情報システムにおける外部セキュリティ制御

External security control in the Information System

谷　口　道　興

Michioki Taniguchi

1. はじめに

高度情報化社会の進展に伴い、情報伝達を担う通信の役割が、多種多様な情報を対象とする方向へと、急速に移行しつつある。こうした情報化社会を構築する際に、必須の技術として希求される情報セキュリティ技術を、外部セキュリティ制御(external security control)と内部セキュリティ制御(internal security control)とに分け、本稿ではまず外部セキュリティ制御について述べる。

計算機セキュリティ、システムセキュリティ、データセキュリティ、あるいは情報セキュリティ[1]といった用語の定義は必ずしも明確ではなく、ほぼ同義に用いられているようであるが、本稿で用いるセキュリティとは「容認できないリスクから解放された状態[2](the absence of unacceptable risk) と定義しておく。

2. 外部セキュリティ制御

計算機システムの利用分野および形態、また用途については、多様なシステムが存在する中にあって、もとより情報セキュリティ対策は、すべてのシステムに均質的に要求されるものではないが、外部セキュリティ技術の主な手段としては、基本的には物理的（技術面・設備面）セキュリティ、運用管理面におけるセキュリティそしてリスク評価として分類することが可能である。

2・1　物理的セキュリティと運用管理面でのセキュリティ

物理的（技術面・設備面）対策とは、計算機システム（端末装置、外部記憶装置を含む）、計算機室への被害を防ぐことを目的としたものであり、それは計算機システムのセキュリティの向上を、システム自身において、ハードウェア的、ソフトウェア的に解決しようとするものであり、障害の態様の観点から

- システムダウンおよび誤動作に関する技術
- データの漏洩、破壊、改ざんおよびシステムの不正使用を防止するための技術

と整理することができる。

また、運用管理面における対策とは、計算機システムの運用に係わる人、および部外者の行動を規制する手続的な対策であり、それは以下の４点に整理できる。[3]

- 組織体制の整備
- 教育訓練および人事管理
- 運用管理規定の制定
- システム監査の導入

これらの対策の基準としては、我が国においては、1977年４月に制定された「電子計算機システム安全対策基準」（通産省）があるが、同基準はその後1984年８月、情報化環境の変化に即して、全面的に改訂されている（図１）。同基準の対策内容は、自然災害、システム構成要素の障害、不法行為等によって生ずるシステムのダウン等を未然に防止し、また発生した場合の影響の最小化および回復の迅速化を図るための、いわば守るべきものを全て網羅したものである。基準は対策内容ごとに、基本基準（C）、標準基準（B）、強化基準（A）の三段階に分類してあり、最高度の安全性、信頼性が必要とされるシステムにおいて、実施することが望ましい対策をA、一般にシステ

ムを運用する上での最低限の安全性、信頼性を確保するために不可決と考えられる対策をC、これらの中間的な対策をBとしている。これらの適用にあたっては、対策の実施により期待される安全性、信頼性等の向上の程度、必要とされる資金の額、システムの停止による社会的、経済的な影響等を勘案して判断することになる。

Ⅰ 設備基準
1. 建　物
(1) 立地及び環境
(2) 建物の位置、周囲、利用形態
(3) 構　造
(4) 開 口 部
(5) 内 装 等
2. 電子計算室及びデータ等保管室
(1) 位置及び配置等
(2) 開 口 部
(3) 構造、内装等
(4) 設　備
(5) 什器、備品等
3. 電源室及び空気調和機械室
(1) 位置及び配置
(2) 開 口 部
(3) 構　造
(4) 設　備
4. 電源設備
5. 空気調和設備
6. 監視制御
Ⅱ 技術設備
1. 信頼性向上機能
2. データ保護・不正使用防止機能
Ⅲ 運用規準
1. 管理体制
2. 入退管理
1 入館、入室資格の付与
2 入退館管理
3 入退室管理
3. 電子計算機システムの運用管理
1 標 準 化
2 運転及び確認
3 管　理
4. データ及びプログラム（ドキュメントを含む）の保管管理
5. 電源設備、空気調和設備、防災設備及び防犯設備の管理
6. 監　視
7. 外部委託
8. 教育訓練等
9. システム監査

