

技術基礎講座

【GE-PON技術】

- 第1回 PONとは
- 第2回 IEEE802.3ah標準規格
- 第3回 DBA機能
- 第4回 GE-PONのシステム化機能

第5回 今後の標準化

本連載の最終回として、GE-PONシステムに関係するいくつかの標準化動向について解説します。これらの標準化仕様を採用することにより、GE-PONシステムの相互接続性の向上が図れることが期待されています。

GE-PONシステムとIEEE802.3ah

前回説明したとおり、GE-PONシステム⁽¹⁾ではIEEE802.3ah標準化機能以外にも、お客さまが契約ユーザであるか否かを識別する認証機能、下りフレームを他ユーザが解読できないようにする暗号化機能、広域ネットワークに対しても迅速に故障検出・対処可能な保守機能といった通信サービス提供に不可欠な機能等を搭載する必要があります⁽²⁾。これらの機能はIEEE802.3ahの中には含まれておらず、通信事業者または装置ベンダ各社がそれぞれの独自仕様で補っている状態です。

もちろん、これら独自仕様は各通信事業者のサービスの差別化としてとらえることもできます。しかし、機能によっては独自仕様のために相互接続（異なる装置ベンダの装置どうしの接続）ができないこととなります。相互接続性を確保することは、端末を開発するベンダにとっては、機器開発が容易になるというメリットがあります。また通信事業者にとっては、異なるベンダの装置を組み合わせるというメリットがあります。このため、いくつかの機能については、IEEE802.3ahとは異なる標準化作業が進められています。

ここでは、これら標準化作業の動向およびGE-PONの相互接続に向けた動向について説明します。

暗号化標準のIEEE802.1AE

GE-PONでは下り信号〔OLT（Optical Line Terminal）ONU（Optical Network Unit）の信号〕は全く同一のものが放送形式で全ONUに到達するため、無線LANのようにユーザデータを保護するための暗号化機能が必要となります。

GE-PONの暗号化については、IEEE802.3ahの標準化に含めるべきかどうかの議論がありましたが、最終的に上位レイヤであるIEEE802.1にて規定することとなりました。この結果、2002年11月にLink Security Study Groupが発足し、IEEE802.1AE（正式名称は、「Media Access Control（MAC）Security」）として現在活動しています。本年7月現在で、ドラフト3.5が制定されています。

IEEE802.1AEは、イーサネットのセキュリティを強化するためMAC Security（MACsec）と呼ばれています。MACsecは、GE-PONだけを対象としたものではなく、イーサネットシステム全般に適用することが可能です。MACsecは図1のとおり、IEEE802.3とブリッジ機能やVLAN（Virtual Local Area Network）機能を規定したIEEE802.1D/Qの中間に位置します。

