電子メールクライアントのプロテクションプロファイル

本書は、米国政府 DoD 傘下の NSA 情報保証局で作成したプロテクションプロファイルの一部を調達要件の検討のため、参考として日本語に直訳したものです。IT セキュリティ評価及び認証制度における適合 PP として利用する場合は、正式な文書である英語版のみとなります。

正式な文書は、以下の URL よりダウンロード可能です。

https://www.niap-ccevs.org/pp/pp_emailclient_v1.0.pdf

2014 年 4 月 1 日

バージョン 1.0

平成 26 年 11 月 25 日　翻訳 暫定第 0.1 版
独立行政法人情報処理推進機構
技術本部 セキュリティセンター
情報セキュリティ認証室

改版履歴

バージョン	日付	内容
1.0	2014 年 4 月 1 日	電子メールクライアント PP

1 概論

本文書では、評価対象 (TOE) である電子メールクライアントのセキュリティ機能要件 (SFR) のベースラインセットを提供する。

電子メールクライアントは、電子メールサーバにより提供される電子メールの送信、受信、及び管理を行うために用いられるアプリケーションである。電子メールの内容と電子メールクライアントの複雑性は、時とともに増大してきた。モダンな電子メールクライアントはプレーンテキストだけではなく HTML も表示でき、Adobe PDF や Microsoft Word 文書などのよく使われる添付フォーマットを表示する機能を有することもある。電子メールクライアントによっては、拡張機能またはプラグインの追加により、利用者による機能の変更が可能なものもある。プロトコルもまた、電子メールクライアントとサーバとの間の通信に定義されている。クライアントによっては、同一のタスクを行うための複数のプロトコルをサポートしているものもあり、電子メールサーバの仕様に従って構成することができる。

モダンな電子メールクライアントは、その複雑さと豊富な機能により、攻撃者のターゲットとなって、セキュリティの問題を招く。本文書は、オペレーティングシステムのセキュリティサービス、暗号標準、及び環境緩和効果の利用を要求することにより、電子メールクライアントのセキュリティの向上を促進させることを意図したものである。また、本文書中の要件は、オペレーティングシステムにより提供されるセキュリティ機能にかかわらず、電子メールクライアントの受容可能なふるまいを定義している。

これらの要件は、基盤となるプラットフォームの構成にかかわらず、任意のオペレーティングシステム上で動作するすべての電子メールクライアントに適用される。本文書の目的において*アプリケーション*は、オペレーティングシステム上で動作するソフトウェアであって、そのプラットフォームの利用者または所有者の代理としてタスクを実行するもの、と定義される。*電子メールクライアント*は、電子メールサーバにより提供される電子メールの取り込みと管理を行うアプリケーションである。*拡張機能とプラグイン*は、電子メールクライアントによりロードされることが可能なコードパッケージであって、そのクライアントに新たなまたは特化した機能を導入するものである。

1.1 TOE の概要

本文書の評価対象 (TOE) は、デスクトップまたはモバイルオペレーティングシステム上で動作する電子メールクライアントアプリケーションである。

1.2 TOE の利用方法

電子メールクライアントは、メールユーザエージェント (MUA) から電子メールを取り込んだり、メール転送エージェント (MTA) を介してメールを送信したりするために用いられる。MUA と MTA の機能は、同一の製品中で利用可能な場合もあり、またメールサーバという用語は MUA と MTA のいずれにも適用され得る。電子メールクライアントを介したアクセスは、インターネット上で、あるいは閉じたネットワーク (イントラネット) 内で行うことができる。一部の電子メールクライアントにはカレンダー、連絡先などを管理する能力が

統合されているが、そのような機能は本プロテクションプロファイルの適用範囲外である。

[使用事例] 電子メールの送信、受信、アクセス、管理、及び表示

電子メールクライアントは、メールサーバと連携して電子メールの送信、受信、閲覧、アクセス、管理を行うために用いられる。電子メールクライアントはプレーンテキストだけではなく HTML も表示でき、またよく使われる添付フォーマットを表示することもできる。

2 セキュリティ課題記述

以下に、適合 TOE が対処する課題を記述する。

2.1 脅威

2.1.1 悪意や欠陥のあるアップデート

最もよく利用される攻撃ベクトルは、既知の欠陥を含むソフトウェアでパッチを当てていないバージョンへの攻撃を利用するものであるため、電子メールクライアントをアップデートして脅威環境の変化へ確実に対処することが必要となる。パッチを適宜適用することによりクライアントが「攻略しにくい目標 (ハードターゲット)」であることが確実となり、その製品がセキュリティ方針を維持管理し強制できる可能性が増大する。しかし、製品へ適用されるべきアップデートは何らかの形で信頼できなければならない (must)。そうでなければ、攻撃者がルートキットやボット、あるいはその他のマルウェアなど、自分たちの選択した悪意のあるコードを含んだ独自の「アップデート」を作成することができてしまう。このような「アップデート」が一度インストールされると、その後そのシステムとそのデータすべての制御権は攻撃者に握られてしまう。

[T.UNAUTHORIZED_UPDATE]

2.1.2 悪意や欠陥のあるプラグインまたは拡張機能

電子メールクライアントの機能は、サードパーティ製のユーティリティやツールの統合により拡張可能である。このような能力の拡張されたセットは、プラグイン及び拡張機能の利用により可能となる。基本的な電子メールクライアントのコードとプラグインや拡張機能の提供する新しい能力とが緊密に統合されているため、攻撃者により悪意を持って、または開発者により意図されずに、深刻な欠陥を悪人が電子メールクライアントへ注入できるリスクが増大する。これらの欠陥により、望ましくないふるまいが起こり得る。これには、電子メールクライアント中の秘密の情報への不正アクセスや、そのデバイスのファイルシステムへの不正アクセスを可能とすること、あるいは他のアプリケーションまたはオペレーティングシステムへの不正アクセスを可能とする特権昇格さえもが含まれるが、これらに限定されるものではない。

[T.UNAUTHORIZED_ADDON]

2.1.3 ネットワークの盗聴

ネットワークの盗聴には、何らかの潜在的に秘密のデータの意図された送信先とシステムとの間の送信を監視するため、攻撃者がネットワーク上の位置を手に入れることが必要となる。電子メールクライアントに関しては、電子メールクライアントと MUA 及び MTA との間のトランザクションの監視が必要とされる。

[T.NETWORK_EAVESDROP]

2.1.4 ネットワーク攻撃

ネットワーク攻撃は、攻撃者がネットワーク上の位置を手に入れることが必要であるという点で、ネットワークの盗聴と同様である。ネットワークの盗聴と異なる点は、攻撃者がシステムとの通信にかかわること、あるいはシステムと何らかのデータの正当な送信先との間のデータを改変することが必要となることである。電子メールクライアントに関しては、そのふるまいに影響を与え得る脆弱性を悪用するために、あるいは MUA または MTA へ送信されるアカウント情報を改変するために、悪意のあるデータを電子メールクライアントへ送信することがネットワーク攻撃に必要となるかもしれない。電子メールクライアント攻撃は、一般的にはインターネットに接続された電子メールクライアントで行われる

が、閉じたネットワーク内で行われることもないとは言えない。電子メールクライアントソフトウェアまたは電子メールクライアント拡張機能に含まれる脆弱性を悪用し得る攻撃の 1 つのクラスには、フィッシング (phishing) などのソーシャルエンジニアリング的なテクニックを用いたエクスプロイト (exploit) の配付が含まれる。この種の攻撃では、利用者が悪意のある添付ファイルを開くか悪意のあるウェブサイトへのリンクをクリックすることにより、多くの場合には利用者へ何の表示もされずに、電子メールクライアントを危殆化させるエクスプロイトが実行される。

[T.NETWORK_ATTACK]

2.2 前提条件

TOE が動作するために期待される基盤となるプラットフォーム及び環境の機能的及びセキュリティ的な能力に関する基本的な前提条件は、附属書 A に定義されている。

3 セキュリティ対策方針

適合 TOE は、以下に列挙されるセキュリティ対策方針に対応し、また TOE への新たな脅威に対応する方針を実装するセキュリティ機能を提供することになる。以下のセクションでは、上に列挙した脅威に対抗するため、本機能の記述を提供する。

3.1 TOE のセキュリティ対策方針

3.1.1 保護された通信

脅威のセクションに記述されたネットワーク攻撃及びネットワークの盗聴の脅威に対処するため、TOE は電子メールクライアントと与えられた電子メールサーバとの間の保護された通信を、要望に応じて提供しなければならない (must)。運用環境におけるこれら 2 つのエンティティ間のデータは、以下の標準プロトコルを 1 つ以上用いて実装される高信頼パス経由して保護される：Transport Layer Security (TLS)、Secure Multipurpose Internet Mail Extensions (S/MIME)、及び Simple Authentication and Security Layer (SASL)。

[O.COMMS]

3.1.2 TOE の構成

電子メールクライアントにより (一時的または永続的に) 保存され、あるいは処理される秘密のデータを保護するため、適合 TOE は管理者により定義されたセキュリティポリシーを定義、設定、及び適用する能力を提供する。エンタープライズのポリシーが管理者により TOE に対して設定される場合、これらはいかなる利用者定義の設定よりも優先されなければならない (must)。

[O.CONFIG]

3.1.3 TOE の完全性

電子メールクライアントの完全性が保たれていることを保証するため、適合 TOE はソフトウェア及びデータの完全性が保たれていることに保険を掛ける（訳注：保証する）ため、セルフテストを実行する。

悪意または欠陥のある電子メールクライアントのソフトウェア、プラグインまたは拡張機能に関連した課題に対処するため、適合 TOE は電子メールクライアントのソフトウェア、プラグイン及び拡張機能の完全性を保証し、またそれらが正当なソース（情報源）から来たものであることを保証するための、メカニズムを実装しなければならない (must)。TOE は、任意のクライアントソフトウェア、プラグイン及び拡張機能について、その後適用されるアップデートと同じように、インストール時及び実行時に検証されるため、利用可能とするメカニズム及びポリシーを提供し、実施しなければならない(must)。さらに、TOE は実行可能形式のダウンロード及び起動についても制御しなければならない (shall)。

[O.INTEGRITY]

3.1.4 秘密の情報のセキュアなストレージ

電子メールクライアントは、数多くの種類の潜在的に秘密の利用者情報 (例えば、パスワード、暗号鍵、デジタル証明書) を取り扱う。保存する際にクライアントがこの情報を保護することは重要である。電子メールクライアントは、この情報を保護するために、電子メールクライアント自身の一部であるメカニズムやライブラリではなく、プラットフォームの暗号及び認証のメカニズムやライブラリを利用しなければならない (shall)。

[O.STORAGE]

4 セキュリティ要件

本セクションに含まれるいくつかのセキュリティ機能要件は、*情報技術セキュリティ評価のためのコモンクライテリア バージョン3.1 改定第4 版*のパート 2 から導出されたものに、拡張機能コンポーネントを追加したものである。本セクションは、TOE 自身、あるいは TOE プラットフォームにより満たされるセキュリティ機能要件に対処している。モバイルプラットフォーム上で動作するよう設計された電子メールクライアントの場合、TOE はそのモバイルプラットフォームの保存データ (DAR) 保護を利用しなければならない (shall)。

4.1 表記

CC では、割付、選択、選択中の割付、及び詳細化という、セキュリティ機能要件に関する操作を定義している。本文書では、以下のフォント規則を用いて、CC により定義される操作を特定する。

- 割付：*イタリック体の*テキストで示す。
- PP 作成者によりなされた詳細化：エレメント番号の後に**太字**で表記された「詳細化」という単語と、**太字**の追加されたテキスト及び必要に応じて取り消し線で表記された削除により示される。
- 選択：下線付きテキストで示す。
- 選択中の割付：*イタリック体の下線付き*テキストで示す。
- 繰返し：例えば (1), (2), (3) など、繰返し回数を括弧内に付記して示す。

明示的に言明された SFR は、TOE SFR の要件名の後にラベル「EXT」を持つことにより特定される。

4.2 セキュリティ機能要件

本セクションは、TOE により満たされ得るセキュリティ機能要件に対応する。

4.2.1 クラス：暗号サポート (FCS)

4.2.1.1 暗号鍵の管理

FCS_CKM_EXT.1 暗号鍵ストレージ

FCS_CKM_EXT.1.1 TSF は、永続的秘密及びプライベート鍵を使用していない時は、永続的秘密及びプライベート鍵をプラットフォームが提供する鍵ストレージに保存しなければならない (shall)。

適用上の注意：

本要件により、永続的秘密 (例えば、パスワード、証明書、その他の資格情報、秘密鍵) 及びプライベート鍵が使用されていない際、セキュアに保存されることを保証する。

本要件は、電子メールクライアントにより使用される永続的秘密及びプライベート鍵が、プラットフォームにより保存されることを、必須としている。

保証アクティビティ：

評価者は、ST における要件を満たすことが必要とされる、それぞれの永続的秘密 (パスワード、資格情報、または秘密鍵) 及びプライベート鍵が、列挙されていることを保証するため、TSS をチェックする。これらの各項目について、評価者は、その項目がどのように識別されるか、何の目的に用いられるか、そしてどのように保存されるか TSS に列挙されていることを確認する。次に評価者は、以下のアクションを行う。

プラットフォームにより操作される永続的秘密及びプライベート鍵

ST に列挙された各プラットフォームについて、評価者は、電子メールクライアントの ST のプラットフォームにより保存されるものとして列挙された永続的秘密及びプライベート鍵が、そのプラットフォームの ST において保護されるものとして識別されていることを保証するため、プラットフォームの ST を検査しなければならない (shall)。

TOE で取り扱う永続的秘密及びプライベート鍵

評価者は、TOE で取り扱うものとして列挙された各項目について、暗号化されずに永続的メモリへ書き込まれないこと、及びその項目がプラットフォームにより保存されることを、TSS が立証していることを決定するために、TSS をレビューする。

4.2.2 クラス：利用者データ保護 (FDP)

4.2.2.1 S/MIME によるデータ保護

FDP_SMIME_EXT.1.1 TSF は、メールの署名、検証、暗号化、及び復号を行うために、Secure/Multipurpose Internet Mail Extensions (S/MIME) を使用しなければならない (shall)。

適用上の注意：*S/MIME は、メール転送エージェントを介した電子メールの送信の際、利用者の要求に応じてメッセージに署名するため(FMT_SMF.1.1 機能 7) に用いられる。S/MIME は、受信者により、メッセージの受信または閲覧の際、署名されたメッセージのデジタル署名を検証するために用いられる。メッセージの暗号化は、メール転送エージェントを介した電子メールの送信の際、利用者の要求に応じて行われ (FMT_SMF.1.1 機能 8)、電子メールの復号は、メッセージの受信または閲覧の際に行われる。本要件は、S/MIME をすべての着信/発信メッセージに対して用いることを義務付けているわけではなく、また TOE がすべての送受信メッセージに対して自動的に暗号化または署名/検証することを義務付けているわけではないことに注意すること。本要件は、デジタル署名及び暗号化のメカニズムが S/MIME でなければならない (must) と規定しているだけである。*

保証アクティビティ：

評価者は、TSS が S/MIME 実装の記述を含むこと、及びデジタル署名を用いた未検出の改変及び暗号化を用いた不正な暴露からメールを保護していることを、検証しなければならない (shall)。評価者は、受信またはメッセージの内容の閲覧の際に、署名の検証及び復号が行われるかどうか、及びメッセージがその S/MIME エンベロープとともに保存されるかどうか、TSS に記述されていることを検証しなければならない (shall)。

評価者は、S/MIME で使用するために証明書を設定するための指示と、電子メールの署名と暗号化についての指示が、AGD ガイダンスに含まれていることを保証しなければならない (shall)。

本エレメントのテストは、FCS_SMIME_EXT.1、FDP_NOT_EXT.1、及び FMT_SMF.1 のテストと組み合わせて実行される。

4.2.2.2 S/MIME による証明書のアクセス

FDP_SMIME_EXT.1.2 [選択：TSF、TOE プラットフォーム] は、S/MIME 暗号化を目的とする証明書リポジトリへのアクセスを提供しなければならない (shall)。

適用上の注意：*暗号化には、X.509v3 証明書の形式で受信者の公開鍵へのアクセスが要求される；したがって、これらの公開鍵は、ローカルまたはリモートのリポジトリを介してアクセス可能でなければならない (must)。本リポジトリの構成は、TOE または TOE プラットフォームのいずれかにより、FMT_SMF.1.1 機能 10 にしたがって実行されることが要求される。*

保証アクティビティ：

評価者は、証明書リポジトリの実装の記述が TSS に含まれることを検証しなければならず (shall)、その記述には少なくともリポジトリがローカル、リモート、あるいはその両方であるか、そしてリポジトリが TOE とプラットフォームのどちらにより管理されるかについて示されなければならない (must)。その記述にリモートリポジトリが利用され得ることが示されている場合、評価者はそのリポジトリとのインタフェースにどのプロトコルが用いられ得るかを記述に示されていることを保証しなければならない (shall)。また評価者は、証明書が自動的にロードされるか、または手作業で追加しなければならない (must) かのいずれであるかについて、ローカルリポジトリの記述に示されていることも検証しなければならない (shall)。自動的にロードされる場合、評価者は、自動メカニズムの記述 (例えば、署名された電子メールが受信された際、関連付けられた証明書がローカルリポジトリへロードされる等) が提供されていることを保証しなければならない (shall)。

また、評価者は、S/MIME 暗号化に用いられる証明書リポジトリを構成するための指示が AGD ガイダンスに含まれていることも検証しなければならない (shall)。TSS にリポジトリがローカルであると示されている場合、評価者は、その指示に証明書がどのようにロードされ、削除されるかについて示されていることを検証しなければならない (shall)。TSS にリポジトリがリモートであると示されている場合、評価者は、その指示に利用者または管理者がどのようにリモートサーバ情報を構成するかについて示されていることを検証しなければならない (shall)。

本エレメントのテストは、FCS_SMIME_EXT.1 及び FMT_SMF.1 のテストと組み合わせて実行される。

4.2.2.3　データ通知

FDP_NOT_EXT.1 電子メール受信の通知

FDP_NOT_EXT.1.1 TSF は、電子メール受信の通知を表示しなければならない (shall)。

適用上の注意：*通知は視覚的なものでも聴覚的なものでもよく、また電子メールについての追加の情報や受信した電子メールの数が含まれても含まれなくてもよい。通知の実装には、短時間ポップアップして電子メールの件名、送信者、及び部分的な内容を表示するようなものがある。FMT_SMF.1.1 機能 1 では、これらの通知を無効化する能力が要求されている。通知に何らかの電子メールの内容が含まれる場合、通知の内容表示を無効化する能力を要求する FMT_SMF.1.1 機能 9 が、ST に含まれなければならない (must)。*

保証アクティビティ：

評価者は、通知が視覚的または聴覚的のいずれかであるか、電子メールに関する何らかの情報が含まれるか、そして電子メールに関する情報が含まれる場合にはどのような情報であるか (電子メールの数、件名、送信者、または部分的な内容等) を含めて、電子メール通知が TSS に記述されていることを保証しなければならない (shall)。電子メールの内容が通知に含まれることが TSS に示されている場合、評価者は、ST に FMT_SMF.1.1 の機能 9 が含まれていることを保証しなければならない (shall)。

評価者は、利用者への通知の記述が (適切な視覚的な形で) AGD ガイダンスに提供されていることを検証しなければならない (shall)。また AGD ガイダンスには、利用者及び／または管理者が通知を無効化し得る方法についても記述されなければならない (must)。通知にメールの内容が含まれることが TSS に示されている場合、評価者は、AGD ガイダンスが通知において内容の表示を無効化するための指示を提供していることを保証しなければならない (shall)。

評価者は、以下のテストを実行しなければならない (shall)。

テスト 1 : 評価者は、クライアントへ電子メールを送信し、記述されているように通知が現れることを検証しなければならない (shall)。

FDP_NOT_EXT.2 S/MIME の状態の通知

FDP_NOT_EXT.2.1 TSF は、受信した電子メールの S/MIME の状態の通知を閲覧の際に表示しなければならない (shall)。

適用上の注意: *S/MIME の状態は、その電子メールが署名または暗号化されているかどうか、そして署名が検証され関連付けられた証明書の有効性が確認されているかどうかである。本通知は、FIA_X509_EXT.2.6 を満たすこと。本通知は、少なくとも電子メールの内容が閲覧される際に表示されなければならない (must)。多くの実装では、すべての電子メールがリストとして閲覧される際にも各電子メールの S/MIME の状態が表示されている。*

保証アクティビティ：

評価者は、S/MIME の状態が電子メールのリストを閲覧する際にも示されるかどうかを含め、S/MIME の状態の通知が TSS に記述されていることを保証しなければならない (shall)。

評価者は、暗号化、検証済み及び有効性確認済みの署名、そして未検証及び有効性未確認の署名のそれぞれが、どのように示されるかを含め、S/MIME の状態の記述が (適切な視覚的な形で) AGD ガイダンスに明確に示されていることを検証しなければならない (shall)。

評価者は、以下のテストを実行しなければならず (shall)、またこれらは FCS_SMIME_EXT.1 のテストと組み合わせて行うことができる。

テスト 1 : 評価者は、クライアントへ暗号化されていない未署名の電子メールを送信し、閲覧の際に通知が提示されないことを検証しなければならない (shall)。

テスト 2 : 評価者は、クライアントへ暗号化された電子メールを送信し、閲覧の際に暗号化の通知が提示されることを検証しなければならない (shall)。

テスト 3 : 評価者は、クライアントへ有効な署名のある電子メールを送信し、閲覧の際に署名の通知が提示されることを検証しなければならない (shall)。

テスト 4 : 評価者は、クライアントへ (例えば、正しい電子メールアドレスを含まない証明書や、ルートストアへ連鎖しない証明書を使って) 無効な署名のある電子メールを送信し、閲覧の際に無効な署名の通知が提示されることを検証しなければならない (shall)。

FDP_NOT_EXT.3 URI の通知

FDP_NOT.EXT.3.1 TSF は、埋め込みリンクについて、その完全な Uniform Resource Identifier (URI) を表示しなければならない (shall)。

適用上の注意: *埋め込みリンクは、リンクの URI をあいまい化するタグ (単語、フレーズ、アイコン、または画像) を持ち得る HTML URI オブジェクトである。本要件の意図は、リンクをあいまいでなくすることである。URI は、「マウスオーバー」イベントとして表示されたり、タグの隣に表示されたりしてもよい。*

