# 制御システムのサイバーセキュリティ：
# 多層防御戦略

作成：Idaho National Laboratory（米国アイダホ国立研究所）

2006年5月

邦訳： 一般社団法人 JPCERT コーディネーションセンター

本翻訳文書は、一般社団法人JPCERT コーディネーションセンターが、原書の著作権を保有する アメリカ国土安全保障省（U.S. Department of Homeland Security: DHS）の許諾を得て翻訳したものです。

日本語版の内容について、原書に沿ってできるだけ忠実に翻訳するよう努めていますが、完全性、正確性を保証するものではありませんので、必要に応じて CSSP（Control Systems Security Program）のホームページより原書 ″Control Systems Cyber Security: Defense in Depth Strategies″ をご参照ください。

また、翻訳監修主体は本文書に記載されている情報により生じる損失または損害に対し、いかなる人物あるいは団体にも責任を負うものではありません。

なお、当文書に関わる最新情報は以下の CSSP のホームページをご参照ください。

http://www.us-cert.gov/control_systems/

# 目次

## キーワード

多層防御、産業用制御システム、SCADA、PCS、サイバーセキュリティ、緩和策、ファイアウォール、IDS、侵入検知、暗号化、DMZ

## はじめに

多数の公共・民間分野にわたる横断的な情報インフラには、ITの配備とデータ通信に関して共通の特性がいくつかある。特に制御システム分野に言えることだが、大部分のシステムは堅牢なアーキテクチャを採用し、外部ネットワーク、業務ネットワーク、制御システムネットワークの統合を推し進めることで業務の強化とコスト削減を図っている。しかし、複数のネットワークを統合するという戦略により組織のセキュリティを大幅に低下させる脆弱性が引き起こされることが多く、ミッションクリティカルな制御システムがサイバー攻撃の脅威にさらされる恐れがある。

本書では、制御システムネットワークを使用している組織向けに、以下のことが要求される多層情報アーキテクチャを維持しつつ、「多層防御」戦略を策定するための指針と方向性を示す。

- さまざまなフィールド機器、遠隔計測収集システム、産業用プロセスシステムの保守
- 遠隔データ通信またはモデム経由による各種施設へのアクセス
- 顧客または企業運営のための公共サービス
- 制御システム領域、外部インターネット、その他の提携先との接続が必要な堅牢なビジネス環境

## 背景

製造業、輸送業、エネルギーなど主要な産業を支える重要インフラシステムは、その指令制御に情報システムを多用している。重要インフラ/主要リソース（critical infrastructure/key resource：CI/KR）システムは依然として旧来の制御システムに大きく依存しているものの、新しい通信技術に移行しつつある。その結果、制御システムの多種多様で独自の構造は、共通の通信プロトコルやオープンアーキテクチャ標準に置き換えられている。これには、プラスの影響とマイナスの影響がある。

移行により、制御システムの利用者や製造者が新しくより効率的な通信手段を提供できるようになるとともに、データの堅牢性が高まり、製品化期間が短縮され、相互運用性が向上する。しかし、制御システムの利用者が多くの機能を利用できるようになることで、新たなリスクが生じる。制御システムに関わるCI/KR情報インフラが隔離されていたときには存在しえなかった、サイバー関連の脆弱性とリスクが生じている。電力部門がそうであるように、複数のCI/KRシステムが相互に依存していることは、2003年の北米の停電など、いくつかの事例で示されている。

制御システムコミュニティにおいて高度な相互運用性と制御を可能にしている新しいプロトコルと通信規格は、インターネットやネットワークの分野で悪用され危険にさらされてきた技術と同じ技術である。歴史的に、制御システムのセキュリティは閉ループシステムの中で問題を見つけ特定することを指していたが、現在では不正侵入や攻撃が、対処すべき新たな問題になりつつある。

図1 – 企業領域と制御領域の従来の分離に、企業領域と制御領域を分離する従来の構造を示す。このアーキテクチャが、データ共有、データ取得、ピアツーピアデータ交換などの業務運用の手段となっていた。しかし、システムのセキュリティは、複雑なアーキテクチャや制御システムLAN上の資源の動作の仕組みを理解している者は、いたとしてもごく少数であるという事実に基づいていた。この「隠すことによる安全」は、外部との通信接続がなく物理的なセキュリティだけに注意していれば済む環境でうまく機能する。

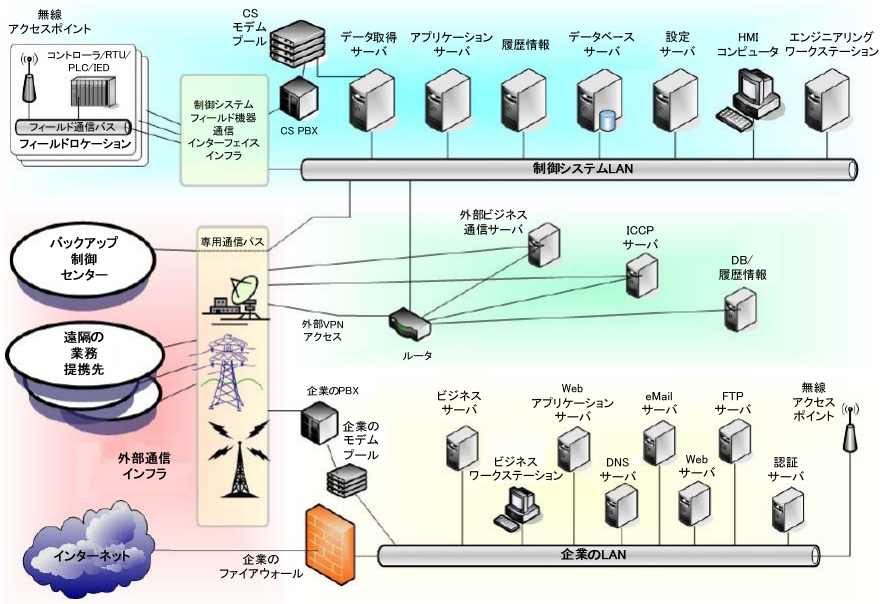


**図1 – 企業領域と制御領域の従来の分離**

## 現代の制御システムアーキテクチャの概要

今日の競争市場において、隔離されていた制御システムネットワークは相互に接続されつつある。これらのネットワークを接続する際や、ITコンポーネントを制御システムに導入する際に、以下の理由からセキュリティ上の問題が生じる。

- オートメーションシステムと制御システムに対する依存度の増大
- 外部ネットワークとのセキュアでない接続
- 既知の脆弱性のある技術の利用
- 制御システム環境でのサイバーセキュリティに関するビジネスケースの不足
- 制御システム技術のセキュリティは限定的であり、ベンダが提供するセキュリティ機能は、一般に管理者がその機能に気付いた場合にだけ有効にされる
- 制御システムの通信プロトコルにはセキュリティ機能がない
- 制御システムの設定と操作に関してかなり多くの情報が公開されている

制御システムの運用上のセキュリティは、運用するシステムの信頼性のレベルとして業界で定義されてきた。外部の信頼できないネットワークから完全に隔離することで、通信セキュリティのレベルを下げ

ることができた。運用に対する脅威は、施設や工場への物理的なアクセスを指していた。そのため、情報インフラのほとんどのデータ通信では、限定的な許可やセキュリティ管理で済んでいた。運用上の指令、指示、データ取得は、すべての通信が信頼できる閉じた環境で行われていた。一般に、権限を持つオペレータだけがシステムにアクセスできたため、ネットワーク経由で送られる指令や指示は、確実に目的地に届き許可された機能を実行すると見なすことができた。

このような仕組みは、効果的なネットワークやITサイバーセキュリティシステムとは明らかに大きく異なる。現代のITアーキテクチャと、有効なセキュリティ対策がとられていない隔離されたネットワークを統合するのは簡単ではない。相互接続のための最も簡単な手段は、ルータやスイッチを使用して単純に接続することであるが、誰かが不正にアクセスした場合、システムへの無制限のアクセスを許してしまうことになる。図2 – 統合されたネットワークに、統合されたアーキテクチャを示す。

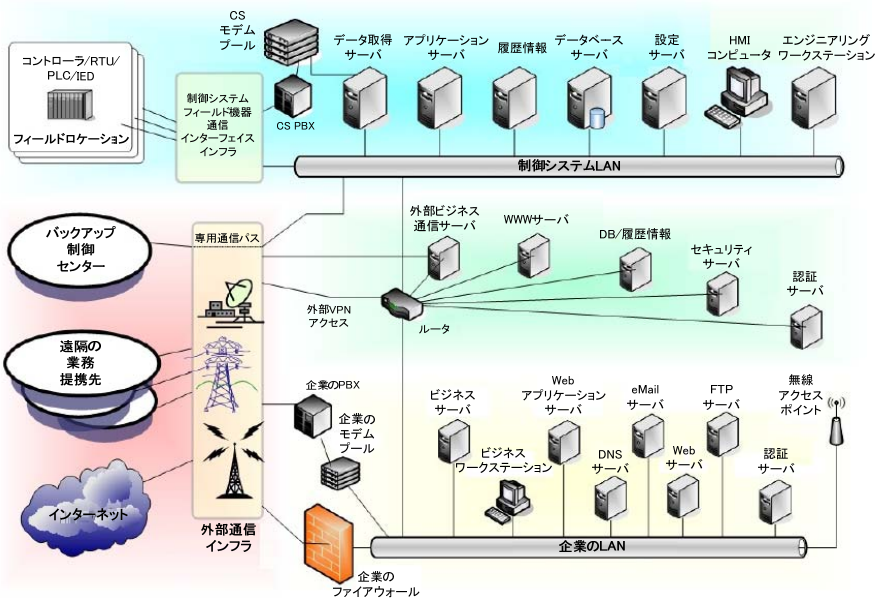


**図2 – 統合されたネットワーク**

図2 – 統合されたネットワークから、このようなアーキテクチャが侵害された場合、社内LAN、制御LAN、通信LAN上の基幹システムにアクセスするためのさまざまな手段を攻撃者に提供することになるのは明らかである。また、アーキテクチャの特性により、さまざまな情報源からのデータ交換が必要となるが、これは明らかに攻撃者に利用されるおそれがある。[1]

