公開鍵基盤 PKI

ネットワークと情報セキュリティ9

菊池　浩明

CONTENTS

- 背景：フィッシング
- PKIの原理
- PKIの課題（失効）
- PKIの応用分野

なぜPKIが必要か？

フィッシング詐欺

Security Threat: *Phishing*

- フィッシング詐欺
  - Fishing（釣り）＋sophisticate（精錬された）の造語
- ウェブサイトやメールの偽造
  - カード番号個人情報抽出
  - 米国24億ドル

手順1. 電子メール（餌）

VERIFIED by VISA
VISA認証サービス

VISA カード保有者のみなさまへ

VISA カードをお持ちのお客様は自動的に VISA 認証サービス プログラム** にご加入いただいております。

VISA 認証サービスでは、お客様の個人パスワードでお持ちの VISA カードのセキュリティを強化します。オンライン ストアでのお支払い手続きの際に、ATM で暗証番号を入力するのと同じようにパスワードを入力していただきます。これで、実際にお店でカードを使用するときと同じように、VISA カードをオンラインで安全に使用することができます。

サービスの中断を避けるため、できる限り早急にカード情報を確認させていただく必要があります。

たいへんお手数ですが、次のカード情報確認ページ* へのリンクをクリックしてください

https://www.visa.co.jp/verified/

お手続きは、次の手順に従ってください。

- カードのお申し込み
- お得なキャンペーン <VISA e-mailclub>
- 安全なオンラインショッピング
- プラチナカードの特典・サービス
- カードの紛失・盗難
- カードご利用のヒント
- プレス・センター
- VISAについて
- VISA TV コマーシャル
- VISA法人カード
- VISAのICカードへの取り組み
- AIS について

このサイトは、高度な SSL (Secure Socket Layer) 暗号化技術を利用しており、個人情報が閲覧、傍受または改ざんされることはありません。

VISA 認証サービス Web サイトで入力されたカード番号情報は、本サービスを開始することを目的として、お客様の VISA カードの発行元金融機関および処理機関に通知する場合を除き、使用または開示されることはありません。

