公開

研 究 終 了 報 告 書

「IoT 機器の実行環境の隔離を実現する IoT 基盤ソフトウェアの構築」

研究期間: 2019年10月～2023年3月
研 究 者: 山内 利宏

1. 研究のねらい

IoT 機器を対象としたマルウェア(以降, IoT マルウェア)の感染活動が活発化しており, インターネットに接続する多くの IoT 機器が攻撃対象となっている. また, IoT マルウェアの感染活動は, Telnet などのリモートログイン可能なサービスの脆弱なパスワード利用だけでなく, ソフトウェアの脆弱性を悪用した感染活動も行われている. IoT 機器には, PC などと異なり, セキュリティ機能が十分に活用されていない機器が多くあり, またセキュリティの自動更新機能がなく, 適切に運用されていない機器も少なくない.

本研究では, 今後も適切に管理や運用がされていない機器, サポート切れの機器が使用されることを想定し, そのような機器であっても, IoT マルウェアの攻撃を防止, もしくはその影響を緩和できる基盤ソフトウェアレベルのセキュリティ機能の基盤技術を実現し, より安全な IoT 機器が今後利用される環境を目指す.

研究目的を実現するためには, 現在の IoT 機器のソフトウェアの実態を明らかにし, どのような課題があるのかを明らかにすることが必要である. 一方で, IoT 機器のソフトウェアのセキュリティ機能の活用状況は明らかでなく, IoT 機器のソフトウェアの課題は明らかでない. また, 新たなセキュリティ機能を提案したとしても, 実際の IoT 機器で利用する際の課題も明確ではない.

そこで, 本研究課題では, IoT 機器向けの新たな基盤ソフトウェアのセキュリティ機能を提案するだけでなく, IoT 機器のソフトウェアのセキュリティ上の課題を明確化, 及びどのようなセキュリティ機能であれば, 製品に受け入れられる可能性があるのかを, IoT 機器のファームウェアの大規模分析, および IoT 機器ベンダへのインタビューにより, 明らかにすることにも取り組む.

2. 研究成果

(1) 概要

IoT 機器のセキュリティ機能を向上させるためには, IoT 機器が IoT マルウェアの攻撃対象になる要因, ソフトウェア構成, 及びセキュリティ機能を明らかにし, IoT 機器のソフトウェアの課題を明らかにする必要がある. このために, IoT 機器のソフトウェアの実態の大規模調査を行った. また, IoT 機器のセキュリティにおける課題を明らかにするためには, ソフトウェアの調査だけでは不十分であり, 実際の開発における課題を把握することも必要である. そこで, IoT 機器を販売しているベンダにインタビューを行い, IoT 機器のソフトウェアの課題を調査した. さらに, IoT マルウェアに有効なセキュリティ機能を実現するには, IoT マルウェアの感染活動の実態を明らかにする必要がある. このために, IoT マルウェアの感染活動をシステムコールレベルでログを取得し分析できるハニーポットを開発し, 分析した. これらの結果を基に, IoT 機器で有効で, かつ実際にベンダに利用可能な Linux 向けセキュリティ機能の実装方式を検討し, 主に 2 つのセキュリティ機能を開発し, 実装と評価を行った.

(2)詳細

研究テーマ A: IoT 機器のソフトウェアの課題の明確化(代表的な論文1)

今後は機器が持つ脆弱性を利用するなど，さらなる攻撃の高度化が予想される．このため，我々は IoT 機器のファームウェア解析に基づいた大規模かつ体系的な分析手法(**図1**)を提案し，実施した．この手法は，IoT 機器のファームウェアや GPL ソースコードを収集し，メモリ破壊攻撃を緩和するセキュリティ機能，Linux カーネルのセキュリティ機能等の利用状況，カーネルやアプリケーションのバージョン情報を自動的に分析するものである．

