学内ネットワークの安全性向上を目指したアクセス制御と脅威検知の導入

宮 下 健 輔[†1]

京都女子大学では2007年8月に学内ネットワークを更改し，幹線経路の広帯域化および耐故障性と安全性の向上を実現することで，より安全で快適な学内ネットワークを構築した．これらのうち安全性を向上するために導入されたのがMACアドレス認証とWWWによるユーザ認証を併用したネットワークアクセス制御機構および振る舞い検知を利用した脅威検知機構である．前者は一部校舎で学内ネットワーク更改当初から運用し，2008年1月より全学的に運用を開始した．また後者は学内ネットワーク更改当初から全学的に運用されている．本稿では両機構の実現と本格運用までの経緯を述べ，運用開始から半年余を経て知見した効果および問題点について報告する．

Deployment of Access Control and Threat Inspection into Campus Network System toward the Security Improvement

KENSUKE MIYASHITA[†1]

In Kyoto Women's University, the author has renewed the campus network system in August of last year. In this renewal the author has deployed the backbone network with wider bandwidth and realized a better extent of fault-tolerance and security implovement. The security implovement has been realized by access control and threat inspection. The former has been deployed in this January by MAC address authentication and user authentication via WWW. The latter is one of behaviour-based inspection systems and has been deployed with the campus network renewal. In this paper, the author describes the deployment and operation of above systems and reports the pros and cons of them he has met with in more than a half year of operation.

1. はじめに

京都女子大学は文学部，家政学部，現代社会学部，発達教育学部と短期大学部からなる女子大学である．京都女子大学では2000年度に本格的な学内ネットワークシステム（Kyoto Women's university Integrated Information Network System，以下KWIINSという）を構築した．KWIINSはほぼ全学を網羅するネットワークであり，ユーザアカウント数は学生や研究生が約6000，教職員と非常勤講師が約1000である．KWIINSのサーバ群は2006年3月から4月にかけて更改され[1),2)]，2007年8月にはKWIINSのネットワーク機器群が更改された[3)]．これら2つの更改によってKWIINSはKWIINS 2.0となり，幹線経路の広帯域化および耐故障性と安全性の向上を実現した．ここで安全性とは，第三者からの攻撃やウイルス感染等の不安のないネットワーク利用をどの程度保証できるかを表わす．

KWIINS 2.0における安全性は，ネットワークアクセス制御と脅威検知の2つの機構を導入することでKWIINSに比べて向上している[3)]．ネットワークアクセス制御機構は，ネットワークの末端に設置したL2スイッチの各ポートにてネットワーク利用開始時にMACアドレス認証とユーザ認証を行なうことで実現した．また，脅威検知には専用アプライアンスを利用し，ネットワークに接続された機器の通信を監視することにより脅威となる可能性のある機器の振る舞い

†1 京都女子大学現代社会学部
Kyoto Women's University, Faculty for the Study of Contemporary Society

を検知する仕組みとした．

これらの2つの機構のうちネットワークアクセス制御機構は一部校舎でKWIINS 2.0運用当初から開始し，2008年1月より全学的に運用を開始した．これは，全学的な運用開始に必要となる学内ネットワーク運用規則変更のための議論や手続きに時間を要したためである．また，脅威検知機構はKWIINS 2.0運用開始当初から動作させている（こちらは運用規則の変更が不要であったため）．そのため，2008年9月現在でネットワークアクセス制御機構は本格運用から8ヶ月余，脅威検知機構は約1年を経ている．

本稿では，KWIINS 2.0の概要を紹介し，上記2つの機構の導入から運用までの経緯と運用開始後からこれまでの状況について具体的に述べる．

2. KWIINSとKWIINS 2.0

この節ではKWIINS 2.0の概要を，適宜KWIINSと比較しながら紹介する．

2.1 特　　徴

KWIINS 2.0のネットワーク構成の概要を図1と図2に示す．図1は幹線経路を含む主な校舎間のネットワーク構成であり，学内のほぼすべての校舎と学生寮を接続している．図2はそれらの校舎や学生寮の内部のネットワークを模式化したもので，L3スイッチやL2スイッチを経由して建物内に入ったネットワークはフロアスイッチとエッジスイッチを通じて末端に達している．