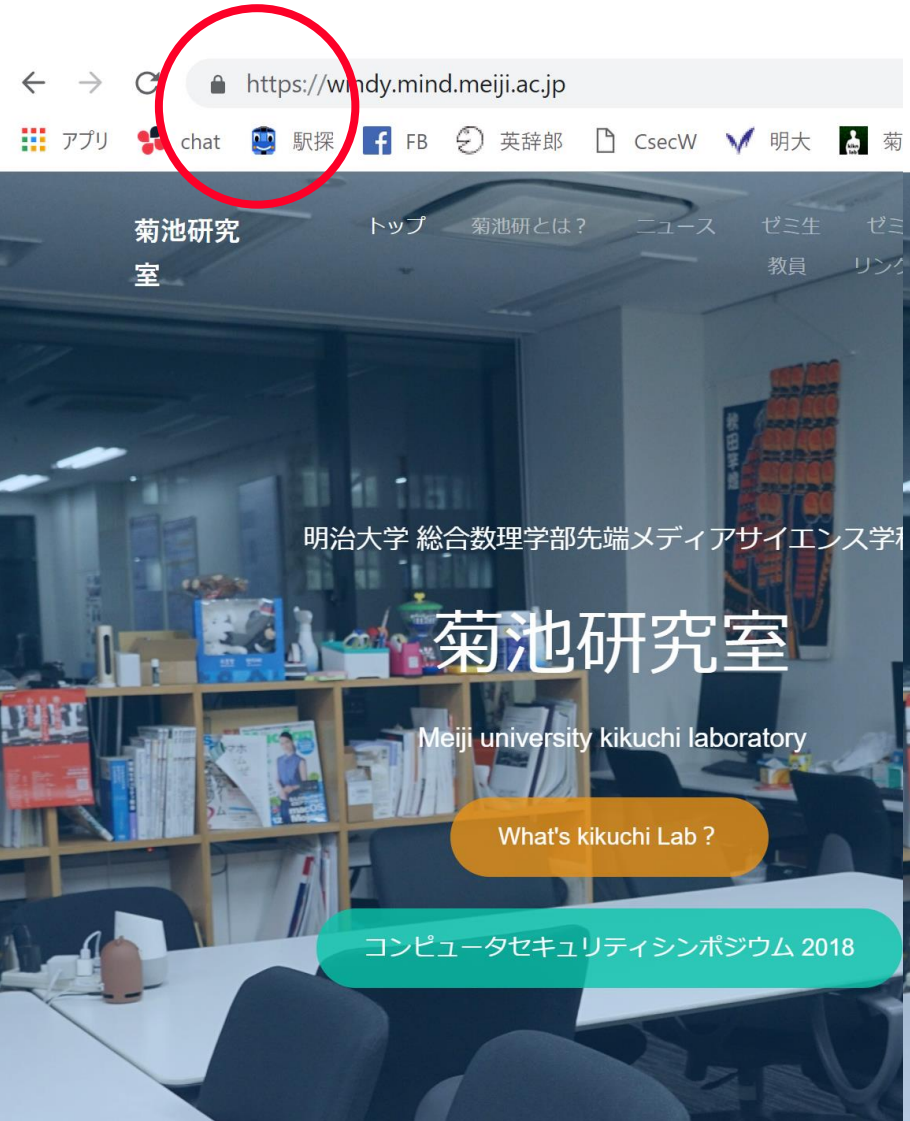
以下のフォームに記入し、カードを登録してください。

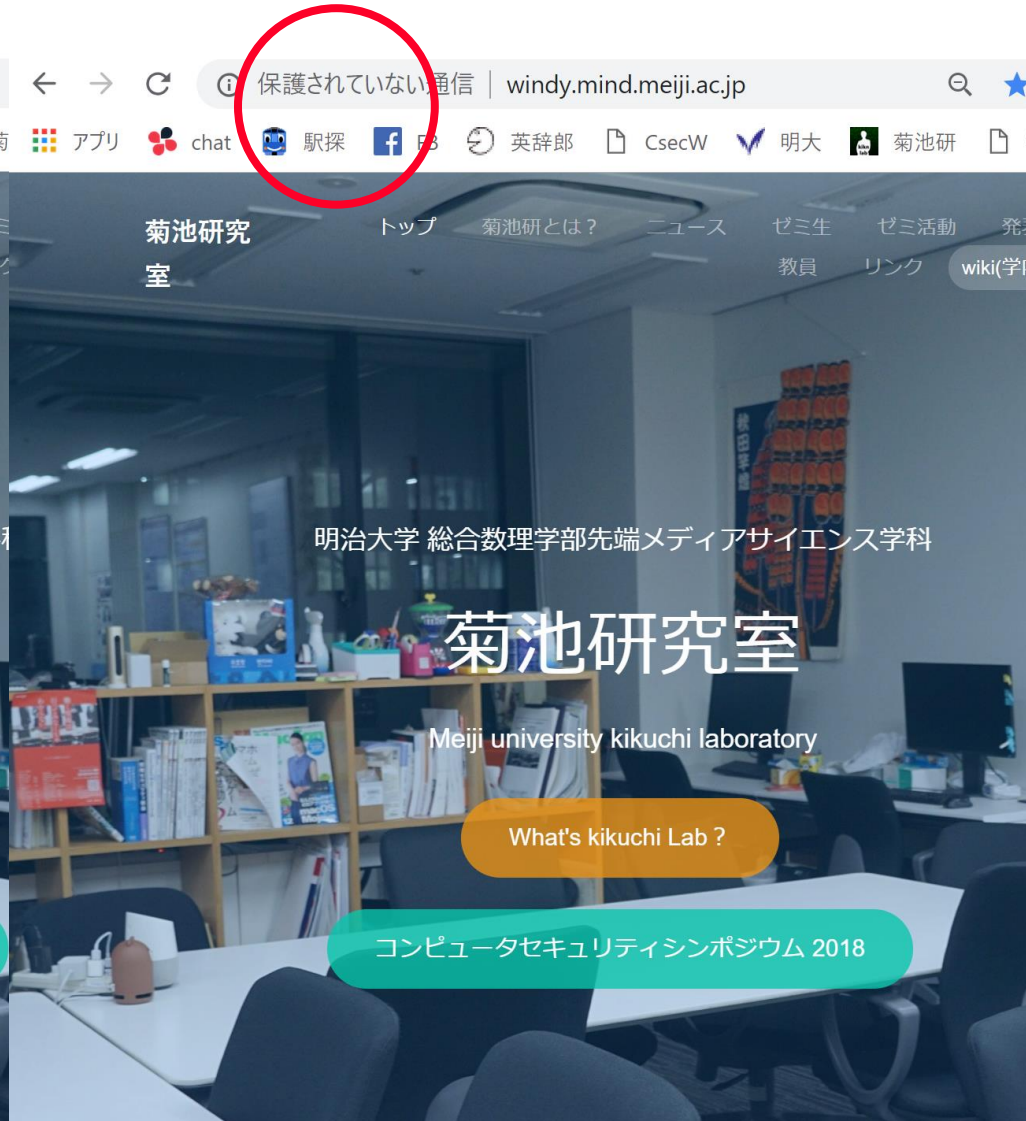
VERIFIED by VISA
VISA認証サービス

カード番号: - - -

カードの有効期限: 月 / 年

どちらがフィッシングサイトか？





公開鍵証明書

- インターネットのパスポート
  - 名前
  - 公開鍵

  (秘密鍵は入っていない)
  - 電子署名:
    本人が作ったものを証明する

チケットと証明書の比較

	チケット	証明書
暗号技術	共通鍵暗号	公開鍵暗号
検証者	指定（秘密を共有している人）	任意（公開鍵を知っている人）
スケーラビリティ	小さい	大きい
有効期限	数時間	数年
モデル	切符	パスポート

