Vol.2014-GN-90 No.22
Vol.2014-CDS-9 No.22
Vol.2014-DCC-6 No.22
2014/1/24

OpenID により利用者認証を分離した TPM の 公開鍵証明書発行方式

篠田昭人[†1]　福田洋治[†2]　廣友雅徳[†3]　毛利公美[†4]　白石善明[†5]

パスワードの盗用は被害にあうまで気がつきにくく，紛失はサービスへのアクセスができなくなったときにはじめて気がつくことになる．サービス利用時に使われる利用者の所有物である端末を認証の要素とすれば，盗難や紛失に気がつきやすくなり不正アクセスによる被害を未然に防ぐことができる．モバイル端末への搭載が進んでいるセキュリティチップ TPM（Trusted Platform Module）で生成される署名鍵 AIK（Attestation Identity Key）に証明書を発行すれば，端末を認証トークンとして使えるようになる．AIK の証明書は，利用者の実在性の確認と認証をした上での発行が求められる．利用者が申請時に入力したメールアドレスに認証局がメールを送信し，その返答により利用者の実在性を確認する方式では，証明書を発行するたびに利用者と認証局で認証を行う秘密情報が生成される．サービス提供者が直接認証することなく，外部の認証サービスを利用できる枠組みである OpenID を導入すれば，利用者の実在性確認と認証の機能を OpenID Provider（OP）に分離できる．本論文では，利用者が OP に登録済みのアカウントで利用者の実在性確認と認証する方式を提案する．複数の証明書を利用する際に利用者が管理するアカウントが一つになり，また，認証局は利用者の秘密情報を管理する必要がなくなることを確認した．

An Issuing Scheme of Public Key Certificate of TPM with User Authentication by OpenID

AKIHITO SHINODA[†1]　YOUJI FUKUTA[†2]　MASANORI HIROTOMO[†3]
MASAMI MOHRI[†4]　YOSHIAKI SHIRAISHI[†5]

Plagiarism of passwords is hard to be found out until explicit damage is caused, and loss of them cannot be found out until we lose access right to service. If the terminal we use during service utilization participates in authentication, detection of plagiarism and loss would become easy. Thus damage caused by unauthorized access can be avoided. Terminals can be used as authentication token as long as we issue certificates for Attestation Identity Key(AIK) generated by Trusted Platform Module(TPM) mounted on more and more terminals. AIK certificates should be issued after the existence confirmation and authentication. In an existence confirmation scheme, which makes sure if the response to CA's E-mail will be returned from the user who enter E-mail address on application, CA generates secrets required in authentication between users and CA every issuance of certificates. Suppose OpenID removing the burden of authentication from service providers is introduced, delegation of existence confirmation and authentication to OpenID Provider(OP) can be realized. We propose an AIK certificate issuing scheme which confirms existence and authenticate users by the account registered into OP. Users should acquire only one account on the occasion of using multiple certificates, and CA need not manage user's secrets.

1. はじめに

ID とパスワードの組による認証は，セキュリティが求められるサービスにおいて一般的に導入されている．パスワードの盗用は被害にあうまで気がつきにくく，紛失はサービスへのアクセスができなくなったときに初めて気がつくことになる．パスワードに代表される“利用者の記憶”ではなく“利用者の所有物”を認証の要素とすれば盗難や紛失に気がつきやすくなり，気がついた時点で対応するサービスのアカウントの利用を凍結するなど，不正アクセスによる被害を未然に防ぐことができる．

利用者の所有物による認証には，IC カードや USB トークンに格納されている秘密情報を持つことをクライアント証明書で検証する方法があるが，サービスを利用する端末を認証トークンとするように秘密情報を物理デバイスに格納できる機能を持たせられれば，利用者は端末以外の所有物を携帯する必要がなくなる．そのような機能を持つ物理デバイスとして TPM（Trusted Platform Module）がある．TPM は TCG（Trusted Computing Group）[1)]が仕様を策定するセキュリティチップであり，ノート PC をはじめモバイル端末への搭載が進んでいる．TPM で生成され，端末を移動できないように管理される RSA 署名鍵である AIK（Attestation Identity Key）の公開鍵証明書（以下では，AIK 証明書と呼ぶ）を発行できれば，端末を認証トークンとして使えるようになる．

AIK を利用者の認証の要素とするには，利用者の実在性

†1 名古屋工業大学
Nagoya Institute of Technology
†2 愛知教育大学
Aichi University of Education
†3 佐賀大学
Saga University
†4 岐阜大学
Gifu University
†5 神戸大学
Kobe University

Vol.2014-GN-90 No.22
Vol.2014-CDS-9 No.22
Vol.2014-DCC-6 No.22
2014/1/24

の確認と認証をした上での AIK 証明書の発行が求められる．AIK 証明書を発行する認証局の処理は TCG により仕様が規定されているが，利用者の実在性確認と認証については規定されていない．利用者の実在性確認と認証には，発行する証明書の保証レベルに合わせていくつかの方法がある．コンシューマ向けに保証レベルの低いクライアント証明書を発行するサービスには，利用者が申請時に入力したメールアドレスに認証局がメールを送信し，その返答により利用者の実在性確認と認証をする方法を用いるものがある [2),3)]（以降，この確認方法をメールアドレス到達性確認方式と呼ぶ）．

