3X-8

TPM を用いたクライアントのインベントリ証明書による アクセス制御システム

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

1. はじめに

ネットワーク経由で IT 資源を利用するクラウドコンピューティング（以下クラウドという）が広まりを見せており[1]，企業情報システムにおいても「所有」から「利用」へのシフトが加速している[2][3]．しかし，「利用」では自社で IT 資源を管理できないため，クラウドの利用を検討している企業はセキュリティやコンプライアンスの面で不安を感じている[4][5].

IBM のセキュリティ・フレームワーク[6]では，ビジネス要求に基づくセキュリティ要件を 6 つのドメインに分類している．本研究では「人とアイデンティティ」のドメインに含まれる認証，特に機器の認証について扱う．

企業情報システムでは，各組織のポリシーに照らし合わせて，適切な権限を持つユーザかつ適切な状態の端末のみが情報システムを利用できることが要求される．既存の端末の状態を検証する技術には検疫ネットワークがある．検疫ネットワークとは LAN に接続する前に端末の検査を行う仕組みのことである．これをクラウドに適用する場合，異なる企業が提供するサービスを併用・連携して使うときに，企業ごとに検査やエージェント（検査を行うソフトウェア）の導入が必要になることがある．このため，複数のクラウドサービスを併用する場合でも利用者の端末を容易に検証可能な仕組みが必要である．

これについて，我々はインベントリの証明書を用いたアクセス制御モデルを論文[7]で既に提案している．ここでのインベントリは端末のハードウェア・ソフトウェアに関する情報を意味する．本稿ではこのアクセス制御モデルのプロトタイプを作成し，評価を行う．

2. インベントリ証明書によるアクセス制御

論文[7]で提案しているアクセス制御モデルを図 1 に示す．このモデルは 3 つのエンティティで構成される．

- クラウドサービス利用端末（CSR） … クラウドサービスを利用するユーザが使う端末.
- 端末構成保証局（ICA） … CSR のインベントリに対してインベントリ証明書（以降，証明書という）を発行する信頼できる第三者機関.
- クラウドサービス提供者（CSP） … CSR にクラウドサービスを提供する企業など．CSR の提示した証明書に従い，サービス提供の可否を決定する．

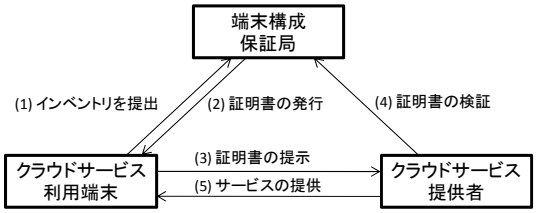

図 1　インベントリ証明書を用いたアクセス制御モデル

アクセス制御の手続きは以下の順に行う．

1. CSR はインベントリを収集し，ICA に提出する．
2. ICA はインベントリを検証し，インベントリ証明書を CSR に発行する．
3. CSR は発行された証明書を CSP に提示する．
4. CSP は ICA と連携して証明書を検証する．
5. CSP は証明書が正当と認められた場合に限り，証明書の内容に応じてサービスを提供する．
6. 以降，定期的に 1，2 を行う

また，本アクセス制御モデルの要件を以下に示す．

（要件 1）　インベントリに関して，記録主体，日時，完全性および記録処理の正確性を証明できること
（要件 2）　CSR と ICA の連携は暗号化通信路を介し，また相互認証を伴うこと
（要件 3）　証明書の発行，提示・検証が迅速・容易に行えること
（要件 4）　CSR および ICA に対して，証明書の提示，検証のためのインターフェースを提供すること

3. システム構成

今回作成したプロトタイプの構成を図 2 に示す．開発言語には Java を利用し，使用したライブラリなどは表 1 に示す．ただし，表 1 中に表記のない構成要素はライブラリを使用していない．

各構成要素の役割を以下に示す．

- 端末構成保証局（ICA）
  - Privacy CA(PCA) … TPM の Identity Key に対して公開鍵証明書を発行する．なお，本プロトタイプではあらかじめ公開鍵証明書が発行されているものとする．
  - Timestamp Server(TS) … タイムスタンプを押す.
  - Credential Server(CS) … 証明書を発行する.
- クラウドサービス提供者（CSP）
  - Authentication Server(AS) … 証明書を検証する.

Access Control System By Client's Inventory Credential Using TPM

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

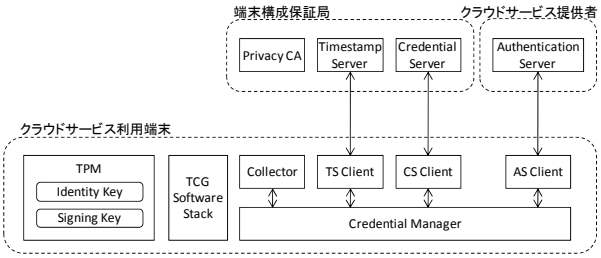

図 2　プロトタイプの構成

表 1　使用した機器，言語，ライブラリ

TPM	Infineon製TPM, Ver. 1.2準拠
TSS	jTSS[10] Ver.0.6
TS/TS Client	IAIK TSP[11] Ver.2.1

- クラウドサービス利用端末（CSR）
  - TPM (Trusted Platform Module) … 耐タンパ性を持つ IC チップ[9]．端末の識別に使う Identity Key と署名に使う Signing Key を持つ．また，相対的時刻のタイムスタンプを押す．
  - TCG Software Stack(TSS) … TPM の機能を利用するためのソフトウェア群．
  - Credential Manager(CM) … 証明書を管理する．なお，CM は信頼できるものとする．
  - Collector … インベントリを収集する．
  - TS Client …TS にタイムスタンプを要求する．
  - CS Client … CS に証明書の発行を要求する．
  - AS Client … AS に証明書を提示する．

