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１０日現在

機関番号：１５３０１
研究種目：基盤研究（Ｃ）
研究期間：2009～2011
課題番号：21500075
研究課題名（和文）　認証およびアクセス制御機能と連携したソフトウェア資産管理システム
研究課題名（英文）　A Software Asset Management System with Authentication and Access Control Functions

研究代表者
岡山　聖彦（OKAYAMA　KIYOHIKO）
岡山大学・情報統括センター・准教授
研究者番号：20252588

研究成果の概要（和文）：

ソフトウェアの不正コピー対策として、組織保有の PC にインストールされたソフトウェアの厳格な管理が求められている。しかし、既存の管理システムでは対象となる PC の管理者権限を要するため、大学のように PC の利用者が管理者であるような環境では、確実にソフトウェア情報を収集することが困難である。これに対し、我々の研究グループでは認証・アクセス制御システムと連携するソフトウェア資産管理システムの研究開発を進めており、当該研究期間においては、実用化のための機能強化および機能拡張を行う。

研究成果の概要（英文）：

Strict management of the software installed on PCs of an organization against illegal copies of software is required. However, since the existing management systems require administrative privileges of PCs, it is difficult to collect software information reliably in such an environment like universities where a user of a PC is also an administrator of the PC. To solve this problem, our research team has developed a software asset management system which works with authentication and access control systems. In the study period, we make enhancements and extensions for practical realization.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００９年度	500,000	150,000	650,000
２０１０年度	1,200,000	360,000	1,560,000
２０１１年度	1,300,000	390,000	1,690,000
総　計	3,000,000	900,000	3,900,000

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：ソフトウェア資産管理、アクセス制御、ユーザ認証

１．研究開始当初の背景

近年の情報通信技術の発展により、大学や企業などの組織が保有するソフトウェア資産は年々増加している。これに伴い、ソフトウェアの不正コピーが社会問題化するなど、組織では厳格にソフトウェア資産管理を行うことが求められている。ソフトウェア資産管理を行うためには、組織が保有するPCにインストールされているソフトウェアの一覧情報（以下、インストール情報という）を収集する必要があり、これを自動的に行うシステムがいくつか提案・実用化されている。既存のシステムでは、各PC に専用のプログラム（以下、エージェントという）を事前にインストールしておき、エージェントがインストール情報を抽出してネットワーク上の資産管理サーバに送信することにより、インストール情報を収集する。また、既存のシステムの中には、事前にPCの管理者情報を資産管理サーバに登録することにより、エージェントのインストールを省略しているものもある。

しかし、既存のシステムでは、エージェントのインストール作業や管理者情報の登録作業はPC管理者の裁量に委ねられている。このため、企業のように特定の管理部門が組織の全PCを管理するような組織では問題なく運用可能であるが、大学のように、PCの管理が教員や学生に委ねられている組織では、これらの作業を強制することが困難な場合がある。特に、PCが教員や学生の個人所有である場合はPCの存在を組織として把握できない可能性が高いため、組織のネットワークに接続するすべてのPCからインストール情報を確実に収集することができないという問題が生じる。

２．研究の目的

上述した問題に対し、我々の研究グループでは、情報コンセントの認証・アクセス制御装置と連携するソフトウェア資産管理システムの研究開発を行っている。提案システムでは、PCが組織のネットワーク（情報コンセント）に接続する際に、ユーザ認証に加えてインストール情報提出の有無を確認する。PCがインストール情報を未提出の場合には、提出するまでネットワークへのアクセスを遮断することにより、個人の持込PCからもインストール情報を強制的に収集することが可能である。

さらに、インストール情報にはPC固有の情報（MACアドレス）のみならず認証結果（ユーザIDなど）を付加することにより、何らかの不正が認められた場合は利用者の追跡も可能である。本研究課題においては、開発済みのプロトタイプシステムをベースに、実用化に向けた機能強化および機能拡張を実施する。

３．研究の方法

開発済みのプロトタイプシステムは、既存の Web ベースの認証・アクセス制御システムにインストール情報収集機能のみを追加したものである。提案システムを実用に供するためには、スケーラビリティの改善や NAT ルータ対策など、さまざまな機能強化および拡張が必要である。そこで当該研究期間においては、以下のサブテーマについて研究開発を行う。

(1) NAT ルータ対策

利用者が NAT ルータを接続した場合、NAT ルータ配下にある PC 群は基幹ネットワークから隠蔽されてしまう。このため、NAT ルータ配下の 1 台の PC がインストール情報を提出すれば、残りの PC は提出しなくてもネットワークを利用できるという問題が生じる。そこで、既存の NAT ルータの拡張により、NAT ルータ配下の PC を基幹ネットワーク側で識別できるような機能を実現する。

