情報セキュリティ報告書（概要）厚生労働省

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		厚生労働省は、医療や年金、雇用対策など、国民生活に直結する政策を担っていることから、業務で取り扱う情報資産は、適切な運用管理の下、あらゆる脅威から守らなくてはならない。そのためには、必要な情報セキュリティの確保とその継続的な強化・拡充に取り組むことが不可欠である。平成23年度は、防衛産業へのサイバー攻撃、また、衆議院や政府機関もサイバー攻撃を受けていたことなど重大事案が頻発したことから、セキュリティ事案の発生時など、様々な機会をとらえ、情報セキュリティポリシーの周知・徹底に努めた。今後も、引き続き、情報セキュリティ対策の継続的な強化・拡充に努めていく。
（2）当該年度の総括	平成23年度の取組（概要）	・平成22年度に起きた尖閣諸島沖中国漁船衝突映像の流出事件以来、これまで以上に政府機関における情報管理の徹底が厳しく求められている状況を踏まえ、セキュリティポリシー及び関連規程類の改訂を実施するとともに、研修等の機会をとらえ、情報管理の重要性について周知・徹底を図った。 ・標的型メール攻撃が社会的問題となっていることを踏まえ、厚生労働省から送信されるメールが、確実に厚生労働省から送付されたものであることを保証する送信ドメイン認証技術の導入を推進した。
	平成23年度の取組（結果）	・概ね適切に情報セキュリティ対策が実施されていたものの、情報システムセキュリティ責任者・管理者において一部遵守事項に対する理解不足がみられる。 ・本報告書が対象とする組織で所有するgo.jpドメインについては、すべて対策が完了した。
	平成24年度の重点目標（概要）	・情報セキュリティ教育を通じ、障害・事故等への対処や情報の適切な取扱いについて周知・徹底する。 ・障害・事故等の迅速かつ適切な報告及び対処を可能とするため、情報システムの管理・運用等を行う職員に対し、常日頃からの連絡体制及び対処手順の確認を呼びかける。

情報セキュリティ報告書（概要）厚生労働省

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)	従来の網羅的な点検方法を改め、点検項目を重点化することにより、情報セキュリティ対策への意識と理解度の向上を図ったため、昨年度の点検結果との単純比較は難しいが、概ね実施率・到達率とも向上した。しかし、情報システムセキュリティ責任者・管理者については、セキュリティリティポリシー及び関連規程類の理解不足が見られる。
(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	これまで情報システムの管理・運用等に携わってこなかった職員が異動に伴い担当となる場合において、これまでは自らが実施主体ではなかった遵守事項に対する遵守意識が希薄であることが、理解不足を招いているものと思われる。このため、適切な時期を踏まえ、割り当てられた役割の確認を促すことや、セキュリティポリシー等の周知・徹底、情報セキュリティ教育の充実を図ることが必要である。

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
ウイルス感染(平成23年11月) 業務情報を得るため特定のホームページへアクセスしたところ、不正プログラムがダウンロードされ、感染したもの。	・原因究明及び再発防止策の実施	・不審なファイルの実行禁止等の確実に実行することが重要な措置や不審なファイル等を確認した場合の対応の周知・徹底。 ・各部局の情報システムにおけるセキュリティ確保について、担当職員に対する注意喚起の実施。
USBメモリ紛失(平成23年12月、平成24年2月) 地方支分部局において、業務情報を含むUSBメモリを紛失したもの。	・原因究明及び再発防止策の実施	・USBメモリ管理状況の緊急点検の実施。 ・外部電磁的記録媒体の使用について、情報システムにおいて一定の制限を実施。 ・職員に対する注意喚起の実施。
ウェブサーバへの不正アクセス(平成24年3月) 施設等機関において、ホームページへの不正アクセスにより、コンテンツが改ざんされたもの。	・原因究明及び再発防止策の実施	・職員に対する注意喚起の実施。

情報セキュリティ報告書（概要）厚生労働省

4. 具体的な情報セキュリティ対策の実施内容等

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）
情報セキュリティ教育（研修の実施）	・昨今の情報セキュリティを取り巻く状況を考慮した、研修内容及び教材の見直しを行った。 ・最高情報セキュリティアドバイザーによる講義を実施した。 ・オンライン研修の受講状況を四半期ごとに各部局へ報告した。	研修内容及び教材を見直すことや最高情報セキュリティアドバイザーによる講義により、重要な事項を適切に教育することができた。また、定期的に受講状況を報告し受講を促すことで、職員に対する情報セキュリティ対策の重要性についての一定の意識付けを行うことができた。
標的型メール攻撃訓練の実施	標的型メール攻撃に対する対処方法や見分け方等の教育を行うとともに、標的型メールを模したメールを実際に職員に送付し、標的型メールを初めとした不審メールの受信時における対応を確認するための訓練を実施した。訓練結果については、CISOの講評・メッセージを添えて全職員宛てに報告した。	職員の標的型メール攻撃に対する意識の向上が図れた。