침입차단시스템 선정지침

이경구
TTA 기획 · 전략특별위원회 위원
한국정보보호센터 기획평가부 기술기준팀 팀장

1. 서론

조직의 내부망을 인터넷과 같은 외부망에 연결할 경우에 가장 일반적으로 사용될 수 있는 정보보호 대책은 두 망의 연결점에 침입차단시스템을 설치하여 조직의 정보보호 정책에 따라 접근을 통제하는 것이다. 이를 위하여 많은 침입차단시스템이 개발되어 제품으로 시장에 나와 있으나 일반 사용자들은 실제로 어떤 제품이 그들의 필요에 적합한 기능과 적절한 보증을 제공하는지 판단하기 어렵다.

이 침입차단시스템 선정지침은 조직의 내부망을 외부의 망과 연결하기 위하여 침입차단시스템을 도입하고자 하는 사용자가 자신의 조직의 위험 수준을 판단하여 보호수준에 부합하는 평가된 침입차단시스템을 선정할 수 있도록 하기 위한 것이다.

2. 침입차단시스템의 개념

2.1 침입차단시스템의 사용목적 및 정의

공개망에 대한 접속은 외부 공격자가 조직내부의 시스템에 침투할 위험을 가져온다. 이것은 모든 공개망에 해당되는 문제점이지만 인터넷에 관해서는 더 심각한 문제이다. 보다 근본적인 원인은 인터넷에서 사용되는 통신 기술이 근본적으로 안전하지 않기 때문이다. 최근에는 내부 사용자가 중요 정보를 외부 수신자에게 전달하는 새로운 보안 문제들이 나타나고 있으며 비록 자료가 합법적으로 인터넷을 통해 전송되는 경우에도 지명된 수신자에게 도달하기 전까지 전 세계 어느 곳을 경유하게 될 지 모르기 때문에 이에 대한 대책 마련이 필요하다. 이러한 문제점들을 효율적으로 해결하기 위하여 사용되는 일반적인 방법이 바로 망간의 접속점에 침입차단시스템을 설치하여 사용하는 것이다.

침입차단시스템이란 정보통신망 간의 상호접속이나 데이터 전송을 안전하게 통제하기 위하여 신분확인, 접근통제, 무결성, 비밀성, 감사기록 및 추적, 보안관리 기능을 제공하는 소프트웨어 및 하드웨어를 말한다. 일반적으로 제품화된 침입차단시스템은 단일한 소프트웨어나 하드웨어로 구성되지만 개념적으로는 라우터, 개인용 컴퓨터, 호스트, 또는 호스트의 집합이 될 수도 있다.

2.2 침입차단시스템의 유형

침입차단시스템은 다양한 방법으로 구현될 수 있으나 일반적인 구현 방식은 크게 패킷 필

터링 방식과 응용 게이트웨이의 두 가지 유형으로 나눌 수 있다. 현재 상용화된 대부분의 제품들은 이런 두 가지 유형 중의 하나이거나 이를 혼합한 형태이다.

2.2.1 패킷 필터링

IP 패킷 필터링은 라우터를 통과하는 패킷을 몇 가지 조건에 따라 필터링 하기 위한 것이다. 패킷 필터링 라우터는 보통 다음에 제시되는 항목들의 전부나 또는 일부에 기반을 두고 IP 패킷을 필터링할 수 있다.

- 발신지 IP 주소
- 목적지 IP 주소
- TCP/UDP 발신지 포트
- TCP/UDP 목적지 포트

2.2.2 응용 게이트웨이

패킷 필터링 라우터와 연관된 문제점들을 해결하기 위해 침입차단시스템은 TELNET이나 FTP와 같은 서비스를 필터링하고 연결하기 위한 응용 소프트웨어를 사용할 수 있다. 그런 응용을 프록시 서비스라고 하며 프록시 서비스가 운영되고 있는 호스트를 응용 게이트웨이(Application Gateway)라고 한다.

응용 게이트웨이가 작동하는 과정은 다음과 같다.

