DM5-06-051

別紙１：雛形

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
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、「電子メールサービス提供ソフトェアのセキュリティ維持に関する規程」を策定する場合の雛形であり、「電子メールサービス提供ソフトェアのセキュリティ維持に関する規程 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。

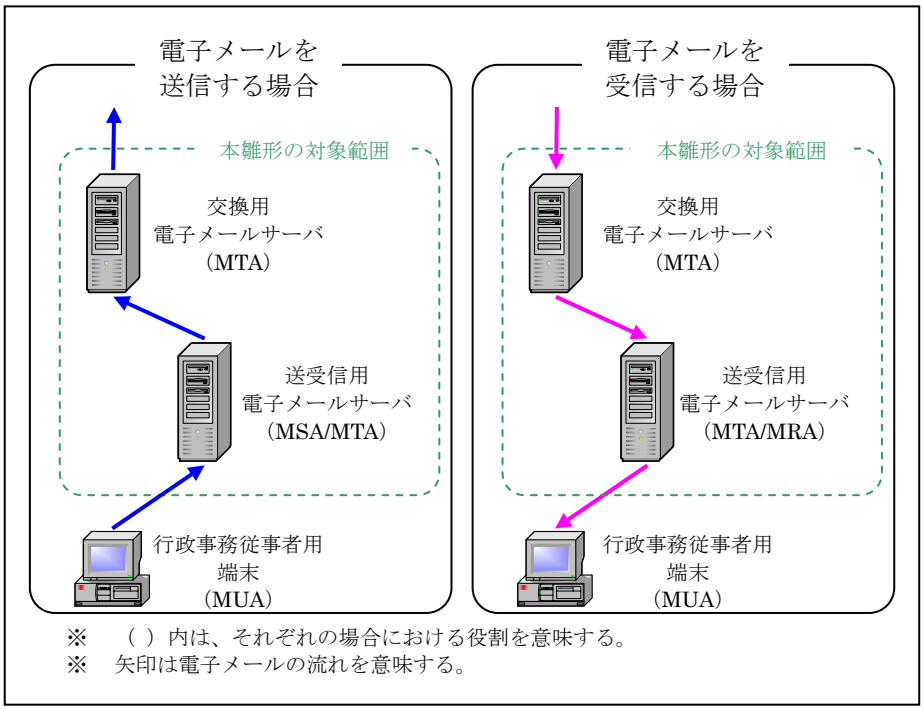
本書の利用方法

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。

- 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



※　（ ）内は、それぞれの場合における役割を意味する。
※　矢印は電子メールの流れを意味する。

- 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、証跡が取得されている。

手直しポイント

「電子メールサービス提供ソフト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。

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

目次

1　本規程の目的

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。

本規程は、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維持に関する規定を提供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、電子メールサービス提供ソフトェアのセキュリティ維持のため、日常的及び定期的に運用管理を実施することが求められているすべての情報システムの情報システムセキュリティ管理者等を対象とする。

3　定義

本規程における用語の定義は次のとおりである。

(1) 「電子メールサービス提供ソフトェア」とは、電子メールの送受信のためにサーバ装置上で動作する MTA、MSA、MRA であって、情報システムセキュリティ管理者によって運用管理が行われているものをいう。

(2) 「MTA」とは、Mail Transfer Agent の略称であり、他のサーバから SMTP で受信した電子メール、又は MSA から渡された電子メールを、必要に応じて、SMTP で他のサーバへ転送したり、ローカルのメールボックスに格納するソフトウェアへ渡したりする処理を行うソフトウェアをいう。いわゆる SMTP サーバ等。

(3) 「MSA」とは、Mail Submission Agent の略称であり、MUA から SMTP で電子メールを受信し、当該電子メールを MTA に渡す処理を行うソフトウェアをいう。MTA の機能に含むとする考え方もある。

(4) 「MRA」とは、Mail Retrieval Agent の略称であり、メールボックスに格納された電子メールを、POP3、IMAP 等で MUA へ渡すソフトウェアをいう。いわゆる POP 3 サーバ、IMAP サーバ等。

