# サーバサイドネットワークを保護するための TPMを用いた接続資格保証基盤

脇田　知彦†　白石　善明†　毛利　公美‡　福田　洋治††　野口　亮司†††
名古屋工業大学†　岐阜大学‡　愛知教育大学††　（株）豊通シスコム†††

## 1. はじめに

高速なネットワークの普及に伴い，XaaS と総称されるネットワークを経由してサービスを利用するという形態が増えている．提供されるサービスによっては，個人情報を取り扱うなどのために高セキュリティが要求されることがある．そのような場合，ID とパスワードを用いたユーザ認証ではなく IC カード認証や生体認証などの，より信頼性の高い認証方法を用いるか併用することになる．それだけでなく，ユーザの利用する端末がサービスを提供するサーバの要求を満たしているか認証（端末認証）をしたい場合があると考えられる．

端末認証をする既存の技術に検疫ネットワークがある．検疫ネットワークでは，端末のセキュリティ情報を検査した後にネットワークに接続できるようになる．しかし，サーバが検疫を受けたことを確認する手段がなく，ネットワーク単位の設定となるためきめ細かい設定をすることができない．

そこで本研究では，ユーザ端末に導入する“内部監査モジュール”が収集したセキュリティ情報を，第三者機関である“端末検証局”が検証した上で接続資格証明書を発行し，サーバはユーザから提示された接続資格証明書の確認を行い，ホストの信頼性をサーバサイドで確認することでサーバサイドネットワークを保護する接続資格保証基盤を提案する．

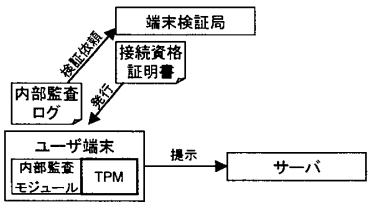


図1　接続資格保証基盤

## 2. 接続資格保証基盤の要件

磯原らはサーバの安全性をクライアントが確認するセキュリティ保証基盤を提案しており，その設計において考慮すべき要件を安全性，柔軟性，即時性の観点からまとめている．

本基盤においても安全性，即時性についてはセキュリティ保証基盤の要件と同等なものとする（表 1中の要件 1～5，8）．[1]の柔軟性の要件 6 については，本基盤ではプロトコルとして送るデータとフォーマットを定めることにより考慮する必要がなくなる．それに代わって，内部監査モジュールの出力するログにより端末に関する様々な情報を提出できる必要があり，同様に証明書により端末に関する様々な情報を証明できる必要があるため，以下の 2 つの要件を追加する．

**[要件 6]** 内部監査ログは様々な情報を格納できる形式であること

**[要件 7]** 接続資格証明書は安全性の情報だけでなく，サービスの提供に必要な様々な情報を証明できること

さらに，本接続資格保証基盤では接続資格証明書内の端末の安全性情報から，サーバはセキュリティポリシを満たしているか検証する必要がある．そこで，容易性に関する要件として以下の要件を追加する．

**[要件 9]** サーバにおいて，端末がセキュリティポリシを満たしていることの検証が容易であること

以上より，接続資格保証基盤の要件は表 1のように整理される．

表1　接続資格保証基盤の要件

| | | |
|---|---|---|
| 安全性 | 要件1 | 相手認証を伴う通信プロトコルであること |
| | 要件2 | 通信内容の盗聴が不可能であること |
| | 要件3 | 内部監査モジュールに対する真正性を担保すること |
| | 要件4 | 接続資格証明書が端末の脆弱性を公開しないこと |
| | 要件5 | 接続資格証明書の発行主体が明確であること |
| 柔軟性 | 要件6 | 内部監査ログは様々な情報を格納できる形式であること |
| | 要件7 | 接続資格証明書は安全性に関する情報だけでなく，サービスの提供に必要な様々な情報を証明できること |
| 即時性 | 要件8 | 証明書の発行・提示が迅速に行えること |
| 容易性 | 要件9 | サーバにおいて，端末がセキュリティポリシを満たしていることの検証が容易であること |

## 3. 端末の信頼性と TPM

安全性の確認対象であるユーザ端末は汎用コンピュータであり，その信頼性をソフトウェアのみで証明することは，そのソフトウェア自身の真正性を確認できないため困難である．そこで，端末に信頼できるハードウェアを設置し，それを用いて端末の安全性を保証する．そのハードウェアが TPM[2]である．

TPM を用いた端末の信頼性の検証方法としてトラステッドブートがある．PC が起動する際には CRTM，BIOS，ブートローダ，OS，アプリケーションの順にプログラムが実行される．このときに，順番にハッシュ値を計算することでシステムが安全に起動したかを確認する仕組みがトラステッドブートである[3]．これによって要件 3 を満たすことができる．

---

Policy-base Access Control Infrastructure For Protecting Server-side Network Using TPM

† Tomohiko Wakita and Yoshiaki Shiraishi・Nagoya Institute of Technology
‡ Masami Mohri・Gifu University
†† Youji Fukuta・Aichi University of Education
††† Ryoji Noguchi・Toyotsu Syscom Corp.

