国家情報セキュリティセンター（NISC）の草案「政府組織の情報セキュリティ措置のための統一基準」（2005 年 12 月用の最初の全体バージョン）に対する米国政府のコメント

２００５年１１月１１日

前置き

米国政府は、NISC の草案「政府組織の情報セキュリティ措置のための統一基準」（2005 年 12 月用の最初の全体バージョン）へのコメントを喜んで提出する。国家標準技術局(NIST)を通じて米国政府は、米国の国家安全保障に関わらない連邦情報システムの基準とガイドラインを作成することで多大な経験を有する。連邦予算管理局 (OMB)も、 NIST の要件のコンプライアンスを連邦各省庁が評価することを手伝うことで多大な経験を有する。

米国は、日本政府の情報システムのためのセキュリティ要件を作成・実施するというチャレンジに満ちた作業に NISC が取り組むことを高く評価する。米国政府は、特にサイバーセキュリティへの脅威、研究、および知識が急速に進展している状況の中で、この分野において両国政府がベストプラクティスを共有することが重要であると信じる。

さらに米国は、 NISC が草案基準への一般からのコメントを求める　ことも高く評価する。 NIST はオープンな基準作成アプローチを同様に使うことによって大いに恩恵を被っている。このようなプロセスは、可能な限りベストでかつ技術的にも最も実現可能な基準を作ることに役立ち、作成される基準・ガイドラインが十分厳しく吟味され　　ることを保証し、それによって容認されやすくなる。また、個人情報を含むシステムの保護という政府の努力に対して、一般市民の意識が高まるとともに、信頼感の強化につながる。

米国はいくつかの全般的なテーマに関して今回コメントを提出している。米国政府は、こうした基準のさらに十分な探索と、一般コメント期間が終了後に日本とアイデアの共有を続けることを心待ちにしている。

NIST は、経済産業省(METI)および情報技術促進局(IPA)との協力的な関係を長い間続けてきており、科学者やその他の担当官と情報セキュリティ課題を定期的に議論している。OMB は、連邦各局の情報セキュリティ評価を議論するために、さまざまな日本政府担当官や産業界の人々と何回も会っている。NIST と OMB の双方は、政府情報システムのセキュリティに関して 、NISC との今後の話し合いの機会を歓迎する。

コメントの評価と統合

米国は、NISC が一般コメント期間中にこの基準に関して寄せられた　全コメントおよびフィードバックを慎重に査定し、結果的に基準・プロセスの改善につながる提案を取り入れるように奨励する。米国は、 NISC に対しコメントを明確にしさらに情報が必要な場合には直接コメント提供者に相談するべく最大限の努力をするよう提言する。

米国は、2005年9月に発表されたタイムラインに基づいて、NISCが 2005年12月にこの基準の最終版を発表する計画である、と理解している。米国は、NISC がこのタイムラインに関し最終基準発表のためにできるだけ柔軟に対応するよう、そして必要とあればこれを延長するように提言する。最終発表の日付に厳しくこだわるより、むしろ重要なことは受け取ったコメントの検討、追加情報の収集、または明確化　　に十分な時間を当てて、適切な場合には改正草案を発表して、追加のコメント期間を設けることである。　この必要性を認識して、NIST は 2002年連邦情報セキュリティ管理法 (FISMA)の下で、米国連邦各局のための法的義務のある最低限の情報セキュリティ要件を作成するために3年間という期間を与えられた。さらに、NISTの特別出版物800-53 (重要なセキュリティコントロールガイドライン)はもともと2004年6月に発表予定だったが、政府や業界顧客からのコメントを取り入れるためにもっと多くの時間が必要だったので2005年2月に発表された。

十分に吟味して改善されることなく情報セキュリティ要件が決定されると、脆弱な基準を作る結果になったり、後に変更することになる要件の実施をユーザーが始めてしまうリスクをおかすことになる。　__さらに、作成のサイクルと一般検討期間を延長することによって、貴国の各省庁は新要件への移行へのよりよい準備ができる。NISC がコメントを統合するためにもっと時間が必要であるものの、基準全体　__の発表を遅らせることができない場合には、NISC が 2005 年 12 月の締め切りに際して、十分に完了していると思えるセクションのみを発表するよう提言する。

