Computer Security Symposium 2018
22 - 25 October 2018

TOMOYO Linux による強制アクセス制御効果の可視化

小倉 有花[†1]　辻 秀典[†1]　橋本 正樹[†1]

概要：サイバー攻撃の巧妙化に伴い，侵入を前提としてシステム内部での破壊活動を阻止する対策が重要となっているが，セキュア OS を用いた防御策はその有効性にも拘わらず普及が進んでいない．その原因は，使いにくさや効果の不明瞭さであると考えられるが，前者を改善する様々な試みが存在する一方で，後者を対象とする研究は現時点では十分に行われていない．本研究では，TOMOYO Linux をインストールしたシステムに対して不正アクセスを行い，その強制アクセス制御機能によってシステムが保護される一連の流れを確認し，効果を可視化する手法を提案する．これによりセキュア OS 導入の効果を容易に認識可能とし，普及拡大の一助となることを期待するものである．

キーワード：OSS，セキュア OS，TOMOYO Linux，強制アクセス制御(MAC)，可視化

Visualizing Mandatory Access Control Effects of TOMOYO Linux

Yuka Ogura[†1]　Hidenori Tsuji[†1]　Masaki Hashimoto[†1]

Abstract: With increasing sophistication of cyber attacks, it is rapidly becoming important to focus on arresting destructive actions inside the system rather than preventing intrusions. Secure OSes are not spreading widely, though having been proved to be effective for protecting information systems from unknown attacks. We estimate that user-unfriendliness and ambiguity of their efficacy prevent secure OSes from spreading widely. Although there are some research approaching their user-unfriendliness, there is currently no such research focused on clarifying the ambiguity of their efficacy. This paper concentrates on visualizing the effect of Mandatory Access Control (MAC) performed by TOMOYO Linux, which is one of the main secure OSes, with the experiment of attacking TOMOYO Linux system and showing the process of preventing attacks. Consequently, this research expects to get synergetic effects, in which both the concept of secure OSes and efficacy of TOMOYO Linux are coming to be acknowledged.

Keywords: OSS, Secure OS, TOMOYO Linux, Mandatory Access Control (MAC), visualization

1. はじめに

1.1 研究の背景と課題

現代社会では情報システムが重要インフラとして浸透しており，人間の日常生活は情報システムなしでは成り立たない．情報システムの爆発的な普及と進化によって私たちが享受できる利便性が飛躍的に向上した一方で，情報システムへのアクセスは容易化・一般化し，コンピュータやサーバ等機器同士の連携もより密になった．それに伴い，特定人物の個人情報から企業固有の営業秘密に至るまでありとあらゆる類の機微な情報が情報システム上で日常的にやり取りされているが，これらの情報資産は常に世界各地からのサイバー攻撃やヒューマンエラーによる漏洩等の危険に晒されているのが現状である．

このような状況においては大切な情報を確実に保護することは困難で，絶対に侵入されないような情報システムを設計することも不可能であると言える．そのため，サイバー攻撃等に遭遇した場合でも攻撃者の意のままにコントロールされることなく，様々な破壊・搾取活動を抑制できるようにすることが大切であり，この目的のために，最小特権の原則を実現するための強制アクセス制御機能を実装した，所謂セキュア OS が開発されている．強制アクセス制御機能の Linux に対する代表的な実装例としては，SELinux，AppArmor，Smack，TOMOYO Linux[1]等が知られており，その有用性がある程度認知されているにも関わらず，普及が進んでいるとは言い難い．

セキュア OS は，「出来ないことが増える」という不自由さがあるだけでなく，利用に伴ってポリシーの理解や修正などの管理作業が必要となるため，使いにくいという難点がある．この他にも，例えば，細粒度のアクセス制御でシステムに制限をかけるため正しく設定しない限りはシステム停止等のトラブルを誘発する可能性があること，現時点での使用事例が少なく効果も不明確なことなどがあり，これらをまとめると，「ポリシー管理業務の手間を引き受けてまで使用することに果たしてメリットがあるのか」という疑念をユーザに想起させていることが容易に推測できる．

セキュア OS の使い難さに関しては，既にその改善に向けてアプローチを行った先行研究が存在しているが，セキュア OS の効果やメリットを明確にすることに焦点を当てた研究は，現在のところ行われていない．

