情 報 保 護 學 會 誌
第17卷 第2號, 2007. 4

보안 산업체의 윈도우즈 비스타로 인한 문제점 및 대응책

김 기 영*

요 약

윈도우즈 비스타(Windows Vista)는 용이성, 안전성, 연결성, 엔터테인먼트 기능의 향상을 기반으로 한다. 특히 사용자 계정 제어, 악성 프로그램에 대한 보호 기능, 인터넷 익스플로러 7(Internet Explorer 7)의 보호 모드 , Windows Defender 등의 제공으로 개선된 보안기능을 제공한다. 기존 응용 프로그램의 대부분은 관리자 권한만을 고려하여 설계 및 작성되었으므로 보안이 강화된 윈도우즈 비스타에서는 호환성에 대한 문제가 제기되었다. 본고에서는 윈도우즈 비스타로 인해 발생한 문제점을 해결하기 위해 새로운 플랫폼이라는 관점에서 대응책을 제안한다.

Ⅰ. 서 론

한국마이크로소프트는 2007년 1월 31일에 '윈도우즈 비스타' 소비자 버전을 공식 출시하였다. 윈도우즈 비스타는 용이성, 안전성, 연결성, 엔터테인먼트 기능의 향상을 기반으로 기존의 운영체제와 다른 새로운 기능이 추가되었다. 특히 사용자 환경을 도입하여 사용자 스스로 정보를 확인, 검색 및 구성하며 컴퓨팅 사용을 통제하도록 설계되었다.

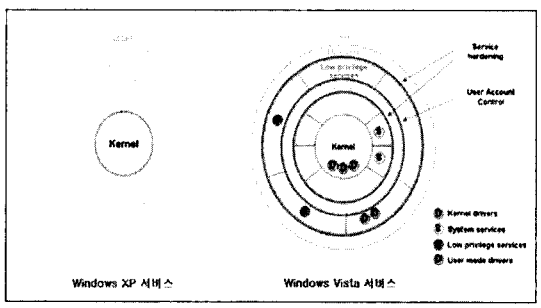
보안적인 측면에서는 사용자 계정 제어를 통해 관리자와 표준 사용자 간의 보안 정책을 설정하였으며 바이러스, 웜, 스파이웨어나 그 밖에 악성 프로그램에 대한 보호 기능이 강화되었다. 또한 데이터 도난이나 노출의 위험에서 개인 정보를 보호할 수 있도록 데이터를 보호하는 기능과 서비스를 추가하였다. 인터넷 익스플로러 7은 보호모드의 도입을 통해 악성 소프트웨어 또는 멜웨어의 공격을 막아주는 동적 보안 보호 기능과 피싱 등으로 인한 개인 정보가 유출되지 않도록 방지하는 방법을 제공한다.

이러한 윈도우즈 비스타의 보안기능으로 인해 기존의 응용 프로그램과의 호환성 문제가 발생되었다. 대부분의 기존 응용 프로그램은 관리자 권한만을 고려하여 설계되고 작성 및 테스트를 수행되었기 때문이다. 따라서 사용자 계정 제어를 지원하는 윈도우즈 비스타에서는 ActiveX 컨트롤 등을 이용하는 기존의 응용 프로그램을 수행할 수 없거나 실행되지 않는 경우가 발생하였다.

본고에서는 윈도우즈 비스타와 기존의 운영 체제의 차이점과 윈도우즈 비스타에서 제공하는 보안 기능에 대해 살펴보고 이로 인해 발생된 문제점을 파악하고자 한다. 또한 제기된 문제를 해결하기 위해 보안 산업체의 대응 방안을 제안하고자 한다.

