様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ６ 月 ２４ 日現在

機関番号：３２７２１
研究種目：基盤研究(B)
研究期間：2012～2014
課題番号：２４３０００００９

研究課題名（和文）次世代情報セキュリティ基盤を実現するＯＳ強化に向けた資源アクセス制御方式

研究課題名（英文）Resource access control system for security-enhanced OS as the next-generation platform of information systems

研究代表者

田中　英彦（Tanaka, Hidehiko）

情報セキュリティ大学院大学・その他の研究科・教授

研究者番号：６００１１１０２

交付決定額（研究期間全体）：（直接経費）　　11,900,000円

研究成果の概要（和文）：本研究では、厳密且つ安全なアクセス制御機構を応用と基盤の協調により実現し、情報システムに階層的防御網を適用する新たなOS技術を提案した。その中核は、応用の実行状況等を考慮して動的に最小のアクセス権限を与える機構の提案と、その強固な実現手段、及びこれらを実用的なものとする、明快・簡便なポリシ記述・管理系の提案である。本研究の特徴は、従来OSでは粗すぎるアクセス制御により攻撃遅延・被害局所化が機能しない問題と、SELinuxに代表されるセキュアOSの細粒度アクセス制御は複雑すぎて実利用に耐えない問題の、両方を解決できることにある。

研究成果の概要（英文）：In this research, we proposed a new operating system technology to implement a defense-in-depth strategy to information systems, which is based on a strict and secure access control mechanism achieved by the cooperation between applications and its infrastructure. Specifically, the main achievements of this research are followings; i) a proposal of a mechanism that gives the minimum access rights dynamically in consideration of the execution status of applications, ii) its robust implementation, and iii) a proposal of a simple and clear policy description language and its management system to make the implementation fit for practical use. The key feature of the research is to solve the problem of general operating systems in terms of insufficiency of compartment function caused by its coarse-grained access control systems, while it can solve the problem of MAC operating systems in terms of impracticality caused by its fine-grained access control systems, at the same time.

研究分野：情報セキュリティ

キーワード：情報セキュリティ　アクセス制御　オペレーティングシステム

１．研究開始当初の背景

昨今、大規模情報漏洩や、特定企業や省庁等に対する標的型攻撃が問題となっている。しかしながら、これらの攻撃で利用される具体的な手法や手順は、ここ十数年、根本的に何ら変わりはない古典的・典型的なものがほとんどである。それにも関わらず、未だに重大なセキュリティ侵犯を防げないポイントの一つに、応用（アプリケーション）と基盤（プラットフォーム）の基本的な構造が、セキュリティ的な観点では変わっていないことがあげられる。

情報システムに対するどのような攻撃であれ、それはなんらかの脆弱性をきっかけとしており、脆弱性は、基礎から応用まで様々な階層に存在し得るものであるが、特にここ数年においては、応用に対する攻撃が増加している。その理由は、近年ではベンダーや開発者の努力により、OS や各種ミドルウェア等の基盤ソフトウェアに含まれる脆弱性は著しく減少しており、以前は主流であったWeb サーバや DB といった汎用応用への攻撃が難しくなった。勿論、これらの脆弱性がなくなったわけではないが、それに対して、今度はそれらの上に構築される個別応用の弱点が相対的に浮き彫りになってきている。すなわち、個別応用のセキュリティ確保の問題は、なによりそれらが個別に構築される点にある。個別であるということは、そのセキュリティレベルは、開発者もしくはベンダーに依存することとなり、大規模ベンダーにより開発され、広く使われる基盤ソフトウェアよりも、潜在的なセキュリティ問題への対処が困難で、「情報システムのセキュリティレベルは最弱点に引きずられる」等の表現があるように、相対的に脆弱なポイントがあれば、そこが積極的な攻撃の対象となる。

ここで最大の問題は、応用レベルの攻撃は連鎖的に大きな被害をもたらすということで、実際に、応用の脆弱性により DB 等に格納されたデータが大量に漏洩するようなセキュリティ侵犯が昨今多発しているのは、このことの証左である。本研究は、基盤の構造を見直すことで、基盤と応用双方の脆弱性対策とし、問題が起きた時の影響範囲を押さえることを目的とした、階層的防御網を情報システムに適用可能する新たな OS 技術の提案である。

