平成２３年度
内閣官房情報セキュリティ報告書

平成２４年５月

内閣官房

目　次

１　はじめに

最高情報セキュリティ責任者からのメッセージ

国民の安全、安心及び信頼の下に電子政府を構築するため、内閣官房はその一員として、適切な情報セキュリティ対策を実施し、継続的かつ安定的な行政事務に資することを基本方針としています。特に、内閣官房は内閣の直属の機関として、他の府省庁以上に秘匿性の高い情報を扱うことから、高度な情報セキュリティ対策を講じる必要があります。

そのため、内閣官房においては、内閣官房の特性を踏まえた情報セキュリティ教育、サイバー攻撃に関する情報の入手・分析等を行い、それらに対応する最新の情報に基づく注意喚起を行うなど情報セキュリティ対策を実施してきました。

しかしながら、平成２３年度においては、標的型攻撃メールの受信や一部のＷｅｂサイトの改ざんといった、内閣官房がサイバー攻撃のターゲットにされていることが明らかとなる事象が散見されました。幸いにも情報漏洩等、重大な事故に至らなかったことは、これまで実施してきた情報セキュリティ対策が一定の効果を上げた結果と言えますが、サイバー空間における脅威は日々増大しており、情報セキュリティの水準には、ここまで達成していればよいという限度はありません。

本報告書は、内閣官房における平成２３年度の情報セキュリティ対策の状況をまとめ、平成２４年度以降の対策実施に資するべく作成したものです。
情報セキュリティ対策は決して現状維持に止まることなく、平成２４年度以降においてもさらに一層の情報セキュリティ水準の向上に努めてまいります。

最高情報セキュリティ責任者
内閣総務官　原　勝則

2　内閣官房における情報セキュリティ対策の枠組

(1)　内閣官房の役割・事務と取り扱う情報の重要性

内閣官房は、内閣の補助機関であるとともに、内閣の首長たる内閣総理大臣を直接に補佐・支援する機関である。具体的には、内閣の庶務、内閣の重要政策の企画立案・総合調整、情報の収集調査などを担っており、情報セキュリティ対策を講じていく上で、次のような組織・事務の特性を有している。

ア　内閣の機密を扱う機関であること。

他の府省庁以上に秘匿性の高い情報を処理し、他の府省庁と適切に共有するために、高度な情報セキュリティ対策を講じる必要があり、特に、総理大臣官邸は日本政府の中心となる組織であり、外部からの攻撃の標的となりやすい。

イ　内閣の重要政策の企画立案・総合調整を強力かつ迅速に行うため、その時々の課題に応じて多数の組織が臨時に設置されること。

職員の多くが他の府省庁からの出向者で構成されており、情報セキュリティに対する認識、理解度が多様であることや、庁舎が分散していることから、組織的な情報管理や職員の情報セキュリティ水準の統一化がされにくい。一方、内閣官房において初任の段階から一貫した情報セキュリティ教育を施して人材育成を行うことは困難である。

また、重要施策の企画立案に関して他の府省庁からの重要情報が集まるため、その取扱いに十分な注意を払う必要がある。

ウ　内閣府と密接な関係があること。

基本的な情報システムの機能を内閣府と共有・共通化していることから、内閣府の情報セキュリティポリシーとの整合性の担保と内閣官房・内閣府の独立性の担保の均衡を図る必要がある。

このように、内閣官房は他の府省庁とは異なる組織・業務特性を有していることから、統一的な情報セキュリティ対策を持続的に講じ、その水準を向上させることに腐心している。

このため、最高情報セキュリティアドバイザーを複数配置し、業務特性に応じた丁寧な研修の実施、秘匿性の高い情報の管理方法の検討などにより、特性に応じた情報セキュリティ対策を講じている。

(2)　情報セキュリティ対策の対象となる組織及び情報

内閣官房では、政府機関の情報セキュリティ対策のための統一基準群（以下「統一基準」という。）及び内閣官房情報セキュリティポリシー（以下「ポリシー」という。）に基づき、内閣官房すべての組織を対象として、情報セキュリティ対策を

