U.D.C. 681.324.078:343.451:654.029.3

ネットワーク セキュリティ技術

Security Techniques for Computer Networks

宝木和夫* *Kazuo Takaragi*
佐々木良一* *Ryôichi Sasaki*
三浦　雄** *Yuu Miura*
奥村　誠*** *Makoto Okumura*

ファームバンキング，株式売買など通信ネットワーク利用ビジネスの普及に伴い，不正アクセスやデータの盗み見，改ざんなどのコンピュータ犯罪も増加する可能性がある。このようなコンピュータ犯罪の脅威や誤操作などから情報システムを保護するため，各種暗号の応用とセキュリティ評価・向上策によって種々のセキュリティ対策を実施する日立情報セキュリティシステム“Hisecurity”の基本技術を開発した。本開発により，高度のセキュリティを確保できるようになるとともに，既開発の総合利用者管理機能“TRUST”と組み合わせて用いることによって，目的に応じたきめ細かいセキュリティ機能を提供できるようになった。

1 緒　　言

近年，情報処理や通信技術の進歩とともに，銀行オンライン システムのようなコンピュータ ネットワークが普及している。また，近い将来，コンピュータ ネットワークを介して会議や種々の取引が本格的に行われるようになると予想される。このような情報化社会の進展に伴い，その影の部分としてコンピュータ犯罪も増加する可能性がある。

昭和62年２月に，筑波のコンピュータに外国からハッカーが侵入するという事件が明らかになった。これは，第三者による不正アクセスの事件であるが，このほか，部内者による不正アクセスやデータせっ(窃)盗，改ざんといった事件が発覚している[1]。今後，この種の犯罪はますます増加するとともに，従来なかった新しいコンピュータ犯罪の可能性も生じると予想される。

このようなコンピュータ犯罪の脅威や誤操作などから情報を保護するネットワーク セキュリティ技術は，昭和52年に米国商務省標準局が暗号アルゴリズムの標準としてDES[2](Data Encryption Standard)を制定したころから，その必要性が強く認識され始め，以後，主にビジネス分野で急速に進展している。

日立製作所では，次の観点からネットワーク セキュリティ技術を構築している。

(1)　漏れのない不正行為防止策

防護の強度をいくら強くしても，システムとしてぜい弱な部分が残れば意味がない。そこで，必要な安全性に対して漏れのない有効なセキュリティ対策を行う。

(2)　システム信頼性の低下防止

セキュリティ対策は，正当な使用者であっても，パスワード入力などの通過手続きが不十分であると通さないという働きを持つ。そこで，使用方法を必要以上に複雑にして使いにくくならないようにするとともに，セキュリティ機構などの故障がシステム本来の業務に悪影響を与えないよう工夫を行う。

これらの観点に基づいて開発した個々のセキュリティ技術を**図１**に示す。このうち，TRUST(Total Resource and User Control Facility：総合利用者管理機能)は一つの計算機で他人のファイルを誤って壊したり，意図的にのぞき見るなどの誤操作，不正行為を防止する技術である。また，Hisecurity (Hitachi Information SECURITY System：日立情報セキュリティシステム)の六つの技術は，二つ以上の計算機間の通信でデータ破壊，盗聴，改ざんなどの誤操作，不正行為を防止する技術である。

本稿では，日立製作所のネットワーク セキュリティ技術であるTRUSTとHisecurityについて述べる。

2 セキュリティ技術の概要

計算機不正使用，データ改ざんなどのセキュリティ上の脅威に対し，利用者管理から物理的な保護に至る七つの対策技術項目が考えられている(**図１**)。対策技術項目の内容と日立製作所の対応は次のとおりである。

2.1 利用者管理，資源アクセス管理

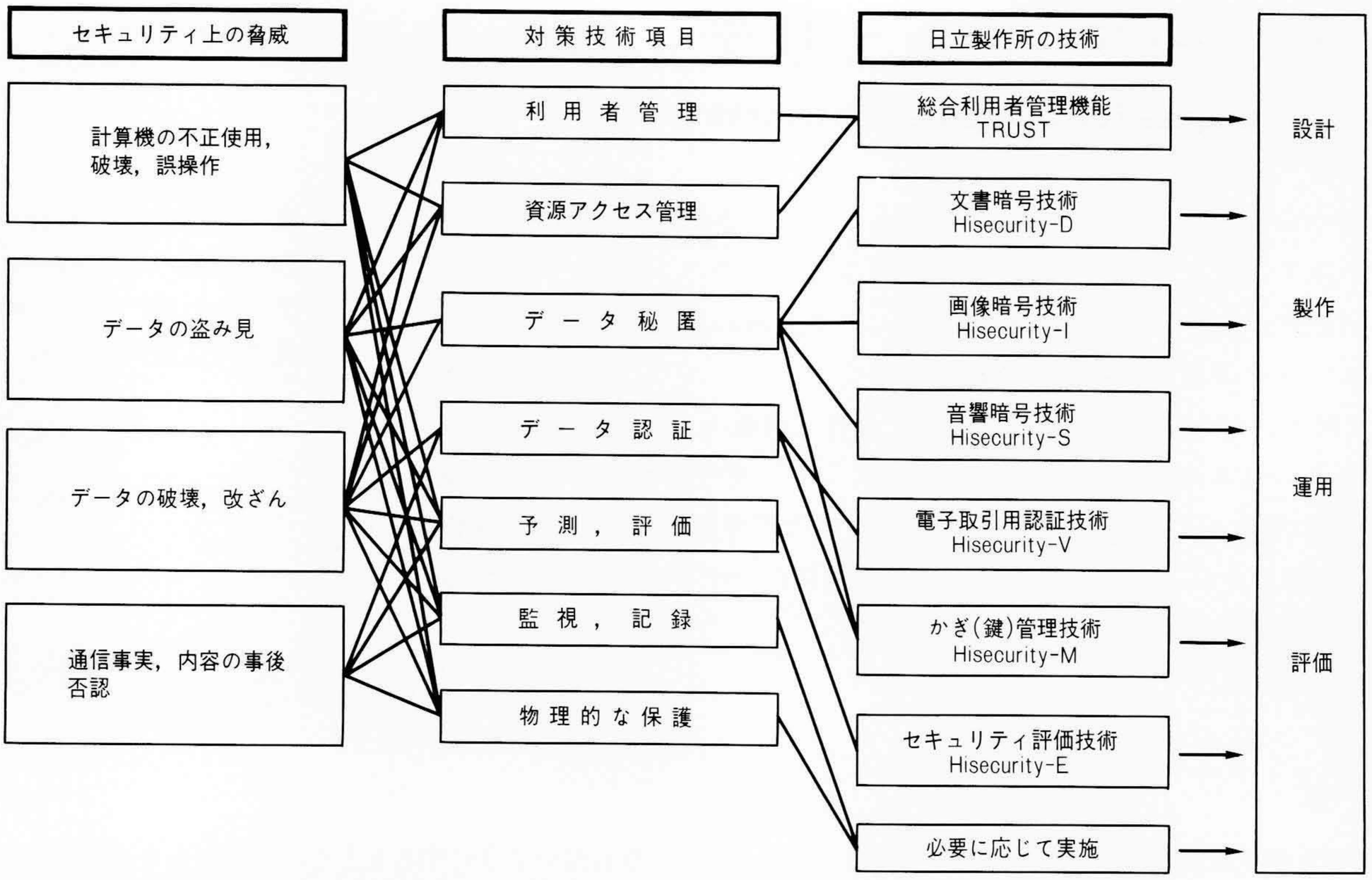
一つの計算機に利用者がアクセスする場合，利用者確認の後，計算機の使用をある範囲内に限定することは重要である。これは，計算機を多数の人に安全に使用してもらうためである。

