ネットワークデバイスプロテクションプロファイル

拡張パッケージ

SIP サーバ

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_nd_sip_ep_v1.0.pdf

Information Assurance Directorate

2013 年 2 月 6 日
バージョン 1.0

平成 26 年 4 月 21 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

改版履歴

バージョン	日付	内容
1.0	2013 年 2 月 06 日	初版発行

1 概論

この拡張パッケージ (EP) は、セッション確立プロトコル (SIP) サーバのセキュリティ要件を記述し、また明確に定義された脅威の低減を目的とした要件の最小ベースラインセットを提供する。しかし、この EP はそれ自体で完結するものではなく、*ネットワークデバイスのセキュリティ要件*プロテクションプロファイル (NDPP) を拡張するものである。この概論では適合評価対象 (TOE) の機能を記述するとともに、この EP が NDPP との関連においてどのように使われるべきかについても論ずる。

この PP は SIP サーバを対象としているため、評価対象 (TOE) は SIP サーバであり、また「SIP server」と「TOE」はこの文書中で区別なく用いられると理解されるべきである (should)。

1.1 適合主張

*ネットワークデバイスのセキュリティ要件*プロテクションプロファイル (NDPP) は、ネットワークインフラストラクチャデバイス一般のベースラインセキュリティ機能要件 (SFR) 及びセキュリティ保証要件 (SAR) を定義する。この EP は、SIP サーバネットワークインフラストラクチャデバイスに特有の追加的 SFR 及び関連する「保証アクティビティ」によって、NDPP ベースラインを拡張するものである。保証アクティビティは、TOE の SFR への適合性を判断するために評価者が実施するアクションである。

この EP 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 版に適合している。CC パート 2 拡張及び CC パート 3 に適合する。

1.2 この拡張パッケージの使用方法

NDPP の EP として、この EP と NDPP 双方の内容が各製品固有のセキュリティターゲットの文脈で適切に組み合わされることが期待される。この EP は、そのような使用方法において困難さやあいまいさが存在しないよう、具体的に定義されている。ST は、適用される NDPP (現行バージョンについては http://www.niap-ccevs.org/pp/を参照) 及びこの EP のバージョンをその適合主張の中で特定しなくてはならない (must)。

1.3 第一世代のプロテクションプロファイル

モビリティに関するセキュリティが、他の技術とは異なる要素は何だろうか？個別デバイスの実際の技術的なセキュリティ機能とは無関係に、有線コンピューティングまたは通信デバイスには暗黙のセキュリティが存在する。それは、デバイスが存在する物理環境が警備員や番犬、そしてフェンスによって保護されている場合である。モビリティに関しては、このような伝統的な物理的保護は期待できない。敵対者にとって無線通信チャネルがより容易に利用可能であるだけでなく、デバイス自身も多用途であり、仕事とエンタープライズデータの両方に利用されることが予想される。モビリティが新たなセキュリティの課題をもたらすことは明白である。

急速に発展しつつあるモビリティ市場に追随するため、Information Assurance Directorate (IAD) は第一世代のモビリティ PP 及び EP を発行することによって、モビリティのセキュリティの欠損または不完全な実装のリスクを管理しようとしている。これらの第一世代のモビリティプロファイルが、IAD が必要とするセキュリティ機能を持った商用製品のプールから選択を行うためのメカニズムとなる。ベンダがすでにモビリティへの取り組みへの参加を要請しており、また第一世代ソリューションの実装に対して IAD が期限を設けているため、精力的なスケジュールが必要である。モビリティ PP の第一世代は、モバイル OS PP と SIP サーバ EP (この文書)、そしてモビリティアプリケーション(VOIP) PP から構成され

る。これらの PP 及び EP の目標は、現状の要件と現時点で何が可能かを提示し、セキュリティ的に不可欠なコンポーネントによってエンタープライズのセキュリティを向上させるための明確な方向付けをすることである。

望まれるモビリティのセキュリティ機能の一部は、今後 18 か月のうちに登場することは望めないかもしれない。現時点での民間企業の最前線を超えるこれらの機能が、暫定的なモビリティソリューションや、第一世代のモビリティプロファイルによってサポートされることはおそらくないだろう。IAD は、ベンダとの共同作業によってこれらの機能を有する製品をどこで、いつ入手できるか、そして対応する PP 及び EP を (いつ) 作成すべきかを判断することになる。