実施している。

なお、内閣官房における情報セキュリティ対策の対象となる情報は、統一基準の定義に基づき、ポリシーにおいて次のように定めている。

・情報システム内部に記録された情報
・情報システム外部の電磁的記録媒体に記録された情報
・情報システムに関係がある書面に記載された情報※

※　書面に記載された情報には、電磁的に記録されている情報を記載した書面（情報システムに入力された情報を記載した書面、情報システムから出力した情報を記載した書面）及び情報システムに関する設計書を含む。

(3)　情報セキュリティ対策の実施体制

内閣官房では、情報セキュリティ対策を実施するために、統一基準及びポリシーに基づき、以下に示す体制を整備している。

ア　最高情報セキュリティ責任者（以下「ＣＩＳＯ」という。）

情報セキュリティ対策に関する事務を統括する。内閣官房では内閣総務官が務める。

イ　情報セキュリティ委員会

内閣官房における情報セキュリティに関する対策基準の策定、改訂等を行う。内閣官房では、委員長はＣＩＳＯ、委員は情報セキュリティ責任者等が務める。

ウ　情報セキュリティ監査責任者

情報セキュリティ監査に関する事務を統括する（年度情報セキュリティ監査計画の策定、監査実施者への指示等）。内閣官房では機微な情報を扱う部局ごとに内閣審議官等が務める。

エ　統括情報セキュリティ責任者

情報セキュリティ対策に関する連絡体制・関係規程の整備、行政事務従事者に対する情報セキュリティ教育の計画立案・実施等に関して、情報セキュリティ責任者を統括する。内閣官房では内閣総務官室の内閣参事官が務める。

オ　情報セキュリティ責任者及び情報セキュリティ副責任者

情報セキュリティ責任者は、部局での情報セキュリティ対策に関する事務を統括する。情報セキュリティ副責任者は、大規模な組織にのみ置くもので、情報セキュリティ責任者と分掌した事務の範囲内における情報セキュリティ対策に関する事務を統括する。