このような利用者管理及び資源アクセス管理を実現するため，TRUSTは次の２点を実施している[2]。

(1)　アクセス権限の管理

計算機の利用者に，まず，利用者識別符号と暗証符号(パスワード)を入力してもらい，次に，その利用者にあらかじめ定

* 日立製作所システム開発研究所 工学博士　** 日立製作所神奈川工場　*** 日立製作所大森ソフトウェア工場



注：略語説明 Hisecurity(Hitachi Information SECURITY system：日立情報セキュリティシステム)
TRUST(Total Resource and User Control Facility)

図1 セキュリティ上の脅威と対策技術 パスワードによるアクセス管理(TRUST)と各種暗号による高度のセキュリティ機能(Hisecurity)などの組合せにより，必要なセキュリティを確保する。

められた範囲内で磁気ディスク ファイルなどの使用を許可する。利用者は，自分に割り当てられたファイルを他の利用者にも使用できるよう他人のアクセス権限を変更することもできる。

(2) 課金の管理

計算機は情報処理速度やファイル容量などの能力に限りがある。複数の利用者が計算機を合理的に使用できるようにするため，CPU(中央処理装置)使用時間，ファイル使用量などに対して利用者別に課金を行う。

2.2 データ秘匿

データ保護方法の一つとして，暗号用のかぎ(鍵)を用いて通信ネットワークを流れる情報や計算機に蓄積されたファイル情報を高速に暗号化し，受信時やファイルの使用時に復号化する暗号技術は，有効かつ実用的である。

暗号化を実施する対象及び暗号化の手段を**図2**に示す。同図に示すように，暗号化の対象と手段には種々のものがある。

(1) 回線暗号機形か，チャネル直結暗号機形か。

(a) 計算機本体には変更を加えず，モデム間単位で暗号化する(ノード ツー ノード暗号)回線暗号機形と，(b) 計算機本体のハード・ソフトを一部変更して，計算機間単位で暗号化する(エンド ツー エンド暗号)チャネル直結暗号機形の二とおりがある。いずれをとるかは，必要な暗号速度，開発コスト，開発期間の制約などによって決まる。

チャネル直結暗号機形を選んだ場合，更に次の選択が生じる。

(2) 暗号化をハードでするか，ソフトでするか。

(a) 計算機チャネルなどの外部インタフェースに暗号機ハードを接続して，そこでデータを暗号化するか，(b) 暗号処理用ソフトウェアを用いてデータを暗号化するか，を選択する。これも，必要な暗号速度，安全性，開発コスト，開発期間の制約などによって選択される。

