プラント制御システムと情報セキュリティ
Plant Control Systems and Information Security

椎木　孝斉 SHIIGI Takayoshi
松本　尚之 MATSUMOTO Naoyuki
金田　光範 KANEDA Mitsunori

発電プラントなどに代表される，大規模なプラント監視制御システムにおいては，ベンダー固有のアーキテクチャ(コンピュータのハードウェア／ソフトウェア設計仕様)と，プラントの物的防護システムに守られていたため，情報セキュリティ上の配慮は，これまでほとんど必要がなかった。しかし，システムがネットワークでつながるようになり，構成機器にも汎(はん)用の基本ソフトウェア(OS)やハードウェアが多く採用されるに伴って，外部からの侵入がきわめて容易となっており，情報セキュリティは重要な問題として無視できなくなってきている。

プラント制御システムの要件を満たすように配慮しつつ情報セキュリティ技術を適用することにより，安全性の高いシステムの構築が可能となる。

Formerly, because of the proprietary architectures provided by each vendor and physical protection from unauthorized system access, information security in large-scale plant monitoring and control systems as used in electric power generating plants was considered to be unnecessary. Now, as operating systems and hardware become less diverse and individual systems become more interconnected, the threat of invasion has become a common reality. Information security can no longer be ignored.

It is possible to construct a highly secure plant control system by adopting information security technology suitable to the particular system.

1 まえがき

プラント制御システムは，社会的に非常に重要な役割をもったシステムである。当社においても，発電監視制御システムを始めとして，数多くのプラント制御システムを構築してきており，現在さまざまな場所で運用されている。

近年のプラント制御システムでは，システムのオープン化が進んでいる。このオープン化の流れは，多くのメリットをもたらす一方で，セキュリティ問題をプラント運転制御にもち込む危険性も増加させており，プラント制御システムにおけるセキュリティ機能の設置／充実が重要な問題となってきている。

しかし，プラント制御システムへの安易なセキュリティ機能の導入はシステムの性能低下や操作性の低下，保守業務の負担増といったデメリットが懸念されるため，プラント制御システムに適した方法でのセキュリティ機能の適用／開発が必要となる。

2 背景(プラント制御システムの現状)

従来のプラント制御システムにおいては，単独の閉じたシステムであったり，システムを構成する機器に，ベンダー固有の製品およびプロトコル(データ送受信のための手順や規約)が採用されていたりすることにより，システム自身がある程度のセキュリティを確保していた。

また，エリアの入退出管理などの物理的セキュリティ対策を行うことによっても，システムのセキュリティを確保してきた。しかし近年，プラント制御システムを取り巻く環境にも以下のような変化が見られるようになった。

2.1 大規模ネットワーク化

プラント制御に直接かかわる制御系のシステムと，プラントの運転データなどを利用する特定の業務系システム，さらには社内の一般情報システムとが接続され，階層的な大規模なネットワークシステムを構成するようになってきた。したがって，ネットワークにつながっていればどこからでも容易に侵入される危険性が増えている。

2.2 オープン化

プラント制御に直接かかわる制御装置では性能や信頼性の問題から，現在もベンダー独自の製品やプロトコルが用いられている例が多いが，上位の監視系システムなどにはTCP/IP(Transmission Control Protocol/Internet Protocol)などのオープンなプロトコルが採用され，構成機器のOSなども汎用のものが採用されるようになってきた。したがって，部外者であっても容易にアクセス可能になってきている。

2.3 マルチベンダー化

2.2のオープン化に伴い，異なるベンダー間のシステムの相互接続が容易に行われるようになってきた。

汎用製品を使うことで，システムのコストを下げることはできたが，逆にセキュリティのリスクは拡大している。

3 プラント制御システムにおける脅威

情報セキュリティの位置づけを図1に示す[1]。情報セキュリティでは主として図の網掛け部分を対象としている。

プラント制御システムにおいても，災害や故障に対する対策や，システムの誤動作，停止などに対する対策については従来から考慮され，十分な対策が施されてきた。一方，故意・過失に対するデータの漏えい・改ざん・破壊，システムの不正使用に対する対策はこれまで余り考慮する必要がなかった。しかし，2章で述べたような環境の変化に従い，プラント制御システムにおいても，この範囲での脅威が増大してきており，早急な対策が必要な状況となってきている。

そこで以下ではまず，プラント制御システムの各階層において，問題となるセキュリティに関する脅威の整理を行う(図2)。

3.1 制御系ネットワーク

制御系ネットワークにはプラント制御を行う制御機器が直接接続されており，システムとして守るべき重要度がもっとも高いところである。制御系ネットワークにおける代表的な脅威を以下に挙げる。

