連載

IETF

第6回
セキュリティエリア

櫻井三子　日本電気（株）
mine@ax.jp.nec.com

石井秀治　（株）インターネットイニシアティブ
shuji@iij.ad.jp

竹谷清康　（財）日本品質保証機構
takeya-kiyoyasu@jqa.jp

坂根昌一　横河電機（株）
Shouichi.Sakane@jp.yokogawa.com

Glenn Mansfield KEENI
（株）サイバー・ソリューションズ　glenn@cysol.co.jp

セキュリティエリアの目標

RFCにはSecurity Considerationsという項目が設けられている[1]．中身はフリーフォーマットであり，過去には「本RFCはセキュリティについて一切考慮していない」と書いてあることもあったが，最近はIESGによるチェックが厳しくなってきている．重要なことは，RFCにかかわる人はすべてセキュリティとの関係について考える機会を与えられるということである．

しかしながら，各人がセキュリティについてばらばらに検討し，独自の技術のみで対応していては大変であり，相互接続性が重要なインターネットでは広く使える汎用なセキュリティ技術が求められる．IETFのセキュリティエリアでは，明記されているわけではないが，他のエリアから使われる技術の標準化を目標にしている．

本稿では，セキュリティエリア全体の動向と，いくつかのWGに関する個別の取り組みについて紹介する．

全体トピック

■技術的な傾向

セキュリティ技術を不正アクセスの予防，検出，対処（対策，解析）という3つの観点で捉えると，セキュリティエリアの対象は，予防技術，および検出をしやすくする技術である．具体的には，以下の技術がある．

- 通信データを秘匿する技術
- なりすましを防止する認証技術
- 通信データの改ざんを検出しやすくする技術
- 通信データの再送攻撃を防止する技術
- 通信記録を収集する技術

これらの技術は暗号技術との関係が密接であるが，IETFではあくまで暗号技術を応用する立場に徹している．新しい暗号技術が出てくれば，それを応用した新規のプロトコル開発や既存のプロトコルへの盛り込みを検討するが，暗号技術自体の開発を検討することはない．

セキュリティエリアには，2002年4月現在で19のWGがある（**表-1**）．

これらのWG間の連携関係を整理してみると**図-1**のようになる．

IETFミーティングでは，Security Area Advisory Group（SAAG）というセッションが毎回あり，WGの動向や新しい暗号技術に関する動向に関して確認しあう機会となっている．

セキュリティエリアからのRFC発行数は1998年から増えており，1998年は19件でIPsec中心，1999年は20件で公開鍵基盤中心，2000年は14件で分散傾向であった．2001年は14件で公開鍵基盤中心であったが，standard track RFCは5件にとどまり，沈静化傾向にある．

その他の技術的な特徴として，通信プロトコルをあまり意識せずに，その上でやりとりするデータフォーマットを重点的に検討する場合があることが挙げられる．そのような場

WG略称	正式名称
aft	Authenticated Firewall Traversal
cat	Common Authentication Technology
idwg	Intrusion Detection Exchange Format
ipsec	IP Security Protocol
ipsp	IP Security Policy
ipsra	IP Security Remote Access
kink	Kerberized Internet Negotiation of Keys
krb-wg	Kerberos
msec	Multicast Security
openpgp	An Open Specification for Pretty Good Privacy
otp	One Time Password Authentication
pkix	Public-key Infrastructure (X.509)
sacred	Securely Available Credentials
secsh	Secure Shell
smime	S/MIME Mail Security
stime	Secure Network Time Protocol
syslog	Security Issues in Network Event Logging
tls	Transport Layer Security
xmldsig	XML Digital Signatures

表-1　セキュリティエリアWG一覧

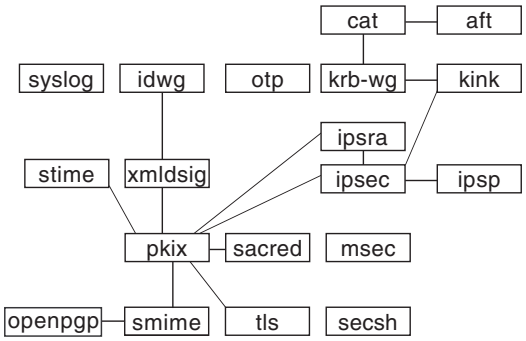

図-1　セキュリティエリアWG連携関係

合，フォーマットのベースとなるデータ表現形式の決定が重要になる．最近の例では，ASN.1（Abstract Syntax Notation One）vs XML（eXtended Markup Language）の議論を見たことがある．

