統合鍵管理技術AMSO$_{TM}$を搭載したANSI準拠スマートメータ

ANSI-Compliant Secure Smart Meter Incorporating AMSO$_{TM}$ Unified Key Management Mechanism

田中　康之　　池田　泰三
■TANAKA Yasuyuki　■IKEDA Taizo

電力用スマートメータ（以下，スマートメータと記す）は，プライバシー情報や系統制御情報を扱うため，通信セキュリティを確保しなければならない。

東芝と東光東芝メーターシステムズ（株）は，統合鍵管理技術AMSO$_{TM}$（Advanced Meter Sign-On）を搭載した北米向けスマートメータを開発した。AMSO$_{TM}$によって，ANSI C12.22（米国規格協会規格 C12.22）で使用する暗号鍵の自動生成及び自動更新ができるようになり，通信セキュリティ強度が向上した。当社は，この北米向けスマートメータを独立行政法人 新エネルギー・産業技術総合開発機構（NEDO）が実施する米国ニューメキシコ州での日米スマートグリッド実証で活用する。

There is a strong need for a secure system for smart meter communications in order to protect both consumers' private information and grid management information.

Toshiba and Toshiba Toko Meter Systems Co., Ltd. have jointly developed a secure smart meter incorporating the AMSO$_{TM}$ (advanced meter sign-on) unified key management mechanism for the North American market. AMSO$_{TM}$ strengthens the security of smart meters by automatically supplying and updating encryption keys based on the C12.22 standard of the American National Standards Institute (ANSI). This smart meter will be used in a Japan-U.S. collaborative smart grid demonstration project in New Mexico that is being implemented by the New Energy and Industrial Technology Development Organization (NEDO).

1　まえがき

スマートメータには，従来の物理的な不正行為の防止装置に加えて，通信に際して認証処理や暗号化などの通信データの保護処理が必要になる。しかし，米国のスマートメータ標準通信規格には，通信データ保護機能はあるものの，データ保護に使用する暗号鍵の自動生成機能や自動更新機能がなく，通信セキュリティ確保の観点から課題があると考えられる。

そこで，東芝と東光東芝メーターシステムズ（株）が開発した北米向けスマートメータには，統合鍵管理技術AMSO$_{TM}$[(1)]を搭載した。AMSO$_{TM}$によって暗号鍵の自動生成や自動更新ができるようになり，通信セキュリティが強化される。ここでは，このスマートメータの特長について述べる。

2　スマートメータの通信セキュリティ要件とその課題

スマートメータは，スマートコミュニティの中で電力会社と需要家をつなぐ役割を果たす。スマートメータと電力会社のサーバが行う双方向通信の概要を**図1**に示す。スマートメータは広域通信ネットワークを介して電力会社のサーバに接続され，スマートメータが計測した電力量データの送信や，電力会社から発行されたデマンドレスポンス信号の受信を行う。

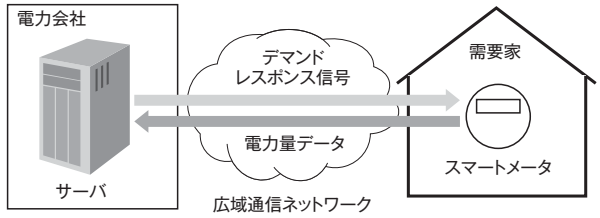

図1．スマートメータの双方向通信の概要 ― 広域通信ネットワークを介して，スマートメータは電力会社のサーバと電力量データやデマンドレスポンス信号をやり取りする。
Outline of interactive communications between smart meter and utility server

プライバシー情報である電力量データや，系統制御情報であるデマンドレスポンス情報を扱うため，スマートメータとサーバ間の通信セキュリティの確保が必須である。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）[(2)]には，スマートメータの通信について次のようなセキュリティ要件が挙げられている。

(1)　ネットワークアクセス認証　　不正な機器がネットワークに接続されるのを防ぐため，正当な機器だけが接続されるように機器認証を行う。

(2) スマートメータとサーバ間の安全な通信　広域通信ネットワーク上でやり取りされるデータの盗聴や改ざんを防止するため，データの認証や暗号化を行う。

(3) データの認証や暗号化に使用する暗号鍵の自動更新　長期間にわたって同じ暗号鍵を使用すると，暗号鍵の解読攻撃や漏えいに対する耐性が低下するため，一定期間ごとに暗号鍵を更新する。これを鍵管理機能と呼ぶ。

これらのセキュリティ要件を満たす通信セキュリティ実装の課題は，必要なセキュリティ強度を保つとともに，その実装規模や処理負荷を最小化することである。組込み機器であるスマートメータは必ずしも十分な計算処理能力を持たないため，通信セキュリティ実装の軽量化が求められる。

