제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

정보시스템 보안성 향상을 위한 표준프로파일에 관한 연구

유정희*, 유인태*, 신신애**
*경희대학교 정보통신 대학원 통신망관리공학과
**한국전산원 정보화표준부

e-mail: yujunghee@dreamwiz.com
itryoo@nms.kyunghee.ac.kr
sashin@nca.or.kr**

A Research on Standard Profile for Improving Security of Information System

Jung-Hee Ryu*, In-Tae Ryoo*, Shin-Ae Shin**
*Dept of Information and Communication,
Kyung-Hee University

**Dept of Information System Standard, NCA

요 약

최근의 정보화 사업들은 인터넷 환경을 기반으로 하여, 웹 시스템으로 구축되고 있다. 그러나 웹 환경은 그 개방성으로 인하여 보안이 매우 취약하지만, 보안에 대한 체계적으로 정립된 보안모델이 없어 정보화사업마다 나름대로의 보안 모델을 만들어 적용하고 있다. 이렇게 자체적으로 정의한 보안모델은 구성 정도에 따라 취약성을 내포할 수 있으며, 일부 시스템 보안성에 문제가 발생하면 네트워크로 연결된 다른 시스템에도 문제가 전이되는 사례를 초래할 수 도 있다. 이러한 문제를 해결하기 위하여 본 연구에서는 정보화 사업들의 보안성 향상을 위하여 지켜야 하는 최소한의 보안 모델을 표준과 함께 제시하고자 한다.

1. 서론

정보통신 기술이 발전됨에 따라 최근의 정보화사업들은 인터넷 환경, 즉 웹 환경으로 개발되고 있다. 그러나 웹 환경은 그 개방성으로 인하여 보안이 매우 중요함에도 불구하고 정보화사업들마다 서로 상이한 보안 정책과 보안 대책을 적용하고 있다. 이는 보안의 취약성을 야기하게 되고, 시스템들이 네트워크 환경으로 구축되어 있기 때문에 일부 시스템 보안에 문제가 생기면 네트워크로 연결된 다른 시스템에도 영향을 미치게 된다. 따라서 본 연구에서는 웹 환경의 정보시스템에 보안성 향상을 위하여 최소한 기본적으로 갖추어야할 보안 표준 프로파일을 제시하고자 한다.

본 연구의 2장에서는 본 연구와 관련된 연구와 문제점에 대해 정의하였고, 3장에서는 본 연구에서 제안하는 보안 모델과 분야를 정의하고, 4장에서는 보안 모델과 모델별 세부 분야에 정의된 항목에 필요한 표준들에 대한 프로파일을 제시하였으며, 5장에서는 본 연구에 관한 결론을 맺는다.

2. 관련연구 및 문제점

2.1 BS7799 영국정부의 정보보안 관리시스템의 표준[10]

BS7799는 영국의 상무성 주관으로 "정보보안관리 실무 규범 (A Code of Practice for Information Security Management)"이라는 제목 하에 조직의 정보보안을 구현하고 유지하는 책임을 지는 관리자들이 참조할 수 있는 보안관리 지침을 제시한 것으로 보안 모델은 표[1]과 같다.

[표1] BS7799의 보안 모델

분야	세부 분야	분야	세부 분야
보안 정책	정보보안 정책	시스템 접근 통제	컴퓨터 접근 통제
보안 조직	정보보안 기반 구조		컴퓨터 접근 통제
	제삼자 접근 보안		애플리케이션 접근 통제
자산 분류와 통제	자산의 책임성		시스템 접근과 사용 감시
	정보 분류	시스템 개발 및 유지보수	시스템 보안 요구사항
인적 보안	직무 정의와 고용 보안		응용 시스템 보안
	사용자 훈련		응용 시스템 파일의 보안
	사고 대응		개발과 지원 환경 보안
물리적 및 환경적 보안	보안 영역	업무 지속성 계획	업무 지속성 계획의 측면
	장비 보안	준수	법적 요구사항 준수
전산기 및 네트워크 관리	운영 절차와 책임		
	시스템 계획과 수락		
	악성 소프트웨어 보호		
	시스템 운영		IT 시스템의 보안 검토
	네트워크 관리		
	매체 처리와 보안		
	데이터와 소프트웨어 교환		
시스템 접근 통제	시스템 접근에 대한 업무 요구사항		시스템 감사 고려사항
	사용자 접근 관리		
	사용자 책임		

2.2 IETF Working Group Report on Internet/Intranet Security[13]

IETF 인터넷/인트라넷 보안 워킹 그룹에서 보안 전문가들이 제시하고 있는 IETF의 전문가들이 제시하고 있는 보안 영역은 [표2]과 같다.

