ISP(Internet Service Provider)의 네트워크 보안 위험을 고려한 예상 자산손실 모델링

문호건*, 이종필*

* KT 기술연구소 차세대기술연구팀 인터넷보안연구실

Expected Asset Loss Estimation Considering Security Risks of ISPs' Networks

Ho Kun Moon*, Jong Pil Lee*

* Internet Security Division, Next Generation Technology Team, KT Technology Laboratory

요 약

본 논문에서는 Internet Service Provider(이하 ISP)의 네트워크에 위험이 발생할 경우 위험의 출현으로 인한 ISP의 자산손실을 추정하는 방법을 제안한다. ISP의 네트워크를 구성하는 자산들의 가치를 서비스 측면에서 분석하고, 개별 자산이 생산하는 서비스 가치를 근사할 수 있는 방법론을 제시함으로써 네트워크의 장애로 인한 손실액을 추정 가능함을 보인다. 또한, 네트워크의 부하 분산, 우회 경로 및 백업 시스템 등 서비스 연속성을 확보를 위한 잉여 설계가 있을 경우, 자산가치 특성함수를 사용한 손실액 추정 모델을 제안한다.

I. 서론

1. 자산 피해 모델링의 필요성

1) 네트워크 위험 증가 추세

2001년 이후에 네트워크 침해 사고는 기하급수적으로 증가하고 있으며 CERT의 보안 경보, 취약성 리포트, 그리고 Hotline 전화와 관련된 일련의 모든 통계는 유사한 트렌드를 보여준다. 이러한 지속적인 침해사고 및 취약성의 증가는 전 세계에 존재하는 모든 IP 및 non-IP 기반의 네트워크를 운영하는 ISP 및 개인 PC 사용자들에게 실질적인 위험을 끊임없이 유발하고 있다. 실제로 국내에서는 2003년 1월 25일 인터넷 대란이 발생하여 전국적인 통신 중단 사태가 발생했으며 KT를 포함한 대규모 ISP 업체들의 인터넷 서비스가 중단되는 초유의 네트워크 보안 위험이 발생하기도 하였다.[1]

ISP 네트워크와 정보자산이 사이버 공격 등 장애유발 요인으로 인해 정상적인 서비스 제공이 불가능해지면, ISP 네트워크의 복구비용 뿐만 아니라 네트워크를 통한 정보유통 의존도가 높은 기업과 개인에 커다란 손실이 발생할 수 있다. 예를 들어 전용회선 서비스의 경우, 네트워크의 일부 또는 전체에 장애가 발생하면 고객과의 계약에 의해 서비스 장애시간 동안의 요금을 변제하거나 심지어 손해배상을 해야 하는 상황도 발생한다[2]. 따라서, 보안사고가 발생시 ISP가 감당해야 할 사업적 위험도 함께 커지고 있다.

2) 기존의 자산 가치 평가 방법들

이러한 네트워크 보안 위험 및 정전, 낙뢰 등의 자연재해, 그리고 장비 자체의 고장 등으로 인한 자산 손실 규모를 산정하기 위하여 기존에는 네트워크를 구성하는 하드웨어의 자산가치 수준을 미리 산정한 후 침해 사고로 인한 자산의 손실이 발생할 경우 해당 기관의 자산 가치를 기준으로 손실액을 산정해 왔다. 통상 이러한 방식들은 표 1과 같은 기준 등에 의해 자산을 보유한 기관의 자산규모 및 매출 규모에 따라서 5단계 내지 10단계 등급을 정하여 자산가치를 평가하는 것이 일반적이다.

표 1: 종래의 자산가치 산정기준.

