제25회 한국정보처리학회 춘계학술발표대회 논문집 제00권 제0호 (2006.00)

신규IT서비스의 정보보호사전평가모델 : RFID 서비스 적용 중심

신동훈, 김국태,이강신*
*한국정보보호진흥원
e-mail:dhshin@kisa.or.kr

Information Security Pre-Evaluation Model for New IT Service : Case of RFID Service

DongHoon Shin, GukTea Kim, GangShin Lee*
*Korea Information Security Agency

요 약

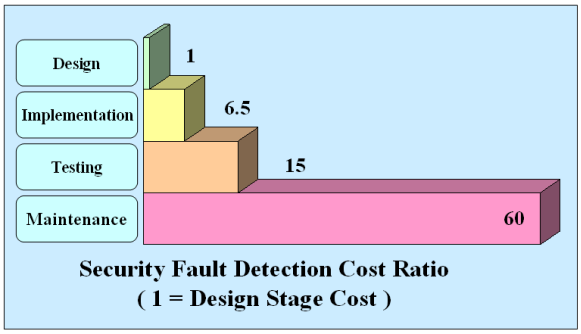
통신기술의 급속한 발전으로 네트워크 환경이 광대역통합망으로 진화되어가고 있다. 이로 인해 개별 네트워크에서 운영되던 IT서비스들 또한 광대역통합망 환경에서 빠른 속도로 융합되고 있다. 하지만, 개별 네트워크에서 운영되던 기존의 IT서비스들이 광대역통합망에서 서로 융합되어 신규 IT 서비스를 생성하는 과정에서 보안요소가 적용되지 않을 경우에 신규 IT서비스의 안정성 및 신뢰성이 떨어질 수 있다. 이러한 문제점을 해결하기 위해서, 본 논문에서는 신규 IT 서비스의 기반구축 및 운영이전인 서비스에 대한 기획 및 설계시에 필수적인 보안대책 제시하여 서비스 운영이전에 보안대책을 적용할 수 있도록 함으로써, 신규 IT 서비스의 안정성과 신뢰성을 확보할 수 있는 방법으로 정보보호사전평가 모델을 제시하고, 이 모델을 RFID 서비스에 적용한 예제를 설명한다.

1. 서론

최근 유무선 통신기술의 급속한 발전과 더불어 네트워크 환경이 광대역통합망으로 진화되어 가고 있다[1][2]. 개별적인 네트워크를 기반으로 운영되던 IT 서비스들 또한 광대역통합망 환경에서 급속히 빠른 속도로 융합화, 복합화되고 있다. 하지만, 개별 네트워크에서 운영되던 기존의 IT서비스들이 광대역통합망에서 서로 융합되어 신규 IT 서비스를 생성하는 과정에서 보안요소가 적용되지 않을 경우에 신규 IT서비스의 안정성 및 신뢰성이 떨어질 수 있다[3].

일반적으로 새로운 IT 서비스를 개발하는 사업자 입장에서는 남들보다 시장을 선점해야 하므로, 조속한 서비스 개시를 위하여 정보보호 기능을 간과하기 쉽다. 이 경우, IT 서비스의 안전·신뢰성 저하로 인해 보안위협이 증가하게 되고, 서비스 운영 중에 침해사고가 발생하면 서비스 복구에 많은 비용이 발생할 수 있다. 이러한 보안결함을 발견하여 해결하는 비용은 설계단계에 비해 구현, 테스트 단계에서 증가하는 것으로 분석되고 있고, 서비스의 운영 단계에서 발생하는 결함을 발견하여 해결하는데 소요되는 비용은 설계단계에서 보안취약성을 해결하는 비용의 60에서 100배에 이르게 된다[4].

이러한 배경에서 본 논문에서는 신규 IT 서비스의 기반구축단계부터 정보보호를 위한 필수 보안요소를 도출하여 적용할 수 있는 방법론인 정보보호사전평가 모델을 소개하고, 이를 홈 네트워크 서비스에 적용한 사례를 통해 서비스 개발이전에 정보보호대책을 수립하여 적용하는 방법을 구체적으로 설명한다.



