資産管理に基づく適切なソフトウェア配布システムの構築

Construction of a software distribution system based on software asset management

松平 拓也†，車古 正樹†，笠原 禎也†，髙田 良宏†，井町 智彦†
Takuya MATSUHIRA†,Masaki SHAKO†, Yoshiya KASAHARA†
Yoshihiro TAKATA†,Tomohiko IMACHI†

takusng@kenroku.kanazawa-u.ac.jp, shako@office0.ipc.kanazawa-u.ac.jp, kasahara@is.t.kanazawa-u.ac.jp
yosihiro@kenroku.kanazawa-u.ac.jp, imachi@kenroku.kanazawa-u.ac.jp

†金沢大学総合メディア基盤センター

†Information Media Center of Kanazawa University

概要

金沢大学総合メディア基盤センターでは，ウイルス対策ソフトウェア等のセキュリティ対策ソフトウェアを中心に，学内教職員ユーザに対して配布している．また，金沢大学では 2008 年よりソフトウェア資産管理を全学的に開始し，全学の PC の台数やソフトウェアライセンスの管理を行っている．ソフトウェア資産管理では，PC に対して固有の ID が割り当てられる．そこで，ソフトウェア配布の際にユーザ認証と併せてその ID を利用することで，インストールした PC を把握できるソフトウェア配布システムを構築した．

本稿では, 構築したソフトウェア配布システムについて説明し, システムのユーザ認証についても述べる．

キーワード

ソフトウェア資産管理，シングルサインオン，LDAP サーバ

Abstract

Information Media Center of Kanazawa University is taking charge of distributing security measures software such as antivirus software. In addition, software asset management is started this fiscal year, and the numbers of PC and software license in all faculties are managed. Due to the software asset management, a unique ID is assigned to a PC. By combining the ID with user authentication, we developed a new software distribution system. In the new system, we can identify PC and installed software which was downloaded through our system.

In this paper, we introduce the configuration of the new system, and authentication mechanism implemented in it.

Keywords

Software asset management, Single Sign On, LDAP Server

1. はじめに

金沢大学総合メディア基盤センター（以下，センターと呼ぶ）では，ウイルス対策ソフトウェアやファイル暗号化ソフトウェア等のセキュリティ対策ソフトを中心に，学内教職員ユーザ（金沢大学が雇用している教職員，以下，ユーザと呼ぶ）に対して配布するサービスを行っている．ソフトウェアを配布する際には，配布したソフトウェアがどのPCにインストールされているかを把握する必要があり，これまではその方法として，ユーザ認証とPCのIPアドレスで管理していた．

一方，金沢大学では2008年7月1日より，ソフトウェア資産管理（以下，資産管理と呼ぶ）の調査を全学的に開始し，大学所有のPCやソフトウェアライセンスの管理を行っている．この資産管理により，PC，ソフトウェアといった資産を誰が管理しているか把握できるよう，資産全てに対して管理者を特定可能な固有のIDを割り当てた．

このことで，ユーザに対して，認証と併せて資産管理上のPC固有のIDを入力させ，誰がどのPCにインストールしたかまで把握できるソフトウェア配布システムが構築できるようになった．また，センターでは大学における認証のあり方について研究開発を進めている．今回，本システムのユーザ認証部分にCentral Authentication Service[1][2][3]（以下，CASと呼ぶ）を用いて，シングルサインオン環境を実現した．

本稿ではまず，資産管理の際に必要になる様々なIDについて説明した後，ソフトウェア配布システムの概要について説明し，実装について述べる．また，システムにアクセスする際のユーザ認証についても述べる．

2. ソフトウェア配布システム

本章では，ソフトウェア配布システムを使用する際に必要となる各種ID，システムを構成するサーバについて説明する．そして，ユーザがシステムからソフトウェアをダウンロードするまでの流れについて述べる．

2.1. システムにおけるIDの役割

ソフトウェア配布システムにおいては，ネットワークID，資産管理用管理者ID（以下，管理者IDと呼ぶ），機器ID，ソフトウェアIDを使用する．以下にそれぞれのIDの役割について説明する．

