相互認証と暗号化処理を統合するスマートメータ用統合鍵管理技術 AMSO$_{TM}$

AMSO$_{TM}$ Unified Key Management Mechanism Integrating Authentication and Encryption for Smart Meters

神田　充　　大場　義洋　　田中　康之
■ KANDA Mitsuru　■ OHBA Yoshihiro　■ TANAKA Yasuyuki

スマートグリッドを構成する重要な要素の一つであるAMI（Advanced Metering Infrastructure）システムでは，双方向通信機能を持ったスマートメータと呼ばれる高機能なメータが必要になる。

東芝は，スマートメータに必要とされる通信セキュリティを強化する統合鍵管理技術 AMSO$_{TM}$（Advanced Meter Sign-On）を開発した。AMSO$_{TM}$は，スマートメータ上で実行される複数の通信アプリケーション個々に必要な相互認証処理と暗号化処理の鍵管理を統合する。これによって組込み機器のため処理能力に制約があるスマートメータでの通信セキュリティの強化を実現し，更に将来登場するスマートメータ用通信アプリケーションへも適用できるようになった。

An advanced metering infrastructure (AMI) system is one of the important elements of a smart grid system. In an AMI system, so-called smart meters with communication functionality are required instead of conventional electrical meters.

Toshiba has developed AMSO$_{TM}$ (advanced meter sign-on), a unified key management mechanism for smart meters, which integrates the key management functions of authentication, encryption, and integrity for all communication applications on smart meters. It can be used for future communication applications for smart meters as well as for strengthening the security of smart meters.

1　まえがき

AMI（Advanced Metering Infrastructure）システムは，双方向通信機能を備えたスマートメータと呼ばれる高機能なメータを中心に構築される。AMIシステムでは，短い時間幅ごとの計量や，遠隔自動検針，電力の見える化，需要家の協力による電力需給制御を行うデマンドレスポンスなどが実現される。スマートメータには，従来の物理的な機器の改ざん防止措置に加えて，通信における認証処理及び，暗号化など通信データの保護処理が必要になる。

東芝は，これら2種類の処理に必要な鍵管理を統合したスマートメータ用統合鍵管理技術AMSO$_{TM}$（Advanced Meter Sign-On）を開発した。

ここでは，AMSO$_{TM}$を構成する技術及びその効果について述べる。

2　スマートメータの通信セキュリティ

AMIシステムの構成例を**図1**に示す。

AMIシステムは，需要家に設置されるスマートメータ，複数のスマートメータからのデータを集約するコンセントレータ，電力会社側に設置されスマートメータの計量データを収集するMDMS（Meter Data Management System）サーバ，デマンドレスポンスを管理するDRMS（Demand Response Management System）サーバ，及びネットワークアクセス認証サーバから成る。スマートメータは，コンセントレータ及び広域通信ネットワークを介して電力会社側の複数のサーバと接続される。ただし実際には，電力会社側のサーバが一つの機器に集約される場合や，コンセントレータが省略される場合がある。

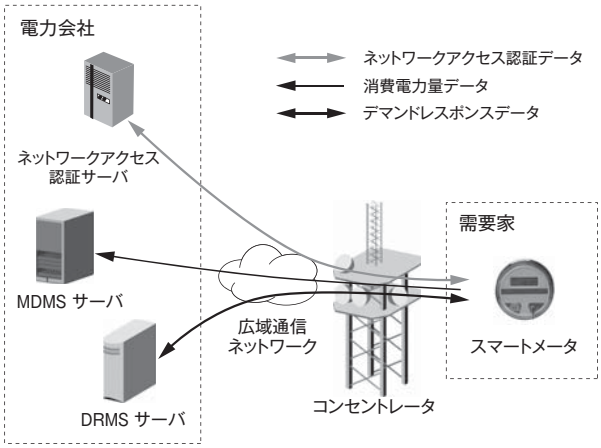

図1. AMIシステムの構成例 ― AMIシステムでは，需要家に設置されたスマートメータと，電力会社側に設置された各種サーバが広域ネットワークを介して接続される。

