IETFセキュリティエリアの動向

富士ゼロックス株式会社
稲田 龍
<Ryu.Inada@fujixerox.co.jp>

JNSAのIETFでの活動

- 第54回 IETF@横浜
  - PKIX-WGにてChallenge PKI 2001(相互接続実験)の報告
- 第55回 IETF@アトランタ
  - PKIX-WGにてChallenge PKI 2001の続報およびChallenge PKI 2002(テストスイーツ)の中間報告
- 第56回 IETF@サンフランシスコ
  - PKIX-WGにてChallenge PKI 2002の報告とデモンストレーション
- 第57回 IETF@オーストリア ウィーン
  - PKIX-WGにてmPKIの説明
- 第58回 IETF@ミネアポリス
- 第59回 IETF@大韓民国 ソウル
  - mPKI I-DとRFC化を画策中

詳細は島岡氏のプレゼンテーションにて

IETFでのSecurityに対しての意識

- **必須！**
- RFCには”Security Consideration”がないと受け付けられない。
- 毎回、初日(通例日曜日)にSecurity Tutorialがある。

- 第59回の場合、参加者は300名程度。満席
  - SUNのRedia Perlman女史
    - インターネットでなせ、Securityが重要であるか
    - 技術的なコンセプト
    - 守るための個別の技術
    - 暗号技術

    を説明

Redia Perlman女史

最近のSecurity Area

- Area Directorの交代
  - MIT Jeffrey Schiller 氏の退任
  - Virgil Security Russ Housley氏に
  - AT&T Bell Steven Bellovin氏は留任

よりアプリケーション向けに活動を遷移するため?

Security Area Directors:
Steven Bellovin氏(左)/ Russ Housley(右)

最近のSecurity Area

- Securityはもはや特別のものではない。
- 今までの議論、蓄積を元に…
  - 各エリアのアプリケーション/プロトコルに次々とセキュリティ機能を追加
    - WindowsのLogon認証にKerberosを利用
    - DNSの内容に対して電子署名(dnssec)
    - TCPパケットにMD5 Signature
    - TLS/CMSをより広範囲のアプリケーションへ採用
- 規格作成から利用への動き
  - ちょうど数年前のIPv6の状況に似ている?

PKIX-WG

- **終焉フェイズへ**
  - **アプリケーションへの応用へ**
    - AAA/SIP**などへの応用→新しい**WG?
    - LTANS、pki4ipsec
  - **基本的なプロファイルはほぼ決定した。**
    - Son of RFC3280
    - QC
    - Proxy Certificate
  - **証明書検証･パス検証に関しては未完**
    - **継続審議**

PKIX-WG Chair Stephan Kent氏

PKIX-WG Chair: Tim Polk氏(左)

PKIX-WG

- TSP
  - LTANS-WG**へ議論が移るか**?
  - JNSA Challenge PKI 2003**との関わりは**?

PKIX-WG

- 証明書の記載情報に関しての議論
  - より個人を特定する方向へ
    - Qualified Certificate
  - その一方で個人情報の保護
    - 韓国のKISA Jongwook Park氏と米国NIST Tim Polk氏の提案するSIM
      - 証明書内に格納するプライバシー情報(住所、生年月日、性別、氏名など)をどう証明書内に表現するかが問題
      - 特定の方式で暗号化した情報を記載
        - » 適切な権限を持った利用者のみに情報が開示される方式を提案

KISA Jongwook Park氏

PKIX-WG

- **相互接続実験**
  - NISTがPPを作成中
  - 米国のベンダにて相互接続実験が行われている
  - JNSAの相互接続実験/mPKIの提案
    - 詳細は島岡氏の講演にて
- **他組織との連携**
  - EUにおける活動
    - ETSI/EESSI
  - OASIS PKI TCとの連携があるか?
    - PKI Action Planとの関わりは?
  - JNSA? アジアPKIフォーラム?

Jim Schaad氏

OASIS PKI TCのSteve Hanna氏

LTANS-WG

- LTANS-WG (Long-term archiving and notary services)
  - **セキュアなデータのアーカイブと公証サービスのためのデータ構造とプロトコルを決めることを目的とする**WG
  - **第**58**回**IETF**に作られた**WG**である。**

IPsec-WG

- IPsec-WGの当初の目標は達成

- しかし…
  - なかなか使われない
  - IKEの実装はすでに完了
    - Shared Secretではほぼ、相互接続性に問題はない
  - IKEが遅い、概念が難しい
    - 新たなスキーマ、より簡便かつ安全な方法の議論
  - IKE2の開発が進められている

pki4ipsec

- IPsecでPKIを使うためのプロファイルを決める
  - 第58回でBOF、第59回で正規のWGへ
  - IPsec-WGでの議論は継続
    - IPsec-WGは、プロトコルの決定
    - Pki4ipsecは、プロトコル上での扱い

    と、すみわける?

IKEv2 Mobility and Multihoming WG

- IPsecにてモバイルでの必要性が高い、ローミングやマルチホーミングを検討するWG
- 第59回にて正規のWGへ

- IPsec-WGと独立/協調して活動をする?

VPN コンソーシアム ポール･ホフマン氏

日本人の台頭

- **奈良先端**/WIDE **山口英氏**(Security**全般**)
- NICT **大野浩之氏**(INCH)
- JPNIC **木村泰司氏**(ENROL)
- **横河 坂根氏**(IPsec)
- **松下電工 福田氏**(INCH)
- **セコムトラストネット 島岡氏**(PKIX)

次は誰?

松下電工 福田氏

- netCocoonの作者
- IPsec/SSL/TLSの評価、設定の正常化のためのツールを作成し、最近はパケットトレースに関してINCHにて活動を行っている

セコムトラストネット 島岡氏

- mPKIのI-Dを著し、マルチドメインの概念の整理と今後の構成に関して提案をしている

次は?