７． ライセンスリポジトリの技術的課題

本章では、ライセンスリポジトリ方式を実現するうえでの技術的課題を検討し、それぞれの課題に対する解決の方策を明らかにする。解決の方策に関わる技術動向や製品がある場合には、それらの調査を行い、ライセンスリポジトリ方式実現に向けて考察する。

７．１ 調査指針

まず、ライセンスリポジトリ方式の利用モデルを想定する。想定モデルからライセンスリポジトリ方式のシステム要件を整理し、その要件から、１)想定される脅威を回避するためと、２)ライセンスリポジトリの必要機能を実現するための２つの観点から課題を検討する。

続いて、各課題において技術的課題を検討し、それぞれの技術的課題に対して解決の方策を明らかにする。なお、解決の方策において参考となる技術動向や製品がある場合には、それらの調査も行う。

７．２ 調査項目の整理

７．２．１ ライセンスリポジトリ方式の想定モデル

ライセンスリポジトリ方式の想定するモデルを図 7-1 に示す。ライセンスリポジトリは、添付資料を管理、発行する主体によって「官」または「民」からの添付資料の登録を受け付ける。さらに申請、審査をトリガにして、申請者以外からの添付資料へのアクセスに対して、添付資料の「公開」「非公開」特性に応じたアクセス制御を行うことと想定する。またライセンスリポジトリ方式は、必要に応じて証明書発行手数料や登録手数料などを電子的な手段で納付を行うことができると想定する。

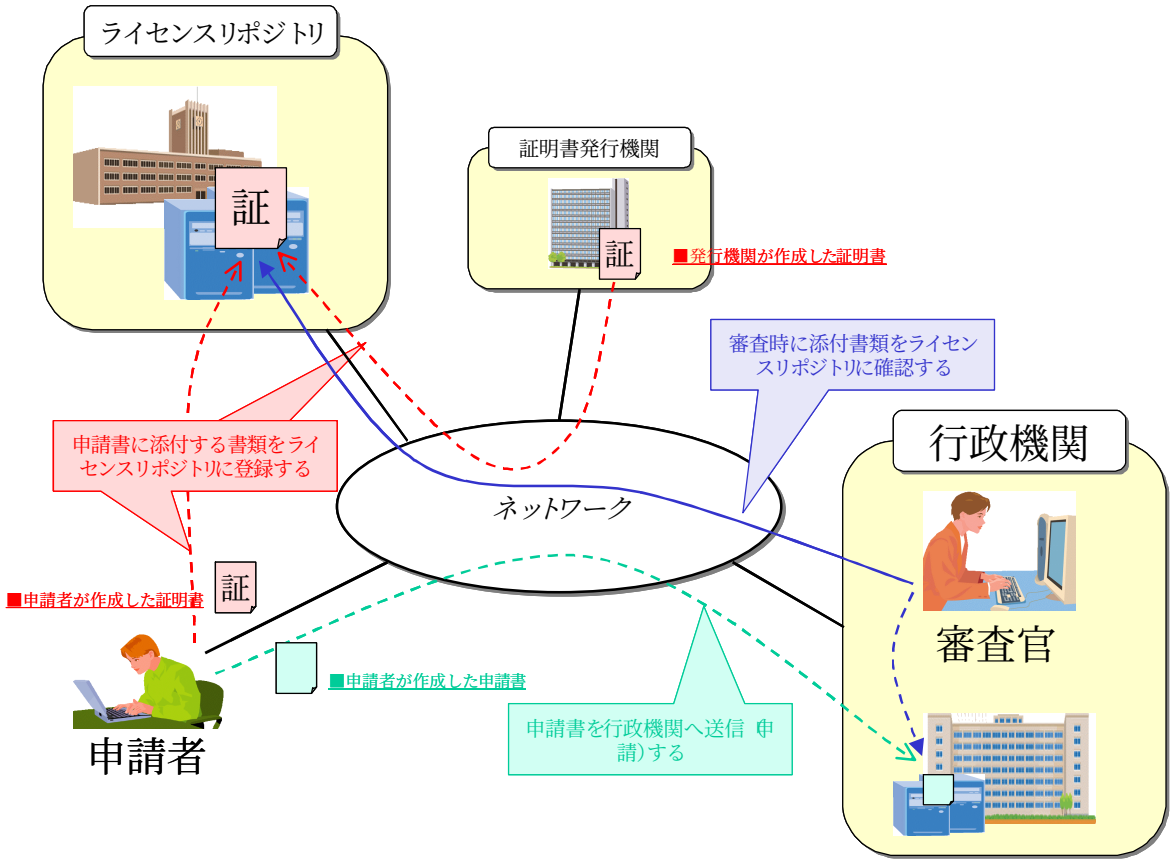


図 7-1　ライセンスリポジトリ方式のモデル図

本報告で定義したライセンスリポジトリ方式の定義と図 7-1 に示したモデルから、ライセンスリポジトリ方式のシステム要件を以下に示す。

（1） 申請者が申請に添付する資料をライセンスリポジトリに登録できること
（2） ライセンスリポジトリ内に登録されている添付資料が、安全に保存され、原本として扱うことができること
（3） ライセンスリポジトリに登録されている情報のネットワークを介した公開は、添付資料に応じて適切な者に行われること
（4） 添付資料に関わる手数料が徴収できること

7．2．2 本報告書で調査対象とする課題

これらの要件より、ライセンスリポジトリ方式の実現においては、以下の課題を検討する必要がある。なお、（1）、（2）、（3）はライセンスリポジトリの実現において想定される脅威を回避するために必要な課題、（4）（5）はライセンスリポジトリ運用の

際に特に検討が必要な課題である。

（1） 外部攻撃からのセキュリティ確保

ライセンスリポジトリは、ネットワークを介した添付資料の公開を行うためにネットワークに接続されている。そのため、ライセンスリポジトリは様々なアクセス者からのアクセスを受けることとなる。正当なアクセス者に対するネットワークからのアクセスのみを許可するため、第三者からのネットワークからのアクセスや攻撃に対する防御が必要である。

（2） システムの信頼性確保

ライセンスリポジトリは、申請に必要な添付資料を管理しているため、申請受付機関からのアクセス時には常に添付資料を公開する必要がある。また、申請者による添付資料の登録、更新に応じて、常に情報を最新な情報を維持し提供する必要がある。

（3） 添付資料の原本性保証

ライセンスリポジトリでは、本来は申請受付機関が申請書データと一緒に管理する添付資料を、申請受付機関に代わって保存、管理を行う。従って、ライセンスリポジトリでは、申請受付機関など第三者に対して添付資料の原本性を保証する仕組みが必要となる。

（4） ライセンスリポジトリ方式における添付資料の管理方法

ライセンスリポジトリでは、ライセンスリポジトリの類型やモデル、また利用形態に適した添付資料の管理を実現する必要がある。

（5） ライセンスリポジトリ方式における手数料の納付方法

現在、添付資料を発行機関より入手する際には発行手数料が必要となる。ライセンスリポジトリによって添付資料が電子化された場合においても、現在と同様に添付資料の発行に必要となる手数料を納付する必要が生じる。そのため、ライセンスリポジトリ方式に電子的な決済手段を導入する必要がある。

７．３ 外部攻撃からのセキュリティ確保

７．３．１ 調査目的

本節では､ライセンスリポジトリ方式の実現においてネットワークを介した外部攻撃からセキュリティ確保を行うための技術的課題を整理し､ライセンスリポジトリ方式に適した解決の方策を明らかにすることを目的とする。

添付資料には、プライバシーを含む重要な情報が含まれている場合も多いため、ライセンスリポジトリ方式導入時においても、情報の登録時、閲覧時ともに高いセキュリティを確保することが必要となるためである｡さらに高いセキュリティを確保するためには、電子署名法における特定認証業務に関する認定制度のような、多面的な技術的な対策が必要となるためである。

７．３．２ 調査内容および結果

本調査では、ネットワークを介して外部から受ける脅威を整理し、その脅威を防ぐための技術的課題と解決の方策を検討した｡さらに解決の方策に関連する製品動向を調査した。

７．３．２．１ セキュリティ確保における技術的課題

近年、不正アクセスやウィルス[1]によるネットワーク経由の攻撃や被害が増加している。2000 年 1 月の省庁ホームページ改ざんや、2001 年 10 月の Nimda などのウィルスによる被害は多大であった。また「コンピュータ不正アクセス対策基準」(平成 8 年通商産業省告示 第 362 号、第 949 号)によって、不正アクセスによる被害の予防、発見及び復旧並びに拡大及び再発防止について企業等の組織及び個人が実行すべき対策がとりまとめられており、ライセンスリポジトリ方式実現においても、ネットワークを介する脅威に対する対策を講じる必要がある。

そこで、ライセンスリポジトリ方式実現におけるネットワークを介する想定脅威、技術的課題と解決の方策について検討した結果を表 7-1 にまとめる｡さらに各解決方策に関連する技術の製品動向を次節でまとめる。

表 7-1　セキュリティ確保における技術的課題

想定される脅威	技術的課題	解決策	関連技術
ネットワークからの不正侵入、DoS 攻撃	ネットワークからのアクセス経路、プロトコルに応じた通信のアクセス制御を実施する	ファイアウォール（FW）の導入により NW アクセスの制御を行う	認証技術 FW
	システムの利用状況を定期的に監査を行い、リアルタイムで監視する	ネットワークからのアクセスログを取得し定期的に監査を行う	FW
		侵入検知システム（IDS）による監視を行う	IDS
ウィルス感染	ウィルスの侵入・感染を検知する仕組みを設ける	アンチウィルスソフトによるウィルスチェックを行う	アンチウィルスソフト

７．３．２．２ 認証技術

認証とは､対象となる人や物に対し本当に主張している人や物なのか識別し証明する手段である｡システムにおいて認証対象となる人や物およびこれら認証対象に応じて認証を行う必要がある（表 7-2)。

ライセンスリポジトリ方式において､ネットワークを介したアクセスを制御するための認証には、表 7-2 に示すアクセス者の本人認証が必須となる。そこで本節では、表 7-3 にまとめる認証技術について製品動向を調査した。

表 7-2　電子申請システムにおける認証の種別

認証種別	認証対象	想定脅威
本人認証	人間（本人）	本人のなりすまし
サーバ認証	サーバ	サーバのなりすまし
クライアント認証(端末認証)	クライアント（端末）	クライアントのなりすまし
メッセージ認証	電子化書類	書類の改竄

表 7-3　認証技術と認証種別との関係

認証技術	認証種別			
	本人	サーバ	クライアント	メッセージ
ID/パスワード認証	○	×	×	×
ワンタイムパスワード認証	○	×	×	×
チャレンジレスポンス認証	○	○	○	×
IC カード認証	○	×	×	×
バイオメトリックス認証	○	×	×	×
ゼロ知識証明認証	○	×	×	×
電子署名	○	×	×	○

（1） ID／パスワードによる認証

(a) 実現方式

予めサービスを提供するシステムにてユーザの ID とパスワードの対を管理しておき、本人認証時に利用者に ID とパスワードの文字列を対で入力させ、この対がシステムに登録されているものと等しいかどうかを比較する方式である（図 7-2）。

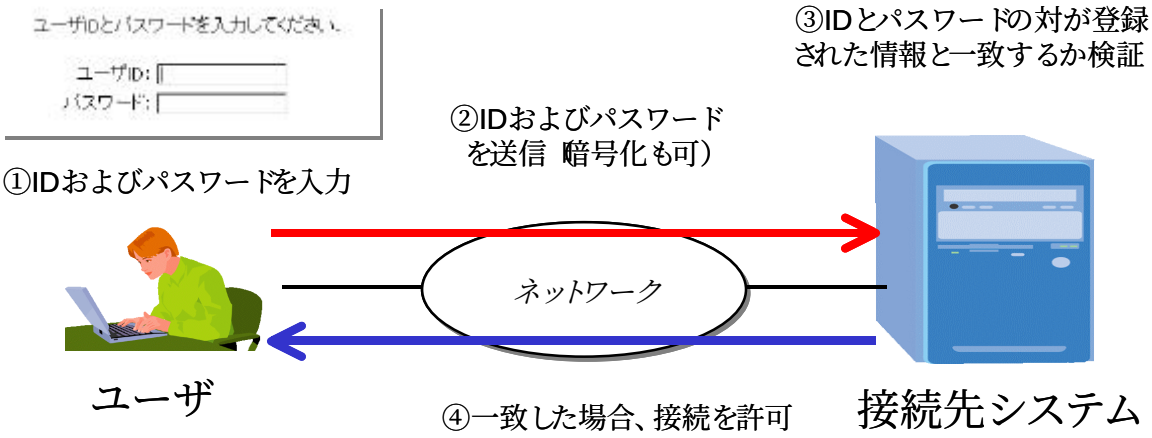


図 7-2 ID／パスワードによる認証方式の概要

(b) 製品動向

認証システム単体の製品はなく、アクセス制御を必要とするシステム（OS やデータベースなど）に備わっている。

（2） ワンタイムパスワードによる認証

(a) 実現方式

前述の ID/パスワード方式では、傍受や試行の繰り返しにより ID およびパスワードの対を見破られる可能性があったが、この方式ではパスワードの有効期限を定め 1 回の認証にのみ有効(One Time)であるパスワードを使用するため、パスワードが解読されても再び同じパスワードを使用することができない等の利点がある（図 7-3）。

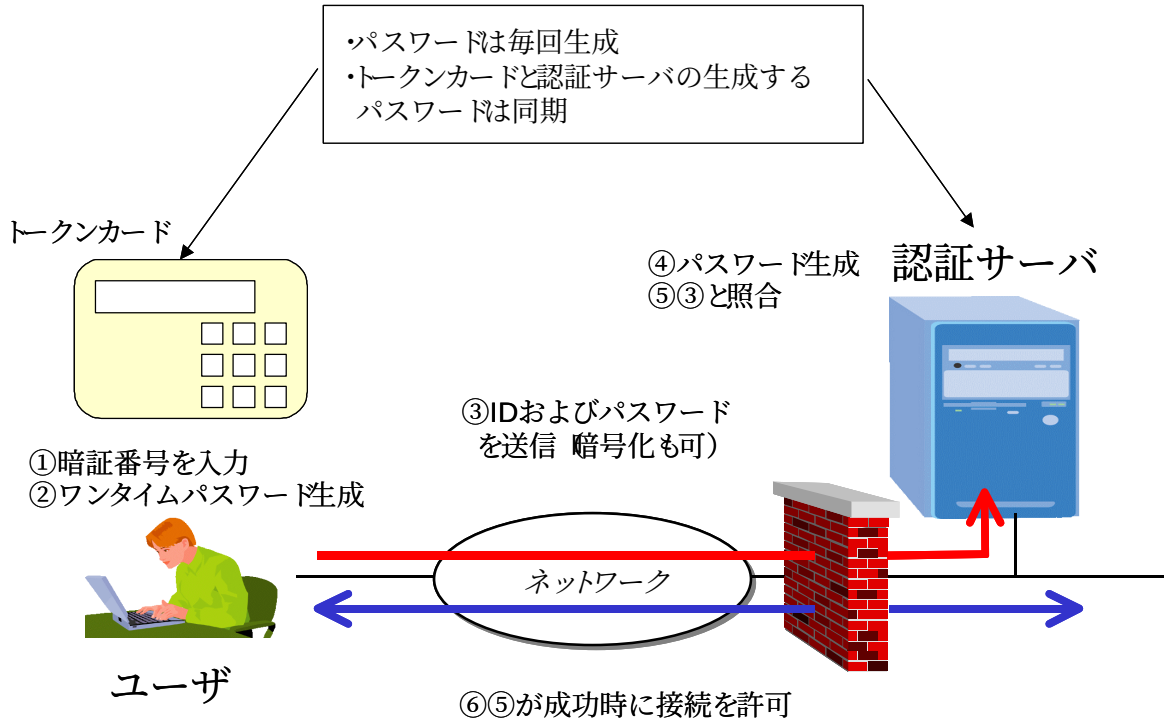


図 7-3　ワンタイムパスワードの利用例とシステム構成

上図では、「認証トークン」（上図ではトークンカード）と呼ばれるハードウェアまたはソフトウェアにより認証を依頼するクライアント側でワンタイムパスワードを生成させ ID と共に送信、これと同期して認証サーバ側で ID に対応するパスワードを生成し照合することにより認証を行っている。

（b）　製品動向

表 7-4 にワンタイムパスワード認証システムの製品一覧を示す。認証サーバと認証トークンとのパスワードの同期方法には三種あり、サーバとトークンで時間を同期させる時間同期方式、チャレンジレスポンス方式、サーバとトークンでカウンタを同期させるカウンタ同期方式などがある。

表 7-4　ワンタイムパスワード認証システム　製品一覧

製品名		開発元	トークンのタイプ	認証方式
認証トークン	認証サーバ			
SecureID	ACE/Server	Security Dynamics[2]	電卓タイプ,PCMCIA	時間同期方式
SoftID			ソフトウェア	
SAFEWORD	SAFEWORD サーバ	Secure Computing[3]	電卓タイプ	カウンタ同期方式
SAFEWORD SofToken			ソフトウェア	
ActivCard Gold	ActivPack	ActivCard[4]	Smart Card	時間同期方式 ﾁｬﾚﾝｼﾞﾚｽﾎﾟﾝｽ方式 カウンタ同期方式
ActivCard			電卓タイプ	
Digipass	VACMAN Server	Vasco Data Security[5]	電卓タイプ	ﾁｬﾚﾝｼﾞﾚｽﾎﾟﾝｽ方式 時間同期方式 カウンタ同期方式
Digipass　Soft			ソフトウェア	

（3）　チャレンジレスポンスによる認証

(a)　実現方式

この方式は、認証者側でチャレンジと呼ばれる乱数を発生させて被認証者へ送付、被認証者側で受信したチャレンジを暗号化またはハッシュ化し再度認証者に送付、認証者側で返送されたチャレンジの正当性を検証する方式である（図 7-4）。