２．研究の目的

本研究の中核は、i) 応用の実行状況とアクセスされる資源の状況とを考慮して動的に適切最小のアクセス権限を与える機構の提案と、ii) それを外部からインターセプトされない形で実現する方法、及び、iii) そのようなアクセス制御ポリシを分散システム上で容易に記述できる仕組みの提案、がその内容である。更に、この研究では、この方式を実際の Linux の上に実装し、方式の有効性を示すとともに、具体的な分散処理応用として、分散トランザクション処理と、今後重要なクラウド環境を取り上げ、それへの適用法と有効性を示すことを目的とする。

このような目的のために、研究代表者らはこれまでの研究において、その汎用的基本アクセス制御アーキテクチャを示した上で、そこに設定するアクセス制御ポリシの記述言語として論理型言語によるプロトタイプ言語を設計し、Linux のカーネル内に実装した。更に、アクセス要求を出す応用プロセスの確実な捕捉のために、プロセスの SVC 履歴を用いる方法を提案してきた。

これらの成果をベースに、今回の研究では、OS と応用との連携による具体的なアクセス制御システムを提案した上で Linux カーネルへの実装を示し、同時に、分散トランザクションや、クラウド環境への適用を与えて評価することで、この提案の有効性を示す。すなわち、3 年内で以下の研究を行う。

① 既存のアクセス制御情報に加えて、資源アクセス要求を出す主体の状態や実行履歴を把握し、環境情報と合わせて認可判定を行う安全な細粒度強制アクセス制御方式を設計する。
② 1 の細粒度強制アクセス制御機構に対するポリシ記述に論理型言語を用いることで、応用開発者に取って見通しのよい強力な最小権限記述法を提示する。
③ 2 の記述の実行コードをカーネル内の細粒度強制アクセス制御機構に設定し、応用からのアクセス要求に対して、その主体に関連する情報を付加して 1 に基づくアクセス制御を行う機構を設計し、Linux カーネルの内部で実装する。
④ 1～3 で構成した単一システム用アクセス制御システムを、複数のシステムから構成される分散系へ拡張する。そのとき、国際標準になっている SAML モデル・XACML 言語の適用を考慮して、本提案のアクセス制御システムとの接合とマッピングを検討する。
⑤ 4～5 で構成した分散系で用いる分散型ポリシの定義を与え、それに基づくローカルシステム相互間のアクセス交渉系を検討する。
⑥ 6 までで出来上がった分散アクセス制御システムを用いて、複数システムを構築し、その上の具体応用として、分散トランザクションと、複数 VM 間協調応用、並びに複数クラウド間協調システムを載せて、評価するとともに、これらへの適用手法を具体的に与える。

３．研究の方法

研究では、厳密な階層的防御網を実現する

実用的な細粒度アクセス制御機構について、まず単一システムに閉じた環境で作り上げる。中心となるテーマは、ポリシの理解容易性・管理の簡便さ、制御対象の細粒度化で、論理型言語によるポリシ記述と柔軟なポリシ管理機能により、人間にとって扱い易く強力なアクセス制御システムを実現する。次に、この方式を拡張し、分散型の細粒度アクセス制御アーキテクチャを設計する。分散系への対応としては、主体や客体の状態を考慮するアクセス制御モデルを設計し、状態の同定手法や、競合するアクセス権の調停等を実現する推論エンジンを検討しながら、国際標準モデルへの適合も計る。その後は、従来方式からの移行・融合方式、クラウド環境への適用手法などを検討した上で、Linux による実験システムに実装し、各種評価と改善を行う。

初年度は、これまでの研究で示した汎用的基本アクセス制御アーキテクチャのうちで、アクセス権記述から認可判定機構までの一連の仕組みと、TOMOYO Linux の強制アクセス制御機構を連結し、高レベルのポリシ記述言語とその設定系を中心に、強制アクセス制御の実用的な実装を実現する。

はじめに、TOMOYO の強制アクセス制御機構に与える細粒度のポリシ記述表現を、開発済のプロトタイプ言語を拡張することで実現し、その処理系を含めた実装を行う。

拡張の要件は、従来からあるアクセス制御情報に加えて、実行履歴によって分類された細かなアクセス主体と、実行時パラメータや環境変数によるプログラムの実行可否を過不足なく明快に表現できることで、記述内容の複雑化や記述量の増加には、プロトタイプ言語の継承機能等、構造化記法を活用することで対応を計る。