■プロトコル実装暗号アルゴリズムについて

これまで，暗号といえば，輸出規制・キーリカバリーなどのあまり明るくないキーワードを連想することが多く，積極的に関与するムードではなかった．しかし，下記の状況変化により，最近，特にsmime，tls，ipsec，pkix WGでは，実装暗号アルゴリズムについて盛んに議論されることが多くなってきた．

（1）RSAの特許権が2000年9月に切れ，パブリックドメイン化されたこと．

（2）DESに代わる米国暗号標準AESを，NISTが2001年11月にFIPS-197[2]として発行したこと．

（3）次世代のセキュアハッシュアルゴリズムや次世代電子署名技術の米国標準をNISTで検討中であること．

これらの暗号技術の変革を受け，プロトコルと実装暗号アルゴリズムを

署名検証	RSA and DSA
署名生成	RSA or DSA
ハッシュ関数	SHA-1
鍵管理	RSA
データ暗号	Triple-DES

表-2　S/MIMEに実装する必須暗号アルゴリズム
（第53回IETF smime WG発表資料より）

別々のInternet-Draftsに分けることが主流となった．また，これまで多くのRFCの必須暗号であったDES，MD5などは使われなくなってきている．例として，smime WGで合意された実装必須暗号アルゴリズムを表2に示す．

このようなIETFにおける実装暗号アルゴリズムの議論に関連した日本の動きとしては，電子政府で利用する暗号技術を評価するプロジェクトCRYPTREC[3] がある．

CRYPTRECの2001年度の報告書では，我が国の電子署名法に係る指針から電子署名に用いるハッシュ関数としてMD5を外すこと，さらに，電子政府での利用を推奨する暗号技術の要件の1つとしてすでに何らかのプロトコル標準となっている暗号技術を考慮すべきだと記載している．このプロトコル標準には，IETFのRFCも含まれると思われる．

このように，IETFの標準化活動は，日本のe-JAPAN計画にも少なからず影響を与えている．

■他のエリア動向

ここ数年，セキュリティエリア以外のWGやBOF においてセキュリティそのものについて議論する機会が多くなっている．たとえば，

＊aaa （Authentication, Authorization and Accounting）
→オペレーション&マネージメントエリア

＊itrace （ICMP Traceback）
→インターネットエリア

といったWG の活動内容はセキュリティエリアに近いといえよう．すこし異色ではあるが，

＊ieprep （Internet Emergency Preparedness）
→トランスポートエリア

も広い意味でのセキュリティといえるだろう．

さらに今回のIETFでは，下で述べるようにルーティングエリアでもルーティングプロトコルセキュリティのBOFが開催された．

これ以外にも，セキュリティエリアのWGの成果を取り込むWGがいくつかある．たとえばipsは，通信部分のセキュリティ機能としてIPsecの採用を検討している．

このように他エリアのWGやBOFにおいて，セキュリティについて積極的に検討しはじめている．この背景には，2つあると考えられる．

1つはインターネットの拡大（商用化）にともなって侵入事件やDoS 攻撃が目につくようになり，セキュリティに対する認識が高まったことである．もう1つはX.509 証明書，IPsec，TLSといった要素となる技術／標準が整ってきたことである．

個別トピック

■ipsec WG

ipsec WGは，データの偽造や盗聴，なりすまし等を防ぐためのセキュリティ機能を，ネットワーク層に提供する仕様を標準化するべく，1992年に発足した．

ipsec WGへの期待は非常に大きい．ネットワーク層にセキュリティ機能が提供されると，上位の通信プロトコルは，それを利用するだけでプロトコルが要求しているセキュリティ機能の大部分を実現できる．ホスト同士の通信の安全性はIPsecに委ねられたと言っても過言ではないほど，多くの通信プロトコルの仕様がIPsecを参照している．また，市場の関心がVPNへ向けられるにつれて，WGへの期待も高まってきたようだ．

IPsecの標準化の過程では，多くのVPNベンダの開発者たちが関与しているため，VPNを仮定した議論が中心にされる時もある．それゆえ，IPsecの仕様はさまざまな通信環境に適応できるように，非常に汎用的に設計された．

IPsecの仕様を大別すると3つに分けられる．1つ目は，基幹となるプロトコルの仕様で1995年に初版が発行された．やがて，インターネットの爆発的な普及とコンピュータの処理速度の増加に伴い，より強力なセキュリティ機能が追加され，1998年に改訂された．そして3年が経過した現在，さらなる要求に答えるために再度手が加えられようとしている．このプロトコルは共通鍵暗号を利用しているが，使用する共通鍵暗号を特定していない．相互接続性のために実装必須とするいくつかのアルゴリズムを定めているのみにとどめている．これは「プロトコル実装暗号アルゴリズムについて」で述べた状況に加え，要求されるセキュリティの高さに応じてさまざまな共通鍵暗号を使えるようになって