1.4 適合評価対象

これは SIP サーバの EP である。エンタープライズ向けボイスオーバーIP (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。セッ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。SIP サーバは VoIP クライアントと対話して、VoIP 呼の確立、処理、そして終了とともに、呼セッ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。登録済みサーバとして、SIP サーバは REGISTER 要求を受け付け、受信した情報をサーバ上のロケーションサービスへ渡す。SIP プロキシサーバとしてのサーバは、トランザクションを管理して SIP 要求及び応答をルーティングするステートフルなサーバである。

記述された脅威環境へ対応して TOE が実装を義務付けられる機能は以下のセクションで詳細にわたって論ずるが、ここで簡単に説明しておくことにする。適合 TOE は、それ自身への脅威に対処するセキュリティ機能を提供する。また、それ自身と VoIP クライアント (すなわち、スマートフォン) や別の SIP サーバとの間の通信も、TLS によって保護されたチャネルを用いて保護しなくてはならない (must)。レジストラサーバとして、SIP サーバは SIP REGISTER を行う SIP 利用者のユーザ／パスワード認証を要求する。この PP によって要求されるプロトコルは証明書を利用するため、SIP サーバは証明書と秘密鍵をセキュアに保存しなくてはならない (must)。図 1 に示すように、SIP サーバは保護されたトランスポート層セキュリティ (TLS) チャネル上で VoIP クライアントとの通信を行う。赤で示したコンポーネントが、この PP の対象となる。青で示したコンポーネントは、関連する PP の対象となる。

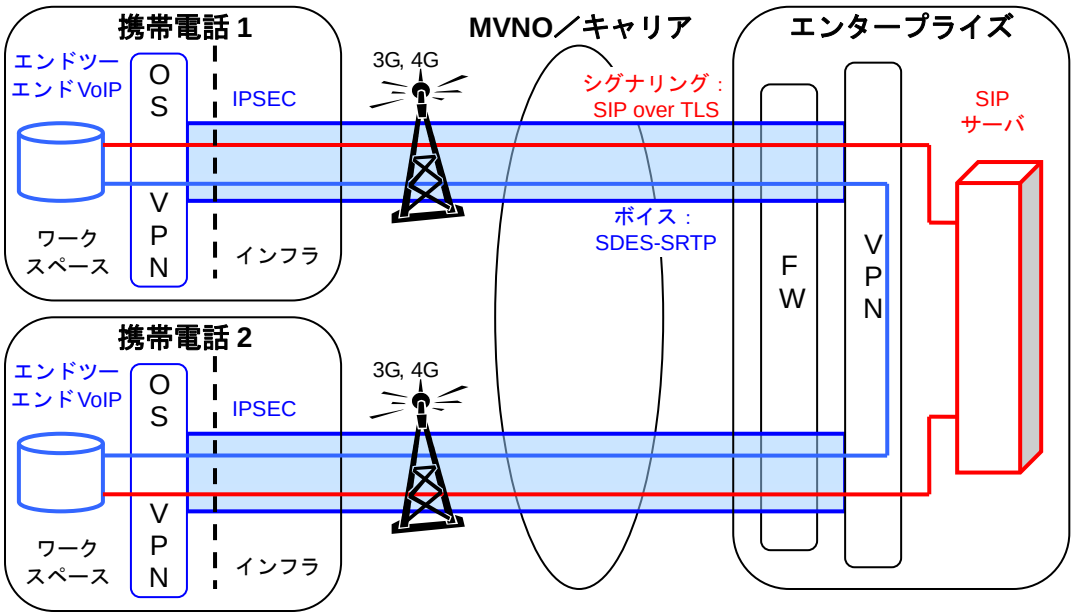

図 1：VoIP 通信

この EP は NDPP 上に構築されるため、適合 TOE は NDPP に要求される機能と共に、本書で以下に論ずる脅威環境に対応して、この EP に定義される追加機能をも実装することが義務付けられる。

この EP における一連の要件は、より迅速かつ安価な評価を推奨してエンドユーザへ価値を提供するため、意図的に範囲が限定されている。大量の追加機能（及び要件）を含むセキュリティターゲット（ST）は推奨されない。

2 セキュリティ課題記述

SIP サーバは、特定の種類の SIP サーバや特定の SIP サーバ機能を対象とするのではなく、SIP サーバー般に共通した脅威及び方針に対処しなくてはならない（must）。附属書 A には、セキュリティ課題記述（SPD）をより「伝統的」な形で提示してある。以下のセクションでは、附属書 A の「伝統的」な言明への参照を含めて、適合 TOE が対処する課題を詳述する。

