情報ネットワークⅡ（情213）
【第6回】
PKI
（教科書：第4章）

担当教員：長田智和

E-Mail: nagayan@ie.u-ryukyu.ac.jp

URL: http://n-lab.info/

（講義日：2017年11月9日）

第4章：PKI

4.1 PKIの基礎

- PKI（Public Key Infrastructure）とは、

  公開鍵暗号化技術の公開鍵ペアを用いて暗号化・復号やディジタル署名を利用するためのフレームワーク（枠組み）

- 構成要素
  - RSAなどの公開鍵暗号化技術
  - 証明書を発行するサーバー（認証局・登録局）
  - 暗号化通信に対応したWeb&Mailサーバー等

4.1 PKIの基礎

- 4.1.1 PKIが必要となる理由
  - 公開鍵暗号化方式は、ITシステムの設計上の脆弱性により、MITM攻撃に対して脆弱である。
  - PKIの目的：公開鍵の信頼性保証の仕組みの実現
- （教科書p.93の図4.1を参照）

4.1 PKIの基礎

- 4.1.2 PKIの実例（HTTPS）
  - HTTPS（HyperText Transfer Protocol over Secure Socket Layer）
    - SSL/TLS（Secure Socket Layer / Transport Later Security）
      通信路上でHTTPを利用する通信プロトコル
- （教科書p.93の図4.2を参照）

4.2 トラストモデル

- トラストモデルとは？
  - 「誰か（何か）」が本物であるかを確認する仕組み
  - 公開鍵をインターネットなどの通信路を使って配布する際、所有者を確認する仕組み
    - Web of Trustモデル
    - 認証局モデル

4.2 トラストモデル

- 4.2.1 Web of Trustモデル
  - 公開鍵の所有者を、自身が信頼できる人物に保証してもらう仕組み。
  - 個人レベルでの信頼関係がベース

    →「友達の友達は、友達」的な考え方
  - 全体を集中して管理する主体が存在しない。

    → メリットでもありデメリットでもある。
  - OpenPGP（Pretty Good Privacy）規格（RFC4880）
- （教科書p.94の図4.3を参照）

4.2 トラストモデル

- 4.2.2 認証局モデル
  - 全体を集中して管理する主体が存在する。
  - 信頼できる第三者機関（TTP:Trusted Third Party）に公開鍵の所有者を保証してもらう仕組み。
  - TTPは、公開鍵の所有者の真正性を確認し、公開鍵とその所有者を保証する証明書を発行する。
  - 証明書は、公開鍵とその所有者を証明する情報が記載され、TTPの署名が施される。
- （教科書p.95の図4.4を参照）

4.3 公開鍵証明書

- 4.3.1 公開鍵証明書のフォーマット
  - X.509v3証明書（RFC5280）
    - 署名前証明書（tbsCertificate）
    - 署名アルゴリズム（signatureAlgorithm）
    - 署名値（signatureValue）
  - 署名前証明書に含まれる情報
    - version（バージョン）, serialNumber（シリアル番号）, signature（アルゴリズム識別子）, issuer（発行者）, validity（有効期限）, subject（主体者）, subjectPublicKeyInfo（主体者公開鍵情報）, issuerUniqueLdentifire（発行者ユニーク識別子）, subjectUniqueIdentifier（主体者ユニーク識別子）, extensions（拡張領域）
- （教科書p.97の図4.5を参照）

4.3 公開鍵証明書

- 4.3.2 X.509v3証明書の拡張領域
  - extnID（識別子）
  - critical（重要度）
    - 「True」の場合はPKIアプリは認識できなければならない。
      （認識できない場合は、その証明書は破棄する）
  - extnValue（拡張値）
- （教科書p.98の図4.6を参照）

4.3 公開鍵証明書

- 4.3.2 X.509v3証明書の拡張領域
  - 標準的な拡張領域
    - Authority Key Identifier（機関識別子）, Subject Key Identifier（サブジェクト鍵識別子）, Key Usage（鍵用途）, Certificate Policies（証明書ポリシー）, Policy Mappings（ポリシーマッピング）, Subject Alternative Name（主体者代替名）, Issuer Alternative Name（発行者代替名）, Subject Directory Attributes（サブジェクトディレクトリ属性）, Basic Constraints（基本制約）, Name Constraints（名前制約）, Policy Constraints（ポリシー制約）, Extended Key Usage（拡張鍵用途）, CRL Distribution Points（CRL配布点）, Inhibit Policy（anyPolicyの禁止）, Freshest（最新CRT）
- （教科書p.99-100の表4.1-4.2を参照）

4.3 公開鍵証明書

- 4.3.3 証明書の例
  - 証明書をテキストエディタで開くとBase64形式のデータとして見ることができる。
  - 拇印（フィンガープリント）によって証明書の真正性を確認できる。
  - 証明書の各フィールドを表示するツールが存在する。
- （教科書p.101-102の図4.7-4.9を参照）

4.4 認証局

- TTPが発行した証明書を用いて公開鍵を配布することで、MITM攻撃を防ぐことができる。
- （教科書p.103の図4.10を参照）

4.4 認証局

- 4.4.1 PKIにおける認証局の意義
  - PKIの認証局モデルで配布された鍵の信頼性は、証明書を発行した認証局に依存する。
  - 全ての参加主体から信頼された認証局が証明書を発行することが前提。
  - 認証局を介した間接的なトラストモデルはスケーラビリティを備えた有効なモデルといえる。
- （教科書p.103の図4.10を参照）

