マルチメディア通信と分散処理 28－3
（１９８６．２．２７）

コンピュータ・ネットワークの安全対策と信頼性確保

黒　川　恒　雄
（日本銀行電算情報局）

1. はじめに

先進中央銀行の意見交換の場でもある国際決済銀行（ＢＩＳ※、スイス、バーゼル在）では、かねてよりコンピュータ・ネットワークを利用した資金決済システムの安全対策問題に多大の関心を示し、加盟主要国の実情、問題点などについて具に調査、検討を重ねてきた。

その研究結果は、コンピュータ・ネットワーク資金決済システムに関し、３５７項目に及ぶ詳細なチエックリスト（リスク対策）を収録した「電子決済システムの安全対策と信頼性確保」（原題：Security and Reliability in Electronic Systems for Payments）、通称〝Yellow Book〟と題して１９７５年に公表され、その後逐時改訂されてきた。

わが国においても大規模なコンピュータ・ネットワークを利用した資金決済システムが進展している現状にあつて、通産省の「電子計算機システム安全対策基準」や「システム監査基準」がすでに公表されているが、前者は産業界全般のコンピュータ・センタを対象に定めており、後者はネットワークを主眼に置いて編集されている。

ＢＩＳの〝Yellow Book〟はコンピュータと通信ネットワーク双方を利用する資金決済システムに関し、安全対策のチエック・リスト３５７項目を単に掲載するにとどまらず、そのチエック・リストの総合評価手法である「安全対策のプロフイールによる評価」や「リスク分析のためのマトリックス手法の採用」などの工夫をこらして他の安全対策基準関係の類書にはない特色を持つているので、ここにその概要を紹介することにした。

※ BIS : Bank for International Settlements

2. コンピュータ・ネットワークの安全対策が注目されるようになつた事情

資金決済システムが近年、より一層脆弱になつてきている原因について次の４つの事情を挙げている。

(1) ネットワーク数の増加

資金決済取引の流れを最初から最後まで電子的に一貫処理しようとするためには、ローカル・ネットワークと全国あるいは国際ネットワーク間の連携を必要とし、その間のインタフエースで新しい安全対策問題が生じる。

(2) 通信回線の問題

伝送メッセージなどを改ざんしようとする意図を持つたアクセスに対し通信回線はどのネットワークでも最も弱く、かつ防禦の最も難しいところである。また、マイクロウエーブと人工衛星を結びつけたシステムでは、それなりの受信設備さえあれば、アクセスは可能となる。このため暗号化が重要な課題となる。

(3) 端末機台数の増加

銀行が資金決済システムに使用する端末機台数は飛躍的に増加しており、これら端末機の無許可使用は、オンライン・コンピュータ・システムの安全対策に対する最大の脅威である。

ＣＤ、ＡＴＭ、家庭端末、ＰＯＳ端末などカードを使用する端末機が増加するにつれ、資金決済システムは、電算機室とか銀行内事務室など外部から

隔離された管理しやすい場所から、道路、空港などの売店、個人の家など管理しにくく被害を受けやすい脆弱な場所へ拡大している。

(4) 悪意に満ちた行為(犯罪)の増加

不満を抱いている従業員が不正行為を行うよりもむしろ過激な手口—テロや爆発物の利用—の脅威の方が最近増加傾向にある。また、経済的利益よりもむしろシステムを破壊したいという欲望—すなわちハッカーによる知的挑戦—という危険もある。

3. 安全かつ信頼できる資金決済システム

このようなコンピュータ・ネットワークの脆弱性の増大に対し、〝Yellow Book〟は安全かつ信頼できる資金決済システムとは次のような条件を備えたものであるとしている。

(1) 資金決済システムに入力された取引データやメッセージが正規に処理されなかつたり、改ざんされたり、複製されたり、あるいは指定時間通りに送信されないといつたことが決して起らないシステム。

