第 3 期中長期目標期間　ネットワークセキュリティ研究所及びサイバー攻撃対策総合研究センター誌上発表論文一覧(2011 年 4 月–2016 年 3 月)

＊外部機関所属

■ネットワークセキュリティ研究所　サイバーセキュリティ研究室

発表年月日日	論文名	誌名／発表機関	巻号	発表者
2011/4/10	Statistical Analysis of Honeypot Data and Building of Kyoto 2006+ Dataset for NIDS Evaluation	Workshop on development of large scale security-related data collection and analysis initiatives (BADGERS 2011)	pp.29-36	宋 中錫　高倉 弘喜＊　岡部 寿男＊ 衛藤 将史　井上 大介　中尾 康二
2011/4/10	nicter : A Large-Scale Network Incident Analysis System	BADGERS 2011	pp.35-43	衛藤 将史　井上 大介　宋 中錫 中里 純二　大高 一弘　中尾 康二
2011/6/1	Personalized mode transductive spanning SVM classification tree	Information Sciences	Vol.181 No.11 pp.2071-2085	Shaoning PANG*　班 涛　門林 雄基 Nikola KASABOV*
2011/6/16	災害時における大規模ダークネット観測網の活用に関する検討	電子情報通信学会　インターネットアーキテクチャ／情報通信システムセ キュリティ研究会 (IA/ICSS)		井上 大介　中里 純二　島村 隼平＊ 衛藤 将史　中尾 康二
2011/6/17	スキャンの特徴抽出による攻撃元プロファイリング手法の提案	電子情報通信学会　インターネットアーキテクチャ／情報通信システムセ キュリティ研究会 (IA/ICSS)		衛藤 将史　高木 彌一郎　宋 中錫 井上 大介　中尾 康二
2011/7/7	Practical Network Traffic Analysis in P2P Environment	The 7th International Wireless Communications and Mobile Computing Conference	pp.1801-1807	班 涛　Shanqing GUO* Zonghua Zhang*　安藤 類央　門林 雄基
2011/7/18	Correlation Analysis between Spamming Botnets and Malware Infected Hosts	SAINT 2011 Workshop on Network Technologies for Security,, Administration and Protection (NETSAP)		宋 中錫　島村 隼平　衛藤 将史 井上 大介　中尾 康二
2011/7/26	P2P Network Traffic Analysis Using Data Mining Engines	IEICE ニューロコンピューティング研究会	Vol.111 No.157 pp.115-118	班 涛　Shanqing GUO*　衛藤 将史 井上 大介　中尾 康二
2011/9/1	An Empirical Evaluation of an Unpacking Method Implemented with Dynamic Binary Instrumentation	IEICE Transactions on Information and Systems	Vol.E94-D No.9 pp.1778-1791	金 亨燦　織井 達憲＊　吉岡 克成＊ 井上 大介　宋 中錫　衛藤 将史 四方 順司＊　松本 勉＊　中尾 康二
2011/9/15	公開型マルウェア動的解析システムに対するデコイ挿入攻撃の脅威	情報処理学会　情報処理学会論文誌	Vol.52 No.9 pp.2761-2774	笠間 貴弘　織井 達憲＊　吉岡 克成＊ 松本 勉＊
2011/10/6	Essential Discriminators for P2P Teletraffic Characterization	The 6th Joint Workshop on Information Security		班 涛　Shanqing GUO*　衛藤 将史 井上 大介　中尾 康二
2011/10/19	マルウェア対策ユーザサポートシステムを用いた CCC DATASet 2011 検体の自動検知と駆除	情報処理学会　コンピュータセキュリティシンポジウム 2011 (CSS2011)		川口 信隆＊　余田 貴幸＊　山口 演己＊ 寺田 真敏＊　笠木 敏彦＊　星澤 裕二＊ 衛藤 将史　井上 大介　中尾 康二
2011/10/21	実行毎の挙動の差異に基づくマルウェア検知手法の提案	情報処理学会　コンピュータセキュリティシンポジウム 2011 (CSS2011)		笠間 貴弘　吉岡 克成＊　井上 大介 松本 勉＊
2011/10/21	ドライブ・バイ・ダウンロード攻撃対策フレームワークの提案	情報処理学会　コンピュータセキュリティシンポジウム 2011 (CSS2011)		笠間 貴弘　井上 大介　衛藤 将史 中里 純二　中尾 康二
2011/10/21	異種センサ統合型ネットワーク観測プラットフォームの提案	情報処理学会　コンピュータセキュリティシンポジウム 2011 (CSS2011)		衛藤 将史　井上 大介　鈴木 未央 中尾 康二
2011/11/1	A Novel Malware Clustering Method Using Frequency of Function Call Traces in Parallel Threads	IEICE Transactions on Information and systems	Vol.E94-D No.11 pp.2150-2158	中里 純二　宋 中錫　衛藤 将史 井上 大介　中尾 康二
2011/11/18	Entropy based Discriminators for P2P Teletraffic Characterization	2011 International Conference on Neural Information Processing	Vol.7063 pp.18-27	班 涛　Shanqing GUO*　衛藤 将史 井上 大介　中尾 康二
2011/11/18	オリジナルコードの一部を利用した自己書き換え型マルウェアに対する類似度判定法	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)		中村 徳昭＊　伊沢 亮一＊　森井 昌克＊ 井上 大介　中尾 康二
2011/11/18	バイトコードの出現頻度に着目したマルウェアの類似度判定および機能推定法	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)		大久保 諒＊　伊沢 亮一＊　森井 昌克＊ 井上 大介　中尾 康二
2011/11/18	Network Flow Classification Based on the Rhythm of Packets	2011 International Conference on Neural Information Processing	Vol.7063 pp.45-52	Liangxiong Li*　Fengyu Wang*　班 涛 Shanqing Guo*　Bin Gong*
2011/12/1	LDA Merging and Splitting with Applications to Multi-agent Cooperative Learning and System Alteration	IEEE Transactions on Systems,, Man,, and Cybernetics,, Part B: Cybernetics		Shaoning PANG*　班 涛　門林 雄基 Nikola Kasabov*
2012/1/31	ハニーポット・トラフィック分析によるゼロデイ・リモート・エクスプロイト攻撃検出	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 (SCIS2012)		神保 千晶＊　藤井 孝好＊　村上 洸介＊ 吉岡 克成＊　四方 順司＊　松本 勉＊ 衛藤 将史　井上 大介　中尾 康二
2012/1/31	多様なセンサの観測情報を用いたマルチモーダル分析	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 (SCIS2012)		笠間 貴弘　中里 純二　鈴木 未央 衛藤 将史　井上 大介　中尾 康二 秋山 満昭＊　青木 一史＊　岩村 誠＊ 八木 毅＊　斉藤 典明＊　針生 剛男＊
2012/2/2	長期間にわたる協調動作に基づくボットネットの行動分析	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 (SCIS2012)		中里 純二　班 涛　衛藤 将史 井上 大介　中尾 康二
2012/3/9	ID・ロケータ分離ネットワークにおける統合セキュリティアプローチ	電子情報通信学会　情報ネットワーク研究会 (IN)	Vol.111 No.469 pp.365-370	Ved Prasad Kafle　李 睿棟　井上 大介 原井 洋明
2012/3/16	マルウェア対策ユーザサポートシステムのフィールド実験と性能評価	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)		笠木 敏彦＊　余田 貴幸＊　山口 演己＊ 星澤 裕二＊　衛藤 将史　井上 大介 中尾 康二

発表年月日	論文名	誌名／発表機関	巻号	発表者
2012/3/26	Malicious software detection using multiple sequence alignment and data mining	The 26th IEEE International Conference on Advanced Information Networking and Applications	pp.8-14	Yi CHEN* Ajit NARAYANAN* Shaoning PANG* 班 涛
2012/4/17	Online Social Network Platforms: Toward a Model-Backed Security Evaluation	Workshop on Privacy and Security in Online Social Media (PSOSM),, co-located with WWW'12		Le Malecot Erwan 鈴木 未央 衛藤 将史 井上 大介 中里 純二
2012/6/11	An Integrated Security Scheme for ID/Locator Split Architecture of Future Network	International Workshop on the Network of the Future ('ICC'12 WS - FutureNet')	pp.7424-7429	Ved Prasad Kafle 李 睿棟 井上 大介 原井 洋明
2012/6/12	A Study on Cost-Effective P2P Traffic Classification	The 2012 IEEE World Congress on Computational Intelligence (IEEE WCCI 2012)	pp.2216-2222	班 涛 Shanqing Guo* 衛藤 将史 井上 大介 中尾 康二
2012/6/22	nicter によるネットワーク観測および分析レポート ー DDoS 攻撃によるバックスキャッタの推移と分類ー	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.112 No.90 pp.37-42	中里 純二 島村 隼平 衛藤 将史 井上 大介 中尾 康二
2012/7/17	Malware Detection Method by Catching Their Random Behavior in Multiple Executions	The 3rd Workshop on Network Technologies for Security,, Administration and Protection (NETSAP 2012)	pp.262-266	笠間 貴弘 吉岡 克成 * 井上 大介 松本 勉 *
2012/8/10	Multipurpose Network Monitoring Platform using Dynamic Address Assignment	The 7th Asia Joint Conference on Information Security (AsiaJCIS 2012)		衛藤 将史 井上 大介 鈴木 未央 中尾 康二
2012/9/6	多段パックされたマルウェアからのコード取得	第 11 回情報科学技術フォーラム（FIT2012）		中村 徳昭 * 森井 昌克 * 伊沢 亮一 井上 大介 中尾 康二
2012/9/6	マルウェアの部分コードによる類似度判定と機能推定	第 11 回情報科学技術フォーラム（FIT2012）		大久保 諒 * 森井 昌克 * 伊沢 亮一 井上 大介 中尾 康二
2012/10/15	Malware Sandbox Analysis with Efficient Observation of Herder's Behavior	情報処理学会　情報処理学会論文誌	Vol.20 No.4 pp.835-845	笠間 貴弘 吉岡 克成 * 松本 勉 * 山形 昌也 衛藤 将史 井上 大介 中尾 康二
2012/10/15	DAEDALUS-VIZ: Novel Real-time 3D Visualization for Darknet Monitoring-based Alert System	VizSec 2012		井上 大介 鈴木 宏栄 鈴木 未央 衛藤 将史 中尾 康二
2012/10/30	多段パックされたマルウェアからのコード取得	マルウェア対策研究人材育成ワークショップ 2012	Vol.2012 No.3 pp.15-21	中村 徳昭 * 森井 昌克 * 伊沢 亮一 井上 大介 中尾 康二
2012/10/30	マルウェアの部分コードによる類似度判定および機能推定法	マルウェア対策研究人材育成ワークショップ 2012	Vol.2012 No.3 pp.9-14	大久保 諒 * 森井 昌克 * 伊沢 亮一 井上 大介 中尾 康二
2012/10/31	ハイブリットセフト攻撃に耐性のある相互認証方式	情報処理学会　コンピュータセキュリティシンポジウム 2012（CSS2012）	Vol.2012 No.3 pp.609-616	國貞 勇人 * 伊沢 亮一 森井 昌克 *
2012/11/14	TrafficS: a behavior-based network Traffic classification benchmark system with traffic Sampling functionality	The 19th International Conference on Neural Information Processing (ICONIP 2012)	Vol.7666 pp.100-107	Xiaoyan YAN* Bo LIANG* 班 涛 Shanqing GUO* Liming WANG*
2012/11/14	Training Minimum Enclosing Balls for Cross Tasks Knowledge Transfer	The 19th International Conference on Neural Information Processing (ICONIP 2012)	Vol.7663 pp.375-382	Shaoning PANG* Fan LIU* 門林 雄基 班 涛 井上 大介
2012/11/14	SDE-Driven Service Provision Control	The 19th International Conference on Neural Information Processing (ICONIP 2012)	Vol.7663 pp.260-268	Gang CHEN* Shaoning PANG* Abdolhossein SARRAFZADEH* 班 涛 井上 大介
2012/11/17	The effects of different representations on malware motif identification	International Conference on Computational Intelligence and Security 2012 (CIS 2012)	pp.86-90	Ajit NARAYANAN* Yi CHEN* Shaoning PANG* 班 涛
2012/11/22	マルチモーダル分析による不正通信の検出	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）		笠間 貴弘 衛藤 将史 井上 大介
2012/11/22	マルウェアのバイナリを用いた機械学習によるパッカの特定手法の提案	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）	Vol.112 No.315 pp.19-24	伊沢 亮一 班 涛 井上 大介
2012/12/1	Towards Cost-Effective P2P Traffic Classification in Cloud Environment	IEICE Transactions on Information and systems	Vol.E95-D No.12 pp.2888-2897	班 涛 Shanqing Guo* 衛藤 将史 井上 大介 中尾 康二
2012/12/1	無線通信環境における認証データベースを用いない匿名認証方式	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	Vol.E95-A No.12 pp.2488-2492	伊沢 亮一 森井 昌克 *
2013/1/1	Catching the Behavioral Differences between Multiple Executions for Malware Detection	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	Vol.E96-A No.1 pp.225-232	笠間 貴弘 吉岡 克成 * 井上 大介 松本 勉 *
2013/1/22	マルウェアのアンパックコードのバイト列に基づく SVM を用いたパッカー特定手法	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（SCIS2013）		伊沢 亮一 班 涛 井上 大介
2013/1/24	マルウェアの攻撃プロセスに着目したマルチモーダル分析	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（SCIS2013）		笠間 貴弘 中里 純二 衛藤 将史 井上 大介 中尾 康二 秋山 満昭 * 岩村 誠 * 八木 毅 * 斉藤 典昭 * 針生 剛男 *
2013/1/24	ブラウザ組込型センサとゲートウェイセンサの観測情報を用いたマルウェア感染ホストの検出	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（SCIS2013）		笠間 貴弘 嶌田 一郎 衛藤 将史 井上 大介

