# コンピュータシステムのセキュリティ技術と具体的対策例について

白石 旭　宮口庄司　岡本龍明　清水明宏

（日本電信電話公社　横須賀電気通信研究所）

## １．はじめに

コンピュータ社会の影の一つと言われている犯罪につながるシステムへの不正行為は、今や社会的問題として法制度面も含めた検討が各方面で取組まれている。本稿では、コンピュータシステムへの不正行為をシステム機構により防御する技術的対策の整理とその具体例について述べる。

まず、システムの安全性の立場から捉えた脅威とその対策の整理をもとに、本稿でのセキュリティ対象範囲を絞り込み、その範囲でのセキュリティ技術について分類すると共にその具体的技術項目を概括する。

次に、具体的対策例として、ＩＳＯで標準化が進められているＤＥＳ暗号機能とメッセージ認証機能及び従来のパスワード認証の欠点を改良したパスワード認証機能を実現したセキュリティ関連パッケージを紹介する。

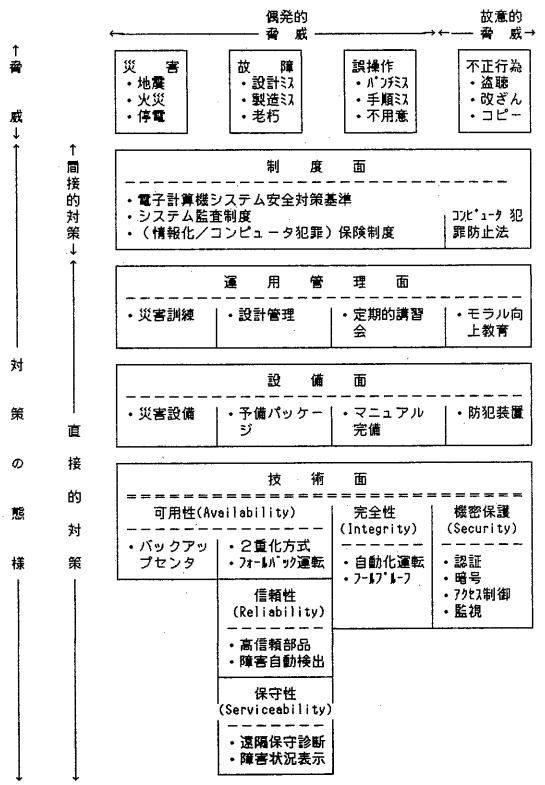



図2.1　システムへの脅威と対策の態様の具体例

## ２．セキュリティ範囲

### ２．１　セキュリティ技術の範囲

システムへの脅威は、自然や人間による偶発的脅威（災害、故障、誤操作）と人間のみによる故意的脅威（不正行為）に分けられる。一方対策の態様は、間接的対策である制度面（法や行政指導による）、直接的対策である運用管理面（システムの開発／運用体制の整備による）と設備面（物理的整備による）及び技術面（システム自身のハード／ソフトウエア的機構による）に分けられる[1][2]。これらの整理に基づく脅威と対策の具体例を図2.1 に示す。

脅威の内容によって、システム状態は異常になる場合と正常のままの場合とがある。異常になる場合の対策手段はシステムを異常状態から回復する手段とその発生を防御する手段とがあり、正常のままの場合は脅威を防御する手段のみである。システムの異常状態に対する回復手段や防御

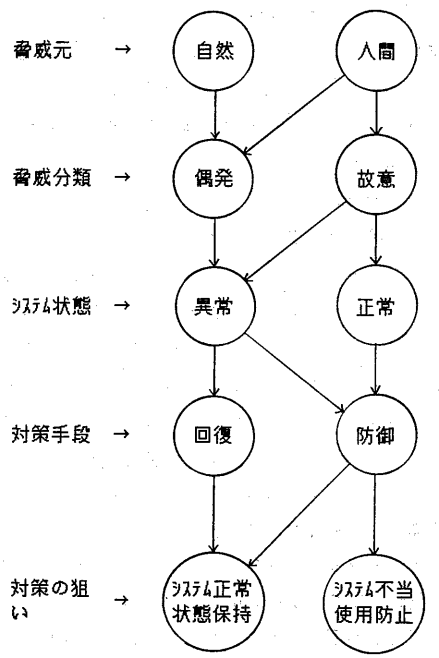



図 2.2　脅威によるシステム状態と対策の関係

手段は、いずれもシステムを正常状態に保持（維持・回復）するのが狙いであり、偶発的あるいは故意的脅威の内容にかかわらず同様の方式に基づく手段が適用され得る。しかし、システムの正常状態における故意的脅威からの防御手段は、システムが不当な目的に使用されるのを防ぐのが狙いであり、前者とは全く異なる方式に基づく手段が必要であると考える（図2.2 ）。

