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		当省は、広範な分野を担当するとともに、外局や地方支分部局を含め多様な機能を持つ組織を擁する機関であることから、組織全体として適切な情報セキュリティ対策を実施していくことは極めて重要である。従来より国土交通省情報セキュリティポリシーに基づく体制構築と責任の明確化、状況の変化に応じた継続的な取り組み等に努めてきた。 今後も各部局において取り扱う情報の内容や業務の実態を踏まえ、柔軟かつ適切な対策・措置を図ることが重要であり、情報の取扱い、情報システムの適切な運用について、全職員に周知徹底するとともに、新しい脅威に対する適切な対策を講じ、引き続き情報セキュリティ対策の維持・強化に努めて参ります。
（2）当該年度の総括	平成23年度の取組（概要）	年度自己点検計画に基づいた職員の情報セキュリティ対策実施状況に関する自己点検及び年度監査計画に基づいた監査等の取り組みを実施した。
	平成23年度の取組（結果）	概ね国土交通省情報セキュリティポリシーに則った運用の実施が確認され、自己点検の実施や職員への周知を通じ、各職員の情報セキュリティに対する意識の浸透が見られた。
	平成24年度の重点目標（概要）	引き続き自己点検や監査等を着実に実施する。また、情報セキュリティ対策の責任・実施体制の再確認や情報格付けの区分に基づく情報の取扱いに努める。自己点検・監査方法の改善を検討し、大きな組織において継続的に情報セキュリティ対策の運用状況を確認できる仕組みの構築を目指す。情報セキュリティ対策の実施効果を一層高めるため職員への分かりやすい形での情報提供を継続的に実施する。

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）	当省では、広範な分野を担当し、外局や地方支分部局を含め多様な機能を持つ大きな組織を有しているため、本省の情報セキュリティ担当部局だけで全組織の情報セキュリティ対策の状況を継続的に確認し指導することが困難であることが課題であり、各部局において自立的、継続的に情報セキュリティ対策を把握・監視する体制の構築が必要である。 また、従来から職員に対する情報セキュリティ確保のための周知徹底や教育を実施しているが、全職員が対策や措置の内容を容易に理解し、実施効果を高めることが課題である。
（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	自己点検の結果を踏まえ各部局内で自立的、継続的に監査を行う（以下「部局内監査」という。）体制を構築し、本年より外局や地方支分部局を含めた全省的な部局内監査を実施した。各部局毎に自己点検結果を活用した監査を実施することにより、広範な組織の全てを対象とした効率的な監査を実施することが確認できた。また、情報セキュリティ対策の実施効果を一層高めるため、全職員に対して情報セキュリティ対策や措置の内容を分かりやすくポイントを絞った形での周知・徹底を行った。

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
モバイルパソコンを入れたバックの盗難が発生した。	個人情報が含まれたファイルを保存してあったために、個人情報が流出したおそれがあり、警察への盗難届を行うとともに、当該端末からのネットワークへのアクセスを無効化した。	個人情報の厳重な管理（パスワード設定・暗号化）を周知徹底した。
送信先である多数のメールアドレスが表示されたままの状態で誤ってメールを送信した。	送信先には、直ちに報告とお詫びを行うとともに当該電子メールの削除を依頼した。	不特定多数の者に電子メールを送信する際には複数の者による確認を実施することとした。
標的型メール攻撃によりプログラムの脆弱性を利用するコンピュータウィルスにパソコンが感染した。	ウィルスの駆除実施。感染したパソコンを経由し、サーバからユーザ情報を抜き取られた可能性があり、当該パソコン及びサーバについてネットワークからの切り離しと運用を停止した。また、個人情報が流出したおそれがあり、関係者へのお詫びを行った。	サーバ上の対策状況とパソコンにおけるセキュリティ対策状況の再確認を行った。
非公開の扱いとされている情報等を撮影した写真が、個人のホームページにおいて公開されていたことが判明した。	掲載者の特定とともに、掲載者による写真の削除及び個人ホームページの閉鎖を実施した。	格付の見直しや情報管理体制等の情報セキュリティ対策を強化した。
外部からサーバに攻撃があり、ID及びパスワードが解析され、不正に侵入されたことが判明した。この結果、当該サーバを踏み台として他機関のサーバに対し攻撃が行われた。	侵入されたサーバのネットワークからの切り離しと運用を停止した。また、ID及びパスワードの変更やアクセス回数の制限を行った。	管理している各サーバの設定状況の確認やファイヤウォールの設定を再確認した。
Webページの一部が不正に改ざんされていた事が判明した。	当該サーバ及び類似のサーバをネットワークから切り離し、運用を停止した。	当該機関における外部公開サーバの総点検と脆弱性検査を実施した。

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）
自己点検結果を活用した部局内監査の実施	当省では、広範な分野を担当し、外局や地方支分部局を含め多様な機能を持つ大きな組織を有しているところ、各情報セキュリティ責任者が自立的に作成した監査実施計画書を基に部局内監査を行う体制を構築し実施した。実施にあたっては、情報セキュリティポリシーを改正し、部局内監査の実施体制を整備した。 また、実施にあたっては、監査実施手順書を各部局に配布し、電話やメールを活用し、効率的な監査実施に努め事務負担の軽減を図るとともに、各部局（本省）の担当者に対し、監査実施手順についての事前説明会を開催した。 なお、昨年度は、地方支分部局を対象として試行的に部局内監査を実施し、今年度より、本省、外局等を含め省内全ての部局を対象として部局内監査を実施した。	各部局毎に自己点検結果を活用した監査を実施することで、広範な組織の全てを対象とした効率的な監査を実施することが確認できた。
メールフィルターによる不審メール対策の強化（本省LAN*1）	外部から受信する全てのメールについて、省庁ドメインを詐称していると思われるメール、フリーメールドメインから送信されたメールについて警告文を本文中に挿入する機能をメールフィルターに追加した。なお、本対策については、保守契約の範囲内で対応出来た。	機能の追加により年間の全体受信数の約1%にあたる約24万通のメールに対し、警告文が本文中に挿入されており、ウィルス感染の防止に一定の効果があったと思われる。

*1　約5000ユーザが対象