The Detailed Evaluation Criteria for Designation of Critical Information Infrastructure in the field of Broadcasting and Communication

SOONTAI PARK[1], WAN S. YI[1], BONG-NAM NOH[2]
[1]Internet Service Protection Team, [2]System Security Research Center
[1]Korea Internet & Security Agency, [2]Chonnam National University
[1]78 Garak-dong Songpa-gu Seoul 138-950, [2]77 Yongbong-ro Buk-gu Gwangju 500-757
KOREA
[1]cptpark@kisa.or.kr, [1]wsyi@kisa.or.kr, [2]bbong@jnu.ac.kr
[1]http://www.kisa.or.kr, [2]http://www.jnu.ac.kr

Abstract: - Increasing to dependency on information infrastructures involves various threats to cyber incidents. Most of nations or organizations work on protect to not only infrastructure but also information infrastructure. Korea established Critical Information Infrastructure Protection Act in 2001 that include 5 evaluation criteria for designation of National CII. This research makes a suggestion that detailed evaluation criteria for objectification and measuring for designation of CII in the field of broadcasting and Communication. Also this paper shows the result of simulation and application using proposed criteria.

Key-Words: - CII (Critical Information Infrastructure), CIIP (CII Protection), Cyber incident, Cyber Security, Designation Criteria, Information Assets

1 Introduction

CIIP means Activities for protecting critical information infrastructures related to communication, finance, military, energy and so on areas from various cyber attacks.

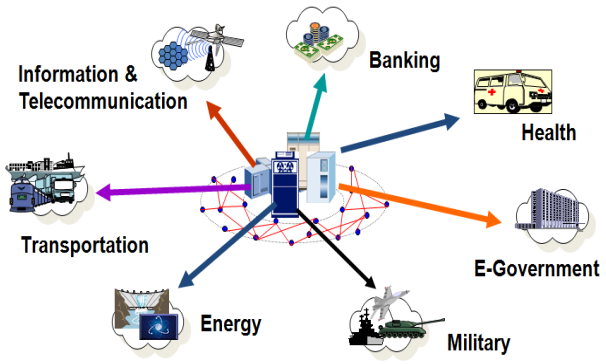

Fig.1 Critical Information Infrastructure in various areas

Each Nations have diversity information infrastructures. The Korean Government enacted a law to protect the major CIIP in January 2001 at the level of national society [1]. This CIIP activities deal with not only Information & Communication Technology sector but also Military, Banking, E-government, Healthcare etc. This research will propose the improved criteria that designation for protecting in many information infrastructures.

2 Related researches

Related researches are composed of Information Asset Profiling, Critical Infrastructure Protection Reliability Standards and CIIP in Korea.

2.1 Information Asset Profiling

The author describes information asset profiling for classifying and assessment of information asset [2]. The first activity is “capture Background Information”. The purpose of this step is to collect information about who is completing the information asset profile and when the profile is being completed. The second activity is “Define the Information Asset”. The purpose of this step is to characterize an information asset. Before any type of analysis activity (e.g., risk assessment) can be performed on an information asset, the organization must understand and agree upon what an information asset contains. The 3rd activity is “Identify the Asset Owner”. The purpose of this activity is to identify and document the owner of the information asset. This activity is important because the owner should work with the individual or group performing the IAP in the remainder of the activities. The 4th activity is “Identify Containers”. The

purpose of this step is to capture a list of all of the containers on which an information asset is stored, transported, or processed and the associated list of the managers of those containers. This step can be done in parallel with Activity 3, as there are no dependencies between the two activities. The 5th activity is "Identify Security Requirements". The purpose of this step is to capture the specific security requirements of the information asset. The 6th activity is "Determine the Information Asset Valuation". The purpose of this step is the risks to an information asset can be assessed, the tangible and intangible value of the asset must be known. Fig.2 shows IAP processes.