一方、不正行為にはシステムを使用して行われるもの（ファイルのコピー等）とシステムを使用せず行われるもの（磁性体によるMT情報の消去等）があるが、後者は運用管理面や設備面での対策に委ねられるものが多い。

上記整理の中から、正常状態にあるシステムを不当な目的に使用する不正行為から防御する技術的対策を、本稿のセキュリティ技術の範囲とする。

## 2．2　セキュリティ領域の範囲

不正行為の内容は、サービス固有の知識を用いた機能範囲の中で行われるもの（架空口座への不正入金等）とサービス内容に依存しないシステム機能範囲の中で行われるもの（MTのコピー等）とに分けられる。前者のセキュリティ領域をサービス域、後者のそれをシステム域と呼ぶ。

ところで、システム域での不正行為の究極目的は、システムが管理する情報（プログラムやデータ等）を盗用（盗聴、コピー等）、改ざん（偽造、偽情報混入等）、破壊（消去等）する事にあると考える。この対象情報は次の各種媒体上に存在し、システム内の各サブシステムにより資源として管理されている。

①磁気記録媒体：ファイル資源としてオペレーティングシステム（ＯＳ）が、またデータベース（ＤＢ）資源としてデータベース管理システム（ＤＢＭＳ）が管理する

②メモリ媒体　：一時主記憶資源としてＯＳが管理する

③回線媒体　　：ネットワーク（ＮＷ）資源として通信制御システムが管理する

したがって、システム域はさらにＯＳ領域／ＤＢ領域／ＮＷ領域に分けられる（図2.3 ）。

コンピュータシステム全体としては、これらの各セキュリティ領域の中で、個別の脅威内容に応じたセキュリティ技術を考える必要があるが、本稿ではシステム域を対象としたセキュリティ技術を考える。

## 3．　セキュリティ技術

### 3．1　不正行為

コンピュータシステムへの不正行為は、主にシステムへの接近を許されている各資格者が有する入口からの侵入により行われる（図3.1 ）。また、これら侵入路からの不正行為としては、図3.2 に示すものが考えられる。

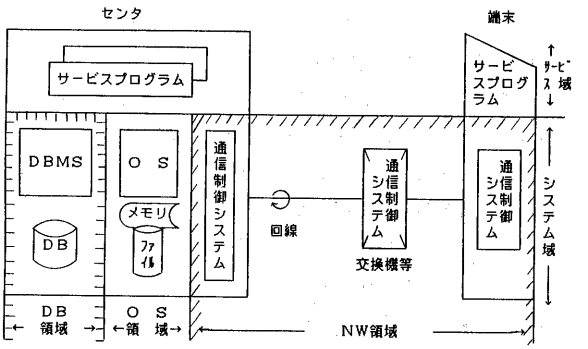



図2.3　セキュリティ領域の区分

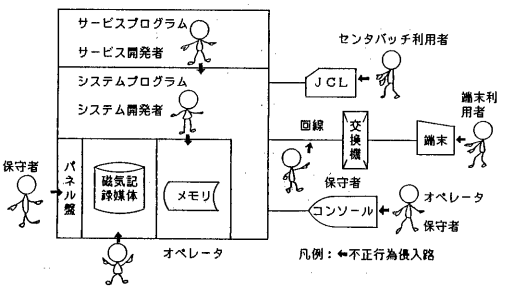



図3.1　コンピュータシステムにおける不正行為侵入路

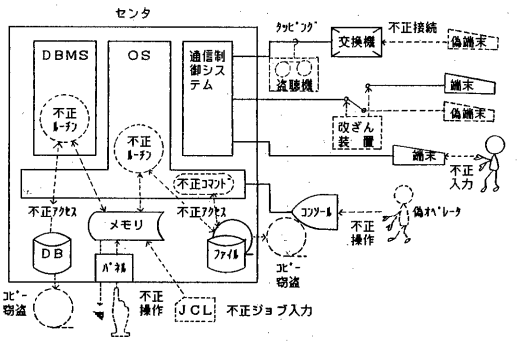



図3.2　システムへの不正行為例

## 3．2　セキュリティの技術分類と項目

不正行為と対策技術の関係は、図3.3 のセキュリティモデル[3] で示される。ここで、主体は不正行為を行うもの（オペレータ、プログラム等）であり、客体は不正行為の対象となるもの（プログラム、データ等）である。

