平成２３年度
情報セキュリティ報告書

平成 24 年 5 月
外　　務　　省

目　　次

１　最高情報セキュリティ責任者のメッセージ及び平成２３年度の総括　.....1
２　報告の基本情報.....2
（１）外務省の概要.....2
（２）対象期間.....2
（３）対象組織.....2
（４）対象情報.....2
（５）本報告書の責任部署.....2
３　情報セキュリティ対策の枠組み.....2
（１）情報セキュリティ対策に関する文書体系.....2
（２）情報セキュリティ対策の推進体制.....3
ア　最高情報セキュリティ責任者.....3
イ　情報セキュリティ委員会.....3
ウ　情報セキュリティ監査責任者.....3
エ　統括情報セキュリティ責任者.....4
オ　情報セキュリティ責任者.....4
カ　情報システムセキュリティ責任者.....4
キ　情報システムセキュリティ取扱責任者.....4
ク　最高情報セキュリティアドバイザー.....4
ケ　ＣＩＯ補佐官.....4
（３）監査等　.....5
ア　監査計画と実施.....5
（ア）関連規定に関する準拠性監査.....5
（イ）自己点検に関する監査.....6
（ウ）電子メールサーバの脆弱性監査.....6
（エ）公開ウェブサーバの脆弱性監査.....6
（オ）例外措置の申請及び許可状況に関する監査.....6
イ　監査結果と評価.....6
（ア）関連規定に関する準拠性監査.....6
（イ）自己点検に関する監査.....6

（ウ）電子メールサーバの脆弱性監査 6
（エ）公開ウェブサーバの脆弱性監査 6
（オ）例外措置の申請及び許可状況に関する監査 6
４　平成２３年度の重点事項の目標、実績及び評価 7
（１）重点事項の目標 7
ア　職員に対する情報セキュリティ対策についての意識啓発 7
イ　障害・事故等についてのより迅速かつ的確な対応方法の検討 7
（２）実績及び評価 7
ア　職員に対する情報セキュリティ対策についての意識啓発 7
イ　当省内のＣＳＩＲＴ体制の充実 8
５　情報セキュリティ対策の実施状況 8
（１）外務省情報セキュリティポリシーに関する自己点検結果 8
ア　課題と対策 8
イ　自己点検結果の状況 8
（ア）外務省全体の把握率 8
（イ）外務省全体の実施率 9
（ウ）外務省全体の到達率 10
ウ　総評 10
エ　自己点検の計画策定、結果に基づく改善指示等の状況 10
（２）情報システム毎の状況 11
ア　課題と対策 11
イ　情報システムの対策状況 11
（ア）公開用ウェブサーバ 11
（イ）メールサーバ 11
（ウ）ＤＮＳサーバ 11
ウ　総評 11
（３）教育・啓発 11
ア　各種集合研修における教育 11
イ　情報セキュリティ教育パンフレット 11
ウ　e ラーニング 12

エ　情報セキュリティ関連情報の収集と職員への提供 12
オ　ＣＩＯ補佐官による情報提供 12
カ　民間有識者による情報提供 12
（４）調達・外部委託 12
６　情報セキュリティに関する障害・事故等報告 13
（１）情報セキュリティに関する障害・事故等の把握 13
（２）ＣＳＩＲＴ体制の整備 13
（３）公表した障害・事故等の概要、それに対する対応等 13
ア　会計課調達室のウェブページ脆弱性 13
イ　本省と在外公館への標的型メール攻撃 14
７　情報セキュリティ対策に関する平成２４年度の計画 14
（１）職員に対する情報セキュリティ対策についての意識啓発 14
（２）当省内のＣＳＩＲＴ体制の充実 14
８　最高情報セキュリティアドバイザーメッセージ 15

１　最高情報セキュリティ責任者のメッセージ及び平成２３年度の総括

平成２３年度においては、インターネット上における種々の攻撃が増し、大手ゲーム関連会社を始めとする様々な会社や組織への不正アクセスを始め、分散型サービス不能攻撃(DDoS 攻撃)、さらには標的型メールによる攻撃（一部の個人を標的として巧妙なメールを送付し、ウィルス（マルウェア）付きの添付ファイルを開封させたり本文に記述したリンクから不正サイトへ誘導させることによりウィルス（マルウェア）に感染させ情報流出を図るとされるもの）が頻発し、防衛関連企業や立法府を含む政府機関が被害を受けたとの報道がなされました。

また、この種の攻撃に対する防御策としては、従来の外部から内部のネットワークへの入り口にファイアーウォールや侵入検知装置といった入口対策、内部に侵入したウィルス（マルウェア）が外部の不正サーバと通信をするのを防ぐ出口対策、さらには内部ネットワーク内でウィルスによる不審な挙動を早期に検知するためのログの監視の強化などが求められるようになりました。

一方、スマートフォンの爆発的な普及とともに、スマートフォンを狙ったウィルス（マルウェア）も急増し、業務上におけるスマートフォンの利用を見据えた情報セキュリティ対策も必要となってきています。

当省においても、特に春以降、多くの標的型メールが接到したことから、当省ネットワーク上でのウィルス（マルウェア）対策は、入口対策と出口対策を含め、今までと違ったよりきめ細かい対応を行っています。同時に、職員に対しても、セキュリティ対策の重要性の啓発、及びＵＳＢメモリを介した感染への注意喚起、並びに取り扱う情報の格付けに応じた保管・管理の徹底につき教育を実施してきました。

