PC クライアントデバイスの BIOS 更新
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_bios_v1.0.pdf

Information Assurance Directorate

2013 年 2 月 12 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

表の目次

改版履歴

バージョン	日付	内容
1.0	2012 年 5 月 4 日	初版発行

1 PP 概論

1.1 TOE の PP 概要

1 これは、PC クライアントデバイスの基本入出力システム (BIOS) のための標準プロテクションプロファイル (PP) の第一世代である。BIOS、またはシステム BIOS は、PC クライアントデバイス上のハードウェア初期化プロセスを実行し、オペレーティングシステムへ制御を受け渡すために用いられる主要なファームウェアである。この PP は、敵対者が PC クライアントデバイス上の BIOS を置き換えることによって永続的な方法で PC クライアント環境を危殆化するという主要な脅威に対処する。

2 この PP の評価対象 (TOE) は PC クライアントデバイスである。PC クライアントデバイスは、デスクトップやラップトップコンピュータなどのモダンなコンピュータである。この PP は、現在及び将来の x86 と x64 アーキテクチャのクライアントプラットフォームに焦点を絞っており、またいかなる特定のシステム設計とも独立したものである。この PP への適合を主張すべき (should) システムには、x86 と x86-64 アーキテクチャのデスクトップとラップトップシステムが含まれる。この PP の評価対象としては意図されていないが、同等の認証された BIOS 更新の保護が実装される可能性があるためこの PP の適用対象となる可能性のあるデバイスの例としては、モバイルデバイス (タブレットやスマートフォンなど) とサーバが挙げられる。

3 BIOS ファームウェアには、いくつかの異なる種類が存在する。一部のコンピュータは 16 ビットの従来の BIOS を使用しているが、より新しい多くのシステムではユニファイドエクステンシブルファームウェアインタフェース (UEFI) 仕様 [12] に基づいたブートファームウェアを用いている。BIOS は通常、相手先ブランド製造業者 (OEM) と独立 BIOS ベンダの両方によって開発され、マザーボード (不揮発性メモリに保存される) またはコンピュータメーカーによってエンドユーザへ配付される。バグ修正や脆弱性のパッチ、そして新しいハードウェアのサポートのため、メーカーは頻繁にシステムファームウェアを更新する。システム BIOS は電気的消去可能プログラマブル ROM (EEPROM) やその他の形態のフラッシュメモリ上に保存され、エンドユーザによって更新が可能である。システム BIOS ファームウェアは、BIOS が保存されている不揮発性記憶コンポーネントについて特別な知識を持ったユーティリティやツールを用いて更新される。システム BIOS は、コンピュータの電源投入時に中央処理装置 (CPU) 上で実行される最初のソフトウェアである。モダンなマシン上での BIOS の主要な役割は、ハードウェアコンポーネントの初期化とテストを行い、そしてオペレーティングシステムをロードすることである。さらに、BIOS は電源管理や熱管理などの重要なシステム管理機能をロードし、初期化する。またシステム BIOS は、ブートプロセス中に CPU マイクロコードのパッチをロードすることもある。

1.1.1 評価対象 (TOE) の利用方法と主要なセキュリティ機能

4 この PP は、PC クライアントシステム上の BIOS ファームウェアの不正な変更を防止するためのセキュリティ機能要件 (SFR) とセキュリティ保証要件 (SAR) を提供するものであり、NIST SP 800-147, *BIOS Protection Guidelines* [4] に記載される勧告に基づいている。この PP における BIOS という用語には、NIST SP 800-147 [4] のセクション 1.2 (1-1 ページ) に記述される以下の定義が含まれる。

> *「この版に用いられているとおり、BIOS という用語は従来の BIOS、エクステンシブルファームウェアインタフェース (EFI) BIOS、そしてユニファイドエクステンシブルファームウェアインタフェース (UEFI) BIOS を指す。この文書は、コンピュータシステムのシステムフラッシュメモリに保存されるシステム BIOS ファームウェア (例えば、従来の BIOS や UEFI BIOS など) に適用され、これにはオプション ROM としてフォーマットされる可能性のある部分が含まれる。しかし、*

コンピュータシステム中の他の部分に保存されるオプションROM やUEFI ドライバ、そしてファームウェアには適用されない。」

5 この PP に定義される TOE は PC クライアントデバイスであるが、この PP に定義されるセキュリティ機能要件はシステムフラッシュメモリ中に保存される BIOS ファームウェアに適用される。これには、システム BIOS ファームウェアとともに保存され、同一のメカニズムによって更新されるオプション ROM や UEFI ドライバが含まれる。コンピュータシステム中の他の部分に保存されるオプション ROM や UEFI ドライバ、そしてファームウェアには適用されない。

6 システム BIOS は、セキュアなシステムの不可欠なコンポーネントである。ブートプロセス中に実行される最初のコードとして、BIOS はシステム内のハードウェアとソフトウェアのコンポーネントから暗黙に信頼されている。したがって、この PP に適合する PC クライアントデバイスは、BIOS の更新に用いられるメカニズムをセキュアに保つことによって、配備された後の BIOS の完全性を維持しなくてはならない (must)。TOE には、認証された BIOS 更新メカニズムが含まれる。この認証された BIOS 更新メカニズムには、BIOS 更新イメージの真正性を確保するためにデジタル署名が用いられる。認証された BIOS 更新メカニズムを用いて BIOS を更新するためには、署名検証アルゴリズムと、BIOS 更新イメージの署名を検証するために必要な公開鍵が含まれた鍵保管を含む、更新の信頼のルート (RTU) が存在しなくてはならない (shall)。鍵保管と署名検証アルゴリズムは、保護された形でコンピュータシステムに保存されなくてはならず (shall)、また認証された更新メカニズムかセキュアなローカル更新メカニズムを用いてのみ変更可能でなくてはならない (shall)。この PP の文脈においては、RTU は鍵保管と暗号アルゴリズムを含む抽象概念であり、TSF の一部である。

7 鍵保管と署名検証アルゴリズムは、保護された形でコンピュータシステムに保存されなくてはならず (shall)、また認証された更新メカニズムかセキュアなローカル更新メカニズムを用いてのみ変更可能でなくてはならない (shall)。この PP の文脈においては、RTU は TSF の一部である。

8 更新メカニズムもまた TSF の一部であり、BIOS 更新イメージがデジタル署名されていること、またそのデジタル署名が RTU 中の鍵を用いて BIOS 更新前に検証可能であることを確証しなくてはならない (shall)。また回復メカニズムが提供される場合には、回復プロセスがセキュアなローカル更新の要件を満たしている場合を除いて、TOE は更新メカニズムを使用しなくてはならない (shall)。

9 TSF のもうひとつの側面は、BIOS や同一のフラッシュメモリ中に保存されるエンティティへの「書き込み」や変更をコントロールする機能である。これによって、BIOS を変更するための唯一の方法に、高信頼更新メカニズムの使用が必要とされることが確実となる。

10 BIOS の実装にはオプションとして、認証された更新メカニズムを用いずにシステム BIOS を更新する、セキュアなローカル更新メカニズムが含まれてもよい。このセキュアなローカル更新メカニズムが実装される場合には、メーカーのオリジナルの BIOS イメージを置き換えるため、または認証された更新メカニズムを用いては修正することのできないシステム BIOS の破損から回復するためにだけ、用いられるべきである (should)。セキュアなローカル更新メカニズムは、物理的な存在を要求することによって、BIOS 更新イメージの真正性と完全性を確証しなくてはならない (shall)。システム BIOS の更新を許可する前に、管理者パスワードの入力や、物理的なロック (例えば、マザーボードのジャンパ) のロック解除を要求することによって、セキュアなローカル更新メカニズムをさらに保護することもできる。

1.1.2 管理

11 ベンダには、サポートされるすべての運用環境について (例えば、製品によってサポートされるすべての O/S について)、BIOS を正しくインストール及び更新し、TSF を管理する (例えば、鍵保管へ新たな鍵をロードしたり、鍵サイズやアルゴリズムを構成したり、暗号アルゴリズムを更新する) ために、インストール及び構成ガイダンス (AGD_PRE, AGD_OPR) を提供することが要求される。

1.1.3 利用できる TOE 以外のハードウェア／ソフトウェア／ファームウェア

12 この PP に定義される TOE は PC クライアントデバイスである。PC クライアントデバイスへ接続されるデバイスであって、更新用の BIOS イメージを提供するために用いられるもの (ネットワークベースのシステム管理ツール、組織によって維持管理される更新サーバ、メーカーの更新サーバなど) はすべて、IT 運用環境の一部である。TOE は、システム BIOS と RTU を更新するためのインタフェースの提供を、運用環境に依存する。ベンダには、運用環境に必要な機能を特定するために十分なインストール及び構成の指示を提供すること、そしてそれを正しくセキュアな方法で構成する方法に関する指示を提供することが期待される。

13 場合によっては、TOE がそのセキュリティ対策方針を満たせるようにするため、具体的な運用環境の構成ガイダンスを TOE ベンダが提供しなくてはならない (have to) 場合もあるだろう。そのようなガイダンスは TOE の操作ガイダンスとみなされ、TOE のエンドユーザに利用可能な文書の一部として提供されるべきである (should)。

2 セキュリティ課題定義

14 保護される主要な資産は、PC クライアントデバイスのシステム BIOS である。BIOS は PC アーキテクチャにおいてユニークかつ特権的な地位にあるため、悪意のあるソフトウェアによる BIOS の不正な変更は、重大な脅威となる。悪意のある BIOS の変更は、恒久的なサービス拒否 (BIOS が破損している場合) または永続的なマルウェアの存在 (BIOS にマルウェアが組み込まれている場合) など、組織への洗練された標的型攻撃の一部として行われるかもしれない。

2.1 脅威

15 脅威は、脅威エージェントと資産、そしてその資産への脅威エージェントの敵対的なアクションによって構成される。

16 主要な脅威エージェントは、インストールされた BIOS ファームウェアをその脅威エージェントがリモートから変更または置き換えすることが可能な場合に資産をリスクにさらすことになるエンティティである。例えば、以下の表の T.UNAUTHORIZED_BIOS_UPDATE では、攻撃者 (脅威エージェント) が不正な BIOS 更新をリモートから挿入すること (敵対的な動作) によって、利用者の PC クライアントデバイス (資産) のセキュリティ機能を危殆化させようとする。脅威エージェントの目的には、データの危殆化や利用者へのなりすまし、あるいはサービス拒否が含まれるかもしれない。

17 この PP では、PC クライアントデバイスのセキュリティ機能を危殆化させるおそれのある、悪意のある BIOS 更新に関連したすべての脅威に対して防御することは TOE に期待されていない。例えば、デバイスがサプライチェーン中を移動している間にシステム BIOS の完全性を検出することは TOE の責任ではない。PC クライアントデバイスが、メーカーの意図したシステム BIOS をインストールして到着したことを前提条件としても、この PP に含まれるセキュリティ機能によってカバーされないシステム BIOS の完全性への脅威は、システムのライフタイム中に数多く存在する。

