웹 서비스 기반의 전자정부 서비스 보안에 관한 연구

이 은 선[†] · 양 진 석[†] · 임 정 묵[†] · 문 기 영[††] · 이 재 승[††] · 정 태 명[†††]

요 약

전자정부 서비스는 국민, 기업, 정부부처에 새롭고 빠른 서비스를 제공하여 업무의 효율성을 향상시킬 뿐만 아니라 열린 정부, 투명한 정부를 지향하고 국가 경쟁력 확보를 위해서 필수 불가결한 국가적 과제이다. 전자정부 서비스는 그 특성상 매우 민감한 데이터를 전송하거나 처리하므로 전자정부 서비스에서 보안은 매우 중요하다. 그러나 현재까지 전자정부에 대한 연구는 다양한 컨텐츠와 인프라에 대한 개발만을 해왔다. 최근에서야 전자정부 선진국을 중심으로 전자정부 서비스에 대한 보안을 고려하기 시작하였다. 전자정부 서비스는 웹 서비스로 구축되어지고 있으며 보안을 고려할 때 웹 서비스 보안 기술에 대한 분석과 이를 전자정부에 적용하기 위한 전자정부에 대한 분석이 선행되어야한다. 본 논문에서는 전자정부 서비스 발전 단계를 고려한 웹 서비스 보안 적용 시나리오를 위해 전자정부와 웹 서비스 보안 기술을 분석하였으며 이를 기반으로 향후 구축될 범정부 통합전산환경에서 웹 서비스 보안 기술 적용을 위한 시나리오와 전체 뷰(view)를 제시하였다.

키워드 : 전자정부, 전자정부 보안, 통합전산환경, 웹 서비스 보안, 웹 서비스

A Study on Security of E-Government Service Based on Web Service

Eun-Seon Lee[†] · Jin-Seok Yang[†] · Jung-Muk Lim[†] · Ki-Young Moon[††]
Jae-Seung Lee[††] · Tai-Myoung Chung[†††]

ABSTRACT

E-Government service is national project that is necessary for international competitiveness, openness of government and effectiveness of governmental work process. E-Government security is very important because it treats data has relatively high sensitivity. But, until now, the development point of E-Government service has been limited to only it's contents and infrastructure based on web without consideration of E-Government security. Lately research for E-Government security has been studied by some advanced country of E-Government service, but it is insufficient. To construct E-Government security based on web Infra, first of all, analysis of web service security technology is needed to precede. And then research for appling the technology to E-Government service are required. We propose secure E-Government service scenario with web service security technology based on development stages of E-Government service. We also suggest overall view and secure scenario of E-Government service in Integrated Computing Environment.

Key Words : E-Government, E-Government Security, Integrated Computing Environment, Web Service Security, Web Service

1. 서 론

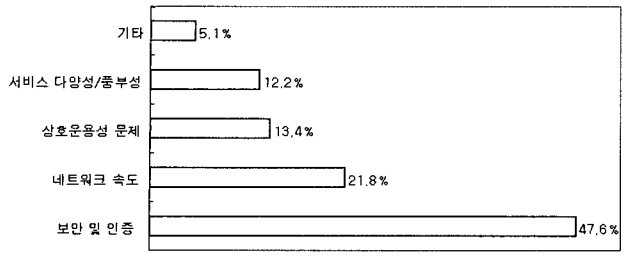
국가 행정 전산화의 중요성이 대두되면서 미국, 영국, 캐나다, 일본 등의 국가들이 정부가 제공하는 서비스를 전산화하려는 노력을 시작했다. 이러한 노력은 최근에 "E-Government"라는 이름으로 국가적인 전자정부 서비스를 제공하기 위한 시스템 및 인프라 구축을 시작하였다.

전자정부 서비스 구축의 목적은 국민들뿐만 아니라 기업, 정부부처에게 새롭고 빠른 행정 서비스를 제공하여 업무의 효율성을 향상시키고 열린 정부, 투명한 정부를 지향하며 궁극적으로는 국가 경쟁력 확보를 위해서이다.

전자정부 서비스는 국민, 기업, 그리고 정부부처에 서비스를 제공하는 전자정부의 특성 상 매우 민감한 정보들을 다루고 있으므로 사용자에게 신뢰를 주어야 성공적인 전자정부 서비스를 구축할 수 있다. 그러나 전자정부 서비스에서 보안은 초기 단계에 있으며 최근에서야 전자정부 서비스 보안을 고려하기 시작하였다.

전자정부 서비스는 분산화 되고 있는 컴퓨팅/네트워킹 기술의 발전과 더 나아가 U-Government로의 발전을 고려하여 웹 서비스 기술로 구축되고 있다. 웹 서비스 기술은 응용프로그램간의 상호 운용성을 제고하기 위한 새로운 소프트웨어 아키텍

※ 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성·지원사업의 연구결과로 수행되었음.
† 준 회 원 : 성균관대학교 정보통신공학부 컴퓨터공학과 인터넷관리기술연구실
†† 정 회 원 : 한국전자통신연구원 정보보호연구단
††† 종신회원 : 성균관대학교 정보통신공학부 컴퓨터공학과 인터넷관리기술연구실
논문접수 : 2004년 12월 7일, 심사완료 : 2005년 4월 4일



(그림 1) 웹 서비스 도입 시 장애요인[3]

처이다[5, 27].

웹 서비스는 서비스의 다양성, 통합의 용이성 등 많은 장점이 있지만 (그림 1)과 같은 부분에서의 단점이 지적되고 있으며 그 중 보안 및 인증을 가장 큰 장애요인으로 보고 있다.

전자정부 서비스에 웹 서비스 보안 기술을 효과적으로 적용하기 위해서는 전자정부의 서비스 별 특징을 파악하고 이에 적합한 보안 기술을 적용함으로써 가능하다. 최근에 전자정부 선진국들도 전자정부 서비스에서 웹 서비스 보안에 대한 관심을 가지고 이를 적용하기 위한 노력을 하고 있다. 국내의 전자정부 서비스는 현재 전자적 거래가 가능한 단계이나 포털을 중심으로 웹 언어, 인증서 기술 등의 전통적 기법을 통해 보안성을 획득하고 있으며, 웹 서비스는 아직 적용되지 않았다. 전자정부의 웹 서비스를 도입을 위한 연구가 현재 진행되고 있지만 실질적 결합모델은 확정되지 않았고 또한 정부 내 부처간 서비스 통합에 대한 상세한 분석이 미진한 실정이다[30, 31]. 본 논문에서는 전자정부 서비스 발전 단계를 고려하여 정부부처 내, 정부와 소비자 간, 정부부처 간의 세 범위에서 전자정부의 동작 구조를 분석하였다. 유사 조직의 웹 서비스 적용 모델 및 웹 서비스 보안 기술의 분석을 통해 전자정부를 위한 웹 서비스 적용 구조와 보안을 위한 웹 서비스 기술 적용방안을 제시하고자 하였다. 이를 기반으로 차후 구축될 통합 전산환경의 웹 서비스 보안 적용 시나리오를 제시한다.

본 논문의 2장은 국내/외 전자정부 구축 동향 및 보안 동향을 알아보고 3장에서는 최근 표준화되고 있는 웹 서비스 보안 기술을 분석한다. 4장은 전자정부 서비스에서 웹 서비스 보안 요구 사항에 대해서 기술하고 5장과 6장에서는 각각 통합전산환경에서 웹 서비스 보안 적용 시나리오와 결론을 기술한다.

2. 전자정부 구축 동향

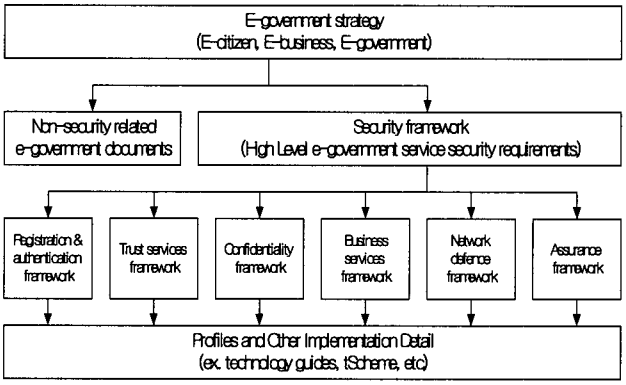
전자정부 서비스는 국민에게 편의성 제공, 국가 재정의 투명성, 정부 부처 업무의 감소 등의 장점으로 1990년대부터 활발히 진행되는 국가적 프로젝트이다. 이번 장에서는 전자정부 선진국으로 불리는 미국, 영국, 일본의 전자정부 구축 동향에 대해서 살펴보고, 우리 나라 전자정부 동향을 살펴본다.

2.1 국외 전자정부 구축 동향

해외의 전자정부 서비스는 영국, 미국, 일본 등을 중심으로 빠르게 구축되고 있다. 지금까지 진행된 대부분의 전자정부 프로젝트는 다양한 컨텐츠를 제공하기 위한 연구가 진행되었지만 보안 서비스에 대한 연구는 아직 초기 단계에 있다. 이번 장에서는 초기 단계에 있는 전자정부 선진국들의 보안 관련 프로젝트 및 정책 추진 동향에 대해서 살펴본다.

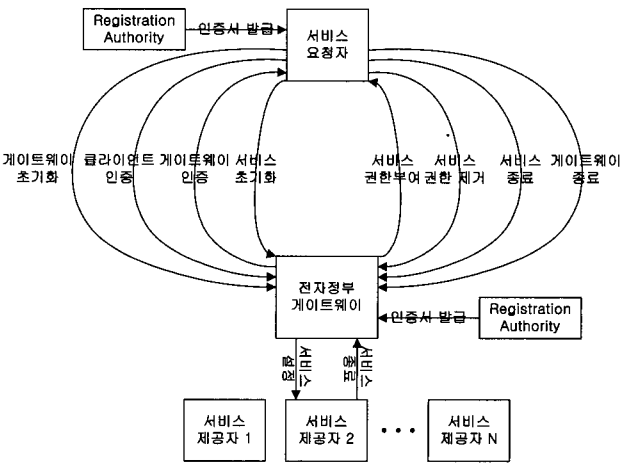
영국은 몇 가지 보안 주제를 가지고 전자정부 서비스 보안에 대한 내용을 기술하고 있다. (그림 2)는 영국의 전자정부 보안 프레임워크가 다루는 보안 분야를 나타낸다.

