制御システムのセキュリティ改善サイクルとセキュリティ演習

PDCA Cycles and Security Exercises to Improve Security of Control Systems for Industrial and Social Infrastructure Systems

上林　達　　伊藤　聡
■KAMBAYASHI Toru　■ITOH Satoshi

スマートグリッドが社会インフラとして構築されつつあり，その主要な構成要素である制御システムに対するセキュリティの確立と向上が大きな課題となっている。そのためには，セキュリティ演習（対攻撃演習など）を含む改善サイクルの実施が不可欠である。

東芝は，産学官が連携して立ち上げた技術研究組合 制御システムセキュリティセンター（CSSC）に参画して制御システムセキュリティの確立と向上に取り組んでおり，そのなかで，改善サイクルの主要なステップとなるセキュリティ演習システムの構築を進めている。

Accompanying the construction of smart grids as an important component of social infrastructures in recent years, there is a pressing demand to establish and improve cybersecurity to an adequate level for industrial control systems (ICSs) and control systems for social infrastructures connected to such smart grids. Plan-do-check-act (PDCA) cycles using cyberattack simulation tests such as security exercises are essential for this purpose.

Toshiba has been engaged in the establishment and improvement of PDCA cycles and security exercises for ICSs and control systems for social infrastructures. As an association member of the Control System Security Center (CSSC) established through industry-government-academia cooperation, we are now developing and constructing a security exercise system as an important step in PDCA cycles for the security management of ICSs and control systems for social infrastructures.

1　まえがき

スマートグリッドは，発電所や変電所などの発電・送配電設備，商用ビルやマンションなどのエネルギー管理設備，及びAMI（Advanced Metering Infrastructure）などの電力システムを，ネットワークでつなぐ統合的な電力インフラである。その目的はICT（情報通信技術）を利用してエネルギーの公正かつ有効な利用を図ることにあり，現在，構築に向けて様々な取組みが進んでいる。スマートグリッドにより，効率的な社会の実現という大きなメリットが期待される一方で，インターネットから社会インフラへの不正侵入やコンピュータウイルスのまん延など，サイバー攻撃の脅威が懸念されている。

複数の社会インフラを結ぶスマートグリッドの運用管理を単一の組織が実施することは困難である。個々に管理されたシステムが連携して動作することで，インターネットが機能しているように，スマートグリッドのセキュリティも，ネットワークで結ばれる個々のシステムでセキュリティを確立し，維持することで実現される。

スマートグリッドを構成する個々のシステムは一般に制御システムである。ここでは，制御システムセキュリティの確立と向上の鍵である改善サイクルについて述べるとともに，改善サイクルの主要なステップであるセキュリティ演習について，技術研究組合 制御システムセキュリティセンター（CSSC）[1]における東芝の取組みを述べる。

表1．制御システムにおけるネットワークセグメント
Network segments in control system

セグメント	対象（例）
一般情報系	データセンター，社内業務システム，など
コントロールセンター系	SCADA，HES，など
制御システムクライアント系	RTU，IED，AMIのFAN機器，など

FAN : Field Area Network

2　制御システムのセキュリティ

制御システムのセキュリティとCSSCの概要を述べる。

2.1　制御システムの構成とセキュリティ

広義の制御システムは，**表1**に示す三つのセグメントから構成される。制御システムクライアント系は，社会インフラにおける現実世界とのインタフェースである。ここには，スマートメータなどのセンサや，コンセントレータなどの中継器が含まれ，センサからのデータを中継器が取りまとめて，更に上位のコントロールセンター系に送る機能を持つ。また，このセグメントには，遠隔監視制御装置（RTU）や電力用インテリジェント端末（IED）が含まれ，プラントの状況を逐一コントロールセンター系に送る機能と，コントロールセンター系からの指示により，各機器を動作制御する機能を持っている。

コントロールセンター系は，制御システムクライアント系を管

理し制御するセグメントであり，監視制御システム（SCADA：Supervisory Control and Data Acquisition）やヘッドエンドシステム（HES：Head End System）などを備えている。一般情報系は，例えば，コントロールセンター系で集められた情報（ビッグデータ）を利用してスマートグリッドの目的であるエネルギーの公正かつ有効な利用を図るセグメントである。

