（様式１４－１号）

学 位 論 文 内 容 の 要 旨

学位論文題目	IoT 環境におけるサイバー攻撃に対する時刻同期技術を利用したイベント検知手法に関する研究
氏　　名	川 村　　保

近年、インターネットに様々なものを接続する IoT が普及し始めている。IoT は、従来のインターネット上のサービスだけでなく、産業用オートメーションや制御システムなどの社会インフラやビジネス、さらに個人生活にも浸透し始めており、実世界とインターネット世界が一体化して、公共や生命、財産に関わる情報を手軽に取り扱うことが可能になっている。その反面、インターネットと同様に、分散サービス拒否（DDoS）攻撃や不正アクセスなどのサイバー攻撃が目立ち始め、被害も深刻化している。このため、IoT に対するセキュリティ対策は緊急の課題となっている。

セキュリティ対策に関する国際標準規格では、対策の規範として、抑止、防止、検知、回復の 4 段階の対応を求めている。抑止や防止が対策の基本ではあるが、それらの対策に不備があったり、未知のサイバー攻撃を受けたりするとシステムや機密情報を守れないため、重篤な被害に陥るのを阻止し迅速な回復を行うためには、検知が重要な役割を果たす。国際標準規格では、システムの周辺状況が出現または変化した状態をイベントとして検知し、より深刻な状態であるインシデントやアクシデントに至るのを阻止することが求められている。

これまでに、一般的なコンピュータネットワークに対する検知手法として、パケットキャプチャやファイヤーウォール、侵入検知システム、ウィルス対策ソフトなどが研究されている。しかし、それらの検知手法は、IoT デバイスのシステムリソース量の制約やリアルタイム検知と専門家による保守作業の困難さなどの問題から、IoT 環境には不向きである。府省の IoT セキュリティガイドラインでは、IoT デバイスのリソース使用量やネットワーク負荷などの状態を把握することが提唱されているが、それらの情報をいかに役立てて精度よくイベント検知を行うかの方法論は未だに確立されていない。

そこで本論文では、コンピュータや IoT デバイスで一般的なネットワーク時刻同期技術を利用するアプローチから、IoT 環境に適するイベント検知手法を明らかにすることを目的とする。本論文で利用する時刻同期技術は、時刻同期サーバと NTP (Network Time Protocol) パケットを交換することにより、システムクロックを標準時に同期させるものである。本論文では、IoT デバイスがサイバー攻撃を受けた場合に、CPU やネットワークインタフェースの割り込み処理が平時と比較して多発し過負荷になることで、システムクロックが大きくずれ、ネットワーク通信時間が遅延する現象に着目する。すなわち、本論文における検知の原理は、被攻撃時に多発する現象に着目することで、検知されたイベントがユーザの通常処理によるものなのか攻撃によるものなのかを精度よく区別することにある。

本論文では、IoTデバイスで直接的に情報を収集し判断を行うホスト型とIoTデバイスが接続される通信処理装置で間接的に情報を収集し判断を行うネットワーク型の両イベント検知手法を提案する。さらに、本提案手法の有用性を実証するために、本手法に基づくイベント検知モジュールを開発し、擬似サイバー攻撃を発生させて、イベント検知の実証実験を行う。本手法には、既存手法が抱える上記の問題を解決するだけでなく、検知のために新たな通信トラヒックを発生させない、また、高価な機器も必要とせず、暗号化通信にも対応しているという利点を有するため、様々な環境での応用が期待される。

本論文の構成は、以下のとおりである。

第1章は緒言であり、本研究の背景と目的について述べる。

第2章では、情報セキュリティ対策に関する国際標準規格と各国政府のガイドラインの方針、目的及び要求事項からイベント検知の重要性を示し、従来のイベント検知手法に関して、検知のタイミングとシステムリソース量の観点で分類しながら研究動向をまとめる。それらの従来手法をIoT環境に適用した場合の問題点を考察した上で、IoTで求められるイベント検知に対する要件を述べる。さらに、予備実験としてIoTにおいて既存の異常検知の内のシステム監視を行った結果を評価し、新たなイベント検知手法の必要性を明らかにする。

第3章では、時刻同期技術を用いたホスト型のイベント検知手法を提案する。本論文で着目する時刻同期技術であるchronyの時刻補正の仕組みを述べた上で、提案するホスト型のイベント検知手法の詳細を述べる。本手法は、NTPパケットから得られる時刻補正量、時刻同期要求・応答の通信遅延の揺らぎを計測することにより、イベントの検知を行う。本手法に基づく検知モジュールを開発してIoTデバイスに組込み、擬似的にサイバー攻撃を発生させた場合のイベント検知の実証実験を行う。本実験により、検知対象のIoTデバイスが、DDoS攻撃の被害者または加害者、不正アクセスの被害者、さらには、非攻撃時のアイドル状態、許可されたユーザ処理としてファイルの送受信を行う場合のいずれにおいても、見逃しと誤検知の少ない精度のよいイベント検知が可能であることを確認し、本手法の有効性を示す。

第4章では、時刻同期技術を用いたネットワーク型のイベント検知手法を提案する。ネットワーク型の場合、外部からの攻撃を検知するために、一次時刻同期サーバとの往復通信の遅延時間の揺らぎを計測し、内部からの攻撃を検知するために、直上位の時刻同期サーバとの往復通信の遅延時間の揺らぎを計測することにより、イベント検知を行う。本手法に基づく検知モジュールをIoTルータに組込み、第3章と同様にDDoS攻撃、不正アクセス、非攻撃時の実証実験を行い、本手法の有効性を示す。

