様式 C-19

科学研究費補助金研究成果報告書

平成２３年６月３日現在

機関番号：３２６５７
研究種目：基盤研究（C）
研究期間：２００８～２０１０
課題番号：２０５００７７
研究課題名（和文）　内部統制強化時代におけるデジタルフォレンジックス技術の研究
研究課題名（英文）　Study on Digital Forensics Technologies in Internal Control Reinforcement Era
研究代表者　佐々木　良一（SASAKI RYOICHI）
東京電機大学・未来科学部・教授
研究者番号：７０３３３５３１

研究成果の概要（和文）：内部統制強化時代においてデジタルデータの証拠性を正しく確保できるようにするため、（１）ヒステリシス署名とセキュリティデバイスを組み合わせて正当性を保証する技術、（２）証拠資料を公平に開示できるようにするための技術、（３）従業員への監視が強化される中で、可能な限りプライバシーを確保できる技術などを確立するとともにその有効性を検証した。

研究成果の概要（英文）：In the internal control reinforcement era, in order to keep the evidence of digital data correctly, we developed the technical methods to guarantee legitimacy using Hysterisis signature and security device, to be able to disclose documents fairly, and to secure the privacy of employees as much as possible while the monitoring to employees is strengthened. Moreover, we also verify the usefulness.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	1,300,000	390,000	1,690,000
2009 年度	1,300,000	390,000	1,690,000
2010 年度	900,000	270,000	1,170,000
年度			
年度			
総　計	3,500,000	1,050,000	4,550,000

研究代表者の専門分野：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：セキュアネットワーク、デジタルフォレンジックス

１．研究開始当初の背景

内部統制の強化時代において、デジタルデータの証拠性を確保し，訴訟などに備えるための技術であるデジタル・フォレンジックスの重要性が増大していた。しかし、このような問題を解決するための研究は少なく、特に、自分たちが訴訟に持ち込まれた場合に自らの正当性を証拠立てる方式の研究はほとんど行われてこなかった。

２．研究の目的

上記のような問題を解決するため、次

のような目的で技術開発を行った。

（１）正当性保証技術：従業員がガイドに沿って行動し、ログシステムに正当な記録を残し、消去や改ざんを行っていないことを証明すると共に、管理者自身がデータを不正に消去したり改ざんしたりしていないことを証明できるようにする技術である。これらの技術は不存在の証明技術(無過失の証明技術)とも言うことができ困難ではあるが非常に必要性が高いものである。

（２）E-Discovery 技術：訴訟された場合に必要・十分な証拠資料を公平に開示するための技術である。特に、必要な文書を提出しつつ、訴訟に関係の無い機密部分をすみ塗りする対応が必要になる。

（３）従業員のプライバシー保護技術：内部統制の進展に伴い、従業員への監視が強化される中で、可能な限りプライバシーを確保できる技術の確立を目的とする。

３．研究の方法

（１）正当性保証技術

中央から監視ができない状況下で従業員がガイドに沿って行動し、ログシステムに正当な記録を残し、データの消去や改ざんを行えないようにするための方式を開発するとともに、PC を改良し、大容量耐タンパー装置としてとして実装する．そのうえで、この装置が目的とする性能と安全性が確保できることを確認する。また、この技術を種々の現実的問題に適用する。

あわせて中央から監視ができる状況とできない状況がある中で安全性と処理効率のよさを実現する方式を開発し実験によって有効性を確認する。

（２）E-Discovery 技術

訴訟された場合に必要・十分な証拠資料を公平に開示するため、①電子署名付の文書に対し、すみ塗りしてもその他の部分の改ざんを検知できるようにするとともに、②キーワードに関連する情報をすべて開示したことを証明できるなどの機能を持つ方式を開発する。あわせて上記の装置に実装し、目的とする機能、性能、安全性が達成可能であることを確認する。

（３）従業員のプライバシー保護技術

WEB アクセスなど電子メール以外の監視を可能な限り自動化し、通常状態では誰がやっている処理かわからないが、不正があることが自動検知されると、直ちに追跡が可能な方式の開発を行う。

４．研究成果

（１）正当性保証技術

中央から監視ができない状況下で従業員がガイドに沿って行動し、ログシステムに正当な記録を残し、データの消去や改ざんを行えないようにするため、ヒステリシス署名とセキュリティデバイスを組み合わせる方式を開発した。あわせて PC のハードを改良するとともに、上記の機能をプロトプログラムとして実装することにより大容量耐タンパー装置 **HiGATE**（High Grade Anti-Tamper Equipment）として PC 上に実現した。あわせて性能評価を行い PC と同様な性能が維持でき目的とする性能を達成することを確認した。また、装置の安全性をフォルトツリー分析を実施することなどによって確認した。また、この技術を疫学調査の解析、不正侵入対策、情報漏洩対策などに適用した。

この方式は海外にもない先行的なものであるので、論文化や海外発表をいろいろ行うとともに、基本方式を特許として出願した。

あわせて中央から監視ができる状況と

できない状況がある中で安全性と処理効率のよさを実現するため、外部からの攻撃を考慮しつつネットワーク状態を監視する方式を開発し、状態によって処理を動的に変化させることにより開発した。また、プロトプログラムを開発し実験によって性能評価を行い、あわせてフォルトツリー分析によってその安全性を確認した。
これらに関連し種々の論文化と海外発表を行った。

