JAEA-Data/Code
2009-004

J-PARC 情報システムグループの認証システムグループによるIC カード PKI 認証方式のフィージビリティ・スタディ実施報告

Activity Report for Feasibility Study on PKI Authentication Method with IC Card in Authentication System Sub Group of J-PARC Information System Group

手島 直哉　青柳 哲雄　橋本 清治　真鍋 篤
湯浅 富久子　中島 憲宏

Naoya TESHIMA, Tetsuo AOYAGI, Kiyoharu HASHIMOTO, Atsushi MANABE
Fukuko YUASA and Norihiro NAKAJIMA

システム計算科学センター
Center for Computational Science & e-Systems

June 2009

Japan Atomic Energy Agency　日本原子力研究開発機構

JAEA-Data/Code

本レポートは日本原子力研究開発機構が不定期に発行する成果報告書です。
本レポートの入手並びに著作権利用に関するお問い合わせは、下記あてにお問い合わせ下さい。
なお、本レポートの全文は日本原子力研究開発機構ホームページ（http://www.jaea.go.jp）
より発信されています。

独立行政法人日本原子力研究開発機構　研究技術情報部　研究技術情報課
〒319-1195　茨城県那珂郡東海村白方白根 2 番地 4
電話 029-282-6387, Fax 029-282-5920, E-mail:ird-support@jaea.go.jp

This report is issued irregularly by Japan Atomic Energy Agency
Inquiries about availability and/or copyright of this report should be addressed to
Intellectual Resources Section, Intellectual Resources Department,
Japan Atomic Energy Agency
2-4 Shirakata Shirane, Tokai-mura, Naka-gun, Ibaraki-ken 319-1195 Japan
Tel +81-29-282-6387, Fax +81-29-282-5901, E-mail:ird-support@jaea.go.jp

© Japan Atomic Energy Agency, 2009

JAEA-Data/Code 2009-004

J-PARC 情報システムグループの認証システムグループによる IC カード PKI 認証方式のフィージビリティ・スタディ実施報告

日本原子力研究開発機構　システム計算科学センター

手島　直哉※, 青柳　哲雄, 橋本　清治*, 真鍋　篤*, 湯浅　富久子*, 中島　憲宏

(2009 年 3 月 24 日受理)

J-PARC 情報システムグループは、不特定多数の利用者による原子力施設の利用において、その情報システムの安全管理を必要不可欠なものとして考え、情報システムにおける使用する認証技術に関する調査、検討を実施するための認証システムグループを発足させた。認証システムグループは、世の中の各種の認証技術について調査しそれぞれのセキュリティレベルを定め、マップ化した。このマップにおいて最も高いセキュリティレベルにある認証方式のうち、J-PARC での使用が想定される IC カードによる PKI 認証方式について、J-PARC 情報システムの様々な使用場面においてフィージビリティ・スタディを実施したので報告する。

フィージビリティ・スタディでは、J-PARC ネットワークに適用・導入する際の課題を事前に明らかにし、以下の 4 つの検証を実施した。

(1) 「EAP-TLS 無線 LAN 認証」
(2) 「SSL-VPN 装置を経由した Web-SSL クライアント認証」
(3) 「NAREGI-CA ソフトウェアが発行する証明書による IC カード PKI 認証」
(4) 「Dual カードタイプ FeliCa を使用した PKI 認証」

本報告書は、これら 4 つの認証方式のフィージビリティ・スタディで実施した検証手順と、検証結果及びフィージビリティ・スタディから得られた知見について報告する。

システム計算科学センター（上野駐在）：〒110-0015 東京都台東区東上野 6-9-3
※ 技術開発協力員
* 高エネルギー加速器研究機構 計算科学センター

JAEA-Data/Code 2009-004

Activity Report for Feasibility Study on PKI Authentication Method with IC Card in Authentication System Sub Group of J-PARC Information System Group

Naoya TESHIMA※, Tetsuo AOYAGI, Kiyoharu HASHIMOTO*, Atsushi MANABE*, Fukuko YUASA* and Norihiro NAKAJIMA

Center for Computational Science & e-Systems,
Japan Atomic Energy Agency
Higashiueno, Taito-ku, Tokyo

(Received March 24, 2009)

The Authentication System Sub Group of J-PARC Information System Group completed the mapping of the several authentication methods in terms of the level of security. Of the methods, the PKI authentication method with IC card provides the Super High Security Level and will be adopted as the authentication method of several J-PARC Information Systems. We study the feasibility of this method with following four examples;

(1) "The EAP-TLS wireless LAN authentication method"
(2) "The Web-SSL client authentication method in SSL-VPN connection"
(3) "The PKI authentication method with a certificate issued by NAREGI-CA software stored in IC card."
(4) "The PKI authentication method with Dual interface FeliCa card"

In each example, we confirmed the feasibility of the method in a practical way. In this report we present the details of the study.

Keywords: Feasibility Study, PKI, IC Card

※ Collaborating Engineer
* Computing Research Center, High Energy Accelerator Research Organization

目　次

Contents

表リスト

図リスト

1. 序　論

1.1. 本書について

本書は、J-PARC 情報システムグループの認証システムグループで実施した J-PARC の情報システムの安全管理を行うための認証方式の実用性の検証（以下、フィージビリティ・スタディ）の結果に関し、J-PARC 情報システムの情報管理にかかわる安全性を認証方式の観点から報告するものである。

1.2. J-PARC 情報システムグループの認証システムグループについて

J-PARC（Japan Proton Accelerator Research Complex）[1]は、日本原子力研究開発機構（以下、原子力機構）と高エネルギー加速器研究機構が共同で進めるプロジェクトである。現在、MW 級の陽子ビームを作り出す加速器とそれを利用する実験施設の建設が進められており、平成 20 年度中にビーム共有を開始する予定である。

J-PARC の加速器は、リニアック、3GeV シンクロトロン および 50GeV シンクロトロンからなり、その施設（J-PARC センター）は茨城県東海村にある原子力機構の原子力科学研究所の敷地内に設置されている。施設の完成後は、MW 級の大強度陽子ビームをによる、原子核・素粒子物理の研究、物質・生命科学の研究、核変換技術の研究開発などが行われる予定である。

施設建設と並行して、J-PARC センターでのネットワーク利用や情報処理全般に関して、J-PARC 情報システムグループが様々な検討を進めている。グループには、ステアリングコミッティである情報システム事務局があり、情報システム事務局を中心として配下に以下のグループが設置されている。

- 基幹ネットワークグループ
- データベースシステムグループ
- 認証システムグループ

J-PARC センターの運用が本格化すれば、さまざまな立場の研究者が施設を利用するが、その際 J-PARC センターの基幹ネットワーク（以後、JLAN）に接続することが想定される。J-PARC 情報システムグループの認証システムグループでは、JLAN の安全な運用を最優先に、J-PARC を利用する研究者の多様な要望に応え利便性を損なうことがないよう、各種の認証要素技術の調査、検討を行っている。

1.3. フィージビリティ・スタディの目的

認証システムグループではこれまで、世の中で使用されている様々な認証要素技術をピックアップし、それぞれの特徴やメリット・デメリットに関し調査・検討を行ってきた。これまでの検討結果として、それら認証要素技術のセキュリティレベルを数値化したセキュリティレベルマップを作成した。認証システムグループで作成したセキュリティレベルマップを図 1-1 に示す。

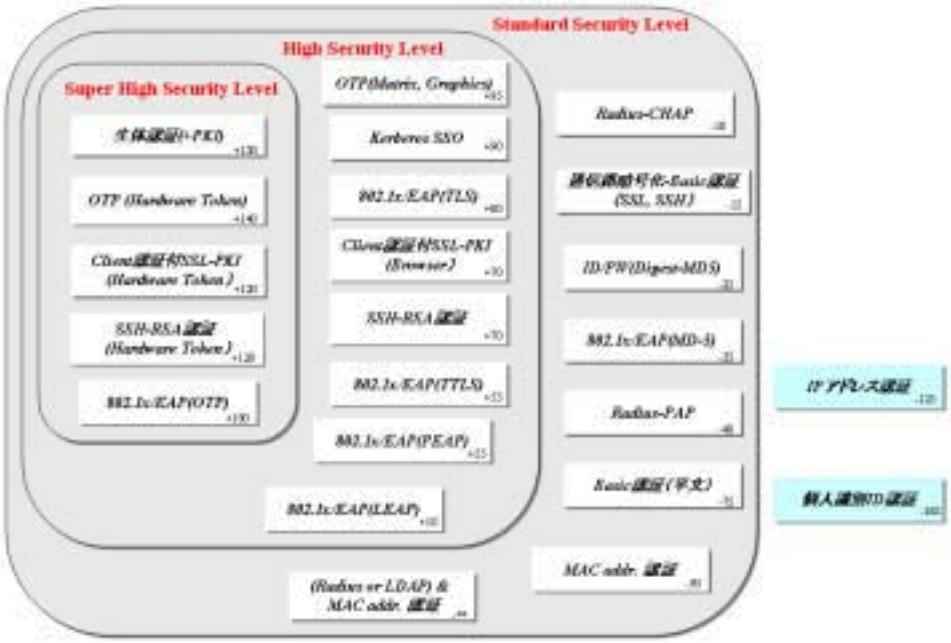

図 1-1 セキュリティレベルマップ

セキュリティレベルマップでは、認証要素技術毎に四角の枠で表現しており、その枠右下にその認証要素技術のセキュリティ強度レベルを表す値を記載している。値が大きければセキュリティ強度が高いことを意味し、セキュリティ強度レベル毎に大まかに以下分類を行なっている。

－100～0	:	セキュリティレベル標準（Standard Security Level）
0～100	:	セキュリティレベル高（High Security Level）
100～	:	セキュリティレベル最強（Super High Security Level）

