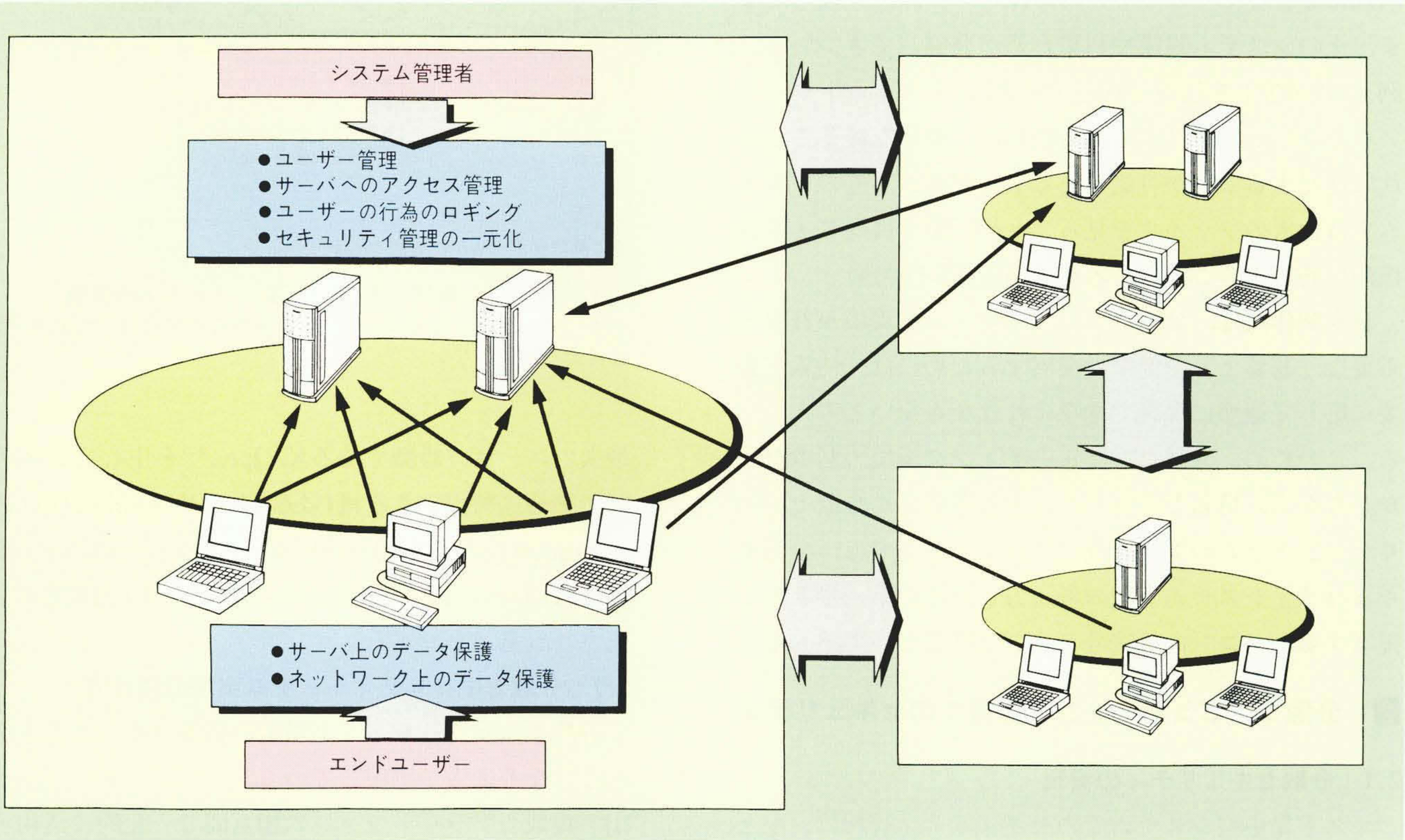
オープン分散環境における企業情報システムのセキュリティ

Information Technology System Security for Open Distributed Computing Environment

久芳　靖*　*Yasushi Kuba*
斉藤洋子*　*Yôko Saitô*
洲崎誠一**　*Seiichi Susaki*



オープン分散環境のセキュリティ管理
オープン分散環境では，ネットワークを意識したエンドユーザーの視点に立ったセキュリティ対策が求められる。そのため，日立製作所はパソコン向けの暗号ライブラリを開発し，情報セキュリティを考慮した分散セキュリティシステムの実現を図っていく。

