4. これまでの研究成果

4.1 附属図書館研究開発室における研究の概要

附属図書館研究開発室では、超高速インターネット構成技術からメタデータ応用、セキュリティ技術、大規模サーバ構成技術、RF-ID の利用技術などの応用技術まで、電子図書館構成技術としてインターネット基盤技術を含む情報サービス構築技術に関する研究開発を行っている。今年度は、これらの中から特に、超高速ネットワークサービスを支えるシステム技術、ユビキタス環境におけるネットワーク資源提供モデル、書籍における RF-ID の利用に関して報告する。超高速ネットワークサービスを支えるシステム技術では、大規模な電子図書館システムを支える超高速ネットワークを実現する際に必要となるオペレーティングシステム技術について報告している。ユビキタス環境におけるネットワーク資源提供モデルでは、必要な権限を持つ利用者がどこからでも電子図書館のリソースにアクセスできるようにするため基礎技術について述べている。書籍における RF-ID の利用では、RF-ID 技術を用い実世界とインターネット上の仮想世界を結びつける研究を基礎に、電子図書館に収められているデータと実際の書籍との対応付けに関する試みについて述べている。

4.2 超高速ネットワークサービスを支えるシステム技術

インターネットの超高速化にともない、ネットワークサービスのボトルネックが、従来の低速で高価なネットワークからサーバに移行してきている。こうした状況に対応するための技術として、サーバのクラスタ化などの分散技術が数多くこれまでに開発されているが、ネットワークの性能向上の速度はプロセッサの性能向上の速度を大きく上回っており、このままではシステムは大規模化する一方である。次世代電子図書館では、学内だけではなく、超高速ネットワークを利用して学外へ知的情報資源の発信が求められており、システムの大規模化だけではなく、個々のサーバの性能を向上させることも重要な課題である。

本研究では，個々のサーバ自体の性能を向上させることを目的として、オペレーティングシステム技術に着目して今後の超高速ネットワーク時代を支えるシステム技術の開発を行った。具体的には、多数のソケットに関するイベントを一括管理する多重化 I/O が、サーバにおいてボトルネックになることに着目し、その機能的なフレームワークを変更することなく、性能のスケーラビリティを改善する技術を開発した。また、実時間スケジューリングを応用することにより、システム負荷に応じたプロセッサ利用率の実現も達成した。これらの手法は、従来のオペレーティングシステムへの変更も不要であり、適応が非常に容易であるという利点も持つ。

4.2.1 研究のねらい

インターネットにおける従来の情報配信サービスでは、ボトルネックは低速で高価なネットワークにあるとされ、そのような状況を改善するために配信の最適化技術が数多く開発されてきた。その代表として挙げられるのがキャッシュ技術であり、現在広く普及しつつある CDN (Contents Delivery Network)サービスもその一例である。

しかしながら，ネットワーク技術の発展は当初の予想を遥かに越えて進んでおり、バックボーンネットワークにおける性能（スループット）は6ヶ月毎に2倍向上して いるという報告があるほどである。そのため、これまでのネットワークサービスインフラストラクチャの構造に多くの歪みが発生してきている。例えば、先に挙げたCDNなどは、当初の目的であった分散化によるネットワーク負荷の軽減という意義が薄れる一方で、一時的なリクエスト集中によるシステムダウンの回避や、経路切断など故障からのサービスの保護、さらにはDoS攻撃などからのサービスの防御など、目的の多様化が進みつつある。

本研究では、そうした「歪み」が最も顕著に現れる場所としてエンドノードすなわちサーバに着目し、超高速ネットワークサービスを支えるシステム技術に焦点を当てて研究を行った。

4.2.2 研究方法と成果

多重化I/Oの実行間隔制御

高速ネットワークサーバでは、数千から数万ものソケットを同時に扱うことができなければならない。特に現在代表的なネットワークサービスの一つであるWebにおいては、HTTP/1.1永続コネクションが導入されたため、サーバにおける同時ソケット数が増加する傾向にある。

Unix上のサーバプログラムなどで、このような同時ソケットにおけるI/O処理を多重化するのによく用いられるselect()やpoll()（多重化I/O）には、サーバ負荷の増加に対する性能のスケーラビリティに欠けるという問題がある。この問題の原因は、select()やpoll()におけるソケットテーブルの走査の処理コストが大きいことにあると広く認識されており、それゆえこれまでに提案されてきた解決手法は、こうしたソケットテーブルの走査を廃止し、特別なイベント通知機構を設けるものが多い。しかし、これらの手法は、オペレーティングシステムの改造が必要であったり、プログラミングモデルの変更を要したりするため、導入コストが高いという別の問題がある。多重化I/Oにおいて真に問題なのは、ソケットテーブルの走査そのものではなく、多重化I/Oがそのイベント駆動的な処理構造により必要以上に頻繁に呼び出されてしまうことにある。

そこで本研究では、多重化I/Oの呼び出し間隔を制御し、サーバの性能を向上させる手法を提案した（図 1 b）。本手法により、高頻度の多重化

I/O 呼び出しによって引き起こされていた CPU 処理能力の枯渇が防止され、サーバの処理能力が向上する（図 2）。また、本手法は従来の select()や poll()を用いたプログラミングモデルを踏襲するため、適用コストが非常に小さいという特長も併せ持つ。

実時間スケジューリングによる実行間隔制御における確定的なプロセッサ利用の実現

本研究で開発した多重化 I/O における実行間隔制御機構において、同時ソケット数が非常に大きい場合、サービス遅延時間の低減などの効果は確認できるものの、いくつかの特異な現象が二点見られた。

一つは、サービス遅延時間の増加傾向である。実行間隔制御を行う場合、一定間隔でソケットのチェックが行われるため、リクエストレートの増加に対してサービス遅延時間はほぼ一定で推移すると考えるのが妥当である。しかし、実験では同時ソケット数が大きい場合は、提案方式を組み込まない場合と比較して大幅にサービス遅延時間の低減を実現しているものの、サービス遅延時間に増加の傾向が観測された（図 2 b）。

もう一つは、プロセッサの利用率がほぼ 100%となってしまう点である（図 3 a）。 実行間隔制御では、リクエストレートに応じてスレッドをブロックするため、プロセッサの利用率はリクエストレートの増加に対して線形に増加すると考えるのが妥当である。

これらの点を考察した結果、制御を行う間隔がオペレーティングシステムのスケジューリングにおけるタイムスライスを越えてしまい、予期しないコンテキストスイッチ等が含まれてしまうことが判明した。そこで本研究では、実時間スケジューリングを用いることでこれらの コンテキストスイッチを防止する手法を提案した（図 1 c）。本方式により、ソケット数が非常に多い場合でも、サービス遅延における スケーラビリティが向上した。また、プロセッサ利用率もリクエストレートに対して線形に推移するようになった（図 3 b）。後者の利点は、特に近年プロセッサの消費電力が増加しているため、データセンターなどにおける大規模 PC サーバクラスタ等で大きな利点になると考える。