この EP では NDPP で特定された脅威を繰り返すことはしないが、この EP の NDPP への適合性、したがって依存性のためにはそれらの脅威がすべて適用されることに注意されたい。また、NDPP には TOE がそのセキュリティ機能を提供するための能力への脅威のみが含まれる一方で、この EP は運用環境におけるリソースへの実際上の（business）脅威のみを取り扱うことにも注意されたい。NDPP の脅威とこの EP に定義される脅威とを合わせて、VPN TOE によって対処されるセキュリティの脅威の包括的なセットが定義されるのである。

2.1 TOE との通信

SIP サーバは、通信ネットワーク上で他の SIP サーバ、VoIP クライアント、そして管理者と通信する。その通信の端点は地理的にも論理的にも TOE から遠くにあり、さまざまな他のシステムを通過する可能性があるが、これらは敵対者の制御下にあるかもしれず、したがって SIP サーバとの通信が危殆化する機会が生じるかもしれない。VPN トンネルによって TOE がエンタープライズと通信する層のセキュリティは提供されるが、さらに呼制御ト

ラフィック及びリアルタイムサービスのメディアストリームを保護するために、追加的なセキュリティ層が必要となる。

SIP サーバとの通信が暗号化されなければ、パスワードや鍵、構成設定、及び経路情報の更新などの重要なデータが中間システムによって直接読まれたり操作されたりするかもしれず、サーバの危殆化を引き起こすおそれがある。いくつかのプロトコルを使って保護を提供することは可能である。しかし、これらのプロトコルには、それぞれのプロトコルを仕様に準拠したままカスタマイズするために使用可能な、多数のオプションが存在する。これらのオプションの一部は、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、たとえ RFC で許可されているものであっても弱い暗号アルゴリズムを使えば、敵対者が暗号化されたチャネル上のデータを読み出したり操作したりすることが可能となるかもしれず、そのような攻撃を防止するために用意された対策が迂回できてしまうかもしれない。さらに、めったに使われない、または非標準のオプションと共にプロトコルが実装されている場合、それはプロトコル仕様には準拠しているかもしれないが、同一のプロトコルを利用する他の機器とは相互運用が不可能であるかもしれない。

通信経路が保護されていたとしても、モバイルデバイスのアプリケーションや SIP サーバなどの外部エンティティ、またはピアルータなどの高信頼 IT エンティティがだまされて、悪意のある攻撃者を SIP サーバだと思い込んでしまうこともあり得る。同様に、SIP サーバもだまされて、実際にはそうではないのに本物のリモートエンティティと通信を確立していると思い込んでしまうかもしれない。また攻撃者が中間者攻撃を仕掛けることによって中間システムが危殆化し、トラフィックが危殆化したシステムによってプロキシされ、調査され、そして改変されてしまうかもしれない。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行われる可能性がある。これらの攻撃の一部は、有効な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ために、攻撃者が認証セッションなどのトラフィックのセグメントをキャプチャしてそのトラフィックを再利用することによって行われる。

[T.UNAUTHORIZED_ACCESS]

3 セキュリティ対策方針

SIP サーバはセキュリティ機能を提供し、サーバへの脅威へ対処するとともに法令によって課される方針を実装する。以下のセクションでは、この機能の記述を提供する。このセキュリティ機能は、サーバのエレメント間の、及び VoIP クライアントへの保護された通信に焦点を絞っている。そのセキュリティ対策方針の記述は、[NDPP] に記述されたものへの追加である。

3.1 保護された通信

セクション 2.1 に記述された SIP サーバへの、そして SIP サーバからの機密性のあるデータの送信に関する課題へ対処するため、サーバは自分自身とエンドポイントとの間の通信経路を暗号化する。これらの通信チャネルは、TLS を用いて実装される。TLS は、相互運用性と攻撃への耐性を提供する。SIP サーバは TLS をサポートしなくてはならない (must) が、追加的なアルゴリズムやプロトコルをサポートしてもよい。これらの追加的なアルゴリズムやプロトコルが評価されるかどうかは、スキームによって異なる。それらが評価されない場合、サーバの運用中にそれらが無効化できるよう管理者へ通知されるか、規定されたセキュリティ機能に影響しないことが示されなくてはならない (must)。

