ボイスオーバーIP (VoIP) アプリケーションの
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_voip_v1.2.pdf

2013 年 10 月 21 日
バージョン 1.2

平成 26 年 10 月 31 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

目次

表のリスト

図のリスト

改版履歴

バージョン	日付	内容
0.6	2013 年 1 月	初版発行
1.2	2013 年 10 月	TOE の詳細化に、VoIP アプリケーションがデバイスプラットフォームと対話することを可能とする API を含めた。TOE、運用環境 (プラットフォーム)、またはその両方によって満たされる必要があるかどうかを反映して、選択済み要件及び保証アクティビティを構造化。

1 概論

本プロテクションプロファイル (PP) は、認証されたリモートエンドポイントまたはサーバへのセキュアなトンネルを提供するために、市販の VoIP アプリケーションの調達をサポートするものである。本 PP では、VoIP アプリケーションとそのサポート環境のための、方針、前提条件、脅威、セキュリティ対策方針、セキュリティ機能要件、及びセキュリティ保証要件を詳述する。

ここでの主な意図は、VoIP アプリケーションによって対処されることになる脅威へ対抗するために必要とされるセキュリティ機能要件を、明確に開発者へ伝えることである。セキュリティターゲット (ST) の TOE 要約仕様 (TSS) の記述には、製品 (評価対象) のアーキテクチャ、及び重要なセキュリティトランザクションが正しく実装されていることを保証するために用いられるメカニズムが文書化されていることが期待される。

1.1 TOE の概要

本文書は、VoIP アプリケーションのセキュリティ機能要件 (SFR) を特定する。VoIP は、2つのエンドポイント間でのプライベートな音声データの保護された伝送を提供する。本 PP の文脈において、VoIP アプリケーションは電話利用者によって利用されるためにインストールされるワークスペースの一部である。VoIP インフラストラクチャは、そのサイズと複雑さの両面において大きく変動する可能性がある。セション境界コントローラ (SBC)、ゲートウェイ、トランキング (trunking)、及びネットワークアドレス変換 (NAT) ならびにファイアウォールトラバーサルなど、多くの種類の機能が可能であり、望まれることが多く、そして時には必要となる。本 PP の文脈において VoIP アプリケーションは、SIP サーバと対話する VoIP クライアントとみなされる。SIP サーバは、SIP リクエストとレスポンスによって VoIP 呼を確立し、処理し、そして終了するための呼セション管理に必要とされる、レジストラ (registrar) 及びプロキシ機能を提供する。

本 PP によって定義される TOE は、リモートアクセスクライアント上で実行されるコンポーネントである VoIP クライアントアプリケーションであるとともに、VoIP クライアントアプリケーションが他のアプリケーションやクライアントデバイスのプラットフォーム (TOE の運用環境の一部) と対話することを可能とする API である。

1.2 TOE の利用方法

VoIP アプリケーションは、リモート VoIP アプリケーションへのセキュアなトンネルの提供を意図している。このトンネルによって、公共ネットワーク上を経由する情報の機密性、完全性、及びデータ認証が提供される。VoIP アプリケーションは、セション記述プロトコル (SDP) 及び SDP のためのメディアストリーム用セキュリティ記述 (SDES) (訳注：RFC4568) を用いて確立されたセキュリティリアルタイムトランスポートプロトコル (SRTP) を用いてピア VoIP アプリケーションと対話することになる。本文書に適合するすべての VoIP アプリケーションは、SDES-SRTP をサポートする。同様に、適合 TOE は自分自身と SIP サーバとの間の通信も、トランスポート層セキュリティ (TLS) によって保護されたシグナリングチャネルを用いることによって保護しなければならない (must)。TOE をドメイン内に登録するためには、TOE が SIP サーバによってパスワード認証されることが必要とされる。TOE には、TLS 接続上の SIP サーバ側と TOE そのものとの両方を、証明書を用いて認証することが、本 PP によって要求される。

図 1 に示すように、TOE は保護されたチャネルを介して、複数の VoIP クライアントや SIP サーバと通信を行う。赤色で示したコンポーネントが、本 PP の対象となる。青色で示したコンポーネントは、関連する PP の対象となる。

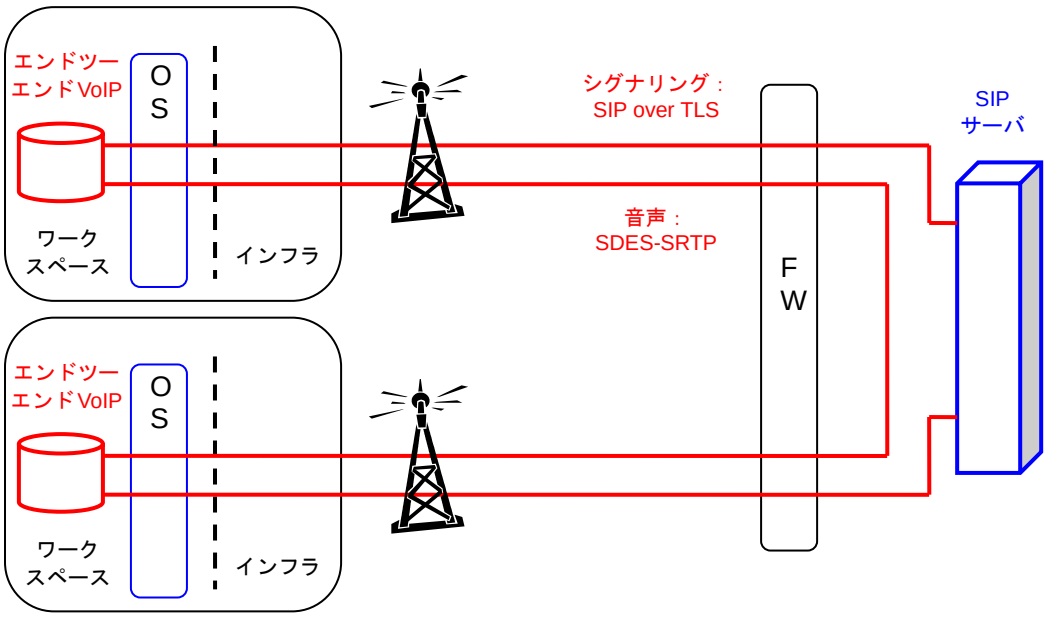

図 1：VoIP 通信

VoIP アプリケーションは適切に実装され、重大な設計ミスが含まれないことが前提となる。VoIP アプリケーションはクライアントマシン保護メカニズムと同様に、その適切な実行に関しては運用環境に依存している：監査レビュー、監査格納、識別と認証、セキュリティ管理、及びセション管理。ベンダは、サポートされているすべての運用環境においてクライアントマシンと TOE を正しくインストールし管理するための設定ガイダンス (AGD_PRE、AGD_OPE) を提供することが要求される。

2 セキュリティ課題記述

本 PP は、利用者が公共ネットワークに依存してセキュアな音声通信を確立する状況へ対処するために作成されている。通信中のデータを暴露や改変から保護するため、セキュアな通信を確立するため VoIP トンネルが作られる。VoIP アプリケーションは、このセキュアな VoIP トンネルの一端を提供し、ネットワークパケットの暗号化及び復号を行う。VoIP アプリケーションの適切な設置、設定、及びアップデートは、その正しい運用のために重要であり、これらの対策方針も同様に含まれる。

附属書 A : 参考表には、セキュリティ課題記述 (SPD) をさらに「伝統的」な形で提示する。

2.1 利用者及び TOE データへの不正なアクセス (T.UNAUTHORIZED_ACCESS)

本 PP には、内部関係者による脅威に対抗して保護できるような要件は含まれていない。正当な利用者は、敵対的、または悪意があるとはみなされず、適切なガイダンスへ従うと信頼されている。正当な要員のみが、VoIP アプリケーションのインストールされたクライアントデバイスへアクセスするべきである (should)。したがって、主要な脅威エージェントは、アクセスを得ようと試行するような、権限のないエンティティである。

音声通信のリモートエンドポイントは、地理的にも論理的にも TOE から遠く、さまざまな他のシステムを通過する可能性がある。これらの中間システムは敵対者の管理下にあるかもしれず、またそれらによってネットワークを介した通信が侵害される機会が生ずるかもしれない。

ネットワークを介した平文の通信は、重要なデータ (パスワード、設定及び利用者データな

ど) が中間システムによって直接傍受されたり操作されたりして、TOE の侵害を引き起こす可能性がある。SDES-SRTP は、この通信の保護を提供するために利用可能である；しかし、RFC に列挙されたプロトコル仕様に適合するプロトコルとして実装可能な数えきれない選択肢が存在する。これらの選択肢の一部は、接続のセキュリティに悪影響を与える可能性がある。例えば、弱い暗号アルゴリズム (RFC で許可されているものであっても、DES のようなもの) によって、敵対者が暗号化されたチャネル上のデータを傍受したり、または操作することさえ可能となり、その結果このような攻撃を防止するために用意された対策を迂回できてしまうかもしれない。さらに、ほとんど使われない、または非標準の選択肢であるプロトコルが実装されている場合、プロトコル仕様には適合しているかもしれないが、他の、大企業で典型的である多様な機器とは対話できないだろう。

通信経路が保護されていたとしても、リモート SIP サーバは、悪意のある第三者のユーザまたはシステムが TOE であると思うよう騙されることがある。例えば、中間者が TOE への接続要求を傍受して、あたかも TOE であるかのように SIP サーバへ応答するかもしれない。同様に、TOE もまた、実際には本物ではないが正規のリモート SIP サーバと通信を確立していると思うよう騙されるかもしれない。また攻撃者が悪意のある中間者タイプの攻撃を仕掛けることによって中間システムが侵害され、このシステムによってトラフィックがプロキシされ、検査され、そして改変されてしまうことも起こり得る。この攻撃は、暗号化された通信チャネルを介した場合であっても、適切な対策が適用されていない場合には埋め込まれる可能性がある。このような攻撃の一部は、悪意のある攻撃者がネットワークトラフィック (例えば、認証セション) をキャプチャし、そのトラフィックを「プレイバック」して、正規のリモートエンティティと通信しているとエンドポイントに思い込ませることによって可能となる。

2.2 TSF の設定不可能 (T.TSF_CONFIGURATION)

VoIP トンネルの設定は複雑で時間のかかるプロセスであり、それを行うためのインタフェースが明確に特定されていなかったり、ふるまいが正しくなかったりする場合、エラーを引き起こしかねない。インタフェースのあるの側面について設定できない事態は、望ましい通信ポリシーや、特定の利用者のサイトについて望ましいまたは要求されるであろう暗号技術の利用における誤った仕様につながる可能性もある。これによって、利用者は自分のデータが保護されていると考える一方で、意図しない弱点、または平文での通信を引き起こすかもしれない。TOE の設定、またはそのセキュリティメカニズム (例えばアップデートのプロセス) の利用におけるその他の側面もまた、VoIP アプリケーションの信頼性の低下につながる可能性がある。

2.3 悪意のあるアップデート (T.UNAUTHORIZED_UPDATE)

よく利用される攻撃ベクトルのひとつに、既知の欠陥を含むソフトウェアのパッチ適用がされていないバージョンへの攻撃を利用するものがあるため、VoIP クライアントをアップデートすることで、脅威環境への変更が対処されることを保証する必要がある。パッチをタイムリーに適用することでクライアントが「攻略しにくい標的」であることを保証し、その結果その製品がセキュリティ方針を維持し実施する可能性が増大する。しかし、製品に適用されるアップデートは何らかの形で信頼できるものでなければならない (must)；さもなければ、攻撃者がルートキット、ボット、また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」を書き込むことができてしまう。このような「アップデート」がいったんインストールされると、攻撃者はそのシステムとすべてのデータを管理できてしまう。

この脅威へ対抗する手法には、通常、アップデートのハッシュを追加したり、、同様にこれらのハッシュに対して暗号操作 (例えば、デジタル署名) 追加することもある。しかし、これらの手法の有効性は、追加的な脅威をもたらす。例えば、弱いハッシュ関数によって、ハッシュが未改変のままで正規のアップデートを改変することが、攻撃者にとって可能となってしまうかもしれない。暗号署名スキームについては、以下への依存性が存在する。

1) 署名の提供に用いられる暗号アルゴリズムの強度、及び
2) エンドユーザが署名を検証する能力 (これには通常、信頼のルート (認証局) までさかのぼってデジタル署名の階層構造をチェックすることが必要となる)。

暗号署名スキームが弱ければ、攻撃者によって侵害される可能性があり、その場合エンドユーザが悪意のあるアップデートを正規のものと思い込んでインストールしてしまうことになる。同様に、信頼のルートが侵害されるような可能性がある場合、強力なデジタル署名アルゴリズムであっても悪意のあるアップデートのインストールを防ぐことはできなくなる (攻撃者が単純に、侵害された信頼のルートを用いて自分自身のアップデートの署名を作成すれば、その悪意のあるアップデートは検出されることなくインストールされてしまうことになる)。

2.4 TSF の故障 (T.TSF_FAILURE)

TOE のセキュリティメカニズムは、一般的にはプリミティブな一連のメカニズム (例えば、メモリ管理、プロセス実行の特権モード) から、より複雑な一連のメカニズムが構築される。プリミティブなメカニズムの故障によって、より複雑なメカニズムの侵害がもたらされ、結果として TSF の侵害が生じるかもしれない。

3 セキュリティ対策方針

適合 TOE は、TOE の脅威に対抗するセキュリティ機能を提供し、また法令により強制される方針を実施する。以下のセクションでは、適合 TOE へ取り込まれるべく先に議論した脅威に照らして、このような機能についての記述を提供する。セキュリティ対策方針は、セクション 2 から導出された、評価対象 (TOE) 及び運用環境に関する要件である。

3.1 セキュアトンネルの確立

セクション 2.1 に記述された、TOE と SIP サーバの間、またはリモート VoIP アプリケーションの間での機微なデータの送信についての課題へ対処するため、適合 TOE は自身と SIP サーバの間、またはリモート VoIP アプリケーションの間の通信経路へ暗号化されたチャネルを提供する。これらのチャネルは、TLS 及び SDES-SRTP を用いて実装される。TLS と SDES-SRTP は、さまざまな実装上の選択を提供する RFC によって特定される。相互運用性と暗号攻撃への耐性を提供するため、これらの選択の一部 (特に、暗号プリミティブに関するもの) に要件が課されている。適合 TOE は ST で特定されたすべての選択をサポートしなければならない (must) が、追加のアルゴリズムやプロトコルをサポートしてもよい。そのような追加のメカニズムが評価されない場合、それらが評価されていないという事実が明確にするため、管理者に対してガイダンスが提供されなければならない (must)。

