List of Published Presentation Papers of Network Security Research Institute and Cybersecurity Research Center (April 2011 – March 2016)

*outsiders

■ Cybersecurity Laboratory, Network Security Research Institute

Date of Publication	Title of Paper	Publisher / Name of Journal	Vol./No.	Name of Author
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	Jungsuk Song Hiroki Takakura* Yasuo Okabe* Masashi Eto Daisuke Inoue Koji Nakao
2011/4/10	**nicter : A Large-Scale Network Incident Analysis System**	BADGERS 2011	pp.35-43	Masashi Eto Daisuke Inoue Jungsuk Song Junji Nakazato Kazuhiro Ohtaka Koji Nakao
2011/6/1	**Personalized mode transductive spanning SVM classification tree**	Information Sciences	Vol.181 No.11 pp.2071-2085	Shaoning PANG* Tao Ban Youki Kadobayashi Nikola KASABOV*
2011/6/16	**A Practical Usage of Large-scale Darknet Monitoring for Disaster Recovery [in Japanese]**	IEICE technical report. Information and communication system security		Daisuke Inoue Junji Nakazato Jumpei Shimamura* Masashi Eto Koji Nakao
2011/6/17	**A Profiling Method of Attacking Hosts based on Scan Feature Extraction [in Japanese]**	IEICE technical report. Information and communication system security		Masashi Eto Yaichiro Takagi Jungsuk Song Daisuke Inoue Koji Nakao
2011/7/7	**Practical Network Traffic Analysis in P2P Environment**	The 7th International Wireless Communications and Mobile Computing Conference	pp.1801-1807	Tao Ban Shanqing GUO* Zonghua Zhang* Ruo Ando Youki Kadobayashi
2011/7/18	**Correlation Analysis between Spamming Botnets and Malware Infected Hosts**	SAINT 2011 Workshop on Network Technologies for Security,, Administration and Protection (NETSAP)		Jungsuk Song Jumpei Shimamura Masashi Eto Daisuke Inoue Koji Nakao
2011/7/26	**P2P Network Traffic Analysis Using Data Mining Engines**	IEICE technical report. Neurocomputing	Vol.111 No.157 pp.115-118	Tao Ban Shanqing GUO* Masashi Eto Daisuke Inoue Koji Nakao
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	Hyung Chan Kim Tatsunori Oriil* Katsunari Yoshioka* Daisuke Inoue Jungsuk SONG Masashi Eto Junji Shikata* Tsutomu Matsumoto* Koji Nakao
2011/9/15	**On the power of decoy injection which threatens public malware sandbox analysis systems [in Japanese]**	Information Processing Society of Japan	Vol.52 No.9 pp.2761-2774	Takahiro Kasama Tatsunori Orii* Katsunari Yoshioka* Tsutomu Matsumoto*
2011/10/6	**Essential Discriminators for P2P Teletraffic Characterization**	The 6th Joint Workshop on Information Security		Tao Ban Shanqing GUO* Masashi Eto Daisuke Inoue Koji Nakao
2011/10/19	**Automatic Detection and Removal of Malware in CCC DATASet 2011 using Anti-Malware User Support System [in Japanese]**	Computer Security Symposium 2011 (CSS2011)		Nobutaka Kawaguchi* Takayuki Yoda* Hiroki Yamaguchi* Masato Terada* Toshihiko Kasagi* Yuji Hoshizawa* Masashi Eto Daisuke Inoue Koji Nakao
2011/10/21	**Malware detection method based on difference between behaviors in multiple executions [in Japanese]**	Computer Security Symposium 2011 (CSS2011)		Takahiro Kasama Katsunari Yoshioka* Daisuke Inoue Tsutomu Matsumoto*
2011/10/21	**A Framework for Countering Drive-by Download Attacks [in Japanese]**	Computer Security Symposium 2011 (CSS2011)		Takahiro Kasama Daisuke Inoue Masashi Eto Junji Nakazatoa Koji Nakao
2011/10/21	**Proposal of Multipurpose Network Monitoring Platform [in Japanese]**	Computer Security Symposium 2011 (CSS2011)		Masashi Eto Daisuke Inoue Mio Suzuki Koji Nakao
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	Junji Nakazatoa Jungsuk Song Masashi Eto Daisuke Inoue Koji Nakao
2011/11/18	**Entropy based Discriminators for P2P Teletraffic Characterization**	2011 International Conference on Neural Information Processing	Vol.7063 pp.18-27	Tao Ban Shanqing GUO* Masashi Eto Daisuke Inoue Koji Nakao
2011/11/18	**Feature estimation scheme for self modifying malwares using parts of their own codes [in Japanese]**	IEICE Information and Communication System Security (ICSS)		Noriaki Nakamura Ryoichi Isawa* Masakatu Morii* Daisuke Inoue Koji Nakao
2011/11/18	**Feature estimation method for malwares based on a histogram of bytecode [in Japanese]**	IEICE Information and Communication System Security (ICSS)		Ryo Okubo* Ryoichi Isawa* Masakatu Morii* Daisuke Inoue Koji Nakao
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* Tao Ban 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* Tao Ban Youki Kadobayashi Nikola Kasabov*
2012/1/31	**Detecting zero-day remote exploit attack by honeypot traffic analysis [in Japanese]**	Symposium on Cryptography and Information Security (SCIS2012)		Chiaki Jimbo* Takayoshi Fujii* Kosuke Murakami* Katsunari Yoshioka* Junji Shikata* Tsutomu Matsumoto* Masashi Eto Daisuke Inoue Koji Nakao

Date of Publication	Title of Paper	Publisher / Name of Journal	Vol./No.	Name of Author
2012/1/31	**Multimodal analysis based on observations from diverse sensors [in Japanese]**	Symposium on Cryptography and Information Security (SCIS2012)		Takahiro Kasama Junji Nakazatoa Mio Suzuki Masashi Eto Daisuke Inoue Koji Nakao Mitsuaki Akiyama* Kazufumi Aoki* Makoto Iwamura* Takeshi Yagi* Noriaki Saito* Takeo Hario*
2012/2/2	**Behavior Analysis of Bot-net Based on the Cooperation Operation over a Long-term Observation [in Japanese]**	Symposium on Cryptography and Information Security (SCIS2012)		Junji Nakazatoa Tao Ban Masashi Eto Daisuke Inoue Koji Nakao
2012/3/9	**Integrated Security Approach for ID/Locator Split-based Network**	IEICE Information Networks (IN)	Vol.111 No.469 pp.365-370	Ved Prasad Kafle Ruidong LI Daisuke Inoue Hiroaki Harai
2012/3/16	**Evaluation of Anti-Malware User Support System through Field Experiments [in Japanese]**	IEICE Information and Communication System Security (ICSS)		Toshihiko Kasagi* Takayuki Yoda* Hiroki Yamaguchi* Yuji Hoshizawa* Masashi Eto Daisuke Inoue Koji Nakao
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* Tao Ban
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 Mio Suzuki Masashi Eto Daisuke Inoue Junji Nakazatoa
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 Ruidong LI Daisuke Inoue Hiroaki Harai
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	Tao Ban Shanqing Guo* Masashi Eto Daisuke Inoue Koji Nakao
2012/6/22	**Network Observation and Analysis Report on nicter -Transition and Categorization of DDoS Backscatter-**	IEICE Information and Communication System Security (ICSS)	Vol.112 No.90 pp.37-42	Junji Nakazatoa Jumpei Shimamura Masashi Eto Daisuke Inoue Koji Nakao
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	Takahiro Kasama Katsunari Yoshioka* Daisuke Inoue Tsutomu Matsumoto*
2012/8/10	**Multipurpose Network Monitoring Platform using Dynamic Address Assignment**	The 7th Asia Joint Conference on Information Security (AsiaJCIS 2012)		Masashi Eto Daisuke Inoue Mio Suzuki Koji Nakao
2012/9/6	**Code Capture from Self-Modifying Malwares [in Japanese]**	Forum on Information Technology (FIT2012)		Noriaki Nakamura Masakatu Morii* Ryoichi Isawa* Daisuke Inoue Koji Nakao
2012/9/6	**Function Estimation Method for Malwares based on part of Binary Code**	Forum on Information Technology (FIT2012)		Ryo Okubo* Masakatu Morii* Ryoichi Isawa* Daisuke Inoue Koji Nakao
2012/10/15	**Malware Sandbox Analysis with Efficient Observation of Herder's Behavior**	Information Processing Society of Japan	Vol.20 No.4 pp.835-845	Takahiro Kasama Katsunari Yoshioka* Tsutomu Matsumoto* Masaya Yamagata* Masashi Eto Daisuke Inoue Koji Nakao
2012/10/15	**DAEDALUS-VIZ: Novel Real-time 3D Visualization for Darknet Monitoring-based Alert System**	VizSec 2012		Daisuke Inoue Koei Suzuki Mio Suzuki Masashi Eto Koji Nakao
2012/10/30	**Code Capture from Self-Modifying Malwares [in Japanese]**	MWS2012 (anti-Malware engineering WorkShop)	Vol.2012 No.3 pp.15-21	Noriaki Nakamura Masakatu Morii* Ryoichi Isawa* Daisuke Inoue Koji Nakao
2012/10/30	**Function Estimation Method for Malwares based on part of Binary Code**	MWS2012 (anti-Malware engineering WorkShop)	Vol.2012 No.3 pp.9-14	Ryo Okubo* Masakatu Morii* Ryoichi Isawa* Daisuke Inoue Koji Nakao
2012/10/31	**Mutual Authentication Scheme against Hybrid Theft Attacks**	Computer Security Symposium 2012(CSS2012)	Vol.2012 No.3 pp.609-616	Yuto Kunisada* Ryoichi Isawa Masakatu Morii*
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* Tao Ban 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* Youki Kadobayashi Tao Ban Daisuke Inoue
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* Tao Ban Daisuke Inoue
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* Tao Ban
2012/11/22	**Malicious Traffic Detection based on Multimodal Analysis [in Japanese]**	IEICE Information and Communication System Security (ICSS)		Takahiro Kasama Masashi Eto Daisuke Inoue
2012/11/22	**Packer Identification Based on Binary Code of Malware Using Machine Learning [in Japanese]**	IEICE Information and Communication System Security (ICSS)	Vol.112 No.315 pp.19-24	Ryoichi Isawa Tao Ban Daisuke Inoue

