OpenPGP作法

特定非営利活動法人
フリーソフトウェアイニシアティブ

鈴木裕信

update:2007-05-8

本日の内容

OpenPGPのWeb of Trust方式による信頼確保の方法はオープンソース開発者に広く受け入れられている。一方で電子署名技術の基礎的理解もなく周囲に流されて使っているというケースも多い。OpenPGPのWeb of Trustは草の根的に使える利点がある半面、個々のユーザが使い方を理解し適切な自己判断できない場合には機能しない。一般にOpenPGPというと暗号技術のうちの秘匿性を中心に解説されるが、オープンソースの配布には完全性が重視され、その補完として認証性が使われる場合が多い。そのような状況を踏まえた上で、電子署名の 基本技術から、Web of Trustを実現していくまでのマナーまでを手短に解説する。

高橋メソッド

OpenPGPの Web of Trust 方式

Web of Trust

友達の
友達

電子署名技術の基礎的理解

基礎

すぐに飽きる

- 高橋メソッドを試してみた
- だめだわ、オレに合わない
- 何事も“ほどほど”が良い

暗号技術

- 暗号技術により次の三つの性質を達成することができる
  - 秘匿性
    - 正しい方法でのみ情報を参照できる
    - それ以外には情報は参照できない
  - 完全性
    - 情報がオリジナルであることを保証する
    - 内容を改ざんするとそれを検知できる
  - 認証性
    - 正しい情報を持つ者であることがわかる
    - 正しい情報を持たないものであることがわかる

電子署名技術

- 完全性
  - 電子署名のスキーム
- 認証性
  - 認証モデル

SchemeとPrimitive

- Scheme
  - １つのことを実現する枠組みレベルのアルゴリズム
  - さらに基本的なアルゴリズムから構成される
- Primitive
  - 基本的なアルゴリズム

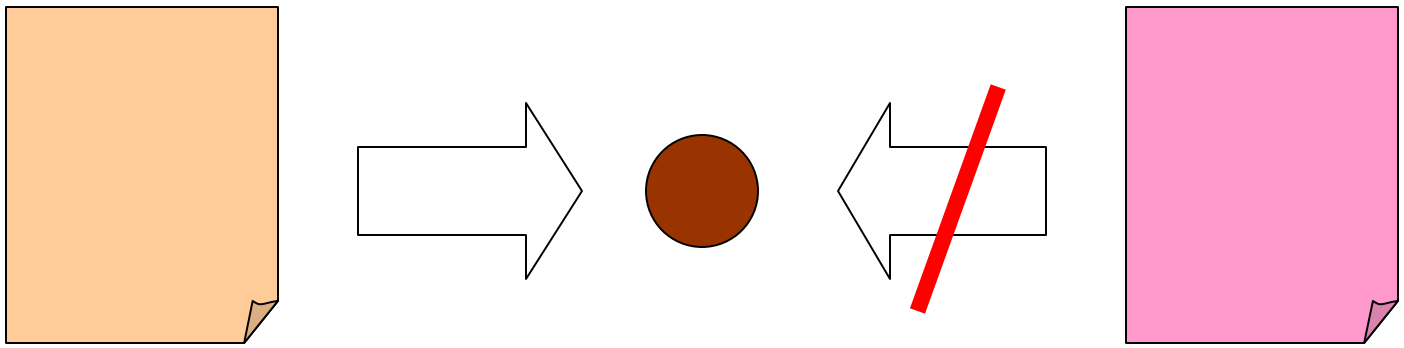
Digital Signature

CRYPTRECだとモジュールと呼んでいる

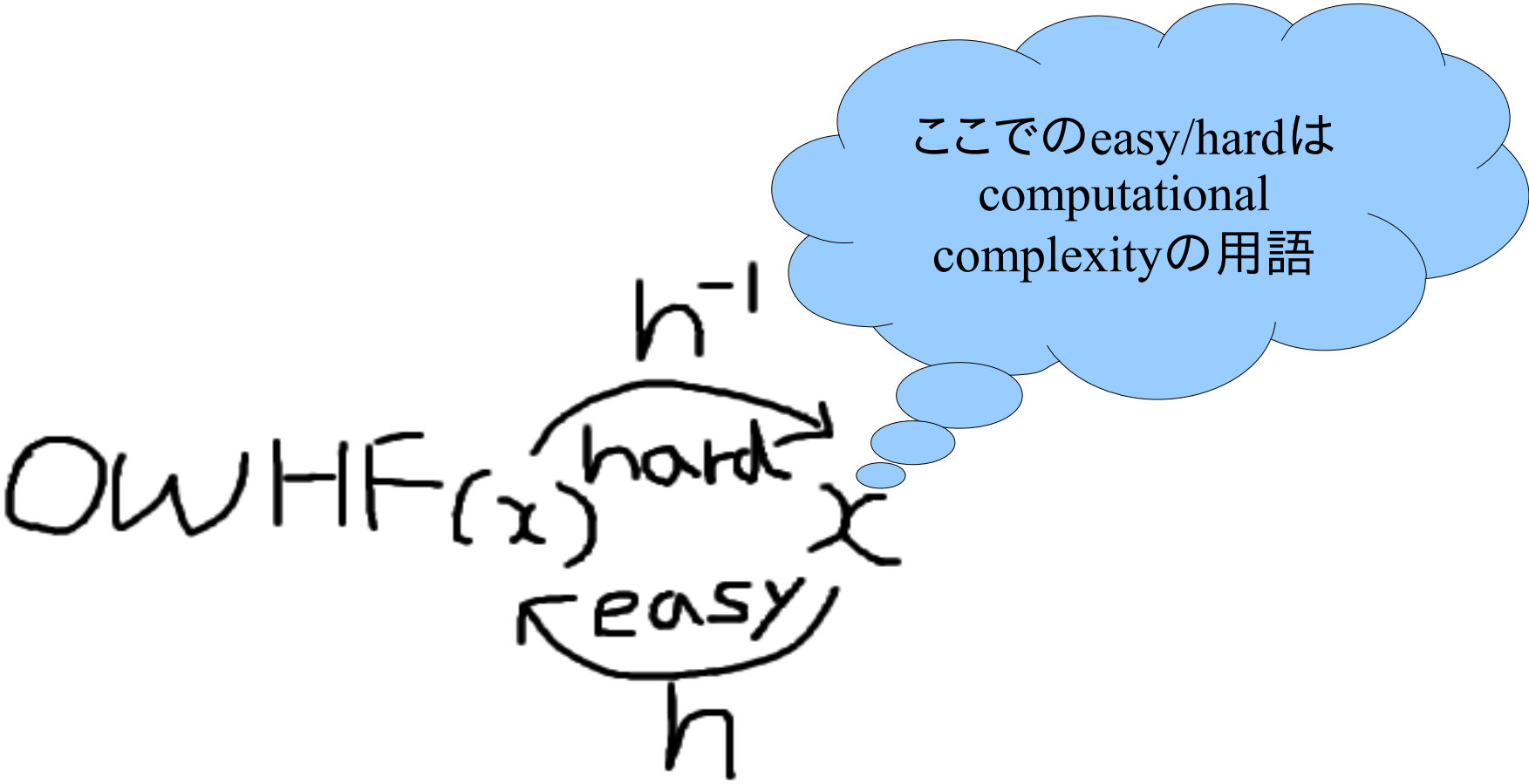
- Digital Signature (電子署名)はスキーム
  - 一方向性ハッシュ関数はプリミティブ
    - MD5, SHA-1, RIPEMD160, etc…
  - 公開鍵暗号法（計算方法）はプリミティブ
    - Diffie-Hellmanベースの計算法 (ElGamal, DSA), RSAの計算法(RSA)

一方向性ハッシュ関数

- One-Way Hash Function (OWHF)
  - ハッシュ値から元のデータを推定できない
- Collision Resistant Hash Function (CRHF)
  - 異なる入力から目的のハッシュ値を作ることができない



もうちょっと数学的に厳密な表記



もうちょっと数学的に厳密な表記

$$x \neq x'$$

$$P_r[CRHF(x) = CRHF(x')] < \epsilon$$

ignoreできる

公開鍵暗号法の考え方

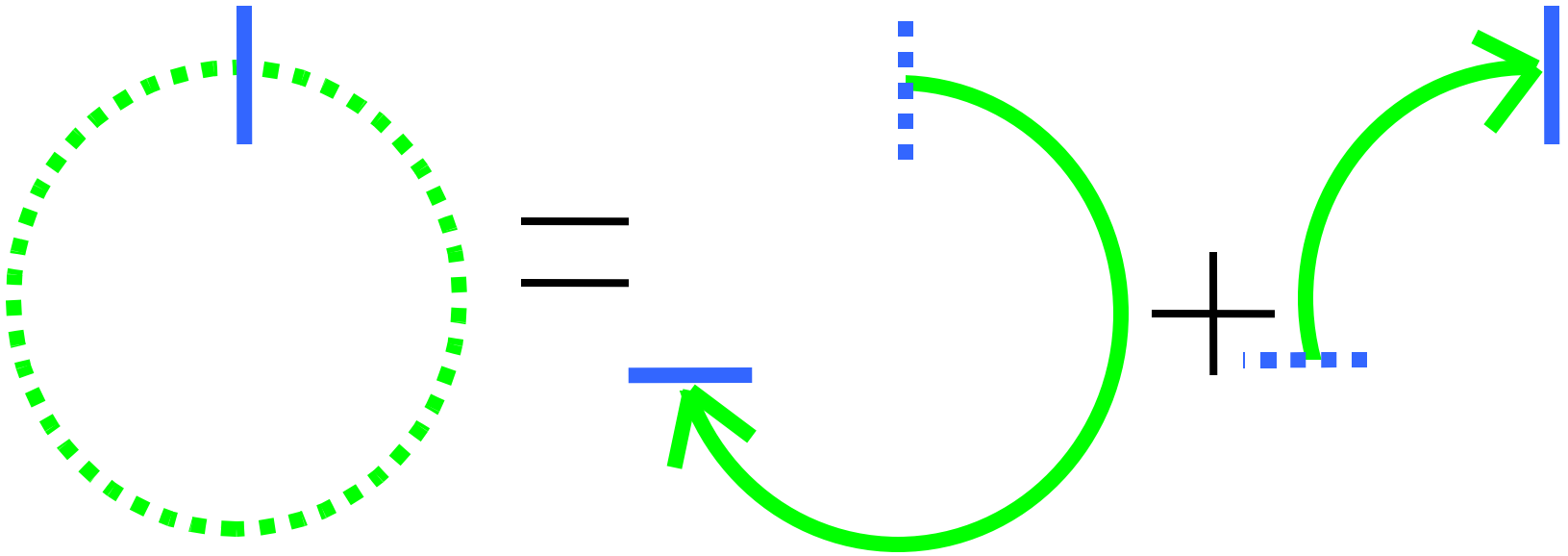
- Trapdoor one way function
  - 一方向にしか計算できないような関数