制御システムのシステム構築者は，一般に複数の機器製造者から機器を調達しシステムを構築する。一つのシステムが複数のサブシステムから構成され，各サブシステムが別のシステム構築者によって構築される場合もある。その際に重要なのは，それぞれのシステムにおける責任の界面を明確化し，責任範囲を定義することである。これにより，システム構築者は構築したシステムのセキュリティに責任を負い，機器製造者は納入した機器のセキュリティに責任を負うことができる。同時に，システム運営・管理者，システム構築者，及び機器製造者がセキュリティに関する必要な情報を相互に円滑に交換し，システム全体のセキュリティを維持し向上させていくことが求められる。

制御システムのセキュリティを確立し向上させていく際の重要ポイントの一つに，PDCA（Plan-Do-Check-Act）サイクルの確立がある。セキュリティのPDCAサイクルの一例を**図1**に示す。機器製造・メンテナンス，システム構築・メンテナンス，及びシステム運営・管理の各役割におけるPDCAサイクルは有機的に関連している。例えば，セキュリティ監視やログ解析の知見を，システムセキュリティの現状としてリスクアセスメントに反映する。あるいは，システムのセキュリティ設計の見直しに伴って，機器のセキュリティ要件を変更する。その結果，機器の更新が行われるかもしれない。このように，機器製造・メンテナンスからシステム運用・管理まで，複数の役割を横断して必要な情報を円滑に共有し，システムセキュリティの維持と向上のためにフィードバックする必要がある。

2.2 CSSCの役割

制御システムのサイバーセキュリティに対する要請の高まりを背景に，CSSCという技術研究組合が2012年3月に設立された。CSSCは宮城県多賀城市と東京お台場に拠点を持ち，制御システムのセキュリティに関する研究開発をはじめ，国際標準化活動や認証，人材育成，普及啓発など多岐にわたる活動を活発に行っている。CSSCには，制御システムの機器製造者，システム構築者，及びシステム運営者のほか，セキュリティベンダーや，大学，研究機関などが組合員として参画している。CSSCの場が存在することで，改善サイクルの加速が期待される。

当社もCSSCの組合員として，変電所システムの模擬プラントをCSSC多賀城本部に設置しており，現在この模擬プラントの拡張作業を行っている。同時に，セキュリティ演習シナリオと評価方法の策定を行い，セキュリティ演習システムを構築している。

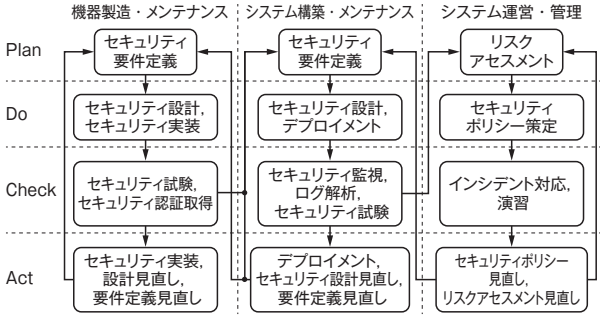

図1．セキュリティのPDCAサイクル例 ― 制御システムのセキュリティを確立し向上させていくためにPDCAサイクルの実行は必須である。
Example of PDCA cycle for improvement of control system security

3 制御システムにおけるPDCAサイクル

制御システムのセキュリティはいくつかの技術的特徴を持っており，PDCAサイクルの実施に際しては，それらを勘案する必要がある。ここでは，制御システムのセキュリティが持つ技術的特徴と，AMIを例にとり，機器のセキュリティ要件の抽出やセキュリティ試験について述べる。