측정스케일	등급화 기준
1(매우낮음)	금전적 손실이 적거나 없는 수준의 금액 (조직 자산의 5% 이내)
2(낮음)	최소한의 금전적손실을 야기하는 수준의 금액 (조직 자산 규모의 10% 이내)
3(중간)	보통의 금전적손실을 야기하고 비즈니스 프로세스에 부정적인 영향을 미치는 수준의 금액 (조직 자산 규모의 20% 이내)
4(높음)	심각한 손실을야기하고 비즈니스 프로세스가 실패가 되는 수준의 금액 (조직 자산 규모의 20% 이내)
5(매우높음)	개별 또는 조직에 막대한 손실을 입히는 수준의 금액 (조직 자산 규모의 50% 이내)

이상과 같이 기존에는 특정 자산 가치를 해당 자산이 장애 또는 운영 중단 시에 소속한 기관이 어느 정도 금전적 피해를 입는가를 대략 유추하여 자산에 대한 가치 수준을 부여한다.

보안사고로 인한 자산 손실액을 산정하는 기존의 방법으로는 복구비용과 영업기회 손실을 1차 손실액으로 하고, 손해보상 또는 예상 이미지 손실을 2차 손실액으로 산정하는 형태가 일반적이다[3]. 그러나, 대규모 네트워크 인프라를 운용하는 ISP의 입장에서 보안사고 발생시 유, 무형 자산손실을 구분하여 산정하는 기존의 방식은 다음과 같은 문제점들이 있다.[4][5]

표 2: 기존 자산가치 산정기준의 문제점

번호	문 제 점
1	가치 수준을 부여하는 사람의 잘못된 판단에 영향받을 가능성이 있음
2	등급으로 정의된 자산가치 수준을 실질적인 금전피해 규모로 수치화하기 어려움
3	등급의 세분화 정도에 따른 자산가치 수준의 정밀도 차이가 발생함
4	자산이 위치한 네트워크 상의 토폴로지(Topology)에 따른 자산의 중요도를 산출하기 어려움
5	잉여 설계(로드 밸런싱, 백업 등)으로 네트워크가 설계되어 특정 자산이 침해 되더라도 정상적인 네트워크 서비스가 가능한 상황에 대한 고려가 불가능
6	고정자산가치만 산정 가능하고 자산이 생산하는 서비스 가치의 정량화와 서비스 가치의 변화량이 존재할 경우에 대한 설명이 어려움

3) 새로운 평가 모델의 필요성

일반적으로 자산이라 함은 조직에 가치를 갖는 모든 것으로 정의하고 그 분류 방법도 다양하게 제시되고 있다.[5][6][7] 기존의 방법들은 다양한 자산들의 가치수준을 몇 개의 등급으로 구분하면서 발생하는 정밀도의 차이와 평가자의 주관에 크게 의존하는 단점이 있어서 ISP와 같은 대규모 네트워크의 자산에 적용하기에는 어려움이 있다.

표 3: 서비스가치를 고려한 자산평가 모델의 요구 조건

번호	자산평가 모델의 요구 조건
1	자산가치 수준 산정이 정량적이어야 함.
2	자산가치의 단순한 등급화가 아닌 자산이 위치한 네트워크상의 토폴로지와 자산의 중요도, 잉여설계된 자산들의 가치를 산출 가능해야 함.
3	자산이 가진 고정자산가치와 서비스가치를 모두 고려해야 함
4	동일한 서비스를 제공하는 복수개의 자산에 대한 평가가 가능해야 함.

본 논문에서는 네트워크 침해 사고 발생시의 손실액 추정방법으로 네트워크에서의 자산의 역할과 구성형태를 고려하여 자산가치를 고정자산가치와 서비스가치로 구분하고 서비스가치의 산정에 있어 표 3의 요구조건을 만족하고 평가자의 주관적 요인을 최소화 할 수 있는 새로운 평가 모델을 제안한다.

II. 본문

1. 서비스 가치를 고려한 자산 손실액 추정 모델

1) 개념화된 네트워크 모델

ISP의 네트워크는 설계 목적 및 네트워크를 구성하는 자산의 형태에 따라서 상이한 구조를 가지고 있지만 일반적으로 다음과 같은 계층적인 형태로 단순화가 가능하다.