- ネットワークベースのシステム管理ツールが、システム BIOS への組織全体にわたる攻撃を行うために用いられるかもしれない。例えば、組織に配備されたシステム BIOS を更新するための、組織によって維持管理された更新サーバを想像してみてほしい。危殆化したサーバは、組織全体にわたるコンピュータシステムへ悪意のあるシステム BIOS をプッシュすることができてしまうかもしれない。BIOS 更新が更新サーバによって署名される場合、この攻撃は成功するだろう。
- BIOS イメージの悪意のあるインストールが、物理的なアクセスによって実現されるかもしれない。利用者がコンピュータシステムへ物理的にアクセスでき、例えばフラッシュメモリを置き換えることができる場合には、この PP に含まれるセキュリティ機能で未承認の BIOS イメージのインストールを防ぐことはできない。この PP の附属書 C には、更新プロセスが失敗し BIOS の更新が成功裏に完了しなかった際、承認された BIOS を復元するための回復プロセスを要求することによって、この脅威へ部分的に対処するオプションの SFR が定義されている。
- これまでに述べた更新メカニズムは、いずれもシステム BIOS を真正だが脆弱性を持つものにロールバックするために用いられるかもしれない。「不良」BIOS が真正な (すなわち、メーカーによって出荷された) ものであるため、この攻撃は特に潜行性 (気づかれにくい) となる。

表 1：脅威

脅威	脅威の説明
T.UNAUTHORIZED_BIOS_UPDATE	攻撃者が PC クライアント中の BIOS を、TOE のセキュリティ機能を危殆化させるおそれのある悪意のあるBIOS更新によって置き換えようとする。
T.UNAUTHORIZED_BIOS_MODIFY	攻撃者が PC クライアント中の BIOS に、TOE のセキュリティ機能を危殆化させるおそれのある変更を加えようとする。

2.2 前提条件

18 セキュリティ課題を定義するこのセクションでは、セキュリティ機能を提供可能とするために運用環境に対して課される前提条件を示す。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、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。前提条件は、運用環境の物理的、人的、及び接続性の側面に関するものであってよい。

表 2：TOE の前提条件

前提条件	前提条件の説明
A.MANUFACTURER_BIOS	PC クライアントシステムは、メーカーの意図したシステムBIOSがインストールされて配付される。
A.AUTHORIZED_ADMINISTRATORS	TOE の正当な管理者とローカルユーザは、管理者によって提供されるすべてのガイダンスを遵守し、適用すると信頼されている。

3 セキュリティ対策方針

19 セキュリティ対策方針は、TOE 及び運用環境に関する要件であって、セクション 2 の脅威及び前提条件から導出されたものである。セクション 4 では、TOE に関するセキュリティ対策方針を SFR として、より形式的に再び述べる。TOE は、SFR に対して評価される。

3.1 TOE のセキュリティ対策方針

20 表 3 は、TOE のセキュリティ対策方針を特定したものである。これらのセキュリティ対策方針は、特定された脅威へ対抗するために言明された意図を反映している。TOE は、SFR を満たすことによって、これらの対策方針を満たさなくてはならない (has to)。指定された対策方針は、主にシステム BIOS 更新のソース及び完全性を検証することに焦点を絞っている。

表 3：TOE のセキュリティ対策方針

対策方針	対策方針の説明
O.BIOS_AUTHENTICATED_UPDATE	TOE は、TOE へのあらゆる BIOS 更新が信頼できると確実に検証できるメカニズムを提供しなくてはならない (must)。
O.ROOT_OF_TRUST_FOR_UPDATE	TOE は、署名検証アルゴリズムと、BIOS 更新イメージの署名を検証するために必要な公開鍵が含まれた鍵保管を含む、RTU を持たなくてはならない (must)。
O.BIOS_INTEGRITY_PROTECTION	TOE は、システム BIOS や RTU の意図しない、または悪意のある変更を防止するためのメカニズムを実装しなくてはならない (must)。
O.BIOS_NON-BYPASSABILITY	TOE は、システム BIOS が認証された BIOS 更新メカニズムによってのみ変更されることを確実にしなくてはならない (must)。

3.2 運用環境のセキュリティ対策方針

21 TOE の運用環境は、TOE がそのセキュリティ機能 (これは、TOE のセキュリティ対策方針によって定義される) を正しく提供できるように支援する、技術的及び手続的手段を実装する。運用環境のセキュリティ対策方針は、運用環境が達成すべき (should) 目標を記述する一連の言明によって構成される。

22 このセクションでは、IT ドメインによって、もしくは非技術的または手続き的手段によって対処されるべきセキュリティ対策方針を定義する。セクション 2.2 中に特定された前提条件は、環境へのセキュリティ対策方針として組み込まれている。これによって環境に対する追加的な要件が課されるが、これらは主に手続き的または管理的手段によって満たされる。表 4 は、環境のセキュリティ対策方針を特定したものである。

表 4：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.MANUFACTURER_BIOS	メーカーは、意図したシステム BIOS がインストールされた PC クライアントシステムを配付しなくてはならない (must)。
OE.TRAINED_ADMINISTRATORS	TOE の正当な管理者とローカルユーザは、適切に教育されるとともに、すべてのセキュリティガイダンスを遵守しなくてはならない (must)。

3.3 セキュリティ対策方針の根拠

23 このセクションでは、前セクションで定義されるセキュリティ対策方針の根拠を記述する。表 5 に、セキュリティ対策方針からの脅威への対応付けを示す。

表 5：セキュリティ対策方針から脅威への対応付け

脅威／方針	脅威及び方針に対処する対策方針	根拠
T.UNAUTHORIZED_BIOS_UPDATE 攻撃者が PC クライアント中の BIOS を、TOE のセキュリティ機能を危殆化させるおそれのある悪意のある BIOS 更新によって置き換えようとする。	O.BIOS_AUTHENTICATED_UPDATE TOE は、TOE へのあらゆる BIOS 更新が信頼できると確実に検証できるメカニズムを提供しなくてはならない (must)。 O.ROOT_OF_TRUST_FOR_UPDATE TOE は、署名検証アルゴリズムと、BIOS 更新イメージの署名を検証するために必要な公開鍵が含まれた鍵保管を含む、RTU を持たなくてはならない (must)。 O.BIOS_NON-BYPASSABILITY TOE は、システム BIOS が認証された BIOS メカニズムによってのみ更新されることを確実にしなくてはならない (must)。	O.BIOS_AUTHENTICATED_UPDATE は、TOE が BIOS と RTU の更新の真正性と完全性を検証する BIOS 更新メカニズムを確実に提供することによって、この脅威を低減する。 O.ROOT_OF_TRUST_FOR_UPDATE は、署名検証アルゴリズムと、BIOS 更新イメージの署名を検証するために必要な公開鍵が含まれた鍵保管を含む、RTU を TOE が実装することを確実にする。 O.BIOS_NON-BYPASSABILITY は、システム BIOS が認証された BIOS メカニズムによってのみ更新されること、またそれによって悪意のある BIOS 更新が認証されずに拒否されることを確実にすることによってこの脅威に対抗する。
T.UNAUTHORIZED_BIOS_MODIFY 攻撃者が PC クライアント中の BIOS に、TOE のセキュリティ機能を危殆化させるおそれのある変更を加えようとする。	O.BIOS_INTEGRITY_PROTECTION TOE は、システム BIOS や RTU の意図しない、または悪意のある変更を防止するためのメカニズムを実装しなくてはならない (must)。 O.BIOS_NON-BYPASSABILITY TOE は、システム BIOS が認証された BIOS メカニズムによってのみ更新されることを確実にしなくてはならない (must)。	O.BIOS_INTEGRITY_PROTECTION は、TOE がシステム BIOS 及び RTU の変更を確実にコントロールし、意図しない、または悪意のあるシステム BIOS 及び RTU の変更を防止することによって、この脅威に対抗する。 O.BIOS_NON-BYPASSABILITY は、システム BIOS が認証された BIOS メカニズムによってのみ更新され、その他の手段での BIOS 更新が失敗することを確実にする。

24　　表 6 に、セキュリティ対策方針から前提条件への対応付けを示す。

表 6：セキュリティ対策方針から前提条件への対応付け

前提条件	前提条件に対処する対策方針	根拠
A.MANUFACTURER_BIOS PC クライアントシステムは、メーカーの意図したシステム BIOS がインストールされて配付される。	OE.MANUFACTURER_BIOS メーカーは、意図したシステム BIOS がインストールされた PC クライアントシステムを配付すること。	OE.MANUFACTURER_BIOS によって、意図したシステム BIOS がインストールされた PC クライアントシステムをメーカーが配付することが確実となる。
A.AUTHORIZED_ADMINISTRATORS TOE の正当な管理者とローカルユーザは、管理者によって提供されるすべてのガイダンスを遵守し、適用すると信頼されている。	OE.TRAINED_ADMINISTRATORS TOE の正当な管理者とローカルユーザは、適切に教育されるとともに、すべてのセキュリティガイダンスを遵守すること。	OE.TRAINED_ADMINISTRATORS によって、TOE をセキュアな方法で管理し利用してシステム BIOS を更新する方法について、TOE の管理者とローカルユーザが適切に教育されることが確実となる。

4 セキュリティ要件と根拠

25 セキュリティ要件は、機能要件と保証要件に大別される。SFR は、セキュリティ対策方針の形式的な具体化であり、適用上の注意と共にセクション 4.1 で提供される。セクション 4.2 は、SFR からセキュリティ対策方針への必要とされる追跡である。

26 SAR は、典型的には SFR とは分離して PP へ挿入され列挙される。そして、選択された SAR に基づいた評価中にはコモンクライテリア評価方法 (CEM) が参照される。コモンクライテリアの SAR と、TOE として特定される特有の技術の性質のため、よりカスタム化されたアプローチがこの PP では取られている。この PP でも SAR は文脈と完全性に応じてセクション 4.3 に列挙されているが、評価者が SFR と SAR のそれぞれについてこの TOE に行う必要のあるアクティビティの大半は、「保証アクティビティ」のパラグラフに詳述されている。保証アクティビティは、評価を完了するために行われなくてはならない (must) アクティビティの規範的な記述である。保証アクティビティはこの PP の 2 か所に配置されている。具体的な SFR と関連付けられたものはセクション 4.1 に配置され、SFR と独立したものはセクション 4.3 に詳述されている。保証アクティビティは、実際にはカスタム化された評価の方法論であり、読みやすさと理解しやすさ、そして便宜のため SFR と共に提示されていることに注意されたい。

27 SFR と直接関連付けられるアクティビティについては、各 SFR の後に 1 つ以上の保証アクティビティが列挙され、適合デバイスに必要とされる保証を実現するために行われる必要のあるアクティビティが詳述される。

28 SFR とは独立したアクティビティを必要とする SAR については、実現される必要のある追加的保証アクティビティが、その SAR と関連付けられた特定の保証アクティビティが書かれる対象となった SFR への参照とともに、セクション 4.3 に示されている。

29 このプロテクションプロファイルの将来の世代では、実際の製品評価から得られた教訓に基づいた、より詳細な保証アクティビティを提供することになるかもしれない。

4.1 セキュリティ機能要件

30 SFR は、TOE のセキュリティ対策方針の変換である。これらは通常、抽象概念よりも詳細なレベルで行われるが、完全な変換でなくてはならない (have to) (セキュリティ対策方針は完全に対処されなくてはならない (must))。CC ではいくつかの理由から、この標準化された言語への変換が要求されている。

- 何が評価されるべきかについて、正確な記述を提供するため。TOE のセキュリティ対策方針は通常自然言語で形式化されるが、標準化された言語への変換によってより正確な TOE の機能の記述が強制される。
- 2 件のセキュリティターゲット (ST) 間で比較を可能とするため。異なる ST 作成者は自分のセキュリティ対策方針の記述に異なる専門用語を使っているかもしれないが、標準化された言語によって同一の専門用語と概念の使用が強制される。これによって容易な比較が可能となる。