メールアドレス到達性確認方式では，認証局が利用者に送信するメールに記載される PIN（Personal Identification Number）を利用者が認証局に送信することにより実在性の確認と認証がなされる．PIN は証明書の発行時だけでなく，利用者による証明書の失効や再発行の際にも使用される．セキュリティの観点からサービスごとに複数の証明書を使い分ける場合，証明書を発行するたびに利用者が管理する PIN が増えることになる．

サービス提供者が直接認証することなく，外部の認証サービスを利用できる枠組みに OpenID[4)]がある．OpenID を導入すれば，OpenID Provider で作成した一つのアカウントの認証結果を複数のサービスで利用できる．認証局から OpenID Provider に利用者の実在性確認と認証の機能を分離すれば，認証局が直接利用者の実在性確認と認証をすることなく証明書を発行できる．

本論文では，利用者のもつ OpenID Provider のアカウントで利用者の実在性確認と認証をした上で認証局が AIK 証明書を発行する方式を提案する．提案方式により，利用者は複数の証明書を利用する際に管理するアカウントを一つにでき，また，認証局はメールアドレスと PIN の対応関係を管理する必要がなくなる．そして，OpenID Provider が利用者のアカウントの作成時にメールアドレスによる利用者の実在性の確認をしていれば，認証局が直接利用者の実在性の確認をする場合と同等の保証レベルの証明書が発行できることを示す．

以降，2 章では利用者の所有物による認証のうち，本論文で TPM に着目する理由を述べ，TPM をもちいた認証に必要な AIK 証明書の発行について説明する．3 章では既存のクライアント証明書発行サービスにおける利用者の実在性確認方式について説明し，4 章で認証局の機能分離に OpenID が有効なことを説明する．5 章で OpenID を導入した AIK 証明書発行の方式を提案し，6 章で方式の実装について述べ，7 章で提案方式により利用者が新たに秘密情報を管理することなく AIK 証明書を発行できることを確認する．8 章で提案方式により発行される AIK 証明書を利用した端末認証システムの構築例を示し，9 章で本論文をまとめる．

2. TPM を用いた端末認証

2.1 利用者の所有物による認証

利用者の所有物による認証には USB トークンや IC カードなどの物理デバイスに認証に用いる情報を保管しておき，端末がそれらの情報を読み取ることで認証に用いる方法がある．このような方法では端末のほかに認証のためのデバイスを用意する．USB トークンや IC カードと同様に，認証に用いる情報を格納する機能をもつ物理デバイスに TPM がある．TPM はノート PC をはじめモバイル端末に搭載されるので，TPM を搭載する端末を認証に用いれば，利用者は端末以外の所有物を携帯する必要がなくなる．本論文では，認証の要素として TPM を搭載する端末を用いることを考える．

2.2 TPM 搭載端末を用いた端末認証

TPM は TCG[1)]が仕様を策定するセキュリティチップである．TPM は非正規な情報の読み取りを防ぐ耐タンパ性を持ち，RSA 鍵を生成する機能がある．TPM で生成される RSA 鍵は，生成時に用途が限定される．ここでは，TPM を使った認証で使う RSA 鍵の説明をする．

TPM で管理される RSA 鍵は migratable（移行可能）か non-migratable（移行不可能）のいずれかの属性を持つ．移行可能な鍵は，他の TPM を搭載する端末に秘密鍵をコピーすることができる．移行不可能な鍵は，生成に使われた TPM に恒久的に紐づけられることになる．TPM には，必ず移行不可能な属性をもつ以下の 3 つの鍵がある．

[EK（Endorsement Key）] EK は 1 つの TPM に対し 1 つだけ存在し，TPM ベンダによって初期出荷時に生成され，それ以降の変更は加えられない RSA 鍵である．EK 秘密鍵は漏えいしないように TPM 内部の耐タンパ領域で保管される．TPM ベンダが EK の公開鍵証明書（EK 証明書）を TPM に封入することで，EK が TPM により保護されていることが証明される．AIK 証明書の発行時には，AIK がある TPM で作られた鍵であることを確認し，その TPM を持つ端末にのみ復号可能な証明書を配付することを一つの用途として EK が使われる．

[SRK（Storage Root Key）] SRK は漏えいしないように TPM 内部の耐タンパ領域で保管される RSA 鍵である．TPM 内で生成する RSA 鍵は SRK の公開鍵で暗号化して TPM 外部のストレージに保管することで，移行不可能な鍵として利用できる．このとき，SRK は生成した RSA 鍵の親鍵であるという．SRK は 1 つの TPM に 1 つとなる．TPM には SRK のリセット機能があり，リセットすると新しい SRK に置き換わり，それ以前に SRK を親鍵として生成した鍵は使えなくなる．

[AIK（Attestation Identity Key）] AIK は必ず SRK を親鍵として生成される RSA 鍵で，生成時の SRK を持つ TPM

Vol.2014-GN-90 No.22
Vol.2014-CDS-9 No.22
Vol.2014-DCC-6 No.22
2014/1/24

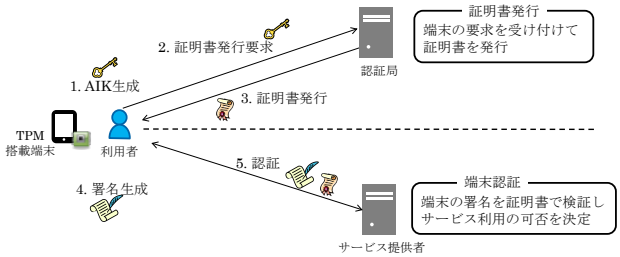

図 1 TPM による端末認証

Figure 1 Terminal authentication by TPM.