[1] この種のアーキテクチャ、及びバックエンド制御システムは、外部攻撃にも内部攻撃にも脆弱である。内部攻撃者は IT システムに対する大きな脅威であるが、図 2 に示すようなアーキテクチャでは、多数の、緊密に接続された、保護されていない、情報インフラからのアクセスを許すことで、問題がさらに悪化する。従来、制御システムに対する脅威は部内者によるものがほとんどであったが、新たな接続性によって外部攻撃者による攻撃の可能性も生まれる。

## 制御システムにおけるセキュリティ上の課題

制御システム内の運用を促進する、業務運営のための社内インフラなど、現代のTCP/IPベースの環境には、対処すべき技術関連の脆弱性が存在する。従来、これらの問題は社内のITセキュリティ組織の担当であり、一般にきわめて重要な情報資産を保護するセキュリティポリシーと運用計画によって管理されてきた。制御システムがこれらの大きなアーキテクチャに属するようになるにつれて、制御システム領域にも対応するセキュリティ手順を提供することが主な関心事となっている。ベンダ固有のプロトコルや旧来システムにおける安全であるという思い込みは基幹システムを保護するには十分ではないため、現代的なネットワーク通信には、制御システム領域で解決すべきセキュリティ上の問題がある。

オープンシステムアーキテクチャにおける脅威のうち、制御システム分野にもそのまま当てはまるものとしては、悪意あるモバイルコード（システムに対して適用可能な場合）、コードの操作による権限の昇格、ネットワークの偵察とデータ収集、隠れたトラフィック分析、境界防衛を通過した、あるいは境界防衛の周辺におけるネットワークへの不正侵入などが挙げられる。制御システムネットワークへの侵入が成功すれば、制御システムプロトコルのリバースエンジニアリング、操作卓への攻撃、結合したピアネットワークや遠隔設備への不正アクセスなどの新たな問題が生じる。情報セキュリティと情報保証を制御システムの領域に全面的に適用するには、従来のITアーキテクチャと制御システム技術の主な違いについて理解する必要がある。

リスク緩和の観点から、ITセキュリティ技術を制御システムに単に配備するだけでは有効な解決策にならない場合がある。最新の制御システムでは、ITネットワークや業務ネットワークで使用されているものと同じプロトコルが使用されるが、制御システムの機能の性質上、実証済みのセキュリティ技術であっても適合しない場合がある。エネルギー、輸送、化学などいくつかの分野では、時間内に処理を終える必要性があるため、セキュリティ対策に伴う待ち時間や「スループット」の問題により、受け入れがたい遅延や劣化が生じたり、システムの性能が許容できないレベルにまで低下したりする恐れがある。

従来のIT環境と制御システム環境には、セキュリティに関連して、いくつかの大きな違いがある。表1に、組織が強化すべき一般的なセキュリティ要素と、それに対するIT分野での対処方法を、制御システムのアーキテクチャと対比させる形で示す。[2]

[2] NIST SP 800-82 には、これらの差違に関する簡潔な説明が記載される予定である。

| セキュリティ項目 | IT | 制御システム |
|---|---|---|
| ウィルス対策/モバイルコード | 一般的<br>広く使用 | 効果的な配備は<br>一般的でない/不可能 |
| サポート技術の寿命 | 2～3年<br>多様なベンダ | 最大20年<br>単一ベンダ |
| 外部委託 | 一般的<br>広く利用 | 運用は外部委託されることもある<br>が、サービス提供者は多くない |
| パッチの適用 | 定期的<br>計画的 | まれ、非計画的<br>ベンダ固有 |
| 変更管理 | 定期的<br>計画的 | 厳格に管理され複雑 |
| 時間に厳しい処理 | 一般に遅延を許容 | 遅延は許されない |
| 可用性 | 一般に遅延を許容 | 24時間365日(連続稼動) |
| セキュリティ意識 | 民間部門でも公共部門でも<br>中程度 | 物理的セキュリティ以外は貧弱 |
| セキュリティテスト/監査 | 優れたセキュリティ<br>プログラムに含まれる | 停電に備えたテストを時折実施 |
| 物理セキュリティ | 安全（サーバ室など） | 遠隔/無人<br>安全 |

表1 - ITと制御システムのセキュリティの視点

### セキュリティプロファイルと攻撃手法

制御ネットワークが、単独の孤立したネットワークから、企業のIT環境と共存する相互接続されたネットワークに進化するにつれて、セキュリティ上の脅威が生じる。たとえば、ウィルス、ワーム、寄生コードの形のモバイルコードは、ネットワーク化された制御システム環境においても非制御システム分野と同じく容易に発症する可能性がある。コントローラやリレーなどファームウェアが組み込まれている装置に対しては、一般に、悪意あるモバイルコードはネットワークの伝搬を通じて影響を与えることはできない。しかし、これらの装置によって定期的にダウンロードされるコンパイル済みコードが悪意あるマルウェアによって破壊されれば、非常に大きな損害が生じる可能性がある。[3]

対処が必要な重大なサイバーセキュリティの問題には、以下のものに関連するものが含まれる。

- ネットワーク境界におけるバックドアやセキュリティホール

[3] この種のセキュリティ侵害が発生する可能性は、現時点では高くないが、将来的な攻撃シナリオを検討する際には、そのような攻撃ベクトルを無視すべきではない。

- 一般的なプロトコルの脆弱性
- フィールド機器への攻撃
- データベース攻撃
- 通信の乗っ取りと中間者（Man-in-the-middle）攻撃

攻撃ベクトルを理解することは、効果的なセキュリティリスク緩和策を立てる上で不可欠である。これらの脆弱性を軽減するために、制御システムコミュニティにおいて、攻撃ベクトルに関する知識レベルを高める必要がある。効果的なセキュリティのためには、制御システムのオペレータとベンダの両者が、アーキテクチャがどのようにして危険にさらされるかについて深く理解することが必要である。[4]

いくつかの詳しい技術的議論が、DHSによる制御システムセキュリティプログラムで、DHS Computer Emergency Readiness Team（US-CERT）を通じて提供されている。この勧告文書に記載されているさまざまな攻撃ベクトルの議論を読むことで、多層防御戦略の有効性を理解できる。

*ネットワーク境界を通じたバックドア攻撃*[5]

一般的なネットワーク環境と同様に、制御システム領域にも無数の脆弱性とセキュリティホールがあり、攻撃者に不正アクセスを許す「バックドア」となる可能性がある。バックドアは、アーキテクチャの境界における単純な弱点の場合もあれば、忘れられていたり、認識されていなかったり、単に軽視されたりしている組み込み機能の場合もある。敵対者（脅威）は、物理的にアクセスすることなくその領域にアクセスできることが多く、検出したあらゆるアクセス機能を利用する。現代的なネットワーク、特に制御システム分野のネットワークには、十分なセキュリティ分析をせずに配備された機能が含まれていることが多く、発見されると攻撃者にアクセスを許す恐れがある。このような「バックドア」は、ネットワークのさまざまな場所で無意識のうちに作り出されることがあるが、最も問題となるのはネットワーク境界である。

ネットワーク境界の構成要素に着目すると、最新のアーキテクチャには信頼できるアクセスを可能にするための技術が提供される。たとえば、ファイアウォール、公共サービス、無線アクセスがある。これらの技術は、提携しているネットワーク間での高度な通信を可能とし、より大きく複雑な情報インフラのサブシステムとなることが考えられる。しかし、これらの構成要素にはセキュリティ上の脆弱性がある可能性があり（実際に多い）、攻撃者はそれを発見して利用しようと試みる。

セキュリティ保護されていない無線アクセスは、多くの組織で頻繁に発生する問題である。無線通信の使い勝手が良いことや、無線技術の配備がセキュリティ上どのような意味を持つかについて十分に理解されていないなどの理由により、セキュリティ保護のない状態で配備されることが多い。また、工場のフロアでは、壁に穴を空けてケーブルを敷設する必要がある従来の有線インフラよりも無線技術のほうが容易に配備できる。