(그림1) 보안결함 탐지비용

2. 관련연구

2.1. TCSEC (Trusted Computer System Evaluation Criteria)

1983년 미국은 안전한 컴퓨터 시스템을 위한 평가 기준인 일명 "Orange Book"이라 불리우는 TCSEC의 초안을 NCSC(National Computer Security Center)에서 제작하였고 2년 뒤인 1985년 미국방성 표준(DoD STD 5200.28)으로 채택되었다 TCSEC은 컴퓨터 시스템의 보안성을 효과적으로 평가하고 안정성 및 신뢰성이 입증된 컴퓨터 시스템을 각 기관에 보급을 목적으로 운영체계를 6등급(C1, C2, B1, B2, B3, A1)으로 분류하고 있다. TESEC은 특히 보안요소 중 비밀성을 강조하고 있다. 기본적인 보안요구사항은 ① 보안정책(Security Policy), ②보안등급 등에 대한 표시(Marking), ③ 신분확인(Identification), ④ 보안에 대한 책임성(Accountability), ⑤ 보안정책. 표시. 신분확인. 책임성이 시스템에 적용됨을 보증(Assurance)하는 카테고리로 분류되고 있다.

2.2. ITSEC (Information Technology Security Criteria)

1991년 5월 프랑스, 독일, 영국, 네덜란드의 유럽 국가들은 각국의 보안성 표준을 조화롭게 통합 조정하여 IT시스템에 대한 공동 보안평가 기준인 ITSEC 초안을 발표하였다. 이들 국가들은 유럽국가간 무역장벽을 없애고, 기본적인 표준안과 시험의 지침서로 활용하기 위해 ITSEC을 개발하였다. ITSEC의 보안기능 요구사항은 기본적으로 보안기능기준과 보증요구사항으로 구분되어진다. ITSEC의 보안기능은 보안목표, 보안기능, 보안체계의 3가지 추상화수준과 보안지침의 가장 중요한 부분인 식별과 인증, 접근제어, 기록성, 감사, 객체 재사용, 정확성, 서비스의 신뢰성, 데이터 교환 등 8개의 기본적인 기능으로 그룹화되어 있다. 또한, 보증기준은 시스템에서 규정된 보안기능의 정확한 구현에 관한 지침과, 시스템 평가과정에서 발전된 보안기능, 보안체계의 효용성을 나타내는 지침을 포함하고 있다.

2.3. CC (Common Criteria)

CC는 선진 각국의 보안 제품 및 시스템 평가 담당기관 및 연구진이 모여서 만든 국제적인 표준이다. 1993년 6월에 CTCPEC, FC, TCSEC, ITSEC 작성자들이 단일의 국제 공통 평가기준(CC : common criteria)을 만들기 위한 프로젝트를 시작하여 1996년 1월에 발표하였고, 국내에서는 한국정보보호진흥원이 2000년에 발표한 정보보호개론에 약간의 수정을 거쳐 1998년 2.0버전이 발표되었다.
CC는 국가별 독립적으로 구성되어져 있는 평가기준을 하나의 표준으로 통일함으로써 중복되는 평가로 인한 자원의 낭비방지를 추구하고 있다. 또한 CC는 개발자, 평가자, 사용자의모든 관점을 지원하고 있고, 시스템과 제품에 대한 많은 정보를 제공하고 있다. CC의 구성과 그 내용은 다음과 같다.

제1부 : 소개 및 일반모델 제시
제2부 : 보안기능 요구사항
제3부 : 보증 요구사항
제4부 : 보호 프로파일
제5부 : 보호 프로파일의 등록절차

2.4. BS 7799

BS7799는 BT, HSBC, Marks and Spencer, Shell International, Unilever 등 주요업체와 더불어 영국의 상무성 주관으로 정보보안관리실무규범(A Code of Practice for Information security management)이라는 제목하에 조직의 정보보안을 구현하고 유지하는 책임을 지는 관리자들이 참조할 수 있는 보편적인 문서로 사용되도록 개발되었으며, 조직의 보안 표준의 기반이 되도록 고안되었다.
BS7799는 기업이 고객정보의 비밀성, 무결성 및 가용성을 보장한다는 것을 공개적으로 확인하는데 초점을 두고 있고, 보안에 대한 지침과 권고안의 두가지 성격을 갖는다.

3. 신규IT서비스의 정보보호사전평가 모델[5]

3.2 정보보호사전평가 개요

■ 모델 정의

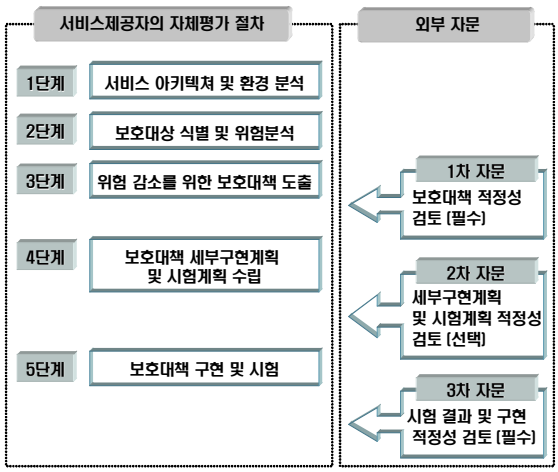
신규 IT 서비스의 운영이전 단계인 서비스 기획 및 설계 단계에 서비스의 특성을 식별하여 기술적, 물리적, 관리적 위협·취약점을 분석하고 필수 보안요구사항을 도출하고, 보호대책을 제시하여 신규서비스에 대한 사전안전관리체계를 마련하기 위한 일련의 절차와 방법론을 말한다.

