H13－認証・公証WG－1

電子署名プログラム

Protection Profile

平成 14年 3月

電子商取引推進協議会
認証・公証WG

第 1 部

電子署名プログラム Protection Profile 解説

第２部

電子署名プログラム Protection Profile

連絡先

電子商取引推進協議会（ECOM）
認証・公証WG
〒 105-0011
東京都港区芝公園　機械振興会館 3 階
TEL. 03-3436-7500
FAX. 03-3436-7570
E-mail：info@ecom.jp
http://www.ecom.jp/

第１部 電子署名プログラムProtection Profile解説

目　次

はじめに

本書「電子署名プログラム Protection Profile」は、第１部「電子署名プログラム Protection Profile 解説」(以下、第 1 部と記す)と第 2 部「電子署名プログラム Protection Profile」(以下第 2 部と記す)からなる。

第１部では、電子署名生成・検証プログラムを開発・提供する企業や同プログラムの導入を検討している企業での利用を想定し、第 2 部を利用する上で必要な前提等を記述している。

第 2 部では、電子署名生成・検証プログラムに必要なセキュリティ要件をまとめている。この Protection Profile に準拠して電子署名プログラムのセキュリティ認証を受けたり、あるいは設計上の参考とすることができる。

第 1 部の構成と概要は以下の通り。

章	内　　容
1 利用方法 2 PP の種類と選択	本報告書の利用方法について説明する。 保証要件のレベル（EAL）について説明する。
3 TOE について	評価対象（TOE）について説明する。
4 暗号技術について	暗号技術の安全性に関して留意すべき点について説明する。
5 IT セキュリティ要件解説	TOE セキュリティ要件と IT 環境セキュリティ要件について説明する。

平成 13 年度は、日本において電子認証・電子署名を経済活動の基礎として広汎に導入するための枠組みの整備が、実質的な形をとりはじめた年である。行政においては、平成 12 年度からの電子認証の導入が、政府認証基盤（GPKI： Government PKI）などの形で具体化している。また、民間での電子認証・電子署名利用に関する法律上の裏付けとして「電子署名および認証業務に関する法律」（通称「電子署名法」）が平成 13 年 4 月 1 日に施行されている。

電子署名法は、二つの側面を持つ。一つは電子署名に関する規定であり、もう一つは電子認証業務を対象とする基準と認定制度である。そして、電子署名については、第三条でその効力に裏付けを与えている。

第三条　電磁的記録であって情報を表わすために作成されたもの（公務員が職務上作成したものを除く。）は、当該電磁的記録に記録された情報について本人による電子署名（これを行うために必要な符号及び物件を適正に管理すること

により、本人だけが行うことができることとなるものに限る。）が行われているときは、真正に成立したものと推定する。

ここで、下線部は、電子署名を行うパソコンや、電子署名に利用する秘密鍵が適正に管理されていて、なりすまし等の不正が行われないことを要請している。このためには、電子署名を生成し、あるいは検証するプログラムに着目しても、外部からの攻撃や誤使用に対して十分な対策を装備していることが求められる。第 2 部は、この観点で当該プログラムが具備すべき機能やその動作環境における前提を、ISO/IEC 15408 (Common Criteria) **に則りプロテクション・プロファイルとして表現したものである。**

第 1 部および第 2 部は、電子商取引推進協議会（ECOM**）の認証・公証 WG で策定した。**

プロテクション・プロファイルの目的に鑑み、他者による利用を何ら制限しない。例えば、次のような利用が無償で認められる。

製品のセキュリティ認証のために、本プロテクション・プロファイルを複製等の方法で利用したセキュリティ･ターゲット(ST)を作成する。

セキュリティ･ターゲットにおいて、本プロテクション・プロファイルを準拠元のプロテクション･プロファイルとして、その旨を表示する。

本プロテクション・プロファイルの内容を参考にし、あるいは流用して、別のプロテクション･プロファイルを作成する。

平成 12 年度の認証・公証 WG では、前述した電子署名法の要件を受けて、「電子署名利用者システムの構築・利用ガイドライン」（H12－認証・公証 WG－1）を作成した。その対象読者と内容は、次のとおりである。

① 電子署名の利用者である企業や個人を対象にした、利用上の留意事項

② 電子署名プログラムの開発者向けの、電子署名の安全性の観点から電子署名プログラムで採るべき対策

③ 電子署名プログラムの開発者向けの、電子署名の利便性の観点から電子署名プログラムで採るべき対策

第 1 部および第 2 部は、上記②の内容を継承している。平成 12 年度作成したガイドラインでは、開発者の留意事項を幅広く挙げている。これに対して、プロテクション・プロファイルは電子署名プログラムのセキュリティ認証に一般的に利用できることを目指し、ま

た実装方法に選択がありうることを考慮して、対策や機能を厳選している。また、電子署名プログラムの利用場面についてはガイドラインに具体的かつ詳細な記述があり、本プロテクション・プロファイルと併せて参照して頂く事を推奨する。

1 利用方法

本報告書の「電子署名プログラム プロテクション・プロファイル」(PP)の利用方法としては、大きく次の３つが考えられる。

1. セキュリティ評価・認証における準拠 PP として

   報告書の PP は、今後 PP として評価・認証を受ける予定である。

   本 PP が評価・認証を受けると、電子署名プログラムのセキュリティ評価を受けるために ST を作成する際に、その製品の TOE が当該 PP の TOE を含んでいれば、ST にこの PP 準拠と記載することで、新たな ST 記述は追加部分のみになるため、ST 作成の負担を軽減することが可能となる。

2. セキュリティ評価・認証における参考資料として

   今回提供した PP とは TOE が異なる等、そのままでは準拠と表示できない製品の認証を受けるための ST を作成するときにも、本 PP を参考にすることで、脅威の網羅性不足等、大きなレベルでの評価項目のもれが防止できる。

3. 開発の指針として

   電子署名利用者プログラムを開発する際に、セキュリティに関して留意すべき要件項目が PP として網羅されていることから、将来のセキュリティ評価に向けて、この PP を指針とした製品開発を行うことができる。

2 PPの種類と選択

「電子署名プログラム プロテクション・プロファイル」(PP)には、評価レベル(EAL; Evaluation Assurance Level)が「2 追加」、「3 追加」および「4」の 3 種類ある。

電子署名プログラムの開発者は、セキュリティ・ターゲット(ST)および製品についてセキュリティ認証を得る際に、この中から適切な EAL のプロテクション・プロファイルを選択して利用できる。

2.1 EAL とは

ISO/IEC 15408 (Common Criteria) においては、保証要件（どれだけ確実にその製品が開発されたかを示す要件）のレベルを EAL として規定している。EAL には 1 から 7 までの 7 段階があり、民需用の製品には一般に 1 から 4 のいずれかを適用する。EAL が高いほど、評価において内部構造や実装を深く調査する。例えば、EAL4 では、プログラムの一部のソースコードも調査する。したがって、適用する EAL が高いほど評価の信頼感が高いが、その反面、評価を受けるベンダーの費用負担・作業負担は高い。詳細は ISO/IEC 15408 (第 2 部 1.4 節の参考資料(1)～(3))を参照されたい。

なお、EAL はあくまでも保証要件のレベルであり、製品が持つセキュリティ機能を評価するための機能要件の質や量には言及していないことについては、注意する必要がある。すなわち、高い EAL レベルで評価を受けた製品であるといっても、それはいかに確実にセキュリティ機能の作り込みが行われたかを保証するだけであり、いかに多くの強力なセキュリティ機能を持っているかについては、PP や ST に記載されている機能要件を直接確認する必要があり、EAL からは何もいえないということである。

2.2 EAL の選択

電子署名プログラムの開発者は、適用する EAL を次の事項を考慮して選択する。

2.2.1 ISO/IEC 15408 における一般的な位置付け

一般的に、各 EAL は次のような位置付けにある。

- **EAL2：製品の一部を OEM 調達している等、完全な開発記録を使用できないがセキュリティ保証が必要な製品に、適用するレベルである。**
- **EAL3：大幅なリエンジニアリングを行わずに、TOE とその開発の調査によるセキ**

ュリティ保証を必要とする製品に、適用するレベルである。

- **EAL4：TOE に民需品ではトップレベルのセキュリティ保証を必要とし、そのためのエンジニアリングコスト（費用、作業量、期間）を負担できる製品に、適用するレベルである。**

2.2.2 電子署名の特性や評価コストの考慮

電子署名はセキュリティを確保するための機能であることから、可能であれば高位の EAL4 を適用することが望ましいと考えられるが、製品の位置付け、開発・評価のためのコスト等も考慮して、開発者はその製品に適切なレベルを決定する必要がある。ここで考慮すべきコストとしては、費用（開発費用及び評価費用）、開発者の作業量、期間（開発期間及び評価期間）、その他（高いレベルの評価には時間がかかり、その分、評価を受けた製品として販売できる期間が短くなること等）があると考えられる。

2.2.3 アプリケーション・プログラムとＥＡＬ

電子署名を含むアプリケーション・プログラムのセキュリティ認定を行う場合に、内蔵している電子署名プログラムの部分については、本プロテクション・プロファイルに基づく認証を受けることが考えられる。この場合、電子署名プログラムに適用する EAL は、位置付けから考えてアプリケーション・プログラムに適用予定の EAL よりは高いことが望まれる。したがって、不特定のアプリケーション・プログラムでの採用を想定する電子署名プログラムにおいては、民間対象の製品として通常採り得る最高の EAL4 を適用することが安全である。

なお、特定のアプリケーション・プログラムのセキュリティ認証においては、当該アプリケーション・プログラムの特性を考慮して EAL を選択する必要がある。例えば、高額の電子商取引に用いるソフトウェアと個人のメール用ソフトウェアでは、異なる EAL を適用することに妥当性がある。

2.2.4 ＥＡＬのカストマイズ

EAL は保証要件項目のセットであるが、製品によっては一部の要件項目を追加（または要件のレベルアップ）したい場合がある。また、機能要件として指定した要件から特定の保証要件が関連で必要になることもある。このような場合には、EAL x に ISO/IEC 15408

の Part 3から必要な項目を追加／レベルアップすることになる。その場合には ST 概要の保証レベルには通常 augmented EAL x (EAL 追加、EAL x+)といった記述が行われる。本 PP では、EAL２と３は追加、EAL4 は EAL のレベルにあわせて作成している。これを製品に適用して ST を作成する際には、必要に応じて保証要件を追加してよい。ただし、追加項目がある場合には、その分開発者や評価者の負担が増加することになるため、必要性について十分考慮すべきである。

製品として指定したい保証要件が、あるレベルの EAL とほぼ同等であるが一部の要件対応が不足しているといった場合には、当該 EAL を適用しているとは見なされず、「EAL x －」のような表現も認められていないため、さらに下位の全項目に適用可能な EAL を元にしてレベルを決定する必要がある。

3 TOE について

3.1 TOE の前提、指針

ここでは、本 PP が対象とする TOE の前提、指針を述べる。

本電子署名プログラムは、ライブラリ的な性格を有し、アプリケーションプログラム等の一環として動作するものを想定している。したがって、電子署名プログラムは、オペレーティングシステム等の環境や、本プログラムを利用するアプリケーションプログラムとの関係、境界などに関し多様性がある。TOE としては、このような署名プログラムの多様性を前提とし、できるだけ多くの実装での準拠、あるいは参考が可能となることを指針としている。

