サイバーセキュリティ研究所誌上発表論文一覧（2016 年 4 月–2024 年 3 月）

＊外部機関所属

■サイバーセキュリティ研究室

発表年月日	論文名	誌名/発表機関	巻号	発表者
2016/4/1	サイバーセキュリティの可視化技術	可視化情報学会　可視化情報学会誌	Vol.36 No.141 pp.27-31	井上 大介
2016/5/15	IoTPOT: A Novel Honeypot for Revealing Current IoT Threats	Journal of Information Processing	Vol.24 No.3 pp.522-533	Yin Minn Pa Pa*　Shogo Suzuki* Katsunari Yoshioka* Tsutomu Matsumoto*　笠間 貴弘 Christian Rossow*
2016/7/6	CROW: OpenFlow を用いた動的 web アクセス模倣システム	マルチメディア、分散、協調とモバイル（DICOMO2016）シンポジウム	pp.32-37	湯村 翼　高野 祐輝　安田 真悟 宮地 利幸
2016/7/7	次世代サイバー演習環境に向けて	マルチメディア、分散、協調とモバイル DICOMO2016 シンポジウム	Vol.2016 No.1 pp.1776-1782	太田 悟史　安田 真悟　湯村 翼 高野 祐輝
2016/7/7	ダークネット観測データを用いたボットネット分類手法の提案	マルチメディア、分散、協調とモバイル DICOMO2016 シンポジウム		土性 文哉＊　杉生 貴成＊　笠間 貴弘 佐々木 良一＊
2016/7/14	マルウェア対策のための研究用データセット -MWS Datasets 2016 -	情報処理学会　第 74 回コンピュータセキュリティ・第 19 回セキュリティ心理学とトラスト合同研究発表会		高田 雄太＊　寺田 真敏＊　村上 純一＊ 笠間 貴弘　吉岡 克成＊　畑田 充弘＊
2016/7/21	Towards Early Detection of Novel Attack Patterns through the Lens of A Large-Scale Darknet	The 13th IEEE International Conference on Advanced and Trusted Computing		班 涛　Shaoning Pang*　衛藤 将史 井上 大介　中尾 康二　Runhe Huang*
2016/7/27	A Neural Network Model for Detecting DDoS Attacks Using Darknet Traffic Features	The International Joint Conference on Neural Networks, 2016	Vol.2016 pp.2979-2985	Siti Hajar Aminah Ali*　小澤 誠一＊ 班 涛　中里 純二＊　島村 隼平
2016/8/1	Incremental and Decremental Max-Flow for Online Semi-Supervised Learning	IEEE Transactions on Knowledge And Data Engineering	Vol.28 pp.2115-2127	Lei Zhu*　Shaoning Pang* Abdolhossein Sarrafzadeh*　班 涛 井上 大介
2016/8/5	Integration of Multi-modal Features for Android Malware Detection Using Linear SVM	The 11th Asia Joint Conference on Information Security		班 涛　高橋 健志　Shanqing Guo 井上 大介　中尾 康二
2016/9/16	早期インシデント対応を目的とした DRDoS 攻撃アラートシステム	情報処理学会　情報処理学会論文誌	Vol.57 No.9 pp.1974-1985	牧田 大佑　西添 友美＊　吉岡 克成＊ 松本 勉＊　井上 大介　中尾 康二
2016/9/16	通信プロトコルのヘッダの特徴に基づく不正通信の検知手法	情報処理学会　情報処理学会論文誌	Vol.57 No.9 pp.1986-2002	小出 駿＊　鈴木 将吾＊　牧田 大佑 村上 洸介＊　笠間 貴弘　鈴木 未央 島村 隼平＊　衛藤 将史　井上 大介 中尾 康二　吉岡 克成＊　松本 勉＊
2016/9/20	SANDPRINT: Fingerprinting Malware Sandboxes to Provide Intelligence for Sandbox Evasion	The 19th International Symposium on Research in Attacks, Intrusions and Defenses (RAID2016)		Akira Yokoyama*　Kou Ishii* Rui Tanabe*　Yin Minn Pa Pa* Katsunari Yoshioka*　Tsutomu Matsumoto* 笠間 貴弘　井上 大介　Michael Brengel* Michael Backes*　Christian Rossow*
2016/9/21	Who Gets the Boot? Analyzing Victimization by DDoS-as-a-Service	The 19th International Symposium on Research in Attacks, Intrusions and Defenses (RAID2016)		Arman Noroozian*　Maciej Korczyński* Carlos Hernandez Gañan*　牧田 大佑 吉岡 克成＊　Michel van Eeten*
2016/9/28	FARIS: Fast and Memory-efficient URL Filter by Domain Specific Machine	International Conference on IT Convergence and Security 2016	pp.204-210	高野 祐輝　三浦 良介
2016/10/12	ダブルバウンスメールを活用した悪性メール対策の有効性	情報処理学会　コンピュータセキュリティシンポジウム 2016（CSS2016）		笠間 貴弘　神宮 真人　清水 雄介 井上 大介
2016/10/12	ダークネットトラフィックの可視化とオンライン更新によるモニタリング	情報処理学会　コンピュータセキュリティシンポジウム 2016（CSS2016）		畑中 拓哉＊　北園 淳＊　小澤 誠一＊ 班 涛　中里 純二＊　島村 隼平
2016/10/13	AmpPot を活用した DRDoS 攻撃対応早期化の取り組み	情報処理学会　コンピュータセキュリティシンポジウム 2016（CSS2016）		蒲谷 武正＊　千賀 渉＊　村上 洸介＊ 牧田 大佑　吉岡 克成＊　中尾 康二
2016/10/13	DRDoS ハニーポットが観測した CDN を回避する攻撃の分析	情報処理学会　コンピュータセキュリティシンポジウム 2016（CSS2016）		西添 友美＊　牧田 大佑　吉岡 克成＊ 松本 勉＊
2016/10/18	The Usability of Metadata for Android Application Analysis	The 2016 International Data Mining and Cybersecurity Workshop		高橋 健志　班 涛　Chin-Wei Tien* Chih-Hung Lin*　井上 大介　中尾 康二
2016/11/25	アクティブ観測結果に基づく攻撃元機器の分類手法	電子情報通信学会　情報通信システムセキュリティ研究会（ICSS）		笠間 貴弘　井上 大介
2016/12/1	NETorium: High-Fidelity Scalable Wireless Network Emulator	The 12th Asian Internet Engineering Conference (AINTEC 2016)	pp.25-32	明石 邦夫＊　井上 朋哉　安田 真悟 高野 祐輝　篠田 陽一
2016/12/7	Feature Subset Selection by SVM Ensemble	2016 IEEE Symposium Series on Computational Intelligence	pp.1-8	班 涛　井上 大介
2016/12/8	Distributed Incremental wLPSVM Learning	2016 IEEE Symposium Series on Computational Intelligence	Vol.2016 pp.1-8	Lei Zhu*　班 涛　Kazushi Ikeda* Shaoning Pang* Abdolhossein Sarrafzadeh*
2016/12/14	Generating Software Identifier Dictionaries from Vulnerability Database	International Conference on Privacy, Security and Trust		高橋 健志　井上 大介
2017/1/26	ダークネット観測による IoT 機器の脅威	電子情報通信学会　暗号と情報セキュリティシンポジウム（SCIS2017）		中里 純二＊　牧田 大佑　島村 隼平 井上 大介　中尾 康二

7　サイバーセキュリティ研究所誌上発表論文一覧

発表年月日	論文名	誌名/発表機関	巻号	発表者
2017/2/11	FARIS: Fast and Memory-efficient URL Filter on CPU and GPGPU	Journal of Convergence Security	Vol.2017 No.2 pp.23-58	高野 祐輝　三浦 良介
2017/3/4	Android マルウェア解析の検討	電子情報通信学会　東京支部学生会 第 22 回研究発表会		前原 一樹 *　笠間 貴弘　宮保 憲治 *
2017/3/13	プロトコル非準拠ハニーポットを用いた新種の DRDoS 攻撃の早期検知	電子情報通信学会　情報通信システムセキュリティ研究会 (ICSS)		西添 友美 *　牧田 大佑　吉岡 克成 *　松本 勉 *
2017/3/14	NIVAnalyzer: a Tool for Automatically Detecting and Verifying Next-Intent Vulnerabilities in Android Apps	IEEE International Conference on Software Testing, Verification and Validation 2017	Vol.2017 pp.1-8	Junjie Tang*　Xingmin Cui*　Ziming Zhao*　Shanqing Guo*　Xinshun Xu*　Chengyu Hu*　班 涛　Bing Mao*
2017/4/11	第 3 章 多層防御や感染後対策を汎用サーバに実装攻撃に強いネットワークの作り方 3 -4：被害発生！ 善後策に必要な情報保全	Software Design[別冊] シリーズ インフラエンジニア教本 ―セキュリティ実践技術編		遠峰 隆史
2017/5/8	An empirical study of third party APK's URL using scriptable API and fast identifier-specific filter	2017 IEEE 9th International Conference on Communication Software and Networks (ICCSN)		安藤 類央 *　高野 祐輝　三輪 信介
2017/8/6	Goods Recommendation Based on Retail Knowledge in a Neo4j Graph Database Combined with an Inference Mechanism Implemented in Jess	2017 IEEE Smart World Congress		Takahiro Kondo*　Runhe Huang*　班 涛　Chuanhe Huang*
2017/8/7	Practical Darknet Traffic Analysis: Methods and Case Studies	2017 IEEE Smart World Congress		班 涛　井上 大介
2017/9/15	大規模ダークネット観測と能動的スキャンによるマルウェア感染 IoT 機器の分類	情報処理学会　情報処理学会論文誌	Vol.58 No.9 pp.1388-1398	笠間 貴弘　井上 大介
2017/10/1	Malicious Events Grouping via Behavior Based Darknet Traffic Flow Analysis	Wireless Personal Communications	Vol.96 No.4 pp.5335-5353	Shaoning Pang*　Dan Komosny*　Ruibin Zhang*　Abdolhossein Sarrafzadeh*　班 涛　井上 大介
2017/10/24	ダークネットトラフィックデータの頻出パターン解析	情報処理学会　コンピュータセキュリティシンポジウム 2017 (CSS2017)		橋本 直輝 *　小澤 誠一 *　班 涛　中里 純二 *　島村 隼平
2017/10/24	サイバー攻撃誘引基盤 STARDUST	情報処理学会　コンピュータセキュリティシンポジウム 2017 (CSS2017)		津田 侑　遠峰 隆史　金谷 延幸　牧田 大佑　丑丸 逸人　神宮 真人　高野 祐輝　安田 真悟　三浦 良介　太田 悟史　宮地 利幸　神薗 雅紀 *　衛藤 将史　井上 大介　中尾 康二
2017/10/24	仮想マシン検知回避機能を持つ動的解析ツールの開発	情報処理学会　コンピュータセキュリティシンポジウム 2017 (CSS2017)		高田 一樹 *　岩本 一樹 *　津田 侑　遠峰 隆史　井上 大介
2017/10/24	マルウェアに実装されている仮想マシン検知機能の調査分析	情報処理学会　コンピュータセキュリティシンポジウム 2017 (CSS2017)		岩本 一樹 *　高田 一樹 *　津田 侑　遠峰 隆史　井上 大介
2017/10/28	A user mode implementation of filtering rule management plane using key-value store	2017 IEEE 17th International Conference on Communication Technology (ICCT)		安藤 類央 *　高野 祐輝　三輪 信介
2017/11/14	Detection of Botnet Activities through the Lens of A Large-Scale Darknet	The 24th International Conference on Neural Information Processing	Vol.10638 pp.442-451	班 涛　Lei Zhu*　島村 隼平　Shaoning Pang*　井上 大介　中尾 康二
2017/11/30	Evolving Cauchy Possibilistic Clustering and Its Application to Large-Scale Cyberattack Monitoring	2017 IEEE Symposium Series on Computational Intelligence	pp.2833-2839	Igor Skrjanc*　小澤 誠一 *　Dejan Dovzan*　班 涛　中里 純二 *　島村 隼平
2017/12/4	Web of cybersecurity: linking, locating, and discovering structured cybersecurity information	International Journal of Communication Systems		高橋 健志　パンタ ボーラ　門林 雄基　中尾 康二
2017/12/7	GINTATE: Scalable and Extensible Deep Packet Inspection System for Encrypted Network Traffic	The Eighth International Symposium on Information and Communication Technology (SoICT 2017)	pp.234-241	三浦 良介　高野 祐輝　三輪 信介　井上 朋哉
2018/1/1	Large-scale cyber attacks monitoring using Evolving Cauchy possibilistic clustering	Applied Soft Computing	Vol.62 pp.592-601	Igor Skrjanc*　小澤 誠一 *　班 涛　Dejan Dovzan*
2018/1/25	環境特徴情報による模擬環境自動構築効率化手法の提案と実装	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2018)		金谷 延幸　津田 侑　遠峰 隆史　安田 真悟　井上 大介
2018/1/25	複数のホスト情報を用いたプロセス異常検知	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2018)		中里 純二 *　津田 侑　高木 彌一郎　井上 大介　中尾 康二
2018/1/25	機械学習を用いた保全対象物選定システムの提案	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2018)		古田 悠人 *　津田 侑　上原 哲太郎 *
2018/1/26	標的型攻撃の被害範囲を迅速に分析するネットワークフォレンジック手法の提案	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2018)		海野 由紀 *　森永 正信 *　及川 孝徳 *　古川 和快 *　金谷 延幸　津田 侑　遠峰 隆史　井上 大介　鳥居 悟 *　伊豆 哲也 *　武仲 正彦 *
2018/3/7	Graphical Lasso を用いたダークネットデータのリアルタイム分析に基づくマルウェア活動検知に関する検討	電子情報通信学会　情報通信システムセキュリティ研究会 (ICSS)		韓 燦洙　島村 隼平　高橋 健志　井上 大介　川喜田 雅則 *　竹内 純一　中尾 康二
2018/3/8	HSDir の snooping と秘匿サービスへのスキャンを組み合わせたダークウェブ分析	電子情報通信学会　情報通信システムセキュリティ研究会 (ICSS)		小野 諒人 *　神薗 雅紀 *　笠間 貴弘　上原 哲太郎 *
2018/3/8	ハニーポットにより観測される DRDoS 攻撃の被害組織に関する分析	電子情報通信学会　情報通信システムセキュリティ研究会 (ICSS)		渡部 和也 *　西添 友美 *　牧田 大佑　森 博志 *　吉岡 克成 *　松本 勉 *
2018/3/23	COUNTER-INFILTRATION: FUTURE-PROOF COUNTER ATTACKS AGAINST EXPLOIT KIT INFRASTRUCTURE	Black Hat Asia 2018		Yin Minn Pa Pa*　Masaki Kamizono*　Horoshi Kumagai*　笠間 貴弘

発表年月日	論文名	誌名/発表機関	巻号	発表者
2018/4/18	A Darknet Traffic Analysis for IoT Malwares Using Association Rule Learning	The 3rd INNS Conference on Big Data and Deep Learning 2018		橋本 直輝＊　小澤 誠一＊　班 涛 中里 純二＊　島村 隼平
2018/6/26	Usable and Secure Cloud-based Biometric Authentication Solution for IoT Devices	IEEE Symposium on Computers and Communications		Chalee Vorakulpipat*　高橋 健志 Ekkachan Rattanalerdnusorn* Phithak Thaenkaew*　井上 大介
2018/6/26	Generative Adversarial Networks を利用したマルウェアの特徴量摘出手法に関する検討	電子情報通信学会　情報通信システムセキュリティ研究会（ICSS）	Vol.118 No.109 pp.77-82	古本 啓祐　伊沢 亮一　高橋 健志 井上 大介
2018/6/26	Twitter 中の異常投稿に対する自動分類の可能性についての考察	電子情報通信学会　情報通信システムセキュリティ研究会（ICSS）		牛込 龍太郎　松田 健＊　園田 道夫 高橋 健志　鈴木 未央　趙 晋輝＊
2018/6/28	Evasive Malware via Identifier Implanting	15th Conference on Detection of Intrusions and Malware & Vulnerability Assessment		Rui Tanabe*　Wataru Ueno*　Kou Ishii* Katsunari Yoshioka*　Tsutomu Matsumoto* 笠間 貴弘　井上 大介　Christian Rossow*
2018/7/9	Online Max-flow Learning via Augmenting and De-augmenting Path	2018 International Joint Conference on Neural Networks (a part of WCCI2018)		Pang Shaoning*　Zhu Lei　Ban Tao Ikeda Kazushi*　Zhang Wangfei* Sarrafzadeh Abdolhossein* Takahashi Takeshi　Inoue Daisuke
2018/7/15	歴史を紐解くセキュリティ技術，その現在，そして未来	情報処理学会　デジタルプラクティス	Vol.9 No.3	中尾 康二
2018/7/26	マルウェア対策のための研究用データセット -MWS Datasets 2018 -	情報処理学会　コンピュータセキュリティ研究発表会（CSEC）		高田 雄太＊　寺田 真敏＊　松木 隆宏＊ 笠間 貴弘　荒木 粧子＊　畑田 充弘＊
2018/7/26	非負値 Tucker 分解を用いたリアルタイムボットネット検知システムの構築	電子情報通信学会		金原 秀明　村上 佑磨＊　島村 隼平 高橋 健志　村田 昇　井上 大介
2018/8/4	Automatically Generating Malware Analysis Reports Using Sandbox Logs	IEICE TRANSACTIONS ON INFORMATION AND SYSTEMS		孫 博　藤野 朗稚＊　森 達哉＊　班 涛 高橋 健志　井上 大介
2018/8/9	A Lightweight Host-Based Intrusion Detection based on Process Generation Patterns	AsiaJCIS 2018 : The 13th Asia Joint Conference on Information Security		津田 侑　Junji Nakazato*　高木 彌一郎 井上 大介　中尾 康二　寺田 健次郎
2018/8/29	Comprehensible Categorization and Visualization of Orchestrated Malicious Domain Names using Linkage Analysis	The 16th Annual Conference on Privacy, Security and Trust 16th Annual Conference on Privacy, Security and Trust	pp.358-359	Shin-Ying Huang*　Tzu-Hsien CHUANG* Shi-Meng HUANG*　班 涛
2018/9/18	Android Application Analysis using Machine Learning Techniques	Intelligent Systems Reference Library	pp.181-205	高橋 健志　班 涛
2018/10/5	A Cross-Platform Study on IoT Malware	The 11th International Conference on Mobile Computing and Ubiquitous Networking		班 涛　伊沢 亮一　吉岡 克成＊ 井上 大介
2018/10/17	POSTER: Audio Hotspot Attack: 指向性スピーカを用いた音声認識機器への攻撃	The 25th ACM Conference on Computer and Communications Security	pp.2222-2224	飯島 涼　南 翔汰＊　Yunao Zhou* 竹久 達也　高橋 健志　及川 靖広＊ 森 達哉＊
2018/10/22	マルウェアデータセットに関する調査	情報処理学会　コンピュータセキュリティシンポジウム 2018（CSS2018）		東 結香＊　津田 侑
2018/10/22	研究用データセット「動的活動観測 2018」	情報処理学会　コンピュータセキュリティシンポジウム 2018（CSS2018）		寺田 真敏＊　佐藤 隆行＊　青木 翔＊ 亀川 慧＊　清水 努＊　津田 侑
2018/10/23	話題誘導するトピックモデルを用いたセキュリティレポート分類	情報処理学会　コンピュータセキュリティシンポジウム 2018（CSS2018）		永井 達也＊　乾 智裕＊　瀧田 愼＊ 古本 啓祐　白石 善明＊　髙野 泰洋＊ 毛利 公美＊　森井 昌克＊
2018/10/23	特定環境で動作するマルウェアへのセキュリティアプライアンスの耐性評価	情報処理学会　コンピュータセキュリティシンポジウム 2018（CSS2018）		田辺 瑠偉＊　上野 航＊　吉岡 克成＊ 松本 勉＊　齋藤 孝道＊　笠間 貴弘 井上 大介
2018/10/25	サイバー攻撃に対する能動的観測による収集データのモデル化と正規化手法	情報処理学会　コンピュータセキュリティシンポジウム 2018（CSS2018）		金谷 延幸　津田 侑　遠峰 隆史 高野 祐輝　井上 大介
2018/10/25	標的型攻撃の被害範囲を迅速に分析するネットワークフォレンジック手法の改良	情報処理学会　コンピュータセキュリティシンポジウム 2018（CSS2018）		海野 由紀＊　森永 正信＊　及川 孝徳＊ 古川 和快＊　金谷 延幸　津田 侑 遠峰 隆史　井上 大介　鳥居 悟＊ 伊豆 哲也＊
2018/11/21	ラベル情報を利用する敵対的生成モデルによるマルウェア解析手法の検討	電子情報通信学会　情報通信システムセキュリティ研究会（ICSS）		古本 啓祐　伊沢 亮一　高橋 健志 井上 大介
2018/11/21	話題誘導するトピックモデルを用いたセキュリティレポートからの攻撃傾向の把握	電子情報通信学会　情報通信システムセキュリティ研究会（ICSS）		永井 達也＊　乾 智裕＊　瀧田 愼＊ 古本 啓祐　白石 善明＊　毛利 公美＊ 髙野 泰洋＊　森井 昌克＊
2018/11/22	機械学習による脆弱性記述に基づく深刻度推定	電子情報通信学会　情報通信システムセキュリティ研究会（ICSS）		中川 舜太＊　永井 達也＊　金原 秀明 古本 啓祐　瀧田 愼＊　白石 善明＊ 高橋 健志　毛利 公美＊　髙野 泰洋＊ 森井 昌克＊
2018/12/6	ANTSdroid:Using RasMMA algorithm to generate Malware Behavior Characteristics of Android Malware Family	The 23rd IEEE Pacific Rim International Symposium on Dependable Computing (PRDC 2018)		Shun-Chieh Chang*　Yeali Sun* Wu Long Chuang*　Meng Chang Chen* 孫 博　高橋 健志
2019/1/13	Establishing Trusted and Timely Information Source using Social Media Services	IEEE Consumer Communications & Networking Conference		牛込 龍太郎　鈴木 未央　班 涛 高橋 健志　井上 大介　松田 健＊ 園田 道夫