公開鍵証明書の原理

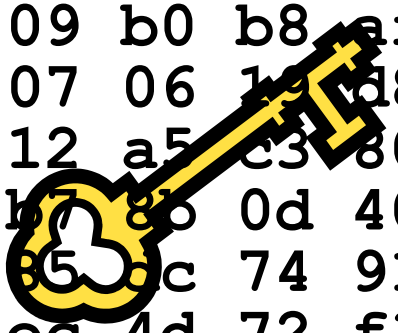
公開鍵証明書の技術

- 1. 公開鍵を証明するしくみ
- 2. 証明を行う認証局
- 3. グローバルな基盤

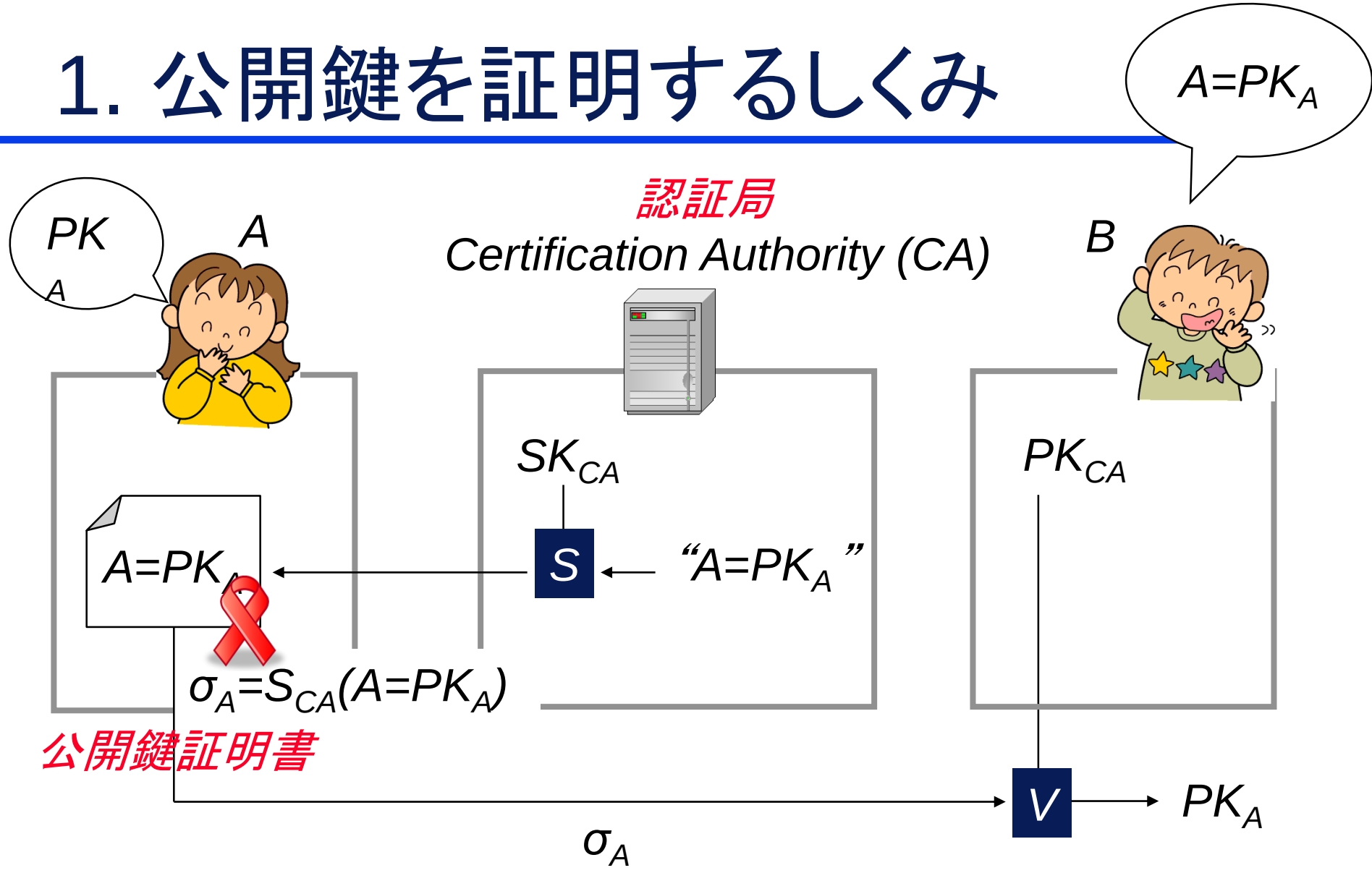
私の公開鍵

- RSA 1024bit（$199/年）

```
n = 30 81 89 02 81 81 00 eb c1 3d 97 24
47 02 a2 2b 25 49 4f da 18 18 f4 99 42 2b
5d 12 e0 f2 67 09 b0 b8 af 13 93 84 b5 18
0c 58 6b 1f 81 07 06 1[illegible]d8 ad d3 a1 d6 45
a9 71 c2 e9 96 12 a5 c3 80 88 32 c3 8d 76
49 66 67 18 8a [illegible] 0d 40 69 e8 d5 85 09
77 5e 5a f7 27 [illegible]c 74 91 cf 5d 9c a8 88
26 cb 17 9a ed ec 4d 72 f3 1b 51 db bc 39
2e 8c 02 c5 29 23 ee 81 d7 05 5a f2 92 5b
1d 6a 20 9f d8 95 af 8b 89 d9 69 02 03 01
00 01
```



1. 公開鍵を証明するしくみ



X.509 証明書フォーマット

バージョン	X.509 のバージョン番号	V3
シリアル番号	発行元証明機関が証明書に割り当てる一意なシリアル番	170300009687af8a90a4726c
発行者	証明書を発行した証明機関	Kaspersky Anti-Virus Personal Root Certificate
有効期間	有効期限の開始と終了日	2010年5月6日 6:11:38
サブジェクト	証明書の発行先の個人、コンピュータ、デバイス、証明機関名	CN = windy.mind.meiji.ac.jp
公開キー	公開キーの種類と長さ	RSA (2048 bit)
拇印アルゴリズム	ハッシュ アルゴリズム	SHA256
拇印	証明書データの要約	4 ee 07 53 58 ..
CRL配布ポイント	CRLの配布元URL	URL=http://EVIntl-crl.verisign.com/
キー使用法	鍵の用途	署名用, 暗号用

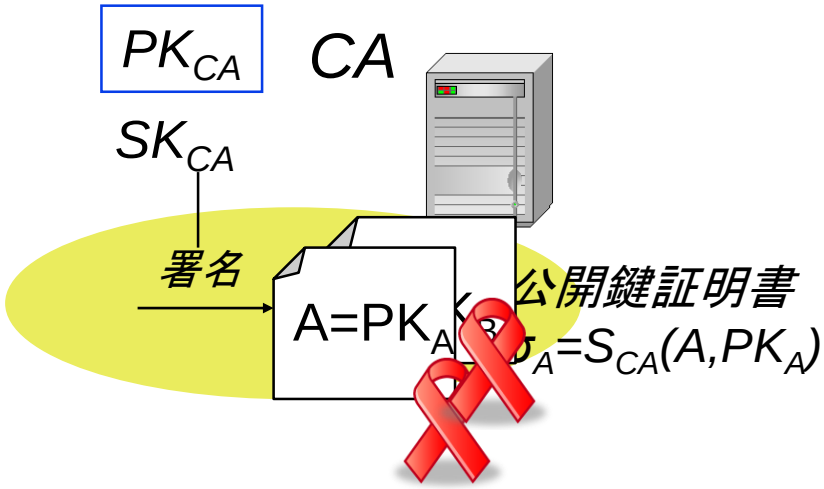
DN

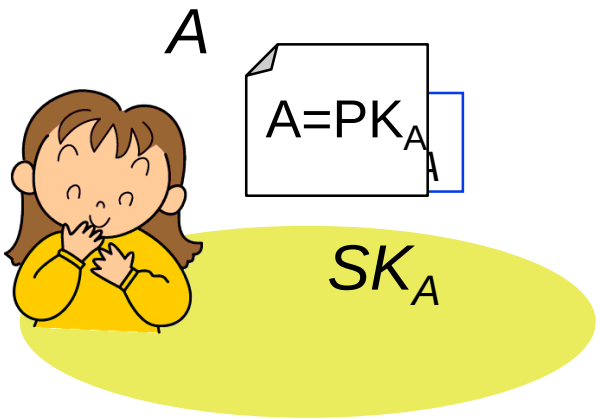
- Distinguished Name　OSIにおける識別名 ID
  - 菊池研
    - » CN = windy.mind.meiji.ac.jp
    - » OU = Domain Control Validated
    - » C = JP
  - 明治大学
    - » CN = www.meiji.ac.jp
    - » OU = System Planning Office
    - » O = Meiji University Education Foundation
    - » L = Chiyoda-ku
    - » S = Tokyo
    - » C = JP

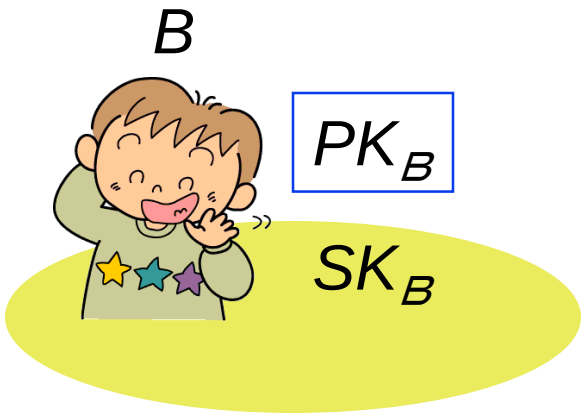
PKI (Public-key Infrastructure)

- 公開鍵基盤
  - グローバルな認証
  - 「名前」と公開鍵の束縛
  - 公開鍵証明書 (Certificate)
    - » 規格 ITU X.509
  - 認証局 (CA: Certification Authority)
    - » VeriSign, Baltimore, GPKI

