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：８２７２３
研究種目：基盤研究(C)（一般）
研究期間：2017～2022
課題番号：１７Ｋ０６４５５

研究課題名（和文）自動復旧・運営維持可能な動的ネットワーク技術に関する先駆的研究

研究課題名（英文）Research on dynamic network technology capable of automatic recovery and operation maintenance

研究代表者

田中　秀磨（Tanaka, Hidema）

防衛大学校（総合教育学群、人文社会科学群、応用科学群、電気情報学群及びシステム工学群）・電気情報学群・教授

研究者番号：３０３２８５７０

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：当初はHWによる実証が主目的であったが、所属組織の移籍やSDN技術の展開の速さのため、予定していた研究計画は大幅に変更された。理論成果が主であり、擬似乱数性に基づいたセキュリティ技術の安全性評価、情報理論的手法やAI技術に基づいたセキュリティ技術の強度評価、グラフ理論に基づいたネットワーク防御手法に分類される。レベルが高い査読付き国際学会を含めて論文21件、学会発表7件であるが、コロナの影響により2019年以降の成果の勢いが削がれた結果となった。

研究成果の学術的意義や社会的意義
主たる研究成果は基礎理論にであるものの、実用性や現在のセキュリティ状況を鑑みたテーマを扱っている。ヒューリスティックに安全性が信じられ運用されている技術に関しても安全性の根拠を明らかにしたり、安全性を達成するための条件を明確にするなど、今後のセキュリティ技術の適用や実装に関する知見を提供できたという点で貢献は大きい。

研究成果の概要（英文）：At first, the main purpose was to demonstrate by HW simulations, but due to the change of the affiliated organization and the speed of deployment of SDN technology, the planned research activity was changed significantly. It is mainly based on theoretical results, and is classified into security evaluation methods based on pseudo-randomness, strength evaluation of security technology based on information theory methods and AI technology, and network defense method based on graph theory. There were 21 papers including high-level peer-reviewed international conferences, and 7 conference presentations.

研究分野：情報セキュリティ

キーワード：情報セキュリティ　ネットワークセキュリティ　擬似乱数　LWE問題　Integral property

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

SDN（Software Defined Networking）はネットワーク接続を動的にソフトウェア制御する技術であり、構成やルーター・スイッチの設定を柔軟に変更することができる。本研究の応募当時はそれほど普及しておらず、特にセキュリティ技術は VPN(Virtual Private Network)に頼っており、相互接続の信頼性やデータの完全生に関する話題は未成熟であった。しかしながら、特に企業における利用は爆発的に増加する傾向になり、特にコロナによる在宅勤務の増加によってトラフィックの管理とセキュリティの両立はいわば当たり前の状況になり、提案技術の考え方自体が遅れを取る結果となった。応募当時の提案者は、ここまで早く普及するとは考えていなかったが広く普及することは予測しており、理論的な研究内容に関しては既に着手していた。具体的には大量のログ解析、不正アクセス検知、DDoS 攻撃の効果向上とその対策、仮想化環境における脆弱性、ネットワークのトポロジーマップによる解析、暗号技術の安全性増強などである。

２．研究の目的

通信効率はネットワークの通信経路を柔軟に変化させることによって向上が可能である。そのための動的ネットワーク制御技術におけるセキュリティ対策として、速やかな攻撃検知のためのログ解析手法による不正アクセス検知や悪意あるサーバ(SDN を構成するサーバの裏切り)の発見がまず必要である。次に、サーバの乗っ取りの手始めとして実行される DDoS 攻撃に関して、その手法の多様性を鑑みて様々な手法と対策を検討する必要がある。また、SDN 環境を考えると実ネットワークだけでなく仮想化環境も考慮に入れる必要があり、本研究では仮想ネットワークも検討対象とした。さらに、ネットワークのトポロジーマップ解析により、弱点となり得るサーバの存在、または攻撃後の有効な迂回路の設定手法などの検討も行なった。この件に関しては、ロシア-ウクライナ戦争における、通信衛星の導入による迂回ネットワークの構築によりロシア側のサイバー攻撃がほぼ無効化されたことが記憶に新しい。また、通信効率の向上とセキュリティの向上は相反する要求であり、どうしてもセキュリティ技術は通信速度を低下させてしまう。また、鍵管理などユーザ側の負担も大きくヒューマンサイドの問題が大きくなる。この点は運営者側も同様であり、ユーザの大量の鍵管理などが安全性の弱点になる可能性が高い。この点に関しても現代暗号技術の観点から安全性増強とともに検討した。

