セミナーレポート

第61回IETFミーティング報告

富士ゼロックス株式会社　稲田　龍
セコム株式会社 IS研究所　島岡　政基
NPO 日本ネットワークセキュリティ協会　安田　直義

11月7日より12日まで米国ワシントンD.C. Hilton Washingtonにて開催された第61回IETF（http://www.ietf.org/）ミーティングに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）のペースでいわゆる「オフライン」の会合を行っている。

今回のミーティングは、26カ国、1314人の参加者があった。米国内でのミーティングであり、必要な人間が必要なタイミングで参加することが定着したためか、全体に出席者は減少している。

今回のミーティングの参加目的は

1. セコムトラストネット島岡氏のMulti-Domain PKI I-Dの共著者であるNIST Nelson E. Hasting氏（nelson.hasting@ nist.gov 以下Hasting氏と表記する）との打ち合わせ
2. IPA/JNSAで行う証明書のUTF8化に関してVPN Consortium Paul Hoffman氏（paul.hoffman@vpnc.org 以下Hoffman氏と表記する）/ PKIX Co-chairであるNIST Tim Polk氏（wpolk@nist.gov）と意見調整および協力の要請
3. PKI関係のWGの状況把握（LTANS/PKI4IPSEC/OPSEC/EASYCERT等）

の3点である。

写真1　会場となったHilton Washington

報告内容要約

1. Multi Domain PKIに関して
   セコム株式会社 島岡 政基氏によるI-D “Memorandum for multi-domain Public Key Infrastructure（PKI）Interoperability”に関して、NIST Hasting氏と意識あわせと、この後の方向性に関して合意を得た。
2. 「UTF8String問題」に関して
   証明書の国際化を行うためのI-DとしてUTF8Stringを扱うI-Dの共同著者であるVPN Consortium Hoffman氏（もう一人の著者であるOASIS PKI TC Chair Steve Hanna氏はIETFに参加していない）に対して、JNSAがIPAより請け負った調査業務の概要と今後のスケジュールおよび現時点での方向性を説明し、合意に至った。
3. セキュリティエリアの各WG（主にPKI関連）の動向を把握することができた。

概　要

Multi-Domain PKI I-D

Hasting氏との打ち合わせは、11/9の11:30より13:30に昼食をとりつつ行った。

Hasting氏は、NISTのInformation Technology LaboratoryのComputer Security Divisionに属するエンジニアであり、PKIX-WGのCo-ChairであるTim Polk氏の同僚にあたる。

島岡氏は、今年の10月にIPAセキュリティセンター宮川氏とNISTに出張し、Hasting氏に島岡氏が作成しているMulti-Domain PKIのI-Dの共著者になることを要請し、快諾されている。今回のIETFの前に島岡氏はHasting氏にI-Dを送付しており、70近くのコメントをもらい、そのコメントを元に新たなI-Dの方針、意識あわせおよび改版したI-Dのスケジュールの調整を行った。

写真２　Nelson E. Hasting氏との打ち合わせの風景
(左より富士ゼロックス 稲田、セコムIS研究所 島岡氏、
IPAセキュリティセンター 宮川氏、NIST Hasting氏)

Nelson氏は、Multi-Domain PKI/Single Domain PKIの用語の定義の明確化とTrust Anchorについての扱いを気にしており島岡氏との間で意見の調整を行った。

証明書のUTF8化

証明書のUTF8化に関しての打ち合わせは、VPN Consortium Paul Hoffman氏と11/10の17:00–18:00に行った。

IPA/JNSAのUTF8に関する今後の活動に関して事前にHoffman氏にはメールを送ってあり、そのメールの内容と今後の展開に関して情報の交換を行った。

Hoffman氏は、証明書におけるString Matchingに関してのI-DをOASIS PKI TC Steve　Hanna氏と記述しており、第60回のときにもこちらの現状を伝えてある。

今回は、IPAの公募に採択されたことにより具体的な活動計画とスケジュールの提示が出来た。JNSAが行う調査案件において2月にIPAに対しての報告書の提出と、それをベースにしたI-Dを書くという話をしたところ、Hoffman氏が記述しているI-Dとの併合を提案された。JNSA側で作成予定のI-Dは、UTF8による証明書発行によりおきうる問題点の提示と認証局に対してUTF8による証明書を発行する際のガイドラインとなる予定であるが、Hoffman氏の意見によると、JNSAが作るI-Dはサンプルを提供する側面が強く、Hoffman氏のI-Dはプロトコルを提示するI-Dになるはずであるとのことである。Hoffman氏は、JNSAのI-DとHoffman氏のI-Dを併合することにより、よりわかりやすく説得力のあるI-Dとなるはずであると主張している。Hoffman氏のI-Dは、12月に第2版(01)が発行される予定であるとのことである。
Hoffman氏の提案に関して即答は避けたが、最低でも互いに参照しあうこと、状況を交換し続けることは意見の一致を見た。

