DM6-04-051

別紙１：雛形

府省庁外の情報セキュリティ水準の低下を招く行為の防止に関する規程

雛形

2006 年 3 月

内閣官房情報セキュリティセンター

本書の位置付け

本書は、「府省庁外の情報セキュリティ水準の低下を招く行為の防止に関する規程」を策定する場合の雛形であり、「府省庁外の情報セキュリティ水準の低下を招く行為の防止に関する規程 策定手引書」の２に示す実施手順に記載すべき事項を、同３に示す文書構成例の枠組みの中に記載したものである。

本書の利用方法

本書において想定する前提

本雛形は、以下を前提として記述している。そのため、以下と異なる場合には、適宜、修正、追加又は削除する必要がある。

- 府省庁外の情報セキュリティ水準の低下を招く行為を防止するための措置を記述した規定を既存の実施手順から独立した１つの文書として作成するのではなく、当該措置を既存の実施手順等の規定として盛り込む構成である。
- 実施手順書等の規定として盛り込む方法として、情報システムに関する事項については情報システムセキュリティ責任者を担当、情報に関する事項については課室情報セキュリティ責任者を担当として、必要な規定を検討し、実施手順書等の規定として盛り込む構成である。

手直しポイント

「府省庁外の情報セキュリティ水準の低下を招く行為の防止に関する規程」を策定するに当たり、以下の点について手直しをする必要がある。

① 付録１に記載している、「府省庁外の情報セキュリティ水準の低下を招く行為を防止するための措置例」について、新たに例示すべき措置の必要性を認識した場合には、適宜追加する。
② 府省庁外の情報セキュリティ水準の低下を招く行為を防止するための措置を記述した規定を既存の実施手順から独立した１つの文書として作成する場合には、各規定の主語を明確にすることで措置を講ずべき主体を特定するとともに、取るべき措置の具体的な内容を記述する。
③ 雛形において*[・・・]*形式で示す設定値（役割等）については、各府省庁内の定めに合わせる。
④ 既存のガイドライン等との整合性を考慮し、適切に分割、統合、相互参照する。

改訂履歴

改訂日	改訂理由
2006/3/31	初版
2006/4/21	各府省庁意見に基づく修正

商標について

目次

1　本規程の目的

府省庁は、府省庁内の情報セキュリティ水準の低下を招くような行為を防止するだけでなく、府省庁外の情報セキュリティ水準の低下を招くような行為をしないことは当然である。また、府省庁外のセキュリティ水準を低下させることは、府省庁を取り巻く情報セキュリティ環境を悪化させることにもなる。

本規程は、情報セキュリティ対策の適所において講ずべき措置を定め、もって府省庁外の情報セキュリティ水準の低下を招く行為を防止することを目的とする。

2　本規程の対象者

2.1　対象者

本規程は、情報セキュリティ責任者等を対象とする。

3　府省庁外の情報セキュリティ水準の低下を招く行為の防止

3.1　措置の整備

(1) 統括情報セキュリティ責任者は、府省庁外の情報セキュリティ水準の低下を招く行為を防止するための具体的措置を例示すること。なお、例示にあたっては、インターネット、ＰＣ、ソフトウェア等の環境の変化、技術の進歩、安全に関する意識の向上等によって変わることに留意すること。

(2) 統括情報セキュリティ責任者は、府省庁外の情報セキュリティ水準の低下を招く行為を防止するための具体的措置について、新たに例示を追加した場合には、必要に応じて、追加した措置を内閣官房情報セキュリティセンターに連絡すること。

(3) *[情報セキュリティ責任者]*は、所管する単位において、府省庁外の情報セキュリティ水準の低下を招く行政事務従事者等の行為を防止するために、*[情報システムセキュリティ責任者及び課室情報セキュリティ責任者]*に対して、防止に必要な措置を検討し、実施手順書等に盛り込むように指示すること。

(4) *[情報システムセキュリティ責任者]*は、所管する情報システムにおいて、統括情報セキュリティ責任者が例示した具体的措置をもとにして、府省庁外の情報セキュリティ水準の低下を招く行政事務従者等の行為を防止するための措置を検討し、実施手順書等に盛り込むこと。

(5) *[課室情報セキュリティ責任者]*は、所管する課室において、統括情報セキュリティ責任者が例示した具体的措置をもとにして、府省庁外の情報セキュリティ水準の低下を招く行政事務従者等の行為を防止するための措置を検討し、実施手順書等に盛り込むこと。

3.2　措置の実施

(1) 行政事務従事者等は、実施手順書等に従い、府省庁外の情報セキュリティ水準の低下を招かないように行動すること。

付録： 府省庁外の情報セキュリティ水準の低下を招く行為を防止するための措置の例示

情報システムセキュリティ責任者は、所管する情報システムにとってリスクと感じる府省庁外の者による行為は、府省庁から府省庁外に対しても行わないことが望ましい。このような視点から、府省庁外の情報セキュリティ水準の低下を招く行為を防止するための措置として、以下のような注意事項が想定される。

