5X-03

制御ネットワーク向け侵入検知システム

桂井　銀河†　　向井　宏明†　横谷　哲也†

金沢工業大学　工学部†

1. はじめに

近年，ビル，工場などの制御システムを狙ったサイバー攻撃が顕在化しており，人命に関わるなど，物理世界に影響が大きい事故が発生することが懸念される．

2016 年 11 月フィンランドにて，ビルが DDoS 攻撃を受け少なくとも 2 つのビルの暖房が停止した事例があった．攻撃を受けた暖房や水温を管理するシステムは，主制御回路を再起動することで攻撃に対応しようとしたが，再起動が何度も繰り返しされたため，最終的にシャットダウンし，暖房が利用できない状況が続いた[1].

ビル管理システムは，便利さと使いやすさを求めている一方でセキュリティが無視されていることが多い．そのため，現状の制御システムには，セキュリティ対策がほとんど施されておらず， 制御システム向けのセキュリティ技術の開発が急務であり，研究開発がおこなわれている[2].

本稿では，低コストかつ小型のハードウェアにて，制御ネットワークに流れるトラフィックを監視することにより制御システムに対するサイバー攻撃を検出する方式を検証したので報告する．

2. 制御ネットワークのサイバー攻撃検知における課題

機器に対するサイバー攻撃対策として，ファイアウォールや侵入検知システム（IDS: Intrusion Detection System）が IT システムで広く利用されている．

ファイアウォールは，運用ポリシーに基づいた通信制御が主な目的であり，運用側が意図するように情報システムへアクセスさせるための機能である．ビル管理システムにおいて，ビル管理者による遠隔操作の妨げになり，利便性が失われることや，多くのビル会社や個人所有者が，ネットワークファイアウォールに投資することを敬遠していることから，ファイアウォールの導入は厳しいことが現状である．

一方，IDS は情報システムに対するセキュリティ上の脅威を積極的に検知しようとするものである．IDS はネットワークに対して不正なアクセスがないかをリアルタイムでチェックし，疑わしい内容があれば管理者へ通知を行う IDS はネットワーク型・ホスト型の 2 種類の監視方法に分けられる．ネットワーク型 IDS はネットワーク上を流れる通信パケットを監視し，そのデータやプロトコルヘッダを解析する．監視対象となるネットワークに設置されるが，直接接続しているネットワークセグメントについてのみ監視できるため，監視したいネットワークが複数ある場合，それぞれに配置する必要がある．

ホスト型 IDS は監視対象のサーバなどにインストールされ，OS が記録するログファイルやサーバ内のファイル改ざんを監視し侵入を検知する．インストールされたホストにのみ動作するため，システムに保護したい端末が複数ある場合はそれぞれにインストールする必要がある．

ビル管理システムでは，サイバー攻撃を想定して運用している機器は少なく，暗号化機能や認証機能が導入されていないことが多い．そのため，コスト面などから CPU 性能とメモリ領域は少ない場合が多く，ホスト型 IDS の適用が困難である．このことから，機器の性能に依存せずに不正通信を監視できるネットワーク型 IDS が適していると考えられる．しかし，一般的な IT システムのネットワークに比較して制御ネットワークに流れるネットワークトラフィックは少ないため[3]，IDS が行なう処理は軽いものとなる．そのため一般的な IT システムの IDS をそのまま利用するとオーバースペックであり，コストやサイズが見合わなくなってしまうことが課題である．

3. 制御ネットワーク向け IDS の提案

一般的なビル管理システムの構成を図 1 に示す．提案方式では，ネットワーク型 IDS 機能をルータと制御機器の間に挟みこむように配置することで，ネットワークトラフィックを監視する．

ビル管理システムにおいてのルータは，制御ネットワークにおいて，制御機器とインターネットを介した管理者が遠隔操作をするための中継する役割の機器である．この周辺に監視機能を実装することで制御機器を狙った，不正な通信を検知することができる．しかし，コスト面から，ミラーリング機能を持たない機器でネットワークが構成されていることが多いため，運用中のネットワーク機器間に IDS を挟みこむ必要があると考えられる．

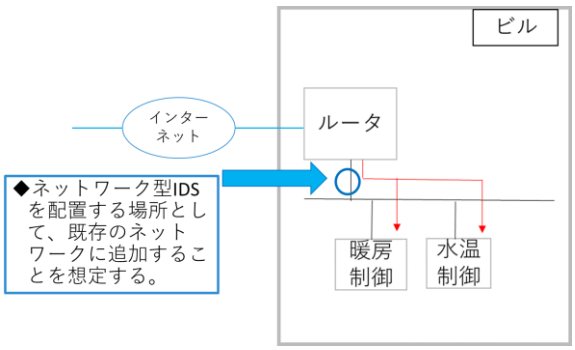

図 1 ビル管理システムにおける IDS 設置箇所

また，制御ネットワークでは，通信のやりとりを行なう利用者ユーザが固定的ため，提案方式では，ホワイトリスト型検知式を採用し，決められた通信のみを通すことで，不正侵入を検知する．

Intrusion detection system for control networks

†Ginga Katsurai, Hiroaki Mukai and Tetsuya Yokotani
College of Engineering, Kanazawa Institute of Technology