$$f:\{0,1\}^{l(n)} \times \{0,1\}^{n} \rightarrow \{0,1\}^{m(n)}$$

円(まる)を思い浮かべてみる

- 出発点からある位置まで円周を進む
- ここから出発の位置に戻るのは
  - ~~通ってきた円周を戻っていく~~
  - さらに円周を元の位置になるまで進む

Not trapdoor one way function



pを法とする

7を法とする

$$4 + 6 \pmod 7 = 3$$

$$3^3 \pmod 7 = 27 \pmod 7 = 6$$

正しいパラメータのペア

- 正しいパラメータのペアのみが正しい計算ができる
- それ以外は間違えた答えが出る

パラメタAとパラメータB

- パラメータAを公開鍵(public key)とする
  - パラメータAを検証鍵(verify key)
- パラメータBを秘匿鍵(secret key)とする
  - パラメータBを署名鍵(sign key)

DSA

- Digital Signature Algorithmの略
  - NISTが作ったアルゴリズム
    - DSS (Digital Signature Standard)の1つ
- 安全性は離散対数問題に依存

$$y = g^x \bmod p$$

$x \rightarrow y$ *easy*

$y \rightarrow x$ *hard*

RSAと同じ
hardさ

RSA

gnupgでは
eは通常41

- RSA公開鍵暗号法を署名に応用
- $n=pq$, $ed \equiv 1 \bmod (p-1)(q-1)$
  - e 検証鍵, d 署名鍵
  - 暗号化 $E = M^e \bmod n$ / 復号 $M = E^d \bmod n$
- 安全性はRSA問題（素因数分解問題）に依存

$$n = pq$$

$$pq \rightarrow n \qquad \textit{easy}$$

$$n \rightarrow pq \qquad \textit{hard}$$

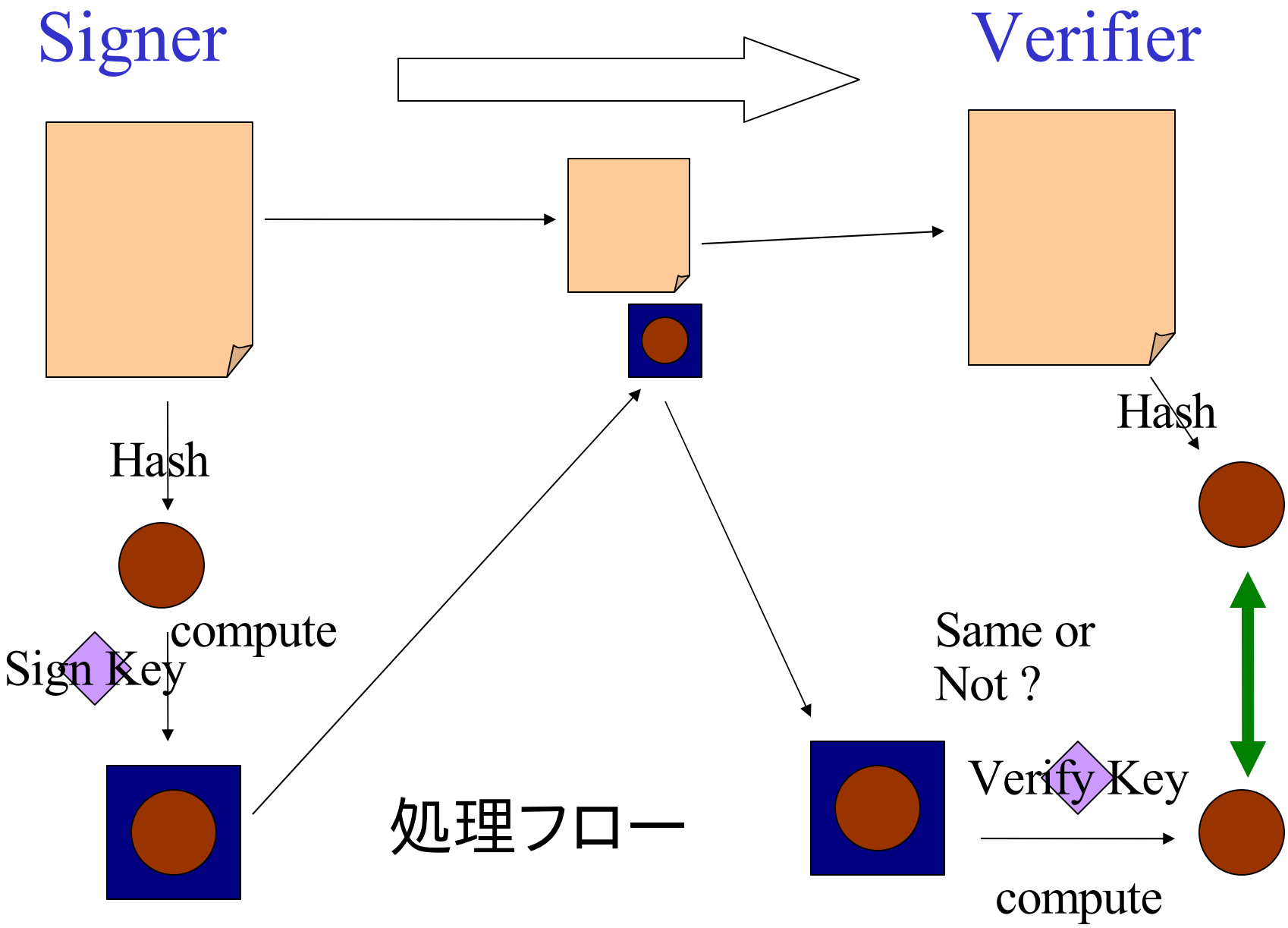
入力すべてに計算するか？

- たとえば1ＭＢのサイズの入力すべてに対して電子署名（公開鍵暗号の計算）をさせるのは非現実的
- ハッシュ値を作りそのハッシュ値に対し署名をかける
  - SHA-1は160bit (20byte)
  - 20byteに対しRSA-1024で検証するとPentium 4-2.4GHzで2-3ms以下

署名鍵と検証鍵

署名鍵で署名したデータは書名鍵と対となっている
検証鍵でのみ正しい値が求められる

- 自分で署名鍵と検証鍵の一対を生成する
- 署名鍵は自分のみ持っている
- 検証鍵を相手に渡す
- 自分の署名鍵でデータを署名する
- 相手に署名したデータを渡す
- 相手は検証鍵で検証する


Signer
Verifier
Hash
Hash
compute
Sign Key
Same or
Not ?
Verify Key
compute
処理フロー

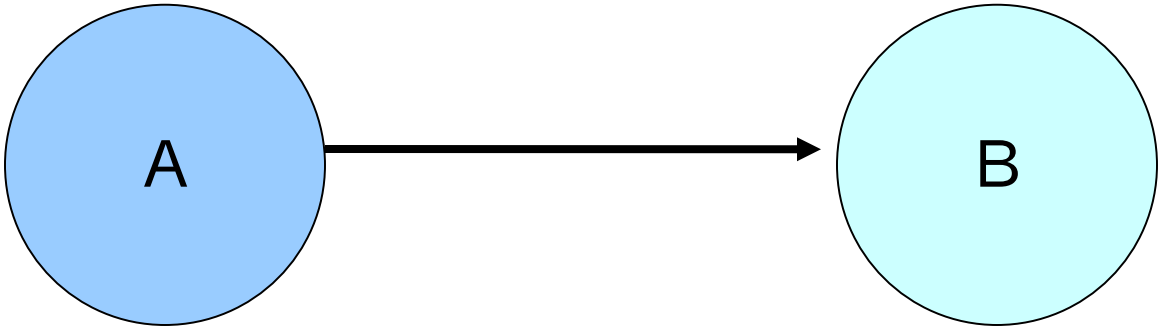
正しい鍵のペアであった

- 完全性は確保した
  - でも、その鍵の持ち主は誰？
  - その鍵に書き込まれている所有者属性なんて、ものは単なるデータ列にしか過ぎない

認証性

- ここでの認証性とは
  - 誰かが誰かだということを示すこと
  - それを確認できること
- 人が人を認証するとゐふこと
  - 人が介在する
    - 計算量云々の問題ではない世界
  - ヒューマンクリプト（by今井秀樹先生）