†1　情報セキュリティ大学院大学
Institute of Information Security

1.2 本研究の目的と貢献

本研究では，特にセキュア OS の中でも TOMOYO Linux に焦点を当て，セキュア OS の効果の可視化を目指す．TOMOYO Linux は，セキュア OS の課題であったシステム管理の困難性を軽減しながら，従来のセキュア OS 同様に，多くの不正アクセス被害を抑制可能な Linux 向け強制アクセス制御実装である．セキュア OS の普及が進まない原因を，「セキュア OS それ自体が使いにくいだけでなく，使用によって得られる効果が不明確で分かりにくいからである」と仮定した時に，使いにくさの軽減に一定の成果がある TOMOYO Linux を対象として効果の可視化を行うことで，普及への相乗効果となることも併せて期待する．

1.3 本稿の構成

本稿の構成は以下の通りである．すなわち，第 1 章で背景と課題，本研究の目的と貢献について説明し，第 2 章で関連研究を整理する．第 3 章では，強制アクセス制御機能によるシステム保護の可視化手法について説明する．その後，第 4 章では評価実験について述べ，第 5 章では評価と考察を行う．最後に第 6 章で，まとめと今後の課題を述べる．

2. 関連研究

本章では，(i) セキュア OS の使い難さの改善とその導入効果の強化に関する関連研究，と(ii) 可視化の目的や技術に関する調査，および サイバーセキュリティ分野において可視化を取り入れた関連研究について説明する．

2.1 セキュア OS に関する研究

原田らの研究[2]では，従来のアクセス制御方式の課題であった，アクセス要求の可否判断のシステムやアプリケーションへの影響および可否判断時点で客体に保存されていた情報の使われ方が考慮されていない問題に対する解決策として，アプリケーションの実行状況を考慮した新たなアクセス制御方式を提案し，その手法の Linux 上での実装である TOMOYO Linux における評価結果を報告している．従来のアクセス制御方式では，アクセス主体であるアプリケーションとアプリケーションがアクセスしようとするファイル等の客体の組み合わせによるアクセス要求の可否判断を行っていたが，原田らの提案手法では，システムが起動されてからアプリケーションが実行されるまでの履歴とアプリケーションのコマンドライン引数やアクセス要求発生時のコマンドライン引数等の様々な情報からアプリケーションの実行状況を解釈し，これらの情報を条件として利用することによってアクセス可否の判断している．提案手法については，不正アクセスや誤操作に伴うリスクを軽減できるだけでなく，典型的な不正アクセス手法の多くに対する効果があることも考察されている．しかし，不正なアクセス要求が発生してから提案手法によって拒否されるに至るまでの具体的な流れに関しては検討対象としていない．

品川の研究[3]では，インターネットを経由して試られる不正アクセスを対象として，研究や開発が行われている OS による不正アクセス防止技術を複数紹介し，これらの不正アクセス防止技術がどのような種類の攻撃に対してどの程度の有効性を持つのかを分類・評価している．既存のいくつかの不正アクセスを受けた際にシステムが被る被害の大きさを計測する指標を導入し，それを基に評価を行い，これらの不正アクセス技術が，論文で導入した指標のどのような点に対して効果を発揮するかについて報告している．しかし，個々の不正アクセス防止技術が具体的にはどのような情報資産を保護することが可能であるかといったような，不正アクセス防止技術が持つ効果に関する検証実験は実施していない．

2.2 可視化に関する研究

白山の研究[4]では可視化を行う対象と方法に応じて既存の可視化手法を，データの可視化(Data Visualization)・情報の可視化(Information Visualization)・対話型の可視化(Interactive Visualization)の 3 つのカテゴリに分けて整理し，膨大量のデータを処理することが求められるビッグデータ時代において，人間の手作業による可視化作業を自動化し，効率化するための可視化エージェントを提案・設計している．可視化における最大の目的は，「みえないもの，見えない関係を，見えるようにすること，分かり易く示すこと」であり，可視化を行うプロセスのみならず，可視化された結果を解釈する段階においても，人間の分析に伴う任意性が生じてしまうことを十分に理解しておく必要があることが強調されている．「可視化から分かることは対象依存であることから一般論を述べることが難しいこと」，「情報工学の発展と歩調を合わせる形で可視化の効率化に関する研究の増加が望まれること」の 2 点を中心に報告されているが，白山の提案手法は可視化作業の効率化に焦点を当てており，分かりにくいデータや情報を可視化によって分かり易く示すという作業には至っていない．

