生産制御システムにおけるホワイトリストベース パケットフィルタリングの評価

小林 大朗† 鉄 穎† 渡邉 直紀†
武部 達明‡ 鈴木 和也‡ 吉岡 克成† 松本 勉†
†横浜国立大学
240-8501 神奈川県横浜市保土ケ谷区常盤台 79 番
{kobayashi-masaaki-ny, tie-ying-fc, watanabe-naoki-bj}@ynu.jp,
{yoshioka, tsutomu}@ynu.ac.jp
‡横河電機株式会社
180-0006 東京都武蔵野市中町 2-9-32
{Tatsuaki.Takebe, Kazuya.S}@jp.yokogawa.com

あらまし 近年，プラント等の生産制御システムのオープン化が進み，それに伴い生産制御システムに対するサイバー攻撃が大きな脅威となっている．Ethernet化，IP化した生産制御システムのセキュリティ向上の一方策として，L2スイッチの各物理ポートにおいて通信を許可するIPアドレスやMACアドレスをホワイトリストとして指定し，これ以外の通信を全て遮断するといった厳密な低レイヤパケットフィルタリングを行う方法が検討されている．実際，制御システム内の通信をパッシブに観測し，ホワイトリストを自動生成する製品が複数存在する．これらのホワイトリストを最大限に活用するためにはIPアドレスベースのフィルタリングが可能なL2 Plus スイッチの導入が理想的であるが，稼働中のシステムにおける機器の入れ替えが運用上困難である場合や，コスト高を理由に通常のL2スイッチがサポートするMACアドレスベースのフィルタしか適用できない場合が想定される．本稿では，MACアドレスベースのフィルタとIPアドレスベースのフィルタの効果について定性的評価を行う．具体的には，生産制御システムで用いられるいくつかの典型的なアプリケーションレイヤプロトコルに対して，なりすましやDoS攻撃をモデル化し，フィルタリングによる効果を見積もる．また，模擬プラント環境において疑似攻撃を行い，フィルタリングにより攻撃が無効化される例を示す．

Evaluation of Whitelist-based Packet Filtering for Industrial Control System

Masaaki Kobayashi† Ying Tie† Naoki Watanabe†
Tatsuaki Takebe‡ Kazuya Suzuki‡ Katsunari Yoshioka† Tsutomu Matsumoto†
†Yokohama National University
79, Tokiwadai, Hodogaya-ku, Yokohama-shi, Kanagawa 240-8501, JAPAN
{kobayashi-masaaki-ny, tie-ying-fc, watanabe-naoki-bj}@ynu.jp,
{yoshioka, tsutomu}@ynu.ac.jp
‡Yokogawa Electric Corporation
2-9-32, Nakamachi, Musashino-shi, Tokyo 180-0006, JAPAN
{Tatsuaki.Takebe, Kazuya.S}@jp.yokogawa.com

Abstract In recent years, technologies used in industrial control systems as well as their network environment are becoming more open to public. In order to fight against increasing cyber-attacks to industrial control systems, whitelist-based low-layer network filtering technique has been studied and deployed. Such whitelists work most effectively with L2-plus switches which can filter packets based on IP address. However, there may be a case that L2-plus switches cannot be deployed immediately because of operational and/or financial reasons. In this paper, we evaluate qualitatively the effectiveness of MAC address based filtering and IP address based filtering. Specifically, we model cyber-attacks, such as spoofing attacks and DoS attacks, on some of typical application layer protocols, Modbus/TCP, FL-net, and Vnet/IP for industrial control systems and evaluate the effectiveness of filtering. Finally, we confirm the effectiveness of filtering method on a test bed of a chemical plant we developed.

1 はじめに

近年，工場などの生産制御システムに対するサイバー攻撃が増加している．従来，生産制御システムでは専用の機器やソフトウェアを使用しており，外部システムとの接続や連携も行われていなかったため，サイバー攻撃を受けづらいとされてきた．しかし，近年では汎用製品やTCP/IPやEthernet等の標準プロトコルが導入され，外部システムとの接続や連携が進んでいる．このため，汎用製品の脆弱性を狙った攻撃や，標準プロトコルのネットワークを介したマルウェア感染など，サイバー攻撃のリスクが高まっており，生産制御システムにおけるインシデントが世界的に年々増加傾向にある[1][2].

生産制御システムに対するサイバー攻撃はなりすまし，DoS，改竄等が考えられるが，どれも大きな

脅威となり得る．例えば，2005 年 8 月にダイムラー・クライスラーの米国にある自動車工場がワームによる DoS 攻撃を受け一時操業停止となり，余波を含めおよそ 1400 万ドルの被害を受けた事故が発生している[3]．また，2010 年にはイランのウラン濃縮施設に感染した Stuxnet [4]により，設定データの改竄が行われ約 8400 台の遠心分離器すべてが稼働不能に陥った．こうした脅威がある一方で，生産制御システムのセキュリティレベルは低く，一般の情報システムに比べて 5～10 年は遅れているとの指摘もある[3]．その背景には，可用性重視によるセキュリティ機能の絞り込みがあると考えられている．

以上のような背景を踏まえ，生産制御システムのセキュリティを高めることを目的として，Sophia [5]，Passive Vulnerability Scanner [6]，CyberLens [7]といった製品が登場している．これらの製品は受動的にネットワークを監視することでホワイトリストを生成し，それに基づいて侵入検知と不正通信の遮断を行う．ホワイトリストは，ネットワークトポロジの変更が少なく通信内容の規則性も高いという生産制御ネットワークの特徴にマッチし，また更新の頻度を抑えることができるため，可用性を最重視する生産制御システムにおけるセキュリティの考え方とも親和性が高い．