4.1.1 クラス：暗号サポート (FCS)

31 これらの機能要件によって対処される主な脅威は、鍵空間に対するブルートフォース攻撃と暗号コンポーネントの故障である。

32 暗号要件はアルゴリズムを記述する標準への参照を行うが、これらの標準の大部分は米国 NIST から Special Publications (800-xxx) または連邦情報処理規格 (FIPS) として入手できる。保証要件は、これらの要件の実装が検証されるべき方法を詳述する。各スキームはオプションとして、暗号保証アクティビティが満たされたとみなされるプロセスを規定することができる。以下に規定するすべての暗号機能は、TOE 内に実装されなくてはならない (must)。

暗号操作 (FCS_COP)

FCS_COP.1(1) **暗号操作 (署名検証)**

FCS_COP.1.1(1) **詳細化**：TSF は、**BIOS 更新イメージの暗号署名検証**を **[選択**：

1) 2048 ビット以上の鍵サイズ (法) を用いたデジタル署名アルゴリズム (DSA)、

2) 2048 ビット以上の鍵サイズ (法) を用いた RSA デジタル署名アルゴリズム (rDSA)、または

3) 256 ビット以上の鍵サイズを用いた楕円曲線デジタル署名 (ECDSA)]

であって、以下を満たすものにしたがって行わなくてはならない (shall)。

デジタル署名アルゴリズムの場合：

- **[FIPS PUB 186-3, "Digital Signature Standard"]**

RSA デジタル署名アルゴリズムの場合：

- **[FIPS PUB 186-3, "Digital Signature Standard"]**

楕円曲線デジタル署名アルゴリズムの場合：

- **[FIPS PUB 186-3, "Digital Signature Standard"]**
- **TSF は、「NIST 曲線」 [選択：P-256、P-384、及び P-521、その他の曲線なし] (FIPS PUB 186-3, “Digital Signature Standard” の定義による) を実装しなくてはならない (shall)。**

適用上の注意：

33 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、この要件はその機能を規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ているパラメタを規定すべきである (should)。特に、ECDSA が署名アルゴリズムのひとつとして選択されている場合には、指定された鍵サイズはアルゴリズム中で用いられる曲線の選択と一致していなくてはならない (must)。

34 楕円曲線ベースの方式に関しては、鍵サイズは基点の次数の 2 の対数を示す。すべての必要な標準とその他の支援情報が完全に確立された後で、デジタル署名の望ましいアプローチとして楕円曲線が必要とされることになる。

保証アクティビティ：

35 この要件は TOE メーカー／開発者からの BIOS 更新に添付されたデジタル署名を、その BIOS 更新を TOE へインストールする前に検証するために用いられる。

36 任意のアルゴリズムについて、評価者は TSS をチェックして署名の検証の全体的な流れが記述されていることを確証する。これには少なくとも、デジタル署名の検証に用いられるデータのフォーマットと一般的な場所の特定、運用環境から受信されたデータが BIOS 上に持ち込まれる方法、そして行われる任意の処理であってデジタル署名アルゴリズムの一部ではないもの (例えば、BIOS 更新と共に提供される公共鍵のハッシュ値を計算し、それが鍵保管中に現れるハッシュ値と一致することを確証する、など) が含まれるべきである (should)。

37

38 鍵生成／ドメインパラメタ生成に関するテスト要件が存在しないことに注意すべきである (should)。これは、配付された BIOS 更新のデジタル署名のチェックに機能が制限されているため、この機能がエンドデバイスに必要とされるとは予期されていないためである。

39 TOE が正しく署名された BIOS イメージを受け付け、誤って署名された BIOS イメージを拒否することを確認するために用いられるテストは FPT_BUA_EXT.1 に記述されており、この要件の最小限の／基本的なテストとしてとらえることができる。

rDSA

署名生成／検証機能の実装には、ANSI X9.31 と PKCS #1 (バージョン 1.5 またはバージョン PSS、あるいはその両方) という、2 つの選択肢が存在する。これらの選択肢のうち、少なくとも 1 つが実装されなくてはならない (must)。実装されたバージョンのそれぞれが、以下に示すようにテストされなくてはならない (must)。PKCS #1 バージョン PSS が選択されている場合には、評価者は TSS をチェックしてソルト長が規定されていることを確証しなくてはならない (shall)。

TOE が 2 つ以上の法のサイズをサポートしている場合には、評価者はすべての法のサイズについて以下のテストを行わなくてはならない (shall)。TOE が 2 つ以上のハッシュアルゴリズムをサポートしている場合、評価者はすべてのハッシュアルゴリズムについて以下のテストを行わなくてはならない (shall)。つまり、実装で 2 つの法サイズと 2 つのハッシュアルゴリズムの選択が許されている場合、評価者は以下のテストを 4 回行うことになる。

評価者は、3 グループのデータを生成しなくてはならない (shall)。各グループのデータは、法と、その法と両立する 4 セットのテストベクトルから構成される。テストベクトルは、公開鍵指数 *e*、疑似ランダム的に生成されたメッセージ、及び関連付けられた秘密鍵を用いたメッセージの署名 (*e* 及び法 *n* と両立するもの) から構成される。つまり、TSF によって

サポートされている法のサイズ／ハッシュアルゴリズムのそれぞれについて、最低でも 12 個のテストベクトルが存在することになる。

テストベクトルの 3/4 において正しい署名が生成された (しかしまだ TSF に「供給」されてはいない) 後、評価者は公開鍵、メッセージ、または署名 (少なくともそれぞれ 2 つについて確実に行うこと) を改変し、署名検証失敗機能がテストされるようにする。次に評価者は、TSF を通してテストベクトルを実行し、結果が正しいことを検証しなくてはならない (shall)。

40 さらに、実装されているアルゴリズムが *Public Key Cryptography Standards (PKCS) #1 v2.1: RSA Cryptography Standard-2002* に規定される RSASSA-PKCS1-v1_5、または X9.31, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)* に記述される RSA アルゴリズムである場合、http://csrc.nist.gov/groups/STM/cavp/documents/dss/SigVer15EMTest.zip (PKCS #1 Version 1.5 の実装について) または http://csrc.nist.gov/groups/STM/cavp/documents/dss/SigVer931IRTest.zip (X9.31 の実装について) から得られる適切な追加テストベクトルを用いて、評価者は実装がこれらのテストをパスすることを検証しなくてはならない (shall)。

DSA

評価者は TSS を調査して、(L, N) に用いられる値が与えられ、用いられるハッシュアルゴリズムが規定されていることを確証する。評価者は、特定の (L,N) に用いられるハッシュアルゴリズムが、SP 800-57, *Recommendation for Key Management --Part I: General (Revised)* のセクション 5.6.1 の表 2 及び表 3 に規定される、必要な強度を提供することを検証する。また評価者は、選択された (L,N) が USB フラッシュドライブ上で用いられる対称 (データ) 暗号化アルゴリズムと同等の強度を持つことを確証しなくてはならない (shall) (例えば、利用者データの暗号化に 128 ビット AES が用いられる場合には、少なくとも (3072, 256) の (L,N) が必要とされる)。

評価者は、サポートされている (L,N) とハッシュの組み合わせのそれぞれについて、以下のテストを行う。評価者は、鍵ペアを生成しなくてはならない (shall)。次に評価者は、疑似ランダム的に 1024 ビットのメッセージ 15 個を生成し、秘密鍵でそれらに署名する。メッセージの約半分において正しい署名が生成された (しかしまだ TSF に「供給」されてはいない) 後、評価者は公開鍵、メッセージ、または署名 (少なくともそれぞれ 2 つについて確実に行うこと) を改変し、署名検証失敗機能がテストされるようにする。次に評価者は、TSF を通してテストベクトルを実行し、結果が正しいことを検証しなくてはならない (shall)。

41

ECDSA

評価者は TSS を調査して、実装に用いられている 1 つまたは複数の曲線が規定されていて要件と一貫していること、及びサポートされている 1 つまたは複数のハッシュが規定されていることを判断しなくてはならない (shall)。評価者は、TSF によって実装されている曲線とハッシュのペアのそれぞれについて、以下のテストを実施しなくてはならない (shall)。

42 評価者は、15 セットのデータを生成する。各データセットは、疑似ランダムなメッセージ、公開鍵／秘密鍵のペア (d,Q)、及び署名 (r,s) から構成される。メッセージの約半分において正しい署名が生成された (しかしまだ TSF に「供給」されてはいない) 後、評価者は公開鍵、メッセージ、または署名 (少なくともそれぞれ 2 つについて確実に行うこと) を変更し、署名検証失敗機能がテストされるようにする。次に評価者は、TSF を通してデータを実行し、結果が正しいことを検証しなくてはならない (shall)。

FCS_COP.1(2)	**暗号操作 (暗号ハッシュ)**
FCS_COP.1.1(2)	**詳細化** : TSF は、**[選択** : **SHA-1、SHA 224、SHA 256、SHA 384、SHA 512]** にしたがい、**メッセージダイジェストのサイズが [選択** : **160、224、256、384、及び 512] ビット**の、以下 : **FIPS Pub 180-3, “Secure Hash Standard”** を満たす**暗号ハッシュサービス**を行わなくてはならない (shall)。

適用上の注意：

43 この要件の意図は、FCS_COP.1(1) に規定されるデジタル署名アルゴリズムに用いられるハッシュ関数を規定することである。ハッシュの選択は、メッセージダイジェストサイズの選択をサポートしなくてはならない (must)。ハッシュの選択は、FCS_COP.1(1) に用いられるアルゴリズムの全体的な強度と一貫しているべきである (should)。

44 また TOE が RTU 中にハッシュ値を保存する場合には、ST 作成者はこの要件を繰返して、BIOS 更新の一部として提供される鍵の完全性を確認するために用いられるハッシュ関数を規定してもよい。TOE は、提供された公開鍵のハッシュ値を計算し、その値を RTU 中に保存されたハッシュ値と比較することになる。

保証アクティビティ：

45 評価者はガイダンス文書をチェックして、必要とされるハッシュのサイズに機能を構成するために必要とされる任意の情報が存在することを判断する。評価者は、ハッシュ機能と他の TSF 暗号機能 (例えば、デジタル署名検証機能) との関連が TSS に文書化されていることをチェックしなくてはならない (shall)。

46 暗号ハッシュのテストは、http://csrc.nist.gov/groups/STM/cavp/documents/shs/SHAVS.pdf から入手できる *The Secure Hash Algorithm Validation System (SHAVS)* [13] を参照する。

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、この PP の要件を満たすために用いられているハッシュアルゴリズムのそれぞれについて、以下のテストのすべてを行わなくてはならない (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くてはならない (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生じることを確証する。

- *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くてはならない (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生じることを確証する。

- *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 $1 \le i \le m$。メッセージの本文は、疑似ランダム的に生成されなくてはならない (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生じることを確証する。

- *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 $1 \le i \le m$。メッセージの本文は、疑似ランダム的に生成されなくてはならない (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生じることを確証する。

- *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機能によって作り出されるメッセージダイジェストの長さである。次に評価者は、[SHAVS] の図 1 に示されるアルゴリズムにしたがって 100 個のメッセージと関連するダイジェストのセットを作成する。次に評価者は、メッセージが TSF へ提供された際に正しい結果が生じることを確証する。

47 上述のアルゴリズムテストに加えて、TOE が正しく署名された BIOS イメージを受け付け、誤って署名された BIOS イメージを拒否することを確認するために用いられるテストは FPT_BUA_EXT.1 に記述されており、この要件の最小限の／基本的なテストとしてとらえることができる。

