EDPシステムにおける データ・セキュリティの体系化

工藤市兵衛・鈴木　達夫・近藤　高司

An Integration of Data Security Concepts and Methods in the EDP Systems

Ichibei KUDO, Tatsuo SÚZUKI and Takashi KONDO

In recent years, management at all levels has become increasingly dependent on the data processing ; Consequently, more concerned about the continuation of accuracy and completeness of results from data processing. Management was faced with serious problems such as computer crimes, hardware failures and errors caused by insufficient debugging. The purpose of the present paper is to integrate various concepts and methods. available in the literature, to obtain an efficent data security system. To make this idea effective data security management should take the following steps :

1. Along consultation with top management on the security policy and idea, determine security object and scopes.
2. Apply the effecient countermeasures to the weak points on the current EDP system.

1．はじめに

高度情報化社会への波が押しよせて来ている今日，産業界においても高い生産性を創造するためＯＡ及びＦＡと呼ばれる高度な合理化運動が進展している。営利を目的とする企業において，かつてない情報というものの重要性が認識されてきている。その収集・伝達・蓄積という情報処理業務にＥＤＰシステム又はコンピュータ・システムが広範囲にあらゆる部門にて利用され，それは，増々質的に高度になる傾向にある。特に，データ通信ネットワークと融合したオンライン処理形態が大幅に普及してきている〔1〕。現在そして将来の企業経営管理にとってコンピュータ・システムは必要不可欠であり，それに極めて高い依存性を求めて日々の業務が遂行されている。しかし，既存の企業組織の中に，十分な考慮がなく急激にシステムが浸透普及して行く傾向も見られる。コンピュータ・システムへの高度依存は反面，数々の脆弱性を内在してしまい，システムの停止や不完全による影響は甚大であり大きな損失を生ずる可能性を秘める。将来，大規模化するコンピュータ・システムが稼働し円滑な企業活動を営む為にはその安全性・信頼性に対する十分な管理行動が重要不可欠であると考える。そこで，コンピュータ・システムを使う業務に対して，どの部分が弱点であるか認識・評価し安全対策を措置するセキュリティ体制の機能強化をしなければならない。この様な観点から我が国では1977年４月に制定され1984年７月改訂された「電子計算機システム安全基準」〔２〕，1982年に郵政省告示の「データ通信ネットワーク安全・信頼性基準」〔３〕が存在し守るべきものを網羅している。又，日本情報処理開発協会では，情報化の基盤整備の一環として「システム監査」〔４〕を提唱しておりシステムの有効性・採算性，信頼性データの安全性をその枠組みとしている。日本公認会計士協会から「ＥＤＰシステムの内部統制質問書」が公表されており会計システムの信頼性監査を主眼点とし，会計記録の適正性の程度を確かめることを目的としている〔５〕。当研究においては企業診断の一分野を将来構成するものと捉えて〔６〕，コンピュータ・システムのセキュリティに対して体系化を試みんとするものである。

2．コンピュータ・システムのセキュリティ診断の体系

セキュリティという用語は，危険・脅威などからの解放そして，安全に保つことである。では，コンピュータ・システムのセキュリティとは，システムに対する様々な危険や脅威〔７〕によって受ける自然的又は人的な災害・事故・障害・エラー・犯罪等に因って引き起こされるであろう又は引き起こされた損害損失に対して，極力少ない費用で，これらを防止・除去・回復する対策措置を講

ＥＤＰシステムの構成要素	
ハードウエア	中央処理装置、　記憶装置、　入出力装置、　その他周辺機器
ソフトウエア 　プログラム 　データ類	システム・プログラム、　オペレーティング・システム アプリケーションプログラム システム設計書、　フローチャート、　マニュアル類 ドキュメンテーション（電磁気的記憶、非電磁気的記憶） 原始データ、　インプット・データ、　アウトプット・データ
データ通信 ネットワーク回線	回線、　回線機器、　端末装置、　モデム ユーザー・サブシステム、　ターミナル・インターフェイス
人　間 　オペレーター 　システム開発者 　保守者	（利用者及び利害関係者） センター・オペレーター、　端末オペレーター 経営者、　管理者、　システムズ・エンジニア、　プログラマー ハードウエア・保守者（ＣＥ）、　建物・設備保守者 通信回線保守者
用品など	磁気記録メディア、　カード、　用紙、　その他
建物付帯設備等	建物、　部室、　電源設備、　空調設備、　その他

