現代のPKIトラストフレームワークにある課題とその将来

David W Chadwick
Kent大学

参考訳：木村泰司

内容

- トラストとは？
- X.509と現代のPKIX
- X.509トラスト・ブローカーの提案
- 認証局の信頼性の評価
- PKIのトラストに関するISOやIETFのそのほかの活動
- 認証(Authentication) or 認可(Authorisation)?

真か偽か?

- あなたを信頼するので契約書にサインする
- あなたを信頼しないが100円を貸す
- トラストマネージメント ≡ リスクマネージメント

信頼 – 意味

- トラスト - 正当性、能力、人物や物の特徴に対する信頼を置くこと [1]
- トラスト - 確実性、事実、能力や強さについて、誰かもしくは何かの確からしさにおいて信頼を置くこと [2]
- トラストの動機：　良くない結果が起こりうるにも関わらず、相対的な安心感のある状況において何かもしくは誰かに頼ろうとすること [3]

[1] Dictionary.com
[2] Oxford English Dictionary
[3] McKnight and Chervany 1996. http://misrc.umn.edu/wpaper/wp96-04.htm を参照

トラストとは何か?

- トラスト ＝ 残存リスク
- もしリスクがなければロス(損失)機会はなく、トラストは必要ない。例：クレジットカードによるインターネットのeコマース
- 契約、罰則、法律、裁判所、制度、スタンダードなどは、ビジネスにおけるトラストを増すものではないが、リスクを受け入れ可能なレベルに減らし、それゆえビジネスに必要となるトラストのレベルを下げてくれるものである。

トラストフレームワークとは?

- トラストフレームワークとは、電子的な本人証明（identity credential）を受け付ける者（依拠当事者）が、本人性、セキュリティ、そして本人証明を発行する者（アイデンティティ・サービス・プロバイダー）のプライバシーポリシーなどに信頼をおけるようにする認証の仕組みのこと
  - The Open Identity Exchange (OIX)

- トラストフレームワークの目的は、トラストする者への残存リスクを減らすこと

X.509 PKI トラストフレームワーク

- あるエンティティの公開鍵を取得して信頼するためのフレームワークである。その公開鍵はそのエンティティが復号できるように情報を暗号化するため、またはそのエンティティの電子署名を検証するために使われる。
  - ところで、エンティティとは誰?
- 公開鍵証明書(public-key certificate - PKC)： ユーザの公開鍵やその他の付帯する情報が、その証明書を発行する認証局の秘密鍵を用いた電子署名によって失われないようにしたもの。
  - それゆえその他の情報がエンティティが誰かを示すのか?
- 認証局はユーザの識別名と公開鍵を含めた情報に署名することでユーザの証明書を生成する。
  - これがエンティティを識別するX.500の識別名である。
  - ここに大きな問題がある。X.500の識別名を使ったり知っていたりする人は少ないため、何も知らないものをトラストするように要求されることになる。

PKIの認証局は何か?

- X.509より
- certification authority (CA): （エンティティへの）公開鍵証明書を作成しアサインするために1以上のユーザに信頼されるオーソリティ/権限のこと。

- よって正しいX.500識別名（そして他の情報もありうる）をエンティティにアサインするCAを信頼しなければならない。
- これがCAの一義的な役割である。

X.509の今まで

- 1988年に初版 (v1 証明書)
- 1993年に第二版 (v2 証明書 – 使われていない)
- 1997年に第三版 (v3 証明書 – 現在のPKIで基本的に使われる)
- 2001年に第四版 (X.509 AC インフラストラクチャ – OASIS SAML 属性アサーションの基礎)
- その後の版: 2005, 2009, 2013 主にバグ修正と細かい拡張
- 2016年7月の版はオープンPKIにための新たなトラストモデルが入る。これが必要なわけは?

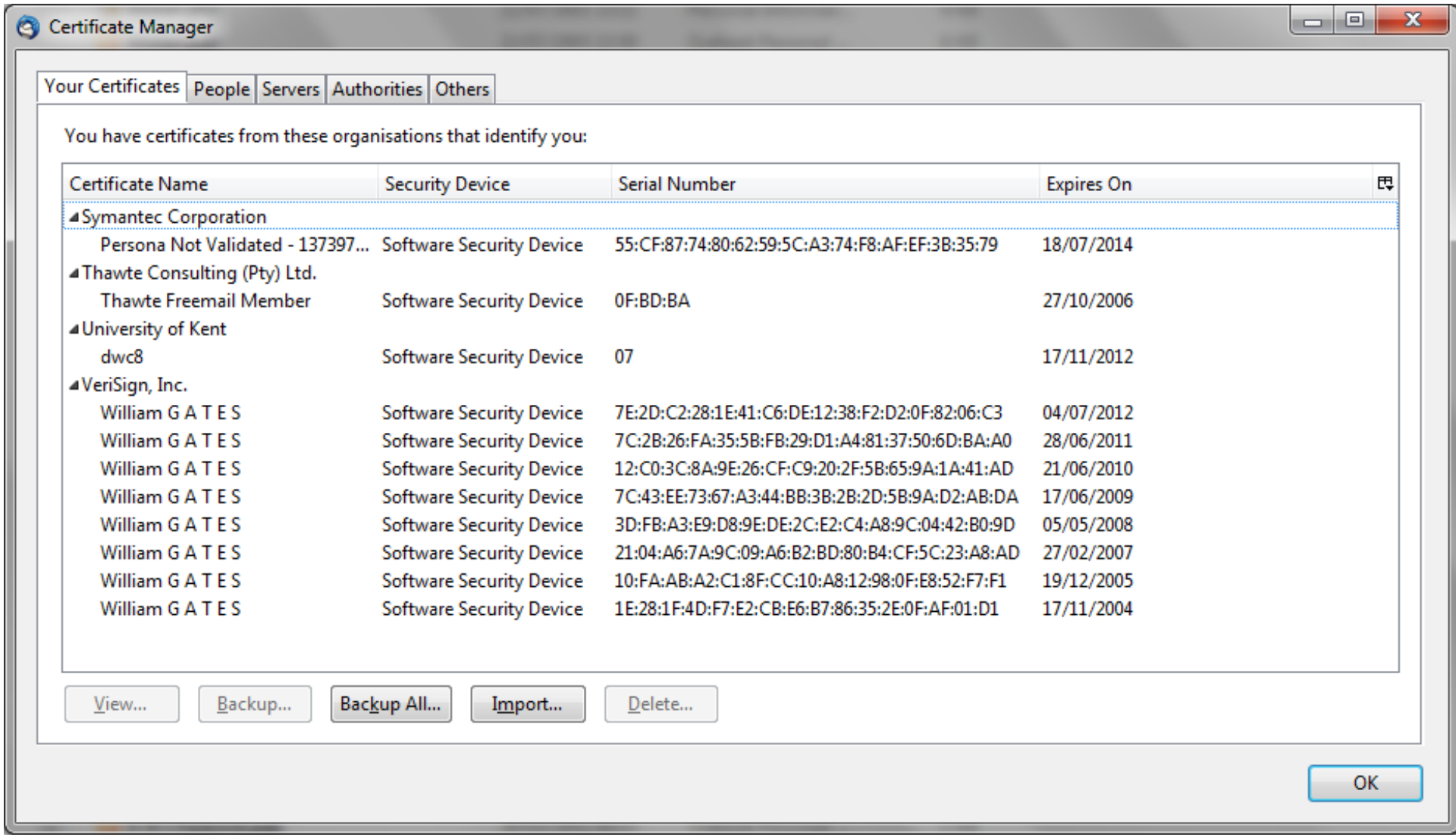
X.509にあった欠落と、それゆえのIETF PKIX

- X.509は認証局と発行先のための運用上のプロトコルを定義していなかった
  - PKIXは証明書管理、タイムスタンプ、オンラインの証明書ステータス、LDAPv2やFTP/HTTPの利用、データ検証と認証サーバ、代理パス検証や代理パス構築、サーバベースの証明書検証、トラストアンカー管理といったプロトコルを提供している。
- X.509は認証局がどのように運用すべきなのかのガイドは提供していない
  - PKIXでは RFC3647「Certificate Policy and Certification Practices Framework」ができている
- X.509はリアルタイムの失効処理を定義していない
  - PKIXからはOCSPが策定されている

