# PKIのRelying Partyにユーザによる想定を取り入れた信頼モデルの提案

木村 泰司[1,2,a)]　奥田 哲矢[3]　砂原 秀樹[1]

**概要**：情報の確からしさは，技術的な仕組みやその仕組みの運用によって支えられるものであると同時に，ユーザが確からしさの判断や利用意思の決定に主体的に関わるべきものである．インターネットにおけるWorld Wide Web(Web) には，Public-Key Infrastructure(PKI) を使って情報の伝送を担う者同士の正当性を確認する仕組みがある．近年，WebPKI において，多数の認証局がユーザの利用意思に関わらず使われることになっている他，ドメイン認証 (DV)，組織認証 (OV)，実在性のある組織認証 (EV) といった証明書の認証レベルの違いが Web ブラウザの表示において分かりにくくなっている．本研究では，PKI においてユーザの主体的な関わりを実現するモデルを提案する．PKI で証明書を使ったエンティティ認証を行う役割である Relying Party (RP) において ユーザの意思決定に基づくアクセス条件を設け，それを履行できるようにする．具体的には，RP である Web ブラウザにおいて，利用する認証局とサイトの組み合わせを確認条件として設定できるようにする．本モデルでは，例えば，銀行・EC サイト・政府といったサイトの真偽について判断を要する特定のサーバにアクセスする際に，ユーザが利用する認証局を限定できる．これによって想定と異なるサイトを区別することが可能になる．本稿ではこのモデルの背景を述べ，実現するための課題と解決の方向性を議論する．

# A PKI trust model considering user's assumption in relying party

Taiji kimura[1,2,a)]　Tetsuya Okuda[3]　Hideki Sunahara[1]

***Abstract:*** Public-Key Infrastructure (PKI) is used as a mechanism to authenticate or verify entities who transact information for the World Wide Web (Web), which is applicably used on the Internet. For WebPKI - PKI adopted for entity authentication on Web, many of CA is used (often called trusted) without user's determinations, in recent years. Those mechanisms and their changes are given for users without their involvements. In this study, we propose a model which achieve user's involvement in PKI. Relying Party (RP) performs authentication using certificate in PKI, establishes requirements based on user decision-making and enables them to be enforced. Specifically, in Web browsers as RP, confirming requirements with combining CA and user's accessing sites are able to be set by users. In this model, users can limit CAs they use for certain servers where users require determined authenticity of the sites, such as banking sites, e-commerce sites, and government sites.

## 1. はじめに

社会活動を支えているインターネットにおいて，ユーザとサービス提供事業者の間でやりとりされる情報の確からしさは重要であり，特に政府や金融といった分野では特に重要である．日常的に使われる World Wide Web(Web) は，これまでの普及の過程においては，ブラウザベンダ，Web サービス提供事業者，認証局，などに対する信頼によって形成された．しかし，これら事業者への信頼に加えて，ユーザの主体的な関わりにより，ユーザは Web サービス利用において，自身のためにより良い意思決定が出来る．

[1] 慶應義塾大学
Keio University
[2] 日本ネットワークインフォメーションセンター
JPNIC
[3] NTT 社会情報研究所
NTT Social Informatics Laboratories
[a)] taiji-k@keio.jp

例えば契約や資産を扱う重要なオンラインサービスの利用にあたって，その確からしさへの判断や意思決定に関わるべき状況がある．近年の，Cookie に関してユーザ同意が求められるようになった動きにも見られる観点である．ユーザが Web サービスの利用において検証可能な情報としては，Web サービス自身が提供する情報はもちろん，信頼される第三者 (Trusted Third Party) である認証局が多くの情報を提供可能である．本稿では，認証局を含む WebPKI の仕組みと近年の WebPKI を巡る動向について概説したのち，WebPKI がユーザの情報の確からしさに関わる信頼の仕組みについて課題を提起し，その克服における既存のトラストの仕組みとユーザ関与の意義を述べる．ユーザの関与が，人の認知としてのトラスト，情報の確からしさに対する確信の根拠を成す意味を，提案するモデルを通じて示す．

## 2. WebPKI の仕組み

Web サービスにおいて，ユーザとサービス提供事業者の間でやりとりされる情報の確からしさを担保する仕組みは，SSL/TLS と WebPKI，証明書，認証局で構成される．SSL/TLS は，ユーザとサービス提供事業者の間の通信の秘匿と改ざん対策を実現すると同時に，サーバ認証の仕組みを提供する．サーバ認証は，通信先のサーバが意図した URL（ドメイン名）に対応するサーバであるかを，サーバ証明書から判定する仕組みであり，サーバ証明書は認証局がサービス提供事業者に対して発行する．本仕組みは，公開鍵暗号，署名の技術で構成されており，WebPKI(Public Key Infrastructure) と呼ばれる．一般に，ユーザは Web ブラウザ - Relying Party(RP) を使って Web サービスとやりとりを行う．