- 처음에 사용자는 TELNET으로 응용 게이트웨이에 연결한 후 내부 호스트의 이름을 입력하여 연결을 요청한다.
- 응용 게이트웨이는 사용자의 발신지 IP 주소를 검사한 후 내부의 접근 방침에 따라 연결을 허용하거나 거부한다.
- 이때 사용자가 일회용 패스워드와 같은 기법을 이용하여 인증을 해야 할 경우도 있다.
- 프록시 서비스는 응용 게이트웨이와 내부 호스트간의 TELNET 연결을 수립한다.
- 연결 수립 후 프록시 서비스는 연결 요청을 통과시키고 서버의 응답을 받아 사용자에게 보낸다. 응용 게이트웨이가 이 연결을 기록한다.

2.2.3 복합형 게이트웨이

복합형 게이트웨이(Hybrid Gateway)는 위에서 언급한 두 가지 침입차단시스템 유형을 결합한 것이다. 복합형 게이트웨이는 단일 제품으로 구현될 수도 있고 서로 다른 유형의 침입차단시스템을 직렬 형태로 구성한 것일 수도 있다.

2.3 침입차단시스템의 구성형태

침입차단시스템은 필요한 보안 수준을 제공하기 위하여 여러 가지 방식으로 설치, 운용될 수 있고 소요되는 비용의 수준도 다양하다. 각 조직에서는 당면하고 있는 위협과 발생 가능한 위험을 고려하여 적절한 제품을 선택할 수 있고 최대의 효과를 얻을 수 있다.

2.3.1 멀티 홈드 호스트

멀티 홈드 호스트(Multi-homed Host)는 하나 이상의 인터페이스를 갖는 침입차단시스템으로 각각의 인터페이스가 논리적, 물리적으로 분리된 통신망 세그먼트에 연결되어 있는 것이다. 다중 홈드 호스트의 가장 흔한 예는 두 개의 인터페이스를 갖는 듀얼 홈드 호스트이다. 듀얼 홈드 호스트는 두개의 인터페이스가 서로 다른 통신망에 연결되어 있는 것이다. 즉 둘 중 한 인터페이스는 일반적으로 외부 또는 신뢰할 수 없는 통신망에 연결하고, 다른 한 인터페이스는 내부 또는 신뢰할 수 있는 통신망에 연결한다.

2.3.2 방어용 호스트

방어용 호스트(Screened Host) 구조는 외부망으로부터의 접속 요청을 내부망의 시스템에 연결하는 대신 안전한 방어용 호스트에 연결하도록 한다. 이를 위해 외부망으로부터의 모든 연결 요청은 방어용 호스트로 보내도록 필터링 라우터를 구성한다.

2.3.3 방어용 서브넷

방어용 서브넷(Screened Subnet)은 본질적으로 방어용 호스트 구조와 같지만, 내부망과 분리되어 안전한 호스트가 상주하는 방어용 서브넷을 만들어 내부망과 외부망을 분리함으로써 추가의 보안을 제공한다.

3. 침입차단시스템 평가기준

침입차단시스템을 평가하기 위한 기준은 등급별 보안기능 요구사항과 보증 요구사항으로 이루어진다. 평가등급은 최저의 평가등급인 K1에서 최고의 평가등급인 K7까지의 7단계로 구분한다.

3.1 침입차단시스템 평가기준의 구조

3.1.1 보안기능 요구사항

- 침입차단시스템에 대한 보안기능 요구사항은 신분확인, 접근통제, 무결성, 비밀성, 감사기록 및 추적, 보안관리의 6가지 사항으로 이루어진다.
- 신분확인은 침입차단시스템에 접근하는 관리자 및 사용자의 신분을 증명하는 기능이다.
- 접근통제는 주체가 침입차단시스템을 통하여 객체에 접근을 시도하는 경우 미리 정해진 접근통제규칙을 적용하여 접근을 통제하는 기능이다.
- 무결성은 침입차단시스템의 중요한 데이터나 침입차단시스템을 통하여 전송되는 데이터에 변경이 발생하는 경우 이를 확인하는 기능이다.
- 비밀성은 침입차단시스템을 통하여 전송되는 데이터가 인가되지 않은 사용자에게 노출되는 경우 그 내용이 알려지는 것을 방지하는 기능이다.
- 감사기록 및 추적기능은 침입차단시스템을 통하여 이루어지는 사용자의 보안관련 활동 및 사건을 기록, 조사하고 침입사건의 발생을 탐지하는 기능이다.
- 보안관리는 관리자가 침입차단시스템의 보안관련 데이터와 보안기능을 안전하게 유지하기 위하여 수행하는 기능이다.

