セキュリティ研究開発の Bibliography

2012 年 11 月

NTT セキュアプラットフォーム研究所

セキュリティ研究開発の Bibliography

2012.11.19

NTT セキュアプラットフォーム研究所

もくじ

第1部　ネットワーク・モニタリング

(1)性能解析基礎

[1] L.L. Peterson and B.S. Davie, "Computer Networks - A System Approach, 3rd ed., [hands-on] Computer Networks - A System Approach, 3rd ed., Network Simulation Experiments manual", Morgan Kaufmann Publishers, 2003.

[2] Raj Jain,"The Art of Computer Systems Performance Analysis - Techniques for experimental design, measurement, simulation, and modeling", John Wiley & Sons, Inc., 1991.

(2)設計・運用

[3] Jeff Smith, Jake Woodhams, and Robert Marg, "Controller-Based Wireless LAN Fundamentals - An end-to-end reference guide to design, deploy, manage, and secure 802.11 wireless networks", Cisco Press, 2011.

[4] Kevin Corbin, Ron Fuller and David Jansen, "NX-OS and Cisco Nexus Switching - The complete guide to planning, configuring, managing, and troubleshooting NX-OS in enterprise environment", Cisco Press, 2010.

[5] Amir Ranjbar, "Troubleshooting and maintaining Cisco IP Networks (TSHOOT) - Foundation Learning Guide", Cisco Press, 2010.

[6] Ray Blair, Arvind Durai, and John Lautmann, "Tcl Scriptng for Cisco IOS - A guide to building and modifying Tcl scripts to automate network administration tasks", Cisco Press, 2010.

[7] Jim Geier, "Designing and Deploying 802.11n Wireless Networks - gain a practical understanding of the underlying concepts of the 802.11n standard and the methodologies for completing a successful wireless network installation", Cisco Press, 2010.

[8] Diane Teare (Editor),"CCDA Self-Study: Designing for Cisco Internetwork Solutions (DESGN)", Cisco Press, 2004.

(3)ログ分析

[9] Jerry Shenk, "Sorting Through the Noise", SANS Eighth Annual 2012 Log and Event Management Survey Results, 2012.

http://www.sans.org/reading_room/analysts_program/SortingThruNoise.pdf

[10] 内閣官房情報セキュリティセンター, "平成23年度　政府機関における情報システムのログ取得・管理の在り方の検討に係る調査報告書", 2012.

http://www.nisc.go.jp/inquiry/pdf/log_shutoku.pdf

[11] Clayton Dukes, "Building Scalable Syslog Management Solutions", Cisco Public Information White Paper, 2011.
http://www.cisco.com/en/US/technologies/collateral/tk869/tk769/white_paper_c11-557812.pdf

[12] 金居良治, "マルウェア解析の最前線と企業がとるべき対策～脆弱性攻撃とマルウェア脅威～",沖縄 ICT フォーラム 2011 サイバーセキュリティと通信の秘密, 2011.
http://www.jaipa.or.jp/event/oki_ict2011/111215_fourteenforty.pdf

[13] データベース・セキュリティ・コンソーシアム 統合ログ WG, "統合ログ管理サービスガイドライン", 2010.
http://www.db-security.org/report/dbsc_complog_ver1.0.pdf

[14] 山西健司, "データマイニングによる異常検知", 共立出版, 2009.

[15] 竹下恵, "パケットキャプチャ実践技術", リックテレコム, 2009.

[16] 加藤淳也, "ファイアウォールログを利用したマルウェア活動の検出手法について", マルウェア対策研究人材育成ワークショップ 2009(NWS2009), A4-2, 2009.
http://www.iwsec.org/mws/2009/paper/A4-2.pdf

[17] Varun Chandola, Arindam Banerjee, and Vipin Kumar, "Anomaly Detection：A Survey", ACM Computing Surveys, Vol. 41, No.3, Article 15, 2009.

(4)コンプライアンス

[18] National Security Agency Router Security Guidance Activity of the System and Network Attack Center (SNAC), "Router Security Configuration Guide Supplement - Security for IPv6 Routers", Report Number: I33-002R-06, 2006.
http://www.nsa.gov/ia/_files/routers/I33-002R-06.pdf

[19] National Security Agency Router Security Guidance Activity of the System and Network Attack Center (SNAC), "Router Security Configuration Guide", Report Number: C4-040R-02, 2005.
http://www.nsa.gov/ia/_files/routers/C4-040R-02.pdf

[20] National Security Agency Router Security Guidance Activity of the System and Network Attack Center (SNAC), "Cisco IOS Switch Security Configuration Guide", Report Number: I33-010R-2004.
http://www.nsa.gov/ia/_files/switches/switch-guide-version1_01.pdf

(5) ネットワークセキュリティデザイン

[21] Jazib Frashim, and Omar Santos, "Cisco ASA All-in-One Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance - Identify, mitigate, and respond to network attacks", Cisco Press, 2010.

[22] Catherine Paquet, "Authorized Self-Study Guide Implementing Cisco IOS Network Security", Cisco Press, 2009.

第2部　マルウェア対策

(1)攻撃検知・収集

[23] 小久保 博崇, 金岡 晃, 満保 雅浩, 岡本 栄司, "攻撃通信検知のための合成型機械学習手法の一検討", 情報処理学会論文誌, Vol. 53, No. 9, pp.2086-2093, 2012.

[24] 市野 将嗣, 市田 達也, 畑田 充弘, 小松 尚久, "トラヒックの時系列データを考慮したAdaBoost に基づくマルウェア感染検知手法", 情報処理学会論文誌, Vol. 53, No. 9, pp.2062-2074, 2012.

[25] John P. John, Fang Yu, Yinglian Xie, Arvind Krishnamurthy, and Martín Abadi, "Heat-seeking Honeypots: Design and Experience", Proc. 20th Conf. on world wide web conference 2011 (WWW '01), pp.207-216, 2011.

[26] T.Yagi, N.Tanimoto, T.Hariu and M.Itoh, "Intelligent High-Interaction Web Honeypots Based on URL Conversion Scheme", IEICE TRANS.COMMUN., Vol. E94-B, No. 5, pp.1339-1347, 2011.

[27] 市野 将嗣, 市田 達也, 畑田 充弘, 小松 尚久, "トラヒックの時系列データを考慮したマルウェア感染検知手法に関する一検討", コンピュータセキュリティシンポジウム 2011(CSS 2011)論文集, pp.283-288, 2011.

[28] 川元 研治, 市田 達也, 市野 正嗣, 畑田 充弘, 小松 尚久, "マルウェア感染検知のための経年変化を考慮した特徴量評価に関する一考察", コンピュータセキュリティシンポジウム 2011(CSS 2011)論文集, pp.277-282, 2011.

[29] T. Yagi, N. Tanimoto, T. Hariu, and M. Itoh, "Intelligent High-Interaction Web Honeypots Based on URL Conversion Scheme", IEICE TRANS. COMMUN.,Vol.E94-B, No.5, pp.1339-1347, 2011.

[30] T.Yagi, N.Tanimoto, T.Hariu and M.Itoh, "Design of Provider-Provisioned Website Protection Scheme against Malware Distribution", IEICE TRANS.COMMUN., Vol.E93-B, No. 5, pp.1122-1130, 2010.

[31] T.Yagi, N.Tanimoto, T.Hariu and M.Itoh, "Life-cycle Monitoring Scheme of Malware Download Sites for Websites", Proc. IEEE International Conference on Service-Oriented Computing and Applications (SOCA 2010), pp.1-6, 2010.

[32] T.Yagi, N.Tanimoto, T.Hariu and M.Itoh, "Investigation and Analysis of Malware on Websites", Proc. 12th IEEE Symposium on Web Systems Evolution (WSE 2010), pp.73-81, 2010.

[33] T.Yagi, N.Tanimoto, T.Hariu and M.Itoh, "Enhanced Attack Collection Scheme on High-Interaction Web Honeypots", Proc. IEEE Symposium on Computers and Communications (ISCC 2010), pp.81-86 Jun, 2010.

[34] Long Lu, Vinod Yegneswaranz, Phillip Porrasz, and Wenke Lee, "BLADE: An

Attack-Agnostic Approach for Preventing Drive-By Malware Infections", Proc. 17th ACM Conference on Computer and Communications security (ACM CCS'10), pp.440-450, 2010.

[35] 桑原 和也, 菊池 浩明, 寺田 真敏, 藤原 将志, "ボットネットの連携感染を判定する発見的手法について", 情報処理学会論文誌, Vo. 51, No.9, pp.1600-1609, 2010.

[36] 吉岡 克成, 村上 洸介, 松本 勉, "マルウェア感染ホスト検出のためのネットワークスキャン手法と検出用シグネチャの自動生成", 情報処理学会論文誌, Vol. 51, No. 9, pp.1633-1644, 2010.

[37] M. Akiyama, M. Iwamura, Y. Kawakoya, K. Aoki, and M. Itoh, "Design and Implementation of High Interaction Client Honeypot for Drive-by-Download Attacks", IEICE TRANS. COMMUN., Vol.E93-B,No.5, pp.1131-1139, 2010.

[38] Jose Nazario, "PhoneyC: A Virtual Client Honeypot", Proc. 2nd USENIX conference on Large-scale exploits and emergent threats (USENIX LEET09), pp.6-6, 2009.

[39] 湯浅 紘一, 小林 和朝, 高田 寛之, "クライアント側 PC でのサーバ的振舞によるボット検出法", コンピュータセキュリティシンポジウム 2009(CSS2009)論文集, No.42, 2009.

[40] 水谷　正慶, 武田　圭史, 村井　純, "Web 感染型悪性プログラムの分析と検知手法の提案", 電子情報通信学会論文誌, Vol.J92-B, No.10, pp.1631-1642, 2009.

[41] 秋山 満昭, 岩村 誠, 川古谷 裕平, 青木 一史, 伊藤光恭, "クライアントハニーポットにおける攻撃検知手法の実装と評価", コンピュータセキュリティシンポジウム 2009(CSS2009)論文集, No.52, 2009.

[42] Niels Provos and Thorsten Holz,"VIRTUAL HONEYPOTS - From Botnet Tracking to Intrusion Detection", Addison Wesley, 2008.

[43] David Watson and Jamie Riden,"The Honeynet Project: Data Collection Tools, Infrastructure, Archives and Analysis", Proc. of the 2008 WOMBAT Workshop on Information Security Threats Data Collection and Sharing, pp.24-30, 2008.

[44] Guofei Gu, Roberto Perdisci, Junjie Zhang, and Wenke Lee, "BotMiner: Clustering Analysis of Network Traffic for Protocol- and Structure-Independent Botnet Detection", Proc. 17th conference on Security symposium(USENIX SS '08), pp.139-154, 2008.

[45] Guofei Gu, Junjie Zhang, and Wenke Lee, "BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic", Proc. 15th Annual Network & Distributed System Security Symposium(NDSS'08), 2008.

[46] Guofei Gu, Phillip Porras, Vinod Yegneswaran, Martin Fong, Wenke Lee, "BotHunter: Detecting Malware Infection Through IDS-Driven Dialog Correlation", Proc. 16th conference on Security symposium(USENIX SS '07), No.12, 2007.

[47] Georgios Portokalidis, Asia Slowinska, and Herbert Bos, "Argos: an Emulator for Fingerprinting Zero-Day Attacks", Proc. 1st ACM SIGOPS/EuroSys European

Conference on Computer Systems 2006, pp.15-27, 2006.

