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　５ 年　 ５ 月 ２９ 日現在

機関番号：１５３０１
研究種目：基盤研究(B)（一般）
研究期間：2019～2022
課題番号：１９Ｈ０４１０９

研究課題名（和文）攻撃耐性を持つ基盤ソフトウェア構築法の研究

研究課題名（英文）Research on Methods for Structuring Attack-Resistant Fundamental Software

研究代表者
山内　利宏（Yamauchi, Toshihiro）

岡山大学・自然科学学域・教授

研究者番号：８０３５９９４２

交付決定額（研究期間全体）：（直接経費）　　10,200,000円

研究成果の概要（和文）：計算機の基盤ソフトウェアであるOSとVMMに着目した新しいセキュリティ機構を実現するために，以下の研究において有効性を示した．まず，VMMによるゲストOSの機密情報の拡散追跡機能を複数のVMを対象として，実現した．また，OSカーネルの情報やセキュリティ機構を保護する機構を，複数の仮想記憶空間を用いて実現する手法や，仮想化技術やArmのTrustZoneを用いて実現する方法を実現した．さらに，ゲストOSの権限昇格を検知し，無効化する手法も実現した．これらの成果により，OSの攻撃耐性を高め，セキュリティ機構への攻撃を困難化できる基盤ソフトウェア技術の構築法を示した．

研究成果の学術的意義や社会的意義
本研究期間中も，サイバー攻撃が活発化し，その手法が高度化しており，計算機の基盤ソフトウェアの重要性は増している．このような状況で，基盤ソフトウェアの中核をなすOSの攻撃耐性を高め，セキュリティ機構の安全性を高める方式を提案しており，提案手法は今後，セキュアな計算機環境の実現に貢献できる．また，クラウド環境などで広く利用されている仮想化環境でも，利用できる手法を研究開発しており，本研究成果の適用範囲は広い．

研究成果の概要（英文）：We have demonstrated the effectiveness of a new security mechanism focusing on the OS and VMM, which are fundamental software of a computer, in the following research. First, we developed a VMM that can track the spread of classified information of a guest OS across multiple VMs. We also realized a method to protect OS kernel information and security mechanisms by using multiple virtual storage spaces, virtualization technology, and Arm's TrustZone. We have also developed a method for detecting and disabling privilege escalation in a guest OS. With these results, we have shown how to build a fundamental software technology that increases OS attack resistance and makes attacks on security mechanisms more difficult.

研究分野：基盤ソフトウェア

キーワード：オペレーティングシステム　仮想化技術　セキュリティ　OS脆弱性　耐攻撃性

様　式　C－１９、F－１９－１、Z－１９（共通）

１．研究開始当初の背景

重要な情報を狙った攻撃や金銭目的のサイバー攻撃が急増し，かつその手口も高度化している．このため，計算機で提供されるサービスには，セキュリティが必要不可欠である．しかし，現在の計算機環境は，ソフトウェアに多数のセキュリティ上の欠陥（脆弱性）が発見され続けており，標準のセキュリティ機構だけでは，安全に計算機を利用することは難しい．

また，計算機の基盤ソフトウェアであるオペレーティングシステム（OS）や仮想マシンモニタ（VMM ：Virtual Machine Monitor），及びネットワークにおいて様々なセキュリティ機構が研究開発されている．しかし，攻撃側は，防御側の対策に対し，防御側が想定していない新しい方法での攻撃，及び未知の脆弱性の悪用を行い，不正なコードの実行やセキュリティ機構の無効化を行う．このため，攻撃側が有利な状況が続いている．

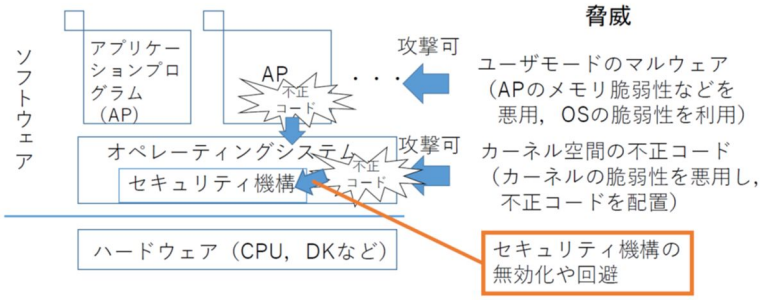

図1　応用プログラム(AP)，OS，及びセキュリティ機構に対する脅威

２．研究の目的

計算機の基盤ソフトウェアである OS と VMM に着目した新しいセキュリティ機構を創出する．また，攻撃者にセキュリティ機構の存在を知られたとしても，セキュリティ機構への攻撃を困難化する機構を提案する．本提案課題では，次の三つの研究を行い，新しい基盤ソフトウェア向けセキュリティ機構による安全な計算機環境構築の実現を目指す．