保証アクティビティ：

評価者は、埋め込みリンクが表示される方法と、そのリンクの URI が表示される手法が、TSS に含まれることを検証しなければならない (shall)。

評価者は、埋め込みリンクの URI を閲覧するための指示が (適切な視覚的図表と共に) AGD ガイダンスに含まれることを保証しなければならない (shall)。

評価者は、以下のテストを実行しなければならない (shall)。

テスト 1 : 評価者は、クライアントへ、タグが URI そのものでないような (例えば、「ここ

をクリック」）埋め込みリンクを持つHTML メッセージを送信しなければならない (shall)。評価者は本メッセージを閲覧し、AGD ガイダンス中の指示に従って、埋め込みリンクの完全な URI が表示されることを検証しなければならない (shall)。

4.2.2.4　メッセージ内容の表示

FDP_REN_EXT.1.1 TSF は、プレーンテキストのみのモードを持たなければならない (shall)。

適用上の注意：*プレーンテキストのみのモードは、画像の自動的なダウンロードと、HTML または JavaScript オブジェクトなどの埋め込みオブジェクトの表示及び実行を防止する。FMT_SMF.1.1 機能 3 が、このモードの構成に対応している。*

保証アクティビティ：

評価者は、プレーンテキストのみのモードでのメッセージの送信及び受信が TSS に記述されていることを保証しなければならない (shall)。評価者は、TOE に HTML または JavaScript を表示し実行する能力があるかどうか、TSS に記述されていることを検証しなければならない (shall)。TOE が HTML または JavaScript の表示または実行が可能な場合、この記述には TOE がプレーンテキストのみのモードにある間 HTML または JavaScript を含む受信済みメッセージをどのように取り扱うか示されていなければならず (must)、また評価者はこれらの種類の埋め込みオブジェクトが表示または実行されず、画像が自動的にダウンロードされないことが、その記述に示されていることを保証しなければならない (shall)。

評価者は、プレーンテキストのみのモードを有効化するための指示が含まれていることを検証するため、TSS を検査しなければならない (shall)。

評価者は、以下のテストを実行しなければならない (shall)。

テスト 1：(条件付き) TOE が HTML を表示する能力を持つ場合、評価者はクライアントへ HTML 埋め込みオブジェクトを含むメッセージを送信しなければならず (shall)、またその HTML が表示されることを検証しなければならない (shall)。次に評価者は、プレーンテキストのみのモードを有効化し、その HTML が表示されないことを検証しなければならない (shall)。

テスト 2：(条件付き) TOE が JavaScript を表示及び実行する能力を持つ場合、評価者はクライアントへ JavaScript 埋め込みオブジェクトを含むメッセージを送信しなければならず (shall)、またその JavaScript が表示され実行されることを検証しなければならない (shall)。次に評価者は、プレーンテキストのみのモードを有効化し、その JavaScript が表示または実行されないことを検証しなければならない (shall)。

4.3 TOE または TOE プラットフォームのセキュリティ機能要件

本セクションは、TOE そのものにより、TOE プラットフォームにより、あるいは TOE と TOE プラットフォームの組み合わせにより満たされ得るセキュリティ機能要件に対応する。

4.3.1 クラス：暗号サポート (FCS)

4.3.1.1　暗号鍵の管理

FCS_CKM.1 暗号鍵の生成

FCS_CKM.1.1(1) **詳細化：** [選択：TSF、TOE プラットフォーム] は、以下にしたがって**鍵確立に用いられる非対称**暗号鍵を生成しなければならない (shall)。

- 楕円曲線ベースの鍵確立スキームならびに「NIST 曲線」 P-256、P-384 及び [選択：P-521、その他の曲線なし] (FIPS PUB 186-4, “Digital Signature Standard” の定義による) の実装については、NIST Special Publication 800-56A,

“Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”

- RSA ベースの鍵確立スキームについては、NIST Special Publication 800-56B, “Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography”

[選択：

- *有限体ベースの鍵確立スキームについては、NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”、*
- *その他のスキームなし*]

また、規定された暗号鍵サイズは *112 ビットの対称鍵強度と同等、またはそれよりも大きくなければならない。*

適用上の注意：

本コンポーネントは、TOE により用いられるさまざまな暗号プロトコル (例えば高信頼チャネル) の鍵確立の目的で用いられる公開鍵/プライベート鍵ペアを TSF または TOE プラットフォームが生成できることを要求する。複数のスキームがサポートされている場合には、ST 作成者は本要件を繰り返して本機能を取り込むべきである (should)。用いられるスキームは、ST 作成者により選択の中から選ばれることになる。

用いられるべきドメインパラメータは本 PP のプロトコル要件により規定されているため、TOE がドメインパラメータを生成することは期待されておらず、したがって本 PP に規定されたプロトコルに TOE が準拠する際には追加的なドメインパラメータの検証は必要とされない。

2048 ビットの DSA 及び RSA 鍵の生成鍵強度は、112 ビットの対称鍵強度と同等、またはそれよりも大きくなければならない。同等の鍵強度に関する情報については、NIST Special Publication 800-57, “Recommendation for Key Management”を参照されたい。

RSA 及び楕円曲線ベースのスキームは、FCS_TLSC_EXT.1 に要求される暗号スイートへ適合するため要求される。

保証アクティビティ：

プラットフォームにより満たされる要件

ST 中に列挙されたプラットフォームのそれぞれについて、評価者は、そのプラットフォームの ST に主張される鍵確立に電子メールクライアントの ST における鍵確立要件が含まれていることを保証するため、プラットフォームの ST を検査しなければならない (shall)。また評価者は、(サポートされるプラットフォームのそれぞれについて) 鍵確立機能が呼び出される方法が記述されていることを検証するため、電子メールクライアントの ST の TSS を検査しなければならない (shall) (これは電子メールクライアントにより実装されないメカニズムにより行われる可能性があることには注意すべきである (should) が、その場合にもそのメカニズムは本保証アクティビティの一部として TSS 中に特定されることになる)。

TOE により満たされる要件

本保証アクティビティは、TOE 上で用いられる鍵生成及び鍵確立方式を検証する。

鍵生成：

評価者は、下記から該当するテストを用いて、サポートされるスキームの鍵生成ルーチンの実装を検証しなければならない (shall)。

RSA ベースの鍵確立スキーム向け鍵生成

評価者は、鍵生成テストを用いて TOE による RSA 鍵生成の実装を検証しなければならない (shall)。本テストは、公開鍵検証指数 e、プライベート素因数 p 及び q、公開モジュラス (modulus) n 及びプライベート署名指数 d の計算を含めた鍵コンポーネントの値を正しく求める TSF の能力を検証する。

鍵ペア生成では、素数 p 及び q を生成するための 5 とおりの方法 (または手法) を規定している。これには、以下のものが含まれる。

- *ランダム素数：*
  - *証明可能素数*
  - *確率的素数*
- *条件付き素数：*
  - *素数 p1、p2、q1、q2、p 及び q を、すべて証明可能素数とする (shall)*
  - *素数 p1、p2、q1 及び q2 を証明可能素数とし (shall)、p 及び q を確率的素数とする (shall)*
  - *素数 p1、p2、q1、q2、p 及び q を、すべて確率的素数とする (shall)*

ランダム証明可能素数手法とすべての条件付き素数手法の鍵生成手法をテストするため、評価者は決定論的に RSA 鍵ペアを生成するために十分なデータをシードとして TSF 鍵生成ルーチンに与えなければならない (must)。これには、1 つまたは複数の乱数シード、RSA 鍵の公開鍵指数、及び望ましい鍵の長さが含まれる。サポートされている鍵の長さのそれぞれについて、評価者は 25 個の鍵ペアを TSF に生成させなければならない (shall)。評価者は、TSF により生成された値を既知の良好な実装から生成された値と比較することにより、TSF の実装の正しさを検証しなければならない (shall)。

有限体暗号 (FFC) ベースの 56A スキーム向け鍵生成

FFC ドメインパラメータ及び鍵生成テスト

評価者は、パラメータ生成及び鍵生成テストを用いて TOE による FFC 向けパラメータ生成及び鍵生成の実装を検証しなければならない (shall)。本テストは、フィールド素数 p、暗号素数 q (p-1 を割り切る)、暗号群生成元 g、ならびにプライベート鍵 x 及び公開鍵 y の計算の値を正しく求める TSF の能力を検証する。

パラメータ生成では、暗号素数 q 及びフィールド素数 p を生成するための 2 とおりの方法 (または手法)：

- *暗号素数及びフィールド素数：*
  - *素数 q 及び p を両方とも証明可能素数とする (shall)*
  - *素数 q 及びフィールド素数 p を両方とも確率的素数とする (shall)*

そして、暗号群生成元 g を生成するための 2 とおりの方法を規定している。

- *暗号群生成元：*
  - *検証可能プロセスにより構築された生成元 g*
  - *検証不可能プロセスにより構築された生成元 g*

鍵生成では、プライベート鍵 x を生成するための 2 とおりの方法を規定している。

- *プライベート鍵 :*
  - *RBG の len(q) ビットの出力、ここで 1 <=x <= q-1*
  - *RBG の len(q) + 64 ビットの出力に、q-1 を法とする剰余演算を行ったもの、ここで 1<= x<=q-1*

RBG のセキュリティ強度は、少なくとも FFC パラメータセットにより提供されるセキュリティの強度と同じでなければならない (must)。

証明可能素数手法の暗号素数及びフィールド素数生成手法、または検証可能プロセスの群生成元 g、あるいはその両方をテストするため、評価者は決定論的にパラメータセットを生成するために十分なデータをシードとして TSF パラメータ生成ルーチンに与えなければならない (must)。

サポートされている鍵の長さのそれぞれについて、評価者は 25 個のパラメータセットと鍵ペアを TSF に生成させなければならない (shall)。評価者は、TSF により生成された値を既知の良好な実装から生成された値と比較することにより、TSF の実装の正しさを検証しなければならない (shall)。検証では、以下

- *g != 0,1*
- *q が p-1 を割り切ること*
- *g^q mod p = 1*
- *g^x mod p = y*

もまた、FFC パラメータセットと鍵ペアのそれぞれについて、確認されなければならない (must)。

楕円曲線暗号 (ECC) ベースの 56A スキーム向け鍵生成

ECC 鍵生成テスト

サポートされている NIST 曲線、すなわち P-256、P-284 及び P-521 のそれぞれについて、評価者は 10 個のプライベート鍵／公開鍵ペアを試験対象実装 (IUT) に生成させなければならない (shall)。プライベート鍵は、承認済みランダムビット生成器 (RBG) を用いて生成されなければならない (shall)。正しさを判断するため、評価者は生成された鍵ペアを既知の良好な実装の公開鍵検証 (PKV) 機能へ提出しなければならない (shall)。

ECC 公開鍵検証 (PKV) テスト

サポートされている NIST 曲線、すなわち P-256、P-284 及び P-521 のそれぞれについて、評価者は既知の良好な実装の鍵生成機能を用いて 10 個のプライベート鍵／公開鍵ペアを生成し、5 個の公開鍵を不正な値となるように変更し、5 個を未変更の (すなわち、正しい) 値のままにしなければならない (shall)。評価者は、これに応じた 10 個の合格/不合格値のセットを取得しなければならない (shall)。

鍵確立スキーム

評価者は、以下から該当するテストを用いて、TOE によりサポートされる鍵確立スキームの実装を検証しなければならない (shall)。

SP800-56A 鍵確立スキーム

評価者は、以下の機能及び検証テストを用いて、SP800-56A 鍵共有スキームの TOE の実装を検証しなければならない (shall)。各鍵共有スキーム向けのこれらの検証テストは、勧告中の仕様にしたがった鍵共有スキームのコンポーネントが TOE に実装されて

いることを検証するものである。これらのコンポーネントには、DLC プリミティブ (共有秘密の値 Z) の計算と、鍵導出関数 (KDF) による導出鍵マテリアル (DKM) の計算が含まれる。鍵確認がサポートされる場合、評価者はまた以下に記述されるテスト手順を用いて、鍵確認のコンポーネントが正しく実装されていることも検証しなければならない (shall)。これには、DKM の解析、MAC データの生成、及び MAC タグの計算が含まれる。

機能テスト

機能テストは、鍵共有スキームを正しく実装する TOE の能力を検証する。本テストを行うために評価者は、TOE のサポートするスキームの既知の良好な実装からテストベクトルを生成または取得しなければならない (shall)。サポートされている鍵共有スキーム・鍵共有役割の組み合わせ、KDF タイプと (サポートされている場合には) 鍵確認役割・鍵確認タイプの組み合わせのそれぞれについて、試験者は 10 セットのテストベクトルを生成しなければならない (shall)。本データセットは、10 セットの公開鍵あたり 1 セットのドメインパラメータ値 (FFC) または NIST 認可曲線 (ECC) からなる。これらの鍵は、テストされるスキームにより静的鍵であるか、短期鍵であるか、あるいはその両方である。

評価者は、DKM、対応する TOE の公開鍵 (静的鍵または短期鍵あるいはその両方)、1 つまたは複数の MAC タグ、及びその他の情報フィールド (OI) や TOE id フィールドなど KDF において用いられる任意の入力を取得しなければならない (shall)。

TOE が SP 800-56A に定義される KDF を利用しない場合、評価者は公開鍵と共有秘密のハッシュ値のみを取得しなければならない (shall)。

評価者は、既知の良好な実装を用いて共有秘密の値を計算し、鍵マテリアル DKM を導出し、そしてこれらの値から生成されるハッシュまたは MAC タグを比較することにより、所与のスキームの TSF の実装の正しさを検証しなければならない (shall)。

鍵確認がサポートされている場合、実装されている認可 MAC アルゴリズムのそれぞれについて、TSF は上記を実行しなければならない (shall)。

検証テスト

検証テストは、相手方の有効及び無効な鍵共有結果を、鍵確認と共に、または鍵確認なしで、認識する TOE の能力を検証する。本テストを実施するため評価者は、SP800-56A 鍵共有実装に含まれるサポートする暗号機能のリストを取得し、どのエラーを TOE が認識可能であるべきか (should) を判断しなければならない (shall)。評価者は、ドメインパラメータ値または NIST 認可曲線、評価者の公開鍵、TOE の公開鍵／プライベート鍵ペア、MAC タグ、及びその他の情報フィールドや TOE id フィールドなど KDF において用いられる任意の入力を含むデータセットから構成される 24 個 (FFC) または 30 個 (ECC) のテストベクトルのセットを生成する。

評価者はテストベクトルの一部にエラーを注入し、以下のフィールドが不正であるために生じる無効な鍵共有結果を TOE が認識することをテストしなければならない (shall)：共有秘密の値 Z、DKM、その他の情報フィールド OI、MAC 対象データ、または生成された MAC タグ。完全な、または部分的な (ECC のみ) 公開鍵検証が TOE に含まれる場合、評価者はまた両者の静的公開鍵、両者の短期公開鍵及び TOE の静的プライベート鍵へ個別にエラーを注入し、公開鍵検証機能または部分的な鍵検証機能 (ECC のみ) あるいはその両方におけるエラーを TOE が検出できることをも保証する。少なくとも 2 個のテストベクトルは未変更のままでなければならず (shall)、したがって有効な鍵共有結果をもたらすべきである (should) (これらのテストベクトルは合格すべきである (should))。

TOE は、これらの改変されたテストベクトルを利用して、対応するパラメータを用いた鍵共有スキームをエミュレートしなければならない (shall)。評価者は TOE の結果を既知の良好な実装を用いた結果と比較して、TOE がこれらのエラーを検出することを検証しなければならない (shall)。

SP800-56B 鍵確立スキーム

現時点では、RSA ベースの鍵確立スキーム向けの詳細なテスト手順は利用できない。TSF が 800-56B に適合していることを示すため、行われた選択に応じて、評価者は TSS に以下の情報が含まれることを保証しなければならない (shall)。

- *TSS には、TOE が適合する 1 つまたは複数の適切な 800-56B 標準のすべてのセクションが列挙されていなければならない (shall)。*
- *TSS に列挙された該当するセクションのそれぞれについて、「しなければならない (shall)」でない言明（すなわち、「してはならない (shall not)」、「すべきである (should)」、及び「すべきでない (should not)」）のすべてにおいて、そのようなオプションを TOE が実装している場合には、それが TSS に記述されなければならない (shall)。含まれる機能が標準においては「してはならない (shall not)」または「すべきでない (should not)」とされている場合には、TOE により実装されたセキュリティ方針に対してこれが悪影響を与えない理由の根拠が TSS に提供されなければならない (shall)。*

800-56B の該当するセクションのそれぞれにおいて (選択に応じて)、「しなければならない (shall)」または「すべきである (should)」との言明に関連した機能が欠けている場合には、それが記述されなければならない (shall)。

FCS_CKM_EXT.4 暗号鍵の破棄

FCS_CKM_EXT.4.1 [選択：TSF、TOE プラットフォーム] は、すべての平文の秘密及び秘密暗号鍵ならびに CSP を、もはや必要とされなくなった際にゼロ化しなければならない (shall)。

適用上の注意：

電子メールクライアントプラットフォームが平文の秘密、秘密暗号鍵、及び CSP を用いる一切の操作を実行しない場合、ST 作成者はプラットフォームを選択すべきである (should)。

あらゆるセキュリティ関連情報 (鍵や認証データ、そしてパスワードなど) は、セキュリティ上重要なデータの開示または改変を防止するため、もはや使われなくなった際にはゼロ化されなければならない (must)。

上述のゼロ化は、平文鍵及び暗号サービスプロバイダ (CSP) のすべての中間ストレージ領域 (すなわち、メモリバッファなど任意のストレージであって、そのようなデータの経路中に含まれるもの) に、その鍵／CSP が別の場所へ転送された際に適用される。

TOE にはホスト IT 環境が含まれないため、必然的に本機能の範囲はいくぶん限定される。本要件の目的においては、TOE がホストの正しい基盤となる機能を呼び出してゼロ化を行えば十分である。データがゼロ化されることを確実にするため TOE にカーネルモードメモリドライバが含まれなければならない (has to) ことは意味しない。ホストプラットフォームが、その内部プロセス中で鍵マテリアルのゼロ化を適切に行うことが前提とされる。

保証アクティビティ：

プラットフォームにより満たされる要件

評価者は、秘密鍵 (対称鍵暗号化に用いられる鍵)、プライベート鍵、及び鍵の生成に用いられる CSP であって TOE へ課される FCS_CKM_EXT.4 要件によりカバーされていないも

ののそれぞれが、TSS に記述されていることをチェックして保証しなければならない (shall)。

ST 中に列挙されたプラットフォームのそれぞれについて、評価者は、上記に列挙された秘密鍵、プライベート鍵、及び鍵の生成に用いられる CSP がカバーされていることを保証するため、プラットフォームの ST の TSS を検査しなければならない (shall)。

電子メールクライアントにより満たされる要件

評価者は、秘密鍵 (対称鍵暗号化に用いられる鍵)、プライベート鍵、及び鍵の生成に用いられる CSP のそれぞれが、それらがゼロ化される時点 (例えば、使用直後、システムのシャットダウン時、など)、及び行われるゼロ化手続きの種類 (ゼロで上書き、ランダムパターンで 3 度上書き、など) と共に TSS に記述されていることをチェックして保証しなければならない (shall)。保護されるべきマテリアルの保存に異なる種類のメモリが用いられる場合、評価者はデータが保存されるメモリに応じたゼロ化手続き (例えば、「フラッシュメモリ上に保存される秘密鍵はゼロで 1 度上書きすることによりゼロ化されるが、内部ハードドライブ上に保存される秘密鍵は書き込みごとに変化するランダムパターンを 3 度上書きすることによりゼロ化される」) が TSS に記述されていることをチェックして保証しなければならない (shall)。ゼロ化を検証するためにリードバックが行われる場合、このことも記述されなければならない (shall)。

TSS に記述される鍵クリア状況のそれぞれについて、評価者は以下のテストを繰り返さなければならない (shall)。

テスト 1：評価者は、TOE 及び計測機能を備えた TOE ビルドに適切な専用の運用環境と開発ツール (デバッガ、シミュレータなど) の組み合わせを利用して、鍵 (その鍵に関する通常の暗号処理中に TOE により内部的に作成される可能性のある鍵の中間コピーのすべてを含む) が正しくクリアされることをテストしなければならない (shall)。

ソフトウェア中の暗号 TOE 実装は、デバッガの下でロード及び行使され、そのようなテストが行われなければならない (shall)。評価者は、TOE により永続的に暗号化される鍵の中間コピーを含め、クリア対象となる鍵のそれぞれについて、以下のテストを実行しなければならない (shall)。

- *計測機能を備えた TOE ビルドをデバッガへロードする。*
- *クリア対象となる TOE 内の鍵の値を記録する。*
- *#1 の鍵に関する通常の暗号処理を TOE に行わせる。*
- *TOE に鍵をクリアさせる。*
- *TOE に実行を停止させるが、終了はさせない。*
- *TOE に、TOE の全メモリフットプリントをバイナリファイルへダンプさせる。*
- *#4 で作成されたバイナリファイルの内容から、#1 の既知の鍵の値のインスタンスを検索する。*

本テストは、ステップ#7 で#1 の鍵のコピーが見つからなかった場合に成功し、それ以外の場合に失敗する。

評価者は本テストを、暗号化された形態で永続するものを含めたすべての鍵に関して行い、中間コピーがクリアされることを保証しなければならない (shall)。

テスト 2：TOE がファームウェアに実装されておりデバッガを用いることができない制限された運用環境で動作している場合、評価者は汎用オペレーティングシステム上で TOE のシミュレータを利用しなければならない (shall)。評価者は、シミュレートされたテスト環

境という計測設備を説明し、得られたテスト結果を正当化する根拠を提供しなければならない (shall)。

4.3.1.2　暗号操作

FCS_COP.1(1) 暗号操作 (暗号化及び復号)

FCS_COP.1.1(1) [選択 : TSF、TOE プラットフォーム] は、以下の規定された暗号アルゴリズム

- *(NIST SP 800-38A に定義される) AES-CBC モード、*

[選択：

- *(NIST SP 800-38D に定義される) AES-GCM、*
- *その他のモードなし*]