発表年月日	論文名	誌名／発表機関	巻号	発表者
2013/1/25	マルウェアの部分コード取得による類似度判定	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（SCIS2013）		平野 亮＊　中村 徳昭＊　森井 昌克＊ 伊沢 亮一　井上 大介　中尾 康二
2013/1/25	DoS 攻撃の分類に向けたバックスキャッタ分析	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（SCIS2013）		中里 純二　島村 隼平　衛藤 将史 井上 大介　中尾 康二
2013/1/25	IPv6 環境におけるセキュリティ上の脅威の分類と対策の検討	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（SCIS2013）	Vol.4D2-3	衛藤 将史　鈴木 未央　井上 大介 中尾 康二
2013/2/1	Design and Implementation of Security for HIMALIS Architecture of Future Networks	IEICE Transactions on Information and System	Vol.E96-D No.2 pp.226-237	Ved Prasad Kafle　李 睿棟　井上 大介 原井 洋明
2013/2/28	Dynamic class imbalance learning for incremental LPSVM	Neural Networks	Vol.2013 No.44 pp.87-100	Shaoning Pang*　Lei Zhu*　Gang Chen* Abdolhossein Sarrafzadeh＊　班 涛 井上 大介
2013/6/20	Hard Learning Problems に基づいた三者間における安全な匿名認証方式	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.112 No.499 pp.13-18	岸部 功太郎＊　伊沢 亮一　森井 昌克＊
2013/6/21	nicter によるネットワーク観測および分析レポート －ネットワークインシデントの前兆－	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）		中里 純二　島村 隼平　衛藤 将史 井上 大介　中尾 康二
2013/6/21	サイバーセキュリティ情報遠隔分析基盤 NONSTOP	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.113 No.94 pp.85-90	竹久 達也　井上 大介　衛藤 将史 吉岡 克成＊　笠間 貴弘　中里 純二 中尾 康二
2013/6/21	データ実行防止機能を用いた汎用的なアンパッキング手法の提案	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）	Vol.112 No.499 pp.73-78	伊沢 亮一　神薗 雅紀　井上 大介
2013/7/19	nicter によるネットワーク観測および分析レポート －組み込みシステムに感染するマルウエアー	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）		中里 純二　島村 隼平　衛藤 将史 井上 大介　中尾 康二
2013/7/23	An Incremental Learning Approach to Continuous Images Change Detection	The 2013 9th International Conference on Natural Computation (ICNC'13) and the 2013 10th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD'13)		Lei Song*　Shaoning Pang* Hossein Sarrafzadeh*　班 涛　井上 大介
2013/7/25	Efficient Malware Packer Identification Using Support Vector Machines with Spectrum Kernel	The 8th Asia Joint Conference on Information Security	pp.69-76	班 涛　伊沢 亮一　Shanqing Guo* 井上 大介　中尾 康二
2013/8/5	The Effects of Different Representations on Static Structure Analysis of Computer Malware Signatures	The Scientific World Journal	Vol.2013 pp.1-8	Ajit Narayanan*　Yi Chen* Shaoning Pang*　班 涛
2013/8/5	Application of String Kernel based Support Vector Machine for Malware Packer Identification	International Joint Conference on Neural Networks	pp.2410-2417	班 涛　伊沢 亮一　Shanqing　Guo* 井上 大介　中尾 康二
2013/8/5	Chunk Incremental IDR/QR LDA Learning	International Joint Conference on Neural Networks	pp.2225-2232	Yiming Peng*　Shaoning Pang* Gang Chen*　Hossein Sarrafzadeh* 班 涛　井上 大介
2013/10/23	ダークネットモニタリングによる DNS トラフィック分析	情報処理学会　コンピュータセキュリティシンポジウム 2013（CSS2013）		中里 純二　島村 隼平　衛藤 将史 井上 大介　中尾 康二
2013/10/23	Exploit Kit の特徴を用いた悪性 Web サイト検知手法の提案	情報処理学会 マルウェア対策研究人材育成ワークショップ 2013（MWS2013）		笠間 貴弘　神薗 雅紀　井上 大介
2013/10/23	ダークネットトラフィックデータの解析によるサブネットの脆弱性判定に関する研究	情報処理学会　コンピュータセキュリティシンポジウム 2013（CSS2013）	Vol.2013 No.4 pp.723-728	西風宗典＊　班 涛　小澤誠一＊
2013/11/3	Referential kNN Regression for Financial Time Series Forecasting	The 20th International Conference on Neural Information Processing (ICONIP 2013)	Vol.2013 No.1 pp.601-608	班 涛　張 睿彬　Shaoning Pang* Abdolhossein Sarrafzadeh*　井上 大介
2013/11/3	汎用的なアンパッキング手法の提案	The 6th International Workshop on Data Mining and Cybersecurity	Vol.8226 pp.593-600	伊沢 亮一　神薗 雅紀　井上 大介
2013/11/12	実行命令系列の出現順序に着目した OEP 特定手法の提案	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）	Vol.113 No.288 pp.13-18	中村 徳昭＊　森井 昌克＊　伊沢 亮一 井上 大介　中尾 康二
2013/11/12	非負値行列分解を用いたボットネット検出実験	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）		川村 勇気＊　島村 隼平　中里 純二 吉岡 克成＊　衛藤 将史　井上 大介 竹内 純一　中尾 康二
2013/11/30	A Learner-Independent Knowledge Transfer Approach to Multi-task Learning	Cognitive Computation	Vol.2013	Shaoning Pang*　Fan Liu*　門林 雄基 班 涛　井上 大介
2013/12/18	User Travelling Pattern Prediction via Indistinct Celluar Data Mining	The 10th IEEE International Conference on Ubiquitous Intelligence and Computing	pp.17-24	Jingwei Wang*　Neil Y. Yen*　Bin Guo* Runhe Huang*　Jianhua Ma*　班 涛 Hong Zhao*
2014/1/1	SVM を用いたパッカー特定手法	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	Vol.E97-A No.1 pp.253-263	伊沢 亮一　班 涛　Shanqing Guo* 井上 大介　中尾 康二
2014/1/22	攻撃元ホストの振る舞い分類を用いたダークネットトラフィックの分析	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（SCIS2014）		土性 文哉＊　笠間 貴弘　島村 隼平 中里 純二　井上 大介　佐々木 良一＊
2014/1/23	DNS アンプ攻撃の早期対策を目的とした DNS ハニーポットとダークネットの突合分析	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（SCIS2014）		牧田 大佑＊　吉岡 克成＊　松本 勉＊ 中里 純二　島村 隼平　井上 大介
2014/1/24	スパムメールに対するオンライン悪性度判定システムの開発	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（SCIS2014）		多田 隼輔＊　中里 純二　班 涛 小澤 誠一＊

8　第 3 期中長期目標期間　ネットワークセキュリティ研究所及びサイバー攻撃対策総合研究センター誌上発表論文一覧

発表年月日	論文名	誌名／発表機関	巻号	発表者
2014/3/5	インシデント分析センタ NICTER とそのスピンオフ技術 ーセキュリティビッグデータへの挑戦ー	第 5 回暗号フロンティア研究会講演		井上 大介
2014/3/6	文字出現頻度をパラメータとした機械学習による悪質な難読化 JavaScript の検出	情報処理学会　第 158 回 DPS・第 64 回 CSEC 合同研究発表会		西田 雅太＊　星澤 裕二＊　笠間 貴弘 衛藤 将史　井上 大介　中尾 康二
2014/3/7	Exploit kit 検知用シグネチャの動的解析に基づく自動作成	情報処理学会　第 158 回 DPS・第 64 回 CSEC 合同研究発表会		柴原 健一＊　笠間 貴弘　神薗 雅紀 吉岡 克成＊　松本 勉＊
2014/3/28	メール転送経路に着目したスパムメール分析	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）		中里 純二　班 涛　島村 隼平 衛藤 将史　井上 大介　中尾 康二
2014/3/28	能動的サイバー攻撃観測プラットフォーム GHOST センサの実装と評価	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）		衛藤 将史　田中 友英＊　鈴木 宏栄 井上 大介　中尾 康二
2014/4/26	Smart Task Orderings for Active Online Multitask Learning	SIAM International Conference on Data Mining 2014 (SDM 2014 Workshop on Heterogeneous Learning)		Shaoning Pang*　Jianbei An* Jing Zhao*　Xiaosong Li*　班 涛 井上 大介　Abdolhossein Sarrafzadeh*
2014/5/21	ダークネットトラフィックデータ解析によるサブネットの分類に関する研究	第 58 回システム制御情報学会研究発表講演会 (SCI' 14)		西風 宗典＊　班 涛　中里 純二 島村 隼平　小澤 誠一＊
2014/5/21	ダークネットパケットに対する DDoS 攻撃によるバックスキャッター判定に関する研究	第 58 回システム制御 情報学会研究発表講演会 (SCI' 14)		古谷 暢章＊　班 涛　中里 純二 島村 隼平　小澤 誠一＊
2014/6/6	解析環境に依存しない文書型マルウェア動的解析システムの開発	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)		神薗 雅紀　岩本 一樹＊　笠間 貴弘 衛藤 将史　井上 大介　中尾 康二
2014/6/6	クライアント環境に応じたリダイレクト制御に着目した悪性 Web サイト検出手法	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)		笠間 貴弘　衛藤 将史　神薗 雅紀 井上 大介
2014/7/4	Backdoor Shell に着目した不正 Web サイトを用いたサイバー攻撃基盤の分析	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)		神薗 雅紀　星澤 裕二＊　笠間 貴弘 衛藤 将史　井上 大介　吉岡 克成＊ 松本 勉＊
2014/8/27	FCDBD: Framework for Countering Drive-by Download	The 9th International Workshop on Security (IWSEC2014),, poster session		松中 隆志＊　浦川 順平＊　半井 明大＊ 窪田 歩＊　川守田 和男＊　星澤 裕二＊ 笠間 貴弘　衛藤 将史　井上 大介 中尾 康二
2014/9/4	An Approach to Detect Drive-by Download by Observing the Web Page Transition Behaviors	The 9th Asia Joint Conference on Information Security (AsiaJCIS 2014)		松中 隆志＊　窪田 歩＊　笠間 貴弘
2014/9/4	Detection of DDoS Backscatter Based on TrafficFeatures of Darknet TCP Packets	The 9th Asia Joint Conference on Information Security (AsiaJCIS 2014)		古谷 暢章＊　班 涛　中里 純二 島村 隼平　北園 淳＊　小澤 誠一＊
2014/10/22	IPv6 通信の学習に基づく NDP 悪用攻撃対策手法の提案	情報処理学会 コンピュータセキュリティシンポジウム 2014 (CSS2014)		衛藤 将史　鈴木 未央　小林 悟史＊ 井上 大介　中尾 康二
2014/10/23	ライブネットにおける低速スキャン検知手法	情報処理学会 コンピュータセキュリティシンポジウム 2014 (CSS2014)	pp.458-465	嶌田 一郎　津田 侑　衛藤 将史 井上 大介
2014/10/23	ダークネットにおける Android 端末の通信分析	情報処理学会 コンピュータセキュリティシンポジウム 2014 (CSS2014)		鈴木 貴之＊　鈴木 男人＊　笠間 貴弘 島村 隼平＊　井上 大介　宮保 憲治＊
2014/10/23	マルチモーダル分析による組込みシステムからの攻撃活動状況の把握	情報処理学会 コンピュータセキュリティシンポジウム 2014 (CSS2014)		笠間 貴弘　島村 隼平＊　井上 大介
2014/10/24	実行命令系列の分類に基づいた汎用的なオリジナルエントリポイント特定手法の提案	情報処理学会 コンピュータセキュリティシンポジウム 2014 (CSS2014)	pp.1148-1155	岸部 功太郎＊　中村 徳昭＊　森井 昌克＊ 伊沢 亮一　井上 大介　中尾 康二
2014/10/31	Detecting Malicious Spam Mails: An Online MachineLearning Approach	The 21st International Conference on Neural Information Processing	Vol.8836 No.365 pp.372-	Yuli Dai*　多田 隼輔＊　班 涛 中里 純二　島村 隼平　小澤 誠一＊
2014/11/28	ダークネットトラフィック観測による DDoS バックスキャッタ判定	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）		古谷暢章＊　班 涛　中里 純二 島村 隼平＊　北園 淳＊　小澤 誠一＊
2015/1/30	PaddyFrog: Systematically Detecting Confused Deputy Vulnerability in Android Applications	Security and Communication Networks (John Wiley & Sons,, Ltd)		Jianliang Wu*　Tingting Cui*　班 涛 Shanqing Guo*　Lizhen Cui*
2015/2/28	Wi-Fi を経由した Android マルウェアのスキャン分析	電子情報通信学会 東京支部学生会 研究発表会		鈴木 男人＊　鈴木 貴之＊　笠間 貴弘 島村 隼平＊　井上 大介　宮保 憲治＊
2015/2/28	Android マルウェアデータセットを活用した通信解析	電子情報通信学会 東京支部学生会 研究発表会		鈴木 貴之＊　鈴木 男人＊　笠間 貴弘 島村 隼平＊　井上 大介　宮保 憲治＊
2015/3/4	大規模ダークネットを用いた送信元アドレス地理情報および AS 情報に基づく災害時ネットワーク死活監視	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.114 No.489 pp.115-120	鈴木 未央　島村 隼平　中里 純二 井上 大介　衛藤 将史　中尾 康二
2015/4/1	GHOST Sensor: A Proactive Cyber Attack Monitoring Platform	IEICE Transactions on Information and Systems	Vol.E98-D No.4 pp.788-795	衛藤 将史　田中 友英＊　鈴木 宏栄 鈴木 未央　井上 大介　中尾 康二
2015/5/15	An Online Malicious Spam Email Detection System Using Resource Allocating Network with Locality Sensitive Hashing	Journal of Intelligent Learning Systems and Application	Vol.7 No.2 pp.42-57	Siti-Hajar-Aminah Ali*　小澤 誠一＊ 中里 純二　班 涛　島村 隼平
2015/5/20	ダークネットトラフィックに基づいた DDoS バックスキャッタ判定	第 59 回システム制御情報学会研究発表講演会	Vol.59	古谷暢章　班 涛　中里 純二　島村 隼平 北園 淳＊　小澤 誠一＊
2015/6/8	Distributed Denial of Service (DDoS) Backscatter Detection System Using Resource Allocating Network with Data Selection	Memoirs of the Graduate Schools of Engineering and System Informatics Kobe University	No.7	Siti-Hajar-Aminah ALI*　古谷 暢章＊ 小澤 誠一＊　中里 純二　班 涛 島村 隼平
2015/6/19	Cross-Organizational Incident Information Sharing using a Darknet Monitoring System	Coordinating Attack Response at Internet Scale (CARIS) Workshop		鈴木 未央　井上 大介　高橋 健志