■ 평가 대상

정보보호사전평가 모델의 평가 대상은 광대역통합망에서 운영될 예정인 신규IT서비스의 구성요소와 서비스에 적용되는 유·무선 통신기술 등으로 볼 수 있다. 구체적인 평가대상은 서비스의 특성이 서로 다르기 때문에 각 서비스마다 다를 수 있다 하지만, 사전평가 대상을 다음과 같이 나누어 생각해 볼 수 있다.

3.2 정보보호사전평가 절차

서비스 개발, 운영이전에 보안대책을 적용하기 위한 정보보호사전평가모델의 평가절차는 아래 (그림 2)와 같다.



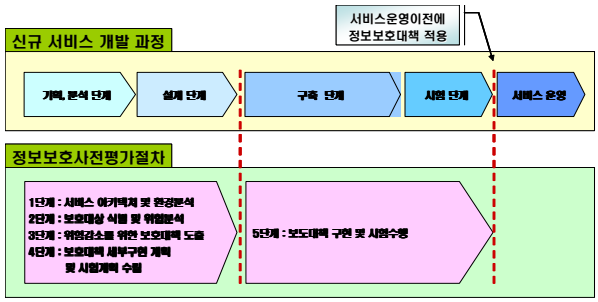
(그림2) 정보보호사전평가 절차

위 그림에서는 서비스 제공자(사업자)의 자체평가 단계와 이에 따라 외부자문기관에서 수행하는 자문단계를 나타내고 있다. 1단계부터 3단계까지는 서비스의 특성 및 정보보호 취약성과 위협을 분석하고, 이에 대한 정보보호 대책을 도출하는 단계이다. 이 단계가 끝나면 서비스 특성 분석 결과, 정보보호 취약성과 위협 분석결과 및 정보보호 대책에 대한 외부 자문을 수행하여 각 단계별 결과에 대해 보완한다. 4단계와 5단계는 수립된 정보보호대책별로 구체적인 세부구현 계획과 시험계획을 수립하고, 수립된 세부구현 계획에 따라서 보호대책을 구현하고 이후 시험계획에 따라 보도대책 구현의 적절성을 검증한다. 이 단계가 끝나고 나면, 정보보호대책 구현 및 시험결과에 대한 외부 자문을 수행하여, 정보보호대책 구현의 적절성을 검증한다.

정보보호사전평가 단계에서 외부자문이 끝난 후에는 앞의 단계로 피드백하여 정보보호에 불완전한 요소를 보완하는 단계를 반드시 거쳐야하며, 필요에 따라서는 앞 단계의 보완 후에 외부자문을 재수행할 수도 있다.

■ 신규IT서비스개발 과정과 정보보호사전평가절차

신규IT서비스의 개발 단계에 따라 정보보호사전평가절차를 적용하는 방법은 아래 그림과 같다.



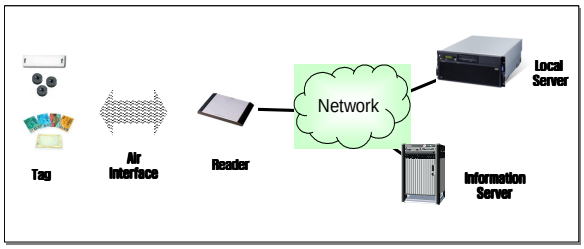
(그림 3) 서비스 개발과 정보보호사전평가 절차

서비스 기획, 분석 단계와 설계단계에는 정보보호사전평가절차 중 서비스 아키텍처 및 환경 분석, 보호대상 식별 및 위험분석, 보호대책 도출(외부자문 병행), 보호대책 세부구현 계획 및 시험계획 수립의 단계를 수행한다. 즉, 서비스 구축이전에 단계에 서비스특성을 분석하여 정보보호 취약점과 위협요소를 도출하고, 이에 대한 대책을 수립하는 단계를 수행하는 것이다. 이렇게 수립된 보호대책에 대한 세부구현계획과 시험계획을 이용하여 서비스 구축단계의 보호대책 세부 구현계획에 따라 보호대책 구현을 병행하여 진행한다. 서비스 구축단계와 운영을 앞 둔 테스트 단계에서 각 세부 보호대책을 구현하고 시험을 수행하여 각각의 보호대책 항목들이 적절하게 구현되어 적용되고 있는지를 검증한다. 즉, 서비스 개발과정에서 정보보호사전평가모델을 적용하면, 서비스 구축이전에 보호대책을 수립하고, 서비스 운영이전단계의 보호대책 구현 및 시험을 통한 검증을 수행하여 서비스의 안정적인 제공환경을 확보하는데 기여할 수 있다.