KWIINS 2.0は主に以下のような特徴を持つネットワークである．

- 学外とはSINETおよび商用回線を通じて各々100Mbpsで接続している．
- 学内はすべてプライベートアドレスで運用し，学外との通信はNAT（アドレス変換）を利用している．
- 基幹L3（Layer 3）スイッチは6台あり，各校舎に分散配置されている．
- 各L3スイッチはWDM（波長分割多重方式）を用いて各々2Gbpsの帯域で接続されている．
- 各L3スイッチを結ぶ幹線経路はすべて二重化されている．
- 各L3スイッチの下流に建物ごとやフロアごとのL2スイッチが合計約80台配置されている．

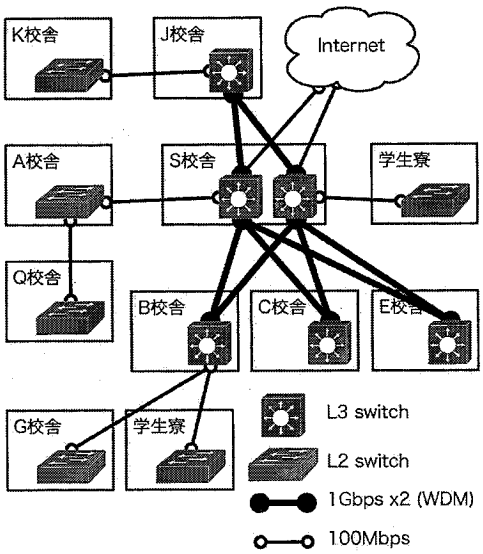

図1　幹線経路と主な建物間のネットワーク

- L2スイッチから情報コンセントまでは100Mbpsで接続している．
- 情報コンセントは学内ほぼすべての教室や研究室，事務室等に1つ以上ずつ配置されている．
- ネットワークアクセス制御機構と脅威検知機構を有する．
- 1つの校舎と学生寮にだけ無線ネットワークが存在する．

KWIINS 2.0の範囲はKWIINSと変わらず，学外との接続に用いているルータからサーバ群を経て各研究室や教室，事務室等にある情報コンセントまでとしている．つまり，各校舎をつなぐ幹線経路や建物内のフロア間ネットワーク等はKWIINS 2.0に含むが，研究室内で教員が接続したPCやプリンタ等の機器はKWIINS 2.0に含まない．

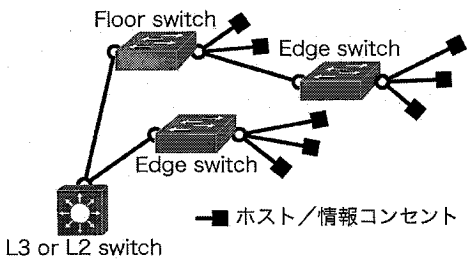

図2　建物内のネットワーク

2.2 運用管理体制

KWIINS 2.0 は KWIINS と同じ体制（教員 2 名，1 つの事務部署および委員会）で運用管理が行なわれている．

教員はネットワーク管理責任者とネットワーク運用責任者という立場で運用管理に関わり，筆者はネットワーク運用責任者を委嘱されている．また KWIINS 2.0 を管轄する事務部署として情報システムセンターが総務部にあり，課長，係長のほか職員 2 名，SE (System Engineer) が 4 名という体制である．KWIINS 2.0 の日常的な運用管理業務はネットワーク運用責任者と SE により行なわれている．

さらに，ネットワーク管理責任者を委員長とする情報システム運営委員会という全学規模の委員会が存在し，KWIINS 2.0 についての重要事項の決定や運用規則の改廃などについての議論を行なう．