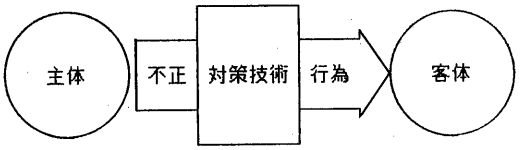



図 3.3　セキュリティモデル

一般に不正行為への対策の基本は主体側の行為を規制または牽制する事にあり、その技術は次の四つに分類できると考える（図3.4 ）。

①認証：主体が正当であるかを確認する

②アクセス制御：主体の資格範囲で客体への行為を許可する

③監視：主体の行為事象を見はる

④隔離：客体を隠す

上記の技術分類に対応する具体的な技術項目を表3.1 に概括する。

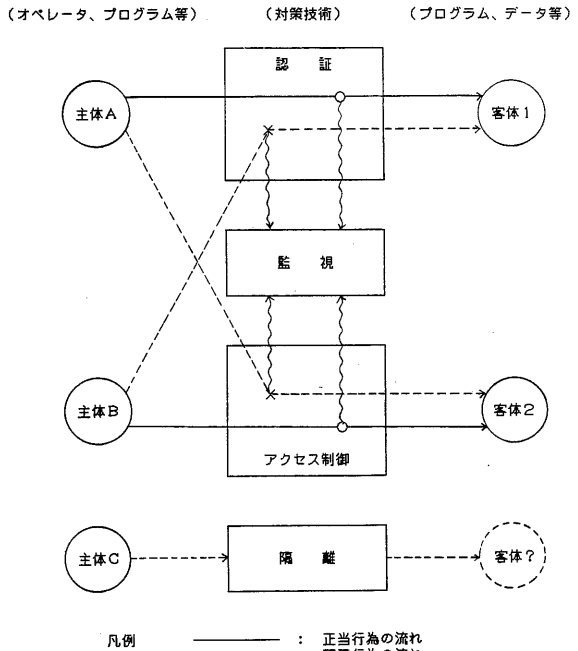



図3.4　対策技術分類

## 4．　セキュリティ対策の具体例

本章ではセキュリティ対策の具体例として、作成したセキュリティ関連パッケージについて、その狙いと実現内容の概要について述べる。

### 4．1　セキュリティ関連パッケージの狙い

システムのセキュリティ対策を全体的に抜け無く施す為には、３章で整理した技術から必要な項目を各セキュリティ領域の中で個々に実現する事となる。しかし、次の問題から個々に実現するよりも出来るだけ機能の共通化を図る事が効率的なシステム設計をする上で重要なポイントであると考える。

表3.1　セキュリティ技術項目

| 技術分類 | 技術項目 | | | 技術内容 |
|---|---|---|---|---|
| 認証<br>主体が正当であるかを確認する | 利用者認証 | パスワード認証 | | 暗証番号等の記憶情報により確認する |
| | | 個人属性認証 | | 指紋、筆跡、音声等により確認する |
| | | 所有物認証 | | ＩＣカード等の保持物により確認する |
| | | Call Back(Dial Back) | | 被起呼側から再度起呼し直す |
| | メッセージ認証 | | | メッセージの改ざんの有無を確認する |
| | ディジタル署名 | | | データの署名者と内容の正当を確認する |
| アクセス制御<br>主体の資格範囲で客体への行為を許可する | 権限リスト | | | 客体側から見た行為主体の資格を管理する（ファイルアクセスに適用） |
| | ケイパビリティリスト | | | 主体側から見た客体への行為資格を管理する（メモリアクセスに適用） |
| | フロー制御 | | | アクセス権譲渡による情報の流れを制御 |
| 隔離<br>客体を隠す | 暗号 | 慣用暗号 | ＤＥＳ暗号 | 同一鍵で暗号／復号する（ＩＳＯ標準） |
| | | | 鍵配送 | 同一鍵を通信相手に送付する |
| | | 公開鍵暗号 | | 暗号／復号鍵が異り暗号鍵を公開する |
| | 仮想計算機 | | | 客体を主体毎に仮想体として見せる |
| 監視<br>主体の行為事象を見はる | セキュリティログ | | | 不正事象の追跡や確認のため行為履歴を記録する |
| | セキュリティコンソール | | | 不正事象の発生を即時通知する |
| | システム監査 | | | システムの正当性監査を支援する |