及び暗号鍵サイズ 128 ビット、256 ビットにしたがって [***暗号化／復号***] を実行しなければならない (shall)。

保証アクティビティ：

プラットフォームにより満たされる要件

ST 中に列挙されたプラットフォームのそれぞれについて、評価者は、そのプラットフォームの ST に主張される 1 つまたは複数の暗号化／復号機能に電子メールクライアントの ST における 1 つまたは複数の暗号化／復号機能が含まれていることを保証するため、プラットフォームの ST を検査しなければならない (shall)。また評価者は、(サポートされるプラットフォームのそれぞれについて) 暗号化／復号機能が呼び出される方法が、電子メールクライアントの ST 中に選択されたモードと鍵サイズごとに記述されていることを検証するため、電子メールクライアントの ST の TSS を検査しなければならない (shall) (これは電子メールクライアントにより実装されないメカニズムにより行われる可能性があることには注意すべきである (should) が、その場合にもそのメカニズムは本保証アクティビティの一部として TSS 中に特定されることになる)。

電子メールクライアントにより満たされる要件

AES-CBC テスト

AES-CBC 既知解テスト

既知解テスト (KAT) には、以下に記述される 4 つがある。すべての KAT において、平文、暗号文、及び IV の値は 128 ビットのブロックとする (shall)。各テストの結果は、直接評価者により、あるいは入力を実装者へ供給しその結果を受領することにより、取得され得る。正しさを判断するため、評価者は結果の値を、同一の入力を既知の良好な実装へ与えることにより得られた値と比較しなければならない (shall)。

- ***KAT-1。****AES-CBC の暗号化機能をテストするため、評価者は 10 個の平文の値のセットを供給し、すべてゼロの鍵の値とすべてゼロの IV を用いて所与の平文の AES-CBC 暗号化から得られる暗号文の値を取得しなければならない (shall)。5 個の平文の値は 128 ビットのすべてゼロの鍵で暗号化されるものとし (shall)、それ以外の 5 個は 256 ビットのすべてゼロの鍵で暗号化されるものとする (shall)。*

  AES-CBC の復号機能をテストするため、評価者は 10 個の暗号文の値を入力として AES-CBC 復号を用いて、暗号化と同一のテストを実行しなければならない (shall)。

- ***KAT-2。****AES-CBC の暗号化機能をテストするため、評価者は 10 個の鍵の値のセ*

ットを供給し、所与の鍵の値とすべてゼロの IV を用いてすべてゼロの平文の AES-CBC 暗号化から得られる暗号文の値を取得しなければならない (shall)。5 個の鍵は 128 ビットの鍵とし (shall)、それ以外の 5 個は 256 ビットの鍵とする (shall)。

AES-CBC の復号機能をテストするため、評価者はすべてゼロの暗号文の値を入力として AES-CBC 復号を用いて、暗号化と同一のテストを実行しなければならない (shall)。

- ***KAT-3。** AES-CBC の暗号化機能をテストするため、評価者は以下に記述する 2 セットの鍵の値を供給し、所与の鍵の値とすべてゼロの IV を用いてすべてゼロの平文の AES 暗号化から得られる暗号文の値を取得しなければならない (shall)。第 1 の鍵のセットは 128 個の 128 ビットの鍵からなるものとし (shall)、第 2 のセットは 256 個の 256 ビットの鍵からなるものとする (shall)。[1,N] の範囲の i について、各セットの鍵 i の左端の i ビットは 1、右端の N-i ビットは 0 とする (shall)。*

  AES-CBC の復号機能をテストするため、評価者は以下に記述する 2 セットの鍵と暗号文の値のペアを供給し、所与の鍵の値とすべてゼロの IV を用いて所与の暗号文の AES-CBC 復号から得られる平文の値を取得しなければならない (shall)。第 1 の鍵／暗号文のペアのセットは 128 個の 128 ビットの鍵／暗号文のペアからなるものとし (shall)、第 2 のセットは 256 個の 256 ビットの鍵／暗号文のペアからなるものとする (shall)。[1,N] の範囲の i について、各セットの鍵 i の左端の i ビットは 1、右端の N-i ビットは 0 とする (shall)。各ペアの暗号文の値は、それに対応する鍵で復号された際にすべてゼロの平文が得られるような値とする (shall)。

- ***KAT-4。** AES-CBC の暗号化機能をテストするため、評価者は以下に記述する 128 個の平文の値のセットを供給し、2 種類の暗号文の値 (それぞれ、すべてゼロの 128 ビットの鍵の値とすべてゼロの IV、及びすべてゼロの 256 ビットの鍵の値とすべてゼロの IV を用いて、所与の平文の AES-CBC 暗号化から得られる) を取得しなければならない (shall)。[1,128] の範囲の i について、各セットの平文の値 i の左端の i ビットは 1、右端の N-i ビットは 0 とする (shall)。*

  AES-CBC の復号機能をテストするため、評価者は暗号化テストにおける平文と同一の形式の暗号文の値を入力として AES-CBC 復号を用いて、暗号化と同一のテストを実行しなければならない (shall)。

AES-CBC 複数ブロックメッセージテスト

評価者は、i 個のブロックからなるメッセージ (ここで 1< i <=10) を暗号化することにより、暗号化機能をテストしなければならない (shall)。評価者は鍵、IV 及び長さ i ブロックの平文メッセージを選び、選んだ鍵及び IV により、試験すべきモードを用いてメッセージを暗号化しなければならない (shall)。暗号文は、同一の平文メッセージを同一の鍵と IV により既知の良好な実装を用いて暗号化した結果と比較されなければならない (shall)。

また評価者は、i 個のブロックからなるメッセージ (ここで 1< i <=10) を復号することにより、各モードについて復号機能をテストしなければならない (shall)。評価者は鍵、IV 及び長さ i ブロックの暗号文メッセージを選び、選んだ鍵及び IV により、試験すべきモードを用いてメッセージを復号しなければならない (shall)。平文は、同一の暗号文メッセージを同一の鍵と IV により既知の良好な実装を用いて復号した結果と比較されなければならない (shall)。

AES-CBC モンテカルロテスト

評価者は、200 個の平文、IV、及び鍵の 3 つ組のセットを用いて、暗号化機能をテストしなければならない (shall)。これらのうち 100 個は 128 ビットの鍵を用いるものとし (shall)、

100 個は 256 ビットの鍵を用いるものとする (shall)。平文と IV の値は、128 ビットのブロックとする (shall)。3 つ組のそれぞれについて、以下のように 1000 回の反復処理が実行されるものとする (shall)。

```
# 入力 : PT, IV, Key
for i = 1 to 1000:
        if i == 1:
                CT[1] = AES-CBC-Encrypt(Key, IV, PT)
                PT = IV
        else:
                CT[i] = AES-CBC-Encrypt(Key, PT)
                PT = CT[i-1]
```

1000 回目の反復処理において計算された暗号文 (すなわち、CT[1000]) が、その試行の結果となる。本結果は、既知の良好な実装を用いて同一の値により 1000 回反復処理を実行した結果と比較されなければならない (shall)。

評価者は、暗号化と同一のテストを用い、CT と PT とを入れ替え、AES-CBC-Encrypt を AES-CBC-Decrypt で置き換えて、復号機能をテストしなければならない (shall)。

AES-GCM モンテカルロテスト

評価者は、以下の入力パラメータ長の組み合わせのそれぞれについて、AES-GCM 認証付き暗号機能をテストしなければならない (shall)。

- ***128 ビット及び 256 ビットの鍵***
- ***2 とおりの平文の長さ。****平文の長さの一方は、128 ビットのゼロ以外の整数倍とする (shall) (サポートされる場合)。他方の平文の長さは、128 ビットの整数倍であってはならないものとする (shall not) (サポートされる場合)。*
- ***3 とおりの AAD の長さ。****1 つの AAD の長さは 0 とする (shall) (サポートされる場合)。1 つの AAD の長さは、128 ビットのゼロ以外の整数倍とする (shall) (サポートされる場合)。1 つの AAD の長さは、128 ビットの整数倍であってはならないものとする (shall not) (サポートされる場合)。*
- ***2 とおりの IV の長さ。****96 ビットの IV がサポートされる場合、テストされる 2 とおりの IV の長さの一方を 96 ビットとする (shall)。*

評価者は、上記のパラメータ長の組み合わせのそれぞれについて、10 個の鍵、平文、AAD、及び IV の組のセットを用いて暗号化機能をテストし、AES-GCM 認証付き暗号から得られた暗号文とタグを取得しなければならない (shall)。サポートされているタグの長さはそれぞれ、10 個のセットにつき少なくとも 1 度はテストされなければならない (shall)。IV の値は、それが既知である限り、評価者により供給されても、テストされている実装により供給されてもよい。

評価者は、上記のパラメータ長の組み合わせのそれぞれについて、10 個の鍵、平文、暗号文、タグ、AAD、及び IV の 5 つ組のセットを用いて復号機能をテストし、認証に関する合格／不合格結果を取得して、合格の場合には平文を復号しなければならない (shall)。セットには、合格となる 5 組と不合格となる 5 組が含まれなければならない (shall)。

各テストの結果は、直接評価者により、あるいは入力を実装者へ供給しその結果を受領することにより、取得され得る。正しさを判断するため、評価者は結果の値を、同一の入力を既知の良好な実装へ与えることにより得られた値と比較しなければならない (shall)。

FCS_COP.1(2) 暗号操作 (ハッシュ)

FCS_COP.1.1(2) [選択：TSF、TOE プラットフォーム] は、規定された暗号アルゴリズム SHA-1、SHA-256、SHA-384、及び [選択：SHA-512、その他のアルゴリズムなし] であって、メッセージダイジェストのサイズが 160、256、384、 [選択：512、その他のサイズなし] ビットの、以下：*FIPS Pub 180-4* を満たすものにしたがって暗号ハッシュを実行しなければならない (shall)。

適用上の注意：

本 PP の将来の版では、SHA-1 は選択肢から削除されるかもしれない。SHA-1 によるデジタル署名の生成はもはや許可されず、また SHA-1 によるデジタル署名の検証は、これらの署名の受容に存在する可能性のあるリスクのため、強く非推奨とされる。SHA-1 及び SHA-256 は、FCS_TLS_EXT.1 に要求される暗号スイートへ適合するため要求される

本要件の意図は、高信頼アップデート及び高信頼チャネルと関連したデジタル署名生成及び検証に用いられるハッシュ機能を規定することである。ハッシュの選択は、メッセージダイジェストサイズの選択をサポートしなければならない (must)。ハッシュの選択は、FCS_COP.1(1) に用いられるアルゴリズムの全体的な強度と一貫しているべきである (should)。

保証アクティビティ：

プラットフォームにより満たされる要件

ST 中に列挙されたプラットフォームのそれぞれについて、評価者は、そのプラットフォームの ST に主張される 1 つまたは複数のハッシュ機能に電子メールクライアントの ST における 1 つまたは複数のハッシュ機能が含まれていることを保証するため、プラットフォームの ST を検査しなければならない (shall)。また評価者は、(サポートされるプラットフォームのそれぞれについて) ハッシュ機能が呼び出される方法が、電子メールクライアントの ST 中に選択されたダイジェストサイズごとに記述されていることを検証するため、電子メールクライアントの ST の TSS を検査しなければならない (shall) (これは電子メールクライアントにより実装されないメカニズムにより行われる可能性があることには注意すべきである (should) が、その場合にもそのメカニズムは本保証アクティビティの一部として TSS 中に特定されることになる)。

電子メールクライアントにより満たされる要件

評価者は、必要とされるハッシュサイズに機能を構成するために行われることが必要とされる構成があれば、それが存在することを決定するために AGD 文書をチェックする。評価者は、ハッシュ機能と他の TSF 暗号機能 (例えば、デジタル署名検証機能) との関連が TSS に文書化されていることをチェックしなければならない (shall)。

TSF ハッシュ関数は、2 つのモードのいずれかで実装できる。第 1 のモードは、バイト指向モードである。本モードでは、TSF は長さがバイトの整数倍であるメッセージのみをハッシュする。すなわち、ハッシュされるべきメッセージのビット長が 8 で割り切れる必要がある。第 2 のモードは、ビット指向モードである。本モードでは、TSF は任意の長さのメッセージをハッシュする。各モードについて異なるテストが存在するため、ビット指向とバイト指向のテストについて、以下のセクションで指示を与える。

評価者は、TSF により実装され、本 PP の要件を満たすために用いられるハッシュアルゴリズムのそれぞれについて、以下のテストをすべて実行しなければならない (shall)。

ショートメッセージテスト—ビット指向モード

評価者は m+1 個のメッセージからなる入力セットを作り上げる。ここで m はハッシュアルゴリズムのブロック長である。メッセージの長さは、0 から m ビットまでシーケンシャル

に変化する。メッセージの本文は、疑似ランダム的に生成されなければならない (shall)。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。

ショートメッセージテスト—バイト指向モード

評価者は m/8+1 個のメッセージからなる入力セットを作り上げる。ここで m はハッシュアルゴリズムのブロック長である。メッセージの長さは 0 から m/8 バイトまでシーケンシャルに変化し、各メッセージは整数個のバイトとなる。メッセージの本文は、疑似ランダム的に生成されなければならない (shall)。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。

選択されたロングメッセージテスト—ビット指向モード

*評価者は m 個のメッセージからなる入力セットを作り上げる。ここで m はハッシュアルゴリズムのブロック長である。i 番目のメッセージの長さは 512 + 99*i となる (ここで 1 ≤ i ≤ m)。メッセージの本文は、疑似ランダム的に生成されなければならない (shall)。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。*

選択されたロングメッセージテスト—バイト指向モード

*評価者は m/8 個のメッセージからなる入力セットを作り上げる。ここで m はハッシュアルゴリズムのブロック長である。i 番目のメッセージの長さは 512 + 8*99*i となる (ここで 1 ≤ i ≤ m/8)。メッセージの本文は、疑似ランダム的に生成されなければならない (shall)。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。*

疑似ランダム的に生成されたメッセージテスト

本テストは、バイト指向の実装にのみ行われる。評価者は、n ビットの長さのシードをランダムに生成する。ここで n はテストされるハッシュ関数により作成されるメッセージダイジェストの長さである。次に評価者は、[SHAVS] の図 1 に示されるアルゴリズムにしたがって 100 個のメッセージと関連するダイジェストのセットを作成する。次に評価者は、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。

FCS_COP.1(3) 暗号操作 (デジタル署名)

FCS_COP.1.1(3) [選択 : TSF、TOE プラットフォーム] は、以下に規定された暗号アルゴリズムにしたがって暗号署名サービスを実行しなければならない (shall)。

- 2048 ビット以上の鍵サイズ (モジュラス) を用いる RSA デジタル署名アルゴリズム (RSA) であって FIPS PUB 186-2 または FIPS PUB 186-4, “Digital Signature Standard”を満たすもの、
- 256 ビット以上の鍵サイズを用いる楕円曲線デジタル署名アルゴリズム (ECDSA) であって FIPS PUB 186-4, “Digital Signature Standard”と (FIPS PUB 186-4, “Digital Signature Standard”に定義される)「NIST 曲線」 P-256、P-384 及び [選択：P-521、その他の曲線なし] を満たすもの、

[選択：

- 2048 ビット以上の鍵サイズ (モジュラス) を用いるデジタル署名アルゴリズム (DSA) であって FIPS PUB 186-4, “Digital Signature Standard”を満たすもの、その他の暗号署名サービスなし]。

適用上の注意：

電子メールクライアントは、FCS_TLS_EXT.1 にしたがって RSA 及び ECDSA デジタル署名を実行しなければならない (must)。また電子メールクライアントは、プラグイン及び拡張機能上の署名を検証してもよい。

複数のスキームがサポートされている場合には、ST 作成者は本要件を繰り返して本機能を取り込むべきである (should)。用いられるスキームは、ST 作成者により選択の中から選ばれることになる。

保証アクティビティ：

プラットフォームにより満たされる要件

ST 中に列挙されたプラットフォームのそれぞれについて、評価者は、そのプラットフォームの ST に主張されるデジタル署名機能に電子メールクライアントの ST におけるデジタル署名機能が含まれていることを保証するため、プラットフォームの ST を検査しなければならない (shall)。また評価者は、(サポートされるプラットフォームのそれぞれについて) デジタル署名機能が呼び出される方法が、電子メールクライアント中に用いられる操作ごとに記述されていることを検証するため、電子メールクライアントの ST の TSS を検証しなければならない (shall) (これは電子メールクライアントにより実装されないメカニズムにより行われる可能性があることには注意すべきである (should) が、その場合にもそのメカニズムは本保証アクティビティの一部として TSS 中に特定されることになる)。

電子メールクライアントにより満たされる要件

鍵生成：

RSA 署名スキームの鍵生成

評価者は、鍵生成テストを用いて TOE による RSA 鍵生成の実装を検証しなければならない (shall)。本テストは、公開鍵検証指数 e、プライベート素因数 p 及び q、公開モジュラス (modulus) n 及びプライベート署名指数 d の計算を含めた鍵コンポーネントの値を正しく求める TSF の能力を検証する。

鍵ペア生成では、素数 p 及び q を生成するための 5 とおりの方法 (または手法) を規定している。これには、以下のものが含まれる。

- *ランダム素数：*
  - *証明可能素数*
  - *確率的素数*
- *条件付き素数：*
  - *素数 p1、p2、q1、q2、p 及び q を、すべて証明可能素数とする (shall)*
  - *素数 p1、p2、q1 及び q2 を証明可能素数とし (shall)、p 及び q を確率的素数とする (shall)*
  - *素数 p1、p2、q1、q2、p 及び q を、すべて確率的素数とする (shall)*

ランダム証明可能素数手法とすべての条件付き素数手法の鍵生成手法をテストするため、評価者は決定論的に RSA 鍵ペアを生成するために十分なデータをシードとして TSF 鍵生成ルーチンに与えなければならない (must)。これには、1 つまたは複数の乱数シード、RSA 鍵の公開鍵指数、及び望ましい鍵の長さが含まれる。サポートされている鍵の長さのそれぞれについて、評価者は 25 個の鍵ペアを TSF に生成させなければならない (shall)。評価者は、TSF により生成された値を既知の良好な実装から生成された値と比較することにより、TSF の実装の正しさを検証しなければならない (shall)。

ECDSA 鍵生成テスト

FIPS 186-4 ECDSA 鍵生成テスト

サポートされている NIST 曲線、すなわち P-256、P-284 及び P-521 のそれぞれについて、評価者は 10 個のプライベート鍵／公開鍵ペアを試験対象実装 (IUT) に生成させなければならない (shall)。プライベート鍵は、承認済みランダムビット生成器 (RBG) を用いて生成されなければならない (shall)。正しさを判断するため、評価者は生成された鍵ペアを既知の良好な実装の公開鍵検証 (PKV) 機能へ提出しなければならない (shall)。

FIPS 186-4 公開鍵検証 (PKV) テスト

サポートされている NIST 曲線、すなわち P-256、P-284 及び P-521 のそれぞれについて、評価者は既知の良好な実装の鍵生成機能を用いて 10 個のプライベート鍵／公開鍵ペアを生成し、5 個の公開鍵を不正な値となるように変更し、5 個を未変更の (すなわち、正しい) 値のままにしなければならない (shall)。評価者は、これに応じた 10 個の合格/不合格値のセットを取得しなければならない (shall)。

ECDSA アルゴリズムテスト

ECDSA FIPS 186-4 署名生成テスト

サポートされている NIST 曲線 (すなわち、P-256、P-284 及び P-521) と SHA 関数のペアのそれぞれについて、評価者は 10 個の 1024 ビットの長さのメッセージを生成し、各メッセージについて公開鍵ならびに得られた署名の値 R 及び S を取得しなければならない (shall)。正しさを判断するため、評価者は既知の良好な実装の署名検証機能を利用しなければならない (shall)。

ECDSA FIPS 186-4 署名検証テスト

サポートされている NIST 曲線 (すなわち、P-256、P-284 及び P-521) と SHA 関数のペアのそれぞれについて、評価者は 10 個の 1024 ビットの長さのメッセージ、公開鍵及び署名の組のセットを生成し、10 組のうち 5 組で値のいずれか (メッセージ、公開鍵または署名) を変更しなければならない (shall)。評価者は、これに応じた 10 個の合格/不合格値のセットを取得しなければならない (shall)。

RSA 署名アルゴリズムテスト

署名生成テスト

評価者は、署名生成テストを用いて TOE による RSA 署名生成の実装を検証しなければならない (shall)。本テストを行うために評価者は、TSF のサポートするモジュラスのサイズ／SHA の組み合わせのそれぞれについて、高信頼リファレンス実装から 10 個のメッセージを生成または取得しなければならない (must)。評価者は、TOE に自分のプライベート鍵とモジュラスの値を用いてこれらのメッセージへ署名させなければならない (shall)。

評価者は、既知の良好な実装及び関連付けられた公開鍵を用いて署名を検証することにより、TSF の署名の正しさを検証しなければならない (shall)。

署名検証テスト

評価者は、署名検証テストを行って、相手方の有効及び無効な署名を認識する TOE の能力を検証しなければならない (shall)。評価者は、公開鍵 e、メッセージ、IR フォーマット、または署名、あるいはこれらのうち 2 つ以上にエラーを導入することにより、署名検証テスト中に作成されたテストベクトルへエラーを注入しなければならない (shall)。TOE は署名の検証を試行し、成功または失敗を返す。

評価者はこれらのテストベクトルを利用して、対応するパラメータを用いた署名検証テストをエミュレートし、TOE がこれらのエラーを検出することを検証しなければならない (shall)。

FCS_COP.1(4) 暗号操作 (鍵付きハッシュによるメッセージ認証)

FCS_COP.1.1(4) [選択：TSF、TOE プラットフォーム] は、規定された暗号アルゴリズム HMAC- SHA-256 及び [選択：SHA-1、SHA-384、SHA-512、その他のアルゴリズムなし]、鍵サイズが [割付 : HMAC に用いられる (ビット単位の) 鍵サイズ]、そしてメッセージダイジェストのサイズが 256 及び [選択：160、384、512、その他のサイズなし] ビットの、以下 : FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code、及び FIPS Pub 180-4, “Secure Hash Standard”を満たすものにしたがって鍵付きハッシュによるメッセージ認証を実行しなければならない (shall)。

適用上の注意：

本要件の意図は、TOE により用いられるさまざまな暗号プロトコル (例えば高信頼チャネル) の鍵確立の目的で用いられる際に用いられる鍵付きハッシュによるメッセージ認証機能を規定することである。ハッシュの選択は、メッセージダイジェストサイズの選択をサポートしなければならない (must)。ハッシュの選択は、FCS_COP.1(1) に用いられるアルゴリズムの全体的な強度と一貫しているべきである (should)。HMAC-SHA256 は、FCS_TLS_EXT.1 に要求される暗号スイートへ適合するため要求される。