2.3 機器の接続

KWIINS に機器を接続するときは，その機器が静的 IP アドレスをもつ予定なら機器接続申請を，動的 IP アドレスなら DHCP 利用申請を行なう必要があった．これは所定の用紙に必要事項を記入して申請するものであり，正式には情報システム運営委員会の議を経て承認の可否が決まるが，実際には情報システム運営委員会の常任委員会において異議がなければ承認される*1．これらの申請は KWIINS 上にアカウントのあるユーザであれば誰でも可能である．

DHCP 利用申請の場合は MAC アドレスが必要であり，管理者側でこれを DHCP サーバに登録することで，ユーザがネットワークに接続する際に MAC アドレス認証を行なう．しかし機器接続申請の場合は申請の承認時に IP アドレス等のネットワーク情報を申請者に提供するのみであり，接続の際には何の認証も行なわない．すなわち DHCP 利用申請の場合は接続時にその機器（厳密にはネットワークインタフェース）を認証するが，静的 IP アドレスを用いた機器接続の場合はなんら認証せずに接続を許していた．これでは，どのユーザが，いつ，どのように KWIINS に接続したのかを管理者が把握することは困難である．実際，ウイルス感染などで調査に赴いた先のホストが管理者不明で利用されていて，感染時に誰が利用していたかもわからないということがあった．また，これらの申請が紙を媒体にして行なわれていることと，その承認に日数がかかることはユーザにとって不便であった．

そこで，KWIINS 2.0 では紙による接続申請を原則として廃止し，後述するようにすべての機器についてネットワーク接続時に認証することとした．これにはユーザ認証と MAC アドレス認証のどちらかを利用することとし，ユーザ認証を行なうことを原則とした．また，ユーザ認証に対応できない機器（詳しくは後述）を接続する場合には MAC アドレスを紙で申請する必要があり，MAC アドレスを記入しなくてよい形式の機器接続申請は廃止された．

これらによって，KWIINS 2.0 ではネットワークに接続されたすべての機器について，ユーザ認証でユーザを特定するか，MAC アドレス認証で機器を特定するかのどちらかが可能となった．MAC アドレスによって機器が特定されれば，提出されている機器接続申請を検索することで申請者を特定できるので，どちらの認証方式の場合でも最終的にはユーザを特定することができ，責任の所在を明確化することが可能となった．

2.4 ウイルス拡散防止

KWIINS ではコンピュータウイルスやワームの活動を防止するため，サーバセグメント以外から送信された ICMP echo パケットがセグメントを越えることを禁止し，ウイルスやワームがよく利用するポート（137 番ポートや 445 番ポートなど）についても同様にセグメントを越えて通信できないようにしていた．これらは基幹 L3 スイッチによって実現していた．

この対策によりウイルスやワームがセグメントを越えて活動することはある程度防げるが，セグメント内での活動は防止できない．実際，教室内でノート PC を利用した授業中にウイルスが蔓延する状況も発生した．また，別セグメントにある機器の ICMP による死活監視や，コンピュータ教室での ping コマンド実習や経路探索実習*2などが実施しづらくなるという弊害もあった．

そこで KWIINS 2.0 では，ウイルスやワームなどの振る舞いを検知してこれを管理者に報告し，さらにネットワークから隔離する機能を持つ機器を導入することによって上記の対策を廃止した．

---

*1 常任委員会による決定は，後日，委員長より情報システム運営委員会に報告される．

*2 Windows 上の tracert コマンドは ICMP パケットを利用している．

3. 安全性の向上

KWIINS では，前述のように接続機器やユーザの特定を行なうことが困難な場合があった．そのため，KWIINS 上には特定不能なユーザが存在する可能性があった．また，KWIINS はセグメント内でのコンピュータウイルスやワーム等の活動を検知したり防止したりする機構を持たなかった．これらのことにより，KWIINS は安全なネットワークとは言い難く，安全性を向上することは KWIINS 2.0 の最大の目的のひとつであった．