セキュリティレベルマップより、セキュリティレベル最強（Super High Security Level）の認証要素技術を考えた際に、IC カードを利用した PKI 認証方式（図 1-1 における Client 認証付 SSL-PKI(Hardware Token)）は重要な技術の一つと定義されている。その理由として、強固なセキュリティを低コストで、簡易に使用可能であることが上げられる。そこで、認証システムグループでは、IC カードによる PKI 認証方式を J-PARC 情報システムに適用・導入する際の問題点を実導入前に明らかにし、その実用性を検証することを目的に、フィージビリティ・スタディを実施した。以下に、実施したフィージビリティ・スタディについての検証内容、検証手順、結果及びそれらより得られた知見について記述する。

2. 検証内容

認証システムグループでは、IC カードによる PKI 認証方式に関するフィージビリティ・スタディの検証内容を設定するにあたり、検証項目の選定基準を以下のように定めた。

【選定基準】

- その認証方式が実運用上問題あると判断された場合、それに変わる代替方式の導入が技術面、コスト面で難しいものに関する検証を優先的に選択する。
- 現在認証システムグループで導入を検討している他技術との親和性に関する検証を優先的に選択する。

以下に、上記選定基準を元に選定した検証項目とそれらの検証項目実施に当っての検証基準、尺度について記述する。

2.1. 検証項目の選定

選定基準を元に、情報システムの使用場面を網羅的に検証できるよう、実運用でのいくつかの場面を想定し、以下に示す 4 つの検証項目を選定した。

検証項目１：「EAP-TLS 無線 LAN 認証」

・ 概要

無線 LAN のアクセスポイントにおける 802.1X 個人認証の中で EAP/TLS 方式を選択した場合において、IC カードによる PKI 認証方式が適用可能かどうか検証を行う。

・ 選定理由

J-PARC の実運用に際し、J-PARC を利用する研究者が自身の PC を持ち込みネットワークに接続するという需要は多いと考えられる。その場合、有線ケーブルの必要のない無線 LAN ネットワークの方が接続ポイントを物理的に選ばなくて良いなどの観点から利便性の面で秀でている。一方、無線通信であるがゆえに通信路におけるデータの傍受が比較的容易であるため、通信の安全性を維持するためには認証と暗号化を実施する必要がある。

LAN 認証方式の規格である 802.1X の中で、他方式と比較してセキュリティ強度が高いと考えられている EAP/TLS 方式を IC カード PKI 認証で利用可能かどうかを検証することは、ユーザの利便性とネットワークの高安全性の両方を満たす上で重要であると判断し、検証項目として選定した。

検証項目２：「SSL-VPN 装置を経由した Web-SSL クライアント認証」

・ 概要

PKI 認証を使った SSL-VPN 接続後に、LAN 内の別のサービスにおいてさらに SSL 認証が必要になるような状況で、正しく認証処理が行われるかどうか検証を行う。

・ 選定理由

認証システムグループでは、JLAN 外部から JLAN へのアクセスは SSL-VPN 方式に一本化することを検討している。実運用を考えた際、JLAN 内で運用されるサービスでその認証に SSL クライアント認証を使用するサービスは存在すると考えられる。

IC カードによる PKI 認証方式が、SSL-VPN 接続後に JLAN 内のサービスでさらに SSL 認証が必要になる状況下においてもその使用に問題がないか検証することは、IC カードの採用を判断する上で重要な要素のひとつであると考え、検証項目として選定した。

検証項目３：「NAREGI-CA ソフトウェアが発行する証明書による IC カード PKI 認証」

・ 概要

NAREGI-CA ソフトウェア[2]で構築した認証局で証明書を発行した証明書を IC カードに格納し、PKI 認証が正常に実施できるか検討を行う。

・ 選定理由

認証システムグループでは、J-PARC 認証システム基盤として NAREGI-CA ソフトウェアで構築した認証局の使用を検討している。

NAREGI-CA ソフトウェアで構築した認証局と IC カードによる PKI 認証方式との親和性の面、実用性の面で問題ないか検証することは、その採用を検討する上で重要であると考えられる。

検証項目４：「Dual カードタイプ FeliCa を使用した PKI 認証」

・ 概要

証明書を格納した Dual カードタイプ FeliCa を使用し、PKI 認証が正常に実施できるか検証を行う。

・ 選定理由

J-PARC では一部の施設への入退室に非接触型の FeliCa の使用が検討されている。通常タイプの FeliCa カードの場合、PKI 方式の処理を行うことはできないが、接触型と非接触型の両方の機能を有する Dual カードタイプ FeliCa では、その接触型通信によりそれを可能としている。Dual カードタイプ FeliCa を使用し、IC カードの PKI 認証方式が使用可能であれば利用者は施設利用において複数のカードを持つ必要がなく利便性の面で有用である。

Dual カードタイプ FeliCa を使用した IC カードによる PKI 認証の実用面での問題点を検証することはその採用を検討する上で重要であると考えられる。

2.2. 検証基準及び検証尺度の設定

本検証にて、検証結果を評価するための検証基準及びその達成度合いを判断するための客観的な検証尺度を表 2-1 のように定めた。

表 2-1 検証基準及び検証尺度

#	検証基準		検証尺度	
(1)	機能実現性	それぞれ想定された使用場面において、目的とする機能が実現できているかどうかを判定する	○	目的の機能が実現されている場合
			△	実現されていないが目的に合致した代替案がある場合
			×	代替案もない場合
(2)	ユーザ利便性	それぞれ想定された使用場面において、その機能を使用する上でのユーザの使い勝手について判定する。	○	通常の PC 使用場面と比較して、使い勝手の低下が見られない場合
			△	少々の使い勝手の低下は見られるが使用には問題がない場合
			×	使い勝手を損なっており使用に重大な欠陥がある場合
(3)	導入容易性	それぞれ想定された使用場面において、それを使用する前準備であるハードウェア及びソフトウェア等のインストール、セットアップが容易に実施可能かどうかを判定する。ユーザが実施するクライアント側の作業と共に、管理者が実施するサーバ側の作業も含めて判定する。	○	通常の PC 使用場面でのアプリケーション導入と比較して、容易性の低下が見られない場合
			△	少々の低下が見られるが許容範囲である場合
			×	容易性が損なわれその導入に困難さが見られる場合

機能実現性に関する検証においては、目的としている機能が実現できているかどうかを判断する。もし目的としている機能を実現していなければ、それが他の観点でどんなに優れた技術であったとしても採用することはできないため、本検証における検証基準の中で最も重視すべき点だと考えられる。

ユーザ利便性に関する検証においては、ユーザにとっての使い勝手などの点を判断する。それが損なわれるとユーザの不満に直接的につながりやすく、ユーザの JLAN に対する評価を大

きく左右する重要な基準だと考えられる。

導入容易性に関する検証においては、ユーザ又は管理者のソフトウェアやハードウェアの初期導入の容易さを判断する。初期導入時の障壁は、前項のユーザ利便性と同じくユーザの不満につながりやすく、重要な基準だと考えられる。ただし 1 回実施することで次回以降はその大部分は実施の必要がなくなると考えられ、またマニュアル類の整備などである程度の緩和が図れると考えられ、他 2 基準と比較するとその重要度は低く設定できると考えられる。

3. 検証手順

検証手順・方法について、以下に記載する。

なお、詳細な手順については付　録１ 環境構築手順及び検証手順詳細を、略語等については付　録２ 用語集を参照のこと。

(1) 検証項目 1

(1-1) 検証環境

検証環境構成図を図 3-1 に示す。

MacOS、WindowsOS を搭載したクライアント端末から、無線 LAN アクセスポイントへの接続時に、RADIUS サーバにて IC カードによる個人認証を行い、無線 LAN 接続の許可・不許可を判別する検証を行う。

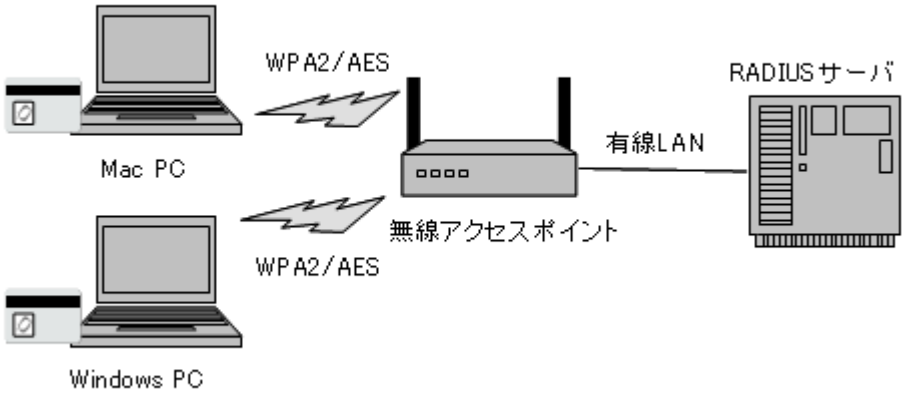

図 3-1 検証環境模式図（検証項目１）

(1-2) サーバ・機器構成

今回検証に使用したサーバ・機器構成は以下の通りである。

- Windows クライアント環境

OS	WindowsXP SP2
IC カード	原子力機構身分証
IC カードリーダ	SCR3310-NTTCom[3]
認証ライブラリ	eSK ツール

- MacOS クライアント環境

OS	MacOSX 10.4.10
IC カード	原子力機構身分証
IC カードリーダ	SCR3310-NTTCom

認証ライブラリ	eSK ツール

- RADIUS サーバ環境

OS	CentOS 4.4
認証サーバ	freeRADIUS 1.0.1

- 無線 LAN アクセスポイント機器

使用機器	enterasys RoamAbout RBT-4102[4]

(2) 検証項目２

(2-1) 検証環境

検証環境模式図を図 3-2 に示す。

まず WindowsOS または MacOS 搭載のクライアントから SSL-VPN 装置への認証に IC カードに格納した証明書を使用し SSL-VPN 接続を確立する。その後、SSL-VPN 接続を介して、その背後の各種サービス(メールサービス、グリッドサービス、ファイルサービス)の認証に SSL-VPN 認証時と同様に IC カードに格納した証明書を用いた認証の検証を行う。

