e-Business Security 프레임웍과 적용 방안

홍승필*, 김명철**, 김재현***, 김민형*
* LG CNS
** 한국 정보통신 대학교 교수
*** 성균관대학교 컴퓨터교육과 교수

요 약

인터넷의 발전과 더불어 빠르게 발전하는 e-Business 환경에서 그 편리함과 유익성에 반비례하여 위험/위협요소에 쉽게 노출되어지고 있다. e-Business 환경에서의 정보보안의 위협은 사용자의 실수등에 의한 사고에 의한 위협(Accidental Threats) 악의적 목적이나 영리추구를 위한 의도적인 위협(Intentional Threats)등으로 나뉘어 매우 빠르게 발생하고 있다. 이와 같이 점점 다양해지고 복잡해지는 e-Business 환경에서 가장 적합하고 안전한 정보보안 솔루션을 구현하기 위해서나, 또는 관련업체의 정보보안 장단점을 알아보기 위한 현황분석 등을 위하여 표준이나 기준이 될 수 있는 가이드라인이 필요하게 되었다, 이에 본 논문에서는 LG CNS에서 제시하는 정보보안의 프레임웍을 이용하여 e-Business 정보보안의 구현 방안에 대하여 설명하고자 한다.

이 프레임웍은 크게 정보보안의 기본전략, 메커니즘, 그리고 관리적 영역과 기술적 영역으로 나뉘어 보여지고 있다. 본 논문에서 제시되는 정보보안 프레임웍에 준하여, 실제 개발자나 정보보안 관련 엔지니어가 좀 더 쉽게 현존하는 시스템 환경에 적용하고 더 나아가 정보보안 구현의 초석이 될수 있는 아키텍처를 소개하였다. 보안 아키텍처는 신뢰성 있는 보안 구현 방안을 제시하기 하기 위해, 네트워크/시스템 영역을 각각의 비즈니스 영역을 고려하여 구분하고, 이 영역별로 차별화 된 보안 솔루션을 구현하여 효과적인 보안구현 전략을 제시하는데 그 의의가 있다.

마지막으로 본 논문에서는 e-Business 환경에서의 통합 정보보안 솔루션을 기반으로 실제 e-Business 환경인 e-Marketplace중 Procurement에 적용될 수 있는 정보보안의 구현 사례를 제시하였다. 실 비즈니스 환경 분석을 통해 야기 될 수 있는 대표적인 위험/위협요소인 사용자 신분인증 및 문서의 위/변조등에 대응하여 적용되는 다양한 보안 솔루션 중 웹 기반에서의 사용자 인증통합 및 비즈니스적 연동이 빈번한 제휴 업체들과의 신뢰할 수 있는 접근통제가 요구되는 환경에서 프레임웍에 준하여 적용되어지는 사례 분석을 해 봄으로써 활용 가치를 증명해 보았다.

e-Business Security Framework and applied to Architecture

Seung-Phil Hong*, Myung-Chul Kim**, Jaehyoun Kim***, Min-Hyung Kim*

ABSTRACT

Many firms are utilizing the Internet and various information technologies to effectively manage their business operations with a goal of gaining a competitive advantage in the rapidly changing business environments. Today, the business is characterized as digital economy where information freely flows and business processes are improved with the use of information technologies. Internet technology is playing a key role in transforming the organization and creating new business models. It has become the infrastructure of choice for electronic commerce because it provides process efficiency, cost reduction, and open standards that can easily be adopted by different organizations. Here, the vast amount of data and information slow among the related parties and security issues are very critical matter of research interests by academicians and practitioners. In this research, we address the importance of security framework in managing the data shared among the related parties in the e-business and suggest the security architecture for effectively supporting the needs of e-business in an organization. This research provides valuable contributions both in academics and industry in terms of how security framework and architecture should be set in order to provide the necessary e-business.