（研究１）OS カーネルへの脆弱性攻撃の無効化とセキュリティ機構の攻撃耐性向上の研究
（研究２）VMM によるゲスト OS(仮想マシン(VM))のセキュア化と回避困難化の研究
（研究３）カーネルの仮想記憶空間の分離によるセキュアな実行機構の研究

３．研究の方法

（研究１）について，以下の手法について，研究を行った．
（１）　Linux OS において保護すべき OS 情報の拡大に伴い，オーバヘッドの増大が見込まれるため，保護すべき情報やセキュリティ機構を調査する．OS の特権情報などセキュリティに関連する重要な情報の改ざんを検知し，改ざんを無効化する手法を検討する．
（２）　セキュリティ機構の攻撃耐性を上げるために，VMM などに実現する手法について検討する．これにより，VMM にセキュリティ機能を実現することで，セキュリティ機構の攻撃耐性の向上を図ることができる．
（３）　スマートフォンや IoT 機器などで利用される Arm TrustZone の機能を利用し，セキュアワールドに OS の権限情報を管理するセキュリティ機構を実現する方式についても検討する．

（研究２）について，以下の手法について，研究を行った．
（１）　仮想マシン（VM）内のゲスト OS 上で攻撃などが行われた際の証拠を取得し，証拠を安全に保全する手法を，仮想化技術を用いて検討する．これにより，情報漏洩が活性した際などに，原因や被害の範囲の調査を支援できることが期待できる．
（２）　仮想化環境で実行される仮想マシン（VM）を保護する手法として，機密情報の拡散追跡機能を VMM に実現方式を研究する．この機構により，ゲスト OS の機密情報を把握でき，情報漏洩に対応できる．
（３）　仮想化技術を用いた場合に，監視されていることをマルウェアなどに検知されると，監視を回避される可能性があるため，監視していることを不可視化する手法を検討する．

（研究３）について，以下の手法について，研究を行った．
（１）　Linux では，OS のコードやデータが存在するカーネル空間を全てのプロセスで共有する．このため，攻撃を受けた際に影響範囲が全てのプロセスに影響する．

（２）　セキュリティ機構も OS と同じカーネル空間に存在するため，カーネルの脆弱性により，攻撃を受ける可能性があるため，仮想記憶空間を分離することで，攻撃耐性を高めることが期待できる．これらの手法を検討する．

４．研究成果

（研究 1）について，以下の研究を行った．

（１）　OS カーネルへの脆弱性攻撃の無効化とセキュリティ機構の攻撃耐性向上の研究について，Linux OS において保護すべき OS 情報の拡大に伴い，オーバヘッドの増大が見込まれるため，表示機能などを評価し，オーバヘッドを軽減する機構を示した．

（２）　ゲスト OS の安全性を向上させるために，仮想化環境の基盤ソフトウェアである VMM 内に特権昇格攻撃を検知する手法を実現した．従来はシステムコール処理中の特権昇格攻撃のみ検知可能であったが，システムコール処理以外のタイミングでの特権昇格攻撃を検知できる手法を提案し，実現した．

（３）　Arm で利用されている TEE 環境である OP-TEE におけるセキュア実行環境の脅威について調査し，報告した．

（４）　IoT 機器などで利用されている Arm アーキテクチャについて，特権昇格攻撃を防止する手法を実現した．特に特権昇格攻撃を検知するセキュリティ機構自体を保護するために，TrustZone の機能を利用して保護する手法を実現し，評価した．この手法では，OS の特権情報をシステムコール呼び出し時に保存し，システムコール実行後に不正な変更がないかを監視する手法で，保存する権限情報を Arm 環境のセキュアワールドに保存する手法を実現した．

