JPCERT CC®

SCADAおよびプロセス制御ネットワークにおける

ファイアウォールの利用についての

NISCCグッド・プラクティス・ガイド

SCADA およびプロセス制御ネットワーク
における
ファイアウォールの利用についての
NISCC グッド・プラクティス・ガイド

National Infrastructure Security Co-ordination Centre (NISCC)用に
British Columbia Institute of Technology (BCIT)が作成

リビジョン番号: **1.4**
文書発行日: **2005 年 2 月 15 日**

Internet Engineering Lab (IEL)
Group for Advanced Information Technology (GAIT)

改訂履歴

リビジョン	発行日	著者	内容
0.1	2004 年 5 月 9 日	Eric Byres, BCIT Internet Engineering Lab Ken Savage, BCIT Internet Engineering Lab	Draft
1.0	2004 年 5 月 22 日	Eric Byres, BCIT Internet Engineering Lab John Karsch, BCIT Internet Engineering Lab Joel Carter, BCIT Internet Engineering Lab	Preliminary Release
1.1	2004 年 7 月 8 日	Eric Byres, BCIT Internet Engineering Lab John Karsch, BCIT Internet Engineering Lab Joel Carter, BCIT Internet Engineering Lab	Grammatical Changes
1.2	2004 年 9 月 27 日	Eric Byres, BCIT Internet Engineering Lab John Karsch, BCIT Internet Engineering Lab Joel Carter, BCIT Internet Engineering Lab	Grammatical Changes
1.3	2005 年 1 月 15 日	Eric Byres, BCIT Internet Engineering Lab John Karsch, BCIT Internet Engineering Lab	Added Scoring System and 4.2 Architecture
1.4	2005 年 2 月 15 日	Eric Byres, BCIT Internet Engineering Lab John Karsch, BCIT Internet Engineering Lab Joel Carter, BCIT Internet Engineering Lab	Public Release

謝辞

ブリティッシュ・コロンビア技術大学（British Columbia Institute of Technology: BCIT）の高度情報技術グループ（Group for Advanced Information Technology (GAIT)）は、私達の取り組みに多大な支援をしてくださったベンダーとエンドユーザの皆様に謝意を表したい。多くの面談に応じていただき、また極めてデリケートと言える文献を提供していただいた。残念なことに、セキュリティ上の理由から名前を挙げることはできませんが、時間を取っていただき、信頼していただき、励まして下さったことに感謝します。

本文書に対する貢献と助言が顕著な方が 4 名おられます。Cisco System のクリティカル・インフラストラクチャ・アシュアランス・グループ(Critical Infrastructure Assurance Group: CIAG)の Darrin Miller、BP International の Andy Cobbett と Ian Henderson、PA Consulting の Justin Lowe です。本当に有難うございました。

最後に、国立インフラストラクチャ・セキュリティ調整センタ(National Infrastructure Security Coordination Center: NISCC)の Karl Williams のビジョンと支援にも謝意を表します。同氏の支援なしには、このプロジェクトは不可能だったでしょう。

BCIT
BRITISH COLUMBIA INSTITUTE OF TECHNOLOGY

Technology Centre
3700 Willingdon Ave.
Burnaby, B.C.
Canada V5G 3H2
P 604-432-8761
F 604-436-0286
E techcentre@bcit.ca
www.tc.bcit.ca

NISCC
National Infrastructure Security Coordination Centre

PO Box 832
London SW1P 1BG

Tel: 0870 487 0748

ここは空白ページである。

目　次

図

要旨

近年、SCADA（Supervisory Controls and Data Acquisition）、プロセス制御、工業製造システムなどは、通信する際にその内容が重要か否かにかかわらず、Ethernet®、TCP/IP、Windows®等の商用情報技術を使うことが多くなってきている。これらの共通プロトコルやOSを使用する利点は多いが、一方極めて重要なSCADAやプロセス制御ネットワーク（PCS）を外界から隔離できる度合いがかなり低くなるという問題を生じる。現在これらのシステムは、十代のスクリプトマニアから熟練した本格的サイバー犯罪者に到るまで、多様な脅威に曝されている。

残念ながら、これらの最重要システムを守るために資産保有者や技術者が取りうる実証された対策は殆どない。よく推奨される対策は、ファイアウォールを使ってSCADAやPCNシステムをインターネットや企業ネットワーク（EN）から隔離することである。しかし、その際にファイアウォールのアーキテクチャ、設定、管理をどうすべきかについての詳しい情報は殆ど示されていない。ファイアウォールは複雑なため、正しく設計し使用するのは困難である。したがって、実際の産業現場でファイアウォールをどのように使用すれば最も良いかについてのガイダンスがあれば大変有用であろう。

そのため、英国のNISCC（National Infrastructure Security Coordination Centre, 国立インフラストラクチャ・セキュリティ調整センタ）は、ブリティッシュ・コロンビア技術大学（BCIT）の高度情報技術グループ（Group for Advanced Information Technology (GAIT)）にSCADA/PCNファイアウォール利用の現状について調査と報告を委託した。その狙いは、産業現場環境を保護するために使用されるファイアウォールのアーキテクチャ、配備、管理について「最先端の状況」を知ることである。

調査チームは2004年3月に、約60組織と業界報道機関に産業現場でのファイアウォールの使用に関する問い合わせを送付した。ファイアウォール製造業者、ＩＴセキュリティ会社、制御システム製造業者を含めて、10社のベンダーから回答があった。また、石油、化学、食品、電気業界の約15社からも回答が寄せられた。これらのベンダーとエンドユーザはすべて、北米またはヨーロッパを本拠とする会社である。提供された情報は、個人的な面談、ホワイトペーパ、ポリシーマニュアル、ネットワーク監査報告、セキュリティ製品に関する文献などである。更に、工業制御セキュリティに関係する標準化団体から文書草案を入手した。その中には、米国石油協会（API）、産業自動化のためのオープン・ネットワーク協会（IAONA）、国際電気標準会議（IEC）、電気電子技術者協会（IEEE）、計測機器・システム・オートメーション協会（ISA）からの文書草案が含まれる。

研究チームは、セキュリティ業務の現状を明らかにするため、収集した情報を、ファイアウォールのアーキテクチャ、設計、配備、管理の各観点からまとめた。次にこれらの業務の現状を分析し、それらが産業用制御環境でどの程度有効かを示す評点を付けた。この分析結果を見ると、産業界で使用されているソリューションには様々なものがあり、それらのセキュリティ面の有効性もバラツキが大きいことが分かった。ワークステーシ

ョン、ブリッジ、ルータを 2 か所に所属させる方法がよく使われているが、この方法を用いると適切な隔離ができない恐れがある。2 ゾーンアーキテクチャによりセキュリティを幾分向上できるが、導入する場合には細心の注意が必要である。一般に、企業ネットワークと SCADA/PCN ネットワークの間に非武装セグメント（DMZ）を設けるアーキテクチャがセキュリティ面で最も効果的である。

ここは空白ページである。

1 まえがき

近年、監視制御データ収集システム(SCADA)、プロセス制御システム、工業製造システムは、通信する際にその内容が重要か否かにかかわらず、Ethernet、TCP/IP、Windows 等の商用情報技術を使うことが多くなってきている。これらの共通プロトコルや OS の使用により、工業用制御装置と外界を接続することが大変容易になった反面、外界から隔離できる度合いがかなり低くなった。企業ネットワーク(enterprise network: EN)および世界のネットワーク・セキュリティの問題が、SCADA やプロセス制御ネットワーク(PCN)に波及し、工業生産および人の安全を危険に曝している。

同時に、私達の情報インフラの中核であるインターネットに対して、サイバー空間を無謀に飛び回る十代の若者からプロのハッカーまで様々な人たちからの攻撃がますます激しくなっている。地球上のほぼ全ての国の人たちが、ネットワークにアクセスできる、そのネットワークは更に、世界中で極めて重要な機能を果たしているネットワークに最終的に接続されている。情報ネットワークに対するサイバー攻撃は恒常的に起こっており、接続されているPCNやSCADAシステムに影響を与えた場合、重大な結果をもたらす。例えば、2000 年にハッカーがオーストラリアのクイーンズランドの下水処理場を攻撃した結果、数百万リットルの汚水が流れだし、その地域の川と公園を汚染した。[1] 3 年後、Slammer Worm（スラマーワーム）が少なくとも 2 つの電力発電／配電システム[2]、原子炉内の安全監視システム[3]、緊急通話システムに影響を及ぼしたことが記録されている。将来の攻撃は、極めて重要なサービスの広範囲の途絶や人命の損失などの深刻な結果をもたらす可能性がある。

これらの重要なシステムの保護が重要なことは広く認識されているが、これらのシステムを保護するために資産の保有者や技術者が取りうる実証された対策は殆どない。確かに、PCNを守る有意義なガイダンスを提供できる一般的な情報セキュリティの実践や標準はあるが、重要な違いもあることを考慮する必要がある。例えば、情報技術(IT)部門の目標は、プロセス制御部門の目標と根本的に異なる。ITの世界では通常、性能とデータの保全が最重要と見るが、産業の世界では、人間と工場の安全が最重要と見ている。他の文書化された相違点として、信頼性要件の差、イベントの影響、性能への期待、OS、通信プロトコル、システム・アーキテクチャを挙げられる。[4] [5] これらの違いは、許容できるセキュリティの実践に非常に大きな違いをもたらすことがある。

よく推奨されるセキュリティ対策は、ファイアウォールを使って SCADA システムや PCN システムを企業システムやインターネット・システムから隔離することである。残念なことに、ファイアウォールは従来の IT セクタで広く配備されているが、SCADA/PCN 環境でのその効果は、いまだに疑わしい。IT ファイアウォールは、一般に SCADA/PCN プロトコルを理解しないので、タイム・クリティカルなシステムに、許容できない待ち時間を持ち込むかもしれず、IT の世界ではあまりない運用制限が起こりかねない。さらに悪いことに、これらのファイアウォールのアーキテクチャ、設定、管

理を具体的にどう使用すべきかについての情報は殆ど入手できない。PCN または SCDA の技術に関する典型的なガイダンスが、以下以上に詳しいことはめったにない。

> 「事務所のLANと工業制御LANを一緒にするな。それらは、ファイアウォール、最低でもブリッジかルータを使用して分離すべきである」[6]

この種の助言は、ファイアウォールは複雑なため、それを効果的に使用するには、注意深い設計、設定、管理が必要であるという事実を見逃している。例えば、PCN と企業ネットワークの間のファイアウォールのルールセットはどのように定めるべきか。それは、アドレス・フィルタリングに限定すべきか、それともプロトコル・フィルタリングも使用すべきか。そして、プロトコル・フィルタリングを使用する場合、どのプロトコルをブロックし、どのプロトコルを許可すべきか。もちろん、SCADA や PCN のシステムにはそれぞれ、他と異なる特徴があるので、これらの質問に対する唯一の答えはないが、実際の産業現場でファイアウォールをどのように使用すれば最も良いかについてのガイダンスがあれば大変有用であろう。

この必要性に取り組むために、英国の NISCC（National Infrastructure Security Coordination Centre, 国立インフラストラクチャ・セキュリティ調整センタ）は、ブリティッシュ・コロンビア技術大学（BCIT）の高度情報技術グループ（Group for Advanced Information Technology (GAIT)）に SCADA/PCN ファイアウォール利用の現状について調査と報告を委託した。その狙いは、産業現場環境を保護するために使用されるファイアウォールのアーキテクチャ、配備、管理について「最先端の状況」を知ることである。プロジェクトの目標は、以下のとおりである。

1. 機器ベンダー、ユーザ、産業の標準化団体から、SCADA/PCN ファイアウォール利用についての入手できるすべての推奨事項を収集する。

2. 収集したファイアウォール利用の推奨事項とベスト・プラクティスを要約する。

3. セキュリティ上の効果および潜在的な弱点に関して、列挙した推奨事項およびベスト・プラクティスを分析する。

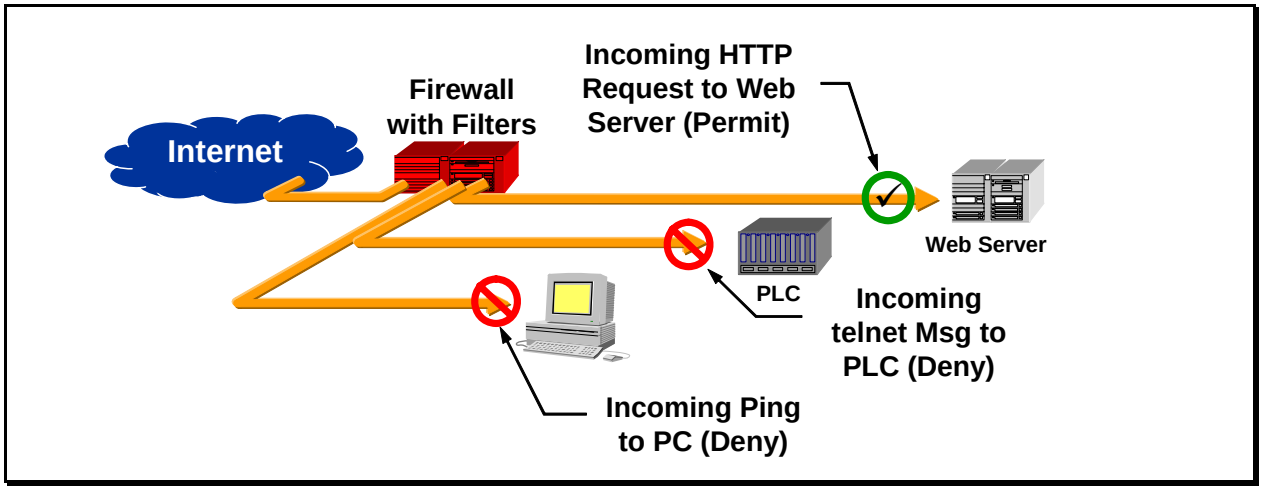
調査チームは 2004 年 3 月に、約 60 組織と業界報道機関に産業現場でのファイアウォールの使用に関する問い合わせを送付した。ファイアウォール製造業者、ＩＴセキュリティ会社、制御システム製造業者を含めて、10 社のベンダーから何らかの回答があった。また、石油、化学、食品、電気業界の約 15 社からも回答が寄せられた。これらのベンダーとエンドユーザの団体はすべて、北米またはヨーロッパを本拠とする会社である。提供された情報は、個人的な面談、ホワイトペーパ、ポリシーマニュアル、ネットワーク監査報告、セキュリティ製品に関する文献などである。更に、工業制御セキュリティに関係する 5 標準化団体から文書草案を入手した。その 5 団体は、米国石油協会（API）、産業自動化のためのオープン・ネットワーク協会（IAONA）、国際電気標準会議（IEC）、電気電子技術者協会（IEEE）、計測機器・システム・オートメーション協会（ISA）である。