Date of Publication	Title of Paper	Publisher / Name of Journal	Vol./No.	Name of Author
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	Tao Ban Shanqing Guo* Masashi Eto Daisuke Inoue Koji Nakao
2012/12/1	**Anonymous Authentication Scheme without Verification Table for Wireless Environments**	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	Vol.E95-A No.12 pp.2488-2492	Ryoichi Isawa Masakatu Morii*
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	Takahiro Kasama Katsunari Yoshioka* Daisuke Inoue Tsutomu Matsumoto*
2013/1/22	**Packer Identification Based on Binary Code of Malware Using Machine Learning [in Japanese]**	Symposium on Cryptography and Information Security (SCIS2013)		Ryoichi Isawa Tao Ban Daisuke Inoue
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 Ruidong LI Daisuke Inoue Hiroaki Harai
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* Tao Ban Daisuke Inoue
2013/6/20	**Three Party Secure Anonymous Authentication Scheme with Hard Learning Problems [in Japanese]**	IEICE Information and Communication System Security (ICSS)	Vol.112 No.499 pp.13-18	Kotaro Kishibe* Ryoichi Isawa Masakatu Morii*
2013/6/21	**Network Observation and Analysis Report on nicter -Close Encounters of Network Incident Sign- [in Japanese]**	IEICE Information and Communication System Security (ICSS)		Junji Nakazatoa Jumpei Shimamura Masashi Eto Daisuke Inoue Koji Nakao
2013/6/21	**NONSTOP: Secure Remote Analysis Platform for Cybersecurity Information [in Japanese]**	IEICE Information and Communication System Security (ICSS)	Vol.113 No.94 pp.85-90	Tatsuya Takehisa Daisuke Inoue Masashi Eto Katsunari Yoshioka* Takahiro Kasama Junji Nakazatoa Koji Nakao
2013/6/21	**Generic Unpacking Method Using Data Execution Prevention [in Japanese]**	IEICE Information and Communication System Security (ICSS)	Vol.112 No.499 pp.73-78	Ryoichi Isawa Masaki Kamizono Daisuke Inoue
2013/7/19	**Network Observation and Analysis Report on nicter -Malware Infection to Embedded Systems- [in Japanese]**	IEICE Information and Communication System Security (ICSS)		Junji Nakazatoa Jumpei Shimamura Masashi Eto Daisuke Inoue Koji Nakao
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* Tao Ban Daisuke Inoue
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	Tao Ban Ryoichi Isawa Shanqing Guo* Daisuke Inoue Koji Nakao
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* Tao Ban
2013/8/5	**Application of String Kernel based Support Vector Machine for Malware Packer Identification**	International Joint Conference on Neural Networks	pp.2410-2417	Tao Ban Ryoichi Isawa Shanqing Guo* Daisuke Inoue Koji Nakao
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* Tao Ban Daisuke Inoue
2013/10/23	**DNS Traffic Analysis by Darknet Monitoring [in Japanese]**	Computer Security Symposium 2013(CSS2013)		Junji Nakazatoa Jumpei Shimamura Masashi Eto Daisuke Inoue Koji Nakao
2013/10/23	**Drive-by-Download Attack Detection based on Characteristics of Exploit Kit [in Japanese]**	MWS2013 (anti-Malware engineering WorkShop)		Takahiro Kasama Masaki Kamizono Daisuke Inoue
2013/10/23	**A Study on Vulnerability Inspection of Internet Subnets by Darknet Traffic Data Analysis [in Japanese]**	Computer Security Symposium 2013(CSS2013)	Vol.2013 No.4 pp.723-728	Hironori Nishikaze* Tao Ban Seiichi Ozawa*
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	Tao Ban Ruibin Zhang Shaoning Pang* Abdolhossein Sarrafzadeh* Daisuke Inoue
2013/11/3	**Generic Unpacking Method Based on Detecting Original Entry Point**	The 6th International Workshop on Data Mining and Cybersecurity	Vol.8226 pp.593-600	Ryoichi Isawa* Masaki Kamizono Daisuke Inoue
2013/11/12	**An OEP Identifying Method based on the Order of Opcodes [in Japanese]**	IEICE Information and Communication System Security (ICSS)	Vol.113 No.288 pp.13-18	Noriaki Nakamura Masakatu Morii* Ryoichi Isawa* Daisuke Inoue Koji Nakao
2013/11/12	**Experimental Evaluation of A Botnet Detection Method based on Non-negative Matrix Factorization [in Japanese]**	IEICE Information and Communication System Security (ICSS)		Yuki Kawamura* Jumpei Shimamura Junji Nakazatoa Katsunari Yoshioka* Masashi Eto Daisuke Inoue Jun-ichi Takeuchi Koji Nakao
2013/11/30	**A Learner-Independent Knowledge Transfer Approach to Multi-task Learning**	Cognitive Computation	Vol.2013	Shaoning Pang* Fan Liu* Youki Kadobayashi Tao Ban Daisuke Inoue
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* Tao Ban Hong Zhao*

Date of Publication	Title of Paper	Publisher / Name of Journal	Vol./No.	Name of Author
2014/1/1	**An Accurate Packer Identification Method using Support Vector Machine**	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	Vol.E97-A No.1 pp.253-263	Ryoichi Isawa Tao Ban Shanqing Guo* Daisuke Inoue Koji Nakao
2014/3/5	**NICTER and Its Spin-off Technologies - Challenge for Security Big Data - [in Japanese]**	The 5th Meeting for Cryptology Frontier Group		Daisuke Inoue
2014/3/6	**Obfuscated Mailicious JavaScript Detection using Machine Learning with Character Frequency [in Japanese]**	IPSJ SIG Technical Report		Masata Nishida* Yuji Hoshizawa* Takahiro Kasama Masashi Eto Daisuke Inoue Koji Nakao
2014/3/7	**Automatic Generation of Exploit Kit Signature Based on Sandbox Analysis [in Japanese]**	IPSJ SIG Technical Report		Kenichi Shibahara* Takahiro Kasama Masaki Kamizono Katsunari Yoshioka* Tsutomu Matsumoto*
2014/3/28	**Spam Analysis based on Mail Relay Route [in Japanese]**	IEICE Information and Communication System Security (ICSS)		Junji Nakazatoa Tao Ban Jumpei Shimamura* Masashi Eto Daisuke Inoue Koji Nakao
2014/3/28	**Implementation and Evaluation of a Proactive Cyber Attack Monitoring Platform [in Japanese]**	IEICE Information and Communication System Security (ICSS)		Masashi Eto Tomohide Tanaka* Koei Suzuki Daisuke Inoue Koji Nakao
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* Tao Ban Daisuke Inoue Abdolhossein Sarrafzadeh*
2014/5/21	**A Study on Internet Subnets Categorization with Darknet Traffic Data Analysis [in Japanese]**	The 58th the Institute of Systems, Control and Infoermation Engineers (SCI'14)		Hironori Nishikaze* Tao Ban Junji Nakazatoa Jumpei Shimamura Seiichi Ozawa*
2014/5/21	**A Study on Judgment of Backscatter by DDoS Attacks for Darknet Packets [in Japanese]**	The 58th the Institute of Systems, Control and Infoermation Engineers (SCI'14)		Nobuaki Furutani* Tao Ban Junji Nakazatoa Jumpei Shimamura Seiichi Ozawa*
2014/6/6	**Development of an Environment-independent Dynamic Analysis System for Document Malware [in Japanese]**	IEICE Information and Communication System Security (ICSS)		Masaki Kamizono Kazuki Iwamoto* Takahiro Kasama Masashi Eto Daisuke Inoue Koji Nakao
2014/6/6	**Malicious Web Site Detection Based on Redirection Control using Client Environment [in Japanese]**	IEICE Information and Communication System Security (ICSS)		Takahiro Kasama Masashi Eto Masaki Kamizono Daisuke Inoue
2014/7/4	**Analysis of Cyber-attack Infrastructure with Malicious Website focused on Backdoor Shell [in Japanese]**	IEICE Information and Communication System Security (ICSS)		Masaki Kamizono Yuji Hoshizawa* Takahiro Kasama Masashi Eto Daisuke Inoue Katsunari Yoshioka* Tsutomu Matsumoto*
2014/8/27	**FCDBD: Framework for Countering Drive-by Download**	The 9th International Workshop on Security (IWSEC2014),, poster session		Takashi Matsunaka* Junpei Urakawa* Akihiro Nakarai* Ayumu Kubota* Kazuo Kawamorita* Yuji Hoshizawa* Takahiro Kasama Masashi Eto Daisuke Inoue Koji Nakao
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)		Takashi Matsunaka* Ayumu Kubota* Takahiro Kasama
2014/9/4	**Detection of DDoS Backscatter Based on TrafficFeatures of Darknet TCP Packets**	The 9th Asia Joint Conference on Information Security (AsiaJCIS 2014)		Nobuaki Furutani* Tao Ban Junji Nakazatoa Jumpei Shimamura Jun Kitazono* Seiichi Ozawa*
2014/10/22	**A Method for Prevention of Attacks Abusing NDP Based on Learning IPv6 Communications [in Japanese]**	Computer Security Symposium 2014 (CSS2014)		Masashi Eto Mio Suzuki Satoshi Kobayashi* Daisuke Inoue Koji Nakao
2014/10/23	**A Slow-Scan Detection Method for Live Network Environments [in Japanese]**	Computer Security Symposium 2014 (CSS2014)	pp.458-465	Ichiro Shimada Yu Tsuda Masashi Eto Daisuke Inoue
2014/10/23	**Communication Analysis of Android Devices in the Darknet [in Japanese]**	Computer Security Symposium 2014 (CSS2014)		Takayuki Suzuki* Nanto Suzuki* Takahiro Kasama Jumpei Shimamura* Daisuke Inoue Noriharu Miyaho*
2014/10/23	**Multimodal Analysis for Understanding Attack Activities of Embedded Devices [in Japanese]**	Computer Security Symposium 2014 (CSS2014)		Takahiro Kasama Jumpei Shimamura* Daisuke Inoue
2014/10/24	**Original Entry Point Detection by Classifying Dynamically Generated Instructions [in Japanese]**	Computer Security Symposium 2014 (CSS2014)	pp.1148-1155	Kotaro Kishibe* Noriaki Nakamura* Masakatu Morii* Ryoichi Isawa Daisuke Inoue Koji Nakao
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* Shunsuke Tada* Tao Ban Junji Nakazatoa Jumpei Shimamura Seiichi Ozawa*
2014/11/28	**Detecting Backscatter of DDoS Attacks from Darknet Traffic [in Japanese]**	IEICE Information and Communication System Security (ICSS)		Nobuaki Furutani* Tao Ban Junji Nakazatoa Jumpei Shimamura* Jun Kitazono* Seiichi Ozawa*
2015/1/30	**PaddyFrog: Systematically Detecting Confused Deputy Vulnerability in Android Applications**	Security and Communication Networks (John Wiley & Sons,, Ltd)		Jianliang Wu* Tingting Cui* Tao Ban Shanqing Guo* Lizhen Cui*
2015/2/28	**Analysis of Android Malware Scan via the Wi-Fi [in Japanese]**	IEICE Student Council of the Tokyo Branch Research Workshop		Nanto Suzuki* Takayuki Suzuki* Takahiro Kasama Jumpei Shimamura* Daisuke Inoue Noriharu Miyaho*
2015/2/28	**Communication analysis that utilizes the Android malware data-set [in Japanese]**	IEICE Student Council of the Tokyo Branch Research Workshop		Takayuki Suzuki* Nanto Suzuki* Takahiro Kasama Jumpei Shimamura* Daisuke Inoue Noriharu Miyaho*