(2) スケーラビリティの改善

プロトタイプシステムの主要部分であるアクセス制御サーバはPCをベースに実装されているため、既存のL2/L3スイッチ間に挟み込む形で配備されることになるが、アクセス制御はIPアドレスに基づいて行われるので、複数のネットワークセグメントを集約してコストを削減することが可能である。しかし、配下にあるPC群のすべての通信がアクセス制御サーバを通過するため、PC数の増加に伴ってボトルネックとなる可能性が高い。そこで、認証機能を有するL2スイッチに資産管理サーバとの連携機能を実装するなどして、スケーラビリティの改善を図る。

(3) PCの属性に応じた制御機能の実現

大学などの組織では、学会などのイベント時に部外者がPCを持ち込んで組織ネットワークに接続することがある。また、VPN技術を利用して組織外から組織内に接続する環境を構築している場合、部内者が自宅のPCを組織ネットワークに接続することもある。これらのPCからインストール情報の提出を求めることは不適切である場合が考えられるため、認証結果や接続場所など、PCの属性に応じてインストール情報提出の必要性を制御する機能を実現する。

(4) 実証実験・性能評価

学内ネットワークに提案システムを設置し、実運用を通じて機能検証や問題点の洗い出しを行う。さらに、PC数と資産管理サーバの負荷との関係などを明らかにするための性能評価実験も実施する。

４．研究成果

前項で示したサブテーマ(1)～(4)それぞれについて、研究の成果を以下に記す。

(1) NATルータ対策

本研究では、NATルータへの対策として、レイヤ2(データリンク層)における機器の識別子であるMACアドレスに注目し、配下にあるPCのMACアドレスを上位ネットワークに伝播させるNATルータ(以下、MACアドレス中継型NATルータという)を考案した。MACアドレス中継型NATルータは、配下のPCから送出されたパケットのMACアドレスをEthernetヘッダに埋め込んだまま、上位ネットワークに中継する。これにより、上位ネットワークにあるアクセス制御サーバはパケットに埋め込まれたIPアドレスではなくMACアドレスを利用することにより、MACアドレス中継型NATルータ配下のPCを識別することが可能となる。

MACアドレス中継型NATルータを試作するため、UNIX系のOSであるFreeBSDのNATルータ機能を拡張した。FreeBSDでは、natdというプログラムがNATの機能を果たすが、FreeBSDカーネルがnatdに受信パケットを渡す際にはEthernetヘッダが取り除かれるので、natdがパケットのEthernetヘッダを読み書きできる機能を追加するとともに、IPアドレスの変換テーブルにPCのMACアドレスを保持するように拡張した。このとき、MACアドレス中継型NATルータが受信するすべてのパケットのEthernetヘッダをnatdが読み込むとスループットの低下が大きくなるため、対象をTCPのコネクション確立パケットに限定するといった工夫を施している。

試作したMACアドレス中継型NATルータを用いて動作確認実験を行い、配下のPCを上位のアクセス制御サーバが正しく識別できることと、上位のL3スイッチにおいてARPキャッシュの不整合は発生しないことを確認した。さらに、100MbpsのEthernet環境にて性能評価実験を行った結果、既存NATルータのスループットが93.92Mbpsであるのに対し、MACアドレス中継型NATルータは

93.89Mbps と、スループットへの影響はほとんどないことが判明した。本研究で考案した MAC アドレス中継型 NAT ルータについては、特許を出願(出願状況を参照)するとともに、国内外の学会および論文誌で成果発表(雑誌論文①および学会発表④⑤)を行った。

上述した MAC アドレス中継型 NAT ルータは、特定のアプリケーションに依存しない代わりに、既存の NAT ルータの置き換えを伴うため、大規模な組織ではコストが大きくなる可能性がある。これを回避するため、アプリケーション層における NAT ルータ対策手法も提案した。提案手法では、インターネットの主要なサービスの一つである HTTP(Web)において、大組織ではトラヒック低減とレスポンスタイム向上のために HTTP プロクシを設置することが多いことに注目し、HTTP プロクシにおける認証機能を拡張してクライアント PC の識別とアクセス制御を実現した。HTTP はアプリケーション層のプロトコルであるため、途中に NAT ルータがあったとしても、HTTP プロクシは NAT ルータ配下のクライアント PC と直接通信することができる。HTTP プロクシにおける認証はユーザ認証であるが、認証時に特別な識別子をクライアント PC に対して発行するように拡張することにより、HTTP プロクシがクライアント PC を識別して個別にアクセス制御することが可能となった。この研究成果については、国内外の学会（学会発表①③）で成果発表を行っている。

