Vol.37 No.6 情 報 処 理 June 1996

解 説

暗号安全性の最近の動向

2. インターネット・セキュリティ†

山 口 英††

1. はじめに

1980年代初頭に米国で学術研究用ネットワークとして開発が始まったインターネット(Internet)は，1990年代に入ってその商用利用が開始され，現在では，80カ国以上，ユーザ数3,000万人とも言われている巨大かつ国際的なコンピュータネットワークとして急速な成長を続けている．さらに近年では，従来から盛んに使われている電子メール，ニュース，ファイル転送などのサービスだけでなく，WWWに代表される情報発信・共有サービスや，さらにはインターネット環境を基盤としてエレクトロニック・コマース(EC:Electronic Commerce)を現実のものにしようとした実験が盛んに行われるようになった．

インターネットにおいて，具体的な経済活動が行われようとする場合，その安全性を保証するセキュリティ保全技術について注目が集まるのは，当然である．このため最近では，よりセキュリティを重視したさまざまなインターネット技術の研究開発が活発化している．

本稿では，インターネット環境におけるセキュリティ技術の現状と展望について述べる．まず，インターネット環境におけるセキュリティに関する基本的な問題を述べ，さらにそれらを解決するために現在使われている代表的な技術を紹介する．さらに，次世代インターネットプロトコルである，IPv6におけるセキュリティ機構についても紹介する．

2. インターネット・セキュリティとは

インターネットは，複数のISP(Internet Service Provider)によって通信路が形成され，世界中に分散した計算機によってサービスが提供されている．このような環境において発生する脅威(thrcats)は多種多様であり，さまざまな技術を用いてセキュリティを保全することが必要となる．ここでは，インターネット環境において考慮すべき脅威と，それらに対する現在の技術的解決の方向性について述べる．

2.1 通信プロトコルから見た脅威

コンピュータネットワークにおけるプロトコル機能として解決すべきセキュリティの問題は，1980年代にVoydockとKentによって，コンピュータネットワークに対する脅威(threats)として以下のように定義された[1]．

- 受動攻撃(Passive Attack)
  1. 盗聴(release of message contents)
  2. トラヒック解析(traffic analysis)
- 能動攻撃(Active Attack)
  1. 通信の改ざん(message stream modification)
  2. 通信の妨害(denial of message services)
  3. 不正なアクセス(spurious association initiation)，なりすまし(masquerading)

Voydockらが述べているように，受動攻撃は防止でき，能動攻撃に対しては少なくとも発見することが可能である．これらの脅威のうち，何を対象とするか，さらにそれをどのプロトコル階層で実現するかによって，さまざまなセキュリティシステムが考えられる．

Voydockらによる定義は，インターネット環境においても，そのまま適用することができる．現在のインターネットで使用されているネットワーク層(IP)とトランスポート層(TCP，UDP)では，セキュリティ機能はまったく提供されていない．したがって，現在のインターネットでのセキュリティ機能は，すべて上位層であるアプリケー

† Internet Security by Suguru YAMAGUCHI (Nara Institute of Science and Technology).
†† 奈良先端科学技術大学院大学情報科学研究科

ション層の機能として実現されている．

米国CERT(Computer Emergency Response Team)による最近のCERT Advisory☆によれば，

(1) Sniffer Attack
(2) Source Address Spoofing
(3) IP packet fragmentation Attack
(4) TCP Connection Hijack
(5) TCP De-synchronous Attack

などが具体的なセキュリティ問題として報告されている．(1)は盗聴によるパスワードの取得，(2)は始点アドレスの改ざんによるなりすまし，(3)～(5)についてはTCP/IPの特徴を逆手に取った不正アクセス手法である．特に，盗聴によるパスワードの入手は深刻な問題である．このため，最近のインターネットにおけるセキュリティ技術として，盗聴および通信の改ざんから通信を守るための暗号化機能と，不正アクセス，なりすましを防ぐための認証機能が，数多くの具体的なアプリケーション・プロトコルに組み込まれるようになってきている．

一方，トラヒック解析については，インターネット環境ではあまり重視されてはいない．通信の存在そのものが重大な情報になる軍事ネットワークとは違い，インターネットはオープンな環境であることが最大の理由である．

また，通信の妨害については，本来考慮すべき脅威である．しかしながら，一般的にインターネットを使って通信ができない場合にそれが障害なのか妨害なのかを判断する方法がないことや，インターネットの管理責任は複数のISPに分散していることによって，通信妨害を考慮したプロトコル開発は，これまで行われていない．