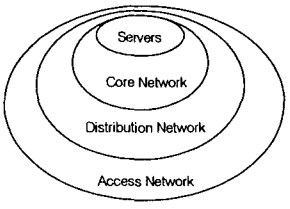

그림 1: 개념적인 네트워크 계층구조

네트워크의 물리적 자산들은 그림 1의 각 계층 요소를 구성하며, 네트워크의 속성상 상위 계층의 자산들이 하위계층의 자산들보다 많은 서비스가치를 생산한다. 따라서, 동일한 기능을 제공하는 자산일지라도 네트워크 상의 계층, 역할 및 구성형태에 따라 침해사고의 발생시 네트워크에 미치는 영향의 범위가 달라진다.

2) 기본 자산 모델

그림 1과 같은 형태로 계층 구조를 갖는 ISP의 서비스 네트워크를 구성하는 자산의 가치는 다음과 같이 모델화 할 수 있다. n 개의 자산으로 구성된 네트워크의 자산들의 집합을 A라고 할 경우

$$A = \{a_1, a_2, a_3, ..., a_n\} \quad (1)$$

A에 속하는 모든 개별 자산 a_k는 다음과 같은 속성을 갖는다.

(가) 자산은 구매시점으로부터 현재까지의 감가상각이 반영된 고정자산가치를 갖는다.

(나) 모든 자산은 ISP의 서비스 가입자에게 제공되는 1개 이상의 서비스 가치를 생산하는데 사용된다.

특정 자산 a_k가 구매시점을 기준으로 x년에 갖는 고정자산가치를 $Vf(a_k, x)$, 그 년도에 생산해내는 서비스가치를 $Vs(a_k, x)$ 라고 하면 해당 연도에 a_k의 총 가치 $Vt(a_k, x)$는 고정자산가치와 서비스가치의 합으로 계산할 수 있다.

$$Vt(a_k, x) = Vf(a_k, x) + Vs(a_k, x) \quad (2)$$

이때 $Vf(a_k, x)$는 고정자산 계정에 대한 회계규정 중 감가상각 방식에 의해서 자산가치가 정해지므로 정액법, 생산량비례법, 정률법, 이중 체감법 등의 방식 중 한가지 방식으로 가치를 계산할 수 있으며 ISP별로 정해진 내부 회계규칙을 적용하면 된다. 그 중 정액법을 적용할 경우

$$Vf(a_k, x) = -\frac{(Vf(a_k, 0) - Vfr)}{n} x + Vf(a_k, 0) \quad (3)$$

단,

x : 경과 연도, $x > 0$ 인 정수

n : 잔존 연도

$Vf(a_k, 0)$: 자산 구매 시점의 자산 가치

Vfr: 잔존가치

로 표시할 수 있다. 즉, $Vf(a_k, x)$는 해가 거듭될 수록 가치가 일정하게 감소하여 통상 회계기준인 5년이 지나면 가치가 0 또는 잔존가치로 수렴하는 특징이 있다.

어떤 ISP가 한 해에 개별 자산 a_k를 통해 m개의 서비스를 고객에게 제공하고, a_k가 특정 서비스에서 만들어내는 서비스가치를 $Vpsw(a_k, x)$라고 하면 a_k를 통해 생성되는 전체서비스가치 즉, ISP가 a_k로부터 얻는 서비스 제공 수입은 수식 (4)와 같이 나타낼 수 있다.

$$Vs(a_k, x) = \sum_{n=1}^{m} V_{psw_n}(a_k.x) \quad (4)$$

만일, 특정한 자산의 서비스가치가 고정자산가치와 $Vs > 10Vf$ 의 관계가 있다면 서비스가치가 자산의 전체가치의 주된 요소이므로 $Vt \cong Vs$ 로 근사화할 수 있다.

3) 자산별 서비스가치 추정 방법

수식 (4)에서 언급한 $V_{psw}(a_k, x)$를 실제의 ISP 네트워크에서 측정하기는 매우 어렵다. 그 이유는 자산이 개별 서비스를 생산하는데 기여하는 정도는 시간에 따라 변화하고. 각 자산이 처리하는 트래픽 중 특정 서비스와 관련된 트래픽을 구분하는 것이 거의 불가능하기 때문이다.