また，TPM は RSA 鍵生成機能を持っており，これにより作成した秘密鍵をユーザ認証に用いる．

## 4. 接続資格保証基盤の設計

### 4.1 適正性の証明

接続資格証明書には安全性に関する情報を格納するが，ソフトウェアのバージョン情報など具体的な情報をいれてしまうと，脆弱性が漏れてしまうおそれがある（要件 4）．そこで安全性に関する評価項目に対する評価を‘最新’のように抽象的に評価することでこれを回避する．また，これらの項目と評価をカンマ区切りで列挙したものを“ポリシ”と呼び，安全性はポリシ単位で評価することとする．サーバは一度許可したポリシをキャッシュすることにより，検証を容易に行うことができると考えられる（要件 9）．

さらに要件 7 を考慮して安全性に関する項目だけでなく，サービスの提供に必要なソフトウェアやハードウェアについても導入されていることが証明できるようにする．そのため，以降では安全性ではなく適正性と呼ぶ．

### 4.2 接続資格証明書の構成

接続資格証明書の構成は X.509 証明書[4]をベースとして図 2のようにした．前節で述べたポリシは主体者適正性情報に格納される．また，要件 5 から発行者を，要件 7 から拡張領域の項目をそれぞれ設けた．拡張領域はポリシだけでは扱いきれない情報がある場合に用いられる．

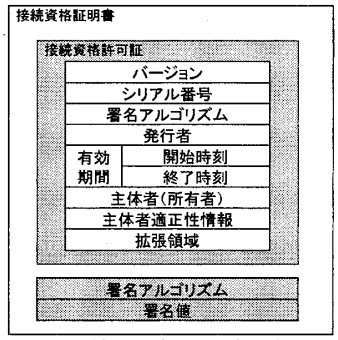


図 2　接続資格証明書の構造

### 4.3 内部監査ログのフォーマット

要件 6 を考慮して，内部監査ログの出力フォーマットには XML を用いることとした．また，収集した情報をソフトウェアとハードウェアの二項目に分類することであらゆる情報を出力できるようにした．ただし，安全性を確認する上で基本的な項目である OS，VDS，FW については，ほとんどのサービスで監査の対象となると考えられるため，独自に項目を作成し出力を必須とすることで，監査ログの分析が容易になるようにした（要件 8）．

### 4.4 証明書発行・提示のプロトコル

証明書発行のプロトコルを図 3に，提示のプロトコルを図 4に示す．はじめに要件 1，2 を考慮して TLS を用いて通信の暗号化とサーバ認証を行う．その後，TPM 内の秘密鍵により作成された署名を検証することでクライアント認証を行う．

なお，提示プロトコルにおいては，接続資格証明書の署名検証を行うために端末検証局の公開鍵証明書をサーバが予め取得しておく必要がある．

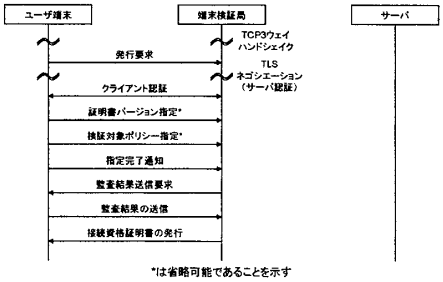


図 3　証明書発行プロトコル

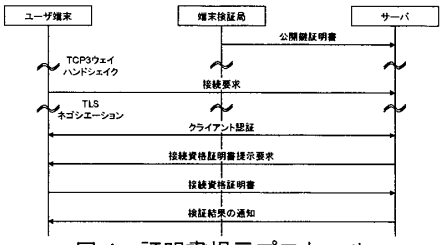


図 4　証明書提示プロトコル

## 5. 従来技術との比較

提案方式と検疫ネットワークとの比較を行い，その結果を表 2にまとめた．提案方式では端末検証局が証明書を発行するため，広域ネットワークで利用可能であり，またサーバに安全性を証明することができる．

表 2　提案方式と従来技術との比較

| 比較項目 | 接続資格保証基盤 | 検疫ネットワーク |
|---|---|---|
| 適用対象 | 広域ネットワーク | 社内LANなど特定のネットワーク |
| 監査対象 | ・OS<br>・VDS<br>・FW<br>・各種SW/HW | ・OS<br>・VDS<br>・FW<br>・各種SW/HW |
| 監査のタイミング | 証明書を発行するとき | ネットワークに接続するとき |
| サーバへの安全性の証明 | 可 | 不可 |
| 提供サービスごとのポリシ設定 | 可 | 不可 |
| TPMの利用 | あり | なし |

## 6. おわりに

本論文では，サービス利用端末の適正性をサーバ側で確認することができる接続資格保証基盤を提案し，設計を行った．内部監査モジュールが収集した適正性情報を，第三者機関である端末検証局が検証し，証明書を発行することでサーバにおいて端末の正当性が検証できる．本基盤では TPM を用いることで内部監査モジュールの正当性の確保や，プロトコルのクライアント認証において安全性を向上させた．また，証明書の設計では，様々な情報を証明できるような設計を行った．

### 参考文献

[1] 磯原 隆将, 石田 千枝, 北田 夕子, 竹森 敬祐, 笹瀬 巌, “検疫結果を保証するセキュリティ保証基盤”, 情報処理学会論文誌, Vol.47, No.02, pp.434-444 (2006).
[2] 中村 智久, 東川 淳紀, “PC 搭載セキュリティチップ(TPM)の概要と最新動向”, 情報処理, Vol.47, No.05, pp.473-478 (2006).
[3] 磯崎 宏, “ソフトウェアを保護するトラステッドコンピューティング”, 東芝レビュー, Vol.64, No.7 (2009).
[4] Russell Housley, Warwick Ford, Tim Polk, David Solo, “Internet X.509 Public Key Infrastructure Certificate and CRL Profile”, RFC2459 (1999).