CREATIVE RISK MANAGEMENT BASED ON REVERSE THINKING HELPING WITH "INNOVATION"

Manabu Sawaguchi

The SANNO Institute of Management

SAWAGUCHI_Manabu@hj.sanno.ac.jp

Abstract

I want to propose "Creative Risk Management Based on Reverse Thinking (CRMBRT)" as one of the Future- oriented Risk Management Techniques in this paper. I've developed this method (CRMBRT) by using examples from "Subversive Analysis (SA)" as the origin of "Anticipatory Failure Determination (AFD)" developed by Ideation Inc. AFD is one of the contemporary TRIZ techniques. Therefore, it is clear that CRMBRT is in the TRIZ field.

To be more precise, based on this way of subversive thinking, CRMBRT initially requires us to create a lot of "bad ideas" for bringing failures or accidents in the system into reality, with the utilization of not only inventive principles in TRIZ but also functional analysis in VE by involving the environmental resources around the society, so that CRMBRT can clarify the mechanism of "Dangerous Scenarios (DS)" about "Unknown Risks (UR)" in the near future.

1. Introduction

The main purpose of "this method (CRMBRT)" is to consider the solutions against any "Dangerous Scenarios (DS)" through future-oriented thinking, and not by chasing causes related to past accidents.

Therefore, we have to develop effective techniques not only to facilitate the sensitivity for "Unknown Risks (UR)"but also to create innovative measures to avoid Future DS. Therefore, this method has a high possibility to lead to innovative ideas dealing with UR.

That is to say, there is strong evidence that "CRMBRT" is a highly-valued method as one of the "Innovative Management Methods in the IT-field" where it is likely to come up with UR based on technological innovation in the near future.

Therefore, in the latter half of this paper, I am going to consider the advantages regarding "CRMBRT" through a one case-study example about new business developments in the IT-field as specific as possible.

2. The various risks companies face

I am going to focus on a series of risks based on the IT field in this paper. However, as you know, Risk itself has a huge variety of aspects and it's said that the number of risks corresponds to the number of companies. Consequently, it's very difficult to define the risk in one sentence. I think however that I will try to outline the concept of risk briefly as mentioned below.

Definition of RISK (Companies face)

Risk is not only the serious losses a company suffers but also the environment within or outside the existing company brought about by serious losses.

Therefore, this study should be considered not only by the serious losses but also the side effects brought by the serious losses. In addition to the "Definition of Risk", I would like to define "IT-Risk" newly as mentioned below.

Definition of IT- RISK (Companies face)

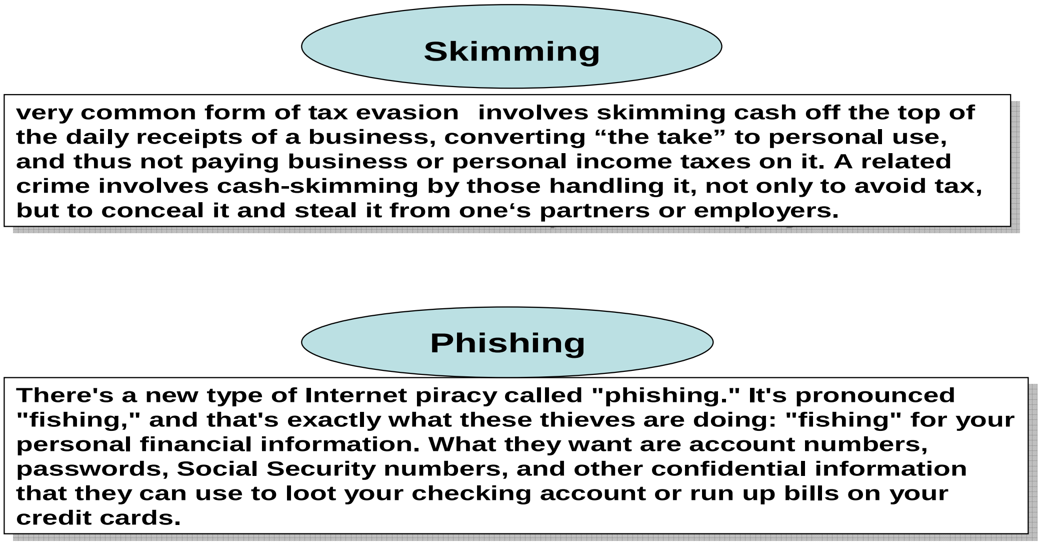
There are various side effects related to serious losses in the IT industry.

1. Losses about data gathering and processing with utilization of computer networking

2. The environment inside and outside the company

2a. Especially, losses regarding to information and telecommunications.

IT-Risks that are concerned in particular, especially real examples failing to take sufficient measures are shown in Fig.1.



Skimming

very common form of tax evasion involves skimming cash off the top of the daily receipts of a business, converting "the take" to personal use, and thus not paying business or personal income taxes on it. A related crime involves cash-skimming by those handling it, not only to avoid tax, but to conceal it and steal it from one‘s partners or employers.

Phishing

There's a new type of Internet piracy called "phishing." It's pronounced "fishing," and that's exactly what these thieves are doing: "fishing" for your personal financial information. What they want are account numbers, passwords, Social Security numbers, and other confidential information that they can use to loot your checking account or run up bills on your credit cards.