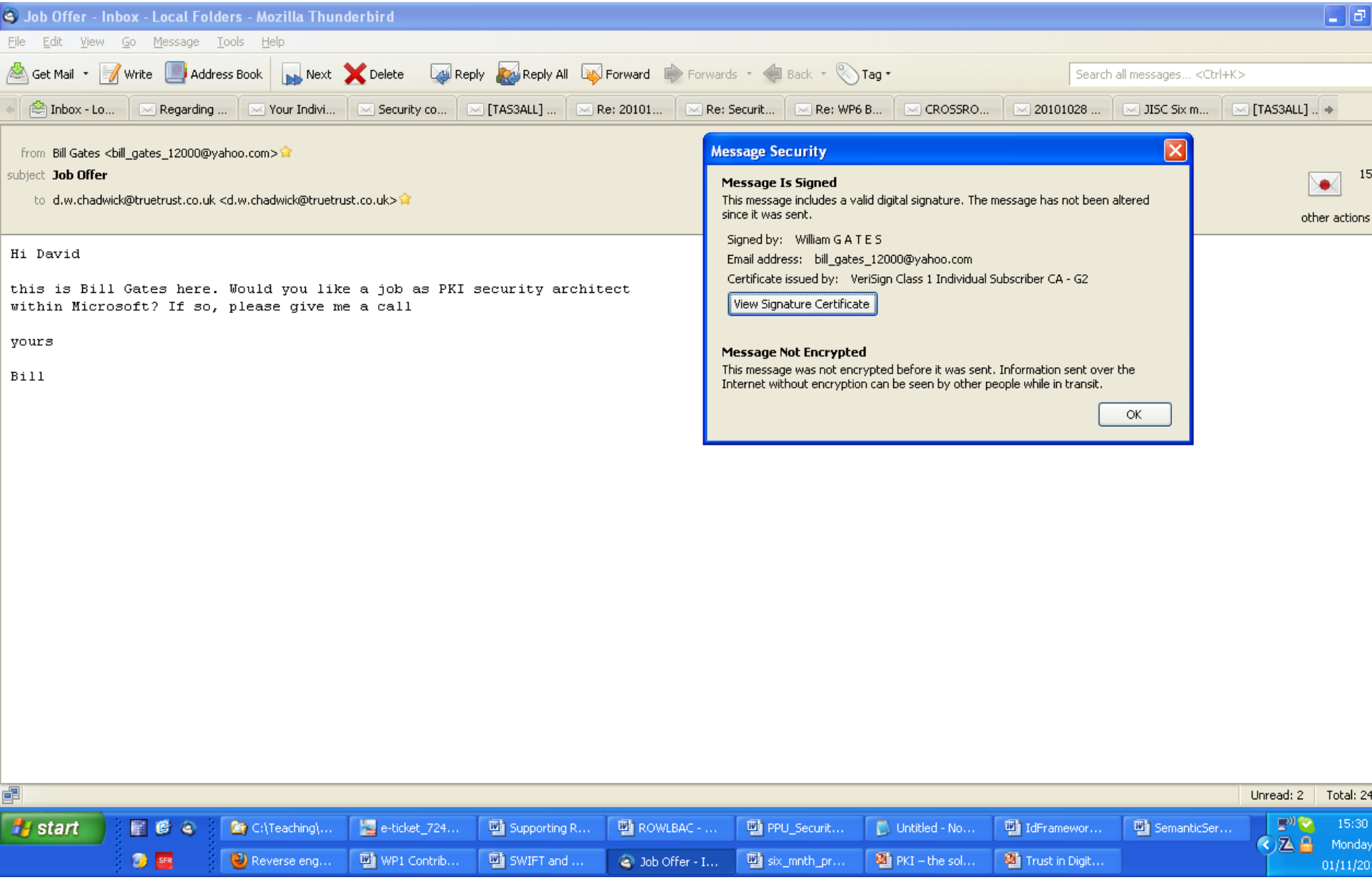
PKIXにもある欠落

- CAの信頼性を図る基準や自動化手法はない。CPとCPSは人の理解のための定性的な文書である。
- 現在のインターネットPKIのスケールは管理するには大きすぎる。
  - 例： 認証局は発行先の本人性を確認しないことがありうるがインターネットでは信頼される対象であり得る
  - 認証局と発行先の証明書は偽造でき、気づかれないことがありうる
  - CRLが巨大になってしまい、処理するための時間が長くなりすぎる可能性がある
- ユーザ（依拠当事者）は、失効された/偽装された/信頼できない証明書を使ってしまったとき、決して賠償されることはない。

私のところにあるビル・ゲイツの証明書



ビル・ゲイツからのメッセージ?



なぜ新しいX.509トラストモデルが考えられているのか?

- 元来のX.509のPKIモデルは誰もが認証局からの証明書(そしてX.509識別名)を持っていると仮定しており、証明書の発行先(subject)も依拠当事者(RP)であった。
- よって誰もが識別名(DN)を持っていてそれを知っている。
- 三つの角を持つトラストモデル
- いずれの依拠当事者(RP)はトラストアンカーやトラストのルートと関係性がある。
- クロス認証(cross certification)は依拠当事者(RP)と発行先(subject)が異なる認証局と関連しているとき、他の認証局とのトラストを保証した。

