平成１４年１１月２５日
情報セキュリティ専門調査会

各省庁における情報セキュリティポリシー実施状況の評価等について（案）

１　評価の経緯

「電子政府の情報セキュリティ確保のためのアクションプラン」（平成１３年１０月、IT 戦略本部情報セキュリティ対策推進会議決定）及び本年５月に改定された「e-Japan 重点計画 2002」（IT 戦略本部決定）において、電子政府の情報セキュリティ確保に向けた重要施策として、「情報セキュリティポリシーの実効性の確保」が掲げられたところ、本施策の一環として、内閣官房において各省庁の情報セキュリティポリシー（以下「ポリシー」という。）の実施状況を評価したものである。

２　評価の目的

各省庁のポリシー及びこれに基づく情報セキュリティ対策の実施状況を評価し、その結果を当該省庁に提供することにより、当該省庁においてポリシーの見直しや更なる対策を実施する際の参考とするとともに、「情報セキュリティポリシーに関するガイドライン」（平成 12 年 7 月、IT 戦略本部情報セキュリティ対策推進会議決定。以下「ガイドライン」という。）の見直し等に資することとする。

３　評価の方法及び対象

各省庁で保有する LAN、ホームページ、汎用受付等システム等から数システムを抽出し、これらについてポリシーの実施状況をチェックシート等による書面調査及び各省庁のシステム管理に携わる者へのヒアリングにより実施した。

なお、本評価は、内閣官房情報セキュリティ対策推進室専門調査チームが実施した。

４　評価結果の概要

評価結果の概要は次のとおり。

（１）総論

各省庁における情報セキュリティ対策に関する取り組みは、平成１２年１月に発生した省庁ホームページ改ざん事件以降、ポリシーの作成や体制整備、政府内緊急連絡網の構築・運用、各種事案への対処等を通じて、省庁の意識と対策の両面において相当の進展が見られる。

今回の評価においては、一昨年、昨年に比べ対策の実施状況が改善しているケースが多く見られ、特にポリシーの運用面で大きな問題が生じている省庁は見られなかった。

一方、限られた予算、体制等の中で実施しなくてはならないという制約等から各種対策が必ずしもポリシーで定められた対策基準に沿って実施されていない場合が見られるほか、ポリシーの対策基準が必ずしも実情に合致していないため対策の実施に支障が生じているものが見られるなど、ポリシーの全ての対策基準が完全に機能しているとはいえない状況が見受けられた。

このため、今後、電子政府の情報セキュリティを確保するための基準として、ポリシーを中心に据えた体系的な対策を一層推進することが必要である。

具体的には、各情報資産で求められる対策を精査し、監査、予算、組織等の必要な措置を電子政府の構築に併せて計画的に実施するとともに、対策基準の評価・見直し、実施手順等の作成等のいわゆる「ポリシーの実施サイクル」を効果的に機能させていくことが必要である。

なお、今回の評価は各省庁の保有する情報資産のうち限られた範囲を対象として行ったものであり、各省庁においては、本評価を参考としつつ抽出範囲以外の情報資産についてもポリシーの実施状況を評価することが必要である。

（２）主な項目の評価と対応策

ア　ポリシー等の策定について

（ポリシー等の策定）

- 全省庁においてポリシーの策定が完了しており、ポリシーに基づいた対策が進められているが、実施手順の文書化については作業途上の省庁が多く見受けられた。また、実施手順の規定方法が明確に体系化されていない状況が見られた。

  このため、今後、システム管理部署、ユーザ、委託業者等が適切に対策を実

施するために必要な手順・要件等について、必要に応じ手順書、契約等における明確化を推進していくことが必要である。

イ　組織体制について

（意思決定体制）

・　省庁における情報セキュリティに係る予算、組織、計画等の重要事項に関する審議・意思決定が、情報セキュリティ委員会等トップレベルの組織において十分にされていない状況が見受けられた。

特に、電子申請・届出等の推進に伴い、重要な情報を扱う情報システムの整備・管理が一省庁内の複数部署において行われる傾向にあることから、省庁全体としての情報セキュリティ確保に向けた総合調整を適切に行うことが重要である。