保証アクティビティ：

プラットフォームにより満たされる要件

ST 中に列挙されたプラットフォームのそれぞれについて、評価者は、そのプラットフォームの ST に主張される 1 つまたは複数の鍵付きハッシュ機能に電子メールクライアントの ST における 1 つまたは複数の鍵付きハッシュ機能が含まれていることを保証するため、プラットフォームの ST を検査しなければならない (shall)。また評価者は、(サポートされるプラットフォームのそれぞれについて) 鍵付きハッシュ機能が呼び出される方法が、電子メールクライアントの ST 中に選択されたモードと鍵サイズごとに記述されていることを検証するため、電子メールクライアントの ST の TSS を検査しなければならない (shall) (これは電子メールクライアントにより実装されないメカニズムにより行われる可能性があることには注意すべきである (should) が、その場合にもそのメカニズムは本保証アクティビティの一部として TSS 中に特定されることになる)。

電子メールクライアントにより満たされる要件

評価者は、HMAC 機能により利用される以下の値が規定されていることを保証するため、TSS を検査しなければならない (shall) : 鍵の長さ、用いられるハッシュ関数、ブロックサイズ、そして用いられる出力 MAC 長。

サポートされているパラメータセットのそれぞれについて、評価者は 15 セットのテストデータを構成しなければならない (shall)。各セットは、1 つの鍵とメッセージデータから構成されるものとする (shall)。評価者は、テストデータのこれらのセットについて TSF に HMAC タグを生成させなければならない (shall)。得られた MAC タグは、同一の鍵と IV により既知の良好な実装を用いて生成された HMAC タグと比較されなければならない (shall)。

4.3.1.3 ランダムビット生成

FCS_RBG_EXT.1 拡張：ランダムビット生成

FCS_RBG_EXT.1.1 [選択 : TSF、TOE プラットフォーム] は、 [選択、*1 つを選択 :* [選択 : *Hash_DRBG (任意)* 、*HMAC_DRBG (任意)* 、*CTR_DRBG (AES)* 、*Dual_EC_DRBG (任意)*] を用いる *NIST Special Publication 800-90A*、*FIPS Pub 140-2 附属書 C : AES* を用い

る X9.31 附属書 2.4] にしたがって、すべての決定論的ランダムビット生成サービスを実行しなければならない (shall) 。

FCS_RBG_EXT.1.2 決定論的 RBG は、鍵とそれが生成するハッシュとの (NIST SP 800-57 による) セキュリティ強度の大きいほうと少なくとも等しい、最小で [選択：*128 ビット*、*256 ビット*] のエントロピーを持つ、 [選択：*ソフトウェアベースの雑音源*、*プラットフォームベースの RBG*] からエントロピーを蓄積するエントロピー源によりシードが供給されなければならない (shall)。

適用上の注意：

FCS_RBG_EXT.1.1 の最初の選択に関しては、ST 作成者は TOE か TOE のインストールされるプラットフォームのどちらが RBG サービスを提供するか選択すべきである (should)。

NIST Special Pub 800-90B の附属書 C には、FIPS-140 の将来のバージョンでおそらく必要とされることになる最小エントロピー量が記述されている。可能であれば直ちにこれを用いるべきであり (should)、また本 PP の将来のバージョンでは要求されることになる。

FCS_RBG_EXT.1.1 の 2 番目の選択に関しては、ST 作成者は RBG サービスが適合する標準 (800-90 または 140-2 附属書 C のいずれか) を選択すべきである (should)。

SP 800-90A には、4 つの異なる乱数生成手法が含まれる。これらはそれぞれ、基盤となる暗号プリミティブ (ハッシュ関数／暗号) に依存している。ST 作成者は利用される関数を選択し (800-90A が選択されている場合)、要件または TSS に用いられる具体的な基盤となる暗号プリミティブを取り込む。特定されたハッシュ関数はいずれも Hash_DRBG または HMAC_DRBG に許可されるが、CTR_DRBG には AES ベースの実装のみが許可される。800-90A に定義された任意の曲線が Dual_EC_DRBG に許可される一方で、ST 作成者は選択された曲線だけではなく、利用されるハッシュアルゴリズムも取り込まなければならない (must)。

FCS_RBG_EXT.1.2 の 2 番目の選択に関しては、ST 作成者はエントロピー源がソフトウェアベースであるか、プラットフォームベースであるか、あるいはその両方であるかを示す。エントロピーの源が複数存在する場合には、ST には各エントロピー源のそれぞれについて、それがソフトウェアベースであるかプラットフォームベースであるかを含めて説明する。プラットフォームベースの雑音源が望ましい。

プラットフォームベースの RBG 源は、プラットフォームにより提供される検証済みの RBG の出力であり、これは FCS_RBG_EXT.1.1 にしたがって TSF の提供する DRBG のエントロピー源として利用される。このようにして、開発者は NIST SP800-90C に記述されているように RBG を連鎖する。

FIPS Pub 140-2 の附属書 C については、現在のところ NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms のセクション 3 に記述される手法のみが有効であることに注意されたい。ここで用いられる AES 実装の鍵の長さが利用者データの暗号化に用いられるものと異なる場合には、FCS_COP.1 を調整するか繰り返して異なる鍵の長さを反映する必要があるかもしれない。FCS_RBG_EXT.1.2(1) の選択については、ST 作成者は RBG にシードを供給するために用いられるエントロピーの最小ビット数を選択する。

また ST 作成者は、任意の基盤となる機能が TOE のベースライン要件に確実に含まれるようにする。

保証アクティビティ：

プラットフォームにより満たされる要件

ST 中に列挙されたプラットフォームのそれぞれについて、評価者は、そのプラットフォー

ムの ST に主張される RBG 機能に電子メールクライアントの ST における RBG 機能が含まれていることを保証するため、プラットフォームの ST を検査しなければならない (shall)。また評価者は、(サポートされるプラットフォームのそれぞれについて) RBG 機能が呼び出される方法が、電子メールクライアント中に用いられる操作ごとに記述されていることを検証するため、電子メールクライアントの ST の TSS を検査しなければならない (shall) (これは電子メールクライアントにより実装されないメカニズムにより行われる可能性があることには注意すべきである (should) が、その場合にもそのメカニズムは本保証アクティビティの一部として TSS 中に特定されることになる)。

電子メールクライアントにより満たされる要件

附属書 E にしたがって、文書が作成されなければならない (shall) (そして評価者はアクティビティを実行しなければならない (shall))。

ST 作成者がプラットフォームベースの雑音源を選択した場合、評価者は、プラットフォームの RBG が検証されていることを検証するため、プラットフォームの ST を検査しなければならない (shall)。評価者は、少なくとも本プロファイルに関して ST 作成者により選択されたエントロピー量が、プラットフォームの RBG に供給されていることを検証しなければならない (shall)。この場合、ST 作成者はプラットフォームの RBG の附属書 E 文書に責任を負わない。

また評価者は、RBG が準拠する標準にしたがって、以下のテストを実行しなければならない (shall)。

FIPS 140-2 の附属書 C に準拠する実装

本セクションに含まれるテストの参照情報は、The Random Number Generator Validation System (RNGVS) である。評価者は、以下の 2 つのテストを実施しなければならない (shall)。「期待値」は、正しいことが知られているアルゴリズムの参照実装により作成されることに注意されたい。正しさの証明は、各スキームに任される。

評価者は、可変シードテストを実行しなければならない (shall)。評価者は (Seed, DT) ペア (それぞれ 128 ビット) の 128 個のセットを TSF の RBG 機能に提供しなければならない (shall)。また評価者は、128 ペアの (Seed, DT) すべてについて一定である (AES アルゴリズムに適切な長さの) 鍵も提供しなければならない (shall)。DT の値は、各セットについて 1 ずつ増やされる。シードの値は、セットの中で繰り返されてはならない (shall not)。評価者は、TSF により返される値が期待値と一致することを保証する。

評価者は、モンテカルロテストを実行しなければならない (shall)。本テストについては、評価者がシード及び DT の初期値 (それぞれ 128 ビット) を TSF の RBG 機能に提供する。また評価者は、テストを通して一定である (AES アルゴリズムに適切な長さの) 鍵も提供しなければならない (shall)。次に評価者は、繰返しのたびに DT の値を 1 ずつ増やしながら、そして NIST-Recommended Random Number Generator Based on ANSI X9.31 Annex A.2.4 Using the 3-Key Triple DES and AES Algorithms のセクション 3 に規定されるように次回の繰返しの際の新たなシードを作成して、TSF の RBG を 10,000 回呼び出す。評価者は、得られた 10,000 番目の値が期待値と一致することを保証する。

NIST Special Publication 800-90A に準拠する実装

評価者は、RBG 実装の 15 回の試行を実行しなければならない (shall)。RBG が構成可能な場合、評価者は各構成について 15 回の試行を実行しなければならない (shall)。また評価者は、RBG 機能を構成するための適切な指示が操作ガイダンスに含まれていることも確認しなければならない (shall)。

RBG が有効な予測困難性を持つ場合、各回の試行は (1) DRBG をインスタンス化し、 (2)

ランダムなビットの最初のブロックを生成し、 (3) ランダムなビットの 2 番目のブロックを生成し、 (4) 非インスタンス化する、という手順になる。評価者は、ランダムなビットの 2 番目のブロックが期待された値であることを検証する。評価者は、各試行に 8 つの入力値を生成しなければならない (shall)。最初はカウント (0～14) である。次の 3 つはインスタンス化操作のエントロピー入力とノンス、そして個別化文字列である。次の 2 つは、最初の生成呼び出しへの追加的入力とエントロピー入力である。最後の 2 つは、2 番目の生成呼出しへの追加的入力とエントロピー入力である。これらの値は、ランダムに生成される。「ランダムなビットのひとつのブロックを生成」とは、返されるビット数が (NIST SP 800-90A に定義される) Output Block Length と等しいランダムなビットを生成することを意味する。

RBG が予測困難性を持たない場合、各回の試行は (1) DRBG をインスタンス化し、 (2) ランダムなビットの最初のブロックを生成し、 (3) シードを再供給し、 (4) ランダムなビットの 2 番目のブロックを生成し、 (5) 非インスタンス化する、という手順になる。評価者は、ランダムなビットの 2 番目のブロックが期待された値であることを検証する。評価者は、各試行に 8 つの入力値を生成しなければならない (shall)。最初はカウント (0～14) である。次の 3 つはインスタンス化操作のエントロピー入力とノンス、そして個別化文字列である。5 番目の値は、最初の生成呼出しへの追加的入力である。6 番目と 7 番目は、シードを再供給する呼出しへの追加的入力とエントロピー入力である。最後の値は、2 回目の生成呼出しへの追加的入力である。

以下のパラグラフには、評価者により生成／選択されるべき入力値のいくつかについて、より多くの情報が含まれている。

***エントロピー入力**：エントロピー入力値の長さは、シードの長さと等しくなければならない (must)。*

***ノンス**：ノンスがサポートされている場合 (導出関数 (df) なしの CTR_DRBG はノンスを利用しない)、ノンスのビット長はシードの長さの半分となる。*

***個別化文字列**：個別化文字列の長さは、シードの長さ以下でなければならない (must)。実装が 1 とおりの個別化文字列の長さしかサポートしていない場合には、両方の値に同一の長さが使用できる。2 とおり以上の文字列の長さがサポートされている場合、評価者は 2 つの異なる長さの個別化文字列を用いなければならない (shall)。実装が個別化文字列を用いない場合、値を供給する必要はない。*

***追加的入力**：追加的入力のビット長は、個別化文字列の長さと同一のデフォルトと制約を持つ。*

4.3.1.4 Secure/Multipurpose Internet Mail Extensions (S/MIME)

FCS_SMIME_EXT.1.1 [選択：TSF、TOE プラットフォーム] は、RFC 5652、5754、及び 3565 に定義される CMS を用い、RFC 5751 に定義される S/MIME v3.2 Agent を送信と受信の両方について実装しなければならない (shall)。

適用上の注意：*これらの RFC は、エージェントが送信または受信、あるいは両方の能力を含むことを可能とする。本要件の意図は、TOE に S/MIME v3.2 メッセージの送信と受信の両方の能力があることを確実にすることである。*

FCS_SMIME_EXT.1.2 [選択：TSF、TOE プラットフォーム] は、AES-128 CBC 及び [選択：AES-256 CBC 選択：その他なし] の ContentEncryptionAlgorithmIdentifier を送信しなければならない (shall)。

適用上の注意：*AES は CMS へ、RFC 3565 に定義されるように追加される。*

FCS_SMIME_EXT.1.3 [選択：TSF、TOE プラットフォーム] は、digestAlgorithm フィール

ドに以下のメッセージダイジェストアルゴリズム識別子を提示しなければならない (shall) [選択：id-sha256、id-sha384、id-sha512] 及びその他なし。

FCS_SMIME_EXT.1.4 [選択：TSF、TOE プラットフォーム] は、AlgorithmIdentifier フィールドに以下を提示しなければならない (shall) sha256withRSAEncryption 及び [選択：sha384WithRSAEncryption 、 sha512WithRSAEncryption 、 ecdsa-with-SHA256 、 ecdsa-with-sha384、ecdsa-with-sha512] 及びその他のアルゴリズムなし。

適用上の注意：*RFC 5751 は、受信及び送信エージェントが SHA256 を用いた RSA をサポートすることを義務付けている。評価される構成においてテストされるべきアルゴリズムは、本要件により制限される。これらの要件に適合しない、その他のいかなる実装されたアルゴリズムも、評価される TOE に含まれるべきではない (should not)。上に列挙した ECDSA アルゴリズムは実装が好ましいものであり、本 PP の将来のバージョンでは義務付けられることになる。*

FCS_SMIME_EXT.1.5 [選択：TSF、TOE プラットフォーム] は、署名と暗号化に別個のプライベート鍵 (及び関連付けられた証明書) を用いなければならない (shall)。

FCS_SMIME_EXT.1.6 [選択：TSF、TOE プラットフォーム] は、digitalSignature ビットがセットされた証明書からの署名のみを受け付けなければならない (shall)。

適用上の注意：*keyUsage 拡張が存在しない場合に、digitalSignature ビットがセットされているとみなすことは許容可能である。*

FCS_SMIME_EXT.1.7 [選択：TSF、TOE プラットフォーム] は、 [選択：必要とされる都度、着信/発信メッセージに、周期的に] 証明書失効リスト (CRL) 及び証明書を取り込むメカニズムを実装しなければならない (shall)。

適用上の注意：*TOE は本メカニズムのふるまいを定義できるが、CRL による失効状態がサポートされ、また送信/受信するメッセージについて証明書が取り込めるようなメカニズムが存在することが要求される。本要件において「周期的」は、ローカルストレージへのワンタイム関数として、定期的にスケジュールされた取り込みとして、あるいは手作業での介入を要求するメカニズムとして解釈できる。取り込みメカニズムが周期的な性質のものである場合には、ST 作成者は CRL のストレージに関する FCS の繰返しを含める必要がある。証明書のストレージは、FCS_CKM でカバーされる。証明書及び証明書連鎖のインポートは、本要件には含まれないが、FIA_X509 及び FMT_MOF でカバーされる。*

保証アクティビティ：

評価者は TSS 中の S/MIME の実装の記述をチェックして、適切なバージョンが指定されていることを保証しなければならない (shall)。さらに、評価者はサポートされているアルゴリズムが指定されていること、及び指定されたアルゴリズムが本コンポーネントに列挙されたものであることを検証しなければならない (shall)。また評価者は操作ガイダンスをレビューして、TSS 中の記述に準拠するように TOE を構成することに関する指示が含まれることを保証しなければならない (shall)。

評価者は、ContentEncryptionAlgorithmIdentifier について、そして要求されるふるまいがデフォルトで実施されるのか構成され得るのかのどちらであるか、TSS に記述されていることを検証しなければならない (shall)。本要件を満たすためにはアルゴリズムが構成されなければならない (must) ことが TSS に示されている場合、評価者は AGD ガイダンスに本 ID の構成が含まれていることを検証しなければならない (shall)。

評価者は、digestAlgorithm について、そして要求されるふるまいがデフォルトで実施されるのか構成され得るのかのどちらであるか、TSS に記述されていることを検証しなければならない (shall)。本要件を満たすためにはアルゴリズムが構成されなければならない

(must) ことが TSS に示されている場合、評価者は AGD ガイダンスにその構成が含まれていることを検証しなければならない (shall)。

評価者は、AlgorithmIdentifier について、そして要求されるふるまいがデフォルトで実施されるのか構成され得るのかのどちらであるか、TSS に記述されていることを検証しなければならない (shall)。本要件を満たすためにはアルゴリズムが構成されなければならない (must) ことが TSS に示されている場合、評価者は AGD ガイダンスに本 ID の構成が含まれていることを検証しなければならない (shall)。

評価者は、CRL と証明書の両方に関する取り込みメカニズムと、これらのメカニズムが実行される頻度が TSS に記述されていることを検証しなければならない (shall)。メカニズムが構成可能であることが TSS に示されている場合、評価者は AGD ガイダンスにこれらのメカニズムの構成が含まれていることを検証しなければならない (shall)。

評価者は、以下のテストを実行しなければならない (shall)。

これらのテストは、証明書/証明書連鎖の検証に関して FIA_X509 に定義されるテストと組み合わせて行うことができる。

テスト 1 : 評価者は、保護なし (署名も暗号化もなし) でメッセージの送信と受信を行って、そのメッセージが適切に送信され、受信側のエージェントで閲覧できることを検証しなければならない (shall)。この送信は、さまざまなメカニズムの一部として行うことができる。メッセージが意図された受信者へ、送信時と同一の内容で到達することを確認すれば十分である。

テスト 2 : 評価者は、要件に対応して ST に規定されたアルゴリズムのそれぞれを用いて、署名されたメッセージの送信と受信を実行しなければならない (shall)。加えて、評価者は中間者ツールを用いてメッセージの少なくとも 1 バイトを改変し、署名がもはや有効でないようにしなければならない (shall)。これは、署名が計算される対象のメッセージの内容を改変することにより、あるいは署名そのものを改変することにより、行うことができる。評価者は、受信されたメッセージが署名検証チェックに失敗することを検証しなければならない (shall)。

テスト 3 : 評価者は、ST に規定されたアルゴリズムのそれぞれを用いて、暗号化されたメッセージの送信と受信を実行しなければならない (shall)。S/MIME は、エンドツーエンドのセキュリティを意図している。その結果として、第三者に電子メールを検査させると共にセキュアなエンドツーエンド通信を行うことは不可能である。したがって、適切な実装と暗号スイートを判断するために暗号化されたトラフィックを検査する必要はない。加えて、評価者は中間者ツールを用いてメッセージの少なくとも 1 バイトを改変し、暗号化がもはや有効でないようにしなければならない (shall)。評価者は、受信されたメッセージが復号に失敗することを検証しなければならない (shall)。

テスト 4 : 評価者は、署名と暗号化の両方が行われたメッセージの送信と受信の両方を実行しなければならない (shall)。本要件の意図を満たすため、暗号化されたトラフィックを検査する必要はない。加えて、評価者は中間者ツールを用いてメッセージの少なくとも 1 バイトを改変し、暗号化と署名がもはや有効でないようにしなければならない (shall)。評価者は、受信されたメッセージが復号に失敗すること、署名検証チェックに失敗すること、あるいはその両方であることを検証しなければならない (shall)。

テスト 5 : 評価者は、digestAlgorithm ID にしたがえばサポートされない署名アルゴリズム (例えば、SHA1) を用いて署名されたメッセージを TOE へ送信しなければならない (shall)。評価者は、そのメッセージを TOE が受け入れないことを検証しなければならない (shall)。

テスト 6 : 評価者は、AlgorithmIdentifier フィールドにしたがえばサポートされない暗号アルゴリズムを用いて暗号化されたメッセージを TOE へ送信しなければならない (shall)。評

価者は、そのメッセージを TOE が受け入れないことを検証しなければならない (shall)。

テスト 7 : 評価者は、digitalSignature ビットがセットされていない証明書により署名されたメッセージを TOE へ送信しなければならない (shall)。評価者は、TOE が利用者へ署名が無効であると通知することを検証しなければならない (shall)。

テスト 8 : 評価者は、extendedKeyUsage に電子メール保護が含まれない証明書により署名されたメッセージを TOE へ送信しなければならない (shall)。評価者は、TOE が利用者へ署名が無効であると通知することを検証しなければならない (shall)。

4.3.1.5　トランスポート層セキュリティ (TLS)

FCS_TLSC_EXT.1.1 [選択：TSF、TOE プラットフォーム] は、以下の暗号スイートをサポートして TLS 1.2 (RFC 5246) を実装しなければならない (shall)：

- 必須暗号スイート：
  - RFC 3268 に定義される TLS_RSA_WITH_AES_128_CBC_SHA
  - RFC 6460 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
  - RFC 6460 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- [選択：オプションの暗号スイート：
  - RFC 3268 に定義される TLS_RSA_WITH_AES_256_CBC_SHA
  - RFC 3268 に定義される TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  - RFC 3268 に定義される TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  - RFC 4492 に定義される TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
  - RFC 4492 に定義される TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
  - RFC 4492 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
  - RFC 4492 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
  - RFC 5246 に定義される TLS_RSA_WITH_AES_128_CBC_SHA256
  - RFC 5246 に定義される TLS_RSA_WITH_AES_256_CBC_ SHA256
  - RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256
  - RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256
  - RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - その他の暗号スイートなし]]。

適用上の注意：評価される構成においてテストされるべき暗号スイートは、本要件により制限される。ST 作成者は、サポートされるオプションの暗号スイートを選択すべきである (should)。必須スイート以外にサポートされる暗号スイートが存在しない場合には、「なし」が選択されるべきである (should)。テスト環境中のサーバ上で評価される構成において管理的に用いられることが可能な暗号スイートを制限することは必要である。上に列挙した Suite B アルゴリズム (RFC 6460) は、実装に望ましいアルゴリズムである。TLS_RSA_WITH_AES_128_CBC_SHA は、RFC 5246 との適合を確実にするため要求されている。

FCS_TLSC_EXT.1.2 [選択：TSF、TOE プラットフォーム] は、証明書に含まれる識別名

(DN) がピアに期待される DN にマッチしない場合、高信頼チャネルを確立してはならない (shall not)。

適用上の注意 : DN は、証明書の Subject Name フィールドまたは Subject Alternative Name 拡張に存在し得る。期待される DN は、構成されてもよいし、あるいはピアにより用いられるドメイン名または IP アドレスと比較されてもよい。