[48] K. G. Anagnostakis, S. Sidiroglou, P. Akritidis, K. Xinidis, E. Markatos and A. D. Keromytis, "Detecting targeted attacks using shadow honeypots", Proc. 14th conference on USENIX Security Symposium(SSYM '05), Vol. 14, pp.9-9, 2005.

[49] Niels Provos,"A Virtual Honeypot Framework",In Proc. of the 13th Conf. on USENIX Security Symposium 2004, pp.1-14, 2004.

[50] David Dagon, Xinzhou Qin, Guofei Gu, Wenke Lee Julian Grizzard, John Levine, and Henry Owen, "HoneyStat: Local Worm Detection Using Honeypots", Proc. 7th International Symposium on Recent Advances in Intrusion Detection (RAID 2004), pp.39-58, 2004.

(2)解析

[51] Zhaoyan Xu, Lingfeng Chen, Guofei Gu, and Christopher Kruegel, "PeerPress: Utilizing Enemies'P2P Strength against Them", Proc. the 2012 ACM conference on Computer and communications security (CCS'12), pp. 581-592, 2012.

[52] Kathy Wain Yee Au, Yi Fan Zhou, Zhen Huang, and David Lie, "PScout: Analyzing the Android Permission Specification", Proc. the 2012 ACM conference on Computer and communications security (CCS'12), pp. 217-228, 2012.

[53] Cong Zheng, Shixiong Zhu, Shuaifu Dai, Guofei Gu, Xiaorui Gong, Xinhui Han, and Wei Zou, "SmartDroid: An Automatic System for Revealing UI-based Trigger Conditions in Android Applications", Proc. the second ACM workshop on Security and privacy in smartphones and mobile devices (CCS'12), pp. 93-104, 2012.

[54] K. Aoki, T. Yagi, M. Iwamura, and M. Itoh, "Controlling Malware HTTP Communications in Dynamic Analysis System using Search Engine", The 3rd International Workshop on Cyberspace Safety and Security (CSS2011), 2011.

[55] M. Akiyama, T. Yagi, and M. Itoh, "Searching Structural Neighborhood of Malicious URLs to Improve Blacklisting", The 12th IEEE/IPSJ International Symposium on Applications and the Internet (SAINT 2011), 2011.

[56] G. Jacob, R. Hund, C. Kruegel, and T. Holz, "JACKSTRAWS: Picking Command and Control Connections from Bot Traffic.", USENIX Security SymposiumUSENIX Association (2011).

[57] 岩本 一樹, 和崎 克己, "制御フロー解析による Android マルウェア検出方法の提案", コンピュータセキュリティシンポジウム 2011(CSS 2011)論文集, pp.714-719, 2011.

[58] 名雲 孝昭, 甲斐 俊文, 佐々木 良一, "ボットネット多段追跡システムにおける最終段階追跡方式の提案と評価", 情報処理学会論文誌, Vol. 52, No.12, pp.3766-3774, 2011.

[59] 千葉 大紀, 八木 毅, 秋山 満昭, 森 達哉, 後藤 滋樹, "多種多様な攻撃に用いられる IP ア

ドレス間の相関解析", コンピュータセキュリティシンポジウム 2011(CSS 2011) 論文集, pp.185-190, 2011.

[60] 新井 悠, 岩村 誠, 川古谷 裕平, 青木 一史, 星澤 裕二,"アナライジング・マルウェア――フリーツールを使った感染事案対処",オライリージャパン,2010.

[61] 岩村 誠, 伊藤光恭, 村岡 洋一, "機械語命令列の類似性に基づく自動マルウェア分類システム", 情報処理学会論文誌, Vol. 51, No.9, pp.1622-1632, 2010.

[62] Y. Kawakoya, M. Iwamura, and M. Itoh, "Memory Behavior-Based Automatic Malware Unpacking in Stealth Debugging Environment", IEEE International Conference on Malicious and Unwanted Software(MALWARE2010), 2010.

[63] Clemens Kolbitsch, Paolo Milani Comparetti, Christopher Kruegel, Engin Kirda, Xiaoyong Zhou, and XiaoFeng Wang, "Effective and Efficient Malware Detection at the End Host", Proc. 18th conference on USENIX security symposium (USENIX SSYM '09), pp.351-366, 2009.

[64] 中尾康二, 井上 大介, 衛藤将史, 吉岡克成, 大高 一弘, "ネットワーク観測とマルウェア解析の融合に向けて-インシデント分析センターnicter の研究開発", 情報処理, Vol. 50, No. 3, pp.235-242, 2009.

[65] D. Song, D. Brumley, H. Yin, J. Caballero, I. Jager, M. G. Kang, Z.Liang, J. Newsome, P. Possankam, and P. Saxena, "BitBlaze: A New Approach to Computer Security via Binary Analysis", Proc. 4th International Conference on Information Systems Security (ICISS '08), pp.1-25, 2008.

[66] Artem Dinaburg, Paul Royal, Monirul Sharif, and Wenke Lee, "Ether:Malware Analysis via Hardware Virtualization Extensions", Proc. 15th ACM conference on Computer and communications security(CCS '08), pp.51-62, 2008.

[67] David Brumley, Cody Hartwig, Zhenkai Liang, James Newsome, Dawn Song, and Heng Yin, "Automatically Identifying Trigger-Based Behavior in Malware", Botnet Detection, Springer Publications, 2008.

[68] I. V. Popov, S. K. Debray, and G. R. Andrews, "Binary obfuscation using signals", Proc. 16th USENIX Security Symposium on USENIX Security Symposium (USENIX SS '07), pp. 275-290, 2007.

[69] R. Lyda, and J. Hamrock, "Using entropy analysis to find encrypted and packed malware", IEEE Security and Privacy, Vol.5, No.2, pp. 40-45, 2007.

[70] Min Gyung Kang, Pongsin Poosankam, and Heng Yin, "Renovo: a hidden code extractor for packed executables", Proc. 2007 ACM workshop on Recurring malcode (WORM '07), pp.46-53, 2007.

[71] Yason, M.V., "The Art of Unpacking", Black Hat Briefings USA 2007

[72] H. Yin, D. Song, M.Egele, C. Kruegel, and E. Kirda, "Panorama: Capturing

System-wide Information Flow for Malware Detection and Analysis", Proc. 14th ACM conference on Computer and communications security (CCS '07), pp.116-127, 2007.

[73] C.Willems, T. Holz, and F. Freiling, "Toward Anutomated Dynamic Malware Analysis Using CWSandbox", IEEE Security and Privacy, Vol. 5, No. 2, pp. 32-39, 2007.

[74] Mihai Christodorescu, Somesh Jha,and Christopher Kruegel, "Mining specifications of malicious behavior", Proc. 6th joint meeting of the European software engineering conference and the ACM SIGSOFT symposium on The foundations of software engineering (ESEC-FSE '07), pp.5-14, 2007.

[75] Michael Bailey, Jon Andersen, Z. Morleymao, and Farnam Jahanian, "Automated classification and analysis of internet malware", Proc. 10th international conference on Recent advances in intrusion detection (RAID '07), pp. 178-197, 2007.

[76] Susanta Nanda, Wei Li, Lap-Chung Lam, and Tzi cker Chiueh, "Bird: Binary interpretation using runtime disassembly", Proc. International Symposium on Code Generation and Optimization (CGO '06), pp. 358-370, 2006.

[77] U.Bayer, A.Moser, C.Krugel, and E.Kirda, "Dyanmic analysis of malicious code", Journal in Computer Virology, Vol.2, No.1,pp.67-77, 2006.

[78] Amit Vasudevan, and Ramesh Yerraballi, "Cobra:Fine-grained Malware Analysis using Stealth Localized-executions", Proc. 2006 IEEE Symposium on Security and Privacy (S&P '06), pp.279-283, 2006.

[79] Fabrice Bellard, "QEMU, a fast and portable dynamic translator", Proc. annual conference on USENIX Annual Technical Conference(ATEC '05), pp.41-41, 2005.

[80] Amit Vasudevan, and Ramesh Yerraballi, "Stealth Breakpoints", Proc. 21st Annual Computer Security Applications Conference (ACSAC '05), pp.381-392, 2005.

[81] M. E. Karim, A. Walenstein, A. Lakhotia, and L. Parida, "Malware phylogeny generation using permutations of code", European Research Journal of Computer Virology 1, 1-2 (Nov. 2005) pp. 13-23, 2005.

[82] M. Gheorghescu, "An automated virus classification system", Proc. Virus Bulletin Conf. 2005, pp. 294-300, 2005.

[83] C. Luk, R. Cohn, R. Muth, H. Patil, A. Klauser, G. Lowney, S. Wallace, V. J. Reddi, and K. Hazelwood, "Pin: Building Customized Program Analysis Tools with Dynamic Instrumentation", Proc. 2005 ACM SIGPLAN conference on Programming language design and Implementation (PLDI '05), pp.190-200, 2005.

[84] Christopher Kruegel, William Robertson, Fredrik Valeur, and Giovanni Vigna, "Static disassembly of obfuscated binaries", Proc. 13th conference on USENIX Security Symposium(USENIX SSYM'04), pp. 255–270, 2004.

[85] E. Carrera and G. Erdelyi, "Digital genome mapping - advanced binary malware

analysis", Proc. Virus Bulletin Conf. 2004, pp. 187-197, 2004.

[86] Cullen Linn, and Saumya Debray, "Obfuscation of executable code to improve resistance to static disassembly", Proc. 10th ACM conference on Computer and communications security (CCS '03), pp.290-299, 2003.

[87] B. Schwarz, S. Debray, and G. Andrews, "Disassembly of executable code revisited", Proc. 9th Working Conference on Reverse Engineering (WCRE '02), pp.45, 2002.

[88] G.Hunt, and D.Brubacher, "Detours: binary interception of Win32 functions", Proc. 3rd conference on USENIX Windows NT Symposium (WINSYM'99), Vol.3, pp.14-14, 1999.

(3)対策

[89] Richard Wartell, Vishwath Mohan, Kevin W. Hamlen, and Zhiqiang Lin, "Binary Stirring: Self-randomizing Instruction Addresses of Legacy x86", Proc. the 2012 ACM conference on Computer and communications security (CCS'12), pp. 157-168, 2012.

[90] C. Giuffrida, A. Kuijsten, and A. S. Tanenbaum, "Enhanced operating system security through efficient and fine-grained address space randomization", Proc. 21st USENIX conference on Security symposium (Security'12), pp.40-40, 2012.

[91] Vasilis Pappas, Michalis Polychronakis, and Angelos D. Keromytis, "Smashing the Gadgets: Hindering Return-Oriented Programming Using In-Place Code Randomization, Vasilis Pappas, Michalis Polychronakis, and Angelos D. Keromytis", Proc. 33rd IEEE Symposium on Security & Privacy (S&P' 12), pp.601-615, 2012.

[92] Suman Jana, and Vitaly Shmatikov, "Memento: Learning Secrets from Process Footprints", Proc. 33rd IEEE Symposium on Security and Privacy (S&P '12), pp.143-157, 2012.

[93] S. Checkoway, L. Davi, A. Dmitrienko, A.-R. Sadeghi, H. Shacham, and M. Winandy, "Return-oriented programming without returns", Proc. 17th ACM conference on Computer and communications security (CCS'10), pp.559-572, 2010.

[94] B. Cox, D. Evans, A. Filipi, J. Rowanhill, W. Hu, J. Davidson, J. Knight, A. Nguyen-Tuong, and J. Hiser, "N-variant systems: a secretless framework for security through diversity", Proc. 15th Conference on USENIX Security Symposium(USENIX SS'06), Vol.15, No.9, 2006.