カ　情報システムセキュリティ責任者

所管する情報システムの情報セキュリティ対策の管理に関する事務を統括す

る（セキュリティ機能の設計、利用手順書等の整備及び安全区域の管理等）。

キ　情報システムセキュリティ管理者

所管する情報システムの情報セキュリティ対策を実施する（定められた手順や判断された事項に従い、対策を実施する）。

ク　課室情報セキュリティ責任者

課室における情報セキュリティ対策に関する事務を統括する（行政事務従事者による情報の取扱い、支給外システムの業務利用に関する許可等）。

ケ　最高情報セキュリティアドバイザー

情報セキュリティ対策に関する専門的な知識及び経験を有した専門家を置き、ＣＩＳＯに対して情報セキュリティ対策に関する様々な事務への助言等を行う。

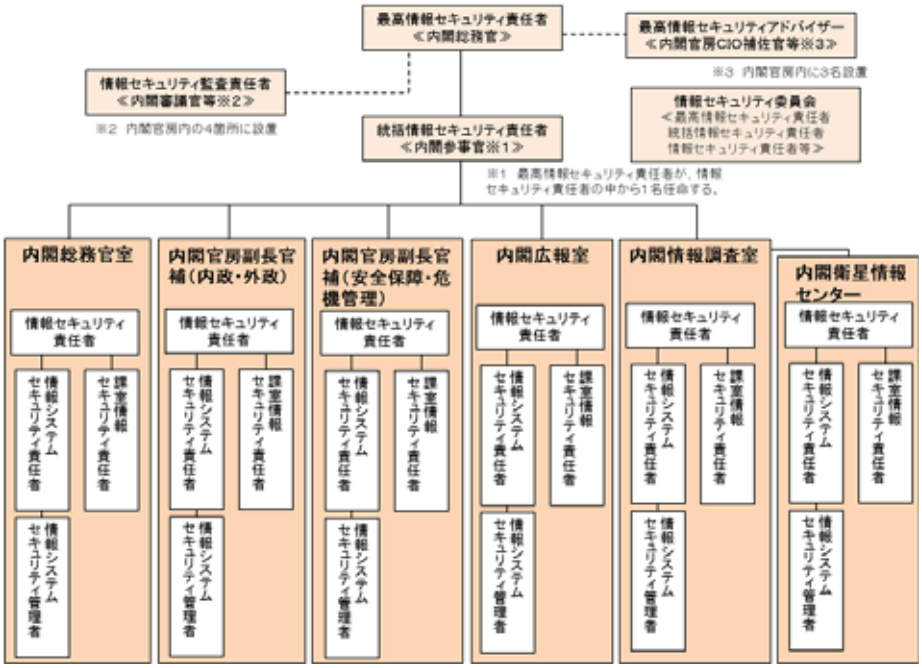

図１　内閣官房における情報セキュリティ対策の体制イメージ

コ　内閣官房における情報セキュリティ対策担当

情報セキュリティ政策会議で決定する各種の計画等に基づき、内閣官房情報セキュリティセンター（以下「ＮＩＳＣ」という。）及び内閣府大臣官房企画調整課情報システム室と連携し、内閣総務官室情報専門職が情報セキュリティ対策を担当している。

(4)　情報セキュリティ対策の概要

ア　情報セキュリティ対策の基本方針及び情報セキュリティ省庁対策基準の整備

内閣官房では、統一基準に基づき、情報セキュリティ対策の基本方針及び情報セキュリティ省庁対策基準としてポリシーを整備している。

イ　実施手順書等の整備

ポリシーに定められた遵守事項を運用していくための手順となる文書として、以下に掲げる実施手順書等を整備している。

- 人事異動の際に行うべき情報セキュリティ対策実施規程
- 内閣官房外の情報セキュリティ水準の低下を防止する規程
- 情報の格付け及び取扱い制限に関する規程
- 例外措置手順書
- 情報取扱手順書
- 内閣官房外での情報処理の手順書
- 内閣官房支給以外の情報システムによる情報処理の手順書
- 障害・事故等対処手順書
- ドメイン名の使用に関する規程
- 内閣官房情報セキュリティ委員会の設置について
- 外部委託における情報セキュリティ対策実施規程
- 暗号及び電子署名規程

ウ　情報セキュリティ教育の実施

統一基準及びポリシーの内容について理解を促進させること、職員一人ひとりが情報セキュリティ対策の体制の中での自分の立ち位置を自覚し、果たすべき役割を理解させることを目的として、内閣官房全職員を対象とした情報セキュリティ教育（以下「教育」という。）を毎年度実施している。

エ　情報セキュリティ自己点検の実施

情報セキュリティ対策の実効性担保のため、すべての行政事務従事者自らが情報セキュリティ関係規程に準拠した運用を行っているか否かについて点検し、その結果に基づいて、それぞれの当事者又はその管理者が、必要な改善策実施の材料とするものである。内閣官房においては、全職員を対象として、ポリシーに定める情報セキュリティ対策の各遵守事項を確認するための情報セキュリティ自己点検（以下「自己点検」という。）を毎年度実施している。

オ　情報セキュリティ監査の実施

情報セキュリティ対策は、ポリシーに基づく情報セキュリティ対策の実施サイクルに従った間断ない取組が必要である。情報セキュリティの水準を適切に維持していくためには、策定したポリシーを確実に運用するとともに、その効果を的確に評価し、必要に応じてポリシーを見直すことが重要である。

このため、内閣官房では毎年度情報セキュリティ監査（以下「監査」という。）を実施している。監査は、ポリシーにおける情報セキュリティ対策の体制（ＣＩ

ＳＯ～行政事務従事者）の外に独立している情報セキュリティ監査責任者による内部監査である。

カ　情報セキュリティ重点検査の実施

　情報セキュリティ重点検査（以下「重点検査」という。）は、内閣官房が運用管理している公開Ｗｅｂサーバ及び電子メールサーバ等について、統一基準に準拠した対策が実施されているかを確認するための検査である。内閣官房では、ＮＩＳＣが配布する調査票により毎年度実施している。

３　平成２３年度の情報セキュリティ対策実施状況

３－１　平成２３年度の対策状況のまとめ

平成２３年度は、政府機関に対するサイバー攻撃の増加に鑑み、サイバー攻撃についての職員の理解を深めるための教育及びソーシャルハッキングの手口を用いる標的型攻撃に関する実践的な訓練を行った。