プロトタイプ言語は、従来固定的に記述されていたポリシを、論理型言語によるプログラムとして柔軟に記述することを目的としたもので、これまでの研究では、Prolog のサブセットである Datalog を用いた実装を行い、様々な既存アクセス制御モデルを構造的に記述する手法を示した上で、SELinux のポリシを実際に記述した実験システムを構成し、認可判定の結果が妥当で、且つ、表現力が従来のポリシ記述言語よりも豊かであることを示した。この点で、従来のセキュア OS や DB、Web サービスなどのアクセス権記法は、それぞれに固有の形式で、限定的なアクセス条件を記述するものであるため、新しい情報をアクセス条件として柔軟に追加できるように設計されておらず、本研究の要件を満たすような拡張には向いていない。

論理型言語によるポリシ記述から期待される効果は、アクセス条件を構成する個々の要素条件を柔軟にプログラムできるため、強制アクセス制御機構からの制約に縛られない、自由度の高いアクセス権記述が解り易い形で表現可能となることである。本提案では、プログラムにより生成したアクセス条件を独立に OS 内で設定するので、アクセス制御機構からの制約には依らない細かな条件を柔軟に適用することが可能となり、アクセス主体／対象の状態等といった新しいアクセス条件の導入による、仮想環境や分散処理に対する必要充分なアクセス権限付与を実現する。

記法と処理系の設計にあたっては、厳密な階層的防御網を柔軟に実現するために、各プロセスの SVC の履歴情報をモニタして蓄積し、それをアクセス主体の同定に用いることで、詳細に分類されたアクセス主体を指定する細粒度のアクセス条件を表現する記法を検討する。また同時に、プログラム実行の可否にあたっては、実行時パラメータや環境変数を指定可能することで、系外活動によるアクセス制御の無効化を引き起こす Covert Channel を原理的に防ぐことを可能とする。

次に、拡張したポリシ記述・処理系と TOMOYO の強制アクセス制御機構を、安全・確実に接続するパスとして、ポリシ管理用の常駐プロセスを用いる新規手法を開発する。

ポリシ管理プロセスの目的は、実行履歴によるアクセス主体分類と、実行時パラメータ評価を導入したことによるポリシ管理の複雑性を低減することで、TOMOYO が備えるポリシの自動学習モードと協調して機能することにより、ポリシの差分管理に基づく前ポリシからの特定アクセス権限付加や除去、自動学習モードへの移行、特定環境条件・トリガー監視取得等を常駐しながら実行し、従来以上に細粒度化した強制アクセス制御を実用的に構成可能とする方式を検討する。

検討のポイントは、論理型言語で記述されたアクセス権を、アクセス制御情報 DB 内に静的のみならず動的にも設定可能とすることである。そのために、アクセス権記述の処理系とアクセス制御情報の設定系を具体化し、記述の正しさとアクセス制御情報 DB に対する設定権限の厳密な検査をおこなうことで、記述から設定への安全・確実なパスを保証する。同時に、各種アクセス制御情報の取得や学習モードの起動、ポリシの差分管理を実現する手法を設計する。

その後は、ポリシ管理プロセスを含むポリシ記述・設定系と、その連携により実現される細粒度の強制アクセス制御機構を評価する。はじめに、ポリシ記述言語を用いて、小規模なアクセス制御情報 DB を構成し、机上実験を行って、適切な粒度、判定計算量、記述力、記述の容易性、検証可能性などを多角的に評価する。同時に、Web サービスを含む幾つかの主要アプリケーションを例として、アクセス制御情報を実際に構成した上で、SELinux 等、強制アクセス制御機構の既存実装と比較し、ポリシ管理が容易でありながらも、厳密な階層的防御網を構成可能であることを実証する。また、不正な問い合わせや、意図しないアクセス権制御、サービス停止攻撃など、アクセス制御情報 DB やポリシ管理

プロセスに対する攻撃を想定し、今年度に設計したポリシ記述・処理系と TOMOYO を、ポリシ管理プロセスにより連結した強制アクセス制御機構が、十分に強固で実用に耐えるものであることを裏付ける。

平成 25 年度は、分散環境において、階層的防御網による被害局所化を有効に実現するために、アクセス主体と対象をその状態に基づいて細かに分類する新規アクセス制御モデルを設計し、ポリシの分散管理・配布を含む分散型強制アクセス制御アーキテクチャを提案・実装する。また、ポリシ記述言語を拡張することで、細粒度の分散処理を記述可能とし、同時に、国際標準である SAML モデルや XACML 言語とのマッピング方式を検討する。

はじめに、これまでの研究で実現した、実行履歴と実行時パラメータを用いるアクセス制御モデルを拡張し、細粒度の多層防御を実現するための、状態に基づくアクセス制御モデルを新規に定義する。

