運用効率を優先したIDCセキュリティの設計

中央コンピューター株式会社

■ 執筆者Ｐｒｏｆｉｌｅ ■

渡邊　明弘

1998年　中央コンピューター（株）入社
　　U社 物流システム運用管理
　　顧客SLA共同策定
2003年　I社 Webシステム運用管理
　　社内セキュリティプロジェクト参画
2005年 現在 K社
　　Webシステムの運用監視の方式策定

※SLAとは,コンピュータシステムを運営する側が提供するサービスの保証品質を明確にし,サービスを享受する側とその品質内容に対して合意を得た上で成立する準契約書.

■ 論文要旨 ■

インフラストラクチャーに定着したコンピュータシステムは，安定稼動が重要視されている.

しかし，昨今その安定稼動がセキュリティ侵害により脅かされる事例が多数報告されており，経営層を始めコンピュータシステムに関わる多くの人にとって悩みの種となってきた.

今回は，データセンタの設計を題材にして，運用管理者の立場から個々の要件を分析し，トータルセキュリティを実現する方法を考察した.

コンピュータシステムのセキュリティ対策としてセキュリティアプライアンス機器やツールの導入が採用されることが多い．更に，セキュリティを侵害する原因を追究すると「セキュリティポリシ」や「人の教育」が重要であるといわれている.

しかし，原因の究明と対策が施されているにもかかわらず，運用を回すという観点でセキュリティ対策を実施していないため、データセンタのセキュリティが完全に守られていない.

そこで，セキュリティの侵害要素を補う方法を【構造】と【人】の観点から分類することにより，運用管理者が実施すべき作業を明確にし，分類された各作業フェーズを実施していくことで堅実なセキュリティシステムを構築できると結論づけた.

■ 論文目次 ■

■ 図表一覧 ■

１．はじめに

１．１　当社の概要

当社は，富士通メインフレームを中心としたコンピュータシステムの顧客への導入をサポートする企業である．運用業務を中心に発展してきた経緯から，システム全般の維持管理に多くのノウハウを有する．

近年は，コンピュータシステムの基盤構築及び開発に業態がシフトしてきているが，依然として運用設計，コンピュータシステムの SLA 策定，セキュリティ対策の導入など，運用面での SI 活動を企業の強みとしている．