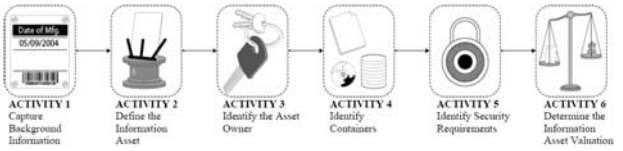

Fig.2 IAP process

2.2 CIP Reliability Standards

US FERC (Federal Energy Regulatory Commission) approved new CIP (Critical Infrastructure Protection) Reliability Standards by NERC (North American Electric Reliability Corporation) for prevention of damage on US electric system against cyber threat in Jan 2008 [3].

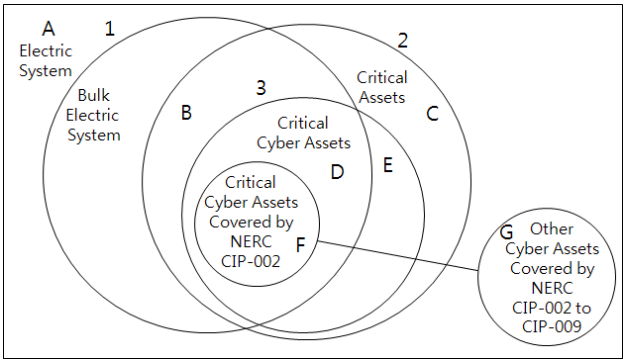

Fig.3 Necessary relationships related to the NERC Cyber Security Standards

Fig.3 shows the Venn diagram that the necessary relationships related to the NERC Cyber Security Standards (CIP-002 through CIP-009) [4]. The purpose of the standard is that NERC Standards CIP-002 through CIP-009 provides a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System [5]. Critical Assets in standards are to be identified through the application of a risk-based assessment such as FIPS PUB 199 [6].

2.3 CIIP in Korea

This paragraph describes CIIP that designation of CII, CII structure and original criteria for designation of CII in Korea.

2.3.1 Designation of CII

Fig.4 shows the Governmental structure of CIIP in Korea. Also Fig.4 shows the pan-national organizational structure for protecting Korea's major IC infrastructures.

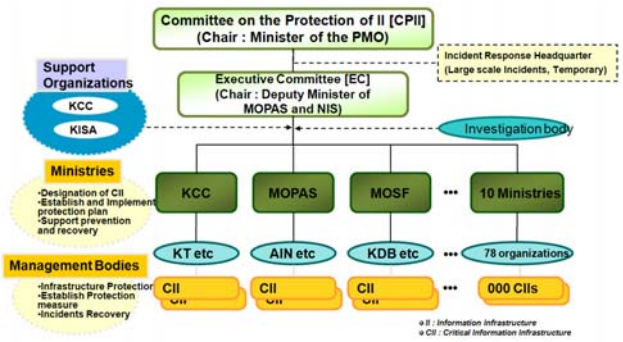

Fig.4 Governmental structure of CIIP in Korea

Looking from the bottom, a number of administration agencies manage the major CIIP. These agencies are mainly communication service providers such as KT, LGDacom, and SKTelecom. Their Internet switch networks belong to the category of major CIIP. The financial area includes the Internet banking system, whereas the energy area includes the electric power communication network of the Korea Electric Power Corporation. Over 100 such facilities are currently designated as major elements of the CIIP. The next-level upper agencies are the government agencies that manage communication, finance, and other areas. These agencies supervise the respective areas, and currently 10 government agencies are related. The next level is the Working Committee for Major CIIP Protection. This organization assists the Major CIIP Protection Committee. The Minister of the Prime Minister's Office is the chairman of this organization. On the right-hand side, you can see the judicial and police organizations. The KCC and the KISA are the support organizations that technical supporting against Cyber incident or Cyber securities. The KISA provides working-level technical support for all these organizations.

Fig.5 shows the procedure and method of designating the major elements of CIIP

Fig.5 Information Infrastructure versus CII

The electronic control and management system, information system, and communication network can be designated as major components of the CIIP. If any infrastructure can affect the country, economy, or society significantly, the government agency in the corresponding area can make public information on the major CIIP based on the review conducted by the Infrastructure Protection Committee. Fig.6 shows 5 phase of designation of CII.