また、SAAG後にHoffman氏より、String Match I-DがSon of RFC 3280(後述)の一部として併合されたことが知らされ、急遽、Son of RFC 3280に対してIPA/JNSAとして活動を起こすことが必要となり、Issueリストとして認識されるように調整を行った(PKIXのセクションを参照のこと)。

写真３　Paul Hoffman氏との打ち合わせ風景


写真４　Paul Hoffman氏との打ち合わせの後
(左より富士ゼロックス 稲田、Paul Hoffman氏、
IPAセキュリティセンター 宮川氏、セコムIS研究所 島岡氏)

PKI関係のWG

LTANS

11/9 9:00–11:30に開催された。出席者は20人程度で低調。裏にBetter-Than-Nothing Security BoFが開催されたためそちらに人気が集中したためと考えられる。
Document Statusの確認を行われた。各ドキュメントのステータスは以下のとおり。

1. Long-term archive service requirementsはまだまだかかりそう
2. Notary requirements Data certificationにフォーカスをあてて作成中
3. ERS（Evidence Record Syntax）
   I-Dとしてほぼ完成しているが、Long-term archiveからのコメントにより調整が必要

Long-termのI-Dは10月に発行された。今後の予定として次回のMinneapolisミーティングまでに1つ以上のバージョンを発行する予定。

現行のLong-termのI-Dにおける問題点として以下のものがあがっている。

1. メカニズムをより中立化する
   暗号・PKI機能をどうするべきか
2. ERSで行うべきことをLong-termでしていないか?
3. ワークフローの定義
   マルチステージでの承認行為は必要なのか?
   →必要である
   ERSでこの要件をサポートする機能を入れるべきである→ERSのI-Dへコメント
4. ポリシー要件の確立と強化が必要
5. その他もろもろ

以上の問題点を議論し、以下のことが決定された。

1. Minneapolis（次回IETF）前にLast Callしたい
2. ERSとの連携
3. WebDAVとの連携の準備
4. DVCSのようなプロトコルの開発が必要

Better than Nothing BoF

11/9 09:00–11:30に開催された。盛況で200名ほどの出席者があった。

IETFにおいて、新規の標準化を行う際は、まず、BoF（Bird of a Feather）を行い、Charterを作り賛同者を集める。BoFを3回行い賛同者が集まらない場合には、その標準化はIETFでは行わない仕組みになっており、今回のBetter than Nothingは、初めてのBoFである。

Chairは Joe Touch <touch@isi.edu>である。

現行のIPsecプロトコルでは、セキュリティに関する設定はall or nothingという選択となっており、IPsecプロトコルは可能性のある脅威に対して広範な防護を行う仕組みを提供しているが使われていない場合がままある。

理由として以下にあげるものがある。

1. 鍵管理基盤が必要
2. 設定の煩雑さ
3. 性能への悪影響等

今回のBoFでは既存のIPsecプロトコルに対して、事前の鍵共有(pre-shared secret)や鍵管理基盤の必要性を減らし性能面で悪影響の少ない、セキュリティ要件を緩和した仕様の策定を行うことを提案した。

この仕様では、既存のIPsecプロトコルと比較してセキュリティ粒度は低くなるが限定した環境内での利用に関しては十分であるとしている(例：Man in the Middle Attack以外の経路外からの攻撃に対する防護は提供可能。通信相手の身元について、裏書きする仕掛けは無いがコネクションそのものは防護可能)。

BCPもしくは、標準化プロトコル仕様として、標準化活動をしたいとのこと。BGPやDNSと併せて利用したいという。

写真5　超満員のBTN-BoF会場

SecSH

11/9の1415–1515に開催された。出席者は150名ほど。SecSH WGは、幾つかのI-Dを提出しているがここ1年、1回もミーティングを行っておらずI-Dも手を入れられない状況になっている。すでにOpenSSHはシステム管理者が利用するリモートアクセスソフトウェアとしてはデファクトスタンダードであり、標準化を推進することが必要である。今回、新たに新著者としてBill Sommerfeld <sommerfeld@sun.com>氏が名乗りを上げ、チェア代理として「標準化を進めるにどうするべきか」に関して議論を行った。

核となるCore I-Dに関してはIESGからのコメントもあり、それらの各コメントに関して議論および今後の方向性を定めた。他にも複数の関連I-Dがあるがこれらの改定は行わないこととなった。

OpSec

11/9 15:45–16 45に開催された。150人ほどが参加し盛況であった。

Operational Security Capabilities for IP Network Infrastructure（opsec）はSan Diegoで開催された第60回IETFで行われたBoFであったが、今回は正規のWGとして活動が開始された。

