

電力システムのサイバーセキュリティを向上する IEC 62351 に対応した SCADA の開発

■ 黒田 英次
Eiji Kuroda

■ 益子 奈々海
Nanami Mashiko

■ 荒井 俊成
Toshinari Arai

近年、電気事業法に基づく技術基準および関連ガイドラインの整備が進んでおり、電力分野におけるサイバーセキュリティ対策の要件が体系的に確立されつつある。これにより、電力システムにおいては、従来の安定供給に加え、通信および制御に関するセキュリティ確保の重要性が一層高まっている。

こうした状況を踏まえ、株式会社ミントウェーブでは、国際規格 IEC 62351 に基づく認証および暗号化技術を、IEC 61850 に対応した SCADA へ適用する取り組みを進めている。本取り組みでは、認証・認可に基づくセキュアなアクセス制御の実現を目的とし、実機およびシミュレータ環境を用いて検証を実施した。本稿では、その実装方式および検証結果について報告する。

1 はじめに

IoT をはじめとするデジタル技術の進展に伴い、電力分野においてもシステムの高度化が進んでいる。一方、国内では、電気事業法に基づく技術基準や関連ガイドラインが整備されており、電力分野において求められるサイバーセキュリティ対策の要件が体系的に整理されている。

このうち、「電力制御システムセキュリティガイドライン」⁽¹⁾ が運用面での指針を示す一方、IEC 62351 は認証や暗号化通信などの技術的な実装方法を規定している。

しかし、これらの指針や規格を実際の変電所システムへ適用する際には、既存システムや運用との整合性が課題となっており、具体的な実装手法は十分に整理されていないのが実情である。

こうした中、電力制御通信に関する規格 IEC 61850 の国内での適用拡大に伴い、認証・認可に基づく安全性の高いアクセス制御技術の重要性が増している。そこで本稿では、電力システムを取り巻くサイバーリスクに対処することを目指し、IEC 62351 の SCADA^{注1)} への適用に着目し、IEC 62351-3⁽²⁾ および IEC 62351-8⁽³⁾ を対象としたセキュリティ機能の検証を行ったので紹介する。なお、本研究開発は、電気学会でも報告をしており、今後の技術応用や実用化に貢献することを目的としている⁽⁴⁾。

2 IEC 62351 に基づくセキュリティ機能の構成

電力システムにおける通信ネットワークおよびセキュリティに関する国際規格として、IEC 62351 が策定されている。本規格は、IEC 61850 通信をはじめとする電力制御通信に対し、改ざん検知、不正アクセス防止、暗号化ならびに認証・認可といった各種セキュリティ機能

を規定している。図 1 に、認証局サーバ、SCADA、および IED・PLC の構成イメージを示す。本規格の適用により構成されるシステムは、大きく「通信を担う機器 (SCADA, IED^{注2)}・PLC^{注3)})」と、それらの認証および管理を行う「認証基盤 (認証局サーバ)」の二つに分類される。以下に、各構成要素を説明する。

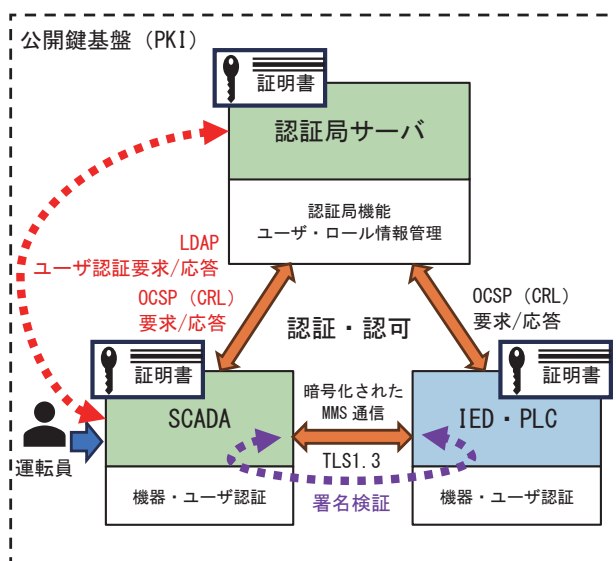


図 1 認証局サーバ構成イメージ

(1) 認証基盤 (認証局サーバ)

