スマートグリッドにおける情報セキュリティ技術

Cybersecurity Technologies for Smart Grids

伊藤　聡　■ITO Satoshi
島田　毅　■SHIMADA Tsuyoshi
神田　充　■KANDA Mitsuru

スマートグリッドのための情報セキュリティ技術の開発や標準化への取組みが各国で進められている。スマートグリッドを大規模なサイバー フィジカルシステムと考え，その特徴を考慮した適切なセキュリティの確立が必要である。

東芝グループは，スマートグリッドを適切な領域に分割し，各領域のセキュリティ要件を整理して，必要な技術を組み合わせることでセキュリティを確立するアーキテクチャを検討している。また，AMI（Advanced Metering Infrastructure：高度計量インフラストラクチャ）分野での具体的なセキュリティ技術の研究開発を進めている。

Efforts for the development and standardization of cybersecurity technologies for smart grids are currently being actively promoted in various countries. It is necessary to establish adequate cybersecurity considering smart grids as large-scale cyber-physical systems.

The Toshiba Group has been developing a smart grid security architecture, which divides the whole system into subsystems based on security characteristics to simplify security requirements and defines essential security components. We are also engaged in the research and development of practical applications for Advanced Metering Infrastructure (AMI) security.

1　まえがき

スマートグリッドとは，発電から送電，配電に至る電力系統や制御機器を情報ネットワーク化したものであり，分散電源の利用も含めた電力需給の監視と最適化を実現する次世代の電力インフラシステムとして期待されている。

一方，このような社会インフラシステムの情報ネットワーク化は新たなサイバー攻撃など情報セキュリティ上のリスクをもたらすことになる。例えば，系統制御システムの乗っ取り，虚偽の制御情報による系統混乱，及びDDoS（Distributed Denial of Service）攻撃によるサービスの妨害や停止といった攻撃は，ライフラインを維持するうえで重大な事態を招く可能性がある。

従来，制御システムは，専用線によるクローズドなシステムであるため安全とされていたが，近年，以下の状況変化により，もはやクローズドという想定は困難となっている。

(1)　保守・運用コストの圧縮　　遠隔保守のためネットワークを接続し，ベンダーごとだった保守用ネットワークを一本化して運用されるようになるため，電力系統の監視制御機器だけがつながるクローズドなシステムではない。

(2)　基幹システムとの密な結合　　組織内の基幹業務（調達や，設備管理，課金など）と連携させ，組織全体の情報資源を一元的に管理することで経営資源を効率的に活用する必要から，いわゆる情報系のネットワークと接続されるのが普通になっている。

(3)　想定外の相互接続　　様々な機能や暗黙の設定を内包する汎用製品適用の促進により，利用しない機能などによって意図していない接続が発生する可能性があり，これを完全に排除することが困難となっている。

このため，スマートグリッドのための情報セキュリティ技術の開発や標準化への取組みが各国で進められている[1]。

ここでは，スマートグリッドにおける情報セキュリティの課題の概要，及びスマートグリッドのためのセキュリティ アーキテクチャについて述べる。次に，東芝グループで研究開発を進めているセキュリティ技術について，AMI（Advanced Metering Infrastructure：高度計量インフラストラクチャ）分野を事例とした具体的な取組みについて述べる。

2　スマートグリッドにおける情報セキュリティの課題

2.1　スマートグリッドの特徴

スマートグリッドには以下の特徴があり，情報セキュリティを確立するうえでこれらを考慮する必要がある。

(1)　セキュリティ特性の優先度の違い　　一般の業務システムの場合は，機密性，完全性，可用性という3種類のセキュリティ特性のうち，機密性がもっとも優先される。しかし，スマートグリッドの場合は，監視制御指令などクリティカルデータの完全性と，監視制御機能などの可用性をより優先すべきである。

(2)　リアルタイム性と信頼性の要求及び末端機器の資源制約　　電力系統の監視制御には，リアルタイムの応答性と高い信頼性が要求される。その一方で，末端機器では，セキュリティ機能に必要なCPU性能やメモリサイズの確保