[4] 攻撃の技術的な仕組みは、本書の範囲を超えている。

[5] http://www.us-cert.gov/control_systems/pdf/backdoor0503.pdf

無線通信の一般的なセキュリティ上の問題として、既定の設定が残っていることが挙げられる。攻撃者は無線通信ポイントを発見すると、無線ネットワークが元来備えている機能を利用するとともに、SSID（サービスセット識別子)ブロードキャスティング、限定的なアクセス制御、暗号化の欠如、限定的なネットワーク分割を利用する。

適切なパッチ管理プログラムを利用することで、システムの安全を維持する際の複雑な作業の多くを回避できるが、地理とアクセスしやすさのどちらも重要な場合、制御システムユニットに対する大きな問題がある。遠隔地に配置され、遠隔接続の通信を経由してアクセスできる制御システム要素に対しては、特別な留意が必要である。システムが商用のオペレーティングシステムを基にしている場合、サービス運用妨害、権限の昇格、あるいはトロイの木馬や論理爆弾などの秘匿ツールといった攻撃が考えられる。

遠隔接続機能が一般的になるにつれ、制御システムへのアクセスを容易にするセキュリティ境界は社内レベルや遠隔オペレータレベルにまで後退している。制御システムにアクセスできるコンピュータ資源のセキュリティが侵害されることは、制御システム自体が侵害されることと同じである。ネットワークへの制御データの傍受、改ざん、再注入、攻撃者が制御領域内で権限を昇格させ、制御信号通信ループ全体にわたってエンジニアリングレベルの命令を実行する可能性などの問題が考えられる。

制御システムネットワークの歴史的な特性、特にセキュリティに影響する平文トラフィックや特有の信頼関係に起因する特性などを考えると、無線アクセスポイントを経由する制御領域への不正アクセスは、攻撃者にとって非常に効果的なバックドアとなり、セキュリティ境界を迂回することも可能となる。

多くのCI/KR分野の組織は、確実な情報伝達のために顧客、プロバイダ、提携先に公的にアクセス可能なサービスを通じてデータを提供している。これらのサービスは、電気や水道など多くの分野の業務運営にとって非常に重要である。この分野では、負荷予測の計算、将来の請求、および関連する事業情報のデータを提供しているためである。これらのサービスは公共分野であるため、アクセス制限なし、もしくはわずかなアクセス制限でインターネットからアクセスできることが多い。通常、これらのサーバ上のデータは、（制御領域から収集された後で）業務領域から提供されたり、公共領域から取得されたりする。

この相互接続された機能は、効果的ではあるものの、攻撃者が保護された業務ネットワークや、制御システムネットワークへのアクセスを獲得するためのベクトルにもなる。多くの場合、攻撃者は、操作、顧客、ファイル転送に関する重要な情報をこれらの公共サーバから収集する。さらに、そのサーバがセキュリティ侵害されると、攻撃者は権限を昇格させ、バックエンドの業務ネットワークまたは制御ネットワークとの通信チャネルを利用する恐れがある。

公共サーバと内部ネットワークを分離するファイアウォールが設置されたネットワークは、この種の攻撃を防ぐのが難しいことが多い。WebサーバやFTPサーバなどの外部のサービスを通じて情報が確実に提供されるためには、Webサーバから内部のデータベースや履歴データベースへの通信が必要となる。この接続はファイアウォール経由で行われる。ファイアウォールとWebサーバの間の信頼関係が効果的なセキュリティ対策がないまま配備されると、外部から内部ドメインへデータが流入するのを許すことになる。このデータが不正なデータで、信頼しているWebサーバを侵害した攻撃によって生成されたものである場

合、攻撃者は、業務LANまたは制御システムLAN上の内部サービスにアクセスするための経路を獲得する。

一般に、業務機能とセキュリティの間は微妙なバランスが取られている。このバランスを正しく評価し頻繁に見直す必要がある。生産性とアクセス性を向上させるために現代的な技術を配備するには、業務ネットワークや制御システムネットワークへのバックドアを防ぐために特別な注意が必要である。

*一般的なプロトコルを使用した攻撃: OPC/DCOM攻撃*[6]

現代的なオペレーティングシステムがもたらす制御システムへの影響は大きい。この数年間でますます多くの組織が、自身の環境でObject Link and Embedding（OLE）、Distributed Component Object Model（DCOM）、Remote Procedure Call（RPC）など、オペレーティングシステムにおけるサービスを使用し始めた。OLE for Process Control（OPC）は、これらのサービスに基づくリアルタイムデータ通信標準である。多くのシステムがMicrosoftベースのOPCモデルから離れつつあるものの、OPCはさまざまな制御システム装置との効率的な接続のために広く使用されている。

歴史的に、OLE、COM、DCOMによって提供されるデータアクセス標準は、一般のコンピューティングプラットフォームで広く利用されており、引き続き重要な攻撃対象となっている。従来隔離されていた制御ネットワークを業務環境と統合することで、攻撃者が悪用する新しい環境ができることになる。ここで非常に興味深い問題は、一般的なネットワークに対する従来のリスク緩和策が、制御システムアーキテクチャでは必ずしも効果的または現実的でないことである。

制御システムで使用されているオペレーティングシステムやアプリケーションにセキュリティパッチを適用するのは容易ではない。変更前に厳格なテストを実施し、変更によって運用に影響がないことを確認する必要がある。このため、セキュリティパッチを適用し、さらにセキュリティ上の脆弱性の影響を緩和することが困難になる。たとえば、制御システムで一般に使用されているMicrosoft XPのSP2では、DCOMを無効にすることで、一部のモバイルコードの攻撃に関連するセキュリティ上の問題が軽減される。このパッチを、相互運用性のためにOPCが使用されている実稼動環境に配備すると、DCOM上のOPCが動作しなくなる。このパッチを生産設備に適用することで、制御システムにおいて完全に機能が停止したり、予期せぬ不合理な動作が生じたりするという例がいくつか報告されている。

制御システムと現代的なネットワーク技術を統合することで、セキュリティ上の脆弱性が生じる。これらの脆弱性の多くには解決策や回避方法はあるものの、制御システムアーキテクチャにおいてそうした緩和策を導入することが現実的であるとは限らない。

*フィールド機器を通じた制御システムの攻撃*

制御システムのアーキテクチャは通常、終端のエンドポイントと遠隔計測装置へのリモートアクセス機能を備えている。場合によっては、フィールド機器自体が、電話や専用の手段などでアクセスできる機能を備えている。運用データと保守データを収集できるように、現代的な一部の装置にはファイルサー

[6] US-CERT の『Security Implications of OPC, OLE, DCOM, and RPC in Control Systems』を参照。

バとWebサーバが組み込まれており、堅牢な通信が可能になっている。技術者や管理者は、他の専用の通信チャネルに加えて、このアクセス機能を使用したこれらのフィールド機器への第二の通信手段を持っていることも多い。

しかし、前述のようにこれらの機器は内部にあり信頼されている領域の一部であるため、機器へのアクセスは攻撃者にとって制御システムアーキテクチャへの不正なベクトルとなりかねない。フィールド機器へのアクセスを獲得することで、攻撃者はセンサネットワークの一部となり、制御システムネットワークに「トンネル」できる。攻撃者は、RTUなどのフィールド機器が制御領域の延長部分であることを認識しているため、攻撃の偵察フェーズとスキャンフェーズで、これらのフィールド機器を有望な調査対象に加える可能性がある。そのような攻撃は、一般にシリアル通信では不可能だが、遠隔装置における現代的なネットワークプロトコルと従来の制御プロトコルの統合に関連し、セキュリティ面での注意が必要である。

ある装置が侵害され、攻撃者がその装置上で制御権を獲得して権限を昇格させることができると、攻撃者は内部の制御ネットワークのスキャン、制御マスターに送信されるデータの改ざん、装置自体の動作の変更などいくつもの手順を実行できる。資源間の信頼関係を考えると、攻撃者は制御ネットワークをスキャンする可能性が高い。これは、制御システム領域全体の通信プロトコルを使用することで可能となる。これが攻撃者にとって特に有利となるのは、接続に対して悪意のあるトラフィックや疑わしいトラフィックが監視されない可能性が高いためである。[7]

*データベースおよびSQLデータインジェクション攻撃* [8]

データベースアプリケーションは、制御システムやそれに関連する記録保管ユーティリティの重要なアプリケーション構成要素になっている。従来のセキュリティモデルでは、制御システムの重要な構成要素を隔離し、脅威に対抗するためのセキュリティ上の労力をこれらのコンピュータやソフトウェア構成要素に集中させることで、システムのセキュリティを高めようとする。制御システム内のデータベースセキュリティもこれらのモデルに従っており、適切に機能する上で互いに依存している、一般に独立したシステムが使用される。2つのシステム間に高い信頼関係があると、脅威対象が広くなる。

多くの場合、制御システムによって使用されるデータベースは、データベースやコンピュータと、業務ネットワークにあるWeb対応のアプリケーションで接続される。事実上すべてのデータ駆動型アプリケーションは、何らかの形のデータベースに移行し、そのほとんどはStructured Query Language（SQL）を使用している。

[7] 一部の侵入検知システム（IDS）は、制御領域を保護するために、制御システムのシグネチャを使用して更新できる。通常、これらのシステムはシグネチャに基づいており、悪意のあるトラフィックを認識するとトリガを起動する。IDS は、有効なシグネチャの代わりに、特定のトラフィック以外のトラフィックに対してトリガを起動したり、予期せぬトラフィックや異常なトラフィックの検出時にトリガを起動したりするように設定できる。IDS については後述する。

