様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２４年　５月　９日現在

機関番号：１５３０１
研究種目：若手研究（B）
研究期間：2009～2011
課題番号：21700034
研究課題名（和文）　機密情報の拡散追跡と保護を実現するオペレーティングシステムの基盤技術の研究
研究課題名（英文）　Study of operating system technology for tracing classified information

研究代表者
山内　利宏（YAMAUCHI　TOSHIHIRO）
岡山大学・大学院自然科学研究科・准教授
研究者番号：80359942

研究成果の概要（和文）：
機密情報の拡散追跡機能のログを可視化する機能，およびリモートコンピュータとの通信を追跡する機能を実現した．これにより，機密情報の拡散経路をより簡単に把握することができる．また，コンピュータの実行履歴であるログを確実に取得し，安全に保存する手法を仮想マシンモニタに実現した．さらに，その有効性を評価により示した．これにより，ログの消失を防止でき，ログの改ざんを防ぐことができる．

研究成果の概要（英文）：
We realized a function that visualizes the diffusion path of classified information. We also realized a function that traces diffusion path between remote computers. The visualization function allows us to understand diffusion path easily. We realized a function that gets logs and safely stores the logs in virtual machine monitor. We evaluated the function and showed the effectiveness of it. This function can prevent attackers from altering the logs.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００８年度			0
２００９年度	1,400,000	420,000	1,820,000
２０１０年度	900,000	270,000	1,170,000
２０１１年度	900,000	270,000	1,170,000
総　計	3,200,000	960,000	4,160,000

研究分野：オペレーティングシステム，コンピュータセキュリティ
科研費の分科・細目：ソフトウェア
キーワード：機密情報，追跡，情報漏洩防止，オペレーティングシステム

１．研究開始当初の背景

現在，計算機からの機密情報の漏洩が大きな問題となっている．情報漏洩の原因としては，内部の人間による犯行や誤操作，設定ミスに起因する情報漏洩が多い．このため，機密情報を安全に管理できるシステムの実現が望まれている．また，従来のオペレーティングシステム(OS)では，セキュリティを確保するには十分とはいえず，より安全な OS の導入を検討する必要がある．

現在の OS は，プログラムがファイルの利用要求を発行したときに，権限を確認するの

みで，その後の利用状況を追跡しない．このため，計算機の管理者や利用者が，機密ファイルがどのファイルにアクセスされ，機密情報がどの範囲に伝播したのかを確認する方法がない．また，情報漏洩が起こったときに，ファイルアクセスの状況を証拠として適切に保存し，その内容を検証できる手段が必要である．

２．研究の目的

これまでに，機密情報の拡散追跡と情報漏洩の検知機能，および設定工数削減と安全性を両立できる統合アクセスパーミッションの提案と評価の研究を行ってきたものの，追跡した機密情報の利用状況をわかりやすく見せ，かつその情報を漏洩事故発生時の証拠として利用するには，まだ課題がある．

本研究では，以下の 2 つの機能を実現する．

(1) 機密情報の拡散追跡機能で収集した情報をわかりやすく提示できる機能の実現

機密情報の拡散追跡機能で収集した情報をうまく利用者に表示する手法を確立し，利用者が計算機内部での機密ファイルの利用状況を容易に把握できる機能を実現する．

また，計算機の利用開始から現在までの特定期間の情報を指定して，アクセス内容と拡散状況を表示できることを実現し，時間をさかのぼって，ファイルの利用履歴をさかのぼれる機能を実現する．

(2) 機密情報へのアクセス情報の安全な保存と完全性検証機能

収集した機密情報のアクセス情報の正当性を検証できる形式で保存できることを実現する．また，保存した情報の完全性（改ざんされていないこと）を後で検証する手法を実現する．

３．研究の方法

(1) 機密情報の拡散追跡機能で収集した情報をわかりやすく提示できる機能の実現

これまでに実現した機密情報の拡散追跡機能は，機密情報の拡散が最初に起こった処理のログのみを取得し，拡散経路を追跡する．このため，任意の時間帯に調査範囲を絞って拡散経路を追跡する場合に，情報が不足している．これを解決するため，すべての拡散経路を可視化するために，必要な情報，およびその情報の取得契機を明らかにする．

また，取得したログを可視化する手法を検討する．取得した情報をすべて可視化するだけでは，表示が複雑になりすぎ，利用者の理解が困難になる場合があると考えられる．利用者が必要とする情報を表示できる手法について，検討する．

さらに，現在は，一つの計算機内部の情報しか取得しないため，計算機間の機密情報伝搬を追跡する手法について検討する．

(2) 機密情報へのアクセス情報の安全な保存と完全性検証機能

OS のログを確実に取得する機構の実現するために，カーネルログとユーザログのそれぞれについて，ログの取得手法を設計し実現する．カーネルログについては，カーネル内のリングバッファにログが書き出されるため，カーネル内部のログを書き出す関数において，仮想マシンモニタ(VMM)に制御が移行するようにブレークポイントを追加し，ログを取得する．

次に，ユーザログについては，ログを送信するシステムコールの発行を契機として，VMM に制御を移行させ，ログを取得する機構を設計する．

また，取得したログを VMM にためておくだけでは，安全にログを保存できないため，ログ保存 OS にログを送信し，ログ保存 OS のファイルシステムに保存する機構を設計する．