発表年月日	論文名	誌名／発表機関	巻号	発表者
2015/7/2	マルウェア対策のための研究用データセット ― MWS Datasets 2015 ―	第 70 回コンピュータセキュリティ・第 14 回セキュリティ心理学とトラスト合同研究発表会		神薗 雅紀＊　秋山 満昭＊　笠間 貴弘 村上 純一＊　畑田 充弘＊　寺田 真敏＊
2015/7/14	A Study on Association Rule Mining of Darknet Big Data	The International Joint Conference on Neural Networks,, 2015	pp.3814-3820	班 涛　衛藤 将史　Shanqing Guo* 井上 大介　中尾 康二　Runhe Huang*
2015/7/14	An Autonomous Online Malicious Spam Email Detection System Using Extended RBF Network	The 2015 International Joint Conference on Neural Networks		Siti-Hajar-Aminah Ali*　小澤誠一＊ 中里 純二　班 涛　島村 隼平
2015/7/14	A Federated Network Online Network Traffics Analysis Engine for Cybersecurity	The 2015 International Joint Conference on Neural Networks		Shaoning Pang*　Yiming., Peng*　班 涛 井上 大介　Abdolhossein Sarrafzadeh*
2015/8/10	Large-Scale Monitoring for Cyber Attacks by Using Cluster Information on Darknet Traffic Features	INNS Conference on Big Data 2015	Vol.53 pp.175-182	西風 宗典＊　小澤 誠一＊　北園 淳＊ 班 涛　中里 純二　島村 隼平
2015/8/10	IoTPOT: Analysing the Rise of IoT Compromises	The 9th USENIX Workshop on Offensive Technologies (WOOT '15)		Yin Minn Pa Pa*　Shogo Suzuki* Katsunari Yoshioka* Tsutomu Matsumoto*　笠間 貴弘 Christian Rossow*
2015/9/15	Empowering anti-malware research in Japan by sharing the MWS Datasets	IPSJ,, Journal of Information Processing	Vol.23 No.5 pp.579-588	畑田 充弘＊　秋山 満昭＊　松木 隆宏＊ 笠間 貴弘
2015/10/21	メタ情報を活用した Android アプリケーションのリスク分析手法に関する検討	情報処理学会 コンピュータセキュリティシンポジウム 2015 (CSS2015)		高橋 健志　班 涛　三村 隆夫＊ 中尾 康二
2015/10/22	ダークネットトラフィックに基づく学習型 DDoS 攻撃監視システムの開発	情報処理学会 コンピュータセキュリティシンポジウム 2015 (CSS2015)	Vol.2015 No.3 pp.1394-1401	古谷暢章＊　北園 淳＊　小澤 誠一＊ 班 涛　中里 純二　島村 隼平
2015/11/5	ベイズ意思決定を用いた低速スキャン検知手法	Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS 2015)		嶌田 一郎　津田 侑　衛藤 将史 井上 大介
2015/11/10	Fine-Grained Risk Level Quantication Schemes based on APK Metadata	The 8th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'15)		高橋 健志　班 涛　三村 隆夫＊ 中尾 康二
2015/11/18	Adaptive DDoS-Event Detection from Big Darknet Traffic Data	the 22nd International Conference on Neural Information Processing (ICONIP2015)	Vol.9492 pp.376-383	古谷 暢章＊　北園 淳＊　小澤 誠一＊ 班 涛　中里 純二　島村 隼平
2015/11/26	通信プロトコルのヘッダの特徴に基づくパケット検知ツール tkiwa の実装と NICTER への導入	電子情報通信学会　情報システムセキュリティ研究会 (ICSS)		小出 駿＊　牧田 大佑　笠間 貴弘 鈴木 未央　井上 大介　中尾 康二 吉岡 克成＊　松本 勉＊
2015/11/27	プロセスの出現頻度を用いた不審プロセス特定	電子情報通信学会　情報システムセキュリティ研究会 (ICSS)		中里 純二　津田 侑　衛藤 将史 井上 大介　中尾 康二
2015/12/9	Fine-Grained Risk Level Quantification Schemes Based on APK Metadata	the 22nd International Conference on Neural Information Processing (ICONIP2015)	Vol.9491 pp.663-673	高橋 健志　班 涛　三村 隆夫＊ 中尾 康二
2015/12/9	MonkeyDroid: Detecting Unreasonable Privacy Leakages of Android Applications	the 22nd International Conference on Neural Information Processing (ICONIP2015)	Vol.9491 pp.384-391	Kai Ma*　Mengyang Liu* Shanqing Guo*　班 涛
2016/1/22	次元圧縮によるダークネットトラフィックデータの可視化	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（SCIS2016）		北園 淳＊　古谷 暢章＊　宇川 雄樹＊ 班 涛　島村 隼平　中里 純二 小澤 誠一＊
2016/1/22	サンドボックス情報収集ツール SandPrint によるマルウェア動的解析環境の実態調査	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（SCIS2016）		横山 日明＊　石井 攻＊　田辺 瑠偉＊ 笠間 貴弘　吉岡 克成＊　松本 勉＊
2016/2/1	パッシブ観測とアクティブ観測を組み合わせた組込み機器の攻撃活動状況の把握	電子情報通信学会　論文誌	Vol.J99-A No.2 pp.94-105	笠間 貴弘　島村 隼平＊　井上 大介
2016/2/15	重要情報へのファイルアクセス失敗挙動に基づく情報探索型マルウェア検知手法	情報処理学会　情報処理学会論文誌	Vol.57 No.2 pp.597-610	田辺 瑠偉＊　笠間 貴弘　吉岡 克成＊ 松本 勉＊
2016/3/3	自律学習能力を有する悪性スパムメール検出システム	電子情報通信学会　情報システムセキュリティ研究会 (ICSS)	Vol.50 pp.19-24	小坂 翔吾＊　北園 淳＊　班 涛 小澤 誠一＊　中里 純二　島村 隼平
2016/3/3	ダークネットトラフィック解析による学習型 DDoS バックスキャッタ検出システム	電子情報通信学会　情報システムセキュリティ研究会 (ICSS)	Vol.67 pp.123-128	宇川 雄樹＊　北園 淳＊　小澤 誠一＊ 班 涛　中里 純二　島村 隼平
2016/3/4	プロセスの出現頻度や通信状態に着目した不審プロセス判定	電子情報通信学会　情報システムセキュリティ研究会 (ICSS)		中里 純二　津田 侑　衛藤 将史 井上 大介　中尾 康二
2016/3/5	バイナリデータの画像化を活用したマルウェア分類法の検討	電子情報通信学会　東京支部学生会 第 21 回研究発表会		鈴木 貴之＊　笠間 貴弘　宮保 憲治＊

■ネットワークセキュリティ研究所　セキュリティアーキテクチャ研究室

発表年月日日	論文名	誌名／発表機関	巻号	発表者
2011/7/7	Practical Network Traffic Analysis in P2P Environment	The 7th International Wireless Communications and Mobile Computing Conference	pp.1801-1807	班 涛　Shanqing GUO* Zonghua Zhang*　安藤 類央　門林 雄基
2011/9/16	暗号プロトコル評価フレームワークの国際標準 ISO/IEC 29128 と CRYPTREC における適用事例	日本応用数理学会年会		松尾 真一郎　大塚 玲 *　宮崎 邦彦 *
2011/10/19	Knuth Bendix completion algorithm を用いたマルウェアログ統合解析の高速化	情報処理学会　シンポジウム	Vol.2011 No.3 pp.101-106	安藤 類央　三輪 信介
2011/11/18	安全性と信頼性を両立した分散ストレージシステムの提案	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）	Vol.111 No.309 pp.19-24	蓑輪 正
2011/11/18	マルチテナントクラウドコンピューティング：セキュリティ上の課題とアプローチ	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　Gregory Blanc*　門林 雄基 Doudou Fall*　櫨山 寛章 *　松尾 真一郎
2011/11/29	Multifactor Authenticated Key Renewal	The Third International Conference on Trusted Systems		松尾 真一郎　森山 大輔　Moti Yung*
2011/11/29	Multifactor Authenticated Key Exchange	Lecture Notes in Computer Science (Proceedings of INTRUST 2011)		松尾 真一郎　森山 大輔　Moti Yung*
2011/12/13	TOWARD GLOBAL CYBERSECURITY COLLABORATION: CYBERSECURITY OPERATION ACTIVITY MODEL	ITU Kaleidoscope 2011		高橋 健志　門林 雄基　中尾 康二
2012/1/1	GF(3^(6・71)) 上の離散対数計算実験（676 ビットの解読）	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	Vol.E95-A No.1 pp.204-212	林 卓也 *　篠原 直行　王 立華 松尾 真一郎　白勢 政明 *　高木 剛 *
2012/1/23	DR manipulation による Windows OS の軽量アクセスフィルタ機構の構築	Communications in Computer and Information Science,, 2011,, Volume 259,, 215-227	Vol.259 pp.215-227	安藤 類央　須崎 有康 *
2012/1/30	多要素認証付き鍵更新	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（SCIS2012）		松尾 真一郎　森山 大輔　Moti Yung*
2012/1/31	DNS を利用した詐称 IP 対策の提案	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（SCIS2012）	Vol.2000 No.1 pp.1-5	守山 栄松
2012/2/1	大容量データに向けた鍵管理不要の安全で確実な分散ストレージ技術の安全性評価	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（SCIS2012）		蓑輪 正
2012/2/2	暗号プロトコル中での群構造維持可能な署名の効率について	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（SCIS2012）		大久保 美也子
2012/3/1	仮想マシンファイルアクセス実時間観測のためのドメイン間通信プロトコル	Journal of Wireless Mobile Networks,, Ubiquitous Computing and Dependable Applications	Vol.3 No.42371 pp.120-137	安藤 類央
2012/3/19	Beyond the Limitation of Prime-Order Bilinear Groups,, and Round Optimal Blind Signatures	Ninth Theory of Cryptography Conference (TCC 2012)	Vol.7194 pp.133-150	徐 在弘　Jung Hee Cheon*
2012/4/1	Short Round Sub-Linear Zero-Knowledge Argument for Linear Algebraic Relations	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	Vol.E95-A No.4 pp.776-789	徐 在弘
2012/4/17	Group to Group Commitments Do Not Shrink	Eurocrypt 2012	Vol.7237 pp.301-317	Masayuki Abe*　Kristiyan Haralambiev* 大久保 美也子
2012/4/26	Enabling Secure Multitenancy in Cloud Computing:Challenges and Approaches	Baltic Conference on Future Internet Communications		高橋 健志　Gregory Blanc*　門林 雄基 Doudou Fall*　Hiroaki Hazeyama* 松尾 真一郎
2012/5/17	Group Signatures with Message-Dependent Opening	The 5th International Conference on Pairing-Based Cryptography,, Pairing 2012		坂井 祐介 *　江村 恵太　花岡 悟一郎 * 川合 豊 *　松田 隆弘 *　面 和成 *
2012/5/18	Workshop on Usable Security (USEC 12) 参加報告	情報処理学会 SPT 研究会		金岡 晃　高橋 健志
2012/5/22	Constant-Round Multi-party Private Set Union Using Reversed Laurent Series	The 15th IACR International Conference on Practice and Theory of Public-Key Cryptography,, PKC2012	Vol.7293 pp.398-412	徐 在弘　Jung Hee Cheon* Jonathan Katz*
2012/5/23	On the Security of Dynamic Group Signatures:Preventing Signature Hijacking	The 15th IACR International Conference on Practice and Theory of Public-Key Cryptography,, PKC2012	Vol.7293 pp.715-732	Yusuke Sakai*　Jacob C.N. Schuldt* 江村 恵太　Goichiro Hanaoka* Kazuo Ohta*
2012/7/11	Poster: Visualization of user's end-to-end security risks	The 8th Symposium on Usable Privacy and Security,, SOUPS2012		高橋 健志　松尾 真一郎　金岡 晃 江村 恵太　高野 祐輝
2012/7/19	利用方法に応じたリスクの可視化と適切なセキュリティ対策実施のためのアーキテクチャのグランドデザイン	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）		松尾 真一郎　金岡 晃　高橋 健志 三輪 信介　蓑輪 正
2012/7/19	インターネット上に存在するサイバーセキュリティ情報のディスカバリ技術に関する検討	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）		高橋 健志　門林 雄基　高野 祐輝
2012/7/24	Constructing Secure-Channel Free Searchable Encryption from Anonymous IBE with Partitioned Ciphertext Structure	The 7th International Conference on Security and Cryptography,, SECRYPT2012	pp.84-93	江村 恵太 Mohammad Shahriar Rahman*
2012/7/25	Flexible Group Key Exchange with On-Demand Computation of Subgroup Keys Supporting Subgroup Key Randomization	The 7th International Conference on Security and Cryptography,, SECRYPT2012	pp.353-357	江村 恵太　Takashi Sato*

