

정보보안 및 정보시스템자산 관리를 위한 내부 감시·통제시스템

An Internal Surveillance and Control System for Information Security and Information System Asset Management

윤한성 (Han-Seong Yoon)

경상대학교 경영대학 경영학부 교수

요약

그동안 기술적으로 관심을 가져온 외부 정보위협의 방지를 위한 방화벽, 침입탐지시스템, 악성코드 백신 등의 보안수단은 피해금액이나 사고건수 면에서 다수를 차지하는 내부 정보보안 위협에 대해서는 거의 효과적이지 않다. 본고에서는 컴퓨터를 통한 내부 정보보안 위협을 방지하기 위해 정보시스템 사용에 대한 감시와 통제가 가능한 시스템에 대하여 구조와 특징, 세부기능과 개발방식 등을 정리하였다. 그리고 정리한 내용을 바탕으로 실제 개발사례가 되는 시스템을 통해 구현될 수 있는 기능을 설명하였다. 본고에서 제시한 시스템은 개방된 인터넷 환경 또는 모바일(mobile) 컴퓨팅과 같은 정보환경을 위해서는 보다 개선된 형태의 개발이 필요하다.

키워드 : 정보보안, 내부 정보보안 위협, 감시·통제 시스템

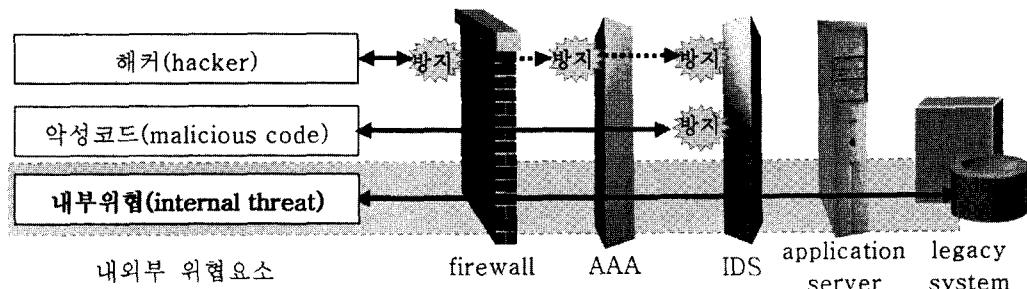
I. 서론

인터넷을 비롯한 통신망에 연결된 정보기기 사용의 확대는 정보처리의 신속정확성 및 효율성과 더불어 정보 및 정보시스템에 대한 정보보안 위협(information security threat)에 대처해야 하는 문제를 심화시키고 있다. 이러한 정보보안위협의 근원지(source)를 고려할 때, 외부위협(external threat)보다는 조직내부의 구성원에 의해 발생하는 내부위협(internal threat)의 심각성이 큰 것으로 지적되고 있다(홍일유 등, 1996). 그리고 주로 조

† 본 연구는 ‘(주)아이템시스템’의 지원 하에 진행되었음.

직구성원 개인별 컴퓨터사용으로 이루어지는 업무환경은 기업전체의 정보시스템자산(하드웨어 또는 소프트웨어) 관리에 어려움을 초래하기도 한다. 내부위협에 의한 정보보안 사고의 사례로서는 종업원의 인터넷을 통한 기업 비밀자료의 불법유출을 들 수 있으며, 정보시스템자산 관리의 어려움으로는 허용되지 않은 소프트웨어의 설치나 개인용 컴퓨터에서 미등록 하드웨어의 사용 등을 사례로 들 수 있다.

그리고 정보보안상의 내부위협은 조직구성원이 사용하는 컴퓨터를 비롯한 기업의 정보시스템 자산을 통해 이루어질 뿐만 아니라 정보시스템자산의 사용에 대한 적절한 통제가 이러한 내부 위



〈그림 1〉 보안도구를 통한 보안위협 방지

협을 방지할 수 있다고 본다면, 정보보안상의 내부위협 방지와 정보시스템자산 관리의 두 측면은 서로 밀접한 관계를 가진다고 할 수 있다. 또한 인터넷을 통한 정보유출 또는 불법복제 등과 같이 조직구성원에 의해 실행되는 내부위협에 대해서는 <그림 1>처럼 외부의 해커나 악성코드 등의 외부위협의 방지에 대해 널리 활용되는 방화벽(firewall)이나 사용자인증(AAA: authentication, authorization, accounting) 또는 침입탐지시스템(IDS: intrusion detection system) 등의 보안도구를 통해 완전한 방지가 사실상 불가능하며, 기업내부의 접근가능한 시스템이나 데이터베이스에 대해 정보보안상의 잠재적인 또는 실질적인 위협요소가 된다.

본고에서는 LAN으로 구성되는 조직내부의 정보환경에서 개별 조직구성원이 사용하는 컴퓨터에 대해 사용내역의 실시간 감시(surveillance) 또는 사용권한을 통제(control)하고, 설치되어 사용하는 하드웨어 및 소프트웨어의 전반적인 사항을 통합하여 관리하는 내부 감시통제시스템(internal surveillance and control system, 이하 'ISCS'라고 함.)에 대하여 정보보안 관리상의 가치, 구성기능, 구현사례 등을 중심으로 정리하고자 한다. 동 시스템은 이상에서 언급한 '내부위협에 의한 정보보안'상의 문제해결 및 '조직내부 컴퓨터를 대상으로 하는 정보시스템자산 관리'에 대해 주요 수단 또는 대안이 될 수 있을 것으로 판단된다.

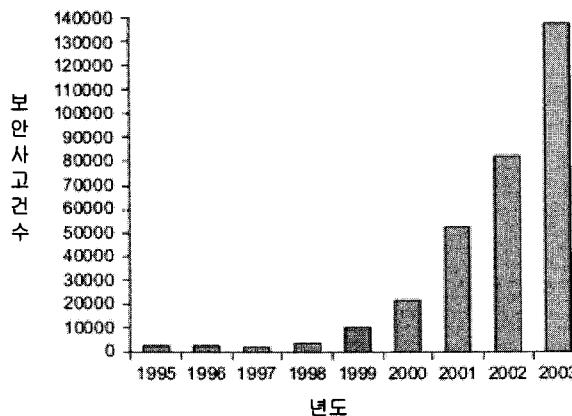
II. ISCS의 목적 및 범위

2.1 정보기반 업무환경과 내부위협

기업의 정보서비스 및 내·외부 정보시스템간 정보교환의 확대는 기업경영의 고도화 및 효율화를 이루고 있는 한편, 조직구성원의 전반적인 정보처리 및 전송과정의 양적 증가에 따라 이에 대한 완전한 관리 및 통제가 사실상 불가능해지고 있다. 다음과 같은 사례는 조직의 내부 구성원에 의한 정보보안위협의 심각성을 짐작하게 한다.

- 기업비밀정보 통제의 어려움과 비권한자의 정보조회
- 내부 구성원의 불법 정보복제 또는 도난·분실에 따른 외부유출
- 휴대용 저장수단(USB, CD 등)을 통한 정보의 무단유출 등

정보보안위협은 보안위협의 근원지(source)에 따라 외부위협(external threat)과 내부위협(internal threat)으로 나누어지는데, 외부위협은 컴퓨터 네트워크를 통한 조직외부로부터의 보안공격(security attack from outside)으로 발생하는 정보보안위협으로서 컴퓨터 바이러스를 포함하는 악의적 코드(malicious code) 또는 해킹(hacking) 등을 포함한다. 내부위협은 주로 조직내부자가 주체가



<그림 2> 정보보안 사고발생 추이

되는 악의적 또는 비고의적 보안침해행위(security violation behaviors)에 기인하여 발생하는 정보보안위협으로서 내부자 위협(insider's threat)이라고도 한다(홍일유 등 1996; Lilian, 2006).