また、当省内におけるＣＳＩＲＴ（ＧＩＳＩＲＴと呼称）については、平成２３年２月に体制整備を行い、継続的な情報収集によるインシデント発生に備えた事前準備活動を展開し、インシデント発生時には迅速な対応が行えるよう普段から状況把握に努めるとともに、関係職員に対するＣＳＩＲＴの研修や演習を実施しました。更に、幹部を含めた職員のセキュリティに関する知識と意識も、向上してきていると考えております。

平成２４年度においても、引き続き情報セキュリティ対策に注力する所存です。

最高情報セキュリティ責任者
（外務省大臣官房長）
木寺　昌人

2　報告の基本情報

（1）外務省の概要

外務省ホームページでも紹介していますが、日本、そして世界の平和と繁栄のために、東京の本省と世界を結ぶ在外公館とのネットワークを通じて、国益を見据えた各国との友好関係の増進、情報収集や交渉、海外にいる日本人の保護、また、日本らしい国際貢献や日本の魅力を外務省ホームページ等による情報発信、といった様々な活動を通じて未来に向かって取り組んでいます。

（2）対象期間

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等に関する取り組みを対象としています。

（3）対象組織

本報告書の対象とする組織は、本省及び在外公館としています。

（4）対象情報

本報告書が対象とする情報は、「政府機関の情報セキュリティ対策のための統一規範」及び「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」並びに「政府機関の情報セキュリティ対策のための統一技術基準」（以下、「政府統一基準群」という。）の定義に基づき、以下の情報を対象としています。

・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（ＵＳＢメモリやＣＤ等）に記録された情報
・情報システムに関連する書面に記載された情報

（5）本報告書の責任部署

外務省大臣官房情報通信課

3　情報セキュリティ対策の枠組み

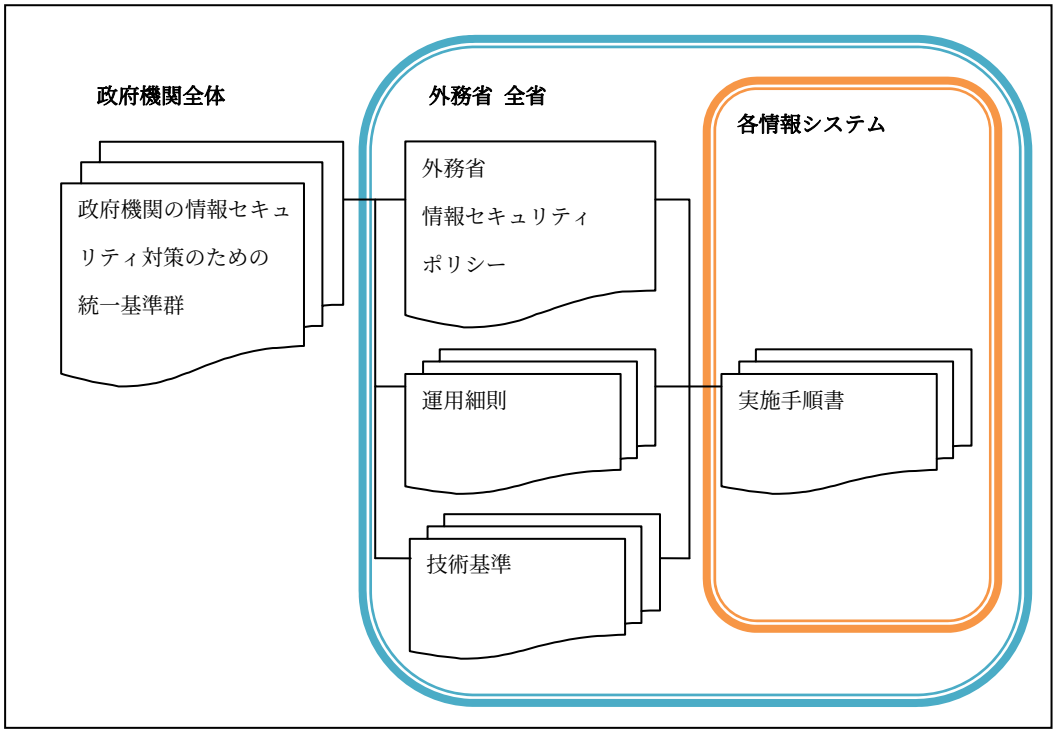
（1）情報セキュリティ対策に関する文書体系

外務省では、情報セキュリティの確保を目的として、政府統一基準群に準拠した「外務省情報セキュリティポリシー」及び同「運用細則」（以下、「運用細則」という。）並びに同「技術基準」（以下、「技術基準」という。）を定めています。また、個別の情報システムについては、各システムの構成を踏まえ、情報セキュリティ対策を具体的に定めた「実施手順書」を整備しています（図１参照）。

更に、機器等の調達や外部委託に際しての情報セキュリティ対策にかかる対応等に関しては、これを具体的に定めた「機器等の調達・外部委託解説書」を整備しています。

これらの情報セキュリティに関わる文書は、内閣官房情報セキュリティセンター（以下、「ＮＩＳＣ」という。）による政府統一基準群の見直し毎に準拠して改定しており、直近では平成２３年１０月に改定するとともに、省内の各情報システムのシステム構

