情 報 保 護 學 會 誌
第18卷 第6號, 2008. 12

情報技術 유출 예방을 위한 기업內 컴퓨팅 환경 최적화 방안 연구

송 성 근*, 박 지 숙**, 우 재 현***, 임 종 인****

요 약

기업 내 정보기술 유출의 대부분은 내부 근무자에서 비롯되고 있다 [1]. 본 연구는 기업 내부 근무자들의 사무환경에서 정보기술 유출 예방을 위해 적용하고 있는 기술적 사례들을 4개의 측면(PC내 정보가 PC 인터페이스 장치에 의해 외부로 나가는 방법을 통제, 네트워크를 통해 사외로 나가는 방법을 통제, PC내 정보를 암호화 저장, 개인 PC를 더미 터미널로 사용하고 실 정보는 서버로 저장하는 네트워크 컴퓨팅)으로 고찰하고 그에 따른 최적화 방안으로 복합형 모델을 제시하면서 이를 적용한 사례와 정책적 요소를 제시하고자 한다.

Ⅰ. 서 론

최근 기업이 보유한 개인정보가 외부로 유출되어 심각한 사회적 물의를 일으키거나 기업의 산업기밀기술이 유출되어 기업 활동에 심각한 피해를 일으키는 사례가 많다. 특히, 지난 9월 GS칼텍스의 고객정보 1,125만건이 유출된 사건으로 자회사 직원 등 4명이 입건된 사건은 기업의 중요한 자산인 고객정보를 보호해야 할 내부 담당자가 자신의 권한을 악용하여 직접 내부 정보를 유출시켰다는 점에서 경악을 금치 못하게 한다. 만일 이러한 정보가 유통되었을 경우, 2차 피해는 물론이며, 기업 측면에서는 정보가 유출된 고객들이 집단 소송으로 1인당 20만원씩의 피해보상만 가정하더라도 2조2천만원의 천문학적 배상이 발생되어 기업활동이 막대한 타격이 발생할 수 있으며, 2008년 12월 시행예정인 정보통신망 이용촉진및정보보호등에관한법률에서는 개인정보보호를 등한시한 경영자에게는 5년 이하의 징역형에 처하는 등 처벌의 수위도 한층 높아지게 되었다. 결국 정보화가 발달할수록 기업 내부에서 보호되어야 할 정보가 외부로 유출 되지 않도록 기업측면에서는 정책, 기술, 교육, 계도 활동 등을 통해 정보유출 방지에 심혈을 기울여야 할 것이다. 본 연구는 산업기밀정보 중 정보기술 분야를 취급하는 사외개발센터에서 정보기술을 보호하기 위한 환경을 구성함에 있어 필요한 기술적 방법을 고찰하고, 그에 따른 장단점을 분석 후, 비지니스 니즈에 적합한 해결 대안을 모색하여 구축 모델을 제시하고 그에 따른 정책적 방안을 도출하고자 한다.

Ⅱ. 선행 연구 조사

사용자 PC의 정보보호 방안의 연구로서 유재근의 "기업 내 효율적인 PC보안 시스템 구축방안에 대한 연구" [2] 사례에서는 PKI 인증 시스템, DRM(문서보안) 시스템, PC 보안시스템의 세 가지 보안 분야의 시스템을 연동한 중앙관리가 가능한 통합 시스템 구축 방안을 제시하여 중요문서의 암호화 적용, 인가자 이외의 이동식 저장 매체 사용 권한 제한, 긴급한 보안정책 수립 및 적용에 편리한 효과를 제시하고 있고 김동진의 "기업환경의 내부보안을 위한 통합 보안 관리 시스템의 설계 및 구현" [3] 에서는 PC보안 모듈, 문서보안(DRM) 모듈, 웹메일 보안모듈, DB 커넥션 점검모듈, ESM (Enterprise Security Management) 모듈 중심으로 기업

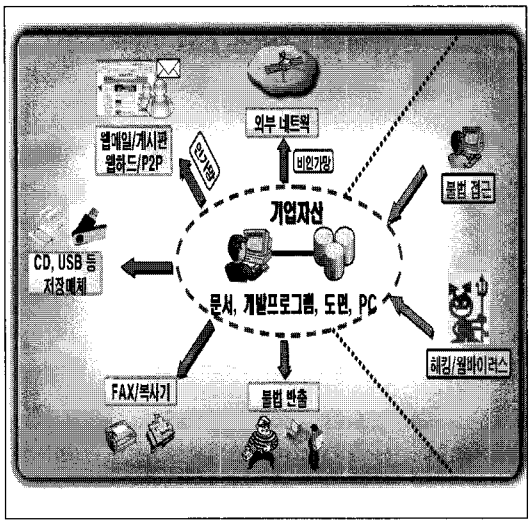
* 삼성SDS 통합서비스사업부 (sk.song@samsung.com)
* 삼성화재 정보기획파트 (jisook.park@samsung.com)
*** 고려대학교 정보경영공학대학원 박사과정 (bull0330@hanmail.net)
**** 고려대학교 정보경영공학대학원 원장 (jilim@korea.ac.kr)

환경에서 통합 보안관리 시스템 사례를 제시하고 있으나, 개인 PC 중심의 접근으로 한정되어 기업 내 다양한 입체적 환경을 고려한 사내 정보의 원천적인 유출 방안까지는 이르지 못하였고, 사용자의 편의성을 고려하거나 보안 정책의 가이드라인을 제시하지 못한 한계가 있었다. 또한 선병욱의 "네트워크 컴퓨터(NC)의 군 적용 방안에 관한 연구" [4] 사례와 조현상의 "NC (Network Computer)를 이용한 군사기밀 보호 방안에 관한 연구" [5] 사례가 있었으나 모두 군용 시스템 구축 사례로서 NC 컴퓨팅의 일반적 개념 비교로 구체적인 기술적 원리에 대한 언급이 없고, 산업 현장과 다소 상이한 적용 기준의 모델임을 알 수 있었다. 결국 기업 내에서 개인 PC, 네트워크, 암호화 등 다양한 환경에서 기술 진화에 따른 종합적으로 다양한 조건의 방안을 융합하여 내부 정보 보호 해결하면서도 사용자에게 편의성을 제공하는 대안을 찾는 연구 사례를 찾기 어려웠다.

Ⅲ. 관련 연구

기업 현장의 정보기술 자산을 보호하기 위해 고려되어야 할 정보보호 경로는 다음과 같이 내부에서 외부, 외부에서 내부 위협의 사례로 크게 구분 할 수 있으며, 각기 다양한 경로가 있다.

본 연구는 내부에서의 외부 유출로의 위협 사례를 예방할 수 있는 산업현장의 컴퓨팅 환경 개선 사례를 중심으로 고찰한다.



〔그림 1〕 기업에서의 정보보호 경로 : 외부에서 침입되는 위협을 막아야 하는 경로와 내부의 정보가 외부로 유출되는 경로를 막아야 한다.

3.1. PC통제 방법

PC내에 저장된 정보가 외부로 나가는 방법을 통제하는 방안을 의미한다. 기업 내 사용되는 PC를 대상으로 하는 PC통제 방법은

. 저장장치 통제
. 포트 통제
. PC와 네트워크 통제
. 데이터 암호화

의 4가지로 고려 할 수 있으나 본 절에서는 데이터 암호화를 제외한 3개의 방안에 대해 분석하겠다.

3.1.1 저장장치 통제

PC내에 있는 정보를 PC외부로 이동, 복사하기 위하여 이동식 정보저장 방식을 파악한 후, 후속으로 기업용 PC에서 이동식 장치로 저장이 불가하도록 조치를 취해 주어야 한다. 현재까지 밝혀진 이동식 저장장치의 종류를 열거하자면 다음과 같다.

(1) FDD Read/Write : FDD 저장이 불가 하도록 조치되어야 한다
(2) CD Read/Write : CD 저장이 불가 하도록 조치되어야 한다
(3) DVD Read/Write : DVD 저장이 불가 하도록 조치되어야 한다
(4) USB Memory : USB 저장이 불가 하도록 조치되어야 한다
(5) 이동식 저장장치 - SD카드, XD카드, 메모리스틱 : 해당 매체로 데이터 저장이 불가 하도록 조치되어야 한다
(6) 외장형 HDD : 외장 HDD 저장이 불가 하도록 조치되어야 한다
(7) MP3 : MP3 저장이 불가 하도록 조치되어야 한다
(8) 음성저장장치 : 음성매체로 저장이 불가 하도록 조치되어야 한다
(9) 핸드폰 : 핸드폰 메모리로 저장이 불가 하도록 조치되어야 한다.(예:MS Outlook의 연락처와 같은 기능내에 저장되어 있는 고객정보가 모바일 기기

로 연결 복사될 수 있다)

기업환경에서는 기업내 PC에서 이러한 이동용 저장장치로 저장이 불가하거나, 이러한 동작이 인지되는 경우 해당 정보(시도한 일시, IP, 담당자, 파일명, size등)를 로깅하는 별도의 소프트웨어를 개발, 적용함으로서 정보유출을 예방하는 활동이 있다. 그러나 이러한 방식은 기술의 발전에 따라 이동식 저장장치의 종류가 매우 다양해지고 있으며, 매번 발생하는 신규 이동장치 방식마다 그 특성에 따른 해결방안을 별도로 모색, 건건이 대응해야 하는 후속조치가 수반되며, 로깅된 수많은 데이터를 별도로 분석, 점검해야 하는 수고가 발생함에 따라 대처 능력의 한계, 유지비용의 발생이 따르는 단점이 있다. 또한 이동저장장치의 통제에 앞서, PC본체의 Hard Disk 자체를 물리적으로 분리, 이동시에는 이러한 노력 자체가 무의미 하여진다.