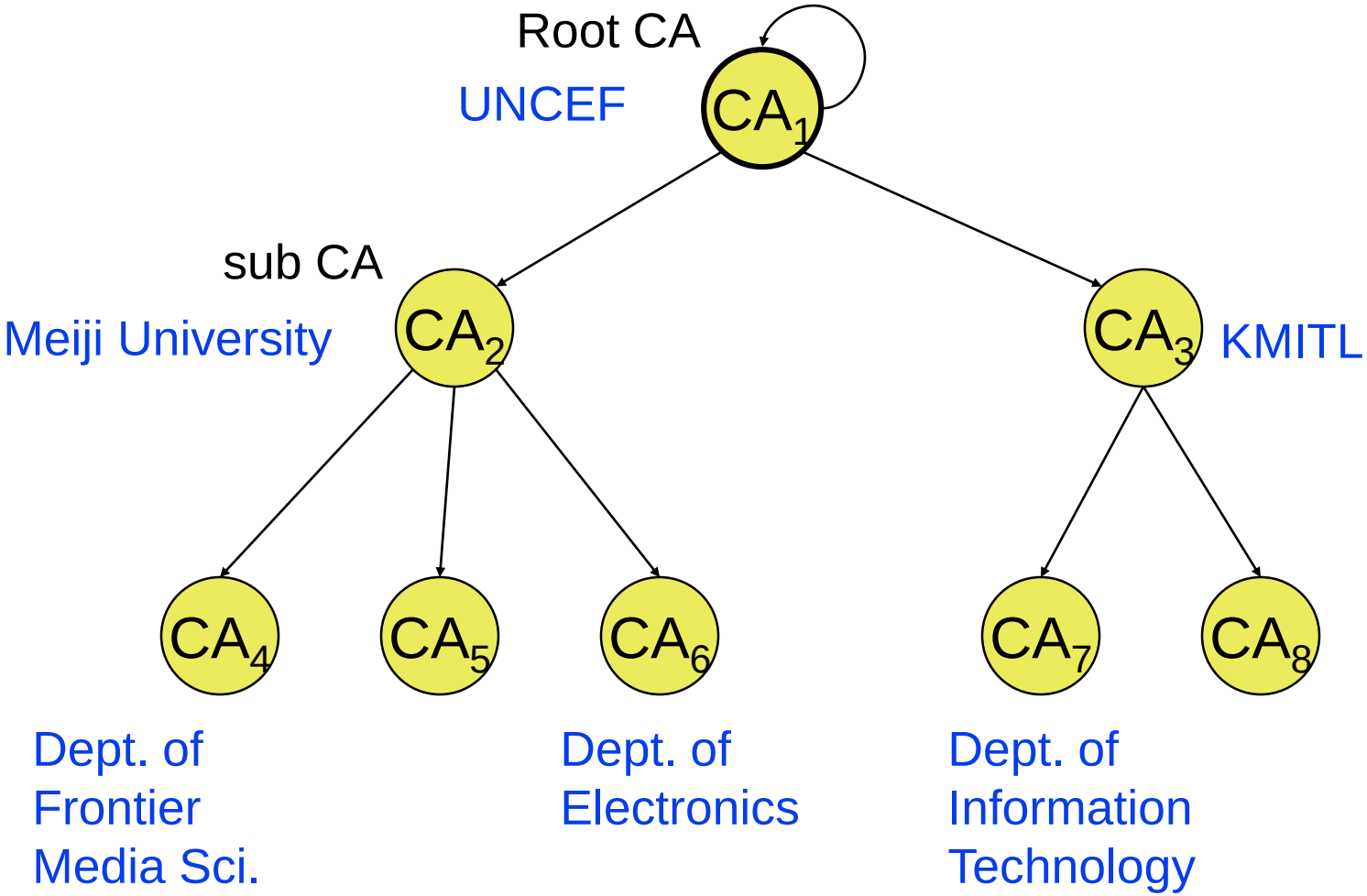
2. 認証局 (Certification Authority)



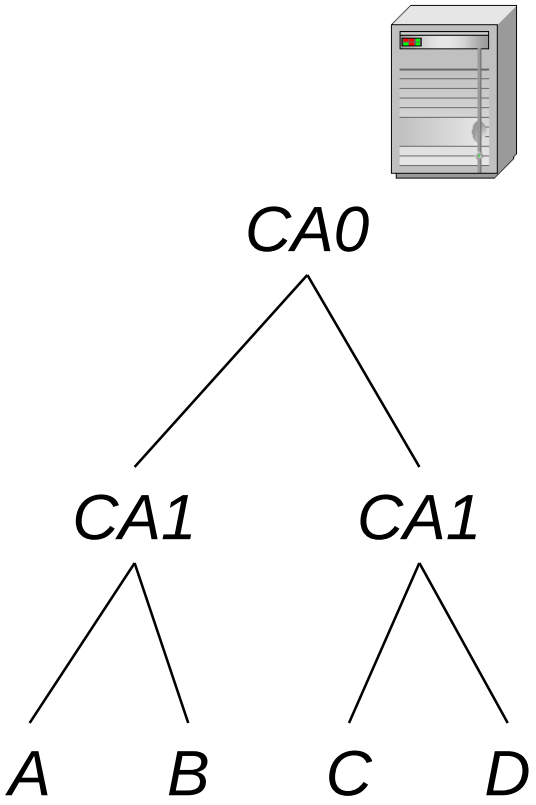


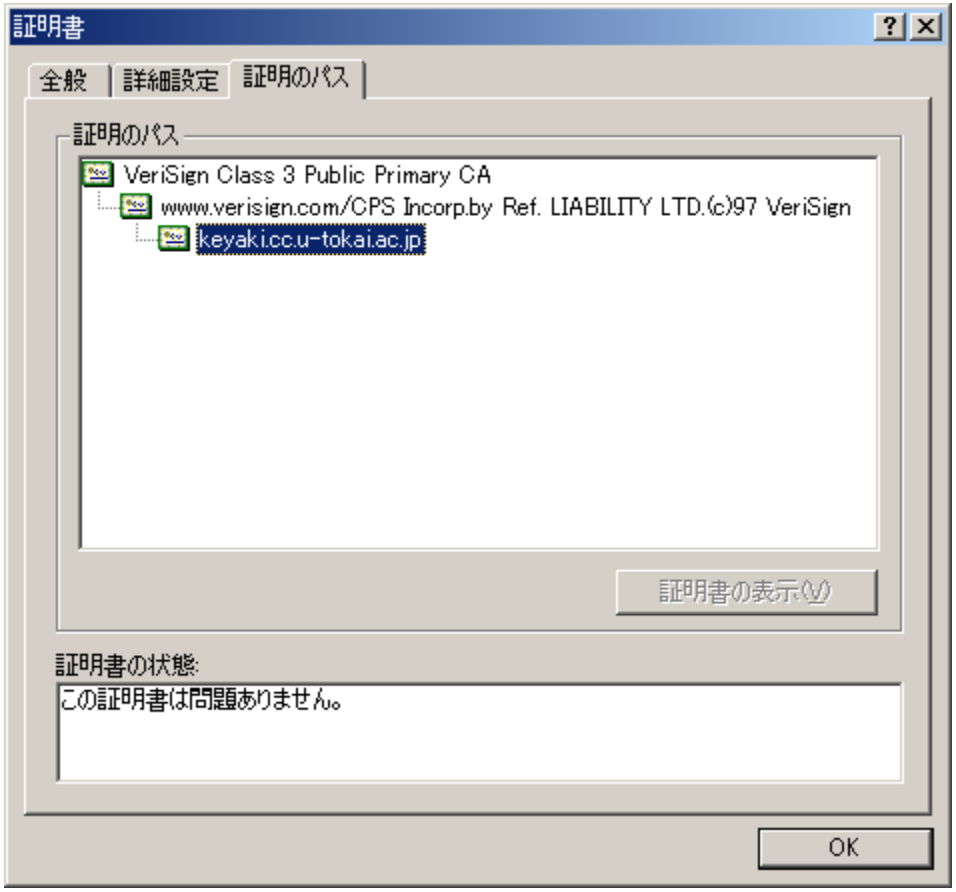


PKI (Public-key Infrastructure)