また、平成２２年度の自己点検及び監査の結果を踏まえ、実施手順書等の追加整備を行うとともに、自己点検時の学習用教材に実際の業務で起こり得る事例を用い、より職員の理解度を深める教育を実施した。

情報システムについては、重点検査結果は良好であるものの、重点検査の対象に当てはまらないＡＳＰサービス※を利用したシステムが増加した。対策の検討が必要と考えられる。

※　ＡＳＰサービス：　Application Service Provider Service。インターネット上で、アプリケーションソフトウェアを顧客にレンタルする事業者が行う役務のこと。例えば、ＡＳＰの提供するＷｅｂサーバを利用すれば、システム構築をすることなく、ＨＰの開設をすることが可能。

３－２　教育・自己点検・監査の状況

(1)　教育の実施状況

①　教育計画の策定、教育の企画、対象者の役割に応じた教育教材の整備

ア　教育計画の策定

平成２３年度の教育は、内閣官房の業務の動向を踏まえつつ、教育に続いて行う自己点検及び監査の予定を勘案し、平成２３年１２月から平成２４年１月にかけて実施した。

イ　教育の企画・対象者の役割に応じた教育教材の整備

平成２３年度の教育の実施に当たっては、ＮＩＳＣ提供の自己点検票雛形に付属している事前学習用例題を用い、内閣官房における実務に合うよう当該例題をより具体的な問題に修正を加え使用した。

②　その他の教育・啓発活動

自己点検における事前学習の他、次のことを実施した。

ア　新規入庁者用教材の作成

通年で新規入庁者が発生する内閣官房では、他の府省庁に比べて新規入庁者向けの画一的な教育･啓発が難しいことから、内閣官房の新規入庁者向け教材を作成して電子掲示板に掲示した。人事異動時期を踏まえ、概ね四半期ごとに部局へ閲覧を促したほか、個別に新規組織への資料配布を実施した。

イ　情報セキュリティ対策担当者の知識向上

ＮＩＳＣが隔月程度開催する「情報セキュリティ勉強会」への参加により知識向上を図った。そこで得られた知見については、内閣官房内へ周知

し、また、個別相談に生かした。

ウ　時事的なセキュリティ事案に関連した教育

政府機関に対するサイバー攻撃の増加に鑑み、標的型攻撃メールをはじめとしたサイバー攻撃全般に関する理解を深める事を目的として、内閣官房情報セキュリティ教育教材を作成し、職員に配布した。

サイバー攻撃については、攻撃のパターンを類型化し、攻撃の対象、攻撃の目的等を分かりやすく解説するとともに、実際に報道されている事件について、経緯、手口、被害規模等を織り交ぜて解説した。また、標的型攻撃メールについては、従来のウイルス感染を目的としたメール攻撃との違い、標的型攻撃に用いられるウイルスの活動、ソーシャルハッキングを用いた実際の手口、標的型攻撃メールを判別するためのポイントの他、日常的に起こりうるソーシャルハッキングとその危険性にまで踏み込んだ解説をした。

エ　標的型攻撃を模したメール訓練の実施

ＮＩＳＣにおいて実施した標的型攻撃を模したメール訓練に参加した。本訓練は、参加府省毎にカスタマイズが可能であったことから、訓練の効果が最大限に発揮できるよう、差出人は実在する職員を装い、メールの件名及び文面については、実際の業務において有り得る内容にし、難易度を高めた設定で訓練を実施した。

(2)　平成２３年度自己点検の結果

自己点検の対象は、内閣官房におけるすべての職員（非常勤職員、期間業務職員を含む）である。実施に当たっては、情報セキュリティ対策の責務に基づき以下のとおり区分し、それぞれの責務に応じて実施すべき情報セキュリティ対策に沿った内容の自己点検票を作成・配布して実施した。

表１　自己点検票の種類

自己点検票の種類
情報セキュリティ責任者向け
課室情報セキュリティ責任者向け
情報システムセキュリティ責任者向け
情報システムセキュリティ管理者向け
権限管理を行う者向け
行政事務従事者向け