１．２　データセンターの特徴

今回対象とするデータセンタを**図１**に示す

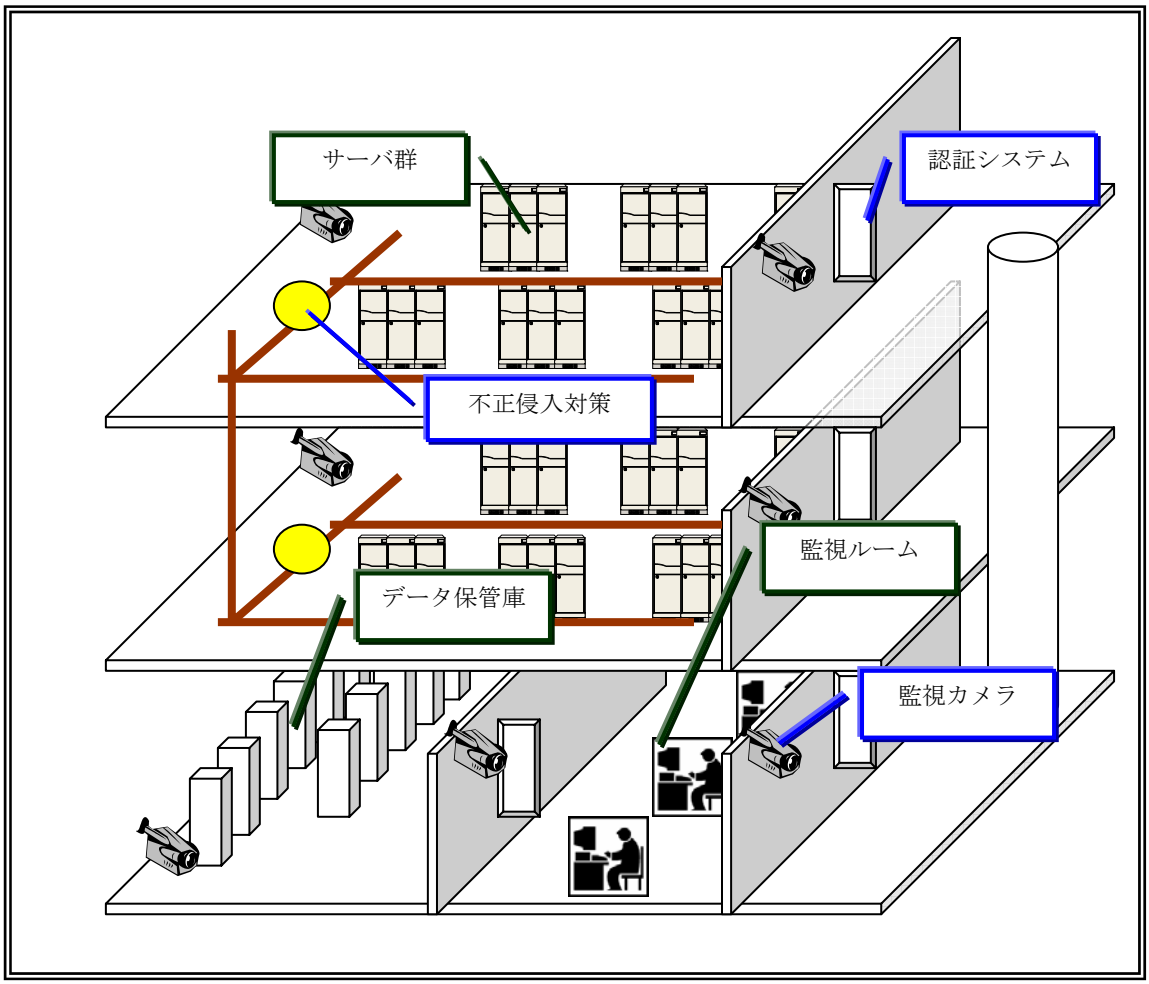

図１ データセンタの概要図

セキュリティシステムとして，監視カメラ・認証システム(指紋・虹彩など)，不正侵入対策(アンチウィルスソフト・ファイアーウォール・侵入検知システムなど)が導入されている．なお，今回の対象システムは上記データセンタであり，クライアントセキュリティを述べたものではないことに留意していただきたい．

２．経営戦略としてのデータセンタ

データセンタを事業の一環として運営する場合，セキュリティ対策が施されていることが利用者から要望される．そのため，どのようにすれば多くの顧客に利用してもらえるのか，費用を抑え価格競争力を持たせるにはどのように運用コストを最適化させるかを，経営戦略の一環として十分考慮した設計を行わなければならない．

セキュリティ要件を分析すると，以下のような理由が挙げられる．

（1）事業戦略の一環として顧客の信頼を得るために行うため
（2）セキュリティ侵害を受けることによる信用失墜を防止するため
（3）情報漏洩や企業情報の破壊にあった際の法的対処の準備をしておくため

顧客がデータセンタを活用するのは，従来の運用に加えて場所と要員の確保・セキュリティ対策といった業務にコストを掛けるメリットが本業と比較してあまりないことに尽きる．この前提に立つとデータセンタの引合いを行う場合，展示場のようにセキュリティ製品を設置し，従業員も服装が規定された物々しい仕組みが成り立つ．

しかし，本当にデータセンタとはこのようなあり方で良いのであろうか．運用効率の方が本来重視される設計なのではないだろうか．現在適用されているセキュリティを次章で分析してみたい．

３．見せるセキュリティはトータルセキュリティに貢献するか

３．１ 一般的な対策

データセンタではどのようなセキュリティ対策が実施されているのか．

（1）建物構造の対策
- データセンタの入り口に受付及びガードマンが配置されている
- コンピュータルームの入り口に IC カードや認証装置が装備されている
- コンピュータルームへの入退室は記録され，持ち物検査が実施される
- データセンター内の随所に監視カメラが設置されている

（2）コンピュータシステムの対策
- ウィルスチェックソフトがネットワークの入り口やサーバに導入されている
- ファイアーウォールが設置され許可された通信のみ通信許可されている
- IDS/IPS を設置しネットワークからの攻撃が監視・防御されている

