情報保護學會論文誌
第 22 卷 第 5 號, 2012. 10

AHP를 이용한 VoIP 정보보호 점검항목의 중요도 분석

윤 석 웅,[1†] 박 해 룡,[1] 유 형 선[2‡]
[1]한국인터넷진흥원, [2]인하대학교

Factor analysis of VoIP Security Checklists using AHP

Seokung Yoon,[1†] Haeryong Park,[1] Hyeong Seon Yoo[2‡]
[1]Korea Internet & Security Agency, [2]Inha University

요 약

스마트 단말 확산, 네트워크 고도화 및 다양한 인터넷전화용 앱의 등장으로 국내 인터넷전화 시장은 지속적으로 성장하고 있다. 그러나 인터넷전화는 인터넷을 기반으로 제공되고 있어, 기존 인터넷의 보안위협 뿐만 아니라 VoIP 프로토콜 적용에 따른 보안 위협이 존재한다. 본 연구는 VoIP 사업자가 침해사고 예방 및 대응을 위해 자율적으로 점검할 수 있는 정보보호 점검항목의 중요도를 AHP(Analytic Hierarchy Process)를 이용하여 파악한다. AHP 분석 결과, 기술적 보안에서는 네트워크 보안이, 관리적 보안에서는 침해사고 대응이, 물리적 보안에서는 출입 및 접근 보안이 가장 중요한 항목으로 나타났다. 본 연구는 VoIP 점검항목의 중요도를 최초로 제시함으로써, VoIP 사업자들이 보안정책 수립하고 이 정책에 따라 점검을 하는데 유용하게 이용될 수 있을 것이다.

ABSTRACT

VoIP service is steadily growing due to the spread of smartphones, enhanced network, and various VoIP applications. But, VoIP has many security vulnerabilities because it is based on IP network. This paper analyzes the important weight of VoIP security checklists for incident prevention and response using AHP. The results of AHP analysis showed that network security, incident response, and access control were the most important in technical, administrative, physical standpoint. This study proposes factor analysis of VoIP security checklist at first time. By doing this, it will be used helpfully when VoIP service providers establish their own security policies and inspect their VoIP environment according to their security policies.

Keywords: VoIP, AHP, VoIP Security Checklists

I. 서 론

국내 인터넷전화(VoIP)는 저렴한 요금, 다양한 정부의 활성화 정책으로 인해 가입자수가 2012년 현재 1,100만명을 넘어서며 지속적으로 성장하고 있다. 최근에는 스마트폰 확산, 4G 네트워크 도입으로 인해 모바일 인터넷전화도 급속한 성장이 예상되고 있다. 그러나 인터넷전화는 인터넷을 기반으로 하고 있어 기존 인터넷의 위협뿐만 아니라 인터넷전화 프로토콜 사용으로 인한 보안위협에 노출되어 있다. 또한 무선네트워크 환경이 확대되고 스마트폰 사용이 늘어나면서 스마트폰 악성코드 감염 등으로 인한 침해사고의 우려 또한 제기되고 있다.

이러한 인터넷전화 보안위협에 대응하고자 그간 방송통신위원회와 한국인터넷진흥원에서는 VoIP 정보보호 가이드라인('07) 및 VoIP 침해사고 대응안내서('10) 개발하여 보급하고 있다[1-2]. VoIP 정보보호 가이드라인에는 부록에 총 130개의 기술적, 관리적

접수일(2012년 4월 18일), 수정일(1차: 2012년 8월 10일, 2차: 2012년 9월 27일), 게재확정일(2012년 9월 27일)
† 주저자, seokung@kisa.or.kr
‡ 교신저자, hsyoo@inha.ac.kr

점검항목을 마련하여 사업자 스스로 가이드라인에서 명시한 정보보호 대책 적용여부를 점검할 수 있도록 하였다. 또한 VoIP 정보보호 가이드라인에서 제시한 총 130개의 점검항목 중, VoIP 사업자 및 보안전문가의 자문을 거쳐 VoIP 사업자가 침해사고를 예방하기 위해 필수적인 총 50개의 기술적·관리적·물리적 점검항목을 VoIP 침해사고 대응안내서에 포함시켰다.