[95] G. S. Kc, Angelos D. Keromytis, and V. Prevelakis, "Countering code-injection attacks with instruction-set randomization", Proc. 10th ACM conference on Computer and communications security (CCS '03), pp.272-280, 2003.

[96] C. Cowan, S. Beattie, J. Johansen, and P. Wagle, "Pointguard: protecting pointers from buffer overflow vulnerabilities", Proc. 12th conference on USENIX Security Symposium (SSYM '03), pp.7-7, 2003.

[97] C. Cowan, C. Pu, D. Maier, H. Hinton, P. Bakke, S. Beattie, A. Grier, P. Wagle, and Q. Zhang, "StackGuard: Automatic detection and prevention of buffer-overflow attacks", Proc. 7th USENIX Security Symposium(SSYM '98), pp.5-5, 1998.

(4)実態調査

[98] Zhou Li, Kehuan Zhang, Yinglian Xie, Fang Yu, and XiaoFeng Wang, "Knowing your enemy: understanding and detecting malicious web advertising", Proc. the 2012 ACM conference on Computer and communications security (CCS'12), pp.674-686, 2012.

[99] Chris Grier, Lucas Ballard, Juan Caballero, Neha Chachra, Christian J. Dietrich, Kirill Levchenko, Panayiotis Mavrommatis, Damon McCoy, Antonio Nappa, Andreas Pitsillidis, Niels Provos, M. Zubair Rafique, Moheeb Abu Rajab, Christian Rossow, Kurt Thomas, Vern Paxson, Stefan Savage, and Geoffrey M. Voelker, "Manufacturing Compromise: The Emergence of Exploit-as-a-Service", Proc. the 2012 ACM conference on Computer and communications security (CCS '12), pp. 821-832, 2012.

[100] amon McCoy, Hitesh Dharmdasani, Christian Kreibich, Geoffrey M. Voelker, and Stefan Savage, "Priceless: The Role of Payments in Abuse-Advertised Goods", Proc. the 2012 ACM conference on Computer and communications security (CCS '12), pp. 845-856, 2012.

[101] Markus Kammerstetter, Christian Platzer, and Gilbert Wondracek, "Vanity, Cracks and Malware: Insights into the Anti-Copy Protection Ecosystem", Proc. the 2012 ACM conference on Computer and communications security (CCS '12), pp. 809-820, 2012.

[102] Chi-Yao Hong, Fang Yu, and Yinglian Xie, "Populated IP Addresses - Classification and Applications", Proc. the 2012 ACM conference on Computer and communications security (CCS'12), pp. 329-340, 2012.

[103] Leyla Bilge, and Tudor Dumitras, "Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World", Proc. the 2012 ACM conference on Computer and communications security (CCS'12), pp. 833-844, 2012.

[104] 甲斐 俊文, 佐々木 良一, "効果的なボットネット追跡に関する調査と検討", 情報処理学会論文誌, Vol. 52, No.3, pp.1136-1143, 2011.

[105] Tongbo Luo, Hao Hao, Wenliang Du, Yifei Wang, and Heng Yin, "Attacks on WebView in the Android System", Proc. 27th Annual Computer Security Applications Conference (ACSAC '11), pp.343-352, 2011.

[106] Adrienne Porter Felt, Matthew Finifter, Erika Chin, Steven Hanna, and David Wagner, "A Survey of Mobile Malware in the Wild", Proc. 1st ACM workshop on Security and privacy in smartphones and mobile devices (SPSM '11), pp.3-14, 2011.

[107] M. Franz, "E unibus pluram: massive-scale software diversity as a defense

mechanism", Proc. 2010 workshop on New security paradigms (NSPW '10), pp.7-16, 2010.

[108] 青木 一史, 川古谷裕平, 秋山 満昭, 岩村 誠, 針生 剛男, 伊藤光恭, "能動的攻撃と受動的攻撃に関する調査および考察", 情報処理学会論文誌, Vol. 50, No. 9, pp.2147-2162, 2009.

[109] Niels Provos, Panayiotis Mavrommatis, Moheeb Abu Rajab, and Fabian Monrose, "All Your iFRAMEs Point to Us", Proc. 17th conference on Security symposium(USENIX SS '08), pp.1-15, 2008.

第3部　脅威・脆弱性

（1）脅威一般

[110] 宮地 利雄, "組織・企業の制御システムを守る", 電気学会誌　Vol.132, No.6, pp.354-359, 2012.

[111] David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni(著),青木 一史,秋山 満昭, 岩村 誠,川古谷 裕平,川島 祐樹,辻 伸弘,宮本 久仁男,岡 真由美(訳),"実践　Metasploit ---ペネトレーションテストによる脆弱性評価",オライリージャパン,2012.

[112] 小出 洋, 金岡 晃, 加藤 雅彦, "新しいタイプの脅威を分析するための情報システムとマルウェアを表現する DSL", 夏のプログラミング・シンポジウム 2011 報告集, pp.89-94, 2012.

[113] 鬼頭 哲郎, 松木 隆宏, 松岡 正明, 仲小路 博史, 寺田 真敏, "パケットマーキングによる不正活動ホスト広報機能の開発", 情報処理学会論文誌, Vol. 53, No. 9, pp.2148-2159, 2012.

[114] 野村 大翼, 松尾 和人, "Bluetooth のセキュアシンプルペアリングに対する中間者攻撃 ", 情報処理学会論文誌, Vol. 53, No. 9, pp.2225-2233, 2012.

[115] 本城信輔,"PC のウィルスを根こそぎ削除する方法",技術評論社,2011.

[116] 原田　泉, "ネット上の危機管理と安全補償", IEEJ Transactions on Electronics Information and Systems, Vol.131, No.2, pp.258-264, 2011.

[117] 山田 建史, 戸部 和洋, 森 達哉, 後藤 滋樹, "OpenFlow スイッチによる悪意のある通信の集約", コンピュータセキュリティシンポジウム 2011(CSS 2011)論文集, pp.301-306, 2011.

[118] 木佐森幸太, 下田 晃弘, 森 達哉, 後藤 滋樹, "TCP フィンガープリントによる悪意のある通信の分析", 情報処理学会論文誌, Vol. 52, No.6, pp.2009-2018, 2011.

[119] 高橋　宏尚, 呂　暁東, 森　欣司, "局所的な HTTP レベルのサイバーアタックを高応答で解析する自律分散 Web アプリケーションファイアウォール(WAF)", 電子情報通信学会論文誌, Vol.J94-D, No.10, pp.1595-1603, 2011.

[120] 原田 敏樹, 金岡 晃, 加藤 雅彦, 勝野 恭治, 岡本 栄司, "ネットワークシステムにおける脆弱性影響の測定手法とシステム実装", 情報処理学会論文誌, Vol. 52, No. 9, pp.2613-2623, 2011.

[121] 寺田 真敏, 菊池 浩明, "マルウェア特集", 情報処理, Vol. 5, No. 3, pp.235-303, 2010.

[122] 丸山 勝久, 戸子田健祐, 大森 隆行, "脆弱性に関する影響の可能性を警告するリファクタリング", 情報処理学会論文誌, Vol. 51, No. 9, pp.1777-1793, 2010.

[123] 武田 圭史, 水谷 正慶, 中井 研, "IPv6 導入に伴うセキュリティリスクに関する分析", コンピュータセキュリティシンポジウム 2009(CSS2009)論文集,2009,No. 83, 2009.

[124] 下田　晃弘, 後藤　滋樹, "フローデータからの Dark IP 抽出による脅威観測法", 電子情

報通信学会論文誌, Vol.J92-B, No.1, pp.163-173, 2009.

[125] Christopher Wells(著),牧野聡(訳),"Ajax アプリケーション& Web セキュリティ",オライリージャパン,2008.

[126] 石黒 正揮, 鈴木 裕信, 村瀬 一郎, 篠田 陽一, "インターネット上の脅威分析を支援する空間および時間的な特徴量に基づく分析手法", 情報処理学会論文誌, Vol. 48, No. 9, pp.3148-3162, 2007.

[127] 大垣靖男,"Web アプリセキュリティ対策入門",技術評論社,2006.

[128] Mark G. Graff, Kenneth R. van Wyk（著）,新井悠一,一瀬小枝(訳),"セキュアプログラミング",オライリージャパン,2004.

(2)レポート

[129] Verizon, "2012 年度データ漏洩/侵害調査報告書",2012.
http://www.verizonbusiness.com/resources/reports/rp_2012_Data_Breach_Investigations_Report_ja_xg.pdf

[130] Symantec, "インターネットセキュリティ脅威レポート 2011 年の傾向",Symantec 第 17 号,2012.
http://www.symantec.com/content/ja/jp/enterprise/white_papers/istr17_wp_201207.pdf

[131] トレンドマイクロ, "インターネット脅威年間レポート - 2011 年度",2011
http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/article/20120106083242.html

[132] ヒューレットパッカード, "2011 年度トップサイバーセキュリティリスクレポート", ヒューレットパッカード テクニカルホワイトペーパー, 2012.
http://h50146.www5.hp.com/products/software/hpsoftware/magazine/201207/pdfs/2011_top_security_report.pdf

[133] McAfee, "McAfee 脅威レポート： 2012 年度第 1 四半期",McAfee Labs レポート,2012.
http://www.mcafee.com/japan/media/mcafeeb2b/international/japan/pdf/threatreport/threatreport12q1.pdf

[134] Chad Dougherty, "Practical Identification of SQL Injection Vulnerabilities",United States Computer Emergency Readiness Team(US-CERT), 2012.
http://www.us-cert.gov/reading_room/Practical-SQLi-Identification.pdf

[135] DHS (U.S. Department of Homeland Security), "Blueprint for a Secure Cyber Future",2011.
http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf

[136] DHS (U.S. Department of Homeland Security), "A Roadmap for Cybersecurity Research",2009.
http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf

(3)Web サイト

[137] JPCERT, http://www.jpcert.or.jp/

[138] US-CERT, http://www.us-cert.gov/
[139] CERT/CC, http://www.cert.org/
[140] NIST, "National Vulnerability Database", http://nvd.nist.gov/
[141] JVN (JPCERT, IPA), "脆弱性対策情報データベース", http://jvndb.jvn.jp/
[142] (独)情報処理推進機構,"情報セキュリティ", http://www.ipa.go.jp/security/

第4部　CERT活動

(1)セキュリティ対策

[143] Paul Vixie, Andrew Fried, "The DCWG Debriefing. How the FBI Grabbed a Bot and Saved the Internet", blackhat USA 2012/DEFCON 20, 2012.

[144] FX, Greg, "Hacking [redacted] Routers", blackhat USA 2012/DEFCON 20, 2012.

[145] Dan Kaminsky, "Black Ops", blackhat USA 2012/DEFCON 20, 2012.

[146] Charlie Miller, "Don't Stand So Close To Me: An Analysis of the NFC Attack Surface", blackhat USA 2012/DEFCON 20, 2012.

[147] Ryan Reynolds, Jonathan Claudius, "Stamp Out Hash Corruption! Crack All The Things", blackhat USA 2012/DEFCON 20, 2012.

[148] Bitweasil, "Cryptohaze Cloud Hacking", blackhat USA 2012/DEFCON 20, 2012.

[149] Nils & Rafael Dominguez Vega, "PinPadPwn", blackhat USA 2012/DEFCON 20, 2012.

[150] Martin Gallo, "Uncovering SAP Vulnerabilities:Reversing and Breaking the Diag Protocol", blackhat USA 2012/DEFCON 20, 2012.

[151] "Kakareka, Almantas（CTO, Demyo, Inc.）, "Insight Into Russian Black Market", 24th Annual FIRST conference, 2012.

