平成 23 年度
情報セキュリティ報告書

平成 24 年 5 月

経済産業省

はじめに

近年の情報通信技術の急速な進歩により、システムの利便性が高まってきている一方で、不正アクセスやウイルス感染による情報漏えいなどのリスク・脅威が増大しています。このような中、日常的に利用するシステムの情報セキュリティ対策の重要性が益々高まってきています。

一方、経済産業省は、我が国の企業や重要インフラの情報セキュリティ水準を高めるための政策を担っています。従って、当省は、政府機関のみならず社会全体の模範となるよう、率先して情報セキュリティ対策に取り組む必要があります。

平成 23 年度は、防衛産業や重要インフラ、衆議院、参議院、国土地理院などに対する標的型サイバー攻撃事案が発生するなど、情報システムに対する攻撃手法が高度化してきており、内閣官房情報セキュリティセンターを中心に、関係政府機関による対策が進められて参りました。

経済産業省は、こうした対策を検討する場において積極的な貢献を果たすとともに、省内においては、昨年度に引き続き、省内各課室における情報の管理徹底を図るべく情報管理に係る運用手続きや体制の整備、情報セキュリティに係る全職員向け e-Learning 研修の実施、アクセス制限付きフォルダを活用した情報管理の徹底等を中心に、各種対策を実施して参りました。

本報告書は、平成 23 年度に経済産業省が実施した情報セキュリティ対策の具体的取組、監査結果等についてとりまとめたものです。現段階では、大きな課題は見つかっておりませんが、リスク・脅威への対策や職員向け教育の充実は、不断の改善努力が必要となります。経済産業省は、今後も引き続き、情報セキュリティの維持・向上に努めて参ります。

最高情報セキュリティ責任者
（経済産業省大臣官房長）
立岡　恒良

目次

1　平成 23 年度の総括

(1) 平成 23 年度の評価

➢ 当該年度の重点事項

・情報管理に係る運用手続きや体制整備の策定・実施

情報管理の徹底に向けた情報セキュリティ対策の策定・実施事項として、省内課室における情報管理に係る運用手続きや体制整備を検討し、経済産業省情報セキュリティポリシーに従い、情報の洗い出しや機密性の格付及び格付に応じた取扱の決定を行い、課内の体制整備を行いました。対象課室としては、省内各局（大臣官房、経済産業政策局等）及び外局（資源エネルギー庁、中小企業庁等）ごとに選定された課室で実施致しました。この結果、職員一人一人の情報セキュリティに対する意識向上につながりました。

・情報セキュリティ関連資料のワンストップ化

情報セキュリティ関係の資料をワンストップ化し、職員がいつでも必要な資料を閲覧できるように、省内イントラネットのトップページにバナーを設け、情報セキュリティコーナーとして、適宜内容の追加・見直しを行っています。

・標的型メール攻撃に係る教育訓練の実施

平成 23 年 11 月及び 12 月に、省内全職員を対象に標的型メールを模倣した訓練メール（添付メール、リンクメール）を配信し、その対応訓練を行いました。訓練実施後は、必要な職員にフォローアップ研修を実施するなど、訓練効果を高める対策を実施致しました。この結果、職員からは、「添付ファイルは良く確認したうえで開けるようにしたい」、「この様な訓練は今後も実施した方が良い」等多くの意見が寄せられ、標的型メールの教育訓練の効果が得られました。

➢ 情報セキュリティ対策の実施状況の自己点検結果

全職員に対し、情報セキュリティ対策の実施状況の自己点検を行った結果、概ね適切に実施されていることが確認できました。なお、一部実施率がやや低い結果となっている項目については、更なる向上を目指し対応を図って参ります。

➢ 情報システムごとの状況

当省の各情報システムの情報セキュリティ対策について重点的な調査を行った結果、全ての公開用 Web サーバ及び電子メールサーバにおいて各種の設定やログの収集等必要な対策が講じられていることが確認され、適切に情報セキュリティ対策が講じられていることが確認されました。

➢ 教育・啓発

イントラネットに情報セキュリティ対策に係るポータルサイトを構築し、適宜職員に必要な情報を提供するとともに、管理職に対する情報セキュリティ対策に係る集合研修、全職員に対する e-learning による情報セキュリティ研修を実施しました。これらの研修で使用した教材については、特に標的型サイバー攻撃に特化したものとして教育を実施したことに加え、標的型メールの教育訓練において、全職員がこの訓練に参加し、標的型メールの実態を自ら体験することにより、より身近に情報セキュリティの重要性を理解するきっかけとなるなど職員の意識がこれまで以上に高まりました。

➢ 調達・外部委託

当省では、情報システム開発等の情報処理業務を外部委託する際に、調達仕様書や契約書への記載事項を標準化し、委託先の情報セキュリティ対策の体制整備や履行状況の確認など、委託先においても当省の情報セキュリティ対策と同等の対策を実施するよう、適切に管理を行っております。

➢ その他取り組んだ事項

当省では、省内ネットワークに検疫システムを導入し、不正端末からの省内ネットワークへのアクセスを防止しています。更に、各種サーバ及びクライアントにおいて、それぞれ異なるアンチウイルス対策ソフトウェアを稼働させるなど、複数のウイルス対策を実施し、最新の脆弱性修正プログラムを適用しております。

また、外部からの不正アクセスに対しては、システムの２４時間監視を行うとともに、フィルタリング機能を利用した迷惑メール（スパムメール）対策を講じるなどセキュリティの確保に努めております。

省内では、暗号機能付き USB メモリの導入や、アクセス制限付きフォルダの活用、電子ファイルのアクセス制限を行う情報漏えい防止サービスの導入を通じ、情報の漏えい防止に努めています。

➢ 情報セキュリティに関する障害・事故等の報告

平成 24 年１月 29 日に、当省の委託事業にて運用を行っているウェブサイトがサイバー攻撃を受けて一部のページが改ざんされ、同サイトの趣旨と無関係なページが表示される事案が発生致しました。なお、同サイトへのウイルス感染や情報流出は確認されませんでした。また、平成 24 年２月３日に、特許庁の端末がウイルス感染していたことが判明しました。発見したウイルスは、２月５日までに庁内全ての端末から駆除（感染していたのは３台）を済ませました。なお、特許出願等に係る未公開情報について、ウイルス感染による流出は確認されませんでした。

(2) 平成 24 年度の目標

当省では、平成 24 年度に重点的に取り組む目標を以下のとおりとし、今後更なる情報セキュリティの向上を目指して参ります。

・省内課室の情報管理に係る運用手続きや体制の整備について、その実施状況を適宜把握するとともに、必要により改善事項の指摘や改善状況の把握等に努めて参ります。
・基盤情報システムの更改により、機密性の高い情報の漏えい防止の徹底に向けたアクセス制限付きフォルダや情報漏えい防止サービス、新たな認証システムなどの技術的手段の活用を推進し、更なる高度化を図って参ります。
・情報セキュリティ研修等において、標的型メールへの対応（訓練や注意喚起等）や当省関連の Web サイト改ざんへの対応等について、重点的に実施して参ります。

