IRRのセキュリティについて

IRRの認証機能について

社団法人 日本ネットワークインフォメーションセンター
技術部　セキュリティ事業担当　木村泰司

概要

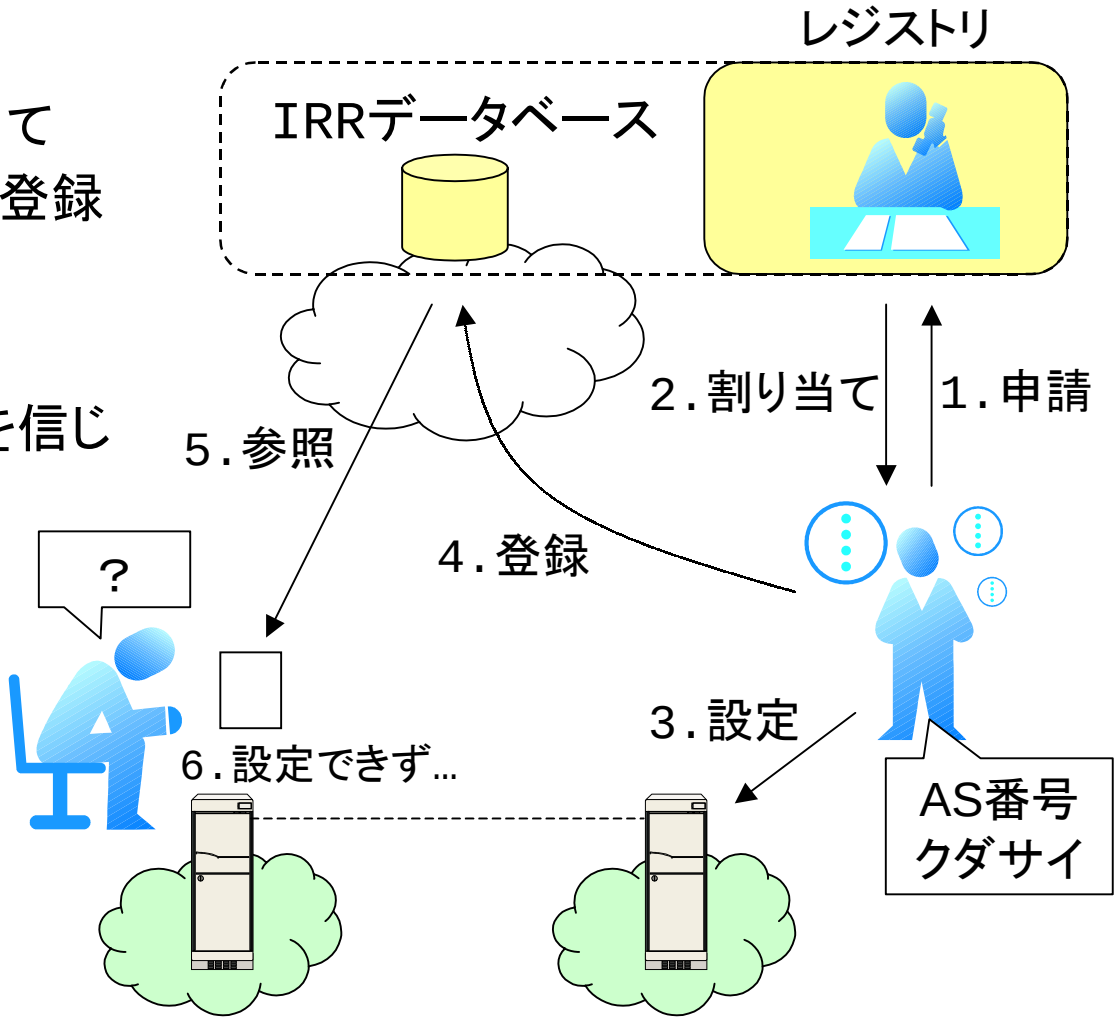
- セキュリティに関する考察
  - IRRデータベースの利用モデルと安全性
  - リスクの種類
  - 原因と安全策
  - 認証方式の種類と運用
  - 提案　-　認証機能
    - ユーザ認証とデータ認証

IRRデータベースの利用モデルと安全性

- 利用概要
  - レジストリによる割り当て
  - IRRデータベースへの登録
  - 参照と設定

- IRRで管理している情報を信じて設定してもよいか

登録情報の安全性
↓
リスクと安全策



リスクの種類

- IRRデータベースが利用不可能になる
  - 登録情報を参照できない状態
    - → ルータの然るべき設定変更ができず(？)、全接続変更不可
  - 登録情報を登録できない状態
    - → 新規のBGPルータの設定ができない(？)。メールで連絡。
- IRRデータベースのエントリが利用不可能になる
  - 登録状況が登録者の意図通りではない状態
    - ユーザ:「登録した通りでない」
  - 登録内容が設定関係者の意図通りではない状態
    - ユーザ:「登録した通り」 IRR・ピア:「登録内容に間違い」

今回の話題

登録状況が登録者の意図通りではない状態と原因

- 登録情報自体の状況
  - 意図しない変更・削除
    - 災害
    - サーバ／クライアントのバグ
    - クライアント／ユーザへのなりすまし行為
  - 登録時の不正
    - サーバへのなりすまし行為 + man-in-the-middle
    - クライアント／ユーザへのなりすまし行為
- 利用上の登録情報の状況
  - 参照時の不正
    - サーバへのなりすまし行為
    - 伝送路での書き換え（参照時、ミラー時）

なりすましや伝送路での書き換えは、暗号技術をうまく使えば防げるのではないか。

認証方式と運用

	mail-from	crypt-pw,md5	公開鍵を使った認証
なりすましの検出	×	△	○*
改ざんの検出	×	×	○*
エンティティ*	メールアドレス＋ユーザ	パスワード＋ユーザ	鍵ペア＋ユーザ

*運用が変わる要素　－　メールを使ったピアの確認より…

- なりすましの検出、エンティティ　－　ユーザと鍵ペアの登録手続き
- 改ざんの検出　－　鍵の有効性の確認

提案　－　認証機能

- 公開鍵暗号を使った認証機能
  - 運用：登録時の鍵の登録
  - 技術：登録情報に鍵を格納、認証方式の追加
    - 格納例
      - auth: x509
      - mntnerかpersonオブジェクトへの鍵の登録
        （要検討）認証対象が誰か
    - データ形式例
      - RPSLかCRISPで署名データを扱う

安全性と認証の仕組みを考える
際の考え方の一つに

RIPE NCC

- RPSL を使って証明書を格納
  - 格納方法
    - auth: X509-<auto generate uniqe id>
    - 証明書の格納に key-cert オブジェクトを利用
      - key-cert: X509-14
        certif: -----BEGIN CERTIFICATE-----
        certif: MIIDm...
        :
        certif: -----END CERTIFICATE-----
    - SSLを想定。将来的にS/MIMEも。（認証情報の一元化）
  - 利用方法
    - LIRPortalで利用
    - PGPと同様に登録された証明書だけを使った検証
      - 証明書パスを辿らない

APNIC

- MyAPNICのデータベースで証明書を格納
  - 格納方法
    - 役割(Corporate, Administrator, Admin, Technical, Training)と関連(？)
    - RPSLのデータmntner, person等との組み合わせはデータベースの上ではない。(登録時にnic-hdlを確認)
  - 利用方法
    - MyAPNIC(TLS)