本稿ではこういった手法のシンプルなモデルとして，Ethernet 化，IP 化された生産制御ネットワークを対象としスイッチ上でホワイトリストに基づく厳密なパケットフィルタリングを行う手法を提案する．さらに，アプリケーションレイヤを想定した実質的な攻撃のモデル化を用い，フィルタリングを行うレイヤとその効果の関係について定性的な評価を行う．

2　生産制御システム

本章では，生産制御システムの特徴と，現状のセキュリティ上の課題について述べる．

2.1　ネットワーク構造

生産制御システムは，生産の管理を担う制御系情報ネットワークと，生産装置の制御を行う制御ネットワークに分けられる．制御系情報ネットワークはオフィスネットワークとファイアウォール等により論理的には分断されているが，物理的には接続されている．制御ネットワークは，制御系情報ネットワークと各種のサーバを介して接続されている．一般的な生産制御システムのシステム構成例を図 1 に示す．

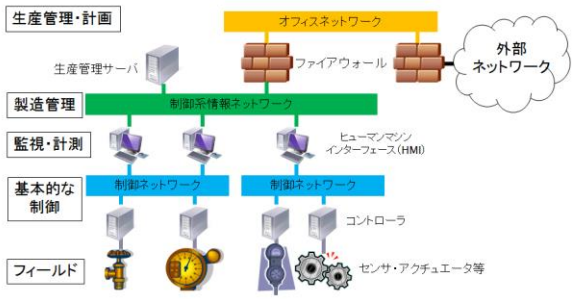

図 1　一般的な生産制御システムのシステム構成例

制御ネットワークでは従来，専用の機器や独自のプロトコルを利用していたが，近年では低コストで対応機器を調達可能であること，システム構築が容易であること，コントローラで扱うデータをそのまま上位システムに吸い上げが可能といった利点から，Ethernet 化，IP 化が進んでいる．

2.2　生産制御システムで使用されるアプリケーションレイヤプロトコルの例

2.2.1　Modbus/TCP [8]

Modicon 社が 1979 年，同社のプログラマブルロジックコントローラ(PLC)向けに策定したシリアル通信プロトコルである Modbus を，TCP/IP 上に実装したのが Modbus/TCP である．マスタ/スレーブ型のプロトコルであり，仕様が公開されていること，利用が無料であること，実装が比較的容易であることなどから，産業用電子機器を接続する手段として広く普及している．基本的な動作としては，コマンド発行権を持つ唯一のノードであるマスタからスレーブに対し TCP セッションを確立し，その後マスタはリクエストを送信する．スレーブはリクエストの指示に従いデータの読み書きや送信を行い，終了後確認のアンサーバックをマスタへと送信する．

2.2.2　FL-net [9]

ファクトリーオートメーション(FA)分野における，PLC や数値制御装置，ロボット，パソコンなどの相互接続を目的とした，オープンなネットワーク規格である．UDP/IP 上に構築されたプロトコルで，後述するように UDP パケットのブロードキャストを用いて通信を行う．トークンバス方式と呼ばれる通信方式を採用しており，以下のようにしてデータをやり取りする．まず，トークンと呼ばれる，獲得したノードだけが唯一データを送信できる権利を，FL-net 上に 1 つ作る．トークンは通信確立中常に巡回するルールになっており，ノードが自身宛てのトークンを獲得した場合，必要なデータフレーム送信を行うとともに，後続のノードに宛てたトークンを送信することでトークンを引き継ぐ．実際にトークンが乗るトークンフレームは UDP ブロードキャストとして配信され，全てのノードはそれを監視し，それに基づいて自身以外に何番のノードがいるのか，自ノード直前・直後のノード番号，現在トークンを保持しているノード等の情報を得る．2012 年に登場した Ver.3 では，汎用コマンドサーバ機能によって，設定ツールから TCP/IP または UDP/IP ベースの通信により各種パラメータの設定や読み出しを行うことも可能となっている．自動車産業を中心に，日本国内で普及している．

2.2.3　Vnet/IP [10]

横河電機が開発した，プロセスオートメーション(PA)用のリアルタイムプラントネットワークシステムであり，UDP/IP 上に構築されたプロトコルである．一部を除き各パケットには共通鍵を用いた認証子が付加されており，それによってなりすましや改竄に対する防御を行っている．データのやり取りにおいて特殊な方式は用いておらず，コントローラによる測定値の報告や HMI からコントローラへの死活監視とその応答，設定値の変更といったほとんどの通信は UDP ユニキャストで行われる．時刻同期等，一部の通信は UDP マルチキャストが用いられる．

2.3　セキュリティ上の課題

2.3.1　可用性の最重視

生産制御システムは一般の情報システムと違い，可用性を最重視する．情報システムにおいては，機密性(Confidentiality)，完全性(Integrity)，可用性(Availability)という，いわゆる C.I.A の順に重きが置かれるが，生産制御システムでは逆に A.I.C の順

に重要とされる．そのため，システム上の負荷となるセキュリティ機能を忌避する傾向にあり，例えば，システム上の負荷となるウイルス監視やプログラムの自動更新などは行われない場合が多い．

