスへのDDoS攻撃の発生

②攻撃目的の多様化

＊ 愉快犯・技術力の誇示、社会的・政治的主張

＊ 金銭詐取、企業の内部情報の窃取・対外情報活動

＊ 社会的な混乱を目的としたテロリズム　等

③東日本大震災による情報システムへの影響

＊ 地震・津波・停電（計画停電含む）に伴う被害の発生

④海外の状況

＊ サイバー空間に対する戦略の策定、国際会議の開催

＊ ボットネットの閉鎖

＊ 情報交換、人材育成に関するカンファレンスの開催

⑤技術の進歩や利用環境の変化

＊ スマートフォン・タブレット端末の利用拡大

政府機関の取組（NISC）

＊赤字：重点取組事項

① 官民連携の強化を図るための対策の策定・実施

・国の重要な情報を扱う契約に係る情報セキュリティの確保

・CSIRT等の機能を有する体制の整備　　等

② 情報セキュリティに係る年次報告書の作成・公表

③ 新たな脅威や技術動向を踏まえた**政府機関統一基準群の見直し**

④ **標的型不審メール訓練の実施**（12省庁 約6万名の職員）

⑤ 公開ウェブサーバに対する**脆弱性検査の実施**（11省庁）

⑥ 政府機関から発信する**電子メールに係るなりすましの防止**

・DNSサーバへのSPFレコードの記録を推進

⑦ **東日本大震災における政府機関の情報システムに対する被害状況の調査・分析を実施**

・実施結果を踏まえ、情報システム運用継続計画ガイドラインを見直し

⑧ 暗号危殆化の危険度判定及び対応フローの決定　等

政府機関における情報セキュリティに係る年次報告（平成23年度）の概要　2／2

政府機関の取組に対する評価

① 対策の実施状況（自己点検結果）に関する評価

＊ 統一基準群を踏まえた**対策の実施率**：99．0%

＊ ただし、職員に対する**情報セキュリティ教育の実施**や**情報の作成・入手等に関する遵守事項**については、更なる対策の向上が必要

② 情報システムへの対策状況（重点検査結果）に関する評価

＊ OS及びサーバアプリケーションの**セキュリティアップデートの実施率**：100%

＊ **DoS攻撃対策等**について、更なる対策の向上が必要

平成23年度の取組における推奨事例

□ 障害・事故等が発生した場合を想定した**支援体制の充実**
（CSIRT体制の充実）

□ 情報セキュリティ関連資料の**ワンストップ化(イントラ掲載)**

□ **課室**における情報管理に係る**運用手続き等の検討・策定**

□ **不審メール受信時の対策の強化**
・不審メール情報とフリーメールとの照合による注意喚起
・メールフィルターによる不確かなメールの注意喚起

平成24年度に取り組むべき政府機関の課題

① 情報セキュリティに関する動向を踏まえた課題

＊ 巧妙化している標的型攻撃に対応するための**体制の整備**
（CSIRTや協力支援体制の構築、研修・訓練の実施）

＊ **スマートフォン**に対する**情報セキュリティ対策の強化**
（個人情報等への脅威、BYODの利活用を踏まえた対策）

＊ **利用環境の変化に対応**した情報セキュリティ対策の強化
（共通利用基盤システム等に係るセキュリティ水準の確保）

＊ **安全な暗号利用の促進**
（安全性の高い暗号アルゴリズムへの着実な移行）

② 平成23年度の政府機関の取組を踏まえた課題

＊ 情報システムの**運用継続に向けた対策の促進**
（優先的に取り組むべき対策を検討し、速やかに実施）

＊ **公開ウェブサーバの脆弱性検査**を引き続き、実施
（危険度高の脆弱性が確認されており、全体の底上げ）

＊ **標的型不審メール対処訓練**の継続的な実施
（より巧妙化が予想されることから、訓練手法を改善）

＊ 設計段階における**セキュリティ要件の精緻化**
（SBDマニュアルの利便性向上、普及促進）

＊ **なりすまし防止対策**の更なる推進
（DKIM、S/MIME等の暗号技術を利用した対策の検討）

年次報告の基本構成

第1章　平成23年度の情報セキュリティに関する動向と政府機関の取組	第1節　国内外における情報セキュリティに関する動向 第2節　政府機関に向けたNISCの取組
第2章　政府機関の取組の評価	第1節　各府省庁における取組の概況 第2節　対策実施状況報告の評価 第3節　重点検査の評価
第3章　平成23年度における重点取組事項	第1節　標的型不審メール対処訓練 第2節　なりすまし防止策の実施状況 第3節　公開ウェブサーバの脆弱性検査 第4節　東日本大震災における情報システムへの影響及び今後の対策 第5節　各府省庁における主な取組事例（推奨事例）
第4章　平成24年度に取り組むべき政府機関の課題	①情報セキュリティに関する動向を踏まえた課題 ②政府機関における取組の評価結果を踏まえた課題