Date of Publication	Title of Paper	Publisher / Name of Journal	Vol./No.	Name of Author
2015/3/4	**Internet Alive Monitoring Method around Disaster Areas Using Large-scale Darknet, Autonomous System Information, and Geographical Information [in Japanese]**	IEICE Information and Communication System Security (ICSS)	Vol.114 No.489 pp.115-120	Mio Suzuki Jumpei Shimamura Junji Nakazatoa Daisuke Inoue Masashi Eto Koji Nakao
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	Masashi Eto Tomohide Tanaka* Koei Suzuki Mio Suzuki Daisuke Inoue Koji Nakao
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* Seiichi Ozawa* Junji Nakazatoa Tao Ban Jumpei Shimamura
2015/5/20	**Detection of DDoS Backscatter Based on Darknet Traffic Features [in Japanese]**	The 59th the Institute of Systems, Control and Infoermation Engineers	Vol.59	Nobuaki Furutani Tao Ban Junji Nakazatoa Jumpei Shimamura Jun Kitazono* Seiichi Ozawa*
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* Nobuaki Furutani* Seiichi Ozawa* Junji Nakazatoa Tao Ban Jumpei Shimamura
2015/6/19	**Cross-Organizational Incident Information Sharing using a Darknet Monitoring System**	Coordinating Attack Response at Internet Scale (CARIS) Workshop		Mio Suzuki Daisuke Inoue Takeshi Takahash
2015/7/2	**Datasets for Anti-Malware Research ～MWS Datasets 2015～**	IPSJ SIG Technical Report		Masaki Kamizono* Mitsuaki Akiyama* Takahiro Kasama Junichi Murakami* Mitsuhiro Hatada* Masato Terada*
2015/7/14	**A Study on Association Rule Mining of Darknet Big Data**	The International Joint Conference on Neural Networks,, 2015	pp.3814-3820	Tao Ban Masashi Eto Shanqing Guo* Daisuke Inoue Koji Nakao 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* Seiichi Ozawa* Junji Nakazatoa Tao Ban Jumpei Shimamura
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* Tao Ban Daisuke Inoue 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	Hironori Nishikaze* Seiichi Ozawa* Jun Kitazono* Tao Ban Junji Nakazatoa Jumpei Shimamura
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* Takahiro Kasama 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	Mitsuhiro Hatada* Mitsuaki Akiyama* Takahiro Matsuki* Takahiro Kasama
2015/10/21	**Studies on Risk Level Evaluation Schemes using APK Metadata [in Japanese]**	Computer Security Symposium 2015 (CSS2015)		Takeshi Takahash Tao Ban Takao Mimura* Koji Nakao
2015/10/22	**Development of Adaptive Event-Monitoring System for DDoS Attacks [in Japanese]**	Computer Security Symposium 2015 (CSS2015)	Vol.2015 No.3 pp.1394-1401	Nobuaki Furutani* Jun Kitazono* Seiichi Ozawa* Tao Ban Junji Nakazatoa Jumpei Shimamura
2015/11/5	**Using Bayesian Decision Making to Detect Slow Scans**	Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS 2015)		Ichiro Shimada Yu Tsuda Masashi Eto Daisuke Inoue
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)		Takeshi Takahash Tao Ban Takao Mimura* Koji Nakao
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	Nobuaki Furutani* Jun Kitazono* Seiichi Ozawa* Tao Ban Junji Nakazatoa Jumpei Shimamura
2015/11/26	**tkiwa: A Detection Tool for Packets with Characteristic Network Protocol Header [in Japanese]**	IEICE Information and Communication System Security (ICSS)		Takashi Koide* Daisuke Makita* Takahiro Kasama Mio Suzuki Daisuke Inoue Koji Nakao Katsunari Yoshioka* Tsutomu Matsumoto*
2015/11/27	**A Suspicious Processes Detection Scheme using Process Frequency [in Japanese]**	IEICE Information and Communication System Security (ICSS)		Junji Nakazatoa Yu Tsuda Masashi Eto Daisuke Inoue Koji Nakao
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	Takeshi Takahash Tao Ban Takao Mimura* Koji Nakao
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* Tao Ban
2016/1/22	**Visualizing darknet traffic data using dimensionality reduction [in Japanese]**	Symposium on Cryptography and Information Security (SCIS2016)		Jun Kitazono* Nobuaki Furutani* Yuki Ukawa* Tao Ban Jumpei Shimamura Junji Nakazatoa Seiichi Ozawa*

Date of Publication	Title of Paper	Publisher / Name of Journal	Vol./No.	Name of Author
2016/2/1	**Understanding Malicious Activities of Embedded Devices Based on Correlating. Observation Results from Passive and Active Monitoring [in Japanese]**	IEICE Transactions on Information and Systems	Vol.J99-A No.2 pp.94-105	Takahiro Kasama Jumpei Shimamura* Daisuke Inoue
2016/2/15	**Detecting Credential Search Focused on File Access Failure [in Japanese]**	IPSJ Journal	Vol.57 No.2 pp.597-610	Rui Tanabe* Takahiro Kasama Katsunari Yoshioka* Tsutomu Matsumoto*
2016/3/3	**Malicious-Spam-Mail Detection System with Autonomous Learning Ability [in Japanese]**	IEICE Information and Communication System Security (ICSS)	Vol.50 pp.19-24	Shogo Osaka* Jun Kitazono* Tao Ban Seiichi Ozawa* Junji Nakazatoa Jumpei Shimamura
2016/3/3	**An Autonomous DDoS Backscatter Detection System from Darknet Traffic [in Japanese]**	IEICE Information and Communication System Security (ICSS)	Vol.67 pp.123-128	Yuki Ukawa* Jun Kitazono* Seiichi Ozawa* Tao Ban Junji Nakazatoa Jumpei Shimamura
2016/3/4	**A Suspicious Processes Detection Scheme using Process Frequency and Network State [in Japanese]**	IEICE Information and Communication System Security (ICSS)		Junji Nakazatoa Yu Tsuda Masashi Eto Daisuke Inoue Koji Nakao

Security Architecture Laboratory, Network Security Research Institute

Date of Publication	Title of Paper	Publisher / Name of Journal	Vol./No.	Name of Author
2011/7/7	Practical Network Traffic Analysis in P2P Environment	The 7th International Wireless Communications and Mobile Computing Conference	pp.1801-1807	Tao Ban Shanqing GUO* Zonghua Zhang* Ruo Ando Youki Kadobayashi
2011/10/19	Faster analysis of malware log using Knuth Bendix completion algorithm [in Japanese]	Computer Security Symposium 2011 (CSS2011)	Vol.2011 No.3 pp.101-106	Ruo Ando Shinsuke Miwa
2011/11/18	A New Distributed Storage System Ensuring Security and Reliability [in Japanese]	IEICE Information and Communication System Security (ICSS)	Vol.111 No.309 pp.19-24	Tadashi Minowa
2011/11/18	Multitenant Cloud Computing : Security Challenges and Approaches [in Japanese]	IEICE Information and Communication System Security (ICSS)		Takeshi Takahash Gregory Blanc* Youki Kadobayashi Doudou Fall* Hiroaki Hazeyama* Shinichiro Matsuo
2011/11/29	Multifactor Authenticated Key Renewal	The Third International Conference on Trusted Systems		Shinichiro Matsuo Daisuke Moriyama Moti Yung*
2011/11/29	Multifactor Authenticated Key Exchange	Lecture Notes in Computer Science (Proceedings of INTRUST 2011)		Shinichiro Matsuo Daisuke Moriyama Moti Yung*
2011/12/13	TOWARD GLOBAL CYBERSECURITY COLLABORATION: CYBERSECURITY OPERATION ACTIVITY MODEL	ITU Kaleidoscope 2011		Takeshi Takahash Youki Kadobayashi Koji Nakao
2012/1/1	Solving a 676-Bit Discrete Logarithm Problem in GF(3^{6n})	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	Vol.E95-A No.1 pp.204-212	Takuya Hayashi* Naoyuki Shinohara Lihua Wan Shinichiro Matsuo Masaaki Shirase* Tsuyoshi Takagi*
2012/1/23	A Lightweight Access Log Filter of Windows OS Using Simple Debug Register Manipulation	Communications in Computer and Information Science	Vol.259 pp.215-227	Ruo Ando Kuniyasu Suzaki*
2012/1/30	Multifactor Authenticated Key Renewal [in Japanese]	Symposium on Cryptography and Information Security (SCIS2012)		Shinichiro Matsuo Daisuke Moriyama Moti Yung*
2012/1/31	Defenses against IP spoofing attacks using DNS [in Japanese]	Symposium on Cryptography and Information Security (SCIS2012)	Vol.2000 No.1pp.1-5	Eimatsu Moriyama
2012/2/1	A secured distributed storage system for bulk data [in Japanese]	Symposium on Cryptography and Information Security (SCIS2012)		Tadashi Minowa
2012/2/2	The Efficiency of Structure Preserving Signature Schemes in Cryptographic Protocols [in Japanese]	Symposium on Cryptography and Information Security (SCIS2012)		Miyako Ohkubo
2012/3/1	Inter-domain Communication Protocol for Real-time File Access Monitor of Virtual Machine	Journal of Wireless Mobile Networks,, Ubiquitous Computing and Dependable Applications	Vol.3 No.42371 pp.120-137	Ruo Ando
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	Jae Hong Seo 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	Jae Hong Seo
2012/4/17	Group to Group Commitments Do Not Shrink	Eurocrypt 2012	Vol.7237 pp.301-317	Masayuki Abe* Kristiyan Haralambiev* Miyako Ohkubo
2012/4/26	Enabling Secure Multitenancy in Cloud Computing:Challenges and Approaches	Baltic Conference on Future Internet Communications		Takeshi Takahash Gregory Blanc* Youki Kadobayashi Doudou Fall* Hiroaki Hazeyama* Shinichiro Matsuo
2012/5/17	Group Signatures with Message-Dependent Opening	The 5th International Conference on Pairing-Based Cryptography,, Pairing 2012		Yusuke Sakai* Keita Emura Goichiro Hanaoka* Yutaka Kawai* Takahiro Matsuda* Kazumasa Omote*
2012/5/18	Workshop on Usable Security (USEC 12) Report	IPSJ Security Psychology & Trust		Akira Kanaoka Takeshi Takahash
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	Jae Hong Seo 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* Keita Emura 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		Takeshi Takahash Shinichiro Matsuo Akira Kanaoka Keita Emura Yuuki Takano
2012/7/19	Architecture Design for Visualizing Risks and Implementing Adequate Security [in Japanese]	IEICE Information and Communication System Security (ICSS)		Shinichiro Matsuo Akira Kanaoka Takeshi Takahash Shinsuke Miwa Tadashi Minowa
2012/7/19	A Study on Cybersecurity Information Discovery Mechanisms over the Internet [in Japanese]	IEICE Information and Communication System Security (ICSS)		Takeshi Takahash Youki Kadobayashi Yuuki Takano
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	Keita Emura 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	Keita Emura Takashi Sato*
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* Jae Hong Seo