Example of configuration of AMI system

スマートグリッドのセキュリティ要件をまとめたNIST IR 7628（米国国立標準技術研究所 Interagency Report 7628）ドラフト[(1)]では，AMIシステムの通信について次のようなセキュリティの確保が求められている。

(1)　ネットワークアクセス認証　　スマートメータなどの機器が接続されるネットワークで，無関係な機器が無断で接続されるのを防止するため，機器がネットワークに接続される際には認証を行う。

(2)　スマートメータと電力会社側サーバの間の安全な通信　広域通信ネットワークを経由してスマートメータと電力会社側サーバの間で通信が行われるため，暗号化などによって盗聴や改ざんを防止する。

(3)　認証や暗号通信などで使用する鍵の動的な更新　通信内容を暗号化しても，長期間にわたって同じ暗号鍵を使い続けた場合，鍵の漏えいなどによって通信内容が盗聴されるおそれがある。一定期間ごとに鍵の動的な更新など（以下，鍵管理と呼ぶ）を行って，これを防止する。

3　AMSO$_{TM}$のコンセプトとアーキテクチャ

ここでは，前述のAMIシステムの通信セキュリティ要件を満たし，更に鍵管理に関する処理負荷を低減できるAMSO$_{TM}$のコンセプトと，実際の通信プロトコルを用いたアーキテクチャについて述べる。

3.1　AMSO$_{TM}$のコンセプト

AMSO$_{TM}$のコンセプトは，任意の通信レイヤに属する任意の通信プロトコルに対して，UKMF（Unified Key Management Function）と呼ぶ単一の鍵管理機能を用いることである。AMSO$_{TM}$は，UKMFの適用範囲によって，完全統合モデルと部分統合モデルの二つに分けられる。

完全統合モデルと部分統合モデルの例を，アプリケーションレイヤとデータリンクレイヤの二つの通信レイヤの鍵管理を対象として**図2**に示す。完全統合モデルと部分統合モデルの概要は，次のとおりである。

(1)　完全統合モデル　　通信レイヤを問わず，暗号処理を必要とする通信プロトコルすべてに対し，単一のUKMFによって鍵管理するモデルである。

(2)　部分統合モデル　　一部の通信プロトコルについてUKMFを使用しないモデルで，対象システムの要求条件や制約から，UKMFを適用できない通信プロトコルが存在する場合に用いられる。部分統合モデル中のUKMFを適用できない通信プロトコルでは，各通信プロトコル固有の鍵管理機能であるDKMF（Dedicated Key Management Function）が用いられる。

AMSO$_{TM}$では，まず端末上のUKMFと，端末が接続されるネットワーク上のサーバのUKMFとの間で相互認証を行い，認証が成功すると有期限のマスタ鍵が生成される。これによって，各通信プロトコルに対する暗号鍵の生成，保持，更新，削除といった鍵管理に関する一連のオペレーションを安全に実行できる。

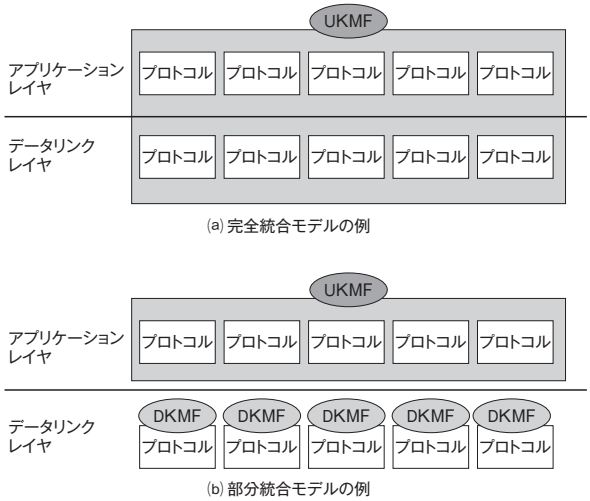

図2．AMSOのコンセプト — AMSO$_{TM}$には，UKMFの管理する範囲によって，完全統合モデルと部分統合モデルの二つのモデルがある。

Concept of AMSO$_{TM}$

従来の鍵管理では暗号鍵を必要とする通信プロトコルそれぞれに対して個別に行っていた相互認証が，AMSO$_{TM}$を用いることで1回で済む。この結果，スマートメータの鍵管理の処理負荷が低減され，更に単一の鍵管理モジュールを用いることでコードサイズも低減される。

