전문가 의견 기반 사이버 침해 예측 방법론 연구

강영길[O*], 윤종현[**], 이수원[*], 박인성[***]
*숭실대학교 대학원 컴퓨터학과
**숭실대학교 사회과학연구소
***국가보안기술연구소
dudrlf34@mining.ssu.ac.kr, iosue@korea.com, swlee@ssu.ac.kr, insung@etri.re.kr

Research for Expert Opinion-Based Cyber Infringement Prediction Methodology

Younggil Kang[O*], JongHyun Yun[**], Soowon Lee[*], Insung Park[***]
*Dept. of Computing, Graduate School, Soongsil University
**Institute of Social Science in Soongsil University
***National Security Research Institute

요 약

사이버 침해란 정보시스템의 취약한 부분을 공격하여 시스템 내부에 침입하거나 시스템을 마비/파괴하는 등의 사고를 유발하는 모든 행위를 말한다. 이러한 사이버 침해의 피해를 줄이기 우해 국내외 많은 연구 기관과 업체에서는 침해탐지시스템과 같은 정보보호 기술을 연구 개발하여 상용화하고 있다. 그러나 기존의 정보보호 기술은 이미 발생한 침해를 탐지하여 피해의 확산을 막는 데만 한정적으로 사용되고, 침해의 발생 가능성을 예측하지는 못하기 때문에 정차 첨단화, 다양화되고 있는 사이버 침해에 대응하기 힘들다는 문제점을 갖는다.

본 논문에서는 보안 취약점을 이용한 사이버 침해를 대상으로 전문가 설문을 통해 사이버 침해의 발생 가능성을 예측하는 방법을 제안하고, 이를 위한 사이버 침해 예측 항목을 추출하였다. 예측 항목 추출은 3 단계로 구성되며, 첫 번째 단계에서는 기존 연구와 사례 분석을 통해 예측 항목의 계층 구조를 생성한다. 두 번째 단계에서는 첫 번째 단계를 통해 생성된 예측 항목들을 델파이 방법을 통해 개선하여 최적의 예측 항목을 결정한다. 마지막 단계에서는 각 항목들에 대한 쌍대 비교 설문을 진행하여 항목 간 가중치를 추출한다.

1. 서 론

사이버 침해란 정보시스템의 취약한 부분을 공격하여 시스템 내부에 침입하거나 시스템을 마비/파괴하는 등의 사고를 유발하는 모든 행위를 말한다. 최근의 사이버 침해의 추세는 다양한 유형의 정보 갈취형 해킹사고가 빈발하면서 시스템 마비, 실력 과시 등의 단순 목적이 아닌 금전적 이득을 노리는 범죄 수단으로 악용되고 있는 것으로 나타났다. 그 예로 방문자가 많은 홈페이지를 해킹하여 악성코드를 은닉하여 개인 정보를 유출하거나, 전자 우편에 의한 백도어 전파 등 다양한 수법의 사이버 침해가 발생하고 있다[1,2]. 또한, 매일 업데이트되는 보안 권고문에 나타난 보안 취약점을 이용한 사이버 침해는 점차 첨단화, 다양화되고 있다.

이에 따라 국내외 많은 연구 기관과 업체에서는 정보보호 기술을 연구, 개발하여 상용화하고 있다. 특히, 네트워크의 보안이 중요한 문제로 대두되면서 방화벽과 함께 네트워크 보안에 대한 신뢰성을 높이기 위한 침해탐지시스템(IDS : Intrusion Detection System)이 차세대 네트워크 보안 솔루션으로 주목을 받고 있다. 침해탐지시스템이 방화벽에 이은 차세대 보안 솔루션으로 부각되는 주된 이유는, 방화벽이 해킹 되었을 경우 이에 따른 피해를 최소화하고 네트워크 관리자 부재 시에 시스템 자체적으로도 해킹 등에 대응할 수 있는 보안 솔루션에 대한 요구가 늘고 있는 상황에서 침해탐지시스템이 이러한 요구를 해결할 수 있는 솔루션이기 때문이다