3.1.2 보증 요구사항

침입차단시스템 보안기능의 신뢰성을 확인하기 위한 보증 요구사항은 개발과정, 시험과정, 형상관리, 운영환경, 설명서, 취약성의 6가지 사항으로 이루어진다.

- 개발과정은 침입차단시스템의 기능명세, 기본설계, 상세설계 및 구현 단계로 이루어지며 각 단계별로 보안목표명세서, 보안모델명세서, 기능명세서, 기본설계서, 상세설계서, 검증명세서, 원시프로그램, 하드웨어 도면을 문서로 작성하는 과정이다.
- 시험과정은 침입차단시스템의 보안기능이 보안목표명세서에 서술된 보안목적에 부합하도록 동작하는지를 확인하는 과정이다.
- 형상관리는 침입차단시스템을 구성하고 있는 형상항목의 변화를 일관성있게 통제하고 관리하기 위한 방법이다.
- 운영환경은 침입차단시스템의 안전한 설치과정과 운용절차에 대한 요구사항이다.
- 설명서는 일반 사용자를 위한 사용자 설명서와 관리자를 위한 관리자 설명서로 이루어진다.
- 취약성에 대한 요구사항은 침입차단시스템의 취약성 분석과 오용분석으로 이루어진다.

3.1.3 등급에 따른 침입차단시스템 기능요약

가. K1 등급

K1등급의 침입차단시스템은 관리자를 식별 및 인증하고 침입차단시스템을 통하여 이루어지는 모든 접속에 대하여 임의적 접근통제를 수행한다. K1 등급의 평가는 침입차단시스템,

보안목표명세서, 기능명세서와 시험서, 형상관리 문서, 설명서를 조사함으로써 기본적인 보증을 제공한다.

나. K2 등급

K2 등급은 K1 등급의 모든 보안기능 요구사항을 포함하며 사용자 식별 및 인증, 데이터 패킷에 대한 임의적 접근통제, 기본적인 감사기록 및 추적을 위한 감사기록 레코드 생성과 이를 위한 추가적인 보안관리 기능을 제공한다. K2 등급의 평가에는 K1 등급에서 수행한 것에 기본설계서와 운영환경 및 취약성에 대한 분석이 포함된다.

다. K3 등급

K3 등급은 K2 등급의 모든 보안기능 요구사항을 포함하며 무결성 기능을 제공한다. 또한 감사기록 및 추적을 용이하게 하기 위한 추가적인 기능을 제공한다. K3 등급의 평가에는 K2 등급에서 수행한 것에 상세설계와 형상관리체계에 대한 분석이 포함된다.

라. K4 등급

K4 등급은 K3 등급의 모든 보안기능 요구사항을 포함하며 재사용 공격에 대한 대처와 강제적 접근통제 기능을 제공한다. K4 등급의 평가에는 K3 등급에서 수행한 것에 원시프로그램과 검증명세서에 대한 분석이 포함된다.

마. K5 등급

K5 등급은 K4 등급의 모든 보안기능 요구사항을 포함하며 상호인증과 데이터 패킷에 대한 강제적 접근통제를 제공한다. K5 등급의 평가에는 K4 등급에서 수행한 것에 보안모델명세서에 대한 분석이 추가되며 더 강한 보증을 제공하기 위하여 설계서의 준정형화와 각 설계단계에서의 검증을 요구한다.

바. K6 등급

K6 등급은 K5 등급의 모든 보안기능 요구사항을 포함하며 침입탐지 기능을 제공한다. K5 등급의 평가에는 K4 등급에서 수행한 것을 포함하여 더 구조적인 설계와 도구를 사용한 형상관리를 수행할 것을 요구함으로써 더 강한 보증을 제공하도록 한다.

사. K7 등급

K7 등급은 K6 등급의 보안기능 요구사항과 동일한 기능을 제공하지만 보증에 있어서 정형화된 기능명세와 기본설계를 요구함으로써 설계를 검증할 수 있도록 하였다. 따라서 K7 등급은 가장 높은 수준의 보증을 제공하게 된다.