4. IDS の検証

4.1 検証環境

前述の制御ネットワークにおける課題を解決するために，低コストで小型のハードウェアに IDS の機能を実装することで，制御ネットワークに適した，セキュリティ対策の実現可能性を検証する．今回の検証で使用する IDS として，オープンソースのネットワーク IDS である Suricata を実装した RaspberryPi4ModelB/4GB を使用した．また，管理者が検知ログを可視化できるようにするために，kibana を実装した．

RaspberryPi に実装した IDS が，DDoS 攻撃を検知できるか，検証を行なう．今回検証を行なった検証環境の構成を図 2 に示す．図 2 の検証環境は，ビル管理システムを PC 上に構築し，ネットワークトラフィックは現実の実際の制御ネットワークのトラフィックを模擬したものである．模擬する環境を構築する理由として，実際のビル管理システムを使用しての検証は危険が伴うためである．

検証では，1 台の不正端末が hping3 コマンドの flood 設定で UDP パケットを疑似 PAC コントローラに送信し，ログを可視化している Kibana の 5601 番ポートにアクセスすることで，結果の確認を行なう．

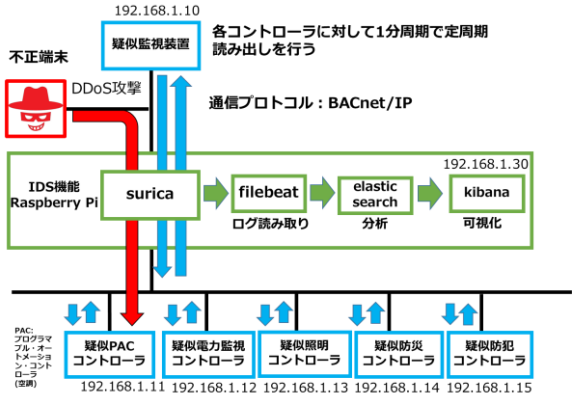

図 2　検証環境

4.2 提案方式の検証

今回の検証環境に合わせた検知ルール設定するために，ホワイトリストの登録と検知条件の設定を行なった．

ホワイトリストへの登録では，疑似監視装置と各疑似コントローラの IP アドレスを登録することにより，正常運用時に，検知ルールを適応しないようにした．

検知条件では，通信を行なっている受信側の IP アドレスが各疑似コントローラの IP アドレスである場合，検知アラートを鳴らす設定を行なった．検知アラートは，不正アクセスを受けた，コントローラの名前をメッセージ表示するように設定を行なった．

作成したルールを IDS 内で有効化した後に，不正端末で疑似 PAC コントローラに大量の UDP を 1 分間送信し，ログ情報を可視化している Kibana の結果を確認した．

Kibana の可視化した結果を図 3 と図 4 に示す．Kibana では，Suricata を通過している送信元の IP アドレスの割合と，タイムスタンプを利用した，リアルタイムの検知状態を表示するように設定した．

図 3　送信元 IP アドレスの割合変化

図 3 の左の円グラフは，正常運用時の送信元 IP アドレスの割合を示しており，右の円グラフは，DDoS 攻撃を受けた後の送信元 IP アドレスの割合を示している．

DDoS 攻撃後の右の円グラフでは，左の正常運用時の円グラフには表示されていなかった，新たな IP アドレスが，全体の 99.77%を占める結果となった．

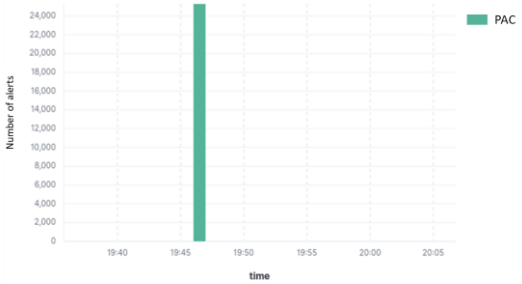

図 4　検知アラート

図 4 にて，時刻 19:46 から 19:47 の 1 分間のみ PAC のアラートが大量に発生している結果となった．

今回の IDS の機能検証では，不正端末からの通信を図 3 の円グラフでは，新たな IP アドレスが全体の 99.77%を占める状態を確認することができ，図 4 の検知アラートグラフでは，DDoS 攻撃の発生タイミングを確認することができたため，正常に IDS が動作していると考えられる．

5. おわりに

本稿では， オープンソースの IDS である Suricata を用い，RaspberryPi のような低コストかつ小型のハードウェアにて，ネットワークに流れるトラフィックから不正な通信を検知し Kibana によってログを可視化する機能の実現性を検証した．今後は，様々な攻撃パターンについての検証や，長期運用による CPU やメモリなどの処理性能についての検証，ホワイトリストの自動登録する機能を検討していきたい．

謝辞

本研究(の一部)は，内閣府が進める戦略的イノベーション創造プログラム(SIP)第 2 期「IoT 社会に対 応したサイバー・フィジカル・セキュリティ」(管理法人:NEDO)によって実施されました．

参考文献

[1] ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第 1 版

[2] NEDO:戦略的イノベーション創造プログラム（SIP）第 2 期／IoT 社会に対応したサイバー・フィジカル・セキュリティ
https://www.nedo.go.jp/activities/ZZJP_100156.html

[3] 阿久津　幹, 向井宏明, 横谷哲也, "制御ネットワークの　異常検知に向けたトラフィック分析", 信学技報, vol. 119, no. 344, NS2019-159, pp. 133-138, 2019 年 12 月.