が困難となる場合がある。

(3) 需要家情報の需給制御への利用　電気機器の電力利用状況など需要家の情報を電力需給を最適化する制御に利用する際，需要家のホームネットワーク上の機器と接続することになるが，これらは電力会社による十分なセキュリティ管理が困難である。そのため，信頼度の低い情報をどのように制御に生かすかという課題がある。

(4) 第三者サービス事業者と連携　電力会社とは別の第三者事業者が提供する省エネサービスなどとの連携が期待されているが，まだビジネスプロセスが固まっておらず，相互接続先の広がりの想定が困難なため，データのアクセス管理が複雑となり，漏れのない実施が困難である。

(5) 所有者及び権限の異なる電力サブシステムが連携
海外の場合，発電，送電，及び配電が独立した事業者で運営され，事業者間のセキュリティポリシーが統一されていない場合が普通である。

2.2 情報セキュリティへのアプローチ

システムの情報セキュリティを策定する場合，具体的なシステム構成に基づき，①保護資産の特定，②脅威の洗出し，③リスク評価，④対策立案の手順で実施するのが一つのアプローチである。この場合，スマートグリッドは大規模なサイバーフィジカルシステムとみなすことができる。システムの特徴に応じて適切な領域に分割し，各領域について，既存の標準的な情報セキュリティ技術とスマートグリッドに特化したセキュリティ技術を組み合わせるようなアーキテクチャによって，全体のセキュリティの確立を図ることが現実的である。

3 セキュリティ アーキテクチャ

前述の考え方に基づいたスマートグリッドのためのセキュリティ アーキテクチャを**図1**に示す。

3.1 システムセキュリティ

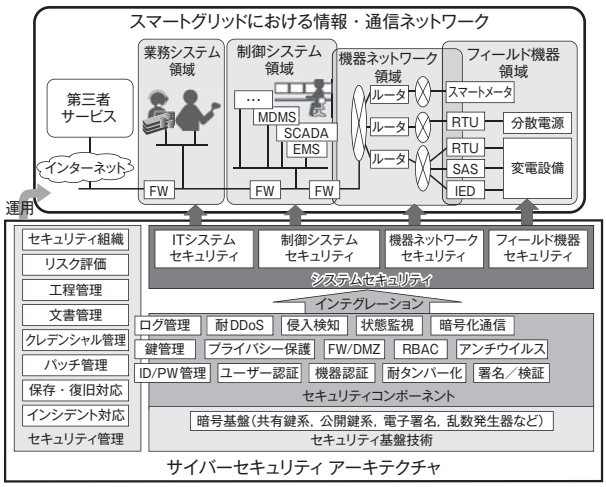
以下の四つの領域に分け，各領域の性質に合わせたシステムセキュリティを構築する。

(1) フィールド機器領域　計算機資源に制約のある機器が屋外や需要家サイドに設置される場合が多く，物理的及びソフトウェア的な耐タンパー性が重要になる。

(2) 機器ネットワーク領域　フィールド機器とコントロールセンターなどに設置された制御システムをつなぐネットワークで，系統制御機器の通信ネットワークでは，通常，高速かつ高信頼の専用線で構成される。AMIでは無線（メッシュ型を含む），電力線通信，及び公共ネットワークなどを含む様々な形態が想定され，通信セキュリティが重要になる。

(3) 制御システム領域　監視制御システム（SCADA：Supervisory Control and Data Acquisition）やメータデータ管理システム（MDMS：Meter Data Management System）などのサーバサイド機器の領域で，アンチウイルスや，ユーザー認証，アクセス制御などの機能が重要になる。これらの機器は，リアルタイムでフィールド機器の監視と制御を行うため，信頼性と可用性の維持も必要になる。

(4) 業務システム領域　顧客管理や設備管理などを含む基幹業務系システムの領域で，外部サービスとの接点となるため，一般的なネットワークセキュリティを施す必要がある。



FW　：ファイアウォール
EMS　：Energy Management System
RTU　：Remote Terminal Unit
SAS　：Substation Automation System
IED　：Intelligent Electronic Device
IT　：情報技術
DMZ　：Demilitarized Zone
RBAC：Role Based Access Control
ID　：Identification
PW　：Password