(1) 不正な機器接続，不正パケット(ユニットとして送られる一定長に分割されたデータ)送信によるネットワークの混乱
(2) ネットワークを流れるデータの改ざん，盗用
(3) 現場機器の保守時における作動状況誤認識
(4) コントローラのパラメータ設定ミス

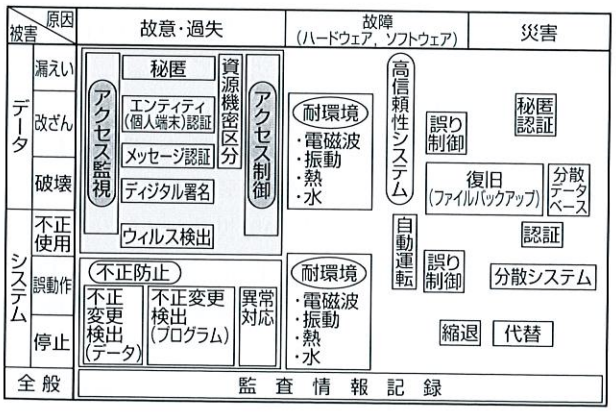

図1．情報セキュリティ技術の位置づけ　故意(悪意)・過失が原因で発生する，情報の漏えい・改ざん・破壊，およびシステムの不正な利用を阻止するのが目的である。

Positioning of information security technologies

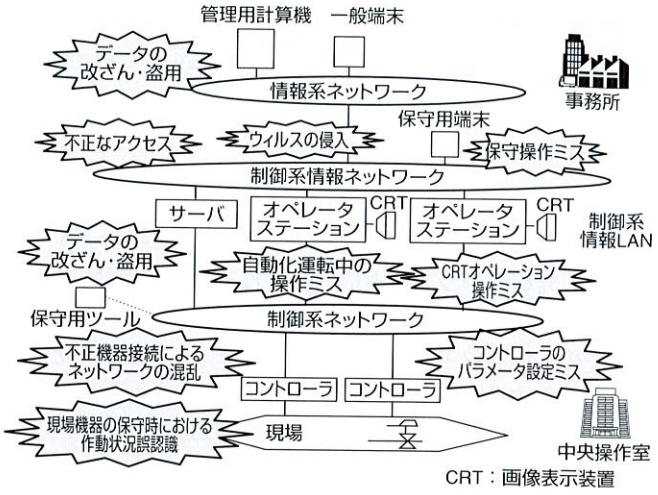

図2．プラント制御システムにおける脅威　システムを構成する各ネットワーク階層でさまざまなセキュリティに関する脅威が存在する。

Security threats to plant control systems

3.2 制御系情報ネットワーク

制御系情報ネットワークは操作員がプラントの監視を行うために必要な機器が接続されているネットワークである。制御系情報ネットワークにおける代表的な脅威を以下に挙げる。

(1) 操作員のスキル不足や思い込みによる誤操作
(2) 現場機器(ポンプ，バルブなど)の保守中における関連機器の誤操作
(3) 重要パラメータの設定ミス
(4) 構内作業員，ソフトウェア保守員をよそおった部外者によるシステム破壊，プラントの誤動作／誤検出。
(5) ソフトウェア保守時のメディア媒体からのウィルスの侵入

3.3 情報系ネットワーク

情報系ネットワークは事務所などに設置される業務用のネットワークである。情報系ネットワークは制御系情報ネットワークと接続され，プラントデータの長期保存を行う管理用計算機などが設置される。情報系ネットワークの代表的な脅威を以下にあげる。

(1) 初期パラメータやログデータの改ざん・盗用
(2) プラントデータの損傷・喪失

4 技術課題と機能要件

4.1 プラント制御システムのセキュリティ機能

情報システムにおけるセキュリティ評価基準としては，CC(Common Criteria)が国際標準として採用される予定である。CCではセキュリティ製品やシステムが備えるべき機能要件の規定も行なっており，全部で11の機能要件