(1) 提供する電磁的記録の内容、形式等による影響

府省庁外へ電磁的記録を提供する際に、当該電磁的記録の内容、形式等によって、府省庁外の情報セキュリティ水準の低下を招かないように、以下の点に留意すること。

- **提供する電磁的記録が不正プログラムを含まないこと。**
- **実行プログラムの形式以外に電磁的記録を提供する手段がない限り、実行プログラムの形式で電磁的記録を提供しないこと。**
- **提供する電磁的記録に改ざん等がないことを知りえる機会を、提供先の者に与えること。**
- **提供先の者が警告等に慣れて無視しないように、提供する電磁的記録の参照時に警告等が出ないようにすること。**

具体的には以下のような事項が想定される。

- 府省庁のウェブサイト、電子メールの添付ファイル、外部記録媒体等でファイルを提供する場合には、アンチウイルスソフトウェア等を利用して不正プログラムの有無を確認すること。
  - 不正プログラムに感染したファイルを府省庁外に送らないようにするため。
- 府省庁のウェブサイト、電子メールの添付ファイル、外部記録媒体等を利用して圧縮したファイルを提供する場合には、自己解凍形式を利用しないこと。
  - 自己解凍形式で圧縮されたファイルは実行可能形式のファイルとなり、当該ファイルを入手した者に不正プログラムの可能性を不必要に想起させ、解凍する際に安全性の確認が必要になるため。
- 府省庁のウェブサイトにおいて、電子署名されていない実行モジュール（Java®アプレット、ActiveX®コントロール等）を提供しないこと。
  - 実行モジュールを悪用することで、不正プログラムの感染、情報の漏えい等の被害が発生する可能性がある。そのような悪意のある実行モジュールではなく、安全な実行モジュールであることを正しい電子署名により保証するため。
- 府省庁のウェブサイトにおいて、実行モジュールを電子署名して提供する場合に、有効でない証明書を利用しないこと。

○ 安全な実行モジュールであることを保証できないだけでなく、当該モジュールを入手した者が、有効でないことを示す警告等に慣れてしまい、他の警告等に対しても危険性を感じとれなくなる可能性があるため。

(2) 提供する電磁的記録を処理することによる直接的な影響

府省庁外へ提供した電磁的記録を提供先の者が参照等する際に、利用する端末等の設定変更を要求することによって、府省庁外の情報セキュリティ水準の低下を招かないように、以下の点に留意すること。

- **府省庁外の者が利用している端末のオペレーティングシステム、ソフトウェア等のセキュリティ設定変更を不用意に指示しないこと。**
- **やむを得ずセキュリティ設定変更を指示する場合には、後に元の設定に戻す方法を、参照しやすい形式で紹介すること。**

具体的には以下のような事項が想定される。

- 府省庁のウェブサイトのコンテンツを参照するために、訪問者のブラウザのセキュリティ設定を変更するよう要求しないこと。
  - ○ ブラウザのセキュリティ設定の変更要求に従った結果、ブラウザのセキュリティレベルが低下し、悪意を持ったウェブサイト等を参照した際に不正プログラムに感染するおそれがあるため。
- 府省庁のウェブサイト、電子メールの添付ファイル、外部記録媒体等を利用して提供するファイルを参照するために、安全性の確認が困難なライセンスフリーの専用ソフトウェア等のインストールを要求しないこと。
  - ○ ソフトウェアのインストールにより、利用可能なソフトウェアの制限の変更又は違反を生じさせるため。また、当該ソフトウェアに脆弱性が発見された場合に、脆弱性を悪用した攻撃の被害にあうおそれがあるため。

(3) 提供する電磁的記録を処理することによる間接的な影響

府省庁外へ提供した電磁的記録を提供先の者が参照等する際に、明示的に利用する端末等の設定変更を要求するわけでないが、電磁的記録を参照できる設定であることを想定することは、暗黙に設定変更を指示したと考えられる。暗黙に指示した設定変更により、府省庁外の情報セキュリティ水準の低下を招かないように、以下の点に留意すること。

- **府省庁外の者にセキュリティ上の問題を生じさせるような設定変更を暗黙に指示する電磁的記録を不用意に提供しないこと。**
- **やむを得ず当該電磁的記録を提供する場合には、後に元の設定に戻す方法を、参照しやすい形式で紹介すること。**

具体的には以下のような事項が想定される。

- 府省庁のウェブサイト、電子メールの添付ファイル、外部記録媒体等を利

用して、マクロ等を含んだファイルを提供しないこと。

- マクロ等を含んだファイルを提供することは、提供先の者に対してセキュリティ設定の変更を明示的に指示することではないが、当該提供先の者がマクロを実行できるような設定にしていることを想定した行為であり、暗黙に設定変更を指示したことと考えることができる。マクロ等には、不正プログラムに感染する問題があり、暗黙に指示した設定変更により、提供先の者に当該問題が生じるおそれがあると考えられるため。

- HTML形式での電子メールを送信しないこと。
  - HTML形式の電子メールを送信することは、受信者に対してセキュリティ設定の変更を明示的に指示することではないが、当該受信者がHTMLを判読できるような設定にしていることを想定した行為であり、暗黙に設定変更を指示したことと考えることができる。HTML形式の電子メールには、フィッシング（本物に似せた偽のウェブサイトへ誘導し、入力情報を詐取する手法)、ウェブビーコン（メールを開いた事実、日時等を確認する手法)等のセキュリティ上の問題があり、暗黙に指示した設定変更により、受信者に当該問題が生じるおそれがあると考えられるため。