2.3.2　システムの長期利用

生産制御システムは通常，10 年以上におよぶ長期間にわたり使用されるため，それに伴いセキュリティが陳腐化してしまう傾向にある．機能の更新は可能であるものの，2.2.1 節で述べたように可用性を最重視するため頻繁な更新を行うことはできず，常に最新のセキュリティを維持することが難しい．

2.3.3　オープン化に伴うリスクの増加

従来，生産制御システムでは専用の機器やソフトウェアを使用しており，外部システムとの接続や連携も行われていなかったため，サイバー攻撃を受けづらいとされてきた．しかし，近年では利便性の向上や開発コストの削減といった目的から，汎用製品や TCP/IP，Ethernet 等の標準プロトコルが導入され，外部システムとの接続や連携が進んでいる．このため，汎用製品の脆弱性を狙った攻撃や，持ち込まれた PC・USB メモリなどの記憶デバイスや標準プロトコルのネットワークを介したマルウェア感染など，サイバー攻撃のリスクが高まっている．

3　ホワイトリストに基づく低レイヤフィルタリング

Ethernet 化，IP 化された制御ネットワークをサイバー攻撃から守る手法として，認められたノード間通信の IP アドレスや MAC アドレスを指定したホワイトリストに基づき，L2 スイッチにおいて厳密なパケットフィルタリングを行うことにより不正な通信を遮断する方法が検討されている．ネットワークトポロジの変更が少なく，通信内容の規則性が高い生産制御ネットワークは，ホワイトリストに基づく厳密で静的なパケットフィルタリングとの親和性が高く，限定的な導入コストでセキュリティ強化が期待できるためである．実際にフィルタリングのためのホワイトリストを自動生成する製品として，Sophia，Passive Vulnerability Scanner，CyberLens 等が存在する．本節では，本稿における評価対象モデルであるホワイトリストに基づく低レイヤフィルタリング手法を提案する．

3.1　対象となる制御ネットワーク

この方式の対象となる制御ネットワークは，HMI やコントローラといったノード群と，それらを接続するスイッチから構成されているものとし，第二層,第三層はそれぞれ Ethernet, IP により実現されているとする．

3.2　目的

この方式は，制御ネットワークにおけるなりすまし通信の検知・遮断を目的とする．すなわち，制御ネットワーク内のあるノードの制御を奪取した攻撃者を想定し，攻撃者が当該ノード以外になりすまして行う通信を検知・遮断することを目的とする．

3.3　パケットフィルタリングルール設定の流れ

(1) ホワイトリストの作成

まず，保護対象の制御ネットワークにおいて通信を認めるノード対のリストを作成する．例えば，ノードAからノードBへのユニキャスト通信を認める場合は(A -> B)のユニキャストエントリを追加する．また，ノードAからのマルチキャスト通信を認める場合は，マルチキャストエントリ(A -> multi)を追加する．

(2) 初期設定

制御ネットワークを構成する全てのスイッチの全てのポートについて，全ての通信を遮断する．

(3) ホワイトリストの適用

ホワイトリストの各エントリについて，それぞれ以下の通りフィルタルールを作成する．

(3-1) ユニキャストエントリからのフィルタルール作成

ユニキャストエントリ(A -> B)に関するフィルタルール作成は，ノードAからノードBへの物理的経路上の全てのスイッチポートに対して行う．まず，ノードAが接続されているスイッチポートにおいて，ノードAのアドレスを送信元，ノードBのアドレスを宛先とするinbound通信を許可する．次に，ノードAからBへの経路上で複数のスイッチを経由する場合，これらを接続するスイッチポートのinbound通信またはoutbound通信に関して同様にノードAからノードBへの通信を許可する．最後にノードBが接続されているスイッチポートに対してフィルタルールを適用する．（図2参照）

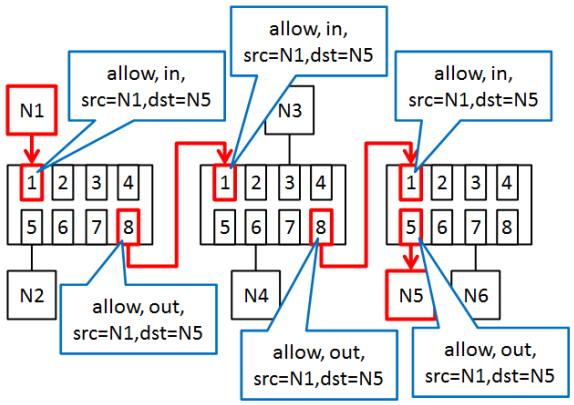

図2　ノードN1からノードN5への通信を許可するフィルタルール作成の例

(3-2) マルチキャストエントリからのフィルタルール作成

マルチキャストエントリ(A -> multi)に対するフィルタルール作成は，ノードAからノードA以外の全てのノードに対するそれぞれの経路について，ユニキャストエントリと同様にフィルタルールを作成することで行う．このとき，送信元アドレスはノードAのアドレス，宛先はシステムで定められたマルチキャストアドレスとする．

(4) フィルタルールの統合

上記ステップ(3)により各ポートに対してフィルタルールが複数生成された場合には，フィルタリングの処理を軽減するため，これらのルールを統合する．例えば，送信元や宛先アドレスについてanyやネットマスクを適用する方法が考えられる．