Date of Publication	Title of Paper	Publisher / Name of Journal	Vol./No.	Name of Author
2012/8/20	**Short Signatures from Diffie-Hellmand: Realizing Short Public Key**	Cryptology ePrint Archive		Jae Hong Seo
2012/8/30	**Flaw and Configuration Analysis of Cloud Component using First Order Logic**	The 7th Asia Joint Conference on Information Security (AsiaJCIS 2012)		Ruo Ando
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* Keita Emura Nuttapong Attrapadung* Goichiro Hanaoka* Hideki Imai*
2012/9/11	**Relations among Notions of Privacy for RFID Authentication Protocols**	ESORICS 2012	Vol.7459 pp.661-678	Daisuke Moriyama Shinichiro Matsuo Miyako Ohkubo
2012/9/21	**Group to Group Commitments Do Not Shrink**	IEICE Transactions on Technical Committee on Information Security(ISEC)		Miyako Ohkubo
2012/10/17	**Behind HumanBoost: Analysis of Users' Trust Decision Patterns for Identifying Fraudulent Websites**	Journal of Intelligent Learning Systems and Applications		Daisuke Miyamoto* Hiroaki Hazeyama* Youki Kadobayashi Takeshi Takahash
2012/10/23	**An Architecture Of Accountable SecurityIn Light Of Security Service Level Agreement**	Wireless world research forum		Takeshi Takahash Joona Kannisto* Seppo Heikkinen* Bilhanan Silverajan* Marko Helenius* Shinichiro Matsuo
2012/11/14	**Secure Distributed Storage for Bulk Data**	International Conference on Neural Information Processing (ICONIP2012)	Vol.7667 pp.566-575	Tadashi Minowa Takeshi Takahash
2012/11/14	**DNS-based Defense Against IP Spoofing Attacks**	19th International Conference on Neural Information Processing	Vol.V No.LNCS 7667 pp.599-609	Eimatsu Moriyama Takeshi Takahash Daisuke Miyamoto*
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* Youki Kadobayashi Tao Ban Daisuke Inoue
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	Jae Hong Seo
2012/12/6	**Linking Cybersecurity Knowledge: Cybersecurity Information Discovery Mechanism**	ACSAC 2012		Takeshi Takahash Youki Kadobayashi Yuuki Takano
2013/1/22	**Formalizing Privacy in Universal Composability [in Japanese]**	Symposium on Cryptography and Information Security (SCIS2013)		Daisuke Moriyama Moti Yung*
2013/1/23	**Universal Composability for RFID Authentication Protocols and its Relation to the Existing Security Models [in Japanese]**	Symposium on Cryptography and Information Security (SCIS2013)		Daisuke Moriyama
2013/1/23	**A Blackbox Construction of Robust Threshold Encryption from Public-key Encryption with Non-interactive Opening [in Japanese]**	Symposium on Cryptography and Information Security (SCIS2013)		Yusuke Sakai* Keita Emura Jacob Schuldt* Goichiro Hanaoka* Kazuo Ohta*
2013/1/23	**Implementation and Evaluation of PUF-based Pattern Matching Key Generation using Circular Shift [in Japanese]**	Symposium on Cryptography and Information Security (SCIS2013)		Yuki Iwai* Daisuke Moriyama Yuuichi Komano* Tadafumi Fukushima* Shinichiro Matsuo Mitsugu Iwamoto Kazuo Ohta Kazuo Sakiyama
2013/2/28	**Revocable Identity-Based Encryption Revisited: Security Model and Construction**	Public Key Cryptography		Jae Hong Seo* Keita Emura
2013/3/1	**Chosen Ciphertext Secure Keyed-Homomorphic Public-Key Encryption**	PKC2013	pp.32-50	Keita Emura Goichiro Hanaoka* Go Ohtake* Takahiro Matsuda* Shota Yamada*
2013/3/1	**Efficient Delegation of Key Generation and Revocation Functionalities in Identity-Based Encryption**	CT-RSA		Jae Hong Seo* Keita Emura
2013/4/23	**An Accountable Security Mechanism in Light of Security Service Level Agreement**	Wireless World Research Forum (WWRF)		Takeshi Takahash Joona Kannisto* Bilhanan Silverajan* Jarmo Harju* Marko Helenius* Shinichiro Matsuo
2013/5/7	**Cryptanalysis and Improvement of Provably Secure RFID Ownership Transfer Protocol**	LightSec 2013		Daisuke Moriyama
2013/5/7	**Risk Visualization and Alerting System: Architecture and Proof-of-Concept Implementation**	International Workshop on Security in Embedded Systems and Smartphones		Takeshi Takahash Keita Emura Akira Kanaoka Shinichiro Matsuo Tadashi Minowa
2013/5/8	**A Group Signature Scheme with Unbounded Message-Dependent Opening**	ASIACCS2013		Kazuma Ohara* Yusuke Sakai* Keita Emura Goichiro Hanaoka*
2013/5/29	**A Forward Privacy Model for RFID Authentication Protocols**	WISTP 2013	Vol.7886 pp.98-111	Daisuke Moriyama Shinichiro Matsuo Miyako Ohkubo
2013/6/3	**Methods for Restricting Message Space in Public-Key Encryption**	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences		Yusuke Sakai* Keita Emura Goichiro Hanaoka* Yutaka Kawai* Kazumasa Omote*
2013/6/23	**Group Signature Implies Public-key Encryption with Non-interactive Opening**	International Journal of Information Security		Keita Emura 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		Daisuke Miyamoto* Takeshi Takahash

Date of Publication	Title of Paper	Publisher / Name of Journal	Vol./No.	Name of Author
2013/7/8	**An Accountable Security Mechanism based on Security Service Level Agreement**	The Eighteenth IEEE Symposium on Computers and Communications		Takeshi Takahash Joona Kannisto* Seppo Heikkinen* Bilhanan Silverajan* Marko Helenius* Shinichiro Matsuo Jarmo Harju*
2013/7/17	**Private Multiparty Set Intersection Protocol in Rational Model**	TrustCom 2013		Keita Emura Atsuko Miyaji* Mohammad Shahriar Rahman*
2013/7/19	**Cryptanalysis and Improvement of a Provably Secure RFID Ownership Transfer Protocol [in Japanese]**	IEICE Technical Report (ISEC)	Vol.113 No.135 pp.255-261	Daisuke Moriyama
2013/7/22	**Privacy-Preserving Two-Party K-Means Clustering in Malicious Model**	STPSA 2013		Rahena Akhter* Rownak Jahan Chowdhury* Keita Emura 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	Takeshi Takahash Joona Kannisto* Jarmo Harju* Seppo Heikkinen* Bilhanan Silverajan* Marko Helenius* Shinichiro Matsuo
2013/9/4	**An RFID Authentication Protocol with Flexible Path Authentication**	2013 IEEE International Conference on RFID Technologies and Applications		Daisuke Moriyama
2013/10/21	**Accountable Security Mechanism based on Security Service-Level Agreements**	Computer Security Symposium 2013 (CSS2013)		Takeshi Takahash Jarmo Harju*
2013/10/22	**Real-Time Risk Analysis and Automatic Configuration for Mobile Devices**	Computer Security Symposium 2013 (CSS2013)		Shuai Chen* Akira Kanaoka Shinichiro Matsuo Masahiko Kato* Yuji Suga* Eiji Okamoto*
2013/10/24	**A Measurement Study of Open Resolvers and DNS Server Version**	Internet Conference 2013	No.72 pp.23-32	Yuuki Takano Ruo Ando Takeshi Takahash Satoshi Uda* Tomoya Inoue*
2013/10/31	**PUF-Based RFID Authentication Secure and Private under Complete Memory Leakage**	ePrint Archive		Daisuke Moriyama Shinichiro Matsuo 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* Keita Emura
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* Keita Emura
2013/11/19	**Toward Practical Searchable Symmetric Encryption**	The 8th International Workshop on Security (IWSEC 2013)	pp.151-167	Wakaha Ogata* Keita Koiwa* Akira Kanaoka Shinichiro Matsuo
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	Daisuke Moriyama Shinichiro Matsuo Miyako Ohkubo
2014/1/21	**A Risk Evaluation Framework for Android Terminal and its PrototypeImplementation**	The 31st Symposium on Cryptography and Information Security		Takeshi Takahash Yuuki Takano Koji Nakao Satoshi Ohta Akira Kanaoka Shoichi Sakane Shinichiro Matsuo
2014/1/22	**Privacy-preserving Access Log Management from Nominative Signatures**	Symposium on Cryptography and Information Security (SCIS2014)		Sanami Nakagawa* Keita Emura Yusuke Sakai* Goichiro Hanaoka* Akihisa Kodate*
2014/1/22	**A Compact Revocable Group Signature Scheme with Scalability**	Symposium on Cryptography and Information Security (SCIS2014)		Kazuma Ohara* Yusuke Sakai* Keita Emura Goichiro Hanaoka* Kazuo Ohta*
2014/1/22	**A Generic Construction of Robust Threshold Public-key Encryption from Public-key Encryption with Non-interactive Opening**	Symposium on Cryptography and Information Security (SCIS2014)		Yusuke Sakai* Keita Emura Jacob C.N. Schuldt* Goichiro Hanaoka* Kazuo Ohta*
2014/1/23	**PUF-Based RFID Authentication Secure and Private under Complete Memory Leakage**	Symposium on Cryptography and Information Security (SCIS2014)		Daisuke Moriyama Shinichiro Matsuo Moti Yung*
2014/1/23	**Formal Security Model for Physically Unclonable Functions**	Symposium on Cryptography and Information Security (SCIS2014)		Daisuke Moriyama
2014/3/25	**Building Secure and Anonymous Communication Channel: Formal Model and its Prototype Implementation**	ACM SAC2014		Keita Emura Akira Kanaoka Satoshi Ohta Takeshi Takahash
2014/5/13	**Chosen Ciphertext Secure Keyed-Homomorphic Public-Key Encryption**	Cryptology ePrint Archive		Keita Emura Goichiro Hanaoka* Koji Nuida* Go Ohtake* Takahiro Matsuda* Shota Yamada*
2014/5/20	**Revocable Hierarchical Identity-Based Encryption**	Theoretical Computer Science		Jae Hong Seo* Keita Emura
2014/6/3	**Salt-and-Pepper Image Watermarking System for IHC Evaluation Criteria**	The First International Workshop on Information Hiding and its Criteria for evaluation (IWIHC2014)	pp.31-36	Hironobu Tozuka* Maki Yoshida Toru Fujiwara*
2014/6/10	**A Revocable Group Signature Scheme From Identity-Based Revocation Techniques: Achieving Constant-size Revocation List**	ACNS2014		Nuttapong Attrapadung* Keita Emura Goichiro Hanaoka* Yusuke Sakai*