Fig.1 Examples about Risks in IT field

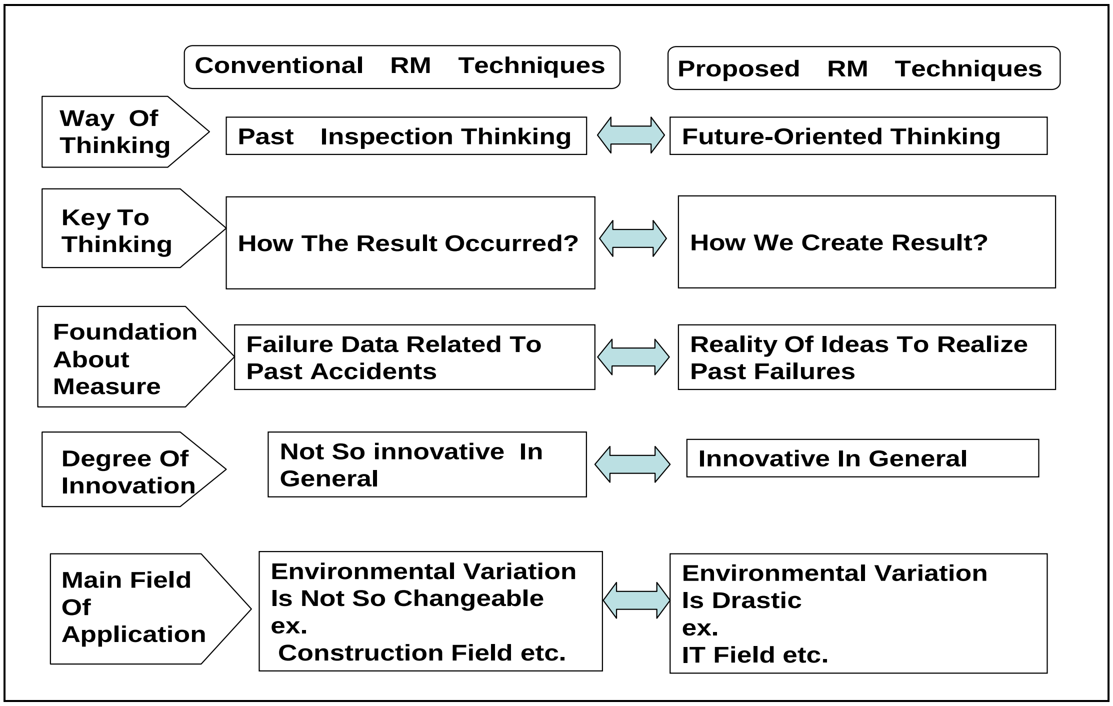
IT Risks like shown in Figure 1 are serious problems we've never faced before in our society. That's why taking sufficient measures against them is very difficult.

To put it more concretely, Effective solutions against IT-risks are required to utilize "Innovation power based on the future- oriented thinking". They are not needed to chase the causes related to the past accidents as much. as we need them for the future.

3. Features of this method (Reverse Thinking Approach)

In the case of IT Risks, It's clear that IT related technologies are growing rapidly and the environmental variation around them is drastic. In consequence, it is reasonable to suppose that the approach to inspection in the past will not take good measures against future IT-Risks. This is because IT-Risks like "Skimming" or "Phishing" do not decrease and effective measures are still under discussion, not put on a firm footing in Japanese society. Consequently, "Reverse Thinking Approach" is expected to actively utilize effective measures in such a scene. The purpose of this method ("Reverse Thinking Approach") is not to find out failure phenomenon from past accidents, but more importantly to define them as "a kind of matters to be realized". After we define then, we have to create the realized ways by utilizing "Functional Analysis in VE" according to the procedure of this method. This is the biggest feature about the "Reverse Thinking Approach".

In short, Future-oriented Risk Management (based on "Reverse Thinking") is very effective against "Unknown Risks", especially in the IT-field. This is because Conventional Risk Management (based on past inspection) does not deal with" IT-Risks" effectively. The Fig.2 shows some features of both Conventional and Proposed Risk Management techniques.



	Conventional RM Techniques		Proposed RM Techniques
Way Of Thinking	Past Inspection Thinking	⇔	Future-Oriented Thinking
Key To Thinking	How The Result Occurred?	⇔	How We Create Result?
Foundation About Measure	Failure Data Related To Past Accidents	⇔	Reality Of Ideas To Realize Past Failures
Degree Of Innovation	Not So innovative In General	⇔	Innovative In General
Main Field Of Application	Environmental Variation Is Not So Changeable ex. Construction Field etc.	⇔	Environmental Variation Is Drastic ex. IT Field etc.

Fig.2 Features of both Conventional and Proposed Risk Management Techniques

4. Practical Procedure of Reverse Thinking Approach

I want to consider both uniqueness and effectiveness about this approach through one of the case studies to have been applied. Fig.3 shows “Practical Procedure of Reverse Thinking Approach” I’m propounding. In consequence, I am going to introduce the case study according to the procedure.

This Case study focuses on the implementation of Risk Management in the “E-learning System for English Conversation”, which is B-Company’s acceptance of order about development and operation for “ESEC” from A- travel agency.

