様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　２ 年　 ６ 月 １９ 日現在

機関番号：１２１０２
研究種目：挑戦的萌芽研究
研究期間：2016～2019
課題番号：１６Ｋ１２４１０

研究課題名（和文）多重世界モデルに基づきプライバシを保護するオペレーティングシステム

研究課題名（英文）An operating system forprotecting privacy basedon a parallel world model

研究代表者
新城　靖（Shinjo, Yasushi）

筑波大学・システム情報系・准教授

研究者番号：００２５３９４８

交付決定額（研究期間全体）：（直接経費）　　2,700,000円

研究成果の概要（和文）：　本研究では、多重世界モデルを用いて、個人情報を保護する。世界とは、プロセスやファイルを入れる箱であり、融合、差分表示といった操作が容易に行える。本研究は、Linux においてコンテナ技術 Docker を用いて多重世界モデルを実現する。２つの世界の中で「双子の Web ブラウザ」を実行し、作成されるファイルや通信を観測する。その結果、そこから多数の利用者追跡に使われる情報を検出できた。
　また、Webサービスごとに環境(世界)を隔離するブラウザを実現した。このブラウザでは、利用者があるWebサービスで取得した機密性のあるファイルを誤って別のサービスに発信することを防ぐ。

研究成果の学術的意義や社会的意義
　現在の Web では、利用者は Web ブラウジングをするだけで、様々な個人識別情報をサーバに発信している。本研究の結果、そのような個人識別情報を簡単に見つけることが可能になった。これにより利用者は、サーバによる追跡を恐れることなく安心して Web ブラウジングを行なうことができるようになる。
　従来、利用者がある Web サービスからダウンロードしたデータを別の Web サービスに誤ってアップロードすることを防ぐには、複数の PC や仮想計算機を利用する方法があったが、利用者の間違いを防ぐことができなかった。本研究の成果を利用すれば、そのような利用者の間違いを完全に防ぐことができる。

研究成果の概要（英文）：In this research, we protect private information using a parallel world model. In this model, a world is a container of processes and files, and it is easy to create a world, merge two worlds, and show differences between two worlds. We have implemented worlds using the Docker container technology in Linux. We create two twin worlds running two twin browsers, and compare the created files and communication messages from the worlds. We were able to find many identifiers for user tracking in these files and messages. We have also implemented a web browser that isolates environments for individual Web services. This browser prevents a user from uploading secret files of a Web service to another Web service.

研究分野：情報工学

キーワード：情報工学　計算機システム　オペレーティングシステム　仮想化技術　個人情報保護

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

現在の PC（Personal Computer）は、非常に複雑である。利用者は、PC で Web ブラウザやワードプロセッサを利用しただけで、個人情報を含むファイルが勝手に作成されたり、個人情報を含む通信が勝手に行われることがある。利用者が悪意を持つプログラム(malware)を実行した場合、利用者は自らのプライバシを保護する術を持たない。

Tails Linux, Whonix, Nymix といった、匿名性を保ったままネットワーク通信を可能にする OS が盛んに研究されている。しかしこれらの OS は、内部告発者を保護することを最優先に設計されているため、カジュアル利用者(コンピュータに不慣れな利用者)には到底扱えるものではない。

申請者は、多重世界モデルという、OS レベルの仮想化技術を研究してきた。世界とは、コンテナのように、プロセスやファイルを入れる箱(実行環境)である。世界はコンテナとは異なり、融合、差分表示、差分編集といった操作が容易に行える。この研究成果を利用することで、カジュアル利用者でも簡単に使える、プライバシを保護する OS が実現できるのではないかという着想を得た。

２．研究の目的

研究期間内に本研究では、次のことを実現する。

- Linux において、多重世界モデルを実現する。
- 多重世界モデルで、「双子の研究」を行う。双子の研究とは、氏名や生年月日等の個人情報をわずかに変化させた類似の実行環境でプログラムを動作させ、その差を調べることである。これにより、プライバシ情報を含むファイルや通信を特定する(図 1)。