表1．機能要件の分類
Classes of security functional requirements

機能クラス	概　要	プラント制御システムとして必要とされる要件
セキュリティ監査	セキュリティ事象に関連した情報の認識，記録，格納，分析に関する要件	セキュリティ侵害の操作員への迅速な通知やセキュリティイベントのログの記録など
通信	データ通信への参加者の識別を保証する否認防止に関する要件	―
暗号サポート	暗号鍵(かぎ)生成／配布／失効の管理，データの暗号化／復号，ディジタル署名の生成／検証などの暗号操作に関する要件	性能面などプラント制御に影響を与えない暗号方式の採用
ユーザーデータ保護	アクセス制御，情報フロー制御，ユーザーデータのインポート／エクスポート時のセキュリティ属性保護，ユーザーデータ伝送時の機密保護などに関する要件	プラント操作に適した形でのアクセス制御(プラントの運転状態などによる動的な権限の変更)，プラントデータの改ざん防止など
識別と保証	ユーザーの身元を確立し，かつ検証するための機能要件	操作員の負担にならない認証方法や操作員の役割に応じた認証など
セキュリティ管理	セキュリティ属性や，セキュリティ機能に関連するデータ(例：認証データ，セキュリティ方針データベース)などの管理に関する要件	プラント制御に適した形式でのユーザーの役割などの設定／管理，アクセス権限データの管理など
プライバシー	他者によるアイデンティティ(身元)の発見(探り出し)と誤使用の防止に関する要件	―
TOE セキュリティ機能保護	セキュリティ機能を提供するメカニズムと内部データの正当性および保護に関する要件	セキュリティ機能が喪失した場合でも，プラント制御への影響を最小限にするなど
資源利用	資源の耐障害性，優先度制御，資源割当てに関する要件	セキュリティ機能が他の優先度の高いプラント制御機能に影響を与えないこと
TOEアクセス	ユーザーセッション(TOE と利用者との間の対話路)確立の制御に関する要件	場所，時間，プラントの運転状態などをセキュリティ属性として，アクセス制御を行う必要がある
信頼経路／チャネル	利用者と TOE との間の高信頼性通信路に関する要件	―

TOE：Target of Evaluation(評価対象製品)
(注)機能クラスの分類および概要は文献(2)による。

に分類されている。CC の機能要件[2]および該当するプラント制御システムに必要な要件を表1にまとめる。[3]

4.2　セキュリティ機能適用の課題

セキュリティ機能をプラント制御システムに適用する場合，以下のような課題が存在する。

4.2.1　システム全体のレスポンス低下　データの暗号化／復号，システム機器の相互認証などの処理時間によるレスポンス低下が考えられるが，プラント制御システムにおいては，プラント機器の動作に追従した実時間処理が要求され，レスポンス低下に対する許容度はかなり小さいものとなる。

4.2.2　操作員や保守員の負担増　パスワードや，IC カードなどによる個人認証を行なった場合，操作員や保守員にパスワード入力や，IC カードの提示といった負担が生ずる。特に，プラント制御においては，緊急時に操作員や保守員が迅速に操作可能であることが要求されるため，操作員や保守員に対する余分な負担は，極力排除する必要がある。

4.2.3　コストアップ　もともとセキュリティの問題には，単にソフトウェア／ハードウェアを導入すればよいのではなく，教育，監査といった人間系の要素が大きく絡み，セキュリティにはコストが掛かると言われている。プラント制御システムにおいては，その上，上記 4.2.1，4.2.2 の要件のため，通常のセキュリティ用ソフトウェア／ハードウェアをそのままシステムに導入することには問題が多く，独自のセキュリティ技術の開発が必要となる場合もある。さらに，その場合においてもネットワークに接続される機器が汎用製品からベンダー固有の機器までさまざまであり，一筋縄ではいかないことなどが想定され，セキュリティ機能構築のためのコストを押し上げる要因となってしまう。

4.2.4　マルチベンダー／オープン化と逆行　セキュリティ機能の作り込みを行いすぎると，汎用製品のシステムへの組込みが困難になってくる。そして，マルチベンダー／オープン化のためのセキュリティ機能であったものが，逆にマルチベンダー／オープン化を阻害してしまう。

以上の中で 4.2.1，4.2.2 は，プラントの安全性と絡む部分であり，特に留意する必要がある。

これらの課題を克服する要素技術の開発，すなわち，高速な暗号化／復号機構の開発や，オペレータの負担にならない個人認証のしくみの開発が急がれることはもちろんであるが，現時点では，これらのマイナスをゼロにすることは困難である。そのためどのレベルまでセキュリティを考慮するかは，これらのマイナス要因と安全性とのトレードオフを考える必要がある。

また，システムに均一なセキュリティを適用するのではなく，重要度などに応じて，適用するセキュリティレベルを柔軟に変化させたシステムを構築する必要がある。

さらに，プラント制御システムへのセキュリティ技術適用には，プラント制御系のセキュリティポリシー定義を含め，プラント制御に関する全体のエンジニアリング力が求められる。

5　システム要件(システムコンセプト)

以上の点を踏まえ当社において，現状プラント制御システムに必要と考えている要件について述べる。

5.1　操作員の認証

プラント制御の場合，一般のオフィス環境とは異なり，各操作用端末が各個人の専用となることはなく，さまざまなレベルの操作員によって入れ替わり立ち替わり操作される。したがって，このような状況では，プラント内の各エリアへの入退出時の認証だけではなく，各操作用端末ごと