コンピュータシステムとネットワークのオープン化は，エンドユーザーを主体とした企業情報システム構築を促すとともに，ネットワークを介した利用者相互間での情報共有や伝達の可能性を広げている。

情報は現代の企業活動にとって，人・物・金に続く第四の財産とも言われており，企業情報システムでは必要不可欠なものである。そのため，エンドユーザー主体のシステムでは使いやすさを追求する一方で，そこで取り扱われる情報を保護するということが重要である。

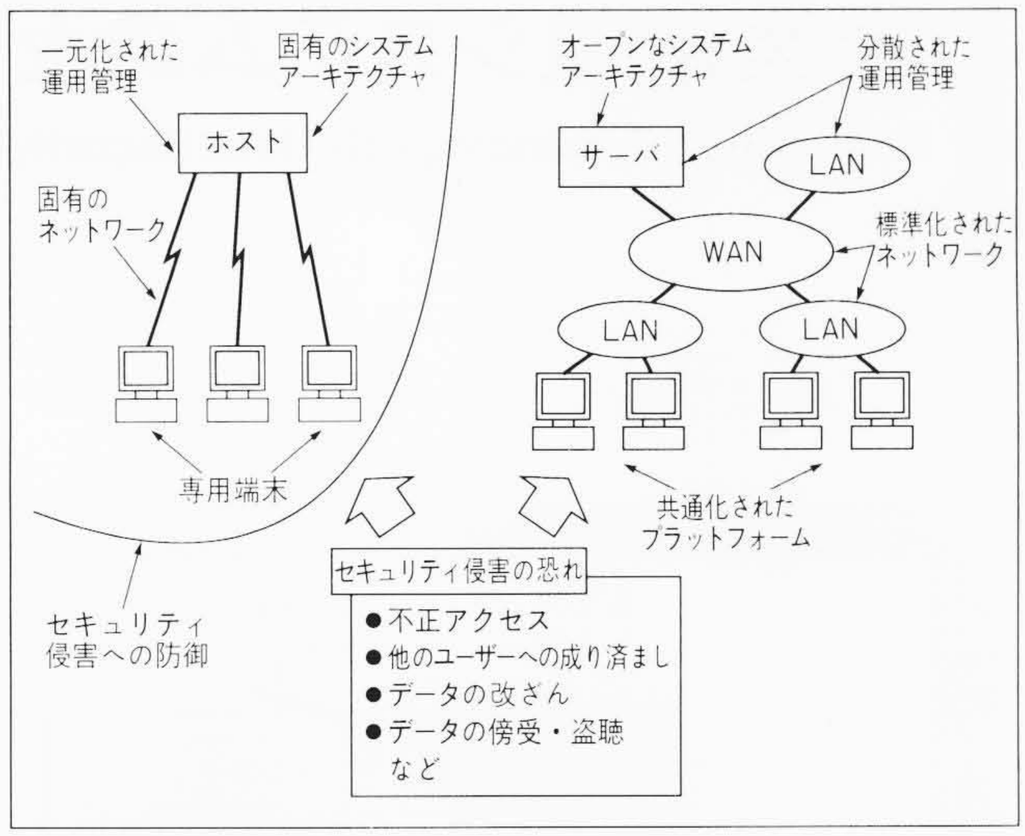
日立製作所は，オープン環境をベースとしたエンドユーザーシステムが発展していくためにセキュリティを一つの重要な基盤であると考え，エンドユーザーの使い勝手を損なわずにセキュリティを確保するための技術開発と製品化を推進している。その第一歩として，共有ファイルやネットワーク上のデータ保護に広く適用可能な，パソコン(パーソナルコンピュータ)向けの暗号ライブラリを他社に先駆けて開発し，さらにシームレスでかつ安全な，オープンシステムの利用環境の実現を図っていく。