米国でのスマートメータとサーバ間の標準通信規格は，ANSI C12.22[3]である。ANSI C12.22にはデータの認証や暗号化を行うデータ保護機能はあるが，暗号鍵の鍵管理機能の仕様がない。また，ネットワークアクセス認証機能の仕様もない。そのため，北米向けスマートメータにはANSI C12.22のデータ保護機能の実装に加えて，ANSI C12.22で使用する暗号鍵の鍵管理機能とネットワークアクセス認証機能を実装しなければならない。

3　ANSI C12.22向けAMSO$_{TM}$の実装

前述の通信セキュリティ実装の課題に対して，当社はAMSO$_{TM}$を開発した。AMSO$_{TM}$では，UKMF（Unified Key Management Function）と呼ばれる鍵管理機能により，独自に鍵管理機能を持たない通信プロトコルの暗号鍵の自動生成や自動更新を実現できる。また，UKMFにより，鍵管理に必要な認証手続きや鍵交換手続きが統合処理されるため，実装を軽量化できる。

3.1　AMSO$_{TM}$実装の詳細

北米向けスマートメータに搭載されるAMSO$_{TM}$実装は，**表1**に示す通信プロトコルから構成される。このAMSO$_{TM}$実装では，事前に設定されたスマートメータの識別子と共有鍵（パスワード）を使い，スマートメータとサーバ間で認証処理を行う。

AMSO$_{TM}$搭載スマートメータが起動してから，電力量データの送信やデマンドレスポンス信号の受信を行うまでの処理の流れを**図2**に示す。

表1．AMSO$_{TM}$実装を構成する主な通信プロトコル
Main protocols used for AMSO$_{TM}$ implementation

RFC番号	通信プロトコル名
3748	Extensible Authentication Protocol (EAP)[4]
4764	The EAP-PSK Protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method[5]
5191	Protocol for Carrying Authentication for Network Access (PANA)[6]

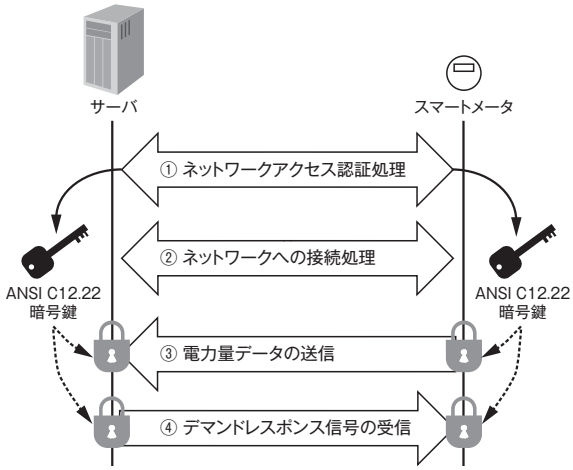

図2．AMSO$_{TM}$搭載スマートメータの処理の流れ ― 事前共有鍵による認証処理の結果，ANSI C12.22用の暗号鍵が生成される。
Processing flow of secure smart meter incorporating AMSO$_{TM}$

まず，スマートメータは，サーバとの間で事前共有鍵によるネットワークアクセス認証処理を行う（①）。起動直後のスマートメータは，ネットワークアクセス認証処理に必要な通信しか許可されない。この認証に成功すると，スマートメータとサーバはそれぞれUKMFを用いてANSI C12.22の128ビットの暗号鍵を生成する。次に，スマートメータは，ネットワークへの接続処理を行う（②）。これ以降，ANSI C12.22による電力量データの送信（③）やデマンドレスポンス信号の受信（④）が可能になる。電力量データやデマンドレスポンスデータはANSI C12.22のデータ保護仕様に基づき，AES（Advanced Encryption Standard）暗号により保護される。

一度認証が成功してから，スマートメータがネットワーク接続を継続できる期間には制限があるため，スマートメータが接続を維持するためには定期的に再認証処理を行わなければならない。再認証処理では，図2の①と同様の事前共有鍵による認証が行われ，認証が成功するたびに，スマートメータとサーバは新しいANSI C12.22暗号鍵を生成する。

このように，定期的に認証が行われ，認証が成功するたびにANSI C12.22暗号鍵が生成されていく。一方で，それぞれのANSI C12.22暗号鍵は有効期限を持つため，有効期限切れの暗号鍵は自動的に破棄されていく。これら暗号鍵の生成と破棄を組み合わせることで，ANSI C12.22暗号鍵の自動更新が実現され，クライアントとサーバは同じANSI C12.22暗号鍵を使い続けることはなくなる。

