# 인터넷 메신저의 보안 체계에 대한 연구

## A Study on the Security Management of Instant Messengers

김 상 균* 이 홍 주**
Sang-kyun Kim Hong-Joo Lee

### 요 약

인터넷 메신저는 개인적인 용도 이외에도 기업환경에서 실시간의 의사소통과 인터넷 상의 자료 전송 등을 통해서 기업의 생산성 향상에 큰 기여를 하고 있다. 그러나, 인터넷 메신저가 기업 내부에서 사용되면서 보안상의 많은 문제점이 지적되고 있다. 본 연구에서는 위험관리 방법론을 통해서 인터넷 메신저에 대한 위험을 분석하고 이에 대한 통제요소를 제시한다. 인터넷 메신저의 다양한 효과를 생각할 때 기업내부에서 인터넷 메신저를 완전히 차단하는 것은 어려운 일이다. 따라서, 본 논문에서 제시한 보안 통제 수단들을 통해서 인터넷 메신저가 지닌 잠재적 위험요소에 적절히 대응하며 이를 기업의 정보인프라로 활용해야 할 것이다.

### Abstract

The instant messenger is not only a wonderful tool for individuals. It is also a great tool which provides real-time dialogue and file transfers for individuals via the Internet and improves an enterprise productivity. However, it has many security risks that may have significant impact in corprate environments. This paper provides an overview of the security risks of the instant messenger with a risk analysis method and the controls that can be used to make it secure. It's hard to eliminate the instant messenger from enterprise environments because of its benefits. If we cannot avoid using it, we must make it secure and reap the full benefits of it.

☞ Keyword : Instant messenger, Risk analysis, Security Management

## 1. 서 론

인터넷 메신저는 실시간 의사소통 및 파일 공유를 지원해주는 소규모 통신 프로그램을 의미한다. 기업내부에서 사용되는 인터넷 메신저의 상당수는 해당 기업 내부 IT (Information Technology) 조직의 정책적인 지원과는 상관없이 직원 개개인의 선택과 사용에 의해 운영되고 있다. 인터넷상에서 무료로 배포되고 쉽게 설치 및 사용할 수 있다는 편리함으로 인하여 많은 사용자들로부터 환영받고 있다. 대부분의 인터넷 메신저 사용자는 기업내부에서 업무상 공유하는 통신 그룹보다 외부의 사용자와 더 큰 규모의 통신 그룹을 유지하게 된다. 이렇듯 인터넷 메신저는 기업 내외부의 다양한 사람들과의 주요 통신 수단으로 자리 잡고 있다.[1]

인터넷 메신저를 사용하는 기업입장에서는 다음과 같은 사항들에 주목해야한다.[2] 1) 인터넷 메신저에 대해서는 국제적으로 제정된 표준이 없으며, 인터넷 메신저 제공업체가 독자적으로 설계 및 개발한 프로그램을 그대로 사용하는 것이다. 2) 인터넷 메신저는 정보보호, 에러 체크 및 재전송 등에 대한 기능이 대부분 매우 취약하다. 3) 기업 내부 직원들이 임의적으로 사용하는 인터넷 메신저에 대해서 기업의 정보시스템 관리자들이 이를 모두 파악하고 관리하기는 매우 어렵다.

* 정 회 원 : (주)소만사 이사
saviourkim@somansa.com (제 1저자)
** 정 회 원 : 연세대학교 지식정보화연구센터 연구원
blue1024@yonsei.ac.kr (제 2저자)
[2005/07/13 투고 - 2005/09/23 심사 - 2005/12/23 심사완료]

인터넷 메신저의 과다한 사용, 비업무용 사용 및 정보 유출 등은 가장 일반적으로 지적되는 인터넷 메신저의 역효과라고 할 수 있다. 국내외에서 사용자 층이 두터운 인터넷 메신저로는 MSN메신저, Yahoo메신저, AOL메신저, ICQ 등을 들 수 있다. 이들 메신저의 공통점은 바이러스나 악성코드의 전파경로로 활용 될 수 있거나, 이미 그러한 피해사례가 보고된 바 있다는 것과 사용자간 의사소통에 대해서 별도의 암호화를 제공하지 않기 때문에 도청에 취약하다는 것이다.[3]

본 논문에서는 인터넷 메신저에 대한 보안상의 위험을 파악하기 위하여 전통적인 위험분석 방법론을 사용한다. 이를 통해서 인터넷 메신저의 정보자산으로의 가치, 취약성, 위협 및 위험 등을 도출하고 이에 대응하기 위한 통제 요소를 제시한다. 마지막으로 본 연구에서 제시한 보안 체계에 따라서 실제 기업에서 인터넷 메신저에 대한 보안 통제를 구축한 사례연구를 통해서 본 연구의 실효성을 파악한다.

## 2. 기존 연구 분석

### 2.1 인터넷 메신저의 기술적 특성

인터넷 메신저는 클라이언트/서버 방식으로 정보를 송수신 한다. 사용자는 클라이언트 프로그램을 자신의 컴퓨터에 설치하여 다른 사용자들과 통신을 하게 된다. 중앙에 위치한 서버 프로그램이 이러한 모든 클라이언트들의 통신을 관리하는 구조이다. 서버는 앞서 열거한 각각의 메신저에 대한 서비스 회사가 직접 운영한다. 즉, AOL, Microsoft, Yahoo 등이 직접 운영하는 것이다. 이러한 구조상 서버는 단순히 클라이언트들 간의 통신을 중계하는 것뿐만 아니라 클라이언트 프로그램을 통해서 접속하는 사용자들을 인증하고 그들의 접속 상태를 확인하는 기능도 담당한다. 즉, 클라이언트 프로그램들 간에 직접적으로만 연결되는 방식이 아니다.[4]

위와 같은 기본 구조상에서 보다 더 세분화된 기술들이 지속적으로 연구되고 있다. Andrew의 연구에 따르면 현재 진행되고 있는 인터넷 메신저와 관련된 주요 연구는 인터넷 메신저의 게이트웨이 기술, 메신저에 대한 식별 및 인증, 송수신되는 컨텐츠에 대한 분석 및 구분기반 라우팅, 송수신 정보에 대한 보관 및 분석 기술, 기업 외부와의 메신저 송수신에 대한 관리 등이 포함된다.[5]

