情 報 保 護 學 會 誌
第18卷 第3號, 2008. 6

U-정보사회에서의 포괄적 네트워크 보안관리 방안

김 영 진*, 권 헌 영**, 임 종 인***

요 약

정보통신 기술의 급속한 발전은 언제, 어디서나 전 세계 네트워크에 접속할 수 있는 유비쿼터스 시대를 가능하게 했다. 이는 모바일 장치 등 새로운 엔드포인트 단말을 기존 게이트웨이 중심의 네트워크 보안 인프라에 통합시킨 새로운 개념의 네트워크 보안 인프라를 출현시켰다. 본 논문에서는 향후 국가 정보통신망 보호를 위해 자리 잡을 새로운 보안 인프라의 중심으로인 네트워크 접근통제(Network Access Control)의 개념과 요소 기술을 살펴보고, 바람직한 네트워크 접근통제 정책 수립을 위해 반드시 고려해야 할 포괄적 네트워크 보안관리 방안을 제시하고자 한다.

Ⅰ. 서 론

1998년 모리스가 네트워크 환경 속에서 자기 자신을 복제하며 네트워크를 통해 전파되는 웜을 만든 지 20년이 지난 지금, 세계는 이미 인터넷이라는 단일 네트워크로 연결되어 있으며 언제 어디서나 네트워크로의 접속이 가능한 유비쿼터스 시대가 되었다. 이러한 거대하고 복합적인 네트워크 환경이 구축되면서 이를 악용하고자 하는 사이버 공격 또한 지능화·고도화 되고 있으며, 그 목적 역시 개인 및 기업, 국가의 중요정보 유출과 같은 형태로 변화하고 있다.

그동안 국가 및 기업의 네트워크 최전방에 위치한 침입차단시스템 및 바이러스 월 등으로 대표되는 게이트웨이 중심의 네트워크 보안 인프라는 외부의 사이버 공격으로부터 어느 정도의 효과를 거두어 왔다.

하지만 유·무선 네트워크 환경의 통합화, 엔드포인트 단말의 다양화, 기업 비즈니스 환경의 확대 등으로 보안상 취약한 노트북이나 출장지 등의 원격지 컴퓨터를 이용해 조직 내부 네트워크에 접근하는 것이 일상적이 된 지금 내·외부 네트워크 경계를 구분하는 기존의 보안 인프라는 한계 상황에 직면해 있다. 즉, 게이트웨이 중심의 보안을 아무리 강화한다고 하더라도 조직 내부의 침해사고는 끊임없이 발생하고 있다. 그렇다면 왜 아직도 윈도 운영체제의 보안 취약점을 이용해 공격하는 새로운 형태의 공격이 계속 나오는 것일까?[1]

가장 근본적인 이유는 위협요소가 취약성이 있는 사용자 및 엔드포인트 단말에 존재하기 때문이다. 또한 사용자 수준의 안티-바이러스나 개인 방화벽과 같은 보안체계를 마련한다 해도 운영체제에 적절한 보안패치를 수행하지 않는 등 보안관리가 미흡하기 때문이다.

이러한 문제점은 엔드포인트 단말 및 사용자 수준의 보안대책이 얼마나 취약한지 여부를 보여주는 것이다. 외부 공격자는 이미 기업의 대부분이 침입방지시스템 등을 이용한 외부의 공격을 적절히 차단하고 있다는 것을 잘 알고 있으며, 보안관리가 취약한 엔드포인트 단말로 공격의 방향을 전환한 것이다. 적절한 보안정책이 수립되지 않은 엔드포인트 단말들이 이런 공격의 대상이 되고 있으며, 공격 당한 시스템은 공격자의 숙주가 되어 내부 네트워크 전체를 위협하는 존재가 되고 있다.[4]

이러한 이유로 인해 엔드포인트 단말에 보안을 네트워크 수준에서 포괄적으로 다루는 새로운 보안 인프라에 대한 필요성이 제기되었으며, 부적격 엔드포인트 단말에 대한 적절한 통제를 기존 게이트웨이 중심의 보안 인프라 속에서 통합하는 과정에서 네트워크 접근통제(Network Access Control, 이하 NAC라 한다) 개념으로 정립되었다.[1,3]

본 논문에서는 향후 국가 정보통신망 보호를 위해 핵심 인프라로 적용될 NAC의 개념과 요소 기술을 살펴

* 고려대학교 정보경영공학전문대학원 정보보호정책 연구실 (yjkim243@korea.ac.kr)
** 광운대학교 과학기술법과대학 교수 (kyu@kw[1].ac.kr)
*** 고려대학교 정보경영공학전문대학원 교수 (jilim@korea[1].ac.kr)

보고, 올바른 NAC 정책 수립을 위해 반드시 고려돼야 할 포괄적 네트워크 보안관리 방안을 제시하고자 한다.