また，電力量計量アプリケーションプロトコルの米国標準規格であるANSI C12.22（米国規格協会規格C12.22）[2]で規定されているような，暗号鍵の自動生成機構を持たないアプリケーションプロトコルに対しても暗号鍵の動的な生成及び更新の仕組みを提供できる。

AMSO$_{TM}$では，UKMF間の相互認証はどのような形態をとってもよい。例えば，端末が通信ネットワークに接続される際に実行されるネットワークアクセス認証でもよいし，アプリケーションレベルの認証であってもよい。多くの場合，端末が最初に通信ネットワークに接続される時点，つまりネットワークアクセス認証の形態をとる。

AMSO$_{TM}$は，通信プロトコルの暗号鍵を複数生成する認証フレームワークを用いて実現できる。当社は実用化の観点から，Wi-Fi®（注1）やWiMAX（注2）で広く普及している認証フレームワークであるEAP（Extensible Authentication Protocol）[3]を相互認証に用いてAMSO$_{TM}$のアーキテクチャを構築している。

3.2　AMSO$_{TM}$のアーキテクチャ

EAPを用いたAMSO$_{TM}$のアーキテクチャを**図3**に示す。

まず，端末のEAPピアとネットワーク上のEAPオーセンティケータ／サーバとの間でEAPを用いた相互認証が行われ（①），

（注1）　Wi-Fiは，米国Wi-Fi Allianceの登録商標。
（注2）　WiMAXは，WiMAX Forumの登録商標。

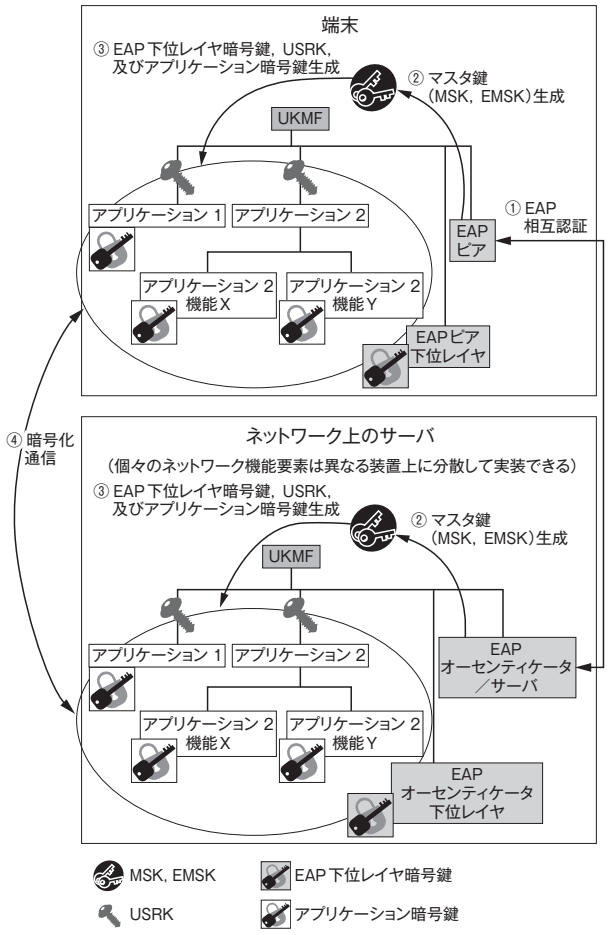

図3. EAPを用いたAMSO$_{TM}$のモデル — 端末とネットワークとの間でEAP相互認証されると，それぞれでマスタ鍵が生成され，UKMFへ渡されてアプリケーション暗号鍵が生成される。

AMSO$_{TM}$ model using Extensible Authentication Protocol (EAP)