7　サイバーセキュリティ研究所誌上発表論文一覧

発表年月日	論文名	誌名/発表機関	巻号	発表者
2019/1/22	サイバー攻撃観測のモデル化とデータ生成・変換手法	電子情報通信学会　暗号と情報セキュリティシンポジウム（SCIS2019）		金谷 延幸　津田 侑　高野 祐輝 井上 大介
2019/1/22	テンソルデータ拡充を用いた組織内ネットワーク攻撃判定方式	電子情報通信学会　暗号と情報セキュリティシンポジウム（SCIS2019）		及川 孝徳＊　西野 琢也＊　矢野 翔太郎＊ 海野 由紀＊　古川 知快＊　鳥居 悟＊ 伊豆 哲也＊　金谷 延幸　津田 侑 井上 大介
2019/1/22	全ポート待受型の簡易ハニーポットによるサイバー攻撃観測	電子情報通信学会　暗号と情報セキュリティシンポジウム（SCIS2019）		牧田 大佑　島村 隼平　久保 正樹 井上 大介
2019/1/22	Memcached ハニーポットによる DRDoS 攻撃の観測および攻撃元分析	電子情報通信学会　暗号と情報セキュリティシンポジウム（SCIS2019）		金銅 瑞樹＊　新谷 夏央＊　保泉 拓哉＊ 牧田 大佑　藤田 彬＊　吉岡 克成＊ 松本 勉＊
2019/1/22	ハニーポットにより観測される DRDoS 攻撃の影響評価	電子情報通信学会　暗号と情報セキュリティシンポジウム（SCIS2019）		新谷 夏央＊　金銅 瑞樹＊　保泉 拓哉＊ 牧田 大佑　藤田 彬＊　吉岡 克成＊ 松本 勉＊
2019/1/23	ダークネットトラフィック分析に基づくサイバー攻撃検知手法の評価	電子情報通信学会　暗号と情報セキュリティシンポジウム（SCIS2019）		韓 燦洙　島村 隼平　高橋 健志 井上 大介　竹内 純一　中尾 康二
2019/2/25	Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai	The Network and Distributed System Security Symposium (NDSS) 2019		Orcun Cetin*　Carlos Gañán* Lisette Altena*　笠間 貴弘　井上 大介 Kazuki Tamiya*　Ying Tie* Katsunari Yoshioka*　Michel van Eeten*
2019/2/28	Toward Automated Threat Detection and Actuation	CARIS2: Coordinating Attack Response at Internet Scale		高橋 健志　津田 侑　鈴木 宏栄 高木 彌一郎　井上 大介
2019/2/28	Toward Automated Vulnerability Handling	CARIS2: Coordinating Attack Response at Internet Scale		高橋 健志　金原 秀明　久保 正樹 村田 昇　井上 大介
2019/3/8	出力クラスを明示的に誘導可能な敵対的生成モデルを利用した脅威情報分析手法の検討	電子情報通信学会　情報通信システムセキュリティ研究会（ICSS）		古本 啓祐　金原 秀明　高橋 健志 白石 善明＊　井上 大介
2019/3/8	組織に対する脅威レポートのオントロジーを用いた生成	電子情報通信学会　情報通信システムセキュリティ研究会（ICSS）		永井 達也＊　瀧田 愼＊　古本 啓祐 白石 善明＊　毛利 公美＊　髙野 泰洋＊ 森井 昌克＊
2019/3/8	脅威情報のモデル化のためのセキュリティレポートからのイベント情報の抽出	電子情報通信学会　情報通信システムセキュリティ研究会（ICSS）		中川 舜太＊　永井 達也＊　金原 秀明 古本 啓祐　瀧田 愼＊　白石 善明＊ 高橋 健志　毛利 公美＊　髙野 泰洋＊ 森井 昌克＊
2019/3/8	Encoder-Decoder モデルを用いたセキュリティレポートに出現する用語の説明文の生成	電子情報通信学会　情報通信システムセキュリティ研究会（ICSS）		乾 智裕＊　永井 達也＊　中川 舜太＊ 古本 啓祐　瀧田 愼＊　白石 善明＊ 毛利 公美＊　髙野 泰洋＊　森井 昌克＊
2019/3/8	インシデント対応に特化したトラブルチケットシステム	電子情報通信学会　情報通信システムセキュリティ研究会（ICSS）	Vol.118 No.486 pp.197-202	津田 侑　遠峰 隆史　神宮 真人 岩崎 圭佑　寺田 健次郎　井上 大介
2019/4/10	A Scalable and Accurate Feature Representation Method for Identifying Malicious Mobile Applications	The 34th ACM Symposium on Applied Computing (SAC 2019)		孫 博　班 涛　Shun-Chieh Chang* Yeali S.Sun*　高橋 健志　井上 大介
2019/6/4	A study of IoT malware activities using association rule learning for darknet sensor data	International Journal of Information Security		Seiichi Ozawa*　班 涛　Naoki Hashimoto* Junji Nakazato*　Jumpei Shimamura*
2019/7/23	マルウェア対策のための研究用データセット -MWS Datasets 2019 -	情報処理学会　コンピュータセキュリティ研究発表会（CSEC）		荒木 粧子＊　笠間 貴弘　押場 博光＊ 千葉 大紀＊　畑田 充弘＊　寺田 真敏＊
2019/7/24	能動的攻撃観測環境における端末の自動駆動システム	電子情報通信学会　情報通信システムセキュリティ研究会（ICSS）	Vol.119 No.143 pp.299-304	安田 真悟　金谷 延幸　津田 侑 太田 悟史　三浦 良介　井上 大介
2019/7/25	スケーラブルで柔軟なトラフィック解析基盤の設計と実装	日本ソフトウェア科学会　学会誌「コンピュータソフトウェア」	Vol.36 No.3 pp.85-103	高野 祐輝　三浦 良介　安田 真悟 明石 邦夫＊　井上 朋哉
2019/8/1	Measurement Study Towards a Unified Firmware Updating Scheme for Legacy IoT Devices	The 14th Asia Joint Conference on Information Security(AsiaJCIS2019)	pp.9-15	Bing-Kai Hong*　Jr-Wei Huang*　班 涛 伊沢 亮一　Shin-Ming Cheng* 井上 大介　中尾 康二
2019/8/6	Real-Time Detection of Malware Activities by Analyzing Darknet Traffic Using Graphical Lasso	IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)		韓 燦洙　島村 隼平　高橋 健志 井上 大介　川喜田 雅則＊　竹内 純一 中尾 康二
2019/8/6	Anomaly Detection in Network Traffic Using Dynamic Graph Mining with a Sparse Autoencoder	IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)		Guanbo Jia*　Paul Miller*　Xin Hong* Harsha Kalutarage*　班 涛
2019/8/6	A Topic-based Unsupervised-learning Approach for Online Underground Market Exploration	IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)		Shin-Ying Huang*　班 涛
2019/9/1	Character-Level Convolutional Neural Network for Predicting Severity of Software Vulnerability from Vulnerability Description	IEICE Transactions on Information and Systems	Vol.E102-D No.9 pp.1679-1682	中川 舜太＊　永井 達也＊　金原 秀明 古本 啓祐　瀧田 愼＊　白石 善明＊ 高橋 健志　毛利 公美＊　髙野 泰洋＊ 森井 昌克＊
2019/9/1	A Cross-Platform Study on Emerging Malicious Programs Targeting IoT Devices	IEICE TRANSACTIONS ON INFORMATION AND SYSTEMS	Vol.102-D No.9 pp.1683-1685	班 涛　伊沢 亮一　Shin-Ying Huang* 吉岡 克成＊　井上 大介

発表年月日	論文名	誌名/発表機関	巻号	発表者
2019/9/15	標的端末上でのみ動作するマルウェアに対するセキュリティアプライアンスの有効性評価	情報処理学会　情報処理学会論文誌		田辺 瑠偉＊　上野 航＊　星澤 裕二＊ 齋藤 孝道＊　笠間 貴弘　井上 大介 吉岡 克成＊　松本 勉＊
2019/10/12	Message from the guest editors	International Journal of Information Security		高橋 健志　Rodrigo Roman Castro* Bilhanan Silverajan*　Ryan K L Ko* Said Tabet*
2019/10/22	サイバー攻撃観測における対象ネットワーク特化型ホワイトリスト作成手法の提案	情報処理学会　コンピュータセキュリティシンポジウム 2019（CSS2019）		金谷 延幸　津田 侑　高野 祐輝 井上 大介
2019/10/23	データセットの分布の違いを表現する指標の検討と予測結果の関係性分析	情報処理学会　コンピュータセキュリティシンポジウム 2019（CSS2019）		東 結香＊　津田 侑
2019/10/24	ダークネットトラフィックの分析に基づく継続的な広域ネットワークスキャンの調査	情報処理学会　コンピュータセキュリティシンポジウム 2019（CSS2019）		中川 雄太＊　藤田 彬＊　韓 燦洙 島村 隼平　高橋 健志　井上 大介 吉岡 克成＊
2019/11/13	高速な系統樹構成アルゴリズムの提案及びその評価	電子情報通信学会　情報通信システムセキュリティ研究会（ICSS）		何 天祥＊　韓 燦洙　伊沢 亮一 高橋 健志　来嶋 秀治＊　竹内 純一 中尾 康二
2019/11/19	Audio Hotspot Attack: An Attack on Voice Assistance Systems Using Directional Sound Beams and its Feasibility	IEEE Transactions on Emerging Topics in Computing	pp.1-1	飯島 涼　南 翔汰＊　Yunao Zhou* 竹久 達也　高橋 健志　及川 靖広＊ 森 達哉＊
2019/12/1	Understanding Attack Trends from Security Blog Posts Using Guided-Topic Model	Journal of Information Processing		永井 達也＊　瀧田 愼＊　古本 啓祐 白石 善明＊　Kelin Xia*　髙野 泰洋＊ 毛利 公美＊　森井 昌克＊
2019/12/4	サイバー攻撃解析共有プラットフォームを用いた悪性サイトの継続的観測	情報処理学会　コンピュータセキュリティ研究発表会（CSEC）		藤井 翔太＊　佐藤 隆行＊　青木 翔＊ 津田 侑　岡野 友輔＊　川口 信隆＊ 重本 倫宏＊　寺田 真敏＊
2019/12/10	Malicious URL Linkage Analysis and Common Pattern Discovery	International Workshop on Big Data Analytics for Cyber Threat Hunting (CyberHunt 2019)		Shin-Ying Huang*　Tzu-Hsien CHUANG* Shi-Meng HUANG*　班 涛
2019/12/11	サイバー攻撃観測における対象ネットワーク特化型ホワイトリスト作成手法の提案	International Workshop on Big Data Analytics for Cyber Threat Hunting (CyberHunt 2019)	pp.3190-3199	金谷 延幸　津田 侑　高野 祐輝 井上 大介
2019/12/14	A Fast Algorithm for Constructing Phylogenetic Trees with Application to IoT Malware Clustering	2019 - 26th International Conference on Neural Information Processing of the Asia-Pacific Neural Network Society		何 天祥＊　韓 燦洙　伊沢 亮一 高橋 健志　来嶋 秀治＊　竹内 純一 中尾 康二
2020/1/6	WD2 ISO/IEC 27035-1 Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management	ISO/IEC SC27 WG4 国際標準化活動における WD2 27035 -1 に対する寄書		久保 正樹
2020/1/29	関数呼び出しシーケンスに着目した IoT マルウェアの機能推定に関する考察	電子情報通信学会　暗号と情報セキュリティシンポジウム（SCIS2020）		川添 玲雄＊　韓 燦洙　伊沢 亮一 高橋 健志　竹内 純一
2020/2/6	Identifying Hidden and Potential Security Threats with Machine Learning Techniques	Data Science in Cybersecurity and Cyberthreat Intelligence		孫 博　高橋 健志　Lei Zhu　森 達哉＊
2020/2/6	Discovering Malicious URLs Using Machine Learning Techniques	Data Science in Cybersecurity and Cyberthreat Intelligence		孫 博　高橋 健志　Lei Zhu　森 達哉＊
2020/2/24	脆弱性情報の自動監視に基づく警告・初動対応自動化技術の構築	電子情報通信学会　情報通信システムセキュリティ研究会（ICSS）		高橋 健志　牛込 龍太郎　鈴木 未央 井上 大介
2020/2/26	IoT マルウェア感染ユーザへの ISP による通知のモデル化とシミュレーション	電子情報通信学会　暗号と情報セキュリティシンポジウム（SCIS2020）		中川 雄太＊　牧田 大佑　日名子 聡志＊ 田辺 瑠偉＊　吉岡 克成＊
2020/3/2	ログのカテゴリー変数に対するダミー変数と項目マッピングを用いた行列変換処理手法	第 12 回データ工学と情報マネジメントに関するフォーラム（第 18 回日本データベース学会年次大会）		輪島 幸治　Aminanto Muhamad Erza 班 涛　伊沢 亮一　高橋 健志 井上 大介
2020/3/2	ダークネット観測における大規模スキャナの判定指標の提案	電子情報通信学会　情報通信システムセキュリティ研究会（ICSS）		遠藤 由紀子　森 好樹　島村 隼平 久保 正樹
2020/3/2	Android 端末に対する JavaScript を用いたタイミング攻撃の検証	電子情報通信学会　情報通信システムセキュリティ研究会（ICSS）		杉田 敬亮＊　伊沢 亮一　森井 昌克＊
2020/3/2	AddressSanitizer を併用したデバイスドライバに対するファジングの有効性検証	電子情報通信学会　情報通信システムセキュリティ研究会（ICSS）		石井 健太郎＊　伊沢 亮一　森井 昌克＊
2020/3/3	セキュリティレポートの時系列トピックモデルを用いた分析	情報処理学会　SPT 研究会		長澤 龍成＊　古本 啓祐　瀧田 愼＊ 白石 善明＊　高橋 健志　毛利 公美＊ 髙野 泰洋＊　森井 昌克＊
2020/3/3	半教師ありトピックモデルによるセキュリティレポートの分類の評価方法について	情報処理学会　SPT 研究会		杉本 健太＊　長田 侑樹＊　瀧田 愼＊ 古本 啓祐　白石 善明＊　高橋 健志 毛利 公美＊　髙野 泰洋＊　森井 昌克＊
2020/3/3	トピックモデルとクラスタリングによるセキュリティレポートのマルチラベル分類	電子情報通信学会　情報通信システムセキュリティ研究会（ICSS）		長田 侑樹＊　瀧田 愼＊　古本 啓祐 白石 善明＊　高橋 健志　毛利 公美＊ 髙野 泰洋＊　森井 昌克＊
2020/3/3	コンセプトドリフトに対応した脆弱性記述に基づく脆弱性特性の自動評価 ～トピック固有単語を用いた特徴抽出手法～	電子情報通信学会　情報通信システムセキュリティ研究会（ICSS）		中川 舜太＊　古本 啓祐　白石 善明＊ 瀧田 愼＊　毛利 公美＊　森井 昌克＊
2020/3/3	Estimating Cyber Kill Chain Phases from Unstructured Technical Reports	情報処理学会　SPT 研究会		THEIN THIN THARAPHE*　江澤 友基＊ 中川 舜太＊　古本 啓祐　白石 善明＊ 中村 徹＊　橋本 真幸＊　毛利 公美＊ 森井 昌克＊

7　サイバーセキュリティ研究所誌上発表論文一覧

発表年月日	論文名	誌名/発表機関	巻号	発表者
2020/4/22	スパイクポイント調査のためのフラグフィールドとポート番号に基づくダークネットパケット分析	25th IEEE Symposium on Computers and Communications (ISCC 2020)		輪島 幸治　Aminanto Muhamad Erza 班 涛　伊沢 亮一　高橋 健志　井上 大介
2020/5/21	POSTER: Android IME Privacy Leakage Analyzer	The 41st IEEE Symposium on Security and Privacy		Peng Lo*　Jia-Chi Huo*　Hsu-Chun Hsiao* Bo Sun　班 涛　高橋 健志
2020/6/15	機械学習を用いたサイバーセキュリティ技術の発展	情報処理学会　学会誌「情報処理」	Vol.61 No.7 pp.672-677	高橋 健志　古本 啓祐　韓 燦洙
2020/6/25	エッジコンピューティングにおける SRv6 を用いたトラフィック誘導手法の提案	情報処理学会　DICOMO2020 シンポジウム	Vol.2020 No.1 pp.1033-1040	遠峰 隆史　名古屋 謙彦 *　阿部 博 * 岡田 和也 *
2020/7/8	Automation of Vulnerability Classification from its Description using Machine Learning	The 25th IEEE Symposium on Computers and Communications (ISCC 2020)		青田 雅輝 *　金原 秀明　久保 正樹 村田 昇　Bo Sun　高橋 健志
2020/8/21	IoT-Malware Detection based on Byte Sequences of Executable Files	The 15th Asia Joint Conference on Information Security	pp.143-150	Tzu-Ling Wan*　班 涛　Yen-Ting Lee* Shin-Ming Cheng*　伊沢 亮一 高橋 健志　井上 大介
2020/8/21	A Privacy-Preserving Federated Learning System for Android Malware Detection Based on Edge Computing	The 15th Asia Joint Conference on Information Security	pp.128-136	Ruei-Hau Hsu*　Yi-Cheng Wang* Chun-I Fan*　孫 博　班 涛　高橋 健志 Ting-Wei Wu*　Shang-Wei Kao*
2020/8/26	Disposable Botnets: Examining the Anatomy of IoT Botnet Infrastructure	The 15th International Conference on Availability, Reliability and Security Proceedings		田辺 瑠偉 *　玉井 達也 *　藤田 彬 * 伊沢 亮一　吉岡 克成 *　松本 勉 * Carlos Gañán*　Michel van Eeten*
2020/10/1	Real-time Detection of Global Cyberthreat Based on Darknet by Estimating Anomalous Synchronization Using Graphical Lasso	IEICE TRANSACTIONS ON INFORMATION AND SYSTEMS	Vol.E103-D No.10	韓 燦洙　島村 隼平　高橋 健志 井上 大介　竹内 純一　中尾 康二
2020/10/6	Efficient Detection and Classification of Internet-of-Things Malware Based on Byte Sequences from Executable Files	IEEE Open Journal of the Computer Society	Vol.1 pp.262-275	Tzu-Ling Wan*　班 涛　Shin-Ming Cheng* Yen-Ting Lee*　孫 博　伊沢 亮一 高橋 健志　井上 大介
2020/10/14	Tracing and Analyzing Web Access Paths Based on User-Side Data Collection: How Do Users Reach Malicious URLs?	The 23rd International Symposium on Research in Attacks, Intrusions and Defenses	pp.93-106	高橋 健志　Christopher Kruegel* Giovanni Vigna*　吉岡 克成 *　井上 大介
2020/10/26	プロアクティブなユーザ保護に向けた Web アクセスパスの分析とドメインリスク評価手法の提案	情報処理学会　コンピュータセキュリティシンポジウム 2020 (CSS2020)		高橋 健志　Christopher Kruegel* Giovanni Vigna*　吉岡 克成 *　井上 大介
2020/10/27	Make TrustZone Great Again	情報処理学会　コンピュータセキュリティシンポジウム 2020 (CSS2020)		高野 祐輝　金谷 延幸　津田 侑
2020/10/27	セキュリティ情報融合基盤 CURE	情報処理学会　コンピュータセキュリティシンポジウム 2020 (CSS2020)		津田 侑　井上 大介　鈴木 宏栄 高木 彌一郎　田中 秀一　金谷 延幸 竹本 亜希　古本 啓祐
2020/10/28	関数呼び出しシーケンスに着目した IoT マルウェアの機能差分調査	情報処理学会　コンピュータセキュリティシンポジウム 2020 (CSS2020)		川添 玲雄 *　韓 燦洙　伊沢 亮一 高橋 健志　竹内 純一
2020/10/28	トピックモデルを用いたセキュリティレポートのマルチラベリングのための分割重複入力	情報処理学会　コンピュータセキュリティシンポジウム 2020 (CSS2020)	pp.840-846	長澤 龍成 *　古本 啓祐　瀧田 愼 * 白石 善明 *　高橋 健志　毛利 公美 * 髙野 泰洋 *　森井 昌克 *
2020/10/28	セキュリティレポートのマルチラベル分類のためのトピックモデルの汎化性能に着目した外れ値検出の適用	情報処理学会　コンピュータセキュリティシンポジウム 2020 (CSS2020)	pp.847-852	長田 侑樹 *　瀧田 愼 *　古本 啓祐 白石 善明 *　高橋 健志　毛利 公美 * 髙野 泰洋 *　森井 昌克 *
2020/10/28	ポート番号埋め込みベクトルを用いたダークネットスキャンパケット解析	情報処理学会　コンピュータセキュリティシンポジウム 2020 (CSS2020)	pp.1010-1016	石川 真太郎 *　小澤 誠一 *　班 涛
2020/10/28	遠隔制御監視システムを模したハニーポットへのアクセス者の挙動の分析	情報処理学会　コンピュータセキュリティシンポジウム 2020 (CSS2020)		熊谷 拓洋 *　佐々木 貴之 *　藤田 彬 吉岡 克成 *　松本 勉 *
2020/11/5	Toward Automated Smart Ships:Designing Effective Cyber Risk Management	The 13th IEEE International Conference on Internet of Things (iThings 2020)	pp.100-105	古本 啓祐　Antti Kolehmainen* Bilhanan Silverajan*　高橋 健志 井上 大介　中尾 康二
2020/11/12	POSTER: Continuous and Multiregional Monitoring of Malicious Hosts	ACM Conference on Computer and Communications Security 2020 (ACM CCS 2020)		Shota Fujii*　Takayuki Sato*　Sho Aoki* 津田 侑　Yusuke Okano* Tomohiro Shigemoto* Nobutaka Kawaguchi*　Masato Terada*
2020/11/18	CDMC'19- the 10th International CybersecurityData Mining Competition	The 27th International Conference on Neural Information Processing	Vol.12533 No.2 pp.235-245	Shaoning Pang*　班 涛　Jungsuk Song* Kaizhu Huang*　Geongsen Poh* Iqbal Gondal*　Fadi Aloul*
2020/11/18	Port-piece Embedding for Darknet TrafficFeatures and Clustering of Scan Attacks	The 27th International Conference on Neural Information Processing	Vol.12533 pp.593-603	石川 真太郎 *　小澤 誠一 *　班 涛
2020/12/2	Threat Alert Prioritization Using Isolation Forest and Stacked Auto Encoder with Day-forward-chaining Analysis	IEEE Access	Vol.8 pp.217977-217986	Muhamad Erza Aminanto*　班 涛 伊沢 亮一　高橋 健志　井上 大介
2020/12/15	Paragraph-based Estimation of Cyber Kill Chain Phase from Threat Intelligence Reports	Journal of Information Processing	Vol.28 pp.1025-1029	THEIN THIN THARAPHE*　江澤 友基 * 中川 舜太 *　古本 啓祐　白石 善明 * 毛利 公美 *　髙野 泰洋 *　森井 昌克 *
2020/12/31	Monitoring Social Media for Vulnerability-Threat Prediction and Topic Analysis	IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)	pp.1771-1776	Shin-Ying Huang*　班 涛