[152] 町村 泰貴,小向 太郎,藤村 明子,金子 宏直,橋本 豪,西山 俊彦,松前 恵環,須川 賢洋, "実践的ｅディスカバリ　－米国民事訴訟に備える－", NTT 出版,2010.

[153] NTT 情報流通プラットフォーム研究所, "事例で学ぶ　セキュリティ運用技術・インシデント対応技術", アスキー, 2006.

[154] NTT 情報流通プラットフォーム研究所, "最新　情報漏洩対策ガイドブック", アスキー, 2006.

[155] NTT 情報流通プラットフォーム研究所, "事例で学ぶ　OS・アプリケーションセキュリティ", アスキー, 2006.

(2)インシデントハンドリング

[156] Douglas Wilson, "Approaching Real-Time: Threat Information Sharing with OpenIOC", GFIRST2012 8th annual natioal conferenc, 2012.

[157] Will Dormann,　"Vulnerability Discovery Through Fuzzing with the CERT BFF and FOE", GFIRST2012 8th annual natioal conferenc, 2012.

[158] Christopher Poulin,　"CyberSecurity: Continuous Monitoring and Real Time Risk Scoring", GFIRST2012 8th annual natioal conferenc, 2012.

[159] Peter Fonash, Tom Millar, Kathleen Moriarty, Phyllis Schneck, and Richard Struse, "Automated Intelligence Sharing to Improve Cybersecurity", GFIRST2012 8th annual natioal conferenc, 2012.

[160] Sabrina Segal, "Hey, You, Get Off of My Cloud!: Negotiate Your Cloud Contract to Get What You Want and Mitigate Risk", GFIRST2012 8th annual natioal conferenc, 2012.

[161] Katsutoshi Ishisoko, and John Wang, "Analysis of SOC Incidents and Continuous Monitoring of Threat", GFIRST2012 8th annual natioal conferenc, 2012.

[162] John Howie, "CloudCERT: An Introduction and Overview to Defending the Cloud Computing Ecosystem", GFIRST2012 8th annual natioal conferenc, 2012.

[163] Julie Mehan, "Are We Really in a CyberWar? - The Real Dangers of Hype", GFIRST2012 8th annual natioal conferenc, 2012.

[164] Mario Santana, "Securing the Cloud - A Cloud Provider's Perspective", GFIRST2012 8th annual natioal conferenc, 2012.

[165] Dan Guido, "The Mobile Exploit Intelligence Project", GFIRST2012 8th annual natioal conferenc, 2012.

[166] Tim Maletic, and Christopher Pogue, "OPFOR 4Ever", GFIRST2012 8th annual natioal conferenc, 2012.

[167] Thad Odderstol, "Enhancing Cybersecurity Awareness and Resiliency Across the 18 Critical Infrastructure and Key Resource (CIKR) Sectors by Collaborating with the National Cyber Security Division's (NCSD) Critical Infrastructure Protection Cyber Security (CIP CS) Program", GFIRST2012 8th annual natioal conferenc, 2012.

[168] Jeff Boerio, and Sean McCracken, "Emerging Threat Landscape: 2012 and Beyond", GFIRST2012 8th annual natioal conferenc, 2012.

[169] Sabrina Hammouda, and Jason Gates, "Bringing Together Emergency Services Sector (ESS) Jurisdictions and Stakeholders to Strategically and Uniformly Address Cyber Risk", GFIRST2012 8th annual natioal conferenc, 2012.

[170] Gerald Derrick, and Cory Mazzola, Technical Manager, "Operationalizing Data: An Intelligent and Systematic Approach", GFIRST2012 8th annual natioal conferenc, 2012.

[171] Steve Winterfeld, "How to Explain Today's Cyber Threats and Challenges to the Non-Technical Members of Your Organization", GFIRST2012 8th annual natioal conferenc, 2012.

[172] Schuster, Andreas(Senior Computer Forensic Examiner, Deutsche Telekom AG), "Poison Ivy for Incident Responders", 24th Annual FIRST conference, 2012.

[173] Ziegast Eric, "Advances in Passive DNS Replication", 24th Annual FIRST conference, 2012.

[174] Reid Gavin, "Where automation ends and people begin - One CSIRT's journey replacing a SIEM with logging", 24th Annual FIRST conference, 2012.

[175] Pawlinski Pawel, "Honey Spider Network 2.0: detecting client-side attacks the easy

way", 24th Annual FIRST conference, 2012.

[176] Kamluk Vitaly and Raiu Costin, "a cyber missile", 24th Annual FIRST conference, 2012.

[177] Anil Suleyman, "Defending Cyberspace - Global Challenges Require Global Responses", 24th Annual FIRST conference, 2012.

[178] Jochem Aart, "The DigiNotar Crisis: from incident response to crisis coordination", 24th Annual FIRST conference, 2012.

[179] Dufkova Andrea and Kijewski Piotr, "Proactive Detection of Network Security Incidents - A Study", 24th Annual FIRST conference, 2012.

[180] Eronen Jussi, "AbuseHelper case studies: Gathering and sharing incident data among different communities", 24th Annual FIRST conference, 2012.

[181] Garci'a Mora'n Francisco, "IT Security @ EC: Challenges & Experiences", 24th Annual FIRST conference, 2012.

[182] ISO/IEC, "Information technology - Security techniques - Vulnerability disclosure", ISO/IEC DIS 29147, 2012.

[183] ISO/IEC, "Vulnerability handling processes", ISO/IEC CD 30111, 2012.

[184] Nadeem Douba, "Sploitego. Maltego's (Local) Partner in Crime", blackhat USA 2012/DEFCON 20, 2012.

[185] 「技術」分科会ワーキンググループ, "証拠保全ガイドライン", 特定非営利活動法人デジタル・フォレンジック研究会, 2012.
http://www.digitalforensic.jp/eximgs/20120713gijutsu.pdf

[186] 林　郁也, "3.11 に CSIRT ができたこと", 情報セキュリティワークショップ in 越後湯沢,2011, 2011.

[187] 辻井重男 監修, "デジタル・フォレンジック事典", 日科技連出版社, 2006.

[188] N. Brownlee, E. Guttman, "Expectations for Computer Security Incident Response", Request for Comments 2350, 1998.
http://www.ietf.org/rfc/rfc2350.txt

第5部　セキュリティマネジメント

(1)法制度

[189] 岡村久道, "情報セキュリティの法律［改訂版］", 商事法務, 2011.

[190] 石井一正, "刑事実務証拠法 第５版", 判例タイムズ社, 2011.

[191] 西垣正勝, 臼井佑真, 山本匠, 間形文彦, 勅使河原可海, 佐々木良一, "賠償リスクを考慮した情報セキュリティ対策選定方式の提案と評価", 情報処理学会論文誌, Vol.52, No.3, pp.1173-1184, 2011.

[192] 日本公認会計士協会, "監査実務ハンドブック〈平成 24 年版〉", 日本公認会計士協会出版局, 2011.

[193] 小向　太郎, "情報法入門 デジタル・ネットワークの法律　第２版",NTT 出版,2011.

[194] 経済産業省, "営業秘密管理指針", 2011.
http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/111216hontai.pdf

[195] 金融庁, "財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の改訂に関する意見書", 2011.
http://www.fsa.go.jp/singi/singi_kigyou/tosin/20110330.html

[196] 間形文彦, 高橋克巳, "ハニーポットによる通信役務の提供と電気通信事業者の通信の当事者性に係る通信の秘密の問題に関する一考察", 情報ネットワーク法学会 情報ネットワーク・ローレビュー, Vol.9, No.1, pp102-117, 2010.

[197] 瀬戸 洋一, 六川 浩明, 新保 史生, 村上 康二郎, 伊瀬 洋昭, "プライバシー影響評価 PIA と個人情報保護", 中央経済社, 2010.

[198] 経済産業省, "逐条解説 不正競争防止法 平成 21 年改正版", 有斐閣, 2010.

[199] 総務省, "電気通信事業における個人情報保護に関するガイドライン（告示）",2010.
http://www.soumu.go.jp/main_content/000076222.pdf

[200] 財務省, "財務省所管分野における個人情報保護に関するガイドライン（告示）",2010.
http://www.mof.go.jp/procedure/disclosure_etc/privacy/guidelines.pdf

[201] 厚生労働省, "医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン（局長通達）", 2010.
http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/170805-11a.pdf

[202] 厚生労働省, "医療情報システムの安全管理に関するガイドライン（局長通達）",2010.
http://www.mhlw.go.jp/shingi/2010/02/s0202-4.html

[203] 間形文彦, 高橋克巳, "ログを証拠に事実を証明する機能に基づく敗訴リスクの定式化", 電子情報通信学会 2009 年総合大会 基礎・境界講演論文集, pp.S-21-22, 2009.

[204] 間形文彦, 高橋克巳, "情報セキュリティ事件の証拠となるログを収集する情報システムの要件に関する一考察",情報処理学会コンピュータセキュリティシンポジウム 2009(CSS2009)論文集第 1 分冊,pp.99-104,2009.

[205] 経済産業省, "個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（告示）", 2009.
http://www.meti.go.jp/policy/it_policy/privacy/kaisei-guideline.pdf

[206] 金融庁, "金融分野における個人情報保護に関するガイドライン（告示）", 2009.
http://www.fsa.go.jp/common/law/kj-hogo/01.pdf

[207] 多賀谷 一照, "電気通信事業法逐条解説", 情報通信振興会, 2008.

[208] 間形文彦, 高橋克巳, 金井敦, "デジタル証拠の法的証明力を高めるための要件に関する一考察", 2008 年暗号と情報セキュリティシンポジウム(SCIS2008)予稿集, 4E1-6,2008.

[209] 経済産業省,"医療情報を受託管理する情報処理事業者向けガイドライン(告示)",2008.
http://www.meti.go.jp/policy/it_policy/privacy/080724iryou-kokuzi.pdf

[210] 門口 正人, 金井 康雄, 難波 孝一, 福田 剛久, "民事証拠法大系〈第 1 巻〉総論(1)", 青林書院, 2007.

[211] 間形文彦, 濱田貴広, "DBMS における業務処理統制機能の要件と課題に関する考察″, 情報処理学会研究報告, EIP-2007-30, pp23-30, 2007.

[212] 経済産業省知的財産政策室, "企業における適切な営業秘密管理―平成 17 年不正競争防止法改正・営業秘密管理指針改訂", 経済産業調査会, 2006.

[213] 藤原静雄, 個人情報保護法制研究会, "個人情報保護法の解説", 園部逸夫（編）, ぎょうせい, 2005.

[214] 門口 正人, 金井 康雄, 福田 剛久, 難波 孝一, "民事証拠法大系〈第 5 巻〉各論(3)鑑定 その他", 青林書院, 2005.

[215] 金融庁, "金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針（告示）", 2005.
http://www.fsa.go.jp/common/law/kj-hogo/04.pdf

[216] 門口 正人, "民事証拠法大系〈第 2 巻〉総論(2)", 青林書院, 2004.