예를 들어 특정 ISP가 2개의 서비스 S_1(500억의 서비스가치가 있음), S_2(1,000억의 서비스 가치)를 특정 라우터를 이용해서 고객들에게 제공하고 있고 한 해에 해당 라우터가 S_1, S_2에 대해 각각 100억, 50억의 서비스 매출을 올리는데 기여했다고 가정할 경우 라우터 자산이 생산해 낸 서비스가치 $Vs(Router)$ = 100억 + 50 억 = 150억이 된다. 이때, 자산(라우터)이 각각의 서비스 생산에 얼마만큼의 기여를 한 것인지를 정확하게 파악하기란 쉽지가 않다. 네트워크의 특성상 서비스 전달 경로의 변화, 부하분산 장치의 동작, 백업 시스템의 존재 등에 의해서 이러한 기여도에 변화가 생기기 때문이다.

그래서 본 논문에서는 개별 자산이 생산해 내는 서비스가치 $V_s(a_k, x)$를 추정하는 방식을 사용한다. 이를 위해 개별 자산의 유기적 결합체인 네트워크의 특성을 반영하여, 서비스 측면에서 자산이 생산해낸 가치를 바탕으로 개별 자산이 생산하는 서비스가치를 역으로 추정하는 접근법을 사용하기로 한다. 이러한 접근법이 가능한 이유는 계층화된 네트워크의 다음과 같은 속성들 - 즉,

(1) 모든 서비스 이용자는 반드시 Access 네트워크의 자산을 이용한다.

(2) 네트워크의 계층구조로 인해 상위계층 서비스의 가치가 하위계층보다 크거나 같다.

을 가지고 있고, 잉여설계가 되어있지 않을 경우, 1년간 특정한 서비스에 대한 동일 계층의 네트워크 자산들의 기여도는 거의 균등하다고 가정할 수 있기 때문이다.

다음과 같은 예를 살펴보자. 예를 들어 어떤 ISP에서 서비스 #0, 서비스 #1, 서비스 #2의 총 3개의 서비스를 제공하고 있다고 하고 일년에 해당 서비스로 벌어 들이는 서비스 매출이 각각 400억, 200억, 그리고 100억이라고 해 보자. 그리고 서비스 #0를 제공하기 위해서는 $a[0]$, $a[1]$, $a[2]$, $a[3]$, $a[4]$ 의 5 개의 서버계층 자산이 사용되고 있다고 가정하면

표 4: 서비스가치 산출예제

서비스명	서비스가치 (단위 억)	관련 자산 #1	관련 자산 #2	관련 자산 #3	관련 자산 #4
서비스 0	400	a[0]	a[1]	a[2]	a[3]
서비스 1	200	a[1]	a[2]	a[3]	a[4]
서비스 2	100	a[2]	a[4]		

단,

$a[i]$: 서버계층의 i 번째 자산

$Vf[i]$: $a[i]$자산의 고정자산가치

$Vs[i]$: $a[i]$자산의 서비스가치

$prio[a_k]$: 동일 계층 내에서의 타 자산과 비교한 $a[i]$의 중요도

자산들의 고정자산가치는 생략

이때 랜덤한 접속 및 서비스 사용의 특성 때문에 1년간 특정한 서비스에 대한 동일 계층의 자산들의 기여도가 균등하다고 가정하면

$a[0]$의 서비스가치 $V_s[0]$ = 400/4 = 100,

$a[1]$의 서비스가치 $V_s[1]$ = 150

$a[2]$의 서비스가치 $V_s[2]$ = 200

$a[3]$의 서비스가치 $V_s[3]$ = 150,

$a[4]$의 서비스가치 $V_s[4]$ = 200/4+100/2 = 100

따라서 각 자산들의 서비스 가치는

$$V_s[2] > V_s[1] = V_s[3] > V_s[0] = V_s[4] \quad (5)$$

가 되고 자산의 동일 계층 내에서의 서비스 가치를 기준으로 한 중요도는 $prio[a_2]$=1 순위, $prio[a_1]$=$prio[a_3]$=2 순위, $prio[a_0]$=$prio[a_4]$=4 순위가 된다.