①セキュリティに関する秘密情報（例えば，パスワードや暗号鍵情報等）を二重に管理する事となる

②セキュリティ機能を提供する個々のプログラム自体の保護が同一目的の対策には同程度のレベルで個別に構ずる必要がある

本稿で紹介するセキュリティ関連パッケージは、以下の考えに基づいて、暗号機能、メッセージ認証機能及びパスワードによるユーザ認証機能を提供するセンタの共通ソフトウェアとして実現したものであり、図4.1 に示す様なシステム形態のもとで各種のセキュリティ効果が期待出来ると考えている。

①上記問題は本プログラムによって解決される

②各サブシステム別に管理している客体の管理方式（管理対象／単位や管理機構）に依存しない為に共通化が図り易い

③各サブシステムはもとよりサービスプログラムからも共通に利用され得る機能である

## 4．2　セキュリティ関連パッケージの提供機能と構成

本パッケージで実現した基本機能の概要を表4.1 に示す[4][5][6][7]。これらに加えて、主にセキュリティ強化の観点から、さらに以下の機能を実現している。

(1) 暗号関連

・マスタ鍵／ノード間共通鍵の登録管理ユーティリティ

表4.1　セキュリティ関連パッケージ提供機能

| 機能項目 | 内　容 | 実現方式 | 記事等 |
|---|---|---|---|
| 暗　号 | 転送／蓄積対象である情報を暗号化／復号化する | 米国ＮＢＳ標準暗号アルゴリズムであるＤＥＳ(Data Encryption Standard)及びＤＣＮＡ規定の階層鍵管理方式[注3]を適用している | ＤＥＳはISO/TC97でも標準化中[注3] 図4.2 |
| メッセージ認証 | 転送／蓄積対象情報の改ざんの有無を検証する | 認証対象情報より作成した認証子（作成アルゴリズムとしてＤＥＳを適用）により検証する[注3] | ISO/TC68で標準化中[注3] 図4.3 |
| パスワードによるユーザ認証 | 指定されたパスワードによりユーザの正当性を確認する | 従来パスワード方式の問題点である回線上／ファイル上等からのパスワード盗聴盗取に弱い点[注1]を改善する為、パスワードを三つの部分より構成しかつＤＥＳを用いた一方向性関数で変換している[注2] | [注1] 図4.4 [注2] 図4.5 |