1. e-Business Security 개요

정보화 시대는 새로운 문명의 탄생 및 발전으로 인류에게 그 편리함과 유익성이라는 혜택을 제공하는 반면 자연적으로 파생되는 역기능으로 인한 피해를 가져다 준다. 그 편리함과 유익성에 반비례하여 매우 위험하고 파괴적인 역기능이 뒤따르고 있으며 인터넷의 발전과 더불어 빠르게 발전하는 e-Business 환경에서도. 이와 같은 위험/위협요소에 쉽게 노출되어지고 있다. e-Business 환경에서의 정보보안의 정의는 인터넷을 기반으로 한 모든 비즈니스 활동이 1) 신뢰할만하고, 2) 다양한 인증방법을 통해 접근가능하며, 3)고객과 사용자에게 맞춤화된 서비스를 제공할 수 있도록 가상공간의 정보시스템을 보호하는 서비스이며 정보보호 목적은 다음과 같이 표현될 수 있다.[1][12][13][15]

1. 정상적인 정보시스템을 유지하여 필요한 정보를 적시적소에 정당한 사용자에게 정보의 변조,훼손,유출 없이 제공함을 목적으로 한다.
2. 개인정보의 안정성 확보로 정보 통신망에서 벌어지는 범죄사고를 퇴치하여 안전하고 건전한 정보사회를 이룩한다.
3. 기업이나 조직,나아가서는 국가의 정보자산 및 지적 재산권을 해킹으로부터 안전하게 보호함을 그 목적으로 한다.
4. 기업이나 조직이 보유하고 있는 정보자산을 파악하여 기밀 자료 분류 및 등급을 정의함으로써 경쟁업체 및 악의의 침해로부터 기업의 정보자산을 보호하는 데 그 목적이 있다.

2. e-Business Security 위험/위협 분석

e-Business 환경에서의 정보보안의 위협은 사용자의 실수등에 의한 사고에 의한 위협(Accidental Threats) 악의적 목적이나 영리추구를 위한 의도적인 위협(Intentional Threats)으로 나뉠 수 있으며 대표적인 위협 요소는 아래 <표 1>과 같다 [6][7][8]

<표 1> e-Business 환경에서의 대표적 위험/위협 요소

대표적인 위협/위험	설명
산업 스파이 및 정보 절취	산업스파이 문제는 현재 계속 증가하고 있으며 이러한 문제는 현재 또는 이전의 고용인에 의해 발생한다. 이러한 산업스파이는 원격 시스템에서 공격하는 공격자들 보다 감지하기가 매우 어려우며 문제 발생시 예방책들이 매우 복잡하고 비용이 많이 요구됨으로, 이러한 예방책들은 오직 치명적인 자원에만 사용되는 것이 적절하다.
악의적 코드 (Malicious Code)	악의적 코드는 간접적인 서비스 방해(Denial of Service) 공격으로 볼 수 있다. 대부분의 사용자들은 이제 바이러스 또는 웜(Worms), 트로이 목마, 유전자 알고리즘(genetic algorithms)에 의한 위협등이 있다.
사회공학 공격 (Social Engineering Attack)	사회공학 공격은 실제 네트워크 또는 컴퓨터의 취약점을 이용하는 공격 방법이 아닌 경험이 없는 사용자를 속에 패스워드를 바꾸도록 하는 것과 같은 방법으로 합법적인 사용자의 ID와 패스워드를 획득하는 등의 공격법이다.

대표적인 위협/위험	설명
합법적 사용자 가장 (Impersonation)	유효한 사용자 ID와 패스워드를 획득한 공격자는 이를 다시 사용하여 시스템에 접근 하는 방법으로. 예를 들어, 어떤 사용자가 원격 시스템에서 접속하기 위해 텔넷 프로그램을 사용할 때 tcpdump 또는 nitsniff등과 같은 Network Sniffer를 사용하는 공격자는 사용자 ID와 패스워드를 가로챌 수 있다.
취약점 악용	취약점 악용은 소프트웨어의 결함을 찾아내는 공격 방법이다. 대부분의 CERT 권고문들은 대부분 이 유형의 공격에 대한 예방책이다. 예를 들어 UNIX의 Sendmail 프로그램은 root 권한으로 실행된다.