（3）従業員の対策
- 業務上必要なものしかデータセンタへの持込みが許されない
- セキュリティに関する侵害行為をしないという誓約書を交わしている
- 正当な従業員であることを証明するための入館証を携帯している

これらを設置・導入しておけばセキュリティが確保できているように見える．事実ある程度は防ぐことができるのでここまでの対策で完了してしまっている．

３．２ 完全ではない一般的対策

しかし，既に知れ渡っているセキュリティ侵害の原因は，『内部情報漏洩』と『システムの設定不備・操作ミス』の 2 点であるという事実であり，表面から悪意を持った攻撃だけを防いだとしても企業の情報資産全体を保護する対策としては不十分であることがわかる．以下，図２の「セキュリティ３原則と実際」の図を基に分析していく。

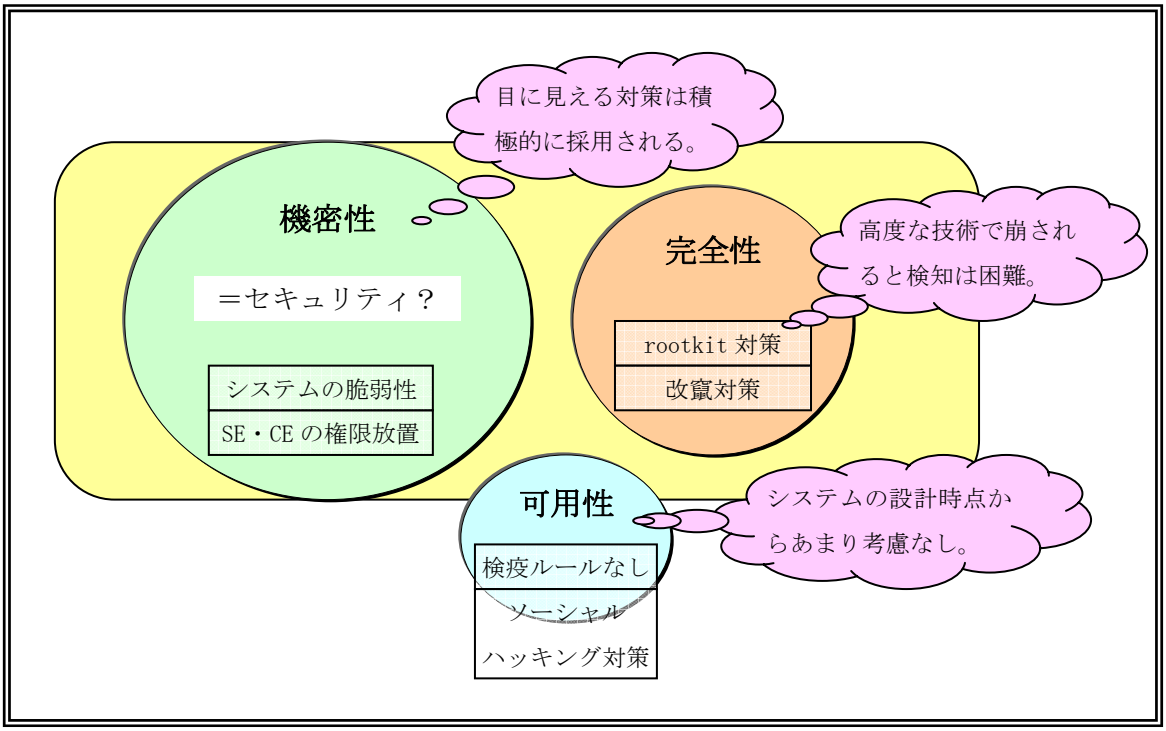

図２ セキュリティ３原則と実際(丸の大きさは対策の比重を表す)

３．３ 内部情報漏洩の分析

内部情報漏洩はデータセンタに入る権限とコンピュータにアクセスする権限が内部の人間には必然的に付与されており，内部の従業員に対して入退室制限を掛けるということは業務に支障が出るため，実質的な防御手段にはならない．そこで，従業員のモラル・教育及び監視という心理的な抑止策に行き着くのである．この対策の効果は非常に抽象的であり，セキュリティ担当者は管理するという目的を啓蒙活動を繰り返し実施することに殆どの労力を費やすことになる．

