平成 17 年 10 月 17 日

# 「政府機関の情報セキュリティ対策のための統一基準」に追加すべき項目（骨子）

内閣官房情報セキュリティセンター

## Ⅰ　機器等の購入　<新規>

【　背　景　】

（1）　情報システム機器等（市販ソフトウェアを含む。以下同じ。）を購入する際には、必要なセキュリティ機能を持つ機器等を適正なコストで購入することが求められている。

（2）　情報システム機器等を購入し、業務に使用する場合に、購入先がその後必要な期間にわたりその保守を行う見込みがないと、府省庁における業務の安定性確保が期待できない。また、情報システム機器等に必要なセキュリティ機能が実装されていること及び脆弱性対策を購入後も継続して実施できることが、府省庁における情報の機密性、完全性及び可用性の確保において必要である。

（3）また、情報システム機器等の購入において、第三者機関による客観的な評価等を基に、セキュリティ機能等の妥当性を評価することが課題となっている。

【　改正の方向　】

〔考え方〕

Ⅰ-①　情報システム機器等の購入に際し、選定手続き等の整備と実施に関する遵守事項として、以下の趣旨の規定を追加する。

（a）　情報システム機器等（以下「機器等」という。）の購入に際し、情報セキュリティ対策の視点を加味して、機器等の購入先の選定手続き、選定基準及び購入先が具備すべき要件を整備し、これに従って、購入先を選定すること。【基本遵守事項】

（b）　購入する機器等に必要な情報セキュリティ機能が実装されていることを担保するために、機器等の購入に先立ち、機器等の選定手続き及び選定基準を整備し、これに従って、機器等を選定すること。【基本遵守事項】

（c）　機器等の納入時の確認・検査手続きを定め、確認・検査を実施すること。【基本遵守事項】

（d） 納入機器等に関して、購入先との間で納入後の保守・点検等の実施者及び実施条件を明確にし、その内容を文書で取り交わすこと。【基本遵守事項】
（e） 機器等の購入において、満足すべきセキュリティ機能の要求仕様がある場合には、これについて、情報セキュリティ評価・認証制度による認証を取得しているかどうかを評価項目として活用すること。【強化遵守事項】

## II ソフトウェア開発 <新規>

【 背 景 】
（1） ソフトウェアを開発する際には、当該ソフトウェアが運用される際に関連する情報資産に対して想定される脅威を分析し、その分析に基づいて脅威から情報資産を保護するためのセキュリティ機能及びその管理機能を適切にソフトウェアに組み込むことが求められている。
（2） 加えて、開発するソフトウェアにセキュリティホールが混入しないための対策も必要となる。

【 改正の方向 】
〔考え方〕
II -① 府省庁においてソフトウェアを開発する場合に、開発工程ごとに実施する遵守事項として、以下の趣旨の規定を追加する。

（a）ソフトウェアの開発工程における情報セキュリティに関連する開発手順及び環境について定め、その際必要性に応じて運用中の情報システムとは分離すること。【基本遵守事項】
（b）開発するソフトウェアにおいて取扱う情報の格付けに応じて、セキュリティ機能を適切に設計すること。【基本遵守事項】
（c）開発するソフトウェア及び当該ソフトウェアが運用される際に関連する情報資産に対して想定されるセキュリティ脅威を検討し、当該脅威への対策について定めること。【基本遵守事項】
（d）ソフトウェアの設計について、セキュリティの観点から設計の妥当性を確認するための設計確認（レビュー）を実施する範囲及び方法を定めること。【基本遵守事項】
（e）開発するソフトウェアにおいて行うデータ処理について、セキュリティの観点から処理するデータの妥当性を確認する範囲及び方法を定めること。【基本遵守事項】
（f）ソフトウェアコード作成に関する規定を整備すること。【基本遵守事項】
（g）開発するソフトウェアに対して、セキュリティの観点から実施する試験項目及び

試験方法について定めること。【基本遵守事項】

（h）脆弱性の原因となるソースコードの有無を検査する方法を定めること。【強化遵守事項】

（i）開発するソフトウェアについて、満足すべきセキュリティ機能の要求仕様がある場合には、これについて、情報セキュリティ評価・認証制度による認証を取得すること。【強化遵守事項】

## III 外部委託

【 背 景 】

（1） 府省庁外の者に情報処理業務等を請負させる場合には、当該府省庁が直接的にその業務の遂行過程や成果物を管理することが困難である。外部委託に係る業務における情報セキュリティレベルの確保のためには、委託先においても各府省庁と同等の対策を実施させるべく、契約行為の中で委託先への要求事項を明確にすることが必要である。

