全学無線 LAN アクセスポイントの増設について

武藏 泰雄[1]

概要: 平成 18 年 3 月 2 日付けで「無線 LAN 使用状況調査 (依頼)」の調査結果が学内に通知されました。その結果によりますと、本学では、研究室等を中心に約 100 箇所余りの無線 LAN が設置され、本学の情報セキュリティポリシー及びその十書手順書を遵守することが不可能であることが判明しました。そこで、昨年平成 18 年 4 月〜12 月の期間に無線 LAN アクセスポイント (AP: 基地局) の調査選定や導入試験を行い、AP 必要数と設置場所を決定し、平成 19 年 3 月までに AP 機器の購入、同年 6 月末までに設置工事および接続試験を実行致しました。今回はこの無線 LAN の設置についてご報告致します。

1 背景

平成 17 年 4 月 1 日より「独立行政法人等の保有する個人情報の保護に関する法律」施行されました。しかしながら残念なことに本大学においても同年 10 月 27 日にメディアで個人情報漏洩事件が報じられました。そして同年 11 月 7 日に「熊本大学保有個人情報保護の取組み強化へのお願い」という文書が教職員に配布されました。また同年 4 月 15 日には本大学のホームページが書き換えられ被害が発生しました。平成 17 年は熊大において重大な情報セキュリティ事件が発生した年でありました。またこの年は無線 LAN の WEP 等の暗号鍵が、比較的容易に特定できる技術やツールが出まわり、更には特定の部局で無線 LAN が乱立していて、外部から容易に接続できることが大学関係者以外に漏れる等の情報が入って来たため、無線 LAN のセキュリティ向上は急務であると認識されました。

そのため、平成 17 年度 12 月 9 日付けで最高情報セキュリティ責任者より「無線 LAN 使用状況調査 (依頼)」があり、そして翌年の平成 18 年 3 月 2 日付けで学内にその調査結果が通知されました。その結果、本学では、研究室等を中心に約 100 箇所余りの無線 LAN 基地局 (アクセスポイント、以後 AP と称す) が設置されていることが分かりました。これらのほとんど AP では、セキュリティの設定が可能であるにも関わらず、ほとんど無条件で自動的に接続されるものが多くありました。したがってこのままの状態を放置すれば、無線 LAN AP を介して個人情報漏洩事件等がいつ発生してもおかしくない状態であることが分かりました。

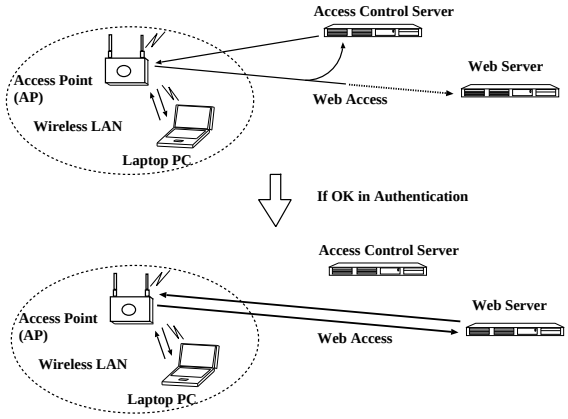

図 1 Web アクセスとアクセス制御サーバ

最初はこの様な AP は即刻取り除くべきであるということになりましたが、無線 LAN の利便性を考えれば、例えば、この報告書の著者も無線 LAN を大学内のみならず、出張先等でも愛用しているような状態であり、空港やホテル等、出張先の公共の場所においてもそのインターネットへのアクセシビリティを確保する上で無線 LAN の提供するサービスは既にインフラであり、必要不可欠なものとして認知されているものと考えられます。

ただ、実際セキュリティレベルを挙げた無線 LAN AP を設置することは意外の他難しいためか、例えば、学外の例としては出張先でのホテル等では、無線 LAN AP を最初の間は設置していたものの、無線 LAN に関するセキュリティ脆弱性がメディア等で報道されるにつれ無線 LAN サービス自体の廃止や、有線 LAN への切り替えまたは戻すケースが増加しております。[2]

しかしながら、セキュリティの問題は合理的で的確な対策を講ずることによって排除または抑制される

[1]熊本大学総合情報基盤センター・ネットコミュニケーション講座

[2]ホテル等の客室によっては何らかの原因で無線電波が届かず不安定であり客からの苦情処理が意外な負担になっているケースがあること等も、無線 LAN サービスの廃止や減少の原因となっています。

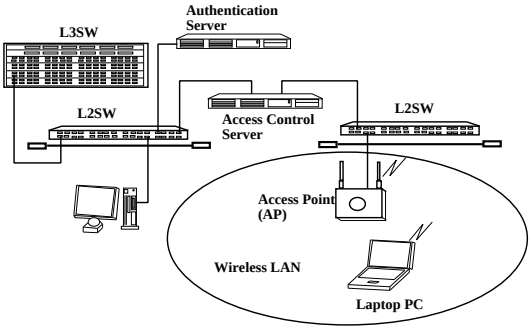

図 2 全学無線 LAN の構成

ものであり、**よりやわらかなサービス**をもたらすであろうユビキタス社会を推進するためにも、サービスの後退ではなく、よりセキュアなサービス展開のためにも、よりセキュアな無線 LAN AP の設置は必須と考えられ、既に導入した全学無線 LAN AP(平成 14 年〜平成 17 年度の期間) の置き換え計画を、平成 18 年 4 月〜平成 19 年 6 月までにかけて立案し、総合情報基盤センターおよび情報企画課とともにこれを実施致しました。

2 全学無線 LAN 強化推進計画

2.1 無線 LAN AP 条件

全学無線 LAN の AP(アクセスポイント) のセキュリティ強化計画は、平成 18 年 4 月〜9 月の期間に掛けて下記の項目を重点的に考慮し、導入すべき AP の調査選定や導入試験を経て立案されました。

(1) **ユーザ認証は大きく変更しないこと**
セキュリティの確保のため

(2) **高性能なアクセスサーバの設置場所の検討**
高いスループットを実現

(3) **通信暗号化**
WEP(Wired Equivalent Privacy) 128bit 以上、L2TP、および IPSec(VPN) 等採用

(4) **Windows, MacOS X や Linux 等に対応**

(5) **最高 54Mbps の帯域を利用可能であること**
無線 LAN の物理的通信規格には、IEEE80211b (11Mbps) および IEEE802.11g (54Mbps) 等があるが、少なくともこの 2 つの規格は満たすこと