(5) 「MUA」とは、Mail User Agent の略称であり、電子メールの読み書き、MSA 経由での電子メールの送信、MRA 経由での電子メールの受信、送受信した電子メールの管理を行うソフトウェアをいう。いわゆるメーラ等。

(6) 「エラーメール」とは、あて先のメールアドレスが存在しない場合等に、送信元のメールアドレス又は MTA の管理者用メールアドレスあてに送信不能を伝えるために、MTA によって自動的に送られる電子メールをいう。

(7) 「メールボックス」とは、あるメールアドレスあてに届いた電子メールを保管しておく電子メールサーバ上の領域をいう。メールボックスは、メールアドレスごとに存在し、メールアドレスあてに届いた電子メールは、当該メールアドレス専用のメールボックスに保管される。

(8) 「交換用電子メールサーバ」とは、他のドメインと電子メールを交換（送受信）するための電子メールサーバであり、DNS 情報において交換用であることが明示されている電子メールサーバであり、MTA が動作しているものをいう。いわゆる MX サーバ。

(9) 「送受信用電子メールサーバ」とは、電子メールを利用している行政事務従事者のメールボックスが存在し、当該行政事務従事者が MUA を利用して電子メールを送受信するために接続するための電子メールサーバであり、MTA、MSA、MRA が動作しているものをいう。

《 対象：情報システムセキュリティ管理者　該当項目：４、５、６》

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

(1) 情報システムセキュリティ管理者は、電子メールを利用している行政事務従事者からパスワードが他者に使用され又はその危険が発生したことの報告を受けた場合には、以下の措置を講ずること。

- 当該行政事務従事者の識別コードを一時的に無効にする。
- 新たなパスワードを設定し、他者に知られないように当該行政事務従事者に連絡した上で、当該識別コードの一時無効を解除する。
- 証跡の分析により他者に使用された可能性を確認する。
- 情報セキュリティ責任者に状況を報告する。

【電子メールサービスにおいてパスワードの通信時に暗号化を行っていない場合】

(2) 情報システムセキュリティ管理者は、電子メールサービスを利用する行政事務従事者に対して、以下の事項を通知すること。

- 電子メールサービスにおいて利用するパスワードは通信回線上を暗号化されずに送受信されるため、盗聴等により容易に漏えいする危険性があること。
- 他の情報システムで利用している重要なパスワードを電子メールサービスにおける主体認証に利用しないこと。

【電子メールサービスにおいてパスワードの保存時に暗号化を行っていない場合（多くの電子メールサービスにおいて該当しない。）】

(3) 情報システムセキュリティ管理者は、電子メールサービスを利用する行政事務従事者に対して、以下の事項を通知すること。

- 電子メールサービスにおいて利用するパスワードは暗号化されずにサーバ装置上に保存されるため、不正侵入等により漏えいする危険性があること。
- 他の情報システムで利用している重要なパスワードを電子メールサービスにおける主体認証に利用しないこと。

4.2　証跡管理

(1) 情報システムセキュリティ管理者は、電子メールサービス提供ソフトェアにより取得される以下の証跡を記録すること。

- 電子メールの送受信に関する、送受信日時、メールアドレス、送受信の成否等の証跡（MTA、MSAにより記録）

【電子メールの送信時に認証を行う場合（強化遵守事項）】

- MUAから電子メールを送信する際の主体認証の成功・失敗の証跡（MSAにより記録）

- メールボックスから電子メールを取得する際の主体認証の成功・失敗の証跡（MRAにより記録）
- メールボックスから電子メールを取得する際の取得日時、取得電子メール数、識別コード等の証跡（MRAにより記録）

(2) 情報システムセキュリティ管理者は、証跡が取得できなくなる事態を避けるため、電子メールサービス提供ソフトェアの証跡を記録しているファイルを*[1ヶ月に1度]*変更すること。また、証跡を改ざんから保護するとともに、証跡を記録したファイルにより記録装置の容量が圧迫されることを防止するため、当該ファイルを適宜外部記録媒体へ移動することが望ましい。

