第 63 回 IETF 参加報告

NPO 日本ネットワークセキュリティ協会
安田　直義

第 63 回 IETF 参加メンバー

セコム株式会社 IS研究所
島岡 政基
富士ゼロックス株式会社
稲田 龍
富士ゼロックス株式会社
黒崎 雅人
(社)日本ネットワークインフォメーションセンター
木村 泰司
NPO 日本ネットワークセキュリティ協会
安田 直義

2005年7月31日から8月5日までパリ凱旋門近くのLe Palais des Congress de Parisにて開催された第63回IETF（http://www.ietf.org/）ミーティングに、JNSA ChallengePKIプロジェクトとして参加したので報告をする。

IETFは、インターネット上のプロトコルの標準化を行っている団体であり、8つのエリアで活動を行っている。通常は、8つのエリア上のWGで電子メール上での議論を行い、標準化を行っているが、年に3回(通常は米国内2回、米国外1回)のペースで「オフライン」での会合を行っている。

今回のミーティングは、36カ国(前回比＋8ヶ国)、1,454人(前回比＋287人)の参加で行われた。ヨーロッパでのミーティングであり、バカンスをかねて家族づれで参加している人も多く、前回の米国開催より参加者は増えている。

今回のミーティングの参加目的と概要は、次のような3点にある。

1. PKI相互運用に関するMulti-Domain PKIの問題について、セコムトラストネット島岡氏のMulti-Domain PKI I-D を中心とした内容に関して、ETSIのPatrick Guillemin氏(以下Patrick氏と表記する)と広く意見交換を行った。Patrick氏は、ETSI（European Telecommunications Standards Institute）のPlugtests Technical Managerをしており、ヨーロッパの相互運用性に関するキーマンである。Patrick氏からETSIを始めとするヨーロッパや世界的な認証に関する動向に関して話が進み、主にUTF8String問題に関して、2006年1月16～17日にSophia AntipolisのETSIで開催されるETSI Security Workshopで講演するために島岡氏等Challenge PKIのメンバーを招待したい、という要請があった。
2. Hash BOFを始めとするハッシュ関数の脆弱性問題に対する最新動向を議論しているWGに参加した。SHA-1の対衝突性を向上するために下記のような提案が行われ議論された。
   - Truncate SHA-256
   - Random Hash
   - Preprocessこれらに関して、NIST Cryptographic Hash Workshopでの継続議論の告知が行われていた。
3. PKI関係だけではなく、情報セキュリティ全般の最新動向を知るため、Security Areaの主要WGに参加する。

SHA-1問題は、新しいアルゴリズムへの移行がポイントになりそうである。また、PKIマルチドメイン問題に限らず、UTF8コードの問題はしばらくはトレンドになる感じがする。匿名認証の関心も高まっており、認証自体の考え方が整理されようとしている。

PKI 相互運用に関する ETSI との意見交換

Patrick Guillemin氏と、Multi-Domain PKIを中心としたPKI相互運用に関連する問題について、広く意見交換を行った。

Challenge PKIの近況説明

島岡氏から、ChallengePKIに関する近況を説明した。

- マルチドメインPKI関連の話題
- 相互運用テストスィートの更新状況

マルチドメインPKI関連として、Multi-Domain-

PKI-I-D（mPKI I-D）の更新状況について説明し、mPKIに関する情報交換などを行った。

また、UTF8String問題に関しても情報交換を行い、ヨーロッパでのUTF8String問題への関心度が高いことを聞いた。

昨年のIETFでPKIX-WGに発表した相互運用テストスィートのその後の改良などについて情報提供と情報交換を行った。タイムスタンプやS/MIMEについてのテストケースを扱えるように拡張されていることについて、特に興味を示された。

Patrick Guillemin 氏との打ち合わせの風景
(左から：黒崎氏、Patrick 氏、稲田氏、木村氏、島岡氏)

JPNICのIPアドレス認証局の説明

木村氏から、JPNICで実現しようとしているIPアドレス認証局について説明がなされ、その後ディスカッションが行われた。IPアドレス管理者とJPNICとの間で双方向認証を行うというメカニズムだが、実用的に運用する際の問題点などについて、忌憚の無い議論が行われた。

ETSI Security Workshopへの招待打診

このようなディスカッションを行った後、Patrick氏からETSIを始めとするヨーロッパや世界的な認証に関する動向に関して話が進み、Patrick氏から、主にUTF8String問題に関して、2006年1月16～17日にSophia AntipolisのETSIで開催されるETSI Security Workshopで講演するために招待したい、という要請があった。

