情報システムに於けるリスク管理の展望

白　石　髙　義

（受付　2006 年 5 月 10 日）

Abstract

This paper surveyed problem of information security and view the future.

At first, on a human action about information system, I examined a cause of a risk and looked at a cause of a risk by electronic commerce as an example based on system specifications.

Same as above, a cause of a risk has to examine this because we should be able to discover risk from each place of a design document.

Next, this paper described a basic design of multi dimensions risk analysis mechanism and examined a simulator on risk analysis.

In late years a Capability Maturity Model for software became a topic. So this paper examined a property of a risk with each level of a growth process of information system.

1. は　じ　め　に

長年情報セキュリティの研究を続けてきたが，これを振り返り情報システムのリスク管理に付き今後の研究のあり方，方向づけをしたい。

情報システムにはリスクは必然的に存在するが，事件が発生した時点で，その原因，対策を行うことが従来のリスク管理手法の主流であった。

ここで，事故の発見，特にあり得ないと思われる事故の発見をどのようにするのか，そのシナリオはどうなるのかを検討したい。

このためには，

1，システム設計，仕様，性能をチェックしリスクの発生源を検出する。

2，事故シナリオのシミュレーション。

3，情報システムの成長サイクルにおける対応。

などを検討する。

また，多元リスク解析への要求がある。

1，多様なリスクがあり，その関係が複雑である。これを整理し，関係を明らかにしたい。

2，個別のリスクについても多元的，多様な環境があり 1 元的に論じることができない。したがって，多元的，色々な角度から議論したい。

3，情報公開が求められている時世であり，これを満たしたい。

この件については，解析機構の構想を提案する。

2. リスクの原因

リスクはシステムが期待したように動作，反応しない状態を呈することにある。それには，システムの寿命，故障など自然の物理的な事故とシステムを運用，利用する人に起因するものがある。ここでは。前者のことは取り上げないで，後者の人に起因する事柄を検討する。

情報システムは，人と人との間で情報を交換しあうのを媒介するものであり，その間には信用関係により成立している。

不正な行為。他人に経済的負担を与える行為。

邪な行為。

無責任な行為。他人の名誉，信用を失墜させる行為。

不快感を与える行為。

これらは在ってはならない。またこのようなことを受けた場合これはリスクとなる。

これはまた，異常なデータを発生させることにもなる。この原因には，操作ミスなどによるものも在る。

情報システムは，前述のように人と人との情報交換を目的とするものでありながら，対人関係は情報機器に向かって行い，相手の顔が直接見えないため，不注意，自己中心的な行為，ゲーム的感覚での行動がともすれば行われてしまう。

また，ネットワークは全世界に広がったため，距離感，時間感は以前とは全く異なってしまった。瞬時に世界の果てまで交信可能であり，宗教，倫理，生活感覚の違いによる意外な結果，思いも因らない事件に巻き込まれることもある。

3. システム仕様のリスクの原因

システム仕様を検査して，リスクの原因を発見しよう。

そもそも，システム仕様は，システムに期待する性能を要求することを重点にまとめられている。従って，これに起因する障害は，十分考慮されてない。

1例として，ネットによるインターネット・ショップを例に調査しよう。

客は，Web のインターネット・ショップにて商品カタログを見て，購入したい商品を選び発注する。

売手は，商品を発送する。

客は，商品と引き換えに代金を払う。

このシステムで，韓国では強盗が発生したと伝えられている[1)]。犯行は，男女2 人組により，商品と代金の引き渡しの際起こった。

犯行の手口は，女が客に「商品が近くに有るので，代金を持ってとりに来てください。」と言い，客を空き家に連れて行くと，そこに男がいて，凶器を突きつけて金銭を強奪した。この犯行は，2，3 度行われた後に，検挙されたとのことである。

これとは別に，商品が実際はないのに受注したとき，先物取引をすることによるリスク，いざこざなどの不正な行為が生じないだろうか。

また，仮想取引による粉飾決済が生じる可能性もある。

このように色々のリスクの可能性が考えられる。

ここではシステム仕様に素って述べたが，さらにデータの流れ等設計資料の各段階で検討すれば，リスクの原因は様々に発見できるはずである。

4. 多元リスク解析機構の構想

解析の基本は，集団発想法に基ずき，最適化決定手法を活用する。リスク波及の検討にはシミュレーションを行う。

集団発想法を採用するのは，リスクに対する十分な数量的なデータがないためもあり何らかのコンセンサスが必要となるためである。

波及分析に，情報セキュリティリスク波及分析（STA）を使ってきたが，これは疑似シミュレーションで骨格のみを表示していた。将来を指向するには，加速試験機のような，アニメィション・シミュレータになる。