Date of Publication	Title of Paper	Publisher / Name of Journal	Vol./No.	Name of Author
2014/6/16	Mechanism for Linking and Discovering Structured Cybersecurity Information over Networks	IEEE International Conference on Semantic Computing	pp.279-284	Takeshi Takahash Youki Kadobayashi
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	Takeshi Takahash Joona Kannisto* Jarmo Harju* Akira Kanaoka Yuuki Takano Shinichiro Matsuo
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* Keita Emura Roman Jagomägis* Akira Kanaoka Shinichiro Matsuo 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* Keita Emura
2014/7/4	A privacy-preserving RFID Yoking-Proof Protocol provably secure against man-in-the-middle attack [in Japanese]	IEICE Technical Report (ISEC)	No.12 pp.17-24	Daisuke Moriyama
2014/7/9	A Secure and Anonymous Communication Protocol and its PrototypeImplementation [in Japanese]	DICOMO2014		Keita Emura Akira Kanaoka Satoshi Ohta Kazumasa Omote* Takeshi Takahash
2014/7/23	Digital Identities and Accountable Agreements in Web Applications	International Conference on Security and Management		Joona Kannisto* Jarmo Harju* Takeshi Takahash
2014/7/24	MindYourPrivacy: Design and Implementation of a Visualization System for Third-Party Web Tracking	Privacy Security Trust 2014	pp.48-56	Yuuki Takano Satoshi Ohta Takeshi Takahash Ruo Ando Tomoya Inoue*
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* Keita Emura
2014/9/2	A Provably Secure Offline RFID Yoking-Proof Protocol with Anonymity	LightSec2014		Daisuke Moriyama
2014/9/9	Provably Secure Two-Round RFID Grouping-proof Protocols	RFID-TA 2014		Daisuke Moriyama
2014/9/18	Performance Evaluation of Additive Watermarking under the Highest Image Quality Category of the IHC Watermark Competition [in Japanese]	IEICE Technical Report (EMM)	Vol.114 No.222 pp.53-58	Hironobu Tozuka* Maki Yoshida Toru Fujiwara*
2014/10/1	The Ecology of DNS Open Resolvers [in Japanese]	IEICE Transactions on Information and Systems	Vol.J97B No.10 pp.873-889	Yuuki Takano Ruo Ando Satoshi UDA* Takeshi Takahash Tomoya Inoue*
2014/10/1	Reference Ontology for Cybersecurity Operational Information	Computer Journal		Takeshi Takahash Youki Kadobayashi
2014/10/5	A Non-repudiable Negotiation Protocol for Security Service Level Agreements	International Journal of Communication Systems		Joona Kannisto* Takeshi Takahash Jarmo Harju* Seppo Heikkinen* Marko Helenius* Shinichiro Matsuo 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		Takeshi Takahash Koji Nakao Akira Kanaoka
2015/1/1	Individual Restoration of Tampered Pixels for Statistical Fragile Watermarking	IEICE Transactions on Information and systems	Vol.98-D No.1 pp.58-64	Maki Yoshida Kazuya Ohkita* Toru Fujiwara*
2015/2/1	On the Impossibility of d-Multiplicative Non-perfect Secret Sharing	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	Vol.E98-A No.2 pp.767-770	Maki Yoshida Toru Fujiwara*
2015/3/4	A Study on Risk Quantification Techniques for Android Applications with Category Information [in Japanese]	IEICE Information and Communication System Security (ICSS)		Takeshi Takahash Takao Mimura* Masata Nishida* Koji Nakao
2015/6/1	SKENO: Secret Key Encryption with Non-interactive Opening	Journal of Mathematical Cryptology		Jiageng Chen* Keita Emura Atsuko Miyaji*
2015/6/3	Accumulable Optimistic Fair Exchange from Verifiably Encrypted Homomorphic Signatures	ACNS 2015		Jae Hong Seo* Keita Emura Keita Xagawa* Kazuki Yoneyama*
2015/6/29	Dynamic Threshold Public-key Encryption with Decryption Consistency from Static Assumptions	ACISP 2015		Yusuke Sakai* Jacob C.N. Schuldt* Keita Emura Goichiro Hanaoka* Kazuo Ohta*
2015/7/4	A KEM/DEM-based Construction for Secure and Anonymous Communication	Compsac 2015		Keita Emura Akira Kanaoka Satoshi Ohta Takeshi Takahash
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* Daisuke Moriyama Patrick Schaumont* Moti Yung*
2015/9/24	End-to-end Design of a PUF-based Privacy Preserving Authentication Protocol	ePrint Archive		Daisuke Moriyama 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	Daisuke Moriyama Moti Yung*
2015/10/21	Studies on Risk Level Evaluation Schemes using APK Metadata [in Japanese]	Computer Security Symposium 2015 (CSS2015)		Takeshi Takahash Tao Ban Takao Mimura* Koji Nakao
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)		Takeshi Takahash Tao Ban Takao Mimura* Koji Nakao

Date of Publication	Title of Paper	Publisher / Name of Journal	Vol./No.	Name of Author
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	Maki Yoshida　Satoshi Obana*
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	Takeshi Takahash　Tao Ban Takao Mimura*　Koji Nakao
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	Daisuke Moriyama
2016/1/12	**Towards a Unified Security Model for Physically Unclonable Functions**	ePrint Archive		Frederik Armknecht*　Daisuke Moriyama Ahmad-Reza Sadeghi*　Moti Yung*
2016/1/19	**StorXCrypt: An Architecture for Multi App Multi Device Cryptographic Support for Android and its Implementation [in Japanese]**	Symposium on Cryptography and Information Security (SCIS2016)		Daisuke Moriyama　Akira Kanaoka 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	Keita Emura　Akira Kanaoka* Satoshi Ohta　Kazumasa Omote* Takeshi Takahash
2016/3/3	**Towards a Unified Security Model for Physically Unclonable Functions**	CT-RSA 2016		Daisuke Moriyama　Frederik Armknecht* Ahmad-Reza Sadeghi*　Moti Yung*
2016/3/16	**Toward Automated Vulnerability Monitoring using Open Information and Standardized Tools**	PerCom 2016		Takeshi Takahash　Daisuke Miyamoto Koji Nakao
2016/3/16	**Offloading Smartphone Firewalling Using OpenFlow-capable Wireless Access Points**	IEEE International Conference on Pervasive Computing and Communications		Daisuke Miyamoto　Ryo Nakamura* Takeshi Takahash　Yuji Sekiya*

■ Security Fundamentals Laboratory, Network Security Research Institute

Date of Publication	Title of Paper	Publisher / Name of Journal	Vol./No.	Name of Author
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	Atsushi Waseda Masahide Sasaki Masahiro Takeoka Mikio Fujiwara Morio Toyoshima Antonio Assalini*
2011/5/19	Numerical Evaluation of PPM for Deep-Space Links	Journal of Optical Communications and Networking	Vol.3No.6 pp.514-521	Atsushi Waseda Masahide Sasaki Masahiro Takeoka Mikio Fujiwara Morio Toyoshima 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	Kaoru Kurosawa* Ryo Nojima LE PHONG
2011/7/14	Generic Fully Simulatable Adaptive Oblivious Transfer (IACR Eprint)	IACR Cryptology ePrint Archive		Kaoru Kurosawa* Ryo Nojima LE PHONG
2011/8/12	A Unified Framework for Small Secret Exponent Attack on RSA	Selected Areas in Cryptography 2011		Noboru Kunihiro* Naoyuki Shinohara Tetsuya Izu*
2011/8/15	Discrete Logarithm Based Additively Homomorphic Encryption and Secure Data Aggregation	INFORMATION SCIENCES	Vol.181 No.16 pp.3308-3322	Licheng Wang* Lihua Wan 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		Hidema Tanaka
2011/10/19	Biometrics authentication technology and Privacy	Computer Security Symposium 2011 (CSS2011)		Sachiko Kanamori Kanako Kawaguchi* Hidema Tanaka
2011/10/20	On the Truncated Differential Property of Generation Function of Extended Key in Block Ciphers	Computer Security Symposium 2011 (CSS2011)	Vol.2011 No.3 pp.235-240	Bungo Taga Hidema Tanaka Toshinobu Kaneko*
2011/11/20	Maximum Leakage Resilient IBE and IPE	IACR Cryptology ePrint Archive		Kaoru Kurosawa* LE PHONG
2011/11/30	Position Information Authentication Using Electric Waves	SITA2011	pp.234-239	Lihua Wan Hidema Tanaka Ryuichi Ichikawa Tsukasa Iwama Yasuhiro Koyama
2011/12/1	On the Truncated Differential Property of Generation Function of Extended Key in Block Ciphers(2)	SITA2011	pp.304-309	Bungo Taga Hidema Tanaka Toshinobu Kaneko*
2012/1/1	Solving a 676-bit Discrete Logarithm Problem in GF(3^{6n})	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	Vol.E95-A No.1 pp.204-212	Takuya Hayashi* Naoyuki Shinohara Lihua Wan Shinichiro Matsuo Masaaki Shirase* Tsuyoshi Takagi*
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.1 pp.70-88	Lihua Wan Licheng Wang* Masahiro Mambo* Eiji Okamoto*
2012/1/30	Identity-Based Proxy Cryptosystems with Revocability and Hierarchical Confidentialities	Symposium on Cryptography and Information Security (SCIS2012)	pp.1D2-6-	Atsushi Waseda Masakazu Soshi*
2012/1/30	Estimation of time complexity of solving DLP over GF(3^{6n})	Symposium on Cryptography and Information Security (SCIS2012)		Naoyuki Shinohara Takeshi Shimoyama* Takuya Hayashi* Tsuyoshi Takagi*
2012/1/31	Reconstructing RSA private keys from keys bits with erasures and errors	Symposium on Cryptography and Information Security (SCIS2012)		Naoyuki Shinohara Noboru Kunihiro* Tetsuya Izu*
2012/1/31	A study of position information and privacy	Symposium on Cryptography and Information Security (SCIS2012)		Sachiko Kanamori Kanako Kawaguchi* Hidema Tanaka
2012/1/31	On partial key exposure attack on RSA	Symposium on Cryptography and Information Security (SCIS2012)		Tetsuya Izu* Noboru Kunihiro* Naoyuki Shinohara
2012/2/1	A CCA Secure Threshold KEM Scheme	Symposium on Cryptography and Information Security (SCIS2012)		Yuanju Gan* Lihua Wan Ping Pan* Licheng Wang* Yixian Yang*
2012/3/1	Consideration for IT-secure password protected secret sharing [in Japanese]	IEICE Transactions on Technical Committee on Information Security(ISEC)	Vol.IEICE-111 No.IEICE-IT-4 pp.41-43	Atsushi Waseda Ryo Nojima
2012/3/1	On Efficient Construction of One Time Signatures [in Japanese]	IPSJ SIG Technical Report	Vol.2012-DPS-1 No.35 pp.1234-1237	Masakazu Soshi* Atsushi Waseda
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	Naoyuki Shinohara Takeshi Shimoyama* Takuya Hayashi* Tsuyoshi Takagi*
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* Lihua Wan 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	Kaoru Kurosawa* Ryo Nojima LE PHONG
2012/8/8	New Leakage Resilient CCA-Secure Public Key Encryption	IACR Cryptology ePrint Archive		Kaoru Kurosawa* Ryo Nojima LE PHONG
2012/9/21	Security Evaluation of Pairing-Based Cryptosystems using _<ηT>-Pairing over GF(3^n) [in Japanese]	IEICE Transactions on Technical Committee on Information Security(ISEC)	Vol.112 No.211 pp.1-5	Takuya Hayashi* Takeshi Shimoyama* Naoyuki Shinohara Tsuyoshi Takagi*
2012/10/29	Consideration for multi-threshold multi-secret sharing schemes	2012 International Symposium on Information Theory and its Applications	pp.265-269	Atsushi Waseda Masakazu Soshi*