以下ではこれら安全性向上のために導入した 2 つの機構について，実現方法と運用開始までの経緯を述べる．

3.1 ネットワークアクセス制御機構

ネットワークアクセス制御のための認証は，ユーザが機器を KWIINS 2.0 に接続したとき，その機器が実際にネットワーク利用を始める前に行なわれる必要がある．そのため，KWIINS 2.0 の末端に配置された L2 スイッチの各ポートに情報コンセント等を通じて機器が接続され，通信が開始されたときにすかさずユーザ認証等を行なうことが必要である．具体的には，動的 IP アドレスを利用する機器については IP アドレスが振られるまでは認証なしで通信させるが IP アドレスが割り振られた後の通信は認証を必要とし，静的 IP アドレスを利用する機器についてはネットワーク利用開始当初から認証を必要とする．

これらの認証にはユーザ認証と MAC アドレス認証の 2 つを用意した．

ユーザ認証は，対応する機器や OS の種類をできるだけ多くする必要があり，認証の際にはユーザが特段の説明なく利用できるくらいに容易なものとするために，WWW を利用するものとした．

また，WWW によるユーザ認証に対応できない機器については MAC アドレス認証を行なうこととした．ユーザ認証に対応できない機器としてはネットワークプリンタや無線ネットワークの基地局，携帯ゲーム機など，WWW ブラウザを持たないか WWW ブラウザを起動することが困難な機器が挙げられる．認証する MAC アドレスは機器接続申請時に提出されたものとする．

3.1.1 実現方法

ネットワークアクセス制御機構は，Apresia 社の L2 スイッチ（2124GT-SS2 など）の NA (Network Authentication) 機能[4] により実現した．Apresia NA 機能では，上記の MAC アドレス認証と WWW によるユーザ認証をこの順で併用することが可能である．また，L2 スイッチの下流に利用者がハブやスイッチを設置していた場合には L2 スイッチの 1 つのポートに対して複数の機器からの通信が行なわれることになるが，その際にも各々の機器に対して別々に認証を行なうことが可能である．

Apresia NA 機能では，まず L2 スイッチのポートに機器が接続され最初の通信が行なわれたときにその MAC アドレスを L2 スイッチが取得し，Radius サーバに問い合わせる．これが Radius サーバに登録されていれば認証成功（MAC アドレス認証成功）となり，それ以降すべての通信を通過させる．KWIINS 2.0 ではユーザ認証に対応していない機器の機器接続申請時に提出された MAC アドレスを Radius サーバに登録している．

この MAC アドレスが Radius サーバに登録されていない場合（MAC アドレス認証失敗）は，DHCP によって IP アドレスが振られるまでの通信だけを許可し，それ以外の通信は遮断する（すなわち静的 IP アドレスの場合はすべての通信が遮断される）．

その後，予め定められた URL に対して HTTP による通信が行なわれると L2 スイッチが認証ページを送出し，ユーザにユーザ名とパスワードの組を入力させ，入力されたものを Radius サーバに問い合わせる．Radius サーバによってこの組が正しいことが確認されればユーザ認証成功となり，そうでなければユーザ認証失敗となる．ユーザ認証が成功すれば，それ以降すべての通信を通過させる．KWIINS 2.0 ではメール受信や Windows 端末へのログオン等に利用するアカウントを統一しており，このユーザ認証でもそのアカウントを利用する．

Apresia NA 機能では，ユーザ認証成功後にどのタイミングで再認証を行なうかについていくつかのパラメータが用意されている．例えば認証成功後の経過時間や無通信時間，ポートのリンクダウンの検出，L2 スイッチからの ICMP による死活確認などである．KWIINS 2.0 では，認証成功後にポートのリンクダウ