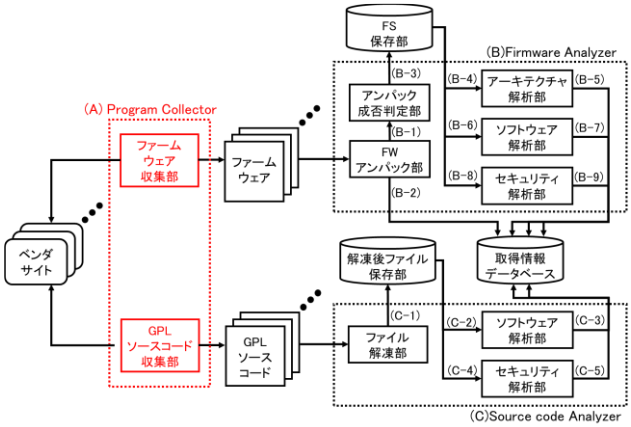

図 1　開発した解析プログラム

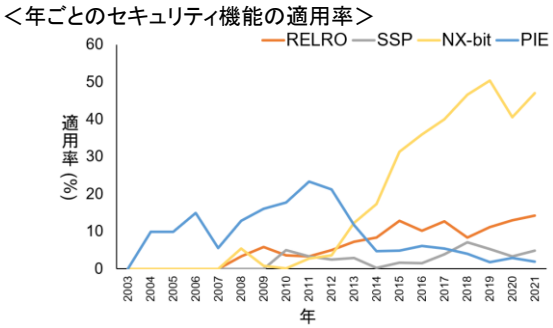

図 2　セキュリティ機能の適用率の変化

分析対象は，18 ベンダのファームウェア 7,339 個，GPL ソースコード 3,045 個である．分析結果から，IoT 機器において，ソフトウェアのセキュリティ機能が活用されていないこと(**図2**)，古いバージョンのソフトウェアが使い続けられていることを明らかにした．また，Linux カーネルのセキュリティ機能や LSM ベースのアクセス制御はほとんど利用されていないことを示した．さらに，実行プログラムのハッシュ値や類似度の比較分析により，ソフトウェアのバージョンを上げるのではなく，バージョンはそのままでパッチを当てられた実行ファイルが多数存在することを明らかにした．これにより，ソフトウェアのバージョン番号で脆弱性の有無を識別することは，不正確な結果となることを示し，IoT 機器の脆弱性把握における課題を示した．

研究テーマ B: IoT 機器のセキュリティにおける課題のベンダへのインタビュー調査(代表的な論文2)

研究テーマ A において，IoT 機器のソフトウェアの大規模分析により，セキュリティ上の問題を示したものの，この問題の要因や改善されない原因は明らかでない．そこで，IoT 機器を開発しているベンダにインタビューを行い．明らかになった問題の要因や実態を調査した．また，予備調査からの新たな調査項目として，カーネルへの攻撃に対するセキュリティ機能，LSM ベースのセキュリティ機能を追加し，新たな調査対象としてファームウェアだけでなく，GPL ソースコードを追加した．

最初のインタビューでは，セキュリティ機能を意識した開発が難しい状況と，セキュリティ機

能の適用率には，チップベンダが提供する SDK の影響が大きいことを明らかにした．また，ソフトウェアの脆弱性は，バージョンアップをせず，パッチの適用で対処することがあることを明らかにした．次のインタビューでは，セキュリティパッチの作成者や，セキュリティパッチの敵意用の判断について調査した．ここでも，チップベンダの影響が大きいことを示した(図3)．

インタビュー調査の結果から，ソフトウェアコンポーネントの透明性と脆弱性評価における課題を指摘し，さらに，IoT 機器のサプライチェーンの課題を示した．また，セキュリティを考慮した IoT 機器を開発するには，サプライチェーンの上流組織へのアプローチが重要であることを示した．

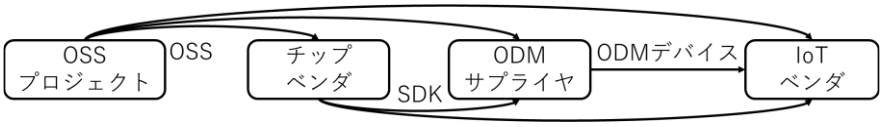

図 3　ソフトウェアコンポーネントの管理

研究テーマ C: IoT マルウェアのシステムコールレベルでの感染動作の解析(代表的な論文3)

