政府機関統一基準に関する説明資料

政府機関の情報セキュリティ対策について、政府機関統一基準を策定し、これによって各府省庁の情報セキュリティ対策の整合化・共通化を促進し、政府機関全体としての情報セキュリティ水準の向上を図る。この方針の具体化のために、政府の基本方針を定め、政府機関統一基準の策定・運用の枠組みを示す統一基準運用指針を策定する。本施策の実施によって、政府機関の情報セキュリティ水準の向上が期待できるとともに、政府機関の情報セキュリティ問題の背景にある専門的人材の不足という構造問題についても補完的効果が期待できる。

１　政府機関における情報セキュリティ対策の現状

政府機関の情報セキュリティ対策については、平成１２年７月１８日に情報セキュリティ対策推進会議が決定した「情報セキュリティポリシーに関するガイドライン」（以下「旧ガイドライン」という。）に基づき、各府省庁がそれぞれ自らの責任において独自に情報セキュリティポリシーを策定し対策を実施してきたところである。その後、平成１４年１１月には、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を行うとともに、旧ガイドラインの一部改訂を行い、さらに、平成１５年９月の情報セキュリティ対策推進会議の決定に基づき、内閣官房が各府省庁の情報システムに対する脆弱性検査を実施するなどにより対策の定着と問題点の把握を図ってきた。

旧ガイドラインの下で、各府省庁は明文化された情報セキュリティポリシーを持つようになり、対策の基本的枠組みが整備されたことにより、政府機関の情報セキュリティは全体として一定の向上を見ているが、上述の脆弱性検査の結果、政府機関の情報セキュリティ対策は、(1)情報セキュリティ水準の高い府省庁と低い府省庁の格差が大きい、(2)内部からの不正アクセスに対して脆弱、といった問題があることが明らかとなった。

２　政府機関における現状の情報セキュリティ対策の問題点

脆弱性検査の結果などから明らかとなった問題の重要な背景の一つとして、情報セキュリティ対策を適切な水準で実行するために必要な人材の大幅な不足という各府省庁に内在する構造的な問題が存在する。

政府機関の情報セキュリティ対策の現状の枠組みは、旧ガイドラインに示されているように、各府省庁が自らの情報資産を把握し、それに適した対策を自ら選択するという、情報セキュリティ対策の一般原則論を踏まえたものであり、政府機関全体としてみると、分散的自己完結責任型の情報セキュリティポリシー体制であると言える。

しかしながら、急激に変化し続けるネットワーク環境と、日々生起する新たな脅威に対して、適切な情報セキュリティ水準を確保し続けることは、かなり高度な専門性を有する仕事である。各府省庁において情報セキュリティに関する知識が豊富な専門家が不足する中で、対策の適切さについて不安を拭うことはかなり難しく、また量的な観点から見ても、情報セキュリティポ

リシーどおりに対策を講じつつ、情報セキュリティポリシー自体も、随時適切に見直していくという業務は、各府省庁にとって大きな負担となっている。

結果として、現在の分散的自己完結責任型の枠組みのみでは、各府省庁が情報セキュリティを適切な水準に確保することは極めて難しいと判断せざるを得ない。このことは、運命共同体的側面を持つ政府機関全体として見たとき、政府機関全体の中に脆弱性を抱え持つ構図となっている。

3　新しい枠組みの構築に向けての方向性

上記の問題の解決の基本は、各府省庁において専門的人材を十分な人数だけ育成・確保することであるが、これには時間を要するため、現時点で早急に対策を充実させるためには、各府省庁の自己責任に基づく情報セキュリティ対策の既存枠組みに加え、内閣官房情報セキュリティセンター（以下、「センター」という。）に情報セキュリティに関する知識と情報を集め、センターが各府省庁の責務の実行を支援するという枠組みを付加することが、最も実行可能性の高い方向性であると考えられる。