3.4　フィルタリングの効果

以上のようなフィルタリングを適用することで，各ノードが侵入を受けた場合でも，当該ノード以外のアドレスに送信元を詐称した通信を行うことはできなくなる．また，当該ノードが通信を行うことが認められているノード以外への通信も行えない．このような通信制限により，具体的にどのような内容と目的のなりすまし通信に対して効果が得られるかについては，上位層で動作するプロトコルに依存する．本稿では

この点について，これ以降で評価を行う．

4　定性的評価

3 章で示したように，認められたノード間通信のホワイトリストに基づきフィルタリングを行い生産制御システムのセキュリティを高めようとする試みは行われているが，フィルタリングを行うレイヤやフィルタリングに用いる情報の種類について，どのようなものが効果的かという検討は充分に行われていない．そこで本稿では，3 章で提案したフィルタリング手法モデルについて，アプリケーションレイヤにおける具体的攻撃をモデル化し，これらに対してどの程度の効果を発揮するのかを定性的に評価する．

4.1　防御手法モデル

評価対象モデルを実装する際，通常の L2 スイッチでは MAC アドレスベースのフィルタしか行うことができないため，IP アドレスベースのフィルタリングを行うためには L2 Plus スイッチの導入が必要である．しかし，稼働中のシステムにおける機器の入れ替えが運用上困難である場合や，コスト高を理由に通常の L2 スイッチしか利用できない場合が想定される．そのため，MAC アドレスベースのフィルタと，IP アドレスベースのフィルタとして，以下の 2 つにモデル化する．

1.　MAC フィルタ

スイッチの各物理ポートに入るパケットの送信元および宛先の MAC アドレスを条件としてフィルタリングを行うモデル．多くの L2 スイッチでサポートされている機能で実現可能である．

2.　MAC･IP フィルタ

スイッチの各物理ポートに入るパケットの送信元および宛先の MAC アドレスと IP アドレスを条件としてフィルタリングを行うモデル．L2 Plus スイッチの機能で実現可能である．

4.2　定性的評価

以上のようなモデルに対して，2 つの評価を行う．評価 1 では，防御手法モデルが不正通信の検知に用いることができる情報を基準として攻撃を分類し，それに対する防御手法モデルの効果の評価を行う．評価 2 では，アプリケーションレイヤにおける具体的な攻撃モデルを想定し，それが評価 1 で分類したどのパターンに当てはまるかを考え，それぞれの攻撃モデルに対する防御手法モデルの効果の評価を行う．

● 評価 1

まず，スイッチ上でのフィルタリングの対象となる攻撃を，ノード乗っ取り攻撃と新規ノード接続攻撃の 2 つに分類する．ノード乗っ取り攻撃は，攻撃者が正規のノードをマルウェア感染等により乗っ取る攻撃である．攻撃者は乗っ取ったノードから不正な通信を発する．新規ノード接続攻撃は，攻撃者がスイッチの未使用ポートに新たなノードを接続し，そのノードから不正な通信を発する攻撃である．

この 2 種類のうち，新規ノード接続攻撃に対しては，あらかじめ未使用ポートを使用不能に設定しておくことで対処するものとする．生産制御システムにおいて正規ノードが新規に接続されることは，大規模なメンテナンス等を除けば考えにくいため，このような運用は可能といえる．ノード乗っ取り攻撃について，以下の 2 条件の組み合わせから 16 通りに分類する．

(条件 1)送信元情報

攻撃者は他ノードになりすますなどの目的で，送信元の IP アドレスまたは MAC アドレスを詐称する可能性がある．この詐称に関して，IP アドレスと MAC アドレスそれぞれについて，詐称するかしないかの 4 通りが考えられる．

(条件 2)宛先情報

攻撃者が不正なパケットを送信した宛先が，本来そのノードが通信する相手であるかどうかを判定する．便宜的に，本来通信する宛先であった場合を『正常』，そうでなかった場合を『異常』と表現する．これも IP アドレスと MAC アドレスそれぞれについて正常か異常かで分類し，4 通りを想定する．MAC フィルタ，MAC･IP フィルタそれぞれの場合において，16 通りの攻撃を検知･遮断できるかどうかをまとめたものが表 1，表 2 となる．

表 1　MAC フィルタ
(○:遮断可能　×:遮断不可能)

送信元 / 宛先	IP のみ	MAC のみ	両方	詐称せず
IP 異常 MAC 正常	×	○	○	×
IP 正常 MAC 異常	○	○	○	○
IP 異常 MAC 異常	○	○	○	○
IP 正常 MAC 正常	×	○	○	×

表 2　MAC･IP フィルタ
(○:遮断可能　×:遮断不可能)

送信元 / 宛先	IP のみ	MAC のみ	両方	詐称せず
IP 異常 MAC 正常	○	○	○	○
IP 正常 MAC 異常	○	○	○	○
IP 異常 MAC 異常	○	○	○	○
IP 正常 MAC 正常	○	○	○	×

● 評価 2

評価 2 では，具体的なアプリケーションプロトコルに対して攻撃を想定し，低レイヤのフィルタリングにより攻撃を遮断できるかを定性的に検証する．

◆ Modbus/TCP

Modbus/TCP はマスタースレイブ間の通信を行うプロトコルである．スレーブはサーバとして通信を待ち受けており，マスタはスレーブに対して TCP 3-way ハンドシェイクを行い，リクエストを送信する．スレーブは送られたリクエストに対して応答を返信する．以下では，攻撃者がマスタになりすまして要求を送る攻撃と，スレーブになりすまして偽の応答を返信する攻撃について検証する．