三つの角を持つ (閉じた) トラストモデル

直接的な信頼関係

間接的な
信頼関係

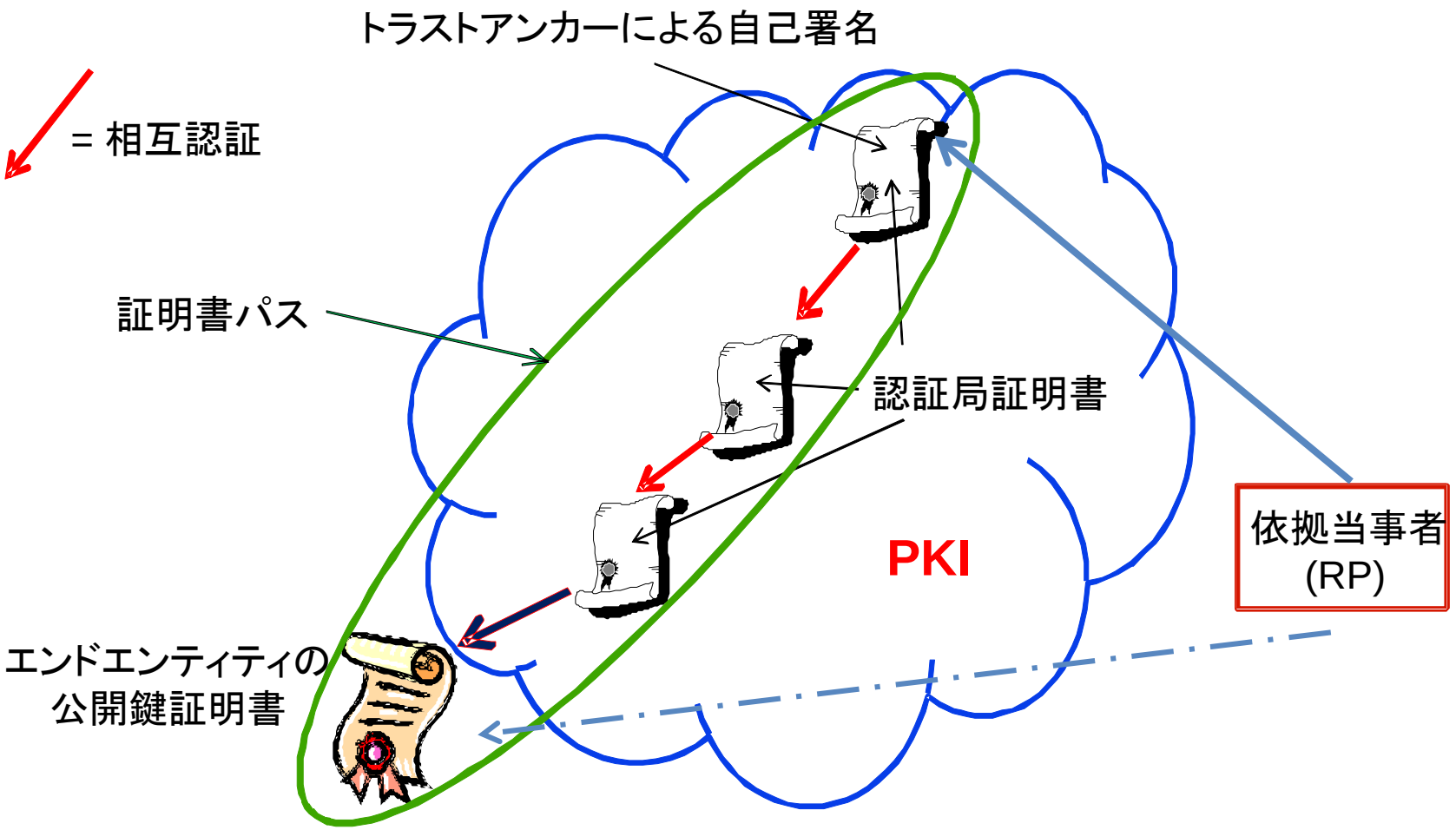
認証局

依拠当事者(RP)

公開鍵証明書

証明書の発行先

証明のパス

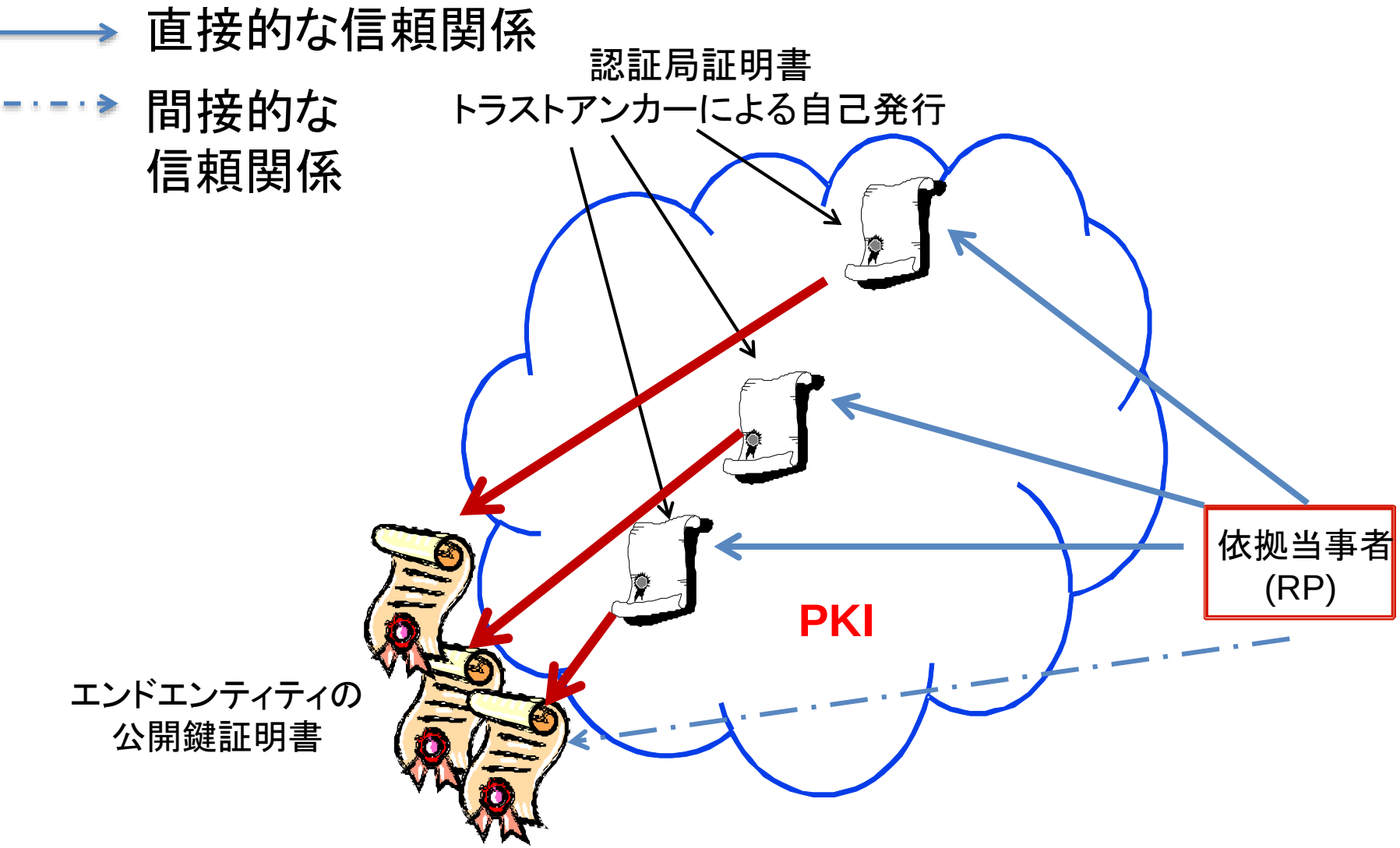


証明のパス

相互認証

- 実際には滅多に/全く行われない。
- トラスト、法律、責任の問題がある。
- 認証元の認証局は認証先の認証局をトラストする必要がある。
- 認証元の認証局が相互認証された認証局の責任を取れば、後者が適切に運用することができなかったり、攻撃を受けたり、ミスをしたときに、認証元の認証局が損害を負担することができる。
- よって弁護士は相互認証は商業上は存続できないことを確信していた。