이러한 기존 정보보호 기술은 이미 발생한 침해를 탐지하여 피해의 확산을 막는 것에 주된 목표이며, 새로운 사이버 침해의 발생을 예측하지는 못한다. 그로 인해 기존에 발생한 사이버 침해와 다른 유형의 사이버 침해 발생할 경우 대응하기 힘들다는 문제점을 갖는다. 따라서 사이버 침해의 피해를 최소화하기 위해서는 발생시점에서 적용할 수 있는 정보보호 기술보다는 발생이전에 발생가능성을 미리 예측하여 대응하는 방법론적인 접근이 필요하다.

본 논문에서는 보안 취약점을 이용한 사이버 침해를 대상으로 전문가 설문을 통해 사이버 침해의 발생 가능성을 예측하는 방법을 제안하고, 이를 위한 사이버 침해 예측 항목을 추출하였다. 예측 항목 추출은 3 단계로 구성되며, 첫 번째 단계에서는 기존 연구와 사례 분석을 통해 예측 항목의 계층 구조를 생성한다. 두 번째 단계

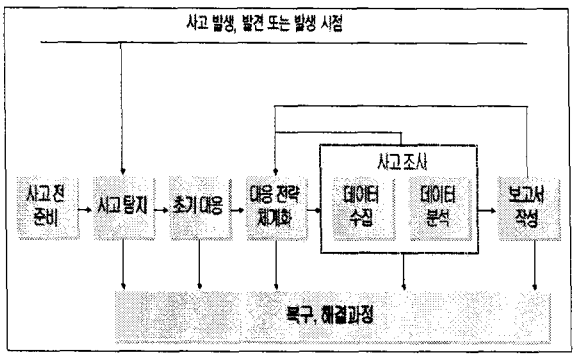
*** 이 논문은 2007년도 한국전자통신연구원 부설연구소의 지원을 받아 연구되었음(07024).

에서는 첫 번째 단계를 통해 생성된 예측 항목들을 델파이 방법을 통해 개선하여 최적의 예측 항목을 결정한다. 마지막 단계에서는 각 항목들에 대한 쌍대 비교 설문을 진행하여 항목 간 가중치를 추출한다.

2. 관련 연구

2.1 침해 사고 대응 단계

기존의 침해 사고 대응 단계에서 사이버 침해의 예측은 사고 탐지 단계에서 IDS를 비롯한 각종 네트워크 장비를 이용하여 현재 침해가 일어났는지를 예측함으로써 이루어졌다. 이러한 기존 방법은 기존의 정보보호 기술들이 가지는 문제점들 때문에 사이버 침해의 발생 자체를 예측하는 것 보다는 현재 발생한 사이버 침해의 피해를 최소화하고 이를 분석하여 향후 동일한 사고의 피해를 최소화하는 것에 한정되었다. 그러나 기존에 발생한 사이버 침해와는 새로운 사이버 침해가 발생할 경우 기존의 사이버 침해 예측 방법으로는 효과적인 대응을 하기 힘들다는 문제점이 있다.