でのみ AIK 秘密鍵を用いる演算ができる．TPM の仕様では，対応する証明書を発行されるまで AIK は利用できないように制御されることとされている．TPM 外部のストレージに暗号化された状態で保管され，利用時に TPM 内の SRK で復号して演算をするため，AIK への解析は困難である．

TPM には，初期出荷時に端末とチップ間で紐づけられた情報があるため，ほかの端末に TPM を移して利用することが不可能な仕組みになっている [5]．つまり TPM から移行できない署名鍵である AIK が生成する署名を検証できれば，端末の認証ができる．本論文では，図 1 に示すように TPM を搭載する端末に証明書発行し，端末認証に対応するサービスで使えるようにすることで，TPM を搭載する端末で利用者を認証できるようにすることを考える．

2.3 AIK 証明書を発行する認証局

TCG の定めるプロトコルでは，AIK 証明書を発行する認証局は，AIK が TPM に紐づけられて生成されたかを検証できるようになっている．図 2 に示した具体的な手順の概要は次のとおりである．認証局はまず，端末から送られてくる TPM_IDENITY_REQ を認証局の秘密鍵で復号し，TPM_IDENTITY_PROOF を取り出す．TPM_IDENTITY_PROOF に含まれる，AIK による署名と EK 証明書を検証する．AIK による署名は，TPM_IDENTITY_PROOF に含まれる AIK 公開鍵で検証する．この検証が成功すると，証明書の発行を要求してきた利用者が AIK の秘密鍵を持つことを認証局が確認できたことになる．EK 証明書は，TPM ベンダの署名が付加されており，ベンダが配布する公開鍵証明書を使って検証する．この検証が成功すると，EK 証明書に含まれる EK 公開鍵と対の秘密鍵が TPM で保護されていることを認証局が確認できたことになる．AIK の署名と，EK 証明書の 2 つの検証が成功すると，TPM_IDENTIY_PROOF に含まれる AIK 公開鍵に対する AIK 証明書を作成する．最後にその AIK 証明書をセッション鍵で暗号化した TPM_SYM_CA_ATTESTATION と，セッション鍵と AIK 公開鍵のダイジェストを含む TPM_ASYM_CA_CONTENTS を EK 公開鍵で暗号化した暗号化 TPM_ASYM_CA_CONTENTS を端末に返す．以下では，TPM_IDENTITY_REQ を AIK 証明書発行要求，

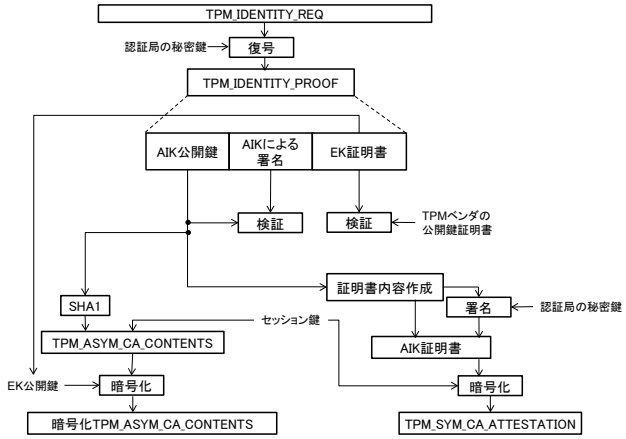

図 2 認証局の AIK 証明書発行処理手順

Figure 2 AIK certificate issuance procedure of CA.

TPM_SYM_CA_ATTESTATION と暗号化 TPM_ASYM_CA_CONTENTS をまとめて暗号化 AIK 証明書と呼ぶ．

以降では，TPM を搭載する端末を認証の要素とするために AIK 証明書を発行するサービスの構築を考える．

3. メールアドレス到達性確認方式による証明書発行

AIK 証明書を発行するサービスの構築にあたり，現在提供されているクライアント証明書の発行サービスのうちコンシューマ向けの証明書発行の方式について説明する．

3.1 クライアント証明書発行サービスの証明書の保証レベル

個人を対象とするクライアント証明書を発行するサービスの認証局の運用規定 [2),3)]によると，認証局が公開鍵ペアを生成する場合は発行した証明書とともに利用者に秘密鍵を渡し，公開鍵ペアを生成しない場合には利用者が秘密鍵を持つことを確認し証明書を発行する．どちらの場合においても，利用者の実在性確認と認証をした上で証明書を発行することとされている．AIK 証明書を発行する場合は，認証局が公開鍵ペアを生成しないことから，2.3 節で利用者が AIK 秘密鍵を持つことを確認する方法について説明している．本論文で取り上げるクライアント証明書発行サービスでは，認証局で公開鍵ペアを生成することから，以降では利用者の実在性確認と認証の方法について述べる．

文献 2)では，発行する証明書の保証レベルに応じて異なる利用者の実在性確認と認証の方法が規定されている．表 1 に示すように保証レベルの低いものから順に，Class 1，Class 2，Class 3 というように証明書のランクが分かれている．Class 1 は利用者の個人名の確認はしないで証明書が発行されるので，正式な個人名を申請しなくても証明書を利用できる．Class 2，Class 3 の証明書は信用機関に登録されている情報や政府機関の発行する身分証をもとに，利用者の氏名が申請時の内容と一致していることを確認したうえ

Vol.2014-GN-90 No.22
Vol.2014-CDS-9 No.22
Vol.2014-DCC-6 No.22
2014/1/24

表 1 証明書のクラスと保証レベル

Table 1 The class and the warranty level of certificates.