(1) のユーザ認証については、セキュリティの要の一つである。本大学における無線 LAN 利用は、一般公衆無線 LAN 網等がとっている方式のうち、最初 Web アクセスを途中で奪って認証 Web サーバへ強制的に接続し、認証が正常に終了後、Web アクセスを含めたすべてのアクセスを許可する方式を採用している。(2) の設置場所の検討は、慎重に行う必要があり、そのため大変お忙しい時期ででしたが、各部局長宛てに平成 18 年 11 月 14 日付けで出された「全学無線ＬＡＮアクセスポイント増設について (依頼)」という調査依頼によって平成 18 年 12 月上旬までにその数や場所が報告され、これらの情報が設置場所や敷設工事等の設計が行われました。(3) の通信暗号化は PC と無線 LAN AP との通信を傍受されないためのものですが、WEP についても長時間の傍受によって通信暗号化ための暗号鍵が解読できる技術が開発されており、よりセキュリティの高い暗号化方式が使えるように AP を選定する必要があります。(4) は当然ですが、OS があまりにも新しいと接続ができない場合がありますので、平成 18 年度での OS を想定しています。(5) については、購入されるノート PC 等の無線 LAN が IEEE802.11b 以上に対応していれば OK ということになります。

2.2 全学無線 LAN の仕組み

全学無線 LAN は、本学の既設学内ネットワーク (KUIC) の一部として構成されています。この KUIC の基幹部分は 10Gbps を備えた L3 スイッチで構成され、各建屋内の各中継盤に設置した L2 スイッチとは 1Gbps で接続され、そして各 PC へは情報コンセントを介して最大 100Mbps で接続されています (図 2)。全学無線 LAN の AP もこの L2 スイッチに接続されていますが、既存のネットワークとは違う IP アドレス体系を設定しています。

この全学無線 LAN 用の専用 IP ネットワークは、既存の IP ネットワークとは分離されており、認証後にアクセス制御装置を介して全学無線 LAN へ接続されます。全学無線 LAN AP の役割は、PC との無線通信接続を行い、IP ネットワークに関する情報は基本的には、アクセス制御装置からの PC までそのまま何も換えずにブリッジング (AP と PC 間の無線通信そのものは WEP 等で暗号化されています) するだけです。

実際 PC が AP と無線交信に成功すると、DHCP によってアクセス制御装置から IP アドレスが自動的に割り当てられます。IP アドレスが PC に割り当てられると、その PC は Web アクセスを開始しますが、その Web アクセスはアクセス制御装置によって認証 Web サーバへ強制的に接続されます。そし

てこの認証が正常に終了しないと、Web アクセスを含めてすべてサービスが使えません。この時点で、部外者の接続を阻止することが可能となります。[3]

2.3 認証サーバの仕組み

認証サーバは、全学無線 LAN の利用開始時に利用者の認証を行うシステムです。認証サーバに接続された PC は、利用者へ ID 等の入力を促す画面を Web ブラウザに表示します (図 2)。この認証サーバは、アクセス制御装置と連携しており、認証が正常に終了すれば該当 PC の IP アドレスから KUIC への接続をある一定期間許可します。この認証サーバの認証用のデータは、本大学ポータルをベースとしたデータで構成されていますので、大学構成員であれば即使用することができます。

2.4 アクセス制御サーバ

図 2 に示すように、アクセス制御サーバは、全学 LAN IP ネットワーク (KUIC) と全学無線 LAN IP ネットワークの間に設置され、認証サーバと連携して、KUIC と全学無線 LAN とのセキュアに接続するための装置です。簡単に言ってしまえば、動的にアクセス制御が可能なファイアーウォールまたはゲートウェイに相当します。そのためこれらのゲートウェイの性能が全学無線 LAN の性能の一つである通信速度に影響を与えます。そのため実際には複数台を設置し、DHCP によって接続先を分散しております (9 台)。

2.5 アクセスポイント (無線基地局)

新たに、導入されるアクセスポイントについては平成 18 年 9 月までの調査結果、Cisco Systems 社製の Cisco Aironet 1131AG-J-K9 に決定されました。この AP に決まった理由は、無線 LAN 通信規格 IEEE802.11b/g/a のすべてに対応していること、また周波数も 2.4GHz/5GHz に対応していること、更に近隣の不正 AP を検知できる機能を有するところからです。また無線データ通信の暗号化では WEP

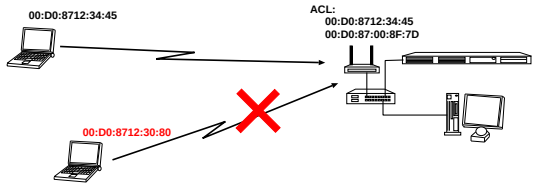

図 3 MAC アドレスベースのセキュリティ

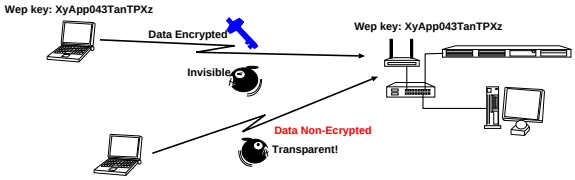

図 4 無線データ通信の暗号化

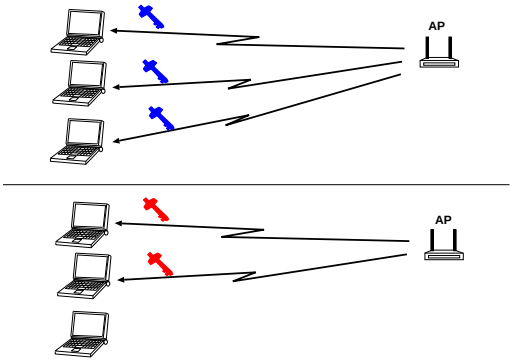

図 5 TKIP のセキュリティ

は当然として、WPA2(AES-CCMP) や TKIP にも対応しています。

無線 LAN のセキュリティは、先に述べた認証との連携の他に、AP 側の MAC アドレスによる制御、すなわち、WEP や WPA2 等による無線通信の暗号化、そして TKIP 等採用することによって守られています。

最初のセキュリティは MAC アドレスを登録することでしたが、PC 側の無線 LAN カードやチップの MAC アドレスを簡単に変更できるところからこの方法ではセキュリティを維持することはできません (図 3)。

そこで無線データ通信そのものを暗号化する技術が開発され、例えば WEP がこれに相当するもので現在でも良く使われています (図 4)。しかしながら、WEP 40bit 程度あれば、2、3 時間で解読できることが分かっており、やはり最低でも WEP 128bit また AES 等を使ったより高度な暗号化を使う WPA2 等を採用することが望ましくなっています。WEP

[3]例え WEP 等の暗号化鍵が判明してそれで接続を試みたとしても、サービスを無断利用する目的であればそれは阻止できます。しかし無線通信を傍受されていることは変わりはないので、SSH や SSL/TLS やメールの暗号化等のアプリケーションレベルでの暗号化通信を使うことが推奨される。