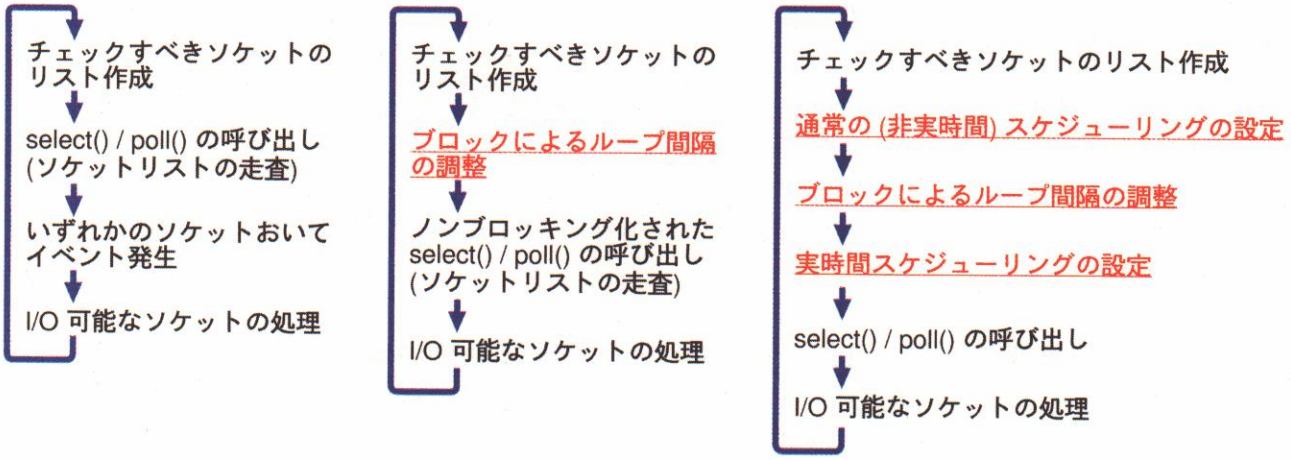
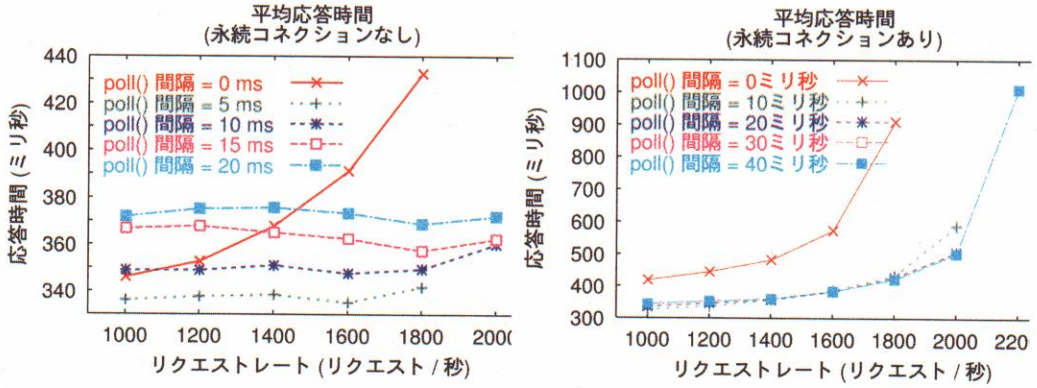
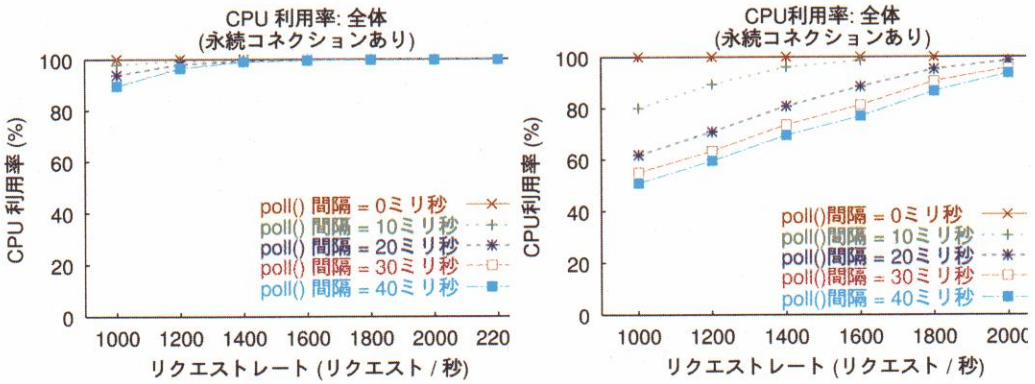


図 1: 多重化 I/O における実行間隔制御



(a) 永続コネクション無効時　　(b) 永続コネクション有効時

図 2: Web アクセラレータに実装した場合の性能 (poll() 間隔が 0 ms の場合は実行間隔制御を全く行わないことを意味する)



(a) 永続コネクション無効時　　(b) 永続コネクション有効時

図 3: Web アクセラレータに実装した場合のプロセッサ利用率
(poll()間隔が 0 ms の場合は実行間隔制御を全く行わないことを意味する)

その他の研究

本研究は、超高速ネットワークサービスを実現するシステム技術の開発を主に行ったが、その他にもいくつかネットワークサービスに関連する開発も行った。本節ではそれらについて簡単に紹介程度にまとめる。

ネットワーク経由のデバイス制御手法の研究

ネットワーク環境の遍在化により、ユビキタスコンピューティング技術に代表されるような、いつでもどこでも計算機を利用可能にする技術が着目を集めている。本研究では、特に USB で接続されるデバイスに着目し、ネットワーク経由で制御するための基本的なフレームワークを開発した。現在のインターネットは高速化してきているが、デバイスを遠隔から制御するのに十分な品質等が確保されているとは言えない。そこで、デバイス制御に関するネットワークにおける要求分析を行い、最適な通信方式およびそれらの自動的な選択方式に関する研究を行った。

ネットワークにおける新しい情報発信・共有モデルの研究

現在、ネットワークを用いた情報システムが広く利用されているが、それらの中で、特にコミュニケーションを主眼として開発されたシステムを用いて情報等の蓄積等が行われている。

例えば、メーリングリストや Web 掲示板等がそうしたシステムにあたるが、これまでのシステムは情報発信者に強いコミュニティ的意識を強いるものがほとんどであった。そのため、多くの場合で、ごく一部の者だけが情報発信し、その他の大勢は情報を受信するだけという状況が形成される。

本研究では、より個人的な視点に立った、情報発信・共有モデルを提案し、システム開発を行った。そこでは、基本的には個人的なメモ蓄積アプリケーションという形をとり、完全に個人の制御下で共有知識として流通させることで、情報発信者の心理的負荷の軽減を実現している。

Webサーバクラスタを用いたリアルタイム情報発信技術の研究

インターネットが情報流通インフラとしての地位を獲得していくにつれ、スポーツのスコア情報や金融情報など、リアルタイム性の高い情報を大規模に配信する必要性が高まっている。本研究では、大規模サーバクラスタにおけるこうした秒単位で更新されていく情報を同期して配信するシステムを開発した。具体的には、更新情報を管理するマスターサーバと、実際にクライアントへ情報を配信するスレーブサーバの間で、更新・確認・公開という三つのフェーズをもつプロトコルを開発した。 本システムは、実際に商用サービスにおいて実証実験を行い、良好な結果を得ている。

Webサービスの IPv6 移行技術の研究

IPv6は日本が主導して普及に取り組んでいる技術の一つであるが、IPv4からの移行の際のコストや、移行後のサービスの欠如などの問題がある。特に、サービス品質、費用対効果、セキュリティなどに非常に敏感である商用サービスなどでは、こうした問題が重要視され、なかなか移行が進んでいないのも事実である。

本研究では、商用Webサービスに焦点を当て、そのIPv6移行に必要な要件を分析し、リバースプロキシサーバを用いた低コストなIPv6サービスフレームワークを提案した。本システムで主に開発したのは、IPv6－IPv4中継機能、高い処理能力を達成するメモリキャッシュ、IPv6に未対応なサービスを一元的に管理するサービスフィルタである。また、本システムは、既存のIPv4ネットワークセキュリティのフレームワークへの組み込みも容易であるという特長も持つ。また、本システムも実際の商用サービスにおいて実証実験を行っている。