[표2] Internet/Intranet Security

보안분야	세부분류	항목
네트워크	IP	- IPSEC - AH - ESP - HMAC - SHA - MD5 - ISAKMP
	DNS	-
	PKIX and X.509.v3	- PKIX-1 Certificate and CRL Profile - PKIX-2 Operational Protocols - PKIX-3 Certificate Management Protocol - PKIX-4 Certificate Policy
	SPKI	- Type D - Type S
	SSH	-

2.3 정보보호 기술 분류[11]

[11]에서는 정보화 추진에 의하여 부수적으로 발생 가능한 문제점 및 그 문제점을 유발하는 위협요소에 대한 대책별로 기술을 정의하고 분류하였다. 다음 [표3]은 [11]에서 정의한 정보보호 기술 분류이다.

[표3] 정보보호 기술분류

기술	구분
인증기술	일반적기술
	암호적 기술
접근통제 기술	접근통제정책
	접근요구역과
	접근요구급지
데이터내용 보호기술	암호 설계
	암호분석
	암호구현
위·변조 기술(무결성)	일방향 함수
	암호적 기술
데이터내용 부인방지기술	송신부인 봉쇄
	수신부인 봉쇄
	TTP

2.4 관련 연구의 문제점

BS7799 영국정부의 정보보안 관리시스템의 표준[10]에서 제시한 보안 모델에서는 실무적인 관점에서 보안 전체적인 부분을 다루고 있다. 하지만 보안 전반적인 정책이나 지침 등 상위 수준에서의 보안 분야를 다루고 있고, 실제 적용 가능한 기술들은 다루고 있지 않기 때문에 웹 환경에서 정보시스템 구축시 필요한 실제적인 보안 기술들의 선정에 어려움을 겪을 수밖에 없다.

Working Group Report on Internet/Intranet Security[13] 에서 제시하고 있는 보안의 분류는 통신보안에 관련된 분야를 세분화하여 제시하고, 응용환경이나 데이터에 관련된 분야의 기술에 대해서는 연구에 포함되어 있지 않다.

정보보호기술분류[11]에서 제시한 보안 분류는 데이터를 보호하기 위한 보안 분류에 치중되어 있어서 웹 환경이나 네트워크와 관련된 기술 및 보안 관리에 대한 부분이 부족하다.

따라서 본 논문에서는 기존연구들의 문제점들을 고려하여 보안 전체를 포괄하면서 그에 따라 필요한 기술들을 중심으로 보안 모델과 표준프로파일에 초점을 두었다.

3. 정보시스템 보안 모델

정보시스템 보안 모델의 분류는 인터넷, 웹 환경의 정보보호를 위해 필요한 가장 기본적으로 고려되어야 하는 응용보안, 네트워크보안, 데이터보안, 관리보안의 네가지 분야로 구성하였다.

- 운영환경 보안: 웹 시스템의 환경을 구성하는데 필요한 보안 분야
- 네트워크 보안: 네트워크의 장치와 관련된 보안 분야
- 데이터 보안: 웹 환경에서의 데이터 기밀성, 무결성, 부인방지를 위한 분야
- 관리 보안: 시스템을 관리할 수 있는 기능 서비스를 제공하기 위한 분야

분야별 세부보안 분야와 관련 보안 기술은 [표4]와 같다.