[8] US-CERT の『Attack Methodology Analysis: SQL Injection Attacks』を参照。

データベースに格納されている情報は、攻撃者にとって価値の高い攻撃対象となる。制御システムのデータベースが業務データベースや経理データベース、データにアクセスするために使用されているアプリケーションが動作するコンピュータに接続されている場合、攻撃者は2つのネットワーク間の通信チャネルを悪用して、制御システム環境を保護するためのセキュリティ機構を迂回する。

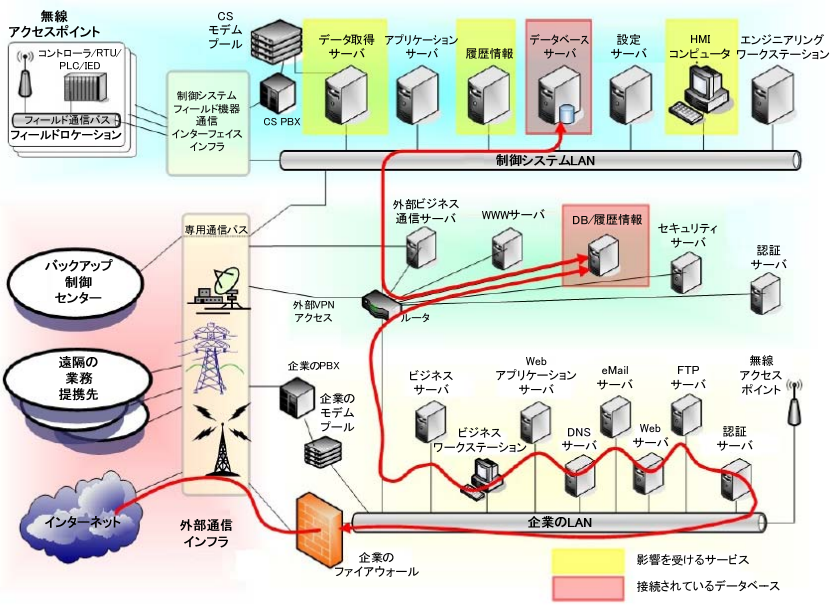


**図3 – データベース経由の攻撃**

図3 – データベース経由の攻撃に、データベース間のオープンな接続の例を示す。この例は、攻撃者が制御ネットワークにアクセスするために利用可能なサーバ間の通信経路を示している。重要なデータが格納されているデータベースにインジェクションが行われると、その影響は広範囲に及ぶが、制御システム環境では、特にデータの精度と完全性が業務上および運用上の意思決定にとってきわめて重要であることから影響が大きい。データベースの内容が改ざんされることにより、データ取得サーバ、履歴、オペレータのHMIコンソールまでが連鎖的に影響を受ける可能性がある。制御システムはデータの精度と完全性に大きく依存しているため、SQLインジェクションにより、多くの一般的なITデータベースよりも大きな被害を受ける。さらに、データベースなどの信頼されている重要資産がセキュリティ侵害を受けると、攻撃者にとっては偵察とコード実行の両方に使用できる資源が増えることになる。

制御システムが指令制御データの保存、精度、アクセスのしやすさに依存しているという点と、制御システムネットワークでSQLデータベースが普及している点を考えると、制御システムの構成要素に対する標準的なSQLインジェクションの手法は、制御システムのセキュリティに対して重大な脅威となる。

*中間者攻撃*[9]

[9] http://www.us-cert.gov/control_systems/pdf/csvul1105.pdf

制御システム環境は伝統的に、ネットワークを隔離することで許可のない人から保護されてきた（あるいは保護されることを目指してきた）。このようなネットワークでは、サーバ、資源、機器の間を流れるデータがセキュリティ保護されていないことが多い。信頼できるという思い込みから生まれるセキュリティ上の主な問題としては、（1）攻撃者によるネットワーク上で伝送中のデータの再ルーティング、（2）平文形式の重要なトラフィックの捕捉と解析、（3）独自プロトコルのリバースエンジニアリングによる制御通信上の指令の取得の3つがある。攻撃者は、これらすべてを組み合わせることで、ネットワーク上を流れるデータを自由に制御し、最終的に実際のトラフィックと「スプーフィングされた」トラフィックをネットワーク資源に送信して、目的の結果を得ることができる。このためには、中間者（MITM）攻撃が実行される。

制御システムであれ業務LANであれ、ネットワーク内のアドレスを管理することは、効果的な運用のために不可欠である。ARP（Address Resolution Protocol）を使用すると、ネットワークアドレスを物理マシンアドレスにマップすることで、ルーティングの保守が容易になる。各ネットワーク装置でARPテーブルを使用することで、コンピュータとその他の装置は、通信を要求する際にどのようにトラフィックをルーティングすれば良いかがわかる。ARPテーブルの操作（ポイズニング）は、攻撃者の主要な目的のひとつである。ARPテーブルをポイズニングすることで、すべてのネットワークトラフィック（制御トラフィックを含む）が、攻撃者がセキュリティ侵害したコンピュータ経由でルーティングされるためである。このようにして、ネットワーク上のすべての資源が、目的のホストと通信していないことを知らないまま攻撃者と通信することになる。さらに、攻撃者はネットワーク上のデータを閲覧、捕捉、再生、注入し、それがあたかも許可されたものであり、正当な送信元から送られたかのように見せることができる。

データ解析は、制御システム領域で重大な問題の1つである。一般的な（オープンな）ネットワークプロトコルと技術を使用した制御システムの場合、データ伝送中のデータ解析の脅威は大きな問題である。現在のローカルな制御環境でやり取りされるデータは、平文であることが多い。従来から、攻撃者はこの脆弱性を利用することで、ユーザ名とパスワードの組み合わせを取得して再利用し、セキュリティ侵害したネットワーク内でアクセス性を高めてきた。

ある攻撃者が、前述のいずれかの攻撃を使用するなどして制御システムネットワークへのアクセスを獲得したとする。攻撃者はネットワークを偵察し、そのネットワーク上で利用できる資源を特定する。攻撃は制御領域上で行われるため、この平文トラフィックが捕捉（盗聴）され、解析と確認のためにオフラインで持ち出される可能性がある。これにより攻撃者は、パケットとペイロードの内容を確認してリエンジニアリングし、攻撃の目的に合わせて命令セットを改ざんし、新たに悪意のあるパケットをネットワークに再注入する。制御トラフィックは、その性質上固有であるにもかかわらず、データペイロード中の命令に使用されている命名法は複雑でない。パケットに含まれているデータは、フィールド機器の動作を制御し、HMI（Human Machine Interface）ステーションにいるオペレータに表示される内容の入力として使用される。

攻撃者は、ARPポイズニングとトラフィック収集を使用して、ネットワーク内の通信に対する完全な制御を確立、維持できる。攻撃者が独自の制御システムプロトコルを取得して解析する必要が生じた場合は、制御データが閲覧、捕捉、操作される可能性がある。攻撃者は重要な制御データをリバースエンジニアリングし、不正目的のためにデータを操作するのに要する時間を得られることになる。

この中間者攻撃は、どの環境でもきわめて危険である。しかし、制御システムネットワークでは、この攻撃手法はさらなる危険性を持つ。攻撃者は、重要な情報資源を支配し中間者攻撃を実行することで、システムに対する次のような攻撃に進むことができる。

- 運用の停止
- 制御データの捕捉、改ざん、再生
- 重要なデータベース中の情報、タイミングクロック、履歴情報を改ざんするための不正確なデータの注入
- フィールド機器に攻撃を行いながら、オペレータHMIへ正常な運用データを再生（HMIが警報を発するのを防止）

### 資産の隔離と保護：多層防御戦略

業務ネットワーク構成要素と制御ネットワーク構成要素の両方に関係する現代的なITアーキテクチャは、用途が多様であるにもかかわらず、多数の共通の特性を持っている。一般に、次の機能を提供する4つの領域（ゾーン）がある。

- インターネット、提携先、バックアップ施設への外部接続（ゾーン1）
- 社内通信のための外部接続（ゾーン2）
- 外部サービスからの制御システム通信（ゾーン3）
- 制御システムの運用。プロセスベースまたはSCADA（Supervisory, Control and Data Acquisition: 監視制御データ収集システム、ゾーン4）