128bit についても、数時分間データを採集できれば概ねキーが解読できることが分かっており、WEP 128bit も完璧ではないことがわかります。

そこで TKIP という技術が開発されました (図 5)。この方法は、先に述べたように、無線データ通信を行うのですが、WEP と同じの弱点を克服するため、時間経過や AP における無線 LAN のトポロジー変更が起こると、暗号化キーの再配布を行い、通信暗号化キーが簡単に解読できないようになっています。

2.6 アクセスポイントの設置場所

今回増設されたアクセスポイントの設置場所 (およそ 200 箇所) は、図 6〜図 12 のそれぞれ赤・で示されています。ただしこれらの点は正確な位置ではありませんので予めご了承ください。実際には中継盤の近くの廊下、会議室、教室等に設置されています。また従来のものは、IEEE802.11b/g/a 対応のものが、橙色・で、また IEEE802.11b/g 対応のものが、青色・で示されています。

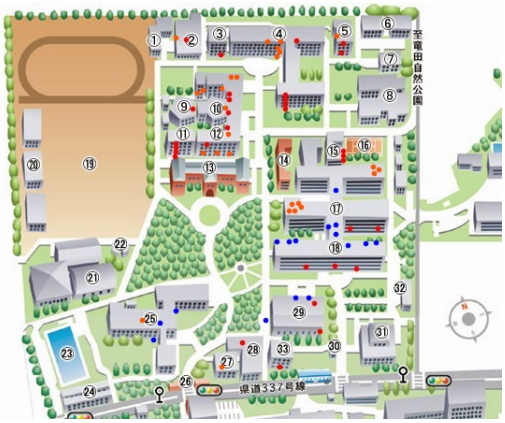

図 6 アクセスポイント設置場所 (黒髪北地区)

図 7 アクセスポイント設置場所 (黒髪地区東教室)

図 8 アクセスポイント設置場所 (黒髪南地区)

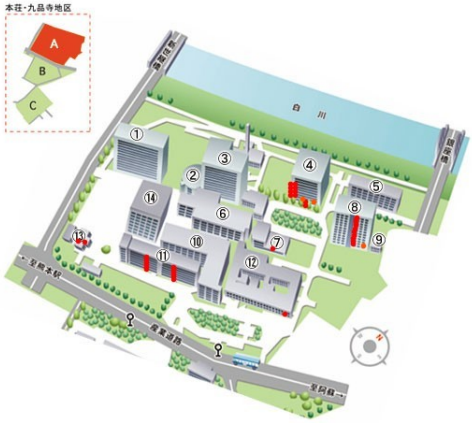

図 9 アクセスポイント設置場所 (本荘・九品寺 A)

図 10 アクセスポイント設置場所 (本荘・九品寺 B)

図 11 アクセスポイント設置場所 (本荘・九品寺 C)

図 12 アクセスポイント設置場所 (大江地区)

3 全学無線 LAN の利用方法

全学無線 LAN の利用方法について簡単に説明します。詳細は、総合情報基盤センターのホームページから、「全学無線 LAN システムの利用方法」をご覧ください。なお、全学無線 LAN の利用有資格者は、在学中のすべて学生および在職中の教職員となります。

3.1 無線 LAN 利用時に必要なもの

(1) セキュリティアップデートされた PC

(2) 無線 LAN 機能を有する PC
IEEE802.11b 規格に対応した無線 LAN 機能

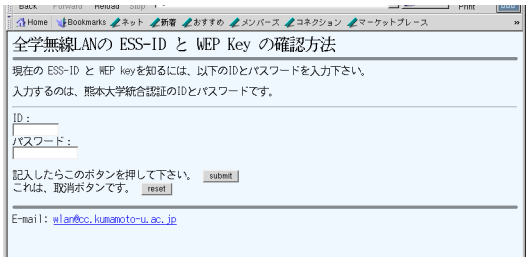

図 13 ESS-ID と WEP キーの入手ページ

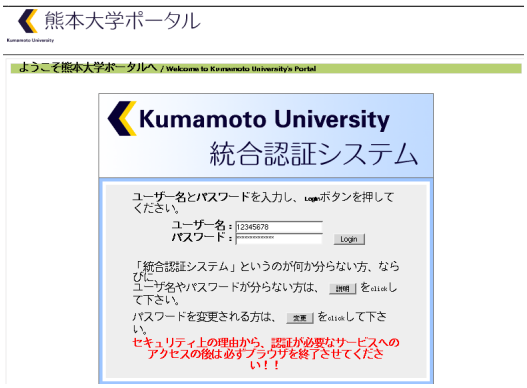

図 14 熊本大学ポータル

を有するノート PC 等がこれに相当します。また無線 LAN 機能を有する最近ノート PC は、Fn キー等で簡単に ON・OFF ができる様になっており、これを押し忘れて、総合情報基盤センター等に尋ねられるケースもありますので、無線 LAN の ON・OFF についてはマニュアル等で十分確認をお願い申し上げます。尚、無線 LAN 機能がない場合は、無線 LAN カードや USB スティック型無線 LAN 装置別途購入してください。この場合は、それらの装置がご利用の OS や環境で確実に動作することを店頭でご確認の上ご購入ください。

(3) ESS-ID と WEP キーの入手
総合情報基盤センターの「ホームページ」→「全学無線 LAN システムの利用方法」から学内 LAN からのみアクセスできる情報をご参照ください (図 13)。

(4) 認証様のユーザ (ID) 名とパスワード
認証用のユーザ ID(アカウント) とパスワードは、「熊本大学ポータル」で使用するものと同じです (図 14)。

3.2 利用上の注意点

利用上の注意は当然ながら厳密に守る必要があります。

- WEP キーや個人のパスワードの取り扱いに注意
- 認証用のユーザ ID 名やパスワードの貸し借りは厳禁
- 多重ログイン等、一つのユーザ ID 名 (アカウント) を同時に利用は不可
- 利用にあたり、法律、社会一般道徳ならびにネットワーク上の道徳の遵守

3.3 PC の無線 LAN 機能を有効にする

PC の無線 LAN 機能をまず ON にします。元々装備されている PC では PC のマニュアルをみながらこの機能を ON にします。無線 LAN カードを別途購入した場合は、カードのマニュアルに従ってドライバ等をインストールしてください。ドライバのインストールは最初だけです。

3.4 無線 LAN AP への接続

はじめて PC から無線 LAN AP へ接続するためには、ESS-ID と WEP キーの設定を行います。この設定も通常は一回で済み、次回から自動的に設定されるようになります。ESS-ID と WEP キーの入手については、総合情報基盤センターの「ホームページ」→「全学無線 LAN システムの利用方法」から学内 LAN からのみアクセスできる情報をご参照ください (図 13)。