一般に，SSL/TLS 通信を確立するためには，サーバ証明書が，ブラウザベンダがリストで管理する認証局により発行されている必要がある．近年，ユーザが利用するかどうかに関わらず多数の認証局がリストに入っている他，DV,OV,EV といった認証レベルの違いが Web ブラウザの表示において分かりにくいようになっている．

DV（ドメイン認証）は，当該ドメインにおけるサーバの存在を確認（認証）して，サーバ証明書を発行するものであり，近年は自動化された DV 証明書の発行が可能となっている．OV（組織認証）は，当該ドメインにおけるサーバを管理する組織の存在を確認（認証）して，サーバ証明書を発行するものであり，認証局による人手の認証業務を通じて発行されることが多い．EV（実在性のある組織認証）は，当該ドメインにおけるサーバを管理する組織の実在性を公的な文書等により確認（認証）して，サーバ証明書を発行するものであり，認証局による人手の認証業務を通じて発行される．EV が最も審査基準としては厳格であり，EV,OV,DV は Web サービス提供事業者における認証の種類，レベルが異なると言える．

Web サービスの正しさや確からしさを担保する方法の一つであるサーバ認証においては，上述の認証レベルの違いによって，ユーザが確認する意義のある情報が含まれている．具体的には，Web サービスが EV 証明書を利用しているのであれば，その Web サービスは公的な文書により組織の実在性を認証局が確認済みということであり，他の認証レベルに比較して相対的に信頼できる Web サービスと考えられる．

## 3. 本研究の貢献

本研究では，ユーザが利用意思の明確な判断を行うことなく利用している，認証局を中心とする WebPKI のトラストアンカーの信頼モデルに対して，ユーザの意思決定を Relying Party(RP) を通じて取り入れたモデルを提案する．これにより，ユーザが利用する CA を選択し，利用する Web サービス毎に利用されている CA をチェックできるようになり，RP を活用することで CA に関する詳細な知識をユーザが持たなくても上記設定ができることを目指す．より具体的には，銀行，EC サイト，政府といった特定の Web サービスにアクセスする際に，ユーザがトラストする認証局 (Certificate Authority, CA) を，ユーザの想定に従って選択／限定できるようにする．これにより，上記の特定の Web サービス利用時に想定と異なる CA が使われた場合を区別することが可能になる．例えば，本来 EV 証明書であるはずのサイトにアクセスしているつもりで，DV 証明書が使われた偽サイトであったような場合に，その判別が可能となる．

## 4. 現在の PKI における課題

本研究では，下記の 2 点を現在の PKI における課題とする．

(1) 国際的に一元的なトラストリスト
国際的に利用されている WebPKI では，同一の CA の一覧（トラストリスト）が使われており，ユーザはトラストリストの構成に関与しない構造になっている．そのためユーザが信頼している CA であるか否かに関わらず，いずれかの CA が発行した証明書を，画一的に信頼する構図となっており，後述の DigiNotar 事件のように，偽の証明書を有効な証明書と判定してしまう事例が存在している．トラストリストの形態は Web のみに留まらず，様々な署名を使ったアプリケーションに影響する．

(2) RP における認証レベルに依らない一元的な表示
近年，Web ブラウザの表示において，サーバ証明書の DV,OV,EV といった認証業務（ドメイン名と組織実在性の確認）が異なる場合でも，認証結果が同じように表示されるケースが増えている．ユーザには，

DV,OV,EV といった CA による認証業務（証明書発行のために行われる確認の種類）の違いが分からず，サーバ認証における認証レベルの違いがユーザの行動に影響を与え難い形態となっている．

課題解決の基本的な考え方としては，下記の方針を想定している．

- ユーザにより近い位置で，トラストリストの構成を可能とすること
- ユーザによる判断や意思決定を促すため，CA の認証内容の情報伝達を行うこと

特に，Web サービスの種類に応じて，例えば，公的機関・金融機関・ユーザ企業・学校，などの種類に応じて，利用する CA をトラストリストで選定することで，かつ CA の認証内容をユーザに必要十分な範囲で情報伝達することで，過去に WebPKI において問題とされてきた多くの事象に対応できるのではないかと想定している．

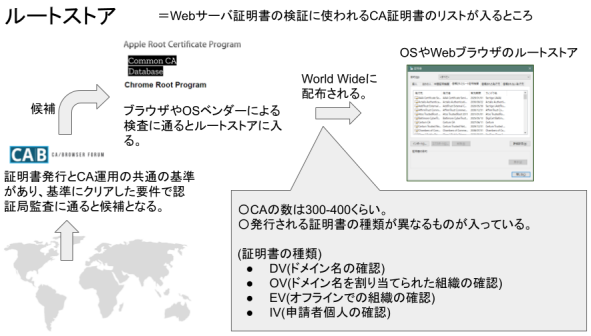


**図 1**　WebPKI におけるトラストリストの管理

### 4.1　トラストアンカー選定の課題

WebPKI のサーバ認証において使われるルート CA は，WebTrust for CA[4] を始めとする監査基準に則った監査が行われ，更に OS や Web ブラウザベンダによるチェックが行われている（図 1）．このチェックは各 CA の証明書発行業務に関する技術的な監査であり，異なる CA の間で整合性のあるサーバ証明書発行が行われているかどうかといった監査ではない．そのため，DigiNotar 事件のような一部 CA における不正な証明書の発行が，過去に問題視されてきた [3]．