通信での暴露(及び改変の検出) からの保護を提供する以外にも、TLS と SDES-SRTP は暗号技術的にセキュアな方法で各エンドポイントの双方向認証を提供する。これは、たとえ 2 つのエンドポイントの間に悪意のある攻撃者が存在したとしても、通信路のいずれかのエンドポイントに対して通信相手として攻撃者が偽ろうとするいかなる試行も検出されることを意味する。この認証は、X.509 証明書を用いて行われ、より大きな保証を認証に提供する。TLS 及び SDES-SRTP プロトコルに関する要件は、プロトコルそのものの構造の他、セクション 2.1 に記述されているリプレイ攻撃に対する保護も提供する。

(O.SECURE_TUNNEL → FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM_EXT.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FIA_SIPC_EXT.1, FCS_SRTP_EXT.1, FCS_TLS_EXT.1, FIA_X509_EXT.1, FTP_ITC.1)

3.2 TOE の設定

セクション 2.2 に記述された、TOE の設定に関連した問題へ対処するため、TLS 及び SDES-SRTP ならびにこれらのプロトコルをサポートする基本的な暗号メカニズムの設定、X.509 証明書の取扱い、そして TOE へのアップデートを管理するためのインタフェースを TOE は提供する。

(O.TOE_CONFIGURATION → FMT_SMF.1)

3.3 検証可能なアップデート

セクション 2.3 で概説したように、クライアントへのアップデートが信頼できることの検証失敗は、セキュリティ機能の侵害につながる可能性がある。アップデートへの信頼を確立する最初のステップは、アップデートのインストールする前に検証可能なアップデートのハッシュを公開することである。これにより、ダウンロードされたアップデートが公開されたハッシュと結びついたものであることを証明するが、アップデートのソースとハッシュの組み合わせが侵害されていたり、信頼できないかどうかを示すものできない。アップデートのソースへの信頼を確立するために、アップデートを取得し、TOE の提供するデジタル署名メカニズムを通してアップデートを暗号技術的にチェックし、そしてアップデートをインストールするために、暗号メカニズムと手続きが提供される。

(O.VERIFIABLE_UPDATES → FPT_TUD_EXT.1, FCS_COP.1(2), FCS_COP.1(3), FIA_X509_EXT.1)

3.4 TSF セルフテスト

TSF によって利用される基本的なセキュリティメカニズムの故障の一部を検出するため、TSF はセルフテストを行う。このセルフテストの範囲は製品開発者に委ねられているが、より広範囲のセルフテストが、エンタープライズアーキテクチャ開発用プラットフォームをより信頼できるものするに違いない (should)。

(O.TSF_SELF_TEST → FPT_TST_EXT.1)

4 セキュリティ要件

本セクションに含まれる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 改訂第4版* (CC) 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。本セクションに含まれるセキュリティ保証要件は、CC のパート 3 から導出されたものである。補足的なガイダンスは、機能要件と関連した保証アクティビティの形でセクション 4.2 及び 4.3 に、同様にセキュリティ保証要件についてはセクション 4.4 に提供される。

4.1 表記法

CC は、セキュリティ機能要件 (SFR) に関する操作を定義している：割付、選択、選択及び詳細化における割付。本文書では、以下のフォント規則を用いて、CC によって定義された操作を特定するため、以下のフォント表記法を用いる：

- 割付：*イタリック体*のテキストで表記される；
- PP 作成者による詳細化：必要に応じて、エレメント番号の後に**太字**の「詳細化」と追加された**太字**テキスト、及び取り消し線による削除により表記される；
- 選択：<u>下線付き</u>テキストで表記される；
- 選択中の割付：<u>*イタリック体の下線付き*</u>テキストで表記される；
- 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表記される。

明示的に書かれた SFR は、TOE SFR の要件名の後にラベル「EXT」を付けることで識別される。

4.2 VoIP アプリケーションのセキュリティ機能要件 (TOE)

本 PP の本体にあるセキュリティ機能要件は、VoIP アプリケーション (TOE) が満たさなければならない (must) ものと、TOE または動作プラットフォームのいずれかによって満たされなければならない (must) ものとに大別される。本セクションは、TOE によって満たされなければならない (must) 要件が述べられている。

4.2.1 暗号サポート (FCS)

FCS_CKM.2(1)　　詳細化：暗号鍵ストレージ

FCS_CKM_EXT.2(1)　　暗号鍵ストレージ

FCS_CKM_EXT.2.1(1) VoIP クライアントアプリケーションは、永続的な秘密鍵及びプライベート鍵を使用していない際には、プラットフォームによって提供され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：

この要件によって、永続的な秘密鍵と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が確実となる。

この要件は、VoIP クライアントアプリケーションによって用いられる永続的な秘密鍵とプライベート鍵がプラットフォームによって保存されることを前提としている。

保証アクティビティ：

評価者は TSS を検査して、利用者クレデンシャル、証明書、永続的な秘密鍵及びプライベート鍵が保存される方法が詳細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、鍵材料が暗号化されずに永続的メモリへ書き込まれることがないこと、また鍵材料がプラットフォームによって保存されること、を決定するために TSS をレビューする。

FCS_SRTP_EXT.1　　セキュアリアルタイムトランスポートプロトコル (SRTP)

FCS_SRTP_EXT.1.1 VoIP クライアントアプリケーションは、RFC 3711 に準拠するセキュアリアルタイムトランスポートプロトコル (SRTP) を実装し、また RFC 4568 に準拠したメディアストリーム用セキュリティ定義 (SDES) を用いて SRTP 接続の鍵情報を提供しなければならない (shall)。

FCS_SRTP_EXT.1.2 VoIP クライアントアプリケーションは、RFC 4568 に従って以下の暗号スイートをサポートする SDES-SRTP を実装しなければならない (shall)：AES_CM_128_HMAC_SHA1_80。

FCS_SRTP_EXT.1.3 VoIP クライアントアプリケーションは、SRTP NULL アルゴリズムが無効化できることを確実にしなければならない (shall)。

FCS_SRTP_EXT.1.4 VoIP クライアントアプリケーションは、SRTP ポートが SRTP 通信に利用されるよう正当な管理者によって特定されることを許可しなければならない (shall)。

適用上の注意：

この要件は、VoIP トラフィックを搬送するために用いられる SRTP セションが、特定された暗号スイートを用いた SDES ダイアログに従って鍵選択されることを特定している。将来は、Suite B 暗号スイートが利用可能となる。

保証アクティビティ：

評価者は TSS を検査して、着呼及び発呼の両方に対して、SRTP セションがどのようにネゴシエーションされるか記述されていることを検証しなければならない (shall)。これには、鍵材料がどのように確立されるか、そして NULL または他の許可されない暗号スイート利用要求がどのように TSF によって拒否されるかが含まれる。また評価者は、以下のテストを行わなければならない (shall)。

- *テスト 1：評価者は、デバイスを初期化するための手続きに従わなければならない (shall)、それによってデバイスが着信と発信を行う準備ができる。次に評価者は、呼の発信と着信の両方を行って、TOE によって送信及び受信されるトラフィックが暗号化されていることを決定しなければならない (shall)。呼が暗号化されることを保証するため、また使用されている暗号スイートを目視するため、パケットキャプチャツールが用いられるべきである (should)。TLS-SIP トラフィックを復号し、SDES ネゴシエーションを目視するため、SIP サーバのプライベート鍵がパケットキャプチャツールへロードされる必要がある。*

4.2.2 利用者データ保護 (FDP)

FDP_VOP_EXT.1　　ボイスオーバーIP データの保護

FDP_VOP_EXT.1.1 VoIP クライアントアプリケーションは、VoIP 呼が保留されている際、VoIP 呼が消音されている際、VoIP 呼が接続されていない場合、及び [割付：その他のアクション、その他のアクションなし] に音声データの送信を停止しなければならない (shall)。

保証アクティビティ：

評価者は TSS を検査して、この要件の各機能の実装方法が記述されていることを検証しなければならない (shall)。また評価者は、以下のテストを行わなければならない (shall)。

- *テスト 1：評価者は、デバイスを初期化するための手続きに従って、デバイスが着信と発信を行えるよう準備しなければならない (shall)。パケットキャプチャツールを用いて、発呼／着呼が行われるまで音声トラフィックが送信されないことを評価者は検証しなければならない (shall)。評価者は発呼を行って、音声トラフィックがセキュアなチャネルを介して送信されていることを検証しなければならない (shall)。次に評価者は列挙された機能のそれぞれ (消音、保留、切断、及びそ*

の他の特定されたアクション) を実行して、音声トラフィックがもはや送信されてい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、デバイスを初期化するための手続きに従って、デバイスが着信と発信を行えるよう準備しなければならない (shall)。パケットキャプチャツールを用いて、発呼／着呼が行われるまで音声トラフィックが送信されないことを評価者は検証しなければならない (shall)。評価者は着呼を行って、音声トラフィックがセキュアなチャネルを介して送信されていることを検証しなければならない (shall)。次に評価者は列挙された機能のそれぞれ (消音、保留、切断、及びその他の特定されたアクション) を実行して、音声トラフィックがもはや送信されていないことを検証しなければならない (shall)。*

4.2.3 識別と認証 (FIA)

TOE のベースライン要件は I&A に関しては比較的限定されている。これは形式的な管理利用者や一般利用者が定義されていないためである。TOE によって行われることが要求される I&A の範囲は、TLS、及び SDES/SRTP 接続を確立する際にマシンレベルで行われる認証に関連したものである。したがって、本セクションの要件は、本 PP で特定されるプロトコルによって用いられるクレデンシャルのみをカバーする。

FIA_SIPC_EXT.1　　セション確立プロトコル (SIP) クライアント

FIA_SIPC_EXT.1.1 VoIP クライアントアプリケーションは、RFC 4566 に準拠するセション記述プロトコル (SDP) を用いて VOIP トラフィックの搬送に用いられるマルチメディアセションを記述する、RFC 3261 に準拠するセション確立プロトコル (SIP) を実装しなければならない (shall)。

FIA_SIPC_EXT.1.2 VoIP クライアントアプリケーションは、利用者にパスワードの入力を要求し、RFC 3261 のセクション 22 で特定される SIP REGISTER 機能要求へのパスワード認証の使用をサポートしなければならない (shall)。

FIA_SIPC_EXT.1.3 VoIP クライアントアプリケーションは、{大文字、小文字、数字、及び以下の特殊文字： “!”、“@”、“#”、“$”、“%”、“^”、“&”、“*”、“(“、及び “)”、ならびに [割付：その他のサポートされる特殊文字]} のセットから少なくとも [割付：8 以上の正の整数] 文字が含まれる SIP 認証パスワードをサポートしなければならない (shall)。

FIA_SIPC_EXT.1.4 FIA_SIPC_EXT.1.2 に従って利用者が入力するパスワードは、REGISTER 要求が成功したことを VoIP クライアントアプリケーションが通知された際に VoIP クライアントアプリケーションによってクリアされなければならない (shall)。

適用上の注意：

(SIP サーバによって) 認証される必要のある唯一の SIP 要求は REGISTER 要求である；TOE は、利用者が入力するパスワードを提供することによってこれをサポートする。SIP サーバは強制を行って正しいパスワードが提示された際にのみ利用者を登録する一方で、上記のエレメントによってクライアントには少なくとも 8 文字の長さ (最大の長さは 2 番目の割付で特定される) であって、FIA_SIPC_EXT.1.3 で特定される文字 (TOE の許可する文字だがエレメントに明示的に列挙されていないものは最初の割付で特定されるべきであり (should)、それ以外の場合には「その他の文字なし」が受容可能な割付である) を含むことのできるパスワードをサポートし、さらに REGISTER 要求の送信時に利用者へパスワードのプロンプトを表示することが要求される。

FIA_SIPC_EXT.1.4 エレメントの意図は、SIP 登録に用いられる平文パスワードがデバイス上に保持されないことである。再度 REGISTER 機能の送信が必要となった場合に使えるように、このパスワードから導出される値 (例えばハッシュ) を保存しておくことは許容可能である。

保証アクティビティ：

評価者は TSS を検査して、SIP セションがどのように確立されるのか記述されていることを検証しなければならない (shall)。これには SIP セションの開始、利用者の登録、そして発呼と着呼の両方が取り扱われる (初期化され、記述され、そして終了される) 方法が含まれなければならない (shall)。またこの記述には、パスワードが利用者によって入力された時点から TSF によってクリアされる時点までの取り扱いの記述も含まれなければならない (shall)。

また評価者は、以下のテストを行わなければならない (shall)。

- *テスト 1：評価者は、SIP サーバへの接続の確立を含め、デバイスを初期化する手順にしたがわなければならない (shall)。評価者は、SIP REGISTER 要求が成功して完了する前に、パスワードのプロンプトが表示されることを確認しなければならない (shall)。*
- *テスト 2：評価者は、SIP サーバへの接続の確立を含め、デバイスを初期化する手順にしたがわなければならない (shall)。評価者は、正しくないパスワードを入力するとデバイスが SIP サーバに登録されない (例えば、発呼や着呼が成功しない) 結果となることを確認しなければならない (shall)。また評価者は、正しいパスワードを入力するとデバイスの登録が成功することを (例えば、発呼や着呼ができることによって) 確認しなければならない (shall)。*
- *テスト 3：評価者は、FIA_SIPC_EXT.1.3 に特定される長さと文字セットを代表するような、さまざまなパスワードが TOE に受け付けられることを示せるようなテスト環境を設定しなければならない (shall)。テスト報告書には、用いられたテストセットが許可された長さと文字を代表するものであることを示す、評価者による根拠が含まれなければならない (shall)。*

4.2.4 セキュリティ管理 (FMT)

TOE が別個の管理役割を維持管理することは要求されていない。しかし、一般利用者には利用可能とすべきではない (should not) TOE 操作の特定の側面を設定する機能を提供することは要求されている。