調査チームは、セキュリティ業務の現状を明らかにするため、収集した情報を、ファイアウォールのアーキテクチャ、設計、配備、管理の各観点からまとめた。次にこれらの業務の現状を分析し、それらが産業用制御環境でどの程度有効かを示す評点を付けた。この要約と分析の成果は、本報告書に収録してある。

後続のプロジェクトにおいて、この報告書で検討された幾つかのベスト・プラクティスを研究室環境でテストするつもりである。これには、SCADA/PCN セキュリティの基準となるファイアウォール・アーキテクチャとルールセットを作成し、次にそれをセキュリティの正しさと性能の面から、幾つかの市販ファイアウォールによりテストする。これら 2 つの調査が一体となって、重要な産業環境でのファイアウォールの設計と実装に関して、SCADA/PCN の技術者と資産保有者に明快なガイダンスを提供できるであろう。

2 ファイアウォールとは何か

ファイアウォールは、ネットワーク上の機器を保護する目的で、ネットワークへのアクセスおよびネットワークからのアクセスを制御および監視するために使用されるメカニズムである。ファイアウォールは、通過するトラフィックを所定のセキュリティ基準またはポリシーと比較し、ポリシー要件に合わないメッセージは廃棄する。実質的にファイアウォールは、無用のネットワーク・トラフィックをブロックし、保護されたネットワークと他のネットワーク（インターネットや現場のネットワークの別の区画等）の間に発生する通信の量と種類を制限するフィルタである。図 1 は簡単なファイアウォールを示す。インターネットから来る無用のトラフィックからパーソナルコンピュータ(PC)とプログラマブル論理制御装置(PLC)を保護するが、企業ウェブサーバに来るリクエストは許可する。



Internet	インターネット
Firewall with Filters	フィルタ付きファイアウォール
Incoming HTTP Request to Web Server (Permit)	ウェブサーバ宛ての着信 HTTP リクエスト（許可）
Web Server	ウェブサーバ
PLC	PLC
Incoming telnet Msg to PLC (Deny)	PLC 宛ての着信テルネット・メッセージ（拒否）
Incoming Ping to PC (Deny)	PC 宛ての着信ピング（拒否）

図 1: ネットワーク上の機器を保護するインターネットに対向したファイアウォールの単純な例

2.1 ファイアウォールの種類

ファイアウォールは、多様な設計と構成が可能である。物理的にネットワークに接続した独立したハードウェア機器（Cisco PIX® や Symantec Security Gateway® ファイアウォ

ール等）、OS ベースのファイアウォール機能を有するハードウェア/ソフトウェア・ユニット（Linux® サーバ上で動作する「iptables」等）、さらには保護されるべきワークステーションに直接インストールされる完全にホストベースのソフトウェア・ソリューション（Norton Personal Firewall®や Sygate Personal Firewall®）でもよい。

独立したハードウェア機器やハードウェア/ソフトウェア・ユニットはネットワーク・ファイアウォールとしばしば呼ばれ、通常、PCN と企業ネットワークを分離するのに最も安全な方法である。これは、専用の機能ユニットであり、非常に巧妙な攻撃のほかはすべて阻むように強固にすることができる。さらに、ネットワーク・ファイアウォールは一般に、遠隔管理が可能なように設計されているので、最善の管理オプションを提供する。

ホストベースのファイアウォールは、ホスト機器の主要機能がセキュリティではなく、データベースへのアクセスやウェブサービスなどのためのワークステーションやサーバ機能なので、一般に妥協の産物となる。また、現在のところホストベースのファイアウォール・ソリューションは、Windows か Unix ベースのプラットフォームしか利用できず、PLC などのネットワーク上の組み込み制御機器宛てのトラフィックを規制することは殆どできない。ホストベースのファイアウォールは、セクション 4.2 で述べるアーキテクチャなど、PCN/SCADA ネットワーク上で使用できる箇所があるかもしれないが、一般に本調査の範囲を超えている。したがって、少しの例外はあるが、本文書では、PCN/SCADA ファイアウォールは、専用ハードウェアまたはハードウェア/ソフトウェア・ソリューションであり、一連のルールを通じて、ネットワーク・トラフィックを制御ネットワークに伝えるのを許可または拒否すると考える。

2.2 ファイアウォールのクラス

ネットワーク・トラフィックは、パケットと呼ばれる不連続のビットのグループで送信される。各パケットは通常、幾つかの個別の情報を収容しており、以下の項目などを含む（がそれに限定されない）。

- 送信者 ID（送信元アドレス）
- 受信者 ID（送信先アドレス）
- パケットが関連するサービス（ポート番号）
- ネットワーク運用状態フラグ
- サービスに配達される実際のデータペイロード

ファイアウォールは、パケット受信時、これらの特性を分析し、パケットをどう処理するか決定する。パケットを廃棄する、パケットが直ぐに通過するのを許可する、サービスクラスの帯域幅限界まで少しの間パケットをバッファに格納する、または当初意図された受信者とは異なる受信者にパケットを転送するなどの、ネットワーク・セキュリティ・ポリシーに則ってふさわしい処理を選択する。この決定は、一般にアクセス制御リ

スト(ACL)と呼ばれる一連のルールに基づいている。様々な種類のファイアウォールが存在し、それぞれが、ますます高度の分析と措置能力を有する。

2.2.1 パケットフィルタ・ファイアウォール

最も簡単なファイアウォールの種類は、パケットフィルタ・ファイアウォールとして知られている。一連のスタティック・ルールを持っていて、そのルールを使用して受信パケットを個別に処理する。パケットフィルタ・ファイアウォールは次の見本のルールを容易に処理することができる。

- ユーザ・データグラム・プロトコル(UDP)ポート 53 番のドメインネームサービス（DNS)応答パケットを受入れる。
- インターネット・プロトコル(IP)アドレス 24.116.25.21 との発着信トラフィックをブロックする。
- 伝送制御プロトコル(TCP)ポート 80、443、3128、8000、8080 番にアクセスする発信パケットをブロックしてウェブサーフィンを防ぐ、ただし企業イントラネット・ウェブサーバの IP アドレス宛の場合を除く。
- 送信元に送信されるパケットは廃棄する。
- 技術操作卓用の特定の IP アドレスの範囲から特定の分散制御システム(DCS)の IP アドレスに向かう TCP ポート 23 番（テルネット）トラフィックを受入れる。

残念なことに、パケットフィルタ・ファイアウォールは、一連のパケット間の関係を理解する能力がない。例えば、大まかな規則「UDP ポート 53 番の DNS 応答パケットを受入れる」は、深刻な欠陥を含む。DNS への問い合わせがまったく行われていなくて、なりすましの DNS「応答」パケットが到着したらどうなるだろうか。この簡単なファイアウォールは、そのパケットを受入れ、「リクエストした」ホストに配達し、たぶんそのホストを混乱させるだろう。中程度の知能のハッカーでも、内部システムを危うくするのに、このファイアウォールの弱点を利用することができる。

パケットフィルタリング・ファイアウォールの長所は、コストが低くネットワーク性能への影響が少ないことだが、その理由はたいてい、パケット中のIPアドレスおよびポート番号だけを検査するからである。この方法は、時にはスタティック・フィルタリングとも呼ばれる。[7] たいてい、専用の「ファイアウォール」ではなくて、レイヤ 3(L3)スイッチまたはルータに直接配備される。

2.2.2 ステートフル・ファイアウォール

ステートフル・ファイアウォールとして知られる、より高性能のファイアウォールは、ファイアウォール通過を許可されたパケット間の関係を知的に追跡する。受入れたパケットの履歴と現在の接続の状態を保有することで、「予期していた」トラフィックだけを受入れることができる。ファイアウォールの知能を利用して、ステートフル・ファイアウォールのルールセットを条件付きにすることができる。その例を以下に示す。

- UDP ポート 53 番の DNS 応答パケットが、発信 DNS クエリーと同じ DNS リクエスト ID を有する場合だけ、それを受入れる。
- 制御チャネル・ネゴシエーションの成功後だけ、ファイル転送プロトコル (FTP)データチャネル・トラフィックの通過を許可する。
- 以前発信した HTTP (Hyper-Text Transfer Protocol)リクエストに対する応答でない限り、TCP ポート 80 番発の着信ウェブトラフィックをすべてブロックする。

この種類のファイアウォールは、セキュリティが高く、処理能力がり、エンドユーザからは気づかれることなくサービスを提供できるが、前記の種類より高価である。本質的に複雑であるため、運用者が有能でない場合、簡単な種類のファイアウォールより安全性が低くなることもある。この方法は、ダイナミック・パケットフィルタリングとも呼ばれる。[8]

2.2.3 アプリケーションプロキシ・ファイアウォール

アプリケーションプロキシ・ファイアウォールは、アプリケーションレイヤでパケットを開き、特定のアプリケーション・ルールに基づきそれを処理し、次に再組み立てして希望する目標の機器に転送する。通常アプリケーションプロキシ・ファイアウォールは、1 台のマシンで多様なアプリケーション・プロトコル（Telnet、FTP、HTTP等）を集中して扱い、次いで各サービスに対応する個別のホストコンピュータにトラフィックを転送するように設計されている。外部サーバに直接接続する代わりに、クライアントはプロキシ・ファイアウォールに接続し、次に、そのプロキシサーバは要求された外部サーバへの接続を開始する。使用されるプロキシ・ファイアウォールの種類にもよるが、ユーザに知られずに、内部クライアントが自動的にこの宛先変更を実施するように構成することは可能である。他の種類では、ユーザがプロキシサーバに直接接続し、指定されたフォーマットで接続を開始する必要があるかもしれない。[9]

プロキシ・ファイアウォールは、ファイアウォールが認識できるプロトコルを制御する、重要なセキュリティ機能を提供する。例えば、アクセスを許可する前に、アプリケーション・プロトコルにユーザまたはシステムに追加の認証情報を提供することを要請する、アクセス制御リストを適用することができる。さらに、特定のプロトコルの内容にかかわるルールセットを作成し、そのプロトコルのサブセクションだけをブロックするようにすることができる。例えば、HTTP に対するファイアウォール・ルールは、スクリプトを含む着信 HTTP トラフィックをすべてブロックするように作成できる。それに反して、フィルタリング・ルータは HTTP トラフィックをすべてブロックするか、全然ブロックしないかで、サブセットだけをブロックすることはできない。

この種類のファイアウォールは、高いセキュリティを提供できるが、ネットワークの性能にかなり大きな影響を及ぼすことがある。さらに、たいていのアプリケーションプロキシ・ファイアウォール製品は、HTTP、FTP、SMTP (Simple Mail Transfer Protocol)などの普及しているインターネット・プロトコルだけをサポートする。そのため、コモン・

インダストリアル・プロトコル®(CIP)やMODBUS/TCP®などの産業用アプリケーションレイヤ・プロトコルを含むメッセージを処理するには、ファイアウォールがステートフル・モードまたはパケットフィルタ・モードでトラフィックを処理する必要があるだろう。[10]

ここ何年間、市場のファイアウォールの大部分は、ステートフル技術とアプリケーションプロキシ技術を組み合わせて使用しており、しばしばハイブリッド・ファイアウォールと呼ばれる。

2.2.4 ディープ・パケット・インスペクション・ファイアウォール

ファイアウォール市場は、「ディープ・パケット・インスペクション」(DPI)または「アプリケーション・ファイアウォーリング」と呼ばれる、第 4 の技術に向かって進んでいる。従来のアプリケーションプロキシに較べ、アプリケーションレイヤにより深く入ったフィルタリングを通常提供するが、TCP 接続上でフルプロキシを実施しない。例えば、DPI ファイアウォールは、ウェブ接続上で拡張マークアップ言語(XML)で書かれた SOAP (Simple Object Access Protocol)を検査することができ、どのオブジェクトがネットワークに入るのを許可/拒否するかのポリシーを実施することができる。この市場はまだ発展中である。

2.3 他のファイアウォール・サービス

トラフィックにフィルタをかける中核サービスに加えて、ごく最近のファイアウォールは、ネットワークベースの他のセキュリティサービスを提供する。これには、以下が含まれる。

1. 問題を起こすように特に設計されたネットワーク・パケットを見分けて、アクセスを拒否したパケットを記録するか、異常なトラフィックパターンを報告することで、侵入検知システム(IDS)の機能を果たす。

2. ファイアウォール上に「最前線」アンチウィルス・ソフトウェアを配備する。感染したトラフィックの特徴が判明した場合、そのトラフィックがネットワークに入る前にブロックできる。

3. ファイアウォールの反対側にある機器に接続したいユーザに、パスワードかそれとも公開鍵暗号などの強力な 2 因子認証方法を使用して、ファイアウォールに対して本物であることを証明するよう要求する認証サービス。

4. ファイアウォールと遠隔ホスト機器の間に暗号化トンネルが設定されている仮想プライベートネットワーク (VPN) ゲートウェイ・サービス。

5. ファイアウォールの一方の側で使用される 1 セットの IP アドレスが反対側で異なるセットにマッピングされる、ネットワーク・アドレス変換 (NAT)。

提供される付加サービスは、購入するファイアウォールの個々の製造元とモデルによって異なる。この付加機能は、コストの追加、複雑さの増加、処理能力の低下を意味することがある。しかし、ファイアウォールを使用することにより、PCN/SCADA ネットワークの全体的なセキュリティをしばしば著しく向上することができる。付加セキュリティサービスのこの種の分析は、本書の範囲を超えているが、設計を行うときや購入を決定するときに、読者が考慮することを勧める。