発表年月日	論文名	誌名／発表機関	巻号	発表者
2012/8/1	Multi-Party Privacy-Preserving Set Intersection with Quasi-Linear Complexity	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	Vol.E95-A No.8	Jung Hee Cheon*　Stanlislaw Jarecki*　徐 在弘
2012/8/20	Short Signatures From Diffie-Hellman: Realizing Short Public Key	Cryptology ePrint Archive		徐 在弘
2012/8/30	一階述語論理を用いたクラウド構成要素の脆弱性と設定のリスク解析システム	The 7th Asia Joint Conference on Information Security (AsiaJCIS 2012)		安藤 類央
2012/9/4	Time-Specific Encryption from Forward-Secure Encryption	8th Conference on Security and Cryptography for Networks,, SCN2012	pp.184-204	Kohei Kasamatsu*　Takahiro　Matsuda*　江村 恵太　Nuttapong Attrapadung*　Goichiro Hanaoka*　Hideki Imai*
2012/9/11	RFID 認証プロトコルのプライバシーの関係	ESORICS 2012	Vol.7459 pp.661-678	森山 大輔　松尾 真一郎　大久保 美也子
2012/9/21	Group to Group Commitments Do Not Shrink	電子情報通信学会 情報セキュリティ研究会 (ISEC)		大久保 美也子
2012/10/17	Behind HumanBoost: Analysis of Users' Trust Decision Patterns for Identifying Fraudulent Websites	Journal of Intelligent Learning Systems and Applications		宮本 大輔 *　櫨山 寛章 *　門林 雄基　高橋 健志
2012/10/23	An Architecture Of Accountable SecurityIn Light Of Security Service Level Agreement	Wireless world research forum		高橋 健志　Joona Kannisto*　Seppo Heikkinen*　Bilhanan Silverajan*　Marko Helenius*　松尾 真一郎
2012/11/14	Secure Distributed Storage for Bulk Data	International Conference on Neural Information Processing (ICONIP2012)	Vol.7667 pp.566-575	蓑輪 正　高橋 健志
2012/11/14	DNS を利用した IP 詐称攻撃対策の一検討	19th International Conference on Neural Information Processing	Vol.V No.LNCS 7667 pp.599-609	守山 栄松　高橋 健志　宮本 大輔 *
2012/11/14	Training Minimum Enclosing Balls for Cross Tasks Knowledge Transfer	The 19th International Conference on Neural Information Processing (ICONIP 2012)	Vol.7663 pp.375-382	Shaoning PANG*　Fan LIU*　門林 雄基　班 涛　井上 大介
2012/12/3	On the (Im)possibility of Projecting Property in Prime-Order Setting	The 18th Annual International Conference on the Theory and Application of Cryptology and Information Security,, ASIACRYPT 2012	Vol.7658 pp.61-79	徐 在弘
2012/12/6	Linking Cybersecurity Knowledge: Cybersecurity Information Discovery Mechanism	ACSAC 2012		高橋 健志　門林 雄基　高野 祐輝
2013/1/22	汎用的結合可能性における匿名性の定式化	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（SCIS2013）		森山 大輔　Moti Yung*
2013/1/23	RFID 認証プロトコルにおける結合可能性とプライバシーモデルの関係	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（SCIS2013）		森山 大輔
2013/1/23	効率的な鍵失効機能付き ID ベース暗号 / 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（SCIS2013）		徐 在弘　江村 恵太
2013/1/23	ある弱いモデルの上でロバストな閾値暗号の一般的構成	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（SCIS2013）		坂井 祐介 *　江村 恵太　Jacob Schuldt*　花岡 悟一郎 *　太田 和夫 *
2013/1/23	巡回シフトを用いた PUF に基づくパターン照合鍵生成システムの実装評価	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（SCIS2013）		岩井 祐樹 *　森山 大輔　駒野 雄一 *　福島 崇文 *　松尾 真一郎　岩本 貢　太田 和夫　崎山 一男
2013/1/24	M2M オーバーレイネットワークにおけるビザンチン攻撃からの防御について	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（SCIS2013）	pp.1-8	蓑輪 正
2013/2/28	Revocable Identity-Based Encryption Revisited: Security Model and Construction	Public Key Cryptography		Jae Hong Seo*　江村 恵太
2013/3/1	Chosen Ciphertext Secure Keyed-Homomorphic Public-Key Encryption	PKC2013	pp.32-50	江村 恵太　花岡 悟一郎 *　大竹 剛 *　松田 隆弘 *　山田 翔太 *
2013/3/1	Efficient Delegation of Key Generation and Revocation Functionalities in Identity-Based Encryption	CT-RSA		Jae Hong Seo*　江村 恵太
2013/4/23	An Accountable Security Mechanism in Light of Security Service Level Agreement	Wireless World Research Forum (WWRF)		高橋 健志　Joona Kannisto*　Bilhanan Silverajan*　Jarmo Harju*　Marko Helenius*　松尾 真一郎
2013/5/7	証明可能安全な RFID 権限移譲プロトコルの解析と改良	LightSec 2013		森山 大輔
2013/5/7	Risk Visualization and Alerting System: Architecture and Proof-of-Concept Implementation	International Workshop on Security in Embedded Systems and Smartphones		高橋 健志　江村 恵太　金岡 晃　松尾 真一郎　蓑輪 正
2013/5/8	A Group Signature Scheme with Unbounded Message-Dependent Opening	ASIACCS2013		Kazuma Ohara*　Yusuke Sakai*　江村 恵太　Goichiro Hanaoka*
2013/5/29	RFID 認証プロトコルにおける Forward Privacy Model	WISTP 2013	Vol.7886 pp.98-111	森山 大輔　松尾 真一郎　大久保 美也子
2013/6/3	Methods for Restricting Message Space in Public-Key Encryption	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences		坂井 祐介 *　江村 恵太　花岡悟一郎 *　川合 豊 *　面 和成 *
2013/6/23	Group Signature Implies Public-key Encryption with Non-interactive Opening	International Journal of Information Security		江村 恵太　Goichiro Hanaoka*　Yusuke Sakai*　Jacob C. N. Schuldt*
2013/7/3	Toward Automated Reduction of Human Errors based on Cognitive Analysis	SEVENTH INTERNATIONAL WORKSHOP ON ADVANCES IN INFORMATION SECURITY		宮本 大輔 *　高橋 健志

発表年月日	論文名	誌名／発表機関	巻号	発表者
2013/7/8	An Accountable Security Mechanism based on Security Service Level Agreement	The Eighteenth IEEE Symposium on Computers and Communications		高橋 健志　Joona Kannisto* Seppo Heikkinen*　Bilhanan Silverajan* Marko Helenius*　松尾 真一郎 Jarmo Harju*
2013/7/17	Private Multiparty Set Intersection Protocol in Rational Model	TrustCom 2013		江村 恵太　Atsuko Miyaji* Mohammad Shahriar Rahman*
2013/7/19	証明可能安全な RFID 所有権譲渡プロトコルの解析と改良	電子情報通信学会 情報セキュリティ研究会 (ISEC)	Vol.113 No.135 pp.255-261	森山 大輔
2013/7/22	Privacy-Preserving Two-Party K-Means Clustering in Malicious Model	STPSA 2013		Rahena Akhter* Rownak Jahan Chowdhury*　江村 恵太 Tamzida Islam* Mohammad Shahriar Rahman* Nusrat Rubaiyat*
2013/7/29	Tailored Security: Building Nonrepudiable Security Service-Level Agreements	IEEE VT magazine / WWRF journal	Vol.8 No.3 pp.54-62	高橋 健志　Joona Kannisto* Jarmo Harju*　Seppo Heikkinen* Bilhanan Silverajan*　Marko Helenius* 松尾 真一郎
2013/9/4	自由な経路検証が可能な RFID 認証プロトコル	2013 IEEE International Conference on RFID Technologies and Applications		森山 大輔
2013/10/21	セキュリティ SLA に基づくユーザ毎のセキュリティレベル設定メカニズム	情報処理学会　コンピュータセキュリティシンポジウム 2013（CSS2013）		高橋 健志　Jarmo Harju*
2013/10/22	モバイル端末のリスク分析と対策の自動適用手法	情報処理学会　コンピュータセキュリティシンポジウム 2013（CSS2013）		陳 帥 *　金岡 晃　松尾 真一郎 加藤 雅彦 *　須賀 祐治 *　岡本 栄司 *
2013/10/24	オープンリゾルバと DNS サーババージョンの調査研究	Internet Conference 2013	No.72 pp.23-32	高野 祐輝　安藤 類央　高橋 健志 宇多 仁 *　井上 朋哉 *
2013/10/31	完全なメモリ漏洩に対する安全性とプライバシを保つ PUF ベース RFID 認証プロトコル	ePrint Archive		森山 大輔　松尾 真一郎　Moti Yung*
2013/11/1	On Discrete Logarithm based Additively Homomorphic Encryption	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	Vol.E96-A No.11 pp.2286-2289	Jae Hong Seo*　江村 恵太
2013/11/1	A Remark on "Efficient Revocable ID-Based Encryption with a Public Channel"	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	Vol.E96-A No.11 pp.2286-2289	Jae Hong Seo*　江村 恵太
2013/11/19	Toward Practical Searchable Symmetric Encryption	The 8th International Workshop on Security (IWSEC 2013)	pp.151-167	尾形 わかは *　小岩 敬太 *　金岡 晃 松尾 真一郎
2014/1/1	Relations among Notions of Privacy for RFID Authentication Protocols	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	Vol.E97-A No.1 pp.225-235	森山 大輔　松尾 真一郎　大久保 美也子
2014/1/21	Android 端末のリスク判定フレームワークとそのプロトタイプ構築	The 31st Symposium on Cryptography and Information Security		高橋 健志　高野 祐輝　中尾 康二 太田 悟史　金岡 晃　坂根 昌一 松尾 真一郎
2014/1/22	証明者限定署名による個人情報漏洩を考慮したアクセスログ管理	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（SCIS2014）		中川 紗菜美 *　江村 恵太　坂井 祐介 * 花岡 悟一郎 *　小舘 亮之 *
2014/1/22	署名長の短い削除機能付きグループ署名	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（SCIS2014）		大原 一真 *　坂井 祐介 *　江村 恵太 花岡 悟一郎 *　太田 和夫 *
2014/1/22	非対話開示機能付き公開鍵暗号からの頑健な閾値暗号の一般的構成	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（SCIS2014）		坂井 祐介 *　江村 恵太 Jacob C.N. Schuldt*　花岡 悟一郎 * 太田 和夫 *
2014/1/22	時限式暗号における情報の受信失敗への対策について	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（SCIS2014）		吉田 真紀　藤原 融 *
2014/1/23	メモリ漏洩に対して安全性とプライバシーを満たす PUF ベース RFID 認証プロトコル	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（SCIS2014）		森山 大輔　松尾 真一郎　Moti Yung*
2014/1/23	Physically Unclonable Functions に対する厳密なセキュリティモデル	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（SCIS2014）		森山 大輔
2014/3/1	ウェブトラッキング可視化実験報告	2013 年度 WIDE 報告書		高野 祐輝
2014/3/25	Building Secure and Anonymous Communication Channel: Formal Model and its Prototype Implementation	ACM SAC2014		江村 恵太　金岡 晃　太田 悟史 高橋 健志
2014/5/13	Chosen Ciphertext Secure Keyed-Homomorphic Public-Key Encryption	Cryptology ePrint Archive		江村 恵太　Goichiro Hanaoka* Koji Nuida*　Go Ohtake* Takahiro Matsuda*　Shota Yamada*
2014/5/20	Revocable Hierarchical Identity-Based Encryption	Theoretical Computer Science		Jae Hong Seo*　江村 恵太
2014/6/3	IHC 評価基準を満たす電子透かし法	The First International Workshop on Information Hiding and its Criteria for evaluation (IWIHC2014)	pp.31-36	戸塚 拓伸 *　吉田 真紀　藤原 融 *
2014/6/10	A Revocable Group Signature Scheme From Identity-Based Revocation Techniques: Achieving Constant-size Revocation List	ACNS2014		Nuttapong Attrapadung*　江村 恵太 Goichiro Hanaoka*　Yusuke Sakai*
2014/6/16	Mechanism for Linking and Discovering Structured Cybersecurity Information over Networks	IEEE International Conference on Semantic Computing	pp.279-284	高橋 健志　門林 雄基