정보보안상의 내부위협은 컴퓨터 기기에 저장된 정보 또는 시스템에 대하여 조직 내부자에 의해 이루어지는 악용·훼손·변조·유출이라고 할 수 있다. 정보보안에 있어서 내부위협은 외부위협보다 피해정도가 보다 심각하며(홍일유 등 1996), 내부자가 사용하는 정보시스템의 다양성, 기업내부 정보처리량 증가 및 인터넷 사용에 따라 그 피해는 증가한다. 최근 미국의 경우, 내부위협에 의한 정보보안상의 연간 피해금액이 외부위협의 그것 보다 50배를 상회하는 2.7백만 달러에 이르는 것으로 조사되고 있다. 또한 <그림 2>에 나타난 전체 정보보안 사고발생수의 80% 이상이 내부위협에 의한 정보보안 사고건수로 파악되고 있다(Herbert, 2004).

기업에서의 업무수행 과정 또는 결과에서 발생하는 기업정보가치의 중요성과 이에 대한 정보보안의 필요성은 지식산업의 고도화와 정비례 하며, 국내 기업의 경우에도 내부 직원의 기밀정보 유출사례 피해가 급증하고 있다(김종원 등, 2003). 정보 유출의 형태를 보면, 주로 컴퓨터 파일(file)로 처

리된 기업정보를 이메일(e-mail) 등을 통한 컴퓨터 네트워크 또는 휴대용 저장장치 등을 활용하는 것으로 알려지고 있다. 이러한 여건에서 지적 정보의 보안이 중요한 단체나 기관에서의 ISCS 도입이 점차적으로 이루어지고 있으며, 기존의 정보보안 도구와 상호보완적인 정보보안의 주요수단이 발전할 것으로 예상된다.

정보보안상의 외부위협에 대해 일반적으로 사용하는 방화벽이나 침입탐지시스템(intrusion detection system), 백신(vaccine) 프로그램 등의 보안수단은 내부위협의 억제수단으로는 효과적이지 않으며(Lilian, 2006; Porter, 2003), 정보시스템의 보안위협 특히 내부위협의 대처수단으로서 감시기술(surveillance technology)에 대한 관심이 커지고 있다. 내·외부 보안위협에 사용되는 정보시스템상의 일반적인 보안도구인 방화벽, 침입탐지시스템, 사용자인증방식 등(<그림 1> 참고)의 일반적인 보안방식과 내부 보안위협에 대한 효과를 <표 1>과 같이 비교해 보면, 정보보안상의 내부위협 방지에는 한계를 가진다. 본고의 시스템은 이러한 내부위협에 대한 기존 보안도구의 한계를 극복하기 위한 주요 수단이 될 수 있다.

정보기술을 통한 감시기술의 응용은 내부 정보시스템 자산 및 내부자의 정보시스템 사용내

<표 1> 보안도구의 보안효과

도구	일반적인 보안방식	내부위협 보안효과
방화벽	- 네트워크 외부로부터의 불법적인 트래픽 유입을 막고, 허가 되고 인증된 트래픽만을 허용(이용준 등, 1998)	- 네트워크 외부로부터의 보안위협에 적절하며, - 내부자에 의한 네트워크 내부 트래픽 통제 및 인증(허가)된 사용자의 정보시스템 사용통제 불가능
침입 탐지 시스템	- 컴퓨터시스템 또는 컴퓨터 네트워크에 대한 외부의 침입을 탐지(유신근 등, 2000)	- 네트워크 외부로부터의 보안위협 또는 내부 네트워크(LAN)을 통한 내부자의 개별 컴퓨터시스템 보안위협에 적절한 보안수단 - 인증(허가)된 사용자의 정보시스템 사용통제 불가능
사용자 인증	- 패스워드 등의 인증방법으로 정당한 사용자(송신자 또는 수신자)인지를 확인(하태용 등, 2004)	- 내·외부 사용자의 적법성을 통한 네트워크, 응용시스템, 테이터 등의 접근을 통제 - 적법한 내부 사용자의 정보시스템 사용통제 불가능

역을 실시간 또는 기간별로 확인할 수 있는 시스템의 개발로 구현될 수 있으며, 이러한 시스템은 조직내부의 정보시스템자산 또는 정보시스템사용 정보를 일방향으로 수집하여 감시(surveillance)하는 기능의 구현을 기본목적으로 한다. 내부위협 방지를 위해 실질적인 정보보안 조치를 위해서는 내부 사용자의 컴퓨터 정보시스템에 대한 기능변경 및 사용 등의 통제(control)기능이 동 시스템의 구현목적에 포함하는 것이 필요하다.

2.2 ISCS의 기능범위

기업내 컴퓨터에 대해 사용자별, 그룹별로 파악하고 사용권한을 설정함으로써 기업 전체의 컴퓨터 기반 정보시스템 자산(하드웨어, 소프트웨어 또는 이를 통해 처리되는 정보 등)을 본고의 시스템으로 실시간 통합하여 파악·관리하는 관리의 통합성과, 원격제어를 통해 필요한 감시 및 통제를 일관적으로 처리하는 시스템 운영의 효율성을 시스템 기능범위의 설정에 있어서의 두 가지 목표로 하였다. 그리고 ISCS의 전체 기능범위를 <표 2>와 같이 ‘내부 감시·통제 정책’, ‘정보시스템 사용통제’, ‘정보시스템 사용감시’, ‘정보시스템자산

관리’ 등의 상하관계를 가지는 4개의 기능범주(functional category)로 구성하였다.

<표 2>의 각 기능범주는 서로 의존적으로 수행되는데, 상위의 기능범주는 하위 범주의 기능 및 처리결과의 기반 위에서 이루어지고 하위 범주의 기능범위는 상위 기능범위의 처리결과에 의해 통제 또는 지원을 받는다. <표 2>에 정리된 ISCS의 기능 범주별 범위와 기능범위간 공유정보는 실제 시스템의 세부기능을 구현하는데 있어서 기본 프레임워크(framework)으로 사용하기로 한다.

