認証局のセキュリティターゲットにおける セキュリティ環境の考察

新井　聡　今枝直彦　永吉　剛　藤村明子　松村隆宏
NTT 情報流通プラットフォーム研究所

１．はじめに

中央省庁は、2001 年 3 月 29 日、行政情報化推進各省庁連絡会議において、「IS015408 に基づいて評価または認証された製品の利用を推進する。」ことを決めており、昨年 8 月 1 日から導入された新しいシステム調達方式では、IS015408 の認証取得を技術点の加点対象とすることができるようになった※3。経済産業省では、「想定している脅威が不十分と判断される場合は認証されないはずだ」とコメントをしている※3。このように、中央省庁では IS015408 については検討を重ねており、製品を提供する側とすると、積極的に IS015408 の取得を目指さなくてはいけないのだろう。

本原稿では、認証局のついての IS015408 の認証で必要なセキュリティターゲット中でセキュリティ環境を記述する上で、検討しておくべき必要な項目を考察するものである。

２．IS015408 の構成

IS015408 については、あまり学会等で論じられていないので、この項では、構成を簡単に説明する。IS015408 の取得の過程では、最初にセキュリティターゲット(以下 ST)を作成することが必須であり、そのセキュリティターゲットは認定機関からの認定が必要である。※1 によるセキュリティターゲットの構成は、表１のような８章で構成している必要がある

表 1　ST の構成

章	章題	内容
1	ST 概説	ST の文書管理情報および概要
2	評価対象製品 (TOE) 記述	評価対象の特定、評価範囲の規定、評価対象の構成
3	TOE セキュリティ環境	評価対象の動作環境、セキュリティ脅威、組織のセキュリティ方針
4	セキュリティ対策方針	技術的セキュリティ対策方針、運用・管理的セキュリティ対策方針
5	IT セキュリティ要件	TOE セキュリティ機能要件、TOE セキュリティ保証要件、IT 環境に対するセキュリティ要件の定義
6	TOE 要約仕様	TOE セキュリティ要件で記述された個々の貢献に対する具体的な実現方法の記述
7	PP 主張	適合する PP の識別、修正、PP の追加
8	根拠	ST が完全で理路整然とした要件のセットであることを示し、セキュリティ対策方針の根拠、セキュリティ要件の根拠、TOE 要約仕様の根拠、PP 主張の根拠

3 章以降は、製品のセキュリティ仕様を示し、2 章で決定した評価対象に対してのセキュリティ環境や対策について述べていくことになる。セキュリティ環境については、前提条件、脅威、組織のセキュリティ方針を記述する必要がある。ここで、セキュリティ環境を検討する際は、どこまで、深く考えればいいか判断が難しい。本考察では認証局を例にとってセキュリティ環境を検討してみる。

３．セキュリティ環境の検証

Consideration of the security environment in the security target of a certificate authority
Satoshi Arai, Naohiko Imaeda, Takeshi Nagayoshi, Akiko Fujimura, Takahiro Matsumura
NTT Information Platform Laboratoryies

認証局のセキュリティ環境に関する、いかに示すある記述例（※２）について吟味する。

前提条件

・TOE の外部に接続されるエンティティは信頼できるエンティティである。
・TOE 環境は許可された電子認証システム管理者のみが物理的にアクセスできる。
・TOE の構成要素にインターネット等の通信を利用する場合は盗聴や妨害に対して、適切に設定されたファイアウォール等の設備を使用し保護される。
・電子認証システム管理者は与えられた権限に対する責務を果たす。
・電子認証システム管理者はシステムの安全な運用に必要な訓練を受ける。
・オペレーティングシステムは TOE への脅威と同程度の脅威を想定して選択される。
・暗号化の操作は本 TOE の外部にある暗号モジュールで行われる。
・監査者は監査ログをレビューする。

脅威

・電子認証システム管理者が TOE に対する操作でミスを犯す。
・証明書所有者が故意あるいは偶発的にデータを改ざんあるいは抹消する。
・TOE 内のデータが故意あるいは偶発的に改ざんされる。
・TOE 内の監査ログが故意あるいは偶発的に改ざんされる。
・権限外のユーザが TOE への悪意あるコードを使用する。
・権限外のユーザが TOE と外部との通信を閲覧あるいは改ざんする。
・権限外のユーザが TOE への不正アクセスを行う。
・システムに対して OS やハードウェアの重大な障害が発生する。

組織のセキュリティポリシー

・情報は承認された目的のために使用される。
・電子認証システム管理者は証明書ポリシーあるいは認証実施規定を守る。
・電子認証システム管理者の権限は分離されている。
・電子認証システムは電子政府において使用するため、IT セキュリティ関連の法律に準拠する。

ところで、認証局に過負荷が加えられたらどうだろうか。認証局の実装によるものもあるが、処理能力を超える負荷がかかった場合は、サービス能力の低下、さらにはサービス停止に陥る。

認証サービスが停止状態に陥ると、証明書の発行処理や失効処理が不能となり、危殆化した証明書が失効されないまま流通し、新たな証明書が発行できなくなる。ゆえに各種のセキュリティサービスに悪影響を及ぼし、その認証基盤が信頼されなくなる。

例として、正規の運用上で、大量の証明書の失効を考えてみる。この場合、大量の失効処理により、認証局の処理能力を超えてしまい、認証局はサービス停止状態に陥る。これは、多くのユーザを抱えるだけ認証局においてその危険性は高い。

以上により、認証局のセキュリティ上の脅威には、過負荷に対する脅威も含めたほうがよいと考える。

４．まとめ

認証サービスは、電子商取引の基盤サービスである。過負荷によって、認証サービスが実質的にサービス停止状態に陥ると、セキュリティサービスが実質上、機能しなくなり、やりとりされるあらゆる情報が信頼されなくなる。ゆえに、認証局のセキュリティ上の脅威には、過負荷に対する脅威も含めるべきと考える。

参考文献

※1 情報処理振興事業協会セキュリティセンター，情報技術セキュリティ評価のためのコモンクライテリア バージョン 2.1 CCIMB-99-031 平成 13 年 1 月翻訳第 1.2 版
※2 情報処理振興事業協会,電子政府向け電子認証サーバプロテクションプロファイル バージョン 0.8.1
※3 日経 BP，日経コンピュータ　2002 年 09 月 09 日号　（18～19 ページ）