[2021]九州大学情報統括本部年報 : 2021年度

出版情報：九州大学情報統括本部年報. 2021, pp.1-, 2022-10-01. Information Infrastructure Initiative, Kyushu University
バージョン：
権利関係：

第 5 章　情報システムセキュリティ研究部門

5.1 スタッフ一覧

職 名	氏 名	研究キーワード
教授	小出 洋	サイバーセキュリティ、プログラミング、ネットワーク、並列分散処理、動的記憶領域管理

5.2 研究事例紹介

5.2.1「情報システムに対するサイバーセキュリティ」

1. はじめに

本稿では、情報システムセキュリティ研究部門において主に 2021 年度に行った研究の一部として、商用クラウドを用いて演習等に利用できる拡張性を持つサイバーレンジを簡単に構築できる KAKOI に関する研究（第 2 小節）、本研究部門で集中的に研究を行っている移動標的防御（Moving Targert Defense; MTD）の研究で 2021 年度に実施した研究の事例として、バイナリファイルのシステムコールに対する移動標的防御の適用に関する研究（第 3 小節）、また情報システムに対する標的型攻撃に代表される脅威がどのような挙動をとるのかシミュレーションする脅威トレースを実際の情報システムからのデジタル来歴を用いて改善する研究（第 4 小節）を紹介する。

2. 商用クラウドを用いて拡張性を持つサイバーレンジを簡単に構築するツール KAKOI の実装

研究の目的はセキュリティ演習を実施するための演習環境であるサイバーレンジの構築、管理の負担を軽減することである。サイバー攻撃の脅威が増大する一方、それらに対応できる人材は不足している。人材育成のために演習を実施することが非常に有効であるが、演習のための環境の構築や管理、演習シナリオの作成など、専門的な知識が必要となり、演習の実施は負担が大きい。

この目的のため、サイバーレンジ運用のための構成管理ツールである KAKOI を開発することで前述した負担を軽減した。サイバーレンジは主に演習ネットワークと演習サーバから構成される。演習ネットワークは安全に演習内容を遂行できるように外部から隔離したネットワークとして構築しなければならない。また、演習サーバは講義する側が用意するシナリオに応じて柔軟にソフトウェア設定やハードウェア設定を変更できる必要がある。これらの構成要素をパブリッククラウドで利用することで柔軟な管理を可能にし、環境の拡張性や再現性を向上させた。また、KAKOI はサイバーレンジの設計を Yaml 形式のファイルで管理し、ほとんどの作業を自動化した。さらに KAKOI はサイバーレンジの設計をテンプレート化することで設計にかかる負担と作業を削減した。

KAKOI を用いて構築した評価環境に対して、接続性や環境に反映される設定の正確性、サイバーレンジ構築に置ける利便性などについて評価した。接続性の評価では、評価環境に対して安全に接続できること、既定の手段以外では評価環境に接続できないこと、評価環境内部から外部ネットワークに接続できないことを確認した。さらに、利便性の評価では、KAKOI を使用した場合にサイバーレンジを構築するための手順が既存の手法に対して大きく削減できていることを確認した[2a]。

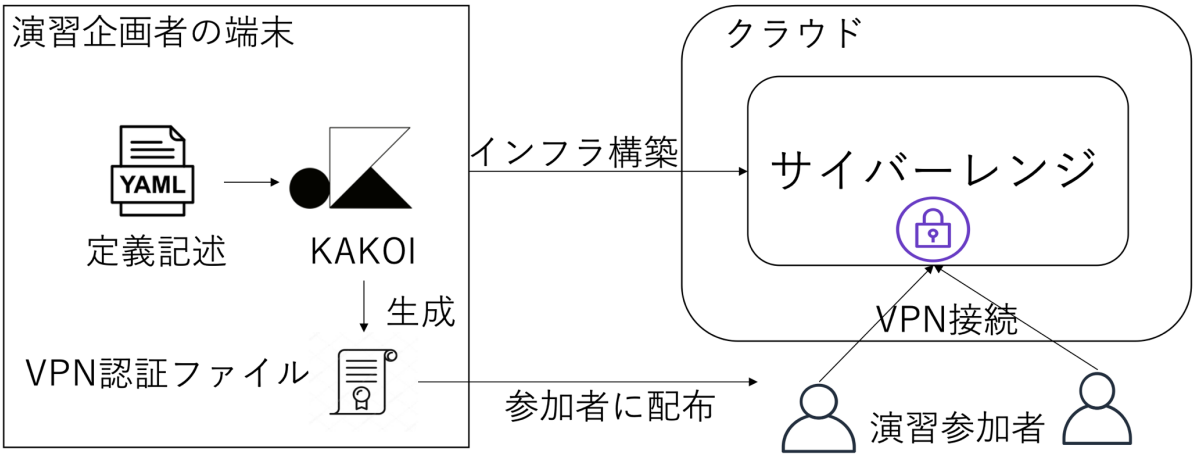

図 2: KAKOI の概要。

[2a] Tomoya Terashima and Masahiro Nakayama and Teruaki Yokoyama and Hiroshi Koide: KAKOI: A New Tool to Make Simple and Secure Build Cyber Ranges Using Public Cloud, 2021 Ninth International Symposium on Computing and Networking Workshops (CANDARW) (Nov. 2021).