III. 시스템 구성 및 세부기능

3.1 시스템 구성 및 환경

기업정보시스템의 일반적인 구성방식인 클라이언트 서버 형태에서는 시스템 사용자 및 시스템 관리자가 각각 업무처리를 위해 클라이언트시스템을 직접 사용하거나 또는 사용지원을 위해 서버시스템을 유지·운영한다. 반면, 일반 시스템과 마찬가지로 클라이언트 서버 구조로 이루어질 수 있는 ISCS는 구성되는 시스템, 감시통제 담당자, 일반 컴퓨터사용자간 구성형태에서 일반적인 경우와 비

〈표 2〉 보안도구의 보안효과

기능범주	범주별 기능범위	상·하위 범주간 전송(공유)정보
내부 감시·통제 정책	- 정보시스템 권한유형 관리 (신규·변경·삭제) - 권한유형별 디폴트(default) 권한 설정/변경 - 내부 감시·통제 평가 및 권한조정	(상위↔하위) • 권한유형, 권한유형별 사용자 그룹 및 기본권한 등 (상위↔하위) • 실제 권한설정치(기본권한과의 차이), 권한의 시도횟수 등
정보시스템 사용통제	- 권한유형별 정보시스템자산에 대한 다음의 접근·사용 분야별 사용·접근의 사용통제 • 하드웨어 및 소프트웨어 • 응용시스템, 데이터, 파일, 네트워크 등 - 개별/그룹별 컴퓨터 원격제어 및 사용통제	(상위↔하위) • 컴퓨터별 사용·접근 권한유형 및 권한설정치 (상위↔하위) • 정보시스템 사용실태
정보시스템 사용감시	- 컴퓨터별 실시간 사용현황 모니터링 • 하드웨어 및 소프트웨어 • 응용시스템, 데이터베이스, 네트워크 등 - 개별 컴퓨터 사용화면의 실시간 조회 및 주기별 사용감시(작업로그 정보 활용)	(상위↔하위) • 정보시스템 사용실태 (컴퓨터별, 활용분야별 등) (상위↔하위) • 컴퓨터별 하드웨어/소프트웨어 변동현황
정보시스템 자산 관리	- 기업내 컴퓨터별 하드웨어/소프트웨어 취득·보유·변경, 사양, 활용도, 과·부족 등 파악 • 개인별, 부서별, 기업전체 등 - 컴퓨터별 정보시스템자원의 원격 관리	

교하여 특징적인 차이를 다음과 같이 정리할 수 있다.

(1) Master Slave 형태

일반적인 클라이언트 서버 형태의 시스템구성과 마찬가지로 ISCS의 서버시스템은 개별 사용자 컴퓨터에 설치된 클라이언트시스템의 통신접속 요청을 대기(listening)하는 형태이나, 이와 구별되는 ISCS의 특징은 다음과 같다.

- ISCS 클라이언트시스템은 설치된 컴퓨터의 작동시점에 바로 실행되어 서버시스템에 접속하며, 해당 컴퓨터의 작동 중에는 통신장애가 없는 한 접속을 유지한다.
- Master Slave 형태: 클라이언트시스템이 서비스 템에서 정한 기준이나 지시에 의해 실행하는 형태로서 클라이언트의 요청을 서버가 실행하는 일반적인 클라이언트 서버 시스템과는 비교되는 형태이다.

따라서 ISCS 클라이언트시스템은 설치된 개별 컴퓨터의 작동시점에 서버시스템과 접속한 이후 실제 이루어지는 감시·통제 기능의 수행은 <그림 3>과 같이 로봇(robot)의 원격제어시스템(teleoperation)에서 ‘Human Operator - Master - Slave - Environment’로 구성되는 Master - Slave 형태(dale, 1993)로 이루어진다. ISCS의 서버 및 클라이언트 시스템이 각각 Master 및 Slave 시스템의 역할을 수행하게 되는데, 정보시스템의 내부 감시·통제의 담당자는 Master시스템인 Server시스템을 통해 사용자별 컴퓨터에 설치된 클라이언트시스템인 Slave시스템에게 해당 컴퓨터의 감시·통제를 지시하고 현황을 파악하여 전체 사용자컴퓨터를 감시·통제하게 되는 형태를 구성하게 된다.

그리고 일반 클라이언트 - 서버 형태의 시스템과는 달리, Master - Slave의 시스템구성 형태에서 ISCS의 주사용자인 내부 감시·통제의 담당자는 클라이언트시스템이 아닌 서버시스템을 통해 필요한 감



<그림 3> Master-Slave 형태의 ISCS 구성

시통제업무를 직접 수행한다. 필요에 따라 해당 업무의 담당자는 <그림 3>과 같이 관리자용 클라이언트시스템을 통해 서버시스템에 접속하거나, 또는 직접 서버시스템을 통하여 필요한 감시·통제 업무를 수행할 수 있다. Slave의 역할을 하는 ISCS 클라이언트시스템은 ISCS 서버시스템의 통제와 지시에 따라 자신이 설치된 컴퓨터에 설치된 정보시스템자산을 파악하고 필요한 감시·통제 등을 실행한다.

(2) 에이전트 시스템(agent system)

일반 사용자인 조직구성원 개개인의 컴퓨터에 설치되어 작동하는 ISCS 클라이언트시스템은 컴퓨터 사용자와 상호작용(interaction) 없이 자동으로 수행되는 에이전트 시스템(agent system)의 형태이다. <그림 3>에서 나타난 ISCS의 클라이언트시스템은 필요에 따라 서버시스템(Master시스템)과 지시사항 및 수행결과를 교신하며, 주어진 조건범위에 따라 자율성(autonomy)을 가지고 필요기능을 자동으로 수행한다. 특히 서버시스템과 통신이 두절되는 경우에도 서버시스템으로부터 전달된 최근의 조건에 따라 필요기능을 자동으로 수행한다.

Master - Slave형태로 구성되는 ISCS의 서버시스템과 클라이언트시스템간 통신은 인터넷기반에서 활용되도록 TCP(Transmission Control Protocol) 및 이를 시스템상에 구현할 수 있는 소켓(Socket) 프로그램으로 가능하고, 서버시스템과 클라이언트시스템이 사용하는 데이터베이스는 SQL서버와 같

은 DBMS를 사용할 수 있다. 이러한 통신상의 여건은 ISCS가 기술적으로 공간적 제한없이 인터넷을 통해 활용이 가능한 것을 의미한다. 그러나 ISCS 자체의 네트워크 차단을 통한 정보유출 통제기능 및 일반적으로 네트워크상에 존재하는 보안수단(방화벽 등) 등으로 인해 조직단위의 근거리통신망(LAN)을 벗어난 ISCS의 사용은 현실적으로 한계가 있다. 그리고 ISCS의 현실적 활용에는 온라인(on-line)으로 이루어지는 시스템특성 이외에도 관리자를 통한 인증 소프트웨어 또는 하드웨어의 오프라인 설치, 공간내의 사용자·부서관리 등과 같이 일정범위의 오프라인(off-line) 업무를 병행하는 것이 필요하다고 판단된다. 따라서 ISCS의 설치 및 활용의 범위는 LAN환경의 적절한 공간적 규모로 이루어지는 단일 조직으로 한정하는 것이 적절할 것이다.

3.2 시스템 세부기능

앞서 살펴본 ISCS와 일반 시스템 간의 특징적 차이를 고려하여 다음의 두 요소를 고려하여 ISCS의 세부기능을 구성하였다.

- ISCS의 기능범주: <표 2>의 ISCS 기능범주별 구현과 기능범주간 정보공유가 원활하도록 세부 구현기능 구성
- ISCS의 관리대상: 정보시스템자산의 관리 및 감시·통제의 대상이 되는 정보시스템 자산 및 정보시스템 활용의 분야를 ‘응용시스템’, ‘네

이터 및 파일(file)', '네트워크 및 통신', '입·출력 장치'의 영역으로 구분하고, 각 영역별로 ISCS의 세부기능을 구성

본 절에서는 ISCS의 기능별주별로 ISCS의 관리 대상 영역별 처리를 위한 ISCS의 세부기능을 정리하기로 한다. 필요에 따라 실제 사례로 구현된 ISCS 시스템의 출력화면을 소개하기로 한다.