通信に開示からの保護と改変の検出を提供する他にも、TLS は暗号学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、もし 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、通信の相手方のふりをしようとしても、その試みは検出され

るということを意味する。また TLS プロトコルは、セクション 2.1 に記述したようなリプレイ攻撃に対する保護も提供する。これは通常、その通信のリプレイが検出できるように、各通信に例えばタイムスタンプなどの一意の値を含めることによって行われる。

(FCS_CKM.1(*), FCS_CKM_EXT.4, FCS_COP.1(*), FCS_TLS_EXT.1, FCS_RBG_EXT.1, FIA_SIPS_EXT.1, FIA_X509_EXT.1, FTP_ITC.1(*))

3.2 システム監視

管理者が SIP サーバの動作を監視できるようにするという課題に対処するため、NDPP に由来するこのセキュリティ対策方針は、以下のように拡張される。

適合 TOE は、TLS セッションの確立、及び SIP セッションの確立をログに記録する能力を実装すること。

(FAU_GEN.1)

3.3 TOE の管理

VPN ゲートウェイ　管理の信頼できる手段に伴う課題に対処するため、NDPP に由来するこのセキュリティ対策方針は、以下のように拡張される。

適合 TOE は、SIP クライアントとの運用に要求される SIP 実装の側面と共に、TLS 接続の暗号的側面を管理者が構成するために必要な機能を提供すること。

(FMT_SMF.1)

4 セキュリティ要件

この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 改定第3 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。

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。この文書では、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 作成者によってなされた詳細化：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って示される。
- 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」を付けることによって特定される。

4.2 TOE セキュリティ機能要件

4.2.1 NDPP セキュリティ機能要件の指示

このセクションでは、SIP サーバ EP 中の関連する SFR をサポートするために、NDPP に含まれる特定の SFR にどの選択を行わなくてはならない (must) かを ST 作成者に指示する。これは、強制的な選択が行われるエレメントを表明することによって達成される。ST 作成者は、残った選択項目を自分の望む通りに選んでよい。特定の機能またはふるまいが TOE に存在することを確実にするため、SFR エレメント中の選択も行われている。

このセクションでは要件に関して保証アクティビティを繰り返すことはしない。これらはすでに NDPP に取り込まれているからである。ここで規定したように SFR に対して ST 及び TOE を評価する際に評価者にとって重要なことは、適切な選択が行われていること、及び要件への適合性を例証するために適切なテストが実施されることである。

FCS_COP.1(1) 暗号操作 (データの暗号化／復号)

FCS_COP.1.1 TSF は、*GCM*、*[割付：1 つ以上のモード] で動作する*、暗号鍵サイズが *128 ビット*、*256 ビット*、*及び [選択：192 ビット*、*その他の鍵サイズなし]* の、下記を満たす規定された暗号アルゴリズム *AES* にしたがって*暗号化及び復号*を行わなくてはならない (shall)。

- *FIPS PUB 197, “Advanced Encryption Standard (AES)”*
- *[選択：NIST SP 800-38A*、*NIST SP 800-38B*、*NIST SP 800-38C*、*NIST SP 800-38D*、*NIST SP 800-38E]*

適用上の注意：

このEP は、TLS プロトコルにおいてGCM の使用を要求する (FCS_TLS_EXT.1)。したがって、TLS 要件と一貫して ST 作成者がこのモードを確実に取り込むよう、NDPP 中の FCS_COP.1.1(1) エレメントがここに規定される。ST 作成者には、NDPP のリモート管理要件をサポートするために他の適切なモードを追加することが期待される。

FMT_SMF.1 管理機能の仕様

FMT_SMF.1.1 TSF は、下記の管理機能を行えなくてはならない (shall)。

a. *SIP を構成する能力、*
b. *FCS_TLS_EXT.1 に関連して実装されたメカニズムを構成する能力、*
c. *SIP クライアントのパスワードを構成する能力、*
d. *FTA_TAB.1 の通知及び同意警告メッセージを構成する能力、*
e. *FTA_SSL_EXT.1 のローカルセッション継続時間のインアクティビティ継続時間を構成する能力。*