将来の基準・ガイドラインの作成と検討

米国は、 NISC が草案・導入、応用、評価および検討のサイクルを通じてセキュリティ基準とガイドラインの評価を今後数年間行う計画である、と理解している。米国はこのアプローチはよいと認識している。情報システムのセキュリティコントロールを選択・特定するための指導を提供する実施ガイドラインは、新技術に対応できるようにできる限り頻繁に最新化されるべきである。政府は一般的でかつ現在も将来も適用できる基準を 配備するようあらゆる努力をすべきであるが、どのような基準も急激な技術進歩の前ではすぐ時代遅れになってしまう。したがって、セキュリティ基準とガイドラインは、技術やビジネス的理由に照らしてより精度を高め最新化する必要があるかどうかを定期的に検討すべきである。

米国は、将来発表される政府の全コンピュータセキュリティ基準とガイドラインに関して、一般コメント手続きやその他のフィードバック入手方法を含むオープンな作成プロセスを NISC が使うよう強く奨励する。NISC は、ガイド・基準アプローチを使うことも検討するかもしれない。すなわち提案中の要件をガイドとして発表し、それが　　__どのように受け入れられ利用されるかをみてみる。各省庁においてこれがうまく機能すれば、基準として発表することになる。

さらに米国は、日本が一般コメント手続きにオープンワークショップと一般ブリーフィングを補足するように提言する。米国は、このような方法が最大限に広範な聴衆とコメントをもたらすために役立つことを経験した。

最後に、米国は NISC がいつでも公式・非公式なコメント（例えば、一般コメント期間が終了後、あるいはユーザーの経験に基づいて）を受け入れるよう提言する 。一般コメント手続きはコメント収集プロセスを簡単にするが、ベストアイデアはいつでも出てくる可能性があるからである。

<u>自主的な標準化団体が作成した基準との一貫性</u>

2004 年の日米規制改革および競争政策イニシアチブの下でのリーダーへのレポートの中で、日本政府は 政府「ガイドラインと基準は適切な場合には、オープン（機密ではない）であり、かつ業界のコンセンサスの上に構成された、自主的な標準化団体により作成された基準と一貫性があるものになる」と確認した。米国は、自主的な標準化団体によって作成された基準と一貫性のある政府セキュリティ基準を発表しようと努力するアプローチに合意する。この目的のために、米国は NISC が基準とガイドラインを発表する際に NIST が使っている以下のアプローチを使うことを検討するように提言する。優先順位をつけて記すと、第一に、既存の自主的な業界基準が使用可能で受け入れられるものであるならば、これを採用するか、適合させる。　もし　そうでない場合には、自主的な業界基準作成努力に参加して、共通の政府業界基準を作成し、完成した基準を政府で使用する基準として採用するか、適合させる。最後の手段として、 NISC の権限と内部の資源を使って各省庁向けの基準とガイドラインを作成する。

<u>技術の中立性</u>

米国は、日本政府の情報セキュリティ全要件ができる限り技術的に中立であることを奨励する。米国は、最初の一連の基準が特定の技術選択を指定しないと理解しており、日本がこのアプローチをとることを　評価する。米国は、各省庁が実施をする際に最大限の柔軟性が与えられ、かつ民間セクターの革新を奨励するために、可能な限り今後のガイドラインや追加基準で日本が特定の技術を促進したり、法的に義務付けたり、不当に優遇することがないことを保証するよう奨励する。 さらに、日本政府のセキュリティ基準やガイドラインに見合うための情報

技術やサービスの調達 は国内海外の全ベンダーにとって公正かつ透明であるべきである。

最低限の政府情報セキュリティ要件の義務付けと実施における一貫性の保証

米国は、日本が各省庁に一連の最低限情報セキュリティ要件を義務付けることに向けて検討するよう提言する。その中には、緊急時計画や侵入探知といったような基本的な要件を含める。また米国の FISMA モデルの検討も参考になるかもしれない。これは立法府が義務付けられた最低限の連邦情報セキュリティ要件の作成を指示し、行政府が適切なセキュリティ基準とガイドラインを実施するというもの。　義務付けられた最低限の要件を示すことにより、各省庁に対しセキュリティのためのより効果的な予算作成のベースラインを提供できる。さらに義務付けられた最低限の要件は、ベンダーに予測性を提供し、各省庁の要件に見合うような方法で商品や管理ツールを合理的に売り込む助けとなりうる。

最後に米国は、最低限の情報セキュリティ全要件が全省庁に一貫性をもって実施されるよう NISC が努力するように提言する。各省庁は　各々特徴をもっており、最低限の要件を超える独自のセキュリティ措置を必要とするかもしれない。しかし、各省庁が同じベースライン要件を使うことにより、その必要性に見合うベンダーや技術をより広く選択できるようになる。