（2） 加えて、対象範囲の明確化や選定基準の整備等契約の事前準備の段階から、納品検査等契約終了時まで、外部委託の各実施段階における対策の実施が必要となる。

【 改正の方向 】

〔考え方〕

III-① 府省庁において外部委託を実施する場合に、契約の事前準備から終了時までの各段階において実施する遵守事項として、以下の趣旨の規定を追加する。

（a）委託先に実施させる情報セキュリティ対策の内容を整備すること。【基本遵守事項】

（b）整備されている選定手続、選定基準及び委託先が具備すべき要件に基づき、委託先を選定すること。【基本遵守事項】

（c）外部委託の終了時に、委託先に請け負わせた業務において行われた情報セキュリティ対策を確認し、その結果を納品検査の判断に加えること。【基本遵守事項】

## Ⅳ　BCP（事業継続計画）との整合的運用の確保　　<新規>

【　背　景　】

（１）災害又は重大な障害等が発生した場合の対応策を定め、事業を継続するための手続きとして BCP（Business Continuity Plan:事業継続計画）の整備が求められているところ、これに関係する情報システムについては、情報セキュリティポリシーによる管理が行われている。したがって、BCP の適正な運用、情報セキュリティの確保双方の目的を適切に達するためには、両者の整合的運用の確保が必要である。

【　改正の方向　】

〔考え方〕

Ⅳ-①　BCP との整合的運用の確保に関する対策基準を定める。

（a）BCP の整備計画について情報セキュリティ委員会が適時に知ることができる体制を構築すること。【基本遵守事項】

（b）BCP の策定に当たり、すべての情報システムについて、BCP との関係の有無を確認し、関係のあるものについて、BCP と情報セキュリティの共通の実施手順を整備すること。【基本遵守事項】

（c）通常時において BCP と情報セキュリティ対策の共通要素を整合的に運用するため、情報セキュリティの枠内で必要な見直しを行うこと。【基本遵守事項】

（d）事態発生時において BCP の実施に障害となる可能性のある情報セキュリティ対策の遵守事項の有無を把握し、整合的運用が可能となるよう事態発生時の規定（例外措置）の整備を行うこと。【基本遵守事項】

## Ⅴ　情報保証のための機能　　<新規>

【　背　景　】

（１）　統一基準では、4.1.1～4.1.4　までの各項により情報セキュリティ機能の必要性の有無の確認と、必要と認められる場合の遵守事項を規定している。これに加えて、アクセスする情報に対してこれら機能が有効に実施されていることを確認するための上位の機能（セキュリティ・コントロールの保証（Security Control Assurance））等があることで、情報セキュリティが高まるという考え方がある。

この考え方は、情報保証（Information Assurance）と呼ばれており、一般的な情報セキュリティよりも上位の概念とされている。また、そのための対策は、限られた情報システムに導入されているのが現状であるが、本基準では、その機能が高度であるから最初から除外するのではなく、必要性の有無を確認し選択的に導入することが求められている。

【　改正の方向　】

〔考え方〕

Ⅴ-① 情報保証のための機能に関して、以下の趣旨の規定を追加する。

（必要な用語定義を追加し、遵守事項を 4.1.5 に追加する予定。）

（a）すべての情報システムについて、セキュリティ・コントロールの保証等の情報保証のための対策を行う必要性の有無を検討すること。【基本遵守事項】

（b）情報保証のための対策を行う必要があると認めた情報システムには、情報保証のための機能を設けること。【基本遵守事項】

## Ⅵ　その他の規定充実整備

【　背　景　】

（1）　各府省庁において、政府機関統一基準に基づき情報セキュリティポリシー及び実施手順等を改定・整備していく上で、政府機関統一基準（2005 年 9 月項目限定版）から読み取ることが基本的には可能であるが、より明示的な記述が望まれる遵守事項がある。

（2）　行政事務従事者の範囲等について再整理を行う必要がある。

（3）　情報システムの廃棄関係等の規定について再整理を行う必要がある。

【　改正の方向　】

〔考え方〕

Ⅵ-① 明示的に記述することが望ましいと思われる以下の趣旨の遵守事項を追加する。

（a）主体認証情報格納装置を利用する必要がなくなった場合には、これを返還すること。（4.1.1　主体認証）【基本遵守事項】

（b）権限管理を行う者は、退職等により行政事務従事者が情報システムを利用する必

要がなくなった場合には、当該行政事務従事者に交付した主体認証情報格納装置を返還させること。（4.1.3　権限管理）【基本遵守事項】

（c）取得した証跡の保存期間を定め、当該保存期間が満了する日まで証跡を保存し、保存期間を延長する必要性がない場合は、速やかにこれを消去すること。（4.1.4　証跡管理）（下線部を追加。）【基本遵守事項】

（d）電子計算機の故障について、故障発生日、故障した電子計算機、故障の内容、対策及び復旧作業内容並びに作業者を含む事項を記録すること。（5.2.1　電子計算機共通対策、5.2.3　サーバ装置　(2)(d)を電子計算機に関する遵守事項として明文化するもの。）【基本遵守事項】

（e）通信回線及び通信回線装置の故障について、故障発生日、故障した通信回線又は通信回線装置、故障の内容、対策及び復旧作業内容並びに作業者を含む事項を記録すること。（5.4.1　通信回線共通対策）【基本遵守事項】

Ⅵ-② 行政事務従事者の定義については、請負業者及び外部委託先等の関係の再整理を行う。

Ⅵ-③ 情報システムの廃棄関係等については、現在複数の場所に関連する規定があるが、これらの記述場所の再整理を行う。