Ⅱ. 윈도우즈 비스타

본 장에서는 기존의 윈도우즈 계열 운영체제인 윈도



〔그림 1〕 윈도우즈 XP와 윈도우즈 비스타 서비스 권한 레벨 계층 비교

* 소프트포럼(주) SW연구개발실 (kiyoung@softforum.com)

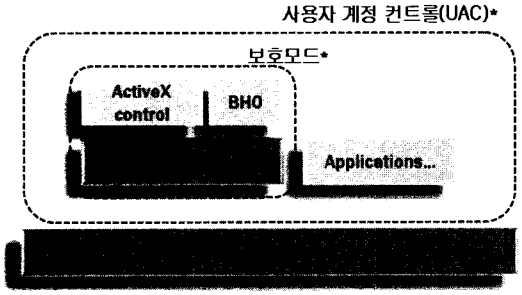
우즈 XP(Windows XP)와의 차이점을 설명하고 윈도우즈 비스타의 개선된 보안기능에서 대해 구체적으로 살펴본다.

2.1 윈도우즈 비스타와 윈도우즈 XP의 차이점

윈도우즈 XP는 커널(Kernal)과 사용자 간의 서비스 권한 레벨 계층 수가 적고 대부분의 서비스에 높은 사용자 권한을 부여하고 있어 실질적인 보안 정책이 이루어지고 있지 않고 있다. 그러나 〔그림 1〕과 같이 윈도우즈 비스타는 서비스 권한 레벨 계층을 기존보다 세분화하였으며 최소한의 권한만을 서비스에 부과하여 위험요소를 최소화시켜 보안을 강화한 것이 특징적이다.

예를 들어 윈도우즈 XP의 경우 사용자가 C 드라이브 및 레지스트리의 모든 부분에 대해 전체 권한이 있다고 가정하기 때문에 일부 응용 프로그램은 사용자가 관리자 권한이 없을 경우 작동하지 않으나, 윈도우즈 비스타에서는 응용 프로그램이 제한된 영역에 쓰기 작업을 시도하는 경우 이 작업이 자동으로 사용자 프로필에 지정된 다른 위치로 리디렉션된다[2]. 또한 관리자가 아닌 사용자가 드라이버를 로드할 수 있다.

윈도우즈 XP에서는 전체 관리자 권한이 없더라도 응용 프로그램 설치 등의 시스템 작업을 수행할 수 있도록 Power Users 그룹을 구성하고 이 그룹의 구성원에게 해당 권한을 부여하였다. 그러나 윈도우즈 비스타에서는 Power Users 그룹이 제거되었으며 필요한 경우 보안 템플릿을 사용하여 이 그룹을 되돌릴 수는 있다. 사용자 접근 제어를 제공하여 대부분의 사용자 응용 프로그램이 제한된 권한으로 실행되도록 한다. 이외에 윈도우즈 비스타는 윈도우즈 XP에 비해 향상된 방화벽 기능을 제공하며 전체 운영 체제 볼륨을 암호화하는 기능을 지원한다.



〔그림 2〕 윈도우즈 비스타의 보안모델 [3]

2.2 윈도우즈 비스타의 보안기능

2.2.1 악성 프로그램 방어

윈도우즈 비스타는 악성프로그램으로부터 사용자의 환경을 보호하도록 새로운 방어 기술을 도입하였다. 악성프로그램은 사용자에게 해로운 모든 프로그램이나 파일로 컴퓨터 바이러스, 웜, 트로이 목마 프로그램, 동의 없이 사용자에 대한 정보를 수집하는 스파이웨어 등을 의미한다. 이러한 보호 기술은 사용자 계정 제어(UAC), Windows Defender, Windows 방화벽, Windows 보안 센터, 악성 소프트웨어 제거 도구, 소프트웨어 제한 정책이 있다.

〔그림 2〕는 윈도우즈 비스타의 보안모델로 컴퓨터 보안이 위협을 받을 경우 악성 프로그램 또는 추가 기능으로부터 피해 정도를 줄이기 위한 조치를 나타낸다.

사용자 계정 제어는 관리자로 접근해야 하는 권한 및 작업 중 일부를 표준 사용자 권한 및 작업으로 분리하기 위한 방법을 제공한다. 모든 어플리케이션은 로그인한 계정과 상관없이 표준 사용자 권한으로 실행되며 관리자 승인 모드 기능으로 어플리케이션의 실행 권한을 표준 사용자 권한에서 관리자 권한으로 상승한 후 어플리케이션을 실행하여 일부 유형의 악성 프로그램으로부터 사용자의 시스템을 보호한다.

