DM5-06-051

電子メールサービス提供ソフトウェアの
セキュリティ維持に関する規程
策定手引書

2006 年 3 月

内閣官房情報セキュリティセンター

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

1　本書の目的

本書は、サーバ装置上で動作し、電子メールサービス提供のために利用しているソフトウェアのセキュリティ維持に関して、情報システムセキュリティ管理者等が遵守すべき規定（以下「電子メールサービス提供ソフトウェアのセキュリティ維持に関する規程」という。）を情報システムセキュリティ責任者が整備するための手引書である。

府省庁においては、「政府機関の情報セキュリティ対策のための統一基準（2005 年 12 月版（全体版初版））」（NISD-K303-052、以下「政府機関統一基準」という。）に基づく省庁基準及び関係する規定を整備することが求められている。「電子メールサービス提供ソフトウェアのセキュリティ維持に関する規程」は、これらの一つとして策定し、府省庁内において電子メールサービスを提供する場合に適用するものである。

電子メールは通信回線を介して提供されるサービスの中で最も普及しているサービスの１つであり、行政事務を円滑に遂行するために不可欠なものになっている。その一方で、電子メールの送受信は情報のやりとりにほかならず、そのやりとりは様々な中継地点を経由して行われるため、その過程における情報の漏えい、改ざんのリスクがある。また、セキュリティホール対策や不正プログラム対策をおこたると、不正中継、ウイルス感染等の府省庁内だけでなく府省庁外にも迷惑をかけるおそれがある。このようなリスクを軽減するため、サーバ装置上で動作し、電子メールサービスにおいて利用されるアプリケーションソフトウェアのセキュリティを維持することが情報システムセキュリティ管理者等に求められる。

本書は、これらの背景の下で、「電子メールサービス提供ソフトウェアのセキュリティ維持に関する規程」に含めるべき事項を具体的に示し、もって統一基準及び省庁基準への準拠性、業務への適用性等において適切な規定の整備に資することを目的とする。

2　実施手順に記載すべき事項

「電子メールサービス提供ソフトウェアのセキュリティ維持に関する規程」には、以下の事項を具体化させて記載すること。

2.1　政府機関統一基準（NISD-K303-052）に定める「電子メールサービス提供ソフトウェアのセキュリティ維持に関する規程」に係る遵守事項

2.2.2　障害等の対応（２）障害等の発生時における報告と応急措置
4.1.1　主体認証機能（１）主体認証機能の導入
4.1.1　主体認証機能（３）行政事務従事者における主体認証情報の管理
4.1.3　権限管理機能（２）識別コードと主体認証情報の付与管理

4.1.4　証跡管理機能（１）証跡管理機能の導入
4.1.4　証跡管理機能（２）情報システムセキュリティ管理者による証跡の取得と保存
4.1.4　証跡管理機能（３）取得した証跡の点検、分析及び報告
4.1.4　証跡管理機能（４）証跡管理に関する利用者への周知
4.2.1　セキュリティホール対策（２）情報システムの運用時
4.2.2　不正プログラム対策（２）情報システムの運用時
4.2.3　サービス不能攻撃対策（２）情報システムの運用時
5.2.3　サーバ装置（２）サーバ装置の運用時
5.3.1　通信回線を介して提供するアプリケーション共通対策（１）アプリケーションの導入時
5.3.1　通信回線を介して提供するアプリケーション共通対策（2）アプリケーションの運用時
5.3.2　電子メール（１）電子メールの導入時

2.2　セキュリティ確保に係るその他の留意事項

2.1 に示す遵守事項のほか、セキュリティ確保に係る留意事項として、以下の項目を考慮すべきである。

- 迷惑メールの取扱い

3　文書構成例

「電子メールサービス提供ソフトウェアのセキュリティ維持に関する規程」は、情報セキュリティ対策の観点を含めた一般的な利用手順書とすべきである。そのため、行政事務従事者の行為に着目した構成が有効である。文書構成の例を以下に示す。

1 本規程の目的
2 本規程の対象者
　2.1 対象者
3 定義

《 対象：情報システムセキュリティ管理者 》
4 電子メールサービス提供ソフトェアに共通のセキュリティ維持のための対策
　4.1 主体認証
　4.2 証跡管理
　4.3 セキュリティホール対策
　4.4 サービス不能攻撃対策
5 交換用電子メールサーバにおけるセキュリティ維持のための対策
　5.1 不正中継に関する対策
　5.2 電子メールに含まれる不正プログラムに関する対策
　5.3 迷惑メールに関する対策

