U.D.C. 〔336.717:65.011.54:681.322.022〕:65.012.8

金融機関におけるシステムセキュリティ技術

Security Techniques for Financial Systems

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

金融機関でコンピュータネットワークの利用が拡大するなかで，人間の誤操作や意図的な不正行為に対するセキュリティ対策への関心が高まっている。日立製作所もこのような時代に対応し，日立情報セキュリティシステムHisecurityなどの名のもとに評価，認証，アクセス管理，暗号などを行う種々の技術を開発している。本稿は，金融機関でのセキュリティ対策の現状と日立製作所の対応としてのHisecurityなどの概要を述べる。また，リスクの発見と評価を計算機支援により効率的に行うセキュリティ評価技術Hisecurity-Eと，その金融機関への適用結果を紹介する。

1 緒　言

近年，金融機関の業務が高度化，広域化するにつれて，電子伝票などのデータの送信，蓄積などを高速かつ確実に行いたいという要求が増大している。一方，これらの要求を満足するうえで中心的な役割を担うコンピュータの利用は，ひとつ間違えば大きなマイナス要因になる可能性があると指摘されている[1]。そこで，コンピュータを結ぶ通信網とデータベースを単に効率の良いものにするだけでなく，これらの設備をいかにして安全に使用できるようにするかが大きな課題となっている。

本稿では，コンピュータの利用に関する安全性，特にコンピュータの不正使用などに対するセキュリティについて述べる。

昭和46年から昭和60年までの間に，我が国で警察が把握した不正データ入力などのコンピュータ犯罪は58件という数になっている。この件数は昭和46年から昭和55年までの10年間に起きた件数が14件であったのに対し，そのあとの5年間で44件が発生するというように，最近になってコンピュータ犯罪が増える傾向を示している[2]。米国では，昭和45年ごろからコンピュータ犯罪が増加し始め，昭和60年までに累計1,000件を超えるコンピュータ犯罪が報告されている。更に，実際に生じた犯罪件数はこれらの数値の6～7倍，あるいはそれ以上であるとも言われている。

このようなコンピュータ犯罪の脅威から情報を保護するため，特に銀行業務の分野で情報セキュリティ技術の標準化が進んでおり，ISO (International Organization of Standardization：国際標準化機構)で暗号を用いたデータ認証手順などが標準化されている[3]。また，欧米先進国の銀行などで，暗号機，ICカードなどの情報セキュリティ関連機器が導入されつつある。我が国の金融機関でもセキュリティに対する関心が高まっており，送信者認証などのセキュリティ対策の実施は増える傾向にある。

日立製作所もこのような時代に対応して，Hisecurity (Hitachi Information SECURITY System：日立情報セキュリティシステム)の名のもとに種々のセキュリティ確保技術を開発中である(**表1**)。Hisecurityの技術一般については，昭和62年9月号の本誌[4]に詳しく述べているので参照されたい。Hisecurityの技術は，金融機関などで種々のセキュリティ対策を行うため有効に活用されることを目指している。特に，セキュリティ評価技術Hisecurity-E(Hisecurity-Evaluation)[5]は金融システムに対し適用実績があり，セキュリティ対策を検討するうえでの基本となる。

以下では，我が国の金融機関でのセキュリティ対策の現状と日立製作所の対応として上記Hisecurityの概要を説明する。また，Hisecurity-Eについては計算機支援ツールの開発と金融機関への適用結果を紹介する。

2 金融機関におけるセキュリティ対策の現状

金融機関のセキュリティに対する脅威は**図1**に示すように大きく分けて二つ存在する。一つはプログラム改ざんなどの意図的なものであり，他の一つは地震，火災などの偶発的なものである。

特に，**図1**の網目部分は人間の意図的，偶発的行為及びその対策用のセキュリティ機能の障害に関するもので，近年のコンピュータ利用の大衆化によって，新たにクローズアップされてきたセキュリティ上の脅威である。