適用上の注意：

上に列挙したエレメントは、ST 作成者によって選択された NDPP 中のエレメントと組み合わされて、TOE によって実装される管理機能の全体セットを形成する。

FPT_TUD_EXT.1 拡張：高信頼更新

FPT_TUD_EXT.1.3 TSF は、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、TOE へのファームウェア／ソフトウェア更新を、それらの更新をインストールする前に検証する手段を提供しなくてはならない (shall)。

適用上の注意：

NDPP では、ST 作成者が検証手法を指定できる選択肢を提供している。この EP へ適合するには、デジタル署名メカニズム (FCS_COP.1(2) に規定されたものの 1 つ) が採用されなくてはならない (must)。ST 作成者は、NDPP の FPT_TUD_EXT.1 のその他の 2 つのエレメントを ST へ取り込むべき (should) であることに注意されたい。

4.2.2 暗号サポート (FCS)

これを含めた以下のサブセクションでは、この EP によって TOE に課される要件であって NDPP に含まれないものが定義される。

FCS_TLS_EXT.1 トランスポート層セキュリティ

FCS_TLS_EXT.1.1 TSF は、証明書と以下の暗号スイートによる相互認証を用いた、Suite B Profile for TLS (RFC 6460) に準拠する TLS 1.2 プロトコル (RFC 5246) を実装しなくてはならない (shall)。

必須暗号スイート：

FIPS-186-2 に規定される 256 ビット prime modulus 楕円曲線を用いた TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256、

FIPS-186-2 に規定される 384 ビット prime modulus 楕円曲線を用いた TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384、

オプションの暗号スイート：

[選択：

なし、

FIPS-186-2 に規定される 256 ビット prime modulus 楕円曲線を用いた TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA、

FIPS-186-2 に規定される 384 ビット prime modulus 楕円曲線を用いた TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA 、

適用上の注意：

評価済み構成に用いられる暗号スイートは、この要件によって制限される。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)。実装によってネゴシエーションされるスイートをこの要件中のものに制限するために管理手順が取られる必要がある場合、AGD_OPE によって要求されるガイダンス中にその適切な指示が含まれる必要がある。

上に列挙した必須 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、この PP の将来の版では、SSL/TLS プロトコルの規定された古いバージョンを使用したすべての接続試行を拒否するための手段を提供することが TOE に求められることになる。

保証アクティビティ：

TSS

評価者は TSS 中のこのプロトコルの実装の記述をチェックして、オプションの特徴 (例えば、サポートされる拡張、サポートされるクライアント認証) が規定され、またサポートされる暗号スイートも規定されていることを確証しなくてはならない (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このコンポーネントに列挙されたものと同一であることを確証しなくてはならない (shall)。

テスト

評価者はまた、下記のテストを実施しなくてはならない (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 接続を確立しなくてはならない (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、SIP 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が成功することを (通信路上で) 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調査する必要はない。

4.2.3 識別と認証 (FIA)

FIA_SIPS_EXT.1 セッション確立プロトコル (SIP) サーバ

FIA_SIPS_EXT.1.1 TSF は、RFC 4566 に準拠するセッション記述プロトコル (SDP) を用いて VOIP トラフィックを搬送するマルチメディアセッションを記述する、RFC 3261 に準拠するセッション確立プロトコル (SIP) を実装しなくてはならない (shall)。

FIA_SIPS_EXT.1.2 TSF は、RFC 3261 のセクション 22 に規定される SIP REGISTER 機能要求にパスワード認証を要求しなくてはならない (shall)。

FIA_SIPS_EXT.1.3 TSF 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くてはならない (shall)。

適用上の注意：

(TOE によって) 認証されることが要求される唯一の SIP 要求は REGISTER 要求である。SIP サーバは強制を行って正しいパスワードの提示によって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 TOE 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_SIPS_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中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することが要求される。

保証アクティビティ：

TSS

評価者は TSS を調査して、SIP セッ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くてはならない (shall)。これには SIP セッションの開始、利用者の登録、そして発呼と着呼の両方が取り扱われる(開始され、記述され、そして終了される) 方法が含まれなくてはならない (shall)。またこの記述には、パスワードが TOE によって受信された時点から利用者が認証される時点までの取り扱いの記述も含まれなくてはならない (shall)。

テスト

テストは、クライアントをテストの遠端として用いる観点から記述されている。同一の機能を示す代替手法は許容される。評価者は、下記のテストを実施しなくてはならない (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従わなくてはならない (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くてはならない (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従わなくてはならない (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くてはならない (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) 確認しなくてはならない (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くてはならない (shall)。テスト報告には、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くてはならない (shall)。*