発表年月日	論文名	誌名/発表機関	巻号	発表者
2021/1/1	Cross Platform IoT-Malware Family Classification Based on Printable Strings	IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)	pp.775-784	Yen-Ting Lee*　班 涛　Tzu-Ling Wan* Shin-Ming Cheng*　伊沢 亮一 高橋 健志　井上 大介
2021/1/20	非負値行列因子分解を用いたマルウェア活動検知手法の評価	電子情報通信学会　暗号と情報セキュリティシンポジウム（SCIS2021）		韓 燦洙　井上 大介　高橋 健志 竹内 純一
2021/1/20	セキュリティ情報検索のためのトピックモデルによるマルチラベリング	電子情報通信学会　暗号と情報セキュリティシンポジウム（SCIS2021）		長田 侑樹＊　瀧田 愼＊　古本 啓祐 白石 善明＊　高橋 健志　毛利 公美＊ 髙野 泰洋＊　森井 昌克＊
2021/1/21	Online URL Blacklist の現状調査と有用性に関する考察	電子情報通信学会　暗号と情報セキュリティシンポジウム（SCIS2021）		海崎 光宏　高橋 健志
2021/3/1	Salesforce Einstein Analytics を用いた IDS データからの脅威アラートスクリーニングの試み	2020 年度第 4 回（IOT 通算第 52 回）研究会	No.1 pp.1-8	輪島 幸治　高橋 健志　井上 大介
2021/3/1	高速な系統樹構成アルゴリズムにおけるスケーラブルなクラスタリング評価	電子情報通信学会　情報通信システムセキュリティ研究会（ICSS）		何 天祥＊　韓 燦洙　伊沢 亮一 高橋 健志　来嶋 秀治＊　竹内 純一
2021/3/1	IoT マルウェアの機能差分調査手法の改善及びクラスタに対する分析	電子情報通信学会　情報通信システムセキュリティ研究会（ICSS）		川添 玲雄＊　韓 燦洙　伊沢 亮一 高橋 健志　竹内 純一
2021/3/1	NIDS アラートに対する原因通信の抽出手法の提案及び考察	電子情報通信学会　情報通信システムセキュリティ研究会（ICSS）		石橋 亮典＊　後藤 大輝＊　韓 燦洙 班 涛　高橋 健志　竹内 純一
2021/3/2	標的端末に保存されたメールアドレスを用いたサンドボックス回避攻撃の概念実証	電子情報通信学会　情報通信システムセキュリティ研究会（ICSS）		井上 雄太＊　田辺 瑠偉＊　笠間 貴弘 井上 大介　吉岡 克成＊　松本 勉＊
2021/3/2	複数アンチウイルスエンジンにおける検出結果の不確実性の評価	電子情報通信学会　情報通信システムセキュリティ研究会（ICSS）		野村 和也＊　秋山 満昭＊　神薗 雅紀＊ 笠間 貴弘
2021/3/2	Memcached サーバを悪用した DRDoS 攻撃の観測および攻撃インフラの分析	電子情報通信学会　情報通信システムセキュリティ研究会（ICSS）		金銅 瑞樹＊　新谷 夏央＊　牧田 大佑 吉岡 克成＊　松本 勉＊
2021/3/16	ハニーポットにより観測される DRDoS 攻撃の影響評価と要因分析	情報処理学会　コンピュータセキュリティ研究発表会（CSEC）		新谷 夏央＊　牧田 大佑　吉岡 克成＊ 松本 勉＊
2021/3/16	ユーザ操作特定のためのカーネル内でのプロセス挙動収集手法	情報処理学会　コンピュータセキュリティ研究発表会（CSEC）		藤枝 慶弘＊　羽角 太地＊　島 成佳＊ 安田 真悟　鄭 俊俊＊　毛利 公一＊
2021/3/22	Investigating Behavioral Differences between IoT Malware via Function Call Sequence Graphs	ACM/SIGAPP Symposium On Applied Computing (SAC)		川添 玲雄＊　韓 燦洙　伊沢 亮一 高橋 健志　竹内 純一
2021/3/25	Designing Comprehensive Cyber Threat Analysis Platform: Can We Orchestrate Analysis Engines?	The 19th International Conference on Pervasive Computing and Communications (PerCom 2021)		高橋 健志　梅村 勇貴　韓 燦洙　班 涛 古本 啓祐　中村 大典　吉岡 克成＊ 竹内 純一　村田 昇　白石 善明＊
2021/3/26	IDS データ項目グループ化に基づく Tableau Desktop を用いた可視化の試み	第 142 回 情報基礎とアクセス技術研究発表会	No.9 pp.1-6	輪島 幸治　井上 大介
2021/4/26	Towards Efficient Labeling of Network Incident Datasets Using Tcpreplay and Snort	ACM Conference on Data and Application Security and Privacy (CODASPY)		倍味 幸平　韓 燦洙　班 涛　高橋 健志
2021/5/6	Partition-Then-Overlap Method for Labeling Cyber Threat Intelligence Reports by Topics over Time	IEICE Transactions on Information and Systems	Vol.E104-D No.5 pp.556-561	長澤 龍成＊　古本 啓祐　瀧田 愼＊ 白石 善明＊　高橋 健志　毛利 公美＊ 髙野 泰洋＊　森井 昌克＊
2021/5/14	FPGA によるソフトウェア解析環境「Iana」の提案	情報処理学会　第 93 回 CSEC 第 53 回 IOT 合同研究発表会		金谷 延幸　津田 侑　高野 祐輝 藤原 吉唯　伊沢 亮一　井上 大介
2021/5/19	Leveraging Machine Learning Techniques to Identify Deceptive Decoy Documents Associated With Targeted Email Attacks	IEEE Access	Vol.9 pp.87962-87971	孫 博　班 涛　韓 燦洙　高橋 健志 吉岡 克成＊　竹久 達也 Abdolhossein Sarrafzadeh* Meikang Qiu*　井上 大介
2021/7/15	User compliance and remediation success after IoT malware notifications	Journal of Cybersecurity	Vol.7 No.1 pp.1-21	Elsa Rodríguez*　Susanne Verstegen* Arman Noroozian*　井上 大介 笠間 貴弘　Michel van Eeten* Carlos H Gañán*
2021/7/19	コンピュータセキュリティシンポジウム CSS2020 開催報告 ～オンライン化を支えたシステムと UX～	情報処理学会　コンピュータセキュリティ研究発表会（CSEC）		白石 善明＊　掛井 将平＊　瀧田 愼＊ 磯部 光平＊　田宮 寛人＊　毛利 公美＊ 箕浦 翔悟＊　冨田 裕涼＊　古本 啓祐 廣友 雅徳＊　福田 洋治＊　池上 雅人＊ 甲斐 博＊　曽根 直人＊　森井 昌克＊
2021/7/20	ID/Password 設定に不備のある IoT 機器におけるマルウェア感染可能性の大規模調査	電子情報通信学会　情報通信システムセキュリティ研究会（ICSS）		村上 洸介　笠間 貴弘　井上 大介
2021/8/9	On-premises Analysis of Advanced Threat Prevention Appliances	14th USENIX Workshop on Cyber Security Experimentation and Test (CSET'21)		藤田 彬　班 涛　高橋 健志　井上 大介
2021/8/9	On-premises Analysis of Advanced Threat Prevention Appliances	The 14th Workshop on Cyber Security Experimentation and Test		藤田 彬　班 涛　高橋 健志　井上 大介
2021/8/9	Combat Security Alert Fatigue with AI-Assisted Techniques	The 14th Workshop on Cyber Security Experimentation and Test		班 涛　Ndichu Samuel　高橋 健志 井上 大介
2021/8/19	Which Packet Did They Catch? Associating NIDS Alerts with Their Communication Sessions	Asia Joint Conference on Information Security (AsiaJCIS)		石橋 亮典＊　後藤 大輝＊　韓 燦洙 班 涛　高橋 健志　竹内 純一
2021/8/27	Offline map matching using time-expanded graph for low-frequency data	Transportation Research Part C: Emerging Technologies	Vol.130	田中 智　立岩 斉明＊　秦 希望＊ 吉田 明広＊　若松 孝＊　長船 将太＊ 藤澤 克樹＊

7　サイバーセキュリティ研究所誌上発表論文一覧

発表年月日	論文名	誌名/発表機関	巻号	発表者
2021/9/9	Can ISPs Help Mitigate IoT Malware? A Longitudinal Study of Broadband ISP Security Efforts	6th IEEE European Symposium on Security and Privacy		Arman Noroozian　Elsa Turcios Rodriguez Elmer Lastdrager　笠間 貴弘 Michel van Eeten* Carlos Hernandez Ganan
2021/10/18	Detecting Android Malware and Classifying Its Families in Large-scale Datasets	ACM Transactions on Management Information Systems	Vol.13 No.2 pp.1-21	孫 博　班 涛　高橋 健志　井上 大介
2021/10/21	Automated Detection of Malware Activities Using Nonnegative Matrix Factorization	IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)		韓 燦洙　竹内 純一　高橋 健志 井上 大介
2021/10/21	Multi-label Positive and Unlabeled Learning and its Application to Common Vulnerabilities and Exposure Categorization	IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)		青田 雅輝 *　班 涛　高橋 健志　村田 昇
2021/10/26	Kitsune 特徴量を用いた悪性通信のパケット分類	情報処理学会　コンピュータセキュリティシンポジウム 2021 (CSS2021)		宮本 耕平 *　後藤 大輝 *　石橋 亮典 * 韓 燦洙　班 涛　高橋 健志　竹内 純一
2021/10/26	セキュリティ設定に不備のある IoT 機器の所有者に対する専用アプリを介した注意喚起の効果検証	情報処理学会　コンピュータセキュリティシンポジウム 2021 (CSS2021)		村上 颯人 *　藤田 彬　佐々木 貴之 * 田辺 瑠偉 *　山田 明　吉岡 克成 * 松本 勉 *
2021/10/27	遺伝的アルゴリズムに基づいた広域スキャンのフィンガープリント特定技術の提案	情報処理学会　コンピュータセキュリティシンポジウム 2021 (CSS2021)		田中 智　韓 燦洙　高橋 健志 藤澤 克樹 *
2021/10/27	悪性ホストの多拠点からの継続的な観測に基づく時系列および地域性の分析	情報処理学会　コンピュータセキュリティシンポジウム 2021 (CSS2021)	pp.357-364	藤井 翔太 *　佐藤 隆行 *　青木 翔 * 津田 侑　川口 信隆 *　重本 倫宏 * 寺田 真敏 *
2021/10/28	グラフ埋め込みを用いた IoT マルウェアの機能推定手法の改善の検討	情報処理学会　コンピュータセキュリティシンポジウム 2021 (CSS2021)		高田 智史 *　川添 玲雄 *　何 天祥 * 韓 燦洙　田中 智　竹内 純一
2021/10/28	Detecting Malicious Websites Based on JavaScript Content Analysis	情報処理学会　コンピュータセキュリティシンポジウム 2021 (CSS2021)	pp.727-732	Rozi Muhammad Fakhrur　班 涛 Sangwook Kim*　小澤 誠一 *　高橋 健志 井上 大介
2021/10/28	HTML タグの構造に着目したグラフ畳み込みネットワークによる悪性サイト判定	情報処理学会　コンピュータセキュリティシンポジウム 2021 (CSS2021)	pp.721-726	山本 貴巳 *　Kim Sangwook*　班 涛 高橋 健志　小澤 誠一 *
2021/10/28	HDL コードに対する SMT ソルバを用いた自動検証システムの提案	情報処理学会　コンピュータセキュリティシンポジウム 2021 (CSS2021)		伊沢 亮一　金谷 延幸　藤原 吉唯 竹久 達也　丑丸 逸人　有末 大 牧田 大佑　三村 聡志　末田 卓巳 井上 大介
2021/10/28	PPG センサを用いたウェアラブルデバイスに対する偽容積脈波提示攻撃に関する一考察	情報処理学会　コンピュータセキュリティシンポジウム 2021 (CSS2021)		竹久 達也　丑丸 逸人　牧田 大佑 有末 大　三村 聡志　末田 卓巳 飯島 涼 *　伊沢 亮一　井上 大介
2021/10/29	能動学習に基づいたマルウェア階層的クラスタリング	情報処理学会　コンピュータセキュリティシンポジウム 2021 (CSS2021)		何 天祥 *　韓 燦洙　高橋 健志 来嶋 秀治 *　竹内 純一
2021/10/29	異常同期性推定に基づくマルウェア活動の早期検知フレームワークの検討	情報処理学会　コンピュータセキュリティシンポジウム 2021 (CSS2021)		韓 燦洙　竹内 純一　高橋 健志 井上 大介
2021/12/6	Scalable and Fast Hierarchical Clustering of IoT Malware Using Active Data Selection	2021 Sixth International Conference on Fog and Mobile Edge Computing (FMEC)		何 天祥 *　韓 燦洙　高橋 健志 来嶋 秀治 *　竹内 純一
2021/12/6	Internet-Wide Scanner Fingerprint Identifier Based on TCP/IP Header	2021 Sixth International Conference on Fog and Mobile Edge Computing (FMEC)		田中 智　韓 燦洙　高橋 健志 藤澤 克樹 *
2021/12/7	Extracting Threat Intelligence Related IoT Botnet From Latest Dark Web Data Collection	The 14th IEEE International Conference on Internet of Things (iThings-2021)		古本 啓祐　海崎 光宏　藤田 彬 永田 貴彦 *　高橋 健志　井上 大介
2021/12/8	JStrack: Enriching Malicious JavaScript Detection Based on AST Graph Analysis and Attention Mechanism	The 28th International Conference on Neural Information Processing	Vol.13109 pp.669-680	Rozi Muhammad Fakhrur　班 涛 小澤 誠一*　Sangwook Kim*　高橋 健志 井上 大介
2021/12/14	IoT Malware Detection Using Function-Call-Graph Embedding	The 18th Annual International Conference on Privacy, Security and Trust (PST2021)	Vol.12 pp.1-9	Chia-Yi Wu*　班 涛　Shin-Ming Cheng* Bo Sun　高橋 健志
2021/12/15	単語のトピック固有度を用いた脆弱性記述に基づく脆弱性特性の自動評価	情報処理学会　情報処理学会論文誌	Vol.62 No.12 pp.1882-7764	中川 舜太 *　白石 善明 *　古本 啓祐 毛利 公美 *　森井 昌克 *
2021/12/17	A Machine Learning Approach to Detection of Critical Alerts from Imbalanced Multi-Appliance Threat Alert Logs	The Workshop on Cyber Threat Intelligence and Hunting with AI 2021		Ndichu Samuel　班 涛　高橋 健志 井上 大介
2021/12/22	Detecting web-based attacks with SHAP and tree ensemble machine learning methods	Applied Sciences	Vol.12 No.1	Ndichu Samuel　Sangwook Kim* 小澤 誠一 *　班 涛　高橋 健志 井上 大介
2022/1/18	標的型マルウェアの通信先情報に基づく C&C サーバ監視による攻撃誘引	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2022)		細見 勇介 *　津田 侑　鄭 俊俊 * 毛利 公一 *
2022/1/18	ハニーポットで観測される絨毯爆撃型 DRDoS 攻撃の分析	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2022)		毛 清昕 *　牧田 大佑　吉岡 克成 * 松本 勉 *
2022/2/1	Dark-TRACER: Early Detection Framework for Malware Activity Based on Anomalous Spatiotemporal Patterns	IEEE Access		韓 燦洙　竹内 純一　高橋 健志 井上 大介
2022/3/7	WebUI のコンテンツ情報と画像特徴量を組み合わせた IoT 機器特定手法	電子情報通信学会　第 58 回 ICSS/SPT 合同研究会		村上 洸介　笠間 貴弘　藤田 彬 浦川 順平 *　井上 大介