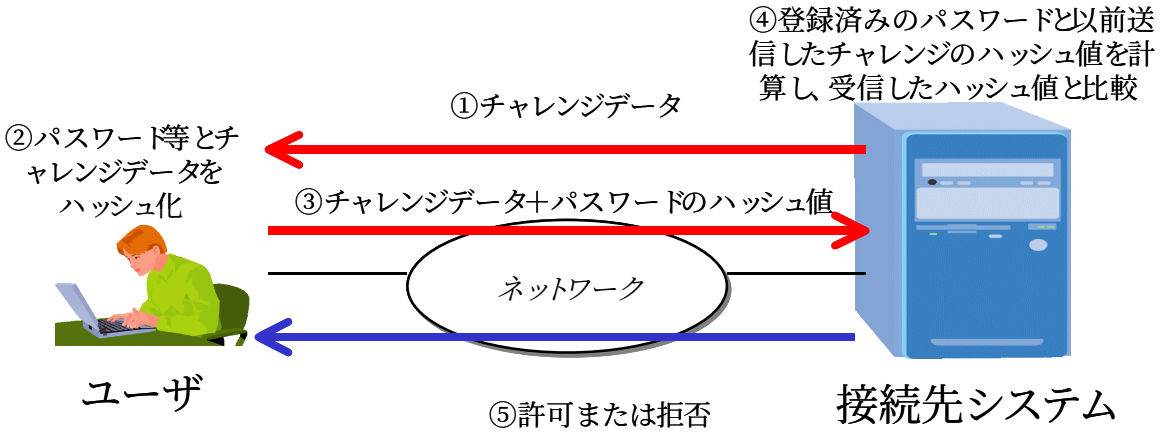


図 7-4　チャレンジレスポンスによる認証方式の概要

(b)　製品動向

この方式は、前述のワンタイムパスワード方式と組み合わせて使用されるケースが多く、市販されている製品もこの方式とワンタイムパスワード方式を組み合わせた認証システムとして提供されている。また、主にダイアルアップ接続の RAS(Remote Access Service) や Microsoft の Windows Network においてユーザ認証プロトコルに採用されている。

（4） IC カードによる認証

(a) 実現方式

この方式は、システムへの接続およびサービスの享受を許可されているユーザに予め個人を特定するための IC カードを配布し、IC カードリーダを持つ端末側で認証を行う方式である。端末側の認証方式は、カード内に記録されている情報を使用する、カード自身の持つ認証機能を使用するなど様々な方式があるが、基本的には物理的にカードを所有していることで本人の識別および認証を行う方式である。

(b) 製品動向

前述のワンタイムパスワードの認証トークンとして使用されている製品(ActivCard Gold 等)が見られる他、各メーカの提供する IC カードに対し、各システムで独自の認証方式を組み込むケースが多い。

（5） バイオメトリクスによる認証

(a) 実現方式

生物の体や行動の特徴（指紋・網膜・虹彩・顔貌・耳形・筆跡（署名）・声紋・掌紋・掌形・手の血管・指形）に注目してそれぞれの個体を識別し認証する方式である。指紋認証を利用した本人認証システムの概要を図 7-5 に示す。

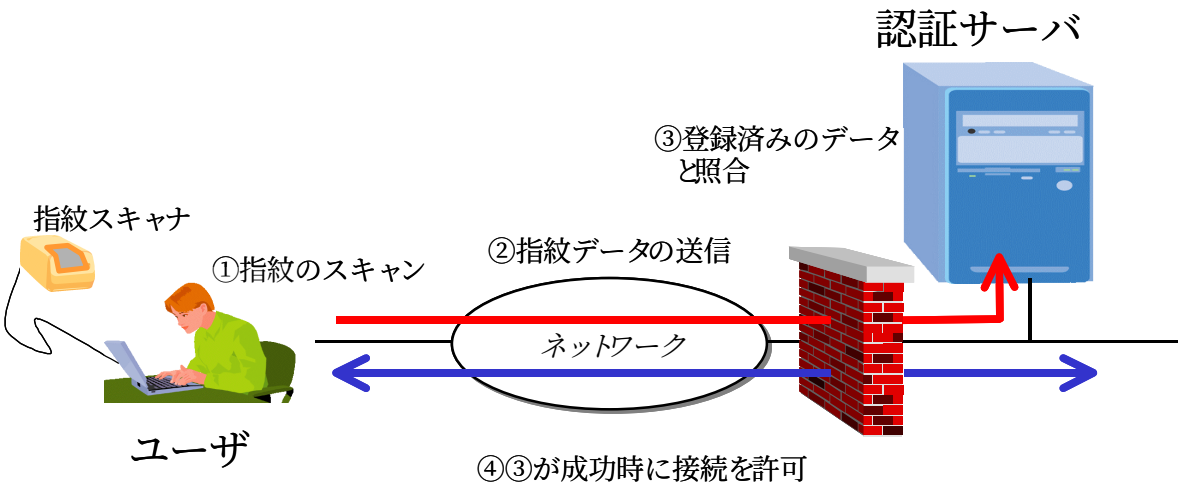


図 7-5　指紋認証システムの概要

(b)　製品動向

バイオメトリクス認証の主な製品を以下に示す。近年指紋認証装置が多く販売されており安価になりつつある。さらに幾つかのパソコンメーカからは OS へのログイン時に指紋認証を組み込んでいるノートパソコンが発売されている。

表 7-5　バイオメトリクス認証システム　製品一覧

製品名	メーカ	対応ＯＳ	価格	認証方式
TrueFace	eTrue[6]	WindowsNT/2000	1,040,000 円―	顔認証
VoiceGATE II	株式会社アニモ[7]	Windows, Solaris,Linux	3,000,000 円―	声紋認証
Cyber-Sign	日本サイバーサイン株式会社[8]	Windows95 以上	99 米ドル―	筆跡認証
指紋認証ユニット	日本電気株式会社[9]	Windows95/98/ NT/2000	34,800 円―	指紋
指紋認識装置	富士通株式会社[10]	Windows95/98/ NT/2000	29,800 円	指紋
指紋照合センサ	オムロン株式会社[11]	Windows98/Me/ NT/2000	19,800 円―	指紋

（6）　ゼロ知識証明による認証

(a)　実現方式

この方式は、パスワードなど本人だけが知っている秘密情報を使った認証において、秘密情報を知っていることを、秘密情報自体は送受信することなく証明する方式である。

検証者が乱数と秘密情報から演算した結果を質問の形で証明者に送り、証明者が回答を検証者に送るというテストを何度も繰り返すことで認証を行う。この方式では 1 回のテストでは秘密情報を知らない人が偶然パスする可能性があるが、何回も繰り返すことにより、確率的に本人である可能性を高め、認証精度を高めることが可能である（図 7-6）。

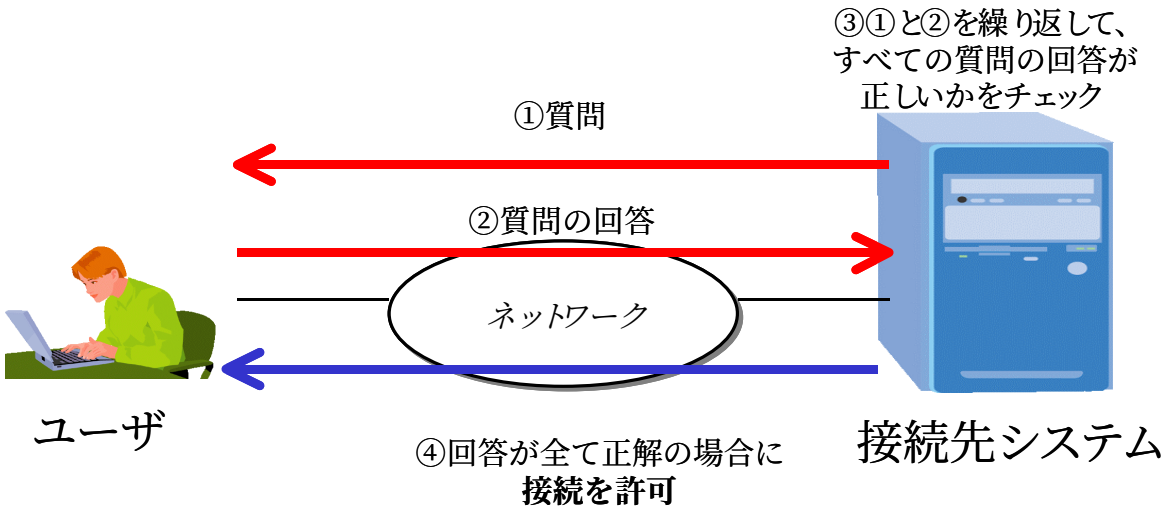


図 7-6　ゼロ知識証明による認証方式の概要

(b)　製品動向

特になし。

（7）　電子署名による認証

(a)　実現方式

電子署名は、RSA 等の公開鍵暗号方式とメッセージダイジェストを用いて行うメッセージ認証方式の一つである。文書作成後に文書作成者は、改ざんがないことを証明するために、紙文書の場合に印鑑を押印するのに対し、作成した文書から生成される電子署名を添付する。電子署名は、文書からメッセージダイジェストと呼ばれるハッシュ値を求め、これに対して作成者の持つ秘密鍵で暗号化して作成されるデータである。メッ

セージダイジェストは通信コストや暗号化処理の効率を考慮し元の文書より遥かに小さい固定長のデータ（例えば 128 ビット等）として抽出され、メッセージダイジェストを抽出するアルゴリズムには一般的に MD5、SHA-1 などが用いられる。次に、電子署名の添付された文書に対し、この文書が通信過程または保管先で改竄されていないことを検証するために、文書受取者は送付された文書のメッセージダイジェストを求めた後、それに添付されている電子署名を文書作成者の公開鍵を使用して復号化、受取者が抽出したメッセージダイジェストと電子署名より復号化したメッセージダイジェストを比較する。これらメッセージダイジェストが等しい場合改竄されていないことを証明することができる。

この方式では、公開鍵暗号方式を使用するため、被認証者すべてに対し公開鍵および秘密鍵の管理が行われていることが前提となる。これより、文書の改ざんを検証する者は電子署名を復号化するために電子署名を作成した者の公開鍵を入手する必要があり、PGP のような公開鍵配布サーバから公開鍵を入手するか、認証局（CA：Certification Authority）の発行する証明書から公開鍵を入手する方法をとる必要がある。

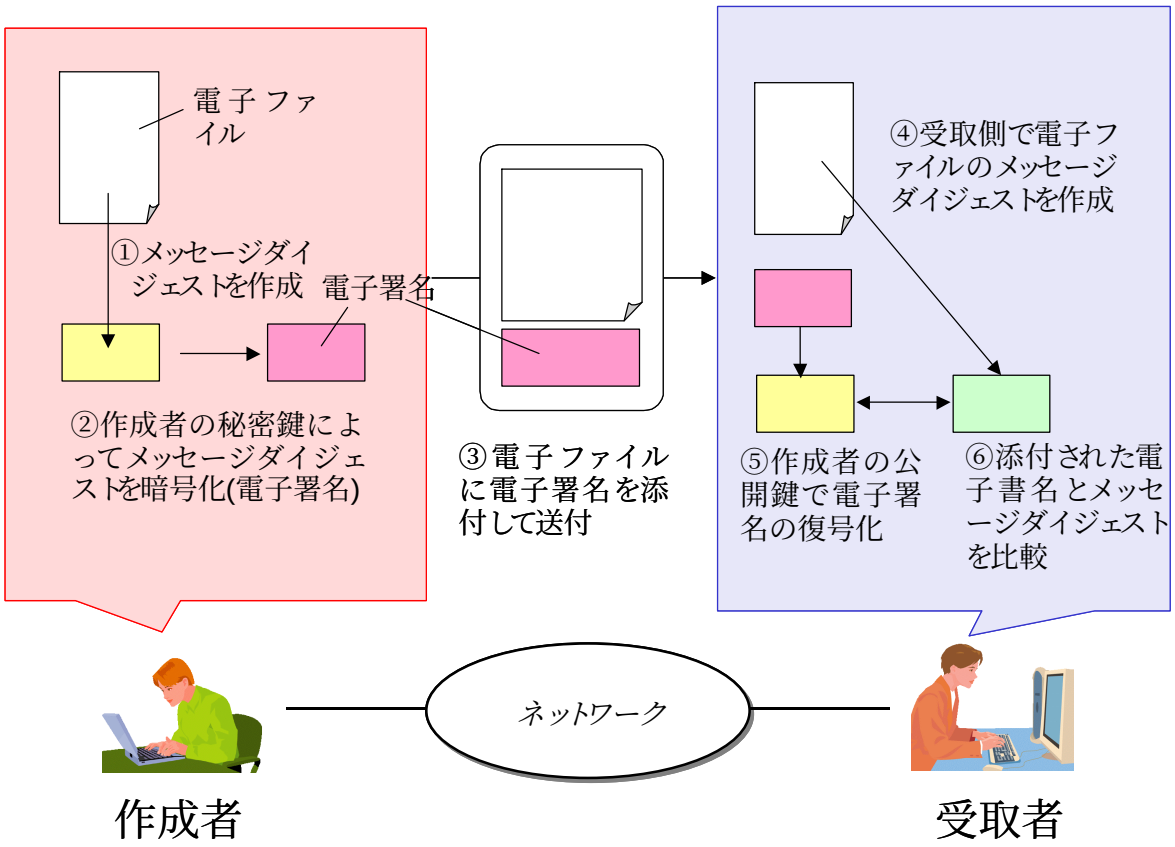


図 7-7　電子署名による認証方式の概要

（b） 製品動向

電子署名を検証する際に必要となる公開鍵暗号方式の公開鍵証明書を発行する機関は、認証局（CA）と呼ばれている。ここでは第三者的に公開鍵を認証し、その証明書を発行するサービス（CA サービス）について整理する。

表 7-6　国内ＣＡサービス一覧

サービス名/製品名	運営組織/メーカ	認証方式
SecureSign	日本認証サービス株式会社[12]	認証サービス
AccreditedSign	日本認証サービス株式会社	電子署名法認定認証業務
OnSite/Go Secure!	日本ベリサイン株式会社[13]	認証サービス
Entrust PKI eGovernment Edition	エントラスト ジャパン株式会社[14]	電子署名法認定認証業務
UniCert	日本ボルチモアテクノロジーズ株式会社[15]	CA 製品
法務省商業登記 CA	法務省	法人用認証サービス

７．３．２．３ ファイアウォール（FW）

ファイアウォールとは､インターネットとこれに接続するローカルエリアネットワーク(LAN)の中間に配置しその間の通信を制御することで､インターネット上の悪意のある第三者から LAN に接続されている基幹システムへの不正なアクセスを防ぐための技術である。

（１） 実現方式

（a） パケットフィルタリング方式

パケットフィルタリング方式は、OSI モデルにおけるネットワーク層でアクセス制御を行う方式であり、発着アドレス、ポート番号、接続を開始する方向性、プロトコルなどに基づいたフィルタリングを行う。通常、ルータなどの経路制御機能を有する装置を利用する。この方式は、ルータのフィルタリング条件を設定するだけで実現が可能であるが、嘘の IP アドレスやポート番号を使ってアクセスされた時（なりすまし）に対して、対処が困難である。

（b） ゲートウェイ（プロキシ）方式

ゲートウェイ方式（プロキシ）方式は、IP フレームを素通りさせるのではなく、プロキシ（代理人）が要求を処理することで、IP フレームを完全に遮断し、外部からの侵入を防ぐ。この方式には、トランスポート層でデータを転送し、外部パケットが内部に直接流れ込むことのないサーキットレベルゲートウェイと､特定のアプリケーションに対応した細やかな制御が可能なアプリケーションゲートウェイがある。

（2） 製品動向

FW 製品について以下にまとめる。なお、FW 製品一覧をまとめるにあたり主に企業が使用する商用ファイアウォールと個人ユーザが使用するパーソナルファイアウォールに分けてまとめた。

(a) 商用ファイアウォール

表 7-7　商用ファイアウォール製品一覧

製品名	メーカ	対応ＯＳ	価格	実現方式
FIREWALL-1	Checkpoint Software Technorogies[16]	HP-UX10.10/10.20, AIX4.2.1/4.3, Solaris2.5/2.6, WindowsNT4.0	490,000 円―	ゲートウェイ方式
SonicWall	SONICWALL [17]	専用 OS	140,000-728,000 円	パケットフィルタリング方式
Symantec Enterprise Firewall	Symantec[18]	WindowsNT/2000	400,000 円―	ゲートウェイ方式
Cisco Secure PIX Firewall	Cisco Systems[19]	専用 OS	2,164,000 円	パケットフィルタリング方式
Internet Security and Acceleration（ISA）Server 2000	Microsoft[20]	Windows2000	288,000 円―	ゲートウェイ方式

(b) パーソナルファイアウォール

表 7-8　パーソナルファイアウォール製品一覧

製品名	発売元	対応ＯＳ	価格	実現方式
WinWrapper	株式会社アスキー・エヌ・ティ[21]	Windows95/98/ NT4.0/2000	5,800 円―	ゲートウェイ方式
BlackICE Defender	株式会社東陽テクニカ[22]	Windows95/98/ NT4.0/2000	6500 円―	ゲートウェイ方式
Zone Alarm	ZONELABS[23]	Windows95/98/ NT4.0/2000	19.95 米ドル	ゲートウェイ方式
Tiny personal FireWall	TINYSOFTWARE [24]	Windows95/98/ NT4.0/2000	29 米ドル	ゲートウェイ方式
ウィルスバスター 2002	トレンドマイクロ株式会社[25]	Windows95/98/ NT4.0/2000	8500 円	ゲートウェイ方式
ノートン・インターネットセキュリティ	Symantec[	Windows95/98/ NT4.0/2000	9800 円	ゲートウェイ方式
Net Barrier 1.5J	Intego[26]	Macintosh	1,5800 円	ゲートウェイ方式
DoorStop Personal Firewall	OpenDoorNetworks [27]	Macintosh	59 米ドル	ゲートウェイ方式
RT105e	ヤマハ株式会社[28]	専用ハード	110,000 円	パケットフィルタリング方式
BRL04FW	プラネックスコミュニケーションズ株式会社[29]	専用ハード	32,800 円	パケットフィルタリング方式
FR314	NETGER[30]	専用ハード	53,000 円	パケットフィルタリング方式
ZyWALL10	株式会社ブレーン [31]	専用ハード	49,800 円	パケットフィルタリング方式
AR320	アライドテレシス株式会社[32]	専用ハード	68,000 円	ゲートウェイ方式
VIAGGIO MR104F	オムロン株式会社	windows95/98/Me/ NT/2000/XP, Mac OS 8.1 以上	18,000 円	パケットフィルタリング方式

