

第 59 回 IETF ミーティング参加報告書

セコム株式会社 IS 研究所

松本 泰、石垣 陽

セコムトラストネット株式会社

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

富士ゼロックス株式会社

益井 隆徳、横田 智文、稲田 龍

2004/2/29-3/5 に韓国 ソウル Lotte Hotel にて開催された第 59 回 IETF(Internet Engineering Task Force: <http://www.ietf.org/>)に参加したので報告する。

IETF は、インターネット上のプロトコルそのほかの標準化を行う団体である。IETF では活動を 8 つのエリアに分け、各々のエリアに Area Director を設け、Area Director の統括の元に WG での標準化活動を行っている。通常の標準化活動はメールベースで行われるが、年に 3 回、実際に顔をあわせる会合が行われる。この会合は、2 回は米国内、1 回は米国外で行われる。今回の韓国での開催は、2002 年の第 54 回に続きアジア内での 2 回目の開催である。

今回の IETF のホストは Korea Telecom と Samsung であり、協賛として TIA、ANF、ETRI、KIPA、KISA - Korean Information Security Agency、KISTI、KRNIC、NCAOSIA など韓国の官民両サイドでのバックアップがなされていた。

また今回、初めての試みであるが IETF に併設して IPv6 Demonstration が行われていた。

今回の参加の目的は以下のとおりである。

1. 日本より提案している Internet-Draft である Multi Domain PKI(セコムトラストネット 島岡氏著)の扱いを調整
2. 証明書の UTF8String に関する議論に参加



図 0 ソウル Lotte Hotel

第 59 回 IETF ミーティングの参加者は 32 カ国から、総勢 1,545 人の参加があった。今回は、韓国での初めての開催のせい、韓国人の参加が目立ち、参加国別の統計は事務局によると第一位 韓国人 45%、第二位 米国人 22%、第三位 日本人 10%とのことであった。

前回の Minneapolis での第 58 回が 1,233 人で、Vienna で行われた第 57 回が 1,304 人、San Francisco の第 56 回が 1,679 人であり、アトランタの第 55 回 IETF ミーティングの参加者は 34 カ国から 334 の組織で、総勢 1,706 人であった。横浜の第 54 回 IETF が 2,064 人、第 53 回のミネアポリスの IETF が 1,756 人であった。同時テロ以前のロンドンで行われた第 51 回 IETF が 2,457 人であったことを考えると、年に一度の米国外でのミーティングである事もあって、出席者は少ない。米国での IT バブルの崩壊の影響は、少しずつではあるが回復しつつあるように感じた。

概観

セキュリティ関連の活動

ここ数年、セキュリティの確保はインターネットにとり大きな課題となっており各社は種々の対策/提案を行なってきた。IETF は、標準化を行なう立場で活動を行っており、多くのプロトコルに関してセキュリティ面での強化を行なっている。

具体的に言えば、ここ数年にわたり初日には Security Tutorial が開催され、インターネット・プロトコルに対して必要とされるセキュリティ要件に関する講義がなされ (後述)、Internet-Draft/RFC に関しては“Security Consideration”の項目が必須となるなどインターネットの標準化に関してセキュリティは必須の要件となっている。

今回の IETF でも、新たに MOBIKE/OPSEC などの新しい WG/BOF が開催されインターネットを自由にかつ安全に利用するための提案がなされている。

また、Security Area の Director である Russell Housley <housley@vigilsec.com>/Steven Bellovin <smb@research.att.com>の両氏は、積極的に多くの WG に参加しコメントを出しセキュリティの重要性を説いている。両氏は、非公式に多くの人間に会い、種々の分野に関してセキュリティを推し進めている。報告者の月曜日の夜に、PKIX-WG の Chair である Steve Kent 氏、Jim Schaad 氏と共に Russell Housley 氏、Steven Bellovin 氏と食事をし、PKI のモデルを今後、どう IETF で扱うかに関して打ち合わせをした。

Steve Kent 氏、 Jim Schaad 氏、 Russell Housley 氏、 Steven Bellovin 氏との打ち合わせに関して

現在、IPA/JNSA と協業している GPKI/PKI 関連の活動において現行の IETF における PKI の利用に関しての標準文書である RFC 3280 では不足がある事が判明している。特に、PKI のドメインが複数あり互いに相互認証する場合のモデルに関してきちんとした文書の整備が必要である事がわかっている。

この面を、セコムトラストネット 島岡氏と協業で Internet-Drafts を作成しているが、この扱いに関して上記のメンバおよび IPA 宮川氏、JNSA 安田氏、セコム株式会社 IS 研究所 松本氏と打ち合わせをおこなった。

当初、59th IETF 開催前に PKIX-WG Chair である NIST Tim Polk 氏(今回は脊椎捻挫のため欠席)および BBN Steve Kent 氏に Internet における PKI のモデルの話であるので PKIX-WG の Work Item として活動を行なえないかと打診をした。両氏からは、PKIX-WG のミッションは標準化を行なうことであること、IESG より PKIX-WG は、新たな Work Item の追加を許されていない事を理由に PKIX-WG での活動にすることはできないと回答があり、Security Area の AD である Russell Housley /Steven Bellovin の両氏に相談すべきと助言された。