* 日立製作所 ソフトウェア開発本部　** 日立製作所 システム開発研究所

1 はじめに

企業の基幹業務を担っているホスト集中型システムは，システムの堅牢(ろう)さと集中化されたシステム運用により，セキュリティが十分に確保されてきた。しかし，オープンシステム技術をベースとし，エンドユーザーが主体となる分散コンピューティング環境では，企業活動に必要なセキュリティの確保という課題を残したまま，そのシステム規模や利用形態が発展してきている。例えばLAN上を伝達されるデータは，そのネットワークプロトコルがオープンであるために，簡単な機器さえあれば傍受することが可能であるし，現状の多くのシステムでは他人のファイルを見ることや，勝手にシステムの稼動を妨害することさえ容易である(**図1**参照)。

日立製作所は，分散コンピューティング環境が社会の重要な一基盤として健全に発展するためには，情報を必要に応じて適切に保護できなければならないと考えている。このため，分散コンピューティング環境の利点を生かしながら，情報セキュリティをも考慮した分散セキュリティシステムの実現を図っていく。ここでは，分散セキュリティシステム実現の考え方と，その第一歩として提案するパソコン向け暗号ライブラリについて述べる。



注：略語説明 WAN (Wide Area Network)

図1 オープン環境におけるセキュリティ上の脅威
オープン環境では標準化，運用の分散などにより，セキュリティ上安全とは言えない。

2 分散コンピューティング環境でのセキュリティ

2.1 分散セキュリティの実現

ホスト集中型システムでのセキュリティ管理は，主としてユーザーによるシステムへのアクセスを管理するためのユーザー識別，認証およびユーザーの行為の追跡，確認(監査)が中心であった。

分散コンピューティング環境では，これに加えネットワークを意識したデータの機密保護，および分散環境全体の一元的な管理が必要であり，エンドユーザーを意識した使い勝手も重要である。

このような技術としては，OSF※1)/DCE※2)のセキュリティ機能があり，現在あるセキュリティ管理ソフトウェアとしては最も完成度が高いと言われている。

従来のセキュリティ機能は，システム独自のプロトコルなど固有の方式で実現されていたため，オープンな分散環境に対応することは困難であった。そこでセキュリティ機能をオープンな分散環境で実現させるため，世界最大のユーザー組織であるX/Open※3)を中心にシステム間で共通に利用できる汎(はん)用API(Application Programming Interface)〔GSS-API(Generic Security Service-API)〕の規定が推進されており，OSF/DCEでも採用される見通しである。

2.2 分散セキュリティシステム実現の考え方

分散コンピューティング環境の情報セキュリティを次のような考え方で実現していく。

(1) 複数のプラットフォーム相互間で一元的に活用可能なセキュリティ管理の実現

(2) エンドユーザーデータの保護

(3) 使い勝手の良さの確保

上記(1)の実現にあたっては，個々のプラットフォームのセキュリティ機能を活用し，その上のアプリケーションにGSS-APIのセキュリティ機能を利用させる。また，異種プラットフォームにまたがる分散環境のセキュリティ管理の一元化を目標として，OSF/DCEを基盤技術として適用する。さらには，情報のより高い機密性を確保するために，日立製作所独自の技術であるMULTI(Multimedia Encryption)暗号アルゴリズムを提供し，各アプリケーションから利用できるようにする。

この方針に基づいて，セキュリティ機能を実現するための機能群をモデル化したものを**図2**に示す。各システ

※1) OSFは，Open Software Foundationの商標である。
※2) OSF/DCEは，OSFの商品名称である。
※3) X/Openは，X/Open Company Limitedの商標である。