７．３．２．４ 侵入検知システム（IDS）

侵入検知システム（IDS）とは、ログやネットワークトラフィックなどを監視することで、ファイアウォールを通過してくるような、攻撃や侵入などの不正行為を検出するシステムである。

（1） 実現方式

IDS の実現方式には、検知する不正侵入の種類によってネットワークベースとホストベースの 2 方式がある。

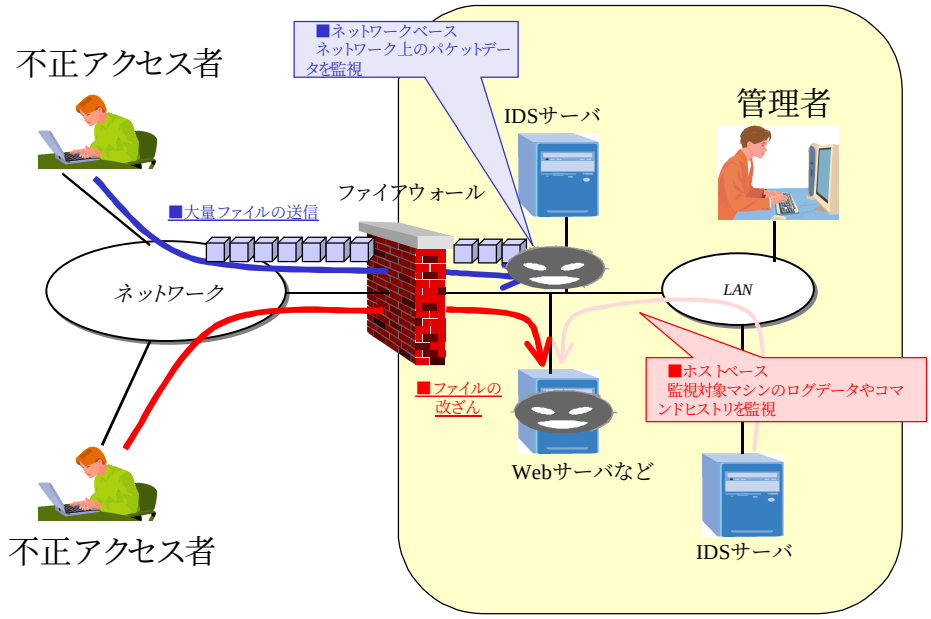


図 7-8　ＩＤＳによる不正侵入検知の概要

(a)　ネットワークベース

ネットワーク上のパケットデータを入力データとして用いる。そのため、大量のパケットを送りつけてコンピュータを麻痺させてしまうような不正アクセスを検出することができる。しかし、全パケットを取り込んで解析するため、高速マシンが必要である。また暗号化された通信には無効である。

(b)　ホストベース

OS や各種アプリケーションが記録するログデータやコマンドヒストリなど、監視対象とするホスト上で生成されるイベント情報を入力情報として用いる。そのため、コンピュータ内のファイルを置換・破壊してしまうような、ファイル操作タイプの不正アクセスを検出することができる。しかし、ファイルに直接変更を加えない不正アクセスの検出には不向きである。

（2） IDS 製品動向

以下に主な IDS 製品を示す。

表 7-9　IDS 製品一覧

製品名	メーカ	対応ＯＳ	価格	実現方式
RealSecure Network Sensor	Internet Security Systems[33]	Windows2000/NT4.0 ,Solaris	1,079,000 円	ネットワークベース
RealSecure Sever Sensor		Windows2000/NT4.0 ,Solaris	194,000 円	ホストベース
BlackICE Defender for Workstation		Windows2000/NT4.0 ,Windows95/98/Me	6,500 円―	ネットワークベース
BlackICE Defender for Server		Windows2000/NT4.0	49,500 円	ネットワークベース
NFR	NFR Security	専用ハード	840,000 円	ネットワークベース
SessionWall-3	Computer Associates[35]	Windows NT4.0	390,000 円	ネットワークベース
CyberCop Intrusion Protection	Network Associates[36]	Windows NT4.0	800,000 円	ネットワークベース/ ホストベース
Tripwire	TRIPWIRE[37]	Windows2000/NT4.0 ,Solaris 2.6,7, HP-UX 10.20,11.00	1,740,000 円	ホストベース
Cisco Secure IDS	Cisco Systems	HP-UX 10.20, Soladis 2.6	1,596,000 円―	ネットワークベース

７．３．２．５ アンチウィルスソフト

システムにおけるウィルスの感染を防ぐには、ウィルススキャンプログラムを使ってウィルスの感染を早期に発見し駆除すると共に、ネットワークに接続する他システムに対して被害が広がらないうちに対策をとる必要がある。

（1） 実現方式

ウィルス対策は、ウィルススキャンプログラムを実行するマシンによって４つの方式がある（図 7-9）。

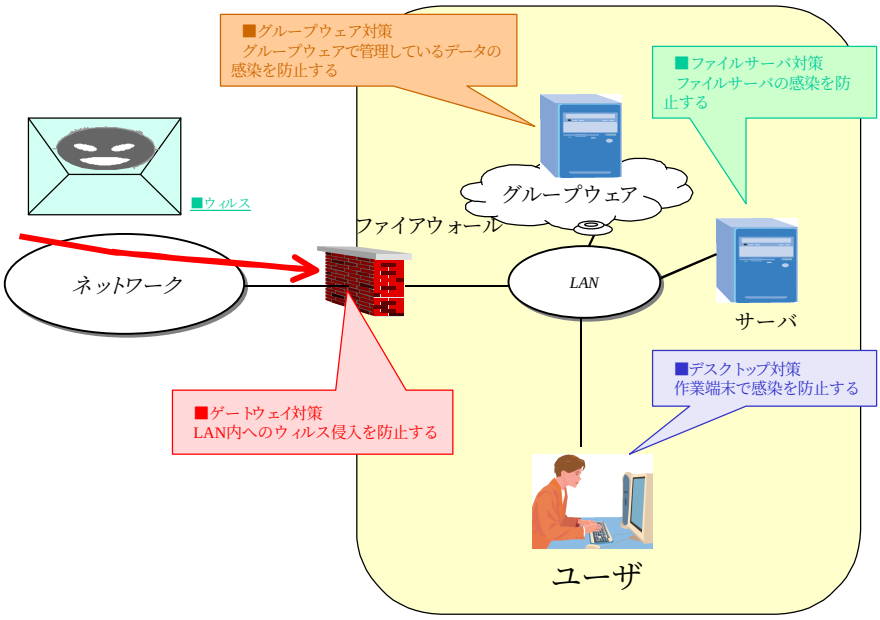


図 7-9　ウィルス対策の実施マシン

(a) ゲートウェイ対策

ネットワークとの境界線上でウィルスチェックを行い、LAN 外のネットワークからの電子メール、ダウンロードファイルのウィルスチェックを行い、LAN 内へウィルスが侵入しないようにする。また、LAN 内のネットワークから LAN 外へのウィルスの発信も防ぐことができる。

（b） グループウェア対策

グループウェア内で流通するメール(添付された文書)や、サーバに格納されるファイルに対し、ウィルスチェックを行う。グループウェアでは、流通するメール(添付された文書)やサーバに格納する文書を圧縮／暗号化したり、独自のフォーマットに変換したりしているため、発見／駆除が難しく、グループウェア毎に専用のソフトを必要とする。

（c） ファイルサーバ対策

製品によっては、ハードディスク、ネットワークドライブに対して入出力されるファイルを常に監視する。また、ウィルスを発見した場合には、「駆除」、「リネーム」、「移動」、「削除」および「放置」といった処理ができる。しかし、ファイルサーバ側ですべてのウィルスの侵入を防止するのは困難なため、デスクトップ対策のソフトと組み合わせて使用する必要がある。

（d） デスクトップ対策

ユーザマシンにウィルススキャンプログラムをインストール・実行する対策である。マシンに常駐し、ローカルディスク、フロッピーディスク、CD-ROM などにアクセスする場合にウィルスチェックを自動的に行い、また、必要がある場合には、ドライブ、ディレクトリを指定して配下にあるファイルを一括してチェックすることにより、感染を防止する。

（2） 製品動向

以下に主なアンチウィルス製品を示す。

表 7-10　アンチウィルス製品一覧

製品名	発売元	対応ＯＳ	価格	実現方式
Norton AntiVirus Enterprise Solution 4.6	株式会社シマンテック	Windows98/Me/ NT4.0/2000/XP	8,800 円―	ファイルサーバ対策 デスクトップ対策
Norton AntiVirus 7.0 for Macintosh	株式会社シマンテック	MAC OS 8.1 以上	9,800 円―	ファイルサーバ対策 デスクトップ対策
Norton AntiVirus 2.5 for Lotus Notes/Domino	株式会社シマンテック	Winrows2000/NT, Solaris 2.6 以上, AIX 4.3.2 以上	3,950 円（1 ライセンス）―	グループウェア対策
Norton AntiVirus 2.5 for Gateways	株式会社シマンテック	Winrows2000/NT, Solaris 2.6, 7.0, 8.0	231,500 円―	ゲートウェイ対策
ウィルスバスター 2002	トレンドマイクロ株式会社	Windows95/98/Me/ NT4.0/2000/XP	7,500 円―	デスクトップ対策
ServerProtect	トレンドマイクロ株式会社	Windows NT4.0/2000, Red Hat Linux	57,000 円 ―（Windows） 298,000―（Linux）	ファイルサーバ対応
InterScan for Microsoft Exchange	トレンドマイクロ株式会社	Windows NT4.0/2000	298,000 円―	グループウェア対策
InterScan for Lotus Notes	トレンドマイクロ株式会社	Windows NT4.0/2000, Solaris 2.5.1 以上, AIX 4.2.0 以上	298,000 円―	グループウェア対策
InterScan VirusWall	トレンドマイクロ株式会社	Windows NT4.0/2000, Solaris2.6/7/8, HP- UX10.2 以上/11, Redhat Linux 6.1/6.2, TurboLinux Server6.1, AIX4.3.3 以上 /5Lver.5.1	360,000 円―（30 ユーザ）	ゲートウェイ対策
VirusScan	日本ネットワークアソシエイツ株式会社	Windows95/98/Me/ NT4.0/2000/XP	6, 900 円―	デスクトップ対策
VirusScan for Macintosh	日本ネットワークアソシエイツ株式会社	Mac OS 7.6/8.6/9.0.2/9.0.4/9.1	7,440 円―	デスクトップ対策
WebShield Solaris	日本ネットワークアソシエイツ株式会社	Solaris 2.6	580,000 円―	ゲートウェイ対策
WebShield e500/e250 appliance	日本ネットワークアソシエイツ株式会社	専用ハード	2,750,000 円（e500） 1,750,000 円（e250）	ゲートウェイ対策
GroupShield Exchange	日本ネットワークアソシエイツ株式会社	Windows NT4.0/2000	75,000 円―	グループウェア対策
GroupShield Domino	日本ネットワークアソシエイツ株式会社	Windows NT4.0	75,000 円―	グループウェア対策
NetShield	日本ネットワークアソシエイツ株式会社	Windows NT4.0/2000	53,000 円―	ファイルサーバ対策

７．３．３ 考察

外部攻撃からのセキュリティ確保は、理想的にはライセンスリポジトリの形態に関わらず対策が必要な課題である。さらに電子政府システムや電子商取引システムなどの出現により、外部攻撃からのセキュリティ確保に対する技術的解決を行う、様々な製品やサービスが登場している。これらを活用すれば容易に外部攻撃からのセキュリティ確保は実現可能と考えられる。しかし、全ての対策を行うとなると、導入コスト、運用コストや人材などが必要となり、特に中小規模のライセンスリポジトリでは対応が困難と推測できる。

そこで、ライセンスリポジトリの形態や運用、添付資料の特徴からライセンスリポジトリの社会的な信頼性、責任などの整理を行ったうえ、各モデルで確保しなければならないセキュリティレベルを示す必要があると考える。ライセンスリポジトリ実現の際には、レベルに応じた解決方策と、ライセンスリポジトリ運営のコストや人材の都合により、効果的な既存の製品やサービスの導入を検討することが重要である。

７．３．４ 参考文献

[1] 2001 年ウィルス発見届出状況（情報処理振興事業協会）：
http://www.ipa.go.jp/security/txt/attach/2002_01-1.html
[2] SecurityDynamics 社ホームページ：http://www.rsasecurity.com
[3] SecureConputing 社ホームページ：
http://www.securecomputing.com/index-js.html
[4] ActivCard 社ホームページ：http://www.activcard.com/activ/
[5] VasoDataSecurity 社ホームページ：http://www.vasco.com/
[6] eTrue 社ホームページ：http://www.etrue.com/
[7] 株式会社アニモホームページ：http://www.animo.co.jp/
[8] 日本サイバーサイン株式会社ホームページ：http://www.cybersign.co.jp/
[9] 日本電気株式会社ホームページ：http://www.sw.nec.co.jp/pid/
[10] 富士通株式会社ホームページ：
http://www.fmworld.net/product/hard/keyboard/fingsensor/
[11] オムロン株式会社ホームページ：
http://www.omron.co.jp/ped-j/product/fp/fps1000.htm
[12] 日本認証サービス株式会社ホームページ：http://www.jcsinc.co.jp/
[13] 日本ベリサイン株式会社ホームページ：http://www.verisign.co.jp/
[14] エントラストジャパン株式会社ホームページ：http://www.entrust.co.jp/
[15] 日本ボルチモアテクノロジーズ株式会社ホームページ：

http://www.baltimore.co.jp/
[16] Checkpoint Software Technorogies 社ホームページ：
http://www.checkpoint.com/
[17] SONICWALL 社ホームページ：http://www.sonicwall.com/
[18] symantec 社ホームページ：http://www.symantec.com/
[19] Cisco Systems 社ホームページ：http://www.cisco.com/
[20] Microsoft 社ホームページ：http://www.microsoft.com/
[21] 株式会社アスキー・エヌ・ティホームページ：http://www.ant.co.jp/
[22] 株式会社東陽テクニカ：http://www.toyo.co.jp/
[23] ZONELABS 社ホームページ：http://www.zonelabs.com/
[24] TINYSOFTWARE 社ホームページ：
http://www.tinysoftware.com/home/tiny?la=EN&va=aa
[25] トレンドマイクロ株式会社ホームページ：http://www.trendmicro.co.jp/
[26] intego 社ホームページ：http://www.intego.com/home.asp
[27] OpenDoorNetworks 社ホームペー―ジ：http://www.opendoor.com/
[28] ヤマハ株式会社ホームページ：http://www.yamaha.co.jp/
[29] プラネックスコミュニケーションズ株式会社ホームページ：
http://www.planex.co.jp/
[30] NETGER 社ホームページ：http://www.netgearinc.com/
[31] 株式会社ブレーンホームページ：http://www.brain-tokyo.jp/
[32] アライドテレシス株式会社ホームページ：http://www.allied-telesis.co.jp/
[33] Internet Security Systems 社ホームページ：http://www.iss.net/
[34] NFR Security 社ホームページ：http://www.nfr.net/
[35] Computer Associates 社ホームページ：http://www.cai.com/
[36] Network Associates 社ホームページ：http://www.nai.com/
[37] TRIPWIRE 社ホームページ：http://www.tripwire.com/

７．４ システムの信頼性確保

７．４．１ 調査目的

本節では､ライセンスリポジトリ方式の実現においてライセンスリポジトリ運用の信頼性を確保するための技術的課題を整理し､ライセンスリポジトリ方式に適した解決の方策を明らかにすることを目的とする。

電子政府実現時においては、24 時間 365 日ノンストップでのサービス提供が必須条件となると考えられ､電子申請についても同様で､ライセンスリポジトリ方式部分のシステムが何らかの理由で運用を停止することは最も避けなければならないことである。この意味から､ライセンスリポジトリ方式の実現にあたっては､バックアップシステム等､冗長性を持たせた構成からなる､高信頼性実現のための技術検討が必要となるためである。

７．４．２ 調査内容および結果

本調査では､システム運営において想定される脅威を整理し､その脅威を防ぐための技術的課題と解決の方策を検討した｡さらに解決の方策に関連する技術動向を調査した。

７．４．２．１ 信頼性確保における技術的課題

想定脅威、技術的課題と解決の方策について検討した結果を表 7-11 にまとめる。さらに解決の方策に関連する技術について次節でその動向を述べる。

表 7-11　信頼性確保における技術的課題

想定される脅威	技術的課題	解決策	調査対象
アクセス集中などによるサーバの過負荷	サーバへの大量なパケットなどによる負荷を分散させる仕組みを設ける	負荷分散装置を設置し、アクセスを複数のサーバに振り分ける	負荷分散装置
ハードウェア故障	機器の故障などによるトラブルに対する冗長性を確保する	クラスタリング技術を用いて、サーバの冗長性を確保する	クラスタリング
		ライセンスリポジトリセンタ内のネットワークを二重化し、冗長性を確保する	クラスタリング
自然災害や媒体劣化によるデータ消失	サーバ以外にデータを復旧することができる仕組みを設ける	計画的にバックアップを取得・保管し、常にリストアが実施できる状態にする	バックアップ

７．４．２．２ 負荷分散装置

ライセンスリポジトリに対して、予期せぬ大量のアクセスが集中した場合、サーバの処理能力不足によるレスポンスの低下が発生し、最悪の場合、レスポンスが極端に悪くなって、見かけ上、サーバがダウンしたのと同じような状態に陥ってしまう。ライセンスリポジトリを構築するにあたっては、こうした大量のアクセスに対する対策を考慮しなければならない。例えば、サーバ単体の CPU やメモリを増設したり、キャッシュ・サーバを設置したりすることで、システムの処理能力をある程度改善することはできるが、大量アクセスに対する根本的な解決策としては、負荷分散装置を導入して、システムのスケーラビリティを確保するのが望ましい。