최근 기업들을 대상으로 지속적으로 발생한 침해사고로 인한 경제적·사회적 손실을 감안할 때, 1,100만명 이상이 사용하고 있는 국내 인터넷전화에서도 침해사고가 발생할 경우 그 피해는 엄청날 것으로 예측되고 있다. 따라서 VoIP 사업자들의 침해사고 예방을 위한 다양한 대책 마련이 요구되고 있는 가운데 본 연구는 침해사고 예방을 위한 점검항목의 우선순위를 처음으로 제시함으로써 사업자가 점검항목의 우선순위에 따라 보안정책을 세우고 선택적으로 점검을 할 수 있도록 하였다.

본 연구에서는 점검항목의 우선순위 도출에 필요한 가중치 산출방식을 현재 가장 많이 사용하고 있는 방식 중 하나인 계층 분석 기법(AHP, Analytic Hierarch Process)방법을 선택하였다. AHP는 의사결정의 계층구조를 구성하고 있는 요소간의 쌍대비교를 통해 평가자의 지식, 경험 및 직관을 포착하는 의사결정방법론 중 하나이다. 또한 AHP는 쌍대비교의 일관성 검정을 통해 응답자의 응답일관성을 검토할 수 있다는 장점으로 인해 최종적인 분석결과에 대해 타당성을 부여할 수 있어 의사결정 문제에 널리 활용되어지고 있다[3].

본 논문은 다음과 같이 구성되어 있다. 제 2장에서는 본 연구의 배경이 되는 VoIP에 대한 소개와 관련 선행연구를 살펴본다. 제 3장은 AHP 활용을 위한 연구모형을 설정하고 제 4장에서는 이를 이용하여 자료를 분석함으로써 점검항목의 우선순위를 살펴본다. 마지막으로 제 5장에서는 결론을 맺는다.

II. 이론적 배경

2.1 인터넷전화(VoIP)

VoIP란 인터넷망을 이용해 음성을 비롯한 다양한 부가서비스를 제공하는 서비스로, 2008년에 번호 이동성 제도 실시 이후에 급속히 성장하여 2012년 현재 가입자 1,100만을 돌파한 보편적인 서비스이다. 최근에는 모바일 인터넷전화, VoLTE(Voice over LTE)로 인해 사용이 지속적으로 증가할 것으로 예상되고 있다.

〔표 1〕 VoiP 보안위협

구분	내용
도청	VoIP 사용자간의 통화내용을 불법적으로 수집하여 재생하는 공격
서비스 거부공격	VoIP 주요시스템에 대한 자원을 고갈시켜 시스템이 서비스를 제공하지 못하도록 하는 공격
서비스 불법사용	인증 받지 않은 사용자가 VoIP 시스템을 해킹 등 불법적으로 이용하는 공격
VoIP 스팸	자동화된 도구를 이용하여 불특정 다수에게 원치 않는 VoIP 스팸을 전송

인터넷전화는 인터넷을 기반으로 서비스를 제공하고 있어 기존 인터넷의 보안위협을 상속받으며, 인터넷전화 프로토콜 사용으로 인한 보안위협이 공존하고 있다. 아울러 상대적으로 보안에 취약한 무선네트워크에서의 사용 확산으로 인해 보안 사고의 우려가 높아지고 있다. 실제로 2008년부터 인터넷전화를 대상으로 하는 다양한 침해사고가 언론을 통해 발표되고 있으며, 이에 따른 대응방법에 대한 연구도 활발하게 진행되고 있다[4-5]. 방송통신위원회와 한국인터넷진흥원에서 제공한 VoIP 정보보호 가이드라인에서는 VoIP 서비스 환경에서 발생 가능한 보안위협을 〔표 1〕과 같이 제시하고 있다[1].

2.2 VoIP 정보보호 점검항목

VoIP 보안위협에 대응하기 위해서는 무엇보다도 VoIP 사업자가 보안정책을 세우고 보안정책에 따라 보안활동을 지속적으로 해야 한다. 이를 위해서는 VoIP 사업자 스스로 자사의 정보보호 수준을 점검할 수 있는 항목이 마련되어야 하고, 이를 기반으로 주기적으로 서비스를 점검하여 문제가 발생할 부분을 사전에 발견하여 제거하는 것이 무엇보다도 중요하다. 이를 위해 방송통신위원회와 한국인터넷진흥원은 2006년부터 산·학·연·관 전문가로 구성된 작업반을 통해 VoIP 정보보호 가이드라인(2007.10)을 개발하였고, 총 130개의 기술적·관리적·물리적 점검사항을 마련하였다.