[217] 経済産業省, "経済産業分野のうち個人遺伝情報を用いた事業分野における個人情報保護ガイドライン（告示）", 2004.
http://www.jba.or.jp/report/industry/document/pdf/09-9.pdf

[218] 文部科学省, "学校における生徒等に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針（告示）", 2004.
http://www.niigata-u.ac.jp/profile1/80_compliance_020/gakko_shishin.pdf

[219] 厚生労働省, "雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針（告示）", 2004.
http://www.mhlw.go.jp/topics/2004/07/tp0701-1.html

[220] 総務省, "行政機関の保有する個人情報の適切な管理のための措置に関する指針（局長通知）", 2004.
http://www.soumu.go.jp/main_sosiki/gyoukan/kanri/040914_1.html

[221] 総務省,"独立行政法人等の保有する個人情報の適切な管理のための措置に関する指針（局長通知）",2004.
http://www.soumu.go.jp/main_sosiki/gyoukan/kanri/040914_2.html
[222] 藤村明子, 鈴木幸太郎, 森田光, "内部告発者保護法制を考慮した個人情報保護方式", 暗号と情報セキュリティシンポジウム 2003(SCIS 2003)予稿集, 8A-1,2003.
[223] 加戸 守行, "著作権法逐条講義", 著作権情報センター, 2003.
[224] 小林 秀之, "新証拠法", 弘文堂, 2003.
[225] 門口 正人, 金井 康雄, 福田 剛久, 難波 孝一,"民事証拠法大系〈第 3 巻〉各論(1)人証", 青林書院, 2003.
[226] 門口 正人, "民事証拠法大系〈第 4 巻〉各論(2)", 青林書院, 2003.
[227] 西村総合法律事務所, "ネットメディアプラクティスチーム, IT 法大全―ビジネス・ローの IT 対応と最先端実務", 日経 BP 社, 2002.
[228] 堀部 政男, "発信電話番号表示とプライバシー", NTT 出版, 1998.
[229] トレッドウェイ委員会組織委員会（著), 鳥羽 至英,高田 敏文,八田 進二（訳),"内部統制の統合的枠組み 理論篇", 白桃書房, 1996.
[230] 最高裁判所事務総局刑事局, "証拠能力に関する刑事裁判例集-非典型的証拠の証拠能力について-", 法曹会, 1991.

(2)規格・標準

[231] NIST SP800, http://csrc.nist.gov/publications/PubsSPs.html
[232] NIST SP800 シリーズ日本語訳　http://www.nri-secure.co.jp/security/nist.html
[233] ISO http://www.iso.org/iso/
[234] JIS http://www.jisc.go.jp/
[235] ISO/IEC, "Information technology -- Security techniques -- Network security -- Part 2: Guidelines for the design and implementation of network security",ISO/IEC 27033-2, 2012.
[236] NIST, "Security and Privacy Controls for Federal Information Systems and Organizations", NIST SP 800-54 Rev.4, 2012.
[237] NIST, "Cloud Computing Synopsis and Recommendations", NIST SP 800-146, 2012.
[238] JASA（日本セキュリティ監査協会）, "クラウド情報セキュリティ管理基準",2012.
http://www.jasa.jp/about/result/pdf2011/2011_cloud_doc02.pdf
[239] ISO/IEC, "Information technology -- Service management -- Part 2: Guidance on the application of service management systems", ISO/IEC 20000-2, 2012.
[240] ISO/IEC, "Information technology -- Service management -- Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1", ISO/IEC 20000-3, 2012.
[241] ISO, "Societal security -- Business continuity management systems ---

Requirements",ISO 22301, 2012.

[242] ISO/IEC, "Information technology -- Security techniques -- Information security risk management",ISO/IEC 27005, 2011.

[243] 経済産業省, "クラウドサービス利用のための情報セキュリティマネジメントガイドライン",2011.
http://www.meti.go.jp/press/2011/04/20110401001/20110401001.html

[244] ISO/IEC, " Information technology -- Service management -- Part 1: Service management system requirements", ISO/IEC 20000-1, 2011.

[245] ISO/IEC, "Information technology -- Security techniques -- Information security management system implementation guidance", ISO/IEC 27003, 2010.

[246] ISO/IEC, "Information technology -- Security techniques -- Network security -- Part 3: Reference networking scenarios -- Threats, design techniques and control issues", ISO/IEC 27033-3, 2010.

[247] ISO, "Guidance on social responsibility", ISO 26000, 2010.

[248] リスクマネジメント規格活用検討会, "ISO31000:2009 リスクマネジメント解説と適用ガイド", 日本規格協会, 2010.

[249] ISO/IEC, "Information technology -- Security techniques -- Information security management -- Measurement", ISO/IEC 27004, 2009.

[250] ISO/IEC, "Information technology -- Security techniques -- Network security -- Part 1: Overview and concepts", ISO/IEC 27033-1, 2009.

[251] ISO/IEC, "Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model", ISO/IEC 15408-1, 2009.

[252] NIST, "Integrating Security into the Capital Planning and Investment Control Process", NIST SP800-65 Rev.1(Draft), 2009.

[253] ISO, "Risk management -- Principles and guidelines", ISO 31000, 2009.

[254] ISO/IEC, "Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations based on ISO/IEC 27002", ISO/IEC 27011, 2008.

[255] 経済産業省, "情報セキュリティ管理基準（平成２０年改正版）",2008.
http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Management_Standard.pdf

[256] ISO/IEC, "Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components", ISO/IEC 15408-2, 2008.

[257] ISO/IEC, "Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components", ISO/IEC 15408-3, 2008.

[258] ISO/IEC, "Information technology -- Security techniques -- Methodology for IT security evaluation", ISO/IEC 18045, 2008.

[259] ISO/IEC, "Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model(R) (SSE-CMM(R))", ISO/IEC 21827, 2008.

[260] ISO/IEC, "Systems and software engineering -- System life cycle processes", ISO/IEC 15288, 2008.

[261] ISO/IEC, "Systems and software engineering -- Software life cycle processes", ISO/IEC 12207, 2008.

[262] ISO/IEC, "Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services", ISO/IEC 24762, 2008.

[263] NIST, "Security Considerations in the System Development Life Cycle", NIST SP800-64 Rev.2, 2008.

[264] ISO/IEC, "Corporate governance of information technology", ISO/IEC 38500, 2008.

[265] 大木 栄二郎,"情報セキュリティ監査公式ガイドブック", 日本セキュリティ監査協会（編), 日科技連出版社, 2007.

[266] JIS, "情報技術―サービスマネジメント―第１部：仕様", JIS Q 20000-1, 2007.

[267] JIS, "情報技術―サービスマネジメント―第２部：実践のための規範", JIS Q 20000-2, 2007.

[268] ISO/IEC, "Information technology -- Security techniques -- IT network security -- Part 5: Securing communications across networks using virtual private networks", ISO/IEC 18028-5, 2006.

[269] JIS, "個人情報保護マネジメントシステム―要求事項 ", JIS Q 15001:2006.

[270] BS, "Business continuity management-Part 1: Code of practice",BS 25999-1, 2006.

[271] BS, "Business continuity management-Part 2: Specification", BS 25999-2, 2006.

[272] ISO/IEC, "Information technology -- Security techniques -- Information security management systems -- Requirements", ISO/IEC 27001, 2005.

[273] ISO/IEC, "Information technology -- Security techniques -- Code of practice for information security management", ISO/IEC 27002, 2005.

[274] ISO/IEC, "Information technology -- Security techniques -- IT network security -- Part 3: Securing communications between networks using security gateways", ISO/IEC 18028-3, 2005.

[275] ISO/IEC, "Information technology -- Security techniques -- IT network security -- Part 4: Securing remote access", ISO/IEC 18028-4, 2005.

[276] 内閣府 防災担当,"事業継続ガイドライン　第一版", 2005.
http://www.bousai.go.jp/MinkanToShijyou/guideline01.pdf

[277] 麗澤大学経済研究センター, "倫理法令遵守マネジメントシステム規格　ECS2000 v1.2", 2000.

(3)トラスト・安心

[278] 山本太郎,植田広樹,関良明,高橋克巳,小笠原盛浩,関谷直也,中村功,橋元良明,"ネットショッピング・オークション利用に際する不安調査結果に対する一考察",情報処理学会コンピュータセキュリティシンポジウム論文集,pp.547-554,2012.

[279] 千葉直子,山本太郎,関良明,高橋克巳,小笠原盛浩,関谷直也,中村功,橋元良明,"被災地住民の情報通信利用の実態と心理 －東日本大震災の被災地住民への訪問留置調査－",情報処理学会 DICOMO シンポジウム 2012 論文集, pp238-245, 2012.

[280] 山本太郎,千葉直子,関良明,高橋克巳,小笠原盛浩,関谷直也,中村功,橋元良明,"被災地住民のインターネット利用における安心と不安",情報処理学会 DICOMO シンポジウム 2012 論文集, pp246-257, 2012.

[281] 千葉直子,関良明,橋元良明,"青少年のネット利用に関する保護者へのグループインタビュー調査の一考察",情報処理学会コンピュータセキュリティシンポジウム論文集,pp.450-457, 2012.

[282] Tiffany Hyun-Jin Kim, Payas Gupta, Jun Han, Emmanuel Owusu, Jason Hong, Adrian Perrig, Debin Gao,"OTO: Online Trust Oracle for User-Centric Trust Establishment ", ACM CCS, 2012

[283] Taro YAMAMOTO, Naoko CHIBA, and Fumihiko MAGATA, "Investigation on anxieties while using the Internet to study about “Anshin” ", IPSJ Journal, Vol.52, No.7, pp.2046-2054, 2011.

[284] 山本太郎,千葉直子,植田広樹,高橋克巳,小笠原盛浩,関谷直也,中村功,橋元良明,"メディア系 CGM 利用における不安調査結果に対する一考察",情報処理学会コンピュータセキュリティシンポジウム論文集 2011(CSS 2011), pp.540-545, 2011.

[285] 山本太郎,植田広樹,高橋克巳,平田真一,関谷直也,中村功,小笠原盛浩,橋元良明,"テキスト系 CGM 利用における不安調査結果に対する一考察",情報処理学会 DICOMO シンポジウム 2011 論文集, pp.1482-1489, 2011.

[286] 千葉直子,山本太郎,植田広樹,高橋克巳,小笠原盛浩,関谷直也,中村功,橋元良明,"インターネット上の有害情報問題に関する国際比較",情報処理学会コンピュータセキュリティシンポジウム論文集 2011(CSS 2011), pp.540-545, 2011.

[287] 山本太郎,千葉直子,間形文彦,高橋克巳,関谷直也,中村功,小笠原盛浩,橋元良明,"ネットワークコミュニケーションに伴う不安調査結果について",情報処理学会 DICOMO シンポジウム 2010 論文集, pp.743-747, 2010.

[288] 山本太郎,千葉直子,間形文彦,高橋克巳,関谷直也,中村功,小笠原盛浩,橋元良明,"インターネット利用における不安に関する国際比較",情報処理学会コンピュータセキュリティシンポジウム論文集 2010(CSS 2010), pp.513-518, 2010.

[289] 関谷直也,橋元良明,小笠原盛浩,中村功,高橋克巳,間形文彦,山本太郎,千葉直子,"ネット・セキュリティにおける「不安」の国際比較",情報処理学会コンピュータセキュリティシンポ

ジウム論文集 2010(CSS 2010), pp.507-512, 2010.
[290] 橋元良明,中村功,関谷直也,小笠原盛浩,"インターネット利用に伴う被害と不安",東京大学大学院情報学環紀要 情報学研究・調査研究編 No.26, pp27-80(2010 年 4 月)
[291] 関谷直也,橋元良明,小笠原盛浩,中村功,高橋克巳,間形文彦,山本太郎,千葉直子,"ネット・セキュリティにおける不安の構造",情報処理学会コンピュータセキュリティシンポジウム論文集 2009(CSS 2009), pp.991-996,2009.
[292] 千葉直子,高橋克巳,"インターネット上の有害情報対策に関する利用者視点に基づく考察", 情報処理学会論文誌,Vol.51, No.9, pp.1702-1710, 2009.
[293] 日景奈津子,カールハウザー,村山優子,"情報セキュリティ技術に対する安心感の構造に関する統計的検討",情報処理学会論文誌, Vol.48, No.9, pp.3193-3203, 2007.
[294] 山岸 俊男, "信頼の構造-こころと社会の進化ゲーム", 東京大学出版会, 1998.