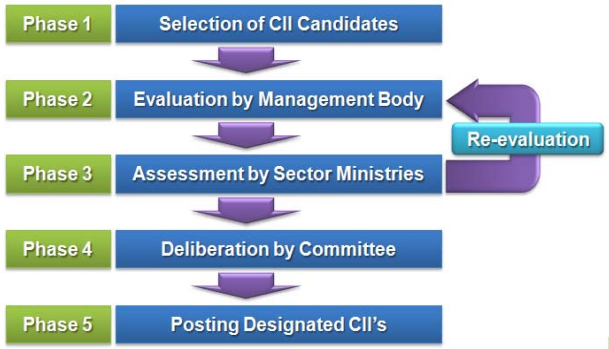

Fig.6 Phase for designation of CII

Self evaluation criteria for designation of CII in the field of communication and broadcasting are composed of 5 domains 10 detailed criteria. Below Table 1 shows detailed criteria and scores.

Table 1 Original designation criteria and score

Designation Criteria category	Score
1. Importance of nation and/or society of Infrastructure	20
2. Dependency for Information Infrastructure's own business	15
3. mutual relation against other information infrastructure	20
4. scale and extent of damage in cyber incident	30
5. possibility of cyber incident or easiness of recovery	15
Total	100

Fig.7 shows the detailed procedure of designating and protecting the major elements of the CIIP.

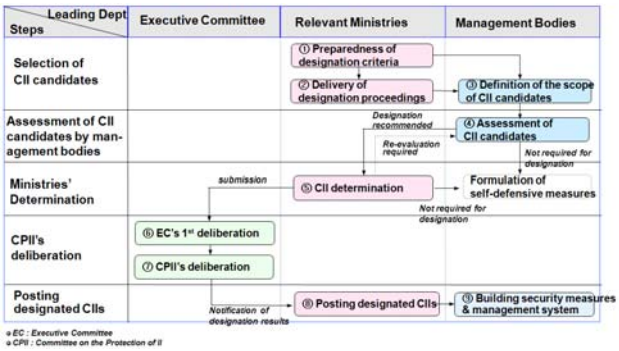

Fig.7 CII Designation flow

2.3.2 Criteria 1 – Importance of nation and/or society of Infrastructure

Table 2 shows Original evaluation criteria 1-A. Criterion 1 means applicable level of public service that needs to national security and/or maintain of social order for its own service of business.

Table 2 Original criteria 1 and score

Evaluation criteria	Score			
Application level - public service in the field of national security, keeping social order, maintenance of stability and/or national life	H	M	L	N/A
	20	16	12	0

2.3.3 Criteria 2 - Dependency for Information Infrastructure's own business

Table 3 shows original evaluation criteria. A criterion 2 is dependency of the providing operation on the IC infrastructure.

Table 3 Original criteria 2 and score

Evaluation criteria	Score			
Business dependency level – Do critical mission using infrastructure and computing system (include rental)	H	M	L	N/A
	15	13	5	0

2.3.4 Criteria 3 - Mutual relation against other information infrastructure

Table 4 shows original evaluation criteria. Criteria 3 concerned interconnection with other infrastructures.

Table 4 Original criteria 3 and score

Evaluation criteria	Score			
3-A	H	M	L	N/A

Relation level – mutual relation against information communication network, computing system in the field of non-government and government	12	10	5	0
3-B	H	M	L	N/A
ripple effect of obstacle of business function	8	6	3	0

2.3.5 Criteria 4 - Scale and extent of damage in cyber incident

Table 5 shows original evaluation criteria. Criteria 4 related size and scope of potential damage to national security, economy and society.

Table 5 Original criteria 4 and score

Evaluation criteria	Score			
4-A	H	M	L	N/A
Capability level - perform business continuously for example substitution in case of incident to target infrastructure	0	3	6	8
4-B	H	M	L	N/A
Level of bring about national crisis - out of public service in case of incident to target infrastructure	15	13	5	0
4-C	H	M	L	N/A
damage level – cause information leakage and modification about confidential, data, technology, privacy etc. when incident to target infrastructure	7	6	4	0

2.3.6 Criteria 5 - Possibility of cyber incident or easiness of recovery

Table 6 shows original evaluation criteria. Criteria 5 related possibility of incident occurrence and the convenience of recovery after considering these five factors, an internal appraisal is carried out in order to simulate the necessity of designation as a major element of information communication infrastructure.