数多くのトラストアンカー認証局が生まれたわけ



最先端 – 現在のPKI

- 技術的にはX.509 PKIが動き、ユビキタスである
- 最も普及しているPKIの用途は、数百万のWebサーバにおけるセキュアな通信のためのSSL/TLSである。
- しかし多くの依拠当事者（ユーザ）は、証明書を持っておらず、もしくは認証局と関係もない。
- 600以上の商用の認証局が存在している。
  - 多くの異なる国にある
- 依拠当事者はそれらの全てが信頼に足るかどうかをどうやって知ることができるのか?
  - 認証局のCPやCPSを読むのは現実的ではない。
- 依拠当事者は認証局が信頼できなかったり注意不足であったり、侵入されるなどしたときにどう被害をこうむるのか。
  - 正式に認証局と関係がないとき
  - 国境を越えた問題

いくつかの認証局は信頼できない！

- 2011年3月、Comodの地域系列会社の登録局（RA）が侵入され、マイクロソフト、Google、Skype、Yahoo,Mozillaを含む7つのドメイン名が入った9のSSL証明書が発行された。
- 2011年9月、Diginotar CAはハッカーの侵入により少なくとも531の偽装された証明書が発行された後に廃業してしまった。
  - Diginotar CAはオランダ政府向けの証明書を発行していた！
- マレーシア農業研究・開発機関 (DigiCert Sdn. Bhd.) は2011年に鍵が盗まれ、ユーザのPCにスパイ行為が行われるようなマルウェアをインストールする偽のAdobe Flash Updaterが作られてしまった。その認証局の証明書は現在はブラウザにおいて失効されている。
- これらは最近のインシデントのいくつかであり、より多くが存在している。

強制的な証明書作成攻撃

- 政府機関が国の認証局にある組織名が入った、もしくは中間認証局の偽のTSL証明書を発行させる。
- この証明書は法執行による中間者攻撃（MITM攻撃）を行うために使われる。
- ユーザのブラウザは”本物の”サイトからの信頼されたSSL証明書を受け入れ、鍵アイコンが表示される。
- 政府機関はMITM攻撃証明書を使ってデータを復号し、本物のWebサイトに向けて再暗号化する。
- （通信販売の）アリゾナからのパケット解析MITM攻撃のための製品が売られる。

パケット解析の広告の一部

PACKET FORENSICS

Technical Details

Man-in-the-Middle Capabilities

Intercept any communication within Secure Socket Layer (SSL) or Transport Layer Security (TLS) sessions

All Packet Forensics targeting and policy capabilities can operate within the encrypted tunnel

Operational Configurations

In-line with hardware bypass / failsafe

Import any certificate / public key or generate your own for presentation

Availability

Available in firmware releases after August 31st, 2009 for all Packet Forensics platforms

Available under customization program

Packet Forensics 5-Series are the most flexible tactical surveillance devices in the world of IP networks. Designed for defense and (counter) intelligence applications, they are fully-embedded without moving parts and available in a variety of sizes, shapes and power footprints, all customized for the client. In under five minutes, they can be configured and installed in-line without knowledge of existing network topology. **Capabilities include:** Keyword, RADIUS, DHCP and **behavior-based** session identification; filtering, modification and injection of packets; compatibility with existing collection systems. With this modular platform, Packet Forensics creates **mission packages** based on customer requirements. Best of all, they're so cost effective, they're disposable--that means less risk to personnel.

The Internet Cafe

The 5-Series is an ideal solution to the "Internet Cafe Problem." Quick deployment and remote control minimize personnel risk and maximize collection capabilities. Small footprint and minimal power requirements make installation easy.

日本におけるMITM攻撃

GENUINE KENT POP3 CERTIFICATE

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
77:eb:7b:b5:09:24:8c:48:58:a4:4f:96:d1:dd:0d:e0
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=NL, O=TERENA, CN=TERENA SSL CA
Validity
Not Before: Apr 19 00:00:00 2013 GMT
Not After : Apr 18 23:59:59 2016 GMT
Subject: OU=Domain Control Validated, CN=csmail.ukc.ac.uk

MITM KENT POP3 CERTIFICATE

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
57:5f:7e:cd:26:24:8c:48:58:a4:4f:96:d1:dd:0d:e0
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=Certificate Authority, CN=FortiGate CA/emailAddress=support@fortinet.com
Validity
Not Before: Apr 19 00:00:00 2013 GMT
Not After : Apr 18 23:59:59 2016 GMT
Subject: OU=Domain Control Validated, CN=csmail.ukc.ac.uk

責任と対応を取れるのはだれか?

- Fortinetファイアウォール（Fortigate）を使っているホテルやその他のゲートウェイ
  - オンデマンドでリモートのSMTPとPOP3サーバに成りすます証明書が作成される場合
- しかし確かなことは知りようがない。

RPはどのように運用されるのか?

- ブラウザメーカーはCAが信頼できることの検証において全てのユーザの代理をおこなう。
- ブラウザベンダーは、信頼されるルート認証局のみをトラスト・ストアに入れるべきである。
- ブラウザベンダーはWebサイトの証明書を検証する前に失効情報をチェックすべきである。
- ブラウザベンダーは、鍵用途（key usage）のようなすべての証明書のポリシー情報をチェックすべきである。
- ブラウザベンダーは信頼されないルートや中間認証局証明書をトラスト・ストアから削除するべきである。
  - APT（標的型攻撃） FlameやStuxnetなどで使われるMD5のルート証明書がまだある。
- ブラウザベンダーは間違いや何かをブラウザベンダーが怠ったことによってユーザがこうむった損害に責任を持つべきである。
- ブラウザベンダーがやる?
- ご覧下さい：Ahmad Samer Wazan, Romain Laborde, David W Chadwick, François Barrere, AbdelMalek Benzekri. “Which web browsers process SSL certificates in a standardized way?” 24th IFIP International Security Conference, Cyprus, May 18-20th, 2009

RPはどのように運用されるのか?

- ブラウザメーカーはCAが信頼できることの検証において全てのユーザの代理をおこなう。
- ブラウザベンダーは、信頼されるルート認証[illegible]トラスト・ストアに入れるべきである。
- ブラウザベンダーはWebサイトの証明書を検証する前に失効情報をチェックすべきである。
- ブラウザベンダーは、鍵用途（key usage）のようなすべての証明書のポリシー情報をチェックすべきである。
- ブラウザベンダーは信頼されないルート証明書や中間認証局証明書をトラスト・ストアから削除することができる。
  - APT標的方攻撃[illegible]Stuxnetなどで使われるMD5のルート証明書がまだある。
- ブラウザベンダーは[illegible]や何かをブラウザベンダーに送ったことによってユーザがこうむる[illegible]害に責任を持[illegible]。
- ブラウザベンダーがやる?
- ご覧下さい：Ahmad Samer Wazan, Romain Laborde, David W Chadwick, François Barrere, AbdelMalek Benzekri. “Which web browsers process SSL certificates in a standardized way?” 24th IFIP International Security Conference, Cyprus, May 18-20th, 2009

NO

他の選択肢は?