第6部 暗号技術

(1)暗号一般

[295] 森山 大輔, 西巻 陵, 岡本 龍明, "公開鍵暗号の数理 (シリーズ応用数理 2) ", 日本応用数理学会 (監修),共立出版, 2011.

[296] 伊豆 哲也, 佐藤 証, 田中 実, 花岡 悟一郎, 岩田 哲, "トコトンやさしい 暗号の本", 今井 秀樹 (監修), 日刊工業新聞社, 2010.

[297] Oded Goldreich, "Foundations of Cryptography: Volume 2, Basic Applications", Cambridge University Press, 2009.

[298] 結城 浩, "新版暗号技術入門 秘密の国のアリス", ソフトバンククリエイティブ; 2008.

[299] Marc Joye, and Gregory Neven (Eds.), "Identity-Based Cryptography", IOS Press, 2008.

[300] Oded Goldreich, "Foundations of Cryptography: Volume 1, Basic Tools", Cambridge University Press, 2007.

[301] 黒澤 馨, 尾形 わかは, "現代暗号の基礎数理（電子情報通信レクチャーシリーズ D-8）" 電子情報通信学会(編), コロナ社, 2004.

[302] 岡本 龍明,山本博資, "現代暗号（情報科学の数学シリーズ）", 産業図書, 1997.

(2)共通鍵

[303] NIST, "Secure Hash Standard (SHS)", Federal Information Processing Standards Publication, 180-4, 2012.

[304] Ted Krovetz, and Phillip Rogaway, "The Software Performance of Authenticated-Encryption Modes", 18th International Workshop on Fast Software Encryption(FSE 2011), LNCS, Vol. 6733, pp.306-327, 2011.

[305] Jian Guo, Thomas Peyrin, and Axel Poschmann, "The PHOTON Family of Lightweight Hash Functions", 31st annual conference on Advances in cryptology (CRYPTO 2011), LNCS, Vol. 6841, pp.222-239, 2011.

[306] Guido Bertoni, Joan Daemen, Michael Peeters, and Gilles Van Assche, "Keccak specifications --- Version 2", NIST submission, 2009.

[307] Tetsu Iwata, and Kan Yasuda:, "BTM:A Single-Key, Inverse-Cipher-Free Mode for Deterministic Authenticated Encryption", Selected Areas in Cryptography 2009, pp.313-330, 2009.

[308] Yu Sasaki, and Kazumaro Aoki, "Finding Preimages in Full MD5 Faster than Exhaustive Search", 28th Annual International Conference on Advances in Cryptology: the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2009), LNCS, Vol. 5479, pp.134-152, 2009.

[309] Florian Mendel, Christian Rechberger, Martin Schlaffer, and Soren Steffen Thomsen, "The Rebound Attack: Cryptanalysis of Reduced Whirlpool and Grostl," 16th International Workshop on Fast Software Encryption(FSE 2009), LNCS, Vol. 5665, pp.260-276, 2009.

[310] NIST, "The Keyed-Hash Message Authentication Code (HMAC) (Federal Information Processing Standards Publication 198-1)", 2008.

[311] Mihir Bellare, "New Proofs for NMAC and HMAC : Security Without Collision-Resistance", 26th annual international conference on Advances in Cryptology (CRYPTO 2006), LNCS, Vol. 4117, pp.602-619, 2006.

[312] Taizo Shirai, and Kyoji Shibutani, "On Feistel structures using a diffusion switching mechanism", 13th international conference on Fast Software Encryption (FSE 2006), LNCS, Vol. 4047, pp.41-56, 2006.

[313] Xiaoyun Wang, and Hongbo Yu, "How to Break MD5 and Other Hash Functions", 24th annual international conference on Theory and Applications of Cryptographic Techniques(EUROCRYPT 2005), LNCS, Vol. 3494, pp.19-35, 2005.

[314] John Kelsey, and Bruce Schneier, "Second Preimages on n-Bit Hash Functions for Much Less Than 2n Work", 24th annual international conference on Theory and Applications of Cryptographic Techniques(EUROCRYPT 2005), LNCS, Vol. 3494, pp.474-490, 2005.

[315] Antoine Joux, "Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions", 24th Annual International Cryptology Conference(CRYPTO 2004), LNCS, Vol. 3152, pp.306-316, 2004.

[316] Jongsung Kim, Seokhie Hong, Jaechul Sung, Changhoon Lee, and Sangjin Lee, "Impossible Differential Cryptanalysis for Block Cipher Structures", 4th International Conference on Cryptology in India(INDOCRYPT 2003), LNCS, Vol. 2904, pp.82-96, 2003.

[317] Kazumaro AOKI, Tetsuya ICHIKAWA, Masayuki KANDA, Mitsuru MATSUI, Shiho MORIAI, Junko NAKAJIMA, and Toshio TOKITA, "The 128-Bit Block Cipher Camellia", IEICE Transactions on Fundamentals, Vol.E85-A, No.1 pp.11-24, 2002.

[318] David Wagner, "A Generalized Birthday Problem", 22nd Annual International Cryptology Conference on Advances in Cryptology(CRYPTO 2002), LNCS, Vol. 2442, pp.288-303, 2002.

[319] NIST, "Specification for the ADVANCED ENCRYPTION STANDARD (AES) (Federal Information Processing Standards Publication 197)", 2001.

[320] NIST, "Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation", 2001.

[321] Eli Biham, Alex Biryukov, and Adi Shamir, "Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials", Workshop on the theory and application of cryptographic techniques on Advances in cryptology(EUROCRYPT '99), LNCS, Vol. 1592, pp.12-23, 1999.

[322] Mitsuru Matsui: "On a Structure of Block Ciphers with Provable Security against Differential and Linear Cryptanalysis", IEICE Transactions on Fundamentals, Vol.E82-A, No.1, pp.117-122, 1999.

[323] Eli Biham, "New Types of Cryptanalytic Attacks Using Related Keys", Journal of Cryptology, Vol.7, No.4, pp.229-246, 1998.

[324] Shiho Moriai, Takeshi Shimoyama, and Toshinobu Kaneko, "Higher Order Differential Attack of a CAST Cipher", 5th International Workshop on Fast Software Encryption(FSE '98), LNCS, Vol. 1372, pp.17-31, 1998.

[325] Kazumaro Aoki and Kunio Kobayashi and Shiho Moriai, "The Best Differential Characteristic Search of FEAL", IEICE Transactions on Fundamentals, Vol. E81-A, No.1, pp.98-104, 1998.

[326] Mitsuru Matsui: "New Block Encryption Algorithm MISTY," 5th ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE 1997), LNCS, Vol. 1267, pp.54-68, 1997.

[327] Joan Daemen, Lars Ramkilde Knudsen, and Vincent Rijmen, "The Block Cipher SQUARE", 4th International Workshop on Fast Software Encryption (FSE '97), LNCS, Vol.1267, pp.54-68, 1997.

[328] Kazumaro Aoki and Kazuo Ohta: "Strict Evaluation of the Maximum Average of Differential Probability and the Maximum Average of Linear Probability," IEICE Transactions on Fundamentals, Vol.E80-A, No.1, pp.2-8, 1997.

[329] Eli Biham, "A Fast New DES Implementation in Software", 5th ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE 1997), LNCS, Vol. 1267, pp.260-272, 1997.

[330] Mitsuru Matsui, "Linear Cryptanalysis Method for DES Cipher", '93 Workshop on the theory and application of cryptographic techniques on Advances in cryptology(EUROCRYPT '93), LNCS, Vol. 765, pp.386-397, 1993.

[331] Lars Ramkilde Knudsen, "Truncated and Higher Order Differentials", 2nd International Workshop on Fast Software Encryption(FSE '94), LNCS, Vol. 1008, pp.196-211, 1994.

[332] Florent Chabaud and Serge Vaudenay, "Links Between Differential and Linear Cryptanalysis", Workshop on the Theory and Application of Cryptographic Techniques(EUROCRYPT '94), LNCS, Vol. 950, pp.356-365, 1994.

[333] Eli Biham, and Adi Shamir, "Differential Cryptanalysis of the Data Encryption Standard", Springer, 1993.

[334] Kaisa Nyberg, "Differentially uniform mappings for cryptography", Workshop on the theory and application of cryptographic techniques on Advances in cryptology (EUROCRYPT '93), LNCS, Vol.765, pp.55-64, 1993.

[335] Michael Luby, and Charles Rackoff, "How to construct pseudorandom permutations from pseudorandom functions", Journal of Computing (Society for Industrial and Applied Mathematics), Vol.17, No.2, pp.373-386, 1988.

(3)公開鍵

[336] Agrawal Shweta, Boneh Dan, and Boyen Xavier, "Efficient Lattice (H)IBE in the Standard Model", Proc. 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2010), pp.553-572, 2010.

[337] Tatsuaki Okamoto and Katsuyuki Takashima, "Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption", Proc. 30th Annual International Cryptology Conference (CRYPTO2010), pp191-208, 2010.

[338] Cash David, Hofheinz Dennis, Kiltz Eike, and Peikert Chris, "Bonsai Trees, or How to Delegate a Lattice Basis",Proc. 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2010), pp.523-552, 2010.

[339] D.Hofheinz, and E.Kiltz, "Practical Chosen Ciphertext Secure Encryption from Factoring", Proc. 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2009), pp313-332, 2009.

[340] Rosen Alon, and Segev Gil, "Chosen-Ciphertext Security via Correlated Products", Proc. Theory of Cryptography, 6th Theory of Cryptography Conference (TCC 2009), pp.419-436, 2009.

[341] Brent Waters, "Dual System Encryption: Realizing Fully Secure IBE and HIBE under Simple Assumptions", Proc. 29th Annual International Cryptology Conference (CRYPTO 2009), pp.619-636, 2009.

[342] Y.Cui, E.Fujisaki, G.Hanaoka, H.Imai, and R.Zhang. "Formal security treatments for IBE-to-signature transformation: Relations among security notions", IEICE Transaction of Fundamentals of electronic Communications and Computer Science, Vol. E92-A1, 2009.

[343] Susan Hohenberger, and Brent Waters, "Short and Stateless Signatures from the RSA Assumption", Proc. 29th International Cryptology Conference (CRYPTO 2009), pp.654-670, 2009.

[344] Stehe Damien, Steinfeld Ron, Tanaka Keisuke, and Xagawa Keita, "Efficient Public

Key Encryption Based on Ideal Lattices", Proc. 15th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT2009), pp.617-635, 2009.

[345] D.Cash, E.Kiltz, and V.Shoup, "The Twin Diffie-Hellman Problem and Applications", Proc. 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2008), pp127-145, 2008.

[346] G.Hanaoka, and K.Kurosawa, "Efficient Chosen Ciphertext Secure Public Key Encryption under the Computational Diffie-Hellman Assumption", Proc. 14th Annual International Conference on the Theory and Application of Cryptology & Information Security (ASIACRYPT 2008), pp. 308-325, 2008.

[347] Peikert Chris, and Waters Brent, "Lossy Trapdoor Functions and Their Applications", Proc. 40th annual ACM symposium on Theory of computing (STOC 2008), pp.187-196, 2008.