WebPKI のサーバ認証において使われるルート CA は CCADB [1] のような一元的な扱いとなり，ルート CA の選定にはユーザは関与せず，ユーザが使わない可能性のある CA が多数含まれている（図 2，図 3）．2014 年の認証局の利用状況に関するサーベイ [15] では，Web のトラストアンカーとして 400 近く登録されている CA の全てが使われているわけではなく，トラストリストの 66%しかサーバ認証に使われていないことが分かっている．これらの実際にはユーザが利用していないトラストアンカーが，一元的にトラストアンカーのリストに入っていることが，上記で述べた DigiNotar 事件の主因であると考えられる．言い換えると，いずれかの CA に不正な証明書が発行されると，フィッシングサイト等に利用されて WebPKI 全体に影響する構造になっている．

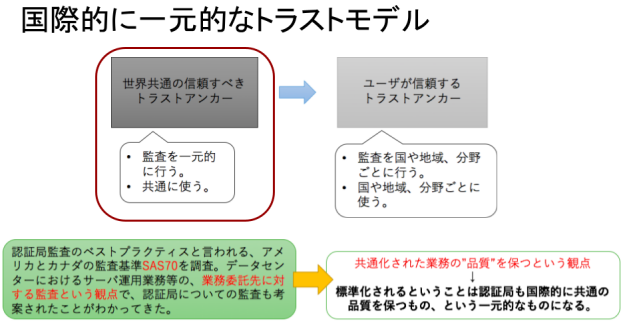


**図 2**　国際的に一元的なトラストモデル

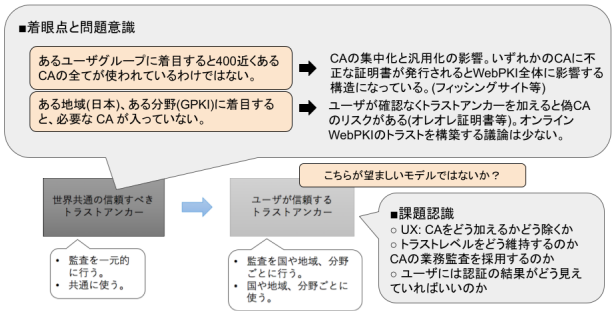


**図 3**　国際的に一元的なトラストモデルの課題

### 4.2　認証レベルの情報伝達の課題

近年は，Web における偽サイトにもサーバ証明書が使われている [13], [17], [18]．Web のサーバ認証に成功すると偽サイトでも鍵マークが表示されてしまう．そのため鍵マークだけでは正しいサイトかどうかの判断ができなくなっている．

一方，USENIX Security 2019 で発表された [20] の EV 証明書のグリーンバー表示のユーザ利用状況に関する調査より，近年は多くのブラウザがこれまで表示していた EV 証明書のグリーンバー表示を PrimaryUI から SecondaryUI に変更している [16]．PrimaryUI は Web サービス利用時に URL バーに最初から表示される一方，SecondaryUI はいわゆる設定画面や詳細画面の位置付けであり，ユーザが意図して操作しなければ表示されることは少ない情報表示画面である．

EV,OV,DV の認証レベルの違いにより，認証局による監査や公的文書による検証など，行われている認証業務には大きな違いがあるのに関わらず，画一的に鍵マークが表示されるだけで，EV,OV,DV の認証レベルの違いがブラウザの表示上からは分かりにくくなっており，EV,OV,DV

の認証レベルの差異がユーザに伝わり難い [14]．そのために，偽サイトが正規サイトになりすましている場合に，ますます識別して判定しにくい状況となっている．

USENIX Security 2019 [20] の EV 証明書のグリーンバー表示のユーザ利用状況に関する調査では，政府や金融といった Web サービスの種類やユーザの意向による利用状況の変化には焦点を当てておらず，これらの Web サービスとユーザの属性に応じた EV 証明書を含むサーバ証明書の情報のユーザ利活用については再考の余地があると我々は考えている．近年の Cookie 利用にユーザ同意が求められるようになった動きなどを見るに，サーバ証明書に記載された認証局が検証済みの情報は，ユーザが主体的に Web サービスの信頼性を判断していく上で有効な情報源と考えられる．ユーザに，EV,OV,DV の認証レベルの違いが伝えられれば，利用している Web サイトが単に DV，すなわち指定したドメイン名で利用できるサーバであるだけなのか，そのドメイン名が実在する組織に割り当てられたものなのかの違いが分かるようになる．

## 5. 課題解決の技術的な提案と方針

本研究では，前章の課題に対する解決方針として，Web サイトの URL，証明書の認証レベル (EV,OV,DV)，認証局の組み合わせをバリデーション・プロファイル (Validation Profile, VP) と呼び，ユーザが選定して Relying Party である Web ブラウザに保持して，従来のサーバ認証に加えて，利用しているサイトが VP に合致しているかどうかを判定する仕組みを提案する．以降で各課題に対して詳述する．