Date of Publication	Title of Paper	Publisher / Name of Journal	Vol./No.	Name of Author
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	Takuya Hayashi* Takeshi Shimoyama* Naoyuki Shinohara Tsuyoshi Takagi*
2013/1/1	Multiparty simultaneous quantum identity authentication secure against fake signal attacks	IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	Vol.E96-A No.1 pp.166-170	Atsushi Waseda
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* Lihua Wan Licheng Wang* Ping Pan* Yixian Yang*
2013/1/23	A Study of Personal Information and Passive Privacy	Symposium on Cryptography and Information Security (SCIS2013)		Sachiko Kanamori Kanako Kawaguchi* Hidema Tanaka*
2013/1/24	Improvement of Faugère et al.'s method to solve ECDLP	Symposium on Cryptography and Information Security (SCIS2013)		Huang Yun Ju* Naoyuki Shinohara 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* Lihua Wan Licheng Wang* Ping Pan* Yixian Yang*
2013/2/15	UC-Secure Multi-Session OT Using Tamper-Proof Hardware Tokens	IACR Eprint		Kaoru Kurosawa* Ryo Nojima 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	Noboru Kunihiro* Naoyuki Shinohara Tetsuya Izu*
2013/6/18	Certificate-Based Proxy Decryption Systems with Revocability in the Standard Model	INFORMATION SCIENCES	Vol.247 pp.188-201	Lihua Wan Jun Shao* Zhenfu Cao* Masahiro Mambo* Akihiro Yamamura* 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	Kaoru Kurosawa* 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)		Yoshinori Aono
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* Lihua Wan Licheng Wang* Ping Pan* Lixiang Li* Yixian Yang*
2013/8/1	Position Authentication Using Homomorphic Encryption [in Japanese]	IEICE Transactions on Information and systems	Vol.J96-D No.8 pp.1913-1924	Hidema Tanaka* Lihua Wan Ryuichi Ichikawa Tsukasa Iwama Yasuhiro Koyama
2013/8/4	New leakage-resilient CCA-secure public key encryption	Journal of Mathematical Cryptology		Kaoru Kurosawa* Ryo Nojima LE PHONG
2013/8/27	Efficient Lattice-Based Signcryption In Standard Model	Hindawi Publishing Corporation、Mathematical Problems in Engineering		Jianhua Yan* Licheng Wang* Lihua Wan Yixian Yang* Wenbin Yao*
2013/9/6	Database construction which prevents data mining to protect privacy [in Japanese]	FIT 2013	Vol.4 pp.91-98	Sachiko Kanamori Kanako Kawaguchi* Hidema Tanaka*
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* Lihua Wan Chengqian Xu*
2013/10/23	After the "Mining Your Ps and Qs" [in Japanese]	Computer Security Symposium 2013 (CSS2013)		Ryo Nojima Takashi Kurokawa Shiho Moriai
2013/11/11	Introduction of the "Memory Retrieval and Graphical Passwords" [in Japanese]	IPSJ SIG Technical Report		Sachiko Kanamori Shiho Moriai
2013/11/18	Kurosawa-Desmedt Key Encapsulation Mechanism,, Revisited	IACR Eprint Achieve		Kaoru Kurosawa* 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* Naoyuki Shinohara Tsuyoshi Takagi*
2013/12/4	Key-PrivateProxy Re-encryption under LWE	Indocrypt 2013		Yoshinori Aono 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	Naoyuki Shinohara 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	Kaoru Kurosawa* Ryo Nojima LE PHONG
2014/1/22	PRINCESS: Proxy Re-encryption with INd-Cca security in Encrypted file Storage System	Symposium on Cryptography and Information Security (SCIS2014)		Lihua Wan Atsushi Waseda Ryo Nojima Shiho Moriai
2014/1/23	CRYPTREC Encryption Technology Evaluation Committee Report	Symposium on Cryptography and Information Security (SCIS2014)		Shiho Moriai
2014/1/23	A Study of Young People's Safe and Secure Smartphone Use Addressing Privacy Concern	Symposium on Cryptography and Information Security (SCIS2014)		Sachiko Kanamori Kanako Kawaguchi* Hidema Tanaka*
2014/1/23	Improvement of Faugère et al.'s method to solve ECDLP	Symposium on Cryptography and Information Security (SCIS2014)		Yun-Ju Huang* Christophe Petit* Naoyuki Shinohara Tsuyoshi Takagi

Date of Publication	Title of Paper	Publisher / Name of Journal	Vol./No.	Name of Author
2014/3/10	**Computer Simulation of Leakage Resilient IBE and IPE [in Japanese]**	IEICE Technical Report (IT2013–69,ISEC2013 –98,WBS2013)		Kazuki Suzurimi* LE PHONG Kaoru Kurosawa*
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		Keita Emura 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* Keita Emura Roman Jagomägis Akira Kanaoka Shinichiro Matsuo Jan Willemson*
2014/7/7	**Differential and Impossible Differential Related-Key Attacks on Hierocrypt-L1**	ACISP 2014 (19th Australasian Conference on Information Security and Privacy)	Vol.8544 pp.17-33	Bungo Taga* Shiho Moriai Kazumaro Aoki*
2014/7/9	**A Secure and Anonymous Communication Protocol and its PrototypeImplementation [in Japanese]**	DICOMO2014		Keita Emura Akira Kanaoka Satoshi Ohta Kazumasa Omote* Takeshi Takahash
2014/9/26	**A Privacy-enhanced Access Log Management Mechanism in SSO Systems from Nominative Signatures**	TrustCom 2014		Sanami Nakagawa* Keita Emura Goichiro Hanaoka* Akihisa Kodate* Takashi Nishide* Eiji Okamoto* Yusuke Sakai*
2014/10/17	**Anonymous Data Collection System with Mediators**	BalkanCryptSec 2014		Hiromi Arai* Keita Emura Takahiro Matsuda*
2014/10/24	**A Report on International Conference ASIACCS2014 [in Japanese]**	Computer Security Symposium 2014 (CSS2014)	No.3E4-3	Hiroaki Anada* Toshihiro Yamauchi* Yoshiaki Hori* Shiho Moriai Kouichi Sakurai*
2014/10/24	**A Privacy Preserving Scheme for Social Networking Services**	Computer Security Symposium 2014 (CSS2014)	Vol.2014 No.2 pp.1177-1184	Sachiko Kanamori Kanako Kawaguchi* Hidema Tanaka*
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	Sachiko Kanamori Kanako Kawaguchi* Hidema Tanaka*
2014/11/11	**Road-to-Vehicle Communications with Time-Dependent Anonymity: A Light Weight Construction and its Experimental Results**	IACR Cryptology ePrint Archive		Keita Emura Takuya Hayashi
2015/1/1	**Highly Secure Network Switches with Quantum Key Distribution Systems**	International Journal of Network Security	Vol.17 No.1 pp.34-39	Mikio Fujiwara Tomoyasu Domeki* Shiho Moriai Masahide Sasaki
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	Kaoru Kurosawa* Ryo Nojima LE PHONG
2015/1/20	**Accumulable Optimistic Fair Exchange**	Symposium on Cryptography and Information Security (SCIS2015)		Jae Hong Seo* Keita Emura Keita Xagawa* Kazuki Yoneyama*
2015/1/21	**Group Signature with Deniability**	Symposium on Cryptography and Information Security (SCIS2015)		Ai Ishida* Keita Emura Goichiro Hanaoka* Yusuke Sakai* Keisuke Tanaka*
2015/1/22	**Keyed-Homomorphic Identity-based Encryption**	Symposium on Cryptography and Information Security (SCIS2015)		Keita Emura Goichiro Hanaoka* Takahiro Matsuda* Koji Nuida* Shota Yamada*
2015/1/22	**A New Progressive BKZ Algorithm**	Symposium on Cryptography and Information Security (SCIS2015)		Yuntao Wang* Yoshinori Aono Takuya Hayashi Tsuyoshi Takagi*
2015/1/23	**Linear regression of confidential data with security update in the encrypted form**	Symposium on Cryptography and Information Security (SCIS2015)		Yoshinori Aono Takuya Hayashi LE PHONG Lihua Wan
2015/1/23	**PRINCESS-based Secure Automobile Information Sharing System**	Symposium on Cryptography and Information Security (SCIS2015)		Lihua Wan Ryo Nojima Shiho Moriai
2015/1/23	**A new progressive BKZ algorithm**	Symposium on Cryptography and Information Security (SCIS2015)		Yuntao Wang* Yoshinori Aono Takuya Hayashi Tsuyoshi Takagi*
2015/1/28	**Non-interactive Zero-Knowledge Proof Systems for Disavowal and Its Applications**	LA Symposium 2014		Ai Ishida* Keita Emura Goichiro Hanaoka Yusuke Sakai Keisuke Tanaka
2015/3/6	**Study on a Scheme of Personal Data Utilization from the Viewpoint of Privacy**	IEICE Transactions on Social Implications of Technology and Information Ethics (SITE)	Vol.SITE2014 No.76 pp.183-188	Sachiko Kanamori Kanako Kawaguchi
2015/3/25	**Improvement of FPPR method to solve ECDLP**	Pacific Journal of Mathematics for Industry	Vol.7 No.1 pp.1-9	Yun-Ju Huang* Christophe Petit* Naoyuki Shinohara Tsuyoshi Takagi*
2015/4/14	**A Secure Automobile Information Sharing System**	ASIACCS2015 1st IoT Privacy,, Trust and Security Workshop		Lihua Wan Ryo Nojima Shiho Moriai
2015/4/14	**Disavowable Public Key Encryption with Non-interactive Opening**	ASIACCS2015		Ai Ishida* Keita Emura 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* Keita Emura