署名していることと認証とは違う



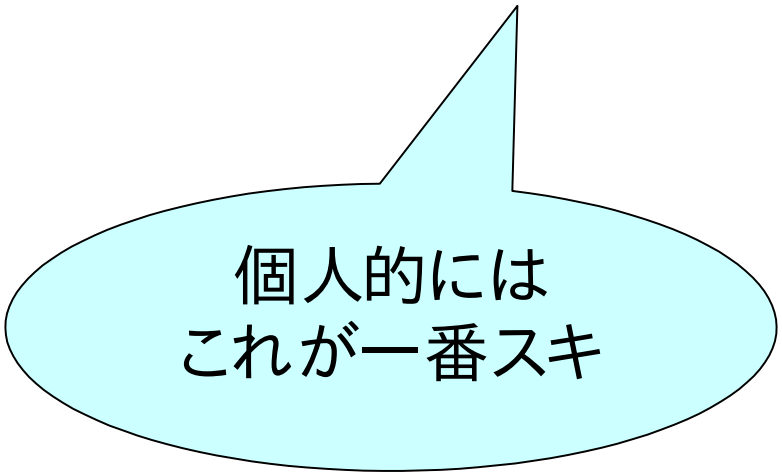
AからBへ署名している

計算可能にしているだけで、それ以上
でもそれ以下でもない

それに意味を持たせるのは人間の行為

認証モデル

- たぶん認証モデルはいくらでも作れる
  - 要は決めの問題
  - X.509, SPKI, Web of Trust, etc



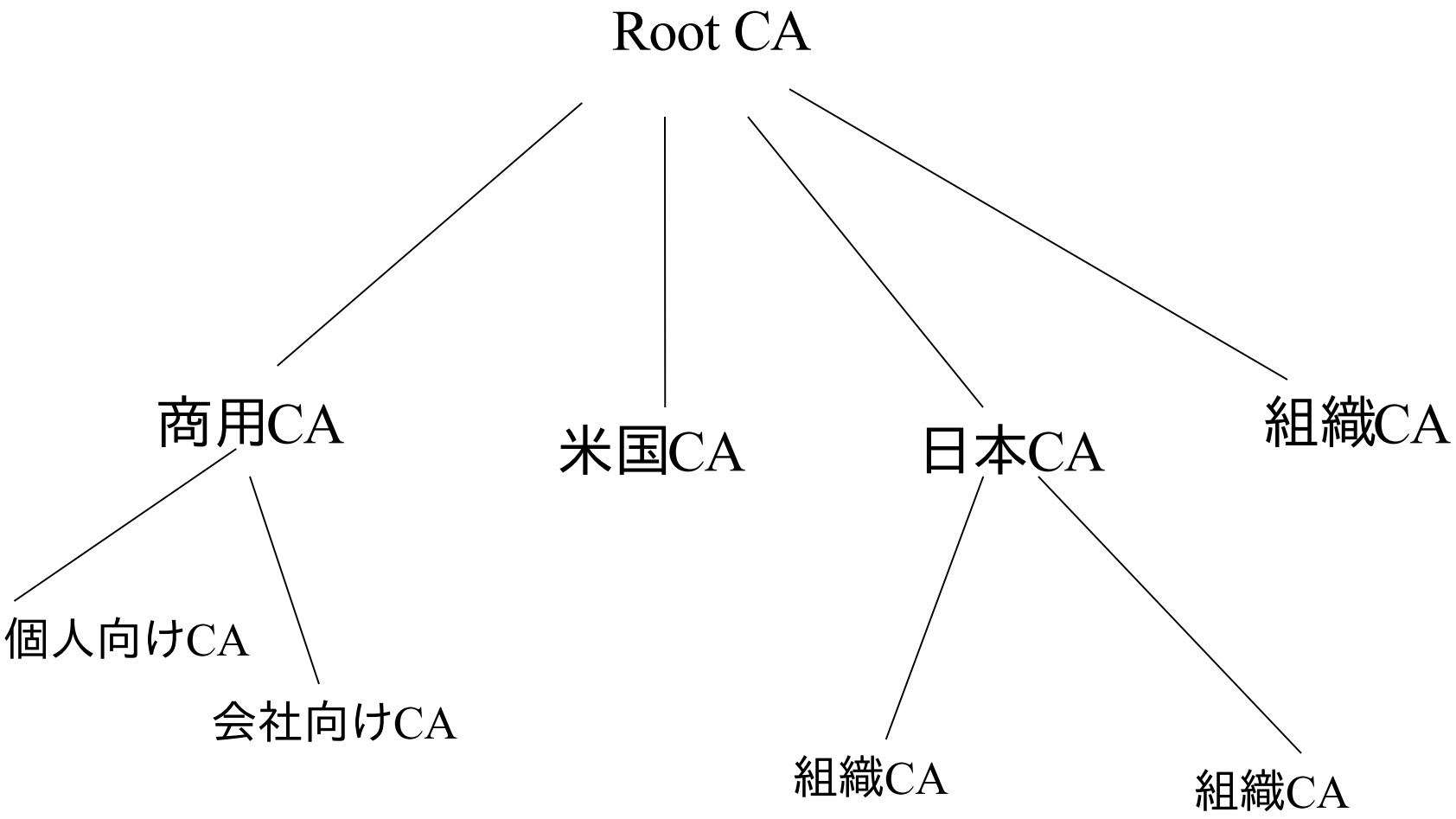
X.509

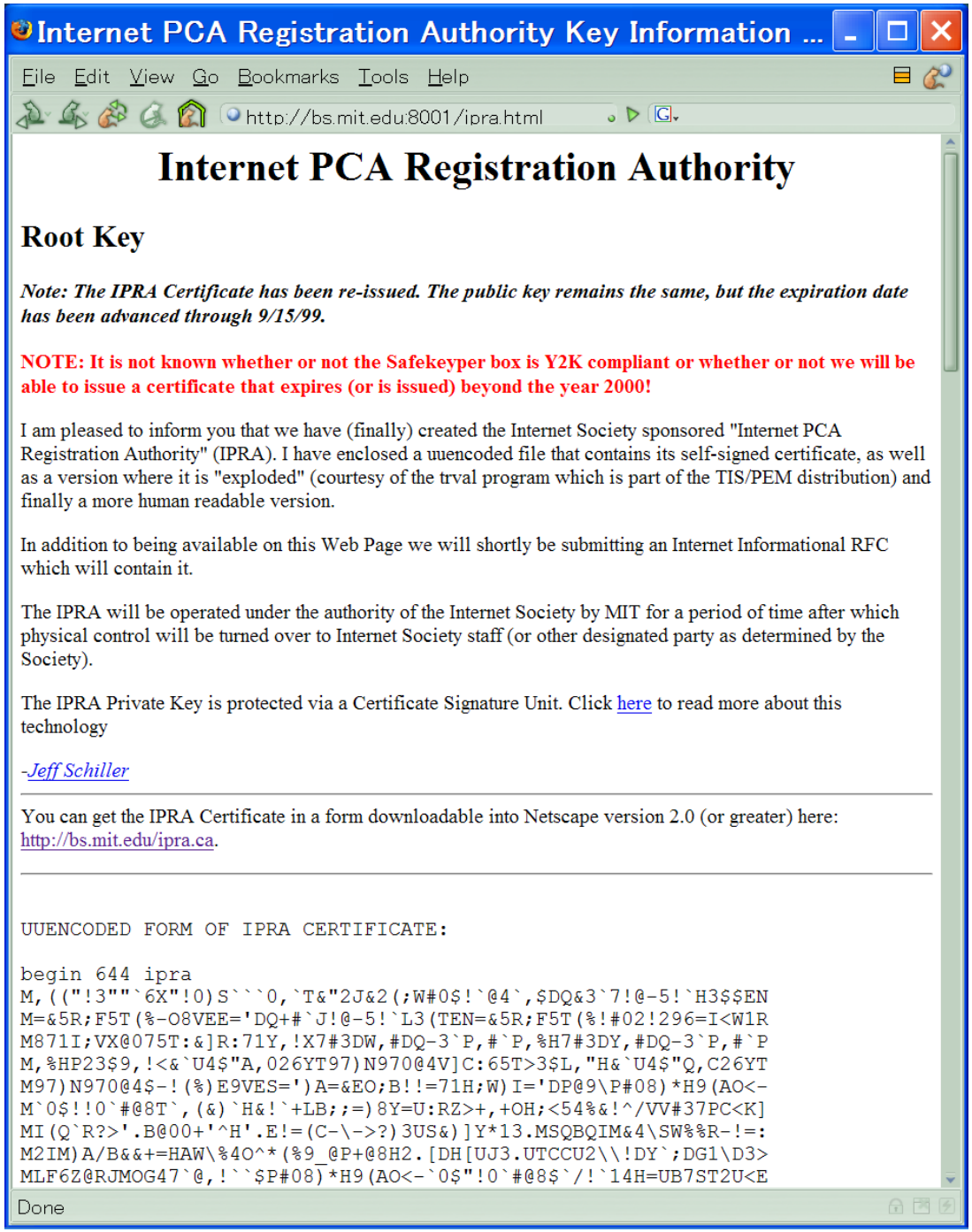
- 電子署名認証のためのモデルとして正式に決められた最初の規格
  - CCITT X.500シリーズの規格だからかなり古い
  - X.500の野望である世界を一つのツリー構造で表現する
    - でも幻想だよこれ

実際のX.509を使った運用

- ISOCのIPRAが実施
  - X.509規格は運用母体などを定義はしていない
  - TIS/PEMのためにRFC1422で認証構造を規定
  - 1994年9月よりに運用
- ルートからツリーで辿れる認証モデル運用
  - 唯一のrootからの本物のツリー構造
    - 親が子を署名して信頼のツリーを作る
  - JIS@MIT.EDUの所でルート鍵を管理
  - 日本では認証実用化実験協議会(ICAT)が日本のツリーの開始ノード