3.5 ネットワークへ接続

全学無線 LAN へ TCP/IP 接続するには IP アドレス、ゲートウェイアドレス、ブロードキャストアドレス、および DNS サーバアドレスは自動取得の設定、つまり DHCP 設定にしてください。上述の無線 LAN AP と PC の接続が完了すると、DHCP によって IP アドレス等を取得後 IP 接続がはじまります。

IP 接続がはじまったら、ブラウザで適当なホームページへアクセスしてください。すると認証サーバがその Web アクセスを奪い取って認証ホームページへ誘導します (図 15)。

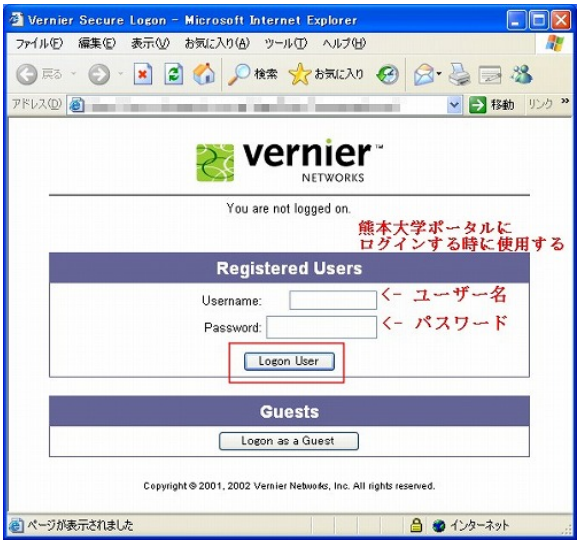

図 15 全学無線 LAN 認証画面

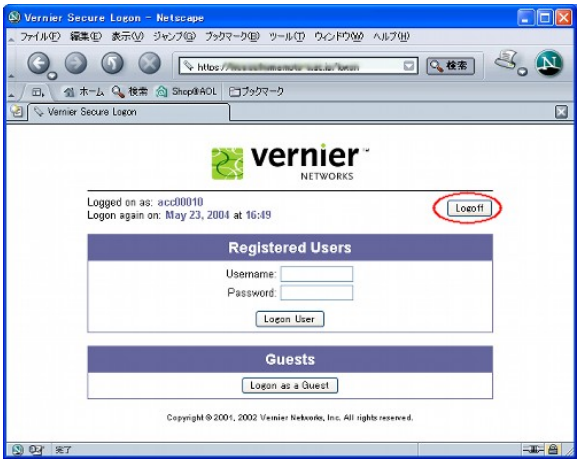

図 16 全学無線 LAN 終了画面

この認証ホームページが表示されたら、ユーザ ID 名とパスワードを入力して、Logon User ボタンをクリックしてください。しばらくするとアクセスしようとしていたホームページに接続されます。

この時点で、Web アクセス以外のメールや SSH/FTP 等のその他のネットワークアプリケーションも利用可能となり、KUIC やインターネットへの接続ができるようになります。

また全学無線 LAN の利用を終了する時は、ブラウザを開き、アドレスに http://1.1.1.1/を入力し、アクセスすると、図 16 の様な画面が開きます。この画面右上の Logoff ボタンをクリックすると接続が終了します。ネットワーク機能は 30 分間の利用がないと、自動的に接続が切れますので恐らく、実際的には適当に放っておいても接続が切れます。

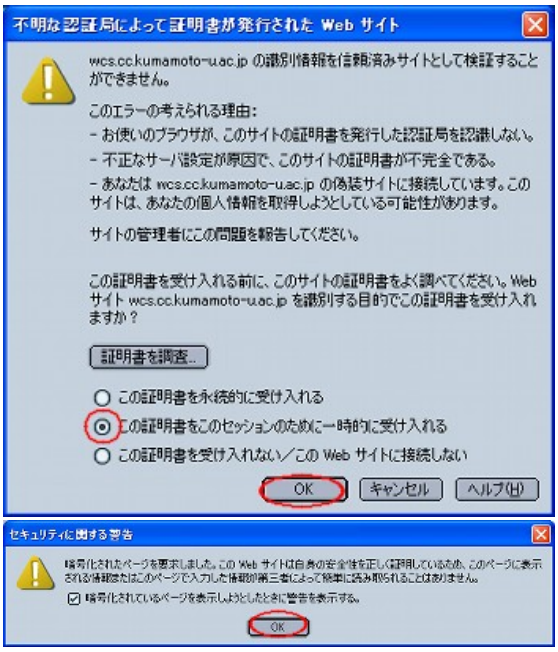

図 17 認証局の問題 (Netscape)

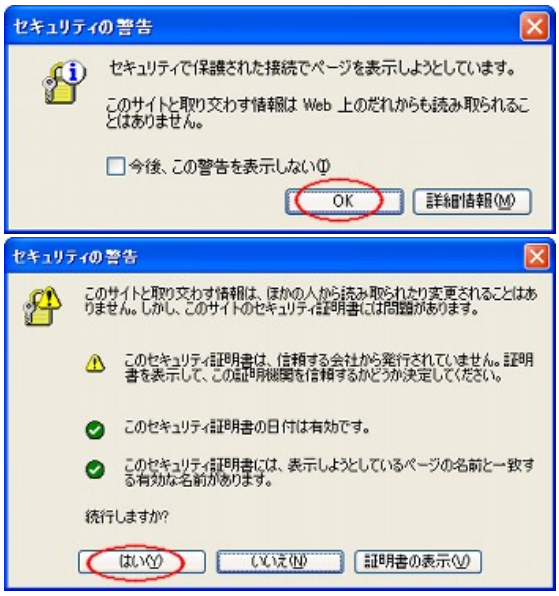

図 18 認証局の問題 (IE)

図 19 認証局の問題 (Firefox2.0)

図 20 Firefox2.0 の SSL2.0 設定 (1)

3.6 認証時の注意点

認証時に Web ブラウザで次の様なウィンドウが表示された場合は、下記の対応をしてください。まず認証局の関係です。

(1) Netscape の場合
画面に図 17 のようなウィンドウやダイアログ等が表示された場合、一時的に現在表示されている認証を受け入れ、熊本大学の認証局にアクセスして PC の Web ブラウザに登録してください。次回からはこのウィンドウが表示されなくなります。
http://ca.kumamoto-u.ac.jp/

(2) IE の場合
画面に図 18 のようなウィンドウやダイアログ等が表示された場合、Netscape の場合と同様に一時的に現在表示されている認証を受け入れ、熊本大学の認証局にアクセスして PC の Web ブラウザに登録してください。次回からはこのウィンドウが表示されなくなります。