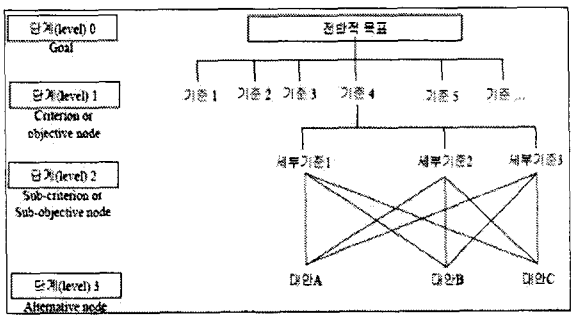
[그림 1] 침해 사고 대응 단계

2.2 보안 취약점 분류 체계

보안 취약점(vulnerability)은 시스템의 결점(weakness) 및 시스템의 비정상적인 수행을 유발할 수 있는 결함으로서 보안 취약점을 이용한 사이버 침해를 분류하는 방법은 시스템의 보안 취약점 위주로 분류하는 방법이 있으며 침해로 인한 영향, 위험성 등에 의해서도 분류하는 방법이 있다. 보안 취약점은 버그, 설계상의 결함(flaw), 프로그래머의 부주의, 바람직하지 못한 사용자 입력, 변수의 경계 검사의 실패 등으로부터 유발된다. 이러한 보안 취약점의 명확한 분류는 시스템 관리자들이 보안 취약점을 이해하고 이 취약점을 제거할 수 있는 지식을 제공할 수 있으며, 정보보호 제품 개발 및 평가에도 활용될 수 있다. 국외에서는 이미 이러한 취약점 분류에 대한 연구가 활발히 진행되고 있으며, 대표적으로 Aslam의 분류법, Landwehr의 분류법, Simon의 분류법 등이 있다 [3,4,5].

2.3 계층분석방법 (AHP : Analytic Hierarchy Process)

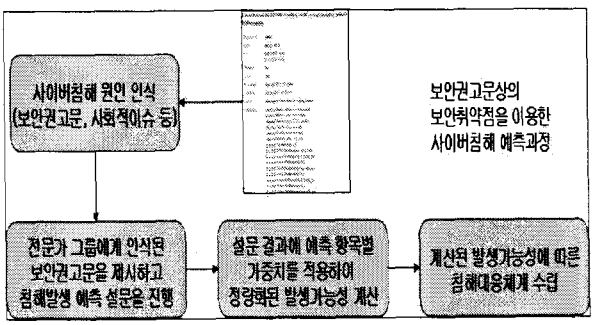
계층분석방법은 의사결정의 계층구조를 구성하고 있는 요소간의 쌍대비교를 통해 평가자의 지식, 경험 및 직관을 포착하는 의사결정방법론 중 하나이다[6]. 계층분석방법의 간략한 과정은 다음과 같다. 우선 직면한 의사결정 문제를 구성하고 있는 모든 요소를 나열한다. 그 요소로는 의사결정의 목적, 대안, 그 대안을 평가할 수 있는 기준 등이 있다. 이러한 요소들을 계층의 형태로 만든다. 이후 그 계층을 구성하고 있는 요소들 간에 1대1로 쌍대비교를 한다. 비교결과를 선형대수학의 고유 벡터 법을 이용하여 요소들의 가중치를 구한다. 마지막으로 각 레벨에서 구한 요소들의 가중치를 상위레벨에서 하위레벨로 곱하게 되면 의사결정대안의 최종가중치가 구해지고, 이를 토대로 의사결정을 내리게 된다.



[그림 2] AHP 계층 구조도

3. 전문가 의견 기반 사이버 침해 예측 과정

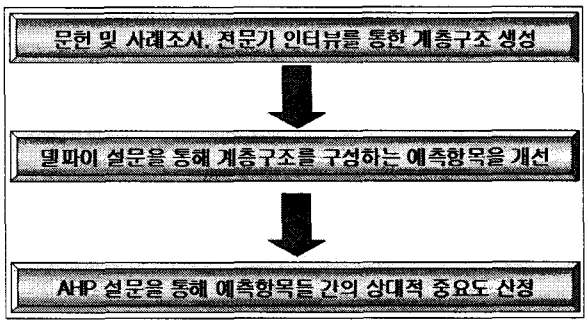
본 연구에서 제안하는 전문가 의견 기반 비정형 사이버 침해 예측 방법론은 기존의 침해 사고 대응 단계 중에서 '사고 전 준비 단계'에서 활용된다. 즉, 새로운 보안 권고문이 공지되었을 때 이 보안 권고문의 내용에 대해 예측항목에 따라 전문가들의 의견을 수집하여 침해 발생가능성을 정량화된 값으로 측정한다. 그리고 측정된 발생 가능성의 값에 따라 대응 체계를 변화시킴으로써 아직 발생하지 않은 사이버 침해에 대한 효과적인 대응이 이루어지도록 한다.