(1) 내부 감시·통제 정책

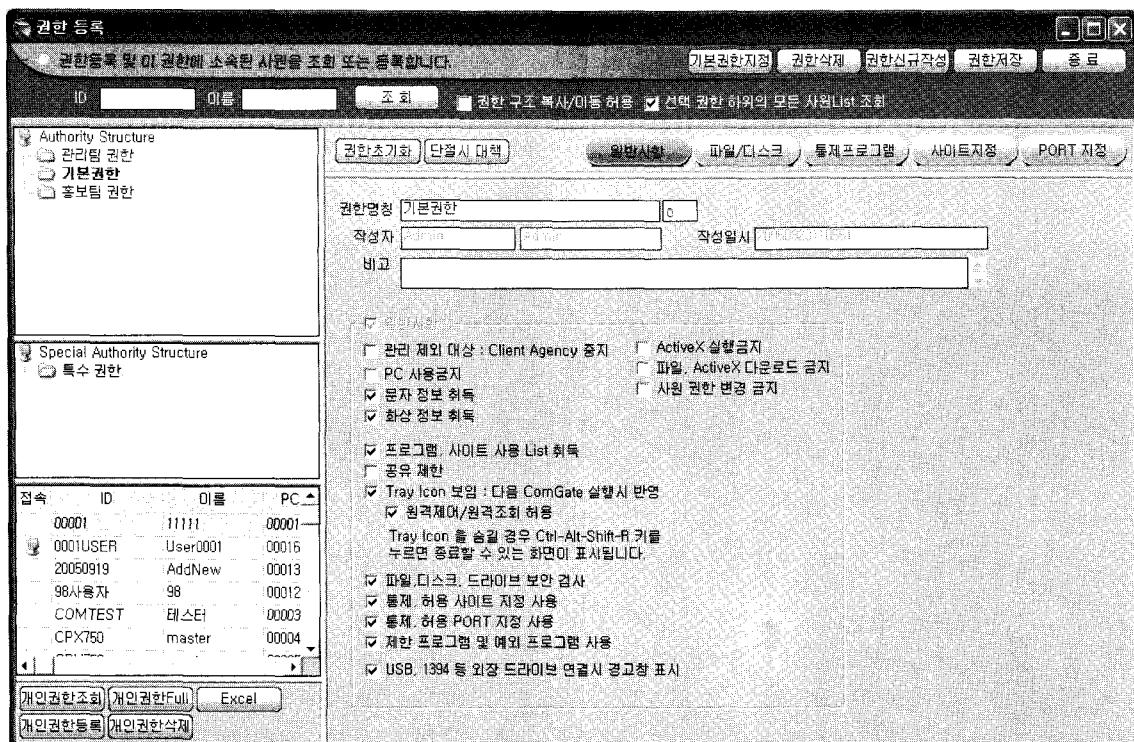
<표 2>에서 정리된 바와 같이, 내부 감시·통제 정책을 위한 세부기능은 정보시스템에 대한 권한관리 및 내부 감시·통제 평가를 처리하기 위한 것이다. ISCS의 대상이 되는 전 영역에 대해 개별 컴퓨터기반의 정보시스템 사용·통제를 관리하며, 세부기능을 정리하면 다음과 같다.

- 권한유형 관리 및 권한설정:

ISCS를 통한 정보시스템사용 감시·통제의 기본 정책이 되는 권한유형을 신규생성, 수정, 삭제하는 기능이며, 필요에 따라 저장 및 기본권한으로 초기화가 가능하다. ISCS 서버시스템(Master시스템) 상에서 권한유형별로 감시 및 통제 대상을 선택 또는 수정함으로써 권한유형을 관리한다. <그림 4>는 여러 권한유형 중 '기본권한'의 설정과정을 보여주는 화면이며, '기본권한'을 가지는 사용자(컴퓨터) 리스트(list)를 같이 조회할 수 있다.

- ISCS의 관리대상 영역별 권한설정:

ISCS 클라이언트시스템(Slave시스템)은 서버시스템을 통해 할당된 권한유형을 데이터베이스로부터 획득하여 해당 컴퓨터의 사용을 감시·통제하는 기준으로 활용하며, 서버로부터의 지시사항의 실행 또는 감시·통제 결과 등의 사항을 서버로 전송하게 된다. 내부 감시·통제 정책



<그림 4> 권한유형('기본권한')의 설정



〈그림 5〉 파일(file), 폴더(folder) 및 입·출력 장치에 대한 권한설정

분야에서 세부기능의 구성은 ‘응용시스템’ 등 의 ISCS 관리대상 영역별 권한설정을 위한 기 능들로서 <표 3>과 같다. 실제 시스템상에서는 파일(file), 폴더(folder) 및 입·출력 장치 및 프 로그램 사용제한에 대한 권한설정 기능의 구 성은 각각 <그림 5> 및 <그림 6>의 화면과 같 이 항목별 선택적 권한설정으로 나타날 수 있다.

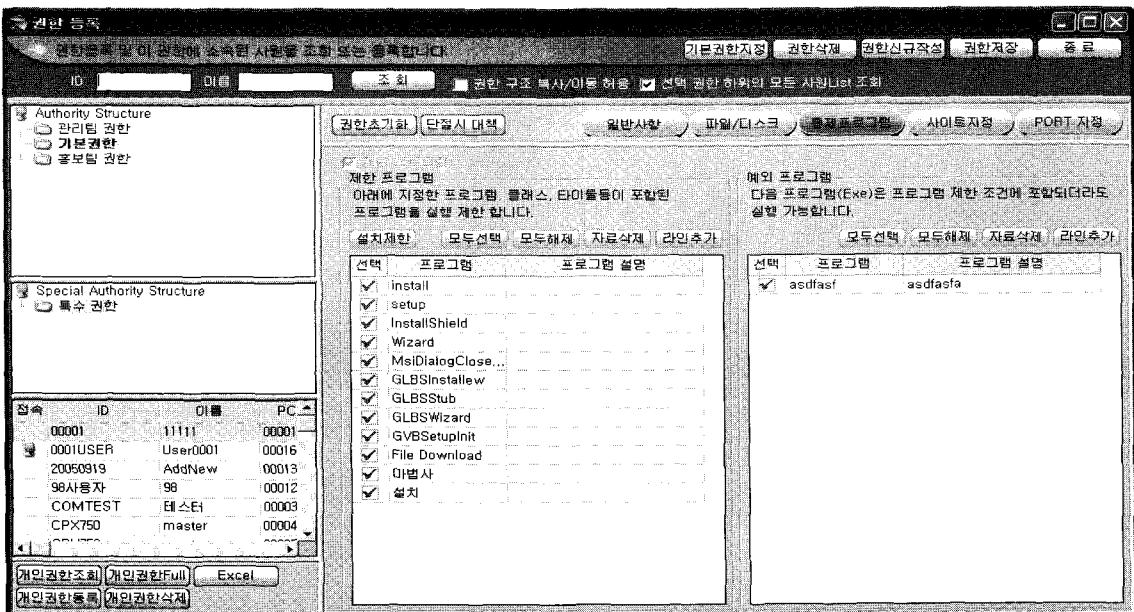
(2) 정보시스템 사용통제

‘내부 감시·통제 정책’의 기능을 통해 설정 또 는 변경된 권한유형 및 권한유형별 사용권한은 ISCS의 데이터베이스에 저장된다. 동시에 ISCS 클 라이언트시스템은 이를 확인하여 자신의 컴퓨터에 개별적으로 보관하여 통신두절 등 이상발생의 경 우에도 자신의 컴퓨터에 저장된 최근의 허용권한 을 정보시스템 사용통제에 활용한다. ISCS 클라이 언트시스템이 가지는 통제기능은 <표 3>과 같은

개별 컴퓨터에 할당된 권한유형에 따라 ISCS의 관리대상에 대하여 사용을 통제하게 되는데, 사 용자가 인식하는 사용통제의 전반적인 세부기능 을 정리하면 <표 4>와 같다. 그리고 일반적인 사 용통제 이외에도 서버시스템은 클라이언트시스템 을 통해 원격으로 제어, 조회 또는 일반적인 유지 보수기능이 가능하다.