3.7 Firefox2.0/IEv7 について

Firefox2.0 並びに IEv7 は、認証時や通常の Web アクセスがうまく行きません。

3.7.1 Firefox2.0 の場合

Firefox2.0 では標準で SSL2.0 での Web アクセスが設定されていないため、図 19 の様なウィンドウが表示されます。そこで、この SSL2.0 の設定を有効にします。設定はまずアドレスバーに、「about:conifg」と入力します (図 20)。設定リストが表示されますので、下記の項目を「false」から「true」に変更します。

- security.enable_ssl2 → 「true」
- security.ssl2.rc4_128 → 「true」

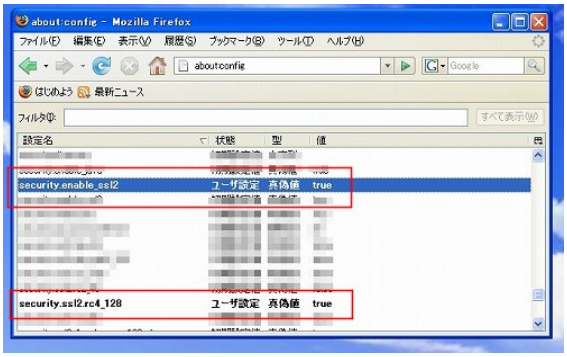

図 21 Firefox2.0 の SSL2.0 設定 (2)

対象の行をダブルクリックで「false」→「true」に変更します (図 21)。Firefox を終了してもう一度 Firefox を起動します。これで無線 LAN で Firefox が利用可能となります。

3.7.2 IEv7 の場合

IEv7 でも標準で SSL2.0 での Web アクセスが設定されていないため、図 22 の様なウィンドウが表示されます。そこで、この SSL2.0 の設定を有効にします。IE のメニュー「ツール」から「インターネットオプション」を選択します (図 23)。そして「詳細設定」→「SSL 2.0 を使用する」にチェックを入れます (図 24)。この後、IE7 を閉じてもう一度 IE7 を起動します。次回から無線 LAN の IEv7 利用が可能になります。

3.8 Windows Vista + IEv7

Windows Vista と IEv7 で全学無線 LAN を使用する場合、下記の設定が必要となります。

まず IEv7 の SSL2.0 の設定を変更します。この変更は先述の小節 3.7.2 を参照して変更してください。次に下記アドレスへアクセスします (図 25)。

http://ca.kumamoto-u.ac.jp/

ウィンドウ中央の【認証局証明書のダウンロードは「こちら」をクリック ･･･ 】の「こちら」を右クリックして、「対象をファイルに保存」を選択します。この時、保存した場所とファイル名を確認しておきます (図 26)。次に、保存した認証局証明書 (ここでは、デスクトップ上にダウンロードしている) をダブルクリックします。セキュリティの警告のウィンドウが開きますが、「開く」をクリックします (図 27)。すると証明書のウィンドウが開きます。「証明書のインストール」をクリックします (図 28)。次に証明書のインポートウィザードのウィンドウが開き

図 22 IEv7 の SSL2.0 の問題

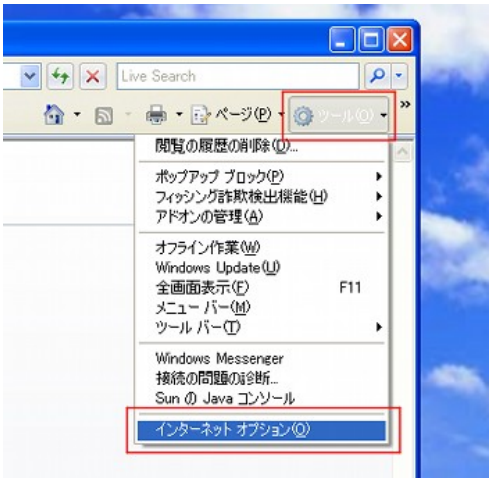

図 23 IEv7 の SSL2.0 の設定 (1)

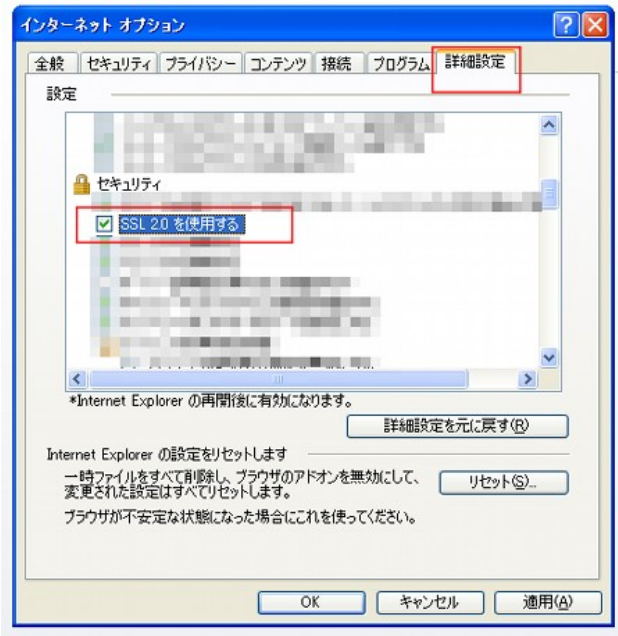

図 24 IEv7 の SSL2.0 の設定 (2)

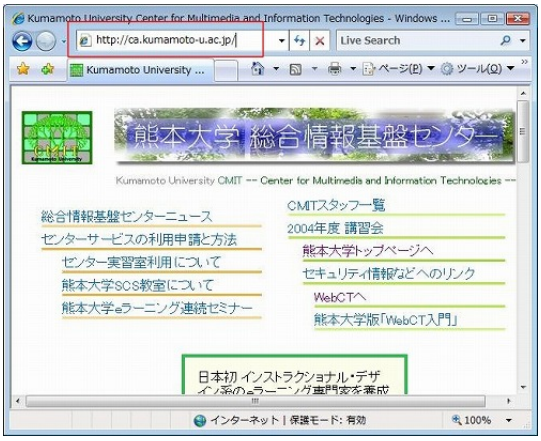

図 25 Windows Vista + IEv7 (1)