3.1.2 포트 통제

PC내에서 외부의 보조장치로 출력을 위해 사용되는 각종 포트를 이용하여 정보가 인쇄, 복사, 전달될 우려가 있기에 이를 제어할 수 있는 방안이 수반되어야 한다. 포트 통제의 대상이 되는 사례는

(1) 1394 포트
(2) Serial 포트
(3) Infared 포트
(4) Parallel 포트

등이 있다. 이 경우도 1번 통제방식과 같이 별도의 통제 가능한 소프트웨어를 개발, 유지보수 하게 되며, 1-1번과 동일한 단점이 따르게 된다.

3.1.3 PC와 네트워크 통제

기업내에 사용하는 PC가 내부 사용자간 혹은 외부 사용자와 연결되는 네트워크 부문을 통제함으로써 정보의 유출을 예방하고자 하는 방안으로서 PC-네트워크 통제, PC-외부 통제, PC프로세스 통제 등 3개의 측면을 고려할 수 있다.

첫째, PC-네트워크 통제에서는 LAN환경, 모뎀환경, 모바일 기기 환경에 대한 통제 방안을 고려해야 한다.

둘째, PC-외부 통제에서는 기업내 PC에서 네트워크 환경을 통해 외부로 전달되는 정보 중에는 공식적으로 업무상 허가를 득하여 나가는 경우와 비공식적으로 외부로 메일 발송되거나 외부 사이트에 게시되거나 하는 메일, 게시물이 있을 수 있으며 특히, 첨부파일은 사이즈가 크고 많은 양의 정보를 포함할 수 있기에 기업은 이에 대한 별도의 예방 대책을 마련할 필요가 있다.(예를들어, 공식적인 메일계정으로 발송한 데이터에 대한 로깅 기록 관리(SMTP), 비공식적인 외부 메일계정 사용여부 및 해당 사항 발생을 고려한 외부 메일 계정 데이터에 대한 로깅 기록 관리(SMTP), 외부 인터넷 사이트에 내부 정보를 게시한 경우(Http)를 고려한 HTTP 등록 통제와 해당 내용 로깅 기록관리 이다) 또한 정보유출 우려가 있는 비업무 프로그램(메신저, P2P, 웹하드PG 등)을 차단하는 방안도 고려해야 한다.

셋째, PC프로세스 통제에서는 네트워크 환경에서 PC 사용시 발생하는 각종 프로세스를 통제할 수 있어야 한다. 또한 이러한 프로세스는 정책의 변화에 따라 수시로 유연하게 조정이 가능하여야 하며 해당 기록의 로깅 및 검색관리 기능이 기업 보안정책에 맞도록 편리하게 준비 되어야 한다.(예를들어, 해킹차단, 바이러스 차단, 비업무용 사이트 접속차단 등)

3.1.4 장단점 분석

PC 정보를 USB, 디스켓, CD 등에 저장하는 수단을 사전 통제하는 방법과 PC 에서 외부로 나가는 네트워크를 사전 통제하는 방법이 있다. 이런 경우 기업에서는 별도의 PC제어용 프로그램이나 내부 보안 프로그램에 의거 타 저장매체로 저장이 불가하게 조치를 한다든지, 외부로 나가는 네트워크 접속은 사전 정의된 첨부 크기 외에는 발송이 제한되며, 별도의 모니터링 기법에 의해 제어되는 인가된 망으로만 사용하고 비인가된 망으로 접속을 금지시키는 방법을 구현하여 각종 SW 와 정책 프로그램을 운영할 수 있다. 그러나 이러한 경로를 제어하는 기법도 결국, 신기술이 발달하고 다양한 우회 경로가 발생, 진화하고 있으므로 새로운 기법이 발생할 때마다, 매번 이를 제어하기 위한 경로를 PC제어용 프로그램이나 SW 개발을 통해서 대응하기란 너무 많은 노력과 시간이 소요되며 대응 시기 또한 즉각적인 대응이 불가하기 때문에 항상 완벽한 대응을 기대하기가 어렵게 된다.

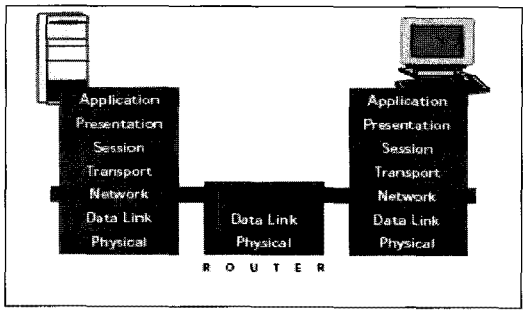
3.2 네트워크 통제방법

기업 내부 정보를 외부로 유출되는 것을 예방하기 위한 측면으로서 네트워크 통제 방법은 방화벽을 통한 통제, 특정 URL명을 지정하는 통제, 애플리케이션 서버를 통하여 통제하는 방법 등 3가지로 분류할 수 있다.

3.2.1 방화벽 통제

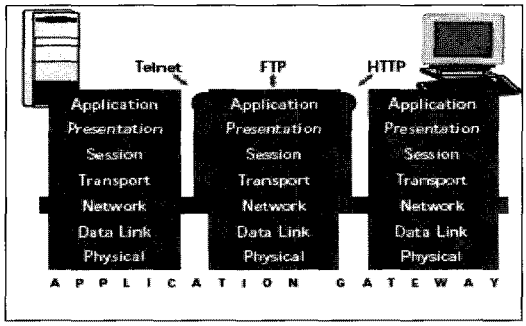
방화벽은 내·외부 네트워크를 보호하기 위한 보안 시스템의 하나로 외부의 불법적인 침입으로부터 내부의 정보자산을 보호하고, 유해정보 유입을 차단하기 위한 정책과 하드웨어 및 소프트웨어를 총칭한다. 또 다른 기능으로는 외부 네트워크와 연동되는 유일한 출입경로로서 인바운드, 아웃바운드의 데이터의 헤더정보를 분석하여 내,외부의 접속을 통제하거나 인증절차를 통해 인가된 사용자를 선별한다. 그리고 접속된 내,외부 네트워크에 대한 트래픽을 모두 기록한다.[6] 기존 방화벽의 유형은 패킷필터링, 프락시, Stateful Inspection형의 세 가지 유형이 있는데 이들의 특징은 그림과 같다.

(1) 패킷필터링형 : 어떤 데이터가 네트워크로 출입할 수 있는지를 통제하는 보안방법으로서, OSI 7 계층 모델의 네트워크와 트랜스포트 계층에 적용 가능한 전형적인 방화벽의 형태로서, IP 패킷과 TCP 세그멘트의 헤더 정보를 통해 허용 및 차단 기능을 Rule이라 부르는 ACL(Access Control List)을 사용하여 이루어진다. 높은 성능과 확장 가능성, 응용프로그램으로부터 독립적이어서 타 방식에 비해 상대적 으로 속도가 빠르다는 장점이 있으나 패킷에서 헤더정보 이상을 조사하지 않아 다른 선택보다 상대적으로 낮은 보안, 연결 상태를 기억하지 않는다는 이슈가 있다.



〔그림 2〕 패킷필터링형 방화벽[7]

(2) 프락시형 : 데몬 형태로 동작하며, 응용계층에서 사용하기 때문에 "프락시 게이트웨이" 또는 "프락시" 라 한다. 패킷 필터링과 같은 접근통제 기능을 제공할 뿐 아니라 서비스별 통제가 가능하고 직접적인 TCP 세션이 없으므로 내부 트래픽 주소를 은폐할 수 있어 Connectionless 상태에서 각 서비스와 세션별 감사가 가능하다. 그러나 프락시 방식은 OSI 7 Layer의 Application Layer까지 올라가고 응용프로그램 및 서비스에 따라 세부적인 내용을 체크하기 때문에, 속도가 많이 느리고 사용환경도 제한적인 경우가 많다 새로운 서비스에 대한 빠른 대응이 불가능하여, 사용자에게 보안성 있는 서비스를 보장 할 수 없다. 속도 저하가 가장 큰 단점이다.