ツリー構造



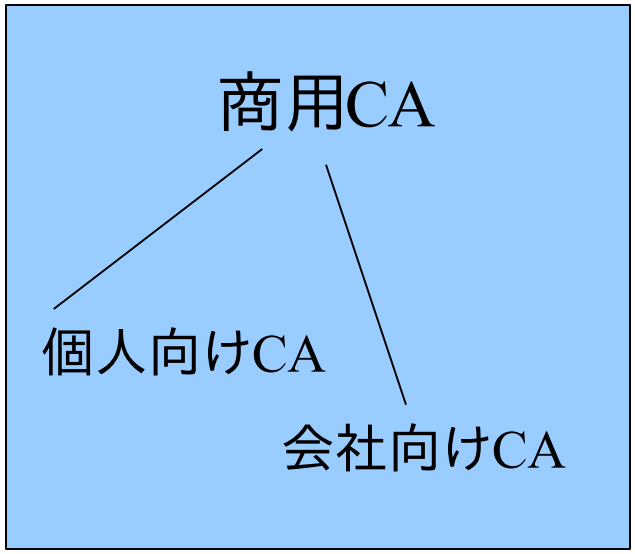


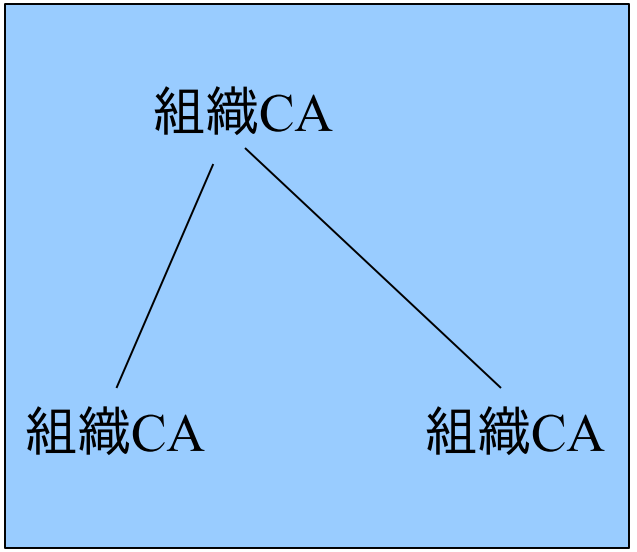
IPRA Root Key

1999年9月15日

- この日をもってRoot CAから辿る認証ツリーは消滅
  - 世界はカオスへ

現在の認証構造





組織CA

組織CA

商用CA

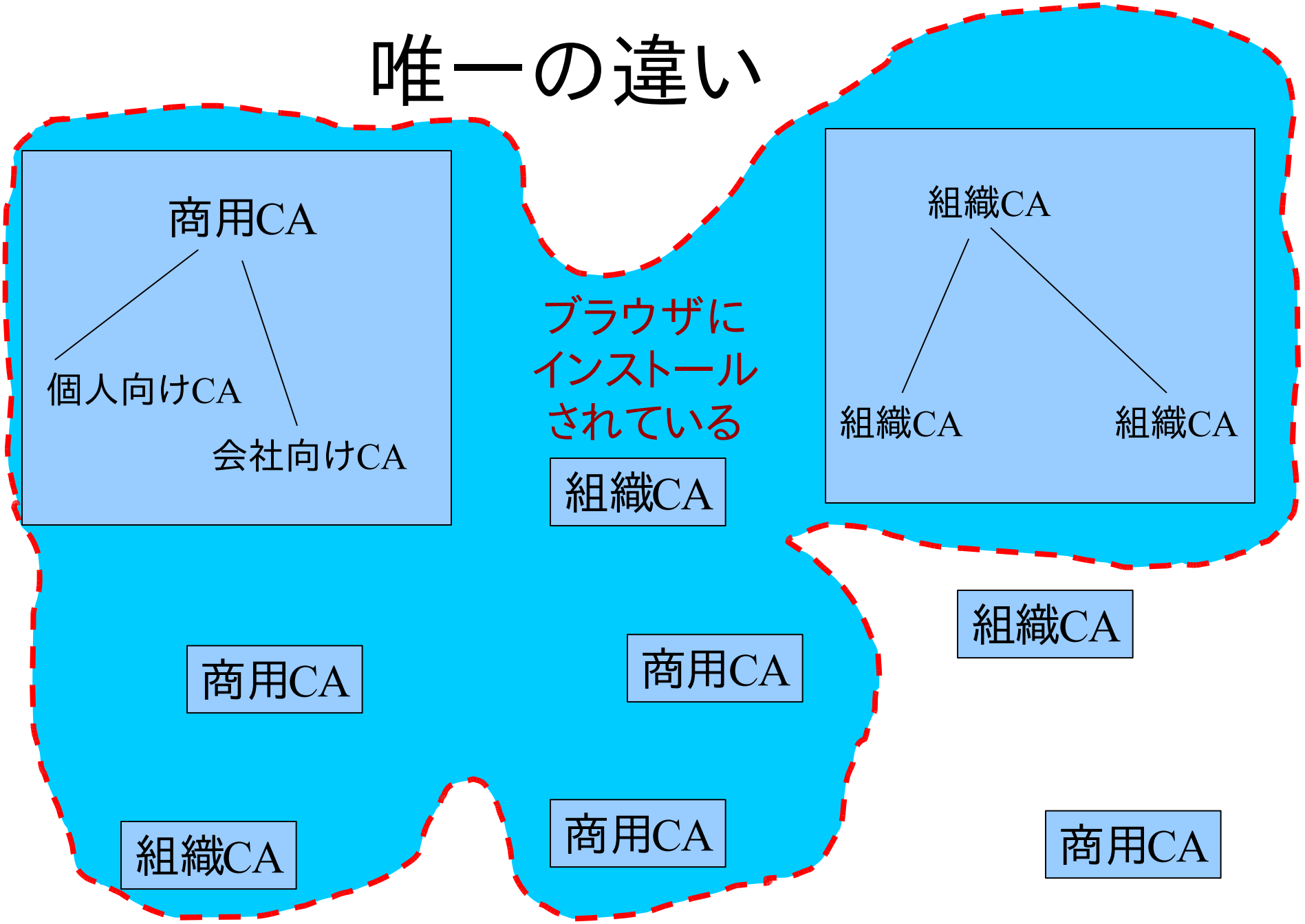
商用CA

組織CA

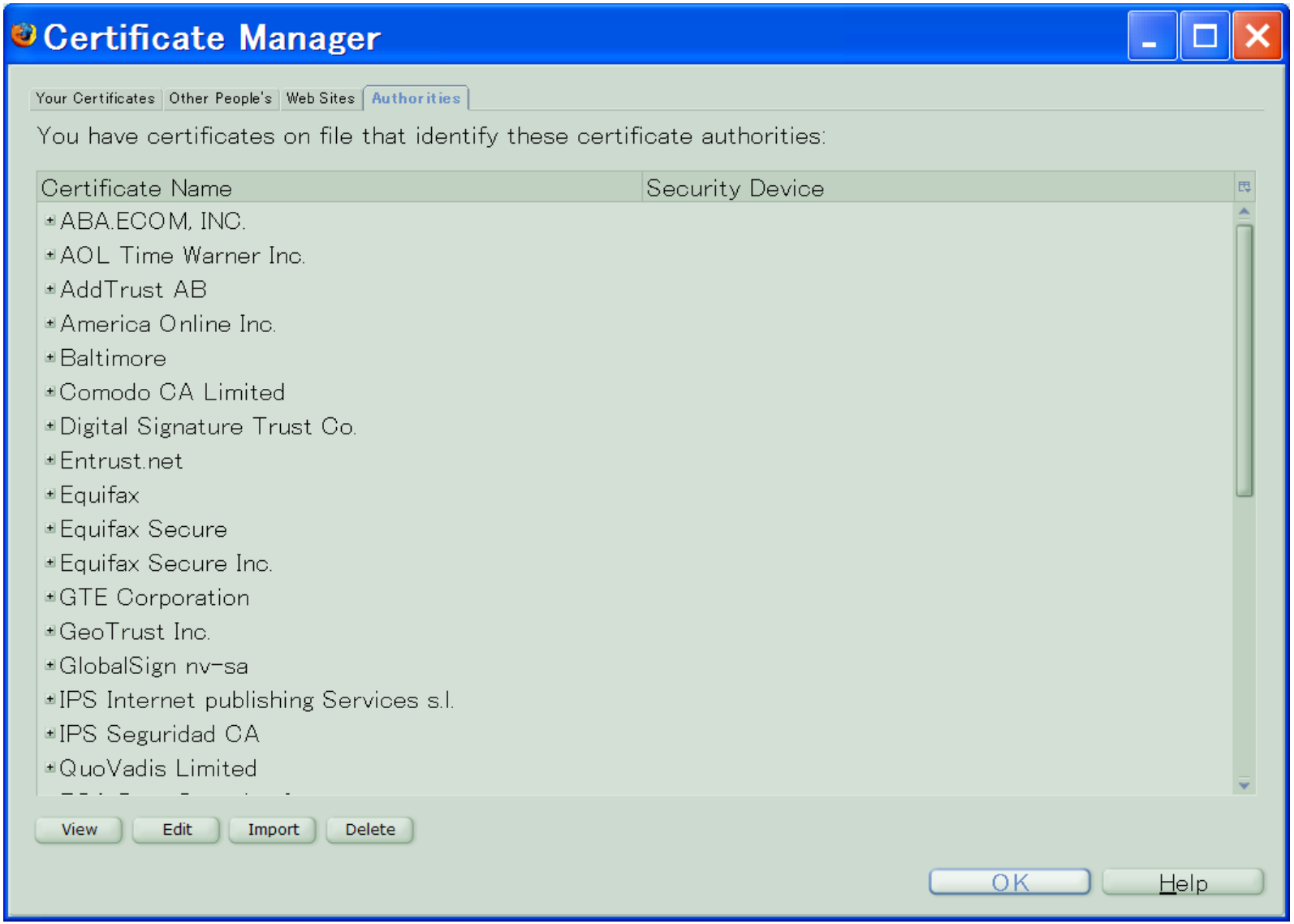
商用CA

商用CA

唯一の違い


商用CA
個人向けCA
会社向けCA
組織CA
組織CA
組織CA
ブラウザに
インストール
されている
組織CA
商用CA
商用CA
組織CA
商用CA
商用CA