従来のアクセス制御モデルでは、アクセス主体やアクセス対象が静的な実体であることを前提としているため、アクセス権限の細粒度化に限界があり、結果として、セキュリティ侵犯があった際の被害の局所化が限定的であった。ここで提案するアクセス制御モデルは、実際のプロセスやファイルが様々な状態を取り得る点に着目し、各々に付与するアクセス権限を動的に変更することを目的とする。状態の同定には、トランザクション処理の実行ステップや外部システムから取得した情報等に加えて、SVC の履歴を用いることを検討しており、それらの情報は、既に開発したポリシ管理プロセスに加えて、SVC 履歴モニタを新たに実装することにより取得可能する。

また、本研究においては、知識ベースとしてのアクセス権記述を推論エンジンで処理することにより、複数のアクセス権の組み合わせから必要十分に細かなアクセス権が動的に設定可能となることを期待している。すなわち、他のサブシステムが管理するリソースに対するアクセスを別のシステム上でおこなう場合に問題となるのは、統合処理をしたときに記述内容が完全には一致しないことで、それに対しては、リソースを要求する側と提供側のアクセス権をミニマックス法で推定し、それを定めて解決を図る。また、この場合、 記述に用いるリソースなどの名前の整合性は、外部の枠組みにより取れていることを想定している。

次に、このアクセス制御モデルを表現・設定するために、前年度に開発したポリシ記述言語を拡張する。拡張の目的は、アクセス制御の細粒度化に伴うポリシ記述の複雑性を低減することで、その具体的内容は、アクセス権限推論アルゴリズムの強化と、個々のアクセス制御規則に対する追加や削除・統合規則を表現し、ポリシ管理プロセスの動作規則を与えるメタ言語の導入である。また、複数ポリシ間の調整や競合解決、集約ポリシの分散配布を実現するためのアクセス権連携手法を開発する。

同時に、提案した分散型の強制アクセス制御機構が、様々なアクセス制御モデルで動作するシステム群と、グローバルに連携することを可能とするために、SAML や XACML といった Web サービス標準が規定するアクセス権記述との互換手法についても検討し、提案機構が異機種混合の分散システムに組み込まれた場合にも問題なく機能するための、アクセス権マッピング方式について検討する。この際には、標準言語から本提案のポリシ記述言語へのマッチングが比較的容易な一方で、その逆は記述粒度の関係から困難であることが予想され、その対策として、ポリシ管理プロセスによる情報流の検証と、その結果に基づくアクセス権限の追加／縮退によって対応する手法を検討する。

最終年度となる平成 26 年度は、前年度までに開発した分散型の細粒度強制アクセス制御機構を実装したシステムを複数接続した上で、グローバルな実験システムを構築し、その有効性の検証と安全性の評価を行う。また、本システムの階層的防御手法を基礎とする、新たな適用対象についても考察すると同時に、現実の情報システムに抵抗なく適用可能とするために、既存システムからの移行方法や既存システムとの融合手法についても検討する。

検証項目は 3 つで、実行履歴と実行時パラメータ、状態に基づくアクセス制御モデルがポリシ管理プロセスの支援により正しく安全に実現されていること、要素システム間の連携機構が正しく動作すること、情報システムが部分的に非安全となっても階層的防御によって被害を局所化し、全体として正しく動作し続けることである。各種モデルの有効性の検証は、提案するモデルおよび機能が実装可能であり且つ様々な脅威に強固であることを確認することがポイントで、その効果をチェックするために、実験システムを複数接続し、提案するモデルおよび機能が効果的に動作することと、安全であることを立証する。実験システムは、Linux のアクセス制御システムを、提案方式によるポリシ記述・設定系と、細粒度強制アクセス制御機構で置き換えることにより実現する計画である。

次に、これらの諸要素検証の後、実際の情報システムに近い形での総合的な実証と最終的なアーキテクチャの提案を行う。また同時に、既存システムから本システムへの移行を、現実の情報システムに適用するための具体的なステップの切り方や、既存システムとの融合手法を検討することで、提案するモデルおよび機能が現実の情報システムに適用可能であり、効果的に動作することを立証する。

この総合的な実証としては、Firewall、IDS、

各種サーバ等の構成要素をもつ典型的な情報システム上で様々なセキュリティ侵犯を想定したテストを行ない、提案システムの効果を立証する。また提案した各種手法や機能について、オーバヘッドや遅延を定量的に測定し、結果を分析することで、本手法の有効性を具体的に示すとともに現実的な対策としてまとめあげ、最終提案を行う。