### 2.2 위험 분석기법

위험 분석 기법은 다양한 정보자산에 대해서 합리적인 수준의 통제를 통해서 보안성을 확보하기 위한 요구사항을 분석해주는 가장 효과적인 방법이다.[6] 위험은 특정 기간이나 시간 및 특정 조건에서 사고, 피해 및 손실이 발생할 가능성 및 확률을 의미한다. 따라서 위험은 일반적으로 위험의 가능성 및 위험으로 인한 손실 규모의 두 가지 속성으로 표현된다. 이러한 요소들을 다루는 위험 분석 기법은 시스템 공학 및 시스템 관리의 다양한 영역과 밀접한 관련을 가지고 있다.[7]

위험은 자산가치, 취약성 및 위협을 통해 도출된다. Mayerfeld의 정의에 따르면 취약성은 자산에 손실을 초래할 수 있는 모든 요소 및 속성을 의미 한다.[8] Fites는 시스템 보안 절차, 설계, 구현 및 내부 통제 상에 존재하는 공격받을 수 있는 약점이나 결함을 취약성으로 정의하고 있다.[9] Roper은 자산에 손실이나 피해를 줄 수 있는 모든 요소, 환경 및 상황을 위협으로 정의하고 있다.[6]

위험 분석의 기법은 크게 정량적 분석과 정성적 분석으로 분류된다. 정량적 분석은 자산가치, 취약성, 위협 및 위험을 화폐 가치, 확률 및 빈도 등을 통해서 수치적인 형태로 산출하고 분석하는 것이다. 정성적 분석은 자산가치, 취약성,

위협 및 위험을 상대적 중요도, 순위 산정, 전문가 의견 등을 통해서 비수치적인 형태로 나타내고 분석하는 것이다.[6] 본 논문에서는 위험 분석의 전통적 기법인 정량적 분석과 정성적 분석 중 정성적 분석의 기법을 통해 인터넷 메신저의 위험을 분석한다.

### 2.3 통제 수단

보안상의 위험 요인에 대한 발생 확률을 경감시키거나 위험 요인이 실현되었을 때 발생하는 손실을 줄여주는 수단을 정보보호의 통제 수단이라고 한다. 통제 수단은 특정한 기술적 메카니즘이나 관리적 절차로 구성될 수 있다.[10]

통제 수단은 크게 관리적 수단, 기술적 수단, 물리적 수단으로 나뉘어 진다.[11,12,13,14,15] 관리적 수단은 관리자 집단에 의하여 정의되고 운영되는 정보보호 정책, 절차 및 지침 등을 의미한다.[16] 기술적 수단은 데이터, 파일, 프로그램 및 시스템 등을 보호하기 위한 접근 통제 시스템을 의미한다.[17] 물리적 수단은 전산자원에 대해 비인가된 자가 물리적으로 접근하여 발생시킬 수 있는 피해, 손실 및 변조 등에 대한 통제를 의미한다.[18] 이러한 통제 수단들은 표 1과 같이 정리된다.

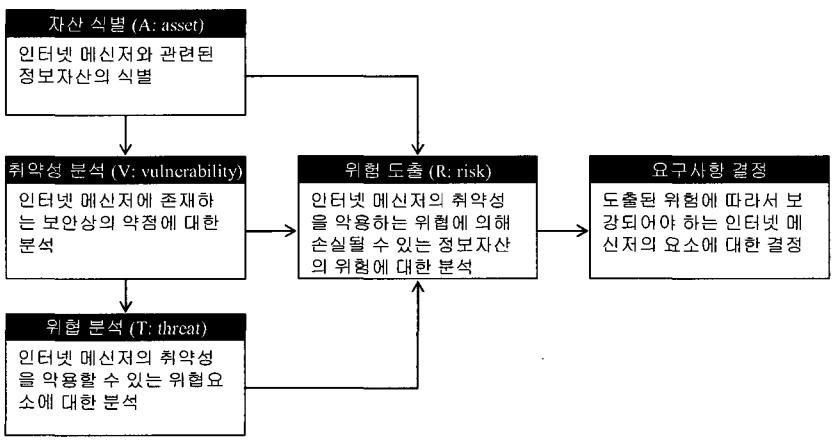
〈표 1〉 통제 수단의 분류 및 해당 요소 [11, 12, 13, 14, 15, 16, 17, 18]

| 관리적 통제 | 기술적 통제 | 물리적 통제 |
|---|---|---|
| · 정책 및 절차<br>· 보안 교육<br>· 인적 통제<br>· 직무 분리<br>· 직무 순환<br>· 미디어 통제<br>· 비상 계획<br>· 위험 관리 | · 식별 및 인증<br>· 권한 관리<br>· 암호화<br>· 접근 통제<br>· 데이터 이중화<br>· 침입 탐지<br>· 모니터링<br>· 타이거팀 운영<br>· 악성코드 대응 프로그램<br>· 통신채널 관리 | · 화재 예방 및 진화 시스템<br>· 예비 전력 시스템<br>· 누수 통제 시스템<br>· 물리적 접근통제<br>· HVAC<br>· 원격 백업 사이트<br>· 비상 대응 계획 |

## 3. 인터넷 메신저에 대한 위험 분석

### 3.1 적용 방법

본 논문에서는 인터넷 메신저에 대한 보안 체계를 제시하기 위하여 전통적인 위험 분석 방법을 사용한다. 기존 연구를 통해서 본 연구에서는 그림 1과 같은 절차에 의해서 인터넷 메신저에 대한 위험 분석 및 이를 통한 보안상의 요구사항을 도출했다.




〈그림 1〉 위험 분석을 통한 인터넷 메신저 보안 요구사항의 결정 절차

〈표 2〉 인터넷 메신저와 관련된 정보자산

| 속성 | 정의 [8] | 관련 정보자산 |
|---|---|---|
| 기밀성 | 비 인가된 자에게 정보가 유출되는 것을 방지하는 것 | A1: 인터넷 메신저를 통해 송수신되는 영업기밀 (trade secret) [1]<br>A2: 인터넷 메신저 사용자의 프라이버시 [2]<br>A3: 인터넷 메신저의 클라이언트 PC에 남겨지는 로그 정보 |
| 무결성 | 비 인가되거나 의도하지 않은 변경이 발생하지 않도록 정보를 보호하는 것 | A4: 인터넷 메신저의 클라이언트 PC자체의 무결성 [10]<br>A5: 인터넷 메신저 사용자의 식별정보 (Identity) |
| 가용성 | 정보를 적절한 시기에 사용가능 하도록 하거나 정보의 손실이 없도록 보장하는 것 | A6: 인터넷 메신저의 클라이언트 PC자체의 가용성 [11]<br>A7: 인터넷 메신저 계정에 대한 가용성 |