그러나 2009년부터 VoIP 서비스 대상 침해사고가 현실화됨에 따라 VoIP 침해사고가 발생했을 경우 피해 최소화를 위한 대응방안 마련이 필요하게 되었고 2010년 다시 산·학·연·관 전문가들이 모여 VoIP

침해사고 대응안내서(2010.12)를 발간하게 되었다. VoIP 침해사고 대응안내서에는 침해사고의 예방 측면에서 VoIP 사업자들이 반드시 점검해야 할 50개의 항목을 마련하였다. 50개의 점검항목은 기술, 관리, 물리 3개의 대분류로 구성되어 있으며, 기술적 대분류 안에는 4개의 중분류와 23개의 점검항목으로 구성되어 있다. 관리적 대분류 안에는 7개의 중분류 및 21개의 점검항목으로 구성되어 있으며, 물리적 대분류에는 3개의 중분류 및 6개의 점검항목으로 구성되어 있으며 상세한 내용은 〔표 2〕와 같다. 이 중에서 기술적,

〔표 2〕 계층도별 평가항목에 대한 정의

구분		점검항목	참고
1. 기술적 보안	1-1 네트워크 보안	1-1-1. VoIP 트래픽 모니터링 시스템 운영 1-1-2. VoIP 보안장비들에 대한 통합 관리 시스템 운영 1-1-3. VoIP 네트워크에 악의적 공격 탐지 기술 적용 1-1-4. 장애에 대비한 우회경로 확보 1-1-5. DoS/DDoS 공격 대응기술 적용 1-1-6. 음성망과 데이터망 분리 1-1-7. VoIP 단말 및 장비 접근제어 1-1-8. 도청방지를 위한 기술적 대책 적용 1-1-9 VoIP 스팸대응 시스템 운영	VoIP 정보보호 가이드라인〔1〕
	1-2 단말보안	1-2-1. 단말 펌웨어 및 전용 어플리케이션의 주기적으로 갱신 1-2-2. 사용자가 단말의 ID/PW 변경 1-2-3. 제어메시지 및 통화내용 암호화 1-2-4. 원격 접속시, 암호화 혹은 접속채널 보호기술 적용 1-2-5. 단말 내 스팸차단을 위한 Blacklist 관리기능 제공	
	1-3 VoIP 설비보안	1-3-1. 백도어 및 불필요한 서비스가 활성화 여부 점검 1-3-2. VoIP 교환장비의 전용사용 1-3-3. 사용자 및 단말을 인증할 수 있는 인증 매커니즘 적용 1-3-4. 관리자 계정의 default password 변경 1-3-5. 운영자, 시스템, 이상 징후 등에 대한 로그 관리 1-3-6. 장비의 주기적인 보안패치 1-3-7. 제어메시지 및 음성데이터 암호화기능	
	1-4 사용자 정보보호	1-4-1. 개인정보저장 및 전송 시 암호화 1-4-2. 개인정보 DB 접근통제	
2. 관리적 보안	2.1 정보보호조직의 구성·운영	2-1-1. 정보보호조직 운영 2-1-2. 정보보호 총괄책임자 지정 2-1-3. 인터넷전화 정보보호 책임자 지정 2-1-4. 인터넷전화 정보보호 관리자 지정 2-1-5. 인터넷전화 정보보호 실무담당자 지정	정보보호 안전진단 해설서〔10〕
	2.2 정보보호계획 등의 수립 및 관리	2-2-1. 정보보호 방침(policy) 수립 2-2-2. 최고경영층(임원급이상) 승인 2-2-3. 정보보호방침을 토대로 당해 연도의 정보보호 실행계획 수립 2-2-4. 정보보호책임자의 정보보호 실행계획 점검 2-2-5. 정보보호 실무지침 마련 2-2-6. 정보보호 책임자가 실무지침을 승인 및 관리	
	2.3 인적보안	2-3-1. 전보 또는 퇴직자의 계정 제거 2-3-2. 정보보호인식 제고 활동 2-3-3. 정기적인 정보보호교육 실시 2-3-4. 외부직원에 대한 보안서약 징구 2-3-5. 전산업무 외부 위탁 방침 마련	
	2.4 이용자 보호	2-4-1. 정보보호관련 정보의 지속적인 제공	
	2.5 침해사고대응	2-5-1. 침해사고 대응계획 마련·시행	
	2.6 정보보호조치점검	2-6-1. 자체적인 정보보호 현황 점검	
	2.7 정보자산관리	2-7-1. VoIP 망구성도 보완·관리	
		2-7-2. VoIP 설비 및 시설의 목록 관리	
3. 물리적 보안	3.1 출입 및 접근보안	3-1-1. 잠금장치 설치 3-1-2. 출입기록 1개월 이상 유지·보관	VoIP 정보보호 가이드라인〔1〕
	3.2 부대설비 및 시설 운영·관리	3-2-1. 백업설비 및 시설 설치·운영	
	3.3 기타	3-3-1. VoIP 시스템 보안대책 마련 3-3-2. 매체 폐기 시, 저장된 정보의 안전한 삭제 3-3-3. 개인정보 DB 폐기 시, 물리적 파괴	