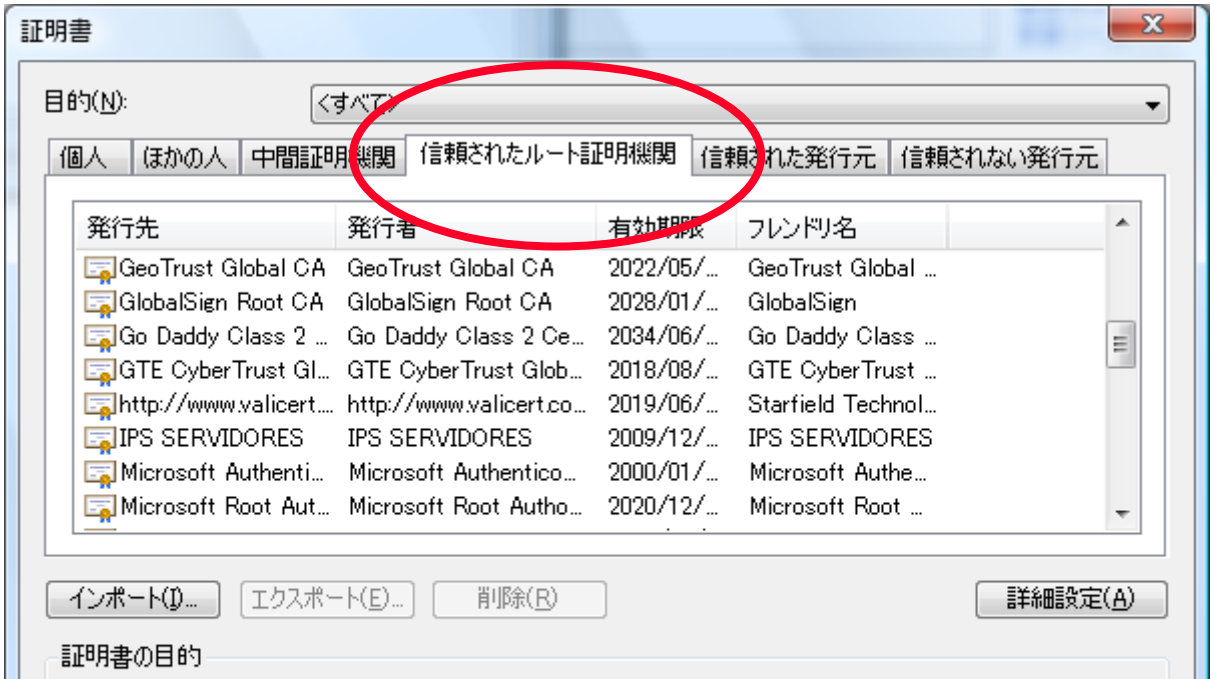
CAの「証明のパス」

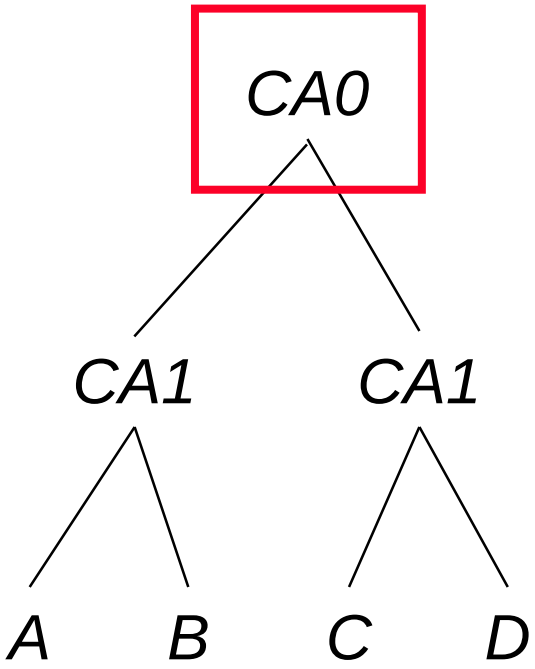

CA0
CA1
CA1
A
B
C
D


証明書
全般
詳細設定
証明のパス
証明のパス
VeriSign Class 3 Public Primary CA
www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign
keyaki.cc.u-tokai.ac.jp
証明書の表示(V)
証明書の状態:
この証明書は問題ありません。
OK