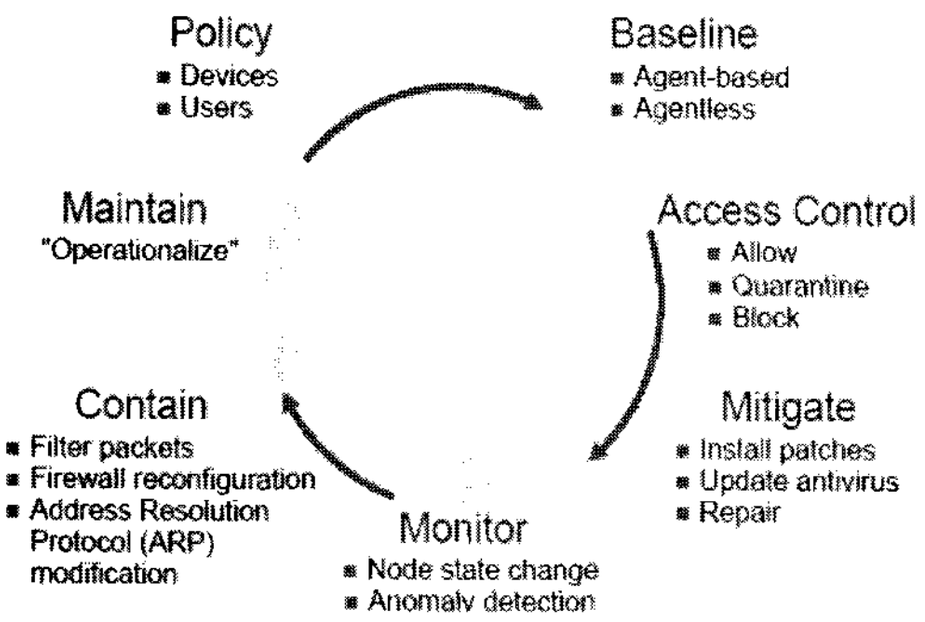
Ⅱ. 네트워크 접근통제(NAC)

2.1 NAC 개념 및 목적

NAC은 모든 네트워크에 접근하는 모든 엔드포인트 단말의 보안을 강제화 할 수 있는 보안 인프라(H/W 및 S/W)를 말하는 것으로, 인가된 사용자가 안전성이 검증된 단말을 이용하여 네트워크 자원을 접속하는 프로세스를 가능하게 한다.[1]

즉, 엔드포인트 단말이 내부 네트워크에 접근하기 전에 보안정책의 준수 여부를 검사해 네트워크 접속을 통제하고 다양한 네트워크 장비와 솔루션과의 유기적인 협력을 통해 엔드포인트 단말에 대한 통제를 수행하는 보안 인프라를 구성하는 것이다. 이는 사용자단의 보안기술을 기존 네트워크 보안관리 솔루션과 결합해 전체 네트워크에 통합 보안 인프라를 구현함으로써 새로운 위협의 출현을 사전에 예방하는 것을 목적으로 한다.

가트너社는 다양한 NAC에 대한 개념을 정리하기 위해 [그림 1]과 같은 네트워크 접근통제 모델[6]을 제시하였다. 이 모델에 의하면 NAC은 엔드포인트 단말에 대한 보안정책 및 보안관리 상태에 대한 평가결과를 기반으로 하여 네트워크 접근의 허용, 격리 및 치료, 보안정책 준수에 대한 지속적인 모니터링 및 유지관리를 수행하는 프로세스로 정의된다.



〔그림 1〕 가트너社의 NAC 프로세스 모델

2.2 NAC 구분 및 적용범위

일반적으로 NAC은 네트워크에 접속하는 사용자를 인증하고 사용자 단말기가 적정 수준의 보안정책을 준수하고 있는지 여부 확인, 결과에 따라 네트워크 접속을 통제하거나(또는 치료하는) 일련의 프로세스와 목적은 동일하지만 구현방식에 따라 다음과 같이 구분된다.

2.2.1 사전 접근허용 vs. 사후 접근허용 방식

NAC은 엔드포인트 단말의 네트워크 접속을 허용하기 전, 후에 보안정책을 강제화 하느냐에 따라 사전 접근허용 방식과 사후 접근허용 방식으로 구분된다.

사전 접근허용 방식의 경우 엔드포인트 단말에 대한 네트워크 접속이 허용되기 이전에 단말의 보안상태에 대한 점검이 수행된다. 예를 들면, 안티-바이러스 제품의 최신 패턴 업데이트가 이루어지지 않은 단말은 네트워크 접속을 차단하는 것이다. 이에 반해 사후 접근허용 방식은 사용자에 대한 네트워크 접속을 허용한 후 사용자 행동에 대한 모니터링을 통해 보안정책 준수를 강제화 하는 것이다.