（５）　Linux カーネルの脆弱性を悪用する PoC（Proof of Concept）コードの実行により，実行されるカーネル関数をトレースにより明らかにする手法を検討し，実現した．この機能により，カーネルの脆弱性を緩和するために，どのような処理を制限すれば良いのかを把握することができる．

（研究 2）について，以下の研究を行った．

（１）　ゲスト OS で行われた処理を後で検証可能とするための VMM 側での証拠保全手法について検討した．この手法は，ゲスト OS 内および VMM 内で情報を取得し，ゲスト OS 内で取得した情報を VMM に安全に取得する手法も実現した．また，ゲスト OS 内のプログラム実行に関する情報を証跡として残す手法を提案し，実現した．

（２）　同一 VMM 上の VM 間の機密情報の拡散追跡と制御について検討した．同一 VMM 上の VM 間での情報を伝搬させる処理について検討し，ソケット通信と NFS で利用する RPC に着目して，機密情報の伝搬を把握する手法を検討し，基本方式を実現した．また，複数の VM を対象とした機密情報の追跡機能において，マルチコア CPU の複数コアを用いて追跡処理を実現する手法を提案し，有効性を示した．また，VM 内の機密情報の伝搬の追跡を，同時に複数の VM を対象に行う手法を実現し，評価結果を報告した．

（３）　デバッグレジスタの読み込み処理と書き込み処理を隠蔽する手法を提案し，提案手法がゲスト OS を監視していることを困難にする手法を実現した．VMM から VM を監視する手法について，デバッグレジスタを監視する手法を VM から隠蔽する 2 つの手法を比較評価した．また，デバッグレジスタを VM 監視に用いている場合に VM 上のゲスト OS からデバッグレジスタを利用できなかったが，デバッグレジスタを利用可能にし，デバッグレジスタの利用可否で監視機構の有無の判定を困難にする手法を実現した．さらに，VMM から VM のシステムコールをフックする箇所を自動的に推定する手法を提案し，有効性を示した．

（研究 3）について，以下の研究を行った．

（１）　セキュリティ機構の攻撃耐性向上のために，セキュリティ機構の存在する仮想記憶空間を分離する手法を提案した．Linux の仮想記憶空間のメモリマップと実装方法を調査し，仮想記憶空間上のカーネルのデータでどのデータをプロセス毎に分離できるか検討した．セキュリティ機構を別の仮想記憶空間で保護する機構を実現し，有効性を示した．

（２）　カーネルの攻撃耐性向上のために，カーネルの仮想記憶空間における排他的なページ利用手法についても基本方式を提案した．また，プロセス毎に排他的に利用するメモリ領域を実現する仮想記憶空間の管理手法を実現し，評価により，有効性を示した．また，カーネル空間のコードやデータを排他的に保護する機構を実現し，データだけでなく，脆弱性を含むことがあるコードも保護することを実現した．これは，OS カーネルの仮想記憶空間の一部のページを特定のシステムコール発行時にアクセス不可に変更する方法である．これにより，カーネル脆弱性を悪用した攻撃を困難化し，攻撃された場合でもセキュリティ機構や他プロセスのメモリの改ざんを防止できることが期待できる．

（３）　Linux におけるセキュリティ機構への攻撃困難化方式を実現するために，OS カーネルの仮想記憶空間をプロセス毎に複数用意し，一つのプロセスへのカーネル脆弱性を悪用した攻撃が，他のプロセスに影響しない方式を提案し，実現方式と評価結果を報告した．また，Linux カーネル用の仮想記憶空間を複数用意し，カーネルの脆弱性を悪用するコードの実行

により，重要なカーネルデータや保護機能のコードが改ざんされるのを防止する機構を検討し，有効性を示した.

（4） カーネル空間を監視するセキュリティ機構を，カーネルの仮想記憶空間とは別の空間に配置し，監視する手法を実現し，セキュリティ機構への攻撃を困難化する手法を実現した.

