2. e-Societyを推進する暗号技術

1. インターネット・無線LAN・放送における暗号化技術

難波 誠一
NHKエンジニアリングサービス
namba@nes.or.jp

小口 正人
お茶ノ水女子大学
oguchi@computer.org

インターネット・無線LANにおける暗号化技術

●インターネットにおける階層別の暗号化手法

ネットワークにおける通信プロトコルは，機能ごとに切り分けられた階層構造を持つことが一般的である．図-1に示すように，インターネットにおける暗号化も階層別にさまざまな手法が提案されてきた．S/MIMEやPGPは電子メールに用いられ，SSL/TLSは主にWebブラウザで利用されているというように，上位層における暗号化手法は特定のアプリケーションに組み込まれることが多い．一方，下位層における暗号化手法は汎用的な通信において利用可能である．

セキュリティに対してパフォーマンスや利便性はトレードオフの関係にあると考えられ，導入の際にはどのような安全性がどこまで必要であるかを明確にした上で，セキュリティ手法の中から選択を行うことが重要である．現状ではインターネット上に平文のデータが流されているケースも多いと考えられるが，重要なデータの通信を行う場合や，盗聴，改ざんなどをされやすい環境においては，暗号化は必須である．以下においては，そのようなセキュリティ手法の利用例であるインターネットVPNと無線LANの暗号化を紹介する．

●インターネットVPN

インターネットにおける暗号化技術の応用の中で現在注目を集めているトピックにVPN（Virtual Private Network）がある．VPNは既存の公衆回線上に仮想的な私的ネットワークを構築する技術の総称であるが，そのうちインターネットをベースとして用いるものを「インターネットVPN」と呼ぶ．インターネットVPNには

- 拠点間（LAN間）接続VPN
- リモートアクセスVPN

という接続形態がある．前者はたとえば会社の事業所が複数の地点に散らばっている場合に，事業所内LAN同士を接続するVPNである．一方後者は，外出先でノートPCから会社のLANへ接続するためなどに用いられる．

インターネットVPNの最大の利点は，通信コストを低く抑えられることである．拠点間を接続する場合，通信事業者の提供する専用線や，閉じたIP網を利用したMPLS（Multi Protocol Label Switching）によるVPN（これはIP-VPNと呼ばれる）を用いるより，インターネットVPNを利用した方がコストを抑えられる．しかしインターネット上にLANアクセスのトラフィックを流す以上，セキュリティに対する配慮を最大限払う必要があり，暗号化や認証は必須の要件である．

インターネットVPNの具体例としては，暗号化や認証をデータリンク層で行うPPTP（Point-to-Point

OSI参照モデル	TCP/IP階層モデル	セキュリティプロトコル
アプリケーション層	アプリケーション層	S/MIME，PGP
プレゼンテーション層		SSH
セッション層		
トランスポート層	トランスポート層	SSL/TLS
ネットワーク層	インターネット層	IPsec
データリンク層	ネットワークインタフェース層	WEP，WPA
物理層		

図-1　階層プロトコルモデルとセキュリティプロトコル例

Tunneling Protocol）[1]を利用した方式，ネットワーク層で行うIPsec（IP Security Protocol）[2]を用いる方式，トランスポート層で行うSSLを用いる方式などがある．現在はIPsecを用いた製品が最も普及しているが，SSLを用いた製品も少しずつ利用され始めている．SSL-VPNはリモートアクセスのクライアントにブラウザを用いるため，専用のソフトウェアを必要とせず，またNAT越しの通信が難しかったIPsec-SSLの弱点を補っているが，動作はWebブラウザ経由で利用できるアプリケーションに限られ，SSL処理チップ（SSLアクセラレータ）が高価であるため現状ではIPsec-SSLよりコストが高くなる場合が多い．

●無線LANにおける暗号化

現在広く用いられている無線LANはIEEE802.11b/a/gの仕様に準拠している．暗号化機能としては，データリンク層（ネットワークインタフェース層）でIEEE802.11委員会TG（Task Group）iにおいて勧告されたWEP（Wired Equivalent Privacy）が標準的に用いられている．

WEPは128ビット／64ビットの共有鍵を用いた暗号方式であり，暗号アルゴリズムにはRC4が用いられているが，現在ではWEPの脆弱性が指摘されている．理由の1つに，実質の暗号鍵長が短いということが挙げられる．WEPの128ビット／64ビットの暗号鍵のうち秘密鍵として用いられるWEPキーはそれぞれ104ビット／40ビットであり，残りの24ビットはIV（Initialization Vector）としてパケットごとに発生させ，暗号鍵と連結されて本文の暗号化に用いられる．その後IVは暗号化されずヘッダに付加されてパケットが送信されるため，IVは秘密鍵としては機能しない．

