情報ネットワークⅡ（情213）

【第5回】

認証技術

（教科書：第3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2日）

第3章：認証技術

3.1 認証技術の基礎

- 3.1.1 認証技術の用語
  - 認証（主体認証）とは「誰にどのリソースにアクセスさせるかをあらかじめ決めること」。
  - 認可とは「どのリソースにどのようにアクセスさせるのかのポリシーを決定・付与すること」。
  - アクセス制御とは「認可ポリシーに従いどのリソースにどのようにアクセスさせるかの実際の制御のこと」。アクセス制御の一覧表をアクセス制御リスト（ACL: Access Control List）と呼ぶ。
- （教科書p.66の図3.1を参照）

3.1 認証技術の基礎

- 3.1.2 素朴な主体認証と認証プロトコル
  - 「主体」は人を指すだけではなく、ITシステム、電子デバイス、ソフトウェアなどを指す場合もある。
  - 素朴な主体認証：利用者の目の前にあるPCなどで管理されているパスワードでの認証。
  - 認証プロトコルによる認証：インターネット等の通信路上に存在する脅威に対する対策をした認証。
  - ID連携（IDフェデレーション）：組織間をまたいでシングルサインオン（SSO）を実現する認証。

3.2 主体認証

- 主体認証とは？
  - 「誰」・「何」を識別する技術
  - 主体認証の3つのカテゴリー
    - 主体の知識による認証
    - 主体の所持するものによる認証
    - 主体の身体的な特性による認証
  - 2要素認証（多要素認証）
    - 主体認証を2つ（以上）組み合わせる認証

3.2 主体認証

- 3.2.1 主体の知識による認証
  - パスワード認証、パスフレーズ認証、PIN（Personal Identification Number）を用いた認証
  - 文字数：パスワード＜パスフレーズ
  - PIN：秘密の識別番号（暗証番号）
  - システム運用ポリシーが重要
    - パスワードは定期的に更新する
    - 辞書にある単語は使用しない
    - 過去に使ったパスワードは再利用しない
    - 利用されていないアカウントの無効化、等
  - 問題点：パスワード等を忘れてしまう可能性がある。

3.2 主体認証

- 3.2.1 主体の知識による認証
  - パスワードデータはハッシュ化して格納
    - 同じパスワードでも異なるハッシュ値となるように「塩（乱数値）」と併せてハッシュ化する。
    - ハッシュ関数は、MD5、SHA-256、SHA-512などを利用。
    - Windowsにおいては、NTLM（v2）方式が推奨されている。
- （教科書p.70-71の図3.2,表3.1を参照）

3.2 主体認証

- 3.2.1 主体の知識による認証
  - パスワードクラックツール
    - 基本的には平文を総当たりでマッチングするブルートフォース型のパスワードクラックツールが多い。
    - レインボーテーブルを使って高速にハッシュ値を解析するツールもある。
  - ワンタイムパスワード（OTP: One Time Password）
    - 認証の際に1度だけ使用するパスワード
      - 暗号学的な一方向性関数を用いたもの
      - ハードウェアトークンを用いた時刻同期型のもの
    - PFS（Perfect Forward Security）を実現する。
- （教科書p.72-73の図3.3-3.5を参照）

3.2 主体認証

- 3.2.2 主体の所有するものによる認証
  - ICカードやワンタイムパスワードでも利用するハードウェアトークンなどによる認証のこと。
  - 一定サイズのデータを保存することができるため、記憶（知識）等に比べて強固な暗号鍵を保持できる。
  - 問題点：紛失や盗難の可能性がある。
- （教科書p.74の図3.6を参照）

3.2 主体認証

- 3.2.3 主体の身体的な特性による認証
  - バイオメトリクス認証（生体認証）
    - 指紋、虹彩、静脈パターンなどを用いる。
  - 記憶などに依存せず、紛失や盗難も難しい。
  - 問題点：一度複製されると変更が難しく、「他人受け入れ」や「本人拒否」が問題となる。
- （教科書p.75の図3.7-3.8を参照）

3.3 認証プロトコルの基礎

- 3.3.1 脅威モデル
  - インターネット等の通信路における脅威
    - 盗聴、改竄、ハイジャック、なりすまし、捏造、再送
- （教科書p.76の図3.9を参照）