FMT_SMF.1　　管理機能の仕様

FMT_SMF.1.1 VoIP クライアントアプリケーションは、以下の管理機能を行えなければならない (shall)。

- 接続に用いる SIP サーバの特定、
- 接続に用いる VoIP クライアントクレデンシャルの特定、
- SIP 認証のパスワード要件の特定、
- 本 PP の別のセクションで特定されるすべてのセキュリティ管理機能を設定できる能力、
- [選択：視覚的警報通知、 [割付：任意の追加的管理機能]、その他の機能なし]。

適用上の注意：

設置の際、VoIP クライアントアプリケーションは IT 環境に依存して管理者をクライアントマシンへ認証させる。

保証アクティビティ：

評価者は、PP によって義務付けられるすべての管理機能が操作ガイダンスに記述され、その記述にはその管理機能と関連付けられた管理職務を行うために必要な情報が含まれていることを確認するためにチェックしなければならない (shall)。評価者は、TOE を設定して

上記要件に列挙されるオプションのそれぞれをテストすることによって、管理機能を提供する TOE の能力をテストしなければならない (shall)。評価者には、ST 及びガイダンス文書に言明される設定管理方法のすべてにおいて、この機能をテストすることが期待される。

ここでのテストは、例えば FCS_TLS_EXT.1 のような他の要件のテストと組み合わせて実施されてもよいことに注意されたい。

4.2.5 TSF の保護 (FPT)

FPT_TUD_EXT.1　　拡張：高信頼アップデート

FPT_TUD_EXT.1.1 TSF は、TOE ファームウェア／ソフトウェアの現在のバージョンを問い合わせる能力をクライアントデバイスプラットフォームへ提供しなければならない (shall)。

適用上の注意：

TOE へのあらゆるアップデートはプラットフォームの機能によって取り扱われることになるため、TOE 自身の機能ではない。しかし、アップデートを行うかどうかの判断を容易にするために、TOE は自分のバージョンをプラットフォームへ正しく報告する能力を持たなければならない (must)。

保証アクティビティ：

評価者は TSS をチェックして、TOE が自分の現在のバージョンを報告する手法が記述されていることを判断しなければならない (shall)。TOE ガイダンスには、TOE の現在のバージョンを取得するために必要な呼出しシーケンスが含まれなければならない (shall)。

評価者は、以下のテストを行わなければならない (shall)。

- *テスト 1：評価者は、TOE の現在のバージョンを問い合わせるプラットフォーム機能を呼び出さなければならない (shall)。評価者は、TOE の現在のバージョンが返されることを確認しなければならない (shall)。*

4.2.6 高信頼パス／チャネル (FTP)

FTP_ITC.1(1)　　TSF 間高信頼チャネル (SDES-SRTP)

FTP_ITC.1.1(1) **詳細化**: VoIP クライアントアプリケーションは、他の通信チャネルとは論理的に分離されていると共に、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改変**及び**開示からの保護を提供する、**FCS_SRTP_EXT.1 で特定される SDES-SRTP を用いた**それ自身と**リモート VoIP アプリケーション**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(1) VoIP クライアントアプリケーションは、TSF またはリモート VoIP アプリケーション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(1) VoIP クライアントアプリケーションは、 [2 つのデバイス間のすべての通信] 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)。

適用上の注意：

この要件は、他のデバイス上の VoIP アプリケーションと TOE との間の通信が確立され、両者ともプロトコルの意味でピアとしてふるまう場合に対応する。

この要件は、通信が最初に確立される際だけではなく、中断後に再開する際にも保護されることを意味している。TOE 設定の一部に、他の通信を保護するトンネルを手作業で設定することが必要となる場合があるかもしれない。また中断後に TOE が (必要とされる) 人手での介入を伴って自動的に通信の再確立を試行する場合、攻撃者が重要な情報を得たり接続を侵害できたりするウィンドウが形成されることがあるかもしれない。

保証アクティビティ：

評価者はTSS セクションを検査して、この要件がTOE 内で実装される方法と、仕様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確認しなければならない (shall)。また評価者は、TSS に列挙されたすべてのプロトコルが特定され、ST の要件に含まれていることを確認しなければならない (shall)。評価者は、ピア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と、万一接続が意図せず切断されてしまった際の回復の指示が含まれていることを確認しなければならない (shall)。評価者は、通信がTSF とリモートVoIP アプリケーションの両方から開始できることを検証しなければならない (shall)。また評価者は、以下のテストを行わなければならない (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って、TOE が要件に特定されたプロトコルを用いてリモートVoIP アプリケーション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、リモートVoIP アプリケーション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)。*
- *テスト3 : 評価者は、リモートVoIP アプリケーションとの通信チャネルのそれぞれについて、チャネルデータの改変がTOE によって検出されることを保証しなければならない (shall)。*
- *テスト4 : 評価者は、TOE からリモートVoIP アプリケーションへの接続を物理的に中断しなければならない (shall)。評価者は少なくとも、接続を自動的に再開しようとする、または新たなリモートVoIP アプリケーションへ接続しようとするあらゆる試行の場合において、それ以降の通信が適切に保護されることを保証しなければならない (shall)。*

これ以外の保証アクティビティは、特定のプロトコルと関連付けられる。

4.3 VoIP クライアントアプリケーションまたはクライアントプラットフォームのセキュリティ機能要件

本 PP 本体のセキュリティ機能要件は、VoIP アプリケーション (TOE) によって満たされるべき (must) ものと、TOE またはその動作するプラットフォームのいずれかによって満たされるべき (must) ものとに大別される。本セクションには、満たされなければならない (must) が、TOE または TOE の動作するプラットフォームのいずれによっても満たすことのできる要件が含まれている。各要件には、 VoIP クライアントアプリケーションとクライアントプラットフォームのどちらが要件の機能を行うのかを ST 作成者が示すための選択が含まれている。TOE がプラットフォームに依存する場合、そのプラットフォームは VoIP クライアントアプリケーションと並行して、またはその前に評価されなければならない (must)。したがって保証アクティビティは、要件が TOE によって満たされる際に適用されるものと、要求される機能を TOE の動作するプラットフォームが実装する際に行われるものとに分けられる。TOE と TOE プラットフォームのどちらにも具体的に関連付けられていないテストまたは文書化の保証アクティビティが特定される場合には、その要件がどこで実装されるかに関わらず適用される。

TLS、SIP、SDP、そして SDES-SRTP という複数のプロトコルが、呼確立中に用いられることには注意すべきである (should)。これらのプロトコル (そして関連した TSS 及びテスト保証アクティビティ) は別個に特定されるが、包括的な記述とエンドツーエンドの (1 つまたは複数の) テストケースを用いてこれらの機能を記述し論証できることが期待される。

4.3.1 暗号サポート (FCS)

FCS_CKM.1(1) 暗号鍵生成 (非対称鍵)

FCS_CKM.1.1(1) **詳細化：** [選択、少なくとも 1 つを選択：VoIP クライアントアプリケーション、クライアントデバイスプラットフォーム] は、以下に従って**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)。

- 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”、及び

[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”、
- 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”、
- その他のアルゴリズムなし]

また、特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：

このコンポーネントは、用いられるさまざまな暗号プロトコル (例えば IPsec) 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 TOE／プラットフォームが生成できることを要求する。

用いられるべきドメインパラメタは本 PP のプロトコル要件によって特定されているため、TOE／プラットフォームがドメインパラメタを生成することは期待されておらず、したがって本 PP に特定されたプロトコルに準拠するに当たって追加的なドメインパラメタの検証は必要とされない。

保証アクティビティ：

プラットフォームによって満たされる要件

ST に列挙されたプラットフォームのそれぞれについて、評価者はプラットフォームの ST を検査して、そのプラットフォームの ST に主張される鍵確立に VoIP クライアントアプリケーションの ST における鍵確立要件が含ま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、VoIP クライアントアプリケーションの ST の TSS を検査して、(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しなければならない (shall) (これは VoIP アプリケーションによって実装されないメカニズムによって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この保証アクティビティの一部として TSS に特定されることになる)。

TOE によって満たされる要件

この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、以下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のための鍵生成

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)。このテストは、公開鍵検証指数 e、秘密素因数 p 及び q、公開される法 (modulus) n 及び秘密署名指数 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) を特定している。これには、以下のものが含まれる。

1. *ランダム素数：*
   - *証明可能素数*
   - *確率的素数*
2. *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しなければならない (shall)*
   - *素数 p1、p2、q1 及び q2 を証明可能素数とし (shall)、p 及び q を確率的素数としなければならない (shall)*
   - *素数 p1、p2、q1、q2、p 及び q を、すべて確率的素数としなければならない (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 によって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って、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 スキームのための鍵生成

FFC ドメインパラメタ及び鍵生成テスト

評価者は、パラメタ生成及び鍵生成テストを用いて TOE による FFC のためのパラメタ生成及び鍵生成の実装を検証しなければならない (shall)。このテストは、フィールド素数 p、暗号素数 q (p-1 を割り切る)、暗号群生成器 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しなければならない (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しなければならない (shall)*

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

暗号群生成器：

- *検証可能プロセスによって構築された生成器 g*

- *検証不可能プロセスによって構築された生成器 g*

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

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 パラメタセットによって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器 g、また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 によって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って、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 スキームのための鍵生成

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／公開鍵ペアをテスト対象実装 (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改変し、5 個を未改変の (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 によって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)。各鍵共有スキームのためのこれらの検証テストは、勧

告中の仕様に従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) による導出鍵材料 (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。この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、テスト要員は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)。このデータセットは、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、またはその両方である。

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、鍵材料 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って、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 は上記を行わなければならない (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換結果を、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。この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) の一連のテストベクトルを生成する。

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のための詳細なテスト手順は利用できない。行われた選択に応じてTSF が800-56A 及び／または800-56B に適合していることを示すため、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 が適合する適切な 800-56 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 によって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)。*

800-56A 及び 800-56B (選択に応じて) の該当するセクションのそれぞれにおいて、「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.1(2)　　暗号鍵生成

FCS_CKM.1.1(2) **詳細化：** [選択、少なくとも 1 つを選択：VoIP クライアントアプリケーション、クライアントデバイスプラットフォーム] は、以下の特定された暗号鍵生成アルゴリズムに従って**認証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)。 [選択：

- RSA スキームについては、FIPS PUB 186-4, “Digital Signature Standard (DSS)” の附属書 B.3、
- ECDSA 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] の実装については、FIPS PUB 186-4, “Digital Signature Standard (DSS)” の附属書 B.4、
- AES を用いる RSA スキームについては、ANSI X9.31-1998 の附属書 A.2.4]

また、特定された暗号鍵長は *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：

生成された公開鍵はX509v3 証明書の識別情報と関連付けられることが期待されるが、この関連付けはTOE によって行われる必要はなく、運用環境の認証局によって行われることが期待される。

楕円曲線ベースの方式に関しては、鍵サイズは基点の位数の 2 の対数を示す。

ANSI X9.31-1998 の選択肢は、本文書の将来のバージョンでは選択から除かれることになる。現状では、モダンなFIPS PUB 186-4 標準への移行を業界が完了するまでにまだ多少時間がかかるため、この選択はFIPS PUB 186-4 のみに限定されてはいない。暗号署名に関する好ましいアプローチとして、本PP の将来のバージョンでは楕円曲線が要求されることになる。

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。

保証アクティビティ：

プラットフォームによって満たされる要件

ST に列挙されたプラットフォームのそれぞれについて、評価者はプラットフォームの ST を検査して、そのプラットフォームの ST に主張される鍵生成機能に VoIP クライアントアプリケーションの ST における鍵生成要件が含ま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、VoIP クライアントアプリケーションの ST の TSS を検査して、(サポートされるプラットフォームのそれぞれについて) 鍵生成機能が呼び出される方法が記述されていることを検証しなければならない (shall) (これは VoIP アプリケーションによって実装されないメカニズムによって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この保証アクティビティの一部として TSS に特定されることになる)。

TOE によって満たされる要件

TSF が FIPS 186-4 署名スキームを実装する場合、この要件は FCS_COP.1(2) の下で検証される。

ESF が ANSI X9.31-1998 スキームを実装する場合、評価者は鍵ペアが生成される方法が 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)。TSF の実装が ANSI X9.31-1998 に適合していることを示すため、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 が準拠する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 によって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)。*

附属書 B の該当するセクションのそれぞれにおいて、「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　　暗号鍵材料の破壊 (鍵材料)

FCS_CKM_EXT.4.1 **詳細化**： [選択、少なくとも 1 つを選択：VoIP クライアントアプリケーション、クライアントデバイスプラットフォーム] は、すべての平文の秘密鍵及びプライベート暗号鍵ならびにクリティカルセキュリティパラメタ (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：

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)。

「クリティカルセキュリティパラメタ」は FIPS 140-2 に「セキュリティ関連情報 (例えば、共通暗号鍵及びプライベート暗号鍵、ならびにパスワードや PIN などの認証データ) であって、その開示または改変が暗号モジュールのセキュリティの侵害をもたらす可能性のあるもの」と定義されている。

上述のゼロ化は、平文鍵／暗号クリティカルセキュリティパラメタ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／暗号クリティカルセキュリティパラメタが別の場所へ転送された際、適用される。

実際には、要件と関連付けられたすべての機能を TOE が実装することはない。これは、そもそも TOE がゼロ化を行う場合、ストレージ領域のクリア／上書き機能を行うプラットフォームインタフェースを呼び出すことによって行われるためである。本 PP の要件を満たす必要のある鍵の少なくとも 1 つについて、TOE が要件に特定されるデータを操作 (読み出し、書き込み) するためこれらのデータを確実にクリアする必要がある場合には、ST 作成者は「TOE」を選択すべきである (should)。これらの場合、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。

データの一部が TOE によって操作され、その他のデータ全体がプラットフォームによって操作されるというありがちな場合には、ST 作成者はこの要件を繰り返さなければならない (shall)。

保証アクティビティ：

プラットフォームによって満たされる要件

評価者は、秘密鍵 (共通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 要件によって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 に列挙されたプラットフォームのそれぞれについて、評価者はプラットフォームの ST の TSS を検査して、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しなければならない (shall)。

TOE によって満たされる要件

評価者は、秘密鍵 (共通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)。保護されるべき材料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ってゼロ化されるが、内部ハードドライブ上に保存される秘密鍵は各書き込みの前に改変されたランダムパターンを 3 度上書きすることによってゼロ化される」) 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)。