５．主な発表論文等

〔雑誌論文〕　計20件（うち査読付論文　20件／うち国際共著　0件／うちオープンアクセス　6件）

１．著者名 Kuzuno Hiroki、Yamauchi Toshihiro	４．巻 13720
２．論文標題 vkTracer: Vulnerable Kernel Code Tracing to?Generate Profile of?Kernel Vulnerability	５．発行年 2023年
３．雑誌名 Lecture Notes in Computer Science (LNCS)	６．最初と最後の頁 222～234
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-25659-2_16	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 Kuzuno Hiroki、Yamauchi Toshihiro	４．巻 30
２．論文標題 Mitigating Foreshadow Side-channel Attack Using Dedicated Kernel Memory Mechanism	５．発行年 2022年
３．雑誌名 Journal of Information Processing	６．最初と最後の頁 796～806
掲載論文のDOI（デジタルオブジェクト識別子） 10.2197/ipsjjip.30.796	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 Kuzuno Hiroki、Yamauchi Toshihiro	４．巻 30
２．論文標題 Prevention of Kernel Memory Corruption Using Kernel Page Restriction Mechanism	５．発行年 2022年
３．雑誌名 Journal of Information Processing	６．最初と最後の頁 563～576
掲載論文のDOI（デジタルオブジェクト識別子） 10.2197/ipsjjip.30.563	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 大谷航平，岡崎俊樹，山内利宏，森山英明，佐藤将也，谷口秀夫	４．巻 63
２．論文標題 複数のコアとVMに対応したKVM上の機密情報の拡散追跡機能の実現と評価	５．発行年 2022年
３．雑誌名 情報処理学会論文誌	６．最初と最後の頁 515～525
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 Sato Masaya、Omori Taku、Yamauchi Toshihiro、Taniguchi Hideo	4．巻 n/a
2．論文標題 Hook Point Estimation for System Call Detection by Virtual Machine Monitor	5．発行年 2022年
3．雑誌名 Proceedings of 2022 Tenth International Symposium on Computing and Networking Workshops	6．最初と最後の頁 358～362
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/CANDARW57323.2022.00069	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 Kuzuno Hiroki、Yamauchi Toshihiro	4．巻 13504
2．論文標題 KDPM: Kernel Data Protection Mechanism Using a Memory Protection Key	5．発行年 2022年
3．雑誌名 Lecture Notes in Computer Science (LNCS)	6．最初と最後の頁 66～84
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-15255-9_4	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 Sato Masaya、Nakamura Ryosuke、Yamauchi Toshihiro、Taniguchi Hideo	4．巻 n/a
2．論文標題 Improving Transparency of Hardware Breakpoints with Virtual Machine Introspection	5．発行年 2022年
3．雑誌名 Proceedings of 2022 11th International Congress on Advanced Applied Informatics (IIAI-AAI 2022)	6．最初と最後の頁 113～117
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/IIAIAAI55812.2022.00031	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 Hideaki Moriyama, Toshihiro Yamauchi, Masaya Sato, Hideo Taniguchi	4．巻 12
2．論文標題 Improvement and Evaluation of a Function for Tracing the Diffusion of Classified Information on KVM	5．発行年 2022年
3．雑誌名 Journal of Internet Services and Information Security (JISIS)	6．最初と最後の頁 26～43
掲載論文のDOI（デジタルオブジェクト識別子） 10.22667/JISIS.2022.02.28.026	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 Kuzuno Hiroki、Yamauchi Toshihiro	4．巻 9
2．論文標題 Mitigation of Kernel Memory Corruption Using Multiple Kernel Memory Mechanism	5．発行年 2021年
3．雑誌名 IEEE Access	6．最初と最後の頁 111651～111665
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2021.3101452	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 Otani Kohei、Okazaki Toshiki、Yamauchi Toshihiro、Moriyama Hideaki、Sato Masaya、Taniguchi Hideo	4．巻 n/a
2．論文標題 Function for Tracing Diffusion of Classified Information to Support Multiple VMs with KVM	5．発行年 2021年
3．雑誌名 Proceedings of 2021 Nineth International Symposium on Computing and Networking Workshops (CANDARW2021)	6．最初と最後の頁 352～358