いる．

2つ目は，基幹となるプロトコルで共通鍵暗号を利用するための方法を定めた仕様だ．暗号アルゴリズムは時代と共に脆弱化し，また強力なアルゴリズムが生まれる．新しい暗号アルゴリズムをIPsecに導入しやすくするために，基幹プロトコルから切り離してある．最初は1995年に3つのアルゴリズムのための仕様が発行され，それらのアルゴリズムが脆弱化したために，1998年に4つ追加された．そして，より強力なアルゴリズムの必要性が望まれて，もうすぐ新しい暗号アルゴリズムが2つ追加されようとしている．

3つ目は，共通鍵暗号に使う鍵を安全に共有するための仕様だが，ここに問題が山積みされている．鍵を正しく共有するためには，通信する相手を認証しなければいけない．限られた通信環境では事前に申し合わせたデータを使って相手を認証できるが，IPsecを広範囲に普及させるためには，より強力で汎用的な認証の仕組みが必要だ．そのために公開鍵暗号の使用が考えられたが，それにはPKIの普及を待たなければならなかった．結局，WGは相手を認証する方法を1つに定めずに，いくつかの方法を選択できるようにして，PKIの普及を待たずに1998年にIKE（Internet Key Exchange）という仕様を発行した．

IKEが標準化されるまでにはさまざまな候補があり，それらを包括するために，汎用的な枠組みと，その枠組みを利用したプロトコルと，そのプロトコルのパラメータを定義する3つのドキュメントに分かれてしまった．これは実装を困難にし，相互接続性に問題が残った．また仕様に曖昧さがあったため，毎年1回から2回，相互接続テストをして問題点を検討し仕様を固めていった．その結果，安全性の問題とプロトコルの欠陥が見つかったために，現在急ピッチでこれに代わる仕様を策している最中である．

IPsecへの期待が大きかっただけに，この事態はIETFの各WGに影響を与えている．また，市場ではすでにIPsecを実装した機器が多く出回っているため，新しい仕様が市場に与える影響も大きいと予想される．これからも動向が注目されるWGである．

■pkix WG

pkix WGは，X.509に基づいた公開鍵基盤（PKI）をインターネットで利用するための仕様を検討すべく，1995年に発足した．

公開鍵暗号を通信で利用するにあたっては，通信相手の持つ秘密鍵に正しく対応した公開鍵を入手することが必要である．PKIは，特に公開鍵を通信相手に正しく伝えるための基盤を提供する．たとえば，インターネットユーザの間で利用するには，誰もが公開鍵フォーマットを解釈できるよう共通化する必要があり，また与えられた公開鍵が本当に通信相手の公開鍵かを確かめる手段が必要である．

X.509がすでに存在しているにもかかわらず，なぜIETFであらためて検討する必要があるか疑問に思うかもしれない．X.509では，通信相手の名前と公開鍵とを対応づけることになっているが，名前の表現形式はX.500で定義されていた．これに対して，インターネットで使われる名前の表現形式は，メールアドレス，ホスト名，IPアドレスなどさまざまであり，X.500以外で定義されている名前の表現形式も扱えるようにする必要があった．

このような背景のもと，通信相手の名前と公開鍵とを対応づける「証明書」と呼ばれるデータのフォーマット検討を始めとして，証明書を発行するためのプロトコルや，証明書が本物かどうかを検証するためのプロトコル検討が行われてきた[4]．

このWGで最初にRFCが発行されたのは1999年で，WG発足後3年かかった．この間，製品やサービス市場がどうなっていたかというと，標準化を待たずにすでに動いていた．というより製品やサービスを提供している企業が，その仕様を標準化に盛り込もうとしている状況であった．

PKIXのプロトコルフォーマットは，X.509の証明書フォーマットがASN.1で定義されている影響からか，今のところASN.1一色である．PKIXで一通りのプロトコル標準化が終わるまでは，ASN.1で進めるのではないかと予想される．

PKIXのモデルでは，たとえば，通信相手の秘密鍵と公開鍵の対を誰が作るかというだけでも，本人か，第三者か，という選択肢を許している．この選択によって描かれるシナリオが異なれば，同じプロトコル対応であっても，選択するオプション