- *<u>テスト 1</u>：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 によって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 によって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、

以下のテストを行わなければならない (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。*

このテストは、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。

評価者はこのテストを、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)。*

FCS_COP.1(1)　　暗号操作 (データの暗号化／復号)

FCS_COP.1.1 **詳細化：** [選択、少なくとも 1 つを選択 : VoIP クライアントアプリケーション、クライアントデバイスプラットフォーム] は、特定された暗号アルゴリズム **CTR、CBC、***及び [選択 : GCM (NIST SP800-38D で特定される)、 [割付 : 1 つ以上のモード]、他のモードなし] で動作する AES* であって、暗号鍵サイズが 128 ビット、及び *[選択 : 256 ビット、192 ビット、その他の鍵サイズなし]* の、以下を満たすものに従って*暗号化及び復号*を行わなければならない (shall)。

- *FIPS PUB 197, “Advanced Encryption Standard (AES)”*
- *NIST SP 800-38A, [選択 : NIST SP 800-38D、その他なし]*

適用上の注意：

本 PP は、SDES 及び TLS プロトコルにおいて CTR 及び CBC モードの使用を要求する (FCS_SRTP, FCS_TLS)。したがって、ST 作成者がこれらのモードを確実に取り込んで PP のプロトコル要件と一貫するよう、FCS_COP.1.1(1) エレメントがここに特定されている。

割付については、ST 作成者は AES が動作する 1 つまたは複数のモードを選択すべきである (should)。最初の選択については、ST 作成者はこの機能によってサポートされる鍵サイズを選択すべきである (should)。第 2 の選択については、ST 作成者は割付中に特定されたモードを記述する標準を選択すべきである (should)。

保証アクティビティ：

プラットフォームによって満たされる要件

ST に列挙されたプラットフォームのそれぞれについて、評価者はプラットフォームの ST を検査して、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 VoIP クライアントアプリケーションの 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しなければならない (shall)。また評価者は、VoIP クライアント

アプリケーションの ST の TSS を検査して、(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、VoIP クライアントアプリケーションの ST で選択されたモードと鍵サイズのそれぞれについて記述されていることを検証しなければならない (shall) (これは VoIP アプリケーションによって実装されないメカニズムによって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この保証アクティビティの一部として TSS に特定されることになる)。

TOE によって満たされる要件

評価者は、ST の選択に基づいて以下のアクティビティを行わなければならない (shall)。

AES-CTR テスト

評価者は、上記の要件をテストする際のガイドとして "The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)" (これらの文書は http://csrc.nist.gov/groups/STM/cavp/index.html から入手できる) から CTR モードに適切なテストを用いなければならない (shall)。このためには、テスト中に検証可能なテストベクトルを作成できるアルゴリズムの信頼できる参照実装を評価者が有していることが必要となる。

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、直接評価者によって、または入力を実装者へ供給しその結果を受領することによって、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って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なければならず (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なければならない (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行わなければならない (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 ビットの鍵としなければならない (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行わなければならない (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 としなければならない (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なければならず (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

ものとしなければならない (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 としなければならない (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しなければならない (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 としなければならない (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行わなければならない (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って、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択し、選択された鍵及び IV によって、テスト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 によって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って、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択し、選択された鍵及び IV によって、テスト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 によって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 ビットの鍵を用いなければならない (shall)。平文と IV の値は、128 ビットのブロックとしなければならない (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なければならない (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。この結果は、既知の良好な実装を用いて同一の値によって 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、以下の入力パラメタ長の組み合わせのそれぞれについて、AES-GCM の認証暗号化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しなければならない (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 (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 としなければならない (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しなければならない (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 (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 ビットとしなければならない (shall)。*

評価者は、上記のパラメ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 認証暗号化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、評価者によって供給されても、テストされている実装によって供給されてもよい。

評価者は、上記のパラメ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、直接評価者によって、または入力を実装者へ供給しその結果を受領することによって、取得することができる。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って得られた結果と比較しなければならない (shall)。

FCS_COP.1(2)　　暗号操作 (暗号署名)

FCS_COP.1.1(2) **詳細化**： [選択、少なくとも 1 つを選択：VoIP クライアントアプリケーション、クライアントデバイスプラットフォーム] は、以下に特定された暗号アルゴリズムに従って**暗号署名サービス (生成及び検証)** を行わなければならない (shall)。

- ***RSA スキームについては、FIPS PUB 186-4, "Digital Signature Standard (DSS)" の附属書 B.3***

[選択：

- ***ECDSA 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] の実装については、FIPS PUB 186-4, "Digital Signature Standard (DSS)"の附属書 B.4***
- ***その他のアルゴリズムなし]***

また、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：

ST 作成者は、デジタル署名を行うために実装されたアルゴリズムを選択すべきである

(should)。2 つ以上のアルゴリズムが利用できる場合、この要件 (及び対応する FCS_CKM.1 要件) はその機能を特定するために繰り返されるべきである (should)。選択されたアルゴリズムについて、ST 作成者は適切な割付／選択を行ってそのアルゴリズムに実装されるパラメタを特定すべきである (should)。

RSA 署名生成及び検証は現在、FCS_TLS_EXT.1 に適合するため要求されている。デジタル署名に関する好ましいアプローチとして、本 PP の将来のバージョンでは ECDSA が要求されることになる。

保証アクティビティ：

プラットフォームによって満たされる要件

ST に列挙されたプラットフォームのそれぞれについて、評価者はプラットフォームの ST を検査して、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 VoIP クライアントアプリケーションの 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しなければならない (shall)。また評価者は、VoIP クライアントアプリケーションの ST の TSS を検査して、(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、VoIP クライアントアプリケーション中に用いられる操作ごとに記述されていることを検証しなければならない (shall) (これは VoIP アプリケーションによって実装されないメカニズムによって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この保証アクティビティの一部として TSS に特定されることになる)。

TOE によって満たされる要件

評価者は、ST の選択に基づいて以下のアクティビティを行わなければならない (shall)。

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)。このテストは、公開鍵検証指数 e、プライベート素因数 p 及び q、公開される法 (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) を特定している。これには、以下のものが含まれる。

1. *ランダム素数：*
    - *証明可能素数*
    - *確率的素数*
2. *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しなければならない (shall)*
    - *素数 p1、p2、q1 及び q2 を証明可能素数としなければならず (shall)、p 及び q を確率的素数としなければならない (shall)*
    - *素数 p1、p2、q1、q2、p 及び q を、すべて確率的素数としなければならない (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 によって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って、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／公開鍵ペアをテスト対象実装 (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改変し、5 個を未改変の (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

CDSA 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のセットを生成し、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)。このテストを行うために評価者は、TSF のサポートする法サイズ／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法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って、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っ

て、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、対応するパラメ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)。これらのテストベクトルを利用して

FCS_COP.1(3)　　暗号操作 (暗号ハッシュ)

FCS_COP.1.1(3) **詳細化**： [選択、少なくとも 1 つを選択：VoIP クライアントアプリケーション、クライアントデバイスプラットフォーム] は、特定された暗号アルゴリズム SHA-1 及び [選択：SHA-256、SHA-384、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 ビット及び [選択：256、384、512 ビット、その他のメッセージダイジェストサイズなし] の、以下：*FIPS PUB 180-3, "Secure Hash Standard"* を満たすものに従って**暗号ハッシュ**を行わなければならない (shall)。

適用上の注意：

本 PP の将来のバージョンでは、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 2013 年 12 月以降には許可されず、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 は現在、FCS_TLS_EXT.1 及び FCS_CKM.1 に適合するため要求されている。

この要件の意図は、ハッシュ関数を特定することである。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、用いられるアルゴリズムの全体的な強度と一貫すべきである (should) (例えば、128 ビットの鍵に SHA-256)。

保証アクティビティ：

評価者は要求されるハッシュサイズ存在する場合の機能を設定するために行われるあらゆる設定決定するため、AGD 文書をチェックする。評価者は、ハッシュ関数と他の 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)。

プラットフォームによって満たされる要件

ST に列挙されたプラットフォームのそれぞれについて、評価者はプラットフォームの ST を検査して、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関数に VoIP クライアントアプリケーションの ST における 1 つまたは複数のハッシュ関数が含ま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、VoIP クライアントアプリケーションの ST の TSS を検査して、 (サポートされるプラットフォームのそれぞれについて) ハッシュ関数が呼び出される方法が、VoIP クライアントアプリケーションの ST で選択されたダイジェストサイズのそれぞれについて記述されていることを検証しなければならない (shall) (これは VoIP アプリケーションによって実装されないメカニズムによって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この保証アクティビティの一部として TSS に特定されることになる)。

TOE によって満たされる要件

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。このモードでは、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。このモードでは、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 によって実装され、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行わなければならない (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

このテストは、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って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従って 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(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) **詳細化：** [選択、少なくとも 1 つを選択：VoIP クライアントアプリケーション、クライアントデバイスプラットフォーム] は、特定された暗号アルゴリズム *HMAC-SHA-1 及び [選択 : HMAC-SHA-256、HMAC- SHA-384、HMAC- SHA-512、その他のアルゴリズムなし]* であって、暗号鍵サイズが *[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 160 及び [選択：256、384、512、その他なし] ビット**の、以下：*FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code、及び FIPS Pub 180-3, "Secure Hash Standard"* を満たすものに従って*鍵付きハッシュによるメッセージ認証*を行わなければならない (shall)。

適用上の注意：

この要件における選択は、鍵付きハッシュメッセージ認証と関連して用いられる鍵長として特定される鍵長と一貫していなければならない (must)。HMAC-SHA-1 は現在、

FCS_TLS_EXT.1 及び FCS_CKM.1 に適合するため要求されているが、本文書の将来のバージョンでは削除されるかもしれない。

上記のメッセージダイジェスト長は、基盤として用いられるハッシュアルゴリズムに対応する。ハッシュの計算後に HMAC の出力を切り捨てることは、さまざまなアプリケーションにおいて適切なステップであることに注意されたい。このことは、この要件への適合性を無効とするものではないが、切り捨てが行われること、最終出力長、そしてこの切り捨てが準拠する標準が ST に言明されるべきである (should)。

保証アクティビティ：

評価者は、鍵付きハッシュ関数と VoIP クライアントアプリケーション ST で特定される他の暗号機能との関連 (これらがプラットフォームによって行われるか、TOE によって行われるかにかかわらず) 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)。

プラットフォームによって満たされる要件

ST に列挙されたプラットフォームのそれぞれについて、評価者はプラットフォームの ST を検査して、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関数に VoIP クライアントアプリケーションの ST における 1 つまたは複数の鍵付きハッシュ関数が含ま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、VoIP クライアントアプリケーションの ST の TSS を検査して、 (サポートされるプラットフォームのそれぞれについて) 鍵付きハッシュ関数が呼び出される方法が、VoIP クライアントアプリケーションの ST で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しなければならない (shall) (これは VoIP アプリケーションによって実装されないメカニズムによって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この保証アクティビティの一部として TSS に特定されることになる)。

TOE によって満たされる要件

さらに、ハッシュの計算後に HMAC の出力が切り捨てられるすべての場合について、この切り捨てがどの操作について行われるか、最終出力のサイズ、そしてこの切り捨てが準拠する標準が言明さ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 TSS を検査して、HMAC 機能によって利用される以下の値が特定されていることを保証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 によって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)。

FCS_RBG_EXT.1　　拡張：暗号操作 (ランダムビット生成)

FCS_RBG_EXT.1.1　[選択、少なくとも 1 つを選択: VoIP クライアントアプリケーション、クライアントデバイスプラットフォーム] 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*] に従って、すべての決定論的ランダムビット生成サービスを行わなければならない (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ってシードを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 または 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を選択すべきである (should)。

NIST Special Pub 800-90 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 800-90 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 (800-90 が選択される場合)、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 (SHA-1, SHA-256, SHA-384, SHA-512) 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。800-90 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、また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って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 に従って 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 に記述されてい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 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って満たされる要件

ST に列挙されたプラットフォームのそれぞれについて、評価者はプラットフォームの ST を検査して、そのプラットフォームの ST に主張される RBG 機能に VoIP クライアントアプリケーションの ST における RBG 機能が含ま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、VoIP クライアントアプリケーションの ST の TSS を検査して、(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、VoIP クライアントアプリケーション中に用いられる操作ごとに記述されていることを検証しなければならない (shall) (これは VoIP アプリケーションによって実装されないメカニズムによって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この保証アクティビティの一部として TSS に特定されることになる)。

TOE によって満たされる要件

附属書 E「エントロピーの文書化と評定」に従って、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行わなければならない (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 ST を検査することによって、プラットフォームの RBG が検証されていることを検証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 作成者によって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。

評価者は、RBG が準拠する標準に従って、以下のテストを行わなければならない (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って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行わなければならない (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 によって返される値が期待値と一致することを保証しなければならない (shall)。

評価者は、モンテカルロテストを行わなければならない (shall)。このテストについては、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 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms のセクション 3 で特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しなければならない (shall)。

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

評価者は、RBG 実装の 15 回の試行を行わなければならない (shall)。RBG が構成可能な場合、評価者は各構成について 15 回の試行を行わなければならない (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) 決定論的 RBG (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 Personalization String である。次の 2 つは、最初の生成呼び出しへの Additional Input 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 Additional Input 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 800-90 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 Personalization String である。5 番目の値は、最初の生成呼出しへの Additional Input 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 Additional Input 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 Additional Input である。

以下のパラグラフには、評価者によって生成／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。*
>
> ***Personalization String**：Personalization String 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 Personalization String 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 Personalization String を用いなければならない (shall)。実装が Personalization String を用いない場合、値を供給する必要はない。*
>
> ***Additional Input**：Additional Input のビット長は、Personalization String の長さと同一のデフォルトと制約を持つ。*

FCS_TLS_EXT.1　　トランスポート層セキュリティ

FCS_TLS_EXT.1.1　[選択、少なくとも 1 つを選択 : VoIP クライアントアプリケーション、クライアントデバイスプラットフォーム] は、証明書による相互認証を用い、以下の暗号スイートをサポートする以下の 1 つ以上のプロトコル [選択：TLS 1.0 (RFC 2246)、TLS 1.1 (RFC 4346)、TLS 1.2 (RFC 5246)] を実装しなければならない (shall) ：