3. バイナリファイルへのシステムコールに対する移動標的防御(Moving Target Defense; MTD)の適用

研究の目的は、コードインジェクション攻撃に対する防御を提供することである。システムが同攻撃に対して脆弱である場合、攻撃者によって用意された任意のコードをシステム上で実行される恐れがある。そのため、この脆弱性は深刻であり、対策は必須である。

そのため本研究では、コードインジェクション攻撃に対する防御手法として、システムコールの番号と機能の対応付けをランダム化する手法を提案した（図 3）[3a]。システムコールは、ユーザアプリケーションがシステムリソースにアクセスする唯一の方法であるため、この手法によりインジェクションされたプログラムが実行可能な処理、およびアクセス可能な資源を大幅に制限することが可能である。既存のシステムコールランダム化に関する研究として、プログラムをメモリにロードする前に 1 度だけランダム化を行うものが存在する。しかし、このような手法は、ランダム化に関する情報が攻撃者に漏洩した場合に有効性が著しく低下する。本研究では、ランダム化情報の漏洩に対抗するため、実行時に複数回継続して再ランダム化を実行することで、システムコールランダム化を強化した。また本研究が提案する手法は、コンパイル済みのバイナリを直接書き換えることで適用することができるため、既存の多くのプログラムに適用可能である。

提案手法の評価を行うため、2 つの実験を行った。1 つ目の実験では、脆弱性を含むプログラムに提案した手法を適用し、実際にコードインジェクション攻撃を防ぐことを確認した。2 つ目の実験では、手法を適用したことにより発生するオーバーヘッドを計測し、その形式化を行った。今後の課題としては、このオーバーヘッドを削減することが挙げられる。

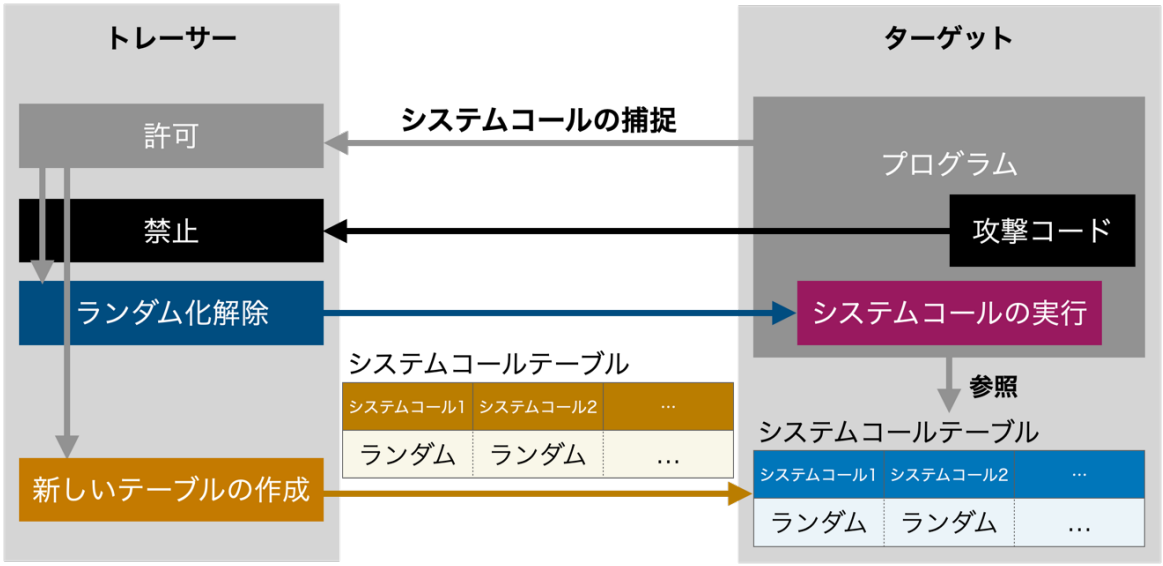

図 3: 提案するシステムコールレベルの MTD。

[3a] Takeshi Masumoto and Wai Kyi Kyi Oo and Hiroshi Koide: MTD: Run-time System Call Mapping Randomization, Proc. 2021 International Workshop on Cyber Security}, pp. 257-263, (Act.2021).