本章では，この網目部分のセキュリティ上の脅威に的を絞って述べる。

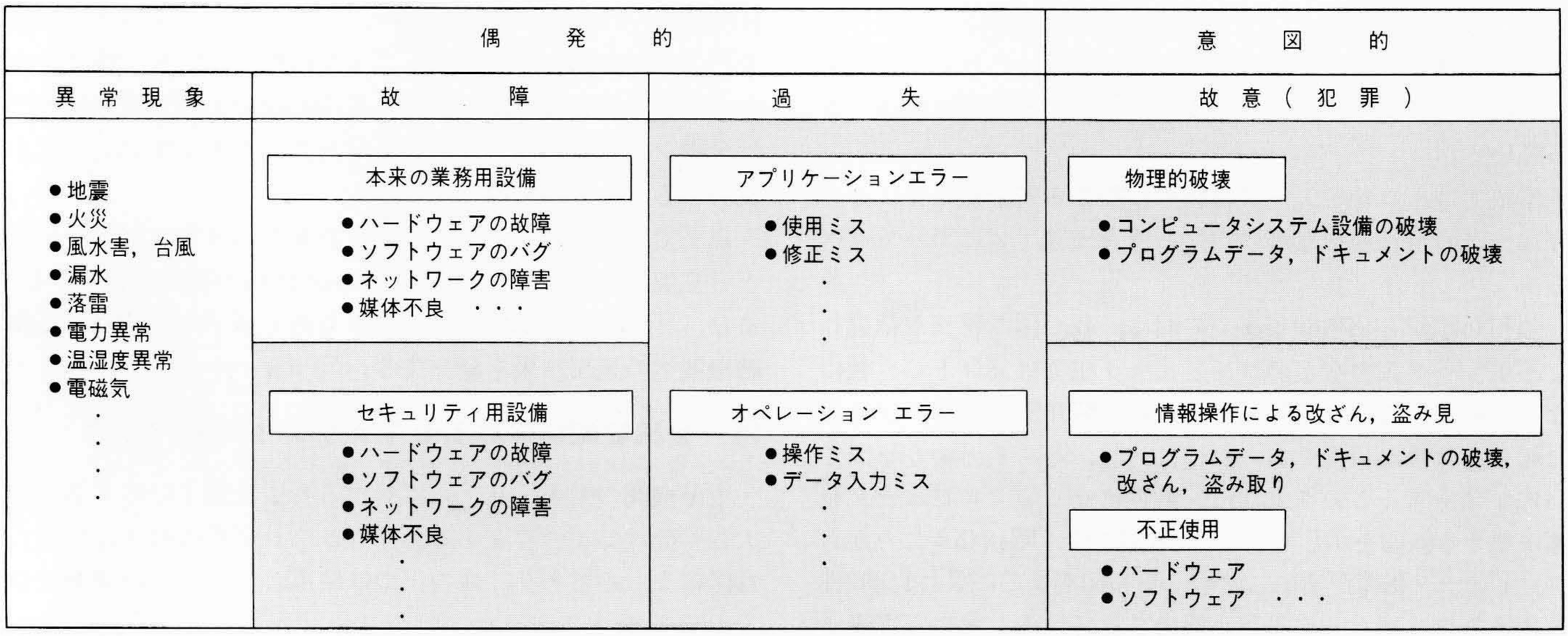
一般に，コンピュータセキュリティ対策のあり方について各省庁(通商産業省，郵政省，大蔵省，自治省，警察庁など)やその関係団体で行政面から検討が行われ，既に幾つかのガイドラインが公表されている[1]。例えば，金融情報システムセンターの安全対策基準[6]によれば，計算機室，伝送路，端末な

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

表1 セキュリティ上の脅威と対策技術 パスワードなどによるアクセス管理(TRUST)と暗号化，認証，評価などの各種セキュリティ機能(Hisecurity)の組合せにより，必要なセキュリティを確保する。

対策技術項目 / 日立製作所の技術 / セキュリティ上の脅威	利用者管理	資源アクセス管理	データ秘匿	データ認証	予測・評価	監視・記録	物理的な保護
	かぎ管理技術 Hisecurity-M（複数計算機間の通信時に使用）		（暗号かぎの生成，配送，管理用）		セキュリティ評価技術 Hisecurity-E	必要に応じて実施	
	総合利用者管理機能TRUST（一つの計算機内での管理に使用）		文書，画像，音響暗号技術 Hisecurity-D, -I, -S	電子取引用認証技術 Hisecurity-V			
計算機の不正使用，破壊・誤操作	○	○	—	—	○	○	○
データの盗み見	○	○	○	—	○	○	○
データの破壊，改ざん	○	○	○	○	○	○	○
通信事実・内容の事後否認	—	—	—	○	○	○	○

注：略語説明 TRUST(Total Resource and User Control Facility：総合利用者管理機能)
Hisecurity(Hitachi Information SECURITY System：日立情報セキュリティシステム)
Hisecurity-D (Hisecurity-Data Encryption：文書データ暗号技術)
Hisecurity-I (Hisecurity-Image Encryption：画像暗号技術)
Hisecurity-S (Hisecurity-Sound Encryption：音響暗号技術)
Hisecurity-V (Hisecurity-Verification：電子取引用認証技術)
Hisecurity-M(Hisecurity-Management：かぎ管理技術)
Hisecurity-E (Hisecurity-Evaluation：セキュリティ評価技術)



注：墨網部分（本稿で対象とするセキュリティ上の脅威）

図1 金融機関におけるセキュリティ上の脅威とHisecurityの適用範囲 コンピュータ利用の普及化に伴い，網目部に示す人間の誤操作あるいは不正行為に関するセキュリティ上の問題がクローズアップされている。

どの広い範囲にわたって具体的なセキュリティ対策が示されている。

昭和60年に我が国の主要な企業に対して情報処理振興事業協会が調査したコンピュータセキュリティ対策の実施状況の一部を**図2**に示す[1]。同図に示すように，金融機関については85％以上が既に認証，モニタリングをなんらかの形で実施しており，更に69％はアクセス権制御を，41％は暗号化を実施しているとされている。ここで，認証はパスワード又は暗証番号を用いるものが大部分であり，モニタリングは使用したユーザーや端末が分かるようにするものがいちばん多い。また，アクセス権制御はユーザー別，プログラム単位で行われるものが多く，暗号化は独自のアルゴリズムを用いるものが多いとされている。

