# 政府機関の情報セキュリティ対策の実施状況に関する重点検査及び評価結果について
## ～2008年度重点検査の評価結果～

2009年2月3日

内閣官房情報セキュリティセンター（NISC）

資料5－1

# 重点検査の概要(端末、ウェブサーバ、メールサーバ)

**1. 検査対象機関・システム等** ： 全19府省庁(本省及び地方支分部局)の情報システム

内閣官房、内閣法制局、人事院、内閣府、宮内庁、公正取引委員会、警察庁、金融庁、総務省、法務省、外務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省、防衛省

**2. 検査期間** ： 平成20年7月(調査票配布)から同年12月(平成20年11月1日時点の実施状況を検査)

**3. 検査方法** ： NISCが配布した調査票に基づき、各府省庁が端末とウェブサーバ、電子メールサーバについて内部調査を行い回答。両者間で回答内容の確認作業等を行い、NISCから1月上旬に評価結果を各府省庁に通知。

① **端末**(据置型PC、モバイルPC)について、3つのカテゴリーに関して検査
**《対象数：約55万台》**

② **ウェブサーバ**(公開ウェブサーバ)について、4つのカテゴリーに関して検査
**《対象数：約1,000台》**

③**電子メールサーバ**について、4つのカテゴリーに関して検査
**《対象台数約1,900台》**

| 端末に関する重点検査項目 | |
|---|---|
| 不正プログラム対策 | ・OSのパッチ等の適用状況<br>・主要APのパッチ等の適用状況<br>・アンチウィルスソフトの運用状況 |
| 情報保護対策 | ・モバイルPCの暗号化機能の運用状況 |
| 端末管理 | ・端末の物理的対策状況 |

| ウェブサーバに関する重点検査項目 | |
|---|---|
| 不正プログラム対策 | ・OSのパッチ等の適用状況<br>・ウェブサーバAPのパッチ等の適用状況等 |
| 不正アクセス対策 | ・不正アクセス対策状況 |
| 情報保護対策 | ・利用者に対する権限管理等の実施状況 |
| サーバ管理 | ・管理者に対する権限管理等の実施状況<br>・データ復旧対策状況 |

| 電子メールサーバに関する重点検査項目 | |
|---|---|
| 不正プログラム対策 | ・OSのセキュリティパッチ適用状況(アップデートの状況)<br>・電子メールサービス提供ソフトウェアのセキュリティパッチ適用状況(アップデートの状況)<br>・電子メールコンテンツに対する不正プログラム対策の状況 |
| 不正アクセス対策 | ・不正中継対策の状況 |
| 情報保護対策 | ・電子メールの受信に係わる利用者に対する認証等の実施状況 |
| サーバ管理 | ・電子メールサーバの管理者に対する認証等の実施状況<br>・電子メールサーバの障害等の発生時における復旧対策の状況<br>・時刻同期機能の動作 |

# 端末、ウェブサーバ、メールサーバに関する情報セキュリティ対策の総合評価

| 府省庁名 | 端末 | | | | | ウェブサーバ | | | | | メールサーバ | | | | | 府省庁名 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 前回 H19.3 | 上昇率 | H20.11 | 上昇率 | H21.3 (含見込み) | 前回 H19.3 | 上昇率 | H20.11 | 上昇率 | H21.3 (含見込み) | 前回 H19.9 | 上昇率 | H20.11 | 上昇率 | H21.3 (含見込み) | |
| 内閣官房 | B | ▷ | A | − | A | B | ▷▷ | ※A | − | A | B | ▷ | B | ▷ | A | 内閣官房 |
| 内閣法制局 | B | ▷ | A | − | A | B | − | ◆対象なし | − | ◆対象なし | B | ▷▷ | A | − | A | 内閣法制局 |
| 人事院 | A | − | A | − | A | B | − | ◆対象なし | − | ◆対象なし | A | − | A | − | A | 人事院 |
| 内閣府 | B | ▷ | A | − | A | B | − | B | − | B | B | ▷ | B | ▷ | A | 内閣府 |
| 宮内庁 | A | − | A | − | A | A | − | A | − | A | B | − | B | − | B | 宮内庁 |
| 公正取引委員会 | A | − | A | − | A | A | − | A | − | A | B | ▷▷ | A | − | A | 公正取引委員会 |
| 警察庁 | A | − | A | − | A | A | − | A | − | A | A | − | A | − | A | 警察庁 |
| 金融庁 | B | ▷ | A | − | A | A | − | B | − | B | A | − | A | − | A | 金融庁 |
| 総務省 | B | − | B | − | B | B | ▷ | A | − | A | B | ▷ | A | − | A | 総務省 |
| 法務省 | B | ▷ | B | ▷ | A | B | ▷ | A | − | A | B | ▷ | B | ▷ | A | 法務省 |
| 外務省 | A | − | A | − | A | B | ▷ | A | − | A | B | ▷ | A | − | A | 外務省 |
| 財務省 | B | ▷ | A | − | A | B | − | B | ▷ | A | A | − | A | − | A | 財務省 |
| 文部科学省 | A | − | B | − | B | A | − | B | ▷ | A | A | − | A | − | A | 文部科学省 |
| 厚生労働省 | B | ▷▷ | B | ▷ | A | B | ▷ | B | ▷ | A | A | − | A | − | A | 厚生労働省 |
| 農林水産省 | A | − | A | − | A | A | − | A | − | A | A | − | A | − | A | 農林水産省 |
| 経済産業省 | A | − | A | − | A | A | − | A | − | A | A | − | A | − | A | 経済産業省 |
| 国土交通省 | B | ▷ | A | − | A | B | ▷▷ | A | − | A | B | ▷▷ | A | − | A | 国土交通省 |
| 環境省 | B | ▷ | A | − | A | A | − | A | − | A | A | − | A | − | A | 環境省 |
| 防衛省 | B | ▷ | A | − | A | A | − | A | − | A | A | − | A | − | A | 防衛省 |

