情報セキュリティ報告書　概要資料　　外務省

1．CISOのメッセージ、平成23年度の総括･平成24年度の重点目標

（１）CISOのメッセージ		平成23年度においては、インターネット上における様々な攻撃が増し、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。 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。 このような状況の中、当省においては、平成23年度中にも各種の追加的対応を行ってきましたが、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。
（２）当該年度の総括	平成23年度の取組（概要）	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が必要となっています。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と呼んでいる）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。これらの対策により、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23年度の取組（結果）	これら対策もあって、本年度、当省においては深刻かつ重大な情報漏洩事案が発生することなく業務を遂行することができました。
	平成24年度の重点目標（概要）	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ついて注力するとともに、新たな脅威に対しても迅速かつ適切な対応が可能となるよう、日々取り組みと、その改善を図っていく所存です。

情報セキュリティ報告書　概要資料　　外務省

2. 情報セキュリティ対策の実施状況

（１）自府省庁の課題（自己点検結果、情報システム・重点検査、教育・啓発、調達・外部委託等）	自己点検の到達率については、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。これについてはさらに内容を調査し、職員の教育に努めていく予定です。
（２）（１）で記述した課題に対する対策状況・改善に向けた指示	平成24年度においても、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について重点的に取り組みます。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有益であると考え、全職員に対して定期的に意識啓発を図ります。

3. 情報セキュリティに関する障害･事故等

障害・事故の概要、原因分析	府省庁の対応	再発防止策
当省電子入開札システムへの不正アクセス	不正な攻撃パケットが検知されたため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。
当省への標的型メール攻撃	本省及び在外公館に対し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おり、日々対策を行っております。なお、各種調査の結果、標的型メールによる秘密情報などの漏洩は確認されていません。	ネットワークからの入口対策に加え、不正サーバとの通信が行えないようネットワークへの出口対策などの追加的措置を講じています。引き続き、情報漏洩防止に向けた対策や監視体制を強化してきています。

情報セキュリティ報告書　概要資料　　外務省

4．具体的な情報セキュリティ対策の実施内容等　※情報セキュリティ報告書全体から特に注力した取組を選択

実施概要（テーマ）	内容（取組の起点・背景、実施目的、具体的な工夫、費用、アピールポイント等）	効果（定量評価、できたこと・できなかったこと、期待される効果等）
無作為抽出した業務システムに対し、情報セキュリティ対策が適切に実施されているかを確認するため、外部専門家による監査を実施しました。	外務省においては、例年無作為に抽出した業務システムに対して外部監査を実施し、情報セキュリティ対策の向上に努めています。	外部専門家による監査を実施することにより、業務システムの安全性が客観的に担保されます。
障害・事故等が発生した場合を想定した、より迅速かつ的確な対応のための支援体制（CSIRT体制）の充実を図りました。	障害・事故等の発生時により迅速かつ的確に対応し、普段からの事前準備体制を整えるべく、省内のCSIRT体制を充実し、CSIRTメンバーによる机上演習を行いつつ、実際に機能するマニュアルを整備してきています。また、有識者等の専門家を講師として招き、CSIRTメンバーや一般職員向けに研修や勉強会を随時開催し意識啓発に努めています。	障害・事故等を未然に防ぐ対策を取ることはもちろんですが、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。
国内及び海外における情報セキュリティ関連の情報を、日々、収集して、当省内における早めの対策に生かすとともに、当該情報を省内・在外の関係職員へ提供しました。	国内外において情報セキュリティに関連する情報（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。	国内外の最新情報の収集により、標的型メール攻撃やこれに付随した不正アクセスについても早い段階から脅威を察知し、この対策方法について省内・在外への注意喚起を図ったことから情報漏洩防止に役立つとともに、システム面での対策についても早い段階から検討することができました。今後も脅威を関係者で広く共有できます。