[그림 3] 전문가 의견 기반 사이버 침해 예측 과정

4. 사이버 침해 예측을 위한 주요 항목 추출

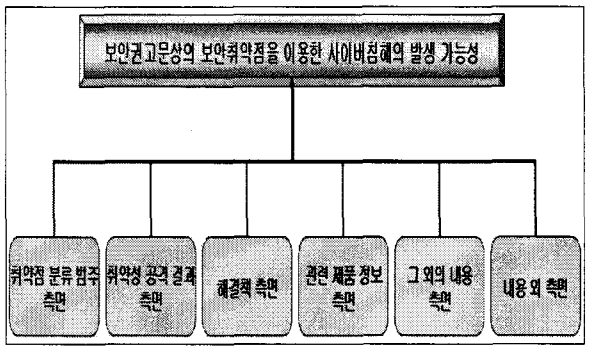
사이버 침해 예측을 위해 전문가를 대상으로 하는 설문을 실행하기 위해서는 먼저 전문가들에게 무엇을 물어보아야 하는 지가 정해져야 한다. 또한, 예측에 있어서 전문가들에게 물어보는 각각의 항목들이 가지는 중요도도 필요하다. 이러한 사이버 침해의 예측을 위한 주요항목 추출을 위해 본 논문에서는 계층분석방법을 기반으로 하는 전문가 의견을 반영한 예측 항목 추출 방법론을 적용하였다. 적용한 방법론은 3 단계로 진행되는데, 첫 번째 단계에서는 기존 연구와 사례 분석을 통해 예측 항목의 계층 구조를 생성한다. 두 번째 단계에서는 첫 번째 단계를 통해 생성된 예측 항목들을 델파이 방법을 통해 개선하여 최적의 예측 항목을 결정한다[7]. 마지막 단계에서는 각 항목들에 대한 쌍대 비교 설문을 진행하여 항목 간 가중치를 추출한다.



[그림 4] 사이버 침해 예측을 위한 주요 항목 추출 과정

4.1 초기 예측 항목 생성

기존의 보안 취약점 분류 체계에 관한 연구 내용을 바탕으로 보안 취약점의 내용을 취약점 분류 범주, 취약점 공격 결과, 해결책, 관련제품정보, 그 외의 내용으로 구분하여 이를 사이버 침해 발생 가능성 예측을 위한 상위 항목으로 선정하였다. 또한, 보안 취약점의 외적인 내용도 추가적인 상위 항목으로 포함하였다.



[그림 5] 상위 항목 계층 구조

그리고 기존 연구 및 전문가 인터뷰를 통해 각각의 상위 항목에 해당하는 하위 항목을 설정하였다[표 1].

[표 1] 초기 사이버 침해 예측 항목

상위 항목	하위 항목
취약점 분류 범주 측면	제시된 보안 권고문에 나타난 취약점의 분류 범주에 대한 Exploit 구현의 난이도
	제시된 보안 권고문에 나타난 취약점의 분류 범주에 해당하는 사이버침해의 경험 여부
취약성 공격 결과 측면	제시된 보안 권고문에 나타난 취약점의 공격 결과에 대한 주관적인 위험도
	공격결과를 통해 공격자가 얻게 될 것이라고 생각되는 가치의 양
해결책 측면	제시된 보안 권고문에 나타난 해결책의 적용 난이도
관련 제품 정보 측면	제시된 보안 권고문에 나타난 관련 제품군의 사용 여부
	관련 제품군들에 대해 업체에서 제공하는 보안 측면의 지원 서비스(취약점에 대한 안내 및 패치 제공 등)의 질
그 외의 내용 측면	보안 권고문에 표기된 위험도에 대한 동의 여부
	보안 권고문에서 충분한 참조정보가 제공되었는지 여부
내용 외적 측면	제시된 보안 권고문의 내용을 언론을 통해 접해본 적이 있는 지 여부
	제시된 보안 권고문의 내용과 유사성을 가지는 사이버침해 사례의 발생 빈도

4.2 델파이 설문을 통한 예측 항목의 개선

2007년 5월 22-24일 기간 동안에 정보보안전문가 9명을 대상으로 1차 설문을 진행하였다. 1차 설문에서는 각 항목에 대한 의견을 '선택', '수정', '삭제'로 구분하여 수집하였다. 여기서 '선택'은 설문 문항에 동의하는 의견이며, '수정'은 어느 정도 동의하나 수정이 필요하다는 의견이며, '삭제'는 설문 문항에 동의하지 않는다는 의견이다.