上記のような多様な実装に対して適用可能とし、さらに ST へ展開する際に本 PP を採用しやすくするために、PP としての TOE の範囲は、電子署名プログラムの中核の部分を定義するに留めている。すなわち、識別認証機能、アクセス制御機能、監査機能等を IT 環境として提供することで、PP としての中立性を確保し、ベンダーが ST 展開時に TOE を拡張させていくことが出来るよう汎用性を考慮している。

3.2 TOE の範囲、保護対象資源

評価対象である TOE は、以下の５つの機能から構成される。

- 鍵管理機能
- 認証局証明書管理機能
- EE 証明書管理機能
- 署名生成機能
- 署名検証機能

また、署名プログラム及び署名プログラムで利用されるデータで保護されなければならないものとして、以下の５つの資源を本 TOE の保護対象資源とする。

- 秘密鍵
- 認証情報
- 認証局証明書
- 監査ログ
- 電子署名プログラム自身

TOE、保護対象資源に関し、特筆すべき点として次のような事項がある。

- 鍵管理機能は、鍵の生成機能を持つこととしている。また、秘密鍵利用時の認証機能を有する。（本 PP における TOE では、電子署名管理システムの外部で作成された秘密鍵を、インポートする機能は含めていないが、電子署名管理アプリケーション開発においては、同機能を実装することを推奨する。）
- 識別認証機能、アクセス制御機能、監査機能等は、本プログラムを実装する上での支援機能として、IT 環境で提供されるものとする。これらは、ベンダーが ST 策定時に ST の TOE に包含することが可能である。
- 監査機能は IT 環境で提供されるものとしているが、TOE の各機能に固有な監査情報は、各機能で収集することとする。
- 秘密鍵、認証情報、監査ログ等保護対象資源のファイルは、IT 環境（オペレーティングシステム等）のファイルシステムの利用を想定している。したがって、IT 環境はファイルへのアクセス制御機能を持つものとする。

4 暗号技術について

4.1 暗号技術の安全性

電子署名プログラムを実装する場合、適用すべき暗号技術は当該電子署名プログラムの利用用途などで異なってくると思われる。例えば、不特定多数の通信相手を想定した電子メールにおける電子署名プログラムなどは、相互運用性などの観点も重視される。

ここでは、電子署名プログラムとして最低限有していなければならない、暗号技術の安全性について考察する。つまり、電子署名プログラムを実装する場合、安全性の観点から、暗号技術を如何に適用するのかについて述べる。

暗号技術に関しては、絶対的な安全性を有するアルゴリズムが存在する訳ではないのが現実である。だからと言って、暗号技術を利用した電子署名プログラムの有用性を活用しないことはできない。何らかの基準を満たしている暗号技術を適用することが現実的である。また、暗号技術は日々の学術／技術的な進歩に大きく関連がある。よって、現在は安全とされる暗号技術でも、将来も安全であるとは限らない。このため、暗号技術の安全性の基準は、随時変化するものと認識する必要がある。

4.2 暗号技術の安全性評価

暗号技術の選択は、暗号技術の安全性に関する評価を参考にすべきである。暗号技術の評価は専門家でも難しく、全ての専門家が同一の評価とならない場合もある。このため、暗号技術の安全性に関する評価は、その過程や評価データなどが公開され、広くコメントを受け付けられる場で行われるべきである。

参考になると思われる暗号技術の安全性評価基準の例を以下に示す。

4.3 暗号技術に関する参考資料

ここでは、参考になると思われる暗号技術の安全性評価基準を紹介する。

4.3.1 「電子署名及び認証業務に関する法律」に基づく特定認証業務の認定に係わる指針

平成 13 年 4 月 1 日に施行された「電子署名及び認証業務に関する法律」（電子署名法）に定められる、特定認証業務に係わる指針である。この第三条において、電子署名の基準

が示されている。

総務省：http://www.soumu.go.jp/joho_tsusin/top/denshi_syomei/

法務省：http://www.moj.go.jp/MINJI/minji32-3.html

経済産業省：http://www.meti.go.jp/policy/netsecurity/digitalsign.htm

4.3.2 CRYPTREC

電子政府で適用可能な暗号技術のリストアップを目的として平成12年度から開始された暗号技術評価委員会である。暗号技術評価報告書が「CRYPTREC REPORT」として公表されている。

IPA：http://www.ipa.go.jp/security/enc/CRYPTREC/

4.3.3 ISO/IEC JTC1 SC27

情報セキュリティ技術の標準化を進める専門委員会であり、暗号技術の標準化を行っている。これは、3つのグループから成り立っており、WorkingGroup2 にて暗号アルゴリズムの標準化を行っている。

ISO/IEC JTC1 SC27：

http://www.jtc1.org/Navigation.asp?Area=Structure&Mode=Browse&CommLevel=SC&SubComm=ISO%2FIECJTC1SC00027&x=7&y=9

4.3.4 IEEE P1363

IEEE はエレクトロニクス関連で世界最大の学会である。1996 年より公開鍵暗号・認証方式の標準化を行っており、その標準規格が P1363 にあたる。

IEEE P1363：http://grouper.ieee.org/groups/1363/

4.3.5 NESSIE

2000 年から 2002 年 12 月までの 3 年計画予定で始まった欧州連合における暗号・認証技術評価プロジェクトである。

NESSIE ：http://cryptonessie.org/

5 IT セキュリティ要件解説

本 PP は、多くの電子署名プログラムに適用されることを目指している。そのため、本 PP の「5. IT セキュリティ要件」は、その範囲を個々の電子署名プログラムやその適用によらずに共通に必要なものに限定している。一方では、製品がより高いセキュリティ要件に対応しているならば、その ST においてより広く IT セキュリティ要件を採用し、製品の高いセキュリティ実装を示すことができる。本章では、本 PP には採用していないが製品には実装される可能性が高く、ST 策定において検討すべき IT セキュリティ要件を解説する。また、本 PP に含む IT セキュリティ要件についても、ST 策定の際の考慮すべき割付の内容等について説明を加えている。

なお、本解説には「割付」の記述を示している部分があるが、これは一般的なシステムを想定した例であり、具体的には「選択」「詳細化」及び「繰返し」の各未決定項目とともに、電子署名管理システムの仕様にあわせて ST 策定時に確定する必要がある。

5.1 TOE セキュリティ要件解説

表中、PP 記述の欄の「なし」は本 PP には採用していないが実装される可能性が高い要件、「(n)」は本 PP のセキュリティ要件 n 番の記述に関する考慮事項を示す。

項　目	PP 記述	解　　説
FCS_COP.1 暗号操作	(1)	本要件は、署名プログラムにおける秘密鍵秘匿のための暗号操作に関するものである。秘密鍵に対する暗号操作については、一般的に、暗号方式やアルゴリズム、鍵長はセキュリティ確保のために公表していないが、保護資産に関する重要な要件であるためセキュリティ要件として採用することが必要である。 本要件への対応では、 ・ST の公開レベルの決定 ・認証取得のための評価機関への資料提示方法の決定 が必要である。 ST の公開レベルとしては、公開・部分的公開（一部の情報を秘匿）・非公開の３つがあり、非公開情報の扱いをどのレベルにするかについて決定する必要がある。 また、評価機関への資料提示については、厳密な守秘義務や、開発元社内等の特定施設での資料確認等についての対応依頼(対応可能な評価機関による評価）等を評価機関と協議し、合意する必要がある。 ［割付：標準のリスト］には、国際規格、国内規格、業界標準などを記述することができ、また省略してもよい。電子署名プログラム向けには現時点では一般的な標準はないため、ST では本割付は省略することを想定している
FDP_RIP.1 サブセット残存情報保護	(2)	本要件は、メモリ上の秘密鍵保護のための項目である。 ［割付：オブジェクトのリスト］には、「暗号化されていないメモリ上の秘密鍵」等を指定する。

項　目	PP記述	解　　説
FCS_CKM.1 暗号鍵生成	(3)	本要件は、署名に使用する公開鍵と秘密鍵のペアの生成・破棄に関するものである。 ［割付：標準のリスト］には、国際規格、国内規格、業界標準などを記述することができ、また省略してもよい。電子署名プログラム向けには現時点では一般的な標準はないため、ST では本割付は省略することを想定している。 ［割付：暗号鍵生成アルゴリズム］及び［ST 割付：暗号鍵長］には、鍵生成時のアルゴリズム及び鍵長を指定する。 ［割付：暗号鍵破棄方法］には、鍵の破棄方法を指定する。
FCS_CKM.4 暗号鍵破棄	(4)	
FIA_UAU.1.1[1] 認証のタイミング	(5)	本要件は、秘密鍵の使用を前提とする操作は認証を受けるまでは TOE が許可しないことに関するものである。 [割付:TSF 調停アクションのリスト]には、認証前に許可する操作を電子署名管理システム(TOE)の仕様に応じて示す。
FIA_UAU.7 保護された認証フィードバック	なし	本要件は、利用者認証の過程において認証の失敗を伝える場面を想定したものである。 電子署名プログラムに関する利用者認証には、一般に次の二つの機能がある。 a. OS やアプリケーションにおいてユーザ ID とパスワードにより行う利用者認証 b. アプリケーション・プログラムから電子署名プログラムを呼び出す際に「ユーザ PIN」等と呼ばれる認証情報を受け渡して行う利用者認証 このうち TOE セキュリティ要件を適用する「b」では、利用者に直接に渡す認証フィードバックは通常はないので、本要件は必要ではなく、PP に含めていない。 「b」について直接の認証フィードバックがないので本要件を満たすとの見方をとり、ST に含めるとの選択も十分にありうる。
FIA_SOS.1 秘密の検証	なし	本要件における「秘密」は、TOE セキュリティ要件としては、利用者認証のためのユーザ PIN がありうる。その「定義された品質尺度」とは、ユーザ PIN の推定を困難にするための、最小文字数や文字列構成の規約等である。しかし、電子署名プログラムでユーザ PIN に対して「定義された品質尺度」に合致することを検証するメカニズムを提供することは一般的には要求できないため、本要件は PP に含めていない。