成変更の際にも実施手順書を見直すなど、常に最新の状況に基づいた情報セキュリティ対策を実施してきています。



（図１）情報セキュリティ対策に関する文書体系

（２）情報セキュリティ対策の推進体制

外務省では、情報セキュリティ対策を推進するために、政府統一基準群及び外務省情報セキュリティポリシーに基づき、以下に示すとおりの体制を定めています（図２）。

ア　最高情報セキュリティ責任者

情報セキュリティに関する事務を統括しています。外務省では大臣官房長が務めています。

イ　情報セキュリティ委員会

外務省の情報セキュリティに関する重要事項の決定、及び関係部署との連絡調整を行う。メンバーは以下の通りです。

・最高情報セキュリティ責任者（委員長）
・情報セキュリティ監査責任者
・統括情報セキュリティ責任者
・監察査察室長、情報防護対策室長、外交記録・情報公開室長、人事課長、会計課長、在外公館課長

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します。外務省では大臣官房総務課長

が務めています。

エ　統括情報セキュリティ責任者

情報セキュリティ責任者を統括し、最高情報セキュリティ責任者を補佐します。外務省では大臣官房情報通信課長が務めています。

オ　情報セキュリティ責任者

本省においては各課室、在外公館においては各在外公館の情報セキュリティに関する事務を統括します。外務省では本省各課室においては課室長、在外公館においては在外公館長の指名する者が務めています。

カ　情報システムセキュリティ責任者

本省各課室または各在外公館が所管する情報システムの計画段階までに置かれ、各情報システムの情報セキュリティ対策に関する事務を統括します。情報システムを保有する課室または在外公館の情報セキュリティ責任者が兼務しています。

キ　情報システムセキュリティ取扱責任者

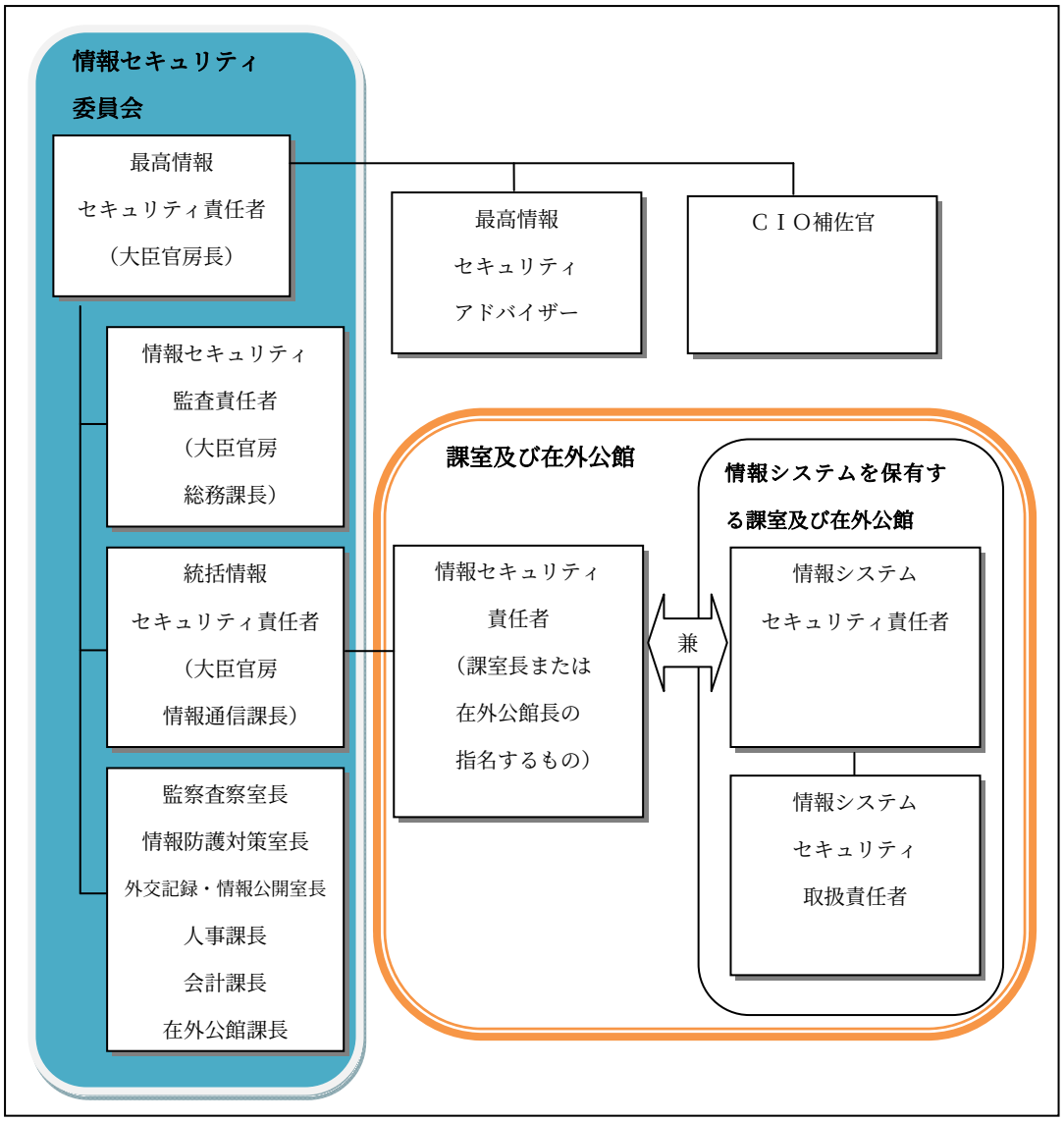
本省各課室または各在外公館が所管する情報システムの管理業務における情報セキュリティ対策を実施しています。本省においては各課室の情報システムセキュリティ責任者が、在外公館においては在外公館長が指名しています。