Russell Housley /Steven Bellovin の両氏は、PKI のモデルに関する記述の不足を認め、Security Area の新たな WG として活動を行なう事を提案してきた。

WG の作成は、正道であり IETF において標準化を行う際には必要となることではあるが、IETF の作法では、まず、BOF を最大 3 回おこない必要性が認められたら WG とするとなっている。最大 3 回の BOF において必要性が認められない場合、そのアイテムは IETF で扱うべきものではないと認定される。

IPA/JNSA で、IETF の新しい WG を目指して活動するか議論を行なったが、現時点では WG を作ることはできれば目指さないという結論を持って今回の打ち合わせを行なった。



図 0 Stephen Kent 氏(左)、Steven Bellovin(中央)、Russell Housley 氏(右)



図 0 Jim Schaad 氏(左)、島岡氏(中央)、宮川氏(右)

今回の打ち合わせにおいて、こちらの状況を説明し何らかの方法で個人的な I-D を RFC にすることはできないかを相談した。

Russell Housley /Steven Bellovin の両氏は、個人として RFC を発行することは可能であるが、IESG が認める事が必要でありそのためには、きちんとした識者によるレビューが必須であるという事が示された(今回の IETF で、行なわれた OPSEC も同様の立場にあるとのこと)。また、レビューアとして適当な人間を数名上げた。

IPA/JNSA としては、この提案を受け、WG を作らず識者によるレビューを受け IESG に BCP として RFC 化を行なうことにした。

今後の予定としては、

1. I-D の改訂
2. PKIX-WG その他関係ある ML に対してアナウンス
3. 議論用の ML の立ち上げとアーカイブの開始
4. 平行して識者へのレビュー依頼
5. 60th IETF において BOF の開催

を行い 2004 年末に RFC 化を目指すこととなった。

IETF のあり方について

IETF は、ここ数年、標準化団体としてのあり方を模索している。インターネットが爆発的に拡大し、今までの IETF の標準化のスタイルでは適応しきれない事例が生じている。すでに

1. 各 WG での議論が専門化し、大半のメンバが追従できていない。
2. Internet-Drafts の WG でのレビュー率が低下
3. 他の標準化機関との連携が必要となっている

これらの要件を明らかにし、IETF 自身が変わろうとしている。

IETF 自身の機構の改革、Nomicomm による IESG/IAB のメンバの推薦方式の変更。Internet-Drafts/RFC の発行のスピード化、事務局のスリム化、スポンサーなしでの IETF の開催など、ここ 2,3 年多くの変革を IETF は行っている。

まだ、改革は始まったばかりではあるが今後どの様に IETF が変わり、インターネットでの標準化がどの様に変化していくかを見極める必要があると感じている。

今回、新たに newtrk(New IETF Standard Track BOF)が開催されるなどインターネットでの標準化のあり方が大きな問題となりつつあると感じた。

PKIX について

今回の PKIX-WG は、Co-Chair である NIST の Tim Polk 氏が脊椎捻挫のため BBN の Stephen Kent 氏により仕切られた。

WG のミーティングは通常の通りにドキュメントステータスより始まり、粛々と議題をこなし議論としては低調な物となった。しかしながら、内容としては Qualified Certificate の RFC 化が進み、Proxy Certificate は RFC 化が決まるなど多くの面で進展が見られた。米国外での IETF であるため、多くの常連となるメンバが出席しない状況でありオフラインでのミーティングは、低調に感じるが WG としてのミッションは確実に消化しつつあるように感じる。

また、IESG からの要請により PKIX-WG は、終息のフェイズにある。今後は、PKI のインターネットでの応用範囲を広げるべく種々の BOF/WG が開かれるものと考えられる。前回の Minneapolis での IETF に引き続き、IPsec での PKI の応用とプロファイルの策定を意図した BOF である pki4ipsec が開かれ、BOF から WG への昇格が決定するようである。



図 0 Stephen Kent 氏

IPv6 Demo について

今回の IETF は、初めての試みとして IPv6 の製品群のデモンストレーションが IETF の一部として行われた。これはホストである韓国 Korea Telecom の思惑と IETF の思惑が一致したために実現したものと考えられる。

会場には、SIP を利用した IP 電話が置かれ国際電話を無料とサービスしていた(通話料は Korea Telecom 持ちのようである)。デモンストレーションを見る限り、特に IPv4/IPv6 の違いを意識せずにアプリケーションを利用できるようである。

SIP 応用の IP 電話は、十分に実用に耐える品質を持っており、3 分ほどではあったが KSP のオフィスへの連絡にも十二分に利用できた。

現時点では SIP のパケットに関しては暗号化・電子署名といった伝送路中での盗聴・改ざん対策はなされていないが、IETF の SIP 関連の WG では、SIP パケットに対して暗号化・電子署名を行うための議論が進められている。