2.2 システム運用面から見た脅威

インターネットに接続されているシステムの運用面から考えた場合，最も注意しなければならない脅威が，システムへの不正侵入である．インターネット環境において攻撃者の大部分は，まずシステムへの不正侵入を試みる．仮にシステムへの侵入に成功すれば，攻撃者にとっては以下のような多くの利点がある．

(1) そのシステムに蓄積されている情報を入手できる．特に特権ユーザの権限を不正に入手した場合には，そのシステム上のすべての情報を入手できるだけでなく，サービスを乗っ取ることができる．

(2) そのシステムを踏み台として他のシステムを攻撃することができる．特に，他国のシステムを踏み台として使う場合には，攻撃者の侵入経路の発見と特定が困難であるため，犯行が発見されにくい．

(3) そのシステムを使って，ネットワークを盗聴できる．盗聴により，そのシステムが直接接続されているネットワーク上のほぼすべてのユーザのパスワードだけでなく，ユーザがログインした遠隔のシステムのアカウントまでを入手することが可能となる．現在CERTなどから報告されているSniffer Attackでは，攻撃者はいったん不正侵入し，ネットワークをモニタリングするプログラムを仕掛け，攻撃者自身はシステムからログアウトした状態にしておくことが多い．この場合，攻撃者は直接発見される危険を犯すことなくネットワークを盗聴できる．

このような理由から，インターネットにおける攻撃者は，不正に入手したパスワードを使ったり，システムアプリケーションが持つバグや裏口などを悪用して，システムに侵入しようと攻撃を仕掛けてくるのである．

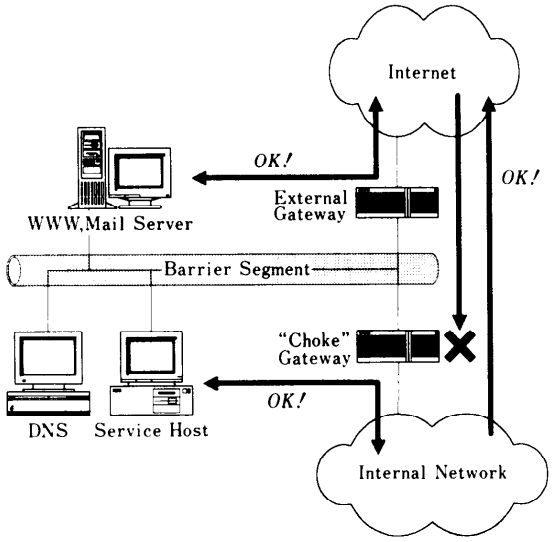
このため，近年では不正侵入に強いネットワーク環境の構築が一般的になってきている．これに使われる技術としては，ファイアウォール(firewall)と呼ばれるゲートウェイシステムを導入したり，使い捨てパスワード(OTP:One-Time Password)などの盗聴に強いユーザ認証を用いたりすることが多い．さらに，仮に不正侵入された場合でも，その発見を早めるためのシステム監査ツールを導入したり，あるいは，ファイルなどの情報資源を暗号化するなどの対策が取られるようになっている．

3. ファイアウォール

ファイアウォール☆☆は，インターネットとの接続を工夫して，接続されるネットワーク全体セキュリティ強度を高める手法であり，1990年代に入って一般化した技術である．

通常，インターネットに接続する場合，単一の

☆たとえばftp://ftp.cert.org/pub/cert_advisories/などから入手できる．



図－1 ファイアウォールの一般的な構成

コンピュータを接続するのではなく，ローカルに運営されているネットワーク(たとえばキャンパスネットワークなど)を接続するのが一般的である．インターネットとの接続において何ら通信の制限を加えない場合，ネットワークシステム全体のセキュリティを保全する時には，そのローカルのネットワークに接続されているすべての計算機において同レベルの対策を実施しなければならない．ローカルのネットワーク環境の規模が小さければ，このような対応も可能であろう．しかしながら，管理すべきネットワークシステムの規模が大きくなれば，接続されているすべてのシステムに対してきめの細かいセキュリティ保全対策を施すのは大変である．このため，インターネットとの接続ポイントにセキュリティ対策を集約し，ローカルのネットワーク全体のセキュリティ保全を高める技術として，ファイアウォールが考え出された．