次に，同調査による業種別セキュリティ対策投資予定をまとめたものを**図3**に示す。これによると金融機関の30％は「多少費用がかかってもやる」としており，通信・情報の34％に次いでセキュリティ対策に積極的な傾向を示している。

総じて，金融，通信情報の分野ではセキュリティに対して

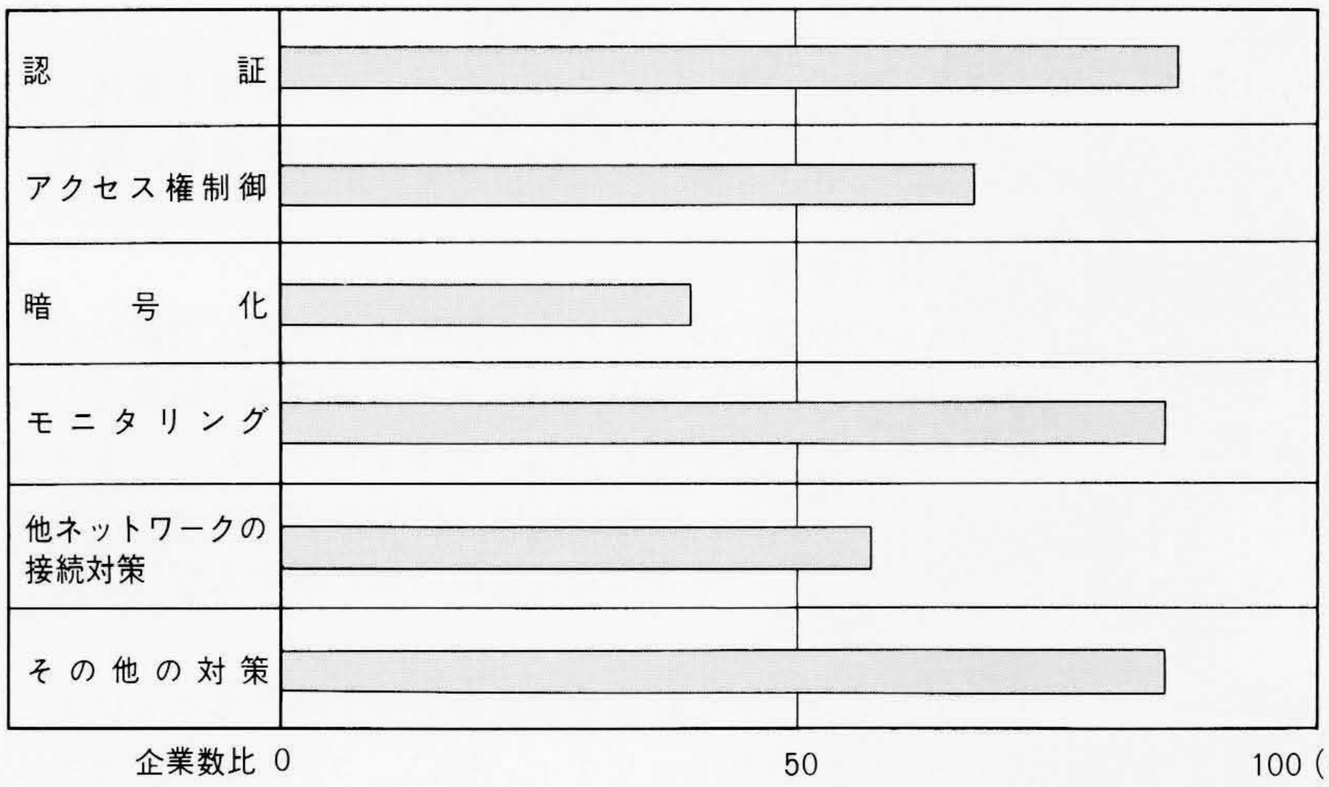


図2　金融機関におけるセキュリティ対策実施状況　　昭和60年に我が国の主要な企業に対して情報処理振興事業協会が調査したコンピュータセキュリティ対策の実施状況を示す。