이 방식으로 특정한 자산이 복수개의 서비스 가치를 생산해 낼 때 동일 계층내의 특정 자산이 연간 생산하는 개별 서비스가치를 추정할 수 있으며 자산의 고정자산가치와 서비스가치를 더한 총자산가치를 구한 후 해당 자산의 동일 네트워크 계층 자산간의 상대적 중요도를 산정할 수 있다. 이런 연산 방식은 모든 네트워크 계층에 대해서 공통적으로 적용 가능하며, 이상의 방식을 적용하여 네트워크의 보안 위험이 발생했을 때 침해를 입은 개별 자산들의 손실액을 총자산가치를 기준으로 추정할 수 있다. 특정 연도의 개별 자산의 총자산가치는 표 5와 같이 일반화가 가능하다.

표 5: 개별자산의 총자산가치 연산방법

(Step 1) ISP가 제공하는 전체 서비스의 개수(m)와 개별 서비스의 가치($S_v[i]$)를 파악한다.
(Step 2) 개별 서비스의 가치 $Sv[i]$ 생산에 몇 개의 자산이 기여하는지를 확인하여 서비스별 자산개수인 $N[Sv[i]]$를 m개의 서비스에 대해서 구한다. 단, 계층별로 연산한다.
(Step 3) $Vs(a_k,x) = \sum_{i=1}^{m} \frac{Sv[i]}{N[Sv[i]]}$ 를 모든 n개의 자산에 대하여 구한다.
(Step 4) 수식 (3)을 이용하여 미리 연산한 $Vf(a_k,x)$에 $Vs(a_k,x)$를 더하여 $Vt(a_k,x)$를 계산한다.
(Step 5) 모든 n개의 자산의 $Vt(a_k,x)$를 비교하여 값이 큰 순서대로 자산별 우선순위 $prio(a_k)$를 구한다. 단, 우선순위는 동일 계층에 있는 자산들만 비교하여 계층별로 구한다.
(Step 6) (Step 1)~(Step 5)를 모든 네트워크 계층에 대하여 반복한다.

4) 복수개의 등가자산의 서비스가치

상기한 방식을 사용하면 모든 자산이 상호 구분 가능한 상황에서 자산의 서비스가치를 평가할 수 있다. 하지만 ISP의 네트워크는 일반 가정 및 기업의 네트워크와는 다르게 여러 가지 원인에 의해 서비스가 중단되는 것을 대비하여 잉여설계가 되

어 있다. 통상 중요한 서버 및 라우터 등은 2개 이상의 자산이 동일 서비스의 연속성을 유지하기 위해서 설치되며 그러한 자산들은 로드밸런싱 또는 백업 및 우회경로의 용도로 활용된다.

(가) 등가자산의 정의

등가자산이란 네트워크 상에서 동일한 서비스 제공을 목적으로 하는 자산이 1개 이상 존재하고 해당 자산의 용도와 기능이 상호 동등할 경우 해당 자산들을 등가자산이라 정의한다.

등가자산의 대표적인 예는 부하분산을 목적으로 설치된 복수개의 웹 서버 및 DNS 서버가 대표적이다. 이러한 등가자산들은 앞에서 설명한 수식들에 의해서는 서비스가치를 추정하기 어려운 특징들이 있다.

예를 들어 30대의 DNS 서버가 특정 ISP에 부하 분산이 가능하도록 설치되어 있다고 가정해 보자. 평상시에 30대의 서버들이 1년간 X 만큼의 서비스가치를 생산하고 있다고 가정할 경우, 어떤 원인에 의해서 특정한 DNS 서버가 다운이 되었다고 해서 그 시점에 X/30 만큼의 손실이 예상된다고 할 수는 없다. 만일 10대의 DNS 서버가 동시에 다운되었다고 할지라도 DNS 서비스에 지장이 없다고 한다면 X/30 × 10만큼의 서비스가치 손실이 예상된다고 이야기할 수 없다.