3 PCN/SCADA ファイアウォールの総合セキュリティ目標

理想を言えば、PCN または SCADA ネットワークは、閉ざされたシステムであって、ヒューマン・マシン・インターフェース(HMI) ステーションやデータ・ヒストリアンなどの信頼できる内部コンポーネントだけがアクセスできるようになっているのが望ましい。現実には、企業ユーザと選ばれたサード・パーティの双方が、外部からアクセスする必要がある。例えば、製造維持管理情報は、管理目的で生産現場の外のコンピュータやユーザに中継する必要がある一方、ベンダーは、サポート目的で制御装置にアクセスする必要があるかもしれない。暗黙のうちにこのことは、外の信頼できない世界と内部の制御コンポーネントの間にネットワークのパスが存在することを意味する。

ファイアウォールの目的は、簡単に言うと、PCN や SCADA システム上の内部コンポーネントへの不正アクセス（または不正なネットワーク・トラフィック）のリスクをできるだけ少なくすることである。そのリスク最小化戦略には通常、以下の一般目標が含まれる。

1. **インターネットから PCN/SCADA ネットワークへの直接接続はない、およびその逆もない。**この理由は、かなり明白であり、以下が含まれる。

   (a) 求められていないインバウンド・トラフィックは、制御ネットワークを輻輳または混乱させ、重要なメッセージが制御機器に到達するのを妨げることがある。

   (b) 無効な制御メッセージまたはサービス不能(DoS)攻撃が制御機器に向けられ、生産を混乱させることがある。

   (c) アウトバウンド・インターネット・トラフィック（FTP、HTTP、SMTP等）は、PCNから発信される場合でさえ、重要な制御トラフィックを輻輳させることがある。さらに、インターネットから受信した埋め込みオブジェクト（添付ファイル、Java®アプレット、Active X®コンポーネント）は、制御ワークステーションを危うくし、その結果、制御ネットワークが遠隔からの攻撃の犠牲になることがある。

   (d) 機密の企業製造データが横取りされる恐れがある。

2. **企業ネットワークから制御ネットワークへのアクセス制限。**企業ネットワークは、生産現場/SCADA レベルの PLC または他の制御機器に、直接問い合わせまたは制御できるべきでない。物理的と論理的の両面で、企業ネットワークと PCN は、隔離されるべきである。

3. **企業ネットワークから PCN/企業共有サーバへの非制限（だが許可されたものだけの）アクセス。**データ・ヒストリアンや保守データベースのような典型的な共有サーバは、制御ネットワークに問い合わせのアクセスを行い、問い合わせをした業務サービスに関連情報を返信する。

4. **制御システムの許可された遠隔サポートに対する安全な方法。**多くの会社が、システムベンダーによるサポートを受けるために PLC/DCS/SCADA 機器へのサード・パーティアクセスを許可する必要がある。緊急保守のために遠く離れた場所から工場の適切なスタッフが、制御ネットワークにアクセスするのを許可する会社もある。両方とも、ファイアウォールの設計の中で明示的に扱う必要がある。

5. **無線機器（使用される場合）に対する安全な接続。**適切なセキュリティが実施されていない場合、生産現場の無線機器は、外界との接続が規制されていないのに等しい。規制されていないインターネット接続と同様に、無効または破壊的な通信メッセージが深刻な運用障害を引き起こす恐れがある。

6. **ネットワーク上で許可されるトラフィックの種類を概観する明確なルール。**このルールは、アクセス制御リスト(ACL)および仮想ローカルエリアネットワーク(VLAN)などのメカニズムによって実施される。トラフィックが PCN 上で予期されていない場合、通過を許可すべきでない。

7. **PCNに入り居座ることを試みるトラフィックの監視。**PCNまたはSCADAネットワークの中に入るまたはそのネットワーク上に居ることを試みる通信トラフィックの性質とパターンに気づくことは重要である。これが、ネットワークへの攻撃かまたはファイアウォール戦略の欠陥を示す唯一の兆候になることが多いからである。これは一般に、侵入検知システム(IDS)を用いて行い、ファイアウォールに組み込まれるかまたは外部機器上で動作する。[i]

8. **ファイアウォール管理用の安全な接続。**ファイアウォールの監視および管理用のトラフィックは、非常に制限された管理機器セットから発信し、セキュアな通信システム上で運ぶべきである。

[i] ファイアウォールに加えてまたはその代わりに、基本PCNトラフィックに使用できる他の監視方法があることに注意することが重要である。例えば、ルータやスイッチのネットフロー機能はトラフィック統計を収集でき、独立した異常検知IDSシステムに組み入れることができる。

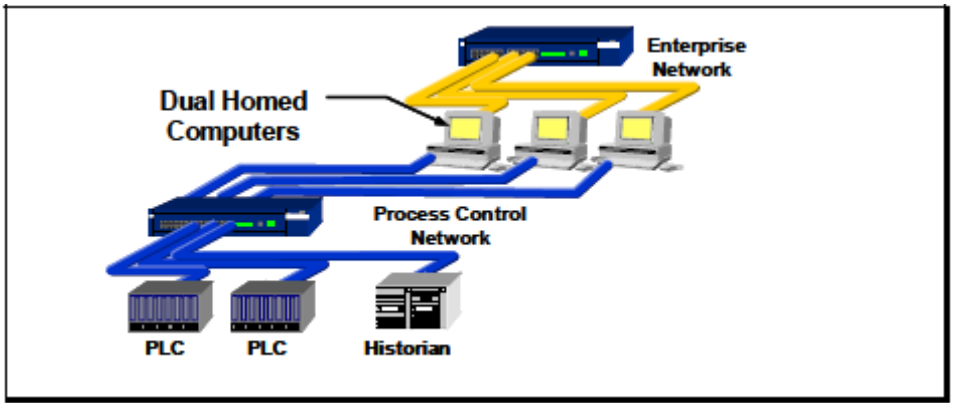
4 代表的な SCADA/PCN 隔離アーキテクチャ

セキュリティ/ファイアウォール/制御システムのベンダー、標準化機関、エンドユーザから収集した文献の調査により、PCN/SCADA ネットワークと企業ネットワークを分離するのに使用される、ネットワーク全体にわたる 8 つのアーキテクチャが得られた。これらは、ネットワーク・インターフェース・カード 2 枚を有するホストから、ファイアウォール、スイッチ、ルータを複層に組み合わせたものまで多岐にわたる。以下にそれぞれを記述し、長所と短所を分析し、以下の評価基準毎に 1（最低）から 5（最高）までの評点をつける。

- **セキュリティ**－起こりそうな攻撃を防ぐアーキテクチャの有効性の度合い
- **管理容易性**－容易且つ効果的にアーキテクチャを管理できる度合い（現地と遠隔の両方で）
- **スケーラビリティ**－アーキテクチャを大規模と小規模の両システムに効果的に配備できる度合い

4.1 デュアルホーミングのコンピュータ

提案の多かったセキュリティ対策は、企業ネットワークとプロセス制御ネットワークの双方に情報アクセスを必要とするワークステーションまたは制御機器に、ネットワーク・インタフェース・カード(NIC)を 2 枚設置するものである。この技術は、しばしばデュアルホーミングと呼ばれる。この設計の典型的な概略図を図 2 に示す。



1	Enterprise Network	企業ネットワーク
2	Process Control Network	プロセス制御ネットワーク
3	Dual Homed Computers	デュアルホーミングのサーバ
4	HMI	HMI（ヒューマン・マシン・インターフェース）
5	PLC	PLC
6	Historian	ヒストリアン

図 2: デュアルホーミングのコンピュータを使用するネットワーク分離

API 標準 1164 の付属書 B で、以下のように言及されている。

> *「コンピュータをデュアルホーミングにすると、コンピュータが 2 つの異なるネットワークに接続することが可能になり、確かに便利な方法である。しかし、安全上の理由で隔離されている 2 つのネットワーク間の通信にデュアルホーミングが使用されている場合、このコンピュータは深刻なセキュリティ・リスクとなる。」*[11]

理想的に構成されたシステムでは、この方法は、最小限のネットワーク分離を可能にする。しかし、大多数の機器に対して、1 つのネットワークに到着したパケットを別のネットワークに自動的に転送するように、機器のネットワーク設定パラメータを調整することは容易なことであり、それによって、ネットワーク隔離の前提の裏をかくことができる。実際のところ、デュアルホームミングのサーバは、ハッカーの社会でいいカモと見られている。例えば、「デュアルホーミングのコンピュータ」という用語を探すことにより、以下の会話をウェブ上で見つけることができる。

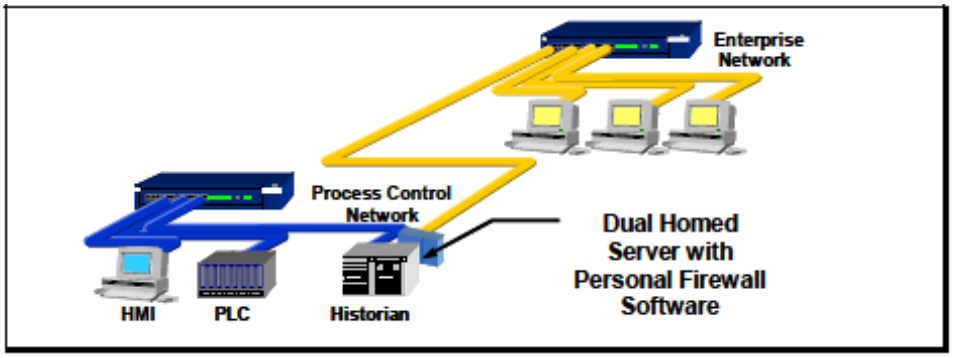
> *ファイアウォールをどう回避するかだって。おいしい狙い目はデュアルホーミングのマシンだ。それは、DMZ と内部ネットワークの両方に接続する 2 枚の NIC を有するコンピュータだ。理論的にあるべきではないが、実際には、ユーザ（そうだなー、パワーユーザと開発者）は、より素早く仕事をできるように頻繁にこれを使用している。*[12]

さらに、2 枚の NIC を持つ機器は PCN の一部であり、インターネットにアクセスするネットワークにも所属して、ウェブブラウザなどの典型的に安全でないソフトウェアを実行できるで、このアーキテクチャは、「PCN から直接インターネットに接続することはない」というセキュリティ目標に違反しかねない。さらに、デュアルホーミングのコンピュータが侵入されると、両方のネットワークも侵入されることになる。2003 年 1 月の Slammer worm にかかわる幾つかのプロセス制御の事件は、この種のアーキテクチャで起きた。最後に、パーソナルコンピュータ向けの遠隔管理ソフトウェアは存在するが、少なからぬデュアルホーミングのマシンを安全且つ効果的に管理するには、並々ならぬ努力が必要である。

要約すると、デュアルホーミングのコンピュータは、同じネットワーク上かまたは同じ PCN システム内の 2 つのネットワーク上にある冗長機器に対しては役立つが、企業/PCN 隔離手段としての使用は、決して理想的ではない。**[セキュリティ＝1、管理容易性＝2、スケーラビリティ＝1]**

4.2 パーソナル・ファイアウォール・ソフトウェアを有するデュアルホーミングのサーバ

前のアーキテクチャの 1 変形は、図 3 に示すように 1 台のデュアルホーミングのマシン（通常はデータ・ヒストリアン・サーバ）にホストベースのパーソナル・ファイアウォール・ソフトウェアのインストールしたものである。PCN と企業ネットワーク間の唯一のトラフィックは共有履歴データであり、これはいずれにしろサーバ上で終了する。したがって、パーソナル・ファイアウォールをサーバから業務ユーザへのデータ要求だけを許可するように使用し、サーバを安価なパーソナル・ファイアウォールで保護するのであれば、非常に安いセキュリティ・メカニズムを実現できるだろう。



1	Enterprise Network	企業ネットワーク
2	Process Control Network	プロセス制御ネットワーク
3	Dual Homed Server with Personal Firewall Software	パーソナル・ファイアウォール・ソフトウェアを有するデュアルホーミングのサーバ
4	HMI	HMI
5	PLC	PLC
6	Historian	ヒストリアン

図 3: パーソナル・ファイアウォール・ソフトウェアをインストールした、デュアルホーミングのサーバを使用するネットワーク分離

このソリューションの第 1 の問題は、サーバデータの共有を許可する仕組みを提供するだけということである。PCN から EN へ境界を横切る必要のある他のトラフィック（コントローラへの遠隔保守アクセス等）がある場合、このアーキテクチャはそのトラフィックを完全にブロックするか、または PCN のセキュリティを低くする。この設計では、細かい調整はできない。

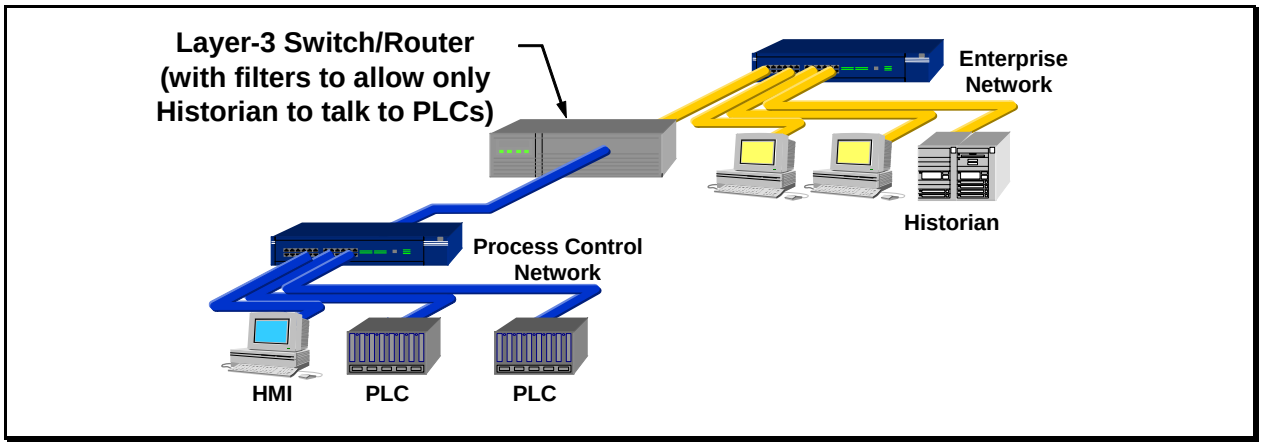
2 番目の問題は、2 台以上のサーバがかかわる場合に生じる。たいていのパーソナル・ファイアウォール・パッケージの遠隔管理はかなり限られており、複数のサーバにわたって首尾一貫したルールセットと管理サービスを維持することは、非常に時間がかかる。最後に、パーソナル・ファイアウォールは、システム強化、ステートフル・インスペクション、スループット、または IDS のような付加機能の面で正式のネットワーク・フ