- 信頼される第三者「トラスト・ブローカー」の導入　－　証明書検証を行うRPとして動作
- RPは、証明書検証に関する保証とトラストの判断に誤りがあった場合の補償を提供するトラスト・ブローカー(TB)と契約関係を持つ。
- トラスト・ブローカーは認証局のCPやCPSを読み、認証局がどの程度信頼でき、証明書がどのような用途に使うことができ、認証局がどんな責任を持つのかを決定する。
- ４つの角を持つトラストモデルとなる。
- 理論的な根拠とモデルを以下で説明:
- Ahmad Samer Wazan, Romain Laborde, François Barrere, Abdelmalek Benzekri, David W Chadwick. "PKI interoperability: Still an issue? A solution in the X.509 realm" Proc 8th World conference on Information Security Education, New Zealand July 2013

トラストの評価

直接的な信頼関係

間接的な信頼関係

トラストブローカー

認証局

4つの角をもつ (オープンな) トラストモデル

依拠当事者（RP）

公開鍵証明書

証明書の発行先

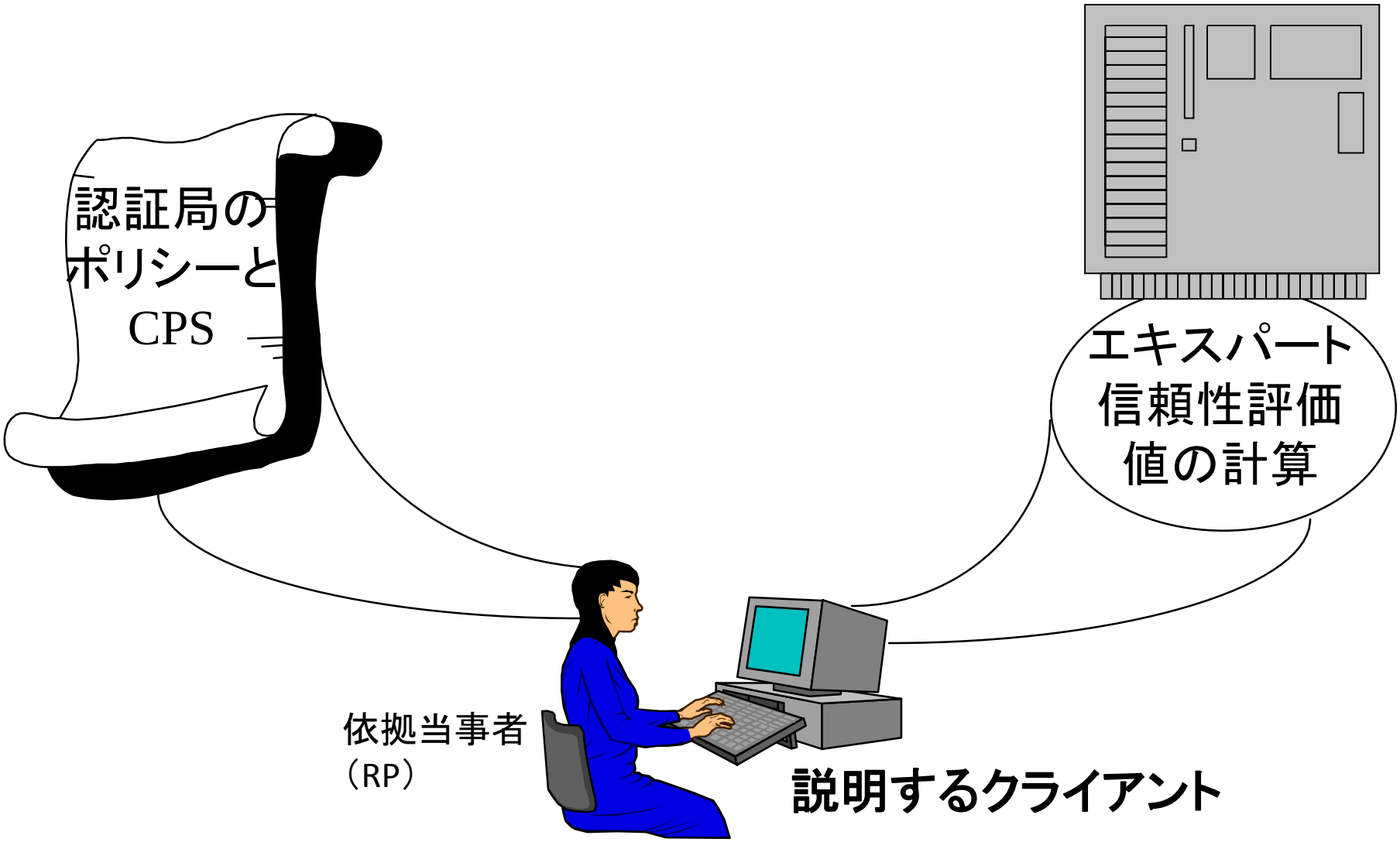
新しいX.509トラストモデルはすべてを解決はしない

- RPとトラスト・ブローカーの間の標準化された通信プロトコルが依然必要になる。
- プラグインかWebブラウザそのものによるトラスト・ブローカーのサポートが必要になる。
- 企業化がトラスト・ブローカーのサービスを確立できるような利益を確保できるビジネスモデルが必要になる。
- これらはすべてITU-T X.509のスコープ外である。

認証局における信頼性の評価

- トラストのインテリジェント評価プロジェクト
  - 1998年1月から2000年12月にイギリスで行われた。
- CP/CPSに基づいたトラスト指数を算出するエキスパートシステムの構築
  - KBS（知識ベース）に展開するために国際的に15のエキスパート（組織） (inc. Chokhani, Ford, Kent ほか)
- 依拠当事者（またはトラストブローカー）が、認証局のCP/CPSに基づく知識ベースを使った質問に答えることができる。