マスタ鍵が生成される(②)。EAPのマスタ鍵には，MSK(Master Session Key)とEMSK(Extended Master Session Key)の2種類がある。生成されたマスタ鍵は，端末ではEAPピアから端末のUKMFへ，ネットワーク上ではEAPオーセンティケータ／サーバからネットワーク上のUKMFへ，それぞれ渡される。端末及びネットワーク上のUKMFは，下位レイヤ暗号鍵をEAPピア下位レイヤ及びEAPオーセンティケータ下位レイヤにそれぞれ渡すとともに，各アプリケーションで使用される鍵をEMSKから生成し，各アプリケーションに渡す(③)。これによって，端末からネットワークを経由したサーバとの暗号化通信が可能になる(④)。

各アプリケーションの鍵は，USRK(Usage Specific Root Key)としてEAPに関係する鍵の導出方法を規定するRFC 5295[注3)(4)]に定義される鍵導出関数KDF(Key Derivation Function)を用いて生成する。

図3のアプリケーション2のように，異なる暗号鍵を用いる複数の機能を持ったアプリケーションに対しては，そのアプリケーションのUSRKから各機能に対応する子供鍵が生成される。例えば，ANSI C12.22では，電力量計量アプリケーションの中で，スマートメータ登録のためのレジストレーションサービスと，スマートメータの通信先ネットワークアドレスを得るためのリゾルブサービスは，二つの異なる機能として扱われ，異なる暗号鍵が使用される。

実際のアーキテクチャには，次の二つがある。

(1) 第一のアーキテクチャ　EAPをネットワークアクセス認証とアプリケーションレベル認証の両方に使用するアーキテクチャである。このとき，ネットワークアクセス認証のEAPはデータリンクレイヤ又はネットワークレイヤのいずれかで行われる。ネットワークレイヤでのネットワークアクセス認証及びアプリケーションレベル認証のEAPの実行には，ネットワークアクセス認証プロトコルとして後述するRFC5191[(5)]を使用する。データリンクレイヤでのネットワークアクセス認証のEAP実行には，各データリンクプロトコル固有のネットワークアクセス認証プロトコルを使用する。このアーキテクチャは図2(a)の完全統合モデルに属する。

(2) 第二のアーキテクチャ　EAPをアプリケーションレベル認証だけに使用するアーキテクチャである。このとき，アプリケーションレベル認証のEAPの実行には後述するRFC5191を使用する。この場合，ネットワークアクセス認証はUKMFとは無関係に行われるため，このアーキテクチャは図2(b)の部分統合モデルに属する。

3.3 RFC5191の概要

RFC5191は，当社が中心になって策定を行ったインターネット標準のネットワークアクセス認証プロトコルであり，アプリケーションレベル認証にも応用可能である。RFC5191は，**図4**

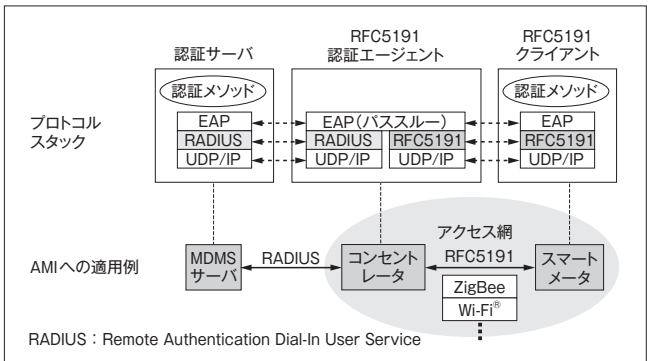

図4. RFC5191の概要 — UDP/IP上で動作するため，ネットワークアクセスの種別やトポロジーに依存しない汎用性の高いプロトコルである。

Outline of RFC5191 Protocol for Carrying Authentication for Network Access (PANA)

(注3) RFC(Request for Comment)は，インターネットについての技術標準を定める団体であるIETF(Internet Engineering Task Force)が発行する公式文書の一つ。

に示すように，UDP（User Datagram Protocol）/IP（Internet Protocol）上で動作するため，ネットワークアクセスの種別やトポロジーに依存しない非常に汎用的なプロトコルである。

RFC5191は，経済産業省が定めるスマートグリッド重要国際標準化注力アイテム26の一つに選ばれている。また，家庭及びビルディングオートメーション用エネルギー制御の標準プロファイルとしてZigBee Allianceで策定中のZigBee(注4) SEP2.0（Smart Energy Profile version 2.0）では，RFC5191を標準ネットワークアクセス認証プロトコルとする検討が進んでいる。