일반적인 확률이론을 적용하면 앞서 설명한 DNS 서버 장애의 경우 네트워크 장애 또는 침해시에 예상되는 서비스가치 손실액은

$$E(Loss) = \#\text{DNS server down} \times \text{DNS 서버당 서비스가치} \times \text{DNS 서버의 Down 확률} \quad (6)$$

이다. 하지만 로드밸런싱 설계 및 고가용성 설계 등에 의해서 실질적으로 확률이론의 기대값이 그대로 적용되기에는 무리가 있다. 왜냐하면 일부 DNS 서버의 장애시에도 다른 활성화 DNS 서버들에 의해 서비스의 연속성이 보장될 수 있기 때문이다. 그러나 DNS 서버가 모두 정상 동작하는 상태와 비교했을 때 서버 1대가 장애가 생겼을 때보다는 서버 10대가 장애가 생긴 상태가 예상 자산손실 규모가 클 개연성(Possibility)가 높다고 할 수 있다. 이런 개연성은 반드시 확률에 비례하는 것도 아니고 작동이 안 되는 장비의 숫자에 선형적으로 비례한다고 말할 수도 없다.

등가자산의 예상 자산손실을 모델링하기 위해서는 네트워크상의 위험이라는 원인이 자산가치 손실을 실체화하는 촉매 역할을 한다는 것을 인식해야 한다. 즉, 자산손실의 개연성에 영향을 미치는 위험의 존재 유무와 위험의 정도에 따라서 자산의 예상 손실액이 달라질 수 있다는 것이다. 각종 위험이 발생하고 그것이 원인이 되어 자산의 장애가 발생한 상태라면 서비스가치 및 고정자산가치 손실의 개연성이 존재하지만 그러한 위험이 없는 가운데 동일한 서비스를 제공하는 등가자산의 일부가 시스템 정지, 다운 등의 상태에 이르렀다면 예상되는 자산손실의 규모가 아주 작거나 또는 없을 것이라고 판단할 수 있다. 본 논문에서는 네트워크 상의 각종 위험의 개연성과 등가자산의 서비스 손실간의 관계를 설명하기 위해 자산가치 특성함수를 사용한다.

동일 계층 내에 복수개의 등가자산이 있고 그 중의 특정 등가자산들이 각종 위험에 의해 영향을 받고 있을 경우 자산이 제공하는 예상 손실 서비스 가치 V_{eqs}는 다음과 같이 표현할 수 있다.

$A_{eq} = \{a_{eq1}, a_{eq2}, ..., a_{eqk}\}$

$A_{eq} = \{a_h | a_h$는 성격이 동일한 등가자산$\}$

$$Veqs(A_{eq}) = \sum_{h=1}^{k} Vs(a_h, x) \cdot f_h(x_1, x_2, ..., x_n) \quad (7)$$

단,

k : 동일 성격의 등가자산의 개수

$X = \{x_1, x_2, ..., x_n\}$: 위험 집합

$f(X)$: 자산가치 특성함수

수식 (7)에 나타난 자산가치 특성함수 $f(x)$는 다음과 같은 조건을 만족해야 한다.

(가) $0 \leq f(X) \leq 1$

(나) $f(X)$ 는 모든 $\{x_1, x_2, ..., x_n\}$에 대하여 연속이고 미분 가능

(다) $P_o(X) \rightarrow 1$, $f(X) \rightarrow 1$

(라) $P_o(X) \rightarrow 0$, $f(X) \rightarrow 1$

여기서 (다), (라)는 $f(X)$의 중요한 특성이며 $P_o(X)$는 위험(Risk)의 개연성을 의미한다. 즉, 자산가치 특성 함수는 위험의 개연성이 커질수록 값이 1에 수렴하기 때문에 수식 (7)의 특정한 등가자산의 예상 서비스가치 손실액은 해당 자산의 서

비스가치로 수렴하며 위험의 개연성이 줄어들면 등가자산의 예상 서비스가치 손실액은 0으로 수렴하게 되어 위험의 영향에 대한 등가자산의 예상 서비스 가치 손실액의 변화를 반영하게 된다.