ア　把握率

自己点検対象者数のうち、実際に自己点検を実施した者の割合は次のとおり。

平成２３年度における自己点検の把握率：100%

イ　実施率

自己点検の点検項目について、対策の責務が生じた者が、対策を実施した項目の割合は次のとおり。

表２　主体別対策実施率

情報セキュリティ責任者等	情報システムセキュリティ責任者等	行政事務従事者
94.8%	96.5%	90.6%

ウ　自己点検の結果の総括

・　一般職員（行政事務従事者）

本年度における自己点検は、「情報の利用」について重点的に検査を行っているが、特に情報の作成・入手時における取扱いについて理解が不足していることが明らかになった。職員の理解力の向上及びセキュリティポリシーの遵守に向けて一層の対策実施が必要と考えられる。

・　課室長級職員（情報セキュリティ責任者、情報セキュリティ副責任者、課室情報セキュリティ責任者）

課室長級職員については、情報セキュリティ対策として、情報セキュリティ教育を行わなければならないこととされているが、実施不足等の回答が散見された。完全な実施に向けてなお一層の取り組みが必要と考えられる。

・　情報システム担当職員（情報システムセキュリティ責任者、情報システムセキュリティ管理者）

システム担当職員については、システムの運用に関するドキュメント類について、一部未整備であることが明らかになった。セキュリティ対策の完全な実施に向けてなお一層の取り組みが必要と考えられる。

(3)　監査の実施結果

①　平成２３年度に実施した監査の内容・対象

ア　関係規程に関する準拠性監査（規程類の対比による遵守事項の確認）

・　統一基準とポリシーの準拠性監査
・　ポリシーと実施手順等の整合性確認

イ　自己点検に関する監査（質問・目視確認等による自己点検票の内容確認）

・　情報セキュリティ対策の体制に関する監査
・　情報システムに対する情報セキュリティ対策の実施状況に関する監査

・　執務室における情報セキュリティ対策の実施状況に関する監査

ウ　その他の監査（関係書類の査閲による履行状況の確認）

・　平成２２年度監査結果で明らかになった課題及び問題点に対する改善計画の改善状況の監査

② 監査の結果

監査の結果、以下のとおり一部に指摘事項が見られた。今後の情報セキュリティ対策の水準向上のために改善の努力が必要である。

ア　関係規程に関する準拠性監査

・　統一基準とポリシーの準拠性監査

統一基準が要求する事項を満たしていることが確認された。

・　ポリシーと実施手順等の整合性確認

各実施手順書は、ポリシーで要求されている項目を概ね満たしていることが確認された。

イ　自己点検に関する監査

・　情報セキュリティ対策の体制に関する監査

自己点検結果は、監査時の調査票回答結果と一致しており、適切に自己点検が実施されていることが確認された。

・　情報システムに対する情報セキュリティ対策の実施状況に関する監査

自己点検結果は、監査時の調査票回答結果と一致しており、適切に自己点検が実施されていることが確認された。

・　執務室における情報セキュリティ対策の実施状況に関する監査

自己点検結果は、監査時の調査票回答結果と一部に不整合があり、必ずしも適切に自己点検が実施されていないことが確認された。

ウ　その他の監査

・　平成２２年度監査結果で明らかになった課題及び問題点に対する改善計画の実施状況の監査

自己点検票の改善及び実施手順等の整備により課題及び問題点の改善が進んでいることが確認されたが、未整備の一部の実施手順等については、早期の整備が望ましいとの指摘があった。

・　ＮＩＳＣが希望する省庁に対し実施した専門機関によるＷｅｂサイトの脆弱性検査への参加

軽微な脆弱性を検出したため、すぐに措置した。今後も外部機関等による検査を定期的に実施する予定である。

(4)　教育・自己点検・監査の結果に基づく対応

今後も引き続き、遵守事項の理解促進と自己点検票の工夫を図り正確な自己点検結果の把握に努める。また、ポリシーに基づき整備することとされている実施手順等の整備を推進する。