これらのうち一組が選定されると，次に暗号アルゴリズムが選定される。

暗号アルゴリズムには，次のものが存在する。

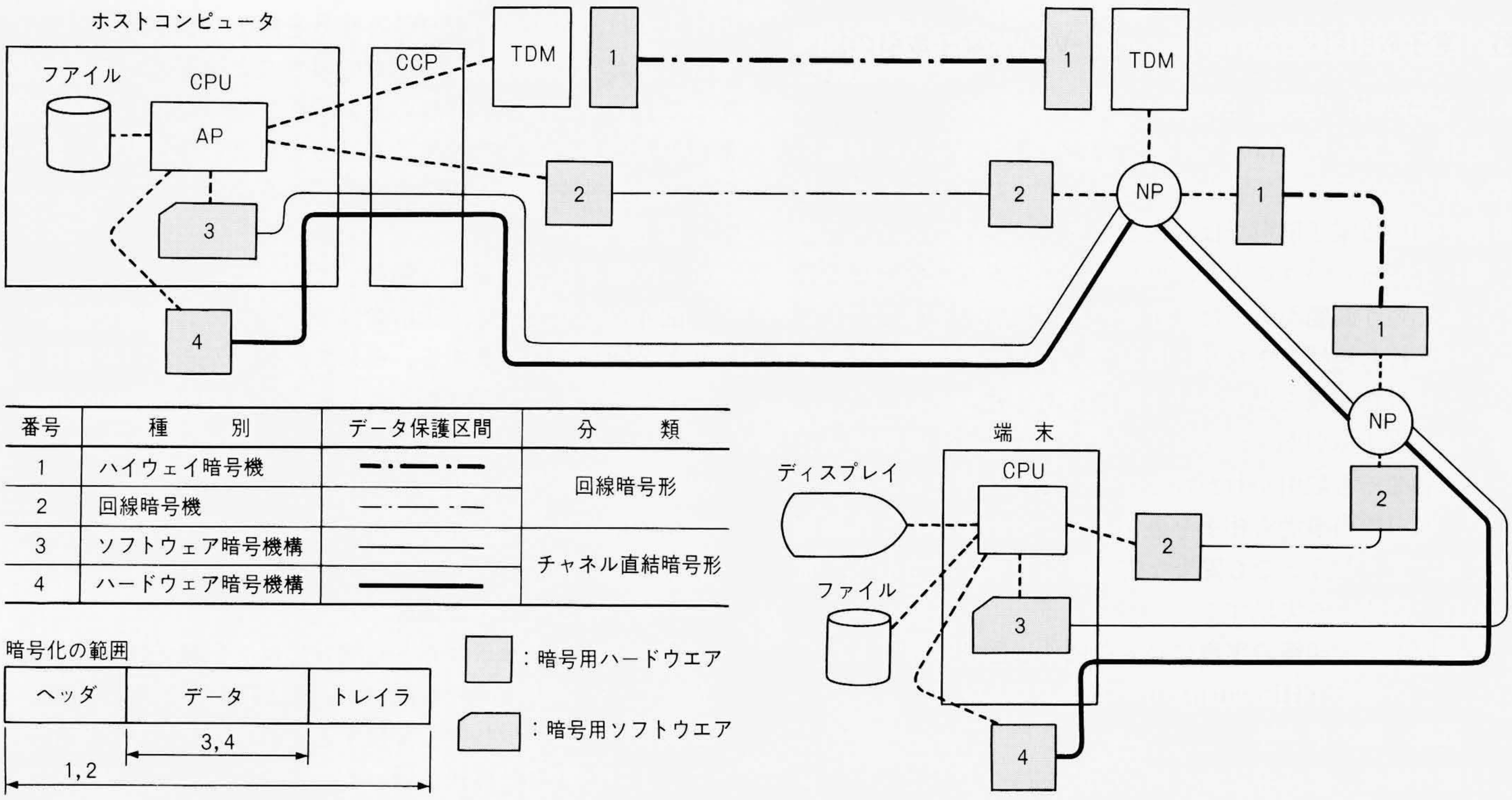
(1) コンピュータ メッセージ，文書データの暗号アルゴリズム

コンピュータ メッセージやワードプロセッサなどを用いて作成された文書を暗号化する。この暗号方式は，(a) 米国データ暗号化規格DES[3]のようにアルゴリズムを公開して，暗号かぎを秘匿する方式と，(b) 一般的な暗号機のようにアルゴリズムと暗号かぎを両方秘匿する方式の2方式がある。暗号の使用環境に応じて，適切なアルゴリズムが選定される。

日立製作所では，文書データの暗号化のため，和積暗号[4]をはじめ数種類のアルゴリズムを開発し，文書暗号技術Hisecurity-Dとして実現している。

(2) 画像データの暗号アルゴリズム

医用画像，テレビ会議画面などの画像データを暗号化する。一般に画像は，(a) データ量が多いうえ，(b) 画像パターンの繰返しなど冗長な部分が多い，(c) 画像が若干変形しても人間の目によるパターン類推が可能，などの特徴を持っている。こ



番号	種　　別	データ保護区間	分　　類
1	ハイウェイ暗号機	―・―・―	回線暗号形
2	回線暗号機	―・―・―	
3	ソフトウェア暗号機構	――――	チャネル直結暗号形
4	ハードウェア暗号機構	――――	

注：略語説明　CPU(中央処理装置)，CCP(通信制御処理装置)，TDM(時分割多重化装置)，NP(ノードプロセッサ)，AP(アプリケーションソフト)

図2　暗号機構とデータ保護区間　　必要なデータ保護区間，開発コストなどに応じて，どの暗号機構にするかを決める。

のため，文書暗号と同様の方式で画像データを暗号化しようとすると，(a)暗号化に時間がかかる，(b)パターン類推されるおそれがあるという問題が生じた。

そこで，画像暗号技術Hisecurity-Ⅰでは，静止画用に高速かつ繰返し類推，パターン類推を防止できる高速暗号方式を開発している[5]。

(3)　音響信号の暗号アルゴリズム

ボイスメールなどの音声・音響信号を暗号化する。音声・音響暗号方式としては，(a)従来の無線暗号のように，音声のアナログ信号を周波数変調などの手段で別のアナログ信号に変換する方式と，(b)音声・音響信号をいったんディジタル信号に変換した後，数式処理による暗号化を行う方式がある。

音響暗号技術Hisecurity-Sとして，上記(b)に関するアルゴリズムを開発中である。

上記(1)～(3)のいずれの暗号を使用する場合でも，暗号用のかぎを適切に管理しないとシステムのセキュリティは損なわれてしまう。

かぎ管理技術Hisecurity-Mは，(a)メモリカードによる安全かつ効率的なかぎの保管と，(b)コードブック暗号による通信かぎパラメータの指定を特徴とするかぎ管理を行う。

2.3　データ認証

近い将来，各種取引業務や納税業務などの大部分がOA(Office Automation)機器を用いて行われるようになると考えられる。この場合，従来の書類の印鑑に代わる機能が必す(須)となる。このため，口座振替，株式売買などの電子伝票に，作成者，取引内容などを保証するような電子的な「印鑑」を実現する[6]。もちろん，印鑑の印影をそのままディジタル信号に変換する方式では，だれでも容易にコピー，再使用できるので，この方式とは違った特別の工夫が必要である。

電子取引用認証技術Hisecurity-Vは公開かぎ暗号を用いて，電子的な「印鑑」を実現している。これについては**3**章で詳述する。

2.4　予測，評価

上記セキュリティ対策を実施したとき，目的としたセキュリティは確保されるかどうかを予測，評価する。

セキュリティ評価技術Hisecurity-Eは，(a)不正行為に対し本当に安全か，漏れはないか，(b)セキュリティ機能の障害がシステム本来の業務に悪影響しないか，の2点から評価を行う[7]。これらについては**4**章で詳述する。

2.5　監視，記録

システムの状態を監視，記録し，不正行為が生じた場合，その発生箇所を追跡，確定する。日立製作所では，必要に応じて監視，記録の機能を提供している。

2.6　物理的な保護

計算機を強固な建造物に収めるなどの物理的な保護を行う。日立製作所では，必要に応じて物理的な保護を実施している。

上記**2.1**～**2.6**節で述べた技術の全部あるいは一部の組み合わせにより，計算機の不正アクセス，データの盗み見，改ざんなど情報の不正操作に関するコンピュータ犯罪から情報システムを保護することが可能となる。

例えば，TRUSTによって，計算機内部のデータはパスワードで保護される。また，データが計算機外部に取り出されるなどパスワードによる保護が外れた場合は，Hisecurityの暗号機構によって，種々の不正行為からデータを保護することが可能となる。

3　電子取引用認証技術Hisecurity-Vによる電子取引の認証

3.1　電子的な「印鑑」の要件

従来，正式な取引は双方が面と向かい合って双方の印鑑を押し合うことによって安全性を確保していた。ところが，計算機を用いる電子取引では，両者が通信ネットワークを介して離れているということと，処理はディジタルのデータで行われるという問題があった。すなわち，取引の途中で一方がなつ印を持ち逃げできたり，取引データは後で改ざんされてもこん(痕)跡が残らないという問題があった。

今後，電子取引が一般化してくると対等関係や競争関係にある二者間でも取引が行われるようになると考えられる。そこで，取引の当事者も相手を裏切ることがあるという性悪説の立場に立ったうえでも安全な電子取引手順，すなわち，電子的な「印鑑」を実現する。

電子取引で，印鑑の実現に必要な要件は**図3**に示す5件である。この順に，Hisecurity-Vの技術を説明する。

(1)　偶然一致の希少性

印鑑の場合，世の中に全く同じ印影を持つものは二つと存在しない。これに対し，Hisecurity-Vでは，一見ランダムな64バイト※)の数値列を電子的な「印鑑」とすることにより，第三者がランダムに作成しても偶然に一致することがほとんどないようにしている。