RFC 3268 による必須暗号スイート：

- TLS_RSA_WITH_AES_128_CBC_SHA

オプションの暗号スイート： [*選択：*

- *TLS_RSA_WITH_AES_256_CBC_SHA*
- *TLS_DHE_RSA_WITH_AES_128_CBC_SHA*
- *TLS_DHE_RSA_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 6460 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256*
- *RFC 6460 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384*
- *RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256*
- *RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384*

- [*割付：その他のサポートされる任意の暗号スイート*]、*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、本要件により限定される。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、実装にとって望ましいアルゴリズムである。さらに、本 PP の将来のバージョンでは Suite B アルゴリズムが要求されることになる。TLS 1.2 は望ましいプロトコルであり、将来は EAP-TLS に要求されることになるかもしれない。

FCS_TLS_EXT.1.2 [選択、少なくとも 1 つを選択：VoIP クライアントアプリケーション、クライアントデバイスプラットフォーム] は、証明書に含まれる Distinuished Name (DN) がピアとして想定される DN と一致しない場合、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 Extension に存在するかもしれない。期待される DN は、構成されてもよいし、またはピアによって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。

保証アクティビティ：

評価者はサポートされる暗号スイートが特定されていることを保証するため、TSS における本プロトコルの実装の記述をチェックしなければならない (shall)。評価者は特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と同一であることを保証するため TSS をチェックしなければならない(shall)。評価者は、TLS が TSS の記述に適合するように (例えば、TOE によって通知される暗号スイートのセットが、要件に合うように限定されなければならない (have to) かもしれない)、TOE の設定における指示が操作ガイダンスに含まれていることを保証するために操作ガイダンスについてもチェックしなければならない (shall)。

評価者は、証明書の 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または 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ていることを保証しなければならない (shall)。

RFC 5246 への準拠をテストするため、将来はさらにテストが追加されるかもしれない。また評価者は、以下のテストを実施しなければならない (shall)。

- *<u>テスト 1</u>：評価者は、要件により特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、上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が成功することを (パケットキャプチャツールを用いて通信路上で) 確認すれば十分であり、暗号化されたトラフィックの特徴を検査して利用されている暗号スイートの判別 (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) を行う必要はない。*
- *<u>テスト 2</u>：以下のテストは、サポートされている証明書署名アルゴリズムのそれぞれについて、繰返し行われる。評価者は、extendedKeyUsage フィールド中に serverAuthentication purpose 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 serverAuthentication purpose 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 が一致するような証明書を用いて接続を試行しなければならない (shall)。評価者は、TSF がうまく接続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 が一致しない証明書を用いて接続を試行しなければならない (shall)。評価者は、TSF がうまく接続できないことを検証しなければならない (shall)。*
- *テスト 4 : 評価者は、サーバが選択した暗号スイートと一致しない証明書を TLS 接続中に送信するようサーバを構成しなければならない (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) (shall)。評価者は、TOE が サーバの証明書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、TOE とサーバとの間に中間者ツールを設置しなければならず (shall) 、またトラフィックに対して以下の改変を行わなければならない (shall) :*
    - *ServerHello ハンドシェイクメッセージ中のサーバのノンスの少なくとも 1 バイトを改変して、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を検証する。*
    - *ServerHello ハンドシェイクメッセージ中のサーバが選択した暗号スイートを、ClientHello ハンドシェイクメッセージ中に存在し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 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) 。*
    - *(条件付き) DHE または ECDHE 暗号スイートがサポートされている場合、ServerKeyExchange 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 を受信した後に接続を拒否することを検証する。*
    - *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。*

4.3.2 識別と認証 (FIA)

TOE のベースライン要件は I&A に関しては比較的限定されている。これは形式的な管理利用者や一般利用者が定義されていないためである。TOE によって行われることが要求される I&A の範囲は、TLS、及び SDES/SRTP 接続を確立する際にマシンレベルで行われる認証に関連したものである。したがって、本セクションの要件は、本 PP で特定されるプロトコルによって用いられるクレデンシャルのみをカバーする。

TSF によって用いられる証明書は、TLS 接続の遠端のものと、利用者の証明書 (及び関連

するプライベート鍵) である。

FIA_X509_EXT.1　　拡張：X509 証明書有効性確認

FIA_X509_EXT.1.1 [選択、少なくとも 1 つを選択：VoIP クライアントアプリケーション、クライアントデバイスプラットフォーム] は、以下のルールに従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。
- すべての CA 証明書について、basicConstraints 拡張が存在し 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って、認証パスを検証する。
- [選択：RFC 2560 にて特定されるオンライン証明書状態プロトコル (OCSP)、RFC 5759 にて特定される証明書失効リスト (CRL)] を用いて証明書の失効状態を検証する。
- 以下のルールに従って、extendedKeyUsage フィールドを検証する。
    - 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)。

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を選択しなければならない (shall)。証明書はピア認証のため (FCS_TLS_EXT.1)、TSF ソフトウェアの高信頼アップデートのため (FPT_TUD_EXT.1) 及びオプションとして完全性検証のために (FPT_TST_EXT.1) 用いられ、また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)。TLS については、証明書を利用して認証が行われなければならず (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)。

証明書の有効性確認は、信頼済みルート証明書に至ることが期待されることに注意すべきである (should)。

FIA_X509_EXT.1.1 は TOE プラットフォームに、TLS サーバによって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。すなわち、サーバ証明書の extendedKeyUsage フィールドに"Server Authentication" が含まれ、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、少なくとも 1 つを選択：VoIP クライアントアプリケーション、クライアントデバイスプラットフォーム] 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：

この要件は、VoIP クライアントアプリケーションまたはプラットフォームによって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 (TOE または TOE プラットフォーム) 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)。TOE がプラットフォームへチェックの実行と結果の提供を要求することもあれば、TOE が自分でチェックを行う場合もある。また評価者は、認証パス検証アルゴリズムの記述が TSS に提供されていることも確認し、検証の連鎖が信頼済みルート証明書で終わることが記述されていることを保証する。

評価者は、有効性のチェックが TOE と TOE プラットフォームのどちらで行われる場合であっても、その設定のために十分な情報がガイダンス文書によって利用者へ提供されていることを保証する。ガイダンス文書には、証明書の有効性に関する情報を提供するエンティティとの保護された通信パスを設定する方法とともに、チェックに用いられる手法を選択する方法の指示が提供される。

「TOE」と「TOE プラットフォーム」の選択に関わらず、評価者は以下のテストを行わなければならない (shall)。このテストは、FCS_TLS_EXT.1 及び FIA_X509_EXT.2 の保証アクティビティで行われるテストと組み合わせて行うこともできる。

- *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、または高信頼ソフトウェアアップデート) が失敗することを論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論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論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 (将来のバージョンでは、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。*

FIA_X509_EXT.2　　拡張：X509 証明書の利用と管理

FIA_X509_EXT.2.1 [選択、少なくとも 1 つを選択：VoIP クライアントアプリケーション、クライアントデバイスプラットフォーム] は、*SDES/SRTP*、*TLS*、及び [選択：ソフトウェアアップデートのコード署名、ソフトウェア完全性検証のコード署名、追加用途なし] のための認証をサポートするため、RFC 5280 によって定義される X.509v3 証明書を用いなけ

ればならない (shall)。

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) 及びソフトウェア完全性検証 (FPT_TST_EXT.1) にオプションとして用いてもよい。これらのコード署名用途のいずれかが選択されている場合、FIA_X509_EXT.2(2) が本体へ取り込まれなければならない (must)。

VoIP クライアントアプリケーションはそれぞれ、一意の X.509v3 証明書を有すること。証明書はクライアント間で再利用されてはならない。

保証アクティビティ：

このエレメントの保証アクティビティは、FCS_TLS_EXT.1 、 (条件付きで) FPT_TUD_EXT.1 及び FPT_TST_EXT.1 の保証アクティビティによってテストされる。

FIA_X509_EXT.2.2 [選択、少なくとも 1 つを選択：VoIP クライアントアプリケーション、クライアントデバイスプラットフォーム] 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、少なくとも 1 つを選択：VoIP クライアントアプリケーション、クライアントデバイスプラットフォーム] は [選択：*このような場合には高信頼チャネルを確立するか確立しない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 をダウンロードしたり、OCSP を実行したりするため、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) 場合がしばしば発生する。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上記の選択が用いられる。TOE は、証明書が FIA_X509_EXT.1 の他の全てのルールに従って有効であると判断された場合、2 番目 (訳注：3 番目の間違い) の選択に示されたふるまいによってその有効性を決定しなければならない (shall)。証明書が FIA_X509_EXT.1 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 作成者によって管理者設定オプションが選択された場合、ST 作成者はまた FMT_SMF.1 における適切な機能についても選択しなければならない (must)。

保証アクティビティ：

評価者は、TOE／プラットフォーム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／プラットフォーム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するため、TSS をチェックしなければならない (shall)。この機能が完全にプラットフォームによって実装されている場合、TOE の操作ガイダンスは各プラットフォームに該当するガイダンスを参照しなければならない (shall)。

評価者は、高信頼チャネルの確立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／プラットフォーム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特定できるという要件が存在する場合には、この設定アクションを実行する方法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評価者は保証しなければならない (shall)。このふるまいが完全にプラットフォームによって実装されている場合、評価者は、このエレメントの選択が各プラットフォームの ST に含まれていることを確認するため、各プラットフォームの ST を検査しなければならない (shall)。

本要件が完全に、または部分的に TOE によって実装されている場合、評価者は証明書の使用を要求するシステムの各機能についてテスト 1 を行わなければならない (shall)。

- *テスト 1：評価者は、TOE 以外の IT エンティティとの通信によって、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論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観察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って設定可能である場合には、評価者は、サポートされているすべての管理者設定可能オプションが、文書化されているようにふるまうことを決定するため、操作ガイダンスに従わなければならない (shall)。

FIA_X509_EXT.2.3 [選択、少なくとも 1 つを選択：VoIP クライアントアプリケーション、クライアントデバイスプラットフォーム] は、ピア証明書が無効とみなされる場合には高信頼通信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 によって行われる SDES/SRTP、TLS のいずれかが含まれる。有効性は、証明書パス、有効期限、RFC 5280 に従った失効状態、及び証明書に含まれる Distinguished Name (DN) によって決定される。

保証アクティビティ：

評価者は、TOE がどの証明書を使用するかを選択する方法が TSS に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設定するための管理ガイダンスに必要な指示が記述されていることを保証するため、TSS をチェックしなければならない (shall)。

評価者は、高信頼チャネルの確立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特定できるという要件が存在する場合、評価者はこの設定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システムのそれぞれの機能について、テスト 1 を行わなければならない (shall)。

- *テスト 1：評価者は、有効な証明書パスのない証明書を使用すると、その機能が失敗することを論証しなければならない (shall)。次に評価者は、管理ガイダンスを利用して、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論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)。*

評価者は、高信頼パスを確立し証明書の利用を要求するシステムにおける各機能について、テスト 2 を行わなければならない (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って、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論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って設定可能である場合には、評価者は操作ガイダンスに従って、サポートされているすべての管理者設定可能オプションが、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)。*
- *テスト 3：評価者は、RSA または ECDSA アルゴリズムを用いて署名された証明書を利用して、高信頼チャネルの確立中に TOE を SIP サーバに対して認証させなければならない (shall)。このテストによって TOE が、SIP サーバの証明書に署名した信頼できる CA の証明書を持っていることと、DN に関してビット単位の比較*

を行うことが保証される。このDN のビット単位の比較によって、SIP サーバが信頼できるCA によって署名された証明書を持つことだけでなく、その証明書が期待されるDN からのものであることもまた保証される。評価者は、TSS (訳注：TOE の間違い) を構成して証明書またはDN (例えば、一部の実装では証明書マップ) を高信頼チャネル接続と関連付けることになる。これが、DN のチェック対象となる。

- *テスト4：評価者は、信頼できるCA から署名された証明書について、DN が一致しない場合 (4 つのフィールドのどれかを期待値と一致しないように変更すればよい) には高信頼チャネルが確立されないことをテストしなければならない (shall)。*
- *テスト5：評価者は、証明書有効性確認エンティティへの接続が到達不可能である場合に高信頼チャネルを確立するか、または確立しないかTOE を設定可能であることを保証しなければならない (shall)。証明書有効性確認のために選択された手法のそれぞれについて、評価者は証明書の有効性確認を試行する。このテストにおいては、証明書が失効するかどうかは問題ではない。高信頼チャネルが確立を許可される「モード」では、接続が行われる。チャネルが確立されるべきでない場合には、接続は拒否される。*

要件が満たされていることを保証するための追加的なテストは、FTP_ITC の要件と組み合わせて行われる。

4.3.3 セキュリティ管理 (FMT)

TOE が別個の管理役割を維持管理することは要求されていない。しかし、一般利用者には利用できるべきではない (should not) TOE 操作の特定の側面を構成する機能を提供することは要求されている。

FMT_SMF.1　　管理機能の仕様

FMT_SMF.1.1 [選択、少なくとも 1 つを選択：VoIP クライアントアプリケーション、クライアントデバイスプラットフォーム] は、以下の管理機能を行うことができなければならない (shall)。

- 本 PP 中で義務付けられたプロトコルに関連する暗号アルゴリズムを構成すること、
- 本 PP のセキュリティ機能に用いられる X.509v3 証明書をロードすること、
- 証明書失効チェックを構成すること、
- TOE をアップデートする能力、及びそのアップデートを検証する能力
- 本 PP の別のセクションにおいて特定されるすべてのセキュリティ管理機能を構成できる能力、
- [選択：証明書の有効性を確認するための接続が確立できなかった際に取られるアクション、 [割付：任意の追加的管理機能]、その他のアクションなし]。

適用上の注意：

設置の際、VoIP クライアントアプリケーションはIT 環境に依存して管理者をクライアントマシンへ認証させる。

SIP サーバが構成情報をVoIP クライアントアプリケーションへ「プッシュ」するような例もあるかもしれない。これは受容可能な管理形態である。ST 作成者はST に、どの管理機能がVoIP クライアントアプリケーションによって行われるのか、そしてどれがSIP サーバによって行われるのかを単純に明示しなければならない (must)。機能が重複する (すなわち、VoIP クライアントアプリケーション上のエンドユーザによって、またはSIP サーバによって行われることが可能な) 場合もあり得るが、ST が明確であってこの機能を行う方法

