RL-007

ソフトウェア不正コピー対策のためのLANアクセス制御システム

A LAN Access Control System Against Unauthorized Copies of Software

山本 賢 † 岡山 聖彦 ‡ 山井 成良 ‡
Satoshi Yamamoto Kiyohiko Okayama Nariyoshi Yamai

1 まえがき

近年，IT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されている[1, 2]．これらのシステムでは，各PCに専用のプログラム(以下，エージェントという)をあらかじめインストールし，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サーバに集約することにより，管理者はサーバ上のデータを集計して整合性の検査などを行うことができる．また，このようなシステムの中には，事前にPCの情報(コンピュータ名，アカウント名，パスワードなど)をサーバへ登録することにより，エージェントのインストールを不要としているものもある[3, 4](以下，これらをまとめて従来のシステムという)．

しかし，従来のシステムでは，上述したエージェントのインストール作業やサーバへの登録作業はPC管理者の裁量に委ねられている．このため，大学などのように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．

このような問題を解決するため，本研究ではソフトウェア不正コピー対策のためのLANアクセス制御システムを提案する．提案システムでは，LANアクセス制御システムにインストール情報収集機能を追加することにより，組織のネットワークに接続する(サーバなど一部のPCを除く)全てのPCからインストール情報を強制的に収集する．具体的には，PCのネットワーク接続時に利用者認証を行った上でインストール情報の提出状況を検査し，未提出であったり有効期限を過ぎている場合には，インストール情報を提出するまで外部へのアクセスを禁止する．これにより，個人所有のPCであってもインストール情報の収集を確実に行うことが可能となる．

†岡山大学大学院自然科学研究科, Graduate School of Natural Science and Technology, Okayama University
‡岡山大学総合情報基盤センター, Information Technology Center, Okayama University

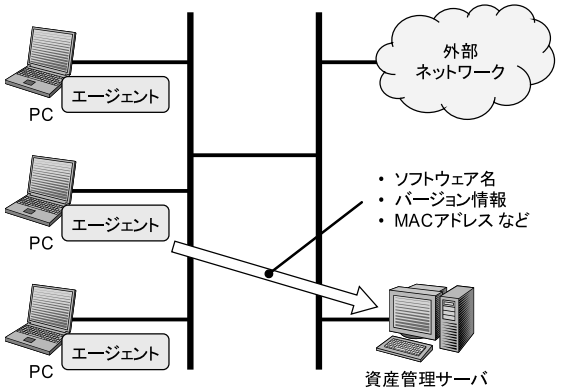

図1: エージェント常駐システム

2 従来のソフトウェア資産管理システムの問題点

従来のシステムは，管理対象となるPCに対してインストール情報を収集するためのエージェントをインストールし，そのエージェントが常駐して動作するシステム(エージェント常駐システム)と，エージェントをインストールすることなくインストール情報を収集するシステム(エージェント非常駐システム)に分類される．

エージェント常駐システムでは，あらかじめ管理対象となる全てのPCにエージェントをインストールしておく．そのエージェントは指定されたタイミングでPCのインストール情報を抽出し，サーバへ送信する(図1)．一方，サーバはエージェントから送られてくるインストール情報を蓄積し，部局や部署などの単位で一覧表示したり，ソフトウェア毎にインストールされているPCの台数を表示したりする機能を持つ．さらに，あらかじめソフトウェア毎のライセンス数を登録することにより，保有ライセンスに対する過不足を検査する機能を持つものもある．

一方，エージェント非常駐システムでは，特別なエージェントのインストールは不要である．システムは基本的にサーバのみで構成されており，PCとサーバが直接連携することによりインストール情報を収集する．例えば，NetBIOSを用いる方法では，事前に管理対象となる全てのPCの管理者権限のアカウント名，パスワードをサーバに登録しておく．そして，NetBIOSを用いて各PCに管理者権限でアクセスし，インストール情報の抽出および収集を行う(図2)．

