科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　　９　日現在

機関番号：　１７１０２
研究種目：　基盤研究(B)
研究期間：　2011～2013
課題番号：　２３３０００２７

研究課題名（和文）サイバーシステムにおける内部攻撃脅威に対する評価指標確立と体系的対策研究

研究課題名（英文）A study on evaluating Insider Threats and fighting against Insider attacks in Cyber Systems

研究代表者
櫻井　幸一（Sakurai, Kouichi）

九州大学・システム情報科学研究科（研究院・教授

研究者番号：６０２６４０６６

交付決定額（研究期間全体）：（直接経費）　　9,400,000円、（間接経費）　　2,820,000円

研究成果の概要（和文）：システムへの攻撃は外部からだけではない。システムを管理・運用する側の不正や、システム内部構成員からの情報漏洩は、その影響を考えると深刻な問題となる。政府系ネットワークや金融関係の内部脅威に関する研究報告は公開されている。しかしソーシャルネットやクラウドサービスにおけるシステムの内外の範囲が多様化し、内部脅威の解析・信頼性評価が複雑化している。本研究では、内部攻撃のモデル化と分類を行い、既存対策の限界を明らかし、ソーシャルエンジニアリング手法導入も含めた新たな対策を提案した。

研究成果の概要（英文）：In cyber systems, we never assume attackers to come from outside. We shall consider serious threats by a system manager and the information leakage via some insiders. We have some published research reports about insider threats on Government networks or banking systems, whereas we do not know so much about insider attacks in recent new cyber systems including social networking or cloud computing services. This research investigates how to modeling insider attacks in cyber security and classify the type of attacks. Also we discuss the limitation of out known protection, and consider new ways of fighting against such insider attacks.

研究分野：　総合領域

科研費の分科・細目：　情報学・計算機システム・ネットワーク

キーワード：　内部脅威　情報漏洩対策　安全性評価　暗号・認証　システムセキュリティ

１．研究開始当初の背景: システム内部からの攻撃は、予測困難でありその影響も深刻であることは 1980 年代から認識されていた。2000 年代には、金融系サービスにおける内部脅威に関する報告書がまとめられ[Insider Threat Study, CERT/US-secret service, 2004]、また内部脅威の定義を試みる論文も登場してきた[Bishop, Gates, Defining Insider threat, 2008]。2008 年には、Bishop や Gollmann など欧米の著名なコンピュータセキュリティ研究者が、伝統ある Dagstuhl セミナーで“内部脅威対策”(http://www.dagstuhl.de/08302)を討議し、2010 年夏には引き続き Dagstuh セミナー”内部脅威：回避・緩和・対応戦略”http://www.dagstuhl.de/10341)を開催している。さらに内部攻撃脅威に特化した国際会議 International Workshop on Managing Insider Security Threats (2009), 1st ACM CCS workshop Insider Threat 2010 が発足し、学術論文誌 Security and Communication Networks の 2010 年特集“Defending Against Insider Threats and Internal Data Leakage”などが企画され、欧米を中心に急速に学術研究グループが形成されつつある。

モバイルアドホックネット(Mobile Ad-hoc Network, MANET)では、参加者がグループでネットワークを構成するため、一部の参加者による内部攻撃を常に意識する必要がある。すでにこの意識のもとでの事例研究はある [Boppona, Su, Secure Routing Techniques to Mitigate Insider Attacks in Wireless Ad Hoc Networks, IEEE Wireless Hive workshop 2007] が、未だ整理体系化された議論には至っていない。

かたや暗号理論では、従来の外部攻撃モデルの拡張として内部攻撃者が導入され、既存の提案システムのいくつかでは内部脅威に対して脆弱であることが示され、改良方式の設計が試みられはじめている(IACR Eprint2009/291 By Gorantla, Boyd and Gonzalez Nieto)。現在急速に普及したソーシャルネットワークは、参加者のだれもが内部攻撃可能な環境であり、またクラウドサービスでは、内部構造が従来システムに比べると曖昧になってきている。