(3) 情報システムセキュリティ管理者は、電子メールサービス提供ソフトェアにより記録された証跡を*[○年間]*保存すること。また、保存期間を延長する必要性がない場合には、速やかにこれを消去すること。

4.3 セキュリティホール対策

(1) 情報システムセキュリティ管理者は、電子メールサービス提供ソフトェアについて変更があった場合には、セキュリティホール対策に必要となる機器情報の文書に反映すること。
文書に記録すべき情報としては、以下の項目が想定される。

- 電子メールサービス提供ソフトェアの一覧（名称、種別、バージョン）

(2) 情報システムセキュリティ管理者は、電子メールサービス提供ソフトェアに関して、以下の方法で、セキュリティホールが発見されていないかどうかを*[毎日]*確認すること。

【公表されているウェブサイト等を利用する場合】

- 電子メールサービス提供ソフトェアの製造・開発・販売元、JVN(JP Vendor Status Notes)、JPCERTコーディネーションセンター等のセキュリティ関連機関等がウェブサイト、電子メール等で公表するセキュリティホール情報を収集し確認する。

【セキュリティホール情報提供サービスを利用する場合】

- セキュリティホール情報提供サービスにより提供される情報を確認する。

(3) 情報システムセキュリティ管理者は、電子メールサービス提供ソフトェアにセキュリティホールが発見されている場合には、当該セキュリティホールに関連する情報（原因、影響範囲、対策方法、攻撃ツールの有無等を含む。）を入手し、情報システムセキュリティ責任者に報告すること。

(4) 情報システムセキュリティ管理者は、情報システムセキュリティ責任者が作成したセキュリティホール対策計画に基づき、セキュリティホール対策を講ずること。

(5) 情報システムセキュリティ管理者は、セキュリティホール対策を実施する場合には、以下の事項に注意すること。

- 対策の実施記録を情報システムセキュリティ責任者に報告すること。
- 対策用ファイル（パッチ、アップデートファイル、最新バージョンのファイル等）に不正プログラムが含まれている可能性があるため、ソフトウェアの製造・開発・販売元からのダウンロード等の信頼できる方法で入手すること。
- 対策用ファイルの完全性を検証する方法が用意されている場合には、その検証を実施すること。

(6) 情報システムセキュリティ管理者は、*[1年に1度]*電子メールサービス提供ソフトェアに関して、以下の事項を確認、分析し、不適切な状態である場合には、是正措置を行うこと。是正措置は、セキュリティホール対策の注意事項に準じて行うこと。

- セキュリティホール対策の状況
- 電子メールの中継に関わる設定の適切性（MTA及びMSAの場合。詳細は「5.1 不正中継に関する対策」及び「6.1 メールボックスの管理」を参照すること。）
- VRFY、EXPN、ETRN、その他悪用されるおそれのあるSMTPコマンドの無効化（MTA又はMSAの場合）
- 主体認証方式及びパスワードの安全性（MRAの場合）

【迷惑メール対策を実施している場合】

- 迷惑メールの排除に関わる設定の適切性（MTAの場合。詳細は「5.3 迷惑メールに関する対策」を参照すること。）

【電子メールの送信時に認証を行う場合（強化遵守事項）】

- 主体認証方法及びパスワードの安全性（MSAの場合）

【サービス不能攻撃対策として電子メールサービスを監視する場合（強化遵守事項）】

4.4 サービス不能攻撃対策

(1) 電子メールサービスは、大量の電子メール（エラーメールを含む。）を受信する攻撃により、通常の利用者が電子メールサービスを利用できなくなる可能性がある。情報システムセキュリティ管理者は、電子メールの配送状況、送受信数等を監視・記録し、平常時の状況を把握すること。

(2) 情報システムセキュリティ管理者は、監視・記録された平常時と異なり、サービスの提供に問題が生じる状況を検出した場合には、情報システムセキュリティ責任者に報告すること。