2.2.2 에이전트 vs. 비-에이전트 방식

NAC의 기본적인 개념은 네트워크를 접속하는 엔드포인트 단말 또는 사용자에 대한 보안상태 정보를 어떻게 획득하느냐에 따라 에이전트 방식과 비-에이전트 방식으로 구분된다.

에이전트 방식의 경우 각 엔드포인트 단말에 설치된 특정 소프트웨어가 단말의 보안상태에 대한 정보를 수집·보고하며, 비-에이전트 방식의 경우 기존 네트워크 장비 및 솔루션 등을 활용한 원격 스캐닝을 통해 엔드포인트 단말에 대한 보안상태 정보를 수집·보고한다.

2.2.3 기존 인프라 활용 vs. 전용 장비 방식

NAC은 엔드포인트 단말 또는 사용자에 대한 보안정책 준수를 강제하는 것이 스위치 등 기존 네트워크 인프라를 활용하느냐, 전용 장비를 이용하느냐에 따라 구분될 수 있다.

기존 인프라 활용 방식의 경우, 각 엔드포인트 단말에 설치된 에이전트가 단말의 보안상태 정보를 수집·보고하고, 이에 따라 스위치 등 네트워크 장비를 활용해 접근통제를 수행한다. 이에 반해 전용 장비 방식은 침입차단시스템과 같이 독립된 형태로 구성되어 모든 네트워크 패킷에 대해 보안정책 준수 여부를 확인한다.

Ⅲ. NAC 표준화 및 보안기술

NAC은 네트워크에 접근하는 모든 엔드포인트 단말의 보안을 강제화 할 수 있는 보안 인프라를 말하는 것으로, 조직에 구축된 엔드포인트 보안 및 네트워크 보안 장비 등에 따라 다양한 형태를 가질 수 있다.

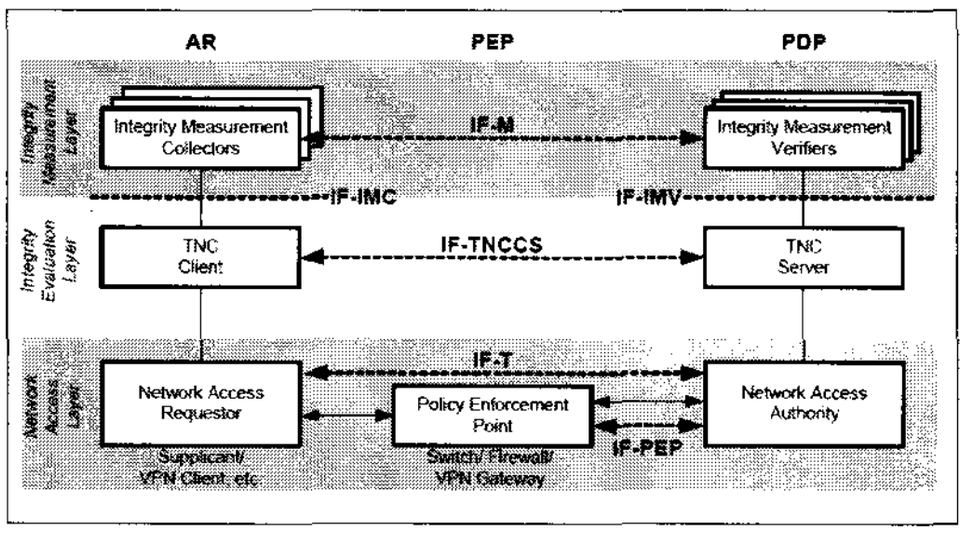
본 장에서는 네트워크 보안 인프라 관련 국제표준 규격을 제정하는 TCG(Trusted Computing Group) 및 IETF(Internet Engineering Task Force)에서 제안한 NAC 표준 아키텍처를 살펴보고 여기서 제공하는 보안 기술에 대해 설명한다.

3.1 NAC 표준 아키텍처

3.1.1 TCG, TNC(Trusted Network Connect)

TCG는 이기종 컴퓨팅 환경에서의 컴퓨팅 플랫폼을 강화시키기 위한 목적으로 만들어진 비영리 단체로, 2004년 TNC 서브 그룹을 발족하면서 NAC에 대한 산업 표준화 아키텍처를 제안하였다.