４．研究成果

機密情報の拡散追跡機能で収集した情報をわかりやすく提示できる機能の実現については，以下の機構を実現した．

(1) すべての機密情報の拡散契機で可視化をするために必要なログを取得する機構

(2) カーネル内で取得したログを保存する機構

(3) ログ情報をフィルタリングして，ユーザが着目しているファイルや期間の情報に関するログのみを出力する機構

(4) 出力されたログを可視化するプログラム

また，実現した可視化機能の評価を以下の観点で行った．

(1) 各状況でのフィルタと拡散経路図の有用性の評価

(2) フィルタリングによる拡散経路図の複雑化防止の評価

(3) 提示方式の違いによる拡散経路把握の正確性と迅速性の評価

一つ目の評価では，提案機能は，利用状況に合わせて，3 つのフィルタを組み合わせて，機密状況の伝搬の可視化ができることを示した．二つ目の評価では，フィルタリングにより，可視化表示の複雑化を防ぐことができることを示した．3 つめの評価では，被験者の回答時間と正答率を，フィルタリングと可視化により，向上させることができ，ログを用いるよりも，正確かつ迅速に機密状況の利用状況を把握できることを示した．

また，リモート計算機への機密情報の拡散を追跡するために，ソケット通信について，機密情報の拡散を追跡する基本機能を提案した．

機密情報へのアクセス情報の安全な保存と完全性検証機能については，VMM の一つである Xen にカーネルログとユーザログをゲスト OS のソースコードを修正することなく，対象の VM（仮想計算機）におけるログ出力直後に VMM が取得する機能を実現した．ログ出力直後に VMM がログを取得することで，ログ書き出しプログラムを介してファイルへ書き出されるまでの間に，ログを改ざんする余地を残さない．また，取得対象となる VM からログを隔離することで，取得したログの安全性を確保できる．

次に，ログを他の VM に保存するログ保存機構を実現した．ログ保存機構は，ログ取得機構が監視対象 OS から取得したログをログ保存 OS 上の syslog を介して自動的にログファイルへ書き出す．ログを自動的に保存することで，計算機の不意の電源断によるログの消失を防止する．

さらに，ログファイルを比較することでログの改ざんを検知する機能を提案し，実現した．本機能は，提案システムで取得したログと監視対象 OS 上のログファイルを比較することで，ログの改ざんの有無だけでなく，改ざん箇所と改ざんや消失を検出できる．ログ保存 OS は，監視対象 OS と同様のログの振り分けを実現しているため，diff コマンドを利用してファイルの差分を取得することで，改ざん箇所や改ざん内容を容易に検出できる．

また，実現したシステムについて，ログの改ざんや消失の起こる環境を想定し，評価した．評価結果から，監視対象 OS 上のログファイルの改ざん検出と syslog デーモンの動作の変更によるユーザログの消失防止が可能なことを示した．また，大量にカーネルログが出力されることで古いログが消失してしまう問題について，提案システムの導入によりこの問題へ対処できることを確認した．

さらに，ログの改ざん検知機能を実在するマルウェアを用いて評価した．評価結果から，マルウェアによるログファイルの改ざんの有無と改ざん箇所を特定できることを示した．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計２件）

①Masaya Sato, Toshihiro Yamauchi, VMM-Based Log-Tampering and Loss Detection Scheme, Journal of Internet Technology, 査読有，2012，掲載決定

②佐藤 将也，山内 利宏，ログの改ざんと喪失を防止するシステムの仮想計算機モニタによる実現，情報処理学会論文誌，査読有，Vol.53，No.2，pp.847-856

（総件数２件）

〔学会発表〕（計８件）

①大坪 展人，機密情報の拡散追跡機能の分散環境への対処法，電子情報通信学会 2012 年総合大会，2012 年 3 月 22 日，岡山大学

②佐藤 将也，仮想計算機モニタによりログの改ざんや消失を検知する方式の実現，2012 年暗号と情報セキュリティシンポジウム（SCIS2012），2012 年 2 月 2 日，金沢エクセルホテル東急

③福島 健太，機密情報の拡散経路を可視化する機能の提案，コンピュータセキュリティシンポジウム 2011 ，2011 年 10 月 20 日，朱鷺メッセ

④ Masaya Sato, VMBLS: Virtual Machine Based Logging Scheme for Prevention of Tampering and Loss, 2011 International Workshop on Security and Cognitive Informatics for Homeland Defense (SeCIHD'11)，2011 年 8 月 22 日，ウィーン工科大学

⑤佐藤 将也，仮想計算機モニタによるカーネルログ取得機能の実現と評価，第 54 回コンピュータセキュリティ・第 1 回情報セキュリティ心理学とトラスト合同研究発表会，2011 年 7 月 13 日，静岡大学

⑥佐藤 将也，仮想計算機モニタによるログの改ざんと喪失防止システムの提案と評価，情報処理学会 コンピュータセキュリティシンポジウム 2010(CSS2010)，2010 年 10 月 20 日，岡山コンベンションセンター

⑦中務 亮，ファイル操作による情報伝搬の追跡機能と可視化機能，第 9 回情報科学技術フォーラム(FIT2010)，2010 年 9 月 7 日，九州大学

⑧植村 晋一郎，複数計算機間における機密情報の拡散追跡機能の設計，2010 年暗号と情報セキュリティシンポジウム(SCIS2010)，2010 年 1 月 22 日，かがわ国際会議場

（総件数９件）

〔図書〕（計０件）

〔産業財産権〕
○出願状況（計０件）

○取得状況（計０件）

〔その他〕
なし.

６．研究組織

(1)研究代表者
山内　利宏（YAMAUCHI　TOSHIHIRO）
岡山大学・大学院自然科学研究科・准教授
研究者番号：80359942

(2)研究分担者
なし

(3)連携研究者
なし