➢ マスタになりすまして要求を送る攻撃

なりすましの成否を検証する際，保護対象とするシステムの各ノードが受信パケットのヘッダに記載されている IP アドレスや MAC アドレスを受信時の処理においてどのように扱っているかが重要となる．

例えば，受信したパケットのヘッダに記載された送

信元 IP アドレスに基づき，送信元がマスタであるかどうかの判断をスレーブがしている場合，攻撃者がなりすましを成功させるためには，なりすましパケットの送信元 IP アドレスをマスタのものに詐称する必要がある．(一方，送信元 MAC アドレスについては詐称する必要はない)．しかしながら，攻撃者が送信元 IP アドレスをマスタのアドレスに詐称して TCP 通信を開始したとしても，TCP SYN パケットを受信したスレーブは本来のマスタの IP アドレスに対して SYN-ACK を返信するため，なりすましノードが当該スレーブとセッションを確立することはできない．そのため，攻撃者は ARP スプーフィングによりスレーブの ARP テーブルを変更し，正規のマスタの IP アドレスに対応する MAC アドレスを攻撃ノードのそれに書換える必要がある．

この際の ARP スプーフィングパケット，およびスプーフィング成功後に攻撃者が送出するパケットは表 3 の網掛け部分に該当する．これと表 1，表 2 を比較すると，宛先が異常である場合は MAC フィルタ，MAC･IP フィルタのどちらでも検知できるが，宛先が正常である場合，MAC･IP フィルタでは検知できるが MAC フィルタでは検知できないことがわかる．

表 3 ARP スプーフィングとマスタ/スレーブへのなりすましに対する各フィルタの効果

送信元 / 宛先	IP のみ	MAC のみ	両方	詐称せず
IP 異常 MAC 正常				
IP 正常 MAC 異常				
IP 異常 MAC 異常	○ ○			
IP 正常 MAC 正常	× ○			

各欄で上は MAC フィルタ，下は MAC･IP フィルタの効果．○は遮断可能，×は遮断不可能を意味する．

一方，そもそもスレーブ側で受信したパケットの送信元 IP アドレスに基づく処理を行っていない場合は，攻撃者は送信元の IP アドレスおよび MAC アドレスの詐称を行う必要がないため，送信されるなりすましパケットは表 4 の網掛け部分に該当することになる．したがって，宛先が正常である場合は MAC フィルタ，MAC･IP フィルタ共に検知できないが，宛先が異常である場合はどちらのフィルタでも検知することが可能である．

表 4 マスタへのなりすましに対する各フィルタの効果(受信側が送信元 IP アドレス，MAC アドレスに基づく処理を行わない場合)

送信元 / 宛先	IP のみ	MAC のみ	両方	詐称せず
IP 異常 MAC 正常				
IP 正常 MAC 異常				
IP 異常 MAC 異常				○ ○
IP 正常 MAC 正常				× ×

各欄で上は MAC フィルタ，下は MAC･IP フィルタの効果．○は遮断可能，×は遮断不可能を意味する．

- スレーブになりすまして要求を受け取り，偽の応答を行う攻撃

次に，スレーブになりすまして，偽の応答を行う攻撃を想定する．このとき，攻撃者は ARP スプーフィングによりマスタの ARP テーブルを書換えた上で，送信元 IP アドレスを正しいスレーブのものであると詐称して通信する(送信元 MAC アドレスを詐称する必要はない)．以上から，表 3 の結果となる．

◆ FL-net

FL-net はトークンバス方式の通信を行うプロトコルである．各ノードは UDP パケットのブロードキャストを用いてメッセージを送信する．Ver.3 では，汎用コマンドサーバ機能によって，設定ツールから TCP/IP または UDP/IP ベースの通信により各種パラメータの設定や読み出しを行うことができる． 以下では，攻撃者が侵入ノード以外になりすまして偽の情報を書き込む攻撃と，設定ツールになりすまして設定を書き換える攻撃について検証する．

- 侵入ノード以外がトークンを保持しているときに，そのノードになりすまして偽の情報を書き込む攻撃

まず，受信したパケットに記載された送信元 IP アドレスに基づき，送信元がトークン保持ノードであるかどうかの判断を各ノードが行っている場合を考える．この場合，攻撃者は，送信元 IP アドレスをトークン保持ノードのものであると詐称して通信する(送信元 MAC アドレスを詐称する必要はない)．この際のなりすましパケットは表 6 の網掛け部分に該当する．したがって，宛先が異常である場合は MAC フィルタ，MAC･IP フィルタのどちらでも検知できるが，宛先が正常である場合，MAC･IP フィルタでは検知できるが MAC フィルタでは検知できない．

表 6 トークン保持ノードへのなりすましに対するフィルタの効果

送信元 / 宛先	IP のみ	MAC のみ	両方	詐称せず
IP 異常 MAC 正常				
IP 正常 MAC 異常				
IP 異常 MAC 異常	○ ○			
IP 正常 MAC 正常	× ○			

各欄で上は MAC フィルタ，下は MAC･IP フィルタの効果．○は遮断可能，×は遮断不可能を意味する．

次に，各ノードが受信したパケットの送信元 IP アドレスに基づく処理を行っていない場合を考える．この場合は，攻撃者は送信元の IP アドレスおよび MAC アドレスを詐称する必要はないため，送信されるなりすましパケットは表 7 の網掛け部分に該当する．したがって，宛先が正常である場合は MAC フィルタ，MAC･IP フィルタ共に検知できないが，宛先が異常である場合はどちらのフィルタでも検知することが可能である．