5.2　IT 環境セキュリティ要件解説

項　目	PP 記述	解　　説
FIA_UID.1.1 識別のタイミング	(6)	本要件は、識別を受けるまでは電子署名認証システムの使用をアプリケーションが許可しないことに関するものである。 [割付:TSF 調停アクションのリスト]には、識別前に許可する操作を電子署名管理システム(アプリケーション)の仕様に応じて示す。
FIA_UAU.1.1[2] 認証のタイミング	(7)	本要件は、認証を受けるまでは電子署名認証システムの使用をアプリケーションが許可しないことに関するものである。 [割付:TSF 調停アクションのリスト]には、認証前に許可する操作を電子署名管理システム(アプリケーション)の仕様に応じて示す。
FIA_UAU.7 保護された認証フィードバック	なし	本要件は、認証情報の入力から判断の間に、認証に関するフィードバックとしてどのような情報を与えるかを定義するものである。IT 環境セキュリティ要件としては、OS やアプリケーション・プログラムが行うユーザ ID とパスワードによる利用者認証の際の認証情報（パスワード）入力時にダミー文字（“＊”等）を表示する等の適用が考えられる。ただし、利用者認証の方法としては他にも生体認証などがあり、その場合の「認証フィードバック」については確定した見方は定着していないと考えられる。このため本要件は PP には含めていないが、利用者認証の実装により、可能であれば本要件を ST に含めることがセキュリティ評価の観点から自然である。特に、ユーザ ID／パスワードによる認証のみを想定するのであれば、本要件は ST において採用すべきである。
FIA_AFL.1 認証失敗の扱い	なし	本要件は、IT 環境セキュリティ要件としては、OS やアプリケーション・プログラムが行うユーザ ID とパスワードによる利用者認証に適用することが考えられる。ただし、利用者認証の方法は他にも生体認証などがあり、その場合には本要件は適用できないので PP には含めていない。利用者認証の実装により、可能であれば本要件を ST に含めることがセキュリティ評価の観点から自然である。特に、ユーザ ID／パスワードによる認証のみを想定するのであれば、本要件は ST において採用すべきである。
FIA_SOS.1 秘密の認証	なし	本要件は、IT 環境セキュリティ要件としては、OS やアプリケーション・プログラムが行うユーザ ID とパスワードによる利用者認証に適用することが考えられる。典型的には、パスワードに利用できる文字列の条件を定め、容易に推測できるものは登録させないような実装が想定される。ただし、利用者認証の方法は他にも生体認証などがあり、その場合には本要件は適用できないので PP には含めていない。利用者認証の実装により、可能であれば本要件を ST に含めることがセキュリティ評価の観点から自然である。

項　目	PP記述	解　　説
FMT_MOF.1 セキュリティ機能のふるまいの管理	(8)	本要件は、システム管理者のみが管理機能を使用できるためのものである。 [割付:機能のリスト]には、電子署名管理システムのセットアップと設定、監査ログの操作、秘密鍵の操作、証明書の操作等が想定される。なお、電子署名管理システムの仕様により機能は大きく異なることから、実装内容に応じて定義すること。 [許可された識別された役割]には、電子署名管理システムを使用する許可者（システム管理者、署名検証者、秘密鍵所有者）が該当するが、実装内容に応じて定義すること。
FAU_GEN.1 監査データの生成	(9)	本要件は、監査ログの記録に関するものである。 [選択:最小、基本、詳細、指定なし]により、監査のレベルを決定する。 [割付:上記以外の個別に定義した監査対象事象]には、一部のセキュリティ機能要件に対して、本機能要件で選択した監査レベルと異なる監査レベルを採用する場合、該当するセキュリティ機能要件の監査イベントを示す。また、電子署名管理システムの仕様に応じて監査対象イベントを示す。 [割付:その他の監査関連情報]には、上記の割付操作に応じて、そのログ情報を示す。
FPT_STM.1 高信頼タイムスタンプ	(10)	本要件は、監査ログの順序性等を確認するための時間情報に関するものである。
FAU_SAA.1 侵害可能性の分析	なし	本要件は、監査事象をモニタするツールで、侵害可能性がある場合のツールによる自動応答等を求めるものである。このような機能をアプリケーションが持っている場合には、ST において採用すべきである。
FAU_SAR.1 監査レビュー	(11)	本要件は、監査ログのレビューにより、ログの追跡を可能とするためのものである。 ［割付:許可利用者］には、電子署名管理システムを使用する許可者（システム管理者、署名検証者、秘密鍵所有者）を指定する。 ［割付:監査情報のリスト］には、FAU_GEN.1 で規定される監査情報を指定する。
FAU_SAR.2 監査レビューの制限	なし	OE.ACCESS により監査ログファイルを保護することにより FAU_SAR.2 の要件も満たされるので、本要件は PP に含めていない。実装上、監査ログ内に公開不可の情報も記録される場合には、本要件を ST に含めることも検討すべきである。
FAU_SAR.3 監査レビューの選択	なし	本要件は、監査データの検索、分類あるいは並べ替えをする能力を要求するものである。この能力の有無は多様な実装に依存すると思われるため、本 PP には含めていない。実装がなされていれば、セキュリティ評価の観点から、本要件を ST に含めることを推奨する。OS が持つファイル名やファイル内容による監査データの検索、分類を、本要件の実装とすることもできる。

項　目	PP記述	解　　説
FAU_SEL1 監査データの選択	なし	本要件は、監査対象の事象を選択する機能を要求するものである。この機能の有無は実装に依存するため、本 PP には含めていない。実装がなされていれば、セキュリティ評価の観点から、本要件を ST に含めることを推奨する。
FAU_STG.1 保護された監査証跡格納	(12)	本要件は、監査ログの削除からの保護に関するものである。 ［選択: 防止、検出］では、監査ログの改変を防止するのか、検出するのかを選択する。
FAU_STG.3 監査データ損失の恐れ発生時のアクション	なし	監査データが満杯に近いか満杯になった場合の対応として、これらの要件（満杯が近づいたときの警告メッセージ、満杯になった際のログの上書き等）の一方を実装することがあるので、本 PP には含めていない。IT 環境の実装が想定できる場合には、これらの要件のうち該当するものを ST に含めることを推奨する。
FAU_STG.4 監査データ損失の防止	なし	
FMT_MTD.1 TSF データの管理	(13)	本要件は、TSF データの管理はシステム管理者に限定するためのものである。 ［割付：TSF データのリスト］には、監査ログ情報、動作環境定義ファイル（セキュリティ属性を除く）などを指定する。必要最低限としては「監査ログ」である。個々のセキュリティ機能要件の管理要件にしたがい管理対象の TSF データを示す。 関連して、「認証情報」と「秘密鍵」は本 PP ではセキュリティ属性としており、その管理には後出の FMT_MSA.1 を適用する。 [割付:許可された識別された役割]には、電子署名管理システムを使用する許可者（通常はシステム管理者）を指定する。
FDP_ACC.1 サブセットアクセス制御	(14)	本要件は、保護資源に対するアクセス制御方針と対象を明確にするためのものである。 [割付:アクセス制御 SFP]には、電子署名管理システムのアクセス制御方針名を示す。アクセス制御方針とは、下記で割付ける「サブジェクトとオブジェクトと操作のリスト」を実施する方針に対してつけられる名称である。電子署名管理システムに複数のアクセス制御方針がある場合には、該当する方針名を明示する。 [割付:サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト]の内容は、次のようなものになる。システムの構成等に基づいて明確にする。 - サブジェクト：電子署名管理システムを使用する許可者（システム管理者、署名検証者、秘密鍵所有者）。 - オブジェクト：電子署名管理システムに関与する全ての資源。 - 操作のリスト：読み取り、書き込み、実行。

項　目	PP記述	解　　説
FDP_ACF.1 セキュリティ属性によるアクセス制御	(15)	本要件は、保護資源に対するアクセス制御を機能させるためのものである。 [割付:アクセス制御 SFP]には、電子署名管理システムのアクセス制御方針名を示す。 [割付:セキュリティ属性、名前付けされたセキュリティ属性のグループ]には、次の事項を指定する。 - 電子署名管理システムを使用する許可者（システム管理者、署名検証者、秘密鍵所有者）のユーザ ID。 - 資源格納域の許可（読み取り権、書き込み権、実行権）。 - 資源の許可（読み取り権、書き込み権、実行権）。 [割付:制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]については、電子署名管理システムに関与する全ての資源は、OS または電子署名管理システムのアクセス制御リスト又は同等の定義情報によって制御されると想定されるので、その規則を示す。通常、利用者のユーザ ID と許可の論理条件により、アクセスが許可または拒否される。ユーザ ID が許可者でない場合は、いずれの権限も行使できない。 [割付:セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則]は、上述のアクセス制御の条件に関係なく指定ユーザの指定資源へのアクセスを許可するものであり、通常は存在しない。電子署名管理システムの仕様により存在する場合には、その規則を示す。 [割付:セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]は、上述のアクセス制御の条件に関係なく指定ユーザの指定資源へのアクセスを拒否するものであり、通常は存在しない。電子署名管理システムの仕様により存在する場合には、その規則を示す。
FMT_MSA.1 セキュリティ属性の管理	(16)	本要件(4 項目)は、セキュリティ属性の管理に関するためのものである。 [割付:アクセス制御 SFP 、情報フロー制御 SFP]には、電子署名管理システムが制御するアクセス制御に関するセキュリティ機能を示す方針名を示す。 [割付:その他の操作]には、電子署名管理システムの仕様に応じてその他の操作を示す。 [割付:セキュリティ属性のリスト]には、本 PP で採用する個々のセキュリティ機能要件の管理要件にしたがって管理対象のセキュリティ属性を示す。必要最低限のセキュリティ属性としては「認証情報」と「秘密鍵」がある。 これらの要件は通常は OS の機能で対応する。ただし、OS により十分な機能を持つものと持たないものがあるので注意が必要である。一般に、UNIX 系の OS は対応機能がある。また、Microsoft 社の Windows では、Windows NT、Windows 2000 とその後継 OS は対応機能があり、Windows 98 や Windows Me にはない。ベンダーは、利用者に OS 選択の指針を示す必要がある。 [割付:許可された識別された役割]には、システム管理者を指定する。

6 メンバーリスト

事務局

紙田　政典　　電子商取引推進協議会　主席研究員
米倉　早織　　電子商取引推進協議会　主席研究員
前田　陽二　　電子商取引推進協議会　主席研究員

顧問

岩下　直行　　日本銀行

リーダー

山下　　真　　富士通株式会社
手塚　　悟　　株式会社日立製作所
佐伯　正夫　　三菱電機株式会社
小松　文子　　日本電気株式会社

ＴＦ1／2 メンバー（編集メンバー）

氏名	会社名
萩原　利彦	ＮＴＴコミュニケーションズ株式会社
立石　広治	株式会社ＮＴＴデータ
鈴木　優一	エントラストジャパン株式会社
川白　弘人	日本電気株式会社
今枝　直彦	日本電信電話株式会社
洲崎　誠一	株式会社日立製作所
笈川　光浩	株式会社日立製作所
村上　　哲	富士通株式会社
麻井　芳文	株式会社富士通北陸システムズ
西山　恵二	株式会社富士通北陸システムズ
宗像　昌朗	富士電機株式会社
桜井　俊一	三菱電機ｲﾝﾌｫﾒｰｼｮﾝｼｽﾃﾑｽﾞ株式会社

SWG1 メンバー（参加メンバー）

氏名	会社名
岸本　輝昭	電子商取引安全技術研究組合
森田　純生	株式会社イーアイティー
杉山　善広	株式会社エヌジェーケー
熊木　克巳	株式会社エヌジェーケー
丹羽　圭二	株式会社エヌジェーケー
中村　逸一	株式会社ＮＴＴデータ
二村　朝康	株式会社ＮＴＴデータ
河田　悦生	ＮＴＴドコモ株式会社
関野　公彦	ＮＴＴドコモ株式会社
杉本　則高	株式会社ＦＦＣ
上甲　　徹	沖電気工業株式会社
保倉　　豊	グローバルフレンドシップ株式会社
高橋　正嗣	グローバルフォーカス株式会社
鈴木　良信	コンピュータ・アソシエイツ株式会社
森　　宣彦	コンピュータ・アソシエイツ株式会社
木下　　剛	株式会社ＵＦＪ銀行
信濃　義朗	昌栄印刷株式会社
久保田　仁志	株式会社シー・アイ・シー
伊藤　　昇	情報処理振興事業協会
正木　淳雄	株式会社ソリトンシステムズ
星野　　理	株式会社帝国データバンク
西川　和比古	株式会社ＵＦＪ銀行
長澤　高史	東京海上火災保険株式会社
能勢　健一朗	株式会社東芝
西岡　誠治	財団法人日本建設情報総合センター
砂川　隆行	日本コムシス株式会社
小野　千秋	株式会社日本システムディベロップメント
浜岡　周作	日本信販株式会社
西本　浩文	日本電子計算株式会社
町田　　陽	日本認証サービス株式会社
本間　史夫	日本認証サービス株式会社
姫崎　光昭	日本ベリサイン株式会社
高橋　正一	日本ボルチモアテクノロジーズ株式会社
玉山　　恭	株式会社日立情報システムズ
高山　聡一郎	株式会社日立製作所
及川　卓也	マイクロソフト　プロダクト　ディベロップメント　リミテッド