P2P 型情報配信技術の研究

今後のネットワークの高速化を考えると、サーバシステムのクラスタ化による負荷分散方式から、P2Pに代表されるような、ユーザが利用する計算機を含めたサービスフレームワークが必要になると考えられる。 本研究では、P2P 型の情報配信網を用いた Web キャッシュシステムを提案した。

従来より、Webキャッシュシステムはキャッシュヒット率でその性能が議論されていた。そのため、Webキャッシュの目標としては、多くアクセスされる、すなわちより高頻度でキャッシュヒットするコンテンツをいか

に効率よく保持しておくかが焦点となっていた。しかしながら、近年のネットワークの高速化により、キャッシュがエンドユーザにおけるサービス遅延の解消にほとんど貢献していないばかりか、逆にキャッシュが性能のボトルネックになってしまう現象まで観測されるようになっている。そこで本研究では、発想の転換を行い、ダウンロードに非常に長い時間を要するコンテンツのみをP2P接続された分散型キャッシュクラスタからダウンロードする機構を開発した。本システムは、従来のシステムではヒットしにくかったサイズの大きなコンテンツや、アクセス頻度の低いコンテンツなどへのアクセスを改善した。

4.2.3 今後の展開

本研究で開発した技術は、主にWebサービスをターゲットとして、可能な限りサーバソフトウエアがオペレーティングシステムと連携することで高速化を実現している。一方で、これらの成果を活用し、さらなるサービスの高速化を実現するためには、システムソフトウエアおよびハードウエアによる支援が必要となる。これらの分野は、開発コストが高く、実用化が難しいと考えられるが、以下に掲げる二つの方向性で研究を発展させる予定である。

高速イベント処理機構の再構築

これまで、高速ネットワークにおけるI/Oならびにイベント処理の効率化を実現するために、その原因の究明と解決法の提案、技術開発を行ってきた。今後はこうした要素技術を体系化し、高速ネットワークサーバプラットホームとしてのオペレーティングシステムの機構的再構築を 行っていきたいと考えている。特にTCP/IPの高速ネットワークへの適応化に関する研究や、ソケットインタフェースなどのプログラミング的な側面など、総合的な検討を行う。

サーバプラットホームにおけるネットワークプロセッサの応用

近年、ネットワーク処理専用のハードウエアとして、ネットワークプロセッサ（NP）技術が注目を集めている。今後、個々のサーバの性能を大幅に向上させるには、オペレーティングシステムにおける構造的な改善だけではなく、このNPを用いた高速ネットワークサービスの実現が必須であると考えている。そこで、本研究で得られた知見をこうしたNPを用いたサーバ技術に応用し成果展開していくことを考えている。

4.3 ユビキタス環境におけるネットワーク資源提供モデル

近年の計算機の小型化・軽量化により、携帯可能な計算機が普及してきている。また、IEE802.11規格をはじめとする無線LAN技術の進歩により、利用者が計算機を持ち歩き、インターネット上の情報やサービスを利用する『モバイルコンピューティング』環境、あるいは『ユービキタスコンピューティング』環境の構築と整備がおこなわれてきた。いまや、インターネットはオフィスや家庭で利用するものから、街角に遍在するものへと変化を遂げており、どこにいても利用者が自分の所有する計算機端末を利用して、インターネット上のサービスを享受することができる。

本学の電子図書館も、インターネットの仕組みを利用しており、このようなモバイルコンピューティングを支援する環境を構築している。本学図書館に来館した利用者がインターネットへ接続する場合、以下のどちらかの形態をとる。

- あらかじめ用意された検索クライアントを利用する
- 利用者が持ち込んだ計算機端末を利用する

これにより、計算機を携帯する利用者にとっては、使いなれた環境で本学電子図書館やインターネット上のサービスを利用することができる。

上記の環境を利用するにあたっては認証を必要としない。すなわち、利用者が自分の計算機を情報コンセントに接続すれば、そのままインターネットに接続できる。これは利用者にとっては利便性という点で利点があるが、管理者の側面からは以下の問題がある。

- 利用者に応じたサービスの提供ができない
- 利用者が問題を起こした場合に特定が困難である

前者は、本学に所属するもののみが利用できる資源や、学外からの利用者にも利用できる資源などのポリシーを定義し、利用者の身分に応じてポリシーを反映した資源アクセス制御をおこなうものである。後者は、不特定多数の利用者からある利用者を特定するためのものである。社会基盤にまで広がったインターネットでは、個人情報の漏洩や誹謗中傷、さらには詐欺まで、さまざまな犯罪が蔓延するようになった。また、コンピュータウィルスなど、ある計算機が他のシステムに危害を加える事件も頻発している。本学図書館のネットワークを利用して犯罪行為がおこなわれたり、コンピュータウィルスに感染した計算機が持ち込まれたりした場合には、その計算機を特定する必要がある。

そこで、本章ではあらかじめデータベースに登録されていない利用者に対し、ネットワーク資源を提供するためのサービスモデルの提案に関して述べ

る。このモデルは、利用者がある証明期間によって発行された個人証明書を携帯し、ネットワークを利用する場面でその証明書を提示することで、利用可能なサービスを記述した属性証明書を発行するものである。これにより、利用者に応じて提供するサービスを制御することが可能になるとともに、必要があればサービスの利用者を特定することも容易になると考えられる。

4.3.1 既存技術と問題点

ユビキタス環境におけるネットワーク資源の提供のために、現在までに、B-mobile やAirH''の様に、携帯電話網のローミングを利用したモバイル端末用のインターネット接続サービスや、インターネットカフェや駅構内などに設置した無線LANからインターネットへの接続性を提供するホットスポット、公共性の高い場所に情報端末を置く情報コンセントシステム等のサービスが提供されている。しかし、これらのサービスには、それぞれ制限が設けられているため、周辺のネットワーク資源を有効に活用することが困難であるだけでなく、サービスの利便性を損なう可能性もある。

既存サービスの制限と問題点

前述した携帯電話網のローミングを利用し、特定のアクセスポイントへ接続することによるモバイル端末用インターネット接続サービスは主に「ネットワーク資源」を、ホットスポットや情報コンセントシステムは主に「場所（点）」を限定した上でサービスを提供している。つまり、携帯電話網を用いたローミング接続サービスは、場所に依存することなく利用可能であるが狭帯域高遅延であり、電波範囲などの影響でサービスが限定される場合が多い。 また、ホットスポット等のサービスは、その場所では快適に提供されるが、そのドメインの運用ポリシに強く依存するため、移動した先々で同一サービスを連続して利用することができない。また、提供された計算機やネットワークの安全性に関しても 問題が残ると云える。つまり、前者では「線」のサービス、後者では「点」のサービスを提供しているが、異なるサービスドメインが有機的に集合しているユビキタス環境を「面」として考える場合、利用者が異なるサービスドメイン間を移動すると、サービス提供に関して、以下のような制限や問題が独立または複合的に生じる。

- 電波強度による通信の不安定状態または切断
- 接続および認証のやりなおしが必要
- 移動先にある計算機周辺機器などの資源が利用不可能
- 事前のアカウント登録とポリシ管理が必要
- 公共端末を用いる場合の、個人情報が残る可能性

これにより、サービス利用者は地下や電波強度の弱い場所ではインターネットへの接続性が断たれる、移動先の運用ポリシに沿って管理されているプ

リンタが利用できない、移動するごとに認証やアクセス制御処理が繰り返される、ゲストアカウント取得などの事前処理がなければ資源を利用できない、などの不便を強いられることになる。

