유·무선 통합환경에서의 IDC 평가방법에 관한 연구

A Study on Evaluation Method of IDC in the Wire/Wireless Integrated Enviroment

이재평, 박진석*, 이만우**, 김순곤*
안양과학대학교, 중부대학교*, 한국관광대학교**

Lee Jea-Pyuing, Park Jin-Seok*, Lee Man-Woo**, Kim Sun-Gohn*
Anyang Technical College, Joongbu Univ*, Korea Tourism College**

요약

한국정보보호진흥원은 2002년부터 정보보호관리체계 인증제도를 시행해, IDC 업체들에 대한 기술적·물리적 보호조치를 포함한 종합적 관리체계가 해당 서비스에 적합한 지를 심사하여 인증을 해주고 있다. 하지만 이 인증제도는 유선과 무선으로 각각 분리된 IDC 환경에 대한 독립된 기준으로, 유·무선 통합 환경에서의 평가기준은 아직까지 마련되어 있지 못한 상태이다. 본 논문에서는 집적정보통신시설보호지침 및 무선랜 보안 운영 권고지침, 국내·외 정보보호 관련 지침 및 권고사항, IDC 환경을 분석한 자료를 바탕으로 유선과 무선이 통합된 IDC 네트워크 모델을 제시하고, IDC 평가기준을 제안하였다.

Abstract

Korea Information Security Agency has executed the certification system for the information security management since 2002 and examines the conformance of the IDCs' total management system including the technical and the physical protection measure. However, this certification system has the standard only for the IDC in the wire/wireless segregated and the evaluation method for the wire/wireless integrated has not been suggested yet. This paper is on the basis of "Accumulation Information Communication Facility Secure Principle", guidelines of Wireless LAN security operation, the existing principles and recommendations of the information security and the data on IDC environment. And the paper suggests the IDC network model in the wire/wireless integrated and the IDC evaluation method.

Ⅰ. 서 론

인터넷 시장이 확대됨에 따라 인터넷과 관련된 네트워크 인프라, 하드웨어 플랫폼, 소프트웨어/솔루션을 한곳에 모아놓고 통신망 자원과 부대 관리를 서비스해 주는 인터넷데이터센터인 IDC가 1998년 이후로 크게 늘어났다. 기업의 내부에서 이러한 모든 서비스를 운용하는 것보다 IDC을 이용하는 것이 네트워크의 안정성과 비용절감 차원에서 더 효율적이기 때문에 IDC의 인기는 높아져 갔다. 하지만 자연재해, 물리적 테러 및 사이버테러로 인한 피해가 대형화됨에 따라 IDC(인터넷데이터센터) 시설에 대한 안전·신뢰성을 확보할 수 있는 관리적, 기술적 환경 및 물리적인 분야에서의 객관적인 평가의 필요성이 요구되었다.

이러한 시대적 요구에 따라 한국정보보호진흥원(KISA)은 2002년 5월부터 정보보호관리체계 인증제도를 시행해, IDC 업체들에 대한 기술적·물리적 보호조치를 포함한 종합적 관리체계가 해당 서비스에 적합한 지를 심사하여 인증을 해주고 있다[1]. 정보보호관리체계 인증제도는 물리적(출입 통제, 인적 보안), 기술적(정보시스템 보호), 관리적(정보보호정책, 정보자산 식별, 위험분석평가 등) 보호 조치 수준에 대한 객관적인 평가를 통해 인증서를 발급하는 것으로서, 국내 실정에 적합한 정보보호관리 수준을 평가하는 제도라고 할 수 있다.

하지만 이는 유선과 무선으로 분리된 IDC 환경에 대한 독립된 기준으로, 유·무선 통합 환경의 인증 기준은 아직까지 마련하지 못한 상태이다.