前章の証明書ストアおよびルート CA の課題は下記で言い換えられる．

(1) ルートストアに入っている CA のいずれかに侵入して不正な証明書を発行すれば，グローバルに有効な証明書を発行できる．特定のドメイン名に対する偽のサーバ証明書を発行できる．ユーザは偽のサイトであることが証明書からは分かりにくい．

(2) 任意のドメイン名で取得できるサーバ証明書 (DV, 自動取得可能) とドメイン名の組織の存在が確認されたサーバ証明書 (EV, 人手の認証業務が必要) が同じ扱いになっている．紛らわしいドメイン名を使った偽のサーバに対して同じ「鍵マーク」が表示され，あたかも正しいかのように見えてしまう．ユーザは偽のサイトであることが証明書からは分かりにくい．

上記の課題 (1) について，偽サイトの判別が付きやすくするには，ルートストアに入る CA の数を減らすことが有効である．従来の WebPKI のトラストモデルでは，OS や Web ブラウザのベンダによる検査に通らないとストアに入らず，ストアに入ったルート CA は一元的かつ横並びで利用される形態であったが，本研究の提案では，ユーザが利用する Web サービスの用途に応じて，利用される CA の候補が提示されるようにする (cf. トラストブローカーモデル/ITU-T [23])．これにより，ユーザが利用する CA のみが実質的にストアに入っている状態とする．

上記の課題 (2) について，偽サイトの判別が付きやすくするには，証明書の認証レベルや種類を限定することが有効である．例えば，特定の分野のサーバ（例えば省庁や銀行）の場合には EV 証明書だけに限定する，特定のアプリケーションは EV 証明書で検証できるサーバのみに限定する，などが考えられる．

また，上記 2 点の解決方法の組み合わせとして，特定の分野のサーバ（例えば省庁や銀行）や特定のアプリケーションは，特定の CA で EV 証明書を発行されたサーバのみに繋がるようにする，なども考えられる．その他，特定の国や言語圏においてサーバ証明書を発行している CA かどうか確認する．国や地域の特定の組織（例：省庁・銀行）にサーバ証明書を発行できる CA の一覧を作る，などの対応方法も考えられる．

上記の解決方法は，図 4 および図 5 に示すような従来の認証局の監査と OS や Web ブラウザのベンダによる検査に加えて，対象のルートストアに，ユーザ側の立場で更なるフィルタリングを設けることに相当する．課題の解決の方向性として，ユーザが使う可能性のある CA に限定することができれば，DigiNotar 事件のように本来とは異なる CA に特定のサーバ証明書が発行されても，その証明書検証の結果が有効とはならない．Web ブラウザが本来とは異なるサーバ証明書を有効とみなさないため，ユーザがそのサーバを利用してしまうことを防ぐことができる．

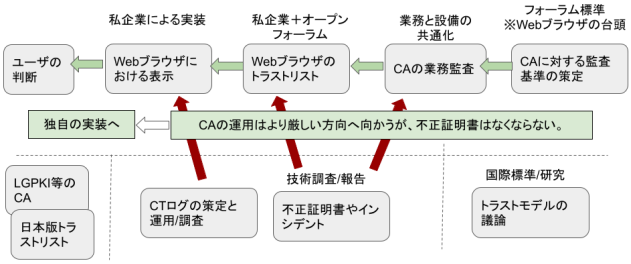


**図 4** WebPKI のトラストアンカーの成り立ち

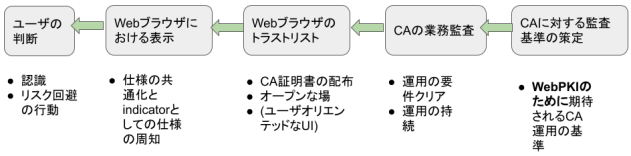


**図 5** 各フェーズの役割

## 6. 従来の PKI 業界における取り組み

本章では，従来の PKI 業界における取り組みについて述

べる．トラストアンカーを一律ではなく利用する CA を限定する従来の取り組みと，これまでにトラストアンカーの選定において課題となった事例を述べる．

トラストブローカーモデルは，Chadwick 氏が ITU で提唱したモデルである [23]．ブローカーモデルは TTP の三つの役割に加えて，CA の信頼性を評価するブローカーという四つ目の役割を持つ．ブローカーは CA の業務を評価してユーザに CA を提示する．ブローカーモデルにおいてはユーザが関知していない CA が提示される可能性があり，我々の研究が目指す，ユーザ側の立場からの CA の選定とは目的が異なる．