(2)　改ざん防止性

第三者及び受信者が通信文を改ざんできないようにするため，公開かぎ暗号(RSA方式)[3]を用いる。公開かぎ暗号では，暗号をかけるかぎ(秘密かぎ)と暗号を解くかぎ(公開かぎ)は異なっており，受信者は送信者の暗号文と同様のものを作成することができない。すなわち公開かぎ暗号を用いると，受信者も送信者の暗号文を改ざんできないという意味で，強い改ざん防止性を実現できるという働きを用いる。

(3)　認 証 性

(a)　印鑑登録に相当する機能

図4に示すように，送信者はまず自分の計算機で秘密かぎと公開かぎを作成する。そして，公開かぎだけを関係者に分かるように公開する。これは，従来の印鑑登録に相当する。

(b)　印鑑の保管に相当する機能

秘密かぎは秘密に保持する。これは，本人が印鑑を保管することに相当する。

(c)　なつ印に相当する機能

なつ印したい伝票ができた場合には，伝票の圧縮文を作成して，なつ印原文の一部とする。圧縮文の計算の仕方は，圧縮文の一部が少しでも変化すると計算結果が全く変わってしまうような計算式を用いる。これによって，内容に即したなつ印ができるとともに，なつ印だけを別の伝票に切りばりするような不正行為を防止できる。更に，日時などの取引状況を示すデータをつないで暗号化すると電子なつ印となる。これは，従来のなつ印に相当する。

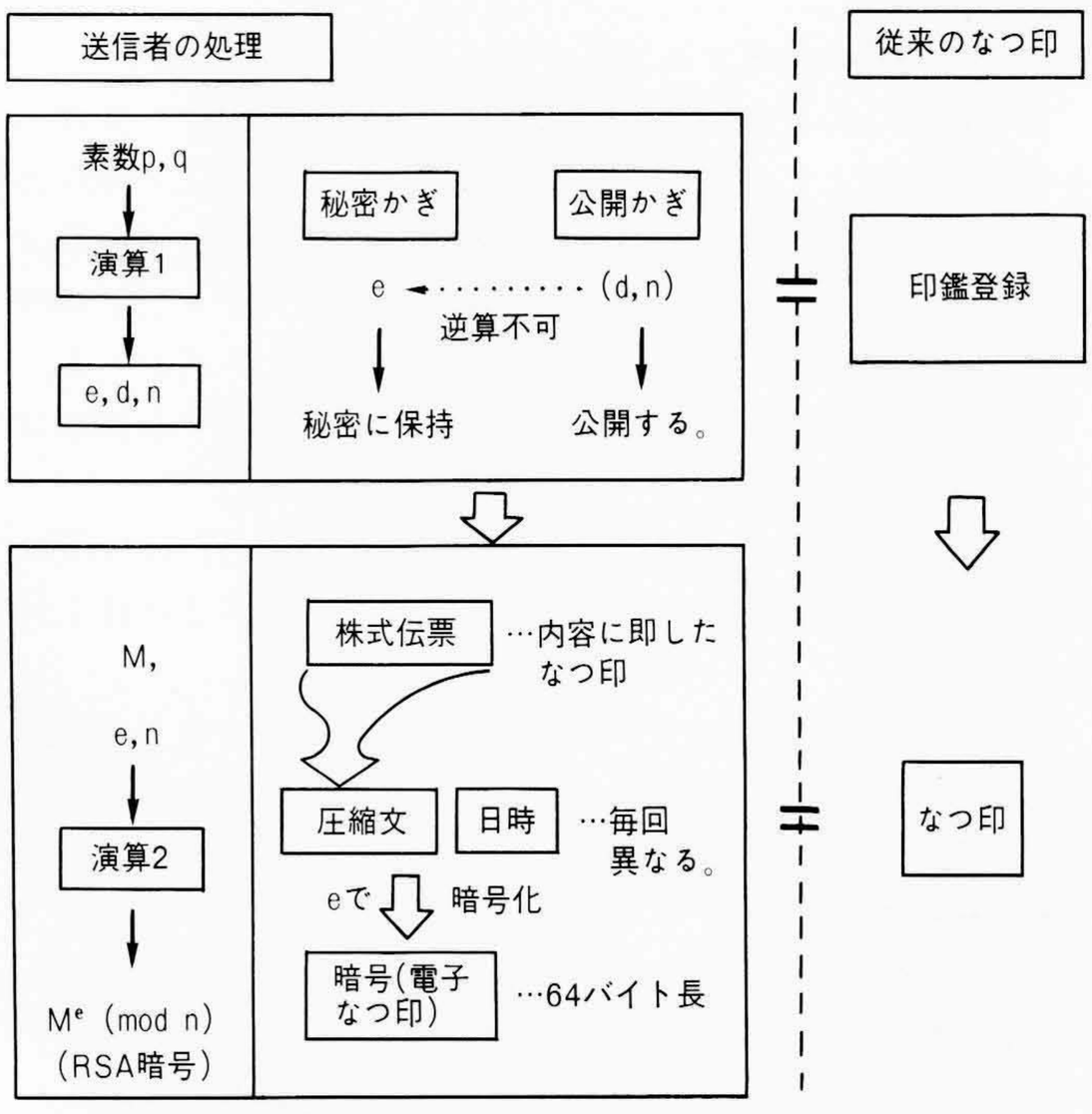
(d)　印鑑証明に相当する機能

電子なつ印を受け取った人は，登録済みの公開かぎで解読することによって，伝票の送信元及び内容を認証できる。

印鑑(山田)の要件		Hisecurity-Vでの対処方法
1	偶然一致の希少性	512ビット長の電子なつ印 2^{-512}の偶然一致確率
2	改ざん防止性 (取引相手を含む。)	公開かぎ暗号利用
3	認証性	
4	二者なつ印時の不正防止	電子仮なつ印を導入
5	使用の容易性	ハード化による高速処理

注：略語説明　Hisecurity-V(Hitachi Information SECURITY System-Verification：電子取引用認証技術)

図3　印鑑の実現に必要な要件　　漢字＋バーコードで表される電子なつ印は，64バイト(512ビット)の情報量を持つデータである。



注：略語説明　RSA暗号(Rivest，Shamir，Adlemanが考案した公開かぎ暗号方式)

図4　電子なつ印の作成手順　　送信者は，あらかじめ秘密かぎと公開かぎの組を生成し，公開かぎだけ関係者に分かるように公開する。公開かぎが公知となっても，秘密かぎの秘密は保たれる。

※)　RSA公開かぎ暗号のアルゴリズムとしての安全性は，このブロック長を持つ整数の素因数分解の困難性に依存している。このため，ブロック長を長くすればするほど(例えば，64バイト長)安全である。