発表年月日	論文名	誌名／発表機関	巻号	発表者
2014/6/27	Expressing Security Requirements: Usability of Taxonomy-based Requirement Identification Scheme	IEEE 2014 International Workshop on Security and Privacy Engineering	pp.121-128	高橋 健志　Joona Kannisto* Jarmo Harju*　金岡 晃　高野 祐輝 松尾 真一郎
2014/6/30	A Secure Genetic Algorithm for the Subset Cover Problem and its Application to Privacy Protection	WISTP 2014	pp.108-123	Dan Bogdanov*　江村 恵太 Roman Jagomägis*　金岡 晃 松尾 真一郎　Jan Willemson*
2014/7/1	Revocable Identity-Based Cryptosystem Revisited: Security Models and Constructions	IEEE Transactions on Information Forensics and Security	Vol.9 pp.1193-1205	Jae Hong Seo*　江村 恵太
2014/7/4	中間者攻撃に対して安全なプライバシ保護型 RFID Yoking-Proof プロトコル	電子情報通信学会 情報セキュリティ研究会 (ISEC)	No.12 pp.17-24	森山 大輔
2014/7/9	暗号化匿名通信プロトコルの提案とそのプロトタイプ実装	情報処理学会　情報処理学会論文誌 マルチメディア，分散，協調とモバイル (DICOMO2014) シンポジウム		江村 恵太　金岡 晃　太田 悟史 面 和成 *　高橋 健志
2014/7/23	Digital Identities and Accountable Agreements in Web Applications	International Conference on Security and Management		Joona Kannisto*　Jarmo Harju* 高橋 健志
2014/7/24	MindYourPrivacy: サードパーティウェブトラッキング可視化システムの設計と実装	Privacy Security Trust 2014	pp.48-56	高野 祐輝　太田 悟史　高橋 健志 安藤 類央　井上 朋哉 *
2014/8/1	Revocable Identity-Based Encryption with Rejoin Functionality	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	Vol.E97-A No.8 pp.1806-1809	Jae Hong Seo*　江村 恵太
2014/9/2	匿名性を有する証明可能安全なオフライン RFID Yoking-Proof プロトコル	LightSec2014		森山 大輔
2014/9/5	チュートリアル：結合可能安全性の形式検証における最近の研究動向	日本応用数理学会 2014 年度年会		吉田 真紀
2014/9/9	証明可能安全な 2 ラウンドの RFID grouping-proof プロトコル	RFID-TA 2014		森山 大輔
2014/9/18	IHC 電子透かしコンテストの高画質カテゴリにおける加法電子透かし法の性能評価	電子情報通信学会 マルチメディア情報ハイディング・エンリッチメント研究会	Vol.114 No.222 pp.53-58	戸塚 拓伸 *　吉田 真紀　藤原 融 *
2014/10/1	DNS オープンリゾルバの実態	電子情報通信学会 通信ソサイエティ 和文論文誌 将来ネットワークに向けたインターネットアーキテクチャ 特集	Vol.J97B No.10 pp.873-889	高野 祐輝　安藤 類央　宇多 仁 * 高橋 健志　井上 朋哉 *
2014/10/1	Reference Ontology for Cybersecurity Operational Information	Computer Journal		高橋 健志　門林 雄基
2014/10/5	A Non-repudiable Negotiation Protocol for Security Service Level Agreements	International Journal of Communication Systems		Joona Kannisto*　高橋 健志 Jarmo Harju*　Seppo Heikkinen* Marko Helenius*　松尾 真一郎 Bilhanan Silverajan*
2014/11/3	Data Model for Android Package Information and Its Application to Risk Analysis System	ACM Workshop on Information Sharing and Collaborative Security		高橋 健志　中尾 康二　金岡 晃
2014/11/4	MarketDrone: Android アプリケーションの動的解析フレームワーク	インターネットコンファレンス 2014	pp.129-130	加藤 邦章 *　高野 祐輝　三浦 良介 太田 悟史　篠田 陽一
2015/1/1	統計的フラジャイル電子透かしに対する改ざんピクセルの復元法	IEICE Transactions on Information and systems	Vol.98-D No.1 pp.58-64	吉田 真紀　大北 和也 *　藤原 融 *
2015/2/1	d- 乗法的不完全秘密分散の実現不能性について	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	Vol.E98-A No.2 pp.767-770	吉田 真紀　藤原 融 *
2015/3/4	カテゴリ及びクラスタに基づくアンドロイドアプリのリスク値定量化技術の検討	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)		高橋 健志　三村 隆夫 *　西田 雅太 * 中尾 康二
2015/5/22	暗号プロトコルの安全性と効率の理論限界について －安全性を情報理論的に保証する場合－	マルチメディア情報ハイディング・エンリッチメント研究会 (EMM)	Vol.115 No.38 pp.69-74	吉田 真紀
2015/6/1	SKENO: Secret Key Encryption with Non-interactive Opening	Journal of Mathematical Cryptology		Jiageng Chen*　江村 恵太 Atsuko Miyaji*
2015/6/3	Accumulable Optimistic Fair Exchange from Verifiably Encrypted Homomorphic Signatures	ACNS 2015		Jae Hong Seo*　江村 恵太 Keita Xagawa*　Kazuki Yoneyama*
2015/6/12	組織内のソフトウェア資産に対する脆弱性監視・警告自動化ツールの検討	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)		高橋 健志　宮本 大輔　パンタ ボーラ 中尾 康二
2015/6/19	Cross-Organizational Incident Information Sharing using a Darknet Monitoring System	Coordinating Attack Response at Internet Scale (CARIS) Workshop		鈴木 未央　井上 大介　高橋 健志
2015/6/29	Dynamic Threshold Public-key Encryption with Decryption Consistency from Static Assumptions	ACISP 2015		Yusuke Sakai*　Jacob C.N. Schuldt* 江村 恵太　Goichiro Hanaoka * Kazuo Ohta*
2015/7/4	A KEM/DEM-based Construction for Secure and Anonymous Communication	Compsac 2015		江村 恵太　金岡 晃　太田 悟史 高橋 健志
2015/9/16	End-to-end Design of a PUF based Privacy Preserving Authentication Protocol	Workshop on Cryptographic Hardware and Embedded Systems 2015	Vol.9293 pp.556-576	Aydin Aysu*　Ege Gulcan*　森山 大輔 Patrick Schaumont*　Moti Yung*
2015/9/24	End-to-end Design of a PUF-based Privacy Preserving Authentication Protocol	ePrint Archive		森山 大輔　Aydin Aysu*　Ege Gulcan* Patrick Schaumont*　Moti Yung*
2015/9/28	The Bright Side Arguments for the Coming Smartphones Crypto War: The Added Value of Device Encryption	IEEE Conference on Communications and Network Security (CNS) 2015	pp.65-73	森山 大輔　Moti Yung*

発表年月日日	論文名	誌名／発表機関	巻号	発表者
2015/10/21	メタ情報を活用した Android アプリケーションのリスク分析手法に関する検討	情報処理学会　コンピュータセキュリティシンポジウム 2015 (CSS2015)		高橋 健志　班 涛　三村 隆夫 * 中尾 康二
2015/11/10	Fine-Grained Risk Level Quantication Schemes based on APK Metadata	The 8th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'15)		高橋 健志　班 涛　三村 隆夫 * 中尾 康二
2015/11/26	On the (In)Efficiency of Non-Interactive Secure Multiparty Computation	The 18th Annual International Conference on Information Security and Cryptology (ICISC2015)	Vol.9558 pp.185-193	吉田 真紀　尾花 賢 *
2015/12/9	Fine-Grained Risk Level Quantification Schemes Based on APK Metadata	the 22nd International Conference on Neural Information Processing (ICONIP2015)	Vol.9491 pp.663-673	高橋 健志　班 涛　三村 隆夫 * 中尾 康二
2016/1/1	Cryptanalysis and Improvement of a Provably Secure RFID Ownership Transfer Protocol	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	Vol.E99-A No.1 pp.130-138	森山 大輔
2016/1/12	Towards a Unified Security Model for Physically Unclonable Functions	ePrint Archive		Frederik Armknecht*　森山 大輔 Ahmad-Reza Sadeghi*　Moti Yung*
2016/1/19	TLS への Logjam 攻撃の ProVerif による形式化と検出	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（SCIS2016）	No.1A1-3	木村 文哉 *　吉田 真紀　米山 一樹 *
2016/1/19	Android アプリ向けの暗号利用のための新しい鍵管理および実装評価	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（SCIS2016）		森山 大輔　金岡 晃　Moti Yung*
2016/3/1	Secure and Anonymous Communication Technique: Formal Model and its Prototype Implementation	IEEE Transactions on Emerging Topics in Computing	Vol.4 No.1 pp.88-101	江村 恵太　Akira Kanaoka*　太田 悟史 Kazumasa Omote*　高橋 健志
2016/3/3	Towards a Unified Security Model for Physically Unclonable Functions	CT-RSA 2016		森山 大輔　Frederik Armknecht* Ahmad-Reza Sadeghi*　Moti Yung*
2016/3/16	Toward Automated Vulnerability Monitoring using Open Information and Standardized Tools	PerCom 2016		高橋 健志　宮本 大輔　中尾 康二
2016/3/16	Offloading Smartphone Firewalling Using OpenFlow-capable Wireless Access Points	IEEE International Conference on Pervasive Computing and Communications		宮本 大輔　Ryo Nakamura*　高橋 健志 Yuji Sekiya*

■ネットワークセキュリティ研究所　セキュリティ基盤研究室

発表年月日日	論文名	誌名／発表機関	巻号	発表者
2011/5/12	Numerical evaluation of coherent signals for deep-space links	2011 IEEE International Conference on Space Optical Systems and Applications (ICSOS)	pp.336-344	早稲田 篤志　佐々木 雅英　武岡 正裕 藤原 幹生　豊嶋 守生　Antonio Assalini*
2011/5/19	Numerical Evaluation of PPM for Deep-Space Links	Journal of Optical Communications and Networking	Vol.3 No.6 pp.514-521	早稲田 篤志　佐々木 雅英　武岡 正裕 藤原 幹生　豊嶋 守生　Antonio Assalini*
2011/6/9	Generic Fully Simulatable Adaptive Oblivious Transfer	9th International Conference on Applied Cryptography and Network Security (ACNS '11)	Vol.6715 pp.274-291	黒澤 馨 *　野島 良　LE PHONG
2011/7/14	Generic Fully Simulatable Adaptive Oblivious Transfer (IACR Eprint)	IACR Cryptology ePrint Archive		黒澤 馨 *　野島 良　LE PHONG
2011/8/12	A Unified Framework for Small Secret Exponent Attack on RSA	Selected Areas in Cryptography 2011		國廣 昇 *　篠原 直行　伊豆 哲也 *
2011/8/15	Discrete Logarithm Based Additively Homomorphic Encryption and Secure Data Aggregation	INFORMATION SCIENCES	Vol.181 No.16 pp.3308-3322	Licheng Wang*　王 立華　Yun Pan* Zonghua Zhang*　Yixian Yang*
2011/8/22	Security analysis of generalized confidential modulation for quantum communication	The 12th international Workshop on Information security		田中 秀磨
2011/10/19	バイオメトリクス情報とプライバシー	情報処理学会　コンピュータセキュリティシンポジウム 2011 (CSS2011)		金森 祥子　川口 嘉奈子 *　田中 秀磨
2011/10/20	ブロック暗号における鍵生成関数の丸め差分特性について	情報処理学会　コンピュータセキュリティシンポジウム 2011 (CSS2011)	Vol.2011 No.3 pp.235-240	多賀 文吾　田中 秀磨　金子 敏信 *
2011/11/20	Maximum Leakage Resilient IBE and IPE	IACR Cryptology ePrint Archive		Kaoru Kurosawa*　LE PHONG
2011/11/30	電波を使った位置情報認証	第 34 回情報理論とその応用シンポジウム (SITA2011)	pp.234-239	王 立華　田中 秀磨　市川 隆一 岩間 司　小山 泰弘
2011/12/1	ブロック暗号における鍵生成関数の丸め差分特性 (2)	第 34 回情報理論とその応用シンポジウム (SITA2011)	pp.304-309	多賀 文吾　田中 秀磨　金子 敏信 *
2012/1/1	GF(3^(6・71)) 上の離散対数計算実験（676 ビットの解読）	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	Vol.E95-A No.1 pp.204-212	林 卓也 *　篠原 直行　王 立華 松尾 真一郎　白勢 政明 *　高木剛 *
2012/1/1	Identity-Based Proxy Cryptosystems with Revocability and Hierarchical Confidentialities	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	Vol.E95-A No.1pp.70-88	王 立華　Licheng Wang* Masahiro Mambo*　Eiji Okamoto*
2012/1/30	CRYPTREC における 128 ビットブロック暗号の丸め差分特性評価	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（SCIS2012）		多賀 文吾　田中 秀磨
2012/1/30	複数閾値複数秘密分散に関する一考察	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（SCIS2012）	pp.1D2-6-	早稲田 篤志　双紙 正和 *
2012/1/30	Estimation of time complexity of solving DLP over GF(3^{6n})	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（SCIS2012）		篠原 直行　下山 武司 *　林 卓也 * 高木 剛 *
2012/1/30	2 次形式を用いた pq^2 型素因数分解に関する実験的考察	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（SCIS2012）	p.27	黒川 貴司
2012/1/31	消失と誤りを含む鍵ビットによる RSA 秘密鍵の復元	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（SCIS2012）		篠原 直行　國廣 昇 *　伊豆 哲也 *
2012/1/31	位置情報とプライバシーに関する一考察	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（SCIS2012）		金森 祥子　川口 嘉奈子 *　田中 秀磨
2012/1/31	RSA に対する部分鍵導出攻撃について	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（SCIS2012）		伊豆 哲也 *　國廣 昇 *　篠原 直行
2012/2/1	A CCA Secure Threshold KEM Scheme	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（SCIS2012）		Yuanju Gan*　王 立華　Ping Pan* Licheng Wang*　Yixian Yang*
2012/2/6	暗号アルゴリズムに対する関連鍵攻撃の安全性評価	警察大学校警察情報通信研究センター　平成 23 年度研究報告		多賀 文吾
2012/2/21	Coppersmith 法の連立方程式への拡張と RSA 暗号への応用について	数理解析研究所講究録「代数系および計算機科学基礎」		青野 良範
2012/3/1	情報理論的に安全なパスワード付秘密分散法	電子情報通信学会 情報セキュリティ研究会 (ISEC)	Vol.IEICE-111 No.IEICE-IT-4 pp.41-43	早稲田 篤志　野島 良
2012/3/1	One time signature の効率的な構成の検討	情報処理学会　コンピュータセキュリティ研究会	Vol.2012-DPS-1 No.35 pp.1234-1237	双紙 正和 *　早稲田 篤志
2012/4/11	Key Length Estimation of Pairing-Based Cryptosystems Using ηT Pairing	The 8th International Conference on Information Security Practice and Experience (ISPEC 2012)	Vol.7232 pp.228-244	篠原 直行　下山 武司 *　林 卓也 * 高木 剛 *
2012/7/1	CSP-DHIES: A New Public-Key Encryption Scheme From Matrix Conjugation	Security and Communication Networks	Vol.5 No.7 pp.809-822	Ping Pan*　王 立華　Licheng Wang* Lixiang Li*　Yixian Yang*
2012/7/18	Relation between Verifiable Random Functions and Convertible Undeniable Signatures,, and New Constructions	Relation between Verifiable Random Functions and Convertible Undeniable Signatures,, and New Constructions	Vol.7372 pp.235-246	黒澤 馨 *　野島 良　LE PHONG
2012/8/8	New Leakage Resilient CCA-Secure Public Key Encryption	IACR Cryptology ePrint Archive		黒澤 馨 *　野島 良　LE PHONG