２．研究の目的: 本研究では、ネットワークシステムにおける内部攻撃のモデル化・分類・対策・限界を明らかにする。

(a) 内部攻撃と脅威の分類
(b) モデル化と安全性の定義
(c) 対策とその限界

ただし、サイバーシステム全体では、本基盤研究の範囲としては広すぎるため、まず研究代表者の研究グループで、これまで、あるいは現在取り組んでいるセキュリティシステムに限定した中での内部脅威に焦点を当てる。具体的には

[対象 1] 電子現金システムをはじめとする暗号プトロトコル
[対象 2] ゲーム理論を用いたモバイルアドホックネットワーク性能評価
[対象 3] アクセス制御に基づくネットワーク不正検知
[対象 4] 正当な構成員が強要された場合の内部攻撃に対するソーシャルエンジニアリング的対策

の４つを取り上げ，課題(a)～(c)を検討する。

３．研究の方法: 暗号・ネットワーク・コンピュータセキュリティの各専門家により混合研究グループを構成し、本課題に取り組む。方法は（3a）これまで研究構成員が設計した暗号プロトコルやセキュアシステムを初めとして、既存のシステムにおける内部脅威と耐性を調べた。（3b）内部攻撃に対して脆弱な場合は対策を検討した。また、その対策が実装可能な技術であるのか検討する。可能な場合には、実験システムの構築を行なう。（3c）内部攻撃に対しても耐性があると思われる場合には、攻撃モデルの拡張と証明を検討した。研究組織は次のとおり：

A （暗号理論班）: 安全性評価・基本対策設計、およびその理論的解析--- 西出（九大[2013 年４月より筑波大]）・櫻井（九大）
B （ネットワーク班）: 対策技術の設計とプトロトタイプシステム実装 ---- 堀（九大[2013 年４月より佐賀大]）・You(海外共同研究者)
C （コンピュータシステム班）: システム設計・ネットワーク実装実験評価 --- 高橋（九州先端研[2011 年１月より鳥取大]）・西出（九大）
D 海外研究協力者

I.S.You(韓国バイブル大学):内部攻撃脅威に特化した国際会議 International Workshop on Managing Insider Security Threats (MIST2009)を立ち上げ、Security and Communication Networks 2010 ジャーナル特集“Defending Against Insider Threats and Internal Data Leakage”を企画した。Prof. You とは国際会議 MIST の開催を含めて、この方面の活性化に連携した。

D.Gollmann（ハンブルグ工科大学）:コンピュータセキュリティの第一人者の一人。欧州地区では ESORICS を初めとする国際会議を数多くホストしてきた。2008 年に開催されたには、Dagstuhl セミナー“内部脅威への対策“の主催者の一人。本研究でも、外部アドバイサーとして本研究遂行に関して助言をもらった。

４．研究成果

(1)暗号プロトコル ①研究代表者の提案した分類と評価手法[宮崎 真悟，櫻井 幸一，オフライン型電子現金システムの分類と管理機関の内部不正に対する安全性評価,情報処理学会論文誌,1999.03]を、それ以降この１０年間に設計された電子現金システムに適用し、内部脅威の観点から安全性を解析した [Nishide, Miyazaki, Sakurai, Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications (JoWUA), Vol. 3, No. 1/2, 2012, pp.55-71] ② 計算能力の高い銀行の内部不正者による、一般利用者の署名偽造に対し、利用者がそれが偽造であることを立証可能な署名方式を提案した [北島暢曜，矢内直人，西出隆志，岸本渡，花岡悟一郎，岡本栄司，Symposium on Information Theory(SITA)，11 月，201] ③

認証サーバ側の内部不正者によるパスワード盗難への対策としてサーバ側を複数分散化し、パスワードを秘匿したまま認証する方式を提案した。[小林佑行，矢内直人，西出隆志，花岡悟一郎，岡本栄司，暗号と情報セキュリティシンポジウム(SCIS) 1月，2014.]