〈표 3〉 인터넷 메신저의 정보자산에 대한 취약성 및 위협

| 정보자산 | 취 약 성 | 위 협 |
|---|---|---|
| A1: 인터넷 메신저를 통해 송수신되는 영업기밀 (trade secret) | V1.1: 암호화되지 않은 통신채널 [1] | T1.1: 도청 공격 |
| | V1.2: 송신되는 정보에 대한 접근통제 부재 [1] | T1.2: 정보 유출 |
| A2: 인터넷 메신저 사용자의 프라이버시 | V2.1: 메신저 서버의 정보 유출 통제를 운영업체에게 전적으로 의존하는 상황 [2] | T2.1: 개인정보의 침해 |
| A3: 인터넷 메신저의 클라이언트 PC에 남겨지는 로그 정보 | V3.1: 로그 정보에 대한 접근통제 부재 | T3.1: 로그 정보 도난 |
| A4: 인터넷 메신저의 클라이언트 PC 자체의 무결성 | V4.1: 악성코드에 대한 방역체제 부재 [19] | T4.1: 트로이목마 또는 바이러스의 침투 [20] |
| | V4.2: 수신되는 컨텐츠에 대한 지적재산권 통제 부재 [19] | T4.2: 지적재산권 침해 [11] |
| A5: 인터넷 메신저 사용자의 식별정보 (Identity) | V5.1: 취약한 인증 기능 [20] | T5.1: 임퍼스네이션 (Impersonation) |
| | V5.2: 송수신된 정보에 대한 증거 부족 [20] | T5.2: 송수신에 대한 부인[11] |
| A6: 인터넷 메신저의 클라이언트 PC 자체의 가용성 | V6.1: 송신되는 정보에 대한 필터링 부재 [21] | T6.1: 스팸의 유입 [20] |
| A7: 인터넷 메신저 계정에 대한 가용성 | V7.1: 패스워드 관리 기능의 부족 | T7.1: 계정 도난 |

## 3.2 위험 분석 결과

정보자산의 보안과 관련된 속성은 크게 기밀성, 무결성, 가용성의 세 가지로 나뉜다. 본 연구에서는 정보보호의 3대 속성을 기준으로 인터넷 메신저와 관련된 정보자산의 요소를 분류한다. 이는 표 2와 같다.

표 2에서 정의한 인터넷 메신저와 관련된 정보자산에 대하여 취약성과 위협을 정리하였다. 이는 표 3과 같다.

표 3에서 제시한 정보자산, 취약성 및 위협은 아직 개별 항목에 대한 통계 자료나 기존 연구가 매우 부족하여 이를 기존에 존재하는 이론적 근거를 바탕으로 정량화된 수치로 비교하는 것이 불가하다. 따라서 본 연구에서는 정보자산, 취약성 및 위협에 대하여 전문가를 대상으로 한 정성적 분석 방법을 통해 계량화했다.[6] 본 연구에서는 표 3에서 제시한 인터넷 메신저의 정보자산, 취약성 및 위협에 대하여 보안 전문가 10명을 대상으로 개별 설문을 실시하였다. 응답자 중 4명은 현직 보안 컨설턴트, 3명은 기업내부의 보안 시스템 운영 책임자, 3명은 보안 시

〈표 4〉 인터넷 메신저의 정보자산에 정성적 위험 분석

| 정보자산 | | 취약성 | | 위 협 | | 위험: R = A * V * T [6] (최소:1~최대:125) | | 위험순위 |
|---|---|---|---|---|---|---|---|---|
| A1 | 5 | V1.1 | 3 | T1.1 | 3 | R1.1 | 45 | 3 |
| | | V1.2 | 4 | T1.2 | 5 | R1.2 | 100 | 1 |
| A2 | 2 | V2.1 | 2 | T2.1 | 2 | R2.1 | 8 | 8 |
| A3 | 2 | V3.1 | 2 | T3.1 | 2 | R3.1 | 8 | 8 |
| A4 | 4 | V4.1 | 4 | T4.1 | 5 | R4.1 | 80 | 2 |
| | | V4.2 | 3 | T4.2 | 2 | R4.2 | 24 | 5 |
| A5 | 3 | V5.1 | 4 | T5.1 | 3 | R5.1 | 36 | 4 |
| | | V5.2 | 2 | T5.2 | 2 | R5.2 | 12 | 7 |
| A6 | 3 | V6.1 | 2 | T6.1 | 2 | R6.1 | 12 | 7 |
| A7 | 2 | V7.1 | 3 | T7.1 | 3 | R7.1 | 18 | 6 |

스템 관련 개발자로 구성되었다. 피응답자는 개별 항목에 대하여 1부터 5까지의 척도에 대하여 답변을 하도록 했다. 정보자산 항목에 대해서는 "1: 가치가 거의 없음, 2: 상대적으로 가치가 적음, 3: 보통임, 4: 비교적 중요함, 5: 매우 중요함"의 5점 척도에 대하여 답변한 것이고, 취약성에 대해서는 "1: 안정적임, 2: 비교적 덜 취약함, 3: 보통임, 4: 비교적 취약함, 5: 매우 취약함"의 5점 척도에 대하여 답변한 것이며, 위협에 대해서는 "1: 위협이 거의 안 됨, 2: 비교적 덜 위협적임, 3: 보통임, 4: 비교적 위협적임, 5: 매우 위협적임"의 5점 척도에 대하여 답변한 것이다. 피응답자 10명의 설문 결과에 대한 평균치 및 이에 대한 계산 결과는 표 4와 같다.