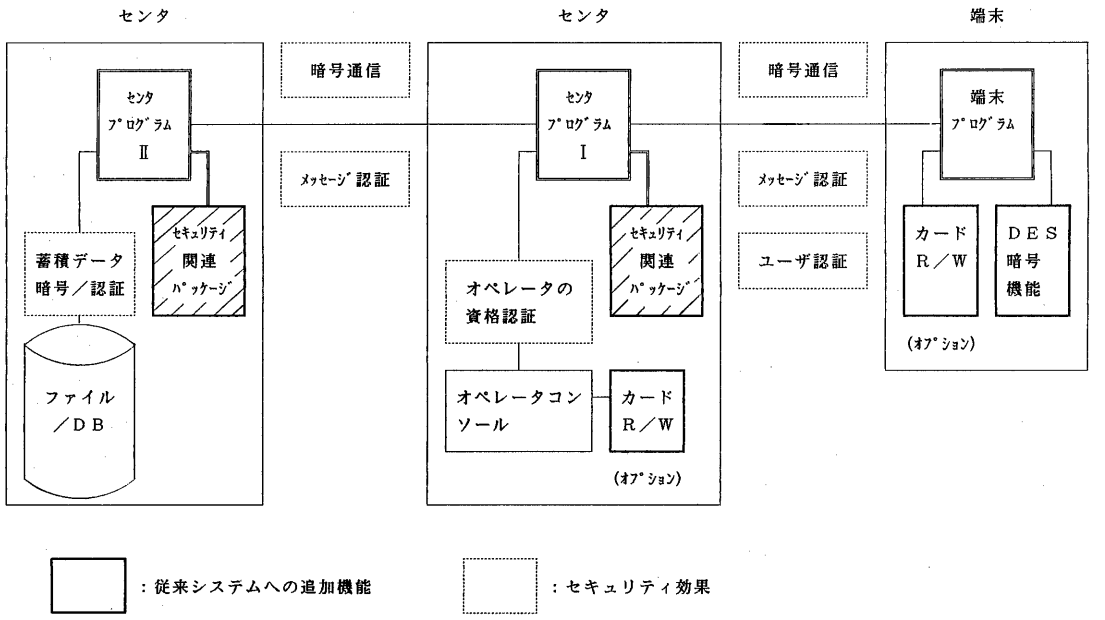
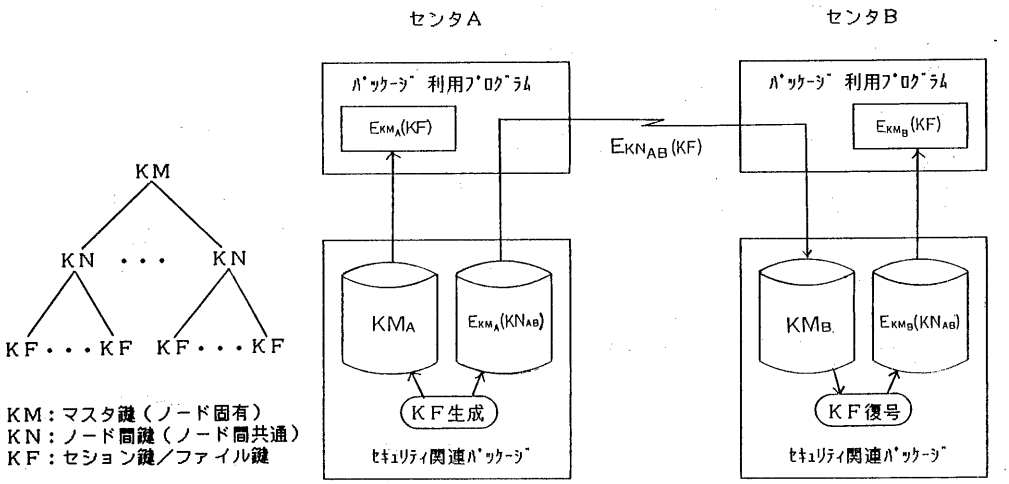



図４．１　セキュリティ関連パッケージ適用のシステム形態とセキュリティ効果

・ＤＥＳ暗号モード[8]で利用する初期ベクトルやセション鍵／ノード間共通鍵用の乱数生成
・マスタ鍵／ノード間共通鍵に対する Week Key [5][9] のチェック

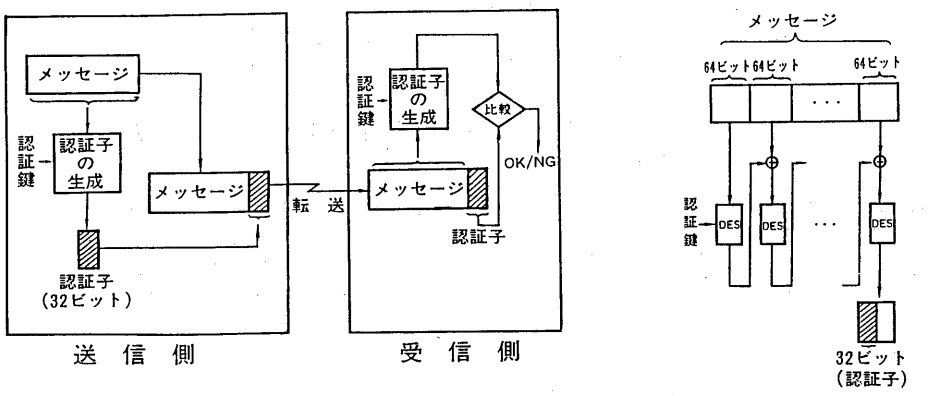
(2) パスワード認証関連
・パスワードファイル管理ユーティリティ
・一方向性関数、記憶／記録パスワード部、変更パスワード部のオプション
・認証結果返答情報（OK時情報のみを被認証側に転送する場合に使用）の変換（認証情報の部分ビット反転）
・認証の不正結果回数のカウント通知と利用プログラム判断によるパスワードのロック
・パスワード更新日付確認（ UID指定→最新日付、日付指定→指定日付以前の UID一覧）
・ユーザ自身によるパスワード登録変更（但し、不正登録を防ぐため認証サービス管理者が登録の許可を設定する・・・なお認証サービス管理者自身もこの時本パッケージで認証を受ける）
・パスワード変更時における旧パスワードチェックによる変更者の正当性確認

