資料６－２

外　　務　　省

１．「『第２次情報セキュリティ基本計画』（仮称）に係る検討の視点（例）」に対する意見

（１）「政府機関・地方公共団体における情報セキュリティ対策について（２）」(P.9)

項目７．については、「政府機関の情報セキュリティ対策は、各府省庁の責任において実施しているが、限られた予算と不十分な人員の下、施策の優先順位付けが必要ではないか。」という視点で検討すべきと考える。

（理由）

「セキュア・ジャパン２００７」第１章第３節「２００６年度の評価」１．において、「「各政府機関でのＰＤＣＡサイクルの確立」、「政府全体でのＰＤＣＡサイクルの確立」という対策の大部分を占める施策がA’となっていることから体制や人員等の不足が大きな課題であることがうかがえる」とされており、人員面が十分でないことは既に明らかになっている。また、厳しい予算事情を考慮すれば、優先順位が不明確な施策に対して予算を満額確保できる保証はなく、経費捻出のために他の施策にしわ寄せが及ぶ懸念がある。したがって、施策の優先順位付けについての検討が必要と考える。

（２）「政府機関・地方公共団体における情報セキュリティ対策について（２）」(P.9)

項目９．「安全保障・外交等の機密情報を扱う場合をどうするか。ＣＩ（カウンターインテリジェンス）との関係」については、削除を検討して頂きたい。

（理由）

「政府機関・地方公共団体における情報セキュリティ対策」では、あくまでも政府・自治体に共通する横断的な「情報セキュリティの仕組み」に関する項目が議論されるべきと考える。

安全保障・外交等の機密等については重要な論点であるが、一部の省庁が保有する特殊な情報のセキュリティについては、当該省庁が各々の情報の性格（指定された機密性等）に応じてセキュリティ対策を施すべきであり、地方公共団体を含めた全体の中での検討には馴染まないものと認識している。

（３）「国際連携・協調の推進に向けた取り組みについて」(P.24)

項目１．について、国際機関での取組みとの整合性について議論すること自体は結構なことであると考える。

当省としては、既存の枠組みで対処可能なものは引き続き関係省庁と協議しつつ、また、新規の提案については内閣官房における更なる具体的検討を踏まえ、可能な協力につき協議に参画していきたいと考えている。

２．政府機関を対象とした情報セキュリティ政策に関する意見

（１）現在進めている、政府機関を対象とした情報セキュリティ政策に対する意見、及び今後の政策への展望について

現在の「第１次情報セキュリティ基本計画」の「第３章　今後３年間に取り組む重点政策－『新しい官民連携モデル』の構築－」内「 第１節 対策実施４領域における情報セキュリティ対策の強化」の「（１）ア 政府機関」の「①政府機関統一基準とそれに基づく評価・勧告による PDCA サイクルの構築」の第２パラグラフに「また、各政府機関の情報セキュリティ対策の実施状況を、政府機関統一基準に基づき、必要な範囲で検査・評価し、勧告を通じた各政府機関の対策の改善と政府機関統一基準等の改善に結びつけることで、政府全体としての PDCA サイクル（Plan-Do-Check-Act サイクル）を確立する。なお、評価の結果については、情報セキュリティの維持・確保にも配慮しつつ公表することとする。」と記述されているところ、（更に、「セキュア・ジャパン２００７」には、「第３章 第１節 ア ①【具体的施策】ウ）本格的な評価の推進及び結果の公表」に「また、評価の結果については、政府全体としての効果的な対策の推進を図るとともに、国民への説明責任を果たすためのものとして情報セキュリティの維持・確保にも配慮しつつ公表することとする。」と記述されているところ、）

（イ）これまで端末・ウェブサーバ、電子メールサーバについての検査を実施し、その評価の結果を各府省毎に公表されてきたが、我が国の政府機関に情報セキュリティ上問題があるということを公表することによる負の側面にも十分な考慮が必要と考える。日本国行政府の、端末・ウェブサーバ、電子メールサーバといった特定のものについての情報セキュリティ対策状況として不十分な点があるということを一般に公表していく場合、世界各国・地域との関係上、我が国の国益を損じることとなる可能性すら排除できない。国民への説明責任の重要性は言を俟たないが、国益を損ずることの無きよう慎重な配慮が必要である。

（ロ）また、当該検査の評価結果を公表することに伴って、各府省庁においては当該検査へリソース（人的、予算的）を傾注せざるを得ず、その負担も大きい。当省（外務省）を含む各府省庁は、極めて限られた人的資源の中で、情報セキュリティ対策に当たっているところ、最小のコストで最大の効果を得るべく対策のためのリソースの最適配分を可能とすることを前提に、公表・不公表のあり方を考えて頂きたい。

（２）当省固有の留意点について

在外公館における情報セキュリティ対策については、国ごとに情報インフラの整備状況が異なり、我が国のように情報インフラが整備されている国ばかりではない点に配慮願いたい。言語や文化、現地業者等、環境は多種多様であり、国内での対策に重点をおいた基準を、在外公館にも一律に適用することは現実的ではない場合が多々ある。対策の趣旨を踏まえつつ個別に対処する方が、限られた予算と人員の下、適切な情報セキュリティ対策が行えると考える。

３．情報セキュリティ対策に係る予算の特殊事情について

情報セキュリティ対策に係る予算については、各府省とも種々の情報システムの中で、OS のアップデートやウィルス防止ソフトのパターンファイルの更新に加えて、システム機器ハードウェア・ソフトウェアの更新及びシステム内アプリケーション・ソフトの更新並びにこれらのソフトの上で稼働している開発済みシステムのアップグレード（稼働テストを含む）が必要となる。このための経費は減価償却が終わるタイミングを待たず、各 OS やアプリケーション・ソフトのサポート切れのタイミングがあるため、それぞれのシステムのヴァージョンに応じて対応することが求められる。この他、当省の特殊事情として、在外公館におけるシステムの更新作業が必要となる。本省から２００程存在する各在外公館にリモート接続で対応できる範囲であればともかく、この種の作業に当たっては、物理的サーバの更新やメモリ増強、OS のアップグレード等、物理的にシステムエンジニアが現地において作業せざるを得ない場面が多い。この結果、全在外公館に短期間でシステムエンジニアを派遣して作業を実施するとなると多額の経費がかかるため、予算上の制約から、現実問題として十分な対応が困難な状況にある。

ついては、政府として情報セキュリティ対策が重要という認識の下で、この手の情報セキュリティ対策を充分かつ適切・迅速に実施していくためには、予算手当に係る情報セキュリティ当局の支援を得て、十分な予算確保を行っていけるよう重点対策のひとつとして掲げていただきたい。

以上