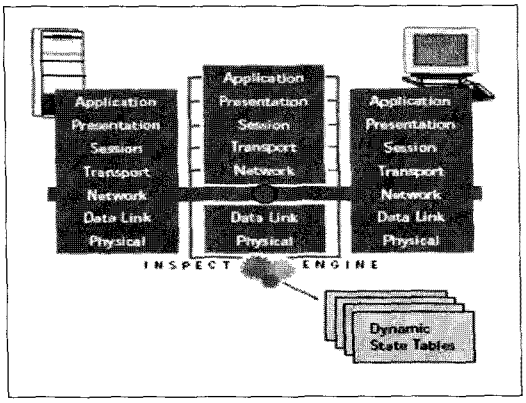


〔그림 3〕 프락시형 방화벽[8]

(3) Stateful Inspection형 : 패킷필터링 방식과 프락시형 방식을 절충한 방식으로, 한 번 방화벽의 보안정

책(ACL)을 통해서 허용된 패킷은 일정 시간 동안 상태 테이블(State Table)에 저장이 되어서, 패킷이 올 때마다 OSI 7 Layer의 Application Layer까지 올라가지 않아도 방화벽에서 허용된 내용에 대한 상태 테이블 정보를 통해, 프락시 방식보다 빠른 속도로 처리를 할 수 있다는 장점과 패킷필터링 방식에서의 단점인 패킷 변조에 대한 취약점을 보강하게 된다.

이들의 장단점을 비교하자면 표 1과 같다.



〔그림 4〕 Stateful Inspection형 방화벽 [9]

〔표 1〕 방화벽 유형별 장단점 비교

유형	기능	장점	단점
패킷필터형	IP주소와 Port를 이용하여 제어	처리속도가 빠르고 단순	TCP/IP 헤더 조작에 대응할 수 없음
프락시형	소스를 감출수 있고, 단순하며, 사용자에게 투명성을 보장	강력한 인증과 부가적 서비스 제공	투명성 보장 못함
Stateful Inspection형	방화벽의 보안정책(ACL)을 통해서 허용된 패킷은 일정 시간 동안 상태 테이블(State Table)에 저장하여 활용	보안성이 높고 성능이 좋다	구축 어려움

3.2.2 URL 통제

기존 방화벽 방식과 달리 패킷분석방식으로 제어하여 네트워크 성능을 보장하면서도 통제가 필요한 관리 용도에 맞게 세부 항목까지 통제 가능토록 해주는 방식의 사례로 URL 통제 방식이 있는데 특징을 비교하면 표2와 같다.

이러한 URL 통제 수단을 통원하면 기업 내 임직원이 업무시간에 비즈니스 외에 인터넷을 이용한 개인적인 일에 소모하는 일과 P2P 프로그램 사용으로 인한 네트워크 대역폭 부족현상, 이로 인한 타인의 업무 방해 및 지연 등 여러 가지 부작용을 예방 할 수 있다. 그러나 URL 통제 툴을 적용한다고 하여 모든 사내 정보를 외부로 유출하는 것을 원천 차단할 수 있는 것이 아니라 여러 불필요한 사이트 접근을 막도록 지원하는 보조적인 활용을 하는 사례라 보면 될 것이다.

〔표 2〕 방화벽과 URL통제 솔루션의 비교 [10]

방화벽	URL 통제 툴
- 네트워크를 지나는 패킷을 일일이 검사 - 패킷을 검사하는 동안 정체현상으로 인해 네트워크 속도저하 발생 - 클라이언트나 메일서버, 웹 프락시 등의 변경이 필요함으로 네트워크 안정성에 위험함	- 네트워크를 지나는 패킷을 수집 - Broadcasting 패킷을 이용하므로 추가 패킷을 생성하지 않기 때문에 속도저하 현상 없음 - 기존 네트워크 구조변경이 없으므로 설치가 간단함
- IP와 Port를 기준으로 차단 - 특정서비스 차단(예, msn메신저 서버IP와 Port 차단)을 처음 설정하면, 수시로 변동되는 것에 대해 대응하기가 힘듬	- IP와 Port를 기준으로 기본 차단과 pattern 차단을 병행 - 특정서비스에 대한 DB(서버IP, Port) 업데이트가 주기적으로 자동적으로 됨
- 정책 설정은 쉬우나 변경은 어려움 - 정책변경시에는 네트워크 사용을 하지 못함	- 정책 설정이나 변경이 간단함 - 정책 변경 시에도 네트워크에는 영향이 없음
- 방화벽 로그에 대한 통계는 모두 수작업으로 계산해야 통계를 산출할 수 있음	- 간단하게 통계 결과를 자동적으로 산출함
- 방화벽 장애발생시에는 임직원이 전체 네트워크을 사용하지 못함	- 툴이 다운되더라도, 자체 서버만 가동이 중단되고, 전체 네트워크에 영향이 없음

3.3.3 애플리케이션 통제

기업 내부 임직원이 외부로 암호화된 형태의 정보를 유출할 경우 이를 통제하기 위한 수단이 필요하며, 외부의 해커가 웹 메일이나 IM, 원격 제어, SSL 애플리케이션 등으로 내부정보를 유출하고자 할 때에도 이에 대비한 체계가 필요하다. 내부에서 외부로 유출될 수 있는 상황을 고려한 통제 가능으로는

첫째, 동적 URL 필터링이 있다. 동적 URL 필터링은 URL 정보를 매칭하여 필터링 여부를 판단하는 것으로서 비인가 사이트 목록을 저장하여 기업 내부 근무자가 근무시간 중에 접속을 못 하도록 차단하여 업무 생산성 향상의 효과가 있다.

둘째, 기업의 주요 업무기밀의 보호하기 위한 내부정보 유출방지 기능이 있다. 웹메일, 웹하드, 메신저 및 암호화된 형태의 기밀 유출을 방지하거나 원격제어 솔루션을 통한 기밀 유출을 방지하고 VontuTM, ReconnexTM, VeriCeptTM등의 콘텐츠 기록 및 제어 솔루션 추가 연동 기능이 있다.

셋째, Authentication, Authorization, Accounting 정책 지원 기능이 있다. 사용자/그룹에 대한 인증 / 권한부여, 활동 감시를 통한 보안 정책 구현하고 사용자, 위치, 목적지, 서비스, 시간, 콘텐트 별 자유롭고 풍부한 정책을 제어하며 프로토콜 별 Method 제어, 인증 유효성 검사 등을 실시하며, 외부에서 원격으로 내부 접속을 시도하고자 할 경우에도 동적 URL에 의한 자동 차단을 한다든지, 원격접속 중계서버 접속을 "Remote Access Tools" 사이트로 분류하여 차단하는 기능이 있고 원격접속 솔루션이 자체 사용 포트 차단 시 80포트, 443포트를 이용하거나 프로토콜 규격 검사를 통한 자동 차단한다든지, 80포트와 443를 이용할 수 있는 agent 를 사전에 정의하거나 해당 agent 가 아닌 경우 자동 차단하는 기능, TCP Tunnel 로 접근하는 모든 사용을 차단하는 기능, 원격 솔루션의 사용 TCP 포트 및 서비스 IP 대역의 차단 기능이 필요하다.

이러한 차단 기능 툴을 이용하여 고도로 암호화 되거나 원격 제어로서 기업내 정보가 외부로 유출되는 사례를 예방할 수 있는 것이다.

3.2.-4 장단점 분석

이상과 같은 네트워크 통제 방식의 장단점을 비교하면 [표 4]와 같다.

〔표 4〕 네트워크 통제 방식의 비교

유형	기능	장점	단점
방화벽 통제	내부 인트라넷과 외부 인터넷망 사이에서 IP, Port로 유출을 통제	- 적용이 단순함 - 안정적 운영 - 비용 저렴	- 복합한 요구사항을 모두 수용하기 곤란 - 정책 변경시 마다 네트워크 영향 큼
URL 통제	패킷을 별도 수집하여 URL 저장정보와 비교 판단함	- 정책변경 자유로운 편 - 네트워크 속도저하 우려 없음	- URL만 통제 (Port 위장시 불가) - 추가 비용 발생
애플리케이션 통제	네트워크 정보를 프락시 장비에서 상세하게 80, 443 포트등을 분석, 판단함	- 암호화된 트래픽 까지 분석할 수 있음 - 원격제어로 침입이나 유출시 대응 가능 - 상세 통제 가능	- 속도 저하 - 비용 가장 고가 - 기 정의된 엔진만 지원함

3.3 데이터 암호화 저장 방법

개인 컴퓨팅 환경에서 저장 이벤트가 발생되면 데이터 자체를 암호화 하여 저장하는 방법으로, 이는 데이터가 유출되더라도 항상 암호화된 상태에서 유출되기때문에 복호화 키가 없는 한 정보자체가 안전하게 보호될 수 있다는 장점이 있다. 문서 암호화를 의미하는 DRM은 "Digital Rights Management"의 약자로 디지털 정보의 신뢰성 있는 유통환경을 제공하기 위해 라이센스, 안전한 저작권과 허가, 신뢰성 있는 환경과 인프라를 가능하게 하는 H/W, S/W 를 포함하는 디지털 저작권 관리를 위한 넓은 의미의 기술, 절차, 처리, 알고리즘을 의미한다. 이를 위해서는 컨텐츠를 정해진 규칙 내에서만 사용되도록 지속적인 제어 기능, 특정 사람/기기에서 인쇄, 복사, 저장, 사용기간, 횟수 등 사용범위를 제어할 수 있는 기능, 컨텐츠의 저작권 보호 및 문서보안의 기반기술 기능이 필요하다. [11] 이를 구현하는 방법에는 저장할 때마다 해당 파일을 암호화 하는 방식(서버 DRM, PC-DRM)과 HW적으로 특정 폴더의 데이터만을 암호화하는 방식, 윈도우 OS 암호화 방식으로 분류된다.