Table 6 Original criteria 5 and score

Evaluation criteria	Score			
5-A	H	M	L	N/A
Possibility of cyber incident against target infrastructure	5	4	1	0
5-B	being		nothing	
Existing of prevention and/or response plan and operate backup system	1		3	
5-C	Over 2 days	within 24 hour	Within 12 hour	within 1 hour
required time for recovery from incident	7	6	4	0

3 Proposed Criteria for Designation of CII

Original criteria for designation of CII have some point of issues those are shortage of objectivity and measuring. So this research make proposal of improved and detailed criteria.

3.1 Summary of detailed Evaluation Criteria

Table 7 shows proposed criteria for that have integrity, objectivity and correctness.

Table 7 Improved detailed designation criteria

Designation Criteria	Detailed Criteria	Score
1. Importance of nation and/or society of Infrastructure	A. Service importance for nation and/or public	10
	B. Importance of information handling	10
2. Dependency for Information Infrastructure's own business	A. Business dependency for infrastructure	10
	B. Dependency for Service Continuity	5
3. mutual relation against other information infrastructure	A. relation of other infrastructure - quantity	5
	B. relation of other infrastructure - quality	5
	C. ripple effect of obstacle of business function	10
4. scale and extent of damage in cyber	A. business continuing capability	10

incident	B. measuring national crisis – regional scope of damage	5
	C. measuring national crisis - sensory scope of damage	5
	D. damage scope of information leakage	10
5. possibility of cyber incident or easiness of recovery	A. possibility of cyber incident	5
	B. required time for recovery	10
Total		100

The criteria that show above Table 7 separated and tailored 13 detailed criteria from 10 detailed criteria for fully evaluation in the scope of 5 designation criteria. Proposed criteria exclude evaluator's subjectivity and get an objectivity of evaluation by embodiment or make a measuring. Also there is improved correctness of evaluation by subdivision of evaluation measure of detailed evaluation criteria.

3.2 Improved Criteria 1

The Criteria means qualitative measure against how much importance reflected nation stability and/or social publicity for information that infrastructures deal and process. Sub evaluation contents include service importance for nation and public and importance level of handled information. Allocated score is totally 20.

3.2.1 Service importance for nation and public

This criterion has total 10 score which zero through 10. The contents shall using independently or combination of criteria.

Table 8 Improved criteria 1-A and Score

criteria	Evaluation contents & measure	
Service importance for nation and public	Business Area	Business Importance Level
		VH(10), H(8), SH(6), M(4), L(2), N/A(0)
	Connection - Broadcasting & Communication	
	Exchange - Broadcasting & Communication	
	Service - Broadcasting & Communication	
	Infrastructures - Broadcasting & Communication	

If business areas are more than 2, final evaluation result calculated the average of sum of each fields. For example, Connection – broadcasting & communication means internet service, Exchange - broadcasting & communication means IX (Internet exchange), Service - broadcasting & communication means VoIP (Voice over Internet Prococol) and Infrastructures - broadcasting & Communication means IDC (Integrated Data Center).

3.2.2 Importance of Information Handling

This criterion has total 10 score which zero through 10. Require level means N/A (Not Applicable), Low, Medium, Some High, High, and Very High. The contents shall using independently or combination of criteria.

Table 9 Improved criteria 1-B and Score

criteria	Evaluation contents & measure	
Importance of information handling	Security Requirement of Information	Required Level
		VH(10), H(8), SH(6), M(4), L(2), N/A(0)
	Confidentiality	
	Integrity (or Correctness)	
	Availability	
	In time	

If security requirements of information are more than 2, final evaluation result calculated the average of sum of each fields. For example, social security numbers used by communication service provider requires confidentialities, information stored in server requires availabilities, network management information requires operated in time.