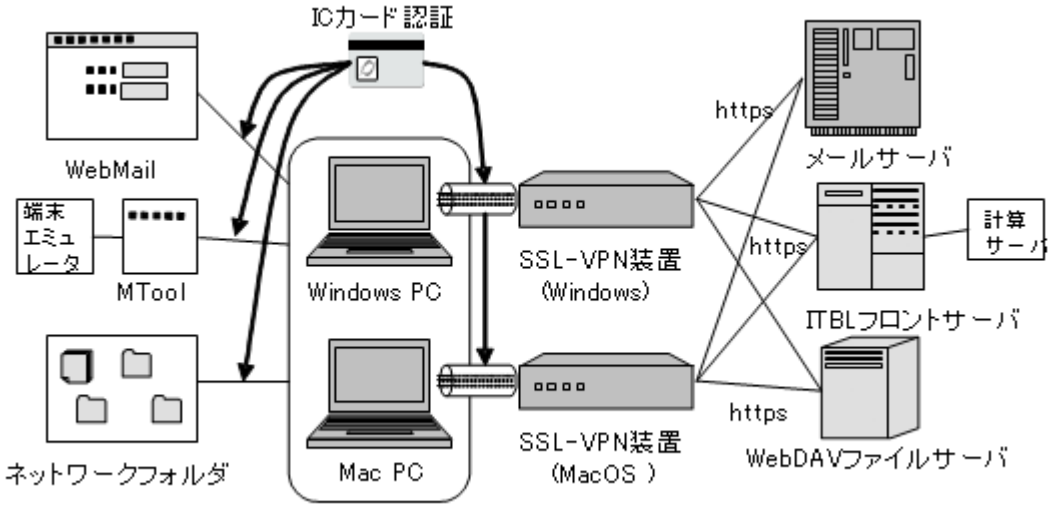

図 3-2 検証環境模式図（検証項目２）

(2-2) サーバ・機器構成

今回検証に使用したサーバ・機器構成は以下の通りである。

- Windows クライアント環境

OS	WindowsXP SP2
IC カード	原子力機構身分証
IC カードリーダ	SCR3310-NTTCom
認証ライブラリ	eSK ツール

- MacOS クライアント環境

OS	MacOSX 10.4.10
IC カード	原子力機構身分証

IC カードリーダ	SCR3310-NTTCom
認証ライブラリ	eSK ツール

- SSL-VPN 装置

使用機器（Windows 用）	F5 Networks 社の FirePass[5]
使用機器（MacOSX 用）	Juniper Networks 社の Secure Access[6]

(3)　検証項目３

(3-1)　検証環境

検証環境模式図を図 3-4、図 3-4 に示す。

図 3-3 には、証明書発行環境の模式図を示す。NAREGI-CA ソフトウェアを使用し、認証局となる CA サーバと、登録局となる RA サーバ及び証明書管理、失効リスト管理を行う LDAP サーバからなる。

図 3-4 には、WindowsOS または MacOS を搭載したクライアント端末から、SSL-VPN の認証及びテストサーバを利用した SSL クライアント認証において、NAREGI CA ソフトウェアにより構築した CA から発行された証明書を格納した IC カードを使用し、SSL-VPN 接続の確立又はサービスアクセスの検証を実施する。

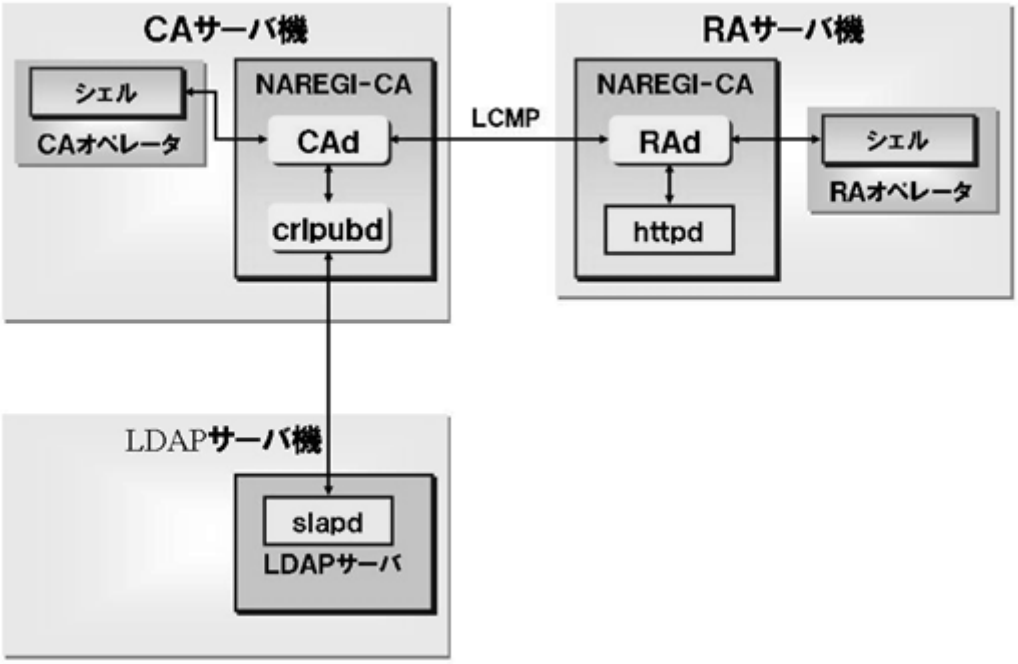

図 3-3 検証環境模式図（検証項目３－１）

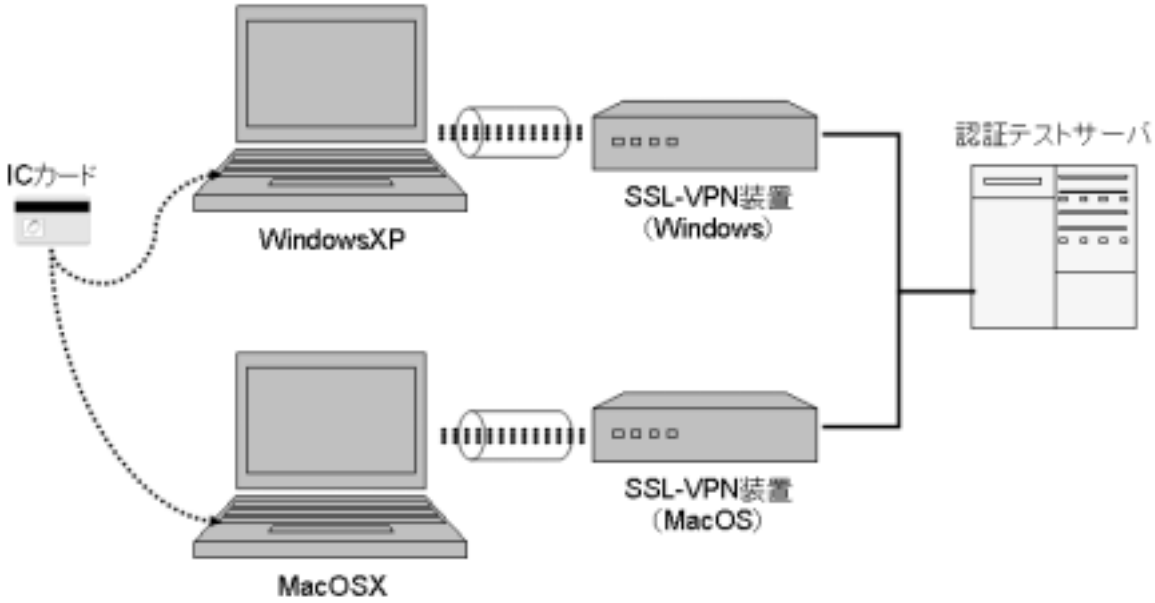

図 3-4 検証環境模式図（検証項目３－２）

(3-2)　サーバ・機器構成

今回検証に使用したサーバ・機器構成は以下の通りである。

【証明書発行環境】

- CA/RA サーバ機

OS	Red Hat Enterprise Linux ES release4
NAREGI-CA	Version 2.2

- LDAP サーバ機

OS	Red Hat Enterprise Linux ES release4
LDAP	OpenLDAP 2.2.13

【検証環境】

- Windows クライアント環境

OS	WindowsXP SP2
IC カード	原子力機構身分証
IC カードリーダ	SCR3310-NTTCom
認証ライブラリ	eSK ツール

- MacOS クライアント環境

OS	MacOSX 10.4.10
IC カード	原子力機構身分証
IC カードリーダ	SCR3310-NTTCom
認証ライブラリ	eSK ツール

- SSL-VPN 装置

使用機器 （**Windows** 用）	F5 Networks 社の FirePass
使用機器	－（実施せず）

（MacOSX 用）	

(4)　検証項目４

(4-1)　検証環境

検証環境模式図を図 3-5 に示す。

WindowsOS または MacOS を搭載したクライアント端末から、SSL-VPN の認証及びテストサーバを利用した SSL クライアント認証において、証明書を格納した Dual カードタイプ Felica を使用して、SSL-VPN 接続の確立又はサービスアクセスの検証を実施する。