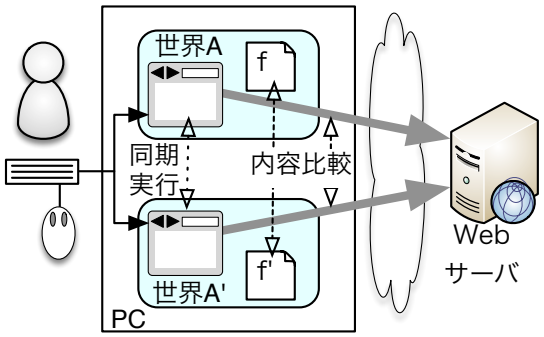

図 1　多重世界モデルを用いた双子の研究による利用者識別子の調査

- 多重世界モデルで複数の Web サービスのアクセスを簡単に管理できるようにする。ここで Web サービスとは、URL で区別される Web サイトの集合である。本研究では利用者の操作に応じて自動的に世界(実行環境)を切り替える機能を実現する。これにより従来の匿名化 OS の利便性を大きく改善し、利用者が誤って別のサービスにデータを漏洩させることを防ぐ (図 2)。

３．研究の方法

本研究では、まず Linux においてコンテナ技術の１つ Docker を用いて多重世界モデルを実装した。双子の研究を行なうために作成する２つのコンテナを、双子の環境と呼ぶ。本研究では、双子の環境に、以下の機能を実現した。

- 双子の環境で保存されるファイルをすべて記録する。Docker において、ファイルシステムとして overlayfs (overlay filesystem) を利用することで実現した。
- 双子の環境が行なうネットワーク通信内容をすべて保存する。Man-In-The-Middle Proxy を用いて実現した。

双子の各環境から得られたファイルの内容や通信内容を比較することで、双子の研究を行なう。比較においては、よく現れるファイルについて、ファイルの種別ごとに前処理を行う。たとえば、Berkeley DB や LevelDB のようなバイナリ形式のファイルをテキスト化するプログラムを作成した。HTML や JavaScript では単語単位の差分を検出するために改行を挿入するなどして標準化を行なった。

こうして生成されたファイルや通信の内容を比較すると、日付や擬似乱数に起因する差分が大量に含まれていることがわかった。このような大量の差分は、ノイズであり、本来見つけたい差分を見つけにくくする。そこで本研究では、各環境で日付や乱数を同一にすることで、ノイズ

を削減した。

本研究では、双子の研究を容易にするために、双子の環境で動作する双子のブラウザを実装した。双子のブラウザとは、ベースとなる Web ブラウザで新たに URL を開いたり、リンクを選択すると、双子の環境内で動作しているブラウザが同じ動作を行なうものである。本研究では、双子のブラウザを Firefox の拡張機能、および、Selenium を用いて実装した。

本研究では、双子のブラウザとは別に、サービスごとに隔離された環境(世界)をもつ Web ブラウザを実装した。このブラウザでは、ブラウジングに伴い、隔離されたファイルシステムを持つ環境が自動的に切り替わる。これにより、利用者があるサービスで取得したファイルを誤って別のサービスに送信することを防ぐ事ができる。この環境(世界)もまた双子の環境と同様に、Docker を用いてコンテナとして実装した。各コンテナでは、協調動作する Web ブラウザを実行する。これにより、利用者複数のブラウザを 1 つのブラウザを使っているかのように扱うことができる。

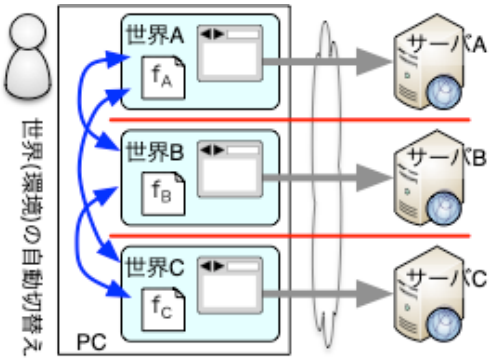

図 2 多重世界モデルにおける Web サービスごと隔離された環境の自動的な切り替え

4. 研究成果

実現した双子の環境で、双子のブラウザやその他のアプリケーションを実行し、生成されるファイルの差分を調査した。その結果、提案手法により利用者の識別子がどのようなファイルに保存されているかを簡単に発見することができた。たとえば、Firefox では、単純なサイトを訪問するだけで、30 個のファイルが生成される。このうち、差分が見られないものが 26 個あり、わずか 4 個ファイルの 13 行にのみ違いが見られた。