3.3.1 저장할 때 마다 암호화하는 방식

패키징(암호화)되는 시점에 따라 서버DRM과 PC DRM으로 나눌 수 있다. 서버 DRM은 시스템에 업로드 되는 시점에서 암호화를 하고, PC DRM의 경우 PC 내 문서가 저장되는 순간에 암호화되어 저장된다. 서버 DRM의 경우 회사내 중요 시스템에 대한 선별적인 보안 적용이 가능한 장점이 있으나 전사적인 문서보안 유통을 대상으로 보안을 구축하기 위해서는 PC DRM이 반드시 고려되어야 한다. PC DRM의 기본 정책으로서는 첫째, PC內저장되는 모든 문서는 저장되는 순간 보

〔표 5〕 데이터 암호화 저장 방식 유형에 따른 장단점 비교

유형	기능	장점	단점
PC DRM	문서 저장시 암호화 실시	- 문서 포맷에 따라 암호화 여부 결정 - 가장 강력한 암호화 방식	.- 정의되지 않은 파일 포맷은 평문 저장 .- 파일 포맷에 따라 암호화 제한적
특정 폴더 암호화	PC내 특정폴더내의 저장 파일은 모두 암호화 함	.- 파일 포맷에 영향받지 않음 .- 손쉽게 적용 가능 .- 악의적인 자료 유출시 효과있음	- 폴더 이동시 복호화 되므로 한계 있음
윈도우즈 OS 암호화(MS EFS) 방식	하드웨어 블럭단위 암호화 함	- 하드디스크 분실시에도 안전 - 악의적인 자료 유출시 효과 있음	- OS로 로그인 되었을 때는 통제 불가

안등급을 지정하고, 강제 암호화되어 운영 되어야 하며, 허가된 사용자만이 문서를 사용하도록 권한(조회, 인쇄, 변경, 저장 등)이 통제되어야 한다. 둘째, PC內사용되는 모든 문서는 생성부터 폐기까지 모든 문서의 사용이력(조회, 인쇄, 변경, 저장, 삭제 等)이 보관되어야 하며 사고 발생시 추적이 가능해야 한다. 셋째, 업무상 외부로 PC 혹은 문서반출이 필요한 경우 회사에서 허가한 방법에 의하여 반출 되어야 한다.

이러한 정책을 수행하기 위한 기본 기능으로서는 유통되는 모든 문서에 대한 사용통제, 유통되는 모든 문서에 대해서 사용내역 추적, 모든 문서 출력시 출력자 정보 삽입이 필요하며 추가로 개인별 사용 현황, 이력분석과 문서 추적관리 기능도 부가될 수 도 있으며 추가로 기업 내 관리되고 있는 PC 자산관리, PC 반출입관리 기능까지 연계되어 다양한 보안 활동을 지원하는 기법으로 진화하고 있는 중이다.

3.3.2 HW 특정 폴더 암호화 방식

PC내의 지정된 특정 폴더에 파일을 저장시에 무조건적으로 암호화를 시킨다. 파일을 암호화 시켜 저장하는 장점이 있긴 하나 사용자가 저장 위치를 임의로 조정 가능하기 때문에 해당 폴더 이외의 장소에 저장된 파일에 대해서는 100% 암호화되었다고 보장할 수 없는 한계점이 있다.

3.3.3 윈도우즈 OS 암호화(MS EFS) 방식

윈도우즈는 보안강화를 위해 NTFS라는 액세스 권한을 사용하여 파일에 액세스 할 수 있는 유저를 제한할 수 있다. 그러나, 액세스 권한을 설정하는 것만으로 안전하다고 할 수 없어서 추가로 보완한 방법이 EFS(Encrypted File System) 방식이다. NTFS는 파일 시스템 드라이버를 경유하는 액세스는 권한을 체크하지만 다른 OS로부터 직접 하드디스크를 액세스하는 경우에는 컴퓨터를 플로피 디스크로 기동한 경우, 플로피 디스크로 MS-DOS를 기동하여 NTFSDOS등의 툴을 이용하면 NTFS 드라이브의 내용을 액세스 권한이 없더라도 읽을 수 있다. 또한, 하드디스크를 다른 컴퓨터에 접속하는 경우, 하드디스크를 접속한 컴퓨터의 관리자 권한만 가지고 있다면 파일의 내용을 자유롭게 열람할 수 있다. 기밀 데이터가 보관되어 있는 하드 디스크가 도난당하면 NTFS의 액세스 권한으로 아무리 데이터를 보호하고 있어도 데이터는 노출되게 된다. 최근에는 오래된 컴퓨터를 파기하는 경우에도 이 부분이 문제가 되고 있다. EFS(암호화 파일 시스템)를 사용하면, 파일을 암호화하여 보존하므로 이러한 문제를 해결할 수 있다. 하드 디스크를 분실해도 EFS를 사용하여 암호화한 파일은 복호화 키를 가지고 있지 않은 한 내용을 읽을 수 없다. EFS는 NTFS의 드라이버와 연계되어 있어 파일의 암호화 및 복호화는 유저가 알지 못하게 실행된다. 유저는 암호화가 설정된 파일에 액세스 할 경우에 EFS가 사용되고 있는 것을 느끼지 못하고 읽을 수 있다. 또한, 해당 파일을 다시 보존하면, 다시 암호화되어 보존된다. EFS 방식의 경우 하드디스크가 도난, 분실되더라도 암호화 방식을 이용하게 한번 더 안전하게 데이터를 보관 할 수 있으나 윈도우즈 계정과 패스워드가 악성코드 등 다른 경로로 노출된 경우에는 방어가 어려운 한계점이 있다.

암호화 저장은 개인PC에 중요정보를 안전하게 저장하기 위한 대책이지만, PC 내 중요정보를 저장하는 구조이기 때문에 개인이 실수로나 악성코드에 의해 인지하지 못하는 동안 인증정보를 노출하는 경우에는 중요정보는 언제든지 노출될 수 있다.

3.3.4 장단점 분석

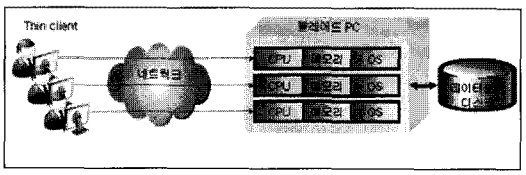
이상과 같은 암호화 저장 방식의 장단점을 비교하면 표5와 같다. 그러나 암호화를 지원하는 파일 포맷의 종류가 제한되어 있어 모든 업무에 적용할 수 없는 제한점이 있다. 특히 프로그램 소스나 실행파일을 암호화 저장하면 이를 실행하는 방법이 곤란해진다.

3.4 NC컴퓨팅

본래 네트워크 컴퓨팅(Network Computing, 이하 'NC'라 함)이란 메인프레임의 더미터미널 개념에서 유래하였으나 현재는 가상화 기법으로 까지 진화되고 있다. 핵심 개념은 기본 처리와 저장은 중앙서버에서 처리하고, 사용자 PC 사양을 최소화하여, PC내 저장요소를 최소화 하거나 없앤 모델로서 개인 PC내 저장 매체를 없애는 취지에서는 강력한 정보보호 효과가 가능하다고 볼 수 있다. 전통적인 PC방식에서는 개인이 일반PC를 혼자 소유하여 사용함으로써 개인으로서는 최고의 성능과 다양한 유연성을 확보할 수 있는 반면, 개인 PC 내의 데이터는 제어할 방법이 어려운 것이 사실이다. 반면 보안 강화 측면이 강조된 중앙집중식 PC는 클라이언트를 가상화 하거나 원격 PC 제어 방식을 도입한 사례로서 블레이드피씨(Blade PC), 터미널서비스/SBC 방식(또는 화면전송형), 가상PC의 세가지 종류가 있다.