4　AMSO$_{TM}$のAMIシステムへの適用方法

ここではAMSO$_{TM}$適用方法の例を，図1に示すAMIシステム構成例を用いて説明する。

AMIシステム上で遠隔検針とデマンドレスポンスを行うためには，スマートメータが広域通信ネットワークに接続される必要がある。このため，スマートメータが起動すると，スマートメータとネットワークアクセス認証サーバの間でネットワークアクセス認証を行い，スマートメータが広域通信ネットワークに接続される。EAPを用いる場合，スマートメータがEAPピア，ネットワークアクセス認証サーバがEAPオーセンティケータ／サーバとなる。

スマートメータが広域通信ネットワークに接続された後，MDMSサーバとスマートメータの間で遠隔自動検針アプリケーションを実行できる。また，DRMSサーバとスマートメータの間では，デマンドレスポンスアプリケーションも実行できるようになる。AMIシステムのネットワークアクセス認証にEAPが使用できる場合，AMSO$_{TM}$の第一のアーキテクチャをAMIシステムに適用する。AMIシステムのネットワークアクセス認証にEAPが使用できない場合は第二のアーキテクチャをAMIシステムに適用し，ネットワークアクセス認証成功後にRFC5191を用いてEAPを実行する。

AMIシステムにAMSO$_{TM}$の第一のアーキテクチャを適用した場合について，以下に述べる。

まず，スマートメータはRFC5191によってネットワークアクセス認証を実行する。遠隔自動検針アプリケーションとデマンドレスポンスアプリケーションのデータは広域通信ネットワーク上で安全に配送される必要があるため，次に，AMSO$_{TM}$によって各アプリケーション用の暗号鍵を生成する。スマートメータにおけるアプリケーション用の暗号鍵の生成手順を**図5**に示す。

認証クライアント（EAPピア）がEMSKを生成し，EMSKをUKMFに通知する。UKMFはEMSKからUSRKを生成し，USRKから遠隔自動検針アプリケーションとデマンドレスポンスアプリケーションの暗号鍵を生成する。それぞれの鍵はUKMFから遠隔自動検針アプリケーションとデマンドレスポンスアプリケーションに通知される。図5に示すように，遠隔自動検針アプリケーションとデマンドレスポンスアプリケーションはそれぞれ別の暗号鍵を持つ。

スマートメータと同様に，電力会社のMDMSサーバとDRMSサーバも暗号鍵を生成する。電力会社内のサーバ間における暗号鍵の通知手順を**図6**に示す。

はじめに，ネットワークアクセス認証サーバ（EAPオーセンティケータ／サーバ）がEMSKを生成し，EMSKをUKMFに通知する。UKMFはEMSKからUSRKを生成し，USRKから遠隔自動検針アプリケーションとデマンドレスポンスアプリ

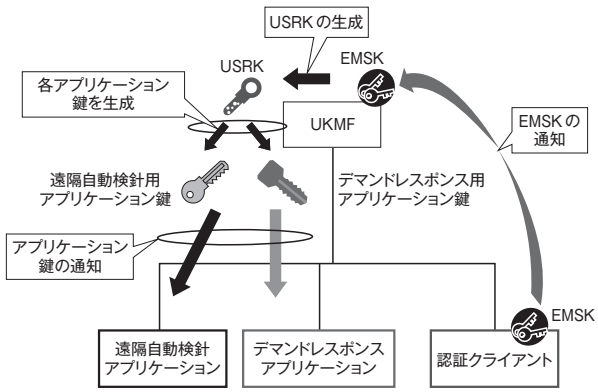

図5．スマートメータにおける暗号鍵の生成 — 各アプリケーションのデータは広域通信ネットワークで安全に配送される必要があるため，AMSO$_{TM}$によって暗号鍵が生成される。