金らの研究[5]では，ファイアウォールを通過しようとするパケットの状況を可視化・解析可能なツールを提案・実装している．金らは，提案手法によってネットワーク管理者がパケットを解析する際に「どのパケットがファイアウォールを通過してどのパケットが拒否されたのか」を瞬時に判断することが可能となったことだけでなく，実装した解析ツールが現場で実用的であることを客観的に示す目的で実施した，ネットワーク専門家に対する聞き取り調査の結果も報告している．しかし，同研究はファイアウォールを対象としたものであり，OS を対象とした研究ではない．

3. 提案手法

3.1 TOMOYO Linux による強制アクセス制御

本研究の対象とする TOMOYO Linux はセキュア OS のひとつであり，アクセス制御機能と，システムの起動から終了までに発生したアクセス許可内容を自動学習によって記録することでシステムの解析を可能にする解析機能の 2 種類の機能を有している．

TOMOYO Linux ではアクセス制御の動作内容に基づいて制御モードを規定しており，制御モードは disabled, learning, permissive, enforcing の 4 つの段階に分かれている．それぞれの制御モードとその動作内容を表 1 に示す．

表 1　TOMOYO Linux の制御モード
Table 1　TOMOYO Linux Mode

モード	内容	動作
disabled	無効	通常のカーネルと同様に動作する
learning	学習	ポリシ違反が発生しても要求を拒否しない ポリシ違反が発生しないようにするのに必要なアクセス許可をポリシに追加する
permissive	確認	ポリシ違反が発生しても要求を拒否しない
enforcing	強制	ポリシ違反が発生したら要求を拒否する

本研究では，TOMOYO Linux の制御モードを disabled(無効)の状態に設定した後、enforcing（強制）の状態にモードを変更し，各モードにおいて構築したシステムに対する不正アクセスを試みることで, その効果を検証する. さらに, TOMOYO Linux の特長である自動学習による解析機能を活用し，どの資源にアクセスしようとして失敗したのか，すなわち「具体的にどのような情報資産が護られたのか」を把握する．このことを用いて，TOMOYO Linux が容易に導入可能であることを示し，TOMOYO Linux の利用によって一定のセキュリティ強化効果が存在することを明示する．

3.2 アクセス制御プロセスの可視化

TOMOYO Linux を用いて不正アクセスを防止することができる様子および TOMOYO Linux 導入による効果を容易に認識可能とするために，TOMOYO Linux が有効化されていない場合と TOMOYO Linux を enforcing モードで有効化した場合とで, 攻撃を阻止できる段階の違いを比較する．提案する可視化手法は TOMOYO Linux の有無および有効化した段階に応じて，侵入およびその後のシステム内部での攻撃者による破壊活動の進行状況を，権限昇格からシステムが最終的に掌握されるまでの過程を下記の 7 ステップに分類し, 4.3 節で示すように図式化する．

表 2　攻撃開始からシステム掌握までのステップ
Table 2　7 steps in cyber attacks

侵入	攻撃対象へ侵入
一般権限取得	一般ユーザ権限を取得
管理者権限取得	管理者へ権限昇格
読み込み	ディレクトリの中身など参照
書き込み	ファイルの内容などを編集
様々な作業の実行	パスワード変更などを実行
システム全権掌握	再起動等を行い，システムを奪取

4. 実験

4.1 実験の概要

Oracle VirtualBox 5.2.6 の上に, ubuntu 14.04 Trusty Tahr をインストールし,TOMOYO Linux 2.5 の有効化を行った．

本実験では，TOMOYO Linux を有効化した Ubuntu 14.04 に対する権限昇格攻撃を実施することにより，TOMOYO Linux が有効化されていない場合(disabled モード, 通常のカーネルと同様)と有効化されている場合(enforcing モード)とを比較し, TOMOYO Linux が有効化されていない場合とされていた場合とで不正アクセスをどのくらい防ぐことができたのかを調査する．

利用する攻撃用コードは，Exploit Database (https://exploit-db.com) に登録されている，2017 年 8 月 13 日登録の ’KASLR / SMEP’ (Linux Kernel <4.4.0-83 / < 4.8.0-58 Ubuntu14.04 / 16.04) ローカル権限昇格の脆弱性を対象とした C 言語プログラム 43418.c である[6].