(3) 정보시스템 사용감시

조직내의 개별 컴퓨터사용에 대한 ISCS의 감 시기능은 클라이언트시스템 및 서버시스템에 의 해 상호보완적으로 2단계에 의해 이루어지는데, 1단계의 클라이언트시스템에 의한 감시기능은 사 용자의 컴퓨터를 통한 모든 정보시스템 사용실태 를 실시간으로 감시한다. 그리고 그 결과를 ‘정보시 스템 사용통제’ 기능과 공유함으로써 사용자의 컴퓨터 사용이 권한 범위 내에 머물도록 한다. 또한 기



〈그림 6〉 프로그램 사용한에 대한 권한설정

〈표 3〉 ISCS의 관리대상 영역별 권한설정

ISCS 대상영역	세부기능의 구성
응용시스템	<ul style="list-style-type: none"> 특정 프로그램의 사용여부 통제 특정 이름을 포함하는 프로그램의 실행가능 여부 결정
데이터 및 파일	<ul style="list-style-type: none"> 파일(file) 및 폴더(folder)의 저장/조회/삭제 권한
네트워크 및 통신	<ul style="list-style-type: none"> 인터넷 사이트 접속통제(등록된 사이트 허용 또는 금지사이트 설정) 네트워크 포트(port)의 사용제한 또는 등록된 네트워크 포트만 허용
입·출력 장치	<ul style="list-style-type: none"> 특정 프로그램의 사용여부 통제 특정 이름을 포함하는 프로그램의 실행가능 여부 결정

〈표 4〉 ISCS의 관리대상 영역별 사용통제

ISCS 대상영역	세부기능의 구성
응용시스템	<ul style="list-style-type: none"> 프로그램의 설치제한 (Install Shield, Wise Install, Visual Studio, MSI 등으로 작성된 설치프로그램의 작동제한) - 미등록 소프트웨어 사용방지 특정 프로그램 또는 특정 단어를 제목에 포함하는 프로그램 실행불가 특정 프로그램의 실행중 원격 중지 ISCS 클라이언트시스템의 최종 접속시간 및 최근 booting 시간 (통제를 벗어나는 개별 컴퓨터 파악)
데이터 및 파일	<ul style="list-style-type: none"> 특정 파일 또는 특정 단어를 제목에 포함하는 파일 및 폴더의 읽기/쓰기 등 사용제한
네트워크 및 통신	<ul style="list-style-type: none"> 접속 가능/불가능 IP대역 구분 및 inbound/outbound Port 접속통제 (정보유출 사전차단 기능) 웹브라우저를 통한 파일, 프로그램 등 다운로드 제한 인트라넷을 포함한 네트워크작업 통제(HTTP, FTP, E-mail, MSN 등)
입·출력 장치	<ul style="list-style-type: none"> 입출력 드라이버 및 외부 저장장치 접속포트 사용제한

〈표 5〉 ISCS의 관리대상 영역별 사용감시

ISCS 대상영역	세부기능의 구성
응용시스템	<ul style="list-style-type: none"> 시스템별 작업시간 및 실행중 시스템의 실행내용(시스템 이름, 프로세스 ID, 메모리 소요량 등), 비인가 프로그램의 접근시도 횟수 응용시스템별 keyboard 입력자료 시스템 사용에 대한 로그(log) 작성
데이터 및 파일	<ul style="list-style-type: none"> 사용자 컴퓨터의 파일 및 폴더 정보 파일 작성/수정/복제 등에 대한 로그(log) 작성
네트워크 및 통신	<ul style="list-style-type: none"> 사용자 컴퓨터의 접속 IP 및 Port번호, 접속 web site, 일별 송/수신 통신량(bytes) 등
입·출력 장치	<ul style="list-style-type: none"> Screen capture, key stroke, 입출력에 관한 로그(log) 이벤트 정보

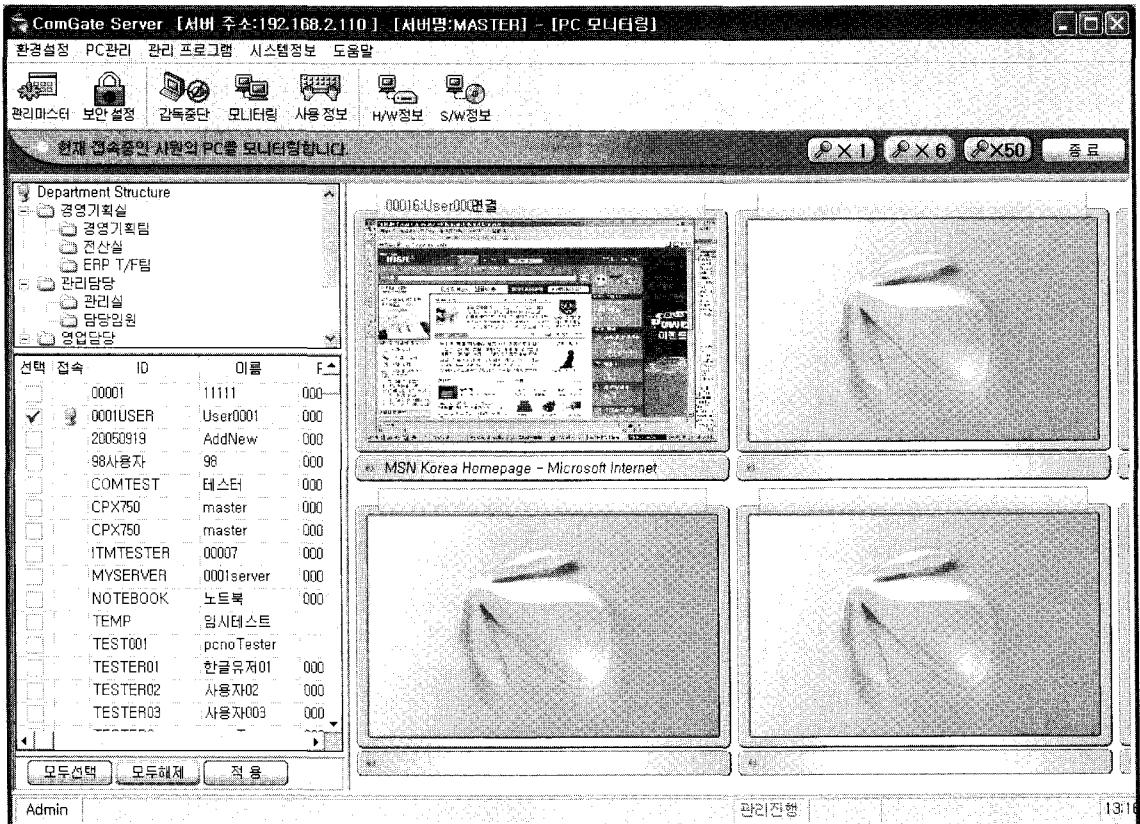
간별 감시현황을 파악할 수 있도록 감시결과를 네이터베이스를 통해 서버시스템과 공유하여 조화할 수 있도록 한다(〈그림 7〉 참조).