しかしながら、上述したように現在では認証技術の多用、特に端末のカメラやセンサーを用いた生体認証との組み合わせ(多要素認証)が爆発的に普及したことや、耐量子計算機暗号を用いた手法の適用などにより、現実的には DDoS 攻撃などかなり primitive な攻撃戦略か、APT による運営者側の不正な運用など、いわばヒューマンエラーに基づく攻撃戦略に集約されつつある。特に Web ブラウザと連携したユーザ認証は飛躍的に安全性を高めており、上述の研究課題は提案から 2 年ほどで時代遅れとなった。また、本研究では攻撃戦略を検討し、これらに応じた総括的な対策手法の開発を行い攻撃後も運営維持可能であることを実機による実験ネットワークによる検証を目的としていた。しかしながら、応募者の所属研究室の変更によりこれが実現できず、さらに上述したような状況により、さらに理論研究を深める方向に変更した。具体的な目標変更と方法は次節で述べる。

３．研究の方法

変更された研究課題は以下のように新たに分類できる。

1) ログ解析手法による不正アクセス検知
2) DDoS 攻撃手法とその対策
3) ネットワークのトポロジーマップ解析
4) 現代暗号技術の安全性増強

3.1 ログ解析手法による不正アクセス検知

ログ解析は人間が直接処理することができない大量のデータを扱う必要がある。本研究では、AI と自然言語を組み合わせた手法を考察し、実験により有効性を確認した[3][4][5][7][8][16]。特に、自然言語的に未知攻撃の検知の可能性を明らかにした点は非常に有用であると考えられる。これは、古いデータベースによって学習したアルゴリズムは、新しいログ解析にどの程度対応できるかを実験によって確認することで結論できた。また通信データ量の時間変遷をフーリエ変換によりスペクトラム変換することで、攻撃パケットと通常パケットを見分ける手法も提案した[12]。

3.2 DDoS 攻撃手法とその対策

前述したように DDoS 攻撃の手法は実ネットワークを対象としたものの仮想ネットワークを対象としたものの 2 種類を検討した。実ネットワークを対象としたものも 2 種類の攻撃手法を検討した。1 つは、Slow Read DDoS 攻撃の攻撃効率の向上と対策である[6][13]。Slow Read DDoS 攻撃は意図的にサーバからの応答を遅らせ、ネットワークがダウンすることはないがアクセスがしにくい状況を維持する攻撃手法である。本研究で提案した攻撃手法により、既存の対策技術は

十分な安全性を実現できないことを明らかにした。提案手法は時間差を用いて連携してリクエストを送信するもので、タイムアウトで減少する que を補充しながらアクセス上限を維持するものである。対策手法は端末の認証を行うことであるが、現在の SDN 環境は十分安全な認証基盤に基づいており、攻撃者の身元を隠した状態でこのような攻撃を実行することは現実的には難しいと予想している。もう 1 つは、登録しているが利用していないドメインへのアクセスと執拗に繰り返す DNS に対する DDoS 攻撃である[10]。企業活動では、不正なドメイン名を使われることに対する対策として、事前に大量のドメイン名を登録しておき独占する傾向が見られる。実際には利用していないため、IP アドレスが割り振られていないのでリクエストはタイムアウトするが、大量にこのようなリクエストが来ると DNS が機能不全に陥る。現在では有効な対策は見つかっていないが、局所的な妨害であるため見過ごされている可能性が高い。SDN 環境における影響について今後も検討する必要がある。

仮想ネットワークを対象としたものは、仮想スイッチが機能不全になることを確認した[9]。SDN 環境ではないが、複数の OS が混在する統合システムなどでは大きな問題になる可能性が高い。しかしながら、例えば VMWare など多くの仮想環境ソフトウェアの最新バージョンでは既にこの問題は修正されている。