(2) システムの作動が時に正常でなく部分障害を起しても、システム全体が完全に作動しなくなる、いわゆる全体障害におちいることは決してないシステム。

(3) 入力、伝送あるいは受信された取引メッセージのフォーマットやその処理過程でのエラーは、発見され次第、そのシステムの運営責任者に直ちに通報されるシステム、とされている。

4. 安全対策と信頼性確保に関するチエック・リスト

上述のように高度に安全で信頼性のあるコンピュータ・ネットワークを利用する資金決済システムの構築には、自然災害、機器の障害、不正行為などから生ずるシステム障害の発生を未然に防止すると共に発生時の影響を最小化し、早期の回復をはかるために必要とされる安全対策基準項目(チエック・リスト)を整備しておく必要がある。〝Yellow Book〟では、①設備などに対する物理的安全対策、②システム構成装置のハードウエア、ソフトウエア面での技術対策、③システムの開発、運用管理体制面での対策に分けて357項目にのぼるチエック・リストを掲載している。

(1) 設備などに対する物理的安全対策……主として同書第2章「物理的安全対策」に掲載の107項目……

コンピュータ・センタの建物、関連設備(電源空調、回線、データ保管など)について、洪水、悪天候、電磁界の有無などの各種自然災害や侵入、破壊などの不法行為、機器故障などから守るための予防、応急対策を具体的に示している。

また、CD、ATMなどが設置された自動機器室を運営する上で室や設備に要求される必要な対策が列挙されている。

物理的安全対策は対策実施対象を、立地環境、建物、部屋、設備ごとに取りまとめたものである。このため、システムの運用実態などにより実施困難の場合は、実施対象変更などの措置を講ずる必要がある。

(2) システム構成装置のハードウエア、ソフトウエア面での技術対策……主として同書第3章「安全対策と信頼性確保のための設計上の要件」に掲載の121項目……

技術対策にはシステム信頼性向上対策と安全性侵害対策がある。

システムの信頼性向上対策は、コンピュータ・ネットワーク・システムの障害発生を極力減少させ、万一障害が発生してもその影響を最小限に食い止め、速やかに回復させるものであり、ハードウエア、ソフトウエアおよび運

用時の信頼性向上対策がある。

ハードウエアの信頼性向上対策とは予防保守〔例えば、機器の各部品のMTBF(平均故障間隔)およびMTTR(平均修復時間)の把握〕やハードウエアの予備〔デュプレックス・システムやマルチプロセッサ・システムおよびロードシエア・システム〕などである。

また、ソフトウエアの信頼性向上対策とは、開発時の品質確保〔例えば、信頼度の高い設計に配慮したエラー局所化ルーチン、標準化設計技法の採用〕やメンテナンス時の正確性確保などである。

運用時の信頼性向上対策には、オペレーションの自動化・簡略化・チエック機能〔例えば、テープハンドリングの極少化、データ入力作業の自動化、入力のチエック、および各種合計の突合機能〕、負荷状態監視制御機能などがある。

障害の早期発見・早期回復対策には、障害の検出・切り分け機能〔運転状況(稼動・停止・エラー)の監視機能やエラー発生時の状態に関する詳細情報のロギング機能、切り分けるための折り返しテスト機能〕や局所化、リカバリー機能〔縮少・再構成機能や取引制限機能、各種リカバリー用ジヤーナル機能〕などである。

安全性侵害対策には、データの保護対策および不正使用防止対策がある。

データ保護対策とは漏洩防止〔暗証番号やパスワードなどの非表示、非印字、重ね打ちなどの対策〕や破壊・改ざん防止〔ファイルに対する排他制御、アクセス制御機能や不良データ検出機能〕や検知策〔故意または過失によるファイル間の不整合を早期に発見するためのファイル突合機能〕などである。

また、不正使用防止対策は、本人確認機能〔カード、役席キー、PIN(個人暗証番号)、パスワードなどの使用〕や端末確認機能〔業務内容の必要性に応じ、端末ID、電話番号、コールバックによる確認〕またはその組合せにより、アクセス権限の確認をすること。