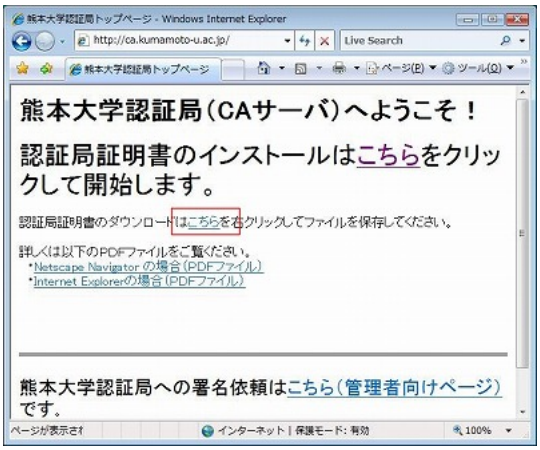

図 26 認証局へのアクセス

ます (図 29)。「次へ」をクリックします。

次に「証明書をすべて次のストアに配置する (P)」を選択します。そして「参照」をクリックします (図 30)。すると証明書ストアの選択のウィンドウが開きます (図 31)。「信頼されたルート証明機関」を選択した後に、「OK」をクリックします。

図 27 認証局の証明書を開く

図 28 認証書のインポート

図 29 証明書のストア設定の選択

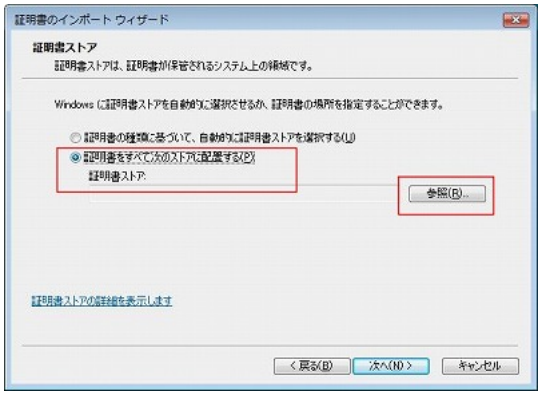

図 30 証明書ストアの設定開始

すると図 31 と同じウィンドウが表示されますが、一部図 32 に示すように、「証明書をすべて次のストアに配置する」の項目で、「信頼されたルート証明機関」になっていること確認します。そして「次」をクリックしてください。

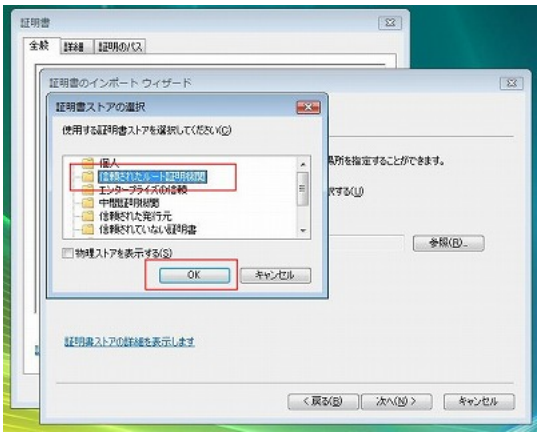

図 31 証明書ストア設定

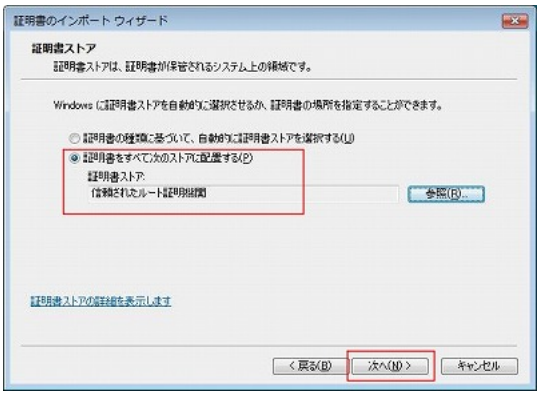

図 32 証明書ストア設定完了

すると図 33 に示すウィンドウが表示されますので。「完了」をクリックします。その後セキュリティ警告のウィンドウが開きますが (図 34)、内容を確認して「はい (Y)」をクリックします。その後小さなウィンドウ (ダイアログ) が表示されたら、「OK」をクリックしてください (図 35)。

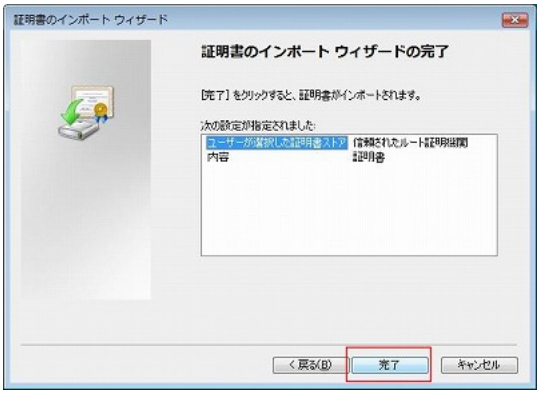

図 33 認証書のインポートの実行

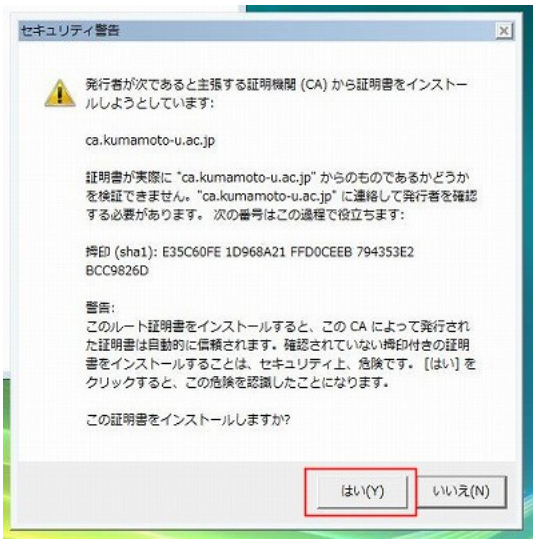

図 34 セキュリティ警告

図 35 証明書インポート確認

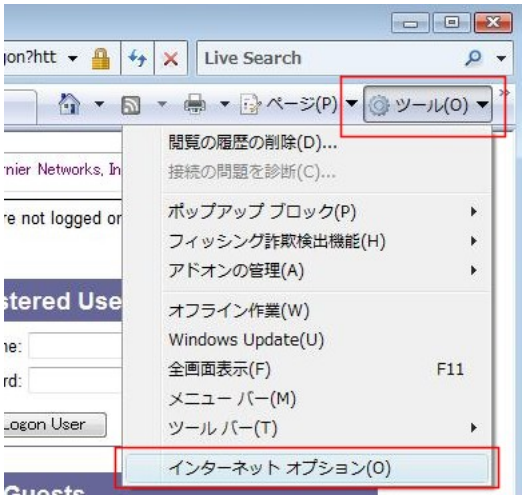

図 36 インターネットオプション

次に IEv7 の「ツールメニュー」から「インターネットオプション」をクリックします (図 36)。インターネットオプション」のウィンドウが開きます。「コンテンツ」タブ→「証明書」をクリックします (図 37)。「証明書」のウィンドウが開きます。「信頼されたルート証明機関」タブをクリックして、そこに「ca.kumamoto-u.ac.jp」があることを確認します (図 38)。

