金融庁情報セキュリティ報告書
（平成２３年度版）

平成 24 年５月

【目　次】

～最高情報セキュリティ責任者のメッセージ～

金融庁の行政の政策目的は、金融システムの安定、利用者の保護・利用者利便の向上、公正・透明な市場の確立です。

金融庁では、これらの目的を達成するため、以下をはじめ、様々な場面で、情報システムを積極的に活用しています。

・投資家等が、公平・迅速に企業の財務情報等を入手できるよう、電子的に情報を開示する「有価証券報告書等電子開示システム」（EDINET）を整備。
・民間金融機関等の検査・監督や、市場のルール遵守状況の監視等を行うため、日々、電子的に民間金融機関や市場関係者等から報告や資料の提出を受け、その内容について、金融庁の内部で、各種の情報システムを用いて整理・分析。

このように、金融庁において活用している情報システムは、金融資本市場における重要な情報インフラの一部を構成するとともに、個別の民間金融機関や市場関係者の情報等、非常に機密性の高い情報を取り扱っているという特徴があります。

このため、金融庁においては、従来から、情報セキュリティ対策の重要性を強く認識し、積極的に取組みを進めてきたところです。しかしながら、近年、情報通信に関する環境の変化や技術の進展等は著しく、特に、政府関係機関等において、標的型攻撃などといったサイバー攻撃等による情報漏えい事案等が発生していることから、金融庁においても情報セキュリティ対策を推進する態勢の整備が、ますます重要になっていると考えております。

以上を踏まえ、金融庁では、平成 24 年度以降も、新たなリスク・脅威に適切に対応する不断の努力を続けるとともに、職員の意識の更なる向上と実施の徹底を図るため、情報セキュリティ教育・訓練の一層の充実に努めて参ります。

平成 24 年５月
最高情報セキュリティ責任者
（金融庁総務企画局総括審議官）
森 信親

１．平成 23 年度の総括及び 24 年度の取組方針

（１）平成 23 年度の評価

平成 23 年度においては、以下のような情報セキュリティ対策を実施しました。

①　情報セキュリティ自己点検

全職員、対象となる情報システムに対して、情報セキュリティ対策実施状況について、81 の調査項目に関する自己点検（以下「情報セキュリティ自己点検」という。）を行った結果、81 項目中 73 項目（90.2%）が実施率 100%の項目となるなど概ね適切に実施されていることが確認できました。残る８項目についても、実施率 100%となるよう、改善を図っていきます。

②　技術的情報セキュリティ対策

全ての情報システムのウェブサーバ、電子メールサーバ等の機器を対象に、技術的な情報セキュリティ対策（以下「技術的セキュリティ対策」という。）の実施状況に関する検査を行った結果、全ての検査項目で適切に実施されていることが確認できました。

今後とも、この状態を維持するよう、適切な技術的セキュリティ対策の実施に努めてまいります。

③　情報セキュリティ教育

全職員に情報セキュリティに関する研修を浸透させるため、情報セキュリティ研修を年度中に 12 回開催し、最近頻発している標的型攻撃の概要、対応策も説明しています。

研修の受講率は改善し、情報セキュリティ対策に関する理解は着実に浸透していますが、業務時間中に実施される情報セキュリティ研修について、業務多忙な職員が受講できるよう、研修の開催時間等の工夫を図っていくこと、情報セキュリティ研修の未受講者に対する課室長からの受講の勧告を行うことなどにより、今後とも、受講率の更なる引上げに努めてまいります。

④　外部委託先の管理に関する取組み

情報システムの開発・運用等の業務を外部に委託する場合において、外部委託先事業者が実施すべき情報セキュリティ対策については、調達仕様書に必ず記載するよう、調達仕様書の記載要領を整備する等の取組みを行いました。

外部委託先事業者が実施すべき情報セキュリティ対策が調達仕様書に必ず記載されるようになることで、契約締結時点で外部委託先事業者との間で遵守事項や対策水準について合意が形成され、また、プロジェクト遂行の中で合意に基づく確認を実施していくことで、情報セキュリティ対策の実効性を高めるための態勢が整備されました。今後とも、外部委託先の管理の向上に努めてま

