≪「**追加資料**」を巻末の付録USBメモリに収録しています ≫

第10部

公開鍵証明書を用いた利用者認証技術

木村 泰司

第１章　moCA WG 2018年の活動

moCA WGはCA(Certification Authority)の振る舞いや証明書の扱いに注目し、WIDEプロジェクトでCAの運用実験を行っているWGである。

moCA WGで運用されているCAであるmoCAでは、WIDEメンバのためのWIDEメンバ証明書と主にTLSのサーバのためのWIDEサーバ証明書が1年おきに一斉に発行されている。前回は2017年6月に行われ[*1]、今年には一斉発行は行われなかった。

2018年、本WGでは、トラストやIPアドレス認証局といった、新たなテーマについて議論が行われた。次の節でmoCAにおける証明書発行の概況を報告したのち、これらの議論について報告する。

第２章　moCAによる証明書発行の概況

執筆現在、電子証明書が発行されるWIDEメンバ総数は896名で、moCAに発行された有効なWIDEメンバ証明書は934であり[*2]、有効なWIDEサーバ証明書は54である。

第３章　WIDE研究会におけるトラストの議論

3.1　概要

2017年12月のWIDE研究会において、Webブラウザにおけるいわゆるパブリックと moCAの乖離と、CT(Certificate Transparency)ログを使ったサーバ証明書や認証局の発行業務を監視できる事や、認定を受けている認証局であるにも関わらずWebブラウザベンダーによって認証局の審査が行われている動向について議論された。

多くのWebブラウザやオペレーティングシステム(以下、OSと呼ぶ)において、トラストアンカーとして設定されている認証局の数は300から400にのぼっている。Webブラウザやスマートフォンなどの OSは、国際的に共通のプラットフォームが利用されているため、ある地域のユーザにとっては一度も使うことがない認証局がトラストアンカーに入っていることになる。この中のいずれかが誤って、国際的にサービスを展開している、よく知られたWebサイトのサーバ証明書を発行してしまうと、多くのユー

＊1　moCA WGで運用されているCAであるmoCAは、4種類のクライアント証明書を発行している。WIDEメンバに発行されるWIDEメンバ証明書、WIDEメンバの秘書さんに発行される秘書さん証明書、一時的にWIDE合宿等に参加するゲスト向けのテンポラリ証明書、WIDE合宿の事務局業務を行うためのWIDE事務局証明書である。サーバ証明書はWIDEサーバ証明書の1種類のみである。moCAによって発行された証明書は、WIDE研究会やWIDE合宿の申し込みなどのユーザ認証やS/MIMEを使った電子メールで使われており、WIDEサーバ証明書はSSL/TLSを使うWebサーバなどで使われている。WIDEプロジェクトで使われているサーバの中にはLet's Encrypt を利用しているものがあり、WIDEメンバの間ではWIDEサーバ証明書と使い分けがなされている。

＊2　WIDEメンバ証明書は、一人のユーザに対して複数の有効な証明書が存在する。発行対象のユニーク数とWIDEメンバの数とは一致しない)

ザに影響してしまう構造になっていると言える。

これらの状況を受けて、WIDE研究会では「トラストのアーキテクチャはどうあるべきか」というテーマでの議論を試みた。グループワークや小規模のグループでの議論のように様々な形式が取られたが、参加者自身が注目している分野の違いや問題意識の違いによって議論の方向性が異なってしまい、結論を出すには難しいものになった。

簡単にまとめられる事は難しいため、本稿では、各会合の様子をまとめつつ、議論の特徴を述べ、挙がったアイディアについて考察したい。

○ 2018年3月合宿のプレナリー (全体会議) - グループワークとキーとなるテーマ

信州松代ロイヤルホテルで2018年3月に行われたWIDE合宿の全体会議では「WIDE的なトラストのアーキテクチャを考える」と題して、主に学生によるグループワークが行われた。

議論の促進のために以下の4つのキーとなるテーマを提示し、4つのグループに分かれて議論した。

(3月合宿で提示した、トラストに関わる4つのテーマ)

a. 集中か分散か (Concentrated / Distributed)
信頼する先である認証局の一覧が集中化されている。利用者の生活に合う形で分散できないか。

b. 信頼はユーザによるものでまばらにある (Sparse selection of trust)
Webブラウザにはデフォルトで認証局が入っていて、ユーザは信頼する事になっている。知らない国や組織の認証局まで。信頼する先はユーザによって決められるものではないのか。

c. 何を根拠に信頼するのか (Variety of trust vector)
認証局や事業を行う組織を信頼する根拠は何なのか。ブランドか、歴史か、第三者による評価か。また対面で会えば相手を信頼できるのかといった議論もある。

d. 通信上の識別と用途による管轄 (Network identifier and jurisdiction)
実在組織と通信する上での識別子(IPアドレスやドメイン名)とは、技術的にどう結び付ければいいのか。ユーザにとって分かりやすいグループ化やラベルは何なのか。またインターネットにおける通信はフラットに実現されていても、用途に応じて認証、または利用可能な範囲が限られてくる。ホームネットワークや企業のネットワークなどが挙げられる。

4つのチームは「Variety of trust vector」「Sparse selection of trust」「WIDE的なアーキテクチャのあり方」「証明書へのラベルによる権限付与を提案」というテーマで発表した。この中で下記のような議論になった。

(3月合宿における議論)

- Sparse(まばら)というよりHeterogeneous(異種の混在)
単一の尺度で信頼性を図るのではなく、様々な信頼関係をトラストするものが持ち込んで認証できるようにするものではないか。
-> 複数の異質な認証方法がある状態が健全な状態であるという考え方が挙がった。