２　報告の基本情報

(1) 経済産業省の概要

当省は、企業、地域、個人、ＮＰＯなどの多様な主体が、持ち得る能力と可能性を最大限に発揮できるように、経済社会システムを支える制度や技術基盤を整備し、内外の情報を提供することにより、わが国の経済活力の向上を目指しております。このため、経済構造改革、産業技術力強化、内外一体の対外経済政策、環境・エネルギー対策、中小企業対策、知的財産保護等の様々な政策課題に取り組んでいます。

こうした様々なミッションを果たすためには、職員一人一人がこれら各種政策の企画・立案・実施能力の向上を図るとともに、省内にある経営資源（人材・予算・情報等）を最適に配置・連携し、創造的、機動的、効率的に日常の業務が実施できるよう業務・システムの環境を整備することが重要な課題となっております。

当省では、これらの課題に対応するために必要な情報システムを構築・運用し、行政業務の効率的かつ着実な遂行に努めております。

経済産業省で構築・運用している主な情報システムは、以下のとおりです。

・経済産業省基盤情報システム

職員が業務遂行に利用するネットワーク（省内 LAN、インターネット）、ソフトウェア及びハードウェアといった当省の情報処理の基盤となる情報システム。

・経済産業省電子申請システム

国民の皆様がインターネットを利用して当省への申請・届出を行うための情報システム。

・特許庁システム

特許、実用新案、意匠、商標等の出願の受付から審査、審判、登録、公報発行まで一連の手続き及び関連業務を電子データにより処理するシステム。

・工業標準策定システム

日本工業規格の制定・公示・公開、国際標準化機構／国際電気標準会議等の国際規格策定業務、JIS マーク制度の管理業務について、インターネットを使用して行うための情報システム。

(2) 対象とする期間

本報告書が対象とする期間は、平成 23 年 4 月 1 日から平成 24 年 3 月 31 日までの情報セキュリティ対策に関する取組を対象としています。

(3) 対象とする組織

本報告書が対象とする組織は、経済産業省の本省、資源エネルギー庁、原子力安全・保安院、特許庁、中小企業庁、各経済産業局としています。

(4) 対象とする情報

本報告書が対象とする情報は、NISC より提示された「政府機関の情報セキュリティ対策のための統一基準群」（平成 23 年 4 月 21 日）（以下、「政府機関統一基準群」という。）で対象とする情報であって、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及び情報システムに関係がある書面に記載された情報としています。

(5) 本報告書の責任部署

経済産業省大臣官房情報システム厚生課

(6) 定員数

本報告書の対象となる当省の定員数は、8,582 人（平成 23 年度）

(7) 情報システム予算額

当省で運用している情報システムに関する予算総額は、3,986,537 千円（平成 23 年度予算：成果重視事業電子経済産業省構築事業庁費）

３　情報セキュリティ対策の枠組み

(1) 情報セキュリティ対策に関する文書体系

当省では、統一的な枠組みの中で各府省庁が情報セキュリティの確保のために実施すべき対策の基準である政府機関統一基準群に準拠した「経済産業省情報セキュリティ管理規程」（以下、「セキュリティ管理規程」という。）及び「経済産業省情報セキュリティ対策基準」（以下、「セキュリティ対策基準」という。）（以下、「セキュリティ管理規程」及び「セキュリティ対策基準」を「経済産業省情報セキュリティポリシー」という。）を平成 18 年３月に制定しました。なお、経済産業省情報セキュリティポリシーは、平成 23 年 7 月 25 日に改正しております。

この経済産業省情報セキュリティポリシーは、当省における情報セキュリティの確保に関する基本規範と位置付けられるものです。

「セキュリティ管理規程」では、情報セキュリティの責任体制や推進体制、情報セキュリティ対策の教育、自己点検及び監査、並びに障害対応等の情報セキュリティマネジメントに関する事項を規定しています。

「セキュリティ対策基準」では、職員が日常的に実施すべき情報セキュリティ対策、情報システムの構築・運用・廃棄に係る情報セキュリティ対策等、行政事務を遂行する上で必要な情報セキュリティ対策に関する事項を規定しています。

また、経済産業省情報セキュリティポリシーに定められた遵守事項について、具体的な実施手順を定めた下位規程として、情報の格付及び取扱制限の具体的な手順を定めた「情報の格付及び取扱制限の基準並びに格付及び取扱制限を明示する手順」及び個人所有パソコン等で業務を行う際の情報セキュリティ対策を定めた「経済産業省支給以外の情報システムにより情報処理を行う場合に講ずるべき安全管理措置」等の下位規程を整備しています。

(2) 情報セキュリティ対策の推進体制

- 情報セキュリティ対策に係る組織体制

情報セキュリティ対策は、職員全員が自ら取り組んでいくことはもちろんのこと、主体毎の権限と責任を明確にし、必要となる推進体制を確立し組織全体として取り組んでいく必要があります。

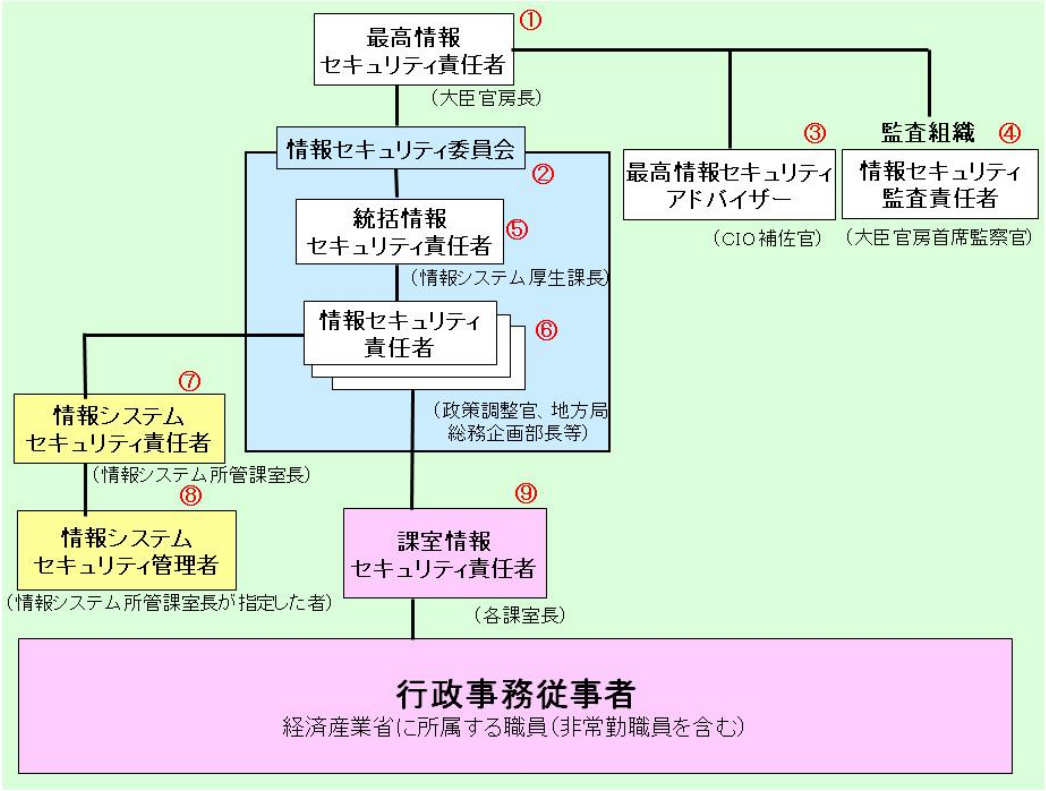
当省では、図１に示すとおり、最高情報セキュリティ責任者の下、各部局に情報セキュリティ責任者、各課室に課室情報セキュリティ責任者を置き、それぞれの責務に応じて、情報セキュリティ対策に取り組んでいます。