본 연구에서는 산출된 위험 중 상대적으로 높은 수준의 위험이라고 할 수 있는 다음과 같은 1~5 순위의 위험에 대하여 통제 수단을 제시한다. 즉, 6~8 순위의 위험 요인에 대해서는 잔존위험(Residual Risk)으로 남겨두며, 1~5 순위의 위험을 인터넷 메신저 보안 체계의 주요 요구사항으로 결정한 것이다.[8]

- *R1.1 (A1 * V1.1 * T1.1)*: 기업의 영업기밀 관련 내용을 메신저로 송수신 할 경우 암호화되지 않은 통신 채널에 대하여 비인가된 제3자가 도청을 하여 정보가 유출되는 위험
- *R1.2 (A1 * V1.2 * T1.2)*: 기업의 영업기밀 관련 내용이 송신에 대한 접근통제를 받지 않는 인터넷 메신저로 인하여 외부로 비인가된 상태로 유출되는 위험
- *R4.1 (A4 * V4.1 * T4.1)*: 인터넷 메신저로 외부의 악성 코드들이 유입되어서 사용자 컴퓨터 시스템의 무결성을 침해하는 위험
- *R4.2 (A4 * V4.2 * T4.2)*: 인터넷 메신저로 외부의 컨텐츠들이 유입되어 타인의 지적재산권을 침해하여 법률적 책임을 지게 되는 위험
- *R5.1 (A5 * V5.1 * T5.1)*: 제3자가 인터넷 메신저의 양 사용자중 한 측의 인증 정보를 도용하여 허위로 해당 사용자 행세를 하는 위험

## 3.3 위험에 대한 통제 수단

본 연구에서는 표 1에서 제시한 통제 수단들을 기초로 인터넷 메신저의 5대 위험 요소에 대한 대응 수단을 제시한다. 이는 표 5와 같이 정리된다.

표 5에서 제시한 인터넷 메신저의 주요 위험 요인에 대한 통제 수단을 Fites et al., Hutt, Vallabhaneni, Krutz and Vines, Schweitzer 등

〈표 5〉 인터넷 메신저의 주요 위험 요인에 대한 통제 수단

| 위험 요인 | 통제 수단 |
|---|---|
| R1.1 | C1.1.1: 기업 외부 망을 경유하여 인터넷 메신저를 사용하는 경우에는 상대방 측과 암호화 채널로 통신하거나 첨부 파일을 암호화 하여 송수신 한다.<br>C1.1.2: 인터넷 메신저의 통신 채널이 암호화 되어 있지 않음을 사용자들에게 주지시킨다. |
| R1.2 | C1.2.1: 기업의 인터넷 메신저 채널에 대해 모니터링을 수행하여, 교류되는 정보의 유형 및 규모를 지속적으로 파악한다.<br>C1.2.2: 기업의 인터넷 메신저 트래픽에 대해 필터링을 수행하여, 영업기밀의 유출을 차단한다.<br>C1.2.3: 인터넷 메신저를 통해서 송수신이 제한되는 기업 영업기밀을 정의하고 사용자에게 주지시킨다. |
| R4.1 | C4.1.1: 안티바이러스 프로그램을 메신저 클라이언트 PC에 함께 설치한다.<br>C4.1.2: 메신저 클라이언트 PC의 주요 시스템 정보 및 데이터를 주기적으로 백업하여 복구 시스템을 마련한다.<br>C4.1.3: 인터넷 메신저를 통한 악성 코드 유입의 가능성을 사용자에게 주지시키고 신뢰할 수 없는 정보에 대한 수신 확인에 주의하도록 한다. |
| R4.2 | C4.2.1: 기업 외부에서 유입되는 인터넷 메신저 트래픽에 대하여 모니터링을 수행하여 저작권 침해에 대응한다.<br>C4.2.2: 인터넷 메신저를 통하여 지적재산권상 문제가 되는 컨텐츠를 사내에 유입하는 행위에 대한 법적인 제재 사항에 대하여 주지시킨다. |
| R5.1 | C5.1.1: 인터넷 메신저 클라이언트 PC의 로그인 기능을 강화한다.<br>C5.1.2: 인터넷 메신저 클라이언트 PC의 화면 보호기 기능을 사용한다.<br>C5.1.3: 기업 업무용으로 허용된 인터넷 메신저의 경우는 대화 중에 표시되는 사용자명에 일정한 규칙을 부여하여 대화 상대의 식별을 용이하게 한다. |

이 제시한 통제 수단의 3대 분류 체계에 따라서 다시 정리하면 다음과 같다 [11, 12, 13, 14, 15]. 관리적 수단에는 C1.1.2, C1.2.3, C4.1.3, C4.2.2, C5.1.3가 포함되며, 기술적 수단에는 C1.1.1, C1.2.1, C1.2.2, C4.1.1, C4.1.2, C4.2.1, C5.1.1, C5.1.2가 포함된다. 물리적 수단이 제시되지 않은 이유는 인터넷 메신저 클라이언트가 설치되는 PC가 기업에서 일상적으로 사용되는 개인별 업무용 PC인 관계로 기존에 사용하던 사업장 내부의 일반적 물리적 보안 통제 이상의 수단을 적용할 필요는 없기 때문이다.

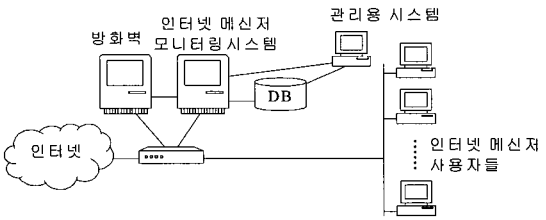
## 4. 사례 연구

본 장에서는 3장에서 제시한 인터넷 메신저의 위험 분석결과를 바탕으로 실제 기업에서 인터넷 메신저에 대하여 보안 체계를 구축한 사례를 소개한다. 본 사례 연구에서는 표 5에서 제시한 통제 수단을 S사의 보안 체계 구축에 활용하였다. S사는 인터넷 메신저를 정보화 전략상에서 정식으로 기업내외부의 주요 통신 수단으로 채택한 상황이다. 따라서 인터넷 메신저를 공식적인 통신 수단으로 사용하는 상황에서 발생할 수 있는 다양한 위험에 대응하기 위하여 보안 체계 구축을 경영진의 의도에 의해 추진한 것이다.

### 4.1 기술적 통제 수단의 구축

S사에 구축된 인터넷 메신저 통제 시스템의 구성은 그림 2와 같다. 구성된 시스템은 크게 서버형태로 운영되는 인터넷 메신저에 대한 관리 시스템과 클라이언트 PC에 설치되는 프로그램으로 나뉘어 진다.