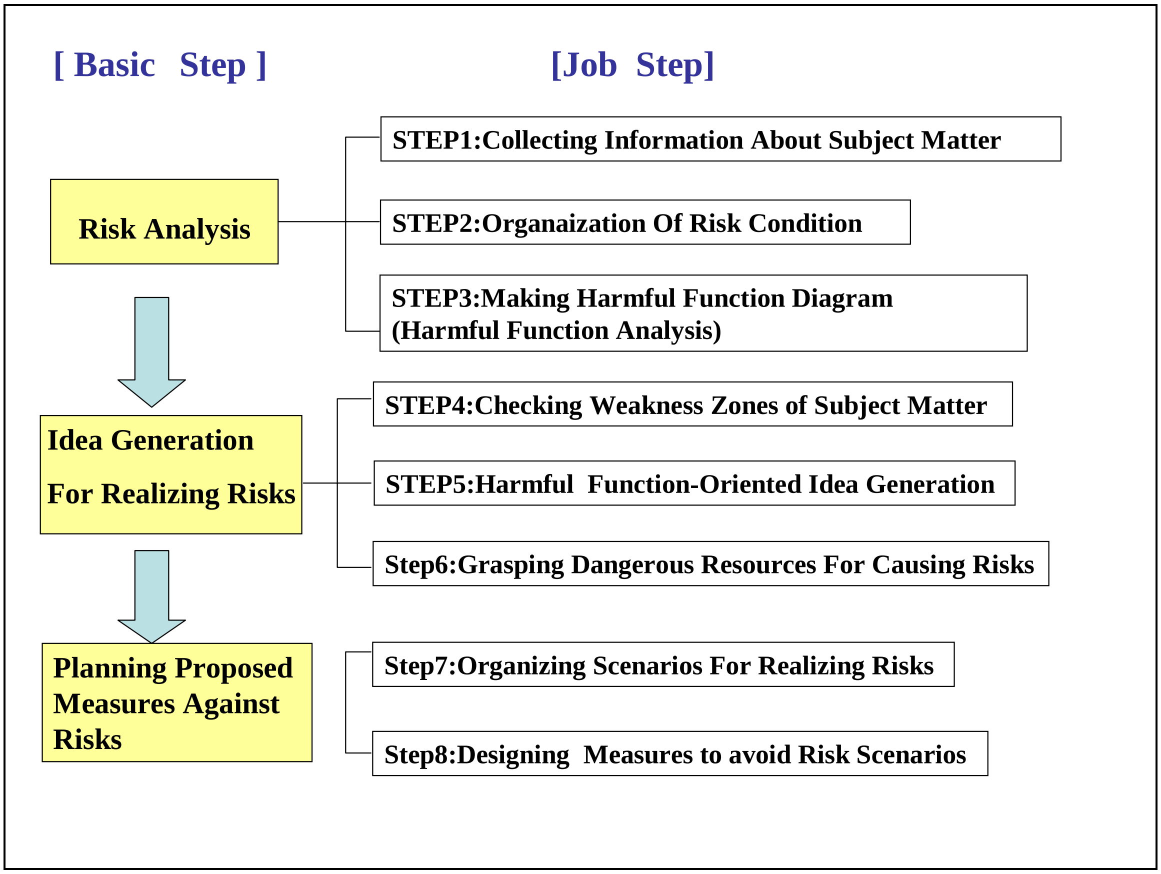
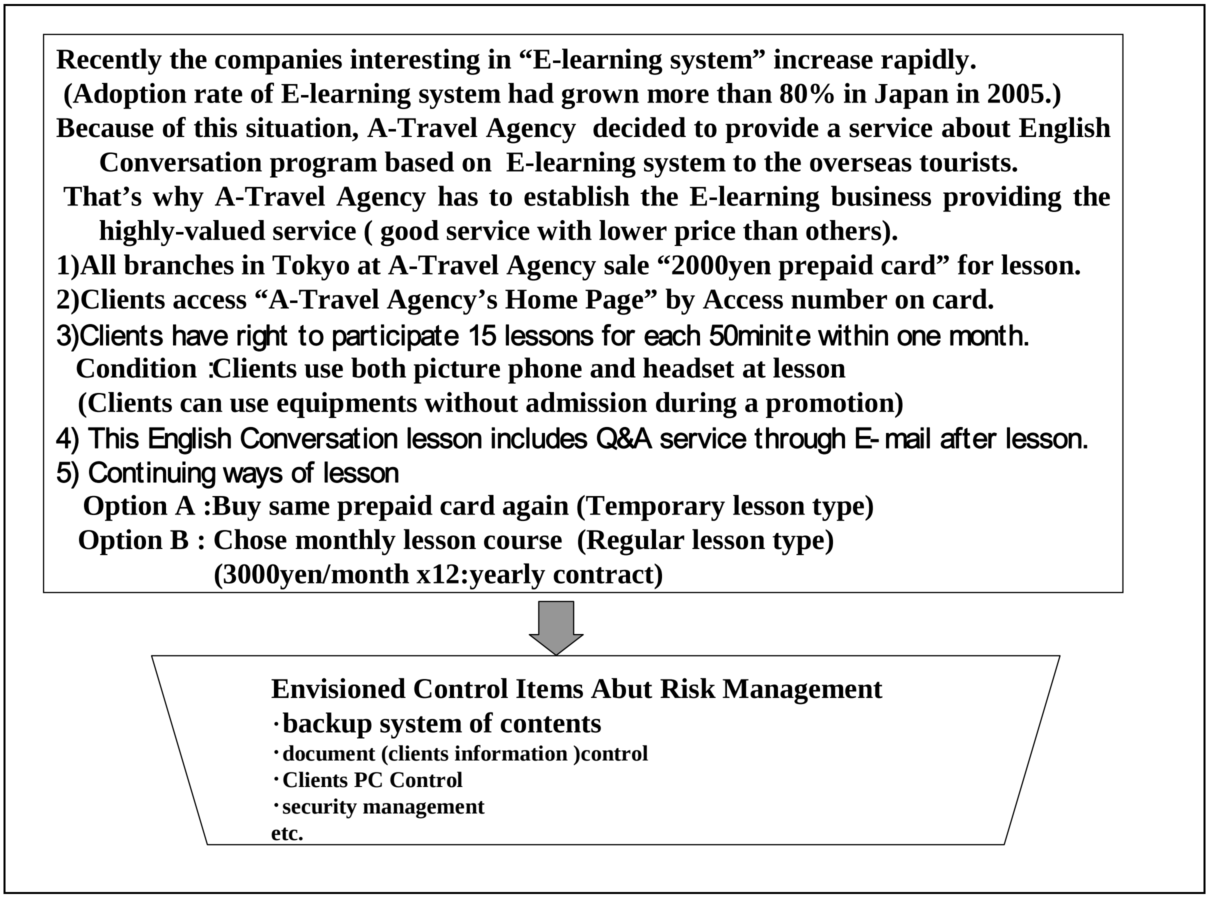

