「サイバーセキュリティ政策に係る年次報告（2013年度）」（案）の概要について①

資料4

本年次報告の位置付け

- 「サイバーセキュリティ戦略」（2013年6月10日情報セキュリティ政策会議決定、対象期間：2013～2015年度）に基づく初めての年次報告。
- 従前は個別に報告・公表してきた、政府機関等における取組、重要インフラ事業者等における取組、各府省庁のサイバーセキュリティ関連施策の評価・実施状況等を1冊に集約。

政府機関等における情勢

【最近の事象の傾向】

攻撃手法の多様化・巧妙化

＜外部からの攻撃＞

○ 攻撃対象の多様化
地方局や宇宙・原子力関連等の独立行政法人などの情報も標的に

○ 標的型攻撃の一層の巧妙化
対象組織の職員がサイトを閲覧すると不正プログラムを自動的に取り込む“水飲み場型攻撃”等

○ 攻撃の高度化
標的型攻撃と“ゼロデイ攻撃”（修正プログラムが公開される前の脆弱性を悪用するもの）との組合せにより不正プログラム感染事態の防止が困難化

＜意図せぬ情報流出＞

○ ITサービス等の不適切な利用や設定による情報流出
無料のクラウドサービスの不用意な利用など

【政府機関への脅威件数等】

24時間365日（約6秒に1回）

	2011年度	2012年度	2013年度
センサー監視等による脅威件数※1	約66万	約108万	**約508万**
センサー監視等による通報件数	139	175	**139**
不審メールに関する注意喚起の件数	209	415	**381**

※1 GSOC（政府機関情報セキュリティ横断監視・即応調整チーム）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。

重要インフラにおける情勢

【重要インフラへの攻撃等件数】

攻撃リスクの拡大

	2011年度	2012年度	2013年度
重要インフラ事業者等からの情報連絡※2件数	15	76	**133**

＜内訳＞
不正アクセス、DoS攻撃 121
ウイルスへの感染 7
その他の意図的要因 5

	2012年度	2013年度
標的型攻撃メール等の情報提供※3件数	246	**385**

※2 NISCへの情報連絡件数のうちサイバー攻撃（意図的要因）に関するもの。
※3 重要インフラ機器製造、電力、ガス、化学、石油の5業界からIPAへ情報提供されたもの。

【重要インフラ分野】

保護対象の多様化

① 情報通信
② 金融
③ 航空
④ 鉄道
⑤ 電力
⑥ ガス
⑦ 政府・行政サービス
⑧ 医療
⑨ 水道
⑩ 物流

○ 化学 ※4
○ クレジット
○ 石油

※4「重要インフラの情報セキュリティ対策に係る第3次行動計画」（2014年5月19日情報セキュリティ政策会議決定）において追加。

「サイバーセキュリティ政策に係る年次報告（2013年度）」（案）の概要について②

サイバーセキュリティ戦略に基づく主な取組実績

	政府機関・独立行政法人等	重要インフラ事業者	企業・一般個人
「強靭な」サイバー空間（守り強化）	「政府機関統一基準群」改定（2014/5/19） 3・18（サイバー）訓練（2014/3/18）	「重要インフラの情報セキュリティ対策に係る第3次行動計画」策定（2014/5/19） 事業継続確保のための分野横断的演習（2013/12/9）	「新・情報セキュリティ普及啓発プログラム」策定（2014/7/10） 「サイバーセキュリティの日」の新設（毎年2月の最初のワーキングデー）
「活力ある」サイバー空間（基礎体力）	「新・情報セキュリティ人材育成プログラム」策定（2014/5/19） 「情報セキュリティ研究開発戦略」改定（2014/7/10）		
「世界を率先する」サイバー空間（国際戦略）	「サイバーセキュリティ国際連携取組方針」策定（2013/10/2）		ASEAN諸国との共同意識啓発活動
組織体制	「我が国のサイバーセキュリティ推進体制の機能強化に関する取組方針」（討議中） GSOC※ の機能強化		※ GSOC：政府機関情報セキュリティ横断監視・即応調整チーム

