情報セキュリティと倫理講習

第1回

ytoku
2015-07-03@MMA部会

情報セキュリティ

- 情報セキュリティとは何か　「何を」「何から」守るのか
  - 狭義の情報セキュリティ:
    - 情報資産を攻撃者から守る
  - 広義の情報セキュリティ:　一般的な定義
    - 情報資産をあらゆる脅威から守る

攻撃者以外の脅威とは?

- 自然災害
- 機器の故障
- 誤操作

など

3･11以降のキーワード「事業継続性」
東京本社が被災しても,
支社で業務を継続できるか?

CIA

- 情報セキュリティの三本柱
  - **C**onfidentiality　(機密性)
    - 許可された人以外には情報にアクセスさせないこと
      - 関連例: 情報漏洩
  - **I**ntegrity　(完全性)
    - 情報が意図した状態に維持されていること
      - 関連例: 某キャリアでダウンロードした画像が**なぜか**劣化してたりとか
  - **A**vailability　(可用性)
    - 必要なときに情報を利用できること
      - 関連例: システムダウン

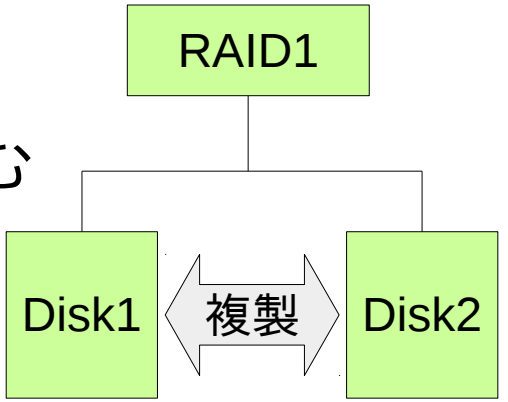
バックアップ

- データの複製を別のところに保存しておく
- 情報が失われないようにするための措置
  - 完全性・可用性

- 物理的に異なる媒体に保存されるべき
  - 同じHDDに保存→ディスク故障
  - 同じPCに保存→雷で全滅
- 地理的に離れた場所にあると更に好ましい
  - 同じ家に保管→火災，津波

RAID1はバックアップの代わりになるか

- RAID1とは
  - 2台以上のHDDなどに常時同じ内容を書き込む
  - 1台壊れても他のHDDで運用が継続可能
    - 可用性



- RAID1は「同じPCの別のHDDにデータをバックアップ」の代わりになるか？
  - A: ならない.
  - 対処できない例
    - 誤操作によるデータ消失
    - ファイルシステムの破損

インターネットは安全ではない

- インターネットの構造
  - 多くのネットワーク事業者によるバケツリレー
  - 経路はネットワーク事業者同士の情報交換で決まる
- 盗聴の危険性
  - 経路上の事業者に中身を覗かれたら？
  - そもそも，本来必要のない経路を通らされたら？
    - cf. BGPハイジャック

公衆無線LANも安全ではない

- 暗号化されていても, たいてい鍵は共通
  - 鍵を知っていれば誰でも復号できる
- そもそも接続先は本物か
  - WPA2 EAP以外では本物か確認する手段がない
- cf. Darkhotel

暗号通信

- 盗聴・改ざんなどを防ぐにはどうすればいいか
  - 暗号技術を利用
- 攻撃に対する対策技術
  - 盗聴: 暗号化
  - 改ざん: メッセージ認証
  - なりすまし: 認証
- 「何を防ぐために暗号を使っているか」を知るのが重要

SSL / TLS

- 通信を暗号化・認証するレイヤー
  - OSI参照モデルの第5層に相当
- 仕組み
  - 公開鍵暗号で通信相手を認証し
  - 公開鍵・共通鍵暗号で通信を暗号化し
  - メッセージ認証コード(MAC)で改ざんを検知する
- TLSはSSLの後継規格
  - いい加減SSLは古くて脆弱性だらけなので滅ぶべき
    - ただしTLSのことをSSLと呼ぶ場面は多い
  - RFC 7568: Deprecating Secure Sockets Layer Version 3.0
    - SSLは死んだんだ。いくら呼んでも帰っては来ないんだ。