(1) ネットワークID

ネットワークIDは，ユーザがセンターで提供しているサービスを利用する際に使用する識別子である．学内のネットワークを利用する際の認証や，学外から学内のネットワークを利用する際の認証（VPN）に使用する．職員番号等，ユーザ固有のIDを認証に利用すると，万一情報が漏れた場合にIDを変更できない。そこで自身で登録・変更可能なネットワークIDを使用することでセキュリティが向上する．

(2) 管理者ID

管理者IDは，資産管理の際に用いるユーザ固有の識別子である．管理者IDは教職員のみ取得可能としている．管理者IDは職員番号を基に，独自に作成した計算式を用いて一意の値になるように生成している．この変換は，運用上の必要性から可逆なものとしているが，推定を困難とするに十分な複雑さを持たせている．職員番号やネットワークIDではなく管理者IDを別途設けるのは，後述する機器IDやソフトウェアIDはPC，ソフトウェアパッケージ等にラベルとして貼り付ける必要があり，第三者に見られた場合，パスワード総当たり攻撃などに悪用される危険性があるからである．

資産の中には部局等で管理しているものも存在するため，組織単位でも管理者IDを取得できるようにしている．センターから配布しているソフトウェアも組織単位の管理者IDで管理している．

(3) 機器ID

機器IDは，それぞれの管理者が管理している大学所有のPC全てに対して割り当てる識別子である．機器IDの決定は管理者IDを使用し，「H_管理者ID_001」のように割り当てる．

(4) ソフトウェアID

ソフトウェアIDは機器ID同様，それぞれの管理者が管理している大学所有のソフトウェア全てに対して割り当てる識別子である．ソフトウェアIDの決定においても管理者IDを使用し，「S_管理者ID_001」のように割り当てる．例として，センターで管理しているソフトウェアは「S_センターの管理者ID_001」というようになる．

2.2. システム概要

ソフトウェア配布システムの概念図を図 1 に示す．ソフトウェア配布システムは，アカウントサービスシステム，アカウント管理システム，LDAP サーバ，管理者 ID 発行システム，CAS サーバ，ソフトウェア配布サーバから構成される．なお，図中の矢印 A はネットワーク ID 登録，矢印 B は管理者 ID 発行，矢印 C はソフトウェアダウンロードの流れをそれぞれ示している．

以下で各サーバの概要について説明する．

2.2.1. アカウントサービスシステム

アカウントサービスシステムは，ユーザがネットワーク ID を登録するためのシステムである． Web ブラウザから本システムにアクセスして，必要な情報を入力することでネットワーク ID を取得することができる．管理者 ID を発行する際には，ネットワーク ID とパスワードで認証し本人確認を行うため，管理者 ID 発行に先立ち，本システムにアクセスする必要がある．

2.2.2. アカウント管理システム

アカウント管理システムはアカウントサービスシステムで入力された情報を LDAP サーバ等のディレクトリサーバに反映させるシステムである．入力された情報は複数のディレクトリサーバに登録される必要があるため，本システムを用いて情報を同期させている．

2.2.3. LDAP サーバ

LDAP サーバは，アカウント管理システムから送られてきた情報を格納するディレクトリサーバである．LDAP サーバは，ネットワーク ID の他，職員番号や雇用形態等の情報も保持している．

2.2.4. 管理者 ID 発行システム

管理者 ID 発行システムは，ユーザの資産管理における管理者 ID の発行を行う．ネットワーク ID とパスワードでユーザ認証を行い，認証に成功した場合に管理者 ID を発行する．なお，認証を行うための情報は LDAP サーバから取得している．