Firefox には「認証局を削除または信頼しない」機能がある．主に不正な証明書発行を行った CA を使わないようにするために使われている．Firefox によって管理および設定が行われる．本機能に関する議論として，LGPKI 等のローカライズされた CA がグローバルに適用されないと，日本国内では独自にインストールする必要がある点がある．ある国や地域 (日本など) で，ある分野 (GPKI など) に，必要な CA が存在する場合，それら CA が Web ブラウザのトラストリストに入っていない場合，ユーザが各自でトラストアンカーを追加する必要があるが，ユーザが各自でトラストアンカーを追加する運用は，自己署名証明書等，偽 CA を信頼するルート CA に追加してしまうリスクがある．以前に日本版トラストリストが作られる構想があり，WebPKI におけるパブリック認証局のような形での実装には至らなかったが，JIPDEC で行われているトラステッド・サービス登録の対象に認証局がある．この認証局は日本における事業という地域的なトラストリストの形成と言える．

同様に, 国際的なトラストモデルの議論およびトラストアンカーの議論が, 既存のルート CA の選定のステークホルダと独立に行われている．NIST PKI R&D Workshop(2002-2007) の中でトラストモデルに関する議論は行われているものの [5], [6], [11], [19], [21], [22]、従来のトラストモデルの適用や CA に対するトラストモデルの議論が行われている．Rebooting Web of Trust (RWoT) (2015-) [2] においては，新たなトラストモデルの議論および提案がなされている．技術的には Self Sovereign ID や Decentralized モデルの議論があり，従来の PKI のモデルを踏襲しながら改善する議論はあまり行われていない．

その他，不正が検知された CA をトラストリストから除外する方向性，もしくはサーバ認証において使われる CA を限定する方向性については，IETF や Web ブラウザベンダを中心に進められている．詳細は [24] に詳しい．例えば，証明書が重複して発行されたサーバの検出手法については，Certificate Transparency [12] が現在多くの Web ブラウザで採用されており，Certificate PINNING [8] は上記に代わられた仕様であるが深く検討された仕組みであった．DNS CAA リソースレコード [9] は，特定のサーバ名に対してユーザが利用する CA を限定するものであるが，ユーザが利用する CA やサーバ認証に必要な条件に，ユーザ自身が関与するモデルではない．我々の提案は，ユーザ側の立場でユーザ自身がトラスト対象の選定に関与するものである．

## 7. トラストアンカーに関する既存の取り組みと提案モデル VP の位置づけ

共通したトラストリストを利用するモデルに対して，このモデルとは異なるアプローチとして位置づけられる既存の取り組みがある．

欧州連合 (EU) の eIDAS 規制 [7] には EU Trust Service と呼ばれる事業者登録の仕組みがある．電子署名・適格 (qualified) タイムスタンプの他，Web サーバの認証に使われる適格証明書を発行する事業者を同規制に基づく基準に則って審査し，登録された事業者の名称の他，CA 証明書を Web ページで公開している．この取り組みは，国際的に共通に利用されるトラストリストと異なり，EU 固有のトラストリストである．この審査の構造は CA/Browser フォーラムにおける WebTrust for CA と類似している．すなわち監査と審査は各国各地域で行われるものの，共通の基準が使われる．ユーザの観点では，ユーザの関知なしにトラストリストが構成されるものと言える．

日本情報経済社会推進協会 (JIPDEC) における JIPDEC トラステッド・サービス登録 [10] は，認証局・電子証明書取扱業務・電子契約を，同協会の基準に則って審査し，登録された事業者の名称を Web ページで公開している．この取り組みもまた，国際的に共通な CA と異なり，国内固有のトラストリストであると言える．審査機関が国内の法人であることで，国内のユーザは登録組織に関する異議申し立てを含むやりとりが国際機関と比べて行いやすく，また同協会の判断で登録解除ができる位置づけにある．

本稿で提案する RP に検証プロファイルを設けるモデルである Validation Profile(VP) は，これらと異なりユーザが利用する CA の選択に関与する．トラストリストに入る CA の候補となる範囲が，国際か欧州かといった CA の属性によって決まるのではなく，ユーザのオンラインにおける事業者に対する認知や，利用するサービスに関する認知によって決まる．例えば所属する国の政府のための CA を利用する，銀行口座を持つ銀行のための CA を利用するというものである．使用するサービスや契約等の関係性に従うため，VP は CA のリストであると同じものではなく，使用するサービスと紐づくものとなる．同時に EU Trust Service や JIPDEC トラステッド・サービス，そして国際的に共通したトラストリストと併用できる位置づけにある．

## 8. 提案モデルとその効果

ユーザがPKIを使ったアプリケーションについて，PKIの技術的な認証プロセスに関与するには，RPの認証処理や表示等に関わる技術的な仕組みが必要になる．ユーザにとっての，利用するトラストアンカーの選択やオンラインでの活動の範囲や種類に合わせて，RPが認証処理の仕方を変える．

本研究における提案は，ユーザのオンラインでの活動範囲や種類と利用するCAといった要素を検証プロファイル(VP)と呼ぶ一式のデータで表現し，ユーザが主体的に取得しRPに適用するというものである．