最後に、第5章で、本論文全体のまとめと、今後の課題と将来性の展望について述べる。

付録Aでは、異常検知に基づくシステム監視によるイベント検知の実現性を確認するための予備実験を行う。IoTデバイスに対して擬似的にDDoS攻撃と不正アクセスを発生させ、CPU使用率、メモリ使用量、ディスク入出力リクエスト数、送受信データ量をなどの統計量を取得し、自己回帰移動平均モデルで解析を行うことでイベント検知を行う。この結果から、一般的なシステム監視によるイベント検知の問題点を明確にすることで、本提案の要件の参考とする。

7．の別紙３

学位論文審査の結果及び試験，試問の結果報告書

（論文博士用）

山口大学大学院理工学研究科

報告番号	理工博乙　第　0143　号	氏　名	川村　保

最終試験担当者	
	主　　査　福士　将
	審査委員　松藤　信哉
	審査委員　浜本　義彦
	審査委員　山口　真悟
	審査委員　平野　靖
	審査委員　藤田　悠介

【論文題目】IoT 環境におけるサイバー攻撃に対する時刻同期技術を利用したイベント検知手法に関する研究
(Study on Event Detection Methods Using Time Synchronization Technique for Cyber Attacks on IoT Environment)

【論文審査の結果及び試験，諮問の結果】

近年，インターネットにスマートセンサーや家電などの様々なものを接続する IoT (Internet of Things) が普及し始めており，そのセキュリティ対策として，サイバー攻撃の予兆を早期に発見するイベント検知の重要性が増している．国際標準規格やガイドラインでは，IoT 機器の処理負荷や通信負荷などの統計情報を用いて，リアルタイムにイベント検知を行う必要性が示されているものの，IoT 環境に適用可能な精度の高いイベント検知の実現方法に関しては，まだあまり研究が進んでいない．

本論文では，IoT 機器やコンピュータなどにおいて一般的に利用される時刻同期技術を利用したイベント検知手法を提案している．本提案手法では，IoT 機器がサイバー攻撃を受けた際に，時刻同期のために用いられる情報に変動が生じる現象に着目することで，検知されたイベントがサイバー攻撃によるものなのか否かを精度よく判別することを可能にする．本提案手法は，イベント検知処理の負荷が軽く，暗号化通信に対応しており，定期的なメンテナンスが不要であるなどの利点を有するため，IoT 向けの実用性の高い手法として貢献するものと考えられる．

本論文の構成と内容は以下の通りである．

第１章では，研究の背景と目的，論文の構成について述べている．

第２章では，本研究に関連する情報セキュリティとサイバー攻撃の基礎的事項を述べるとともに，コンピュータネットワーク環境を対象とした従来のイベント検知手法とそれらの問題点をまとめ，IoT 環境におけるイベント検知の要件を明らかにしている．

第３章では，ネットワークを介した時刻同期の基本原理を説明した上で，IoT 機器が自身に対する攻撃を直接的に検知可能なホスト型のイベント検知手法を提案している．IoT 機器がサイバー攻撃を受けた場合に，システム内で多発する内部割り込みの影響により，時刻同期における時刻調整量が大きく変動する現象に着目することで，サイバー攻撃と平常時のイベントを判別可能にする．本手法に基づくイベント検知モジュールを開発し，サービス妨害攻撃や不正アクセスを含む疑似的なサイバー攻撃を発生させた実証実験により検知精度を評価し，提案手法の有効性を検証している．

第４章では，IoT ルータなどの通信装置が他の IoT 機器に対する攻撃を間接的に検知可能なネットワーク型のイベント検知手法を提案している．被攻撃時に，IoT 機器と時刻同期サーバ間の通信遅延が大きく変動する現象に着目することで，精度のよいイベント検知を可能にする．本手法に基づくイベント検知モジュールを開発し，疑似的なサイバー攻撃を発生させた実証実験により検知精度を評価し，提案手法の有効性を検証している．

第５章では，本論文の成果をまとめ，今後の展望を述べている．

公聴会には本学の教員，学生が参加し，活発な質疑応答がなされた．その主な内容として，

(1) 提案手法によるイベント検知後に取り得る対策
(2) 実験で用いた IoT 機器の妥当性
(3) 実験における疑似サイバー攻撃の発生方法とその妥当性
(4) 提案手法の適用先が異なる場合の誤検知の可能性
(5) 提案手法を適用する際の IoT 機器のオペレーティングシステムに関する制約
(6) 自動車内の制御ネットワークに対する提案手法によるイベント検知の可能性と問題点

等の質問があり，いずれに対しても申請者から的確な回答がなされた．

以上より，本研究は，新規性，信頼性，有効性，実用性ともに優れており，博士（工学）の論文に十分に値するものと判断した．論文内容，並びに，審査会，公聴会での質問に対する応答などから総合的に判断して，最終試験は合格とした．

なお，主要な関連論文の発表状況は，以下の通りである．

1. 川村保，福士将，平野靖，藤田悠介，浜本義彦，IoT へのサイバー攻撃に向けた時刻同期サービスを利用したイベント検知手法，電子情報通信学会論文誌，Vol. J101-D，No. 5，pp. 742-753，May 2018.
2. Tamotsu Kawamura, Masaru Fukushi, Yasushi Hirano, Yusuke Fujita, Yoshihiko Hamamoto, An NTP-based Detection Module for DDoS Attacks on IoT, Proc. of ICCE-TW, pp. 15-16, June 2017.
3. Tamotsu Kawamura, Masaru Fukushi, Yasushi Hirano, Yusuke Fujita, Yoshihiko Hamamoto, A Network-based Event Detection Module Using NTP for Cyber Attacks on IoT, Proc. of CANDARW, pp. 86-91, Nov. 2018.