いります。

⑤　業務継続計画の改定等

首都直下地震を想定した「金融庁業務継続計画」については、東日本大震災の発生を踏まえ、平成 23 年 12 月に職員の参集体制の強化等、所要の改定を行いました。

今回の「金融庁業務継続計画」の改定により、国民等のほか、財務局や自主規制団体等の対外的な利用者に影響が生じるおそれがある情報システムについて、非常時優先業務に準じ、個別マニュアルを作成することとしました。

更に、東日本大震災の発生を踏まえ、当庁で現在運用している主な情報システムについて対策状況を点検した結果、一部対策が不足している項目について、所要の改善を行いました。

（２）　平成 24 年度の取組方針

平成 24 年度においては、以下のような取組みを実施して、更なる情報セキュリティの改善に努めてまいります。

①　情報セキュリティ自己点検の実施
②　技術的セキュリティ対策の推進
③　情報セキュリティ教育・訓練の充実
④　情報セキュリティ監査の実施
⑤　情報セキュリティ対策ロードマップの策定
⑥　金融庁 CSIRT(Computer Security Incidents Response Team)の設置

２．報告の基本情報

（１）金融庁の基本的な情報

① 金融庁の概要

金融庁は、金融システムの安定、利用者の保護・利用者利便の向上、公正・透明な市場の確立という三つの大きな政策目的を達成するため、以下のような事務を行っています。

（ア）金融制度の企画立案に関すること
（イ）銀行、保険会社、金融商品取引業者等の民間金融機関、金融商品取引所等の市場関係者などに対する検査・監督に関すること
（ウ）有価証券届出書、有価証券報告書その他の書類の審査・処分に関すること
（エ）企業会計基準の設定その他の企業の財務に関すること
（オ）公認会計士及び監査法人に関すること
（カ）金融商品取引に係る法令遵守状況等の監視に関すること
（キ）金融に関する広報、研修に関すること　　等

② 金融庁の主な情報システム

金融庁の主な情報システムとしては、以下のようなものがあります。

（ア）金融検査監督データシステム
民間金融機関等に対する検査・監督を支援するシステム
（イ）証券総合システム
金融商品取引業者等に対する検査等を支援するシステム
（ウ）電子申請・届出システム
金融庁に対して行われる申請・届出を電子的に受け付け、受付結果の通知等を行うシステム
（エ）「金融商品取引法に基づく有価証券報告書等の開示書類に関する電子開示システム」（EDINET）
有価証券届出書、有価証券報告書、その他の書類について、一連の手続き等を電子的に行い、インターネット上で情報を開示することにより、投資家等による情報へのアクセスの平等・迅速化を図るシステム
（オ）公認会計士試験システム
公認会計士試験の実施に関する業務を支援するシステム
（カ）金融庁ウェブサイトシステム
金融庁の行政情報を、インターネットを通じて国民に提供するとともに、

国民から提供される情報を受け付けるシステム

（キ）金融庁ネットワークシステム

情報交換・情報共有等、職員の業務遂行を基盤として支えるシステム

（２）対象とする期間

本報告書が対象とする期間は、原則として平成 23 年４月 1 日から 24 年３月 31 日までの１年間です。

（３）対象とする組織

本報告書が対象とする組織は、金融庁の内部部局（総務企画局、検査局及び監督局)、証券取引等監視委員会事務局及び公認会計士・監査審査会事務局（以下「各局等」という。）です。

（４）対象とする情報

本報告書が対象とする情報は、「金融庁情報セキュリティポリシー第３版」（平成 21 年 11 月 11 日）に、以下の①～③のとおり規定されています。

① 情報システム内部に記録された情報

② 情報システム外部の電磁的記録媒体に記録された情報

③ 情報システムに関係がある書面に記載された情報

（注１）対象となる情報には、作業途上の文書も含まれます。また、上記③の「情報システムに関係がある書面」には、電磁的に記録されている情報を出力した書面や、情報システムに関する設計書等が含まれます。