3. e-Business Security 프레임웍(Framework)

e-Business 환경에서 정보보안의 기본 영역 및 구현 방안을 소개하는 프레임웍을 설명하는 것은 매우 어려운 부분임에도 불구하고 다양해지고 복잡해지는 e-Business 환경에서 가장 적합하고 안전한 정보보안 솔루션을 구현하기 위해서나, 또는 자사의 정보보안 장단점을 알아보기 위한 현황분석 등을 위하여 표준이나 기준이 될 수 있는 가이드라인이 필요하며, 요즘 정부에서도 정보보안의 중요성을 인식하고 정보보안에 대한 분석을 통한 업체나 관련 업계의 도움이 되는 표준화 성격이 문서가 소개되고 있다. 다음은 LG CNS에서 제시하는 정보보안의 프레임웍을 이용하여 e-Business 정보보안의 구현 방안에 대하여 설명하고자 한다.

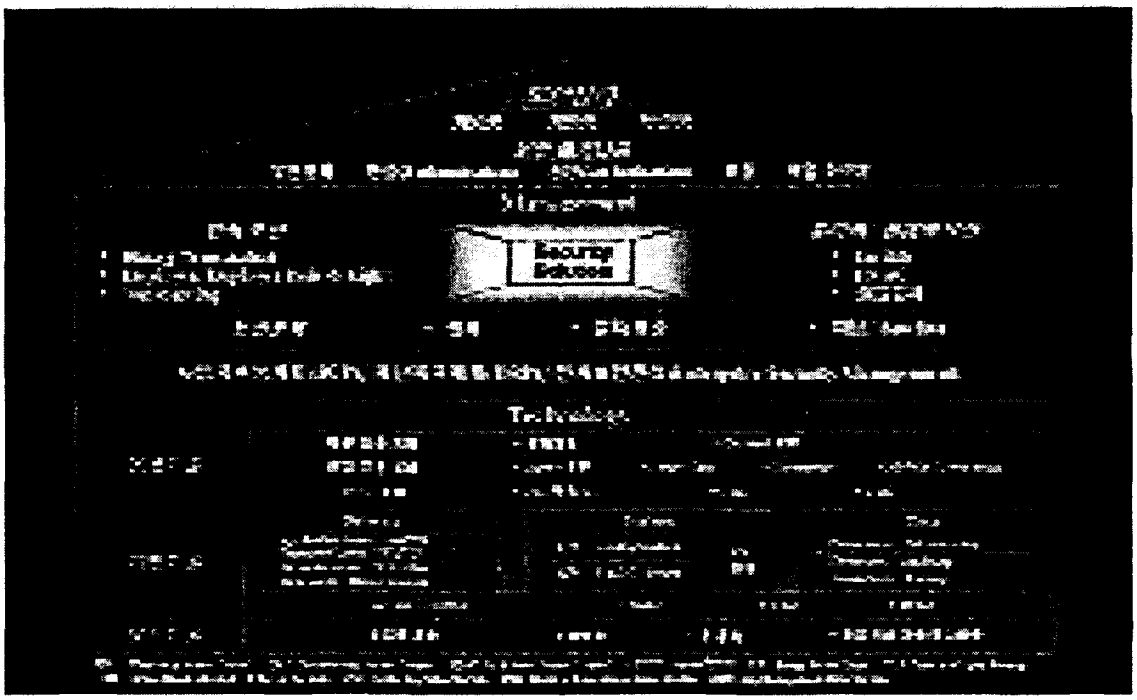
이 프레임웍은 크게 정보보안의 기본전략, 메커니즘, 그리고 관리적 영역과 기술적 영역으로 나뉘어 보여지고 있다. 무엇보다 보안 정책 수립 및 인적/물적 보안관리가 중요하며, 보안기술은 이들의 취약부분을 그에 준하는 기술을 적용하여 보안정책을 효과적으로 집행하고 관리하는 데 도움을 주도록 구성될 뿐이다. 이런 이유로 기업의 업무지속성 계획(Business Continuity Planning), 재난복구 계획(Disaster Recovery Planning), 전사적 보안관리(Enterprise Security Management)라는 세 가지 관점에서 보안의 관리적 측면(정책수립, 인적보안관리, 물적보안관리)이 강조되며, 정보보안기술과 솔루션의 유기적인 결합이 이를 뒷받침되어야 한다. [6][7]

정보보안 기술영역을 분류함에 있어서는 수직으로는 기술의 쓰임세에 따라 세 가지 계층별 분류(요소기술, 기반기술, 응용기술)를, 수평적으로는 각 계층 내에서 기술의 적용범위나 적용대상에 따라 영역별(Network, System, Data, Access Control) 분류와 상세 계층별(복합/단일/기반응용, 네트워크 4계층 모형) 분류를 병행하였다.