証明書のクラス	保証レベル	申請できる利用者の名前	利用者の実在性確認と認証の方法
Class 1	低	ペンネーム，匿名が可	申請されたメールアドレスにメールを送り利用者が応答できるかを確認（メールアドレス到達性確認方式）
Class 2	中	正式な個人名のみ	Class 1の方法に加え，利用者の申請内容と信用機関の情報を照合
Class 3	高	正式な個人名のみ	Class 2の方法に加え，利用者と対面の上，政府機関の発行する身分証と別のもうひとつの身分証を照合

で発行される．本論文では，利用者の氏名を確認することなくアカウントが発行され利用できるようなコンシューマ向けのサービスを対象とし，認証の要素に Class 1 程度の保証レベルの証明書を使うことを考える．

3.2 メールアドレス到達性確認方式

Class 1 の証明書は，表 1 に示すようにメールアドレス到達性確認方式により利用者の実在性確認と認証をし，発行される．ここでは個人向けの Class 1 の証明書を発行するサービス [6]を例に証明書が発行されるまでの具体的な手順を説明する．

証明書発行にかかわるエンティティとその役割は次の通りである．

［利用者］ クライアント証明書を発行される対象．

［認証局］ クライアント証明書を発行するサーバ．利用者の実在性確認と認証をしたうえで証明書を発行する．

図 3 に示す手順で，証明書が発行される．

i. 利用者は認証局の証明書発行申請ページにアクセスし氏名，メールアドレスを送信する
ii. 認証局は PIN が書かれたメールを利用者に送信する
iii. 利用者は，認証局からクライアント証明書をダウンロードする URL と PIN が書かれたメールを受信する
iv. iii のメールに記載されている URL にアクセスし，ダウンロードページで PIN を入力する
v. 認証局で PIN の検証をし，検証に成功したら利用者はクライアント証明書をダウンロードする
vi. v でダウンロードしたクライアント証明書を端末にインストールする

この方式により発行される PIN は証明書発行時の利用者の実在性確認と認証に使われるだけでなく，証明書の発行後に利用者による証明書の失効や再発行を要求する際の認証にも使われる [7]．利用者は他者に知られないように PIN を管理しなければ，なりすましにより意図しない証明書の失効などの被害を受ける恐れがある．認証局との認証に利用者が普段利用する認証サービスを利用できれば，利用者は新たに PIN を管理することなく証明書の発行を受けることができる．

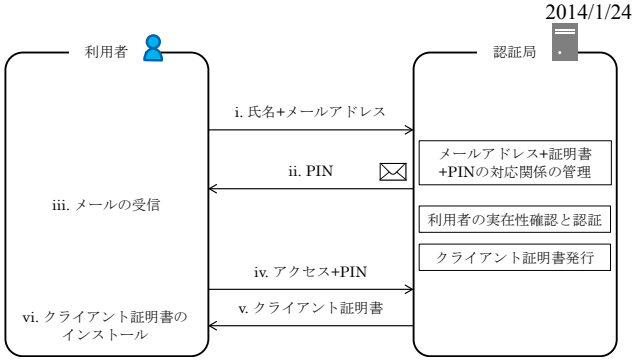

図 3 メールアドレス到達性確認方式による証明書発行

Figure 3 Certificate issuance by reachability testing of E-mail.

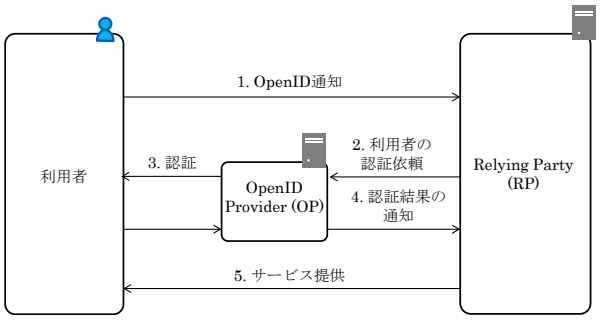

図 4 OpenID の動作

Figure 4 Operation procedure of OpenID

4. 複数の証明書を発行するための OpenID による認証の導入

複数のサービスで利用する認証の鍵を同一のものにすると，端末の匿名性が失われるとされている [5]．端末の匿名性が失われないようにサービスごとに異なる AIK を用いれば，サービス提供者に AIK がどの端末のものかを特定されない．端末の匿名性を保ちつつ複数のサービスで AIK を認証の要素とするために，利用者一人につき複数の証明書を発行することを考える．

メールアドレス到達性確認方式では，証明書発行時に利用者を認証局が認証する際に用いる PIN が生成される．PIN は証明書の失効や再発行する際に利用するため，証明書発行後も利用者が他者に漏らさないように管理するべき秘密情報である．複数の証明書を利用する場合，利用する証明書の数だけ利用者が管理する秘密情報が増加する．