なお、セキュリティ関連パッケージはソフトウェアで実現している為に他ソフトウェア等からの脅威（メモリ情報の盗見等）が考えられる。したがってパッケージ内部自身で幾つかのセキュリティ対策を構じている。




（ａ）鍵の階層構成　　（ｂ）鍵の管理・配送方式

図4.2　鍵の管理配送方式




(a) 手　順　　(b) 認証子生成部

図4.3　メッセージ認証方式

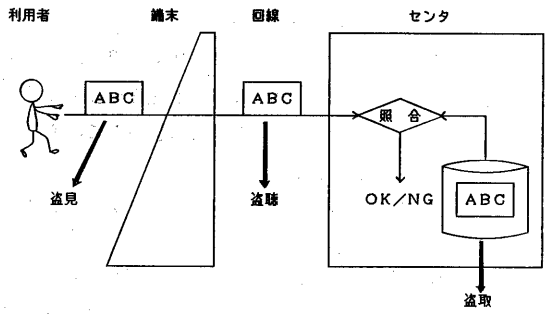



図4.4　従来パスワード方式の欠点

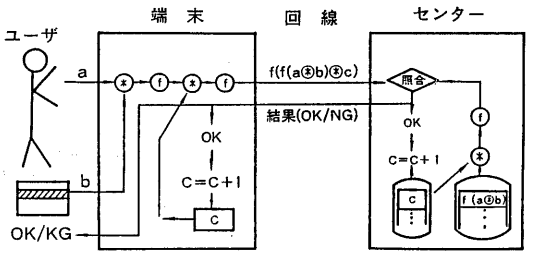
本パッケージのプログラムは、以下の理由から図4.6 に示す構成で設計されている。

①ＤＥＳ関連暗号処理はいずれの基本機能にも使われる方式である為、パッケージ内部の共通機能となる

②ＤＥＳ関連暗号処理は将来ハードウェア化を考える

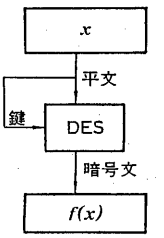
③ＤＥＳ処理部はＤＥＳ処理の高速プログラムやＤＥＳ以外のアルゴリズムから成るプログラム等の開発時に置き替えを可能とする

図4.6 に示す開放マクロは利用者プログラムに提供するサービス機能の仕様を開示しているインタフェースの処理を、また内部マクロでは階層化鍵や暗号モード及び乱数生




（備考）・a：パスワードの一部でユーザが記憶しておく部分
・b：パスワードの一部でカード等の記録媒体に記録しておく部分
・c：パスワードの一部で認証処理毎に変更する部分
・$f$：一方向性関数

