J. Plasma Fusion Res. Vol.97, No.4 (2021) 238-239

研究速報

電力変動監視によるマルウェア検出方法

Malware Detection Method by Power Fluctuation Monitoring

田中　卓，力石浩孝[1)]，田中恵子，細見令香[2)]，三浦啓輔
TANAKA Taku, CHIKARAISHI Hirotaka[1)], TANAKA Keiko, HOSOMI Reika[2)] and MIURA Keisuke
京都大学，[1)]核融合科学研究所，[2)]京都工芸繊維大学

（原稿受付：2020年12月16日／原稿受理：2021年２月９日）

核融合炉などの大規模プラントでは，制御システムのセキュリティ確保が重要な研究課題である．この課題に対して従来の研究では，主に市販の情報デバイスを標的にした既知のマルウェアをソフトウェアで検知し，駆除を試みるのが一般的である．本研究ではサーバー攻撃の検知を侵入したマルウェア自身が使用する消費電力の監視により行い，その電力変動の有意差を持って早期検知を試みるものである．

Keywords:
fusion plant, control system, security, malware detection, power monitor

1．はじめに

Internet に接続された機器（Internet of Things，IoT）や大規模プラントの制御など，近年，コンピュータ制御はその対象を多岐に広げており，核融合プラントもその中に含まれる．IoT のセキュリティ対策の重要性について言及している研究には，柏山[1]，大野[2]などがあり，江本[3]では，大規模プラント制御系の統合化が進むにつれて，セキュリティ強化が必要となることが指摘されている．

従来の制御システムに用いられているマルウェア検出ソフトは，制御システムと同一のOS上で動作している．マルウェア等により OS 自体に不具合が発生した場合，それに付随してマルウェア検出ソフトの動作に問題が生じる可能性が考えられる．したがって，制御システムから物理的に分離したマルウェア検出手法を考える必要がある．核融合プラントなどの制御システムでは，定周期でプログラムが稼働しており，正常動作時には制御周期と同期した電力変動が観測される性質がある．この電力変動に着目すると，ソフトウェアの一種であるマルウェアも最初に兆候が現れるのは消費電力であると推察でき，定周期で稼働するプログラムとマルウェアの電力変動の有意差をモニタリングすることで異常動作を従来のセキュリティソフトウェアよりも初期の段階で検知し，制御システムを早期に安全側シーケンスに入れることが可能と考えられる．また，マルウェア毎の電力変動の特徴を把握することで，異常波形の再現時にその特徴からマルウェア種別を判定し，早期に的確な対策を講じることも可能になる．さらに制御システムとは物理的に分離したマルウェア検出のモニター系を用いることで，マルウェア検出の仕組みが制御システムの動作に悪影響を与える可能性はほぼなく，広範囲の制御システムに適用可能である．

2．マルウェア検出のモニター系の要件

前項で提案した原理に基づくマルウェア検出のモニター系の要件として，モニター系が制御システムから物理的に分離され，制御システム全体の機能低下を誘発しないこと，また，マルウェア攻撃そのものに対して影響を受けず，電力変動を計測できることが挙げられる．

3．要件を満たすプロトタイプの機能と実装

前項の要件を満たすプロトタイプを製作した．**図１**にプロトタイプの構成図を示す．図において破線より左半分は対象とする制御システムであり，右半分がマルウェア検出のモニター系である．(a)の ATX はマザーボード用電源，CPU は CPU 用電源，HDD はハードディスク（HDD）用電源であり，その右側に各電圧を示す．(b)の埋め込みセンサにより，これら８本すべての電流を計測し，(d)の外付けセンサでは CPU12V のみを計測した．

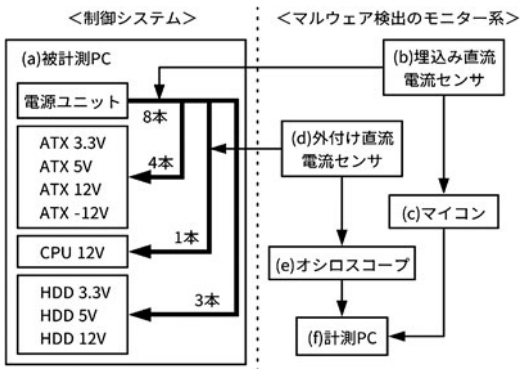

図１　プロトタイプの構成図．

Kyoto University, KYOTO 606-8501, Japan
corresponding author's e-mail: tanaka.taku.5w@kyoto-u.ac.jp

4．プロトタイプを使用した予備実験

前項のプロトタイプを用いて予備実験を行った．

実験１として，OS 及び付随ソフトのみが動作している状態における(a)の電流値を得るために，(b)のセンサ値を100ms 間隔で3000回（約５分間）(c)で取得し，(f)で電流値に変換した．想定される負荷の例を**図2**-(A)に模式的に示す．この実験１では，すべての電流値に大きな変動は見られなかった．

実験２として，(a)に定期的な負荷をかけた場合の電流値を調べるために，実験１の約15分後，(a)で１～10000の間の素数を求めるプログラム A（処理時間約10秒）を通常ソフトウェアに見立てて実行しながら，実験１と同じ計測を行った．プログラム A は，センサ値の取得開始約30秒後から約１分毎に５回実行した．想定される負荷の例を**図3**-(A)に模式的に示す．