これは，従来の印鑑証明に相当する。

ここまで述べた方法は，米国の大学を中心に研究が行われているディジタル署名と言われる技術に対応するものである。ディジタル署名を用いる技術は，例えばテレビショッピングのように送信者のなつ印一つだけが必要な取引に限って安全性を確保できた。

(4) 二者なつ印時の不正防止性

土地売買契約のように，両者のなつ印があって初めて契約が成立するような場合，次の問題が生じる。すなわち，書類の場合，例えば，甲がなつ印した後，乙が契約をやめたと言った場合，その書類を破棄することによってなつ印の悪用を防止できる。一方，電子取引の場合，甲が電子なつ印を通信ネットワークの向こう側に送信した後，乙がなつ印しないと言った場合，書類を破棄するようなことができない。

具体的には，甲にしてみれば，自分の電子なつ印を送った後，乙は電子なつ印を送り返さないで具合の悪いタイミングで不正使用しないか，という不安があった。乙にしてみれば，内容を了承できない甲の電子なつ印付き契約書が勝手に送られてきた場合，断りたくても甲の電子なつ印の記録を消したことを証明するのが困難であった。

電子取引手続き中のトラブルを防止するため，仮なつ印に相当する電子仮なつ印を新たに導入した(**図5**参照)。これは，仮なつ印に相当する行為を一度行って相手に契約の意思だけをあらかじめ伝えておこうというものである。そして，仮なつ印を最初に行った後，それを担保として双方の電子なつ印を交換するという手順を開発した。

ディジタルの世界でどのように仮なつ印を実現するかというと，例えば，圧縮文全体にではなく一部に対して公開かぎ暗号による暗号化を行うと電子的な仮なつ印となる。そして，仮なつ印の段階で取引を中止したい場合には，一定期間内にセンターに届ければよいようにした。このように作成される電子的な仮なつ印及びなつ印のことを電子仮なつ印及び電子なつ印と呼んでいる。

この手順に対し，種々のセキュリティ評価を行った結果，基本的に安全な取引が可能であることを確認している。

(5) 使用の容易性

本方式を実現するうえで，あい路となる事項が一つあった。それは，本方式は公開かぎ暗号という多量の計算を必要とする暗号方式を採用したため，例えば，パーソナルコンピュータで処理しようとすると5分以上かかるという問題があった。

本方式の処理を高速化するため，並列処理が容易な高速演算方式を考案し，標準的な乗算LSIや加算LSIなどを多数組み合わせて，RSA暗号処理用にボードを試作した。本試作では，0.14秒/なつ印を得，実用化可能であることを実証した。

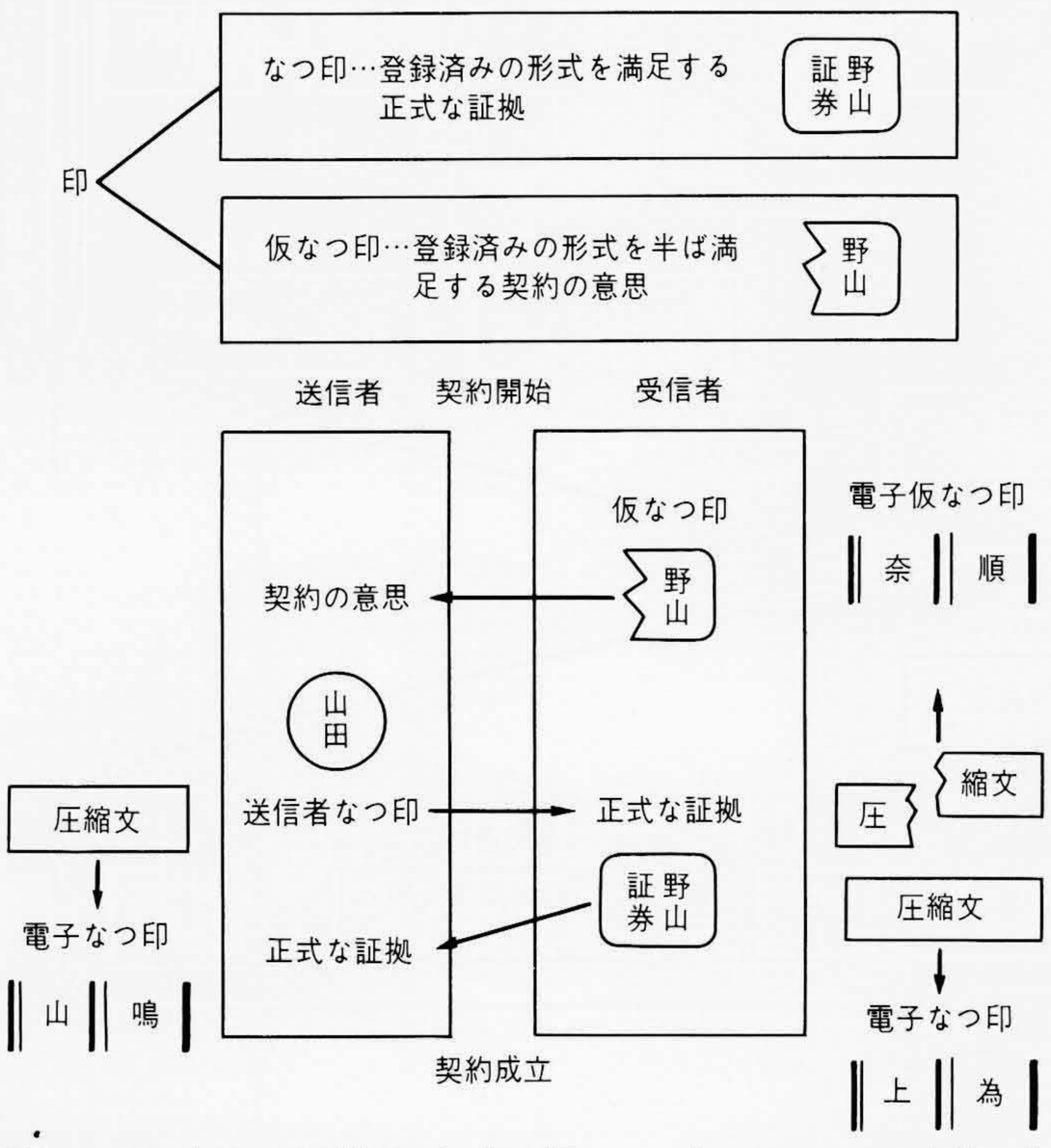


図5 電子仮なつ印利用の契約手順 正式な電子なつ印交換の前に，契約の意思の証拠となる電子仮なつ印を送っておく。電子なつ印持ち逃げなどの不正を防止する。

4 Hisecurity-Eによるセキュリティ評価

4.1 セキュリティ評価の必要性

情報システムが大衆化するに従い，不特定多数の人が一つのシステムにアクセスする場合が生じる。そのとき，第三者による不正行為や小人数のときは無視できたような小さなヒューマンエラーの確率が現実的な意味を持つ。