3.4.1 블레이드피씨 型

최소형화된 PC를 여러대씩 한 개의 Rack에 넣어, 중앙기계실에서 통합관리 하는 방식으로 개인은 씬클라이언트 방식의 단말을 사용하고, PC본체라 할 수 있는 CPU와 메모리는 중앙 전산실 위치한다. 이때 중앙

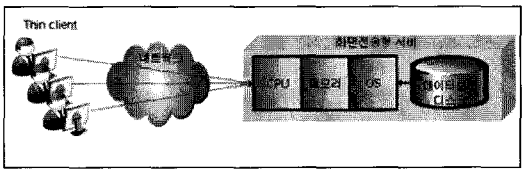


〔그림 5〕 블레이드피씨형 개요도

전산실의 PC는 개인별로 할당 되는 개념이며 개인은 씬클라이언트에서 이미지만 전송 받으므로 NW 부하가 적고 서버가 개인별로 할당되기에 서버 부하도 경감될 수 있으며 중앙에 있는 개인의 컴퓨팅 디바이스상의 각종 OS나 SW를 일원화 관리 하므로 보안관리 측면도 유리하고 기존 PC 환경대비 사용자 편리성이 가장 유사하다. 그러나 개인별 데이터를 통합 서버내에 관리함에 따라 관리의 복잡성이 수반되고, 중앙접속 시스템 이상시 업무 연속성 지속 유지 방법을 고려해야 한다.

3.4.2 화면전송 型

화면전송형 방식은 다른 용어로 애플리케이션 가상화 방식, 터미널 서비스, SBC (Server Based Computing) 방식 이라고도 한다. 이 방식은 대형서버에서 프로그램을 실행, 저장하고 단말기에서는 단순히 화면조회를 하는 방식으로 개인 단말은 씬클라이언트 개념으로, 모든 작업 처리와 저장은 중앙 서버에서 담당한다. 개인은 이미지만 전송 받아 네트워크 부하가 적고, 서버가 모든 사용자 작업을 담당하기에 대용량 서버가 필요하며, 중앙에 있는 개인의 컴퓨팅 디바이스상의 각종 OS나 SW를 일원화 관리 하므로 보안관리측면이 유리해지나 항상 사용자 개인PC와 데이터센터내의 중앙 서버가 네트워크로 연결되어 있어야 하며, 네트워크의 부하가 발생하기에 대량의 많은 인원을 한꺼번에 수용하기에는 많은 네트워크 비용이 수반되며, 개인별 데이터를 통합 서버내에 관리함에 따라 관리의 복잡성 수반되고, 기존 PC 환경대비 사용자 편리성이 낮은 단점이 있다.

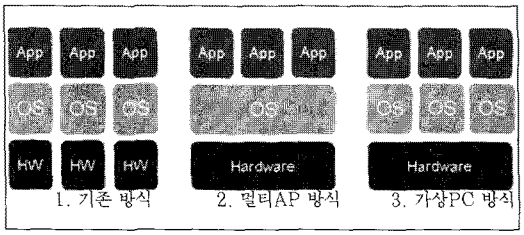


〔그림 6〕 화면전송형 개요도

3.4.3 가상PC 型

컴퓨팅 기술이 발전하면서, 컴퓨터 성능이 기존에 비하여 획기적인 발전을 하였지만, 애플리케이션을 단일 OS에 운영하는 것은 기술적 및 운영적인 제약이 있어, 또 다른 방안으로 가상화 기술이 연구되기 시작하였다. 그림 7에서 보듯이 기존의 전통적인 컴퓨팅 방식은 하나의 하드웨어 위에 하나의 OS가 올라가고 그 위에 여

러 가지 애플리케이션이나 소프트웨어가 탑재되어 구동되는 방식(1. 기존 방식)이었다. 그런데 하드웨어 성능의 획기적인 발전에 따라 하드웨어의 리소스를 효율적으로 사용하기 위하여 여러 개의 애플리케이션을 운영할 수 있는 방안으로 멀티 애플리케이션 방식이 도입되었다.(2. 멀티AP 방식) 앞 절에서 설명한 화면전송형 방식도 이러한 사례중의 하나이다. 그러나 이 방식은 첫째, 애플리케이션 장애가 전체 애플리케이션 장애로 전파되고 둘째, OS 리소스의 격리가 불가하다는 단점이 따른다. 이러한 단점을 극복하기 위해 애플리케이션 및 OS의 격리를 제공하고 파티셔닝을 이용한 가상의 서버 환경을 제공하는 가상PC 방식으로 진화가 이루어 졌다.(3. 가상PC 방식) 이 방식은 첫째, 애플리케이션별로 별도의 OS 환경을 지원하고 둘째, 시스템 자원의 격리 및 최적화된 사용을 보장할 수 있으며 셋째, H/W에 독립적인 표준 서버 인프라를 구축할 수 있다는 장점이 있다. 그러나 하나로 구성된 하드웨어에서 모든 OS가 작동하므로 하드웨어 장애가 발생할 경우 모든 애플리케이션이 장애 영향을 받게 되고 다수의 사용자가 집중되는 경우 하나의 하드웨어에 접속하기 위한 네트워크 부하가 발생한다는 단점이 있다.



〔그림 7〕 컴퓨팅 기술 발달에 따른 가상화 환경으로 진화

3.4.4. NC컴퓨팅의 장단점 비교

이상과 같은 네트워크 통제 방식의 장단점을 비교하면 표6과 같다. 블레이드피씨형은 다른 방식에 비하여 상대적으로 장점을 많이 보유하고 있으며, 화면전송형은 여러 가지 장점이 있으나 서버 성능에 의존적이며, 특히 하나의 서버에 많은 접속자가 집중될 경우 부하 처리에 문제점이 노출되고 비싸다는 단점이 특징이다. 또한 가상PC형은 새로이 부상되고 있는 기술로서 현재 적용된 실제 적용 사례(Reference site)가 미흡하다는 단점도 있다.

〔표 6〕 NC컴퓨팅 방식 비교표

평가 항목		블레이드 피씨型	화면전송型	가상PC型
구성 아키텍처	서버 규모	중형	대형	대형
	디스크	중형	대형	대형
	단말 규모	최소	최소	최소
	서버 부하	보통	많음	많음
	네트웍 부하	낮음	낮음	높음
관리성	업무 연속성	유지	중단 있음	중단 있음
	신규 프로그램 설치	개인 배포	관리자조치	관리자조치
	사용이력 로깅	가능	가능	가능
	해킹 위협	낮음	중간	중간
사용자	개인/그룹별 SW환경 제공	가능	불가	가능
	사용자 속도	빠름	빠름	보통
	기존 PC대비 불편성	낮음	높음	높음
	비용	저가	고가	고가

3.5 문제점 제기

이상과 같이 Ⅲ장에서는 기업에서 내부 정보 유출을 예방할 수 있는 조치와 기술적 접근법에 대해 검토해 보았고 이를 표7에 정리하였다. 결국 어떠한 접근 방법

〔표 7〕 정보 유출 통제 방식 비교표

유형	개요	장점	단점
PC 통제	PC IO장비를 통한 데이터나 정보 유출을 예방하는 툴을 적용 차단함	개인PC를 툴로 관리	새로운 장비나 기술의 발달속도에 대응하기 어려움
NW 통제	외부로 연결된 네트워크에서 유출정보를 차단	사용자 편리	네트워킹을 통한 정보유출 예방으로 한정
암호화저장	데이터를 암호화하여 저장	가장 강력한 예방 방식	기술 성숙도가 미숙하여 암호화 지원 안 되는 파일포맷이 있음 특히, 프로그램소스를 실행할 수 없음
NC 컴퓨팅	데이터를 중앙서버에 저장	정보 유출 원천 예방 가능	인터넷 접속 등 사용자에게 불편, 비용이 소요

도 기업 내부 정보 유출 예방을 위한 하나의 독립된 모범답안으로서는 해법을 제시해 주지 못하고 있다.

Ⅳ. 새로운 개선 대안 도출

4.1. 비즈니스 요구사항에 따른 구현방안 검토

A사의 경우, 기존의 프로그램 개발업무를 회사 외부에 위치한 개발센터를 활용, 아웃소싱하는 방식을 채택하게 됨에 따라 이에 상응하는 프로그램 소스 유출 방지를 위한 보안 관리 방안을 연구를 착수하게 되었다. 이에 따른 대표적인 요구사항은 첫째, 기존의 내부 개발자의 개발환경과 외부 개발센터에 개발 환경이 동등해야 하고 둘째, 내부 개발자와 외부 개발센터의 개발자간의 업무 교환 프로세스가 필요하며, 셋째, 업무별로 접속권한이 각기 다르게 적용되므로 동일한 업무를 수행하는 내부 개발자와 외부 개발자만이 동일한 소스를 공유토록 해야 한다. 넷째, 외부 개발센터 개발자는 원할한 업무 수행을 위하여 사내 메일과 인터넷 사용이 가능하여야 한다.