図 0 SIP 利用 IPv6 電話のデモ

今回の IETF でも、SIP-WG で、SIP パケットを PKI ベースの CMS(Cryptographic Message Syntax)で暗号化・電子署名を行うことが提案されており、比較的早期に暗号化・電子署名が導入されると思われる。

韓国は、国策として IPv6 を推進しており、Seoul 市内に大規模な IPv6 デモンストレーション場(KEIS6、IETF 会場より見学ツアーあり)を用意するなど IPv6 の普及を図っている。

日本においても国策として IPv6 の発展・普及は行われているが韓国に比べるといまいちと感じた。

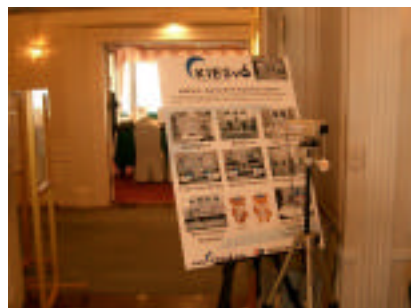


図 0 KEIS6 の案内

SIP 関連

今回の IETF では、IP 電話の普及期にあたるのせいか SIP 関連の WG ミーティングが多く開催された。

具体的には

開催日時	WG 名	参加人員
3/1 09:00-11:30	Session Initiation Proposal Investigation WG	150 名程度
3/1 15:00-17:30	Session Initiation Protocol WG	150 名程度
3/1 19:30-22:00	SIP for Instant Messaging and Presence Leveraging Extensions WG	100 名程度
3/3 13:00-15:00	Session Initiation Proposal Investigation WG	100 名程度

と 4 セッション SIP 関連のミーティングが行なわれた。

いずれのセッションも多くの話題で活発な議論が取り交わされていた。

特に、Session Initiation Proposal Investigation WG (SIPPING)は 2 回おこなわれ多くの課題がある事が伺われる。SIPPING では、特に SIP での暗号化/電子署名として採用が決まった CMS(Cryptographic Message Syntax)において証明書をどう扱うかについての議論がおこなわれた。現行の IP 電話で用いられている SIP においては暗号化/電子署名がなされていないため盗聴/改竄/課金のごまかしの問題が生じた場合の対応が事実上不可能であるため、何らかの対応をおこなう必要があるためである。

また、SIP for Instant Messaging and Presence Leveraging Extensions WG(SIMPLE)においては、Microsoft 社の技術者が Windows Messenger/Windows Media Player への対応を考えているようであった。

会場のネットワーク環境に関して

会場となった Lotte Hotel Seoul は、すでにホテルのネットワーク環境として有線/無線のいわゆるブロードバンド環境を持っており有償で利用できる。各階で若干の違いはあるが、基本はホテルの客室内ではどこでも快適なネットワーク環境が利用できる。

今回の IETF では、恒例の会場付近の 802.11a/b(802.11a は免許の関係で日本から持参した物では使用出来ない)のアクセス、ターミナルルームでの有線環境の提供を行っていた。無線 Access Point が会場内の随所に設置されており、会場内、ホテル内のレストラン、バーなどにも設置されており、食事もしくは WG 後、軽くバーでいっぱいというときでもインターネットに接続できる環境になっていた。メインラウンジ、ワインバーのそこかしこで非公式の打ち合わせ、情報交換などが行われており、その佐相に付随したデータの取得、覚書の交換、次回の予定の調整などに使われているものと思われる。また、Lotte Hotel Seoul には無線 LAN が設置されており、この無線 LAN に関しても会期中は、「無償」で利用できるようになっていた。そのため、客室と会場では SSID の違い、Public IP(IETF 提供)/Private IP(Lotte Hotel Seoul)の違いはあるものも十二分に快適にネットワークの利用が出来た。

いずれの無線ネットワークも RSA Conference の場合とは異なり特に暗号化もされておらず、SSH/IPsec などでパケットの暗号化を行うことが推奨されていた。IETF はセキュリティに関しての意識も高く、また、実際に開発を行っている立場でもあり、なまじインフラストラクチャとしてセキュリティ環境を提供するよりも、基本的な環境を提供し、後は利用者自身が利用者の環境に応じたセキュリティを自己責任で行うことが望ましいというスタンスであると思われる。RSA Conference が 802.1X 認証を全面的に導入したセキュリティ技術のショーケース的な使い方・提供の仕方と対照的である。