高信頼通信チャネルには、TSF により実施される TLS、HTTPS、または S/MIME のいずれかが含まれる。高信頼チャネルを確立するための有効性チェックは、FIA_X509_EXT.1 と組み合わせて行われる。

FCS_TLSC_EXT.1.3 [選択：TSF、TOE プラットフォーム] は、Client Hello 中の signature_algorithm 拡張に以下のハッシュアルゴリズムを提示しなければならない (shall)： [選択：SHA256、SHA384、SHA512] 及びその他のハッシュアルゴリズムなし。

適用上の注意：本要件は、クライアントによるデジタル署名検証の目的でサポートされるハッシュアルゴリズムを制限すると共に、サーバによるデジタル署名生成の目的でサポートされるハッシュにサーバを制限する。signature_algorithm 拡張は、TLS 1.2 のみによりサポートされる。

FCS_TLSC_EXT.1.4 [選択：TSF、TOE プラットフォーム] は、Client Hello 中の Supported Elliptic Curves Extension 拡張に以下の NIST 曲線を提示しなければならない (shall)： [選択：secp256r1、secp384r1、secp521r1] 及びその他の曲線なし。

適用上の注意：本要件は、認証及び鍵共有のために許可される楕円曲線を、**FCS_COP.1(3)** 及び **FCS_CKM.1(1)** ならびに **FCS_CKM.1(2)** からの NIST 曲線に制限する。本拡張は、楕円曲線暗号スイートをサポートするクライアントについて要求される。

著者の注記：上記の FCS 要件の繰返しは、各 PP において異なる。これらの数字は Mobile Device PP からのものであり、デジタル署名生成/検証、鍵確立鍵生成、及び認証鍵生成の要件を示す。

保証アクティビティ：

評価者は TSS 中の本プロトコルの実装の記述をチェックして、サポートされる暗号スイートが規定されていることを保証しなければならない (shall)。評価者は TSS をチェックして、規定された暗号スイートが本コンポーネントに列挙されたものを含むことを保証しなければならない (shall)。また評価者は操作ガイダンスをチェックして、TLS が TSS 中の記述と適合するように TOE を構成することに関する指示が含まれることを保証しなければならない (shall)。

評価者は、証明書中の DN が期待される DN と比較される方法が TSS に記述されていることを検証しなければならない (shall)。DN が自動的にドメイン名や IP アドレスと比較されない場合、評価者はその接続に期待される DN の構成が AGD ガイダンスに含まれることを保証しなければならない (shall)。

評価者は、signature_algorithm 拡張について、そして要求されるふるまいがデフォルトで実施されるのか構成され得るのかのどちらであるか、TSS に記述されていることを検証しなければならない (shall)。本要件を満たすためには signature_algorithm 拡張が構成されなければならない (must) ことが TSS に示されている場合、評価者は AGD ガイダンスに signature_algorithm 拡張の構成が含まれることを検証しなければならない (shall)。

評価者は、Supported Elliptic Curves 拡張について、そして要求されるふるまいがデフォルトで実施されるのか構成され得るのかのどちらであるか、TSS に記述されていることを検証しなければならない (shall)。本要件を満たすためには Supported Elliptic Curves 拡張が構成されなければならない (must) ことが TSS に示されている場合、評価者は AGD ガイダン

スに Supported Elliptic Curves 拡張の構成が含まれることを検証しなければならない (shall)。

また評価者は、以下のテストを実行しなければならない (shall)。

- テスト 1 : 評価者は、要件に規定された暗号スイートのそれぞれを用いて、TLS 接続を確立しなければならない (shall)。この接続は、より高位のプロトコルの確立の一部として確立されてもよい (例えば、EAP セッションの一部として)。テストの意図を満たすには、暗号スイートのネゴシエーション成功を確認すれば十分であり、利用されている暗号スイート (例えば、暗号アルゴリズムが 128 ビット AES であって 256 ビット AES でないこと) を識別するために暗号化されたトラフィックの特徴を検査する必要はない。
- テスト 2 : 評価者は、extendedKeyUsage フィールド中にサーバ認証目的を含むサーバ証明書を持ったサーバを用いて接続を確立する試行を行い、接続が確立されることを検証しなければならない (shall)。次に評価者は、extendedKeyUsage フィールド中にサーバ認証目的を含まないこと以外は有効なサーバ証明書をクライアントが拒否し、接続が確立されないことを検証する。理想的には、2 つの証明書は extendedKeyUsage フィールドを除いて同一であるべきである (should)。
- テスト 3 : 評価者は、構成された期待される DN またはピアのドメイン名／IP アドレスのいずれかに DN がマッチする証明書による接続を試行しなければならない (shall)。評価者は、TSF が接続を成功できることを検証しなければならない (shall)。評価者は、構成された期待される DN またはピアのドメイン名／IP アドレスのいずれにも DN がマッチしない証明書による接続を試行しなければならない (shall)。評価者は、TOE が接続を成功できないことを検証しなければならない (shall)。接続の失敗を示す利用者通知は、FIA_X509_EXT.2.3 にしたがって受容可能である。
- テスト 4 : 評価者は、TLS 接続中にクライアントの signature_algorithm 拡張にしたがえばサポートされない証明書を送信する (例えば、SHA-1 署名を持つ証明書を送信する) ようにサーバを構成しなければならない (shall)。評価者は、TOE が ServerCertificate ハンドシェイクメッセージを受信した後に切断することを検証しなければならない (shall) 。
- テスト 5 : 評価者は、サポートされない曲線 (例えば P-192) を用いて ECDHE 鍵交換を行うようサーバを構成しなければならず (shall)、そして TOE が ServerKeyExchange ハンドシェイクメッセージを受信した後に切断することを検証しなければならない (shall) 。
- テスト 6 : 評価者は、サーバにより選択された暗号スイートとマッチしない証明書を TLS 接続中に送信する (例えば、TLS_RSA_WITH_AES_128_CBC_SHA 暗号スイートを利用しているのに ECDSA 証明書を送信したり、ECDSA 暗号スイートのいずれかを使用しているのに RSA 証明書を送信したりする) ようサーバを構成しなければならない (shall)。評価者は、TOE が ServerCertificate ハンドシェイクメッセージを受信した後に切断することを検証しなければならない (shall) 。
- テスト 7 : 評価者は、TLS_NULL_WITH_NULL_NULL 暗号スイートを選択するようサーバを構成し、クライアントが接続を拒否することを検証しなければならない (shall)。
- テスト 8 : 評価者は、TOE とサーバとの間に中間者ツールを設定しなければならず (shall)、またトラフィックに以下の改変を実行しなければならない (shall)。
    - ServerHello 中のサーバにより選択される TLS バージョンを、サポートされない TLS バージョン (例えば 03 04 の 2 バイトにより表現される 1.3) に変更し、クライアントが接続を拒否することを検証する。

- ServerHello ハンドシェイクメッセージ中のサーバのノンス中の少なくとも 1 バイトを改変して、ServerKeyExchange ハンドシェイクメッセージをクライアントが拒否すること (DHE または ECDHE 暗号スイートの場合) またはクライアントの Finished ハンドシェイクメッセージをサーバが拒否すること検証する。
- ServerHello ハンドシェイクメッセージ中のサーバの選択された暗号スイートを、ClientHello ハンドシェイクメッセージ中に提示されない暗号スイートに改変する。評価者は、クライアントが ServerHello の受信後に接続を拒否することを検証しなければならない (shall) 。
- サーバの KeyExchange ハンドシェイクメッセージ中の署名ブロックを改変して、クライアントが ServerKeyExchange の受信後に接続を拒否することを検証する。
- 相互認証を要求するようサーバを構成し、次にサーバの CertificateRequest ハンドシェイクメッセージ中の CA フィールド中の 1 バイトを改変する。改変された CA フィールドは、クライアントの証明書の署名に用いられた CA であってはならない (must not)。評価者は、サーバがクライアントの Finished ハンドシェイクメッセージを受信した後に接続を拒否することを検証しなければならない (shall) 。
- サーバの Finished ハンドシェイクメッセージの 1 バイトを改変して、受信後にクライアントが fatal alert を送信しアプリケーションデータを全く送信しないことを検証する。
- クライアントが ChangeCipherSpec メッセージを発行した後にサーバから暗号化されていないパケットを送信し、クライアントが接続を拒否することを検証する。

4.3.2 クラス：識別と認証 (FIA)

4.3.2.1 S/MIME

FIA_SMIME_EXT.1.1 [選択：TSF、TOE プラットフォーム] は、FCS_SMIME_EXT.1 に定義された暗号アルゴリズムを用いてのみ、メッセージを送信/受信しなければならない (shall)。TSF は、より弱いアルゴリズムが暗号化に用いられることを許可してはならない (shall not)。

適用上の注意：*S/MIME v.3.2 はデフォルトのアルゴリズムを要求するが、これらのデフォルトのアルゴリズムは本 PP により要求されるものよりもかなり弱い。本要件は、クライアントの評価される構成ではこれらのより弱いアルゴリズムが無効化されなければならない (must) ことを示している。*

保証アクティビティ：

本要件と関連付けられた TSS の記述と操作ガイダンスは、FCS_SMIME_EXT.1 と組み合わせて行われる。

評価者は、以下のテストを実行しなければならない (shall)。

テスト 1：評価者は、許可されないアルゴリズムにより署名及び暗号化されたメッセージのクライアントへの送信を試行しなければならず (shall)、またクライアントがそのメッセージを拒否することを検証しなければならない (shall)。

4.3.2.2 SASL

FIA_SASL_EXT.1.1 [選択：TSF、TOE プラットフォーム] は、RFC 4422 に準拠する Simple Authentication and Security Layer (SASL) のサポートを実装しなければならない (shall)。

保証アクティビティ：

評価者は、SASL 接続の観点からメールユーザエージェント及びメール転送エージェントへ

の TOE の接続の詳細と、仕様中に反映されていない可能性のある TOE 特有のオプションまたは手続きが記述されていることを決定するため、TSS を検査しなければならない (shall)。

評価者は、メールユーザエージェント及びメール転送エージェントへの接続を確立するための指示が操作ガイダンスに含まれていることを確認しなければならない (shall)。また評価者は、以下のテストを実行しなければならない (shall)。

テスト 1 : 評価者は、操作ガイダンスに記述されたように接続を設定し通信が成功することを保証することにより、TOE が要件中に規定された POP、IMAP、及び任意の割り付けられたプロトコルを用いてメールユーザエージェントとの通信を開始できることを保証しなければならない (shall)。

テスト 2 : 評価者は、SASL ハンドシェイクが行われ成功することを検証しなければならない (shall)。本テストを行うために、評価者はスニファ及びパケットアナライザを使用しなければならない (shall)。パケットアナライザにより、使用されているプロトコルが SASL であることが示されなければならない (must)。

FIA_SASL_EXT.1.2 [選択：TSF、TOE プラットフォーム] は、SASL メカニズムのための POP3 CAPA 及び AUTH 拡張をサポートしなければならない (must)。

FIA_SASL_EXT.1.3 [選択：TSF、TOE プラットフォーム] は、SASL メカニズムのための IMAP CAPABILITY 及び AUTHENTICATE 拡張をサポートしなければならない (must)。

FIA_SASL_EXT.1.4 [選択：TSF、TOE プラットフォーム] は、SASL メカニズムのための SMTP AUTH 拡張をサポートしなければならない (must)。

適用上の注意：*本文書において要求される POP3、IMAP 及び SMTP 向けの PKI X.509 証明書を電子メールクライアントがサポートするためには、そのクライアントは RFC 4422 に記述される Simple Authentication and Security Layer (SASL) 認証手法、RFC 5043 に記述される POP3 の AUTH 及び CAPA 拡張、RFC 4959 に記述される IMAP の AUTHENTICATION 及び CAPABILITY 拡張、ならびに RFC 4954 に記述される SMTP の AUTH 拡張をサポートしなければならない (must)。*

保証アクティビティ：

評価者は、SASL 接続の観点からメールユーザエージェント及びメール転送エージェントへの TOE の接続の詳細と、仕様中に反映されていない可能性のある TOE 特有のオプションまたは手続きが記述されていることを決定するため、TSS を検査しなければならない (shall)。

評価者は、メールユーザエージェント及びメール転送エージェントへの接続を確立するための指示が操作ガイダンスに含まれていることを確認しなければならない (shall)。また評価者は、以下のテストを実行しなければならない (shall)。

テスト 1 : 評価者は、操作ガイダンスに記述されたように接続を設定し通信が成功することを保証することにより、TOE が POP、IMAP 及び SMTP を用い、SASL を要求して、メールユーザエージェントとの通信を開始できることを保証しなければならない (shall)。

テスト 2 : 評価者は、テスト 1 における正当な IT エンティティとの通信チャネルのそれぞれについて、有効な SASL ハンドシェイクが行われることを保証しなければならない (shall)。本テストを行うために、評価者はスニファ及びパケットアナライザを使用しなければならない (shall)。パケットアナライザにより、使用されているプロトコルが SASL であることが示されなければならない (must)。

4.3.2.3　X.509 有効性確認

FIA_X509_EXT.1 拡張：X509 有効性確認

FIA_X509_EXT.1.1 [選択：*TSF*、*TOE プラットフォーム*] は、以下のルールにしたがって証明書の有効性を確認しなければならない (shall)：

- RFC 5280 証明書有効性確認及び認証パス検証。
- TSF は、すべての CA 証明書について、basicConstraints 拡張の存在と cA フラグが TRUE にセットされていることを保証することにより、認証パスを検証しなければならない (shall)。
- TSF は、RFC 5759 に規定される証明書失効リスト (CRL) 及び [選択：*RFC 2560 に規定されるオンライン証明書状態プロトコル (OCSP)*、*その他の失効状態チェックメカニズムなし*] を用いて証明書の失効状態を検証しなければならない (shall)。
- TSF は、以下のルールにしたがって extendedKeyUsage フィールドを検証しなければならない (shall)。
    - 高信頼アップデート及び実行可能コードの完全性検証に用いられる証明書は、コード署名目的 (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) を持たなければならない (shall)。
    - TLS に提示されるサーバ証明書は、extendedKeyUsage フィールドにサーバ認証目的 (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) を持たなければならない (shall)。
    - 電子メールの暗号化及び署名に提示される S/MIME 証明書は、extendedKeyUsage フィールドに電子メール保護目的 (id-kp 4 with OID 1.3.6.1.5.5.7.3.4) を持たなければならない (shall)。

適用上の注意：

FIA_X509_EXT.1.1 には、証明書有効性確認を行うためのルールが列挙されている。ST 作成者は、失効状態が OCSP か CRL のどちらを用いて検証されるか選択しなければならない (shall)。証明書は、TOE の高信頼アップデートのため (FPT_TUD_EXT.1.3) 及びプラグインや拡張機能のインストールのため (FPT_TUD_EXT.1.2) にオプションとして用いてもよく、また TOE により実装されている場合には、コード署名目的 extendedKeyUsage を含むことが検証されなければならない (must)。FCS_TLSC_EXT.1 を用いたウェブサーバとの認証を行うには証明書が利用されなければならず (must)、また証明書にサーバ認証目的 extendedKeyUsage が含まれることが検証されなければならない (must)。FCS_SMIME_EXT.1 を用いた S/MIME 電子メール暗号化及び署名には証明書が利用されなければならず (must)、また証明書に電子メール保護目的 extendedKeyUsage が含まれることが検証されなければならない (must)。

TSF あるいは TOE プラットフォームの選択にかかわらず、証明書の有効性確認はプラットフォームにより管理されるルートストア中の信頼済みルート証明書に至ることが期待される。

FIA_X509_EXT.1.1 は TOE プラットフォームに、TLS サーバにより提示される証明書に関して一定のチェックを行うことを要求しているが、クライアントにより提示される証明書に関してサーバが実行しなければならない (have to) これに対応するチェックも存在する。すなわち、クライアント証明書の extendedKeyUsage フィールドに "Client Authentication" が含まれ、デジタル署名ビットがセットされ、また鍵共有 (key agreement) ビット (Diffie-Hellman 暗号スイートの場合) または鍵暗号化 (key encipherment) ビット (RSA 暗号スイートの場合) がセットされていることである。TOE による使用のため取得される証明書がエンタープライズ内で使用されるためには、これらの要件に適合しなければならない (have to)。

FIA_X509_EXT.1.1 は TOE プラットフォームに、S/MIME のため提示される証明書に関して一定のチェックを行うことを要求しているが、クライアントにより提示される証明書に関して送信者/受信者が実行しなければならない (have to) これに対応するチェックも存在する。すなわち、クライアント証明書の extendedKeyUsage フィールドに "Email Protection" が含まれ、(S/MIME 署名向けの) デジタル署名ビットがセットされ、また鍵共有 (key agreement) ビット (Diffie-Hellman 暗号スイートの場合) または鍵暗号化 (key encipherment) ビット (RSA 暗号スイートの場合) がセットされていることである。TOE による使用のため取得される証明書がエンタープライズ内で使用されるためには、これらの要件に適合しなければならない (have to)。

FIA_X509_EXT.1.2 [選択：*TSF*、*TOE プラットフォーム*] は、basicConstraints 拡張が存在し CA フラグが TRUE にセットされている場合にのみ、証明書を CA 証明書として取り扱わなければならない (shall)。

適用上の注意：

本要件は、電子メールクライアントまたはプラットフォームにより用いられ処理される証明書に適用される。

保証アクティビティ：

評価者は、どこで証明書の有効性のチェックが行われるか TSS に記述されていることを保証しなければならない (shall)。また評価者は、認証パス検証アルゴリズムの記述も TSS に提供されていることも確認する。

記述されるテストは、FIA_X509_EXT.2.1 中の使用事例を含め、他の証明書サービス保証アクティビティと組み合わせて行われなければならない (must)。extendedKeyUsage ルールのテストは、これらのルールを要求する用途と組み合わせて行われる。

テスト 1：評価者は、有効な認証パスのない証明書の有効性確認を行うと、その機能 (アプリケーションの検証、高信頼チャネルの設定、あるいは高信頼ソフトウェアアップデート) が失敗することを例証しなければならない (shall)。次に評価者は、その機能で使われる証明書の検証に必要とされる 1 つまたは複数の証明書をロードし、その機能が成功することを例証しなければならない (shall)。次に評価者は、これらの証明書の 1 つを削除して、その機能が失敗することを示さなければならない (shall)。

テスト 2：評価者は、有効期限を過ぎた証明書の有効性確認を行うと、その機能が失敗することを例証しなければならない (shall)。

テスト 3：評価者は、CRL と OCSP のどちらが選択されているかに応じて、TOE が失効した証明書を適切に処理できることをテストしなければならない (shall)。両方とも選択されている場合には、それぞれの手法についてテストが行われる。評価者は信頼の連鎖の 1 つ上位のみをテストする必要がある (将来の版では、上位の連鎖全体について検証が行われることを保証することが要求されるかもしれない)。評価者は、有効な証明書が用いられること、そして証明書有効性確認機能が成功することを保証しなければならない (shall)。次に評価者は、失効するはずの証明書 (選択において選択された手法のそれぞれについて) を用いてテストを試行し、もはや証明書が有効ではない場合には証明書有効性確認機能が失敗することを保証する。

テスト 4：評価者は、TOE の証明書を発行する CA の証明書に basicConstraints 拡張が含まれないような認証パスを構築しなければならない (shall)。この認証パスの検証は失敗する。

テスト 5：評価者は、TOE の証明書を発行する CA の証明書の basicConstraints 拡張中の cA フラグがセットされていないような認証パスを構築しなければならない (shall)。この認証パスの検証は失敗する。

テスト 6：評価者は、TOE の証明書を発行する CA の証明書の basicConstraints 拡張中の cA フラグが TRUE にセットされているような認証パスを構築しなければならない (shall)。この認証パスの検証は成功する。

テスト 7：評価者は、証明書の中間のバイトを 1 つだけ改変し、その証明書の有効性確認が失敗することを例証しなければならない (shall)。

4.3.2.4　X.509 認証及び暗号化

FIA_X509_EXT.2 拡張：X509 認証及び暗号化

FIA_X509_EXT.2.1(1) [選択：*TSF*、*TOE プラットフォーム*] は、RFC 5280 に定義される X.509v3 証明書を用いて TLS 接続の認証をサポートしなければならない (shall)。

FIA_X509_EXT.2.1(2) [選択：*TSF*、*TOE プラットフォーム*] は、RFC 5280 に定義される X.509v3 証明書を用いて S/MIME の暗号化と認証をサポートしなければならない (shall)。

FIA_X509_EXT.2.1(3) [選択：*TSF*、*TOE プラットフォーム*] は、RFC 5280 により定義される X.509v3 証明書を用いて TOE アップデートのコード署名及び [選択：*拡張機能インストールのコード署名*、*プラグインインストールのコード署名*、*追加用途なし*] をサポートしなければならない (shall)。

適用上の注意：

証明書は、TOE ソフトウェアの高信頼アップデートに用いられなければならず (must)、またプラグインや拡張機能のインストールにオプションとして用いられてもよい。

FIA_X509_EXT.2.2 [選択：*TSF*、*TOE プラットフォーム*] が証明書の有効性を判断する接続を確立できないとき、[選択：*TSF*、*TOE プラットフォーム*] は [選択：*このような場合には証明書を受容するかどうかの選択を管理者に許可する*、*証明書を受容する*、*証明書を受容しない*] ようにしなければならない (shall)。

適用上の注意：

CRL のダウンロードにせよ、OCSP の実行にせよ、証明書の失効状態の検証を行うために接続を確立しなければならない (must) 場合は多々生ずる。この選択は、そのような接続が確立できない場合 (例えば、ネットワークエラーのため) のふるまいを記述するために用いられる。TOE が、証明書は FIA_X509_EXT.1 中の他の全てのルールにしたがって有効であると判断した場合、2 番目の選択に示されるふるまいにより有効性が判断されなければならない (shall)。証明書が FIA_X509_EXT.1 中の他の有効性確認ルールのいずれかに失敗する場合、TOE はその証明書を受容してはならない (must not)。ST 作成者により管理者構成オプションが選択された場合、ST 作成者は FMT_SMF.1 中の機能 10 もまた選択しなければならない (must)。

FIA_X509_EXT.2.3 [選択：*TSF*、*TOE プラットフォーム*] は、ピア証明書が無効とみなされる場合には高信頼チャネルを確立してはならない (shall not)。

適用上の注意：

高信頼通信チャネルには、TSF により実施される TLS のいずれかが含まれる。有効性は認証パス、有効期限、及び RFC 5280 にしたがう失効状態により判断される。