ファイアウォールには太刀打ちできない。したがって、このアーキテクチャは、非常に安いが、非常に限定的な隔離ソリューションである。

[セキュリティ＝2、管理容易性＝1、スケーラビリティ＝1]

4.3 PCN と EN の間のパケットフィルタリング・ルータ/L3 スイッチ

幾つかのベンダーの設計資料および初期の産業界の文書[13]は、トラフィックを制御する基本的なフィルタを装備したブリッジ、ルータまたはL3 スイッチの使用を推奨していた。典型的な設計の概略を図 4 に示す。これらの機器の多くは、事実上パケットフィルタ・ファイアウォールの機能を果たし、前述のように、高度な攻撃に対して限定的な保護を提供する。基本的な機器から機器へのルールセットを実施する効果はあるが、ステートフル・インスペクションがないので、パケットの内容をあいまいにするパケット・フラグメンテーションなどの技術を巧みに利用する攻撃を防ぐことはできないだろう。



Layer-3 Switch/Router (with filters to allow only Historian to talk to PLCs)	L3 スイッチ/ルータ（ヒストリアンだけが PLC と通話するのを許可するフィルタ付き）
Enterprise Network	企業ネットワーク
Historian	ヒストリアン
Process Control Network	プロセス制御ネットワーク
HMI	HMI
PLC	PLC

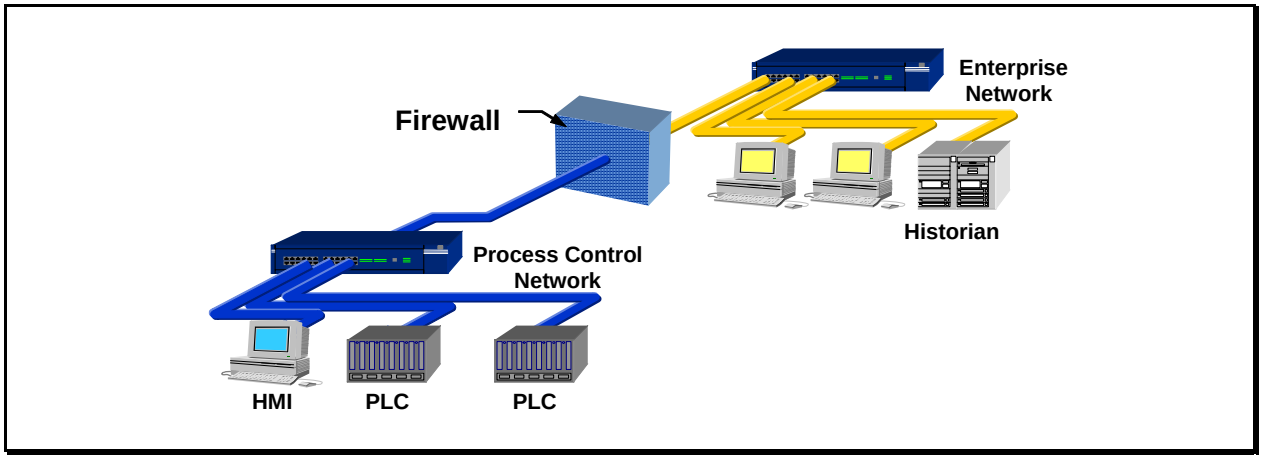
図 4: ACL フィルタ付きネットワーク隔離ルータまたは L3 スイッチ

この種のパケットフィルタ設計が安全なのは、企業ネットワークがそれ自体で高度に安全で、通常攻撃にさらされていない場合だけである。他方、幾つかの市場の高性能のルータは現在、比較的安価にステートフル・ファイアウォールにアップグレードできる。アップグレードする場合、このアーキテクチャは、セクション 4.4 または 4.6 で検討されるアーキテクチャと同等と見做すことができる。**[セキュリティ＝2、管理容易性＝2、スケーラビリティ＝4]**

4.4 PCN と EN の間に 2 ポートのファイアウォール

企業ネットワークとプロセス制御ネットワークの間に簡単な 2 ポートのファイアウォールを導入することにより、セキュリティを大きく改善することができる。現市場の大部分のファイアウォールは、全 TCP パケットに対しステートフル・インスペクションを提供し、FTP、HTTP、SMTP などの普及しているインターネット・アプリケーション レイヤ・プロトコルに対してアプリケーション・プロキシサービスを提供する。強固に設定すれば、PCN への外部からの攻撃が成功する可能性を大幅に減少することができる。この調査のために面談した企業の多くは、PCN/SCADA セキュリティの標準設計としてこれを使用していた。

残念なことに、この設計には 2 つの問題が残る。第 1 に、企業/PCN が共有するサーバ（データ・ヒストリアン等）はどちらのネットワーク上に配置されるか。データ・ヒストリアンが企業ネットワーク上に存在する場合、データ・ヒストリアンが PCN 上の制御機器と通信するのを許可するルールが、ファイアウォール内に存在しなければならない。企業ネットワーク上の悪意あるホストまたは間違って設定されたホストを起源とする（データ・ヒストリアンのように見える）パケットは、個々の PLC に転送されるだろう。



Enterprise Network	企業ネットワーク
Historian	ヒストリアン
Firewall	ファイアウォール
Process Control Network	プロセス制御ネットワーク
HMI	HMI
PLC	PLC

図 5: 1 台のファイアウォールによるネットワーク分離

データ・ヒストリアンがプロセス制御ネットワーク上に存在する場合、企業の全ホストがヒストリアンと通信するのを許可するファイアウォール・ルールが存在しなければならない。通常は、この通信は構造化照会言語(SQL)または HTTP がリクエストするとき

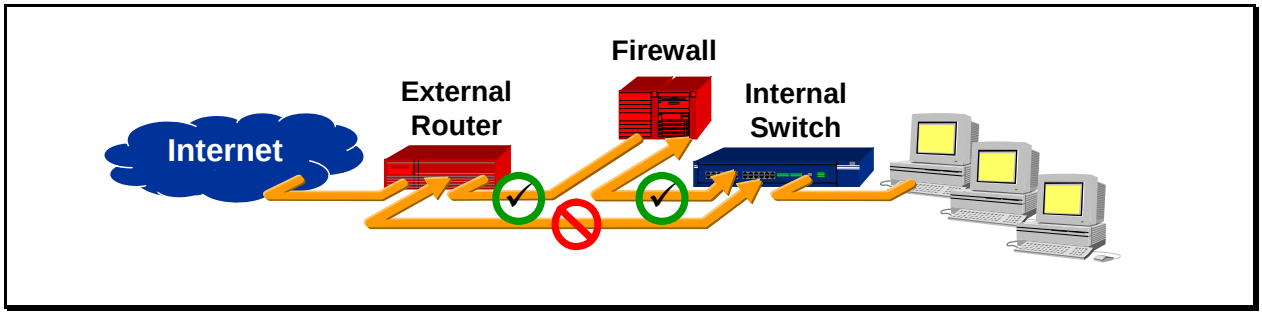
に起こり、ヒストリアンのアプリケーションレイヤ・コードの欠陥がヒストリアンを危うくすることがある。いったんヒストリアンが危うくされると、プロセス制御ネットワーク上の残りのノードは、ワーム/ウィルスの増殖またはインタラクティブ攻撃を受けやすくなる。

第 2 に、PCN に影響を及ぼすことができるなりすましパケットが組み立てられ、変換されたデータが許可されたプロトコルの中をトンネルで抜けることができるかもしれない。例えば、HTTP パケットがファイアウォールの通過を許可された場合、HMI または PCN のラップトップに偶然に取り込まれたトロイの木馬ソフトウェアは、遠隔の人物から制御され、データ（取得したパスワード等）を正当なトラフィックと偽装してその人物に送信することが起こりうる。

要約すると、このアーキテクチャは先の 2 つに対して大幅な改善ではあるが、ルールセットの中に企業の機器と PCN/SCADA 機器の間の直接通信を許可するという開口部を作る必要がある。このことは、非常に注意深く設計し監視しないと、セキュリティが侵害される恐れがある。**[セキュリティ＝3、管理容易性＝5、スケーラビリティ＝4]**

4.5 PCN と EN の間にルータとファイアウォールの組み合わせ

少しだけより高度な設計は、ルータとファイアウォールを組み合わせることである。ルータがファイアウォールの前に置かれ、基本的なパケットフィルタリング・サービスを提供する一方で、ファイアウォールはステートフル・インスペクション技術かまたはプロキシ技術を使用してもっと複雑な問題を扱う。この種の設計は、インターネットに面するファイアウォールでは非常に多く使用されている。その理由は、DoS 攻撃の場合は特にそうだが、大量の着信パケットを高速なルータが扱うため、ファイアウォールの負荷が減るからである。攻撃者が擦り抜けなければならない 2 つの非常に異なる機器があるので、深層防護も向上する。最後に、ルータ内の簡単なルールにより、パケットが複雑なアーキテクチャのファイアウォールの裏をかくのを防ぐことができる。



Internet	インターネット
External Router	外部ルータ
Firewall	ファイアウォール
Internal Switch	内部スイッチ

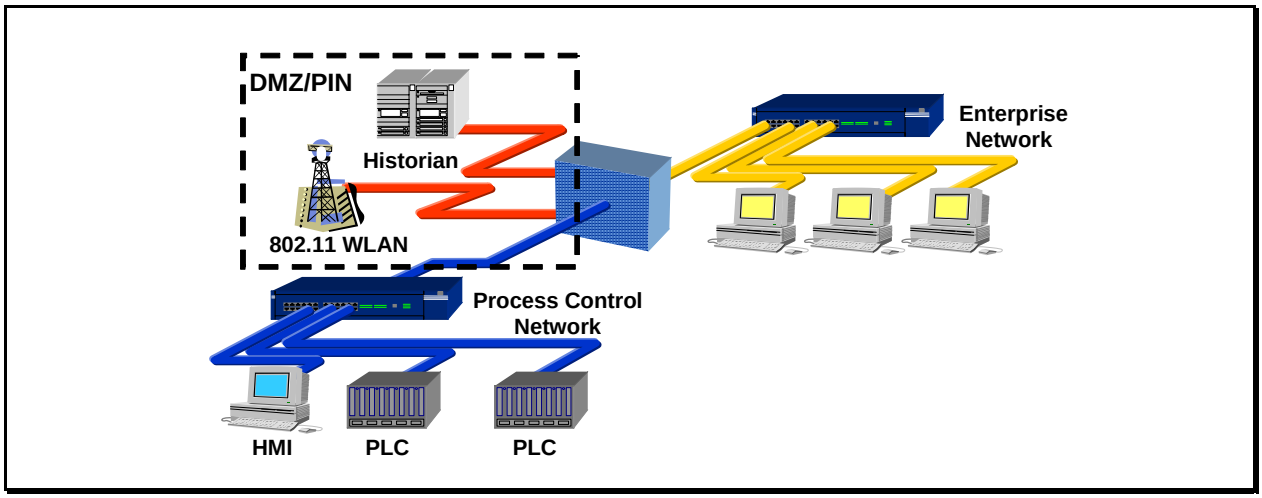
図 6: ファイアウォールとルータの組み合わせによるネットワーク分離（インターネットの例）

不定期に発行される産業用文書の中では言及される（企業 IT の世界では非常に人気がある）が、この設計は、PCN/SCADA 環境ではめったに使用されないようである。調査チームが発見した 2、3 の例では、PCN/SCADA ファイアウォールの前に置かれたルータは、セキュリティ機能のために使用されているようには見えなかった。**[セキュリティ＝3.5、管理容易性＝3、スケーラビリティ＝4]**

4.6 PCN と EN の間に非武装地帯を持つファイアウォール

幾つかの非武装地帯(DMZ)を設定できるファイアウォールを企業ネットワークとプロセス制御ネットワークの間で使用することにより、著しく改善できる。各 DMZ は、データ・ヒストリアン、ワイヤレス・アクセス・ポイントまたは遠隔やサード・パーティ・アクセスシステムなどの個別の「重要な」コンポーネントを収容する。実質的に、DMZ 能力があるファイアウォールの使用により、プロセス情報ネットワーク(PIN)と呼ばれることのある中間ネットワークの作成を可能にする。

DMZ を作成するには、ファイアウォールが、通常のパブリックとプライベートのインターフェースでなく、3 つ以上のインターフェースを提供する必要がある。インターフェースの 1 つは、企業ネットワークに接続し、第 2 は、PCN/SCADA ネットワークに接続し、残りのインターフェースは、データ・ヒストリアン・サーバまたはワイヤレス・アクセス・ポイントなどの共有または安全でない機器と接続する。図 7 は、PCN/SCADA 環境における典型的な DMZ ファイアウォール設計を示す。



Enterprise Network	企業ネットワーク
DMZ/PIN	DMZ/PIN
Historian	ヒストリアン
802.11 WLAN	802.11 無線 LAN
Process Control Network	プロセス制御ネットワーク
HMI	HMI