３－３　情報システムごとの状況

(1)　平成２３年度の重点検査

平成２３年度は、平成２３年１０月１日時点における、公開Ｗｅｂサーバ、電子メールサーバ及びＤＮＳサーバを対象に重点検査を実施した。

検査結果については以下のとおり。

ア　公開Ｗｅｂサーバ

一部の公開Ｗｅｂサーバにおいて、ＳＳＬ通信※に係る脆弱性の無効化対策等がなされていないものが確認された。

イ　電子メールサーバ

一部の電子メールサーバにおいて、メール受信時におけるＳＰＦ認証※の設定がなされていないものが確認された。

ウ　ＤＮＳサーバ

ＤＮＳサーバにおいては、重点検査に係る指摘事項はなかった。

※　ＳＳＬ通信：　情報を暗号化して送受信する際のプロトコル

※　ＳＰＦ認証：　メールの送信元アドレスの偽装を防止する技術

(2)　重点検査の結果に基づく対応

重点検査において、問題点が指摘された公開Ｗｅｂサーバ及び電子メールサーバについては、指摘された問題点の解消に向けた検討を行うこととする。

なお、重点検査の範囲外で、ＡＳＰサービスによるＷｅｂサイトの開設があることから、これらのＷｅｂサイトに対するセキュリティ水準をどのように改善・確保していくべきか、今後の検討課題である。

３－４　調達・外部委託についての状況

情報システム及び情報処理業務の調達・外部委託に際しては、内閣官房の求める情報セキュリティ対策の水準が委託先において担保される必要がある。内閣官房では、平成２３年度において次の対策を行った。

・　調達や外部委託を行うものについては、構想段階からポリシーに反しないかどうかの確認、調達・外部委託時に行うべき情報セキュリティ対策のアドバイスを行い、調達事務に生かせるようにした。

３－５　その他の取組事項

(1)　情報セキュリティに関する情報の提供

年間を通し、ＮＩＳＣ及び内閣府大臣官房企画調整課情報システム室から提供される脆弱性情報及び注意喚起事項について、必要に応じて職員に周知を行った。また、セキュリティに関する情報を独自に収集し、有益と考えられるものについては職員周知を行った。

(2)　イベント・事案発生時における注意喚起

情報セキュリティ月間（平成２４年２月）等のイベント開催時に合わせ、関連する情報セキュリティ対策の内容をまとめた周知啓発資料を職員向けに発出した。また、他の府省庁等で情報セキュリティ事案が起きた際、必要に応じ、事案を踏まえた情報セキュリティ対策について周知・注意喚起を行った。

(3) 電子掲示板における共有

電子掲示板に情報セキュリティ関連規程や教育の教材を掲示し、職員がいつでも参考にできるようにした。

３－６ 情報セキュリティに関する障害・事故等報告

平成２３年度、内閣官房においては、以下のようなセキュリティ事案が発生した。幸い、情報漏洩等、重大な事故に至らなかったものの、内閣官房がサイバー攻撃の対象となっていることが明らかなことから、再発防止に向けた取組が必要である。

(1) 標的型攻撃メールによるウイルス感染

ア 経緯

平成２３年９月１５日、内閣官房に標的型攻撃と思われる不審メールが到着し、添付ファイルを実行したためにウイルスに感染するという事案が発生した。職員は添付されていたファイルを実行したものの、文書が開かなかったことからウイルス感染の可能性有りと判断、直ちに端末をネットワークから隔離したことから、２次感染及び情報漏洩等の被害は発生しなかったものである。

その後、ＮＩＳＣ分析によると、当該ファイルはトロイの木馬に分類されるウイルスであり、感染すると外国のサーバに対し通信を試みるものであることが判明した。

イ 対策

本件で用いられたメールをサンプルとして、不審なメールの見分け方のポイント、ソーシャルハッキングのテクニックを用いた手口について解説した資料を作成し、職員に対し注意喚起を行った。

(2) Ｗｅｂサイトの改ざん

ア 経緯

平成２４年１月２８日夜、内閣官房で運用しているＷｅｂサイトの内、２つのＷｅｂサイトが不正アクセスを受け、コンテンツの一部が改ざんされる事案が発生した。本件は、攻撃者が、Ｗｅｂサイトのトップページに一般的に用いられるファイルを予め準備し、不正アクセスに成功した２つのＷｅｂサイトにおいて、当該ファイルを上書きしたものであるが、幸いにも大きな被害にはならなかった。