1. 자산가치 특성함수의 설계

1) 정성적 기준의 정량화

자산가치 특성함수는 앞서 설명한 바와 같이 4가지 조건을 만족시키되 적용하는 ISP의 네트워크 특징에 따라 달라질 수 있다. 통상적으로 ISP의 네트워크를 구성하는 자산들은 해당 ISP의 고객 특성 및 네트워크 설계 기준에 따라서 위험에 대해 취약한 정도가 다르고 관리체계 및 보안 장비의 설치 유무, 백업 및 로드밸런싱 장비의 대수와 네트워크 형상(Topology) 등에 따라서 자산가치 특성 함수가 크게 달라진다. 자산가치 특성함수는 자산에 대한 위험 요인들과 그들의 특성을 면밀히 파악 후 특성을 반영할 수 있도록 설계 되어야 한다.

본 논문에서는 상기한 바와 같이 정량화되기 어렵고 단순한 모델링이 불가능한 네트워크 보안 위험(Risk)과 자산가치 함수화의 모델링에 Kosko의 퍼지 인지 맵(Fuzzy Cognitive Map)을 개선한 이종필의 I-FCM(Improved Fuzzy Cognitive Map)을 사용한다.[9][10] 퍼지 인지 맵은 각각의 개념과 개념 사이의 링크로 구성이 된다. FCM은 다양한 복합 변수들 사이의 상호관계가 잘 드러나지 않는 시스템에서 각 개념사이의 인과관계를 잘 나타내 줄 수 있다.

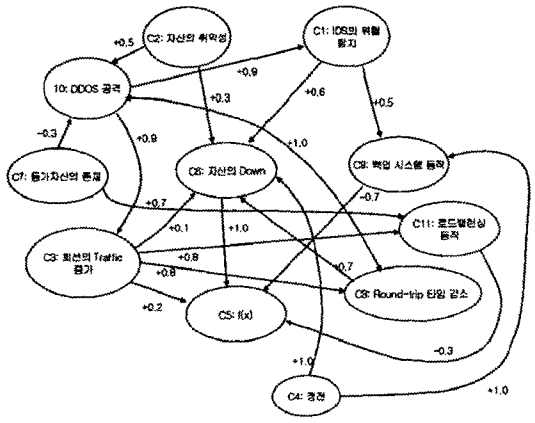

그림 2: ISP의 자산가치 특성함수 설계를 위한 FCM 예제

그림 2는 퍼지 인지 맵을 이용해서, ISP의 자산가치 특성함수의 값을 결정하는 예를 보여준다. FCM은 각 개념의 인과관계 사이의 강도(强度)를 이용해서 각 시스템 변수들의 변화 과정과 최종적으로 특정한 안정화 상태 및 진동 상태로 천이하는 과정을 살필 수 있는 장점이 있다. 그러나 FCM의 개념을 연결하는 각 링크의 강도를 결정하는 것은 전문가의 개인적인 판단에 의존하는 문제가 있기 때문에 이종필이 제안한 I-FCM을 이용해서 복수의 전문가의 의견을 수렴해서 특정 링크의 잘못된 연산을 방지하도록 하는 것이 바람직하다.

ISP가 보유한 자산들의 자산가치 특성함수 $f(X)$는 표 6의 순서대로 설계하면 된다. 네트워크상의 위험이 발생했을 때 $f(X)$의 값은 수식 (8)을 이용해 결정한다.