3.3 認証プロトコルの基礎

- 3.3.2 パスワードによる認証プロトコル
  - 概念①: 当事者しか知らない情報の所持を確認する
    - 全ての脅威に対して脆弱！
  - 概念②: パスワードをそのまま送らない
    - 再送攻撃（リプレイ攻撃）に対して脆弱
  - 概念③: Challenge/Responseを使う
    - クライアントがサーバーを認証しない（脆弱）
  - 概念④: 相互にChallenge/Responseを使う
    - ほぼ安全に認証可能
- （教科書p.77-79の図3.10-3.13を参照）

3.3 認証プロトコルの基礎

- 3.3.3 公開鍵ペアを用いた認証プロトコル
  - 公開鍵ペアを暗号化に使った認証
    - サーバーとクライアントが各々が持つ公開鍵・秘密鍵を使ってChallenge/Responseを交換することで相互に認証。
- （教科書p.80の図3.14を参照）

3.3 認証プロトコルの基礎

- 3.3.3 公開鍵ペアを用いた認証プロトコル
  - デジタル署名を使った認証
    - 秘密鍵でデジタル署名し、公開鍵で復号することで認証。
    - この仕組みは盗聴可能であるが、相互認証がokであればDH鍵共有アルゴリズムと組み合わせることにより、あとは安全に共通鍵暗号化方式の暗号化鍵を交換可能。
- （教科書p.81の図3.15を参照）

3.4 ID連携

- ID連携とは？
  - 利用者のID情報及びそれに付随する属性情報を、別々の組織で運営されているサービス間で連携して交換する仕組み。
  - 属性情報：IDによって特定される、年齢、性別、所属などの主体に付随する情報。
  - ID連携の標準技術：SAML、OpenID

3.4 ID連携

- 3.4.1 ID連携を用いたSSO
  - SSO（Single Sign On）とは、利用するサービスごとにログインし直さずともサービスを利用できる仕組み。
  - SSOでは、サービス間でパスワード情報を提示する必要なく各サービスを利用できる。
  - ID連携を用いたSSOでは、連携する組織間で予め連携のための情報を交換しておき、ある組織のサービスにログインすると別組織のサービスも利用可能。
- （教科書p.83-84の図3.16-3.17を参照）

3.4 ID連携

- 3.4.2 ID連携の実装技術
  - SAML（Security Assertion Markup Language）
    - OASISによって策定された認証・認可プロトコル
    - 政府や大企業（そのSaaS）が適用対象
    - Shibboleth, OpenSAMLで実装
    - 認証と2つの認可（属性情報、アクセス制御）
    - 認証情報はあらかじめ想定したサーバーのみに限定

      → 閉じたサービス形態
    - 構成要素
      - IdP（Identity Provider）, SP（Service Provider）, トラストサークル, メタデータ, Name Identifier
- （教科書p.85の図3.18を参照）

3.4 ID連携

- 3.4.2 ID連携の実装技術
  - SAMLを用いたSSO
    - WebブラウザによるSPへのアクセスをトリガーとするSP-Initiated SSO（主流）と、IdPへのアクセスをトリガーとするIdP-Initiated SSOの2種類。
- （教科書p.87の図3.19-3.20を参照）

3.4 ID連携

- 3.4.2 ID連携の実装技術
  - OpenIDについて
    - OpenID Foundationが推進
    - URL形式のIDを用いるのが特徴
      - 例：https://example.com/Cifq4SRHabyY3YAaFAg
        - https://example.com/ : OPのURL
        - Cifq4SRHabyY3YAaFAg : 利用者の識別子
    - 現行はOpenID2.0、次世代はOpenID Connect。
    - 構成要素
      - OP（OpenID Provider）, RP（Relying Party）, User-Supplied Identifier, Claimed Identifier, OP Identifier, OpenID AX（Attribute eXchange）（拡張仕様）
- （教科書p.88の図3.21を参照）

3.4 ID連携

- 3.4.2 ID連携の実装技術
  - OpenIDを用いたSSO
- （教科書p.89の図3.23を参照）

【次回予告】
第6回
PKI
（第4章）

また来週！