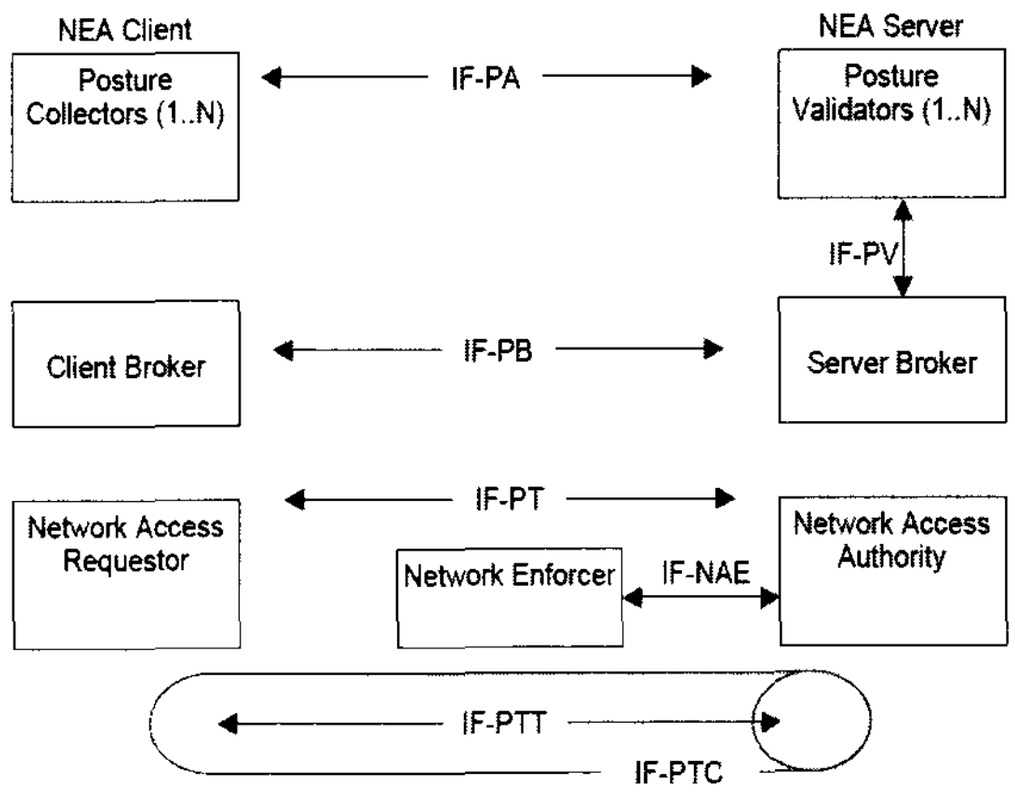
TNC 모델[7]에서는 엔드포인트 단말의 보안상태 평가, 격리, 치유 기능을 구현하기 위해 [그림 2]와 같이 AR(Access Requestor), PEP(Policy Enforcement Point), PDP(Policy Decision Point)의 3가지 컴포넌트 구조를 채택하고 있으며, 기능 레이어별로 역할을 구분하고 있다.



〔그림 2〕 TNC 표준 아키텍처

3.1.2 IETF, NEA(Network Endpoint Assessment)

NEA는 현재 IETF 내에 작업반이 만들어진 상태로 엔드포인트 단말의 네트워크 접근을 평가하는 규격을 제정하는 역할을 수행한다. NEA 아키텍처[8]에서는 [그림 3]과 같이 클라이언트, 서버의 2가지 컴포넌트 구조



〔그림 3〕 IETF 표준 아키텍처

를 채택하고 있으며, 이들 간의 데이터 전달과 흐름에 사용되는 프로토콜을 정의하고 있다.

3.2 NAC 보안기술

NAC은 보안기술은 기존 엔드포인트 보안기술을 기존 네트워크 보안관리 장비 및 솔루션과 결합해 전체 네트워크에 통합 보안 인프라를 구축하는 개념으로 다음과 같이 3가지 요소기술로 대표된다.[2]

3.2.1 사용자 인증기술

사용자 인증기술은 엔드포인트 단말 및 사용자 인가에 대한 검증기능으로, 제공되는 기능이 구현된 네트워크 계층에 따라 [표 1]과 같이 구분된다.

〔표 1〕 사용자 인증기술

구분		설명
L2	IEEE 802.1x	• 유·무선 랜 접근제어 표준으로 클라이언트 S/W 탑재 필요 • 네트워크 장비가 802.1x를 지원해야만 구축 가능하며, 가장 뛰어난 보안성 제공
	MAC	• 주로 ARP를 이용, 단말 유형과 무관하게 적용 가능 • 네트워크별 별도의 독립 장비 설치 필요
L3	IP	• IP 관리 제품의 고유 기능 차용
	IPSec	• 주로 VPN에서 사용되는 인증 메커니즘 사용
	DPI	• L7 네트워크 장비를 이용한 경우 인증 패킷을 분석하여 인증 여부 확인

구분		설명
L3	인증 토큰	• 인증 단말에 네트워크 접근을 위한 토큰 발행
	SSL	• 웹을 이용한 사용자 인증
	DHCP	• DHCP 옵션 필드를 이용한 사용자 인증 또는 단말 MAC 주소를 이용한 인증
	기타	• 네트워크 방화벽이 주로 사용

3.2.2 격리 및 강제기술

격리 및 강제기술은 네트워크 접근통제가 이루어지는 NAC의 핵심기술로, 기능이 구현된 방식에 따라 [표 2]와 같이 구분된다.