表 7 トークン保持ノードへのなりすましに対するフィルタの効果(受信側が送信元 IP アドレス，MAC アドレスに基づく処理を行わない場合)

宛先＼送信元	IP のみ	MAC のみ	両方	詐称せず
IP 異常 MAC 正常				
IP 正常 MAC 異常				
IP 異常 MAC 異常				○ ○
IP 正常 MAC 正常				× ○

各欄で上は MAC フィルタ，下は MAC･IP フィルタの効果．○は遮断可能，×は遮断不可能を意味する．

- 設定ツールになりすまし，汎用コマンドサーバ機能を使って設定を書き換える攻撃

まず，受信パケットの送信元 IP アドレスに基づき，送信元が設定ツールであるかどうかの判断を各ノードが行っている場合を考える．この場合，攻撃者は送信元 IP アドレスを設定ツールのものであると詐称して通信する(送信元の MAC アドレスを詐称する必要はない)．このとき，汎用コマンドサーバ機能が TCP/IP ベースで実装されている場合は，攻撃者は送信元 IP アドレスを設定ツールのアドレスに詐称して TCP 通信を開始したとしても，TCP SYN パケットを受信したノードは本来の設定ツールの IP アドレスに対して SYN-ACK を返信するため，なりすましノードが当該ノードとセッションを確立することはできない．そのため，攻撃者は ARP スプーフィングにより攻撃対象ノードの ARP テーブルを変更し，正規の設定ツールの IP アドレスに対応する MAC アドレスを攻撃ノードのそれに書換える必要がある．この際の ARP スプーフィングパケット，およびスプーフィング成功後に攻撃者が送出するパケットは表 8 の網掛け部分に該当する．したがって，宛先が異常である場合は MAC フィルタ，MAC･IP フィルタのどちらでも検知できるが，宛先が正常である場合，MAC･IP フィルタでは検知できるが MAC フィルタでは検知できない．

表 8　ARP スプーフィングと設定ツールへのなりすましに対するフィルタの効果(汎用コマンドサーバ機能が TCP/IP ベースの場合)

宛先＼送信元	IP のみ	MAC のみ	両方	詐称せず
IP 異常 MAC 正常				
IP 正常 MAC 異常				
IP 異常 MAC 異常	○ ○			
IP 正常 MAC 正常	× ○			

各欄で上は MAC フィルタ，下は MAC･IP フィルタの効果．○は遮断可能，×は遮断不可能を意味する．

一方，汎用コマンドサーバ機能が UDP/IP ベースで実装されている場合は，攻撃者は ARP スプーフィングを行う必要はなく，送信元 IP アドレスを設定ツールのものであると詐称して通信するだけでなりすましが可能である．この際に送出されるなりすましパケットは，表 9 の網掛け部分に該当する．したがって，宛先が異常である場合は MAC フィルタ，MAC･IP フィルタのどちらでも検知できるが，宛先が正常である場合，MAC･IP フィルタでは検知できるが MAC フィルタでは検知できない．

表 9　ARP スプーフィングと設定ツールへのなりすましに対するフィルタの効果(汎用コマンドサーバ機能が UDP/IP ベースの場合)

宛先＼送信元	IP のみ	MAC のみ	両方	詐称せず
IP 異常 MAC 正常				
IP 正常 MAC 異常				
IP 異常 MAC 異常	○ ○			
IP 正常 MAC 正常	× ○			

各欄で上は MAC フィルタ，下は MAC･IP フィルタの効果．○は遮断可能，×は遮断不可能を意味する．

次に，受信パケットの送信元 IP アドレスに基づく処理を各ノードが行っていない場合を想定する．この場合，攻撃者は送信元の IP アドレスおよび MAC アドレスの詐称を行う必要がないため，送信されるなりすましパケットは表 10 の網掛け部分に該当する．したがって，宛先が正常である場合は MAC フィルタ，MAC･IP フィルタ共に検知できないが，宛先が異常である場合はどちらのフィルタでも検知することが可能である．

表 10　設定ツールへのなりすましに対するフィルタの効果(受信側が送信元 IP アドレス，MAC アドレスに基づく処理を行わない場合)

宛先＼送信元	IP のみ	MAC のみ	両方	詐称せず
IP 異常 MAC 正常				
IP 正常 MAC 異常				
IP 異常 MAC 異常				○ ○
IP 正常 MAC 正常				× ×

各欄で上は MAC フィルタ，下は MAC･IP フィルタの効果．○は遮断可能，×は遮断不可能を意味する．

◆ Vnet/IP

Vnet/IP は UDP/IP 上に構築されたプロトコルである．各パケットには共通鍵を用いた認証子が付加されており，それによってなりすましや改竄に対する防御を行っているが，一部のパケットには仕様上認証子が付加されない．そのため，この種類のパケットを利用することでなりすまし攻撃が可能である．以下では，攻撃者が侵入ノード以外になりすまして偽の情報を送信する攻撃について検証する．

- 他ノードになりすまし，偽の情報を送信する攻撃

まず，受信したパケットの送信元 IP アドレスに基

づき，受信ノードが送信元を判別している場合を考える．この場合，攻撃者は送信元 IP アドレスをなりすますノードのものであると詐称して通信を行う(送信元の MAC アドレスを詐称する必要はない)．この際に送出されるなりすましパケットは表 11 の網掛け部分に該当する．したがって，宛先が異常である場合は MAC フィルタ，MAC･IP フィルタのどちらでも検知できるが，宛先が正常である場合，MAC･IP フィルタでは検知できるが MAC フィルタでは検知できない．