（注２）「金融庁情報セキュリティポリシー」（以下「セキュリティポリシー」という。）は、内閣官房情報セキュリティセンターが策定している「政府統一基準」（以下「政府統一基準」という。）に準拠して策定しています。

（５）責任部署

本報告書の責任部署は、総務企画局総務課情報化・業務企画室であり、連絡先は、総務企画局総務課情報化・業務企画室情報化推進業務企画係です。

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

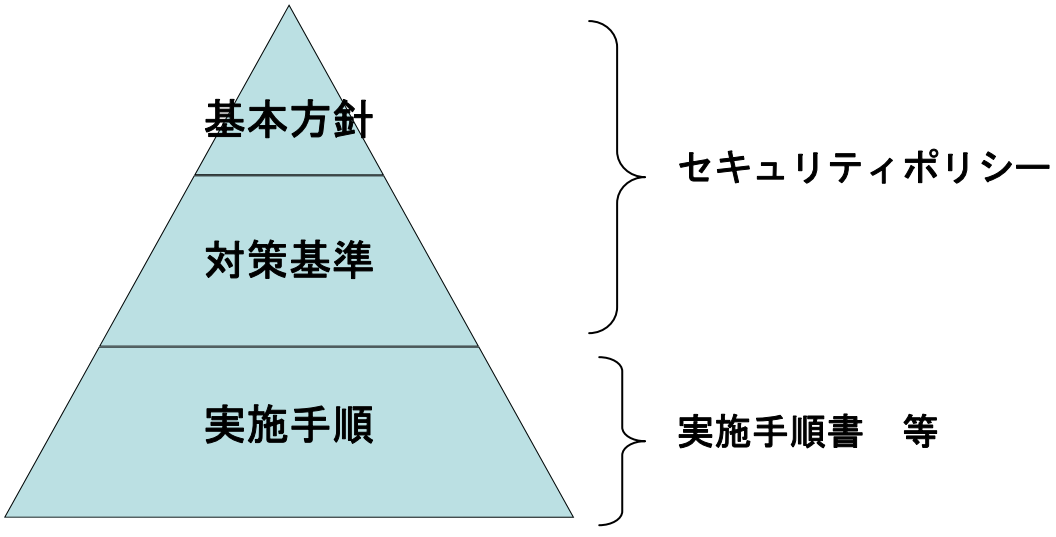
①　情報セキュリティ対策の基本方針及び対策基準等

情報セキュリティ対策の基本的な考え方（基本方針）及び具体的な情報セキュリティ対策を規定するもの（対策基準）として、セキュリティポリシーを定めています。

また、セキュリティポリシーに定められた情報セキュリティ対策を実施するための手順を定めた文書として、以下に掲げる 11 の実施手順書等を整備しています。（図１）

（ア）金融庁行政情報化 LAN システムにかかる実施手順
（イ）セキュリティポリシーに基づく例外措置実施手順
（ウ）情報システム障害等対応手順
（エ）外部委託における情報セキュリティ対策実施規程
（オ）モバイル PC 利用手順
（カ）要機密情報を庁外にメール送信する際の実施規則
（キ）情報の格付け・取扱いに関する実施手順
（ク）機器等の調達における情報セキュリティ対策実施規程
（ケ）ソフトウェア開発における情報セキュリティ対策実施規程
（コ）金融庁外の情報セキュリティ水準の低下を招く行為の防止に関する規程
（サ）安全区域（サーバ室）管理規程

（図１）　情報セキュリティ対策に関する文書の位置づけ



② 各情報システムにおける運用管理規程の整備

情報システムの円滑な運用に資するため、セキュリティポリシーに沿って、個々の情報システム毎に運用管理規程を整備しています。

③ 情報セキュリティ対策に関する文書の理解を深めるための方策

情報セキュリティ対策に関する文書について、職員が利用する金融庁ネットワークシステムのポータルサイトから参照できるよう、整理の上、掲載しています。

（２）情報セキュリティ対策の推進体制

① 行政情報化推進会議

情報セキュリティ対策に関する事項を総括し、セキュリティポリシーの承認等の重要事項の決定や、重要事項に関する関係部署との連絡及び調整を行う組織として設置されています。座長は、総括情報セキュリティ責任者が務めます。