3.1 制御システムセキュリティの技術的特徴

個々の制御システムにおけるサイバーセキュリティは，以下のようないくつかの技術的特徴を持っている。

(1) インターネットで標準的ではないプロトコルを含む

制御システムでは，例えば，IEC 60870-5-101（国際電気標準会議規格60870-5-101）/104やIEC 61850-8/9といった制御システム特有の規格に準拠したプロトコルが用いられる。これらは，インターネットにおける標準的なプロトコルではないため，標準的な侵入検知システムIDS（Intrusion Detection System）が利用できない。

(2) 低負荷のセキュリティプロトコルが用いられている

フィールド機器は屋外に設置され，保守なしで長期間正常に稼働することが求められる。そのため，冷却用ファンやHDD（ハードディスクドライブ）など可動部分を持つ部品を搭載することができず，結果として，CPUの性能やストレージの容量などに制約が課されることとなる。このように，フィールド機器には一般に，処理負荷の大きなセキュリティプロトコルを搭載することが困難である。

一般に，通信セキュリティではエンド ツー エンドのセキュリティモデルが用いられる。送信側と受信側が鍵（共有鍵）を共有し，送信側は共有鍵で送信データを暗号化し，受信側は共有鍵で受信データを復号する。これにより，送信されるデータが悪意ある中間者による盗聴や改ざんから守られる。しかし，前述したハードウェア上の制約から，一部のフィールド機器は，組込みの（あるいは一体

化された）暗号化機能を持つことができず，エンド ツー エンドのセキュリティが利用できない場合がある。

これら二つの特徴は，基本的に制御システムクライアント系機器の特性に由来している。一般情報系のセグメントは通常のLANで接続されたパソコンやサーバマシンなどが収容されている。また，コントロールセンター系のセグメントも同様で，SCADAやHESなど制御システムのサーバもWindows®(注1)やLinux®(注2)のサーバマシン上で稼働している。

3.2 AMIにおけるPDCAサイクル

AMIの一例を**図2**に示す。コンセントレータは複数のメータからの情報を束ねてHESに送る。HESは複数のスマートメータを管理しており，コンセントレータから受け取ったデータを，メータごとに分離してデータベースに格納する。MDMS（Meter Data Management System）はメータの検針データを集計し，課金情報と関連付ける。スマートメータからメータデータを読み取り，それを利用者に表示するのは，HEMS（Home Energy Management System）の機能の一つである。スマートメータやコンセントレータはフィールド機器である。

AMIでは，例えば，スマートメータとHESの間のデータ伝送規格としてIEC 62056が採用される。フィールド機器における通信規格としては，IEEE 802.15.4のマルチホップ無線通信などが利用される。マルチホップ無線通信では，スマートメータ自身が中継機器となり，他のスマートメータの検針データをコンセントレータに送る。

3.2.1 セキュリティ要件の抽出とセキュリティ設計

スマートメータやコンセントレータはフィールド機器であるが，検針データは課金の基礎となる情報であり，同時に個人のプライバシーに関わる情報でもあるため，その保護には大きな注意が払われる。例えば，以下のようなセキュリティ要件が課せられることになる。

（1） スマートメータの検針データは他のスマートメータから読み取れない。

（2） HESは，検針データをメータごとに確実に識別できる。

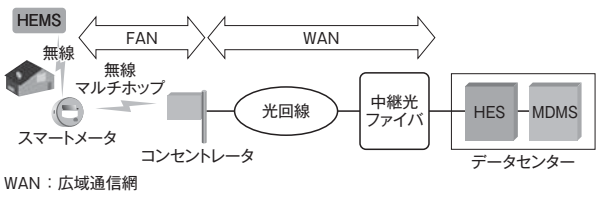

図2. AMIの構成例 ― スマートメータの検針データの通信には，セキュリティ上の保護が必要である。
Example of configuration of advanced metering infrastructure (AMI) system

（3） 検針データは通信経路上で改ざんされてはならない。

セキュリティ設計者は，前記(1)，(2)，及び(3)のセキュリティ要件を満たすように，セキュリティプロトコルを設計する。その際は，フィールド機器に許容される計算リソースを考慮する必要がある。それはまた，そのAMIに固有の通信規格や通信プロトコルに適合するものでなければならない。