4.1.2 クラス：TSF の保護 (FPT)

48 以下の機能要件は TSF を構成するメカニズムの完全性と管理、そして TSF データの完全性に関連したものである。これによって TSF データが改ざん不可能であり、また TSF メカニズムがバイパス不可能であるという要件が提供される。

拡張：BIOS 更新メカニズム (FPT_BUM_EXT)

FPT_BUM_EXT.1	**拡張：BIOS 更新メカニズム**
FPT_BUM_EXT.1.1	TSF は FPT_BUA_EXT.1 に記述される認証された BIOS 更新メカニズムと、 [選択、1 つを選択：FPT_SLU_EXT.1 に記述されるセキュアなローカル更新メカニズム、その他のメカニズムなし] を提供して BIOS システムの更新を行わなくてはならない (shall)。

適用上の注意：

49 セキュアな BIOS 更新メカニズムは、BIOS 更新の真正性と完全性を検証するために、そしてセキュアな更新プロセスの外側での変更から保護されていることを確実にするために用いられる。認証された BIOS 更新メカニズムは、少なくとも RTU 及びシステム BIOS を保護するもの以上の強度を持つメカニズムによって、意図しない、または悪意のある改変から保護されなくてはならない (shall)。

50 この要件の意図は、認証された BIOS 更新メカニズムと (オプションの) セキュアなローカル更新メカニズムが提供されることを確実にすることである。認証によって、BIOS が真正のソースによって生成され、改変されていないことが検証される。システム BIOS へのすべての更新は、FPT_BUA_EXT.1 に記述される認証された BIOS 更新メカニズムを通過しなくてはならない (shall)。さらに、TOE がセキュアなローカル更新メカニズムを提供する場合には、適切な選択がなされるとともに ST 作成者は附属書 C に規定される FPT_SLU_EXT.1 を選択しなくてはならない (must)。

保証アクティビティ：

51 評価者は、この要件に関する保証アクティビティを行う際に、ST の TSS を参照しなくてはならない (shall)。評価者は、BIOS 更新イメージがシステムへ更新される方法と、認証された BIOS 更新メカニズムが適用されるポイントに関して包括的に記述されていることを確証することに焦点を絞る。

52 レビューを行うにあたって、評価者は BIOS 更新プロセスの際に発生するアクティビティの記述が TSS に含まれていることを判断しなくてはならない (shall)。RTU が BIOS 中に統合されていない場合、その更新プロセスもまた、その完全性を保証するセキュリティメカニズムの規定とともに、TSS 中に説明されていなくてはならない (shall)。また評価者は、認証された BIOS 更新メカニズムの詳細な記述がその他の証拠資料 (AGD、ADV 及び ATE) に含まれていることをチェックしなくてはならない (shall)。オプションのセキュアなローカル更新メカニズムを TOE がサポートしている場合には、評価者はこのメカニズムの動作方法とこのメカニズムを用いることのできる場合が TSS とその他の証拠資料に記述されていることをチェックしなくてはならない (shall)。

拡張：BIOS 更新認証 (FPT_BUA_EXT)

FPT_BUA_EXT.1	**拡張：BIOS 更新認証**
FPT_BUA_EXT.1.1	TSF は、FCS_COP.1(1) に規定されるデジタル署名アルゴリズムを用い、 [選択：公開鍵、公開鍵のハッシュ値] を含む鍵保管を用いて、BIOS 更新のソースを認証しなくてはならない (shall)。
FPT_BUA_EXT.1.2	TSF は、FCS_COP.1(1) に規定されるようにデジタル署名の検証が成功した場合に限り、更新のインストールを許可しなくてはならない (shall)。

適用上の注意：

53 この認証された BIOS 更新メカニズムには、BIOS 更新イメージの真正性を確保するためにデジタル署名が用いられる。TOE は、署名検証アルゴリズムと、BIOS 更新イメージの署名を検証するために必要な公開鍵が含まれた鍵保管を含む、RTU を提供する。RTU 内の鍵保管には、BIOS 更新イメージ上の署名を検証するために用いられる*公開鍵*か、BIOS 更新イメージと共に公開鍵が提供される場合には*公開鍵のハッシュ*が含まれなくてはならない (shall)。後者の場合、提供された公開鍵を用いて BIOS 更新イメージの署名を検証する前に、更新メカニズムは BIOS 更新イメージと共に提供された公開鍵をハッシュし、鍵保管中に現れるハッシュと一致することを確証しなくてはならない (shall)。公開鍵のハッシュが選択された場合、ST 作成者は FCS_COP.1(2) 要件を繰返して用いられるハッシュ関数を指定してもよい。

54 この要件の意図は、認証された BIOS 更新メカニズムは BIOS 更新イメージがデジタル的に署名されていること、そしてそのデジタル署名が BIOS 更新前に公開鍵を用いて検証できることを確実にしなくてはならない (shall)、と規定することにあった。またこの要件は、認証された BIOS 更新メカニズムが、TSF による検証の成功したデジタル署名を持つ BIOS 更新のみのインストールを可能とすることも規定している。

保証アクティビティ：

55 評価者は、この要件に関する保証アクティビティを行う際に、ST の TSS を参照しなくてはならない (shall)。評価者は、TSF が RTU を実装する (すなわち、RTU キーストレージに公開鍵または公開鍵のハッシュが含まれる) 方法が、包括的に記述されていることを確証することに焦点を絞る。

56 TSS には、初期化プロセスと、BIOS/RTU 更新イメージのデジタル署名が BIOS/RTU の更新前に検証されることを確実にするために行われるアクティビティがカバーされているべきである (should)。レビューを行うにあたって、評価者はデジタル署名検証プロセスの記述が TSS に含まれていることを判断しなくてはならない (shall)。また評価者は、BIOS/RTU イメージのデジタル署名を TSF が検証できない (すなわち、BIOS/RTU イメージが署名されていないか、RTU 中に保存された鍵を用いて署名が検証できない、などの) 場合に何が起こるか、その他の証拠資料 (AGD、ADV 及び ATE) に記述されていることを調査しなくてはならない (shall)。

57 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、TOE (システム) に存在する BIOS の現在のバージョンを判断する。以下のテストに記述されている更新テストの後、評価者はこのアクティビティを再び行って、バージョンが更新された BIOS のバージョン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、操作ガイダンスに記述された手順を用いて BIOS の本物の更新イメージを取得または作成し、BIOS 更新の TOE へのロードが成功することを検証する。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、更新が期待されたとおり機能していることを例証する。
- テスト 3 : 評価者は、以下の場合のそれぞれについて偽物の BIOS 更新イメージを取得または作成し、TOE (システム) へのインストールを試みる。

    a) 未署名のイメージ、

    b) 誤った鍵で署名されたもの、

    c) 正しい鍵で署名されているが、破損した BIOS イメージ。

評価者は、試みたすべての BIOS 更新を TOE が拒否することを検証する。

58 TSF がシステム BIOS とは分離して更新可能な場合には、ST 作成者は附属書 C から要件 FPT_TUD_EXT.1 を取り込むべきである (should)。

拡張 : BIOS の保護 (FPT_PBR_EXT)

FPT_PBR_EXT.1	**拡張 : BIOS の保護**
FPT_PBR_EXT.1.1	TSF は、FPT_BUM_EXT.1 に記述された更新メカニズムによってのみ、BIOS の変更を可能としなくてはならない (shall)。

適用上の注意 :

59 BIOS (不揮発性メモリに保存される BIOS によって用いられる構成データを除く) と TSF のソフトウェア部分 (例えば、RTU (鍵保管と署名検証アルゴリズム)) は、TOE の書込み保護された領域に保存されなくてはならない (shall)。BIOS は、FPT_BUA _EXT.1 に記述された認証された更新メカニズムまたは FPT_SLU_EXT.1. に記述されたセキュアなローカル更新メカニズムを用いてのみ変更可能でなくてはならない (shall)。ST 作成者は FPT_BUM_EXT.1 中の適切な選択を行って、用いられる正確なメカニズムを規定することになるだろう。TSF は、FPT_TUD_EXT.1 (附属書 C) に規定されるメカニズムを用いてのみ、変更が可能である。

保証アクティビティ：

60 評価者は TSS セクションをチェックして、鍵保管と署名検証アルゴリズムが書込み保護された領域に保存されることが規定されていることを判断しなくてはならない (shall)。TSF が更新可能な場合、ST 作成者は FPT_TUD_EXT.1 要件を取り込むことになり、関連する TSF 更新の保証アクティビティはそこに含まれることになる。これによって、鍵保管の変更とともに、暗号アルゴリズムへの更新が取り込まれる。

61 評価者は操作ガイダンスをチェックして、RTU 中の鍵保管と署名検証アルゴリズムをセキュアに変更する方法の指示が存在することを判断しなくてはならない (shall)。評価者は、鍵保管と署名検証アルゴリズムを更新する (置き換える) プロセスの説明と、更新が不成功だった場合に何が起こるかの説明が、その他の証拠資料 (ADV 及び ATE) に含まれていることをチェックしなくてはならない (shall)。

62 評価者は、下記のテストを行わなくてはならない (shall)。

- テスト 1 : TSS やその他の証拠資料 (AGD、インタフェース仕様) に含まれている情報を用いて、評価者は認証更新をバイパスしながらシステム中の BIOS を上書きまたは変更しようと試みなくてはならない(shall) (例えば、変更された GRUB などの Linux ブートローダを用いて BIOS が保存されているフラッシュメモリへの書き込みを試みる)。
- テスト 2 : TSS やその他の証拠資料 (AGD、インタフェース仕様) に含まれている情報を用いて、評価者はシステム中の TSF コンポーネント (鍵保管、署名検証アルゴリズム) を上書きまたは変更しようと試みなくてはならない(shall)。

4.2 セキュリティ機能要件の根拠

63 このセクションでは、セクション 4.1 に定義される TOE SFR の根拠を記述する。表 7 に、SFR からセキュリティ対策方針への対応付けを、その対策方針が要件によって対処される根拠と共に示す。ST 作成者／ベンダは、セクション 4.1 の要件の選択や割付を完了した際には、この表へ追加を行うとともに、(おそらく) ベースライン要件に附属書 C の要件を追加すべきである (should)。

表 7：TOE セキュリティ機能要件の根拠

対策方針	対策方針へ対処する要件	根拠
O.BIOS_AUTHENTICATED_UPDATE TOE は、TOE へのあらゆる BIOS 更新が信頼できると確実に検証できるメカニズムを提供しなくてはならない (must)。	FPT_BUM_EXT.1	FPT_BUM_EXT.1 は、認証された BIOS 更新メカニズムと（オプションの）セキュアなローカル更新メカニズムが提供されることを要求する。認証によって、BIOS 更新イメージが真正のソースによって生成され、改変されていないことが検証される。