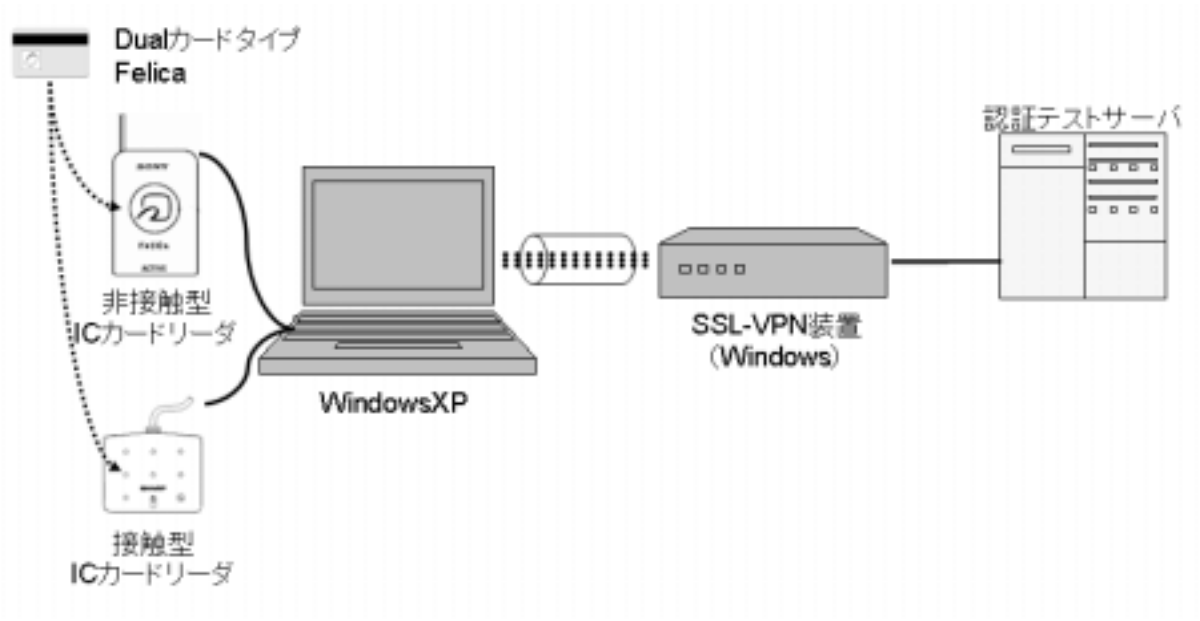

図 3-5 検証環境模式図（検証項目４）

(4-2)　サーバ・機器構成

今回検証に使用したサーバ・機器構成は以下の通りである。

- Windows クライアント環境

OS	WindowsXP SP2
IC カード	RC-S952/3MV[7]
IC カードリーダ	非接触タイプ：PaSoRi RC-S320[8] 接触タイプ　：SCR3310-NTTCom
認証ライブラリ	Felica PKI Option

- MacOS クライアント環境

OS	ー（実施せず）
IC カード	ー（実施せず）
IC カードリーダ	ー（実施せず）
認証ライブラリ	ー（実施せず）

- SSL-VPN 装置

使用機器	F5 Networks 社の FirePass

（Windows 用）	
使用機器 （MacOSX 用）	ー（実施せず）

4. 検証結果

検証結果の一覧を表 4-1 に示す。

表 4-1 では、実施した各検証項目に対する2.2 節で定めた検証基準毎の結果を記載している。

表 4-1 検証結果一覧

検証項目	ｸﾗｲｱﾝﾄ OS	検証基準			
		機能実現性	ユーザ利便性	導入容易性	
				ｸﾗｲｱﾝﾄ	ｻｰﾊﾞ
検証項目１	Windows XP	○	○	○	△
	MacOSX	○	○	○	
検証項目２	Windows XP	○	○	○	○
	MacOSX	○	○	○	
検証項目３	Windows XP	○	○	○	△
	MacOSX	○	○	○	
検証項目４	Windows XP	○	○	○	―
	MacOSX	×	―	―	

以下に、それぞれの検証項目毎に詳細な検証結果について記述する。

(1) 検証項目１

(1-1) 機能実現性

クライアント端末の OS が Windows XP の場合、SP2 に対して WPA2 のサポートのためパッチ（ワイヤレス クライアント更新プログラム (KB917021)[3]）適用が必要であることが判明した。通常の Windows XP SP2 のみの適用では導入されず、利用する Windows XP SP2 端末で該当パッチが適用されていない場合、Microsoft のページからダウンロードしパッチ適用する必要がある。その他設定、認証においては問題は検出されなかった。以上より、Windows XP クライアント端末の場合の機能実現性を○と判断する。

クライアント端末の OS が MacOSX で、OS のキーチェーンに認証とは無関係な証明書が格納された場合、RADIUS サーバ（freeRADIUS1.0.1）が異常終了する可能性があることが確認された。また、MacOSX では無線 LAN 認証方式の選択が自動となり、選択される認証方式は前回アクセスした認証方式に依存していることが確認された。

MacOSX 検証時の freeRADIUS サーバの異常終了に関して、MacOSX のキーチェーンに無関係な証明書を加えないことで回避が可能であり、また本件 freeRADIUS v1.0.1 に内在するバグであり既に修正版がリリースされていることを確認している[10]。実運用に当っては、アクセス認証サーバとして freeRADIUS を使用する場合、freeRADIUS のバージョンに留意し、上記バグ修正版以降のバージョンを使用することが必要である。また、MacOSX での無線 LAN 認証方式の自動選択された件、検証環境構築時の確認不足であり、MacOSX サポートページ[11]に記載された認証方式設定手順にて正常に TLS を設定できることを確認している。明示的に TLS 設定された状態での認証の検証は実施していないが、自動選択状態で TLS が選択された場合の正常認証を確認しており、明示的に指定した場合でも問題ないと推測される。以上より、MacOSX クライアント端末の場合の機能実現性を○と判断する。

(1-2)　ユーザ利便性

Windows XP および MacOSX 端末とも、IC カードでの認証時におけるユーザ利便性の低下につながるような事象はみられなかった。以上より、ユーザ利便性を○と判断する。

(1-3)　導入容易性

Windows XP, MacOSX クライアント端末の場合、無線 LAN の設定に関してその設定手順は OS 毎に異なり、また設定ミスを導きやすい手順が見受けられ、実際の検証時でも設定の間違いが見られた。ただし、本検証を受け、その手順を明確化し、ドキュメントとして整備することで導入時には回避可能であると考えられる。以上より、両 OS 共にクライアントの導入容易性を○と判断する。

サーバ機器の場合、今回使用した freeRADIUS サーバの設定は、サーバのターミナルから設定ファイルを直接テキスト編集する必要がある。UNIX 系 OS の操作に不慣れな管理者の場合、その設定手順には困難さが伴うと思われる。しかし、もし RADIUS サーバとして今回使用した freeRADIUS ではなく商用のソフトウェアを使用するのであれば、このような点は改善されている可能性が高い。以上より、サーバの導入容易性を△とする。

(2)　検証項目２

(2-1)　機能実現性

Windows XP, MacOSX クライアント端末共に、IC カードにより正常に認証できることが確認された。以上より、その機能実現性を、両 OS 共に○と判断する。

(2-2)　ユーザ利便性

Windows XP および MacOSX 端末とも、IC カードでの認証時におけるユーザ利便性の低下につながるような事象はみられなかった。以上より、両 OS 共にユーザ利便性を○と判断する。

(2-3)　導入容易性

Windows XP, MacOSX クライアント端末とも、導入時に問題となる点は見受けられなかった。以上より、両 OS 共クライアントの導入容易性を○と判断する。

SSL-VPN の導入に関し、専用の管理コンソールの GUI による設定が可能であり、導入に伴う困難さは見受けられなかった。以上より、サーバの導入容易性を○と判断する。

(3)　検証項目３

(3-1)　機能実現性

Windows XP, MacOSX クライアント端末共に、IC カードにより正常に認証できることが確認された。以上より、両 OS 共に機能実現性を○と判断する。

(3-2)　ユーザ利便性

Windows XP および MacOSX 端末とも、IC カードでの認証時におけるユーザ利便性の低下につながるような事象はみられなかった。以上より、両 OS 共にユーザ利便性を○と判断する。

(3-3)　導入容易性

Windows XP, MacOSX クライアント端末への導入に関して、問題点は検出されなかった。以上より、両 OS 共にクライアントの導入容易性を○と判断する。

一方 CA 環境構築では、当初 CA サーバと RA サーバが連携し、ユーザからの証明書発行申請、RA オペレータによる操作を受け、動的に CA サーバへ証明書発行依頼が行われる構成を検討していた。しかし、公開されている NAREGI ソフトウェアに関するドキュメント手順に従い環境構築を実施したが、CA サーバと RA サーバ間の動的な連携環境を構築することができなかった。そのため、証明書発行依頼を人手で引き渡し、証明書を発行することとし検証を実施した。当

検証で実施したように回避策はあるが、実運用では問題となると考えられる。以上より、サーバの導入容易性を△と判断する。

(4)　検証項目４

(4-1)　機能実現性

Windows XP クライアント端末の場合、カードへの証明書の書き込み、非接触／接触カードリーダを通して、正常に認証できることが確認された。以上より、Windows XP の場合の機能実現性を○と判断する。

MacOSX クライアント端末の場合、製品提供元より MacOSX 向け認証ライブラリ（WindowsXP 版は FeliCa カードリーダ付属）が提供されていないため、MacOSX での検証は実施できなかった。そのため、今後製品提供元より MacOSX 向け認証ライブラリが提供されるまで、MacOSX での機能を実現することはできない。以上より、MacOSX 端末の場合の機能実現性を×と判断する。

(4-2)　ユーザ利便性

Windows XP クライアント端末の場合、IC カードでの認証時におけるユーザ利便性の低下につながるような事象はみられなかった。以上より、Windows XP 端末のユーザ利便性を○と判断する。

MacOSX クライアント端末の場合、機能実現不可能のため検証は実施していない。

(4-3)　導入容易性

Windows XP クライアント端末の場合、必要なソフトウェアの導入はすべてインストーラにより行われ、困難な点は見受けられなかった。以上より、Windows XP 端末の導入容易性を○と判断する。

MacOSX クライアント端末の場合、機能実現不可能のため検証は実施していない。

また、本検証では、サーバ機器へソフトウェアの導入等は必要なかった。

5.　まとめ

J-PARC 情報システムでの使用が想定される IC カードによる PKI 認証方式に対し、JLAN に適用・導入する際に生じうる課題の抽出を目的として、フィージビリティ・スタディを実施した。フィージビリティ・スタディでは、４つの検証項目についてクライアント端末として Windows XP SP2 および MacOSX10.4 を対象として、機能実現性、ユーザ利便性、導入容易性の検証基準により検証を実施した。