PLC	PLC

図 7:企業/PCN 共有機器用の非武装地帯を持つファイアウォール

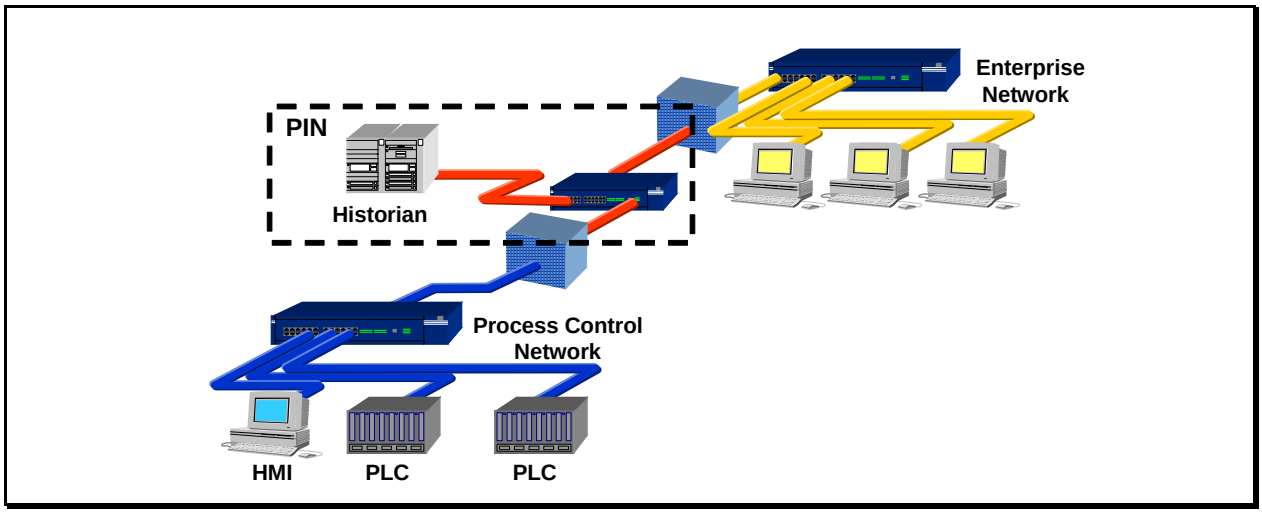
企業がアクセスできる機器を DMZ に置くことにより、企業ネットワークから生産現場への直接の通信パスは不要で、各ネットワークは事実上 DMZ で終端する。たいていの高度なファイアウォールでは、複数の DMZ を設定可能で、どの種類のトラフィックを DMZ のゾーン間で転送できるかを指定できる。上記のように、ファイアウォールは企業ネットワークからの恣意的なパケットが PCN に入るのをブロックするが、他のネットワークゾーンからのトラフィックも規制する。アクセス制御リストを慎重に使用することにより、PCN ネットワークと他のネットワークの間に、企業ネットワークと PCN/SCADA ネットワークの間を通過するトラフィックが殆ど、またはまったくない、明確な分離が可能である。

この種のアーキテクチャの主要なセキュリティ・リスクは、DMZ 内のコンピュータが侵害された場合、攻撃者はそのコンピュータを、DMZ から PCN へ許可されたアプリケーション・トラフィックを使用して、PCN に対する攻撃を開始するのに使用できることである。DMZ 内のサーバを強固にし、パッチを当てるよう協調努力し、且つ PCN 機器が開始した PCN と DMZ の間の接続だけを許可するようにファイアウォール・ルールを設定することにより、このリスクは大幅に減らすことができる。

面談したエンドユーザがこの設計について懸念していることは、複雑さが増すことと（1 社は、インターフェースが複数あるためACLルールが複雑になり、エラーの可能性を増すと指摘した）、3 つ以上のポートを持つファイアウォールはコストが高いことである。しかし、調査チームは、セキュリティの改善がこの短所を相殺する以上の効果があると信じる。API-1164 などの幾つかの標準および幾つかの高度なベンダー[14][15]とエンドユーザの文書は、この種の設計を提案している。**[セキュリティ＝4、管理容易性＝4.5、スケーラビリティ＝4]**

4.7　PCN と EN の間の 1 対のファイアウォール

DMZを有するファイアウォールを使用するソリューションの変形は、企業ネットワークとPCNの間に 1 対のファイアウォールを配置することである。（データ・ヒストリアン等）共有サーバは、ファイアウォールとファイアウォールの間の、PINレイヤまたは生産実行システム(MES)レイヤと呼ばれるDMZのようなネットワークゾーンに置かれる。[16] 上記のアーキテクチャのように、第 1 のファイアウォールが、恣意的なパケットがプロセス制御ネットワークまたは共有のヒストリアンに進むのをブロックする。第 2 のファイアウォールは、侵害されたサーバから無用のトラフィックがPCNに入るのを防ぐか、またはPCNトラフィックが共有サーバに影響を及ぼすのを防ぐことができる。



Enterprise Network	企業ネットワーク
PIN	PIN
Historian	ヒストリアン
Process Control Network	プロセス制御ネットワーク
HMI	HMI
PLC	PLC

図 8:企業/PCN 共有資産用の非武装地帯を有する 1 対のファイアウォール

異なる製造業者 2 社のファイアウォールが使用された場合、このソリューションは「深層防護」の長所を提供する可能性がある。[ii] また、プロセス制御グループおよびITグループは、それぞれが自グループのファイアウォールを管理することができるので、責任対象の機器を明確に分離できる。実際に、連邦エネルギー規制委員会(FERC)のセキュリティ標準に関する提案の中でこの設計が推奨されているのはこの理由からだと、本調査チームは理解している。

このアーキテクチャの変形は、「企業ネットワークー制御ネットワーク・プロファイル(ECI) [17]」に関するIEC/SC65C/WG13 草稿の基礎となっている。しかし、ENからDMZへのファイアウォールとしてルータを提案しており、全体的なセキュリティを弱くする可能性がある。ルータにより提供されるパケットフィルタリング・サービスは、DMZ内のサーバをENからの高度な攻撃にさらす可能性があり、侵害された場合、PCNへの攻撃の足場として使用されうる。

2 台のファイアウォールを持つアーキテクチャの主要な短所は、コストの上昇と管理の複雑さである。厳しいセキュリティ要件や明確な管理の分離の必要性がある環境では、

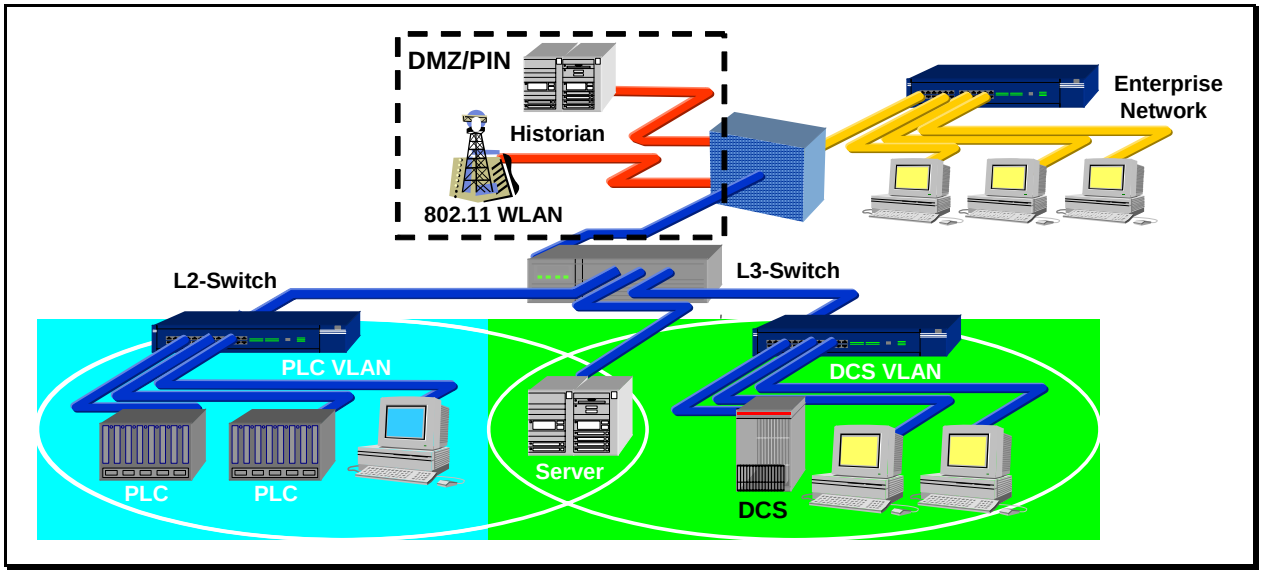
[ii] ファイウォール自体が破られることはまれにしかないので、2 つの異なるファイアウォール使用することで、著しい利益があるかどうかについては議論の余地がある。現在観測されているPCNへの侵入の大半は、許可されたサービスを通じてのウィルス/ワームの通過かまたはベンダーに無関係のファイアウォール設定ミスの結果である。

このアーキテクチャに優れた長所がある。**[セキュリティ＝5、管理容易性＝3、スケーラビリティ＝3.5]**

4.8 ファイアウォールと VLAN ベースのプロセス・ネットワークの組み合わせ

これまでの設計では、PCN/SCADA ネットワークをただ 1 つの存在として扱ってきた。しかし、多くの事例で、PCN や SCADA システム内に機能上の区画やセルがあり、区画間の通信は必要ない（またはたぶん望まれない）。SCADA や PCN を幾つかの VLAN にさらに分割するように上記のアーキテクチャを拡張すると、L3 スイッチ内の簡単なパケットフィルタで VLAN 間通信を制御できる。L3 スイッチの下に幾つかの VLAN 用の L2 スイッチがあり、同一 VLAN 上の機器間の直接通信を扱うが、VLAN 間のトラフィックについては L3 スイッチのフィルタリングに委ねる。

VLAN は、PCN スタッフによる不測のアクセスまたは持ち込まれたウィルスからの無用なトラフィックが、PCN 全体にわたり伝搬するのを防ぐ。この設計は、「PCN 上のラップトップが持ち込むウィルス」の問題を軽減するのにも役立つ。VLAN と企業ネットワークの間の他のファイアウォールの結果として、PCN/SCADA 環境のセキュリティが高いと想定すると、それ以上に高度なファイアウォールはこのレベルでは必要とされない。



Enterprise Network	企業ネットワーク
DMZ/PIN	DMZ/PIN
Historian	ヒストリアン
802.11 WLAN	802.11 無線 LAN
L2-Switch	L2 スイッチ
L3-Switch	L3 スイッチ
PLC VLAN	PLC VLAN

DCS VLAN	DCS VLAN
PLC	PLC
Server	サーバ
DCS	DCS

図 9: 非武装地帯を有するファイアウォールと SCADA/PCN VLAN

いくつかの主要自動車製造業者は、この設計の変形を使用している。DMZ もこの設計で使用されていれば、このアーキテクチャは非常に安全である。主要な短所は、管理の複雑さとコストの上昇である。**[セキュリティ＝4.5、管理容易性＝3、スケーラビリティ＝5]**

4.9 ファイアウォール・アーキテクチャの要約

本調査中記録された PCN/SCADA と EN を隔離する 8 つのアーキテクチャは、3 つの一般的な種類に分けることができる。

1. デュアルホーミングのワークステーション、ブリッジ、ルータなどの非ファイアウォール機器を使用する分離（アーキテクチャ 1～3）

2. DMZ のない 2 ゾーン・ファイアウォールを基にした設計（アーキテクチャ 4、5）

3. DMZ を有する 3 ゾーン・ファイアウォールを基にした設計（アーキテクチャ 6～8）

表 1 に、8 つの隔離アーキテクチャのそれぞれに対し、セキュリティ、管理容易性、スケーラビリティに関する調査チームの評価を示す。図 10 は、同じ情報をグラフで示している。これらの評価はおおよそのものであり、報告書の時点で広く利用できる技術だけが使用され、典型的な設定で利用されるという想定に基づいていることに注意することは大事である。例外的な環境、技術または配備では、これらの評価を状況に合わせて変える必要がある。

表 1：PCN/SCADA 隔離アーキテクチャに対するセキュリティ、管理容易性、スケーラビリティの概略評価

アーキテクチャ	セキュリティ	管理容易性	スケーラビリティ
1 デュアルホーミングのコンピュータ	1	2	1
2 パーソナル・ファイアウォールを有するデュアルホーミングのサーバ	2	1	1

3 パケットフィルタリング・ルータ/L3 スイッチ	2	2	4
4 2 ポート・ファイアウォール	3	5	4
5 ルータとファイアウォールの組み合わせ	3.5	3	4
6 DMZ を有するファイアウォール	4	4.5	4
7 1 対のファイアウォール	5	3	3.5
8 ファイアウォールの VLAN ベースの組み合わせ	4.5	3	5

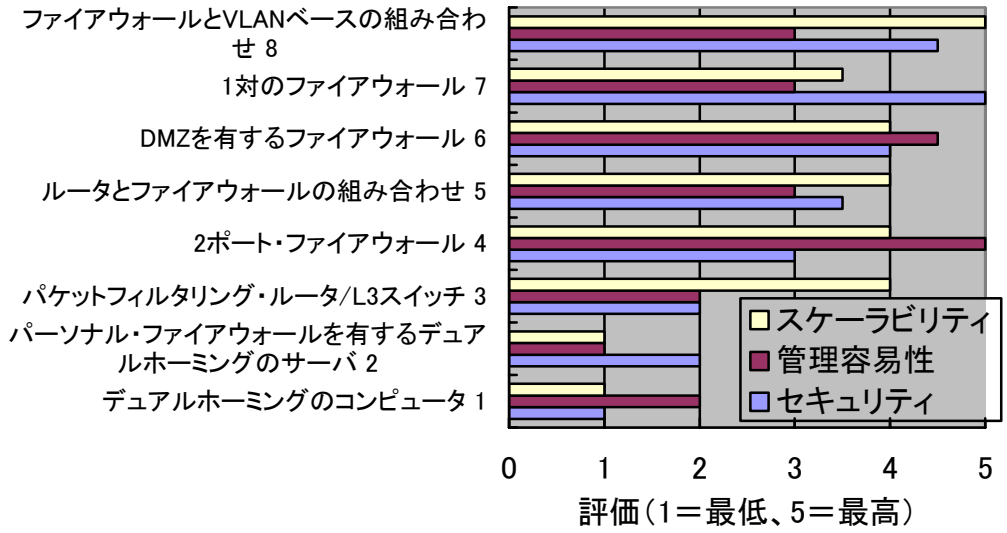


図 10：**PCN/SCADA 隔離アーキテクチャ比較図**

要約すると、調査チームの見解は、次のとおりである。ファイアウォールを使用しない対策は一般に、PCN/SCADA ネットワークと企業ネットワークの間に適切に隔離できない。2 ゾーン対策は辛うじて受入れることができるが、細心の注意を払って配備すべきである。最も安全で管理が容易でスケーラビリティがある PCN/SCADA 隔離アーキテクチャは、セクション 4.6、4.7、4.8 で記述されたアーキテクチャのような 3 ゾーン・システムである。