ンが生じた場合または無通信時間が1時間を越えた場合にそれ以降の通信が遮断され，通信再開には再認証が必要になるというポリシーを採用した．

コンピュータ教室に設置されたホストにもこのユーザ認証を適用することとすれば，授業開始時のアクセスが大量に発生するためL2スイッチの応答時間が遅ければ運用不能となることが推測できる．この点に着目して運用実験を行なった文献[5]もあるが，コンピュータ教室のホストは，ユーザがホストのOS（WindowsまたはMac OS）にKWIINS 2.0のアカウントでログインしなければ利用できないので，ネットワーク利用時にさらにユーザ認証を行なう必要はないと判断した．

3.1.2 試験運用

ネットワークアクセス制御機構は一部の校舎でKWIINS 2.0運用開始と同時に運用した．これはそれらの校舎でKWIINSとはIPアドレスの体系が変更されたことをユーザに浸透させるための措置であると同時に，この機構が正しく機能することを確認し，この機構に対するユーザの反応を見るためのテストケースとしての意味もあった[3]．

前述のようにKWIINSの運用規則では機器接続に際して申請を行なわなければならないが，ネットワークアクセス制御機構を導入することでそれが原則不要になる．そのため，KWIINS 2.0運用開始前に，上記校舎は運用規則の例外とするということについて情報システム運営委員会の承認を得ておく必要があった．

ネットワークアクセス制御機構を有効にした校舎では，KWIINS 2.0運用開始直後に問い合わせや苦情が多く寄せられた．問い合わせの大部分は認証の仕組みや操作方法に関することで，ネットワーク接続時に認証が必要になっていることを知らないことが原因であった．これらは広報の拡充と，より詳細な説明書を掲示・配付することにより対応する必要があると考えられた．

苦情の中には「認証が面倒である」というものや「再認証の必要性についての疑義」が多かった．前者に対してはネットワークの安全性とネットワーク利用時の責任の明確化などについて説明することで対応した．後者については，ユーザにとってどのようなタイミングで再認証するのがよいのかを考えるための材料として詳しくインタビューした．これらの問い合わせや苦情は運用開始直後には1日に数十件の規模で生じたが，2週間ほど後には1日数件程度まで減少した．

3.1.3 本運用

ネットワークアクセス制御機構を全学規模で本格的に運用を開始するには運用規則を改正する必要があり，これは2007年12月に行なわれた．そのため，全学規模での本格運用は2008年1月に開始された．

本格運用開始の際にも上述のような問い合わせや苦情があったが，その数は想定されたものより少なく1日数件程度であり，また適切で素早い対応が可能であった．これは一部校舎での運用開始の際に寄せられた問い合わせに対応するためのマニュアルや資料が充実していたことや，そのときに操作方法等を体得した教員・学生による口コミ，および運用規則の改正が各教員に浸透していたことによる効果と考えられる．ただし，再認証の必要性や再認証のタイミングに対する苦情は少ないながらも継続して聞かれ，これは現在のポリシーから改善する余地があることを示していると考えられる．

3.2 振る舞い検知機構

KWIINS 2.0で導入した，ウイルスやワームなどの振る舞いを検知してこれを管理者に報告し，さらにネットワークから隔離する機能を持つ機器について以下で詳しく述べる．

3.2.1 実現方法

KWIINS 2.0では，Mirage Networks社のCounter Pointというアプライアンスを導入することで振る舞い検知によるネットワーク監視を実現した．Counter Pointは，接続されたネットワーク上でポートスキャンや大量のICMP echoパケットの送信等を監視することで，ウイルスやワーム，不正利用者などの振る舞いを監視する装置である．またCounter Pointはネットワーク上で使用されていないIPアドレスを利用した囮ホストを生成することができ，上記のような振る舞いの検知や攻撃の遅延のためにそれらを利用する．

Counter Pointは上記のような振る舞いが観測されたとき，そのことを管理者に通知するとともに予め定められた対応（例えば当該機器のネットワークからの隔離）を行なう．Counter Pointは1台で複数のセグメントを監視できる．

KWIINS 2.0では学内すべてのセグメントを監視対象とするために，Counter Pointを基幹L3スイッチと同様に各校舎に分散配置し，各々のL3スイッチに