요소기술은 정보기술시스템의 기반을 형성하는 기술로, 만일 이러한 기술이 밑받침 되지 않는다면 현실세계를 사이버 상에 그대로 재현할 때 반드시 전제되어야 할 안전성과 신뢰성을 유지할 수 없다.

기반기술은 요소기술을 바탕으로 물리적인 정보 인프라를 건설하기 위해 요구되는 기술로서 정보의 생성과 처리(System 영역), 정보의 저장(Data 영역), 정보의 공유(Network 영역)를 담당하는 인프라를 구축한다.

4. e-Business security 구현 방안



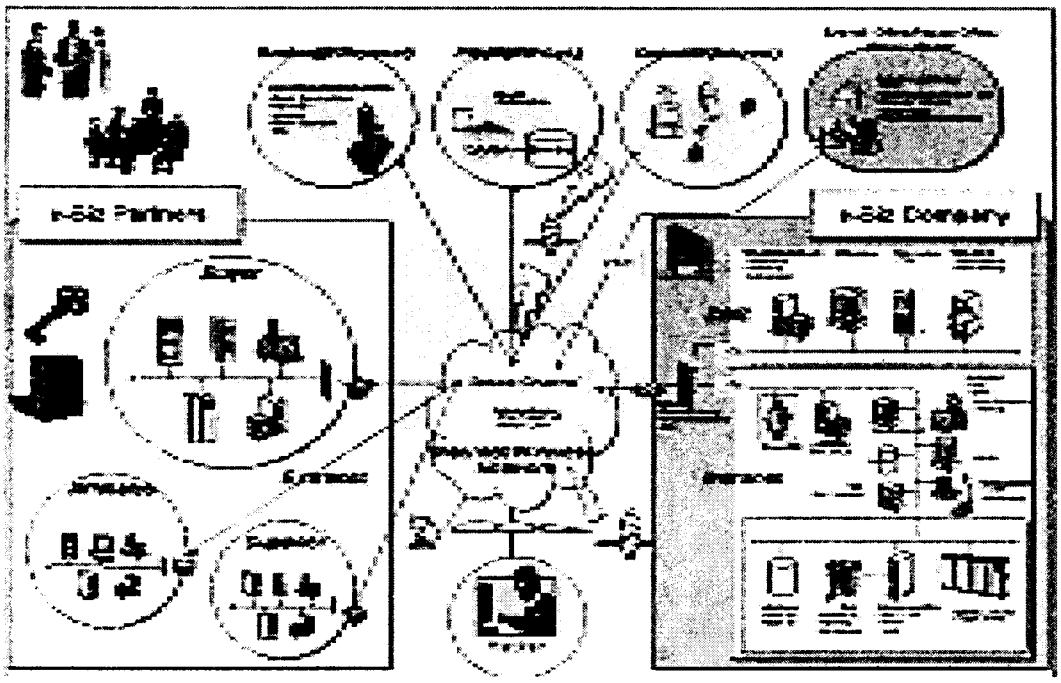
(그림 1) 정보보안 프레임웍 (LG CNS 예)

4.1 e-Business 정보보안 아키텍쳐

e-Business 정보보안 아키텍쳐는 보안의 깊이와 강도 그리고 선택된 기술과 제품을 바탕으로, 특정 e-Business기업을 대상으로 한 것이 아닌, 보편적인 보안 구성을 제시한다. 그러나 현실 적용에 따라 깊이 있는 분석과 평가에 근거한 변형된 구성 형태를 가질 수 있으며, (그림 2)에 제시된 보안 아키텍쳐는 보안 구현을 효과적으로 하기 위해, 네트워크/시스템 영역을 각각의 비즈니스 영역을 고려하여 구분하고, 이 영역별로 차별화 된 보안 솔루션을 구현하여 효과적인 보안구현 전략을 제시하는데 그 의의가 있다.