물리적 점검항목은 VoIP 가이드라인에 언급되어 있는 항목들 중 사업자의 설문을 거쳐 우선순위가 높은 항목을 선별하였으며, 관리적 점검항목은 "정보통신망 이용촉진 및 정보보호 등에 관한 법률" 제46조의3(정보보호 안전진단)에서 명시하고 있는 항목을 준용하였다. 이는 사업자가 법으로 정한 최소한의 보호조치를 이행함으로써 VoIP 침해사고를 예방하려는데 그 목적이 있다.

2.3 계층분석기법(AHP)

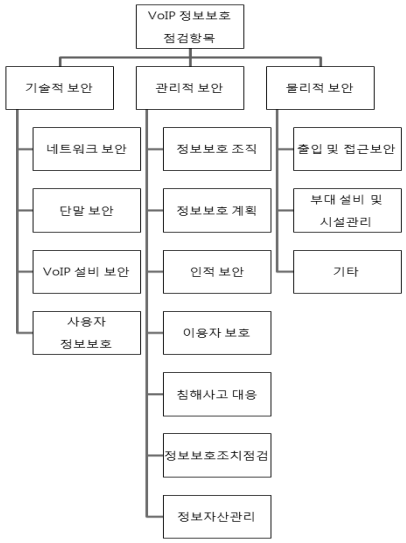
Saaty에 의해서 1970년대 초반에 개발된 AHP기법은 의사결정과정을 단순화시킴으로써 복잡한 문제에 대하여 효과적인 의사결정을 할 수 있도록 도와준다[6]. AHP의 특성은 기준에 대한 절대평가가 아니라 쌍 비교(pairwise comparison)를 통한 평가자의 일관성 있는 판단을 근거로 정량적인 요소와 정성적인 요소를 동시에 고려함으로써 의사결정 문제의 해결을 위한 포괄적인 틀을 제공해 준다는 점이다[7]. 이러한 장점으로 인해 다양한 정보보호 지표의 중요도를 판별하는데 널리 활용되고 있으며, 본 논문에서도 가중치를 결정하는 방법으로 사용하였다[8-9].

AHP 기법의 절차를 보면 첫째, 측정하고자 하는 사항을 계층제적 구조 하에 배열한다. 대체적으로 목표, 영역 또는 기준, 그리고 요소나 대안 등을 계층화시킨다. 이 때, 목표-영역-요소로 계층을 구성함에 있어서 점차 작은 요소로 분해한다. 둘째, 계층별 상대비교를 수행한다. 셋째, 상대비교행렬로부터 고유치방법(Eigenvalues Method)을 사용하여 각 계층내의 의사결정요소의 상대적 중요도를 추정한다. 마지막으로 일관성 검증을 수행한다. 본 연구에서 쌍대비교를 위한 설문항목의 예시는 [표 3]과 같다.