図1 「電子計算機システム安全体策基準（改訂版）」の概要

同基準は、付言するならば
(1) 設備基準は、152項目からなり、電子計算機室、データ等保管室を火災、地震等の自然災害、不法侵入者による破壊行為等のあらゆる危険から、物理的に保護するための対策。
(2) 技術基準は、13項目からなり、電子計算機システムの安全性、信頼性等の向上をシステム自身において、ハードウェア的、ソフトウェア的に解決するための対策。
(3) 運用基準は、63項目からなり、電子計算機システムの運用管理面を充実させていくことにより、システムの安全性、信頼性等の向上を図るための対策。
からそれぞれ構成されている。

2・2 リスク管理

リスク管理とは、一般的には (1)リスクの鑑定測定、コントロールを通じて、最小の費用でリスクの不利益な影響を最小化すること。 (2)できるだけ少ない費用で、組織に与えられる偶然的損失の不利益を最小化するため、組織の資産ならびに活動を、計画、組織、指揮、統制するプロセスをとり、組織（企業）を脅かすリスクに対応する理論といえる。この点に関してGeorge. L. Headは、リスク管理を次のように定義している。

「組織をおそう偶発的な損失の経営上、財務上の不利益な影響を最小化するため、組織の資産・諸活動を、計画化、組織化、指揮・統制化するのが、リスク管理である」[4] 本稿で論じるリスク管理は、このような広い体系の中のサブ・モジュールをなすものであり、自然災害、システムおよび設備障害、不法行為からのリスク管理を対象としている。