図4– 一般的なアーキテクチャのゾーンに、これらすべてのゾーンを含む一般的な現代のアーキテクチャを示す。

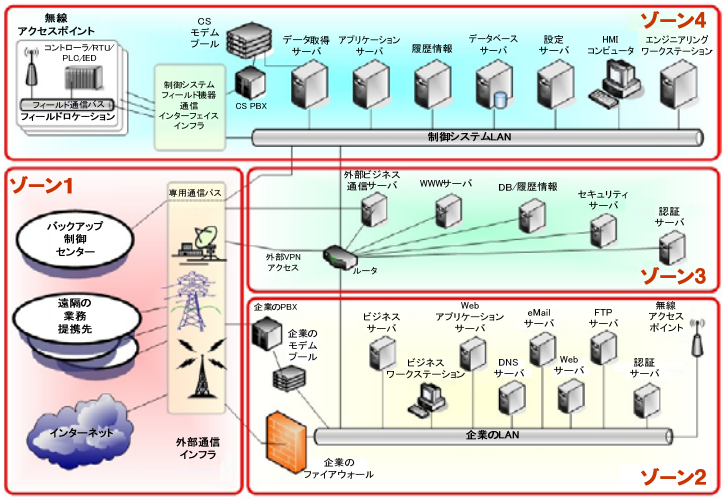


**図4– 一般的なアーキテクチャのゾーン**

これらの各ゾーンで、セキュリティ上の固有の注意が必要となる。詳細な分析によれば、重要インフラのシステムに影響を与えようとする攻撃者は、中核となる制御領域を探す可能性が最も高いことがわかっている。[10]この重要なゾーンがセキュリティ侵害されると、制御システム情報資源が破壊的に操作される恐れがある。多くの分野で、制御システムが悪意を持って攻撃されると、現実に物理的な結果が生じる。

本書や、DHSによりUS-CERTを通じて提供されている推奨文書では、さまざまな分類の攻撃と結果について説明されている。その各シナリオでは、制御ゾーンの外側の地点で侵入が始まり、攻撃者は徐々にアーキテクチャの内部をのぞき見る。

そのため、中心となるそれぞれのゾーンを保護する防御戦略を策定することで多層防御戦略が構築され、管理者に情報と資源制御のためのより多くの機会が提供されるとともに、必ずしも業務機能の妨げとならない段階的な対策が実施される。

*ファイアウォール*

ファイアウォールは、従来からあるルータを補強する追加の防御レベルを提供し、さまざまなネットワークセグメントやゾーンの間の通信に対し、より厳格で複雑なルールを追加するための機能を提供する。制御システムにとって非常に重要なことは、ファイアウォールの実装方法と、ファイアウォールの中核機能が環境の業務機能全体に与える影響である。

ファイアウォールの種類は多く、特定の制御アーキテクチャに適したファイアウォールの種類を見極めるには、ある程度の調査が必要である。前述のセキュリティゾーンの概念は、特定のゾーンに関係するリスクと結果を判断するのに役立つ。この分析を使用すれば、資産を保護するのに最適なファイアウォールの種類と属性を選択できる。一般に、ファイアウォールの種類としては、パケットフィルタ、サーキットレベルゲートウェイ、プロキシゲートウェイ、ステートフルインスペクションの4種類がある。

**パケットフィルタファイアウォール：**このファイアウォールは、分離されたネットワークに出入りするパケットを分析し、事前に設定したルールに基づいて通過を許可または拒否する。パケットフィルタリングルールは、ポート番号、プロトコル、データ要求の種類に関係するその他の定義済みデータに基づいて定義される。このタイプのファイアウォールでは、一般に規則を柔軟に割り当てることができるが、すばやい接続が必要で、機器のアドレスに基づいてルールを作成できる環境に最も適している。制御システムなどの、固有のアプリケーションとプロトコルに基づいたセキュリティが必要な環境に有効である。

**プロキシゲートウェイファイアウォール：**このファイアウォールは、保護対象となるネットワークを隠蔽する上できわめて重要であり、保護されている資源からの接続を代理して行うプライマリゲートウェイとして使用される。これは、アプリケーションレベルゲートウェイとも呼ばれ、アプリケーションを扱うこと以外は、サーキットレベルゲートウェイに似ている。OSIモデルのアプリケーション層でフィル

[10] 当然、攻撃者の目的によって変わる。一般に、制御システムの中核サービスと運用機能の完全な制御は攻撃価値が高いと考えられている。

タリングを行い、プロキシが利用できない接続は許可しない。これらのファイアウォールは、アプリケーション内部のデータ（POST、GETなど）を解析したり、ユーザの活動（ログオン、管理など）に関するデータを収集したりするのに適している。このファイアウォールはゲートウェイであるため、ユーザは接続先をファイアウォールにする必要がある。また、分析を行うという特性から、ネットワークの性能にある程度の影響がある。制御システム環境では、この種類のファイアウォールは、業務LANと制御LANを分離したり、非武装地帯（DMZ）や、アプリケーション固有の防御が必要なその他の資産を保護したりするのに適している。

**ステートフルインスペクションファイアウォール：**このファイアウォールには、他のすべての種類のファイアウォールの特性が含まれている。このファイアウォールはネットワーク層でフィルタ処理を実行し、セッションの正当性を判断し、パケットの内容をアプリケーション層で評価する。このファイアウォールではプロキシを実行するのではなく、データを処理するアルゴリズムを使用することが多い。このファイアウォールは、インターフェイスに到着するパケットの検査を大量に実行する。パケットの「状態」を調べ、事前に設定された活動に照らして分析するため、許可すべきパケットと拒否すべきパケットを決定する際に高いレベルの信頼性が得られる。これらのファイアウォールは、有効なセッションを追跡する機能を備えており、制御分野の重要な資産を保護するための優れた選択肢となっている。制御システムにおける脆弱性の多くは、サーバと機器の間の信頼関係が原因となっているため、有効なセッションと無効なセッションを追跡し対応できることのメリットは大きい。

図5 – 各アーキテクチャゾーンを保護するファイアウォールに、複数ゾーンアーキテクチャにおける階層化されたファイアウォールの配置を示す。

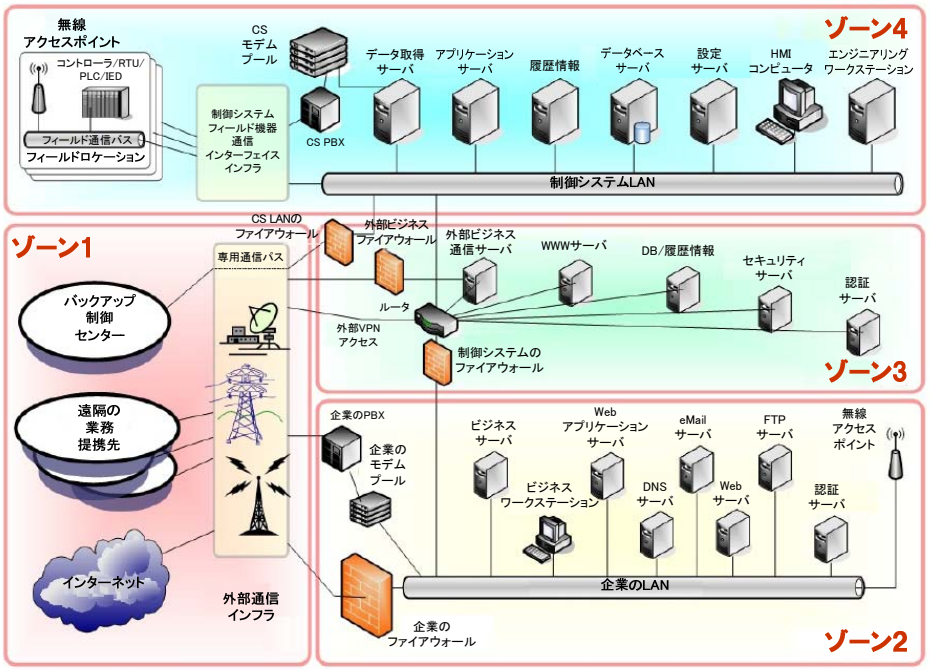


**図5 – 各アーキテクチャゾーンを保護するファイアウォール**

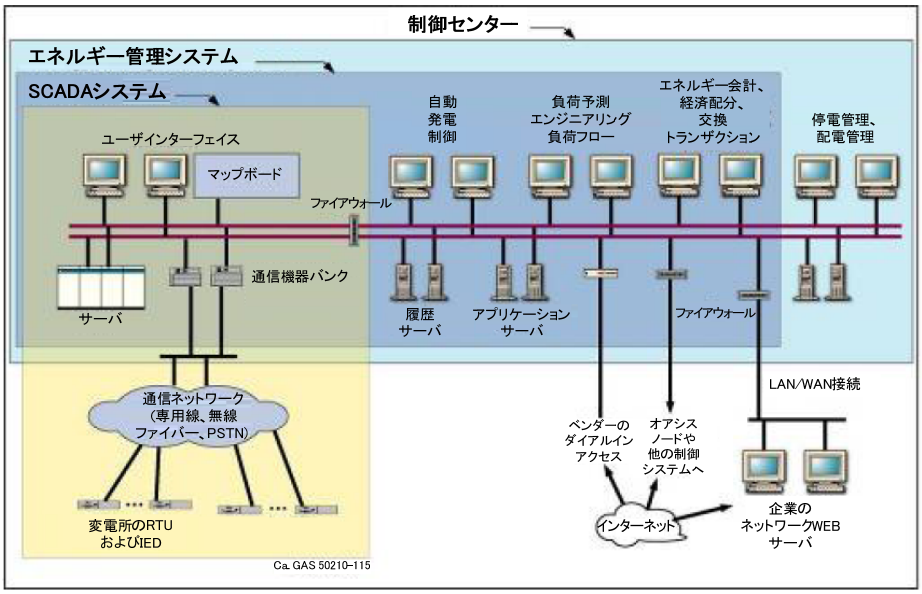


**図6 – エネルギー管理ネットワークにおけるファイアウォールの配備**

ファイアウォールを配備してネットワーク分離を堅牢化する方法についての理解を深めるために、図6 – エネルギー管理ネットワークにおけるファイアウォールの配備にエネルギー管理分野におけるファイアウォールの配備例を示す。この例では、ファイアウォールは企業領域から切り離されており、制御センターにあるEMS（Energy Management System：エネルギー管理システム）技術を保護している。多層防御を行うため、EMS領域をSCADAシステムから分離する別のファイアウォールが配備されている。