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/CANDARW53999.2021.00066	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 Kuzuno Hiroki、Yamauchi Toshihiro	4．巻 12835
2．論文標題 KPRM: Kernel Page Restriction Mechanism to Prevent Kernel Memory Corruption	5．発行年 2021年
3．雑誌名 Lecture Notes in Computer Science (LNCS)	6．最初と最後の頁 45～63
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-85987-9_3	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 Nakamura Toru、Ito Hiroshi、Kiyomoto Shinsaku、Yamauchi Toshihiro	4．巻 12835
2．論文標題 (Short Paper) Evidence Collection and Preservation System with Virtual Machine Monitoring	5．発行年 2021年
3．雑誌名 Lecture Notes in Computer Science (LNCS)	6．最初と最後の頁 64～73
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-85987-9_4	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 Sato Masaya、Taniguchi Hideo、Nakamura Ryosuke	４．巻 none
２．論文標題 Virtual Machine Monitor-based Hiding Method for Access to Debug Registers	５．発行年 2020年
３．雑誌名 Proceedings of 2020 Eighth International Symposium on Computing and Networking (CANDAR)	６．最初と最後の頁 none
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/CANDAR51075.2020.00036	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 Moriyama Hideaki、Yamauchi Toshihiro、Sato Masaya、Taniguchi Hideo	４．巻 1264
２．論文標題 Improvement and Evaluation of a Function for Tracing the Diffusion of Classified Information on KVM	５．発行年 2020年
３．雑誌名 Advances in Networked-Based Information Systems, NBiS 2020, Advances in Intelligent Systems and Computing	６．最初と最後の頁 338～349
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-57811-4_32	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 Kuzuno Hiroki、Yamauchi Toshihiro	４．巻 12231
２．論文標題 MKM: Multiple Kernel Memory for Protecting Page Table Switching Mechanism Against Memory Corruption	５．発行年 2020年
３．雑誌名 Lecture Notes in Computer Science (LNCS)	６．最初と最後の頁 97～116
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-58208-1_6	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 Yamauchi Toshihiro、Akao Yohei、Yoshitani Ryota、Nakamura Yuichi、Hashimoto Masaki	４．巻 none
２．論文標題 Additional kernel observer: privilege escalation attack prevention mechanism focusing on system call privilege changes	５．発行年 2020年
３．雑誌名 International Journal of Information Security	６．最初と最後の頁 none
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10207-020-00514-7	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 KUZUNO Hiroki、YAMAUCHI Toshihiro	４．巻 E103.D
２．論文標題 Identification of Kernel Memory Corruption Using Kernel Memory Secret Observation Mechanism	５．発行年 2020年
３．雑誌名 IEICE Transactions on Information and Systems	６．最初と最後の頁 1462～1475
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2019ICP0011	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 福本 淳文, 山内 利宏	４．巻 61
２．論文標題 KVM上のゲストOSにおける権限の変更に着目した権限昇格攻撃防止手法	５．発行年 2020年
３．雑誌名 情報処理学会論文誌	６．最初と最後の頁 1507～1518
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 吉谷 亮汰, 山内 利宏	４．巻 61
２．論文標題 64-bit ARM環境における権限の変更に着目した権限昇格攻 撃防止手法	５．発行年 2020年
３．雑誌名 情報処理学会論文誌	６．最初と最後の頁 1531～1541
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 Kuzuno Hiroki, Yamauchi Toshihiro	４．巻 11879
２．論文標題 KMO: Kernel Memory Observer to Identify Memory Corruption by Secret Inspection Mechanism	５．発行年 2019年
３．雑誌名 Lecture Notes in Computer Science	６．最初と最後の頁 75～94
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-34339-2_5	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 －