単一のアカウントで複数の認証を必要とするサービスを利用できるようにする枠組みに OpenID がある．OpenID は図 4 に示すように，Relying Party（RP）が OpenID Provider（OP）に利用者の認証を委託する枠組みである．RP は OP による利用者の認証結果から，RP が直接利用者を認証することなく，利用者本人であることを確認する．OpenID を導入すれば，利用者が管理するアカウントを OP で作成したものだけとしながら対応する複数のサービスを利用できるので，利用者が管理するアカウントに対応する秘密情報が増えない．証明書発行時の利用者の認証に OpenID を導入し認証局が RP となれば，複数回の証明書発行を受けても，

Vol.2014-GN-90 No.22
Vol.2014-CDS-9 No.22
Vol.2014-DCC-6 No.22
2014/1/24

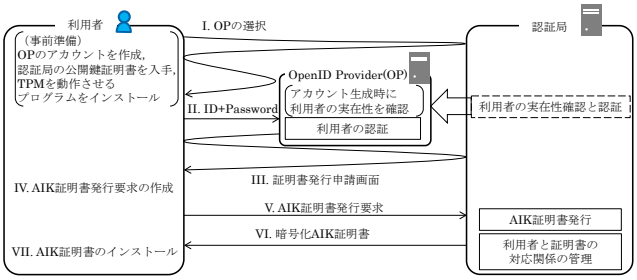

図 5 提案方式による証明書発行手順

Figure 5 Certificate issuance procedure of the proposed scheme.

管理する秘密情報の数は OP との 1 つで済む. 本論文では, 利用者のもつ OP のアカウントで利用者の実在性確認と認証を行うことで, 認証局から利用者の実在性確認と認証の機能を分離する AIK 証明書発行方式を考える.

5. OpenID を用いた TPM の公開鍵証明書発行方式

OpenID を用いた AIK 証明書発行方式に関わるエンティティを 5.1 で示し, 図 5 を用いて証明書の発行手順を 5.2 で説明する.

5.1 エンティティ

[端末] TPM を搭載する端末.

[利用者] AIK 証明書の発行対象となる者. TPM 搭載端末を所有する.

[認証局（RP）] AIK 証明書を発行するサーバ. 利用者から, 証明書発行の要求を受けて証明書発行処理をする.

[OpenID Provider（OP）] 証明書発行時に利用者の認証をする.

5.2 証明書発行手順

（事前準備）利用者は OP のアカウントを作成する.
認証局の公開鍵を入手する.
TPM を動作させるプログラムのインストールする.

I. 認証局にアクセス, OP を選択し OP の認証画面に遷移.

II. 利用者は OP の認証画面で ID と Password を入力する.

III. OP による認証に成功すると認証局の証明書発行申請画面にリダイレクトされる.

IV. 利用者は端末を使い認証局の公開鍵証明書を入力とし AIK 証明書発行要求を作成する.

V. 利用者は, 認証局に AIK 証明書発行要求を送信し, 証明書発行を要求する.

VI. 認証局で AIK 証明書発行処理がなされ, 利用者は認証局から暗号化 AIK 証明書をダウンロードする.

VII. 利用者は暗号化 AIK 証明書を TPM で復号し, AIK 証明書を端末にインストールする.

この方式により, 利用者の実在性確認を認証局から OpenID Provider に分離した証明書発行ができる.

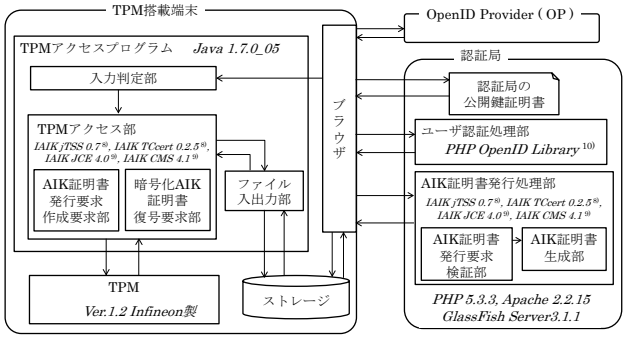

図 6 提案方式の構成

Figure 6 Architecture of the proposed scheme.

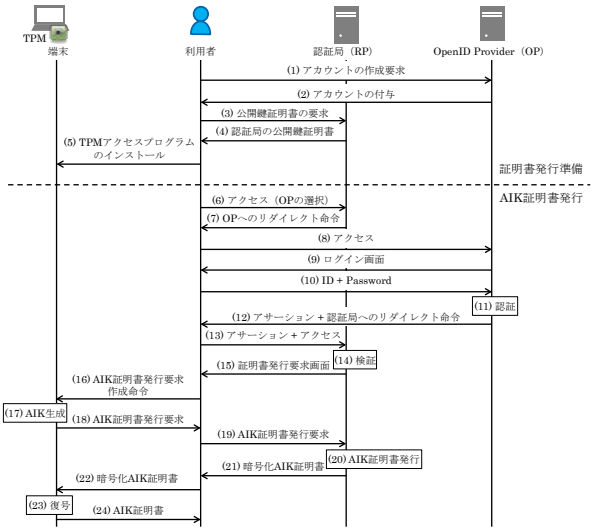

図 7 提案方式の動作手順

Figure 7 Operation procedure of the proposed scheme.

6. 提案方式の実装

5 章で提案した方式の構築方法を示す. 図 6 に示す構成で, 提案方式を実装した. 利用したライブラリや言語は図 6 中の各部に併記する. 以下に, 図 6 と図 7 を用いて動作を説明する.

【証明書発行準備】

利用者はまず証明書発行手続きの準備として, 次の 3 点を行う.