発表年月日	論文名	誌名/発表機関	巻号	発表者
2022/3/8	マルウェア感染ユーザへの ISP による注意喚起活動のシミュレーション	電子情報通信学会　第 58 回 ICSS/SPT 合同研究会		黄 緒平＊　望月 俊輔＊　藤田 彬 吉岡 克成＊
2022/3/8	BERT モデルを用いたキーボード打鍵音による入力推定攻撃とその対策	電子情報通信学会　第 58 回 ICSS/SPT 合同研究会		飯田 雅裕＊　秋山 満昭＊　神薗 雅紀＊ 笠間 貴弘　服部 祐一＊　井上 博之＊ 猪俣 敦夫＊
2022/3/8	関数呼び出しシーケンスグラフとクラスタリングを用いた IoT マルウェアの機能分析	電子情報通信学会　第 58 回 ICSS/SPT 合同研究会		高田 智史＊　何 天祥＊　韓 燦洙 田中 智　竹内 純一
2022/3/8	HDL コードに対する SMT ソルバを用いた入力パターン自動生成に関する検討	電子情報通信学会　ハードウェアセキュリティ研究会（HWS）		伊沢 亮一　金谷 延幸　藤原 吉唯 竹久 達也　丑丸 逸人　有末 大 牧田 大佑　三村 聡志　井上 大介
2022/3/24	Malicious Packet Classification Based on Neural Network Using Kitsune Features	International Conference on Intelligent Systems and Patterns Recognition		宮本 耕平＊　後藤 大輝＊　石橋 亮典＊ 韓 燦洙　班 涛　高橋 健志　竹内 純一
2022/5/17	Cyber-Physical Firewall: Monitoring and Controlling the Threats Caused by Malicious Analog Signals	The 7th International Workshop on Malicious Software and Hardware in the Internet of Things-IoT 2022		飯島 涼＊　竹久 達也　森 達哉＊
2022/5/18	NEMIANA: Cross-Platform Execution Migration for Debugging	3rd ACM/IEEE International Conference on Automation of Software Test		金谷 延幸　津田 侑　高野 祐輝 藤原 吉唯　伊沢 亮一　井上 大介
2022/5/19	SenseInput: An Image-Based Sensitive Input Detection Scheme for Phishing Website Detection	IEEE International Conference on Communictions		Shih-Chun Lin*　Pang-Cheng Wu* Hong-Yen Chen*　Tomohiro Morikawa* 高橋 健志　Tsung-Nan Lin*
2022/5/25	Exposed Infrastructures: Discovery, Attacks and Remediation of Insecure ICS Remote Management Devices	The 43rd IEEE Symposium on Security and Privacy		佐々木 貴之＊　藤田 彬 Carlos Hernandez Ganan* Michel van Eeten*　吉岡 克成＊　松本 勉*
2022/6/1	Generating Labeled Training Datasets Towards Unified Network Intrusion Detection Systems	IEEE Access		石橋 亮典＊　宮本 耕平＊　韓 燦洙 班 涛　高橋 健志　竹内 純一
2022/6/23	実機を使用した不正ログイン後の IoT 機器悪用可能性の調査	電子情報通信学会　第 59 回 ICSS/IA 合同研究会		村上 洸介　笠間 貴弘　井上 大介
2022/6/23	IoT Botnet Detection Based on the Behaviors of DNS Queries	2022 IEEE Conference on Dependable and Secure Computing (DSC)		Chun-I Fan　Cheng-Han Shie* Che-Ming Hsu*　班 涛　森川 智博＊ 高橋 健志
2022/6/30	Amplification Chamber: Dissecting the Attack Infrastructure of Memcached DRDoS Attacks	The 19th Conference on Detection of Intrusions and Malware & Vulnerability Assessment	Vol.13358 pp.178-196	Mizuki Kondo*　Rui Tanabe* Natsuo Shintani*　牧田 大佑 Katsunari Yoshioka* Tsutomu Matsumoto*
2022/7/1	Flexible Function Estimation of IoT Malware Using Graph Embedding Technique	27th IEEE Symposium on Computers and Communications (ISCC 2022)		大塩 慶＊　高田 智史＊　韓 燦洙 田中 智　竹内 純一
2022/7/2	Public Blocklist Provider の特徴理解	27th IEEE Symposium on Computers and Communications (ISCC 2022)		海崎 光宏　森川 智博＊　藤田 彬 高橋 健志　Tsung-Nan Lin*　井上 大介
2022/8/7	Cybersecurity Comic: An Image Change to “Cool Cybersecurity” Findings and Challenges to Raise Children’s Security Awareness	the Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022 Posters)		Jennifer Friedauer*　Harunobu Yagi* Nissy Sombatruang　Youki Kadobayashi* Daisuke Miyamoto*　藤田 彬
2022/8/8	Understanding Non-Experts’ Security and Privacy Related Questions on a Q&A Site	Symposium on Usable Privacy and Security (SOUPS)		長谷川 彩子　山下 直美＊　森 達哉＊ 井上 大介　秋山 満昭＊
2022/8/15	Security-Alert Screening with Oversampling Based on Conditional Generative Adversarial Networks	The 17th ASIA Joint Conference on Information Security		Ndichu Samuel　班 涛　高橋 健志 井上 大介
2022/8/16	An HDL Simulator with Direct Register Access for Improving Code Coverage	The 17th Asia Joint Conference on Information Security (AsiaJCIS 2022)		伊沢 亮一　金谷 延幸　藤原 吉唯 竹久 達也　丑丸 逸人　有末 大 牧田 大佑　三村 聡志　井上 大介
2022/8/31	RTL 回路に対するファジングを用いたバグ検出の有効性評価	DA シンポジウム 2022 －システムと LSI の設計技術－		伊沢 亮一　藤原 吉唯　金谷 延幸 井上 大介
2022/9/1	サイバーセキュリティの観点でのドローン	電子情報通信学会誌	Vol.105 No.9 pp.1130-1135	竹久 達也　古本 啓祐　中尾 康二
2022/9/13	継続的かつ複数拠点からの観測に基づく悪性サイトのクローキング調査	第 21 回情報科学技術フォーラム（FIT 2022）	Vol.4 pp.9-16	藤井 翔太＊　佐藤 隆行＊　青木 翔＊ 津田 侑　川口 信隆＊　重本 倫宏＊ 寺田 真敏＊
2022/9/15	サイバーセキュリティ DX を促進する自動化技術の発展	情報処理学会　学会誌「情報処理」		高橋 健志
2022/9/15	Disposable Botnets: Long-term Analysis of IoT Botnet Infrastructure	Journal of Information Processing	Vol.30 pp.577-590	田辺 瑠偉＊　渡辺 露文＊　藤田 彬 伊沢 亮一　Carlos Ganan* Michel van Eeten*　吉岡 克成＊ 松本 勉＊
2022/10/24	系統樹に基づくスケーラブルなマルウェアクラスタリングのオンライン処理手法の実装と評価	情報処理学会　コンピュータセキュリティシンポジウム 2022（CSS2022）		何 天祥＊　韓 燦洙　田中 智　高橋 健志 竹内 純一
2022/10/24	パケット単位分類に基いたセッション単位での通信分類	情報処理学会　コンピュータセキュリティシンポジウム 2022（CSS2022）		宮本 耕平＊　武石 啓成＊　飯田 昌澄＊ 韓 燦洙　班 涛　高橋 健志　竹内 純一
2022/10/26	アジャイル型のサイバー攻撃解析用模擬 ICT 環境構築・管理システム	情報処理学会　コンピュータセキュリティシンポジウム 2022（CSS2022）		金谷 延幸　津田 侑　遠峰 隆史 鈴木 悦子　佐藤 茂　田中 秀一 井上 大介
2022/10/26	ダークウェブからの収集情報を利用したマーケットサイト間の販売トレンドの分析とライフサイクル推定	情報処理学会　コンピュータセキュリティシンポジウム 2022（CSS2022）		古本 啓祐　海崎 光宏　藤田 彬 永田 貴彦＊　高橋 健志　井上 大介

7　サイバーセキュリティ研究所誌上発表論文一覧

発表年月日	論文名	誌名/発表機関	巻号	発表者
2022/10/26	オープンソースソフトウェアを活用して構築した 5G コアネットワークのセキュリティ評価	情報処理学会　コンピュータセキュリティシンポジウム 2022 (CSS2022)		澤本 敏郎　遠峰 隆史　鈴木 未央 井上 大介　中尾 康二
2022/10/26	Explainable Artificial Intelligence for Cybersecurity:A Literature Survey	Annals of Telecommunications		Charmet Fabien Tanuwidjaja Harry Chandra Solayman Ayoubi* Pierre-Francois Gimenez*　Yufei Han* Houda Jmila*　Gregory Blanc* 高橋 健志　Zonghua Zhang*
2022/10/26	Multi-labeling with topic models for searching security information	Annals of Telecommunications	Vol.77 pp.777-788	長田 侑樹 *　長澤 龍成 *　白石 善明 * 瀧田 愼 *　古本 啓祐　高橋 健志 毛利 公美 *　森井 昌克 *
2022/10/27	ダークネット解析に基づくマルウェア活動の早期検知フレームワークの有効性の検証と今後の拡張	情報処理学会　コンピュータセキュリティシンポジウム 2022 (CSS2022)		韓 燦洙　田中 智　高橋 健志
2022/10/27	フィンガープリントを用いたスキャナの分類及び宛先ポートセットの分析	情報処理学会　コンピュータセキュリティシンポジウム 2022 (CSS2022)		田中 智　韓 燦洙　高橋 健志
2022/10/27	VirusTotal と Web アクセスログを用いた URL ブロックリストの作成・管理手法の改良	情報処理学会　コンピュータセキュリティシンポジウム 2022 (CSS2022)		平石 知佳 *　高尾 恭平 *　高田 一樹 * Charmet Fabien　藤田 彬　井上 大介 田辺 瑠偉 *　吉岡 克成 *　松本 勉 *
2022/11/7	ダークネット解析に基づくスキャンキャンペーンの追跡手法の提案	電子情報通信学会　情報通信システムセキュリティ研究会 (ICSS)		韓 燦洙　田中 智　高橋 健志 竹内 純一
2022/11/8	脆弱な IoT 機器管理用パスワードの設定状況と注意喚起効果の分析	電子情報通信学会　情報通信システムセキュリティ研究会 (ICSS)		村上 洸介　笠間 貴弘　井上 大介
2022/11/8	コンシューマ向け IoT 機器のサポートポリシーの設定・開示状況の調査	電子情報通信学会　情報通信システムセキュリティ研究会 (ICSS)		笠間 貴弘　村上 洸介　藤田 彬 井上 大介
2022/11/24	Service Function Chaining security survey: Addressing security challenges and threats	Elsevier, Computer Networks		Montida Pattaranantakul* Chalee Vorakulpipat*　高橋 健志
2022/12/13	IoT Malware Classification Based on Reinterpreted Function-Call Graphs	Computer & Security	Vol.126 No.103060	Chia-Yi Wu*　班 涛　Shin-Ming Cheng* 高橋 健志　井上 大介
2022/12/15	学内 CSIRT と連携した学生自主運用型マルウェア対策教育プログラムの提案	情報処理学会　情報処理学会論文誌	Vol.63 No.12 pp.1716-1725	松井 紘大 *　前田 幸平 *　青木 翔 * 藤田 圭佑 *　津田 侑　寺田 真敏 *
2022/12/15	Understanding the Influence of AST-JS for Improving Malicious Webpage Detection	Applied Sciences	Vol.24	Rozi Muhammad Fakhrur　小澤 誠一 * 班 涛　Sangwook Kim*　高橋 健志 井上 大介
2022/12/17	Darknet Analysis-Based Early Detection Framework for Malware Activity: Issue and Potential Extension	2022 IEEE International Conference on Big Data		韓 燦洙　田中 智　高橋 健志
2022/12/17	Critical-Threat-Alert Detection using Online Machine Learning	2022 IEEE International Conference on Big Data		Ndichu Samuel　班 涛　高橋 健志 井上 大介
2022/12/31	Experiences, Behavioral Tendencies, and Concerns of Non-Native English Speakers in Identifying Phishing Emails	Journal of Information Processing (JIP)		長谷川 彩子　山下 直美 *　秋山 満昭 * 森 達哉 *
2023/1/23	Scalable and Fast Algorithm for Constructing Phylogenetic Trees with Application to IoT Malware Clustering	IEEE Access		何 天祥 *　韓 燦洙　伊沢 亮一 高橋 健志　来嶋 秀治 *　竹内 純一
2023/2/1	各種脅威インテリジェンスの横断分析に関する研究動向について	電子情報通信学会　学会誌	Vol.106 No.2 pp.143-148	森川 智博 *　古本 啓祐
2023/2/3	AI-Assisted Security Alert Data Analysis with Imbalanced Learning Methods	Applied Sciences	Vol.13 No.3 pp.1-22	Ndichu Samuel　班 涛　高橋 健志 井上 大介
2023/2/23	Towards Long-Term Continuous Tracing of Internet-Wide Scanning Campaigns Based on Darknet Analysis	International Conference on Information Systems Security and Privacy		韓 燦洙　田中 智　竹内 純一 高橋 健志　Tomohiro Morikawa* Tsung-Nan Lin*
2023/2/27	Detecting Coordinated Internet-Wide Scanning by TCP/IP Header Fingerprint	IEEE Access		田中 智　韓 燦洙　高橋 健志
2023/3/3	Multimodal Feature Integration for High-Accuracy Network Intrusion Detection	International Conference on Computer Applications and Information Security (ICCAIS)		飯田 昌澄 *　宮本 耕平 *　川中 翔太 * 武石 啓成 *　韓 燦洙　班 涛　高橋 健志 竹内 純一
2023/3/6	日米の産業界におけるパブリックおよび自社製のセキュア開発ガイドラインの利用実態調査	情報処理学会　コンピュータセキュリティ研究発表会 (CSEC)		金井 文宏 *　長谷川 彩子　塩治 榮太朗 * 秋山 満昭 *
2023/3/13	高精度なネットワーク侵入検知のための特徴量の統合	電子情報通信学会　情報通信システムセキュリティ研究会 (ICSS)		飯田 昌澄 *　宮本 耕平 *　武石 啓成 * 川中 翔太 *　韓 燦洙　班 涛　高橋 健志 竹内 純一
2023/3/13	単語埋め込みと LSTM を用いたパケット単位異常通信分類モデルに関する考察	電子情報通信学会　情報通信システムセキュリティ研究会 (ICSS)		柏原 芳克 *　宮本 耕平 *　飯田 昌澄 * 川中 翔太 *　韓 燦洙　班 涛　高橋 健志 竹内 純一
2023/3/13	Web 管理画面への不正ログイン成功時の悪用リスク調査	電子情報通信学会　情報通信システムセキュリティ研究会 (ICSS)	Vol.122 No.422 pp.91-96	村上 洸介　笠間 貴弘　井上 大介
2023/3/13	ロールプレイング型調査に基づくマルウェア感染通知の実効性分析	電子情報通信学会　情報通信システムセキュリティ研究会 (ICSS)		藤田 彬　松田 美慧　笠間 貴弘 井上 大介
2023/3/13	セキュリティ専門用語辞書の構築に関する一考察	電子情報通信学会　情報通信システムセキュリティ研究会 (ICSS)		松田 美慧　藤田 彬　津田 侑 piyokango*　井上 大介

発表年月日	論文名	誌名/発表機関	巻号	発表者
2023/3/13	VirusTotal と Web アクセスログを用いた URL 警告リストの作成・管理手法の提案	電子情報通信学会　情報通信システムセキュリティ研究会（ICSS）		高尾 恭平＊　平石 知佳＊　高田 一樹＊ 藤田 彬＊　井上 大介　田辺 瑠偉＊ 吉岡 克成＊　松本 勉＊
2023/3/14	Can’t Stop The Scan: インターネットスキャンのオプトアウト実態調査	電子情報通信学会　情報通信システムセキュリティ研究会（ICSS）	Vol.122 No.422 pp.169-174	笠間 貴弘　遠藤 由紀子　久保 正樹 井上 大介
2023/3/15	Simulating and Estimating the Effectiveness of Security Notification by ISP to Malware-Infected Users	情報処理学会　情報処理学会論文誌	Vol.64 No.3	黄 緒平＊　望月 俊輔＊　藤田 彬 吉岡 克成＊
2023/4/14	動的情報フロー追跡によるハードウェアトロジャン検出支援システムの提案	電子情報通信学会　ハードウェアセキュリティ研究会（HWS）	Vol.123 No.6 pp.26-31	伊沢 亮一　金谷 延幸　井上 大介
2023/4/25	Analyzing the Use of Public and In-house Secure Development Guidelines in U.S. and Japanese Industries	CHI 2023		金井 文宏＊　長谷川 彩子　塩治 榮太朗＊ 秋山 満昭＊
2023/5/9	Work in Progress: New Seed Set Selection Method of the Scalable Method for Constructing Phylogenetic Trees	ACM International Conference on Computing Frontiers		何 天祥＊　韓 燦洙　田中 智　高橋 健志 竹内 純一
2023/5/29	Breaking Alert Fatigue: AI-Assisted SIEM Framework forEffective Incident Response	Applied Sciences	Vol.13 No.6610 pp.1-29	班 涛　高橋 健志　Ndichu Samuel 井上 大介
2023/6/29	Towards Functional Analysis of IoT Malware Using Function Call Sequence Graphs and Clustering	IEEE Annual Computers, Software, and Applications Conference (COMPSAC)		大塩 慶＊　高田 智史＊　何 天祥＊ 韓 燦洙　田中 智　高橋 健志 竹内 純一
2023/7/7	Birds of a Feather? A Comparative Analysis of DDoS Victimisation by IoT Botnet and Amplification Attacks	The 22nd Workshop on the Economics of Information Security (WEIS)		Swaathi Vetrive＊　Arman Noroozian＊ 牧田 大佑　Katsunari Yoshioka＊ Michel van Eeten＊　Carlos H. Gañán＊
2023/7/11	FINISH: Efficient and Scalable NMF-based Federated Learning for Detecting Malware Activities	IEEE Transactions on Emerging Topics in Computing		Yu-Wei Chang＊　Hong-Yen Chen＊ 韓 燦洙　Tomohiro Morikawa＊ 高橋 健志　Tsung-Nan Lin＊
2023/7/12	Color-coded Attribute Graph: Visual Exploration of Distinctive Traits of IoT-Malware Families	ISCC 2023 : International Symposium on Computers and Communications		Jiaxing Zhou＊　班 涛 Tomohiro Morikawa＊　高橋 健志 井上 大介
2023/8/7	User Comprehension of Technical Terms in Privacy Policies and Expectations of the Privacy Protection Law in Japan	SOUPS2023 Poster		金森 祥子　池田 美穂＊　亀石 久美子＊ 長谷川 彩子
2023/8/9	Internet Service Providers’ and Individuals’ Attitudes, Barriers, and Incentives to Secure IoT	31st USENIX Security Symposium		Sombatruang Nisamanee　Ingolf Becker＊ Tristan Caulfield＊　藤田 彬　笠間 貴弘 中尾 康二　井上 大介
2023/8/15	Packet-Level Intrusion Detection Using LSTM Focusing on Personal Information and Payloads	Asia Joint Conference on Information Security (AsiaJCIS)		川中 翔太＊　柏原 芳克＊　宮本 耕平 飯田 昌澄＊　韓 燦洙　班 涛　高橋 健志 竹内 純一
2023/9/1	A Large-Scale Investigation into the Possibility of Malware Infection of IoT Devices with Weak Credentials	IEICE Transactions on Information and Systems	Vol.E106D No.9 pp.1316-1325	村上 洸介　笠間 貴弘　井上 大介
2023/9/1	Mitigate: Toward Comprehensive Research and Development for Analyzing and Combating IoT Malware	電子情報通信学会　英文論文誌 D	Vol.106 No.9 pp.1302-1315	Koji Nakao＊　Katsunari Yoshioka＊ Takayuki Sasaki＊　Rui Tanabe＊ Xuping Huang＊　高橋 健志　藤田 彬 Jun’ichi Takeuchi＊　Noboru Murata＊ Junji Shikata＊　Kazuki Iwamoto＊ Kazuki Takada＊　Yuki Ishida＊ Masaru Takeuchi＊　Naoto Yanai＊
2023/9/15	絨毯爆撃型 DRDoS 攻撃の実態把握に向けた DRDoS ハニーポット観測データの分析	情報処理学会　情報処理学会論文誌	Vol.64 No.9 pp.1266-1276	毛 清昕＊　牧田 大佑　吉岡 克成＊ 松本 勉＊
2023/9/19	Detecting Malicious JavaScript Using Structure-Based Analysis of Graph Representation	IEEE Access	Vol.11 pp.102727	Rozi Muhammad Fakhrur　班 涛 小澤 誠一＊　山田 明＊　高橋 健志 Kim Sangwook＊　井上 大介
2023/9/25	Peering into the Darkness: The Use of UTRS in Combating DDoS Attacks	28th European Symposium on Research in Computer Security	Vol.14345 pp.23-41	Radu Anghel＊　Swaathi Vetrivel＊ Elsa Turcios Rodriguez＊ Kaichi Sameshima＊　牧田 大佑 Katsunari Yoshioka＊　Yury Zhauniarovich＊
2023/9/30	Analysis of Non-Experts’ Security- and Privacy-Related Questions on a Q&A Site	IEICE Transactions on Information and Systems	Vol.106D No.9 pp.1380-1396	長谷川 彩子　秋山 満昭＊　山下 直美＊ 井上 大介　森 達哉＊
2023/10/31	検索を起点として偽ショッピングサイトに到達するユーザの振る舞いの調査	情報処理学会　コンピュータセキュリティシンポジウム 2023（CSS2023）		才納 明英＊　高田 一樹＊　藤田 彬 小出 駿＊　金井 文宏＊　秋山 満昭＊ 田辺 瑠偉＊　吉岡 克成＊　松本 勉＊
2023/10/31	パケット単位の特徴量に基づいた通信の逐次的な早期分類	情報処理学会　コンピュータセキュリティシンポジウム 2023（CSS2023）		宮本 耕平　韓 燦洙　班 涛　高橋 健志 竹内 純一
2023/11/1	プライバシーポリシーに使用される技術用語および個人情報保護法に対するユーザの理解度の調査	情報処理学会　コンピュータセキュリティシンポジウム 2023（CSS2023）	pp.1012-1019	金森 祥子　池田 美穂＊　亀石 久美子＊ 長谷川 彩子
2023/11/1	インターネットスキャナのクラスタ追跡可能性評価	情報処理学会　コンピュータセキュリティシンポジウム 2023（CSS2023）		韓 燦洙　田中 智　高橋 健志
2023/11/1	オンライン詐欺や犯罪へ誘導する SNS 投稿文の類型化と特徴の分析	情報処理学会　コンピュータセキュリティシンポジウム 2023（CSS2023）		松田 美慧　川口 大翔＊　藤田 彬 吉岡 克成＊

7　サイバーセキュリティ研究所誌上発表論文一覧

発表年月日	論文名	誌名/発表機関	巻号	発表者
2023/11/1	Understanding the Different Perspectives of VPN Users	情報処理学会　コンピュータセキュリティシンポジウム 2023 (CSS2023)		Moore Lachlan　Mori Tatsuya*
2023/11/17	日本を狙ったテクニカルサポート詐欺の手口に関する実態調査	電子情報通信学会　情報通信システムセキュリティ研究会 (ICSS)		伊東 大幸　梶本 幸佑 *　影山 徹哉 * 青木 太一 *　笠間 貴弘　井上 大介
2023/11/17	コンシューマ向けルータにおける初期 Wi-Fi パスワードの推測可能性調査	電子情報通信学会　情報通信システムセキュリティ研究会 (ICSS)		笠間 貴弘　神野 亮 *　萩原 雄一 * 井上 大介
2023/11/21	Consolidating Packet-Level Features for Effective Network Intrusion Detection: A Novel Session-Level Approach	IEEE Access		宮本 耕平　飯田 昌澄 *　韓 燦洙　班 涛 高橋 健志　竹内 純一
2023/11/30	Model Selection for Continuous Operation\\ of Automated Vulnerability Assessment System	Workshop on Recent Advances in Resilient and Trustworthy ML Systems in Autonomous Networks (ARTMAN)	pp.11-15	Jung Soohyun*　古本 啓祐　高橋 健志 白石善明 *
2023/11/30	Hybrid Explainable Intrusion Detection System: Global vs. Local Approach	ARTMAN2023, ACM CCS Workshop		Tanuwidjaja Harry Chandra Takahashi Takeshi　Tsungnan Lin* Boyi Lee*　Ban Tao
2023/12/7	One Million ASUS Routers Under Control: Exploiting ASUS DDNS to MITM Admin Credentials	Black Hat Europe		久保 正樹　森 好樹　奥川 莞多 *
2023/12/17	Machine Learning–Based Security Alert Screening with Focal Loss	2023 IEEE International Conference on Big Data		Ndichu Samuel　Ban Tao Takahashi Takeshi　Inoue Daisuke
2024/1/23	耐誘導コミュニケーション研究のための生成 AI を用いた会話生成	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2024)		角尾 幸保 *　松田 美慧　藤部 果帆 *
2024/1/23	アクティブスキャンによる IoT デバイスフィンガープリントを利用したマルウェア感染端末数の推定	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2024)		宮武 和咲 *　遠藤 由紀子　山田 明 * 班 涛　高橋 健志　小澤 誠一 *
2024/1/24	Cloak-Bench：大規模言語モデルによるセキュリティ分析の定量的評価方法の提案 - フィッシングキットのクローキング検出への応用	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2024)		中野 瑠人 *　山田 明 *　班 涛 高橋 健志　小澤 誠一 *
2024/2/26	VPN Awareness and Misconceptions: A Comparative Study in Canadian and Japanese Contexts	NDSS USEC 2024		Moore Lachlan　Mori Tatsuya*
2024/3/14	プライバシーポリシーにおける収集データと目的の対応関係の実態調査	情報処理学会　SPT 研究会		原 亨 *　長谷川 彩子　Jack Jamieson* 秋山 満昭 *
2024/3/18	関数呼び出しの推移に基づいたユーザ定義関数の特定	情報処理学会　コンピュータセキュリティ研究発表会 (CSEC)		赤羽 秀　韓 燦洙　岩本 一樹 * 伊沢 亮一　高橋 健志　井上 大介
2024/3/19	動的情報フロー追跡によるハードウェアトロジャン検出支援システムの改良	情報処理学会　コンピュータセキュリティ研究発表会 (CSEC)	Vol.CSEC-104 No.51 pp.1-8	伊沢 亮一　金谷 延幸　井上 大介
2024/3/21	One Million Router Under Control: DDNS 機能を有する IoT 機器の脆弱性	電子情報通信学会　情報通信システムセキュリティ研究会 (ICSS)		奥川 莞多 *　森 好樹　久保 正樹 笠間 貴弘　毛利 公一 *　井上 大介