招待講演のお誘いが9月12日に届いており、島岡氏、稲田氏を中心に参加する方向で調整している。

参考：

http://portal.etsi.org/securityworkshop/Home.asp

> Date: Mon, 12 Sep 2005 15:49:01 +0200
> From: "Dionisio Zumerle"
>
> （中略）
>
> I have been discussing with Patrick on JNSA and UTF8 in Certificate/PKI.
>
> I think the occasion is ideal to invite you to the ETSI Future Security Workshop (see http://portal.etsi.org/securityworkshop/Home.asp) to be held in ETSI's Headquarters in Sophia-Antipolis, France on 16-17 January 2006.
> The workshop is about revising what has been done in the security areas (so PKI and Signatures is a significant part of it), and deciding on what has to be done from now on.
> I think it would be a good occasion to present your views and ideas. If of your interest you could propose a presentation.
>
> In parallel, I would like to have your view on a JNSA possible participation in ETSI's work on electronic signatures (TC ESI).
>
> Kindest Regards,
> Dionisio Zumerle
> ETSI Technical Officer

Hash BOF

8月1日 18:15～19:45に開催された。出席者は100人程度以上で満杯状態だった。HASHは直前にSHA-1の脆弱性が発表されるなど、高い関心を集めており、熱気にあふれていた。IETFでHashに関するBOFが開催された背景と論点、結論をまとめると下記のようになる。

- **背景：**
  - SHA-1に対する衝突攻撃の成立に対する検討が必要

- ハッシュ関数の衝突攻撃(Collision Attack)にフォーカスして議論
  ☆原像攻撃(Pre-image Attack)についてはOut of Scopeである

● **論点:**
- IETFの中で議論できるWGを立ち上げるべきか?
- ハッシュ関数の見直しを図り標準化すべきか?

● **結論:**
- IETFはハッシュ関数の設計には取り組まず、あくまでハッシュ関数を使ったプロトコルの設計をする
- NIST Workshopで、より詳細な情報が集まるはずなので、次回IETFで再度検討すべきだろう

次に、Hash BOFでの特徴的なプレゼンテーションを紹介しておく。

NIST Cryptographic Hash Workshop

NISTのCryptographic Hash Workshop開催の告知が行われ、議論の継続とIETFで対応できない課題についての議論を行いたいとの紹介があった。

● **発表者**
- NIST/CSDのWilliam Burr氏
- 口頭でのアナウンスのみ

● **開催要領**
- 期間: 2005年10月31日～11月1日
- 場所: Maryland州 NIST

● **詳細**
- http://www.csrc.nist.gov/pki/HashWorkshop/index.html
- SHA-256へ移行するにあたっての課題(移行、対症療法)
- 後述の一部のSHA-1対症療法の紹介

新しいハッシュ関数の展開

SHA-1に変わるハッシュ関数の実装とそれまでの対策についての検討を示した。

● **発表者**
- Steve Bellovin氏(元Security AD, コロンビア大)
- Eric Rescorla氏(TLS WG Chair, IESG)

● **課題**
- 次の新しい実装が入手できるまでの対策を考える
- S/MIME, TLS, IPsec/IKEについてハッシュ関数の影響を分析する
- ほとんどのプロトコルにおいて、移行のためのBCPが必要だろう

メッセージ前処理によるSHA-1の対衝突性向上

SHA-1を若干モディファイし、問題となった対衝突性を向上させるアイディアが説明された。

● **発表者**
- Russ Housley氏(元RSA社, Security AD)
- 現状の問題点の指摘
- SHA-1の耐衝突性低下のメカニズム等

● **提案内容**
- メッセージ前処理(SHA1pp)による耐衝突性向上を提案
- 前処理方法にはいくつかのバリエーションがある
  ☆2つの変換方式:
  Message WhiteningとMessage Interleaving
  ☆2つの実装方式:
  within SHA-1とoutside SHA-1
- 既存のSHA-1と互換性が高い

● **結論**
- 最小の影響でSHA-1を一時的に延命させる技術
- 最終的には新しいハッシュ関数が求められる

乱数をハッシュの一部に含める

ハッシュの一部に乱数を含めることにより、対衝突性を向上させようという提案で、以下にランダムなSaltを生成するかを熱心に説明していたが、かなり数学的な内容を含んでいたので、難解だった。

● **発表者**
- Ran Canetti氏(IRTF CFRG Chair, IBM)

● **提案内容:**
- Use Hr（x）instead of H（x）
  r is a random "salt value"
- To sign a message x:
  With new random salt r, set h = Hr（x）
  s = RSA-1（encode（h,r））
  The signature is the pair（r,s）