トラストアンカー

- 信用の起点
  - 1. OSやブラウザに初期登録された証明書
  - 2. 階層型の信頼の木のルート



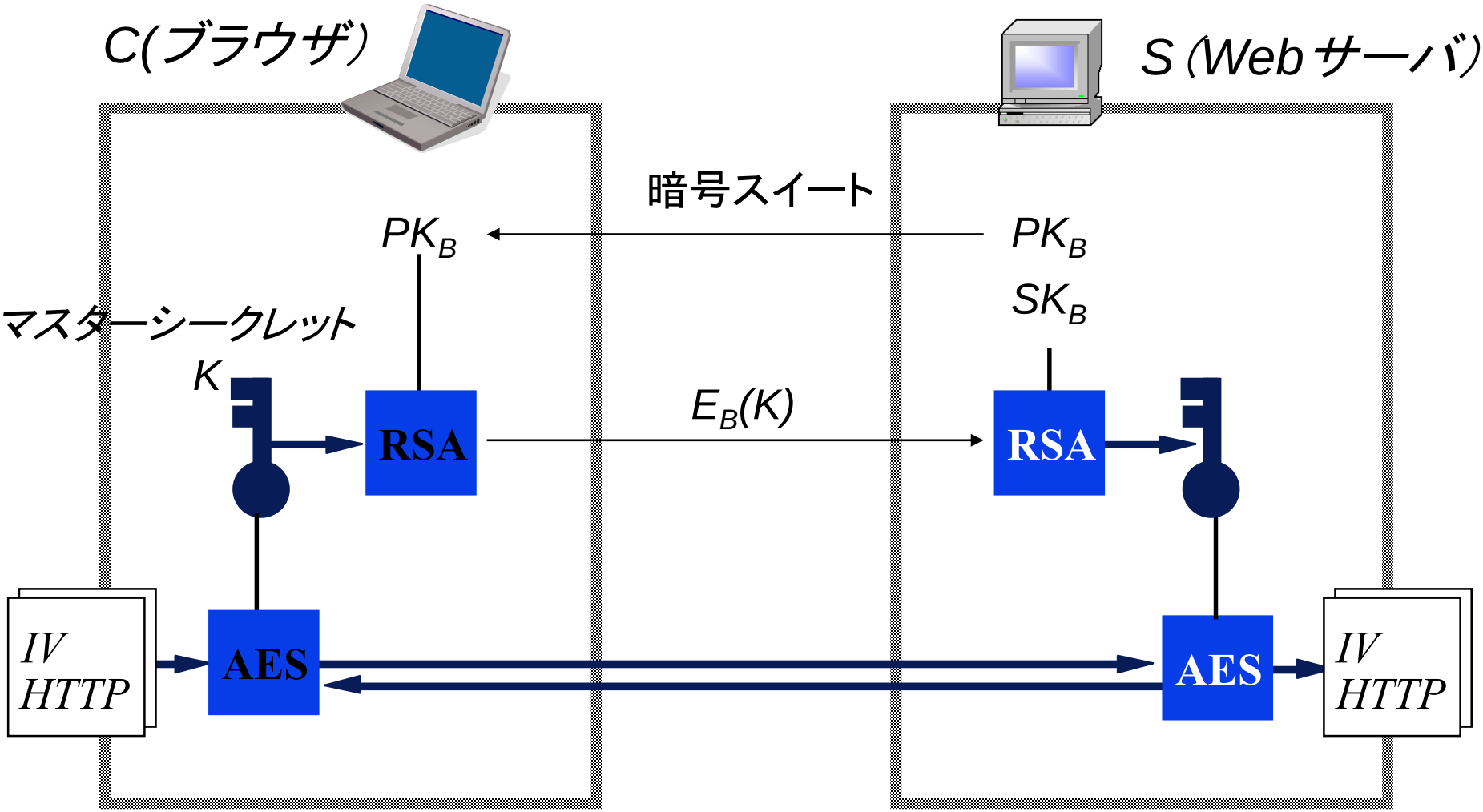


SSL/TLS

OSIレイヤーモデル

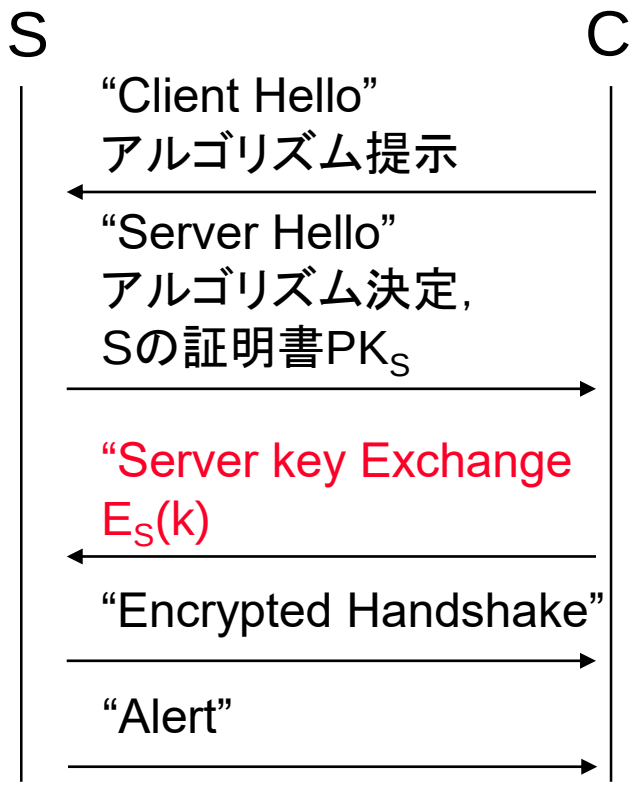
<table>
<tr><th>OSI</th><th>TCP/IPの例</th><th>セキュリティ</th><th>識別子</th></tr>
<tr><td>アプリケーション層</td><td rowspan="3">アプリケーション</td><td rowspan="2">S/MIME</td><td rowspan="2">メールアドレス</td></tr>
<tr><td>プレゼンテーション層</td></tr>
<tr><td>セッション層</td><td>SSL/TLS</td><td>SA</td></tr>
<tr><td>トランスポート層</td><td>TCP/UDP</td><td rowspan="2">IPSEC</td><td rowspan="2">SPI
(IPアドレス)</td></tr>
<tr><td>ネットワーク層</td><td>IP</td></tr>
<tr><td>データリンク層</td><td>Ethernet / FDDI</td><td></td><td></td></tr>
<tr><td>物理層</td><td>ADSL/電気信号</td><td></td><td></td></tr>
</table>

SSL/TLSのHandshake

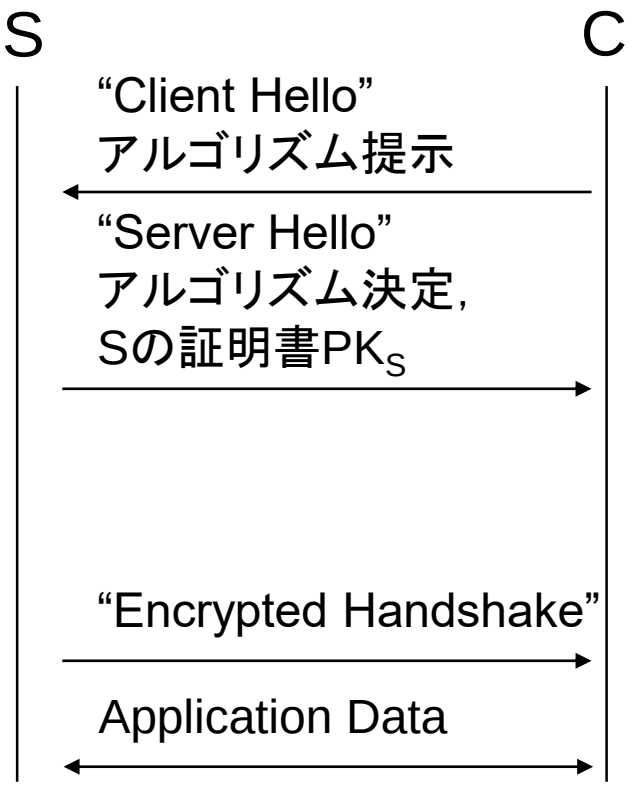


ハンドシェイクプロトコル

- (a) 初期



- (b) 既存セッション



TLSで保証されるもの

- 機密性 (C)
  - エンドツーエンドの暗号化
  - 例）EDH+AES
- 認証 (完全性 I)
  - サーバ： 公開鍵証明書，必須
  - クライアント： クライアント証明書（オプション）
  - 例）RSA+SHA

SSL Cipher Suites

- 暗号技術の識別
  - 公開鍵暗号　×　共通鍵暗号　×　ハッシュ
  - 例）
    TLS_RSA_WITH_AES_128_CBC_SHA
- 公開鍵
  - RSA
  - DH (DH_RSA (DSS): 証明書付きDH,
    DHE_RSA (ephemeral「短命の」DH,
    DH_anon: 証明書なしDH)

BEAST, POODLE攻撃

- BEAST攻撃
  - CBCモードの脆弱性。ブロックの一部を解読。メッセージの分割などにより対処可

- POODLE攻撃
  - SSL 3.0のパディングの脆弱性。2014年12月に発見

スノーデン事件とフォワードセキュリティ

- Edward Joseph Snowden
  - 元米中央情報局CIA職員、米国家安全保障局NSAへ出向していた
  - 2013年6月13日、香港英文紙に、米国政府が世界中の数万の標的を対象に電話記録やインターネット利用を極秘裏に監視していたことを暴露
- Perfect Forward Secrecy (PFS)の重要性が再認識
  - PFS: ある時刻の鍵が漏洩しても、それ以前、以降の暗号通信の解読に影響を与えないこと
  - RSA: PFSでない（鍵固定）
    DH: PFSでない
    DHE (DH Ephemeral): PFSを満たす
    ECDHE (楕円版DHE): PFSを満たす