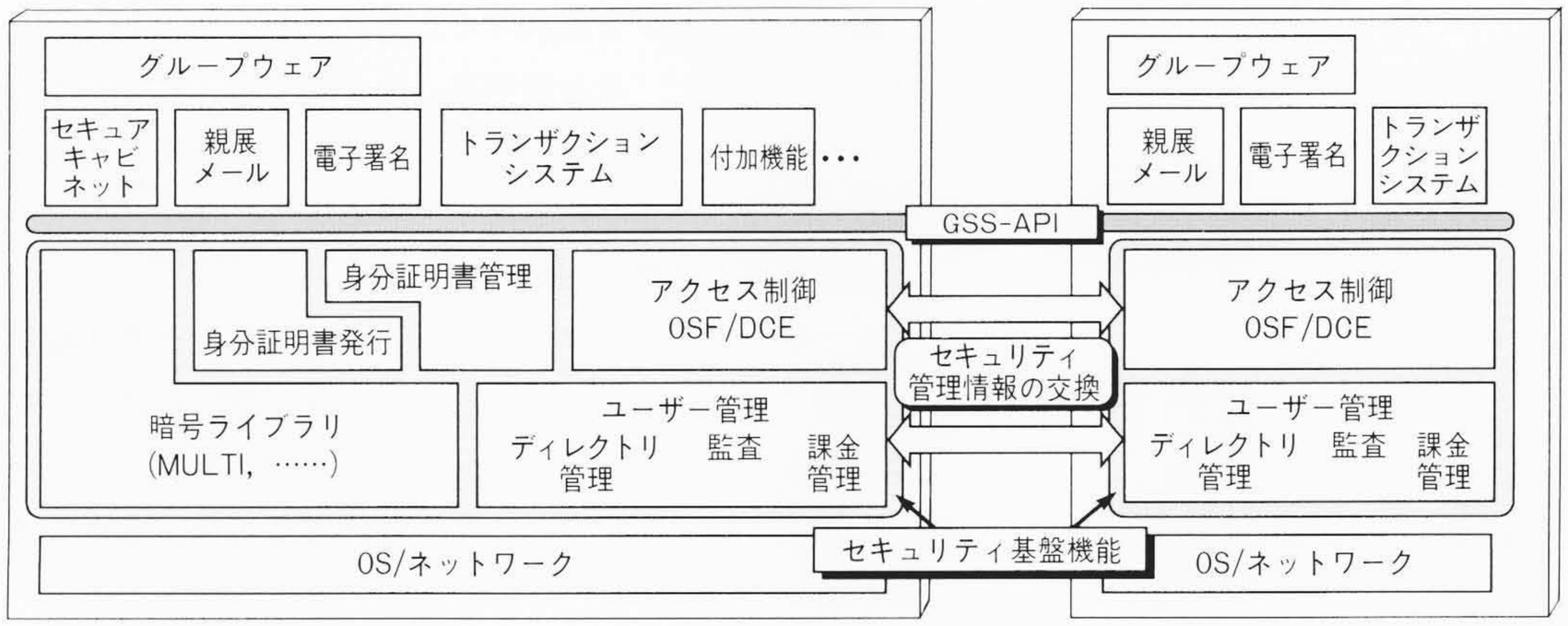


図2　分散環境に対応したセキュリティ製品提供の考え方

システム間相互のセキュリティ管理は，OSF/DCEを利用して一元化する。

ムで共通かつ最低限必要となるセキュリティ基盤機能として，OSが備えているユーザー管理機能，およびユーザーのアクセス管理機能を提供する。さらに，データの機密保護を実現するための基盤として，暗号ライブラリを提供する。セキュリティ基盤機能を利用するアプリケーションには，メール，セキュアキャビネット，電子署名などを提供し，ユーザーニーズに合わせたシステム構築を可能としていく。

3　分散セキュリティ実現のための基盤技術

3.1　GSS-API

GSS-APIの特長は，データ保護などのセキュリティ機能を特定の環境，セキュリティメカニズム，および通信プロトコルに依存せずに，アプリケーションに提供できることにある。

二つの異なるシステム上のアプリケーションやユーザー間でセキュアな通信を行う場合，相手のアプリケーションやユーザーが互いに正しい相手であることを確認し合うこと，送信側が転送したデータを確かに相手に伝えることが必要である。

例えば，アプリケーションがGSS-APIを利用して互いに通信する場合，アプリケーションに代わってセキュリティ基盤機能がアプリケーションの身分を証明する身分証明書をセキュリティサーバに発行してもらい(**図3**の①参照)，それを互いに交換することで安全な通信路を確立することができる(同図②参照)。さらにデータ転送時，アプリケーションはデータを確実に送受信するために暗号化・復号化および署名の作成・確認という機能を利用できる(同図③参照)。

このようにGSS-APIを採用したシステムでエンドユーザーは，セキュリティのメカニズムを意識せずに，セキュリティ機能を利用することが可能である。

3.2　MULTI暗号

(1)　MULTI暗号の概要

今回分散コンピューティング環境に適用するMULTI暗号は，日立製作所が1989年にMULTI2-Nという名称で発表した暗号アルゴリズムである。

MULTI暗号では，基本的なデータ攪(かく)乱方法の一つである換字処理，転置処理を計算機で複雑に繰り返すことにより，暗号強度を任意に高めることが可能である。

データの暗号化，暗号文の復号化時には暗号キーを使用するが，MULTI暗号は暗号化時と復号化時に同一の暗号キーを使用する対称暗号方式である。この方式は異なる暗号キーを使用する非対称暗号方式と比べて処理速度が速いという特長を持つ。また，MULTI暗号は，暗号アルゴリズムを公開した手続き公開型暗号でもある。仕様が公開されているため，オープンな環境で使われる製品に適している。