情報システムのセキュリティを評価する場合，次の2点を分析，評価することは重要である(**表1**)。

(1) 不正行為や誤操作に関するセキュリティ

ハッカーなどの第三者や部内者の不正行為，誤操作に対して漏れなく対策がなされているか。

(2) セキュリティ機構障害に関するセキュリティ

セキュリティ関連の機器故障やソフト的障害が生じたとき，本来の業務に支障が生じないように十分に対策が立てられているか。

従来，これらを体系的に実施する方式は提案されていなかった。

4.2 評価手順

セキュリティ評価技術Hisecurity-Eで採用している評価手順は次のとおりである[7]。

表1 事故原因分析，故障波及分析の実施優先順位 不正行為については，事故原因分析を行い，セキュリティ機構障害については，故障波及分析を行うことが重要である。

評価項目	事故原因	故障波及
	原因 → 事故故障 → 波及	
不正行為，誤操作に関するリスク評価	○ 必要性大	△
セキュリティ機構の障害に関するリスク評価	△	○ 必要性大

(1) フォルトツリー解析による不正行為成立の原因分析

不正行為成立などの不具合事象が生じるのは，どのような原因が重なったときかなどの事故原因の詳細を，フォルトツリーを用いて記述する。

(2) シーケンスツリー解析によるセキュリティ機構の故障波及分析

セキュリティ機構に関するハード・ソフト的障害が生じたとき，障害はどのように波及するか，途中で新たな障害が生じたら波及はどう変わるか，などの故障波及の全容を**図6**のシーケンスツリーのように記述する。

(3) 確率と影響の大きさを評価

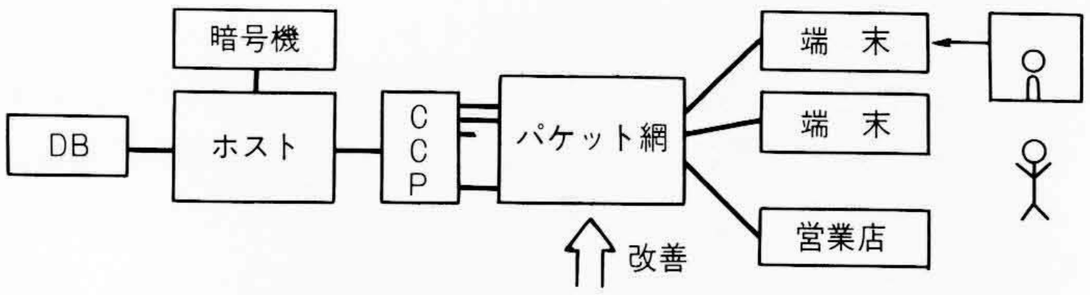
ツリーが展開されたら，事象の生起確率と大きさを与える。

(4) クリティカル事故一覧の作成

上記の解析結果を，事故の深刻度順(例えば，確率×影響の大きい順)に一覧表に整理する(**図7**参照)。

(5) 対策案の検討

事故の深刻度順に対策案を記入し，会議に提示し，採否を検討する。



クリティカルな不正行為，誤操作一覧

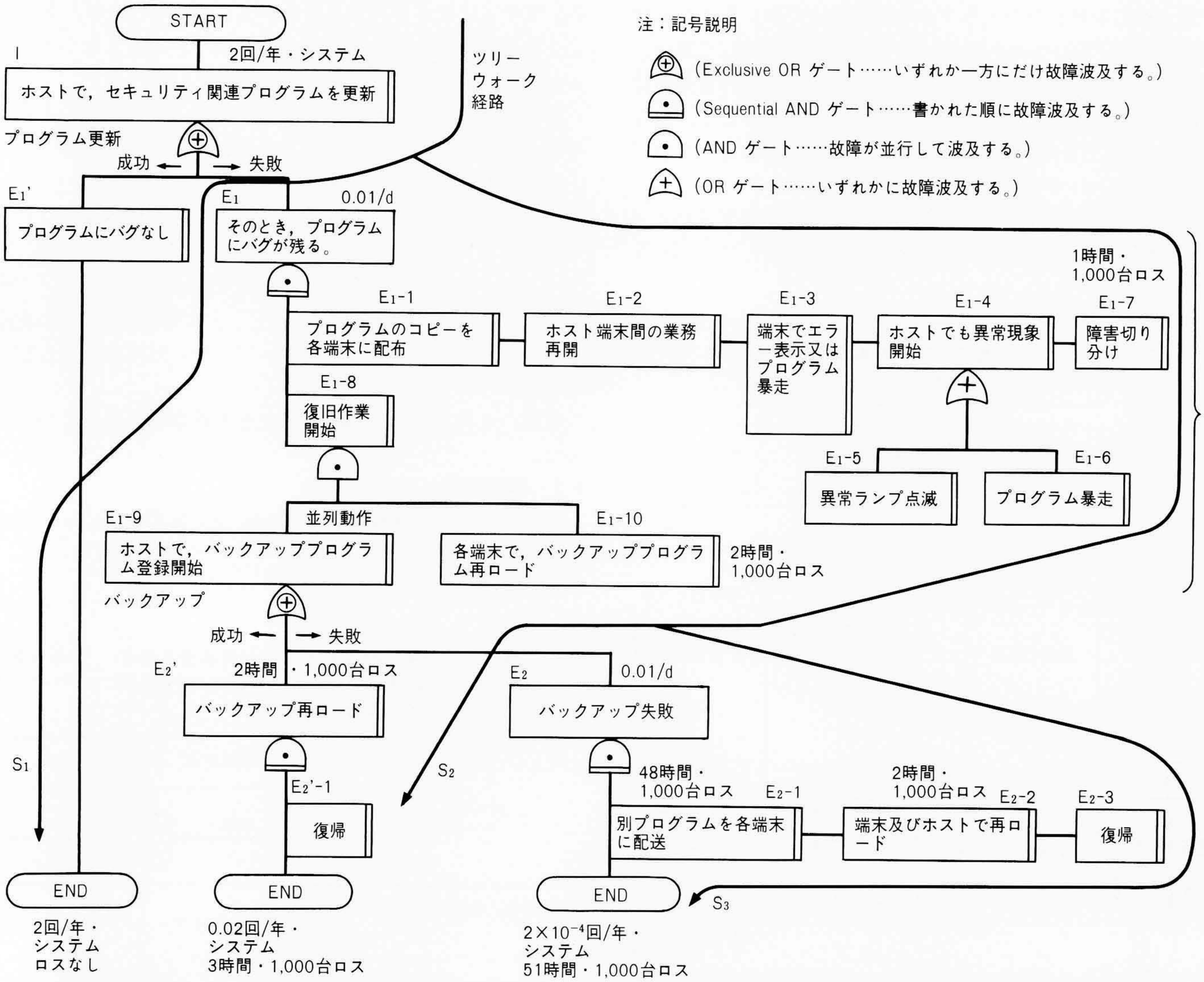
No.	事象シーケンス		個別確率	シーケンス発生頻度	検討事項
1	オペレータの操作ミス	操作ミス	1×10^{5} 回/年システム	5回/年	(1) チェック機能の
		マシンチェックにかからない。	0.5		