また、当省の各情報システムについては、それぞれの所管課室長を情報システムセキュリティ責任者とし、所管する情報システムの情報セキュリティ対策に取り組んでいます。

さらに、最高情報セキュリティアドバイザーを置き、当省の各種情報セキュリティの

企画、実施、課題対応等あらゆるマネジメントに関し助言を得ています。

図１　経済産業省の情報セキュリティ体制



① 最高情報セキュリティ責任者
（大臣官房長）
省内の情報セキュリティに係る事務を統括

② 情報セキュリティ委員会
情報セキュリティに関する重要事項の審議

③ 最高情報セキュリティアドバイザー
（CIO補佐官）
情報セキュリティに関する専門的な助言

④ 監査組織
情報セキュリティに関する監査

⑤ 統括情報セキュリティ責任者
（情報システム厚生課長）
最高情報セキュリティ責任者の補佐
情報セキュリティ責任者の統括

⑥ 情報セキュリティ責任者
（政策調整官、地方局総務企画部長等）
部局内の情報セキュリティに係る事務を統括

【情報システム所管課の役割】

⑦ 情報システムセキュリティ責任者
（情報システム所管課室長）
所管する情報システムの運用管理の統括

⑧ 情報システムセキュリティ管理者
（情報システム所管課室長が指定した者）
所管する情報システムの運用管理

【各課室における役割】

⑨ 課室情報セキュリティ責任者
（各課室長）
課室内の情報セキュリティに係る事務を統括

➢ 情報セキュリティ対策に係る推進部署の体制

当省における情報システム及び情報セキュリティ対策に係る具体的な推進部署及び体制は図２のとおりです。

当省の情報システムの整備及び管理を担当している大臣官房情報システム厚生課では、情報セキュリティに係る以下の役割を担っています。

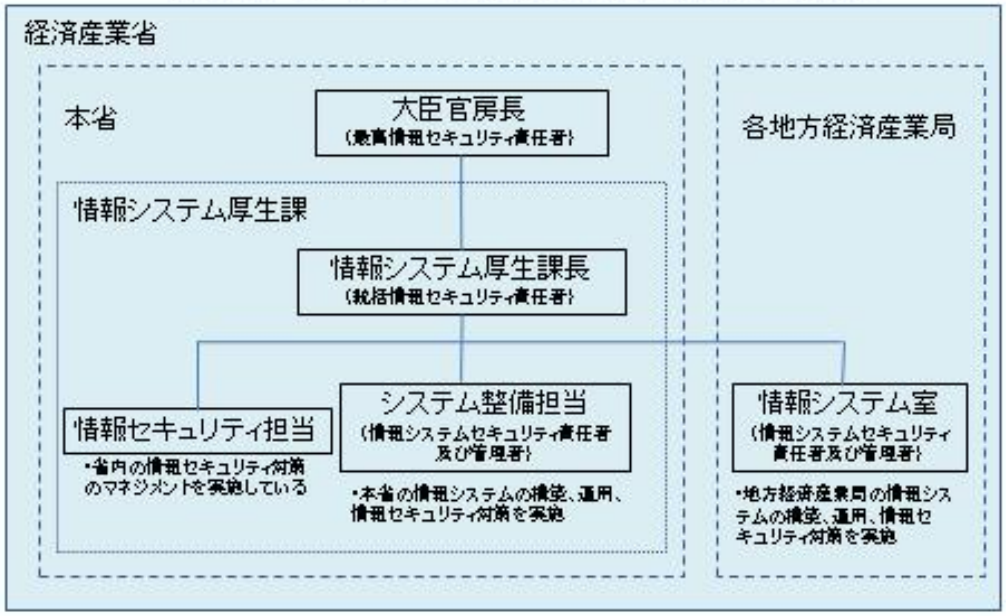
・情報セキュリティ担当

当省の情報セキュリティに関する事務を統括し、情報セキュリティ関連規程の整備や情報セキュリティ対策の教育、普及・啓発、セキュリティ監査等を実施しています。

・システム整備担当

当省の情報処理の基盤となる経済産業省基盤情報システムの運用や、省内各課室の業務に係る業務情報システムの運用支援を実施するなど、これらのシステムに係る情報セキュリティ対策を実施しています。

図２　経済産業省の情報セキュリティ対策に係る推進部署及び体制



(3) 情報セキュリティ監査等

➢ 情報セキュリティ監査の実施

当省では、政府機関統一基準群及びセキュリティ管理規程に基づき、毎年度、情報セキュリティ監査を実施しています。

当省の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、政府機関統一基準群に準拠した経済産業省情報セキュリティポリシーを適切に整備・運用することによってその実効性を確保し、その準拠性と妥当性を客観的に確認する必要があります。

また、各業務システムの情報セキュリティ対策の実施状況を適切に評価し、評価結果に応じて見直しや改善を行うというPDCAサイクルを適切に実施することが重要です。

これらの点を踏まえ、当省の情報セキュリティ監査は、独立性を有する外部の監査組織に委託し実施しています。

監査の内容は、当省の情報セキュリティポリシーの政府機関統一基準群への準拠性の監査や各種情報システムの情報セキュリティ対策の実施状況の監査です。監査対象となる情報システムは、毎年度、情報システムのライフサイクル等を考慮し選定しています。

平成23年度に実施した情報セキュリティ監査の内容は次のとおりです。

○監査対象・内容

(ｱ)情報セキュリティ監査

①経済産業省情報セキュリティポリシーの政府機関の情報セキュリティ対策のための統一基準群への準拠性監査

②各実施手順の経済産業省情報セキュリティポリシーへの準拠性監査

③平成22年度に実施した情報セキュリティ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状況の監査

(ｲ)システム監査

①システム運用時における情報セキュリティ対策実施状況の監査

②標的型サイバー攻撃に係るシステムの対応状況に係る監査（認証システムの安全性等の監査）

○監査の結果

(ｱ)情報セキュリティ監査

経済産業省情報セキュリティポリシーの政府機関の情報セキュリティ対策のための統一基準群への準拠性監査、及び各実施手順の経済産業省情報セキュリティポリシーへの準拠性監査において、組織や個人に大きな影響を及ぼすような不備はないことが確認されました。

また、平成22年度に実施した情報セキュリティ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状況の監査においては、指摘された不備に係る事項は対応が済

んでいることが確認されました。

(ｲ)システム監査

システム運用時における情報セキュリティ対策実施状況の監査において、組織や個人に大きな影響を及ぼすような不備はないことが確認されました。なお、ログ保管やパスワード管理等いくつかの事項において軽微な不備が確認されました。

○監査結果を踏まえた対応

(ｱ)情報セキュリティ監査

経済産業省情報セキュリティポリシーの政府機関統一基準群への準拠性監査等において、大きな不備は見られないことから、今後は、経済産業省セキュリティポリシーの実効性を高めるべく、普及啓発の徹底や技術的対策の検討等を実施して参ります。