4. 정보통신망 위험 수준 결정

4.1 개 요

정보통신망의 위험 수준을 결정하는 일은 현재 사용중인 통신망에 존재하는 위협을 분석하고 해당 위협이 발생하였을 경우 이로 인한 피해가 어느 정도인지를 예측하고 예상되는 위험 수준을 결정하는 작업이다. 이 표준에서는 침입차단시스템의 도입이라는 제한된 목적으로 적정 평가등급을 결정하기 위해 필요한 개략적인 위험 수준의 판단이 목표이므로 일반적인 정교한 위험분석 방법론을 따르는 대신 위험분석 전문가가 아니더라도 기관의 정보통신망 담당자가 판단하고 따를 수 있는 단순화된 위험 수준 결정 공식을 제시한다.

일반적으로 위험을 계량적으로 파악하기 위해서는 위협사건의 발생빈도와 이러한 사건이 미치는 피해의 양으로 연간 예상 손실을 계산하여 이를 위험의 양으로 사용한다. 즉,

연간 예상 손실(위험) = 피해 × 발생빈도

로 나타낸다. 이 값을 정확히 알아낼 수 없으

므로 피해와 발생빈도를 등급으로 나누어 예상 손실의 대략적인 크기를 파악하고 이 비용을 기준으로 대책을 수립하는 것이 일반적이다. 이 표준에서는 이러한 기본 공식을 따르되 피해와 발생빈도의 추정에 고려하는 요소들을 단순화하여 침입차단시스템의 등급결정에 활용할 수 있는 위험 수준 결정 방법을 제시한다.

4.2 위협 수준

4.2.1 위협의 존재 정도

위협이란 정보를 폭로, 수정, 파괴하거나 또는 중요한 서비스를 방해함으로서 조직에 해를 주는 잠재적인 사건이나 상황을 의미한다. 위협은 인간의 실수, 하드웨어/소프트웨어의 고장 또는 자연 재해와 같은 악의가 없는 것에서부터 허용되지 않은 정보를 얻거나 타인의 정보를 파괴하고 기능을 떨어뜨리는 악의적인 것으로 범주화될 수 있다.

이 표준에서는 적정 평가등급의 침입차단시스템을 선정한다는 목적에 맞추어 망간의 연결에서 고려하여야 할 위협만을 분석한다. 따라서 침입차단시스템을 선정하기 위한 위협의 존재 정도는 통신망의 활용 환경에 따라 다음과 같이 분류할 수 있다.

- 낮음 - 외부망에서 내부망으로 접속하는 경우 반드시 필요한 프로토콜 외에는 지원하지 않으며 여러가지 제한이 있다. 외부망에서 내부망으로 접속가능한 사용자 계정 역시 엄중 관리되며 수가 많지 않다.
- 중간 - 외부망에서 내부망에 접속하여 일정한 작업의 수행이 가능하다. 그러나 내부망에서 접속하는 경우보다는 제한된 기능만을 제공하며 안전하지 않은 것으로 알려진 프로토콜은 제한된다. 접속계정은 업무상의 필요성을 검토한 후 발급된다. 조직의 네트워크 운영에 관한 전체적인 현황이 파악되고 관리된다.
- 높음 - 외부망에서 내부망으로 접속하는 경우와 내부망에서 접속하는 경우에 권한이나 기능의 차이가 없다. 대부분의 프로토콜이 지원되며 모든 계정이 외부망에서 접속하여 사용 가능하다. 또는 조직의 네트워크 접속이 부서마다 별도 관리되어 현황 파악 및 통제가 어려운 경우가 해당된다.

4.2.2 내부 정보 공개 정도

내부 정보의 공개 정도란 악의를 가진 사용자가 내부 시스템에 흥미를 갖도록 하는 정보가 유통되거나 그러한 사용자가 공용 도메인에서 침투하고자 하는 시스템에 대해 얻을 수 있는 정보의 양을 의미한다.

이 표준에서는 상세한 시기별 위험분석을 목표로 하지 않으므로 개략적인 정책을 기반으로 내부 정보의 공개 정도를 분석한다. 인터넷에 기반을 둔 대부분의 위협은 본질적으로 기회를 노리는 성격을 갖기 때문에 조직의 내부 정보 공개 정도는 악의를 가진 공격자가 공격을 시도하려고 마음먹게 하는 하나의 중요한 요인이다.

내부 정보의 공개 정도는 조직의 상황에 따라 다음과 같이 분류할 수 있다.