前回よりCharterが制定され主にISP/Enterpriseレベルのネットワークに対してのBest Current Practiceを提供するようこととなった。

今後、全体のフレームワークに関する文書、BCP、個々のデバイスに関する文書をISP向け/エンタープライズ向けに作成することとなった。

pki4ipsec

11/10 09:00–11:30に開催された。150人ほどの参加者がおり盛況であった。

Chair Paul Knight <paul.knight@nortelnetworks.com>, Gregory Lebovitz <gregory-ietf@earthlink.net>

写真 6　pki4ipsec-WGの会場風景

IPsecにおいてPKIの利用を行うためのプロファイルを策定するためのWG。IPsecは、5年以上前に標準化されたものであり、X.509電子証明書の利用も仕様に含まれている。しかし、現時点では大半のIPsecを使える機器類は証明書を使っていない。これらの原因として、「X509電子証明書の利用に関しての規定がIPsecでは明確になっていない」もあげられている。また、証明書の取得方式およびその他の証明書の操作（更新、削除など）も具体的な記述がなされていないなどもあげられている。

今回のWGでは、IPsecにおける証明書検証要件に関する議論の中で、証明書の失効検証や中間証明書の（取得および）検証についての是非が議論された。これらの処理には、時間がかかりIPsecのような下位層で通信を維持しつつ行うことは困難が伴うという理由で、多くの実装はこれらの処理に関して手抜きを行っている。

この議論については微妙な表現があり、当初は“allow to verify”とすべきかどうかを議論していたが、途中から“deny to verify”とすべきかどうかの議論へとかわっていった。

1. “allow to verify”
   賛成：verifyをoptionalな実装として認める。
   反対：verifyを明確な要件とはしない。
2. “deny to verify”
   賛成：verifyを実装すると仕様から逸脱することになる。
   反対：verifyを明確な要件とはしない。

今回は“deny to verify”がagreeされたのだが、これは“allow to verify”に対するdisagreeを意味するわけではないので、今後の実装を左右する大きな判断となったと思われる。

また、peer同士が互いの自己署名証明書を用いることの是非についても議論が交わされた。

今回のWGでは、標準化の方向性に関して以下の合意を得た。

1. CRLの取得はネットワークを用いた取得は仕様としない。
2. 複数階層に渡るPKIにおいて、中間認証局の証明書はネットワークを用いて取得する仕様とする。

pkix

11/10 13:00–15:00に開催された。150名ほどの出席者があり盛況。

通常のPKIXのミーティングと異なり、今回は事前にMLに対してCRLの扱いに関して大量のメールがやりとりされており、CRLの扱いに関しては白熱した議論がなされた。

また、すでにアナウンスされているがPKIX WGは、現在扱っている事案の処理が終わり次第、WGがクローズすることが決まっている。なかなか、クローズできる状況

写真 7　pkix-WGのチェアのTim Palk氏（左）とStephen kent氏

ではなかったが、おそらく次回、遅くても次々回のミーティングではPKIX WGのクローズがほぼ確実であると見られる。

今後、PKIに関する話題はSAAG（Security Area Advisory Group）にて議論されることになる。

インターネットにおけるPKIの利用のプロファイルとなっているRFC 3280の改訂作業が行われており（Son of RFC 3280と呼ばれている）、著者としてNISTのDavid Cooper氏が選出されたことがアナウンスされた。また、Son of RFC 3280に盛り込むべき事柄を11/19に迄にDavid Cooper氏にインプットすることが要請された。JNSAとして証明書のUTF8関連の問題をインプットした。

Son of RFC 3280は、今年中にI-Dとして発行される予定である。

SCVP（Simple Certificate Verification Protocol）の状況が説明された。SCVPのI-Dは16版となっており、15版より大幅な変更が行われており注意の喚起がなされた。SCVPのI-Dは、17版で終わりとすることになり今後は編集上の修正のみとし、機能の拡張は行わないこととなった。

新たにCRLの扱いに関して、AIA（Authority Information Access）を用いてCRLの署名者の証明書を得る仕様が提案された。これはIn-direct CRLなどを用いた場合、CRL単体ではCRLの署名者が正当な署名者であることを確定できないという問題点を解決するために、証明書の拡張領域であるAIAに正当なCRLの署名者の証明書を得るための情報を入れることを提案している。この提案は受け入れられた模様。

inch

11/11 09:00–11:30に行われた。30名ほどの参加者であった。

インシデント（セキュリティ事故）情報の交換フォーマットとしてIODEFというものがあり、これの標準化を行うWGである。昨今は、RIDという追跡情報のフォーマットも標準化している。

日本からはIPAの非常勤研究員のGlenn Mansfield博士と松下電工の福田氏がそれえぞれRIDの関しての利用のアーキテクチャとRIDの実装に関する経験に関して発表を行った。