- ブラウザを用いて OP のアカウントを作成する(1), (2)
- ブラウザを用いて認証局の公開鍵証明書を取得する(3), (4)
- TPM 搭載端末に TPM アクセスプログラムをインストールする(5)

利用者が OP のアカウントをすでに持っている場合は, (1), (2)は行わない. (1), (2)は利用者 1 人につき 1 回, (3)-(5)は端末 1 台につき 1 回行う.

【AIK 証明書発行】

- 利用者はブラウザで認証局にアクセスし, OP を選択す

Vol.2014-GN-90 No.22
Vol.2014-CDS-9 No.22
Vol.2014-DCC-6 No.22
2014/1/24

る(6)

- 認証局は，ユーザ認証処理部で利用者が選択した OP へリダイレクト命令を返す(7)
- 利用者は，認証局からのリダイレクト命令を受けて OP にアクセスし，OP のアカウントの ID とパスワードを入力する(8), (9), (10)
- OP は利用者を ID とパスワードの組で認証し，認証に成功したら認証に成功したことを証明するアサーションをブラウザに返し認証局へのリダイレクト命令をする(11), (12)
- 認証局は利用者から受け取ったアサーションを検証し，検証に成功したら証明書発行要求画面に遷移させる(13), (14), (15)
- 利用者はブラウザから TPM アクセスプログラムを起動し，入力判定部で要求されている処理を判定し TPM アクセス部の AIK 証明書発行要求作成要求部を介して TPM で AIK 証明書発行要求を作成し，ファイル入出力部を介してストレージに保存する(16), (17), (18)
- 利用者は TPM 搭載端末のストレージに保存された AIK 証明書発行要求をブラウザを介して認証局に送信する(19)
- 認証局は(19)で受け取った AIK 証明書発行要求を，AIK 証明書発行処理部の AIK 証明書発行要求検証部で検証し，AIK 証明書生成部で暗号化 AIK 証明書を生成する(20)
- 利用者は認証局からブラウザを介して受け取った暗号化 AIK 証明書をストレージに保存する (21)
- 利用者は TPM アクセスプログラムを起動し，入力判定部で要求されている処理を判定し TPM アクセス部からファイル入出力部を介してストレージに保管されている暗号化 AIK 証明書を読み込み，暗号化 AIK 証明書復号要求部を介して TPM で暗号化 AIK 証明書を復号し TPM アクセス部に返す(22), (23)
- 復号した AIK 証明書はファイル入出力部を介してストレージに保存する(24)

以上の手順で TPM 搭載端末に AIK 証明書が発行される．

実装した提案方式で AIK 証明書発行処理にかかる時間を 10 回計測した．平均時間はおよそ 29.6 秒であり，その内訳を次に示す．(6)～(15)の OpenID による利用者の認証の処理時間は 25.49 秒，(16)～(18)の利用者が TPM アクセスプログラムを起動してから AIK 証明書発行要求を受け取りストレージに保存するまでに 2485.6 ミリ秒，(19)～(21)の利用者が認証局(RP)に AIK 証明書発行要求を送ってから暗号化 AIK 証明書を受け取りストレージに保存するまでに 196.3 ミリ秒，(22)～(24)の利用者が TPM アクセスプログラムを起動してから AIK 証明書をストレージに保存するまでに 1468.6 ミリ秒であった．

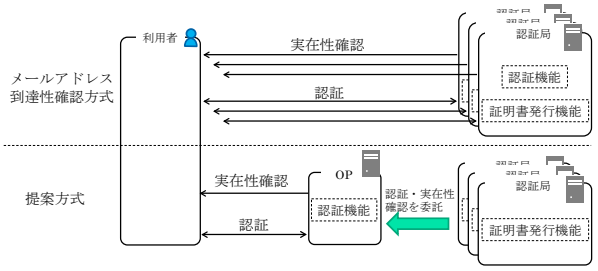

図 8 提案方式とメールアドレス到達性確認方式の各エンティティが持つ機能の比較

Figure 8 Comparison of each entity's functions.

表 2 比較項目とその評価

Table 2 Comparison items and evaluation.

評価項目			メールアドレス到達性確認方式	提案方式
N箇所の認証局の証明書発行	実在性確認の回数		N回	1回
	認証に用いる情報		N個の異なるPIN	1つのパスワード
	利用者が認証情報を入力する回数		N回	高々N回(セッション管理により減らせる)
	利用者が管理する秘密情報		N個のPIN	1つのアカウント
認証局	証明書発行機能		あり	あり
	認証機能		あり	OPに委託
	実在性確認機能		あり	OPに委託
	認証局が管理する情報	利用者情報と証明書の対応関係	要（名前，メールアドレス）	要（名前，OpenID）
		証明書とそのPINの対応関係	要	不要
	認証局がもつ利用者の秘密情報		PIN	なし

7. 評価

本章ではまず，5 章で説明した提案方式と，3.2 節のメールアドレス到達性確認方式による証明書発行を比較し，発行される証明書の保証レベルが同等であることを述べる．次に，N 回の証明書発行をする場合の手順，認証局の機能と管理する情報を比較する．