また、一般にリスク管理のプロセスは、図2のステップをとって展開される。

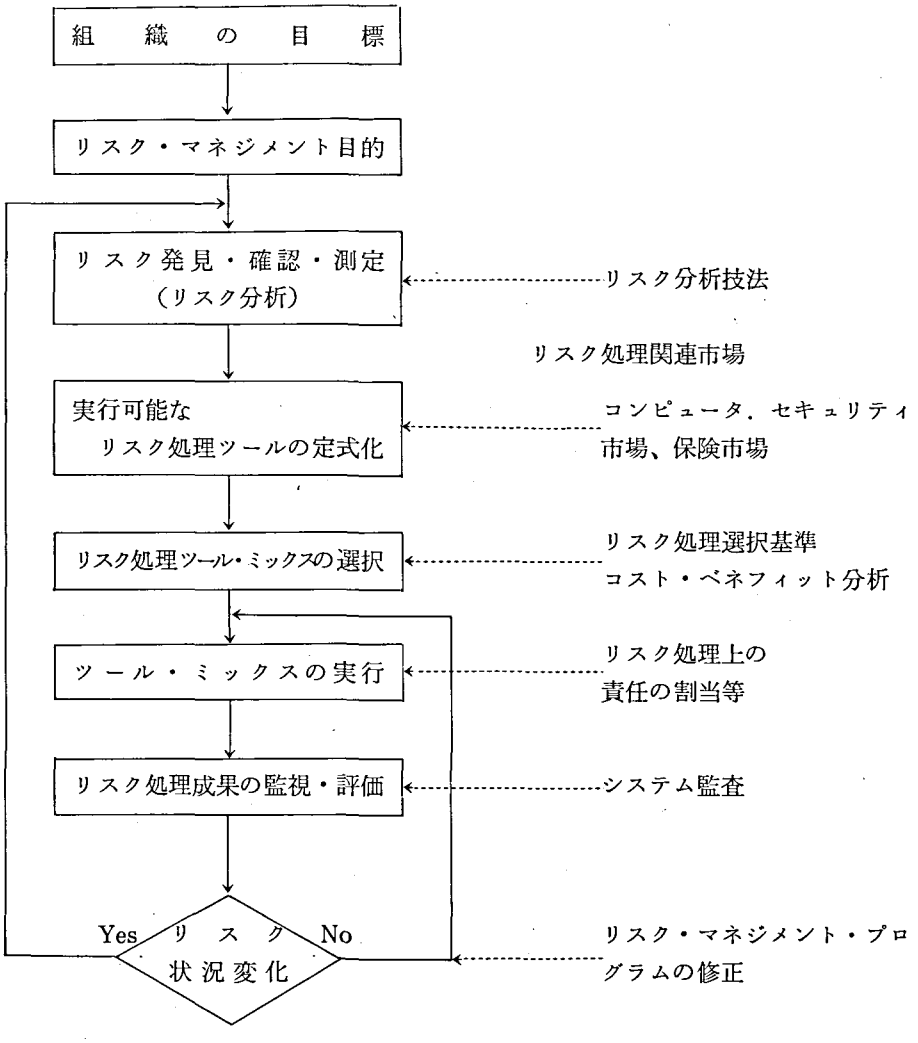

図2　リスク管理プロセス[5]

2・2・1　リスク分析

この目的は、(1) 考えられる損失やその頻度を分析し、可能な限り少ない費用で損失の発生を防ぐ、または、(2)損失発生の場合の被害や回復費用を最小にすることである。

ここでリスクをr、脅威の発生割合または確率をp、脅威の作動に基づいて発生する損失をeとすると、r＝p×eが成立する。

脅威は予測可能な方法で損失を引き起こす傾向がある。発生の頻度と損失額との間には、統計的な相関が存在する。極めて頻繁に起こるリスクは、小さな損失を、また稀に起こるものは破局的な損失を引き起こす傾向がある。

また、セキュリティと効率との間には、トレードオフが存在する。同様にコントロールの費用とリスク減少で表わされた便益との間にも、トレードオフが存在する。コントロールのための支出が増加するに従い、損失の減少か脅威発生の確率の縮小かのいずれかにより増分便益は減少する。最適点はコントロールの費用と保護レベルが交差するところまで、コントロールに資金を消費することである。したがってリスク分析には、損失発生の頻度と損失が発生した場

合の予想損失額を推定するための作業が必要となる。また、損失発生の要因としては、次の事柄が考えられる[6]。

(1) 有形資産の物理的な破損または盗難 — 破損または盗難にあった資産の再設備に要する費用と、データ処理の遅延によりユーザがうける損失。

(2) データまたはプログラム・ファイルの粉失または破損。

(3) 情報の盗難 — 金銭的損失や信用損、失行者としての優越的地位の喪失。

(4) 資産の間接的盗難 — データ処理システムの適用業務の対象となっている他の資産、たとえば現金、在庫品あるいは、種々のサービスなどが計算機を通じて盗まれる場合の損失。