本研究では，IoT 機器内部で IoT マルウェアの感染活動を観測し，OS の設定の不備や，ソフトウェアの脆弱性で侵入されたとしても，攻撃を防止，もしくは緩和できるセキュリティ機構を提案する．このために，IoT マルウェアの感染活動を詳細に分析する必要がある．そこで，Telnet でリモートからログインした IoT マルウェアの実行コマンドと，実行コマンドにより発行されたシステムコールを対応付けて分析することにより，IoT マルウェアの感染処理を分析し，7 段階の感染動作があることを明らかにした(図4)．また，各段階の操作における共通的なシステムコールを明らかにし，システムコールのアクセス制御で活用できる情報を得た(表1)．

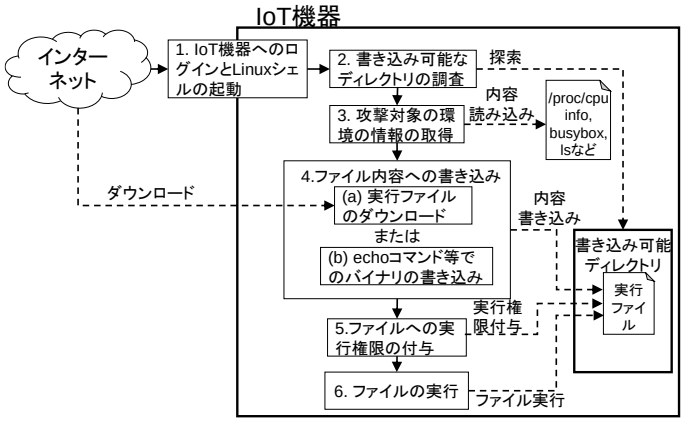

図 4　ログから推測した IoT マルウェアの動作

表 1　各処理で実行されるコマンドと呼び出される主要なシステム

処理	コマンド	主要なシステムコール
Linux シェルの起動	sh	execve
	ベンダ特有のシェル起動コマンド	未調査
書き込み可能なディレクトリの探索	出力のリダイレクトと cd	openat, chdir
攻撃対象の環境情報の取得	入力のリダイレクトと echo	openat, read, write
	cat, hexdump, dd	openat, read, write
ファイルのダウンロード	wget, tftp, curl	socket, connect, openat, write
echo コマンドによるバイナリ書き込み	出力のリダイレクト echo	openat, write
ファイルへの実行権限付与	chmod	fchmodat
	cp	openat, read, write
シェルスクリプトの実行	sh	execve
バイナリファイルの実行	作成されたプログラム	execve

研究テーマ D： IoT マルウェアの動作を考慮したシステムコールレベルのアクセス制御機構（代表的な論文3）

研究では，このような IoT マルウェアの攻撃を対策の対象とする．IoT マルウェアの各段階の動作について，どれか 1 つの動作を防止することができれば，後続の処理を防止でき，結果としてマルウェアの実行を防ぐことができるため，各段階について対策手法を検討した．この中で，提案手法の要件を考慮し，“(1) Linux シェルの起動”，“(5) ファイルへの実行権限の付与”，“(6)-(a)シェルスクリプトの実行” の 3 つの段階をアクセス制御で防止する対象とした．

提案するアクセス制御機構では，上記 3 つの段階の処理に関係のある3つのシステムコールにおいて，システムコール発行の防止，もしくはシステムコール引数を変更し，実行ファイルの生成，実行ファイルへの書き込み，および実行権限の付与を防止することを実現した(表2)．また，誤検知を防止するため，プロセスの親子関係をチェックし，外部からリモートログイン後に起動されたプロセスのみをアクセス制御対象とし，誤検知を防止する．