図－1に一般的なファイアウォールの構成を示す．ファイアウォールでは，インターネットを内部のネットワークと接続するときに直接接続するのではなく，チョーク(choke)と呼ばれるゲートウェイを置く．チョークでは，インターネットから内部ネットワークへの直接のアクセスを阻止する．この実現にはパケット・フィルタリングやトランスポート層ゲートウェイ(たとえばsocks)などの技術が利用できる．WWW，DNS，電子メールなどのサービスを提供するサーバは，インターネットから直接アクセスできるようにチョークの外側に置く．これらのサーバを接続しているネットワークセグメントのことをバリアセグメント(barrier segment)あるいは境界セグメント(border segment)というように呼ぶことが多い．バリアセグメントにあるサーバは，内部ネットワークからも自由にアクセスできるように設定する．バリアセグメント上のサーバ群とチョーク・ゲートウェイのセキュリティ保全を万全に行えば，内部ネットワークへの不正侵入はかなり防ぐことができる．

チョーク・ゲートウェイとしては，ルータを使用して構成することができる．さらに最近では，チョーク・ゲートウェイとして使用できるさまざまなファイアウォール製品が数多く提供されており，それらを使ってファイアウォールを構築することも一般的になってきている．

現在のインターネット環境を考えた場合，今やファイアウォールを導入するのは当然という状況になっている．日本国内では，特に大学を中心にファイアウォールの導入をしていない組織がまだまだ数多い．セキュリティに関する問題を減らすという意味でも，今後の積極的な導入が必要である．

4. 使い捨てパスワード

使い捨てパスワード(OTP)[2]は，近年多くのインターネットサイトで積極的に導入されている技術である．

先に述べたようにインターネットで使用されているIP，および，TCPでは，パケットのデータ領域は暗号化されない．さらに，インターネット環境で遠隔システムへのターミナルアクセスに使用されるtelnet，rloginなどのプロトコルでは通信内容の暗号化機能は提供していなかった．このため，telnet，あるいはrloginの通信内容を盗聴すれば簡単にユーザのパスワードが盗める．1994年にSniffer Attackと呼ばれる盗聴手法を使用し

☆☆ 現在では数多くの解説書があるが，Marcus J. Ranum : Thinking About Firewalls, Proceedings of Second International Conference on System and Network Security and Management (SANS-II) (Apr. 1993).において初期にファイアウォールを体系的に分類している．以下のFTPサイトから入手できる． ftp://ftp.greatcircle.com/pub/firewalls/papers/ranum/fwalls.ps.Z

て，実際に米国において数千人のパスワードが盗まれるという事件が発生して以来，パスワードの保護するさまざまな技術が広く使われるようになった．この中の1つが使い捨てパスワードである．

4.1 使い捨てパスワードの方式

使い捨てパスワードとは，システムにログインするたびに毎回異なったパスワードを使用するユーザ認証方式である．使い捨てパスワードが持つべき特性は以下のようなものがある．

・使用するパスワードの周期が十分に長い．
・現在使用したパスワードが盗聴されたとしても，次に使用するパスワードの推定ができない．
・使い捨てパスワードを使用しているシステムに不正侵入されても，そのシステム上のユーザのパスワードについての情報が漏洩しない．

このような特性を持った使い捨てパスワードシステムとして，同期乱数生成器(synchronized random generator)の手法を使ったものと，Message Digest を使用した方式がある．

前者の方式の原理は，同期した2つの乱数発生器をユーザ側とサーバ側で持ち，ログインしようとした時に生成されてる乱数をパスワードとして使うものである．同期方法としては，時刻をベースとしてゆっくり(たとえば1分間に1つの乱数の生成をする)と乱数を発生させるものと，ユーザのログイン回数に応じて乱数を発生させるものがある．同期乱数生成器による方式では，一般に特別なハードウェアを使用することが多く，実際に実用化されている商品のほとんどがカード型電卓に似た特別な乱数発生器を使用している．