クリティカルなセキュリティ障害一覧

No.	障害内容	発生頻度	影 響	検討事項
1	暗号かぎDB破損	0.5回/年	2,000台	DB二重化

注：略語説明 DB(データベース)，CCP(通信制御処理装置)

図7 セキュリティ評価技術Hisecurity-Eの出力イメージ 最もクリティカルな不正行為，セキュリティ機構障害から順に出力される。分析結果がシステムの改善に用いられる。



注：記号説明

(Exclusive OR ゲート……いずれか一方にだけ故障波及する。)

(Sequential AND ゲート……書かれた順に故障波及する。)

(AND ゲート……故障が並行して波及する。)

(OR ゲート……いずれかに故障波及する。)

図6 故障波及分析用シーケンスツリーの例 いちばん上側の事象を初期事象として，各ゲートの規則に従って，故障が波及することを表現する。

Hisecurity-Eを用いた定量的なセキュリティ評価により，セキュリティ対策上のキーポイントの発見が可能になる。実際の適用で具体的改善策を得るという効果を得ている。

5　株式売買への適用例

現在，株式売買では，投資家が証券会社に電話して株の売買を依頼するという注文の仕方が採用されている。しかし，今後は，通信技術の進展に伴い，電話でなくパーソナルコンピュータなどの通信端末を使って，注文伝票をディジタルの信号で送るようになると予想される。

電子取引用認証技術Hisecurity-Vの理解を助けるための適用例として，株式売買を取り上げ，運用方法と効果について述べる。

株式売買システムの構成例を**図8**に示す。本システムで，投資家と証券会社の間で株式売買を行っている。調停者はトラブル時以外は介入しない。ここで，調停者は，公平な立場で後で詳しく述べるトラブル時の調停を行う人，又は機関のことである。

株式売買の手順を次に述べる。

(1)　ICカードセット

投資家はICカードをセットし，暗証符号を入力する。これにより，ICカード内の秘密かぎが電子なつ印装置に設定され，電子仮なつ印及び電子なつ印作成用の暗号かぎとして用いられる。このICカードは投資家の印鑑に相当する。

(2)　株式注文伝票の作成

投資家は，株式注文伝票をパーソナルコンピュータを用いて作成し，証券会社に送信する。

(3)　電子なつ印交換

証券会社から株式注文に応じる意思を示す電子仮なつ印が送られた後，双方の電子なつ印が交換され，伝票に表示される(**図9**)。

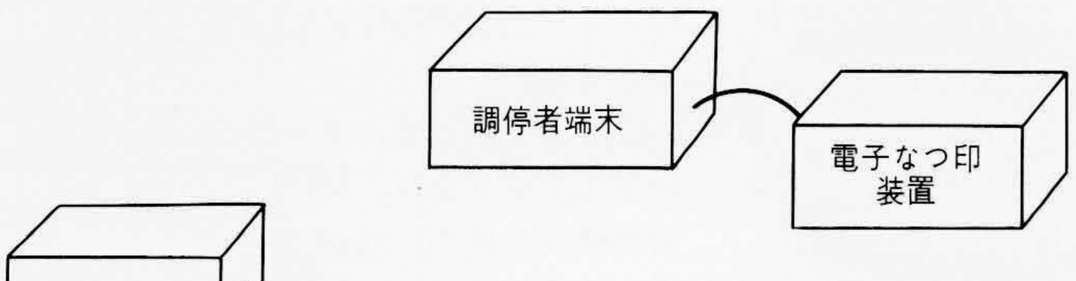


図8　株式売買システムの構成例　　公衆回線を介して，投資家と証券会社が株の売買を行う。両者は各々(秘密かぎ，公開かぎ)の組を生成し，公開かぎだけを調停者に届けておく。

トラブル発生時の調停例を次に述べる。

電子なつ印交換中になつ印を持ち逃げするなどのトラブルが生じた場合，電子仮なつ印を調停者に提示させることによってどちらが不正であるかが判定できるので，トラブルは解決される[6]。

電子なつ印交換後は，電子なつ印付きの注文伝票を保持していれば，その伝票はだれがいつなつ印したものであるかを証明することができる。その伝票は改ざんできない。

電子なつ印交換後のトラブルの一例として，投資家が不正をして，もとの伝票が9万株の「売り」であったものを9万株の「買い」に改ざんして，証券会社にクレームを付けた場合を考える。このとき，トラブルはどのように解決されるかを次に示す(**図10**)。

(1)　双方の立会いのもとで，改ざんされた伝票を調停者の端末に入力する。

図9　電子なつ印を押し合った状態の注文伝票　　投資家山田桃太郎と証券会社野山証券株式会社は，異なる秘密かぎで電子なつ印を作成するので，それぞれ異なった漢字＋バーコードとなる。