(2)ゲーム論的セキュリティ評価

ゲーム論的手法を用いてのセキュリティ評価を内部脅威に適用した。研究代表者のグループはネットワーク経済やセキュリティ経済に取り組んできた。その中でモバイルアドホックネットワーク(MANET)における内部攻撃者を細分化し、既存の３種{正規者、不正者、自己的}に加えて、新たに”懐疑的”内部者を導入し、ネットワークプロトコルの解析を理論的に行なった。

MANET では、参加者がネットワークを構成するため、基本的には全員がシステム内部に含まることに注意する。しかし、他のシステムでも、内部と外部脅威の区別に加えて、それぞれにも、異なるレベルの不正が考えられ、上記研究と同様のアプローチが適用可能となることを、いくつかのネットワークゲームにおいて明らかにした。[Hao, Adhikari, Sakurai, INTRUST 2011: 239-257][Hao, Sakurai, AINA 2012: 495-502]

(3)ネットワークにおける内部攻撃対策

ネットワークにおける内部攻撃対策として、利用者の挙動により生成されるトラヒックをモニタリングし通常の挙動と大きく異なる挙動を示した際に、内部攻撃の兆候としてアラームを生成するシステムについて考案した。さらに、アプリケーションの挙動を解析するためにはネットワーク層で得られる情報に加え、より上位の層との連携機構が重要であることを指摘した。

ネットワークにおけるインサイダー脅威対策のためには、情報資源にアクセスするユーザ（信頼されているアクセス者）がどのようにアクセスしようとしているかの振舞いに関する情報を通信チャネル上で伝送される情報を用いてモニタ記録し、それを分析することで、アクセスが正常に行われているか不正に行われているかを判定する必要がある。もし、振舞に異常が見られた場合は、アラームを上げることにより、不正検知にかかる工数を減少させることができる。図１は、インサイダー脅威に対応するための枠組みである。

内部脅威解析者は、情報資源へのアクセス状況を蓄積しログ収集に努めるとともに、逐次異常がないか解析を行う。解析の結果、異常が判別された場合には、それがポリシに反していないか比較注意する。このような異常検知を用いてもインサイダー脅威対策を行うことができる。

過去のアクセス等の履歴情報を含むアクセス情報から、通常業務とは異なる振舞を検知する機構を実現することでインサイダー脅威に対抗することができる。そのために、機械学習分野において研究がすすめられている異常検知技術を導入し、アクセス者の挙動に関してそのモデル化ならびに異常検出を実施することが重要である。時間の変化に伴いネットワークを介してアクセスを行う利用者の挙動を、一連の挙動としてモデル化することで、ネットワークを用いた異常アクセスを検出する手法を導入する。情報資源のアクセス主体からのネットワークを介した情報システムへのアクセスを学習により正常を示すルールおよび異常を示すルールとして、ルール生成を行う。生成されたルールとの対比により異常アクセスを検知する。

本研究では、インサイダー脅威とその対策について議論を行った。インサイダー脅威は、権限を有するものの裏切りなど、内部と外部を区別する境界が存在しないことから、情報セキュリティ対策として従来から行われてきた境界におけるアクセス制御は、そのポイントが明確でなくなるため困難となる。インサイダー脅威検知のため、異常検知手法をインサイダー脅威のモデルに適用し、通常業務とは異なる振舞を機械的に評価する手法を考案した。特に、ネットワークサービスへのアクセス状況をモニタし、異常なアクセスを数理的手法により評価する。検知されたインサイダー脅威を防止するために、脅威から情報資源を守るためのアクセス制御機構を動的に生成し、配置する必要があることを示した。[堀良彰，西出隆志，櫻井幸一，暗号と情報セキュリティシンポジウム (SCIS)，1月，2011][Yoshiaki Hori, Takashi Nishide, Kouichi Sakurai, Proc. of the Third International Conference on Intelligent Networking and Collaborative Systems (INCoS 2011), pp. 634-636, 11月, 2011]

個人情報漏洩の原因の約 7 割は内部者の管理ミス、誤操作、持ち出しなどによって発生している（日本ネットワークセキュリティ協会， 2012 年情報セキュリティインシデントに関する調査報告書 ver 1.1.）。また、これらの行為は、内部者に行われるため、ログを改ざんするなどしてこれらの行為を隠ぺい可能という問題がある。そこで、オペレーティングシステムのカーネルレベルで機密情報の漏洩経路を追跡することで、ログの改ざんを困難としつつ、その漏洩原因のマシンを特定する仕組みを実現した。