3.3 ネットワークのトポロジーマップ解析

ネットワークのトポロジーマップは隣接行列やラプラシアン行列などを用いて表現できる。これらの固有値解析により、情報の集中や分断とクラスタ分け(例えば全体を特定の 2 つの集合に分断し、それぞれ違う情報を流布させる、など)の実行のしやすさを評価できる[14]。本研究では、大規模なネットワークを対象とするため、所属組織が所有するダークネットログを用いて攻撃元の IP アドレスまでを traceroute で辿り、特定地域のトポロジーマップを導出した。そのトポロジーマップに対してサーバダウンや偽サーバの設置などの攻撃を行い、アクセス集中や異なる情報の流布に関する効果を検証した。その結果、必ずしも中心的役割を担うサーバを攻撃する必要はなく、周辺サーバの連結によっても高い効果が得られるトポロジーマップ形状があることを発見した。本研究は引き続き継続されており、現在では AS(Autonomous System)を対象としたものへ発展させ継続している。

3.4 現代暗号技術の安全性増強

セキュリティ技術の根幹は現在でも暗号技術に帰着されており、この点に関しても研究を実施した。内容は以下のように多岐に渡る。

・秘密分散に関する研究

再生符号と秘密分散の組み合わせによるデータの安全な保全手法について取り組んだ[15]。この手法は他の秘密分散手法によっても実現できるが、任意の条件に合致するシェアの生成手法を容易に導出できる特徴がある。この研究を通じて、ハミング重みを固定した一種の擬似乱数生成器の検討が必要になりその研究も実施した。このような特殊な乱数とその安全性は、視覚秘密分散のシェアの安全性の根幹にもなっていることを発見した[20]。視覚秘密分散は情報理論的安全性を達成できると示唆されていたが、この結果により、その達成には真性乱数が必要であり、シェア作成の生成行列によっては計算量的安全性しか達成できないことを明らかにした。

・暗号技術の安全性評価

代数的攻撃手法に対する安全性評価について検討を行なった[1][2][11][17]。主に計算機実験による検証であるが、数理計画法を用いるなど、いわゆる全数探索に頼らない手法を主に適用しこれまで見過ごされてきた特性を発見できた。ただし既存の安全性評価を更新することはなく、評価対象とした暗号の安全性を保証する結果となった。また、耐量子計算機暗号の 1 つである格子暗号の安全性根拠となっている LWE 問題について、その安全性予測としての指標となっている 2016 Estimate の検証に関しても実施した[19]。その結果、十分な安全性を有する大きなパラメータサイズに対してはその評価が妥当であるものの、実装性能重視で小さいパラメータを選択すると安全性が過大評価される危険性があることを明らかにした。

・その他

前述したように、最近の端末はセンサー類が豊富でありこれらを用いた多要素認証が爆発的に普及している。しかしながら、ユーザのプライバシー保護の面からは安全性とトレードオフになっている。この問題を解決するため、ユーザは自分の位置情報を直接伝えないが特定の場所にいることを示すプロトコルの提案を行なった[18]。また、最近のサイバー攻撃がユーザ自身を攻撃対象としているため、安全なパスワードの利用の必要性が高まっている。各ネットワークサービスなどは独自の安全基準を定めているが、同じパスワードであっても強度判定にばらつきが大きく、ユーザを混乱させている。この問題を解決するため、漏洩したパスワードの文字列の条件付き確率に基づいた自己エントロピー算出による強度評価手法を提案した[21]。

４．研究成果

上述したように、先行して理論研究を進めていたため、2017 年度成果が最も充実している。本来は、この内容をもとに検証する予定であった。査読付き国際学会を含めて論文 21 件(コロナの影響により終了年度を 1 年遅らせたため、2022 年度までの成果を挙げていることに注意)、国内学会発表 7 件である。特に 2020 年度以降はコロナの影響により研究活動が思うように進まず成果の勢いが削がれた。主たる研究成果は基礎理論であるものの、実用性や現在のセキュリティ状況を鑑みたテーマを扱っている点は強調したい。特にヒューリスティックに安全性が信じられ運用されている技術に関しても安全性の根拠を明らかにし、安全性を達成するための条件を明確にするなど、今後のセキュリティ技術の適用や実装に関する知見を提供できたという点で貢献は大きいと考える。