（１） 実現方式

負荷分散装置は、図 7-10 のように、外部ネットワークとサーバとの間に設置され、外部ネットワークからのアクセスを一元的に管理し、配下の複数のサーバに対して処理の振り分けを行う。これにより、それぞれのサーバに負荷が分散され、サーバ周りのボトルネックを解消することができる。サーバの呼び出し側からは、サーバが１つしかないように見えるため、呼び出し側の設定は特に変更する必要がない。

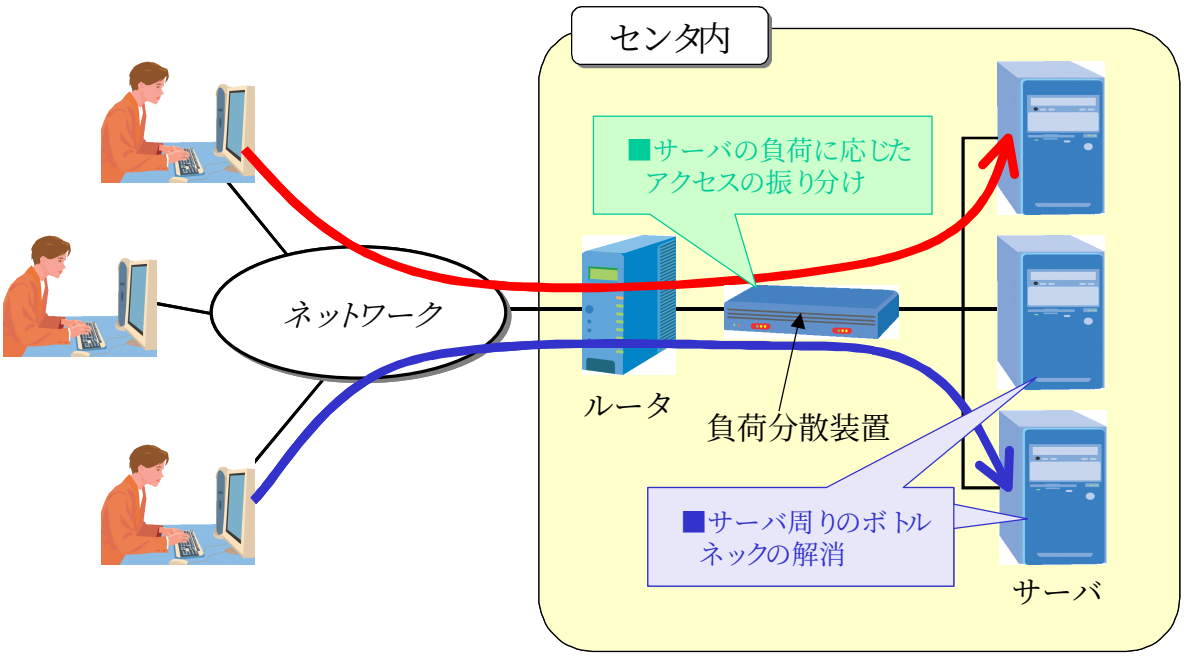


図 7-10　負荷分散装置の導入によるアクセスの分散処理

負荷分散装置では、あらかじめ定義されたルールに基づいて、アクセスの振り分けを

行うが、アクセスを振り分ける方法として、以下のような方式が用いられている。

（a） ラウンドロビン方式

最も単純な方法であり、受け付けたアクセスを配下のサーバに対して順番に割り当てるもの。個々のサーバの処理能力とそこで行われる処理が均等な場合に有効な方法で、一般に「ラウンドロビン」と呼ばれている。（図 7-11ａ）

（b） 重み付けラウンドロビン方式

配下のサーバの処理能力に差がある場合などに用いられる方法で、処理能力の高いサーバに対しては多めの処理を割り当てるといったように、サーバごとに設定された重み付けの割合に応じてアクセスを振り分ける。（図 7-11ｂ）

（c） コネクション数による振り分け方式

最もコネクション数の少ないサーバに優先してアクセスを振り分ける。（図 7-11ｃ）

（d） 応答時間による振り分け方式

Ping などでサーバの応答時間を測定し、最も応答時間の速いサーバに優先してアクセスを振り分ける。（図 7-11ｄ）

（e） CPU やメモリの使用率による振り分け方式

サーバにインストールしたエージェント・ソフトウェア、あるいは、SNMP（簡易ネットワーク管理プロトコル）の情報などにより、サーバの CPU やメモリの使用率などを収集して、最も負荷の少ないサーバに優先してアクセスを振り分ける。（図 7-11ｅ）

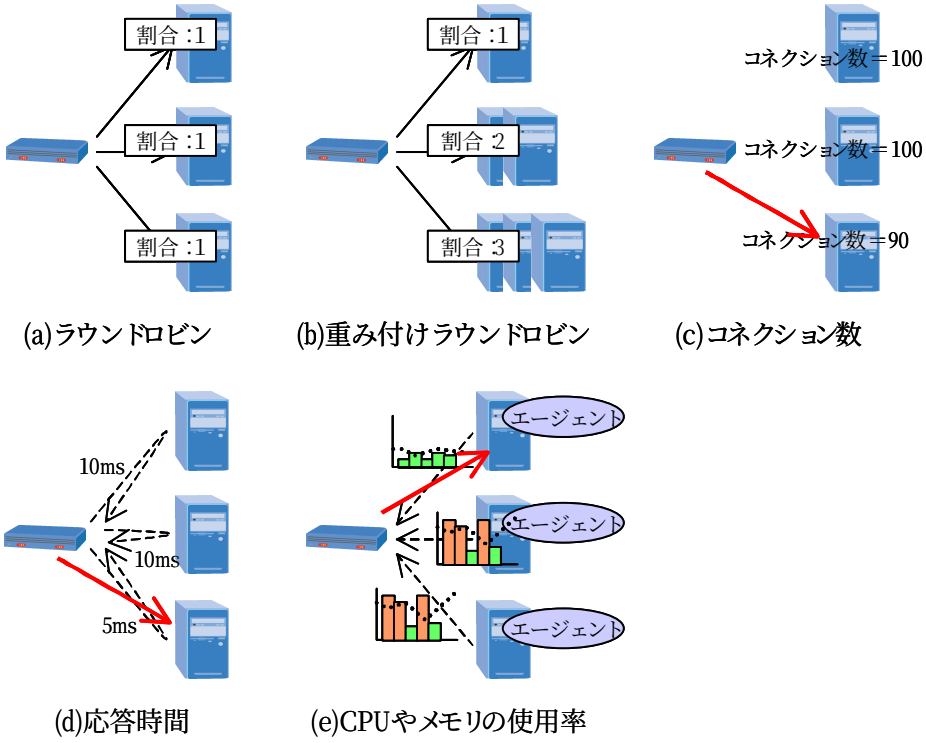


図 7-11　負荷分散装置におけるアクセス振り分け方式

負荷分散装置を用いたアクセスの振り分けにおいて、例えば、トランザクション処理のように、同じクライアントとサーバとの何度もやりとりを行う必要がある場合、ただ単純にクライアントからのアクセスをサーバに振り分ければいいとは限らない。この場合、一連のトランザクションが終了するまで、クライアントとサーバの接続を維持する必要がある。レイヤ7（アプリケーション層）対応の負荷分散装置では、アプリケーションレベルの情報を識別して、同一クライアントからのアクセスを同じサーバに振り分ける機能を持つ（図 7-12）。

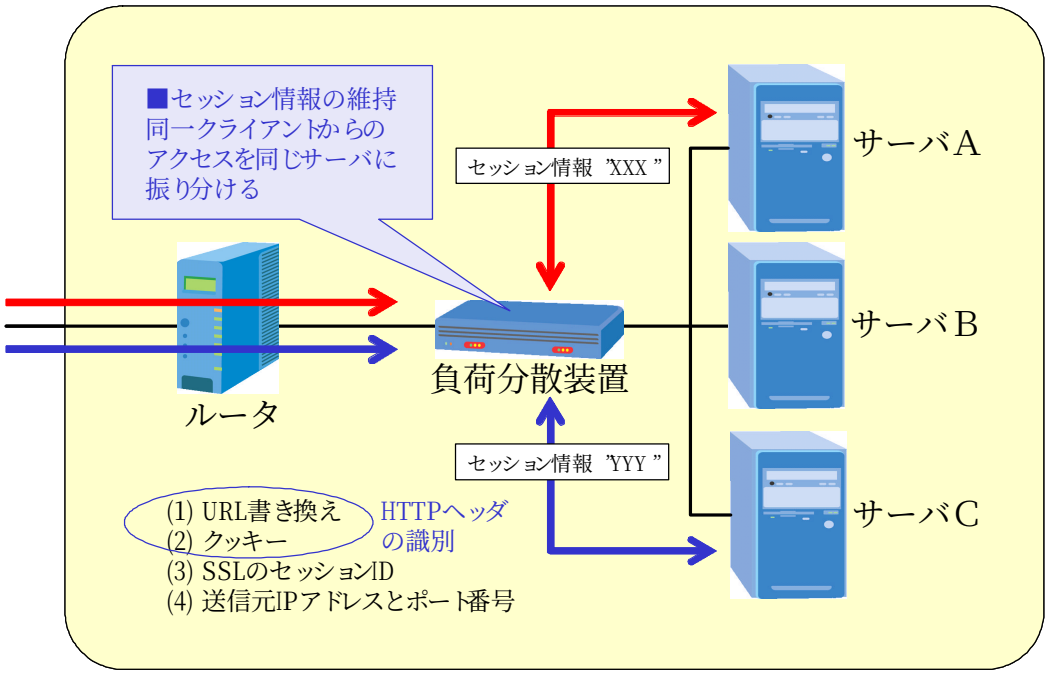


図 7-12　レイヤ 7 対応の負荷分散機能

（2） 製品動向

負荷分散装置の製品について、表 7-12 に整理した。

表 7-12　負荷分散装置

製品名	開発元	レイヤ 7 対応
BIG-IP コントローラ	F5 Networks [1]	○
Equalizer E250/E350/E450	Coyote Point Systems [2]	×
LocalDirector 416/430	Cisco Systems [3]	○
NetStructure 7180/7185 e-Commerce Director	Intel [4]	○
ServerIron XL,XL/G,400,800	Foundry Networks [5]	○
Summit 1i/5i/7i/48i	Extreme Networks [6]	×
Web Server Director	RADWARE [7]	○
X-Pedition 2000/2100/8000/8600/er16	Enterasys Networks [8]	×

7．4．2．3 クラスタリング

24 時間／365 日のサービス提供を前提としたライセンスリポジトリの構築においては、システムの可用性を確保し、ダウンタイムを限りなく 0 に近づけなければならない。一般に、システムの可用性を高めるには、システムの冗長化が有効な手段である。システムを冗長化するための方法として、「クラスタリング技術」が用いられる。

（1） 実現方式

図 7-13 は、クラスタリングを用いたシステム構成の例である。2 台以上のサーバ（ノード）を組み合わせて仮想的に 1 台のシステムを作り、システムの一部に障害が発生しても、他のサーバ（ノード）が処理を引き継ぎ、システム全体がダウンすることがないようにする。

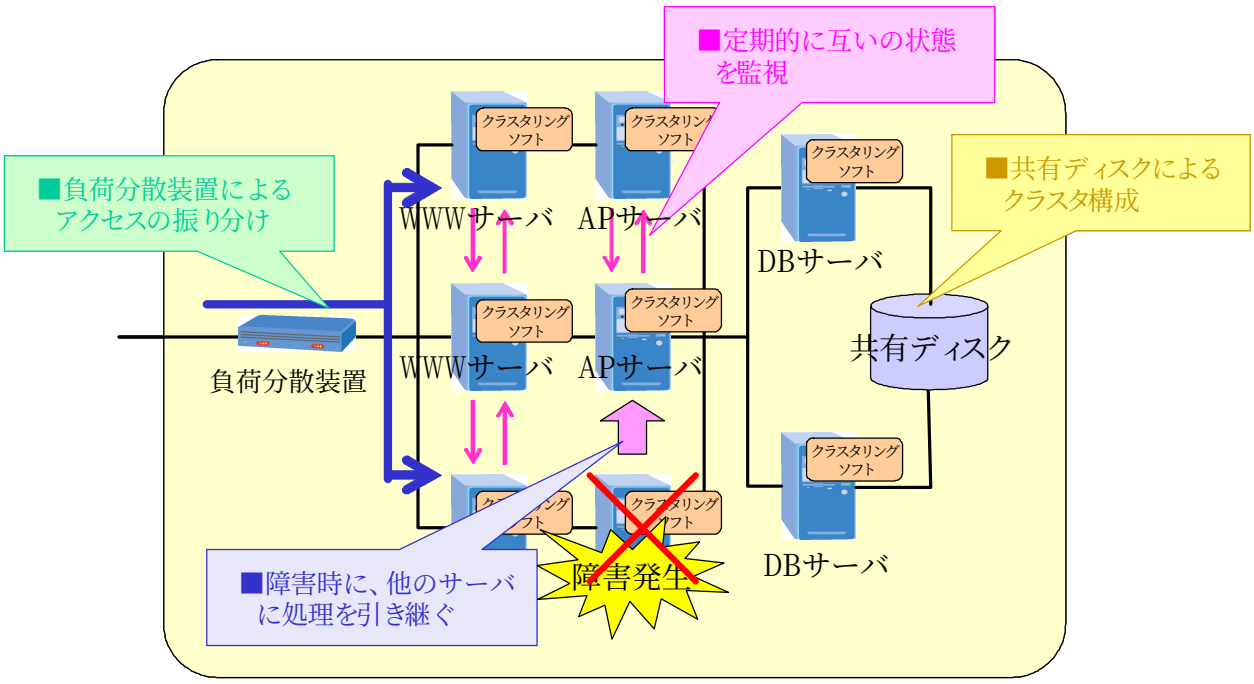


図 7-13　クラスタ構成によるサーバの冗長化

システムの信頼性を向上させるには、ネットワークも冗長化しておくことが望ましい。図 7-14 に示すように、主要なサーバには 2 つのインターフェースを持たせ、ルータやスイッチ類などのネットワーク機器、それに至る経路も含めて冗長構成にしておくことで、ネットワーク障害に対する耐性を高めることができる。

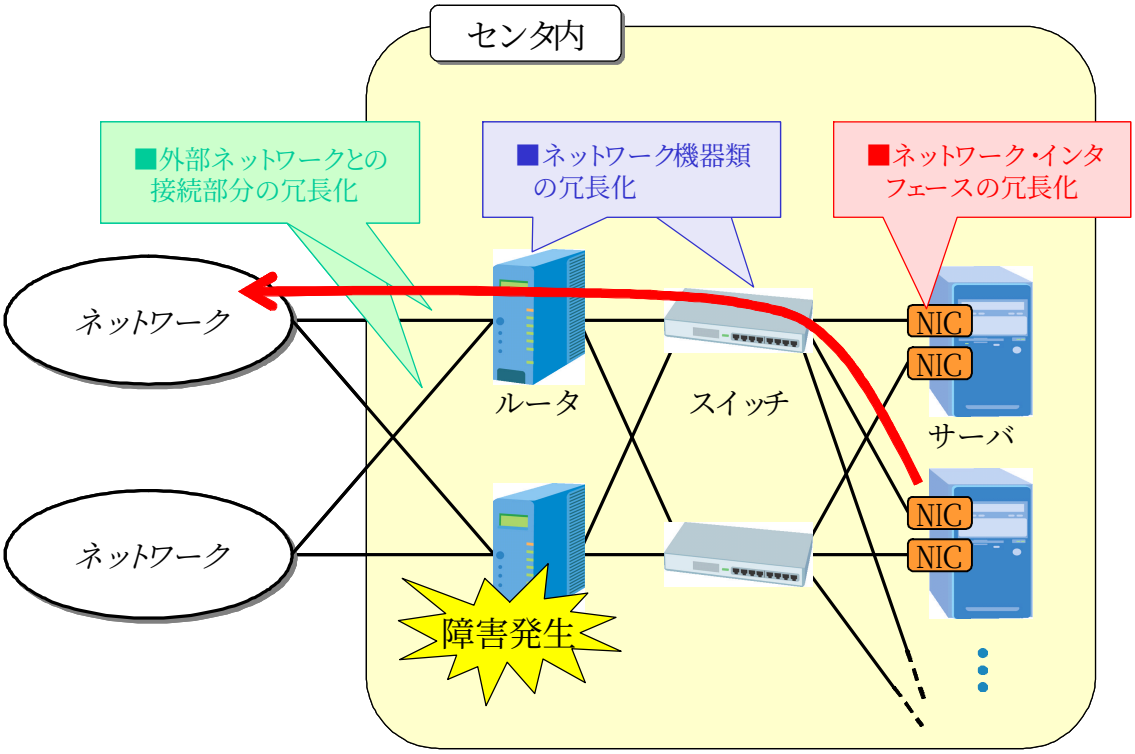


図 7-14　ネットワークの冗長化

（2） 製品動向

クラスタリング・ソフトウェアの製品について、表 7-13 に整理した。

表 7-13　クラスタリング・ソフトウェア

製品名	開発元	用途	対応 OS
CLUSTERPRO 6.0	日本電気株式会社 [9]	WWW, DB	Windows NT/2000, Linux
ClusterServer 2.0	VERITAS Software [10]	DB	Windows NT, Solaris, HP-UX
DNCWARE ClusterPerfect	株式会社東芝 [11]	WWW, DB	Windows NT/2000, Solaris, Linux
MC/ServiceGuard	Hewlett-Packard [12]	DB	HP-UX
Resonate Central Dispatch	Resonate [13]	WWW	Windows NT/2000, Solaris, AIX
SafeCLUSTER	富士通 [14]	DB	Windows NT/2000, Solaris
SunCluster 3.0	Sun Microsystems [15]	DB	Solaris