[348] Gentry Craig, Peikert Chris, and Vaikuntanathan Vinod, "Trapdoors for Hard Lattices and New Cryptographic Constructions", Proc. 40th annual ACM symposium on Theory of computing (STOC 2008), pp.197-206, 2008.

[349] Abe Masayuki, Gennaro Rosario, and Kurosawa Kaoru, "Tag-KEM/DEM: A New Framework for Hybrid Encryption", Journal of Cryptology, Vol. 21, No. 1, pp.97-130, 2007.

[350] T.Kobayashi, and E. Fujisaki, "Security of ESIGN-PSS", IEICE Transaction of Fundamentals of electronic Communications and Computer Science Vol. E90-A7, pp.1395-1405, 2007.

[351] ISO/IEC, "Information technology -- Security techniques -- Encryption algorithms -- Part 2: Asymmetric ciphers", ISO/IEC 18033-2:2006, 2006.

[352] Regev Oded, "On lattices, learning with errors, random linear codes, and cryptography", Proc. 37th annual ACM symposium on Theory of computing (STOC '05), pp.84-93, 2005.

[353] B.Waters, "Efficient identity-based encryption without random oracles", Proc. 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2005), pp.114-127, 2005.

[354] Dan Boneh and Jonathan Katz, "Improved Efficiency for CCA-Secure Cryptosystems Built Using Identity-Based Encryption", Proc. Topics in Cryptology (CT-RSA 2005), pp87-103, 2005.

[355] Fujisaki Eiichiro, Okamoto Tatsuaki, Pointcheval David, and Stern Jacques, "RSA-OAEP Is Secure under the RSA Assumption", Journal of Cryptology, Vol. 17, No. 2, pp.81-104, 2004.

[356] R.Cramer, V.Shoup, "Design and Analysis of Practical Public-Key Encryption Schemes Secure Against Adaptive Chosen Ciphertext Attack", SIAM Journal of Computing, Vol.33, No. 1, pp.167-226, 2004

[357] K.Kurosawa, and Y.Desmedt, "A New Papradigm of Hybrid Encryption Scheme", Proc. 24rd Annual International Cryptology Conference (CRYPTO 2004), pp 426-442, 2004.

[358] D.Boneh, and X.Boyen, "Secure identity based encryption without random oracles", Proc. 24th Annual International Cryptology Conference (CRYPTO 2004), pp.443-459, 2004.

[359] R.Canetti, S.Halevi, and J.Katz, "Chosen-ciphertext security from identity based encryption", Proc. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2004), pp.207-222, 2004

[360] D.Boneh, and X.Boyen, "Short signatures without random oracles", Proc. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2004), pp.56-73, 2004.

[361] R.Cramer, and V.Shoup, "Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption", Proc. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2002), pp45-64, 2002.

[362] D.Boneh, and M.Franklin., "Identity-based encryption from Weil paring", Proc. International Cryptology Conference (CRYPTO 2001), pp.213-229, 2001.

[363] Dan Boneh, Ben Lynn, and Hovav Shacham, "Short signatures from the Weil pairing",Proc. 7th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2001), pp.514-532. 2001.

[364] D.Dolev, C.Dwork, and M.Naor, "Non-malleable cryptography", SIAM Journal on Computing, Vol. 30, No. 2, pp391-437, 2000.

[365] R.Sakai, K.Ohgishi, and K.Kasahara, "Cryptosystems on Pairing", 暗号と情報セキュリティシンポジウム(SCIS 2000)予稿集, C20, 2000.

[366] Ronald Cramer and Victor Shoup, "Signature schemes based on the strong RSA assumption", ACM Transactions on Information and System Security (TISSEC), Vol.3 No.3, pp.161-185, 2000.

[367] E.Fujisaki, and T. Okamoto, "Secure integration of asymmetric and symmetric encryption schemes", Proc. 19th Annual International Cryptology Conference on Advances in Cryptology(CRYPTO '99), pp537-554, 1999.

[368] M.Abe, and T.Okamoto, "A signature scheme with message recovery as secure as discrete logarithm", Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT '99), pp.378-389, 1999.

[369] M.Bellare, A.Desai, D.Pointcheval, and P.Rogaway, "Relations among notions of security for public-key encryption schemes", 18th Annual International Cryptology Conference (CRYPTO '98), LNCS 1462, pp.26-45. 1998.

[370] M. Ajtai, and C. Dwork, "The First and Fourth Public-Key Cryptosystems with Worst-Case/Average-Case Equivalence", Proc. 29th annual ACM symposium on Theory of computing (STOC '97), pp.284-293, 1997.

[371] O.Goldreich, S.Goldwasser, and S.Halevi, "Public-key cryptosystems from lattice reduction problems", Proc. 17th Annual International Cryptology Conference (CRYPTO '97), pp.112-131, 1997.

[372] M.Bellare, and P.Rogaway, "The exact security of digital signatures -- how to sign with RSA and Rabin", Proc. International Conference on the Theory and Application of Cryptographic Techniques Saragossa (EUROCRYPT '96), pp.399-416, 1996.

[373] D.Pointcheval, and J.Stern. "Security proofs for signature schemes", Proc. 15th annual international conference on Theory and application of cryptographic techniques (EUROCRYPT '96), pp.387-398, 1996.

[374] M.Bellare, and P.Rogaway, "Optimal asymmetric encryption", Workshop on the Theory and Application of Cryptographic Techniques (EUROCRYPT '94), LNCS, Vol. 950, pp.92-111, 1995.

[375] M.Bellare, and P.Rogaway, "Random oracles are practical: a paradigm for designing efficient protocols",Proc. 1st ACM Computer and Communications Security Conference (CCS '93), pp.62-73. 1993.

[376] CP. Schnorr, "Efficient signature generation for smart cards", Journal of Cryptology, Vol. 4, pp.161-174, 1991.

[377] M.Naor, and M.Yung, "Public-key cryptosystems provably secure against chosen ciphertext attacks", Proc. twenty-second annual ACM symposium on Theory of computing (STOC '90), pp.427-437, 1990.

[378] T.Okamoto, and A.Shiraishi, "A fast signature scheme based on quadratic inequalities", 1985 Symposium on Security and privacy (SSP '85), pp.123-133, 1990.

[379] S.Goldwasser, S.Micali, and R.Rivest, "A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks", SIAM Journal of Computing, Vol. 17, No.2, pp.281-308, 1988.

[380] 岡本龍明, "単一公開情報による複数利用者の認証方式", 電子情報通信学会論文誌, Vol. J69-D, No. 10, pp.1481-1489, 1986.

[381] A.Fiat, and A.Shamir, "How to prove yourself: Practical solutions to identification and signature problems", Proc. Advances in cryptology (CRYPTO '86), pp.186-194, 1986.

[382] ElGamal, Taher., "A Public Key Cryptosystem and a Signature Scheme Based on

Discrete Logarithms", IEEE Transaction on Information Theory, Vol. 31, No. 4, pp.469-472, 1985.

[383] A.Shamir, "Identity-based cryptosystems and signature schemes", Proc. CRYPTO 84 on Advances in cryptology, pp.47-53, 1985.

[384] S.Goldwasser, and S.Micali, "Probabilistic encryption", Journal of Comp. and Sys. Sci., Vol. 28, pp. 270-299, 1984.

[385] M. O. Rabin, "Digitalized Signatures and Public-Key Functions as Intractable as Factorization", Technical Report, MIT/LCS/TR-212, MIT, 1979.

[386] Leslie Lamport, "Constructing digital signatures from one-way functions", Technical Report SRI-CSL-98, SRI International Computer Science Laboratory, 1979.

[387] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, Vol. 21, No. 2, pp.120-126, 1978.

[388] Diffie W. and Hellman M. E., "New Directions in Cryptography", IEEE Transactions on Information Theory, Vol. 22, pp. 644-654, 1976.

(4)暗号応用

[389] M. Joye, and M. Tunstall, "Fault Analysis in Cryptography (Information Security and Cryptography)", Springer, 2012.

[390] S. Skorobogatov, and C. Woods, "Breakthrough silicon scanning discovers backdoor in military chip", 14th International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2012), LNCS, Vol. 7428, pp. 23-40, 2012.

[391] Atsushi Fujioka, and Koutarou Suzuki, "Designing Efficient Authenticated Key Exchange Resilient to Leakage of Ephemeral Secret Keys", Proc. The Cryptographers' Track at the RSA Conference 2011(CT-RSA 2011), pp.121-141,2011.

[392] B. B. Brumley, and N. Tuveri, "Remote Timing Attacks are Still Practical", The European Symposium on Research in Computer Security (ESORICS'11), LNCS, Vol. 6879, pp.355-371, 2011.

[393] Atsushi Fujioka, Koutarou Suzuki, and Berkant Ustaoglu: "Ephemeral Key Leakage Resilient and Efficient ID-AKEs That Can Share Identities", Proc. 4th International Conference on Pairing-Based Cryptography (Pairing 2010), pp.187-205, 2010.

[394] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds", Proc. the 16th ACM conference on Computer and communications security (CCS 2009), pp. 199-212, 2009.

[395] S. Mangard, E. Oswald, and T. Popp, "Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security)", Springer, 2007.

[396] J. Ambrose, A. Ignjatovic, and S. Parameswaran, "Power Analysis Side Channel Attacks", VDM Verlag Dr. Muller, Saarbrucken, 2007.

[397] Fumitaka Hoshino, Tetsutaro Kobayashi, and Kazumaro Aoki: "Compressed Jacobian Coordinates for OEF", Proc. 1st International Conferenceon Cryptology in Vietnam (VIETCRYPT 2006), pp.147-156, 2006.

[398] 神永正博, "カードセキュリティのすべて", 日本実業出版社, 2006.

[399] N. Nedjah, and L. D. M. Mourelle, "Embedded Cryptographic Hardware: Design & Security", Nova Science Publishers, 2006.

[400] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan, "The Sorcerer's Apprentice Guide to Fault Attacks", Proc. IEEE, vol. 94, No. 2, pp. 370-382, Feb. 2006.

[401] D. A. Osvik, A. Shamir, and E. Tromer, "Cache Attacks and Countermeasures: the Case of AES", The Cryptographers' Track at RSA Conference (CT-RSA '06), LNCS, Vol. 3860, pp.1-20, 2006.

[402] 神永正博, 渡邊高志, "情報セキュリティの理論と技術　（暗号理論からＩＣカードの耐タンパ技術まで）", 森北出版社, 2005.

[403] N. Nedjah, and L. D. M. Mourelle," Embedded Cryptographic Hardware: Methodologies and Architectures", Nova Science Publishers, 2004.

[404] S. Chari, J. R. Raom, and P. Rohatgi, "Template Attacks", 4th International Workshop on Cryptographic Hardware and Embedded Systems(CHES 2002), LNCS, Vol. 2523, pp.13-28, 2003.

[405] G. Piret, and J. J. Quisquater, "A differential fault attack technique against SPN structures, with application to the AES and KHAZAD", 5th International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2003), LNCS, Vol. 2779, pp.77-88, 2003.

[406] S. P. Skorobogatov and R. J. Anderson, "Optical Fault Induction Attacks", 4th International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2002), LNCS, Vol. 2523, pp.31-48, 2003.

[407] C. Aumuller, P. Bier, W. Fischer, P. Hofreiter and J.-P. Seifert, "Fault Attacks on RSA with CRT: Concrete Results and Practical Countermeasures", 4th Intenational Workshop on Cryptographic Hardware and Embedded Systems (CHES 2002), LNCS, Vol. 2523, pp.81-95, 2003.