표 6: FCM의 설계 방법

(Step 1) 그림 3과 같이 각종 위협과 이벤트, 자산 및 자산가치 특성함수를 개념화하고 각 개념(C_i)들 간의 인과관계의 강도(W_{ji})를 결정한다.
(Step 2) 수식 (8)의 식을 이용하여 각종 개념들 사이의 인과관계가 제대로 설계되었는지 시뮬레이션하여 확인한다.
(Step 3) 필요 없는 개념, 잘못된 인과관계의 강도를 수정한다.
(Step 4) 설계가 완료되면 특정한 이벤트가 생길 경우 수식 (8)을 이용하여 각 인과관계의 전파 결과를 연산하여 $f(X)$의 값을 결정한다.
(Step 5) 필요에 따라 (Step 1)~(Step 4)를 반복한다.

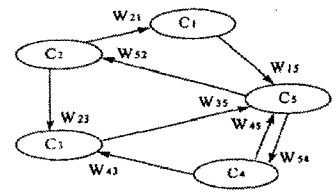

그림 3: 일반적인 FCM의 그림

$$A_i^t = h\left(\sum_{j=1, j\neq i}^{n} A_j^{t-1} W_{ji}\right) \quad (8)$$

단,

A_i^t : t 번째 단계에서의 개념 C_i의 값

W_{ji} : 개념 C_j에서 개념 C_i로 향하는 인과관계의 강도

h : Threshold 함수

FCM, 또는 I-FCM을 사용할 경우 전통적인 퍼지 추론 엔진이 갖는 언어 변수의 사용, 근사 추

론, 비선형 시스템에의 응용 만이 아닌 퍼지 추론 엔진이 갖추지 못한 추론시스템의 Scalability까지도 확보할 수 있는 장점이 있다.

III. 결론

본 연구에서는 네트워크 보안 위험시의 네트워크 자산의 서비스가치 손실을 모델화하기 위하여 네트워크를 계층화하고 계층화된 네트워크에서 자산의 서비스가치를 추정하는 방식을 제안하였다. 또한, 상이한 ISP의 네트워크 특성을 현실적으로 반영할 수 있도록 자산가치 특성함수의 개념을 도입하였으며 정성적으로 기술되는 인간 전문가의 지식과 네트워크 특성이 자동 연산되는 퍼지 인지맵(FCM)을 자산가치 특성함수의 연산에 도입하였다.

본 연구의 결과는 자산가치 추정을 정량적으로 할 수 있으며 자산가치 추정 시에 네트워크의 토폴로지, 잉여 자산이 설치된 네트워크의 서비스가치 산정이 가능하고 등가 자산 존재시의 예상 서비스손실액의 모델링이 가능하다는 것을 보여준다.

IV. 참고문헌

[1]임재명, "국내외 해킹 현황 및 대응 기술", NETSEC-KR 2003 pp547-580, 2003. 4
[2] 통신위원회 보도자료, "제94차 통신위원회 회의결과", 정보통신부, 2003.10.13
[3] 고려대학교. "해킹, 바이러스 피해액 산출방법 연구", 한국정보보호진흥원 최종연구보고서, 2002.11.30.
[4] 이현숙 외,"대학교를 대상으로 한 위협에 따른 손실의수치화", 한국정보보호학회, VOL.12, NO.4pp. 3-14, 2002. 8
[5] 우병구 외," 정보통신망의 효율적 보안관리를 위한 비즈니스 프로세스 기반의 자산평가모델 및 방법론에관한 연구" 한국정보처리학회, 10-C-4호, pp. 423-432, 2003. 8
[6] 최상수 외,"보안관리 및 위험분석을 위한 분류체계, 평가기준 및 평가스케일의 조사연구", 정보보호학회 pp38-49, 2003. 6
[7] 한국전산원,"위험분석 방법론 및 자동화 도구 기술이전 교육 교재", 1998.9
[8] KT," 관련 교재나 지침 등",
[9] Bart Kosko, "Fuzzy Thinking", 1993
[10] 이종필, "Design of Fault Diagnosis Expert System Using Improved Fuzzy Cognitive Maps and Rough Set Techniques", 1997