平成14年3月発行
発行：電子商取引推進協議会
東京都港区芝公園3－5－8
機械振興会館3階
Tel　03-3436-7500
E-mail　info@ecom.jp

第２部　電子署名プログラム

Ｐｒｏｔｅｃｔｉｏｎ Ｐｒｏｆｉｌｅ

2002 年　3 月 22 日

第 1.2 版

電子商取引推進協議会

履歴

版数	作成・更新日	変更履歴	作成・更新者
第 1.0 版	2002/1/31	初版	電子商取引推進協議会
第 1.1 版	2002/3/15	評価版	電子商取引推進協議会
第 1.2 版	2002/3/22	評価済発行版	電子商取引推進協議会

目　次

1 ＰＰ概説

本ＰＰでは、保証レベルとして「ＥＡＬ２追加、ＥＡＬ３追加、ＥＡＬ４」を想定し、保証レベルによって記述が異なる部分は、場合わけをして記述する。（1.1、および5.3）

1.1 ＰＰ識別

① 「保証レベル：ＥＡＬ２追加」の場合

名称：電子署名プログラム　Protection Profile
バージョン：V1.2
作成日：2002 年 3 月 22 日
作成者：電子商取引推進協議会
保証レベル：ＥＡＬ２追加

② 「保証レベル：ＥＡＬ３追加」の場合

名称：電子署名プログラム　Protection Profile
バージョン：V1.2
作成日：2002 年 3 月 22 日
作成者：電子商取引推進協議会
保証レベル：ＥＡＬ３追加

③ 「保証レベル：ＥＡＬ４」の場合

名称：電子署名プログラム　Protection Profile
バージョン：V1.2
作成日：2002 年 3 月 22 日
作成者：電子商取引推進協議会
保証レベル：ＥＡＬ４

1.2 ＰＰ概要

本 PP は、電子署名プログラムを TOE として記述する。電子署名プログラムは電子署名管理アプリケーションの一部分であり、電子署名の生成、検証、管理において、最も重要な以下の機能で構成されている。

- 秘密鍵と証明書の管理を実施する管理機能
- 電子署名を生成する電子署名生成機能
- 電子署名を検証する電子署名検証機能

上記以外の機能に関しては、OS やアプリケーションを含む IT 環境によって提供されることを想定している。したがって、本 PP を利用する ST 作成者は、これらを十分に考慮して ST を作成しなければならない。

1.3 ISO/IEC 15408 への適合

本ＰＰは以下の規格に適合している。

- ISO/IEC 15408, Information Technology - Security techniques - Evaluation criteria for IT security - Part1, 99/12
- ISO/IEC 15408, Information Technology - Security techniques - Evaluation criteria for IT security – Part2, 99/12
- ISO/IEC 15408, Information Technology - Security techniques - Evaluation criteria for IT security - Part3, 99/12

1.4 参考資料

- Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031
- Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032
- Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033
- JIS X 5070-1:2000 セキュリティ技術－情報技術セキュリティの評価基準－第１ 部：総則及び一般モデル
- JIS X 5070-2:2000 セキュリティ技術－情報技術セキュリティの評価基準－第２ 部：セキュリティ機能要件
- JIS X 5070-3:2000 セキュリティ技術－情報技術セキュリティの評価基準－第３ 部：セキュリティ保証要件
- 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 パート 1 ： 概説と一般モデル バージョン 2.1 1999 年 8 月 CCIMB-99-031
- 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 パート 2 ： セキュリティ機能要件バージョン 2.1 1999 年 8 月 CCIMB-99-032
- 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 パート 3 ： セキュリティ保証要件バージョン 2.1 1999 年 8 月 CCIMB-99-033
- 電子署名プログラム Protection Profile 第１部 ： 電子署名プログラム Protection Profile 解説 2002 年 3 月 電子商取引推進協議会

1.5 電子署名プログラム ＰＰ用語定義

<略語>

EE ：End Entity の略語であり、個人や組織を示す。

<用語>

電子署名 ：電子文書について発信者を証明する情報を付加したデータ。

秘密鍵 ：公開鍵暗号を用いた署名において電子署名を生成する者が保持する署名生成に用いるデータ。対応する鍵として公開鍵があり、電子署名を検証する際に用いられる。

認証局 ：個人または組織について識別情報と公開鍵が対応することを認証する組織。

証明書 ：認証局が発行するデータであり、個人または組織について識別情報と公開鍵が対応していることを示す情報を含む。

EE 証明書 ：個人や組織に対する証明書。

認証局証明書：電子署名の検証において証明書を信頼するかどうか判断する際の基準点として用いる証明書。

2 TOE 記述

2.1 TOE の種別

本 PP が対象とする TOE は「電子署名プログラム」である。電子署名プログラムは、電子署名を扱うアプリケーションまたはシステムを構成する主要プログラムとして、以下の動作を行う。

- 電子署名の生成で必要な秘密鍵の生成、管理及び電子署名の生成
- 電子署名の検証で必要な証明書の管理及び電子署名の検証

2.2 TOE の基本機能

本 PP の TOE である電子署名プログラムは、以下の機能から構成される。

- 鍵管理機能
- 認証局証明書管理機能
- EE 証明書管理機能
- 署名生成機能
- 署名検証機能

なお、本 PP における TOE では、電子署名管理システムの外部で作成された秘密鍵を電子署名プログラム内にインポートする機能は含まない。

2.2.1 鍵管理機能

鍵管理機能は、電子署名を利用する際に必要となる秘密鍵情報を管理する。管理対象とする秘密鍵を以下に示す。

- 電子署名プログラム内で生成した秘密鍵

上記の管理対象に対し、鍵管理機能は以下の操作を行う。

- 秘密鍵の生成
- 秘密鍵の廃棄
- 秘密鍵利用時の認証

2.2.2 認証局証明書管理機能

認証局証明書管理機能は、電子署名を利用する際に必要となる認証局証明書を管理する。具体的には、認証局証明書に対して登録と削除の操作を行う。

2.2.3 EE 証明書管理機能

EE 証明書管理機能は、電子署名を利用する際に必要となる EE 証明書を管理する。具体的には、外部で作成された EE 証明書に対して以下の操作を行う。

- EE 証明書の登録
- EE 証明書の削除
- EE 証明書の要求

2.2.4 署名生成機能

署名生成機能は、電子署名を生成する機能である。

2.2.5 署名検証機能

署名検証機能は、電子文書に付加された電子署名を検証する機能である。

2.3 TOE の利用形態

電子署名プログラムは単体では利用されず、電子署名プログラム自身の機能と関連する情報の管理及び操作を補完する機能を組み合わせたアプリケーションまたはシステムとして利用されることを想定している。

図 2-1.に、アプリケーションまたはシステム内における TOE の位置付けを示す。

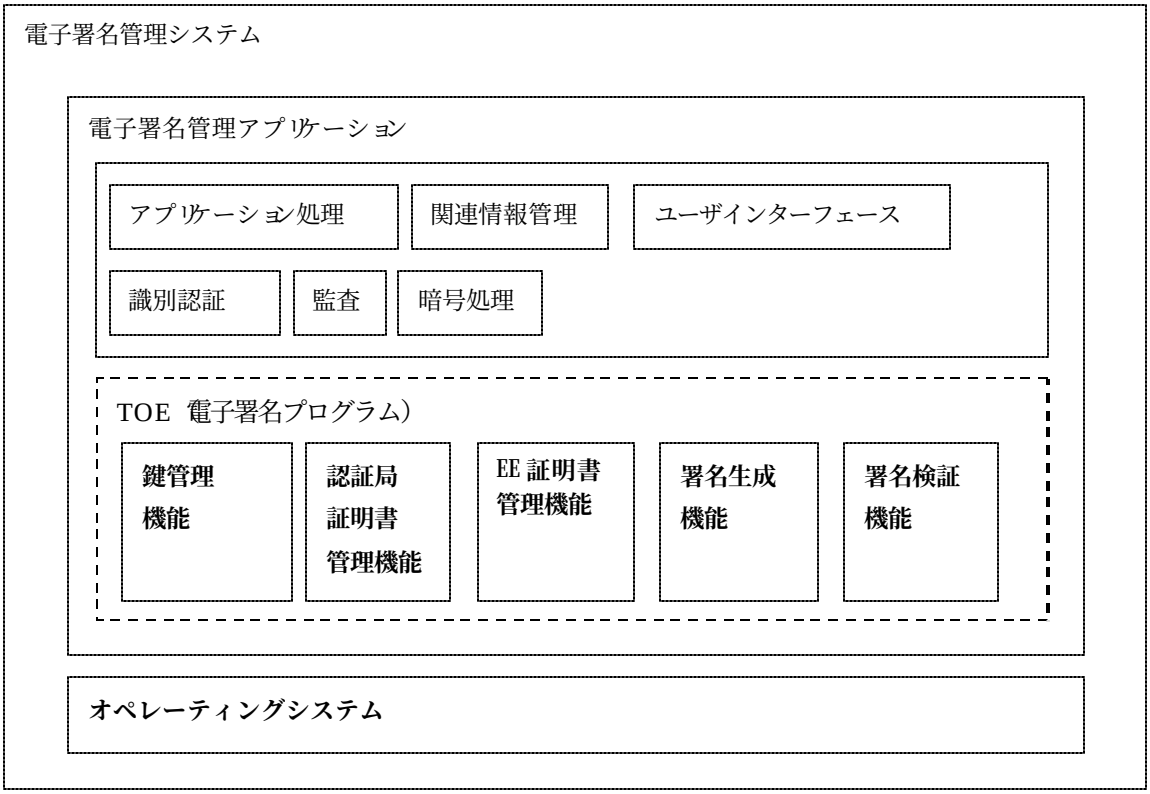

図 2-1アプリケーションまたはシステム内におけるTOE の位置付け

以降の文中では、電子署名プログラムを含む電子署名管理アプリケーションまたは電子署名管理システムを、総じて電子署名管理システムと表す。

2.4 電子署名管理システムにおける保護対象資源

電子署名管理システムでは、以下の資源を保護対象とする。

- 秘密鍵
- 認証情報（電子署名管理システムが電子署名プログラムの利用者に対して識別認証を実施する際に使用する認証情報、及び、秘密鍵を利用する秘密鍵所有者に対して認証を実施する際に使用する認証情報）
- 認証局証明書
- 監査ログ
- 電子署名プログラム自身