전반적으로 예측 항목에 대한 선택의 의견이 다수를 차지하였다. 추가 의견으로는 '제시된 보안 권고문에 나타난 해결책의 적용 난이도'와 관련해서 해결책 조치 시 발생할 수 있는 문제 및 해결책 조치 중 오류 가능성 등의 추가 항목이 필요하다는 의견, CVSS와 관련된 항목의 추가 의견, 관련제품정보와 관련된 추가 의견 등이 있었다. 그리고 가장 삭제 요구가 많았던 항목은 '제시된 보안 권고문의 내용을 언론을 통해 접해본 적이 있는 지 여부'로서 이미 언론을 통해 알려졌다면 사이버 침해가 발생한 것이기 때문에 예측에는 도움이 되지 않는다는 의견이 제시되었다[표 2].

[표 2] 사이버 침해 예측 항목 (1차 수정)

상위 항목	하위 항목
취약점 분류 범주 측면	제시된 보안 권고문에 나타난 취약점의 분류 범주에 대한 Exploit 구현의 난이도
	제시된 보안 권고문에 나타난 취약점의 분류 범주에 대한 Exploit의 반복적 사용가능성
	제시된 보안 권고문에 나타난 취약점의 분류 범주에 해당하는 사이버침해에 대한 직접적인 경험의 빈도
	제시된 보안 권고문에 나타난 취약점의 분류 범주에 해당하는 사이버침해에 대한 간접적인 경험의 빈도
취약성 공격 결과 측면	제시된 보안 권고문에 나타난 취약점의 공격 결과에 대해 생각되는 주관적인 위협도
	공격결과를 통해 공격자가 얻게 될 것이라고 생각되는 가치의 정도
해결책 측면	제시된 보안 권고문에 나타난 해결책이 전체 시스템에 영향을 주는 정도에 따른 적용 난이도
	제시된 보안 권고문에 나타난 해결책을 적용할 경우 시스템 장애 및 오류가 발생할 가능성
	제시된 보안 권고문에 나타난 해결책 생성 주체에 대한 주관적인 신뢰도
관련 제품 정보 측면	제시된 보안 권고문에 나타난 관련 제품군에 대해 알려져 있는 보급률의 정도
	관련 제품군들에 대해 개발 업체 및 유지보수 업체에서 제공하는 보안 업데이트 주기의 적절성
	관련 제품군들에 대해 개발 업체 및 유지보수 업체에서 제공하는 관련 정보 제공 빈도
	관련 제품군들의 오픈 소스 여부
	보안 권고문에 나타난 관련된 제품의 개발 업체에 대한 일반적인 사용자들이 갖는 부정적인 이미지의 정도
그 외의 내용 측면	보안 권고문에 CVSS에 따른 위험도를 제공하는 지 여부
	보안 권고문에 표기된 위험도(CVSS 등)를 기반으로 추정한 주관적인 위험도
	보안 권고문에서 충분한 참조정보가 제공되었는지 여부
내용 외 측면	제시된 보안 권고문의 내용과 침해분류범주 측면과 공격결과 측면 및 관련제품정보 측면에서 유사성을 가진다고 생각되는 사이버침해 사례의 발생 빈도
	보안 권고문과 관련된 침해 사례를 언론(뉴스, 신문, TV 등)을 통해 접해본 적이 있는지 여부

이러한 1차 설문 결과를 통해 수정된 예측항목들에 대해 2007년 7월 9-13일 기간 동안에 정보보안전문가 14명을 대상으로 2차 설문을 진행하였다. 2차 설문에서는 각 항목에 대한 의견을 '적극 찬성', '찬성', '반대하지 않음', '반대', '적극 반대'로 구분하여 설문에 응하는 전문가의 의견의 강도를 반영하였다.