以下に査読付き国際学会以上の論文成果のみ挙げる。

2017 年度

[1] Haruhisa Kosuge, Hidema Tanaka: Improvements on Security Evaluation of AES against Differential Bias Attack. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. 100-A(11): 2398-2407 (2017)
[2] Haruhisa Kosuge, Hidema Tanaka: Differential Bias Attack for Block Cipher Under Randomized Leakage with Key Enumeration. AFRICACRYPT 2017. LNCS10239: 95-113
[3] Mamoru Mimura, Yuhei Otsubo, Hidehiko Tanaka, Hidema Tanaka: A Practical Experiment of the HTTP-Based RAT Detection Method in Proxy Server Logs. AsiaJCIS 2017: 31-37
[4] Mamoru Mimura, Hidema Tanaka: Long-Term Performance of a Generic Intrusion Detection Method Using Doc2vec. CANDAR 2017: 456-462
[5] Mamoru Mimura, Yuhei Otsubo, Hidema Tanaka, Atsuhiro Goto: Is Emulating "Binary Grep in Eyes" Possible with Machine Learning? CANDAR 2017: 337-343
[6] Shunsuke Tayama, Hidema Tanaka: Analysis of Effectiveness of Slow Read DoS Attack and Influence of Communication Environment. CANDAR 2017: 510-515
[7] Mamoru Mimura, Hidema Tanaka: Reading Network Packets as a Natural Language for Intrusion Detection. ICISC 2017. LNCS10779: 339-350
[8] Mamoru Mimura, Hidema Tanaka: Heavy Log Reader: Learning the Context of Cyber Attacks Automatically with Paragraph Vector. ICISS 2017. LNCS10717: 146-163
[9] Son Duc Nguyen, Mamoru Mimura, Hidema Tanaka: Leveraging Man-in-the-middle DoS Attack with Internal TCP Retransmissions in Virtual Network. ICISS 2017. LNCS10717: 367-386
[10] Bold Munkhbaatar, Mamoru Mimura, Hidema Tanaka: Dark Domain Name Attack: A New Threat to Domain Name System. ICISS 2017. LNCS10717: 405-414
[11] Haruhisa Kosuge, Hidema Tanaka: Theoretical Security Evaluation Against Side-Channel Cube Attack with Key Enumeration. LATINCRYPT 2017. LNCS11368: 145-165
[12] Hidema Tanaka: EFFECTIVENESS AND WEAKNESS OF QUANTIFIED/AUTOMATED ANOMALY BASED IDS. International Journal of Network Security & Its Applications. vol.9 no.6：1-11
[13] Shunsuke Tayama, Hidema Tanaka: Analysis of Slow Read DoS Attack and Communication Environment Mobile and Wireless Technologies 2017. LNEE425: 350-359
[14] Ayumi Ishimaru, Hidema Tanaka: A Study on Effectiveness of Network Attack Using Analysis of Eigenvalue. Mobile and Wireless Technologies 2017. LNEE425: 350-359

2018 年度

[15] Junta Imai, Mamoru Mimura, Hidema Tanaka: Verifiable Secret Sharing Scheme Using Hash Values. CANDAR Workshops 2018: 405-409
[16] Mamoru Mimura, Hidema Tanaka: A Linguistic Approach Towards Intrusion Detection in Actual Proxy Logs. ICICS 2018. LNCS11149: 708-718

2019 年度

[17] Hiroki Sato, Mamoru Mimura, Hidema Tanaka: Analysis of Division Property using MILP Method for Lightweight Blockcipher Piccolo. AsiaJCIS 2019: 48-55

2020 年度

[18] Hidema Tanaka, Keisuke Fukushima: Secure Calculation for Position Information of IoT Device with Few Communication and Small Secret Information. ICISS 2020. LNCS12553: 221-240