4. RFID 서비스에 정보보호사전평가 모델 적용

■ 1단계 : 서비스 아키텍처 및 환경 분석

RFID(Radio Frequency Identification) 서비스란 전자칩을 부착하고 무선통신 기술을 이용하여 사물의 정보를 확인하고, 주변 상황정보를 감지하는 센서기술로, 식료품부터 축산물관리, 폐기물관리, 환경관리, 물류/유통 · 보안 등 우리생활의 다양한 분야에 적용될 전망이다. **RFID** 서비스의 구성요소와 데이터 흐름을 알 수 있는 서비스 구조도는 아래 그림과 같다.[6][7][8][9][10]

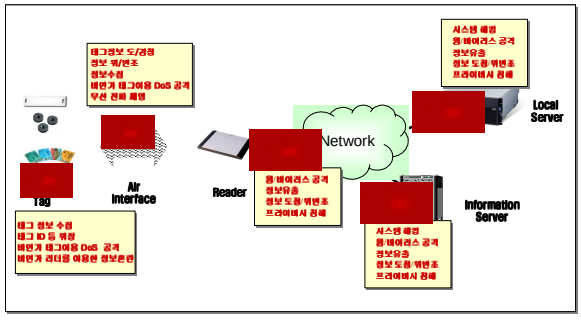


(그림 4) **RFID** 서비스 구조도

■ 2단계 : 보호대상 식별 및 위험분석

RFID 서비스 제공을 위한 주요구성요소는 앞의 그림에서도 알 수 있듯이, 다양한 물품에 부착되고, 정보를 저장하고 있는 칩과 전파를 송수신하기 위한 안테나로 구성되어 있는 전자태그, 태그와 직접통신하면서 태그에 저장된 정보를 미들웨어로 전송하는 리더, 리더에서 전송받은 정보의 글로벌 식별자를 이용하여 객체정보를 검색하기 위한 환경을 제공하는 **RFID** 미들웨어, **RFID** 식별정보를 이용하여 정보서버내의 유효컨텐츠를 검색하는 객체검색 시스템, 그리고 실제 정보를 저장하고 있는 정보서버이다.

RFID 서비스를 제공하는 각 구성요소들은 아래와 같은 위협 혹은 취약성을 갖는다.[11]



(그림5) **RFID** 서비스의 보안 위협

■ 3단계 : 위험감소를 위한 보호대책 도출

2단계에서 식별된 구소요소별 위험분석결과를 이용하여 보호대책을 아래와 같이 보호대책을 수립하였다.

[표 1] 구성요소별 정보보호 대책

	정보보호 대책
태그	○ 태그 충격방지 ○ 태그와 리더의 상호인증 메커니즘 적용 ○ 태그 정보의 암호화 ○ 암호키, 인증정보 등의 관리대장
리더	○ 전송라인, 전력선의 접근제한 ○ 전송 데이터 암호화 ○ 불량 태그 자동차단 ○ 패치, 업그레이드 수행 ○ 시스템 관리대장 마련 ○ 주기적인 보안점검 수행
객체검색 시스템 & 정보서버	○ 데이터전송라인, 전력선 접근제한 ○ 시스템에 보안기능/솔루션 적용 ○ 바이러스 탐지/차단 적용 ○ 유해사이트 자동 차단 ○ 관리자 인증 및 접근제어 적용 ○ 전송 데이터 암호화 및 VPN 적용 ○ 주요 정보의 관리대장 마련 ○ 시스템에 대한 주기적인 취약점 점검 ○ 보안패치 및 업그레이드 ○ 네트워크 트래픽 등에 대한 상시 모니터링 ○ 백업 및 복구 시스템 구축 ○ 정보보호 전담조직, 정책, 지침 등 마련 ○ 관리자의 정보보호 교육실시 ○ 용역업체 보안관리기준 적용

정보보호사전평가의 실효성을 증대시키기 위한 방안으로 수립된 보호대책에 대한 정보보호 전문가의 보호대책 적정성을 검토받도록 한다.