4.4 認証局

- 4.4.2 PKIを構成する主体
  - 認証局（CA: Certification Authority）
  - 登録局（RA: Registration Authority）
  - リポジトリ（repository）
  - 証明書所有者（certificate holder）
  - 証明書利用者（relying party）
- （教科書p.104の図4.11を参照）

4.4 認証局

- 4.4.3 パブリック認証局とプライベート認証局
  - パブリック認証局：広く信頼されている機関が運営している認証局。一般的なOSやブラウザに予め同梱されている場合が多い。外部に対して証明書の配布や設定の手間がかからない。ただし、証明書発行は一般に有料。
  - プライベート認証局：企業等の組織内で独自に運営される認証局。信頼の範囲内での利用には運用の自由度は高いが、証明書の配布や設定に手間がかかる。ただし、証明書発行に費用はかからない。プライベート認証局が発行した証明書は「プライベート証明書」又は「オレオレ証明書」などと呼ぶことがある。

4.4 認証局

- 4.4.4 EV（Extended Validation）SSL証明書
  - 厳密な認証プロセスに基づいて発行される証明書
  - 大企業などのWebサーバーで利用される。
  - 通常の証明書に比べて（非常に）高価である。
- （教科書p.106の図4.12-4.13を参照）

4.5 証明書の利用

- 証明書の種類
  - サーバー証明書
    - サーバーを識別するための証明書
    - SSL/TLSサーバーが証明書のSubjectとなる。
  - クライアント証明書
    - クライアントを識別するための証明書
    - クライアントが証明書のSubjectとなる。
  - ルート証明書（自己署名証明書）
    - 認証局が自らの秘密鍵で署名する証明書
    - 認証局が発行する証明書の真正性を示す。
- （教科書p.107の図4.14を参照）

4.5 証明書の利用

- 4.5.1 証明書チェーン
  - HTTPS（SSL/TLS）通信の場合
    - HTTPSサーバーはクライアントにサーバー証明書とルート証明書の組を送信する。
    - クライアントは、ルート証明書及びサーバー証明書を検証する。
- （教科書p.108の図4.15を参照）

4.6 PKIの運用

- 4.6.1 証明書の発行
  - 手順:
    - 主体は公開鍵ペアを作成する。
    - 主体はCSR（Certificate Signing Request）を作成する。
      - CSRは署名前証明書の情報が含まれる。
    - 登録局はCSRをもとに本人性を確認する。
    - 認証局は自身の署名をして証明書を発行する。
- （教科書p.109-110の図4.16-4.17を参照）

4.6 PKIの運用

- 4.6.2 証明書の検証
  - 手順：
    - 証明書利用者は証明書の有効期間や利用目的、失効証明書ではないか、FQDNを確認する。
    - 証明書利用者はルート証明書（ラストアンカー）の公開鍵で証明書の真正性を確認する。
    - ルート証明書は自身の公開鍵で検証できるが、ルート証明書は信頼できる方法で入手したものか、信頼できる認証局が発行したものであることが前提。
- （教科書p.111の図4.18を参照）

4.6 PKIの運用

- パブリック認証局
  - WebTrust for CA（Certification Authority）を満たしたパブリック認証局は信頼性が高いとみなされる。
  - メジャーなOSやWebブラウザのベンダーは、WebTrust for CAを取得した認証局が発行したルート証明書を同梱している場合が多い。この場合、このルート証明書は、ラストアンカーとすることができる。

4.6 PKIの運用

- 4.6.2 証明書の検証
  - 下位認証局がある場合
    - 証明書チェーンが長くなる。
    - ラストアンカーまで再帰的に検証を行わなければならない。
    - 安価な証明書は下位認証局が発行しているケースが多い。
- （教科書p.113の図4.19を参照）

4.6 PKIの運用

- 4.6.3 証明書の失効
  - 証明書は有効期間内でも破棄するケースがある。
    - 証明書の秘密鍵を紛失又は漏洩した場合
    - 証明書に記載した事項に変更が生じた場合
  - 証明書失効を公開する手段
    - CRLモデル
    - OCSPモデル

4.6 PKIの運用

- 4.6.3 証明書の失効
  - CRL（CRL: Certificate Revocation List）モデル
    - 認証局が失効された証明書リストを定期公開する方式
    - 証明書失効リスト（CRL: Certificate Revocation List）
    - CRLモデルの問題：失効した証明書が記載されるまでにタイムラグが発生する。（delta CRLで問題を緩和）
- （教科書p.114-115の図4.20-4.22を参照）

4.6 PKIの運用

- 4.6.3 証明書の失効
  - OCSP（Online Certificate Status Protocol）モデル
    - 証明書の正当性をリアルタイムで確認可能
    - OCSPサーバーが証明書利用者からの証明書失効情報の問い合わせに「有効」「無効」「不明」で応答
- （教科書p.115の図4.23を参照）

【次回予告】
第7回
演習（1）
（中間試験対策）

また来週！