集約されるすべてのセグメントにCounter Pointが接続されるようにした．

このCounter Pointの導入によってKWIINSで行なわれていた前述の通信制限を撤廃できた．これはユーザの利便性を向上することに通じる．また，KWIINSでは不可能だったセグメント内でのウイルスやワームの活動の検知・防止や，不正利用者の発見・隔離が可能となり，これらはネットワークの安全性向上につながるものである．

3.2.2 運　　用

振る舞い検知機構の運用はKWIINS 2.0の運用開始と同時に始めた．そのときの運用ポリシーは，囮ホスト等を利用してウイルスやワーム等の振る舞いを検知したときには管理者にメールで報告するのみとし，自動隔離等の強制措置は執らないというものであった．これは，KWIINSでの経験からウイルスやワーム等がKWIINS 2.0内で活動している可能性は小さいと思われたことと，誤検知した場合の対応にかかる手間とを勘案して決められた．

運用開始直後には本来検知すべきでない正常な振る舞いが攻撃／不正利用と報告された例がいくつかあった．主なものを挙げれば，コンピュータ教室端末の利用状況を調査するときや，Trendmicro社Virus Busterサーバから同クライアントに対してウイルスパターンファイルを更新するときに利用されるサーバセグメントからのICMPパケット等である．これら以外に，教員や学生が利用しているPC等がネットワーク接続されたプリンタやスキャナ等の機器を探索する際のポートスキャンや，無線ネットワークの基地局の切替えが瞬時に複数回生じた場合に同一のMACアドレスが異なるセグメント上にほぼ同時に出現すること等，誤検知ではないが不正利用との区別が難しい事例がいくつかあった．

前者についてはそのサーバを検知対象から除外する設定を行なうことで誤検知を回避している．後者は機械的な判断が困難であり，管理者への検知報告が届くたびに利用者を突き止めて問い合わせを行なっている．校舎の発生頻度は多くても1ヶ月に2〜3件程度である．

Counter Pointは2008年5月にEndpoint Controlという製品に更新された[6]が，これにも上記と同様の設定を行なって振る舞い検知機構の運用を続行している．

KWIINS 2.0の運用開始からほぼ1年間に約3500件の振る舞い検知報告が管理者宛に行なわれたが，そのうちの大部分は上述のような事例であり，これらはできるだけ自動で回避するように設定を調整してきた．また，検知された事例がウイルスやワームの活動，ネットワークの不正利用等であったことは一度もない．

4. 運用開始後の状況

MACアドレス認証とユーザ認証によるネットワークアクセス制御機構および振る舞い検知機構は，本格運用開始からそれぞれ8ヶ月余と1年を経過した．以下，運用開始後の状況について述べる．

4.1 ネットワークアクセス制御機構

ネットワークアクセス制御機構の導入によって紙による機器接続申請が原則不要となったことは多数のユーザに歓迎された．

これは例えば授業でノートPCを接続する必要がある学生や複数の機器を接続している教員や非常勤講師等である（KWIINSでは年度ごとに機器接続申請をし直す必要もあった）．学生と非常勤講師は事前の申請をしなくても授業開始時にその場でユーザ認証を行なうことで接続でき，複数の機器を接続している教員は年度ごとの煩雑なMACアドレス調査と申請から解放された．

また学内で開催される研究会等でKWIINS 2.0にアカウントを持たない参加者が一時的に機器を接続する場合，これまでは事前に学内での開催責任者がそれらの機器のMACアドレスを調査して機器接続の申請をしていた．しかし，今では管理者側がゲストアカウントを用意し，学内での開催責任者が接続時に参加者に周知するだけで済むようになっている．

前述の通り，ネットワークアクセス制御機構に対しての問い合わせや苦情は少なくなったが，再認証の必要性やタイミングに対する苦情は月に数件程度の頻度で継続している．これは現在のポリシーから改善する余地があることを示していると考えられる．