(5) 計算機処理の遅滞または妨害。

つぎに、リスク分析の実施手順を図式化すると図3のように表現できる。

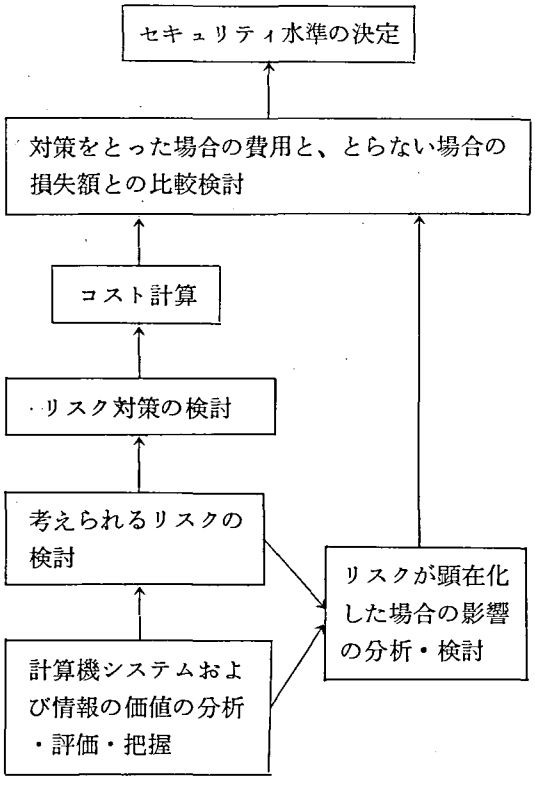

図3 リスク分析の実施手順

2・2・2 リスク管理の数量化

損失の可能性とその影響度を、可能なかぎり正確に数量化することが、リスク管理の成否を左右する。このことは、望ましくない出来事が発生する可納性を、我々がどの程度認織できるかという問題でもある。損失の形態は通常、破壊（破損）、暴露と正しくない変更の三つに分類できる[7]。これらのイベントが生じる頻度(P)と、1回生じた場合の予想損失金額(V)を推定できれば、ある一定の持続する期間内（たとえば1年間）に生じる（年間）予想損失(L)は、L＝P×Vで計算できる。しかし、この方式ではVあるいはPの推定値に極めて敏感に反応するという欠点がある。そこで、R. Courtney[8]は、「これまでに現実化した脅威の各々を基礎にして、それらに起因する損失の発生頻度と、1回あたりの損失額から予測する方式を提唱した。それは、1年間に発生する脅威の年間予想損失額をEとしてE＝$10^{(P+V-3)/3}$を与え、P、Vは下記の引数に変換して求める方式である。

V		P	発生頻度
0	$0	0	実質的にゼロ
1	$10	1	300年に1回
2	$100	2	30年に1回
3	$1,000	3	3年に1回
4	$10,000	4	100日に1回
5	$100,000	5	10日に1回
6	$1,000,000	6	1日に1回
7	$10,000,000	7	1日に10回
8	$100,000,000	8	1日に100回

図4－1 損失の発生頻度と予想損失額の代替案

ここで脅威とは、差し迫った望ましくない出来事の徴候の意。損失が生じるのは、欠陥と脅威が積集合の関係になる場合である。リスク分析においては、欠陥と脅威のいずれに問題があるのかを明確化できれば、より効果的なセキュリティ手段を選択できよう。

また、次の表を与えて、図4－1から必要なVとPの値を選び、図4－2でそれらに該当するV行とP列の交差する位置を求めれば、公式を用いての計算に比べてEの値は簡単に求まる。

V ＼ P	1	2	3	4	5	6	7	8
1					$ 300	3 K	30 K	300 K
2				$ 300	3 K	30 K	300 K	3 M
3			$ 300	3 K	30 K	300 K	3 M	30 M
4		$ 300	3 K	30 K	300 K	3 M	30 M	300 M
5	$ 300	3 K	30 K	300 K	3 M	30 M	300 M	
6	$ 3 K	30 K	300 K	3 M	30 M	300 M		
7	$ 30 K	300 K	3 M	30 M	300 M			
8	$ 300 K	3 M	30 M	300 M				

図4－2　Eの値の決定表

（年間）予想損失額を推定するこの方法は、予想損失額を軽減させるために、どの程度の資源をセキュリティ対策に投資すべきかという決定に際し、強力な助けとなる。しかし、こうした計算プロセスを完了するためには、相当の情報を必要とし、妥当な資産損失額と各資産に生ずる事件の予想発生頻度をそろえなければならない[9]。数年間にわたる頻度の高い損害を網羅した損失額データは、年間予想損失額を求める際の、最適のデータベースとなろう。こうしたデータが利用できない場合は、当然この方法は価値の低いものになってしまう。

さて、日本情報処理開発協会（以下JIPDECと略記する）がオンラインユーザーのみを対象にして実施した「コンピュータセキュリティに関するリスク分析調査」（昭和60年7月アンケート方式により実施。アンケート発送数2,149事業体、回収数1,383事業体。回収率64.4％）によると、リスク分析を実施している事業体は、21.8％と少数である。リスク分析がこのように普及しえない最大の原因は、「確立された分析方法がない」ことに起因する。また、リスクの発生に伴う損失額を予測している事業体に至っては、5.1％と極端に少なく、システム規模が100億円以上の事業体（64事業体）でも8.1％であり、殆んどの事業体が、この種の分析に取り組んでいないことを示している。損失額を予測している事業体の算定基準によれば、最大の事故を想定した予測損失額は、コンピュータ犯罪が21,250万円、火災が270,568万円、地震が309,375万円、エラーが1,026万円となっている。これは、コンピュータ犯罪を1とした場合、エラーは約20分の1、火災は約13倍、地震は約15倍となる。情報システムの価値と評価（金額換算）している事業体は、全体で18.4％であるが、システム期模が100億円以上のユーザーでみると35.6％と3件に1件の割合で評価を行っている。ただ、情報およびプログラムの価値と評価（金額換算）している事業体は20.7％で、システムを評価しているユーザーよりも多い。