영국의 전자정부 보안 프레임워크는 크게 등록/인증, 신뢰서비스, 기밀성, 비즈니스 서비스, 네트워크 방어, 보증 프레임워크로 나뉜다. 프레임워크를 기술하는 각각의 문서들은 해당되는 분야의 보안 레이블링을 하였으며 이에 따른 위험과 대응방법을 추상적으로 기술하고 있다[9, 10, 11 12, 13, 14, 15]. 또한 영국은 (그림 3)에서 보는 바와 같이 전자정부 보안 아키텍처를 제시하였다[8].



(그림 2) 영국의 전자정부 보안 프레임워크

서비스를 이용하고자 하는 요청자는 먼저 등록을 통해 인증서를 발급받아 서비스에 접근할 수 있다. 서비스 요청자는 인증을 위해서 먼저 전자정부 게이트웨이를 통과해야하며 전자정부 게이트웨이는 단일사용자인증이 가능하여 인증 이후 서비스에 대해서는 추가적인 인증 절차가 불필요하다.



(그림 3) 영국의 전자정부 보안 아키텍처

미국에서 가장 중요한 보안 분야로 생각하고 있는 전자인증은 정보유출, 프라이버시 침해의 우려를 최소화하면서 온라인

거래의 안전성을 확보하기 위해 법/제도적으로 뿐만 아니라 정부부처가 지침서 등을 내놓고 이를 실천하기 위한 노력을 하고 있다. 미국의 전자인증은 평판 또는 명성의 손상, 재정적 손실, 공공이익 피해, 개인의 안전, 범죄 가능성, 민감한 정보 유출을 고려해 크게 4단계로 구분하였다. 인증 시 4단계의 인증수단으로 1~3단계의 온라인 거래가 가능하고 한사람이 여러 개의 인증 수단을 가질 수 있다. 또한 한번의 인증으로 전자정부의 모든 서비스를 제공할 수 있도록 게이트웨이를 만드는 사업을 진행 중에 있다. 그러나 한번의 인증으로 모든 서비스를 이용하는 것은 현실적으로 불가능하여 한번의 인증으로 최대한 많은 서비스를 이용할 수 있도록 변경하였다. 법/제도적 측면에서 미국은 정보보호 정책을 추진하는데 정보보호 프로그램에 대한 관리 측면과 허가 받은 사람만이 자료를 검색, 수정, 삭제할 수 있는 접근 통제가 가장 취약함을 인식하고 이에 대해 법/제도적 측면에서 강화시키고 있다[22].

일본은 전자정부 구축과 동시에 안전성 및 신뢰성의 확보를 위해서 "정보 보안에 관한 자격 제도의 정비", "개인정보보호 관련 법안" 이 국회에 제출되었다. 또한 2006년까지 정보보안, 행정, 국민 생활 등 사회 전반적인 분야에서 IT 전자화를 집중적으로 추진할 계획을 가지고 있으며 5만명 이상의 개인정보를 가진 기관 및 기업이 인터넷을 통해 이를 다루는 경우 의무적으로 외부 침입과 데이터 보호를 위한 대책을 세워야 하는 개인 정보보호 관련법 등을 통해 앞으로 구축될 일본의 전자정부 프로젝트의 보안의 중요성을 알 수 있다[22].

2.2 국내 전자정부 동향

우리나라의 전자정부 추진경과를 살펴보면, 1987년부터 1992년까지 주요 업무를 위주로 전산화를 목적으로 주민/부동산/자동차 등 행정 데이터베이스를 구축하였다. 1993년부터 2000년까지 정보화 확대 및 일부 연계를 위하여 조달, 특허, 국세, 관세 등을 정보화하였고 여권발급, 부동산투기방지시스템 등을 연계하였다.

2001년부터 2002년까지 전자정부 기반 구축을 위하여 G4C (Government for Citizen), 전자조달, 인터넷국세서비스, 국가재정정보 등의 범정부 차원의 핵심기반 정보화 11대 사업을 추진하였으며 이를 성공적으로 완료하였다[26].

2003년은 전자정부 11대 과제를 고도화 및 신규 과제 발굴을 목표로 진행되었으며 이를 반영하여 2004년에는 국민참여와 정부 혁신을 촉진하는 전자정부의 구현과 전자정부 서비스 이용의 비활성화와 체감 효과 부족 문제를 해결하기 위해 "정부 혁신과 전자정부"라는 이름으로 4개 분야, 10개 아젠다, 31대 과제를 선정하여 전자정부 로드맵을 완성하였다[29]. 31대 과제는 정보보호 체계 구축 과제를 포함하여 범정부 통합전산환경 구축 등 서비스 고도화를 위한 체제 및 관리 혁신에 중점을 두고 있다.

현재까지 국내의 전자정부 서비스에 대한 보안은 전자정부 포털에 접속 시 전송 계층 수준의 정보보안을 위해서 보안 인증서를 배포하고 있으며 정보 기술 표준화의 일환으로 정보시스템 구축 운영기술 가이드라인을 발표하여 전자정부 구현 시 권고 및 추천하는 웹 서비스 보안 기술을 간략히 명시하고 있다[28].

지금까지 선진 4개국 전자정부 구축 동향에 대해서 살펴보았다. 상기 기술한 바와 같이 영국을 제외한 미국, 일본, 우리나라는 전자정부 보안에 대한 연구가 미진한 실정이다.

3. 웹 서비스 보안 표준화 동향

이번 장에서는 웹 서비스 보안 기술의 최근 동향을 살펴본다. 웹 서비스 보안 표준화는 공식 기구인 W3C, OASIS, WS-I 등과 IBM과 Microsoft를 중심으로 하는 기업체로 나누어 진행되고 있다. 공식 기구에서 진행되고 있는 보안 기술은 <표 1>과 같다[30, 31]. <표 1>의 보안 표준의 내용은 XML 문서의 암호화, 기밀성 등 XML 보안의 기본 구성 요소가 된다. 이러한, 문서에 대한 인증, 암호화와 같은 메시지 보안 및 안정적인 전달 등을 위한 규약에 관한 표준화가 대부분 완료된 현 시점에서 향후 웹 서비스 보안의 발전의 초점이 되는 부분은 웹 서비스 간의 연합, 정책관리, 신뢰관리, 권한 관리 등이다. 이것은 웹 서비스가 제공하는 저비용의 시스템 통합이란 특성에 기반한다[23].

〈표 1〉 웹 서비스 보안 표준

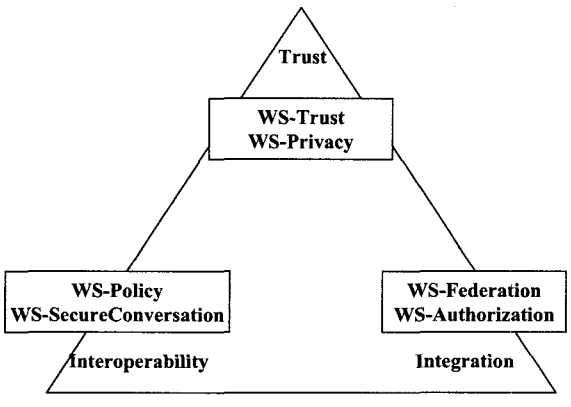
기구	현황	설명
W3C	XML Signature	XML 문법을 이용한 전자서명
	XML Encryption	XML 문서를 위해 특화된 암호화 기술
	XML Key Management	XML 문서의 서명을 검증하거나 암호화하는 공개키의 관리를 위한 프로토콜을 정의
OASIS	Security Assertion Markup Language (SAML)	엔티티에 대한 인증, 권한부여, 속성 등의 정보를 XML 형식을 통해 지정하는 방법에 관한 명세
	eXtendsible Access Control Markup Language (XACML)	접근 제어 정책 언어와 양측향 통신을 위한 요구/응답 언어 및 언어의 표현을 위한 XML 엘리먼트의 표준 집합을 정의
	Web Services Security	메시지 무결성, 메시지 기밀성, 단일 메시지 인증을 통한 보호의 질을 향상하기 위해 SOAP 메시지에 대한 강화
WS-I	Basic Security Profile	상호 동작성을 향상시키는 스펙 기술
	WS-I Security Scenarios	일반적인 보안 목표 또는 시나리오 상에서 특정 보안 요구의 선택을 알리는 특징

웹 서비스의 보안 관리를 위해서는 분산된 서비스 구조에 기반하여 보안기술이 설계되어야 한다. 현재 웹 서비스 보안은 통합된 보안 관리를 위한 기술 표준화로 발전하고 있다.

〈표 2〉 IBM의 웹 서비스 보안 표준

표준명	설명
Web services security protocol[1]	서비스에 필요한 다양한 등급의 보안 모델을 제안
WS-Policy Framework[16]	웹 서비스 정책을 설명하고 통신하는 범용 모델과 이에 상응하는 문법을 정의하여 서비스 소비자가 공급자가 제공한 서비스에 액세스 하여 필요한 정보를 발견
WS-Secure Conversation[6]	WS-Security와 WS-Policy 모델의 상위계층에 구현되어 서비스 간 안전한 통신을 책임
WS-Security Policy[4]	대형 Policy Framework 내부의 보안 정책 assertion을 설명하고 통신하는 모델과 문법을 정의
WS-Trust[17]	WS-Security의 안전한 메시지 교환 메커니즘을 사용하여 추가적인 프리미티브와 확장 및 보안 토큰의 교환 및 타당성 검사를 정의
WS-Federation[7]	이질적인 분산 환경에서 연합된 ID의 지원 등을 통해 신뢰 관계를 유지 및 해지하는 연합 인증 및 관리 메커니즘
WS-Authorization[7]	웹 서비스가 권한 데이터와 권한 정책을 관리하는 방법에 대해 정의
WS-Privacy[7]	조직이 프라이버시 정책을 명세하고 이를 서비스 요청자에게 전달할 수 있는 체계를 제공

(그림 4)는 IBM에서 현재 표준화 진행 중인 신뢰, 통합, 상호운영을 위한 WS-Security 기술을 표현한다. <표 2>의 IBM 기구의 표준은 XML Encryption, XML Signature 등의 기술을 구성요소로 사용한 웹 서비스 간의 통신 보안 표준을 포함하여, 웹 서비스의 통합관리, 정책의 규정 및 협약을 위한 표준들로 구성되어 있다.