2단계의 서버시스템에 의한 감시기능은 클라우드시스템과 공유하는 감시결과의 조회 및 실

시간 원격감시기능을 들 수 있다. 서버시스템과 클라이언트시스템간 감시결과 공유 및 조회를 위한 기능을 ISCS의 관리대상별로 나열하면 〈표 5〉와 같다. 그리고 서버시스템에 의한 시스템사용의 실시간 원격감시는 사용자 컴퓨터의 현재 작업

사용자	ID	이름	접속일	사용시간	작업내용
00001	1111	00	2005-08-23 12:55	75	File Open - Cannot find server
0001USER	User0001	00	2005-08-23 12:54	3	File Open - C:\Temp\W123.tkt
20050919	AddNew	00	2005-08-23 12:54	1	File Open - C:\Temp\W123.tkt
98사용자	98	00	2005-08-23 12:54	1	File Open - 123.tkt - 메모장
COMTEST	테스터	00	2005-08-23 12:54	1	File Open - MSN Korea Homepage - Microsoft Internet Explorer
CPX750	master	00	2005-08-23 12:55	IP... 202.43.214.151 (202.43.214.151)	접근일시
CPX750	master	00	2005-08-23 12:55	www.yahoo.co.kr 202043214151 (www.yahoo.co.kr)	접근일시
ITMTESTER	00007	00	2005-08-23 12:55	www.daum.net 21111507213 (www.daum.net)	접근일시
MYSERVER	0001server	00	2005-08-23 12:55	www.empas.com 220095223008 (www.empas.com)	접근일시
NOTEBOOK	노트북	00	2005-08-23 12:55	IP... 220.95.223.8 (220.95.223.8)	접근일시
TEMP	임시테스터	00	2005-08-23 12:55		접근일시
TEST001	pcnoTester	00	2005-08-23 12:55		접근일시
TESTER01	한글유저01	00	2005-08-23 12:55		접근일시
TESTER02	사용자02	00	2005-08-23 12:55		접근일시
TESTER03	사용자03	00	2005-08-23 12:55		접근일시
TESTER02	pcnoT	00	2005-08-23 12:55		접근일시
USER001	한글사용자01	00	2005-08-23 12:55		접근일시

〈그림 7〉 사용자별 프로그램 사용에 관한 감시결과 조회



〈그림 8〉 여러 사용자 컴퓨터의 화면캡쳐를 통한 실시간 원격 사용감시

상황에 대한 실시간 조회기능으로 <그림 8>과 같이 서버시스템에서 구현될 수 있다.

(4) 정보시스템 자산관리

정보시스템자산의 적절한 사용통제를 위해서는 개별 사용자의 개인용 컴퓨터 기반의 하드웨어 및 소프트웨어의 보유현황 및 변경사항, 그리고 사용현황을 정확히 파악하는 것이 필요하다. 예를 들면, <그림 9>와 같이 ISCS 서버시스템에서 기업전체에서 보유하고 있는 하드웨어 또는 소프트웨어를 파악하기 위한 기능 등이 필요하다. 이를 위해 ‘응용시스템’ 등의 ISCS 관리대상 영역의 실행을 가능하게 하는 소프트웨어 및 하드웨어로 나누어 정보시스템자산 관리를 위한 기

능을 정리하면 다음과 같으며, 이러한 기능들로써 기업의 주요 정보시스템자산인 개별 컴퓨터상의 하드웨어 또는 소프트웨어에 대하여 보유현황, 버전(version), 취득 및 폐기 등의 정보시스템자산의 관리를 수행 또는 지원할 수 있다.

· 소프트웨어 관리기능

- ① ISCS 클라이언트시스템의 기능: 개별 컴퓨터 상의 등록된 또는 미등록된 소프트웨어의 설치 파악, 정보시스템 활용 정도(송·수신 통신량, 사용중인 메모리 등), 특정 소프트웨어의 설치 및 삭제 등
- ② ISCS 서버시스템의 기능: 클라이언트시스템을 통한 개별 컴퓨터상의 정보시스템자산 항목 별 원격관리(소프트웨어 설치/삭제, 알림발

		Excel	모든선택	모든제거	자료선택	인쇄	종료
구 분	설치 프로그램 명칭	제작회사	내선				
상품	ComGate Client	Microsoft Corporation	20041028,175203				
상품	Microsoft Office Professional Edition 2003	ITMSystem	1,00,0000				
	Security Update for Windows XP (KB893930)	Microsoft Corporation	1				
	Security Update for Windows XP (KB890046)	Microsoft Corporation	1				
	Security Update for Windows XP (KB893056)	Microsoft Corporation	2				
	Security Update for Windows XP (KB896358)	Microsoft Corporation	1				
	Security Update for Windows XP (KB896422)	Microsoft Corporation	1				
	Security Update for Windows XP (KB896420)	Microsoft Corporation	1				
	Security Update for Windows XP (KB891214)	Microsoft Corporation	1				
	Security Update for Windows XP (KB89235)	Microsoft Corporation	1				
	IT4	Microsoft Corporation	20050114,005213				
	Update for Windows XP (KB89641)	Microsoft Corporation	1				
	WebFltrs XP	Microsoft Corporation	9,50,7523				
	Windows Installer 3.1 (KB893003)	Microsoft Corporation	3.1				
	Windows XP Hotfix - KB897399	Microsoft Corporation	20041117,093459				
	Windows XP Hotfix - KB885250	Microsoft Corporation	20050118,202711				
	Windows XP Hotfix - KB895835	Microsoft Corporation	20041027,181713				

(1) 기업전체의 단위조직별/개인별 보유 소프트웨어 현황 파악

		모든선택	모든제거	정보현황	자료선택	인쇄	종료
구 분	기본정보						
상품	PC No.	00016	MAC Address	00 40 00 45 51 39			
상품	IP 주소	192.168.2.109	작업그룹	WORKGROUP	집 풋터명	HAN	
상품					AHIP	192.168.2.110	
상품							
	제조사	MTC	모델	Montara-GM			
	운영체계	Microsoft Windows XP Professional					
	운영체계버전	5.1.2600	서비스팩	Service Pack 1			
	프로세서	Intel(R) Pentium(R) M processor 1400MHz	메모리	S12			
	Physical HDD						
	드라이브	모델명	용량 (Gbyte)				
	HDD 1		0				
	HDD 2	IC25N040DATMR04-0	35				
	Logical Drive						
	드라이브	전체	여유공간	파일시스템			
	C:	19.53	7.26	NTFS			
	D:	17.71	2.68	FAT32			
	E:	0.00	0.00	CFDS			
	G:	0.00	0.00	COFS			