WEPの問題点としてはほかに，同一のWEPキーとIVを用いた暗号化パケット同士を比較することによる暗号解読の可能性が指摘されている．さらに特定のIVを用いたWEPは解読が容易であるといった報告もなされている[3]．

このようなWEPの問題点から，無線LANの暗号化方式を強固なものに変更しようという動きが進んでいる．まずWEPを強化したWPA（Wi-Fi Protected Access）[4]という規格が制定され，準拠した製品がすでに登場している．また無線LANにおけるさらに強固なセキュリティを定める仕様としてIEEE802.11i[5]が提案され，2004年7月に批准された．IEEE802.11iは，WPA2という名称で2004年9月からWi-Fiアライアンスによって準拠製品の認定が開始された[4]．

WPAにおいては，TKIP（Temporal Key Integrity Protocol）という暗号化プロトコルを用いる．TKIPでは，端末ごとに異なる鍵を用いる，IVとユーザの暗号鍵に攪拌等の前処理を施してからRC4に代入するなど，手順を複雑化して安全性を高めている．またTKIPはRC4の回路を利用できるため，従来製品からファームウェアの変更で対処できる．一方IEEE802.11iでは暗号アルゴリズムにAES（Advanced Encryption Standard）を用い，より強固なセキュリティが期待できる．

このように無線LANにおける暗号化は，WEPの脆弱性から，これに代わる方式が導入され始めている．ただし暗号化方式を強固にしても，正しく利用されなければまったく意味がないため，管理者やユーザに対するセキュリティ啓蒙が重要であることは言うまでもない．さらにインターネットへのセキュリティ導入においては，どのような場合にどのプロトコル階層で暗号化を行うかといった議論を十分に行うべきである．

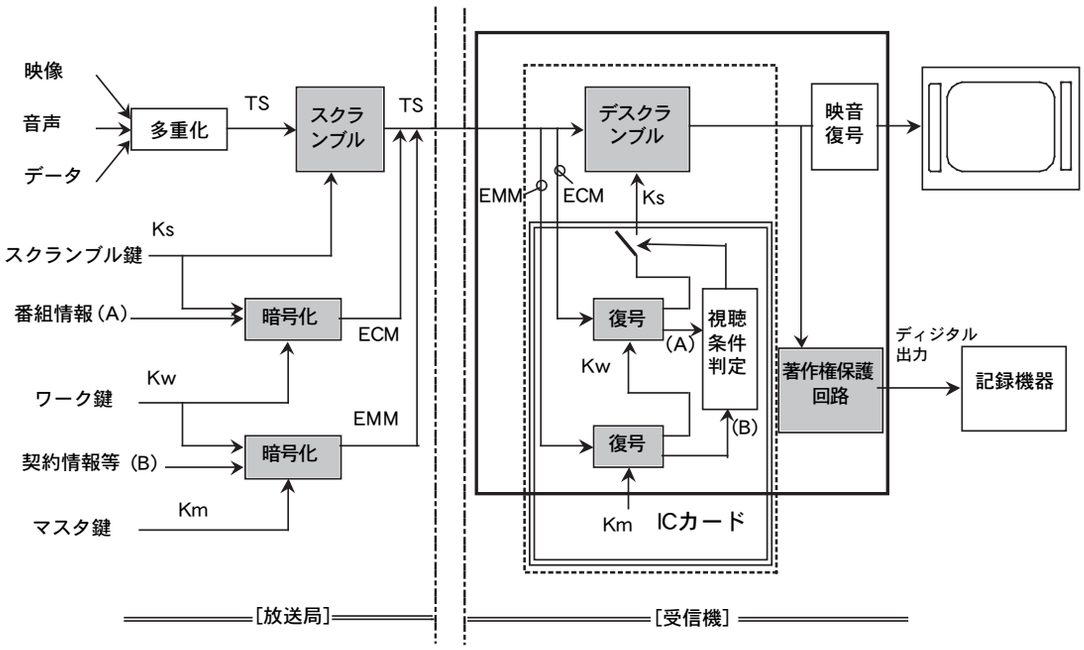
放送における暗号化技術

●放送と暗号化技術

放送での暗号化技術は，暗号化の本来の目的である伝送される情報の内容を秘匿するためではなく，有料放送を実現する，あるいは，放送される情報に関する権利を保護するといった目的のために使用される．この分野は，身近に置かれる暗号応用のシステムとして急速に数を増しているものであり，暗号のセキュリティを考える上でも，暗号装置の端末が各家庭内に置かれること，コンピュータでの放送受信が増えることなどから，重要な分野となっている．