これは、課金やサービスの協調・連携の枠組みが異なるドメイン間で確立されていないことが原因と考えられる。つまり、従来のインターネットは利用者や計算機が移動することを前提として設計・運用されていないため、移動してきた利用者に対して、サービスドメイン内部のポリシを反映した利用者認証および資源へのアクセス制御や権限委譲などの 対応が困難であることに起因する。

また、物理的な位置情報や時刻、ネットワークの状態など、利用状態や状況などの情報が動的に変化する場合にも、各サービスドメインのセキュリティポリシや運用ポリシに沿った柔軟なサービスの提供を行うためには、インターネット上の分散システムの構築と運用に関して、従来の手法に囚われない新しいネットワークアーキテクチャモデルが必要となる。

つまり、場所や時間に依存することなくインターネットへの接続性やローカルな計算機周辺機器などの資源のサービスを利用する場合、利用者は複数の通信メディアを用いることが可能であり、かつ、その利用者に対して、移動先の組織での運用ポリシが的確に反映された資源へのアクセス制限および権限委譲が行われる仕組みが必要となると云える。

4.3.2 ネットワーク資源提供モデルの提案

ユビキタス環境におけるサービスの連続性を考える上では、「自分がたしかに自分であることを移動先で証明」した上で、「証明された人物に、移動先(内部)の運用ポリシが反映された形で動的にネットワーク資源を提供する」というサービスモデルが必要となる。ここで、ネットワーク資源とは、インターネットへの接続性を提供するための情報や各サービスドメイン内で管理されているサービス機器などを指す。普段利用していない場所に移動した場合でもインターネットへの接続性が提供される場合は、IMAP [4,5]やVNC(Virtual Network Computing) [7]、VPN(Virtual Private Network) [6]、PPPoE(Point-to-Point Protocol over Ethernet) [8]などの 技術を用いることで、日常利用している環境へのアクセスやある程度の再現が可能となると考える。

本章では、前述の問題を解決するためのユビキタス環境におけるネットワーク資源提供モデルについて提案する。

ネットワーク資源提供モデル

従来のインターネット接続性の提供は、事前のアカウント登録とそれに対応するアクセス制御に依存している。しかし、ユビキタス環境では、利用者が移動するため、その移動先のサービスドメインに対する事前のアカウント

登録・削除などの処理が困難である。また、動的に変化する利用者の特性や実空間の情報を反映させることができないため、運用ポリシに即した形での柔軟サービス提供や対応を行うことが困難である。

これは、利用者のホーム環境（外部）で定義された識別子や権利などを示す属性情報を、移動先のサービスドメイン内部（内部)ポリシに 動的に対応づけることができないことに起因する。

そこで、本研究では、ユビキタス環境におけるネットワーク資源提供モデルとして、公開鍵暗号基盤で利用されている 個人証明書や一時属性証明書を用いた認証とアカウント管理およびアクセス制御技術に着目した（図 4）。

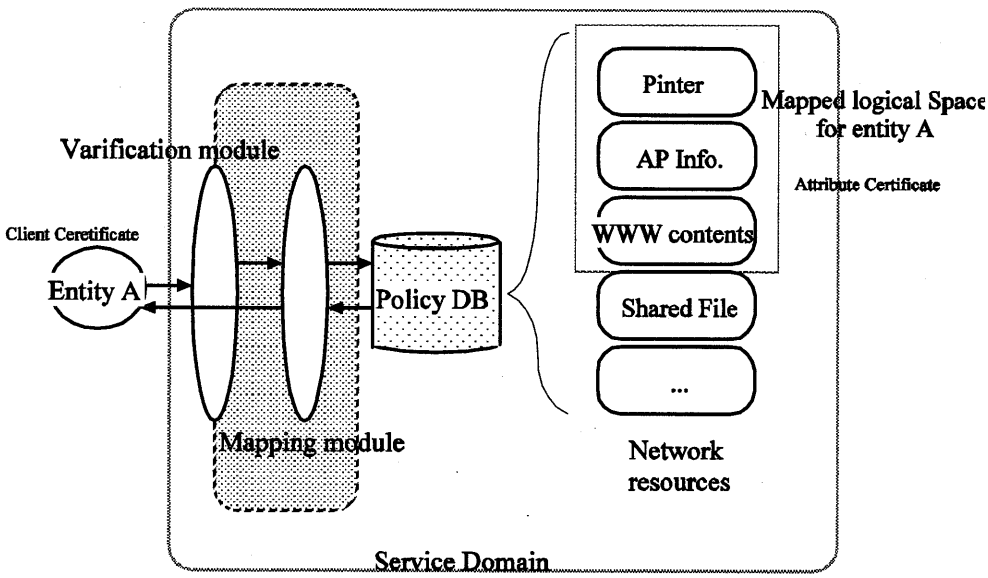


図 4: ネットワーク資源提供モデル

利用者（エンティティ）の識別および証明を行う個人証明書を用いた認証技術と、内部でのアクセス制御や権限委譲を表現できる属性証明書を用い、個人証明書の検証結果と内部で定義されているポリシとを対応づける機能（Mapping module）を導入することで、エンティティと資源の利用権限との対応づけを行う。これにより、シームレスにサービスを利用するユビキタス環境において、移動先のサービス提供組織内の運用ポリシを反映させた段階的かつ動的なサービスを利用者に提供する仕組みを提案する。

提案モデルの構成要素と機能

提案するネットワーク資源提供モデルに関して、抽象化した構成要素とその特性を図 4 に示した。ここでは、それぞれの機能について概説する。

- エンティティ
- サービス利用者に該当

- 移動することが前提
- 個人を識別する情報を持ち歩く
- ネットワーク資源
- 接続性を提供するための情報
- プリンタや共有ファイルなどの内部（各サービスドメイン内）で管理されているサービス機器
- 外部定義と内部ポリシとのマッピング機構
- ネットワーク資源とエンティティのインタフェイス
- 個人証明書検証とポリシ対応づけの二つのデーモンにより構成
- 外部定義による利用者の識別情報を一元的に管理
- 内部で適応するアクセス制御または権限委譲構造に対応づける
- 内部での利用者の検証は可能

このモデルでは、ネットワーク資源として、サービスを構成するコンポーネント（情報、サーバ、メモリやディスクスペースなど）が分離されており、かつ、それぞれに利用のための権限が記されていると考える。その分離したネットワーク資源に対する権限と外部で定義（証明）された情報を持つ利用者の権限との対応づけを、動的に定義する。

個人証明書と内部ポリシとのマッピング機構

エンティティは個人識別情報を持ち歩く。移動した先で認証サービスを検索し、応答した認証サービスに向けて個人識別情報を提示する。つまり、エンティティは個人情報を格納するソフトウェア的またはハードウェア的なセキュリティデバイスを保持している。ここでは、公開鍵暗号基盤の個人証明書を念頭に議論するが、個人を識別・証明できる情報であれば、バイオメトリックスや他の情報でも対応可能とする。公開鍵暗号基盤の個人証明書には、個人を識別する情報の他に、それを証明する機関の名前（所属）や肩書き、有効期限などの情報が記載されている。したがって、個人を識別するだけでなく、その発行元を検証することで、「特定の大学関係者」「大学のスタッフ」「匿名」などといった識別とその証明が可能である。