III. AHP 모형설계

AHP 적용절차의 첫 단계는 평가하고자 하는 요인과 그와 관련된 항목을 설정하고 평가 항목에 대한 기준을 확실히 규정하는 것이다[11]. 본 연구에서는 VoIP 정보보호 가이드라인에 수록된 점검항목을 기반으로 VoIP 사업자 및 정보보호 전문가와의 토론을 통해 VoIP 정보보호 점검항목을 도출하였다. VoIP 정보보호 점검항목은 기술적·관리적·물리적으로 구분되며 총 50개의 항목이 존재한다. 이에 대한 AHP 모형은 [그림 1]과 같다.

가중치 설문 항목은 VoIP 정보보호 점검항목들의 계층구조에 맞게끔 대분류, 중분류로 구분하여 평가항목을 쌍대비교(Pairwise)방식으로 구성하였다. 1문항에서는 응답자의 신원정보를, 2문항에서는 VoIP 정검항목의 대분류인 기술적·관리적·물리적 요인에



[그림 1] VoIP 정보보호 점검항목 중요도 산출을 위한 AHP 모형

[표 3] VoIP 정보보호 점검항목에 대한 쌍대비교 설문항목 예시

순번	조사 영역 A	평가척도																	조사 영역 B
		〉 (A가 B보다 중요)								=	〈 (B가 A보다 중요)								
		극히 중요		매우 중요		중요		약간 중요		동등		약간 중요		중요		매우 중요		극히 중요	
1	기술적 보안	⑨	⑧	⑦	⑥	⑤	④	③	②	①	②	③	④	⑤	⑥	⑦	⑧	⑨	관리적 보안
2	기술적 보안	⑨	⑧	⑦	⑥	⑤	④	③	②	①	②	③	④	⑤	⑥	⑦	⑧	⑨	물리적 보안
3	관리적 보안	⑨	⑧	⑦	⑥	⑤	④	③	②	①	②	③	④	⑤	⑥	⑦	⑧	⑨	물리적 보안

대한 상대비교 문항을 배열하였으며, 3문항에서 4문항까지는 중분류 및 점검항목에 대한 상대비교 문항을 배열하였다.

IV. 분석 결과

3장에서 제시한 AHP 모형을 기반으로 2012년 2월 15일부터 29일까지 약 2주일간 온라인을 통해 10명을 대상으로 1차 설문조사를 수행하였으며, 표본집단의 크기를 객관성을 확보할 수 있도록 7월 말에 약 1주일간 온라인을 통해 5명을 추가하여 2차 설문조사를 수행하였다. 따라서 총 15명(VoIP 사업자 10명, 정보보호 전문가 5명)을 대상으로 설문조사를 실시하였으며, 응답의 신뢰성을 높이기 위해 인터넷전화와 관련된 전문적 지식을 보유한 인터넷전화 사업자의 보안담당자 및 인터넷전화 관련 보안컨설팅을 수행한 경험이 있는 전문가로 한정하였다. 직급별로 살펴보면 부장급 3명, 과장급 8명, 대리급 4명이다. AHP기법 적용이 필요한 문제에 있어서 실무 지식과 전문적 경험이 있을 경우 표본크기가 10명~15명 내외인 것으로 알려졌다[11].

4.1 AHP 일관성 검증

AHP에서 사용되는 데이터는 설문응답자의 이해부족, 무성의 등의 이유로 일관성이 결여될 수 있기 때문에 일관성 검증을 수행해야 한다. 일관성 검증은 일관성 지수(Consistency Index: C.I.)를 경험적 자료로 얻어진 난수지수(Random Index)로 나눈 일관성 비율(Consistency Ratio: C.R.)로 설문응답에 대한 일관성을 검증하며, C.R. ≤ 0.1 일때만 신뢰성이 있다고 판단한다[12-13]. VoIP 점검항목의 각 계층별 CR값은 [표 5]와 같이 Saaty가 제시한 0.1보다 낮은 수치로, 높은 일관성을 가지고 있는 것으로 나타났다.