3.2.2 脆弱（ぜいじゃく）性試験

スマートメータやコンセントレータ，HESなどを製造する機器製造者は，各製品に脆弱性試験を行い，脆弱性を排除することが求められる。脆弱性試験は大きく静的解析と動的解析の二つに分けられる。

多くの機器はCPUを持ち，機器の機能はプログラムによって実現されている。静的解析は，検査ツールを用いて機器のプログラム自体を解析し，既知の脆弱性が含まれていないかを検査するものである。検査ツールは，最新の脆弱性データベースと連携していることが望ましい。動的解析は，検査ツールが機器に対して不正なパケットを送るなどして，機器の脆弱性を見つけるものである。動的解析は，既知の脆弱性のほかに，未知の脆弱性を見つけるために行われる。

機器に対して脆弱性試験を実施したからと言って，その機器の脆弱性を全て見つけることができるとは限らない。そのため，機器製造者は随時脆弱性試験を行い，機器の脆弱性に由来するリスクを可能なかぎり排除しようとする。重大な脆弱性が発見された場合は，既存の機器にもアップデートなどの対策を施す。

セキュリティの確立と向上に必要なセキュリティ試験は，機器単体の脆弱性試験だけではない。システムのセキュリティ管理者は，例えば，次のような項目に関して試験と評価を行うことが望ましい。

（1） リアルタイム又は事後に侵入を検知できるか。

（2） 脅威の拡大を防止できるか。

4 CSSCのセキュリティ演習

セキュリティ演習は，制御システム運用管理におけるPDCA改善サイクルのステップの一つとして重要である。CSSCのセキュリティ演習の意義の一つは，様々な分野で制御システムの運用管理に携わっている企業や組織に，参考例を提示することである。当社はCSSCと協力して，広域制御システムの変電所模擬プラントを拡充し，演習システムを構築する計画である。その演習システムの概要を**図3**に示す。

変電所は，電圧の変換や系統の開閉を行う。ここでは，無人変電所を想定しており，変電所内の機器の状態はSC（Substation Computer）を通じてコントロールセンターのSCADAサーバに送られ，ヒューマンマシンインタフェース（HMI）に表示される。コントロールセンターのオペレーターの指示は，SCADAサーバから発行され，SCを介して各機器に伝えられる。

（注1） Windowsは，米国Microsoft Corporationの米国及びその他の国における商標又は登録商標。
（注2） Linuxは，Linus Torvalds氏の日本及びその他の国における登録商標又は商標。

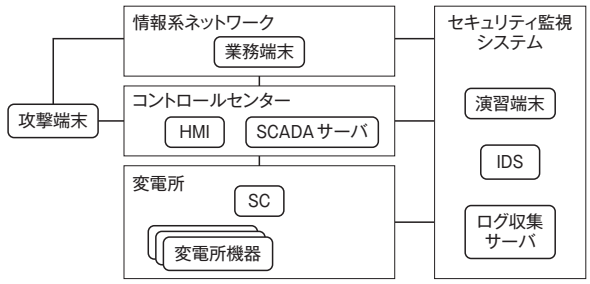

図3. セキュリティ演習システムの概要 ― 広域制御システムの変電所模擬プラントを拡充してセキュリティ演習システムを構築している。
Overview of control system simulator for security exercises

攻撃端末はこの演習システムに対する擬似的な攻撃を発生させる。セキュリティ監視システムは，情報系ネットワーク，コントロールセンター，及び変電所のネットワークトラフィックといくつかの機器のログを監視する。

演習の対象者としては次を想定している。

(1) ユーティリティ（電力会社，特定規模電気事業者など）のオペレーター

(2) システムのセキュリティ管理者

オペレーターはコントロールセンターで異常に気づき，初動措置を行って問題を切り分け，緊急対応を実施する。システムのセキュリティ管理者は，これを受けて原因究明に当たり，被害拡大防止策や対策の立案などを実施する。オペレーターが異常を検知するのは，セキュリティ監視システムからのアラートや，実システムの挙動の異常などであるが，できるだけ早い段階でインシデント発生に気づくことが被害の拡大を防ぐうえで望ましい。これを実現するうえでは，セキュリティ監視システムの導入は不可欠である。もしそれが存在しない場合，オペレーターは，そのインシデントが機器の異常に起因するものか，サイバー攻撃によるものかを切り分けることすら不可能である。