発表年月日日	論文名	誌名／発表機関	巻号	発表者
2012/9/21	GF(3^n) 上のηT ペアリングを用いたペアリング暗号の安全性評価	電子情報通信学会 情報セキュリティ研究会 (ISEC)	Vol.112 No.211 pp.1-5	林 卓也 *　下山 武司 *　篠原 直行 高木 剛 *
2012/10/29	Consideration for multi-threshold multi-secret sharing schemes	2012 International Symposium on Information Theory and its Applications	pp.265-269	早稲田 篤志　双紙 正和 *
2012/12/3	Breaking pairing-based cryptosystems using ηT pairing over GF(3^97)	The 18th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2012)	Vol.7658 pp.43-60	林 卓也 *　下山 武司 *　篠原 直行 高木 剛 *
2013/1/1	Multiparty simultaneous quantum identity authentication secure against fake signal attacks	電子情報通信学会　論文誌	Vol.E96-A No.1 pp.166-170	早稲田 篤志
2013/1/4	Efficient Construction of CCA-Secure Threshold PKE Based on Hashed Diffie-Hellman Assumption	The Computer Journal,, Oxford University Press (http://comjnl.oxfordjournals.org/)	Vol.56 No.10 pp.1249-1257	Yuanjun Gan*　王 立華　Licheng Wang* Ping Pan*　Yixian Yang*
2013/1/22	確率 1 の鍵スケジュール部差分特性を用いた Hierocrypt-L1 に対する関連鍵攻撃	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（SCIS2013）	pp.1B1-1-	多賀 文吾　盛合 志帆　青木 和麻呂 *
2013/1/23	個人情報と受動的プライバシーに関する一考察	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（SCIS2013）		金森 祥子　川口 嘉奈子 *　田中 秀磨 *
2013/1/24	Improvement of Faugère et al.'s method to solve ECDLP	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（SCIS2013）		Huang Yun Ju*　篠原 直行 Tsuyoshi Takagi*
2013/2/13	Publicly Verifiable Secret Sharing Scheme with Provable Security Against Chosen Secret Attacks	International Journal of Distributed Sensor Networks		Yuanju Gan*　王 立華　Licheng Wang* Ping Pan*　Yixian Yang*
2013/2/15	UC-Secure Multi-Session OT Using Tamper-Proof Hardware Tokens	IACR Eprint		黒澤 馨 *　野島 良　LE PHONG
2013/2/28	Recovering RSA Secret Keys from Noisy Key Bits with Erasures and Errors	The 16th International Conference on Practice and Theory in Public-Key Cryptography (PKC 2013)	Vol.7778 pp.180-197	國廣 昇 *　篠原 直行　伊豆 哲也 *
2013/6/18	Certificate-Based Proxy Decryption Systems with Revocability in the Standard Model	INFORMATION SCIENCES	Vol.247 pp.188-201	王 立華　Jun Shao*　Zhenfu Cao* 満保 雅浩 *　山村 明弘 * Licheng Wang*
2013/6/26	Leakage Resilient IBE and IPE under the DLIN assumption	The 11th International Conference on Applied Cryptography and Network Security (ACNS 2013)	Vol.7954 pp.487-501	黒澤 馨 *　LE PHONG
2013/7/3	Minkowski sum based lattice construction for multivariate simultaneous Coppersmith's technique and applications to RSA	18th Australasian Conference on Information Security and Privacy (ACISP 2013)		青野 良範
2013/7/4	Efficient Threshold PKE with Full Security Based on Dual Pairing Vector Spaces	International Journal of Communication System	Vol.27 pp.4059-4077	Yuanju Gan*　王 立華　Licheng Wang* Ping Pan*　Lixiang Li*　Yixian Yang*
2013/8/1	準同型暗号技術による位置情報認証	電子情報通信学会　論文誌 D	Vol.J96-D No.8 pp.1913-1924	田中 秀磨 *　王 立華　市川 隆一 岩間 司　小山 泰弘
2013/8/4	New leakage-resilient CCA-secure public key encryption	Journal of Mathematical Cryptology		黒澤 馨 *　野島 良　LE PHONG
2013/8/27	Efficient Lattice-Based Signcryption In Standard Model	Hindawi Publishing Corporation、Mathematical Problems in Engineering		Jianhua Yan*　Licheng Wang*　王 立華 Yixian Yang*　Wenbin Yao*
2013/9/6	データマイニングによるプライバシー侵害を防ぐデータベース構築	第 12 回情報科学技術フォーラム FIT2013	Vol.4 pp.91-98	金森 祥子　川口 嘉奈子 *　田中 秀磨 *
2013/10/1	Chameleon Hash Functions and One-Time Signature Schemesfrom Inner Automorphism Groups	Fundamenta Informaticae	Vol.126 No.1 pp.103-119	Ping Pan*　Licheng Wang* Yixian Yang*　Yuanju Gan*　王 立華 Chengqian Xu*
2013/10/23	“Mining Your Ps and Qs” のその後	情報処理学会　コンピュータセキュリティシンポジウム 2013 (CSS2013)		野島 良　黒川 貴司　盛合 志帆
2013/11/11	“Memory Retrieval and Graphical Passwords” の紹介	第 7 回 SPT 研究発表会 (SOUPS2013 論文読破会)		金森 祥子　盛合 志帆
2013/11/18	Kurosawa-Desmedt Key Encapsulation Mechanism,, Revisited	IACR Eprint Achieve		黒澤 馨 *　LE PHONG
2013/11/18	Improvement of Faugère et al.'s method to solve ECDLP	The 8th International Workshop on Security,, IWSEC2013	Vol.8231 pp.115-132	Yun-Ju Huang*　Christophe Petit* 篠原 直行　Tsuyoshi Takagi*
2013/12/4	Key-PrivateProxy Re-encryption under LWE	Indocrypt 2013		青野 良範　Xavier Boyen* Le Trieu Phong*　Lihua Wang*
2014/1/1	Key Length Estimation of Pairing-based Cryptosystems Using ηT Pairing over GF (3^n)	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	Vol.E97-A No.1 pp.236-244	篠原 直行　Takeshi Shimoyama* Takuya Hayashi*　Tsuyoshi Takagi*
2014/1/1	Relation between Verifiable Random Functions and Convertible Undeniable Signatures,, and New Constructions	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	Vol.E97-A No.1 pp.215-224	黒澤 馨 *　野島 良　LE PHONG
2014/1/21	線形代数ステップにおける Lanczos 法の実装実験	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（SCIS2014）		林 卓也 *　青木 和麻呂 *　下山 武司 * 篠原 直行　高木 剛 *
2014/1/21	Active な攻撃者に対して情報理論的秘匿性を持つパスワード認証機能付き秘密分散法	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（SCIS2014）	pp.1E1-2-	早稲田 篤志　尾形 わかは *　野島 良 盛合 志帆
2014/1/21	高速フーリエ変換を用いた線型解読法の実装および FEAL-8X に対する応用	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（SCIS2014）		先小山 翔 *　平野 亮 *　藤堂 洋介 * 青木 和麻呂 *　盛合 志帆　森井 昌克 *

発表年月日	論文名	誌名／発表機関	巻号	発表者
2014/1/22	PRINCESS: プロキシ再暗号化技術を活用したセキュアなストレージシステム	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（SCIS2014）		王 立華　早稲田 篤志　野島 良 盛合 志帆
2014/1/23	CRYPTREC 暗号技術評価委員会活動報告	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（SCIS2014）		盛合 志帆
2014/1/23	スマートフォン利用における青少年のプライバシーに関する一考察	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（SCIS2014）		金森 祥子　川口 嘉奈子 *　田中 秀磨 *
2014/1/23	Improvement of Faugère et al.'s method to solve ECDLP	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（SCIS2014）		Yun-Ju Huang*　Christophe Petit* 篠原 直行　Tsuyoshi Takagi
2014/3/10	鍵漏洩に対し安全な IBE と IPE の計算機シミュレーション	信学技報　（社団法人電子情報通信学会）		硯見 一磯 *　LE PHONG　黒澤 馨 *
2014/6/3	An *r*-hiding Revocable Group Signature Scheme: Group Signatures with the Property of Hiding the Number of Revoked Users	Journal of Applied Mathematics		江村 恵太　Atsuko Miyaji* Kazumasa Omote*
2014/6/30	A Secure Genetic Algorithm for the Subset Cover Problem and its Application to Privacy Protection	WISTP 2014	pp.108-123	Dan Bogdanov*　江村 恵太 Roman Jagomägis　金岡 晃 松尾 真一郎　Jan Willemson*
2014/7/7	Hierocrypt-L1 の関連鍵攻撃および関連鍵不能差分攻撃	ACISP 2014 (19th Australasian Conference on Information Security and Privacy)	Vol.8544 pp.17-33	多賀 文吾 *　盛合 志帆　青木 和麻呂 *
2014/7/9	暗号化匿名通信プロトコルの提案とそのプロトタイプ実装	情報処理学会　情報処理学会論文誌 マルチメディア，分散，協調とモバイル (DICOMO2014) シンポジウム		江村 恵太　金岡 晃　太田 悟史 面 和成 *　高橋 健志
2014/9/26	A Privacy-enhanced Access Log Management Mechanism in SSO Systems from Nominative Signatures	TrustCom 2014		Sanami Nakagawa*　江村 恵太 Goichiro Hanaoka*　Akihisa Kodate* Takashi Nishide*　Eiji Okamoto* Yusuke Sakai*
2014/10/17	Anonymous Data Collection System with Mediators	BalkanCryptSec 2014		Hiromi Arai*　江村 恵太 Takahiro Matsuda*
2014/10/24	国際会議 ASIACCS2014 報告	情報処理学会　コンピュータセキュリティシンポジウム 2014 (CSS2014)	No.3E4-3	穴田 啓晃 *　山内 利宏 *　堀 良彰 * 盛合 志帆　櫻井 幸一 *
2014/10/24	SNS におけるプライバシー保護技術の現状	情報処理学会　コンピュータセキュリティシンポジウム 2014 (CSS2014)	Vol.2014 No.2 pp.1177-1184	金森 祥子　川口 嘉奈子 *　田中 秀磨 *
2014/10/27	Study on a Scheme for the Right to Be Forgotten	ISITA2014(the International Symposium on Information Theory and Its Applications 2014)	pp.55-59	金森 祥子　川口 嘉奈子 *　田中 秀磨 *
2014/11/11	Road-to-Vehicle Communications with Time-Dependent Anonymity: A Light Weight Construction and its Experimental Results	IACR Cryptology ePrint Archive		江村 恵太　林 卓也
2015/1/1	Highly Secure Network Switches with Quantum Key Distribution Systems	International Journal of Network Security	Vol.17 No.1 pp.34-39	藤原 幹生　百目木 智康 *　盛合 志帆 佐々木 雅英
2015/1/15	Generic Fully Simulatable Adaptive Oblivious Transfer	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	Vol.E98-A No.1 pp.232-245	黒澤 馨 *　野島 良　LE PHONG
2015/1/20	ツケ払いに適した楽観的公平交換	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（SCIS2015）		Jae Hong Seo*　江村 恵太　草川 恵太 * 米山 一樹 *
2015/1/21	開示者指定グループ署名	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（SCIS2015）		中川 紗菜美 *　江村 恵太 花岡 悟一郎 *　金山 直樹 *　西出 隆志 * 岡本 栄司 *
2015/1/21	否認可能グループ署名	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（SCIS2015）		石田 愛 *　江村 恵太　花岡 悟一郎 * 坂井 祐介 *　田中 圭介 *
2015/1/21	検証可能暗号化準同型署名	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（SCIS2015）		Jae Hong Seo*　江村 恵太　草川 恵太 * 米山 一樹 *
2015/1/22	鍵付き準同型 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（SCIS2015）		江村 恵太　花岡 悟一郎 *　松田 隆弘 * 縫田 光司 *　山田 翔太 *
2015/1/22	A New Progressive BKZ Algorithm	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（SCIS2015）		Yuntao Wang*　青野 良範　林 卓也 高木　剛 *
2015/1/23	整数計画問題による binary-LWE 問題の求解アルゴリズム	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（SCIS2015）		町野 義貴 *　青野 良範　高安 敦 * 國廣 昇 *
2015/1/23	ITS におけるプライバシ情報漏洩に関する一考察	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（SCIS2015）	pp.4C1-2-	早稲田 篤志　野島 良
2015/1/23	セキュリティアップデータブル準同型暗号を用いた秘匿データの線形回帰計算	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（SCIS2015）		青野 良範　林 卓也　LE PHONG 王 立華
2015/1/23	PRINCESS を利用したセキュアな自動車情報共有システム	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（SCIS2015）		王 立華　野島 良　盛合 志帆
2015/1/23	A new progressive BKZ algorithm	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（SCIS2015）		王　贇弢 *　青野 良範　林 卓也 高木　剛 *
2015/1/28	否定に関する非対話ゼロ知識証明とその応用	LA シンポジウム 2014		石田 愛 *　江村 恵太　花岡 悟一郎 坂井 祐介　田中 圭介
2015/3/6	プライバシーの観点からのパーソナルデータ利活用に関する一考察	技術と社会・倫理研究会 (SITE)	Vol.SITE2014 No.76 pp.183-188	金森 祥子　川口 嘉奈子