FIA_X509_EXT.2.4 [選択：TSF、TOE プラットフォーム] は、コード署名証明書が無効とみなされる場合にはそのコードをインストールしてはならない (shall not)。

適用上の注意：

証明書は、システムソフトウェアの高信頼アップデート (FPT_TUD_EXT.1.3) にオプションとして用いてもよい。

FIA_X509_EXT.2.5 [選択：TSF、TOE プラットフォーム] は、電子メール保護証明書が無効とみなされる場合には電子メールを暗号化してはならない (shall not)。

FIA_X509_EXT.2.6 [選択：TSF、TOE プラットフォーム] は、電子メールが無効な証明書で署名されている場合には利用者へ通知しなければならない (shall)。

保証アクティビティ：

評価者は TSS をチェックして、TOE がどの証明書を利用するか選ぶ方法が記述されていること、及び TOE がその証明書を利用できるように運用環境を構成するために必要な指示があれば、それが管理ガイダンスに記述されていることを保証しなければならない (shall)。

評価者は、高信頼チャネルの確立及び電子メールの保護に用いられる証明書の有効性確認中に接続が確立できなかった際の TOE のふるまいが記述されていることを確認するため、TSS を検査しなければならない (shall)。管理者がデフォルトのアクションを規定できるという要件が存在する場合には、この構成アクションを行う方法に関する指示が操作ガイダンスに含まれていることを評価者は保証しなければならない (shall)。

評価者は、証明書の使用を要求する FIA_X509_EXT.2.1 に列挙される機能のそれぞれについて、テスト 1 を実行しなければならない (shall)。

テスト 1：評価者は、有効な認証パスのない証明書を使用すると、その機能が失敗するか、利用者通知が受領されることを例証しなければならない (shall) (エレメント 3、4、5、及び 6 により要求されるように)。次に評価者は、その機能で使われる証明書の検証に必要とされる任意の証明書をプラットフォームのルートストアへロードし、その機能が成功するか、利用者通知に至らないことを例証しなければならない (shall)。

テスト 2：評価者は、TOE 以外の IT エンティティとの通信により、有効な証明書の使用には少なくとも一部の証明書有効性確認のチェック実行が必要とされることを例証しなければならない (shall)。次に評価者は、TOE が証明書の有効性を検証できないように環境を操作し、FIA_X509_EXT.2.2 で選択されたアクションが行われることを確認しなければならない (shall)。選択されたアクションが管理者により構成可能である場合には、評価者は操作ガイダンスにしたがって、サポートされているすべての管理者構成可能オプションが、文書化されているようにふるまうことを判断しなければならない (shall)。

4.3.3 クラス：セキュリティ管理 (FMT)

4.3.3.1 TSF 内の機能の管理

FMT_MOF.1.1(1) TSF 及び [選択：TOE プラットフォーム、その他のメカニズムなし] は、以下の

1. 埋め込みオブジェクトのダウンロードをグローバルに、及び [選択：ドメインにより、送信者により、その他の手法なし] 有効化/無効化する
2. プレーンテキストのみのモードをグローバルに、及び [選択：ドメインにより、送信者により、その他の手法なし] 有効化/無効化する
3. 添付の表示及び実行をグローバルに、及び [選択：ドメインにより、送信者により、その他の手法なし] 有効化/無効化する

[選択：

4. 電子メール通知を有効化/無効化する、
5. S/MIME 利用向けに証明書を構成する、
6. TLS 利用向けに証明書を構成する、

7. 電子メール通知中の電子メールの内容の表示を有効化/無効化する、
8. 暗号化向けに証明書リポジトリを構成する、
9. TSF が証明書の有効性を判断するための接続を確立できなかった場合に高信頼チャネルを確立するか、あるいは確立を禁止するかを構成する、
10. その他の管理機能なし]

機能を行う能力を、管理ポリシーにしたがって管理者に制限しなければならない (shall)。

適用上の注意：*管理者は、エンタープライズにより電子メールクライアントへ適用されるポリシーの設定を含めた、管理アクティビティに責任を負う。この管理者はリモートから操作を行うと考えられ、また集中化された管理コンソールまたはダッシュボードを介して操作を行う MTA 管理者であるかもしれない。*

本要件の意図は、利用者により上書きされ得ないポリシーにより TOE を構成することを管理者に可能とすることである。管理者が特定の機能向けのポリシーを設定しなかった場合、利用者は依然としてその機能を実行し得る。ポリシーの強制は TOE そのものにより、あるいは TOE と TOE プラットフォームが互いに協調して行われる。

FIA_X509_EXT.2.2 による機能 #9 に関して管理者には、検証できない証明書をすべて受容または拒否する、検証できない特定の証明書を受容する、あるいは検証できない特定の証明書を受容しないという選択肢がある。FIA_X509_EXT.2.2 において管理者が行った選択により、高信頼接続は検証できない証明書についてすべて許可されるか、検証できない証明書についてすべて許可されないか、検証できない特定の証明書について許可されるか、あるいは検証できない特定の証明書について許可されないかのいずれかとなる。

保証アクティビティ：

評価者は、以下のテストを実行しなければならない (shall)。

テスト 1：評価者は、テスト環境を用いて電子メールクライアントへポリシーを展開しなければならない (shall)。

テスト 2：評価者は、FMT_MOF.1.1(2) に定義される (エンタープライズ) 管理者によりコントロールされ、利用者により上書きできない、すべての管理機能を一括して含むポリシーを作成しなければならない (shall)。評価者はクライアントへこれらのポリシーを適用し、利用者として各設定の上書きを試行し、そして TSF がこれを許可しないことを保証しなければならない (shall)。

4.3.3.2　管理機能の仕様

FMT_SMF.1.1 TSF 及び [選択：TOE プラットフォーム、その他のメカニズムなし] は、以下の管理機能を行えなければならない (shall)。

1. 電子メール通知を有効化/無効化する
2. 埋め込みオブジェクトのダウンロードをグローバルに、及び [選択：ドメインにより、送信者により、その他の手法なし] 有効化/無効化する
3. プレーンテキストモードをグローバルに、及び [選択：ドメインにより、送信者により、その他の手法なし] 有効化/無効化する
4. 添付の表示及び実行をグローバルに、及び [選択：ドメインにより、送信者により、その他の手法なし] 有効化/無効化する
5. S/MIME 利用向けに証明書を構成する
6. エンタープライズにわたって電子メールを S/MIME で自動的に署名する選択肢を構

成する

7. エンタープライズにわたって電子メールを S/MIME で自動的に暗号化する選択肢を構成する
8. TLS 利用向けに証明書を構成する

[選択：

9. 電子メール通知中の電子メールの内容の表示を有効化/無効化する
10. 暗号化向けに証明書リポジトリを構成する。
11. TSF が証明書の有効性を判断するための接続を確立できなかった場合に高信頼チャネルを確立するか、あるいは確立を禁止するかを構成する、
12. その他の管理機能なし]

適用上の注意：*上記の管理機能は、セキュリティ管理機能を規定するものである。*

管理機能 3、4、及び 5 は、クライアントにより処理される電子メール向けのグローバルなルールとして構成されなければならない (must) が、ドメインごと、または送信者ごとに設定されてもよい。

埋め込みオブジェクトの管理には、すべての HTML 及び JavaScript 内容が含まれなければならない (must)。

プレーンテキストモードは、埋め込みオブジェクトの表示及び実行を無効化する。

証明書リポジトリは、FDP_SMIME_EXT.1.2 にしたがいプラットフォームにより、または TOE により管理され得る。証明書リポジトリが TOE により管理される場合、機能 10 が ST に含まれなければならない (must)。証明書リポジトリは、ローカルであってもリモートであってもよい。リモート証明書リポジトリは、例えば LDAP サービスが実行されているような、ディレクトリサーバである。したがって、リモート証明書リポジトリの構成には、サーバへの接続情報を提供することが必要となる。

管理者による構成の選択が FIA_X509_EXT.2.2 においてなされている場合には、機能 11 が含まれなければならない (must)。つまり、FIA_X509_EXT.2.2 により管理者には、検証できない証明書をすべて受容または拒否する、検証できない特定の証明書を受容する、あるいは検証できない特定の証明書を受容しないという選択肢がある。FIA_X509_EXT.2.2 において管理者が行った選択により、高信頼接続は検証できない証明書についてすべて許可されるか、検証できない証明書についてすべて許可されないか、検証できない特定の証明書について許可されるか、あるいは検証できない特定の証明書について許可されないかのいずれかとなる。

保証アクティビティ：

評価者は、TSS に各機能が記述され、また利用者か管理者かあるいはその両方がその管理機能を行い得るのか示されていることを検証しなければならない (shall)。

評価者は AGD ガイダンスを参照して以下のテストのそれぞれを行い、利用者及び管理者の両方がその機能を行い得る場合には各テストを繰返さなければならない (shall)。以下のテスト番号は、機能番号に対応する。

テスト 1 : 評価者は電子メール通知を有効化し、FDP_NOT_EXT.1 のテストと組み合わせて通知が起こることを検証しなければならない (shall)。次に評価者は電子メール通知を無効化し、クライアントへ電子メールを送信し、そして通知が起こらないことを検証しなければならない (shall)。

テスト 2 : 評価者はクライアントへ、外部サーバからのダウンロードを要求する埋め込みオブジェクト (例えば、画像) を含むメールを送信し、ダウンロードが有効化されている場合に画像がダウンロードされることを検証しなければならない (shall)。次に評価者はダウンロードを無効化し、再度電子メールを送信し、そしてオブジェクトがダウンロードされないことを検証しなければならない (shall)。

テスト 3 : 本機能のテストは、FDP_REN_EXT.1.1 と組み合わせて行われる。

テスト 4 : 評価者は、TOE に画像添付ファイルを送信し、それが表示されることを検証しなければならない (shall)。次に評価者は表示を無効化し、画像が表示されないことを検証しなければならない (shall)。評価者は、TOE に実行可能な添付ファイルを送信し、それが実行され得ることを検証しなければならない (shall)。評価者は添付ファイルの実行を無効化し、その後その添付ファイルが実行できないことを検証しなければならない (shall)。

テスト 5 : 評価者は、S/MIME とともに使われるように証明書を構成しなければならず (shall)、また FCS_SMIME_EXT.1 と関連付けられたテストを実行しなければならない (shall)。評価者は証明書を削除し、メッセージの署名と復号を行うテストを繰り返し、そしてそれらが失敗することを検証しなければならない (shall)。

テスト 6 : 本機能のテストは、FCS_SMIME_EXT.1 と組み合わせて行われる。

テスト 7 : 本機能のテストは、FCS_SMIME_EXT.1 と組み合わせて行われる。

テスト 8 : 評価者は、TOE とテスト環境サーバを相互に認証された TLS を用いるよう構成しなければならず (shall)、また本目的のために TOE 上の証明書を構成しなければならない (shall)。評価者は TOE に TLS を介した通信を開始させ、接続が確立できることを検証しなければならない (shall)。評価者はパケットアナライザを用いて、構成された証明書が接続の認証に用いられることを検証しなければならない (shall)。

テスト 9 : (条件付き) 評価者は TOE に電子メールを送信し、その電子メールの内容が通知に含まれることを検証しなければならない (shall)。評価者は通知中の電子メールの内容の表示を無効化し、テストを繰り返し、そして電子メールの内容が通知に含まれないことを検証しなければならない (shall)。

10 :(条件付き) 評価者は証明書リポジトリを AGD ガイダンスに従って構成しなければならない (shall)。TOE がローカルにリポジトリを持つ場合、評価者は受信者向けの証明書をロードし、受信者への暗号化された電子メールの送信を試行し、そしてそれが成功することを検証しなければならない (shall)。次に評価者は証明書を削除し、暗号化された電子メールの送信を試行し、そしてその試行が失敗することを検証しなければならない (shall)。TOE がリモートにリポジトリを持つ場合、評価者はリモートのリポジトリを構成し、リポジトリ中の利用者へ暗号化された電子メールの送信を試行し、そしてその試行が成功することを検証しなければならない (shall)。次に評価者はリポジトリへの接続を削除し、暗号化された電子メールの送信を施行し、そしてその試行が失敗することを検証しなければならない (shall)。

テスト 11 : (条件付き) 本機能のテストは、FIA_X509_EXT.2.2 と組み合わせて行われる。

4.3.3.3　FMT_SMR.1 セキュリティ管理役割

FMT_SMR.1.1 [選択 : TOE、TOE プラットフォーム] は、以下の役割を維持管理しなければならない (shall) : *管理者*。

FMT_SMR.1.2 [選択 : TOE、TOE プラットフォーム] は、利用者を役割と関連付けることができなければならない (shall)。

保証アクティビティ :

TSS

評価者は、管理者の役割、役割に付与される権限及び役割の制限が記述されていることを検証するため、TSS 及び利用者文書を検査しなければならない (shall)。

ガイダンス

評価者は、TOE を管理するための指示とどのインタフェースがサポートされるかが含まれることを保証するため、操作ガイダンスを検査しなければならない (shall)。

テスト

評価のためテストアクティビティを実行するにあたって、評価者は、すべてのサポートされるインタフェースを利用しなければならない (shall) が、各インタフェースについて管理アクションを伴う各テストを繰り返す必要はない。しかし、評価者は、本 PP の要件に適合する TOE 管理のサポートされた手法のそれぞれがテストされることを確実にしなければならない (shall)。例えば、TOE がローカルなハードウェアインタフェースまたは TLS/HTTPS を介して管理可能な場合には、評価チームのテストアクティビティ中で両方の管理手法が行使されなければならない (must)。

4.3.4 クラス：TSF の保護 (FPT)

4.3.4.1 TSF セルフテスト

FPT_TST_EXT.1 拡張：TSF のセルフテスト

FPT_TST_EXT.1.1 [選択：TOE、TOE プラットフォーム] は、最初の起動中 (電源投入時) に一連のセルフテストを実行し、その実行可能形式及びデータの完全性を保証しなければならない (shall)。

保証アクティビティ：

TSS

評価者は、起動時に行われるセルフテストが規定されていることを保証するため、TSS を検査しなければならない (shall)。本記述には、実際に行われるテストの概要 (例えば、TOE 実行可能形式の完全性を検証する) が含まれるべきである (should)。TSS には、セルフテスト失敗の際に TSF または TOE プラットフォームが入り得る任意のエラー状態、及びそのエラー状態を抜けて通常動作を再開するために必要な条件とアクションが含まれなければならない (must)。評価者は、これらのセルフテストが起動時に自動的に実行されること、そして利用者またはオペレータからの入力やアクションは一切必要とされないことが TSS に示されていることを検証しなければならない (shall)。

ガイダンス

N/A

テスト

評価者は、以下のテストを実行しなければならない (shall)。

- テスト 1：評価者は、既知の良好な TSF 実行可能形式に関する完全性チェックを行い、そのチェックが成功することを検証しなければならない (shall)。
- テスト 2：評価者は、TSF 実行可能形式を改変し、その改変された TSF 実行可能形式に関する完全性チェックを行い、そのチェックが失敗することを検証しなければならない (shall)。
- テスト 3：評価者は、既知の良好な TOE データに関する完全性チェックを行い、そのチェックが成功することを検証しなければならない (shall)。

- テスト 4 : 評価者は、TOE 構成データを改変し、その改変された TOE データに関する完全性チェックを行い、そのチェックが失敗することを検証しなければならない (shall)。

4.3.4.2　高信頼アップデート

FPT_TUD_EXT.1 拡張 : 高信頼ソフトウェアアップデート及びパッチ

FPT_TUD_EXT.1.1 [選択 : TOE、TOE プラットフォーム] は、TOE ソフトウェア、 [選択 : 拡張機能、プラグイン、その他のアドオンなし] の現在のバージョンを問い合わせる能力を提供しなければならない (shall)。

FPT_TUD_EXT.1.2 [選択 : TOE、TOE プラットフォーム] は、TOE ソフトウェア、 [選択 : 拡張機能、プラグイン、その他のアドオンなし] のアップデート及びパッチを開始する能力を提供しなければならない (shall)。

FPT_TUD_EXT.1.3 [選択 : TOE、TOE プラットフォーム] は、TOE へのソフトウェアアップデート及びパッチ、 [選択 : 拡張機能のアップデート、プラグインのアップデート、その他のアップデートなし] の検証を、デジタル署名メカニズム及び [選択 : 公開ハッシュ、その他の機能なし] を用いて、それらのアップデート及びパッチをインストールする前に検証する手段を提供しなければならない (shall)。

FTP_TUD_EXT.1.4 [選択 : TOE、TOE プラットフォーム] は、TOE へのソフトウェアアップデート及びパッチ、 [選択 : 拡張機能、プラグイン、その他のアドオンなし] を、検証後に自動的にインストールする能力を提供しなければならない (shall)。

適用上の注意 :

3 番目のエレメントにおいて参照されているデジタル署名メカニズムは、FCS_COP.1(3) に規定されたものである。参照されている公開ハッシュは、FCS_COP.1(2) に規定された関数のいずれかにより生成される。

上記の拡張機能またはプラグインが選択される場合、附属書 C から該当する選択に基づく要件もまた ST の本体に含まれなければならない (must)。

保証アクティビティ :

TSS

TOE へのアップデートは正当なソースにより署名され、またそれと関連付けられたハッシュを持つことがある。正当なソースの定義は、アップデート検証メカニズムにより用いられる証明書がシステムへ取り込まれる方法の記述とともに、TSS 中に含まれなければならない (must)。評価者は、本情報が TSS に含まれることを保証しなければならない (shall)。

また評価者は、アップデート候補が取得される方法、アップデートのデジタル署名の検証またはアップデートのハッシュの計算に関連した処理、そして成功の (ハッシュまたは署名が検証された) 場合と不成功の (ハッシュまたは署名が検証できなかった) 場合に行われるアクションが、TSS (または操作ガイダンス) に記述されていることを保証しなければならない (shall)。これらのアクティビティが完全に基盤となるプラットフォームにより行われる場合、要求される機能が各プラットフォームについて含まれることを示す各プラットフォームの ST への参照が、評価者により検証されなければならない (shall)。

ガイダンス

評価者は、TOE ソフトウェアの現在のバージョンを検証し、TOE ソフトウェアへのアップデート及びパッチを開始し、そしてソフトウェアアップデート及びパッチの検証を構成するためのステップが文書化されていることを検証するため、操作ガイダンスを検査しなければならない (shall)。

テスト

評価者は、以下のテストを実行しなければならない (shall)。

- テスト 1 : 評価者は、バージョン検証アクティビティを行って製品の現在のバージョンを判断しなければならない (shall)。評価者は、操作ガイダンスに記述されている手順を用いて本物のアップデートを取得し、その TOE へのインストールが成功することを検証しなければならない (shall)。その後、評価者はその他の保証アクティビティテストのサブセットを行い、アップデートが期待されたとおり機能していることを例証しなければならない (shall)。アップデートの後、評価者はバージョン検証アクティビティを再び行って、そのバージョンがアップデートのものと正しく対応していることを検証しなければならない (shall)。
- テスト 2 : 評価者は、バージョン検証アクティビティを行って製品の現在のバージョンを判断しなければならない (shall)。評価者は、偽物のアップデートを取得または作成し、その TOE へのインストールを試行しなければならない (shall)。評価者は、そのアップデートを TOE が拒否することを検証しなければならない (shall)。
- テスト 3 : 評価者は、署名されていないパッチまたはアップデートのインストールを試行しなければならず (shall)、またそのアップデートが失敗することを検証しなければならない (shall)。
- テスト 4 : 評価者は、無効な証明書でパッチまたはアップデートに署名しなければならない (shall)。評価者は、そのパッチまたはアップデートのインストールを試行しなければならず (shall)、またそのアップデートが失敗することを検証しなければならない (shall)。
- テスト 5 : 評価者は、コード署名 entendedKeyUsage (訳注：extendedKeyUsage の間違いと思われる) 拡張のない、あるいは無効な証明書でパッチまたはアップデートに署名しなければならない (shall)。評価者は、そのパッチまたはアップデートのインストールを試行しなければならず (shall)、またそのアップデートが失敗することを検証しなければならない (shall)。
- テスト 6 : 評価者は、署名されたパッチまたはアップデートのインストールを試行しなければならず (shall)、またそのインストールが成功し署名が検証された後自動的に行われることを検証しなければならない (shall)。

4.3.5 クラス：高信頼パス／チャネル (FTP)

4.3.5.1 高信頼チャネル通信

FTP_ITC.1 TSF 間高信頼チャネル

FTP_ITC.1.1 [選択： TSF、TOE プラットフォーム] は、TLS を利用して、他の通信パスとは論理的に分離されているとともに、そのエンドポイントの保証された識別とチャネルデータの開示からの保護及びチャネルデータの改変の検出を提供する、それ自身と以下の能力 [選択： ディレクトリサーバ、管理構成サーバ、その他のエンティティなし] をサポートする正当な IT エンティティとの間の通信チャネルを提供しなければならない (shall)。

FTP_ITC.1.2 [選択： TSF、TOE プラットフォーム] は、TSF が高信頼チャネルを介して通信を開始することを許可しなければならない (shall)。

FTP_ ITC.1.3 [選択： TSF、TOE プラットフォーム] は、[選択： *IMAP*、*SMTP*、*POP*、*HTTP の MAPI 拡張*、*MAPI/RPC*、*ActiveSync*] について、高信頼チャネルを介して通信を開始しなければならない (shall)。

保証アクティビティ：

評価者は、TLS 接続の観点からメールユーザエージェント及びメール転送エージェントへの TOE の接続の詳細と、仕様中に反映されていない可能性のある TOE 特有のオプションまたは手続きが記述されていることを決定するため、TSS を検査しなければならない (shall)。

評価者は、メールユーザエージェント及びメール転送エージェントへの接続を確立するための指示が操作ガイダンスに含まれていることを確認しなければならない (shall)。また評価者は、以下のテストを実行しなければならない (shall)。

テスト 1 : 評価者は、操作ガイダンスに記述されたように接続を設定し通信が成功することを保証することにより、TOE が要件中に規定された POP、IMAP 及び任意の割り付けられたプロトコルを TLS 上で用いてメールユーザエージェントとの通信を開始できることを保証しなければならない (shall)。

テスト 2 : 評価者は、操作ガイダンスに記述されたように接続を設定し通信が成功することを保証することにより、TOE が要件中に規定された SMTP 及び任意の割り付けられたプロトコルを TLS 上で用いてメール転送エージェントとの通信を開始できることを保証しなければならない (shall)。