アクセス権限確認が十分でない場合または不正アクセスの危険性が高いと認められる場合には、利用範囲を制限する対策〔端末権限規制、取引規制、取引禁止などの機能〕を講ずるとともに、検知策として不正アクセスや異例取引の監視機能〔暗証番号の入力エラー監視、何回かのアクセスの失敗に対し強制終了、取引禁止等を行う機能〕を設けること、などである。

(3) システムの開発、運用管理体制面での対策……主として同書第4章「事務準則」、第5章「管理上の配慮事項」に掲載の129項目……

ここではコンピュータ・ネットワークを使用した資金決済システムに係わる組織、責任体制、承認手順等を中心に取りまとめている。

すなわち、コンピュータ・センタの業務組織の整備、規程の整備、入退管理、システムの関連機器などの運用管理やシステム開発・変更に係わる承認・確認手順また各種設備管理、運用全体に係わる教育・訓練、要員管理、さらにシステム監査、検査体制についても言及している。

管理体制は、運用管理に係わる基本であり、管理には①入退館(室)管理〔資格付与、鍵、磁気カード、識別コードなどの管理〕、②コンピュータ・システム関連機器、設備などの運用管理と監視〔通常時および障害時マニュアルの整備、アクセス権限の管理、オペレーション管理、データ・ファイル管理、プログラム管理、ドキュメント管理、帳票管理など〕のほか、前述の「設備などに対する物理的安全対策」や「システム構成装置のハードウエア、ソフトウエア面での技術対策」を踏まえて、安全対策に係わる運用を的確に

行うため、③教育・訓練〔オペレーション習熟のための訓練、障害時・災害時に備えた運用訓練や防災・防犯訓練〕および要員管理〔人事および健康管理〕が必要である。

また、いかように事故防止装置が完備され、しかも事故発生時の処理方法が詳細に規定されていても、これらが作動しなければ無意味である。安全対策の実施状況を客観的に評価分析し、実効性を上げるため、十分作動するよう定期的に検査、監査制度によつてチエックすることが必要である。

さらに新しいシステム構築に際しては、その計画段階から安全性や管理手法に十分注意する必要があり、したがつて検査、監査制度が計画の初期段階から関与する方がよいと提言している。

また、経営陣はコンピュータ・ネットワーク・システムを使用する資金決済システムに関しリスクの本質を熟知すると同時に、安全対策が一旦破壊された時の影響は一国の銀行制度の信用喪失にいたるほど重大なることからリスク対策についても十分理解していなければならないと勧告している。

5. 安全対策のオーバビューやプロフィールによる評価

オーバービュー（Overview）やプロフィール（Profile）とは管理者が前述357項目にのぼるチエック・リストに対する解答を何らかの形で集計し、安全対策の望ましい水準に到達していない分野を見分け、かつシステムを総合的に評価するための手段として考案されたものである。

コンピュータ・ネットワークを使用する資金決済システムから得られる便益は、そのシステムで利用（あるいは所有、リース、契約）される諸々の資源を、安全対策の三つのキー・ワード、すなわち、

①アクセス（Access）

②信頼性の確保と緊急時対策（Reliability & Contingency Plan）

③管理責任の分担（Accountability）

で評価して判断される。

これを具体的に言えば、①資源が許可されていないアクセスから守られているか、②望ましいレベルの信頼性が保証されているか、そして緊急時においてもこの資源が正常な状態と同じ機能を発揮できるか、③資源に対する管理責任は明定され、しかるべく割当てられているか、という三つのキーワードによる評価は「致命的欠陥あり」（Critical Deficient）、問題あり（Questionable）、許容できる（Acceptable）、良好（Good）および大変堅固（Very Strong）の五つに区分される。