一時属性証明書の配布

ネットワーク資源に対するアクセス制御や権限委譲を属性証明書として利用者に一時的に発行する。

エンティティの個人証明書の検証後、外部定義と内部ポリシとのマッピング機構によってエンティティが内部の一時的な論理空間に対応づけられ、この論理空間を記述した一時的な属性証明書などが付与される。この論理空間では、内部で定義されたポリシ適用の構造を基にした、利用可能なネットワーク資源や権限委譲の集合を扱う。これにより、外部で定義されたエンティティが、内部での特定のネットワーク資源を利用するのためのアクセス制御

または権限委譲を一時的に許可された空間に 対応づけられ、権利を証明された証明書を用いて活動を行う。内部でに許可される空間は時限つきであるため、有効期限を短く設定することで、CRL (Certificate Revocation List:証明書失効リスト) に関する仕組みを省略する。

個人証明書の携帯

個人を識別・証明する情報は、現実社会では、パスポート、免許証、クレジットカード、社員証、メンバーズカードなどの様に、利用者一人に対して複数存在する。したがって、利用者は複数の個人証明書を保持し、サービス要求を行う場合には適宜選択した上で提示する。

複数の個人識別情報の使い分けが想定する場合、「自己に関わる情報について一定のコントロールをおよぼす権利（自己情報制御権）」 [9]に関する検討が必要になる。

これらの仕組みにより、エンティティは自分の保持する個人識別情報を選択的に提示するだけで、事前登録や申請をすることなく移動先でも適切なサービスを利用することが可能である。また、外部定義と内部ポリシとの対応づけを行うことにより、外部で定義されたエンティティに対して内部のポリシに沿った形でネットワーク資源を提供する構造が可能となる。

4.3.3 プロトタイプシステムの設計例

提案モデルを基に、ユビキタス環境におけるネットワーク資源提供のためのプロトタイプシステムの設計の例を示す。

ここでは、openssl-0.9.7b のライブラリを用いて個人証明書および一時属性証明書の発行および検証を行い、PostgreSQL などのリレーショナルデータベースを用いて内部ポリシを管理する。

図 5は、個人証明書提示から属性証明書発行までの処理の流れ、および識別子・ネットワーク資源の割り当て処理を示している。

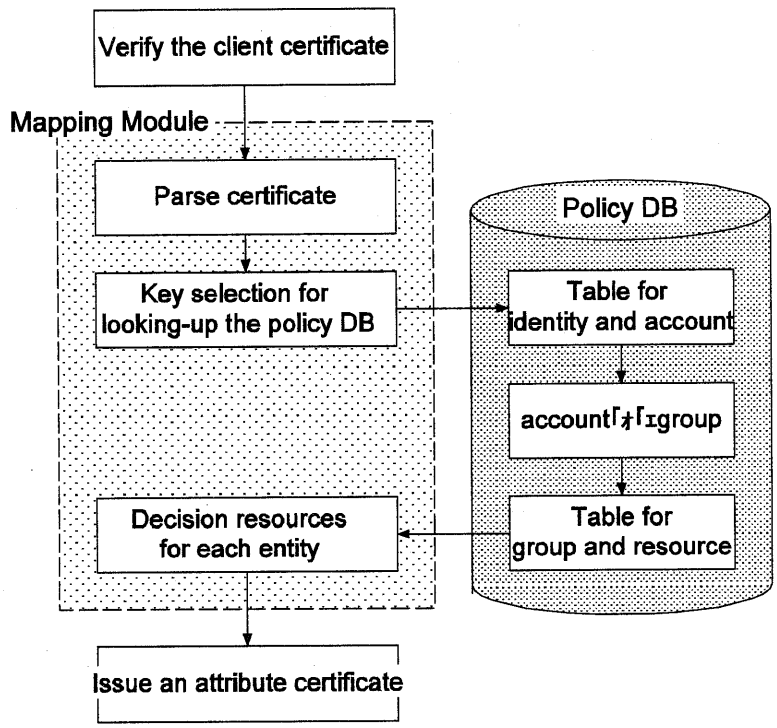


図 5: 識別子と資源の割り当て処理

個人証明書と内部ポリシとのマッピング機構は、サービスドメイン内で有効な識別子（HomeUser アカウントや Guest など）を検出するフェーズと、サービスドメイン内で利用可能な資源を決定するフェーズに分けられる。

リレーショナルデータベースの利用

マッピング機構では、個人証明書の検証結果と内部ポリシデータベースとの折衝を行う。内部ポリシデータベースは、あるエンティティに対して対応づけられる複数のネットワーク資源や権限を表現するために、以下の三つのテーブルにより構成される.

- 各サービスドメイン内で有効な識別子（account）毎のレコードとして, 証明書記述内容を属性にもつテーブル
- サービスドメイン内のネットワーク資源の利用権限を体系づける識別子（group）毎のレコードとして、ネットワーク資源を属性にもつテーブル
- （1）、（2）の関係を表すテーブル

図 6 にエンティティとネットワーク資源を含めた処理の流れを示す。

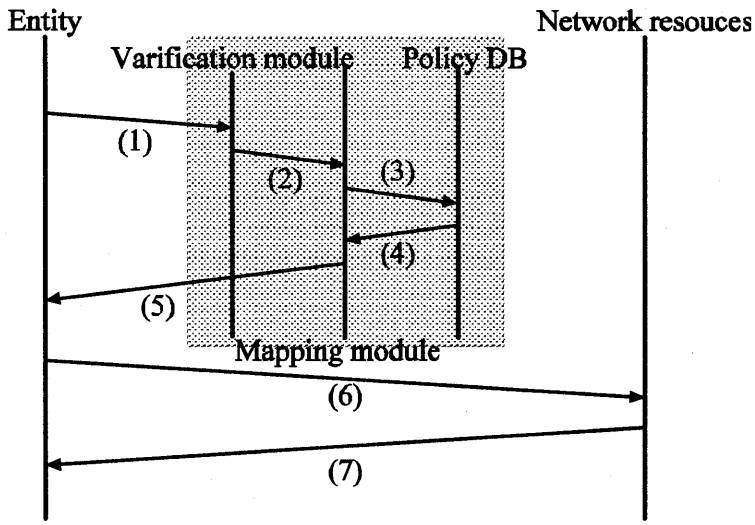


図 6: プロトタイプシステムの処理の流れ

エンティティがあるサービスドメイン内に移動し、ネットワーク資源の利用を要求してから、実際にネットワーク資源を利用可能となるまでの処理は以下の 6 段階に分けられる。

- SLP (Service Location Protocol) 等のサービス発見機構を用いて証明書を検証するサーバを発見し、自己を証明するための個人証明書を提示する。
- 提示された証明書を検証し、その結果をマッピング機構に転送する。
- エンティティの検証結果と内部ポリシを記述したポリシデータベースとの折衝を行う。
- エンティティに割り当て可能な論理空間を検出する。
- 割り当てられた論理空間を、一時属性証明書としてエンティティに発行する。
- 一時属性証明書を用いてネットワーク資源を利用する。

証明書検証サーバとエンティティの間の通信は、SSL(Secure Socket Layer)/TSL(Transport Layer Security) などを用いて保護される必要がある。

特定のサービスドメイン内で限定されたネットワーク資源へのアクセス管理や権限委譲を行うため、プロトタイプシステムでは、そのサービスドメインで独自に作成したプライベート CA(Certificate Authority)や プライベート RA(Registration Authority)を作成し、サーバの証明書や属性証明書の発行または失効処理を行う。