2차 조사의 결과는 전반적으로 예측항목들에 대한 긍정으로 기울어져 있는 경향을 보였다. 이러한 경향으로 인해 무시될 수 있는 소수의 반대 의견들을 반영하기 위해 평균값에 대한 비율에 의견의 긍정도에 따른 차등화된 점수를 적용하여 각각의 항목에 대한 의견을 점수화하였다. 점수화한 결과, '보안 권고문에 나타난 관련된 제품의 개발업체에 대한 일반적인 사용자들이 갖는 부정적인 이미지의 정도'와 '보안 권고문과 관련된 침해 사례를 언론(뉴스, 신문, TV 등)을 통해 접해본 적이 있는 지 여부'등이 비교적 부정적인 의견이 많았기 때문에 값이 음수로 나온 것을 확인하여 삭제할 항목으로 선택하였다.

그 외에도, 예측 항목들에 대한 정량화된 측정 기준에 대한 요구 의견이 있었으나, 이는 도출된 예측항목들을 적용한 설문과정에서 설문 대상이 되는 전문가들의 특성 정보 및 각종 통계 정보를 바탕으로 점차적으로 개선해 나가야 할 부분으로서 3차 설문에 반영해야 할 내용은 아니라고 판단하였다. 단, 측정하기 모호한 수식어가 사용된 항목들에 대한 수정의견은 받아들여 이를 3차 설문에 반영하였다[표 3].

[표 3] 사이버 침해 예측 항목 (2차 수정)

상위 항목	하위 항목
취약점 분류범주 측면	제시된 보안 권고문에 나타난 취약점의 분류 범주에 대한 Exploit 구현의 난이도
	제시된 보안 권고문에 나타난 취약점의 분류 범주에 대한 Exploit의 반복적 사용가능성
	제시된 보안 권고문에 나타난 취약점의 분류 범주에 해당하는 사이버침해에 대한 직·간접적인 경험의 빈도
취약점 공격결과 측면	제시된 보안 권고문에 나타난 취약점의 공격 결과에 대해 생각되는 주관적인 위협도
	공격결과를 통해 공격자가 얻게 될 것이라고 생각되는 가치의 정도
해결책 측면	제시된 보안 권고문에 나타난 해결책이 전체 시스템에 영향을 주는 정도에 따른 적용 난이도
	제시된 보안 권고문에 나타난 해결책을 적용할 경우 시스템 장애 및 오류가 발생할 가능성
	제시된 보안 권고문에 나타난 해결책 생성 주체에 대한 주관적인 신뢰도
관련제품 정보 측면	제시된 보안 권고문에 나타난 관련 제품군에 대해 알려져 있는 보급률의 정도
	관련 제품군들에 대해 개발 업체 및 유지보수 업체에서 제공하는 보안 업데이트 주기의 적절성
	관련 제품군들에 대해 개발 업체 및 유지보수 업체에서 제공하는 관련 정보 제공 빈도
	관련 제품군들의 오픈 소스 여부
그 외의 내용 측면	보안 권고문에 CVSS에 따른 위험도를 제공하는 지 여부
	보안 권고문에 표기된 위험도(CVSS 등)를 기반으로 추정한 주관적인 위험도
	보안 권고문에서 충분한 참조정보가 제공되었는지 여부
내용 외적 측면	제시된 보안 권고문의 내용과 침해분류범주 측면과 공격결과 측면 및 관련제품정보 측면에서 유사성을 가진다고 생각되는 사이버침해 사례의 발생 빈도

4.3 AHP 설문을 통한 예측 항목 가중치 산정

2007년 7월 23-27일 기간 동안에 정보보안전문가 14명을 대상으로 전문가 의견조사 설문지에 대한 3차 설문을 실시하였다. 3차 설문은 1·2차 설문을 통하여 도출된 사이버침해 예측을 위한 항목들 간의 상대적 중요성

(relative importance)을 측정하기 위한 것으로 설문의 결과는 AHP 분석 도구인 Expert Choice 2000 프로그램을 이용하여 분석하였다.