更に，内部情報漏洩に加担する人を分類して対応をとらないとセキュリティの３原則のバランスを崩すことになり，そのセキュリティ設計には歪が生じる．例えば，内部情報漏洩は内部の従業員と単純に定義してしまった場合，データセンタにおいては 24 時間 365 日働いているオペレータが"危険"ということになる．だが，彼らと同等の権限があってデータセンタ内部から活動でき，システムの仕様とサーバ操作方法を知っている SE の方がよっぽど"危険"度は高い． 障害対応で駆けつけた CE に関しても部品交換と称してディスクを簡単に外部へ持出すことが容易に認められている．

３．４ システムの設定不備の分析

次に，システムの設定不備であるが，システムの設計・開発上の脆弱性が挙げられる．近年の殆どのシステムには Web 技術が導入されている．企業ホームページ，営業や受注活動，社内情報共有のためのグループウェアなど Web を利用して行うことが普通に行われる．これらのシステムを利用する場合は，公開される領域(インターネット)から営業情報や取引先，個人情報が直接的ではないにしても接続されているため，システムの脆弱性や設定ミスから情報を漏洩してしまう危険性が高い．

今までの開発者や基盤構築者は業務を動かすことだけを考慮して事後の検証で，セキュリティの脆弱性を補うための知識とスキルをもって対処を施していない．

３．５ 操作ミスの分析

操作ミスに関しては，確認やチェックをしかるべきルートに乗せて実施する以外に対応策はないであろう．人間はいつもミスする性質をもっているので予測不可能な事故に巻き込まれた場合は防ぎようがない．

人為的なミスで情報漏洩してしまう例として，怖いのはソーシャルハッキングである．以前，総務所属の従業員を語る電話がシステム運用部門へ掛かってきたことがある．その時の話の内容は「座席表の調査」というものであった．別に，座席くらいと思いその自称総務部の人に伝えたところ，周到にも数ヵ月後に座席表のメンバに個人融資の勧誘電話が頻繁に掛かってくるという事態となった．座席表ではなく，コンピュータシステムやデータセンターのレイアウト図であれば，物理的な侵入経路を示すこととなり，後々後悔した経験がある．怪しいと思うか，疑わしいと思った時はどのように対応するのか事前に知識があれば防げた事例である．

３．６ 機密性の偏重がトータルセキュリティの歪み

実は，不十分な点を残すにしても基本的なセキュリティ対策を実施することで８割から９割のセキュリティ侵害行為は防御できるといわれている．

残りの 1 割のリスク対策を考慮する必要があるが，セキュリティシステムに完璧という対策がない以上，リスクを最小限に抑えるのが最も現実的な対策ということになる．

現実問題として漏洩してしまえばそれで終わりである．インシデントレスポンスという考え方があるので対応は採れるにしても，漏れてしまった情報を取り戻すことは難しい．漏れてしまった人の情報がネットワークに流れてしまえば対応は困難を極める．見てしまった人の記憶を消すのは不可能に近い．企業としては，漏れてしまった人からの問合せや法律相談，情報変更手続きのための費用補填などの対応をとり事後の営業リスクを軽減することができるが，金券や数ヶ月無料サービスで補ったとしても完全には保証されるものではない．

リスクは認識しているがどんな対策を実施しても完璧ではないからこそ，わざと目に見える対策を重視して満足しているためセキュリティ３原則の"機密性"への偏重という結果に至りトータルセキュリティを歪めていることがわかる．

４．データセンタの運用設計のギャップ

データセンタには，物理的に様々なコンピュータ機器が設置されている．業務としては，コンピュータシステムの運用とセキュリティの保持，予算があれば SE や CE を常駐させて基盤設計やシステム構築及び障害対応を行う．

ここでは，機器・運用・セキュリティをデータセンタの構成要素と捉え以下の手順で物理設計を行う．

（１）情報資産を分類
（２）情報資産の分類に重要度を設定
（３）運用効率の観点から物理的に情報資産の配置
（４）情報資産の重要度毎に再配置
（５）運用効率と重要度の要件が重なった場合は前者を優先する