がガイダンス文書に記述されている限り、これは問題ない。

保証アクティビティ：

評価者は、PP によって義務付けられるすべての管理機能が操作ガイダンスに記述され、その記述にはその管理機能と関連付けられた管理職務を行うために必要な情報が含まれていることをチェックして確認しなければならない (shall)。評価者は、TOE を構成して上記要件に列挙されるオプションのそれぞれをテストすることによって、管理機能を提供する TOE の能力をテストしなければならない (shall)。

適用上の注意に言明されているように、TOE はローカルに構成されてもよいし、または SIP サーバによってリモートに構成されてもよい。ST には、ローカル及びリモートに行える機能が明確に言明されること。ガイダンス文書には、これを行う方法も記述されること。評価者には、ST 及びガイダンス文書に言明される構成管理方法のすべてにおいて、この機能をテストすることが期待される。

ここでのテストは、例えば FCS_TLS_EXT.1 のような他の要件のテストと組み合わせて実施されてもよいことに注意されたい。

4.3.4 TSF の保護 (FPT)

FPT_TST_EXT.1　　拡張：TSF セルフテスト

FPT_TST_EXT.1.1 [選択、少なくとも 1 つを選択：VoIP クライアントアプリケーション、クライアントデバイスプラットフォーム] 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、TSF の正しい動作を論証しなければならない (shall)。

FPT_TST_EXT.1.2 [選択、少なくとも 1 つを選択：VoIP クライアントアプリケーション、クライアントデバイスプラットフォーム] は、TSF の提供する暗号サービスの使用により、保存された TSF 実行可能コードが実行のためにロードされた際にその完全性を検証する機能を提供しなければならない (shall)。

適用上の注意：

TOE は典型的には IT 環境中で動作するソフトウェアパッケージであるが、それでも上記で求められるセルフテストアクティビティを行うことは可能である。しかし、上述のテストによって提供される保証の評定において、ホスト環境への多大な依存が存在する (ホスト環境が侵害した場合にはセルフテストは意味をなさなくなることを意味する) ことは理解されるべきである (should)。

保証アクティビティ：

評価者は TSS を検査して、起動時に TSF によって実行されるセルフテストが詳述されていることを保証しなければならない (shall)。この記述には、実際に行われるテストの概要 (例えば、「メモリがテストされる」と言うだけではなく、「各メモリロケーションに値を書き込み、それを読み出して書き込んだ値と同一であることを保証することによってメモリがテストされる」のような記述が用いられなければならない (shall)) が含まれるべきである (should)。評価者は、TSF が正しく動作していることをテストが十分に論証するという論拠が TSS 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 TSS を検査して、保存された TSF 実行可能コードが実行のためにロードされた際にその完全性を検証する方法が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、TSF 実行可能コードの完全性が侵害されていないことをテストが十分に論証するという論拠が TSS 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、TSS (または操作ガイダンス) に成功の (例えば、ハッシュが検証された) 場合と不成功の (例えば、ハッシュが検証されなかった) 場合に行われるアクションが記述されていることも検証する。評価者は、以下のテストを行わなければならない (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する。

- *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する。*

FPT_TUD_EXT.1　　拡張：高信頼アップデート

FPT_TUD_EXT.1.2 [選択、少なくとも 1 つを選択：VoIP クライアントアプリケーション、クライアントデバイスプラットフォーム] は、TOE ファームウェア／ソフトウェアへのアップデートを開始する能力を正当な管理者へ提供しなければならない (shall)。

FPT_TUD_EXT.1.3 [選択、少なくとも 1 つを選択：VoIP クライアントアプリケーション、クライアントデバイスプラットフォーム] は、TOE へのファームウェア／ソフトウェア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を検証する手段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(2) に特定されているものである。参照されている公開ハッシュは、FCS_COP.1(3) に特定された関数のいずれかによって生成される。

保証アクティビティ：

TOE へのアップデートは、正当なソースによって署名されると共にそれと関連付けられたハッシュを持つか、または正当なソースによって署名される。デジタル署名が用いられる場合、正当なソースの定義が、アップデート検証メカニズムによって用いられる証明書がデバイスへ取り込まれる方法の記述とともに、TSS に含まれる。評価者は、この情報が TSS に含まれることを保証する。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する。

- *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する。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する。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論証する。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する。*
- *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する評価者は、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する。評価者は、TOE がそのアップデートを拒否することを検証する。*

4.3.5 高信頼パス／チャネル (FTP)

FTP_ITC.1(2)　　TSF 間高信頼チャネル (TLS/SIP)

FTP_ITC.1.1(2) **詳細化：** [選択、少なくとも 1 つを選択：VoIP クライアントアプリケーション、クライアントデバイスプラットフォーム] は、**FCS_TLS_EXT.1 にて特定される他のプロトコルではなく TLS のみを用いた**それ自身と **SIP サーバ**との間の通信チャネルであって、他の通信チャネルとは論理的に分離されていると共に、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改変及び開示からの保護を提供するものを提供しなければならない (shall)。

FTP_ITC.1.2(2) [選択、少なくとも 1 つを選択 : VoIP クライアントアプリケーション、クライアントデバイスプラットフォーム] は、TSF が高信頼チャネルによる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(2) [選択、少なくとも 1 つを選択 : VoIP クライアントアプリケーション、クライアントデバイスプラットフォーム] は、 [SIP サーバとのすべての通信について] 高信頼チャネルによる通信を開始しなければならない (shall)。

適用上の注意 :

TOE は起動時に SIP サーバとの接続を確立し、これはデバイスの電源が入っていて呼を送信／受信できる限り永続する。TOE には、TLS を利用してこの接続を確立できることが要求される。

保証アクティビティ :

評価者は TSS セクションをチェックして、この要件が TOE へどのように実装されているか記述されていることを確認しなければならない (shall)。

- *テスト 1 : 以下のテストは、サポートされる証明書署名アルゴリズムのそれぞれについて、繰返し行われる。評価者は、extendedKeyUsage フィールド中にサーバ認証目的を含む認証サーバ証明書を持った SIP 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 2 : 以下のテストは、サポートされる証明書署名アルゴリズムのそれぞれについて、繰返し行われる。評価者は、TSF が extendedKeyUsage フィールド中に Client Authentication 目的を含む証明書のみを用いることを検証し、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 Client Authentication 目的を含まないこと以外は有効なクライアント証明書を TSF 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)。*

4.4 セキュリティ保証要件

セクション 3 の TOE に関するセキュリティ対策方針は、セクション 2 に特定された脅威へ対抗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。

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、評価者によって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 4.2 及びセクション 4.3 の両方に詳述されている。

それぞれのファミリには、(もしあれば) 開発者によって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 (セクション 4.2 及びセクション 4.3 にすでに含まれているものに加えて) が記述される。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 4.2 及びセクション 4.3 にて特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 1 に要約されており、本 PP のセクション 2 に特定された脅威へ対抗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。

表 1：TOE セキュリティ保証要件

保証クラス	保証コンポーネント	保証コンポーネントの記述
開発	ADV_FSP.1	基本機能仕様
ガイダンス文書	AGD_OPE.1	利用者操作ガイダンス
	AGD_PRE.1	利用者準備ガイダンス
テスト	ATE_IND.1	独立テスト—適合
脆弱性評定	AVA_VAN.1	脆弱性分析
ライフサイクルサポート	ALC_CMC.1	TOE のラベル付け
	ALC_CMS.1	TOE の CM 範囲

4.4.1 ADV クラス：開発

本 PP に適合する TOE については、TOE に関する情報は ST ガイダンスの TOE 要約仕様 (TSS) 部分とともに、エンドユーザに利用可能な文書にも含まれている。TOE 開発者が TSS を作成することは要求されてはいないが、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 及びセクション 4.3 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)。

4.4.1.1 ADV_FSP.1 基本機能仕様

機能仕様は、TOE のセキュリティ機能インタフェース (TSFI) を記述するものである。これらのインタフェースの形式的または完全な仕様は必要とされない。さらに、本 PP に適合する TOE は必然的に TOE の利用者によって直接呼び出すことのできない運用環境へのインタフェースを持つことになるため、そのようなインタフェースは間接的なテストしかできないことから、そのようなインタフェースの記述を特定することにはあまり意味がない。本 PP では、このファミリに関するアクティビティは、機能仕様へ対応した形で TSS に提示されるインタフェースと、AGD 文書に提示されるインタフェースを理解することに焦点を絞るべきである (should)。特定された保証アクティビティを満たすために、追加的な「機能仕様」文書が必要とはされない。

評価される必要のあるインタフェースは、独立した抽象的なリストとしてではなく、列挙された保証アクティビティを行うために必要な情報を通して特徴づけされる。

開発者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ている。機能仕様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 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・提示エレメント：

ADV_FSP.1.1C　機能仕様は、SFR 実施及び SFR 支援の各 TSFI の目的と使用方法を記述しなければならない (shall)。

ADV_FSP.1.2C　機能仕様は、SFR 実施及び SFR 支援の各 TSFI に関連するすべてのパラメタを識別しなければならない (shall)。

ADV_FSP.1.3C　機能仕様は、暗黙的に SFR 非干渉として分類されているインタフェースについて、その分類の根拠を提供しなければならない (shall)。

ADV_FSP.1.4C　追跡は、機能仕様での TSFI に対する SFR の追跡を論証するものでなければならない (shall)。

評価者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、証拠の内容・提示に対する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 の正確かつ完全な具体化であることを決定しなければならない (shall)。

保証アクティビティ：

これらの SAR に関連付けられた特定の保証アクティビティはない。機能仕様文書はセクション 4.2 及び 4.3 に記述された評価アクティビティと、AGD、ATE 及び AVA の 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ている。機能仕様情報の内容についての要件は、実施されるその他の保証アクティビティに基づいて暗黙に評価される。不十分なインタフェース情報のために評価者がアクティビティを実施できなかった場合、十分な機能仕様が提供されていなかったことになる。

4.4.2 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対する役割を満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、非形式的なスタイルかつ正当な利用者によって読解可能であるべきである (should)。

ガイダンスがは、ST で主張されたとおり製品がサポートしているすべての運用環境に関して提供されなければならない (must)。このガイダンスには、以下が含まれる：

- その環境へ TOE をインストールできるようにするための指示、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、ならびに
- TOE の機能、環境の機能、またはこれら 2 つの組み合わせのいずれかを用いることによって、保護された運用管理機能を提供するための指示。

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なければならない (must)。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 及び 4.3 において特定された保証アクティビティに含まれている。

4.4.2.1 AGD_OPE.1 利用者操作ガイダンス

開発者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、開発者はこの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)。これによって、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・提示エレメント：

AGD_OPE.1.1C 利用者操作ガイダンスは、適切な警告を含め、セキュアな処理環境で管理するべき (should) 正当な利用者がアクセス可能な機能と権限について、利用者の役割ごとに記述しなければならない (shall)。

AGD_OPE.1.2C 利用者操作ガイダンスは、TOE により提供された利用可能なインタフェースをセキュアな方法でどのように使用するかを利用者の役割ごとに記述しなければならない (shall)。

AGD_OPE.1.3C 利用者操作ガイダンスは、正当な利用者を対象として、利用可能な機能とインタフェース、特に利用者の管理下にあるすべてのセキュリティパラメタを、必要に応じてセキュアな値を示して、記述しなければならない (shall)。

AGD_OPE.1.4C 利用者操作ガイダンスは、正当な利用者を対象として、TSF の管理下にあるエンティティのセキュリティ特性の変更を含む、利用者がアクセス可能で実行が必要な機能に関連するセキュリティ関連事象の各タイプについて、明確に提示しなければならない (shall)。

AGD_OPE.1.5C 利用者操作ガイダンスは、TOE の操作のすべての可能なモード(障害や操作誤りの後の操作を含む)、それらの結果、及びセキュアな運用を維持するために必要なことを識別しなければならない (shall)。

AGD_OPE.1.6C 利用者操作ガイダンスは、正当な利用者を対象として、ST に記述された運用環境のセキュリティ対策方針を満たすために従うべきセキュリティ手段を記述しなければならない (shall)。

AGD_OPE.1.7C 利用者操作ガイダンスは、明確で、合理的なものでなければならない (shall)。

評価者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、証拠の内容・提示に対する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)*。

適用上の注意：

利用者操作ガイダンスは、単一の文書に含まれる必要はない。利用者、管理者及びアプリケーション開発者のためのガイダンスが、複数の文書またはウェブページに分散されていてもよい。必要に応じて、ガイダンス文書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) で表現される。

ここで繰返し情報を提示するのではなく、開発者はこの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)。これによって、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。

保証アクティビティ：

管理機能に関しては、いくつかはすでにセクション4.2 及び4.3 で述べたが、追加的情報が以下のように必要とされる。

暗号エンジンを実装するTOE については、TOE の評価される構成と関連付けられた暗号エンジンを構成するための指示が操作ガイダンスに含まれなければならない (shall)。TOE のCC 評価の中で、他の暗号エンジンの利用が評価もテストもされなかったという警告が、与えられなければならない (shall)。

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って、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、この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)。

- *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) メカニズムによって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って取得されてもよい。*
- *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)。*

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。

操作ガイダンスには、SRTP に用いられるポートを指定するための指示が含まれなければならない (shall)。

4.4.2.2 AGD_PRE.1 準備手続き

開発者アクションエレメント：

AGD_PRE.1.1D 開発者は、その準備手続きを含めて TOE を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、開発者は保証アクティビティを検査して準備手続きに関して必要とされる内容を判断すべきである (should)。

内容・提示エレメント：

AGD_PRE.1.1C 準備手続きは、開発者の配付手続きに従って配付された TOE のセキュアな受入れに必要なすべてのステップを記述しなければならない (shall)。

AGD_PRE.1.2C 準備手続きは、TOE のセキュアな設置、及び ST に記述された運用環境のセキュリティ対策方針に従った運用環境のセキュアな準備に必要なすべてのステップを記述しなければならない (shall)。