対策方針	対策方針へ対処する要件	根拠
O.ROOT_OF_TRUST_FOR_UPDATE TOE は、署名検証アルゴリズムと、BIOS 更新イメージの署名を検証するために必要な公開鍵が含まれた鍵保管を含む、RTU を持たなくてはならない (must)。	FPT_BUA_EXT.1 FCS_COP.1(1) FCS_COP.1(2)	FPT_BUA_EXT.1 は、署名検証アルゴリズムと、BIOS 更新イメージの署名を検証するために必要な公開鍵が含まれた鍵保管を含む RTU を TSF が提供することを規定している。この要件は、BIOS 更新イメージがデジタル的に署名されていること、そして BIOS 更新前にそのデジタル署名が公開鍵を用いて検証できることが認証された BIOS 更新メカニズムによって確証されることを規定している。またこの要件は、認証された BIOS 更新メカニズムによって、TSF による検証の成功したデジタル署名を持つ BIOS 更新のみのインストールが許されることも規定している。 FCS_COP.1(1) は、TOE の用いるデジタル署名検証アルゴリズムを規定している。FCS_COP.1(2) は、FCS_COP.1(1) に規定されるデジタル署名アルゴリズムに用いられるハッシュ関数を規定している。

対策方針	対策方針へ対処する要件	根拠
O.BIOS_INTEGRITY_PROTECTION TOE は、システム BIOS や RTU の意図しない、または悪意のある変更を防止するためのメカニズムを実装しなくてはならない (must)。	FPT_PBR_EXT.1	FPT_PBR_EXT.1 は、認証された更新メカニズムまたはセキュアなローカル更新メカニズム、あるいはその両方によってのみ BIOS と RTU が更新できることを要求している。 またこの要件では、TSF が BIOS と RTU を不正な変更から保護しなくてはならない (shall) とも規定している。
O.BIOS_NON-BYPASSABILITY TOE は、システム BIOS が認証された BIOS メカニズムによってのみ更新されることを確実にしなくてはならない (must)。	FPT_PBR_EXT.1	FPT_PBR_EXT.1 は、認証された更新メカニズムまたはセキュアなローカル更新メカニズムを用いてのみ BIOS が更新できることを要求している。

4.3 セキュリティ保証要件

64 セクション 3.1 中の TOE に関するセキュリティ対策方針は、セクション 2.1 に特定された脅威へ対処するために構築された。セクション 4.1 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。

65 セクション 4.1 に示されているように、このセクションには 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このセクションと共にセクション 4.1 の両方に詳述されている。

66 それぞれのファミリについて、「開発者への注意」が開発者アクションエレメントについて提供され、(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／アクティビティを説明している。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 4.1 にすでに含まれているものに加えて) が記述されている。さらに、この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 4.1 に規定されたものとは相補的な関係にある。

67 TOE のセキュリティ保証要件は表 8 に要約されており、この PP のセクション 2.1 に特定された脅威へ対処するために必要とされる管理及び評価アクティビティが特定されている。セクション 4.4 には、このセクションのセキュリティ保証要件を選択したことについての簡潔な正当化が提供される。

表 8：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
脆弱性の評定	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 CM カバレージ

4.3.1 ADV クラス：開発

68 この PP に適合する TOE については、TOE に関する情報は ST の TOE 要約仕様 (TSS) 部分とともに、エンドユーザに利用可能なガイダンス文書にも含まれている。セクション 4.1 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上で ST 作成者に十分な情報を提供すべきである (should)。

4.3.1.1 ADV_FSP.1 基本機能仕様

69 機能仕様は、TSF インタフェース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規定は必要とされない。さらに、この 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それ自体を規定することにはあまり意味がない。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ためである。この PP の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)。規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」文書が必要とされるべきではない (should not)。

70 TOE へのインタフェースを理解するにあたっては、対抗すべき主要な脅威が利用者主導による悪意のあるシステム BIOS のインストールであることを考慮することが重要である。TOE 更新インタフェースが、最も重要である。前述したように、置き換えられる任意のコードが適切に署名され、その署名が検証されることが不可欠である。

71 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。

開発者のアクションエレメント：

ADV_FSP.1.1D 開発者は、機能仕様を提供しなくてはならない (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くてはならない (shall)。

開発者への注意： この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。機能仕様中の保証アクティビティは、文書及び TSS セクションに存在すべき (should) 証拠資料を参照している。これらは SFR と直接関連付けられているため、エレメント ADV_FSP.1.2D 中の追跡は暗黙にはすでになされており、追加的な文書は必要とされない。

内容及び提示エレメント：

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

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

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

ADV_FSP.1.4C　追跡は、機能仕様における SFR から TSFI への追跡を例証するものでなくてはならない (shall)。

評価者のアクションエレメント：

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

ADV_FSP.1.2E　評価者は、機能仕様が SFR の正確かつ完全な実体化であることを判断しなくてはならない (shall)。

保証アクティビティ：

72　これらの SAR と関連付けられた保証アクティビティは、CC の内容要件を満たしていることをチェックする専用のものとなる。機能仕様文書はセクション 4.1 に記述された評価アクティビティと、AGD、ATE、及び AVA SAR に関して記述されたその他のアクティビティをサポートするために提供されている。機能仕様情報の内容についての要件は、行われるその他の保証アクティビティの特質により暗黙に評定される。不十分なインタフェース情報しか存在しなかったために評価者がアクティビティを行うことができなかった場合には、十分な機能仕様が提供されていなかったことになる。

4.3.2 AGD クラス：ガイダンス文書

73　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。概論で述べたように、実際の「管理者」の職務はかなり制約されているため、ガイダンス文書には TOE のすべての利用者に必要とされると共に用いられる情報が含まれることになる。このため、以下の本文では大部分の場合、「正当な利用者」を用いる。「管理者」が用いられる場合 (CC からの逐語的な要件を除いて)、BIOS のインストール／更新や、その他の人間の介入を必要とする任意の TOE セキュリティ機能を可能とするために運用環境をセットアップする責任を持つ利用者のサブセットを指す。

74 ガイダンスには、運用環境がセキュリティ機能にそれ自身の役割を果たすことができることを正当な利用者が検証する方法の記述が含まれなくてはならない (must)。この文書は、正当な利用者によって読解可能な非形式的なスタイルであるべきである (should)。

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

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

76 また、特定のセキュリティ機能に関するガイダンスも提供される。そのようなガイダンスに関する要件は、セクション 4.1 に規定された保証アクティビティに含まれている。

4.3.2.1 AGD_OPE.1 利用者操作ガイダンス

開発者のアクションエレメント：

AGD_OPE.1.1D 開発者は、利用者操作ガイダンスを提供しなくてはならない (shall)。

開発者への注意： 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、受容可能なガイドラインの作成に必要な情報が提供されることになる。

内容及び提示エレメント：

AGD_OPE.1.1C 利用者操作ガイダンスには、利用者の役割のそれぞれについて、利用者にアクセス可能な機能及び特権であってセキュアな処理環境において制御されるべき (should) ものが、適切な警告を含めて記述されなくてはならない (shall)。

AGD_OPE.1.2C 利用者操作ガイダンスには、利用者の役割のそれぞれについて、TOE によって提供される利用可能なインタフェースをセキュアな方法で利用する方法が記述されなくてはならない (shall)。

AGD_OPE.1.3C 利用者操作ガイダンスには、利用者の役割のそれぞれについて、利用可能な機能及びインタフェース、特に利用者の制御下にあるすべてのセキュリティパラメタが、該当する場合にはセキュアな値を示しつつ、記述されなくてはならない (shall)。

AGD_OPE.1.4C 利用者操作ガイダンスには、利用者の役割のそれぞれについて、利用者にアクセス可能な機能であって、TSF の制御下にあるエンティティのセキュリティ的な特徴の変更を含めて、実行される必要のあるものに関連するセキュリティ関連イベントのすべての種類が明示されなくてはならない (shall)。

AGD_OPE.1.5C 利用者操作ガイダンスには、TOE のすべてのあり得る運用モード (故障または操作エラー後の運用を含めて) と、その結果及びセキュアな運用を維持することへの影響が特定されなくてはならない (shall)。

AGD_OPE.1.6C　利用者操作ガイダンスには、利用者の役割のそれぞれについて、ST に記述される運用環境に関するセキュリティ対策方針を達成するために遵守されるべきセキュリティ対策が記述されなくてはならない (shall)。

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

評価者のアクションエレメント：

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

保証アクティビティ：

77　文書には、TOE への更新が意図されたソース (ほとんどの場合は TOE のベンダ) からのものであることを検証するためのプロセスが記述されなくてはならない (must)。検証プロセスは、正当な利用者によって開始されるかもしれないが、クライアントマシン上の TOE によって行われる。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くてはならない (shall)。

1. 更新そのものを取得するための指示。これには、更新を TOE からアクセス可能とするための指示が含まれるべきである (should)。
2. 更新プロセスが成功したか不成功だったかを判別するための指示。

78　この TOE には明示的に利用者／管理者と関連した SFR が存在しないため、AGD_OPE の要件の一部は適用されない場合がある (例えば、利用可能な機能及びインタフェースの記述)。しかし、AGD_OPE 要件の一部は、附属書 C の中に定義される FPT_SLU_EXT.1 が取り込まれる場合には適用可能となる場合がある。したがって AGD_OPE 証拠資料は、該当する場合には、この SAR に関する詳細を提供しなくてはならない (must)。

4.3.2.2　AGD_PRE.1 準備手続き

開発者のアクションエレメント：

AGD_PRE.1.1D　開発者は TOE を、その準備手続きを含めて提供しなくてはならない (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調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)。

内容及び提示エレメント：

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

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

評価者のアクションエレメント：

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

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

保証アクティビティ：

79　上の概論で述べたように、特に TOE の機能要件をサポートする運用環境の構成にあたっては、文書に関して多大な期待が存在する。評価者は、TOE に提供されたガイダンスが、ST 中に TOE について主張されているすべてのプラットフォームへ十分に対応していることをチェックして確証しなくてはならない (shall)。

4.3.3 ATE クラス：テスト

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

4.3.3.1 ATE_IND.1 独立テスト—適合

81　テストは、TSS と、提供された管理 (構成及び操作を含む) 文書に記述された機能を確認するために行われる。テストで重視されるのは、セクション 4.1 に規定された要件が満たされていることの確認であるが、いくつかの追加的テストがセクション 4.3 中の SAR について規定されている。保証アクティビティは、これらのコンポーネントと関連付けられた最小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、ならびにこの 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てカバレージの論拠を文書化した、テスト報告を作成する。

開発者のアクションエレメント：

ATE_IND.1.1D 開発者は、テストに用いられる TOE を提供しなくてはならない (shall)。

内容及び提示エレメント：

ATE_IND.1.1C TOE は、テストに適当なものでなくてはならない (shall)。

評価者のアクションエレメント：

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

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

保証アクティビティ：

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

83 テスト計画にはテストされるプラットフォームが特定され、そしてテスト計画には含まれていないが ST に含まれているプラットフォームについては、そのプラットフォームをテストしないことについての正当化をテスト計画が提供する。この正当化には、テストされるプラットフォームとテストされないプラットフォームとの違いを取り上げ、行われようとしているテストにその違いが影響しないという論拠を示さなくてはならない (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い。根拠が提供されなくてはならない (must)。ST 中の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。

84 テスト計画にはテストされるべき各プラットフォームの構成が記述され、また AGD 文書に含まれるもの以外に必要な設定があれば、それも記述される。テストの一部としての、または標準的なテスト前の条件としての、各プラットフォームの設置及び設定について、評価者が AGD 文書にしたがうことが期待されていることには注意すべきである (should)。これには、特別なテストドライバまたはツールも含まれるかもしれない。ドライバまたはツールのそれぞれについて、そのドライバまたはツールが TOE 及びそのプラットフォームによる機能の実行に悪影響を与えないという、(単なる主張ではなく) 論拠が提供される。