| 評価 | 実施率 | 評価 | 実施率 | 評価 | 実施率 | 評価 | 実施率 |
|---|---|---|---|---|---|---|---|
| A | x=100% | B | 80%≦x<100% | C | 60%≦x <80% | D | x< 60% |

| 上昇率 | | 上昇率 | | 上昇率 | |
|---|---|---|---|---|---|
| ▷▷ | x> 10% | ▷ | x> 0% | − | x≦0% |

※内閣官房のウェブサーバについては、内閣府との共有システムを除く
◆内閣法制局、人事院のウェブサーバについては、ホスティング、e-gov移行済みのため対象なし

# 評価結果を受けての対応方針

| | 平成２１年３月末時点の評価（含見込み） | | | 対応完了予定 |
|---|---|---|---|---|
| | 端　末 | ウェブサーバ | メールサーバ | |
| 内閣官房 | A | A | B→A | メールサーバ：平成20年度中 |
| 内閣法制局 | A | 対象無し | A | 対策実施済み |
| 人事院 | A | 対象無し | A | 対策実施済み |
| 内閣府 | A | B | B→A | ウェブサーバ：平成21年度中、メールサーバ：平成20年度中 |
| 宮内庁 | A | A | B | メールサーバ：平成21年度中 |
| 公正取引委員会 | A | A | A | 対策実施済み |
| 警察庁 | A | A | A | 対策実施済み |
| 金融庁 | A | B | A | ウェブサーバ：平成21年度中 |
| 総務省 | B | A | A | 端末：平成21年度中 |
| 法務省 | B→A | A | B→A | 端末、メールサーバ：平成20年度中 |
| 外務省 | A | A | A | 対策実施済み |
| 財務省 | A | B→A | A | ウェブサーバ：平成20年度中 |
| 文部科学省 | B | B→A | A | 端末：平成21年度中　ウェブサーバ：平成20年度中 |
| 厚生労働省 | B→A | B→A | A | 端末、ウェブサーバ：平成20年度中 |
| 農林水産省 | A | A | A | 対策実施済み |
| 経済産業省 | A | A | A | 対策実施済み |
| 国土交通省 | A | A | A | 対策実施済み |
| 環境省 | A | A | A | 対策実施済み |
| 防衛省 | A | A | A | 対策実施済み |

※ 「B→A」の表記は、平成20年11月時点でのB評価が、平成21年3月末時点でA評価（見込み）となることを示す

# 第1次情報セキュリティ基本計画における重点検査の総評

## 1．重点検査結果について

### ○　政府機関全体における検査対象の保有台数及び情報セキュリティ対策の実施率・評価

- **端末：約55万台（前回：約53万台）**　98％・評価Ｂ（前回：93%・評価Ｂ）
- **ウェブサーバ：約1,000台（前回：約1,400台）**　99％・評価Ｂ（前回：93%・評価Ｂ）
- **電子メールサーバ約1,900台（前回：約1,900台）**　99％・評価Ｂ（前回：96%・評価Ｂ）

政府機関統一基準に準拠した適切な対策が概ね実施されているものの、一部に対策が不十分な項目がみられる。

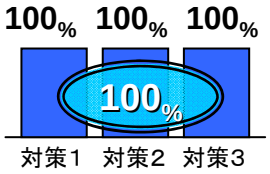
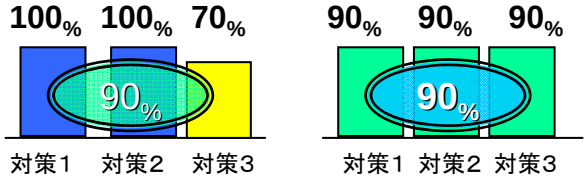
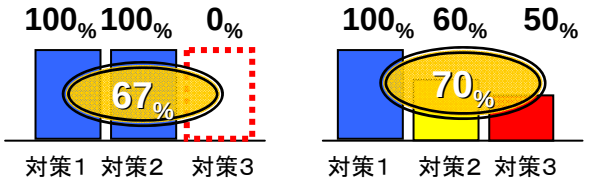
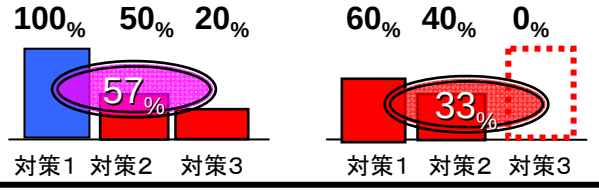
## 2．所見