- 낮음 - 보안을 중요시하여 조직의 구조나 기능이 외부에 거의 알려지지 않는다. 웹서비스 등은 제공하지 않거나 제공하는 정보가 제한된다.
- 중간 - 조직의 보안이나 공개 원칙이 뚜렷하지 않거나 경우에 따라 달라진다. 행사 등을 통해 정기적으로 일반인들에게 조직의 구조나 기능을 공개한다.
- 높음 - 공개 원칙에 따라 조직이 운영되고 있으며 웹이나 다양한 행사를 통하여 지속적으로 조직의 구조나 기능을 공개한다.

4.2.3 위협 수준 결정

위협 수준은 위협의 존재 정도와 내부 정보

공개 정도의 함수로 나타낸다. 이를 표현하기 위하여 위협의 존재 정도 및 내부 정보 공개 정도에 대하여 각각 L, M, H의 값을 할당한다. 이를 [표 4-1]에서 보였다.

[표 4-1] 위협 수준을 결정하기 위한 정도값

위협의 존재 정도	정도값	내부정보 공개 정도	정도값
낮음	L	낮음	L
중간	M	중간	M
높음	H	높음	H

이때 위협의 존재정도를 P, 내부정보의 공개정도를 O라 하면 위협 수준 T는 P와 O의 합으로 결정된다.

$T = f_1(P, O)$

$= w_P \cdot P + w_O \cdot O$

단 O, P = {L, M, H}이고 w_P, w_O는 두 요소의 값을 동일한 척도로 나타내기 위한 가중치이다.

〈위협수준의 수치값 결정방법 1〉

O와 P를 수치적으로 표현하기 위해서 먼저 "낮음"과 "중간"의 비율과 "중간"과 "높음"의 비율을 정하면 "낮음"을 1로 놓았을 때 "중간"과 "높음"의 크기를 수치적으로 정할 수 있다. 이를 [표 4-2]에서 보였다.

[표 4-2] 정도의 수치값 결정

정도값	L	M	H
수치값	1	"중간"/"낮음"	"높음"×"중간"×M

그리고 나서 위협의 존재정도와 내부정보 공개정도의 "낮음" 값이 위협에 미치는 영향을 고려하여 w_O/w_P 의 비를 결정한다.

이 값을 식 "$T = w_P \cdot P + w_O \cdot O$"에 대입하면 위협수준의 수치값을 구할 수 있다.

〈위협수준의 수치값 결정방법 2〉

수치값을 직접 판단하여 결정하는 것이 어려운 경우에는 다음과 같은 방법을 사용할 수 있다.

T의 값의 크기는 위에서 언급한 가중치와 실제 수치값에 따라 달라지므로 이러한 값이 어떻게 결정되더라도 T를 표현할 수 있도록 O와 P의 값에 따라 [표 4-3]과 같이 표현한다.

[표 4-3] 위협 수준표

내부정보 공개정도 \ 위협의 존재정도	낮음	중간	높음
낮음	LL	LM	LH
중간	ML	MM	MH
높음	HL	HM	HH

정의상 L〈M〈H의 관계가 있으므로 T가 갖는 각 값은 다음과 같은 부분 순서 관계를 갖는다.

LL〈LM ; LM〈MM ; MH〈HH

LL〈ML ; ML〈MM ; HM〈HH

이때 만일 내부정보의 공개정도와 위협의 공개정도가 위협 수준에 미치는 영향이 비슷하다고 판단된다면 가중치를 $w_O = w_P = 1$로 놓을 수 있고 다음과 같은 순서관계가 발생한다.

LM = ML ; MH = HM

이렇게 되면 위협수준의 각 값들의 순서관계는 LH = HL = MM ; LH = HL〉MM ; LH = HL〈MM ; 인 세가지 경우로 나눌 수 있다.

즉, 이들의 대소관계는 다음과 같은 세가지 순서가 나타날 수 있다.

i) LL〈LM = ML〈MM = LH = HL〈MH = HM〈HH

ii) LL〈LM = ML〈MM〈LH = HL〈MH = HM〈HH

iii) LL〈LM = ML〈LH = HL〈MM〈MH = HM〈HH

이러한 순서관계는 L, M, H의 상대적 크기에

따라 나타난다. L과 M의 차이가 M과 H의 차이와 같으면 MM = LH = HL 이 되고 L과 M의 차이가 M과 H의 차이보다 적으면 MM〈 LH = HL이 된다. 그리고 L과 M의 차이가 M과 H의 차이보다 크면 MM〉LH = HL이 된다.