- 信用する対象は技術と人間の2つ
Blockchainに見られるように技術そのものに対する信頼性に着目する必要性が示された。

分散型: Blockchainなどで複数人がそれぞれこのシステムがいいという状況
集中型:ある人が権限を持ってこれは良い悪いと判断する状況

トラストの構造に関する議論が学生の自由な発想で行われた。ここでの概念的な議論であり、実現するための技術や運用の在り方、そしてWIDEにおけるアクションなどには話は至らなかった。

○ 2018年5月研究会 - 派生した2つのテーマ

大阪府の慶應大阪シティキャンパスで2018年5月に行われたWIDE研究会では、前述の4つのテーマを受けて、WIDEメンバーの声を反映した下記2点のような議論になった。

(5月研究会における議論)

e. トラスト対象(ユーザとの関係)

トラスト対象を点として評価するのではなく、ユーザとトラスト対象との関係という「線」、その太さなどで評価するモデルの議論。オンラインのサービスを提供するGoogle、Apple、Facebook、Appleのような社名はトラストの対象として捉える事ができるが、ユーザとそのサーバの間には、DNSやBGPを使ったルーティング、TLSといった様々な要素がある。これらの信頼性は社名のラベルとは別の要素となる。これをどう考えるか。

f. サービスによる検証の厳しさの違い(どう実現するのか)

会社組織や大学における印鑑の扱い、例えば秘書による契約書への捺印はその行為の権限が委譲されていると捉える事ができる。これをトラストの構造としてはどうとらえればいいのか。

おとぎ話のかぐや姫に様々な難題が課せられる話がある。ある敷地に入るという意味で、軍事基地に入るのとは異なる要件が課されていると言える。あるサービス利用のためのユーザ認証においても、そのサービスによって検証の厳しさが異なるのではないか。また通信路の安全性と、情報の信頼性を分けて考えないといけないのでは。

トラストというキーワードについて参加者の注目する信頼性や権限行使の確からしさ、ネットワークと情報の信頼性といった様々な要素にばらける結果となった。トラストが、様々な構造や期待されるセキュリティを想起するキーワードである事が分かってきた。

○ 2018年9月合宿 - トラストリストの分類

信州松代ロイヤルホテルで行われた9月合宿では、トラストBoFと題してこれまでの議論の整理を行った。時間が限られていたため、次の節で述べる「IPアドレス認証局」にも関連してトラストリストに関する議論になった。

- 従来のWebブラウザのように単一種類ではなく「街」「仕事」といった分類を分ける想定をする。例えば銀行のWebサイトについては銀行協会がトラストリストを作る案。
- 未知のトラスト候補が現れた時にユーザにどう提示すべきか。

○ 2018年12月研究会 - 総括とトラスト検討の必要性

東京大学で行われた12月研究会では、WIDEにおけるトラストに関する議論の簡単なまとめが行われた。この機会に初めてトラストに関する議論に触れた参加者がいて、例えばホームネットワークにおいて複数のメーカーの機種を扱う際に重要になるのでは、といったコメントが寄せられた。

○ 考察

「トラスト」という言葉には様々な意味があると共に、トラストという単語からWIDEメンバが想起する、技術的な分野も多岐に渡る。議論の際には、どのような状況において何が期待されるものなのか、といった整理が重要になると考えられる。これはWIDE研究会に限らずに他の研究会や勉強会における議論にも似たものがある。一見曖昧な言葉であるが、様々な場面で考察される概念であるとも言える。今後もWIDE研究会内外の議論に注目したい。

第４章　IPアドレス認証局

IPアドレス認証局とは、IPアドレスが記載された電子証明書を発行する認証局で、IPを使った通信における通信路の安全性や通信データの安全性を確保するための仕組みである。JPNICでは、公益的な観点でオープンソースのプロジェクトとして取り組まれている。

(IPアドレス証明書の利用想定)

- IoTのような場面で、ユーザ・インターフェースが限られていて電源を入れるだけで使われる。
- 自動的に電子証明書が取得/更新されTLSなどで使える。
- ノードにホスト名がつけられることは想定せず、またDNSの利用も想定しない。

2018年9月の合宿で下記のような議論が行われた。

(IPアドレス認証局に関する議論)

- どういう世界が望ましいのか/IPアドレスの証明書の利

用の前に目指す仕組みの前提は何か。例えばIPアドレスが変わる事は想定するのか。
- 東京大学のGreenITプロジェクトでは、管理者が分かりやすいFQDNを導入した。
- ドメイン名の確認ができないHEMS(Home Energy Management System)ではどう適用されるか。

JPNICではデザインチームが作られ、上記の論点や頂いたコメントを検討課題として引き続いて議論が行われている。デバイス認証においてデバイスそのものが電子証明書を保持するのと、IPアドレス証明書を保持するのとでは何が違うのかといった根本的なテーマである。

IETFにおいても、IoTのような場面を前提としたプロトコルの策定が進められているが、そこで利用される電子証明書の発行/管理に関してはまだ議論が進んでいない。

IPアドレス認証局の検討が、IoTのような検討余地のあるセキュリティのデザインに資するべく取り組んでいきたい。

第５章　WIDE Root CA 03フィンガープリント

WIDEプロジェクトにおける電子証明書のトラストアンカーを提供するために運用されている認証局の証明書「WIDE Root CA 03」のフィンガープリントを以下に示す。

SHA-256フィンガープリント
3B:CB:EC:C3:6C:96:ED:D5:A2:98:81:19:C4:C6:F0:4B:
DE:AB:43:63:48:D3:7B:05:F9:36:5F:1C:AF:B4:0F:8C

SHA-1フィンガープリント
42:75:7B:24:E3:BB:DB:AB:9E:D7:FE:32:D1:27:18:58:EE:
3E:81:66