이에 본 논문에서는 유·무선 통합 환경의 IDC 시설에 대한 안정적인 서비스를 위해 보안성 검토를 시행하고 인터넷의 안전성과 신뢰성을 제고하고자 한다. 더불어 물리적, 관리적, 기술적인 부분에 대해 평가항목을 도출하고 이를 토대로 유·무선 통합 환경의 IDC시설에 대한 실질적인 적용을 통해 안전성과 신뢰성을 확보 할 수 있는 평가기준을 제안하고자 한다.

Ⅱ. 관련 연구

1. IDC 관련 평가 기준과 지침

1.1 집적정보통신시설보호지침

집적된 정보통신 시설을 운영·관리하는 사업자가 정보통신 시설의 안정적 운영을 위하여 취하여야 할 보호조치 대한 최소한의 기준을 제시한 지침이다. 주요 내용은 접근제어 및 감시, 가용성, 방호성, 방재성을 포함한 물리적·기술적 보호조치 20개 항목과 보호관리 체계화, 관리용 정보시스템 장비보호를 포함한 관리적 보호조치 9개 항목으로 구성되어 있다[2].

1.2 ITU-T 권고안

ITU-T M.3000은 TMN(Telecommunication Management Network)의 응용분야, TMN 권고안이 연구되어지는 영역과 TMN 권고안에 의해 참조되어 지는 영역으로 구성되어 있다. ITU-T M.3016은 TMN에 대한 보안 위협을 식별하는 개관과 틀을 제공하고 사용 가능한 보안 서비스가 어떻게 TMN 기능적 구조안에서 적용될 수 있는지에 대한 개요를 제공한다. ITU-T M.3200에서는 TMN 사용자 입장에서 인지된 전기통신망의 운용, 유지보수, 관리 및 제공 요구사항들을 정의한 TMN관리서비스와 관리대상이 되는 전기 통신 관리영역에 대해 규정하고 있다[3].

1.3 무선랜 보안 운영 권고 지침

IEEE는 802.11b라 불리는 무선랜에 대한 추가 확장된 표준을 제정하였으며 이 표준안에서는 이더넷에서 처리되는 속도처럼 11Mbps의 무선랜 제품에 대한 표준을 포함하고 있어서 무선랜 장비 도입 시 요구사항이 된다. 이 지침은 IEEE의 802.11b 표준과 무선랜의 보안 취약점 및 안전한 운영 방법을 적극 홍보하여 장기적으로는 무선랜의 안전성 제고를 위한 제도적, 기술적 기반을 마련, 권고하고 있다[4].

1.4 BITS 권고사항

모바일 응용서비스의 기술 인프라는 인가된 최종 사용자에게 적합한 컨텐츠를 전달하는데 필요한 무선통신망, 모바일 기기, 응용소프트웨어 등 3개의 범주로 구성된다. 이러한 인프라는 변화하는 고객의 요구를 반영하고, 응용서비스 업체가 수용할 수 있는 높은 수준의 보안성과 호환성을 제공해야 하므로 그에 대한 세부적인 권고안을 제공하고 있다[5].

기타 정보호관리체계인증, 정보통신망 안전·신뢰성에 관한 기준, BS7799, SSE-CMM 모델, 블루투스 보안, 무선/휴대장비의 보안에 관한 지침 등이 마련되어 있다.

2. IDC의 물리적 환경

2.1 입지 및 건물

IDC 건물의 위치는 교통이 편리하고 접근성이 좋아야 하며, 자연재해로부터 안전한 곳에 위치해야 한다.

2.2 물리적 보안

IDC에는 사전에 등록된 고객에 한해서만 출입이 가능하며, 건물 및 장비실 출입을 통제해야 한다.

2.3 전원 설비

전원 설비는 수전, 변전, 배전 설비와 자가 발전설비, UPS 등을 갖추어야 하며 충분한 용량의 전원을 공급 받아야 한다.

2.4 항온 항습 설비

고가의 민감한 장비가 온도 및 습도에 영향으로 장애가 발생하는 것을 방지하기 위해서 항온항습기를 설치해야 한다.