이에 따른 최적 대안을 도출하기 위해 앞에서 검토한 여러 가지 통제 방식에 대해 우선 순위를 부여하기 위해 XY매트릭스법으로 유효성을 평가하기로 한다. 평가요소로서는 기업 활동에 필요한 내용을 중심으로 6개 항목을 선정하였다.

(1) 비용

기업 활동에 가장 민감한 항목인 비용을 첫째 항목으로 꼽았다. 다른 방식과 비교하여 상대적으로 가격이 낮으면 3점, 높으면 1점을 부여한다.

(2) 속도

사용자가 해당 방식을 사용할 때 체감할 수 있는 응답속도를 의미한다. 다른 방식과 비교하여 상대적으로 속도가 빠르면 3점, 늦으면 1점을 부여한다.

(3) 사용 환경

개인 사용자 환경의 편리성을 의미한다. 다른 방식과 비교하여 상대적으로 사용자가 부담없이 PC를 사용하듯이 편리하게 이용하는 환경이면 3점, 개인 PC 사용보다 많이 불편하면 1점을 부여한다.

(4) 안정성

해당 방식을 이용하였을 때 해당 인프라가 얼마나 안정적으로 유지되는가에 대한 평가이다. 기술적으로 성숙하여 안정성이 높으면 3점, 낮으면 1점을 부여하고, 특히 초기 도입된 기술로 Reference Site 가 없으면 0점 처리 한다.

(5) 호환성

해당 방식을 사용하였을 때, 다른 기기들과 연결하여 사용이 가능한가에 대한 평가이다. 다른 방식과 비교하여 상대적으로 호환성이 좋으면 3점, 낮으면 1점을 부여한다. 그러나 호환이 전혀 불가할 경우 0점 처리한다.

(6) 통제성

정보 유출을 통제하는 효과 정도를 평가하였다. 해당 방식을 사용하였을 때 다른 방식과 비교하여 상대적으로 정보유출을 원천적으로 예방 가능할 경우 3점, 상대적으로 유출 가능성이 클 경우 1점 처리한다.

평가 대상중 PC통제 방식은 항상 위협 요인이 있는 것으로 간주하여 평가를 제외하였다.

이상과 같은 기준으로 방식을 유효성을 평가하여 본 결과, 표8 과 같이 방화벽 방식이 16점으로 가장 높았으나 네트워크 방식 자체가 PC데이터를 외부 유출 할 수 있는 여러 가지의 경로 중 하나의 종류에 국한되는 지엽적 수단임을 감안하여 NC컴퓨팅의 블레이드피씨형을 1순위로 선정하였다.

〔표 8〕 통제 방식 비교표

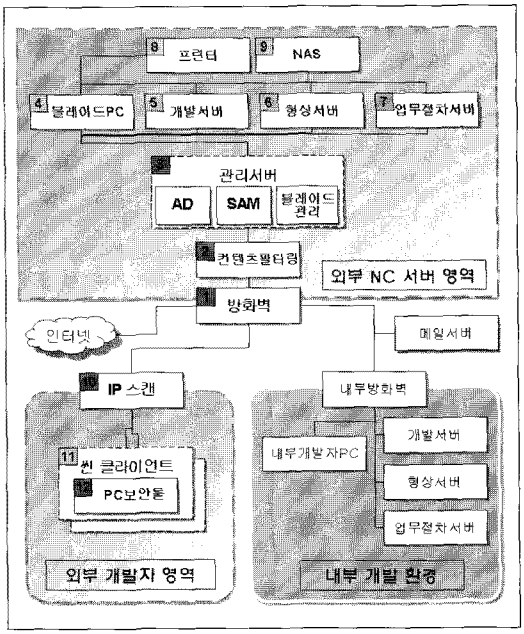
평가 항목		비용	속도	사용환경	안정성	호환성	통제성	계	비고
NW 통제	방화벽	3	3	3	3	3	1	16	지엽 수단
	URL	1	2	3	2	3	2	13	
	프락시	1	1	3	1	3	3	12	
암호화저장	문서DRM	2	3	1	1	0	3	10	기술성숙미숙
	OS DRM	3	3	2	0	2	1	11	
	폴더DRM	2	3	2	1	2	1	11	
NC컴퓨팅	블레이드	2	2	3	3	2	2	14	1순위
	화면전송	0	1	1	2	1	3	8	
	가상PC	2	1	2	0	1	2	8	

선정된 블레이드피씨형 NC컴퓨팅 방식을 기반으로 개선 대안을 찾도록 하겠다. 우선 블레이드피씨 방식의 문제점 및 제한 사항을 알아보도록 하겠다. 블레이드피씨 방식은 화면전송방식에 비해 개인 사용자에게 높은 성능과 자율성을 제공하고 있지만 자료 전송 통제 기능은 거의 제공하지 않고 있다. 즉, 사용자가 임의의 프로그램을 설치하여 블레이드피씨에서 사용자 PC로

파일을 전송할 수 있을 뿐만 아니라, 블레이드피씨에서 제공하는 RDP 자체에도 파일을 전송하는 기능이 있어 이를 통제하는데 어려움이 있다. 또한, 다른 NC컴퓨팅 방식처럼 사용자에게 프로그램 설치 기능을 부여하지 않았을 경우 프로그램 개발 업무의 제약이 발생할 수 있다. 실제 프로그램 개발 업무에서 디버깅 및 일부 사용자 편의 프로그램 설치가 어려울 경우 사용자가 이용할 수 조차 없는 문제점이 된다. 이러한 문제점을 극복하기 위하여 보완 수단으로 AD(Active Directory)와 NW 보안통제(방화벽, URL 필터링 툴)을 적용하여 자료 통제에 활용하기로 한다.

첫째, AD(Active Directory)을 이용하여 사용자 인증과 RDP의 파일전송 기능을 비 활성화시킨다.

둘째, 중앙에서의 비인가 프로세스(FTP와 같은 자료전송 툴)를 통제한다 이때는 NW 보안통제(방화벽, URL 필터링툴)을 활용하여 RDP(3389/tcp)를 제외하고 All deny 정책을 적용한다. 단, 예외사항으로 보안 업데이트 및 관리 포트만 오픈하며 사내 시스템의 경우 특정 URL만 오픈해 준다.



〔그림 8〕 블레이드 방식을 채택한 NC컴퓨팅 개념도

4.2. 구현상의 특이사항

외부 개발 환경을 「외부 NC서버 영역」과 「외부 개발자 영역」으로 구분하여 신규 구성하고 기존의 기업내 「내부 개발 환경」과 연결되도록 하여 신규 환경을 그림8과 같이 구축하였다.

(1) 방화벽 : 외부 NC 영역의 네트워크 접근 제한을 위해 설치한다.

(2) 컨텐츠 필터링 : 외부 개발자가 블레이드피씨에서 내부 개발 환경에 있는 기존의 사내 시스템을 접근하기 위한 방안을 허용하기 위하여 설치한다.

(3) 관리서버 : 외부 NC 서버 영역내에 있는 블레이드피씨를 개발자별로 할당, 관리하기 위한 목적으로 설치한다. 여기에는 AD(Active Directory) 서버, SAM (Session Allocation Manager)서버, 블레이드관리서버 등이 있다.

(4) 블레이드피씨 : 외부 개발자가 자신이 개발하기 위해 서버영역에서 인당 하나씩 할당받는 개별 PC의 집합체

(5) 개발서버 : 외부 개발자가 프로그램 개발을 하면서 테스트를 하기 위한 개발환경의 테스트용 서버

(6) 형상서버 : 외부 개발자가 개발한 프로그램 소스를 저장하는 장소. 이 서버는 내부 개발환경에 있는 형상서버와 동기화 작업을 수행하게 된다.

(7) 업무절차서버 : 외부 개발자가 내부 개발자로부터 개발 요청부터 완료까지의 단계를 진행할 수 있도록 업무 프로세스 진행을 위한 사내 시스템이 설치된 서버. 이 서버도 내부 개발환경에 있는 업무절차서버와 동기화 작업을 수행하게 된다.

(8) 프린터 : 블레이드피씨에서 작성된 내용을 인쇄하면 출력되는 프린터로서 외부개발자는 NC서버 영역내에서 이루어진 산출물의 출력을 이 곳을 통해서만 출력할 수 있어 출력물에 대한 보안통제가 가능해 진다.

(9) NAS : 외부 NC 서버 영역에서 작업되어진 데이터들이 저장되는 장소로서 개발자 간의 공유해야 할 자료들의 자료 공유를 손쉽게 하기 위해 NAS DISK를 선정하였다.