(ｲ)システム監査

各情報システムのライフサイクルや予算等も踏まえ、指摘があった軽微な不備について対応を図って参ります。

- 情報システムのセキュリティ診断の実施

情報システムの安全性を高めるためには、最新情報に基づいた各種情報システムの脆弱性に関するセキュリティ診断を継続的に実施することが重要です。

このため、当省では、省内職員がその業務遂行に利用している基盤情報システム等について、外部から擬似的な攻撃を行うなど、当該情報システムのセキュリティホールの有無や運用管理上の問題点の有無等を確認するため、セキュリティ診断を毎年度実施しています。

平成23年度も基盤情報システム等のサーバ及びWebアプリケーションに対し、診断ツールや手法を用いたセキュリティ診断を実施致しました。この結果、基盤情報システム等のサーバ及びWebアプリケーションの一部に、攻撃に利用される可能性のある脆弱性が検出されました。

この結果を踏まえ、診断対象のサーバやWebアプリケーションの諸情報を確認し、セキュリティ修正プログラム（以下、「セキュリティパッチ」という。）の適用、並びに各種設定の見直し及び修正等を行い、脆弱性への対処を実施致します。

(4) 情報セキュリティ対策の予算額

当省の情報セキュリティ対策関連予算は、情報セキュリティ監査、情報セキュリティ診断、24時間情報セキュリティ監視等に係る予算として、以下の額を計上しています。

38,951（千円）

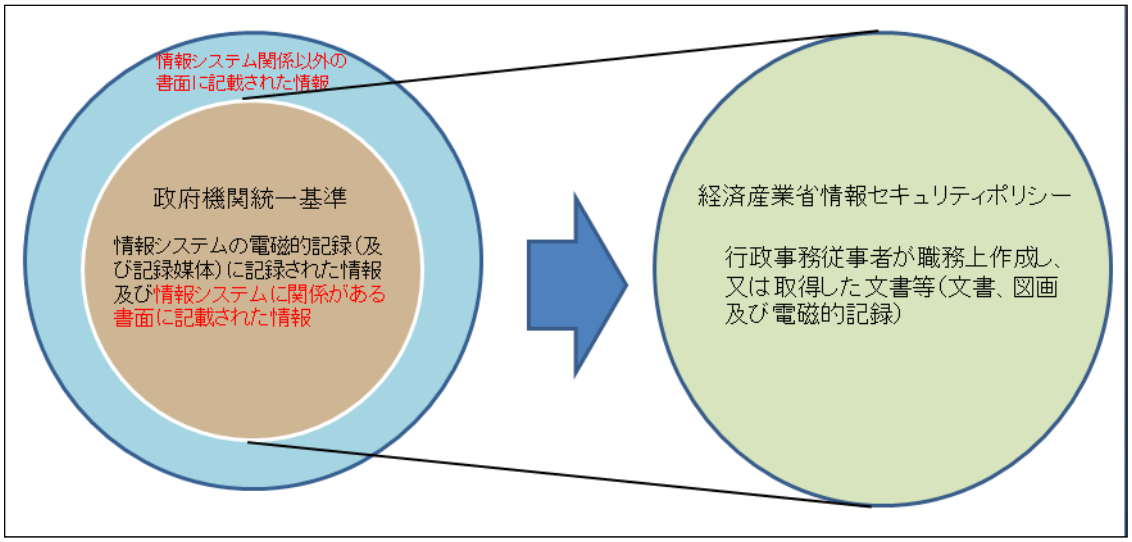
（平成23年度予算：成果重視事業電子経済産業省構築事業庁費のうち、情報セキュリティの確保）

(5) 政府機関統一基準群と経済産業省情報セキュリティポリシーの差異

①対象範囲

政府機関統一基準群の情報の定義では、「情報とは、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及び情報システムに関係がある書面に記載された情報をいう。」と定義し、情報システムに関係がある書面を除き、書面のみ存在している情報を対象としていませんが、経済産業省セキュリティポリシーでは、対象範囲としています。

図３　情報の範囲



②格付の区分

経済産業省情報セキュリティポリシーでは、より機密性の高い情報を重点的に保護するために、政府機関統一基準群に規定されている情報の格付の分類のうち「機密性３情報」を細分化し、政府機関統一基準群にはない「機密性４情報」を当省独自に設けています（表１参照）。

これに伴い、「機密性４情報」の取扱に関しては、課室情報セキュリティ責任者ではなく、その上位の責任者である情報セキュリティ責任者から持ち出し等の許可を得る必要があるなど、より厳格な規定としています。

表１　情報の機密性に応じた格付区分

経済産業省情報セキュリティポリシー		政府機関統一基準群（第５版）	
格付けの区分	格付の基準	格付の区分	格付の基準
機密性４情報	行政事務で取り扱う情報のうち、事案の内容の漏えいを特に防止する必要があり、その漏えいが国の安全、利益に損害を与えるおそれがある情報をいう。	機密性３情報	行政事務で取り扱う情報のうち、秘密文書に相当する機密性を要する情報
機密性３情報	行政事務で取り扱う情報のうち、機密性４情報に次いで、事案の内容の漏えいを特に防止する必要がある情報をいう。		
機密性２情報	行政事務で取り扱う情報のうち、機密性４情報又は機密性３情報には該当しないが、その漏えいにより、国民の権利が侵害され又は行政事務の遂行に支障を及ぼすおそれがある情報をいう。	機密性２情報	行政事務で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、漏えいにより、国民の権利が侵害され又は行政事務の遂行に支障を及ぼすおそれがある情報
機密性１情報	「機密性１情報」とは、機密性２情報、機密性３情報又は機密性４情報以外の情報をいう。	機密性１情報	機密性２情報又は機密性３情報以外の情報

また、「機密性２情報」を①省外へ持ち出す際、②他者へ情報提供を行う際、③省外で情報処理を行う際には、政府機関統一基準群では課室情報セキュリティ責任者への届出が必要となっていますが、経済産業省情報セキュリティポリシーでは、課室情報セキュリティ責任者の許可が必要と規定しています。

さらに「機密性４情報」を①省外へ持ち出す際、②他者へ情報提供を行う際、③省外で情報処理を行う際には、経済産業省情報セキュリティポリシーにおいては、情報セキュリティ責任者の許可を得ることとしており、より厳格な基準としています。（表２参照）

表２　機密性に応じた許可等の取得

情報の取扱区分	機密性の区分	経済産業省情報セキュリティポリシー		政府機関統一基準群（第５版）	
		情報セキュリティ責任者	課室情報セキュリティ責任者	情報セキュリティ責任者	課室情報セキュリティ責任者
情報の移送	機密性４	許可	－		
	機密性３	－	許可	－	許可
	機密性２	－	許可	－	届出
情報の提供	機密性４	許可	－		
	機密性３	－	許可	－	許可
	機密性２	－	許可	－	届出
省外での情報処理	機密性４	許可	－		
	機密性３	－	許可（注１）	－	許可（注１）
	機密性２	－	許可（注１）	－	届出（注２）

注１：課室情報セキュリティ責任者の他に、情報システムセキュリティ責任者の許可が必要
注２：課室情報セキュリティ責任者の他に、情報システムセキュリティ責任者への届出が必要