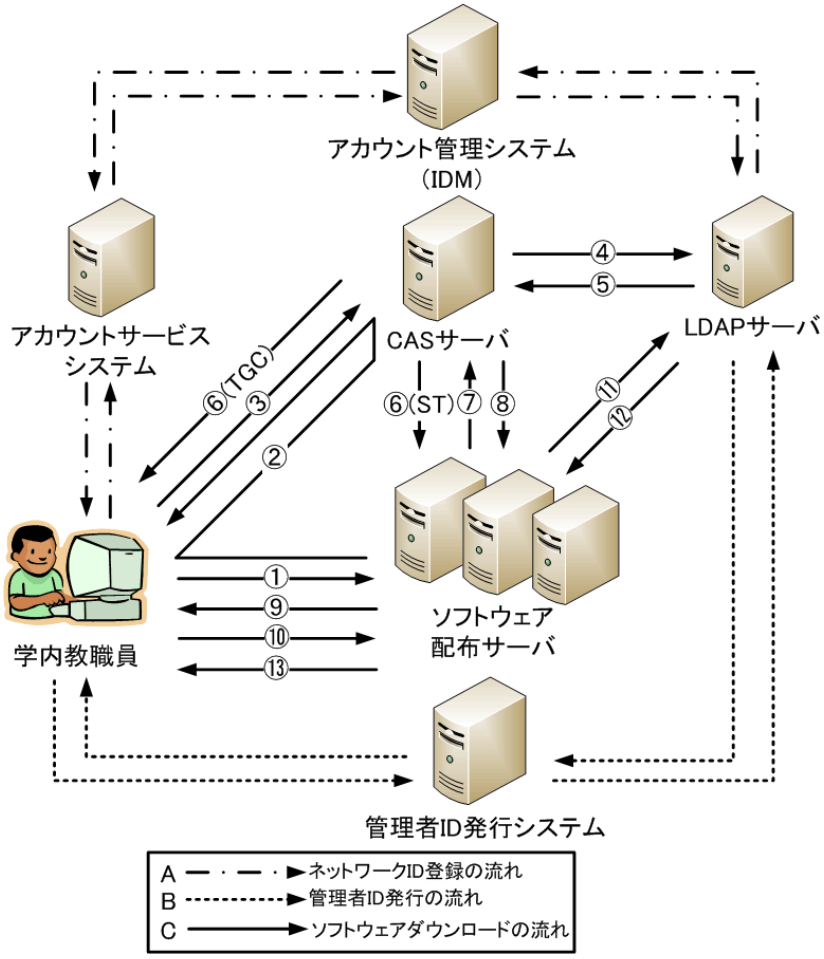

図 1　ソフトウェア配布システム概念図

2.2.5. CAS サーバ

ソフトウェア配布サーバでは，適切なユーザであることを確認するためにネットワーク ID とパスワードを用いたユーザ認証を行う．しかし，Web アプリケーション毎に認証を実装していては，システム管理者にかかる負担が大きく，また，ユーザシステム毎に認証を行うことには煩雑さを感じるものと思われる．そこで，ソフトウェア配布サーバにおける認証に CAS を用いて，シングルサインオン環境を導入した．

CAS は Java Architecture Special Interest Group（JA-SIG）が開発している Web ベースのアプリケーションで，シングルサインオン環境を実現できるオープンソースソフトウェアである．CAS サーバを用いて認証を行う Web アプリケーションを CAS クライアントと呼ぶ．CAS クライアントには PHP，Perl，Apache 等の多様な種類のライブラリが用意されているため，様々なシステムに容易に導入することができ，管理者の負担を軽減できる．

また，ユーザにおいても一度の認証手続きで複数のサービスを受けられるようになり，煩雑さが軽減される．なお，CAS サーバ自身は認証に必要な情報を持たないため外部データを利用する必要があり，本システムにおいては先に述べた LDAP サーバを利用している．

2.2.6. ソフトウェア配布サーバ

ソフトウェア配布サーバは，ソフトウェアをユーザに対して配布するサーバであり，ユーザインターフェースもここが担当する．

ソフトウェア配布サーバの Web アプリケーションはすべて CAS クライアントを実装しているため，最初のアクセスではネットワーク ID とパスワードによる認証が必要であるが，セッションを切らない限りはそれ以上の認証手続きを行う必要はない．認証が成功した場合，ダウンロード画面を表示し，ログインしたネットワーク ID に対応する機器 ID を入力させる．CAS クライアントは CAS サーバでの認証時に入力されたネットワーク ID の情報を参照し，ネットワーク ID をキーとして LDAP サーバに職員番号をバインドする．そして，それを基に該当ユーザの管理者 ID を生成し，機器 ID が正しいものであるかを判断し，正しい場合のみダウンロードを許可する．