ブラウザに登録されているCA



そもそも信用できるの？

- どんな基準で入っているわけ？
- どんな確認をしてCAリストに入れたわけ？
- ブラウザに含まれるCA情報をダウンロードする際に何か確認しているわけ？

思考停止

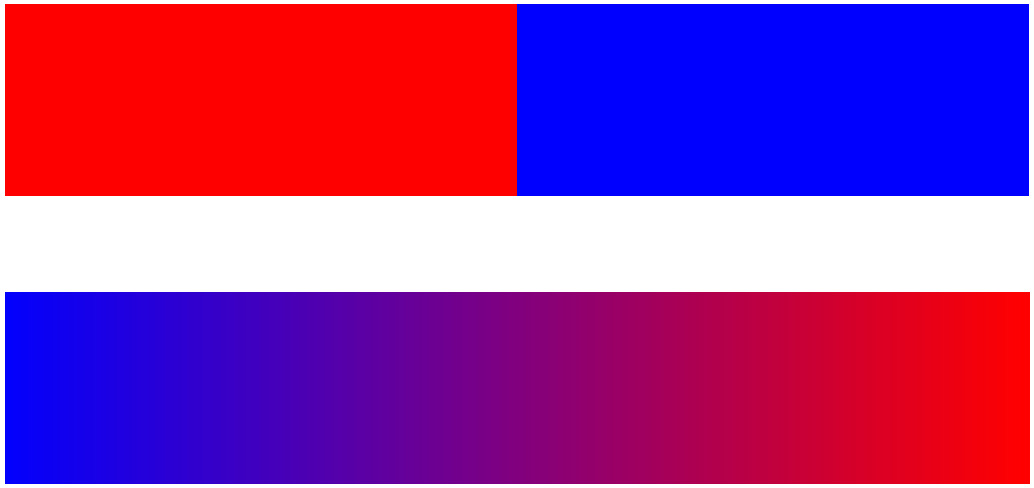
- 正しいものは正しいなぜなら正しいからだ
  - ではそこまで百歩譲りましょう

そこから発行された証明書は正しいの？

- 書類手続きをすればいいだけで、それはいくらでも騙せる方法はある
- 認証を出すところを一箇所騙せばそれでおわり
  - 偽者マイクロソフトに対しマイクロソフトの証明書を出した

あんしん･あんぜん

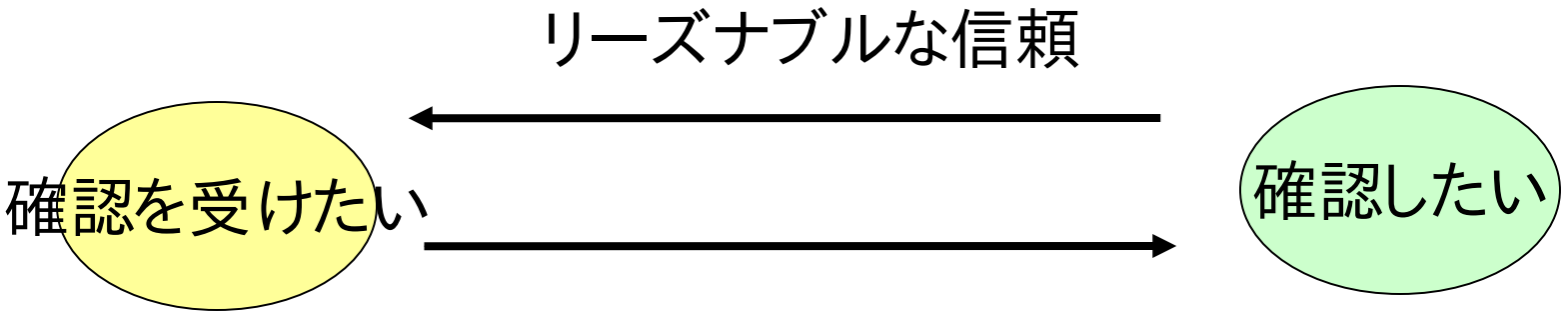
- 所詮は100％なんてものはありえない
- 信用できない･信用できる
  - 単純に二値を取るようなものではない
  - グラデーションのように変化するもの



授信モデルを考えてみる

- 有向グラフを考えてみる
  - 署名する方向を有向グラフと考える
  - どのようなグラフ構造が信頼性が高くなるかなどのクライテリアを考えたりするのは学術的に面白いテーマ
    - 修士論文や博士論文に最適なテーマ
    - まだ誰も発表していないぞ！今がチャンス
      - まだパスを見つけるレベルまでしかやってないぞ！