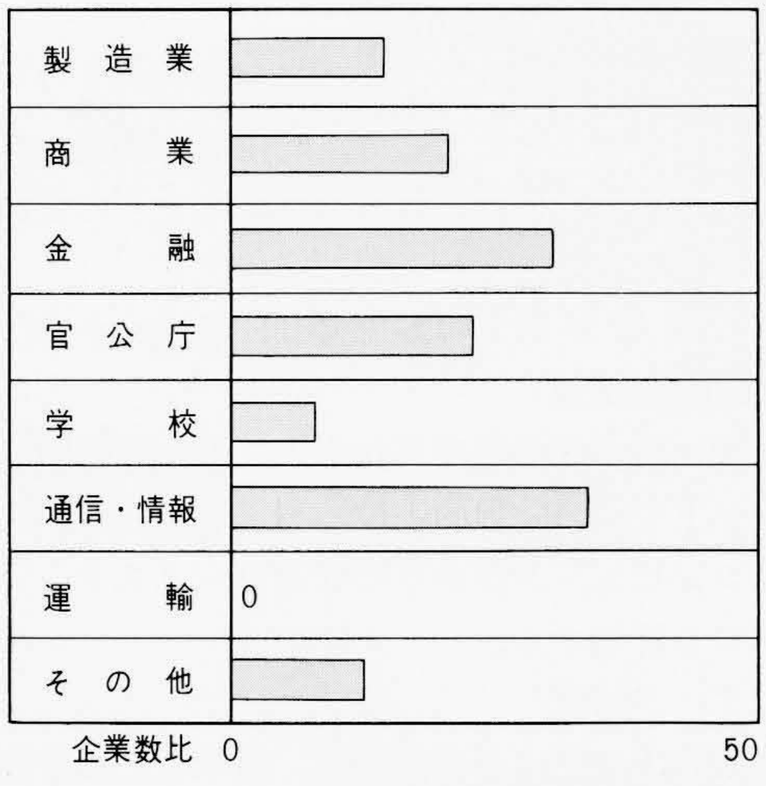


図3　セキュリティ対策投資予定「多少費用がかかってもやる」と答えた企業の業種別の割合
　昭和60年に，我が国の主要な企業に対して情報処理振興事業協会が調査した業種別セキュリティ対策投資予定を示す。

関心が深く，認証，アクセス権制御，モニタリングが実施されている割合が高い。また，実施率がまだ低いものとして，ネットワーク相互接続を意識した対策や暗号化などがあるが，今後の課題であると認識されている。

3　日立製作所のセキュリティ技術の概要

2章で述べた種々のセキュリティ対策を実現するうえでの基本的な考え方と，日立製作所の技術内容について述べる。

まず，セキュリティ対策を考えるとき，コストとリスクの観点からバランスのとれたものを選定することが重要である。ここでリスクとは，将来に対するものごとの悪い面からみた指標であり，例えば，「事故の発生頻度×影響の大きさ」で示される。

図4は，リスクを考慮した場合の意思決定の手法[7]の一部を示しており，種々の設備，運用案に対するコストとリスクの関連を描いた関連図である。ここで，意思決定は次のように行われる。つまり，種々の設備，運用策に対してコスト及びリスクが評価され図に記入される。これらの案のうち，コストが許容範囲(同図の網目部分)に入っているものについて，リスクが最小となる最適解，リスクが二番目に小さい準最適解などが選定される(コスト制約下のリスク最小化問題)。そして，選定結果は意思決定会議に提示され，最終的に意思決定される。

このようにセキュリティ対策を考える場合，リスクの発見と評価を行うことがまず重要であり，その後，適切な選択が行われる。したがって，リスク分析を行う手法の開発とリスクを軽減するための代替案として種々のセキュリティ確保技術をそろえることが必要である。