2.3. 動作手順

ユーザが，必要とするソフトウェアをダウンロードするまでの動作手順をフローチャートにしたものを図 2 に示す．

ソフトウェア取得手続きに先立ち，ユーザはアカウントサービスシステムにアクセスし，ネットワーク ID を登録する．登録した情報は，アカウント管理システムから LDAP サーバに反映される．次に，管理者 ID 発行システムにアクセスし，登録したネットワーク ID とパスワードで認証を行い，管理者 ID を取得する．ここまでの動作は一度行えば今後行う必要はない．

ネットワーク ID と管理者 ID を取得したユーザはソフトウェア配布サーバにアクセスする．既に CAS サーバで認証済みの場合は，ここでの認証手続きは不要である．CAS サーバで認証を行っていない場合は CAS サーバの認証画面にリダイレクトされる．そこで，ネットワーク ID とパスワードを入力し，認証手続きを行う．認証に成功すると，該当ソフトウェアのダウンロード画面を表示する．ユーザはインストールする PC の機器 ID を入力し，ダウンロードボタンをクリックする．ソフトウェア配布サーバはアクセスしているユーザのネットワーク ID と入力した機器 ID が整合しているかを確認する．確認は，LDAP サーバから抽出した職員番号から管理者 ID を生成し，機器 ID の管理者 ID 部分が食い違っていないかを判定することで行う．

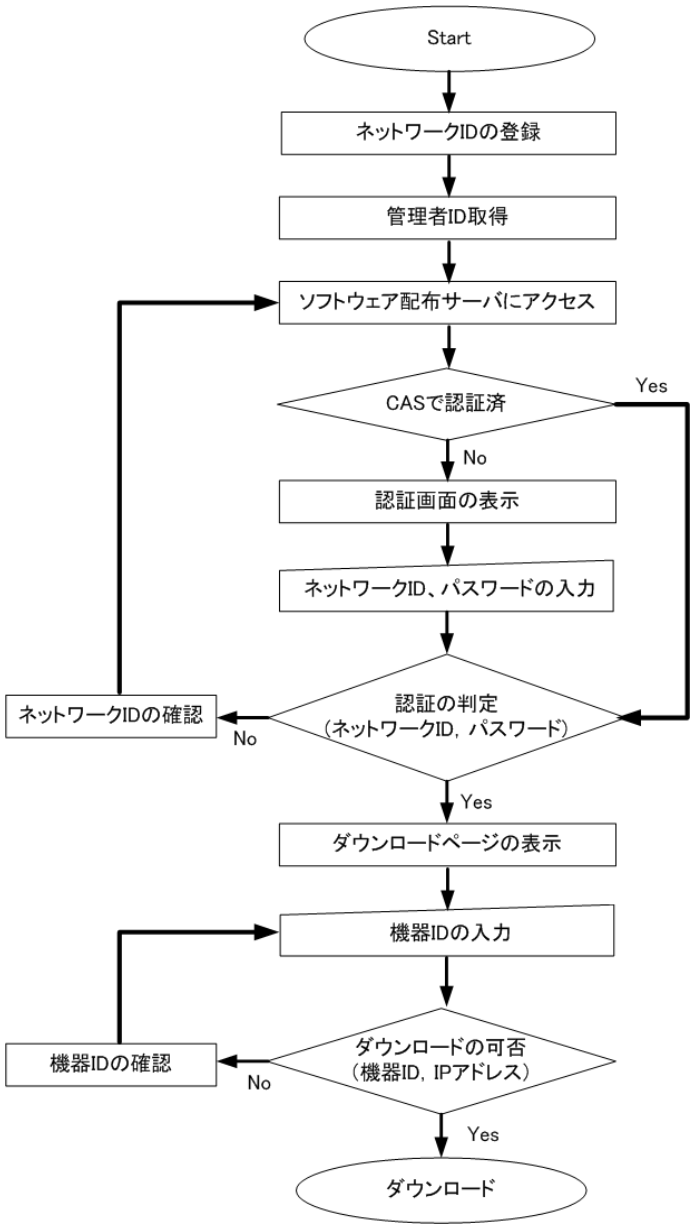

図 2　動作手順

利用記録は機器 ID をキーとして行う．アクセス元 IP アドレスで管理を行った場合，プライベートネットワーク配下の PC には対応できない問題があったが，機器 ID を用いることで，PC を一意に特定して記録することができる．