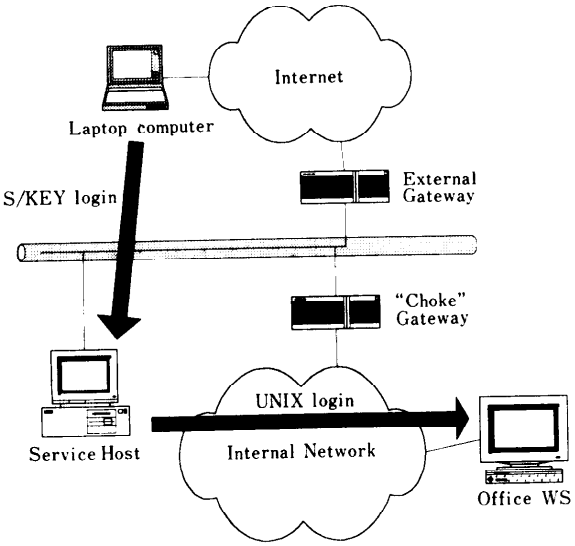


図-2 ファイアウォールでの使い捨てパスワードの利用

一方，後者の方式では，一方向関数であるMessage Digest 関数(MD)を利用している．インターネットで標準化されている MD[3),4)]は，

・任意のバイト列を入力として，出力に16バイトの整数値を与える．
・同じ出力を与える入力(衝突する入力)の発見が難しい．
・逆関数を定義するのが困難である．

といった特徴を持つ．

ここで，バイト列 k が入力である MD を MD(k)と表記する．さらに，バイト列 k に対して n 回繰り返し MD を適用したものを $MD^n(k)$ と表記することにする．MD を使用した使い捨てパスワードのアルゴリズムは，次のようになる．

1. サーバ側では，各ユーザについて n と $MD^n(k)$ を記録しておく．
2. あるユーザがログインする場合には，サーバ側では，そのユーザについて n-1 をクライアント側に提示する．
3. クライアント側では，$MD^{n-1}(k)$ をローカルに計算し，それをサーバに送る．
4. サーバ側では，クライアント側から送られてきたバイト列 s から MD(s)を計算する．この値と，記録してあった $MD^n(k)$ が一致した場合には，正当なユーザとしてログインを認める．さらに，サーバ側では，そのユーザについての記録を n-1 と s(すなわち $MD^{n-1}(k)$)に更新する．

ここで k を一般にパスフレーズ(passphrase)と呼ぶ．このアルゴリズムから分かるように，ネットワーク上，およびサーバ上で取り扱われるものはすべて MD であり，平文の k は唯一クライアント側で $MD^{n-1}(k)$ を計算するときに使われる．この計算は，ラップトップコンピュータなどの安全な環境で計算すれば，k が危険にさらされることはない．

4.2 S/KEY

MD を使用した使い捨てパスワードの代表的なものとして，米国 Bellcore が開発した S/KEY がある[5),6)]．S/KEY では，k としてユーザが覚えておくべきパスフレーズと，シード(seed)から構成される．ユーザがパスフレーズを変えなくても

シードだけを変えれば，使用するパスワードの系列を変えることができ，系列の再初期化時に毎回パスフレーズを変える必要がない．S/KEY はフリーソフトウェアとして提供されており導入しているサイトが非常に多い．さらに 1995 年からは IETF において使い捨てパスワードの標準化作業が開始されており，MD を使用した S/KEY 以外の使い捨てパスワード機構も考慮したツール群が広く提供されるようになってきた．

4.3 使い捨てパスワードとファイアウォール

ファイアウォールを使用している環境では，使い捨てパスワードを併用することで，そのセキュリティ的な強度を高めることができる．

一般に，インターネットから内部ネットワークにアクセスするために，ファイアウォール上にユーザがいったんログインをするホストを用意することが多い(図－2 参照)．このようなホストをサービスホストと呼ぶ．サービスホストへのログインに使い捨てパスワードを使うことで，ファイアウォールの強度を高められる．一方，このサービスホストから内部のシステム(図では Office WS)へのログインは，通常の UNIX ログインを使っても問題はない．内部のホストに対してはインターネットから直接アクセスすることはできないため，不正侵入を試みる者はいったんサービスホストに侵入しなければならないからである．サービスホストと同様に，バリアセグメント上の他のサーバについても，使い捨てパスワードを使うことが一般的になっている．

5. アプリケーションでのセキュリティ

インターネットにおける盗聴の問題を解決するために，アプリケーション層プロトコルにおいて，通信データの暗号化機能や認証機能を付加したアプリケーションが数多く利用可能になってきている．ここでは，代表的なものとして電子メール，telnet，WWW について述べる．

5.1 電子メールの暗号化

セキュリティ問題の解決のためだけでなく，プライバシー保護の立場からも，電子メールの暗号化については関心が高く，最近では，PEM (Privacy Enhanced Mail)[7]，MOSS(MIME Object Security Service)[8]，PGP(Pretty Good Privacy)[9]などのシステムが使われている．提供されるサービスとしては，電子メールに対する署名，内容の暗号化，送受信者の認証，データの完全性の保証，さらにメールの送信に対する非否認性の保証を行うことができる．