2.5 방재 설비

종합 방재실을 24시간 365일 운영해야 하며 조기 화재감지 및 감시시스템, 자동 소화시스템을 갖추어야 한다. 방화벽, 방화문 설치 및 불연자재 사용은 필수 조건이다.

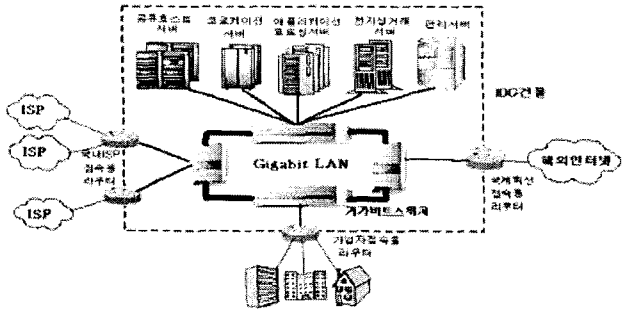
3. IDC의 기술적관리적 환경

IDC에는 보호 관리를 체계화하여 상근경비원, 전문기술자, 관리책임자 등을 지정해야 하며, 네트워크 및 보안 시스템을 안전하게 관리해야 한다. 또한 장비의 보호를 위해 침입차단 시스템, 침입탐지시스템 등을 설치하고 취약성 분석, 바이러스 대응 기술을 갖추어야 한다[6].

Ⅲ. 유무선 통합 IDC 모델 제시

우선 기존의 유선 환경 IDC 모델을 분석하고, 무선 환경에서의 IDC 네트워크 운용 모델을 제시한 후 이를 토대로 유·무선 통합 환경의 IDC 모델을 제시하고자 한다.

1. 기존의 유선 환경 IDC 모델



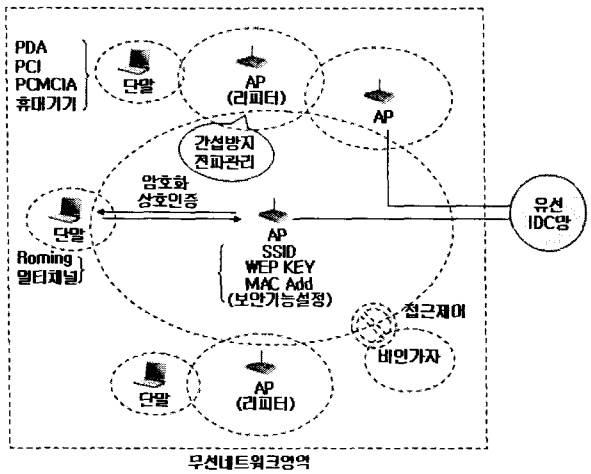
▶▶ 그림 1. 기존의 유선 IDC 구조도

2. 무선 환경의 IDC 모델 제시

(그림 2)은 무선 IDC 네트워크를 최적의 형태로 유지, 운용하기 위한 각 네트워크 요소들의 구성과 설계에 대한 개략적인 구조를 보여주고 있다.

또한 무선 IDC의 핵심적 구성요소인 AP와 무선 클라이언트들 그리고 AP와 유선 백본 영역의 연결과 각 구성에 있어서의 관련 내용에 대한 간략한 개념 및 관계도를 표현하고 있다. 우선적으로 각 무선 단말 클라이언트들과 AP들은 각각 액세스 유효범위를 갖고 있으며, 이 유효 범위의 교차로 인해 통신이 이루어 질 수 있음을 보여준다. 단 동일 주파수(동일채널)을 사용한다는 조건을 전제로 한다.

무선 IDC 장비와 서비스 및 관련 기술들에 대한 내용을 바탕으로 각 장비들간의 연계성과 효과적 네트워크 관리, 운용을 위한 네트워크 모델이라 할 수 있다[7].