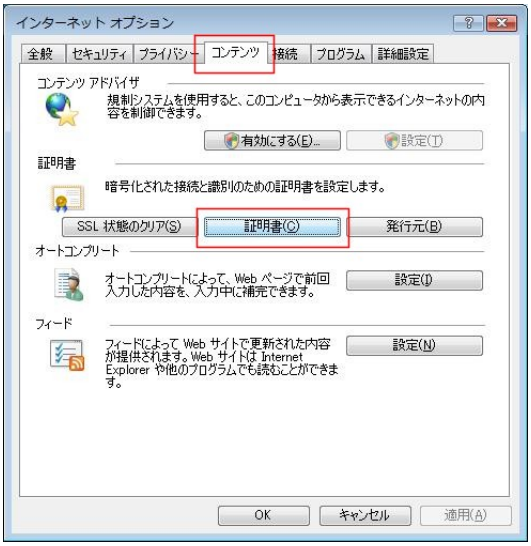

図 37 コンテンツと証明書

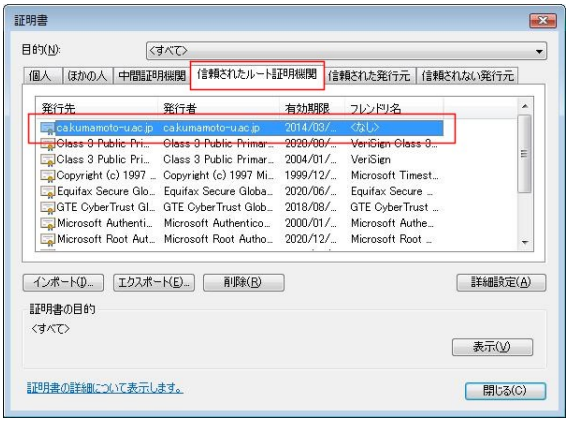

図 38 信頼されたルート証明機関

「ca.kumamoto-u.ac.jp」が確認できたらここで終了です。しかしながら、この時点でまだ「ca.kumamoto-u.ac.jp」が確認できない場合は更に次の手を打ちます。

まず「スタート」メニューから「検索の開始」欄に「mmc」と入力し (図 39)、「Enter」キーを押します (この時、「ユーザアカウント制御」のウィンドウが開きますが、「続行」をクリックして下さい)。すると「コンソールルート」が起動します (図 40)。「ファイル」→「スナップインの追加と削除」をクリックします。「利用できるスナップイン」で「証明書」をダブルクリックします。なお、「証明書」は下の方にありますので、スクロールバーで移動してください (図 41)。

次に証明書スナップインのウィンドウが開きます。「コンピュータアカウント (C)」を選んで「次へ」をクリックして下さい (図 42)。

図 39 コンソールルートの検索

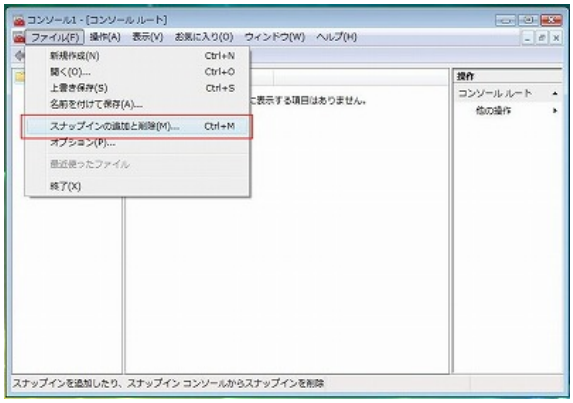

図 40 コンソールルートの起動

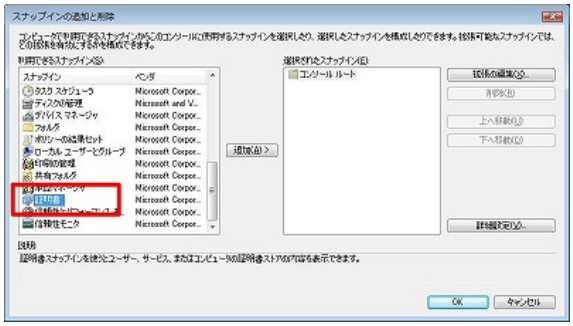

図 41 証明書の選択

図 42 証明書スナップイン

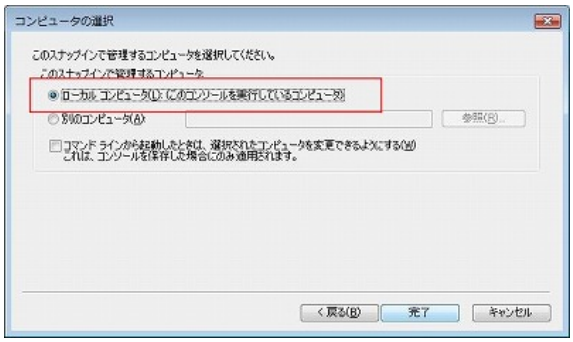

図 43 コンピュータの選択

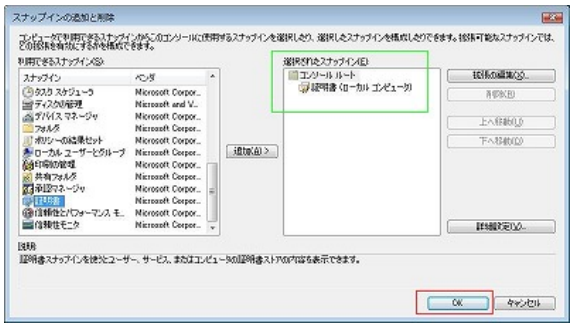

図 44 スナップインの選択と確認

するとコンピュータの選択のウィンドウが開きます (図 43)。「ローカルコンピュータ (L):(このコンソールを実行しているコンピュータ)」を選んで、「完了」をクリックして下さい。「選択されたスナップイン」に「証明書 (ローカルコンピュータ)」が追加されている事を確認後、「OK」をクリックします (図 44)。