3.3 Improved criteria 2

The Criteria – business dependency means qualitative measure against how much dependent for infrastructure which controlled under management body to business. Sub evaluation contents include

business dependency for infrastructure and service continuity dependency. Allocated score is totally 15. Criteria 2-A means dependency for infrastructure and 2-B means dependency for continuity of service.

3.3.1 Business dependency for infrastructure

This criterion has total 10 score which zero through 10. For example DNS (Domain Name System) failure means impossible because there are no alternative means.

Table 10 Improved criteria 2-A and Score

criteria	Evaluation contents & measure	
Business dependency for infrastructure	Dependency Level	Density concerned Business
	Impossible - Broadcasting & Communication	Very High(10, 9)
	Obstacle - Broadcasting & Communication	High(8, 7)
	Business Delay - Broadcasting & Communication	Some High(6, 5)
	Business Quality Down - Broadcasting & Communication	Medium(4), Low(3)
	Not Concern - Broadcasting & Communication	N/A(0)

In case of complex degree, we make an application of high rank dependency. For example, DNS server broke down means Impossible - Broadcasting & Communication because there is no alternative measure. In case of there is a alternative mean such as off-line operation by remote control, it means Oobstacles - Broadcasting & Communication. Related system fault has a probability of business Delay - Broadcasting & Communication. Business quality down - Broadcasting & Communication means performance down of switch.

3.3.2 Dependency for Service Continuity

This criterion has total 5 score which zero through 5. If there are very complex dependencies, apply above dependency concept.

Table 11 Improved criteria 2-B and Score

criteria	Evaluation contents & measure	
Dependency for service continuity	Business Continuity Level	Required Level
	Real time	Very High(5,4)
	Non Real time	High(4,3)
	Allowed Short term interruption	Some High(3)
	Allowed middle term interruption	Medium(2)
	Allowed long term interruption	Low(1)
	Allowed interruption	N/A(0)

In case of complex degree, we make an application of high rank continuity. Internet connection service requires real time. Network management system requires non-real time. Web server or mail systems allow short terms interruption. If you have a traffic analysis system, maybe it will allow long terms interruption.

3.4 Improved criteria 3

The Criteria – mutual relation with other infrastructure adopted using not only its own infrastructure but also other organization's infrastructure. Allocated score is totally 20. It concerned with related quantity, related quality and ripple effect of functional break down.

3.4.1 Relation of other infrastructure - quantity

This criterion has total 5 score which zero through 5. The high score is 5, medium score is 3 and low score is zero.

Table 12 Improved criteria 3-A and Score

criteria	Evaluation contents & measure	
Relation of other infrastructure - quantity	Quantity of Relation	Degree of Relation
	Relation strength – Medium	High(5)
	Relation strength - weakness	Medium(3)
	Independence Business	N/A(0)

A matter under consideration is that if infrastructure's related quantity is complex, you may apply high rank related quantity. Certification authority system is considered relation strength – medium and Internet access network is considered relation strength - weakness. If there is no related other system, it is considered independence business.

3.4.2 Relation of other infrastructure - quality

This criterion has total 5 score which zero through 5. The score is that very high 5, high 4, medium 3, low 2. If the business is independence, the score is zero.

Table 13 Improved criteria 3-B and Score

criteria	Evaluation contents & measure	
Relation of other infrastructure - quality	Related type	Related quality
	Related – other infrastructures	Very High(5)
	Related – core service	High(4)
	Related – other services	Medium(3)
	Related – just linked	Low (2)
	Independence business	N/A(0)

For example Internet exchange system is considered related – other infrastructures and certification authority system is considered related – core service. The system for back up is considered related – other services in accordance with it's a specific character and mail service is considered related – just linked.

3.4.3 Ripple effect when obstacle of infrastructure

This criterion has total 10 scores which 10 to zero. The detailed criteria for designation is ripple effect to other infrastructures when obstacle of own infrastructure.