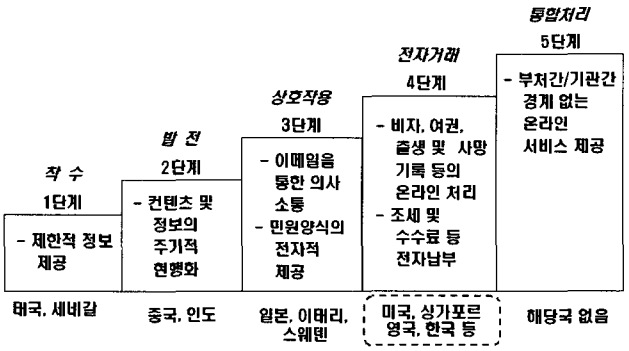
(그림 4) 신뢰, 통합, 상호운영의 WS-Security 삼각형[7]

4. 전자정부 서비스에서 웹 서비스 보안

이번 장에서는 웹 서비스 기반의 전자정부 서비스 보안 적용 시나리오를 기술하기 위해 먼저 전자정부 서비스의 발전 단계를 살펴보고 이를 기반으로 전자정부 서비스의 보안 발전 단계를 나누었다. 이렇게 나누어진 각 단계별 보안 요구 사항과 각 단계에 적용되는 웹 서비스 보안 기술을 분석한다.

4.1 보안 요구 사항

전자정부 서비스의 발전 단계는 (그림 5)에서 보는 바와 같이 크게 5단계로 구분하고 있다[18].



(그림 5) 전자정부 발전 단계[18]

(그림 5)에서 기술한 전자정부 발전 단계는 전자정부 서비스 측면의 발전 단계이다. 전자정부 발전단계를 전자정부 서비스의 서비스 구조(Framework)[24, 32]에 기반하여 보안 측면에서 3단계로 재분류할 수 있으며 각 단계의 보안 요구사항을 <표 3>과 같이 정리할 수 있다[19].

1단계의 경우는 전자정부 서비스의 컨텐츠가 제공되는 범위가 매우 제한적이고 정적인 특성을 가지며, 이메일이 주 의사소통 수단으로 이용된다. 부처 및 기관에서 생성되는 데이터에 대한 무결성과 기밀성이 요구된다[25].

인증 : 1단계의 부처 내의 발생 규모로 한정하며, 정부 직원과 응용 프로그램 또는 데이터베이스에 대한 인증으로 볼 수 있다. 전통적 인증 메커니즘을 사용하거나 부처 내 계정관리가 이루어질 수 있다.

기밀성/무결성 : 부처 내에서 생성되는 문서 및 데이터에 대해 부처 외부에 전송될 경우에도 기밀성과 무결성의 특성을 가질 수 있는 처리능력이 존재해야 한다.

〈표 3〉 전자정부 서비스의 보안 요구 사항

웹 서비스 보안을 고려한 전자정부 발전 단계	전자정부 발전 단계	보안 요구 사항
1단계	착수/발전/상호작용 단계	인증, 기밀성, 무결성
2단계	전자거래 단계	1단계 보안 요구 사항 + 단일사용자 인증, 부인방지, 전역적 접근제어, 키 관리
3단계	통합처리 단계	2단계 보안 요구 사항 + 국지적 접근제어, 신뢰관리, 인가관리, 정책관리, 연합, XML 기반의 모니터링/감사

2단계는 전자거래가 가능한 단계로써 사용자와 정부 사이에 전자정부 서비스를 통해 조세 및 수수료 납부 등 온라인 전자거래가 발생하는 단계를 말한다. 2단계는 기본적으로 1단계의 보안 요구 사항을 모두 만족해야한다. 전자거래 단계에서는 개인 및 정부의 재정적 손실을 입힐 수 있다는 측면에서 1단계보다 더 많은 보안 요구 사항이 발생하며 일반적으로 전자상거래에서 발생하는 보안 요구 사항과 일치한다. 전자상거래의 보안 요구 사항에는 인증, 무결성, 부인방지, 접근제어, 각종 거래 정보의 기밀성을 보장해야 한다. 그러나 전자정부 서비스에서 추가적으로 요구되는 보안 기술은 단일사용자인증 기술이 있는데 이는 전자거래 시 다양한 웹 서비스를 통해 전자거래가 이루어지는 경우가 있기 때문이다.

단일사용자인증 : 다양한 전자정부 서비스를 편리하게 이용하기 위해 한번의 인증으로 다양한 서비스를 이용할 수 있는 단일사용자인증 기술이 요구된다. 단일사용자인증 기술은 SAML로 구현이 가능하다.

부인방지 : 전자거래 시 필수적으로 부인 방지에 대한 요구 사항이 발생한다. 지불된 세금이나 수수료에 대해서 부인으로 인한 사용자 손실 등의 경우를 방지하기 위해 부인방지 기술이 요구된다.

접근제어 : 웹 서비스 기반의 전자정부 서비스에 대한 접근 제어는 기존의 보안 장비에 한계가 존재하기 때문에 전자정부 서비스를 위한 통합전산환경을 고려하여 단일지점에서의 접근 제어가 요구되며 이 때 XML 컨텐츠 기반의 접근제어 기법이 요구된다.

키관리 : 전자거래단계에서 암호화와 서명은 필수적인데 이와 동시에 키관리가 필요하다. 키관리는 암호화와 관련된 응용 프로그램의 신뢰성 부여를 위해 필요하다. 키관리 기술은 서명을 검증하거나 공개키 사용자에게 키의 위치를 알려주는 역할을 수행한다.

3단계는 통합처리 단계로써 정부 내 부처 및 기관 간, 외부 연계 시스템과의 통합 처리가 가능한 단계를 말한다[20]. 이 단계에서는 분산된 서비스의 통합을 위한 과정에서 보안 요구 사항이 발생하며 기본적으로 2단계의 요구 사항을 모두 만족해야한다. 또한 국지적 접근제어, 신뢰관리, 정책관리, 표준화된 보안 메커니즘, 권한 관리, 프라이버시 보장, 이기종 간의 보안 연합의 보안 요구 사항이 발생한다[21].

접근제어 : 2단계에서 이루어지는 접근제어가 통합전산환경기반의 게이트웨이에서 접근제어임에 비해 3단계에서 접근제어는 각 부처 및 기관에 속한 국지적 접근제어를 뜻한다. 국지적인 접근제어는 각 부처가 XACML, 사설 UDDI를 이용하거나 WS-Addressing 기술을 이용하여 가능하다.

신뢰관리 : 신뢰관리는 각 부처/기관, 기업 등에게 투명한 서비스 제공을 위해 필수적이다. 신뢰관리는 각 부처/기관 간의 보안 토큰의 발행, 갱신, 검증 등 신뢰관계를 검증하기 위한 방법들을 제공한다.

연합 : 연합은 인증을 위해 서로 다른 토큰 방식을 사용하는 기관 간의 통신을 위한 인증 방식의 협약을 위해 사용된다. 조직 간의 연합을 위해서는 먼저 조직의 정책 및 신뢰관계가 정의되어야 하며 이 정책을 안전하게 통신할 수 있는 메커니즘이 보장되어야한다.

정책관리 : 각 부처/기관은 서로 다른 보안 정책을 정의하는데 서로 다른 정책 도메인 간의 정책을 서로 공유할 수 있는 방법을 제공한다.

인가관리 : 전자정부 서비스는 인증을 통해 적절한 권한을 인가받은 후에 제공받을 수 있는데 서로 다른 보안 도메인을 갖는 환경에서는 도메인 간의 인가정보를 관리할 수 있는 메커니즘이 필요하다.

프라이버시 : 서비스 요청자의 개인 정보가 외부에 노출되지 않음을 보장하는 서비스 제공자의 능력과 서비스 요청자의 프라이버시 요구사항에 대한 상호의 정보 교환이 필요하다.

모니터링/감사 : 기존의 모니터링/감사 도구는 웹 서비스 기반의 환경에서는 한계가 있으며 XML의 특성을 고려한 모니터링 방법이 요구된다. 감사는 사용자가 어떠한 행동을 했는지에 대한 기록을 남겨두는 기술로 전자정부 서비스에서 사용자가 법적으로 어긋난 행동을 했을 경우 처벌을 위한 데이터를 제공할 수도 있으며 시스템에 문제가 생겼을 경우 이를 분석하기 위한 데이터를 제공한다.

4.2 웹 서비스 보안 기술 분석

4.1에서 기술한 정자정부 서비스의 단계 별 보안 요구 사항을 웹 서비스 보안 기술과 매핑하면 <표 4>와 같이 요약할 수 있다.

인증/단일사용자인증 : 1단계의 인증은 전자정부 구축 초기단계로 부처 내 인증방식에 의존한다. 2단계와 3단계에서는 다양한 웹 서비스 기술을 편리하게 사용하고 사용자에게 투명성을 제공하기 위해 단일사용자인증 기술이 요구된다. 단일사용자인증 기술은 SAML로 구현이 가능하고 크게 Pull, Push 모델로 나뉜다. Pull 모델은 인증을 담당하는 사이트가 서비스를 제공받고자하는 사이트로 증명(assertion)을 보내주어 인증을 하는 방법이고, Push 모델은 사용자가 인증을 담당하는 사이트로부터 증명을 받은 후 이를 서비스를 제공받고자 하는 사이트로 직접 전달하여 인증을 받는 방법이다. 기술한 인증 방법은 보안 측면에서 장단점이 존재하며 이를 전자정부 서비스에 적용할 때 장단점을 고려하여 적용해야한다.

기밀성/무결성 : 기밀성과 무결성을 보장하는 기술은 XML 암호화, XML 전자서명으로 보장할 수 있다.