2・3　リスク管理実施の評価

計算機システムのセキュリティ確保の手段として、システム監査がある。リスク管理実施の評価は、このシステム監査がその役割を担うものである。システム監査という用語が我が国で使われ始めたのは、昭和49年JIPDECが情報化社会の秩序づくりの一環として提唱して以来であるが、システム監査の重要性が認識されるようになったのは、昭和56年以降のことである。

ここで、システム監査の定義を紹介すると、「システム監査とは、監査対象から独立した客観的な立場で、コンピュータを中心とする情報処理システムを総合的に点検・評価し、関係者に助言・勧告することをいい、その有効利用の

促進と幣害の除去とを同時に追求して、システムの健全化をはかるものである」。(JIPDEC システム監査委員会) となっており、内部監査としての位置づけである (図5)。また、昭和60年1月には通産省から、システム監査のガイドラインとして「システム監査基準」(図6) が公表された。これをうけて昭和61年10月から、情報処理技術者試験の中に従来からの認定試験に加えて、「システム監査技術者試験」も実施することになった。このことは、今後の情報化進展を推進するに当って、システムの開発から参加できるだけの知識を有するシステム監査人が不可欠であるとの認識によるものである。[10]

監査区分	内容による分類 / 監査主体による分類	業務監査	会計監査	根拠
外部監査	公認会計士		○	証取法第193条の2 監査特例法第2条
	監査役	○	○	商法第274条 281条
内部監査	内部監査人 (システム監査)	○	○	任意

図5　監査の分類 (文献5による)

Ⅰ　一般基準
1. 目　的
2. 対　象
3. システム監査人
4. 監査時期
5. 監査計画
6. 監査手順

Ⅱ　実施計画
1. 企画業務
① 計　画
② 調査・分析
③ 開発検討
④ 要員管理
2. 開発業務
① 開発手順
② 要員管理
③ システム設計
④ プログラム設計
⑤ プログラミング
⑥ システム・テスト
3. 運用業務
① オペレーション
② 入力データの作成及び入力
③ データ及びプログラムの管理
④ ファシリティ管理
⑤ 出力情報の管理及び活用
⑥ 要員管理
⑦ 外部委託

Ⅲ　報告基準
1. 監査結果
2. 報告内容
3. 提　出
4. フォローアップ

図6　「システム監査基準」の概要

システム監査は、「システムの効率性、信頼性、正確性、セキュリティ、幣害の除去を目的にして、計算機部門を含む業務全体を監視し、その結果について、助言・勧告等を含む報告書を提出し、健全な経営活動を支援する役割を果す」ことが目的であり、そして有効にして、適切なる内部統制 (Internal Control) を確立することにある。ここで、「内部統制」の定義であるがそれは次のアメリカ公認会計士協会 (以下 AICPA と略記) の見解が一般的である。すなわち「企業がその資産の安全を図り、その会計データの正確性と信頼性を照査し、業務

能率を増進し、指示された管理上の政策への合致をおし進めていくために、企業内で採用しているすべての方法と手段、および組織計画から構成される」。このAICPA の定義は、内部統制の目的に重点を置くものであるから、EDPS (Electronic Data Processing System) には影響されない。しかし、「この目的を達成するのに必要な組織と手続は、EDPSにより影響を受けることになる。また、内部統制の機能としては、誤謬と不正が適切に迅速に発見されることを保証し、それによって、財務記録の信頼性と安全性が保証されることである」[11]。また、内部統制の分類法としては、組織上からみた「全般統制」と、部門ごとの内部統制、目的からみた場合の「会計的統制」と「経営的統制」に分類される。EDPS に関する内部統制については、すべてのアプリケーションシステムに対して共通に適用される「全般統制」(general control) と、個々のアプリケーション固有の「適用業務統制」(application control)とである。全般統制の構成内容を細分化すると次の通りである。