図１　ＥＤＰ・システムの構成要素

ずることであると考える。ここで捕らえているコンピュータ・システムの構成要素を図１に示す。コンピュータ・システムのセキュリティには，企業における重要な情報を取り扱う情報処理機能を損なわなくする管理行動の一面（コンピュータ・セキュリティ）と情報あるいはソフトウェアやデータの機密性の保持管理（データ・セキュリティ）と言う二面を持つものと考えられる。このようなシステムのセキュリティを診断することは，企業の外部からも客観的に，そして科学的に，システムに対する各種の危険・脅威を，事前に評価・認識し分析して被害から回避，又未然に有効で適切に防止する対策を検討し選択して，コンピュータ・システムの管理者・企業の経営者へ勧告，助言することであろう。もし，その対策措置が実行されたならば，その後のフォローアップが必要であり再度，有効に機能しているから確認することである。セキュリティ診断は企業診断と同様に広範囲の事像を取り扱い様々な観点から綜合的に評価分析することが必要である。従ってセキュリティの診断を方針・理念から手順，対象，対策措置に大別して，その体系をより明確にする。

３．セキュリティ診断の方針・理念

コンピュータ・システムに対する危険を防止・回避し損害発生を未然に防ぐために第１番目に，セキュリティの方針を明確にしなければならない。診断の対象がどの程度の安全性を求めているか，その目標安全度〔８〕を設定すれば，そのレベルの安全度を確保することは可能である。又，そのために講ずるべき対策・措置の数は多くある。目標安全度は，できるだけ定量的に表わすべきであり，例えば許容ダウンタイムや，受けるべき危険からの予想される損害による金額換算で表示することが望ましいと考えるが，定量化されにくい要素が多いので，最小限，維持すべきシステムの機能やデータ，あるいはプログラムなどについて定性的に記述することによってでも方針の目標を設定すべきである。特に重要な点は対象となるシステムのハードウェアよりもソフトウェアであること。一般的にはシステムのハードウェアは交換取り替えが容易であるのに対して，データやソフトウェアは，その記憶の状態から一般的には再生が非常に困難であるか，不可能である場合が多く，その再生に要する費用は莫大になることが多いと考えられる。従って，診断方針を設定する場合，①システムの機能が停止する。遅延時間の許容限度。機能停止により業務の遂行がどの範囲まで許されるか。②システムに蓄積されているデータの重要度。データ破壊又はなくなった場合，復元再生に要する費用と時間分析。③システムに蓄積されているデータの機密性。データが漏洩した場合の企業経営に与える影響の分析診断を行う。特に機密性は診断方針のうち

システムのセキュリティ診断体系

方針・理念
（戦略的　管理的　業務的）

セキュリティ診断の手順

1　診断の基本方針の決定

2　危険度の事前評価、確認、分析

3　コンピュータ・システムの安全対策措置の検討、構想

4　勧　告、助　言

5　コンピュータ・システムの安全対策措置後フォローアップ

セキュリティ診断による対策措置

①　未然防止策・拡大防止策
②　迅速応急策
③　復旧策・再開処理

物理的対策	管理的対策	技術的対策
緩衝地帯	運用管理	ソフトウエア
構造の改善	組織計画	構造化設計
耐火構造	教育訓練	テスト法
耐震構造	入退室管理	ハードウエア
耐水構造	環境整備	二系統化
施設設備改善	保管管理	診断機能
消火設備強化	保守点検	通信回線
移転分散化	緊急管理体制	識別技術
バックアップ	暗号化	
開発作業管理		

セキュリティ診断の対象・範囲

（システムに対する危険・脅威・損害）

1．一般的危険要因

（自然的災害）
火災・水害・台風・洪水・地震・風害・氷雪害・塩害・落雷・動物害
爆発・人為的破壊
建築物施設・附帯設備機器障害・静電気影響
供給電源設備障害
電圧電流変化　停電　瞬電　周波数変動
（故障・エラー）
システム（ハードウエア）障害・不良
演算装置・記憶装置・入出力装置
周辺端末機器・データ通信回線機器
オフライン機器
システム（ソフトウエア）障害・エラー・バグ

2．システム運用管理における危険要因
（人的災害 → 意図的・非意図的）
↓
事故　不正　犯罪　怠慢

運用管理制度不備
教育訓練不足
運用管理規定不備
システム取り扱い不良
ハードウエア管理不良
ソフトウエア管理不良
データ・ファイル管理不良
ドキュメント管理不良
システム開発設計不良
設備設計施工不良