上記の考えと2章で述べたセキュリティ対策の動向を踏まえ，日立製作所が開発している種々のセキュリティ確保技術を**表1**に示す。

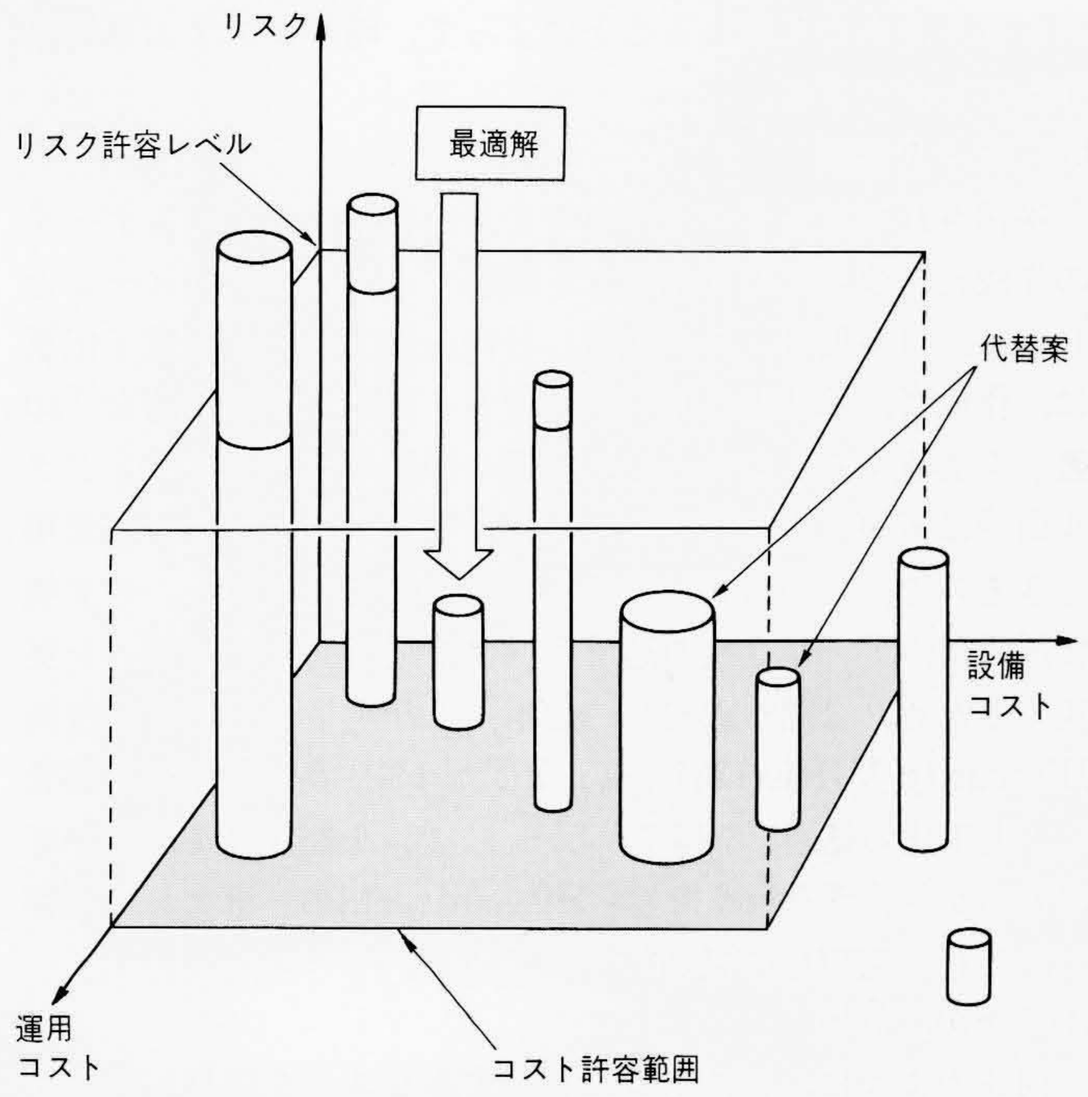


図4　コスト-リスクを考慮した意思決定の一例　　コスト許容範囲あるいはリスク許容範囲に入る代替案のうち，最適解，準最適解などが選ばれ意思決定者に示される。

(1)　利用者管理，資源アクセス管理

不特定多数の利用者がCD(Cash Dispenser)，POS(Point of Sales)端末を利用する場合や，ホストコンピュータをTSS(Time Sharing System)の端末から使用する場合などで，利用者を確認したり，計算機をある範囲内に限定して使用することを許可する。日立製作所では，次の二つの技術により，利用者管理，資源アクセス管理を行うことを可能にしている。

(a)　総合利用者管理機能TRUST(Total Resource and

User Control Facility)[8]

一つの計算機内で，主に識別子とパスワードを利用者に入力させることによって，利用者を識別し確認する。その後，利用者に応じてデータベースなどの資源へのアクセスを管理する。

(b) 暗号かぎ管理技術Hisecurity-M (Hisecurity-Management)

強い安全性を要求される複数の計算機間通信で，主にICカードなどの物理的手段で利用者を確認する。また，ホストコンピュータばかりでなくワークステーションへのアクセスを管理する。

(2) データ秘匿

通信路上のデータや計算機，端末などに蓄積されたファイルデータを暗号化する。日立製作所は，コンピュータメッセージや文書データを暗号化する文書データ暗号技術Hisecurity-D(Hisecurity-Data Encryption)[9]，画像データを暗号化する画像暗号技術Hisecurity-I (Hisecurity-Image Encryption)[10]，音声，音響データを暗号化する音響暗号技術Hisecurity-S(Hisecurity-Sound Encryption)を開発している。これらと暗号かぎの管理を行うかぎ管理技術Hisecurity-Mを組み合わせて用いることによって，暗号システムを構築することができる。

(3) データ認証

送信されてきたデータやファイルに蓄積されているデータの作成元，改ざんの有無などを確認する。具体的イメージとしては，口座振替，株式売買，社内決済文書などの電子伝票に，作成者，承認者，取引内容などを保証する電子的な「印鑑」を実現する。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，だれでも簡単にコピーし再使用できるので，この方式とは違った特別の工夫を行う。日立製作所では，ディジタルの通信データで電子的な「印鑑」を実現するため，公開かぎ暗号の応用により電子取引用認証技術Hisecurity-V(Hisecurity-Verification)[11]及び試作機を開発し，実用化の見通しを得ている[12]。また，上記試作で公開かぎ暗号のかぎ管理を行う機能もHisecurity-Mの一部として試作し，これも実用化の見通しを得ている。

(4) 予測，評価

前述のように，システムに存在するリスクを発見し評価することは，セキュリティ対策の検討を行ううえでまず必要である。そこで，事故の原因を分析し，その発生の可能性はどの程度かを評価する事故原因分析と，逆に，不当行為やシステム内の障害などが波及して思わぬ事故につながらないかなどを評価する事故波及分析を実施する。

セキュリティ評価技術Hisecurity-Eは，(a)不当行為，誤操作に対して本当に安全か，対策に漏れはないか，(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。これについては**4**章で詳述する。