相互確認

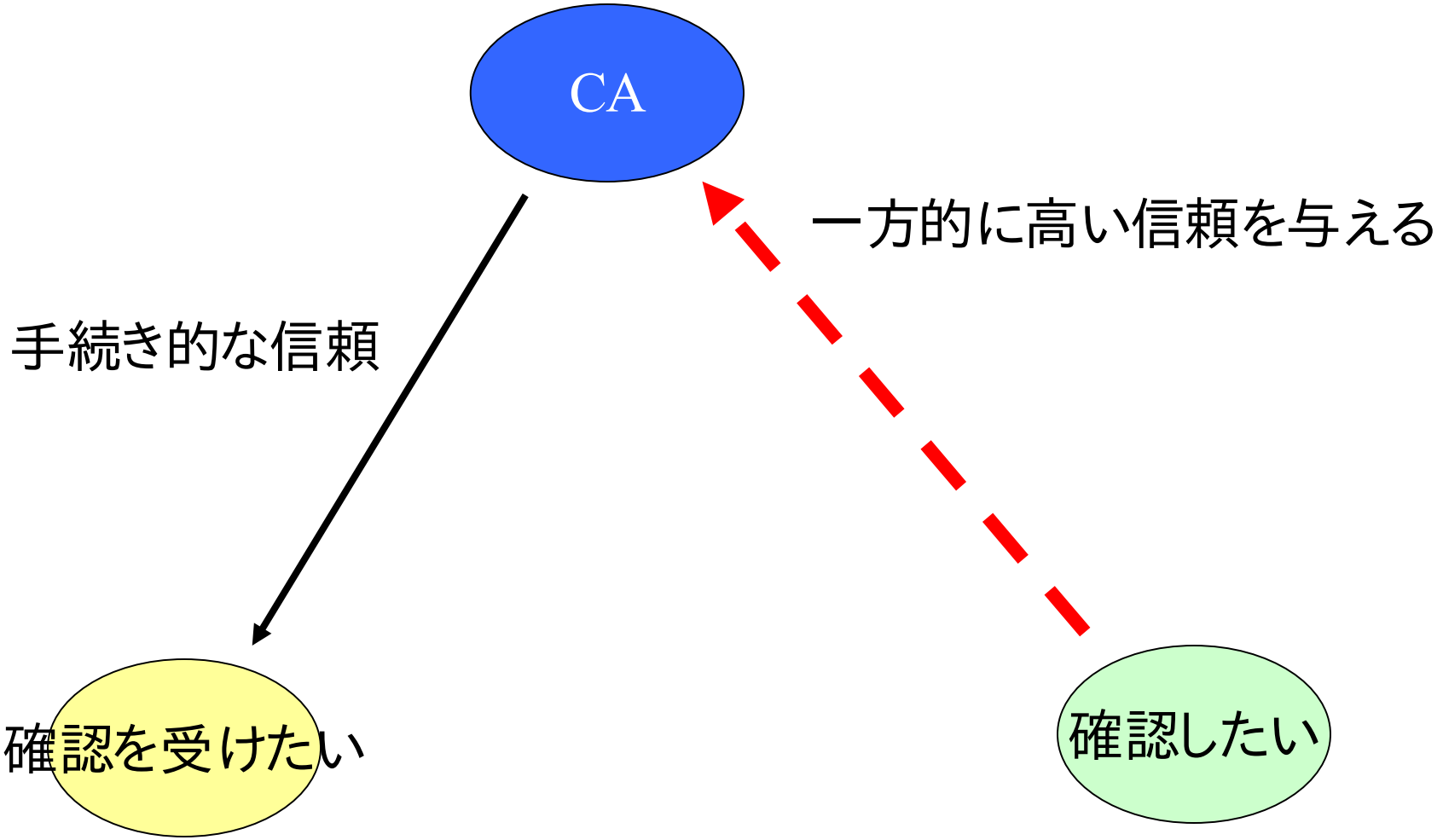


紹介者を使う

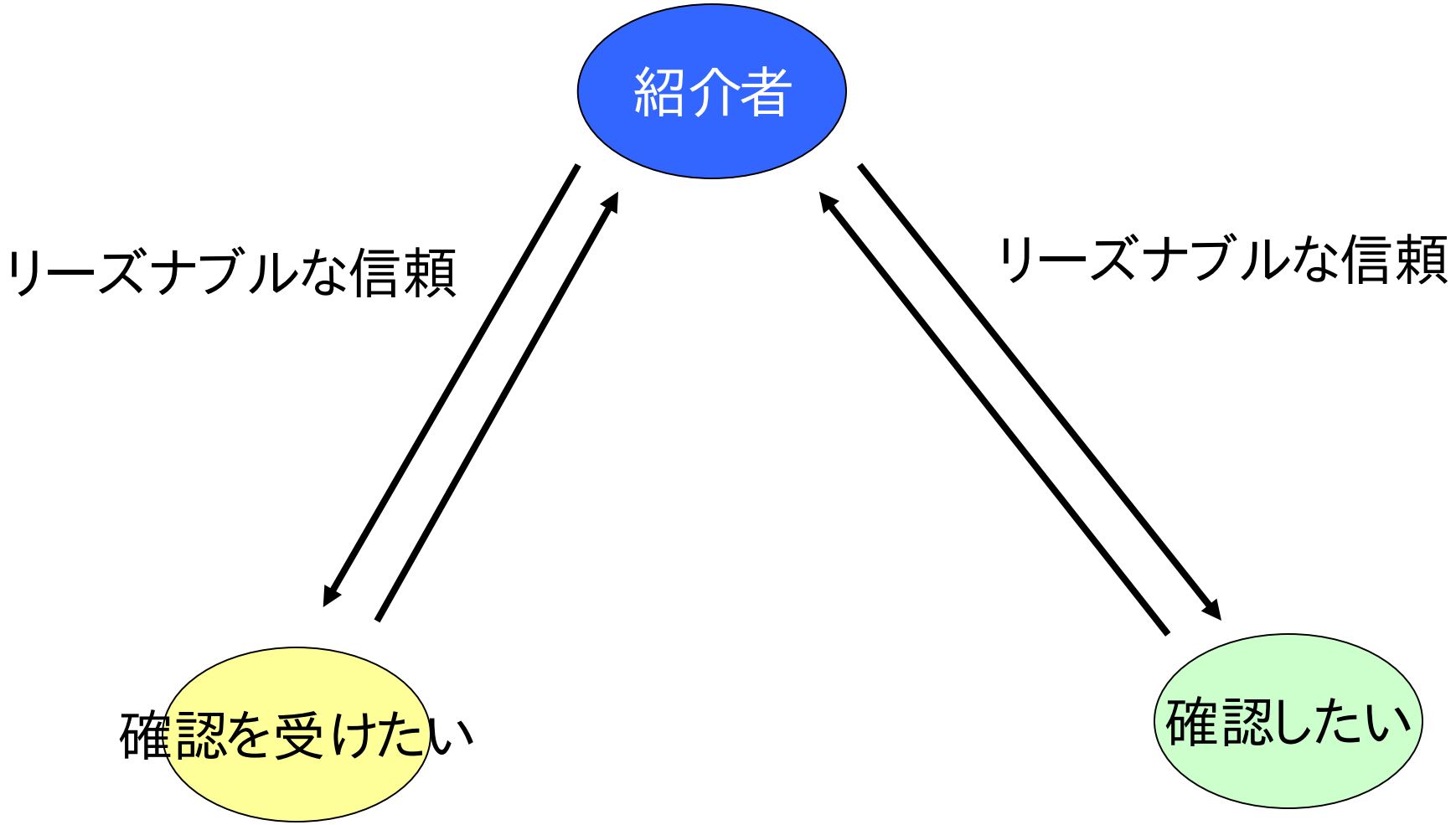
確認を受けたい

確認したい

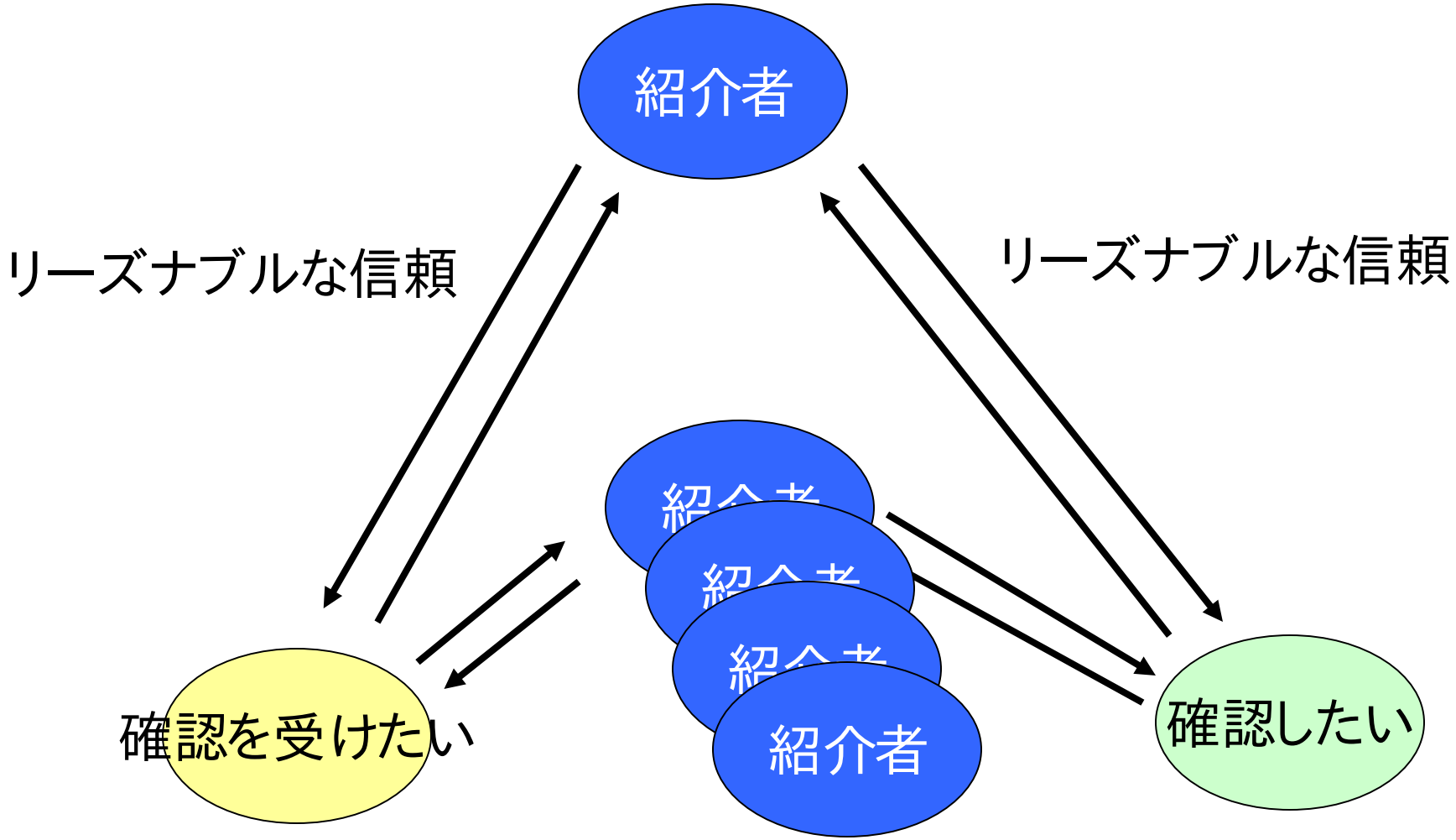
今のX.509の運用



Web Of Trust (simple)



Web Of Trust (multiple routing)



友達の友達は友達

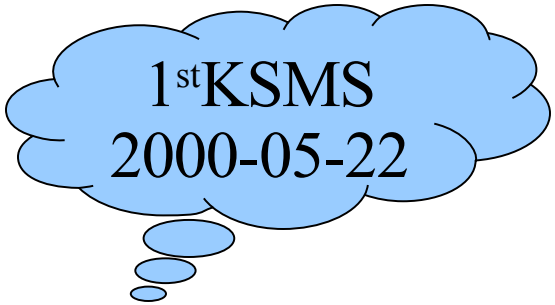
- 信頼のチェーンを使う
- 一対一の場合はとてもわかり易い
- チェーンにした場合、何をどう信頼するかは単純な基準がないので今ひとつわかりづらい
  - 単純に多くのリンクが来ているのが信頼されるわけではない（のは、言わなくてもわかるよね）
  - 自分から信頼できるルートを通って信頼できるようになっているかどうかがポイント
    - そのルート数が増えれば増えるほど偽造も確率的に難しくなる

サードパーティ署名

- 信頼できる手続きを得てサードパーティに署名してもらう
- サードパーティを信頼する人には有効
  - 気持ち的にX.509のCAだと思う人がいるがあくまでもWeb of Trustの一種

```
sig  C368EA31    Boeing CERT <compsec@maple.a1.boeing.com>
sig  71D5F43A    NIIBE Yutaka <gniibe@fsij.org>
sig  2F99027D    Susan B. Levy Haskell <sblh@nts.umn.edu>
```