〔표 2〕 격리 및 강제기술

구분			설명
클라이언트	전용 ACL Driver		• 주로 Outbound 패킷통제를 위한 간략한 형태의 Driver • 3rd-Party 단말 보안 솔루션 연동 형태의 제품의 탑재
	HIPS, PC F/W		• 에이전트와 연계된 HIPS, F/W 등을 이용하여 구현 • 단말 보안기능을 내장한 형태의 제품에서 제공
네트워크	스위치	ACL	• 단말 접속 포트별 ALC을 조정하여 구현
		802.1x VLAN	• 802.1x를 이용한 동적 VLAN 적용 또는 Switch의 자체기능 이용 • 단말의 상태 변경에 대한 대응이 관건
	DHCP		• 격리 대상 IP Pool을 미리 설정하고 정책 미준수 단말인 경우 격리 및 강제화 구현 • 보안성이 낮으며, Static IP 설정에 취약
	보안장비	NIPS, F/W	• 네트워크 보안장비 형태 적용
	전용장비	In-line	• 방화벽을 각 Switch 포트나 Uplink에 배치하는 것과 유사
		Passive	• 패킷 Mirroring과 ARP Poisoning을 이용한 격리 및 강제화 구현

3.2.3 베이스라인 기술

베이스라인 기술은 보안정책이 먼저 수립되고 나서, 네트워크에 접속하려는 접속 단말의 상태가 먼저 수립된 보안정책과 일치하는지 여부를 점검하는 기술로 [표 3]과 같은 형태로 구현된다.

〔표 3〕 베이스라인 기술

구분		설명
에이전트 기반	3rd Party Plugin	• 자체 점검 가능한 부분을 제외하고는 기존의 단말 보안솔루션과의 연동을 통해 관련 정보를 수집
	Integrated Agent	• 정책 점검을 위한 정보 수집을 기존 Legacy 단말 보안 솔루션과 중복 수행 가능성 존재
비에이전트 기반	경량 Agent	• Active-X, Java 등을 이용하여 Agent 배포 및 설치 간편성을 향상시킨 방법
	네트웍 스캐닝	• nmap, wmi 등 원격에서 단말 상태 정보를 수집할 수 있는 기술을 이용한 방법 • 원격 접근권한 필요시 제한적일 수 있음
	DPI	• 주로 In-line 형태의 전용장비 또는 NIPS, Firewall을 이용
	NBA	• 주로 Passive 형태의 전용장비

Ⅳ. U-정보사회에서의 포괄적 네트워크 보안관리 방안

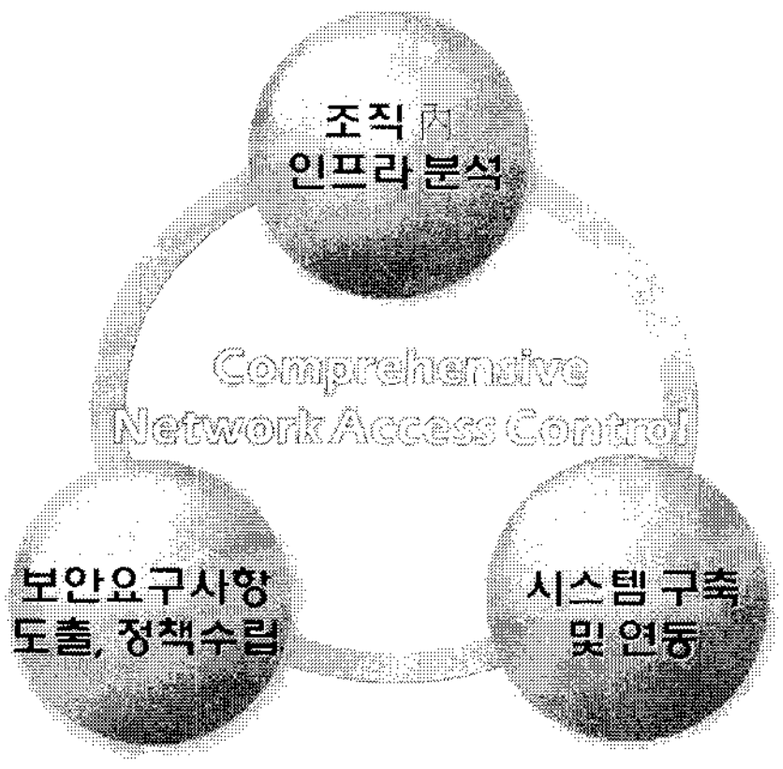
NAC은 정보사회의 발전에 따른 잠재적 위험을 최소화하고 알려지지 않은 외부 위협요인을 사전예방 할 수 있는 보안 인프라를 제공하지만, 엔드포인트 단말 및 보안기능의 적용범위, 기존 네트워크 인프라와의 통합 등 다양한 요소들에 의해 신뢰성이 결정된다. 따라서 바람직한 NAC 구축 및 운영을 위해서는 다음과 같은 사항들을 반드시 고려하여 포괄적인 네트워크 보안관리가 이루어질 수 있도록 해야 한다.