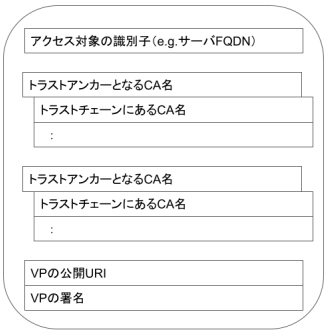


**図 6** 検証プロファイル (VP) のデータ形式

### 8.1 VP データ配布方式

WebPKIのサーバ認証においては，サーバ認証の処理に成功したかどうかということ以外に，サーバ名やCAの識別子といった技術的な要素がある．これらをVPに含めて，サービスの主体がユーザによる選択ができるように提供する．ユーザはVPを自らが確からしさを持つ経路で入手し，WebPKIのRPであるWebブラウザやオペレーティングシステムにセットしておく．ユーザがサービスを利用する際には，Webブラウザ等はサーバ認証の処理を行うだけでなく，そのサーバ名や使われたCAがVPで定義されたものの範囲に入るどうかを判定する．これによって本来使われているCAと異なる等のなりすましのために起きる現象を検知し，なりすましサイトへのアクセスを避ける情報源とする．

本提案は，アクセス制御をユーザの活動範囲を主体にして行うものであり，なりすましの原因となったCAを国際共通的に無効化するような一元的なボトムラインを設けるものではない．例えば学生にとって確からしさを求めるWebサイトは，学校やSNS，ひいては金融機関のサイトや公共機関のサイトであり，国際的に広く存在するセキュアなHTTPSを使ったあらゆるサイトということではない．一連のVPは認証処理に確からしさを求める範囲をユーザ自らが規定するものであると言える．

### 8.2 VP データにおける管理単位の粒度

ユーザがVPを取得し一連のVPに追加したり削除したりすることは，ユーザが確からしいアクセスを行うサーバを個々にホワイトリストとして扱うこととは異なる．前者は，社会的に行われる登録，PKIにおける証明書発行に先立つ本人性確認手続きの頻度に合わせて定義される範囲が選択要素となる．例えば金融機関のVPは，金融機関の組織の実在性を確認しサーバ証明書を発行するCAとその金融機関のサーバ名であり，同じ金融機関によって運営される複数のサーバ名が含まれる．後者のように，ユーザがサーバを個々に扱うと，ユーザによる選択が細かすぎてしまい一つのサービスを使うために確からしさの確認が増えすぎてしまうと考えられる．

### 8.3 提案モデルの効果

VPによって期待されることはサーバにおけるなりすましの判別である．Webではコンテンツは複製可能であることや，サーバ名が多い場合にユーザが覚えきれないことを踏まえると，VPは，URLを意識しないアクセスの場面で効果を発揮することが期待される．サーバ名を認識して意図的にアクセスし，CAの証明書を確認できるようなユーザには，VPの効果は期待できない．例えば，Web検索や電子メールでURLが得られたときに，そのURLが本来の正しいものかどうかが分からずにアクセスするときに，なりすましサイトであるかどうかを判別するために役立つという位置づけである．

## 9. 提案モデルを実現するための課題

提案モデルには，VPのデータを管理する体制，そのVPデータを配布する方式，VPに基づいて行われるRPにおける認証処理といった構成要素がある．各々の課題を述べる．

### 9.1 VP のデータ管理体制

VPを提供するためには，予めCAとサーバ名の組み合わせの確からしさを確認し，ユーザがその確からしさを確認できる形で提供する必要がある．またその確からしさを維持するためにVPを更新したり失効させたりする必要もある．ユーザの主体的な関与のためにはVPの確からしさについて申し立てを受け付け，対処できる主体がVPのデータ管理を担う必要がある．例えば，国という範囲においてはJIPDECトラストサービスのように国内の公益事業を担う組織が審査登録することが考えられる．ユーザは，VPのデータ自体を必ずしもVPデータ管理主体から入手しなければならないわけではないが，VPデータの確からしさの観点でVPデータ公開とユーザの入手地点とは十分に連携している必要がある．

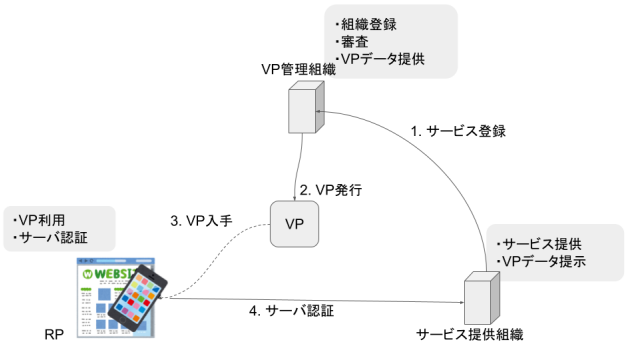


**図 7** 検証プロファイル (VP) の管理体制と利用

VP のデータが提供されると，ユーザはそれを入手し，自らの RP に適用する．配布経路としてはユーザにとっての確からしさのために，物理的に確認する方向性とユーザが依拠する配布経路での評価を元に確認する方向性がある．サービス主体がユーザの物理的な行動範囲に存在するときには，サービス主体が予め VP データ管理主体から作成された VP データを入手しておき，ユーザはその場所や対面によって入手し RP にセットすることが考えられる．例えば，学校に入学した際にその学校の VP を入手する．銀行口座を設けた際に VP を入手するといった社会的な契約のタイミングがある．オンラインまたは物理的な行動範囲にないサービス主体の場合には，ユーザが依拠する配布経路が必要になる．例えば，オペレーティングシステムで提供されるアプリケーション等の提供プラットフォームがある．VP の確からしさに対する評価やレーティング，偽の VP が現れたときにその VP が利用されないように配布を停止する等の対応ができる必要がある．