IEEE802.1AEで規定されているのは、実際に暗号化・復号化を実施する暗号化モジュールとの信号のやり

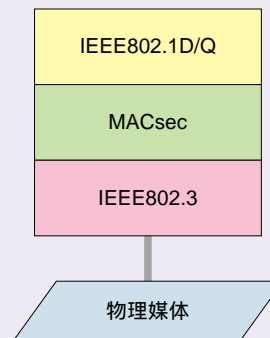


図1 MACsecのレイヤ構成

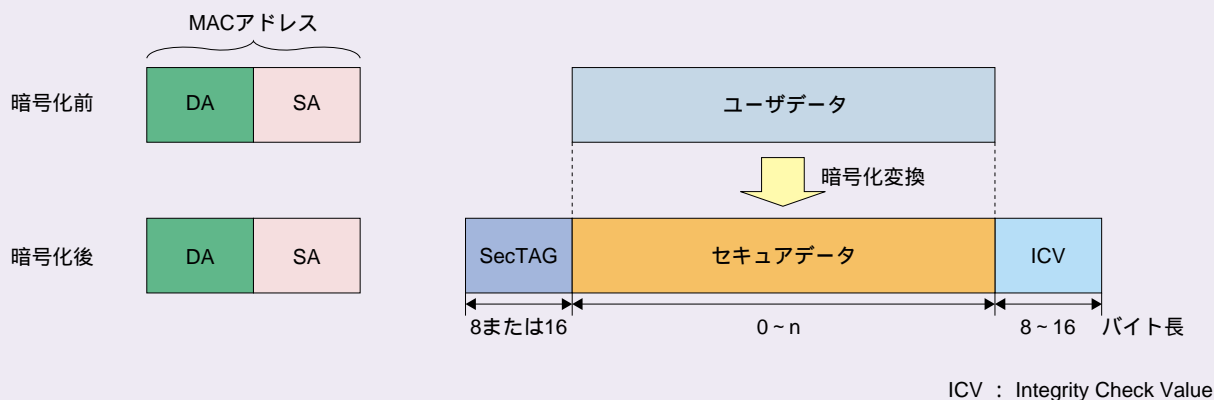


図2 MACsecのフレームフォーマット

取り，暗号化時のフレームフォーマットおよび上位レイヤ・下位レイヤとの信号の受け渡し等です．暗号化モジュールで使用する暗号化アルゴリズムは本標準内では規定せず，既存のアルゴリズムの中から選択することとなります．実装する暗号化アルゴリズムについてはまだ未定ですが，デフォルトアルゴリズムだけGCM-AES-128 (FIPS197として規定された暗号化アルゴリズムの1つ)に決定しています．

暗号化フレームフォーマットを図2に記載します．暗号化はユーザデータだけに実施され，MACヘッダ部分〔DA (Destination Address)，SA (Secure Address)，Ether Type〕にはかけられません．MACsecで使用する情報は，ユーザデータの前に付加されるSecTAG (MAC Security tag)に収容されます．SecTAGには，MACsecフレームであることを識別するためのEther Typeフィールド，パケット番号，暗号化フレームが属しているチャンネル情報 (SCI) および各種の暗号化制御情報が入っています．MACsecでは，各端末もしくは端末内のポート間にSC (Secure Channel) という暗号化用のトンネルをつくり，この間で共通鍵を用いた暗号化を実施します．なおMACsecでは，GE-PONにおけるブロードキャスト通信 (すべてのONUにて受信可能な信号) に対応したSCも規定されています．このSCでは，すべてのONUが同じ暗号鍵を使用することになります．

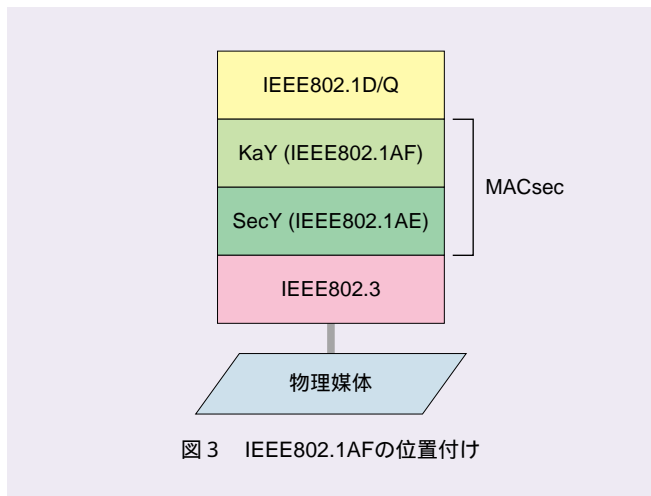
IEEE802.1AEは図2のとおり，従来のイーサネットフレームに付加情報を加えるかたちとなり，最大2000バイトまでイーサネットフレームを拡張する必要があります．従来のイーサネットフレームは1522バイトが最大であるため，既存の装置との整合性が1つの問題となります．このため，すでに各装置ベンダが実装している暗号化方式をデファクト化する動きもあります．

IEEE802.1AEに関するさらに詳しい情報は<http://www.ieee802.org/1/pages/802.1ae.html>に記載されています．標準化作業はまだしばらくかかりそうです．

認証標準のIEEE802.1AF

IEEE802.1AEの暗号化を実施するために必要な認証および鍵交換方法を規定しているのがIEEE802.1AFです．正式名称は，「Authenticated Key Agreement for Media Access Control (MAC) Security」です．IEEE802.1AFは認証規格であるIEEE802.1Xを拡張するかたちで規格化されており，最終的にはIEEE802.1Xに追加される予定です．本年7月現在で，ドラフト0.2が制定されていますが，まだ未決定の部分がかかり残っています．