システムは以下の順に動作する．

手順1. Collector はインベントリを収集し，TPM・TSS で Signing Key による署名とタイムスタンプを得る．また，TS Client は TPM のタイムスタンプに対するタイムスタンプを TS に発行してもらう．

手順2. CS Client はインベントリと署名，タイムスタンプを CS に送り，証明書の発行を要求する．CS はインベントリを検証し証明書を発行する．

手順3. AS Client は証明書を AS に提示する

手順4. AS は証明書を検証する．証明書に問題がなければ AS は証明書に基づいてアクセス制御を行う．

手順5. AS Client は AS にサービスの提供を要求する．

今回作成したプロトタイプでは論文[8]の TPM とタイムスタンプサービスの連携による時刻保証を手順 1 でインベントリに対して行う．完全性については TPM の Signing Key による署名で，記録主体についてはインベントリに Collector 自身の情報も含めることで対応する．これより，要件 1 の記録主体，日時，完全性については満足する．

CSR と ICA の連携については TLS によりサーバ認証と暗号化を行う．また，クライアント認証については TPM の Identity Key にて行う．Identity Key による認証については論文[9]に示されている手順に基づくことで，相互認証と暗号化の要件 2 を満たす．

要件 4 については AS をクラウドのゲートウェイに設置し，プロキシサーバの機能を持たせるようにすることで，CSR と ICA の既存のシステムへのインターフェースを提供できる．よって要件 4 を満たせる．

4. 速度評価

プロトタイプが要件 3 を満たすか評価するために，

I. CSR がインベントリを ICA に送り始めてから証明書を受け取るのに要する時間（発行時間）

II. CSR が証明書を CSP に送り始めてから証明書の検証結果を受け取るのに要する時間（検証時間）

の 2 つの時間を計測した．計測に利用した機器の構成を表 2 に，結果を表 3 に示す．なお，TLS 認証，Identity Key 認証など，予備通信にかかる時間は含まれていない．

仮に証明書の発行を 1 日 1 回，端末起動時に行うとすると，始業時間の前後に発行要求の集中が予想される．表 3 から 1 時間で処理できる CSR 数は 13800 程度と推測されるため，十分対応できると考えられる．また，検証については要求されるタイミングが分散され，サーバの増設により負荷分散もできるため，検証についても処理速度は十分速いと考えられる．よって要件 3 を満たす．

表 2　実験機の構成（サーバ･クライアント共通）

CPU	Intel Core i5 M560 2.67GHz
メモリ	4GB
OS	Windows7 Professional x64
JVM	JRE 1.6.0_23

表 3　発行・検証に要する時間（100 回の平均）

I. 発行時間	259.3 [ms]
II. 検証時間	262.9 [ms]

5. おわりに

本稿ではインベントリの証明書を発行し，証明書によるアクセス制御を行うモデルのプロトタイプを作成した．本モデルは証明書に基づくアクセス制御をおこなうことで，複数のサービス提供者が連携するようなサービスでも機器の認証が容易にできると考えられる．

作成したプロトタイプはインベントリの証明書によるアクセス制御モデルの要件 1 の記録日時，完全性，記録主体についてと，要件 2，4 を満足する．また，証明書の発行と検証に要する時間を測定した結果，要件 3 を満たすと考えられる．今後の課題としてソフトウェアを安全に実行する方法について検討し，要件 1 の記録処理の正確性を証明できるようにすることがある．

参考文献

[1] 総務省：情報通信白書平成 22 年版，p.351，ぎょうせい，東京（2010）．
[2] 矢野経済研究所：ユーザ企業の IT 投資実態と予測　2009，p.706，矢野経済研究所，東京（2009）．
[3] 太田智朗：クラウドコンピューティング概況と日本ユニシスの取り組み，ユニシス技報，Vol.29，No.1，pp.65-78（2009）
[4] ITmedia：企業のクラウド利用に伴うセキュリティ意識の変化に関するアンケート調査，TechTarget ジャパン（オンライン），入手先〈 http://techtarget.itmedia.co.jp/tt/news/1011/26/news02.html 〉（参照 2010-12-27）
[5] MultiNet International Inc.：クラウド意識調査アンケート結果，MultiNet（オンライン），入手先〈http://www.multinet-usa.com/ITinfracture/CloudService/CloudSurvey.aspx〉（参照 2010-12-27）．
[6] IBM：IBM セキュリティー・フレームワーク，IBM（オンライン），入手先〈 http://www-935.ibm.com/services/jp/index.wss/offerfamily/its/b1332799〉（参照 2010-12-27）
[7] 脇田知彦，福田洋治，白石善明，毛利公美，野口亮司：クラウド環境におけるインベントリ証明書を用いた端末制御，マルチメディア，分散，協調とモバイル(DICOMO2010)シンポジウム 論文集，pp.1448-1452（2010）
[8] 掛井翔平，脇田知彦，毛利公美，福田洋治，白石善明，野口亮司：端末内のイベント発生時刻保証のための TPM とタイムスタンプサービスの連携，第 73 回情報処理学会全国大会講演論文集，6Y-5（2011）
[9] 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.5，pp.473-478（2006）
[10] Trusted Computing for the Java(tm) Platform, http://trustedjava.sourceforge.net/（参照 2011-01-04）
[11] Secure Information and Communication Technologies, http://jce.iaik.tugraz.at/sic（参照 2011-01-04）