図1. セキュリティアーキテクチャ ― 四つに分割された領域（エリア）に対し3階層構成のアーキテクチャで全体のセキュリティ設計を容易にする。
Architecture of cybersecurity system

3.2 セキュリティ コンポーネント

認証や，アクセス制御，監視及び検出，暗号技術などのセキュリティ機能を実現する部品であり，各領域のセキュリティは，その要件に応じたセキュリティ コンポーネントをインテグレートすることで実現される。これらコンポーネントには暗号基盤技術が広く適用され，計算機資源の制約も考慮して，負荷が軽く，高速な処理能力を備える必要がある。

3.3 セキュリティの管理と運用

情報セキュリティを高めるには，セキュリティを維持する適切な管理プロセスの確立と，その継続的な運用がたいせつである。スマートグリッドは重要な社会インフラシステムであるため，特にセキュリティの管理と運用に関して厳しい取組みが求められる。一例であるが，米国では連邦エネルギー規制委員会が，NERC CIP[2]（North American Electric Reliability Corporation Critical Infrastructure Protection）として知られるセキュリティ管理・運用基準への適合を電力事業者に義務付けている。この基準は，重要情報資産の識別，セキュリティ

管理策，セキュリティに関する人的リスクアセスメントや教育，電子的なセキュリティ境界，重要情報資産の物理的保護，システムセキュリティ管理，インシデントの報告と対応計画，及び重要情報資産の復旧計画，といった広範囲の管理要件から成る。

こうした基準への適合を図るために，システムを構築するごとに管理プロセス及び運用施策を一から作り上げるのでは時間が掛かる。NERC CIPや国際標準のISO/IEC 27001（国際標準化機構／国際電気標準会議規格27001：情報セキュリティマネジメントシステム－要求事項），ISO/IEC 27002（情報セキュリティマネジメントの実践のための規範）に沿って，セキュリティの管理と運用のベストプラクティスを開発しておき，個々のシステムの特性に合わせてカスタマイズする手法が効率的である。

4　AMI分野における具体的な取組み

AMIシステムにおけるセキュリティを考える。AMIシステムでは，スマートメータの計測データはAMIネットワークを介してMDMSに蓄積される。MDMSは，他のサーバ，クライアント，及び他のサービスからの要求に応じて情報を提供する。

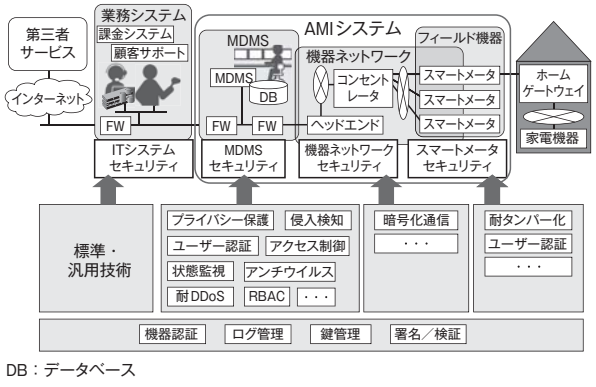
AMIシステムを3章で述べた領域に分割（**図2**）し，各領域における必要なセキュリティ要件と，研究開発事例について以下に述べる。

(1)　フィールド機器　　スマートメータではメータのソフトウェアやデータの改ざんを防ぐために，ハードウェア及びソフトウェアの耐タンパー化が必要になる。また，メータデータの流出によるプライバシー侵害への懸念があるため，ユーザー認証の仕組みが必要になる。

(2)　機器ネットワーク　　無線メッシュ型通信やインターネットの利用も含めた様々な構成が想定されるため，機器認証による不正機器の排除と，盗聴を防ぐための通信の秘匿化が必要になる。

(3)　MDMS　　多数のユーザーのデータを扱うため，強固な保護の仕組みが必要であり，外部からの不正アクセスはもとより，内部不正者による業務システムからのアクセスへの対策も必要になる。また，機器ネットワークからのDDoS攻撃への対応も必要になる。