ク　最高情報セキュリティアドバイザー

最高情報セキュリティ責任者が、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーとして任命しています。

ケ　ＣＩＯ補佐官

政府における「電子政府構築計画」に基づき、外務省の情報化統括責任者（大臣官房長）および省内情報システムに対して、情報セキュリティ対策を含む支援・助言を行う専門家をＣＩＯ補佐官として任命しています。



（図２）情報セキュリティ対策の推進体制

（３）監査等

ア　監査計画と実施

外務省における情報セキュリティ対策が政府統一基準群及び外務省情報セキュリティポリシーに準拠しているか、適切に運用されているか等を確認するため、毎年度情報セキュリティ監査を実施しています。また、監査結果は情報セキュリティ対策の内容見直し、重点対策事項の検討、自己点検項目の検討等に活用することを目的としています。

平成２３年度においては、以下の監査を行いました。

（ア）　関連規定に関する準拠性監査

・平成２３年度は政府統一基準群改定に伴い外務省情報セキュリティポリシーを

改定したため準拠性監査を実施しました。

・各業務システムにおける情報セキュリティ対策の実施手順書が外務省情報セキュリティポリシーに準拠していることを確認するため、無作為抽出した業務システムの実施手順書に対し、外務省情報セキュリティポリシーの準拠性監査を実施しました。

（イ）自己点検に関する監査

自己点検が適正に実施されたこと等を確認するため、監査を実施しました。

（ウ）電子メールサーバの脆弱性監査

インターネットに接続している電子メールサーバに、外部からのリモートによる脆弱性が無いことを確認するため、外部専門家による監査を実施しました。

（エ）公開ウェブサーバの脆弱性監査

公開ウェブサーバのうち３システムを対象に、ＮＩＳＣにより、脆弱性の有無につき、監査が実施されました。

（オ）例外措置の申請及び許可状況に関する監査

例外措置の適用審査記録台帳が外務省情報セキュリティポリシーに従って管理がなされているかを確認するため、監査を実施しました。

イ　監査結果と評価

（ア）関連規定に関する準拠性監査

外務省情報セキュリティポリシー、運用細則及び技術基準が政府統一基準群の定める項目と比較したところ、問題となるようなものは無く準拠性を満たしていると判断しました。

また、対象とした業務システムの実施手順書についても外務省情報セキュリティポリシー、運用細則及び技術基準に対して、問題となるような対策項目の漏れはなく、準拠性を満たしていると判断しました。

（イ）自己点検に関する監査

対象とした主体に対し、質問・査閲により確認した結果、自己点検は適正に実施されたものと判断しました。

（ウ）電子メールサーバの脆弱性監査

委託先からの監査報告書の内容を確認し、外部監査人からの指摘があった事項は適切に対策が講じられるよう現在対応策につき調整中です。

（エ）公開ウェブサーバの脆弱性監査

ＮＩＳＣによる結果報告の事項について情報システムの主管課により対策が実施されました。この対策結果に対し、再度外部専門家による監査を実施し問題のないことを確認しました。

（オ）例外措置の申請及び許可状況に関する監査

例外措置の適用審査記録の台帳について、外務省情報セキュリティポリシーに

従った管理がなされていることを確認しました。

4　平成２３年度の重点事項の目標、実績及び評価

（1）重点事項の目標

外務省では、世界各国に設置している在外公館と連携して業務を行っています。そのため、全世界規模の様々な環境の中で業務に使用するための高度な安全を要求されるネットワークを維持し、運営しなければなりません。平成２１年度に在メキシコ大使館で不正アクセス事案が発生し、平成２２年度には在スウェーデン大使館でＵＳＢメモリが盗難に遭うなど、障害・事故等を１００％回避することは不可能との前提に立つと、まずは障害・事故等発生時に迅速に対応すること、同時に被害の極小化を図ることが重要と考えています。また普段からインシデントの発生に備えた事前準備体制を整えておくことも重要と考えています。

そこで、平成２３年度における情報セキュリティ対策については、基本的な対策に加え、以下の目標について重点的に取り組んできました。

ア　職員に対する情報セキュリティ対策についての意識啓発

従来から職員に対する情報セキュリティ教育を実施してきているが、外務省全体の情報セキュリティ意識を高く維持するために継続することが重要であり、引き続き全職員に対して定期的に意識啓発を図る。

イ　障害・事故等についてのより迅速かつ的確な対応方法等の検討（当省内のＣＳＩＲＴ(Computer Security Incident Response Team)体制の充実）

平成２２年度の重点事項にも掲げた通り、パソコンの盗難やウィルス付詐称メール、不正アクセスや大量アクセス攻撃（DDoS 攻撃）等、最近の多様化する脅威から外務省の情報システムを保護するため、より迅速かつ的確に障害・事故等に対応し、普段からの事前準備体制を整えるべく構築した当省内のＣＳＩＲＴ（ＧＩＳＩＲＴ：Gaimusho Information Security Incident Response Team と呼称）体制の充実を図る。

（2）実績及び評価

平成２３年度においても、普段からの情報収集により、より高度化した標的型メール攻撃、大量アクセス攻撃（DDoS 攻撃）等があるとの前提で、事前の職員への意識啓発と備えを実施するとともに、体制の充実を図りました。