このことを実現するために以下の課題について取り組んだ。

[課題 1] 機密情報かそうでないかの区別：プロセスは設定ファイルなどさまざまなファイルを読み込んでいるため、すべてのファイルの拡散を追跡することは難しい。このため、読み込んだファイルが機密情報であるか否かを判断する必要がある。

[課題 2] 書き出す情報が機密情報であるかの判断：ファイルやプロセスに情報を書き出す際に、書き出す情報が機密情報であった場合、書き出したファイルなどに機密情報が拡散する。プロセスが過去に機密情報を読み込んでいる場合は、書き出された情報も機密情報である可能性がある。そのため、プロセスが情報を書き出す際に、プロセスが過去に機密情報を読み込んでいるか判断することが必要となる。

[課題 3] プロセス間通信で受信した情報が機密情報であるかの判断：プロセス間通信

(ソケット通信)の際に受信した情報が機密情報であるかの判断である。受信した情報が機密情報である場合は、書き出されたファイルも機密情報として扱わなければ情報漏洩につながる可能性がある。しかし、受信側では受信した情報が機密情報であるかどうか分からない。そこで、受信した情報が機密情報であるか判断するためには、送信側からのなんらかの知らせが必要である。送信側から送信した情報が機密情報であることを知らせる通知をどのように実現するかがプロセス間通信(ソケット通信)による課題となる。

[課題 4] 共有メモリに格納されている情報が機密情報であるかの判断:共有メモリにより情報を共有した場合、共有メモリに格納されている情報が機密情報であるかの判断である。共有メモリは他のプロセスから共有され、通常のメモリ操作と同様に扱える。このため、共有メモリに読み書きされるタイミングや読み書きされた情報を取得することは難しい。

そこで、これらの課題を解決したシステムを、Linux カーネル 3.9.6 上で実装した。拡散の対象は、ファイル操作と子プロセスの生成およびソケット通信、共有メモリとした。

計算機を 2 台用意し、2台の計算機間でファイル操作とソケット通信による機密情報の拡散追跡を確認した結果、機密情報の拡散が追跡できていることが確認できた。また、読み込みと書き込みの情報を比較しない場合と比較する場合で追跡対象が削減できるか検証するために、密情報をアプリケーションで開き、機密情報の内容を新規ファイルにコピーする。データ保存後、追跡対象となっている数を比較した。結果、追跡対象ファイル数が減少できていることが確認できた。しかし、機密情報が編集され、バイト数や先頭 10 バイトが変わってしまった場合には、書き出す情報が機密情報でないと判断され、追跡ができないため、これに対する対策は今後の課題である。[前田明彦, 高橋健一, 川村尚生, 菅原一孔, 電気・情報関連学会中国支部第 63 回連合大会講演論文集, pp. 427-428, 2012][前田明彦, 高橋健一, 川村尚生, 菅原一孔, 第 14 回 IEEE 広島支部学生シンポジウム CDROM 論文集, pp. 205-206, 2012][前田明彦, 高橋健一, 川村尚生, 菅原一孔, 第 12 回情報科学技術フォーラム講演論文集, 第 4 分冊, pp. 221-224, 2013][Akihiko Maeta, Kenichi Takahashi, Takao Kawamura, Kazunori Sugahara , International Conference on IT Convergence and Security (ICITCS2013), pp. 392-395, 2013][前田明彦, 高橋健一, 川村尚生, 菅原一孔, 暗号と情報セキュリティシンポジウム (SCIS), 1月, 2014]

(4)ソーシャルエンジニアリング的側面：強制投票

ACM CCS workshp Insider Theat 2010 で発表された "Duress Detection for Authentication Attacks Against Multiple Administrators" by Emil Stefanov et al. では、管理者が攻撃者に強要されてシステムへのアクセスが行われる際に、強要された事実が把握できる認証システム構築に関する研究を行なっている。強要の場合のパスワードを決めておくことや、本来のパスワードに続いて強要情報を付加する等様々なケースについて論じている。強要対策は、電子選挙システムにおける強要不正の問題として、暗号理論の世界では、15 年以上前から計算機科学者が検討してきた[J. Benaloh, D.Tuinstra, “Receipt-Free Secret-Ballot Elections”, Proc. of STOC ’94]。 研究代表者も強要不正に耐性をもつ電子入札方式を研究してきた[許, 櫻井, “無証拠性を持つ秘密入札プロトコルの安全性”, 暗号と情報セキュリティシンポジウム, Proc. SCIS2004]。今回の研究では、指紋をはじめとする生体認証プロトコルに焦点をあて、認証履歴が如何に保存され、履歴に証拠能力があるか、フォレンジックの立場から、既存の提案方式の分類を行った。プライバシ保護を可能とする生体認証として，キャンセラブルバイオメトリクスや非対称生体認証などが提案されており，リモートでの利用が想定されている.