(5) 監視，記録

不当行為防止策などのセキュリティ対策に一見すき(隙)があるような場合でも，行為者は後で必ず判明し罰せられるという状況下では，不当行為は生じにくい。また，不当行為が生じた場合に，即座にアラームなどで検知されるようにしておくことも有効である。そこで，システムの状態を監視，記録し，不当行為が生じた場合，その発生箇所を追跡，確定，対処する。

(6) 物理的な保護

外部からの破壊，侵入に対する物理的ガード，内部からの破壊，障害に対する二重化，バックアップ機器の設置などの物理的な保護対策は有効であり，従来からなされているセキュリティ対策である。具体的には，計算機を強固な建造物に収める，端末操作パネルに錠付き扉のふたをするなどの手段がある。

上記(1)～(6)で述べた技術を組み合わせて用いることによって，金融機関でのセキュリティ，特に，コンピュータセキュリティを確保することが可能になる。

4 セキュリティ評価技術の金融システムへの適用

表1の対策技術項目のうち,「予測・評価」を行うセキュリティ評価技術Hisecurity-Eについて述べる。これは，情報システムに存在するリスクの発見と評価を行うものであり，セキュリティ対策の検討を行ううえで，まず実施されるものである。Hisecurity-Eの基本方式については既に別文献[5]で詳しく述べているので，ここではその概略を説明した後，今回新たに開発したセキュリティ評価支援用ツールとその適用結果を紹介する。

4.1 セキュリティ評価技術Hisecurity-Eの基本方式

Hisecurity-Eは，**図5**に示すように2種類の分析を行う。

(1) フォルトツリー分析

生じては困るような事故の原因をツリー状に展開し，分析する。

(2) シーケンスツリー分析

電源断などのシステム内外の変化を出発点として，どのような経過で事故に波及し得るかをツリー状に展開し，分析する。

例えば，ある債券を通信ネットワークを介して売買する業務があったとする。ここで，生じ得ると考えられる事故の原因及びその発生頻度を予測するため，フォルトツリーを展開する。フォルトツリーを展開することによって，例えば，トップイベント「債券売買業務で，誤操作，障害による事故発生」の原因として債券登録中にセンターダウンが発生し，そのとき，営業店のオペレータが対処しそこなうというダブルミスがクリティカルになっていることなどが分かる。更に，その結果として年に5回の頻度でセンターに登録されていない客が換金に来るという事態の発生などが予測される。

一方，シーケンスツリーはこれとは逆に，例えば，センターダウンが発生したときに，前記債券売買のほかどのような業務にどういう影響を与え得るかという事故波及の全容を描く。

フォルトツリーとシーケンスツリーを組み合わせて用いることにより，情報システムの複雑な動作に対する分析が可能になるとともに，安全対策上のキーポイントや安全上不必要にコストが費やされている部分を発見することが可能になる。