① 端末･ウェブサーバ及び電子メールサーバは、対策が不十分な場合、情報の漏えいや改ざん、破壊等の要因となり、府省庁業務や利用する国民･職員に影響を及ぼすリスクが高く、また、検査対象の項目は、政府機関統一基準の基本遵守事項であることから、本来100%実施することが期待されるものである。このため、**第1次情報セキュリティ基本計画(2006～2008年度)の最終年度であることを踏まえ、対策が不十分な項目について早急な改善が必要である。**

② **政府機関全体で、ウェブサーバ約1,000台、電子メールサーバ約1,900台がそれぞれ設置･運用**されており、ウェブサーバについては、前回検査(H19.3)から一定の削減又は集約化が図られているものと想定される。一般に、多数の計算機を設置･運用し、管理工数やコストが増えるとセキュリティ維持の工数も増大する。その結果、すべての計算機の対策確認が疎かになりやすいなど、セキュリティリスクが高まることから、情報セキュリティの観点からも各府省庁の業務や実情に応じて、**ウェブサーバ及び電子メールサーバの集約化を選択肢の一つとして検討するべきである。**

③ 重点検査は、各府省庁が、すべての項目で統一基準に準拠した対策が実施されているA評価の部分を維持するとともに、不十分な項目がみられるB評価等の部分を認識し、改善していくための指標として有意義であった。今後は、第2次情報セキュリティ基本計画(2009～2011年度)の実現に向け、同計画の下で作成･策定される情報セキュリティ報告書やそのガイドラインを踏まえつつ、検査内容のさらなる充実を図る必要がある。

# 政府機関の情報セキュリティ対策の総合評価の見方について

| 評価 | 実施率 | 対策状況 | 個別対策項目についての評価パターン例 |
|---|---|---|---|
| A | 100% | 適切に実施すべき対策について、**すべての項目で**統一基準に準拠した**対策が実施**されている。 |  |
| B | 80%≦x＜100% | 適切に実施すべき対策について、**概ねすべての項目で**統一基準に準拠した**対策が実施**されているが、**一部の項目で不十分なもの**が含まれている。 |  |
| C | 60%≦x＜80% | 適切に実施すべき対策について、**不備の項目が一部に見られる**など、対策が遅れている。 |  |
| D | 60%未満 | 適切に実施すべき対策について、**不備の項目が相当数、見られるなど**、対策が著しく遅れている。 |  |

◆ **評価方法** ：

各カテゴリーの平均実施率（項目毎に算出した対策実施率（※）の総平均値）の平均値を総合評価の実施率とした。

政府機関統一基準で求める情報セキュリティ対策がすべて実施されていれば、総合評価の実施率は100%、すなわち“A評価”となる。

$$（※）対策実施率 = \frac{実際に情報セキュリティ\underline{対策を実施している対象数}（端末・サーバ台数）}{情報セキュリティ\underline{対策を実施すべき対象数}（端末・サーバ台数）} \times 100 \quad （\%）$$

# 参考　補完調査の主な結果について

## １．サーバ証明書の暗号アルゴリズムの活用状況

○　インターネット上で一般的な暗号化データ通信（SSL/TLS通信）をする際には、サーバ証明書が活用されているところ、それに用いられている暗号アルゴリズムも今後移行していく必要があり、その証明書の発行者について、状況を調査した。

→　補完調査の結果、各府省庁においては、約3割が政府認証基盤（GPKI）等政府機関発行のサーバ証明書を、約7割が民間認証局発行のサーバ証明書を使用していることがわかった。このため、今後の移行に際しては、GPKI等の政府機関のみならず、民間も含めて適切な移行を促していく必要があることが再確認された。

　なお、一部の証明書には、MD5等の安全性に問題のある暗号アルゴリズムを使用していたので、該当する府省庁においては、原則、GPKIを活用し、安全な暗号アルゴリズムへの変更を行うこととする。

## ２．送信ドメイン認証の対応状況

○　ウイルス付きメール等の迷惑メールへの対策において効果的である、送信ドメイン認証技術の対応状況について調査した。

→　補完調査の結果、現時点で送信ドメイン認証技術が導入されている府省庁は数％（IPアドレスを活用した方式：約8％、電子署名を活用した方式：約5％）であったが、対応可能なサーバを保有している府省庁は、それぞれ約4割程度あることがわかった。今後、政府機関においては、これらのうち、一般に普及しており、かつ、導入が容易なSPF（ Sender Policy Framework ）の採用等を推進していき、政府機関を狙ったウイルス付きメールなどに効果的な対策を講じていくこととする。

補完調査とは、強化遵守事項の適用状況や迷惑メール対策等情報セキュリティ対策上重要な事項に関する状況の把握等を行うものであり、重点検査で調査する項目に補完調査項目を追加する形で実施されるもの（「情報セキュリティ政策2008年度の評価等に向けた『作業方針』（2008年12月10日情報セキュリティ政策会議資料）」より）。