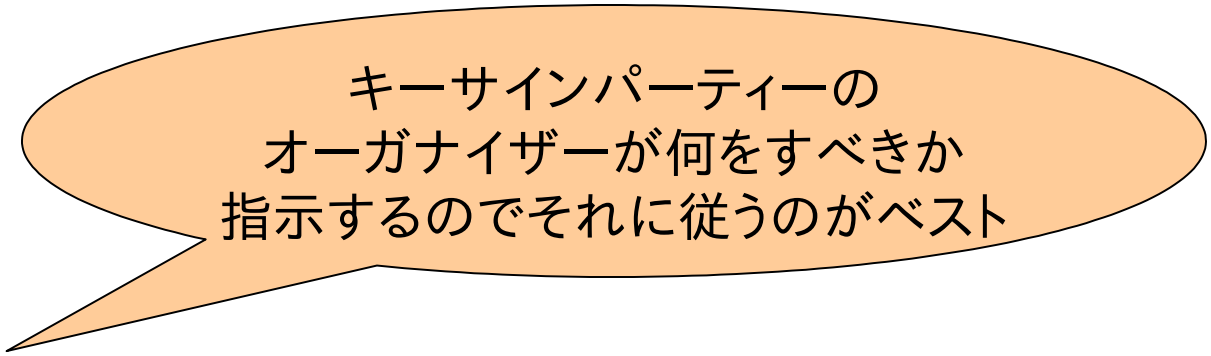
友達づくり



- 親しい友人同士でサインしあう
- キーサインパーティと呼ばれる署名会を開く
  - 全員の鍵と本人確認をして回る
    - $O(n^2)$方式：鍵の情報と本人を確認できるものを持って総当たりしていく
    - 自己紹介もかねているので面白いけどね
  - ササーマン方式
    - $O(n)$方式：最初にリストを作り、本人かどうかの確認を行う担当がいて確認し、リスト上の情報を確認する
    - キーサインパーティーをやったらPGPを開発したPhilip Zimmermannが一番うんざりしていた・「もっと効率の良い方法を考えてくれ」と同行していたL. Sassaman に指示した

チェック･チェック

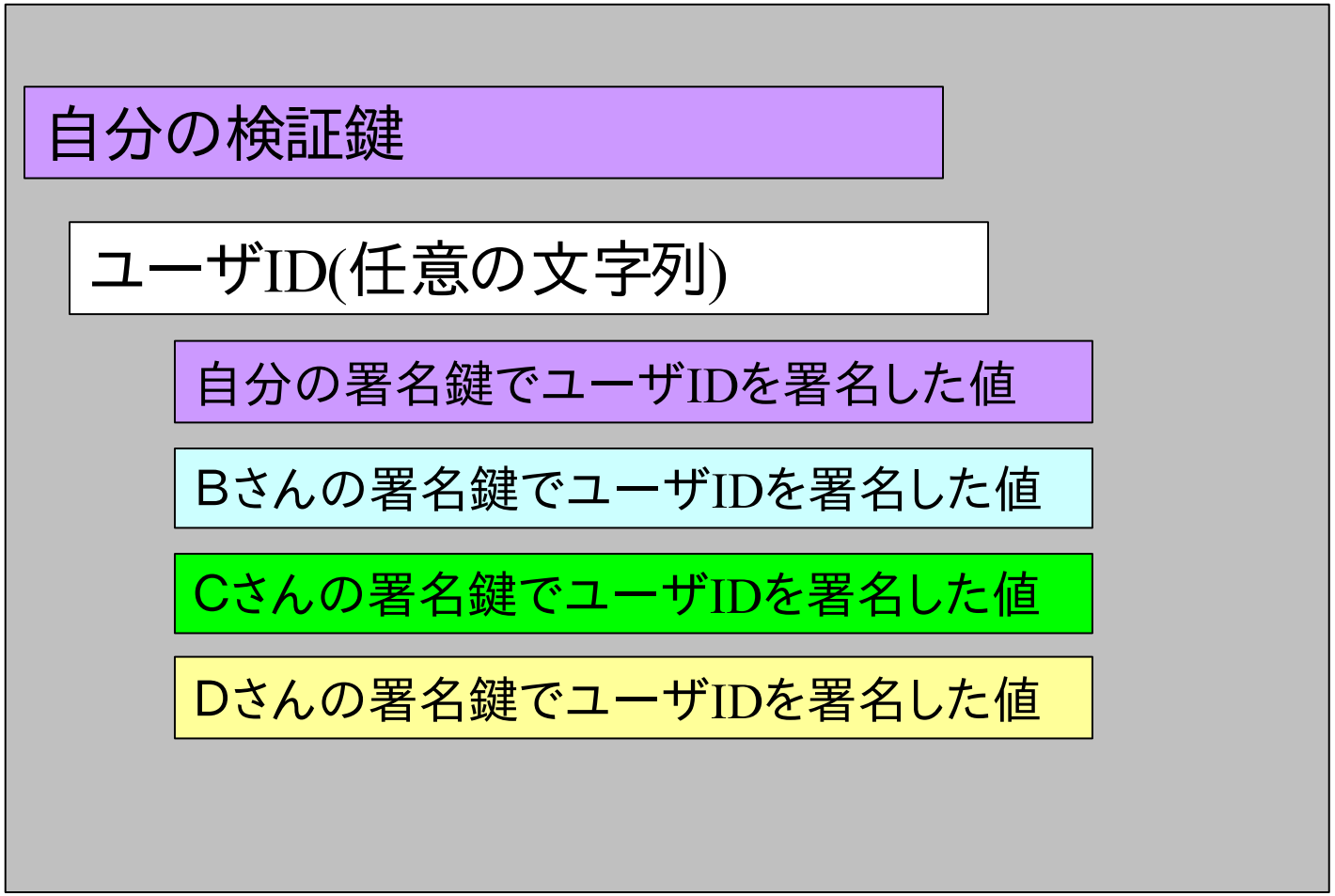
- Finger printチェック
  - 公開鍵のパラメータにつかっている値にハッシュ値をかけたもの
- 本人チェック
  - 写真つきの公的な身分証明書
    - 運転免許書やパスポート



キーサインパーティの実際を見て思った個人的感想

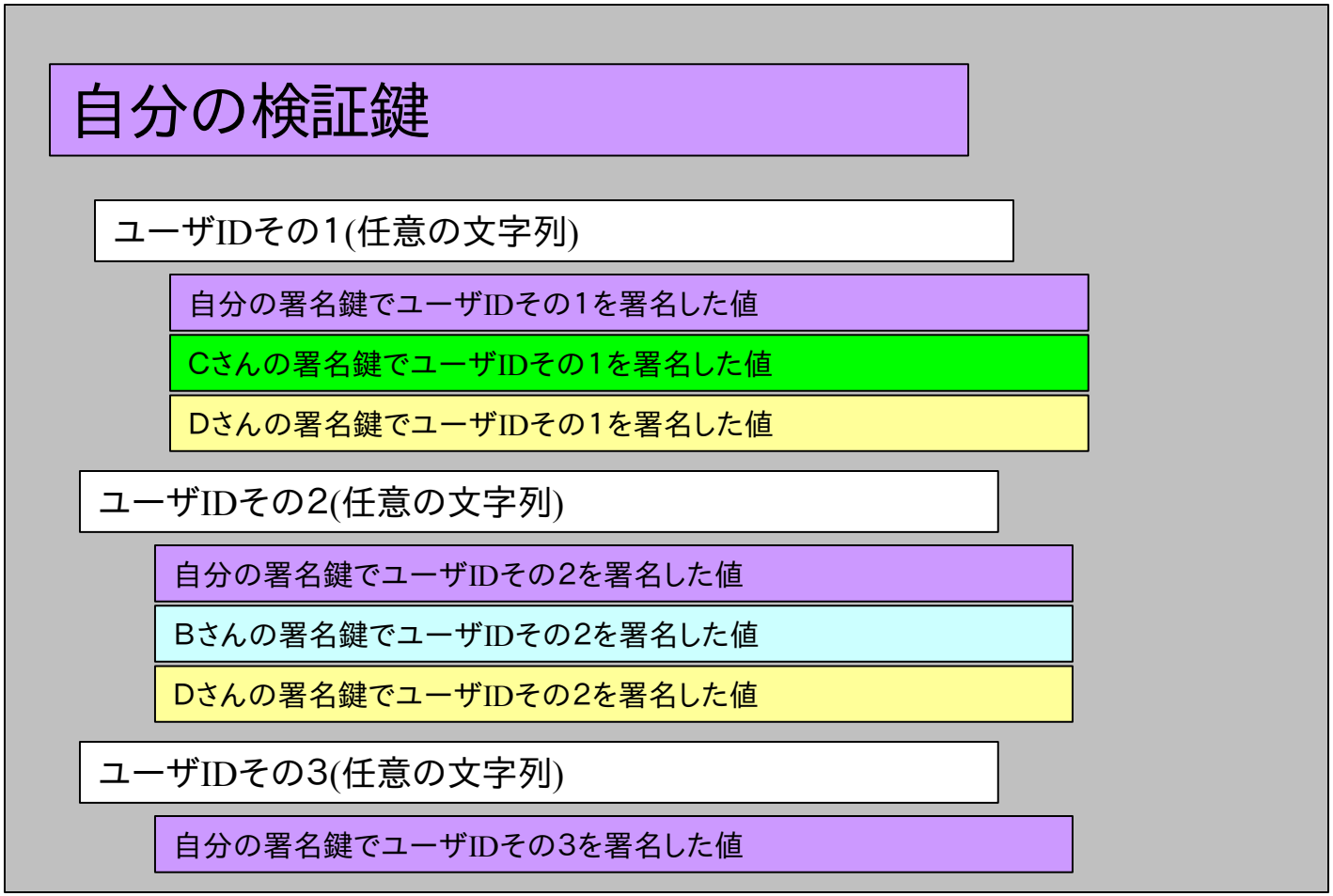
- ササーマン方式がベースになっているようだが
  - いまひとつ理解度が足りていない気がする
  - ササーマンというよりはオレ様ルールじゃないかなぁ
- そもそも信頼ってなんだろう？
  - そのサインをするコミュニティの署名に対する理解度が、そのコミュニティでの署名関係の信頼性に反映されているような気が…