図 8 に示すように，メールアドレス到達性確認方式では，認証局が直接利用者の実在性確認と認証をした上で証明書を発行する．それに対して提案方式では認証局が OP に実在性の確認と認証を委託しており，OP が直接利用者の実在性確認と認証をする．認証局は直接実在性の確認と認証をしないので，発行される証明書の保証レベルは OP による実在性確認と認証の方法に依存することになる．提案方式において，OP が利用者の実在性確認と認証をメールアドレス到達性確認方式と同等の方法で行い，認証局が OP による利用者の認証結果を信頼するという条件のもと，両方式で発行される証明書は同等の保証レベルを提供する．

提案方式とメールアドレス到達性確認方式の比較結果を表 2 に示す．両方式で，N 回の証明書発行をする場合，メールアドレス到達性確認方式では，利用者は N 回の実在性確認と認証を受け，それぞれで発行される異なる PIN を利

Vol.2014-GN-90 No.22
Vol.2014-CDS-9 No.22
Vol.2014-DCC-6 No.22
2014/1/24

用者が管理することになる．それに対して，提案方式では利用者が OP でアカウントを生成する際に 1 回だけ実在性確認を受けてパスワードを発行し，以降は生成したアカウントに対応するパスワードが入力された場合に実在性確認をした利用者によるアクセスであると判断する．これにより提案方式では利用者は 1 つのパスワードのみを管理すればよくなる．証明書発行時の認証に同じアカウントを用いているので，OP 認証結果の利用の有効期限をセッション管理するように設定すれば，連続して証明書を発行する場合に，利用者がパスワードを入力する回数を減らせる．

認証局が持つ機能と管理する情報を比較する．メールアドレス到達性確認方式では利用者の認証と実在性確認を認証局が直接行ったうえで証明書を発行している．それに対して，提案方式では認証と実在性確認は OP に委託するので認証局が持つのは証明書発行機能のみとなる．加えて，メールアドレス到達性確認方式では利用者を認証するために証明書とその PIN の対応関係や利用者の秘密情報を管理する必要があったのに対して，提案方式では秘密情報を管理する必要がなくなる.利用者の認証に使う秘密情報は OP が管理することになるので，仮に認証局から漏えいした情報を用いても第三者が利用者になりすますことはできない.

8. TPM を用いた Web 端末認証システムの構築例

提案方式によって発行された AIK 証明書を用いて，端末認証システムを構築することができる．本章では，Web サービスでの端末認証システムの構築例を示す．図 9 は Web 端末認証システムの構成例である．

Service Provider は，Web サービス提供のために Apache HTTP Server，PHP，MySQL，OpenSSL などの一般的な構成で Web サーバを構築するものとする．端末認証のためのモジュールは，GlassFish Server 上で動作する Java プログラムとして提供する．Service Provider は端末認証モジュールをインストールするだけで，認証のための処理として複雑な実装をすることなく Web 端末認証システムを構築できる．

Web サービスの利用者は，TPM を利用するための Java プログラムを利用端末にインストールする．端末認証に関わる処理はブラウザを通じて行われ，利用者は一般的な Web サービスを利用するのと同様の操作でサービスを利用することができる．

以下では，図 9 の構成の Web 端末認証システムの動作を，図 10 に沿って説明する．

【アカウント登録】

- 利用者はブラウザより Service Provider にアクセスし，ユーザ情報の登録を行う．Service Provider は，アカウント作成部でユーザ情報をユーザ管理データベースに登録する＜1＞，＜2＞，＜3＞

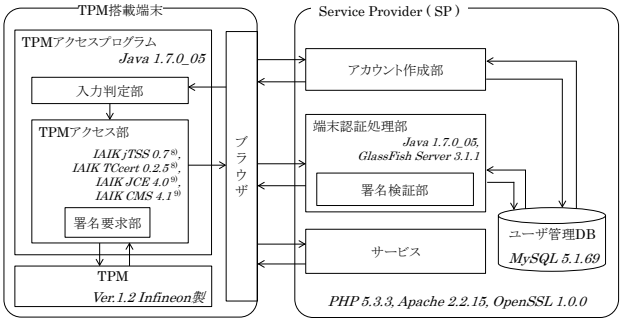

図 9 Web 端末認証システムの構成例
Figure 9 Architecture of the web-based terminal authentication.

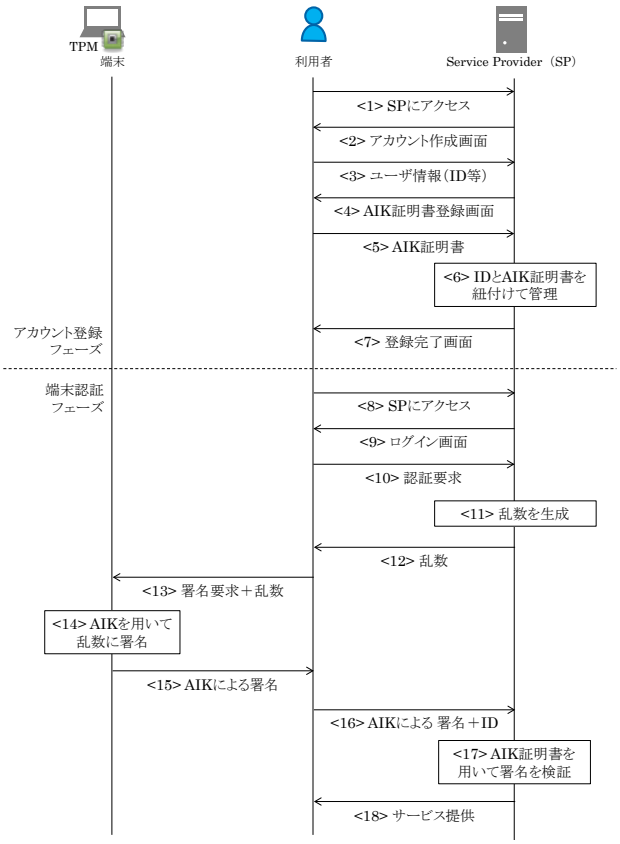

図 10 Web 端末認証システムの動作手順
Figure 10 Operation procedure of the web-based terminal authentication