にどのようなレベルの操作員であるかの認証が必要である。

このような認証の具体化の方針としては，プラント内の各エリアへの入退出時にはICカードなどの接触型の認証用媒体を用い，各操作用端末での認証では無線カードなどの非接触型媒体を用いるといった，操作員が操作用端末間を移動するときに負荷を感じさせないような認証システムが望ましい。

5.2 操作員のアクセス制御

プラント制御においては，操作員の役割は基本的に固定しているが，1人の操作員の役割でも，プラントの運転状況あるいは保守状況，操作員の勤務体制，操作員の操作場所などによってさまざまに変化する。また操作員のスキル(技能レベル)などによって，各操作員ごとの役割も異なったものとなってくる。また，状況によって各操作員の役割を交換したり，譲渡したりする必要も生じてくる。このような状況に対応できる柔軟なアクセス制御のしくみを考える必要がある。

具体的には，操作員を大まかなカテゴリーに分けて，そのカテゴリーごとのアクセス権をプラントの運転状況や保守状況などに応じて，ダイナミックに変更していくことを考える。

これにより，過失や，システム不正使用によるダメージをある程度避けることができる。

5.3 ネットワークに接続する機器の認証

不正な機器の接続による，盗聴やネットワークの混乱などの弊害を避けるため，ネットワーク上につながれた，計算機，制御装置，PI/O(プロセス入出力)装置などさまざまな機器自身の正当性の保証を行う必要がある。

このような目的のためには，通信時に機器相互の認証を高速で行う通信用ミドルウェアを開発し，そのミドルウェアに基づいてシステムを構築するようなアプローチが望ましいと考えられる。

5.4 データの暗号化

プラントで保持しているさまざまなプロセスデータ，性能データなど，外部に出したくないデータを暗号化した形でディスクに保存する。マンマシン機能などでそれらのデータを利用し，表示，印字を行う場合，復号処理をして利用する。また，ネットワーク上の通信データの暗号化も考える必要がある。

このためには，上記の通信ミドルウェアの一機能として，高速の暗号化／復号通信機能をもたせることが必要である。

5.5 プラント固有ユーザーインタフェースとの融合

プラント制御システムにおいてはセキュリティが脅かされた場合，速やかに操作員への通知が必要となる。そのためには，プラント固有のユーザーインタフェースとセキュリティ機能との融合，調和を考える必要がある。

例えば，セキュリティが脅かされた場合に警報を出力したり，大型スクリーンに表示したりといったことが考えられる。

以上のセキュリティ機能については，今後検討を進めていく予定である。

6 あとがき

プラント制御システムに対するセキュリティ技術への取組みはまだ始まったばかりである[4]。

セキュリティシステムには，誤操作を減らし，安全性を高めることができるといった直接的なメリットや，汎用製品を利用しても安全にシステムを組むことができるといった間接的なメリットがあり，今後のプラント監視制御の自動化や高度化のニーズに対応するためにはますます重要なものとなっていくと考えられる。

今後も，システムにかかわるユーザー／ベンダー双方がセキュリティ対策の重要性を十分認識し，プラント制御システムに適した形でのセキュリティ技術の適用および開発の検討を進めていく必要がある。

文 献

(1) 才所敏明，他．情報セキュリティ技術体系とその動向．東芝レビュー．52, 2, 1997, p. 4-7.

(2) 情報処理振興事業協会 セキュリティセンター．Common Criteria：機能要件．URL：http://www.ipa.go.jp/SECURITY/ccj/cotf/cc_func.htm.

(3) 情報処理振興事業協会 セキュリティセンター．Common Criteria セキュリティ要件解説書 機能要件編 CS 2 相当抜粋．第1.0版．1998, 155 p.

(4) 通商産業省 大規模プラント・ネットワーク・セキュリティ対策委員会．大規模プラント・ネットワーク・セキュリティについて．中間報告書．1998, 124 p.

椎木 孝斉 SHIIGI Takayoshi
電力システム社 府中電力システム工場 エネルギー共通技術システム部。技術業務支援システムの開発・設計に従事。情報処理学会会員。
Fuchu Operations-Power Systems

松本 尚之 MATSUMOTO Naoyuki, D. Sci.
電力システム社 府中電力システム工場 エネルギー制御開発部，理博。
発電監視制御計算機システムの開発・設計に従事。
Fuchu Operations-Power Systems

金田 光範 KANEDA Mitsunori
電力システム社 電力事業部 情報技術システムセンター担当部長。技術業務支援システムの企画，開発に従事。情報処理学会会員。
Power Systems Div.