ここは空白ページである。

5 ファイアウォールの実装と設定

5.1 一般ファイアウォール・ポリシー

いったんファイアウォール・アーキテクチャが決まると、厳密にどのトラフィックがファイアウォールを通過することを許可するかを決定する作業が始まる。RFC (Request for Comment) 2196 のサイト・セキュリティ・ハンドブックが以下のように述べている。

> *難しい部分は、ドアを通るパケットのアクセスを許可または拒否する基準を確立することである。*[18]

業務の必要性から絶対に必要なピンホールを除いて、ファイアウォールを「すべて拒否(Deny All)」に設定することは、あらゆる企業の基本前提であるが、現実ははるかに複雑である。「業務に絶対必要」とは正確には何を意味するだろうか、それらの「ピンホール」を開けることはセキュリティへどう影響するだろうか。例えば、多くの会社は、多くのデータ・ヒストリアン・サーバに関する業務のために、SQLトラフィックにファイアウォールの通過を認めることが必要だとしている。残念なことに、SQLはSlammer wormに対する病原媒介物でもあった。現実は、HTTP、FTP、OPC®/DCOM®、EtherNet/IP™、MODBUS/TCPなどの産業界で使用される多くの重要プロトコルが、深刻なセキュリティ・リスクである。

共有サーバに対し DMZ のない簡単な 2 ポートのファイアウォールを設置する場合（すなわち、セクション 4.4 に記述されたアーキテクチャ）、ルールの設計で細心の注意を払う必要がある。最低でも全ルールは、IP アドレスとポート（アプリケーション）の両方を限定するステートフル・ルールであるべきである。ルールのアドレス部分は、企業ネットワーク上のアドレスの管理されたセットから、PCN 上の共有機器（例えばデータ・ヒストリアン）の非常に小さいセットに着信するように、トラフィックを制限すべきである。企業ネットワーク上のどの IP アドレスからも PCN 内のサーバにアクセスできるように許可することは、推奨されない。さらに、許可するポートは、HTTPS などの比較的安全なプロトコルに注意深く限定すべきである。HTTP、FTP または暗号化されていない SCADA プロトコルがファイアウォールを通過するのを許可することは、トラフィックを盗聴されたり変更されたりする危険があるので、セキュリティ・リスクである。

一方、DMZ アーキテクチャが使用された場合、企業ネットワークと PCN/SCADA ネットワークの間を直接行き来するトラフィックがないように、システムを設定することは可能である。少しの特別の例外はあるが（以下に記述）、どちら側のトラフィックもすべて DMZ 内のサーバで終端できる。これにより、ファイアウォールの通過を許可するプロトコルを柔軟に選択できる。例えば、PLC からデータ・ヒストリアンへの通信には MODBUS/TCP を使用し、ヒストリアンと企業クライアントの間の通信には HTTP を使用する。両プロトコルは、本質的に安全でないが、それでもこの場合、両プロトコルとも企業と PCN の間を行き来しないので、安全に使用できる。

この概念の拡張として、すべての PCN－企業間通信で「排反する（disjoint）」プロトコルを使用する考えがある。すなわち、あるプロトコルを PCN と DMZ の間で許可する場合、DMZ と企業ネットワークの間では明示的に「拒否」する。この設計は、Slammer などのワームが PCN/SCADA ネットワークの中に実際に進む可能性を大幅に減らす。その理由は、ワームは、2 つの異なるプロトコル上の 2 つの異なるセキュリティ上の弱点を突かなければならないからである。

実践上で多くの変形がありうる領域は、PCNから外に向かうトラフィックの制御である。この種のトラフィックに対して非常に無防備な態度を取る組織があるが、調査チームは、このトラフィックが管理されない場合には、重大なリスクがあると信じる。一例は、セクション 4.3 で先に述べたように、アウトバウンド・ルールの定義がうまくない場合に、それに付け込んでHTTPトンネリングを使用するトロイの木馬ソフトウェアである。したがって、アウトバウンド・ルールはインバウンド・ルールと同じように厳しくすることが重要である。ISAのSP-99 技術報告第 2 の付属書Aには、このことを明確にするのに役立つ指針例が含まれている。その要約は以下のとおりである。[19]

1. PCN ファイアウォールを通過するアウトバウンド・トラフィックは、不可欠の通信だけに限定すべきである。

2. PCN から企業ネットワークへの全アウトバウンド・トラフィックは、スタティック・ファイアウォール・ルールを使用してサービスとポートで送信元と送信先を制限する。

3. PCN ファイアウォールを越えるマップド・ドライブは回避すべきである。

これらのルールに加えて、ファイアウォールは、偽のIPパケットがPCN/SCADAネットワークまたはDMZから出て行くのを止めるようにアウトバウンド・フィルタリングを設定すべきである。この意図は、PCNネットワークが、DoS攻撃で頻繁に使用されるなりすまし（すなわち偽の）通信の送信元となることを防ぐことである。したがって、ファイアウォールは、パケットがPCN/SCADAネットワークまたはDMZネットワークに対する正しい送信元のIPアドレスを有する場合だけ、IPパケットを転送するように設定すべきである。[20]

最後に、PCN/SCADA とインターネットの接続および通信の問題については、多種多様な実践がありうる。例えば、API -1164 は次のように述べる。

> *「インターネット接続は、SCADAネットワークで直接終端すべきでない。SCADAネットワークとインターネットを隔離するためにファイアウォールを使用すべきである」*[21]

対照的に、エンドユーザ向けの文書の 1 つは次のように述べる。

「PCN は、ファイアウォールによって保護されている場合でも、インターネットに直接接続しないものとする」

第 1 のルールが適切な特別な状況（遠隔サポートのためのアクセス等）があるだろうけれども、第 2 のルールがはるかに安全であり、目標とすべきであると信じる。どちらにせよ、PCN 上の機器からインターネットへのアクセスは、思いとどまらせるべきである。

要約すると、調査チームは、以下が一般的なファイアウォールのルールセットに関する推奨されたプラクティスと考える。

1. 基本のルールセットは、「すべて拒否（DENY ALL）、何も許可しない（PERMIT NONE）」であるべきである。

2. PCN環境と外部ネットワークの間のポートとサービスは、具体的に 1 件ごと個別に権限と許可が与えられるべきである。リスク分析を含む業務上の正当性を述べた文書と、許可された着信または発信の各データ・フローに対する責任者が存在すべきである。[22]

3. 「許可」の全ルールは、IP アドレスと TCP/UDP ポートの両方で限定されるべきであり、適切な場合はステートフルであるべきである。

4. ルールはすべて、トラフィックを特定の IP アドレスまたはアドレス範囲内に制限するものとする。

5. PCN/PIN 上のトラフィックはすべて通常、TCP/IP または UDP/IP の、ルート選定できる IP プロトコルのトラフィックだけにすべきである。したがって、IP プロトコル以外は廃棄されるべきである。

6. トラフィックが PCN/SCADA ネットワークから企業ネットワークへ直接通過するのを防ぐ。トラフィックはすべて、DMZ の中で終端すべきである。

7. PCN と DMZ の間で許可されるどのプロトコルも、DMZ と企業ネットワークの間で明示的に「拒否」する（およびその逆）。

8. PCN から企業ネットワークへのアウトバウンド・トラフィックはすべて、スタティック・ファイアウォール・ルールを使用して、サービスとポートにより送信元と送信先を限定すべきである。

9. パケットが PCN 機器または DMZ 機器に割り当てられた正しい送信元 IP アドレスを有する場合だけ、PCN または DMZ からのアウトバウンド・パケットとして許可する。

10. PCN 機器は、インターネットにアクセスするのを許されるべきでない。

11. PCN は、ファイアウォールによって保護されている場合でも、直接インターネットに接続しないものとする。

12. ファイアウォール管理トラフィックはすべて、独立した安全な管理ネットワーク（例えば、帯域外）かまたは 2 因子認証の暗号化ネットワークを媒体とすべきである。トラフィックも、IP アドレスにより特定の管理ステーションに限定されるべきである。

これらは指針に過ぎないと考えるべきであると読者に警告しておく。個々の制御環境を注意深く評価することが、ファイアウォールのどのルールセットを実施する前にも必要である。さらに、これらのルールには常に例外がありうる。例えば、PCN 上のデータ・ヒストリアンと企業全体のデータベースを同期させるために、データベース間の直接接続が、推奨事項 4 に違反して必要になるかもしれない。同様に、PCN 上の機器の時間を同期させるため、企業タイムサーバへのタイムサービス通信が、PCN ファイアウォール通過しなければならないかもしれない。これらの例外およびそれにどう取り組むかは、本報告書の後のセクションで詳細に述べる。

5.2 特定のサービスに対するルール

上記の一般ルールの他には、特定のプロトコルに対する万能のルールを述べるのは困難である。必要性およびベスト・プラクティスは、どのプロトコルに対しても産業間で大きく変わるので、会社ごとに分析すべきである。産業自動化のためのオープン・ネットワーク協会（IAONA）は、機能、セキュリティ・リスク、最悪の場合の影響およびその対策に関して産業環境で普通に見られる各プロトコルを評価し分析[23] するための、テンプレートを提供している。以下に、IAONAの文書の要点と、ISA TR2 付属書Aと数冊のユーザポリシー文書が提案するプラクティスを要約する。読者には、ルールセットを作成するとき、これらの文書を直接読むことを勧める。

5.2.1 ドメインネームサービス (DNS)

ドメインネームサービス (DNS)は主に、ドメイン名（control.com 等）と IP アドレス（192.168.1.1 等）の間を翻訳するために使用される。たいていのインターネット・サービスは DSN にひどく依存しているが、生産現場での使用は、最近ではまれである。たいていの場合、DNS リクエストが PCN から企業ネットワークに行くのを許可する理由は殆どなく、DNS リクエストが PCN に入るのを許可する理由は全くない。PCN から DMZ への DNS リクエストは、1 件ごと個別に扱われるべきである。ローカル DNS またはホストファイルの利用が推奨される。

5.2.2 ハイパーテキスト転送プロトコル(HTTP)

ハイパーテキスト転送プロトコル(HTTP)は、インターネット上のウェブ閲覧サービスの基礎をなすプロトコルである。DNS のように、これはたいていのインターネット・サービスで極めて重要である。生産現場では万能問い合わせツールとしてますます使用

されるようになっている。残念なことに、セキュリティ機能は殆どなく、非常に多数のマニュアル攻撃およびワームを転送してしまう。さらに、HTTP アプリケーションは脆弱性を持ち、悪用されることでも有名である。

一般に HTTP が、企業から PCN へ通過するのを許可すべきでない。許可する場合は、HTTP プロキシが、インバウンド・スクリプトおよび Java アプリケーションをすべてブロックするように、ファイアウォールを設定すべきである。着信 HTTP 接続は、重大なセキュリティ・リスクを引き起こすので、PCN に入ることを許可すべきでない。PCN への HTTP サービスが絶対に必要な場合、代わりに HTTPS を使用し、非常に限定した機器だけを使用することを勧める。

5.2.3 ファイル転送プロトコル(FTP)およびトリビアル・ファイル転送プロトコル(TFTP)

ファイル転送プロトコル(FTP)およびトリビアル・ファイル転送プロトコル(TFTP)は、機器間のファイル転送に使用される。これらは、極めてよく知られており、最小限の処理能力だけを使用するので、多くの DCS、PLC、遠隔端末装置(RTU)を含む殆どすべてのプラットフォーム上で実装される。残念なことに、両方のプロトコルとも、セキュリティを念頭において作られなかった。FTP の場合は、ログイン用のパスワードは暗号化されておらず、TFTP の場合は、ログインがまったく必要とされない。その上、FTP 実装の中には、バッファあふれ脆弱性を突かれた履歴を持つものもある。その結果、TFTP はすべてブロックすべきであり、FTP はアウトバウンド・セッションだけ、あるいは追加のトークンベースの 2 因子認証および暗号化トンネルで安全にされた場合にのみ許可すべきである。

5.2.4 テルネット（Telenet）

テルネット・プロトコルは、クライアントとホストの間の対話式のテキストベースの通信セッションを規定する。リソースが限られているシステムまたはセキュリティの必要性が限定されているシステムへの遠隔ログインサービスと簡単な制御サービスに主に使用される。パスワードを含むテルネット・トラフィックのすべては、暗号化されておらず、遠隔の操作者に機器に対するかなり大きな制御を許可するので、深刻なセキュリティ・リスクである。したがって、企業から PCN へのインバウンド・テルネット・セッション・コマンドは、トークンベースの 2 因子認証および暗号化トンネルで安全にされない限り、禁止すべきである。アウトバウンド・テルネット・セッションは、暗号化トンネルを通じて特定の機器とだけに許可すべきである。

5.2.5 SMTP (Simple Mail Transfer Protocol)

SMTP (Simple Mail Transfer Protocol)は、インターネット上の主要な電子メール転送プロトコルである。電子メールメッセージは、ウィルスを含むことで悪評が高いので、どの PCN 機器への着信電子メールも許可すべきでない。PCN から企業への送信 SMTP メールメッセージは容認できる。

5.2.6 シンプル・ネットワーク管理プロトコル(SNMP)

シンプル・ネットワーク管理プロトコルは、中央管理操作卓とルータ、プリンタ、PLC などのネットワーク機器の間に、ネットワーク管理サービスを提供するのに使用される。SNMP はネットワークを保守するために極めて有用なサービスではあるが、そのセキュリティの弱さは悪名高い。SNMP のバージョン 1 と 2 は、機器（PLC などの機器を含む）からの読み出しとその設定の両方で、暗号化されていないパスワードを使用し、多くの場合、パスワードは周知であり変更できない。バージョン 3 は、相当に安全ではあるが、あまり利用されていない。さらに、埋め込まれた機器への SNMP の実装は、多くの場合に深刻な欠陥があることが示されている。したがって、SNMP コマンドは、PCN に出入りする双方向とも、独立した安全な管理ネットワークを通じてでない限り、禁止すべきである。

5.2.7 分散型コンポーネント・オブジェクト・モデル (DCOM)