2.5 TOE 利用時のモデルケース

電子署名管理システムを利用する場合のモデルケースを以下に記述する。

2.5.1 電子署名管理システムをとりまく人物

電子署名管理システムを使用する許可者として、以下の利用者が想定される。

- システム管理者：電子署名管理システムを管理することができる者である。システム管理者は、証明書の管理、及び、署名検証者と秘密鍵所有者に関する利用者情報の管理などを行うことができる。ただし秘密鍵所有者が持つ秘密鍵を利用して電子署名を生成することはできない。個人であればシステム所有者が、企業であればシステム管理担当者などを想定することができる。
- 署名検証者　：電子署名管理システムを、電子署名の検証を行うことを目的として使用する者である。個人であればシステム所有者が、企業であれば業務担当者などを想定することができる。
- 秘密鍵所有者　：電子署名管理システムを、秘密鍵の生成と所有、及び、電子署名の生成を行うことを目的として使用する者である。個人であればシステム所有者が、企業であれば業務部門責任者などを想定することができる。

また、電子署名管理システムの使用を許可されていない非許可者には、意図的な不正行為を企てようとする不正者を含むことが想定される。

2.5.2 TOE の利用形態

電子署名管理システムの利用形態としては以下の場合が想定される。

- 個人利用
- 企業利用

以降では、個人利用と企業利用のそれぞれについて利用形態のモデルケースを記述する。
なお、文中で利用者とはシステム管理者、署名検証者、または、秘密鍵所有者を表す。

2.5.3 個人利用

電子署名管理システムを個人が利用する形態としては以下の事例が想定できる。

- 電子メールへの利用

- インターネットショッピングへの利用

電子メールに対しては、利用者は秘密鍵及び証明書を利用して以下の操作を行う。電子署名の生成時には、秘密鍵を使用するための認証を受ける必要がある。

- 電子メールに対する電子署名の生成
- 電子メールに存在する電子署名の検証

インターネットショッピングでは、利用者は秘密鍵及び証明書を利用して以下の操作を行う。電子署名の生成時には、秘密鍵を使用するための認証を受ける必要がある。

- 注文書に対する電子署名の生成
- 注文確認書に存在する電子署名の検証

上記の事例では、利用者は秘密鍵に対し以下の操作を行う。秘密鍵の廃棄時には、秘密鍵を操作するための認証を受ける必要がある。

- 秘密鍵の生成
- 秘密鍵の廃棄

また、利用者は証明書に対し以下の操作を行う。

- 証明書の登録
- 証明書の廃棄

上記で述べた操作を行う際に、利用者は電子署名管理システムを介して TOE が持つ以下の機能を利用する。

- 鍵管理機能
  秘密鍵の生成、廃棄、及び、秘密鍵の使用を前提とする電子署名の生成や秘密鍵の廃棄などの操作実施前における認証を行うために利用する。
- 認証局証明書管理機能及び EE 証明書管理機能
  電子メール及び注文確認書に存在する電子署名を検証するための証明書に対して、登録と廃棄に関する管理を実施するために利用する。
- 署名生成機能
  電子メール及び注文書に対する電子署名の生成を実施するために利用する。
- 署名検証機能
  電子メール及び注文確認書に存在する電子署名の検証を実施するために利用する。

これらの TOE が持つ機能は、電子署名管理システムが提供する識別、認証、アクセス制御機能により許可された者のみが利用できる。

2.5.4 企業利用

電子署名管理システムを企業が利用する形態としては、行政機関との間で行う申請、調達などの手続きや、企業間の電子商取引における取引、決済、契約などの事例を想定することができる。

この場合、申請、取引などを行う利用者は秘密鍵及び証明書を利用して以下の操作を行う。電子署名の生成時には、秘密鍵を使用するための認証を受ける必要がある。

- 申請に対する電子署名の生成と検証
- 応募に対する電子署名の生成と検証
- 取引情報に対する電子署名の生成と検証
- 決済情報に対する電子署名の生成と検証
- 契約書に対する電子署名の生成と検証

上記の事例では利用者は秘密鍵に対し以下の操作を行う。秘密鍵の廃棄時には、秘密鍵を操作するための認証を受ける必要がある。

- 秘密鍵の生成
- 秘密鍵の廃棄

また、利用者は証明書に対し以下の操作を行う

- 証明書の登録
- 証明書の廃棄

上記で述べた操作を行う際に、利用者は電子署名管理システムを介して TOE が持つ以下の機能を利用する。

- 鍵管理機能
  秘密鍵の生成、廃棄、及び、秘密鍵の使用を前提とする電子署名の生成や秘密鍵の廃棄などの操作実施前における認証を行うために利用する。
- 認証局証明書管理機能及び EE 証明書管理機能
  受信メール及び契約書に存在する電子署名を検証するための証明書に対して、登録と廃棄に関する管理を実施するために利用する。
- 署名生成機能
  電子メール及び契約書に対する電子署名の生成を実施するために利用する。
- 署名検証機能
  電子メール、契約書及び確認書に存在する電子署名の検証を実施するために利用する。

これらの TOE が持つ機能は、電子署名管理システムが提供する識別、認証、アクセス制御機能により許可された者のみが利用できる。

2.6 TOE の利用条件

利用形態で記述したように、秘密鍵及び証明書の管理は TOE が行う。一方、秘密鍵及び証明書以外

で保護対象となる資源に対する管理と操作の制御は、IT 環境で実施する必要がある。本 PP では、IT 環境が以下の機能を提供することを想定している。

- 電子署名管理システムを利用するための識別認証機能
- 保護対象資源の管理及び操作に関するアクセス制御機能
- セキュリティ侵害の検知及び侵害分析に必要なログを生成する監査機能
- 秘密鍵の生成及び電子署名生成時に利用する暗号処理機能

3 TOE セキュリティ環境

3.1 前提条件

3.1.1 導入、適切な状態の維持管理

ASM_INST 運用環境への導入

電子署名管理システムは、正常に導入されている。

ASM_ADMIN 運用管理

電子署名管理システムは、適切なOS のアクセス制御や正確なシステム時間が維持された安全な状態で運用され、監査ログの定期的なバックアップなどの管理行為が日常的に実施されている。

3.1.2 人的管理

ASM_USER 正当な利用者

電子署名管理システムの使用を許可されている利用者は、利用者毎に定められた権限の範囲内で電子署名管理システムを使用し、意図的な不正行為を行わない。

3.1.3 動作環境に関わる規定

ASM_TRUSTPOINT 認証局証明書

電子署名の検証を行うために TOE が管理する認証局証明書は、信頼できる認証局によって発行及び失効される。

ASM_CRYPT 暗号処理

電子署名管理システムで使用される暗号アルゴリズムの強度は保証されている。

3.1.4 証明書

ASM_CA 証明書

電子署名を生成する秘密鍵所有者の秘密鍵に対応した証明書は、信頼できる認証局によって発行及び失効される。

3.2 脅威

T.MASQUERADE システム管理者及び署名検証者へのなりすまし

不正者がシステム管理者及び署名検証者になりすまして電子署名管理システムを不正に操作することにより、証明書の不正な廃棄や電子署名への虚偽の検証を行う。

T.MASQUERADE_KEY 秘密鍵所有者へのなりすまし

不正者が秘密鍵所有者になりすまして電子署名管理システムを不正に操作することにより、虚偽の電子署名を生成したり、秘密鍵の廃棄を行う。

T.AUDITLOG 監査ログへの不正な加工

不正者が監査ログファイルに対して改ざんや削除などの不正な加工を施すことにより、電子署名管理システムを操作した記録を事後分析できないようにする。

T. PRIVATEKEY 秘密鍵の不正利用

不正者が認証情報や秘密鍵の所在を探し出し秘密鍵を奪取することにより、秘密鍵の暴露や破壊、不正使用などの行為を行う。

T.TRUSTPOINT 認証局証明書の改変、破壊

不正者が認証局証明書の所在を探し出し、認証局証明書の改ざんや破壊などの不正行為を行う。

T.MIS-OPERATION 誤操作

電子署名管理システムの使用許可者が、電子署名管理システムの操作時に不注意などから誤操作を施してしまうことにより、意図しない電子署名の生成や検証、秘密鍵の廃棄を行う。

3.3 組織のセキュリティ方針

本ＰＰで想定される組織のセキュリティ方針は存在しない。

4 セキュリティ対策方針

4.1 TOE のセキュリティ対策方針

O.SEC_KEY 認証情報や秘密鍵の保護

TOE は、秘密鍵使用時の認証情報、及び、秘密鍵を秘匿にすることで、不正者が秘密鍵使用時の認証情報、及び、秘密鍵の所在を探し出し、不正な行為を行うことを防止する。

O.DEL_KEY 秘密鍵の抹消

TOE は、秘密鍵の使用を前提とした操作実施後に残存する秘密鍵を抹消し、不正者による秘密鍵の奪取を防止する。

O.CTL_KEY 秘密鍵の管理

TOE は、秘密鍵を安全に管理し、生成、廃棄に対する操作を行う。

O.AUTH_KEY 秘密鍵使用時の認証

TOE は、秘密鍵を使用する秘密鍵所有者に対して、正当性を確認するために認証を行う。

4.2 環境セキュリティ対策方針

OE.ID_AUTH 利用者の識別と認証

電子署名プログラムの使用を許可された利用者に対して、電子署名管理システムは許可者であることの正当性を確認するために識別し及び認証を実施する。

OE.ADMIN 機能管理

電子署名管理システムは、許可された利用者のみがセキュリティに関する機能の管理行為を実施できるようにすることで、不正者によるシステム破壊や虚偽の電子署名検証などを防止する。

OE.AUDIT_LOG 監査ログの記録

電子署名管理システムは、セキュリティ侵害を監査ログとして記録し、電子署名プログラム、認証局証明書、認証情報、秘密鍵に対して施された不正行為や誤操作の事後分析を可能とする。

OE.LOG_SEARCH 追跡機能

電子署名管理システムは、記録した監査ログを追跡するための機能を提供し、電子署名プログラム、認証局証明書、認証情報、秘密鍵に対して施された不正行為や誤操作の事後分析を可能とする。

OE.ACCESS 保護資源へのアクセス制限

電子署名管理システムは、保護資源へのアクセス制限を行うことで、不正者により電子署名プログラムが不正に操作されることを防止し、更に、監査ログの改ざんや削除、認証局証明書、認証情報、秘密鍵の奪取や破壊などの不正行為も防止する。

OE.UI　ユーザインターフェース

電子署名管理システムは、アプリケーションプログラムとしての操作をシンプルにし、電子署名の生成や秘密鍵の廃棄などの重要な操作意思を確認するユーザインターフェースを提供することで、不注意による誤操作を防止する。

OE.TRUST 教育、啓蒙

電子署名管理システムの使用を許可された利用者には情報セキュリティに関する注意、啓蒙を行うための手順書が提供され、セキュリティ事故の発生を防止する。

OE.BACKUP *バックアップ*

電子署名管理システムは、最低限監査ログを安全な形式でバックアップ／リストアすることで、不正者が監査ログファイルに対して改ざんや削除などの不正な加工を施した状態から元の状態への復元を可能とする。

OE.INSTALL 導入及び管理

電子署名管理システムの使用を許可された利用者には、電子署名管理システムを安全に導入するための手順書、及び、安全な運用を維持するための継続的な管理行為について定めた手順書が提供され、情報セキュリティ事故の発生を防止する。

OE.TRUST_CA 証明書

電子署名プログラムで取り扱う証明書は、利用者が正しい手続き処理を遂行することで、信頼できる認証局より発行及び失効される。

OE.CRYPT 暗号処理

電子署名プログラムで使用される暗号アルゴリズムは、アルゴリズムの信頼性や鍵長などの品質尺度を十分に吟味した上で採用することにより、情報の漏洩、改ざんを防ぐ。

OE.TIME 時間管理

電子署名管理システムは、厳密な時間管理を行うことで虚偽の電子署名生成時刻付与、証明書が有効でない時刻での不正な電子署名生成、及び、不当な電子署名の検証結果出力を防止する。

5 IT セキュリティ要件

5.1 TOE セキュリティ要件

（1）FCS_COP 暗号操作

FCS_COP.1 Cryptographic operation
暗号操作

Management:

None

Audit:

Minimal: Success and failure, and the type of cryptographic operation.

