

- 平成24年度の情報セキュリティ事象や取組につき、**数値的に把握・分析**。今後の取組の方向を提示
- 各府省庁が個別に公表していた情報セキュリティ報告書を年次報告に**一括掲載することにより、政府としての取組状況の一覧性を向上**

第1編 情報セキュリティに関する脅威とその対策 (情報セキュリティ事象の種別ごとの分析と対策)

事象の種別	事象の発生状況	取組の状況
過失・故意による事象	機密情報の紛失など一定数の事象が依然発生	勉強会の開催等により情報セキュリティポリシー浸透を図る取組を実施。引き続き、職員に対する情報セキュリティポリシー浸透・遵守の一層の徹底を図る
ウェブサイト等への攻撃	示威を目的にするものによると思われる攻撃等が発生。不正アクセス等の増加	ウェブサイトの脆弱性検査、GSOC※での情報収集・監視等により対処。今後は被害拡大防止策としての事象発生時の緊急時対応に係る訓練を充実 ※政府機関情報セキュリティ横断監視・即応調整チーム
国の重要な情報をねらう攻撃	機微な情報を扱う特定の政府組織等に対して「標的型攻撃」とおぼしきサイバー攻撃事象が発生	サイバー攻撃等への対応体制を整備(全府省庁においてCSIRTの整備完了、CYMAT※設置)。また、メール攻撃訓練等の不審メール対策を実施。今後は 重要な業務・情報に重点を置いたリスク評価ベースの対策を検討 ※府省庁横断的な情報セキュリティ緊急支援チーム

第2編 各府省庁の取組と評価 (NISCによる評価と各府省庁の情報セキュリティ報告書)

○ 各府省庁における取組の評価

- ① 対策の実施状況に関する評価
 - * 情報セキュリティ対策を実施した者の割合について高水準を維持
- ② 情報システムへの対策状況に関する評価
 - * 昨今のサイバー攻撃等を踏まえ、SQLインジェクションの脆弱性への対策等の対策状況を重点的に検査。高水準で対策が実施されていることを確認
- ③ 情報セキュリティ対策に係る推奨事例の選定
 - * コピー・プリンタ複合機の監査の取組 等

○ 各府省庁の取組(情報セキュリティ報告書)

- ① 内閣官房
 - ② 内閣法制局
 - ③ 人事院
 - ...
 - ㉑ 防衛省
- ・ CIS0からのメッセージ
 - ・ 平成24年度の評価・次年度の目標
 - ・ 情報セキュリティ対策の実施状況
 - ・ 障害・事故報告
 - ・ 最高情報セキュリティアドバイザーからのメッセージ