ここでいう資源とは、施設、ユーテイリテイおよび公共サービス、ソフトウエア、計画と手順、データ、人員、契約、協約等である。

経営者がシステムの安全対策と信頼性確保に関するオーバービューを理解する一助として典型的な電子決済システムの資源のうち特に重要なものは次のとおりである。

①設備（中央、バックアップ、再配置の場所）……不動産および建物、コンピュータ、ターミナル、通信ネットワーク、ビルデイング設備（暖房、通風装置と空調、電気、機械、水道工事、警報器、防護装置、消火器）オフイスと他の設備（オフイス、家具、エレベーター、階段と廊下、その他の設備休憩場所等）と金庫室。

②ユーテイリテイとその他の公共サービス……電気、電話、燃料、水、オフイスの提供するもの、その他外部からのサービス（警察、消防、医者）等。

③ソフトウエア……オペレーテイング・システム（アプリケーション、機能管理、送信サブシステム）、ソフトウエアの開発とメンテナンス、ドキュメンテーション等。

④計画と手順……オペレーションの

手順と安全対策および制御手順。緊急時対策、再スタートないしフォールバックの手順、用地計画。

⑤データ……メッセージ/伝送(付替)と要求/応答。レコード,ファイル,デイスク,テープ,ドキュメント。

⑥人員……スタッフ(オペレーター,サポーター,管理者)、メーカーとその他の訪問者。

⑦契約・協約等……顧客、銀行と他の金融機関、他の決済システムメーカーと提供者、ユーテイリテイ、コンサルタント、保険会社との間の契約等システムの安全性および信頼性を確保するうえでシステムの所有者なり管理者が危険の度合いをどのように判断するかが1つのポイントである。他の事情が等しければ、危険の度合は投下する資本と支払う費用に逆比例する。

経営者は危険の確率を評価し、その他の要因も考慮して危険とコストのバランスをどのようにとるかを決定する。

安全対策と信頼性の確保が必要とされる度合いはシステムにより異なるがシステムとその利用者の長期的な利益を守るには実施可能な最も高いレベルの安全対策と信頼性を確保することが必要となる。

いま、同じようにコンピュータ・ネットワークを利用する二つのシステムすなわちメッセージ交換システムと資金決済システムを例にとると、資金決済システムは単なるメッセージ交換に止まらず、支払という行為とそれに関連するサービス(価値の移転、清算)を行い、勘定と責任関係が含まれ、その性質上、全関係者の利益を保護するため単純な指示メッセージ交換システムより一層レベルの高い安全対策と信頼性の確保が必要とされる。

資源グループごとに集計された評価(プロフアイル)は右表に例示された望ましい水準に達しなければならないし、また達成のため改善を必要とする分野を認識し、適切な改善処置をとることとなる。

6. リスク分析のためのマトリック手法

マトリックス手法はコンピュータ・ネットワーク・システムに固有なリスクの水準をかなり正確に評価する手段として〝 Yellow Book 〟に1985年1月追録された。

アメリカの中央銀行である連邦準備制度はFEDWIREと呼ばれる広域のコンピュータ・ネットワーク決済システムを運用しているが、そのセキュリテイ対策としてこのマトリックス手法を「セキュリテイ・アーキテクチヤ」と名付け、コンピュータ・ネットワーク・システムのリスク(脆弱性)を綿密に調査し、これをリストアップして、それぞれについて対策を立てるのに使用している。

「セキュリテイ・アーキテクチヤ」(マトリックス手法)の構築方法は概略次の通りである。

(1) システムの主要処理・通信機能の確定

先ず、セキュリテイ対策を講ずべきシステムの主要な機能(Functions)を確定する。例えば、資金付替および決済業務(Automated Clearing House)、金融統計報告、経理や内部管理情報交換などの機能である。

(表) メッセージ交換および資金決済システムにおける資源別必要安全対策と信頼性確保のレベルのオーバビュー

〔安全対策と三つのキーワード①Access, ② Reliability & Contingency Plan, ③ Accountability〕

3つのキーワードによる資源評価	欠陥あり	問題あり	許容出来る	良好	大変堅固
設備					
ユーテイリテイ等					
ソフトウエア					
計画と手順					
データ					
職員					
契約・協約など					