最小：成功と失敗及び暗号操作の種別。

Basic : Any applicable cryptographic mode(s) of operation,subject attributes and object attributes.

基本：すべての適用可能な暗号操作のモード、サブジェクト属性、オブジェクト属性。

――

FCS_COP.1.1

The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment:*cryptographic algorithm*] and cryptographic key sizes [assignment:*cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

TSFは、［割付：標準のリスト］に合致する、特定された暗号アルゴリズム［割付：暗号アルゴリズム］と暗号鍵長［割付：暗号鍵長］に従って、［割付：暗号操作のリスト］を実行しなければならない。

（2）FDP_RIP　残存情報保護

FDP_RIP.1 Subset residual information protection
サブセット残存情報保護

Management:

The choice of when to perform residual information protection (i.e. upon allocation or deallocation) could be made configurable within the TOE.

いつ残存情報保護を実施するかの選択（すなわち、割当てあるいは割当て解除において）が、TOEにおいて設定可能にされる。

Audit:

None

FDP_RIP.1.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to*, *deallocation of the resource from*] the following objects: [assignment: *list of objects*].

TSFは、以下のオブジェクト［選択：への資源の割り当て、からの資源の割り当て解除］において、資源の以前のどの情報の内容も利用できなくする事を保証しなければならない：［割付：オブジェクトのリスト］。

（3）FCS_CKM 暗号鍵管理

FCS_CKM.1 Cryptographic key generation
暗号鍵生成

Management:

the management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption).

暗号鍵属性の変更の管理。鍵の属性の例としては、鍵種別（例えば、公開、秘密、共通）、有効期間、用途（例えば、ディジタル署名、鍵暗号化、鍵交換、データ暗号化）などがある。

Audit:

Minimal: Success and failure of the activity.

最小：動作の成功と失敗。

Basic : The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).

基本：オブジェクト属性及び機密情報（例えば共通あるいは秘密鍵）を除くオブジェクトの値。

FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment:*cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

TSFは、以下の［割付：標準のリスト］に合致する、指定された暗号鍵生成アルゴリズム［割付：暗号鍵生成アルゴリズム］と指定された暗号鍵長［割付：暗号鍵長］に従って、暗号鍵を生成しなければならない。

（4）FCS_CKM 暗号鍵管理

FCS_CKM.4 Cryptographic key destruction
暗号鍵破棄

Management:

the management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption).

暗号鍵属性の変更の管理。鍵の属性の例としては、鍵種別（例えば、公開、秘密、共通）、有効期間、用途（例えば、ディジタル署名、鍵暗号化、鍵交換、データ暗号化）などがある。

Audit:

Minimal: Success and failure of the activity.

最小：動作の成功と失敗。

Basic : The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).

基本：オブジェクト属性及び機密情報（例えば共通あるいは秘密鍵）を除くオブジェクトの値。

FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

ＴＳＦは、以下の［割付：標準のリスト］に合致する、指定された暗号鍵破棄方法［割付：暗号鍵破棄方法］に従って、暗号鍵を破棄しなければならない。

（5）FIA_UAU 利用者認証

FIA_UAU.1[1] Timing of authentication
認証のタイミング

Management:

a) management of the authentication data by an administrator;
管理者による認証データの管理;

b) management of the authentication data by the associated user;
関係する利用者による認証データの管理；

c) managing the list of actions that can be taken before the user is authenticated.
利用者が認証される前にとられるアクションのリストを管理すること。

Audit:

Minimal: Unsuccessful use of the authentication mechanism;
最小: 認証メカニズムの不成功になった使用；

Basic : All use of the authentication mechanism;
基本: 認証メカニズムのすべての使用；

Detailed : All TSF mediated actions performed before authentication of the user.
詳細: 利用者認証以前に行われたすべてのTSF調停アクション。

FIA_UAU.1.1[1]

The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.
TSFは、利用者が認証される前に利用者を代行して行われる[割付:TSF調停アクションのリスト]を許可しなければならない。

FIA_UAU.1.2[1]

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
TSFは、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

5.2 IT 環境セキュリティ要件

（6）FIA_UID 利用者識別

FIA_UID.1 Timing of identification
識別のタイミング

Management:

a) the management of the user identities;

利用者識別情報の管理；

b) if an authorized administrator can change the actions allowed before identification, the managing of the action lists.

許可管理者が、識別前に許可されるアクションを変更できる場合、そのアクションリストを管理すること。

Audit:

Minimal: Unsuccessful use of the user identification mechanism,including the user identity provided;

最小：提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用；

Basic : All use of the user identification mechanism, including the user identify provided.

基本：提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用。

FIA_UID.1.1

The TSF shall allow [assignment: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified.

TSFは、利用者が識別される前に利用者を代行して実行される[割付:TSF調停アクションのリスト]を許可しなければならない。

FIA_UID.1.2

The TSF shall require each user to be succesfully identified before allowing any other TSF-mediated actions on behalf of that user.

TSFは、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。

（7）FIA_UAU 利用者認証

FIA_UAU.1[2] Timing of authentication
認証のタイミング

Management:

a) management of the authentication data by an administrator;
管理者による認証データの管理;

b) management of the authentication data by the associated user;
関係する利用者による認証データの管理；

c) managing the list of actions that can be taken before the user is authenticated.
利用者が認証される前にとられるアクションのリストを管理すること。

Audit:

Minimal: Unsuccessful use of the authentication mechanism;
最小: 認証メカニズムの不成功になった使用;

Basic : All use of the authentication mechanism;
基本: 認証メカニズムのすべての使用；

Detailed : All TSF mediated actions performed before authentication of the user.
詳細: 利用者認証以前に行われたすべてのTSF調停アクション。

FIA_UAU.1.1[2]

The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.
TSFは、利用者が認証される前に利用者を代行して行われる[割付:TSF調停アクションのリスト]を許可しなければならない。

FIA_UAU.1.2[2]

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
TSFは、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

（8）FMT_MOF TSFにおける機能の管理

FMT_MOF.1 Management of security functions behaviour
セキュリティ機能のふるまいの管理

Management:

managing the group of roles that can interact with the functions in the TSF;

TSFの機能と相互に影響を及ぼし得る役割のグループを管理すること;

Audit:

Basic : All modifications in the behaviour of the functions in the TSF.

基本：TSFの機能のふるまいにおけるすべての改変。

FMT_MOF.1.1

The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: *the authorised identified roles*].

TSFは、機能[割付:機能のリスト][選択:のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する]能力を[割付:許可された識別された役割]に制限しなければならない。

（9）FAU_GEN セキュリティ監査データの生成

FAU_GEN.1 Audit data generation
監査データの生成

Management:

None

Audit:

None

FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [selection: *minimum, basic, detailed, not specified*] level of audit; and

c) [assignment: *other specifically defined auditable events*].

TSF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:

a) 監査機能の起動と終了;

b) 監査の[選択:最小、基本、詳細、指定なし]レベルのすべての監査対象事象;及び

c) [割付:上記以外の個別に定義した監査対象事象]。

FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*]

TSFは、各監査記録において少なくとも以下の情報を記録しなければならない:

a) 事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果(成功または失敗敗); 及び

b) 各監査事象種別に対して、PP/STの機能コンポーネントの監査対象事象の定義に基づいた、[割付:その他の監査関連情報]

（１０）FPT_STM　タイムスタンプ

FPT_STM.1 Reliable time stamps
高信頼タイムスタンプ

Management:

Management of the time.
時間の管理。

Audit:

Minimal: changes to the time;
最小: 時間の変更;

Detailed : providing a timestamp.
詳細: タイムスタンプの提供。

FPT_STM.1.1

The TSF shall be able to provide reliable time stamps for its own use.
TSFは、それ自身の使用のために、高信頼タイムスタンプを提供できなければならない。

（１１）FAU_SAR　セキュリティ監査レビュー

FAU_SAR.1　Audit review
監査レビュー

Management:

maintenance (deletion, modification, addition) of the group of users with read access right to the audit records.
監査記録に対して読み出し権のある利用者グループの維持（削除、改変、追加）。

Audit:

Basic　: Reading of information from the audit records.
基本：監査記録からの情報の読み出し。

――

FAU_SAR.1.1

The TSF shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of audit information*] from the audit records.
TSFは、［割付:許可利用者］が、［割付:監査情報のリスト］を監査記録から読み出せるようにしなければならない。

――

FAU_SAR.1.2

The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
TSFは、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない。

（１２）FAU_STG　セキュリティ監査事象の格納

FAU_STG.1 Protected audit trail storage
保護された監査証跡格納

Management:

None

Audit:

None

FAU_STG.1.1

The TSF shall protect the stored audit records from unauthorised deletion.
TSFは、格納された監査記録を不正な削除から保護しなければならない。

FAU_STG.1.2

The TSF shall be able to [selection: *prevent, detect*] modifications to the audit records.
TSFは、監査記録の改変を［選択: 防止、検出］できねばならない。

（１３）FMT_MTD　TSFデータの管理

FMT_MTD.1 Management of TSF data
TSFデータの管理

Management:

managing the group of roles that can interact with the TSF data.
TSFデータと相互に影響を及ぼし得る役割のグループを管理すること。

Audit:

Basic　: All modifications to the values of TSF data.
基本：TSFデータの値のすべての改変。

FMT_MTD.1.1

The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].

TSFは、[割付:TSFデータのリスト]を[選択:デフォルト値変更、問い合わせ、改変、削除、消去、[割付:その他の操作]]する能力を[割付:許可された識別された役割]に制限しなければならない。

（１４）FDP_ACC　アクセス制御方針

FDP_ACC.1 Subset access control
サブセットアクセス制御

Management:

None

Audit:

None

FDP_ACC.1.1

The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].