(그림 2)의 e-Business 정보보안 아키텍쳐에서는 비즈니스 기능 전담과 통합을 고려해 아래와 같은 요소별 보안 솔루션을 적용하였다 [4][9][10][11]

1. 침입차단시스템(Firewall)/침입탐지시스템(IDS)/가상 사설망(VPN) 서버
2. 공개키 기반구조(PKI)/실시간 인증서 유효확인(OCSP)/ 디렉터리 서비스(Directory)/ 통합login(SSO)/서버 접근제어(Server Access Control)
2. 네트워크 데이터 검색(Content Inspection or Virus Wall)
3. 사용자 일괄관리와 감사 로그 통합 관리(Admin & Audit)
4. 시스템 위험 분석(Risk Analysis Tool)
5. 일회용 패스워드와 스마트카드 / HSM (Hardware Security Module)

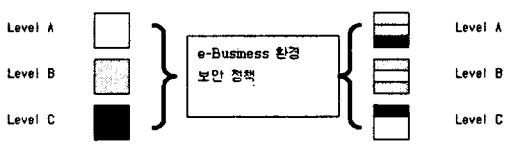


(그림 2) e-Business 정보보안 아키텍처

위에서 제시된 e-Business 보안 아키텍처는 e-Business의 규모에 따라 다양한 상황 및 환경에서 변화된 모습을 가질 수 있다. 다양한 고객의 시스템/업무 환경에 대한 보안 아키텍처가 구현/적용되는 모습을 효과적으로 구현할 수 있다, 예를 들어 상거래 트랜잭션에 대해, SET, secure EDI, SSL, PKI등의 다양한 방법을 제공하여 보안을 구현하는 방안을 제시하고 있다. 이는 차후 e-Business 환경에서의 정보보안 구현 솔루션 선정 및 적용 시 선택된 기술과 제품이 목적한 보안 기능 요구 사항들을 충분히 만족시키며 구현되었는지를 검증할 수 있는 척도로서 활용될 수 있다.

4.2 보안 정책 (Security Policy)

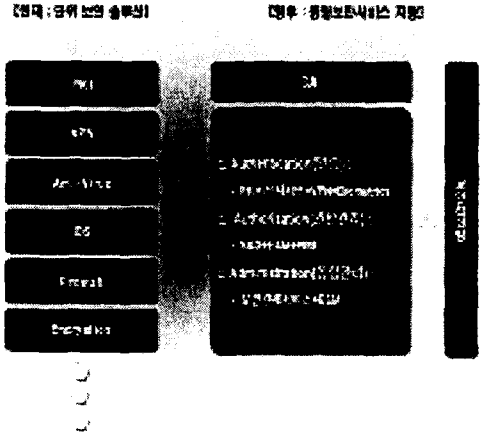
점점 분산화 되고, 다양해 지는 e-business 환경에서는 앞에서 제시한 명확한 형태의 보안 정책 및 절차(Procedure) 보다는 인터넷 시스템 환경에 적합한 형태의 안전하고 실용 적인 보안 정책을 인프라적 요소로 구현하는 것이 중요시 되고 있으며, 이는 기존의 군사체제에서와 같이 엄격하고 명확한 보안 정책 보다는 비즈니스 요구에 능동적으로 대처 할 수 있는 하이브리드 형식의 보안 정책이 적용되고 있다.[7][15]



(그림 3) e-Business 환경의 보안 정책의 적용

4.3 구현 기술 및 전망

e-Business 환경에서의 가장 두드러진 정보보안의 전망은 기존의 방화벽, 백신 프로그램, 시스템 레벨의 정보보안 솔루션 등 단일화 되어 있던 솔루션이나 기술이 통합 구현되어 지고 있다는 점이라 할 수 있다.