(10) IP스캔 : 외부 개발자용 씬클라이언트들간의 LAN환경을 모니터링하고 IP통제를 할 수 있는 용도로 설치하였다.

(11) 씬클라이언트 : 개발자가 할당받는 하나의 PC

로서 인터넷이나 사내 메일 접속은 자유롭게 할 수 있으나 업무상 개발된 프로그램 소스는 저장할 수 없도록 네트워크 통제를 받는 것이 특징이다.

(12) PC보안툴 : 개발자의 씬클라이언트에서 발생할 수 있는 보안 이슈를 미리 예방하기 위하여 설치한 보안강화 프로그램이다.

이러한 신규 아키텍처의 보안적 특징을 살펴보면 다섯가지의 주요한 특징이 있다.

(1) 방화벽

RDP 3389 Inbound 포트 만을 Open 하고 All Deny 모드를 취한다. 즉, 서버에 있는 저장 정보를 씬클라이언트에서 볼 수 있도록 보내는 RDP 포트만을 통과시키고 나머지 모든 포트는 막아 놓음으로서 서버에 저장된 개인별 블레이드피씨내의 정보가 관리영역이외로 유출되는 것을 원천 차단시킨다. 단, 관리자의 경우 Active Directory나 SAM 관리서버에 접속이 가능하여야 하므로 인가된 자에 한하여 AD나 SAM서버 접속용 80포트만을 Open 시킬 수 있도록 허용한다. Open 절차는 별도의 인가 프로세스를 두어 운영토록 한다.

(2) 컨텐츠 필터링

첫째, 개발자가 서버에 있는 개인의 블레이드피씨 영역에서 사내 시스템을 사용하고자 할 때, 모든 사내 시스템은 기본적으로 Single Sign On 이 되어야 이용 가능하기 때문에 본사에 있는 레가시 시스템과 개발자의 서버영역 사이에 Single Sign On이 가능하도록 방화벽이 열려 있어야 하며, 둘째, 서버 영역에 있는 형상관리 서버와 본사에 있는 형상관리 서버간의 소스 전송, 복제를 위해 방화벽이 열려 있어야 한다. 이를 위해서는 모든 방화벽 경로를 막아 놓았으므로 컨텐츠 필터링 기능을 이용하여 SSO, 형상서버와 같은 특정 URL만 허용토록 한다. 컨텐츠 필터링이 아닌 프락시 방식을 이용하여 더욱 자세한 필터링을 적용할 수도 있겠으나 프락시 방식의 경우 컨텐츠필터링에 비하여 3배 이상의 고가장비이기에 컨텐츠 필터링 방식을 채택하였다.

(3) 관리서버

(3)-1 Active Directory 인증

조직별 인원관리를 위한 AD설계를 적용 하였다. 실질적인 업무 조직과 동일한 형태로 액티브 디렉토리 논리구조를 설계하여 권한 제어까지 연계 하였다. 이렇게 되면 예를들어 신입사원이 배치되더라도 소속된 해당 조직트리내로 등록이 되고 나면 그에 따른 블레이드피씨를 할당받고 NC 서버 영역내에 허가된 정보 자원만 접근할 수 있도록 제어가 된다.

또한 AD는 본래 3389 포트를 이용한 파일 전송이 가능하다. 이를 통한 정보 유출을 예방하기 위하여 3389 포트를 통한 파일 전송이 불가하도록 Global Policy를 차단한다. 관리자 등 특정 인원이 이를 사용하기 위해서는 선별적인 인가 프로세스를 통해서 허용토록 관리한다.

(3)-2 SAM

SAM서버는 AD를 통해 사용자가 등록되면 이들이 사용할 서버내의 블레이드피씨 영역을 할당하고 이후 사용자가 접속할 때마다 해당 블레이드피씨로 자동 연결시켜주는 역할을 수행하게 된다.

(3)-3 블레이드 관리서버

서버내에 있는 블레이드피씨의 관리 역할을 수행한다. 예를들어 사용자별로 해당되는 OS나 SW를 설치하고 해당 OS의 패치가 필요할 경우 일괄 자동 패치작업 등을 수행하는 역할을 담당한다.

(4) IP Scan

첫째, 개발자 환경에서 비인가된 PC가 접속되면 네트워크 접속을 차단시키는 역할과 둘째, 개발자의 씬클라이언트에서 IP변경이 일어날 경우 네트워크 접속이 불가하도록 관리한다. IP변경을 통제하는 이유는 IP변경으로 인해 일어날 수 있는 MAC Spoofing 으로 비인가자가 서버 접속을 시도할 수 있기 때문에 사전 예방차원에서 점검하는 것이다. IP변경 통제의 원리는 ARP(Address Resolution Protocol)를 이용하여 LAN 구간 모니터링을 통해 씬클라이언트의 IP와 MAC 값을 감지한 후, 사전에 등록된 IP MAC Address Mapping Table의 값과 일치하는지 여부를 점검하여 해당 값이 틀릴 경우 네트워크 통제 조치를 취하는 것이다.

(5) PC보안 솔루션

이미 대다수의 정보는 서버에 저장되어 있으나 이중보완 차원으로 개발자 개인이 사용하는 씬클라이언트를 통한 정보 유출을 예방하기 위하여 씬클라이언트에 PC보안 솔루션을 적용한다. 이런한 툴을 이용할 때의 효과는

. USB, CD등의 매체에 Write 기능 제한

. 무선 LAN, 모뎀 차단

. IP 변경 통제(이미 IP Scan에서 조치하고 있으나 이

중으로 보완조치를 취함)

. 비인가 소프트웨어 설치 차단 등을 통해 씬클라이언트내 정보를 외부로 유출할 수 없게 된다.

4.3 보안정책의 적용

외부 개발센터의 보안성을 향상하기 위해 기술적 접근을 통한 인프라 적용을 하였으나, 이를 실제 운영함에 있어 제반 보안 정책을 준비하였다.

4.3.1 준수 사항

(1) 외부 개발센터에서 개발되는 소스는 별도의 공동서버에서 보관한다.
(2) 외부 개발센터의 소스를 보관하는 장소에는 비인가자가 접속 할 수 없다.
(3) 중앙 NC서버에 저장된 산출물과 소스는 개인 PC에 저장할 수 없음을 원칙으로 하지만, 관리자의 인가를 받을 경우에 한하여 내려 받기가 가능토록 한다.
(4) 중앙 NC서버 접속시에는 항상 관리용 서버를 경유하여 접속해야한다.
(5) 관리용 서버에서는 접속자의 권한을 점검해야 한다.
(6) 개발자의 개인PC에서 사용하는 이력은 모두 사내 보안 규정에 의거하여 로깅 관리를 한다.

4.3.2 외부 개발센터 개발자 업무 처리

외부 개발센터 개발자의 개인 PC에는 개발 소스가 없어야 하며 개발자의 개인 PC에서 서버영역으로 저장하는 방법도 불가하다.

(1) 개발업무 : 블레이드피씨에서 프로그램 소스를 작성 한다.
(2) 문서인쇄 : 블레이드피씨에 저장된 문서 인쇄시 관리자에게 출력 요청하며, 개발자 씬클라이언트 PC의 개인문서는 개인별 출력가능하다.
(3) 사내메일 : 개발자 PC에서만 접속가능하고, 블레이드피씨는 사내메일도 접속할 수 없다.
(4) 인터넷 : 개발자 PC에서만 접속 가능하다.
(5) 개발서버 및 형상관리 서버 : 업무에 따라 블레이드피씨에서만 접속가능(SSO 접속) 하다.
(6) 개발자는 항상 주어진 IP내에서만 네트워크 접속 가능하며, 자의적으로 해당 IP를 변경하는 사례에는 네트워크 접속 불가하다.

4.3.3 보안 관리자의 업무 처리

(1) NC 시스템 운영관리
- AD서버에서 계정 발급 및 사용자(관리자) 권한부여와 삭제
- 보안 취약점 및 보안 정책 우회경로 탐색 및 차단
- 블레이드피씨의 관리자 권한 제거
- 개발자 PC와 블레이드피씨의 파일 전송 권한부여

(2) 보안 시스템(방화벽, 컨텐츠필터링툴, IPScan) 운영관리
- 신규 사용자 및 임시 사용자 IP Address 통제함
- 개발센터 外部 네트워크(사내 개발서버 等)와 NC 영역의 접근 통제한다.
- 불필요 정책 제거 및 정기, 비정기 모니터링을 실사한다.

(3) 주기적인 보안장비 모니터링 및 취약점 제거
- 개발자 PC, NC 영역, 개발서버의 취약점 점검 및 제거, 개발자 PC를 수시점검을 통해 개발자 PC에서 개발소스가 발견時 경고조치 한다.
- 외부 NC 서버 영역의 출력물 차단을 위해서 기계실內部에 프린터를 설치하고 중간 관리자(그룹장)에게만 출력권한을 부여하며 출력물 반출은 보안담당자가 일괄 처리한다.