■セキュリティ基盤研究室

発表年月日	論文名	誌名/発表機関	巻号	発表者
2016/4/1	Structure-Preserving Signatures and Commitments to Group Elements	Journal of Cryptology	Vol.29 No.2 pp.363-421	Masayuki Abe*　Georg Fuchsbauer* Jens Groth*　Kristiyan Haralambiev* 大久保 美也子
2016/5/12	Improved Progressive BKZ Algorithms and their Precise Cost Estimation by Sharp Simulator	Eurocrypt 2016	Vol.9665 No.1 pp.789-819	青野 良範　Yuntao Wang*　林 卓也 高木 剛 *
2016/5/30	Constructions of dynamic and non-dynamic threshold public-key encryption schemes with decryption consistency	Theoretical Computer Science	Vol.630 pp.95-116	Yusuke Sakai*　江村 恵太 Jacob C.N. Schuldt　Goichiro Hanaoka* Kazuo Ohta*
2016/5/31	Privacy-Preserving Logistic Regression with Distributed Data Sources via Homomorphic Encryption	IEICE (Special Section on Security, Privacy and Anonymity of Internet of Things)	Vol.E99-D No.8 pp.2079-2089	青野 良範　林 卓也　LE TRIEU PHONG 王 立華
2016/7/1	Unbreakable distributed storage with quantum key distribution network and password-authenticated secret sharing	SCIENTIFIC REPORTS	No.28988 pp.1-8	藤原 幹生　早稲田 篤志　野島 良 盛合 志帆　尾形 わかは *　佐々木 雅英
2016/8/25	On the Leakage Resilient Cryptography in Game-theoretic Settings	SPAPT 2016		Mohammad Shahriar Rahman* 江村 恵太　Shinsaku Kiyomoto*
2016/9/2	Progressive BKZ アルゴリズムを用いた格子暗号の安全性評価	電子情報通信学会　情報セキュリティ研究会 (ISEC)		青野 良範　王 鑽弢 *　林 卓也 高木 剛 *
2016/9/9	Analyzing Randomized Response Mechanisms under Differential Privacy	The 19nd Annual International Conference on Information Security Conference	pp.271-282	早稲田 篤志　野島 良
2016/9/12	A Note on Using Sigma Protocols in Cryptographic Protocols	日本応用数理学会 2016 年度 年会		Hideki Sakurada*　Kazuki Yoneyama* Yoshikazu Hanatani*　吉田 真紀
2016/10/1	Time-Specific Encryption from Forward-Secure Encryption: Generic and Direct Constructions	International Journal of Information Security	Vol.15 No.5 pp.549-571	Kohei Kasamatsu*　Takahiro Matsuda* 江村 恵太　Nuttapong Attrapadung* Goichiro Hanaoka*　Hideki Imai*
2016/10/1	Constant-Size Structure-Preserving Signatures: Generic Constructions and Simple Assumptions	Journal of Cryptology	Vol.29 No.4 pp.833-878	Masayuki Abe*　Ryo Nishimaki* Melissa Chase*　Bernardo David* Markulf Kohlweiss*　大久保 美也子
2016/10/11	まぜるな危険準同型暗号	情報処理学会　コンピュータセキュリティシンポジウム 2016 (CSS2016)		江村 恵太　林 卓也　國廣 昇 * 佐久間 淳 *

発表年月日	論文名	誌名/発表機関	巻号	発表者
2016/10/12	素数位数群における効率的な鍵失効機能付き ID ベース暗号の構成法	情報処理学会　コンピュータセキュリティシンポジウム 2016 (CSS2016)		渡邉 洋平 *　江村 恵太
2016/10/12	PWSCUP: 履歴データを安全に匿名加工せよ	CSS 2016		菊池 浩明 *　小栗 秀暢 *　野島 良 濱田 浩気 *　村上 隆夫　山岡 裕司 * 山口 高康 *　渡辺 知恵美 *
2016/11/1	Toward Securing Tire Pressure Monitoring Systems: A Case of PRESENT-based Implementation	ISITA 2016	pp.408-412	江村 恵太　林 卓也　盛合 志帆
2016/11/1	How Does the Willingness to Provide Private Information Change?	The International Symposium on Information Theory and Its Applications (ISITA2016)	pp.423-427	金森 祥子　野島 良　佐藤 広英 * 太幡 直也 *　川口 嘉奈子 *　諏訪 博彦 * 岩井 淳 *
2016/11/14	An Efficient Construction of Non-Interactive Secure Multiparty Computation	15th International Conference on Cryptology and Network Security (CANS2016)	Vol.10052 pp.604-614	尾花 賢 *　吉田 真紀
2016/11/15	Group Signature with Deniability: How to Disavow a Signature	CANS 2016	pp.228-244	Ai Ishida*　江村 恵太 Goichiro Hanaoka*　Yusuke Sakai* Keisuke Tanaka*
2016/11/25	Anonymous and Leakage Resilient IBE and IPE	Designs, Codes, and Cryptography	pp.1-26	黒澤 馨 *　LE TRIEU PHONG
2016/12/5	Analyzing and Fixing the QACCE security of QUIC	The 3rd International Conference on Research in Security Standardisation (SSR2016)	Vol.10074 pp.1-31	Hideki Sakurada*　Kazuki Yoneyama* Yoshikazu Hanatani*　吉田 真紀
2016/12/21	Fast and Scalable Bilinear-Type Conversion Using Integer Programming	電子情報通信学会　情報セキュリティ研究会 (ISEC)	Vol.73	Masayuki Abe*　Fumitaka Hoshino* 大久保 美也子
2016/12/25	秘密分散法とその暗号応用	北陸数論研究集会		江村 恵太
2017/1/1	Related-Key Attacks on Reduced-round Hierocrypt-L1	IEICE Trans. Fundamentals	Vol.E100-A No.1 pp.126-137	多賀 文吾 *　盛合 志帆　青木 和麻呂
2017/1/24	加法準同型暗号を用いたプライバシー保護深層学習	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2017)		青野 良範　林 卓也　LE TRIEU PHONG 王 立華　盛合 志帆
2017/1/25	適応的安全な無効化可能属性ベース暗号の一般的構成	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2017)		山田 古都子 *　Nuttapong Attrapadung* 江村 恵太　花岡 悟一郎 *　田中 圭介 *
2017/1/25	SIS 問題の計算量評価	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2017)		青野 良範　清藤 武暢 *　四方 順司 *
2017/1/25	購買履歴データの匿名加工における距離関数を使った指標設計法	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2017)		野島 良　小栗 秀暢 *　菊池 浩明 * 中川 裕志 *　濱田 浩気 *　村上 隆夫 山岡 裕司 *　山口 高康 *　渡辺 知恵美 *
2017/1/25	良い仮名化 悪い仮名化	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2017)	pp.2D1-6-	早稲田 篤志　野島 良　盛合 志帆 菊池 浩明 *
2017/1/25	匿名加工・再識別コンテスト PWSCUP 2016 の報告 - 安全性と有用性の評価 -	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2017)		小栗 秀暢 *　菊池 浩明 *　中川 裕志 * 野島 良　濱田 浩気 *　村上 隆夫 山岡 裕司 *　山口 高康 *　渡辺 知恵美 *
2017/1/25	効率のよい匿名かつ maximum leakage resilient な ID ベース暗号	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2017)		黒澤 馨 *　小塙 将司 * スウィ - フエイ ヘン * LE TRIEU PHONG
2017/1/26	署名鍵有効期限付きグループ署名の効率化とその実装評価	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2017)		江村 恵太　林 卓也　石田 愛 *
2017/1/26	完全匿名性を満たす検証者ローカル失効グループ署名の一般的構成	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2017)		石田 愛 *　坂井 祐介 *　江村 恵太 花岡 悟一郎 *　田中 圭介 *
2017/1/26	効率的な準同型内積演算の一般的構成	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2017)		林 卓也　青野 良範　LE TRIEU PHONG 王 立華
2017/1/26	人の視覚特性を利用したビジュアルハッキング回避方式の提案	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2017)	No.3D1-1	吉田 真紀
2017/1/26	A Comparison of Three-Dimensional Sieve Methods for Number Field Sieve over GF(p^6)	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2017)		Kun Wang*　林 卓也　高木 剛 *
2017/2/3	復号可否を指定できる属性ベース暗号	LA シンポジウム 2016		山田 古都子 *　Nuttapong Attrapadung* 江村 恵太　花岡 悟一郎 *　田中 圭介 *
2017/2/17	New Revocable IBE in Prime-Order Groups: Adaptively Secure, Decryption Key Exposure Resistant, and with Short Public Parameters	CT-RSA 2017		Yohei Watanabe*　江村 恵太 Jae Hong Seo*
2017/2/24	Establishing Secure and Anonymous Communication Channel: KEM/DEM-based Construction and Its Implementation	Journal of Information Security and Applications		江村 恵太　金岡 晃　太田 悟史 高橋 健志
2017/4/2	Efficient Key-Rotatable and Security-Updatable Homomorphic Encryption	The Fifth International Workshop on Security in Cloud Computing (ASIACCS2017-SCC)	pp.35-42	青野 良範　林 卓也　LE TRIEU PHONG 王 立華
2017/4/4	Mis-operation Resistant Searchable Homomorphic Encryption	ACM ASIACCS 2017		江村 恵太　林 卓也　Noboru Kunihiro* Jun Sakuma*
2017/4/5	LINCOS: A Storage System Providing Long-Term Integrity, Authenticity, and Confidentiality	Asia Conference on Computer and Communications Security (ASIACCS) 2017	pp.461-468	Johannes Braun*　Johannes Buchmann* Denise Demirel*　Matthias Geihs* 藤原 幹生　盛合 志帆　佐々木 雅英 早稲田 篤志

7　サイバーセキュリティ研究所誌上発表論文一覧

発表年月日	論文名	誌名/発表機関	巻号	発表者
2017/4/5	公開鍵暗号型の高機能暗号を巡る研究動向	日本銀行金融研究所 ディスカッションペーパーシリーズ		清藤 武暢＊　青野 良範　四方 順司＊
2017/4/6	Group Signatures with Time-bound Keys Revisited: A New Model and an Efficient Construction	ACM ASIACCS 2017		江村 恵太　林 卓也　Ai Ishida*
2017/5/2	Random Sampling Revisited: Lattice Enumeration with Discrete Pruning	Eurocrypt 2017	Vol.10211 No.1 pp.65-102	青野 良範　Phong Q. Nguyen*
2017/5/12	公開検証可能なプライバシー保護時系列データ統計計算	電子情報通信学会　情報セキュリティ研究会（ISEC）		江村 恵太
2017/7/4	Privacy-Preserving Aggregation of Time-Series Data with Public Verifiability from Simple Assumptions	ACISP 2017		江村 恵太
2017/7/6	Privacy-Preserving Deep Learning: Revisited and Enhanced	International Conference on Applications and Technologies in Information Security (ATIS) 2017	Vol.719 pp.100-110	LE TRIEU PHONG　青野 良範　林 卓也 王 立華　盛合 志帆
2017/7/14	高機能暗号の金融分野での応用に関する考察	情報処理学会　第 78 回コンピュータセキュリティ・第 24 回セキュリティ心理学とトラスト合同研究発表会		清藤 武暢＊　青野 良範　四方 順司＊
2017/7/21	Input and Output Privacy-Preserving Linear Regression	IEICE Trans. D (Special Issue on Security, Privacy and Anonymity in Computation, Communication and Storage Systems)	Vol.E100-D No.10 pp.2339-2347	青野 良範　林 卓也　LE TRIEU PHONG 王 立華
2017/7/24	Privacy-Preserving Deep Learning via Additively Homomorphic Encryption	IACR Eprint		LE TRIEU PHONG　青野 良範　林 卓也 王 立華　盛合 志帆
2017/8/15	IBE and Function-Private IBE under Linear Assumptions with Shorter Ciphertexts and Private Keys, and Extensions	International Journal of Applied Cryptography (IJACT)	Vol.3 No.3 pp.210-224	黒澤 馨＊　LE TRIEU PHONG
2017/8/21	Compact Structure-preserving Signatures with Almost Tight Security	CRYPTO2017	Vol.10402 pp.548-580	Masayuki Abe*　Dennis Hofheinz* Ryo Nishimaki*　大久保 美也子 Jiaxin Pan*
2017/8/22	A Generic Construction of Secure-Channel Free Searchable Encryption with Multiple Keywords	NSS 2017		江村 恵太
2017/8/22	A Generic yet Efficient Method for Secure Inner Product	11th International Conference on Network and System Security (NSS2017)	Vol.LNCS No.10394 pp.217-232	王 立華　林 卓也　青野 良範 LE TRIEU PHONG
2017/8/22	Privacy-Preserving Stochastic Gradient Descent with Multiple Distributed Trainers	International workshop on Security in Big Data (SECBD-2017)		LE TRIEU PHONG
2017/9/1	Group Signature with Deniability: How to Disavow a Signature	IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences	Vol.E100-A No.9 pp.1825-1837	Ai Ishida*　江村 恵太 Goichiro Hanaoka*　Yusuke Sakai* Keisuke Tanaka*
2017/9/1	ペアリング暗号解読の世界記録とその安全性評価	IEICE	Vol.J100-B No.9 pp.582-592	高木 剛＊　下山 武司＊　篠原 直行 林 卓也
2017/9/6	秘密分散とマトロイド	日本応用数理学会 2017 年度年会，数理的技法による情報セキュリティ（FAIS）	pp.143-144	吉田 真紀
2017/9/15	Generic Constructions for Fully Secure Revocable Attribute-Based Encryption	ESORICS2017		山田 古都子＊　Nuttapong Attrapadung* 江村 恵太　花岡 悟一郎＊　田中 圭介＊
2017/10/23	確率的格子点探索の計算量の下界について	情報処理学会　コンピュータセキュリティシンポジウム 2017（CSS2017）		青野 良範　清藤 武暢＊　四方 順司＊
2017/10/23	プライバシー保護異常検知フレームワーク	情報処理学会　コンピュータセキュリティシンポジウム 2017（CSS2017）		荒井 ひろみ＊　江村 恵太　林 卓也
2017/10/24	加法準同型暗号を用いたプライバシー保護 Extreme Learning Machine	情報処理学会　コンピュータセキュリティシンポジウム 2017（CSS2017）		栗 昌平＊　林 卓也　大森 敏明＊ 小澤 誠一＊　青野 良範 LE TRIEU PHONG　王 立華　盛合 志帆
2017/10/24	プライバシーポリシーを読まない理由に関する一考察	情報処理学会　コンピュータセキュリティシンポジウム 2017（CSS2017）	Vol.2017 No.2 pp.874-881	金森 祥子　野島 良　岩井 淳＊ 川口 嘉奈子＊　佐藤 広英＊　諏訪 博彦＊ 太幡 直也＊
2017/10/30	A Framework of Privacy Preserving Anomaly Detection: Providing Traceability without Big Brother	Workshop on Privacy in the Electronic Society (WPES) 2017		Hiromi Arai*　江村 恵太 Takuya Hayashi*
2017/11/28	Privacy Preserving Extreme Learning Machine Using Additively Homomorphic Encryption	2017 IEEE Symposium Series on Computational Intelligence (SSCI 2017)		Shohei Kuri*　林 卓也　Toshiaki Omori* Seiichi Ozawa*　青野 良範 LE TRIEU PHONG　王 立華　盛合 志帆
2017/11/29	A New Secure Matrix Multiplication from Ring-LWE	16th International Conference on Cryptology And Network Security (CANS2017)	Vol.LNCS No.11261 pp.93-111	王 立華　青野 良範　LE TRIEU PHONG
2017/11/30	Verifiably Multiplicative Secret Sharing	The 10th in a series of International Conference on Information Theoretic Security (ICITS2017)	No.10681 pp.73-82	吉田 真紀　Satoshi Obana*

発表年月日	論文名	誌名/発表機関	巻号	発表者
2017/12/8	An Experimental Study of Kannan's Embedding Technique for the Search LWE Problem	he 2017 International Conference on Information and Communications Security (ICICS 2017)		Yuntao Wang* 青野 良範 Tsuyoshi Takagi*
2017/12/21	公開検証可能なプライバシー保護時系列データ統計計算の実装評価	電子情報通信学会　情報セキュリティ研究会 (ISEC)		鈴木 達也 * 江村 恵太　木村 隼人 * 大東 俊博 *
2017/12/29	Privacy-Preserving Deep Learning via Additively Homomorphic Encryption	IEEE Transactions on Information Forensics and Security	Vol.13 No.5 pp.1333-1345	LE TRIEU PHONG　青野 良範　林 卓也 王 立華　盛合 志帆
2018/1/1	Efficient Homomorphic Encryption with Key Rotation and Security Update	IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS, COMMUNICATIONS AND COMPUTER SCIENCES	Vol.E101-A No.1 pp.39-50	青野 良範　林 卓也　LE TRIEU PHONG 王 立華
2018/1/8	A Privacy-enhanced Access Log Management Mechanism in SSO Systems from Nominative Signatures	International Journal of Applied Cryptography		Sanami Nakagawa*　Takashi Nishide* Eiji Okamoto*　江村 恵太 Goichiro Hanaoka*　Yusuke Sakai* Akihisa Kodate*
2018/1/23	Pairing Type Optimization Problem and Its Hardness	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2018)		Fumitaka Hoshino*　Masayuki Abe* 大久保 美也子
2018/1/24	検証乗算可能な秘密分散	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2018)	No.2A3-2	吉田 真紀　尾花 賢 *
2018/1/25	Ring-LWE を用いたセキュアな行列乗算のためのパッキング方法	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2018)		王 立華 ミシュラ プラディイプ クマル * 青野 良範　LE TRIEU PHONG 安田 雅哉 *
2018/1/25	ペアリングを用いた暗号方式の擬似コードレベルでのパフォーマンス評価	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2018)		Masayuki Abe*　Fumitaka Hoshino* 大久保 美也子
2018/1/26	標準的な仮定で安全かつスケーラブルなメンバ削除可能グループ署名	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2018)		江村 恵太
2018/1/26	複数キーワードをサポートしたセキュアチャネルフリー検索可能暗号の実装評価	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2018)		伊藤 勝彦 * 江村 恵太　大東 俊博 *
2018/1/26	ISO/IEC 20008 におけるグループ署名方式の安全性に関する考察	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2018)		石田 愛 * 坂井 祐介 * 江村 恵太 花岡 悟一郎 * 田中 圭介 *
2018/1/26	プライバシーポリシー自動解析のための学習データ構築に向けた取り組み	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2018)	No.4C2-3	金森 祥子　野島 良　岩井 淳 * 川口 嘉奈子 * 佐藤 広英 * 諏訪 博彦 * 太幡 直也 *
2018/2/1	Road-to-Vehicle Communications with Time-Dependent Anonymity: A Lightweight Construction and its Experimental Results	IEEE Transactions on Vehicular Technology	Vol.67 No.2	江村 恵太　林 卓也
2018/3/1	On the Optimality of Lattices for the Coppersmith Technique	Applicable Algebra in Engineering, Communication and Computing	Vol.29 No.2 pp.169-195	青野 良範　Manindra Agrawal* 佐藤 孝和 * 渡辺 治 *
2018/3/9	Plausible Deniability の Deniability について	電子情報通信学会　情報セキュリティ研究会 (ISEC)	Vol.117 No.487 pp.225-230	早稲田 篤志　野島 良
2018/3/23	Verifiable Chebyshev maps-based chaotic encryption schemes with outsourcing computations in the cloud/fog scenarios	Concurrency and Computation: Practice and Experience (Wiley)		Jing Li*　Licheng Wang*　王 立華 Xianmin Wang*　Zhengan Huang　Jin Li*
2018/3/26	On the (In)Efficiency of Non-Interactive Secure Multiparty Computation	Designs, Codes and Cryptography	Vol.86 No.8 pp.1793-1805	吉田 真紀　Satoshi Obana*
2018/3/28	Improved (Almost) Tightly-Secure Structure Preserving Signatures	PKC 2018	Vol.10769 No.II pp.123-152	Charanjit S. Jutla*　大久保 美也子 Arnab Roy*
2018/4/1	Accumulable Optimistic Fair Exchange from Verifiably Encrypted Homomorphic Signatures	International Journal of Information Security		Jae Hong Seo*　江村 恵太 Keita Xagawa*　Kazuki Yoneyama*
2018/6/7	Chosen Ciphertext Secure Keyed-Homomorphic Public-Key Cryptosystems	Designs, Codes and Cryptography	Vol.86 No.8 pp.1623-1683	江村 恵太　花岡 悟一郎 *　縫田 光司 * 大竹 剛 *　松田 隆弘 *　山田 翔太 *
2018/7/6	Lower Bounds on Structure-Preserving Signatures for Bilateral Messages	IACR ePrint Archieves		Masayuki Abe*　Miguel Ambrona* 大久保 美也子　Mehdi Tibouchi*
2018/7/25	まぜるな危険準同型暗号を用いた医療データに対する χ^2 独立性検定	電子情報通信学会　情報セキュリティ研究会 (ISEC)		江村 恵太　林 卓也　陸 文傑 * 盛合 志帆　佐久間 淳 *　山田 芳司 *
2018/7/25	セキュアチャネルフリー検索可能暗号と公開鍵暗号との安全な併用について	電子情報通信学会　情報セキュリティ研究会 (ISEC)		鈴木 達也 * 江村 恵太　大東 俊博 *
2018/8/1	Efficient Fully Structure-Preserving Signatures and Shrinking Commitments	Journal of Cryptology (Springer)		Masayuki Abe*　Jens Groth* Markulf Kohlweiss*　大久保 美也子 Mehdi Tibouchi*
2018/8/20	Lower Bounds on Lattice Enumeration with Extreme Pruning	CRYPTO 2018	Vol.10992 pp.608-637	青野 良範　Phong Q. Nguyen* 清藤 武暢 *　四方 順司 *