SSL/TLSのバージョンと安全性

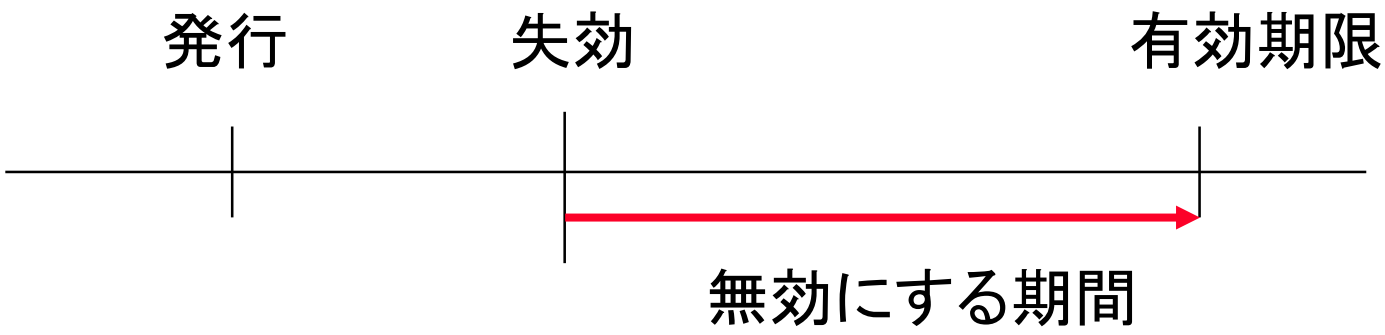
SSL/TLSへの攻撃方法に対する耐性	TLS1.2	TLS1.1	TLS1.0	SSL3.0	SSL2.0
ダウングレード攻撃（最弱の暗号アルゴリズムを強制的に使わせることができる）	安全	安全	安全	安全	脆弱
バージョンロールバック攻撃（SSL2.0を強制的に使わせることができる）	安全	安全	安全	安全	脆弱
ブロック暗号のCBCモード利用時の脆弱性を利用した攻撃（BEAST/POODLE攻撃など）	安全	安全	パッチ適用要	脆弱	脆弱
利用できる暗号アルゴリズム	**TLS1.2**	**TLS1.1**	**TLS1.0**	**SSL3.0**	**SSL2.0**
128ビットブロック暗号（AES, Camellia）	可	可	可	不可	不可
認証付暗号利用モード（GCM, CCM）	可	不可	不可	不可	不可
楕円曲線暗号	可	可	可	不可	不可
SHA-2ハッシュ関数（SHA-256, SHA-384）	可	不可	不可	不可	不可

SSL/TLS暗号設定ガイドライン～安全なウェブサイトのために（暗号設定対策編）～

証明書のライフサイクル

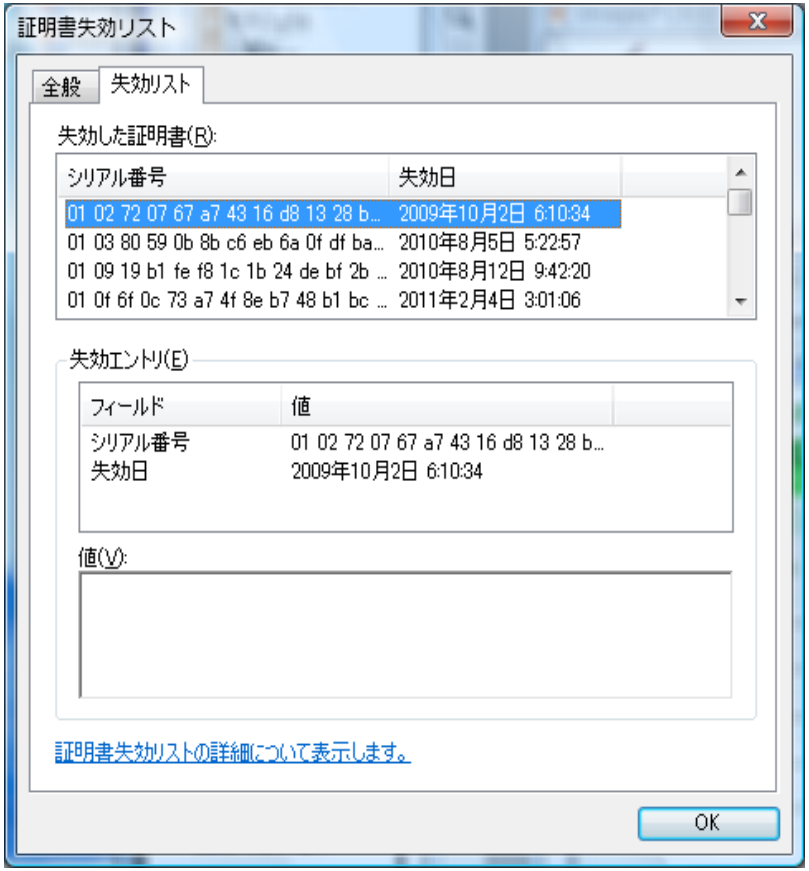
証明書の失効

- 失効
  - 本来の有効期限より前に無効にすること
  - 理由: 秘密鍵の漏洩や損失，組織の変更，退職，アルゴリズムの脆弱性



CRL (Certificate Revocation List)

- 失効証明書リスト
  - シリアル番号1
  - 失効日1
  - シリアル番号2
  - 失効日2 ….
- 発行者
- 有効開始日＋次の更新予定 (毎週)