85 テスト計画には、高レベルのテスト目的とともに、これらの目的を達成するために行われるべきテスト手順も特定される。これらの手順には、期待される結果も含まれる。テスト報告 (テスト計画へ単に注釈を加えたものであってもよい) には、テスト手順が実施された際に行われたアクティビティが詳述され、またテストの実際の結果が含まれる。これは累積的な記述でなくてはならず (shall)、したがって失敗に終わったテストの実行が存在し、修正がインストールされ、そして次にテストの再実行が成功した場合、報告には単なる「成功」の結果だけではなく、「失敗」及び「成功」の結果 (及びそれを支持する詳細) が示される。

4.3.4 AVA クラス：脆弱性評定

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

4.3.4.1 AVA_VAN.1 脆弱性調査

開発者のアクションエレメント：

AVA_VAN.1.1D 開発者は、テストに用いられる TOE を提供しなくてはならない (shall)。

内容及び提示エレメント：

AVA_VAN.1.1C TOE は、テストに適当なものでなくてはならない (shall)。

評価者のアクションエレメント：

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

保証アクティビティ：

87 ATE_IND と同様に、評価者は報告を作成し、この要件に関連する自分たちの結論を文書化しなくてはならない (shall)。この報告は、物理的には ATE_IND に言及される全体的なテスト報告の一部であってもよいし、あるいは別個の文書であってもよい。評価者は、公開された情報の検索を行って、BIOS 製品一般に発見されている脆弱性と、特定の TOE に関する脆弱性を特定する。評価者は、参考としたソースと発見された脆弱性を報告中に文書化する。発見された脆弱性のそれぞれについて、評価者はそれが該当しないことを示す根拠を提供するか、あるいはそのほうが適切であれば脆弱性を確認するためのテストを (ATE_IND に提供されるガイドラインを用いて) 策定するかのどちらかを行う。適切かどうかは、その脆弱性を利用するために必要とされる攻撃ベクトルの評定によって判断される。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、この 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、脆弱性の悪用に電子顕微鏡と液体窒素が必要とされる場合には、テストは適当ではなく、適切な根拠が策定されることになるであろう。

4.3.5 ALC クラス：ライフサイクルサポート

88 この 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おいて開発者の手腕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なのである。

4.3.5.1 ALC_CMC.1 TOE のラベル付け

89 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指定できるように、TOE を識別することを目標としている。

開発者のアクションエレメント：

ALC_CMC.1.1D 開発者は、TOE 及び TOE への参照情報を提供しなくてはならない (shall)。

内容及び提示エレメント：

ALC_CMC.1.1C TOE は、そのユニークな参照情報によってラベル付けされなくてはならない (shall)。

評価者の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資料の内容及び提示のすべての要件を満たしていることを*確認しなくてはならない (shall)*。

保証アクティビティ：

90 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確証しなくてはならない (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、識別情報が ST 中のものと一貫していることを確証しなくてはならない (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調査して、ST 中の情報がその製品を識別するために十分であることを確証しなくてはならない (shall)。

4.3.5.2 ALC_CMS.1 TOE の CM カバレージ

91 TOE の対象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。

開発者の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くてはならない (shall)。

内容及び提示エレメント：

ALC_CMS.2.1C 構成リストには、以下が含まれなくてはならない (shall)：TOE そのもの、及び SAR によって要求される評価証拠。

ALC_CMS.2.2C 構成リストには、構成要素がユニークに識別されなくてはならない (shall)。

評価者の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資料の内容及び提示のすべての要件を満たしていることを*確認しなくてはならない (shall)*。

保証アクティビティ：

92 この PP において「SAR によって要求される評価証拠」は、ST 中の情報と、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確証する (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) 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。

4.4 セキュリティ機能要件の根拠

93 これらのセキュリティ保証要件を選択した根拠は､この PP がこの技術に関する最初の米国政府プロテクションプロファイルだからである。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。

5 適合主張

94 適合主張は、PP または ST によって満たされ、評価をパスした要件の集合のソースを示している。満たされなくてはならない (must) 特定の要件をさらに明確にするため、適用上の注意が SFR 及び SAR セクション中で提供される。

5.1 PP 適合主張

95 この PP は、CC 3.1r4 に適合し、CC パート 2 拡張及び CC パート 3 適合である。

96 この PP への適合を主張する ST は、CC パート 1 (CCMB-2006-09-001) のセクション D3 に定義される正確 PP 適合の最低基準を満たさなくてはならない (shall)。

97 正確 PP 適合は、PP 中の要件が満たされ、ST が PP の具体化であることを意味している。ST は、PP よりも広範囲であってよい。ST は、TOE が少なくとも PP と同一の動作をするが、運用環境はたかだか PP と同じ動作をすることを規定する。この PP では、規定された要件の意図と、ベンダが要件を満たすための方法に関する期待とを、さらに明確化し説明するために、適用上の注意が提供される。ST の評価者には、ST 及びその記述された TOE がこの PP 中のすべて (場合によってはそれよりもさらに多く) の言明を含むだけでなく、適用上の注意によって言明される期待を満たすことも判断することによって、正確 PP 適合を確証することが期待される。

5.2 PP 適合の根拠

98 この PP は、他の PP への適合を主張しない。

附属書A： 参考表と参照資料

[1] Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, July 2011

[2] Federal Information Processing Standards Publication (FIPS-PUB) 180-4, Secure Hash Standard, March, 2012

[3] Federal Information Processing Standard Publication (FIPS-PUB) 186-3, Digital Signature Standard (DSS), National Institute of Standards and Technology, June 2009

[4] NIST Special Publication 800-147, BIOS Protection Guidelines, April 2011

[5] NIST Special Publication 800-107, Recommendation for Applications Using Approved Hash Algorithms, February 2009

[6] NIST Special Publication 800-89, Recommendation for Obtaining Assurances for Digital Signature Applications, November 2006

[7] NIST Special Publication 800-102, Recommendation for Digital Signature Timeliness, September 2009

[8] ANS X9.31, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry, 1998

[9] RFC 3447, PKCS #1: RSA Cryptography Specifications Version 2.1, February 2003

[10] ANS X9.62, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 2005

[11] ITU-T Recommendation X.509, November 2008

[12] UEFI Specification Version 2.3. Unified EFI Forum. May 2009. http://www.uefi.org/specs/

[13] The Secure Hash Algorithm Validation System (SHAVS), by Lawrence E. Bassham III, July 2004 http://csrc.nist.gov/groups/STM/cavp/documents/shs/SHAVS.pdf.

略語

ANSI	米国規格協会
BIOS	基本入出力システム
CAVP	暗号アルゴリズム検証プログラム
CC	コモンクライテリア
CM	構成管理
CPU	中央処理装置
DSA	デジタル署名アルゴリズム
ECDSA	楕円曲線デジタル署名アルゴリズム
EEPROM	電気的消去可能プログラマブル読み出し専用メモリ
EFI	エクステンシブルファームウェアインタフェース
FIPS	連邦情報処理規格
ISSE	情報システムセキュリティエンジニア
IT	情報技術
ITU	国際電気通信連合
NIST	国立標準技術研究所
OEM	相手先ブランド製造業者
PC	パーソナルコンピュータ
PP	プロテクションプロファイル
PKCS	公開鍵暗号標準
PUB	公開
RTU	更新の信頼のルート
RSA	R. Rivest、A. Shamir と L. Adleman.
SAR	セキュリティ保証要件
SF	セキュリティ機能
SFR	セキュリティ機能要件
SHA	セキュアハッシュアルゴリズム
SHS	セキュアハッシュ標準
ST	セキュリティターゲット
TOE	評価対象
TSF	TOE セキュリティ機能
TSFI	TSF インタフェース
TSS	TOE 要約仕様

UEFI	ユニファイドエクステンシブルファームウェアインタフェース

附属書B： NIST SP 800-53/CNSS 1253 との対応付け

99 NIST SP 800-53/CNSS 1253 管理策のいくつかは、適合 TOE によって完全または部分的に対処されている。このセクションは対処されている要件を概説し、また TOE がその運用構成に組み込まれた際に (もしあれば) どんな追加的テストが必要かを認証員が判断するために利用することができる。

100 適用上の注意：このバージョンでは、単純な対応付けのみが提供されている。将来のバージョンでは、検定チームへさらに情報を提供する追加的な説明文が含まれることになる。追加的情報には、SFR から管理策への対応付けに関する詳細が含まれ、TOE によって提供される適合の程度が論じられることになる (例えば、完全に管理策を満たす、部分的に管理策を満たす)。さらに、規定された保証アクティビティの包括的なレビューと、SAR を満たす過程で行われる評価アクティビティがまとめられ、適合が判断される方法 (例えば、文書レビュー、ベンダの主張、テスト／検証の程度) に関する情報を検定チームへ提供することになる。この情報は、規定された管理策への適合の程度を判断するために (もしあれば) どんな追加的アクティビティを行う必要があるかを検定チームへ示すことになる。

101 ST では選択に関して選択が行われ、また割付が記入されることになるため、ST が完成し評価されるまで最終的なストーリーは必ずしもでき上がらないかもしれない。したがって、この情報は PP に加えて ST にも含まれるべきである (should)。また、特定の実装に基づいて評価者によって行われるアクティビティには何らかの解釈 (例えば「変更」) が必要となるかもしれない。スキームは、監督者 (例えば、検証者) にこの種の情報を記入させることもできるし、あるいは評価者に評価アクティビティの一環として行わせることもできるであろう。検証アクティビティは、評価チームの作業に加えて検定チームが (もしあれば) 何をする必要があるかを判断できるように、提供されなくてはならない (must) 不可欠の情報である。

識別子	**名称**	**該当する SFR**
AC-3	アクセス制御の実施	FPT_BUA_EXT.1.1, FPT_RTU_EXT.1.1
SC-3	セキュリティ機能の隔離	FPT_BUA_EXT.1.1, FPT_RTU_EXT.1.1
SC-13	暗号の使用	FPT_BUA_EXT.1.2, FCS_COP.1(1) FCS_COP.1(2)
SC-24	既知状態での故障	FPT_TEE.1.2, FPT_RCV.1.1
SI-7	ソフトウェア及び情報の完全性	FPT_BUA_EXT.1.2
SI-9	情報入力の制限	FPT_SLU_EXT.1 .1
SI-10	情報入力の検証	FPT_TEE.1.1

SI-11	エラー処理	FPT_RCV.1.1
SI-6	セキュリティ機能の検証	FPT_BUM_EXT.1
SI-3	悪意のあるコードからの保護	FPT_PBR_EXT.1

附属書C： 追加的要件

102 このバージョンの PP では、この附属書には追加的コンポーネントが含まれるが、それをサポートする脅威、対策方針、根拠、または保証アクティビティは含まれない (しかし、選択されたコンポーネントについてはガイダンスが提供される場合がある)。現在のレビューサイクルと並行して、このサポート情報は開発され、PP の次回リリースに取り込まれることになる。このセクションに含まれる情報へのコメント (ここに含まれる要件が適合 TOE 候補へ適用されかどうかについても、この附属書には含まれないが BIOS 製品には広く適用できる要件についても、どちらでも) は、歓迎され募集される。

103 この PP の概論で示したように、TOE が実装してもよく、その場合にも TOE が依然としてこの PP に適合するような追加的要件が存在する。これらの機能は必要とはされないが、運用環境への依存が生じることになる (例えば、TOE 管理者の識別と認証)。しかし、そのような機能を TOE が実装する場合には、ST 作成者は以下の情報を ST へ取り込むことになる。この附属書に含まれない要件が含まれてもよいが、それらは評価を監督する国家スキームによるレビュー及び承認を受けてから、本 PP への適合主張が行えるようになる。