〔学会発表〕　計31件（うち招待講演　0件／うち国際学会　7件）

１．発表者名
葛野弘樹，矢野智彦，面和毅，山内利宏

２．発表標題
脆弱性管理の調査を通じたソフトウェアサプライチェーンセキュリティの検討と考察

３．学会等名
第50回情報セキュリティ心理学とトラスト研究発表会

４．発表年
2023年

１．発表者名
大谷航平，小林論，山内利宏，谷口秀夫

２．発表標題
VM間通信に対応したKVM上の機密情報の拡散追跡機能の実現

３．学会等名
第100回コンピュータセキュリティ研究発表会

４．発表年
2023年

１．発表者名
Masaya Sato, Taku Omori, Toshihiro Yamauchi, Hideo Taniguchi

２．発表標題
Hook Point Estimation of Monitoring Address for System Call Detection by Virtual Machine Monitor

３．学会等名
9th International Workshop on Information and Communication Security (WICS 2022)（国際学会）

４．発表年
2022年

１．発表者名
葛野 弘樹，矢野 智彦，山内 利宏

２．発表標題
オープンソースソフトウェアに対するセキュリティリスク指標の提案と評価

３．学会等名
コンピュータセキュリティシンポジウム 2022 (CSS2022)

４．発表年
2022年

１．発表者名
大森 卓，佐藤 将也，山内 利宏，谷口 秀夫

２．発表標題
仮想計算機モニタによるシステムコール検知箇所の推定

３．学会等名
第21回情報科学技術フォーラム（FIT2022）

４．発表年
2022年

１．発表者名
葛野 弘樹，山内 利宏

２．発表標題
権限情報の動的な再配置による特権昇格攻撃防止手法の提案と評価

３．学会等名
第21回情報科学技術フォーラム（FIT2022）

４．発表年
2022年

１．発表者名
Hiroki Kuzuno, Toshihiro Yamauchi

２．発表標題
KDPM: Kernel Data Protection Mechanism Using a Memory Protection Key

３．学会等名
17th International Workshop on Security (IWSEC 2022)（国際学会）

４．発表年
2022年

１．発表者名
Hiroki Kuzuno, Toshihiro Yamauchi

２．発表標題
vkTracer: Vulnerable Kernel Code Tracing to Generate Profile of Kernel Vulnerability

３．学会等名
23rd World Conference on Information Security Applications (WISA 2022)（国際学会）

４．発表年
2022年

１．発表者名
Masaya Sato, Ryosuke Nakamura, Toshihiro Yamauchi, Hideo Taniguchi

２．発表標題
Improving Transparency of Hardware Breakpoints with Virtual Machine Introspection

３．学会等名
14th International Conference on E-Service and Knowledge Management (ESKM 2022)（国際学会）

４．発表年
2022年

１．発表者名
仲村 亮祐, 山内 利宏, 佐藤 将也, 谷口 秀夫

２．発表標題
監視プログラムのデバッグレジスタ利用をAPから隠蔽する手法の比較評価

３．学会等名
2022年電子情報通信学会総合大会

４．発表年
2022年

１．発表者名
大谷 航平, 山内 利宏, 森山 英明, 佐藤 将也, 谷口 秀夫

２．発表標題
マルチコアで動作するVMに対応したKVM上の機密情報の拡散追跡機能の評価

３．学会等名
コンピュータセキュリティシンポジウム 2021 (CSS2021) 論文集

４．発表年
2021年

１．発表者名
芝 海人, 葛野 弘樹, 山内 利宏

２．発表標題
OP-TEEのセキュアワールドにおける脅威の調査

３．学会等名
コンピュータセキュリティシンポジウム 2021 (CSS2021) 論文集

４．発表年
2021年

１．発表者名
葛野 弘樹, 山内 利宏

２．発表標題
カーネルにおけるMemory Protection Keyを用いた権限情報保護機構の提案

３．学会等名
コンピュータセキュリティシンポジウム 2021 (CSS2021) 論文集

４．発表年
2021年

１．発表者名
葛野 弘樹, 山内 利宏

２．発表標題
攻撃ユーザプロセスの利用するカーネルコードの追跡と特定手法の提案と評価

３．学会等名
第20回情報科学技術フォーラム (FIT2021) 講演論文集

４．発表年
2021年

１．発表者名
Otani Kohei、Okazaki Toshiki、Yamauchi Toshihiro、Moriyama Hideaki、Sato Masaya、Taniguchi Hideo

２．発表標題
Function for Tracing Diffusion of Classified Information to Support Multiple VMs with KVM

３．学会等名
8th International Workshop on Information and Communication Security (WICS2021)（国際学会）

４．発表年
2021年

１．発表者名
Kuzuno Hiroki、Yamauchi Toshihiro

２．発表標題
KPRM: Kernel Page Restriction Mechanism to Prevent Kernel Memory Corruption

３．学会等名
The 16th International Workshop on Security (IWSEC 2021)（国際学会）

４．発表年
2021年

１．発表者名
Nakamura Toru、Ito Hiroshi、Kiyomoto Shinsaku、Yamauchi Toshihiro

２．発表標題
(Short Paper) Evidence Collection and Preservation System with Virtual Machine Monitoring