次世代ハッシュ関数の提案

NISTのTim Palkから、ハッシュ値長を固定と次世代ハッシュ関数の提案があった

● **発表者**
- Tim Polk（PKIX WG Chair, NIST）

● **次世代ハッシュの課題**
- ハッシュ値の長さを仮定しているアプリが多い

● **提案**
- ハッシュ値を160bitに切り捨て、互換性を保つ
- 耐衝突性を低下しないためにメッセージにIVを付与してからハッシュを取る

● **懸案**
- IVの計算方法、安全性証明などが課題

3つのアプローチの比較

以上の提案の新しいアプローチを比較してみた。それぞれ特徴があり、今後の議論が待たれる。

	Truncate SHA-256	Random Hash	Preprocess
Hash Output Truncation	√		
Change Signature Size		√	
Randomness Required		√	
Replace SHA1 Code	√		
Change Message before Hashing		√	√
Execution Cost (time increase)	50-200% Depends on SHA-256 slowdown on platform	(not %) Depends on random generation	33-100% Depends whitening parameter

セキュリティエリアの動向

今回のIETFでのセキュリティエリアでの動向は下記のような感じであった。

● **PKIX WG**
- SCVP, 3280bis, CAdESなどの議論が進んでいる

● **LTANS WG**
- "Notary"から"Data Validation and Certification"へ用語変更した

● **MASS（Message Auth Signature Service）BOF**
- DKIM（Domain Keys Identified Mail)にフォーカスしている
- まずは "threat analysis" から始めようという方向でで進んでいる

● **SAAG**
- ITU-T X.805の紹介
  ☆Security Architecture for System providing End-to-end Communications
- Unicode Security Considerations（TR#36)の解説がされていた

● **Alien BOF, BTNS WG, PKI4IPsec WG, etc.**
- 上記のWGでも活発な議論があったようである

セキュリティエリアのまとめ

セキュリティエリアの全体的な流れとして、SHA-1ハッシュ関数問題、マルチドメインでの相互運用性、UTF8コード問題、匿名認証等々の話題がホットであった。

● **SHA-1問題**
- 新しいハッシュ関数への移行方法が鍵である
- NISTのHash WorkshopはWatchしておく必要があるだろう
- SHA-1互換で安全なハッシュの検討が必要
- SHA-256への移行は本当に可能だろうか？

- 2回の移行プロセスを踏むインパクトやコストを議論しなければならない

● **マルチドメイン問題**
- PKIに限らずマルチドメインでの相互運用の課題は大きい
- Unicode問題はしばらくトレンドになるかもしれない

● **その他**
- 認証における仮名、匿名などの使い分けはIETFでも関心が高まってきている
- もしかするとSecurity AreaよりもApplication Area, Internet Areaの方で議論は進んでいるかも知れないのでもう少し調査が必要だろう

村井先生が Postel 賞を受賞

IETF Plenaryで慶應義塾常任理事、WIDEプロジェクト代表の村井純教授がPostel賞を受賞した。

Postel賞は、故Jonathan Postel氏にちなんで1999年ISOCが設置したもので、インターネットに多大な貢献をした人に贈られている。村井氏は、歴代7人目の受賞でアジア初となる。アジア太平洋地域でのInternet普及への貢献と、IPv6の技術開発と普及への努力が受賞理由である。

For his vision and pioneering work that helped countless others to spread the Internet across the Asian Pacific region.
アジア太平洋地域のインターネットの展開に注がれた、彼の広い視野と開拓精神に基づく計り知れない貢献に対して。

端末ルーム

今回のIETFのターミナルルームは、場所の制約のせいと思われるが、24時間営業をしていなかった。会場と隣接しているConcorde La Fayetteホテルのロビーと、会場向かいのLe Meridien Etoileホテルのロビーでは24時間の接続サービスが行われていた。今回は無線LANの802.1XとWPAが使えるようになっていた。インターネット接続の概要を下記にまとめておく。

● 有線LAN（1ヶ所）
- ターミナルルームのみ

● 無線LAN（3ヶ所）
- 会場全体（夜10時まで）
- Concorde La Fayette（ホテル, 24時間接続）
  ☆会場に隣接
- Le Meridien Etoile（ホテル, 24時間接続）
  ☆会場の向かい
- 今回初めて802.1X認証が提供された。（無線LANのみ）
  ☆WPA _ PEAP/MSCHAPv2
  ☆France Telecomから発行されたサーバ証明書