Table 14 Improved criteria 3-C and Score

criteria	Evaluation contents & measure	
Ripple effect when obstacle of infrastructure	Effect to other infrastructure	Ripple speed
	Effect - Full business	Very Fast(10), Fast(9), Medium(8), Slow(7), Very Slow(6)
	Effect - Core business	Very Fast(9), Fast(8), Medium(7), Slow(6), Very Slow(5)
	Effect – the others	Very Fast(8), Fast(7), Medium(6), Slow(5), Very Slow(4)
	Unrelated	N/A(0)

The consideration is that if the effected level is various, we may apply high rank effected level. DNS service is considered effect – full business and voice over internet protocol is considered effect – core business. Integrated security management and control system is considered effect – the others.

3.5 Improved criteria 4

The next criteria is Criteria – Scale and Extent of Damage in cyber incident. It includes business continuing capability, measuring national crisis – regional scope of damage, measuring national crisis - sensory scope of damage and Damage scope of information leakage. Allocated score is totally 30.

3.5.1 Business continuing capability

This criterion has total 10 score which zero through 10. Damage score is conclude very high the score is 10, high the score is 9, some high the score is 8, medium the score is 7, low the score is 5 and N/A the score is zero.

Table 15 Improved criteria 4-A and Score

criteria	Evaluation contents & measure	
Business continuing capability	Business effect	Damage
	Loss – Full business	Very High(10)
	Loss – core business	High(9)
	Delay – core business	Some High(8)
	Loss - supporting biz	Medium(7)
	Delay – supporting biz	Low(5)
	Non Applicable	N/A(0)

The criteria classified 6 levels of business effect. A matter under consideration is that if infrastructure has variety of business effect, we shall apply high rank business effect. The damage of wireless internet access network shall cause loss – full business. The break down of certification authority system is considered loss – core business and fault of inter internet access network cause delay – core business. The damage of Voice over IP user management system means loss – supporting business. If web service damaged by cyber incident, it is considered delay – supporting business.

3.5.2 Measuring national crisis – regional scope of damage

This criterion has total 5 score which zero through 5. Damage score is conclude very high the score is 5, high the score is 4, medium the score is 3, restricted the score is 2 and N/A the score is zero.

Table 16 Improved criteria 4-B and Score

criteria	Evaluation contents & measure	
Measuring	Extent of damage	Damage

national crisis – regional scope of damage	International	Very High(5)
	National	Very High(5)
	Administrative district	High(4)
	Organization, Enterprise	Medium(3)
	Relevant system	Restricted(2)
	Non Applicable	N/A(0)

The criteria classified 6 levels of extent of damage. A matter under consideration is that if infrastructure has variety of regional scope of damage, we shall apply regional scope of damage of a high rank concept. The damage of voice over IP is considered international. Local Internet exchange system is considered administrative district damage. If an enterprise has an own group ware system, it is considered organization and/or enterprise. If Organization's own mail server broke down, the damage is restricted in relevant system.

3.5.3 Measuring national crisis - sensory scope of damage

This criterion has total 5 score which zero through 5. Damage score is conclude very high the score is 5, high the score is 4, medium the score is 3 and N/A the score is zero.

Table 17 Improved criteria 4-C and Score

criteria	Evaluation contents & measure	
Measuring national crisis – sensory scope of damage	Sensory damage	Domain
	Out of normal life	Very High(5)
	Make disorder	High(4)
	Inconvenience	Medium(3)
	Normal life	N/A(0)

The criteria classified 4 levels of sensory damage. A matter under consideration is that if infrastructure has a variety of scope of damage, we shall apply a scope of damage of a high rank concept. For example, a damage of DNS cause out of normal life. We have experienced in Internet stoppage at 25 Jan 2003 by SQL slammer worm. Damage of certification authority is considered make disorder and damage of voice over IP is considered inconvenience.

3.5.4 Damage scope of information leakage

This criterion has total 10 score which zero through 10. Damage levels are concludes 4 levels. Each damage level have 3 damage scores all, unspecific majority, and minority. If there is no information, the damage score is zero.