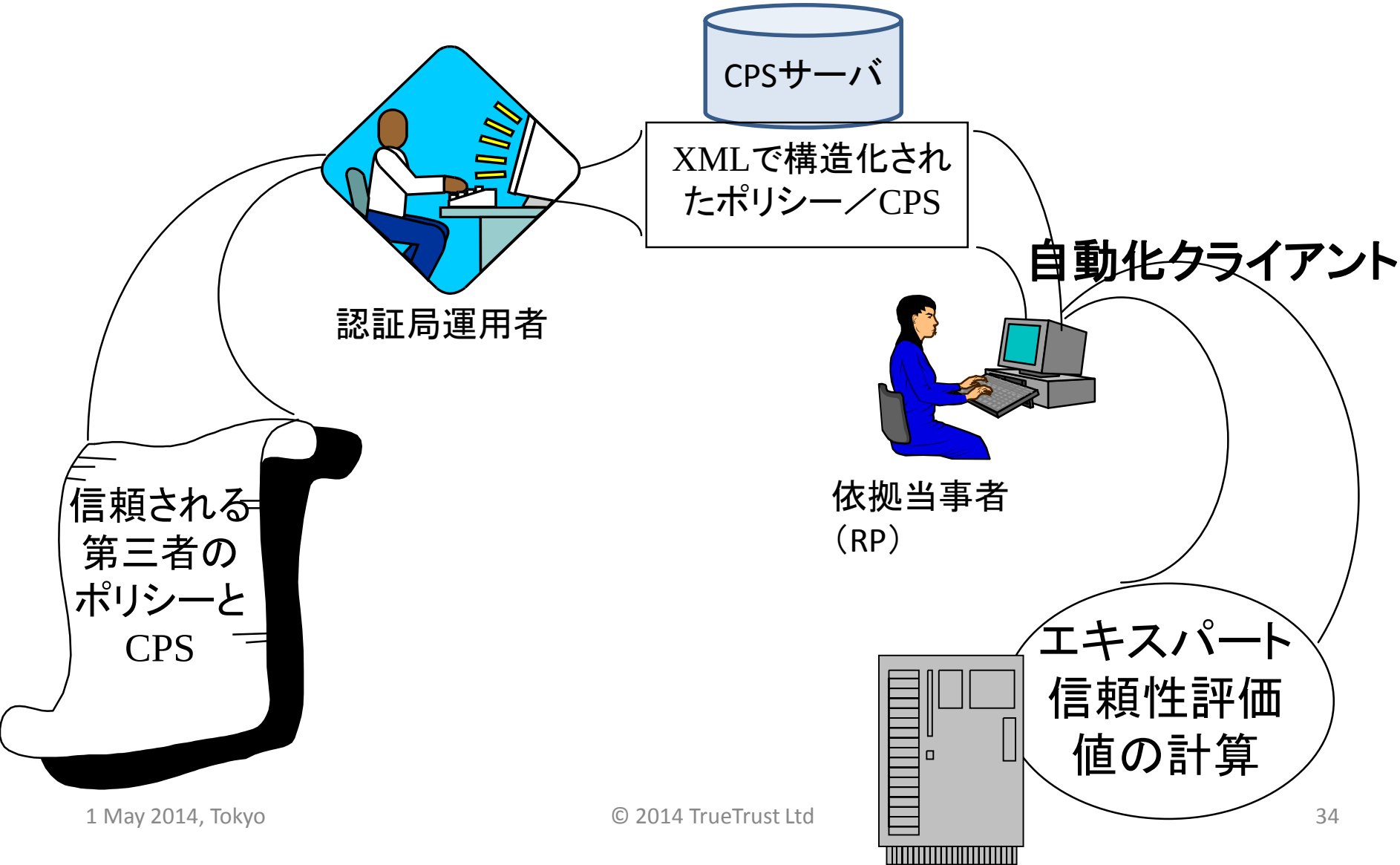
動作のモード:方式1



自動化に向けたシステム

- このオリジナルのシステムは時間がかかってしまい、間違いが起きやすい、そのため
- CA/CPSをXML形式に変換して処理しやすくし、CPSのサーバに格納する。
- 知識ベースに投げかけられる質問に自動的に答えが見つけられるようにパーサー（文章処理プログラム）が情報を展開できるようにする。

動作のモード：方式2



まだ十分ではないため

- この状態は認証局自身がどう信頼できるのかを**公表しているか**に基づいて指数が計算できるだけである。
- 実用的にできることではない。
- そこで、認証局の監査人によって発行される監査証明書（XMLで）を定義した。
- またトラスト・チェック・サーバを提案している。
  - 認証局のCRLを入手して発行頻度をチェック
  - 監査証明書を入手してCP/CPSへの準拠性をチェック
  - 実際のトラスト指数を算出

X.509 (2016)で挙げられているその他の変更点

- 文章の整理
  - 間違いや不一致を削除したり説明の良くないところを入れ替え
- X.509からPKIやPMIでない部分を削除
  - “directory authentication specifications”をX.509からX.511に移動
  - パスワードポリシー仕様をX.509からX.511に移動
  - パスワードポリシースキーマをX.509からX.520に移動
- PKIとPMIを明確に分けて異なるセクションに配置
  - 8月13日に属性証明書（AC）と公開鍵証明書が同じCRLに現れうる文章について修正レポート
- 使われておらず重複しているASN.1データ構造を削除
  - certificationPath, forwardCertificationPath and crossCertificate (代わりにpkiPathが使われる)

2014年公開のX.509におけるその他の修正

- 異なるバージョンにある異なる書式があるIDP（issuing distribution point）拡張の問題 (DR 398)
- 証明書リストのバージョン構成と、それがない場合のバージョンについての不明瞭な仕様 (DR 397)
- PKIX仕様に合う必要のある、トラストアンカーに関する不十分な説明 (DR 394)
- expiredCertsOnCRL X.509拡張の不明瞭な文章 (DR 393)
- 証明書種別と失効リスト。属性証明書と公開鍵証明書、もしくはその両方の失効について、いつ標準として述べられるかを明確化するための大きな修正 (DR 391)
- X.500の修正の全リスト

http://x500standard.com/index.php?n=Ig.DefectReports

その他のX.509活動

- PKIプロファイル
  - スマートグリッド
  - 無線LANのPKI (WPKI)
  - クラウドコンピューティング
- Cryptographic Message Syntax (CMS)
  - 使われなくなったすべてのASN.1の構造を削除してASN.1の標準化されたエンコードルールで使えるようにする。
- PKIの確立のプロセスとメンテナンス
  - マシン to マシンのやり取りにおける、巨大なPKIのネットワークのため
- 保証されたメール伝送と保証されたPost Office Protocol
  - 郵便と同等なものの電子化

ISO/IEC JTC1/SC27

- 新たなスタディ・グループ：2013年4月に開始した Framework for PKI Policy / Practices / Audit
- 委託等取り決め事項（Term of Reference）: マネージメント、運用、評価、保証レベルの異なるPKIのトラスト・サービス・プロバイダの認証への、相互運用性のある開発と標準化された取り組みに関する評価基準のため
- 最初のフォーカスはPKIトラスト・サービス・プロバイダーの監査に関するもの
- 2013年10月24日 韓国・仁川、2014年4月7日～8日 香港、加えてWebExの7回のミーティングが行われている。
- アメリカ（共同議長）、フランス（共同議長）、イギリス、ルクセンブルグ、スペイン、イタリア、ドイツ、韓国とETSIからのインプット

ISO PKIスタディ・グループの成果

- 最終レポートに、TR14516/X.842 (2002)の見直しを始めることの合意
- “Guidelines for the use and management of Trusted Third Party Services”（信頼された第三者サービスの利用と管理に関するガイドライン）
  - TTPサービスの利用と管理のためのガイドラインの提供：基本的な義務や提供されるサービス、TTPサービスの説明と目的、役割と責任のユーザ
  - 複数のTTPへの対応：タイムスタンプ、否認防止、鍵管理、証明書管理と電子公証サービス
- 必要とされていた二つの大きな修正：
  - 1. 認証局のコンポーネントである確かな鍵について、認証局における鍵生成とCPSを含めて取り組まれていなかった。
  - 2. ISO/IEC 2700x シリーズに入れ替わって削除されていたTR 13335 “Guidelines for the management of IT security”への多くの参照を作成
- 提案事項は複数のパートのrecommendationsに入った
  - TR14516-1: TSPの概要とコンセプト
  - TR14516-2: TSPの情報セキュリティに関するTSP-PKIガイドライン
  - TR14516-3: PKIサービスの供給（provision）のためのTSP-PKIガイドライン

IETFにおけるトラスト関連活動

- Certificate Transparency - RFC 6962
  - 証明書における透かし
- HTTP Strict Transport Security (HSTS) – RFC 6797
  - HTTPにおける厳密なトランスポートセキュリティ (HSTS)
- Public Key Pinning Extension for HTTP
  - 公開鍵ピンニング拡張
- Web PKI Operations (wpkops) working group
  - Web PKI運用

GoogleのCertificate Transparency

- 2013年6月 Experimental(実験的) RFC 6962, June 2013
- 全ての発行済み証明書の（追加のみのログである）Merkleハッシュ木を署名つきで持つログサーバを運用。どの認証局でもログサーバに証明書を送り、返答として署名つきのタイムスタンプが得られる。このタイムスタンプは、TLSハンドシェイク中の証明書に付随される。
- 定期的に全てのログサーバをチェックする監視サーバは、許可されていないようなもしくは疑わしい証明書にフラグを立てる。
- 監査者（ブラウザで実行されている）は、ログに証明書とタイムスタンプが現れているかをチェックする。なければそのSSLサイトの証明書には疑いがあり信頼されるべきでないものとする。
- これによってMITM攻撃や強制的な証明書発行攻撃、鍵が盗まれたことによる重複する証明書といったものをなくす。
- 電子フロンティア財団によるソブリン・キー（Sovereign Keys）も同様の考え方で、Web歳との公開鍵を持つ”タイムラインサーバ”を用いる。

