平成23年度　情報セキュリティ報告書　概要　経済産業省

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年度は、防衛産業や重要インフラ等に対する標的型サイバー攻撃事案が発生するなど、情報システムに対する攻撃手法が高度化してきており、内閣官房情報セキュリティセンターを中心に、関係政府機関による検討や対策が進められてきた。 経済産業省は、こうした対策を検討する場において積極的な貢献を果たすとともに、省内においては、昨年度に引き続き、省内各課室における情報の管理徹底を図るべく情報管理に係る運用手続きや体制の整備、情報セキュリティに係る全職員向けe-Learning研修の実施、アクセス制限付きフォルダを活用した情報管理の徹底等を中心に各種情報セキュリティ対策を実施した。
（2）当該年度の総括	平成23年度の取組（概要）	・情報管理の徹底に向けた各種セキュリティ対策の策定・実施事項として、省内課室における情報管理に係る運用手続きや体制整備を検討し、経済産業省情報セキュリティポリシーに従い、情報の洗い出しや機密性の格付及び格付に応じた取扱の決定を行い、課内の体制整備を実施。 ・機密性の高い情報の漏えい防止の徹底に向けた情報漏えい防止サービスなどの技術的手段の活用の推進 ・公開ウェブサーバ及び電子メールサーバの情報セキュリティ対策実施状況の重点検査の実施
	平成23年度の取組（結果）	・省内課室の情報管理に係る運用手続きや体制の整備を通じ、職員の情報セキュリティ対策の重要性に係る意識向上につながった。 ・機密性の高い情報の漏えい防止の徹底に向け、アクセス制限付きフォルダや情報漏えい防止サービスなどの技術的手段の活用推進を図った。 ・公開ウェブサーバ及び電子メールサーバの情報セキュリティ対策について、重点的な調査を行ったところ、適切に情報セキュリティ対策が講じられていることが確認された。
	平成24年度の重点目標（概要）	・省内課室の情報管理に係る運用手続きや体制の整備について、その状況を適宜把握するとともに、必要により改善事項の指摘や改善状況の把握等に努める。 ・基盤情報システムの更改により、機密性の高い情報の漏えい防止の徹底に向けたアクセス制限付きフォルダの活用や情報漏えい防止サービス、新たな認証システムなどの技術的手段の活用を推進し、更なる高度化を図る。 ・情報セキュリティ研修等において、標的型メールへの対応（訓練や注意喚起等）や当省関連のWebサイト改ざんへの対応等について、重点的に実施する。

平成23年度　情報セキュリティ報告書　概要　経済産業省

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）	①これまで実施してきた情報セキュリティ対策の効果をより確実なものとし、情報管理を徹底するためのフォローアップとして一層の対策強化を図る必要があった。このため、「情報の機密性の格付や取扱の手続きが具体化されているか」、「運用手続きが課室職員全員に共有され確実に守られているか」等について、実態調査を行った。この結果、情報の格付や取扱等運用手続きの具体化、機密性の高い情報の保管等において、一部不備が見られた。 ②近時、防衛産業や重要インフラ等に対する標的型サイバー攻撃事案が発生するなど、情報システムに対する攻撃手法が高度化してきており、技術的対策や運用的対策を含め、喫緊に対応を図る必要がある。
（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	①については、省内課室における情報の管理徹底を図るべく、情報管理に係る運用手続きや体制整備の検討・策定事項として、経済産業省情報セキュリティポリシーに従い、情報の洗い出しや機密性の格付及び格付に応じた取扱の決定を行い、課内の体制整備を実施した。この結果、職員の意識向上につながるとともに、省内の情報セキュリティ対策の強化につながった。 ②平成23年11月及び12月に、省内全職員を対象に標的型メールを模倣した訓練メール（添付メール、リンクメール）を配信し、その対応訓練を行った。訓練実施に当たっては、事前に関係諸会議にて訓練概要を説明するなど準備を図り、訓練実施後は、必要な職員にフォローアップ研修を実施するなど、訓練効果を高める対策を実施した。この訓練の結果、職員から多くの意見が寄せられ、標的型メールの教育訓練の効果が得られた。

平成23年度　情報セキュリティ報告書　概要　経済産業省

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
平成24年１月、委託先にて運用を行っているウェブサイトがサイバー攻撃を受けて一部のページが改ざんされ、同サイトの趣旨と無関係なページが表示される状況になった。なお、同サイトへのウイルス感染や情報流出は確認されなかった。	内閣官房情報セキュリティセンター等の関係機関と連携し、迅速な情報共有を図り、Webサイトの復旧を行った。	Webサーバの脆弱性に対する的確なセキュリティ対策を図るため、技術的対応策等の実施に係る周知徹底を行った。
平成24年２月、特許庁の端末がウイルス感染していたことが判明した。なお、特許出願等に係る未公開情報について、ウイルス感染による流出は確認されなかった。	発見したウイルスは、全て駆除（感染していたのは３台）し、庁内全ての端末のウイルスチェックを実施した。	出口対策を徹底するためフィルタリング機能を強化するとともに、職員向けに、電子メール、Web、小型可搬媒体等の利用に関する注意喚起を行い、情報セキュリティ対策の徹底を図った。

平成23年度　情報セキュリティ報告書　概要　経済産業省

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）
省内課室における情報管理に係る運用手続きや体制整備の検討・策定を実施した。	情報管理の徹底に向けた情報セキュリティ対策の策定・実施事項として、省内課室における情報管理に係る運用手続きや体制整備を検討し、経済産業省情報セキュリティポリシーに従い、（イ）保有する情報の洗い出し、（ロ）機密性の格付の決定、（ハ）情報の格付に応じた取扱の決定を行い、課内の体制整備を行った。 対象課室としては、省内各局（大臣官房、経済産業政策局等）及び外局（資源エネルギー庁、中小企業庁等）ごとに選定された課室で実施した。	職員の意識向上につながるとともに、省内の情報セキュリティ対策の強化につながった。具体的には、以下の効果が望めた。 ①機密性の格付及び取扱について、省内で統一的な情報管理を行うことができること。 ②課室情報セキュリティ責任者である課室長が、課室内の情報管理を行う上で適切にリスクマネジメントができること。 ③機密性の高い情報（機密性4情報、機密性3情報）を省内で横断的に把握できること。
情報セキュリティ関係資料のワンストップ化を行った。	省内イントラネットのトップページにバナーを設け、情報セキュリティコーナーとして、情報セキュリティ関係の資料をワンストップ化し、職員がいつでも必要な資料を閲覧できるように、適宜内容の追加・見直しを行った。また、職員が資料を有効活用するべく、省内連絡など省内職員向けのメールを通じ、各職員に周知している。	各種情報セキュリティ対策の実施において、システム関係部門と職員との情報共有が促進され、職員の情報セキュリティに向上につながった。
標的型メール攻撃に係る教育訓練を実施した。	平成23年11月及び12月に、省内全職員を対象に標的型メールを模倣した訓練メール（添付メール、リンクメール）を2回配信し、2回とも開封した職員に対し、標的型メール攻撃に関するフォローアップ研修を実施するなど、訓練効果を高める対策を実施した。	職員からは、「添付ファイルは良く確認のうえ開けるようにしたい」、「少しでも不審なメールは電話等で送信者に確認したい」、「この様な訓練は今後も実施した方が良い」等多くの意見が寄せられ、標的型メールの教育訓練の効果が得られた。