(그림 4) e-Business 환경에서의 정보보안 전망

위의 (그림 4)에서와 같이 단일화된 보안 솔루션을 향후 3A (Authentication, Authorization, Administration) 와 같이 통합 인증된 솔루션의 효율적 관리와 정보보안 컨설팅과 같은 서비스가 접목되어 제공되어 진다고 볼 수 있다. 다음은 실제 이와 같이 접목된 기술이 e-Business 환경 내에서 적용 될 수 있는 분야를 아래 <표 2>와 같이 알아보자 [10][14]

5. e-Business Security 적용사례

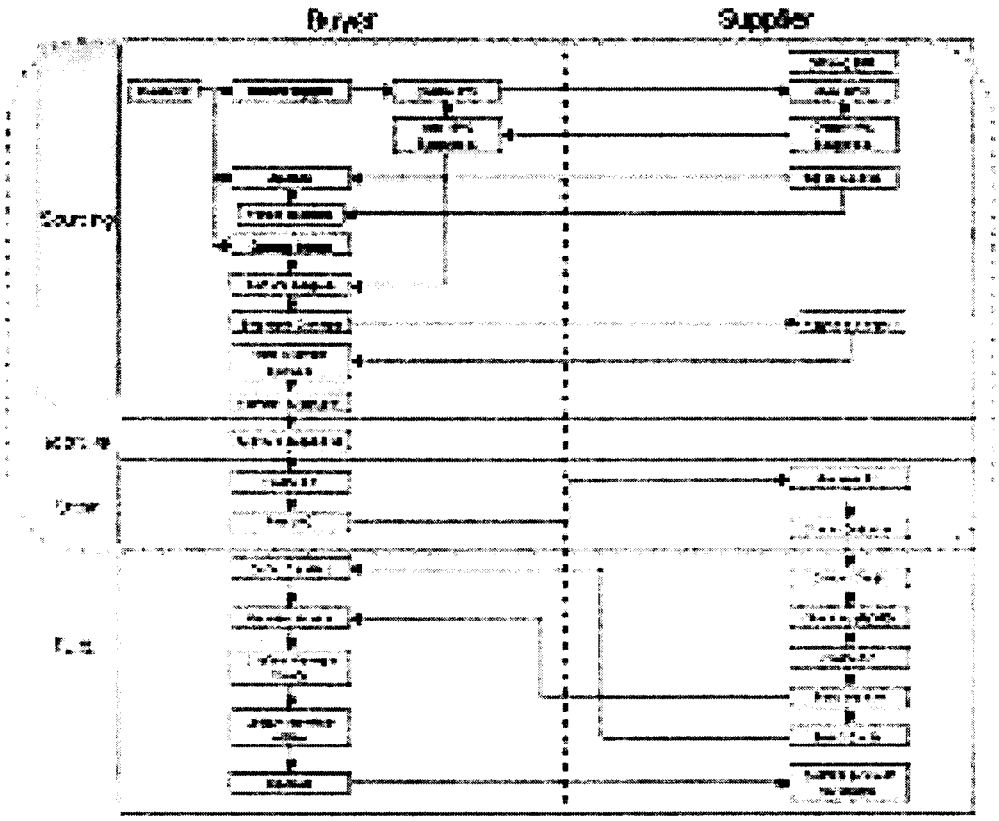
이번에는 실제 e-Business 환경인 e-Marketplace 중 Procurement에 적용될 수 있는 정보보안의 예를 들어 설명한다. 아래 (그림 5)는 e-Marketplace에서 요구되는 전반적인 비즈니스 프로세스이다.

<표 2> 적용 분야 및 적용 기술 Set

적용 분야	적용기술
Secure Transaction	통합 N/W 솔루션 구현방안 VPN/Firewall/IDS - 침입차단과 침입 탐지, 그리고 원격지간의 안전한 정보 전송을 위한 기술의 통합 구현 기술
Secure System	통합 시스템 솔루션 구현방안 Host 기반의 침입탐지시스템(IDS)과 역할 기반접근의(Role Based Access Control) 접목 기술
Application PKI / WPKI	B2B / B2C 사용자 인증 통합 기술 구현방안 CA/RA, OCSP. LDAP, Single-Sign-On과 같은 통합 사용자 인증 기술과 Mobile환경에서의 Wireless PKI 적용 기술

여기서 우리는 비즈니스 환경 분석을 통해 야기 될 수 있는 대표적인 위험요소인 사용자 신분인증 및 문서의 위/변조등에 대응하여 적용되는 다양한 보안 솔루션 중 웹 기반에서의 사용자 인증통합 및 비즈니스적 연동이 빈번한 제휴 업체들과의 신뢰할 수 있는 접근통제가 요구되는 환경에서 적용하여 보기로 한다. (그림 6)은 e-Marketplace에서 e-Procurement가 Buyer와 Supplier측을 기준으로 적용되는 아키텍쳐이다. [2][3]