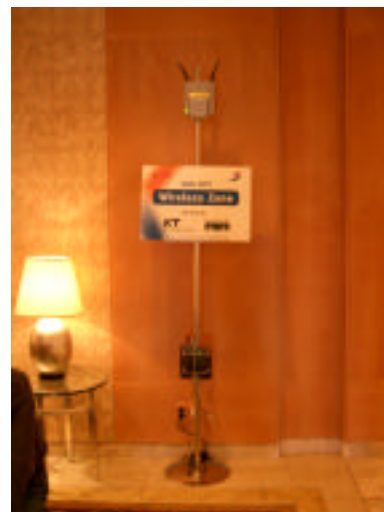


図 0 無線 AP



図 0 ターミナルルーム

また、今までの IETF 同様にターミナルルームも用意されていたが規模は小さかった。



図 0 HP のプリンタ

各 WG セッション

New Comer's Training

2/29 の 13:00-14:00 に開催された。今回は、初めての試みとして通常の英語でのセッションのほか、韓国語でのセッションも開催された。

英語でのセッションは、約 120 名が参加し IETF の概要と標準化の流れが説明された。

IETF の標準化の考えの基本は“Rough consensus and running code”であることが説明された。一言で言えば、「細かなことは気にせず、動くものを (追認して)標準化する」ということであり、ITU-T/ISO などとは異なる標準化ポリシーの元に「標準化」が進められていることが説明されている。IETF のこのスタンスが、インターネットの急速な発展と 1 dog year といわれる急速な変化に何とか追従をしていることを表している。

Editor's Training

2/29 の 13:00-15:00 に開催された。参加者は 40 名ほどであった。

Editor's Training は、Internet-Drafts/RFC を書く人に対するセッションであり、RFC Editor がどのような観点で「編集」を行い IETF での標準化文書が作られる過程の説明を行う。Editor としての心得、どのタイミングで RFC Editor に送るべきかなどが話された。

Internet-Drafts/RFC を作成する面で役に立つツール類の紹介もあった。Internet-Drafts/RFC は、基本は nroff で作成されるが、XML にも対応されており、それらの Tips などの説明があった。

セッションは、多くの質問が寄せられ当然ではあるが、Internet-Drafts/RFC を書くことがセッション参加者主な興味対象であることが感じられた。

紹介されたツール類は、以下のようなものである

1. Text Formatting Tools / <http://www.rfc-editor.org/formatting.html>
2. xml2rfc / <http://www.ietf.org/rfc/rfc2629.txt>
3. nroff(groff)
4. Microsoft word template / <ftp://ftp.ietf.org/internet-draft/2-Word-template.rtf>
5. LaTeX
6. MIB reference and compilers

Security Tutorial

2/29 の 15:00-17:00 に開催された。参加者は 300 名程度。満席であった。

SUN の Redia Perlman 女史が説明した。Redia 女史は、ARP の開発者としても知られている人物で IETF の長老(女性に対して長老とは失礼かもしれないが)の一人である。

インターネットでなせ、Security が重要であるかについての解説より技術的なコンセプト、守るための個別の技術などを平易に、説明しており暗号技術に関しても多くの説明を行っていた。



図 0 Redia Perlman 女

史(中央)と稲田 Mgr(左)
暗号に関しては、「勝手に暗号を作るべきではなく、きちんと レビューを受けたものを使うのが望ましい」というコメントを残していた。セキュリティプロトコルは大変難しいので、全部自分でやるのではなく、複数の人間が共同して行うことが重要とも言っていた。

セッション終了後、Redia 女史に「大変有効なセッションなのでスライドをもらえないか」と聞いたところ、「すでに IETF のページのどこかにはあるはずであるが、場所は知らない」とのことで、探し見たが見つからず、再度、スライドをもらえないか交渉したところ「来週一週間は香港にいるので対応できないが、その後なら対応可能なのでそのころに Reminder してくれ」とのことであった。

WG Chair Training

2/29 の 13:00-15:00 に開催。Mararet Wasserman が説明した。

WG Chair になった人またはこれからなろうとしている人向けに、WG Chair の役割と責任の範囲を説明された。また、WG を公正かつオープンかつ生産的に運用するためのノウハウが紹

介された。このセッションは IETF 参加者全員が聞くことが出来、特に WG の Chair として指名されていない場合でも聞くことは可能である。

参加者は、10 数名程度と少数であった。

WG 運営に必要な作業や情報の紹介は、WG を運営しようとする人々だけでなく、WG に参加して具体的な活動をしていく(例えば I-D を執筆したりする人々)にとっても非常に有益なセッションだった。

オープン性と公正性を保つための工夫として、オフラインミーティングに参加できない人々に配慮して必ず ML での確認を求めたり、言語や文化の異なる人々のために、オフラインミーティングでも口頭でのコミュニケーションに頼らず文書を記録として残せるよう注意を促すなど、IETF の本質的な運営ノウハウが非常に興味深かった。

WG Chair となるべき人々に対して、IETF の基本思想である "Rough Consensus, Running code" を改めて説明するあたり、基本思想の維持徹底を心がける努力を欠かしていないことも窺えた。

IKEv2 Mobility and Multihoming WG(mobike)

Paul Hoffman <paul.hoffman@vpnc.org>

Jari Arkko <Jari.Arkko@ericsson.com>

3/1 09:00-11:30 に開催された。参加人数は 200 人程度。関心が高かった。

IPsec で利用される IKEv2 のコアプロトコルとは独立に、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 である。