テスト 3 : 評価者は、テスト 1 及び 2 における正当な IT エンティティとの通信チャネルのそれぞれについて、チャネルデータが平文で送信されないことを保証しなければならない (shall)。本テストを行うために、評価者はスニファ及びパケットアナライザを使用しなければならない (shall)。パケットアナライザにより、使用されているプロトコルが TLS であることが示されなければならない (must)。

5 セキュリティ保証要件

セクション 5.4 (訳注: セクション 4 の間違い) 中の TOE に関するセキュリティ対策方針は、セクション 5.2 (訳注：附属書 A.2 の間違い) に特定される脅威へ対処するために構築された。セクション 4.2 のセキュリティ機能要件 (SFR) は、セキュリティ対策方針の形式的な実体化である。PP は CC からセキュリティ保証要件 (SAR) を選び出し、評価者が評価の対象となる文書を評定して独立テストを行う範囲を設定する。

本セクションには CC からの SAR の完全なセットが含まれている一方で、評価者により行われるべき保証アクティビティは本セクションと共にセクション 5.2 (訳注：セクション 4 の間違い) の両方に詳述されている。

本 PP に適合するよう作成された ST に対して、TOE の評価を行う一般的なモデルは以下のようなものである。

ST が評価されることが承認されると、コモンクライテリアテスト機関 (CCTL) が TOE 及びその支援 IT 環境へのアクセス、ならびに TOE の管理ガイダンスを取得する。そして、ST に列挙された保証アクティビティ (これは CCTL により ST 中で、または別個の文書の中で TOE 特有となるように詳細化される) が、CCTL により行われる。これらのアクティビティの結果は、検証のために (利用された管理ガイダンスと共に) 文書化され提示される。

それぞれのファミリには、(もしあれば) 開発者により提供される必要のある追加的文書／アクティビティを明確にするため、開発者アクションエレメントについて「開発者への注意」が提供される。内容／提示及び評価者アクティビティエレメントについては、エレメントごとにではなく、ファミリ全体について追加的アクティビティが記述されている。さらに、本セクションに記述された保証アクティビティは、セクション 5.2 (訳注：セクション 4 の間違い) に規定されたものとは相補的な関係にある。

TOE のセキュリティ保証要件は表 2 (訳注：該当する表は存在しないようである) に要約されており、本 PP のセクション 5.2 (訳注 : 附属書 A.2 の間違い) に特定された脅威へ対処するために必要とされる管理及び評価アクティビティが特定されている。

5.1 ADV クラス：開発

TOE に関する情報は ST の TOE 要約仕様 (TSS) 部分とともに、エンドユーザに利用可能なガイダンス文書にも含まれている。TOE 開発者は TSS に含まれる製品の記述を、機能仕様との関連において一致させなければならない (must)。セクション 4.2 に含まれる保証アクティビティは、TSS セクションにふさわしい内容を判断するために十分な情報を ST 作成者へ提供すべきである (should)。

ADV_FSP.1　基本機能仕様

開発者のアクションエレメント：

ADV_FSP.1.1D　開発者は、機能仕様を提供しなければならない (shall)。

ADV_FSP.1.2D　開発者は、機能仕様から SFR への追跡を提供しなければならない (shall)。

開発者への注意：本セクションの概論で述べたように、機能仕様は AGD_OPR 及び AGD_PRE 文書に含まれる情報と、ST の TSS に提供される情報との組み合わせで構成される。機能仕様中の保証アクティビティは、文書及び TSS セクションに存在すべき (should) 証拠資料を参照している。これらは SFR と直接関連付けられているため、エレメント ADV_FSP.1.2D 中の追跡は暗黙にはすでになされており、追加的な文書は必要とされない。

内容及び提示エレメント：

ADV_FSP.1.1C *機能仕様には、SFR を強制する、及び SFR をサポートする TSFI のそれぞれについて、使用の目的と手法が記述されなければならない (shall)。*

ADV_FSP.1.2C *機能仕様には、SFR を強制する、及び SFR をサポートする TSFI のそれぞれについて、関連するすべてのパラメータが特定されなければならない (shall)。*

ADV_FSP.1.3C *機能仕様には、SFR 非干渉と暗黙に分類されているインタフェースについて、その根拠が提供されなければならない (shall)。*

ADV_FSP.1.4C *追跡は、機能仕様における SFR から TSFI への追跡を例証するものでなければならない (shall)。*

評価者のアクションエレメント：

ADV_ FSP.1.1E *評価者は、提供された情報が証拠資料の内容及び提示のすべての要件を満たしていることを確認しなければならない (shall)。*

ADV_ FSP.1.2E *評価者は、機能仕様が SFR の正確かつ完全な実体化であることを判断しなければならない (shall)。*

保証アクティビティ：

これらの SAR に関連付けられた具体的な保証アクティビティは存在しない。機能仕様文書はセクション 4.2 に記述された評価アクティビティと、AGD、ATE、及び AVA SAR に関して記述されたその他のアクティビティをサポートするために提供される。機能仕様情報の内容についての要件は、行われるその他の保証アクティビティの特質により暗黙に評定される。不十分なインタフェース情報しか存在しなかったために評価者がアクティビティを行うことができなかった場合には、十分な機能仕様が提供されていなかったことになる。

5.2 AGD クラス：ガイダンス文書

ガイダンス文書は、開発者のセキュリティターゲットと共に提供される。ガイダンスには、運用環境がセキュリティ機能にそれ自身の役割を果たすことができることを正当な利用者が検証する方法の記述が含まれなければならない (must)。本文書は、正当な利用者により読解可能な非形式的なスタイルであるべきである (should)。

製品がサポートすると ST で主張されているすべての運用環境について、ガイダンスが提供されなければならない (must)。本ガイダンスには、以下が含まれる。

- その環境への TOE のインストールを成功させるための指示、及び
- 製品として、またより大規模な運用環境のコンポーネントとして、TOE のセキュリティを管理するための指示。

また、特定のセキュリティ機能に関するガイダンスも提供される。そのようなガイダンスに関する具体的な要件は、セクション 4.2 に規定された保証アクティビティに含まれている。

AGD_OPE.1　利用者操作ガイダンス

開発者のアクションエレメント：

AGD_OPE.1.1D　開発者は、利用者操作ガイダンスを提供しなければならない (shall)。

開発者への注意：　ここで繰返し情報を提示するのではなく、開発者は本コンポーネントに関する保証アクティビティをレビューして、評価者が

チェックすることになるガイダンスの詳細を確認すべきである (should)。これにより、受容可能なガイダンスの作成に必要な情報が提供されることになる。

内容及び提示エレメント：

AGD_OPE.1.1C 利用者操作ガイダンスには、セキュアな処理環境において制御されるべき (should) 正当な利用者にアクセス可能な機能及び特権が、適切な警告を含めて記述されなければならない (shall)。

AGD_OPE.1.2C 利用者操作ガイダンスには、正当な利用者を対象として、TOE により提供される利用可能なインタフェースをセキュアな方法で利用する方法が記述されなければならない (shall)。

AGD_OPE.1.3C 利用者操作ガイダンスには、正当な利用者を対象として、利用可能な機能及びインタフェース、特に利用者の制御下にあるすべてのセキュリティパラメータが、該当する場合にはセキュアな値を示しつつ、記述されなければならない (shall)。

AGD_OPE.1.4C 利用者操作ガイダンスには、正当な利用者を対象として、利用者にアクセス可能な機能であって、TSF の制御下にあるエンティティのセキュリティ的な特徴の変更を含めて、実行される必要のあるものに関連するセキュリティ関連イベントのすべての種類が明示されなければならない (shall)。

AGD_OPE.1.5C 利用者操作ガイダンスには、TOE のすべてのあり得る動作モード (故障または操作エラー後の動作を含めて) と、その結果及びセキュアな動作の維持への影響が特定されなければならない (shall)。

AGD_OPE.1.6C 利用者操作ガイダンスには、正当な利用者を対象として、ST に記述される運用環境に関するセキュリティ対策方針を達成するために遵守されるべきセキュリティ対策が記述されなければならない (shall)。

AGD_OPE.1.7C 利用者操作ガイダンスは、明確かつ妥当なものでなければならない (shall)。

AGD_OPE.1.8C 利用者操作ガイダンスは、セキュリティの自動化をサポートするためセキュリティ設定チェックリスト記述形式 (XCCDF) で表現されなければならない (shall)。[米国のみの追記] 利用者操作ガイダンスは、XCCDF チェック項目検査方法エレメントとしてレジームの適合チェックを行うために利用できる構成ガイダンス項目のそれぞれを表現し、またその項目が満たす NIST 800-53 管理策への参照を提供しなければならない (shall)。

評価者のアクションエレメント：

AGD_OPE.1.1E 評価者は、提供された情報が証拠資料の内容及び提示のすべての要件を満たしていることを確認しなければならない (shall)。

保証アクティビティ：

操作ガイダンスの内容の一部は、セクション 4.2 の保証アクティビティと CEM にしたがった TOE の評価により検証されることになる。

文書には、ハッシュのチェックまたはデジタル署名の検証のいずれかにより、TOE へのアップデートを検証するためのプロセスが記述されなければならない (must)。評価者は、本

プロセスに以下の手順が含まれることを検証しなければならない (shall)。

1. *TOE ソフトウェアの現在のバージョンを問い合わせるための指示。*
2. *ハッシュについては、所与のアップデートについてのハッシュがどこで取得できるかという記述。デジタル署名については、署名されたアップデートが証明書の所有者から受信されていることを保証するために、FCS_COP.1(2) メカニズムにより用いられる証明書を取得するための指示。これは、最初から製品と共に供給されてもよいし、何らかの別の手段により取得されてもよい。*
3. *アップデートそのものを取得するための指示。これには、アップデートを TOE からアクセス可能とするための指示 (例えば、特定のディレクトリへの格納) が含まれるべきである (should)。*
4. *アップデートプロセスを開始するための、そしてそのプロセスが成功したか失敗したかを判別するための指示。これには、ハッシュ／デジタル署名の生成が含まれる。*

AGD_PRE.1　準備手続き

開発者のアクションエレメント：

AGD_PRE.1.1D 開発者は TOE を、その準備手続きを含めて提供しなければならない (shall)。

開発者への注意：操作ガイダンスと同様に、開発者は、準備手続きに関して必要とされる内容を決定するため、保証アクティビティを確認するべきである (should)。

内容及び提示エレメント：

AGD_PRE.1.1C 準備手続きには、開発者の配付手続きにしたがって配付された TOE をセキュアに受領するために必要なすべての手順が記述されなければならない (shall)。

AGD_PRE.1.2C 準備手続きには、TOE のセキュアな設置に必要なすべての手順と、ST に記述される運用環境のセキュリティ対策方針にしたがった運用環境のセキュアな準備に必要なすべての手順が記述されなければならない (shall)。

評価者のアクションエレメント：

AGD_PRE.1.1E 評価者は、提供された情報が証拠資料の内容及び提示のすべての要件を満たしていることを確認しなければならない (shall)。

AGD_PRE.1.2E 評価者は、TOE が運用のためにセキュアに準備できることを確認するために、準備手続きを適用しなければならない (shall)。

保証アクティビティ：

上の概論で述べたように、特に TOE の機能要件をサポートする運用環境の構成にあたっては、文書に関して多大な期待が存在する。評価者は、TOE に関して提供されたガイダンスが、ST 中に TOE について主張されているすべてのプラットフォーム (すなわち、ハードウェアとオペレーティングシステムの組み合わせ) へ十分に対応していることを保証するため、チェックしなければならない (shall)。

5.3 ALC クラス：ライフサイクルサポート

本 PP に適合する TOE に提供される保証レベルでは、ライフサイクルサポートは TOE ベンダの開発及び構成管理プロセスの調査に限定される。これは、製品の全体的な信頼度の向

上に開発者のプラクティスが果たす重要な役割の結果である。

ALC_CMC.1 TOE のラベル付け

開発者のアクションエレメント：

ALC_CMC.1.1D　開発者は、TOE 及び TOE への参照情報を提供しなければならない (shall)。

内容及び提示エレメント：

ALC_CMC.1.1C　*TOE は、その一意な参照情報によりラベル付けされなければならない (shall)。*

評価者のアクションエレメント：

ALC_CMC.1.1E　*評価者は、提供された情報が証拠資料の内容及び提示のすべての要件を満たしていることを確認しなければならない (shall)。*

保証アクティビティ：

評価者は、TOE がその一意な参照ラベル付けと共に提供されていることを検証しなければならない (shall)。評価者は、CM 文書が提供されており、またそれに各構成項目を一意に特定するために用いられる手法が記述されていることを検証しなければならない (shall)。評価者は、開発者が CM システムを使用しており、また本システムが各構成項目を一意に特定していることを検証しなければならない (shall)。

ALC_CMS.1 TOE の CM カバレージ

開発者のアクションエレメント：

ALC_CMS.1.1D　開発者は、TOE の構成リストを提供しなければならない (shall)。

内容及び提示エレメント：

ALC_CMS.1.1C　*構成リストには、以下が含まれなければならない (shall)：TOE そのもの、及び SAR により要求される評価証拠。*

ALC_CMS.1.2C　*構成リストには、構成要素が一意に識別されなければならない (shall)。*

評価者のアクションエレメント：

ALC_CMS.1.1E　*評価者は、提供された情報が証拠資料の内容及び提示のすべての要件を満たしていることを確認しなければならない (shall)。*

保証アクティビティ：

評価者は、上記に明示された各項目を含む TOE の構成リストを開発者が提供していることを検証しなければならない (shall)。評価者は、構成リスト中の各項目が一意に特定され、またその開発者が示されていることを検証しなければならない (shall)。

5.4 ATE クラス：テスト

テストは、システムの機能的側面と、設計または実装の弱点を利用する側面について規定される。前者は ATE_IND ファミリにより行われるが、後者は AVA_VAN ファミリにより行われる。本 PP に規定された保証レベルにおいては、テストは通知された機能及びインタフェースに基づき、設計情報の利用可能性に依存して行われる。評価プロセスの主要なアウトプットのひとつは、以下の要件に規定されるテスト報告である。

ATE_IND.1 独立テスト—適合

テストは、TSS と、提供された管理 (構成及び操作を含む) 文書に記述された機能を確認するために行われる。テストで重視されるのは、セクション 4.2 に規定された要件が満たされていることの確認であるが、いくつかの追加的テストがセクション 4.3 中の SAR について規定されている。保証アクティビティは、これらのコンポーネントと関連付けられた追加的テストアクティビティを特定する。評価者は、テストの計画及び結果、ならびに本 PP への適合を主張するプラットフォーム／TOE の組み合わせに焦点を絞ったカバレージの論拠を文書化した、テスト報告を作成する。

開発者のアクションエレメント：

ATE_IND.1.1D　*開発者は、テストに用いられる TOE を提供しなければならない (shall)。*

内容及び提示エレメント：

ATE_IND.1.1C　*TOE は、テストに適当なものでなければならない (shall)。*

評価者のアクションエレメント：

ATE_IND.1.1E　*評価者は、提供された情報が証拠資料の内容及び提示のすべての要件を満たしていることを確認しなければならない (shall)。*

ATE_IND.1.2E　*評価者は、TSF が規定されたように動作することを確認するために TSF のサブセットをテストしなければならない (shall)。*

保証アクティビティ：

評価者は、システムのテストの側面を文書化したテスト計画とテスト報告を作成しなければならない (shall)。テスト計画は、CEM と本 PP の保証アクティビティの本体に含まれるすべてのテストアクションをカバーする。保証アクティビティ中に列挙されたテストのそれぞれについて 1 つのテストケースを用意する必要はないが、ST 中の該当するテスト要件のそれぞれがカバーされていることを評価者はテスト計画中に文書化しなければならない (must)。

テスト計画にはテストされるプラットフォームが特定され、そしてテスト計画には含まれないが ST に含まれるプラットフォームについては、そのプラットフォームをテストしないことについての正当化をテスト計画が提供する。この正当化には、テストされるプラットフォームとテストされないプラットフォームとの違いを取り上げ、行われるべきテストにその違いが影響しないという論拠を示さなければならない (must)。単にその違いが影響しないと主張するだけでは十分ではなく、根拠が提供されなければならない (must)。ST 中に主張されるすべてのプラットフォームがテストされる場合には、根拠は必要とされない。

テスト計画にはテストされるべき各プラットフォームの構成が記述され、また AGD 文書に含まれるもの以外に必要な設定があれば、それも記述される。テストの一部としての、または標準的なテスト前の条件としての、各プラットフォームの設置及び設定について、評価者が AGD 文書にしたがうことが期待されていることには注意すべきである (should)。これには、特別なテストドライバまたはツールも含まれるかもしれない。ドライバまたはツールのそれぞれについて、そのドライバまたはツールが TOE 及びそのプラットフォームによる機能の実行に悪影響を与えないという、(単なる主張ではなく) 論拠が提供される。またこれには、用いられるべき暗号エンジンの構成が含まれる。このエンジンにより実装される暗号アルゴリズムは、本 PP により規定され、評価される暗号プロトコル (IPsec, TLS/HTTPS) により用いられるものである。

テスト計画には、高レベルのテスト目的とともに、これらの目的を達成するために行われるべきテスト手順も特定される。これらの手順には、期待される結果も含まれる。テスト報告 (テスト計画へ単に注釈を加えたものであってもよい) には、テスト手順が実施された

際に行われたアクティビティが詳述され、またテストの実際の結果が含まれる。これは累積的な記述でなければならない (shall)。したがって失敗に終わったテストの実行が存在し、修正がインストールされ、そして次にテストの再実行が成功した場合、報告には単なる「成功」の結果だけではなく、「失敗」及び「成功」の結果 (及びそれを支持する詳細) が示される。

5.5 AVA クラス：脆弱性評定

168. 本プロテクションプロファイルの第一世代については、オープンソースの調査を行って、これらの種類の製品にどのような脆弱性が発見されているのかを調査することが評価機関に期待される。多くの場合、これらの脆弱性には基本的な攻撃者を超える巧妙さが必要とされる。ペネトレーションツールが作成されて評価機関へあまねく配付されるまでは、評価者には TOE 中のこれらの脆弱性のテストを行うことは期待されない。評価機関には、ベンダにより提供された文書を考慮して、これらの脆弱性の存在する可能性についてコメントすることが期待される。本情報はペネトレーションテストツールの開発と、将来のプロテクションプロファイルの開発のために用いられることになる。

AVA_VAN.1 脆弱性調査

開発者のアクションエレメント：

AVA_VAN.1.1D　開発者は、テストに用いられる TOE を提供しなければならない (shall)。

内容及び提示エレメント：

AVA_VAN.1.1C　*TOE は、テストに適当なものでなければならない (shall)。*

評価者のアクションエレメント：

AVA_VAN.1.1E　*評価者は、提供された情報が証拠資料の内容及び提示のすべての要件を満たしていることを確認しなければならない (shall)。*

AVA_VAN.1.2E　*評価者は、TOE 中に潜在する脆弱性を特定するために、パブリックドメインソースの検索を実行しなければならない (shall)。*

AVA_VAN.1.3E　*評価者は、基本的な攻撃能力を有する攻撃者により行われる攻撃に TOE が耐えられることを判断するために、特定された潜在する脆弱性に基づいて、ペネトレーションテストを実施しなければならない (shall)。*

保証アクティビティ：

ATE_IND と同様に、評価者は報告を作成し、本要件に関連する自分たちの結論を文書化しなければならない (shall)。本報告は、物理的には ATE_IND に言及される全体的なテスト報告の一部であってもよいし、あるいは別個の文書であってもよい。評価者は、公開された情報の検索を行って、MDM (訳注：電子メールクライアントの間違い) 一般に発見されている脆弱性と、特定の TOE に関する脆弱性を判断する。評価者は、参考としたソースと発見された脆弱性を報告中に文書化する。発見された脆弱性のそれぞれについて、評価者はそれが該当しないことを示す根拠を提供するか、あるいはそのほうが適切であれば脆弱性を確認するためのテストを (ATE_IND に提供されるガイドラインを用いて) 策定するかのどちらかを行う。適切かどうかは、その脆弱性を利用するために必要とされる攻撃ベクトルの評定により判断される。例えば、ブート時にあるキーの組み合わせを押すことにより脆弱性が検出できる場合、本 PP の保証レベルにおいてはテストが適当であろう。例えば、脆弱性の悪用に専門的なスキルと電子顕微鏡が必要とされる場合には、テストは適当ではなく、適切な根拠が策定されることになるであろう。

6 根拠

脅威から対策方針へ、対策方針から要件へ、トレースする根拠については、セクション 2.0 及び 3.0 の文章に含まれている。唯一の残課題であるマッピングは前提条件と組織のセキュリティ方針に関してのものである：これらは以下の附属書 A に含まれている。

附属書A： 参考表

本プロテクションプロファイルでは、本文書の最初のセクションにおける焦点は、ネットワークデバイスに対する脅威；その脅威を低減するための手法；適合 TOE により達成される低減の範囲、についての全般的なわかりやすさの向上を図るため物語風の説明を用いている。この説明のスタイルは形式化された評価アクティビティにはそのまま適用できないため、本附属書では、本文書に関連する評価アクティビティについて使用可能な表形式のアーティファクトを用いている。

A.1 前提条件

以下のサブセクションに列挙する具体的な条件が、TOE の運用環境に存在することが前提となる。これらの前提条件には、TOE セキュリティ要件の開発と、TOE の使用において基本的な環境条件の両方における実際の現実が含まれる。

ST 作成者は、自分たちの特有の技術について前提条件が引き続き満たされることを保証すべきである (should)；表は適宜改変されるべきである (should)。

表 1：TOE の前提条件

前提条件の名称	前提条件の定義
A.PLATFORMS	本文書に記述される電子メールクライアントは、基盤となるプラットフォームにかかわらず、任意のオペレーティングシステム上で動作する。
A.PHYSICAL	TOE 及びそれに含まれるデータの価値に対応した物理的セキュリティが、環境により提供されることが前提とされる。
A.TRUSTED_ADMIN	TOE 管理者は、すべての管理ガイダンスを遵守し信頼された方法で適用すると信頼されている。
A.TRUSTED_USER	電子メールクライアントの利用者は悪意を持たず、適切な予防措置を講じる。
A.PLATFORM_FUNCTIONS	電子メールクライアントをサポートするプラットフォームは、ファイルシステムやその他のオペレーティングシステム機能を提供しなければならない (shall)。

A.2 脅威

以下の脅威は、本文書に記述された要件を含める際に、PP 作成者により技術に特有な脅威と統合されるべきである (should)。要件に対する改変、省略、及び追加は、本リストに影響を与えるかもしれないので、PP 作成者はこれらの脅威が適切となるように、改変または削除すべきである (should)。