[Basic Step]
[Job Step]
Risk Analysis
STEP1:Collecting Information About Subject Matter
STEP2:Organaization Of Risk Condition
STEP3:Making Harmful Function Diagram (Harmful Function Analysis)
Idea Generation For Realizing Risks
STEP4:Checking Weakness Zones of Subject Matter
STEP5:Harmful Function-Oriented Idea Generation
Step6:Grasping Dangerous Resources For Causing Risks
Planning Proposed Measures Against Risks
Step7:Organizing Scenarios For Realizing Risks
Step8:Designing Measures to avoid Risk Scenarios

Fig.3 Practical Procedure of Reverse Thinking Approach

5. Case Study: Risk Management about the “E-learning System for English Conversation”

5.1 Step1: Collecting Information About A Subject Matter

Subject matter for Risk Management should be defined. As I mentioned above, Subject matter showing in this paper is “Development and Operation for E-learning System for English Conversation”. In short, Subject Matter is in the field of It-Risks related to information and telecommunications systems and the Overview of SM is shown in Fig.4.



Recently the companies interesting in “E-learning system” increase rapidly.
(Adoption rate of E-learning system had grown more than 80% in Japan in 2005.)
Because of this situation, A-Travel Agency decided to provide a service about English Conversation program based on E-learning system to the overseas tourists.
That’s why A-Travel Agency has to establish the E-learning business providing the highly-valued service (good service with lower price than others).

1)All branches in Tokyo at A-Travel Agency sale “2000yen prepaid card” for lesson.
2)Clients access “A-Travel Agency’s Home Page” by Access number on card.
3)Clients have right to participate 15 lessons for each 50minite within one month.
Condition :Clients use both picture phone and headset at lesson
(Clients can use equipments without admission during a promotion)
4) This English Conversation lesson includes Q&A service through E- mail after lesson.
5) Continuing ways of lesson
Option A :Buy same prepaid card again (Temporary lesson type)
Option B : Chose monthly lesson course (Regular lesson type)
(3000yen/month x12:yearly contract)

Envisioned Control Items Abut Risk Management
･backup system of contents
･document (clients information)control
･Clients PC Control
･security management
etc.

Fig. 4 Overview of Subject Matter

5.2 Step2: Organization Of Risk Condition

We have to organize the situation about the “Envisioned Risks (defects)”, which might occur in the near future, at this step. To be concrete, we have to organize the relationship between the final losses (final serious results) and causes brought about by them from the point of view causality analysis. (See Fig.5)

The work at this step is essentially the same as usual "Past Inspection Thinking "(Conventional Risk Management Approach).

5.3 Step3: Making Harmful Function Diagram (Harmful Function Analysis)

We tried to make the "Harmful Function Diagram" showing the relationship between "the final loss= top harmful function" and "each cause brought about by each loss=each harmful function". Its diagram must be drawn by utilizing "Organization Table of Risk Condition (See Fig.5)" at the previous step. To put it more concretely, we have to make that diagram (See Fig.6) according to "Functional Analysis" based on "purpose and means logic", which is the technique to organize each function. FA is one of the techniques in the VE field. However, as VE practitioners know, FA usually focuses on useful function (It's called just function in VE). But, in this case, we have to focus on harmful function. In order to define harmful function, we have to define a cause as a function. To put it another way, each function must be defined by description method showing "verb and noun in English". After that, each function would be organized by "purpose and means logic in FA".