写真 8　inch-WGで発表するJNSAの福田氏（松下電工）

easycert

11/11 13:00–15:00に開催された。約200名が参加。盛況であった。

Easy-to-Use Certificate BoFは、前回の60th IETFのSAAGにて開催が決まったBoFである。

BoFのチェアは、セキュリティエリアのADであるRussell Housley氏<housley@vigilsec.com>およびSteven Bellovin氏<smb@research.att.com>が務めた。

今回のBoFでは、すでにPKIを広く利用している3者の経験を話してもらい、その内容に関しての議論を行った。プレゼンテーションを行ったのは、MIT（マサチューセッツ工科大学）、Johnson & Johnson社およびDoD（国防総省）である。

プレゼンテーションおよびその後の議論の結果、PKIを

写真 9　easycert-WGチェアのSteven Bellovin氏（左）と Russell Housley氏

適切に使うためにはPKIに参加するメンバーの情報のデータベースがあり、認証の基盤を事前に構築しておくことが重要であると認識された。

PKIを使うためのプロトコルに関しては、すでに十分なものになっているとも認識された。その一方で、各プロトコルはそれぞれが証明書を要求することが一般的になっており、利用者が複数の証明書を持つ可能性があり、利用者が適切な方法で証明書を選択できる仕組みが欠けていることも認識された。

議論と議論の結論は、Steven Bellovin氏によりInformational RFCとしてまとめられることとなった。

Open Security Area Directorate (saag)

11/11 15:30–17:00に開催された。200名ほどの出席者がおり、盛況であった。

Open Security Area Directorateは、Security Areaの各WGの進捗状況と方向性を確認する場となっている。また、適宜に招待講演を行い、その後にSecurity Area全般の話題が議論される（ここしばらくはPKIに関しての議論が行われている）。

写真 10　SAAG-WGのミーティングの様子

今回の招待講演は、VPN Consortium のHoffman氏のIPsecにおける鍵交換プロトコルであるIKE（Internet Key Exchange）v1の暗号アルゴリズムの選択に関してと、NSAの新しい暗号ライセンスの担当者であるジュン・スタサク氏が楕円暗号に関してのライセンスに関してのプレゼンテーションを行った。

Security Area全般の話題としては、他のエリアで策定されているセキュアでないプロトコルをどうセキュアにしていくのかに関しての話題があった。

またSecurity AreaのArea Directoryとして長く務めたSteven Bellovin氏が引退し、新たにSam Hartman氏<hartmans-ietf@mit.edu>が就任した。Sam Hartman氏はSASL-WGのチェアを長く務めSASLの標準化に貢献している。

IETF Plenary

11/10 19:30–22:00に開催された。

IETFでは通常、水曜日と木曜日の夜のセッションにPlenaryが当てられているが、今回は水曜日のみとなった。

今回のIETFの参加者は1314名であり、26カ国より参加しているとのことであった。参加者の国籍の内訳は、米国が53%、日本が10%、韓国が5%、以下ドイツ、フランスと続き全体としてアジア勢が多く参加している状況である。特に今回のIETFでは、日本人が目に付いた。多くの日本人は、IPv6関連の活動を行っている。

今後はセキュリティ関連にも日本人が増えることを期待している。

写真 11　IETF Plenaryの会場風景

Plenaryとしての話題は、IETFのリストラクチャリングが大きな話題となっており、今回、従来は独自の財源で運営されていたIETFがISOCの下部組織として性格が変わったというアナウンスがあった(従来もISOCより運営資金の寄付が行われていたが、今回の改革ではIETFはISOCの一部門として性格づけられるように思える)。また、RFC Editorの改革が行われ多くのドキュメント類を迅速に処理できるようになったことが報告された。今回のIETFでは、RFC EditorのHelp Deskが用意されていた。RFC/I-Dなどの作成に関しての全般的なサポートを行っており、これが好評であったとの報告もなされた。

端末ルーム

今回のターミナルルールは、今までのIETFとは異なり、PCの設置は行われず電源、ネットワークコネクションおよびプリンタ(HP)の提供のみとなった。また、Hilton Hotelの提供するHi-Speed network ConnectionもIETFのスタッフにより運営された。

ミーティングルーム、ロビーおよびバーでは802.11a/b/gの各規格の無線ネットワークが用意され随所に電源も用意されていた。

無線に関しては、WEPなし、WEPあり、802.11x認証つきの3種類の無線ネットワークが用意され必要に応じて使い分けることが行われていた。これらのネットワークを使う際に、「ネットワークは守られていない。パスワードなどの情報を流す場合は、別の手段で守ること」との注意が換起されていた。

Hilton HotelのHi-Speed network Connectionに関しても同様の注意が求められていた。

写真 12　ターミナルルームの風景