●有料放送実現への応用

有料放送を実現するためには，本来広く情報を伝えるための放送信号を契約者の受信機のみに限定して伝える技術（限定受信方式，コンディショナルアクセス方式などと呼ばれる）が必要である．この技術は放送される信号を一律にスクランブルする技術と，契約した受信機のみで復元するための技術で成り立っており，これらに暗号化技術が適用される．一般的なシステム構成は**図-2**のようになっており[6]，(1) 信号をスクランブル伝送する系統，(2) このスクランブルを制御する鍵（Ks）（秒単位で更新）をKw（月～年単位で更新）とKm（受信機に固有）の階層化した鍵で暗号化して送る系統，(3) 各番組の受信を契約の有無で制御する系統，で構成される．受信機でのセキュリティの処理は，我が国のディジタル放送の規格では図-2の2重線で囲まれたICカードの部分で行われるが，ヨーロッパ等ではデスクランブル部分も含めた点線で囲まれた部分を取り外し可能なモジュール化する方式が規格化されている．



TS：トランスポート・ストリーム　　ECM：関連情報（全受信機に共通の情報）　　EMM：関連情報（受信機ごとに個別の情報）

図 -2　ディジタル放送における限定受信方式の基本的構成

信号のスクランブルについては，いわゆるアナログ放送では信号の性質に応じて色々な方法が用いられたが[7]，ディジタル放送の信号では暗号方式を用いて統一的にスクランブルされる．我が国のディジタル放送では，信号をストリームのかたちで送る場合についてはMULTI2暗号化方式による方式が規格化されており，受信機本体が自由に製造できるようになっているが[8), 9)]，信号をファイルのかたちで送る場合の暗号化方式は規定されていない．

契約した受信機のみで受信できるようにするためには，関連情報と呼ばれる情報（図-2のECM，EMM）を送って各放送番組の情報と受信機の契約内容とを照合した上で，暗号を復号する鍵が再生される．この関連情報の不正利用を防ぐために暗号化が行われるが，この暗号化と復号は，放送局の設備と受信機に装填されるセキュリティモジュールでの処理が対応していればよく，非公開の暗号方式で実現される例が多い．

現在，受信機に大容量の記憶装置を持って新たな放送サービスを行うサーバ型放送が検討されているが，この放送では，暗号化した状態で記憶しておき，再生時に課金等の処理を行うことも可能になる．このような技術は限定再生方式と呼ばれる[8), 9)]．

●著作権保護への応用

ディジタル放送では，受信機でデスクランブルされた後の信号の複製を制限できることが重要である．特に，受信機からディジタル信号のかたちで記録機器等へ出力される場合には，著作権を保護する機能を持っていることが必要で，これを確実に保証するために，放送信号をスクランブルして送り，デスクランブル用のセキュリティモジュールをこの保護機能を持つ受信機のみに供給する方法が用いられている[9)]．我が国では，このような権利保護を目的としたスクランブル放送が2004年4月から開始されている．

参考文献
1）Point-to-Point Tunneling Protocol（PPTP），http://www.ietf.org/rfc/rfc2637.txt
2）IP Security Protocol（ipsec）Charter，http://www.ietf.org/html.charters/ipsec-charter.html
3）Fluhler，S. et.al.: Weakness in the Key Scheduling Algorithm of RC4，http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf
4）Wi-Fi Protected Access（WPA），http://www.weca.net/OpenSection/protected_access.asp
5）IEEE P802.11. The Working Group for Wireless LANs，http://www.ieee802.org/11/
6）難波：7.5 限定受信，放送システム（山田宰編著），pp.176-183，コロナ社（2003）．
7）難波：4.最近のセキュリティ技術とその応用 4-1 放送，テレビジョン学会誌，Vol.47，No.2，pp.149-154（1993）．
8）電波産業会標準規格：デジタル放送におけるアクセス制御方式，ARIB STD-B25．
9）映像情報メディア学会編:デジタル放送ハンドブック，第8編「限定受信・著作権保護方式」，第10編「サーバ型放送」．

（平成16年9月30日受付）