ア　職員に対する情報セキュリティ対策についての意識啓発

職員一人一人の意識を啓発すべく、一般省員向けに外部専門家による研修を実施するとともに、特に情報セキュリティや情報システムに関わる課室を対象としても、説明会を開催するなど、意識啓発に努力してきました。また、省内ホームページや回章により、仮に不正アクセスがあっても保護すべき情報が漏洩することのないよ

う、繰り返し省内・在外の職員に保管する情報の整理・管理を徹底するよう周知してきました。

イ　当省内のＣＳＩＲＴ体制の充実

普段からの情報収集により、より高度化した標的型メール攻撃や不正アクセス、大量アクセス攻撃（DDoS 攻撃）等の脅威があるとの前提で、これに備えた対策として、情報漏洩を未然に防ぐべく、上記（１）のとおり職員への意識啓発をする対策を進めるとともに、情報セキュリティに関する事案発生時に迅速に対応するため、ＣＳＩＲＴ体制の更なる整備を推進しました。

また、特に標的型メール攻撃に対しては、職員への具体的な対処方法の周知に加え、ウィルス（マルウェア）情報等につきＮＩＳＣと継続的かつ密接に共有しました。同時に、専門家の意見を踏まえたフォレンジック調査等を含むウィルス（マルウェア）駆除作業を実施しました。

更に、情報セキュリティに関する事案発生時に迅速に対応するための支援体制推進の一環として、省内関係者へのＣＳＩＲＴに関する研修を実施するとともに、関係者によるサイバー演習を実施しました。

５　情報セキュリティ対策の実施状況

（１）外務省情報セキュリティポリシーに関する自己点検結果

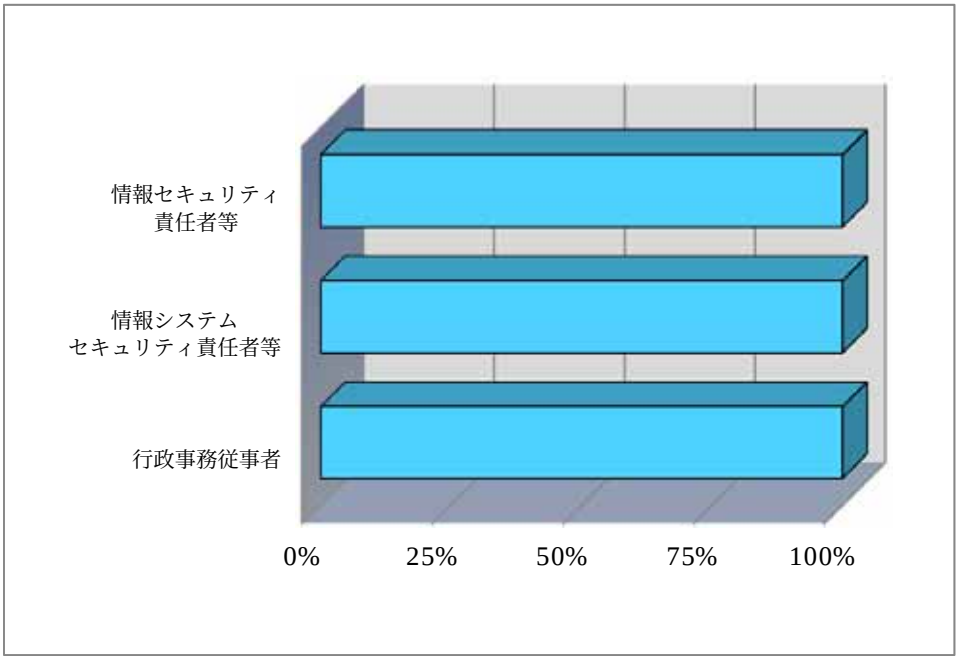
ア　課題と対策

外務省では、外務省情報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の実施状況を確認するため、平成１８年度から毎年度自己点検を実施しています。平成２３年度も当省における情報セキュリティ意識向上を目標に、外務省本省と全在外公館の全職員と情報システムを取り扱う勤務者（行政事務従事者）を対象として「自己点検」を実施しました。

イ　自己点検結果の状況

（ア）外務省全体の把握率

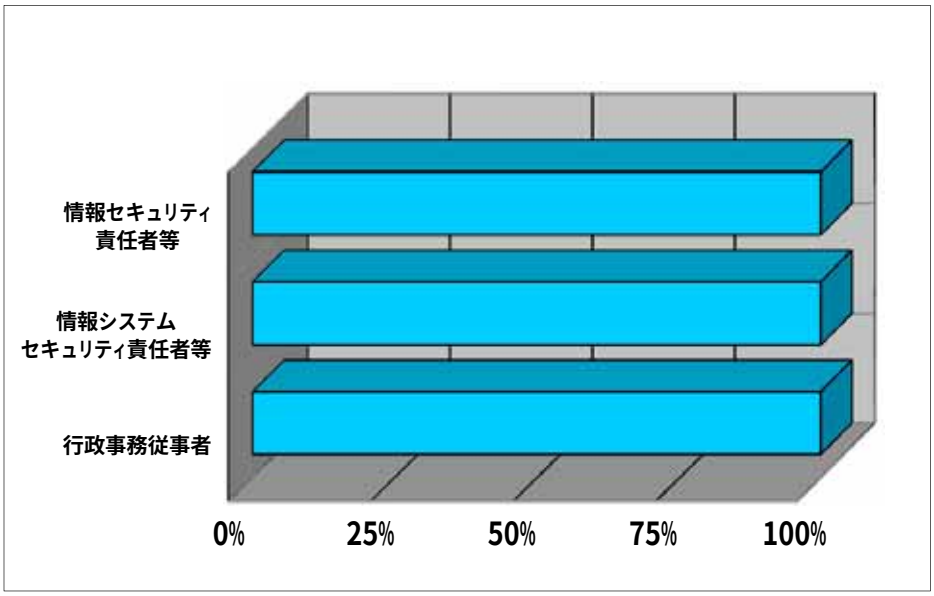
把握率とは自己点検対象者を母数に、実際に自己点検を実施した割合です。平成２３年度の把握率は１００％を達成（すべての対象者が自己点検を実施）しています（図３）。