発表年月日	論文名	誌名／発表機関	巻号	発表者
2015/3/25	ECDLP を解くアルゴリズムである FPPR 法の改良	Pacific Journal of Mathematics for Industry	Vol.7 No.1 pp.1-9	Yun-Ju Huang*　Christophe Petit* 篠原 直行　Tsuyoshi Takagi*
2015/4/14	A Secure Automobile Information Sharing System	ASIACCS2015 1st IoT Privacy,, Trust and Security Workshop		王 立華　野島 良　盛合 志帆
2015/4/14	Disavowable Public Key Encryption with Non-interactive Opening	ASIACCS2015		Ai Ishida*　江村 恵太 Goichiro Hanaoka*　Yusuke Sakai* Keisuke Tanaka*
2015/4/21	Revocable Hierarchical Identity-Based Encryption: History-Free Update,, Security Against Insiders,, and Short Ciphertexts	CT-RSA 2015	Vol.9048 pp.106-123	Jae Hong Seo*　江村 恵太
2015/4/29	Generic Constructions of Secure-Channel Free Searchable Encryption with Adaptive Security	Security and Communication Networks	pp.1547-1560	江村 恵太　Atsuko Miyaji* Mohammad Shahriar Rahman* Kazumasa Omote*
2015/7/10	Fast and Secure Linear Regression and Biometric Authentication with Security Update	IACR Eprint		青野 良範　林 卓也　LE TRIEU PHONG 王 立華
2015/7/15	否認開示機能付き公開鍵暗号	ＬＡシンポジウム 2015		石田 愛＊　江村 恵太　花岡 悟一郎＊ 坂井 祐介＊　田中 圭介＊
2015/7/20	Japan CRYPTREC Activity on Lightweight Cryptography	NIST Lightweight Cryptography Workshop 2015		盛合 志帆
2015/8/20	Keyword Revocable Searchable Encryption with Trapdoor Exposure Resistance and Re-generateability	Trustcom 2015		江村 恵太　LE PHONG Yohei Watanabe*
2015/8/26	Adaptive-ID Secure Revocable Hierarchical Identity-Based Encryption	IWSEC 2015		Jae Hong Seo*　江村 恵太
2015/9/10	A Light-weight Group Signature Scheme with Time-token Dependent Linking	LightSec 2015		江村 恵太　林 卓也
2015/10/1	Revocable Group Signature with Constant-Size Revocation List	The Computer Journal	Vol.58 pp.2698-2715	Nuttapong Attrapadung*　江村 恵太 Goichiro Hanaoka*　Yusuke Sakai*
2015/10/6	Can We Securely Use CBC Mode in TLS1.0?	AsiaARES 2015	Vol.9357 pp.151-160	黒川 貴司　野島 良　盛合 志帆
2015/10/13	PRINCESS: A Secure Cloud File Storage System for Managing Data with Hierarchical Levels of Sensitivity	22nd ACM Conference on Computer and Communications Security (ACM CCS2015)	pp.1684-1686	王 立華　林 卓也　金森 祥子 早稲田 篤志　野島 良　盛合 志帆
2015/10/23	車々間通信におけるプライバシ漏洩の実証実験	情報処理学会　コンピュータセキュリティシンポジウム 2015 (CSS2015)	Vol.2015 No.3 pp.1273-1280	早稲田 篤志　野島 良
2015/10/27	Hardness Estimation of LWE via Band Pruning	Cryptology ePrint Archive		青野 良範　LE TRIEU PHONG　王 立華
2015/12/1	Disavowable Public Key Encryption with Non-interactive Opening	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	Vol.E98-A No.12	Ai Ishida*　江村 恵太 Goichiro Hanaoka*　Yusuke Sakai* Keisuke Tanaka*
2016/1/1	Semi-generic Transformation of Revocable Hierarchical Identity-Based Encryption and its DBDH Instantiation	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	Vol.E99 No.1	江村 恵太　Jae Hong Seo* Taek-Young Youn*
2016/1/19	ランダム回答方式とその拡張の差分プライバシによる評価	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（SCIS2016）		早稲田 篤志　野島 良
2016/1/19	セルフレス匿名性を満たす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（SCIS2016）		石田 愛＊　江村 恵太　花岡 悟一郎＊ 坂井 祐介＊　田中 圭介＊　山田 翔太＊
2016/1/19	期間に依存した匿名性を持つグループ署名とその路車間通信への応用	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（SCIS2016）		江村 恵太　林 卓也
2016/1/19	プライバシー情報提供の可否に関する一調査	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（SCIS2016）	No.1C2-2	金森 祥子　野島 良　佐藤 広英＊ 太幡 直也＊
2016/1/20	クラウド環境に適用された再暗号化技術の安全性評価手法の考察	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（SCIS2016）		王 立華　Licheng Wang　満保 雅浩＊
2016/1/20	拡大体上の離散対数問題に対する数体篩法について	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（SCIS2016）		井上 明子＊　林 卓也　高木 剛＊
2016/1/27	グループ署名におけるセルフレス匿名性	LA シンポジウム 2015		石田 愛＊　江村 恵太　花岡 悟一郎＊ 坂井 祐介＊　田中 圭介＊　山田 翔太＊
2016/2/9	Scalable and Secure Logistic Regression via Homomorphic Encryption	IACR Cryptology ePrint Archive		青野 良範　林 卓也　LE TRIEU PHONG 王 立華
2016/2/15	Revocable hierarchical identity-based encryption via history-free approach	Theoretical Computer Science	Vol.615 pp.45-60	Jae Hong Seo*　江村 恵太
2016/2/19	Improved Progressive BKZ Algorithms and their Precise Cost Estimation by Sharp Simulator	IACR Cryptology ePrint Archive		青野 良範　王 鐘弢＊　林 卓也 高木 剛＊
2016/3/1	On the security of CBC Mode in SSL3.0 and TLS1.0	Journal of Internet Services and Information Security	Vol.6 No.1 pp.2-19	黒川 貴司　野島 良　盛合 志帆
2016/3/1	Secure and Anonymous Communication Technique: Formal Model and its Prototype Implementation	IEEE Transactions on Emerging Topics in Computing	Vol.4 No.1 pp.88-101	江村 恵太　Akira Kanaoka*　太田 悟史 Kazumasa Omote*　高橋 健志
2016/3/9	Scalable and Secure Logistic Regression via Homomorphic Encryption	ACM CODASPY 2016		青野 良範　林 卓也　LE TRIEU PHONG 王 立華

発表年月日日	論文名	誌名／発表機関	巻号	発表者
2016/3/9	**Secure Logistic Regression via Homomorphic Encryption**	The sixth ACM Conference on Data and Applications Security and Privacy	pp.142-144	青野 良範　林 卓也　LE TRIEU PHONG　王 立華
2016/3/17	**軽量暗号に関する最新動向 ー IoT 時代に向けてー**	2016 年総合大会講演論文集		盛合 志帆
2016/3/24	**Proxy Re-Encryption Schemes with Key Privacy from LWE**	IACR Eprint		LE TRIEU PHONG　王 立華　青野 良範　Manh Ha Nguyen*　Xavier Boyen*