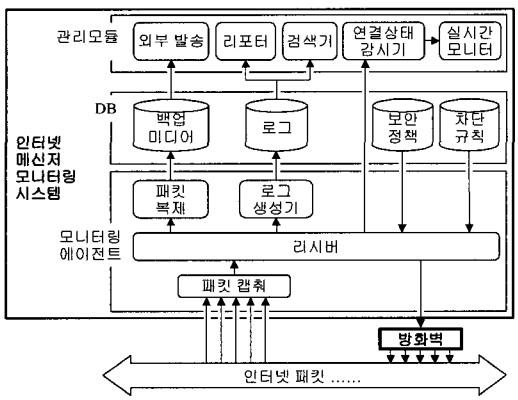
C1.1.1, C4.1.1, C4.1.2, C5.1.1, C5.1.2에 대해서는 기존에 S사에서 운영하던 VPN (Virtual Private Network) 시스템, 바이러스백신, 데스크톱 백업 프로그램, PC용 방화벽 프로그램을 사용하여 해당 통제 수단을 대체하였다.[22] 따라




〈그림 2〉 인터넷 메신저 통제 시스템의 설치

서 S사에서는 C1.2.1, C1.2.2, C4.2.1에 해당하는 통제 수단의 구축을 진행하였다. 즉, 그림 2에서 나타난 인터넷 메신저 모니터링 시스템의 개발 및 구축으로 통해서 기업의 인터넷 메신저 채널에 대해 모니터링을 수행하여, 교류되는 정보의 유형 및 규모를 지속적으로 파악하고, 기업의 인터넷 메신저 트래픽에 대해 필터링을 수행하여, 영업기밀의 유출을 차단하며, 기업 외부에서 유입되는 인터넷 메신저 트래픽에 대하여 모니터링을 수행하여 저작권 침해에 대응하도록 한 것이다.

그림 2에서 제시된 시스템은 크게 방화벽과 인터넷 메신저 모니터링 시스템으로 구성된다. 두 시스템의 메커니즘은 그림 3과 같다.




〈그림 3〉 인터넷 메신저의 기술적 통제 구조

두 시스템은 유기적으로 연계되어서 인터넷 메신저 트래픽에 대한 획득, 분석, 차단, 저장 및 보고 등의 기능을 수행한다. 본 연구과정에서 개발된 인터넷 메신저 모니터링 시스템은 모니터링 에이전트, DB 및 관리 모듈의 세 부분으로 구성되며 전체적으로 다음과 같은 기능을 담당한다. 1) 네트워크 패킷의 스니핑 [23]; 2) 스니핑된 패킷으로부터 메신저 트래픽을 재정렬하여 송수신 내용을 생성; 3) 메시저를 통해 송수신된 정보의 사본을 DB 에 보관; 4) 송수신 관련 특징 정보를 로그로 기록; 5) 포트 차단 (방화벽을 통해서 메신저 송수신의 중대한 보안 위험 발생시 포트를 차단); 6) 보관된 사본 및 로그를 바탕으로 다양한 검색 및 보고 기능 제공

본 시스템의 구현 과정에서 가장 어려운 부분은 모니터링 에이전트내부의 리시버 모듈에 대한 개발이었다. 리시버 모듈은 앞서 제시한 기능 중 "2) 스니핑된 패킷으로부터 메신저 트래픽을 재정렬하여 송수신 내용을 생성"하는 역할을 담당한다. 다음과 같은 세 가지 이유가 리시버 모듈의 개발을 어렵게 하였다. 1) 인터넷 메신저에 대해서는 정확하게 규정된 국제 표준이 없다. 2) 인터넷 메신저 서비스 제공업체 마다 독립적으로 규정한 프로토콜을 사용한다. 3) 모든 인터넷 메신저 프로토콜은 비공개를 원칙으로 하고 있다.[3,4,5]

본 연구에서는 리시버 모듈을 개발하기 위하여 실제 인터넷 메신저를 활발하게 사용하는 환경에서 장기간에 걸쳐 패킷을 스니핑하여 분석했다. 패킷 수집은 총 1개월간 총 여섯개의 메신저를 대상으로 진행했다. 수집된 패킷에 대하여 총 2개월간 다섯명의 분석인력이 패킷의 선후 관계를 추정하여 프로토콜을 분석해냈다. 분석된 메신저별 프로토콜에 따라서 이를 자동으로 수집하고 분류할 수 있는 모듈을 개발한 것이다. 분석된 메신저의 대부분은 네트워크 환경 및 사용하는 메신저의 기능에 따라서 하나의 메신저가 여러 개의 프로토콜을 동시에 가지고 있었다. 일예로 M사의 인터넷 메신저의 경우에는 프로토콜내에 총 5개의 동작 모드가 존재하고 있었다.

## 4.2 관리적 통제 수단의 구축

S사의 정보보호 책임자와 협력하여 S사에 적용 가능한 인터넷 메신저에 대한 보안 정책을 수립하였다. 보안 정책에는 C1.1.2, C1.2.3, C4.1.3, C4.2.2, C5.1.3의 내용이 모두 포함되도록 구성하였다.

무엇보다 인터넷 메신저의 모니터링에 대한 직원들의 반발 및 불만이 클 것으로 예상하여, 어떤 목적으로 모니터링을 실시하는가와 모니터링 한 결과를 보안에 결부된 매우 제한적인 용도로만 사용하고 권한이 부여된 일부 관리자에 의하여만 참조가 된다는 부분을 강조하였다[24]. 관리적 통제의 구축 과정에서 생길 수 있는 법적인 분쟁을 방지하고, 정책 운영의 효과를 증진시키기 위하여 Harris, Vallabhaneni, Krutz and Vines가 제시한 정책개발, 의식개선, 서면합의, 운영의 단계를 준수하였다.[11,14,20] 전체적인 과정은 그림 4와 같다.

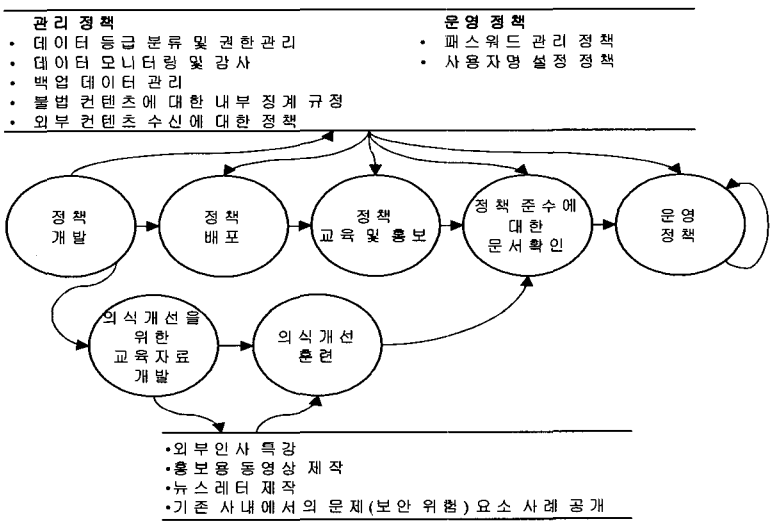
정책은 크게 관리 정책과 운영 정책으로 분류하였다.[20,25] 관리 정책에는 인터넷 메신저 관리 시스템의 개발, 운영 및 활용에 대한 정책과 메신저를 통해서 보호되어야 하는 정보의 분류 및 등급 등에 대해서 정의하였다. 운영 정책에는 인터넷 메신저의 사용자 입장에서 참조할 수 있는 패스워드 관리, 사용자명 설정 및 메신저 사용 시 주의 사항 등을 포함하였다.