③管理体制

政府機関統一基準群では、行政事務従事者が格付を決定することになっていますが、経済産業省情報セキュリティポリシーでは、行政事務従事者が格付を行ったものを課室長（課室情報セキュリティ責任者）が妥当性の判断を行います。また、課室長は機密性４情報又は機密性３情報について、その指定を行い、アクセスを認める者の範囲を定めなければなりません。

図４　管理体制

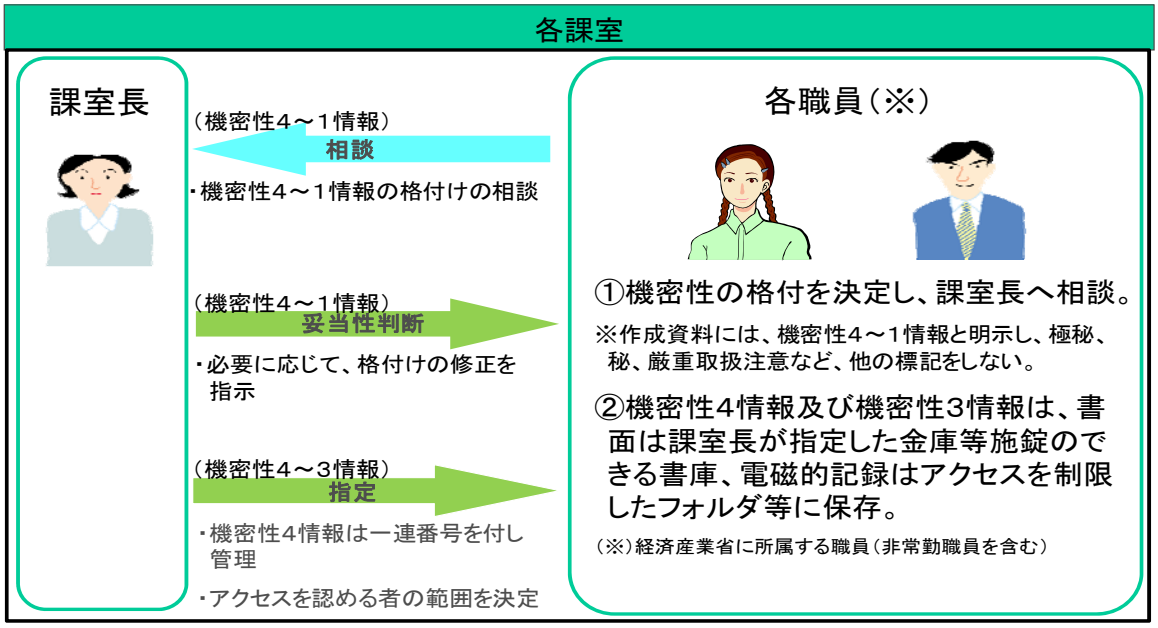
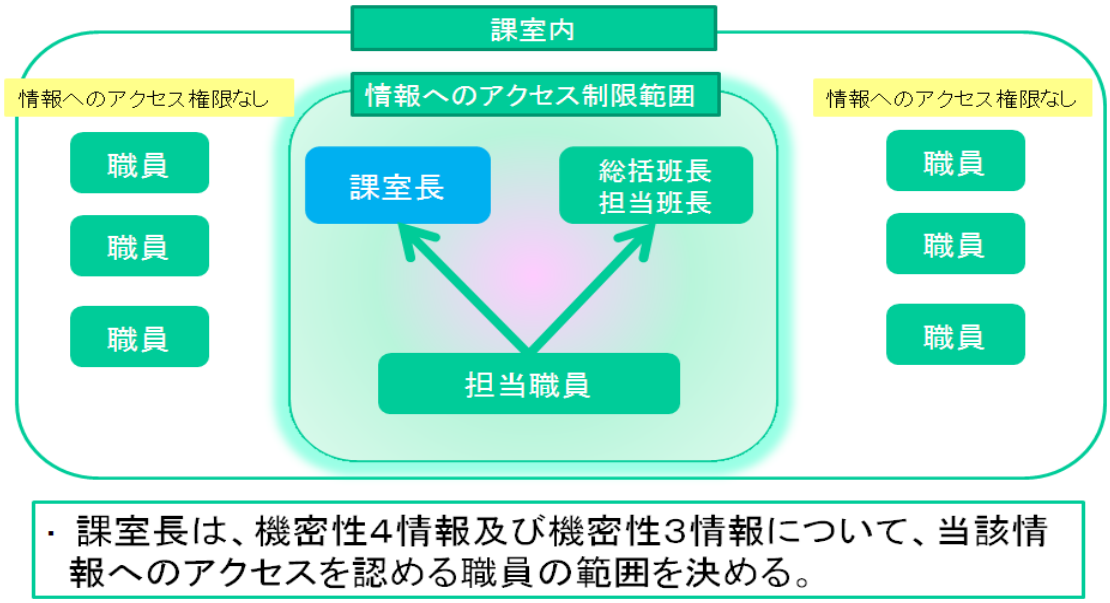


図５　アクセス範囲



(6) 業務・システム最適化における取組の管理

当省では、情報システムの企画段階において、業務・システム最適化計画を策定し、情報システムの安全性・信頼性を確保するための取組を管理しております。

例えば、経済産業省基盤情報システムについて策定された最適化計画では、情報セキュリティの更なる強化を規定し、政府機関統一基準群を踏まえ、当該情報システムの構築の要求仕様策定段階における情報セキュリティ対策の要件定義を記載し、情報システムの安全性・信頼性を確保しております。

(7) 情報システム管理台帳の整備と活用

経済産業省では、省内の各種情報システムの情報システムセキュリティ責任者、システムを所有する部署、アプリケーションのメンテナンスを管理する部署等を明示した情報システム管理台帳を整備し、毎年見直しを図っています。

この情報システム管理台帳を活用することにより、情報セキュリティ対策の実施状況の確認の際の利用に加え、政府関係機関の Web サイト改ざん事案の発生やソフトウェアの脆弱性情報が発見された際には、対策が必要な情報システムの管理者に対して直ちに注意喚起を促す等、迅速かつ的確な情報セキュリティ対策を可能とすべく、本台帳を活用しております。

また、省内各課室にて、情報システムの企画・調達・運用・保守等のライフサイクルを円滑に実施する際に必要となる情報システム厚生課からの支援や連携強化のための貴重な参考資料としても本台帳を活用しております。

(8) 情報セキュリティ対策に関する文書の見直し状況

政府機関統一基準群の改正が行われた際には、経済産業省情報セキュリティポリシーに適切に反映させ、準拠性を確保することとしております。また、情報セキュリティ監査での指摘や運用上での不具合が生じた場合についても、適宜見直しを行っております。

平成 23 年度は、経済産業省行政文書管理規程の秘密文書の管理に関する規定を経済産業省情報セキュリティポリシーに取り込む改正を行いました（平成 23 年 4 月 1 日改正)。更に、政府機関統一基準群の改正内容を取り込むため、経済産業省セキュリティポリシーの改正を行いました（平成 23 年 7 月 25 日改正)。

(9) 業務継続計画の策定

当省では、首都直下型地震発生を想定した業務継続計画を策定しています。これに基づき、当省における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を沖縄県に設置し、非常時にも当省のホームページによる情報提供や電子メールによる連絡を可能とする環境を整備しています。