Windows Defender는 스파이웨어나 기타 원하지 않는 소프트웨어로 인해 발생하는 팝업, 성능 저하, 보안 위협 등으로부터 시스템을 보호한다[4]. 시작 폴더나 레지스트리의 자동 실행 항목 등 주요 시스템 위치를 실시간으로 모니터링하며 스파이웨어나 원치 않은 소프트웨어 옵션으로 사용자의 개인 정보 보호를 제공한다.

Windows 방화벽은 윈도우즈 XP 서비스 팩 2(Windows XP SP2)에서 제공하는 방화벽 기능과 동일하게 운영체제 시작점에서부터 기본적으로 활성화된다. 예기치 않은 동작을 보이는 운영 체제 리소스를 제한하며 인 바운드 및 아웃 바인드 필터링을 제공한다. 또한 방화벽 관리 기능은 인터넷 프로토콜 보안(IPSec) 기능과 통합되어 하나의 콘솔을 이용하여 IPSec 및 방화벽을 모두 관리할 수 있도록 한다.

Windows 보안 센터는 방화벽, 자동 업데이트, 악성 프로그램 방어, 인터넷 익스플로러 보안 설정 및 사용자 계정 제어의 상태를 지속적으로 확인, 표시한다.

악성 소프트웨어 제거 도구는 감염된 컴퓨터에서 악성 프로그램을 제거하도록 도움을 제공한다. 이는 바이

러스 백신 제품이 아니므로 바이러스 백신 소프트웨어와 함께 사용하도록 권장하고 있다.

소프트웨어 제한 정책은 관리자가 응용 프로그램 소프트웨어를 식별하고 로컬 컴퓨터에서 해당 소프트웨어의 실행을 제어할 수 있도록 지원한다. 다중 사용자 컴퓨터에서 특정 파일에 대한 액세스를 제한하거나 컴퓨터, 조직 구성단위, 사이트 및 도메인 수준에서 설정된 정책 집합을 기반으로 로컬 컴퓨터에서 실행 파일이 실행되지 않도록 하는 등의 기능을 제공한다[4].

2.2.2 데이터 보호

윈도우즈 비스타는 데이터 도난이나 노출의 위협을 방지하고자 클라이언트 컴퓨터의 데이터를 보호하는 기능 및 서비스를 제공한다. 이러한 보호 기술은 BitLocker 드라이브 암호화, 파일 시스템 암호화(EFS), 권한 관리 서비스(RMS), 장치 제어가 있다.

BitLocker 드라이브 암호화는 윈도우즈 볼륨 전체가 암호화되어 다른 사용자가 무단으로 윈도우즈파일 및 보안이 적용된 드라이브의 정보를 오프라인으로 보지 못하도록 막아 준다. 또한 시작 프로세스의 초기 단계에서 클라이언트 컴퓨터의 시스템 및 하드웨어 무결성을 검사한다[4].

파일 시스템 암호화는 파일과 폴더를 암호화하여 무단 접근으로부터 데이터를 보호한다. 이는 NTFS 파일 시스템에 통합되어 있으며 동작 과정은 응용 프로그램에 노출되지는 않는다. 만약 사용자가 암호화된 파일에 접근하면 그 내용을 보기 위한 키를 요구하는 메시지가 수행되며 암호화 및 복호화 과정이 자동으로 수행된다.

권한 관리 서비스는 중요한 전자 메일, 문서, 웹 콘텐츠 및 기타 유형의 정보에 대한 보안을 강화하고, 사용 정책을 적용할 목적으로 설계되었다[4]. 엔터프라이즈나 인터넷에서 파일을 전송할 때 암호화하여 인증된 사용자와 명시적 권한이 부여된 사용자만 파일에 접근하도록 한다.