7　サイバーセキュリティ研究所誌上発表論文一覧

発表年月日	論文名	誌名/発表機関	巻号	発表者
2018/9/1	Generic Constructions for Fully Secure Revocable Attribute-Based Encryption	IEICE Transactions		Kotoko Yamada* Nuttapong Attrapadung* 江村 恵太 Goichiro Hanaoka* Keisuke Tanaka*
2018/9/5	Fully Anonymous Group Signature with Verifier-Local Revocation	SCN 2018		石田 愛＊ 坂井 祐介＊ 江村 恵太 花岡 悟一郎＊ 田中 圭介＊
2018/9/5	Lower Bounds on Structure-Preserving Signatures for Bilateral Messages	11th Conference on Security and Cryptography for Netowrks (SCN2018)	Vol.11035 pp.3-22	Masayuki Abe* Miguel Ambrona* 大久保 美也子 Mehdi Tibouchi*
2018/9/5	ProVerif の検証過程の可視化	日本応用数理学会 2018 年度 年会	pp.367-368	吉田 真紀
2018/9/5	Scyther tool の検証過程の可視化	日本応用数理学会 2018 年度 年会	pp.369-370	吉田 真紀
2018/9/10	Privacy-Preserving Deep Learning for any Activation Function	arXiv.org (Cornell University Library)		LE TRIEU PHONG TRAN THI PHUONG*
2018/9/12	A Revocable Group Signature Scheme with Scalability from Simple Assumptions and Its Implementation	ISC 2018		江村 恵太 林 卓也
2018/9/26	A Generic Construction of Integrated Secure-Channel Free PEKS and PKE	ISPEC2018		鈴木 達也＊ 江村 恵太 大東 俊博＊
2018/10/23	A Continuous Genetic Algorithm for Optimizing Pruning Function for Lattice Enumeration	情報処理学会 コンピュータセキュリティシンポジウム 2018 (CSS2018)		Trong-Thuc Trang* 青野 良範 高木 剛*
2018/10/24	超小型衛星・小型ロケット用セキュア通信のための情報理論的安全性の検討	日本航空宇宙学会 第 62 回宇宙科学技術連合講演会		森岡 澄夫＊ 尾花 賢＊ 吉田 真紀
2018/10/25	鍵更新機能付き検索可能暗号：効率化に向けた一工夫	情報処理学会 コンピュータセキュリティシンポジウム 2018 (CSS2018)		松崎 なつめ＊ 穴田 啓晃＊ 金岡 晃＊ 渡邉 洋平
2018/10/25	CBDH 仮定に基づく効率的な閾値公開鍵暗号	情報処理学会 コンピュータセキュリティシンポジウム 2018 (CSS2018)		海老名 将宏＊ 渡邉 洋平 四方 順司＊
2018/10/29	Card-Based Majority Voting Protocols with Three Inputs Using Three Cards	International Symposium on Information Theory and Its Applications (ISITA) 2018		渡邉 洋平 黒木 慶久＊ 鈴木 慎之介＊ 古賀 優太＊ 岩本 貢＊ 太田 和夫＊
2018/11/19	Securing Named Data Networking: Attribute-Based Encryption and Beyond	IEEE Communications Magazine	Vol.56 No.11 pp.76-81	Licheng Wang* Zonghua Zhang* Mianxiong Dong* 王 立華 Zhenfu Cao* Yixian Yang*
2018/12/3	Quantum Lattice Enumeration and Tweaking Discrete Pruning	the 24th Annual International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2018)	Vol.11272 No.1 pp.405-434	青野 良範 Phong Q. Nguyen* Yixin Shen*
2018/12/3	Improved (Almost) Tightly-Secure Simulation-Sound QA-NIZK with Applications	Asiacrypt2018	Vol.11272 No.1 pp.627-656	Masayuki Abe* Charanjit S. Jutla* 大久保 美也子 Arnab Roy*
2018/12/4	Hardness Evaluation for Search LWE Problem Using Progressive BKZ Simulator	電子情報通信学会 EA Special Issue: Information Theory and Its Applications	Vol.E101-A No.12 pp.2162-2170	Yuntao Wang* 青野 良範 高木 剛＊
2018/12/8	Implementation and Analysis of Fully Homomorphic Encryption in Wearable Devices	The Fourth International Conference of Information Security and Digital Forensics (ISDF 2018)		Amonrat Prasitsupparote* 渡邉 洋平 四方 順司＊
2018/12/11	Verifiably Multiplicative Secret Sharing	IEEE Transactions on Information Theory	Vol.65 No.5 pp.3233-3245	吉田 真紀 Satoshi Obana*
2018/12/14	Privacy-Preserving Naive Bayes Classification Using Fully Homomorphic Encryption	ICONIP 2018	Vol.11304 pp.349-358	Sangwook Kim* 大森 正裕＊ 林 卓也 大森 敏明＊ 王 立華 小澤 誠一＊
2019/1/1	Fast and Scalable Bilinear-Type Conversion Method for Large Scale Crypto Schemes	IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences	Vol.E102-A No.1 pp.251-269	Masayuki Abe* Fumitaka Hoshino* 大久保 美也子
2019/1/23	鍵生成センタに対して安全な ID ベース暗号	電子情報通信学会 暗号と情報セキュリティシンポジウム (SCIS2019)		江村 恵太 勝又 秀一＊ 渡邉 洋平
2019/1/23	より効率的で適応的に安全な鍵失効機能付き ID ベース暗号の構成	電子情報通信学会 暗号と情報セキュリティシンポジウム (SCIS2019)		高安 敦＊ 渡邉 洋平 江村 恵太
2019/1/23	アニーリング計算による素因数分解について	電子情報通信学会 暗号と情報セキュリティシンポジウム (SCIS2019)	No.2B4-3 pp.1-8	清水 俊也＊ 伊豆 哲也＊ 篠原 直行 盛合 志帆 國廣 昇＊
2019/1/24	GDPR 対応したプライバシーポリシーに関するユーザ評価	電子情報通信学会 暗号と情報セキュリティシンポジウム (SCIS2019)		金森 祥子 岩井 淳＊ 川口 嘉奈子＊ 佐藤 広英＊ 諏訪 博彦＊ 太幡 直也＊ 盛合 志帆
2019/1/25	スケーラブルなメンバ削除可能グループ署名を用いた ID 管理システム	電子情報通信学会 暗号と情報セキュリティシンポジウム (SCIS2019)		江村 恵太 林 卓也
2019/2/15	準同型暗号を用いた秘密計算とその応用	システム情報制御学会 学会誌「システム／制御／情報」	Vol.63 No.2 pp.64-70	林 卓也
2019/2/18	Implementation and Analysis of Fully Homomorphic Encryption in Resource-Constrained Devices	International Journal of Digital Information and Wireless Communications	Vol.8 No.4 pp.288-303	Amonrat Prasitsupparote* 渡邉 洋平 坂本 純一＊ 四方 順司＊ 松本 勉＊
2019/2/28	Multi-Party Computation for Modular Exponentiation Based on Replicated Secret Sharing	IEICE Transaction on on Fundamentals of Electronics, Communications and Computer Sciences		大原 一真＊ 渡邉 洋平 岩本 貢＊ 太田 和夫＊

発表年月日	論文名	誌名/発表機関	巻号	発表者
2019/3/4	小型衛星・小型ロケット用通信のセキュリティモデルとプロトタイプ実装	情報処理学会　第 84 回 CSEC 研究発表会	Vol.2019-CSEC-No.3 pp.1-8	尾花 賢 *　吉田 真紀　森岡 澄夫 *
2019/3/16	Atomic block を利用した楕円曲線暗号に対するサイドチャネル攻撃対策	情報処理学会　第 81 回全国大会	Vol.6ZA No.2	竹村 友佑 *　伯田 恵輔 *　篠原 直行
2019/3/22	Strong Robustness を有する ID ベース暗号の具体的構成と実装評価	2019 年電子情報通信学会総合大会		岡野 寛 *　江村 恵太　鈴木 達也 * 大東 俊博
2019/3/28	A Generic Construction of Integrated Secure-Channel Free PEKS and PKE and its Application to EMRs in Cloud Storage	Journal of Medical Systems		Tatsuya Suzuki　江村 恵太 Toshihiro Ohigashi*
2019/4/1	Privacy-Preserving Aggregation of Time-Series Data with Public Verifiability from Simple Assumptions and Its Implementations	The Computer Journal		江村 恵太　Hayato Kimura* Toshihiro Ohigashi*　Tatsuya Suzuki*
2019/4/7	On the convergence proof of AMSGrad and a new version	arXiv (arXiv.org)		TRAN THI PHUONG*　LE TRIEU PHONG
2019/4/15	Privacy-Preserving Deep Learning via Weight Transmission	IEEE Transactions on Information Forensics and Security	Vol.14 No.11 pp.3003-3015	LE TRIEU PHONG　TRAN THI PHUONG*
2019/5/13	On the Convergence Proof of AMSGrad and a New Version	IEEE Access	Vol.7 pp.61706-61716	TRAN THI PHUONG*　LE TRIEU PHONG
2019/7/10	Proper Usage of the Group Signature Scheme in ISO/IEC 20008-2	ASIACCS 2019		石田 愛 *　坂井 祐介 *　江村 恵太 花岡 悟一郎 *　田中 圭介 *
2019/7/23	観測ロケット MOMO3 号機による小型衛星・小型ロケット用セキュア通信方式の基礎実験	情報処理学会　第 86 回コンピュータセキュリティ・第 34 回セキュリティ心理学とトラスト合同研究発表会	Vol.2019CSEC86 No.10 pp.1-8	吉田 真紀　森岡 澄夫 *　尾花 賢 *
2019/8/14	Plaintext Recovery Attacks against XTS Beyond Collisions	SAC 2019		五十部 孝典　Kazuhiro Minematsu*
2019/8/14	Iterative Differential Characteristic of TRIFLE-BC	SAC 2019		Fukang Liu*　五十部 孝典
2019/8/20	Efficient Collision Attack Frameworks for RIPEMD-160	CRYPTO 2019	Vol.11693 pp.117-149	Fukang Liu*　Christoph Dobraunig* Florian Mendel*　五十部 孝典 Gaoli Wang*　Zhenfu Cao*
2019/8/26	Group Signatures with Message-Dependent Opening: Formal Definitions and Constructions	Security and Communication Networks	Vol.2019	江村 恵太　Goichiro Hanaoka* Yutaka Kawai*　Takahiro Matsuda* Kazuma Ohara*　Kazumasa Omote* Yusuke Sakai*
2019/8/28	More Results on Shortest Linear Programs	The 14th International Workshop on Security (IWSEC 2019)	Vol.11689 pp.109-128	Subhadeep Banik*　Yuki Funabiki* 五十部 孝典
2019/8/28	Tweakable TWINE: Building a Tweakable Block Cipher on Generalized Feistel Structure	IWSEC 2019	Vol.11689 pp.129-145	Kosei Sakamoto*　Kazuhiko Minematsu* Nao Shibata*　Maki Shigeri* Hiroyasu Kubo*　Yuki Funabiki* Andrey Bogdanov*　Sumio Morioka* 五十部 孝典
2019/8/28	An Efficient F4-style Based Algorithm to Solve MQ Problems	The 14th International Workshop on Security (IWSEC 2019)	Vol.11689 pp.37-52	伊藤 琢真　篠原 直行　内山 成憲 *
2019/8/29	Preimage Attacks on Reduced Troika with Divide-and-Conquer Methods	The 14th International Workshop on Security (IWSEC 2019)	Vol.11689 pp.306-326	Fukang Liu*　五十部 孝典
2019/8/29	Quadratic Frobenius Pseudoprimes with Respect to x^2+5x+5	Japan Society for Industrial and Applied Mathematics (JSIAM) Letters	Vol.11 pp.53-55	長島 早紀 *　篠原 直行　内山 成憲 *
2019/9/1	Shortening the Libert-Peters-Yung Revocable Group Signature Scheme by Using the Random Oracle Methodology	IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences	pp.1101-1117	Kazuma Ohara*　江村 恵太 Goichiro Hanaoka*　Ai Ishida* Kazuo Ohta*　Yusuke Sakai*
2019/9/3	Opcount: A Pseudo-Code Performance Estimation System for Pairing-Based Cryptography	IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences	Vol.E102-A No.9 pp.1285-1292	Masayuki Abe*　Fumitaka Hoshino* 大久保 美也子
2019/9/3	F4-style アルゴリズムを基にした MQ 問題の求解	日本応用数理学会　2019 年度　年会		伊藤 琢真　篠原 直行　内山 成憲 *
2019/9/20	New Semi-Free-Start Collision Attack Framework for Reduced RIPEMD-160	FSE 2020 / ToSC	Vol.2019 No.3 pp.169-192	Fukang Liu*　Christoph Dobraunig* Florian Mendel*　五十部 孝典 Gaoli Wang*　Zhenfu Cao*
2019/9/20	Cryptanalysis of Plantlet	FSE 2020 / ToSC	Vol.2019 No.3 pp.103-120	Subhadeep Banik*　Khashayar Barooti* 五十部 孝典
2019/9/25	Identity-Based Encryption with Security against the KGC: A Formal Model and Its Instantiation from Lattices	ESORICS 2019		江村 恵太　勝又 秀一 *　渡邉 洋平
2019/9/30	格子暗号解読のための数学的基礎 - 格子基底簡約アルゴリズム入門	近代科学社		青野 良範　安田 雅哉 *
2019/10/21	Ring-LWE ベース準同型暗号を用いたプライバシー保護決定木分類	情報処理学会　コンピュータセキュリティシンポジウム 2019（CSS2019）	pp.321-327	福井 智 *　王 立華　林 卓也 小澤 誠一 *
2019/10/21	プライバシーポリシーのユーザ理解支援ツール構築のための Web アンケート調査国別比較	情報処理学会　コンピュータセキュリティシンポジウム 2019（CSS2019）		金森 祥子　佐藤 広英 *　太幡 直也 * 盛合 志帆
2019/10/22	ブロックチェーンシステムにおける匿名トークン付与に関する一考察	情報処理学会　コンピュータセキュリティシンポジウム 2019（CSS2019）		佐藤 哲平 *　江村 恵太　面 和成

7　サイバーセキュリティ研究所誌上発表論文一覧

発表年月日	論文名	誌名/発表機関	巻号	発表者
2019/10/22	検証可能な乗法秘密分散の効率向上	情報処理学会　コンピュータセキュリティシンポジウム 2019 (CSS2019)		吉田 真紀　尾花 賢 *
2019/11/8	情報理論的安全性を有する小型衛星・小型ロケット用セキュア通信方式の基礎実験	日本航空宇宙学会　第 63 回宇宙科学技術連合講演会		森岡 澄夫 *　尾花 賢 *　吉田 真紀
2019/11/8	A Fast Privacy-Preserving Multi-Layer Perceptron Using Ring-LWE-based Homomorphic Encryption	IEEE International Conference on Data Mining The 2nd International Workshop on Cross-disciplinary Data Exchange and Collaboration (CDEC2019)	pp.37-44	Takehiro Tezuka*　王 立華　林 卓也 Seiichi Ozawa*
2019/11/28	Implementation of a Strongly Robust Identity-Based Encryption Scheme over Type-3 Pairings	CANDAR 2019		Hiroshi Okano*　江村 恵太 Takuya Ishibashi*　大東 俊博 鈴木 達也 *
2019/11/28	ECC Atomic Block against Strong Side-Channel Attacks using Binary Curves	CANDAR 2019	pp.387-393	Yusuke Takemura*　Keisuke Hakuta* 篠原 直行
2019/12/9	Shorter QA-NIZK and SPS with Tighter Security	Asiacrypt2019		Masayuki Abe*　Charanjit S. Jutla* 大久保 美也子　Jiaxin Pan*　Arnab Roy* Yuyu Wang*
2020/1/1	A Revocable Group Signature Scheme with Scalability from Simple Assumptions	IEICE Transactions		江村 恵太　林 卓也
2020/1/28	ブロックチェーンシステムにおける匿名信頼性付与手法の実装・評価	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2020)		佐藤 哲平 *　江村 恵太　面 和成
2020/1/29	公開鍵長が定数である完全匿名な検証者ローカル失効グループ署名	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2020)		江村 恵太　石田 愛 *　坂井 祐介 *
2020/1/30	Intel SGX を用いた公開検証可能な関数型暗号の構成と実装評価	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2020)		鈴木 達也 *　江村 恵太　面 和成 大東 俊博
2020/1/30	Gröbner 基底を用いた MQ 問題の求解	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2020)		伊藤 琢真　篠原 直行　内山 成憲 *
2020/1/31	情報理論的安全性を有する小型衛星・小型ロケット用セキュア通信方式の実装検討と飛行評価	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2020)		森岡 澄夫 *　尾花 賢 *　吉田 真紀
2020/1/31	国内外企業のプライバシーポリシーの特徴比較 - 固有表現の曖昧性と情報量による分類 -	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2020)		金森 祥子　佐藤 広英 *　太幡 直也 * 野島 良
2020/3/1	Group Signatures with Time-Bound Keys Revisited: A New Model, an Efficient Construction, and its Implementation	IEEE Transactions on Dependable and Secure Computing		江村 恵太　林 卓也　石田 愛 *
2020/4/16	Distributed SGD with Flexible Gradient Compression	IEEE Access	Vol.8 pp.64707-64717	TRAN THI PHUONG*　LE TRIEU PHONG
2020/5/20	NEM のブロックチェーンシステムにおける匿名信頼性付与手法の実装・評価	電子情報通信学会　情報セキュリティ研究会 (ISEC)		藤谷 知季　江村 恵太　面 和成
2020/6/2	On Black-Box Extensions of Non-interactive Zero-Knowledge Arguments, and Signatures Directly from Simulation Soundness	PKC 2020	Vol.12110 No.1 pp.558-589	Masayuki Abe*　Miguel Ambrona* 大久保 美也子
2020/6/11	プライバシーポリシーの固有表現の曖昧性と情報量による分類 - 透明性に関する一考察 -	人工知能学会　人工知能学会全国大会 (JSAI2020)		金森 祥子　佐藤 広英 *　太幡 直也 * 野島 良
2020/6/21	Aggregate Message Authentication Codes with Detecting Functionality from Biorthogonal Codes	2020 IEEE International Symposium on Information Theory (ISIT 2020)		小川 善功 *　佐藤 慎悟　四方 順司 * 今井 秀樹 *
2020/7/1	Implementation of a Strongly Robust Identity-Based Encryption Scheme over Type-3 Pairings	International Journal of Networking and Computing	Vol.10 No.2 pp.174-188	Hiroshi Okano*　江村 恵太 Takuya Ishibashi*　Toshihiro Ohigashi* Tatsuya Suzuki*
2020/7/1	ECC Atomic Block with NAF against Strong Side-Channel Attacks on Binary Curves	International Journal of Networking and Computing	Vol.10 No.2 pp.277-292	Yusuke Takemura*　Keisuke Hakuta* 篠原 直行
2020/7/8	Efficient Constructions of Non-Interactive Secure Multiparty Computation from Pairwise Independent Hashing	17th International Conference on Security and Cyrptography (SECRYPT 2020)	Vol.4	Satoshi Obana*　吉田 真紀
2020/7/16	Extended partial key exposure attacks on RSA: Improvement up to full size decryption exponents	Theoretical Computer Science	Vol.841 pp.62-83	鈴木 海地 *　高安 敦　國廣 昇 *
2020/8/15	Non-transferability in Proxy Re-Encryption Revisited	Journal of Internet Services and Information Security (JISIS)	Vol.10 No.3 pp.1-30	Arinjita Paul*　王 立華 S. Sharmila Deva Selvi* C. Pandu Rangana*
2020/8/19	Automatic Verification of Differential Characteristics: Application to Reduced Gimli	CRYPTO 2020		Liu Fuakng*　五十部 孝典　Willi Meier*
2020/8/24	A Compact Digital Signature Scheme Based on the Module-LWR problem	ICICS 2020	Vol.12282 pp.73-90	岡田 大樹 *　高安 敦　福島 和英 * 清本 晋作 *　高木 剛 *
2020/9/1	Enhanced Secure Comparison Schemes Using Homomorphic Encryption	The 23rd International Conference on Network-Based Information Systems (NBiS-2020)		王 立華　Tushar Kanti Saha*　青野 良範 Takeshi Koshiba*　盛合 志帆
2020/9/11	プライバシー意識の日米独比較—GDPR に対する理解の違いに着目して—	日本パーソナリティ心理学会　第 29 回大会		太幡 直也 *　佐藤 広英 *　金森 祥子 野島 良　盛合 志帆
2020/9/11	情報プライバシーとプライバシーポリシーの理解度，評価との関連	日本パーソナリティ心理学会　第 29 回大会		佐藤 広英 *　太幡 直也 *　金森 祥子 野島 良