Final Losses (Final Bad Result)	Causes Bring About Final Losses
The huge asset loss and erosion of company's trust.	1) ID and password were robbed 2)Failure of headset 3) Appearance of illegal prepaid card ………
Erosion of company's trust because of increase of complaint about the system operation	1) Impolite teachers 2) Complaint related to the answer to a question 3)crossed sending about the answer 4) Trouble about playout and uplink 5) Loss of individual information
Erosion of company's trust because of out-of-service state	Out of order in server ………

Fig.5 Organization of Risk Condition about Subject Matter

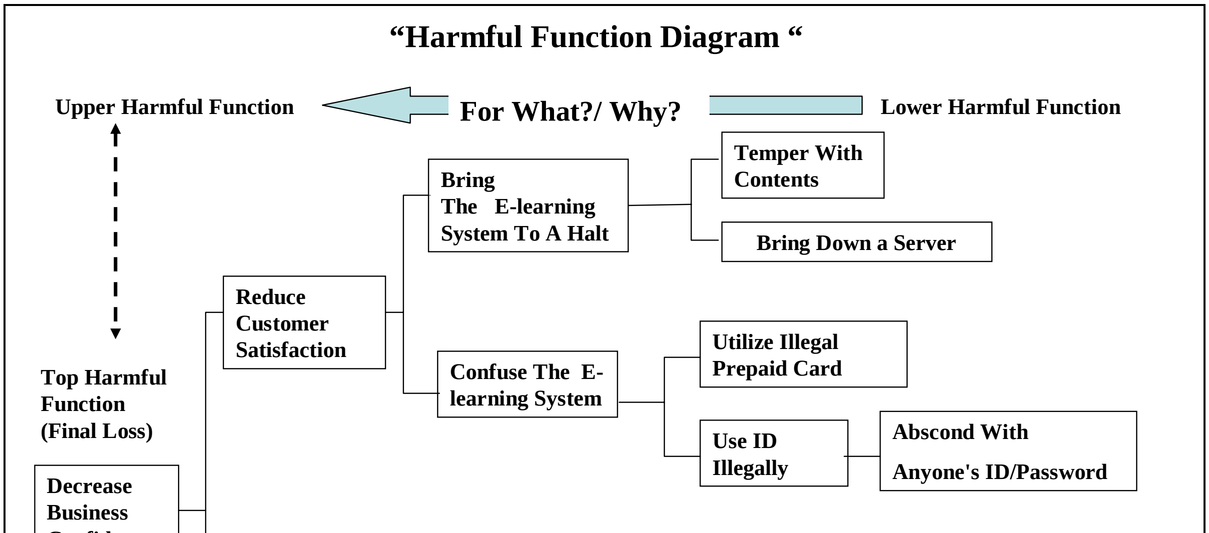

"Harmful Function Diagram "
Upper Harmful Function
For What?/ Why?
Lower Harmful Function
Bring The E-learning System To A Halt
Temper With Contents
Bring Down a Server
Reduce Customer Satisfaction
Confuse The E-learning System
Utilize Illegal Prepaid Card
Use ID Illegally
Abscond With Anyone's ID/Password
Top Harmful Function (Final Loss)
Decrease Business

Fig.6 Harmful Function Diagram

5.4 Step4: Checking Weak areas of Subject Matter

At step4, distinguishing Weak areas from others in the subjects matters, we have to define Weak areas as “the big triggers” to bring about the final loss. On the other hand, well-protected areas, which are stable against causes brought about by the serious losses, exist in it too. Weak areas in the case study are shown in Fig.7. Especially, the areas we’ve never made an inspection before, which might be weak areas. Because, these areas have never caused serious accidents to happen for a long time, even without precaution measures.

That is to say, above-mentioned weak areas are a kind of “blind side” for the human-being. Therefore, through step4, we need to recognize and to define thoroughly “what weak areas are”, because, dangerous resources in the subject matter might lead to harmful functions connected with weak areas.