3．システムの損害形態

焼失・熱分解・煙害・汚損・腐蝕・浸水冠水・塵挨障害・損傷砂壊・構内、建物への侵入
コンピュータ室・ファイル保管室などへの侵入
データ消滅・漏洩・変形・破壊・盗用・改ざん
システム不正使用
システム・ダウン
コンピュータ・エラー
データ・エラー
盗聴・漏話・通信システムへの侵入
損傷破壊・障害回復時間延長
損害の拡大・信用失墜

図2　セキュリティ診断の体系図

でも戦略的レベルや，管理的レベル等の経営組織の上層で重要な問題である。しかし，企業の全データは原則には機密性を有すると考えるべきである。目標安全度を確立するために必要な費用は最小でなければならない。対策措置によって発生する費用は直接的に企業利潤を増加させる訳ではなく極力低く押さえなければならない。

4．セキュリティ診断の手順・方法

診断の手順・方法は，大きくわけて５つのステップになる。図２に体系図として示す。第１番目の基本方針の決定は，上述の通り，費用対効果あるいはそのシステムの経営的レベルでの安全目標を明確にしておく。第２番目は，システムに対する危険脅威の度合いを，事前に評価し，何が危険であるか確認し総合的に分析することである。診断の対象について，全般的大局的に危険度の確認評価を行なうには，チェックリスト〔８，９〕等を用いることが有効で，そこで検出された疑問点問題点については個別に詳細に確認をすることが必要である。システムに損害を与える危険・脅威は，自然現象と人的要因からなっていることは先に述べたとおりである。人的要因では，意図的又は故意によって生ずる損害と，非意図的なものとがある。自然からの損害はシステムの破壊を生じさせるだけで，システムの情報・データの不正な変更や機密の漏洩はないが，人的要因によってのみ，重要な情報・データの変更，盗用がなされるわけで，特に人間の関係する危険は複雑化している。診断の基本目的は，損害に係わる出費の極小化であるので，基本方針でも金額で表現する定量的な評価が分析ステップでも要求される。定性的に表現されるのでは対策に対する意思決定が困難である。従って，分析評価では，損害発生の確率と，損害が発生した場合の予想される出費の金額を予測することが必要である。事前に評価することは大きな診断の目的であるが，顕在的に検知された危険への迅速な対応も必要であり，損害の拡大を防がなければならない。そして，分析評価上の重要点は，今までに発生した危険の損害の履歴を活用することで，いかに危険が発生し，いかなる被害をもたらしたかが確実的な実績として理解できるからである。これらの実績データ履歴を十分に活用して，発生し得る被害の程度を予測することである。そして，過去にない様々な危険脅威が起こりうるので十分な推定予測が必要である〔10〕。第３ステップのコンピュータ・システムの安全対策措置の検討構想では，前ステップの分析結果の資料をもとに対策措置を検討する。主要な安全対策は，危険脅威の低減，抑制対策である。それは，管理的対策，物理的対策，技術的対策から構成される。又，対策には防止策，事後の応急策，復旧策があるが，診断では，事前対策を主眼点としている。更に，低減対策のうち，危険脅威を分散することも重要で，集中化を避ける方式も考慮すべきである。そして，もう一点はコンピュータ総合保険や情報処理開発業者賠償責任保険〔11〕を有効に使う方式で事後の損害に対する保障を考えるべきである。このように，対策措置は，物理的，管理的，技術的側面から，検討されるが，診断の目的は企業経営管理の一部門として認識することであり，管理の対象としてシステムの技術，物理的装置設備建物をも含むものである。そして人間が行う管理組織体制によって，システムをより安全な方向に向けることであり，その成否は，そこで業務を遂行する人間によって左右される部分が多く，実際の業務遂行には，責任の所在と権限を明確にしなければならない点が重要である。又，組織の中の内部としては，業務遂行のしやすさと正確さを維持し，危険を抑止する仕組みを持つことは，当然であり，内部の，牽制制度の充実である。そのため，責任の分割化と職務の分離が考えられ，重要な機能をもつ業務は同一人に全部をまかせるのではなく，必ず２人以上，複数の人に分担させ，各自の責任の範囲を限定することをさす。そして，業務を分割しあい，他人の仕事の結果を自然とチエックし，監視し合うので組織の信頼が高ずる。さらに業務の流れの中で，適切な点において，仕事の状態を評価する管理ポイントをもうける仕組みを組織に持たせる点を考えるようにすることである〔12〕。