▶▶ 그림 2. 무선 IDC 네트워크 운용 모델

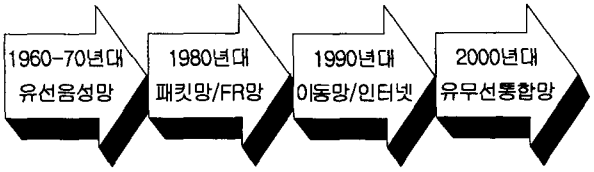
3. 유무선 통합 환경의 IDC 모델 제시

유·무선 통합 서비스는 망유형, 단말기 형태, 사업자에 상관없이 소비자가 원하는 서비스를 접속에서부터 과금까지 하나의 형태로 제공할 수 있는 서비스이다. 그리고 유선망, 무선망, 데이터망 등 각각의 망을 IP기반으로 하나의 Infrastructure로 통합하여 가입자의 접근에 무관하게 다양한 서비스를 단일 통신망에서 제공하는 서비스이다.

3.1 통신서비스 분야의 유·무선 통합 현황

통신서비스분야에서는 유선과 무선 통합이 이미 실현되고 있다. UMA(Unlicensed Mobile Access)는 무선 이동통신망과 고정 IP망(핫스팟) 사이의 핸드오버가 가능한 차세대 유·무선통합 기술표준으로, 이를 적용한 UMA폰은 무선과 유선을 넘나들며 자유롭게 음성 및 데이터통신을 할 수 있다.

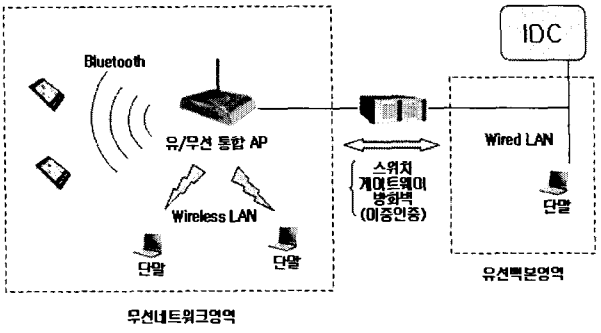
앞으로는 서로 다른 주파수 영역을 사용하는 무선인터넷, RFID, 블루투스, 와이브로 등 각종 무선 기술을 주파수간 연결 기능을 통해 하나로 통합시키는 기술인 'RF스위칭' 시대가 곧 도래할 것이다.



▶▶ 그림 3. 통신망의 발전과정

3.2 유·무선 통합 환경의 IDC 네트워크 모델

유선과 무선 환경의 IDC 모델을 기반으로 향후 IDC 분야에서의 유·무선 통합 모델을 아래 (그림 4)과 같이 제시하고자 한다.



▶▶ 그림 4. 유무선 통합 IDC 네트워크 운용 모델

Ⅳ. 유무선 통합 IDC 평가기준 제안

앞에서 제시한 유·무선 통합 환경에서의 네트워크 모델과 IDC 관련 평가 기준의 분석을 통하여 유·무선 통합 IDC에 대한 물리적, 관리적, 기술적 평가기준을 다음과 같이 제안하

고자 한다.

1. 물리영역

유·무선 통합 IDC 시설 및 장비에 대해 자연재해나 고의 또는 실수로 인한 중단, 파괴, 자료 훼손 등의 대내외적 위협에 관련된 평가기준을 제안한다.