### 9.2 VP にもとづく RP における処理

VP を RP にセットするとその VP で定められた範囲のサイトには確からしい認証処理が行われる．その認証処理の結果，ユーザにアクセスさせる，アクセスできても入力できないようにする，一切アクセスできないようにするといった RP の処理が必要になる．VP は確からしい認証を前提とするため，基本的にそうではない一般のサイトを VP の処理が有効化された RP でアクセスできる必要はない．VP を扱う RP の処理設計において，課題となることは，VP が得られていない未知のサービスではあるが，確からしい認証を本来的に要する場合である．例えば，国際的に移動しているときに現地の政府や金融機関といった主体によって提供されているサービスを一時的に利用する必要があるときに，RP がそのアクセスをどのように扱うのかという課題である．この VP を使った検査がない状態とある状態とがユーザに伝わるような UI にしなければ，従来のサーバ認証の種類が分かりにくいためになりすましサイトの判別がつきにくい状況に近づいてしまうことが考えられる．

## 10. トラストモデルの社会認知的な拡張

VP は PKI の RP にユーザが主体的に関与するトラストモデルであると言える．本研究ではユーザの主体性は国際的に提供されるトラストフレームワークの一ユーザという技術的な観点の他に，ユーザ自身が認知する社会においてトラストモデルを形成し，そのモデルに立脚するオンラインの認証を行えるようにすることに着目している．

ユーザは，地域的，社会的な立場を持つ他，確からしい認証対象との契約や就学・就職といったセッション性のある立場を持っている．これはオンラインにおける行動にも言えるが，オンラインサービスへのサブスクリプションのようなサービス受容のために，サービス主体の確からしさを評価するモデルについては，更に先の課題に位置づけたい．

法人の確からしさには，その実体存在の他に，第三者，例えば国による法人登記と証明行為がユーザにとって重要な位置づけにある．ある時ユーザがその法人と確からしいやりとりを行う必要があった時に，やりとりの相手がその法人であるのかを確認するためのリファレンスが必要になる．またもしなりすましなどが行われたときに，その状態から復帰を図るためには社会的になりすまし行為の主体を区別し，また本来の主体が正当性を示すことが必要になる．

国という地域における，前述のセッション性を担う主体には，金融機関・学校法人・裁判所・政府機関等公共機関，そしてその他認定事業者が挙げられる．これらは社会的に前述の法人登記と同じ役割を担う制度はあるが，オンラインで検証可能な形での証明データは必ずしも存在しない．本研究で提案している VP は，この証明データとオンライン利用に必要な識別子等の組み合わせであるため，ユーザが認知する対象組織をカバーするような，社会におけるオンラインのための拡張が必要になる．

## 11. おわりに

WebPKI は，その成り立ちから，オブジェクトの認証ではなく通信相手の認証を基軸として，多くのサーバを認証出来ること，また信頼されるべき CA のリストとしてのトラストアンカーが，使われてきた．いわゆるパブリックなトラストアンカーの適用範囲が拡大する一方，それら CA の認証レベルの違いはユーザへの表示において簡略化され，あたかもセキュアであるかのような表示になるサーバ認証につながっている．本稿で議論した RP に設けられる特性は，情報や通信相手に対する認証の根拠となるトラストを形成する方向性に従来と異なったものを表したものである．つまりユーザがオンラインの社会生活において置く通信への信頼は，複合的な第三者によって与えられるだけのものではなく，ユーザの主体性によって初めて成立するものである．一方，ユーザは必ずしも認証分野の専門家で

はないため，主体的な判断への，補助的・示唆的な意義を持つ仕組みが必要とされる．トラストアンカーが多種多様な CA の集合になりその表示が簡略化されたいま，ユーザの「トラスト」に対する主体性についての議論が重要性を増している．本稿は，元来のユーザにとっての「確からしさ」を織りなす事項と考え得るモデルを述べた．

## 参考文献


[1] : Common CA Database.

[2] : Rebooting the Web of Trust.

[3] Amann, J., Gasser, O., Scheitle, Q., Brent, L., Carle, G. and Holz, R.: Mission accomplished?: HTTPS security after diginotar, *Proceedings of the 2017 Internet Measurement Conference, IMC 2017, London, United Kingdom, November 1-3, 2017* (Uhlig, S. and Maennel, O., eds.), ACM, pp. 325–340 (2017).