[표4] 정보시스템 보안 모델

보안 분야	세부 분류	
응용	- 웹 환경	- SSL V3/TLS - HTTP Server
네트워크	- IP 보안 구조	- IPSEC
	- SNMP	- SNMP
	- VPN	- IPSEC, IKE, SEED, 3DES
	- 메시지 전송	- SSL V3/TLS - FTP - SSH
	- 접근성	- Firewall - SOAP
	- 컴퓨터바이러스	
데이터	- XML 보안	
	- 암호	- 3DES - SEED
	- 해쉬	- SHA - 1 - HAS-160
	- 인증	- BER/CER/DER인코딩 - CMP - TSP - NTP V3.0 - SNTP
관리	- 위험관리	
	- 보안평가	
	- 비상계획 및 재해복구	

응용 보안분야의 세부 항목으로는 본 논문에서 제안하는 보안모델이 웹 기반 정보시스템을 기반으로 함으로, 웹 시스템의 운영과 관련된 웹 환경 보안 분야를 제시하였다.

- 웹 환경 보안 분야 : 웹 환경 구축 및 운영을 위한 보안 요소와 기법을 제시한다.

네트워크 보안분야의 세부 항목으로는 인터넷 및 공중망을 통한 웹 시스템에의 접근과 관련된 VPN 분야, IP 보안 분야, SNMP 분야, 접근제어 분야, 메시지 전송분야

를 제시하였다.

- VPN 분야 : VPN은 공중 통신망 기반시설을 터널링 프로토콜과 보안 절차 등을 사용하여 개별기업의 목적에 맞게 구성한 데이터 네트웍으로 이와 관련된 보안 분야를 제시한다.
- IP 보안 분야 : 네트웍 통신의 패킷 처리 계층에서 보안을 위해 본질적으로 데이터 송신자의 인증을 허용하는 인증 헤더(AH)와, 송신자의 인증 및 데이터 암호화를 함께 지원하는 ESP(Encapsulating Security Payload)등, 두 종류의 보안 서비스를 제시한다.
- SNMP 분야 : 네트웍 관리 및 네트웍 장치와 그들의 동작을 감시, 통제하는 서비스를 제시한다.
- 접근제어 분야 : 패스워드 등 권한 받지 않은 방식이나 시스템 자원의 활용을 막기 위한 서비스를 제시한다.
- 메시지 전송분야 : 응용 계층과 전송계층 사이에 클라이언트와 서버간의 안전한 채널을 형성하여 안전한 메시지를 전송하는 서비스를 제시한다.

데이터 보안분야의 세부 항목으로는 정보화사업의 데이터 교환포맷으로 많이 이용되고 있는 XML의 보안분야와 암호화 분야, 인증 분야를 제시하였다.

- XML 보안분야 : 정보 교환 포맷의 표준으로 활용이 증가되고 있는 XML의 보안과 관련된 서비스를 제시한다.
- 암호화 분야 : 정보처리시스템 및 정보통신망 환경에 암호의 데이터 변환 암호화 알고리즘과 DES와 같은 블록 암호알고리즘에 기초하여 임의의 길이 비트열을 고정된 길이(160비트)의 출력 값인 해쉬 코드로 압축하는 방법을 제시한다.
- 인증 분야 : 프로세스, 시스템 및 사람이 유일하게 증명됨을 보장하기 위한 서비스로 인증서 프레임워크, 인증서 효력정지 및 폐지목록, 인증서 관리프로토콜, 타임스태프 분야가 해당된다.

관리 보안분야의 세부 항목으로는 시스템을 관리하기 위하여 위험관리 분야, 보안평가 분야, 비상계획 분야를 제시하였다.

- 위험 관리 분야 : 공공정보시스템을 운영하거나 구축하고자 하는 보안담당자가 효과적인 위험관리를 수행할 수 있도록 위험분석의 세부 절차와 위험분석수행을 위한 구체적인 기술을 제시한다.
- 보안 평가 분야 : 정보기술의 보안성 평가의 기준을 제시한다.
- 비상계획 분야 : 재해에 대한 효율적인 대처 및 피해를 최소화하는 서비스를 제공한다

4. 보안 표준 프로파일

표준 프로파일이란 주어진 목적에 맞는 요구사항을 지원하기 위해 필요한 기능성을 구체적으로 설명한 표준의 모음(set)으로 표준의 목적을 충족하고 특정 업무 기능에 제공되는 기술을 지원하기 위해 필요한 최소한의 기준을 의미한다.

"2. 정보시스템 보안모델"에서 제시한 각 세부 보안 분류 항목별 표준프로파일은 다음 기준을 고려하여 식별하였다.