IETF Webセキュリティ・ワーキンググループ

- HTTP Strict Transport Security (HSTS)
  - RFC 6797, 2012年11月
  - WebサイトがHTTPSでのみ通信できること宣言できる
  - HTTPレスポンスヘッダーにはサイト・セキュリティ・ポリシーが含まれる
  - ブラウザはポリシーを記憶しており厳密に行使
  - これによって、信頼されていないWebサイトについてセキュリティ・警告を出すことでユーザの”クリック・スルー”を良くしくする。例：ユーザのクッキーをキャプチャーしておいてユーザに成りすますような、成りすましWebサイトへのリダイレクトなど

- HTTPにおける公開鍵ピンニング拡張
  - WebセキュリティWGのInternet draft
  - HTTPプロトコル拡張により、Webサイトが、ブラウザに特定の期間保持されたホストの公開鍵を”ピン”で留めておくことができるようにする
  - この期間は、ブラウザが”ピン”で留められたものと一致した公開鍵を一つ以上含む証明書チェインの証明書を、ホストに要求する。
  - ホストのポリシーによってサブドメインが含まれることをブラウザに知らせることができる。

Web PKI Operations (WPKOPS) working group

- Webセキュリティの挙動の一貫性を向上させる
- 現在使われているWeb PKIの数百のバリエーションによって起こる問題を特定する。
- Web PKIが実際にブラウザとサーバにおいて、どのように動作し、現在どのように一般的に使われているのかを文書化
  - その元になっているトラストモデル
  - フィールドと拡張の内容の処理
  - 様々な失効スキームの処理
  - TLSスタックがPKIをどのように扱うのか。様々な解釈や実装エラー、ユーザに対する状態変化を含めて
  - ユーザが見ることができ、または制御できる状態変化（ユーザによる判断を予測したり、Web PKIの効果を特定するのに役立てるため）
  - Web PKIがいつ他のアプリケーションによって使われ、そしてその再利用の意味することを特定する
- このワーキンググループで行われないこと
  - Web PKIがどのように動作すべきなのか
  - 発行者における証明書の扱いを確認すること
  - アプリケーションの調査（クライアント認証、ドキュメント署名、コード署名、セキュアメール）

WPKOPS – 進捗状況

- 4つのInternet Drafts公開
  - トラストモデル - draft-ietf-wpkops-trustmodels-00
  - ブラウザの処理 - draft-wilson-wpkops-browser-processing-00
  - 失効 - draft-hallambaker-pkixstatus-01
  - TLSスタック - draft-agl-wpkops-tlsstack-00
- PKIプロバイダへのアンケートを三ヶ月前に配布
  - 7中2つのブラウザベンダーが回答 (Mozilla、Comodo), 2つが回答することを約束 (MS、Google)
  - 15中の1のサーバベンダーが回答 (CloudFlare), 1 つが回答を約束 (MS)、2が回答を拒否 (Oracle、OpenSSL)
  - 67中の20のOCSPプロバイダーが回答
  - 近日中に回答が集まらなければPKIの現状を書いたドキュメント作成は難しい状況

いくつかの興味深い結果

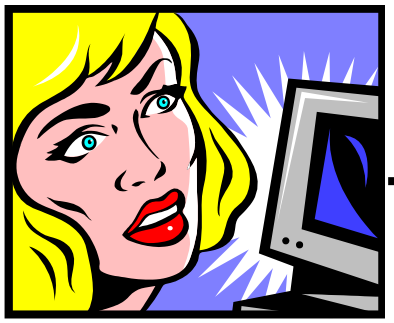
- FirefoxはCRLについてとても限られたサポートのみで、今後なくなる予定
- Chromeは通常CRLのチェックやOCSPレスポンス入手を行わないが、ブラウザに対するソフトウェアアップデートとしてCRLSetsのプッシュを行う。
  - CRLSetsはGoogleの開発したもので、”重要な”CRLの一式を入手しておいて定期的にブラウザにプッシュする。

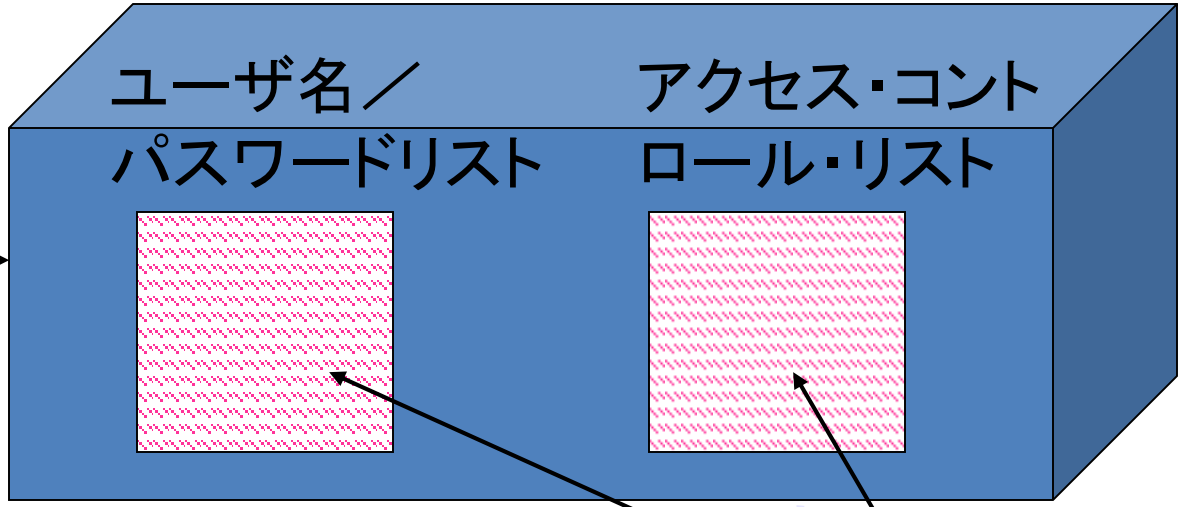
今後に関する考察:
認証（Authentication） or 認可（Authorization）?

- *ほとんどのサービスは、誰が何をすることが許可されているのかを知りたいわけではない。*
- 認証はアクセス制御の最初のステップである。そのユーザが許可されているかどうかを特定することが本質的なゴールである。

伝統的なアプリケーション

- 認証と認可はアプリケーション内部で行われる。
- 弱い認証に基づいているのが典型的





複数のパスワード
複数のユーザ名
わかりにくい!!