X.509 公開鍵証明書の利用

エンティティは個人識別情報を持ち歩く。移動した先で認証サービスを検索し、応答した認証サービスに向けて個人識別情報を提示する。つまり、エンティティは個人情報を格納するソフトウェア的またはハードウェア的なセキュリティデバイスを保持しており、また、サービス発見プロトコルなどを用いて移動先での認証サービスを問い合わせる機能を持つ。その後、状況に応じて利用する個人識別情報を選択し、応答したサーバに向けて発信する。個人証明書を含むX.509公開鍵証明書は、識別子と公開鍵がバインドされたものであり、以下の3つの主要コンポーネントにより構成される。

- 署名前証明書（tbsCertificate）
- 署名アルゴリズム（signatureAlgorithm）
- 署名値（signatureValue）

証明書の所有者や公開鍵、有効期間などの情報は、署名前証明書に記載され、署名前証明書に対するCAのデジタル署名が署名値に記述されている。署名前証明書には、発行者（issuer）、有効期限、主体者（subject）などの情報の他に、バージョンやシリアル番号 等が記載されている。発行者や主体者は、X.500識別名（DN）において記述されているため、本プロトタイプシステムでは、図 5の情報の切り出し処理において、このDNを属性値（c、o、ou、cn）毎に切り分け、マッピングモジュールでこの属性値を検索キーとして識別子テーブルと対応づける。

また、図 5における属性証明書の発行には、マッピングモジュールがプライベートRAの役割を担い、発行する属性証明書に対して自分の証明書を付加することで、エンティティに対して、そのサービスドメイン内の資源利用および権限についてを証明する。

個人証明書に関する情報は、プロトタイプシステム設計時にはノートPCにX.509個人証明書を複数保存することを想定しているが、将来的にはICカードや携帯電話に保存したX.509個人証明書 以外の個人情報を用いることや、RFC3039 [12]にある特定証明書（Qualified Certificate）への適応も考慮する必要がある。

評価項目の検討と議論

ここでは、提案モデルに基づくプロトタイプシステムを実装する場合に評価すべき項目について検討する。

スケーラビリティ

提案モデルを基にプロトタイプシステムを設計した際のスケーラビリティについてを検証する場合、比較対象は、属性証明書を用いたネットワー

ク資源提供モデルおよび従来のアカウント発行に基づく資源提供モデルであり、処理可能なエンティティの数と拠点数を軸とした整理と評価が必要である。しかし、本提案で用いる一時属性証明書や個人証明書に基づく認証の性能は、証明書発行頻度に依存する。つまり、証明書発行頻度はポリシに依存することになるが、性能のばらつきを吸収するための正規化が必要となるといえる。

安全性と管理・運用コスト

エンティティが提示する個人証明書は利用者の個人情報を含むため、通進路の安全性や、個人情報の蓄積および開示場所について慎重に検討する必要がある。また、安全性や柔軟性、拡張性の高いシステムを設計しても、導入・管理および運用コストの高いものは淘汰される。大規模なポリシデータベースとの連携や個人識別情報の処理時間短縮などに関して工夫するための検討が必要である。

新しいアプリケーションへの適応

ユビキタスコンピューティング環境では、新しい応用アプリケーションの発現や フレームワークの構築に関して研究開発が進んでいる。

たとえば、プローブ情報システム [10]や AutoID センター [11]のように、移動する計算機やセンサが情報発信を行い、インターネット上で情報が有機的に集約・加工され、有用なサービスとして提供される。 つまり、情報提供者とサービス提供者（情報加工者）が異なっている。 これに特有の問題として、情報発信時は、本当にその場所から、その人によって送信された情報かどうかを保証および検証不可能であることが挙げられる。つまり、従来の情報送信技術だけでは、実空間に依存する動的な情報の正当性を検証または保証することができないため、この問題に対する対応が求められる。

本提案モデルでは、サービス利用要求を出すエンティティが、移動先で自分の個人証明書を用いて認証を行うため、これらのエンティティが送信するプローブ情報の送信元の保証は検証可能である。しかし、新しいサービスモデルの発現と共に顕在化した、サービス利用者や情報発信者の個人情報の保護、場所や時間などの動的に変化する実空間情報の正当性や完全性の保証といった問題については、さらに議論する必要がある。

以上の評価項目を考慮した上で、今後、プロトタイプシステムを実装し、提案モデルの有効性について検証していく。

4.3.4 むすび

個人が小型の計算機を携帯し、街角でインターネットに接続する場面が増えてきた。本学の電子図書館でも、利用者が持ち込んだ計算機をインターネットに接続する環境を提供している。しかし、認証のモデルやメカニズムが十分に検討されていないため、このような計算機利用に関しては、利用者に応じたサービス提供や、必要に応じた利用者の特定が困難であった。これは、新規のサービスを柔軟に提供したり、問題が発生した場合の原因追求を阻害する原因ともなっていた。

本章では、利用者の移動を前提としたユビキタス環境におけるネットワーク資源提供のためのサービスモデルを提案した。このモデルでは、利用者が自分のホーム環境において証明された個人証明書を携帯し、移動先にその証明書を適宜提示することで、移動先でのサービス提供を要求する。各サービスドメイン内では、定義された運用またはセキュリティポリシと提示された証明書の情報を対応づけ、アクセス制御や権限委譲などの処理を行う。対応づけられた権限やネットワーク資源は、一時属性証明書に記述される。利用者はこの一時属性証明書を用いることで、あらゆる場所で、その場所のポリシに沿った形でのサービスおよび資源を利用することが可能となる。

この提案モデルに基づいたプロトタイプ設計例として、公開鍵暗号基盤の個人証明書および一時属性証明書と、リレーショナルデータベースを用いたシステムを提示し、処理の流れを示した。また、今後の課題として、このプロトタイプシステムを実装した際に評価すべき項目と、さらに議論が必要な検討課題について述べた。

4.3.A 参考文献

石橋勇人, 坂本晃, 山井成良, 安倍広多, 大西克実, 松浦敏雄, ``利用者ごとのアクセス制御を実現する情報コンセント不正利用防止方式,'' 情報処理学会論文誌, vol.42, No.1, pp.79-88, 2001.

P. Calhoun and C. Perkins, ``Mobile IP Network Access Identifier Extension for IPv4,'' RFC 2794, 2000.

S. Corson and J. Macker, ``Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations,'' RFC 2501, 1999.

J. Myers, ``IMAP4 Authentication Mechanisms,'' RFC 1731, 1994.

C. Newman, ``Using TLS with IMAP, POP3 and ACAP,'' RFC 2595, 1999.

Charlie Scott, Paul Wolfe, Mike Erwin, ``Virtual Private Networks 2nd Edition,'' OREILLY, 2002.

Tristan Richadson, Quentin Stafford-Fraser, Kenneth R. Wood and Andy Hopper, ``Virtual Network Computing,'' IEEE INTERNET COMPUTING, vol.2, No.1, 1998

L. Mamakos and K. Lidl and J. Evarts and D. Carrel and D. Simone and R. Wheeler, ``A Method for Transmitting PPP Over Ethernet (PPPoE),'' RFC 2516, 1999.
浜田 良樹, ``プライバシーの権利とインターネット, '' Japan Cyber Security Management, vol.3,5,6, 2000.
和田 光示, ``プローブ情報システム (IPCar) プロジェクト, '' 情報処理学会学会誌, vol.43, No.4, pp.363-368, 2002.
AutoID Center Home Page, http://www.autoidcenter.org
S. Santesson, W. Polk, P. Barzin, and M.Nystrom, ``Internet X.509 Public Key Infrastructure Qualified Certificates Profile,'' RFC3039, 2001.