1. 組織および運営計画統制
2. システム開発とその文書化、検閲、吟味、承認の統制
3. ハードウェアおよびシステム・ソフトウェアの統制
4. アクセス統制
5. データおよび手続きの統制

一方、適用業務統制は「データの記録、処理および報告が適性に行なわれているということに合理的な確証を与えることである」[12]といえよう。これはまた、計算機処理のプロセスに沿った入力統制、処理統制、出力統制の3統制に分類されることがある。前述の「システム監査基準」によれば、内部監査による計算機セキュリティ監査は、断片的・個別的であることが多いが、究極的には各適用業務システムが作成・記憶している情報と提供しているサービス、並びに情報資産の保護・確保が監査の対象となるのは明白である。運用中のアプリケーションシステムのシステム監査に至る手順は次のようであり、これは日本公認会計士協会(JICPA) で定義する「全般統制」に該当する。

1. データ処理資源管理
2. データ処理資源取得
3. システム・ソフトウェア
4. 全般的セキュリティ（物理的・技術的セキュリティ）
5. 全般統制
6. SDLC (system development life cycle) 法

2・4 補完措置としての保険

セキュリティ対策を最大限講じたとしても、計算機システムにおける不測のリスクに備え、情報化保険の活用を図ることもセキュリティ対策の補完措置として有効である[13]。また、リスク管理面の観点から計算機システムの障害等に関連して予測される損失や影響を分析して、その再生、置換コスト、回復のための経済的負担の担保手段として、情報化保険を積極的に位置づけることも可能である。情報化保険の概要を述べると、情報機器、情報メディア（磁気テープ、ディスク等）・臨時費用・利益（営業の中断により被った喪失利益を支払う……情報処理業者のみが対象）の損害を総合的に担保する「コンピュータ総合保険」、および情報処害業者が負担する賠償責任の危険を担保する「情報処理業者賠償責任保険」から構成されている。しかしながら現在、情報化保険の利用率は一般に低く（加入状況は前者が10％程度、後者が10％弱）、保険の内容についての十分な理解も得られていない状況にある。このため利用者の要望を踏まえ、保険の担保範囲の見直し、条件の改訂等による制度の充実、利用の拡大に向けて十分な検討が望まれる。

2・5 おわりに

計算機システムを利用する組織（企業）にとって、リスク分析の対象は、すでに2・1の項で示した物理的セキュリティと、運用管理面でのセキュリティにおいて明らかである。即ち、計算機室、空調設備・環境制御装置、電源等の物理的資産、非常に高価でしかも非常に傷害を受けやすいソフトウェア資産、複雑な電子機器に影響を及ぼすありとあらゆる種類の物理的脅

威にさらされているハードウェア資産、計算機の利用に関わる収益の喪失、賠償責任、さらに人的資産がその対象として該当する。

その場合、リスク分析に関しての最大の問題点は、情報の経済的価値である。情報は計算機システムの最終製品であり、最も価値が高く、また最も傷害を受けやすい。計算機内に蓄積された情報は、組織体の運営全体に決定的な影響力を保持する。基本的な記録、成果等の損失があれば組織体に壊滅的な打撃を与えるであろう。また、情報の不正使用によって、組織体は損害を蒙るであろう。

計算機に蓄積された情報がさらされている脅威には、一般的なものから計算機システム特有なものに至るまで、多種多様な形態で存在する。それは、「情報処理に関係する情報の瑕疵、変形、偽造、消去、盗用等の側面と、情報の流れに関係した情報の不完全、中断、不置、遅滞等の側面があり」[14]、各々に客観的に情報自体の価値を評価することが困難である。さらに、情報へのアクセスの進展・拡大に伴い、従来、専門家によってのみ操作されていた情報通信システムが、非専門家にも操作されるようになったこと、加えてネットワークの拡大により、トランザクションの発生から帰結までが複雑となり、通過するノードの数、種類も多数となる。また、通信の自由化により新規の通信事業者の市場への参加もあって、ネットワーク自体の接続も複雑化している。従って、情報に関わる事故の発生箇所の確認にも、困難性が存在することを肯定せざるを得ない。