なお、本件改ざん事案は、１月２８日の深夜に発覚したものであるが、翌１月２９日午前７時過ぎにはＷｅｂサイトの復旧を行った。

イ 対策

本件はＷｅｂサイトにおいて脆弱性が残っていたことから、攻撃者の侵入

を許したものであったため、直ちにＷｅｂサーバのセキュリティ設定の見直しを行った。また、請負業者と担当者の間で連絡体制の不備が有ったことから、体制整備の見直しを行った。

なお、内閣官房内で情報セキュリティに関する障害・事故等が発生した場合は、ポリシーで定めている体制（図１）に基づき、関係者間での連絡をはじめ、必要に応じて、ＣＩＳＯにまで速やかに状況を報告し、必要な指示を受けて対処を講じることとなっている。

４　情報セキュリティ対策に関する平成２４年度の取組

平成２４年度における内閣官房の情報セキュリティ対策については、以下の取組を実施する。

(1)　標的型攻撃等に対応した職員教育の実施

標的型攻撃に用いられるメールの内容は、ソーシャルハッキングの技術を用いた新たな手口が日々生み出されていることから、新たな手口に対応し、攻撃を防ぐための職員教育を実施する。

(2)　自己点検の工夫

自己点検の実施に当たっては、設問の意図が正確に伝わるよう工夫をし、より正確に内閣官房の情報セキュリティ対策の状況が把握できるように努める。

(3)　情報セキュリティ関係規程の整備及び見直し

整備が完了していない実施手順書等の整備を早期に完了するとともに、「政府機関の情報セキュリティ対策のための統一管理基準及び統一技術基準」が情報セキュリティ政策会議で決定され次第、既に整備されているポリシーや実施手順書等を見直し、準拠させる。

(4)　情報システムを用いた情報発信に係るセキュリティ対策の検討

システム構築を伴わないＡＳＰサービスによるＷｅｂサイトの新設やソーシャルネットワーキングサービスを活用した情報発信の増加が想定されるため、そのようなサービスを利用する場合の情報セキュリティの在り方について検討を行い、対策を講じる。

５　むすび

最高情報セキュリティアドバイザーからのメッセージ

内閣官房は、内閣総理大臣、内閣官房長官のスタッフとして比較的フラットで多様かつ流動的な組織となっている。主任大臣の下、内閣の事務をラインで分担する他の府省庁と異なる組織構造となっており、情報セキュリティポリシーを徹底させるため、固有の困難さを有している。一方で、各府省庁の情報セキュリティ対策の調整を行う内閣官房情報セキュリティセンター(ＮＩＳＣ)、また、高度な情報保全を行う必要のある内閣情報調査室も置かれており、政府の情報セキュリティ対策の範を示すことも期待されている。

そのため、最高情報セキュリティ責任者である内閣総務官は、内閣官房への着任時及びその後継続的に丁寧な職員教育について、実施の徹底を図るよう指示するなどの努力を重ねているものの、情報セキュリティ責任者をはじめとする幹部の意識はまだ十分とは言い難いことから、平成２４年度は新たな発想での取り組みが求められる。

内閣官房は官邸ウェブサイトなど、サイバー空間において、政府あるいは我が国を代表した情報発信を行っている。また、政府の高度な情報が他の府省庁から集約するとともに自ら収集を行っている。平成２３年度は、重大な事故には至らなかったものの、情報セキュリティ関する事故が発生し、内閣官房はサイバー攻撃や情報の窃取を企図する者にとって標的になっていることが明らかとなった。情報セキュリティ上の脅威は極めて高いことを自覚せねばならない。そのため、適切な脆弱性対策を継続し、標的型攻撃への対策実施等、セキュリティの高度化を図ることで、高いレベルでのリスク管理を実現することが望まれる。

内閣総務官を中心に、「情報セキュリティ報告書」がとりまとめられた。我々、最高情報セキュリティアドバイザーも内閣総務官、総務官室スタッフに対し専門的な見地からアドバイスを行い、セキュリティリスクを見極め、その対応を行うセキュリティの質の向上を深めていきたい。今後とも、情報セキュリティへの取組が進むことで、情報の安全性がさらに高まることを期待する。

最高情報セキュリティアドバイザー
中川　健治／木本　裕司