認証局サーバは、公開鍵基盤 (PKI: Public Key Infrastructure) の役割を担い、SCADA および IED・PLC に対して証明書の発行および管理を行うことで、機器認証および暗号化通信の基盤を提供する (認証局機能)。各機器に配布された証明書は、通信確立時の認証処理に利用される。また、認証局サーバは IEC 62351-8 に示される RBAC^{注4)} (ロールベースのアクセス制御) の考え方に基づき、LDAP^{注5)} (階層構造で管理する通信プロトコル) を用いて SCADA のユーザ情報およびロール情報 (役割情報・権限情報) を一元的に管理する。

SCADA からの認証要求に対しては、ユーザ証明書および LDAP による資格情報の検証を行い、認証結果とともにロール情報を送信する。SCADA はこれに基づき操作権限を制御し、RBAC に基づく運用を実現する。

(2) 通信を担う機器 (SCADA, IED・PLC)

SCADA および IED・PLC では、IEC 62351-3 に規定される通信セキュリティの考え方に基づき、暗号化通信 (TLS^{注6)}) 確立時に自装置および相手側の証明書に対して署名の検証を行うとともに、証明書チェーン^{注7)}を遡って信頼できる認証局により発行されたものであることを確認する。さらに、有効期間の確認に加え、OCSP^{注8)} または CRL^{注9)} (ルールや失効一覧表) を用いた失効確認を実施し、証明書の有効性を総合的に検証する。これにより、有効期限切れや失効済み証明書による通信を排除し、通信相手の正当性を担保する。

3 セキュリティ機能の実装・検証

(1) 検証システムの構成

本検証システムは、セキュリティ機能の検証を目的として、IEC 62351 に基づく認証および暗号化通信機能を実装した MintSCADA (株式会社ミントウェブ製 SCADA)、暗号化通信の検証が可能な IED シミュレータ (同社開発品)、ワゴジャパン株式会社 (以下、WAGO 社) 製 PLC (750 シリーズ)、ならびに証明書管理を担う認証局サーバにより構成される (図 2)。認証局サーバは、コスト面を考慮し、Linux をベースとしたオープンソースソフトウェアで構築している。また、暗号化通信 (TLS) に対応した IED 機器が市場において限定的であることから、IED シミュレータを使用している。

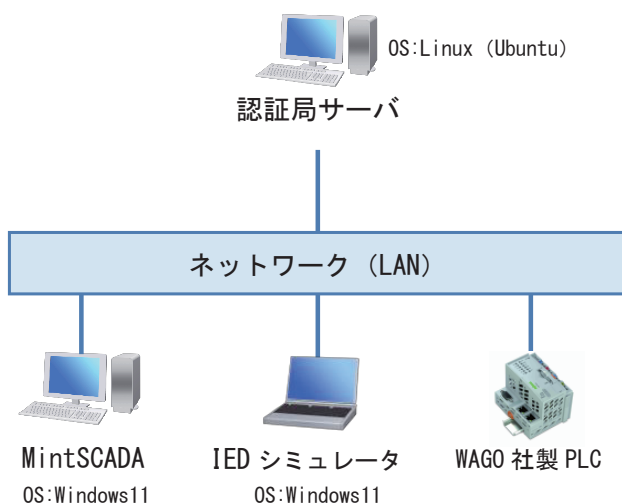


図 2 システム構成図

(2) セキュリティ機能の実装

認証局サーバは、公開鍵基盤 (PKI) に基づき、MintSCADA および IED シミュレータ、WAGO 社製 PLC に対して証明書の発行・管理を行い、機器認証および暗号化通信の基盤として構築した。発行した証明書は、USB メモリなどの外部媒体を用いて各機器に配布し、通信確立時の機器認証に利用することで、信頼できる機器間通信の確立を可能としている。さらに、認証局サーバは IEC 62351-8 に基づき、LDAP を用いてユーザ認証ならびにユーザ情報 (識別情報・認証情報) およびロール情報 (役割情報・権限情報) を一元管理する。この構成により、MintSCADA のユーザは付与された役割に応じて利用可能な機能が制御され、システム運用におけるアクセス制御の厳格化が図られる。