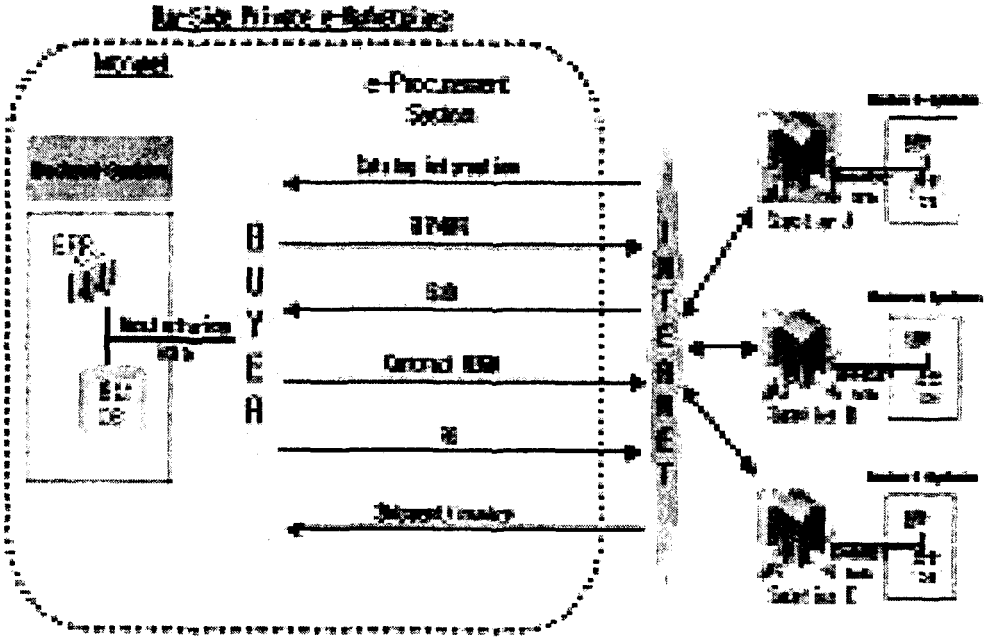
이제 우리는 아래 <표 3>과 같은 통합 보안 솔루션을 비즈니스 프로세스 분석을 통한 적용되는 경우를 알아보기로 한다.



(그림 5) e-Procurement의 Business Process

<표 3> 보안 적용 기술 및 서비스 내역

보안적용기술/서비스	구현 방안
역할별 접근통제	Buyer는 구매/발주를 내는 비즈니스 주체로써, Supplier는 구매/발주를 받아 처리하는 비즈니스 주체로써의 관련 업체들과의 부서별 접근 통제 및 권한 제한
사용자 계정 정책 및 권한 관리	Buyer Site와 Supplier Site에는 각각의 필요에 따른 직위별/업무별 권한/ 계정 관리 및 정책 수립
통합사용자인증 (Single-Sign-On)	인증 정보가 있는 경우와 없는 경우에 대한 적합한 권한정책에 따른 사이트 접근 가능
중앙집중적 관리 방안	웹 환경에서 중앙집중적 통합관리 지원 인터페이스 제공 관련 사이트에 대한 정책은 이 통합관리 인터페이스를 통해서만 설정/변경이 가능해야 함



(그림 6) e-Procurement 아키텍처

6. 결 론

우리는 간략하나마 e-Business 환경에서의 정보보안 위협/위험 요소, 프레임웍의 필요성과 e-Business 아키텍처 통합 기술과 정보보안 서비스를 통한 Trend 분석, 그리고 마지막으로 실제 e-Marketplace에서 비즈니스 프로세스 분석을 통한 정보보안 구현 방안을 통하여 적용 방안에 대하여 알아보았다. 실제로 위와 같은 e-Marketplace 시스템 환경에서의 정보보안 구현은 매우 복잡하고 어렵지만 위의 구현의 예를 통하여 e-Business 대비 정보보안의 구현 방안을 제시하였으며, 이는 다른 e-business domain 간에 적용될수 있는 정보보안의 가이드가 될수 있으리라 사려된다.