しかしながら，これらの提案において，プロトコル上認証サーバ側に登録者に関する情報が「証拠」として残る可能性があることを指摘した[上繁，櫻井，SCIS2014 2014 年 暗号と情報セキュリティシンポジウム，1 月，2014]。

さらに生体認証プロトコルにおける「無証拠性」確保の必要性について検討するとともに，2 つの生体認証プロトコルについて，「無証拠性」の性質の解析をおこなった [上繁，櫻井，電子情報通信学会， 3月，2014]。

(5) 国際研究集会の開催・参加と学術交流

研究代表者はドイツ Gollmann と諮問(Steering)委員の立場で International Workshop on Managing Insider Security Threats 会議発足当初からに参画している。

MIST2012 開催：平成２４年１１月８日から同月９日まで、九州大学西新プラザにて 4th International Workshop on Managing Insider Security Threats (MIST 2012)を開催した(http://isyou.info/conf/mist12/)。国内１０名、海外２０名の参加があった。同時期に、同じ情報セキュリティ分野を扱う第７回情報セキュリティに関する国際ワークショップ（IWSEC2012）参加者１１７名（国内９４名、海外２３名）が同会場で開催されており、参加者の一部は両方の会議に参加したことから、招待講演の相互聴講許可、バンケットの共同開催等により、１２０名超の研究者との国際交流が行われた。

本国際会議は、２件の招待講演、２０件の研究発表講演、１件のパネル討論を実施した。１件目の招待講演は、米国パデュー大学の Eugene H. Spafford 教授を招聘し実施した。Spafford 教授は 1980 年代からインサイダー脅威問題に取り組んでいる先駆者である。Inside, Outside -- But Clearly Not on *Our* Side と題して、インサイダー脅威対策について講演した。2 件目の招待講演は、ドイツハ

ンブルク工科大学の Dieter Gollmann 教授を招聘し実施した。Gollmann 教授からは、サイバー・フィジカル・システムにおけるセキュリティについて講演した。公募研究発表は、インサイダー脅威管理、情報漏えい防止、暗号関連技術等のセッションが設けられ、最新の研究成果の共有と、今後に向けての議論が行われた。
謝辞：MIST2012 は、一部九州大学基金助成事業［社会との連携活動支援］の支援を受けた。

MIST2013 (http://isyou.info/conf/mist13/)
5th International Workshop on Managing Insider Security Threats (MIST 2013) October 24-25, 2013 Busan, Korea に参加した。今回で 5 回目である。参加者は 20 名程度、日本からは、IPA,企業研究所の研究員各一名と櫻井の計３名が参加していた。
基調講演１件（Dr. Felix Wu (Professor, UC Davis, USA)、Title: Anomaly Detection and Social Interactions:A Social Informatics approach for Insider Threats）に加えて、欧米から一線の研究者を招いてのパネル討論が行われた（座長 William R. Claycomb (Carnegie Mellon University, USA)、パネリスト S. Felix Wu (UC Davis, USA) , Dr. Christian W. Probst (Technical University of Denmark))。特にデンマークの Probst は、欧州の内部脅威対策プロジェクトの中心人物の１人である。

5. 今後の課題
内部脅威の中でも、情報漏洩が社会問題として顕在化している。本研究でも、アンドロイドなどスマートフォンにおける情報漏洩機能の解析と対策を検討した [梶原直也，堀良彰，櫻井幸一， 暗号と情報セキュリティシンポジウム (SCIS)，1月，2013]．今後は情報漏洩によるプライバシの影響や対策がさらに重要な課題となる。