実験３として，実験２の(a)に，さらに定期的な負荷をかけた場合の電流値を調べるために，実験２の約15分後，実験２の追加負荷として，１～30000の間の素数を求めるプログラム B（処理時間約40秒）をマルウェアに見立てて実行しながら，実験１と同じ計測を行った．プログラム B は，センサ値の取得開始約10秒後から約１分毎に５回実行した．想定される負荷を**図3**-(E)に模式的に示す．

実験２と実験３の結果，ともに５回のプログラム実行時において，実験２では ATX5V，ATX12V，CPU12V の電流値が，実験３では ATX5V，CPU12V の電流値が上昇していることが確認された．特に CPU12V の変化は顕著であった．これらの最初の１分間の電流波形を**図3**-(B)～(D)，(F)～(H)に示す．なお，他の電流波形については，いずれの実験においても大きな変化は見られなかった．

5．考察

本論文では前提条件として，制御プログラムは定期的に同じ動作を行い，人間や他のコンピュータの関与，外的要因の影響は受けないことを想定とした．実験１では電流波形に大きな変動は見られなかったことから，外的要因のうち，対象制御システムの OS の動作による影響は少ないと考えられる．実験２においては，通常プログラム処理での電力変動が現れ，実験３ではマルウェア自身の電力変動が CPU12V において明瞭に検出された．ATX12V 及び ATX5V においては大きな違いは認められなかった．これらの結果から，特に CPU12V をモニターすることにより，本論文で提案する検出方法が適用可能であると考える．この電力変動は外付けセンサである(d)でも同様に検知されている．これから，配線への埋め込みが不要である外付けセンサにより既存装置への後付でのマルウェア検知も可能であると考える．今後の課題として，機械学習等を用いて，通常運転時の電力変動パターンの学習を試み，余地的な検知速度の向上，電力変動監視によるマルウェア種別判定，攻撃手法別のシステム防御方法の選択決定に至るシーケンスの改良等を予定している．

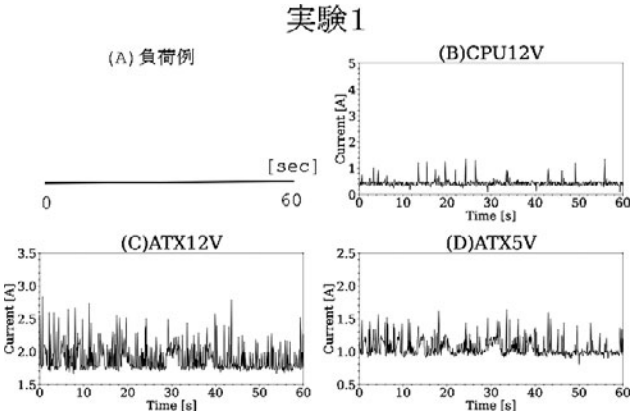

図２　実験１における各部の電流波形．
(A)は電流波形模式図，(B)～(D)は電流の実測波形．

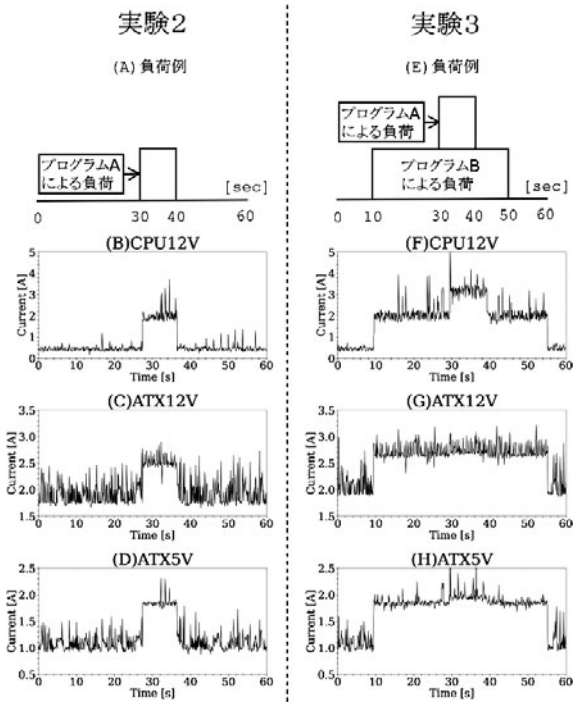

図３　実験２，３各部の電流波形．
(A)，(E)は電流波形模式図，(B)～(D)，(F)～(H)は電流の実測波形．

謝　辞

本研究の一部は NIFS 共同研究 NIFS20KERA017として実施しています．終始適切な助言を賜った岡部寿男先生，関係各位にお礼申し上げます．

参 考 文 献

［１］柏山正守 他：電気学会論文誌 D, IEEJ Trans. Industry Appl. **140**, 15 (2020).
［２］大野浩之：科学研究費補助金 基盤研究(C)課題番号 15K00119 研究成果報告書（2019）．
［３］江本雅彦：「LHD コンピューターシステムの統合化の研究」博士（学術）学位論文 総合研究大学院大学（2002）．