このような特長を持つ暗号アルゴリズムとしては，他に米国標準のDES(Data Encryption Standard)暗号，日本電信電話株式会社によるFEAL(Fast Data Encipherment Algorithm)暗号がある。

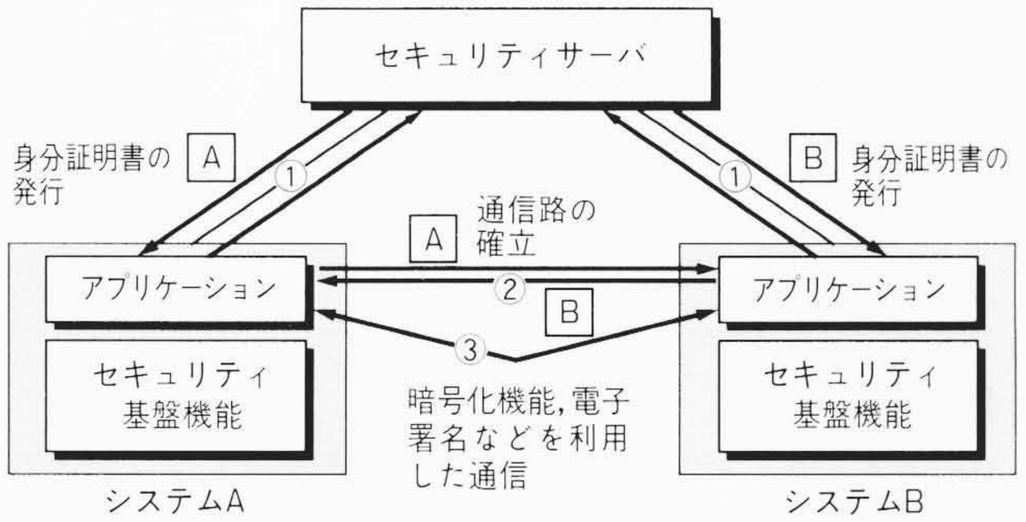


図3　GSS-APIを利用したアプリケーション間通信

セキュリティ基盤機能が提供するGSS-APIを利用することにより，アプリケーションに意識させずに安全な通信路を確保し，データ保護を図れる。

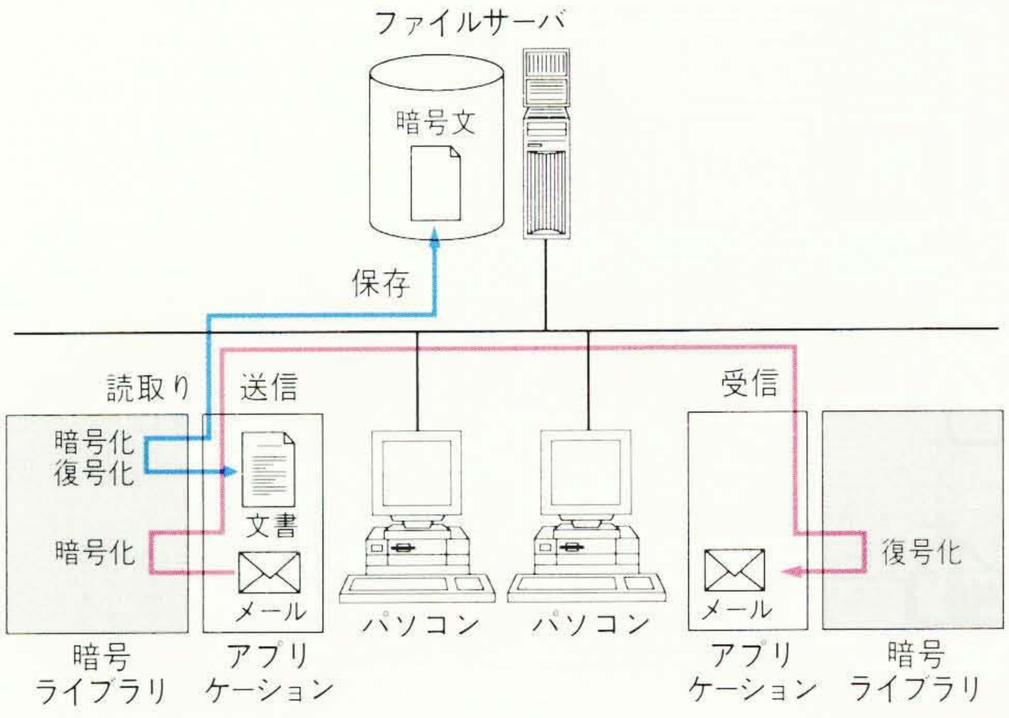


図4 暗号ライブラリを使用したセキュリティシステムの構築例
暗号ライブラリを用いて，ワープロ文書などを暗号化したうえでネットワーク上のファイルサーバに保管し，またメールの内容を暗号化して相手に送ることができる。

(2) 分散コンピューティング環境適用の優位性

MULTI暗号では換字・転置処理を32ビット単位で行っているため，最近主流となった32ビットパソコンでは，1ビット単位で処理しているDES暗号に比べ数十倍の性能が得られる。したがって，トラフィックの高いネットワーク上のデータに対しても暗号化を容易に行うことができる。

また，手続き公開型暗号であり，ソフトウェア処理でも高速であることから，オープン環境の各種のプラットフォーム上で共通に使用可能なソフトウェアとして提供できる。ハードウェアを必要としないことから，低コストでのシステム構築が容易である。

4 暗号ライブラリの開発

4.1 暗号ライブラリの概要

企業情報システムでは，重要情報を含む種々の情報処理をパソコンで行っており，パソコンでの適切な安全確保が緊急の課題となっている。このため，エンドユーザーの情報を保護するための基盤機能として，以下の特長を持つ暗号ライブラリを開発した。

(1) 身分証明書によるユーザー管理

個々のユーザーを識別するために，ユーザー名とパスワードを含んだ「身分証明書」を使用する。暗号ライブラリの使用開始時に，事前に発行した身分証明書を照合することで，不正利用を防止できる。

(2) 暗号による機密保護