しかし，従来のシステムはいずれも，エージェントのインストールやPC管理者情報のサーバ登録はPC管理者の裁量に委ねられているため，組織のPC管理形態によってはすべてのPCから確実にインストール情報を収集できないという問題がある．例えば，企業などのように，管理部門が全PCを集中管理するよう

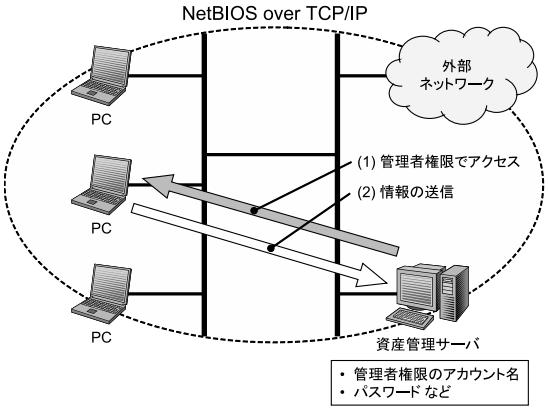

図 2: エージェント非常駐システム

な組織では問題なく運用可能であると考えられる．ところが，大学などのように部局の独自性が高い組織では，PC の管理は部局の教員や学生などに委ねられており，エージェントのインストールや PC 管理者情報のサーバ登録を強制することが困難な場合がある．特に，PC が構成員の個人所有である場合，組織としてこのような PC の存在を把握できないため，これらがソフトウェア不正コピーの温床となる可能性がある．

また，大学などの教育機関では，Windows 系 OS だけでなく，伝統的に Macintosh や UNIX 系 OS のユーザも多いため，システムはマルチプラットホーム対応でなければならない．しかし，従来のシステムの多くは Windows 系 OS を対象として開発されており，エージェントのインストールを容易にするために ActiveX を利用しているなど Windows 系 OS に大きく依存した実装となっているため，他の OS に移植することが困難であるという問題もある．

3 ソフトウェア情報収集機能を持つ LAN アクセス制御システムの提案

3.1 実現方針

前章で述べた問題点を解決するためには，インストール情報を強制的に収集する仕組みが必要である．そこで本研究では，LAN アクセス制御機能とインストール情報収集機能を組み合わせることとした．LAN アクセス制御とは，ネットワークを構成するスイッチなどの機器において，PC のネットワーク接続時に利用者認証を行い，認証に成功した PC のみに対してアクセスを許可する機能である．したがって，LAN アクセス制御を行う機器において，利用者認証と共にインストール情報の提出の有無に基づいてアクセスの可否を制御すれば，管理者が把握していない個人所有の PC についても，インストール情報の提出を強制することができると考えられる．さらに，利用者認証時のユーザ名をインストール情報と関連付けることにより，インストール情報の集計時に PC の利用者を追跡調査することも可能となる．

一方，従来システムのように，管理対象となる全ての PC にあらかじめエージェントをインストールさせる方法では，インストールの手間が大きく，個人所有の PC への対応が困難である．このため，提案システムでは Web ベースでインストール情報を収集するものとし，エージェントは Java アプレットで作成するものとした．これにより，ユーザは PC の利用者認証時に表示される Web ページをクリックするだけでエージェントのダウンロードと実行ができるため，事前インストールの必要がなくなる．

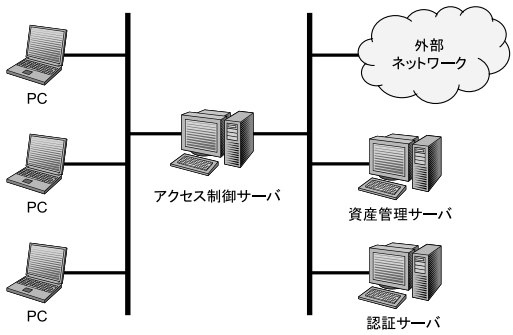

図 3: 提案システムの構成例

さらに，Java は OS への依存性が低いプログラミング言語であるため，Java アプレットに OS の判別機能と OS 毎のインストール情報収集機能を持たすことにより，単一の Java アプレットでのマルチプラットホーム対応が容易に実現できる．なお，Java アプレットを実行するためには，PC に Java ランタイム環境 (JRE) が必要である．しかし，現在では多くの Web サイトで Java の利用が一般的となっているため，JRE のインストールは運用上大きな問題にはならないと考えられる．