3. 実装

2 章で説明した内容を基に，ソフトウェア配布システムの実装を行った．システム概念図（図 1），動作手順（図 2）の流れに合わせて説明する．

3.1. 各サーバのスペック

実装を行った各サーバのスペックを示す．

[アカウントサービスシステムサーバ]
機種：PRIMEPOWER450
OS：Solaris10
CPU：SPARC64 V 1.98GHz×2
メモリ：6GB
ソフトウェア：Interstage Application Server Standard -J Edition V8.0[4]

[アカウント管理システムサーバ]
機種：PRIMEPOWER450
OS：Solaris10
CPU：SPARC64 V 1.98GHz×2
メモリ：6GB
ソフトウェア：Interstage Application Server Standard -J Edition V8.0

[LDAP サーバ]
機種：Sun Fire T2000
OS：Solaris10
CPU：UltraSPARC T1 1.0GHz
メモリ：8GB

[管理者 ID 発行システムサーバ]
機種：PRIMERGY　RX200
OS：Red Hat Linux Enterprise4
CPU：Zeon 1.60GHz
メモリ：2GB

[CAS サーバ]
機種：JCS Type 1U-XEF
OS：CentOS5.0
CPU：Zeon 2.66GHz
メモリ：2GB

3.2. システム実装

次に実装部分をシステムの流れに沿って説明する．
アカウント管理システムにおいては，アカウントサービスシステムで入力された情報を複数のディレクトリサーバで同期させる．アカウント管理システムとして，ディレクトリ統合管理システムである Sun Java System Identity Manager 6.0[5]（以下，IDM と呼ぶ）を使用している．アカウントサービスシステムで入力した情報を IDM のアカウントサービスシステム連携処理モジュールに送り，IDM エンジンから各ディレクトリサーバに登録する．なお，ソフトウェア配布システムではLDAP サーバの情報を参照するため，LDAP サーバのシステム構成を説明する．LDAP のソフトウェアとして，Sun Java Directory Server 5[6]を使用している．LDAP サーバは重要な情報を保持しているため，図 3 に示すように 4 台で構成しており，LDAP マスタサーバを 2 台構成とし，データ書き込み機能を冗長化（マルチマスタ）している．

管理者 ID 発行システムは Apache で Web サーバを構築し，PHP を使用して Web アプリケーションを作成している．管理者 ID 発行システムにアクセスすると図 4 の画面を表示し，ユーザにネットワーク ID とパスワードを入力させる．LDAP サーバから情報をバインドし，正しい場合は図 5 に示す管理者 ID 取得画面を表示する．

ソフトウェア配布サーバにおける Web アプリケーションは，PHP，Perl，Apache，Asp のライブラリを利用して CAS クライアントを実装している．CAS サーバのソフトウェアはバージョン 3.2.1 を使用している．そして，CAS サーバが利用不可になった場合を想定し，同一の設定の CAS サーバをコールドス