정책 개발 완료 후에는 정책의 배포 및 활용에 앞서서 의식개선 작업을 중점적으로 추진하였다. 이는 인터넷 메신저로 외부의 부적절한 컨텐츠를 내부에 유입할 때 발생할 수 있는 위험요인, 송수신 정보의 도청 가능성, 대화 상대정보의 위장 가능성, 송수신 되는 정보로 인하여야기될 수 있는 지적 재산권 침해, 성/인종 차별 등의 문제를 주로 다루었다.

최종적으로는 정책의 시행에 앞서서 전임직원을 대상으로 본 정책의 내용을 충분히 숙지하고 정책의 시행에 동의하였음을 확인하는 협약서를 작성하였다.[11,20]

## 4.3 효과에 대한 검증

정보보호 통제 수단의 도입에 대한 효과 검증과 관련된 기존 연구는 비교적 취약한 편이다.




〈그림 4〉 인터넷 메신저의 관리적 통제 구조

이 분야와 관련된 주된 연구는 Blakely, Kim, Scott, Witty의 연구를 들 수 있다.[26,27,28,29] 이들 연구는 주로 통제 수단의 구축에 소요되는 비용과 그에 따른 효과를 대비하는 방식을 취한다. 본 사례에 대해서도 기존 연구에서 제시하는 비용 대비 효과 분석을 사용할 경우 비용 부분에 대해서는 상당 부분 정량적으로 산출이 가능하다. 특히, Kim이 제시한 정보보호 통제 수단에 대한 9분면 모델을 통해서 비용을 종합적으로 집계할 수 있다.[27] 그러나 인터넷 메신저와 관련된 직접적 효과의 정량화에 대해서는 아직 활용할만한 연구가 부족하여 기존 이론을 본 사례의 정량적 효과분석에 그대로 적용하기에는 어려움이 존재했다. 따라서 본 연구에서는 Kim이 제시한 운영 효과와 전략 효과의 일부 항목에 대하여 S사의 직원들을 대상으로 표 6과 같은 방법으로 설문을 실시하였다.

〈표 6〉 사례연구의 효과 검증을 위한 설문 개요

| 결정 요인 | 적용 내용 |
|---|---|
| 설문 형태 | 정성적 방법을 사용하여 다음의 두 가지 유형으로 조사<br>• 정형화된 설문: 항목별로 피응답자가 주관에 의하여 순위를 결정<br>• 자유 서술: 운영상의 문제점 및 불만에 대하여 자유롭게 서술 |
| 설문 대상 | • 정보보호 정책 및 운영 관련자: 5명 (직급 및 업무별로 균등하게 선정)<br>• 인터넷 메신저 사용자: 15명 (무작위 선정) |
| 설문 기간 | 인터넷 메신저 관련 보안 시스템 및 정책 시행 뒤 한달 이후 |
| 조사 방법 | 피응답자가 개별적으로 비공개로 설문에 응답 |
| 설문 항목 | Kim의 운영 효과와 전략 효과 중 일부 항목 |
| 기 타 | 설문 결과는 비공개이며, 설문 결과가 실제 인터넷 메신저의 보안 통제 체제를 변화시키기 위한 기초 자료로는 활용되지 않을 것임을 사전에 공지했음 (즉, 학술적 분석 자료로만 사용될 것임을 주지시켰음) |

개별 설문 항목 및 항목에 대한 응답 결과의 통계는 표 7과 같다. 설문 항목별로 피응답자는 1부터 5까지의 척도(1: 효과가 거의 없음, 2: 효과가 크지는 않음, 3: 비교적 효과가 있음, 4: 효과가 우수함, 5: 효과가 매우 우수함)에 대하셔 주관에 의하여 선택을 했다.

〈표 7〉 사례연구의 효과에 대한 설문 응답 결과 (정형화된 설문 문항)

| 설문 분야 | 조사 내용 | 설문 항목 | 정책 및 운영 관련자 | 인터넷 메신저 사용자 | 종합 |
|---|---|---|---|---|---|
| 운영 효과 | 비용절감 | 보상비용(법적인 분쟁) 감소 효과 | 4 | 3 | 3.5 |
| | | 영업기밀 유출 방지 효과 | 5 | 5 | 5 |
| | 생산성 증대 | 업무 생산성 증가 | 4 | 2 | 3 |
| | 업무기능 강화 | 정보소통 원활화로 의사결정 시간 단축 | 3 | 3 | 3 |
| 전략 효과 | 협업 수준 향상 | 외부기관/기업과의 협업 용이성 | 3 | 3 | 3 |
| | 고객과의 관계 개선 | 고객응대의 편의성 증가 | 2 | 1 | 1.5 |
| | 경쟁자 대비 | 기업의 신뢰도 증대에 기여하는 수준 | 4 | 3 | 3.5 |

설문 결과를 보면 관리자와 사용자 모두 영업기밀 유출에 대한 방지를 본 보안 체계의 가장 큰 효과로 꼽고 있음을 알 수 있다. 관리자와 사용자 층에서 가장 큰 차이를 보인 부분은 업무 생산성 증가에 대한 것이다. 관리자측은 보안 체계를 통해 인터넷 메신저 사용에 대해 불필요한 사용이 감소하여 업무 생산성이 증가한 것으로 판단한 반면에 사용자들은 모니터링에 대한 부담감으로 오히려 적절한 수준의 의사소통까지도 저해하는 부분이 있다고 주장한 것이다. 설문 항목 중 "고객응대의 편의성 증가"와 관련해서는 조사 대상기업에서 고객사를 대상으로 인터넷 메신저를 사용하는 경우자체가 거의 없다는 것이 효과가 낮게 평가된 이유로 판단되었다.