特に問題なのは一旦認証に成功した後に無通信時間が1時間を越えた場合の再認証であり，このときユーザはネットワークへのアクセスを何度か（または何分か）試行した後で初めて再認証が必要であることに気付く．再認証をせずに繰り返されるネットワークアク

セスがことごとく拒否されるという現象は，ユーザにとってはWWWブラウザやMUAが応答しない状況が続く現象とだけ観察され，このことはKWIINS 2.0への不信感にも繋がりやすい．これは固定されたURLをユーザ認証に用いている限り不可避な問題かと思われるが，Apresia NA機能には再認証のためのパラメータが複数用意されているので，これらを組み合わせてユーザの利便性をできるだけ損なわないような再認証を行なうようにしたいと考えている．また，ユーザ不在時に施錠される研究室のような場所に設置された機器に対しては，誰でも接続できる場所に設置された機器とは異なる再認証ポリシーを適用できないか検討している．

2008年7月，筆者の所属する現代社会学部の1, 2回生に対して学内ネットワークについてのアンケート調査を行ない，95件の有効回答を得た．その中の質問“学内ネットワークに機器を接続する際にユーザ認証が必要なことを知っていますか”に対して，64%の学生が“知っている”と回答している．これは“ノートPC等を学内ネットワークに接続したことがありますか”という質問に対して“接続したことがない”と回答した学生が76%であることと比較すると，ネットワークアクセス制御機構の存在が学生によく知られている（ネットワークに機器を接続したことがない学生にさえ知られている） ことを示すと考えられる．

4.2 脅威検知機構

脅威検知機構については，運用開始からこれまでの間にコンピュータウイルスやワームの活動，ネットワークの不正利用や攻撃など真の脅威に繋がる情報を検知したことはない．しかし前述のようにこれに類似した振る舞いを検知し，故意にポートスキャン等を行なって動作テストを実施した場合には正しく検知するので，真の脅威に繋がるような事例を見逃している可能性は非常に小さいと考えられる．

以上により，KWIINS 2.0はKWIINSに比べてユーザの利便性が向上し，また安全性も向上したネットワークであると結論付けることができる．これはMACアドレス認証とユーザ認証を利用したネットワークアクセス制御機構と，振る舞い検知を利用した脅威検知機構によって実現されたものである．

5. おわりに

京都女子大学では2007年8月に学内ネットワーク機器を更改し，それに伴ってネットワークアクセス制御機構と脅威検知機構を運用開始した．本稿ではこれらネットワークアクセス制御機構と脅威検知機構の実現方法，運用の経緯，運用後の状況と問題点について報告した．

これらの機構の運用により，KWIINS 2.0はKWIINSに比べて安全性が向上したと考えられる．しかしネットワークアクセス制御機構については前述したような再認証にかかわる問題点があるので，これを改善することでユーザの利便性をもっと向上させたいと考えている．

参考文献

1) 宮下健輔，水野義之：京都女子大学における情報機器更新計画，情報処理学会研究報告 2005-DSM-39，情処研報，Vol.2005, No.40, pp.25–30 (2005).
2) 宮下健輔：Mac OS X Serverを利用したWindowsドメイン運用，情報処理学会研究報告 2006-DSM-41，情処研報，Vol.2006, No.42, pp.7–12 (2006).
3) 宮下健輔：京都女子大学におけるネットワーク機器の更新 —安全・快適なネットワークを目指して—，分散システム／インターネット運用技術シンポジウム2007論文集，IPSJ Symposium Series, Vol.2007, No.13, pp.59–64 (2007).
4) 日立電線株式会社：Apresiaの認証機能：Apresia NA，http://www.apresia.jp/products/func/function/na.html.
5) 前田香織，河野英太郎，北村俊明：キャンパスネットワークへの認証システムの導入，情報処理学会研究報告 2006-DSM-47，情処研報，Vol.2007, No.47, pp.19–24 (2007).
6) Networks, M.: Network Access Control with Mirage NAC - Mirage Networks, http://www.miragenetworks.com/nac/.