- 続いて利用者は，発行済みの AIK 証明書を Service Provider に送信する＜4＞，＜5＞
- Service Provider は，受信した AIK 証明書をアカウント作成部で利用者の ID と紐付けてユーザ管理データベースに登録し，アカウント登録が完了となる＜6＞，＜7＞

【端末認証】

- 利用者はブラウザより Service Provider へアクセスし，サービスを利用するための認証を要求する＜8＞，＜9

Vol.2014-GN-90 No.22
Vol.2014-CDS-9 No.22
Vol.2014-DCC-6 No.22
2014/1/24

＞，＜10＞

- Service Provider は端末認証処理部で乱数を生成し，それを利用者のブラウザに送信する＜11＞，＜12＞
- ブラウザは受信した乱数を TPM アクセスプログラムに渡し，TPM アクセスプログラムは入力判定部，TPM アクセス部内の署名要求部を通じて TPM に乱数への署名を要求する＜13＞
- TPM は乱数に署名し，それをブラウザに渡す＜14＞，＜15＞
- 利用者は，ブラウザより署名と自身の ID を Service Provider に送信する＜16＞
- Service Provider は，受信した ID に対応する証明書をユーザ管理データベースより検索し，署名検証部で証明書を用いて署名を検証する＜17＞
- 検証が成功するとサービスの提供が開始される＜18＞

以上の構成例で Web システムとして独自のものとなるのは端末認証モジュールのみであり，それらの導入は Service Provider，利用者それぞれで端末認証モジュールをインストールするだけでよい．端末認証モジュールの処理速度は，5 回試行の平均時間で図 10 の＜11＞乱数生成で 4.3 ミリ秒，＜14＞乱数への署名で 3316.1 ミリ秒，＜17＞署名の検証で 7.9 ミリ秒であり，セッションのはじめに一度のみの処理であることを考えると実用的であるといえる．

9. おわりに

本論文では，まず，紛失や盗難に気づきやすく他の認証用のデバイスを携帯する必要のない TPM を搭載する端末を認証トークンとするために，TPM で生成される公開鍵ペア AIK の公開鍵証明書を発行する方式を検討した．既存の証明書発行方式では，利用者の実在性確認と認証をするために利用者の管理すべき秘密情報が増えることを説明し，利用者が管理する秘密情報を増やすことなく証明書を発行できる方式となるように一つのアカウントの認証結果を複数のサービスに利用できる枠組みである OpenID に着目した．OpenID を導入し，認証局から OpenID Provider に利用者の実在性確認と認証の機能を分離する AIK 証明書発行方式を提案した．提案した方式により，メールアドレス到達性確認方式と比べ利用者が管理する秘密情報を減らし，また，認証局が持つ機能を減らせるようになった．

次に，提案方式によるシステムが構築可能であることを確認するため，構築方法を検討し実装により動作を確認した．提案方式により発行される AIK 証明書の適用先として Web 端末認証システムの構築例を示した．実装した各システムの主要なモジュールの処理時間を計測した．

参考文献

1) Trusted Computing Group: TPM Main Specification Level 2 Version 1.2, Revision 116 (online), available from <http://www.trustedcomputinggroup.org/resources/tpm_main_specification> (accessed 2013-12-19).
2) 日本ベリサイン：日本ベリサイン株式会社 認証業務運用規定（Certification Practice Statement） Version 3.8.7，入手先 <https://www.verisign.co.jp/repository/CPS/>（参照 2013-12-09）.
3) GMO GlobalSign：GlobalSign CA Certification Practice Statement（認証業務運用規程）v7.4，入手先 <https://jp.globalsign.com/repository/>（参照 2013-12-09）.
4) OpenID Foundation: OpenID Authentication 2.0, available from<http://openid.net/specs/openid-authentication-2_0.html> (accessed 2013-12-19).
5) 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）.
6) 日本ベリサイン：シマンテックからの試用版 Class1 Digital ID 取得方法について｜ベリサイン 個人用電子証明書｜日本ベリサイン，入手先<https://www.verisign.co.jp/personal/trial/>（参照 2013-12-19）.
7) Verisign : Solution Details | Digital IDs for Secure Email (Class 1) Support | Support | US Home, available from < https://knowledge.verisign.com/support/digital-id-support/index?page=content&id=SO7093&actp=search&viewlocale=en_US&searchid=1386052815483> (accessed 2013-12-19).
8) Institute for Applied Information Processing and Communications (IAIK): Trusted Computing for the Java™ Platform (online), available from <http://trustedjava.sourceforge.net/> (accessed 2013-12-19).
9) Institute for Applied Information Processing and Communications (IAIK): Secure Information and Communication Technologies / Home - Stiftung SIC, available from <http://jce.iaik.tugraz.at/sic> (accessed 2013-12-19).
10) Janrain: PHP OpenID Library, available from<http://janrain.com/openid-enabled/> (accessed 2013-12-19).