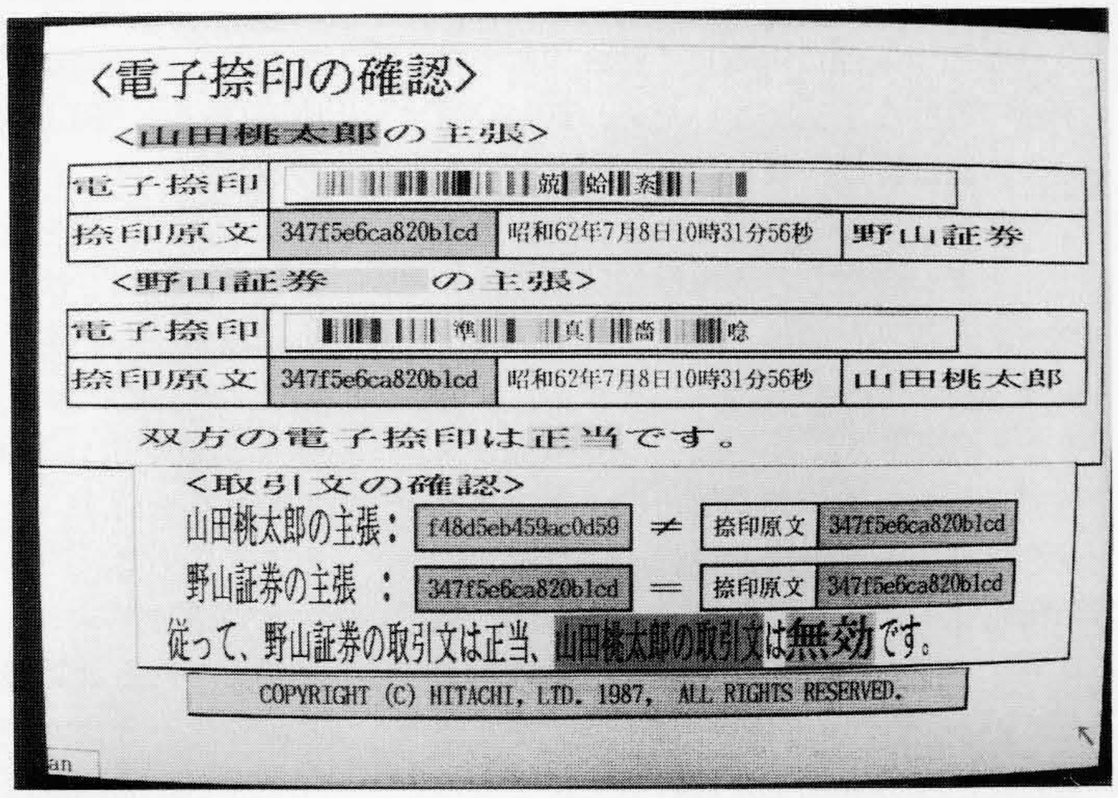


図10　調停者端末での不正伝票検査結果　　調停者の端末は，入力された電子なつ印付き電子伝票を検査する。改ざんされた伝票はなつ印原文と矛盾することを検出する。

(2) 調停者の端末は，登録済みの山田桃太郎の公開かぎと野山証券株式会社の公開かぎを用いて，双方の電子なつ印を復号化する。復号化結果，圧縮文及び時刻データは一致するので，電子なつ印は正当であることが認められる。
(3) 次に，改ざんされた伝票の圧縮文を作成し，それと先ほど復号化された電子なつ印の原文に含まれている圧縮文とを比較し，双方が一致しないことから投資家の伝票は無効であると判断し，表示する。

株式売買にHisecurity-Vを適用すると次の効果が得られる。

(1) 投資家の手間は，銘柄，金額などを指定し，ICカードをセットし，暗証符号を入力するだけなので，使用時の手間は銀行キャッシュカード使用時の手間と同等である。
(2) 契約の意思のある場合だけ，電子仮なつ印を用いる手順となっているので，証券会社は電子仮なつ印を送らないことによって投資家の注文を断ることができる。
(3) 注文修了後，投資家は株式売買を注文した事実を否認できない。証券会社は投資家の注文を引き受けた事実を否認できない。
(4) 証券会社の社員すべてが，投資家の注文伝票を偽造していないことを証明できる。

6 結　言

日立製作所のネットワーク セキュリティ技術として利用者総合管理機能TRUSTと日立情報セキュリティシステムHisecurityの技術内容，及び特徴について述べた。

今後，情報システムのいっそうの高度化，普及化に伴い，ネットワーク セキュリティ技術の重要性が増大すると予想される。これにこたえられるように，ネットワーク セキュリティ技術を発展させていきたいと考えている。

最後に，セキュリティ技術の研究開発で御指導，御協力いただいた関係各位に深謝申し上げる。

参考文献

1) NHK放送研修センター編：狙われるコンピュータ，日本放送出版協会(昭62-1)
2) 日立製作所：プログラムプロダクトVOS3総合利用者管理機能，TRUST，エンドユーザ向け使用の手引，8090-3-352-10(昭61-12)
3) 一松，外：データ保護と暗号化の研究，日本経済新聞社(昭58-7)
4) 白石：積暗号アルゴリズムの解析，電子通信学会論文誌，'86/12 Vol. J69-A No.12，1564～1570(昭61-12)
5) 前田，外：ディジタル画像に適したデータ暗号化の一方法，電子通信学会論文誌，'86/11 Vol. J69-B No.11，1385～1392(昭61-11)
6) 宝木，外：ICカード利用の電子取引用認証方式，電気学会論文誌C分冊，107巻，1号，46～53(昭62-1)
7) 宝木，外：情報システムにおけるセキュリティ評価方法—電子認証システムへの適用例とともに—，1987年暗号と情報セキュリティワークショップ講演論文集，電子情報通信学会情報セキュリティ時限研究専門委員会，CIS研究会，35～49(昭62-7)

論文抄録

2次元解析の拡張によるある種の鍛伸加工問題の解析

日立製作所　田中伸司・佐藤一雄

日本塑性加工学会誌　28—314，257～263 (昭62-3)

塑性加工プロセスの開発・設計を行うには，プロセス中の被加工材の塑性流動を正確に把握することが不可欠である。従来，多様な加工条件に対処して塑性流動を解析する一般的な手法がないため，新しいプロセスの設計には，長期にわたる試行錯誤的な実験が必要とされてきた。一方，最近では，チタン合金などの恒温鍛造加工をはじめとする新素材の加工プロセスの開発で，被加工材内部の材質の変化を精密に予測することが要求されている。以上の背景から，被加工材の塑性流動を解析的に予測する手段を確立することは，従来のプロセス設計の精密化・迅速化だけにとどまらず，新プロセスを開発する上で重要な技術課題となっている。筆者らは，これを解決する手段として，多様な加工条件に対処できるはん(汎)用解析システム(シミュレータ)の開発を進めてきた。これまでに，剛塑性有限要素法を改良して，軸対称，平面ひずみ変形などの2次元問題に対処できる鍛造解析シミュレータ“PLUM”を開発した。

本論文では，新たに棒材の鍛伸加工のような3次元問題を近似的に解析する手法を提案し，先の2次元シミュレータの機能を更に拡張した。本手法の特徴は「一般化平面ひずみ」，すなわち2次元変形する平面に垂直なZ方向に，全面にわたって均一なひずみの存在を許す，という変形モデルを用いることにある。この結果，将来の完全な3次元鍛造加工シミュレータを実現する上で必要とされる計算機の大容量化，計算速度の高速化，3次元変形処理アルゴリズムの開発などの諸問題の解決をまたずに，ある種の3次元変形問題に対処することが可能となった。

解析の例として，タービンブレードの鍛伸加工を取り上げ，円形断面及び長方形断面の棒状の被加工材が，工具の空洞部に充満する過程のシミュレーションを行った。解析の結果，所望のタービンブレードの形状を得るための，加工中に軸方向へ与えるべき最適なひずみ速度，及び軸力のスケジュールを得ることができた。また，被加工材の断面形状が製品のひずみ分布に及ぼす影響や，加工中にマニピュレータに作用するトルクの有無，軸力の大きさの変化など，鍛伸加工プロセスの設計に有力な知見を得ることができた。