この方向性を具体化し、政府機関全体として高いレベルで水準のそろった情報セキュリティを確保するため、政策会議として次の３つの文書を定める。

（１）政府としての基本的な方針を定めた「政府機関の情報セキュリティ対策の強化に関する基本方針」（政府基本方針）

（２）政府機関統一基準を運用する具体的な枠組みを示すものとして「政府機関の情報セキュリティ対策のための統一基準の策定と運用等に関する指針」（統一基準運用指針）

（３）各府省庁が採るべき対策等を定め、対策強化・整合化の主要な手段となる「政府機関の情報セキュリティ対策のための統一基準」（政府機関統一基準）

4　政府基本方針の考え方

「政府機関の情報セキュリティ対策の強化に関する基本方針」は、政府が行うべき基本的事項として以下の事項を挙げている。

（１）政府機関統一基準の策定
（２）各府省庁での情報セキュリティポリシー等の見直し
（３）各府省庁での自己点検等
（４）政府全体でのＰＤＣＡサイクルの確立
（５）情報セキュリティ確保に有効な制度等の活用の促進
（６）独立行政法人等のセキュリティ対策の改善
（７）新たな脆弱性等に対するセンターと府省庁との連携
（８）情報セキュリティ人材の育成の支援・促進
（９）その他、政府全体での中長期的な対策の強化

5　政府機関統一基準の内容について

政府機関統一基準は、情報セキュリティに関する国際基準であるＩＳＯ／ＩＥＣ１７７９９を始め、内外の基準を踏まえて我が国政府機関のために策定したものであり、各府省庁が最低限行うべき対策（基本遵守事項）及びより重要度の高い情報に対する対策（強化遵守事項）を

定めている。

基準の構成は以下の通り。

第１部　総則	第４部　情報セキュリティ要件の明確化に基づく対策
第２部　組織と体制の構築	第５部　情報システムについての対策
第３部　情報についての対策	第６部　個別事項についての対策

6　統一基準運用指針に示された運用枠組みのポイント

統一基準運用指針に示された政府機関統一基準の運用の枠組みは、次に示す３つの取組みを骨格として構成されている。

（１）政府機関統一基準の策定と各府省庁における情報セキュリティポリシーの見直し

政府機関統一基準を策定し、各府省庁においては、政府機関統一基準に準拠して、自らの情報セキュリティポリシー（省庁ポリシー）の見直しを図り、対策の底上げを図るという取組み

（２）対策実施手順書の整備の支援（各府省庁に対する草の根支援）

省庁ポリシーを反映した多数の実施手順書等を各府省庁が作成するうえで、手引き又は参考となるガイドライン群をセンターが作成し、各府省庁の利用に供するという取組み

（３）対策実施状況の確認と評価に基づくＰＤＣＡサイクルの確立

各府省庁自らが行う自己点検・自主検査、第３者の視点でセンターが行う検査と評価、当該評価結果をもとに情報セキュリティ政策会議が行う勧告、これらを受けて政府機関統一基準と省庁ポリシーを見直すというＰＤＣＡサイクルの取組み

7　政府機関統一基準の運用等に関するスケジュール

今回の政策会議では、政府基本方針、統一基準運用指針及び政府機関統一基準の２００５年項目限定版（以下、「項目限定版」という。）を定める。政府機関統一基準に係る今後の取組み予定は以下のとおり。

◆　項目限定版を使った、対策の早期着手（ファーストトラック）

項目限定版の政府機関統一基準は、緊急度の高い対策のための基礎となる基準を中心に項目を限定して策定したもので、これに基づき各府省庁の基準整備、対策実施から評価までのＰＤＣＡサイクルを２００５年度内に１サイクル実行する。

◆　政府機関統一基準全体版を使った、標準的年度サイクルの開始

１２月に予定する次回政策会議において、項目限定でない全体版の政府機関統一基準を策定し、これをもとに２００６年度から、年度の１年を区切りとしたＰＤＣＡサイクルで対策を実施する。

※　上記スケジュールに合わせて、各府省庁に対する草の根支援として、各府省庁が省庁ポリシーを反映した多数の実施手順書等を作成しやすくするため、センターは個別のガイドラインを多数作成（個別ガイドライン群）