Firefox の他に、同じく Web ブラウザ Google Chrome、メールリーダ Thunderbird、オフィスツール LibreOffice についても調査を行なった。その結果、大量にファイルが更新されたとしても、提案手法により、差分がないファイルを排除することができ、解析する範囲を狭めることができることが可能となった。

ファイルの内容に続き、実現した双子の環境で、双子のブラウザやその他のアプリケーションを実行し、通信内容の差分を調査した。その結果、HTTP の要求メッセージや応答メッセージの中に、利用者を追跡するための識別子が埋め込まれていることを簡単に発見することができた。具体的には、Web ブラウザではよく知られている cookie: ヘッダの他に、If-None-Match: ヘッダ, X-*-Request-Id: ヘッダ、および本文中の meta name や nonce に識別子らしい情報が埋め込まれていることがわかった。メールリーダでも、Web ブラウザと同様に HTTP による通信の差分が多数観測された。

サービスごとに隔離された環境(世界)を持つ Web ブラウザでは、機密性がある情報を扱いたい職場環境、および、一般的な検索を行ないたい環境、SNS を利用する環境の 3 つの環境を用いて実験を行なった。その結果、それぞれの環境の切り替えが 0.1 秒程度であり、インターネットへのアクセス時刻と比較して無視できることがわかった。また機密性がある情報をダウンロードした職場環境のファイルを誤って SNS に投稿することができないことを確認した。

本研究の結果、多重世界モデルに基づき「双子の研究」が容易になることが示された。当初は、生年月日や氏名等のデータを僅かに変化させることで差分を観測するつもりであったが、それを行なうまでもなく、Web サーバ側が利用者を追跡するための識別子を個々の応答メッセージに含めていることが分かった。Web ブラウザには、利用者の追跡を防止するための拡張機能が多数開発されている。本研究の成果を用いれば、そのような拡張機能の効果を検証することが容易になるほか、拡張機能の開発者にとっても有用性が高いことがわかった。今後は、双子のブラウザだけでなく、様々なアプリケーションを双子の環境で動作させ、個人識別情報を削除するツールの開発を支援していきたい。

サービスごとに隔離された環境(世界)を持つ Web ブラウザでは、利用者が Web サーバからダウンロードしたセンシティブなデータを誤って別のサーバに送信することを防ぐことができた。これにより、利用者はセンシティブな情報の漏洩を心配することなく、Web ブラウザを利用することができるようになった。現在は、コンテナ内で独立した Web ブラウザを実行している。この方法では、利用者は独立した複数のブラウザを利用していることを意識させられることがある。たとえば、ブックマークや拡張機能は環境ごとに独立している。今後は、ブラウザが直接環境を操作できるように改良して行きたい。これにより、利便性が大きく改善できると期待される。