図 0 Paul Hoffman 氏 (右)と Jari Arkko 氏(左)

セッションでは、以下の 2 つのドラフト説明が行われた。

1. Address Management for IKE version 2

モバイル環境で、重要となるアドレス管理を IKE に追加する提案であり I-D となった。

IKEv2 でのアドレス管理は、NAT traversal で提案されているが、モバイルで問題となる、IPv6 での NAT 対応やマルチホーミング対応を保管するための別提案としている。

2. Design of the MOBIKE protocol

MOBIKE の設計に関する説明で、前回の 58 回 IETF での BOF での意見を受けた修正案の説明である。前回、IKEv2 のオプションを使用できることを指摘されたため、IKEv2 を最大限に利用するように変更した。

pki4ipsec (Profiling Use of PKI in IPSEC WG)

Paul Knight <paul.knight@nortelnetworks.com>

Gregory Lebovitz <gregory@netscreen.com>

3/1 13:00-15:00 に開催された。参加者 200 名ほど。

IPsec は、過去 5 年間以上にわたって標準化が行われてきた。同じ期間、X.509 証明書の利用についても定められてきた。しかし、証明書を利用する IPsec の採用事例はほとんどない。その理由のひとつは、X.509 証明書の IPsec における利用についての明快な文書の欠如である。また、IPsec システムについて、証明書の入手等、証明書に関するライフサイクル運用について単純明確に規定された方法論の欠如も理由である。

WG としてのチャーターが <http://www.ietf.org/html.charters/pki4ipsec-charter.html> のように決まったことの報告と現行の draft-ietf-ipsec-pki-profile-04.txt に関する議論が行なわれた。

Public-Key Infrastructure WG

Stephen Kent <kent@bbn.com>

Tim Polk <wpolk@nist.gov>

3/1 15:30 - 17:30 に行なわれた。参加者数は 49 人。

Chair の一人である Tim Polk 氏が脊椎捻挫のため出席せず、BBN の Stephen Kent 氏がミーティングを仕切っていた。

WG のミーティングは通常の通りにドキュメントステータスより始まり、粛々と議題をこなす議論としては低調な物となった。しかしながら、内容としては Qualified Certificate の RFC 化が進み、Proxy Certificate は RFC 化が決まるなど多くの面で進展が見られた。米国外での IETF であるため、多くの常連となるメンバが出席しない状況でありオフラインでのミーティングは、低調に感じるが WG としてのミッションは確実に消化しつつあるように感じる。

また、IESG からの要請により PKIX-WG は、終息のフェイズにある。今後は、PKI のインターネットでの応用範囲を広げるべく種々の BOF/WG が開かれるものと考えられる。前回の Minneapolis での IETF に引き続き、IPsec での PKI の応用とプロファイルの策定を意図した BOF である pki4ipsec が開かれ、BOF から WG への昇格が決定するようである。

1. Document Status

RFC 3709 Internet X.509 Public Key Infrastructure: Logotypes in X.509 certificates が RFC 化された

Proxy Certificate は、RFC Editor の処理待ちである

Qualified Certificates は IESG の承認待ち

Warranty extension は修正が必要である

Permanent Identifier, Attribute Certificate Policies, Wireless LAN Extensions, Repository Locator Service, CRMF, CMP は AD の処理待ち

SCVP, PK Algorithms は WG Last Call 中である

Path Building, ECC (NIST Curves)は WG での Last Call 待ちである

2. CRMF (RFC2511bis)

Jim Schaad 氏が Editor を引き継ぎ、多くの変更を行なっている。

POP(Proof of Possession)の方式の一つに脆弱性がある事がわかり、この部分の修正もしくは削除が必要。DH-MAC POP に関してアルゴリズムをきちんと決める必要あり(ECC が有力視されている模様)。

3. RFC 3039bis (Qualified Certificates)

Russ Housley 氏より Denis Pinkas 氏から 38 ものコメントが寄せられた事が報告された。そのうち 33 に関しては解決できたが、まだ 5 つのコメントが解決できていないとの事である。

4. Subject Identification Method

韓国の KISA Jongwook Park 氏と米国 NIST Tim Polk 氏の連名での報告があった。韓国では既に国民に対して証明書を発行しており、米国も計画がある。その際に、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になっている(日本の公的個人認証サービスも同様の問題を抱えているが、日本の場合は、公的個人認証サービスの証明書を利用するのは官側のみと規定し問題がないとしている。実際には、そうは民間でも広く使われそうであるが...)