以下，提案システムの構成と動作手順について述べる．

3.2 システム構成

提案システムの構成例を図 3 に示す．提案システムは，既存のネットワークに対して，以下の要素を追加することによって実現する．

- アクセス制御サーバ
  PC が接続するネットワークの対外接続点に設置され，認証サーバや資産管理サーバと連携して，PC の利用者認証やインストール情報提出の有無を確認すると共に，これらの結果に基づいて PC のネットワークアクセスを制御する．
- 認証サーバ
  組織内の全ユーザのアカウント情報を持ち，アクセス制御サーバを経由して PC の利用者認証を行う．アクセス制御サーバとの通信が可能であれば，組織ネットワーク内のどこに設置してもよい．
- 資産管理サーバ
  各 PC のインストール情報を格納するデータベースであり，アクセス制御サーバと連携して，インストール情報の収集や検査を行う．組織ネットワーク内のどこに設置してもよいが，PC からインストール情報を直接受信するため，アクセス制御サーバの設定により PC とは常に通信可能でなければならない．

上述した構成要素のうち，利用者認証に基づくアクセス制御サーバと認証サーバについては，既存のシス

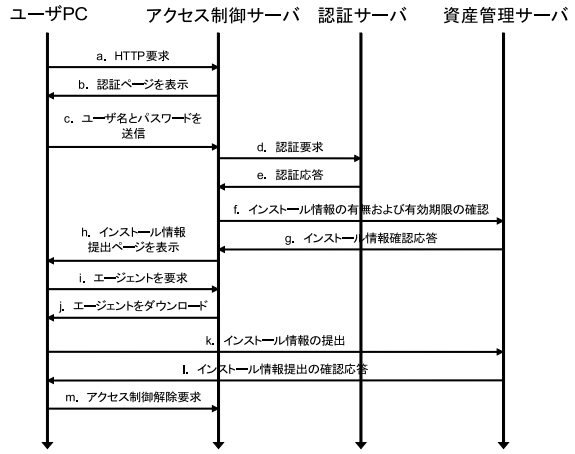

図 4: 提案システムの動作手順

テムが流用可能である．したがって，本研究ではアクセス制御サーバに対してインストール情報の検査機能を追加するものとし，資産管理サーバおよび PC で実行するエージェントを新規作成した．

3.3 PC の識別

前節で述べた通り，アクセス制御サーバは利用者認証を行うので，PC の利用者情報を得ることができる．しかし，1 人の利用者が複数の PC を利用する場合や，複数の利用者が 1 台の PC を利用する場合があるため，インストール情報は利用者単位ではなく PC 単位で管理する必要がある．TCP/IP ネットワークにおいて，PC は IP アドレスにより識別される．しかし，DHCP 環境のように，IP アドレスが動的に割り当てられる場合，PC がネットワークに接続する度に IP アドレスが変化する可能性があるので，PC 固有の情報とはいえない．一方，データリンク層レベルでは，PC はネットワークインターフェイス固有の識別子で識別される．例えば，広く普及している Ethernet であれば，PC の識別に MAC アドレスが用いられている．多くの場合，PC にはネットワークインターフェイスが内蔵されており，故障などの理由がない限り交換されないので，提案システムでは PC の識別に MAC アドレスを用いるものとし，アクセス制御サーバが利用者認証時に収集するものとする．

3.4 提案システムの動作手順

図 3 のようなネットワーク構成において，インストール情報未提出の PC がネットワークに接続する場合の動作手順を図 4 に示す．アクセス制御サーバは，初期状態では PC から外部へのアクセスを遮断しており，PC から送信される全ての HTTP 要求をアクセス制御サーバが横取りし，その応答として認証ページのコンテンツを返すものとする．また，PC の IP アドレスは手動で設定されているか，あるいは PC が直接通信可能な DHCP サーバによって動的に割り当てられる．