TSFは、[割付:サブジェクト、オブジェクト、及びSFP で扱われるサブジェクトとオブジェクト間の操作のリスト]に対して[割付:アクセス制御SFP]を実施しなければならない。

（１５）FDP_ACF　アクセス制御機能

FDP_ACF.1 Security attribute based access control
セキュリティ属性によるアクセス制御

Management:

Managing the attributes used to make explicit access or denial based decisions.
明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。

Audit:

Minimal: Successful requests to perform an operation on an object covered by the SFP.
最小: SFP**で扱われるオブジェクトに対する操作の実行における成功した要求。**

Basic : All requests to perform an operation on an object covered by the SFP.
基本: SFP**で扱われるオブジェクトに対する操作の実行におけるすべての要求。**

Detailed : The specific security attributes used in making an access check.
詳細: **アクセスチェック時に用いられる特定のセキュリティ属性。**

――

FDP_ACF.1.1

The TSF shall enforce the [assignment: *access control SFP*] to objects based on [assignment: *security attributes, named groups of security attributes*].
TSF**は、[割付:セキュリティ属性、名前付けされたセキュリティ属性のグループ]に基づいて、オブジェクトに対して、[割付:アクセス制御**SFP**]を実施しなければならない。**

――

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].
TSF**は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうか決定するために、次の規則を実施しなければならない: [割付:制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]。**

FDP_ACF.1.3

The TSF shall explicitly authorise access of subjects to obje cts based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

TSFは、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない: [割付:セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則]。

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

TSFは、[割付:セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

（１６）FMT_MSA　セキュリティ属性の管理

FMT_MSA.1 Management of security attributes
セキュリティ属性の管理

Management:

a) managing the group of roles that can interact with the security attributes.
セキュリティ属性と相互に影響を及ぼし得る役割のグループを管理すること。

Audit:

Basic　: All modifications of the values of security attributes.
基本: セキュリティ属性の値の改変すべて。

――

FMT_MSA.1.1

The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to restrict the ability to [selection: *change_default, query, modify, delete,* [assignment: *other operations*]] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].
TSFは、セキュリティ属性[割付:セキュリティ属性のリスト]に対し[選択: デフォルト値変更、問い合わせ、改変、削除、[割付:その他の操作] をする能力を[割付:許可された識別された役割]に制限するために[割付:アクセス制御SFP 、情報フロー制御SFP]を実施しなければならない。

（１７）FMT_MSA　セキュリティ属性の管理

FMT_MSA.2 Secure security attributes
セキュアなセキュリティ属性

Management:

None

Audit:

Minimal: All offered and rejected values for a security attribute;
最小: **セキュリティ属性に対して提示され、拒否された値すべて；**
Detailed : All offered and accepted secure values for a security attribute.
詳細: **セキュリティ属性に対して提示され、受け入れられたセキュアな値すべて。**

FMT_MSA.2.1

The TSF shall ensure that only secure values are accepted for security attributes.
TSF**は、セキュアな値だけがセキュリティ属性として受け入れられることを保証しなければならない。**

（１８）FMT_MSA　セキュリティ属性の管理

FMT_MSA.3 Static attribute initialisation
静的属性初期化

Management:

a) managing the group of roles that can specify initial values;
初期値を特定できる役割のグループを管理すること；

b) managing the permissive or restrictive setting of default values for a given access control SFP.
所定のアクセス制御ＳＦＰに対するデフォルト値の許可的あるいは制限的設定を管理すること。

Audit:

Basic : Modifications of the default setting of permissive or restrictive rules.
基本: 許可的あるいは制限的規則のデフォルト設定の改変。

Basic : All modifications of the initial values of security attributes.
基本: セキュリティ属性の初期値の改変すべて。

FMT_MSA.3.1

The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to provide [selection: *restrictive, permissive, other property*] default values for security attributes that are used to enforce the *SFP*.
TSFは、そのSFPを実施するために使われるセキュリティ属性として、[選択:制限的、許可的、その他の特性]デフォルト値を与える[割付:アクセス制御SFP、情報フロー制御SFP]を実施しなければならない。

FMT_MSA.3.2

The TSF shall allow the [assignment: *the authorised identified roles*] to specify alternative initial values to override the default values when an object or information is created.
TSFは、オブジェクトや情報が生成されるとき、[割付:許可された識別された役割]が、デフォルト値を上書きする代替の初期値を指定することを許可しなければならない。

（１９）FMT_SMR　セキュリティ管理の役割

FMT_SMR.1 Security roles
セキュリティ役割

Management:

managing the group of users that are part of a role.
役割の一部をなす利用者のグループの管理。

Audit:

Minimal: modifications to the group of users that are part of a role;
最小:役割の一部をなす利用者のグループに対する改変;

Detailed : every use of the rights of a role.
詳細:役割の権限の使用すべて。

FMT_SMR.1.1

The TSF shall maintain the roles [assignment: *the authorised identified roles*].
TSFは、役割[割付:許可された識別された役割]を維持しなければならない。

FMT_SMR.1.2

The TSF shall be able to associate users with roles.
TSFは、利用者を役割に関連づけなければならない。

5.3 セキュリティ保証要件

① 「保証レベル：ＥＡＬ２追加」の場合

TOE は、電子署名に関する情報を扱うプログラムとして、外部インターフェースと内部インターフェースを識別した設計とテストを行うことによりセキュリティ上問題なく利用できるプログラムであることを保証するＥＡＬ２とする。

追加の保証要件は ADV_SPM.1 とする。電子署名プログラムが扱う証明書及び秘密鍵情報は、個人または組織の信用情報を有するため、明確な情報管理ポリシモデルを保証する要件として追加する。

② 「保証レベル：ＥＡＬ３追加」の場合

TOE は、電子署名に関する情報を扱うプログラムとして、基本的な開発管理体制の下で外部インターフェース、内部インターフェースを識別できる設計とテストを施すことにより、セキュリティ上問題なく利用できるプログラムであることを保証するＥＡＬ３とする。

追加の保証要件は ADV_SPM.1 とする。電子署名プログラムが扱う証明書及び秘密鍵情報は、個人または組織の信用情報を有するため、明確な情報管理ポリシモデルを保証する要件として追加する。

③ 「保証レベル：ＥＡＬ４」の場合

TOE は、電子署名に関する情報を扱うプログラムとして、適切な開発管理体制の下で外部インターフェース、内部インターフェース、内部構造、実装表現を識別できる設計とテストを施すことにより、セキュリティ上問題なく利用できるプログラムであることを保証するＥＡＬ４とする。

5.4 セキュリティ機能強度

TOE は商用で取り扱われる電子署名管理システムに搭載され、電子署名に関する重要性の高い情報を扱うプログラムとして、十分とみなすことができるセキュリティ強度を確保する必要がある。したがって、中レベルの攻撃力を持つ攻撃者からの侵害に対し適切に対抗できる SOF-medium を提供する。

6 根拠

6.1 脅威に対するセキュリティ対策方針の適合性

セキュリティ対策方針 ＼ 脅威	T.MASQUERADE	T.MASQUERADE_KEY	T.AUDITLOG	T.PRIVATEKEY	T.TRUSTPOINT	T.MIS-OPERATION
O.SEC_KEY（認証情報や秘密鍵の保護）				●		
O.DEL_KEY（秘密鍵の抹消）				●		
O.CTL_KEY（秘密鍵及び証明書の管理）				●		
O.AUTH_KEY（秘密鍵使用時の認証）		●				
OE.ID_AUTH（システム管理者及び署名検証者の識別・認証）	●					
OE.ADMIN（機能管理）			●	●	●	
OE.AUDIT_LOG（監査ログの記録）	●	●	●	●	●	●
OE.LOG_SEARCH（追跡機能）	●	●	●	●	●	●
OE.ACCESS（保護資源へのアクセス制限）			●	●	●	
OE.UI（ユーザインターフェース）						●
OE.TRUST（教育、啓蒙）						●
OE.BACKUP（バックアップ）			●			
OE.INSTALL（導入）						
OE.TRUST_CA（証明書）						
OE.CRYPT（暗号処理）				●		
OE.TIME(時間管理)						

6.1.1 脅威に対するセキュリティ対策方針の説明

T.MASQUERADE：システム管理者及び署名検証者へのなりすまし

この脅威に対抗するためには、電子署名管理システムを利用させる前に不正な侵入を防止し、かつ、システム管理者及び署名検証者を確認することが重要になる。具体的には、以下の対策方針により脅威に対抗する。

「OE.ID_AUTH」により、電子署名管理システムを利用する前にシステム管理者及び署名検証者の識別認証を行い、本人自身であることの正当性を確認することでなりすましを防止する。

「OE.AUDIT_LOG」により、識別認証に関する事象を監査ログに記録し、「OE.LOG_SEARCH」により、監査ログを調査することで、不正者によるシステム管理者及び署名検証者へのなりすましを検知する。

T.MASQUERADE_KEY：秘密鍵所有者へのなりすまし

この脅威に対抗するためには、秘密鍵を使用する前に秘密鍵所有者を確認することが重要になる。具体的には、以下の対策方針により脅威に対抗する。

「O.AUTH_KEY」により、秘密鍵使用時の認証を行うことで秘密鍵所有者へのなりすましを防止する。

「OE.AUDIT_LOG」により、認証に関する事象を監査ログに記録し、「OE.LOG_SEARCH」により、監査ログを調査することで、不正者による秘密鍵所有者へのなりすましを検知する。

T.AUDITLOG 監査ログへの不正な加工

この脅威に対抗するためには、監査ログの保護、及び、管理が重要になる。具体的には、以下の対策方針により脅威に対抗する。

「OE.ADMIN」により、監査ログへの操作を管理することで不正行為を防止する。

「OE.ACCESS」により、監査ログへのアクセス制限を行うことで不正行為を防止する。

「OE.BACKUP」により、監査ログのバックアップ／リストアを実施することで監査ログへの不正な加工（改ざんや削除）から復旧する。

「OE.AUDIT_LOG」により、監査ログへのアクセスを記録し、「OE.LOG_SEARCH」により、監査ログを調査することで監査ログへの不正行為を検知する。

T.PRIVATEKEY :秘密鍵の不正利用

この脅威に対抗するためには、電子署名生成時に利用する秘密鍵の保護、及び、管理が重要になる。具体的には、以下の対策方針により脅威に対抗する。

「O.SEC_KEY」により、秘密鍵使用時の認証情報、及び、秘密鍵を秘匿にすることで秘密鍵に対する不正行為を防止する。

「OE.ACCESS」により、秘密鍵へのアクセス制限を行うことで秘密鍵に対する不正行為を防止する。

「O.CTL_KEY」により、安全に秘密鍵を管理し、生成・廃棄を確実に行うことで秘密鍵に対する不正行為を防止する。

「OE.ADMIN」により、秘密鍵への操作を管理することで不正行為を防止する。

電子署名管理システム上に残存している不使用の秘密鍵に対しては「O.DEL_KEY」により、秘密鍵の使用を前提とした操作実施後における使用済みの秘密鍵を確実に抹消することで、秘密鍵の不正利用を防止する。

「OE.AUDIT_LOG」により、秘密鍵に関するイベントを監査ログに記録し、「OE.LOG_SEARCH」により、監査ログを分析することで秘密鍵への不正行為を検知する。

「OE.CRYPT」により、信頼のある暗号アルゴリズムを使用することで秘密鍵に対する不正行為を防止する。

T.TRUSTPOINT :認証局証明書の改変、破壊

この脅威に対抗するためには、電子署名検証時に利用する認証局証明書の保護、及び、管理が重要になる。具体的には、以下の対策方針により脅威に対抗する。

「OE.ACCESS」により、認証局証明書へのアクセス制限を行うことで認証局証明書に対する不正行為を防止する。

「OE.ADMIN」により、認証局証明書への操作を管理することで不正行為を防止する。

「OE.AUDIT_LOG」により、認証局証明書に関するイベントを監査ログに記録し、「OE.LOG_SEARCH」により、監査ログを調査することで認証局証明書への不正行為を検知する。