[표 4] 조사대상자 집단

구분		빈 도	
		인원(명)	백분율(%)
성별	남	15	100
	여	0	0
직종	VoIP 사업자	10	66.7
	보안전문가	5	33.3
직급	부장	3	20
	과장	8	53.3
	대리	4	26.7

[표 5] 일관성 비율

구분		CR값
전체		0.018
대분류	기술적	0.015
	관리적	0.091
	물리적	0.046

4.2 가중치 분석

본 연구에서는 중요도 평가를 15명의 전문가가 개별적으로 중요도를 평가한 후 통합하는 방법을 사용하였으며, 15 명의 전문가의 의견을 기하평균(Geometric mean)을 사용하여 중요도를 산출하였다[14]. VoIP 정보보호 점검항목의 상대적 중요도 및 우선순위는 [표 6]과 같다.

VoIP 점검항목의 대분류에서 상대적 중요도는 기술적 보안(0.424), 관리적 보안(0.376), 물리적 보안(0.200) 순으로 나타났다. 기술적 보안의 세부 요인에 대한 상대적 중요도는 네트워크보안(0.304), VoIP 설비보안(0.269), 사용자 정보보호(0.231), 단말보안(0.196)으로 나타났다. 각 중분류별 가장 중요한 우선순위를 갖는 점검항목을 살펴보면 네트워크 보안에서는 "VoIP 트래픽 모니터링 시스템 운영", "VoIP 단말 및 장비 접근제어"가, VoIP 설비보안에서는 "관리자 계정의 default password 변경"이, 사용자 정보보호에서는 "개인정보저장 및 전송 시 암호화"가 마지막 단말보안에서는 "원격 접속시, 암호화 혹은 접속채널 보호기술 적용"이다. 이는 최근 언론상에서 자주 소개되었던 취약한 VoIP 사업자의 교환기를 통해 발생했던 국제전화 과금사고를 방지할 수 있는 항목이기 때문에 이와 같은 결과가 나온 것으로 판단된다. 아울러 우선순위가 가장 낮은 항목들을 살펴보면 VoIP 스팸같이 보안 위협이 아직 현실화되지 않았거나 투자비용 대비 효과가 미비하여 상대적으로 중요도가 낮은 것으로 판단된다.

관리적 보안의 세부 요인에 대한 상대적 중요도 및 가장 중요한 우선순위를 갖는 점검항목을 살펴보면 침해사고 대응(0.156)-"침해사고 대응계획 마련・시행", 정보보호계획 등의 수립 및 관리(0.148)-"정보보호 방침(policy) 수립", 인적보안(0.145)-"전보 또는 퇴직자의 계정 제거", 정보보호 조치 점검(0.142)-"자체적인 정보보호 현황 점검", 정보보호 조직의 구성・

〔표 6〕 VoIP 점검항목별 상대적 중요도와 우선순위

대분류	상대적 중요도	중분류	상대적 중요도	평가항목	상대적 중요도
기술적 보안	**0.424 (1)**	**네트워크 보안**	**0.304(1)**	**1-1-1**	**0.132 (1)**
				1-1-2	0.098 (7)
				1-1-3	0.108 (5)
				1-1-4	0.106 (6)
				1-1-5	0.124 (3)
				1-1-6	0.098 (7)
				1-1-7	**0.132 (1)**
				1-1-8	0.119 (4)
				1-1-9	0.083 (9)
		단말보안	0.196 (4)	1-2-1	0.198 (3)
				1-2-2	0.202 (2)
				1-2-3	0.191 (4)
				1-2-4	**0.218 (1)**
				1-2-5	0.191 (4)
		VoIP 설비보안	0.269 (2)	1-3-1	0.142 (4)
				1-3-2	0.154 (2)
				1-3-3	0.143 (3)
				1-3-4	**0.165 (1)**
				1-3-5	0.126 (7)
				1-3-6	0.128 (6)
				1-3-7	0.142 (4)
		사용자 정보보호	0.231 (3)	**1-4-1**	**0.504 (1)**
				1-4-2	0.496 (2)
관리적 보안	0.376 (2)	정보보호조직의 구성·운영	0.140 (5)	2-1-1	0.196 (3)
				2-1-2	0.190 (5)
				2-1-3	0.202 (2)
				2-1-4	**0.220 (1)**
				2-1-5	0.192 (4)
		정보보호계획 등의 수립 및 관리	0.148 (2)	**2-2-1**	**0.183 (1)**
				2-2-2	0.181 (2)
				2-2-3	0.164 (3)
				2-2-4	0.163 (4)
				2-2-5	0.162 (5)
				2-2-6	0.147 (6)
		인적보안	0.145 (3)	**2-3-1**	**0.222 (1)**
				2-3-2	0.186 (4)
				2-3-3	0.176 (5)
				2-3-4	0.209 (2)
				2-3-5	0.207 (3)
		이용자 보호	0.136 (6)	2-4-1	1.000
		침해사고대응	**0.156 (1)**	2-5-1	1.000
		정보보호조치점검	0.142 (4)	2-6-1	1.000
		정보자산관리	0.133 (7)	**2-7-1**	**0.518 (1)**
				2-7-2	0.482 (2)
물리적 보안	0.200 (3)	**출입 및 접근보안**	**0.387 (1)**	**3-1-1**	**0.528 (1)**
				3-1-2	0.472 (2)
		부대설비 및 시설 운영·관리	0.280 (3)	3-2-1	1.000
		기타	0.333 (2)	3-3-1	0.324 (2)
				3-3-2	0.321 (3)
				3-3-3	**0.355 (1)**