IEEE802.1AFのレイヤは図3のようになります．IEEE802.1AEで説明したMACsecは，正確には2つのモジュールから構成されます．SecY (Mac Security Entity) は暗号化を実施するモジュールであり，



IEEE802.1AEはこのSecYについて規定しています。この上位に、IEEE802.1AFで規定されているKaY (Mac Security Key Agreement Entity) が位置しており、SecYで使用する暗号鍵の交換をつかさどります。

残念ながら、今現在は暗号鍵の交換方法の詳細については未規定です。

IEEE802.1AFに関するさらに詳しい情報は<http://www.ieee802.org/1/pages/802.1af.html>に記載されています。標準化作業はまだしばらくかかりそうです。

GE-PONのMIB

MIBとはManagement Information Baseの略で、SNMP (Simple Network Management Protocol) で管理されるネットワーク機器が、自分の状態を外部に知らせるために公開する情報のことです。

GE-PONのMIBについては、IEEE802.3ahの30章にて、GE-PONの各層 (MPCP, OAM, RS/PCS, PMD) ごとに規定されています。

この規定を引用するかたちで、インターネットの標準化団体であるIETF (Internet Engineering Task Force) 中のEthernet Interfaces and Hub MIBワーキンググループ (hubmib) でもMIBの規定が進んでいます。hubmibは、IEEE802.3標準に準拠した機器、MAU (Media Access Unit)、インタフェースを持つMIBを規定するワーキンググループです。今回も、IEEE802.3ahの標準化に合わせてMIBの規定を行って

います。

これらはdraft-ietf-hubmib-efm-epon-mib-03およびdraft-ietf-hubmib-efm-mib-03としてInternet-Draftとして公開されています。

Internet-draftをご覧になりたい場合は、<http://www.ietf.org/internet-drafts/draft-ietf-hubmib-efm-epon-mib-03.txt>および<http://www.ietf.org/internet-drafts/draft-ietf-hubmib-efm-mib-03.txt>にたてることが可能です。

ここまで述べてきた標準化動向をまとめると図4のようになります。ここで、黄色で示した機能が現在、標準化もしくは一部標準化が進んでいる機能です。ここでも分かるとおり、これらの標準化により、GE-PONシステムの大部分を標準化機能とすることが可能となります。

相互接続に向けた取り組み

ここまで何度か述べてきたように、標準化の目的は異なる装置ベンダの装置どうしを接続可能とすることです。これを相互接続といいます。このおかげで、例えばLANの実質的な標準となっている10BASE-Tや100BASE-TXのインタフェースを持ったNIC (Network Interface Card) とHUB等を、ベンダを気にすることなく接続することができるのです。

しかしながら、標準化に準拠していれば確実に相互接続が可能であるかという点、必ずしもそうではありません。例えば、100BASE-TXのインタフェースを持った機器どうしても、いまだに相性によって接続がうまくいかないものもあります。これは、標準化に規定されていることが、必ずしもすべてではないことや、規定の解釈による差分、測定方法が完全には確立されていないことなどが起因しています。

これらの相互接続性の不具合を解消する方法として、実際に異なる機器を共同で接続して検証したり、基準となる試験サイトをつくり、そこで試験を実施する方法があります。

GE-PONに関しては、University of New Hampshire内のInter-Operability Laboratory (UNH-IOL) にて、この試みが始まっています。ここでは、持ち込まれたGE-PON装置を決められた試験要項に基づいて