(メッセージ交換)
(資金決済)

(2) 機能とリスクのマトリックス

各機能に対するリスク(Threats)をマトリックス形式で表わす。リスクには、内部あるいは外部の者が許可を得な

いで情報を見ること、データの修正を行うこと、不注意によるデータ変更、メッセージあるいは取引が伝送されないこと、短・長期にわたる業務拒否などが挙げられ、各機能はリスクごとに、高度（High Concern）、中度（Medium Concern）、低度（Low Concern）のランクが付けられる。

(3) リスクに対するシステムの脆弱性のマトリックス

各リスクに対応するシステムの脆弱性（Vulnerabilities）をマトリックスに表わす。システムの脆弱性は、通信面（盗聴によるメッセージの挿入、改ざんなど）、ソフトウエア面（設計・開発・更新時点における不正、メーカー提供管理システムの不良など）、要員／手続き面（データの不正入力、不正オペレーションなど）、機器（ハードウエアの障害、設備不良など）ごとにリストアップし、各リスクに対応する評点を計算する。

(4) システムの脆弱性に対する安全対策のマトリックス

安全対策は個々のリスクに対応する防御手段である。安全対策は極めて数多く、技術的安全対策、物理的安全対策、手続き、経営方針など色々と異なるカテゴリーに分類される。

上記3つの基本的なマトリックス、すなわち(1)機能とリスク、(2)リスクとシステム脆弱性、(3)システムの脆弱性と安全対策マトリックスから始まり、これらのマトリックスを掛け合わせることにより、その論理積（帰結）として最も重要な(4)機能と安全対策のマトリックスが導き出される。

マトリックス手法を有効に利用するためには次の2点に配慮すべきであるといわれている。

第一は、マトリックスのセル（cell）の評価を決定する際に、注意深く判断しなければならないということである。

評価とは(1)〝機能とリスク〟および、(4)〝機能と安全対策のマトリックス〟では高、中、低の程度であり、(2)リスクと脆弱性、および(3)脆弱性と安全対策のマトリックスでは、その関係の有無である。これは構成要素の数が増えるにつれて一段と難解となり、その間の斉合性も問題になるためである。

第二は上記の理由およびマトリックス個有の複雑さのため、パソコンなどを使用し、手法を自動化する必要がある。

アメリカ連銀でのパソコン利用の経験では、マトリックスが複雑であるため、マトリックスのセルに関連して取らねばならぬ判断は通常数千個に達するようである。

この手法のもう一つの特徴は、個々のマトリックスが、それぞれ個有の評価を行うため極めて重要であることである。一つは技術者にとつて重要な〝システムの脆弱性一安全対策マトリックス〟、もう一つは経営者、利用者にとつて重要な〝機能一安全対策マトリックス〟である。

このようにマトリックス手法は、システムを評価する上で疑う余地もない有効な手段で、とりわけマイクロコンピュータによる自動処理の柔軟性を考慮して、構築されたものである。

さらに、調査対象システムの安全性水準を評価するため、技術者と経営者が別個に調査結果を提出できるユニークなシステムであることを強調しておきたい。

冒頭にも述べたように金融機関のコンピュータ・ネットワーク・システムは最近特に企業、家庭など外部とのネットワークの拡大の可能性に伴い急速な展開を見せている。コンピュータ・ネットワークを使用した資金決済システムに一旦障害、犯罪が生じると金融機関業務の性格上、一国の経済活動並びに国民生活に多大の影響、被害を与えるものと懸念される折、是非〝Yellow Book〟の一読をすすめたい。

〔なお、本予稿集とほぼ同様の内容をコンピュータ＆ネットワークLAN'86 3月号（オーム社）に紹介しているので参照されたい。〕　（以　上）