4.4 書籍における RFID の利用

4.4.1 はじめに

電子図書館は電子化された資料を扱う図書館であるが、著作権などの問題により、重要な資料であっても電子化が難しい場合も多い。しかしながら、書誌情報などの電子化が進むにつれ、実際に存在する通常の書籍であっても、コンピュータを用いた検索などの処理が行えるようになってきている。図書館における所蔵図書の管理を行うために、RFID の利用が近年注目を集めている。

図書館において RFID を利用することにより、貸し出し、返却の効率化や棚卸などの日常業務に役立てることが考えられており、いくつかの公共図書館などでは、このようなシステムが運用されはじめている。しかしながら、これらのシステムではそれぞれの図書館が独自に、図書の受け入れとともにタグを添付する方法をとっており、データ構造、タグの添付位置などの互換性がなく、タグに関してもそれぞれのシステムにより異なるものが利用されることが考えられる。このような場合には、図書館相互での貸借において問題が生じることが想定される。

現在、出版業界においても出版物にたいして RFID を添付することにより、業務の効率化や著作権の管理などを行いたいという動きが存在している。倉庫や店頭における検品、数量の確認などや、返本の効率化などにおいて、RFID は大きな期待をもたれている。しかしながら、書籍に対してタグをどのように実装するか、流通過程において破損しないか、といった問題は解決されていない。

さらに RFID を用いることにより「どの本を持っているか」といったことを遠隔から知ることが可能になるため、プライバシの問題が危惧されている。

そこで、実際の流通プロセス上で流通する書籍に RFID を添付し、その問題点を探る実証実験を行った。本実験では、大きく 2 つの問題に関する知見を得ることを目標とした。

１つはタグを実装した製品の製造および流通における技術的な問題点を探ることである。

もう１つの目的は RFID の入った製品が市場に流通することによる、社会的な問題点を抽出することである。

1.　出版業界における RFID の利用

日本における RFID の利用に関して、熱心なのはアパレル業界および出版業界である。

出版業界では、在庫の管理、盗難の防止、レンタル品の管理などに RFID による個体管理を行うことを想定している。特に日本においては、書籍の店頭における盗難は大きな問題となっている。そこで、業界団体が主導して出版物への RFID の応用を研究している。しかしながらタグの実装方法に関する研究は進んでいない。さらにタグを添付した出版物を出版し、流通させた場合には社会的にどのような問題が生じるかについての検証は行われていない。

4.4.2 EPC Network と AUTO-ID Labs.

RFID およびその周辺技術に関する標準規格として、EPC Network と呼ばれる仕組みが提案されている。EPC Network は EPC(Electronic Products Code)とよばれる番号体系とそれを利用する RFID を中心に、ネットワーク上に配置した情報システムを用いた RFID のトータルなシステムである。EPC Network は MIT で始まった AUTO-ID Center で開発された技術を継承したものであり、現在では国際 EAN 協会と米国 UCC という 2 つのバーコードに関する標準化団体により設立された EPC global という非営利組織により標準化および普及活動がすすめられている。[1]

Auto-ID Center はバーコードに代わる次世代の物体の自動認識システムおよびそれを利用したサプライチェーンマネジメント (SCM) を実現するための研究開発機関である。1999 年に MIT で始まった同センターは現在ではイギリス、オーストラリア、日本、スイス、中国に研究開発拠点を持つ。主に無線タグ(RFID)を用いた低コストだがネットワークを利用した拡張性のある自動認識システムの研究をおこなっていたが、2003 年の 10 月末をもってその役割の多くを EPC Global に移管した。

MITをはじめとする大学側のAUTO-ID CenterはAUTO-ID Labsという名称で、EPC Globalとともに研究開発を継続することとなっている。[2]

日本でのAUTO-ID Labsの研究拠点はAuto-ID Centerに引き続き、慶応大学湘南藤沢キャンパス内に設けられている。

4.4.3 本実験の目的

本実験の目的は出版物（書籍）に RFID を付加し、実社会に EPC コードのついた製品を出荷することにより、技術的および社会的な問題を探ることである。

図１： インターネット不思議発見隊

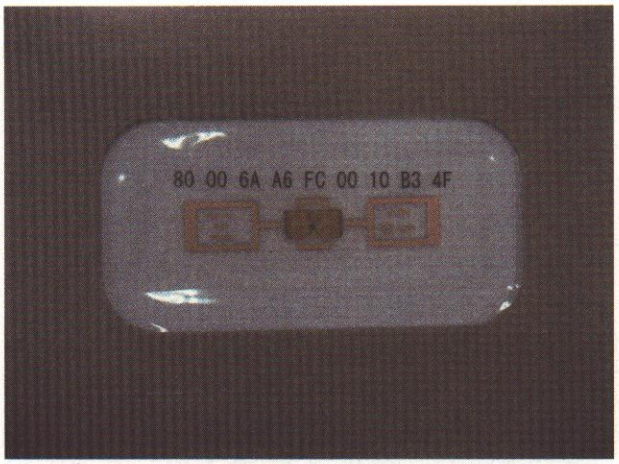


図 2： 2.45GHz RFID

題材となる書籍は日本の AUTO-ID Labs の代表である慶応義塾大学の村井純教授による「インターネット不思議発見隊」という本を利用した。[図 1]この本は小中学生向けのインターネット技術の読み物であり、その中に新しいテクノロジーとして RFID についても一部述べられている。本実験で添付するタグは 米国の Alien Technology 社による 2.45GHz 帯のものであり、読者に対する付録として利用するため、流通過程で利用することは考慮していない。

この本は RFID タグが添付しているが、一般の書籍と同様の方法で製本、配本、販売されるため、現在の流通過程が RFID を添付した書籍に対してどれだけの問題があるかを知ることが可能である。

また、この RFID は単なる付録ではなく、書籍を持った読者が、インターネットを通じてコミュニケーションを行うための ID として利用できる。今後はこの RFID を利用したイベントを行うことにより、ユーザ間のコミュニケーションを高めることが計画されている。

次にタグを実際に添付する場合に考慮しなくてはならない問題点と、現在の解決方法について述べる。

4.4.4 実装上の課題とその解決

実際に行われている書籍の流通過程において、RFID がついた書籍が流通するために必要な課題とその解決方法について述べる。

制度・商慣習における課題

書籍の流通は日本において特別なケースにあたる。日本の書籍はすべての書店において定価で販売される。定価販売を行う代償として、出版社は売れなかった本の責任をとる必要があり、これを再販制度と呼ぶ。

再販制度とは書籍が書店において販売されなかった場合には、出版社へと no penalty で返却することが可能である制度である。出版社は戻ってきた書籍は在庫として利用するため、カバーなどを renew し新たな書籍として再生する。こ

のとき、RFIDのついた書籍の場合には、表面上のrenewのみならず、書籍についたRFIDに関する検証が必要となる。

EPCタグが動作していない場合にはタグの交換などの手順が必要となるため、タグは容易に交換できることが望ましい。

今回のケースの場合には、タグは流通過程で利用せず、付録という立場であるため、出版社における在庫あるいは返却品におけるEPCタグの動作チェックは行っていない。

EPCタグが万引き防止や購買のチェックに利用されるには、店頭においてEPCタグが正常に動作している必要があるため、EPCタグのチェックは出版社における重要な作業になると考えられる。

タグの実装技術の問題

将来的には、すべての書籍にRFIDが挿入されることが目標となっている。そのような場合にはRFIDは出版物内部に見えないように添付されることになると想定できる。

現在のところ、表紙の内部あるいは背表紙にタグを挿入することがもっとも一般的に考えられている。しかしながら、書籍の流通過程において背表紙はもっとも衝撃をうける可能性がある部分であり、その内部にRFIDを埋め込んだ場合には破損することが考えられる。