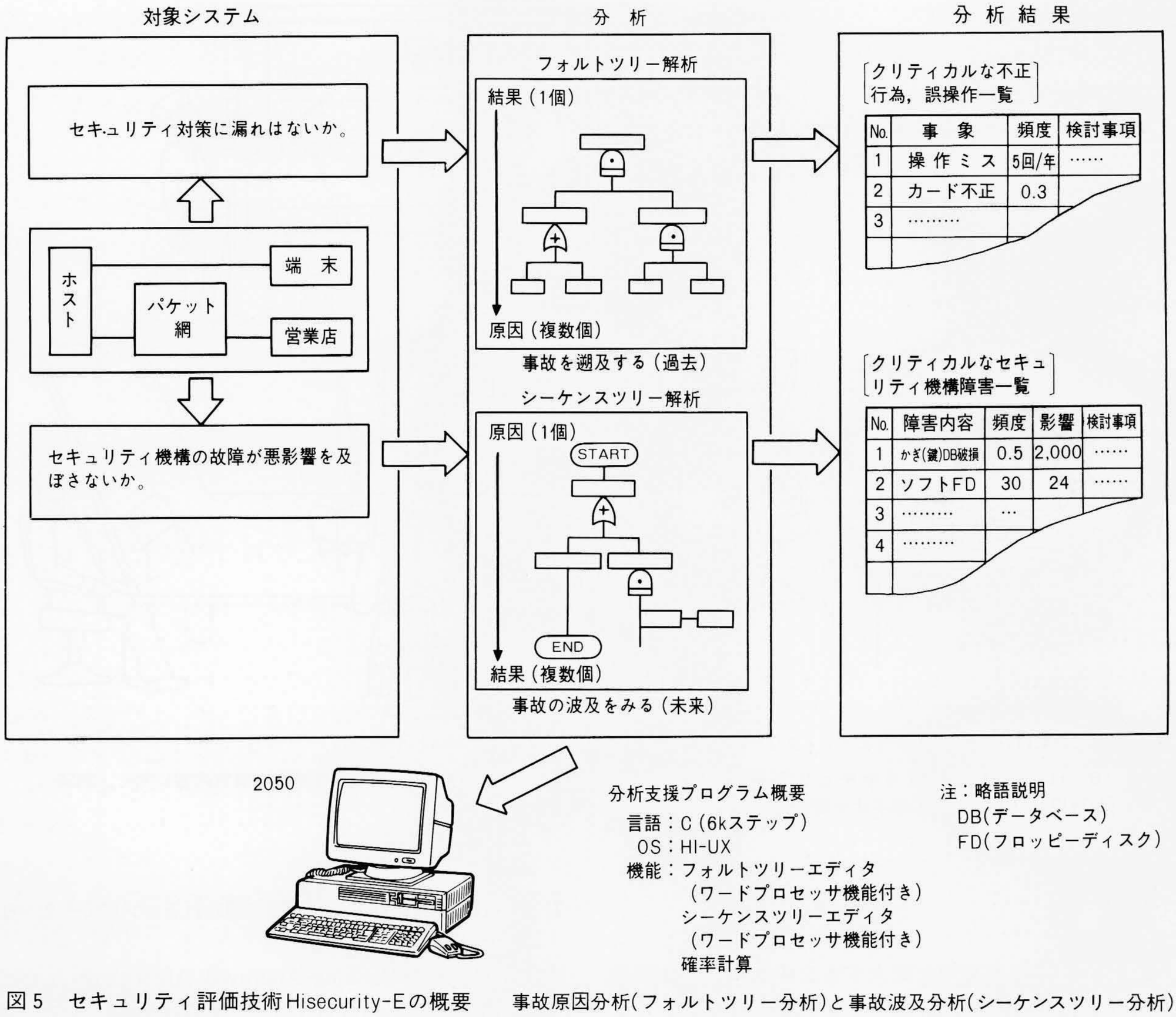


図5　セキュリティ評価技術Hisecurity-Eの概要
を計算機(2050)支援で行う。

4.2　解析ツール

情報システムのセキュリティ評価を行ううえであい(隘)路となるのは，解析のためのマンパワーが大きいことである。そこで，解析効率を向上させる計算機支援プログラムを開発した。本プログラムは，クリエイティブワークステーション2050(以下，2050と略す。)上で動作し，マウス，キーボードを用いて，フォルトツリー，シーケンスツリーの作図，修正，確率の計算などを行う(**図5**)。

本プログラムを用いてセキュリティ評価を行う一形態を**図6**に示す。2050及び会議で使用する電子黒板とOHP(オーバヘッドプロジェクタ)を用い，数人から十数人が参加して行う。

その使用方法と特徴は次のとおりである。

(1)　解析の途中経過で，司会者は参加者の発想を直ちに電子黒板に書き込む。これにより，全員のチェックが直ちに受けられ解析作業がスムーズに進む。

(2)　電子黒板に書き込まれた手書きの解析内容は，2050及び専用ソフトに備付けの機能を用いて活字化する。更に，活字化された解析内容はOHPを用いて電子黒板に再表示する。これにより，参加者はきれいに清書された解析内容を見ながら解析内容を再検討できるとともに，手書きのままの表示に比べて思考の整理，解析漏れの発見などが促進される。

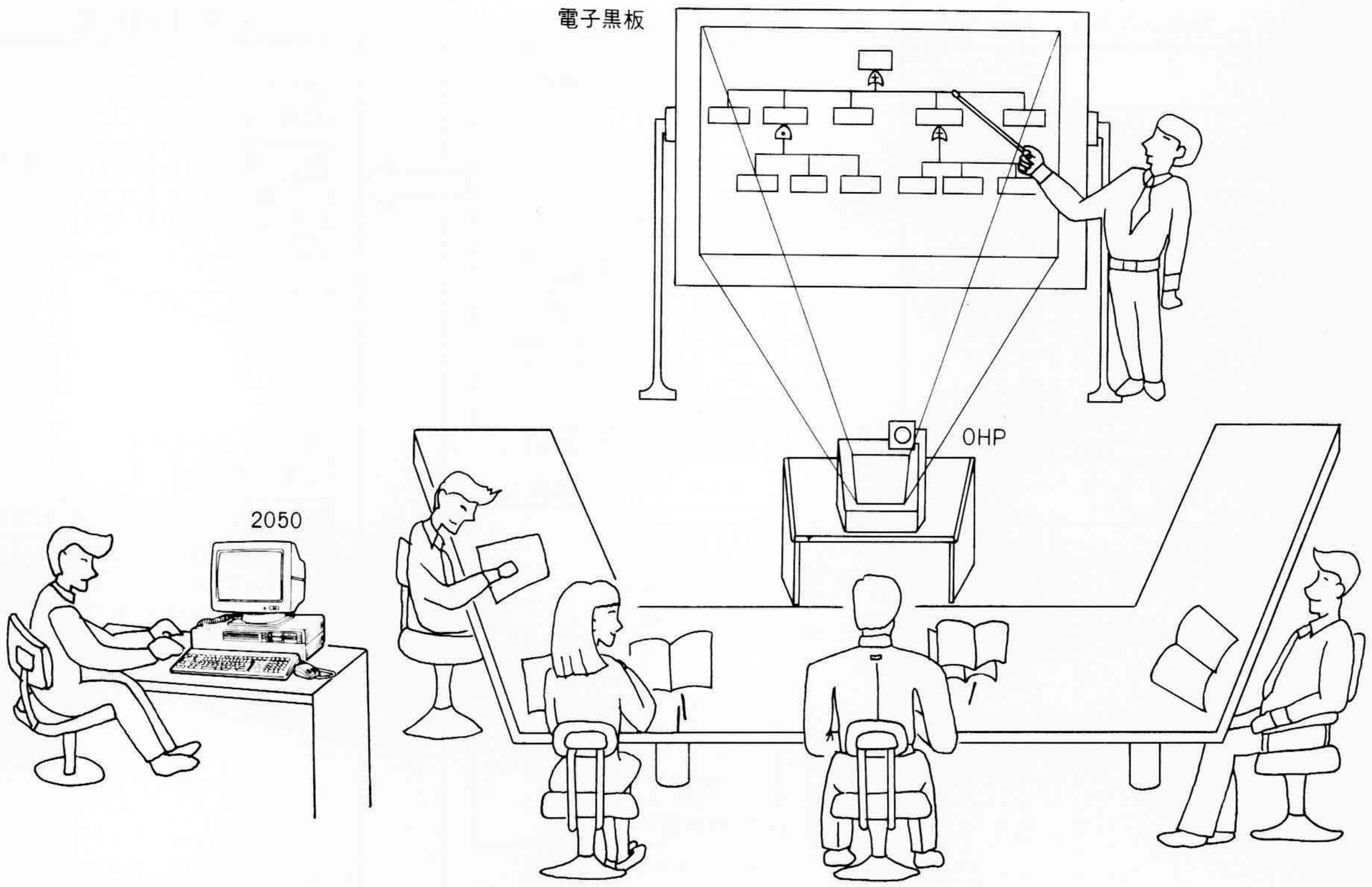
(3)　フォルトツリーの中間事象の挿入のような図面修正などを2050及び専用ソフトを用いて行う。更に，修正結果はOHPを用いて電子黒板に直ちに表示する。これにより，電子黒板を用いるだけでは手間のかかる図面修正などを簡単に行うことができる。