2021 年度

[19] Amane Takeshige, Haruhisa Kosuge, Hidema Tanaka: Experimental Verification of Estimated Block Size of BKZ Algorithm Against LWE. ICISS 2021. LNCS13146: 173-184

2022 年度(コロナにより終了年度を 1 年繰り下げ)

[20] Binh Le Thanh Thai, Hidema Tanaka, Kohtaro Watanabe: Improved scheme and evaluation method for progressive visual cryptography. EURASIP J. Inf. Secur. 2022(1): 9 (2022)
[21] Binh Thanh Thai Le, Hidema Tanaka: An analysis of password security risk against dictionary attacks. ISITA2022

５．主な発表論文等

〔雑誌論文〕　計17件（うち査読付論文　17件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Takeshige Amane、Kosuge Haruhisa、Tanaka Hidema	４．巻 LNCS 13146
２．論文標題 Experimental Verification of?Estimated Block Size of?BKZ Algorithm Against LWE	５．発行年 2021年
３．雑誌名 Book cover International Conference on Information Systems Security	６．最初と最後の頁 173～184
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-92571-0_11	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 Tanaka Hidema、Fukushima Keisuke	４．巻 LNCS 12553
２．論文標題 Secure Calculation for Position Information of IoT Device with Few Communication and Small Secret Information	５．発行年 2020年
３．雑誌名 Information System Security	６．最初と最後の頁 221～240
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-65610-2_14	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 Mamoru Mimura Hidema Tanaka	４．巻 11149
２．論文標題 A Linguistic Approach Towards Intrusion Detection in Actual Proxy Logs	５．発行年 2018年
３．雑誌名 Information and Communications Security - 20th International Conference	６．最初と最後の頁 708-718
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-01950-1_42	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 Kosuge Haruhisa、Tanaka Hidema	４．巻 10239
２．論文標題 Differential Bias Attack for Block Cipher Under Randomized Leakage with Key Enumeration	５．発行年 2017年
３．雑誌名 Progress in Cryptology - AFRICACRYPT 2017	６．最初と最後の頁 95, 113
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-57339-7_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 Haruhisa KOSUGE　Hidema TANAKA	4．巻 E100-A No.11
2．論文標題 Improvements on Security Evaluation of AES against Differential Bias Attack	5．発行年 2017年
3．雑誌名 IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 2398,2407
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E100.A.2398	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 Mamoru Mimura, Yuhei Otsubo, Hidehiko Tanaka, Hidema Tanaka	4．巻 1
2．論文標題 A Practical Experiment of the HTTP-Based RAT Detection Method in Proxy Server Logs	5．発行年 2017年
3．雑誌名 2017 12th Asia Joint Conference on Information Security (AsiaJCIS)	6．最初と最後の頁 31,37
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/AsiaJCIS.2017.13	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 Mamoru Mimura, Hidema Tanaka	4．巻 1
2．論文標題 Long-Term Performance of a Generic Intrusion Detection Method Using Doc2vec	5．発行年 2017年
3．雑誌名 Computing and Networking (CANDAR) 2017 Fifth International Symposium on	6．最初と最後の頁 456,462
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 Mamoru Mimura, Yuhei Otsubo, Hidema Tanaka, Atsuhiro Goto	4．巻 1
2．論文標題 Is Emulating "Binary Grep in Eyes" Possible with Machine Learning?	5．発行年 2017年
3．雑誌名 Computing and Networking (CANDAR) 2017 Fifth International Symposium on	6．最初と最後の頁 337,343
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 Shunsuke Tayama, Hidema Tanaka	４．巻 1
２．論文標題 Analysis of Effectiveness of Slow Read DoS Attack and Influence of Communication Environment	５．発行年 2017年
３．雑誌名 Computing and Networking (CANDAR) 2017 Fifth International Symposium on	６．最初と最後の頁 510,515
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 Mimura Mamoru、Tanaka Hidema	４．巻 10779
２．論文標題 Reading Network Packets as a Natural Language for Intrusion Detection	５．発行年 2018年
３．雑誌名 Information Security and Cryptology ICISC 2017	６．最初と最後の頁 339～350
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-78556-1_19	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 Mimura Mamoru、Tanaka Hidema	４．巻 10717
２．論文標題 Heavy Log Reader: Learning the Context of Cyber Attacks Automatically with Paragraph Vector	５．発行年 2017年
３．雑誌名 Information Systems Security	６．最初と最後の頁 146,163
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-72598-7_9	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 Nguyen Son Duc、Mimura Mamoru、Tanaka Hidema	４．巻 10717
２．論文標題 Leveraging Man-in-the-middle DoS Attack with?Internal TCP Retransmissions in?Virtual?Network	５．発行年 2017年
３．雑誌名 Information Systems Security	６．最初と最後の頁 367,386
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-72598-7_23	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 Munkhbaatar Bold、Mimura Mamoru、Tanaka Hidema	４．巻 10717
２．論文標題 Dark Domain Name Attack: A New Threat to?Domain Name System	５．発行年 2017年
３．雑誌名 Information Systems Security	６．最初と最後の頁 405～414
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-72598-7_25	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 Hidema Tanaka	４．巻 vol.9 no.6
２．論文標題 TOPOLOGY MAP ANALYSIS FOR EFFECTIVE CHOICE OF NETWORK ATTACK SCENARIO	５．発行年 2017年
３．雑誌名 International Journal of Computer Networks & Communications	６．最初と最後の頁 101, 117
掲載論文のDOI（デジタルオブジェクト識別子） 10.5121/ijcnc.2017.9608	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 Hidema Tanaka	４．巻 vol.9 no.6
２．論文標題 EFFECTIVENESS AND WEAKNESS OF QUANTIFIED/AUTOMATED ANOMALY BASED IDS	５．発行年 2017年
３．雑誌名 International Journal of Network Security & Its Applications	６．最初と最後の頁 1, 11
掲載論文のDOI（デジタルオブジェクト識別子） 10.5121/ijnsa.2017.9601	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 Shunsuke Tayama, Hidema Tanaka	４．巻 425
２．論文標題 Analysis of Slow Read DoS Attack and Communication Environment	５．発行年 2017年
３．雑誌名 Mobile and Wireless Technologies 2017	６．最初と最後の頁 350, 359
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-981-10-5281-1_38	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 Ayumi Ishimaru, Hidema Tanaka	４．巻 425
２．論文標題 A Study on Effectiveness of Network Attack Using Analysis of Eigenvalue	５．発行年 2017年
３．雑誌名 Mobile and Wireless Technologies 2017	６．最初と最後の頁 340, 349
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-981-10-5281-1_37	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6件（うち招待講演　0件／うち国際学会　2件）