C.1 TSF の保護 (FPT)

C.1.1 手作業による回復 (FPT_RCV)

FPT_RCV.1	**手作業による回復**
FPT_RCV.1.1	**詳細化**：**BIOS の更新が失敗するかブートに失敗した場合**、TSF は **FPT_SLU_EXT.1 に記述されるセキュアなローカル更新メカニズムを用いて**、セキュアな状態への復帰能力が提供されるメンテナンスモード~~に入らなくては~~**を提供**しなくてはならない (shall)。

適用上の注意：

104 BIOS 更新の回復メカニズムの提供はオプションである。しかし、回復メカニズムを TOE が提供する場合には、この要件が ST によって取り込まれることになるだろう。

105 この要件の意図は、TSF が認証された BIOS 更新メカニズムを用いて修正することができない、破損または正常に動作しないシステム BIOS からの回復を可能とすることである。TSF は、ブートプロセス中に物理的に存在する利用者が、現在のシステム BIOS を既知の良好なバージョンと構成で置き換えることを可能とするメカニズムを提供することになる。管理者ガイダンスには、管理者が回復プロセスにしたがうための指示が含まれることになるだろう。ST 作成者は FMT_SMF.1 を取り込んで、管理者がこのプロセスを通して BIOS を手作業で回復できるようにするセキュリティ管理機能を記述することになるだろう。

106 この要件は、FPT_SLU_EXT.1 セキュアなローカル更新に依存していることに注意されたい。

保証アクティビティ：

107 評価者は TSS セクションを調査して、BIOS 回復メカニズムを使用して適切なバージョンの BIOS のみがインストールされることを確実にする方法が記述されていることを確認しなくてはならない (shall)。評価者は AGD ガイダンスをレビューして、セキュアなローカル更新プロセスを用いるための指示によって手作業による回復が行えることを判断しなくてはならない (shall)。ガイダンス文書中のインタフェース記述は、そのメカニズムの動作の詳細と一貫している (例えば、TSS に取り込まれていない機能や特徴を提供するインタフェースのオプションやパラメタが存在しない) ことを確証するためにチェックされる。評価者は、AGD ガイダンスに提供される指示に従うことによって、プロセスを検証する。

108 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 : この要件をテストするため、評価者は BIOS 更新が完了する前に PC システムのシャットダウンを強制する (例えば PC の電源プラグを抜く) ことによって BIOS 更新プロセスを停止させ、回復プロセスを起動してもよい。
- テスト 2 : 評価者は、セキュアなローカル更新メカニズムを用いて、既知の良好なバージョンの BIOS に BIOS を更新する。

109 このコンポーネントが取り込まれる場合、以下の脅威、対策方針、及び根拠が ST に追加されるべきである (should)。

T.UNAUTHORIZED_BIOS_RECOVERY	攻撃者が、システム BIOS の (脆弱性の存在する可能性のある) バージョンをインストールすることになる、正当な回復プロセスを開始しようと試みるおそれがある。

O.BIOS_MANUAL_RECOVERY	TOE は、セキュアなローカル更新メカニズムを用いることによって、BIOS 更新が失敗またはブートが失敗した場合にセキュアな状態へ復帰することができなくてはならない (shall)。

T.UNAUTHORIZED_BIOS_RECOVERY 攻撃者が、システム BIOS の (脆弱性の存在する可能性のある) バージョンをインストールすることになる、正当な回復プロセスを開始しようと試みるおそれがある。	O.BIOS_MANUAL_RECOVERY TOE は、セキュアなローカル更新メカニズムを用いることによって、BIOS 更新が失敗またはブートが失敗した場合にセキュアな状態へ復帰することができなくてはならない (shall)。	O.BIOS_MANUAL_RECOVERY は、TOE がセキュアなローカル更新メカニズムを提供することを確実にすることによって、この脅威を低減する。このメカニズムは、ぜい弱性の存在する可能性のある古いファームウェアを攻撃者がフラッシュメモリへ書き込むことを防止する。

O.BIOS_MANUAL_RECOVERY TOE は、セキュアなローカル更新メカニズムを用いることによって、BIOS 更新が失敗またはブートが失敗した場合にセキュアな状態へ復帰することができなくてはならない (shall)。	FPT_RCV.1	FPT_RCV.1 は、BIOS 更新が失敗またはブートが失敗した場合にセキュアな状態へ復帰する機能を TOE が提供しなくてはならない (shall) と規定している。

C.1.2 拡張：セキュアなローカル更新 (FPT_SLU _EXT)

FPT_SLU_EXT.1	**拡張：セキュアなローカル更新**
FPT_SLU_EXT.1.1	TSF は、システム BIOS の更新を許可する前に正当な利用者が TOE への物理的なアクセスできることを要求する、 [割付：更新メカニズムの記述] セキュアなローカル更新メカニズムを提供しなくてはならない (shall)。
FPT_SLU_EXT.1.2	セキュアなローカル更新メカニズムは、 [選択：メーカーのオリジナルな BIOS イメージへの更新、FPT_BUA_EXT.1 に記述される認証された更新メカニズムを用いて修正することのできないシステム BIOS の破損からの回復] のためにのみ用いられなくてはならない (shall)。

適用上の注意：

110 この要件は、認証された更新メカニズムを用いることなくシステム BIOS を更新するセキュアなローカル更新メカニズムを含む BIOS の実装を特定する。セキュアなローカル更新メカニズムは、TOE への物理的な存在を要求することによって、BIOS 更新イメージの真正性と完全性を確証しなくてはならない (shall)。セキュアなローカル更新メカニズムの例としては、BIOS の更新を許可する前に、管理者パスワードの入力や、物理的なロック (例えば、マザーボードのジャンパ) のロック解除を要求するものが挙げられる。ローカル更新メカニズムの使用は、FPT_SLU_EXT.1.2 中の選択によって制約される。

111 管理ガイダンスには、管理者がローカル更新メカニズムのインタフェースを使用するための指示が含まれることになるだろう。ST 作成者は FMT_SMF.1 SFR を追加して、該当する場合にローカル更新メカニズムを開始する能力を管理者へ提供するための管理機能を取り込むことになるだろう。

保証アクティビティ：

112 評価者は TSS セクションをチェックして、セキュアなローカル更新機能がどのように実装されているかが明確かつ徹底的に記述されていることを確認しなくてはならない (shall)。評価者は AGD ガイダンスをレビューして、更新が成功したことを検証する方法を含め、BIOS 更新を完了するために必要なアクションがセキュアなローカル更新を利用するための指示に明確かつ完全に記述されていることを判断しなくてはならない (shall)。評価者は、AGD ガイダンスに提供される指示に従うことによって、セキュアなローカル更新をテストする。

113 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：セキュアなローカル更新は、以下の 2 つの機会にのみ利用されることになる。(1) 最初の BIOS イメージのロード、または (2) 認証された更新メカニズムを用いて修正することのできないシステム BIOS の破損からの回復、あるいはその両方。評価者は BIOS イメージを作成または取得し、認証された更新メカニズムによって BIOS 更新がインストールできなかった後にこのメカニズムを用いることができるかもしれない。

114 このコンポーネントが取り込まれる場合、以下の対策方針及び根拠が ST に追加されなくてはならない (must)。

O.BIOS_SECURE_LOCAL_UPDATE	TOE は、物理的な存在を要求することによって BIOS 更新イメージをインストールするメカニズムであって、更新の完全性を確証できるものを実装する。

T.UNAUTHORIZED_BIOS_UPDATE 攻撃者が PC クライアント中の BIOS を、TOE のセキュリティ機能を危殆化させるおそれのある悪意のある BIOS 更新によって置き換えようとする。	O.BIOS_SECURE_LOCAL_UPDATE TOE は、物理的な存在を要求することによって BIOS 更新イメージをインストールするメカニズムであって、更新の完全性を確証できるものを実装する。	O.BIOS_SECURE_LOCAL_UPDATE は、認証された BIOS 更新に代わるものとして、BIOS 更新の完全性を確証するために TOE への物理的な存在を要求することによって、この脅威を低減する。

O.BIOS_SECURE_LOCAL_UPDATE TOE は、物理的な存在を要求することによって BIOS 更新イメージをインストールするメカニズムであって、更新の完全性を確証できるものを実装する。	FPT_SLU_EXT.1	FPT_SLU_EXT.1 は、システム BIOS を更新するために物理的な存在を必要とするセキュアなローカル更新メカニズムを TOE が提供することを要求する。

C.1.3 外部エンティティのテスト (FPT_TEE)

FPT_TEE.1	**外部エンティティのテスト**
FPT_TEE.1.1	**詳細化**: TSF は **BIOS の更新前に**一連のテストを実行して、**[割付: BIOS 更新のバージョンが現在インストールされているバージョンよりも新しいことを確認する手法]** が満たされることをチェックしなくてはならない (shall)。
FPT_TEE.1.2	**詳細化**：このテストが失敗した場合、**TSF は以前の本物のバージョンへの BIOS の不正なロールバックを防止し、現在インストールされている BIOS を用いた通常のブートサイクルを開始しなくてはならない (shall)。ただし、以下の条件は除外される: [割付：ロールバックが許可されることになる条件を列挙する]。**

適用上の注意：

115 この要件は、BIOS が以前の真正のバージョンへ不正にロールバックされることを防止する。これによって、既知のセキュリティ上の弱点のある以前の真正の BIOS のバージョンがインストールされる可能性が排除される。FPT_TEE.1.2 中の選択は、インストール可能な BIOS の以前の真正のバージョンに関する条件を ST 作成者が規定することを要求している。

116 管理者ガイダンスには、該当する場合に管理者がロールバック防止メカニズムを構成するための指示が含まれることになるだろう。ST 作成者は FMT_SMF.1 SFR を取り込んで、該当する場合にロールバックメカニズムを開始する能力を提供するための管理機能を記述することになるだろう。

保証アクティビティ：

117 評価者は TSS セクションをチェックして、FPT_TEE.1.2 の割付の中に規定される条件が満たされない場合にインストールされようとしている BIOS 更新バージョンが以前の真正のバージョンでないことを TSF が確認する方法が明確かつ徹底的に記述されていることを確認しなくてはならない (shall)。評価者は TSS セクションをチェックして、インストール可能な BIOS の以前の真正のバージョンに関する条件が記述されていることを確認しなくてはならない (shall)。評価者は、AGD ガイダンスに提供される指示に従い、以下のテストを行うことによって、ロールバックメカニズムをテストする。

118 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、FPT_TEE.1.2 の割付の中に規定される条件が満たされていない場合に、認証された更新メカニズムを用いて以前の真正の BIOS バージョンのインストールを試みる。評価者は、システムが BIOS の更新を許可しないこと、及び現在インストールされている BIOS を用いてリブートすることを検証する。リブート中、評価者は BIOS バージョンが最後の成功した更新のものと同一であることを検証すべきである (should)。
- テスト 2：評価者は、FPT_TEE.1.2 の割付の中に規定される条件が満たされている場合に、以前の真正の BIOS バージョンのインストールを試みる。評価者は、システムが BIOS の更新を許可すること、及び以前の BIOS バージョンを用いてリブートすることを検証する。リブート中、評価者は BIOS バージョンを検証すべきである (should)。

119 このコンポーネントが取り込まれる場合、以下の脅威、対策方針、及び根拠が ST に追加されるべきである (should)。

T.UNAUTHORIZED_BIOS_ROLLBACK	攻撃者が、システム BIOS の (脆弱性の存在する可能性のある) 古いバージョンをインストールしようと試みるおそれがある。