分散型コンポーネント・オブジェクト・モデル (DCOM)は、よく知られている OPC (OLE for Process Control)と ProfiNet の両方の基礎をなすプロトコルである。Microsoft のリモートプロシージャコール（RPC)サービスを利用するが、そのサービスは、Blaster Worm（ブラスタ・ワーム)が弱点を突いた既知の脆弱性がある。さらに、OPC (DCOM)は、広い範囲のエフェメラルポート(1024 番～65535 番)を動的に開き、ファイアウォールでフィルタにかけるのが極めて難しい。このプロトコルは、PCN ネットワークと DMZ ネットワークの間でだけ許可すべきであり、DMZ と企業ネットワークの間では明示的にブロックすべきである。また、ユーザには、DCOM を使用する機器のレジストリを修正することにより、使用されるポートの範囲を制限することを勧める。

5.2.8 SCADA と産業用プロトコル

MODBUS/TCP、EtherNet/IP、DNP3 などの SCADA と産業用のプロトコルは、たいていの制御機器との通信のために極めて重要である。残念なことに、これらのプロトコルはセキュリティを念頭に置かずに設計されたので、遠隔から制御機器上でコマンドを実行するのに通常は認証を必要としない。したがって、これらのプロトコルは、PCN と PIN の間でだけ許可すべきであり、企業ネットワークに渡るのを許可すべきではない。

5.3 ネットワーク・アドレス変換(NAT)

意見が分かれる「ベスト・プラクティス」の 1 つは、ファイアウォール上でネットワーク・アドレス変換(NAT)を使用するか否かである。例えば、ISA SP-99 技術報告書 No.2 は次のように述べる。

> *「NATはPCN上で使用しない」*[24]

それに対して、エンドユーザのファイアウォール実践の中では、指針は次のように書いている。

「NATは（企業ネットワーク）に接続するインターフェース上で使用される」

セクション 2.3 で言及したように、NAT は、必要な場合に、ファイアウォールの片側で使用された IP アドレスを、反対側で異なるセットにマッピングするサービスである。NAT は、インターネット・アクセスをたまに必要とする多数の機器を有する会社が、それより少ないインターネット・アドレスのセットを使ってやっていけるように、元は IP アドレスを減らす目的で作られた。

そのために、NAT は、任意の瞬間にすべての内部機器が外部のホストとアクティブに通信していることはないとの前提に立っている。ファイアウォールは、限られた数の外から見える IP アドレスを持つように設定される。内部のホストが外部のホストとの通信を求めるとき、ファイアウォールは内部の IP アドレスとポートをその時点で使用されていない、より限定されたグローバル IP アドレスの 1 つに再マッピングして、発信トラフィックをより少ない IP アドレスに事実上集める。ファイアウォールは、各接続の状態と、内部用のプライベート IP アドレスと送信元ポートのそれぞれが、外から見える IP アドレスとポートの対にどのように再マッピングされたかを、追跡監視しなければならない。戻りのトラフィックがファイアウォールに到着したとき、マッピングが逆にされ、パケットは適切な内部ホストに転送される。

例えば、PCN ベースの機器は、外部の非 PCN ホストとの接続を確立する必要があるかもしれない（例えば、重要な警告メールの送信のため）。NAT は、送信を開始する PCN ホストの内部 IP アドレスをファイアウォールに置き換えるのを可能にし、引続く返信トラフィックのパケットは再マッピングされて内部 IP アドレスに戻り、適切な PCN 機器に送信される。さらに具体的には、PCN にプライベート・サブネット 192.168.1.xxx を割り当てられ、インターネットのネットワークは、その機器がその企業に割り当てられた 142.232.yyy.zzz の範囲のアドレスを使用すると期待している場合、NAT ファイアウォールは、PCN 機器で生成された各アウトバウンド IP パケットのアドレスに、送信元アドレス 142.232.yyy.zzz を代入する（そして追跡する）。

NAT を行ったトラフィックは、ファイアウォールが接続の開始者であるかのように（IP アドレスの観点からは）見えることになるので、現在 NAT は、セキュリティ機能としてしばしば奨励される。NAT は、内部のホストと外部のホストの間の仲介者の役割を果たすことで、内部ホストの正体を効果的に隠蔽する。機器が外部ネットワークとアクティブに通信していない場合、その機器に対する NAT のマッピングはファイアウォール内に存在せず、したがって、外部からルート選定できるアドレスが外界に見えることはない。内部機器がプライベート・アドレスでアドレス指定される場合（RFC 1918 によって示されるように）、ルータは、インターネットからのトラフィックが直接その機器に到着することを許可するはずがない。内部機器と通信する唯一の方法は、NAT による接続を通してである。もちろん、ファイアウォールを通してアクティブな接続をしている機器は、外界から見える。

NAT が本当に本物のセキュリティ技術であるか、それとも単に「不明瞭さを通じたセキュリティ」であるかどうかは、ネットワーキング・コミュニティで議論が分かれる。しかし、NAT の使用がある特定の状況ではまずい結果を生むことがあることには、殆ど疑いの余地はない。先ず、ファイアウォールのデバッグまたはファイアウォールのルールセットが安全か検証することは、NAT を使用することでより難しくなる。その理由は、現在オープンな接続も、通過して戻ることを許可されなければならない IP アドレスとポートの組み合わせも時々刻々変わることである。

さらに、特定のプロトコルは、直接アドレス指定ができないため、NATで分割される。例えば、OPCは、NATと連動するには特別のサード・パーティトンネルソフトウェアを必要とする。EtherNet/IPおよびFoundation Fieldbus HSE®などの生産者－消費者プロトコルは、特に面倒である。それは、これらのプロトコルが全サービスを提供する際に必要とするマルチキャストベースのトラフィックをNATがサポートしないからである。

要約すると、NAT は明確に長所があるが、配備する前に、実際の産業用プロトコルと設定への影響を注意深く評価すべきである。

5.4 具体的な PCN ファイアウォールの問題

5.4.1 データ・ヒストリアン

この報告書で先に述べたように、データ・ヒストリアンや資産管理サーバなどの PCN/企業共有サーバの存在は、ファイアウォールの設計と設定に大きな影響をもたらすことがある。3 ゾーン・システムでは、DMZ にこれらのサーバを置くことは、比較的単純であるが、2 ゾーン設計では、問題は複雑になる。ヒストリアンをファイアウォールの企業側に配置すると、MODBUS/TCP や DCOM などの安全でない幾つかのプロトコルがファイアウォールを通過するのを許可されなければならないし、ヒストリアンに報告する各制御機器はネットワークの企業側にさらされることになる。他方、ヒストリアンを PCN 側に設置すると、HTTP や SQL などの同様に疑わしい別のプロトコルがファイアウォールを通過するのを許可されなければならなくなるし、企業のほぼ全員がアクセスできるサーバが PCN に存在することになる。

一般に、最善のソリューションは、2 ゾーン・システムを避け、3 ゾーン設計を使用し、データ収集装置を PCN 内に置き、ヒストリアン構成要素を DMZ または PIN に置くことである。この場合でさえ、ある状況では問題になることがある。企業ネットワーク上の多数のユーザから DMZ 内のヒストリアンへのアクセスが多くなり、ファイアウォールのスループット能力に重い負担をかけかねない。1 つの対策は、2 台のサーバを設置することである。第 1 のサーバは PCN 内に設置し、制御機器からのデータを収集する。第 2 のサーバは企業ネットワークに設置し、第 1 のサーバをミラーし、クライアントの問い合わせを可能にする。もちろん、このことは、サーバとサーバ間の直接通信を可能にする特別の穴をファイアウォールに通す必要があるが、正しく行われれば、これによるリスクは小さい。

5.4.2 遠隔サポートアクセス

PCN/SCADA ファイアウォール設計のもう 1 つの問題は、PCN へのサード・パーティまたは遠隔からのアクセスである。明らかに、遠隔のネットワークから PCN にアクセスするどのユーザも、トークンベース認証などの適切な強度を有するメカニズムを使用して認証すべきである。制御グループは、DMZ 上に 2 因子認証を持つ独自の遠隔アクセスシステムを設置することが可能であるが、多くの会社では、IT 部門が設置した既設システムを使用するほうが通常はより効率的である。このような場合は、IT 遠隔アクセスサーバからファイアウォールを通過する接続が必要である。

インターネットを通してまたはダイヤルアップモデムにより接続する遠隔サポート要員は、一般用企業ネットワークに接続するために、企業 VPN 接続クライアントを起動し、トークンベースの 2 因子認証の仕組みを使用して認証すべきである、と述べている文書が幾つかある。いったんそこに接続された後も、PCN ネットワークへのアクセス許可を得るために、PCN ファイアウォールで 2 度目の認証（2 因子認証を使用して）をすべきである。制御トラフィックが、無条件に企業ネットワークを通過することを許可しない会社では、IP セキュリティ・プロトコル（IPsec) VPN 内にセキュア・ソケット・レイヤ(SSL) VPN を使用するなど、PCN へのアクセスを得るためにカスケードまたは第 2 トンネル・ソリューションを必要とする。

5.4.3 マルチキャスト・トラフィック

マルチキャストは、送信元の機器が一群の送信先の機器に同時に 1 つのデータメッセージを送信できる通信方法である。各送信先に同じメッセージを順次送信するのとは対照的に、メッセージはネットワーク上を 1 度だけ送信され、その送信に「チューンされた」どのホストもそれを受取れる。

EtherNet/IP および Foundation Fieldbus HSE などのイーサネット上で動作するたいていの工業生産者－消費者（または出版社－購読者）プロトコルは、IP マルチキャストを使用している。IP マルチキャストの第 1 の長所は、ネットワーク効率であり、複数の送信先にデータ送信を繰り返さないので、ネットワーク負荷を著しく減少させることができる。第 2 の長所は、送信元ホストは、ブロードキャスト情報をリッスンしているあらゆる送信先ホストの各 IP アドレスを知る必要がないことである。第 3 の長所は産業用の制御目的でたぶん最も重要なものであり、ただ 1 つのマルチキャスト・メッセージは複数のユニキャスト・メッセージより、複数の制御機器間の時間同期を取るのに、はるかに優れていることである。

IP 環境でのマルチキャストは通常、クラス D の IP アドレス範囲（224.0.0.0～239.255.255.255）に直接マッピングされるマルチキャストのグループ ID を使用して行う。各アドレスは、別個の送信周波数と見做される。マルチキャスト・パケットをリッスンするホストは、受信を望む送信のグループ ID（IP アドレス）に「チューン」しなければならない。

マルチキャスト・パケットの送信元と送信先の間に介在するルータまたはファイアウォールがない場合、マルチキャストの伝送は比較的シームレスである。[iii] しかし、送信元と送信先が同じLAN上にない場合、送信先にマルチキャスト・メッセージを転送することは、もっと複雑になる。マルチキャスト・メッセージのルーティングの問題を解決するため、ホストは、インターネット・グループ管理プロトコル(IGMP)を使用して、自ネットワーク上のマルチキャスト・ルータに関連するグループIDを通知することにより、グループにjoin（またはleave）する必要がある。マルチキャスト・ルータはそれ以降、自ネットワーク上のマルチキャスト・グループのメンバーを知り、自ネットワーク内に受信したマルチキャスト・メッセージを転送するか否かを判定することができる。マルチキャスト用のルーティング・プロトコルも必要である。ファイアウォール管理の観点からは、IGMPトラフィックを監視しフィルタすることは、管理が必要なルールセットが一つ増えることであり、ファイアウォールの複雑さが増すことになる。

マルチキャストに関連するもう 1 つのファイアウォールの問題は、NAT の使用である。外部のホストからマルチキャスト・パケットを受信する NAT を行っているファイアウォールは、データを送信すべき内部のグループ ID に変換する逆マッピング機能を持たない。そのファイアウォールが IGMP を理解する場合、知っているあらゆるグループ ID（それらのうち 1 つは正解だろう）にブロードキャストすることができるが、意図しない制御パケットが重要なノードにブロードキャストされた場合、これは深刻な問題を引き起こす。ファイアウォールが取れる最も安全な措置は、パケットを廃棄することである。したがって、マルチキャストは一般に、NAT にとって扱い憎いと考えられる。

[iii] マルチキャストは設定が容易で管理の必要が殆どないので、制御システム・サプライヤの間で人気を得つつある。しかし、状況によっては、ひどい混乱を起こすことがある。少なくとも大きなエンドユーザの 1 社は、大規模なVLANと多くのPLCを有するPCN上の正規のマルチキャスト・トラフィックによる深刻な問題を報告した。

6 PCN/SCADA ファイアウォールの管理

ファイアウォールは、PCN/SCADAセキュリティの中心であり、当初の設計と使用開始だけでなく、継続する監視、事故管理、アップグレード、技術サポートに相当なリソースを必要とする。この仕事の複雑さを、過小評価すべきではないが、残念なことにしばしば過小評価している。例えば、Avishai Woolのファイアウォール設定エラーについての最近の文書は、大企業の中核のファイアウォールさえも、下手に書かれたルールセットを使用しており、攻撃に脆弱なことがあることを示している。[25] その調査で、著者は 12 の深刻なファイアウォール設定エラー（それぞれ大変一般的内容のものである）を明らかにし、次に大企業 27 社のファイアウォール設定を調査した。その著者は、1 台のファイアウォールにつき平均 7 つの深刻なエラーを見つけ、中には 12 ものエラーを見つけた。この調査結果は、ファイアウォール管理が複雑なことをはっきりと示している。

以下は、ファイアウォールを設定するとき考慮すべき管理タスクである。

1. **変更管理と文書化:** SCADA/PCN の設定とルールセットは、大部分の設備の生産と安全に大きな影響を及ぼすことがある。したがって、ファイアウォール・ポリシーはすべて、注意深く文書化され、PLC や DCS が従うのと同じ変更管理要件に従わなければならない。

   アクセス制御リストをすべて文書化すること、およびこの文書に各ルールの目的、相互依存性、セキュリティ考慮事項を含むことが推奨される。この機器のルールは、接続に関する業務がまだ有効であり、セキュリティ管理が適用されていることを確実にするため、定期的に見直す必要がある。

2. **ファイアウォール・ログおよび IDS の監視:** ファイアウォールに対し責任があるチームは、ログと IDS イベントの両方の監視とそれに伴う警報発令を実施しなければならない。