7．4．2．4 バックアップ

ライセンスリポジトリの信頼化対策として、ライセンスリポジトリに蓄積されるデータの保護も重要な課題である。RAID やミラーリング技術により、ディスクのクラッシ

ュによるデータ消失の可能性はかなり小さくなったが、万が一の場合に備えて、常に最新のデータをバックアップしておく必要がある。

（1） 実現方式

バックアップには、大きく分けて「コールドバックアップ」と「オンラインバックアップ」の 2 つの方式がある。コールドバックアップは、データベースをすべて停止した状態で行うバックアップであり、「オフラインバックアップ」などとも呼ばれるが、ライセンスリポジトリでは、サービスを停止しないことが前提であるので、データのバックアップ／リカバリの作業も、サービスを継続しながら行う必要がある。以下では、オンラインバックアップを対象とする。

(a) ソフトウェアのみによるバックアップ方法

特別なハードウェアを用意せず、ソフトウェアの機能だけで、オンラインバックアップを行う方法であり、最も手軽で安価な方法である。例えば、RDBMS（リレーショナルデータベース管理システム）のオンラインバックアップ機能を用いることで、表領域単位でのオンラインバックアップを行うことができる。ただし、データのバックアップ中は、オンラインの性能は低下してしまう。また、バックアップ中に一時オンラインから切り離した表領域を再びオンラインに戻す際に、それまでに更新されたデータを蓄積されたログをもとに書き戻すため、その処理の間はサーバの負荷が一気に高まることになる。

(b) レプリケーション機能を利用したバックアップ方法

サーバに負荷をかけることなくオンラインバックアップを行うには、本番機とは別にバックアップ機を用意する方法が考えられる。RDBMS のレプリケーション機能を用いて、本番機に対するデータの更新が、自動的にバックアップ機に反映されるようにしておき、バックアップ時には、このバックアップ機のデータを用いるようにする。その際、バックアップ機を切り離してバックアップする方法とバックアップ機を止めずに、オンラインバックアップする方法が考えられる（図 7-15）。

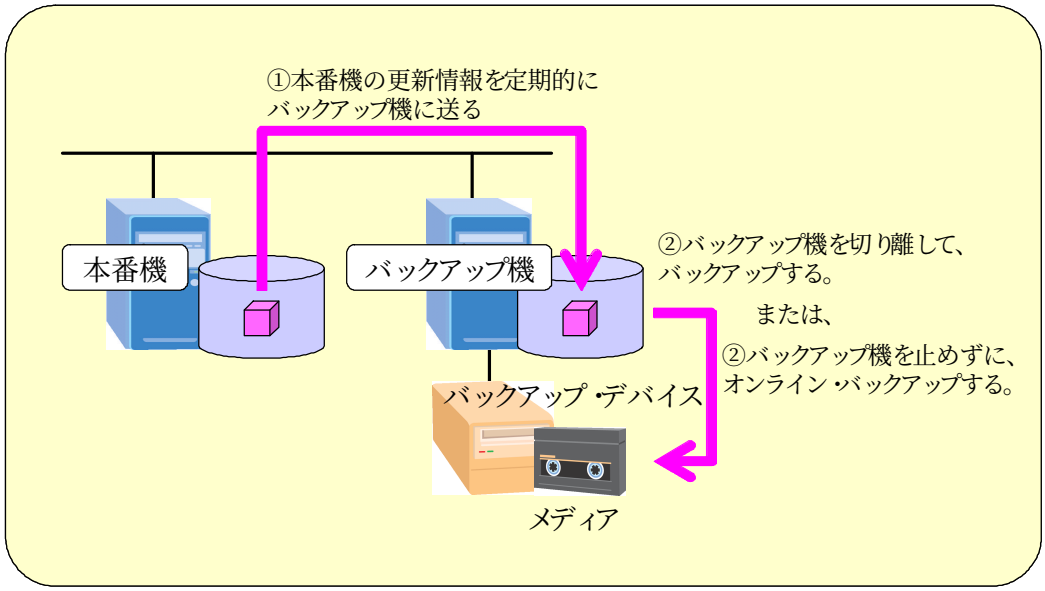


図 7-15　レプリケーション機能を利用したバックアップ

（c）　ディスクのミラーリング技術を利用したバックアップ方法

オンラインバックアップの手段として、ディスクのミラーリング技術を利用した「スプリット・ミラー」と呼ばれる方法がある（図 7-16）。具体的な手順としては、①サーバのマスタディスク上のデータを更新すると、②ディスクの同期化によって、複製ディスク上にまったく同じ内容が反映され、（オンラインバックアップを実施するタイミングにおいて、）③複製ディスクをミラー関係からスプリット（切り離し）し、④この切り離された状態の複製ディスクを利用してバックアップを実行する、というものである。切り離された複製ディスクを再接続すると、切り離されている間に発生したデータの更新が自動的に反映され、データの同期が行われる。

スプリット・ミラーによるオンラインバックアップにより、サービスを継続したまま、データのバックアップを行うことが可能になる。サーバのレプリケーション機能を利用したバックアップ方法と比較すると、ディスク装置やソフトウェアに掛かるコストは高くなるが、リストア時にサーバのパフォーマンスに与える影響もないため、サービスの継続性をさらに強化することができる。

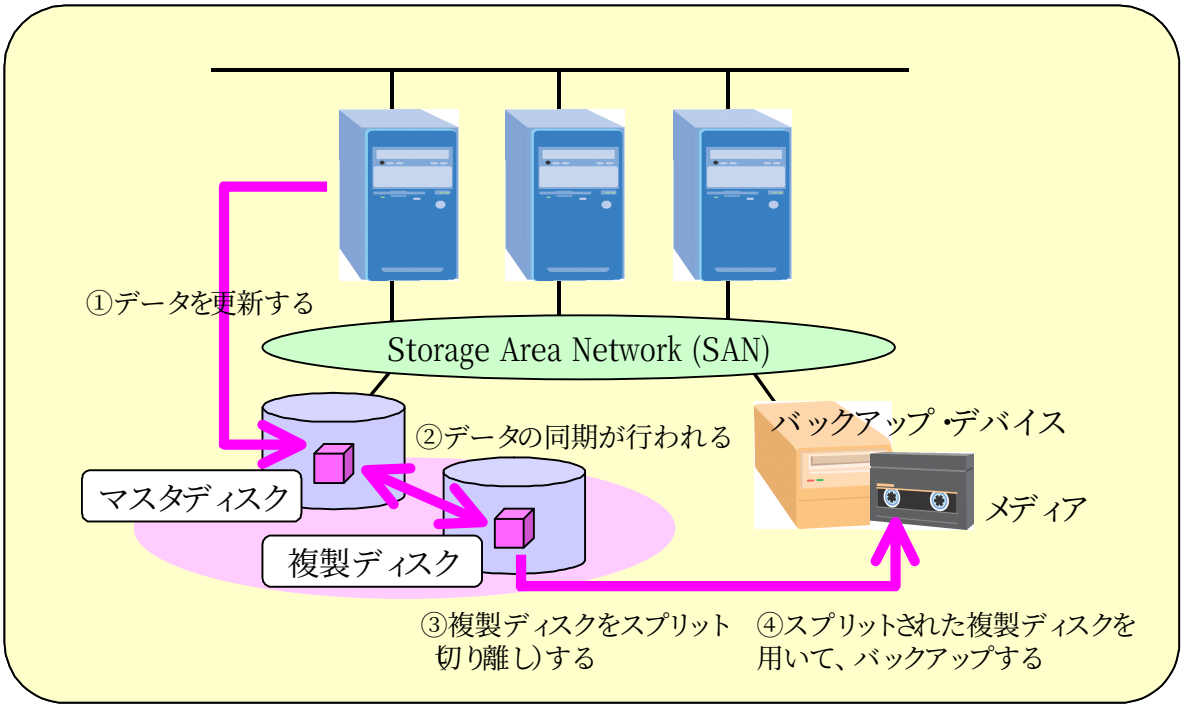


図 7-16　スプリット・ミラーによるオンラインバックアップ

（2） 製品動向

バックアップ・ソフトウェア製品ついて、表 7-14 に整理した。また、スプリット・ミラーの機能を有するソフトウェア製品(ディスク装置に組み込まれた機能として提供されているものを含む）について、表 7-15 に整理した。

表 7-14　バックアップ・ソフトウェア

製品名	開発元	対応 OS
ARCserve 2000, ARCserve 7 for NetWare, ARCserveIT for Linux	Computer Associates [16]	Windows NT/2000, NetWare, Linux
HP OpenView omniback II 4.0 for Windows & unix HP OpenView omniback II 3.51 for Solaris	Hewlett-Packard	Windows NT/2000, HP-UX, Solaris, AIX, Netware
NetVault 6.5	BakBone Software [17]	Windows NT/2000, HP-UX, Solaris, AIX, Netware, Linux, IRIX
Legato Networker 6.1	Legato Systems [18]	Windows NT/2000, HP-UX, Solaris, AIX, Netware, Linux, IRIX
Tivoli Storage Manager 4.1	Tivoli Systems [19]	Windows NT/2000, HP-UX, Solaris, AIX, OS/390
VERITAS NetBackup BusinesServer/DataCenter	VERITAS Software	Windows NT/2000, HP-UX, Solaris, AIX, IRIX

表 7-15　スプリット・ミラー機能を有するソフトウェア

製品名	開発元
ESS FlashCopy	IBM [20]
HMRCF (ShadowImage)	日立製作所 [21]
OPC (One Point Copy)	富士通株式会社
SnapShot	Storage Technology (StorageTek) [22]
SureStore Business Copy XP	Hewlett-Packard
TimeFinder	EMC [23]

７．４．３ 考察

ライセンスリポジトリは、大量のアクセスが集中する参照系のシステムであり、24時間／365 日の運用が要求される。ライセンスリポジトリに対するアクセス数は、利用者（ライセンスリポジトリに接続する機関）の増加や回線のブロードバンド化により、将来に向けて継続的に増加するものと予測される。そのため、ライセンスリポジトリを構築する際の信頼化対策としては、負荷分散装置やクラスタリング技術を利用して、システムの冗長化とスケーラビリティの確保を行う必要がある。

一方で、ライセンスリポジトリに蓄積されるデータの保護も重要であり、サービスの継続性を確保しつつ、常に最新のデータのバックアップを取ることで、データ消失などのリスクに対処する。また、いざ障害が発生した場合のリカバリ手順の確立も、システムの信頼性を高める上で、必要不可欠な要素といえる。

７．４．４ 参考文献

[1] F5 Networks 社ホームページ：http://www.f5networks.co.jp/
[2] Coyote Point Systems 社ホームページ： http://www.coyotepoint.com/
[3] Cisco Systems 社ホームページ：
http://www.cisco.com/japanese/warp/public/3/jp/
[4] Intel 社ホームページ：http://www.intel.co.jp/
[5] Foundry Networks 社ホームページ：http://www.foundry.co.jp/
[6] Extreme Networks 社ホームページ： http://www.extremenetworks.co.jp/
[7] RADWARE 社ホームページ：http://www.radware.com/
[8] Enterasys Networks 社ホームページ：http://www.enterasys.co.jp/
[9] 日本電気株式会社ホームページ：http://www.ace.comp.nec.co.jp/
[10] VERITAS Software 社ホームページ：http://www.veritas.com/jp/
[11] 株式会社東芝ホームページ：http://www.toshiba.co.jp/

[12] Hewlett-Packard 社ホームページ：http://www.jpn.hp.com/
[13] Resonate 社ホームページ：http://www.resonate.com/
[14] 富士通株式会社ホームページ：http://jp.fujitsu.com/
[15] Sun Microsystems 社ホームページ：http://www.sun.co.jp/
[16] Computer Associates 社ホームページ：http://www.caj.co.jp/
[17] BakBone Software 社ホームページ：http://www.bakbone.co.jp/
[18] Legato Systems 社ホームページ：http://www.legatosystems.co.jp/
[19] Tivoli Systems 社ホームページ：http://www.tivolisystems.co.jp/
[20] IBM 社ホームページ：http://www.ibm.com/jp/
[21] 日立製作所ホームページ：http://www.hitachi.co.jp/
[22] Storage Technology 社ホームページ：www.storagetek.co.jp/
[23] EMC 社ホームページ：http://www.emc2.co.jp/

７．５ 添付資料の原本性保証

７．５．１ 調査目的

本節では､ライセンスリポジトリ方式の実現においてライセンスリポジトリで保管している添付資料の原本性を確保するための技術的課題を整理し､ライセンスリポジトリ方式に適した解決の方策を明らかにすることを目的とする。

電子申請において申請手続を成立させるためには､電子化された添付資料において原本性が確保されていることが必要である。つまり、電子文書が紙文書と比べて劣ると思われる特性、「記述内容の改ざん・書き換え・他のものとのすり替えが極めて容易でその痕跡がほとんど残らないこと」「記憶媒体そのものの経年劣化等で内容の消失が起きやすいこと」「事後に改ざん行為を検出することが困難であること」等の各々に対して技術的対策を行わなければならない。

同時に、添付資料の場合はその性格上、「いつの時点で作成されたものか」「いつの時点まで内容が有効か」ということが大変重要な意味を持つ。電子文書の「作成時点」「有効期限」を管理するための技術の検討も必要となるためである。

７．５．２ 調査内容および結果

本調査では、ライセンスリポジトリ内の添付資料管理で想定される脅威を整理し、その脅威を防ぐための技術的課題と解決の方策を検討した。さらに解決の方策に関連する製品動向を調査した。

７．５．２．１ 原本性確保における技術的課題

システムにおける電子文書の原本性確保の対策要件として、「共通課題研究会中間報告」[1]では「完全性」「機密性」「見読性」の確保が必要と記されている。また「高度情報通信社会推進本部制度見直し作業部会報告書」[2]では「真正性」「見読性」「保存性」の確保があげられている。それぞれの報告書では対象とする文書や対策要件に見方の若干の違いはあるものの共通的な内容が多いため、本報告書では「共通課題研究会中間報告」の対策要件で検討することとする。また、「電子署名文書長期保存に関する中間報告」[3]では電子署名が施された電子署名文書の署名有効性を電子証明書の有効期限が過ぎた後も検証可能とする方法が報告されている。

これらの報告書を踏まえ､ライセンスリポジトリで保管管理している添付資料に対する想定脅威、技術的課題と解決の方策について検討した結果を表 7-16 にまとめる。さ

らに解決の方策に関連する技術について次節でその動向を述べる。

表 7-16　原本性確保における技術的課題

想定される脅威	技術的課題	解決策	調査対象
見読性、完全性、機密性の保証	添付資料の原本性を確保する	原本性確保装置等によって添付資料の原本性の確保を行う	原本性確保装置
管理期間中における添付資料（署名も含む）の期限切れ	添付資料に対して長期の原本性を確保する	ライセンスリポジトリセンタにおける登録時刻の保証と原本性確保により、管理期間中に署名の有効期限が切れた添付資料に対してライセンスリポジトリが担保を行う	原本性確保装置 タイムスタンプ
指定した時刻における添付資料の存在証明	添付資料の登録、更新、削除の時刻を保証する仕組みを設ける	添付資料の登録・更新・削除の時刻をタイムスタンプで記録し保存する	タイムスタンプ

７．５．２．２ 原本性確保装置

（１） 原本性確保装置に求められる機能

原本性確保装置とは､ソフトウェアもしくはハードウェアによって電子文書を厳重に保管する機能を有するシステムのことである｡なお電子文書を原本として保管するために必要な機能について､「共通課題研究会中間報告」では表 7-17 のように報告されている。

表 7-17　原本性確保に求められる機能

機能内容	完全性	機密性	見続性
電子文書の保存・管理についての責任及び権限を明確化するため、管理責任者等を定めること	○	○	○
ホストコンピュータ、端末機、通信関係装置、プログラムその他のハードウェア及びソフトウェアの全部又は一部により構成されるものであて、電子文書にアクセスする者を ID, パスワード等によって識別し、認証すること	○	○	―
電子文章を記録した媒体は、保管場所を定め、施錠して保管し、保管場所からの搬出入及び授受は管理記録を整備して行うこと	○	○	―
電子文書保管・管理システムに対するアクセスを監視及び記録すること	○	○	―
電子文書保存・管理システムには、電子文書の内容・性格に応じて、アクセス権限を設定すること	○	○	―
電子文書の保存、参照、更新、複写及びは行きの日時並びに実施者を記録するログを取得し、保存すること。当該ログは、安全な場所及び媒体に一定期間保存すること。	○	○	―
電子文書の更新履歴が確認できること。当該更新履歴は、安全な場所及び媒体に一定期間保存すること	○	―	―
更新前の電子文書についても、必要に応じ一定期間保存すること	○	―	―
電子文書の盗難、漏洩等に備えるとともに、改竄等を防止するため、必要に応じ電子文書を暗号化して保管すること	○	○	―
必要に応じ改竄検出機能を有する電子署名を電子文書に施して保管すること	○	―	―
システムタイマーの設定・変更等の作業履歴が確認できること。当該作業履歴は安全な場所及び媒体に一定期間保存すること	○	―	―
電子文書のバックアップを定期的に行い、当該バックアップを適切に保管すること	○	―	―
電子文書を記録した媒体及びそのバックアップについては定期的に保管状態及びデータの内容が正常であるか否かの点検を行うこと	○	○	―
外部からの入手した電子文書は、ウィルスチェック後に利用すること	○	―	―
電子文書の出力に必要な電子計算機、プログラム、通信関係装置、ディスプレイ、プリンタ等を備え付け、いつでも必要な場合には電子文書をディスプレイの画面に出力することができるようにすること	―	―	○
電子文書保存・管理ｼｽﾃﾑの保守、点検、改造等は計画的に行い、当該行為の期間中における電子文書の保護措置を講ずること。	○	○	―
停電、誤切断等による電子文書の消失、破壊等を防止するため、無停電電源等の必要な措置を講ずること	○	―	―
プログラムのバックアップを行い適切に保存すること	○	―	○

（2） 原本性確保装置の製品動向

国内メーカが開発している主な原本性確保装置製品を表にまとめる。現状では「共通課題研究会中間報告」を意識した製品のほかにも、医療分野での原本性確保装置もいくつか発売されている（表 7-18）。