（２）E-Discovery 技術

訴訟された場合に必要・十分な証拠資料を公平に開示するため、電子署名方式を改良し、電子署名付の文書に対し、すみ塗りしてもその他の部分の改ざんを検知できるようにする方式を開発した。また、墨塗りをしている部分は何かはわからないがキーワードに関連する情報が含まれてなく、関連した情報をすべて開示したことを証明できる機能を持つ方式を開発した。さらにプロトプログラムを開発し、上記の HiGATE 上に実装した。目的とする機能、性能、安全性が達成可能であることを確認した。

これらは海外にもないアプローチであるので、いろいろな論文化や海外発表を行った。

（３）従業員のプライバシー保護技術

WEB アクセスなど電子メール以外の監視を可能な限り自動化し、通常状態では誰がやっている処理かわからないが、不正があることが自動検知されると、直ちに追跡が可能な方式を公開鍵暗号に基づくカギ供託技術を改良することによって実現した。あわせて安全性評価をフォルトツリー分析などを用いて実施した。

５．主な発表論文

〔雑誌論文〕（計１１件）

①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、査読有、VOL.52,No.3、２０１１、1136-1143

②　川上昌俊、安田浩、佐々木良一、情報セキュリティ教育のためのｅラーニング教材作成システムＥＬＳEC の開発と評価、情報処理学会論文誌、査読有、VOL.52,No.3、２０１１、266-1278

③村上　真教、甲斐　俊文、佐々木良一、他１名、ＩＰトレースバックにおける出国印方式の拡張と評価、情報処理学会論文誌、査読有、VOL.51,No.9、２０１０、1610-1621

④三原　元、佐々木良一、数量化理論と攻撃データ（CCCDATAset2009）を利用したボットネットの C&C サーバー特定手法の提案と評価、情報処理学会論文誌、査読有、VOL.51,No.9、２０１０、1579-1590

⑤藤田　圭祐、芦野　佑樹、佐々木良一、他１名、不正プログラムの起動制御機能を持つＤＦシステムの提案と評価、情報処理学会論文誌、査読有、VOL.51,No.9、２０１０、1507-1519

⑥Jigang Liu、Tesutaroh Uehara, Ryoichi Sasaki 、 Development of digital forensics practice and research in Japan 、 Wireless Communications And Mobile Computing(Wiley InterScience) www.interscience.wiley.com、査読有、２０１０、40-253

⑦竹下　数明、小林　偉昭、佐々木良一、脆弱性対策教育のための e ラーニングシステムの開発と評価、日本セキュリティマネジメント学会誌、査読有、VOL.24,No.1、２０１０、17-26

⑧田村　佑輔、甲斐　俊文、佐々木良一、ユーザ標的型 Web サイト改ざんに対する検索エンジンを用いた検知手法の提案､情報処理学会論文誌、査読有、第 51 巻第 1 号、２０１０、191-198

⑨植松　建至、芦野　佑樹、佐々木良一、他 3 名,構造計算書不正検知システムの提案,情報処理学会論文誌、査読有、第 49 巻,2008,3199-3208

⑩高塚　光幸、多田　真崇、佐々木良一、開示情報の墨塗りと証拠性確保を両立させる e-Discovery システムの提案､情報処理学会論文誌、査読有、第 49 巻、２００８、3191-3198

⑪佐々木良一、ディジタルフォレンジックの最新動向、電子情報通信学会雑誌、査読無、91 巻、２００８、744-745

〔学会発表〕（計２３件）

①Koji Hasebe,Development of a method for using High-Grade Anti-Tamper Equipment for privacy protection in epidemiology investigation that use data from multiple organization, ICIMT2010,2010.12.28,HongKong

② Naoki Masashige, Proposal and Evaluation of Sound Storage Authentication System for the Visually Impaired, ICIMT2010, 2010.12.28, HongKong

③ Yui Sakurai,HiGATE(High Grade Anti-Tamper Equipment)Prototype and Application to e-Discovery, ADFSL2010, 2010.05.25,USA(Virginia)

④ Maiko Furusawa, Development of a system using the APIHook function to protect personal information leakage from USB memory,IWISA2009 ,2009.12.10, Korea

⑤ Koushou Yoshioka, Proposal and evaluation of a high-speed data erasure method for mass storage devices,ＪＷＩＳ:Joint Workshop on Information Security2009,2009.8.6.Taiwan

⑥Yuki Ashino, Extension and Evaluation of Boot Control for a Digital Forensic System,5th Annual IFIP WG11.9International Conference on Digital Forensics,2009.1.26.Flolida,USA

⑦Kenshi Uematsu,Proposal of Falsification Detection System in Structural Design ,The Fourth International conference on Intelligent Information Hiding and Multimedia Signal Processing, 2008.8.15,China

［産業所有権］

○ 出願状況（計１件）

名称:プログラムの不正起動防止システム及び方法

発明者:佐々木良一,藤田圭祐,芦野佑樹、上原哲太郎

権利者:学校法人東京電機大学

種類:特許

番号:2008-110270

出願年月日: 平成 20 年 4 月 21 日

国内外の別:国内

６．研究組織

(1)研究代表者

佐々木　良一（SASAKI RYOICHI）

東京電機大学・未来科学部・教授

研究者番号：70333531

(2)研究分担者

なし