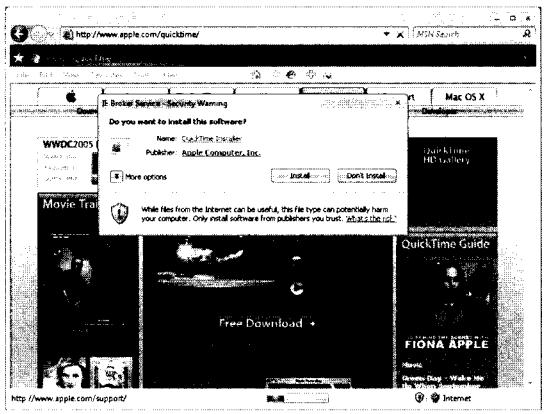
사용자가 USB 키 드라이브이나 이동식 저장 장치와 같은 플러근 앤 플레이(PnP) 하드웨어를 자신의 클라이언트 컴퓨터에 마음대로 추가할 수 있는 경우 관리자 입장에서는 보안문제가 발생할 수 있다. 따라서 관리자는 그룹 정책을 사용하여 지원되지 않거나 승인되지 않은 장치에 대한 설치를 관리한다.

2.2.3 인터넷 익스플로러 7 방어 기술

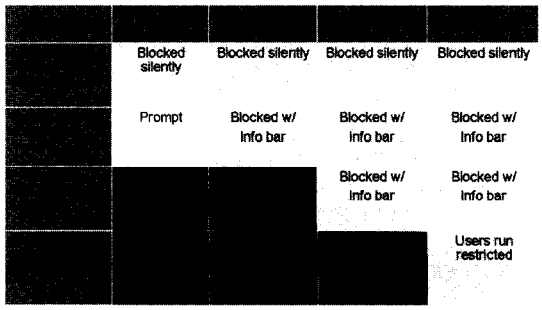
인터넷 익스플로러 7은 브라우저 보안과 개인 정보 보호 강화에 초점을 두어 인터넷 익스플로러 보호 모드, ActiveX 선택, 도메인 간 스크립팅 공격 방어, 보안 상태 표시줄, 피싱 필터 등을 제공한다.

인터넷 익스플로러 보안 모드는 브라우저 확장 기능을 통해 악성 코드가 자동으로 설치될 가능성을 제거하여 소프트웨어 취약점을 줄여준다[4]. 또한 축소된 권한으로 실행되어 사용자의 명시적 동의 없이는 사용자 또는 시스템 파일이나 설정을 변경하지 못하도록 지원한다. [그림 3]은 보호 모드 상에서의 ActiveX 컨트롤 실행 시 동작되는 예시 화면이다.

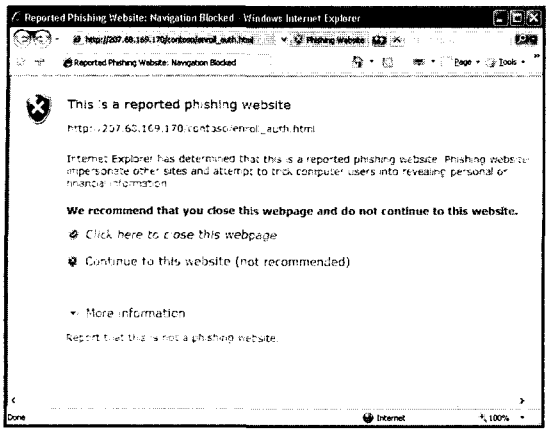
ActiveX 선택 기능은 사용자가 명시적으로 허용하지 않은 모든 컨트롤을 자동으로 비활성화 하여 악용 가능성을 줄여준다. 알림 메커니즘을 통해 각 컨트롤별로 접근을 허용하거나 거부할 수 있으므로 공격에 이용될 수 있는 영역을 줄인다. [그림 4]는 인터넷 익스플로러 상에서의 ActiveX 컨트롤에 대한 기본 설정을 나타낸 것



[그림 3] 인터넷 익스플로러 7의 보호모드 상에서 ActiveX 컨트롤을 수행하는 경우 예시[5]



[그림 4] 인터넷 익스플로러의 ActiveX 컨트롤의 기본 설정 [5]



〔그림 5〕 피싱 필터 예시 화면[5]

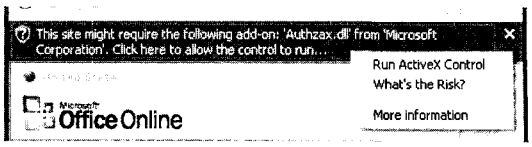
이다.