当該システムについては、非常時に迅速にシステム切り替えを行うために、手順書等を整備しています。

４　当該年度の重点事項

(1) 情報管理に係る運用手続きや体制整備の策定・実施

情報管理の徹底に向けた情報セキュリティ対策の策定・実施事項として、省内課室における情報管理に係る運用手続きや体制整備を検討し、経済産業省情報セキュリティポリシーに従い、（イ）保有する情報の洗い出し、（ロ）機密性の格付の決定、（ハ）情報の格付に応じた取扱の決定を行い、課内の体制整備を行いました。

対象課室としては、省内各局（大臣官房、経済産業政策局等）及び外局（資源エネルギー庁、中小企業庁等）ごとに選定された課室で実施致しました。

この結果、職員一人一人の情報セキュリティに対する意識向上につながるとともに、省内の情報セキュリティ対策の強化につながりました。具体的には、以下の効果が望めました。

①機密性の格付及び取扱について、省内で統一的な情報管理を行うことができること。
②課室情報セキュリティ責任者である課室長が、課室内の情報管理を行う上で適切にリスクマネジメントができること。
③機密性の高い情報（機密性４情報、機密性３情報）を省内で横断的に把握できること。

機密性の高い情報については、書面については課室長が指定した施錠付きの金庫等、電磁的記録についてはアクセス制限付きフォルダ等に保存し、アクセス権のない課室員は機密性の高い情報を閲覧できないように規定しております。また、複写については、機密性４情報については原則禁止、機密性３情報については課室長の承認を受けることとし、必要以上に複写してはならないことと規定しております。

また、機密性表示については、省内の徹底を図るため、文書や電子メール等のヘッダーに自動的に機密性の表示を行うなどの技術的対策を実施致しました。

(2) 情報セキュリティ関係資料のワンストップ化

情報セキュリティ関係の資料をワンストップ化し、職員がいつでも必要な資料を閲覧できるように、省内イントラネットのトップページにバナーを設け、情報セキュリティコーナーとして、適宜内容の追加・見直しを行っています。また、省内連絡など省内職員向けのメールを通じて、各職員に周知しております。

掲載している資料は、分かりやすく複数のカテゴリーに分類し、

①情報セキュリティ対策として取り組んでいる情報管理に係る運用手続きや体制整備等に係る資料や情報セキュリティポリシーの改正等を解りやすく図解した資料
②E-learning で実施している研修資料やウイルスメール、標的型メール、不審メールを見分ける方法などの資料
③「仕様書に記載する情報セキュリティに関する事項の雛型」や「情報システムに係る

政府調達におけるセキュリティ要件策定マニュアル」などの参考資料
④不審メール受信時の対応、例外申請手続き等の問い合わせ先
等を掲載しています。

なお、情報セキュリティコーナーに掲載している資料は、職員が理解し易いよう図解を多用するなどの工夫をしています。

各種情報セキュリティ対策の実施において、システム関係部門との情報共有が促進され、職員の情報セキュリティの向上につながりました。また、簡単な問い合わせであれば参照先を指示するのみで解決できるようになり、業務効率化にもつながっています。

図６　情報セキュリティコーナー（イントラネット）

(3) 標的型メール攻撃に係る教育訓練の実施

平成 23 年 11 月及び 12 月に、省内全職員を対象に標的型メールを模倣した訓練メール（添付メール、リンクメール）を配信し、その対応に係る訓練を行いました。

訓練実施に当たっては、事前に関係会議にて訓練概要を説明するなど事前準備を図り、訓練実施後は、必要な職員にフォローアップ研修を実施するなど、訓練効果を高める対策を実施致しました。

この訓練の結果、職員からは、「添付ファイルは良く確認したうえで開けるようにしたい」、

「少しでも不審なメールは電話等で送信者に確認したい」、「この様な訓練は今後も実施した方が良い」等多くの意見が寄せられ、標的型メールの教育訓練の効果が得られました。

また、メールの自動返信を設定している例もあったため、攻撃者にその所在情報を与えることにつながる恐れから、極力自動返信はしないよう周知徹底を行いました。

５　情報セキュリティ対策の実施状況

５．１　情報セキュリティ対策の実施状況の自己点検結果

(1) 自己点検について

情報セキュリティ対策の実施状況の自己点検（以下、「自己点検」という。）は、セキュリティ対策基準の各遵守事項について各職員自らが実施状況を確認し、自己評価を行うものです。

自己点検の実施は、各職員が情報セキュリティに向き合う良い機会であり、自己点検を通じて、各職員の情報セキュリティに対する意識の醸成に繋がるものと考えています。

このような考えから自己点検の対象者は、平成 18 年度の開始当初は課室長クラス以上、平成 19 年度には課長補佐クラス以上と順次拡大し、平成 20 年度以降では全職員を対象として実施しています。

(2) 平成 23 年度自己点検結果の状況

- 経済産業省全体の把握率

全職員（非常勤職員を含む）を対象にした自己点検について、平成 23 年度の自己点検の把握率（※）は 95.0%となりました。

（※）把握率：報告対象者のうち、自己点検を提出した者の割合。

- 経済産業省全体の実施率

平成 23 年度の自己点検の実施率は、各主体とも 9 割を超える高い実施率（※）となりました。（表３参照）

（※）実施率：自己点検を提出した者のうち、全ての対策を実施した者の割合。

表３　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
実施率	98.4%	96.2%	92.2%

- 経済産業省全体の到達率

平成 23 年度の自己点検の到達率は、行政事務従事者においてやや低い割合となりました。（表４参照）

（※）到達率：自己点検を提出した者のうち、一定の割合（100%、95%、90%）以上の者が対策を実施した遵守事項の割合。
例えば、「到達率 100%」とは、項目毎の「実施」の割合が 100%であるもの、すなわち全ての回答者が「実施」と回答した項目が、全体の項目数の中でどの程度の割合を占めているかを示します。

表４　主体別到達率

	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
到達率 100%	86.3%	62.5%	0.0%
到達率 95%	96.1%	70.8%	33.3%
到達率 90%	96.1%	70.8%	83.3%

(3) 総評

平成 23 年度の自己点検の結果は、把握率が 95.0％と 9 割を超える高い水準を確保しています。

これは、自己点検を実施する職員の負担軽減を図るため、イントラネットを活用し、簡便に自己点検を実施できるよう技術的な対策を講じたことに加え、様々な周知普及の対策実施の効果として、情報セキュリティ対策の必要性に関する職員の意識が高まってきたことによるものと考えられます。

なお、対策の実施率は、把握率と同様高い水準にあるものの、主体別に見ると行政事務従事者（一般職員）において、「情報の作成及び入手時の対策」に係る事項がやや低い割合となるなどの傾向が見られました。

また、到達率についても、行政事務従事者（一般職員）においてやや低い水準に留まるなどの傾向が見られ、今後の改善すべき課題と考えています。

５．２　情報システムごとの状況

(1) 重点検査について

当省で導入している情報システムの公開用 Web サーバ及び電子メールサーバに対する情報セキュリティ対策に関して、政府機関統一基準群で定められた遵守事項の実施状況に係る重点的な検査（以下、「重点検査」という。）を実施致しました。