適切に設定されたファイアウォールは、制御システムのセキュリティにとって不可欠である。通信は、システムの機能に必要なものに制限すべきである。制御システムのトラフィックを監視し、必要なアクセスだけを許可するルールを作成する。ファイアウォールのルール集の中で例外を作成する場合は、ホスト、プロトコル、ポート情報など、できるだけ具体的にする。

見落としがちなのは、送信トラフィックを制限しないことである。ファイアウォールルールでは、ファイアウォールを通過する双方向のトラフィックを考慮する必要がある。ほとんどの管理者は、制御ネットワークに流れるトラフィックを効果的に遮断するが、ネットワークから出て行くトラフィックはフィルタリングしない。送信トラフィックに対してもルールを作成し、初期状態では例外を含めないようにする。これらのルールを微調整して、不要なトラフィックをすべて除去するようなルール集を作成する。必要な送信トラフィックが特定されたら、必要な通信以外のすべてのトラフィックを遮断する、より安全な設定を作成できる。

従来、ネットワークを防御する上でのファイアウォールの役割は単純である。制御システムを対象とする攻撃者は、業務ネットワークに対する攻撃と同様に、制御システムから情報を取得し、ファイルやコマンドを送信する必要がある。制御システム上のコンピュータで実行している攻撃コードをリモートで制御するには、制御ネットワーク側からの接続を確立する必要がある。制御システム領域にある資源への攻撃に関しては、攻撃コードは少量である必要があり、攻撃者が対象のコンピュータに侵入するのに

十分なコードだけが含まれている。これは、一般に攻撃者が高度な機能を入手するために、装置上にロジックを追加する十分な領域がないためである。したがって、攻撃行為の探索段階に進むには、攻撃者からの追加の命令が必要になる。送信フィルタリングを正しく実装すれば、攻撃者はこの戻りの接続を受信することができず、悪用されたコンピュータを検出、制御することができない。[11]

*非武装地帯（DMZ）の作成*

従来から、ネットワークの分割は複数のルータを使用することで実現されてきた。DMZを設けて制御ネットワークを保護するには、ファイアウォールを使用する。提携先との接続、データ履歴データベース、SCADAシステム内のInter Control Center Communications Protocol（ICCP）サーバ、セキュリティサーバ、複製サーバ、開発用サーバなど、機能やアクセス権を分離するため、複数のDMZを設けることもできる。図7に、複数のDMZを配備した堅牢なアーキテクチャを示す。

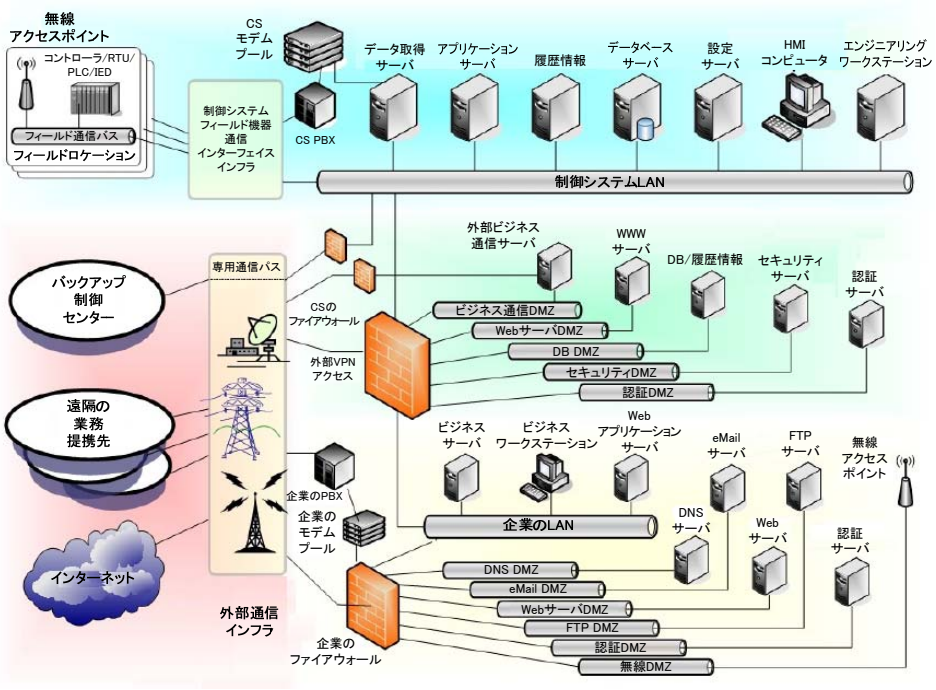


**図7 – DMZを配備したアーキテクチャ**

制御システムLANへの接続はすべてファイアウォールを経由してルーティングされ、それを迂回する接続はない。ネットワーク管理者は、制御システムLAN、他の保護されたサブネット、DMZ、社内ネットワーク、外部との接続の正確なネットワーク図を維持する必要がある。

複数のDMZは、さまざまな運用上の要求がある複数のネットワークで構成される大規模なアーキテクチャを保護する上で、非常に有効であることがわかっている。図7 – DMZを配備したアーキテクチャに示す完全な例は、制御システムネットワークと業務ネットワークが結合されたネットワークである。この例

[11] http://www.cpni.gov.uk/docs/re-20050223-00157.pdf

で、さまざまな環境を出入りするデータの安全な流れが、運用にとってきわめて重要である。複数のDMZがあることで、仮想LAN（VLAN）ホッピングや信頼の悪用を使用した攻撃から情報資源が保護される。この方法は、セキュリティ体制を強化し多層防御戦略に階層を1つ追加するための非常に優れた方法である。

*侵入検知システム*

攻撃者が制御ネットワークへのセキュリティ侵害を試みる際の最も論理的な経路を考えると、アーキテクチャを徐々に詮索するときの攻撃経路を簡単に視覚化できる。攻撃者は、外部環境から周辺部を通過し、最終的にネットワークとそのネットワーク上のホストにアクセスしようとする。このアクセスは、リモートアクセス要件によって制御システムアーキテクチャに脆弱性が持ち込まれるかもしれない、フィールド機器を経由する場合があることに注意する。攻撃者はいったん標的のネットワークに到達すると、偵察によって情報収集し、より多くの構成要素のセキュリティを侵害しようとする。これらの各ケースで、通常時以上の不正な活動がネットワークに存在することが考えられるため、この活動を監視（および対処）することで防御のレベルを1つ増やすことができる。

ネットワークの異常な活動や不正な活動を監視するための一般的な方法はいくつかあるが、最も効果的なのは侵入検知システム（IDS）である。侵入検知は単一の製品や技術でないことに注意する。IDSは総合的なツールセットであり、管理者がネットワークの使用状況を完全に把握できるネットワーク監視機能を備えている。これらのさまざまなツールを導入することで、攻撃者の活動を認識する上でより効果的な多層防御アーキテクチャを構築できる。

侵入検知システムは、その仕組み上受動的なものである。ネットワークに配備したときのIDSの機能は、トラフィックに影響を与えることなくトラフィックやネットワーク活動を監視して評価することである。IDSは、データを収集すると事前に定義されたルール集や既知の攻撃「シグネチャ」と突き合わせてデータを比較する。IDSはポート番号とデータペイロードを調べ、不正な活動が行われているかどうかを判断する。攻撃パターンが認識された場合や、正常/許可されるトラフィックとして定義された内容からずれている場合は、システム管理者に警告するなど一連の命令を実行する。今日入手できるほとんどのIDSは、広範なログ記録機能も備えている。

ほとんどのIDSはシグネチャに基づいている。最新の業務環境では、これは非常に受け入れやすい。なぜなら、最新のプロトコルとオペレーティングプラットフォームを使用した多くのネットワークアーキテクチャおよびホストアーキテクチャ向けに、多くのシグネチャがあるためである。現代の業務分野におけるセキュリティ上の脆弱性も一般に知れ渡っているため、広く普及した技術を使用してネットワークやホストのIDSを微調整することも容易であることが多い。パッチなどのセキュリティ技術を制御システムで配備する際の問題と同様に、IDSの設定と配備は簡単ではない。たとえば、現在のIDSシグネチャファイルの多くは非常に堅牢でさまざまな攻撃を検知できるが、制御ネットワーク中の悪意のあるトラフィックを監視するために必要なシグネチャは十分ではない。ModbusやDNP3などの、制御システムで使用されている専用の通信プロトコルを見てみると、特定のペイロードとポート番号は、現在のIDSのシグネチャには含まれていない。つまり、制御システムネットワークに現在のIDSを配備しても、制御システムに対する攻撃の種類を認識できない可能性がある。