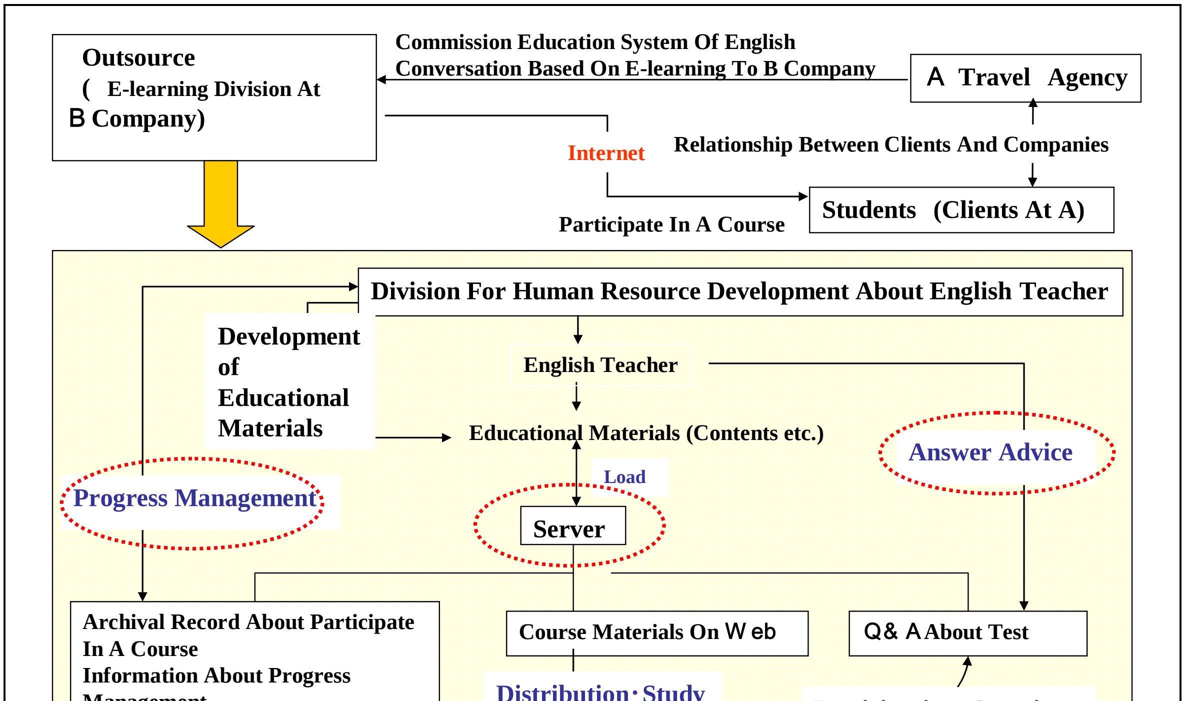

Outsource
(E-learning Division At
B Company)
Commission Education System Of English
Conversation Based On E-learning To B Company
A Travel Agency
Internet
Relationship Between Clients And Companies
Students (Clients At A)
Participate In A Course
Division For Human Resource Development About English Teacher
Development
of
Educational
Materials
English Teacher
Educational Materials (Contents etc.)
Answer Advice
Load
Progress Management
Server
Archival Record About Participate
In A Course
Information About Progress
Management
Course Materials On Web
Q& A About Test
Distribution: Study

Fig.7 Weakness Zone in the Case Study

5.5 Step5: Harmful Function-Oriented Idea Generation

After checking on the harmful functions connected with weak areas (See Fig.7) in the diagram (See Fig.6), beginning with the harmful functions penetrating weak areas directly, we have to grasp “the critical path on the diagram(See Fig.8)” consisting of a series of harmful functions, which could be connected with final losses (top harmful function) logically. Then, we are going to create a lot of ideas to realize a series of harmful functions as broad as possible, with focusing on the critical pass, based on “the way of function-oriented thinking” in the VE field. But this time, in order to break free from fixed thinking like “past inspection activities”, we must move “Normal Site” in VE activities to “Reverse Site” in Subversive activities. In this case, Fig.9 shows examples about idea generation based on harmful functions.