[特徴]運用効率を考えた上で，セキュリティ対策でフィルターし，運用効率とセキュリティの両立を成す．

図３は，どのように情報資産を配置し，その情報資産を保護するかをイメージして図示したものである．物理的に重要度に応じて分けたり，他の顧客資産が混在しないように人の作業に必要な動きを考慮して配置する．従業員の権限に応じてアクセスできる経路をルール付けてしまえば不要な情報資産に触れることもなく，意図的犯行・作業ミスによる被害・監査証跡の分析といったセキュリティに関する運用が実施し易くなる．

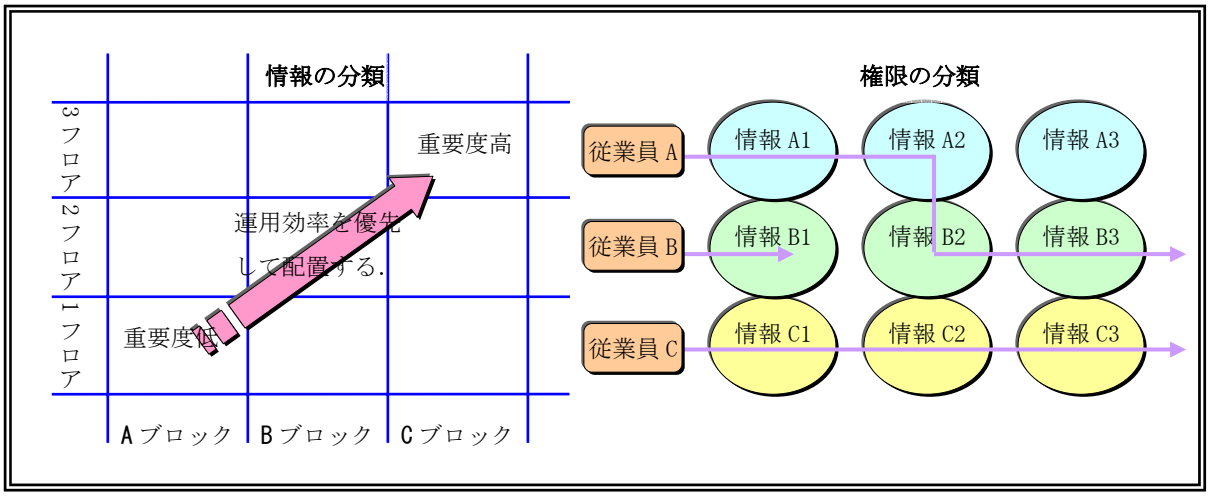

図３ データセンタの物理・論理概要図

運用効率とは人の動線のことである．セキュリティ３原則のうちの可用性に該当すると捉えている。なお，機密性と可用性は相反する要素でありどちらかを優先しなければどの程度のセキュリティレベルにするかという決断が下せない．

企業活動としては日々の運用業務を優先するのは至極当たり前の決断である．

クラッカーと称する高度な知識をもつ侵入者や，本当に犯罪を犯そうとして内部から活動を行う犯罪者に対応するには，上記対策では不十分である．逆にいえば，そこまでの対策はセキュリティに対する費用が嵩むため，現行業務を優先して実施しないという手段もありえる．しかし，データセンタの設計を見るとセキュリティ優先で実施されていることが多く運用設計を行う身にとっては運用上のギャップを至る所に発見する結果となる．

５．運用効率と堅実なセキュリティの共存を目指して

５．１ みえない脅威の具現化

セキュリティ管理は有権限者のモラルに期待するしかない．しかしながら，リスク管理という観点からは，モラルという抽象的な基準に信頼を置くことは適切ではない．

rootkit を仕掛けられたシステムは対応が難しい．rootkit とは，アクセス手段の確立，システムへの攻撃，証拠の隠蔽などセキュリティ侵害に必要な機能を集めたツールのことであり，ログを抹消したり，コマンドの出力結果を詐称したり，kernel 部分に直接働きかけて機能を歪めたりすることで，ファイアーウォールや IDS(侵入検知システム)などの既存のセキュリティシステムを骨抜きにしてしまうことができる．