[4] CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly - Trusted Certificates Version 1.8.4 (2022).

[5] Carl Ellison, W. Polk, N. H. S. S.: NISTIR 7085 2nd Annual PKI Research Workshop Proceedings (2004).

[6] Clifford Neuman, Nelson Hastings, W. P.: NISTIR 7224 4th Annual PKI R&D Workshop "Multiple Paths to Trust" Proceedings (2005).

[7] European Union: eIDAS Regulation.

[8] Evans, C., Palmer, C. and Sleevi, R.: Public Key Pinning Extension for HTTP, *RFC*, Vol. 7469, pp. 1–28 (2015).

[9] Hallam-Baker, P. M., Stradling, R. and Hoffman-Andrews, J.: DNS Certification Authority Authorization (CAA) Resource Record, *RFC*, Vol. 8659, pp. 1–17 (2019).

[10] JIPDEC: JIPDEC トラステッド・サービス登録｜一般財団法人日本情報経済社会推進協会.

[11] K. Sankar, W. Polk, N. H.: NISTIR 7122 3rd Annual PKI Research Workshop Proceedings (2004).

[12] Laurie, B., Messeri, E. and Stradling, R.: Certificate Transparency Version 2.0, *RFC*, Vol. 9162, pp. 1–53 (2021).

[13] Meyer, U. and Drury, V.: Certified Phishing: Taking a Look at Public Key Certificates of Phishing Websites, *Fifteenth Symposium on Usable Privacy and Security, SOUPS 2019, Santa Clara, CA, USA, August 11-13, 2019* (Lipford, H. R., ed.), USENIX Association (2019).

[14] Okuda, T., Chiba, N., Akiyama, M., Fukunaga, T., Suzuki, R. and Kanda, M.: Brand Validation: Security Indicator to Better Indicate Website Identity, *HCI for Cybersecurity, Privacy and Trust - Third International Conference, HCI-CPT 2021, Held as Part of the 23rd HCI International Conference, HCII 2021, Virtual Event, July 24-29, 2021, Proceedings* (Moallem, A., ed.), Lecture Notes in Computer Science, Vol. 12788, Springer, pp. 432–447 (2021).

[15] Perl, H., Fahl, S. and Smith, M.: You Won't Be Needing These Any More: On Removing Unused Certificates from Trust Stores, *Financial Cryptography and Data Security - 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers* (Christin, N. and Safavi-Naini, R., eds.), Lecture Notes in Computer Science, Vol. 8437, Springer, pp. 307–315 (2014).

[16] Roessler, T. and Sladhana, A.: Web Security Context: User Interface Guidelines (2010).

[17] Sakurai, Y., Watanabe, T., Okuda, T., Akiyama, M. and Mori, T.: Discovering HTTPSified Phishing Websites Using the TLS Certificates Footprints, *IEEE European Symposium on Security and Privacy Workshops, EuroS&P Workshops 2020, Genoa, Italy, September 7-11, 2020*, IEEE, pp. 522–531 (2020).

[18] Sakurai, Y., Watanabe, T., Okuda, T., Akiyama, M. and Mori, T.: Identifying the Phishing Websites Using the Patterns of TLS Certificates, *J. Cyber Secur. Mobil.*, Vol. 10, No. 2, pp. 451–486 (2021).

[19] Sean Smith, W. Polk, N. H.: NISTIR 7059 1st Annual PKI Research Workshop Proceedings (2003).

[20] Thompson, C., Shelton, M., Stark, E., Walker, M., Schechter, E. and Felt, A. P.: The Web's Identity Crisis: Understanding the Effectiveness of Website Identity Indicators, *28th USENIX Security Symposium, USENIX Security 2019, Santa Clara, CA, USA, August 14-16, 2019*, pp. 1715–1732 (2019).

[21] W. Polk, K. S.: NISTIR 7427 6th Annual PKI R&D Workshop "Applications-Driven PKI" Proceedings (2007).

[22] W. Polk, Nelson Hastings, K. S.: NISTIR 7313 5th Annual PKI R&D Workshop "Making PKI Easy to Use" Proceedings (2006).

[23] Wazan, A. S., Laborde, R., Barrère, F., Benzekri, A. and Chadwick, D. W.: PKI Interoperability: Still an Issue? A Solution in the X.509 Realm, *Information Assurance and Security ducation and Training - 8th IFIP WG 11.8 World Conference on Information Security Education, WISE 8, Auckland, New Zealand, July 8-10, 2013, Proceedings, WISE 7, Lucerne Switzerland, June 9-10, 2011, and WISE 6, Bento Gonçalves, RS, Brazil, July 27-31, 2009, Revised Selected Papers* (Jr., R. C. D. and Futcher, L., eds.), IFIP Advances in Information and Communication Technology, Vol. 406, Springer, pp. 68–82 (2013).

[24] 島岡政基：今理解しておくべき Web PKI を支えるトラストの動向，Internet Week 2017, 認証局と HTTPS の最新技術動向，JPNIC.