4.1 변화하는 비즈니스 환경을 고려한 포괄적 보안관리 프로세스 수립

무선 모바일 환경의 확대, 접속 엔드포인트 단말의 다양화, 내부 네트워크에서의 무선랜 활용 및 외부와의 협업 증가 등 IT 비즈니스 환경의 변화는 IT 인프라의 끊임없는 진화를 필요로 한다.

이는 결과적으로 관리·보호해야 할 대상을 끊임없이 증가시켜 IT 인프라의 복잡성을 증가시킨다. 복잡성이 높아지면 이에 비례하여 예측 불가능한 잠재적 위험이 증가하며, 이에 대처하기 위한 보안대책 또한 복잡성이 증가한다.

이러한 복잡성이 높은 환경에서는 알려지지 않은 위협을 최소화하기 위해 사후 대응이 아닌 사전 예방적이



〔그림 4〕 포괄적 보안관리 프로세스

고 포괄적인 보안관리가 요구된다. 사전 예방적이란 잠재적 보안위협에 효과적으로 대응할 수 있고 조기경보 시스템 등을 통해 사전 조치가 가능한 보안환경을 의미하며, 포괄적이란 네트워크 경계만을 고려하는 것이 아닌 조직 전체 자원이 유기적인 협력관계를 통해 관리되는 것을 의미한다.

이를 위해서는 조직 내 사용자, 엔드포인트 단말, 네트워크 장비 등 모든 자산이 [그림 4]와 같은 순환적 관리 프로세스를 통해 비즈니스 환경 변화에 즉시 대응할 수 있어야 할 것이다.

4.2 잠재적 위험을 고려한 위험분석 방법론 개발

조직 내 IT 인프라의 효율적인 보안관리를 위해서는 위험분석이 필수적으로 요구된다. 일반적으로 최적의 정보시스템 보안관리 체계를 구축하기 위한 위험분석은 조직의 정보시스템 운영환경을 분석하고, 보안취약점과 이를 위협하는 요인을 파악하여 효율적인 대응책을 찾는 프로세스를 갖는다.

그러나 이러한 기존의 위험분석 방법론은 새로운 정보기술에 의한 예측 불가능한 잠재적 위험에 노출된 유비쿼터스 환경에 적용하는데 한계를 가진다. 특히 유비쿼터스 시대의 IT 인프라의 핵심기술인 RFID, USN, VoIP, BcN, Wibro 등의 잠재적 취약성과 정보 침해 가능성은 다양한 잠재적 위험을 내포하고 있어 기존 위험분석 방법론의 적용이 어려워진다.

이는 잠재적 위험을 평가할 수 있는 새로운 위험분석 방법론에 대한 연구가 필요함을 의미한다. 하지만 아직 국내·외적으로 이러한 잠재적 위험(불확실성)에 대한 위험평가 연구는 미흡한 실정이다.

따라서 퍼지 이론(fuzzy theory), 신념 모델(belief model) 등과 같은 불확실성을 평가할 수 있는 다양한 이론[5]을 적용한 위험분석 방법론에 접목, 유비쿼터스 환경에 맞는 새로운 방법론을 개발해 나가야 할 것이다.

4.3 시스템 연동 및 인터페이스 표준 개발

새로운 정보기술의 출현과 디지털 컨버전스 현상은 조직 내 IT 인프라와 새로운 정보기기와의 연동을 필요로 한다. 특히 유비쿼터스 환경에 의해 다양한 엔드포인트 단말들이 조직 내 네트워크에 결합된다면 연동을 위한 복잡도는 엄청나게 증가할 것이다.

이러한 복잡한 연동 문제를 효율적으로 해결하기 위한 합리적 기준이 바로 표준이다. 특히 정보기술 등에 적용되는 신기술에 대한 선행적 표준화는 첨단 산업기술의 기반이 될 수 있을 뿐만 아니라 조직 내 일관된 보안정책을 수립·시행하는데 중요한 수단이 된다.