インストール情報未提出の PC がネットワークに接続し，アクセスが許可されるまでの処理手順は以下のようになる．

1. PC 利用者が Web ブラウザを用いて，任意の Web サイトに HTTP 要求を送信する．(a)
2. アクセス制御サーバが HTTP 要求を横取りし，認証ページのコンテンツを返す．利用者はユーザ ID とパスワードを認証ページに入力し，アクセス制御サーバ経由で認証サーバに送信する．(b，c，d)
3. 認証サーバは利用者を認証し，認証結果をアクセス制御サーバに返す．(e)
4. アクセス制御サーバは，資産管理サーバへ利用者 PC の MAC アドレスを送信する．(f)
5. 資産管理サーバは MAC アドレスに基づいてインストール情報データベースを検索し，当該 MAC アドレスに対するインストール情報がないことを確認して，インストール情報が未提出であるという結果をアクセス制御サーバに返す．(g)
6. アクセス制御サーバは，エージェントへのリンクを含むインストール情報提出ページを PC に返す．(h)
7. PC がインストール情報提出ページを受信すると，ブラウザはエージェントのリンクにしたがってアクセス制御サーバ内のエージェントを自動的にダウンロードし，実行する．(i，j)
8. PC がエージェントに含まれるインストール情報提出ボタンをクリックすると，抽出されたインストール情報が資産管理サーバに送信される．(k)
9. 資産管理サーバは提出確認応答を PC のエージェントに返す．(l)
10. PC のエージェントはアクセス制御サーバにアクセス制限の解除を要求する．(m)
11. アクセス制御サーバは PC のアクセス制限を解除し，これ以降，PC は外部ネットワークにアクセス可能となる．

なお，インストール情報は頻繁に変更されるものではないため，資産管理サーバが保存するインストール情報には有効期限を設定している．インストール情報を提出済みの PC が接続した場合，資産管理サーバはインストール情報の提出日時を検査し，管理者により設定された有効期限内であればインストール情報の再提出を求めることなく，PC のアクセス制限を解除する．

4 実装と動作確認

4.1 試作システムの実装

前章で述べたシステムの動作を検証するため，図 3 に示した構成要素のうち，アクセス制御サーバおよび資産管理サーバと，PC で実行されるエージェントを実装した．なお，認証サーバには既存の LDAP サーバをそのまま利用している．

4.1.1 アクセス制御サーバ

アクセス制御サーバには，情報コンセント用アクセス制御システムとして知られている Opengate[5] を拡張したものを用いた．Opengate は，PC が接続するネットワーク機器と外部ネットワークとの接続点に設置され，PC 接続時に Web ベースで利用者認証を行うシステムである．また，アクセス制御サーバを実装する OS として，ブリッジ動作，すなわち一方のネットワークインターフェイスから入力された Ethernet フレームを

もう一方のネットワークインターフェイスにデータリンク層レベルで転送可能な FreeBSD 4.11 を用い，Web サーバには Apache2 [6]，ファイアウォールには ipfw を用いた．本研究では，利用者認証後にソフトウェア資産管理に関する Web ページを表示させる機能を Opengate に追加すると共に，アクセス制御解除のタイミングを利用者認証成功時からインストール情報の提出確認時へ変更した．

4.1.2 資産管理サーバ

資産管理サーバは，エージェントからインストール情報とアカウント情報を受信し，PC 毎にファイルとして保存する．DHCP 環境にも対応するため，インストール情報のファイル名として PC の MAC アドレスを付与するものとした．これにより，インストール情報の検索は MAC アドレスをキーとしたファイル検索，有効期限の確認はファイルの更新日時を現在の日時と比較することにより，容易に実現できる．

本研究では，資産管理サーバを Linux 上で動作するプログラムとして，C 言語および Java 言語により作成した．

4.1.3 エージェント

本研究では，OS への依存度が低いエージェントを実現するために，エージェントを Java アプレットとして作成した．このアプレットは実行時に Java の機能を用いて OS を判別し，OS 毎に異なる方法を用いてインストール情報を抽出する．現時点で対応している OS とインストール情報の抽出方法の概略を以下に示す．