表 2　感染動作に対する対策と対策処理の有効性

番号	感染動作	実行ファイルへの書込禁止	シェルの実行禁止	実行権限の付与禁止
(1)	Linux シェルの起動	×	○	×
(2)	書き込み可能なディレクトリの探索	×	×	×
(3)	攻撃対象の環境情報の取得	×	×	×
(4) - (a)	ファイルのダウンロード	×	×	×
(4) - (b)	echo コマンドによるバイナリ書き込み	×	×	×
(5)	ファイルへの実行権限付与	○	×	○
(6) - (a)	シェルスクリプトの実行	×	○	×
(6) - (b)	バイナリファイルの実行	×	×	×

実際の IoT マルウェアによる攻撃に対して評価した結果，提案手法により，IoT マルウェアの感染動作を防止できることを示した．

研究テーマ E： Seccomp フィルタを用いたアクセス制御機構

IoT 機器への攻撃は，既知のログイン情報を用いるものや，簡単なパスワードを用いて侵入するものが多かったが，IoT 機器のソフトウェアの脆弱性を悪用して侵入し感染する事例がある．今後は，後者のソフトウェアの脆弱性を悪用した攻撃が増加すると考えており，ソフトウェアに脆弱性が見つかったとしても，容易に感染しない防御機能を備えていることや，脆弱性に対して対策できる IoT 機器向けのセキュリティ機能が必要不可欠である．

そこで，本研究では，脆弱性のあるアプリケーションを保護することを目的にして，Linux カーネルやアプリケーションを改変することなく，発行できるシステムコールを制限する Seccomp の Berkeley Packet Filter（BPF）をアプリケーションに適用する機能を

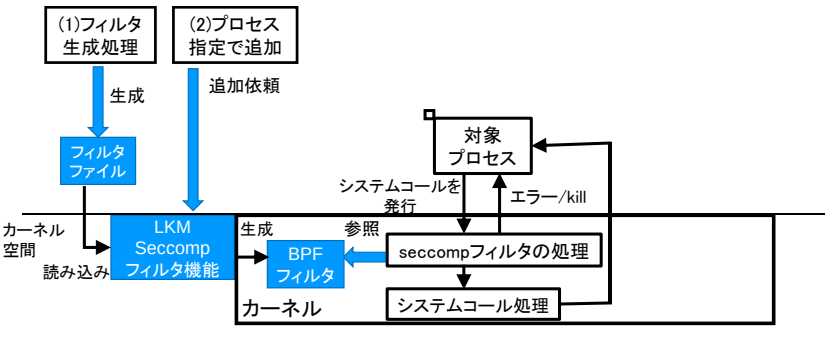

図 5　Seccomp フィルタによるアクセス制御の実現方式

Loadable Kernel Module（LKM）に実現し，アクセス制御する手法を提案した（図5）．また，保護対象のアプリケーションを動作させ，Seccomp フィルタを生成する手法では，アプリケーションが発行するシステムコールをすべて網羅できないことを示し，保護対象のアプリケーションの実行ファイルを静的解析する手法と併用することで，システムコールの網羅率を向上させたSeccomp フィルタを生成する手法を提案した．

提案手法を適用したアプリケーションに対して，Seccomp フィルタのシステムコール網羅率を評価し，フィルタ生成手法の有効性を示した．また，いくつかの脆弱性攻撃を防止できることを示し，攻撃に使用される可能性の高いシステムコールを提案手法により，制限できることを示した．

研究テーマ F： Linux の LSM に対応した独自のセキュア OS の設計

Linux には，LSM に対応した強制アクセス制御を採用したセキュア OS がいくつか実現されている．IoT 機器への攻撃に対して，これらのセキュア OS（SELinux，AppArmor，Smack，TOMOYO Linux）の有効性を評価した．

また，IoT 機器向けの LSM 対応の独自のセキュア OS の検討を行っている．現在，機械学習を活用したものを検討しているが，カーネル内での実装においては課題が多いため，機械学習を用いないものも含めて，今後検討する予定である．

3. 今後の展開

本研究では，IoT 機器のソフトウェアの課題を大規模調査し，またベンダへのインタビューを通して，セキュリティ上の課題が生じる要因や，IoT 機器のサプライチェーン上の問題を調査した．IoT 機器のソフトウェアの課題の調査引き続き調査を継続し，IoT 機器のセキュリティ機能の活用状況とその阻害要因の調査を継続する．また，課題解決のために，IoT 機器ベンダへのインタビューなどにより，調査を継続する．