AMSO$_{TM}$を使用しない場合のスマートメータの処理例を**図3**に示す。AMSO$_{TM}$を使用した図2の処理では，図3の②’で示すANSI C12.22暗号鍵の鍵交換処理が，ネットワークアクセス認証処理に統合されている。これにより，スマートメータの処理負荷や実装規模が低減される。

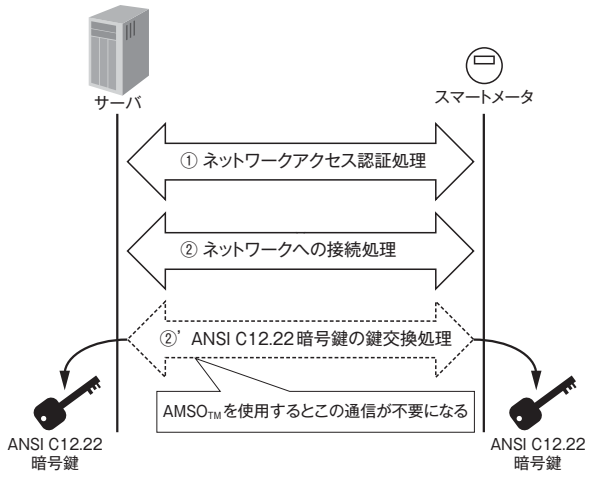

図3. AMSO™を使用しない場合のスマートメータの処理例 — AMSO™を使用しない場合，別途ANSI C12.22暗号鍵の鍵交換処理が必要になる。
Example of conventional processing flow of smart meter without AMSO™

3.2 AMSO™実装の特長

前述のAMSO™実装には，主に二つの特長がある。

一つ目の特長は，スマートメータ間のネットワークアクセス認証処理が，スマートメータとサーバ間の通信に使用するネットワークアクセスの種別に依存することなく実行できる点である。これは，UDP（User Datagram Protocol）/IP（Internet Protocol）上で動作するRFC(注1)5191を使用していることから得られる特長である。スマートメータのネットワークアクセスの種別としては，イーサネットや，無線LAN，無線メッシュネットワーク，PLC（Power Line Communication）などが考えられるが，いずれの場合でもAMSO™を適用できる。

二つ目の特長は，認証方式の選択に対して柔軟に対応できる点である。スマートメータとサーバ間の認証方式は，国や地域，電力会社により異なる場合がある。また，10年以上使用されるスマートメータのシステムでは，当初採用した認証方式や暗号アルゴリズムが時間とともに時代遅れになり，新しい方式への変更が必要になる場合もある。AMSO™では，認証方式の変更が容易なため，これらの場合に低コストで対応できる。例えば，前述のAMSO™実装では事前共有鍵による認証を行うが，デジタル証明書による認証が好ましい場合や，特定の暗号アルゴリズムを用いた認証を行いたい場合には，表1のRFC 4764実装だけを適切な認証方式に置き換えればよい。

このように，北米向けスマートメータに搭載するAMSO™実装は，処理負荷や実装規模の面だけでなく，通信メディアや認証方式の選択に対する柔軟性の面でもスマートメータに適していると考えられる。

（注1） RFC（Request for Comment）は，インターネットについて技術標準を定める団体IETF（Internet Engineering Task Force）が発行する公式文書の一つ。

4 AMSO™搭載北米向けスマートメータの特長

AMSO™搭載北米向けスマートメータの外観を**図4**に，主な仕様を**表2**に示す

このスマートメータのソケットタイプ2Sは，米国でもっとも一般的な定格であるが，日本の単相3線式とは異なり中性線がメータ内部に配線されないため，電圧1回路と電流2回路で計量をする。

このスマートメータの主な機能は，次のとおりである。

(1) データ保存機能により，電力使用量トレンド分析や需要予測のために，計量データを15分間隔で保存する。

(2) 時間帯別計量機能により，多様な時間帯別料金メニューに対応した計量を行う。

図4. 北米向けスマートメータ SH2E1 — 電力会社との通信に使用するイーサネット通信インタフェースのほか，インホームディスプレイとの通信に使用するIEEE 802.15.4通信インタフェース，及びスマートメータ設定用機器との接続に使用する赤外線通信インタフェースを持つ。
SH2E1 ANSI-compliant secure smart meter