O.BIOS_ROLLBACK	TOE は、BIOS の以前の真正のバージョンへの不正なロールバックを防止するメカニズムを実装すること。

T.UNAUTHORIZED_BIOS_ROLLBACK 攻撃者が、システム BIOS の (脆弱性の存在する可能性のある) 古いバージョンをインストールしようと試みるおそれがある。	O.BIOS_ROLLBACK TOE は、BIOS の以前の真正のバージョンへの不正なロールバックを防止するメカニズムを実装すること。	O.BIOS_ROLLBACK は、TOE が BIOS の以前の真正のバージョンへの不正なロールバックを防止するメカニズムを実装することを確実にすることによって、この脅威を低減する。

O.BIOS_ROLLBACK TOE は、BIOS の以前の本物のバージョンへの真正なロールバックを防止するメカニズムを実装すること。	FPT_TEE.1	FPT_TEE.1 は、TSF が BIOS イメージのバージョンをチェックすることと、BIOS 更新バージョンが現在インストールされているバージョンよりも新しいことを検証する手法を持つことを要求している。また、ロールバックを許可することになる一部のその他のアクションを例外として、TSF が真正の本物のバージョンへ BIOS が不正にロールバックされることを防止し、現在インストールされている BIOS を用いた通常のブートサイクルを開始することも要求している。

C.1.4 高信頼 TSF 更新 (FPT_TUD)

拡張：高信頼更新 (FPT_TUD_EXT.1)

FPT_TUD_EXT.1	**拡張：高信頼更新**
FPT_TUD_EXT.1.1	TSF は、TSF 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提供しなくてはならない (shall)。
FPT_TUD_EXT.1.2	TSF は、TOE ソフトウェアの更新を開始する能力を提供しなくてはならない (shall)。
FPT_TUD_EXT.1.3	TSF は、FCS_COP.1(x) に規定されるようにデジタル署名の検証が成功した場合に限り、TSF 更新のインストールを許可しなくてはならない (shall)。
適用上の注意：	3 番目のエレメントで参照されているデジタル署名メカニズムは、ST 本体の FCS_COP.1(x) に規定されているものである。ST 作成者は、採用されるアルゴリズムが BIOS への更新の検証に用いられるものと同一である場合には最初の繰返しを用いてもよいし、あるいは異なるアルゴリズムが用いられる場合には FCS_COP.1 を繰返してもよい。
保証アクティビティ：	TSF への更新は、権限のあるソースによって署名される。権限のあるソースの定義は、更新検証メカニズムによって用いられる鍵が TOE にインストールされる方法の記述とともに、TSS 中に含まれる。評価者は、この情報が TSS に含まれ、また更新鍵のインストールに対応する任意の指示が操作ガイダンスに詳述されていることを確証する。また評価者は、更新候補が取得される方法、更新のデジタル署名の検証に関連した処理、そして成功の (署名が検証された) 場合と不成功の (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も確証する。 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、バージョン検証アクティビティを行って TSF の現在のバージョンを判断する。以下のテストに記述されている更新テストの後、評価者はこのアクティビティを再び行って、バージョンが更新のバージョン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、操作ガイダンスに記述されている手順を用いて本物の更新を取得し、その TOE へのインストールが成功するることを検証する。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、更新が期待されたとおり機能していることを例証する。 • テスト 3 : 評価者は、偽物の更新を取得または作成し、TOE へそれをインストールしようと試みる。評価者は、TSF がその更新を拒否することを検証する。

附属書D： 文書の表記

120 英国式つづりを米国式つづりに置き換えた以外には、この PP に用いられる記法、様式、及び表記はコモンクライテリア (CC) のバージョン 3.1 と一貫している。PP の読者を助けるため、選択された表記法についての議論をここで行う。

121 この PP に用いられる記法、様式、及び表記は、CC のバージョン 3.1 に用いられるものとおおむね一貫している。PP の利用者を助けるため、選択された表記法についての議論をここで行う。CC では、機能及び保証要件に対していくつかの操作を行うことを許可している。詳細化、選択、割付、及び繰返しが CC 3.1 のパート 1 の附属書 C4 に定義されている。これらの操作のすべてが、この PP で用いられている。

詳細化の表記

122 **詳細化**の操作は、要件に詳細を付け加え、これによってさらに要件を制約するために用いられる。セキュリティ要件の詳細化は、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、太字で表記された要件中の追加的な本文によって示される。

選択の表記

123 **選択**の操作は、CC によって要件の言明中に提供された 1 つ以上の選択肢を選択するために用いられる (CC 3.1 のパート 1、附属書 C.4.3 を参照)。PP 作成者によってなされた選択は**太字**で表記されたその選択と、大括弧及び「選択」の文字を削除して示される。ST 作成者によって記入されるべき選択は、大括弧中に選択が行わるべきことを示す指示によって示される： [選択：]。

割付の表記

124 **割付**の操作は、例えばパスフレーズの長さのように、まだ規定されていないパラメタへ特定の値を割り付けるために用いられる (CC 3.1 のパート 1、附属書 C.4.2 を参照)。**太字**で示された値は、その割付が PP 作成者によってなされたことを示し、大括弧と「割付」の文字は削除される。ST 作成者によって記入されるべき割付は、大括弧中に割付が行わるべきことを示す指示によって示される： [割付：]。

繰返しの表記

125 **繰返し**の操作は、変化する操作と共にコンポーネントが繰り返される場合に用いられる (CC 3.1 のパート 1、附属書 C.4.1 を参照)。繰返し回数 (iteration_number) は、コンポーネントの識別子に引き続く括弧の中で示される。

126 繰返しの操作は、すべてのコンポーネント上で実行できる。PP/ST 作成者は、同一のコンポーネントに基づく複数の要件を取り込むことによって、繰返し操作を行う。コンポーネントの各繰返しは、そのコンポーネントの他のすべての繰返しとは異なっていなくてはならず (shall)、これは割付及び選択を異なる方法で完成させることによって、または異なる方法で詳細化を適用することによって、実現される。

127 附属書 C に記述される要件については、そのコンポーネントがこの PP に用いられる場合、繰返し番号は「(#)」として示され、ST 作成者が「#」を適切な繰返し番号で置き換えなくてはならない (must) ことを意味している。

拡張要件の表記

128 拡張要件は、作成者のニーズを満たす適切な要件を CC が提供していない場合に許される。**拡張要件**は特定されなくてはならず (must)、またその要件を関連付けるにあたって CC のクラス／ファミリ／コンポーネントモデルを利用することが要求される。拡張要件は、コンポーネント中に「EXT」を挿入することによって示される。

適用上の注意

129 適用上の注意には、適合 TOE のセキュリティターゲットの構築に関連する、または役立つと考えられる追加的なサポート情報に加えて、開発者や評価者、そして ISSE への一般的な情報が含まれる。また適用上の注意には、コンポーネントの許可された操作に関するアドバイスも含まれる。

保証アクティビティ

130 保証アクティビティは、TOE に課された機能要件が脅威を低減するための共通評価方法として役立つ。このアクティビティには、TSS に文書化された TOE の特定の側面を評価者が分析するための指示が含まれているため､ST 作成者にはこの情報を TSS セクションへ取り込むという暗黙の要件が課される。このバージョンの PP においては、これらのアクティビティは機能及び保証コンポーネントと直接関連付けられているが、将来のバージョンではこれらの要件が別個の附属書または文書へ移動されるかもしれない。

附属書E： 用語集

基本入出力システム (BIOS) - 従来の BIOS、エクステンシブルファームウェアインタフェース (EFI)、そしてユニファイドエクステンシブルファームウェアインタフェース (UEFI) に基づいたブートファームウェアの総称。

従来の BIOS - 多くの x86 互換コンピュータシステムに用いられる、レガシーなブートファームウェア。また、レガシーBIOS とも呼ばれる。

エクステンシブルファームウェアインタフェース (EFI) - オペレーティングシステムとプラットフォームファームウェアとの間のインタフェースに関する仕様。EFI 仕様のバージョン 1.10 が EFI 規格の最終版であり、ユニファイド EFI フォーラムによって作成されたそれ以降のリビジョンは UEFI 仕様の一部である。

フラッシュメモリ - システム BIOS の不揮発性ストレージ領域であって、通常マザーボード上の電気的消去可能プログラマブル読み出し専用メモリ (EEPROM) フラッシュメモリに存在する。システムフラッシュメモリは技術固有の用語であるが、システムフラッシュメモリへ言及するこの文書のガイドラインはシステム BIOS を含む任意の不揮発性ストレージ媒体への適用を意図している。

ファームウェア - 読み出し専用メモリ (ROM) に含まれるソフトウェア。

運用環境 - 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。ホストプラットフォームやそのファームウェア、そしてオペレーティングシステムを含む。

オプション ROM - システム BIOS によって呼び出されるファームウェア。オプション ROM には、増設カード (例えば、ビデオカード、ハードドライブコントローラ、ネットワークカード) 上の BIOS ファームウェアや、システム BIOS の機能を拡張するモジュールが含まれる。

永続的メモリ - 電源が切られた際にもデータを保持するデータストレージ。

プロテクトモード - x86 互換プロセッサに見られる動作モードであって、メモリ保護、仮想メモリ、及びマルチタスキングをハードウェアでサポートする。

更新の信頼のルート (RTU) - この文書での用法は、 a. 署名検証アルゴリズム、 b. BIOS 更新イメージ上の署名を検証するために必要な公開鍵を含む鍵保管、または c. 公開鍵が更新される BIOS と共に提供される場合には公開鍵の代わりに公開鍵のハッシュ、を含む信頼のルートである。

SAR (セキュリティ保証要件) - 開発者やラボがセキュリティ機能要件への適合を例証するための開発及び評価方法を記述する。

SFR (セキュリティ機能要件) - TOE によって満たされなくてはならないセキュリティ機能を記述する。

ST (セキュリティターゲット) - TOE のセキュリティ属性を記述し特定する。

評価対象 (TOE) - ホストマシン上の利用者データを暗号化／復号するための要件を満たす製品または製品のセットを指す。これには、この PP の要件を満たすために用いられるすべてのハードウェア、ファームウェア、及びソフトウェアが含まれる。

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から構成されるセットであって、TSP を正しく強制するために信頼されなくてはならないもの。

TOE セキュリティ方針 (TSP) - TOE 内で資産がどのように管理され、保護され、そして配付されるかを規制する一連のルール。

TOE 要約仕様 (TSS) - TOE の動作とセキュリティ機能要件の実装が理解できる程度にまで十分に詳細に、TOE が SFR を満たす方法を記述した説明文。

ユニファイドエクステンシブルファームウェアインタフェース (UEFI) - 従来の BIOS に取って代わる候補で、新しい x86 ベースのコンピュータシステムで広く用いられるようになってきている。UEFI 仕様は、EFI の後継である。

揮発性メモリ - 電源が切られた際にその内容が失われるメモリ。

附属書F： PP 識別情報

タイトル：	Protection Profile for PC Client Devices (PC クライアントデバイスのプロテクションプロファイル)
バージョン：	1.0
スポンサー：	(米国) 国家安全保障局 (NSA)
CC のバージョン：	Common Criteria for Information Technology Security Evaluation (CC) Version 3.1, R3 July 2009 (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 (CC) バージョン 3.1 改訂第 3 版､2009 年 7 月)
キーワード：	認証された BIOS 更新、BIOS、RTU