資料３－１

2013年度の政府機関における情報セキュリティ対策に関する取組と評価等について

政府機関等におけるサイバーセキュリティに関する情勢

○ 2013年度に政府機関等において発生した情報セキュリティインシデントは「外部からの攻撃」、「意図せぬ情報流出」に大別され、それぞれ「脅威の増大」、「新たな課題等の顕在化」といった傾向がみられる。

外部からの攻撃に係る情報セキュリティインシデント

○ 新たな手法による標的型攻撃が発生するなど、攻撃が巧妙化・多様化
- 特定のウェブサイトを閲覧しただけで、標的とする組織の端末のみが不正プログラムに感染するタイプの攻撃が発生
- ソフトウェアのアップデート時に不正プログラムに感染する情報セキュリティインシデントが発生

○ GSOC※の監視結果の分析からも、リスクが深刻化している傾向がみられる

○ 独立行政法人の被害も多くみられる

※ Government Security Operation Coordination team（政府機関情報セキュリティ横断監視・即応調整チーム）

○ 政府機関への脅威※1

2011年度	2012年度	2013年度
約66万件	約108万件	約508万件※2

※1 GSOCにより各府省庁等に置かれたセンサーが検知等したイベントのうち、正常なアクセス・通信とは認められなかった件数

※2 約6秒に1回検知している計算

○ 不正アクセス等の検知※3

2011年度	2012年度	2013年度
139件	175件※4	139件※5

※3 監視活動により不正アクセス等を検知した際の当該政府機関への通報件数

※4 2012年度は特殊事情（12月に大量の不審メールを受信）のため多くなっている

※5 数値の増加はみられないが、不正アクセス等のタイプや割合をみるとリスクが深刻化

意図せぬ情報流出に係る情報セキュリティインシデント

○ ITサービス等の不適切な利用や利用時の不適切な設定による従来とは質の異なる事案も発生
- 政府機関において、無料のクラウドサービスの不適切な利用に起因する情報流出事案が発生
- 国立大学において、複合機で読み取った学生らの個人情報がインターネット上で誰でも閲覧できる状態になっていた事案が発生

※会議開催後、誤記の修正をしています。

政府機関全体の取組と評価①

○ 2013年度における政府機関全体の取組について、サイバーセキュリティに関する情勢及びその分析結果に照らして総括するとともに、対策状況の評価を行った。

外部からの攻撃等の情報セキュリティインシデントへの対処等に係る取組に関する総括

○ 政府機関統一基準群の改定において標的型攻撃の脅威への対応のための規定を整備
○ 高度化する標的型攻撃に対応するため、その標的とされる蓋然性が高い業務・情報に係るリスク評価を実施し、対策の重点化による多重防御の実現に向けた取組を推進

※ 高度サイバー攻撃対処のためのリスク評価等のガイドライン（試行版）を策定。2013年10月に試行を開始し、2014年度から正式運用開始予定

○ 府省庁CSIRTやCYMAT※の要員を対象とした研修等に加え、3・18（サイバー）訓練を実施し、サイバー攻撃対処態勢を充実・強化

※ CYber Incident Mobile Assistance Team
（府省庁横断的な情報セキュリティ緊急支援チーム）

○ ウェブサイトの脆弱性検査の実施等により、府省庁における脆弱性対策の徹底を推進
○ 独立行政法人に対するサイバー攻撃の発生状況に鑑み、独立行政法人における情報セキュリティ対策の強化に関する検討を開始

ITの利用動向の変化に伴う新たな課題等への対応に係る取組に関する総括

○ 政府機関統一基準群の改定においてSNS等の利用時の機密情報の取り扱いを禁止する規定を整備
○ 意図せぬ情報流出に係る事案の発生時において、政府機関全体として実態調査、対策状況の点検等を実施
○ 諸外国の動きも踏まえ、クラウドサービスの利用に当たり必要となる要件等に関する検討を開始

政府機関全体の取組と評価②

○ 2013年度における政府機関全体の取組について、サイバーセキュリティに関する情勢及びその分析結果に照らして総括するとともに、対策状況の評価を行った。

対策実施状況に係る評価の概要

○ 対策の実施状況（各府省庁による自己点検の結果）に関しては、一般職員を含む各役割者のポリシー実施率は高水準を維持し、対策の浸透が認められた。

○ 行政事務従事者のポリシー実施率※1調査

2011年度	2012年度	2013年度
95.9%	96.8%	96.8%

※1　把握した者のうち、責務が生じた者に占める対策を実施した者の割合

○ 責任者等※2のポリシー実施率調査

2011年度	2012年度	2013年度
99.5%	99.6%	99.3%

※2　最高情報セキュリティ責任者・統括情報セキュリティ責任者・情報セキュリティ責任者・課室情報セキュリティ責任者

重点検査による評価の概要

○ 重点検査においては、公開ウェブサーバ、電子メール、複合機、ウィンドウズXP等に係る対策状況等を対象として実施し、検査時点においては一部問題も把握されたが迅速に対処を完了。サーバ集約化についても当初目標（2008年度比で半減）を達成。

○ SQLインジェクション脆弱性の確認状況

対象	確認を実施した率
公開ウェブサーバ※3	95%

※3　インターネット上で公開しているウェブサーバを持つ情報システムのうち、SQLインジェクション脆弱性が技術的に存在し得るもの

○ サーバ集約化※4

	2008年度	2013年度
ウェブサーバ	約1,000台	約600台
メールサーバ	約1,900台	約770台

※4　府省庁におけるハードウェア台数の集計

※会議開催後、誤記の修正をしています。

「サイバーセキュリティ政策に係る年次報告（2013年度）」への掲載

○「サイバーセキュリティ政策に係る年次報告（2013年度）」にサイバーセキュリティ2013に掲げた各施策の評価や重要インフラ事業者の取組等と併せて一括掲載し、情報セキュリティ政策会議の決定を諮ることを予定している。

■「サイバーセキュリティ政策に係る年次報告（2013年度）」の構成（案）

※下線の部分が政府機関に係る取組と評価に関連する主な部分