５．主な発表論文等

〔雑誌論文〕　計14件（うち査読付論文　3件／うち国際共著　0件／うちオープンアクセス　12件）

１．著者名 Wu Zhaoxin、Shinjo Yasushi	４．巻 －
２．論文標題 Improving Web Browsing Experience with Personalized Edge Computing	５．発行年 2019年
３．雑誌名 The 4th International Workshop on Multi-access Edge Computing and Networking (MECN-2019)	６．最初と最後の頁 －
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/IUCC/DSCI/SmartCNS.2019.00149	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Yang Chung-Fan、Shinjo Yasushi	４．巻 －
２．論文標題 Obtaining hard real-time performance and rich Linux features in a compounded real-time operating system by a partitioning hypervisor	５．発行年 2020年
３．雑誌名 The 16th ACM International Conference on Virtual Execution Environments	６．最初と最後の頁 59-72
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3381052.3381323	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 河野 匠, 新城 靖, 中村 公洋, 三村 賢次郎	４．巻 －
２．論文標題 ユーザ間データ共有を支援する分散型WebブラウザのWebRTCによる実装	５．発行年 2019年
３．雑誌名 情報処理学会第31回コンピュータシステム・シンポジウム	６．最初と最後の頁 62-75
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 加藤 風芽, 新城 靖	４．巻 －
２．論文標題 機密実行環境を利用した自己破壊・出現データの実装方式の提案	５．発行年 2019年
３．雑誌名 情報処理学会第31回コンピュータシステム・シンポジウムポスターセッション	６．最初と最後の頁 1-2
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 中村 公洋，新城 靖	4．巻 —
2．論文標題 分散台帳技術を用いた分散ファイルシステムの構想	5．発行年 2019年
3．雑誌名 情報処理学会第31回コンピュータシステム・シンポジウムポスターセッション	6．最初と最後の頁 1-2
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 —

1．著者名 張 世申，新城 靖，三村 賢次郎	4．巻 -
2．論文標題 個人情報及び個人識別子を含むファイルと通信を検出するための双子の環境	5．発行年 2018年
3．雑誌名 情報処理学会第30回コンピュータシステム・シンポジウム(ComSys2018)	6．最初と最後の頁 29-36
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 —

1．著者名 三村 賢次郎，新城 靖，張 世申	4．巻 -
2．論文標題 コンテナ技術を用いたサービスごとに隔離された環境を持つWebブラウザ	5．発行年 2018年
3．雑誌名 情報処理学会第30回コンピュータシステム・シンポジウム(ComSys2018)	6．最初と最後の頁 37-46
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 —

1．著者名 田嶋 孝好，新城 靖	4．巻 -
2．論文標題 アスペクト指向プログラミングを用いた特化によるプロセス間通信の高速化の提案	5．発行年 2017年
3．雑誌名 情報処理学会第29回コンピュータシステム・シンポジウム	6．最初と最後の頁 58-68
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 —

1．著者名 田中 創樹，新城 靖	4．巻 -
2．論文標題 ノード間通信が可能なボランティアコンピューティング	5．発行年 2017年
3．雑誌名 情報処理学会第29回コンピュータシステム・シンポジウム	6．最初と最後の頁 96-104
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 三村 賢次郎，新城靖，張 世申	4．巻 -
2．論文標題 Web サービスごとに隔離されたブラウジング環境の提案	5．発行年 2017年
3．雑誌名 情報処理学会第29回コンピュータシステム・シンポジウムポスターセッション	6．最初と最後の頁 1-2
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 張 世申，新城 靖，三村 賢次郎	4．巻 -
2．論文標題 個人情報を含むファイルと通信を検出するための双子の環境の提案	5．発行年 2017年
3．雑誌名 情報処理学会第29回コンピュータシステム・シンポジウムポスターセッション	6．最初と最後の頁 1-2
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 細田 将大，中井 央，佐藤 聡，新城 靖	4．巻 10
2．論文標題 拡張可能な構文解析器生成 系による構文エラー処理機能の実装	5．発行年 2017年
3．雑誌名 情報処理学会論文誌:プログラミング	6．最初と最後の頁 1-13
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 山本 諒裕, 新城靖, Oscar Fernando Garcia Alvarado	４．巻 －
２．論文標題 Reverse VMRPCによるゲストOSの操作	５．発行年 2016年
３．雑誌名 情報処理学会第28回コンピュータシステム・シ ンポジウム	６．最初と最後の頁 60-71
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 田嶋 孝好, 新城 靖, 佐藤聡, 中井央	４．巻 －
２．論文標題 AOP を用いた特化によるプロ セス間通信の高速化の提案	５．発行年 2016年
３．雑誌名 情報処理学会第28回コンピュータシステム・シ ンポジウム ポスターセッション	６．最初と最後の頁 1-2
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計0件

〔図書〕　計0件

〔産業財産権〕

〔その他〕

筑波大学コンピュータサイエンス専攻ソフトウェア研究室
http://www.softlab.cs.tsukuba.ac.jp/

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考