② 総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事務を統括します。総括情報セキュリティ責任者は、総務企画局総括審議官が務めます。

③ 次席総括情報セキュリティ責任者

総括情報セキュリティ責任者を補佐して、下記④の主任情報セキュリティ責任者を統括するとともに、関係規程の整備や情報セキュリティ教育を実施します。次席総括情報セキュリティ責任者は、総務企画局総務課長が務めます。

④ 主任情報セキュリティ責任者

各局等において、情報セキュリティ対策に関する事務を統括します。主任情報セキュリティ責任者は、各局等の総務課長相当職の職員が務めます。

なお、主任情報セキュリティ責任者の下で事務を実施する情報セキュリティ担当者は、主任情報セキュリティ責任者所属課室の総務担当係長が務めます。

⑤ 情報システムセキュリティ責任者

情報システムを所管する課室において、情報セキュリティ対策の管理に関する事務を統括します。情報システムセキュリティ責任者は、情報システムを所管する課室の長が務めます。

なお、情報システムセキュリティ責任者の下で事務を実施する情報システム

セキュリティ担当者は、情報システムを所管する担当係長等が務めます。

⑥　課室情報セキュリティ責任者

職員の情報の取扱い、情報の庁外への持出しの許可等、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します。課室情報セキュリティ責任者は、各課室の長が務めます。

なお、課室情報セキュリティ責任者の下で事務を実施する課室情報セキュリティ担当者は、各課室の総務担当係長が務めます。

⑦　情報セキュリティ監査責任者

総括情報セキュリティ責任者の指示に基づき、情報セキュリティ監査計画の策定、監査の実施、監査結果に対する対応等、監査に関する事務を統括します。情報セキュリティ監査責任者は、総括情報セキュリティ責任者が指名することとされており、現在、総務企画局政策課情報セキュリティ担当補佐が指名されています。

⑧　情報セキュリティアドバイザー

総括情報セキュリティ責任者が定めた業務の内容等について、情報セキュリティ対策等の実施に関する助言等を行います。現在、情報セキュリティに関する専門的な知識及び経験を有する専門家が、情報セキュリティアドバイザーとして指名されています。

（３）情報セキュリティ監査

①　情報セキュリティ監査の概要

情報システムについての情報セキュリティ対策の改善に役立てることを目的として、政府統一基準及びセキュリティポリシーに基づき、毎年度、情報セキュリティ監査を実施しています。

情報セキュリティ監査については、情報セキュリティ監査責任者が実施するほか、監査の客観性及び専門性を担保するため、第三者である外部監査事業者が実施することとしています。

②　監査計画の策定

情報セキュリティ監査責任者は、毎年度、監査の実施計画を策定し、総括情報セキュリティ責任者の承認を得ることとしています。

③　監査の内容

原則、以下の（ア）から（ウ）の監査を毎年度実施することとしています。

（ア）　情報システムの脆弱性に関する監査

情報システムの情報セキュリティ水準が、セキュリティポリシーに定める要件を満たしているかどうかを確認する監査です。高度な技術を有する外部監査事業者が、金融庁の情報システムにアクセスを行うこと等により、情報システムの脆弱性の有無を確認します。