운영(0.140)-"인터넷전화 정보보호 관리자 지정", 인적보안(0.145)-"전보 또는 퇴직자의 계정 제거", 이용자 보호(0.136)-"정보보호관련 정보의 지속적인 제공", 정보자산관리(0.133)-"VoIP 망구성도 보완·관리"로 나타났다. 이는 각 항목들이 침해사고를 예방할 수 있는 관리적 예방활동의 핵심이고, 전사 보안 정책 수립시 가장 우선시 되어야 하는 항목들이기 때문에 위와 같은 결과가 나온 것으로 판단된다. 우선순위가 가장 낮은 항목들을 살펴보면 사업자의 경우 정보보호 책임자가 최고 책임자를 겸직하는 경우가 많아서라고 판단된다.

마지막으로 물리적 보안의 세부 요인에 대한 상대적 중요도 및 가장 중요한 우선순위를 갖는 점검항목을 살펴보면 출입 및 접근보안(0.387)-"잠금장치 설치", 기타(0.333)-"개인정보 DB 폐기 시, 물리적 파괴, 부대설비 및 시설 운영·관리(0.280)-"백업설비 및 시설 설치·운영"으로 나타났다. 이는 VoIP 설비를 외부의 침입으로부터 보호하고 장애 발생 시 신속하게 대응 할 수 있는 항목들이기 때문에 이와 같은 결과가 나온 것으로 판단된다.

V. 결 론

본 연구는 VoIP 침해사고 대응 안내서(2010)에서 제시하고 있는 VoIP 정보보호 점검항목에 대한 우선순위를 살펴보았다. 인터넷전화는 국내에서 이미 1,100만명을 넘어선 보편적인 서비스이며, 4G 활성화와 더불어 향후에도 성장이 예상되는 서비스이다. 하지만 인터넷전화는 상대적으로 취약한 IP를 기반으로 하고 있어 지속적으로 보안위협에 대한 우려가 제기되고 있다. 이러한 위협에 대응하기 위해서는 사업자 스스로 보안정책을 설정하고 이에 따라 주기적으로 서비스를 점검하여 침해사고를 예방하는 활동이 무엇보다도 중요하다.

VoIP 정보보호 점검항목의 우선순위를 살펴보기 위해 최근 가장 널리 사용하고 있는 AHP기법을 사용하였으며 총 15명의 인터넷전화 사업자의 보안담당자 및 인터넷전화 보안컨설팅 업무를 현재 수행하고 있는 보안전문가들에게 설문조사를 실시하여 결과를 분석하였다. 결과를 살펴보면 기술적인 측면에서는 국제전화 과금사고를 예방할 수 있는 VoIP 단말 및 장비의 접근제어 설정 및 디폴트 패스워드 변경 등이 중요하며 관리적인 측면에서는 정보보호 방침을 수립하고 이에 따라 정보보호 관리자를 지정하여 주기적인 점검을 하는 것이 중요한 것으로 나타났다. 마지막으로 물리적인 측면에서는 사업자 내부의 VoIP 설비를 외부의 침입으로부터 보호하고 VoIP 가입자의 정보를 저장하고 있는 DB 관리가 중요하다고 나타났다. 아직까지 국내외적으로 VoIP 점검항목에 대한 연구가 이루어지지 않는 점을 감안하면 이러한 연구결과는 VoIP 사업자가 정보보호 점검항목을 우선순위에 따라 분류하여 일간, 월간, 분기별로 점검하는데 크게 활용될 것으로 생각된다. 향후 연구에서는 VoIP 점검항목을 침해사고 예방 및 대응으로 구분하여 계층화하고 다중회귀분석을 이용하여 VoIP 사업자의 정보보호 지수를 도출하는데 활용할 예정이다.