（図３）職種別把握率

（イ）外務省全体の実施率

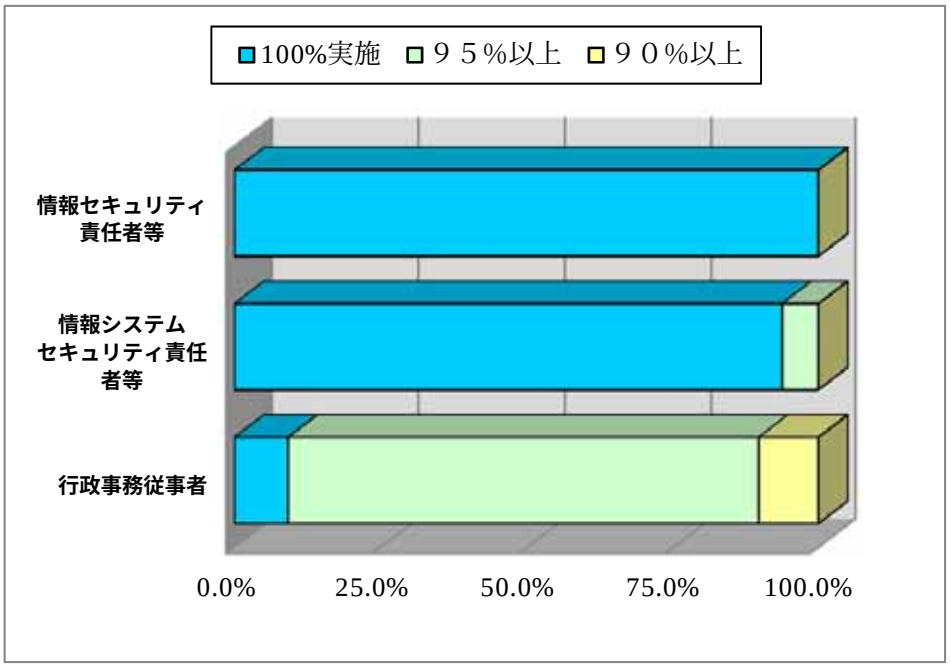
実施率は、把握した者のうち対策を「実施」と回答した者の割合です。自己点検結果として、実施主体別の遵守項目の平均実施率は平成２２年度より改善されています（図４）。



（図４）職種別実施率

（ウ）外務省全体の到達率

到達率とは、各遵守事項について、一定の割合（100%,95%,90%）以上の者が対策を実施した事項の割合です。平成２３年度の情報セキュリティ責任者等は１００％を達成しましたが、職員ならびに情報取扱勤務者の到達率において、１００％実施した項目数の比率が低い結果となっています（図５）。



（図５）職種別到達率

ウ　総評

把握率については自己点検開始以来１００％達成を継続しており、平成２３年度においても職員に対し電子的な自己点検実施の機会を拡大するなどの工夫を行い、把握率の維持に努めました。

実施率については情報セキュリティ責任者等及び情報システムに関わる情報システムセキュリティ責任者等については１００％となっており、責任者が高い情報セキュリティ意識を持っていることを示しています。他方、行政事務従事者についてはわずかに１００％達成に至らず、今後も情報セキュリティに関する教育・啓発が必要であると考えています。

到達率については、行政事務従事者の１００％実施項目の割合が低くなっています。これについては職員の教育方法等を改善し到達率の向上に繋がるよう努めます。

エ　自己点検の計画策定、結果に基づく改善指示等の状況

外務省では毎年度自己点検結果の分析を行い、その内容を職員に周知し、情報セキュリティ意識の向上に努めています。また、後述する e ラーニングシステムを活用し、職員の教育受講機会の拡大に努めることとします。

（２）情報システム毎の状況

ア　課題と対策

重点検査とは、ウェブサーバ及び電子メールサーバ並びにＤＮＳサーバにおいて政府統一基準群に準拠した情報セキュリティ対策が実施されているかを確認するために、ＮＩＳＣが実施している調査です。調査はＮＩＳＣが配付した調査票を基に実施しています。当省では、平成１９年度からすべての調査対象について実施率１００％を達成しています。

イ　情報システムの対策状況

（ア）公開用ウェブサーバ

対象サーバについて、不正プログラム対策、不正アクセス対策、情報保護対策、サーバ管理における対策事項の実施率は、過去２年間に引き続き２３年度もすべて１００％を達成しています。

（イ）メールサーバ

対象サーバについて、不正プログラム対策、不正アクセス対策、情報保護対策、サーバ管理における対策事項の実施率は、過去２年間に引き続き２３年度もすべて１００％を達成しています。