4.3.4 방화벽 및 컨텐츠 필터링 툴 등록 절차

예외적인 인가 신청을 할 경우는 아래와 같은 절차를 수행하여 관리자로부터 인가된 건에 한 하여 예외처리를 허가 한다.

신청(개발자 기안) → 관리자 1차 검토(그룹장 합의) → 보안성 검토(보안관리자 합의) → 관리자 2차 검토(센터장 결재) → 등록(운영자 통보)

4.4. 적용 효과

이상과 같은 방안으로 외부 개발센터에 새로운 인프라를 적용함으로서 얻을 수 있는 효과는 다음과 같다.

(1) 외부 센터의 개발자가 개발한 소스 또는 생성한 문서를 중앙서버에서 보호할 수 있어 자료 유출로부터 원천적으로 안전하게 보호할 수 있다.

(2) 사고 발생시 기록된 로그 추적으로 완벽한 분석이 가능하다.

(3) 인가 받지 않은 사용자의 블레이드피씨 영역 통제 (AD를 이용하여 사용자권한 분류)가 가능하고 사용 이력을 보관할 수 있다.

(4) 사용자(개발자)의 빈번한 교체에도 자료의 연속성을 보장할 수 있다.

(5) 까다로운 보안구성에도 불구하고 사용 편의성과 개발 효율성은 저하되지 않는다. 즉, 개발자의 인터넷 및 사내 메일 사용은 자유롭다.

(6) 외부 개발센터와 사내 사업장과 자료 공유가 용이하다.

(7) 사용자별로 희망하는 환경구성이 용이하다.

즉, 사용자가 요구하는 O/S, Program 등을 중앙에서 사용자/부서별로 손쉽게 제공할 수 있고 다양한 O/S 환경에도 사용이 가능하다.

(8) 정보자산이 물리적으로 분리되어 개인PC의 물리적인 유출이 일어나도 주요 정보보호대상(프로그램 개발소스)은 외부 유출이 안 된다.

(9) 임시 사용자(출장자 및 임시 개발자)에게는 공용 블레이드피씨를 동적으로 제공할 수 있어 비용 효과가 효율적 이다.

V. 결 론

기업에서 산업기밀 유출 관련자는 대다수가 퇴직자, 현직사원, 협력업체 직원 등 기업 내부 근무자로 비롯되고 있어, 기업체에서는 내부 근무자를 통한 정보 유출을 예방하는 방안에 대해 많은 고민을 하고 있다.

이를 극복하기 위한 방안들에 대한 기존의 논문들을 분석한 결과, 개인 PC중심 관점에서, 제한적으로 정보유출을 예방하는 방안과 네트워크컴퓨팅 방안을 활용한 정보유출 예방 방안이 있었으나 모두 기업 환경의 다양한 환경요소까지 다루지 못한 한계점이 있었다.

본 논문에서는 기업 내 다양한 컴퓨팅 환경에서 정보기술 유출을 예방할 수 있는 관점을, 개인 PC내에 저장된 정보가 외부로 나가는 방법을 통제하는 PC통제 방법, 사용자 PC를 외부 네트워크와 선별적으로 단절시키는 NW통제 방법, 데이터를 저장할 때 마다 암호화 저장하여 데이터가 유출되더라도 비 인가자가 열람할 수 없도록 하는 데이터 암호화 저장 방법, 사용자 PC를 더미 터미널화 하여 PC에는 OS와 같은 최소한의 필요한 소프트웨어만 구비하고 데이터는 별도의 공동서버에 저장하는 NC(Network Computing) 방법 의 네 가지 측면으로 분류하여 각각의 장단점을 분석한 결과, 어느 하나의 기법만으로 해결될 수 있는 방안은 불가능하며 각 방안의 장점을 선별, 취합한 복합방안을 선정하여 새로운 개선 모델로 제시하였다.

개선 모델은 블레이드피씨 모델을 기반으로 한 네트워크 컴퓨팅 방식으로서 부분적인 제한 사항을 보완하기 위하여, 방화벽, 컨텐츠필터링, Active Directory 서버 관리, IP스캐닝, PC보안 툴 기술을 혼용한 복합 모델 사례로서, 개인 사용자는 개인PC에서 인터넷 사용이나 사내 메일을 편리하게 이용하면서도 업무와 관련된 주요 정보기술 데이터는 개인PC가 아닌 공용 서버 영역에서 다루도록 하여 정보 유출을 원천 차단한 것이 특징이다.

제시된 모델의 기술적 완성도가 높다 할 지라도 이를 운영함에 있어 개별 사용자가 준수해야 할 규정, 관리자가 관리, 감독하여야 할 규정 등의 보안 정책을 수립함으로써 향후 관리적인 누수가 일어나지 않도록 정책적 측면까지 제시하였다.

개선 모델 적용에 따라 기업에서는 사내의 보호하여야 할 정보기술이 외부로 유출 될 수 있는 요소를 외형적인 인프라 측면에서는 원천적으로 예방할 수 있게 되었다고 할 수 있으나 향후에는 해당 모델을 좀 더 효율적인 기술 기법으로 향상시킬 수 있는 방안과 이를 적용한 효과를 세부 정량적으로 측정하여 제시하는 연구가 필요하겠다.

참고문헌

[1] 노민선, "기업연구소 산업기밀 관리실태 및 개선방안", 한국산업기술진흥협회, 2006.8

[2] 유재근, "기업 내 효율적인 PC보안 시스템 구축방안에 대한 연구", 동국대학교 국제정보대학원, 2004.12

[3] 김동진, "기업환경의 내부보안을 위한 통합 보안 관리 시스템의 설계 및 구현", 창원대, 2008.5

[4] 선병욱, "네트워크 컴퓨터(NC)의 군 적용방안에 관한 연구, 배재대학교 정보통신대학원 정보통신학과, 2006.6

[5] "NC(Network Computer)를 이용한 군사기밀 보호 방안에 관한 연구", 동국대학교 국제정보대학원, 정보보호학과, 2006.12

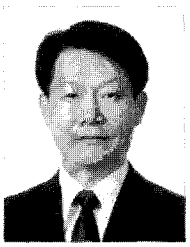
[6] 전정훈, 전상훈, 효율적인 네트워크 보안운영을 위한 Exclusive Firewall 관한 연구, 한국컴퓨터정보학회논문집, 2007.

[7][8][9] Stateful Inspection Technology, Check Point Software Technologies, Inc., http://www.checkpoint.com.

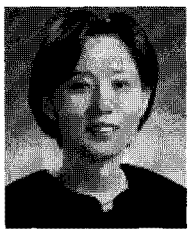
[10] 비업무용 웹사이트 제어 솔루션 WebKeeper, 소만사, 2008, www.somansa.com

[11] 양성은, DRM(Digital Rights Management) 솔루션을 이용한 문서보안에 관한 연구, 2008, 동국대학교.

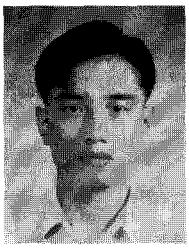
<著 者 紹 介>



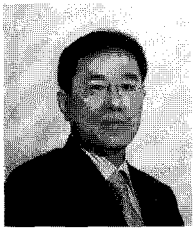
송 성 근 (Song seong keun)
1987년 2월 : 고려대학교 지질학과 졸업
2006년 3월~현재 : 고려대학교 정보경영공학과 석사과정
관심분야 : 웹2.0, Collabollation, 정보보호, 포탈시스템



박 지 숙 (Park ji sook)
1997년 2월 : 이화여자대학교 기독교학과 졸업
2001년 8월 : 이화여자대학교 정보과학대학원 컴퓨터학과 석사
2005년 3월~ 현재 고려대학교 정보경영공학대학원 박사과정
관심분야 : 정보보호, 금융보안, 어플리케이션 보안, 암호응용



우 재 현 (Woo jae hyeon)
1996년 2월 : 서울대학교 기계공학과 졸업
2002년 2월 : 서울대학교 전자컴퓨터공학부 석사
2007년 3월~현재 : 고려대학교 정보경영공학과 박사과정
관심분야 : 전자공학, 통신공학, 정보보호



임 종 인 (Lim jong in)
1980년 2월 : 고려대학교 수학과 졸업
1982년 2월 : 고려대학교 수학과 석사 학위 취득
1986년 2월 : 고려대학교 수학과 박사 학위 취득
현 고려대학교 정보경영공학전문대학원((구)정보보호대학원) 원장, 정부혁신지방분권위원회, 대통령 자문 전자정부 특별위원회, 법무부 형사사법 통합정보체계 추진단 자문위원 등
관심분야 : 정보법학, 디지털 포렌식, 개인정보보호, 전자정부보안