- Windows 2000/XP/Vista
  インストーラを利用してインストールされたソフトウェアは，レジストリにソフトウェア名，バージョン情報などが保存されているので，レジストリを走査するための Windows API を用いることによりソフトウェアの一覧情報を取得する．
- MacOX 10.5.1
  OS 標準のシステム情報管理ユーティリティである System_Profiler を外部コマンドとして実行し，ソフトウェアの一覧情報を取得する．
- Linux Red Hat 系/Debian 系
  Red Hat 系ディストリビューションについては RPM を，Debian 系ディストリビューションについては dpkg を外部コマンドとして実行し，ソフトウェアの一覧情報を取得する．

なお，セキュリティ上の理由から，標準では Java アプレットの機能は制限されており，レジストリの読み込みや外部コマンドの実行は許可されていない．しかし，電子署名の施された Java アプレットではこのような制限を受けないため，本研究では電子署名付きの Java アプレットをダウンロード，実行させるものとした．

4.2 動作確認実験

提案システムの動作を確認するため，4.1.3 節に示した OS が動作する PC を 5 台用意して図 3 と同様の実験ネットワークを構築し，以下の実験を行った．

表 1: 実験に使用した OS

OS	ブラウザ	JRE
Windows Vista Business	IE7, Firefox2	1.5, 1.6
Windows XP Professional SP2	IE7, Firefox2	1.5, 1.6
Windows XP Home SP2	IE7, Firefox2	1.5, 1.6
Windows 2000 Professional SP4	IE6, Firefox2	1.5, 1.6
MacOS X version 10.5.1	Safari3, Firefox2	1.5
fedora 8	Firefox2	1.6
Ubuntu 7.10	Firefox2	1.6

- OS 対応確認実験
  表 1 に示す各 OS についてインストール情報未提出の状態でネットワークに接続し，インストール情報が取得できるか確認した．
- 同時接続実験
  インストール情報未提出の PC と提出済みの PC を混在させ，複数の PC をほぼ同時にネットワークに接続することを繰り返し試みた．

上記の実験を行った結果，OS 対応確認実験では，実験に使用した OS，ブラウザ，JRE の組み合わせに関しては正しくインストール情報の抽出および提出ができることを確認し，アクセス制御も正しく行われていることを確認した．また，同時接続実験では，インストール情報未提出の PC およびインストール情報の有効期限切れの PC が接続した場合には，インストール情報が資産管理サーバに提出されるまで外部ネットワークに接続できず，インストール情報を提出済みで有効期限内の PC については，利用者認証のみで外部ネットワークに接続できることを確認した．

5 あとがき

本論文では，インストール情報を確実に収集するための LAN アクセス制御システムを提案し，試作システムを実装してその動作確認を行った．

今後の課題として，試作システムでは PC と外部ネットワークとの通信が全てアクセス制御サーバを経由するため，同時接続する PC の数が増加するとアクセス制御サーバがボトルネックになる可能性がある．このため，今後は通信性能に関する評価を行うと共に，PC が直接接続するスイッチにおいてアクセス制御を行う方法などについても検討する予定である．

参考文献

[1] 内田洋行，“ASSETBASE”，http://www.asset-base.jp/.
[2] 株式会社ハンモック，“Asset View HYPER”，http://www.hammock.jp/asset/.
[3] 株式会社デジベリー，“Asset Tracker”，http://www.digiberry.com/assettracker/.
[4] 株式会社蒼天，“LogVillage”，http://www.so-ten.co.jp/products/logvillage/.
[5] 渡辺義明，渡辺健次，江藤博文，只木進，“利用と管理が容易で適用範囲が広い利用者認証ゲートウェイシステムの開発”，情報処理学会論文誌，Vol42，No.12，pp.2802–2809，2001.
[6] Apache Software Foundation, The apache web server，http://www.apache.org/.