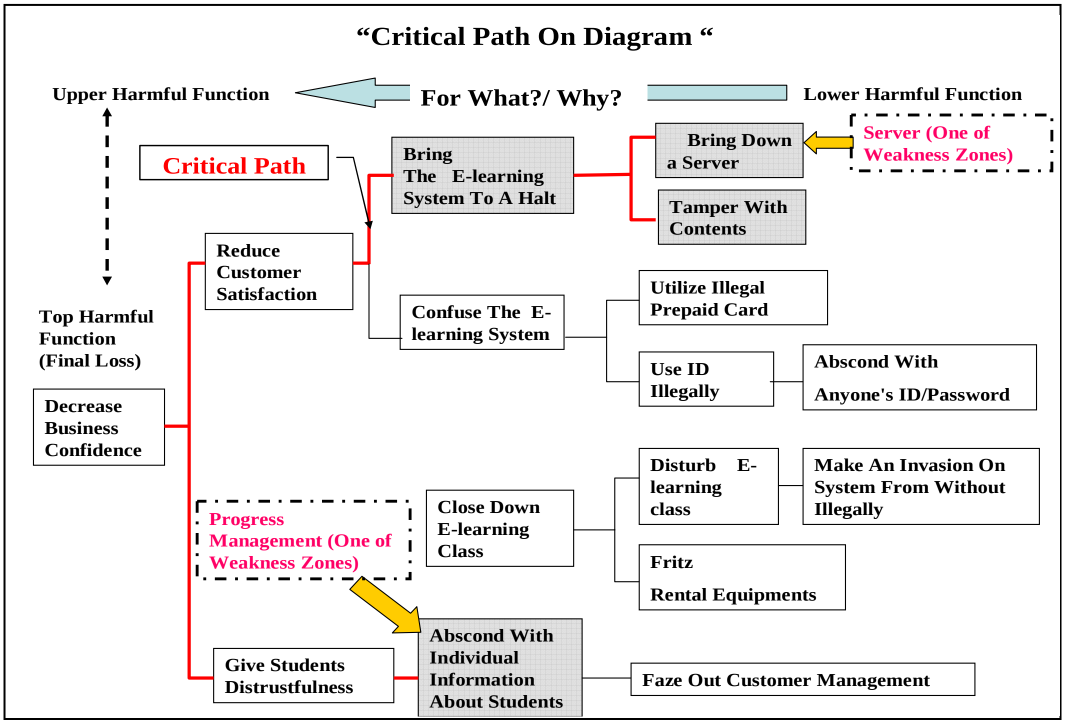

“Critical Path On Diagram “
Upper Harmful Function
For What?/ Why?
Lower Harmful Function
Critical Path
Bring The E-learning System To A Halt
Bring Down a Server
Server (One of Weakness Zones)
Tamper With Contents
Reduce Customer Satisfaction
Utilize Illegal Prepaid Card
Confuse The E-learning System
Top Harmful Function (Final Loss)
Use ID Illegally
Abscond With Anyone's ID/Password
Decrease Business Confidence
Disturb E-learning class
Make An Invasion On System From Without Illegally
Progress Management (One of Weakness Zones)
Close Down E-learning Class
Fritz Rental Equipments
Abscond With Individual Information About Students
Give Students Distrustfulness
Faze Out Customer Management

Fig.8 Critical Path on the Diagram

Idea Generation Based On Harmful Functions Related To Weakness Zones

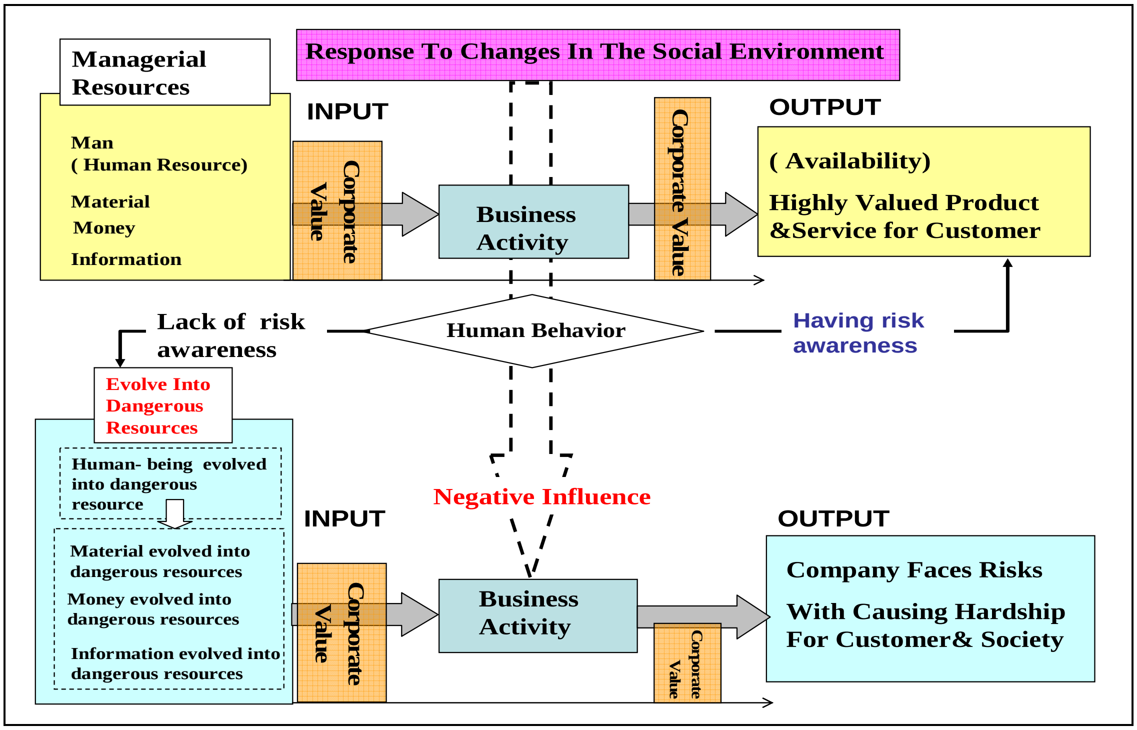
Harmful Functions related to Weakness Zones	Ideas to realize Harmful Functions
Bring Down a Server	1.Cut the power supply 2.Deliver an attack against DOS 3.Trigger a power failure 4.Place fire

Fig.9 Idea Generation based on Harmful Functions

5.6 Step6: Grasping Dangerous Resources for Causing Risks

In order to evaluate the possibility to realize the created ideas through the previous step, we have to grasp “the dangerous resources” to be useful for the outbreak of risks. In addition, managerial resources sometimes fall within the range of dangerous resources, of which “four factors“ (Man, Material, Money, and Information)” must be considered the most dangerous. These four factors are defined as highly-valued resources contributing to the efficiency of business administration under normal conditions. Moreover, one of them, “Man” could evolve into a very dangerous resource more frequently, called “Human Resource”. That’s why human-being become a hot bed of human error.

Fig.10 shows the conceptual process how managerial resources evolve into dangerous resources.



Managerial Resources
Response To Changes In The Social Environment
Man
(Human Resource)
Material
Money
Information
INPUT
Corporate Value
Business Activity
Corporate Value
OUTPUT
(Availability)
Highly Valued Product &Service for Customer
Lack of risk awareness
Human Behavior
Having risk awareness
Evolve Into Dangerous Resources
Human- being evolved into dangerous resource
Material evolved into dangerous resources
Money evolved into dangerous resources
Information evolved into dangerous resources
Negative Influence
INPUT
Corporate Value
Business Activity
Corporate Value
OUTPUT
Company Faces Risks
With Causing Hardship For Customer& Society

Fig.10 Conceptual Process How Managerial Resources Evolve into Dangerous Resources

Organizing the necessity of conditions to realize each idea created at this step, evaluating whether the resources on these conditions exist or not, we finally have to do “a reality check “. Considering the reality of each idea, what needs to be emphasized is what we judge after confirming the mechanism about resources connected to the breakout of risks.