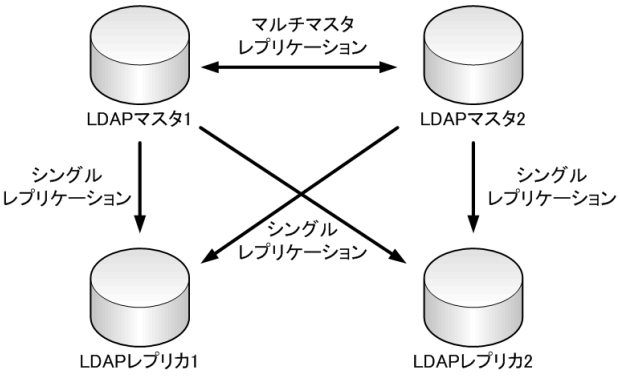

図 3　LDAP 構成図

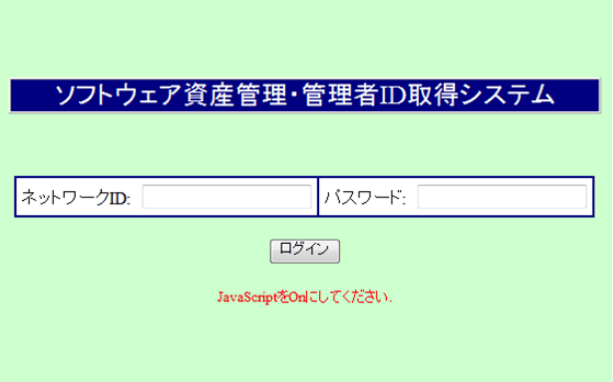

図 4　管理者 ID 発行システムログイン画面

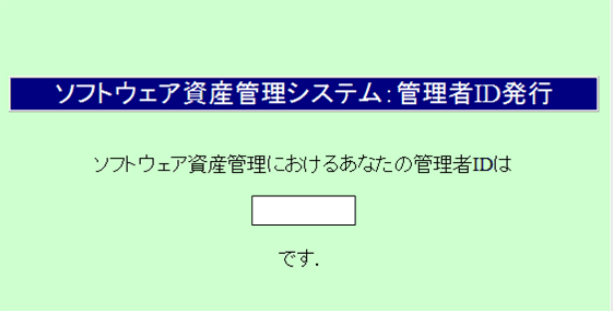

図 5　管理者 ID 発行システム ID 発行画面

タンバイさせている．

ユーザがソフトウェア配布サーバからダウンロードするまでの動作を図 1 の矢印 C に基づき説明する．説明文中の括弧内の数字は，図 1 に記載された矢印の番号と対応する．

ここでは

ソフトウェア配布サーバの URL は

https://app.oooo/dl.php

CAS サーバの URL は

https://cas.oooo/

であるものと仮定する．

最初にユーザは https://app.oooo/dl.php にアクセスする（①）．最初は認証を行っていないため，CAS クライアントは https://cas.oooo/login に通信をリダイレクトし，その際に service パラメータとして自身の URL である https://app.oooo/ dl.php を挿入し，CAS サーバに再転送先の URL を伝える．すなわち，ユーザの Web ブラウザは URL https://cas.oooo/login?service =https://app.oooo/dl.php を受け取り，図 6 に示す認証画面を表示する（②）．認証画面において，ユーザは自分のネットワーク ID とパスワードを入力すると（③），CAS サーバは外部認証サーバ（LDAP サーバ）で，ユーザから入力された情報が正しいか認証を行う（④，⑤）．認証に成功すると，CAS サーバはユーザの Web ブラウザに対して，Ticket Granting Cookie（TGC）と呼ばれる，ブラウザが認証済みかを判断するクッキーを配布し，service パラメータで指定した URL に対するリダイレクションを行う．URL には ticket パラメータとして Service Ticket（ST）と呼ばれる CAS クライアントにアクセスする際のワンタイムチケットが含まれる．つまり，https://app.oooo/?ticket=ST-xxxxxxx の形になる（⑥）．ticket パラメータを受理したソフトウェア配布サーバは ST を CAS サーバに送付する（⑦）．CAS サーバは Validation サーブレットで ST に問題が無いことを確認し，認証を行ったユーザの情報をソフトウェア配布サーバに送る（⑧）．ソフトウェア配布サーバはユーザの Web ブラウザに図 7 に示すようなダウンロード画面を表示させる（⑨）．

ダウンロード画面においてユーザが連絡先 E-mail アドレスと，ダウンロードするソフトウェアをインストールする PC の機器 ID を入力すると（⑩），ソフトウェア配布サーバは，参照可能なネットワーク ID を基に，LDAP サーバから職員番号をバインドする．そして該当ユーザの管理者 ID を生成し，機器 ID として使用している管理者 ID が正しいものであるかを検証し（⑪，⑫）ダウンロードを許可する（⑬）．以上の仕組みにより，ユーザ及び機器 ID の正当性が検証でき，配布したソフトウェアを誰がどの PC にインストールしたかを把握することができる．