■サイバー攻撃対策総合研究センター　サイバー防御戦術研究室

発表年月日日	論文名	誌名／発表機関	巻号	発表者
2013/5/9	Man-in-the-Browser 攻撃を行うマルウェ アの安全な動的解析手法	情報処理学会　第 61 回 CSEC・第 21 回 IOT 合同研究発表会		瀬川 達也＊　神薗 雅紀　星澤 裕二＊ 吉岡 克成＊　松本 勉＊
2013/6/20	CTF で変える情報セキュリティの現場 ～ CTF 越しに見た日本と世界のセキュリティ ～	電子情報通信学会　信学会技術研究報告		福森 大喜
2013/6/21	サイバーセキュリティ情報遠隔分析基盤 NONSTOP	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.113 No.94 pp.85-90	竹久 達也　井上 大介　衛藤 将史 吉岡 克成＊　笠間 貴弘　中里 純二 中尾 康二
2013/6/21	データ実行防止機能を用いた汎用的なアンパッキング手法の提案	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）	Vol.112 No.499 pp.73-78	伊沢 亮一　神薗 雅紀　井上 大介
2013/10/9	コンテンツ保護機構を備えたインターネット生放送システムの実現可能性の評価	情報処理学会論文誌	Vol.55 No.1 pp.300-310	津田 侑　黄 亮錦＊　森村 吉貴＊ 侯 書会＊　上原 哲太郎＊　上田 浩＊
2013/10/21	標的型攻撃情報共有のためのマルウェア感染文書の墨塗り手法	情報処理学会　情報処理学会誌「情報処理」		齊藤 真吾＊　吉岡 克成＊　神薗 雅紀 星澤 裕二＊　松本 勉＊
2013/10/21	マルウェア対策のための研究用データセットの取り組み － MWS 2013 Datasets －	情報処理学会　情報処理学会誌「情報処理」		神薗 雅紀　畑田 充弘＊　寺田 真敏＊ 秋山 満昭＊　笠間 貴弘　村上 純一＊
2013/10/23	ライブネットにおける不正通信の早期検知手法	情報処理学会　コンピュータセキュリティシンポジウム 2013（CSS2013）	pp.737-744	嶌田 一郎　津田 侑　神薗 雅紀 井上 大介　中尾 康二
2013/10/23	SNS の特性を活かした不正アカウント検知手法	情報処理学会　コンピュータセキュリティシンポジウム 2013（CSS2013）	pp.1010-1017	津田 侑　遠峰 隆史　井上 大介
2013/10/23	Exploit Kit の特徴を用いた悪性 Web サイト検知手法の提案	情報処理学会 マルウェア対策研究人材育成ワークショップ 2013（MWS2013）		笠間 貴弘　神薗 雅紀　井上 大介
2013/11/3	汎用的なアンパッキング手法の提案	The 6th International Workshop on Data Mining and Cybersecurity	Vol.8226 pp.593-600	伊沢 亮一　神薗 雅紀　井上 大介
2014/1/24	AES-NI 命令に対する例外処理攻撃のマルウェア解析への応用	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（SCIS2014）		竹久 達也　津田 侑　岩村 誠 神薗 雅紀　遠峰 隆史　福森 大喜 井上 大介
2014/3/7	Exploit kit 検知用シグネチャの動的解析に基づく自動作成	情報処理学会　第 158 回 DPS・第 64 回 CSEC 合同研究発表会		柴原 健一＊　笠間 貴弘　神薗 雅紀 吉岡 克成＊　松本 勉＊
2014/3/27	SNS ユーザ協力型の不正アカウント報告システム	情報処理学会　セキュリティ心理学とトラスト研究発表会		津田 侑　遠峰 隆史　井上 大介
2014/3/28	複数ホストを横断可能なタイムライン型イベントログ閲覧システム	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.113 No.502 pp.125-130	遠峰 隆史　津田 侑　神薗 雅紀 杉浦 一徳＊　井上 大介　中尾 康二
2014/5/22	電子文書型マルウェアからシェルコードを抽出する方法の提案	情報処理学会　コンピュータセキュリティ研究発表会		岩本 一樹＊　神薗 雅紀　津田 侑 遠峰 隆史　井上 大介　中尾 康二
2014/5/23	複数種類のハニーポットによる DRDoS 攻撃の観測	情報処理学会　コンピュータセキュリティ研究会	Vol.65 No.16	筒見 拓也＊　野々垣 嘉晃＊　田辺 瑠偉＊ 牧田 大佑　吉岡 克成＊　松本 勉＊
2014/5/23	標的型攻撃のシナリオ再現環境の構築	情報処理学会　コンピュータセキュリティ研究発表会		津田 侑　神薗 雅紀　遠峰 隆史 安田 真悟　三浦 良介　宮地 利幸 衛藤 将史　井上 大介　中尾 康二
2014/6/6	解析環境に依存しない文書型マルウェア動的解析システムの開発	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）		神薗 雅紀　岩本 一樹＊　笠間 貴弘 衛藤 将史　井上 大介　中尾 康二
2014/6/6	クライアント環境に応じたリダイレクト制御に着目した悪性 Web サイト検出手法	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）		笠間 貴弘　衛藤 将史　神薗 雅紀 井上 大介
2014/6/17	DNS ハニーポットによる DNS アンプ攻撃の観測	情報処理学会論文誌	Vol.55 No.9 pp.2021-2033	牧田 大佑　吉岡 克成＊　松本 勉＊
2014/7/4	Backdoor Shell に着目した不正 Web サイトを用いたサイバー攻撃基盤の分析	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）		神薗 雅紀　星澤 裕二＊　笠間 貴弘 衛藤 将史　井上 大介　吉岡 克成＊ 松本 勉＊
2014/10/22	複数国ダークネット観測による攻撃の局地性分析	情報処理学会　コンピュータセキュリティシンポジウム 2014（CSS2014）		鈴木 将吾＊　小出 駿＊　牧田 大佑 村上 洸介＊　笠間 貴弘　島村 隼平＊ 衛藤 将史　吉岡 克成＊　松本 勉＊ 井上 大介
2014/10/22	標的型攻撃再現のための攻撃シナリオ定義インタフェースの実装	情報処理学会　コンピュータセキュリティシンポジウム 2014（CSS2014）		津田 侑　神薗 雅紀　遠峰 隆史 安田 真悟　三浦 良介　宮地 利幸 衛藤 将史　井上 大介　中尾 康二
2014/10/22	複数のダークネット観測拠点で同時期に急増する攻撃を検知する手法の提案	情報処理学会　コンピュータセキュリティシンポジウム 2014（CSS2014）		村上 洸介＊　蒲谷 武正＊　千賀 渉＊ 鈴木 将吾＊　小出 駿＊　島村 隼平＊ 牧田 大佑　笠間 貴弘　衛藤 将史 吉岡 克成＊　井上 大介　中尾 康二
2014/10/22	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・分類手法	情報処理学会　コンピュータセキュリティシンポジウム 2014（CSS2014）		小出 駿＊　鈴木 将吾＊　牧田 大佑 村上 洸介　笠間 貴弘　島村 隼平 衛藤 将史　井上 大介　吉岡 克成 松本 勉
2014/10/23	ライブネットにおける低速スキャン検知手法	情報処理学会　コンピュータセキュリティシンポジウム 2014（CSS2014）	pp.458-465	嶌田 一郎　津田 侑　衛藤 将史 井上 大介

発表年月日日	論文名	誌名／発表機関	巻号	発表者
2014/10/23	DNS ハニーポットによる DNS Water Torture の観測	情報処理学会　コンピュータセキュリティシンポジウム 2014 (CSS2014)		牧田 大佑　吉岡 克成　松本 勉 * 島村 隼平 *　井上 大介　中尾 康二
2014/10/23	ホスト型 IDS を用いた標的型攻撃対策	情報処理学会　コンピュータセキュリティシンポジウム 2014 (CSS2014)		中里 純二　津田 侑　高木 瀧一郎 衛藤 将史　井上 大介　中尾 康二
2014/10/24	Linux 上で動作するマルウェアを安全に観測可能なマルウェア動的解析手法の提案	情報処理学会　コンピュータセキュリティシンポジウム 2014 (CSS2014)		田辺 瑠偉 *　筒見 拓也 *　小出 駿 * 牧田 大佑　吉岡 克成　松本 勉 *
2015/1/21	早期対応を目的とした統合型 DRDoS 攻撃観測システムの構築	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（SCIS2015）		牧田 大佑　西添 友美 *　小出 駿 * 筒見 拓也 *　金井 文宏 *　森 博志 * 吉岡 克成 *　松本 勉 *　井上 大介 中尾 康二
2015/1/21	ホスト型 IDS を用いた不審プロセスの特定	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（SCIS2015）		中里 純二　津田 侑　高木 瀧一郎 衛藤 将史　井上 大介　中尾 康二
2015/1/21	プロトコル非準拠のハニーポットによる DRDoS 攻撃の観測	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（SCIS2015）		西添 友美 *　牧田 大佑　吉岡 克成 * 松本 勉 *
2015/1/21	ハニーポット監視による DRDoS 攻撃の早期規模推定	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（SCIS2015）		浦川 順平 *　澤谷 雪子 *　山田 明 * 窪田 歩 *　牧田 大佑　吉岡 克成 * 松本 勉 *
2015/1/22	HTML5 セキュリティ強化実行基盤「SEHTML5」を使ったパスワードマネージャ 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（SCIS2015）		金谷 延幸　野田 敏達 *　長谷部 高行 *
2015/3/3	プラガブルかつプログラマブルなログ分析フレームワーク	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）		津田 侑　神薗 雅紀　遠峰 隆史 衛藤 将史　井上 大介
2015/3/4	悪性 USB デバイスに対する検査機能付き USB ハブの提案	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）	Vol.114 No.489 pp.61-68	竹久 達也　岩村 誠　丑丸 逸人 井上 大介
2015/3/15	DNS アンプ攻撃の事前対策へ向けた DNS ハニーポットとダークネットの相関分析	情報処理学会　情報処理学会論文誌	Vol.56 No.3 pp.921-931	牧田 大佑　吉岡 克成 *　松本 勉 * 中里 純二　島村 隼平 *　井上 大介
2015/10/13	インターネット生放送におけるユーザの活動の分析	システム制御情報学会論文誌	Vol.28 No.10 pp.407-418	津田 侑　上原 哲太郎 *　森村 吉貴 * 森 幹彦 *　喜多 一 *
2015/10/23	DRDoS ハニーポットが観測した攻撃の履歴を用いた攻撃対象の傾向分析	情報処理学会　コンピュータセキュリティシンポジウム 2015 (CSS2015)		牧田 大佑　西添 友美 *　吉岡 克成 * 松本 勉 *　井上 大介　中尾 康二
2015/10/23	ハニーポットによる TCP リフレクション攻撃の観測と分析	情報処理学会　コンピュータセキュリティシンポジウム 2015 (CSS2015)		小出 駿 *　牧田 大佑　吉岡 克成 * 松本 勉 *
2015/10/23	携帯型セキュリティアプライアンス上に HTML5 にて実装したパスワードマネージャの提案と実装	情報処理学会　コンピュータセキュリティシンポジウム 2015 (CSS2015)		金谷 延幸　野田 敏達 *　長谷部 高行 *
2015/11/4	AmpPot: Monitoring and Defending Against Amplification DDoS Attacks	The 18th International Symposium on Research in Attacks,, Intrusions and Defenses (RAID'15)	pp.615-636	Lukas Kramer*　Johannes Krupp* 牧田 大佑　Tomomi Nishizoe* Takashi Koide*　Katsunari Yoshioka* Christian Rossow*
2015/11/5	ベイズ意思決定を用いた低速スキャン検知手法	Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS 2015)		嶌田 一郎　津田 侑　衛藤 将史 井上 大介
2015/11/27	プロセスの出現頻度を用いた不審プロセス特定	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）		中里 純二　津田 侑　衛藤 将史 井上 大介　中尾 康二
2016/3/4	プロセスの出現頻度や通信状態に着目した不審プロセス判定	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）		中里 純二　津田 侑　衛藤 将史 井上 大介　中尾 康二
2016/3/4	時系列に基づいたイベント情報管理手法の提案とその基礎調査	電子情報通信学会　インターネットアーキテクチャー研究会（IA）	Vol.115 No.482 pp.227-232	遠峰 隆史　津田 侑　加藤 朗 * 砂原 秀樹 *　井上 大介

■サイバー攻撃対策総合研究センター　サイバー攻撃検証研究室

発表年月日日	論文名	誌名／発表機関	巻号	発表者
2013/10/25	野生動物行動による DTN の技術要件に関する検討	インターネットコンファレンス 2013		安田 真悟　Beuran Razvan　崔 瞬星 * 三輪 信介　篠田 陽一 *
2013/11/30	A Learner-Independent Knowledge Transfer Approach to Multi-task Learning	Cognitive Computation	Vol.2013	Shaoning Pang*　Fan Liu*　門林 雄基 班 涛　井上 大介
2013/12/4	Emulation-based ICT System Resiliency Verification for Disaster Situations	Workshop on Resilient Internet based Systems (REIS 2013)		安田 真悟　明石 邦夫 *　宮地 利幸 Beuran Razvan　牧野 義樹　井上 朋哉 * 三輪 信介　篠田 陽一
2014/5/23	標的型攻撃のシナリオ再現環境の構築	情報処理学会　コンピュータセキュリティ研究発表会		津田 侑　神薗 雅紀　遠峰 隆史 安田 真悟　三浦 良介　宮地 利幸 衛藤 将史　井上 大介　中尾 康二
2014/6/16	Mechanism for Linking and Discovering Structured Cybersecurity Information over Networks	IEEE International Conference on Semantic Computing	pp.279-284	高橋 健志　門林 雄基
2014/7/24	MindYourPrivacy: サードパーティウェブトラッキング可視化システムの設計と実装	Privacy Security Trust 2014	pp.48-56	高野 祐輝　太田 悟史　高橋 健志 安藤 類央　井上 朋哉 *
2014/10/1	DNS オープンリゾルバの実態	電子情報通信学会論文誌　将来ネットワークに向けたインターネットアーキテクチャ 特集	Vol.J97BNo.10 pp.873-889	高野 祐輝　安藤 類央　宇多 仁 * 高橋 健志　井上 朋哉 *
2014/10/1	Reference Ontology for Cybersecurity Operational Information	Computer Journal		高橋 健志　門林 雄基
2014/10/22	標的型攻撃再現のための攻撃シナリオ定義インタフェースの実装	情報処理学会　コンピュータセキュリティシンポジウム 2014 (CSS2014)		津田 侑　神薗 雅紀　遠峰 隆史 安田 真悟　三浦 良介　宮地 利幸 衛藤 将史　井上 大介　中尾 康二
2014/11/4	MarketDrone: Android アプリケーションの動的解析フレームワーク	インターネットコンファレンス 2014	pp.129-130	加藤 邦章 *　高野 祐輝　三浦 良介 太田 悟史　篠田 陽一
2015/1/15	SF-TAP: 柔軟で規模追従可能なトラフィック解析基盤の設計	情報通信マネジメント研究会	Vol.114No.389 pp.7-12	高野 祐輝　三浦 良介　明石 邦夫 * 井上 朋哉
2015/6/24	DynamiQ: A Tool for Dynamic Emulation of Networks	10th International Conference on Testbeds and Research Infrastructures for the Development of Networks & Communities		Beuran Razvan　安田 真悟　井上 朋也 * 高野 祐輝　宮地 利幸　篠田 陽一
2015/6/24	Towards an Interactive Experiment Framework: DynamiQ	10th International Conference on Testbeds and Research Infrastructures for the Development of Networks & Communities		Beuran Razvan　安田 真悟　井上 朋也 * 高野 祐輝　宮地 利幸　篠田 陽一
2015/10/13	ビルディングブロック型模擬環境構築システム	インターネットコンファレンス 2015	No.77 pp.69-78	安田 真悟　三浦 良介　太田 悟史 高野 祐輝　宮地 利幸
2015/11/11	SF-TAP: Scalable and Flexible Traffic Analysis Platform on Commodity Hardware	USENIX LISA 2015	pp.25-36	高野 祐輝　三浦 良介　安田 真悟 明石 邦夫 *　井上 朋哉 *
2016/3/1	Secure and Anonymous Communication Technique: Formal Model and its Prototype Implementation	IEEE Transactions on Emerging Topics in Computing	Vol.4No.1 pp.88-101	江村 恵太　Akira Kanaoka*　太田 悟史 Kazumasa Omote*　高橋 健志