３．学会等名
The 16th International Workshop on Security (IWSEC 2021)（国際学会）

４．発表年
2021年

１．発表者名
佐藤将也，谷口秀夫，仲村亮祐

２．発表標題
VMMによるデバッグレジスタの読み出しと書き込みの隠蔽手法の提案

３．学会等名
第184回マルチメディア通信と分散処理・第89回電子化知的財産・社会基盤合同研究発表会

４．発表年
2020年

１．発表者名
葛野 弘樹，山内 利宏

２．発表標題
カーネル仮想記憶空間における排他的ページ参照機構によるデータ保護能力と性能評価

３．学会等名
第19回情報科学技術フォーラム（FIT2020）

４．発表年
2020年

１．発表者名
葛野 弘樹，山内 利宏

２．発表標題
コンテナ向けカーネル仮想記憶空間の分離制御機構

３．学会等名
コンピュータセキュリティシンポジウム 2020（CSS2020）

４．発表年
2020年

１．発表者名
伊藤 寛史，中村 徹，清本 晋作，山内 利宏

２．発表標題
VMMによるプログラム実行時のライブラリ情報取得機能の設計

３．学会等名
2021年暗号と情報セキュリティシンポジウム（SCIS2021）

４．発表年
2021年

１．発表者名
葛野 弘樹，山内 利宏

２．発表標題
カーネル仮想記憶空間における排他的ページ参照機構の実現方式と性能評価

３．学会等名
電子情報通信学会第54回情報通信システムセキュリティ(ICSS)研究会

４．発表年
2021年

１．発表者名
葛野 弘樹，山内 利宏

２．発表標題
カーネル脆弱性を利用した攻撃に対する仮想記憶空間の切替え処理の保護と改ざん検出

３．学会等名
第18回情報科学技術フォーラム（FIT2019）

４．発表年
2019年

１．発表者名
福本 淳文，山内 利宏

２．発表標題
KVM上のゲストOSにおける権限の変更に着目した権限昇格攻撃防止手法の評価

３．学会等名
第18回情報科学技術フォーラム（FIT2019）

４．発表年
2019年

１．発表者名
吉谷 亮汰，山内 利宏

２．発表標題
64-bit ARM環境における権限の変更に着目した権限昇格攻撃防止手法の評価

３．学会等名
第18回情報科学技術フォーラム（FIT2019）

４．発表年
2019年

１．発表者名
森山 英明，山内 利宏，佐藤 将也，谷口 秀夫

２．発表標題
機密情報の拡散追跡機能におけるログ表示機能の実装

３．学会等名
2019年度 電気・情報関係学会九州支部連合大会

４．発表年
2019年

１．発表者名
福本 淳文，山内 利宏

２．発表標題
単一フックポイントのゲストOS監視による検知可能な権限昇格攻撃の拡大とオーバヘッド削減の実現

３．学会等名
コンピュータセキュリティシンポジウム 2019（CSS2019）

４．発表年
2019年

１．発表者名
吉谷 亮汰，山内 利宏

２．発表標題
権限昇格攻撃防止手法におけるARM TrustZoneを利用した権限の保護

３．学会等名
コンピュータセキュリティシンポジウム 2019（CSS2019）

４．発表年
2019年

１．発表者名
葛野 弘樹，山内 利宏

２．発表標題
カーネル仮想記憶空間における排他的ページ参照によるカーネルの攻撃耐性の実現と評価

３．学会等名
コンピュータセキュリティシンポジウム 2019（CSS2019）

４．発表年
2019年

１．発表者名
仲村 亮祐，佐藤 将也，谷口 秀夫

２．発表標題
デバッグレジスタの読み出しと書き込みの隠蔽手法の提案

３．学会等名
情報処理学会第82回全国大会

４．発表年
2020年

１．発表者名
伊藤 寛史，中村 徹，橋本 真幸，山内 利宏

２．発表標題
仮想計算機モニタによるプログラム実行の証拠保全システムの設計

３．学会等名
2020年電子情報通信学会総合大会

４．発表年
2020年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

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
研究分担者	谷口　秀夫 (Taniguchi Hideo) (70253507)	岡山大学・自然科学研究科・特命教授 (15301)	

6．研究組織（つづき）

	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
研究分担者	森山　英明 (Moriyama Hideaki) (00633009)	有明工業高等専門学校・創造工学科・准教授 (57102)	
研究分担者	佐藤　将也 (Sato Masaya) (30752414)	岡山県立大学・情報工学部・准教授 (25301)	

7．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

8．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関