Table 18 Improved criteria 4-D and Score

criteria	Evaluation contents & measure	
Damage scope of information leakage	Damage Level	Damage
	Nation and/or Society	All(10), Unspecific majority (9), Minority(8)
	Region	All(8), Unspecific majority (7), Minority(6)
	Organization, Enterprise	All(6), Unspecific majority (5), minority(4)
	No information	N/A(0)

In case of complex degree, we make an application of high rank damage level. For example, the information leakages of certification authority exert influence on unspecific majority nation and/or society. The information leakages of information in government service network shall exert influence on region. The information leakages of information in mail server of enterprise are a bad influence to its own enterprise itself.

3.6 Improved criteria 5

The next criteria are possibility of cyber incident or easiness of recovery. It includes possibility of cyber incident and required time for recovery. Allocated score is totally 15.

3.6.1 Possibility of cyber incident

This criterion has total 5 score which zero through 5. Service type levels are concludes 4 levels. Each level of connection type is internet, secure, closed and off-line. Possibility of cyber incident type has 3 service type – public, restricted area and restricted.

Table 19 Improved criteria 5-A and Score

criteria	Evaluation contents & measure	
Possibility of cyber incident	Service type	Connection type
	public	Internet(5), secure(4), closed(3), off-line(2)
	restricted area	Internet(4), secure(3), closed(2), off-line(1)
	restricted	Internet(3), secure(2), closed(1), off-line(1)

A matter under consideration is that if the type of user service is complex, we shall use service of high

rank. The evaluation contents and measures are concluded relation of service type versus connection type. If service type is public, the score has 5 through 2. An otherwise the allocated score has 3 through 1 in case of restricted service type. Service of Internet access is considered as a public service in the field of broadcasting and communication. If the service type is restricted area, the example is integrated security management and control system.

3.6.2 Required time for recovery

This criterion has total 10 score which zero through 10. Recovery type levels are concludes 4 levels. Each level of recovery type is full system, core service, supporting service and unnecessary. Required level according to real time recovery is itemized very high, high, medium, low, very low and unnecessary.

Table 20 Improved criteria 5-B and Score

criteria	Evaluation contents & measure	
Required time for recovery	Recovery type	Required level – real time recovery
	Full system	VH(10), H(9), M(8), L(7), VL(6)
	Core service	VH(9), H(8), M(7), L(6), VL(5)
	Supporting service	VH(8), H(7), M(6), L(5), VL(4)
	Unnecessary	N(0)

A matter under consideration is that if the type of recovery is complex, we shall apply recovery type of high rank concept. The evaluation contents and measures are concluded relation of recovery type versus required level of real time recovery. In case of internet exchange, it requires recovery type of full systems and its degree of requiring real time recovery is very high.

3.7 Summary of Proposed Criteria

We explained original criteria and improved criteria. Table 21 shows the summary of formerly criteria and proposed criteria. The * mark means added sub criteria and + mark means tailored sub criteria.

Table 20 Comparison of Original criteria versus improved criteria

Criteria for designation	Designation details criteria			
	Original	score	Improved	score
Importance of nation and/or society of	Importance of nation and/or society of	20	Service importance for nation and	10
Infrastructure	Infrastructure		public	
			Importance of information handling*	10
Dependency for Information Infrastructure's own business	Dependency for Information Infrastructure's own business	15	Business dependency for infrastructure	10
			Dependency for service continuity*	5
mutual relation against other information infrastructure	relation of other infrastructure	12	Relation of other infrastructure - quantity	5
			Relation of other infrastructure – quality*	5
	ripple effect of obstacle of business function	8	Ripple effect when obstacle of infrastructure *	10
scale and extent of damage in cyber incident	capability level to perform business	8	Business continuing capability+	10
	Level of bring about national crisis	15	Measuring national crisis –regional scope of damage	5
			Measuring national crisis - sensory scope of damage*	5
	damage level - information leakage or change	7	Damage scope of information leakage*	10
possibility of cyber incident or easiness of recovery	possibility of cyber incident	5	Possibility of cyber incident+	5
	existing of prevention and/or response plan	3	Required time for recovery+	10
	required time for recovery	7		
Total Score		100		100

4 Simulation & Application Result

This chapter shows simulation result using proposed criteria and its application result.