따라서 운영자는 T = MM인 경우와 T = HL 또는 LH 인 경우의 영향을 비교하여 자신의 판단이나 전문가의 의견에 따라 위의 세가지 예 중 하나를 택하여 사용하면 된다.

4.3 피해 수준

4.3.1 실제적인 피해 정도

네트워크에 잠재적으로 존재하는 위협이 공격자에 의해 위험으로 현실화되었을 경우 그로 인해 발생하는 피해의 규모를 정확히 측정하기란 대단히 어려운 일이다. 일반적으로는 즉각적으로 나타나는 비용상의 손실을 주로 파악하게 되지만 그러한 사고로 인한 기능의 손상 및 내·외부의 영향은 즉각적일 수도 있으나 주로 장기적으로 영향을 미치게 된다. 따라서 이 표준에서는 이 두 측면을 나누어 각각의 피해 정도의 합으로 전체적인 피해 정도를 나타낸다.

○ 실제적인 피해 정도(기업의 경우)

- 낮음 - 피해로 인한 비용의 추가지출이 적어 계획된 예산 내에서 처리할 수 있다.
- 중간 - 피해로 인한 비용이 계획된 예산을 초과하여 기업 수입에 타격을 입는다.
- 높음 - 기업 내부 뿐만 아니라 관련된 여타 기업까지 피해가 확산된다.

실제적인 피해 정도(공공기관의 경우)

- 낮음 - 국민 개인에 미치는 피해가 거의 없거나 경미하다.
- 중간 - 피해로 인해 관련 개인의 사생활권이나 개인의 재산권이 침해된다.
- 높음 - 개인의 신체나 생명 손상이 가능하다. 또는 피해의 범위가 넓어 불특정 다수에게 피해가 확산된다.

4.3.2 기능 손상 정도

이 항목에서는 사건의 일차적인 영향보다는 시간이 지나면서 지속적인 영향을 미치는 측면을 반영하고자 조직의 기능이나 외부와의 관계에 미치는 영향을 다음과 같이 분류하였다. 이것은 기업체나 공공기관 모두가 동일하게 적용한다.

- 낮음 - 피해가 쉽게 복구 가능하거나 대체절차로 수행가능하여 해당 부서 내에서 해결된다.
- 중간 - 복구기간이 길어 업무 수행에 지속적인 영향을 미치며 대외 이미지를 손상시킨다.
- 높음 - 조직의 기능이 파괴되거나 손상되어 사회적이나 국가적으로 문제가 된다.

4.3.1절에서 언급한 경우에는 피해 발생으로 인해 영향을 받는 대상이 국민이나 비용이었으나 이 경우에는 조직의 업무 기능이 피해의 대상이라는 점에서 앞서 분류한 내용과는 구별된다. 즉, 4.3.1절의 내용이 사건 발생으로 인한 구체적인 손실의 측면을 다루는 것이라면 4.3.2절은 조직의 지속적인 기능 수행에 대한 피해의 측면을 강조한 것이다.

4.3.3 피해 수준 결정

전체적인 피해 수준은 실제적인 피해 정도와 기능 손상 정도의 함수로 나타낸다. 이를 표현하기 위하여 실제적인 피해 정도 및 기능 손상 정도(낮음, 중간, 높음)에 대하여 L, M, H의 값을 할당한다. 이를 [표 4-4]에서 보였다.

[표 4-4] 피해 수준을 결정하기 위한 정도값

실제적인 피해 정도	정도값	기능 손상 정도	정도값
낮음	L	낮음	L
중간	M	중간	M
높음	H	높음	H

위협 수준의 결정시와 마찬가지로 실제적인 피해 정도를 A, 기능 손상 정도를 F 라 하면 피해 수준 D는 A와 F의 함으로 결정된다.

$D = f_2(A, F)$

$= w_A \cdot A + w_F \cdot F$

단 A, F = {L, M, H} 이고 w_A, w_F는 두 요소의 값을 동일한 척도로 나타내기 위한 가중치이다.

〈피해수준 수치값 결정방법 1〉

A와 F를 수치적으로 표현하기 위해서 먼저 "낮음"과 "중간"의 비율과 "중간"과 "높음"의 비율을 정하면 "낮음"을 1로 놓았을 때 "중간"과 "높음"의 크기를 수치적으로 정할 수 있다.