4. 脅威トレースの実環境への適用

目的は高度標的型攻撃をはじめとするサイバー攻撃のローカルネットワーク上での振る舞いをシミュレートするソフトウェアを構築することである[4c]。そのための既存の脅威トレース[4a,4b]を拡張し、実際のネットワークから情報を得て、その情報を基にシミュレートするようにすることで、より現実に近いシミュレーションを実現できるようにする。ネットワーク管理者はこの拡張された脅威トレースを使用することで、ネットワークの状況を正しく把握し、問題点の発見やその対策を行えるようになる。脅威トレースはサイバー攻撃の解析やネットワークのハードニングを助けるためのシミュレーターであるが、シミュレーションには事前定義された特定のシナリオの実行のみを提供するため、現実に即したシミュレーションには不十分であるという課題があった。

行った脅威トレースの拡張は大きく 2 つに分かれる。一つは実際のネットワークから情報を得る方法である。本研究ではこれをデジタル来歴（以下、来歴）と呼ぶ。来歴の収集には CamFlow と呼ばれる Linux Security Modules を用いた。来歴は情報システムの実行の履歴であり、収集したデータを解析し脅威トレースに適用する。本研究では gRPC サーバーを脅威トレースのインターフェイスとして追加採用し、脅威トレースのクライアントを様々なプログラミング言語によって開発できるように拡張した（図 4）。

実装が提案手法の目的を満たしているかを確認するための実験を行った。実験では擬似マルウェアを来歴の収集を行うマシン上で動作させ、収集した来歴を脅威トレースに適用させた時に脅威トレース上でその挙動が再現できることを確認した。この結果により実装が提案手法の目的を満たしていることが示されており、脅威トレースが従来よりも現実に即したシミュレーションを行えるようになった。

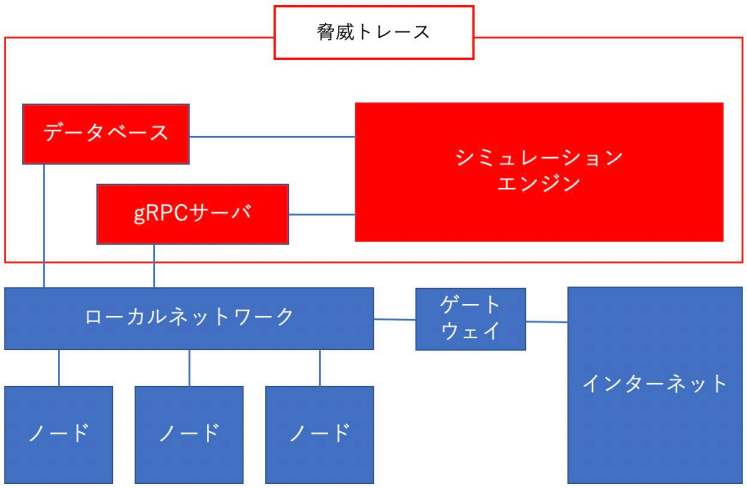

図 4: 拡張された脅威トレースのシステム概要。

[4a] Kato, Masahiko and Matsunami, Takumi and Kanaoka, Akira and Koide, Hiroshi and Okamoto, Eiji : Tracing advanced persistent threats in networked systems, Automated Security Management, pp. 179--187, Springer (2013).

[4b] Takatoshi Murakami and S. Kumano and Hiroshi Koide: An implementation of tracing attacks on advanced persistent threats by using actors model, 2014 Joint 7th International Conference on Soft Computing and Intelligent Systems (SCIS) and 15th International Symposium on Advanced Intelligent Systems (ISIS), pp.1316–1320 (2014).

[4c] Yuya Tajima and Hiroshi Koide: Applying the Attacks Tracer on Advanced Persistent Threats to Real Networks, 2021 Ninth International Symposium on Computing and Networking Workshops (CANDARW), pp.392—397, (Nov. 2021).

5.3 研究内容紹介

5.3.1 小出 洋

研究内容

1. Moving Target Defense（MTD）に関する研究

Moving Target Defense（MTD）は情報システムにおけるさまざまなパラメータ（例えばOS、システムコール番号、実行可能バイナリのマジックナンバー、ネットワーク識別子）を変化させ、攻撃を困難にする近年注目されている手法である。本研究では、特定のアプリケーションや特定の情報システムに向いたMTDの開発と評価、あるMTDを情報システムに適用したときの平均攻撃成功時間間隔などのMTDのサイバー攻撃に対する防御性を評価する方法に関する考察、ひとつの情報システムに複数の異なるMTDを適用した場合の防御性を評価する方法について研究を行っている。