분석을 위해 AHP의 비일관성 지수(inconsistency index)가 0.1이하인 전문가의 응답들의 평균값을 개별 항목의 최종 중요도로 산출하였다. 분석의 결과에 따르면 전문가들은 '공격결과 측면'이 0.32 정도로 사이버 침해 발생에 있어서 가장 영향을 주는 것으로 보여주었다. 다음으로 '해결책 측면'(0.22)이 영향을 미치는 것으로 나타났다. 이 외에도 '관련제품정보 측면'(0.19), '분류범주 측면'(0.14), '내용 외적 측면'(0.07), '그 외의 내용 측면'(0.06)의 순서로 상대적 중요도를 갖는 것으로 나타났다. 그 외의 하위 항목에 대한 가중치는 아래의 [표 4]와 같다.

[표 4] 사이버 침해 예측 항목 및 가중치

상위 항목	하위 항목
취약점 분류범주 측면 (0.14)	제시된 보안 권고문에 나타난 취약점의 분류 범주에 대한 Exploit 구현의 난이도 (0.46)
	제시된 보안 권고문에 나타난 취약점의 분류 범주에 대한 Exploit의 반복적 사용가능성 (0.34)
	제시된 보안 권고문에 나타난 취약점의 분류 범주에 해당하는 사이버침해에 대한 직·간접적인 경험의 빈도 (0.20)
취약점 공격결과 측면 (0.32)	제시된 보안 권고문에 나타난 취약점의 공격 결과에 대해 생각되는 주관적인 위협도 (0.55)
	공격결과를 통해 공격자가 얻게 될 것이라고 생각되는 가치의 정도 (0.45)
해결책 측면 (0.22)	제시된 보안 권고문에 나타난 해결책이 전체 시스템에 영향을 주는 정도에 따른 적용 난이도(0.43)
	제시된 보안 권고문에 나타난 해결책을 적용할 경우 시스템 장애 및 오류가 발생할 가능성 (0.29)
	제시된 보안 권고문에 나타난 해결책 생성 주체에 대한 주관적인 신뢰도 (0.28)
관련제품 정보 측면 (0.19)	제시된 보안 권고문에 나타난 관련 제품군에 대해 알려져 있는 보급률의 정도 (0.50)
	관련 제품군들에 대해 개발 업체 및 유지보수 업체에서 제공하는 보안 업데이트 주기의 적절성 (0.25)
	관련 제품군들에 대해 개발 업체 및 유지보수 업체에서 제공하는 관련 정보 제공 빈도 (0.16)
	관련 제품군들의 오픈 소스 여부 (0.09)
그 외의 내용 측면 (0.06)	보안 권고문에 CVSS에 따른 위험도를 제공하는 지 여부 (0.41)
	보안 권고문에 표기된 위험도(CVSS 등)를 기반으로 추정한 주관적인 위험도 (0.49)
	보안 권고문에서 충분한 참조정보가 제공되었는지 여부 (0.20)
내용 외적 측면 (0.07)	제시된 보안 권고문의 내용과 침해분류범주 측면과 공격결과 측면 및 관련제품정보 측면에서 유사성을 가진다고 생각되는 사이버침해 사례의 발생 빈도

4.4 사이버 침해 발생 가능성 예측의 예제

지금까지 보안 취약점을 이용한 사이버 침해를 예측하기 위한 주요 항목과 이들의 상대적 중요도를 확인하였다. 그렇다면 어떤 식으로 예측이 가능한지를 가상의 예를 들어서 설명하고자 한다. 우선, 상위 항목의 최고 점수를 1로 정한다. 그리고 개별 항목의 점수는 연구자가 정한 5개의 수준에 따라서 0, 0.25, 0.5, 0.75, 1점을 부여하는 것으로 한다. 예를 들어 '분류범주 측면'에 해당하는 항목인 '제시된 보안 권고문에 나타난 취약점의 분류 범주에 해당하는 사이버침해에 대한 직·간접적인 경험의 빈도'에서 설문에 응한 전문가가 경험한 사이버 침해의 빈도가 6이고, 빈도 값이 5이상~10미만인 경우에 대하여 0.5라고 점수를 주기로 정했다면 이 항목의 점수는 0.5가 된다.