複数の管理者
高い管理コスト
包括的なセキュリティポリシーはない

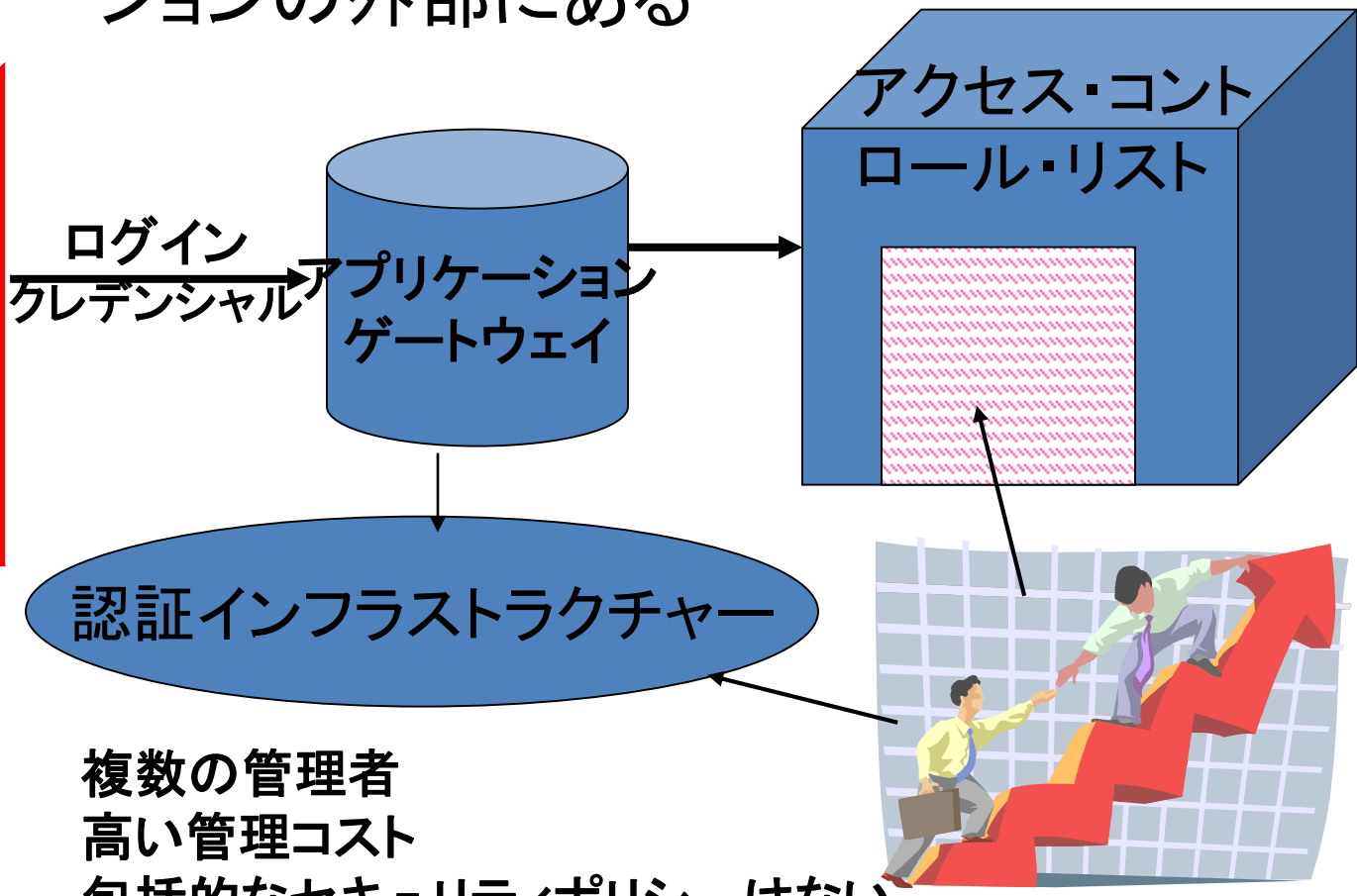
- **コストがかかりがちで、インターネット規模に拡張しづらい**
- しかし外部のエンティティに対するトラストは必要ない。

認証インフラストラクチャー

e.g. PKI, OpenID, Shibboleth etc

- 認証はアプリケーションの外部にある

一つのパスワードか
PINでクレデンシャル
にアクセスできる
幸せなユーザ!



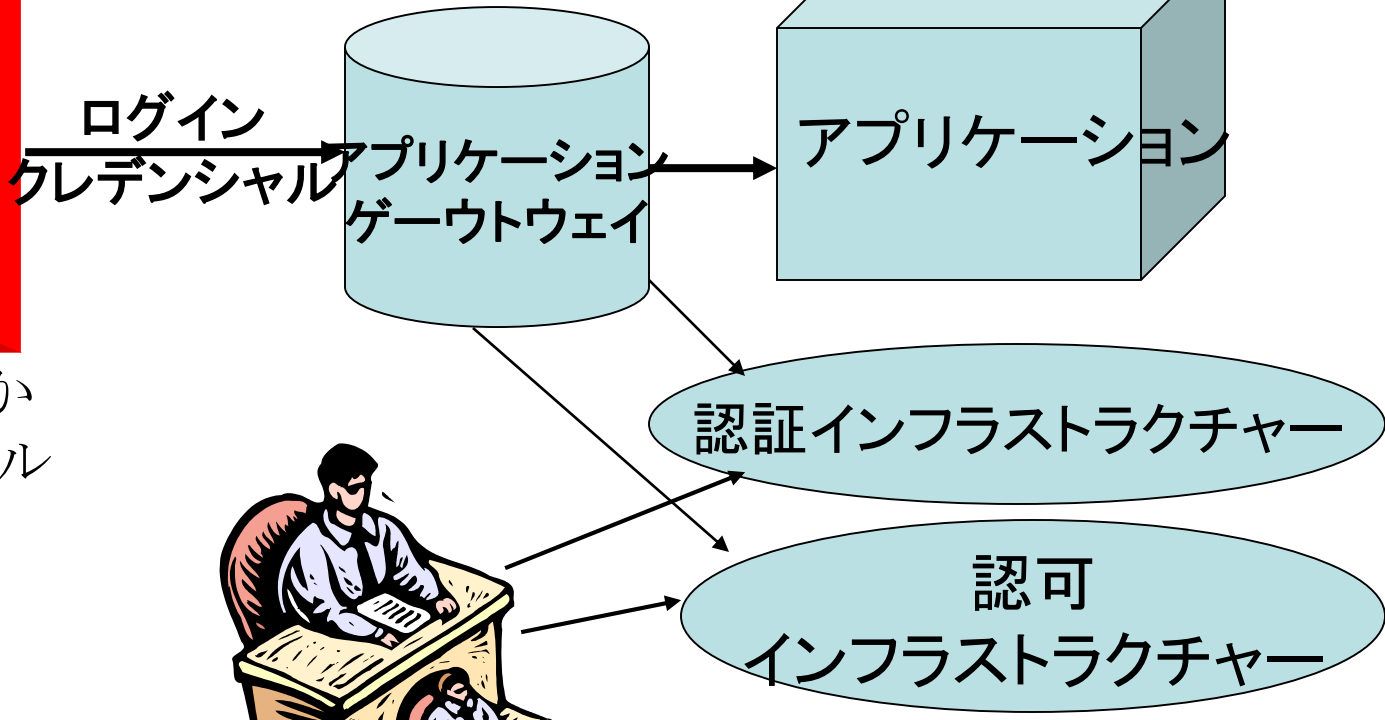
複数の管理者
高い管理コスト
包括的なセキュリティポリシーはない

- **より低いコスト、ただし外部の認証インフラストラクチャーへのトラストが必要になる。**

権限管理インフラストラクチャー

- 認証と認可はアプリケーションの外部にある。

一つのパスワードか
PINでクレデンシャル
にアクセスできる
幸せなユーザ!



少ない管理者
より低い管理コスト
包括的なセキュリティポリシー

- より低いコスト、しかし必要なトラストは最も多い

認可トラストフレームワーク

- PKIと認証トラストフレームワークよりも更に複雑
- きたる時代に向かっていくためにするべきことは多い

ご質問