참고문헌

[1] Sudip Bhattacharjee, R. Ramesh, and Stanley Zionts, A Design Framework for e-Business Infrastructure Integration and Resource Management , IEEE Transactions on Systems, Man, and Cybernetics, Vol. 31, No. 3., August 2001, pp.304-319.

[2] Yanlong Zhang, Hong Zhu, Sue Greenwood, and Qingning Huo, Quality Modelling for Web-Based Information Systems , Proceedings of the Eighth IEEE Workshop on Future Trends of Distributed Computing Systems, 2001.

[3] M. E. Porter, Competitive Advantage: Creating and Sustaining Superior Performance, New York: The Free Press, MacMillan, 1985.

[4] Recommendation X.509. Information Technology- Open systems Interconnection The Directory: Authentication Framework, 1993 ISO/IEC9594-8:1993

[5] D.Wagner and B.Schineiner, Analysis of the SSL 3.0 Protocol. , in Proceedings of the Second UNIX Workshop on Electronic Commerce, November 1996.

[6] Deborah Russell and G.T. Gangemi Sr., Computer Security Basics, OReilly & Associates, Inc. 1991

[7] Harold F. Tipton and Micki Krause, Information Security Management Handbook, Auerbach, 2000

[8] Information processing systems Open Systems Interconnection Basic Reference Model Part 2 : Security Architecture, ISO 7498-2 : 1989(E)

[9] Boeyen S., Howes T., and Richard P., Internet X.509 Public Key Infrastructure LDAPv2 Schema , RFC 2587, June 1999

[10] Housley R., Ford W., Polk W., and Solo D., Internet X.509 Public Key Infrastructure Certificate And CRL Profile , RFC 2459, January 1999

[11] Charles P.pfleeger, Security in computing 2nd edition, Prentice Hall, 276-286

[12] Rendleman, J., Service Providers To Drive Internet, Communications Week, October 24, 1994b,

[13] Rendleman, J., Business Booming On the Internet, Communications Week, August 29, 1994

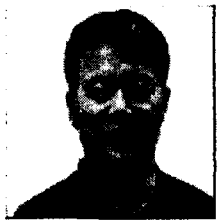
[14] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, and Charles E. Youman, Role-Based access control models , IEEE Computer: vol.29, no.2, pp. 38-47, Febuary, 1996.

[15] 홍승필,김명철,안길준,윤정태, e-Business Security , 파워북, 12, 2000,

홍 승 필

Indiana State Univ. Computer Science (이학사)
Ball State University Computer Science(이학석사)
Illinois Institute of Technology 박사수료 (인터넷 응용보안/ 연구)
현재 LG CNS Co. Ltd. 연구소에서 다수의 보안 프로젝트/컨설팅 수행 및 관련기술 연구
정보통신대학원 박사과정 재학중
CISSP (Certified Information System Security Professional)
전산망 침해사고 대응 및 협의회 회원
한국 PKI 포럼 회원
CALS / EC 협회 회원
IEEE Information Security Member
Open Group Security forum Member

김 명 철

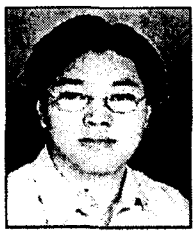


KAIST 컴퓨터네트워크 전산학석사
Univ. of British Columbia 전산학박사
한국통신, 연구실 실장
1998~현재 정보통신 대학원 교수 / 공학부장
관심분야 : 네트워크 프로토콜 응용 분야, e-Business 보안

김 재 현

성균관 대학교 수학과 졸
(미) Western Illinois University 전산학석사
(미) Illinois Institute of Technology 전산학 박사
(구) 주택은행 전산본부, CTO
2002.3~현재 성균관 대학교 / 컴퓨터 교육과

김 민 형



인하대학교 전자공학과(공학사)
현재 LG CNS Co., Ltd. 연구소에서 생체인증 및 스마트카드 보안 솔루션 연구
CISA (Certified Information System Auditor) / CISSP (Certified Information System Security Professional)