[표 4-5] 정도의 수치값 결정

정도값	L	M	H
수치값	1	"중간"/"낮음"	"높음"/"중간"×M

그리고 나서 위협의 존재정도와 내부정보 공개정도의 "낮음"값이 전체 피해수준에 미치는 영향을 비교하여 w_A/w_F의 비를 결정한다.

이 값을 위의 식 "$D = w_A \cdot A + w_F \cdot F$"에 대입하면 피해수준의 수치값을 구할 수 있다.

〈피해수준 수치값 결정방법 2〉

위협수준의 경우와 마찬가지로, D의 값의 크기는 위에서 언급한 가중치에 따라 달라지므로 이러한 값이 어떻게 결정되더라도 D를 표현할 수 있도록 A와 F의 값에 따라 [표 4-6]과 같이 표현한다.

[표 4-6] 피해 수준표

실제적인 피해 / 기능손상	낮음	중간	높음
낮음	LL	LM	LH
중간	ML	MM	MH
높음	HL	HM	HH

이때 이들의 대소관계는 위협수준의 경우와 마찬가지로 다음과 같은 세가지 순서가 나타날 수 있다.

i) LL〈LM = ML〈MM = LH =HL〈MH = HM〈HH

ii) LL〈LM = ML〈MM〈LH =HL〈MH = HM〈HH

iii) LL〈LM = ML〈LH =HL〈MM〈MH = HM〈HH

따라서 운영자는 D= MM인 경우와 D = HL 또는 LH의 경우의 영향을 비교하여 자신의 판단이나 전문가의 의견에 따라 위의 세가지 예 중 하나를 택하여 사용하면 된다.

4.4 위험 수준의 결정

위험 수준을 앞 절에서 설명한 바와 같은 방식으로 공식을 작성한다면 위험 수준 R은 위협 수준 T와 피해 수준 D의 함수로 결정되며 다음과 같이 표현될 수 있다.

$R = f_3(T, D)$

여기에서는 4.1절에서 언급한 고전적인 위험 산정 공식인 연간 예상 손실(위험) = 피해 × 발생빈도의 공식을 따른다. 즉, R = T × D 가 된다.

〈위험수준 결정방법 1〉

위협의 존재정도, 내부정보 공개정도, 실제적인 피해정도, 기능 손상 정도의 수치값을 위협 수준 수치값 결정방법 1, 2에서 설명한 방식으로 결정하고 이를 수식에 대입하면 위험의 수준을 결정할 수 있다. 그러나 이 경우 각 요소의 최소값(L)은 1로 결정되나 최대값은 특정의 값으로 한정되지 않는다. 따라서 이를 보정하기 위해 위험 수준값을 최대값으로 나누어 위험수준의 수치값이 0과 1사이의 값이 되도록 한다.

$R = T/Max(T) \times D/Max(D)$

이렇게 하면 위험의 최대값은 1이 되고 다음

과 같은 범위에 따라 높음, 중간, 낮음의 등급으로 분류한다.

낮음 : R〈0.3, 중간 : 0.3≤R〈0.6, 높음 : 0.6≤R≤1

〈위험수준 결정방법 2〉

위협수준 및 피해수준 결정방법 2에서 설명한 $w = w_O = w_P = w_A = w_F = 1$인 경우에 대하여 MM과 LH와의 관계정립에 따라 다양한 경우가 발생할 수 있다.

예를 들어 MM = HL = LH인 경우는 {L, M, H} = {1, 2, 3}으로 정함으로써 위험 수준을 계산할 수 있다. 이때 가능한 경우는 [표 4-7]처럼 분류되고 최종 위험 수준치는 [표 4-8]로 나타난다. 실선과 음영으로 낮음, 중간, 높음의 위험 수준을 구분하였다.