접근제어 : 접근제어는 웹 서비스 기반의 접근제어가 요구된다. 예를 들어 기존의 방화벽과 같은 접근제어 장비들은 위치 기반의 접근제어를 수행하므로 80번 포트를 이용하는 웹 서비스는 무용지물이다[2]. 2단계에서 접근제어는 통합전산환경을 고려한 게이트웨이에서의 접근제어를 말한다. 그러나 3단계의 경우 보안 레벨을 높이기 위한 각 부처/기관에서의 접근

제어를 의미하며 이는 정부 내부 XACML 메커니즘, 사설 UDDI 등으로 가능하다. 사설 UDDI는 서비스에 대한 검색, 등록 등을 제한함으로써 접근제어가 가능하다. 또한 접근제어가 가능한 웹 서비스 기술로는 WS-Addressing이 있는데 이 기술은 라우팅 경로를 지정하여 접근제어가 가능하다.

〈표 4〉 전자정부 발전 단계별 웹 서비스 보안 기술

전자정부 보안 발전단계	웹 서비스 보안 기술
1단계 (착수/발전/상호작용)	- XML Encryption - XML Signature
2단계	- XML Encryption - XML Signature - XACML - XKMS - SAML
3단계	- XML Encryption - XML Signature - XACML - XKMS - SAML - WS-Trust - WS-Federation - WS-Security - WS-Authorization - WS-Privacy - WS-Addressing - WS-Policy - WS-Manageability

부인방지 : 전자상거래 단계에서 필수적으로 요구되는 보안 기술은 2단계에서의 보안 요구 사항과 일치한다. 따라서 부인방지는 2단계와 3단계에서 필수적인 기술이다. 부인방지 기술은 XML 전자서명 기술로 보장할 수 있다.

키관리 : 키관리 기술은 XKMS 기술로 구현이 가능하다. XKMS는 X-KISS와 X-KRSS 두 영역으로 나눌 수 있다. X-KISS는 주어진 식별자 정보에 필요한 공개키의 위치를 부여하고 유효성을 검사한다. X-KRSS는 키의 재발행, 폐기, 복구와 같은 키관리를 위한 프로토콜을 정의하고 있다.

정책관리 : 대규모 분산환경에서 정책관리 기술은 필수적으로 요구된다. 또한 정책 관리 기술은 다른 웹 서비스 보안 기술을 위한 기반을 제공한다. 정책 관리는 WS-Policy 기술로 구현이 가능한데 WS-Policy는 송수신자 간의 보안 요구사항과 프라이버시, 인코딩 포맷, 지원 알고리즘 등 기본 서비스 속성들을 명시하는 보안 정책 사항과 제약을 표현하기 위한 방법을 정의한다.

신뢰관리 : 신뢰 관리는 보안 토큰의 발행, 갱신, 검증을 위한 방법과 신뢰 관계를 성립, 평가, 연계하기 위한 방법을 제공한다. 신뢰 모델은 토큰을 저장하고 서비스에 제공하는 보안 토큰 서비스(Security Token Service) 시스템의 적용 방식에 따라 크게 3가지를 고려할 수 있는데 고정된 신뢰 루트를 사용하는 방법, 신뢰 계층을 사용하는 방법, 인증 서비스를 사용하는 방법이 있다. 고정된 신뢰 루트들을 사용하는 방법은 가장 간단한 방법으로 단일 신뢰 루트를 두는 것보다 부하 분산의 효과를 기대할 수 있다. 신뢰 계층을 사용하는 방법은 고정된 신뢰루트들을 둠으로써 얻을 수 있는 부하 분산의 효과보다 더 큰 효과를 기대할 수 있지만 신뢰 계층에 대한 설계가 미리 정확하게 선행되어야만 한다. 인증 서비스를 사용하는 방법은 별도로 신뢰 루트는 구성하지 않고 기존의 인증 서비스가 신뢰 관리를 대행하도록 하는 방법으로 기존 인프라를 이용할 수 있는 이점이 있다.

인가관리 : 인가관리 기술은 분산 컴퓨팅 환경에서 통합처리를 위해 필수적이다. 인가관리 기술은 WS-Authorization 기술로 구현이 가능하다. WS-Authorization은 웹 서비스가 권한 데이터와 권한 정책을 관리하는 방법에 대해서 정의한다.

프라이버시 : 프라이버시를 위한 웹 서비스 보안 기술은 WS-Privacy로, 프라이버시를 위해 통신의 양 노드의 상대에 대한 요구사항을 교환하는 모델을 정의한다. 이를 구현하기 전에 조직의 정책 및 신뢰관계 및 메커니즘이 요구된다. 이는 WS-Policy, WS-Trust, WS-Security를 통해 구현될 수 있다.

연합 : 연합은 WS-Federation으로 구현되고, 연합을 위해 선행되어야 하는 웹 서비스 보안 기술은 WS-Policy, WS-Trust, WS-SecureConversation 기술이 있다.

모니터링/감사 : 모니터링은 WS-Manageability 기술로 구현이 가능하며 감사는 XML 기반의 새로운 감사 방법이 요구된다.

전자정부 서비스는 통합을 고려한 웹 서비스 기반으로 구축되고 있을 뿐만 아니라 기존의 보안 장비로는 웹 서비스에 대한 보안에 한계가 발생한다[2, 27]. 따라서 전자정부 서비스 보안을 고려할 때 웹 서비스 보안 기술을 고려해야한다. 그러나 웹 서비스 보안 기술은 아직 표준화되지 않은 많은 분야가 존재하기 때문에 웹 서비스 기반의 여러 가지 새로운 보안 솔루션을 적용 시 확장성 측면에서 새롭게 적용될 기술과 기존에 구축되어 있는 기술들을 고려하여 적용되어야할 것이다.

5. 전자정부 서비스에서 보안 적용 시나리오

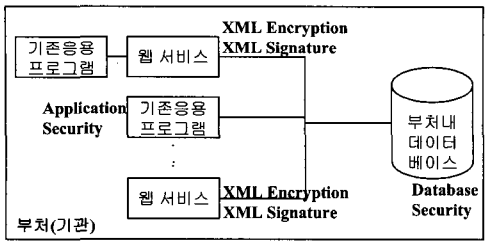
이번 장에서는 4장에서 기술한 내용과 전자정부 발전 단계별 특징을 고려하여 보안 적용 시나리오를 기술하고 최종적으로 통합전산환경에서 통합처리단계로 발전하기 위한 웹 서비스 보안에 대한 내용을 기술한다.

웹 서비스 환경의 보안을 위해서는 신뢰, 상호연동, 통합 등이 모두 함께 만족되어야 한다. 표준들은 신뢰, 상호연동 등 위에 언급된 보안 요구사항들을 위해 요구되는 많은 기술적 명세들로 구성되며, 각각이 웹 서비스 보안 구조의 기초 구성요소이므로 웹 서비스를 도입하는 한 조직에서 보안성을 위해서는 위 보안 기술들의 적용이 대부분 공통적으로 요구된다.

전자정부 각 발전 단계의 보안 요구사항은 앞 단계의 보안 요구사항을 포괄한다. 전자정부 3단계 중 현재 완성단계에 있는 1,2 단계에서 적용된 보안 사항들에 대해 간략히 기술하고 앞으로 부처 간 통합을 위한 3단계의 보안 적용 방안에 대해 기술한다. 마지막으로 실질적인 전자정부 개발 환경이 될 통합전산환경에서의 적용 구조를 기술한다.

5.1 1 단계 보안 적용

부처 내부 통합을 위한 1단계 보안 적용 시나리오는 문서, 데이터베이스, 서비스와 같은 자원에 대한 전자화 및 보호 기술이다. 각 부처는 데이터 베이스 등 부처 내 전자데이터에 대한 응용 보안기술과 부처 외부로 전송될 데이터에 대한 웹 서



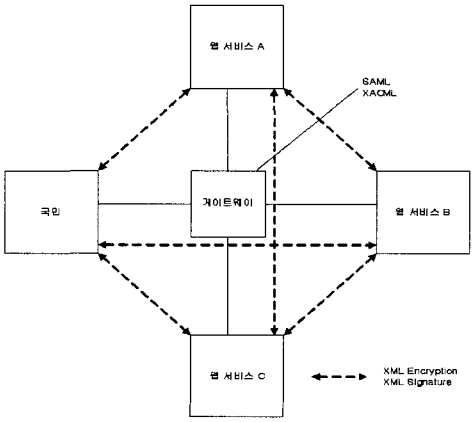
(그림 6) 부처 자원들에 요구되는 보안 기능

비스 기술을 활용하여 기밀성 및 무결성을 보장해야 한다. (그림 6)은 부처 내 자원들의 보안 기능을 나타낸다.

웹 서비스 기술 측면에서 1단계에서는 각 부처별로 해당 기밀성 및 무결성 보장에 대한 기술을 적용해야하며 이는 XML Encryption이나 XML Signature를 사용하여 보장할 수 있다. 국민과 웹 서비스 간 또는 각 웹 서비스 간의 경우도 역시 기밀성과 무결성을 보장할 수 있다. 그러나 XML Signature가 제공하는 부인방지는 1단계에서 필수적으로 요구되지는 않는다. 즉 전자정부 서비스의 모든 구성요소는 기밀성과 무결성 보장을 위해 XML Encryption과 XML Signature 기술을 적용해야만 한다. 1단계의 인증은 부처 내부 직원과 응용프로그램 또는 데이터베이스 간, 응용 프로그램과 데이터베이스 간과 같이 부처 내 자원 간에 발생한다. 이를 위해 응용 프로그램에서 제공하는 기본 인증메커니즘 또는 부처 기관 내부 계정 등이 사용될 수 있다.

5.2 2 단계 보안 적용

2단계에서는 전자거래가 이루어지기 때문에 1단계에서와는 달리 요청자에게 금전적인 손실 등의 피해가 발생할 수 있다. 따라서 이에 대한 보안 요구 사항이 발생한다. 전자거래단계의 보안 요구 사항은 일반적으로 전자상거래에서의 보안 요구사항과 일치하지만 기존의 전자상거래의 보안 요구사항과 구별되는 점은 다양한 서비스를 제공하기 때문에 단일사용자인증 기술이 요구된다. 즉 국민/기업과 정부간의 보안 요구사항으로는 단일사용자인증 기술, 부인방지, 접근제어, 키관리 등이 포함된다.