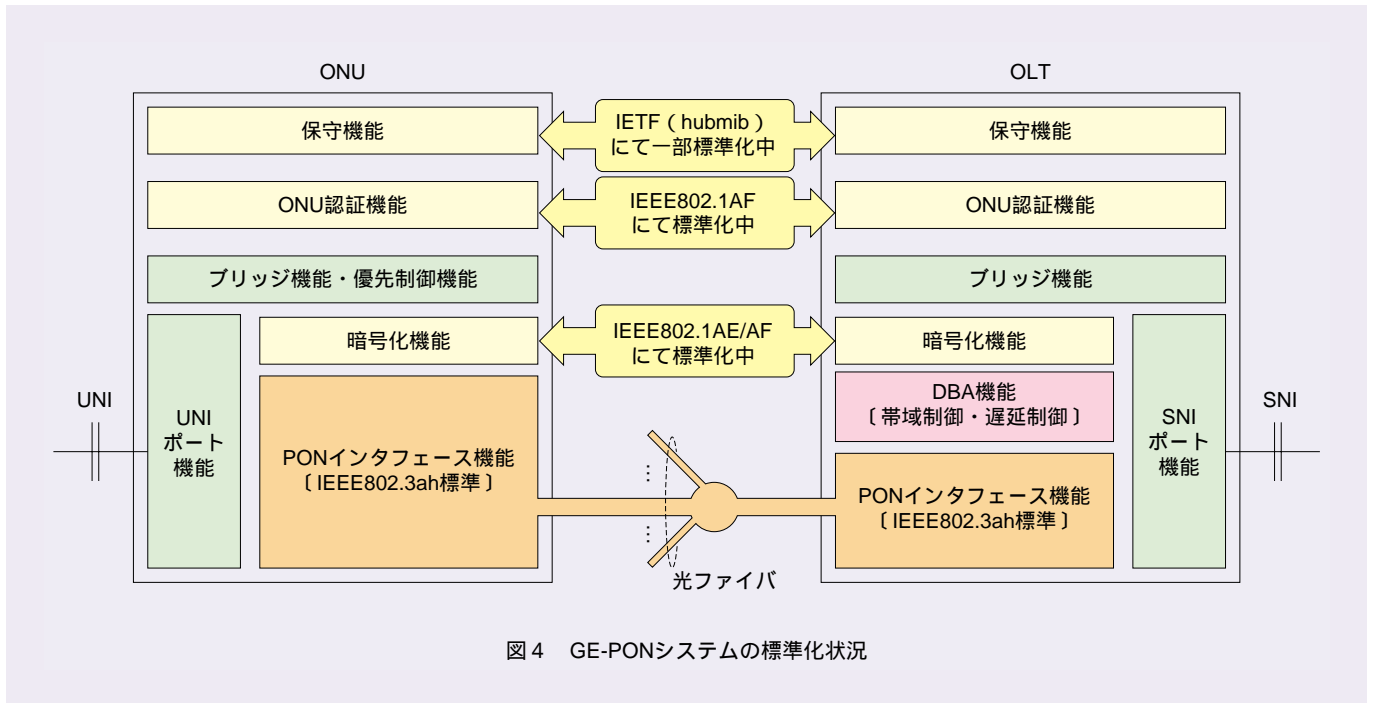


図4 GE-PONシステムの標準化状況

試験し、その結果が公開されることとなります。UNH-IOLでは、このほかにも10BASE-T, Fast Ethernet, Gigabit Ethernet等の相互接続試験も実施しています。

さらに詳しい情報が必要であれば、<http://www.iol.unh.edu/consortiums/efm/>にてご覧いただけます。

GE-PON推進に向けた取り組み

標準化とは直接関係ありませんが、GE-PONのさらなる発展のために、IEEE内にオンラインのコミュニティとしてEPON Forumがあります。ここでは、GE-PONに関するニュース、論文、特許などの情報が交換されています。詳しくは<https://www.ieeecommunities.org/epon/>にて確認してください。

GE-PONの今後

5回にわたりGE-PONについて解説してきた本講座も今回で終わりです。GE-PONはIEEE802.3ahにて昨年6月に標準化された新しい技術です。高速通信を低コストで実現することが期待されていますが、相互接続を考えると第4回、第5回でみてきたように検討の余地がま

だ残っています。今後のGE-PONのさらなる発展には、これらの検討課題を解決していく必要があります。

参考文献

- (1) 落合・立田・藤本・田中・吉原・太田・三鬼：“Gigabit Ethernet-PON (GE-PON) システムの開発,” NTT技術ジャーナル, Vol.17, No.3, pp.75-80, 2005.
- (2) “技術基礎講座 GE-PON技術 第4回 GE-PONのシステム化機能,” NTT技術ジャーナル, Vol.17, No.11, pp.59-61, 2005.

問い合わせ先

NTTアクセスサービスシステム研究所
 第一推進プロジェクト IPアクセス推進DP
 TEL 043-211-3290
 FAX 043-211-8875
 E-mail tatsuta@ansl.ntt.co.jp

このコーナーで取り上げて欲しいテーマをE-mailで編集部までお寄せください。
 (社)電気通信協会内 NTT技術誌事務局 E-mail jrr@tta.or.jp