具体的には、当省ホームページの公開用 Web サーバ及び電子メールサーバを対象に、それぞれに搭載しているＯＳ等のソフトウェアのセキュリティパッチの適用状況や不正アクセス、不正プログラム対策等の情報セキュリティ対策実施状況について、内部調査を行い確認致しました。

平成 23 年度の重点検査の結果は、公開用 Web サーバ及び電子メールサーバに対する情報セキュリティ対策の実施率が 100％であり、適切に情報セキュリティ対策が講じられていることが明らかとなりました。

表５　重点検査の評価

評価	対策の実施率	対策状況
A	x＝100%	適切に実施すべき対策について、全ての項目で統一基準に準拠した対策が実施されている。
B	80%≦x＜100%	適切に実施すべき対策について、概ね全ての項目で統一基準に準拠した対策が実施されているが、一部の項目で不十分なものが含まれている。
C	60%≦x＜80%	適切に実施すべき対策について、不備の項目が一部に見られるなど、対策が遅れている。
D	x＜60%	適切に実施すべき対策について、不備の項目が相当数見られるなど、対策が著しく遅れている。

表６　公開 Web サーバの重点検査項目

対策の種類	重点検査項目
HTTPS 通信対応	・SSL バージョン 2 の無効化状況 ・SSL 通信で弱い暗号方式の無効化状況
Dos 攻撃等対策	・大量送信型のサービス不能攻撃（Dos 攻撃、DDos 攻撃）への対策の状況
OS の最新化	・OS の最新化の状況（パッチ適用（アップデート）の状況）
アプリケーションの最新化	・ウェブサーバアプリケーションの最新化の状況（パッチ適用（アップデート）の状況）

表７　電子メールサーバの重点検査項目

対策の種類	重点検査項目
OS の最新化	・OS の最新化の状況（パッチ適用（アップデート）の状況）
アプリケーションの最新化	・電子メールサーバアプリケーションの最新化の状況（パッチ適用（アップデート）の状況）

(2) 情報システムの対策状況

平成 23 年度の重点検査における情報システムの対策状況は、以下の結果となりました。

- 公開用 Web サーバ

  全ての公開用 Web サーバの HTTPS 通信の対応、Dos 攻撃等への対策、OS の最新化等の対策事項の実施率は、全て 100％を達成しています（評価：A）。

- 電子メールサーバ

  全ての電子メールサーバの SPF 認証対応、OS やアプリケーションの最新化等の対策事

項の実施率は、全て 100%を達成しています（評価：A）。

(3) 総評

当省では、情報システムの情報セキュリティ対策は適切に対策を講じており、平成 23 年度の重点検査の結果、全ての情報システムの情報セキュリティ対策について、100%の実施率となっています。

今後も、この状態を継続して維持するよう、引き続き適切な情報セキュリティ対策の実施に努めて参ります。

(4) 特筆すべき事項

当省の全職員が利用している基盤情報システムにおいては、外部からの不正アクセス等の攻撃への対策や迷惑メール（スパムメール）対策を実施しています。

特に、インターネットと内部ネットワークとの接続ポイントにおいて、各種のフィルタリング機能を有するファイアウオールを設置し、また外部から内部及び内部から外部への通信状況を 24 時間監視し、不正な通信を確認した場合には、当該通信を遮断するなどのセキュリティ対策を実施しています。

これにより、不正アクセスやウイルス感染等を未然に防ぐなど的確な対応を図り、特に電子メールを介した攻撃等については、職員に到達する前にそのほとんどをブロックしています。

５．３　教育・啓発

(1) 教育

- 教育計画の策定、教育の企画等

情報セキュリティ対策を着実に取り組んでいくためには、職員一人一人が情報セキュリティ関連規程に基づく具体的な情報セキュリティ対策を理解し、日々実践していくことが大切です。そのためには、各職員に対し、情報セキュリティ教育を行うことが必要です。

当省では、毎年度、e-learning 及び集合研修により情報セキュリティ教育を実施しています。平成 23 年度には、秘書課にて実施する服務研修と連携し、課室情報セキュリティ責任者に対する情報セキュリティ対策に係る集合研修を実施するなど研修効果を高めるとともに、全職員に対する e-learning による研修を実施しました。

一般職員に対しては、イントラネットに e-learning システムを導入し、各職員が執務室の机上のパソコンでいつでも学習ができる環境を整備しています。

また、新規採用職員や情報システム関係職員に対しては、異動時などに必要な情報セキュリティ教育を集合研修により実施しています。

その中で、特に情報セキュリティ教育の効果が大きいと考えられる新規採用職員に対

しては、組織における情報セキュリティ確保の重要性や具体的に取り組むべき具体的対策について、十分理解できるような内容として適宜見直しを図っています。

- 対象者の役割に応じた教育教材の整備

  課室情報セキュリティ責任者、一般職員及び新規採用職員等を対象とした情報セキュリティ教育の教材をそれぞれ整備しています。

  平成23年度は、課室情報セキュリティ責任者、一般職員を対象とした情報セキュリティ教育の教材を見直すとともに、近時多数発生している標的型メールへの対応等を追加致しました。このコンテンツの内容は、NISCの主催した標的型メールの教育訓練において作成されたもので、全職員がこの訓練に参加し標的型メールの実態を体験することにより、より身近にセキュリティの重要性を理解するきっかけとなるなど職員の意識がこれまで以上に高まり、教育の効果を高めました。

- 教育受講状況の管理

  e-learningを利用した教育コンテンツについて、受講の有無、確認テストの成績等の受講状況を管理し、理解度の確認を行っています。全職員に対するe-learningによる研修の確認テストでは、満点を獲得しない場合には履修済みとしなかったため、受講者は研修内容を十分理解するまで確認テストを受けることとし、その理解度の徹底を図りました。

- 情報セキュリティ対策担当者の知識向上等

  情報セキュリティ対策に関するセミナー等への参加等により、情報セキュリティ対策担当者の知識向上を図っています。

(2) 情報セキュリティ対策等資料参照の容易化

情報セキュリティ関連規程や職員が取り組むべき具体的な情報セキュリティ対策等の資料をイントラネット（情報セキュリティコーナー）に掲載し、職員が容易に参照できるよう環境を整備しています。

平成23年度は、情報セキュリティ対策に係る運用手続きや体制整備に関する関連資料や経済産業省情報セキュリティポリシーの改正、標的型メールの対応方法、クラウドサービス利用のための情報セキュリティマネジメントガイドライン等に加え、NISCから提示のあった「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」などをイントラネットの情報セキュリティコーナーに掲載しました。

５．４　調達・外部委託

(1) 外部委託先の管理

情報システム開発等の業務を外部に委託して実施する際には、当省の求める情報セキュリティ水準が委託先においても確保される必要があります。

このため、当省では、委託先が受託業務を実施する際の情報セキュリティ対策に関して、契約時、実施時、納品時それぞれにおいて遵守すべき事項を記載した調達仕様書のひな型を整備しその適用を図っています。

これにより、情報システムの開発等の外部委託時に、外部委託先に求める情報セキュリティ対策に関し、各システムの調達担当者が調達仕様書に遺漏なく反映できるようにしています。

また、調達仕様書に外部委託先における情報セキュリティ対策の体制整備や履行状況の確認に関する条項を盛り込むことにより、契約期間中の情報セキュリティ対策の体制整備や履行状況を確認し、履行状況が不十分であった場合の対策が確実に講じられることを担保しています。これに基づき、外部委託先が実施する情報セキュリティ対策の実施状況について、確実に実施できているかどうか、その確認を契約履行期間中及び納品時に実施することとしています。