これらの方式については，それぞれ一長一短があるが，世界的に見ると現状では PGP が広く使われている．さらにインターネットメールの新たな書式を定義している MIME に対して，PGP を適合させる PGP/MIME の作業も進められており，プライバシーを保証し，より適応性の高いインターネットメールが実現されようとしている．また，これら代表的な方式以外にも，新たな方式を用いた電子メールの暗号化機構が現在でも開発されており，多種多様なシステムが提供され続けると考えられる．

5.2 PET

PET(Privacy Enhanced Telenet)は，PEM で使用していた利用者認証の機構を利用して，telnet において安全な通信を実現するものとして開発された．先に述べたように telnet では，パスワードを含めて，すべての通信が平文のまま行われている．このため，盗聴による情報の漏洩の問題があった．PET はこの問題を解決する機構である．国内においては，WIDE Project と富士通研究所が共同で開発したシステムが利用可能となっている．

5.3 WWW

WWW における通信の暗号化とユーザの認証は，インターネット上のエレクトロニック・コマースの実現ということからの要請が強い．現在 WWW で商品の購入をする場合には，クレジットカードを使った決済が一般的である．この場合，基本的にクレジットカード番号だけで商品が購入できるため，クレジットカード番号をどのように安全に送信するかが問題となっていた．さまざまなシステムが提案されてきたが，現状では Netscape，Terisa Systems などが中心となって標準化を進めている SSL/SHTTP が広く使われるシステムとなっている[10),11)]．この機構では，TCP/IP の上位に SSL と呼ばれる通信路での暗号化を実現するセション層を導入し，さらに，従来の HTTP を拡張して安全な WWW トランザクション通信ができる SHTTP を使用する．これにより，盗聴から通信を守るだけでなく，必要ならば

サーバの認証も可能となっている．しかしながら，ユーザ認証ができないといった欠点も残されている．このようなことから，SSL/SHTTP よりもより実用的な機構を開発しようとする動きがある．1995 年に設立された認証実用化実験協議会☆では，1996 年中の実用化を目標に HTTP に対して暗号化，ユーザ認証・サーバ認証，署名などの機能を含めた新たな機構を開発している．

6. IPv6 でのセキュリティ機能

従来，TCP，および IP において不足していたセキュリティ機能を補うために，これまで多くの機能拡張が行われてきた．具体的には，IP に対しては swIPe，IP/Secure など，トランスポート層に対しては Secure TCP などが開発され，さらに IETF IPSEC-WG の活動により IP におけるセキュリティ機能の標準化が行われた．

これを背景として，1995 年に標準化案が決められた次のインターネットプロトコルである IPv6 では，当初より強力なセキュリティ機能が採用されている[12]．

IETF は IPv6 の標準化作業でセキュリティ機能を追加するために 3 つの仕様を作成している．

- IP Authentication Header[13]
- ESP(Encapsulated Security Payload)[14]
- 鍵管理

Authentication Header は，IPv6 ヘッダとともにつけられ，通信を行うホスト間での認証に使われる．ここでの認証は，ホスト単位での認証も，ユーザ単位での認証もできるようになっている．これは，相互に認証ができている関係(Security Association と呼ぶ)の識別を，通信相手のアドレスと，Authentication Header 内の SPI(Security Parameter Index)の組合せで識別する．ホスト単位での認証を行う場合は，同一のホストに対する Authentication Header 内の SPI は同じ値を使用する．一方，ユーザ単位の認証を行う場合には，ユーザごとに SPI を変えるという方法で対応している．認証方式に対しては，この標準案では定義していない．また，Authentication Header を使うことで，データの完全性(integrity: 改ざんされていないこと)を検証できる．

ESP は，Authentication Header と共に使われ，IPv6 での通信データの暗号化の機能を提供する．現状では，パケットの書式を定義しただけであり，具体的な暗号化方式などについてはいっさい規定していない．

鍵管理は，現在標準化が進められている段階であり，Photuris[15]や SKIP[16]などが提案されている．基本的には，公開鍵暗号を使用した通信鍵の交換を基礎にしているが，現状では最終的な標準案は決定していない．