(2) 기업전체의 단위조직별/개인별 보유 하드웨어 현황

(그림 9) 소프트웨어 및 하드웨어의 보유현황 파악

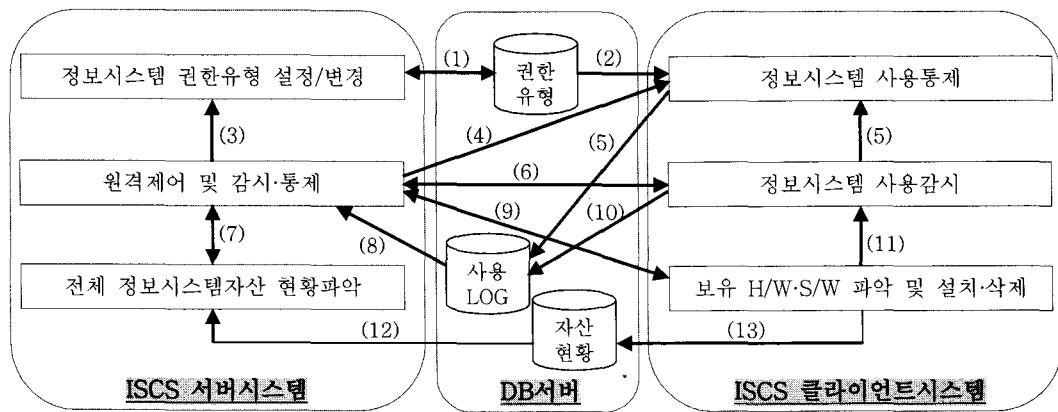
전송 등 포함) 및 집계, 개별 컴퓨터의 클라이언트시스템을 통한 특정 소프트웨어의 설치 및 삭제 등

· 하드웨어 관리기능

- ① ISCS 클라이언트시스템의 기능: 개별 컴퓨터의 작동과 함께 구동되는 클라이언트 시스템이 거의 모든 하드웨어 항목(BIOS, CPU, 내장 메모리, 사운드카드, 하드디스크 등 외장

메모리, 각종 드라이버 등의 제반 하드웨어 자신의 보유여부, 용량, 처리속도, 제조일자, 설치일자 등)을 확인하여 컴퓨터별 사양 및 변경사항을 파악하고, 미등록 하드웨어의 사용방지 등을 수행

- ② ISCS 서버시스템의 기능: 등록 및 설치된 하드웨어 품목관리 및 클라이언트시스템으로 부터 전달된 항목별 파악내용 집계



- (1) 단위조직별/개인별 정보시스템 사용권한 저장/조회
 (2) 통제의 기준인 개별 컴퓨터(사용자)의 사용권한 조회
 (3) 개별 컴퓨터에서 사용권한을 넘어선 시도내용
 (4) 유사사 또는 특별한 경우 강제적 통제사항 지시
 (5) 정보시스템의 모든 건별 사용내역에 대한 통제의뢰
 (6) 필요시 클라이언트를 통한 서버의 실시간 감시·통제
 (7) 설치 소프트웨어 확인 및 원격 설치·제거 사항 통지
 (8) 기간별 사용실태 분석을 위한 사용로그 조회
 (9) 보유 H/W 및 S/W의 실시간 파악 및 원격 설치·삭제
 (10) 개별 컴퓨터(사용자)의 사용내역을 저장
 (11) 설치·삭제에 의한 정보시스템자산 변동사항 전달
 (12) 정보시스템자산의 현황 조회
 (13) 정보시스템자산의 변동사항 생성

〈그림 10〉 ISCS 시스템 구조

IV. 시스템 설계 및 개발

4.1 시스템 구조

사용자를 포함한 ISCS의 시스템은 <그림 3>과 같이 Master Slave의 형태로 구성될 수 있으며, ISCS 클라이언트(client) 및 서버(server) 시스템의 내부는 필요기능의 모듈(module)과 모듈간 전달정보들로 구성될 수 있다. DB서버를 포함하여 ISCS 시스템의 구조를 <그림 10>과 같이 도식화할 수 있으며, 각 모듈간 또는 데이터베이스와 시스템 모듈간 전달정보에 대한 설명을 포함하였다. 본고에서 사례로 제시한 ISCS시스템의 구조상 특징이 될 수 있는 사항은 다음과 같다.

(1) 서버시스템은 권한유형 등의 가이드라인(guide-line)을 제시하며, 정보시스템사용에 대한 감시·통제의 실질적 수행은 클라이언트시스템이 수행한다.

(2) 조직내부의 정보시스템 감시·통제를 담당하는 ISCS시스템의 사용자는 서버시스템을 통해 간접적으로 개별 컴퓨터의 사용을 통제하고 현황을 파악한다.

4.2 시스템 개발

본고에서 사례로 제시한 ISCS시스템은 마이크로소프트 윈도우즈(Microsoft Windows) 환경에서 <그림 10>의 구조로 개발되었으며, 실제 개발된 시스템의 사례는 본고의 본문내용에서 화면 위주로 소개하였다. 기업과 같은 조직에서 사용하는 정보시스템이 윈도우즈(Windows)를 포함하는 여러 다양한 운영시스템을 활용한다는 측면에서 윈도우즈 환경만을 고려한 점은 한계가 될 수 있다.

그리고 ISCS 서버시스템과 클라이언트시스템의 여러 수행기능은 마이크로소프트(Microsoft)사 또는 외부로부터 도입한 컴포넌트(componenet) 기능을 활용할 수도 있는데, 본고의 사례가 된 시

스템에서도 많은 필요기능을 외부로부터 도입한 컴포넌트 기능을 사용하여 개발하였다. 본고의 사례가 된 시스템에서 ISCS 서버시스템과 클라이언트시스템의 개발에 사용한 대표적인 컴포넌트 기능은 다음과 같다.

- (1) GUI관련 기능: 각종 그래픽 구현, 스프레드 쉬트(spread sheet) 콘트롤, 윈도우즈(windows) 콘트롤(toolbar, status bar, listview, treeview 등 작성기능) 등
- (2) 사용자 정보전송 기능: 파일 송·수신, 파일 송·수신시 압축·압축풀기, 컴퓨터간 대화(ISCS 관리자의 개별 컴퓨터사용자에 대한 경고메세지 전송) 등
- (3) 컴퓨터간 정보전송 기능: 소켓(Socket) 활용, 데이터베이스 서버와의 통신
- (4) 정보시스템자산 정보취득 기능: 컴퓨터에 설치된 모든 하드웨어/소프트웨어 내역 파악
- (5) 정보시스템사용 감시·통제 기능: ‘옹용시스템’, ‘데이터 및 파일(file)’, ‘네트워크 및 통신’, ‘입·출력 장치’의 정보시스템 활용분야에 대한 사용자의 모든 컴퓨터사용 프로세스(process) 감시 및 통제, 컴퓨터간 사용화면의 캡쳐·전송

위의 컴포넌트 기능에 대해 ISCS 서버시스템이 필요한 항목은 (1), (2), (3)에 해당하며, ISCS 클라이언트시스템이 필요로 하는 항목은 (2), (3), (4), (5)에 해당하는 것들이다. 특히, (4)와 (5)는 각각 정보시스템자산의 관리 및 내부 감시·통제 기능과 가장 밀접한 항목이다. 마이크로소프트에서 제공되는 일반적인 컴포넌트로서 (1)에 해당하는 것은 WCC(Windows Common Control), (2)에 해당하는 것은 Internet Control, (3)에 해당하는 것은 MDAC(Microsoft Database Access Control), (4)에 해당하는 것은 WMI(Window Management Instrument), (5)에 해당하는 것은 kernel32 등이다 (Microsoft, 2006).