その結果、一部検証項目において検証で使用した製品の提供元より MacOSX 用のライブラリが供給されていないため機能実現できないことが判明したが、他検証においては大きな問題点は見受けられなかった。ユーザ利便性の点では、どの検証項目においても問題は検出されなかった。いくつかの検証項目において、主に使用したソフトウェアのセットアップ手順が不明確な点があり、導入容易性について少々問題点が見受けられた。ただしこれは、本フィージビリティ・スタディを受け、導入手順等の明確化を図りドキュメントとして整備することで、実際の導入時には解消されることが期待される。

IC カードを使用した PKI 認証方式は、それを J-PARC の認証方式として採用した場合に想定される様々な使用場面において、Windows XP または MacOSX などののクライアント環境によらず、ユーザ利便性の低下も伴わず、機能実現性が確保されることが確認された。

謝　辞

J-PARC 情報システムグループのリーダである、平山 俊雄 日本原子力研究開発機構システム計算科学センターセンター長、及び川端 節彌 高エネルギー加速器研究機構計算科学センターセンター長には、本フィージビリティ・スタディを始めとした認証システムグループの活動に対し、有益な助言を多くいただいた。ここに感謝を表する。

参考文献等

[1] J-PARC ホームページ http://j-parc.jp/
[2] NAREGI CA ソフトウェア http://middleware.naregi.org/Download/
[3] エヌ・ティ・ティ・コミュニケーションズ社 SCR3310-NTTCom http://www.ntt.com/jpki/
[4] エンテラシス・ネットワークス社 RoamAbout RBT-4102 http://secure.enterasys.com/jp/products/wireless/RBT-4102/
[5] F5 ネットワークスジャパン社 FirePass http://www.f5networks.co.jp/product/firepass/index.html
[6] ジュニパーネットワークス社 Secure Access http://www.juniper.co.jp/products_and_services/ssl_vpn_secure_access/
[7] ソニー社 RC-S952/3MV http://www.sony.co.jp/Products/felica/pdt/dmd.html
[8] ソニー社 PaSoRi RC-S320 http://www.sony.co.jp/Products/felica/pdt/rdw3.html
[9] Windows XP SP2 用ワイヤレス クライアント更新プログラム (KB917021) http://support.microsoft.com/kb/917021/ja
[10] freeRADIUS Bugzilla Bug 94 http://bugs.freeradius.org/show_bug.cgi?id=94
[11] MacOSX サポート http://docs.info.apple.com/article.html?path=Mac/10.4/jp/mh1736.html

付　録１　環境構築手順及び検証手順詳細

(1)　検証項目 1

1. RADIUS サーバの準備

1.1 既存の CentOS4.4(dir.edo.jaea.go.jp)に freeRADIUS1.0.1 をインストール

```
# yum install freeradius.i386
```

1.2 パーソナルファイアーウォールの穴あけ

```
# system-config-securitylevel-tui
  radius:udp を追加。
```

1.3 乱数ファイルの作成

```
# dd -if=/dev/urandom of=/etc/raddb/cetrs/dh count=1 bs=128
# dd -if=/dev/urandom of=/etc/raddb/cetrs/random count=1 bs=128
```

1.4 サーバ証明書の用意

1.4.1 試験用サーバ CA 局の構築

```
$ cp /usr/share/ssl/misc/CA .
$ cp /usr/share/ssl/openssl.cnf .
```

拡張キー使用法に TLS Web Server Authentication を含めるようにする。
openssl.cnf の [usr_cert] セクションに以下を追加（Windows で必要）
extendedKeyUsage = 1.3.6.1.5.5.7.3.1

```
$ ./CA -newca
  ⇒  demoCA/cacert.pem              CA 証明書　DN は newreq 参照。CN=TESTCA
  ⇒  demoCA/private/cakey.pem       CA 秘密鍵
```

1.4.2 試験用サーバ証明書の発行

```
$ ./CA -newreq    ⇒  newreq.pem   証明書要求
  Country Name            : JP
  State or Province Name  : Tokyo
  Locality Name           : Taito-ku
  Organization Name       : JAEA
  Organization Unit Name  : CCSE
  Common Name             : dir.edo.jaea.go.jp
$ ./CA -sign      ⇒  newcert.pem  証明書
# cp newcert.pem /etc/raddb/certs/svr8cert.pem      サーバ証明書
# cp newreq.pem /etc/raddb/certs/svr8key.pem        サーバキーファイル
```

1.5 構成ファイルの変更

・/etc/raddb/radiusd.conf を編集、authorize セクションに eap を追加

```
authorize {
   preprocess
   eap
   files
}
```

・/etc/raddb/radiusd.conf を編集、authenticate セクションに eap を追加

```
authenticate {
   unix
   eap
```

```
    }

・/etc/raddb/eap.conf を編集、eap セクションをアンコメント、内容変更
  eap {
     default_eap_type = tls
     md5,laep,get,mschapv2 セクションをコメントアウト
     tls {
        private_key_password = xxxxxxxx
        private_key_file = ${raddbdir}/certs/svr8key.pem
        certificate_file = ${raddbdir}/certs/svr8cert.pem
        #CA_file = ${raddbdir}/certs/jaeaca.pem   身分証 CA 局証明書
        又は
        CA_file = ${raddbdir}/certs/itblrca.cer   ITBL CA 局証明書
        dh_file = ${raddbdir}/certs/dh
        random_file = ${raddbdir}/certs/random
        fragment_size = 1024
        include_length = yes
     }
  }

・/etc/raddb/clients.conf を編集、無線ＡＰのアドレス範囲と共有鍵を指定
  client 172.17.0.0/22 {
     secret      = soft99
     shortname   = private-network-2
  }
```

2. 無線アクセスポイントの設定

enterasys RoamAbout RBT-4102 を使用した。

2.1 システム初期設定

・Reset ボタンを５秒以上押して構成を工場出荷時に戻す。

・コンソールケーブルをＰＣのシリアルインターフェースに接続してログイン

```
Username: admin
Password: password
```

・Web インターフェースが利用可能になるまでの初期設定を行う

```
# configure
(config)# interface ethernet
(if-ethernet)# no ip dhcp
(if-ethernet)# exit
# reset board

再起動後、ログイン
# configure
(config)# interface ethernet
(if-ethernet)# ip adddress 172.17.3.73 255.255.252.0 172.17.3.225
(if-ethernet)# end
(config) # exit
```

2.2 Web インターフェースからの設定

・TCP/IP Settings

```
IP Address:      172.17.3.73
Subnet Mask :    255.255.252.0
Default Gateway: 172.17.3.225
```

```
Primary DNS:     172.17.0.1
Secondary DNS:   172.17.0.2
```

・RADIUS の設定

```
・Primary RADIUS Server Setup 画面で
IP Address/Server Name:dir.edo.jaea.go.jp
Port Number:          1812
Key:                  Soft99
Confirm Key:          Soft99
```

・802.11a Interface Radio Setting

```
Interface Status: Disable
```

・802.11b/g Interface Radio Setting

```
Interface Status: Enable
Network Name(SSID):RoamAbout Default Network Name 0
Secure Access: Enable
Radio Channel: 3
```

・802.11b/g Interface Security の設定

```
Detail Setting → Default Interface
Authentication Type Setup
          Type:     WPA(Windows)/WPA2(MacOSX)
          Encryption:   Enable
WPA/WPA2 Clients:   Required
Multicast Cipher Mode:  TKIP(Windows)/AES-CCMP(MacOSX)
802.1x Setip:       Required
MAC Authentication: Disable
```

3. WindowsXP からのアクセス

【検証に使用した WindowsXP クライアント端末情報および無線 AP の設定情報】

・Panasonic Let's note CF-W4、WindowsXP Pro SP2
・IC カードリーダライタ：SCR3310-NTTCom、インストール済み
・機構身分証用認証ライブラリ eSK ツール、インストール済み
・**WindowsXP SP2 における WPA2 のサポートのため以下パッチ適用が必要。適用済み。**
　・**ワイヤレス クライアント更新プログラム (KB917021)**
　・**参考 URL : http://support.microsoft.com/kb/917021/ja**
・無線ＡＰの認証設定を WPA2/AES に設定する。

3.1 ITBL 証明書による接続

・/etc/raddb/eap.conf の eap セクションの CA_file を ITBLCA 証明書に設定する
・RADIUS サーバ起動
　# radiusd
・WindowsXP に ITBL 証明書をインストールする。証明書のインポートウィザードで「秘密鍵の保護を強力にする」を**選択してはならない**。
・コントロールパネル→ネットワーク接続→ワイヤレスネットワーク接続。ここを右クリックしてプロパティを表示→ワイヤレスネットワークタブ→追加
　アソシエーションタブで以下を入力・選択
　　ネットワーク名(SSID)：RoamAbout Default Network Name 0
　　ネットワーク認証：WPA2
　　データ暗号化：AES

認証タブで以下を入力・選択
EAP の種類：スマートカードまたはその他の証明書
プロパティをクリックして以下を選択
接続のための認証方法：「このコンピュータの証明書を使う」を選択
「単純な証明書の選択を使う」を選択
「サーバ証明書を有効化する」のチェックを外す。
注）これは正確には「サーバ証明書を検証する」である。**1.4.1** で作成したサーバ証明書のＣＡ証明書をシステムストアの「信頼されたルート証明機関」にインストールしている場合は、「サーバ証明書を有効化する」を選択できる。
ＯＫをクリック
ＯＫをクリック
・接続成功