5．セキュリティ診断の対象・範囲

セキュリティ診断の顕在的対象範囲は図１の如くコンピュータ・システムの構成要素であり企業の情報処理機能と又これに付随する設備建物等も，システムの業務に携わる人間も包含した広範囲な要素から構成されている。それは具体的体系は，①ハードウェア，②ソフトウェア，③データ，④通信回線，⑤人，⑥用品等，⑦建物，付帯設備等であり前述の様に複雑に結合融合され，大規模なシステムになればなるほど脆弱な点が生じて来る。セキュリティ診断では，その脆弱性を検出認識すべく潜在的危険要因を診断評価することになる。システムが被るであろう損害は大別すれば，①人的災害（意図的，非意図的）②自然災害であり両者の複合から①一般的危険要因が，前者の運用管理の不備不足から，②運用管理における危険要因とに分類される。一般的危険要因は火災，地震，水害などの自然災害，供給電源やシステムのハードウェアの異常や障害故障不良そしてソフトウェアのエラーである。運用管理における危険要因は主として企業又はシステムの利用者の運用管理上に問題点があり運用管理組織の不備，教育訓練不足，管理規定の不備などで

ある。これらの危険要因が様々な損害をシステムに与えてしまう事が有る。

6．セキュリティ診断による対策措置

コンピュータ・システムのセキュリティ診断により安全対策措置が検討構想されてシステムの改善強化復旧が実施されるが，基本的には三つの段階から成立していると考えられよう。第1には防止対策措置であり損失損害の未然防止であり，又は損害を最小限に抑える拡大防止である。システムを日頃から診断すること，即ち損失の発生の事前評価分析で危険要因を認識することが最も重要であり疑問の余地はない。第2は，応急対策措置で早期に検知して迅速に対応すること。万全の防止対策措置を講じてもシステムに対する損失被害は発生してしまうのであるが可能なかぎり早期に検知し回復しなければならない。第3は復旧対策措置で損失被害が発生し早期に対応しても後々まで種々の問題を残すことがあるので事後処理そしてシステムの再開処理が必要となって来る。次に対策措置をその内容的に類型化すれば上述の通り①管理的対策，②物理的対策，③技術的対策になる。第1の管理的対策はセキュリティ診断の最も基本となるコンピュタ・システムを取り扱う人間の要素が大きく，企業経営管理の一部門としても対策措置実施の効果は高く広範囲の危険要因に対応が可能である。具体的にはシステムを構成しているオペレータ，システム開発者，利用者，保守者の人的組織の計画運用，システムの利用方法，要員の教育訓練等である。第2の物理的対策ではコンピュータ・システムが一般的危険要因から安全に保護する対策で建物等の構造の改善強化であり自然災害からの損害を回避してシステムに付随している設備あるいは施設の強化改善である。第3の技術的対策はコンピュタ・システムのハードウェアそしてソフトウェアの技術の問題点を改良改善強化し損害を防止復旧することである。

7．むすび

以上コンピュータ・システムのセキュリティ診断の体系化を試み診断の方針・理念，手順，対象範囲そして対策措置について述べた。今日，コンピュータ・システムの技術革新が急激に進展する中，多くの技術的問題点は改善されていくであろうが，一層大規模で高度に複雑化するであろうシステム，特にデータ通信ネットワークやＶＡＮに又新しい種類の問題点や危険性を発生させてしまうことになろう。そこで，今以上の有効な安全対策への管理行動としてのセキュリティ診断の体系を企業組織内の管理の中へ融合させることが重要となって来ると考える。特に対策措置の中でも組織管理運営面での十分な考慮が基本的に機能する様に高度化し，システムに携わる人間と組織がセキュリティに対し高い認識を持つ様にしなければならない。

参考文献

1．日本情報処理開発協会編，コンピュター白書1983, p.204，1983
2．通商産業省機械情報産業局，電子計算機システム安全基準，1977，1984
3．郵政省，データ通信ネットワーク安全•信頼性基準，1982
4．日本情報処理開発協会，システム監査実施への道路標，1980
5．日本公認会計士協会編，ＥＤＰシステムの内部統制，p.19，1981
6．青木茂男，経営診断の今後の展望，経営診断学会年報，第16集，p.54
7．日本情報処理開発協会監修，コンピュター安全性・信頼性対策資料，83年版，1983
8．行政管理庁行政管理局，データ保護マニュアル，p.13，1982
9．Leonald I. Krauss, SAFE, Security Audit and Field Evaluation for Computer Facilities and Information Systems, AMACOM, 1972
10．鵜沢昌和，コンピュター•犯罪とエラー，p.135，1982
11．岡本行二，田口孝弘，安全管理マニュアル，p.191，1980
12．鵜沢昌和，コンピュター，犯罪とエラー，p.166，1982

（受理　昭和61年1月25日）