以上、情報セキュリティ技術に関して、本稿では外部セキュリティ技術に限定して検討した。ハードウェアにおける技術革新、情報・通信技術の発達とその結果としてのネットワークの高度化によって、情報化は今後さらに広範に、かつ深く浸透していくものと思われる。そのような状況の中で“高信頼化技術”の導入は、社会的な要請となってきている。このように、高信頼化技術の重要性は、認識されてきているものの、その内容がきわめて多岐にわたっており、しかも、十分に確立されていない面も多く、計算機システムの様々な脆弱性が指摘されているのも事実である。今後、内部セキュリティ技術の理論上および実用上の研究はもとより、外部セキュリティ技術に関しては、リスク分析の意義を確認し、リスク分析の重用性を評価・確立する必要がある。

注

1) 上園忠弘：コンピュータ・セキュリティ、近代科学社（1981）

情報セキュリティとは、リスク発生原因として考えられる①自然災害（地震、火災、風水害、落雷等）、②システムおよび設備障害（ハードウェア障害、ソフトウェア障害、回線故障、付帯設備（電力、空調等）の障害、停電、断水、異常乾そう等）、③不法行為（データの漏洩、犯罪、破壊、改ざん、不正アクセス等）から情報システムを防護すること。 ①～③は、リスクの種類であり、また静的リスクである。

2) ロナルド・カラム：情報システムの計画・設計実務、日経マグロウヒル社（1986）

リスクとは、業務に損害をおよぼすなんらかの機会であり、計算機セキュリティでのリスクは、①資源の損失（社会的信用など無形資産の損失を含む）、②業務の遅れ、③法律違反の3種に分類できる。

3) 田口孝弘：セキュリティ概論、日本情報処理開発協会情報処理研修センター（1983）

4) George L. Head, “Updating the ABCs of Risk Management,” P. 50. (1986)

5) 宇佐美博：システム監査概要、IIT（1983）

6) National Bureau of Standards, US Department of Commerce : Federal Information Processing Standards (FIPS) 31, Guidelines for Automatic Data Processing Physical Security and Risk Management.

7) 土居範久・小山謙二：コンピュータ．セキュリティ、共立出版

8) R. Courtney : “Security risk assessment in electronic data Processing systems,” in Proceedings NCC (Arlington, Va : AFIPS press), ed. pp. 97－104

9) ドン・パーカー：コンピュータ・セキュリティ、日本情報処理開発協会監訳、企画センター

10) 米国では、内部監査として位置づけられたEDP監査(Electronic Data Processing Audit)が広く行われるようになっており、こうした動きを受けて、日本でも各種団体でシステム監査の研究会や委員会を設置して、調査、研究に乗り出している。日本公認会計士協会には電子会計委員会、(ここでは「企業およびその他の組織体において、データ処理の一部または全部がＥＤＰシステムによっている場合、これを対象として監査することをＥＤＰ監査という。監査目的を達成するために、コンピュータを利用することもあれば、利用しないこともある」と定義し、外部監査としての立場を示している。)日本監査協会にはＥＤＰ監査委員会があり、米国のＥＤＰ監査関連団体の日本支部も設立されている。これらの団体は所管庁が異なることもあって、独自に活動しており、技術交流などの場はなかった。このような状況の中で通産省は、システム監査技術者の横断的な組織として、「システム監査学会(仮称)」を昭和62年春までに設立することになった。

11) 市田陽児：システム開発の新潮流と内部統制、情報科学研究第2号日本大学商学部情報科学研究所(1986)

12) 上提書 11)、P59

13) 一般に静的リスクは、十分な時間が与えられ、発生のパターンを予測できるデータが収集可能なようなリスクであるから、大数の法則を満足する。即ち、保険の対象となり得る。

しかし、計算機システムの利用がリアルタイム的になると、保険以外の補完措置を考慮しなければならなくなる。なぜならリアルタイム・システムでの損失が、仮に金銭的に事後的に補償されたとしても、損失時間を回復することは不可能となり、その場合のリスク回避の一つの方策としては、プロセス制御が必要となってくる。

14) 日本情報処理開発協会：コンピュータ・セキュリティに関するリスク分析調査報告書(1986)