3.2 機構身分証明書による接続
・/etc/raddb/eap.conf の eap セクションの CA_file を身分証ＣＡ証明書に設定する
・RADIUS サーバ再起動
kill -HUP `cat /var/run/radiusd/radius.pid`
・IC カードリーダライタを接続、機構身分証をセット
・コントロールパネル→ネットワーク接続→ワイヤレスネットワーク接続。ここを右クリックしてプロパティを表示→ワイヤレスネットワークタブ→`RoamAbout Default Network Name 0` 選択→プロパティをクリック
アソシエーションタブで以下を確認
ネットワーク認証：`WPA2`
データ暗号化：`AES`
認証タブで以下を入力・選択
EAP の種類：スマートカードまたはその他の証明書
プロパティをクリックして以下を選択
接続のための認証方法：「自分のスマートカードを使う」を選択
「サーバ証明書を有効化する」のチェックを外す。
ＯＫをクリック
ＯＫをクリック
・資格情報の選択バルーンをクリック→スマートカードにアクセスしています→ＰＩＮ入力→ＯＫ
・接続成功

4. MacOS10.4 からのアクセス
【検証に使用した MacOS および無線 AP の設定情報】
・Mac iBook G4、MacOS10.4.10
・IC カードリーダライタ：SCR3310-NTTCom、インストール済み
・機構身分証用認証ライブラリ eSK ツール、インストール済み
・無線ＡＰの認証設定を WPA2/AES に設定する。

4.1 ITBL 証明書による接続
・/etc/raddb/eap.conf の eap セクションの CA_file を ITBLCA 証明書に設定する
・RADIUS サーバ再起動
kill -HUP `cat /var/run/radiusd/radius.pid`
・キーチェインアクセスを起動し、環境設定→「自分のキーチェインをリセット」をクリック

注）キーチェインに接続に無関係な証明書と秘密鍵が格納されていると **freeRADIUS** がセグメンテーションフォールトを起こす。
注２）本件、**freeRADIUS** サーバ（**ver1.0.1**）のバグであり、バージョン **1.0.5** にて修正されていることを確認。

・MacOS に ITBL 証明書をインストールする。「ログイン」キーチェインに格納するよう指示する。
・システム環境設定→ネットワーク→AirMac を選択して「設定」をクリック→追加
　ネットワーク名：RoamAbout Default Network Name 0
　ワイヤレスセキュリティ：WPA2 エンタープライズ
　ユーザ名：(入力しない)
　パスワード：(入力しない)
　802.1X 設定：自動　（**EAP-TLS** を明示的に選択できない）
ＯＫをクリック→今すぐ適用

・システム環境設定→ネットワーク→AirMac を選択して「接続」をクリック。インターネット接続アプリが起動する。→AirMac を入にする
[接続できないケース]
　802.1X 認証のユーザ名とパスワードを入力する画面が出現する。→接続失敗
[接続できるケース]
　このサーバ証明書を検証できませんでした。ルート証明書が見つかりません→続ける→接続成功
注）接続可否は直前の無線 **LAN** の接続方法が何であったかに依存している。直前に **EAP-TLS** 認証している場合は成功する。どちらになるのか、明確な条件を見出すことができなかった。
注２）自動選択は設定手順のミスで、**MacOSX** サポートページ（**http://docs.info.apple.com/article.html?path=Mac/10.4/jp/mh1736.html**）に記載された手順にて認証方式を **EAP-TLS** に設定可能であることを確認している。設定方法については、下記「**MacOSX** での **EAP-TLS** 設定方法」を参照のこと。

4.2 機構身分証明書による接続
・/etc/raddb/eap.conf の eap セクションの CA_file を機構身分証明書に設定する
・RADIUS サーバ再起動
　# kill -HUP `cat /var/run/radiusd/radius.pid`
・MacOS に ITBL 証明書をインストールする。「ログイン」キーチェインに格納するよう指示する。
・システム環境設定→ネットワーク→AirMac を選択して「設定」をクリック、以下を確認
　ネットワーク名：RoamAbout Default Network Name 0
　ワイヤレスセキュリティ：WPA2 エンタープライズ
　ユーザ名：(入力しない)
　パスワード：(入力しない)
　802.1X 設定：自動
ＯＫをクリック→今すぐ適用

・システム環境設定→ネットワーク→AirMac を選択して「接続」をクリック。インターネット接続アプリが起動する。→AirMac を入にする
・キーチェーンのパスワードを入れてください。→ＰＩＮを入力
　・このサーバ証明書を検証できませんでした。ルート証明書が見つかりません→続け

る
・接続成功

※ MacOSX での EAP-TLS 設定方法

1. 「インターネット接続」(「アプリケーション」フォルダにあります）を開く。
2. 「ファイル」＞「新規 802.1X 接続」と選択する。
3. 「設定」ポップアップメニューから設定を選択する。使用可能な設定がない場合は、「設定を編集」を選択し、新しい設定を作成する。ネットワーク管理者から入手した情報を入力する。
4. 「設定」ウインドウの下部にある「追加」（＋）または「削除」(-) ボタンをクリックして、設定を追加または削除できます。
5. 「ネットワークポート」ポップアップメニューから「AirMac」または「内蔵 Ethernet」を選択する。「AirMac」を選択した場合は、「ワイヤレスネットワーク」ポップアップメニューから AirMac ネットワークを選択する。
6. 必要に応じて、ネットワークの名前とパスワードを入力する。
7. 「接続」をクリックし接続する。

(2) 検証項目 2

【クライアント端末が WindowsXP SP2 の場合】

1 テストに使用するクライアントの設定

・Panasonic Let's note CF-W4、WindowsXP Pro SP2
・IC カードリーダライタ：SCR3310-NTTCom、インストール済み
・機構身分証用認証ライブラリ eSK ツール、インストール済み

2 SSL-VPN 装置の設定

SSL-VPN 装置として F5 Networks 社の FirePass を使用した。

・ブラウザで FirePass にログインし、管理コンソールをクリック。
・FirePass に機構身分証のＣＡ局証明書をインストールする。
　・デバイス管理：セキュリティ：証明書　をクリック
　・「クライアントルート証明書とＣＲＬのインストール」のセクションで「クライアントルート証明書」をクリック。
　・「ＰＥＭフォーマットで新しいクライアントルート証明書を表示するか、以下のボックスに貼り付けてください：」のフィールドで「参照」をクリックして機構身分証のＣＡ局証明書をインストール
　・サービスを再起動
　・「クライアントルート証明書とＣＲＬのインストール」のセクションで「ログイン時、クライアント証明書を要求」をチェック。「ログインユーザ名に証明書のコモンネーム（ＣＮ）を使用」を選択して「更新」をクリック

・FirePass に利用者を登録する。
　・ユーザ：グループ：マスターグループ　をクリック
　・「新しいグループを作成」を選択して以下を入力する。
　　新しいグループ名：usercert
　　認証方法：クライアント証明書（パスワード無し）
　　「作成」をクリック
　・リソースグループタブを選択して「選択済み」に sslvpn を追加、「更新」をクリック

・アカウント aoyagi.tetsuo を作成する。
　・ユーザ：ユーザ管理　をクリック

ユーザアカウントの作成で「個別入力」を選択、「Ｇｏ」をクリック、aoyagi.tetsuo を追加。

3 SSL-VPN 装置へログイン
・身分証明書を使ってログイン。アカウント aoyagi.tetsuo。
・「メールサーバへのリモートエントリー」（ＶＰＮ）をクリック。
・接続成功、PC に PPP adapter のインターフェースが出現。ＰＣ側 192.168.10.170, ネット側 133.53.8.59

4 クライアント認証付き Web サーバにアクセス
・Internet Explorer と Firefox で https://ms.jaea.go.jp/webmail をアクセス。証明書に機構身分証を選択→アクセス成功
・MTool（ITBL のアプリケーションの１つ。クライアント認証付き SSL でサーバと接続する）を介して端末エミュレータ(TeraTerm)から計算サーバ(jaerif)をアクセス。証明に機構身分証を選択→アクセス成功。３０分ほどログインしていたが、問題は発生しなかった。このときの経路は TeraTerm→(MTool→(PPP adapter→FirePass)→ITBL フロントサーバ)→ITBL 中継サーバ→jaerif。
・AEGIS コミュニティのアクセス。WebDAV ファイルサーバをクライアント認証付き https でネットワークフォルダとして表示→成功。

【クライアント端末が MacOSX 10.4 の場合】
5 テストに使用するクライアントの設定
・Mac iBook G4、MacOS10.4.10
・IC カードリーダライタ：SCR3310-NTTCom、インストール済み
・機構身分証用認証ライブラリ eSK ツール、インストール済み

6 SSL-VPN 装置の設定
SSL-VPN 装置として Juniper Networks 社の Secure Access を使用した。
・ＣＡ証明書は既にインストール済み。
・テスト用に機構ネットワークを直接利用可能とする登録をしていただいた（情報システム管理室）。

7 SSL-VPN 装置へログイン
・身分証明書を使ってログイン。アカウント、パスワードは空欄。レルム Client_Certificate_Group。
・クライアントアプリケーションセッションで「ネットワークコネクト」を開始する。
・クライアントソフトウェアのダウンロードとインストールが開始される。
・接続成功、PC に新しいインターフェース jnc0 が出現。ＰＣ側 133.53.249.103, ネット側も同じ。

8 クライアント認証付き Web サーバにアクセス
・Safari と Firefox で https://ms.jaea.go.jp/webmail をアクセス。問題なし。
・MTool（ITBL のアプリケーションの１つ。クライアント認証付き SSL でサーバと接続する）を介して端末(Terminal)から計算サーバ(jaerif)をアクセス。証明に機構身分証を選択→アクセス成功。このときの経路は Terminal→(MTool→(jnc0→SA)→ITBL フロントサーバ)→ITBL 中継サーバ→jaerif。
・AEGIS コミュニティのアクセス。Safari で原子力科学研究所から見えるアドレスを使って認証ゲートウェイにアクセス。その後ファイルサーバのファイルリストが見えることを確認。

(3) 検証項目 3

1. NAREGI-CA ソフトウェアによる証明書発行
・証明書署名要求を RA サーバへ移動
・NAREGI-CA ソフトウェアから証明書を発行
・RA オペレータが、シェル上で NAREGI-CA ソフトウェアのコマンドを実行して証明書署名要求に対して証明書を発行