表 7-18　原本性確保装置　製品一覧

製品名	メーカ	対応ＯＳ	備考
TrustyCabinet	株式会社リコー[4]	WindowsNT/2000 Solaris7,8	原本確保ソフトウェア
原本性保証電子保存装置	オリンパス光学工業株式会社[5]	専用ハード	原本確保装置
eFiling Meister	株式会社東芝[6]	―	CRM ソリューション
ディジタルイメージングシステム	コニカ株式会社[7]	専用ハード	医療画像の運用管理システム
HITLOOKS V3	日立コンピュータ機器株式会社[8]	Windwos98/Me/ NT/2000	電子カルテシステム

（３） 原本性確保装置の製品比較

「共通課題研究会中間報告」の機能要件と、各原本性確保装置製品の機能の対応を表 7-19 に整理する。「共通課題研究会中間報告」の機能要件には製品の機能とは関連の低いものも含まれるため、原本性確保装置ですべての機能を実現することはできない。電子文書の原本性を確保するためには、製品で実現できない機能については運用で補う必要がある。

表 7-19　原本性保証システムのサポート機能

機能	製品				
	Trusty Cabinet	原本性保証電子保存装置	eFiling Meister	ディジタルイメージングシステム	HITLO OKS V3
電子文書の保存・管理についての管理責任者	×	×	×	×	×
電子文書にアクセスする者の識別・認証	○	○	○	○	○
電子文書を記録した媒体の保管及び管理記録	×	×	×	×	×
電子文書保管・管理ｼｽﾃﾑに対するアクセスの監視及び記録	○	○	○	×	×
電子文書保存・管理ｼｽﾃﾑへのアクセス権限を設定	○	○	○	○	○
電子文書の保存、参照、更新、複写及び廃棄の日時並びに実施者を記録するログの取得・保存	○	○	○	○	○
電子文書の更新履歴の確認	○	○	○	×	×
更新前の電子文書の保存	○	○	×	×	×
電子文書を暗号化して保管	×	×	○	×	×
電子署名を電子文書に施して保管	○	○	○	○	○
システムタイマーの設定・変更等の作業履歴の確認	○	○	×	×	×
電子文書のバックアップ	○	×	×	×	×
電子文書を記録した媒体及びそのバックアップについては定期的に保管状態及びデータの内容が正常であるか否かの点検	×	×	×	××	×
外部からの入手した電子文書のウィルスチェック	×	×	×	×	×
電子文書の出力	×	×	×	×	×
電子文書保存・管理ｼｽﾃﾑの保守、点検、改造等は計画的に行い、当該行為の期間中における電子文書の保護措置を講ずること。	×	×	×	×	×
無停電電源等の措置	×	×	×	×	×
プログラムのバックアップ	×	×	×	×	×

７．５．２．３ タイムスタンプ

（１） サービス動向

電子署名が施された電子文書の署名有効性を、電子証明書の有効期限が過ぎた後も検証可能とするため、ある時刻における電子文書の存在や有効性を保証する仕組みが必要である。仕組みとして技術的なタイムスタンプと制度的な公証人による確定日付の付与がある。なお、電子公証制度については「公証制度に基礎を置く電子公証制度」[9]が定められ 2002 年 1 月より日本公証人連合会によりサービス提供が開始されている（表 7-20）。

表 7-20　タイムスタンプ・電子公証サービス一覧

サービス名	運営団体	価格	備考
SecureSeal	株式会社 NTT データ[10]	240,000 円/2000 件・月―	電子化された情報の非改ざんと存在時刻を証明
電子公証業務サービス	日本公証人連合会[11]	700 円/件（電子確定日付の付与）	「公証制度に基礎を置く電子公証制度」に基づく電子公証サービス
ベリサイン電子公証サービス	日本ベリサイン[12]	電子認証サービス「VeriSign OnSite」の追加機能	―
dPROVE	日本電子公証機構[13]	240 円/件	―

（２） 実現方式

ここでは、タイプスタンプ（SecureSeal）と電子公証サービスの概要について説明する。

（a） SecureSeal の概要

利用者は証明したい電子文書のハッシュ値(電子文書から一方向ハッシュ関数を用いて作成した電子文書のダイジェスト）を NTT データの証明サーバに送信することにより、証明記録が利用者に送り返される。証明記録には証明したい電子文書の正当性を実証するのに必要な情報が含まれており、利用者はオリジナルの電子文書と、取得した証明記録を保管する。
利用者が事前に証明記録を取得した電子文書の正当性を証明する際には、以下の手続きが行われる。

・利用者側で正当性を証明したい電子文書のハッシュ値を生成し、証明記録内のハッシュ値と照合する。
・照合により問題がなければ証明記録が実証サーバに送信される。
・実証サーバでは送られた証明記録内の情報と、NTT データで管理するスーパーハッシュ値との関係から、客観的に電子文書の正当性を証明することができる。

ハッシュ値（図 7-17）は、電子文書の代役となる情報であり、ハッシュ値から元の電子文書を生成する事が不可能であり、また同じハッシュ値を持つ別の電子文書を見つけ出すのが難しい（異なる２つの電子文書のハッシュ値が一致する確立は 10 の 87 乗分の 1）という特徴を持つ。

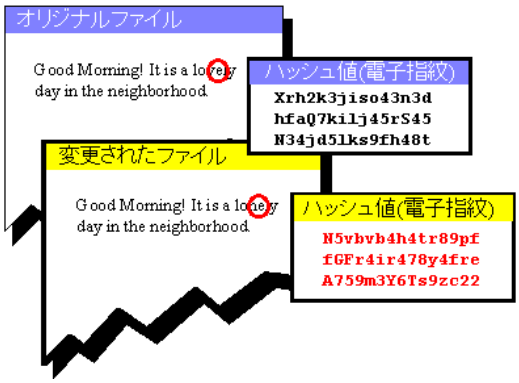


図 7-17　ハッシュ値の例

利用者から電子文書のハッシュ値を受け取る証明サーバでは、ある単位時間内に受信した全てのハッシュ値から二分木を構成し、隣り合う二つのハッシュ値を合わせて新たなハッシュ値を計算し、これを再帰的にルート要素まで計算することにより、ルートハッシュ値（以後、RHV と呼ぶ）を生成する。つまり、RHV は同時刻に受信したハッシュ値の代表としてある時刻に１つだけ生成される（図 7-18）。

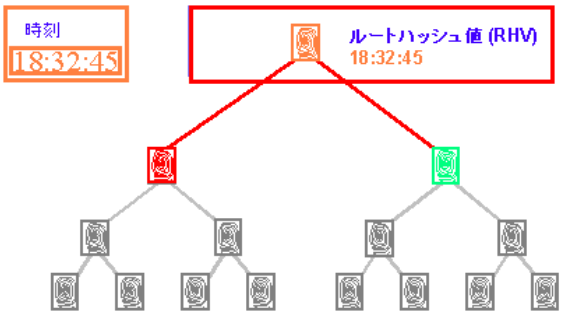


図 7-18　ルートハッシュ値の生成

また、ある時刻に対するスーパーハッシュ値（以後、SHV と呼ぶ）は、同時刻に生成された RHV と前の時刻に生成された SHV とを合わせて新たなハッシュ値を計算したものである（図 7-19）。一週間に一度、その週の全ての SHV から二分木を構成して、RHV の生成と同様な方法により週の代表となる SHV を生成し、これを広く情報公開する。

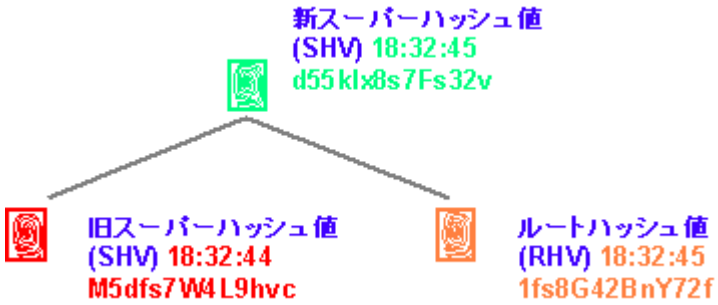


図 7-19　スーパーハッシュ値の生成

このような証明方法を採用しているため、電子文書証明サービスを利用する利点は以下の通りである。

- 利用者からは証明したい電子文書を送る必要がないため、電子文書自体を送信する方式と比較して通信にかかる負担が少なく、また利用者のプライバシーが守られる。
- 利用者と無関係な別の利用者からのハッシュ値も組み合わせて SHV を生成するため、電子文書の正当性を客観的に証明することができる。
- 週の代表となる SHV を公開するため、当サービスの運営母体である NTT データが後日ハッシュ値の改竄を行う恐れがない。

ただし、以下の点について留意する必要がある。

- オリジナルの電子文書と証明記録は利用者側で保管する必要がある。
- 電子文書の改竄行為そのものを防ぐことはできない（利用者が改竄した電子文書を流通させることが可能である）。

（b） 電子公証サービスの概要

電子公証は、信頼される第三者が電子文書（電子ファイル）の作成者や作成日時を証明するサービスである。電子公証が提供する主なサービスは「電子文書の認証サービス」「電子確定日付サービス」「電子文書の保管および証明サービス」がある。

・電子文書の認証サービス

電子文書の認証を希望するユーザ（嘱託人）は、ユーザの電子署名が付された電子文書を公証人に送信する。公証人は、送信されてきた電子文書に付された電子署名を検証し、関係主体の存在及び意思の確認を行うとともに、違法性の有無を審査する。その後、公証人は、認証文及び日付を付記して公証人本人の電子署名を付しユーザに送信し、同時に認証した電子文書のデータをファイルに保管する。

・電子確定日付の付与サービス

公証人は、ユーザから送信された電子文書に確定日付を付与した上で、ユーザに送信する。なお、電子署名が付与されていない電子文書や画像データ等にも確定日付を付与することが可能である。

・電子文書の保管及び証明サービス

公証人が認証した電子文書、電子確定日付を付与した電子文書等のデータを保管し、後日、各種文書の存在と内容について公証人が証明する。

また、これらサービスを実現するために、「電子公証システムガイドライン」（平成 10 年 5 月、電子商取引推進協議会）において機能要件（送受信者特定機能、到達確認機能、改竄検知機能、時刻付与機能、アクセス記録機能、プロセス記録機能、電子保存機能）が示されている。

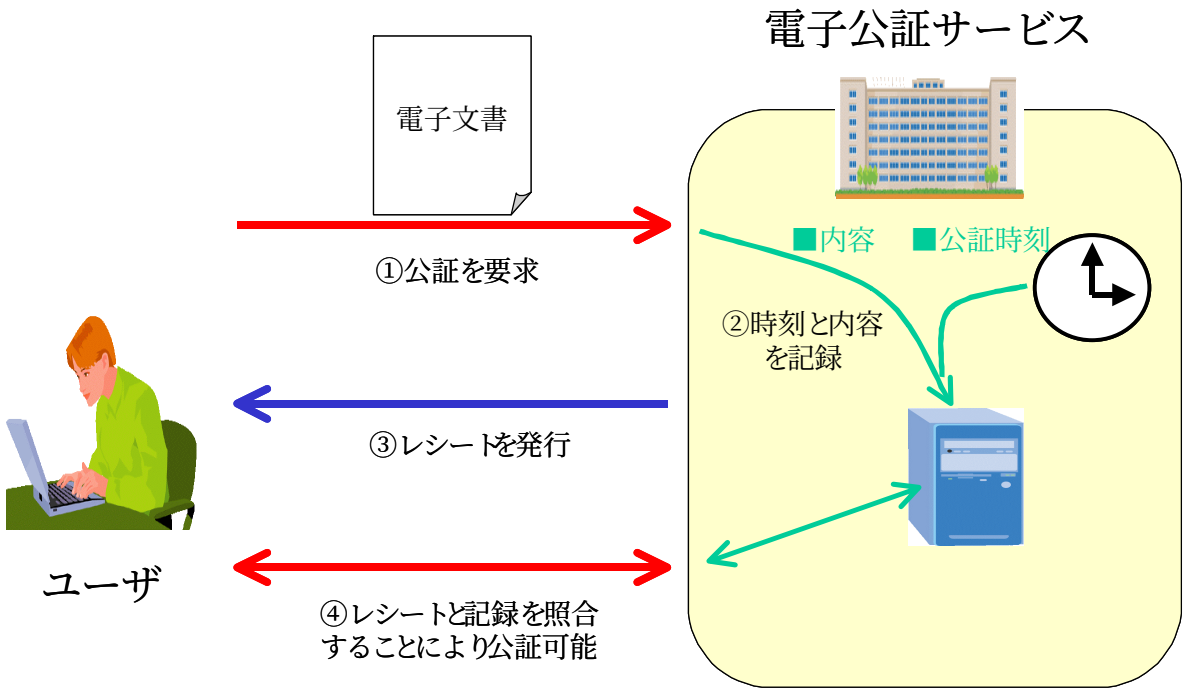


図 7-20　電子公証サービスの概念図

７．５．３ 考察

「共通課題研究会中間報告」で報告されている原本性の要件を満たすためには、既存の製品導入やサービス利用などの手段だけでなく、運用による対応や人材育成などの手段も必要である。つまりライセンスリポジトリにおける原本性を確保するとなると、システム構築だけでなく、システムの運営管理の体制を整える必要がある。そのため。中小規模のライセンスリポジトリにおいては十分な対応は困難であると推測する。

そこで、ライセンスリポジトリの形態や運用、添付資料の特性を検討するなかで、各モデルにおいてのライセンスリポジトリに求められる原本性の要件を整理する必要がある。ライセンスリポジトリ実現の際には、効果的な既存の製品やサービスの導入を検討することが重要である。

７．５．４ 参考文献

[1]「共通課題研究会中間報告」（平成 11 月 4 月、総務庁）：
http://www.soumu.go.jp/gyoukan/kanri/honbun.pdf
[2]「高度情報通信社会推進本部制度見直し作業部会報告書」（平成 8 年 6 月）：

http://www.lasdec.nippon-net.ne.jp/its/03/0806201.pdf
[3]「電子署名文書長期保存に関する中間報告」（平成 13 年 3 月、電子商取引推進協議会）：http://www.ecom.or.jp/report/h12seika/certification_wg/cert_wg3.pdf
[4] 株式会社リコーホームページ：http://www.ricoh.co.jp/tcab/
[5] オリンパス光学工業株式会社ホームページ：http://www.olympus.co.jp/
[6] 株式会社東芝ホームページ：http://www.toshiba.co.jp/index_j3.htm
[7] コニカ株式会社ホームページ：http://www.konica.co.jp/mi/index.html
[8] 日立コンピュータ機器株式会社ホームページ：
http://www.hitachi-cp.co.jp/product/iryou/hlookg/index.html
[9]「公証制度に基礎を置く電子公証制度」について（法務省）
http://www.moj.go.jp/
[10] 株式会社 NTT データホームページ：
http://www.nttdata.co.jp/services/s090054.html
[11] 株式会社日本電子公証機構ホームページ：http://www.jnotary.com/
[12] 日本ベリサインホームページ：http://www.verisign.co.jp/
[13] 日本電子公証機構ホームページ：http://www.jnotary.com/
[14] 「電子公証システムガイドライン」（平成１０年５月、電子商取引推進協議会）
http://www.ecom.jp/qecom/about_wg/wg15/press/h9-guideline-summary.htm

７．６ ライセンスリポジトリ方式における添付資料の管理方法

７．６．１ 調査目的

本節では、ライセンスリポジトリの運用における添付資料管理の機能要件を整理し、技術的課題および解決の方策を明らかにすることを目的とする。

ライセンスリポジトリ方式においては、添付資料情報を持つデータベースへ申請手続を所管する行政機関等が閲覧することになる。この場合重要なのが、申請者の許可を取った上ではじめてアクセス権が得られること、そしてそれ以外の理由では、何人も（行政機関であったとしても）添付資料情報へのアクセスを不可能にすることである。

また必要に応じて、添付資料の特徴によってはアクセス制御だけではなく、閲覧者の不正利用による添付資料情報を保護するために、添付資料情報の公開内容の自動制御や、閲覧者による添付資料情報の利用制御を行うことが必要である。

７．６．２ 調査及び検討内容

ライセンスリポジトリセンタにおける添付資料管理の機能要件を整理する。さらに機能を実現するための技術的課題を検討し、それぞれの課題について解決の方策を検討する。なお、解決方策に関して製品があるものは調査を行った。

７．６．２．１ 添付資料管理における機能要件

ライセンスリポジトリセンタにおける添付資料管理における機能要件として、7.3 節外部攻撃からのセキュリティ確保、7.4 節システムの信頼性、および 7.5 節添付資料の原本性保証は、必須の要件である。しかし、本節ではこれら以外の要件について、添付資料の情報管理という観点で機能要件を整理する。

ライセンスリポジトリセンタは、アクセス者の属性に応じて管理している添付資料へのアクセス制御を行い、添付資料を閲覧する者を管理する必要がある。また将来的には、正当なアクセス者からの情報漏洩を防止するために、閲覧者に対して過剰の情報公開を行うことはせず、必要最低限な公開にとどめておくことも重要である。

従って、以下の 2 つの機能要件が挙げられる。

（1） アクセス者の属性に応じた添付資料へのアクセスが管理できること
（2） 添付資料情報を保護できること

7．6．2．2 添付資料管理における技術的課題

ライセンスリポジトリセンタでの添付資料管理の機能要件に対する、技術的課題と解決の方向性を以下にまとめる（表 7-21）。

表 7-21　添付資料管理における技術的課題

機能要件	技術的課題	解決の方向性
添付資料へのアクセス管理	ライセンスリポジトリへアクセスする際に、アクセス者の属性認証を行う。	アクセス者が予め自分の属性をライセンスリポジトリに登録する
		公開鍵証明書などによりアクセス者の属性を認証する。
	アクセス者の属性に応じて、添付資料へのアクセスを制御する。	文書管理システムを利用する
添付資料情報の保護	添付資料情報の一部を隠蔽する。	添付資料内の隠蔽する必要がある部分を伏字にする
		公開できる情報の部分を抽出する。
	添付資料情報の利用を制御する。	添付資料情報に利用制御情報を埋め込む。

7．6．2．3 ライセンスリポジトリにおける属性認証モデル

ライセンスリポジトリセンタでは、管理している添付資料へアクセスする者に対して、添付資料の公開可否の判定を行うために、アクセス者の属性を認証する仕組みが必要である。本報告では、属性認証を行うモデルとして、(1)ID／パスワードモデル、(2)電子証明書を利用したモデルを解決方策として提案する。