（イ）　実施手順書等のセキュリティポリシーへの準拠性監査

監査対象である実施手順書等の内容が、セキュリティポリシーに準拠しているかどうかを確認する監査です。

（ウ）　セキュリティポリシーの政府統一基準への準拠性監査

監査対象であるセキュリティポリシーの内容が、政府統一基準に準拠しているかどうかを確認する監査です。

平成 23 年度においては、セキュリティポリシーは改定されていないことから、監査対象としませんでした。

④　監査報告の実施

情報セキュリティ監査責任者は、監査報告書を作成し、総括情報セキュリティ責任者に報告することとしています。

⑤　平成 23 年度の監査結果及び監査指摘事項の改善状況

平成 23 年度に実施した、情報セキュリティ監査の指摘事項及びその改善状況は、以下のとおりです。

（ア）　情報システムの脆弱性に関する監査

監査の結果、情報システムの脆弱性に関する対策の実施状況は、概ね良好であると評価されました。

一部の事項について問題点が指摘されたことから、その改善に取り組んでおります。

（イ）　実施手順書等のセキュリティポリシーへの準拠性監査

監査の結果、実施手順書等の内容は、セキュリティポリシーに定める要件を満たしていることが確認されました。

４．平成 23 年度における情報セキュリティ対策の実施状況

平成 23 年度においては、情報セキュリティの観点から対策が必要な事項を整理した情報セキュリティ対策ロードマップを作成し、以下のような情報セキュリティ対策を実施しました。

（１）情報セキュリティ自己点検

①　情報セキュリティ自己点検の概要

各省庁は、政府統一基準に基づき、情報セキュリティ自己点検の結果を内閣官房情報セキュリティセンターに報告することが定められています。

金融庁においても、職員、課室長及び情報システム管理者を対象に、情報セキュリティ対策の実施状況を確認するため、情報セキュリティ自己点検を実施しました。

②　対象者

情報セキュリティ自己点検の対象は、各局等に所属する全職員です。

③　内容及び手法

情報セキュリティ自己点検は、平成 23 年 12 月中旬から 24 年２月下旬にかけて、全職員に対して共通の質問を行ったほか、課室長及び情報システム管理者に対しては、それぞれの業務に関連する追加質問を行い、回答の集計・分析を行いました。

④　平成 22 年度に実施した情報セキュリティ自己点検における課題と対策

【課題】全職員のうち回答した者の比率（回答率）は、99.9%でした。機密情報漏えい等の情報セキュリティ事故は、たった１人の不注意からでも生じうることから、全職員が情報セキュリティについて十分意識するよう、回答率の向上が必要です。

【対策】平成 23 年度は、点検結果を各課室で取りまとめの上、責任部署に報告する方式で実施し、実施忘れ等を防止しました。

⑤　平成 23 年度に実施した情報セキュリティ自己点検の結果

（ア）情報セキュリティ自己点検の回答率

全職員のうち回答した者の比率（回答率）は、100.0%であり、平成 22 年度の課題であった回答率は向上しました。

（イ）情報セキュリティ対策の実施状況

全職員、課室長及び情報システム管理者に対して実施した合計 81 の点検項目に係る情報セキュリティ対策の実施状況は、

・情報セキュリティ対策を実施すべき者の全員が実施している項目は、73 項目(90.2%)、
・95%以上の者が実施している項目は、79 項目（97.6%）
（95%以上 100%未満の者が実施している項目は、6 項目（7.4%））、
・90%以上の者が実施している項目は、80 項目（98.8%）
（90%以上 95%未満の者が実施している項目は、1 項目（1.2%））、
・90%未満の者が実施している項目は、1 項目（1.2%）

であることが確認されました。

情報セキュリティ対策の実施状況の詳細は、下表のとおりです。

（表）　　情報セキュリティ対策の実施状況の詳細

対象者	点検項目数	実施率100%の項目		実施率95%以上100%未満の項目		実施率90%以上95%未満の項目		実施率90%未満の項目	
		数	割合(%)	数	割合(%)	数	割合(%)	数	割合(%)
【共通の質問】全職員	6	0	0.0	6	100.0	0	0.0	0	0.0
【追加質問】課室長	51	50	98.0	0	0	1	2.0	0	0.0
情報システム管理者	24	23	95.8	0	0	0	0	1	4.2
合計	81	73	90.2	6	7.4	1	1.2	1	1.2
項目・割合(%)の累計	－	73	90.2	79	97.6	80	98.8	81	100.0