2. 証明書の IC カードへの書き込み
NAREGI-CA ソフトウェアにより発行した証明書を原子力機構身分証に追加書き込みを実施（詳細、省略）

【クライアント端末が WindowsXP SP2 の場合】
3. テストに使用するクライアントの設定
・IBM ThinkPad X40、WindowsXP Pro SP2
・IC カードリーダライタ：SCR3310-NTTCom、インストール済み
・機構身分証用認証ライブラリ eSK ツール、インストール済み

4. クライアント認証付き Web サーバにアクセス
・検証用サーバ（https:///flanker.edo.jaea.go.jp/aegistest/show.cgi）へアクセス
・カードリーダに、証明書を格納した原子力機構従業員カードをセットし、PIN コード入力。正常に認証され、該当ページが表示されることを確認。

5. SSL-VPN 装置へログイン
・SSL-VPN サーバ（JAEA 情報システム管理室のテスト用 SSL-VPN 装置）へアクセス
・非接触カードリーダによるアクセス認証→OK
・接触カードリーダによるアクセス認証→OK
・表示される炉ログオン画面にてユーザ名を入力しログオン
・ユーザ名：teshima.naoya
・正常にログオンでき、TOP 画面が表示されることを確認。

【クライアント端末が MacOSX 10.4 の場合】
6. テストに使用するクライアントの設定
・Mac iBook G4、MacOS10.4.10
・IC カードリーダライタ：SCR3310-NTTCom、インストール済み
・機構身分証用認証ライブラリ eSK ツール、インストール済み

7. クライアント認証付き Web サーバにアクセス
・Firefox にて、検証用サーバ（https:///flanker.edo.jaea.go.jp/aegistest/show.cgi）へアクセス
・カードリーダに、証明書を格納した原子力機構従業員カードをセットし、PIN コード入力。正常に認証され、該当ページが表示されることを確認。

注）ブラウザとして Safari を使用した場合、MacOSX の IC カード中から証明書を自動で選択し提示されてしまい、正常に認証することができなかった

(4) 検証項目 4

1. 書き込みに使用するサーバ・クライアントの設定
サーバ：JAEA 内のテスト用証明書書き込みサーバを使用
・検証用証明書の発行準備

・書き込み用サービスプロバイダーとして、「Sony Felica Cryptgraphic Provider」を使用するよう設定

クライアント：

・WindowsXP SP2
(FeliCa カード付属ソフトウェアが MacOS に対応していないため MacOS では実施しない)
・以下の FeliCa カード付属ソフトウェアをセットアップ
・Sony FeliCa リーダー／ライター
・Sony FeliCa PKI Option

2. 証明書の書き込み

2.1 テスト用証明書書き込みサーバへアクセス

・以下テスト用証明書書き込みサーバ（https://flanker.edo.jaea.go.jp/aegismgr）へアクセス
・ユーザ名：teshima.naoya
・パスワード：*****
・表示される内容を確認し、書き込みキーを入力し、書き込みボタンをクリック
・氏名：手島 直哉
・職員番号：*****
・書き込みキー：*****

2.2 書き込みの実行

・券面の一致確認にチェックを入れる
・書き込み対象の Dual カードタイプ FeliCa を非接触カードリーダにセットし、実行ボタンをクリック
・以下、警告プロンプトが表示される。[はい]をクリック
・「この Web サイトはユーザーの代わりに新しい証明書を要求しています。ユーザーの代わりに証明書を要求できるのは、信頼された Web サイトだけに制限する必要があります。証明書を要求しますか？」
・表示されるプロンプトに、PIN コードを入力
・PIN コード：****
・以下、警告プロンプトが表示される。「はい」をクリック
・「この Web サイトは 1 つ以上の証明書をこのコンピュータに追加しています。信頼していない Web サイトがユーザーの証明書を更新できるようにすると、セキュリティ上、危険です。信頼されていない証明書が Web サイトによりインストールされ、さらに信頼されていないプログラムがこのコンピュータ上で実行され、ユーザーのデータにアクセスする可能性があります。
このプログラムで証明書を追加しますか？この Web サイトを信頼している場合は、[はい]をクリックします。信頼していない場合は、[いいえ]をクリックします。」
・書き込み完了

3. クライアント認証付き Web サーバにアクセス

・検証用サーバ（https:///flanker.edo.jaea.go.jp/aegistest/show.cgi）へアクセス
・非接触カードリーダに、証明書格納した Felica カードをセットし、PIN コード入力。正常に認証され、該当ページが表示されることを確認。
・接触カードリーダに、証明書格納した FeliCa カードをセットし、PIN コード入力。正常に認証され、該当ページが表示されることを確認。

4. SSL-VPN 装置へログイン

・SSL-VPN サーバ（JAEA 情報システム管理室のテスト用 SSL-VPN 装置）へアクセス
　・非接触カードリーダによるアクセス認証→OK
　・接触カードリーダによるアクセス認証→OK
・表示されるログオン画面にてユーザ名を入力しログオン
　・ユーザ名：teshima.naoya
・正常にログオンでき、TOP 画面が表示されることを確認。

付　録２ 用語集

用語	正式名称	意味
PKI	Public Key Infrastructure	利用者の身元について信頼できる第三者（Certificate Authority：CA）が審査を行い、保証を実現する仕組みのこと。
EAP	Extensible Authentication Protocol	PPP（Point to Point Protocol）を拡張し、認証方式を備えたプロトコル。RFC 2284 として標準化されている。
RADIUS	Remote Authentication Dial-In User Service	利用者の認証とアカウンティングをネットワーク上のサーバコンピュータに一元化することを目的とした IP 上のプロトコル。元来はダイヤルアップ・インターネット接続サービスを実現することを目的として開発されたが、しかし現在は、インターネット接続サービス、無線 LAN、VLAN など様々な場面で幅広く利用されている。RFC 2138 として標準化されている。
AES	Advanced Encryption Standard	米国商務省標準技術局(NIST)によって DES に変わる暗号化標準として公募により集められた方式の中から選ばれた米国政府の次世代標準暗号化方式。
TLS	Transport Layer Security	情報を暗号化して送受信するプロトコルの一つ。TLS は公開鍵暗号や秘密鍵暗号、デジタル証明書、ハッシュ関数などのセキュリティ技術を組み合わせ、データの盗聴や改ざん、なりすましを防ぐことができる。現最新バージョンである、TLS 1.1 が RFC4346 として標準化されており、本バージョンから暗号化アルゴリズムとして AES をサポートしている。
WPA2	Wi-Fi Protected Access 2	無線 LAN の業界団体 Wi-Fi Alliance が 2004 年 9 月に発表した、無線 LAN の暗号化方式の規格。2002 年に発表された WPA の新バージョンで、より強力な AES に対応している。
SSL-VPN	－	暗号化にセッションレイヤーである SSL を利用する VPN 技術。多くの Web ブラウザやメールソフトは標準で SSL に対応しているため、追加アプリケーションのインストールなく、容易に導入可能である。
NAREGI-CA ソフトウェア	－	「最先端・高性能汎用スーパーコンピュータの開発利用プロジェクト：NAREGI プログラム」で開発したオープンソースの認証局ソフトウェア。
Dual カードタイプ FeliCa	－	FeliCa（フェリカ）は、ソニーが開発した非接触型 IC カードの技術方式であるが、接触型と非接触型の両方の機能を有するのが Dual カードタイプ FeliCa である。通常 FeliCa は公開鍵暗号方式の処理を行う規格はないが、Dual カード

		タイプ FeliCa は非接触型通信によりそれを可能としている。

国際単位系（SI）

表１．SI 基本単位

基本量	SI 基本単位	
	名称	記号
長さ	メートル	m
質量	キログラム	kg
時間	秒	s
電流	アンペア	A
熱力学温度	ケルビン	K
物質量	モル	mol
光度	カンデラ	cd

表２．基本単位を用いて表されるSI組立単位の例

組立量	SI 基本単位	
	名称	記号
面積	平方メートル	m^2
体積	立法メートル	m^3
速さ，速度	メートル毎秒	m/s
加速度	メートル毎秒毎秒	m/s^2
波数	毎メートル	m^{-1}
密度，質量密度	キログラム毎立方メートル	kg/m^3
面積密度	キログラム毎平方メートル	kg/m^2
比体積	立方メートル毎キログラム	m^3/kg
電流密度	アンペア毎平方メートル	A/m^2
磁界の強さ	アンペア毎メートル	A/m
量濃度[a]，濃度	モル毎立方メートル	mol/m^3
質量濃度	キログラム毎立法メートル	kg/m^3
輝度	カンデラ毎平方メートル	cd/m^2
屈折率[b]	（数字の） 1	1
比透磁率[b]	（数字の） 1	1

(a) 量濃度（amount concentration）は臨床化学の分野では物質濃度（substance concentration）ともよばれる。
(b) これらは無次元量あるいは次元１をもつ量であるが、そのことを表す単位記号である数字の１は通常は表記しない。

表３．固有の名称と記号で表されるSI組立単位

組立量	SI 組立単位			
	名称	記号	他のSI単位による表し方	SI基本単位による表し方
平面角	ラジアン[b]	rad	1 [b]	m/m
立体角	ステラジアン[b]	sr[c]	1 [b]	m^2/m^2
周波数	ヘルツ[d]	Hz		s^{-1}
力	ニュートン	N		$m\ kg\ s^{-2}$
圧力，応力	パスカル	Pa	N/m^2	$m^{-1}\ kg\ s^{-2}$
エネルギー，仕事，熱量	ジュール	J	N m	$m^2\ kg\ s^{-2}$
仕事率，工率，放射束	ワット	W	J/s	$m^2\ kg\ s^{-3}$
電荷，電気量	クーロン	C		s A
電位差（電圧），起電力	ボルト	V	W/A	$m^2\ kg\ s^{-3}\ A^{-1}$
静電容量	ファラド	F	C/V	$m^{-2}\ kg^{-1}\ s^4\ A^2$
電気抵抗	オーム	Ω	V/A	$m^2\ kg\ s^{-3}\ A^{-2}$
コンダクタンス	ジーメンス	S	A/V	$m^{-2}\ kg^{-1}\ s^3\ A^2$
磁束	ウエーバ	Wb	Vs	$m^2\ kg\ s^{-2}\ A^{-1}$
磁束密度	テスラ	T	Wb/m^2	$kg\ s^{-2}\ A^{-1}$
インダクタンス	ヘンリー	H	Wb/A	$m^2\ kg\ s^{-2}\ A^{-2}$
セルシウス温度	セルシウス度[e]	℃		K
光束	ルーメン	lm	cd sr[c]	cd
照度	ルクス	lx	lm/m^2	$m^{-2}\ cd$
放射性核種の放射能[f]	ベクレル[d]	Bq		s^{-1}
吸収線量, 比エネルギー分与, カーマ	グレイ	Gy	J/kg	$m^2\ s^{-2}$
線量当量, 周辺線量当量, 方向性線量当量, 個人線量当量	シーベルト[g]	Sv	J/kg	$m^2\ s^{-2}$
酸素活性	カタール	kat		$s^{-1}\ mol$

(a)SI接頭語は固有の名称と記号を持つ組立単位と組み合わせても使用できる。しかし接頭語を付した単位はもはやコヒーレントではない。
(b)ラジアンとステラジアンは数字の１に対する単位の特別な名称で、量についての情報をつたえるために使われる。実際には、使用する時には記号rad及びsrが用いられるが、習慣として組立単位としての記号である数字の１は明示されない。
(c)測光学ではステラジアンという名称と記号srを単位の表し方の中に、そのまま維持している。
(d)ヘルツは周期現象についてのみ、ベクレルは放射性核種の統計的過程についてのみ使用される。
(e)セルシウス度はケルビンの特別な名称で、セルシウス温度を表すために使用される。セルシウス度とケルビンの単位の大きさは同一である。したがって、温度差や温度間隔を表す数値はどちらの単位で表しても同じである。
(f)放射性核種の放射能（activity referred to a radionuclide）は、しばしば誤った用語で"radioactivity"と記される。
(g)単位シーベルト（PV,2002,70,205）についてはCIPM勧告2（CI-2002）を参照。

表４．単位の中に固有の名称と記号を含むSI組立単位の例

組立量	SI 組立単位		
	名称	記号	SI 基本単位による表し方
粘度	パスカル秒	Pa s	$m^{-1}\ kg\ s^{-1}$
力のモーメント	ニュートンメートル	N m	$m^2\ kg\ s^{-2}$
表面張力	ニュートン毎メートル	N/m	$kg\ s^{-2}$
角速度	ラジアン毎秒	rad/s	$m\ m^{-1}\ s^{-1}=s^{-1}$
角加速度	ラジアン毎秒毎秒	rad/s^2	$m\ m^{-1}\ s^{-2}=s^{-2}$
熱流密度，放射照度	ワット毎平方メートル	W/m^2	$kg\ s^{-3}$
熱容量，エントロピー	ジュール毎ケルビン	J/K	$m^2\ kg\ s^{-2}\ K^{-1}$
比熱容量，比エントロピー	ジュール毎キログラム毎ケルビン	J/(kg K)	$m^2\ s^{-2}\ K^{-1}$
比エネルギー	ジュール毎キログラム	J/kg	$m^2\ s^{-2}$
熱伝導率	ワット毎メートル毎ケルビン	W/(m K)	$m\ kg\ s^{-3}\ K^{-1}$
体積エネルギー	ジュール毎立方メートル	J/m^3	$m^{-1}\ kg\ s^{-2}$
電界の強さ	ボルト毎メートル	V/m	$m\ kg\ s^{-3}\ A^{-1}$
電荷密度	クーロン毎立方メートル	C/m^3	$m^{-3}\ sA$
表面電荷	クーロン毎平方メートル	C/m^2	$m^{-2}\ sA$
電束密度，電気変位	クーロン毎平方メートル	C/m^2	$m^{-2}\ sA$
誘電率	ファラド毎メートル	F/m	$m^{-3}\ kg^{-1}\ s^4\ A^2$
透磁率	ヘンリー毎メートル	H/m	$m\ kg\ s^{-2}\ A^{-2}$
モルエネルギー	ジュール毎モル	J/mol	$m^2\ kg\ s^{-2}\ mol^{-1}$
モルエントロピー, モル熱容量	ジュール毎モル毎ケルビン	J/(mol K)	$m^2\ kg\ s^{-2}\ K^{-1}\ mol^{-1}$
照射線量（X 線及びγ線）	クーロン毎キログラム	C/kg	$kg^{-1}\ sA$
吸収線量率	グレイ毎秒	Gy/s	$m^2\ s^{-3}$
放射強度	ワット毎ステラジアン	W/sr	$m^4\ m^{-2}\ kg\ s^{-3}=m^2\ kg\ s^{-3}$
放射輝度	ワット毎平方メートル毎ステラジアン	$W/(m^2\ sr)$	$m^2\ m^{-2}\ kg\ s^{-3}=kg\ s^{-3}$
酵素活性濃度	カタール毎立方メートル	kat/m^3	$m^{-3}\ s^{-1}\ mol$

表５．SI 接頭語

乗数	接頭語	記号	乗数	接頭語	記号
10^{24}	ヨタ	Y	10^{-1}	デシ	d
10^{21}	ゼタ	Z	10^{-2}	センチ	c
10^{18}	エクサ	E	10^{-3}	ミリ	m
10^{15}	ペタ	P	10^{-6}	マイクロ	μ
10^{12}	テラ	T	10^{-9}	ナノ	n
10^{9}	ギガ	G	10^{-12}	ピコ	p
10^{6}	メガ	M	10^{-15}	フェムト	f
10^{3}	キロ	k	10^{-18}	アト	a
10^{2}	ヘクト	h	10^{-21}	ゼプト	z
10^{1}	デカ	da	10^{-24}	ヨクト	y

表６．SIに属さないが、SIと併用される単位

名称	記号	SI 単位による値
分	min	1 min=60s
時	h	1h =60 min=3600 s
日	d	1 d=24 h=86 400 s
度	°	1°=(π/180) rad
分	’	1’=(1/60)°=(π/10800) rad
秒	”	1”=(1/60)’=(π/648000) rad
ヘクタール	ha	$1ha=1hm^2=10^4m^2$
リットル	L，l	$1L=11=1dm^3=10^3cm^3=10^{-3}m^3$
トン	t	$1t=10^3$ kg

表７．SIに属さないが、SIと併用される単位で、SI単位で表される数値が実験的に得られるもの

名称	記号	SI 単位で表される数値
電子ボルト	eV	$1eV=1.602\ 176\ 53(14)\times10^{-19}J$
ダルトン	Da	$1Da=1.660\ 538\ 86(28)\times10^{-27}kg$
統一原子質量単位	u	1u=1 Da
天文単位	ua	$1ua=1.495\ 978\ 706\ 91(6)\times10^{11}m$

表８．SIに属さないが、SIと併用されるその他の単位

名称	記号	SI 単位で表される数値
バール	bar	$1\ bar=0.1MPa=100kPa=10^5Pa$
水銀柱ミリメートル	mmHg	1mmHg=133.322Pa
オングストローム	Å	$1\ Å=0.1nm=100pm=10^{-10}m$
海里	M	1 M=1852m
バーン	b	$1\ b=100fm^2=(10^{-12}cm)2=10^{-28}m^2$
ノット	kn	1 kn=(1852/3600)m/s
ネーパ	Np	SI単位との数値的な関係は、対数量の定義に依存。
ベル	B	
デジベル	dB	

表９．固有の名称をもつCGS組立単位

名称	記号	SI 単位で表される数値
エルグ	erg	$1\ erg=10^{-7}\ J$
ダイン	dyn	$1\ dyn=10^{-5}N$
ポアズ	P	$1\ P=1\ dyn\ s\ cm^{-2}=0.1Pa\ s$
ストークス	St	$1\ St=1cm^2\ s^{-1}=10^{-4}m^2\ s^{-1}$
スチルブ	sb	$1\ sb=1cd\ cm^{-2}=10^4cd\ m^{-2}$
フォト	ph	$1\ ph=1cd\ sr\ cm^{-2}\ 10^4lx$
ガル	Gal	$1\ Gal=1cm\ s^{-2}=10^{-2}ms^{-2}$
マクスウェル	Mx	$1\ Mx = 1G\ cm^2=10^{-8}Wb$
ガウス	G	$1\ G=1Mx\ cm^{-2}=10^{-4}T$
エルステッド[c]	Oe	$1\ Oe \triangleq (10^3/4\pi)A\ m^{-1}$

(c) ３元系のCGS単位系とSIでは直接比較できないため、等号「≙」は対応関係を示すものである。

表10．SIに属さないその他の単位の例

名称	記号	SI 単位で表される数値
キュリー	Ci	$1\ Ci=3.7\times10^{10}Bq$
レントゲン	R	$1\ R = 2.58\times10^{-4}C/kg$
ラド	rad	$1\ rad=1cGy=10^{-2}Gy$
レム	rem	$1\ rem=1\ cSv=10^{-2}Sv$
ガンマ	γ	1γ=1 nT=10-9T
フェルミ		1フェルミ=1 fm=10-15m
メートル系カラット		1メートル系カラット = 200 mg = 2×10-4kg
トル	Torr	1 Torr = (101 325/760) Pa
標準大気圧	atm	1 atm = 101 325 Pa
カロリー	cal	1cal=4.1858J（「15℃」カロリー），4.1868J（「IT」カロリー）4.184J（「熱化学」カロリー）
ミクロン	μ	1 μ =1μm=10^{-6}m

（第8版，2006年改訂）

この印刷物は再生紙を使用しています