表 2：脅威

脅威の名称	脅威の定義

T.UNAUTHORIZED_ADDON	悪意のある、または悪用可能な拡張機能またはプラグインが、開発者により意図的に、あるいは意図せず用いられ、その結果、プラットフォームのシステムソフトウェアに対する攻撃能力を生じさせてしまうかもしれない。
T.UNAUTHORIZED_UPDATE	悪意のある、または悪用可能なソフトウェアが、開発者により意図的に、あるいは意図せず用いられ、その結果、プラットフォームのシステムソフトウェアに対する攻撃能力を生じさせてしまうかもしれない。
T.NETWORK_EAVESDROP	ワイヤレス通信チャネル上やネットワーク上のどこかに位置する場合、攻撃者は、電子メールクライアントと他のエンドポイントとの間で交換されるデータに対して、盗聴やアクセスの獲得ができてしまうかもしれない
T.NETWORK_ATTACK	攻撃者は、電子メールクライアントとの通信を開始したり、電子メールクライアントと他のエンドポイントとの間の通信を改変するかもしれない。

A.3 TOE のセキュリティ対策方針

表 3：TOE のセキュリティ対策方針

TOE セキュリティ対策方針	TOE 対策方針の定義
O.COMMS	TOE は、TOE の外部へ送信されるデータの機密性を維持する手段として、1 つ (以上) の標準プロトコルを用いて通信を行う能力を提供すること。
O.CONFIG	TOE は、セキュリティポリシーを構成し適用する能力を提供すること。これにより、電子メールクライアントが、保存または処理し得る利用者及びエンタープライズデータを保護できることを保証する。
O.INTEGRITY	TOE は、重要な機能、ソフトウェア／ファームウェア及びデータの完全性が保たれていることを保証するため、セルフテストを行う能力を提供すること。また TOE は、ダウンロードされたアップデートの完全性を検証し、また拡張機能及びプラグインの完全性とともにそれらが信頼されるソースからのものであることを検証する手段を提供すること。
O.STORAGE	TOE は、その保存するデータの機密性を保証するため、すべての利用者及びエンタープライズデータ及び認証鍵を暗号化する能力を提供すること。

A.4 セキュリティ対策方針へのセキュリティ脅威

以下の表には、セキュリティ脅威から TOE の対策方針へのマッピングが含まれている。

表 3：セキュリティ脅威から対策方針へのマッピング

脅威	対策方針
T.UNAUTHORIZED_ADD-ON	O.INTEGRITY
T.UNAUTHORIZED_UPDATE	O.INTEGRITY
T.NETWORK_EAVESDROP	O.COMMS
T.NETWORK_ATTACK	O.COMMS; O.ISOLATION
T.DATA_ACCESS	O.STORAGE; O.CONFIG

附属書B： オプションの要件

本 PP の概論で示すように、本 PP の本文にはベースライン要件 (TOE またはその基盤となるプラットフォームにより実施されなければならない要件 (must)) が含まれている。さらに、附属書 B、C、及び D で規定する 3 種類の他の要件がある。

第 1 の種類 (本附属書にて) は、ST に含むことができる要件であるが、TOE が本 PP への適合主張するためには必ずしも必要とされないものである。第 2 の種類 (附属書 C にて) は、PP の本文での選択に基づく要件：特定の選択がなされた場合、その附属書の追加的要件を含める必要がある。第 3 の種類 (附属書 D にて) は、本 PP へ適合するためには要求されないが、本 PP の将来のバージョンでベースライン要件に含まれるようなコンポーネントである。ST 作成者は、附属書 B、附属書 C、附属書 D の要件に関連するが列挙されていないような要件 (例えば、FMT タイプの要件) も ST に含まれることを保証する責任があることに注意されたい。

どの時点でも、これらは ST に含めることができ、その場合でも TOE は依然として本 PP に適合する。

B.1 クラス：利用者データ保護 (FDP)

B.1.1 保存データ (DAR)

FDP_DAR_EXT.1 (訳注：FDP_DAR_EXT.1.1 の間違い) TSF は、すべての電子メール、永続的秘密、プライベート鍵、及び [選択：カレンダーの予定、連絡先、[割付：その他の利用者データ]、その他の利用者データなし] を秘密（Sensitive）としてマークしなければならない (shall)。

適用上の注意：*電子メールクライアントはそれ自身の保存データ暗号化を提供することは要求されないが、その代わりデバイスがロック状態にある間は電子メールが暗号化されることを保証するため、モバイルデバイスの保存データ保護メカニズムを用いること。モバイルデバイス基盤のためのプロテクションプロファイル (MDFPP) では、3 つのレベルのデータ保護が定義されている：TSF データ、保護データ、及び秘密データ。本要件の意図は、電子メールクライアントが秘密データレベルの保存データ保護を利用するということである。MDFPP では、TSF がデータを秘密としてマークするために用いられるメカニズムについての要件が提供されている。*

本メカニズムを用いて、電子メールクライアントは、ロック状態において、電子メールデータ、永続的秘密 (パスワード、他のクレデンシャル、秘密鍵) 及びプライベート鍵が暗号化されていることを保証しなければならない (must)。オプションとして、電子メールクライアントは、カレンダーの予定、連絡先、及びその他の利用者データ (例えば、タスクリスト、チャットメッセージ) を含めて、クライアントにより保持されるその他の利用者データを同様にあるいは保護レベルを用い保護してもよい。

保証アクティビティ：

評価者は、電子メールクライアントが要求される利用者データに秘密としてマークする方法が TSS に記述されていることを保証するため、TSS を検査しなければならない (shall)。

開発者は、利用者データがプラットフォームにより正しく保護されることを正当化するために、評価者に対して、十分なソースコード (必要なのは数行のみである) またはコンパイル情報を提供しなければならない (shall)。評価者は、プラットフォームの API ガイダンスと一致する、利用者データを秘密とマークしているソースコードまたはコンパイル情報を提供していることを検証するため、TOE によりサポートされることが示されているプラットフォームの API 文書を検査しなければならない (shall)。

附属書C： 選択に基づいた要件

本 PP の概論で示したように、本 PP の本文には、ベースライン要件 (TOE またはその基盤となるプラットフォームにより実施されなければならない要件 (must)) が含まれている。PP の本文中の選択に基づく追加的要件がある：特定の選択がなされた場合には、以下の追加的要件が含まれる必要がある。

C.1 クラス：利用者データ保護 (FDP)

C.1.1 情報の削除

C.1.1.1. FDP_DEL_EXT.1 拡張：拡張機能情報の削除

FDP_DEL_EXT.2.1 (訳注：FDP_DEL_EXT.1.1 の間違い)　TOE は、拡張機能、構成エレメント、及び保存された情報を含む、すべての情報が削除されるように、拡張機能を削除する能力を提供しなければならない (shall)。

保証アクティビティ：

TSS

評価者は、拡張機能がどこに保存されるか、拡張機能が情報をどこに保存することが許可されているか、について TSS に文書化されていることを保証するため、TSS を検査しなければならない (shall)。

ガイダンス

評価者は、どのようにすれば利用者が拡張機能を削除できるかについての指示が操作ガイダンスに含まれていることを検証するため、操作ガイダンスを検査しなければならない (shall)。

テスト

評価者は、以下のテストを実行しなければならない (shall)：

- テスト 1：評価者は、TOE 拡張機能をインストールした後、拡張機能及び拡張機能データが文書化されたとおり保存されていることを検証するため、TOE のファイルシステムを検査しなければならない (shall)。次に、評価者は、TOE 拡張機能をアンインストールし、拡張機能及び拡張機能データが文書化された場所から削除されていることを検証するため、TOE のファイルシステムを検査しなければならない (shall)。

C.1.1.2. FDP_DEL_EXT.2 拡張：プラグイン情報の削除

FDP_DEL_EXT.3.1 (訳注：FDP_DEL_EXT.2.1 の間違い)　TOE は、プラグイン、構成エレメント、及び保存された情報を含むすべての情報が削除されるように、プラグインを削除する能力を提供しなければならない (shall)。

保証アクティビティ：

TSS

評価者は、プラグインがどこに保存されるか、プラグインが情報をどこに保存することが許可されているか、そしてすべてのプラグイン情報を削除するためのオプションが存在するかどうか、について TSS に文書化されていることを保証するため、TSS を検査しなければならない (shall)。

ガイダンス

評価者は、どのようにすれば利用者がプラグイン及び関連付けられた内容を削除できるかの指示が操作ガイダンスに含まれていることを検証するため、操作ガイダンスを検査しな

ければならない (shall)。

テスト

評価者は、以下のテストを実行しなければならない (shall) :

- テスト 1 : 評価者は、TOE プラグインをインストールした後、プラグイン及びプラグインデータが文書化されたとおり保存されていることを検証するため、TOE のファイルシステムを検査しなければならない (shall)。次に評価者は、TOE プラグインをアンインストールして、文書化された場所からプラグイン及びプラグインデータが削除されていることを検証するため、TOE のファイルシステムを検査しなければならない (shall)。

C.2 クラス：TSF の保護 (FPT)

C.2.1 高信頼アップデート

C.2.1.1. FPT_TUD_EXT.1 拡張：高信頼拡張機能アップデート

FPT_TUD_EXT.1.1 TOE は、拡張機能の現在のバージョンを問い合わせる能力を提供しなければならない (shall)。

FPT_TUD_EXT.1.2 TOE は、拡張機能のアップデートを開始する能力を提供しなければならない (shall)。

FTP_TUD_EXT.1.3 TOE は、拡張機能または拡張機能のアップデートをインストールする前に、デジタル署名メカニズムを用いて拡張機能または拡張機能のアップデートを検証する手段を提供しなければならない (shall)。

FTP_TUD_EXT.1.4 TOE は、拡張機能の自動的なインストールを防止しなければならない (shall)。

適用上の注意：

拡張機能は、クライアントがデフォルトでは提供しない特定の機能を追加するために、電子メールクライアントへ追加されるコード群である。拡張機能は、電子メールクライアントベンダ、または第三者により開発され、また電子メールクライアントが理解する電子メールの内容を閲覧し、対話するためにフルアクセスが許可される。

保証アクティビティ：

TSS

評価者は、拡張機能と拡張機能のアップデートが信頼できるソースからのものであることを検証する TSF の能力が記述されていることを検証するため、TSS を検査しなければならない (shall)。評価者は、承認されていないソースからの拡張機能を TSF が拒否することが述べられていることを検証するため、TSS を検査しなければならない (shall)。

ガイダンス

評価者は、信頼される拡張機能のソースを持つ TOE をどのように構成するかについての指示が含まれていることを検証するため、操作ガイダンスを検査しなければならない (shall)。

テスト

評価者は、以下のテストを実行しなければならない (shall) :

- テスト 1: 評価者は、信頼されるソースを持つ TOE を構成しなければならない (shall)。評価者は、信頼されるソースにより署名された拡張機能を作成または取得し、インストールを試行しなければならない (shall)。評価者は、拡張機能の署名が有効であるこ

とを検証しなければならない (shall)。

- テスト 2 : 評価者は、信頼できないソースにより署名された拡張機能を作成または取得し、インストールを試行しなければならない (shall)。評価者は、その署名された拡張機能が拒否されることを検証しなければならない (shall)。
- テスト 3 : 評価者は、無効な証明書を用いて署名された拡張機能を作成または取得し、インストールを試行しなければならない (shall)。評価者は、その署名された拡張機能が拒否されることを検証しなければならない (shall)。
- テスト 4 : 評価者は、信頼されるソースにより署名された拡張機能を作成または取得し、再署名することなくその拡張機能を改変し、インストールを試行しなければならない (shall)。評価者は、その署名された拡張機能が拒否されることを検証しなければならない (shall)。

C.2.1.2. FPT_TUD_EXT.2 拡張 : 高信頼プラグインアップデート

FPT_TUD_EXT.2.1 TOE は、プラグインの現在のバージョンを問い合わせる能力を提供しなければならない (shall)。

FPT_TUD_EXT.2.2 TOE は、プラグイン及びプラグインアップデートのダウンロードを開始する能力を提供しなければならない (shall)。

FTP_TUD_EXT.2.3 TOE は、プラグインをインストールする前に、デジタル署名メカニズム及び [選択 : 公開ハッシュ、その他の機能なし] を用いて、プラグインを検証する手段を提供しなければならない (shall)。

FTP_TUD_EXT.2.4 TOE は、プラグインの自動的なインストールを防止しなければならない (shall)。

保証アクティビティ :

TSS

評価者は TSS を調査して、未承認ソースからのプラグインを TSF が拒否することが述べられていることを検証しなければならない (shall)。

ガイダンス

評価者は操作ガイダンスを調査して、TOE に高信頼プラグインソースを構成する方法に関する指示が含まれていることを検証しなければならない (shall)。

テスト

評価者は、以下のテストを実行しなければならない (shall) :

- テスト 1 : 評価者は、信頼されるプラグインのソースを持つ TOE を構成しなければならない (shall)。評価者は、信頼されるソースにより署名されたプラグインを作成または取得し、インストールを試行しなければならない (shall)。評価者は、プラグインの署名が有効であることを検証しなければならない (shall)。
- テスト 2 : 評価者は、信頼できないソースにより署名されたプラグインを作成または取得し、インストールを試行しなければならない (shall)。評価者は、その署名されたプラグインが拒否されることを検証しなければならない (shall)。
- テスト 3 : 評価者は、無効な証明書を用いて署名されたプラグインを作成または取得し、インストールを試行しなければならない (shall)。評価者は、その署名されたプラグインが有効である (訳注 :「拒否される」の間違い) ことを検証しなければならない (shall)。

- テスト 4 :　評価者は、信頼されるソースにより署名されたプラグインを作成または取得し、再署名することなくそのプラグインを改変し、インストールを試行しなければならない (shall)。評価者は、その署名されたプラグインが拒否されることを検証しなければならない (shall)。

附属書D： オブジェクティブな要件

本 PP の概論で示したように、本 PP の本文にはベースライン要件 (TOE またはその基盤となるプラットフォームにより実施されなければならない要件 (must)) が含まれている。本附属書には、これ以外にも望ましいセキュリティ機能として特定される追加的要件が存在し、これらの要件は本附属書に含まれる。これらの要件は、本 PP の将来のバージョンにて、オブジェクティブな要件からベースライン要件へ移行することが期待される。

D.1 クラス：利用者データ保護 (FDP)

D.1.1 永続的情報のストレージ (FDP_PST)

FDP_PST_EXT.1.1 TOE は、ファイルシステムへ永続的情報を保存することなく動作可能でなければならない (shall)。

適用上の注意：*本要件の例外としては、クレデンシャル（資格情報）及び設定情報がある。*

保証アクティビティ：

評価者は、幅広いさまざまな TOE の機能が確実に動作していることを保証するため、一定の期間、TOE を運用しなければならない (shall)。その際、評価者は、クレデンシャル又は設定情報以外にファイルシステムにいかなるファイルも書き込まれないことを保証するため、TOE を検査しなければならない (shall)。

附属書E： エントロピーの文書化と評定

エントロピー源に関する文書化は、それを読んだ後に評価者が、エントロピー源を理解し、それがエントロピーを供給すると信頼できる根拠を完全に理解できるように、十分に詳細であるべきである (should)。本文書には、設計記述、エントロピーの正当化、運用条件及びヘルステストという、複数の詳細なセクションが含まれるべきである (should)。本文書は、TSS の一部としては要求されない。

E.1 設計記述

文書化では、エントロピー源のすべてのコンポーネントの相互作用を含め、エントロピー源の全体的な設計が含まれなければならない (shall)。これには、どのように動作するのか、どのようにエントロピーが生成されるのか、そしてどのように未処理 (生の) データをエントロピー源の内部からテスト目的で取り出すことができるのか、を含めてエントロピー源の操作について記述することになる。文書化では、ランダム性がどこから由来し、次にどこへ渡されるのか、生の出力の任意の後処理 (ハッシュ、XOR など)、保存されるのであればどこに保存されるのか、そして最後に、どのようにしてエントロピー源から出力されるのか、を示すように、エントロピー源の設計についてのウォークスルー（段階的な説明）を行うべきである (should)。処理における条件等があれば (ブロッキング等)、それもエントロピー源の設計の中で記述されるべきである (should)。図や例の利用が推奨される。

この設計には、エントロピー源のセキュリティ境界の内容に関する記述と、境界外部の敵対者がエントロピー量に影響を与えられないことを、どのようにしてセキュリティ境界が保証するかに関する記述についても含まれなければならない (must)。

もし、サードパーティのアプリケーションが実装される場合、設計の記述には、サードパーティのアプリケーションがどのようにしてRBGへエントロピーを追加できるかに関する記述が含まれなければならない (shall)。電源オフから電源オンまでの間に保存されるあらゆる RBG の状態に関する記述が含まれなければならない (shall)。

E.2 エントロピーの正当化

エントロピー源の予測不可能性がどこに由来し、エントロピー源が確率論的なふるまいを示すことがなぜ確信できるのかという技術的な議論が存在するべきである (確率分布の説明と、その分布が特定のエントロピー源により得られるという正当化を行うことは、これを記述する方法のひとつである) (should)。この議論には、期待されるエントロピー量の記述と、十分なエントロピーが TOE のランダム化シード供給プロセスへ与えられることをどのように保証するかに関する説明が含まれることになる。この議論は、エントロピー源がエントロピーを持つビットを生成すると信頼できる理由の正当化の一部となる。

エントロピーの正当化には、任意のサードパーティアプリケーション、または再起動までの間に保存される任意の状態から、追加される一切のデータが含まれてはならない (shall not)。

E.3 運用条件

また文書には、エントロピー源がランダムデータを生成すると期待される運用条件の範囲も含まれることになる。これには、これらの条件の下でエントロピー源が動作し続けることを確実にするために、システムの設計に取り入れられた対策が明確に記述されることになる。同様に、文書にはエントロピー源が動作不良又は矛盾した動作となることがわかっている条件も記述されなければならない (shall)。エントロピー源の故障または機能低下を検出するための手法が、含まれなければならない (shall)。

E.4 ヘルステスト

さらに具体的に、すべてのエントロピー源ヘルステストとその根拠が文書化されることになる。これには、ヘルステストの記述、各ヘルステストが行われる頻度及び条件 (例えば、起動時、連続、またはオンデマンド)、各ヘルステストに期待される結果、そしてそれぞれのテストがエントロピー源の 1 つ以上の故障を検出するために適当であると信じられる理由を示す根拠が含まれることになる。

附属書F：　用語集と略語

F.1 技術的定義

ActiveSync	モバイル環境とデスクトップ環境との間でデータを同期化するための Microsoft のプロトコル
IMAP	Internet Message Access Protocol—TCP/IP 上で電子メールクライアントが電子メールサーバから電子メールを取り出すためのプロトコル；IMAP4 は RFC 3501 に定義されている
MAPI	Messaging Application Programming Interface for HTTP—電子メールの送信/受信のため Microsoft Exchange により用いられるプロトコル；MS-OXCMAPIHTTP に定義されている
MUA	メールユーザエージェント (Mail User Agent)
MTA	メール転送エージェント (Mail Transfer Agent)
POP	Post Office Protocol—TCP/IP 上で電子メールクライアントが電子メールサーバから電子メールを取り出すためのプロトコル；POP3 は RFC 1939 に定義されている
RPC	Remote Procedure Call—MAPI コマンドを送信/受信するため Microsoft Exchange により用いられるプロトコル; MS-OXCRPC に定義されている
SMTP	Simple Mail Transfer Protocol—TCP/IP 上で電子メールクライアントが電子メールサーバへ電子メールを送信するためのプロトコル；SMTP は RFC 5321 に定義されている

F.2 コモンクライテリア定義

保証 (Assurance)	TOE が SFR を満たしているという確信の根拠 [CC1]。
CC	コモンクライテリア (Common Criteria)
PP	プロテクションプロファイル (Protection Profile)
SAR	セキュリティ保証要件 (Security Assurance Requirement)

SFR	セキュリティ機能要件 (Security Functional Requirement)
セキュリティターゲット (Security Target) (ST)	特定の識別された TOE に関するセキュリティニーズについての実装依存のステートメント。
評価対象 (Target of Evaluation) (TOE)	評価中のソフトウェア、ファームウェア及びハードウェアのセットで、ガイダンスを伴う。
TOE セキュリティ機能 (TSF)	SFR の正しい実施のために信頼されなければならない TOE のすべてのハードウェアとソフトウェア、及びファームウェアが結合された機能
TOE 要約仕様 (TOE Summary Specification) (TSS)	TOE における SFR 実装の記述を評価者に提供する文書。

F.3 略語

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CRL	証明書失効リスト (Certificate Revocation List)
CSP	暗号サービスプロバイダ (Cryptographic Service Provider)
DHE	Diffie-Hellman 鍵交換 (Diffie-Hellman Key Exchange)
DN	識別名 (Distinguished Name)
DSA	デジタル署名アルゴリズム (Digital Signature Algorithm)
ECC	楕円曲線暗号 (Elliptic Curve Cryptography)
ECDSA	楕円曲線デジタル署名アルゴリズム (Elliptic Curve Digital Signature Algorithm)
FFC	有限体暗号 (Finite-Field Cryptography)
FIPS	連邦情報処理規格 (Federal Information Processing Standards)
GCM	Galois/Counter Mode
HMAC	Keyed Hash Message Authentication Code
HTML	ハイパーテキストマークアップ言語

	(HyperText Markup Language)
HTML5	ハイパーテキストマークアップ言語バージョン 5 (HyperText Markup Language version 5)
HTTP	ハイパーテキスト転送プロトコル (HyperText Transfer Protocol)
HTTPS	ハイパーテキスト転送プロトコルセキュア (HyperText Transfer Protocol Secure)
IETF	インターネットエンジニアリングタスクフォース (Internet Engineering Task Force)
IV	初期化ベクトル (Initialization Vector)
KAT	既知解テスト (Known Answer Test)
KDF	鍵導出関数 (Key Derivation Function)
NIST	国立標準技術研究所 (National Institute of Standards and Technology)
OCSP	オンライン証明書状態プロトコル (Online Certificate Status Protocol)
OID	オブジェクト識別子 (Object Identifier)
PDF	ポータブル文書フォーマット (Portable Document Format)
RFC	Request for Comment (IETF)
RSA	Rivest Shamir Adelman
SHA	セキュアハッシュアルゴリズム (Secure Hash Algorithm)
TLS	トランスポート層セキュリティ (Transport Layer Security)