（ウ）評価

情報セキュリティ自己点検の結果、情報セキュリティ対策は、調査項目 81 項目中 73 項目（90.2%）が実施率 100%の項目となるなど概ね適切に実施されていることが確認できました。残る８項目についても、実施率 100%となるよう、改善を図っていきます。また、平成 22 年度の点検で明らかとなった安全区域（サーバ室）の入室時の遵守事項についての課題については、安全区域（サーバ室）入室時の確認を徹底した上で入室を許可する

こととするなど、改善しています。

（２）技術的セキュリティ対策

① 技術的セキュリティ対策の概要

金融庁の情報システムは、金融システムの安定に関わる情報など、非常に機密性の高い情報を取り扱っており、適切な技術的セキュリティ対策を実施する必要があります。

このため、以下のように、技術的セキュリティ対策の実施状況に関する検査を実施するとともに、新たなソフトウェアの導入等により、技術的セキュリティ対策の強化を実施しました。

② 技術的セキュリティ対策の実施状況に関する検査

全ての情報システムのウェブサーバ、電子メールサーバ等の機器を対象に、技術的セキュリティ対策の実施状況に関する検査を実施しました。

（ア）検査の結果

(a) ウェブサーバ

全てのウェブサーバに関し、不正プログラム対策、不正アクセス対策、情報保護対策（例：利用者権限管理）及びサーバ管理（例：管理者の権限管理）が適切になされていました。

(b) 電子メールサーバ

全ての電子メールサーバに関し、不正プログラム対策、情報保護対策（例：利用者の認証）及びサーバ管理（例：管理者の権限管理）が適切になされていました。

（イ）評価

技術的セキュリティ対策の実施状況に関する検査の結果、技術的セキュリティ対策は、全ての検査項目で適切に実施されていることが確認できました。

今後とも、この状態を維持するよう、適切な技術的セキュリティ対策の実施に努めてまいります。

③ 技術的セキュリティ対策の強化

職員の不注意による電子メールの誤送信により、情報漏えい事案に繋がることを防止するため、誤送信を軽減するためのソウトウェアを導入することとしました。

政府関係機関等において、標的型攻撃などといったサイバー攻撃等による情報漏えい事案が発生している事実を踏まえ、内閣官房情報セキュリティセンタ

ーが提供する不審メール情報に基づき、速やかに技術的な対応を行っています。

また、政府全体での情報共有の観点から、金融庁で受け付けた不審メール情報については、必要に応じて、内閣情報集約センターや内閣官房情報セキュリティセンターに速やかに報告しています。

（３）情報セキュリティ教育・訓練

① 情報セキュリティ教育の概要

金融庁では、全職員に情報セキュリティに関する理解を浸透させるため、各種の研修を実施しています。

特に、下記③（ア）の情報セキュリティ研修については、全職員に、最低１年に１回は受講させるため、同研修を年度中に 12 回開催しました。こうした取組みにより、平成 22 年度には情報セキュリティ研修の受講率は 92.0%でしたが、23 年度には受講率が 97.9%に改善しました。

職員の情報セキュリティ対策に関する理解は着実に浸透していると思われますが、一層の浸透に努めることが必要です。

このため、業務時間中に実施される情報セキュリティ研修について、業務多忙な職員が受講できるよう、研修の開催時間等の工夫を図っていくこと、情報セキュリティ研修の未受講者に対する課室長からの受講の勧告を行うことなどにより、今後とも、研修の受講率の更なる引上げに努めてまいります。

② 対象者

情報セキュリティ教育の対象は、各局等に所属する全職員です。

③ 研修の内容

情報セキュリティに関する研修の内容は、以下のとおりです。

（ア） 情報セキュリティ研修

全職員を対象に、情報セキュリティ全般に関する研修を実施しています。研修では、情報セキュリティの重要性、セキュリティポリシー、各種実施手順書等についての理解の促進、暗号化ソフトの使用方法、最近頻発している標的型攻撃の概要など、必要な事項を、具体的な対応策も含めて説明しています。