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

(1) 情報システムセキュリティ管理者は、電子メールの中継制御に関して、以下のような設定を、*[1年に1度]*確認すること。

- MTAにおいて、自ドメインあての電子メールのみを送受信用電子メールサーバに中継し、それ以外の電子メールを受信拒否とする設定

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

(1) 情報システムセキュリティ管理者は、不正プログラムに関する情報の収集に努めること。

(2) 情報システムセキュリティ管理者は、収集した情報について、以下のように特段の対処が必要な場合には、行政事務従事者に注意喚起又は対応方法を周知徹底すること。

- 急激に感染を拡大する不正プログラムが報告されている場合
- 交換用電子メールサーバ上で動作しているアンチウイルスソフトウェアで未対応の不正プログラムが報告されている場合

(3) 情報システムセキュリティ管理者は、交換用電子メールサーバ上で動作しているアンチウイルスソフトウェア、不正プログラム定義ファイル等を常に最新の状態に維持すること。

(4) 情報システムセキュリティ管理者は、交換用電子メールサーバ上で MTA 及び MSA により取り扱われる電子メールに関して、電子メールの本文、添付ファイル等に対して不正プログラムのチェックを自動的に行う機能を有効にすること。

(5) 情報システムセキュリティ管理者は、府省庁内の端末から不正プログラムが含まれる電子メールが送信されていることを検知した場合には、当該電子メールを送信している端末を通信回線から隔離する等して不正プログラムが含まれる電子メールの送信を抑制し、情報セキュリティ責任者に感染の事実を報告すること。

(6) 情報システムセキュリティ管理者は、府省庁外から不正プログラムが含まれる電子メールが送信されていることを検知した場合には、送信元の MTA の管理者等にその旨を連絡し、対処を促すことが望ましい。

【迷惑メール対策を実施している場合】

5.3　迷惑メールに関する対策

(1) 情報システムセキュリティ管理者は、行政事務従事者あての迷惑メールの排除基準及び取扱方法（受信拒否（恒久的エラー／一時的エラー）、受信後削除、受信等）に関する MTA の設定を適宜見直し、必要に応じて修正すること。

(2) 情報システムセキュリティ管理者は、MTA において設定されている排除基準及び取扱方法の修正により、迷惑メールに該当しない業務上必要な電子メールまでもが排除されることのないように配慮すること。

【記録装置の状態を監視し、容量の圧迫を検知する場合（強化遵守事項）】

5.4　電子メールキューの管理

(1) 情報システムセキュリティ管理者は、電子メールキュー（配送不能等の理由で再配送待ち状態の電子メールが保存される領域。）に、大量の再配送待ち電子メールが滞留し、記録装置の容量を圧迫していないかどうかを適宜確認すること。

(2) 情報システムセキュリティ管理者は、電子メールキューに大量の再配送待ち電子メールが滞留している場合で、当該電子メールが迷惑メールのときは、エラーメールにより府省庁外の電子メールサーバに負荷をかけるおそれがあるため、当該電子メールを配送不能とせずに破棄すること。ただし、当該電子メールが迷惑メールでないときは、配送不能として送信元のメールアドレスにエラーメールを返すことが望ましい。

5.5　エラーメールの管理

(1) 情報システムセキュリティ管理者は、MTA・MSA の管理者用メールアドレス（postmaster 等）あてに届いているエラーメールを適宜確認し、電子メールの配送不能等の問題がないことを確認すること。

(2) 府省庁から送信したように送信元メールアドレスを詐称した迷惑メールが第三者によって送信された場合、配送不能で大量のエラーメールが管理者用メールアドレス又は行政事務従事者のメールアドレスあてに届く場合がある。情報システムセキュリティ管理者は、多量のエラーメールが届いている場合には、エラーメールの内容を確認し、送信元メールアドレスを詐称した迷惑メールと判断できるときには、情報セキュリティ責任者に詐称の事実を報告すること。

(3) 情報システムセキュリティ管理者は、多量のエラーメールを受信することによって MTA が動作するサーバ装置のリソース（CPU、メモリ、HDD 等を含む。）が消費され、通常の電子メールの送受信に影響を及ぼすおそれがある場合には、受信拒否等の方法により影響を抑えること。