따라서 바람직한 NAC 구축 및 운영을 위해서는 조직 내 IT 인프라에 포함된 모든 엔드포인트 단말 및 네트워크 장비 등에 대해 상호 연동을 위한 인터페이스 및 프로토콜이 표준화 되어야 한다. 이러한 표준화는 엔드포인트 단말에 대해 수립된 보안정책이 조직의 네트워크 환경에서 적절히 준수하고 있는지의 여부를 확인할 수 있는 통제수단을 제공하며, 새로운 정보기술의 출현으로 인한 IT 환경 변화에 능동적으로 대처해 나갈 수 방안을 제시해 줄 것이다.

4.4 새로운 정보기술에 대한 보안성평가 확대

앞서 말한 바와 같이 새로운 정보기술의 급속한 출현이 가져올 잠재적 위험 증가는 새로운 엔드포인트 단말 및 네트워크 장비 등에 대한 보안성 평가방안을 요구한다. 사전 검증된 정보기술의 조직 내 사용은 새로운 정보기술이 가져올 예측 불가능한 위험을 최소화하고 신뢰성을 확보하기 위한 핵심적인 기술이라고 할 수 있다.

현재 국내에는 CC인증 및 암호검증 등 다양한 IT 정보기술의 보안성 평가제도가 운영되고 있다. CC인증제도는 2006년 5월 우리나라가 국제상호인정협정(CCRA)에 가입하게 되면서 국제공통평가기준에 따라 IT제품에 적용된 보안기술의 안전성을 평가, 신뢰성을 확보하는 것으로 최근에는 VoIP·WLAN 등 첨단기술에까지 활

용되고 있으며, 암호검증제도는 정보통신망을 통해 유통되는 중요정보의 위·변조, 훼손, 유출 등을 방지하기 위해 사용되는 암호기술의 안전성을 평가하기 위해 적용되고 있다. 이러한 평가제도를 통해 모든 정보기술은 적절한 신뢰성을 확보할 수 있으며, 그 사용 및 발전여부가 사용자들에 의해 결정되는 것이다.

하지만 이러한 평가제도는 새로운 정보기술의 변화를 모두 수용하기에는 어려움이 존재한다. 따라서 지속적인 해외 평가제도에 대한 벤치마킹을 통해 새로운 정보기술에 대한 평가의 효율성을 제고하고 활성화할 수 있는 방안에 대한 연구가 필요하다.

4.5 국내·외 IT 컴플라이언스 준수 환경 조성

국내·외적으로 각종 규제에 대해서는 갈수록 철폐하고 완화해 가고 있는 경향이나 IT 비즈니스 환경의 급격한 변화는 국가를 비롯한 개인의 보안관리 문제에 있어 오히려 규제의 범위와 강도를 과거보다 강화해야 한다는 의견이 제기되고 있다.

이는 개인정보보호법들과 SOX, HIPPA 등 국내·외 IT 컴플라이언스들이 억지로 지켜야 하는 번거로운 규제가 아니라 예측 불가능한 잠재적 위험요소들을 사전에 억제하고 관리할 수 있도록 해주는 안전장치임을 인식했기 때문이다. 삼성·현대 등 세계 시장에 진출에 있는 국내 기업들이 적절한 컴플라이언스를 준수하지 않음으로 인해 못해 국제 경쟁력을 잃지 않기 위해서는 이 문제가 더욱 중요하다.

컴플라이언스와 관련하여 기업들이 겪고 있는 가장 큰 어려움은 각종 규제 정보들이 국가·기관별로 산재해 있어 이를 파악하기가 어렵다는 점이다. 준수 여부와 상관없이 그 구체적 내용의 파악 자체가 쉽지 않은 것이다. 따라서 현재 국내·외 운영중인 다양한 IT 컴플라이언스에 대한 벤치마킹과 분석을 통해 국내 기업들에게 합리적인 대응방안을 제시해 줄 수 있는 기구의 운영이 필요하다. 또한 컴플라이언스를 준수하는 경우 적절한 인센티브를 제공하고, 준수하지 못했을 경우 불이익과 제재를 받을 수 있도록 함으로써, IT 컴플라이언스 준수를 유도할 수 있는 활성화 방안이 검토되어야 한다.

V. 결 론

정보기술의 발전에 따른 유비쿼터스 시대로의 진입은 정부·기업·개인들을 예측 불가능한 잠재적 위험에 직면하게 했다. 2003년 1월 국내에서 발생한 인터넷 대란, 2007년 5월 인터넷 강국 에스토니아에서 발생한 사이버테러는 이러한 위험이 현실화됨으로써 국가 전반에 미칠 수 있는 영향력을 짐작해 볼 수 있다.