評価者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、証拠の内容・提示に対する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 が運用に向けて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設定にあたっては、文書に関して多大な期待が存在する。評価者は、TOE に提供されたガイダンスが、ST 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とコンポーネント (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に確認しなければならない (shall)。

評価者は、以下のガイダンスが提供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)。

- *概論材料に示したように、TOE の管理は TOE の全利用者のグループのサブセットである、1 人以上の管理者によって行われる。システムが全体として (TOE プラス運用環境) この機能を提供することは事実でなければならない (must) が、その機能を実装する責任は、完全に運用環境の責任から、完全に TOE の責任まで変動する可能性がある。高レベルにおいては、ガイダンスには運用環境が責任を持つ機能の部分を提供できるように運用環境を構成するための適切な指示が含まれていなければならない (must)。利用者全体から管理ユーザを分離するためのメカニズムを TOE が提供しない場合には、例えば、OS の I&A メカニズムが一意の (OS ベースの) 識別情報を利用者へ提供するような OS の構成をカバーするような指示と、1 つまたは複数の TOE 管理識別情報を用いた OS の DAC メカニズムの構成を設置者に指示するようなさらなるガイダンスとが与えられ、TOE 管理者のみが管理用実行可能形式へアクセスできるようにする。TOE がこの機能の一部または全部を提供する場合には、適切な要件が附属書 C から ST へ取り込まれ、これらの要件と関連付けられた保証アクティビティが TOE と運用環境の両方に必要とされるガイダンスの詳細を提供する。*

また評価者は、以下のテストを実施しなければならない (shall)。

- *テスト 1 [条件付き]：すべての TOE 利用者からの管理ユーザの分離が運用環境の構成を通してのみ行われる場合、評価者は、ST 中に主張されるすべての構成について、管理ガイダンスに従ってシステムを構成した後には管理者以外の利用者が TOE の管理機能へアクセスできないことを保証する。*

4.4.3 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特定される。前者は ATE_IND ファミリによって行われるが、後者は AVA_VAN ファミリによって行われる。本 PP に特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、設計情報の可用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、以下の要件に特定されるテスト報告書である。

4.4.3.1 ATE_IND.1 独立テスト—適合

テストは、TSS と、提供された管理 (設定及び操作を含む) 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 及び 4.3 に特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 4.4 の SAR について特定されている。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、テスト報告書を作成する。

開発者アクションエレメント：

ATE_IND.1.1D　開発者は、テストのための TOE を提供しなければならない (shall)。

内容・提示エレメント：

ATE_IND.1.1C	TOE は、テストに適していなければならない (shall)。
	評価者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、証拠の内容・提示に対する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 が仕様どおり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書とテスト報告書を作成しなければならない (shall)。テスト計画書は、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 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書に文書化しなければならない (must)。

テスト計画書にはテストされるプラットフォームが特定され、そしてテスト計画書には含まれないが 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書が提供する。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 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。

テスト計画書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。評価者は、テストの一部として、または標準的なテスト前の条件として、AGD 文書に従って各プラットフォームの設置及び設定を行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設定が含まれる。このエンジンによって実装される暗号アルゴリズムは、本 PP によって特定され、評価される暗号プロトコル (SDES 及び TLS) によって用いられるものである。

テスト計画書には、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。テスト報告書 (テスト計画書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、報告書には単なる「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。

4.4.4 AVA クラス：脆弱性評定

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検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。侵入テスト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 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、ベンダによって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。この情報は侵入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。

4.4.4.1 AVA_VAN.1 脆弱性調査

開発者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・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、証拠の内容・提示に対する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*行わなければならない (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って行われる攻撃に 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、評価者は報告書を作成し、この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)。この報告書は、物理的には ATE_IND に言及される全体的なテスト報告書の一部であってもよいし、または別個の文書であってもよい。評価者は、公開情報の検索を行って、モビリティ {モビリティコンポーネント} 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書に文書化する。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、また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。適合性は、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って判断される。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って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、適切な正当とする理由が策定されることになるであろう。

4.4.5 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ではなく、ライフサイクルのエンドユーザに可視の側面に限定される。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を減じようとするものではない。そうではなく、この保証レベルにおける評価に関して利用可能とされるべき情報を反映したものである。

4.4.5.1 ALC_CMC.1 TOE のラベル付け

このコンポーネントは、TOE を同一ベンダの他の製品またはバージョンから区別でき、またエンドユーザによって調達される際に容易に特定できるように、TOE を識別することを目標としている。

開発者アクションエレメント：

ALC_CMC.1.1D 開発者は、TOE 及び TOE への参照を提供しなければならない

(shall)。

内容・提示エレメント：

ALC_CMC.1.1C　TOE は、その一意な参照でラベル付けされなければならない (shall)。

評価者アクションエレメント：

ALC_CMC.2.1E　評価者は、提供された情報が、証拠の内容・提示に対する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 ST をチェックして、ST の要件を満たすバージョンを具体的に特定する識別情報 (製品名／バージョン番号など) が含ま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 AGD ガイダンス及びテスト用に受け取った TOE サンプルをチェックして、バージョン番号が ST のものと一貫していることを保証しなければならない (shall)。ベンダが TOE を宣伝するウェブサイトを維持管理している場合、評価者はそのウェブサイト上の情報を検査して、ST の情報がその製品を識別するために十分であることを保証しなければならない (shall)。

4.4.5.2　ALC_CMS.1 TOE の CM 範囲

TOE の適用範囲とそれに関連した評価証拠の要件を考慮して、このコンポーネントの保証アクティビティは ALC_CMC.1 に関して列挙された保証アクティビティによってカバーされる。

開発者アクションエレメント：

ALC_CMS.2.1D　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・提示エレメント：

ALC_CMS.2.1C　構成リストには、TOE 自体、及び SAR が要求する評価証拠を含まなければならない (shall)。

ALC_CMS.2.2C　構成リストは、構成要素を一意に識別しなければならない (shall)。

評価者アクションエレメント：

ALC_CMS.2.1E　評価者は、提供された情報が、証拠の内容・提示に対する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：

本 PP において「SAR によって要求される評価証拠」は、ST の情報と、AGD 要件の下で管理者及び利用者に提供されるガイダンスとの組み合わせに限られる。TOE が具体的に識別され、その識別情報が ST 及び AGD ガイダンスの内容と一貫していることを (ALC_CMC.1 に関する評価アクティビティ中で行われるように) 保証することによって、評価者はこのコンポーネントによって要求される情報を暗黙に確認する。

根拠

これらのセキュリティ保証要件を選択した根拠は、以前汎用 CEM プロセスを用いて達成されたものよりも、より客観的かつ再現可能なレベルの保証が得られるためである。とは言え、これらの保証アクティビティは CEM のアクティビティに基づくものであるが、この技術にカスタム化され、本 PP に含まれる機能仕様に特有のものとなっている。保証要件及びアクティビティは、PP に提示された脅威を軽減し対策方針を達成するための十分な文書とテストを体現している。これらの種類の製品に脆弱性が発見された場合には、より厳格なセキュリティ保証要件が、現実のベンダのプラクティスに基づいて義務付けられることになるかもしれない。

附属書A： 参考表

本プロテクションプロファイルにおいて、本文書の最初のセクションでは主に説明文による提示により、ネットワークデバイスへの脅威、これらの脅威を軽減するために用いられる手法、及び適合 TOE によって達成される軽減の程度について、全体的にわかりやすく説明しようと試みた。この提示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、本附属書では表形式のアーティファクトを用いて、本文書に関連付けられる評価アクティビティを説明する。

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における実質的な事実と、TOE の使用にあたって不可欠な環境条件の両方が含まれる。TOE がこれらの前提条件を満たさない運用環境に配置された場合、もはや TOE はそのセキュリティ機能のすべてを提供することはできないかもしれない。

表 2：TOE の前提条件

前提条件の名称	前提条件の名称
A.AVAILABILITY	ネットワークリソースは、VoIP クライアントがミッション要件を満たし、情報を送信するために、利用可能でなければならない (shall)。
A.OPER_ENV	TOE の運用環境は、TOE そのものには適用されないが、TOE の正しい動作をサポートするために必要な、要件、脅威、及び方針へ適切に対処する。
A.TRUSTED_CONFIG	TOE を構成する要員とその運用環境は、該当するセキュリティ構成ガイダンスを遵守すること。

脅威

以下の表に、VoIP クライアントアプリケーションと運用環境によって対処される脅威を列挙する。以下に特定されるすべての脅威について、前提とされる攻撃者の専門的知識のレベルは、しろうと (熟練者でない) である。

表 3：脅威

脅威	脅威の説明
T.TSF_CONFIGURATION	TSF の構成を許可できないことによって、その利用者が自分たちに特有のセキュリティ対策方針を十分に実装できず、利用者情報の侵害を招く可能性がある。
T.TSF_FAILURE	TOE のセキュリティメカニズムが故障し、TSF の侵害をもたらす可能性がある。
T.UNAUTHORIZED_ACCESS	利用者が、TOE データへ不正にアクセスを行う可能性がある。悪意のある利用者、プロセス、または外部 IT エンティティが、データまたは TOE リソースへ不正にアクセスするために正当なエンティティに成りすます可能性がある。悪意のある利用者、プロセス、または外部 IT エンティティが、自分自身を TOE と偽って提示し、識別と認証のデータ

	を取得する可能性がある。
T.UNAUTHORIZED_UPDATE	悪意のある当事者が製品へのアップデートをエンドユーザへ供給しようと試み、TOEのセキュリティ機能を侵害させる可能性がある。
T.USER_DATA_REUSE	音声データが、音声呼以外で送信されるため、意図しない宛先へ不用意に送信される可能性がある。

TOE のセキュリティ対策方針

表 4：TOE のセキュリティ対策方針

対策方針	対策方針の説明
O.PROTECTED_COMMUNICATIONS	TOE は、正当な IT エンティティ (SIP サーバ及び他の VoIP アプリケーション) との保護された通信チャネルを提供すること。
O.TSF_SELF_TEST	TOE は、TOE が適切に動作していることを確実にするため、TOE のセキュリティ機能の何らかのサブセットをテストする機能を提供すること。
O.VERIFIABLE_UPDATES	TOE は、TOE へのいかなるアップデートも改変されておらず、また (オプションとして) 信頼されたソースからのものであることが管理者によって検証できることを確実にするための機能を提供すること。

以下の表には、運用環境の対策方針が含まれる。前提条件が PP に追加された際には、これらの対策方針もそのような追加を反映して増補されるべきである (should)。

表 5：運用環境のセキュリティ対策方針

対策方針	対策方針の説明
OE.AUTHORIZED_USER	TOE の利用者は、悪意を持たず、すべての利用者ガイダンスを遵守する。
OE.OPER_ENV	運用環境は、VoIP 接続を確立するための SIP インフラストラクチャ、証明書を提供するための PKI、そして TOE の正しい動作をサポートするための実行ドメインを提供すること。
OE.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。

附属書B： オプションの要件

本 PP の概論で示したように、本 PP の本体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って行われなければならない (must) もの) が含まれている。これに追加して、これ以外の 3 種類の要件が附属書 B、C、及び D において特定されている。

第 1 の種類 (本附属書に含まれる) は、ST に取り込むことができる要件であるが、TOE が本 PP への適合を主張するためには必要とされないものである。第 2 の種類 (附属書 C に含まれる) は、PP の本体中の選択に基づく要件である。特定の選択がなされた場合には、その附属書の追加的要件が取り込まれることが必要となる。第 3 の種類 (附属書 D に含まれる) は、本の 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のベースライン要件に取り込まれることになっているコンポーネントであり、VPN クライアント (訳注：VoIP クライアントの間違い) ベンダによる採用が推奨される。ST 作成者には、附属書 B、附属書 C、または附属書 D に含まれる要件と関連する可能性があるが列挙されていない要件 (例えば、FMT タイプの要件) もまた、ST へ取り込まれることを確実にする責任があることに注意されたい。

現時点では、オプションの要件は存在しない。将来のバージョンでは、本セクションには ST 作成者が取り込む責任のある追加的要件が含まれるかもしれない。

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 の本体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って行われなければならない (must) もの) が含まれている。PP の本体中の選択に基づく追加的要件が存在する。特定の選択がなされた場合には、以下の追加的要件が取り込まれることが必要となる。

識別と認証 (FIA)

FIA_X509_EXT.2(1) 拡張：X509 認証

FIA_X509_EXT.2.4(1) [選択、少なくとも 1 つを選択：VoIP クライアントアプリケーション、クライアントデバイスプラットフォーム] 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 [選択：インストール、実行] 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) 及びソフトウェア完全性検証 (FPT_TST_EXT.1.2) にオプションとして用いてもよい。これらのコード署名用途のいずれかが FIA_X509_EXT.2.1 で選択されている場合、FIA_X509_EXT.2.4 が本体へ取り込まれなければならない (must)。

保証アクティビティ：

この要件の保証アクティビティは、FIA_X509_EXT.1 及び FIA_X509_EXT.2 の保証アクティビティと関連して行われる。

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 の本体にはベースライン要件 (TOE またはそのプラットフォームによって行われなければならない (must) もの) が含まれている。望ましいセキュリティ機能を特定す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では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。

どの時点においても、これらは ST へ取り込むことができ、その場合でも TOE は依然として本 PP に適合する。

セキュリティ監査 (FAU)

監査の生成が TOE によって提供される場合には、ST 作成者が適切な選択及び割付を行った上で、以下の監査要件が ST に取り込まれなければならない (must)。

監査データの生成 (FAU_GEN)

FAU_GEN.1　　監査データの生成

FAU_GEN.1.1 VoIP クライアントアプリケーションは、以下の監査対象事象の監査記録を生成できなければならない (shall)：

a) 監査機能の開始及び終了、

b) すべての管理アクション、

c) [表 6 に列挙される具体的に定義された監査対象事象]。

適用上の注意：

ST 作成者は、他の監査対象事象を直接表中に取り込むことができる。監査対象事象は、提示されたリストには限定されない。

項目「a」の場合、言及される監査機能は TOE によって提供されるものである。例えば、TOE がスタンドアロンの実行可能形式であった場合、この項の要件を満たすには TOE そのものの開始及び終了で十分であろう。