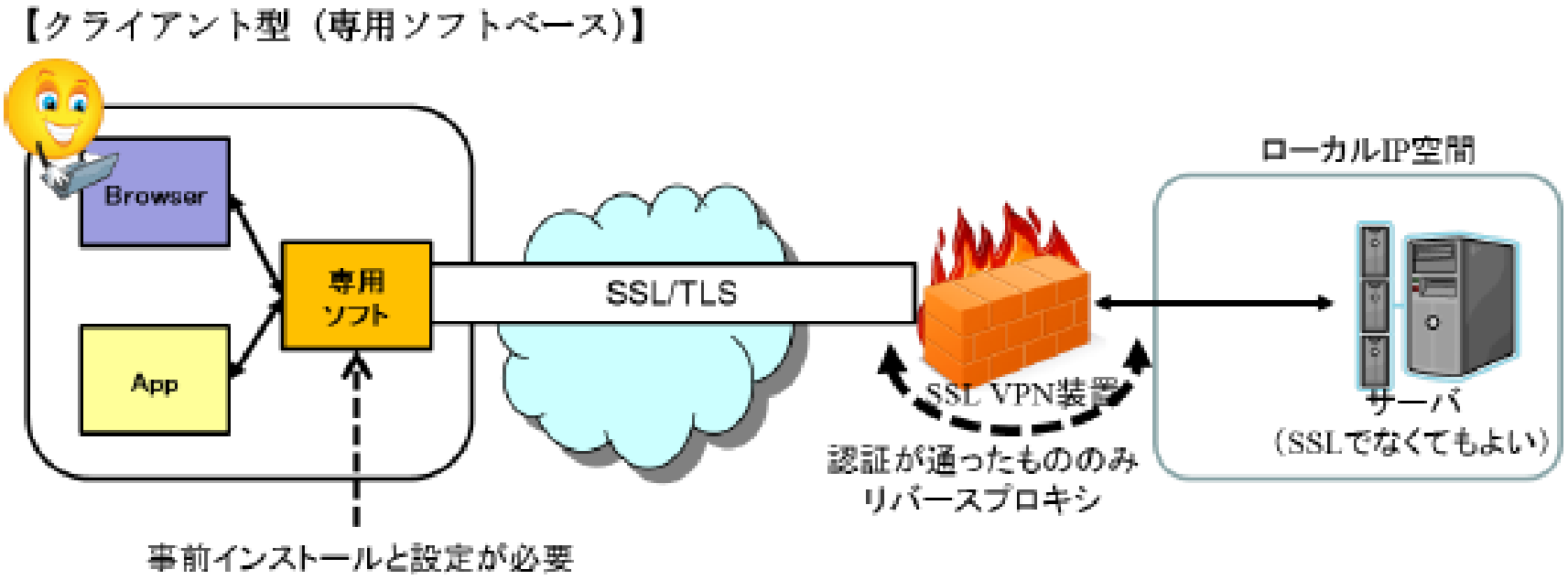


CRLの拡張

- 差分CRL
- CRL配布ポイント
- OCSP (Online Certificate Status Protocol)

PKIの応用分野

SSL-VPN

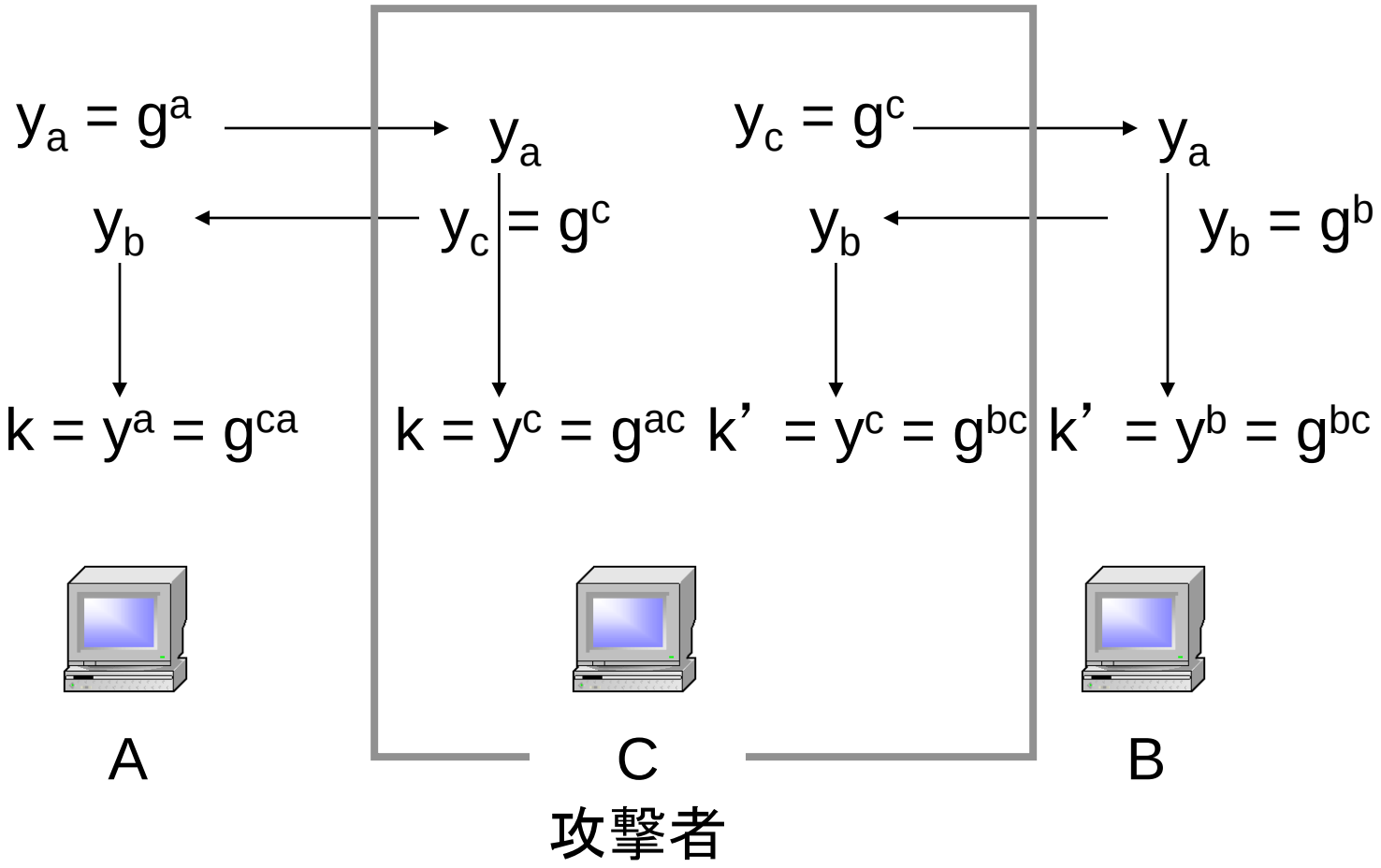


SSL/TLS暗号設定ガイドライン～安全なウェブサイトのために（暗号設定対策編）～

アプリ開発コードサイニング証明書

- iOS開発者登録 年会費10,800円

中間者攻撃


$y_a = g^a$
y_a
$y_c = g^c$
y_a
y_b
$y_c = g^c$
y_b
$y_b = g^b$
$k = y^a = g^{ca}$
$k = y^c = g^{ac}$
$k' = y^c = g^{bc}$
$k' = y^b = g^{bc}$
A
C
B
攻撃者

まとめ

- フィッシング詐欺を防止するには，PKI(和訳：　　)が有効である.
- 証明書の形式は，ITUの(　　)で定められており，DN形式で持ち主を表す(　　)と発行者，公開鍵が(　　)の鍵で署名されている.
- 有効期限より前に証明書を無効にすることを(　　)といい，定期的に(　　)を発行することで失効を保証している.

演習

- A,B,C,Dの証明書が次の表の様にある.
  - 1. 空欄に適切な鍵を埋めよ
  - 2. CがDに署名を送るとき必要な証明書は？
  - 3. AのCRLの発行者は誰か？
  - 4. トラストアンカーは誰か？

No.	Subject	Issuer	格納されている鍵	発行に使う鍵	検証に使う鍵
1	Alice	Bob	PK_A		
2	Bob	Bob		SK_B	
3	Carroll	Alice			PK_A
4	Dave	Alice			