[408] J. Blomer, and J.-P. Seifert, "Fault Based Cryptanalysis of the Advanced Encryption Standard (AES)", 7th International Conference on Financial Cryptography (FC 2003), LNCS, Vol. 2742, pp.162-181, 2003.

[409] Y. Tsunoo, T. Saito, T. Suzaki, M. Shigeri, and H. Miyauchi, "Cryptanalysis of DES Implemented on Computers with Cache", 5th International Workshop on

Cryptographic Hardware and Embedded Systems (CHES 2003), LNCS, Vol. 2779, pp.62-76, 2003.

[410] D. Brumley, and D. Boneh, "Remote Timing Attacks are Practical", Proc. 12th conference on USENIX Security Symposium (SSYM'03), vol. 12, pp.1-1, 2003.

[411] Masayuki Abe, and Koutarou Suzuki, "M+1-st Price Auction Using Homomorphic Encryption", Proc. 5th International Workshop on Practice and Theory Public Key Cryptography (PKC 2002), pp.115-124, 2002.

[412] L. Goubin, "Refined Power-Analysis Attack on Elliptic Curve Cryptosystems", 6th International Workshop on Theory and Practice in Public Key Cryptography (PKC 2003), LNCS, Vol. 2567, pp.199-210, 2002.

[413] Masayuki Abe, and Fumitaka Hoshino, "Remarks on Mix-Network Based on Permutation Networks", Proc. 4th International Workshop on Practice and Theory in Public Key Cryptography (PKC 2001), pp.317-324, 2001.

[414] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: concrete results", 3rd International Workshop on Cryptographic Hardware and Embedded Systems (CHES2001), LNCS, Vol. 2162, pp.251-261, 2001.

[415] D. Boneh, R. DeMillo, and R. Lipton, "On the importance of checking cryptographic protocols for faults, " Journal of Cryptology, Vol. 14, No. 2, pp. 101-119, 2001.

[416] T. S. Messerges, "Using Second-Order Power Analysis to Attack DPA Resistant Software," 2nd International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2000), LNCS, Vol. 1965, pp. 238-251, 2000.

[417] J. S. Coron, and Louis Goubin, "On Boolean and Arithmetic Masking against Differential Power Analysis", 2nd International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2000), LNCS, Vol. 1965, pp. 1-14, 2000.

[418] J.-J. Quisquater, and D. Samyde, "ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards", International Conference on Research in Smart Cards: Smart Card Programming and Security (E-SMART2000), LNCS, Vol. 2140, pp.200-210, 2000.

[419] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis", 19th Annual International Cryptology Conference(CRYPTO '99), LNCS, Vol. 1666, pp. 388-397, 1999.

[420] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Power analysis attacks of modular exponentiation in smartcards", 1st International Workshop on Cryptographic Hardware and Embedded Systems (CHES 1999), LNCS, Vol. 171, pp.144-157, 1999.

[421] J. S. Coron, "Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems", 1st International Workshop on Cryptographic Hardware and

Embedded Systems (CHES 1999), LNCS, Vol. 1717, pp.292-302, 1999.

[422] E. Biham, and A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems", 17th Annual International Cryptology Conference (CRYPT0 '97), LNCS, Vol. 1294, pp.513-525, 1997.

[423] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, and Kenneth H. Rosen, "Handbook of Applied Cryptography (Discrete Mathematics and Its Applications) ", CRC Press, 1996.

[424] P. C. Kocher, "Timing Attacks on Implementations of Die-Hellman, RSA, DSS, and Other Systems", 17th Annual International Cryptology Conference, Asvanced in Cryptology (CRYPTO '96), LMCS, Vol. 1109, pp.104-113, 1996.

[425] Tony Eng, and Tatsuaki Okamoto, "Single-Term Divisible Electronic Coins", Proc. Workshop on the Theory and Application of Cryptographic Techniques (EUROCRYPT '94), pp.306-319, 1994.

[426] Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta, "A Practical Secret Voting Scheme for Large Scale Elections", Proc. Workshop on the Theory and Application of Cryptographic Techniques (AUSCRYPT '92), pp.244-251, 1992.

[427] Tatsuaki Okamoto, and Kazuo Ohta, "Universal Electronic Cash", Proc. 11th Annual International Cryptology Conference (CRYPTO 1991), pp.324-337, 1991.

(5)プライバシ保護

[428] 五十嵐大, 千田浩司, 高橋克巳, "数値属性における, k-匿名性を満たすランダム化手法", コンピュータセキュリティシンポジウム 2011(CSS2011)予稿集, 2D3-4, 2011.

[429] 千田浩司, 五十嵐大, 濱田浩気, 高橋克巳, "エラー検出可能な軽量 3 パーティ秘匿関数計算の提案と実装評価", 情報処理学会論文誌, Vol.52, No.9, pp.2674-2685, 2011.

[430] 五十嵐大, 濱田浩気, 千田浩司, 高橋克巳, "軽量検証可能 3 パーティ秘匿関数計算の効率化及びこれを用いたセキュアなデータベース処理", 2011 年暗号と情報セキュリティシンポジウム(SCIS2011)予稿集 2C3-6, 2011.

[431] 濱田浩気, 五十嵐大, 千田浩司, 高橋克巳, "秘匿関数計算上の線形時間ソート", 2011 年暗号と情報セキュリティシンポジウム(SCIS2011)予稿集, 2C3-5, 2011.

[432] Raymond C.-W. Wong, and Ada W.-C. Fu, "Privacy-Preserving Data Publishing - An Overview", Morgan&Claypool Publishers, 2010.

[433] Benjamin C.M. Fung, Ke Wang, Ada W.-C. Fu, and Philip S. Yu, "Introduction to Privacy-Preserving Data Publishing - Concepts and Techniques", CRC Press, 2010.

[434] 佐久間淳, 小林重信, "プライバシ保護データマイニング", 人工知能学会誌, Vol.24, No.2, pp.283-293, 2009.

[435] 五十嵐大, 千田浩司, 高橋克巳, "k-匿名性の確率的指標への拡張とその適用例", コンピュ

ータセキュリティシンポジウム 2009(CSS2009)予稿集, E7-4, 2009.

[436] Charu C. Aggarwal, and Philip S. Yu, "Privacy-Preserving Data Mining: Models and Algorithms", Springer, 2008.

[437] Cynthia Dwork, "Differential Privacy: A Survey of Results", Theory and Applications of Computation, 5th International Conference (TAMC 2008), LNCS, Vol. 4978, pp.1-19, 2008.

[438] Ashwin Machanavajjhala, Daniel Kifer, Johannes Gehrke, and Muthuramakrishnan Venkitasubramaniam, "L-diversity: Privacy beyond k-anonymity", ACM Transactions on Knowledge Discovery from Data, Vol.1, No.1, 2007.

[439] Ninghui Li, Tiancheng Li, and Suresh Venkatasubramanian, "t-Closeness: Privacy beyond k-anonymity and l-diversity", Proc. IEEE 23rd International Conference on Data Engineering (ICDE 2007), pp.106-115, 2007.

[440] Jaideep Vaidya, Christopher W. Clifton, and Yu M. Zhu, "Privacy Preserving Data Mining", Springer, 2006.

[441] Rakesh Agrawal, Ramakrishnan Srikant, and Dilys Thomas, "Privacy Preserving OLAP", Proc. ACM International Conference on Management of Data (SIGMOD 2005), pp.251-262, 2005.

[442] Murat Kantarcioglu, and Chris Clifton, "Privacy-Preserving Distributed Mining of Association Rules on Horizontally Partitioned Data", IEEE Transactions on Knowledge and Data Engineering, Vol.16, No.9, pp.1026-1037, 2004.

[443] Michael J. Freedman, Kobbi Nissim, and Benny Pinkas, "Efficient Private Matching and Set Intersection", International Conference on the Theory and Applications of Cryptographic Techniques(EUROCRYPT 2004), LNCS, Vol. 3027, pp.1-19, 2004.

[444] Berry Schoenmakers, and Pim Tuyls, "Practical Two-Party Computation Based on the Conditional Gate", 10th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2004), LNCS, Vol. 3329, pp.119-136, 2004.

[445] Rakesh Agrawal, Alexandre V. Evfimievski, and Ramakrishnan Srikant, "Information Sharing Across Private Databases", Proc. ACM International Conference on Management of Data (SIGMOD 2003), pp.86-97, 2003.

[446] Latanya Sweeney, "k-Anonymity: A Model for Protecting Privacy", International Journal of Uncertainty, Fuzziness and Knowledge-based Systems, Vol.10, No.5, pp.557-570, 2002.

[447] Benny Pinkas, "Cryptographic Techniques for Privacy-Preserving Data Mining", ACM Special Interest Group on Knowledge Discovery and Data Mining (SIGKDD) Explorations, Vol.4, No.2, pp.12-19, 2002.

[448] Chris Clifton, Murat Kantarcioglou, Jaideep Vaidya, Xiaodong Lin, and Michael Y. Zhu, "Tools for Privacy Preserving Data Mining", ACM Special Interest Group on Knowledge Discovery and Data Mining (SIGKDD) Explorations, Vol.4, No.2, pp.28-34, 2002.

[449] Ronald Cramer, Ivan Damgard, and Jesper B. Nielsen, "Multiparty Computation from Threshold Homomorphic Encryption", International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2001), LNCS, Vol. 2045, pp.280-299, 2001.

[450] Pat Doyle, Julia I. Lane, Jules J.M. Theeuwes, and Laura V. Zayatz, "Confidentiality, Disclosure, and Data Access - Theory and Practical Applications for Statistical Agencies", ELSEVIER, 2001.

[451] Rakesh Agrawal, and Ramakrishnan Srikant, "Privacy-Preserving Data Mining", Proc. ACM International Conference on Management of Data (SIGMOD 2000), pp.439-450, 2000.

[452] Yahuda Lindell and Benny Pinkas, "Privacy Preserving Data Mining", Proc. 20th Annual International Cryptology Conference (CRYPTO 2000), LNCS, Vol. 1880, pp.36-54, 2000.

[453] Jose M. Gouweleeuw, Peter Kooiman, Leon C.R.J. Willenborg, and Peter-Paul de Wolf, "Post Randomisation for Statistical Disclosure Control: Theory and Implementation", Journal of Official Statistics, Vol.14, No.4, pp.463-478, 1998.

[454] Hugo Krawczyk, "Secret Sharing Made Short", 13th Annual International Cryptology Conference (CRYPTO '93), LNCS, Vol. 773, pp.136-146, 1994.

[455] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson, "Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation (Extended Abstract)", Proc. 20th Annual ACM Symposium on Theory of Computing (STOC '88), pp.1-10, 1988.

[456] David Chaum, Claude Crepeau, and Ivan Damgard, "Multiparty Unconditionally Secure Protocols", Proc. 20th Annual ACM Symposium on Theory of Computing (STOC '88), pp.11-19, 1988.

[457] Oded Goldreich, Silvio Micali, and Avi Wigderson, "How to Play any Mental Game or A Completeness Theorem for Protocols with Honest Majority", Proc. 19th Annual ACM Symposium on Theory of Computing (STOC '87), pp.218-229, 1987.

[458] Andrew C.-C. Yao, "How to Generate and Exchange Secrets (Extended Abstract)", Proc. IEEE 27th Annual Symposium on Foundations of Computer Science (FOCS '86), pp.162-167, 1986.

[459] Adi Shamir, "How to Share a Secret", Communications of the ACM, Vol.22, No.11,

pp.612-613, 1979.

[460] George R. Blakley, "Safeguarding cryptographic keys", Proc. 1979 AFIPS National Computer Conference, pp.313-317, 1979.