Web

- Webの通信はデフォルトでは暗号化されていない
- Webで機密情報を送信する機会は多い
  - 個人情報
  - クレジットカード番号
- 通信を暗号化するのは重要
- 安全性を確保するために確認すべきこと
  - 産総研 RCIS: 安全なWebサイト利用の鉄則 http://www.rcis.aist.go.jp/special/websafety2007/

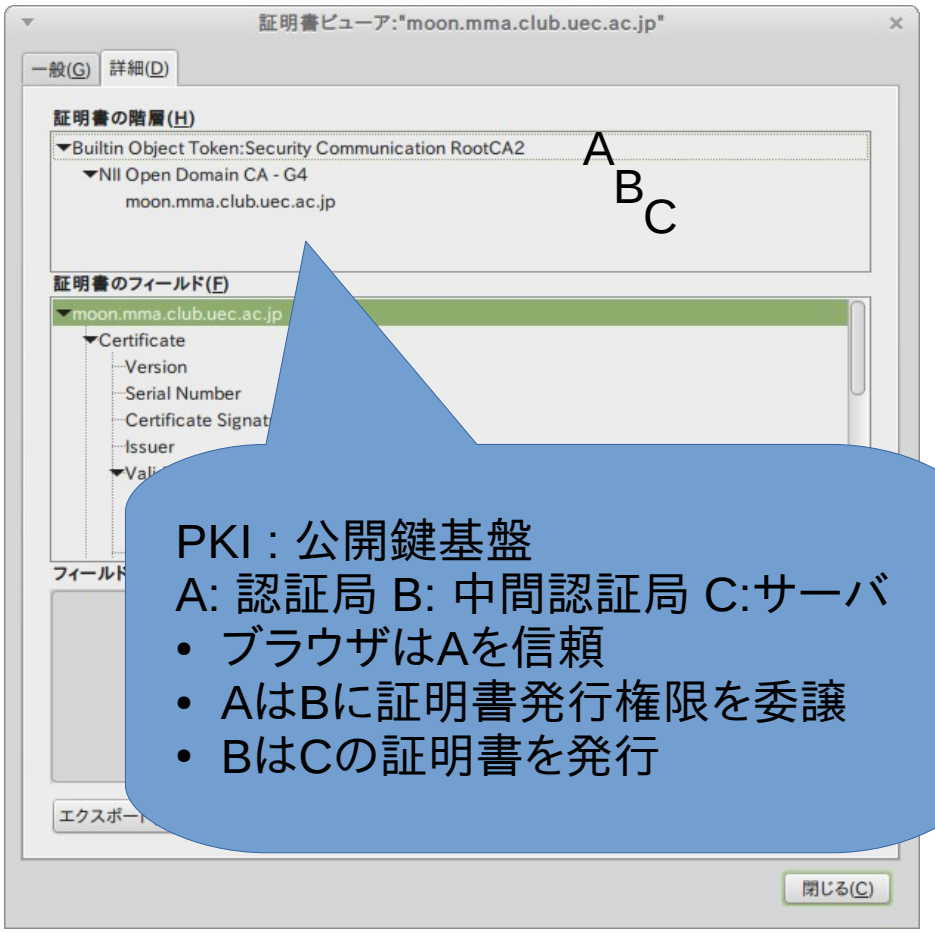
Web :: SSL/TLS

- WebブラウザでSSL/TLS通信しているときは鍵マークが表示される

- 鍵マークからわかること
  - 通信相手との通信が暗号化されている
  - 通信相手との通信が改ざんされていない
  - 通信相手はそのドメイン名の正当な利用者である
- 鍵マークだけからは分からないこと
  - 通信相手が意図した法人・人物か
    - そのドメイン名、本物ですか？

Web :: サーバ証明書

- 証明書: 通信相手の身元を証明
  - ただし「身元」のレベルには差がある



Web :: EV証明書

- EV証明書: 対象の法人の実在性まで証明
- ブラウザ上で緑色+鍵マークの横の法人名で表示

- 従来の証明書:「身元の確認の度合い」にバラつき
- 証明書の発行に厳格な条件が設定

Eメール

- Eメールも通常は暗号化されていない
- 暗号化規格はWeb程は普及が進んでいない
  - S/MIME
  - PGP/MIME
    - 手軽に使えるのはPGP/MIME
- SMTP, POP3, IMAPの「暗号化」設定は
  あくまでも「サーバ<->クライアント」間の暗号化
  - メールサーバ間の配送は保護されない