表2. スマートメータの主な仕様
Main specifications of smart meter

項　目	仕　様
形名	SH2E1
相線式	単相3線式（ソケットタイプ2S）
定格	240 V　200 A　60 Hz
計測項目	積算値　：有効電力量（正，逆，正+逆，正−逆），無効電力量（遅れ，進み） ロードプロファイル：15分間隔，30日間分データ保存 デマンド　：ブロックデマンド（インターバル時間30分） 瞬時値　：有効電力，無効電力，電圧，電流，周波数，皮相電力
時間帯区分	6区分，48分割
通信インタフェース	Ethernet 10Base-T/100Base-TX（TCP/IP）：MDMS通信用 IEEE 802.15.4（2.4 GHz）：インホームディスプレイ，HEMS通信用 赤外線ポート：スマートメータの設定や保守通信用
開閉器	通信による遠隔制御可能な開閉器内蔵
準拠規格	ANSI C12.1-2008　（電力量計） ANSI C12.10-2004（電力量計構造） ANSI C12.20-2010（0.2％級及び0.5％級電力量計） ANSI C12.18-2006（赤外線通信プロトコル） ANSI C12.19-2008（データ構造） ANSI C12.22-2008（ネットワーク通信プロトコル）

TCP　：Transmission Control Protocol
MDMS：Meter Data Management System

一般論文

(3) デマンド計量機能により，最大需要電力に料金契約（デマンド契約）に対応した計量を行う。

(4) 開閉器を内蔵し，遠隔指令で電力供給の停止又は開始を行う。

スマートメータは，電力会社のサーバとの通信に使用する10BASE-T/100BASE-TXイーサネット通信インタフェースのほか，IEEE 802.15.4（電気電子技術者協会規格802.15.4）通信インタフェースと赤外線通信インタフェースを持つ。

IEEE 802.15.4通信インタフェースは，インホームディスプレイやHEMS（Home Energy Management System）などの需要家内機器との接続に使用する。需要家内接続でも，機器認証やデータの暗号化によりセキュリティを確保する。当社と東光東芝メーターシステムズ（株）が開発したインホームディスプレイの外観を**図5**に示す。このインホームディスプレイはスマートメータから電力量データを取得し，電力使用状況の見える化や電力使用量トレンドの表示などを行う。

赤外線通信インタフェースは，スマートメータ設置時の設定や保守などに使用する。スマートメータは，不正改造やいたずらなどを防止するため，全面カバーで覆われ封印されている。赤外線通信インタフェースを使うことで，スマートメータを封印したまま，スマートメータの設定や保守作業をパソコンなどの設定用機器から実施できる（**図6**）。赤外線通信インタフェースで使用する通信プロトコルは，ANSI C12.18である。スマートメータは，ユーザー名とパスワードにより赤外線通信インタフェースでの接続を制限し，不正な機器による接続を防止する。

図5．インホームディスプレイ ― スマートメータから電力量データを取得し，電力使用状況の見える化や電力使用量トレンドの表示などを行う。
In-home display

図6．赤外線通信インタフェースの接続方法 ― 赤外線通信インタフェースを使用することで，スマートメータを封印したまま，設定用機器と通信できる。
Connection method using infrared communications interface

5 あとがき

当社と東光東芝メーターシステムズ（株）は，AMSO$_{TM}$を搭載した北米向けスマートメータを開発した。AMSO$_{TM}$により，スマートメータと電力会社間の暗号通信に使用する暗号鍵を自動的に生成するとともに更新できるようになり，通信セキュリティ強度が向上した。

当社は，この北米向けスマートメータをNEDOの米国ニューメキシコ州における「スマートグリッドの日米共同実証プロジェクト」で活用する。

文 献

(1) 神田 充 他. 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$_{TM}$. 東芝レビュー. **65**, 9, 2010, p.23－27.

(2) NIST. "NIST IR 7628 Guidelines for Smart Grid Cyber Security". NIST. <http://csrc.nist.gov/publications/PubsNISTIRs.html>, (accessed 2012-07-20).

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

(4) Aboba, B. et al. "RFC 3748 Extensible Authentication Protocol (EAP)". Internet Engineering Task Force (IETF) Documents. <http://tools.ietf.org/html/rfc3748>, (accessed 2012-07-20).

(5) Bersani, F. et al. "RFC 4764 The EAP-PSK Protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method". IETF Documents. <http://tools.ietf.org/html/rfc4764>, (accessed 2012-07-20).

(6) Forsberg, D. et al. "RFC 5191 Protocol for Carrying Authentication for Network Access (PANA)". IETF Documents. <http://tools.ietf.org/html/rfc5191>, (accessed 2012-07-20).

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研究主務。インターネットのセキュリティ及び組込み機器向けプロトコルスタックの研究・開発に従事。
Network System Lab.

池田 泰三 IKEDA Taizo
東光東芝メーターシステムズ（株） 開発部 設計第一グループ主務。海外向け電力量計の設計・開発に従事。
Toshiba Toko Meter Systems Co., Ltd.