43418.c は，CVE-2017-1000112[7]を利用した攻撃コードであり，Linux カーネルがメモリ破壊攻撃に脆弱であることを利用している．同プログラムの実行を成功させることができた場合，攻撃者は管理者権限を用いて任意の攻撃コードを実行することが可能であり，攻撃に失敗した場合には攻撃対象への DoS (Denial of Service) の状態につながる可能性がある．

4.2 実験の詳細　(不正アクセス)

(i)　disabled モードに設定した場合

TOMOYO Linux 2.5 を有効化した攻撃対象マシン Ubuntu 14.04 の一般ユーザ(tomoyo)を作成し，tomoyo のホームディレクトリ ~/tomoyo に攻撃コードである 43418.c をダウンロードした. ~/tomoyo への保存後, コンパイルした 43418 を実行したところ，図 1 のような挙動を示し，管理者権限を奪取することが可能であった．

その後, 引き続き TOMOYO Linux が disabled mode の状態でいくつかの任意のコマンド(ls, mkdir，cat/etc/passwd など) を実行したところ，図 2 のように任意のコマンドを実行することが可能となった．

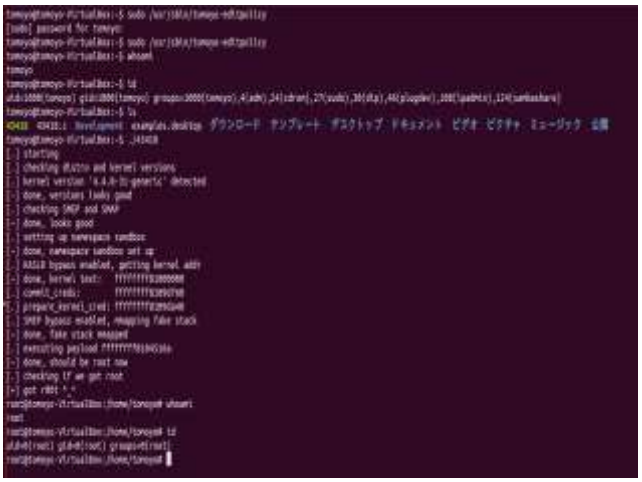

図 1　攻撃コード　43418.c の実行
Picture 1　exploit to the target machine with 43418.c

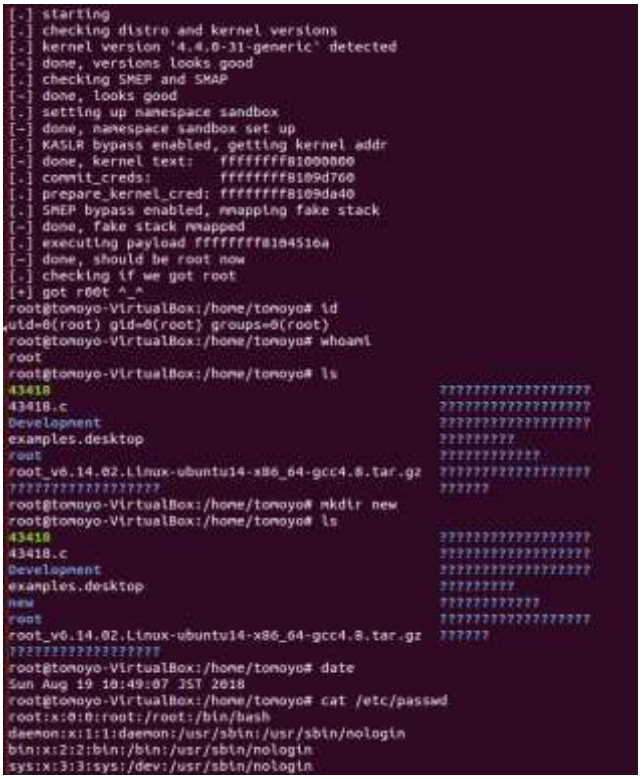

図 2　管理者権限取得後の任意コマンドの実行
Picture 2　executing arbitrary commands after gaining root

(ii)　enforcing モードに設定した場合

a)　攻撃コードの実行前に enforcing モードにした場合

実験(i)の後，TOMOYO Linux のモードを切り替えてから攻撃コードを実行したところ，図 3 のような挙動となり，攻撃コードそのもの実行が拒否され，攻撃は失敗した．