■ 4단계 보호대책 세부구현 계획 및 시험계획 수립

앞의 3단계에서 수립된 보호대책의 구체적인 구현계획을 수립한다. 또한 4단계에서는 각각의 보호대책이 제대로 구현되어 적용되었는지 여부를 확인할 수 있는 시험계획도 같이 수립한다. 아래는 앞의 3단계에서 수립된 보호대책의 구현계획과 시험계획의 예제를 나타내고 있다.

[표 2] 구성요소별 정보보호 대책(예제)

	보호대책	세부구현계획	시험계획
태그	○태그 충격방지	○태그제작 및 부착시 충격완화 고려	○태그부착사물에 충격 실험실시
	○태그와 리더의 상호인증 메커니즘 적용	○태그 제작시 인증 알고리즘 구현 및 적용	○상호인증 패킷분석을 통한 적용여부 분석
	○태그정보 암호화	○태그제작시 암호프로토콜 구현 및 적용	○리더와의 통신 패킷 분석을 통한 암호화 여부 확인
	○암호키,인증정보 등의 관리대장	○운영시 관리대장 마련 및 기입	○서비스 운영을 위한 관리대장 준비 및 적용여부 확인

■ 5단계 보호대책 구현 및 시험

수립된 보호대책 세부계획에 따라서 보호대책을 구현하고, 각 보호대책이 제대로 구현되었는지 여부를 시험계획에 따라 확인한다. 보호대책 시험결과 불합격인 항목에 대해서는 반드시 수정·보완하는 프로세스를 수행하도록 해야 한다. 이 단계에서도 정보보호 전문가에 의해서 시험결과에 따라 보호대책을 적정성을 검토받아, 향후 발생할 수 있는 보안상의 문제점을 줄일 수 있도록 한다.

4. 결론 및 향후 연구과제

현대사회는 사물과 사람, 사물과 사물 사이의 네트워크 통신이 가능한 유비쿼터스 컴퓨팅에 대한 관심이 높아지고 있고, 이러한 유비쿼터스 컴퓨팅의 기반이 되는 기술인 사물의 정보를 부여하는 **RFID**에 대한 연구와 이를 이용한 사업 또한 활발히 진행되어가고 있다.

하지만, 새로이 등장하고 있는 **RFID**서비스는 광대역통합망에서 운영되고 있는 타 서비스와 많은 연관이 되어 있어, **RFID** 서비스에 전자적 침해가 발생하게되면 이와 연계된 많은 타서비스에도 악영향을 미칠 수 있을 것이다.

이에 본 논문에서는 광대역통합망을 기반으로 운영될 예정인 신규 융합형 IT서비스에 대한 신뢰성과 안전성을 확보할 수 있는 방안으로 신규 IT서비스에 대한 정보보호 사전평가 모델을 제시하였고, 이를 **RFID** 서비스 적용하여 모델의 수행 절차를 구체적으로 설명하였다.

향후, 광대역통합망의 구축이 완료되고 안정적으로 운영되면, 다수의 융합형 신규IT서비스가 등장할 것이다. 이를 위해, 본 논문에서 제시한 정보보호사전평가모델을 더욱 구체화되고 다양한 IT 서비스에 적용 가능한 범용 방법론으로 구체화 시키는 연구가 계속 진행되어야 할 것이다.

참고문헌

[1] "광대역통합망(BcN)구축 기본계획" 정보통신부, 2004
[2] 이영로, "BcN 시범사업 현황 및 추진방향", 한국전산원, TTA 저널 96호
[3] "8대 서비스의 정보보호 요구사항 분석", 전자통신연구원, 2004
[4] IBM의 시스템과학연구소(**Systems Science Institute**)
[5] 신동훈,김성훈,이강신, "신규IT서비스의 정보보호사전평가모델 연구", 한국정보처리학회 2005추계학술발표회
[6] 이근호, 한호현, 강병권, 조영빈, "유비쿼터스 컴퓨팅의 핵심 **RFID** 핸드북", 영진출판사, 2004
[7] 유승화, "유비쿼터스 사회의 **RFID**", 전자신문사, 2004
[8] 한국전산원, "2004 **RFID** 기술 및 관련 정책연구", 2004.12
[9] 함일한, " **RFID** 모델과 도입방안", LG **CNS**, 2004
[10] 한국전산원, "**RFID/USN** 응용사례 및 시연", 2004, 6
[11] 한국전산원, "전파식별(**RFID**)보급 활성화를 위한 역기능 및 정보보호 대책연구", 2004.11