このため、各部署の情報セキュリティ対策に関するレビュー等を適切に行うため、委員会事務局の機能及び体制の強化、情報管理部門（監査班等がある場合には当該部署）による部局を超えた情報セキュリティ監査に係る権限及び体制の強化について検討することが必要である。

（情報管理部門等の体制）

・　情報システムの整備・管理に携わる各部署において担当者への負担が極めて大きく、セキュリティ対策上の支障が懸念される状況が一部見受けらることから、十分な体制が確保されているか評価する必要がある。

ウ　物理的・人的・技術的セキュリティについて

（評価結果を踏まえた措置）

・　今回の評価で認識した脆弱性や新しい技術の導入による問題点等について、現在保有する情報資産及び近い将来に保有する予定のある情報資産に対するリスクを検討し、ポリシーの対策基準及び対策の実施に過不足がないかどうか評価することが必要である。

（教育・訓練）

・　システム管理に携わる者及び一般職員に対する教育・訓練について、専用のマニュアルや教材を作成し実施している省庁がみられる一方、イントラネットでポリシーを掲示するのみの省庁も見受けられた。

今後、職員一人一人のセキュリティ意識の醸成、情報システムの管理等に携わる者の知識・能力を育成するための取組を更に推進する必要がある。

（外部委託時の対策）

・　外部委託時における資料・記録の管理、開発・運用時等の手続き、下請業者管理等に関するセキュリティに係る要件が書面等で明確化されていないケースが一部見受けられることから、外部委託時におけるセキュリティ要件の明確化を一層推進する必要がある。

エ　運用について

（監査）

・　第三者による情報システムの技術的な脆弱性調査については多くの省庁で実施されているが、予算の事情等により実施されていない状況も見受けられた。
　また、運用や人的セキュリティ等のポリシーの実施状況に関する監査を実施しているところは少なかったが、情報資産の重要性に応じ、今後検討していくことが必要である。

（監視・緊急時対応体制）

・　監視について、侵入検知装置の設置や 24 時間監視体制の整備等がされていないケースが見受けられ、リスクの大きさに応じた適切な脅威の監視が行われているか再検討する必要がある。
・　緊急時対応計画が手順や契約等で明文化されていないケースが見受けられ、緊急時の迅速な対処のため、サービスの停止、幹部への連絡・報告、国民への広報等について、侵害の度合いに応じて予め判断基準・手順を作成することが必要である。

5　ポリシーの実効性の確保に向けた今後の取組みについて

今回の評価を受け、ポリシーの実効性の確保に向け、今後、次の取組みを推進し、電子政府の情報セキュリティ確保に万全を期すこととする。

（１）政府全体の取組みについて

ア　「情報セキュリティポリシーに関するガイドライン」の見直しについて

評価結果を踏まえ、次の点についてガイドラインの見直しを行う。

（ア）実効性を一層高めるための見直し

評価結果から実効性を一層高めることが必要と思われる項目について、記述の見直しを行なう。

（イ）新たに考慮するべき事項の追加

新しい技術の導入や電子申請・届出等の実施等を踏まえ、対策基準として考慮するべき事項を追加する。

（ウ）各省庁の実情に合わせた取組みのための見直し

各省庁がポリシーを評価・見直しを行なう際、各省庁の実情に合わせた取組みを推進するための記述の見直しを行なう。

イ　ベストプラクティスの作成について

ポリシーに従った実施手順等については作成途上の省庁が多く見受けられることから、「ポリシー例」の見直しに合わせて、実施手順等を検討する際にベストプラクティスとして参考となるような資料を本年中に作成する。

（２）各省庁における取組みについて

ア　ポリシー等の評価・見直し

・　今回の評価結果及びガイドラインを参考として、自省庁におけるポリシー、実施手順等の評価・見直しを本年度中に行う。

イ　ポリシーに基づく実施手順の整備等

・　評価結果を参考として、未実施の対策やその他必要と思われる対策も含めて必要性及び重要性を検討し、優先度の高いものから順次、迅速に実施するも

のとし、この際、予算、組織体制等を伴うものについては計画的に措置するなどしてポリシーの運用の徹底を図る。

- **ポリシーに基づく実施手順について、他の規定との整合性等を考慮に入れるなど体系的な規定方法を検討し、手順書、契約等における明確化を推進する。**