6. 主な発表論文等
〔雑誌論文〕（計１０件）

① Akihiko Maeta, Kenichi Takahashi, Takao Kawamura, Kazunori Sugahara , Implementation of Logging for Information Tracking on Network, Proc. of the International Conference on IT Convergence and Security, 査読有, 2013, pp.392-395.
DOI: 10.1109/ICITCS.2013.6717841
② Fangming Zhao, Takashi Nishide, Yoshiaki Hori, Kouichi Sakurai, Analysis of Methods for Detecting Compromised Nodes and Its Countermeasures, Proc. of the International Conference on IT Convergence and Security, 査読有, 2013, pp.53-60.
DOI: 10.1007/978-94-007-5860-5_7
③ Yuuki Nishimoto, Naoya Kajiwara, Shinichi Matsumoto, Yoshiaki Hori, Kouichi Sakurai, Detection of Android API Call Using Logging Mechanism within Android Framework, Proc. of the 4th International Workshop on Applications and Techniques in Information Security, 査読有, 2013, pp.393-404.
DIO: 10.1007/978-3-319-04283-1_25
④ 千葉一輝，堀良彰，櫻井幸一，HTTP リクエストの情報量の異常値検出を用いた漏洩検知，情報処理学会論文誌，査読有，Vol.54, No.3, 2013, pp.1071-1076.
URL:
http://ci.nii.ac.jp/naid/110009552593
⑤ Dong Hao, Kouichi Sakurai, A Resource Minimizing Scheduling Algorithm with Ensuring the Deadline and Reliability in Heterogeneous Systems, Proc. of the 26th IEEE International Conference on Advanced Information Networking and Applications, 査読有, 2012, pp.495-502.
DOI: 10.1109/AINA.2011.87
⑥ Takashi Nishide, Shingo Miyazaki, Kouichi Sakurai, Security Analysis of Offline E-Cash Systems with Malicious Insider, Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications, 査読有, Vol. 3, No. 1/2, 2012, pp.55-71.
URL:
http://www.techrepublic.com/resource-library/whitepapers/security-analysis-of-offline-e-cash-systems-with-malicious-insider/
⑦ Kazuki Chiba, Yoshiaki Hori, Kouichi Sakurai, Detecting Information Leakage via a HTTP Request Based on the Edit Distance, Journal of Internet Services and Information Security, 査読有, Vol.2, Issue 3/4, 2012, pp.18-28.
URL:
http://isyou.info/jisis/vol2/no34/jisis-2012-vol2-no34-02.pdf
⑧ Dong Hao, Avishek Adhikari, Kouichi Sakurai, Mixed-Strategy Game Based Trust Management for Clustered Wireless Sensor Networks, Proc. of Third International Conference on Trusted Systems, 査読有, 2011, pp.239-257
DOI: 10.1007/978-3-642-32298-3_16
⑨ Yoshiaki Hori, Takashi Nishide, Kouichi Sakurai, Towards Countermeasure of Insider Threat in Network Security, Proc. of the Third International Conference on Intelligent Networking and Collaborative Systems, 査読有, 2011, pp.634-636.
DOI: 10.1109/INCoS.2011.156
⑩ Takashi Nishide, Kouichi Sakurai, Security of Offline Anonymous Electronic Cash Systems Against Insider Attacks By Untrusted Authorities Revisited, Proc. of 3rd International Conference on Intelligent Networking and Collaborative Systems, 査読有, 2011, pp.656-661
DOI: 10.1109/INCoS.2011.146