IPv6 でのセキュリティ機能が実現されると，Internet 上で安全な通信が基礎から保証されるようになる．もちろんこれだけでセキュリティの問題がすべて解決するわけではないが，現在のインターネットの状況と比較すれば，状況は大きく改善されると考えられる．現時点では，IPv6 のセキュリティ機能の実装が始まったばかりであり，認証方式，暗号化方式，鍵管理方式としてより具体的なものが提案されるのは 1996 年中になると考えられている．

7. おわりに

インターネットにおけるセキュリティ機能は，近年急激に強化されつつあり，特に現在のインターネットでのセキュリティ問題の増加を解決し，さらに将来の EC を実現するために注目されている．また，次のインターネットプロトコルである IPv6 のセキュリティ機能は，次のインターネットの基礎となるため，多くの研究者，技術者が注目している領域である．

インターネットにおけるセキュリティ研究では，実システムの開発とその評価が必須であり，多くの組織，研究者が積極的に技術開発に取り組んでいる．このため，インターネットにおけるセキュリティ技術の推移は早い．この分野における研究者，技術だけでなく，セキュリティ保全技術を必要としているユーザも，注意深くこの研究領域の変動を見続けることが必要であろう．

また，セキュリティ保全はその技術だけでなく，教育，制度，運用方針，物理的なセキュリティなど，多くの要素から構成されるものである．したがって，セキュリティ保全には総合的な視点に立った実施，評価が必要となる．日本ではセキュリティ関係の研究者・技術者・コンサルタントが非

☆ 協議会の活動についての情報は http://www.icat.or.jp から入手できる．

常に不足していると言われている．来るべきネットワーク社会に向けて，この領域へのより積極的な取り組みが期待されている．

参 考 文 献

1)Victor, L. Voydock and Stephen, T. Kent : Security Mechanisms in High-Level Network Protocols, ACM Computing Surveys, Vol.15, No.2, pp.135-171 (1993).
2) Lamport, L. : Password Authentication with Insecure Commnication, CACM, Vol.24, No.11, pp.770-772 (1981).
3) Rivest, R. : The MD5 Message-Digest Algorithm, RFC1321 (Apr. 1992).
4) Rivest, R.: The MD4 Message-Digest Algorithm, RFC1320 (Apr. 1992).
5) Haller, N. : The S/KEY One-Time Password System, RFC1760 (Feb. 1995).
6) Haller, N. : The S/KEY One-Time Password System, Proceedings of the ISOC Symposium on Network and Distributed System Security (Feb. 1994).
7) Linn, J., Kent, S., Balenson, D. and Kaliski, B. : Privacy Enhanced Mail, RFC1421, 1422, 1423, 1424 (Feb. 1993).
8) Crocker, S. et al. : MIME Object Security Services, RFC1848 (Oct. 1995).
9) Garfinkel, Simson : PGP: Pretty Good Privacy, O'Reilly & Associates, Inc. (1995).
10) Rescorla, E. and Schiffman, A. : The Secure HyperText Transfer Protocol, Internet Draft, draft-ietf-wts-shttp-00.txt (July 1995).
11) Freier, A., Karlton, P. and Kocher, P.C. : SSL Version 3.0, Internet Draft, draft-freier-ssl-version3-00.txt (Dec. 1995).
12) Atkinson, R. : Security Architecture for the Internet Protocol, RFC1825 (Aug. 1995).
13) Atkinson, R. : IP Authentication Header, RFC1826 (Aug. 1995).
14) Atkinson, R. : IP Encapsulating Security Payload (ESP), RFC1827 (Aug. 1995).
15) Karn, P. et al : The Photuris Session Key Mnagement Protocol, Internet Draft, draft-ietf-ipsec-photuris-08.txt (Nov. 1995).
16) Aziz, A. et al : Simple Key-Management for Internet Protocol (SKIP), Internet Draft, draft-ietf-ipsec-skip-06.txt (Dec. 1995).

(平成8年2月2日受付)

山口 英（正会員）

昭和61年大阪大学基礎工学部情報工学科卒業．昭和63年同大学院博士前期課程修了．平成2年同博士後期課程を退学し，同大情報処理教育センター助手に着任．以後，平成4年奈良先端科学技術大学院大学情報科学センター助手，同年同大学情報科学センター助教授を経て，平成5年同大学情報科学研究科助教授．平成3年工学博士（大阪大学）．インターネットアーキテクチャ，ネットワークセキュリティ，高速ネットワークに関する研究に従事．電子情報通信学会，IEEE，Internet Society各会員．