表 11 他ノードへのなりすましに対するフィルタの効果(送信元 IP アドレスに基づき送信元を判別している場合)

送信元 / 宛先	IP のみ	MAC のみ	両方	詐称せず
IP 異常 MAC 正常				
IP 正常 MAC 異常				
IP 異常 MAC 異常	○ ○			
IP 正常 MAC 正常	× ○			

各欄で上は MAC フィルタ，下は MAC･IP フィルタの効果．○は遮断可能，×は遮断不可能を意味する．

次に，受信パケットの送信元 MAC アドレスを用いて送信元を判別している場合を考える．この場合，攻撃者は送信元 MAC アドレスをなりすますノードのものであると詐称して通信を行う(送信元の IP アドレスを詐称する必要はない)．

この場合のなりすましパケットは表 12 の網掛け部分に該当する．したがって，MAC フィルタ，MAC･IP フィルタのどちらでも検知できる．

表 12 他ノードへのなりすましに対するフィルタの効果(送信元 MAC アドレスに基づき送信元を判別している場合)

送信元 / 宛先	IP のみ	MAC のみ	両方	詐称せず
IP 異常 MAC 正常				
IP 正常 MAC 異常				
IP 異常 MAC 異常		○ ○		
IP 正常 MAC 正常		○ ○		

各欄で上は MAC フィルタ，下は MAC･IP フィルタの効果．○は遮断可能，×は遮断不可能を意味する．

4.3 考察

以上から，MAC アドレスだけを条件とする MAC フィルタでは検知できない攻撃例があったが，MAC アドレスと IP アドレス双方を条件とする MAC･IP フィルタならば，想定した攻撃例のほぼすべてを検知できるという結果になった．このことから，生産制御システムのセキュリティ向上を目的として，スイッチ上でホワイトリストに基づくフィルタリングを行う場合，MAC･IP フィルタのように送信元および宛先の IP アドレスと MAC アドレスの双方を監視する手法が単純ながら効果が高いと言える．また，攻撃のいくつかは ARP スプーフィングを前提としているため，そもそも各ノードの ARP テーブルを固定とすることで，これらの攻撃を防ぐことができる．すなわち，ネットワーク機器におけるホワイトリストフィルタだけでなく，ノードにおいても通信先の静的ホワイトリスト化を行うことでなりすましを防ぐ効果が期待できる．

5 検証実験

プラント等で実用されているものと同機種のコントローラ等を用いた模擬プラント環境を用意し，4 章で低コストかつ効果が高いとされた MAC･IP フィルタについて，模擬プラント環境のスイッチ上に実装した場合に意図したとおりの効果を発揮するかどうか，検証実験を行った．

5.1 実験環境

実験環境となる模擬プラント環境は，図 3 のように，HMI2 台とそれぞれ 2 重化されたコントローラ 2 組が L2 Plus スイッチを介して接続された構成になっている．使用されている各機器はプラント等で実用されているものと同機種を用いており，各ノード間の通信は Vnet/IP で行われている．スイッチは Vnet/IP の仕様であるバスの 2 重化を模擬的に再現するため，VLAN を用いて仮想的に 2 つに分割されており，各機器はそれぞれの VLAN に対応したポートに 1 本ずつ結線されている．

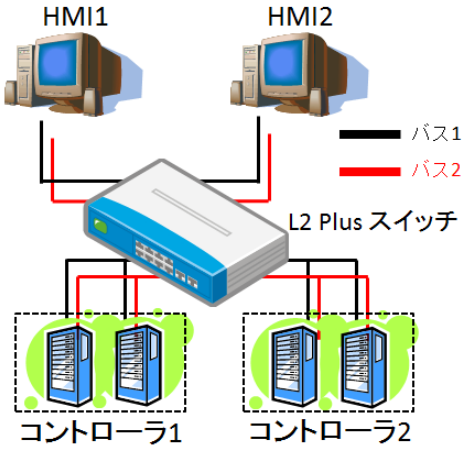

図 3 実験環境構成図

コントローラは模擬データに基づき，以下のように化学プラントにおける温度制御動作を模擬している．

● 温度制御模擬動作

(1) コントローラ 1 は模擬情報の温度データを取得し(実際のプラントにおける温度センサからの温度データ取得を模擬)，コントローラ 2 に送信する

(2) コントローラ 2 は受け取った温度データに基づき，目標温度値に近づけるための冷却水の流量を計算

(3) コントローラ 2 は目標流量になるようなアクチュエータ操作量を計算しコントローラ 1 に送信

(4) コントローラ 1 は受け取った操作量に基づきアクチュエータ模擬データに命令．これによりアクチュエータ状態模擬データが変化し，伴って流量模擬データも変化する