次に考えられる場所として、表紙ないし背表紙が考えられる。この場合にはなんらかの方法で圧力を逃がす構造を持つ必要がある。

これらの部分にタグを添付した場合には、書籍の厚みがあるため複数読み取りの場合に、その電波の届く範囲が制限され、複数同時読み取りの性能が劣化することがわかっている。

予備実験では、そのまま表紙内部にタグを添付した場合には、圧力によりすべてのRFIDが破損した。これは書籍が流通の過程において、多数を一度に梱包し、パレットを用いて運搬するからであると考えられる。

4.4.5 実装方法

今回のケースでは児童向けの出版物であり、RFIDに対する理解を深めるという目的があったため、EPCタグは露出した形で添付している。そのため、透明フィルムを利用してタグが目視できる形式での添付を行った。

タグを見せる必要がない場合には、カバーのためのフィルムを不透明かつ、台紙と同色とすることにより、タグの添付位置を目立たなくすることが可能であると考えられる。

実際の作業手順を以下に示す

① RFIDタグを透明なシールにはりつけ、ラベル形状にする。

EPC番号はシール上に印字しておく。これはタグが読み書き不能になった場合に目視によりタグ内部にあるものと同じEPCデータを知ることができる必要が

あるためである。また、今回はユーザを含んだ別の実験においてタグを利用することを想定しており、この場合にもユーザはリーダがない場合には自分で数字を打ち込むことによりリーダと同等に自分の持っている書籍を識別することが可能である。

② ラベルタグのデータ書き込み

ISO15693 のタグの場合、ラベル印字と同時にデータを書き込む一体型のラベルライタが製品化されている。今回利用した Alien technology 社の 2.4GHz 帯タグはこのようなシステムに対応していないため、すべてを手作業で行っている。

タグの表面には EPC コードおよび EPC コードのチェックサムが記載されている。それぞれのタグに書き込まれた EPC データを目視することが出来るため、リーダを持たなくてもどのような EPC が割り振られているかを確認できる。

これは、ユーザの利便性を向上させるとともに、RFID に障害が発生した場合の対策でもあり、実際に流通現場において RFID を利用する場合においても必須であると考えられる。

③ 張り込み

タグを保護するための台紙として厚紙を用意した。厚紙は２枚で一組となっており、台紙と保護のための穴のあいた紙が重ねあわされている。タグは台紙にあけられた穴のくぼみに取り付けられる。これにより、書籍を積み重ねた場合に生じる圧力からタグを保護する。

今回の実験では張り込み作業の後、もう 1 度タグが機能しているかどうかのチェックを行っている。

④ 製本

書籍全体の製本が終了したのち、タグを張り込んだ台紙を別途、裏表紙にたいして取り付ける。タグを最終段階で取り付けることによりタグの不良や作業工程におけるミスによる書籍全体への損害が出ないようになっている。

⑤ チェック

製本後の書籍はもう一度１冊毎にチェックされる。

以上のプロセスを用いて、製本を行った。今回は、製本数が 6000 部であり、設備投資が不可能であるため多くの部分は手作業で行っている。将来的に、書籍への RFID の添付が一般的になった場合には、タグの作成などの部分が自動化されると考えられる。また、チェックも製造工程の装置上で行うことが可能になると想定される。

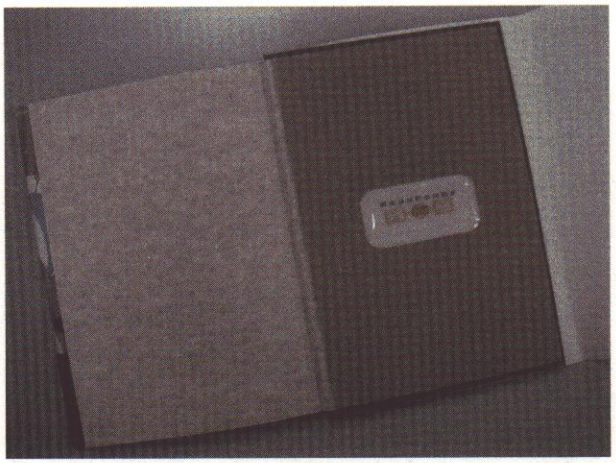


図３：書籍に実装された RFID

4.4.6 プライバシとタグの盗聴防止

書籍などのように持ち歩く可能性のある製品において、RFID のデータが流出する可能性は否定できない。本実験では、流通段階では RFID を利用しないため書店において kill などの処理を施すことはできない。

そこで、書籍に折り込みの注意を入れることで対応した。対応策としては以下の 3 点を提示している。

- タグをアルミホイルでくるむ。この方法はタグが外部からの電波により動作することを利用し、外部からの電波を遮断する方法である。これにより、タグを利用したい場合には、アルミホイルを取り外して利用し、利用したくない場合には、ホイルを用いてくるむことにより、タグの選択的な利用を可能にする。この方法は著者からの推奨として、書籍に添付された折込み冊子に書かれている。

- 出版社に送り返してタグの動作停止処理をすることにより、見た目がなんらかわらないまま、タグを読み取り不可能にする。タグの停止処理はリーダライタを用いて行う必要があるため、今回の場合には店頭ではなく、リーダライタのある出版社に送る必要があるが、将来的には店頭にあるリーダライタを用いて行われる。

- タグを物理的に取り外す。タグはシールで貼り付けられているのでカッターナイフなどを用いて切り取ることが可能である。しかしながら、書籍を傷つけることになるため、このような方法は推奨していない。タグを盗難防止の目的にも利用することを考えると、物理的なタグの取り外しやすさは将来的にも考慮されないことが想定される。しかしながら、書籍を古紙回収などのリサイクルのプロセスに載せる場合には、なんらかの対応策が必要であると考えられる。

4.4.7 おわりに

まず、書籍に対してタグを取り付ける場合には、タグの破損を防ぐために、タグを保護する必要があることがわかった。また、取り付け位置に関しても、背表紙はタグの破損が生じる可能性が高いが電波的に有利であること、表紙の裏側はタグの保護のための手段を講じることが可能であるが、複数の書籍が重なった状態での読み取りは難しい。

また、タグの取り付け方法に関しても、数千～数万部程度の一般書籍では問題にならないが、雑誌やコミックのように大量に印刷、製本する必要がある場合には、シールによる方法では追いつかないと考えられる。

RFID とプライバシの問題においては、タグが添付されていることや、そのタグにより情報が入手できることを明確にしめした上で利用者にその選択を委ねる”インフォームドコンセント”の考え方を導入することを提案した。

タグの利用を拒否する場合には、タグを破棄することや、動作しないように処理するといった方法がある。今回の実験では選択的に必要なときだけタグを読み取り可能にするためには、アルミホイルを利用したカバーを提案した。

このようにRFIDを書籍に対して出版段階から取り付けるためには、多くの研究開発やプロセスの改善が必要であるといえる。

図書館においても出版社より配本される段階においてRFIDの添付が行われることは、その作業効率の向上に十分に有効であるが、個人の持ち物である書籍以上にプライバシの問題などへの対応が必要になると考えられる。

4.4.A 協力

本実験は、編集および出版におけるあらゆる問題に関して、太郎次郎社および太郎次郎社エディタスの協力をいただいた。また、タグの添付作業に関しては凸版印刷および、トッパンフォームズ、RFID タグの提供に関してはエイリアンテクノロジーおよび、東レインターナショナルの協力をいただいた。

4.4.B 参考文献

[1] EPC Global http://www.epcglobalinc.org/
[2] AUTO-ID Labs. http://www.autoidlabs.org/