（イ） IT 基礎知識研修

新入職員及び受講希望者を対象に、情報技術に関する基礎的な事項の研修を実施しています。研修では、情報セキュリティに関する事項も含めて説明しています。

（ウ） 情報システム担当者研修

人事異動により各課室において新たに情報システムに関する事務を担当することとなった職員を対象に、業務上必要な関連知識や情報システムの運用管理に関する研修を実施しています。研修では、内閣官房情報セキュリティセンターが策定している「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」等の記載事項も踏まえつつ、情報セキュリティに関する事項も含めて説明しています。

（エ）他省庁主催研修

総務省が主催している情報システムに関する各種研修（情報セキュリティ関連講座を含む。）や内閣官房情報セキュリティセンターが実施する勉強会を、情報システムに関する事務を担当する職員が、積極的に受講するよう勧奨しています。

④ 情報セキュリティ対策訓練の実施

サイバー攻撃への速やかな対応という観点から、内閣官房情報セキュリティセンターが実施したサイバー攻撃訓練に参加し、省庁間での情報共有体制に問題がないか確認を行いました。

（４）外部委託先の管理に関する取組み

情報システムの開発・運用等の業務を外部に委託する場合には、外部委託先事業者において、金融庁の要求する情報セキュリティ水準が確保される必要があります。

このため、外部委託先事業者が実施すべき情報セキュリティ対策が調達仕様書に必ず記載されるようになることで、契約締結時点で外部委託先事業者との間で遵守事項や対策水準について合意が形成され、また、プロジェクト遂行の中で合意に基づく確認を実施していくことで、情報セキュリティ対策の実効性を高めるための態勢が整備されました。

① 調達仕様書の記載要領の整備

調達仕様書の記載要領を整備して、外部委託事業者が実施すべき情報セキュリティ対策を明確化し、上記（３）③（ウ）のシステム担当者研修において説明しました。

② 総務企画局総務課情報化・業務企画室等による点検

調達仕様書の作成に当たっては、各情報システムの所管部署の担当者が作成し

た調達仕様書の記載事項を必要に応じ、総務企画局総務課情報化・業務企画室の専門知識を有する職員及び情報セキュリティアドバイザーが点検しました。

また、調達仕様書の記載事項に不足がないか、情報化統括責任者補佐官に意見を求めました。

③ 実態調査の実施

調達仕様書の記載事項の実態を調査し、問題点の把握等を行いました。

今後も、必要に応じ、調達仕様書の記載要領の修正等を行う予定です。

（５）業務継続計画の改定等

金融庁では、平成 20 年６月に首都直下地震を想定した「金融庁業務継続計画」を策定し、主要な業務に関する業務を非常時優先業務と位置づけ、それぞれのシステム毎に業務継続のための個別マニュアルを策定しています。

東日本大震災の発生を踏まえ、平成 23 年 12 月、同計画改定に併せ、個別マニュアルを拡充し、業務継続の向上を図りました。

また、東日本大震災の発生、計画停電、電力供給の逼迫状況等を踏まえ、当庁で現在運用している主な情報システムについて、インフラや設備の障害、予期せぬシステム障害といった非常事態への対策状況を点検した結果、一部対策が不足している項目について、以下のような情報システムの基盤の強化を行いました。

・大規模災害による停電発生時においても、情報システムの安全な稼働を実現するため、無停電電源装置（UPS）の追加設置。

・金融庁情報システムのバックアップデータの遠隔地保管の更なる追加実施。

（６）その他

〇資産台帳の整備と活用

金融庁では、庁内の情報システムを対象に資産台帳を毎年度更新し、情報システムに関連する情報（システムの概要、ハードウェア・ソフトウェア構成、開発・運用費用等）を網羅的に整備しています。

これらの情報整備により、庁内の情報システムに関する状況を一元的に把握することが可能となっており、ソフトウェアに関する脆弱性情報への対応を促す場合等有効に活用しています。