5.4 電子メールキューの管理
5.5 エラーメールの管理
6 送受信用電子メールサーバにおけるセキュリティ維持のための対策
6.1 不正中継に関する対策
6.2 メールボックスの管理

《 対象：権限管理を行う者 》
7 電子メールサーバのセキュリティ維持のための対策
7.1 メールアドレス発行・削除に伴う権限管理

《 対象：情報システムセキュリティ責任者 》
8 電子メールサーバのセキュリティ維持のための対策
8.1 主体認証
8.2 証跡管理
8.3 セキュリティホール対策
8.4 サービス不能攻撃対策
9 メールアドレスの発行・削除における注意事項
9.1 メールアドレス発行における注意事項
9.2 メールアドレス削除における注意事項

《 対象：情報セキュリティ責任者 》
10 電子メールサーバのセキュリティ維持のための対策
10.1 不正プログラム対策

4 策定する上での留意事項

「電子メールサービス提供ソフトウェアのセキュリティ維持に関する規程」は、以下のことに留意して策定する。

(1) 電子メールサービス提供のために利用しているソフトウェアのセキュリティ維持に関して、情報システムセキュリティ管理者、権限管理を行う者、情報システムセキュリティ責任者、情報セキュリティ責任者ごとに遵守すべき規定を整理・分類する。各者に求められる役割は以下のとおりである。

- 情報システムセキュリティ管理者は、セキュリティ維持のための運用管理の主たる実施主体である。
- 権限管理を行う者は、電子メール送受信における主体の権限管理を行う主体である。
- 情報システムセキュリティ責任者は、セキュリティホール対策計画の作成、証跡管理における証跡の保護等の実施主体である。
- 情報セキュリティ責任者は、不正プログラム対策の見直し等の実施主体である。

(2) 規定の主語は、実施主体ごとに「情報システムセキュリティ管理者は」などに統一する。

(3) 前記 2 の実施手順に記載すべき事項を「電子メールサービス提供ソフトウェアのセキュリティ維持に関する規程」に反映するに当たっては、当該事項の内容に応

じて、以下のいずれかの方針で記述する。

[具体化]・・・「電子メールサービス」に限定されず一般的・抽象的に記述されており、具体化が必要と思われる遵守事項については、これを「電子メールサービス」に適用し、表現をより具体的に修正・追加する。

[転記]・・・・記述内容が具体性を持ち、変更が不要と思われる遵守事項については、これを転記する。

[詳細化]・・・記述内容が具体性を持っているが、行政事務従事者の利便性を考慮して、より詳細な解説を付すべきと思われる遵守事項については、解説書等を参考に、これを詳細化する。

[背景]・・・・主にセキュリティ機能の実装に関する内容であり、これを背景として行政事務従事者による注意義務が発生すると思われる遵守事項については、これを行政事務従事者の立場から解釈し直す。

[別立場]・・・行政事務従事者の立場ではなく、責任者側又は管理者側の立場から記述されている遵守事項については、これを行政事務従事者の立場から解釈し直す。

[参考引用]・・直接「電子メールサービス」に関連した内容ではないが、行政事務従事者の理解促進に寄与すると思われる遵守事項については、これを参考引用する。

[一般]・・・・直接「電子メールサービス」に関連した内容ではないが、一般論として手順書に記載しておくことが望ましいと思われる遵守事項については、これを周辺知識として盛り込む。

5　参考資料

「電子メールサービス提供ソフトウェアのセキュリティ維持に関する規程」の策定に際しては、以下のような資料が参考となる。

5.1　政府及び政府関係機関の資料

(1) 総務省の「迷惑メール対策」
URL: http://www.soumu.go.jp/joho_tsusin/d_syohi/m_mail.html

(2) 独立行政法人 情報処理推進機構(IPA)の「UBE（迷惑メール）中継対策」
URL: http://www.ipa.go.jp/security/ciadr/antirelay.html

(3) 独立行政法人 情報処理推進機構(IPA)の「電子メールのセキュリティ」の「電子商取引における電子メールに関するセキュリティ上の課題」
URL: http://www.ipa.go.jp/security/fy10/contents/over-all/email.html