本文書に取り込まれた SFR の監査対象としての側面の多くは、管理アクションに関するものである。上記の項目「c」はすべての管理アクションが監査対象であることを要求しているため、これらのアクションが監査対象であるという追加的な特定は表 6 には提示されていない。TOE それ自身は管理者へ I&A を行う能力を提供する必要がないため、この要件は「管理アクション」として PP に記述される事象 (主に、TOE によって提供される機能の設定に関するもの) を監査する機能を TOE が有することを意味している。AGD ガイダンスには、TOE によって生成される監査データが基盤となる IT 環境の監査機能と統合されることを確実にする手順が詳述されることが期待される。

保証アクティビティ：

評価者は操作ガイダンスをチェックして、すべての監査対象事象が列挙されており、また監査記録のフォーマットが提供されていることを保証しなければならない (shall)。監査記録のフォーマットの種類はすべて、各フィールドの簡潔な記述とともに、カバーされなければならない (must)。評価者は、PP によって義務付けられるすべての監査事象の種類が記述され、またフィールドの記述には FAU_GEN.1.2 に要求される情報と、表 6 において特定される追加的情報が含まれることをチェックして保証しなければならない (shall)。

評価者は特に、失敗した暗号事象の内容に関して操作ガイダンスが明確であることを保証しなければならない (shall)。表 6 においては、操作の暗号モード及び暗号化されようとしているオブジェクトの名称または識別子を詳述することが要求されている。評価者は、その名前または識別子によって十分に管理者が監査ログをレビューして暗号操作の文脈 (例

えば、鍵ネゴシエーションの交換中に行われた、通過するデータの暗号化中に行われた) と、他のIT システムとの通信に関連した暗号の失敗に関する接続のTOE とは反対側のエンドポイントを判断できることを保証しなければならない (shall)。

また評価者は、本 PP の文脈において関連する管理アクションの判断を行わなければならない (shall)。TOE には、その機能がSFR において特定されていないという理由で本 PP の文脈においては評価されない機能が含まれているかもしれない。この機能は、操作ガイダンスに記述される管理的側面を持っているかもしれない。そのような管理アクションは TOE の評価される構成では行われることがないため、評価者は操作ガイダンスを検査して、管理コマンド (サブコマンドを含む)、スクリプト、そして構成ファイルのどれが、PP において特定された要件の実施に必要な TOE に実装されたメカニズムの構成 (有効化または無効化を含む) に関連しているのかを判断し、それによって「すべての管理アクション」のセットを形成しなければならない (shall)。評価者はこのアクティビティを、AGD_OPE ガイダンスが要件を満たしていることの保証と関連付けられたアクティビティの一部として行ってもよい。

評価者は、本 PP の機能要件と関連付けられた保証アクティビティに従って TOE に監査記録を生成させることによって、TOE が正しく監査記録を生成できる能力をテストしなければならない (shall)。また評価者は、本 PP の文脈において該当する管理アクションのそれぞれが監査対象であることをテストしなければならない (shall)。テスト結果を検証する際に、評価者はテスト中に生成された監査記録が管理ガイドにおいて特定されたフォーマットと一致することと、各監査記録のフィールドが適切なエントリを有することを保証しなければならない (shall)。

ここでのテストは、セキュリティメカニズムの直接的なテストと組み合わせて達成できることに注意されたい。例えば、提供された管理ガイダンスが正しいことを保証するために行われるテストは、AGD_OPE.1 が満たされることを検証するため、監査記録が期待どおり生成されたことの検証に必要な管理アクションの呼び出しに対応しているはずである (should)。

FAU_GEN.1.2 [選択、少なくとも 1 つを選択：VoIP クライアントアプリケーション、クライアントデバイスプラットフォーム] は、少なくとも以下の情報を各監査記録内に記録しなければならない (shall)：

- 事象の日付及び時刻、
- 事象の種類、
- サブジェクトの識別情報、
- 事象の結果 (成功または失敗)、及び
- 表 6 の追加的情報。

適用上の注意：

先ほどのコンポーネントと同様に、ST 作成者は生成された追加的情報があればそれによって表 6 をアップデートすべきである (should)。この要件の文脈において「サブジェクトの識別情報」とは、例えば、管理者の利用者 ID または影響されるネットワークインタフェースのどちらかとなる。

保証アクティビティ：

このアクティビティは、FAU_GEN.1.1 のテストと組み合わせて達成されるべきである (should)。

セキュリティ監査事象の選択 (FAU_SEL)

FAU_SEL.1　　選択的監査

FAU_SEL.1.1 VoIP クライアントアプリケーションは、以下の属性に基づいて、すべての監査対象事象のセットから監査されるべき事象のセットを選択できなければならない (shall)：

a) 事象の種類、

b) 監査対象セキュリティ事象の成功、

c) 監査対象セキュリティ事象の失敗、及び

d) [割付：その他の属性]。

適用上の注意：

この要件の意図は、監査事象を引き起こすために選択可能なすべての基準を特定することである。これは、利用者／管理者が呼び出すクライアント上のインタフェースを介して構成することもできるし、またはどの事象が監査されるべきかをクライアントに指示するために SIP サーバが利用するインタフェースであるかもしれない。ST 作成者は、割付を用いて任意の追加基準を列挙するか、または「なし」とする。監査対象事象の種類は、表 6 に列挙されている。

保証アクティビティ：

評価者は管理ガイダンスをレビューして、ガイダンスにすべての事象の種類が列挙されていることと、要件に従って選択可能であるべきすべての属性が (割付中に列挙された属性を含め) 記述されていることを保証しなければならない (shall)。また管理ガイダンスには、事前選択を設定する方法、または SIP サーバがクライアントを構成する方法に関する指示が含まれると共に、(存在するならば) 複数値の事前選択を行うための構文が説明されなければならない (shall)。また管理ガイダンスには、現在強制されている選択基準に関わらず、常に記録される監査記録も特定されなければならない (shall)。

また評価者は、以下のテストを行わなければならない (shall)。

- *テスト 1：要件に列挙される属性のそれぞれについて、管理者はその属性の選択によってその属性を持つ監査事象 (または、管理ガイダンスに特定される、常に記録される監査事象) のみが記録されることを示すテストを考案しなければならない (shall)。*
- *テスト 2 [条件付き]：TSF がさらに複雑な監査事前選択基準 (例えば、複数の属性、属性を用いた論理式) をサポートしている場合には、評価者はこの機能が正しく実装されていることを示すテストを考案しなければならない (shall)。また評価者は、テスト計画書中に、そのテストのセットが典型的なものであり、その機能を行使するのに十分であることを正当化する短い説明文を提供しなければならない (shall)。*

表 6：監査対象事象

要件	監査対象事象	追加監査記録の内容
FAU_GEN.1	なし。	
FAU_SEL.1	監査収集機能が動作している間に生じたすべての監査構成への変更。	なし。
FCS_CKM.1	鍵生成アクティビティの失敗。	なし。
FCS_CKM.2	なし。	
FCS_CKM_EXT.4	鍵ゼロ化プロセスの失敗。	クリアされようとしていたオブジェクトまたはエンティティの識別情報。
FCS_COP.1(1)	暗号化または復号の失敗。	操作の暗号モード、暗号化／

要件	監査対象事象	追加監査記録の内容
		復号されようとしていたオブジェクトの名称／識別子。
FCS_COP.1(2)	暗号署名の失敗。	操作の暗号モード、署名／検証されようとしていたオブジェクトの名称／識別子。
FCS_COP.1(3)	ハッシュ関数の失敗。	操作の暗号モード、ハッシュされようとしていたオブジェクトの名称／識別子。
FCS_COP.1(4)	非データ完全性暗号ハッシュの失敗。	操作の暗号モード、ハッシュされようとしていたオブジェクトの名称／識別子。
FCS_RBG_EXT.1	ランダム化プロセスの失敗。	なし。
FCS_SRTP_EXT.1	SDES/SRTP セションの確立失敗。 SDES/SRTP セションの確立／終了。	失敗の理由。接続の TOE とは反対側のエンドポイント (IP アドレス)。
FCS_TLS_EXT.1	TLS セションの確立失敗。TLS セションの確立／終了。	失敗の理由。接続の TOE とは反対側のエンドポイント (IP アドレス)。
FDP_VOP_EXT.1	なし。	
FIA_SIPC_EXT.1	ピアとのセション確立。	送信元及び送信先アドレス。
FIA_X509_EXT.1	なし。	
FMT_SMF.1	なし。	
FPT_TST_EXT.1	TSF セルフテストのこのセットの実行。検出された完全性違反。	完全性違反については、その完全性違反を引き起こした TSF コードファイル。
FPT_TUD_EXT.1	アップデートの開始。 アップデートの完全性の検証のあらゆる失敗。	追加的情報なし。
FTP_ITC.1	高信頼チャネルを確立しようとするすべての試行。 チャネルデータの改変の検出。	そのチャネルの TOE とは反対側のエンドポイントの識別情報。

高信頼パス／チャネル (FTP)

FTP_ALT_EXT.1　　拡張：高信頼チャネル警報

FTP_ALT_EXT.1 VoIP クライアントアプリケーションは、FTP_ITC.1 において特定されたセキュアなチャネル以外で発呼または着呼があったとき、視覚的警報を提供しなければならない (shall)。

適用上の注意：

この警報は、音声呼が保護されていないことを利用者へ通知する役目をする。開錠された鍵、赤いバナーなど、あらゆる方法の視覚的警報が受容可能である。これは、VoIP アプリケーションが実行中になされた呼にのみ適用される。VoIP アプリケーションは、VoIP アプリケーション／VoIP 技術を利用しないデバイスへの、またはそのようなデバイスからのすべての呼を監視する必要はない。この視覚的警報が設定可能な通知である場合、ST 作成者は FMT_SMF.1 の選択を取り込まなければならない (must)。

保証アクティビティ：

評価者は TSS をチェックして、呼が保護されていない状況と、利用者への視覚的通知を提

供するために用いられる手法とが記述されていることを検証しなければならない (shall)。この視覚的警報が設定可能な通知である場合、TOE ガイダンスにはこの警報を適切に構成するために必要な情報が含まれなければならない (shall)。

評価者は、以下のテストを行わなければならない (shall)。

- *テスト 1 : 評価者は、セキュアチャネルが立ち上がっていることを保証しなければならず (shall)、また TOE への発呼と着呼との両方を行うこと。評価者は、何の視覚的通知も受信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、TSS に記述されている状況のそれぞれに環境を構成し、保護されていない発呼と着呼との両方を TOE で行わなければならない (shall)。評価者は、視覚的警報が表示されることを検証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

エントロピー源の文書は、それを読んだ後の評価者が完全に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理由を理解できるように、十分に詳細であるべきである (should)。本文書には、設計の記述、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の一部である必要はない。

設計の記述

文書には、すべてのエントロピー源コンポーネントの相互作用を含めた、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)。これにはエントロピー源の動作が記述され、どのように動作するのか、どのようにエントロピーが作り出されるのか、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、などが含まれることになる。本文書では、エントロピー源の設計の概略が説明され、ランダム性がどこから由来し、次にどこへ渡されるのか、任意の生の出力の後処理 (ハッシュ、XOR など)、保存されるのか (保存されるとすればどこに)、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が示されるべきである (should)。処理に課される条件があれば (例えば、ブロッキング)、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。

また、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の説明と、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がどのようにしてセキュリティ境界によって確実とされるのかという説明が含まれなければならない (must)。

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的な挙動を示すことがなぜ確信できるのか (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って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) という、技術的な議論が存在すべきである (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と確信できる理由の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含むビットを作り出すと信頼できる理由の正当化の一部となる。

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不調または一貫しない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)。

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

管理者 (Administrator) - TOE を構成する管理特権を有する利用者

正当な (Authorized) - オブジェクト、システムまたはシステムエンティティへのアクセス特権を与えられたエンティティ

クリティカルセキュリティパラメタ (CSP) - セキュリティ関連情報 (例えば、秘密鍵及びプライベート暗号鍵、ならびにパスワードや PIN などの認証データ) であって、その開示または改変が暗号モジュールのセキュリティの侵害をもたらす可能性のあるもの

エントロピー源 (Entropy Source) - この暗号機能は、1 つ以上の雑音源からの出力を蓄積することによって乱数生成器にシードを供給する。この機能には、所与の出力を推測するために必要とされる最低限の労力の計量と、雑音源が適切に動作していることを確実にするためのテストが含まれる。

FIPS 承認暗号機能 (FIPS-approved cryptographic function) - セキュリティ機能（例えば、暗号アルゴリズム、暗号鍵管理技術、または認証技術）であって、 1) 連邦情報処理規格 (FIPS) において特定されているか、 2) FIPS に採用され、FIPS の附属書または FIPS によって参照される文書のどちらかにおいて特定されているもの

IT 環境 (IT Environment) - TOE 境界の外部に存在するハードウェア及びソフトウェアであって、TOE の機能及びセキュリティ方針をサポートするもの

運用環境 (Operational Environment) - その中で TOE が運用される環境

公共ネットワーク (Public Network) - すべての利用者及びエンティティに可視であり、不正なアクセスからの保護が行われないネットワーク (例えばインターネット)

セキュリティ保証要件 (SAR) - TOE が SFR を満たしているという保証を得る方法の記述

セキュリティ機能要件 (SFR) - TOE のセキュリティ対策方針を、標準化された言語に変換したもの

セキュリティターゲット (ST) - 具体的な特定された TOE に関する、実装に依存したセキュリティの必要性の言明

評価対象 (TOE) - ソフトウェア、ファームウェア、またはハードウェアからなるセットで、ガイダンスが伴うことがある。本 PP に関しては、TOE は VoIP クライアントアプリケーションである

脅威エージェント (Threat Agent) - データの破壊、開示、改変、またはサービス拒否、あるいはこれらの組み合わせによって情報システムに危害を加えようと試みるエンティティ

TOE セキュリティ機能 (TSF) - TOE のすべてのハードウェアとソフトウェア、そしてファームウェアの結合した機能であって、SFR の正しい実施のために信頼されなければならない (must) もの

TOE 要約仕様 (TSS) - TOE が SFR のすべてを満たす方法の記述

VoIP クライアントアプリケーション (VoIP Client Application) - 利用者が、保護されていない公共ネットワークを介して暗号化された SDES/SRTP トンネルを確立し、音声データの送信を可能とする TOE

VoIP クライアントアプリケーション利用者 (VoIP Client Application User) - TOE を操作する利用者