[표 1] 유·무선 통합 IDC의 물리영역 평가기준

구분			항목	유선	무선
1	물리적 접근제어 및 감시	1.1	출입통제장치	●	
		1.2	출입기록	●	
		1.3	고객 정보시스템 장비보호	●	
		1.4	중앙감시실	●	
		1.5	CCTV	●	
		1.6	경보장치	●	
		1.7	보안센서	●	
		1.8	무선침입탐지센서		●
2	물리적장비 및 운용 환경	2.1	백업장비	●	
		2.2	UPS장비	●	
		2.3	축전지설비	●	
		2.4	자가발전설비	●	
		2.5	수변전설비	●	
		2.6	접지시설	●	
		2.7	항온항습기	●	
		2.8	비상조명 및 유도등 설비	●	
		2.9	소방시설	●	
		2.10	전력감시실	●	
		2.11	DC전원장치	●	
		2.12	전원공급	●	
		2.13	통신장비보호	●	
		2.14	무선통신장비보호		●
		2.15	무선관리부서운영		●
3	위치 및 구조 조건	3.1	벽면구성	●	
		3.2	유리창문설비	●	
		3.3	하중안전성	●	
		3.4	건축자재	●	
		3.5	수해방지	●	
		3.6	건물입지	●	
		3.7	내진설비	●	
		3.8	경계 및 영역		●
		3.9	위치선정		●

2. 관리영역

유·무선 통합 IDC 시설, 장비와 운영 인력 및 서비스 부문에 대한 관리에 대한 평가기준을 제안한다.

[표 2] 유·무선 통합 IDC의 관리영역 평가기준

구분			항목	유선	무선
1	인적보안	1.1	상근경비원	●	●
		1.2	전문기술자	●	●
		1.3	인적보안	●	●
		1.4	요원관리	●	●
2	교육 및 훈련	2.1	교육 및 훈련요원	●	●
		2.2	교육 및 훈련주기와 계획	●	●
		2.3	교육 및 훈련내용	●	●
		2.4	교육 및 훈련대상	●	●
3	보안시스템 관리	3.1	침입차단시스템	●	●
		3.2	시스템취약성 관리	●	●
		3.3	침입탐지시스템	●	●
4	시스템 접근통제	4.1	데이터베이스 접근통제	●	●
		4.2	소프트웨어 접근통제	●	●
		4.3	네트워크 접근통제	●	●
		4.4	운영체제 접근통제	●	●
		4.5	사용모니터링	●	●
5	네트워크 운용관리	5.1	악성소프트웨어 보호	●	●
		5.2	매체처리와 보안	●	●
		5.3	세율 및 과금관리	●	●
		5.4	서비스 품질 및 통신망 성능관리	●	●
		5.5	용량관리	●	●
		5.6	트래픽관리	●	●
		5.7	라우팅 및 번호분석관리	●	●
6	유지보수 관리	6.1	유지보수 절차	●	●
		6.2	예방점검 실시	●	●
7	장애관리	7.1	장채조치	●	●
		7.2	장애기록관리	●	●
8	로그관리	8.1	로그파일관리	●	●
		8.2	로그파일복구	●	●
9	사용자 접근관리	9.1	사용자 계정관리	●	●
		9.2	계정관리주기	●	●
		9.3	패스워드관리	●	●
		9.4	패스워드 관리주기	●	●
10	사고처리 및 후처리관리	10.1	보안문제 대처방법	●	●
		10.2	시스템복구	●	●
11	정보보호 정책 및 감사관리	11.1	각종지침, 절차수립 및 관리	●	●
		11.2	정보보호정책 및 지침감사	●	●
		11.3	정책 및 지침의 배포	●	●
		11.4	정책 및 지침 점검	●	●
		11.5	침해사고 정책	●	●
12	백업관리	12.1	백업절차와 계획수립	●	
		12.2	백업복구관리	●	
13	AP관리	13.1	AP 보호		●
		13.2	SSID 계정관리		●
		13.3	SSID 계정주기		●
		13.4	WEP키 사용관리		●
		13.5	WEP키 사용주기		●
		13.6	MAC주소 사용관리		●
		13.7	AP 연장		●
		13.8	채널 관리		●

		13.9	전파 조절		●
14	보안정책	14.1	보안 평가	●	●
		14.2	취약점 조사	●	●
15	무선장비 관리	15.1	장비 목록관리		●
		15.2	장비사용자 기록관리		●
		15.3	패치 및 업그레이드		●
		15.4	인증 및 접근관리		●
		15.5	바이러스 관리		●
16	서비스관리	16.1	무선 서비스 영역		●
		16.2	무선 서비스 품질		●

3. 기술영역

보안과 신뢰성 확보를 위한 보안 기술이나 자원 운용, 인증 방법, 통신망 유효 영역의 확장에 대한 평가기준을 제안한다.