図 6　CAS 認証画面

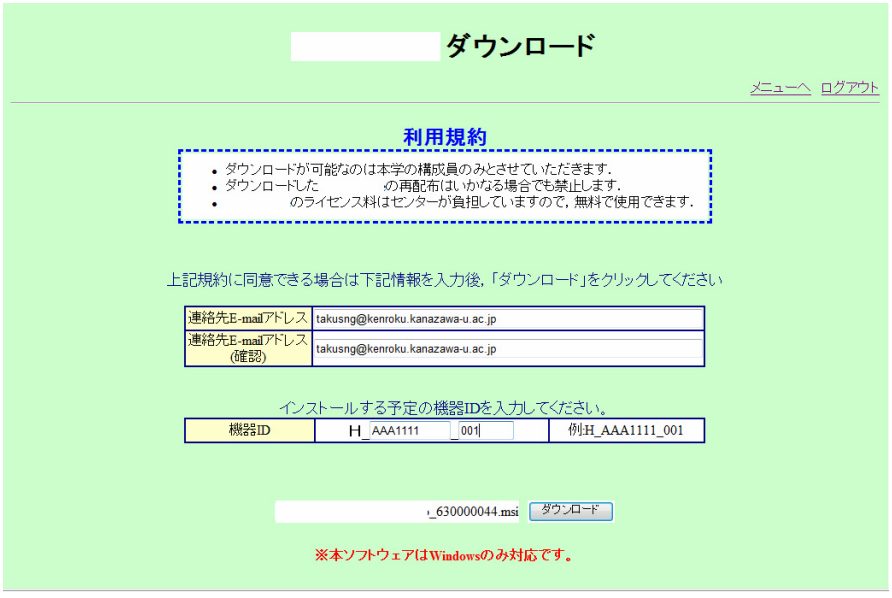

図 7　ソフトウェアダウンロード画面

3.3. 運用状況

ソフトウェア配布システムは 2008 年 4 月 1 日から 6 月 30 日まではセンター内でテストを行い, 2008 年 7 月 1 日のソフトウェア資産管理施行と共にテスト版として公開している．現在，ソフトウェア配布サーバは 3 式, 5 つの Web アプリケーションで CAS クライアントの実装を行い，運用を行っている．

4. まとめ

今回，資産管理に伴い，大学所有の全ての PC とソフトウェアに ID を割り当てることで，誰がどの PC にセンター配布のソフトウェアをインストールしたかを把握できるシステムを構築した．また，資産管理において，職員番号やネットワーク ID を直接利用する代わりに管理者 ID を別途設けたことにより，セキュリティを保てることができた．そして，ソフトウェア配布サーバでの認証をシングルサインオンとしたことで，ソフトウェアの種類やソフトウェアサーバが増えても認証の実装が容易になり，ユーザの認証による煩雑さも解消することができた.

今後の課題として，ユーザがアンインストールを行った場合のライセンス管理の対応があり，これを上手くシステムに組み込む必要がある．また，現在の CAS サーバでのシングルサインオンは認証（Authentication）のみをサポートしており，認可（Authorization）については職員，学生のみの判断をしているだけである．近年，シングルサインオンの構築においては，認証は当然で，認可をどのように管理するかに注目が集まっている．そのため，今後は複雑な認可においても対応可能なシングルサインオン環境の構築を行っていきたいと考えている．

参考文献

(1) JA-SIG(Java Architecture Special Interest Group) : http://www.ja-sig.org/products/cas/

(2) 内藤久資，梶田将司，小尻智子，平野靖，間瀬健二：“大学における統一認証基盤としての CAS とその拡張”，情報処理学会誌，Vol. 47, No. 4，pp.1127-1135 (2006)

(3) 梶田将司，内藤久資，小尻智子，平野靖，間瀬健二：“CAS によるセキュアな全学認証基盤の構築”, 情報処理学会研究報告, Vol.2005, No.39, pp.35-40 (2005)

(4) Fujitsu : ”Interstage Application Server” http://interstage.fujitsu.com/jp/apserver/

(5) Sun Microsystems : “Sun Java System Identity Manager” http://jp.sun.com/products/software/identity/identity_mgr/

(6) Sun Microsystems : “Sun Java Directory Server” http://jp.sun.com/products/software/identity/directory_srvr_ee/