Date of Publication	Title of Paper	Publisher / Name of Journal	Vol./No.	Name of Author
2015/4/29	Generic Constructions of Secure-Channel Free Searchable Encryption with Adaptive Security	Security and Communication Networks	pp.1547-1560	Keita Emura Atsuko Miyaji* Mohammad Shahriar Rahman* Kazumasa Omote*
2015/7/10	Fast and Secure Linear Regression and Biometric Authentication with Security Update	IACR Eprint		Yoshinori Aono Takuya Hayashi LE TRIEU PHONG Lihua Wan
2015/7/15	Disavowability on Public Key Encryption with Non-interactive Opening	LA Symposium 2015		Ai Ishida* Keita Emura Goichiro Hanaoka* Yusuke Sakai* Keisuke Tanaka*
2015/7/20	Japan CRYPTREC Activity on Lightweight Cryptography	NIST Lightweight Cryptography Workshop 2015		Shiho Moriai
2015/8/20	Keyword Revocable Searchable Encryption with Trapdoor Exposure Resistance and Re-generateability	Trustcom 2015		Keita Emura LE PHONG Yohei Watanabe*
2015/8/26	Adaptive-ID Secure Revocable Hierarchical Identity-Based Encryption	IWSEC 2015		Jae Hong Seo* Keita Emura
2015/9/10	A Light-weight Group Signature Scheme with Time-token Dependent Linking	LightSec 2015		Keita Emura Takuya Hayashi
2015/10/1	Revocable Group Signature with Constant-Size Revocation List	The Computer Journal	Vol.58 pp.2698-2715	Nuttapong Attrapadung* Keita Emura Goichiro Hanaoka* Yusuke Sakai*
2015/10/6	Can We Securely Use CBC Mode in TLS1.0?	AsiaARES 2015	Vol.9357 pp.151-160	Takashi Kurokawa Ryo Nojima Shiho Moriai
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	Lihua Wan Takuya Hayashi Sachiko Kanamori Atsushi Waseda Ryo Nojima Shiho Moriai
2015/10/23	On the Experiment of Privacy Leakage in a Vehicle to Vehicle Communication [in Japanese]	Computer Security Symposium 2015 (CSS2015)	Vol.2015 No.3 pp.1273-1280	Atsushi Waseda Ryo Nojima
2015/10/27	Hardness Estimation of LWE via Band Pruning	Cryptology ePrint Archive		Yoshinori Aono LE TRIEU PHONG Lihua Wan
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* Keita Emura 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	Keita Emura Jae Hong Seo* Taek-Young Youn*
2016/1/19	Selfless Anonymity on Group Signature	Symposium on Cryptography and Information Security (SCIS2016)		Ai Ishida* Keita Emura Goichiro Hanaoka* Yusuke Sakai* Keisuke Tanaka* Shota Yamada*
2016/1/19	A Study of Willingness for Private Information Providing	Symposium on Cryptography and Information Security (SCIS2016)	No.1C2-2	Sachiko Kanamori Ryo Nojima Hirotsune Sato* Naoya Tabata*
2016/1/20	A Study on the Security Evaluation Methods of Proxy Re-Encryption Applied to Cloud Environments	Symposium on Cryptography and Information Security (SCIS2016)		Lihua Wan Licheng Wang Masahiro Mambo*
2016/2/9	Scalable and Secure Logistic Regression via Homomorphic Encryption	IACR Cryptology ePrint Archive		Yoshinori Aono Takuya Hayashi LE TRIEU PHONG Lihua Wan
2016/2/15	Revocable hierarchical identity-based encryption via history-free approach	Theoretical Computer Science	Vol.615 pp.45-60	Jae Hong Seo* Keita Emura
2016/2/19	Improved Progressive BKZ Algorithms and their Precise Cost Estimation by Sharp Simulator	IACR Cryptology ePrint Archive		Yoshinori Aono Yuntao Wang* Takuya Hayashi Tsuyoshi Takagi*
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	Takashi Kurokawa Ryo Nojima Shiho Moriai
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	Keita Emura Akira Kanaoka* Satoshi Ohta Kazumasa Omote* Takeshi Takahash
2016/3/9	Scalable and Secure Logistic Regression via Homomorphic Encryption	ACM CODASPY 2016		Yoshinori Aono Takuya Hayashi LE TRIEU PHONG Lihua Wan
2016/3/9	Secure Logistic Regression via Homomorphic Encryption	The sixth ACM Conference on Data and Applications Security and Privacy	pp.142-144	Yoshinori Aono Takuya Hayashi LE TRIEU PHONG Lihua Wan
2016/3/17	State of the Art in Lightweight Cryptography : Towards the Era of Internet of Things [in Japanese]	Proceedings of the IEICE Engineering Sciences Society/NOLTA Society Conference		Shiho Moriai
2016/3/24	Proxy Re-Encryption Schemes with Key Privacy from LWE	IACR Eprint		LE TRIEU PHONG Lihua Wan Yoshinori Aono Manh Ha Nguyen* Xavier Boyen*

■ Cyber Tactics Laboratory, Cybersecurity Research Center

Date of Publication	Title of Paper	Publisher / Name of Journal	Vol./No.	Name of Author
2013/5/9	A Safe Sandbox Analysis Method for Malware that AttemptMan-in-the-Browser Attacks [in Japanese]	IPSJ SIG Technical Report		Tatsuya Segawa* Masaki Kamizono Yuji Hoshizawa* Katsunari Yoshioka* Tsutomu Matsumoto*
2013/6/21	NONSTOP: Secure Remote Analysis Platform for Cybersecurity Information [in Japanese]	IEICE Information and Communication System Security (ICSS)	Vol.113 No.94 pp.85-90	Tatsuya Takehisa Daisuke Inoue Masashi Eto Katsunari Yoshioka* Takahiro Kasama Junji Nakazatoa Koji Nakao
2013/6/21	Generic Unpacking Method Using Data Execution Prevention [in Japanese]	IEICE Information and Communication System Security (ICSS)	Vol.112 No.499 pp.73-78	Ryoichi Isawa* Masaki Kamizono Daisuke Inoue
2013/10/9	A Feasibility Study of an Internet Live Broadcasting System with Contents Protection [in Japanese]	IPSJ Journal	Vol.55 No.1 pp.300-310	Yu Tsuda Liangjin Huang* Yoshitaka Morimura* Shuhui Hou* Tetsutaro Uehara* Hiroshi Ueda*
2013/10/21	Sanitizing sensitive contents from document malware for accelerating sample sharing [in Japanese]	IPSJ Journal		Shingo Saito* Katsunari Yoshioka* Masaki Kamizono Yuji Hoshizawa* Tsutomu Matsumoto*
2013/10/21	Datasets for Anti-Malware Research ~ MWS 2013 Datasets ~ [in Japanese]	IPSJ Journal		Masaki Kamizono Mitsuhiro Hatada* Masato Terada* Mitsuaki Akiyama* Takahiro Kasama Jyunichi Murakami*
2013/10/23	Realtime Detection Method to Malicious Traffic in Livenet [in Japanese]	Computer Security Symposium 2013 (CSS2013)	pp.737-744	Ichiro Shimada Yu Tsuda Masaki Kamizono Daisuke Inoue Koji Nakao
2013/10/23	A Method for Detecting Fake Profiles Using the Characteristics of Online Social Networks [in Japanese]	Computer Security Symposium 2013 (CSS2013)	pp.1010-1017	Yu Tsuda Takashi Tomine Daisuke Inoue
2013/10/23	Drive-by-Download Attack Detection based on Characteristics of Exploit Kit [in Japanese]	MWS2013 (anti-Malware engineering WorkShop)		Takahiro Kasama Masaki Kamizono Daisuke Inoue
2013/11/3	Generic Unpacking Method Based on Detecting Original Entry Point	The 6th International Workshop on Data Mining and Cybersecurity	Vol.8226 pp.593-600	Ryoichi Isawa* Masaki Kamizono Daisuke Inoue
2014/3/7	Automatic Generation of Exploit Kit Signature Based on Sandbox Analysis [in Japanese]	IPSJ SIG Technical Report		Kenichi Shibahara* Takahiro Kasama Masaki Kamizono Katsunari Yoshioka* Tsutomu Matsumoto*
2014/3/27	A System for Sharing and Alerting to Fake Profiles among Online Social Networks Users [in Japanese]	IPSJ SIG Technical Report		Yu Tsuda Takashi Tomine Daisuke Inoue
2014/3/28	Timeline-Based Event Log Viewer over Multi-Host Environment [in Japanese]	IEICE Information and Communication System Security (ICSS)	Vol.113 No.502 pp.125-130	Takashi Tomine Yu Tsuda Masaki Kamizono Kazunori Sugiura* Daisuke Inoue Koji Nakao
2014/5/22	Proposal for Shellcode Extraction from Malicious Document File [in Japanese]	IPSJ SIG Technical Report		Kazuki Iwamoto* Masaki Kamizono Yu Tsuda Takashi Tomine Daisuke Inoue Koji Nakao
2014/5/23	Observing Distributed Reflection Denial-of-Service Attacks by Several Kinds of Honeypots [in Japanese]	IPSJ SIG Technical Report	Vol.65 No.16	Takuya Tsutsumi* Yoshiaki Nonogaki* Rui Tanabe* Daisuke Makita* Katsunari Yoshioka* Tsutomu Matsumoto*
2014/5/23	Implementation of an Environment for Reproducing Targeted Attacks [in Japanese]	IPSJ SIG Technical Report		Yu Tsuda Masaki Kamizono Takashi Tomine Shingo Yasuda Ryosuke Miura Toshiyuki Miyachi Masashi Eto Daisuke Inoue Koji Nakao
2014/6/6	Development of an Environment-independent Dynamic Analysis System for Document Malware [in Japanese]	IEICE Information and Communication System Security (ICSS)		Masaki Kamizono Kazuki Iwamoto* Takahiro Kasama Masashi Eto Daisuke Inoue Koji Nakao
2014/6/6	Malicious Web Site Detection Based on Redirection Control using Client Environment [in Japanese]	IEICE Information and Communication System Security (ICSS)		Takahiro Kasama Masashi Eto Masaki Kamizono Daisuke Inoue
2014/6/17	Observing DNS Amplification Attacks with DNS Honeypot [in Japanese]	IPSJ Journal	Vol.55 No.9 pp.2021-2033	Daisuke Makita* Katsunari Yoshioka* Tsutomu Matsumoto*
2014/7/4	Analysis of Cyber-attack Infrastructure with Malicious Website focused on Backdoor Shell [in Japanese]	IEICE Information and Communication System Security (ICSS)		Masaki Kamizono Yuji Hoshizawa* Takahiro Kasama Masashi Eto Daisuke Inoue Katsunari Yoshioka* Tsutomu Matsumoto*
2014/10/22	Analysis on Local Characteristics of Cyber Attacks from International Darknet Monitoring [in Japanese]	Computer Security Symposium 2014 (CSS2014)		Shogo Suzuki* Shun Koide* Daisuke Makita* Kosuke Murakami* Takahiro Kasama Jumpei Shimamura* Masashi Eto Katsunari Yoshioka* Tsutomu Matsumoto* Daisuke Inoue
2014/10/22	Implementation of an Interface to Define Attacking Scenarios for Reproducing Targeted Attacks [in Japanese]	Computer Security Symposium 2014 (CSS2014)		Yu Tsuda Masaki Kamizono Takashi Tomine Shingo Yasuda Ryosuke Miura Toshiyuki Miyachi Masashi Eto Daisuke Inoue Koji Nakao