一方、MintSCADA では、既存の IEC 61850 通信機能を拡張する形で IEC 62351-3 に基づく TLS を実装し、MintSCADA と IED シミュレータ、WAGO 社製 PLC 間における証明書検証および暗号化通信を実現する。図 3 に、MintSCADA と IED シミュレータ、WAGO 社製 PLC 間における TLS セッション確立の処理フローを示す。TLS ハンドシェイク^{注10)} においては、SCADA と IED・PLC 双方が証明書を用いた相互認証 (Certificate) を実施し、正当な機器であることを確認した上で TLS セッションを確立する。さらに、セッション確立後は、暗号化された通信路上で IEC 61850 通信を行うことにより、通信内容の機密性および完全性を確保する。

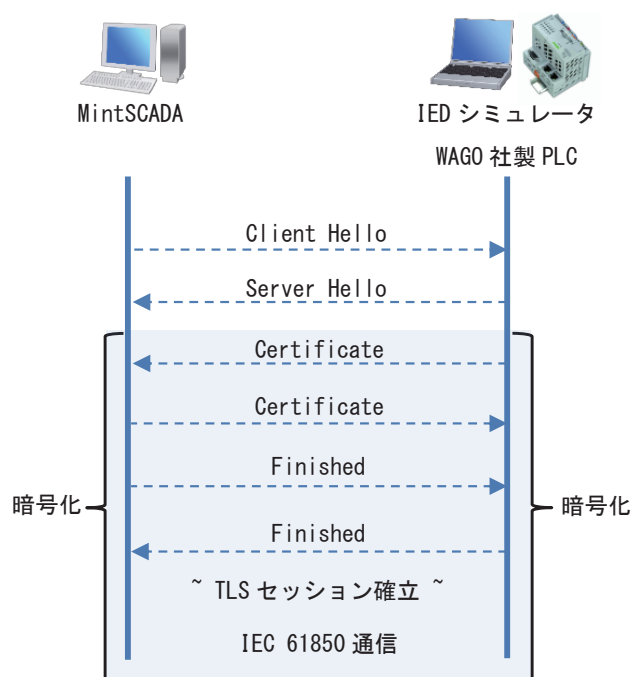


図 3 TLS セッション確立の流れ (TLS ハンドシェイク)

(3) セキュリティ機能の検証

MintSCADA と IED シミュレータ・WAGO 社製 PLC との間において、パケットキャプチャを接続することで通信データを可視化し、TLS セッション確立後、相互認証ならびに暗号化通信が可能であることを確認した。

図 4 に TLS 通信を実装した MintSCADA の平文通信および暗号化通信の様子を示す。

正当な証明書を持っていない IED・PLC からの接続要求については、TLS セッション確立時に認証エラーとして処理され、通信が開始されないことを確認している。さらに、有効期限の検証に加えて、OCSP および CRL を用いた証明書失効確認機能を適用した結果、失効済み証明書を用いた接続要求についても、同様に TLS セッション確立時に認証エラーとなり、通信が開始されないことを確認した。図 5 に、MintSCADA に表示される有効期限の検証時および認証エラー時のメッセージ画面を示す。

RBAC に基づく認可制御については、ユーザのロールに応じて利用可能な機能が適切に制限されることを確認している。具体的には、ユーザの登録、削除、変更といった管理操作機能は、RBAC 管理者のみが実行可能であり、オペレータ (OPERATOR) および閲覧者 (VIEWER) では、これらの管理操作機能を実行できないことを確認した。図 6 に、管理操作機能のユーザ登録およびロール変更の画面を示す。