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

(1) 情報システムセキュリティ管理者は、電子メールの中継制御に関して、以下のような設定を、*［1 年に 1 度］*確認すること。

- MTAにおいて、自ドメインあての電子メールのみを受信した上で該当する電子メールアドレスのメールボックスに保存し、それ以外の電子メールを受信拒否とする設定

【電子メールの送信時に認証を行わない場合】

- MSAにおいて、庁内LANの端末からの接続により送信された電子メールのみを転送し、それ以外の電子メールを受信拒否とする設定

【電子メールの送信時に認証を行う場合（強化遵守事項）】

- MSAにおいて、電子メール送信時に認証が行われた端末からの接続により

送信された電子メールのみを転送し、それ以外の電子メールを受信拒否とする設定

6.2 メールボックスの管理

(1) 情報システムセキュリティ管理者は、メールボックスにより利用されている記録装置の容量を*[1ヶ月に1度]*確認すること。

(2) 情報システムセキュリティ管理者は、メールボックスの容量がサーバ装置の運用に問題が生ずるほど大きい場合には、メールボックスの整理を行い、サーバ装置の正常な運用を確保すること。

《 対象：権限管理を行う者　該当項目：７》

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

(1) 権限管理を行う者は、情報システムセキュリティ責任者からメールアドレスの発行を指示された場合には、以下の事項に注意してメールアドレスを発行すること。なお、当該指示のないメールアドレスを発行しないこと。

- MRAが動作するサーバ装置上に、当該メールアドレスに対応するメールボックス、及び当該メールボックスから電子メールを取得するための識別コードを作成し、当該識別コードに初期パスワードを設定すること。
  また、設定する初期パスワードについて、以下の事項を考慮すること。
  - ８文字以上とすること。
  - ２つ以上のアルファベットと１つ以上の非アルファベットを含むこと。
  - ４つの異なる文字を含むこと。
  - 辞書にある言葉や一般的な言葉を単独で使用しないこと。

【電子メールの送信時に主体認証を行う場合（強化遵守事項）】

- MSAが動作するサーバ装置上に、当該メールアドレスに対応する電子メールを送信するための識別コードを作成し、当該識別コードに初期パスワードを設定すること。
  初期パスワードについては、MRAにおける考慮事項に準じて設定すること。

- 当該識別コード及び初期設定のパスワードを、行政事務従事者に連絡する際には、封書で直接手渡しする等、他の者に知られない安全な方法を用いること。

(2) 権限管理を行う者は、メールアドレスを発行する際に、以下の事項を発行する行政事務従事者に通知すること。

- 共有識別コード、共有ではない識別コードの別。

【情報システムセキュリティ責任者が、初回ログイン時に初期パスワードを変更させると判断した場合】

- 初期設定のパスワードを速やかに変更すること。

(3) 権限管理を行う者は、情報システムセキュリティ責任者からメールアドレスの削除を指示された場合には、以下の事項に注意してメールアドレスを削除すること。

- MRAが動作するサーバ装置上に作成した、当該メールアドレスに対応する受信用識別コード及びメールボックスを削除すること。

【電子メールの送信時に主体認証を行う場合（強化遵守事項）】

- MSAが動作するサーバ装置上に作成した、当該メールアドレスに対応する送信用識別コードを削除すること。

- 当該メールアドレスに関する転送等の設定を無効にすること。
- 不要な識別コードの有無を確認し、不要な識別コードが発見された場合には、当該識別コードを無効にすること。

(4) 権限管理を行う者は、電子メールの受信時に行う主体に対して、識別コードに対応した電子メールアドレスのメールボックスに限りアクセスできるようにすること。

【識別コードの発行記録を取得する場合（強化遵守事項）】

(5) 権限管理を行う者は、メールアドレスの発行に伴い行政事務従事者に識別コードを付与した場合には、当該行政事務従事者及び当該メールアドレスを記録すること。当該記録を消去する場合には、情報セキュリティ責任者から事前の承認を得ること。

【識別コードの再利用を禁止する場合（強化遵守事項）】

(6) 権限管理を行う者は、メールアドレスの発行に伴って行政事務従事者に付与した識別コードについて、当該識別コードを削除した場合であっても、別の行政事務従事者に対して同一の識別コードを発行しないこと。

