#### 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。<sup>2</sup>

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

<sup>&</sup>lt;sup>1</sup>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

<sup>&</sup>lt;sup>2</sup>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LANAP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。<sup>3</sup>

### 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ば、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

<sup>&</sup>lt;sup>3</sup>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 PCIEEE802.11b 規格に対応した無線 LAN 機能

Back Forward Heldad Stop / -		Print	000
↓ Home ↓ Bookmarks えネット え新者 えおすすめ えメンバーズ えコネクション えマー	ケットプレース		*
全学無線LANの ESS-ID と WEP Key の確認方法			
現在の ESS-ID と WEP keyを知るには、以下のIDとパスワードを入力下さい。			
入力するのは、熊本大学統合認証のIDとパスワードです。			
10: パスフード:			
記入したらこのボタンを押して下さい。 これは、取消ボタンです。 reset			
E-mail: <u>wlan@cc.kumamoto-u.ac.jp</u>			

図 13 ESS-ID と WEP キーの入手ページ



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、 下n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 オタンを 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)

#### **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。

 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。



図18 認証局の問題 (IE)

警告		
_		
	ОК	

図 19 認証局の問題 (Firefox2.0)

🕑 ソフトウェアの更新 - Mozilla Firefox		
ファイル(1) 編集(1) 表示(1) 雇匪(2) ブックマーク(2) ツール	9 ~17H	
🐗 = 🔿 = 🧭 🔕 🏠 📄 aboutconfig		•
⑧ はじめよう 🔂 最新ニュース		
タンフトウェアの更新 G Mozilla Firefoo	スタートページ	

図 20 Firefox2.0のSSL2.0設定(1)

#### 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 <sup>r</sup> true J

🕲 about:config - Mozilla Fi	refox			
7ァイル(E) 編集(E) 表示(少)	履歴(S) ブックマーク(B) ツール	し ヘルプ(日)		1
🔶 - 🕑 📀 🟠	aboutconfig		- Google	Q
🥮 はじめよう 🔜 最新ニュース				
7-11-9Q:			[ৰুগবে	表示( <u>w</u> )
設定名	▽ 状態 型	ſ₫		E
				^
security.enable_ssl2	ユーザ設定 真偽値	true		
The section of the	ANNOLLARIA ALANA	i here i		
I THE CONTRACTOR OF A CONTRACTOR OF	International Accession	1 1000		
ALL REPORTS OF THE PARTY OF	CONTRACTOR DESIGNATION	1 H		
the state of the s	LINE A LINE	100		
And in case of the local division of the	CONTRACTOR OFFICE	and the second s		
THE REPORT OF LOT	TRACTOR DISC.	1000		
and the second second		No. of Concession, Name		
security.ssl2.rc4_128	ユーザ設定 真偽値	true		1
		-		~

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。 次に下記アドレスヘアクセスします (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)

Humamoto University Center for Multimedia and	Information Technologies - Windows
CO V E http://ca.kumamoto-u.ac.jp/	• + X Live Search
🚖 💠 🔜 Kumamoto University 🔤 🖄	・ 🗟 ・ 🖶 ・ 🔂 ページ(E) ▼ ۞ ツール(Q) ▼ "
能本大学)後	合情報基盤センター
Kumamoto University CMIT 総合情報基盤センターニュース センターサービスの利用申請と方法	Center for Multimedia and Information Technologies
センター実習室利用について 能本大学SOS教室について	セキュリティ情報などへのリンク
熊本大学eラーニング連続セミナー	WebCT个 熊本大学版「WebCT入門」
	ストラクショナル・デザ シーーング 直開 安东 番 成

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。

cacert	このファイルを描述さすか? 名称 C. K. Visers ¥ Sougou ¥ Desktop ¥ Cacert.cer 発行元 不馴な発行元 推頻 セネリファイ証明書 発信元 C. ¥ Users ¥ Sougou ¥ Desktop ¥ Cacert.cer 開K(の) キャンセル
	図この種類のファイルであれば常に警告する(W) <u>1とクーネットのファイルは決に定ちますが、このファイルの種類はコンピュージに同識</u>
	を起こす可能性があります。異自己の影響できない場合は、このソフトウェアを開かないでくたさい。他球性の設計用

図 27 認証局の証明書を開く

このCAルー	書の情報 
SCI?	
発行先:	cakumamoto-u.ac.jp
発行者:	cakumamoto-u.ac.jp
有効期	間 2004/04/01 から 2014/03/30