(그림 7) 국민/기업에서 기밀성/무결성/접근제어 /단일사용자인증 기술 적용 범위

(그림 7)은 국민과 기업이 웹 서비스 보안 기술 중 기밀성, 무결성, 접근제어, 단일사용자인증 기술이 적용되는 범위이다. 각각의 보안 메커니즘의 자세한 적용 방법은 다음과 같다.

5.2.1 기밀성/무결성

기밀성, 무결성의 특성은 1단계의 부처내부에서의 XML Encryption, XML signature 등의 기술을 통해 만족되게 된다. 2 단계에서 정부와 국민/기업 간 송수신되는 정보의 기밀성, 무결성의 특성을 위해 위 기술들은 WS-Security 또는 WS-SecureConversation과 같은 통신채널을 보호하는 기술의 구성요소로 포함되어 사용된다.

5.2.2 단일사용자인증

각 서비스로 연결된 단일입구인 게이트웨이에 SAML의 토큰 발급 시스템(asserting party)을 구현하여, 게이트웨이를 통해 국민을 인증하고 인증결과를 서비스와 연계함으로써 단일사용자인증이 가능하다. 단일사용자인증의 방법은 그 특징에 따라 서비스 별로 다르게 적용되어야 한다.

• 부처 간 서비스를 위한 적용 시나리오

각 부처 간의 서비스를 하는 통신 채널은 안전하다는 가정하에 Push 방식의 적용이 가능하다. 사용자는 인증 정보인 증명을 서비스로 직접 전송하여 토큰 발급 시스템의 부하를 감소시킨다.

• 국민/기업 간 서비스를 위한 적용 시나리오

정부와 기업/국민 간의 서비스를 하는 통신 채널이 반드시 안전하다는 가정을 할 수 없으므로 Pull 방식의 적용이 가능하다. 사용자의 인증 정보인 증명을 직접적으로 전송하지 않고 증명참조(artifact)를 통한 간접적인 전송 방식을 사용한다. Pull 방식은 두 가지 시나리오가 있을 수 있다.

- Local-Site-First Scenario : 사용자가 정부 게이트웨이로부터 인증을 받고 증명에 대한 증명참조를 획득하여 원하는 서비스에 접속한다.
- Destination-Site-First Scenario : 사용자가 원하는 서비스에 우선 접속한 후 인증을 위해서 정부 게이트웨이로의 리다이렉션을 통해 인증을 받은 뒤 원하는 서비스로 다시 리다이렉션한다.

5.2.3 접근제어

2단계에서의 접근제어는 전자정부 게이트웨이에서 이루어지는 국민/기업에 대한 인증과 인가를 의미한다. 게이트웨이에서 국민/기업은 인증서 또는 패스워드 등 사용자 고유정보를 사용하여 인증한다. 사용자는 인증이 성공하면, 인증성공 및 권한을 증명하는 토큰을 부여받는다. 이 토큰은 전자정부 내부에 존재하는 서비스 이용 시 국민/기업이 권한소유를 증명하기 위해 사용된다.

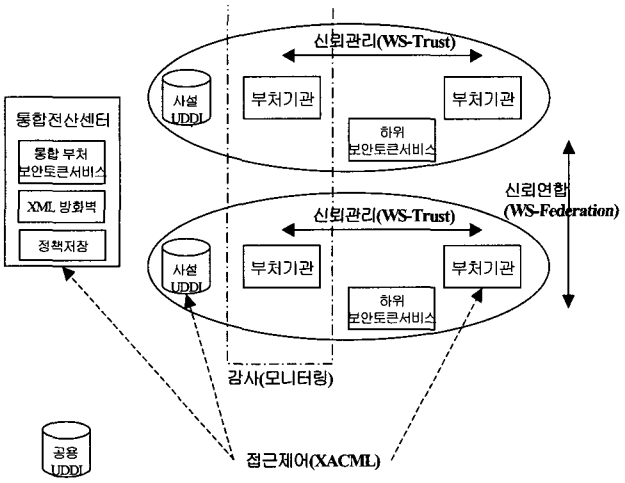
5.2.4 부인방지

정부와 국민/기업 간 XML signature를 포함하여 양측이 자

신이 제공한 정보에 대해 부인하는 행위를 방지할 수 있다. 상대의 XML signature를 필요로 하는 측은 WS-Policy를 이용한 자신의 정책명세 중에 XML signature 요구를 포함하고, 상대와의 통신 교환과정에서 WS-Privacy 표준을 이용하여 XML signature에 대한 요구사항을 상대가 따르도록 한다.

5.3 3단계 보안 적용

3단계에서는 정부부처 및 기관 간의 연계 및 통합을 위한 보안 요구사항을 웹 서비스 보안 기술과 XML을 사용하여 적용하는 방안을 기술한다. 3단계의 보안 요구사항은 접근제어, 신뢰관리 및 연합, 정책관리, 모니터링 등이다.

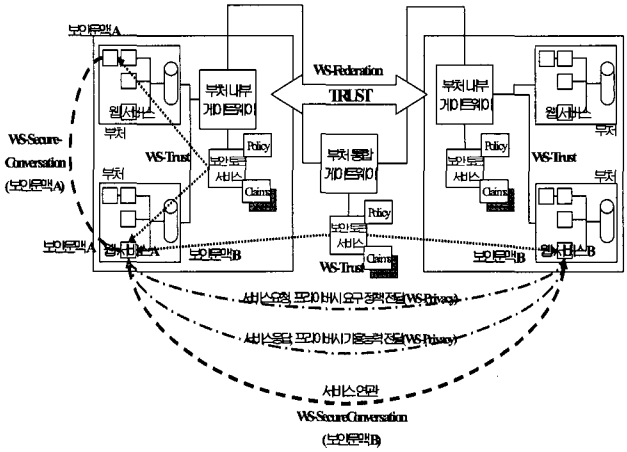


(그림 8) 부처 간 보안 기능의 적용 범위

(그림 8)은 3단계의 대표적 보안 기능들의 적용 범위를 표현하였다. 신뢰관리는 동일한 보안 토큰 서비스 시스템이 발급한 토큰으로 접근 가능한 부처기관으로 구성된 범위 내에서 발생하며, 하위 보안 토큰 서비스는 전산센터의 통합 부처 보안 토큰 서비스의 하위 계층으로 존재한다. 상이한 토큰방식을 사용하는 보안 토큰 서비스 간은 신뢰 연합을 통해 상호의 토큰을 수용할 수 있도록 한다. 감사는 한 개 전자정부 서비스를 이루는 개별 웹 서비스를 제공하는 여러 부처들로부터의 기록을 수집하여 이루어진다. 접근제어는 일차적으로 게이트웨이 역할을 하는 전산센터에서, 후에 부처내부의 접근제어 메커니즘에서 이루어진다. 각각의 보안 메커니즘의 자세한 적용 방법은 다음과 같다.

5.3.1 신뢰 관리 및 연합

신뢰 관리 구조 중 인증 시스템을 사용하여 기존 인프라의 활용효과를 갖는 장점을 전자정부 게이트웨이에 적용할 수 있다. 또한 높은 보안성을 제공하기 위해 다단계 인증 메커니즘을 도입할 수 있는데, 이에 따라 인증을 수행하고 사용자 토큰 정보를 저장하는 게이트웨이가 계층적으로 구성될 수 있다. 이를 위해, 신뢰관리 구조 중 신뢰 계층을 사용하는 방법을 함께 적용한다. 즉, 기존 인증시스템을 사용하는 구조와 신뢰계층 구조를 혼합 적용한다. (그림 9)는 계층적인 게이트웨이에 보안 토큰 서비스 시스템을 둔 것으로 부하 분산의 이점과 함께 이미 존재하는 통합 부처 게이트웨이와 부처 내부 게이트웨이 인프라를 활용할 수 있는 이점이 있다. 예를 들어, 한 사용자가 2단계의 인증을 거쳐 한 서비스를 이용해야 할 경우, 해당 서비스는 사용자의 요청 메시지를 수신한 후, 2개 보안 토큰 서비스 시스템에 각각 사용자 인증을 증명하는 보안 토큰을 요청한다.



(그림 9) 계층적인 게이트웨이에 보안 토큰 서비스 시스템을 두는 방식

전자정부 서비스는 여러 부처의 개별 웹 서비스들이 결합되어 구성되므로 (그림 9)에서 한쪽 부처의 웹 서비스 A와 또 다른 부처의 웹 서비스 B로 구성된 전자정부 서비스가 존재할 것이다. 이 경우, 사용자가 개별 웹 서비스가 소속된 보안 토큰 서비스의 인증 메커니즘에 모두 인증하지 않도록 하기 위해, 한쪽 부처의 보안 토큰 시스템에서 발급 받은 보안토큰이 다른 부처에서도 수용될 수 있도록 부처 간 신뢰정보에 대한 사전 연계가 이루어져야 할 것이다. 그림에서 양 정부 내부 게이트웨이의 각 보안 토큰 서비스 시스템은 토큰과 같은 신뢰정보를 서로 연합할 수 있도록 사전 협약되어야 하며, 이 협약을 바탕으로 한쪽 보안 토큰 서비스 시스템의 토큰을 통해 다른 시스템의 토큰을 얻는 교환 과정은 WS-Federation 표준에 따라 동작해야 한다.

5.3.2 접근 제어

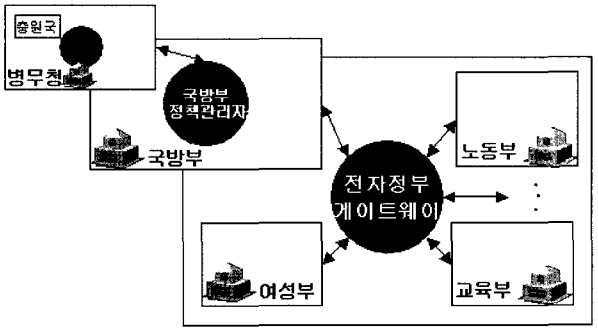
접근제어를 위해서는 우선 신뢰 관리 구조가 기반되어야 한다. 접근의 허용 여부를 결정할 정책의 저장 및 접근 요청의 허용 및 여부를 결정하는 기능요소를 위한 XML 표준으로는 XACML이 정의되었다. XACML을 활용한 접근제어 메커니즘을 구현하기 위해서는 전자정부 환경의 접근제어 동작방식이 반영되어 결정된 접근제어 모델을 기반으로 XACML의 접근제어 정책을 표현해야 한다. 전자정부 조직 내에서 동일한 접근 체계를 갖는, 즉 동일한 접근 제어 모델로 표현되는 환경에 포함된 XACML PDP(Policy Decision Point)에 저장되는 XACML 태그(tag)는 동일한 관계구조로 표현될 수 있다. 따라서 이를 스키마로 작성하여 공통적으로 사용하도록 하면, 조직

에 발생한 접근체계의 변경 시 이의 반영이 용이하고, XACML PDP와 연관되어 동작하는 타 모듈에 대한 자동화된 인터페이스를 제공하는 것이 가능하다.