도메인 간의 스크립팅 공격 방어는 악성 웹 사이트에서 다른 웹 사이트의 취약점을 활용할 가능성을 제한한다. 또한 보안 상태 표시줄은 의심스러운 사이트나 공격에 사용되는 사이트와 인증된 웹사이트를 구별할 수 있으며 피싱 필터를 통해 피싱 웹 사이트를 사용자에게 알려 사용자가 더 안전하게 콘텐츠를 탐색할 수 있도록 지원한다. 〔그림 5〕는 피싱 필터에 대한 예시 화면이다.

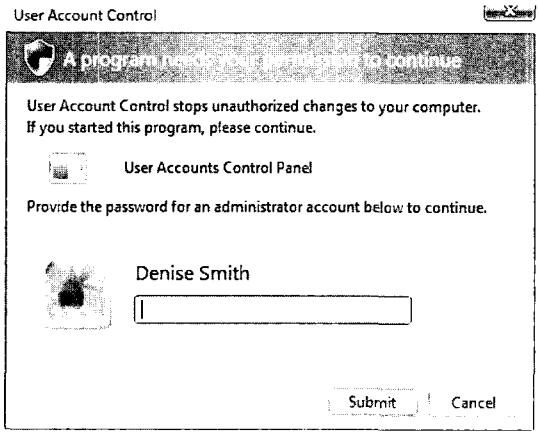
Ⅲ. 윈도우즈 비스타의 호환성 문제점

윈도우즈 비스타에서 제공하는 사용자 계정 제어 등의 보안 기능은 기존의 응용 프로그램과 호환성이 이루어지지 않는 문제점이 제기되었다. 특히 ActiveX 기술을 적용한 웹사이트 운영이 되지 않는다는 문제점이 나오고 있다. 이는 윈도우즈 비스타에서 제공하는 ActiveX 컨트롤 Opt-In 정책, 인터넷 익스플로러 보호 모드, 사용자 계정 제어와 밀접한 관련이 있다.

ActiveX 컨트롤 Opt-In 정책은 웹사이트로부터 직접 설치되지 않는 ActiveX 컨트롤이 바로 실행되지 않고 정보 표시줄에서 사용자가 동의했을 때 실행되는 것을 의미한다. 또한 보호 모드 하에 있는 인터넷 익스플로러는 최소한의 권한으로 ActiveX 컨트롤을 실행하여 〔표 1〕의 신뢰도 메커니즘에 따라 신뢰 단계가 낮은 폴더 이외에는 파일 쓰기를 금지한다[7]. 사용자 계정 제어 하에서 인터넷 익스플로러에서 실행되는 ActiveX 컨트롤은 프로그램 파일 폴더와 같은 신뢰 관계가 높은 폴더에 대한 파일 쓰기를 할 수 없으면 권한이 높은 프로세스에 윈도우 메시지를 전달할 수 없다. 인증 받지 못



〔그림 6〕 ActiveX 컨트롤 Opt-in[5]



〔그림 7〕 사용자 계정 제어로 인한 권한 상승 창[5]

〔표 1〕 신뢰도 메커니즘[6]

접근 수준	시스템 권한
높음(High IL)	관리자
보통(Media IL)	사용자
낮은(Low IL)	신뢰 안함

한 ActiveX의 실행을 막고 보호 모드를 통해 시스템의 특정 영역에만 사용할 수 있도록 하였다.