(4)　業務アプリケーション　　権限あるユーザーだけを許可するユーザー認証とともに，マルウェアや外部からの不正侵入の防止を徹底する必要がある。



DB：データベース

図2．AMIシステムにおけるセキュリティの構築 ― セキュリティアーキテクチャをAMIシステムへ適用したときのイメージである。
Construction of cybersecurity for AMI system

4.1　AMSO$_{TM}$/RFC 5191

AMIシステムにおける通信セキュリティを実現する統合鍵管理技術AMSO$_{TM}$（Advanced Meter Sign-On）を開発した。AMSO$_{TM}$では，スマートメータのような計算機資源の限られた端末で以下の機能を実現している。

(1)　不正機器によるネットワーク接続を防止するためのネットワークアクセス認証

(2)　スマートメータとMDMSとの間の暗号通信

(3)　認証や暗号通信で使用する鍵の動的な更新

AMSO$_{TM}$は，端末が実行するネットワークアクセス認証手続き（**図3**の①）の中で，計量データの収集やデマンドレスポンス処理など，アプリケーションごとの通信用暗号鍵生成に必要なマスタ鍵を更新（図3の②）する。一度の認証手続きでネットワークアクセス認証と暗号鍵更新を実現し，計算負荷の高い鍵更新処理の回数を減らすことが可能になった。

AMSO$_{TM}$のアーキテクチャでは，認証フレームワークとしてEAP（Extensible Authentication Protocol）[3]を使用する。EAPは，インターネット関連技術の標準化を行っているIETF（Internet Engineering Task Force）で東芝が標準化した，ネットワークアクセス認証プロトコルのRFC 5191[4]によって伝送され，端末内のEAPピアとサーバ内のEAPオーセンティケータ間で相互認証が行われる。相互認証の結果生成されるマスタ鍵が鍵管理機能であるUKMF（Unified Key Management Function）に渡され，このマスタ鍵を元にアプリケーションごとに必要な暗号鍵を生成（図3の③）する。これによりアプリケーションごとに個別の鍵交換を行う処理を不要にした。

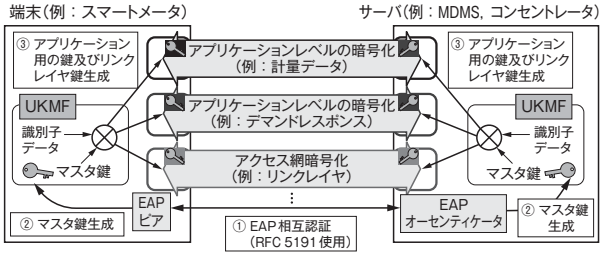


図3．AMSO$_{TM}$の仕組み ― AMSO$_{TM}$の処理により効率的に鍵を生成する。
Architecture of AMSO$_{TM}$ (Advanced Meter Sign-On)

4.2 MDMSにおけるプライバシー保護[5]

MDMSに蓄積されたメータデータの保護に秘密分散を用いる方式の研究を行っている。データを分割して記録し管理するため，片方のデータだけでは決して原データを復元することができず，内部者の悪意や過失によるデータ流出への対策を実現している。この方式のもう一つの特長は，分割により保護されているデータのまま加算演算が可能な点で，これにより，詳細な利用状況を開示せずに必要な数値情報を計算し復元することができる。例えば1か月の積算処理を行い，その結果だけを復元して課金処理に渡したり，ある地域全体の使用電力総量を積算して需給制御に利用したりすることが実現できる。この方式の原理を**図4**に示す。

4.3 DDoS耐性が高い認証技術

計算機資源の制約があるフィールド機器を志向し，低処理負荷でDDoS攻撃への耐性が高い機器認証方式の研究を行っている。この研究は，東芝が開発した，サーバへの接続要求時にチャレンジレスポンスなどのない，軽い片方向認証を行う技術であるTAP（TCP（Transmission Control Protocol）Layer Application Protector）[6]の考え方をベースとしている。TAPではサーバはSYNパケットの受信時に秘密鍵に基づく1パス認証を行うことで，攻撃者からTCPサーバの存在が見えないようにできるため，ポートスキャンへの対抗も可能である（**図5**）。