Key generation on smart meters

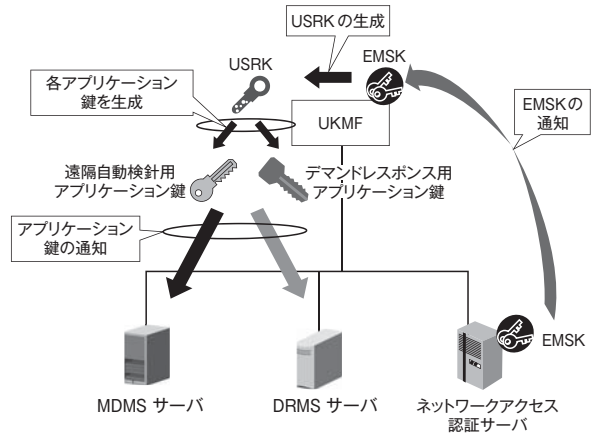

図6．電力会社内のサーバによる暗号鍵の生成 — スマートメータと同様に，電力会社のMDMSサーバとDRMSサーバも暗号鍵を生成する。

Key generation on utilities' servers

（注4）　ZigBeeは，ZigBee Allianceの米国及びその他の国における登録商標。

ケーションの暗号鍵を生成する。それぞれの鍵はUKMFからネットワークアクセス認証サーバ，MDMSサーバ，及びDRMSサーバに通知される。

AMSO$_{TM}$を使わずに遠隔検針やデマンドレスポンスの暗号鍵を確立する場合には，それぞれのアプリケーションごとに暗号鍵の交換手続きがスマートメータと各サーバの間で行われる。組込み機器であるスマートメータがアプリケーションごとに暗号鍵を交換するのは計算資源の制約上好ましくない。AMSO$_{TM}$を使うとアプリケーションが使用する暗号鍵の交換手続きが不要になり，AMIシステム上のアプリケーションの種類が増えても鍵交換手続きの回数は変わらない。このように，AMSO$_{TM}$はスマートメータなどの組込み機器が複数の暗号鍵を使うAMIシステムのようなシステムに有効である。

5　あとがき

AMSO$_{TM}$は，スマートグリッドのAMIシステムにおける通信セキュリティを単に確保するだけでなく，鍵管理の処理負荷とコードサイズを低減する。また，スマートメータと電力会社など通信先との間で複数のアプリケーションの鍵管理を一度の動作で統合的に扱うことができる。

当社は，今後出現する通信セキュリティを必要とする様々なAMIシステム用のアプリケーションに対してもAMSO$_{TM}$を適用して，スマートメータの高度化を推進していく。

文　献

(1) NIST. "NIST IR-7628 Smart Grid Cyber Security Strategy and Requirements" (DRAFT). NIST Homepage. <http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628_2nd-public-draft.pdf>, (参照2010-08-03).

(2) ANSI C12.22 : 2008. American National Standard Protocol Specification For Interfacing to Data Communication Networks.

(3) Aboba, B., et al. "RFC3748 Extensible Authentication Protocol (EAP)". The Internet Engineering Task Force (IETF) Homepage. <http://www.ietf.org/rfc/rfc3748.txt>, (参照2010-08-03).

(4) Salowey, J., et al. "RFC5295 Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK)". The Internet Engineering Task Force (IETF) Homepage. <http://www.ietf.org/rfc/rfc5295.txt>, (参照2010-08-03).

(5) Forsberg, D., et al. "RFC5191 Protocol for Carrying Authentication for Network Access (PANA)". The Internet Engineering Task Force (IETF) Homepage. <http://www.ietf.org/rfc/rfc5191.txt>, (参照2010-08-03).

神田　　充　KANDA Mitsuru
研究開発センター　ネットワークシステムラボラトリー研究主務。IPv6やIPsecなどのインターネットプロトコルの研究・開発に従事。
Network System Lab.

大場　義洋　OHBA Yoshihiro, Ph.D.
研究開発センター　ネットワークシステムラボラトリー主任研究員，工博。インターネットのセキュリティ，及びモバイル関連の標準化と研究・開発に従事。IEEE会員。
Network System Lab.

田中　康之　TANAKA Yasuyuki
研究開発センター　ネットワークシステムラボラトリー。組込み用TCP/IPスタックの研究・開発に従事。
Network System Lab.