具体的には、作業に使用するソフトウェアのパッチ適用や、セキュリティホール対策、不正プログラム対策、ファイル交換ソフト対策、アクセス制御対策、情報漏えい対策等を講じるとともに、契約期間中にこれらの対策に関する情報セキュリティ教育を作業担当者に実施し、また、当該業務に係る情報の管理状況等について確認することとしています。

また、委託先を選定する際、情報セキュリティ上重要な案件に関しては、情報セキュリティマネジメントシステムに関する適合性評価制度（ISMS）に基づく認証を取得していることを応札条件とするなど、外部委託先候補の情報セキュリティ水準を踏まえた調達手続きに取り組んでいます。

なお、近時、各課室から委託等で構築・運用している Web サイトが多数散見されることから、それら Web サイトの信頼性向上や脆弱性低減のため、必要なセキュリティ対策を図ることとし、各種の注意喚起を行っております。

（注意喚起例）

・仕様書に「情報セキュリティに関する事項」を記載すること。

・Web サイトのドメインは「.go.jp」とすること。

・なりすまし防止対策（SPF レコード）を設定すること。

（※）SPF：Sender Policy Framework

５．５　その他取り組んだ事項

(1) 検疫システムの導入

検疫システムを導入し、職員が使用している端末（パソコン）のＯＳ等のセキュリティパッチが適用されていない場合やウイルス対策ソフトのパターンファイルが最新のものになっていない場合には、省内ネットワークへの接続を拒否し、強制的に最新状態にした上で、省内ネットワークに接続できるようにしています。

これにより、対策が施されていない端末（パソコン）や不正な端末の省内ネットワークへの接続防止を図っています。

(2) 情報漏えい防止サービスの利用周知

情報漏えい防止の観点から、取り扱う電子ファイル（PDF ファイル）に対して細かくアクセス制限の設定を可能とする仕組み（情報漏えい防止サービス）の利用率が低いため、職員にその活用促進について周知しました。

この機能は、電子ファイルを参照できる者を限定する設定や複製及び印刷を制限する設定を可能とする機能を有しており、これらの設定を行うことにより、アクセス権のない者にはファイルの内容を参照することができないよう、また複製や印刷ができないよう制御が可能となります。

これにより、当該 PDF ファイルを USB メモリ等の外部記録媒体で省外へ持ち出し、万一紛失した場合やメールに誤って添付し省外に送信した場合であっても、情報漏えいのリスクを低減することが可能となります。

(3) 暗号化機能付き USB メモリの導入

暗号化機能付きの USB メモリを導入し、職員が情報を省外に持ち出す必要がある場合には、この USB メモリを使用することとしています。これにより、万一 USB メモリを紛失した場合であっても、情報漏えいのリスクの低減が図られることとなります。

(4) 情報セキュリティ対策実施状況の自己点検の自動化

毎年度実施している情報セキュリティ対策の実施状況の自己点検の実施において、平成 20 年度から e-learning システムの機能を活用して、職員が簡便に自己点検を実施できるようにしています。

これにより、職員毎の自己点検実施状況がリアルタイムに把握できるため、自己点検未実施者向けに自己点検実施の督促が容易になり、提出率の向上に寄与しています。

また、自己点検結果の集計作業についても、多大な労力を要することなく集計可能となり、集計・分析作業の効率化を図っています。

6　情報セキュリティに関する障害・事故等の概要

平成 24 年１月 29 日に、当省の委託事業にて運用を行っているウェブサイトがサイバー攻撃を受けて一部のページが改ざんされ、同サイトの趣旨と無関係なページが表示される事案が発生致しました。同サイトは同日中に復旧を行いました。なお、同サイトへのウイルス感染や情報流出は確認されませんでした。

また、平成24年２月３日に、特許庁の端末がウイルス感染していたことが判明しました。発見したウイルスは、２月５日までに庁内全ての端末から駆除（感染していたのは３台）を済ませました。なお、特許出願等に係る未公開情報について、ウイルス感染による流出は確認されませんでした。

当省では、コンピュータウイルスの駆除やパターンファイルの適用などシステム上の対処を迅速に行うとともに、不審なメールは開かない（不審な URL はクリックしない）よう求める職員向け注意喚起を重ねて行うとともに、内閣官房情報セキュリティセンター等の関係機関と連携を図り必要な情報提供・情報共有など対処を行いました。

7　情報セキュリティ対策に関する平成 24 年度の計画

平成 24 年度は、23 年度に続きセキュリティ管理規程において実施することとされている情報セキュリティ対策に関する自己点検及びセキュリティ監査を実施するとともに、情報システムの重点検査を実施致します。また、24 年度は、更なる情報セキュリティの向上を目指し、以下の取組を実施して参ります。

・省内各課室の情報管理に係る運用手続きや体制整備について、その実施状況を適宜把握するとともに、必要により改善事項の指摘や改善状況の把握等に努めて参ります。
・基盤情報システムの更改により、機密性の高い情報の漏えい防止の徹底に向けたアクセス制限付きフォルダの活用や情報漏えい防止サービス、新たな認証システムなどの技術的手段の活用を推進し、更なる高度化を図って参ります。
・情報セキュリティ研修等において、標的型メールへの対応（訓練や注意喚起等）や当省関連の Web サイト改ざんへの対応等について、重点的に実施して参ります。

おわりに

行政サービスの効率化及び高度化、オープンガバメント等の日々高まるニーズに対して、行政機関では、ＩＴの利活用を推進しています。行政機関でＩＴの利活用を推進するためには、クラウドサービス、スマートフォン、タブレット端末、電子書籍等の非常に進歩の早い新たな情報技術を有効的に取り入れていく必要があります。

一方、近年の重要インフラ、行政機関等に対する標的型サイバー攻撃事案は、従来、高度な技術を使った興味本位と思われる単発的な情報システムへの攻撃が、特定の社会的な目的を持ったサイバー攻撃に変質してきたことを示しています。

そのため、行政機関では、安全・安心な行政サービスを提供するには、新たな情報技術を取り入れつつ、積極的に情報セキュリティ対策に取り組む必要があります。特に、経済産業省は、情報産業を所管すると共に、電子政府を強力に推進しており、自ら率先して情報技術の効果と情報セキュリティのバランスを図りつつ、ＩＴの利活用を推進していくことが重要です。

当省では、必要性及び有効性を検討しながら、情報セキュリティ対策のための情報技術を導入しています。また、導入した情報技術や経済産業省情報セキュリティポリシーを有効かつ効果的に利活用するために、各課室での情報の格付と取扱実施の徹底及び定着化を推進し、総合的な情報セキュリティ対策に取り組んでいます。

最高情報セキュリティアドバイザー及び CIO 補佐官としては、電子政府及び経済産業省の業務効率化の推進、職員の生産性向上と情報セキュリティの確保のバランスを念頭において、総合的な改善・推進を今後も支援していく所存です。今後も、経済産業省が電子政府の模範となるよう努めて参りたいと思います。

最高情報セキュリティアドバイザー
（経済産業省 CIO 補佐官）
満塩　尚史