참고문헌

〔1〕 방송통신위원회, 한국인터넷진흥원, "VoIP 정보보호 가이드라인," 2007년

〔2〕 방송통신위원회, 한국인터넷진흥원, "인터넷전화(VoIP) 침해사고 대응 안내서," 2010년

〔3〕 곽병호, "AHP의사결정방법에서 양방향 순위도출방법을 이용한 쌍대비교의 일관성 검정," 석사학위논문, 한양대학교, 2007년 2월

〔4〕 주영도, "인터넷전화(VoIP) 서비스의 보안 기술에 관한 연구," 산한기술연구소논문집 제 25호, pp.129-146, 2008년 9월

〔5〕 윤상희, "모바일 인터넷전화 서비스를 위한 보안위협 대응방안 연구," 석사학위논문, 건국대학교, 2011년 8월

〔6〕 T.L. Saaty, "The Analytic Hierarchy Process," McGraw Hill, New York, 1980.

〔7〕 정형철, "개인정보보호 수준진단 지표의 중요도에 대한 AHP 및 비모수 검정 연구," J Korean Data Anal Soc vol.12 no.3(B) pp.1499-1510, 2010년 6월

〔8〕 이강수, 김기윤, 나관식, "정보보호를 위한 다속성 위협지수: 시뮬레이션과 AHP 접근방법," 한국IT서비스학회지, 제7권 제1호 pp.117-130, 2008년 3월

〔9〕 이미숙, 이태환, 김진수, "AHP를 활용한 기술이전 측정항목 중요도에 관한 연구: 국공립연구소 및 국립대학기술을 도입한 기업을 대상으로," 한국산하기술학회논문지, 제11권 제8호 pp.2758-2765, 2010년 8월

〔10〕 방송통신위원회, 한국인터넷진흥원, "정보보호 안

전진단 해설서," 2011년
〔11〕 이창효, "집단의사결정론," 세종출판사, 2000년
〔12〕 T.L. Saaty, "How to Make a Decision: The Analytic Hierarchy Process," European Journal of Operation Research, Vol. 48, pp.9-26, 1990.
〔13〕 T.L. Saaty and G.V. Luis, "Diagnosis with Dependent Symptoms: Bayes Theorem and the Analytic Hierarchy Process," Operation Research, Vol. 46, No. 4, pp491-502, 1998.

〈著者紹介〉

윤 석 웅 (Seokung Yoon) 정회원
1998년 2월: 인하대학교 자동화공학과 졸업(학사)
2003년 2월: 인하대학교 전자계산공학과(공학석사)
2003년 1월~2006년 8월: 삼성전자 무선사업부 선임연구원
2006년 8월~현재: 한국인터넷진흥원(KISA) 서비스인프라보호팀 책임연구원
〈관심분야〉 정보보호, VoIP/스마트TV 등 신규 IT서비스 보안

박 해 룡 (Haeryong Park) 종신회원
1999년 2월: 전남대학교 수학과 학사
2001년 2월: 서울대학교 수학과 석사
2006년 8월: 전남대학교 정보보호학과 박사
2000년 12월~현재: 한국인터넷진흥원(KISA) 서비스인프라보호팀장
〈관심분야〉 암호알고리즘 설계 및 분석, 개인정보보호기술 개발, Digital ID Management, 정보보호 안전진단, 정보보호 사전점검, VoIP/IPTV/스마트TV 보안 등

유 형 선 (Hyeong Seon Yoo) 정회원
1974년: 인하대학교 기계공학과(공학사)
1976년: 한국과학기술원 기계공학(공학석사)
1983년: Ghent University, Belgium, 기계공학(박사)
현재: 인하대학교 컴퓨터공학부 정교수
관심분야: Applied Cryptography, Scientific Computation