韓国/米国はこの問題を重要なものとして捉え、特定の方式で暗号化した情報を記載することにより、適切な権限を持った利用者だけに情報が開示される方式を提案している。個人的には現在、日本で展開されている公的個人認証サービスについても同様な問題を抱えており、広く官民で利用できるようにするためには証明書に記載されるプライバシー情報などを適切に扱える仕組みが必要と感じており、このアプローチは注目している。現在の I-D のステータスの報告と、更なる修正が必要との報告が行なわれた。

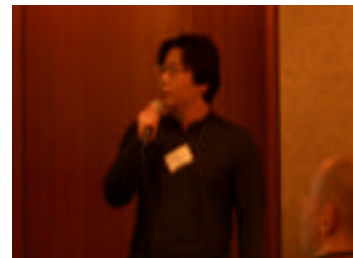


図 1 Jongwook Park 氏

Operational Security Requirements BOF

3/2 09:00 - 11:30 に開催された。参加人数は 150 名ほど。

エンタープライズ/ISP において運用に関して必要となるであろうセキュリティに関しての BCP(Best Current Practice) RFC をまとめる事を目的とした BOF である。

Security Area Director である Steven Bellovin 氏が場を仕切っており、Security Area としてのこの手の文書が必要であるとの認識を持っているように感じた。

作成した I-D を Informational RFC にするか BCP RFC にするか の議論が行なわれ BCP RFC にする事が合意された。



図 1 Steven Bellovin 氏(左)

Simple Authentication and Security Layer WG

Sam Hartman <hartmans@mit.edu>

Kurt Zeilenga <kurt@openLDAP.org>

3/2 17:00 - 18:00 に開催された。参加人数は 40 名程度。

質疑等もほとんど無く実際に実装を行なっている 4、5 人で話をしているような状態であった。

SASL の識別情報の文字コード(UTF-8)について、UTF-8 を実際に使った検証が不足しているとの指摘があった。仕様について、3 月中に修正を行うように依頼が有り、エディタが困惑している場面も見受けられた。

AVT

3/3 09:00-11:30 に開催された。参加人数 400 名程度。活気のあるセッションであった。

ユニキャスト/マルチキャストの UDP を使ったオーディオ/ビデオのリアルタイム転送を検討する WG。今回、タイトルに引かれて参加したが、分野違いということもあり、ほとんど理解できないセッションであった。

Erickson、SONY、Panasonic など携帯電話メーカーが中心に発表をしており、インド系の技術者が多いもの注目される。

リアルタイム通信を行う汎用プロトコル「RTP」をベースとして、既存の映像・音声フォーマットを RTP のペイロードに乗せる場合のフォーマットの提案が多数目立った。

提案対象のフォーマットは以下の通り。

AMR-WB+

ATRAC3 (Advanced Transform Acoustic Coding) ATRAC-X

3GPP(3rd Generation Partnership Project) timed text

OpenPGP

Derek Atkins <derek@ihtfp.com>

3/2 11:30-13:00 に開催された。参加人数 数十名程度。小康状態にある WG と見られる。

セッションでは、以下の報告が短時間になされた。

1. ホワイトスペース終端の取り扱いについて (署名のためのホワイトスペースの正規化の話であるが、正規化の仕様を追加すると下位互換性がなくなり、問題であると指摘がなされた。)
2. メッセージボディ内の非 UTF-8 文字列について
3. ElGamal 暗号の削除について
4. v3 での IDEA のアルゴリズム衝突について
5. RFC2440bis を IESG に提出
6. マルチ署名のドラフトを IESG に提出
7. RFC2440bis と PGP/MIME の相互接続テストを開始する

AAA

3/2 14:15-15:15

セッションで以下の報告がなされた。

Diameter Mobile IP Application

双方向のそれぞれで別の SymetricKey を使った暗号にするとの提案がなされているが、そもそも別々の鍵を使わなければならない根拠を提示するよう依頼があった。

Diameter SIP application

S/MIME

Sean Turner <turners@ieca.com>

Blake Ramsdell <blake@sendmail.com>

暗号メールの規格の 1 つである S/MIME を検討する WG である。以下の Update と Status について報告があった。

1. MSGbis (S/MIMEv3.1 Message Spec) 3/8 まで Last Call。編集上のコメントが Russ Houseley 他から寄せられている。
2. CERTbis(S/MIMEv3.1 Certificate Handling) 3/8 まで Last Call。編集上のコメントが David P. Kemp 他から寄せられている。
3. GOST 3/8 まで Last Call。GOST はロシア標準の暗号方式であり、GOST を S/MIME に取り込む仕様である。
4. SEED KISA の Jongwook Park から説明報告があった。SEED は韓国標準の暗号方式。次の 2 つの I-D が Update された。
SEED Encryption Algorithm (draft-park-seed-01.txt)
Use of the SEED Encryption Algorithm in CMS (draft-park-cms-seed-01.txt)
SEED のテストベクタを記述するようとの依頼がなされた。