To put it another way, utilizing the logic about AND/OR, we had better practice the relationship analysis focusing on these resources. That is to say, it is clear that the resources based on the OR relationship make implementability of ideas higher.

Fig.11 shows the evaluation table based on “Resource Relationship Analysis” for each created idea as mentioned above. Such ideas should be selected as “materials” to generate “Risk Scenario”.

Harmful Function： Bring Down a Server							
Idea List 1	Necessary Condition For Realization	Dangerous Resources (Relevant Resources To Realize Dangerous Things)	Possibility For An Outbreak Of Dangerous Things				Possibility Of Ideas (Event probability of ideas) Consider Logic about OR&AND
			high	Middle	Low	No	
Cut the power supply	The environment like everyone can operate the server	Breakdown of the key			*		C level (Rejected)
		No presence of the key			*		
		………………	…				
Deliver an attack against DOS	The environment like everyone can break into the network system	Firewall that supports information processing is not sufficient			*		B level (Accepted)
		Forget to update Firewall					
	………	Server system is not designed as robustness system					
Produce an increase in temperature in server room	Temperature more than --℃	Failure of the fan		*			B level (Accepted)
		Design error of the room			*		
		Manager with lack of knowledge		*			
	Humidity more than --%	Design error of the room			*		
		Failure of the air conditioner			*		
Harmful Function：Abscond With Individual Information About Students							
Idea List2 Abscond with data after accessing with spoofing	No regulation bring the important document	………					-------
		………					
Bring data out of company	………	………					-------
		………					
		………					

A level: (possibility of idea) high-middle B level: middle-low C level: low D level: absolutely low

Fig.11 Evaluation table based on “Resource Relationship Analysis” for ideas

5.7 Step7: Organizing Scenarios For Realizing Risks

Fitting together selected ideas (evaluated as A or B level (See Fig.11)) logically without contradictions, we are going to organize selected ideas as a series of “Risk Scenarios” (See Fig.12).

5.8 Step8: Designing Measures to avoid Risk Scenarios

Through this step, seeing about the measures to avoid the implementation of” Risk Scenarios”, we have to evaluate the effectiveness of discussed measures. And then, not having trouble, we have to choose them as highly -valued measures (See Fig.12).

After choosing them, with having risk awareness, we have to practice the measures against Risks. Several “Directions” to think on the proposed measures against Risks are as mentioned below.

Several Directions show “How to **eliminate** Dangerous Resources in Subject Matter”, “To **prevent** Dangerous Resources from acting on Weakness Zone”,” To **reduce** the influence of Dangerous Resources” and “To **isolate** the Dangerous Resources in Subject Matter”

The Scenario To Generate A Risk (1)				
Final Loss	Envisioned Process To Reach The Loss	Existed Dangerous Resources	Proposed Measures	Evaluation
After the invasion from outside to the network, anyone take malicious attack against DOS in PC, and put the resources of the server out of commission , then Accessing for E –learning would be impossible.	Company have caught DOS attack because somebody made mistake of setting of Firewall and forgot update to the latest edition ,moreover security level related to both server and contents were fragile.	a) Server b) Firewall c) Weakness of Security d) Non-educated workers ----------------	1) Review installation of firewall periodically	Accepted
			2) Do the batch treatment to Server periodically	Accepted
			3) Update anti-virus software periodically	Accepted
			4) Redesign education system for maintenance worker through OJT	Accepted
The Scenario To Generate A Risk (2)				
Anybody can access the data of the individual information about each client , and bring them outside. Then finally, --------				

Fig.12 Each Scenario to Generate a series of Risks

6. Conclusion *“Proposed Method (CRMBRT) is a highly-valued tool for Innovation activities.”*

Planning an innovative product is the most important challenge for the industry, as well as the IT field keeping up with the constant changes in technology. But, at the same time, planning an innovative product makes it clear that we have to respond to “Unknown Risks (UR)” we’ve never seen in past inspection activities. Therefore, if we are able to decide how to deal with UR, such activities in itself are just innovative. We can say with fair certainty that “Useful Value” of the proposed method (CRMBRT) increases under such conditions. In other words, this method is expected to facilitate the innovative power focusing on the ability to avoid “Future-Oriented Risks (UR)”.

References

1.Ideation International Inc.,”AFD:Anticipatory Failure Determination ver.2.0(software)”

2.Ideation International Inc.,(2002)”Anticipatory Failure Determination Russian name Subversive Analysis (power point material)”

3. Manabu Sawaguchi, (2005),”The Risk Management Techniques for Information System by Reverse Thinking Functional Analysis”, The 38th Annual National VE Conference Proceedings Vol.36,(in Japanese)

4.Hiroyuki Tada(2004),”A Trend of Risk and Crisis Management in Business Environment”,Japan Industorial Management Assciation Vol.14,No.2.76-80,(in Japanese)