자유 서술 방식으로 진행된 문제점 및 불만에 대한 조사에서는 크게 두 가지의 의견이 나타났다. 관리자측은 인터넷 메신저 관리 시스템의 기능상 문제를 많이 거론하였다. 구축된 시스템이 자사 내부에서 사용되는 모든 종류의 인터넷 메신저에 대하여 완벽한 모니터링 및 기록 저장이 이루어지지 못한다는 것이다. 또한, 모니터링이 가능한 메신저 내에서도 일부 송수신 정보를 누락하는 경우가 있음을 지적하였다. 이는 앞서 지적한 것과 같이 비공개이며 비표준인 메신저의 프로토콜을 역공학으로 분석하여 시스템을 구축하는 과정에서 발생한 문제로 파악되었다. 사용자측은 모니터링된 메신저 송수신 정보의 관리 및 참조에 대한 권한 관리 및 운영 정책에 대하여 많은 우려를 나타내었다. 이와 관련해서는 초기 정책 수립과 의식개선 활동 과정에서 많은 주의가 기울여진 부분이고 사용자들에게도 많이 교육된 내용임에도 불구하고 실제 사용자들의 본 문제에 대한 신뢰도는 낮게 나타났다.

## 5. 결 론

인터넷 메신저는 실시간으로 일대일 통신을 하기 위한 대표적 수단으로 자리 잡고 있다. 아직까지 대부분의 메신저는 안정적인 성능을 무상으로 제공되고 있으며, 그 기반이 되는 인터넷 환경에 대하여 인터넷 메신저의 활용을 위해 추가적인 비용 부담을 해야 하는 요소가 거의 없기 때문이다. 또한, 다른 사용자와 전화, 팩스, 전자우편 등을 통해 통신하는 경우에 비하여 사용자가 느끼는 편의성이 상대적으로 매우 높으며, 단순한 메시지 전달과 파일 공유 이외에 화상 회의, 부재중 표시, 단문 메시지 서비스와의 연계 등 매우 다양한 기능을 제공하기 때문이다.

본 논문에서는 이렇듯 기업의 정보화 환경에서 필수적인 요소로 자리 잡고 있는 인터넷 메신저가 가지고 있는 잠재적 위험에 대하여 분석하고 이에 대한 대응책을 제시하였다. 위험 요인에 대해서는 전통적인 위험 분석 기법 중 정성적 분석을 통해서 항목화 및 우선 순위를 나누었는데 기업의 영업기밀 관련 내용을 메신저로 송수신 할 경우 암호화되지 않은 통신 채널에 대하여 비인가된 제3자가 도청을 하여 정보가 유출되는 위험, 기업의 영업기밀 관련 내용이 송신에 대한 접근통제를 받지 않는 인터넷 메신저로 인하여 외부로 비인가된 상태로 유출되는 위험, 인터넷 메신저로 외부의 악성 코드들이 유입되어서 사용자 컴퓨터 시스템의 무결성을 침해하는 위험 등이 가장 큰 위험 요소로 평가되었다. 대응책인 통제 수단에 대해서는 기존에 존재하는 보안 통제의 요소를 각각의 위험에 연계하였다. 또한, 본 연구에서 제시한 보안 체계의 실효성을 점검하기 위하여 실제 기업에서 인터넷 메신저의 보안 체계를 본 연구에서 제시한 방법을 통해 구축하였으며, 사례에 대한 검증을 통해 본 이론의 효율성 및 개선점을 고찰하였다. 인터넷 메신저의 기존 보안 체계 및 이에 대해 본 연구의 제시한 보안 체계를 정리해보면 표 8과 같다.

본 연구는 연구 대상의 특성상 분석 대상 메신저의 서비스 업체별 특성, 사례연구 적용기업의 특징 및 실제 운영과 관련된 세부적 결과를 제시하지 못하고 있다. 따라서 특정 환경에서 본 연구에서 제시한 보안 체계를 개선 없이 적용하는 것에는 많은 어려움이 있을 것이다. 그리고 효과 검증이 정량적이지 못했기에 본 보안 체계의 도입 추진 과정에서 문제시 될 수 있는 의사결정 자료의 부족은 본 연구의 한계점이다.[27,30]

사례연구의 검증 부분에서 설명한 것과 같이 본 연구에서 제시한 내용 중 다음과 같은 부분들이 추후 보강되어야 할 것이다. 1) 인터넷 메신저 관리 시스템에 대한 연구: 인터넷 메신저에 대한 관리 시스템과 관련해서는 향후에도 많은 연구와 개발이 뒷받침되어야 한다. 이는 인터넷 메신저를 기업 내부의 통신 수단으로만 사용하는 것이 아닌 기업 내외부의 공통된 통신 수단으로 사용하려는 목적 상 공개된 인터넷 메신

〈표 8〉 인터넷 메신저의 기존 보안 체계 및 본 연구에서 제시한 보안 체계

| 인터넷 메신저의 기존 보안 체계 | 본 연구에서 제시한 보안 체계 |
|---|---|
| 통신 채널이 암호화 되어있지 않음 | 내부망에서는 인터넷 메신저의 통신 채널이 암호화 되어 있지 않음을 사용자에게 주지시키고, 외부 망을 경유하는 경우에는 상대방 측과 암호화 채널로 통신하거나 첨부 파일을 암호화하도록 한다. |
| 정보 송수신에 대한 접근 통제가 없음 | 인터넷 메신저를 통해서 송수신이 제한되는 기업 영업기밀을 정의하여 사용자에게 주지시키고, 채널에 대해 모니터링을 수행하여 교류되는 정보의 유형 및 규모를 파악하고 필터링을 수행한다. |
| 외부에서 유입되는 트래픽에 대한 통제가 없음 | 메신저 클라이언트 PC의 주요 시스템 정보 및 데이터를 주기적으로 백업하여 복구 시스템을 마련하고, 안티바이러스 프로그램을 메신저 클라이언트 PC에 함께 설치한다. 또한, 외부에서 유입되는 인터넷 메신저 트래픽에 대하여 모니터링을 수행하여 저작권 침해에 대응한다. |
| 사용자 인증 정보에 대한 보안기능이 약함 | 업무용으로 허용된 인터넷 메신저의 경우는 대화 중에 표시되는 사용자명에 일정한 규칙을 부여하여 대화 상대의 식별을 용이하게 하고, 인터넷 메신저 클라이언트 PC의 로그인 기능을 강화하고 화면 보호기 기능을 사용한다. |

저를 주로 사용하게 되는 환경에서 그 기능과 프로토콜 등이 점점 복잡해지는 메신저용 프로그램들에 대하여 기업 내부에서 적절한 모니터링과 접근 통제를 수행하기 위함이다. 2) 비용 대비 효과 분석에 대한 연구: 기존의 보안 투자에 대한 효과 분석 연구로는 이와 같은 보안 체계 구축에 대한 효과를 정량화하기가 어렵다. 따라서 보안 통제하에서의 인터넷 메신저 사용으로 인한 업무 효율성 증대 및 정보 유출 방지효과 등에 대한 연구가 보강되어야 할 것이다. 3) 세부적 정책, 절차 및 지침의 개발: 개별 기업의 특징, 인터넷 메신저의 종류, 인터넷 메신저의 사용 목적 및 형태 등에 따라서 적용 가능한 세분화되고 세부적인 정책, 절차 및 지침서의 내용에 대한 개발이 추가되어야 한다.