ユーザーやアプリケーションが指定するデータを暗号化する。正しい身分証明書を持ったユーザーだけが，暗号文をもとのデータに復号化することができる。データの暗号化・復号化のための暗号技術としては，**3**章で述べたMULTI暗号を利用している。

(3) 標準APIの採用

アプリケーションから暗号ライブラリを利用するためのインタフェースとして，GSS-APIを使用している。標準化されたインタフェースであるため，アプリケーションの適用範囲が広がることが期待できる。

4.2 オープンシステムへの適用

オープンな環境で，暗号ライブラリを利用したセキュリティシステムの構築例を**図4**に示す。このような形態で情報の機密保護を実現する利点を次に述べる。

(1) 暗号処理部分をアプリケーションから切り離しているため，複数のアプリケーションから共通に利用でき，あるアプリケーションが生成したファイルを別のアプリケーションでも利用可能である。

(2) 特別なハードウェアを使用しないため，低コストであり，システム構築が容易である。

(3) 個人単位やグループ単位で暗号キーを持つことにより，必要なユーザー単位で情報の共有・専有を使い分けることが可能である。

5 おわりに

ここでは，分散セキュリティシステムの実現の考え方と暗号ライブラリについて述べた。分散コンピューティング環境の発展に必要なセキュリティ基盤の確立と，セキュリティ技術を積極的に活用した新しい企業情報システムへの展開を二つの軸として，今後とも企業を支える情報システムのセキュリティに取り組んでいく。

参考文献

1) 宝木，外：マルチメディア向け高速暗号アルゴリズムHisecurity-Multi 2の開発と利用方法，1989年情報理論とその応用，暗号と情報セキュリティジョイントワークショップ資料，電子情報通信学会，167～173(平1-8)
2) 小山，外：現代暗号理論，電子通信学会発行，41～62(昭61-9)
3) S.Miyaguchi, et al.：Expansion of FEAL Cipher, NTT Review, Vol. 2, No. 6 (1990)
4) 柴宮，外：セキュリティ管理の技術，日本科学技術連盟(1993)