이러한 때 NAC은 제로-데이(Zero-Day) 공격과 같은 보안위협으로부터 네트워크 접속을 차단·격리하고 내부자원을 보호하여 신뢰된 국가 네트워크 환경을 구축하는데 최고의 대안으로 고려되고 있다. 즉, NAC은 u-정보사회에 적합한 네트워크 자산의 자동화된 통합관리를 가능하게 한다.

이를 위해 국가나 기업은 사용자 및 엔드포인트 단말, 네트워크 장비를 포괄할 수 있는, 능동적인 대응이 가능한 IT 인프라를 구축해 나가야 한다. 단말 장치에 대해 수용 가능한 범위의 보안정책을 수립해 나가야 하고, 해당 엔드포인트 단말 및 네트워크 장비들이 수립된 보안정책을 준수하는지에 대한 확인과 통제가 최대한 보장될 수 있는지 확인해야 하며, 이를 전체 IT 인프라로 지속적으로 확산시켜 나가려는 노력을 계속해야 한다. 또한 기존 IT 환경에 큰 변화를 요구하지 않고 모든 IT 인프라에 적용이 가능하도록 기술적인 개발과 투자도 지속 확대해야 할 것이다.

하지만 표준화의 부재로 인한 호환성 미비, 새로운 기술과 기존 IT 인프라와의 통합을 위한 지속적인 투자는 국가 및 기업, 개인 모두가 신뢰된 국가 정보통신망 환경 구축을 위해 지속적으로 노력해 나가야 할 과제이다.

참고문헌

[1] 김태형, "NAC 네트워크 보안 해결사 될까", 정보보호 21C, 3(2), pp. 40-46, 2008.5

[2] 박현미, "NAC 기반 및 기반기술 분류에 따른 제품군 분석", KISA TR, 2008.3

[3] 안호천, "기업 내부보안의 파수꾼, NAC" CIO Korea, 2007.3

[4] 최용, "NAC와 안티 바이러스 연동 제어 및 업계 동향", 네트워크 타임즈, 2006.8

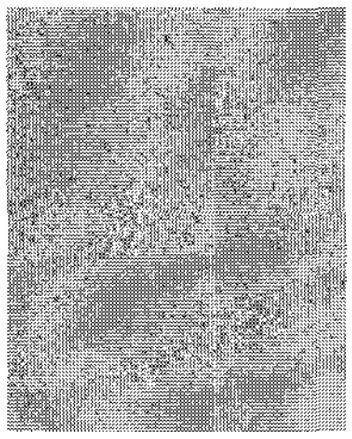
[5] 최승, "불확실성을 고려한 위험분석 방법론 연구", KIPS 논문집 제11권 제2호, 2004.11

[6] Gartner, Network Access Control Market Overview, 2004.12

[7] TCG TNG,

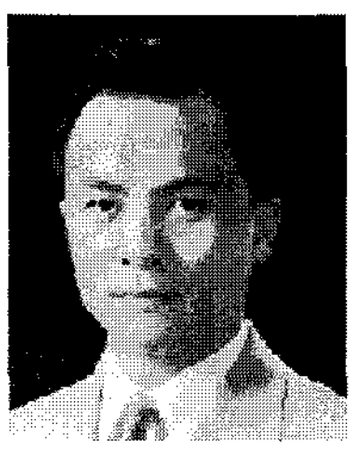
https://www.trustedcomputinggroup.com
[8] IETF NEA,
http://www.ietf.org/html.charters/nea-charter.html

〈著者紹介〉



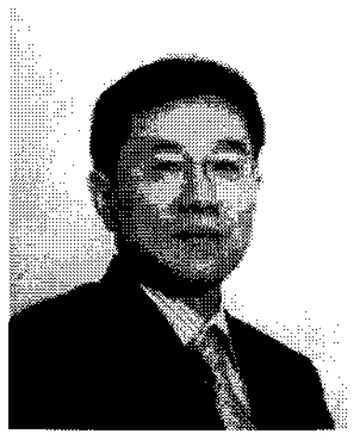
김 영 진 (Kim Young Jin)

2007년 6월~현재 : 고려대학교 정보경영공학전문대학원 박사과정
<관심분야> 정보보호, 정보보호정책, 평가인증, 프라이버시 보호



권 헌 영 (Kwon Hun Yeong)

2005년 3월~현재 : 광운대학교 과학기술법학과 교수
<관심분야> 정보통신정책, 사이버범죄, 법 · 제도



임 종 인 (Lim Jong In)

종신회원

2006년 10월~현재 : 고려대학교 정보경영공학전문대학원 원장
<관심분야> 정보보호, 암호화, 정보보호정책, 프라이버시