5.2　政府・政府関係機関以外の資料

なし

6　雛形の利用方法

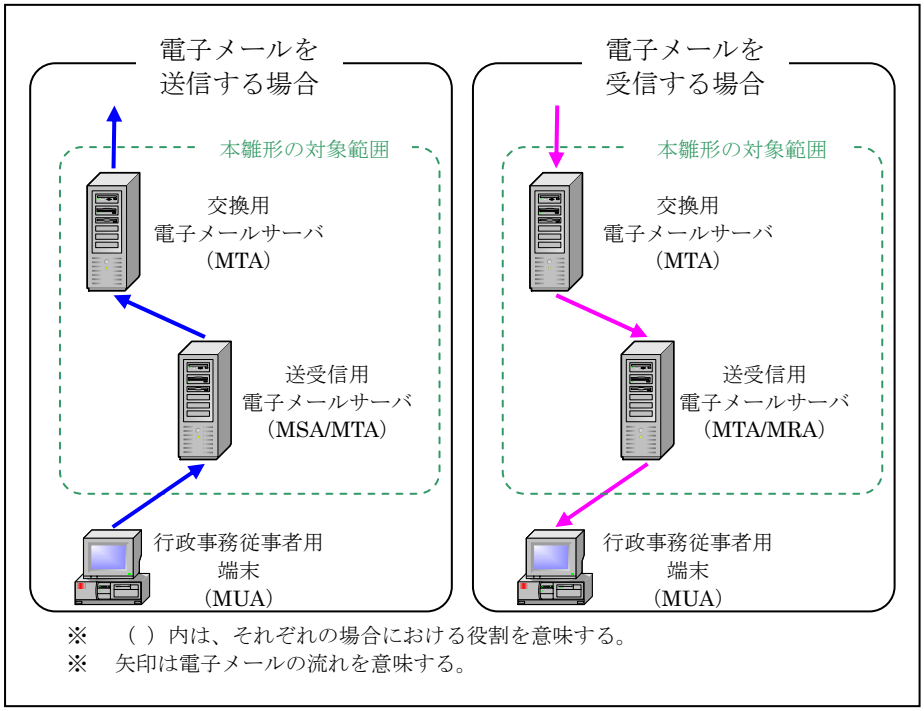
別紙１の雛形を参考にして、「電子メールサービス提供ソフトウェアのセキュリティ維持に関する規程」を策定すると効率的である。別紙１の雛形は、前記２の実施手順に記載すべき事項を、前記３の文書構成例の枠組みの中に記載したものである。

6.1　雛形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。

- 電子メールの送受信にかかわる電子メールサーバ及び端末の構成、電子メールの送受信の経路は、以下の図のとおりである。

図：サーバ及び端末の構成、電子メール送受信経路のイメージ



- 交換用電子メールサーバにおいて、送受信する電子メールに対する不正プログラムのチェックが実施されている。
- MRAから電子メールを受信する際に行う主体認証は、知識による認証方式が利用されている。（MSAに電子メールを送信する際に主体認証を利用す

る場合も同様。)。

- 行政事務従事者が、MRAから電子メールを受信する際の主体認証に利用するパスワードを、容易に変更できる機能が用意されている。(MSAに電子メールを送信する際に主体認証を利用する場合も同様。)
- MTA、MSA及びMRAにおいて、電子メール送受信、主体認証等の証跡が取得されている。

6.2 手直しポイント

「電子メールサービス提供ソフトウェアのセキュリティ維持に関する規程」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) 「通信回線を介して提供するサービス」に応じて内容を変更する必要がある。雛形は電子メールサービスを対象に記載されているが、例えば、ウェブサービスの場合には、HTTP 基本認証による主体認証、コンテンツのアクセス制御、SSL/TLS を利用した暗号化通信等に関する運用管理の実施手順について記述することとなる。

(2) メールアドレスを発行・削除を伴う人事異動等に関する情報の連絡経路について、「人事異動等における情報セキュリティ対策実施規程」に合わせる。

(3) 雛形において、*[・・・]* 形式で示す設定値（期間等）については、各府省庁内の定めに合わせる。

(4) 雛形において、【・・・の場合】形式で示す記述については、想定される複数の案を記したものであり、各府省庁の判断により適宜、選択又は修正する。

(5) 雛形と既存の実施手順書との整合性を考慮し、適切に分割、統合、相互参照する。特に、本雛形は電子メールに関連するアプリケーションソフトウェアのセキュリティ維持に関する規定を記載しているため、サーバ装置の運用管理手順書との、統合、相互参照をすると良い。

(6) 情報システムセキュリティ管理者、情報システムセキュリティ責任者等の役割ごとに規定を記述しているため、既存の規定の構成に合わせて分割、統合すると良い。