X509 証明書 (FIA_X509_EXT)

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 (及び関連する秘密鍵) である。

FIA_X509_EXT.1 拡張：X.509 証明書

FIA_X509_EXT.1.1 TSF 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くてはならない (shall)。

適用上の注意：

RFC 5280 には、この要件にしたがって TOE が実装しなくてはならない (must) 証明書有効性確認と認証パス検証の要件が定義されていることに注意すべきである (should)。

FIA_X509_EXT.1.2 TSF は、この PP に規定されるセキュリティ機能によって使用される X.509v3 証明書をエンタープライズが TOE へロードする機能を提供しなくてはならない (shall)。

FIA_X509_EXT.1.3 TSF は、[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)、RFC 5759 に規定される証明書失効リスト (CRL)] を用いて証明書を検証しなくてはならない (shall)。

FIA_X509_EXT.1.4 TSF は、証明書が無効と判断された場合、TLS 接続を確立してはならない (shall not)。

FIA_X509_EXT.1.5 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いとき、TSF は、エンタープライズによる構成により、TLS 接続を確立するか、あるいは TLS 接続の確立を禁止しなくてはならない (shall)。

FIA_X509_EXT.1.6 TSF は、証明書を保存し不正な削除及び改変から保護しなくてはならない (shall)。

適用上の注意：

FIA_X509_EXT.1.5 の意図は、証明書有効性確認情報を提供する役割のエンティティに TOE が接続できない場合に、TOE にセッションの確立を許可するか禁止するか構成できるようにしておくことである。例えば、マシンがダウンしているかネットワークパスが切断されているために CRL が取得できない場合には、CA へ到達できないという理由で TOE が新たな接続を確立できなくしてしまうのではなく、引き続きセッションを確立できるように TOE を構成することを管理者は選択するかもしれない。

保証アクティビティ：

TSS

評価者は、この EP の要件を満たすために使われる証明書を含め、実装されたすべての証明書ストアが TSS に記述されていることを確証しなくてはならない (shall)。この記述には、証明書がストレージへロードされる方法と、ストレージを不正なアクセスから保護する方法に関する情報が含まれなくてはならない (shall)。

ガイダンス

評価者はガイダンス文書を調査して、証明書の不正な改変または削除を防止するために TOE または環境のいずれかを構成する方法が記述されていることを確証しなくてはならない (shall)。

テスト

評価者は、証明書の使用を要求するシステム内の機能のそれぞれについて、以下のテストを行わなくてはならない (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ことを例証しなくてはならない (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くてはならない (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くてはならない (shall)。

要件が満たされていることを確証するためのテストは、FTP_ITC.1(2) 中の TLS 要件と組み合わせて行われる。

4.2.4 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**：TSF 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~~または~~開示からの保護を提供する、**FCS_TLS_EXT.1 [選択：「のみ」、「及び FCS_DTLS_EXT.1」] に規定される TLS [選択：「及びその他のプロトコルなし」、「及び DTLS」] を用いた**それ自身と **SIP クライアント**との間の通信チャネルを提供しなくてはならない (shall)。

FTP_ITC.1.2(2) TSF は、TSF クライアント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くてはならない (shall)

FTP_ITC.1.3(2) TSF クライアントは、 [SIP サーバとのすべての通信] について、高信頼チャネルを介して通信を開始しなくてはならない (shall)。

適用上の注意：

SIP クライアントは起動時に TOE との接続を確立し、これは SIP クライアントを含む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が、DTLS も許容される。DTLS も実装される場合には、ST 作成者は FTP_ITC.1.1(2) 中の各選択の 2 番目を選択するべきである (should)。それ以外の場合には、最初が選択されることになる。DTLS が実装される場合、附属書 C の DTLS 要件も ST の本文へ移動されることになる。

保証アクティビティ：

TSF

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くてはならない (shall)。

テスト

評価者は、通信が SIP クライアントから開始できることを検証しなくてはならない (shall)。

FTP_ITC.1(3) TSF 間高信頼チャネル (改変または開示からの保護 - SIP サーバ)

FTP_ITC.1.1(2) **詳細化**：TSF 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、 **[選択：IPsec、SSH、TLS、TLS/HTTPS] を用いた**それ自身と他の **SIP サーバ**との間の通信チャネルを提供しなくてはならない (shall)。