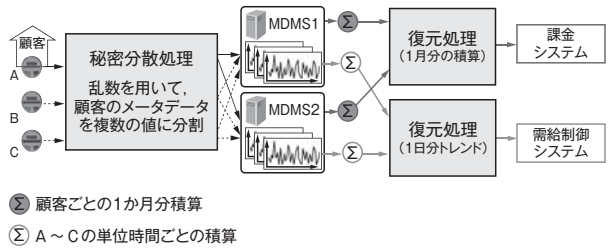


図4．秘密分散の原理を用いたメータデータの保護 — データを分割して記録し管理するため，片方のデータだけでは決して原データを復元することができない。

Metadata protection using secret sharing mechanism

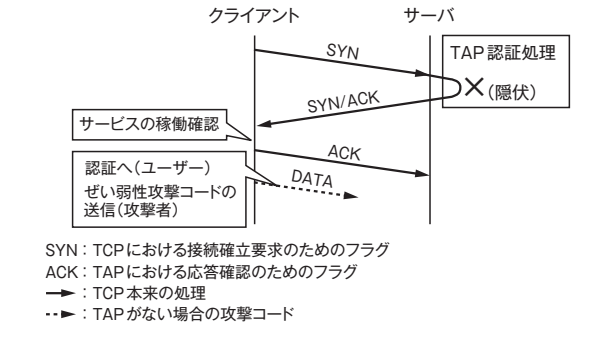


図5．TCPレイヤ認証の仕組み — サーバはSYNパケットの受信時に秘密鍵に基づく1パス認証を行うことで，攻撃者からTCPサーバの存在が見えないようにできるため，ポートスキャンにも対抗できる。

Mechanism of TCP (Transmission Control Protocol) layer authentication

5 あとがき

スマートグリッドにおける，情報セキュリティの課題の概要及びセキュリティ アーキテクチャと，東芝グループの取組み事例を述べた。

スマートグリッドは大規模なシステムであるため，システムの各部分の特徴に応じて領域に分割し，各領域について，既存の標準的情報セキュリティ技術とスマートグリッドに特化したセキュリティ技術を組み合わせ，適切なアーキテクチャを検討することが有効である。ここで述べたセキュリティのアーキテクチャと構成要素の実効性について，実証実験の場で評価し確認する必要がある。実効性が確認できた技術については，積極的に国際標準化の検討を進めていく。

文 献

(1) NIST. "PUBLICATIONS/IR 7628:Guidelines for Smart Grid Cyber Security". <http://csrc.nist.gov/publications/PubsNISTIRs.html>, (accessed 2011-08-22).
(2) NERC. "Reliability Standards/Critical Infrastructure Protection (CIP)". <http://www.nerc.com/page.php?cid=2|20>, (accessed 2011-08-22).
(3) Aboba, B. et al. "RFC 3748 Extensible Authentication Protocol (EAP)". The Internet Engineering Task Force (IETF) Homepage. <http://www.ietf.org/rfc/rfc3748.txt>, (accessed 2011-08-22).
(4) Ohba, Y. et al. "RFC 5191 Protocol for Carrying Authentication for Network Access (PANA)". IETF Homepage. <http://www.ietf.org/rfc/rfc5191.txt>, (accessed 2011-08-22).
(5) 伊藤 聡 他．“北米におけるスマートグリッド・セキュリティの取組”．平成23年度 電気学会全国大会 予稿集．大阪．2011-03，電気学会．第1分冊H2 p.5－8.
(6) 高橋俊成 他．“隠伏サーバを実現するTCP認証方式”．第47回プログラミング・シンポジウム 予稿集．神奈川，2006-01，情報処理学会．p.129－140.

伊藤 聡 ITO Satoshi
研究開発センター コンピュータアーキテクチャ・セキュリティラボラトリー主任研究員。著作権保護技術及びシステムセキュリティ技術の研究・開発に従事。情報処理学会会員。
Computer Architecture & Security Systems Lab.

島田 毅 SHIMADA Tsuyoshi
東芝ソリューション（株）IT技術研究所 研究開発部主幹。システムセキュリティの評価・設計・開発，及びスマートコミュニティの研究・開発に従事。IEEE会員。
Toshiba Solutions Corp.

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.