OpenPGP公開鍵内部構造モデル



(注)キーサインを行った時にどうユーザIDへ署名されているかに着目して説明しています。OpenPGPのパケット構造はもっと複雑になっています。

OpenPGP公開鍵内部構造モデル2



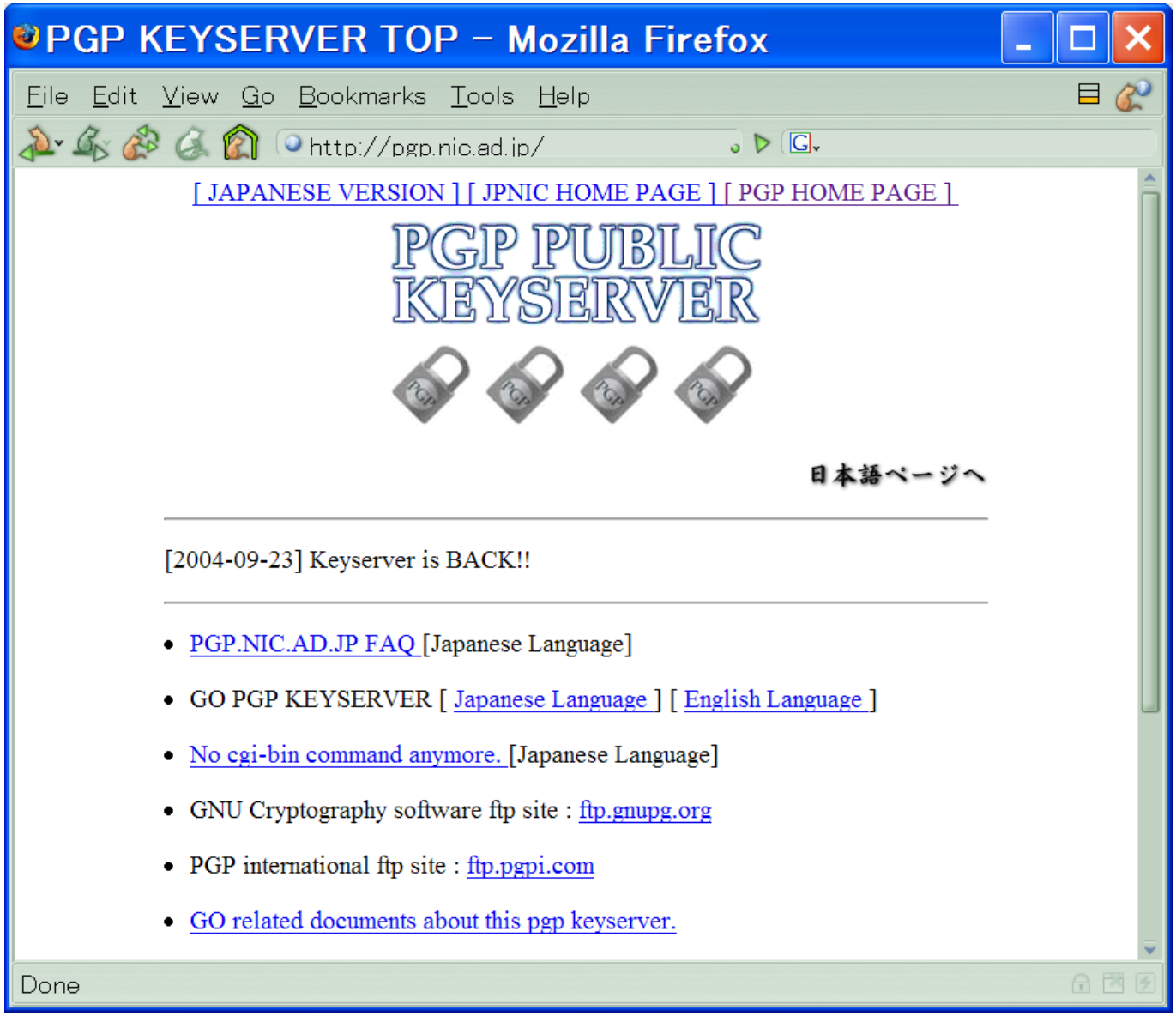
公開鍵の交換

- メールでやり取りしても良いし
- Webに貼り付けておいてURLを示すのもよい
- でももうちょっとスマートな遣り方があってもいいんじゃないか？

公開鍵サーバ

- 一々公開鍵をやり取りするのは面倒なので公開鍵サーバをつくり、そこにプールする
  - 公開鍵を保持しておくだけで何の保証もしていない
  - gnupgコマンドは　keyserver, --send-key, --recv-keyなどのオプションでダイレクトに呼び出せる
  - Webブラウザ経由でもアクセスできる
- 日本国内のサーバ
  - pgp.nic.ad.jp
    - JPNICに置かせてもらっているサーバ
  - openpksd.org
    - Hironobu's OpenPGP Public Keyserver

pgp.nic.ad.jp


PGP KEYSERVER TOP – Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://pgp.nic.ad.jp/
[JAPANESE VERSION] [JPNIC HOME PAGE] [PGP HOME PAGE]
PGP PUBLIC KEYSERVER
日本語ページへ
[2004-09-23] Keyserver is BACK!!
PGP.NIC.AD.JP FAQ [Japanese Language]
GO PGP KEYSERVER [Japanese Language] [English Language]
No cgi-bin command anymore. [Japanese Language]
GNU Cryptography software ftp site : ftp.gnupg.org
PGP international ftp site : ftp.pgpi.com
GO related documents about this pgp keyserver.
Done

openpksd.org

Spamの温床？

- 古典的公開鍵サーバはどこかに登録すると世界中の公開鍵サーバに登録される
  - ちなみにopenpksd.orgは外部からは取り込んでいるが、他のサーバへは送っていない
  - 登録、情報参照、鍵の取り出しなどができる
- 公開鍵の内容を自動的にダンプしたページを作っているウェブサイトは少しありがた迷惑
- 公開鍵サーバの検索表示に対しGoogleアタックを防止していない公開鍵サーバサイトがある
  - Googleが出来るということはspam業者も同じことができるはず

かなりありがた迷惑


"Hironobu SUZUKI" site:www.cs.uu.nl - Google 検...
File Edit View Go Bookmarks Tools Help
http://www.google.co.jp/search?h
Google
ウェブ イメージ ニュース グループ ディレクトリ more »
"Hironobu SUZUKI" site:www.cs.uu.nl
Google 検索
検索オプション
表示設定
ウェブ全体から検索 日本語のページを検索
ウェブ "Hironobu SUZUKI" の検索結果のうち www.cs.uu.nl からの約 188 件中 1 - 10 件目 (0.27 秒)
PGP trust paths : Hironobu SUZUKI -> Christoph Martin - [このページを訳す BETA]
PGP trust paths : Hironobu SUZUKI → Christoph Martin. from, stats Hironobu SUZUKI (Independent Software Consultant) <hironobu.at.h2np.net>. to, stats Christoph Martin <Christoph.Martin.at.Uni-Mainz.DE>. find, reverse path ...
www.cs.uu.nl/people/henkp/henkp/pgp/pathfinder/paths/02912C53/to/F95C2F6D.html - 16k - キャッシュ - 関連ページ
PGP trust paths : Hironobu SUZUKI -> Peter Nai Wan - [このページを訳す BETA]
PGP trust paths : Hironobu SUZUKI → Peter Nai Wan. from, stats Hironobu SUZUKI (Independent Software Consultant) <hironobu.at.h2np.net>. to, stats Peter Nai Wan <peter.wan.at.cc.gatech.edu>. find, reverse path ...
www.cs.uu.nl/people/henkp/henkp/pgp/pathfinder/paths/02912C53/to/09590CFD.html - 16k - キャッシュ - 関連ページ
PGP key statistics : Hironobu SUZUKI (Independent Software ... - [このページを訳す BETA]
PGP key statistics : Hironobu SUZUKI <hironobu.at.h2np.net>. msd. ↑ click to enlarge ↓. rank ... 02912C53 - Hironobu SUZUKI (Independent Software Consultant) <hironobu.at.h2np.net>. trust paths :. from to. from to. see also : ...
www.cs.uu.nl/people/henkp/henkp/pgp/pathfinder/stats/02912C53.html - 36k - 2005年10月22日 - キャッシュ - 関連ページ
Done

公開鍵サーバ不要論

- 段々と公開鍵サーバには置かないユーザも増えてきている
  - でも勝手に他人の公開鍵を公開鍵サーバに置くことができる
- 公開鍵所有者が自分の鍵をコントロールできない
  - 最近はウェブサーバ上に登録しておき、こちらを使うように指示するユーザも多い
- これはいかん

OpenPKSD Trusted Key Server

- 鍵ペアを持っている
  - 公開鍵を登録する
  - それに対応する署名鍵･秘匿鍵を持っている
  - それがあるならデータを秘匿･検証できる
- だったら公開鍵所有者のみが自分の公開鍵を操作できるようにしてしまえ

OpenPKSD-TKS Coming Soon

- 基本システムは既に完成
  - 平成16年度はIPAから予算獲得
- サーバサイト環境構築にはまだ時間がかかる
  - 運用はプログラムだけじゃないから、まだまだ準備が大変
  - その後、しばらく運用テスト
- OpenPKSD.ORGはTKSベースに移行
  - 新しいタイプの公開鍵サーバとして置き換え
  - 一般に公開するのは2007年4月を目標とする

まとめ

- 完全性に使われる技術の紹介
- 認証性とは何か
- 認証モデルの解説
- キーサインパーティーのお話
- 公開鍵サーバの紹介