発表年月日	論文名	誌名/発表機関	巻号	発表者
2020/10/21	Distributed SignSGD With Improved Accuracy and Network-Fault Tolerance	IEEE Access	Vol.8 pp.191839-191849	LE TRIEU PHONG　TRAN THI PHUONG*
2020/10/24	Compact Verifiably Multiplicative Secret Sharing	2020 International Symposium on Information Theory and its Applications (ISITA2020)	Vol.1	吉田 真紀　Satoshi Obana*
2020/10/26	Cache-22: A Highly Deployable Encrypted Cache System	ISITA 2020		江村 恵太　盛合 志帆 Takuma Nakajima*　Masato Yoshimi*
2020/10/26	協調学習スキームを導入したプライバシー保護 XGBoost	情報処理学会　コンピュータセキュリティシンポジウム 2020 (CSS2020)	pp.228-235	山本 楓己 *　王 立華　小澤 誠一 *
2020/10/27	ストリーム暗号 Salsa20 における Probabilistic Neutral Bits の解析	情報処理学会　コンピュータセキュリティシンポジウム 2020 (CSS2020)		宮下 翔太郎 *　伊藤 竜馬　宮地 充子 *
2020/10/27	プライバシーポリシーを読むユーザへの支援に関する一考察 - 支援ツール構築とその効果検証 -	情報処理学会　コンピュータセキュリティシンポジウム 2020 (CSS2020)	pp.697-703	金森 祥子　佐藤 広英 *　太幡 直也 * 野島 良
2020/10/27	集団検査機能を有する準同型認証暗号	情報処理学会　コンピュータセキュリティシンポジウム 2020 (CSS2020)		佐藤 慎悟
2020/11/18	New Approaches to Federated XGBoost Learning for Privacy-Preserving Data Analysis	ICONIP2020 (The 27th International Conference on Neural Information Processing)	Vol.LNCS No.12533 pp.558-569	Fuki Yamamoto*　王 立華 Seiichi Ozawa*
2020/11/30	Galaxy: A Family of Stream-Cipher-Based Space-Hard Ciphers	Australasian Conference on Information Security and Privacy (ACISP) 2020		Yuji Koike*　Kosei Sakamoto* Takuya Hayashi*　五十部 孝典
2020/12/1	Secure-channel free searchable encryption with multiple keywords: A generic construction, an instantiation, and its implementation	Journal of Computer and System Sciences	Vol.114 pp.107-125	江村 恵太　Katsuhiko Ito* Toshihiro Ohigashi
2020/12/7	Non-Interactive Composition of Sigma-Protocols via Share-then-Hash	Asiacrypt2020		Masayuki Abe*　Miguel Ambrona* Andrej Bogdanov*　大久保 美也子 Alon Rosen*
2020/12/11	超電導量子回路を用いた離散対数問題の求解実験	第 43 回量子情報技術研究会（QIT43）		青野 良範　Sitong Liu*　田中 智樹 * 宇野 隼平 *　Rodney Van Meter* 篠原 直行　野島 良
2020/12/17	Rotational Cryptanalysis of Salsa Core Function	The 23rd Information Security Conference (ISC) 2020		伊藤 竜馬
2021/1/1	Privacy Preserving Data Analysis: Providing Traceability without Big Brother	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences		Hiromi Arai*　江村 恵太 Takuya Hayashi*
2021/1/1	On the Security of Keyed-Homomorphic PKE: Preventing Key Recovery Attacks and Ciphertext Validity Attacks	IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences		江村 恵太
2021/1/1	New Iterated RC4 Key Correlations and Their Application to Plaintext Recovery on WPA-TKIP	IEICE Trans. Fundamentals		伊藤 竜馬　Atsuko Miyaji*
2021/1/1	Solving the MQ Problem Using Gröbner Basis Techniques	IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences	Vol.104-A No.1 pp.135-142	伊藤 琢真　篠原 直行　内山 成憲 *
2021/1/6	Revocable Identity-based Encryption with Bounded Decryption Key Exposure Resistance: Lattice-based Construction and More	Theoretical Computer Science	Vol.849 pp.64-98	高安 敦　渡邉 洋平 *
2021/1/20	スマートコントラクトを用いたプライバシー保護集金システム	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2021)		藤谷 知季　江村 恵太　面 和成
2021/1/21	多変数公開鍵暗号の安全性評価におけるグレブナ基底計算での多項式選択	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2021)		伊藤 琢真　篠原 直行　内山 成憲 *
2021/1/22	準同型暗号を用いたプライバシー保護決定木アンサンブルによる外れ値検知	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2021)		糸数 健吾 *　王 立華　小澤 誠一 *
2021/1/22	k- 匿名化と（乱択）決定木の融合について	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2021)		野島 良　王 立華
2021/3/2	ユーザがプライバシーポリシーを読むための支援ツール構築に関する再検証	情報処理学会　第 41 回セキュリティ心理学とトラスト研究発表会		金森 祥子　佐藤 広英 *　太幡 直也 * 野島 良
2021/3/9	PNB 解析に基づくストリーム暗号 Salsa20 への差分攻撃	電子情報通信学会　2021 年電子情報通信学会総合大会		宮下 翔太郎 *　伊藤 竜馬　宮地 充子 *
2021/3/16	情報理論的に安全な完全準同型暗号に関する考察	情報処理学会　第 92 回 CSEC 研究会	Vol.2021-CSEC-No.69 pp.1-6	佐藤 慎悟　四方 順司 *
2021/3/18	鍵生成センタに対して安全な ID ベース暗号の実装評価	情報処理学会　第 83 回全国大会		佐藤 裕太 *　江村 恵太　大東 俊博
2021/4/8	Efficient revocable identity-based encryption with short public parameters	Theoretical Computer Science	Vol.863 pp.127-155	江村 恵太　Jae Hong Seo* Yohei Watanabe*
2021/4/20	Communication-Efficient Distributed SGD with Error-Feedback, Revisited	International Journal of Computational Intelligence Systems		TRAN THI PHUONG*　LE TRIEU PHONG
2021/5/5	An Anonymous Trust-Marking Scheme on Blockchain Systems	IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2021)		Teppei Sato*　江村 恵太 Kazumasa Omote*

7　サイバーセキュリティ研究所誌上発表論文一覧

発表年月日	論文名	誌名/発表機関	巻号	発表者
2021/5/13	Bit-wise Cryptanalysis on AND-RX Permutation Friet-PC	Journal of Information Security and Applications		伊藤 竜馬　芝 廉太郎 *　阪本 光星 * Fukang Liu*　五十部 孝典 *
2021/5/15	Adaptively secure revocable hierarchical IBE from k -linear assumption	Designs, Codes and Cryptography		江村 恵太　高安 敦　渡邉 洋平 *
2021/5/19	検索可能暗号を用いた暗号化ストレージ・チャットシステムの実装評価	電子情報通信学会　情報セキュリティ研究会（ISEC）		江村 恵太　金森 祥子　野島 良 渡邉 洋平 *
2021/6/3	Tag-based ABE in prime-order groups via pair encoding	Designs, Codes and Cryptography	Vol.89 No.8 pp.1927-1963	高安 敦
2021/6/5	Adaptively Secure Lattice-based Revocable IBE in the QROM: Compact Parameters, Tight Security, and Anonymity	Designs, Codes and Cryptography	Vol.89 No.8 pp.1965-1992	高安 敦
2021/7/1	Security Analysis of End-to-End Encryption for Zoom Meetings	IEEE Access		伊藤 竜馬　五十部 孝典 *
2021/7/20	Outlier Detection by Privacy-Preserving Ensemble Decision Tree Using Homomorphic Encryption	IJCNN 2021：International Joint Conference on Neural Networks		Kengo Itokazu*　王 立華　Seiichi Ozawa*
2021/7/20	ハイブリッド乗法的秘密分散	セキュリティサマーサミット 2021（電子情報通信学会 EMM 研究会）	Vol.121 No.123 pp.136-140	吉田 真紀
2021/7/21	乗法的秘密分散の実現不可能性と通信複雑性	LA Symposium 2021　夏の LA		吉田 真紀
2021/8/20	A Privacy-Preserving Enforced Bill Collection System using Smart Contracts	16th Asia Joint Conference on Information Security (AsiaJCIS2021)		Tomoki Fujitani　江村 恵太 Kazumasa Omote
2021/9/1	A Compact Digital Signature Scheme Based on the Module-LWR Problem	IEICE Transactions on Fundamentals of Electronics, Communications, and Computer Sciences	Vol.E104-A No.9 pp.1219-1234	岡田 大樹 *　高安 敦　福島 和英 * 清本 晋作 *　高木 剛 *
2021/9/9	Decentralized Descent Optimization With Stochastic Gradient Signs for Device-to-Device Networks	IEEE Wireless Communications Letters (IEEE WCL)	Vol.10 pp.1939-1943	TRAN THI PHUONG*　LE TRIEU PHONG
2021/9/14	鍵生成センタに対して安全な ID ベース暗号の実装評価（第 2 報）	電子情報通信学会　2021 年電子情報通信学会ソサイエティ大会		江間 俊太郎　佐藤 裕太 *　江村 恵太 大東 俊博
2021/9/24	IoT-Based Autonomous Pay-As-You-Go Payment System with the Contract Wallet	Security and Communication Networks		Shinya Haga*　面 和成
2021/10/7	Security Analysis of SFrame	European Symposium on Research in Computer Security - ESORICS 2021		五十部 孝典 *　伊藤 竜馬　峯松 一彦 *
2021/10/20	Hybrid Multiplicative Secret Sharing	The 2021 IEEE Information Theory Workshop (ITW2021)		吉田 真紀
2021/10/27	エンドツーエンド暗号化 SFrame に対する安全性評価	情報処理学会　コンピュータセキュリティシンポジウム 2021（CSS2021）		五十部 孝典 *　伊藤 竜馬　峯松 一彦 *
2021/10/28	放送サービスに適したセキュアメッセージング用グループ鍵共有	情報処理学会　コンピュータセキュリティシンポジウム 2021（CSS2021）		梶田 海成 *　江村 恵太　野島 良 小川 一人　大竹 剛 *
2021/10/29	入札額の上限漏洩を防止した資金拘束型の封印入札オークション	情報処理学会　コンピュータセキュリティシンポジウム 2021（CSS2021）		陳 浩太 *　江村 恵太　佐藤 慎悟 面 和成
2021/11/4	Polynomial selection for computing Grobner bases	Japan Society for Industrial and Applied Mathematics (JSIAM) Letters	Vol.13 pp.72-75	伊藤 琢真　新田 篤志 *　星 雄大 * 篠原 直行　内山 成憲 *
2021/11/5	Verifiable Functional Encryption using Intel SGX	ProvSec 2021		Tatsuya Suzuki*　江村 恵太 Toshihiro Ohigashi*　Kazumasa Omote*
2021/11/10	遅延開示 GNSS 認証プロトコルの暗号アルゴリズムと鍵長について	日本航空宇宙学会　第 65 回宇宙科学技術連合講演会		吉田 真紀　森岡 澄夫 *　尾花 賢 *
2021/11/12	The Present and Future of Discrete Logarithm Problems on Noisy Quantum Computers	arXiv.org e-Print archive		青野 良範　Sitong Liu*　田中 智樹 * 宇野 隼平 *　Rodney Van Meter* 篠原 直行　野島 良
2021/11/25	Implementation and Evaluation of an Identity-Based Encryption with Security Against the KGC	8th International Workshop on Information and Communication Security (WICS) 2021		Shuntaro Ema*　Yuta Sato*　江村 恵太 Toshihiro Ohigashi
2021/12/1	Security Analysis of End-to-End Encryption for Zoom Meetings	The 26th Australasian Conference on Information Security and Privacy (ACISP 2021)		五十部 孝典 *　伊藤 竜馬
2021/12/3	Distinguishing and Key Recovery Attacks on the Reduced-Round SNOW-V	The 26th Australasian Conference on Information Security and Privacy (ACISP 2021)		寶木 仁 *　五十部 孝典 *　伊藤 竜馬 Fukang Liu*　阪本 光星 *
2022/1/8	Identity-based encryption with security against the KGC: A formal model and its instantiations	Theoretical Computer Science		江村 恵太　Shuichi Katsumata* Yohei Watanabe*
2022/1/10	Distinguishing and key recovery attacks on the reduced-round SNOW-V and SNOW-Vi	Journal of Information Security and Applications	Vol.65 No.103100	寶木 仁 *　五十部 孝典 *　伊藤 竜馬 Fukang Liu*　阪本 光星 *
2022/1/18	参加者情報を秘匿する非同期グループメッセージング方式	電子情報通信学会　暗号と情報セキュリティシンポジウム（SCIS2022）		江村 恵太　梶田 海成 *　野島 良 小川 一人　大竹 剛 *
2022/1/18	プライバシー情報提供の可否に関する調査 - 経年変化に関する考察 -	電子情報通信学会　暗号と情報セキュリティシンポジウム（SCIS2022）		金森 祥子　佐藤 広英 *　太幡 直也 * 野島 良
2022/1/19	動的サンプリングを使用した勾配ブースティング決定木の連合追加学習	電子情報通信学会　暗号と情報セキュリティシンポジウム（SCIS2022）		三浦 啓吾 *　王 立華　小澤 誠一 *

発表年月日	論文名	誌名/発表機関	巻号	発表者
2022/1/19	情報理論的安全性を有する宇宙ロケット用セキュア通信方式の性能実証飛行	電子情報通信学会　暗号と情報セキュリティシンポジウム（SCIS2022）	No.2F1-1 pp.1-8	森岡 澄夫＊　尾花 賢＊　吉田 真紀
2022/1/20	低リソースデバイス制御のための匿名放送型認証技術の提案	電子情報通信学会　暗号と情報セキュリティシンポジウム（SCIS2022）		青野 良範　四方 順司＊
2022/1/21	F4 -style アルゴリズムの MQ 問題に対する多項式選択方法	電子情報通信学会　暗号と情報セキュリティシンポジウム（SCIS2022）		伊藤 琢真　黒川 貴司　篠原 直行 内山 成憲＊
2022/2/2	Long-Term Secure Distributed Storage Using Quantum Key Distribution Network With Third-Party Verification	IEEE transactions on Quantum Engineering	Vol.3 No.3135077 pp.1-11	藤原 幹生　野島 良　鶴丸 豊広＊ 盛合 志帆　武岡 正裕　佐々木 雅英
2022/2/10	Construction of a Support Tool for User Reading of Privacy Policies and Assessment of its User Impact	8th International Conference on Information Systems Security and Privacy (ICISSP2022)		金森 祥子　佐藤 広英＊　太幡 直也＊ 野島 良
2022/3/3	Flight Demonstration Results of Information Theoretically Secure Wireless Communication on a Sounding Rocket MOMO	33rd International Symposium on Space Technology		Sumio Morioka*　Satoshi Obana* 吉田 真紀
2022/3/11	AES Instruction を用いたラージブロック置換の改良とその応用	電子情報通信学会　情報セキュリティ研究会（ISEC）		中橋 元輝＊　芝 廉太朗＊　阪本 光星＊ Fukang Liu*　伊藤 竜馬　峯松 一彦＊ 五十部 孝典＊
2022/3/15	プライバシーポリシーの内容を確認する状況の整理	信州大学人文科学論集第 9 号（第 2 冊）	Vol.9 No.2 pp.43-52	佐藤 広英＊　太幡 直也＊　金森 祥子 野島 良
2022/4/27	State-free End-to-End Encrypted Storage and Chat Systems based on Searchable Encryption	24th International Conference on Enterprise Information Systems (ICEIS2022)		江村 恵太　伊藤 竜馬　金森 祥子 野島 良　渡邉 洋平＊
2022/5/4	eFL-Boost: Efficient Federated Learning for Gradient Boosting Decision Trees	IEEE ACCESS	Vol.10 pp.43954-43963	Fuki Yamamoto*　Seiichi Ozawa* 王 立華
2022/5/13	Distributed differentially-private learning with communication efficiency	Journal of Systems Architecture		TRAN THI PHUONG*　LE TRIEU PHONG
2022/5/18	準同型暗号の安全性について	システム制御情報学会　第 66 回システム制御情報学会 研究発表講演会		江村 恵太
2022/5/30	Generic Construction of Public-key Authenticated Encryption with Keyword Search Revisited: Stronger Security and Efficient Construction	The 9th ACM ASIA Public-Key Cryptography Workshop (APKC 2022)		江村 恵太
2022/6/7	On Cryptographic Algorithms and Key Length for Delayed Disclosure Authentication of GNSS	2022 International Conference on Localization and GNSS (ICL-GNSS 2022)	pp.1-6	吉田 真紀　Sumio Morioka* Satoshi Obana*
2022/6/14	Decentralized Stochastic Optimization With Random Attendance	IEEE Signal Processing Letters		TRAN THI PHUONG*　LE TRIEU PHONG
2022/6/16	The Present and Future of Discrete Logarithm Problems on Noisy Quantum Computers	IEEE Transactions on Quantum Engineering	Vol.3 pp.1-21	青野 良範　Sitong Liu*　田中 智樹＊ 宇野 隼平＊　Rodney Van Meter* 篠原 直行　野島 良
2022/6/20	Keyed-Fully Homomorphic Encryption Without Indistinguishability Obfuscation	20th International Conference on Applied Cryptography and Network Security (ACNS 2022)		Shingo Sato*　江村 恵太 Atsushi Takayasu*
2022/6/23	Output Prediction Attacks on Block Ciphers using Deep Learning	4th International Workshop on Artificial Intelligence and Industrial Internet-of-Things Security (AIoTS)		木村 隼人＊　江村 恵太　五十部 孝典 伊藤 竜馬　小川 一人　大東 俊博
2022/6/27	Hybrid Multiplicative Non-perfect Secret Sharing	The 2022 IEEE International Symposium on Information Theory (ISIT)	pp.649-653	吉田 真紀
2022/7/20	LWE 仮定に基づく適応的 CCA 安全な平文一致確認可能 ID ベース暗号の効率的な構成	電子情報通信学会　情報セキュリティ研究会（ISEC）		淺野 京一　江村 恵太　高安 敦＊
2022/8/1	Secure deep learning for distributed data against malicious central server	PLOS ONE		LE TRIEU PHONG
2022/8/22	A Sealed-bid Auction with Fund Binding: Preventing Maximum Bidding Price Leakage	IEEE Blockchain 2022		陳 浩太＊　江村 恵太　佐藤 慎悟 面 和成
2022/8/25	Membership Privacy for Asynchronous Group Messaging	WISA 2022		江村 恵太　梶田 海成＊　野島 良 小川 一人　大竹 剛＊
2022/9/9	New Cryptanalysis of ZUC-256 Initialization Using Modular Differences	Transactions on Symmetric Cryptology 2022 (3)		Fukang Liu*　Willi Meier*　Santanu Sarkar* Gaoli Wang*　伊藤 竜馬　Takanori Isobe*
2022/9/9	Cryptanalysis of Rocca and Feasibility of Its Security Claim	Transactions on Symmetric Cryptology 2022 (3)		Akinori Hosoyamada*　Akiko Inoue* 伊藤 竜馬　Tetsu Iwata* Kazuhiko Minematsu* Ferdinand Sibleyras*　Yosuke Todo*
2022/9/22	動的サンプリングを用いた連合学習型勾配ブースティング決定木の継続学習	第 30 回インテリジェント・システム・シンポジウム FAN 2022	Vol.22SY0005 pp.235-239	三浦 啓吾＊　井上 広明＊　金 相旭＊ 王 立華　小澤 誠一＊
2022/10/26	CCA 安全な平文一致確認可能属性ベース暗号の一般的構成	情報処理学会　コンピュータセキュリティシンポジウム 2022（CSS2022）		淺野 京一　江村 恵太　高安 敦＊ 渡邉 洋平＊
2022/10/26	鍵付き準同型暗号の応用による制御システムの秘匿化	情報処理学会　コンピュータセキュリティシンポジウム 2022（CSS2022）		宮本 将希＊　江村 恵太　小木曽 公尚＊