b)　攻撃コードの実行後に enforcing モードにした場合

実験 (ii)の a) を行った後，ターミナルを再起動し，改めて攻撃を実行し,管理者権限を取得されてしまった後に TOMOYO Linux を強制モードに切り替えたところ，図 4 に示すような挙動となり，攻撃コードの実行によって任意のコマンドの実行を制限することができたことを確認した．

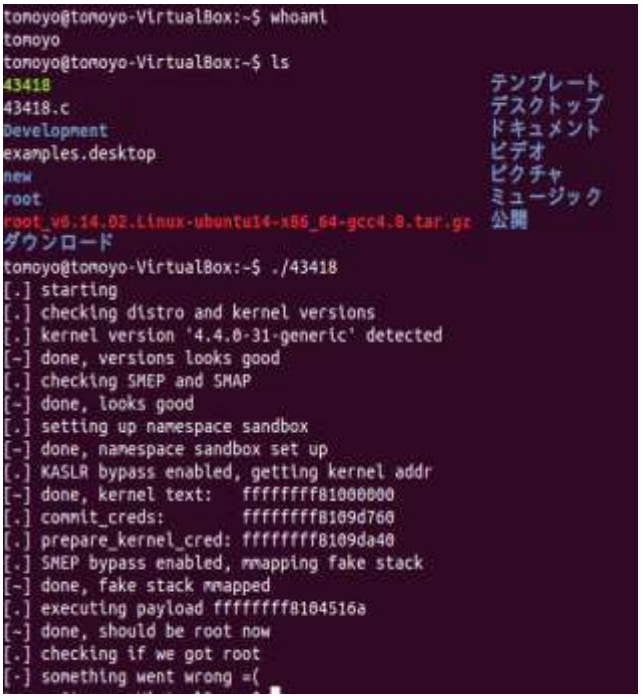

図 3　TOMOYO Linux の強制モード
Picture 3　TOMOYO Linux in enforcing mode

実験 (i) ~ (ii)の結果から，TOMOYO Linux を disabled モードにした時と，enforcing モードにした時とで Root 権限取得 (侵入) /読み込み(Read) / 書き込み(Write) /実行(eXecute) の 4 点に対する制限の違いを表 2 にまとめる．

表 2　実験 (i) ~ (ii) b)の結果
Table 2　Results of the experiments

	TOMOYO なし	TOMOY あり (攻撃実行前から)	TOMOYO あり (攻撃実行後から)
権限昇格	○	×	○
R	○	×	×
W	○	×	×
X	○	×	×

4.3 TOMOYO Linux の不正アクセス防止効果の可視化

実験内容の可視化にあたり，攻撃者による攻撃開始からシステムの全権が掌握されるに至るまでの過程を図 5 のように 7 つのステップに分類した．前項で行った実験では，リモートからの侵入ではなく，ローカルでの権限昇格であ

ったことから，今回は侵入・一般ユーザの権限取得の 2 段階については両方とも行われたものとして可視化を行った．

図 6 および図 7 は，いずれも TOMOYO Linux による強制アクセス制御を行った場合でのシステム内部の破壊活動の進行度を示しており，図 6 は攻撃コード (./43418)の実行前にあらかじめ TOMOYO Linux を enforcing モードに設定しておいた場合，図 7 は攻撃コードが実行されて権限昇格が行われた後に TOMOYO Linux を enforcing モードに設定した場合の攻撃の進行状況である．