なを，原因分析は，今後も残るのだが，波及分析を中心として，災害防止策を検討するべきである。従って，防止策による性能等の劣化，費用負担などの検討がどうしても必要になる。

このことを別の角度から見ると，原因分析，波及分析が各々切り離されて議論されてきたが，これにより統合できる。しかし，当然のことであるが，システム計画，設計などの，システム稼働前のリスク検討に波及分析を単独，または原因分析と組み合わして行うことになる。

5. シミュレータ

ここで使用するシミュレータは，図式表現が容易にできるもが好ましい，従って，Pro-

1） 報道ステーション：「ソウル市警密着24時 part 3 韓国ネット犯罪のすべてを撮った！」TV-朝日 3/16（http://www.tv-asahi.co.jp/hst/contents/special/060316.html）

graph, Stella のようなものが適している。

現在中心的に使用されている，C や Java などの言語は当然使用できる。問題は，プログラムの作成，アルゴリズムの理解の共有にある。

これには，計算量，アルゴリズムの複雑化が十分理解されなければならない。

また，加速度試験が実現したい，これは，波及分析に必要な要求である。

さらに，ライフサイクルの成長モデル（CMM）との関連を考慮しなければ効果が十分に発揮できないかもしれない。

これには，初期レベルでから，最高位の最適化レベルの各段階に対応できる分析ツールが提案できるかが重要である。

今後，量子コンピュータが実現すると，シミュレータの分野は大きく発展し計算量の問題もある程度解決する。これには大いに期待したい。

6. 成長モデルへの対応

近年話題になっている，Capability Maturity Model（CMM）は，ソフトウェアプロセスの発展過程を指し示したモデルである。これは，5 段階の成熟度レベルを規定している。

表　CMM の成熟度レベル[2)]

成熟度レベル	概　　要	特　　徴
1：初期レベル	プロセスが確立されていない初期段階	・作業が場当たり的で，時には混沌的 ・ほとんどのプロセスは未定義
2：反復できるレベル	基本的なプロジェクト管理が実施できているレベル	・日程，費用，機能性の初歩的管理プロセスを確立 ・おなじ領域の成功経験を反復できるプロセス規律の存在
3：定義されたレベル	組織的にプロセス管理を行っているレベル	・管理プロセスと開発プロセスの定義と統合化 ・全プロジェクトが文書化されたプロセスを遵守
4：管理されたレベル	プロセスおよびプロダクトの定量的管理が実施できているレベル	・プロセスとプロダクトの詳細な品質データを収集 ・データに基づいたプロセスとプロタクトの理解と制御
5：最適化するレベル	プロセス改善に全員が参加し，改善活動が日常化しているレベル	・プロセスからフィードバックと革新的技術の志向による持続的な改善

2）宮下：特集 CMM とは何か？　IT 自分戦略研究所
http://jibun.atmarkit.co.jp/fengineer/special/cmm01/ccm03.html

このように，CMM は，誕生から壮年期までのいわゆる成長過程をとりあげているが，システムは，誕生から青年，壮年期を経て，老年期に至りやがて終焉する。この間，リスクへの関心，扱いはどのように関わるのであろうか。

誕生した初期は，システムの性能の達成が最大の関心事であり，リスクへの関心は薄い。初期を脱した，青年期から壮年期はノウハウも充分蓄積され，リスク対応も行われる。

熟年期を過ぎ老年期に至ると，次世代システムの計画も進み，交代の時までの稼働を保つのが目的で，コストをかけた対策はできない。また，担当者は手薄になり，ともすれば，技術力が低下する。

このようにシステムの成長段階に応じたリスクへの取り組む姿勢を考慮しなければならない。

7. 結　　言

情報セキュリティの課題を整理し，今後を展望した。

まず，情報システムに関わる人間の行動を中心に，リスクの原因を検討し，システム仕様を基に一例として電子取引の例でリスクの原因を眺めた。これと同様に，設計資料の各所からリスクの原因は発見できるはずなのでこれを検討する必要がある次いで，多元リスク解析機構の基本構想を述べ，リスク解析のためのシミュレータについて検討した。

最後に，近年話題になっている成長モデルにつき，情報システムの成長過程の各レベルでのリスクの性質を検討した。