[표 3] 유·무선 통합 IDC의 기술영역 평가기준

구분			항목	유선	무선
1	침입차단 기술	1.1	침입차단시스템	●	●
		1.2	라우팅 장비의 활용	●	●
2	침입탐지 기술	2.1	침입탐지시스템	●	●
3	시스템취약성 진단기술	3.1	시스템 취약성 진단시스템	●	●
		3.2	취약성 분석	●	●
4	바이러스 대응기술	4.1	바이러스 진단	●	●
		4.2	바이러스 대응 및 예방	●	●
		4.3	바이러스 조치	●	●
5	인증기술	5.1	사용자 인증을 위한 암호화	●	●
		5.2	사용자 인증	●	●
		5.3	인증 방법	●	●
6	접근통제 기술	6.1	접근감시기능	●	●
		6.2	접근통제기술	●	●
7	자원운영	7.1	데이터관리	●	●
		7.2	데이터전송	●	●
		7.3	기록매체	●	●
		7.4	데이터암호화	●	●
8	자료유출 방지기술	8.1	자료유출에 대한 대처	●	●
		8.2	도청 방지	●	●
		8.3	데이터 암호화	●	●
9	장애대처 기술	9.1	장애감지	●	●
		9.2	장애복구기술	●	●
10	통신망 영역	10.1	데이터교환망	●	
		10.2	접근 및 단말장치	●	
		10.3	전송망	●	
		10.4	전용 및 가변형 회선망	●	
		10.5	통신관리망	●	
		10.6	장애 극복		●
		10.7	유효영역 확장		●
11	백업기술	11.1	백업체제 구축	●	
		11.2	백업방식	●	
		11.3	백업대상과 범위	●	
		11.4	보관 및 관리장소	●	

V. 결 론

IDC는 태동한지 채 10년도 안되었지만, 이제는 일반 기업의 사적 시설이 아니라 국가의 중요한 시설로 인식되고 있다. IDC 시설은 통신망서비스와 부대시설 및 장비를 이용하는 업체들에 대해서 안정된 서비스를 보장해 주어야 한다. 이를 위해서는 무엇보다도 변화된 유·무선 통합 환경에서의 안전성과 신뢰성을 보장할 수 있는 지침이나 평가기준 마련은 시급한 일이라 볼 수 있다.

이에 본 논문에서는 집적정보통신시설보호지침 및 무선랜 보안 운영 권고지침, 국내·외 정보보호 관련 지침 및 권고사항을 분석한 자료를 바탕으로 유·무선 통합 환경에서의 IDC 평가기준을 제안하였다. 본 논문에서 제안한 평가기준이 실제 IDC 시설에 대해 적용 된다면 유·무선 통합 환경의 IDC 시설에 대한 보다 안전하고 신뢰성을 담보할 수 있는 고품질의 서비스가 실현될 수 있을 것이다.

▌참 고 문 헌▐

[1] http://www.kisa.or.kr

[2] "IDC 보안 실태조사를 통한 집적시설의 보호대책에 관한 연구", 한국정보보호진흥원, 2001.11

[3] ITU-T Recommendation M.3200, "TMN management services and telecommunications managed areas"

[4] 무선랜 보안 표준과 구현 방안, WSF, 2003.10

[5] BITS Mobile Financial Services, 2002

[6] "IDC 안전·신뢰성 평가항목 연구", 정보보호진흥원, 2002. 12

[7] "무선환경의 IDC에 대한 안전·신뢰성 평가방법 연구", 정보보호진흥원. 2003. 12