(5) (1)に戻る

HMI は，上記プロセスが正常に動作しているかどうかをモニタリングする．やり取りされている各種パ

ラメータの数値，およびそれらの値を時刻ごとに描画したグラフが表示される．正常に動作している場合，図 4 のようになる．

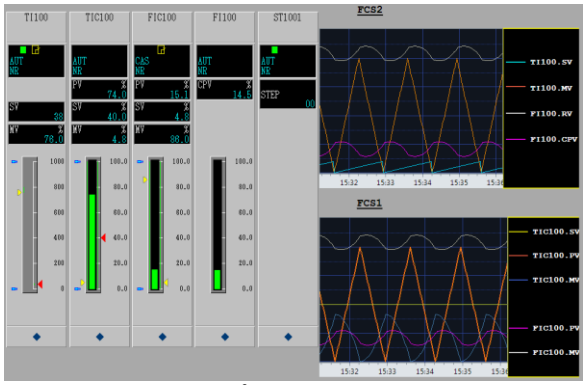

図 4　模擬プラント環境監視画面

5.2　模擬攻撃

模擬攻撃は，スイッチに新規に接続したノート PC から行う．Vnet/IP のパケットは通常，共通鍵を用いたメッセージ認証子が付加されておりなりすましは困難だが，一部認証子が付加されないパケットがある．その種類のパケットのうち，ある特定のものを繰り返し送信すると，図 5 のように監視画面に乱れが生じる．この攻撃を防ぐことができるかどうかを検証する．

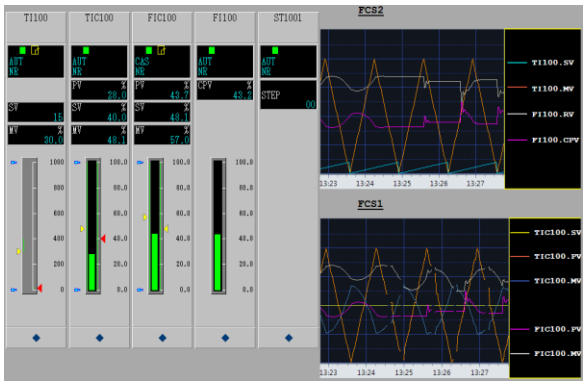

図 5　模擬攻撃によって乱れた監視画面

5.3　実験方法

スイッチにフィルタを適用していない場合と，3 章の手法に基づき 4 章の MAC･IP フィルタを L2 Plus スイッチ上に実装した場合の双方において 5.2 節で述べた模擬攻撃を行い，HMI の監視画面の変化を比較した．フィルタの設定は，スイッチの各ポートにおいて inbound フィルタを設定し，送信元 IP アドレスおよび送信元 MAC アドレスがそのポートに接続される機器のものであり，宛先 IP アドレスおよび宛先 MAC アドレスが他の正規ノードおよびマルチキャストのものであるパケットのみを許可し，それ以外を遮断する設定とした．ただし，使用したスイッチの仕様上適用できるフィルタの数に限りがあったため，バス 1 のポートのみの設定とし，バス 2 のポートについてはすべて許可する設定とした．未使用のポートについては，バス 1，バス 2 共にすべてのパケットを遮断する設定とした．

5.4　実験結果

- フィルタを適用していない場合

図 5 で示すような監視画面の乱れが生じた．

- フィルタを適用した場合

監視画面に乱れは生じず，図 4 のような周期的なグラフが描画され続けた．

5.5　考察

5.4 節の結果から，フィルタリングにより模擬攻撃からシステムを防御することに成功した．この実験では特定のシステムにおける特定の一例を示すだけにとどまったが，今後はこれ以外の模擬攻撃に対しても実験を行い，フィルタの有効性を示すと共にフィルタ適用による遅延の増加等の影響を検証したい．

6　まとめと今後の課題

本稿では，まず生産制御システムのセキュリティ上の問題点を整理した．その上で，Ethernet 化，IP 化された制御ネットワークにおいて，認められたノード間通信のホワイトリストに基づきスイッチ上で厳密なパケットフィルタリングを行うことによりなりすまし通信を遮断する手法について，アプリケーションレイヤの具体的な攻撃モデルを想定し評価を行った．その結果，低コストで導入できる一手法として，送信元および宛先の IP アドレスと MAC アドレスの双方を監視する手法が単純ながら効果が高いことが分かった．今回評価を行った防御手法モデルのどちらを用いても検知できない攻撃もあるため，今後はそうした攻撃に対抗する手法についても検討を行いたい．

謝辞

本研究の一部は，JSPS 科研費 24680006 の助成により行われた．

参考文献

[1] RISI - The Repository of Industrial Security Incidents, http://www.risidata.com/
[2] サイバーセキュリティと経済　研究会　中間とりまとめ, http://www.meti.go.jp/committee/kenkyukai/shoujo/cyber_security/report01_02_01.pdf
[3] IPA(独立行政法人情報処理推進機構), “重要インフラの制御システムセキュリティと IT サービス継続に関する調査報告書”
http://www.ipa.go.jp/files/000013981.pdf
[4] W32.Stuxnet, http://www.symantec.com/ja/jp/security_response/writeup.jsp?docid=2010-071400-3123-99
[5] Sophia,
http://nexdefense.com/about-sophia/
[6] Passive Vulnerability Scanner,
http://www.tenable.com/products/passive-vulnerability-scanner
[7] Dragos Security,
http://dragossecurity.com/products/
[8] OPEN MODBUS/TCP SPECIFICATION, http://www.rtaautomation.com/modbustcp/files/Open_ModbusTCP_Standard.pdf
[9] 一般社団法人　日本電機工業会, "OPCN 規格･技術資料,"
http://www.jema-net.or.jp/Japanese/standard/opcn/opcn07.html
[10] リアルタイム･プラント･ネットワーク･システム Vnet/IP,
https://www.yokogawa.co.jp/rd/pdf/tr/rd-tr-r04902-010.pdf