Security Issues in Network Event Logging WG

Chris Lonvick <clonvick@cisco.com>

3/3 15 : 30-17 : 30 に開催された。参加人数は 60 名程度。

システムイベントのロギングを検討/標準化する WG である。Syslog に関する以下のステータス報告があった。

1. Syslog Sign
2. Syslog Device MIB

Syslog 操作のモニタおよび Syslog 処理のコンフィギュレーション/制御を目的とする。

最新 I-D は、draft-ietf-syslog-device-mib-05.txt。

懸案事項であった、SNMP Notification 対応や NO-DNS lookup 対応についてのサポートについて対応済みとなった。

Kerberos WG

Douglas Engert <deengert@anl.gov>

Jeffrey Hutzelman <jhutz@cmu.edu>

3/4 09:00-11:30 に開催された。参加人数は 100 名程度。

ネットワーク認証方式である Kerberos の検討を行う WG である。セッションでは、以下の項目が報告された。

1. Tom You の Kerberos 拡張に対する代替案の提示(By Sam Hartman)
Clarification が冗長のため変更/実装仕様詳細を削除/名前付け事項の追加/トランスポート事項の追加/クリアアップのタイミング追加/その他レイアウト変更が報告された。
2. PKINIT のステータス
I-D (draft-ietf-cat-kerberos-pk-init-18.txt) が発行された。現在、Open Issue として、以下が未解決であり、今後議論してゆく。
 - ・ユーザ証明書の SubjectName をどうするか
 - ・ClientName の正規化方法
 - ・OCSP 対応
 - ・事前認証子タイプ

LTANS

Carl Wallace <cwallace@orionsec.com>

Tobias Gondrom <tobias.gondrom@ixos.de>

3/4 13 : 00-15 : 00 に開催された。参加人数は 40 名程度。

LTANS-WG(Long-term archiving and notary services)は、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 であり、前回の Minneapolis での第 58 回 IETF に作られた WG である。

現状 2 つの I-D が提案されているが、まだ Standard Track の RFC はない。

Requirements review (Chokhani/Open Discussion)

タイムスタンプを様々な情報基盤として利用した場合、考慮すべき点がいくつか示された。

RFC3161 利用における議論 (特にタイムスタンプの更新処理について) :

- ・ 時間が経つにつれ，非常に多くのデジタル署名が存在することになる
- ・ ハッシュリンクと比べた場合，更新回数（refresh frequency）が多くなる
ハッシュリンクによるタイムスタンプは IETF の context だろうか？

データフォーマットに関する議論：

- ・ データフォーマットの migration/emulation が問題となる
- ・ プロトコル構造を定義することが優先事項
- ・ 最初のゴールは，エビデンスの構造とプロトコルを体系化すること

Authorization:

- ・ アーカイブを閲覧あるいは編集するための権限管理が重要な課題
- ・ authentication/authorization の情報を長期に渡ってどのように管理するのか
- ・ 秘密鍵は長期に渡って管理可能か（長期に渡って署名検証が可能かといっている？）

ERS(Evidence Record Syntax) review (Hunter)

関連ドラフト：

<http://www.ietf.org/internet-drafts/draft-ietf-its-ers-00.txt>

(アブストラクトの訳)

- ・ 一般に，ユーザは文書の完全性と存在証明を確認する手段を必要とする．
- ・ 特にデジタル署名されたデータについて，これらの要求が高い．
- ・ このとき，出来る限り半永久的に，汎用的な方法で確認できることが望ましい．
- ・ 本文書は証拠レコード（ER, Evidence Record）の文法と処理方法を示す．
- ・ ER は，存在が証明されたデータについて，長期に渡る否認防止を提供するために設計された．
- ・ 特にデジタル署名されたデータの交換時には，ER が有用であると考えられる．

電子ドキュメントの長期保存について，Chokhani さんより以下の内容で詳細な議論を行なった。

- ・ アルゴリズム危殆化
- ・ 証明書の期限切れ
- ・ 検証に必要なデータが有効でなくなる
- ・ フォーマットやメディアの問題

これらを検討するために、ArchiSig project 2001-2003 というのが行われた。
http://www.sit.fraunhofer.de/english/MINT/mint_projects/project_details/archisig.html

このプロジェクトは、デジタル署名された文書のアーカイピングのためのコンセプトを開発しているようである。

(以下 HP の簡単な訳)

- ・ 技術的・組織的・法的な面から検討を行う
- ・ SigG, BDSG などの各種法律に準拠する
- ・ 安価で実現可能なコンセプトを目指す
- ・ 病院や政府機関におけるプロトタイプを完成させる。
ハイデルベルグ大学で実際に clinical trial をしていると言っていた
- ・ 専門家などによる評価と試験を行う
- ・ ERS に与える影響も調査

データ構造の要求：

1. 証拠と存在証明を行うことができ、エンティティ同士で交換可能な汎用的データ構造
2. データ型やアーキテクチャに依存せず、どのアーカイブプロバイダでも使える証拠記録の外部仕様
3. 暗号化されたデータへの対応

LTANS の要求：

1. 存在証明を行う可能性がある全てのタイムスタンプを含むこと
2. どんなに沢山のデータが蓄積されようとも、データ構造は効率的に証拠機能を提供できること

ERS(前述)の概観：

- ・ アーカイブタイムスタンプの文法と、(特に検証に関する)処理方法を定義している
- ・ TAA(Trusted Archive Authority)による中央集約的なアーカイブを想定している(この他に外部とのデータ交換で用いられるサービスプロトコルと、アーカイブシステムのアーキテクチャも規定)