5.3.3 정책 관리

공통의 정책을 중앙 저장소에 저장하여 관리상의 이점을 얻을 수 있다. 전자정부 환경에서 정책을 중앙 저장해 두는 목적으로 가장 적절한 시스템은 범정부 통합전산센터이다. 정책의 무결성 및 가용성을 보장해야 하는 측면에서, 보안성이 높은 통합전산센터는 요구사항을 만족한다. 접근제어, 정책, 감사 등의 각종 정책을 적용 범위에 따라 WS-Policy를 이용하여 기술한 후 식별자를 부과하여 전산센터에 저장한 후, 기관 및 시스템에서 능동적으로 접근해서 사용할 수 있도록 한다.

(그림 10)은 전자정부 조직에서 계층적인 정책 관리를 나타낸다. 이와 같은 구조에서 정책의 통합 관리를 위해서는 다음과 같은 내용이 명세되어야 한다.



(그림 10) 전자정부 조직에서의 정책 계층 구조

• 정책의 표준화된 기술 언어

정책이 기관 간 상호 이해, 결합될 수 있는 공통된 문법 체계를 가져야 한다. 웹 서비스에서는 공통된 언어인 XML이 존재하고, 이를 활용한 정책 스키마를 구성할 수 있으나, 이미 정책을 기술하기 위한 공통된 스키마가 표준화 되어 있다. WS-Policy 표준을 활용하여 정책을 기술한다.

• 정책의 관리 구조

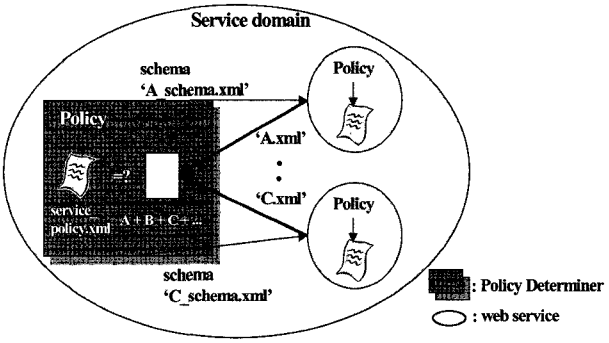
전자정부 환경에서 중앙의 정책저장소의 역할은 범정부 통합전산센터가 담당하는 것이 적절하다. 정책의 무결성 및 가용성을 보장해야 하는 측면에서, 보안성이 높은 통합전산센터는 요구사항을 만족한다. 접근제어, 정책, 감사 등의 각종 정책을 적용 범위에 따라 WS-Policy를 이용하여 기술한 후 식별자를 부과하여 전산센터에 저장한 후, 기관 및 시스템에서 능동적으로 접근해서 사용할 수 있도록 한다.

• 정책의 분배 방법

정책의 영향을 받는 대상은 조직 내 구성원, 조직에 서비스를 요청하는 외부 사용자로 구성된다. 예로, 서비스 요청자 A가 기관 B의 웹 서비스에 서비스 요청을 보냈을 때, 웹 서비스가 A에게 전달해야 하는 정책은 조직 내에 적용되는 동일한 정책을 저장하는 중앙관리센터로부터 획득한다. 이 경우에 정책이 전달되는 방식은 Pull, Push 의 두 가지가 존재할 수 있다. 웹 서비스가 중앙관리센터에서 정책을 획득하여 요청자에게 전달하는 방법, 중앙관리센터로부터 요청자에게 정책을 전달하도록 요청하는 방법의 두 가지가 그 예이다.

5.3.4 감사

웹을 기반으로 하는 전자정부 서비스는 일반적으로 여러 부처, 개별기관의 웹 서비스 컴포넌트가 결합되어 구성된다. 별도의 기관 또는 시스템에 의해 서로 다른 정책과 보안 모델로 관리되는 웹 서비스에서 자체적인 접근제어가 이루어지고 있다 하더라도, 개별 웹 서비스의 접근제어 처리내용이 한 개 전자정부 서비스에 대한 정책에 합당하게 이루어지고 있는지를 확인할 수는 없다. 또한 웹 서비스 컴포넌트의 관리자 오류로 인한 정책 위반 또한 발생할 수 있다. 현재 전자정부는 기관 내부의 보안 관리가 양호하지 못하고, 개발 및 테스트 시스템이 분리되지 않고 운영되는 등 내부자의 우발적 실수 및 악의적 보안사고의 발생 가능성이 높은 상황이다. 따라서 개별 웹 서비스에서 접근제어 내용이 전자정부 전체 정책에 부합하였는지를 확인하기 위해 개별의 접근 결과들을 한곳으로 수렴하여 모니터링하는 방법에 대해 기술한다.



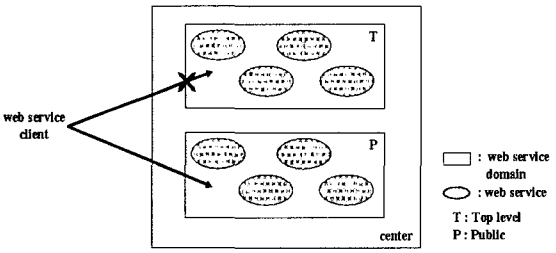
(그림 11) 접근제어 정책 검사시스템으로의 개별 웹 서비스 정책 설정 정보의 수렴

(그림 11)에서 개별 웹 서비스들은 한 개의 전자정부 서비스의 구성 요소이다. Policy Determiner는 전자정부 서비스에 관한 정책을 저장하고, 개별 웹 서비스에서 처리된 정책 내용을 수렴하여 전자정부 서비스와의 부합여부를 검사할 시스템이다. Policy Determiner의 관리자는 전자정부 서비스의 정책을 토대로, 개별 웹 서비스가 전달해야 하는 접근제어 결과항목의 요구사항을 정의한다. 다음으로, Policy Determiner는 개별 웹 서비스에게 포함할 항목에 대한 요구사항을 스키마로 표현한 후, 개별 웹 서비스로 분배한다. 개별 웹 서비스들은 전달받은 스키마 형식을 따라 자신의 정책정보를 문서화하고 Policy Determiner에게 반환한다. Policy Determiner에서 필요한 각 문서의 결합 규칙은 개별 웹 서비스에 전달한 스키마문서에 기반 하여 관리자가 생성한다. 따라서 이러한 결합과정의 결과는 대상 전자정부 서비스가 개별 웹 서비스를 통과하며 처리되는 접근통제 규칙 및 결과를 반영한다. 이의 결과를 대

상 전자정부 서비스의 정책을 표현한 'service_policy.xml'과 비교하여 적용 내용이 일치하는가를 검사할 수 있다. 사용자의 등급 유형을 나타내는 스키마 파일인 'A_schema.xml', 객체 등급 유형을 나타내는 스키마 파일인 'C_schema.xml'을 들면, 첫째 웹 서비스의 관리자는 웹 서비스 내 정책적용내용이 변경될 경우 A.xml 문서에 A_schema.xml 형식에 맞도록 정책 적용정보를 형식화하여 저장한다. 이는 관리자에 따라 자동화할 수도 있고, 수동적으로 제작할 수도 있다. Policy Determiner에서 필요한 각 문서의 결합규칙은 전자정부 서비스 정책이 변경되지 않는 한 수정될 필요가 없기 때문에 자동화가 가능하다.

5.3.5 XML 방화벽을 이용한 메시지 기반 필터링

전자정부 시스템에서 웹 서비스 기술을 이용한 메시지 기반의 접근 제어가 가능하다. 메시지 기반의 접근제어란 웹 서비스의 요청메시지에 서비스의 요청주체에 관한 역할, 등급, 환경 정보 등을 포함시키는 공통 화된 정보를 포함하도록 규약하는 것이다. XML을 사용하여 위 규약을 스키마로 선언하여 접근주체에 대한 필터링 항목으로 사용하면, 필터링 규칙의 변경이 용이하고, XML 계층의 정보를 기반으로 매우 세밀한 접근제어를 할 수 있다. XML 문서의 특정 태그 내용을 조사하는 기능을 갖는 XML 방화벽의 사용을 제안한다. XML 방화벽은 특정 보안 특성을 공유하는 웹 서비스 집합을 보호한다. 웹 서비스는 분산된 형태로 구성되나, 보안요구 수준이 높으며 특정 접근요청에 대해서는 모두 거부하는 특성을 공유하는 웹 서비스의 집합이 있을 수 있다.



(그림 12) 서로 다른 보안 도메인에서 사용자의 접근 허용 및 거부를 단위로 처리하는 경우

(그림 12)는 한 도메인에서 보안성이 높은 웹 서비스 그룹에 대한 접근이 집단적으로 필터링되는 것을 보이고 있다. 높은 보안이 요구되는 서비스(콘텐츠)의 관리작업과 같은 특정 등급 이상의 접근자만을 허용하는 요구사항을 가지는 상황에 XML 방화벽을 적용할 수 있다. 통합전산환경을 고려한 XML 방화벽의 적용은 다음과 같은 경우가 가능하다.

• 게이트웨이

범정부 통합전산센터는 전자정부의 적용범위 별로 적용되어야 하는 정책, 표준, 메타데이터에 관한 데이터베이스를 저장하고, 중요 서비스에 관한 참조를 가지고 서비스들을 연결해주는 중요 지점으로 동작한다. 통합전산센터 내에 저장되는 정보에 대한 엄격한 접근관리가 요구된다. 통합전산센터 내에는 일반국민이 접근할 수 없는 웹 서비스와 데이터베이스가 집중되어 있으므로, 이들에 대한 사용자 접근 제어 메커니즘을 개별 웹 서비스에 별도로 구현하는 것보다는, 이들에 대한 통합적인 접근을 관리하는 게이트웨이를 XML 방화벽을 통해 구현하는 것이 효과적이다.