- 기능적인 요구사항 만족도
- 개방 시스템 환경에 적합한 공공의 표준인지 확인
- 상용시장의 다양한 제품으로 이용 가능도
- 표준에 적용된 기술의 성숙도
- 설치된 하부구조와 양립성 보장도
- 보안 요구사항 충족도

위의 기준이 고려된 후의 우선 순위는 다국적 조약에 의한 표준 > 국제표준 > 지역표준 > 국가표준> 단체표준 > 포럼표준> 업체표준 순이다.

보안모델에 사용된 세부 항목 각각에 필요한 표준을 도출하는데 있어서 위의 우선순위에 따라 기본적으로 적용할 표준들을 도출한 결과는 [표5] 와 같다.

[표5] 보안 표준 프로파일

보안 분야	세부 분류	관련 표준
응용	웹 환경	- SSL V3/TLS (RFC2246) - HTTP Server (RFC2068) - 공공기관홈페이지구축운영지침서 - 웹환경구축및운영을위한보안관리지침서 (TTAS.KO-10.0090) - 공공기관인트라넷보안지침서 (TTAS.KO-10.0088)
네트워크	IP 보안 구조	- IP-SEC (RFC2402, RFC2404, RFC2406-8)
	SNMP	- RFC854, RFC1157
	VPN	- IPSEC, IKE, SEED, 3DES - IP 계층에서의 VPN 보안기술 표준 (TAS.KO-12.0014)
	메시지 전송	- SSL V3/TLS(secure HTTP, RFC2246) - FTP (RFC2228) - SSH (RFC959)
	접근성	- 침입차단 시스템 선정지침 (TTA.KO-12.0003) - Firewall(k4등급이상) - SOAP - 인터넷 접속시 보안관리를 위한 지침서 (TTA.KO-10.0081)
	컴퓨터 바이러스	- 컴퓨터바이러스 방지 지침(TTAS.KO-12.0010)

보안 분야	세부 분류	관련 표준
데이터	XML 보안	- XML Encryption - XML Signature Requirements
	암호	- 3DES (FIPS PUB 46-3) - SEED (TTAS.KO-12.0004)
	해쉬	- SHA-1 (FIPS PUB 180-1) - HAS-160 (TTAS.KO-12.0011/R1)
	인증	- 전자서명 인증서 프로파일 (TTAS.KO-12.0012) - 디렉토리:공개키 및 인증 프레임워크 (TTAS.IT-X.509/R2) - BER/CER/DER인코딩 ASN.1인코딩(ITU-T X.690) - PEM 인코딩 (IETF RFC 1421) - 전자서명 인증서 효력정지 및 폐지 목록 프로파일 표준 (TTAS.KO-12.0013) - 인터넷 X.509 (IETF RFC2459) - CMP (IETF RFC2510) - TSP (IETF RFC3161) - NTP V3.0 (IETF RFC1305) - SNTP (IETF RFC1361)
관리	위험관리	- 위험분석 방법론 모델 (TTAS.KO-12.0007) - 공공정보시스템 보안을 위한 위험 분석 표준-개념과 모델 (TTAS.IS-TR13335.1) - IT보안관리를위한가이드라인 (ISO/IEC13335)
	보안평가	- 정보기술보안성 평가 기준 (TTAE.IS-15048)
	비상계획 및 재해복구	- 공공기관 정보시스템을 위한 비상계획 및 재해복구에 관한 지침서(TTAS.KO-12.0009)

5. 결론

웹 환경이 급속히 발전하면서 정보화 사업들이 인터넷 환경을 기반으로 구축되고 있으나 인터넷 환경의 개방성으로 인해 보안이 매우 중요하게 되었다. 그러나 정보화 사업마다 나름대로의 보안 모델과 표준들을 사용하고 있기 때문에 보안 취약성을 야기하게 되고 네트워크 환경으로 연결된 시스템에서 일부 시스템 보안에 문제가 발생하면 네트웍으로 연결된 다른 시스템에도 영향을 미치게 되었다. 이를 해결하기 위하여 정보화 사업들이 공통적으로 활용할 수 있는 최소한 갖추어야할 보안 표준 목록을 체계적으로 정리할 필요가 있다.