制御システムにIDSを配備する際、一意のシグネチャを追加する機能を使用する必要がある。また、既定のシグネチャと応答機能のうち、制御システムネットワークに該当しないものを削除することもよくある。しかし、機能を改良および増強した状態で、IDSが本来備えている機能を利用できることを確認するために分析を行う必要がある。制御システムのセキュリティに特化したベンダを含め、多くのセキュリティベンダが制御アーキテクチャに配備されるIDS向けのシグネチャを作成している。制御システムネットワークにIDSを配備する際には、その分野固有のルールセットとシグネチャを使用することが不可欠である。セキュリティシグネチャとルールは、制御システムベンダとの協力関係の中で開発するのが非常に有利であることがわかっている。

業界で見られるありがちな問題の1つとして、ネットワーク監視用に配備されたツールが、実装はされたが適切に更新、監視、検証されていないことが挙げられる。任命された要員が訓練を受け、システムデータログの監視と各種ツール設定を最新に保つ責任を負う必要がある。

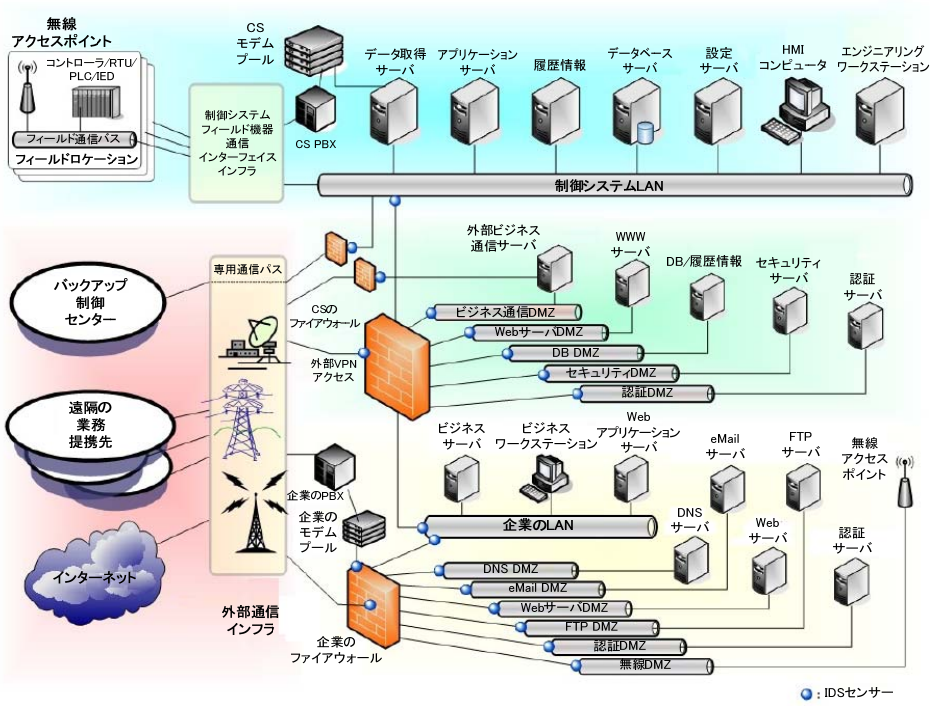


**図8－IDSを使用した完全な多層防御戦略**

IDSのホストレベルでの配備は、ネットワークレベルでの配備に似ているが、IDSはネットワークの活動を監視するのではなく、ルールセットに従って監視する。これらのルールは、非常に堅牢かつ広範なものとすることができ、ホストが実行しているプラットフォームやオペレーティングシステムに一意の定義済みのシグネチャに対する警告を含めることができる。ホストレベルでIDSを配置することにより、多層防御のレベルをさらに1つ増やすことができ、これを利用して境界レベルとネットワークレベルに配備した防御策を増強できる。

IDSは元来受動的なものであることから、どの程度セキュリティリスクが緩和され攻撃が認識されるかは、ログファイルを分析する頻度とその有効性に依存することを理解することが重要である。IDSログを適時に分析することを指示する厳格なポリシーが非常に重要である。攻撃者がシステムにアクセスし、ログファイルが確認される前に攻撃を行うと、IDSと攻撃に対処する機能は意味をなさなくなる。

*セキュリティポリシー*

効果的なセキュリティポリシーと手続きは、セキュアな制御システムネットワークへの第一歩である。社内システム向けのITセキュリティに採用されているのと同じポリシーの多くを、そのまま制御システムネットワークに適用できる。SANS Instituteは、多くの種類のセキュリティポリシーの無料テンプレートを提供しており、制御システムネットワークの管理者が各自のポリシーを策定する際の貴重な情報源となっている。

NERC（North American Electric Reliability Council：北米電力信頼度協議会）の電力システム向けのサイバーセキュリティ要件のように、制御システム固有の要件を追加できる。[12]

セキュリティポリシーを効果的なものにするには、ポリシーが現実的で実施可能であることと、ポリシーに従うことが可能であることが必要である。ポリシーによって生産性に大きく影響したり、コストがあまりにも高かったり、支持されないといったことがあってはならない。これを達成するには、経営者とシステム管理者をポリシーの策定に参加させるのが最も良い。

ネットワークと制御システムの管理者は技術的な知識を持っているが、ポリシーを実装するには経営者の承認と支援が必要である。経営者は、制御システムのセキュリティを実装、管理するための適切な要員の任命と育成を支援する必要がある。

*セキュリティ訓練*

多くの場合、制御システムネットワークを管理する要員は、十分なセキュリティ訓練を受けていないことがある。このような状況の原因は一般に、訓練の費用や訓練の重要性に対する正しい認識が不足していることである。訓練は何よりも重要なセキュリティ意識向上プログラムの中心部分であり、重要な情報と情報資源の保護を支援するいくつかの特性からなる。

制御システム分野に特化したセキュリティ訓練と十分なセキュリティ意識向上プログラムは、制御システムのセキュリティだけでなく、あらゆる自動化工程に関係する制御システムの安全性にとってもきわめて重要である。企業分野向けに作成されたセキュリティ意識向上プログラムと同様に、制御システムの分野を対象としたプログラムには、継続的で測定可能なセキュリティ対策を推進するのに役立つ重要な構成要素がある。NIST SP800-50『Building an Information Technology Security Awareness and Training

[12] http://www.nerc.com/filez/standards/Cyber_Sec_Renewal.html

Program』[13] に記載されている一般的なセキュリティ意識向上プログラムの中で、適用可能なセキュリティ意識と訓練課程を作成できる。これには次のものが含まれる。

- 目的とスコープ
- 資料作成
- 実施計画
- 監察とフィードバック
- 成功指標

ネットワークセキュリティ管理者は、ネットワークセキュリティ分野における急速な変化や進展について常に最新の情報を得るため、継続的な訓練を必要とする。これには最新のネットワークアーキテクチャ設計や、ファイアウォールとIDSの設定が含まれる。コンピュータネットワークを攻撃および防御するための新たな手法は常に開発されている。包括的なコンピュータセキュリティ訓練を受けることは、システム管理者だけでなく、個々の利用者にとっても非常に重要である。

正式な訓練を受けるにはコストがかかりすぎる場合は、この情報の一部を、サイバーセキュリティおよび制御システムセキュリティに関する書籍、資料、Webサイトから収集できる。たとえば、制御システム固有の訓練課程の詳細を作成するのに役立つリソースとして、US-CERTは制御システムのサイバーセキュリティに特化したWebサイトを提供している（http://www.us-cert.gov/control_systems/）。

*インシデント対応*

多層防御戦略を完全に支援するには、堅牢なインシデント対応能力が必要である。制御システム分野でセキュリティ関連のインシデントが発生した場合、認識、対応、緩和、再開のための行動を確立する必要がある。インシデント対応手順により、ネットワーク上のコンピュータがセキュリティ侵害された場合にとるべき手順を従業員に指示する。すべての従業員は、インシデントが起きる前に対応手順について訓練を受け、手順を実施できることが必要である。インシデント対応手順で答えるべき質問の例としては、次のものがある。

- インシデントが発生したことを示す兆候、または現在発生していることを示す兆候は何か。
- 当面どのような行動をとるべきか（コンピュータをネットワークから切断すべきかなど）。
- 誰にどのような順序で連絡すべきか。警察に相談すべきか。
- 法的証拠をどのようにして保存すべきか（メモリ内の証拠を残すためにコンピュータの電源を入れたままにすべきかなど）。
- どのように影響を受けたコンピュータを復旧させるか。

NIST（National Institute of Standards and Technology）のSP 800-53、『Computer Security Incident Handling Guide』に、セキュリティ担当者がインシデント対応手順を策定する上での指針が示されている。また、US-CERTは任意の制御システムセキュリティインシデントに利用できる広範な情報とインシデント報告機能を用意している。インシデント報告は、http://www.us-cert.gov/control_systems/ で行うことができる。

[13] http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

## 具体的な推奨事項と対策

情報インフラを保護する際に、優れたセキュリティ体制をとるには予防型セキュリティモデルから始める。この反復型のモデルは、図9 – 予防型セキュリティモデルに示すいくつかの重要なセキュリティ戦略からなる。