• 전자정부 서비스 창구

현재 전자정부 단일창구는 전자정부 서비스 유형별로 별도로 운용되고 있다. 단일창구에서는 인증된 사용자에 대해 다른 웹 서비스에 대한 참조를 제공한다. 단일창구에서 인증을 마친 사용자는 일차적으로 타 웹 서비스를 이용할 수 있는 보안 토큰으로 사용할 수 있는 권한을 부여받는다. 이렇게 인증과 함께 부여된 권한에 의해 일차적으로 전자정부 서비스를 이용할 수 없는 사용자를 필터링한다.

• 정부 기관

정부기관 중 서비스 및 저장문서의 외부 개방 수준이 낮은 곳에 속하는 시스템에서 제공하는 웹 서비스들은 서비스 요청을 할 수 있는 접근 주체의 보안등급이 매우 한정될 수 있다.

상기 기술한 접근 점에 XML 방화벽 적용을 할 경우에는 다음과 같은 장점이 있을 수 있다.

• 웹 서비스의 보안 관리비용 감소

특정 웹 서비스 그룹에서 모두 거부되는 보안 등급에 속하는 요청자에 대한 접근제어 기능이 XML 방화벽에 집중된다. 또한 XML 방화벽의 필터링 규칙을 변경하면 개별 웹 서비스들에서 함께 동일한 접근제어 규칙 변경할 필요가 없다. 비용이 방화벽 한 곳에 집중되어 그룹 전체 측면의 비용 절감이 발생한다.

• 불필요한 메시지의 감소

XML 방화벽에서 다수 웹 서비스에 대한 요청 메시지의 진입을 차단함으로써 웹 서비스 그룹 내부에서의 불필요한 메시지가 감소된다. 다수의 개별 웹 서비스에의 접근시도 및 웹 서비스의 접근결정 메커니즘이 동작하는 것을 방지할 수 있다.

• 모니터링

방화벽에서 접근 요청 및 처리 결과(허용/거부)를 기록하여 해당 웹 서비스 그룹에 발생했던 접근에 관한 모니터링을 수행할 수 있다. 해당 웹 서비스 그룹에서 거부되는 접근 요청이 지속적으로 발생하거나 예상되지 않는 접근 유형의 발생을 감지하여 안정적인 서비스를 제공할 수 있다.

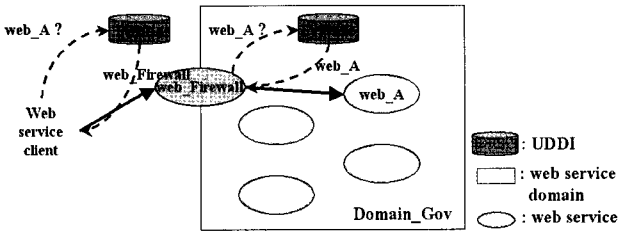
5.4 그 외 웹 서비스를 이용한 보안 기술적용

5.4.1 UDDI

사용자가 전자정부 서비스를 검색하고자 할 때 국가적으로

구축된 하나의 UDDI 레지스트리의 내용을 검색하고 서비스 등록할 것으로 예상된다. 그러나 보안상 매우 민감한 서비스의 또 다른 사설 UDDI를 사용하여 서비스에 대한 접근 제어를 가능하게 한다. UDDI의 활용 형태는 서비스의 등록과 검색의 허용 대상을 제한하는 범위에 따라 차별화 되며, 여기서는 두 가지 형태를 제안한다.

- 포털 UDDI : 부처의 외부인은 서비스 검색은 가능하지만 등록은 불가능하다.
- 파트너 카탈로그 UDDI : 방화벽 안 쪽에 위치하며 UDDI에 등록된 서비스는 외부인이 아닌 신뢰할 수 있는 정부부처에 의해서만 검색 및 등록이 가능하다.



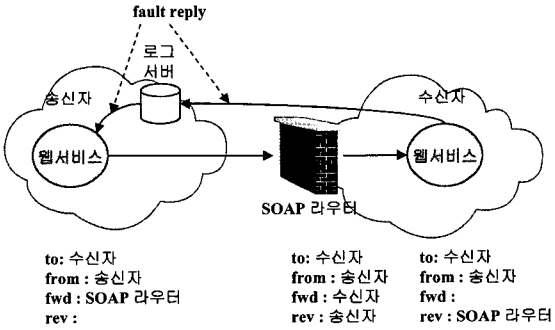
(그림 13) XML 방화벽과 UDDI의 응용

위의 방화벽을 XML 방화벽으로 사용하여 UDDI의 활용 시나리오를 다음과 같이 들 수 있다. (그림 13)에서 한 개 웹 서비스 그룹인 Domain_Gov 내의 개별 웹 서비스들이 공용 UDDI에 광고(publish)될 때, 개별 웹 서비스들의 접근주소(URL)를 XML 방화벽인 web_Firewall의 접근주소로 대체하여 표기한다. 웹 서비스의 요청자는 공용 UDDI에서 XML 방화벽의 주소를 취득한 후, XML 방화벽으로 웹 서비스의 WSDL을 요청한다. 이 때, web_Firewall은 요청자의 요청메시지에 포함된 권한정보를 기반으로 접근허용 여부를 결정한다. 접근이 허용되지 않는 경우, WSDL 전달 실패가 요청자에게 전달될 것이고, 접근이 허용되는 경우, 요청자가 요구했던 웹 서비스들의 WSDL이 web_Firewall 또는 개별 웹 서비스로부터 전달될 것이다.

5.4.2 WS-Addressing

한 기관 및 조직의 네트워크 방화벽 내에 구현된 웹 서비스에 대해서는 WS-Addressing 기능을 사용할 수 있다.

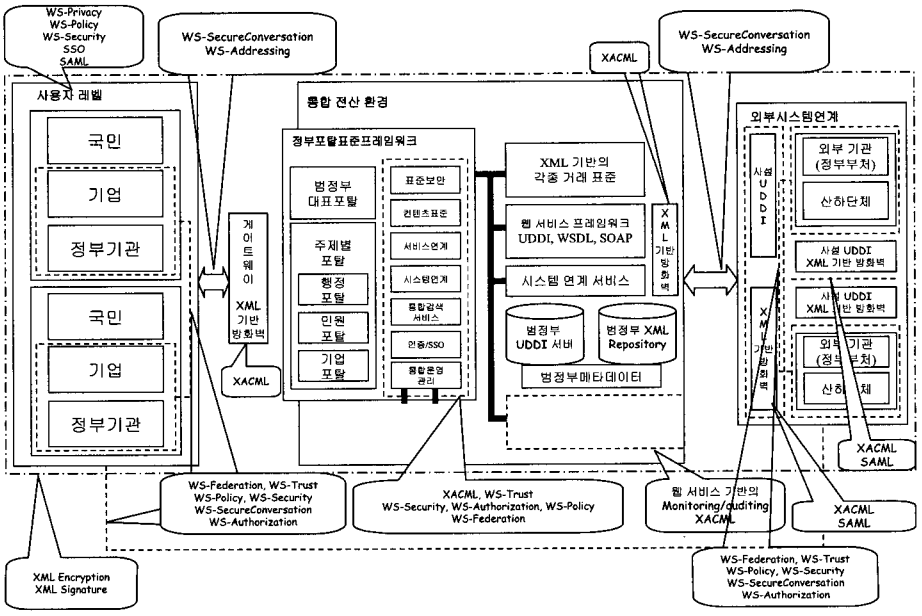
WS-Addressing을 통하여 중간 경로의 방화벽 또는 게이트웨이가 존재하여도 종단간 웹 서비스 요청 및 처리의 투명성을 보장받을 수 있다. 또한 로그에 대한 저장을 전담하는 시스템으로 fault reply가 수집되도록 설정하여 서비스에 대한 안정성과 보안성을 지속적으로 점검할 수 있다. (그림 14)에서 수신자의 fault reply는 송신자 메시지에서 요청된 대로 송신자 네트워크의 로그서버로 보내진다.



(그림 14) WS-Addressing의 활용 예제

5.5 범정부 통합전산환경의 보안 적용

(그림 15)는 지금까지 기술한 내용을 기반으로 범정부 통합



(그림 15) 범정부 통합전산환경에서 웹 서비스 보안 기술 적용

전산환경에서 웹 서비스 보안 기술 적용에 대한 전체 뷰(view)를 나타낸다. 먼저 전체 인프라에 대해서는 범정부 게이트웨이로부터 외부로 향하는 XML 기반 전송에 있어서 기밀성, 무결성, 부인방지를 제공해주기 위해서 XML Encryption과 XML Signature 기술을 적용하고 XML 기반 컨텐츠에 대한 기밀성, 무결성, 부인방지를 제공해주기 위해 역시 XML Encryption과 XML Signature 기술을 적용한다. 또한, 인증/단일 사용자인증 서비스를 위해서 SAML과 XACML 기술을 적용하고 범정부 UDDI와 범정부 XML Repository의 접근제어를 위해 마찬가지로 SAML과 XACML 기술을 적용한다.

범정부 통합 전산환경에서 보안에 대한 뷰를 나타내기 위해 크게 3가지 구성요소-사용자 레벨, 통합전산환경, 외부 시스템-로 나누어 기술한다.

사용자 레벨에서는 개인 프라이버시를 보호하기 위해 WS-Privacy를 사용해야 한다. 그러나 WS-Privacy를 적용하기 위해서는 WS-Policy, WS-Trust, WS-Security 기술이 먼저 적용되어야 한다. 여기서 국민과 기업/정부기관은 다른 보안 고려사항이 존재할 수 있다. 정부 기관은 신뢰 관계 속에서 연합을 고려해야하며 따라서 WS-Federation 기술이 적용되어야 한다. WS-Federation은 정부기관과의 관계뿐만 아니라 정부기관이 외부 시스템과 연계되는 경우에도 적용되어야 하고 안전한 연합을 위해 WS-SecureConversation, WS-Trust, WS-Policy 기술이 먼저 적용되어야 하며 WS-Authorization 기술이 적용되어야 연합이 가능하다.