〔学会発表〕（計２１件）

① 上繁義史，生体認証プロトコルにおける無証拠性確保に関する考察，電子情報通

信学会総合大会, 2014 年 3 月 20 日, 新潟
② 小林佑行, プロキシ型しきい値パスワード鍵共有, 暗号と情報セキュリティシンポジウム, 2014 年 1 月 23 日, 鹿児島
③ 前田明彦, 機密情報の拡散追跡における追跡対象の削減, 2014 年暗号と情報セキュリティシンポジウム, 2014 年 1 月 24 日, 鹿児島
④ 上繁義史, 生体認証プロトコルにおける証拠性・無証拠性に関する一検討, 2014 年 暗号と情報セキュリティシンポジウム, 2014 年 1 月 23 日, 鹿児島
⑤ Akihiko Maeta, Implementation of Logging for Information Tracking on Network, International Conference on IT Convergence and Security, 2013 年 12 月 17 日, マカオ
⑥ 北島暢曜, 多人数の署名者による Fail-Stop 署名とその応用, 第 36 回情報理論とその応用シンポジウム, 2013 年 11 月 27 日, 静岡
⑦ Naoya Kajiwara, Detection of Android API Call Using Logging Mechanism within Android Framework, the 4th International Workshop on Applications and Techniques in Information Security, 2013 年 9 月 26 日, オーストラリア
⑧ 前田明彦, ネットワークへの情報拡散追跡のためのデータ取得, 第 12 回情報科学技術フォーラム, 2013 年 9 月 5 日, 鳥取
⑨ 梶原直也, 情報フロー追跡を用いた Android 端末における情報送信制御, 2013 年暗号と情報セキュリティシンポジウム, 2013 年 1 月 24 日, 京都
⑩ 前田明彦, 複数計算機間での機密情報拡散を追跡するためのログ管理手法, 第 14 回 IEEE 広島支部学生シンポジウム, 2012 年 11 月 17～18 日, 岡山
⑪ Motoki Kitahara, Embedding Information in a Public Key Efficiently, 7th International Workshop on Security, 2012 年 11 月 8 日, 福岡
⑫ 北原基貴, RSA 公開鍵における情報埋め込みサイズの上限に関する考察, コンピュータセキュリティシンポジウム, 2012 年 10 月 31 日, 島根
⑬ Fangming Zhao, A Note on Detection of Compromised Resource-Constrained Nodes and Its Countermeasure, コンピュータセキュリティシンポジウム, 2012 年 10 月 31 日, 島根
⑭ 前田明彦, 複数計算機でのファイル拡散追跡に関するログ管理, 電気･情報関連学会中国支部第 63 回連合大会, 2012 年 10 月 20 日, 島根
⑮ Dong Hao, A Differential Game Approach to Mitigating Primary User Emulation Attacks in Cognitive Radio Networks, IEEE 26th International Conference on Advanced Information Networking and Applications, 2012 年 3 月 27 日, 福岡
⑯ 西本祐揮, 動的解析を用いた Android における端末情報の取得検知手法, 火の国情報シンポジウム 2012, 2012 年 3 月 15 日, 福岡
⑰ Yoshiaki Hori, Towards Countermeasure Against Insider Threat on Network Security, 3rd International Workshop on Managing Insider Security Threats, 2011 年 12 月 1 日, 福岡
⑱ Takashi Nishide, Security of Offline Anonymous Electronic Cash Systems Against Insider Attacks By Untrusted Authorities Revisited, 3rd International Workshop on Managing Insider Security Threats, 2011 年 12 月 1 日, 福岡
⑲ Yoshiaki Hori, Towards Countermeasure of Insider Threat in Network Security, Third International Conference on Intelligent Networking and Collaborative Systems, 2011 年 11 月 30 日, 福岡
⑳ Dong Hao, Mixed-Strategy Game Based Trust Management for Clustered Wireless Sensor Networks, Third International Conference on Trusted Systems, 2011 年 11 月 29 日, 中国
㉑ 堀良彰, ネットワークセキュリティにおけるインサイダー脅威対策, 2011 年暗号と情報セキュリティシンポジウム (SCIS 2011), 2011 年 1 月 18 日, 福岡.

〔その他〕
ホームページ等
- 九州大学-研究者情報 [櫻井 幸一 (教授) システム情報科学研究院 情報学部門] http://hyoka.ofc.kyushu-u.ac.jp/search/details/K000220
- 櫻井研究室 http://itslab.inf.kyushu-u.ac.jp/

６．研究組織

(1)研究代表者
櫻井 幸一 (SAKURAI, Kouichi)
九州大学・システム情報科学研究院・教授
研究者番号：60264066

(2)研究分担者
高橋 健一 (TAKAHASHI, Kenichi)
鳥取大学・工学研究科・准教授
研究者番号： 30399670

西出 隆志 (NISHIDE, Takashi)
筑波大学・システム情報系・准教授
研究者番号：70570985

堀 良彰 (HORI, Yoshiaki)
佐賀大学・全学教育機構・教授
研究者番号：90264126