図 5～図 7 の可視化結果より，TOMOYO Linux を有効化しない場合ではシステム内部の破壊活動が進み，最終的にシステムの全権が掌握されたのに対し，TOMOYO Linux の強制アクセス制御機能を利用した場合には，システム内部の破壊活動を阻止できることを視覚的に確認できる．

```
tomoyo@tomoyo-VirtualBox:~$ ./43418
[.] starting
[.] checking distro and kernel versions
[.] kernel version '4.4.0-31-generic' detected
[~] done, versions looks good
[.] checking SMEP and SMAP
[~] done, looks good
[.] setting up namespace sandbox
[~] done, namespace sandbox set up
[.] KASLR bypass enabled, getting kernel addr
[~] done, kernel text:   ffffffff81000000
[.] commit_creds:        ffffffff8109d760
[.] prepare_kernel_cred: ffffffff8109da40
[.] SMEP bypass enabled, mmapping fake stack
[~] done, fake stack mmapped
[.] executing payload ffffffff8104516a
[~] done, should be root now
[.] checking if we got root
[+] got r00t ^_^
root@tomoyo-VirtualBox:/home/tomoyo# id
bash: /usr/bin/id: Operation not permitted
root@tomoyo-VirtualBox:/home/tomoyo# date
bash: /bin/date: Operation not permitted
root@tomoyo-VirtualBox:/home/tomoyo# mkdir new
bash: /bin/mkdir: Operation not permitted
root@tomoyo-VirtualBox:/home/tomoyo# cat /etc/passwd
bash: /bin/cat: Operation not permitted
root@tomoyo-VirtualBox:/home/tomoyo# uname -a
bash: /bin/uname: Operation not permitted
root@tomoyo-VirtualBox:/home/tomoyo# ls -l
bash: /bin/ls: Operation not permitted
root@tomoyo-VirtualBox:/home/tomoyo# sleep 5s
bash: /bin/sleep: Operation not permitted
root@tomoyo-VirtualBox:/home/tomoyo# shutdown -r now
bash: /sbin/shutdown: Operation not permitted
root@tomoyo-VirtualBox:/home/tomoyo# ps aux
bash: /bin/ps: Operation not permitted
root@tomoyo-VirtualBox:/home/tomoyo# passwd tomoyo
bash: /usr/bin/passwd: Operation not permitted
root@tomoyo-VirtualBox:/home/tomoyo# vi /etc/passwd
bash: /usr/bin/vi: Operation not permitted
root@tomoyo-VirtualBox:/home/tomoyo# rm examples.desktop
bash: /bin/rm: Operation not permitted
root@tomoyo-VirtualBox:/home/tomoyo# dmesg
bash: /bin/dmesg: Operation not permitted
root@tomoyo-VirtualBox:/home/tomoyo# ifconfig
bash: /sbin/ifconfig: Operation not permitted
```

図 4　TOMOYO Linux による強制アクセス制御
Picture 4　TOMOYO Linux in enforcing mode

5. 評価と考察

5.1 評価の軸

本研究の最終的な目標は，TOMOYO Linux，ひいてはセキュア OS を利用することによる不正アクセス防止効果を明確にすることである．効果を明確に示すにあたり，上記の実験および可視化の結果について筆者が作成した表 3 の評価軸を利用し効果が明確に示せているか否かを検討する．

表 3　　評価軸と評価
Table 3　Results of the evaluation

評価軸	評価内容
図の見やすさ	△
語句の分かり易さ	△
専門分野外の人が見た時の分かり易さ	△
守られた資産の分かり易さ	×

この評価については，○・△・×の 3 段階で定性的に行った．評価手法は検討段階にあり，アンケートなども実施できていないことから主観的な評価に留まっているが，図を可能な限りシンプルにすることで，図の見やすさを更に高めることを目標としている．図の横に記載する各ステップについての説明の分かりやすさ，専門分野外の人が見た時の分かりやすさについては今後大きな改善余地が見込まれることから，△と表記している，破壊活動の進行防止によって守ることができた資産の分かり易さに関しては，現時点において可視化することが出来ていないため，今後に向けて可視化を行う必要がある．

5.2 考察

本研究で行った実験では，まずローカルでの権限昇格を行いシステム侵入後の破壊活動を行う攻撃を例に，TOMOYO Linux が disabled の場合と enforcing の場合とを比較し，更に TOMOYO Linux を enforcing モードに設定するタイミングを攻撃コードの実行前と実行後の 2 パターンに分け，両者の間で破壊活動の進行にどの程度の差が生じるかを比較した．その上で，侵入からシステムの全権掌握までの 7 つの段階に破壊活動を分類し，3 つの実験それぞれにおいてどこまで破壊活動が進んだか (= どこからの破壊活動を阻止することができたか)を可視化することにより，TOMOYO Linux を用いない場合よりも TOMOYO Linux を用いた場合の方が破壊活動を阻止する効果の観点で有意な差があることを視覚的に認識することが可能となった．