통합전산환경은 시스템에 접근하는 시스템 연계, 서비스에 접근하는 서비스 연계 처리 모듈에서 웹 서비스 기반의 접근제어, 신뢰 관리, 정책, 연합 등의 보안 고려 사항이 있을 수 있으며 가용성을 보장하기 위한 웹 서비스 기반의 네트워크 관리 기술 등이 적용되어야 하며 시스템 접근 및 오류에 대한 감사가 가능해야 한다.

통합전산환경과 외부 시스템과의 연계에 있어서 전송되는 데이터의 기밀성을 유지하기 위한 WS-SecureConversation 기술이 활용될 수 있으며 WS-Addressing을 활용하여 접근에 대한 모니터링 및 감사를 수행 할 수 있다. 연계되는 외부 시스템은 각 기관의 서비스 접근 제어를 위한 사설 UDDI(포털 혹은 파트너 카탈로그)와 XML 기반의 방화벽을 설치하여 사용할 수 있다.

6. 결론 및 향후 연구

전자정부 서비스는 국민의 행정 편리성과 공공 효율성 향상을 목표로 한 국가적 과제이다. 전자정부 서비스는 개인의 신상 정보, 기업의 중요 정보, 국가 기밀 정보 등의 매우 민감한 정보들을 관리하므로 이에 대한 보안은 필수적이다. 그러나 전자정부 서비스는 정부부처의 문서 전자화작업과 정부 내부 네트워크 설치 등과 같은 전자정부 서비스 인프라의 구축에 중심을 두고 성장하였고, 보안에 고려는 최근에 시작되었다. 현재 전자정부 보안은 전자정부 서비스의 기반기술인 웹 서비스의 기초 보안 기술들과 전통적인 네트워크, 응용계층의 보안 기술들을 비체계적으로 적용한 실정이다. 전자정부와 웹 서비스의 공통적 특징은 분산된 서비스 제공자가 서로 연합되어 사용자에게 한 가지 서비스를 제공하는 구조로 동작한다는 것이다. 따라서 현 시점의 전자정부 보안 요구사항의 중심은 정부의 각 개별 부처 및 기관의 개별 서비스의 연계 과정에서 발생한다.

본 논문에서는 전자정부의 보안성이 요구되는 범위가 한 개 부처 내부의 정보 보안, 전자정부 서비스 이용자와 정부 간의 상호 통신과정을 위한 보안, 정부부처 간의 연계에서 요구되는 보안의 세 범위로 분리될 수 있음을 인식하여, 이를 기준으로 전자정부 보안 발전 단계를 3단계로 나누고 각 단계에서 요구되는 보안 요구사항을 만족시키기 위한 웹 서비스 활용 시나리오를 제시하였다. 또한 이를 기반으로 향후 구축될 범정부 통합 전산환경에서의 웹 서비스 보안 적용에 대한 뷰를 제시하였다.

본 논문에서는 전자정부 전체적인 보안 요구사항에 대해 기술하였다. 이 중 신뢰관리를 기반으로 하고 있는 접근제어를 위해서는 전자정부 서비스에서의 자원과 서비스 요청자의 보안 등급 및 역할 등에 대한 분류작업이 선행된 후 설계가 이루어져야 한다. 이를 위해서는 전자정부 서비스를 제공하는 부처 간 관계구조와 업무 프로세스에 대한 구체적인 분석이 이루어져야 할 것이다. 이러한 보다 구체적인 분석을 토대로 전자정부 서비스를 위한 접근제어 모델과 메커니즘의 설계를 향후 계획한다.

참 고 문 헌

[1] Bob Atkinson, "Web Services Security (WS-Security)", IBM, April, 2002.

[2] Dmitri Tcherevik, "웹 서비스의 관리 및 보안", Computer Associates, July, 2003.

[3] evans data corporation, http://www.evansdata.com, Aug., 2002.

[4] Giovanni Della-Libera, "Web Services Security Policy (WS-SecurityPolicy)", IBM, December, 2002.

[5] H.M. Deitel, et al., "Web Services: A Technical Introduction", Prentice Hall, 2003.

[6] IBM, "Web Services Secure Conversation Language (WS-Secure Conversation)", May, 2004.

[7] Jothy Rosenberg, David Remy, "Securing Web Services with WS-Security", SAMS, 2004.

[8] Office of the e-Envoy, "Security Architecture e-Government Strategy Version 2.0", UKOnline, Sept., 2002.

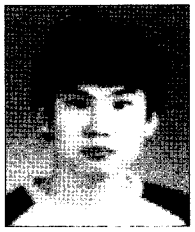
[9] Office of the e-Envoy, "Security e-Government Strategy Framework Policy and Guidelines", UKOnline, Sept., 2002.

[10] Office of the e-Envoy, "Registration and Authentication e-Government Strategy Framework Policy and Guidelines", UKOnline, Sept., 2002.

[11] Office of the e-Envoy, "Trust Services e-Government Strategy Framework Policy and Guidelines", UKOnline, Sept., 2002.
[12] Office of the e-Envoy, "Confidentiality e-Government Strategy Framework Policy and Guidelines", UKOnline, Sept., 2002.
[13] Office of the e-Envoy, "Business Services e-Government Strategy Framework Policy and Guidelines", UKOnline, Sept., 2002.
[14] Office of the e-Envoy, "Network Defence e-Government Strategy Framework Policy and Guidelines", UKOnline, Sept., 2002.
[15] Office of the e-Envoy, "Assurance e-Government Strategy Framework Policy and Guidelines", UKOnline, Sept., 2002.
[16] Siddharth Bajaj, "Web Services Policy Framework (WS-Policy)", IBM, September, 2004.
[17] Steve Anderson, "Web Services Trust Language (WS-Trust)", IBM, May, 2004.
[18] Stephen A. Ronaghan, "Benchmarking E-government: A Global Perspective", UN, Jun., 2002.
[19] Sungmin Kang, "Designing the Organizational e-Security Framework for e-Supply Chain Management", Entrue Research Papers, January, 2004.
[20] 김경섭, "성공적인 전자정부 구현을 위한 구성요소 분석", 정보통신정책 ISSUE 제 15권 1호, 2003년 3월.
[21] 김현곤, "전자정부 전략과 정보보호", Symposium on Information Security, 2003년 7월.
[22] 류석상, "주요 4개국 전자정부 비교, 분석 - 한국, 미국, 영국, 일본을 중심으로", 한국전산원, 2003년 5월.
[23] 박종환, "웹 서비스 표준의 현재와 미래", SDS IT Review, 2004년 4월.
[24] 양태종 외 5인, "다부처 연계사업의 성공적 추진 방안 : G4C 사례를 중심으로", Entrue Research Papers, 2004년 7월.
[25] 유은숙, "전자정부의 전자문서유통체계 추진 현황", 디지털 행정 제 96호, 2004년 여름호.
[26] 이석균, "2004년도 정보화예산 편성방향 및 현황", 기획예산처, 2003년 12월.
[27] 정부연, "웹 서비스의 현황 및 비즈니스 모델의 변화 ", 정보통신정책연구원, 제14권 15호, 2002년 8월.
[28] 정보통신부, 한국전산원, "정보시스템 구축 운영 기술 가이드라인 버전 1.0", 2004년 3월.
[29] 행정자치부, "참여정부의 전자정부 과제와 추진 전략", 행정자치부, 전자정부컨퍼런스 2004, 2004년 5월.
[30] 한국전산원, "웹 서비스 보안 기술 분석 및 응용 방안 연구", 2003년 12월.
[31] 한국전산원, "웹 서비스 개발운영 환경 분석 및 전자정부 도입 전략 연구", 2003년 12월.
[32] 황종성, "미래 전자정부 청사진", 한국전산원, 전자정부 컨퍼런스 2003, 2003년 6월.

이 은 선
e-mail : eslee99@imtl.skku.ac.kr
2003년 성균관대학교 정보통신공학부(학사)
2003년~현재 성균관대학교 컴퓨터공학과 석사과정
관심분야 : VPN, IPv6, 네트워크 보안, 이동 멀티캐스트

양 진 석
e-mail : jsyang@etri.re.kr
2003년 성균관대학교 정보공학과(학사)
2005년 성균관대학교 컴퓨터공학과 석사
2005년~현재 국가보안기술연구소 연구원
관심분야 : 액티브 네트워크, 침입감내, 유비쿼터스 보안, IPv6, 네트워크 보안



임 정 묵
e-mail : izeye@imtl.skku.ac.kr
2004년 성균관대학교 정보통신공학부(학사)
2004년~현재 성균관대학교 컴퓨터공학과 석사과정
관심분야 : 네크워트, 보안

문 기 영
e-mail : kymoon@etri.re.kr
1986년 경북대학교 전자공학과 졸업
1989년 경북대학교 대학원 전자공학과 석사
1992년~1994년 (주)대우정보시스템 기술연구소 대리
1994년~현재 한국전자통신연구원 정보보호연구단 생체인식기술연구팀 팀장
관심분야 : 생체인식, 웹서비스 보안, 분산시스템 등

이 재 승

e-mail : jasonlee@etri.re.kr

1993년 서강대학교 수학과(이학사)

1997년 포항공과대학교 정보통신학과(공학석사)

1997년~1999년 데이콤 정보통신연구소 (연구원)

1999년~현재 한국전자통신연구원 정보보호연구단(선임연구원)

관심분야 : 웹서비스 정보보호, 유비쿼터스 정보보호, 전자상거래 정보보호

정 태 명

e-mail : tmchung@ece.skku.ac.kr

1981년 연세대학교 전기공학과(학사)

1984년 일리노이 주립대학 전자계산학과(학사)

1987년 일리노이 주립대학 컴퓨터공학과(석사)

1995년 퍼듀 대학 컴퓨터공학 (박사)

1984년~1987년 Waldner and Co., System Engineer

1987년~1990년 Bolt Bernek and Newman Labs. Staff Scientist

1995년~현재 성균관대학교 정보통신공학부 교수

관심분야 : 실시간시스템, 네트워크 관리, 네트워크 보안, 시스템 보안, GRID 네트워크, 전자상거래