[표 4-7] 위협수준과 피해수준이 모두 MM=HL=LH 인 경우

MM=LH=HL / MM=LH=HL	LL	LM=ML	MM=LH=HL	MH=HM	HH
LL	LLLL	LLLM LLML	LLMM, LLLH LLHL	LLMH LLHM	LLHH
LM=ML	LMLL MLLL	LMLM, LMML MLLM, MLML	LMMM, LMLH LMHL, MLMM MLLH, MLHL	LMMH, LMHM MLMH, MLHM	LMHH MLHH
MM=LH=HL	MMLL LHLL HLLL	MMLM, MMML LHLM, LHML HLLM, HLML	MMMM, MMLH MMHL, LHMM LHLH, LHHL HLMM, HLLH HLHL	MMMH, MMHM LHMH, LHHM HLMH, HLHM	MMHH LHHH HLHH
MH=HM	MHLL HMLL	MHLM, MHML HMLM, HMML	MHMM, MHLH MHHL, HMMM HMLH, HMHL	MHMH, MHHM HMMH, HMHM	MHHH HMHH
HH	HHLL	HHLM, HHML	HHMM, HHLH HHHL	HHMH, HHHM	HHHH

[표 4-8] 위협수준과 피해수준이 모두 MM=LH=HL인 경우 위험수준

MM=LH=HL / MM=LH=HL	LL (2)	LM=ML (3)	MM=LH=HL (4)	MH=HM (5)	HH (6)
LL(2)	0.11	0.17	0.25	0.28	0.33
LM=ML(3)	0.17	0.25	0.33	0.42	0.5
MM=LH=HL(4)	0.22	0.33	0.44	0.56	0.67
MH=HM(5)	0.28	0.42	0.56	0.69	0.83
HH(6)	0.33	0.5	0.67	0.83	1

5. 정보통신망의 위험수준에 따른 침입차단시스템 선정 방법

위험 수준과 침입차단시스템 평가등급을 대응시키는 이 표준은 각 평가등급에서 요구되는 보안기능 요구사항이 제안된 위험 수준에 대해 적절히 대처할 수 있는가의 여부에 따라 결정하였다.

결정된 위험수준에 적절히 대응할 수 있는 침입차단시스템을 선정하고자 할 때는 침입차단시스템 평가기준의 특성상 낮은 위험 수준의 경우 K1, K2 평가등급을, 중간 위험 수준의 경우 K3, K4 평가등급을, 마지막으로 높은 위험 수준의 경우 K5, K6, K7 평가등급을 사용하는 것이 적절하다. 위험의 수준에 따른 상세한 선정 지침은 [표 5-1]과 같다.

정보통신망의 위험을 정확히 분석하는 것은 매우 어려운 일이므로 적절한 평가등급의 침입차단시스템을 선정하기 위하여 필요한 기본적인 위험 수준을 판단하는 것에 초점을 맞추어 개략적인 위험 수준을 결정하기 위한 방법론을 제시하였고, 이에 따라 적합한 침입차단시스템의 평가 등급을 제시하였다. 또한 높은 위험 수준에 적합한 고등급의 침입차단시스템이 아직 개발되지 못한 현재의 상황을 고려하여 이러한 상황에서도 적용할 수 있는 위험 수준에 따른 침입차단시스템의 구성 예를 제시하였다.

그러나 위험 수준에 적합한 평가등급의 침입차단시스템을 선정, 도입한 경우에라도 이것만으로 정보통신망의 보안이 해결되었다고 생각하는 것은 매우 위험한 일이다. 침입차단시스템은 내부망과 외부망 간의 통신만을 통제하는 것으로 내부망 내에서 일어나는 위협에는 적절한 대책이 되지 못한다. 또한 평가된 침입차단시스템을 적절한 구조로 구성하였다고 하더라도 설치 과정 및 운영 관리상의 문제로 제 기능을 발휘하지 못할 수도 있다. 따라서 침입차단시스템의 안전한 설치 및 운영에도 만전을 기하여야 한다.

[표 5-1] 위험수준의 분류

위험수준 R	0≤R<0.1	0.1≤R<0.2	0.2≤R<0.3	0.3≤R<0.4	0.4≤R<0.6	0.6≤R<0.7	0.7≤R<0.8	0.8≤R≤1
평가등급	없음	K1(E)	K2(E)	K3(E)	K4(E)	K5(E)	K6(E)	K7(E)

암호화 기능은 모든 등급에서 선택 가능하므로 특별한 설명을 제시하지 않았으며 암호화 기능이 필요한 경우 K1(E)~K7(E)등급의 침입차단시스템을 선정, 사용하면 된다.

6. 결론

지금까지 정보통신망의 위험수준을 결정하고 이에 적합한 침입차단시스템을 선정하고 구성하기 위한 요구사항을 설명하였다.

이 표준은 침입차단시스템의 도입을 고려하는 많은 사용자들에게 실제적인 도움이 될 수 있다. TTA