Ⅱ장 1절에서 살펴보았듯이 기존의 운영체제에서는 표준 사용자는 시스템 사용이 제한되어 있었다. 대부분의 응용 프로그램은 특정 버전의 윈도우 운영체제와 특정 버전의 브라우저를 기반으로 관리자 권한을 가지고 설계, 작성되어 테스트를 수행하였다. 따라서 낮은 권한을 가지고 실행되는 인터넷 익스플로러나 응용 프로그램은 파일에 대한 접근을 할 수 없어 호환성의 문제가 발생한다. 윈도우즈 비스타의 64비트 환경에서는 16 비트 응용 프로그램과 32비트 드라이버가 지원되지 않는다[4]. 따라서 응용 프로그램의 표준을 준수하지 않는다면 수행할 수 없으므로 SW구조를 변경하거나 재개발이 필요할 수도 있다. 또한 바이러스 백신 소프트웨어 및 방화벽 조작을 위한 계층을 제공하는 새로운 시스템 API가 제공되므로, 이러한 기능을 수행하는 응용 프로

그램이 이에 맞추어 수정되지 않았다면 호환성의 문제가 발생할 수 있다.

Ⅳ. 대응 방안

윈도우즈 비스타는 보안 개발 생명 주기(SDL) 지침에 따라 개발된 운영체제로 기존의 윈도우즈 운영체제와의 다른 관점에서 보아야 한다. 즉 Ⅲ장에서 고려한 바와 같이 운영체제의 단순한 업그레이드가 아닌 새로운 운영 체제로서의 인식 전환이 필요하다. 응용 프로그램 설계 단계에서 표준 사용자 권한 및 보호 모드에 대한 시나리오를 작성하고 그룹에 대한 보안 정책을 수립하며 응용 프로그램의 표준을 준수해야 한다. 뿐만 아니라 사용자 계정 제어로 인해 권한을 획득해야 하는 불편함도 해커 및 악성 프로그램의 공격으로부터 안전하기 위한 수단으로 인식해야 한다. 마이크로소프트사에서 발표한 것처럼 사용자의 편의를 위해 보안정책을 세우는 것은 보안상 바람직하지 않다.

따라서 윈도우즈 비스타를 새로운 플랫폼으로 인식하여 다양한 플랫폼을 지원하도록 개발을 해야 하며, 인터넷 익스플로러, 파이어 폭스(Firefox)및 네스케이프(Netscape) 등의 브라우저 환경도 고려하여 개발을 해야 높은 호환성을 제공할 수 있다. 예를 들면 플래시(Flash)와 자바 애플릿(Java Applet)을 들 수 있다. 플래시는 다양한 운영체제를 지원하는 Player(VM)를, 자바 애플릿은 JVM을 바탕으로 각 브라우저에 맞는 플러그인(Plugin), ActiveX 컨트롤을 개발하여 대응하고 있다. 그러나 Java 바이트 코등의 경우 플랫폼에 영향을 받지 않는 반면에 Decompile이 되어 소스가 보호받지 못한다는 심각한 단점이 있다. 이러한 이유로 Java의 경우 주로 서버 프로그램이나 핸드폰 단말기와 같이 일반인으로부터 보호되는 환경에서 주로 사용이 된다. 따라서 이식성이 강한 보안 프로그램을 개발하기 위해서는 다양한 운영체제를 지원하는 VM개발과 함께 코드가 보호될 수 있는 애플릿(Applet) 기술 개발을 해야 한다.

또한 키보드 보안과 같이 드라이버 기술을 사용하는 경우도 기존 소스를 그대로 사용할 수 없어 개발에 많은 비용이 들 수 있지만 기존의 윈도우즈 업그래이드 정도로 인식하지 말고 새로운 운영체제라고 인식을 하고 윈도우즈 비스타의 드라이버 정책과 기술에 맞게 개발을 해야 한다.

이 외에도 윈도우즈 비스타에서는 CNG(Cryptography : Next Generation)와 같은 암호환경을 제공하므로 암호 제품의 경우 이를 활용하는 것도 고려해 볼 수 있다.