3. **事故レスポンスの策定:** 事故レスポンス計画は、疑わしいかまたは実際の事故に対する緊急レスポンス・プロセスを定め、管理チームが事故に対処する措置を定める。これには、PCN を企業ネットワークから切り離し、その後再接続するプロセスを含む。完全な切離しが実際的でないところでは、必要なときに実施できる最大限の制限を定めるべきである。

   再接続のプロセスは、いわゆる「ピンホール」設定の詳細も含みうる。この「ピンホール」は、極めて小さな信頼できるリソースセットへの臨時アクセスを可能にし、そのセットから、情報と、例えばアンチウィルス対策を取得することができるようにし、完全な接続を回復する前にプロセス制御環境の防護が最新の状態になるようにする。

4. **サポート、パッチ、アップデート:** 管理チームは、適切な脆弱性リスト、ベンダーアップデートリスト、コンピュータ緊急事態レスポンスチーム(CERT)セキュリティ警報を監視すべきである。適切な資格と権限のある要員が、アップデート、アップグレード、アンチウィルス・アップグレード、ユーザ/アカウント管理、能力監視を定期的に行うべきである。

上記の管理サービスは、プロセス制御部門または IT 部門などの現地スタッフが提供することもできるし、企業またはサード・パーティの中央リソースから提供することもできる。面談した 15 社のうち、大企業の多くは PCN ファイアウォールを中央で管理していたが、小企業は内部リソースを使用し現地で管理していた。経験に基づく法則として、10 を超える PCN/SCADA ファイアウォールを有するグループでは中央での管理が好ましい。

中央管理を選ぶか現地管理を選ぶかにかかわらず、ほぼすべてのエンドユーザが指摘したことは、ファイアウォール・システムを設計、実装、保守するチームの一員として制御技術者を含む必要があることである。一般にファイアウォールをよく理解し設定する人は、プロセス制御の詳細を知らない。例えば、たいていのセキュリティ専門家は、インターネットに専念していて、大部分の制御システムが PCN 内で DNS を使用していないことを知らない。その結果、多くの場合、DNS リクエストがファイアウォールを侵害する試みかまたは PCN 上の不当な行為の兆候であるときでさえ、DNS リクエストを正当なものと見るかもしれない。職能上の枠を超えた制御/IT セキュリティチームの作成は、PCN/SCADA ファイアウォール管理に大いに推奨される。

7 特殊または未来の技術

7.1 SCADA プロトコルを理解するファイアウォール

現時点では、市販のファイアウォールは、伝統的なインターネットおよび企業アプリケーションレイヤ・プロトコルを対象としており、MODBUS/TCP や EtherNet/IP などの産業用プロトコルの存在に気づいていない。その結果、アプリケーションレイヤで SCADA パケットを検査またはフィルタできないし、これらのプロトコルに対しプロキシ・サービスを提供できない。理想的ファイアウォールは、プロトコルをよく理解しており、特定の SCADA 機能をブロックするルールを可能にするものである。例えば、MODBUS 読み込みコマンドだけがファイアウォールを通過するのを許可し、無効または未許可の機能コードを持つ全パケットを廃棄するルールである。

市販製品は現時点ではないけれども、Linux カーネルに対するオープンソースの MODBUS アウエア・ファイアウォールの拡張が、Cisco Systems のクリティカル・インフラストラクチャ・アシュアランス・グループ(CIAG)の Matthew Franz と Venkat Pothamsetty により開発された。これは、http://modbusfw.sourceforge.net/から無料で入手できる。

7.2 分散マイクロ・ファイアウォール

数人の研究者が、厳重な保護を必要とする各 PLC や RTU の前に設置できる分散マイクロ・ファイアウォール器具の考えを提案した。各ユニットは、その目的に固有のセキュリティ・アプリケーションで構成され、中央管理システムに結ばれる。このファイアウォール・アプリケーションは、セキュアチャネルを通じて通信して、悪意ある攻撃からその器具とその背後の PLC の両方をさらに保護する。この方法の利点は、PCN ファイアウォールの内側に相当強力な第 2 層の防護を提供し、内部からの攻撃から重要な機器を保護できることである。

この種の製品は、SCADA 市場では現在入手できないが、プロトタイプを開発する研究プロジェクトがブリティッシュ・コロンビア技術大学で現在行われている。さらに、Siemens が、分散マイクロ・ファイアウォールとしても機能する VPN ゲートウェイを 2004 年の終わりに販売開始する計画を発表している。

7.3 サービス品質 (QoS)

この調査中に見つかった提案の 1 つに、DoS 攻撃の効果が PCN で限定的にものにする方法として、ネットワーク機器のサービス品質(QoS)機能を使用することがあった。QoS は、パケットが出会う各ルータやスイッチでどのように扱われるべきかを示す特別の優先順位フィールドをパケットに付加する考えである。この理由から、QoS の IEEE 802.1q の変形が、産業環境で注目を得ているが、まだ広く使用されてはいない。しかし、

QoS が産業界で広く使用されるようになれば、これは有用なセキュリティの武器となるだろう。

この QoS 使用の軽減技術が効果を発揮するには、検知メカニズム（IDS/AV 等）を必要とすることに注意すべきである。QoS メカニズムが NBAR (Network-Based Application Recognition)を使用する機器上に実装された場合、この軽減の実効性は著しく向上する。機器がトラフィックを調べられない場合には、ネットワーク機器に来るパケットのマーキングが信頼できる場合だけ、QoS は効果がある。残念なことに、最近の 2、3 のワームは、QoS タグの優先順位を高くしており、よい伝搬特性を得ている。

7.4 1 方向通信パス

PCNから出るトラフィックだけを許可する 1 方向通信パスの概念が、IEEE標準 7-4.3.2[26]、「原子力発電所の安全システム内のデジタル・コンピュータに関するIEEE標準」の付属書Gで議論されている。この検討はシリアルリンクを念頭に置いて設計されているようであるが、より広く知られているTCPの代わりに、UDPを使用してIP接続上にこの 1 方向パスを作成することは可能である。現時点では、現場にこの技術を配備している会社を知らないが、ACLが提供できる以上に厳しいセキュリティを必要とする現場では有望であろう。

略語

略語	英語	日本語
ACL	Access Control List	アクセス制御リスト
AIChE	American Institute of Chemical Engineers	アメリカ化学工学会
API	American Petroleum Institute	米国石油協会
BCIT	British Columbia Institute of Technology	ブリティッシュ・コロンビア技術大学
CERT	Computer Emergency Response Team	コンピュータ緊急事態対策チーム
CIAG	Critical Infrastructure Assurance Group (Cisco Systems Inc.)	クリティカル・インフラストラクチャ・アシュアランス・グループ（シスコシステムズ社）
CIP	Common Industrial Protocol	コモン・インダストリアル・プロトコル
DCOM	Distributed Component Object Model	分散型コンポーネント・オブジェクト・モデル
DCS	Distributed Control System	分散制御システム
AV	Anti-Virus	アンチウィルス
DH	Data Historian	データ・ヒストリアン
DMZ	DeMilitarised Zone	非武装地帯
DNS	Domain Name Service	ドメインネームサービス
DoS	Denial of Service	サービス不能
DPI	Deep Packet Inspection	ディープ・パケット・インスペクション
EN	Enterprise Network	企業ネットワーク
ESD	Emergency Shutdown System	緊急停止装置
FERC	Federal Energy Regulatory	連邦エネルギー規制委員会

	Commission	
FTP	File Transfer Protocol	ファイル転送プロトコル
GAIT	Group for Advanced Information Technology	高度情報技術グループ
HMI	Human Machine Interface	ヒューマン・マシン・インターフェース
HTTP	Hyper-Text Transfer Protocol	ハイパーテキスト転送プロトコル
IAONA	Industrial Automation Open Networking Association	産業自動化のためのオープン・ネットワーク協会（IAONA）
IDS	Intrusion Detection Systems	侵入検知システム
IEC	International Electrotechnical Commission	国際電気標準会議
IEEE	Institute of Electrical and Electronics Engineers	電気電子技術者協会
IGMP	Internet Group Management Protocol	インターネット・グループ管理プロトコル
IP	Internet Protocol	インターネット・プロトコル
IPsec	Internet Protocol Security	IP セキュリティ・プロトコル
ISA	Instrumentation, Systems and Automation Society	計測機器・システム・オートメーション協会
ISO	International Organization for Standardization	国際標準化機構
IT	Information Technology	情報技術
LAN	Local Area Network	ローカルエリアネットワーク
MES	Manufacturing Execution System	生産実行システム
NAT	Network Address Translation	ネットワーク・アドレス変換
NBAR	Network-Based Application Recognition	NBAR

NIC	Network Interface Card	ネットワーク・インターフェース・カード
NISCC	National Infrastructure Security Coordination Centre	国立インフラストラクチャ・セキュリティ調整センタ
OPC	OLE for Process Control	OPC
OS	Operating System	オペレーティング・システム
PC	Personal Computer	パーソナルコンピュータ
PCN	Process Control Network	プロセス制御ネットワーク
PIN	Process Information Network	プロセス情報ネットワーク
PLC	Programmable Logic Controllers	プログラマブル論理制御装置
Qos	Quality of Service	サービス品質
RFC	Request for Comment	RFC
RPC	Remote Procedure Call	リモートプロシージャコール
RTU	Remote Terminal 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
SOAP	Simple Object Access Protocol	シンプル・オブジェクト・アクセス・プロトコル
SQL	Structured Query Language	構造化照会言語
SMTP	Simple Mail Transfer Protocol	SMTP
SNMP	Simple Network Management Protocol	シンプル・ネットワーク管理プロトコル
SSL	Secure Socket Layer	セキュア・ソケット・レイヤ
TCP	Transmission Control Protocol	伝送制御プロトコル
TFTP	Trivial File Transfer Protocol	トリビアル・ファイル転送プロトコル

UDP	User Datagram Protocol	ユーザ・データグラム・プロトコル
VLAN	Virtual Local Area Network	仮想ローカルエリアネットワーク
VPN	Virtual Private Network	仮想プライベートネットワーク
WLAN	Wireless Local Area Network	無線 LAN
XML	Extended Markup Language	拡張マークアップ言語

8 参考文献

[1] Smith, T.; “Hacker jailed for revenge sewage attacks,” *The Register*, October 31, 2001, http://www.theregister.co.uk/content/4/22579.html

[2] "SQL Slammer Worm Lessons Learned For Consideration By The Electricity Sector", *North American Electric Reliability Council*, Princeton NJ, June 20, 2003

[3] "NRC Information Notice 2003-14: Potential Vulnerability of Plant Computer Network to Worm Infection", United States Nuclear Regulatory Commission, Washington, DC, August 29, 2003

[4] E. Byres, J. Carter, A. Elramly and D. Hoffman; “Worlds in Collision: Ethernet on the Plant Floor”, ISA Emerging Technologies Conference, *Instrumentation Systems and Automation Society*, Chicago, October 2002

[5] E.J. Byres and D. Hoffman; “IT Security and the Plant Floor”, InTech Magazine, *Instrumentation Systems and Automation Society*, Research Triangle Park, NC, p. 76, December 2002

[6] The Ten Commandments of Industrial Ethernet, B&B Electronics Manufacturing Company, March 30, 2004

[7] Technical Report ISA-TR99.00.01-2004: Security Technologies for Manufacturing and Control Systems, *Instrumentation, Systems and Automation Society (ISA),* March 2004

[8] ibid - Technical Report ISA-TR99.00.01-2004

[9] B. Fraser, “RCF 2196 - Site Security Handbook”, *Internet Engineering Task Force*, September 1997, Pg. 22

[10] ibid - Technical Report ISA-TR99.00.01-2004

[11] “API Standard 1164 – SCADA Security (Draft) – Appendix B”, *American Petroleum Institute*, March 2004

[12] http://udell.roninhouse.com/bytecols/1999-10-13.html

[13] E.J. Byres; “Designing Secure Networks for Process Control”, IEEE Industry Applications Magazine, *Institute of Electrical and Electronics Engineers*, New York, Vol. 6, No. 5 p. 33 -39, September/October 2000

[14] “Process Control Network Reference Architecture v 1.0”, *Invensys Inc*., January 2004, pg. 2, 5

[15] "Experion PKS Network and Security Planning Guide EP-DSX173, Release 210", Honeywell Limited Australia, October 2004

[16] “Presentation: Securing SIMATIC PCS7 and SIMATIC IT in Networks”, *Siemens, 2003*

[17] IEC/SC 65C/WG 13 Draft v1.04 "Enterprise Network-Control Network Interconnection Profile (ECI)", *International Electrotechnical Commission*, December 2004

[18] B. Fraser, “RCF 2196 - Site Security Handbook”, *Internet Engineering Task Force*, September 1997, Pg. 21

[19] “Technical Report ISA-TR99.00.02-2004: Integrating Electronic Security into the Manufacturing and Control Systems Environment”, *Instrumentation, Systems and Automation Society (ISA),* April 2004, Page 79

[20] Process Control Digital Security Practice: Firewall Practice Release 1.0, (Name withheld on request), 2003.

[21] “API Standard 1164 – SCADA Security (Draft)”, *American Petroleum Institute*, March 2004, Page 20

[22] ibid-IEC/SC 65C/WG 13 Draft v1.04, Page 11

[23]“The IAONA Handbook for Network Security - Draft/RFC v0.4”, *Industrial Automation Open Networking Association (IAONA),* Magdeburg, Germany, 2003

[24] ibid, “Technical Report ISA-TR99.00.02-2004” Page 77

[25] Avishai Wool, "A quantitative study of firewall configuration errors "IEEE Computer Magazine, *IEEE Computer Society*, June 2004, Page 62-67

[26] IEEE Standard 7-4.3.2, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations.", *Institute of Electrical and Electronic Engineers*

[22] John C. Netzel, *Network Security Across Wide Area Networks & the Internet,* IndComm 2003, Melbourne Australia, May 2003.

[23] Technical Architecture Whitepaper Network Zone Model v1.2E, The Dow Chemical Company, 2004.

[24] Process Network Security: Firewall Configuration and Policies, Invensys Inc., 2004.

[25] Montgomery Watson Harza, “Security for SCADA IP Networks”, 2003.