尚、本研究においては、研究代表者である田中英彦を中心にシステムの構想と具体的な設計を行い、それに基づいた詳細なモデルとプロトコルの作成、実装を研究分担者である橋本正樹が中心に行う。各種成果物に対する評価と分析、実証実験、さらに最新技術動向との比較検討、対外発表については、研究分担者である辻秀典を中心に行うものとする。また、研究協力者として、博士課程の学生 2 名と修士課程の学生数名が、各システム実装とその他補助を担当する。

４．研究成果

本研究では、厳密且つ安全なアクセス制御機構を応用と基盤の協調により実現し、情報システムに階層的防御網を適用する新たな OS 技術を提案した。その中核は、応用の実行状況等を考慮して動的に最小のアクセス権限を与える機構の提案と、その強固な実現手段、及びこれらを実用的なものとする、明快・簡便なポリシ記述・管理系の提案がその内容である。また、これらを Linux 上に実装し、分散トランザクション処理やクラウド環境への適用法と有効性を示した。本研究の特徴は、従来 OS では粗すぎるアクセス制御により攻撃遅延・被害局所化が機能しない問題と、SELinux に代表されるセキュア OS の細粒度アクセス制御は複雑すぎて実利用に耐えない問題の、両方を解決することにある。

初年度の研究では、汎用的基本アクセス制御アーキテクチャのうちで、アクセス権記述から認可判定機構までの一連の仕組みと、TOMOYO Linux の強制アクセス制御機構を連結し、高レベルのポリシ記述言語とその設定系を中心とした強制アクセス制御の実用的な実装を実現した。具体的には、強制アクセス制御機構に与えるポリシ記述表現を、プロトタイプ言語の拡張により実現し、その処理系を実装した。その後、拡張したポリシ記述・処理系と強制アクセス制御機構を、安全・確実に接続するパスとして、ポリシ管理用の常駐プロセスを用いる新規手法を開発した。言語拡張の要件は、実行履歴によって分類された細かなアクセス主体と、実行時パラメータや環境変数によるプログラムの実行可否を過不足なく明快に表現できることで、ポリシ管理プロセスの目的は、ポリシの差分管理に基づく前ポリシからの特定アクセス権限付加や除去、自動学習モードへの移行、特定環境条件・トリガー監視取得等を常駐しながら実行し、従来以上に細粒度化した強制アクセス制御を実用的に構成可能とすることである。

平成 25 年度は、各々のプロセスに付与するアクセス権限を動的に最小化する新規アクセス制御方式を検討し、この設計を行った。新規アクセス制御方式は、実際のプロセスやファイルが様々な状態を取り得る点に着目し、応用の実行状況等に合わせた最小のアクセス権限を指定し、これを確実に強制するように設計されている。同時に、当初の計画を変更し、新規アクセス制御方式を組み込んだ評価実験用システムの設計を行った。計画の変更は、状態分析・アクセス制御判定モジュールの実装を OS カーネル内からユーザ空間に移すことで、アクセス制御方式や、ポリシ設定の頻繁な変更・修正・テストを容易に行えることを狙ったものであるが、本研究の有効性評価は、全体モジュールをカーネル内に置いた場合の形として評価することを想定し、評価実験用システムを設計した。また、この変更と合わせて、新規アクセス制御方式の適用対象についても考察し、現実の情報システムに抵抗なく適用可能とするために、既存システムからの移行方法や既存システムとの融合手法についても検討を行った。

最終年度となる平成 26 年度は、これまでに検討・設計を行った、各々のプロセスに付与するアクセス権限を動的に最小化する新規アクセス制御方式について、Linux 上に実装した。また、前年度までに検討・設計した評価実験用システムを実装し、提案方式が効果的に機能し、安全であることを立証した上で、その有効性評価として、全体モジュールをカーネル内に置いた場合の形についても想定し、評価を行った。最後に、提案方式の適用対象についても考察し、現実の情報システムに抵抗なく適用可能とするために、既存システムからの移行方法や既存システムとの融合手法、仮想化技術への組み込み手法についても検討を行った上で、現実的な対策としてまとめあげ、最終提案を行った。

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　8　件）

① 三村守，大坪雄平，田中英彦，ファイル構造検査の悪性 PDF ファイル検知への応用，情報処理学会論文誌，査読有，Vol.55，No.10，pp.2281-2289，2014.
http://id.nii.ac.jp/1001/00106367/