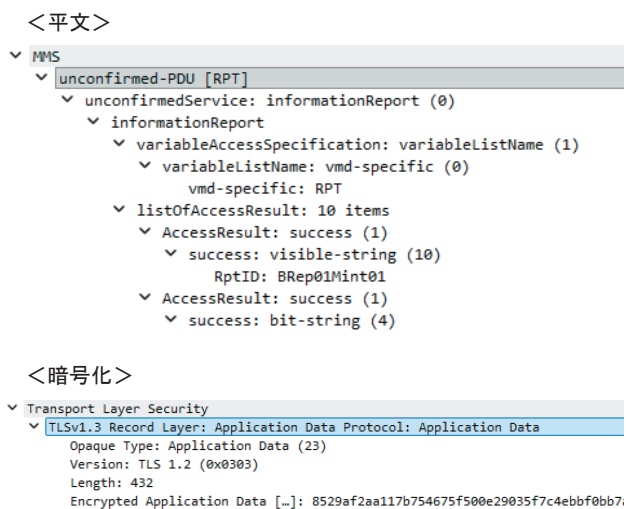


図 4 パケットキャプチャによる IEC 61850 通信

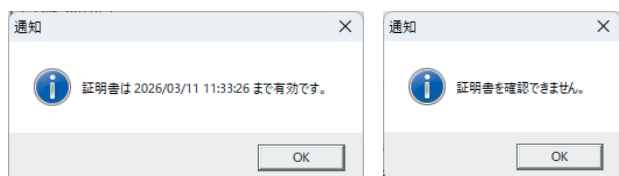


図 5 有効期限・認証エラー時のメッセージ画面



図 6 ユーザ登録およびロール変更の画面

4 検証結果から見た課題

本検証では、認証局サーバから各機器への証明書配布を USB メモリによる手動方式としたが、機器数の増加に伴う作業負担の増大や人的ミスのリスクが懸念される。実運用においては証明書配布の自動化が不可欠である。

また、監視データ点数の増加に伴い、SCADA の応答時間が増加する傾向が確認された。この要因として、暗号化・復号処理に起因する処理負荷が影響していると考えられる。リアルタイム性を維持するためには、暗号化・復号処理の効率化および高速化も不可欠である。

さらに、RBAC は IEC 62351-8 で示されている考え方ではあるが、IEC 62351-8 上で SCADA におけるユーザやロールの変更を IED や PLC へ通知する明確な手段は規定されていない。このため、RBAC 管理者が変更したユーザおよびロール情報を各機器へ一貫して反映するための仕組みを確立することが、今後の重要な課題である。

5 まとめ

本検証では、MintSCADA に対して IEC 62351 に基づく通信セキュリティおよび認証・認可機能の検証を行った。具体的には、TLS による MintSCADA と IED シミュレータ・WAGO 社製 PLC 間の暗号化および相互認証、PKI に基づく証明書管理、ならびに IEC 62351-8 に準拠した RBAC の概念に基づくユーザ認証・認可機能を実装し、その有効性を検証した。電力システムにおけるサイバーリスクの高まりを背景に、SCADA および IED・PLC のセキュリティ強化は今後一層重要となる。

本検証で得られた知見、および明確になった課題 (証明書配布の自動化や処理の高速化など) への対策を深めるとともに、電力システムの安全性向上に寄与し、より高度で信頼性の高い監視制御システムの提供を目指していく。

■参考文献

- (1) JEAG I111-2024 「電力制御システムセキュリティガイドライン」一般社団法人日本電気協会 (令和 7 年 5 月 30 日発刊)

- (2) IEC 62351-3:2023, Power systems management and associated information exchange–Data and communications security–Part 3: Communication network and system security–Profiles including TCP/IP
- (3) IEC 62351-8:2020, Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control for power system management
- (4) 黒田英次他：「IEC 62351 に基づく認証・暗号化に対応した SCADA の開発」, 電気学会保護リレーシステム研究会 PPR-26-009 (2026)

■語句説明

- 注1) SCADA：「Supervisory Control And Data Acquisition」の略称。コンピュータによる監視制御システム。
- 注2) IED：「Intelligent Electronic Device」の略称。電力設備において保護・制御・監視機能を担う装置。
- 注3) PLC：「Programmable Logic Controller」の略称。工場や設備の制御を行うための装置。
- 注4) RBAC：「Role-Based Access Control」の略称。役割に応じて操作権限を管理するアクセス制御方式
- 注5) LDAP：「Lightweight Directory Access Protocol」の略称。ユーザ情報や組織情報などを階層構造で管理する通信プロトコル
- 注6) TLS：「Transport Layer Security」の略称。データの盗聴や改ざんを防ぐための通信プロトコル
- 注7) 証明書チェーン：証明の根拠を段階的につなぐ仕組み
- 注8) OCSP：「Online Certificate Status Protocol」の略称。証明書が失効していないかを確認する通信プロトコル
- 注9) CRL：「Certificate Revocation List」の略称。認証局が発行した証明書の失効一覧をまとめたリスト
- 注10) TLS ハンドシェイク：通信を担う機器間での安全な通信路を確立するための初期交渉プロセス

黒田 英次

株式会社ミントウエーブ
技術開発部 ソフト設計グループ 所属

益子 奈々海

株式会社ミントウエーブ
電力システムソリューション事業部 所属

荒井 俊成

株式会社ミントウエーブ
電力システムソリューション事業部 所属