これが１割の脅威に分類されるわけだが，rootkit の防御策を多くの予算を組んで施すよりはセキュリティインシデントが発生することを前提とした事後対応策を検討した方が現実的である．モラルなどのみえない脅威の対策も具現化することで可能となる．

５．２ セキュリティ対策の手法

図４は，ネットワークからの脅威と人的起因による脅威を比率で分類し，採れるべきセキュリティ対策を当て込んだものである．下の四角の枠内に記載してある対策はセキュリティの脅威全般に有効な対策である．

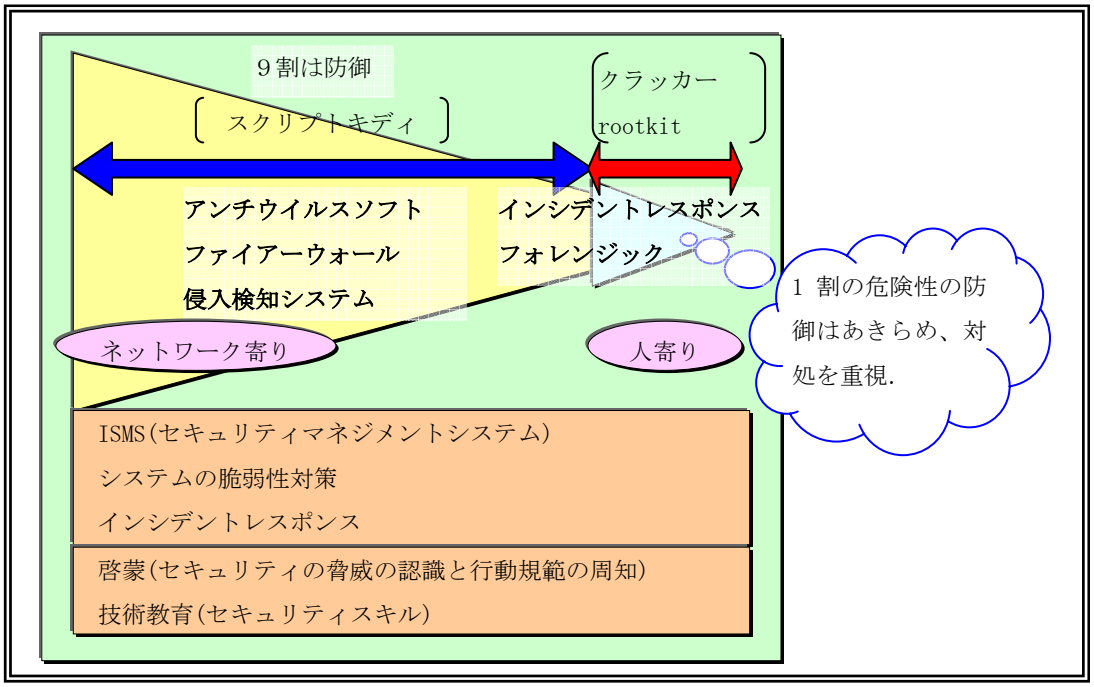

図４ セキュリティの脅威の比率と対策

図中の対策を簡単に説明する.

（1）インシデントレスポンスとは，「意図的及び偶発的なコンピュータシステムに対する人為的事象(セキュリティインシデント)が発生した場合の対策手順」のことである.

（2）フォレンジックとは，「法的措置を行うことを目的とし，事後において実際に行われた証拠保全，解析，それに伴う報告を行う科学捜査」のことである.

⇒セキュリティインシデントが発生することを前提とした事後対応策をとることが現実的であると述べたが，この事後対応策に有効な手段が[インシデントレスポンス]と[フォレンジック]である.

（3）ISMS とは，「情報セキュリティマネジメントシステムを意味し，情報資産をセキュリティの脅威から保護し，セキュリティ侵害に対する復旧するための仕組み」のことである.

⇒情報資産を分類する実効的な手法も公開されており，これをサンプルにして情報システムを管理することができる.

（4）啓蒙とは，「セキュリティに関する正しい知識を植えつけること」である.

⇒e-learning が有効である．過去にある顧客で個人情報保護対策が目的のセキュリティに関する教育を受けたことがある．これが従業員向けに作られおり内容も非常に充実していたため十分な知識を植えつけることができた．e-learning である特性上，全従業員の受講管理と教育環境の提供がスムーズにいった良い事例であるといえる.