アーカイブタイムスタンプ：「ハッシュ木 (Merkle)」, 「電子署名を含むタイムスタンプ」, 「様々な文書に対するシングルタイムスタンプ」の3要素で構成される。

イニシャルスタンプ：「イベント」, 「ハッシュ値の木」, 「ストアアーカイブスタンプ」で構成され、必要であれば随時更新を行う

<タイムスタンプの更新>

- ・ 古いアルゴリズムを使ったタイムスタンプに，新しいアルゴリズムを用いたスタンプを付与する
- ・ 新しいアーカイブスタンプを付与する

性質：

- ・ データ構造にはアクセスしなくてよい
- ・ 全てのアーカイブに対して，1つのスタンプを押すだけですむ

<ハッシュ木の更新>

ハッシュ木のチェーン自体が危殆化した場合：

- ・ アーカイブタイムスタンプのチェーンを構築する
- ・ ハッシュのチェーンとハッシュのデータ構造に対して新しいアーカイブスタンプを付与する

性質：

- ・ データ構造に対してアクセスする必要がある
- ・ avoidable via redundant hash trees

ここで、「リポジトリは信用できないのに、どうやって元本性を保證するのか？」という質問が寄せられた。

Hunter 氏は、「アーカイブプロバイダが保證するため，バックエンドのアーキテクチャで解決できる」と答えていた。また、「アルゴリズム危殆化などの議論は，セキュリティ考察に書くべきでは？」というコメントが提案された。

まとめ：

- ・ ER は，アーカイブスタンプ要素の文法と処理方法
- ・ 効率的で中央集約的なタイムスタンプの利用法
- ・ 多くの文書の保管に有効
- ・ 様々なデータオブジェクトに対応

ERS discussion (Open Discussion)

Chokhani 氏によって，ERS に関する論点を示された．論点は主に2つの点に集約できる．

- ・ E-archive の基盤とオペレーション
- ・ E-archive のデータ構想

基盤モデルについては，6つのレイヤに分けることができる：

1. EE controlled interface into a work flow applications
2. EE parametrisable security and protocol layer
3. company internal relay/broker
4. company outgoing backend
5. backend service notarisation from t a service
6. backend storage services

(これはドラフトに書かれているわけではなく、Chokhani 氏の解釈である)

Inter-layer プロトコルとして、以下のものが考えられる：

- ・ レイヤ 1/2 またはレイヤ 3/4 におけるシンプルなセキュア通信プロトコル（応答に署名は必要無く，最小限の信頼に基づく）
- ・ レイヤ 4/5 における，バックエンドで第三者による保証に基づいたもの。(DVCS がよい例)

この他に、arch/Notary サービス」「Sec.Mes. timestamp」「Control & Audit」の三要素について、BS17799 などのモデルを ERS に当てはめて考察が行なわれていた。

アーカイブサービスのセキュリティ考察：

- ・ セキュリティはレイヤ 4/5 のオペレーションで提供される
- ・ integrity ensuring mechanism にもとづいたセキュリティ評価が行われる

何のセキュリティについて考察しているのか不明瞭だというコメントが寄せられました。

抽象プロトコルへの要求：

- ・ アーカイブや公証サービスによって実装される
- ・ 3つの要求 submission/management/responses が存在する
- ・ メッセージタイプ：どのメッセージも，送り手と受け手を表現できる
- ・ リプレイ攻撃に対応しなくてはならない

Geographic Location/Privacy WG

Allison Mankin <mankin@psg.com>

Randall Gellens <rg+ietf@qualcomm.com>

Andrew Newton <andy@hxr.us>

3/4 15:30-17:30 に開催された。参加人数は 60 名程度。

リソース/エンティティの位置情報を必要とする Navigation、緊急通報などのサービスを提供するために必要なプロトコル/データ構造を決定する WG である。セッションでは、以下の報告があった。

1. Documents Status

RFC 3693 – GEOPRIV Requirements/RFC 3694 GEOPRIV Threats Analysis の 2 つの文書が RFC となったことが報告された。

2. DHCP Civil Location Option Civil Location をデバイスに伝達するためのプロトコルを規定する。人が存在する部屋の識別や文字セットについてまだ Open Issue となっている。

会場では、エディタである Schulzrinne が Last Call をかけたいとの要求を提案したが、広範囲に影響するため、レビュー時間をとるようにとの指摘があった。

3. GLI System Architecture

慶応大学の Yasuhito Watanabe 氏が、彼らが作ったプロトタイプの GSI (Geographical Location Information System) に関する報告を行った。RFC3693 の GEOPRIV 要求のコンフォーマンスをもつとの事であった。この活動は、WIDE プロジェクトの村井純氏の指導で行なわれ、いわゆる ICAR コンソーシアムの協力で行なわれているものである。

以上