(4)　解析内容を2050にいったん格納する。その後，2050の数値計算機能を応用することによって，フォルトツリー確率計算などのセキュリティの定量的評価を自動的に行わせる。これにより，セキュリティ解析作業が大幅に効率化される。

4.3　適用結果の概要

二つの具体的金融システムに対して，上記のHisecurity-Eを適用し，対象システムの基本的安全性を確認するとともに，幾つかの改善案を提案することができた。これにより，本方式の有効性を確認した。

また，**4.2**節で述べた解析ツールの適用結果，手作業では800時間/システムかかっていた解析マンパワーを，400時間/システム程度に低減でき，解析作業を大幅に効率化できることを確認した。



注：略語説明 2050(クリエイティブワークステーション2050)，OHP(Over Head Projecter)

図6 Hisecurity-Eによるセキュリティ評価作業の一形態 電子黒板に書き込まれた手書きの解析内容に対し，2050及び専用ソフトによって活字化や確率計算などの処理が行われる。

5 結 言

近年，コンピュータの利用が拡大するなかで，人間の誤操作，不当行為などに対するセキュリティへの関心が高まっている。特に，金融機関で認証，アクセス管理などのセキュリティ対策の実施に積極的な傾向がみられる。

日立製作所はこのような時代に対応し，日立情報セキュリティシステムHisecurityなど種々のセキュリティ技術を開発中である。特に，セキュリティ評価技術Hisecurity-Eについては，基本方式及びセキュリティ評価支援ツールまで開発し，セキュリティ対策の検討などに活用している。

本稿では，上記金融機関でのセキュリティ対策の現状と日立製作所の対応としてHisecurityなどの概要を述べた。更に，今回新たに開発したセキュリティ評価支援ツールを紹介するとともに，その具体的金融システムへの適用結果として評価作業のマンパワー低減などの効果が得られたことを示した。

参考文献

1) 情報処理振興事業協会技術センター：コンピュータ・ネットワークにおけるセキュリティの調査報告書，情報処理振興事業協会技術センター報告書番号60技-062(昭61-3)
2) 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)
3) ISO/8731：Banking-Approved Algorithms for Message Authentication(1987)
4) 宝木，外：ネットワークセキュリティ技術，日立評論，**69**，9，847～854(昭62-9)
5) 宝木，外：情報システムにおけるセキュリティ評価方法，1987年暗号と情報セキュリティワークショップ資料，CIS研究会，35～49(昭62-7)
6) (財)金融情報システムセンター：金融機関等コンピュータシステムの安全対策基準，(財)金融情報システムセンター(昭60-12)
7) 佐々木，外：システム高信頼化技術のプラントおよび情報システムへの適用，電子通信学会技術研究会報告，FTS85-32，27～34(昭61-2)
8) 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き，8090-3-352-10(昭61-12)
9) 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)
10) 前田，外：ディジタル署名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)
11) 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)
12) 永井，外：電子取引用認証システムの機能試作機の開発，1987年暗号と情報セキュリティワークショップ資料，CIS研究会，電子情報通信学会セキュリティ時限研究専門委員会，109～121(昭62-7)