（ウ）ＤＮＳサーバ

対象サーバについて、不正プログラム対策、不正アクセス対策、情報保護対策、サーバ管理における対策事項の実施率は、すべて１００％を達成しています。

ウ　総評

ウェブサーバ及び電子メールサーバ並びにＤＮＳサーバについては、１００％を達成しています。今後も引き続き１００％を達成するよう政府統一基準群に基づく情報セキュリティ対策を実施していく予定です。

（３）教育・啓発

外務省では、職員の情報セキュリティ意識の向上を図るために、年度当初に「情報セキュリティ対策教育計画」を策定しています。

以下の各研修方法を採用することで、職員に年一回以上の情報セキュリティ教育の受講機会を提供し、「外務省情報セキュリティポリシー」を実現するために各職員の役割に応じた教育内容としています。

ア　各種集合研修における教育

外務省では年間を通して、人事に関わる集合研修及び情報システムの操作に関わる研修を実施しています。これらの研修の機会において、各研修の内容及び対象者の役割に応じ「外務省情報セキュリティポリシー」に基づいた情報セキュリティ教育を行っています。研修受講者の名簿により受講状況を把握しています。

イ　情報セキュリティ教育パンフレット

情報セキュリティ対策の基本に関わる事項の周知を目的として、全職員にパンフ

レットを配布しています。パンフレットは図や表を多用して分かりやすくなるように心がけています。自己点検の際に、点検項目として設定することで、浸透度を把握しています。

ウ　e ラーニング

情報セキュリティ対策の基本に関わる事項について、上記情報セキュリティ教育パンフレットよりも教育内容を詳細化するとともに、音声ガイドや動的な画面とすることで理解の向上を目指しています。また、情報ネットワーク基盤上に e ラーニングシステムを構築したことで、職員が受講を各自の業務都合に合わせやすくすることで受講率の向上も図っています。

受講状況は、e ラーニングシステムにより自動的に把握可能としています。未受講者に対するペナルティを付与するとの周知により受講を徹底させています。

エ　情報セキュリティ関連情報の収集と職員への提供

国内外において日々発生する情報セキュリティに関する情報（ニュース）を日々収集することにより、当省における情報セキュリティ上の脅威を早めに察知するとともに、取り得るべき対策を検討し、省内・在外への注意喚起を含め、システム上の対策に生かし、また、当該情報を省内・在外の関係職員にメール等により情報発信しています。また、標的型メールへの対策やソフトウェアの脆弱性情報など特に職員に注意を促すべき情報については、回章等の手段を用いて情報発信しています。

オ　ＣＩＯ補佐官による情報提供

情報システムに関わる省内・在外の職員を対象として、ＣＩＯ補佐官から情報セキュリティに関する最新情報を提供し、情報セキュリティ対策の検討や見直しに活用しています。

カ　民間有識者による情報提供

情報セキュリティに造詣の深い民間有識者を招いて職員に対し説明会等を開催し、意識啓発を図っています。

（４）調達・外部委託

外部委託先の管理

外務省では情報通信課とＣＩＯ補佐官が、情報システム保有課室と情報システムの調達から始まるライフサイクル全体について情報共有を行っています。

その情報共有の過程において情報通信課とＣＩＯ補佐官は情報セキュリティの観点から、調達仕様書、構築設計書及び運用設計書等の情報システム関連文書内容に助言し、また設計書に限らず運用時においても必要に応じて担当会社との会議に参加し、具体的な対策を提示しています。

この調達に関する仕組みにより、各情報システム保有課室に情報セキュリティに関する知識が蓄積され、年々情報セキュリティ対策レベルが向上してきています。また情報セキュリティ対策が情報システム関連文書に記述されることで、新たに調

達を行う際にも情報セキュリティ対策のレベルが保たれています。

また、情報システムに関わる契約時には「秘密保全に関する条項」が添付され、保秘や情報セキュリティ体制の構築と連絡体制の整備等を含む情報セキュリティ対策が契約として締結される手続きとしています。

第２８回情報セキュリティ政策会議で報告された「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」の中で「Ⅰ.標的型攻撃に対して政府が講ずるべき情報共有等に関する対策」の一分野「（ｉ）政府としてとるべき方策、特に調達等に際して調達先企業に求める情報セキュリティ要件」について標準的ひな形「調達における情報セキュリティ要件の記載について」が示されたところ、これについては、今後対応を図っていく予定です。

６　情報セキュリティに関する障害・事故等報告

（１）情報セキュリティに関する障害・事故等の把握

・　障害・事故等を発見した職員は、「情報セキュリティ責任者」又は「情報システムセキュリティ責任者」に対して報告する。

・　報告を受けた情報セキュリティ責任者又は情報システムセキュリティ責任者は必要に応じて統括情報セキュリティ責任者へ報告する。

上記二点を「外務省情報セキュリティポリシー」にて定め、職員への周知・教育を実施しています。

また、統括情報セキュリティ責任者は、行政事務の遂行に特に重要な情報システムについて、その情報システムセキュリティ責任者及び情報システム取扱責任者の緊急連絡網の整備を指示しています。

「外務省情報セキュリティポリシー」により統括情報セキュリティ責任者は最高情報セキュリティ責任者の補佐をする役割であることから、統括情報セキュリティ責任者が受領した報告について、必要に応じて最高情報セキュリティ責任者へ報告します。