（1） ID／パスワードモデル

ID／パスワードモデルは、アクセス者が事前にライセンスリポジトリセンタに登録を行いアクセスのための ID とパスワードを取得し、アクセス者がライセンスリポジトリへ添付資料の閲覧をする際にはその ID とパスワードも用いて、認証を行うモデルである。

このモデルの場合、ライセンスリポジトリでは、ライセンスリポジトリへのアクセス認証の際に ID／パスワードを用いることにより、本人認証と属性認証を効率的に行うことができる。また、添付資料へのアクセス権をライセンスリポジトリ毎に自由に決定することが可能であることから、様々な添付資料特性に応じた対応が可能と考えられる（表 7-21）。ただし、このモデルでは、以下の点について気をつける必要がある。

- アクセス者はライセンスリポジトリ毎に事前に登録をする必要がある。
- アクセス者は自らの ID／パスワードを管理する必要がある。
- ライセンスリポジトリでは、ユーザ管理とアクセス権管理を行う必要がある。

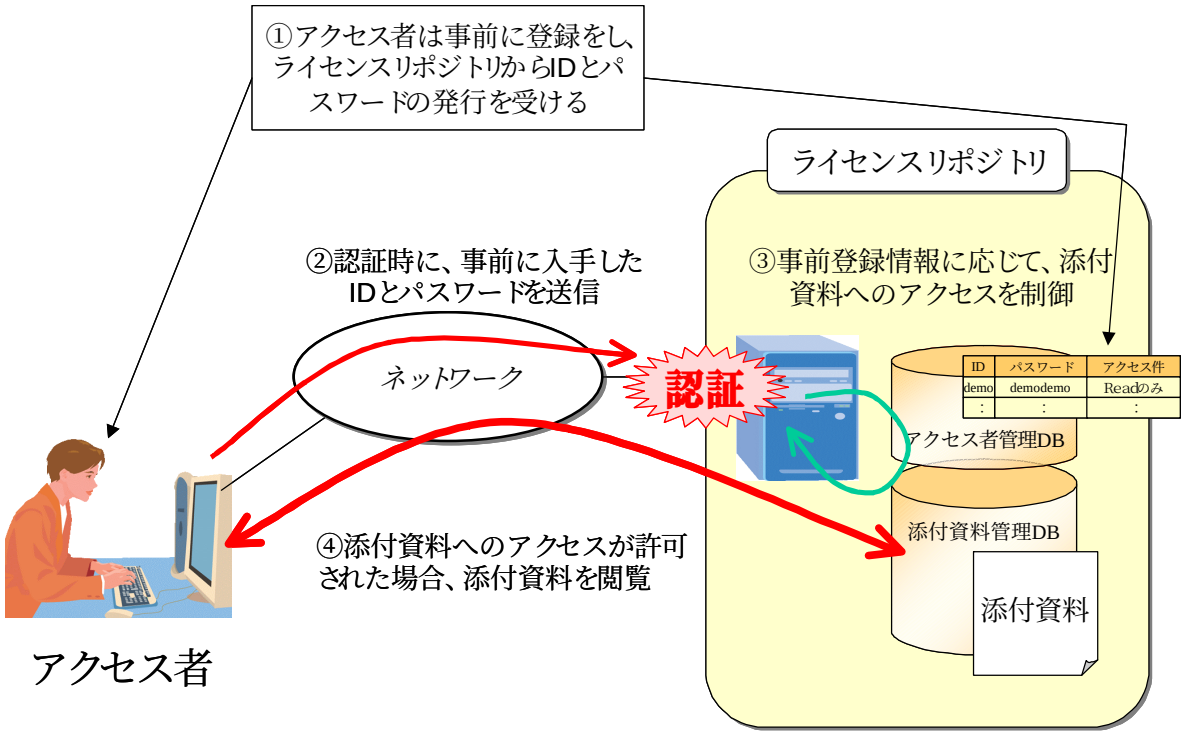


図 7-21　ID/パスワードによるアクセス者の属性認証

（2） 電子証明書を利用したモデル

電子証明書を利用したモデルは、アクセス者は事前に電子証明書を取得し、アクセス時にその証明書によってアクセス者の本人性もしくは属性を認証するモデルである。

このモデルでは、必ずしもライセンスリポジトリ毎にユーザ管理を行う必要がなく、電子証明書の情報でアクセス管理することが可能である。しかし、ライセンスリポジト

リの運用において認証方式やアクセスログによっては、ライセンスリポジトリ内でユーザ管理を行うデータベースを持つ必要があり、この場合は ID／パスワードモデルの仕組みを同時に持つこととなる（表 7-22）。なおこのモデルでは、以下の点について気をつける必要がある。

- アクセス者は事前に証明書を取得する必要がある。
- アクセス者は認証時に証明書付き署名データをライセンスリポジトリに送信する必要がある。
- ライセンスリポジトリでは、アクセス者の認証の度に証明書の有効性を確認する必要がある。
- ライセンスリポジトリでは、アクセス権管理を行う必要がある。

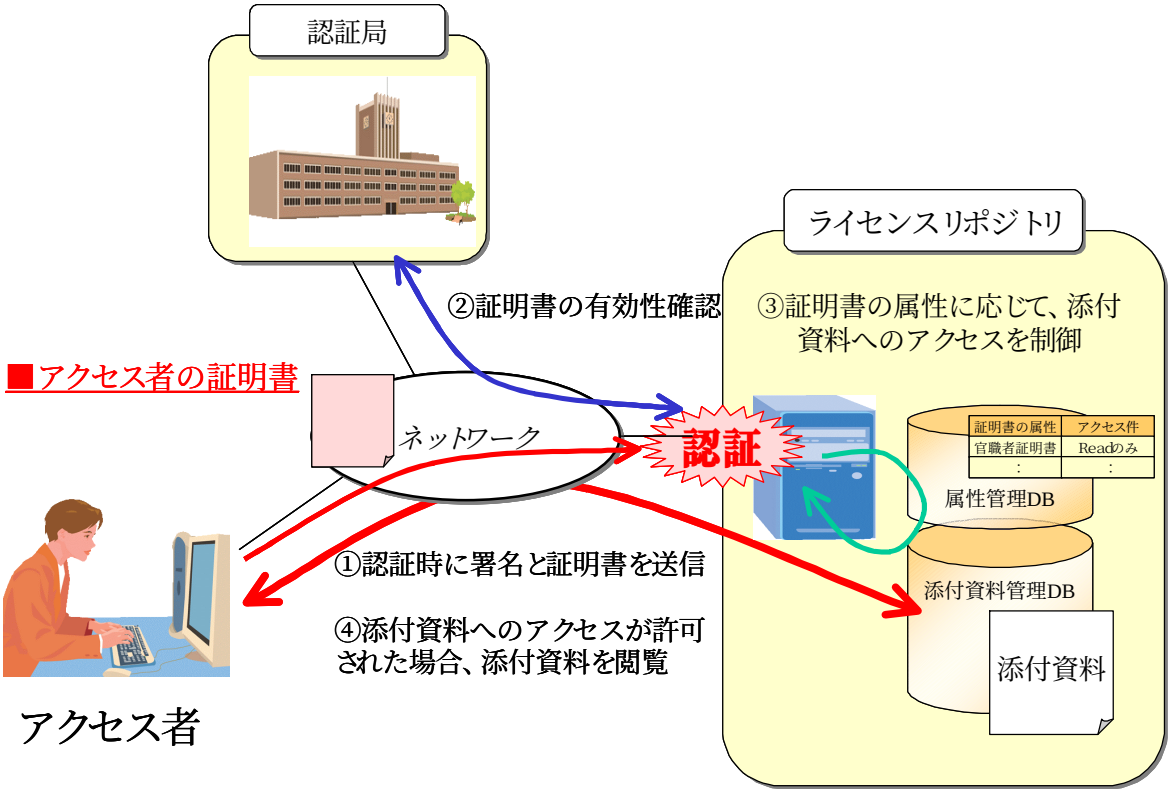


図 7-22　証明書を利用したアクセス者の属性認証

７．６．２．４ 添付資料へのアクセス制御の方法

ライセンスリポジトリ方式では､アクセス者の認証によって取得したアクセス者の属性情報によって、添付資料へのアクセスを制御する仕組みが必要である。本報告では、ライセンスリポジトリ内における添付資料管理の機能要件を整理し､既存の文書管理システムアプリケーションを調査する。

（1） 添付資料管理の機能要件

ライセンスリポジトリにおける添付資料管理で必要となる機能要件は以下のとおりである。ここでは、アクセス制御の観点の他にも、添付資料を管理する上で必要となる機能も一緒に整理している。

- アクセス権設定機能
  アクセス者の属性に応じた添付資料へのアクセス権を設定することができること。
- バージョン管理機能
  添付資料のバージョンを管理することにより、常に最新バージョンを公開することできること。また必要に応じて過去のバージョンを指定して閲覧することが可能であること。
- 履歴管理機能
  添付資料の変更履歴を記録できること。
- 文書ファイル管理機能
  様々な形式の文書ファイルが保存管理できること
- イメージファイル管理機能
  様々な形式のイメージファイルが保存管理できること

（2）　文書管理システム製品動向

ここでは、代表的な文書管理システムアプリケーションをまとめる。なおライセンスリポジトリはネットワークを介した公開を想定しているため、Web 対応の文書管理システムアプリケーションのみを対象とした（表 7-22）。

表 7-22　文書管理システムアプリケーション　製品一覧

製品名	開発元	対応ＯＳ	価格
Livelink8	OPENTEXT[1]	WindowsNT,Solaris, HP-UX（サーバ） Windows95/98/NT, MacOS,Solaris, HP-UX(クライアント)	5,250,000 円（25 ユーザ）―
Documentum 4i eBusiness Platform	Documentum[2]	WindowsNT/2000,Solaris	6,300,000 円―
Ridoc Document System	株式会社リコー[3]	WindowsNT/2000	980,000 円―
DOCS Open/Fusion	hummingbird[4]	WIndowsNT/2000	831,000 円―

（3）　各製品の機能比較

ライセンスリポジトリの文書管理機能要件と各文書管理システムアプリケーションとの関係を表 7-23 にまとめる。

表 7-23　文書管理システムアプリケーションの機能比較

機能要件 / 製品名	アクセス権設定機能	バージョン管理機能	履歴管理機能	文書ファイル管理機能	イメージファイル管理機能
Livelink8	○	○	×	○	○
Documentum 4i eBusiness Platform	○	○	×	○	○
Ridoc Document System	○	○	×	○	○
DOCS Open/Fusion	○	○	○	○	○

７．６．２．５ 添付資料情報の一部を隠蔽する方法

ライセンスリポジトリ方式のモデルや添付資料の特性を検討していく上で、将来的に

ライセンスリポジトリの機能要件として、アクセス者やアクセス者の属性に応じて添付資料情報の一部を隠蔽もしくは抽出して公開する機能が求められる可能性がある。そこで本報告では、(1)添付資料の一部を隠蔽する方式、(2)添付資料の一部を抽出する方式について、解決方策の方向性について検討する。

（1）　添付資料の一部を隠蔽する方式

方式の概念図を以下に示す。添付資料にメタ情報として隠蔽する情報を付加しておき、アクセス者へ添付情報を公開する際に、アクセス者の属性とメタ情報を照合することにより添付資料情報の一部を隠蔽する。

なお、この方式を実現するためには以下の点を行う必要がある。

- 添付資料に隠蔽情報をメタ情報として埋め込むことが必要である
- サーバで、メタ情報とアクセス者の属性情報をもとに情報隠蔽の自動処理を行う必要がある

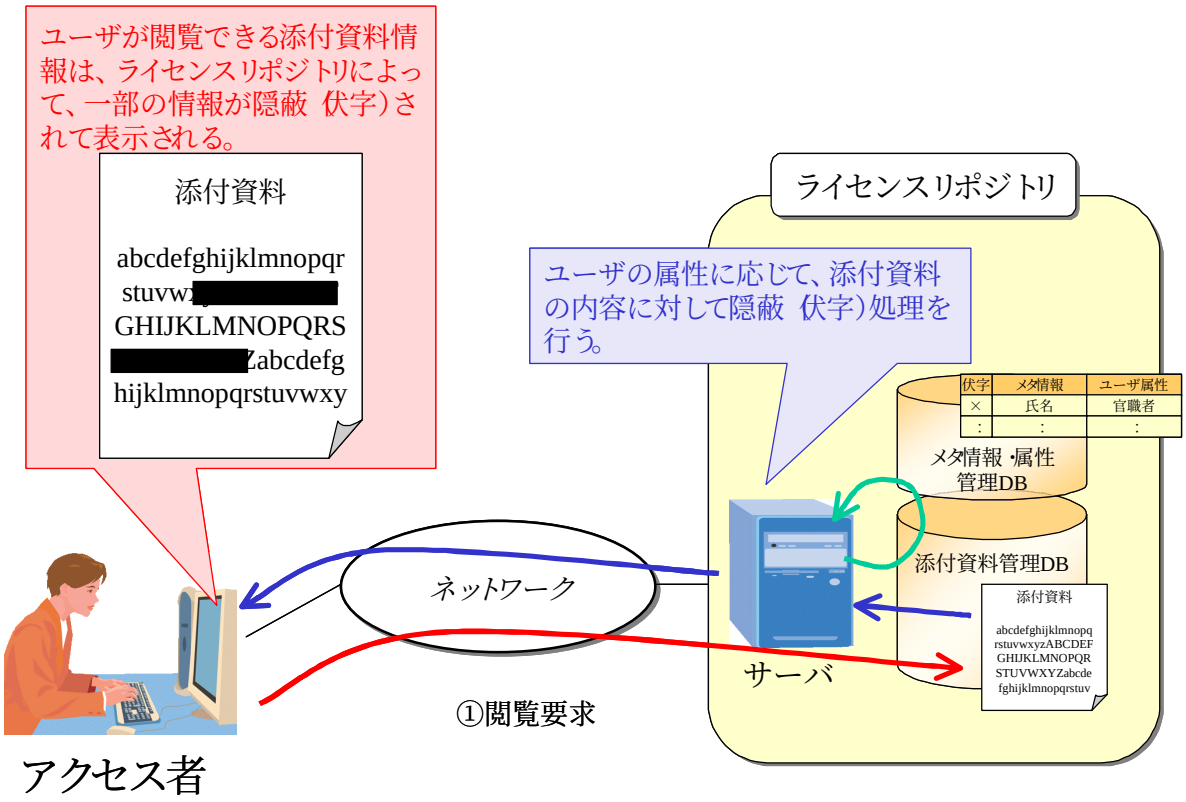


図 7-23　ID/パスワードによるアクセス者の属性認証

（２）　添付資料の一部を隠蔽する方式

方式の概念図を以下に示す。添付資料にメタ情報を付加しておき、アクセス者へ添付情報を公開する際に、アクセス者の属性とメタ情報を照合することにより添付資料情報の一部を抽出する。

なお、この方式を実現するためには以下の点を行う必要がある。

- 添付資料に隠蔽情報をメタ情報として埋め込むことが必要である
- サーバで、メタ情報とアクセス者の属性情報をもとに情報の自動抽出処理を行う必要がある

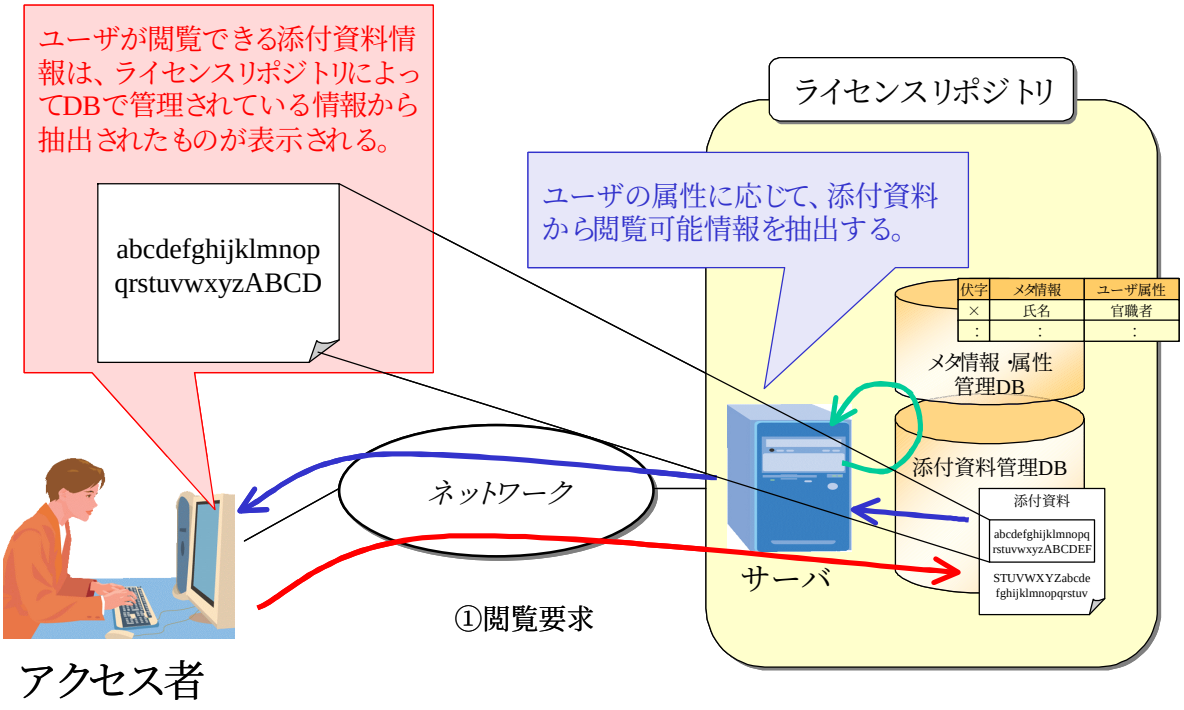


図 7-24　ID/パスワードによるアクセス者の属性認証

７．６．２．６ 添付資料情報の利用制御方法

ライセンスリポジトリで管理している添付資料情報は、アクセス者によるネットワークを介したアクセスにより、ライセンスリポジトリからアクセス者へその内容情報が送信される。たとえ添付資料情報を取得できる者が、認証などにより正当なアクセス者と確認できたとしても、アクセス者へ送信された添付資料情報の利用制御までは不可能である。