본 논문에서는 인터넷 환경에서 필요한 정보보호를 위해 필요한 정보시스템 보안 서비스 모델 즉, 웹 환경에서 필요한 정보시스템 보안 서비스 모델(ISSM)을 응용, 네트워크, 데이터, 관리분야로 나누고 세부적으로 응용분야는 웹 환경으로, 네트워크 분야는 IP 보안 구조, SNMP, VPN, 메시지 전송, 접근성, 컴퓨터바이러스로 분류하였으며 데이터 분야는 XML 보안, 암호, 해쉬, 인증분야로 분류하였으며, 관리분야는 위험관리, 보안 평가, 비상계획 및 재해복구로 분류하였다. 또한 4장에서는 3장에서 제시한 정보시스템 보안 서비스 모델(ISSM)에 따라 가장 기본적으로 사용되어야 하는 표준목록들을 정리하여 표준 프로파일로 제시하였다.

ISSM의 타당성을 증명하기 위하여 구체성, 포괄성, 용이성 측면에서 분석하여 보면, BS7799[10]는 전체적인 보안 모델을 구성하고는 있으나 세부기술은 제시하고 있지 않아 구체성이 부족하고 이는 기술 선정에 어려움을 겪는다.

IETF 관련연구인 internet/intranet security[13]는 통신 분야에 집중되어 있어서 전체적인 기술들을 다루고 있지 못하다. 또한 국내 관련연구인 정보보호기술분류[11]에서도 마찬가지로 데이터 보안에 집중되어 있고, 분야별 적용기술을 표준수준까지 제시하고 있지 않기 때문에 정보시스템 보안 대책을 수립하고자 하는 사용자들이 사용하는데 불편하다.

그러나 본 논문에서 제시하고 있는 보안 모델에서는 정보시스템 전 분야에 걸쳐 구체적인 보안 표준까지 제시하고 있다. 이를 종합한 평가 결과는 [표6]과 같다.

[표6] 기준에 따른 평가

구분	ISSF	BS7799	Internet/Intranet Security	정보보호기술분류
구체성	○	X	○	X
포괄성	○	○	X	X
용이성	○	△	○	○

본 논문에서 제시하는 정보시스템 보안 서비스 모델과 보안표준 프로파일은 정보화 사업을 수행하는데, 인터넷 환경에서 최소한의 보안성을 보장하고, 보다 안정적인 시스템 구축 및 활용을 가능하게 할 것이다.

참고 문헌

[1] 정보시스템 보안/통제 감리지침 연구, 한국전산원 1998. 10

[2] 정보화 표준 프로파일, 한국전산원 1999. 12

[3] 정보화 표준 적용 틀, 한국전산원 2000. 12

[4] 전자상거래 감리 지침(보안)에 관한 연구, 한국전산원 2001. 12

[5] 정보화사업 상호운용성 확보를 위한 공통기술 표준(안), 한국전산원 2002. 3

[6] 표준 암호알고리즘 국제 공모사업 동향, 천동현, 정보보호 학회지 2002. 6

[7] XML암호화 표준동향, 김주환, 정보보호학회지 2001. 8

[8] 국내외 전자서명 및 인증제도 동향 분석, 이대기, 정보보호학회지, 2001. 8

[9] 인터넷 보안, 한국정보문화센터 부설정보기술교육원, 1998

[10] 외국의 정보시스템감리 관련제도 조사 연구, 한국전산원 2000. 12

[11] 정보보호 기술 분류, 고승철, 정보처리학회지, 1997. 3

[12] 분산 애플리이션을 위한 보안 서비스 프레임워크, 마영식, 정보과학회, 1996 가을

[13] B.C. Davis, T. Ylonen, Working Group Report on Internet/Intranet Security, 6th Workshop on Enabling Technologies Infrastructure for Collaborative Enterprises (WET-ICE '97), June 18 - 20, 1997.

[14] Yahya Y. Al-Salqan, Future Trends In Internet Security, 6th IEEE Workshop on Future Trends of Distributed Computing Systems (FTDCS '97), October 29 - 31, 1997.

[15] http://www.nca.or.kr

[16] http://www.tta.or.kr

[17] http://www.ietf.org/rfc.html

[18] http://www.itu.org

[19] http://www.mogaha.go.kr/kor can/index.html