次に，本研究の目的の IoT 機器のセキュリティ上の問題を解決する基盤ソフトウェアについては，リモートログインされた場合の IoT マルウェアの動作を分析に，アクセス制御により，感染を防ぐことはある程度できている．今後は，IoT マルウェアが悪用する攻撃手段についての分析と対策を進める．また，引き続き，IoT 機器ベンダとの協力することにより，実際に活用できるセキュリティ機能の実装形態などを明らかにする．

4. 自己評価

IoT 機器ファームウェアの分析においては，多くのファームウェアを分析でき，IoT 機器のソフトウェアの課題を明確化できた．予想以上に，IoT 機器でのセキュリティ機能の活用が進んでいない状況があるため，今後も調査を継続したい．また，ファームウェアの大規模分析について，数回講演する機会をいただいたが，予想以上に興味を持ってくださる方がいたので，このような分析の意義を再認識した．

IoT マルウェアの活動分析については，リモートログインされた後の分析しかできていないため，ソフトウェアに脆弱性があったとしても，攻撃を防止できる機能の実現に向けた研究を継続する必要がある．

IoT マルウェアの感染活動に着目したシステムコールレベルのアクセス制御は，攻撃防止の効果は確認できたものの，実際の IoT 機器の動作において，誤検知による正常動作への影響は評価できていないため，実際の IoT 機器を想定した環境をファームウェア等で作成し，評価を進め，実際の機器での適用可能性を評価する必要がある．

Seccomp フィルタを用いたアクセス制御手法は，フィルタの作成方法が，実際にアプリケーションを動作させたログを元にした方法だけであり，実行されなかった機能がある場合に，正常処理を防止してしまう可能性がある．このため，静的解析により，実行される得るシステムコールを実行ファイルから検出する手法を研究開発している．実行ログによる方法と静的解析による手法を併用することで，誤検知を無くし，IoT マルウェアの影響を防止できる機能として活用できるように研究を進める．

研究成果の科学技術及び社会・経済への波及効果について，研究成果の科学技術での波及効果については，難関国際会議への投稿できるレベルに対策技術の研究を進め，できるだけ，早期に発表できるように進める．また，社会への波及効果については，IoT 機器ベンダと意見交換など行える環境にあるため，IoT 機器のセキュリティ上の課題を進められるように，より多くの企業と意見交換などを行い，研究成果が活用されるような方向性を見いだしたい．また，IoT 機器のファームウェア等の調査から，IoT 機器のサプライチェーン上の課題が明らかになったため，本研究の成果を広く周知することで，IoT 機器のセキュリティ上の問題を改善する方向に様々な関係者に働きかけるとともに，開発現場における課題解決を支援するようなソフトウェア分析手法など，新たに検討を進めていきたい．

5. 主な研究成果リスト

(1)代表的な論文(原著論文)発表

研究期間累積件数:27件

1. 山内利宏，吉元亮太，吉岡克成，IoT マルウェアの感染処理に着目したアクセス制御手法の提案，コンピュータセキュリティシンポジウム 2022 (CSS2022)論文集，2022，Vol.2022，160-167
IoT マルウェア活動は活発に継続しているものの，IoT 機器のソフトウェアの最新化は進んでおらず，セキュリティ機能の活用が進んでいない状況が続いている．また，IoT 機器のセキュリティを根本的に向上させるためには，OS レベルの対策が重要である．そこで，本研究では，IoT マルウェアの感染時に実行されるコマンドとシステムコールをロギングする機構を研究開発し，IoT マルウェアの感染活動を詳細に分析可能にした．また，分析結果から，IoT マルウェアの感染動作を明らかにし，正常な処理に影響を与えずに，効果的にシステムコール実行を防止する手法を提案した．提案手法をLinuxベースのIoT機器に組み込みしやすいLKMとして実装し，実際のIoTマルウェアによる攻撃実験を行った．評価の結果，IoT マルウェアの感染動作をすべて防ぐことができたことを示した．
2. 白石周碁，吉元亮太，塩治榮太朗，秋山満昭，山内利宏，ソフトウェア差分に着目したIoT機器サプライチェーンセキュリティ上の課題発見と大規模実態調査，電子情報通信学会技術研究報告，2022，Vol.121，No.410，105-110
IoT 機器の普及に伴い，IoT 機器を標的とした攻撃によるセキュリティインシデントの発生が