Date of Publication	Title of Paper	Publisher / Name of Journal	Vol./No.	Name of Author
2014/10/22	**A Proposal of Method for Detecting Synchronized Increase of Attacks on Multiple Darknet Sensors [in Japanese]**	Computer Security Symposium 2014 (CSS2014)		Kosuke Murakami* Takemasa Kamatani* Wataru Chiga* Shogo Suzuki* Shun Koide* Jumpei Shimamura* Daisuke Makita* Takahiro Kasama Masashi Eto Katsunari Yoshioka* Daisuke Inoue Koji Nakao
2014/10/22	**Detection and Classification Method for Malicious Packets with Characteristic Network Protocol Header [in Japanese]**	Computer Security Symposium 2014 (CSS2014)		Shun Koide* Shogo Suzuki* Daisuke Makita* Kosuke Murakami Takahiro Kasama Jumpei Shimamura Masashi Eto Daisuke Inoue Katsunari Yoshioka* Tsutomu Matsumoto*
2014/10/23	**A Slow-Scan Detection Method for Live Network Environments [in Japanese]**	Computer Security Symposium 2014 (CSS2014)	pp.458-465	Ichiro Shimada Yu Tsuda Masashi Eto Daisuke Inoue
2014/10/23	**Observing DNS Water Torture by DNS Honeypot [in Japanese]**	Computer Security Symposium 2014 (CSS2014)		Daisuke Makita* Katsunari Yoshioka* Tsutomu Matsumoto* Jumpei Shimamura* Daisuke Inoue Koji Nakao
2014/10/23	**A Countermeasure for Targeted Attacks Using Host Based IDS [in Japanese]**	Computer Security Symposium 2014 (CSS2014)		Junji Nakazatoa Yu Tsuda Yaichiro Takagi Masashi Eto Daisuke Inoue Koji Nakao
2014/10/24	**A Proposal of Malware Sandbox Analysis Method for Safe Observation of Linux Malware [in Japanese]**	Computer Security Symposium 2014 (CSS2014)		Rui Tanabe* Takuya Tsutsumi* Shun Koide* Daisuke Makita* Katsunari Yoshioka* Tsutomu Matsumoto*
2015/1/21	**Development of Integrated DRDoS Attack Observation System [in Japanese]**	Symposium on Cryptography and Information Security (SCIS2015)		Daisuke Makita* Tomomi Nishizoe* Shun Koide* Takuya Tsutsumi* Fumihiro Kanai* Hiroshi Mori* Katsunari Yoshioka* Tsutomu Matsumoto* Daisuke Inoue Koji Nakao
2015/1/21	**Observing DRDoS Attacks with Protocol-noncompliant Honeypot [in Japanese]**	Symposium on Cryptography and Information Security (SCIS2015)		Tomomi Nishizoe* Daisuke Makita* Katsunari Yoshioka* Tsutomu Matsumoto*
2015/1/21	**An Early Scale Estimation of DRDoS Attack Monitoring Honeypot Traffic [in Japanese]**	Symposium on Cryptography and Information Security (SCIS2015)		Jumpei Urakawa* Yukiko Sawaya* Akira Yamada* Daisuke Makita* Katsunari Yoshioka* Tsutomu Matsumoto*
2015/3/3	**A Pluggable and Programmable Platform for Analyzing Security Logs [in Japanese]**	IEICE Information and Communication System Security (ICSS)		Yu Tsuda Masaki Kamizono Takashi Tomine Masashi Eto Daisuke Inoue
2015/3/4	**Novel USE Hub against the Malicious USE Devices [in Japanese]**	IEICE Information and Communication System Security (ICSS)	Vol.114 No.489 pp.61-68	Tatsuya Takehisa Makoto Iwamura Hayato Ushimaru Daisuke Inoue
2015/3/15	**Correlation Analysis between DNS Honeypot and Darknet toward Proactive Countermeasures against DNS Amplification Attacks [in Japanese]**	IPSJ Journal	Vol.56 No.3 pp.921-931	Daisuke Makita* Katsunari Yoshioka* Tsutomu Matsumoto* Junji Nakazatoa Jumpei Shimamura* Daisuke Inoue
2015/10/13	**Analyzing Users Behaviors on the Internet Live-Broadcasting Services [in Japanese]**	ISCIE Journal	Vol.28 No.10 pp.407-418	Yu Tsuda Tetsutaro Uehara* Yoshitaka Morimura* Mikihiko Mori* Hajime Kita*
2015/10/23	**An Analysis of Attack Targets Observed by DRDoS Honeypots [in Japanese]**	Computer Security Symposium 2015 (CSS2015)		Daisuke Makita* Tomomi Nishizoe* Katsunari Yoshioka* Tsutomu Matsumoto* Daisuke Inoue Koji Nakao
2015/10/23	**Observation and Analysis of TCP-based Reflection Attacks Using Honeypot [in Japanese]**	Computer Security Symposium 2015 (CSS2015)		Shun Koide* Daisuke Makita* Katsunari Yoshioka* Tsutomu Matsumoto*
2015/10/23	**Proposal and Implementation of Password Manager in HTML5 on a Portable Security Appliance [in Japanese]**	Computer Security Symposium 2015 (CSS2015)		Nobuyuki Kanaya Bintatsu Noda* Takayuki Hasebe*
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* Daisuke Makita* Tomomi Nishizoe* Takashi Koide* Katsunari Yoshioka* Christian Rossow*
2015/11/5	**Using Bayesian Decision Making to Detect Slow Scans**	Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS 2015)		Ichiro Shimada Yu Tsuda Masashi Eto Daisuke Inoue
2015/11/27	**A Suspicious Processes Detection Scheme using Process Frequency [in Japanese]**	IEICE Information and Communication System Security (ICSS)		Junji Nakazatoa Yu Tsuda Masashi Eto Daisuke Inoue Koji Nakao
2016/3/4	**A Suspicious Processes Detection Scheme using Process Frequency and Network State [in Japanese]**	IEICE Information and Communication System Security (ICSS)		Junji Nakazatoa Yu Tsuda Masashi Eto Daisuke Inoue Koji Nakao

Date of Publication	Title of Paper	Publisher / Name of Journal	Vol./No.	Name of Author
2016/3/4	**A Proposal of Timeline-Based Event Log Management Method [in Japanese]**	IEICE Technical Report	Vol.115 No.482 pp.227-232	Takashi Tomine Yu Tsuda Akira Kato* Hideki Sunahara* Daisuke Inoue

Cyber Range Laboratory, Cybersecurity Research Center

Date of Publication	Title of Paper	Publisher / Name of Journal	Vol./No.	Name of Author
2013/10/25	**Study of Technology Requirements for Wild Animal Oriented DTN [in Japanese]**	Internet Conference 2013		Shingo Yasuda Beuran Razvan Sunseong Choe* Shinsuke Miwa Yoichi Shinoda*
2013/11/30	**A Learner-Independent Knowledge Transfer Approach to Multi-task Learning**	Cognitive Computation	Vol.2013	Shaoning Pang* Fan Liu* Youki Kadobayashi Tao Ban Daisuke Inoue
2013/12/4	**Emulation-based ICT System Resiliency Verification for Disaster Situations**	Workshop on Resilient Internet based Systems (REIS 2013)		Shingo Yasuda Kunio Akashi* Toshiyuki Miyachi Beuran Razvan Yoshiki Makino Tomoya Inoue* Shinsuke Miwa Yoichi Shinoda
2014/5/23	**Implementation of an Environment for Reproducing Targeted Attacks [in Japanese]**	IPSJ SIG Technical Report		Yu Tsuda Masaki Kamizono Takashi Tomine Shingo Yasuda Miura Ryosuke Toshiyuki Miyachi Masashi Eto Daisuke Inoue Koji Nakao
2014/6/16	**Mechanism for Linking and Discovering Structured Cybersecurity Information over Networks**	IEEE International Conference on Semantic Computing	pp.279-284	Takeshi Takahash Youki Kadobayashi
2014/7/24	**MindYourPrivacy: Design and Implementation of a Visualization System for Third-Party Web Tracking**	Privacy Security Trust 2014	pp.48-56	Yuuki Takano Satoshi Ohta Takeshi Takahash Ruo Ando Tomoya Inoue*
2014/10/1	**Reference Ontology for Cybersecurity Operational Information**	Computer Journal		Takeshi Takahash Youki Kadobayashi
2014/10/22	**Implementation of an Interface to Define Attacking Scenarios for Reproducing Targeted Attacks [in Japanese]**	Computer Security Symposium 2014 (CSS2014)		Yu Tsuda Masaki Kamizono Takashi Tomine Shingo Yasuda Miura Ryosuke Toshiyuki Miyachi Masashi Eto Daisuke Inoue Koji Nakao
2015/1/15	**SF-TAP : Design of Scalable and Flexible Traffic Analysis Platform [in Japanese]**	IEICE Technical Committee on Information and Communication Management (ICM)	Vol.114 No.389 pp.7-12	Yuuki Takano Miura Ryosuke Kunio Akashi* Tomoya Inoue
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 Shingo Yasuda Tomoya Inoue* Yuuki Takano Toshiyuki Miyachi Yoichi Shinoda
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 Shingo Yasuda Tomoya Inoue* Yuuki Takano Toshiyuki Miyachi Yoichi Shinoda
2015/11/11	**SF-TAP: Scalable and Flexible Traffic Analysis Platform on Commodity Hardware**	USENIX LISA 2015	pp.25-36	Yuuki Takano Miura Ryosuke Shingo Yasuda Kunio Akashi* Tomoya Inoue*
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	Keita Emura Akira Kanaoka* Satoshi Ohta Kazumasa Omote* Takeshi Takahash