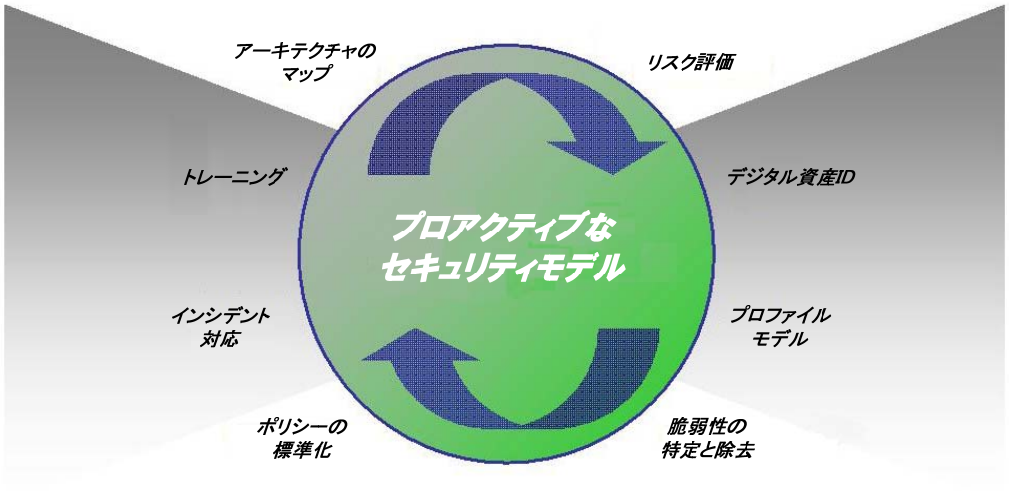


**図9 – 予防型セキュリティモデル**

一般に、多層防御戦略を策定するにはまず制御システムアーキテクチャのマップを作ることから始める。アーキテクチャを十分かつ正確に文書化することで、組織はセキュリティ意識を高め、効果的なセキュリティ対策を導入し、セキュリティインシデントを理解しやすい体制を整えることができる。アーキテクチャを理解することで、管理者は保護すべき対象を知ることができる。また、アーキテクチャを確実に理解することで、リスク評価において評価パラメータとプロセスの策定を、制御システム環境の既存の（既知の）情報資産に容易にすり合わせることができるため、効果的なリスク評価を行うことができる。

セキュリティ評価を実施できると、今度は制御領域内で資産IDを割り当てることができ、指令制御環境の全体プロファイルの定義につながる。リスク緩和策の最終段階の大部分は、反復的かつ継続的なセキュリティ訓練によって支えられる技術の配備に関係するため、プロファイルの策定後に多層防御戦略を配備できる。

*制御システムに対する5つの重要なセキュリティ対策*

制御システム環境においてサイバーセキュリティ活動を推進するための5つの重要な対策を以下に示す。

1. セキュリティポリシー：制御システムネットワークとその個々の構成要素に対するセキュリティポリシーを策定する。ただし最新の脅威環境、システム機能、必要なセキュリティレベルを反映するように、セキュリティポリシーは定期的に見直す。

2. 資源とサービスへのアクセスの遮断：この手法は一般に、ファイアウォールやプロキシサーバなど、アクセス制御リストを持つ周辺装置を通じてネットワーク上で配備される。ホストベースのファイアウォールやウィルス対策ソフトウェアを通じて有効にできる。

3. 悪意のある活動の検出：悪意のある活動の検出は、ネットワークベースでもホストベースでも実行でき、通常は経験豊富な管理者による定期的なログファイルの監視が必要となる。侵入検知システムは、ネットワーク上の問題を識別する一般的な手段であるが、個々のホスト上にも配備できる。監査ログとイベントログは、できるだけ個々のホスト上で有効にする。

4. 潜在的な攻撃の影響の緩和：多くの場合、脆弱性を除去することでシステムが動作しなくなったり効率が低下したりする可能性があることから、その脆弱性の存在が不可避な場合がある。リスク緩和により管理者は、脆弱性を悪用できない方法で脆弱性に対するアクセスを制御できる。これは、技術的な回避策の有効化、フィルタの確立、特定の設定を持つサービスやアプリケーションの実行によって可能になることが多い。

5. 基本的な問題の修正：基本的なセキュリティ問題を解決するには、ほぼ必ずソフトウェアの脆弱性の更新、アップグレード、パッチ適用や、脆弱なアプリケーションの除去が必要となる。ソフトウェアのセキュリティホールは、3つの階層（ネットワーク、オペレーティングシステム、アプリケーション）のどれにでも存在しうる。可能な場合、リスク緩和策はベンダや開発者から提供され、管理者が適用するのが望ましい。

**推奨する資料**

- INLのリスクドキュメント（公開準備中）
- INLのSQLのドキュメント（公開準備中）
- INLのOPC/DCOMのドキュメント（公開準備中）
- 『Control Systems Cyber Security Awareness』（公開準備中）
- 『An Undirected Attack Against Critical Infrastructure: A Case Study for Improving your Control System Security』

  http://www.us-cert.gov/control_systems/pdf/undirected_attack0905.pdf
- 『Backdoors and Holes in Network Perimeters: A Case Study for Improving your Control System Security』

  http://www.us-cert.gov/control_systems/pdf/backdoor0503.pdf
- 『Common Control System Vulnerability』

  http://www.us-cert.gov/control_systems/pdf/csvul1105.pdf
- 『A Comparison of Electrical Sector Cyber Security Standards and Guidelines』（2004年10月）

http://www.us-cert.gov/control_systems/pdf/electrical_comp1004.pdf

- 『Intruder Detection Checklist』（公開準備中）
- 『Personnel Security Guidelines』

  http://www.us-cert.gov/control_systems/pdf/personnel_guide0904.pdf
- 『A Comparison of Oil and Gas Segment Cyber Security Standards』

  http://www.us-cert.gov/control_systems/pdf/oil_gas1104.pdf

## 用語集

ASN – Abstract Syntax Notation（抽象構文記法）
CC – Common Criteria（コモンクライテリア）
CERT – Computer Emergency Response Team（コンピュータ緊急対応チーム）
COE – Common Operating Environment（共通運用環境）
COM – Common Object Model
DCE – Data Communications Equipment（データ通信機器）
DCOM – Distributed Common Object Model
DCS – Distributed Control System（分散制御システム）
DHS NCSD – DHS National Cyber Security Division
DOS – Denial of Service（サービス運用妨害）
DNP – Distributed Network Protocol
DOI – Domain of Interest
DTE – Data Terminal Equipment（データ端末装置）
EOP – Emergency Operating Procedures（緊急時運転手順）
EPA – Enhanced Performance Architecture
ES-ISAC – Energy Sector ISAC
FIPS – Federal Information Processing Standard（連邦情報処理規格）
FTP – File Transfer Protocol（ファイル転送プロトコル）
I&W – Indications and Warning（兆候と警告）
ICS – Industrial Control System（産業用制御システム）
IEC – International Electrotechnical Commission（国際電気標準会議）
IEC TC – International Electrotechnical Commission technical Committee
IED – Intelligent Electronic Device（インテリジェント電子装置）
IP –Internet Protocol（インターネットプロトコル）
ISAC – Information Sharing and Analysis Center（情報共有分析センター）
ISO – International Standards Organization（国際標準化機構）
NIPC – National Infrastructure Protection Center（基盤構造保護センター）
NIST – National Institute of Standards and Technology（米国標準技術局）
OEM – Original Equipment Manufacturer（相手先ブランド製造）

OLE – Object Linking and Embedding（オブジェクトのリンクと埋め込み）
OPC – OLE for Process Control
OSI – Open Systems Interconnectivity
PCS – Process Control System（プロセス制御システム）
PLC – Programmable Logic Controller（プログラマブル論理制御装置）
POTS – Plain Old Telephone Service（アナログ音声通話のみ可能な旧来の電話サービス）
PSTN – Packet Switched Telephone Network（公衆電話交換網）
RPC – Remote Procedure Call（リモートプロシージャコール）
RTU – Remote Terminal Unit/Remote Telemetry Unit（遠隔端末装置）
SCADA – Supervisory Control and Data Acquisition（監視制御データ収集システム）
SIRC – Security Incident Response Capability
SMTP – Simple Mail Transfer Protocol
SNMP – Simple Network Message Protocol
SOP – Standard Operating Procedures
SSID – Service Set Identifier：無線ネットワーク上のすべてのパケットに添付されるコードで、そのネットワークに含まれる各パケットを識別する。
TCP –Transmission Control Protocol（トランスミッションコントロールプロトコル）
TCSEC – Trusted Computer System Evaluation Criteria（通称オレンジブック）
TFTP – Trivial File Transfer Protocol
UDP – User Datagram Protocol（ユーザデータグラムプロトコル）
WARDIALING – モデムが搭載されたPCから、公開されていない他のモデムを見つけ、コンピューティング分野またはPCS分野の不正アクセスを行うために、電話番号に連続してダイヤルすること。
WARDRIVING – 通信ネットワークにアクセスし、コンピューティング分野または制御システム分野の不正アクセスを行うために、無線アクセスポイントを繰り返し探すこと。
X86 – 「エックスハチロク」と読む。インテル製32ビットプロセッサに対する標準的な略称。