T.MIS_OPERATION :誤操作

この脅威に対抗するためには、操作手順の明確化と管理が重要になる。具体的には、以下の対策方針により脅威に対抗する。

「OE.UI」により、操作をシンプルにし、削除や変更に対しては操作の意思を確認するユーザインターフェースを取り入れることで誤操作を防止する。

「OE.AUDIT_LOG」により、電子署名プログラムへの操作を監査ログに記録し、「OE.LOG_SEARCH」により、監査ログを調査することで誤操作を追跡する。

「OE.TRUST」により、教育や啓蒙を行うことで誤操作を回避する。

6.2 想定条件に対する環境セキュリティ対策方針の適合性

想定条件 / セキュリティ対策方針	ASM_INST	ASM_ADMIN	ASM_USER	ASM_TRUSTPOINT	ASM_CRYPT	ASM_CA
OE.ID_AUTH（システム管理者及び署名検証者の識別・認証）						
OE.ADMIN（機能管理）						
OE.AUDIT_LOG（監査ログの記録）						
OE.LOG_SEARCH（追跡機能）						
OE.ACCESS（保護資源へのアクセス制限）						
OE.UI（ユーザインターフェース）						
OE.TRUST（教育、啓蒙）			●			
OE.BACKUP（バックアップ）		●				
OE.INSTALL（導入）	●	●				
OE.TRUST_CA（証明書）				●		●
OE.CRYPT（暗号処理）					●	
OE.TIME（時間管理）		●				

6.2.1 想定条件に対するセキュリティ対策方針の説明

ASM_INST :運用環境への導入

電子署名管理システムが正しく導入されているためには、「OE.INSTALL」により定められた手順書に従って導入を実施する。この対策により当想定条件を実現する。

ASM_ADMIN :運用管理

電子署名管理システムが正しく管理・運用されるためには、「OE.INSTALL」により定められた手順書に従って日常的な管理行為を実施する。また、監査ログに関しては「OE.BACKUP」により安全な形式でバックアップ／リストアを実施する。更に、「OE.TIME」により厳密に時間管理を行う。これらの対策により当想定条件を実現する。

ASM_USER :正当な利用者

電子署名管理システムの使用を許可されている利用者が不正を行うことを防止するためには、「OE.TRUST」により教育、啓蒙を行い、使用を許可されている利用者に起因するセキュリティ事故を防止し、責任範囲を明確にする。この対策により当想定条件を実現する。

ASM_TRUSTPOINT :認証局証明書

TOE が管理する信頼点の基点から EE までのリンクにおける全ての証明書は、信用できる認証局により確実な発行及び失効に関する処理が施される必要があるために、「OE.TRUST_CA」により信頼できる認証局を正しい手続き処理のもとで利用する。この対策により当想定条件を実現する。

ASM_CRYPT :暗号処理

暗号アルゴリズムの強度を保証するために、「 OE.CRYPT」によりアルゴリズムの信頼性や鍵長などの品質尺度を十分に吟味した上で暗号アルゴリズムを採用することにより、十分な強度を確保した暗号化を行う。この対策により当想定条件を実現する。

ASM_CA :証明書

証明書が信用できる認証局により確実な発行及び失効に関する処理を施されるために、「OE.TRUST_CA」により信頼できる認証局を正しい手続き処理のもとで利用する。この対策により当想定条件を実現する。

6.3 セキュリティ対策方針に対するセキュリティ要件の適合性

セキュリティ対策方針 / セキュリティ要件	O.SEC_KEY	O.DEL_KEY	O.CTL_KEY	O.AUTH_KEY	OE.ID_AUTH	OE.ADMIN	OE.AUDIT_LOG	OE.LOG_SEARCH	OE.ACCESS	OE.UI	OE.TRUST	OE.BACKUP	OE.INSTALL	OE.TRUST_CA	OE.CRYPT	OE.TIME
FCS_COP.1	●															
FDP_RIP.1		●														
FCS_CKM.1			●													
FCS_CKM.4			●													
FIA_UAU.1[1]				●												
FIA_UID.1					●											
FIA_UAU.1[2]					●											
FMT_MOF.1						●										
FAU_GEN.1							●									
FPT_STM.1							●									
FAU_SAR.1								●								
FAU_STG.1							●									
FMT_MTD.1									●							
FDP_ACC.1									●							
FDP_ACF.1									●							
FMT_MSA.1									●							
FMT_MSA.2									●							
FMT_MSA.3									●							
FMT_SMR.1									●							
ADV_SPM.1									●							

6.3.1 セキュリティ対策方針に対するセキュリティ要件の説明

O.SEC_KEY 認証情報や秘密鍵の保護

O.SEC_KEY は、秘密鍵使用時の認証情報、及び、秘密鍵の保護を実施する対策であることから、次の要件を適用する。

「FCS_COP.1」により、秘密鍵使用時の認証情報、及び、秘密鍵に対して暗号操作を行うことで、当対策方針を実現する。

O.DEL_KEY 秘密鍵の抹消

O.DEL_KEY は、秘密鍵の使用を前提とした操作実施後における使用済みの秘密鍵の抹消を実施する対策であることから、次の要件を適用する。

「FDP_RIP.1」により、動作中の電子署名プログラムが使用した秘密鍵に関する残存情報を保護することで、当対策方針を実現する。

O.CTL_KEY 秘密鍵及び証明書の管理

O.CTL_KEY は、秘密鍵の管理を実施する対策であることから、次の要件を適用する。

「FCS_CKM.1」により秘密鍵を生成し、「FCS_CKM.4」により秘密鍵の廃棄を行う。これらを適切に機能させることにより、当対策方針を実現する。

O.AUTH_KEY 秘密鍵使用時の認証

O.AUTH_KEY は、秘密鍵使用時の認証を実施する対策であることから、次の要件を適用する。

「FIA_UAU.1[1]」により、秘密鍵の使用を前提とする操作は秘密鍵所有者が認証を受けるまでは許可しないことにより、当対策方針を実現する。

6.3.2 環境セキュリティ対策方針に対するセキュリティ要件の説明

OE.ID_AUTH 利用者の識別と認証

OE.ID_AUTH は、利用者の識別と認証を実施する対策であることから、次の要件を適用する。

「FIA_UID.1」及び「FIA_UAU.1[2]」により、利用者が識別及び認証を受けるまでは電子署名管理システムに対する操作は許可しない。これらを適切に機能させることにより、当対策方針を実現する。

OE.ADMIN 機能管理

OE.ADMIN は、機能管理に関する対策であることから、次の要件を適用する。

「FMT_MOF.1」により、セキュリティに関する機能に対して、システム管理者のみが管理行為を実施できるようにすることで、当対策方針を実現する。

OE.AUDIT_LOG 監査ログの記録

OE.AUDIT_LOG は、監査ログの記録を実施する対策であることから、次の要件を適用する。

「FAU_GEN.1」及び「FPT_STM.1」より、正確な時間情報を付与したアクセス状況の監査情報を記録する。「FAU_STG.1」により、監査ログデータを保護する。これらを適切に機能させることにより、当対策方針を実現する。

OE.LOG_SEARCH 追跡機能

OE.LOG_SEARCH は、監査ログの追跡を実施する対策であることから、次の要件を適用する。

「FAU_SAR.1」により、監査ログのレビューを実施できるようにすることで、当対策方針を実現する。

OE.ACCESS 保護資源へのアクセス制限

OE.ACCESS は、保護資源へのアクセス制御を実施する方針であることから、次の要件を適用する。

「FDP_ACC.1」及び「FDP_ACF.1」により、保護資源に対するアクセス制御方針を定め、定められた方針を機能させる。「FMT_MSA.1」、「FMT_MSA.2」及び「FMT_MSA.3」により、定義されたアクセス制御方針を構成するセキュリティ属性の管理をセキュアに行う。「FMT_MTD.1」により、TSF データの管理はシステム管理者のみが設定・変更できる。「FMT_SMR.1」より、保護資源へのアクセスが可能な役割をシステム管理者に維持する。

また、セキュリティ属性の管理がセキュアであることは、「ADV_SPM.1」により明確なセキュリティポリシモデルを提供することにより保証する。これらを適切に機能させ、また、保証することにより、当対策方針を実現する。

OE.UI ユーザインターフェース

OE.UI は、ユーザインターフェースに関する電子署名管理システムの基本的な設計思想に関する対策方針であり、設計上の仕様に関する方向性を示すことを主眼としている。したがって、電子署名プログラムを搭載する電子署名管理システムの基本仕様に依存することから、対応する機能要件は存在しない。

OE.TRUST 教育、啓蒙

OE.TRUST は、教育、啓蒙の方針であることから、システムの運用に依存するものであり、対応する機能要件は存在しない。

OE.BACKUP バックアップ

OE.BACKUP は、バックアップの方針であることから、システムの運用に依存するものであり、対応する機能要件は存在しない。

OE.INSTALL 導入及び管理

OE.INSTALL は、導入と維持管理の方針であることから、システムの運用に依存するものであり、対応する機能要件は存在しない。

OE.TRUST_CA 証明書

OE.TRUST_CA は、電子署名管理システムで取り扱う証明書の方針であることから、システムの運用に依存するものであり、対応する機能要件は存在しない。

OE.CRYPT 暗号処理

O.CRYPT は、暗号アルゴリズムの方針であることから、システムの運用に依存するものであり、対応する機能要件は存在しない。

OE.TIME 時間管理

O.TIME は、時間管理の方針であることから、システムの運用に依存するものであり、対応する機能

要件は存在しない。

6.3.3 セキュリティ要件間の依存関係

項番	要件	依存する要件	参照項番
1	FCS_COP.1	FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	3 4 17
2	FDP_RIP.1	None	-
3	FCS_CKM.1	FCS_COP.1 FCS_CKM.4 FMT_MSA.2	1 4 17
4	FCS_CKM.4	FCS_CKM.1 FMT_MSA.2	3 17
5	FIA_UAU.1[1]	(*1)	-
6	FIA_UID.1	None	-
7	FIA_UAU.1[2]	FIA_UID.1	6
8	FMT_MOF.1	FMT_SMR.1	19
9	FAU_GEN.1	FPT_STM.1	10
10	FPT_STM.1	None	-
11 12	FAU_SAR.1 FAU_STG.1	FAU_GEN.1 FAU_GEN.1	9 9
13	FMT_MTD.1	FMT_SMR.1	19
14	FDP_ACC.1	FDP_ACF.1	15
15	FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	14 18
16	FMT_MSA.1	FDP_ACC.1 FMT_SMR.1	14 19
17	FMT_MSA.2	ADV_SPM.1 FDP_ACC.1 FMT_MSA.1 FMT_SMR.1	- 14 16 19
18	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	16 19
19	FMT_SMR.1	FIA_UID.1	6

(*1)「FIA_UAU.1[1]」は本来「FIA_UID.1」に依存するが、本要件における認証の対象は秘密鍵の操作であり、秘密鍵自身を選択する操作が識別に相当する操作であるため、本ＰＰに含まれない。

電子商取引推進協議会（ECOM）
認証・公証WG
〒105-0011
東京都港区芝公園　機械振興会館3階
TEL. 03-3436-7500
FAX. 03-3436-7570
E-mail：info@ecom.jp
http://www.ecom.jp/