図 28 認証書のインポート

[明書のインポート ウィザード		
<b>F</b>	証明書のインボート ウィザードの開始 このウィザードでは、証明素、証明素(含肥)スト、および証明書売のか) 入ドをディスカが注訳書太トアにコピーします。 証明細胞にとって発行された証明表は、ローザー D を規模し、データ では感した。入まれがやらいディン語表がたやパーン目的表現性 するための情報を含んています。証明書から知る、証明書が体管され るシステム上の情報です。 統行するとは、D太へJ をクリックしてください。	
	(東部) (次への) キャンセ	ŀ

図 29 証明書のストア設定の選択

正明書ストア		
証明書ストアは、証明書が保管されるシステム。	」の領域です。	
Windows に証明書ストアを自動的に選択させる	が、証明書の場所を指定する。	とができます。
○ 証明書の種類に参ついて、目前所に証 ◎ 原則日本をすべてられて下がご記書すべた	相響ストアを選択する(山)	
新聞書之下P.		
		参照( <u>B</u> )
利用書入トアの詳細を表示します		

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

「明確ストア」 証明書ストアは、証明書が保密されるシステム上の領域です。	
Windows に証明書ストアを自動的に選択させるか、証明書の場	幣を指定することができます。
◎ 138日金小舗装5-基ペップ 自動45-138日金2 しつちざい	#3(1)
<ul> <li>         ・         ・         ・</li></ul>	200
1788ak2.kp	
(注頼されたルート版明思聞)	◆照(R)
明治2トアの詳細な表示します	

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)。

	証明書のインボー	トゥィザードの完了
	「売了」をクリックすると、証明 次の設定が指定されました:	月書がインボートされます。
-	ユーザーが営択した証明 内容	32.122 信頼されたルート証明知識問 証明書
	(戻る	(B) 完了 茶ャンオ

図 33 認証書のインポートの実行



図 34 セキュリティ警告

1	[明書のイ]	ンポートウ	ハザード		X
	<b>()</b>	<b>E</b> しくイン	ポートされ	ました。	
			ſ	ОК	

図 35 証明書インポート確認





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」タプをクリックして、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

発行先	発行者		有効期限	フレン門名	
📰 cakumamoto	-u.ac.jp ca.kuma	moto-u.ac.jp	2014/03/	くなし>	
Glass 3 Publ	ic Pri Olass 9	Public Primar	2020/00/	VeriSign Olass (	
Class 3 Publ	ic Pri Class 3	Public Primar_	2004/01/	VeriSign	
Gopyright (c)	1997 _ Copyright	nt (c) 1997 Mi_	1999/12/	Microsoft Times	t
👼 Equifax Secu	re Glo Equifax	Secure Globa	2020/06/	Equifax Secure	
GTE CyberTr	ust GI GTE Cy	berTrust Glob	2018/08/	GTE CyberTrust	
🗔 Microsoft Au	thenti Microso	ft Authentico	2000/01/	Microsoft Authe	
🗔 Microsoft Ro	ot Aut Microso	ft Root Autho	2020/12/	Microsoft Root .	2
(ンポート(D) [ [明書の目的 すべて>	エクスポード( <u>E</u> )]	育明除( <u>R</u> )			詳細設定(

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

<ul> <li>■ コンソール1 - (コンソール ルート)</li> <li>■ ファイル(F) 操作(A) 表示(V) お気に入り(0)</li> </ul>	ウィンドウ(W) へいげ(H)
スナップインの追加と崩除(M) Ctrl+M オプション(P) 最近使ったファイル 終了(X)	
スナップインを追加したり、スナップイン コンソールから	スナップインを削除

図 40 コンソールルートの起動

スナップイン	10.5		11 TAY-16 16-1-	「「「「「「「」」」」
<ul> <li>3525 スケジュー5</li> <li>ディングロルデ理 ディングロルデ理 デルパス マネージャ フォルズ フォルズ フォルズ ローカル ユーザーとグループ 当日等の増加 、 共和プラルズ 、</li> </ul>	Nicrosoft Corpor. Nicrosoft and V. Nicrosoft Corpor. Nicrosoft Corpor. Nicrosoft Corpor. Nicrosoft Corpor. Nicrosoft Corpor. Nicrosoft Corpor.		:Bto(A)>	RUND EARNOLD TARNOLD
1997年 1993年の日本の日本の日本の日本の日本の日本 1993年の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の	Nizzozeft Corpor. Nizzozeft Corpor. Nizzozeft Corpor.	, , , ,	aoližiikāz krostušaat težst.	Interest

### 図 41 証明書の選択

証明書スナップイン	*
このスナックインで管理する証明得: ○ ユーザー アカウンド(M) <del>○ サービス アカウンド(S)</del> ※ 賞送 <u>えーラ アカウンド(S)</u>	
	< 戻る(B) 次へ(NQ) キャンセル