7 段階の攻撃ステップに分類して可視化を行い，シンプルな図を用いて破壊活動の進行状況の差を図示したことで

TOMOYO Linux がある場合には攻撃の進行防止に大きな効果があることを示すことができたが，より容易に TOMOYO Linux の効果を認識可能とし，利用者の TOMOYO Linux およびセキュア OS 導入に役立ててもらうためには，具体的にどのようなコマンドの実行が制限され，それによってどのような資産が保護されたのかを詳細に可視化結果へ取り入れていく必要がある．

提案手法では認識のし易さを重視しており， 4.3 節で示した可視化結果に含まれる情報量は非常に少なく，「TOMOYO Linux がある場合にはない場合と比較してシステム内部の破壊活動を途中で食い止めることができた」以上の情報は読み取ることが出来ない状態である．可視化結果を見る人に TOMOYO Linux およびセキュア OS を利用することの効果を十分に認識してもらうことができるよう，情報量を増やした可視化結果を示す必要性が急務であると考えられる．

図 5　実験内容 (i) についての可視化結果
Picture 5　Visualization results of experiments (i)

図 6 実験内容 (ii) a) についての可視化結果
Picture 6　Visualization results of experiments (ii) a)

図 7　実験内容 (ii) b) についての可視化結果
Picture 7　Visualization results of experiments (ii) b)

6. まとめと今後の課題

本研究では，TOMOYO Linux およびセキュア OS の効果を容易に認識可能とすることを目的として，以下の 3 つの実験と実験内容の可視化，および可視化結果に対する評価と考察を行い，下記のことが分かった．

① TOMOYO Linux を無効化した Ubuntu システムに対するローカルにおける権限昇格・不正アクセス
→ 管理者権限の取得もシステム内部での破壊活動のいずれも防ぐことが出来なかった．

② TOMOYO Linux を有効化した Ubuntu システムに対するローカルにおける権限昇格・不正アクセス (攻撃コードの実行する前に強制モードに設定)
→ 管理者権限の取得を防止することができ，その後の破壊活動も防ぐことができた．

③ TOMOYO Linux を有効化した Ubuntu システムに対するローカルにおける権限昇格・不正アクセス (攻撃コードの実行した後に強制モードに設定)
→ 管理者権限の取得は防止出来なかったが，その後の破壊活動は防ぐことができた．

④ 上記実験における破壊活動の防止効果の可視化
→ TOMOYO Linux が無効化されている場合に較べ，TOMOYO Linux が有効化されている場合では攻撃者によるシステム内部の破壊活動を有意に防げることをシンプルな図を用いて視覚的に認識することができた．

今後に向けては，ローカルではなくリモートからの攻撃を実行した上で上記のような実験を行っていく必要があること，更なる情報量を盛り込んだ可視化結果を作成し，客観的な視点からの評価を実施するなどの課題が残っている．

参考文献

[1] TOMOYO Linux 公式 HP (http://tomoyo.osdn.jp/index.html.ja)
[2] 原田季栄，半田哲夫，橋本正樹，田中英彦，「アプリケーションの実行状況に基づく強制アクセス制御方式」，情報処理学会論文誌，Vol.53 No.9 1-18 (2012)
[3] 品川高廣：「オペレーティングシステムによる不正アクセス防止技術」，コンピュータソフトウェア， Vol. 21, No. 6, pp. 482–493 (2004).
[4] 白山晋：「可視化から何が分かるのか」，システム創生学 第二回　学術講演会
[5] H.Kim et al, “ Firewall ruleset visualization analysis tool based on segmentation”, Visualization for Cyber Security (VizSec) 2017
[6] Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Privilege Escalation (KASLR / SMEP), https://www.exploit-db.com/exploits/43418/(accessed 2018-08-20).
[7] NVD - CVE-2017-1000112, https://nvd.nist.gov/vuln/detail/CVE-2017-1000112(accessed 2018-08-20).