次に、「コンソールルート」のウィンドウにて、「コンソールルート」→「証明書 (ローカルコンピュータ)」→「信頼されたルート証明機関」→「証明書」を順次ダブルクリックしていきます。ウィンドウの右側の「操作」から「他の操作」をクリックして、「すべてのタスク」→「インポート」をクリックします (図 45)。すると「証明書のインポートウィザード」のウィンドウが開きます。「次へ」をクリックして下さい (図 46)。CA 局からダウンロードした証明書ファイルを、「参照」をクリックして選択します。その後「次へ」をクリックします (図 47)。「証明書ストア」で「証明書を全て次のストアに配置する」を選択します。証明書ストアが「信頼されたルート証明機関」になっている事を確認します。「次へ」をクリックします (図 48)。そして「証明書のインポートウィザードの完了」です。ここで「完了」をクリックします (図 49)。次に「正しくインポートされました。」というウィンドウが開きます。「OK」をクリックします (図 50)。この時点で、証明書がインポートされます。「ca.kumamoto-u.ac.jp」がインポートされている事を確認してください (図 51)。

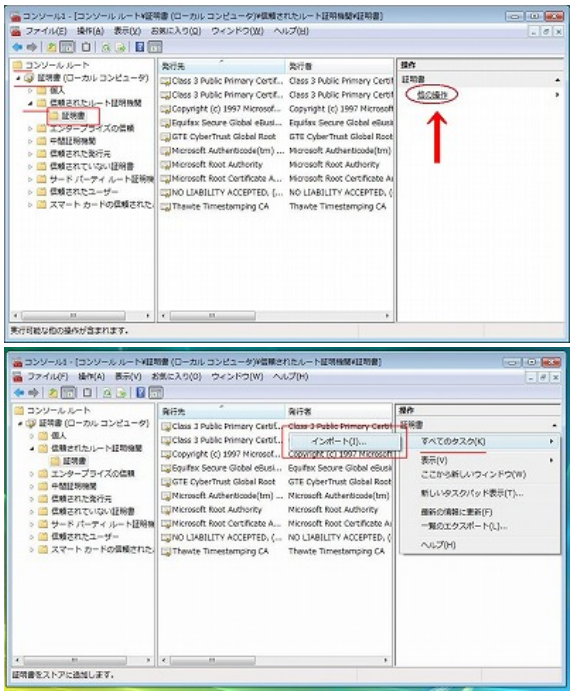

図 45 すべてに証明書インポート

図 46 証明書インポート開始

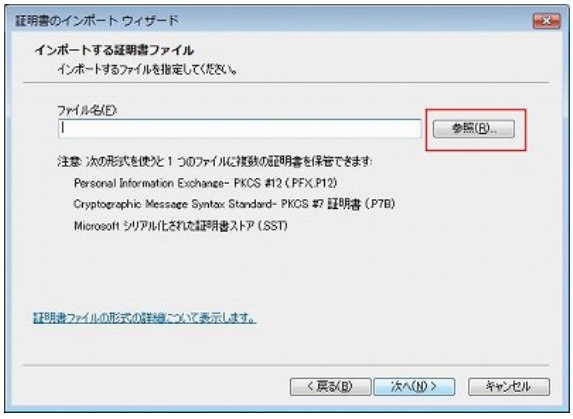

図 47 証明書インポート用ファイルの指定

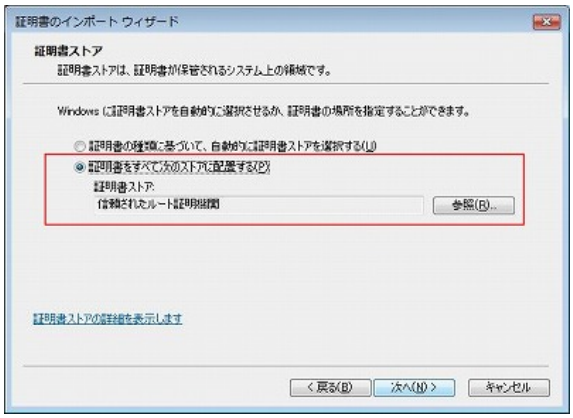

図 48 証明書を全ての次のストアに配置

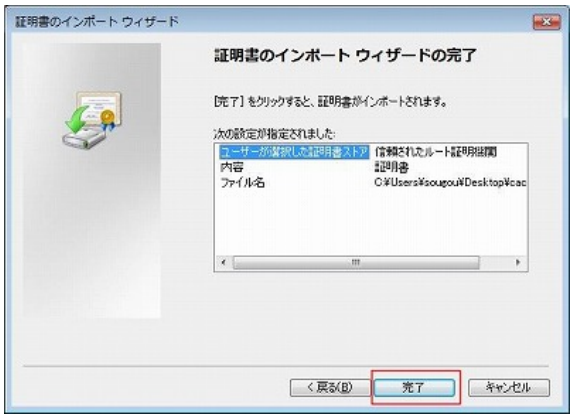

図 49 証明書インポート完了

図 50 インポート完了メッセージ

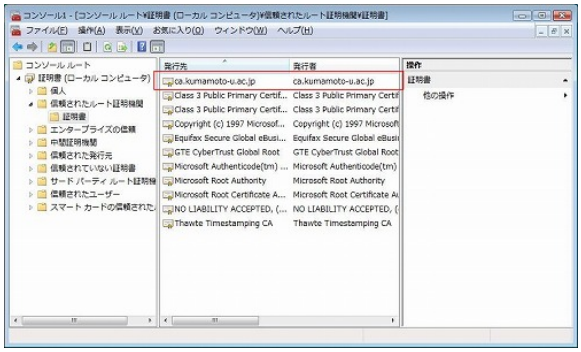

図 51 証明書インポート確認

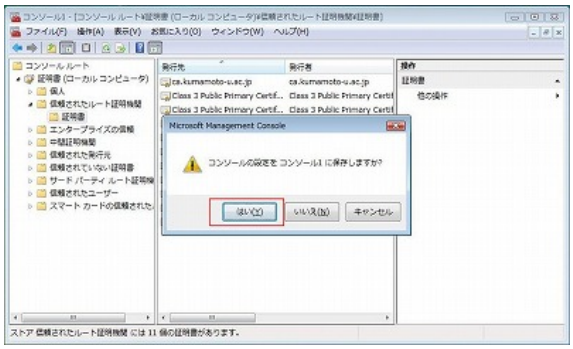

図 52 コンソールの設定保存と終了

「ファイル」→「終了」をクリックして、コンソールの設定を保存して終了します (図 52)。

これらの設定は有線 LAN でお願いします。無線 LAN 以外に方法がない場合は、別の PC で USB キーディスク等を介して Firefox2.0 等のブラウザをインストールする方法があります。

謝辞. 平成 18 年度の全学無線 LAN の整備は、高度情報化キャンパス整備計画の一つであり、高度情報化キャンパス推進化費で行われております。熊本大学の教職員および学生の皆様のご理解ご協力につきまして、この場を借りて厚く感謝申し上げる次第です。

参考文献

1) http://www.cisco.com/japanese/warp/-public/3/jp/product/hs/wireless/airo1130/-prodlit/pdf/1130ag_ds.pdf