図 42 証明書スナップイン



図 43 コンピュータの選択

ちゅうちょう	10.8	*	10000000000000000000000000000000000000	tellouinco.
97,5 スケジュー5  ディスクの部列	Nicrosoft Corpor Nicrosoft and V		「「「「「」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」	( A#%B)
91412 77-54 7+10	Nicrosoft Corpor			E<0.00
ポリシーの結果セット ローカル ユーザーとクループ 自時的な理 承知フマルク 承担フマネージッ	Microsoft Corpor. Nicrosoft Corpor. Nicrosoft Corpor. Nicrosoft Corpor. Nicrosoft Corpor. Nicrosoft Corpor. Nicrosoft Corpor. Nicrosoft Corpor.	iBto(A)>	)	TABIO

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 「 証明書 (ローカルコンピュー ンソールルート」 「信頼されたルート証明機関」 「証明書」 **夕**)」 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

<b>証明書のインボート ウィザードの開始</b> このウィザードでは、証明書、証明書信頼リスト および証明書失効 ストをすくから証明者ストパニピーします。 証明報知識によって知行された証明書は、ユーザー D を確認した、データ 好報した、お好た「おりた証明書は、ユーザー D を確認した、データ 好報した、お好た」サイン「経営社会社」の学生の主要を行いた。	
このウィザードでは、証明書、証明書(注例リスト、および証明書供Sが) ストをディングから証明書ストルニコピーします。 証明照明によって発行された証明書は、ユーザー D を確認し、データ を見る規模が整合されています。証明書法が見ませれたのペトワージ開発を提供 するための情報を含ったいます。証明書法が指示され	
証明得限的によって発行された証明書は、ユーザー ID を確認し、データ を保護したり、またはセキュリティで経滅されたネットワーク接続を提供 するとめの情報を含んています。証明書えたでは、証明書が保管され	
るシステム上の領域です。	
統行するには、じたへ」をクリックしてください。	
(夏季(日) (大へ(N)) 参考されれ	_
	統行するには、D5へ3をクリックしてください。 < 戻る(日) (法へ(ND) 年ャンセル)

図 46 証明書インポート開始

証明書のインポート ウィザード		
インボートする証明書ファイル インボートするファイルを指定してください。		
7r(1146)E) 	参照(B)	1
注意 次の形式を使うと1 つのファイルに複数の証	明書を保管できます。	1
Personal Information Exchange- PKCS #12	(PFX,P12)	
Cryptographic Message Syntax Standard-	PKCS #7 証明書 (P7B)	
Microsoft シリアル化された証明書ストア (SS)	n	
証明書ファイルの形式の詳細について表示します。		
	< 戻る(B) 次へ(N) キャンセ	14

図 47 証明書インポート用ファイルの指定

<b>明寺フトフ</b>		
明確ストア 証明書ストアは、証明書が保管されるシステム	し上の領域です。	
Windows (調節明書ストアを自動的に選択され	おか、証明書の場所を指す	定することができます。
◎ 証明書の種類に基づいて、自動的に調	証明書ストアを選択する(山)	
◎ 証明書をすべて次のストアに配置する	ex.	
証明書ストア		
信頼されたルート証明期間		参照(民)
月書ストアの詳細を表示します		

図 48 証明書を全ての次のストアに配置

	証明書のインボ	ート ウィザードの完了	
	[売了] をりりっクすると、言 )次の設定が指定されまし	証明書がインボートされます。 た	
~	<u>ユーサーが対視した</u> 相 内容 ファイル名	明書ストア (清朝されたルート記明 証明書 C米Users¥sougou¥De	l <b>ilili</b> esktop¥cac
		m	,

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

ニコンソールルート	易行党 "	発行者	接出	
<ul> <li>● 証明書(ローカルコンピュータ)</li> <li>&gt; ○ 個人</li> <li>● 価値構整されたルート証明機関</li> </ul>	Caskumamoto-u.ac.jp Class 3 Public Primary Certif Class 3 Public Primary Certif	ca kumamoto-u.ac.jp Class 3 Public Primary Certif Class 3 Public Primary Certif	118日 18の時作	
<ul> <li>         ご 証明書         <ul> <li>             ご エンタープライズの信頼         </li> </ul> </li> </ul>	Nicrosoft Management Consol	e 🖷		
<ul> <li>ご 価額された現行用</li> <li>ご 価額された現行用</li> <li>ご 価額されたいない証明書</li> <li>ご サードパーディルート証明時</li> <li>ご 価額されたユーザー</li> <li>ご 気マート カードの価額された</li> </ul>	(1000)	ロンソール1 に保存しますか? いいえ( <u>10</u> ) キャンセル	)	

#### 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