② 金子朋子，山本修一郎，田中英彦，CC-Case コモンクライテリア準拠のアシュアランスケースによるセキュリティ要求分析･保証の統合手法，情報処理学会論文誌，査読有，Vol.55，No.9，pp.2602-2612，2014.
http://id.nii.ac.jp/1001/00103086/

③ 大坪雄平，三村守，田中英彦，ファイル構造検査による悪性 MS 文書ファイルの検知，情報処理学会論文誌，査読有，Vol.55，No.5，

pp.1530-1540, 2014.
http://id.nii.ac.jp/1001/00101159/

④ 三村守，大坪雄平，田中英彦，悪性文書ファイルに埋め込まれた RAT の検知法，情報処理学会論文誌，査読有，Vol.55，No.2，pp.1089-1099，2014.
http://id.nii.ac.jp/1001/00098511/

⑤ 三村守，田中英彦，多変量解析による標的型攻撃の分類，情報処理学会論文誌，査読有，Vol.54，No.12，pp.2461-2471，2013.
http://id.nii.ac.jp/1001/00096742/

⑥ 三村守，田中英彦，Handy Scissors： 悪性文書ファイルに埋め込まれた実行ファイルの自動抽出ツール，情報処理学会論文誌，査読有，Vol.54，No.3，pp.1211-1219，2013.
http://id.nii.ac.jp/1001/00091312/

⑦ 安藤類央，橋本正樹，山内利宏，仮想化技術による安全なファイルアクセスログ外部保存機構，情報処理学会論文誌，査読有，Vol.54，No.2，pp.585-595，2013.
http://id.nii.ac.jp/1001/00090264/

⑧ 原田季栄，半田哲夫，橋本正樹，田中英彦，アプリケーションの実行状況に基づく強制アクセス制御方式，情報処理学会論文誌，査読有，Vol.53，No.9，pp.2130-2147，2012.
http://id.nii.ac.jp/1001/00083922/

〔学会発表〕（計 25 件）

① 橋本正樹，滝澤峰利，高山扶美彦，辻秀典，田中英彦，SELinux ポリシ処理系のユーザ空間実装，第 26 回コンピュータシステム・シンポジウム (ComSys2014)，2014.11.20，芝浦工業大学豊洲キャンパス.
http://id.nii.ac.jp/1001/00106939/

② 橋本正樹，滝澤峰利，高山扶美彦，辻秀典，田中英彦，論理型言語による SELinux 向け認可判定機構の実装と評価，コンピュータセキュリティシンポジウム 2014 (CSS2014)，2014.10.23，札幌コンベンションセンター.
http://id.nii.ac.jp/1001/00106596/

③ 唐沢勇輔，橋本正樹，辻秀典，田中英彦，HTA ファイルを用いたワンクリック詐欺の検出手法の提案，2014 年暗号と情報セキュリティシンポジウム (SCIS2014)，2014.1.21，城山観光ホテル.

④ 堀田知宏，橋本正樹，辻秀典，田中英彦，実運用を考慮した電子メール誤送信対策，第 154 回 DPS・第 60 回 CSEC 合同研究発表会，2013.3.15，東京電機大学千住キャンパス.
http://id.nii.ac.jp/1001/00091066/

⑤ 仲間政信，橋本正樹，辻秀典，田中英彦，C&C サーバの振る舞い情報抽出システムの提案，2013 年暗号と情報セキュリティシンポジウム(SCIS2013)，2013.1.22，ウェスティン都ホテル京都.

⑥ 三村守，田中英彦，複数のエンコード方式に対応した実行ファイル自動抽出ツール，第 18 回インターネットと運用技術研究発表会，2012.6.18，東京学芸大学.
http://id.nii.ac.jp/1001/00082634/

〔図書〕（計 件）

〔産業財産権〕
○出願状況（計 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織

(1)研究代表者
田中 英彦（TANAKA HIDEHIKO）
情報セキュリティ大学院大学・情報セキュリティ研究科・教授
研究者番号：60011102

(2)研究分担者
辻 秀典（TSUJI HIDENORI）
情報セキュリティ大学院大学・情報セキュリティ研究科・客員教授
研究者番号：90398975

(3)研究分担者
橋本 正樹（HASHIMOTO MASAKI）
情報セキュリティ大学院大学・情報セキュリティ研究科・准教授
研究者番号：10582158

(4)連携研究者
原田 季栄（TOSHIHARU HARADA）
株式会社 NTT データ・技術開発本部
研究者番号：-