オペレーターの初動措置において問題が正しく切り分けられていないと，初動段階でも二次災害が起こる可能性がある。例えば，サイバー攻撃による被害であるにも関わらず，サイバー攻撃を想定せずに初動した場合，サイバー攻撃者がHMIの表示を操作することにより，オペレーターが誤った操作を行う危険性がある。この場合，セキュリティ監視センターから得られる情報を勘案したうえで問題の切分けを行い，適切な初動措置を行うことが求められる。また，必要に応じて，システムのセキュリティ管理者への報告を行わなければならない。

システムのセキュリティ管理者は，オペレーターからインシデントの状況や初動措置に関する聞き取りを行い，IDSやOS（基本ソフトウェア）のログ，ネットワークログに基づいて原因究明を行う。そのうえで対策立案を行う。また中長期的な観点で，システムのセキュリティ設計の見直しを行うこともシステムのセキュリティ管理者に期待される役割である。

この演習では，演習対象者が演習を受けるだけでなく，演習者の習熟度を評価する仕組みを導入する予定で，それには次のような目的がある。

(1) 演習対象者の現時点でのインシデント対応能力を多面的に評価し，結果を本人にフィードバックできるようにすることで，今後の改善方法の指導に役だてる。

(2) 評価結果をCSSCが蓄積し，演習対象者の習熟度に関する統計的な傾向を把握できるようにすることで，指導方法の向上などに役だてる。

この演習システムの作成にあたっては，CSSCの他の組合員の協力を得ている。制御システムについては各社非公開の部分も存在するが，可能な範囲で協力することで，互いに制御システムのセキュリティに関する知見を広げ，より良いセキュリティの実現に向けて活動することが可能になる。これもCSSCという組合組織の意義の一つである。

5 あとがき

制御システムセキュリティの確立と向上の鍵である改善サイクルを，AMIを例にして述べた。また，当社がCSSCで取り組んだ，改善サイクルの主要ステップであるセキュリティ演習について述べた。当社は今後も，CSSC組合員企業の一社として，制御システムセキュリティの確立と向上に貢献していく。

文 献

(1) 制御システムセキュリティセンター. <http://www.css-center.or.jp/index.html>,（参照 2013-12-16).

(2) Stouffer, K. et al. Guide to Industrial Control Systems (ICS) Security. National Institute Standards and Technology (NIST), U.S. Department of Commerce, 2011, 155p. (NIST SP800-82).

(3) NERC CIP-005-03a: Cyber Security - Electronic Security Perimeter(s). North American Electric Reliability Corporation.

(4) Smart Grid Interoperability Panel Cyber Security Working Group. Guidelines for Smart Grid Cyber Security: Vol.3, Supportive Analyses and References. NIST, 2010, 219p. (NISTIR 7628).

(5) 情報処理推進機構（IPA）セキュリティセンター. “2010年度制御システムの情報セキュリティ動向に関する調査報告書”. IPA, 2011, 110p.

(6) ISA Secure Compliance Institute. “ISASecure プログラムの説明”. ISASecureホームページ. <http://www.isasecure.org/ISASecure-Program/Japanese-ISASecure-Program.aspx>,（参照 2013-12-16).

上林 達 KAMBAYASHI Toru
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研究主幹。ヒューマンインタフェース，著作権保護，スマートグリッド セキュリティなどの研究・開発に従事。
Computer Architecture & Security Systems Lab.

伊藤 聡 ITOH Satoshi
社会インフラシステム社 府中社会インフラシステム工場 スマートメーター通信システム部参事。プラント制御ソフトウェア設計支援技術，システムセキュリティ技術の開発に従事。
Fuchu Operations - Social Infrastructure Systems