５．３ 運用とセキュリティが共存するデータセンタの設計

データセンタを設計する際には，どの程度のセキュリティレベルを実現するのか最終形態をあらかじめ想定しておくと良い．表１には，四段階のセキュリティレベルに【構造(システムと資産の配置)】と【人(システムの従事者)】の面から対策分類してある．これをすべて適用できれば高いセキュリティを確保できる．但し，表の一番下にある運用面を考慮することを忘れてはならない．仕組みを作っても運用で回せなければ歪みにより結果として運用効率もセキュリティも実現できないことになる．むしろ，1 枚のポリシーと第一段階の対策を確実に運用した方が堅実なセキュリティシステムといえる．以下，要点を４つに絞って述べる.

（1）セキュリティを確保する上で最も重要なことは，企業としてのルール(ポリシー)があることが大前提となる．常識的なことかもしれないが意外とこのポリシーがなかったり，現状とポリシーがあっていない場合が多い．セキュリティポリシーを策定する際に，運用面を考慮した規定を盛り込んでおけば一冊のルールブックでデータセンタの設計が行えるので便利である．新規に情報通信システムを構築する顧客は少ないので第二段階の対策を施すタイミングで実施すると良い.

（2)既に述べたが情報漏洩などのセキュリティの脅威は内部の有権限者が起因している．業務上彼らから権限を取り上げることはできないのでモラルとセキュリティインシデントに対する正しい知識を植え付けることでセキュリティを維持し，情報資産を保護する．そのために，人のモラルとスキルの養成を行う.

（3）運用効率を考慮してデータセンタの物理設計を行う．※４章参照

（4）既存のセキュリティ対策で９割のセキュリティ侵害を防ぎ，残りの１割をどう対処するのかを考える．ここでは，インシデントレスポンスとフォレンジックの採用である．

	第一段階	第二段階	第三段階	第四段階
システムへのセキュリティ施策	ウィルス対策ソフト ファイアウオール 侵入検知システムの導入	啓蒙 技術教育 ※対象はシステムに関わる人	構造上のシステム脆弱性検査	ISMS の適用インシデントレスポンス フォレンジック
セキュリティ担当者の役割	上記，システムの維持管理 セキュリティ関連情報の収集	OS の脆弱性 Web システムの問題 ログ解析 の知識と手法の習得	ハッキング手法の検証と防御知識の習得	上記，施策の PDCA 運用管理
基本思想	運用効率(管理の手間を省く，運用担当者の動線)を常に優先して考える			

<新規>(殆どあり得ない)
セキュリティポリシーの策定
情報資産の分類
データセンタの設計

<既存>
セキュリティポリシーの策定
情報資産の分類と配置
データセンタの設計見直し

表１ セキュリティ対策の適用フェーズ

６．終わりに

本文においては経験と今まで見聞きしてきたことを参考にして筆者が独自に分析し，解決策を構成したものである．表題は，実際に運営されているデータセンタがベースになっており，その運用面での疑問を考察してある．その中でもやりたかったことは，運用面での疑問を認識していながら，その根拠を示すことができなかったがために運用効率もセキュリティも中途半端なまま改善が行えず運営してきてしまった反省の払拭である．

第５章の内容は BS7799 Part2 の詳細管理策の内容に近く，ISMS の適用に準じてデータセンタの設計を見直す機会に応用する予定である．

個人的な思想であるが，セキュリティ対策を堅牢に施すよりは，確実に運用できる施策を徐々にレベルアップしていく体制で堅実に施した方が実態の伴ったセキュリティ対策であり，経営戦略としての実行価値が高いと信じている．

※BS7799 とは，情報セキュリティを管理するための実践的なガイドラインを示した英国規格協会が発行した規範(Part1)および仕様(Part2)で,ISO や JIS にも採用されている標準規格．

参考文献

［１］p5 情報漏洩の原因(内部)･･･2003 CSI/FBI Computer Crime and Security Survey
［２］p5 情報漏洩の原因(設定不備・操作ミス)･･･2004年度　情報セキュリティインシデントに関する調査報告書(http://www.jnsa.org/houkoku2004/incident_survey.pdf)