そこで本報告では、ライセンスリポジトリから流通する添付資料情報に要求する利用制御機能を検討し、既存の関連製品の調査を行う。

（１） 添付資料情報の利用制御機能

ライセンスリポジトリのモデルや運用さらに添付資料の特性によって、添付資料情報の利用制御の必要性や必要機能は異なることが考えられる。ここでは、ライセンスリポジトリ方式の検討をもとに、添付資料情報の利用制御に必要と考えられる機能を以下にまとめる。

- 閲覧可否の設定
  ダウンロードしたファイル内容を閲覧するための制御情報（認証など）を設定できること。
- 有効期間の設定
  ダウンロードしたファイルの有効期間を設定することができること
- 利用回数（複製作成回数）の設定
  ダウンロードしたファイルの複製を作成する回数を設定できること
- 印刷可否の設定
  ダウンロードしたファイルの印刷に関して利用制御（印刷をできなくする、印刷のためのパスワードを設定するなど）を設定できること
- 編集可否の設定
  ダウンロードしたファイルの内容の編集に関して利用制御（編集を不可能にする、編集のためのパスワードを設定するなど）を設定できること

（２） 利用制御に関する関連製品動向

ここでは、添付資料情報の利用制御に関する関連製品をまとめる。表に示す主な製品群の多くは DRM（Digital Rights Management：デジタル著作権管理）技術の製品や

システムである（表 7-24）。

表 7-24　利用制御に関する関連製品　製品一覧

製品名	発売元	対応ＯＳ	対象ファイル
Content Server	Adobe[5]	Windows95/98/ 、Me/NT4.0/2000/XP	PDF のみ
Access Ticket System	株式会社アクセスチケットシステムズ[6]	Windows95/98/NT4.0/2000	ファイル全般
DIGICAPSULE	三菱電機株式会社[7]	Windows 95/98/NT	ファイル全般
PageRecall	Authentica[8]	WindowsNT/2000,Solaris	MicroSoft Office のファイル PDF
RIGHTS｜PDF	Intertrust[9]	Windows 95/98/Me/ NT/2000	PDF のみ

（3）　各製品の機能比較

利用制御機能と関連製品の関係を表 7-25 にまとめる。実際に利用制御機能の実現を検討する際には、添付資料情報ファイルや、ライセンスリポジトリの運用を考慮した機能検討や製品選定の検討が必要である。

表 7-25　利用制御に関する製品の機能比較

製品名	閲覧	有効期間	利用回数（複製作成回数）	印刷可否	編集可否
Content Server	○	○	×	○	×
Access Ticket System	○	○	○	×	×
DIGICAPSULE	○	○	○	○	×
PageRecall	○	×	×	○	×
RIGHTS｜PDF	○	×	×	○	×

７．６．３ 結論

ライセンスリポジトリ上での添付資料管理が、アクセス者に応じた添付資料へのアクセス制御をするのみであれば、多くの技術的課題は Web 技術と認証技術で解決することができる。しかし、ライセンスリポジトリの形態や目的、添付資料の特性によって、ライセンスリポジトリに添付資料の変更履歴や版管理などの文書管理機能を必要となると、文書管理技術の導入が必要となる。その場合、既存の文書管理システムアプリケーションの活用が効率的である。

添付資料の保護に関しては、添付資料をアクセス者の属性に応じて加工などを施すた

め、添付資料の見え方がアクセス者によって異なることとなる。そのため、添付資料の原本性に関わる法制度的な解釈のもと検討が必要である。また技術的には未熟な分野であり、早期な実現は不可能と考える。

７．６．４ 参考文献

[1] OPENTEXT 社ホームページ：http://www.opentext.com/
[2] Documentum 社ホームページ：http://www.documentum.com/
[3] 株式会社リコーホームページ：http://www.ricoh.co.jp/
[4] hummingbird 社ホームページ：http://www.hummingbird.com/
[5] adobe 社ホームページ：http://www.adobe.com/main.html
[6] 株式会社アクセスチケットシステムズホームページ：
http://www.accessticket.com/index.html
[7] 三菱電機株式会社：http://www.melco.co.jp/index.html
[8] Authentica 社ホームページ：http://www.authentica.com/
[9] Intertrust 社ホームページ：http://www.intertrust.com/

７．７ ライセンスリポジトリ方式における手数料の納付方法

７．７．１ 調査目的

本節では、ライセンスリポジトリの運用における電子的な決済手段を実現する仕組みを検討し、運用に適した方策を明らかにすることを目的とする。

添付資料の中には発行にあたって手数料等が必要なものが数多く含まれており、ライセンスリポジトリ方式実現時にも、これら手数料を何らかの形で徴収することが必要である。

ライセンスリポジトリ方式による納付は、通常の決済に求められるセキュリティなどの要件に加え、価格体系等についての検討が必要となる。

現状では申請書に添付するために住民票を取得する場合を例にとると、「一枚いくら」という価格体系になっており、申請回数に応じて手数料が必要になっていた（従量制）。一方、添付資料を電子化した場合、何度利用しても物理的には消滅しないため、「（何回使っても）何ヶ月でいくら」という価格体系を取る方が自然であるという考え方もある（定額制：事実、法務省の「商業登記制度に基礎をおく電子認証制度」においては定額制を採用している）。

全ての添付資料を「従量制・定額制」のどちらかに統一することは困難だと思われるため、ライセンスリポジトリ方式においては、双方ともに可能とする技術の検討が必要となる。

７．７．２ 調査および検討内容

ライセンスリポジトリ方式における決済の要件を整理する。電子的な決済手段において要件を満たすモデルを調査、検討を行う。

７．７．２．１ ライセンスリポジトリにおける決済要件

ライセンスリポジトリ方式の実現にあたり、決済におけるシステム要件は以下の２つが挙げられる。

（１） 証明書を閲覧するにあたって、納付済みであることが担保されること

手数料の取り逃しが発生しないよう、証明書等を閲覧するにあたって、事前に納付されていることが確認できる仕組みが必要となる。

（２） 従量制、定額制が実現できること

申請手続の特性に応じて、「従量制」、「定額制」のどちらの手段も実現可能であることが求められる。

７．７．２．２ 決済実現モデル

7.7.2.1 節に記載した要件を満たす実現モデルについて、以下に検討結果を記す。

（１） 証明書を閲覧するにあたって、納付済みであることが担保されること

発行機関に対する証明書発行に係る手数料等の取り逃しは、行政機関が発行機関に対して証明書の照会を行うことで、防ぐことができる。

以下に納付済みの場合の照会結果（図 7-25）と未納付の場合の照会結果（図 7-26）を記す。

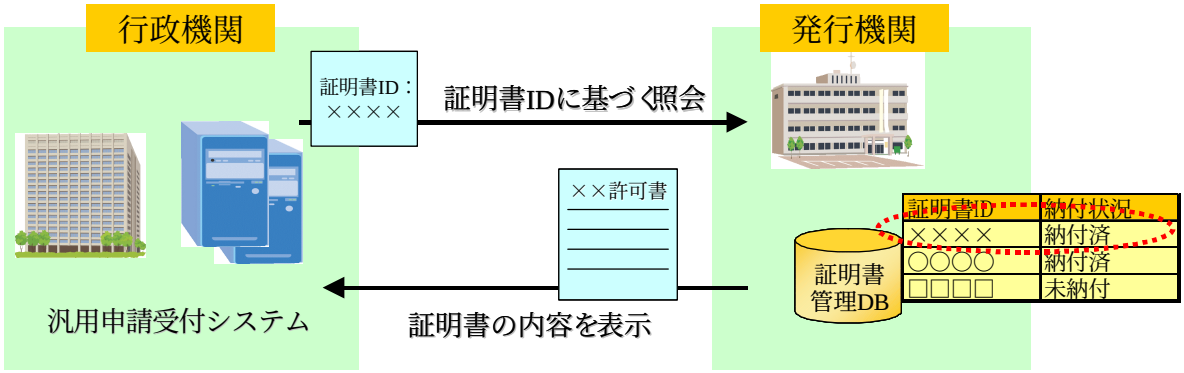


図 7-25　照会結果の通知（納付済みの場合）

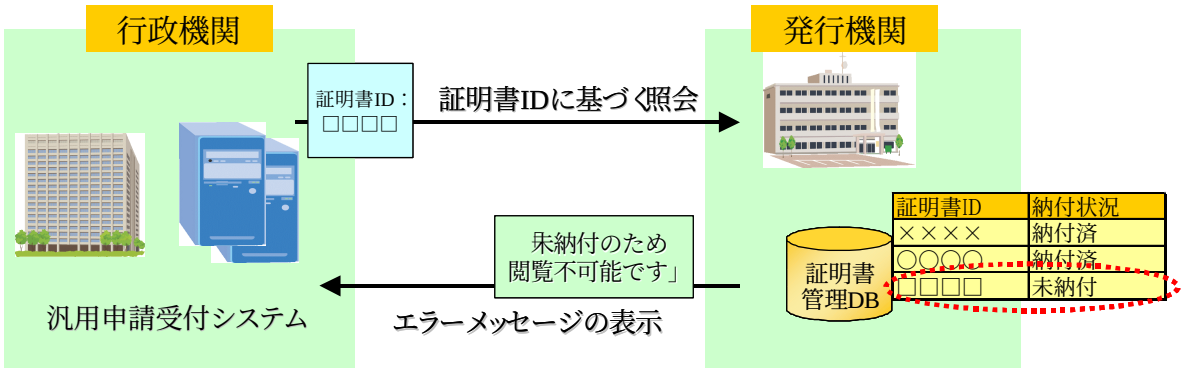


図 7-26　照会結果の通知（未納付の場合）

図 7-26 に示したとおり、発行機関に対する手数料が未納付であった場合、証明書の照会を行った際に、「未納付であるため閲覧が不可能である」旨のメッセージを返し、

照会させないことで、事実上申請者は行政サービスを享受することが不可能となる。
この対応法により、行政サービスの享受を望む申請者に対して確実に納付させ、取り逃しを防止することが可能となる。

（２） 添付資料の参照回数を制限できること

証明書の発行に伴う、手数料等の価格体系に関しては、現在の紙媒体による証明書の形態をベースとした「従量制」と、電子媒体の特性（原本と同じものを容易にコピー可能である）を考慮した、有効期限等に基づく「定額制」の２パターンが考えられる。

（a） 従量制の実現モデル

従量制を採った場合の実現モデルを以下に示す（図 7-27）。

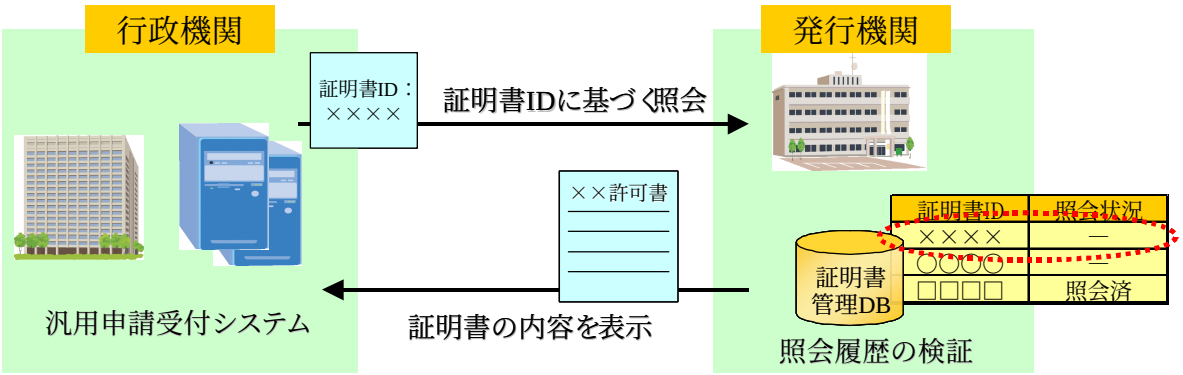


図 7-27 従量制の実現モデル

行政機関側から発行機関に対し証明書の照会を行った際に、発行機関側で当該 ID の照会履歴を検証する。これにより、証明書の内容表示回数を制限し、従量制の課金体系を実現することが可能となる。

(b) 定額制の実現モデル

定額制を採った場合の実現モデルを以下に示す（図 7-28）。

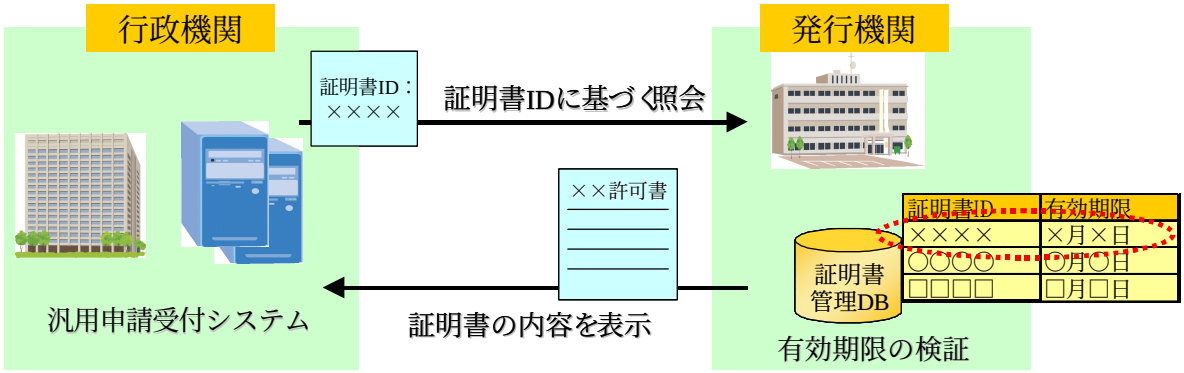


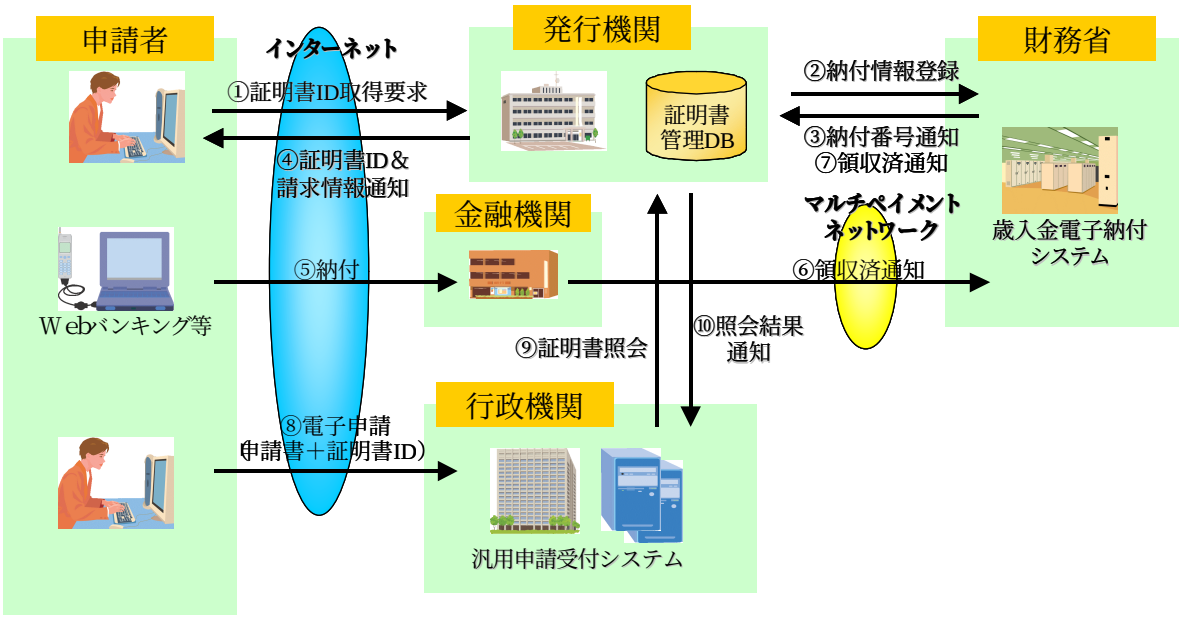
図 7-28　定額制の実現モデル

行政機関側から発行機関に対し証明書の照会を行った際に、発行機関側で当該 ID の有効期限を検証する。これにより、従量制の課金体系を実現することが可能となる。

７．７．３ 結論

ライセンスリポジトリ方式における手数料等の電子納付は前述のモデルを用いることにより、可能となる。しかしながら、証明書の照会履歴による従量制課金を実現する場面においては、第三者がランダムな証明書 ID により申請を行った場合に履歴としてカウントされてしまう可能性が存在するため、申請者・行政機関・発行機関の３者間での証明書 ID の秘匿性が重要なものとなる。

また、参考として現在中央省庁において検討されているマルチペイメントネットワークによる電子納付方式を用いた際の実現モデルを以下に示す（図 7-29）



① 申請者は、添付資料となる許可書等の発行機関となる発行主体に対して、証明書IDの取得要求を行う。
② 発行機関は申請を契機に歳入金電子納付システムに対し、申請者が納付時に必要となる納付情報登録依頼を行う。
③ 歳入金電子納付システムは発行機関に対し、納付番号の通知を行う。
④ 発行機関は証明書IDと共に、納付に必要となる各種請求情報（請求金額や、納付番号等）を申請者に通知する。
⑤ 申請者はWebバンキングや金融機関のATM等を用いて、納付を行う。
⑥ 納付された旨が、マルチペイメントネットワークを通じて、歳入金電子納付システムに通知される。
⑦ さらに歳入金電子納付システムから、発行機関に通知される。
⑧ 申請者は申請書と証明書IDを行政機関に対し申請する。
⑨ 行政機関は証明書IDを基に、発行機関に対して、証明書の照会を行う。
⑩ 発行機関は証明書IDを基に照会結果を、行政機関に通知する。

図 7-29　マルチペイメントネットワークを用いた電子納付実現モデル