５．情報セキュリティ対策に関する平成 24 年度の取組方針

平成 24 年度においては、以下のような情報セキュリティ対策を実施する予定です。

（１）情報セキュリティ自己点検の実施

情報セキュリティ自己点検の調査項目について、実施率が 100%とならなかった調査項目のフォローアップ調査を実施することで、改善を促していきます。

（２）技術的セキュリティ対策の推進

電子メールの誤送信を軽減するためのソフトウェアを導入し、庁内での本格的な運用を開始します。

（３）情報セキュリティ教育・訓練の充実

業務時間中に実施される情報セキュリティ研修について、業務多忙な職員が受講できるよう、研修の開催時間等の工夫を図っていくこと、情報セキュリティ研修の未受講者に対する課室長からの受講の勧告を行うことなどにより、今後とも、研修の受講率の更なる引上げに努めること、研修内容に標的型攻撃の手法、電子メール誤送信を軽減するための施策を盛り込むなど、情報セキュリティ教育の充実に努めてまいります。

また、内閣官房情報セキュリティセンターが実施する予定の不審メール受付訓練に参加し、金融庁の職員自らが不審メールの受信を体験することで、不審メールに対する対応能力の向上を図っていきます。

（４）情報セキュリティ監査の実施

情報セキュリティアドバイザーの指導を受け、情報セキュリティ監査の適切な実施に努めてまいります。

（５）情報セキュリティ対策ロードマップの策定

「機密性」（アクセスを許されていないものから守ること）、「完全性」（改ざん等されないように完全な状態を保持すること）、「可用性」（いつでも利用できる状態を保持すること）を確保するため、情報システムにとっての脅威を、①サイバー攻撃等外部からの攻撃、②人為的ミス、③内部者による犯行に分類した上で、必要な対策を網羅した上で、実施状況、今後の改善事項を一元的に管理する「情報セキュリティ対策ロードマップ」を策定します。

（６）金融庁 CSIRT(Computer Security Incidents Response Team)の設置

「情報セキュリティ対策に関する官民連携の在り方について」（平成 24 年１月

19 日情報セキュリティ対策推進会議決定）に基づき、情報セキュリティ事案が発生した際に緊急対応を行う金融庁 CSIRT を設置し、緊急対応態勢の強化を図ります。

６．おわりに　～最高情報セキュリティアドバイザーのメッセージ～

社会の情報システムへの依存度は高くなっています。例えば、氏名・住所・生年月日・性別・口座番号などといった種々の個人情報を、情報システムに入力する機会が増大しており、機密情報が外部に漏洩することによって情報システムへの信頼性が損なわれれば、現代の経済社会の存立基盤を揺るがすことになりかねません。

そういった状況下において、近年、大規模な情報漏えい、サイバー攻撃に関する報道が頻発しています。また、政府関係機関等においても、標的型攻撃などといったサイバー攻撃等による情報漏えい事案等が発生しています。

攻撃手法は日々進化しており、攻撃の痕跡が消去されている例もあると言われるなど非常に大きな脅威となっています。金融庁では、民間金融機関等から提出された機密性の高い情報を取り扱っていることから、高度の情報セキュリティ水準を維持していく必要があると認識しています。

このような状況に鑑み、金融庁では、情報システムにとっての脅威を、①サイバー攻撃等外部からの攻撃、②人為的ミス、③内部者による犯行に分類し、「機密性」（アクセスを許されていないものから守ること）、「完全性」（改ざん等されないように完全な状態を保持すること）、「可用性」（いつでも利用できる状態を保持すること）を確保するため、私自身も十分に関与した上で、情報セキュリティ対策ロードマップの策定を検討しています。

今後、「計画」・「対策実施」・「チェック」・「改善」のサイクルを作り上げ、継続的な情報セキュリティ対策の推進に努めていきます。

本情報セキュリティ報告書は、国民の皆様にご理解いただけるよう、金融庁の取組みの全体像を提示しました。平成 24 年度以降も、本報告書に記載された内容に基づき、情報セキュリティ対策の推進に向け、不断の努力を積み重ねていきたいと考えています。

金融庁最高情報セキュリティアドバイザー
村瀬　一郎