FTP_ITC.1.2(2) TSF は、**TOE またはピア SIP サーバ**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くてはならない (shall)

FTP_ITC.1.3(2) TSF は、 [*SIP サーバピアへ SIP データを渡す*] 際に、高信頼チャネルを介して通信を開始しなくてはならない (shall)。

適用上の注意：

この要件は、TOE が他の SIP サーバとの通信を確立する場合に対処する。このチャネルは、NDPP 中のリモート管理接続と同様に保護されることが要求される。上で ST 作成者によって選択されたプロトコルは、NDPP から ST へ取り込まれるべきである (should)。

保証アクティビティ：

TSF

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くてはならない (shall)。

テスト

評価者は、通信が TSF と他の SIP サーバの両方から開始できることを検証しなくてはならない (shall)。NDPP から取り込まれたコンポーネントに基づいて、追加的な保証アクティビティが必要とされるかもしれない。

4.2.5 セキュリティ監査

セキュリティ監査に関する追加的 SFR は存在しないが、NDPP に見出される FAU_GEN.1 SFR を拡張するための追加監査対象イベントが存在する。それゆえ、適合セキュリティターゲットの文脈において下記のイベントは NDPP のイベントと結合されるべきである (should)。

下記の監査イベントが、この EP に要求される。

4-1 FAU_GEN.1 監査イベント及び詳細

要件	監査対象イベント	追加監査記録の内容
FCS_TLS_EXT.1	ピアとのセッション確立	送信元及び送信先アドレス 送信元及び送信先ポート TOE インタフェース
FIA_X509_EXT.1	CA とのセッション確立	送信元及び送信先アドレス 送信元及び送信先ポート TOE インタフェース
FIA_SIPS_EXT.1	ピアとのセッション確立	送信元及び送信先アドレス 送信元及び送信先ポート TOE インタフェース

4.3 セキュリティ保証要件

この EP に対して評価される TOE は、本質的に NDPP に対しても評価されることは重要なので注意されたい。NDPP には、セキュリティ機能要件 (SFR) 及び SAR の双方に関連する数多くの保証アクティビティが含まれている。それに加えて、この EP には NDPP に特定された EAL に関連付けられた SAR を同様に詳細化する、SFR ベースの保証アクティビティが数多く含まれている。NDPP によって規定される SAR に関連付けられた保証アクティビティは TOE 全体に対して行われる。

根拠

脅威を対策方針へ、そして対策方針を要件へ追跡する根拠は、セクション 2.0 及び 3.0 の本文に含まれている。未解決となっている対応付けは前提条件と組織のセキュリティ方針についてのもののみであり、これらは下記の附属書 A に含まれている。

附属書 A： 参考表

このプロテクションプロファイルにおいて、この文書の最初のほうのセクションでは全体的なわかりやすさの向上を重視して、ネットワークデバイスへの脅威、これらの脅威を低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低減の程度について、説明文を提示した。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、この附属書では表形式のアーティファクトを用いて、この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。

PP 作成者は、自分たちの特有の技術においてもこれらの前提条件が引き続き満たされることを確実にすべきである (should)。表は適宜変更されるべきである (should)。

表 3：TOE の前提条件

前提条件の名称	前提条件の定義
A.NO_GENERAL_PURPOSE	TOE の動作、管理、及びサポートに必要なサービス以外に、TOE 上で利用可能な汎用コンピューティング機能 (例えば、コンパイラやユーザアプリケーション) が存在しないことが前提とされる。
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、環境によって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信頼された方法で遵守し適用すると信頼されている。

脅威

以下の脅威は、この文書に記述された要件を取り込む際に、PP 作成者によって技術に特有の脅威と統合されるべきである (should)。要件の変更、削除、及び追加はこのリストに影響を与えるかもしれないので、PP 作成者は適宜これらの脅威を変更または削除すべきである (should)。