인터넷 메신저는 기업 업무 효율성 증대를 위해 앞으로도 더 많은 기여를 할 것으로 기대된다. 그러나 그에 버금가는 많은 위험 요인도 내포하고 있는 것이 사실이다. 따라서 인터넷 메신저를 주요 통신 수단으로 채택하는 기업에서는 인터넷 메신저의 잠재적 위험에 대한 적절한 통제 수단의 구축과 운영에 많은 노력을 기울여야 한다. 본 논문에서 제시한 위험 분석 결과와 기술적, 관리적 통제 수단의 체계는 이와 같은 노력에 기여하는 바가 있을 것이다.

## 참 고 문 헌


[1] Grey, M., "Love It or Hate It: Instant Messaging Invades the Enterprise", Gartner, 2001.

[2] Grey, M., Batchelder, R., "Free Instant Messaging: Taming the Wild Beast", Gartner, 2001.

[3] Beer, S., "Instant Mayhem", SMH, 2003.

[4] Andrews, W., "Not So Fast: IM's Evolution Needs Auxiliary Technologies", Gartner, 2001.

[5] Piccard, P., "Risk Exposure: Instant Messaging and Peer-To-Peer Networks v2.0", Internet Security Systems, 2002.

[6] Ropoer, C.A., "Risk Management for Security Professionals", Butterworth Heinemann, 1999.

[7] Sage, A.P., "Systems Engineering", John Wiley & Sons, New York, 1992.

[8] Mayerfeld, H., "Definition and Identification of Assets as the Basis for Risk Management", in Proceedings 1988 Computer Security Risk Management Model Builders Workshop, 1988.

[9] Fites, et al., "Controls and Security of Computer Information Systems", Computer Science Press, 1989.

[10] Amoroso, E.G., "Fundamentals of Computer Security Technology", Prentice Hall, 1994.

[11] Vallabhaneni, R., "CISSP Examination Textbooks", SRV Professional Publications, 2000.

[12] Fites, P.E., Kratz, M.P.J., Brebner A.F., "Controls and Security of Computer Information Systems", Computer Science Press, 1989.

[13] Hutt, A.E. "Management's Roles in Computer Security", in Hutt, A.E., Hoyt, D.B. and Bosworth, S. (Ed.), Computer Security Handbook, Macmillan Publishing Company, 1987.

[14] Krutz, R.L., Vines, R.D., "The CISSP Prep Guide: Mastering the Ten Domains of Computer Security", John Wiley & Sons, New York, 2001.

[15] Schweitzer, J.A., "Protecting Information in the Electronic Workplace: A Guide for Managers", Reston Publishing Company, Reston, VA, 1983.

[16] Madnick, S.E., "Management Policies and Procedures Needed for Effective Computer Security", Sloan Management Review, Vol.19 No.3, 1978.

[17] Fine, L.H., "Computer Security - A Handbook for Management", William Heinemann, 1983.

[18] Li, D.H., "Controls in a Computer Environment: Objectives, Guidelines, and Audit Procedures", EDP Auditors Foundation, 1983.

[19] Simpson, R., McHugh, D., Wheatman, V., Stiennon, R., "New Instant Messaging Virus Exploits Your Trust", Gartner, 2002.

[20] Harris, S., "CISSP All-in-One Exam Guide", Second Edition. McGraw-Hill, 2003.

[21] Stiennon, R., "What May Lurk in Your IM Session", Gartner, 2001.

[22] Kim, S., Kang, S., "A Study on the Security Vulnerabilities and Defense Mechanism for SET-based Electronic Commerce", The Journal of CALS/EC, Vol. 4, No. 2, 1999.

[23] Kushida, T., "An Empirical Study of the Characteristics of Internet Traffic", Computer Communications, 1999.

[24] Wood, C.C., "Effective Information Security Management", Elsevier Advanced Technology, Oxford, 1991.

[25] Stoneburner, G., Goguen, A., Feringa, A., "Risk Management Guide for Information Technology Systems", NIST, 2001.

[26] Blakley, B., "Returns on Security Investment: An Imprecise but Necessary Calculation", Secure Business Quarterly, Vol. 1, 2001.

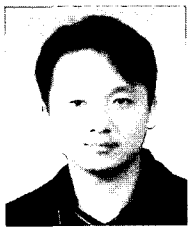
[27] Kim, S., Lee, H.J., "Cost-Benefit Analysis of Security Investments: A Methodology and Case Study", Lecture Notes in Computer Science, vol.3482, Springer Verlag, 2005.

[28] Scott, D., "Security Investment Justification and Success Factors", Gartner, 1998.

[29] Witty, R. et al., "The Price of Information Security, Strategic Analysis Report", Gartner, 2001.

[30] Kim, S., Leem, C.S., "An Information Engineering Methodology for the Security Strategy Planning", Lecture Notes in Computer Science, Vol 3043, 2004.

## ◐ 저 자 소 개 ◑



**김 상 균**
2005년 연세대학교 대학원 인지과학 · 컴퓨터산업공학과 졸업(박사)
2002 ~ 현재 (주)소만사 이사
관심분야 : Information Security, Information Engineering, e-Business
E-mail : saviour@yonsei.ac.kr

**이 홍 주 (Hong Joo Lee)**
2006년 연세대학교 대학원 컴퓨터산업공학과 졸업(박사)
-연세대학교 지식정보화연구센터 연구원
-대우일렉트로닉스 품질신뢰성연구소 연구원
-홍익대학교/고려대학교/단국대학교 강사
관심분야 : Strategic use of new technology, Business Intelligence, Information Engineering
E-mail : phileo21@empas.com