3・18（サイバー）訓練

サイバー攻撃が発生した際の対処について、NISCと各府省庁・重要インフラ事業者等との連携習熟を図る訓練を実施。

分野横断的演習

重要インフラに対して連続的に情報セキュリティインシデントが発生した場合の対処について、実践的な演習を官民連携で実施。

情報セキュリティ普及啓発ロゴマーク

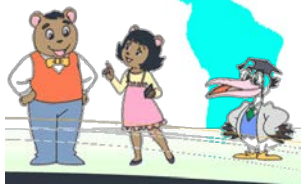
商標登録5648615号・5648616号

誰もが安心して情報通信技術の恩恵を享受し、国民一人ひとりが情報セキュリティについての関心を高めることを企図して策定。

ASEAN-JAPAN 意識啓発ポスター

意識啓発アニメーションDVD贈呈式

意識啓発アニメーション



ASEAN各国と共同での意識啓発活動の一環として、日本語版・英語版・ASEAN各国字幕版の意識啓発アニメーションの作成等を実施。

「サイバーセキュリティ政策に係る年次報告（2013年度）」（案）の概要について③

政府機関全体としての対策状況の評価

○ 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

サイバーセキュリティ関連施策の評価

- 「サイバーセキュリティ2013」においては、サイバーセキュリティ戦略の体系に沿って各府省庁のサイバーセキュリティ政策に関係する具体的な取組が掲載されており、これらの取組は着実に進捗し、おおむね所期の成果を挙げたものと認められる。
- 今後、サイバー空間を取り巻くリスクの深刻化が一段と進むと想定され、NISCの機能強化、2020年の東京オリンピック・パラリンピック開催に向けた新たな課題にも対応するため、本評価も踏まえ、「サイバーセキュリティ2014」に沿って、個々の施策について、具体化・深化させて推進等していくことが必要。

（参考）「サイバーセキュリティ政策に係る年次報告（2013年度）」（案）の構成

- 「サイバーセキュリティ戦略」（2013年6月10日情報セキュリティ政策会議決定、対象期間：2013～2015年度）に基づく初めての年次報告。
- 従前は個別に報告・公表してきた、政府機関等・重要インフラ事業者等における取組、各府省庁の関連施策の評価・実施状況等を1冊に集約。

年次報告 本編

- **Ⅰ 2013年度のサイバーセキュリティに関する情勢**
  - 1 我が国におけるサイバーセキュリティ全般の状況
  - 2 政府機関等・重要インフラ企業におけるサイバーセキュリティに関する情勢
    - (1) 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
    - (2) 重要インフラ企業におけるサイバーセキュリティに関する情勢
  - 3 2013年度の政府の主な政策の取組実績
  - 4 今後の取組
    - (1) 我が国のサイバーセキュリティ推進体制の強化
    - (2) その他のサイバーセキュリティ施策の推進
- **Ⅱ 政府機関における取組と評価**
  - 1 政府機関全体における情報セキュリティ対策に関する取組
    - (1) 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
    - (2) 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
    - (3) 情報セキュリティ対策に係る教育
  - 2 政府機関全体としての対策状況の評価
    - (1) 対策実施状況に係る評価
    - (2) 重点検査による評価
- **Ⅲ 重要インフラ事業者等における対策状況の成果と課題**
  - 1 成果
  - 2 課題
- **Ⅳ サイバーセキュリティ関連施策の評価**
  - 1 「強靱な」サイバー空間の構築
  - 2 「活力ある」サイバー空間の構築
  - 3 「世界を率先する」サイバー空間の構築
  - 4 推進体制等

年次報告 別添

- **別添１ 各府省庁における情報セキュリティ対策に関する取組**
- **別添２ 「サイバーセキュリティ2013」に盛り込まれた施策の実施状況**
  - 1 「強靱な」サイバー空間の構築
  - 2 「活力ある」サイバー空間の構築
  - 3 「世界を率先する」サイバー空間の構築
  - 4 推進体制等
- **別添３ 政府機関等における情報セキュリティ対策に関する取組等**
  - 別添３－１ 「政府機関の情報セキュリティ対策のための統一基準群」の改定
  - 別添３－２ 高度サイバー攻撃への対処
  - 別添３－３ 教育・訓練に係る取組
  - 別添３－４ なりすまし防止策の実施状況
  - 別添３－５ 公開ウェブサーバの脆弱性検査結果の概要
  - 別添３－６ 暗号移行
  - 別添３－７ 独立行政法人等の情報セキュリティ対策の現状について
  - 別添３－８ NISC発出注意喚起文書及び情報セキュリティ対策推進会議決定等
  - 別添３－９ 政府機関等に係る2013 年度の情報セキュリティインシデント一覧
  - 別添３－10 政府のサイバーセキュリティ関係予算額の推移
- **別添４ 重要インフラ事業者等における情報セキュリティ対策に関する取組等**
  - 別添４－１ 第２次行動計画の各施策の成果と課題
  - 別添４－２ 安全基準等の浸透状況等に関する調査
  - 別添４－３ 安全基準等の継続的改善状況等に把握及び検証
  - 別添４－４ セプター概要
  - 別添４－５ セプターマップ
  - 別添４－６ セプター訓練
  - 別添４－７ 分野横断的演習
  - 別添４－８ 補完調査
- **別添５ 最近の主な脅威の概要とその対策**
- **別添６ 用語解説**

＜凡例：従前の報告・公表事項等との対応＞

- 主に「201x年度の情報セキュリティ政策の評価等」として報告してきた内容
- 主に「政府機関における情報セキュリティに係る年次報告」として報告してきた内容
- 主に重要インフラ専門委員会で報告・公表してきた内容
- 本年次報告に当たって新規に設けた内容