（２）ＣＳＩＲＴ体制の整備

情報漏洩につながる可能性のあるパソコン等の盗難、ウィルス付詐称メール、不正アクセスや大量アクセス攻撃（DDoS 攻撃）等、最近の多様化する脅威から外務省の情報システムを保護するため、大臣官房総務課、情報防護対策室、外交記録・情報公開室、大臣官房情報通信課が中心となり情報インシデント対応を支援する組織体制（CSIRT 体制）を平成２３年２月に立ち上げ、迅速に事案に対応できる体制と普段からの事前準備体制を整備してきています。

（３）公表した障害・事故等の概要、それに対する対応等

ア　会計課調達室のウェブページ脆弱性

当省の電子入開札システムに不正なアクセスがなされたとの検知があり、これに対する調査を実施しましたが、内部への侵入はなされておらず、入札関連情報等の

流出は確認されていないことが判明しました。引き続き、不正なアクセスによる内部侵入を阻止すべく、通信状況の監視を行うとともに、不正なアクセスを検知した際に迅速かつ適切な事実関係の確認と対応に努めてまいります。

イ　本省と在外公館への標的型メール攻撃

平成２３年１０月２６日以降、外務省と在外公館への標的型メール攻撃が行われた旨の報道がありました。標的型メール攻撃は、過去数年前から不審メールとして政府機関に送付されてきており、現在に至るも、その攻撃は止むことはありません。特に、平成２３年度に入って春以降は、その数は膨大になっており、特に6月7日には、当省職員６７８名に対する不審メールが接到するなど、判明している不審メールの延べ総数は１，０００通を超えています。標的型メールによりウィルス（マルウェア）に感染しても最新のウィルス対策ソフトでは検知出来ない場合にはその発見は困難を極めます。しかしながら、ウィルス対策ソフトのベンダーと協力し、未知ウィルスの調査・発見及びその駆除を行っています。さらに、外部から内部のネットワークへの入り口にファイアーウォール等の入口対策に加え、内部に侵入したウィルス（マルウェア）と外部の不正サーバとの通信を防ぐ出口対策、さらには、内部ネットワーク内でのウィルスによる不審な挙動を早期に検知するためのログ監視の強化も含めた追加的な対策も講じています。

なお、標的型メールが送信されてきているのは、秘密の情報を扱わないオープン系ネットワークであり、また、フォレンジック分析等の調査結果を含め、秘密情報の漏洩は確認されていません。

しかしながら、政府関係機関への標的型メール攻撃が頻発していることから、外務本省及び全在外公館で改めて標的型メールへの対応やＵＳＢメモリの取扱いなどに関する注意喚起を継続的に実施し、情報漏洩防止に向けた対策や体制を強化してきています。

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年度の情報セキュリティ対策については、基本的な対策に加え、以下の目標について重点的に取り組みます。

（１）職員に対する情報セキュリティ対策についての意識啓発

平成２３年度の重点事項に掲げたとおり、従来から職員に対する情報セキュリティ教育を実施してきていますが、外務省全体の情報セキュリティ意識を高く維持するために継続することが重要であり、引き続き全職員に対して定期的に意識啓発を図ります。

（２）当省内のＣＳＩＲＴ(Computer Security Incident Response Team)体制の充実

平成２３年度の重点事項に掲げたとおり、当省内ＣＳＩＲＴ体制の更なる充実を図っていきます。特に、未知ウィルス感染や不正アクセス、ＤＤｏＳ攻撃の脅威は益々高度

化していることから、これらに関する普段からの情報収集と情報インシデント発生前の事前対策の充実につき、可能な限り（予算が許される範囲で）図っていきます。

８　最高情報セキュリティアドバイザーメッセージ

ＣＩＳＯのメッセージにもあるように、平成２３年度は攻撃手法の進化・複合化が進み、ソーシャル・エンジニアリングの要素が色濃く反映された標的型攻撃が多数出現した年でした。また、攻撃目標も従来の情報通信システムだけでなく、社会インフラを構成する制御システムへと拡大されてきています。

このような攻撃手法・攻撃目標の変化に対して、従来の侵入防止に主眼を置いた防御策だけでは対応できず、侵入を前提とした多重防御や不審な通信の監視や遮断といった出口対策の必要性も明らかになっています。さらに、日頃の一般職員に対する意識付けや教育・訓練も欠かすことができない重要な施策であることが明らかになってきています。

平成２３年度は、当省においても一般事務処理を担うオープン系のシステムに対する攻撃が明らかになりました。当省は、職務上、在外公館が全世界に点在しており、各公館が直接攻撃にさらされるという構造的な特徴をもっています。しかも、各公館では極めて少人数で対応せざるを得ないという環境にあるだけでなく、対応する職員も必ずしも情報セキュリティの専門家ではありません。このような環境の下で、事前の多重防御システム・情報漏洩対策などの技術的対策と緊急即応体制が功を奏し、重要情報の漏洩は阻止することができたと考えます。

このことは、事前の検討や体制の構築があったればこその成果であり、事前準備が重要であることを示唆しています。日頃、当省情報システムの防御を担っている関係者に敬意を表します。

しかし、この結果に満足することなく今後も攻撃を受けること、侵入されることを前提とし、侵入があっても被害を極小化する技術的対策や組織的な対応策の検討を継続してほしいです。文字通り「継続は力なり。」です。

外務省最高情報セキュリティアドバイザー
山岸　篤弘
松井　充