《 対象：情報システムセキュリティ責任者　該当項目：８、９》

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

(1) 情報システムセキュリティ責任者は、当該電子メールサーバにおける主体認証において共有識別コードの利用許可について、その必要性を判断すること。

(2) 情報システムセキュリティ責任者は、共有識別コードの必要性に関する判断の結果を、情報システムセキュリティ管理者に周知徹底すること。

8.2　証跡管理

(1) 情報システムセキュリティ責任者は、証跡を改ざん、漏えい、消去等から保護するため、以下の措置を講ずること。

- 証跡が保存されたファイルは電子メールサーバを管理する者しか参照できないように、アクセス制御する。
- 証跡が保存された外部記録媒体を施錠可能な棚等に保管し、当該棚等の鍵は情報システムセキュリティ責任者が管理する。

【取得した証跡の点検、分析及び報告を行う場合（強化遵守事項）】

(2) 情報システムセキュリティ責任者は、取得した証跡を*[３ヶ月に１度]*点検及び分析し、その結果に応じて必要なセキュリティ対策を講じ、又は情報セキュリティ責任者に報告すること。

(3) 情報システムセキュリティ責任者は、証跡を点検及び分析する場合には、以下の事項を重点的に点検し、また通常と異なる状況が見られた場合には、より詳細に点検及び分析を行うこと。

- 不正中継による電子メール受信の拒否（MTA、MSAの証跡）
- パスワードクラックによる多数の主体認証の失敗（MRAの証跡）

【電子メールの送信時に主体認証を行う場合（強化遵守事項）】

- パスワードクラックによる多数の主体認証の失敗（MSAの証跡）

8.3　セキュリティホール対策

(4) 情報システムセキュリティ責任者は、情報システムセキュリティ管理者が入手したセキュリティホールに関連する情報から、当該セキュリティホールが情報システムにもたらすリスクを分析した上で、以下の事項について判断し、セキュリティホール対策計画を作成すること。

- 対策の必要性
- 対策方法

- 対策方法が存在しない場合の一時的な回避方法
- 対策方法又は回避方法が情報システムに与える影響
- 対策の実施予定
- 対策テストの必要性
- 対策テストの方法
- 対策テストの実施予定

(5) 情報システムセキュリティ責任者は、作成したセキュリティホール対策計画に基づいて、情報システムセキュリティ管理者にセキュリティホール対策の実施を指示すること。

(6) 情報システムセキュリティ責任者は、入手したセキュリティホールに関連する情報に関して、必要に応じて、電子メールサービス提供ソフトェアを運用管理している他の情報システムセキュリティ責任者と共有すること。

8.4 サービス不能攻撃対策

(1) 情報システムセキュリティ責任者は、情報システムセキュリティ管理者からサービス不能攻撃を検出した旨の報告を受けた場合には、定められた手順に従って対処すること。

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

(1) 情報システムセキュリティ責任者は、*[庶務担当者]*から行政事務従事者の転入の連絡があり、当該行政事務従事者にメールアドレスを発行する必要がある場合には、権限管理を行う者にメールアドレス発行に伴う権限管理の指示を出すこと。

(2) 情報システムセキュリティ責任者は、電子メールの送受信に関する証跡の取得、保存、点検及び解析を行う可能性があることを、メールアドレスを発行する行政事務従事者にあらかじめ説明すること。

9.2 メールアドレス削除における注意事項

(1) 情報システムセキュリティ責任者は、*[庶務担当者]*から行政事務従事者の転出の連絡があり、当該行政事務従事者にメールアドレスを発行していた場合には、権限管理を行う者にメールアドレス削除に伴う権限管理の指示を出すこと。

《 対象：情報セキュリティ責任者　該当項目：１０》

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

(1) 情報セキュリティ責任者は、電子メールサービスにおける不正プログラム対策の状況を適宜把握し、その見直しを行うこと。

【外部の専門家の支援を受ける場合（強化遵守事項）】

(2) 情報セキュリティ責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておくこと。