# 電子証明書を用いたインターネット成績通知証明システムの設計と実装

村上陽子[†]　小川浩司[‡]　大川恵子[†]　村井 純[†‡]

電子証明書を用いて、インターネットにおける信頼性・守秘性を確保した成績通知証明システムを構築した。システムは授業担当者、履修者、大学の 3 者を主体とし、登録・通知・証明機能から構成される。成績の信頼性及び守秘性を確保するため、認証、成績管理情報の共有、成績証明の発行には電子証明書を用い、さらに成績情報の保存にも暗号化技術を用いた。本稿では、このインターネット成績通知証明システムの設計及び実装について述べる。

本システムは、インターネットを基盤とした大学環境の実現を目指す School of Internet ("SOI") システム上で行われた実証実験に基づいて評価を行った。SOI システムが実際の大学の授業を利用したシステムであることから、本システムがインターネットを基盤とする学習環境のみならず、大学をはじめとする既存の学習環境における成績通知証明システムとしても有効であることが証明された。また、本システムはインターネットにおける信頼可能な情報流通を実現するシステムの 1 例としての意味も持つ。

# Design and Implementation of Internet Transcript System with Digital Certificate

YOKO MURAKAMI[†], KOJI OGAWA[‡], KEIKO OKAWA[†], JUN MURAI[†‡]

We established a system to issue transcript in learning environment on the Internet. This system consists of three functions of registration; notification and issue of transcript, and faculty, students and administrator carry out these functions. We achieved reliability and secrecy by using digital certificate for authentication, communication and issue of transcript. We also use cryptograph to keep grade data safe. In this paper, design and implementation of this system is described.

We evaluate this system through the result of experimentation on "School of Internet" (“SOI”) system, which aims to establish an environment for higher education on the Internet. As SOI system is based on the courses performed on existing universities, it is proved that this system is also applicable to them.

## 1. はじめに

ディジタルテクノロジによって実現された広域分散環境においては、学習のみならず、その学習成果を利用する場も広域に分散する。すなわち、インターネットを利用することにより、従来のように場所や時間の制約を受けることなく、身につけたスキルや知識を活かすことが可能になるのである。

そのため、学習評価のフィードバックのみならず、学習の成果を証明する方法も従来の紙メディアではなく、ディジタルコミュニケーションに適した形式でなされなければ学習者や利用者の要求に応えることはできない。

しかし、学習成果を表す成績情報は信頼性が要求されるものであり、同時に個人のプライバシに関する情報でもある。この特性ゆえに、インターネットにおける成績情報の流通には困難が多い[1]。

このため、現在のインターネットを基盤とする学習環境には、学習者が学習の評価を得て、その成果を第三者に証明するためのしくみは確立されていない。このことが、学習者のインセンティブを低める要因となっていることは否定できない。

† 慶應義塾大学大学院政策・メディア研究科
Graduate School of Media and Governance, Keio University
‡ 慶應義塾大学環境情報学部
Department of Environmental Information, Keio University

そこで本研究では、インターネットにおける成績通知証明システムを構築し、電子証明書を中心とした暗号技術を用いて信頼性の確保とプライバシの保護に考慮しつつ[2]、容易に授業担当者が成績を登録でき、学習者が自分の評価を確認、証明できるようにした。本システムは、インターネットを基盤とする学習環境のみならず、大学をはじめとする既存の学習環境における成績証明システムとしても利用可能である。

以下、インターネットを基盤とした大学環境の実現を目指す School of Internet システム[3]上で実験運用を行った成績通知証明システムの設計及び実装、その評価について述べる。

## 2. 設計

本章では、成績通知証明システムの目的及び要求事項を明確にし、システムの設計について述べる。

### 2.1. 登場人物

まず、本システムに登場する人物とその役割について記述する。登場人物としては、(1)ファカルティ、(2)TA/SA、(3)授業履修者、(4)大学(大学管理者)、(5)第三者が挙げられる。

ファカルティは、授業履修者に対して成績をつけ、その成績を大学に提出する役割を持つ。TA/SA と呼ばれる授業アシスタントは、ファカルティのこれらの作業を補助し、必要な場合にはファカルティの代わりに成績を大学に提出する。授業履修者は成績の通知を受け、また、第三者からの要求に応じて、自分の成績を証明するよう大学に要求する。大学はこの成績証明書を発行する役割を担う。

それぞれの登場人物の関係を図 1 に示す。

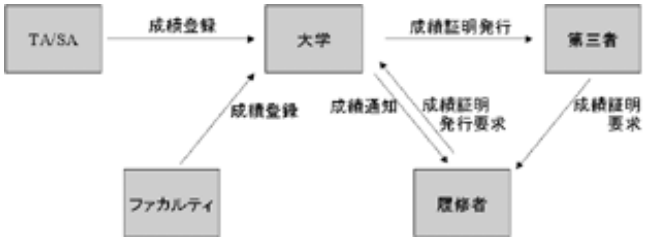


図 1　登場人物間の関係

### 2.2. 目的

本システムでは、次の 3 つを目的とする。

1. ファカルティ及び TA/SA が授業の履修者に対して容易に成績を登録できる
2. 履修者が自分の成績を確認できる
3. 履修者が自分の成績を第三者に証明できる

### 2.3. 要求事項

成績情報の信頼性確保及びプライバシ保護に考慮しつつ、上記目的を達成するために必要な要求事項は以下の 5 つと定義する。

1. ファカルティ及び TA/SA のみが成績登録でき、なりすましを防止できる
2. 成績が改竄・捏造されない
3. 管理者、ファカルティ、履修者、履修者が指定する第三者以外には成績が見られない
4. 管理者のみが成績証明を発行でき、発行された証明の有効性が確認できる
5. 成績の登録・通知・証明が容易にできる

### 2.4. システムの構成要素

本システムは、(1)登録機能、(2)通知機能、(3)証明発行機能の 3 つの機能に別れる。登録機能は、ファカルティや TA/SA に電子証明書を用いて成績登録を行わせる。通知機能は登録された成績を履修者に通知する。証明発行機能は、履修者が指定する第三者に対して成績証明を発行する。これらの機能は 1 または 2 個のサーバから構成される。

登録機能で用いられる電子証明書は、大学が信用する機関の発行するものであることが必要だが、ファカルティや TA/SA がそれらを持たない場合には、大学が電子証明書を発行する。この証明書発行機能を登録機能の補助機能として定義する。

各サーバの機能及び役割については表 1 で記述し、その全体のシステム構成図を図 2 に示す。

また、使用される鍵とその使用者、使用方法の一覧を表 2 に示す。

表 1 各機能を構成するサーバ

| | |
|---|---|
| 登録機能 | 成績登録サーバ |
| 通知機能 | 成績通知サーバ<br>成績表示サーバ |
| 証明発行機能 | 成績証明発行サーバ |
| 証明書発行機能<br>（補助機能） | ファカルティ登録サーバ<br>証明書発行サーバ |

### 2.4.1 登録機能

登録機能は成績登録サーバから構成される。

**成績登録サーバ**

履修者の成績を登録する。成績登録サーバは、電子証明書を用いてファカルティ及び TA/SA の認証を行う。

新規登録の場合、ファカルティが成績データと管理用暗号鍵を入力すると、成績登録サーバはこの暗号鍵を用いて成績データを暗号化し、保有する。同時に、この暗号鍵を TA/SA 及び大学に暗号化してメールで送る。これは、暗号鍵を成績登録サーバに残さないことにより、成績登録サーバへの不正侵入による成績の改竄や捏造を防止するためである。

成績の追加登録・修正の場合、ファカルティが管理用暗号鍵を入力すると、成績登録サーバがこの暗号鍵を用いて成績データを復号化し、ファカルティに提示する。ファカルティが追加・修正した成績データを送り返してくると、成績登録サーバは再び同じ暗号鍵でデータを暗号化して保有する。

成績データの登録が完了し、ファカルティが通知要求を送ると、成績登録サーバは暗号化された成績データを成績通知サーバに送る。

登録や通知の重複を避けるため、一度通知要求が成されると、成績登録サーバはそれ以降の修正や通知要求を一切拒否する。

### 2.4.2 成績通知機能

成績通知機能は成績通知サーバと成績表示サーバから構成される。

**成績通知サーバ**

個人成績データの作成及び各履修者に対する履修者用暗号鍵の通知を行なう。成績通知サーバは、電子証明書によるアクセスコントロールを行い、大学管理者にのみアクセスを許可する。

大学管理者が管理用暗号鍵を入力すると、成績通知サーバは成績登録サーバから受け取った成績データを復号化し、履修者ごとの個人成績データを作成する。次に、履修者ごとの暗号鍵を生成し、この履修者用暗号鍵を用いて個人成績データを暗号化する。成績通知サーバは、この暗号化された個人成績データを成績データベースに送り、生成した履修者用暗号鍵を各履修者に送付する。この時、履修者用暗号鍵はメールで送付され、成績通知サーバに残されることはない。これは、登録の場合と同様、成績通知サーバへの不正侵入による成績の改竄や捏造を防止するためである。

**成績表示サーバ**

履修者に成績を表示する。

履修者があらかじめ登録してある Email アドレスと認証鍵、成績通知サーバから送られてきた履修者用暗号鍵を入力すると、成績表示サーバは、登録されている履修者情報に基づいて認証を行う。認証が正しく行われれば、成績データベースから個人成績データを受け取り、履修者用暗号鍵を用いてこれを復号化し、履修者に表示する。

### 2.4.3 成績証明発行機能

成績証明発行機能は、成績証明発行サーバから構成される。

**成績証明発行サーバ**

履修者が指定する第三者に対して成績証明の発行を行う。

履修者があらかじめ登録してある Email アドレスと認証鍵、成績通知サーバから送られてきた履修者用暗号鍵と第三者の証明書情報を入力すると、成績表示サーバは、登録されている履修者情報に基づいて認証を行なう。認証が正しく行なわれれば、成績データベースから個人成績データを受け取り、履修者用暗号鍵を用いてこれを復号化する。そしてこの個人成績データを、第三者の証明書を用いて暗号化し、大学の署名をしてメールで第三者に送付する。

### 2.5. 証明書発行機能（補助機能）

証明書発行機能はファカルティ登録サーバと証明書発行サーバから構成される。

**ファカルティ登録サーバ**

ファカルティを授業担当者として登録する。

ファカルティが氏名と Email アドレス、認証鍵を入力してくると、ファカルティ登録サーバは大学管理者にその登録内容をメールで通知する。大学管理者はオフラインで登録内容の確認し、その正当性を確認するとファカルティ登録サーバにそのファカルティに対する登録要求を送る。ファカルティ登録サーバは、証明書取得用認証鍵を生成し、この証明書取得用認証鍵と登録された Email アドレス、ファカルティ認証鍵を証明書発行サーバに渡す。また、生成した証明書取得用認証鍵をファカルティにメールで送付する。同様の方法で TA/SA も登録する。

ここで用いられるファカルティ認証鍵はファカルティの本人認証のためのものであり、証明書取得用認証鍵は成績登録段階で重要となる Email アドレスの到達性を確保するためのものである。

**証明書発行サーバ**

ファカルティに電子証明書を発行する。

ファカルティが登録した Email アドレス、ファカルティ認証鍵、証明書取得用認証鍵を入力してくると、ファカルティ登録サーバから受け取った情報に基づいて認証を行い、認証が正しく行われた場合に電子証明書を発行する。同様の方法で TA/SA にも電子証明書を発行する。

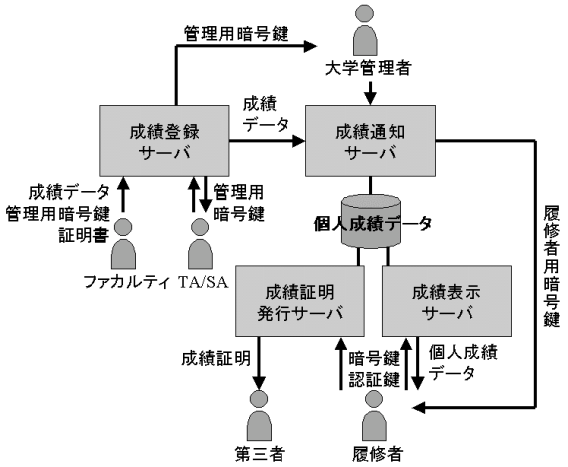


図 2 システム構成

### 2.6. 処理の流れ

本システムにおける処理の流れを、以下に記述する。

1. ファカルティが、成績データと管理用暗号鍵を登録する
2. 大学管理者と TA/SA が、暗号化されたメールで管理用暗号鍵を受け取る
3. 必要な場合は、ファカルティまたは TA/SA が、管理用暗号鍵を用いて成績データを修正して登録しなおす
4. ファカルティまたは TA/SA が、成績通知要求を送る
5. 大学管理者が、管理用暗号鍵を用いて履修者への通知を行なう
6. 履修者が、履修者用暗号鍵を受け取る
7. 履修者が、履修者用暗号鍵を用いて成績を表示させる
8. 履修者が、履修者用暗号鍵と第三者の証明書を用いて、署名・暗号化されたメールで成績証明を第三者に送らせる
9. 第三者が、履修者の成績証明を受け取る

**補助機能**

1. ファカルティが、氏名、Email アドレス、認証鍵を登録する
2. 大学管理者が、ファカルティの氏名と Email アドレスをメールで受け取る
3. 大学管理者が、ファカルティにオフラインで登録内容を確認する
4. 大学管理者が、ファカルティの登録を要求する
5. ファカルティが、証明書取得用認証鍵をメールで受け取る
6. ファカルティが、証明書の発行を要求す
7. ファカルティが、証明書を受け取る

表 2 使用される鍵一覧

| 鍵 | 使用者 | 使用方法 |
|---|---|---|
| 管理者暗号鍵 | ファカルティ、TA/SA、大学管理者 | 成績データの暗号化・復号化 |
| 履修者用暗号鍵 | 履修者 | 個人成績データの暗号化・復号化 |
| 履修者認証鍵 | 履修者 | 成績表示における |
| ファカルティ認証鍵 | ファカルティ、TA/SA | 証明書取得における認証 |
| 証明書取得用認証鍵 | ファカルティ、TA/SA | 証明書取得における認証 |

## 3. 実装

本章では、2 章の設計に基づいて行った実装について述べる。

本実装では、安全な通信路を確保するために、暗号通信プロトコル SSL(Secure Socket Layer)[4]を用い、ユーザインターフェースとして SSL 対応 Web ブラウザ (Netscape Navigator または Internet Explore)、サーバとして SSL 対応サーバ(Apache1.3.6 + SSLeay0.9.3)を採用した。各サーバには、証明書発行サーバから発行されたサーバ証明書を使用した。

以下、各サーバの実装について記述する。本システムの全てのサーバは、SunOS5.6 オペレーティングシステム上で実装した。

### 3.1. 成績登録サーバ

成績登録サーバは、OpenSSL[5]と Perl を用いた CGI スクリプトを用いて実装した。

成績登録サーバは、各ファカルティの証明書情報を保持し、接続時にクライアント証明書を要求する方法でアクセスコントロールを行う。

ファカルティは WWW クライアントで成績登録フォームを呼び出し、成績データと管理用暗号鍵を記入して成績登録サーバに送信する。成績登録サーバは、成績データから成績ファイルを作成し、管理用暗号鍵を用いて暗号化して保有する。暗号化には DES(Data Encryption Standard)[6]を用いる。

修正時には同じ暗号鍵で成績ファイルを復号化して、データをクライアントに送信する。

登録終了後、クライアントから通知要求を受けると、暗号化された成績ファイルを成績通知サーバに渡す。

### 3.2. 成績通知サーバ

成績通知サーバは、OpenSSL と Perl を用いた CGI スクリプトを用いて実装した。

この成績通知サーバは、大学管理者の証明書情報を保持し、接続時にクライアント証明書を要求する方法でアクセスコントロールを行う。

大学管理者は WWW クライアントで通知フォームにを要求し、管理用暗号鍵を記入して送信する。成績通知サーバは、送られた暗号鍵で成績ファイルを復号化し、履修者毎の個人成績ファイルを作成する。また、成績通知サーバは履修者毎に履修者用暗号鍵を生成し、この履修者用暗号鍵で各個人成績ファイルを暗号化する。暗号化された個人成績ファイルは成績データベースに渡され、履修者用暗号鍵は各履修者宛にメールで送付される。

### 3.3. 成績表示サーバ

成績表示サーバは、OpenSSL と Perl を用いた CGI スクリプトによって実装した。

この成績表示サーバは、履修者によってあらかじめ登録された Email アドレスと認証鍵から成る履修者情報を保持する。この履修者認証鍵は、DES に基づくハッシュ関数で暗号化されている。

履修者は WWW クライアントで通知要求フォームを呼び出し、登録した Email アドレスと履修者認証鍵、履修者用暗号鍵を記入して送信する。成績表示サーバは、この入力された Email アドレスと認証鍵が登録されているものと一致した場合に、成績データベースから個人成績ファイルを受け取り、履修者用暗号鍵を用いて復号化し、クライアントに表示する。

### 3.4. 成績証明発行サーバ

成績証明発行サーバは、OpenSSL と Perl を用いた CGI スクリプトを用いて実装した。

この成績証明発行サーバは、成績通知サーバと同様の履修者情報を保持する。

履修者は WWW クライアントで成績証明発行フォームを呼び出し、Email アドレスと認証鍵、履修者用暗号鍵と X.509 証明書[7]を記入して送信する。成績証明発行サーバは、この入力された Email アドレスと認証鍵が登録されているものと一致した場合に、履修者用暗号鍵で個人成績ファイルを復号化してデータを取り出し、この個人成績データと X.509 証明書を署名･暗号化メール作成モジュールに渡す。

### 3.5. 署名・暗号化メール作成モジュール

署名・暗号化メール作成モジュールは、C 言語を用いた実装である。

このモジュールには、あらかじめ大学管理者の証明書及びその秘密鍵を組み込んでおく。

署名・暗号化メール作成モジュールは、X.509 証明書と個人成績データを受け取り、この個人成績データをもとに、モジュールに組み込まれている秘密鍵と受け取った証明書に含まれる公開鍵を用いて、署名・暗号化された MIME メッセージ[8]を作成する。このメッセージを Internet Message(IM-100)[9]を用いて、証明書に記載されている Email アドレス宛にメールで送信する。

### 3.6. ファカルティ登録サーバ

ファカルティ登録サーバは、Perl を用いた CGI スクリプトとして実装した。

ファカルティは WWW クライアントを用いて申請フォームを呼び出し、氏名と Email アドレス、ファカルティ認証鍵を記入してファカルティ登録サーバに送信する。ファカルティ登録サーバは、この認証鍵を DES に基づくハッシュ関数で暗号化して Email アドレスとともに保有し、氏名と Email アドレスを大学管理者にメールで送信する。

大学管理者は WWW クライアントで登録フォームを呼び出し、ファカルティとして登録するファカルティの Email アドレスを記入してファカルティ登録サーバに送信する。ファカルティ登録サーバは証明書取得用認証鍵を生成し、この証明書取得用認証鍵と Email アドレス、ファカルティ認証鍵を証明書発行サーバに渡す。また、生成された証明書取得用認証鍵はメールでファカルティ宛に送付される。

### 3.7. 証明書発行サーバ

証明書発行サーバは、SSLeay0.9.0[10]と CA パッケージ ICAP2.44 [11]を用いて実装した。

ファカルティは WWW クライアントで申請フォームを呼び出し、氏名、Email アドレス、ファカルティ認証鍵、証明書取得用認証鍵を記入し、クライアントで作成した公開鍵とともに証明書発行サーバに返す。証明書発行サーバは、入力された Email アドレスとファカルティ認証鍵、証明書取得用認証鍵が証明書発行サーバから受け取ったものと一致した場合に、大学の証明書の秘密鍵で署名された X.509 証明書をクライアントに送信する。

証明書に記載する内容は表 3 に示されるとおりである。

表 3 証明書の主な記載内容例

| | |
|---|---|
| Issuer | C=JP,<br>O=School of Internet,<br>OU=School of Internet CA |
| Validity | NotBefore:Aug29 05:00:47 1999<br>NotAfter: Aug 28 05:00:47 2000 |
| Subject | C=JP,<br>O=School of Internet,<br>OU=Faculty,<br>Email=yoko@sfc.wide.ad.jp,<br>CN=Yoko Murakami |
| NetscapeCertType | SSLClient,S/MIME |

## 4. 評価

本システムが 2.3 の要求事項を満たすものであるかを検証するために、School of Internet で開講された授業に本システムを適用し、実験運用を行った。また、授業の履修者 149 人を対象に、アンケート調査を実施した。以下、その結果に基づいて本システムの評価を行う。

実験は 1999 年度秋学期に SOI で開講されたコミュニケーションネットワーク論において実施し、アンケートの回答率は 57%であった。この講義は慶應

義塾大学湘南藤沢キャンパスで実際に行われた講義を利用したものである。

### 4.1. アンケート結果

**質問 1：インターネットを用いて成績通知がなされることについて**

・今後もやってほしい　65 人
・どちらでもよい　17 人
・やめてほしい　2 人

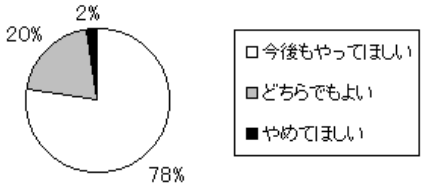


図 3 インターネットによる成績通知

**質問 2：成績通知において最も重要だと思うもの**

・迅速な通知　17 人
・プライバシ　24 人
・正確さ　43 人

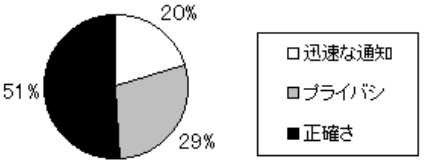


図 4 成績通知における重要要素

**質問 3：成績通知方法について**

・web の方がよい　12 人
・メールの方がよい　49 人
・どちらでもよい　23 人

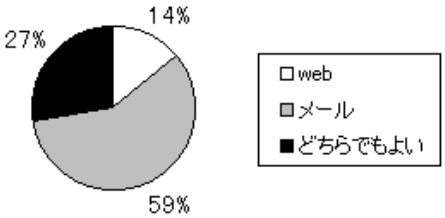


図 5 成績通知方法

### 4.2. 認証

X.509 証明書を用いた SSL クライアント認証を行うことにより、成績の登録や修正を行うファカルティ及び TA/SA の認証を実現した。電子証明書の取得段階での本人認証は、暗号化された通信路をもちいて本人のみが知り得る認証鍵を登録させ、登録をオフラインで確認することによって実現した。また、証明書を発行する段階でも、通信路を暗号化することによってその後の成りすましの防止を実現した。

履修者の認証に関しては、あらかじめ登録しておいた Email アドレスと認証鍵を用いて行ったが、ファカルティ同様、証明書を用いて認証の精度を高めることが課題として残る。

### 4.3. 改竄・捏造の防止

登録された成績データを暗号化し、その暗号鍵を証明書を用いて暗号化したメールで共有するという方法を採ることにより、サーバにおける成績データの改竄や捏造の防止を実現した。

しかし、履修者用暗号鍵を通知するメールが暗号化されていないことから、改竄・捏造防止の精度を上げるためにも履修者による証明書の利用が課題として残る。

### 4.4. 盗み見の防止

成績の登録・修正・通知のいずれの段階でも SSL を用いて通信路を暗号化することにより、盗み見の防止を実現した。また、成績証明の送信段階でも、履修者が指定する第三者の証明書を用いて暗号化したメールで送信することによって盗み見を防止した。

### 4.5. 成績証明の信頼性

成績証明を行うサーバを大学管理者のみが管理する安全なホスト上に置き、さらに成績証明発行用の秘密鍵を署名・暗号化メール作成モジュールに組み込み、バイナリ形式で用いることにより、秘密鍵の安全性及び信頼性を高めた。また、CA が発行する CRL を確認することにより、発行された証明の有効性を確認することができるようにし、成績証明の信頼性を確保した。

### 4.6. 簡便性

成績の登録や確認作業を簡単にするため、WWWによるユーザインターフェースを提供した。

しかし、証明書発行も含めると、ファカルティやTA/SAについては使用する鍵が3種類もあることから、その削減が課題として残る。また、アンケート結果が示すように、成績通知インターフェースとしては、WWWよりもメールの方が簡便であると考える履修者が多いことから、今後、証明書を用いて暗号化したメールで通知する方法も検討する必要がある。

## 5. まとめと今後の課題

本システムは、インターネット上における成績通知及び成績証明の発行を実現した。電子証明書等の暗号技術を用いることにより、信頼性および守秘性を確保し、インターネット上でも簡単かつ安全に、信頼できる成績証明を発行することを可能にした。本システムが、インターネット上で学ぶ学習者の学習インセンティブを高めるとともに、全ての学習者がグローバルにその成果を利用できる環境を実現すると予想される。

今後の課題としては、履修者の認証及び暗号鍵の通知に電子証明書を導入することが挙げられる。そのためには、多様な学習環境に対応できる証明書発行方法およびその管理方法を確立することが必要である。

また、LDAPサーバ[12]等を用いて成績証明発行先の証明書を自動検索する方法についても検討が必要である。

## 6. 謝辞

本研究を進めるにあたり、実験にご協力くださったSOIの諸先生方ならびに学生の皆様､授業TA/SAの方々に感謝いたします。また、暗号技術に関するアドバイスをくださったWIDEプロジェクトmoCAワーキンググループの皆様に感謝します。最後に、常に研究を支えてくれた慶應義塾大学School on the Internet研究グループの諸氏に感謝の念を表します。

## 7. 参考文献

[1] Tom Creed, "Extending the Classroom Walls Electronically", New Paradigms for College Teaching, Interaction Book Co., 1997

[2] チャーリ・カフマン，ラディア・パールマン，マイク・スペシナー（石橋啓一郎，菊池浩明，松井彩，土井祐介訳）「ネットワークセキュリティ」，プレティスホール出版，1997年

[3] 大川恵子，伊集院百合，村井純，「School of Internet－インターネット上での『インターネット学科』の構築－」，情報処理学会，1998年

[4] Hickman, Kipp, "The SSL Protocol", Netscape Communications Corp., 1995

[5] OpenSSL, http://www.openssl.org/

[6] ANSI X3.106, "American National Standard for Information Systems-Data Link Encryption," American National Standards Institute, 1 983.

[7] R. Housley, W. Ford, W. Polk, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC2459, s1999

[8] P. Hoffman, B. Ramsdell, L. Lundblade, L. Repka, "S/MIME Version 2 Message Specification" RFC2311, 1998

[9] Internet Message(IM-100), http://www.mew.org/

[10] SSLeay, http://www.psy.uq.oz.au/~ftp/Crypto/

[11] 服部裕之, 櫻井三子, 小林良至, 菊池浩明, 「オンライン証明書発行用パッケージ(ICAP)の実装と評価」，SCIS97，1997年

[12] OpenLDAP, http://www.openldap.org/