4.1 Simulation Result

We simulated using proposed criteria for apply of new criteria and validation of the point at issue and its effectiveness. Selected organizations are ISP (internet service provider) A and VoIP (Voice over Internet Protocol) service provider B. Table 21 shows the simulation result using proposed criteria for designation of CII.

Table 21 simulation result

Criteria for designation		score			
		Allocation	A	B-1	B-2
Importance of nation and/or society of Infrastructure	Service importance for nation and public	10	9	4	4
	Importance of information handling	10	9.5	6	9
Dependency for Information Infrastructure's own business	Business dependency for infrastructure	10	9	8	6
	Dependency for service continuity	5	4	5	5
mutual relation against other information infrastructure	Relation of other infrastructure - quantity	5	5	5	5
	Relation of other infrastructure - quality	5	5	3	4
	Ripple effect when obstacle of infrastructure	10	10	7	8
scale and extent of damage in cyber incident	Business continuing capability	10	9	8	8
	Measuring national crisis –regional scope of damage	5	5	3	5
	Measuring national crisis - sensory scope of damage	5	4	3	3
	Damage scope of information leakage	10	9	5	7
possibility of cyber incident or easiness of recovery	Possibility of cyber incident	5	5	3	4
	Required time for recovery	10	10	8	10
Total Score		100	93.5	68	78

Fig.8 shows the graph of simulation result. In case of company A has high score because of business character that support Internet exchange or Internet connection. In case of company B has middle score because of VoIP service of low user of a member.

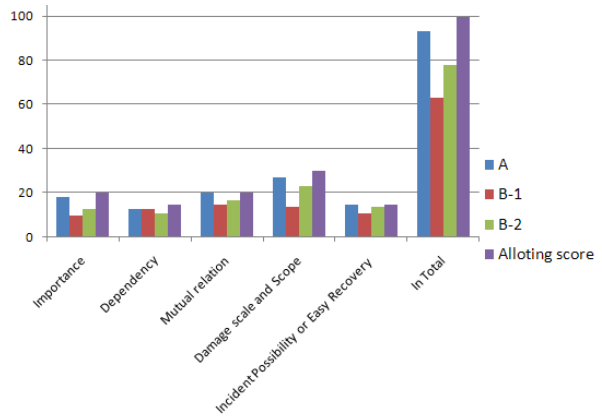

Fig.8 Simulation result using new criteria

4.2 Application Result

We made an application of proposed designation criteria to IPTV service. The target is IPTV service operated by 3 IPTV service providers A, B, C companies in Korea. The result score were over 80 points at each company. So we understand IPTV service is very important and have to manage under CIIP framework.

5 Conclusion

This research made a suggestion that detailed evaluation criteria for objectification and measuring for designation of CII in the field of information communication and broadcasting. If you adopt the new criteria for designation of CII, you shall improved manage CII effectively.

References:

[1] The National Assembly of Korea, *Information Infrastructure Protection Act*, the national assembly of Korea, 2008.

[2] James F. Stevens, CMU/SEI-2005-TN-021, *Information Asset Profiling*, Networked Systems Survivability Program, June 2005.

[3] FERC, CIP *Reliability Standards*, http://www.ferc.gov/industries/electric/indus-act/reliability/cip.asp

[4] NERC, FAQ Cyber Security Standard CIP-002-1, http://www.nerc.com/page.php?cid-2|20

[5] NERC, *reliability Standards for the Bulk Electric Systems of North America*, NERC, Sep 2009.

[6] NIST, FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, NIST, Feb 2004.
[7] SOONTAI PARK, WAN S. YI, The Evaluation Criteria for Designation of Critical Information Infrastructure, *Proceeding of the 8th WSEAS International Conference on E-ACTIVITIES (E-ACTIVITIES '09) and 8th WSEAS International Conference on INFORMATION SECURITY and PRIVACY (ISP '09)*, pp. 77-83, Dec 2009.