増加している. しかし, 既存の IoT 機器に関する包括的なセキュリティ調査は少ない. 本研究では, IoT 開発ベンダにインタビュー調査を実施し, ソフトウェアアップデートやセキュリティパッチの作成や適用について, セキュリティを阻害するサプライチェーン上の制約を明らかにした. また, バージョン番号を変更せずに暗黙的にパッチが適用されることがあるため, バージョン番号に基づく脆弱性評価では誤検知が発生することを大規模なファームウェア分析によって定量的に示した. 最後に, IoT 機器のセキュアな製造を促進するための取り組みとして, ソフトウェアコンポーネントの透明性と脆弱性評価, および IoT サプライチェーンの課題について議論した.
3. 白石 周碁, 福本 淳文, 吉元 亮太, 塩治 榮太朗, 秋山 満昭, 山内 利宏, ソフトウェア解析とベンダインタビューによる IoT 機器のセキュリティに関する大規模実態調査, コンピュータセキュリティシンポジウム 2020 (CSS2020) 論文集, 2020, 875-882
IoT 機器を標的とした攻撃による被害が深刻化と, さらなる攻撃の高度化が予想される. このため, 我々は IoT 機器のファームウェア解析に基づいたファームウェアの分析調査を大規模かつ体系的に実施した. 調査により, IoT 機器で利用されるセキュリティ機構の利用率が低く, 古いバージョンのソフトウェアが使用されている実態を明らかにした. さらに, ファームウェアのバージョンアップ時のソフトウェアのアップデートがあまり行われない状況を明らかにした. これにより, 体系的な調査を実施するための新たな調査手法を確立した. また, 調査によって判明したセキュリティ上の問題点の要因を明らかにするために IoT 機器のベンダにインタビューを実施し, 開発現場でのセキュリティ機能の適用と, ソフトウェアバージョンの課題を示した.

(2)特許出願

研究期間全出願件数: 1 件(特許公開前のものも含む)

(3)その他の成果(主要な学会発表、受賞、著作物、プレスリリース等)

1. CSS2020 優秀論文賞, 白石周碁, 福本淳文, 吉元亮太, 塩治榮太朗, 秋山満昭, 山内利宏, 情報処理学会コンピュータセキュリティシンポジウム 2020(CSS2020)プログラム委員会, 2020 年 10 月 28 日
2. ICSS 2021 年度研究賞, 白石周碁, 吉元亮太, 塩治榮太朗, 秋山満昭, 山内利宏, 電子情報通信学会 情報通信システムセキュリティ(ICSS)研究専門委員会, 2022 年 6 月 23 日
3. CSS2022 優秀論文賞, 山内利宏, 吉元亮太, 吉岡克成, 情報処理学会コンピュータセキュリティシンポジウム 2022(CSS2022)プログラム委員会, 2022 年 10 月 27 日
4. 山内利宏, 吉元亮太, LKM を介した Seccomp フィルタの適用によるアクセス制御手法の提案と評価, 情報処理学会第 93 回 CSEC・第 53 回 IOT 合同研究発表会, 情報処理学会研究報告, vol.2021-CSEC-93, no.12, pp.1-6 (2021).
5. 原田真ノ介, 吉元亮太, 塩治榮太朗, 秋山満昭, 山内利宏, ファームウェア解析に基づいた IoT 機器上で自動実行されるプログラムの実態調査, 電子情報通信学会 第 62 回情報通信システムセキュリティ研究会 (ICSS), 電子情報通信学会技術研究報告, vol.122, no.422, ICSS2022-59, pp.67-72 (2023).