フィールドが変わり，相互接続は成り立たない．したがって，PKIXのRFCに従った相互接続実験を行う場合には，利用シナリオを想定した絞り込みがかけられる．なお，国内でもJNSA（日本ネットワークセキュリティ協会）などによる相互接続実験が行われている．

筆者（櫻井）は，PKIXがどうして汎用にこだわるか一時期納得がいかなかった．しかし，ある時，秘密鍵と公開鍵の対を第三者に作らせるシナリオを描いた後でPKIXのプロトコルを眺めたところ，独自拡張なしにシナリオに対応できると気づいた．PKIXの目指す汎用性と基盤の意味をようやく理解できた瞬間である．PKIXが収束しつつあるということは，現状のシナリオに限らず，別のシナリオを展開するチャンス到来と捉えるべきだろう．

■idwg

idwgは，互いに協調する必要があるネットワーク侵入検知システムや，ネットワーク管理システム間で情報共有するためのデータフォーマット，および情報交換手順の策定を目的に1998年10月に発足した．

現在，侵入検知情報交換のためのアラートメッセージの形式と通信プロトコルを，要件案に沿って議論している．この要件案は，侵入検知システムが扱う情報モデルよりもメッセージの標準形式に重点を置いており，WGの方針を表している．

アラートメッセージの形式については，XML DTD 採用ということでほぼ決まり，IESGの最終勧告を待っている状況である．

議論の過程で，アラートメッセージの交換モデルとしてアナライザからマネージャに送られるメッセージの中にすべての情報が埋め込まれるプッシュ型モデルの提案が採択され，マネージャが随時必要な追加情報をアナライザから回収するプル型モデルは対象外となった．ネットワーク管理システムでよく使われるSNMPで標準の，ASN.1により定義されたMIB形式ではプル型が利用できるが，これは受け入れらなかった．このことは結果として標準形式に重大な影響をもたらした．

通信プロトコルについては，有力候補は汎用BEEP（Blocks Extensible Exchange Protocol）を用いた方法であるが要件案の要件をすべて満たすのは難しいと考えられ，検討にはまだ時間がかかりそうである．通信プロトコルは，決まったとしても推奨扱いであり，相互接続性はアラートメッセージの形式レベルで確保されることに注意が必要である．

idwgは，仕様を実装し，実際に運用して経験を積むべき時期にさしかかっている．

第53回IETFから

2002年3月18～22日に，米国ミネアポリスにて開催されたIETFにおける話題を紹介する．

まず，全体の動向として，セキュリティエリア以外でセキュリティ機能に関するWGやBOFがいくつか開催されていた．

* Routing Protocol Security Requirements BOF
  → ルーティングエリア
* Protocol for carrying Authentication for Network Access
  → インターネットエリア
* Secure Internet Key Distribution BOF
  → オペレーション&マネージメントエリア

また，"Security Area Directorate"と呼ばれる組織の創設提案があった．これは，近年セキュリティに対する他エリアのWGからの要求が高まったことに対応するもので，セキュリティエリアのWGチェアとアドバイザグループ（新設）から構成される組織である．主に他エリアに対してセキュリティに関する助言を行う．

セキュリティエリアについては，まず，ipsec WGでのIKEの次バージョン検討が大きな話題であった．次バージョンの候補として，現バージョンとの互換性を考慮したIKEv2と，まったく新規に設計されたJFK（Just Fast Keying）の2つが検討されていた．今回のセッションでは，この2グループが歩みより，合同で次バージョンを設計していくことが発表された．

また，新しくinch（Extended Incident Handling）BOFが開催された．これは，不正アクセスを受けた場合に，CSIRTs（Computer Security Incident Response Teams）などの対応機関との情報交換を容易にする目的で，データフォーマットやデータモデルを検討しようという趣旨であった．最近の不正アクセス増加に対するIETFの敏感な反応を示しているといえる．

IETFへの参加に向けて

このエリアは，日本からの貢献がまだまだ少ない．他のエリアと同様，個人プレーにとどまらず，少なくとも組織の戦略を掲げて，理想的には早い段階で複数の組織と組んでとりかかる必要がある．

参考文献

1）Postel, J. and Reynolds, J.:Instructions to RFC Authors, RFC2223（1997）.
2）FIPS-197:http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
3）CRYPTREC：http://www.ipa.go.jp/security/enc/CRYPTREC/index.html or http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/index.html
4）櫻井三子：PKI，bit別冊 情報セキュリティ，第9章 pp.245-254，共立出版（2000）.

（平成14年5月7日受付）