（a）手　順




（b）DESを用いた一方向性関数

図4.5　改良パスワード方式

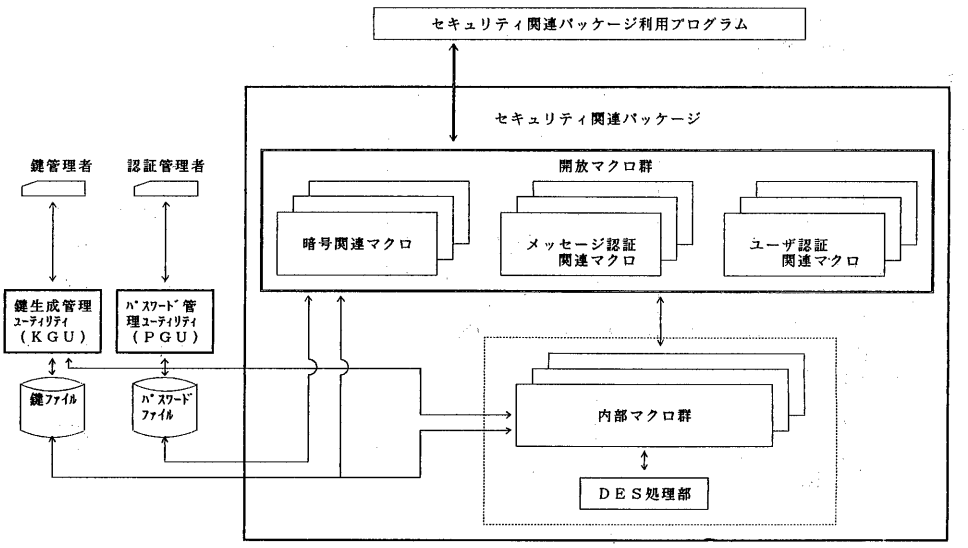



図4.6　プログラム構成

成等の処理を行う。またＤＥＳ処理部はアルゴリズムのみの処理を行う。

## ４．３　セキュリティ関連パッケージの評価

本パッケージでは、暗号／メッセージ認証／パスワード認証各方式の基本となっているＤＥＳ暗号処理をソフトウェアで実現している。したがって、ここでは暗号処理によるシステム性能への影響度合を評価する。

図4.7 に某システムにおける単電文当りの処理において、暗号機能により生ずるＤＳ増加率を示す。ＤＥＳの暗号単位である８Byte（以下ではＤＥＳ暗号単位である８Byteに対して述べる事とする）でも約10％の増加率を示している。

ところで、図4.6 のプログラム構成における暗号機能のＤＳの内訳は図4.8 の割合いで示され、ＤＥＳ処理部のみで約60％を占めている。またメッセージ認証機能のシステムへの影響はほぼ暗号機能と同じ率を示し、その内訳は図4.9 に示す様に暗号処理部で約70％を占めている。

パスワード認証機能の場合の影響は、その利用形態から考えて、セション開設時における一時的ＤＳ増であり、同一セッション内の電文トラヒック数で平均化すればその影響は小さくなると考える。しかし各電文単位を対象とするような暗号やメッセージ認証の場合はシステムへの影響がかなり大きいため、暗号処理（特にＤＥＳ処理部）の性能向上を図る必要がある。

この度、ＤＥＳ処理部は、その性能向上が図れる方式を得た[10]事により、約75％のＤＳ削減が可能となった。この結果図4.8 に示すように暗号機能全体では約45％のＤＳ削減となり、システムへの影響は今までの約半分の 5％におさえる事が可能となった。

システムがセキュリティ機能による性能への影響をどこまで許容できるかは、各システムのセキュリティに対するリスクアナリシスの判断に依存する。したがってどの程度まで性能向上を図るべきかの目標は一律に定められないが、