(2) スケーラビリティの改善

スケーラビリティの改善手法として、アクセス制御機能を L2 スイッチで実現する方法を提案した。最近は、MAC アドレス認証や WEB 認証などの機能を持つ L2 スイッチが増えており、WEB 認証機能を持つ L2 スイッチの中には外部 WEB サーバと連携できるものがある。外部 WEB サーバであれば、L2 スイッチに比べて変更・拡張が容易であるため、外部 WEB サーバにソフトウェア資産管理機能を組み込んだ。これにより、認証とソフトウェア資産管理機能を外部 WEB サーバに集約する一方、アクセス制御機能は末端の L2 スイッチに分散することにより、認証およびインストール情報提出後のトラヒックが特定のサーバに集中しないようにすることが可能となった。この成果については、国内研究会(学会発表②)で成果発表を行っている。

一方、アクセス制御機能を L2 スイッチに分散すると、PC がスイッチ間を移動した場合に、移動先 L2 スイッチで再認証を要求される場合がある。無線 LAN 環境では、無線ローミングによる移動に伴う接続先 L2 スイッチの変更をユーザが意識しないため、特に問題となりうる。これに対し、本研究では、PC が認証に成功したという情報をレイヤ 2 スイッチ間で共有する機能を認証サーバに組み込むことにより、PC がスイッチ間を移動しても、WEB 認証が再度行われないようにした。

(3) PC の属性に応じた制御機能の実現

前項のスケーラビリティ改善手法で導入した外部 WEB サーバによる認証時に、認証データベースとして LDAP あるいは Shibboleth を使用することにより、ユーザアカウントに属性情報を付加してインストール情報提出の要・不要を決定する機能を設計・実装した。これにより、組織の構成員ではないゲストユーザに対しては、インストール情報の提出を求めないような制御が可能となった。

(4) 実証実験・性能評価

アプリケーション層における NAT ルータ対策手法について性能評価実験を実施して、PC の台数が増加しても大きな性能低下は見られないことを確認した。

また、本研究期間内に開発したシステムは、いずれも研究室内での運用にとどまってお

り、所属組織である岡山大学のキャンパスネットワークでの実証実験は今後の課題である。

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１件）

① 山井成良、村上亮、岡山聖彦、中村素典、内部ネットワーク上のホストを外部から識別するためのMACアドレス中継型NATルータ、情報処理学会論文誌、査読有、52巻、3号、2011、pp. 1348-1356

〔学会発表〕（計５件）

① Y. Ishikawa, N. Yamai, K.Okayama and M. Nakamura、An Identification Method of PCs behind NAT Router with Proxy Authentication on HTTP Communication、The 11th IEEE/IPSJ International Symposium on Applications and the Internet (SAINT2011 C3NET Workshop)、2011年7月20日、Holiday Inn Hotel（ドイツ国ミュンヘン市）

② 史小文、岡山聖彦、山井成良、ソフトウェア資産管理システムにおける認証スイッチを用いたスケーラビリティの改善、情報処理学会インターネットと運用技術研究会、2011年7月15日、岡山大学津島キャンパス五十周年記念館（岡山市北区津島中）

③ 石川義基、岡山聖彦、山井成良、中村素典、HTTP通信におけるプロクシ認証を利用したNATルータ配下のPC識別手法、第9回情報科学技術フォーラム（FIT2010）、2010年9月7日、九州大学伊都キャンパス（福岡県福岡市）

④ R. Murakami, N. Yamai and K. Okayama、A MAC-address Relaying NAT Router for PC Identification from Outside of a LAN、The 2010 International Symposium on Applications and the Internet (SAINT2010 C3NET Workshop)、2010年7月19日、JW Marriott Hotel（韓国ソウル市）

⑤ 村上亮、岡山聖彦、山井成良、LAN内PCを外部から識別するためのMACアドレス中継型NATルータ、情報処理学会第2回インターネットと運用技術シンポジウム（IOTS2009）、2009年12月11日、エルフ金沢（石川県金沢市）

〔図書〕（計０件）

〔産業財産権〕
○出願状況（計１件）
名称：ネットワーク通信方法及びアクセス管理方法とパケット中継装置
発明者：山井成良、岡山聖彦
権利者：国立大学法人 岡山大学
種類：特許
番号：特願2009-259265
出願年月日：２００９年１１月１２日
国内外の別：国内

○取得状況（計０件）

〔その他〕
特になし

６．研究組織

(1)研究代表者
岡山　聖彦（OKAYAMA　KIYOHIKO）
岡山大学・情報統括センター・准教授
研究者番号：20252588

(2)研究分担者
山井　成良（YAMAI　NARIYOSHI）
岡山大学・情報統括センター・教授
研究者番号：90210319