위의 과정을 통해 개별 항목의 점수가 결정된 후에는 각각의 세부항목별 가중치를 적용하여 상위항목의 점수를 계산한다. 예를 들어 '분류범주 측면'의 세부항목인 ' 제시된 보안 권고문에 나타난 취약점의 분류 범주에 대한 Exploit 구현의 난이도'와 '제시된 보안 권고문에 나타난 취약점의 분류 범주에 대한 Exploit의 반복적 사용가능성', '제시된 보안 권고문에 나타난 취약점의 분류 범주에 해당하는 사이버침해에 대한 직·간접적인 경험의 빈도'의 점수가 각각 0.25, 0.75, 0.5이고, 이 들의 가중치가 0.46, 0.34, 0.20이라고 하자. 이 경우에 '분류범주 측면'의 점수는 각 세부항목의 점수에 가중치를 곱한 값의 합인 0.47(=0.25*0.46+0.75*0.34+0.5*0.20)이 된다. 이러한 과정을 통해 모든 상위항목의 점수가 결정된 후에는 각각의 상위항목 가중치를 곱하여 전체의 합을 구하는 것으로 발생가능성을 계산할 수 있다.

5. 결론 및 향후 연구

본 연구에서 제안하는 전문가 의견 기반 사이버 침해 예측 방법론은 기존의 침해 사고 대응 단계에서 사고 전 준비 단계에 대해 적용하여 발생 가능성에 따라 대응 체계를 변화시킴으로써 효과적인 침해 대응이 이루어지도록 한다. 이를 위해 본 연구에서는 사이버 침해의 예측을 위한 주요항목 추출을 위해 전문가 의견을 반영한 예측 항목 추출 방법론을 적용하였다. 적용한 방법론에서는 전문가들을 대상으로 델파이 방법과 계층분석방법을 통해 사이버 침해의 예측을 위한 주요항목을 추출하고, 이러한 항목들을 활용하기 위한 항목 간 가중치를 추출하였다.

본 연구의 결과로 생성된 사이버 침해 예측을 위한 주요 항목과 항목 간 가중치를 실제 전문가 예측 설문에 활용하기 위해서는 각 항목의 값을 측정하기 위한 명확한 기준에 대한 연구가 필요하다. 또한, 보다 정확한 발생 가능성 예측을 위해 발생할 것이라고 예측되는 사이버 침해와 유사한 기존의 사이버 침해 사례를 분석하여 활용하기 위한 방법에 대한 연구와 기존의 사이버 침해 사례를 기계학습 방법을 이용해 학습한 결과를 사이버 침해 발생 가능성 예측에 활용함으로써 예측 정확성을 높이는 연구 등이 추가적으로 필요할 것으로 생각된다.

6. 참조 문헌

[1] 한국정보보호진흥원, 침해사고 분석 절차 가이드, 2006.
[2] 국가사이버안전센터, 2005년도 사이버 침해 사고 사례집, 2005.
[3] Taimur Aslam, Ivan Krsul, Eugene H. Spafford, "Use of A Taxonomy of Security Faults", 19th NIST - NCSC, 1996
[4] Carl E. Landwehr, Alan R. Bull, John P. Mcdermott, William S. Choi, "A Taxnomy of Computer Program Secrurity Flaws", ACM Vol.26, No.3, 1994
[5] Simon Hansman, Ray Hunt, "A Taxonomy of network and computer attacks", Computers & Security, 2004
[6] 조근태, 조용곤, 강현수, "앞서가는 리더들의 계층분석적 의사결정", 2003
[7] 이종성, "델파이 방법", 2001