１．発表者名 Hiroki Sato, Mamoru Miura, Hidema Tanaka
２．発表標題 Analysis of Division Property using MILP Method for Lightweight Blockcipher Piccolo
３．学会等名 The 14th Asia Joint Conference on Information Security (AsiaJCIS2019)（国際学会）
４．発表年 2019年

１．発表者名 Junta Imai, Mamoru Mimura, Hidema Tanaka
２．発表標題 Verifiable Secret Sharing Scheme Using Hash Values
３．学会等名 CANDAR Workshops 2018（国際学会）
４．発表年 2018年

１．発表者名 佐藤 寛樹、三村 守、田中 秀磨
２．発表標題 軽量ブロック暗号PiccoloのMILP手法を用いたDivision Propertyの検証
３．学会等名 コンピュータセキュリティシンポジウム2018
４．発表年 2018年

１．発表者名
今井淳太，三村守，田中秀磨

２．発表標題
排他的論理和を用いた消失訂正符号に基づく条件付き閾値秘密分散

３．学会等名
第16回　情報科学技術フォーラム(FIT 2017)

４．発表年
2017年

１．発表者名
ムンフバートル ボルド，三村守 ,田中秀磨

２．発表標題
DNS水責め攻撃効果に関する一考察

３．学会等名
第16回　情報科学技術フォーラム(FIT 2017)

４．発表年
2017年

１．発表者名
今井淳太，三村守，田中秀磨

２．発表標題
排他的論理和を用いた条件付き閾値秘密分散の構築

３．学会等名
第40回情報理論とその応用シンポジウム　(SITA2017)

４．発表年
2017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

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