7　サイバーセキュリティ研究所誌上発表論文一覧

発表年月日	論文名	誌名/発表機関	巻号	発表者
2022/11/11	A Generic Construction of CCA-Secure Attribute-Based Encryption with Equality Test	ProvSec 2022		淺野 京一　江村 恵太　高安 敦 * 渡邉 洋平 *
2022/11/12	準同型性を利用したサイバー攻撃に堅牢な暗号化制御系の構築および数値的評価	日本機械学会　第 65 回自動制御連合講演会		宮本 将希 *　江村 恵太　小木曽 公尚 *
2022/11/22	Permissioned Blockchain-based XGBoost for Multi Banks Fraud Detection	The 29th International Conference on Neural Information Processing (ICONIP 2022)	Vol.LNCS13625	Septiviana Savitri Asrori*　王 立華 Seiichi Ozawa*
2022/11/28	PNB-focused Differential Cryptanalysis of ChaCha Stream Cipher	The 27th Australasian Conference on Information Security and Privacy (ACISP 2022)		宮下 翔太郎 *　伊藤 竜馬　宮地 充子 *
2022/12/4	インターネット版プライバシー次元尺度改訂版の作成	日本パーソナリティ心理学会　第 31 回大会		佐藤 広英 *　太幡 直也 *　金森 祥子 野島 良
2022/12/6	Multi Pair Swap-Based Weather Derivative DeFi	22nd International Conference on Software Quality, Reliability and Security Companion (QRS-C 2022)		Shinya Haga*　Taisei Takahashi* 面 和成
2022/12/7	Virtual Wiretap Channel Based on Wireless Two-way Interferometry	IEEE Globecom		志賀 信泰　安田 哲　世永 公輝 滝沢 賢一　吉田 真紀
2022/12/15	Privacy-Preserving Federated Learning for Detecting Fraudulent Financial Transactions in Japanese Banks	情報処理学会論文誌特集号「持続可能な社会の IT 基盤に向けた情報セキュリティとトラスト」	Vol.30 pp.789-795	金森 祥子　阿部 妙子　伊藤 琢真 江村 恵太　王 立華　山本 俊太郎 LE TRIEU PHONG　Kaien Abe* Samgwook Kim*　野島 良 Seiichi Ozawa*　盛合 志帆
2022/12/19	Home Information Security Conference paper More Efficient Adaptively Secure Lattice-Based IBE with Equality Test in the Standard Model	The 25th International Conference on Information Security (ISC 2022)		淺野 京一　江村 恵太 Atsushi Takayasu*
2022/12/22	Polynomial selection of F4 for solving the MQ problem	Japan Society for Industrial and Applied Mathematics (JSIAM) Letters	Vol.14 pp.135-138	伊藤 琢真　星 雄大 *　篠原 直行 内山 成憲 *
2022/12/26	Differentially private stochastic gradient descent via compression and memorization	Journal of Systems Architecture		LE TRIEU PHONG　TRAN THI PHUONG*
2022/12/30	Providing Membership Privacy to the Asynchronous Ratcheting Trees Protocol without losing Scalability	Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications		江村 恵太　Kaisei Kajita*　野島 良 小川 一人　Go Ohtake*
2023/1/24	決定木と (k-) 匿名化の関係について	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2023)		若林 亮輔 *　王 立華　野島 良 早稲田 篤志
2023/1/24	BFL-Boost: Blockchain-based Federated Learning for Gradient Boosting to Enhance Security in Model Training	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2023)		Septiviana Savitri Asrori*　王 立華 Seiichi Ozawa*
2023/1/24	Non-Interactive Proof of Knowledge from Fiat-Shamir and Correlation Intractable Hash	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2023)		Zehua Shang*　大久保 美也子 Mehdi Tibouchi*　Masayuki Abe*
2023/1/24	Composition of Zero-knowledge Proof Protocols from MPC-in-the-Head with Pre-processing	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2023)		Zhiyu Peng*　大久保 美也子 Mehdi Tibouchi*　Masayuki Abe*
2023/1/25	空間計算量を考慮した M4GB アルゴリズム	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2023)		伊藤 琢真　篠原 直行　内山 成憲 *
2023/1/26	アカウントアブストラクションを利用したプライバシー保護コントラクトウォレットシステム	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2023)		陳 浩太 *　江村 恵太　面 和成
2023/2/8	Construction of a Support Tool for Japanese User Reading ofPrivacy Policies and Assessment of its User Impact	IEICE Transactions on Information and Systems	Vol.E106 No.5	金森 祥子　佐藤 広英 *　太幡 直也 * 野島 良
2023/2/24	An End-To-End Encrypted Cache System with Time-Dependent Access Control	ICISSP 2023		江村 恵太　Masato Yoshimi*
2023/2/27	Selection Strategy of F4-style Algorithm to Solve MQ Problems Related to MPKC	MDPI Cryptography		黒川 貴司　伊藤 琢真　篠原 直行 山村 明弘 *　内山 成憲 *
2023/3/1	A Generic Construction of CCA-Secure Identity-Based Encryption with Equality Test against Insider Attacks	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	No.3 pp.193-202	江村 恵太　高安 敦 *
2023/3/1	ヘルスケアデータを提供する場面におけるプライバシーに関する不安の整理	信州大学人文科学論集		佐藤 広英 *　太幡 直也 *　金森 祥子 野島 良
2023/3/6	Tornado Cash における実態調査〜 NFT フィッシング事件の事例分析とともに〜	情報処理学会　コンピューターセキュリティ研究会 (CSEC)		ユンミヌ *　陳 浩太　面 和成
2023/3/6	Areion: Highly-Efficient Permutations and Its Applications to Hash Functions for Short Input	IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES) 2023 (2)		Takanori Isobe*　伊藤 竜馬　Fukang Liu* Kazuhiko Minematsu*　Motoki Nakahashi* Kosei Sakamoto*　Rentaro Shiba*
2023/3/14	高精度時空間同期技術を活用した秘匿通信	電子情報通信学会　高信頼制御通信研究会		世永 公輝　志賀 信泰　安田 哲 滝沢 賢一　吉田 真紀
2023/4/23	Analysis of RIPEMD-160: New Collision Attacks and Finding Characteristics with MILP	EUROCRYPT 2023		Fukang Liu*　Gaoli Wang* Santanu Sarkar*　Ravi Anand* Willi Meier*　Yingxin Li*　五十部 孝典
2023/4/23	Coefficient Grouping: Breaking Chaghri and More	EUROCRYPT 2023		Fukang Liu*　Ravi Anand*　Libo Wang* Willi Meier*　五十部 孝典
2023/4/26	Continuous Group Key Agreement with Flexible Authorization and Its Applications	The 9th ACM International Workshop on Security and Privacy Analytics (IWSPA 2023)		Kaisei Kajita*　江村 恵太　小川 一人 野島 良　Go Ohtake*

発表年月日	論文名	誌名/発表機関	巻号	発表者
2023/5/11	Cybersecurity-Enhanced Encrypted Control System Using Keyed-Homomorphic Public Key Encryption	IEEE Access		Masaki Miyamoto*　Kaoru Teranishi* 江村 恵太　Kiminao Kogiso*
2023/5/17	学歴証明書 NFT を用いた企業の人気度推定システムに向けて	電子情報通信学会　情報セキュリティ研究会 (ISEC)		矢内 景梧 *　高橋 大成 *　面 和成
2023/5/17	ブロックチェーンを用いたセキュアなコンタクトトレーシング手法の検討	電子情報通信学会　情報セキュリティ研究会 (ISEC)		土田 瑞基 *　面 和成
2023/5/17	需要予測を行うスマートコントラクトを用いた VMI 構成に向けて	電子情報通信学会　情報セキュリティ研究会 (ISEC)		萩原 健太 *　面 和成
2023/5/28	Bit-level evaluation of piccolo block cipher by satisfiability problem solver	IET Information Security		Shion Utsumi*　Kosei Sakamoto* 五十部 孝典
2023/6/6	Secure Communication via GNSS-based Key Synchronization	International Conference on Localization and GNSS 2023 (ICL-GNSS 2023), Work-in-Progress in Hardware and Software for Location Computation (WIPHAL 2023)	Vol.3434	吉田 真紀　Sumio Morioka* Satoshi Obana*
2023/6/26	On the Communication Complexity of Private Function Sharing and Computation	IEEE International Symposium on Information Theory, ISIT 2023	pp.258-263	吉田 真紀
2023/7/24	外部匿名性を満たす放送型検索可能暗号の一般的構成	電子情報通信学会　情報セキュリティ研究会 (ISEC)		江村 恵太　梶田 海成 *　大竹 剛 *
2023/7/24	ヘルスケアアプリのユーザの意識調査 – 利用動機とプライバシー懸念の観点から –	情報処理学会　第 52 回セキュリティ心理学とトラスト研究発表会	No.24 pp.1-8	金森 祥子　佐藤 広英 *　太幡 直也 * 野島 良
2023/7/29	Differentially-Private Distributed Machine Learning with Partial Worker Attendance: A Flexible and Efficient Approach	CITA 2023: The 12th Conference on Information Technology and its Applications	Vol.734 pp.15-24	LE TRIEU PHONG　TRAN THI PHUONG*
2023/8/7	User Comprehension of Technical Terms in Privacy Policies and Expectations of the Privacy Protection Law in Japan	SOUPS2023 Poster		金森 祥子　池田 美穂 *　亀石 久美子 * 長谷川 彩子
2023/8/10	Compact Structure-Preserving Signatures with Almost Tight Security	Journal of Cryptology	Vol.36 No.37	Masayuki Abe*　Dennis Hofheinz* Ryo Nishimaki*　大久保 美也子 Jiaxin Pan*
2023/8/15	Development of the Edge Computing Platform based on Modular Architecture using Intel SGX	The 18th Asia Joint Conference on Information Security (AsiaJCIS 2023)		Yuma Nishihira*　Takuya Ishibashi* Yoshio Kakizaki*　大東 俊博 Hidenobu Watanabe*　Tohru Kondo* Reiji Aibara*
2023/8/18	Parallel SAT Framework to Find Clustering of Differential Characteristics and Its Applications	Selected Areas in Cryptography 2023		阪本 光星 *　伊藤 竜馬　五十部 孝典
2023/8/24	Coefficient Grouping for Complex Affine Layers	CRYPTO 2023		Fukang Liu*　Lorenzo Grassi* Clémence Bouvier*　Willi Meier* 五十部 孝典
2023/9/1	PNB Based Differential Cryptanalysis of Salsa20 and ChaCha	IEICE Transactions on Information and Systems		Nasratullah GHAFOORI*　Atsuko Miyaji* 伊藤 竜馬　Shotaro MIYASHITA*
2023/9/15	Cryptanalysis on End-to-End Encryption Schemes of Communication Tools and Its Research Trend	情報処理学会論文誌「サイバー空間を安全にするコンピュータセキュリティ技術」特集号		五十部 孝典　伊藤 竜馬　峯松 一彦 *
2023/9/15	A Deeper Look into Deep Learning-based Output Prediction Attacks Using Weak SPN Block Ciphers	Journal of Information Processing		木村 隼人 *　江村 恵太　五十部 孝典 伊藤 竜馬　小川 一人　大東 俊博
2023/9/15	アルゴリズム変換型共通鍵ブロキシ再暗号化とその実装	情報処理学会論文誌		西平 侑磨 *　鈴木 達也 *　渡邉 英伸 * 大東 俊博
2023/9/19	Distributed Stochastic Gradient Descent with Compressed and Skipped Communication	IEEE Access	Vol.11 pp.99836-99846	TRAN THI PHUONG*　LE TRIEU PHONG KAZUHIDE FUKUSHIMA*
2023/9/20	Can Sleep Apnea Be Detected from Human Pulse Waveform with Laplace Noise?	The Journal of Advanced Computational Intelligence and Intelligent Informatics (JACIII)	Vol.27 No.5 pp.942-947	Itaru Kaneko*　LE TRIEU PHONG Keita Emura*　Emi Yuda*
2023/10/17	GNSS 時刻情報を用いたセキュア通信用鍵同期機構における鍵キャッシュ設計	日本航空宇宙学会　宇宙科学技術連合講演会	No.1R07	森岡 澄夫 *　尾花 賢 *　吉田 真紀
2023/10/31	Anonymous Broadcast Authentication with Logarithmic-order Ciphertexts from LWE	The International Conference on Cryptology and Network Security (CANS)		青野 良範　四方 順司 *
2023/10/31	分散型 SNS プロトコル Nostr に対する改ざん攻撃	情報処理学会　コンピュータセキュリティシンポジウム 2023 (CSS2023)		木村 隼人 *　伊藤 竜馬　峯松 一彦 * 五十部 孝典
2023/10/31	匿名化において差分プライバシーは十分に安全な指標になっているか？	情報処理学会　コンピュータセキュリティシンポジウム 2023 (CSS2023)	pp.288-293	野島 良　王 立華　菊池 浩明 *
2023/11/1	耐量子計算機暗号の安全性評価動向	電子情報通信学会会誌	Vol.106 No.11 pp.1015-1020	青野 良範
2023/11/1	プライバシーポリシーに使用される技術用語および個人情報保護法に対するユーザの理解度の調査	情報処理学会　コンピュータセキュリティシンポジウム 2023 (CSS2023)	pp.1012-1019	金森 祥子　池田 美穂 *　亀石 久美子 * 長谷川 彩子
2023/11/9	Generic Construction of Fully Anonymous Broadcast Authenticated Encryption with Keyword Search with Adaptive Corruptions	IET Information Security		江村 恵太

7　サイバーセキュリティ研究所誌上発表論文一覧

発表年月日	論文名	誌名/発表機関	巻号	発表者
2023/11/23	Differential Private (Random) Decision Tree without Adding Noise	The 2023 International Conference on Neural Information Processing (ICONIP2023)	Vol.CCIS1963 pp.162-174	野島 良　王 立華
2023/12/6	A technique to reduce memory usage of M4GB algorithm	Japan Society for Industrial and Applied Mathematics (JSIAM) Letters	Vol.15 pp.125-128	伊藤 琢真　小林 耕太郎 *　黒川 貴司 篠原 直行　内山 成憲 *
2023/12/8	Key Committing Security of AEZ and More	IACR Transactions on Symmetric Cryptology		Yu Long Chen* Antonio Florez-Gutierrez*　Akiko Inoue* 伊藤 竜馬　Tetsu Iwata* Kazuhiko Minematsu*　Nicky Mouha* Yusuke Naito*　Ferdinand Sibleyras* Yosuke Todo*
2024/1/5	Frameworks for Privacy-Preserving Federated Learning	IEICE TRANSACTIONS ON INFORMATION AND SYSTEMS	Vol.107 No.1 pp.2-12	LE TRIEU PHONG　TRAN THI PHUONG* 王 立華　Seiichi Ozawa*
2024/1/23	深層学習ベースの出力予測攻撃が共通鍵暗号設計に及ぼす効果	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2024)		渡部 颯斗 *　伊藤 竜馬　大東 俊彦
2024/1/24	プライバシーバジェットの決定にデータ提供者の意思を反映させるにはどうすればいいか？：文献調査，問題整理と一提案	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2024)		小野 元　紀伊 真昇 *
2024/1/24	決定木への k- 匿名性と l- 多様性の適用	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2024)		伊藤 優策 *　王 立華　野島 良 早稲田 篤志 *
2024/1/24	Expanding Challenge Space on Composing Generalized Sigma-Protocols	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2024)		Shang Zehua*　大久保 美也子 Masayuki Abe*　Mehdi Tibouch*
2024/1/24	検索可能暗号に対する漏洩悪用攻撃の正確な性能評価に向けて	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2024)		甘田 拓海 *　並木 拓海 *　岩本 貢 * 渡邉 洋平
2024/1/24	Grobner 基底計算における第二先頭単項式の有用性	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2024)		伊藤 琢真　黒川 貴司　篠原 直行 内山 成憲 *
2024/1/24	複合的な多項式選択法を用いたグレブナー基底計算による MQ 問題の求解	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2024)		鈴木 俊博　伊藤 琢真　黒川 貴司 篠原 直行　内山 成憲 *
2024/1/25	分割統治 SAT を用いた AES と Camellia の最大差分／線形特性確率の導出	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2024)		高 和真 *　阪本 光星 *　伊藤 竜馬 芝 廉太朗 *　内海 潮音 *　五十部 孝典
2024/1/25	宇宙ロケット用セキュア通信のための GNSS 測位情報を用いた鍵同期方式	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2024)		森岡 澄夫 *　尾花 賢 *　吉田 真紀
2024/2/28	Security Evaluation of Decision Tree Meets Data Anonymization	10th International Conference on Information Systems Security and Privacy (ICISSP 2024)	pp.853-860	Ryousuke Wakabayashi*　王 立華 野島 良　Atsushi Waseda*
2024/3/7	Generic Construction of Forward Secure Public Key Authenticated Encryption with Keyword Search	ACNS 2024		江村 恵太
2024/3/13	継続学習型連合学習モデルにおける効率的なリプレイデータの選択	電子情報通信学会　RCC・ISEC・IT・WBS 合同研究会	pp.135-141	北野 優斗 *　王 立華　小澤 誠一 *
2024/3/21	分散型 SNS プロトコル Nostr に対する改ざん攻撃の網羅的調査	電子情報通信学会　情報通信システムセキュリティ研究会 (ICSS 研究会)		木村 隼人 *　伊藤 竜馬　峯松 一彦 * 五十部 孝典
2024/3/22	SIMON バリアントの脆弱な構造の特定	電子情報通信学会　情報通信システムセキュリティ研究会 (ICSS 研究会)		渡部 颯斗 *　伊藤 竜馬　大東 俊彦
2024/3/29	プライバシーポリシーの理解を促進する要因の検討―情報プライバシーおよび情報セキュリティの知識の観点から―	信州大学人文科学論集第 11 巻 2 号		佐藤 広英 *　太幡 直也 *　金森 祥子 野島 良

■サイバーセキュリティネクサス

発表年月日	論文名	誌名/発表機関	巻号	発表者
2022/8/1	東京 2020 大会のセキュリティオペレーションへの国研の協力	電子情報通信学会誌 別冊特集 東京 2020 オリンピック・パラリンピック競技大会のテクノロジーとイノベーション	Vol.105 No.8 pp.1057-1062	井上 大介　久保 正樹　寺田 健次郎 森 好樹　遠藤 由紀子　神宮 真人 松本 隆志　石原 翔太　牧田 大佑
2022/8/1	Cyber Security Cooperation of National Institute to Support the Tokyo 2020 Games	THE JOURNAL OF IEICE, Special Issue: Technology and Innovation in the Olympic and Paralympic Games Tokyo 2020	Vol.105 No.8 pp.294-300	井上 大介　久保 正樹　寺田 健次郎 森 好樹　遠藤 由紀子　神宮 真人 松本 隆志　石原 翔太　牧田 大佑
2023/12/7	One Million ASUS Routers Under Control: Exploiting ASUS DDNS to MITM Admin Credentials	Black Hat Europe		久保 正樹　森 好樹　奥川 莞多 *

■ナショナルサイバートレーニングセンター

発表年月日	論文名	誌名/発表機関	巻号	発表者
2019/1/23	ダークネットにおける深層学習を用いたボットネット協調動作の解析	電子情報通信学会　暗号と情報セキュリティシンポジウム (SCIS2019)		小松 聖矢 *　白石 啓一 *　佐藤 公信 衛藤 将史
2019/3/8	セキュリティインシデント対応に適したノンテクニカルスキルマップの提案	電子情報通信学会　第 46 回情報通信システムセキュリティ合同研究会		笠間 貴弘　安田 真悟　佐藤 公信 神薗 雅紀 *　小島 恵美 *　山口 孝夫 * 奈良 和春 *

発表年月日	論文名	誌名/発表機関	巻号	発表者
2019/3/16	初心者向け人工衛星（CanSat）入門キット（100kinSAT）の開発およびノウハウ共有 web，git を組み合わせたハードウエア独習フレームワークの提案	情報処理学会　全国大会		山本 悠介＊　服部 聖彦＊　安田 真悟 横山 輝明
2020/1/29	ネットワーク間の協調による DRDoS 攻撃対策手法	電子情報通信学会　暗号と情報セキュリティシンポジウム（SCIS2020）		中田 有哉＊　笠間 貴弘　衛藤 将史 神薗 雅紀＊　猪俣 敦夫＊　井上 博之＊
2021/1/21	ノンテクニカルスキル向上のためのサイバー演習フレームワーク	電子情報通信学会　暗号と情報セキュリティシンポジウム（SCIS2021）		小島 恵美＊　鈴木 将吾＊　野村 健太＊ 伊藤 大貴＊　神薗 雅紀＊　安田 真悟 佐藤 公信　笠間 貴弘
2022/7/25	Consideration on Automatic Generation of Injection Attacks using Neural Networks	the 2022 World Congress in Computer Science, Computer Engineering, and Applied Computing (CSCE 2022)	Vol.2022 No.9 pp.1-3	松田 健＊　園田 道夫
2022/10/24	キーボードにおける距離の概念を考慮したパスワードの脆弱性評価	情報処理学会　コンピュータセキュリティシンポジウム 2022（CSS2022）		園田 道夫　松田 健＊
2022/10/25	モダリティと感情影響に注目したデマの構文解析	情報処理学会　コンピュータセキュリティシンポジウム 2022（CSS2022）		園田 道夫　松田 健＊
2024/3/12	クラスタリングによる自由記述回答の要約と選択肢回答空間に射影による解答群間の連関の可視化	言語処理学会　第 30 回年次大会		根本 颯汰＊　藤本 一男