表 4：脅威

脅威の名称	脅威の定義
T.ADMIN_ERROR	管理者が意図せず TOE に正しくないインストールまたは構成を行い、その結果としてセキュリティメカニズムの効果がなくなるおそれがある。
T.TSF_FAILURE	TOE のセキュリティメカニズムが故障し、TSF の危殆化をもたらすおそれがある。
T.UNDETECTED_ACTIONS	悪意のある遠隔利用者または外部 IT エンティティが、TOE のセキュリティに悪影響を及ぼすアクションを取るおそれがある。これらのアクションが検出されないままとなり、したがってその影響が効果的に低減できないおそれがある。
T.UNAUTHORIZED_ACCESS	利用者が、TOE データ及び TOE 実行可能形式コードへの権限のないアクセスを行うおそれがある。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 リソースへアクセスするために正当なエンティティに成りすますおそれがある。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おそれがある。
T.UNAUTHORIZED_UPDATE	悪意のある当事者が製品への更新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危殆化させるおそれがある。
T.USER_DATA_REUSE	利用者データが、本来の送信者が意図しない宛先へ不用意に送信されるおそれがある。

TOE のセキュリティ対策方針

表 6：TOE のセキュリティ対策方針

TOE セキュリティ対策方針	TOE セキュリティ対策方針の定義
O.PROTECTED_COMMUNICATIONS	TOE は、管理者、分散 TOE の他の部分、そして正当な IT エンティティへ、保護された通信チャネルを提供すること。
O.VERIFIABLE_UPDATES	TOE は、TOE へのいかなる更新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。
O.SYSTEM_MONITORING	TOE は、監査データを生成し、そのデータを外部 IT エンティティへ送信する機能を提供すること。
O.DISPLAY_BANNER	TOE は、TOE の利用に関して助言する警告を表示すること。
O.TOE_ADMINISTRATION	TOE は、管理者のみがログインして TOE を構成できることを確実にするメカニズムを提供し、またログインした管理者へ保護を提供すること。
O.RESIDUAL_INFORMATION_CLEARING	TOE は、保護されたリソースに含まれるいかなるデータも、そのリソースが再割り当てされた際に入手できないことを確実にすること。
O.SESSION_LOCK	TOE は、放置されたセッションがハイジャックされるリスクを低減するメカニズムを提供すること。
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。

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追加を反映して増補されるべきである (should)。

表 7：運用環境のセキュリティ対策方針

TOE セキュリティ対策方針	TOE セキュリティ対策方針の定義
OE.NO_GENERAL_PURPOSE	TOE の動作、管理、及びサポートに必要なサービス以外に、TOE 上で利用可能な汎用コンピューティング機能 (例えば、コンパイラやユーザアプリケーション) が存在しない。
OE.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、環境によって提供される。
OE.TRUSTED_ADMIN	TOE 管理者は、すべての管理ガイダンスを信頼された方法で遵守し適用すると信頼されている。

附属書C： 追加的要件

この PP の本体で示したように、適合 TOE が対策方針へ対処するために要求される特定のセキュリティ機能を行う方法はいくつか存在する。PP 本体の中の要件は、TSF によって実装されなくてはならない (must) これらの機能を示す。しかし、TSF とモバイル OS のどちらかによって実装されてもよい、あるいはまったく実装されなくてもよい、その他の機能も存在する。以下のセクションには、そのような要件のリストが含まれている。これらが TSF によって実装される場合には、その要件は ST 作成者によって ST の本体へ移動されることになる。

行われた選択によっては、ST の冒頭の説明的情報に軽微な調整が必要とされるかもしれないことに注意されたい。

C.1.1 データグラムトランスポート層セキュリティ

TLS 上の SIP は、TOE によって実装されなくてはならない (must)。しかし、TLS に加えて DTLS が実装されることも許容可能である。DTLS がサポートされる場合、以下の要件が ST 作成者によって取り込まれることになる。

FCS_DTLS_EXT.1 拡張：データグラムトランスポート層セキュリティ

FCS_DTLS_EXT.1.1 TSF は、RFC 6347 にしたがって DTLS プロトコルを実装しなくてはならない (shall)。

FCS_DTLS_EXT.1.2 TSF は、RFC 6347 にしたがった変動が許可される場合を除き、DTLS の実装には FCS_TLS_EXT.1 の中の要件を実装しなくてはならない (shall)。

適用上の注意：

DTLS と TLS との違いは RFC 6347 に概説されている。それ以外の点では、これらのプロトコルは同一である。特に、TOE に定義される適用可能なセキュリティ特性については、2 つのプロトコルに違いはない。したがって、FCS_TLS_EXT.1 に列挙されたすべての適用上の注意と保証アクティビティは、DTLS の実装に適用される。

保証アクティビティ：

評価者は、FCS_TLS_EXT.1 に列挙された保証アクティビティを行って、このコンポーネントを検証しなくてはならない (shall)