V. 효과 및 결론

본고에서 소개한 시스템은 <그림 4>~<그림 9>에서 같이 활용이 가능한 상태로 개발되어 내부자에 의한 보안위협에 대응하고자 하는 시스템의 여러 기능을 구현할 수 있었다. ISCS를 실제 사용중인 기업의 정보관리자와 인터뷰를 통해 ISCS의 효과를 평가한 결과, <표 2>에서 분류한 ISCS의 기능범주 및 범주별 기능범위에 대해 충분히 만족하고 있음을 확인하였다. 즉, ISCS 관리자는 네트워크(인터넷) 또는 휴대용 메모리장치를 통한 내부 정보의 불법유출이라는 가장 관심이 되는 내부위협에 대해 본인의 의지대로 ISCS의 기능범위 내에서 효과적인 방지가 가능할 수 있었다. 예를 들면, 정보보안이 필요한 부서에 대해 개인용 컴퓨터의 사용통제를 보다 엄격히 함으로써 정보의 불법유출가능성을 최소화하는 것이다.

정보보안의 기술적인 측면에서 많이 강조되는 방화벽, 침입탐지시스템, 악성코드 백신 등으로 방지하고자 하는 외부 보안위협의 방지보다, 보안사고에 있어서 현실적으로 가장 큰 비중을 차지하는 조직내부의 보안위협에 대한 관심이 커지고 있다. 동 분야의 정보시스템 업계 또는 일반 기업에서는 이러한 내부 정보보안 위협에 대응하기 위한 내부 감시·통제시스템의 개발과 활용에 대한 관심이 커지고 있으며, 사례가 되는 시스템들이 개발되어 활용되기 시작하고 있다. 이에 대해 본고에서는 정보시스템의 내부 감시·통제를 위한 기능을 갖춘 시스템의 구조와 필요기능, 개발사례 등을 정리하고 개발사례를 제시함으로써 이론적인 정리와 함께 추가적인 연구의 진행에 기여하고자 하였다.

본고에서 사례로 제시된 내부 감시·통제시스템은 연구개발이나 컨설팅 등과 같이 내부의 정보자산이 중요한 기업이나 단체에 보다 중요하며, 실제 활용되는 경우에 있어서도 긍정적인 평가를 받고 있다. 이와 같은 시스템은 정보기술적

인 면에서 내부 감시·통제의 기능을 충분히 구현해야 하는 요구 이외에도, 내부 구성원의 정보시스템 활용을 감시·통제한다는 점에서 상충될 수 있는 조직구성원의 프라이버시(privacy) 침해와 관련되는 심리·조직행태적인 관점의 연구(Lilian, 2006)가 병행될 필요가 있다.

참 고 문 헌

- 김종원, 최종욱, “기업정보유출방지를 위한 기술”, *한국정보처리학회지*, Vol.10, No.2, pp. 87-99, 2003.
- 유신근, 이남훈, 심영철, “침입탐지시스템 평가 방법론”, *한국정보처리학회지*, Vol.7, No. 11, pp. 3445-3461, 2000.
- 이용준 등, “전산망 보호를 위한 혼합형 방화벽 시스템 구현”, *한국정보처리학회지*, Vol.5, No.6, pp. 1593-1602, 1998.
- 하태용, 신용백, “디지털 생산성 향상을 위한 신경망 사용자 인증모형 연구”, *생산성논집*, Vol.18, No.3, pp. 1-18, 2004.
- 홍일유, 이종상, “국내기업들의 정보시스템 보안위협에 관한 연구”, *한국경영정보학회'96 추계학술대회 논문집*, pp. 143-154, 1996.
- Cert Coordination Center, CERT/CC statistics, http://www.cert.org/stats/cert_stats.html, 2006.
- Dale A.L., “Stability and transparency in bilateral teleoperation”, *IEEE Transactions on Robotics and Automation*, Vol.9, No.5, pp. 624-637, 1993.
- Hansman S. and Hunt R., “A taxonomy of network and computer attacks”, *Computers and Security*,

- Vol.24, pp. 31-43, 2005.
- Herbert H. Thompson, James A. WhittakerMike Andrews, “Intrusion detection: Perspectives on the insider threat”, *Computer Fraud & Security*, Vol. 2004, Issue 1, pp. 13-15, 2004.
- Karin Hone and J.H.P. Eloff, “Information security policy - what do international information security standards say?”, *Computers & Security*, Vol. 21, Issue 5, pp. 402-409, 2002.
- Lilian Mitrou and Maria Karyda, “Employees’ privacy vs. employers’ security: Can they be balanced?”, *Telematics and Informatics*, Article in press, 2006.
- Microsoft, “Controls(MFC)”, [http://msdn2.microsoft.com/ko-kr/library/47xcww9x\(VS.80\).aspx](http://msdn2.microsoft.com/ko-kr/library/47xcww9x(VS.80).aspx), 2006.
- Microsoft, “Visual C++ ActiveX Control for hosting Office documents in Visual Basic or HTML”, <http://search.support.microsoft.com/kb/311765/>, 2006.
- Microsoft, “MDAC(ADO, OLEDB, ODBC)”, <http://support.microsoft.com/default.aspx?scid=fh;enus;mdac>, 2006.
- Microsoft, “WMI Window Management Instrument”, <http://www.microsoft.com/whdc/system/pnppwr/wmi/default.mspx>, 2006.
- Microsoft, “How RPC works”, <http://technet2.microsoft.com/WindowsServer/en/library/4dbc4c95-935b-4617-b4f8-20fc947c72881033.mspx?mfr=true>, 2006.
- Porter, D., “Insider fraud: spotting the wolf in sheep’s clothing”, *Computer Fraud & Security*, Vol.1, No.4, pp. 12-15, 2003.

Information Systems Review

Volume 9 Number 1

April 2007

An Internal Surveillance and Control System for Information Security and Information System Asset Management

Han-Seong Yoon*

Abstract

Several security systems (firewall, intrusion detection system, vaccine for malicious codes and so on), whose purposes are to prevent the external information security threat, have gathered more technological concerns. However, they are little effective for the area of defending the internal information security threat which occurs more frequently and results in much more monetary damages. In this paper, a system for internal surveillance and control on the use of information systems is suggested and described with its architecture, features, necessary functions and development methods. And a case system is introduced to show the reality of this paper.

Keywords: *Information Security, Internal Security Threat, Surveillance and Control System*

* Professor, School of Business Admin., Gyeongsang National University

● 저 자 소 개 ●



윤 한 성 (hsyun@dreamwiz.com)

서울대학교 산업공학과 학사, KAIST 산업공학과 석사 및 경영정보공학 박사 학위를 취득하였으며, (주)SK와 SK C&C(주)에서 DSS, Internet 응용 시스템 및 사업 분야 등에서 근무하였다. 현재 경상대학교 경영학부 부교수로 재직하고 있으며, 경상대학교 경영경제연구센터 책임연구원으로 있다. 주요 관심분야로는 e-비즈니스 전략 및 시스템, 정보보안, SCM 등이다.

논문접수일 : 2006년 11월 08일
1차 수정일 : 2007년 01월 16일

제재확정일 : 2007년 01월 30일