2. 脅威トレースに関する研究

APT攻撃に利用されるマルウェアに代表される脅威が情報システムに侵入したときの活動を予測し、脅威が行う攻撃を阻止したり、情報漏洩を防いだりするには何が必要かを明らかにし、情報システムの設計や運用に資することを目的として脅威トレースの提案、実装、評価を行っている。脅威トレースはマルウェアとそれが動作する情報システムと攻撃に使われるマルウェアを抽象度の高いモデルで表現し、その挙動をシミュレーションすることで解析している。

3. Webアプリケーションのための攻撃検知システムに関する研究

Webアプリケーションを作成する際には、Webアプリケーション・フレームワークが必ず利用される。サイバー攻撃の検知やサイバー攻撃からシステムを防御するための機能はWebアプリケーション・フレームワークが備えるべき機能といえるが、実際はWebアプリケーション・ファイヤーウォールやセキュリティアプライアンス等の別のシステムになっていることが多い。サイバー攻撃からの防御のための機能をWebアプリケーション・フレームに組み込んだ場合、Webアプリケーション内部の情報やWebアプリケーションの特徴にあわせた攻撃検知とすることができる。Webアプリケーションの特徴に合わせた攻撃検知や攻撃をハニーポットに誘導する機能をWebアプリケーション・フレームワークに実装して評価する研究を行っている。

所属学会名

ACM，ソフトウェア科学会，電子情報通信学会，情報処理学会

研究プロジェクト

- サイバー攻撃が困難な情報システムを構築するためのフレームワーク
  2021.04～2025.03, 代表者:小出　洋, 九州大学, 九州大学(日本)
- 戦略的国際共同研究プログラム(SICORP)「国際共同研究拠点（インド）」「安全な IoT サイバー空間の実現」
  2016.10～2021.09, 代表者：岡村 耕二, 九州大学, 国立研究開発法人　科学技術推進機構（日本)

研究業績

● 国際会議

1. Tomoya Terashima, Masahiro Nakayama, Teruaki Yokoyama and Hiroshi Koide, KAKOI: A New Tool to Make Simple and Secure Build Cyber Ranges Using Public Cloud, 2021 Ninth International Symposium on Computing and Networking Workshops (CANDARW), IEEE, Nov. 2021.
2. Yuya Tajima, Hiroshi Koide, Applying the Attacks Tracer on Advanced Persistent Threats to Real Networks, 2021 Ninth International Symposium on Computing and Networking Workshops (CANDARW), pp. 392-397, Nov. 2021.
3. Takeshi Masumoto, Wai Kyi Kyi Oo and Hiroshi Koide, MTD: Run-time System Call Mapping Randomization, Proc. 2021 International Workshop on Cyber Security, pp. 257--263, Act, 2021.
4. Mariama Mbow and Hiroshi Koide and Kouichi Sakurai, An Intrusion Detection System for Imbalanced Dataset Based on Deep Learning, 2021 Ninth International Symposium on Computing and Networking (CANDAR), pp. 38-47, Nov. 2021.

● 学会発表

1. 井上 幸紀，小出　洋，複数のプロキシを使用した経路変更 Moving Target Defense によるマルウェア検知・隔離，情報処理学会九州支部，2022.03.

研究資金

● 科学研究費補助金

1. 2021 年度～2024 年度， 基盤研究(C)， 代表， サイバー攻撃が困難な情報システムを構築するためのフレームワーク

● 競争的資金

1. 2017 年度～2022 年度，文部科学省研究拠点形成費等補助金（成長分野を支える情報人材の育成拠点の形成(enPiT) enPiT-Pro)，連携，企業・官公庁等の IT 実務、設計･製造実務における情報セキュリティに関わるプロ人材育成コースの開発・実施

● 共同研究、受託研究

1. 2021.06～2022.03，代表，情報システムを攻撃から防御するための Moving Target Defense に関する研究

教育活動

● 教育活動概要

1. 2017 年～現在　enPiT-Pro ProSec-IT の主体的実施

● 担当授業科目

1. 2021 年度・後期，通信工学通論 A
2. 2021 年度・後期，通信工学通論 B
3. 2021 年度・後期，コンピュータシステム通論 A
4. 2021 年度・後期，コンピュータシステム通論 B

社会貢献・国際連携

● 社会貢献活動

1. 2019.04.01～，福岡県警サイバー犯罪対策テクニカルアドバイザーとして委嘱された（再委嘱）。
2. 2021.06.13～，直方市情報公開･個人情報保護審査委員として委嘱された（再委嘱）。

大学運営

● 学内運営に関わる各種委員・役職等

1. 2020.04～2022.03，情報基盤研究開発センター副センター長
2. 2019.04～，　　情報統括本部情報共有基盤室長