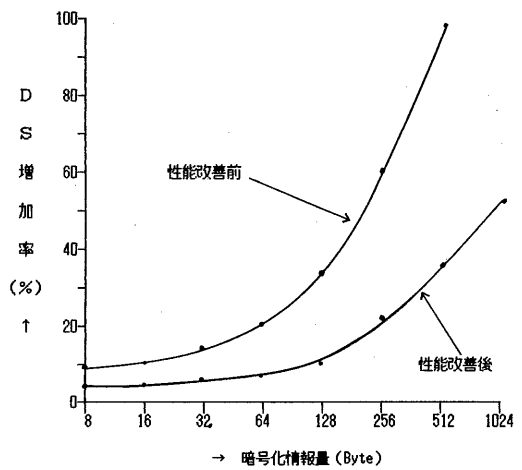



図4.7　暗号機能のシステムへの影響度合

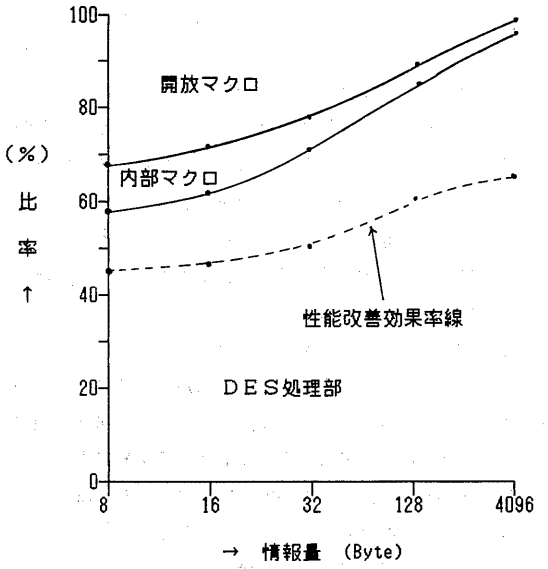



図4.8　暗号処理性能の割合

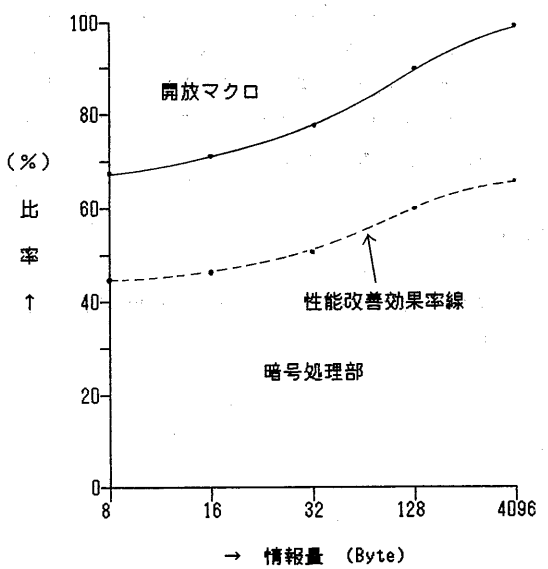



図4.9　メッセージ認証処理性能の割合

暗号対象情報量が大きい場合は未だかなりの影響を与えていると考えるべきであろう。この為、プログラム構成の理由で述べたよう暗号処理部のハードウェア化を併用した提供方法が今後必要であると考える。

## 5. おわりに

本パッケージの適用において懸念される以下の事項を今後の主な課題とし、本パッケージの試行評価を通じてその対策を検討してゆきたい。

①システム障害時の保守対策への影響

暗号化されたメモリあるいはファイル上の情報内容が障害解析に係わる場合、どの様な手順で解析作業を行うべきか、また誰にも情報の復元が出来ず障害解析が不可能となる事象が起り得ないか、さらに暗号化されたジャーナル情報からの復旧作業時間は大幅に長くなるため復旧方式を見直す必要がないか

②端末側への本方式の適用の可能性

ホームバンキング／ＯＡ等で多く利用されるポータブル端末やパソコン等の端末へ本方式を適用する場合、端末側で必要となるＤＥＳ暗号機能や鍵管理・配送機能の実現が容易か、また処理能力的に許容できるか（暗号等を組入れた汎用的セキュリティボード開発の必要性）

③パッケージ機能の提供形態の柔軟性

鍵の階層化による管理／パッケージ自体のセキュリティ対策等、開発側独断の設計によるセキュリティ強化が利用者側にとって必要以上の強度になってないか、またこの為による運用時の不要な煩雑さを利用者に与えていないか（利用者判断に基づくセキュリティ強度に応じた機能選択への対応の必要性）

## 謝辞

本稿を発表できる機会を与えて下さった関係各位に深謝します。

## <参考文献>

[1] 「電子計算機システム安全対策基準」：通産省（昭和59.7）

[2] 「コンピュータセキュリティ対策のあり方について」：産業構造審議会情報産業部会中間答申（昭和58.12）

[3] 新版「情報処理ハンドブック」：オーム社

[4] 「ＤＣＮＡネットワーク管理プロトコル」技術参考資料：日本電信電話公社（1983）

[5] FIPS PUB 46 DATA ENCRYPTION STANDARD 、JANUARY 1977

[6] ISO Standard Test Key 、ISO/TC68/SC2/WG2 N80

[7] 岡本、白石：”パスワード認証方式に関する一提案” 昭和58年度信学会情報システム部門全国大会 S8-3

[8] FIPS PUB 81 DES MODES OF OPERATION 、DECEMBER 1980

[9] Data Encryption Specification Algorithm DEA1 ISO/DP227 (1982-12)

[10]宮口、白石：”等価アルゴリズムを用いたＤＥＳ暗号高速アルゴリズム設計法”、信学技報 Vol.84 No152 IN84-51(1984.9)