이와 같이 윈도우즈 비스타는 전반적으로 기존의 Microsoft의 운영체제와 많은 차이가 있기 때문에 그에 맞게 개발을 해야 하며 특히 보안에 있어서는 운영체제 자체에서 기본적인 기능을 제공하고 있고 이를 활용 또는 대체할 수 있게 되어 있기 때문에 그에 맞게 제품을 구현할 수 있겠다.

Ⅴ. 결 론

윈도우즈 비스타는 화려한 사용자 인터페이스, 막강한 검색기능과 강화된 보안 정책을 내세우며 기존 윈도우즈 계열 운영체제와 차별화를 선언했다. 특히, 강화된 보안 정책으로 안전한 운영체제를 표방한 것이 주목된다. 이로 인해 사용자의 불편함이 가중되고, 호환성 문제로 인해 윈도우즈 비스타용으로 구조를 새로 디자인해야하며 ActiveX 컨트롤들도 다시 개발해야하는 문제가 발생하였다. 이는 윈도우즈 비스타가 단순한 기존 운영체제의 확장판이 아니라 새로운 운영체제로 인식하고 대응을 해야 함을 의미한다.

따라서 Ⅳ장에서 살펴본 플래시와 자바 애플릿처럼 다양한 운영체제 및 웹 브라우저 확장 기술 개발 및 전반적인 응용 프로그램 포트폴리오가 요구되며 표준을 준수한 개발이 필요하다.

윈도우즈 비스타는 보안을 소프트웨어 설계의 핵심요소로 간주하여 보안 중심의 엔지니어링 프로세스를 바탕으로 개발되었으므로 보안 산업체에는 더욱더 개선된 보안기능을 제공할 수 있는 새로운 기회가 될 것이다.

참고문헌

[1] "최소 권한 부여 환경에서 어플리케이션 개발자를 위한 모범 사례 및 지침", Microsoft Corporation, 2005.

[2] Michael Niehaus, "Windows Vista 배포에 대해 알아야 할 10가지 사항", TechNet Magazine, Microsoft Corporation, 2006.

[3] 류한석, "Windows Vista에서의 ActiveX 컨트롤", 한국마이크로소프트, 2006.

[4] "Windows Vista 보안 가이드(http://www.microsoft.

com/korea/technet/windowsvista/security/guide.mspx)", Microsoft Corporation.

[5] 이기영, "Internet Explorer 7 소개", 한국마이크로소프트, 2006.

[6] 이동석, "Windows Vista IE7의 새로운 보안 하에서 ActiveX 컨트롤 개발", 한국마이크로소프트, 2006.

[7] Alex Heaton, "사용자 계정 컨트롤을 사용하여 관리자가 아닌 사용자로 실행," TechNet Magazine, Microsoft Corporation, 2006.

[8] Jeremy Moskowitz, "Windows Vista 의 보다 강력해진 그룹 정책", TechNet Magazine, Microsoft Corporation, 2006.

[9] Justin Harrison, "Windows Vista의 새로운 보안 기능으로 PC 보호", TechNet Magazine, Microsoft Corporation, 2006.

[10] 송윤섭, "Windows Vista의 새로운 기능", 한국마이크로소프트, 2006.

[11] Sharon Cohen, Rob Franco, "ActiveX Security: Improvements and Best Practices", Microsoft Corporation, 2006

[12] 정성태, "Internet Explorer 7.0 호환성 백서", Microsoft Corporation, 2006.

[13] Marc Silbey, Peter Brundrett, "Internet Explorer 보호 모드의 이해 및 작업", Microsoft Corporation, 2006.

〈著者紹介〉

김 기 영 (Kim, Ki Young)
1997년 2월 : 한양대학교 전자공학과 졸업
1997년 3월 : 포스코그룹 입사
1998년 3월 : 한국후지쯔 연구개발부 입사
2000년 10월~현재 : 소프트포럼 SW연구개발실 연구소장
관심분야 : 정보보호, 유비쿼터스