情報保護學會論文誌
第20卷 第6號, 2010. 12

안티바이러스 시스템 보안기능 분석을 통한 보안SLA 등급화 지표 개발

이 완 석[1†], 이 동 범[2], 원 동 호[1], 곽 진[2‡]
[1]성균관대학교 정보보호그룹, [2]순천향대학교 정보보호학과

Development of S-SLA based on the Analyses of Security Functions for Anti-virus System

Wan-Suck Yi[1†], Dongbum Lee[2], Dongho Won[1], Jin Kwak[2‡]
[1]Information Security Group, SungkyunkwanUniversity,
[2]Department of Information Security Engineering, SoonchunhyangUniversity

요 약

최근 다양한 사이버 침해사고의 개인정보 유출 사례를 살펴보면 공격 대상이 서비스 제공자를 대상으로 하고 있지만 실제적인 피해 대상은 사용자라고 할 수 있다. 정당한 서비스 계약을 체결하였음에도 불구하고 정상적인 서비스를 받을 수 없거나 서비스를 위해 제공한 개인정보가 유출되는 피해가 발생하고 있다. 이에 따라 사업자 및 사용자간 제공되는 서비스에 대한 SLA와 관련하여 보안SLA가 크게 주목받고 있다. 특히 안티바이러스 서비스를 제공하는 서비스 제공자의 경우 보안SLA를 통해 보다 높은 수준의 보안서비스를 제공해야 한다. 그러나 국내에서는 보안SLA와 관련된 연구가 미비하여 유지보수 수준의 SLA만 제공되는 상황이다. 따라서 본 논문에서는 안티바이러스 시스템의 보안기능을 분석하여, 보안SLA의 지표를 개발하고 보안기능별 등급화 방안을 제안한다.

ABSTRACT

If one analyzes recent cyber incidents including personal information infringement cases, it seems like actual attack is targeting Internet service providers but actually they are targeting Internet service users. For many users, all the services were not provided to them as they have signed for in the contract or personal informations, which users have provided to service providers when signing contracts, were disclosed to public without users' consent causing aftereffect. As a result, importance of S-SLA indexes, which is to be included in the SLA to be signed between a user and a service provider, is ever more increasing. Especially, if there is a S-SLA indexes for anti-virus services, service providers have to provide a high quality of service as they have signed in the SLA. However, there wasn't any researches in the S-SLA area domestically and there are only limited SLA indexes related to system or service maintenances at the moment. Therefore, this paper analyses security functions in anti-virus services and proposes S-SLA indexes for different security level.

Keywords: S-SLA, Anti-Virus System, Security Function

I. 서 론

최근 IT서비스에 대한 품질제고 요구 확산으로 통신사의 초고속 인터넷 서비스에 대한 최저속도 보장을 유도하여 해당 서비스의 품질을 크게 개선한 바 있으나, 응용 서비스나 보안서비스 등에서는 체계적인 보안품질관리가 미흡한 실정이다.

접수일(2010년 9월 25일), 수정일(2010년 12월 8일), 게재확정일(2010년 12월 15일)
† 주저자, wsyi@kisa.or.kr
‡ 교신저자, jkwak@sch.ac.kr

보안서비스에 대한 보안서비스수준협약(SLA : Service Level Agreement) 지표 도입을 통한 품질 관리는 해당 서비스의 정보보호 품질을 높여 서비스 제공자의 사업 경쟁력 강화와 사용자가 제공 받는 보안서비스에 대한 안전성 요구 충족을 통해 궁극적으로 인터넷 망의 안전성 강화를 기대할 수 있다.

또한 최근 유비쿼터스화 및 융·복합화로 망간 연계가 늘어나고 구조가 복합해지는 등 서비스의 고도화에 따라 사이버 침해 공격을 통한 서비스 품질의 악영향도 커질 수 밖에 없어 신규 서비스들에서 보안 품질 관리는 더욱 더 중요해지고 있다.

따라서 본 논문에서는 보안서비스의 품질 제고를 위해 정보보호 서비스 제공자와 사용자 사이의 SLA에서 다루어져야 할 안티바이러스 서비스에 대한 보안 SLA(S-SLA : Security Service Level Agreement) 지표를 개발하고 사용자가 원하는 보안서비스 수준의 다양화를 위한 등급화 방안을 제안한다. S-SLA의 지표 도출을 위해 분석한 안티바이러스 시스템은 대표성 및 공정성을 위하여 IT인증사무국에 등록된 공통평가기준(CC : Common Criteria) 인증 제품을 기준으로 분석 하였다.

본 논문의 구성은 다음과 같다. 2장에서는 S-SLA의 정의와 필요성에 대해서 기술하고, 3장에서는 S-SLA 등급화 지표 개발 대상에 대해서 분석한다. 4장에서는 분석된 보안기능을 토대로 안티바이러스 시스템에 대한 S-SLA의 지표를 개발하고, 보안기능별 등급화 방안을 제안한다. 5장에서는 본 논문에서 제안한 S-SLA의 파급 효과에 대해서 분석하고, 마지막으로 6장에서 결론을 맺는다.

II. S-SLA

2.1 정의

서비스에 대한 품질 제고 요구가 확산되면서, 서비스 제공에 관계된 시스템의 운영관리 요소들은 단순한 업무 활동보다는 하나의 필수 요소로써 인식되게 되었고, 이를 정량화하여 관리하는 서비스수준관리(SLM : Service Level Management)의 개념이 최근 운영관리 전반에 걸쳐 도입되고 있다. 서비스수준협약(SLA)은 SLM을 통해 작성 및 관리된다. 고객과 서비스 제공자간에 제공되는 서비스의 수준을 보장하기 위한 계약을 의미하며, 서비스 제공에 관계된 정보시스템의 운영관리에 대한 다양한 측면에서의 성과 척도를 명시하고 이를 만족하기 위한 활동들을 제시한다[1][2].

〔표 1〕 SLA 정의

기관	정의
ITU-T (E.860)	둘 또는 그 이상의 주체들간에 협상을 통해 합의된 공식적인 합의서로서 서비스 특성, 책임, 그리고 모든 면에 있어서 우선순위들을 평가하기 위한 범위와 관련한 공식 동의서
ETSI	서비스 수준이란 서비스 성능을 나타내기 위해 서비스 특성, 양적 측면, 질적 측면, 시간성, 사용 조건, 요금 및 비용 등과 같은 요소들을 하나 이상 포함하는 합의된 프로세스
TMF	두 주체간의 협상 하에 동의된 공식적 규약. 이것은 서비스 제공자와 고객간의 계약으로서 서비스 품질, 우선순위, 책임 등에 관한 공통의 이해를 만들기 위해 작성되는 것

SLA에 대한 정의 또한 기관별로 약간씩 다르게 정의하고 있는데 기본적으로 '서비스 수준에 대해 둘 이상의 주체간에 합의나 협의에 의해 작성되는 책임과 의무에 관한 계약사항'이라는 공통적인 의미를 내포하고 있다. 다음은 각 기관에서 정의하고 있는 SLA를 나타낸다[10]-[13].

일반적으로 SLA를 다룰 때 기밀성, 가용성, 무결성 측면에서 보안사항을 고려하도록 일반적인 SLA 문서에서 권고하고 있으나, 실제적으로는 서비스 개별적으로 각 서비스 특성에 따라 보안특성 분석이 필요하여 SLA에서 보안 항목이 잘 다루어지지 않고 있다. 이러한 이유로 SLA에서 보안항목을 다룰 필요성에 따라 S-SLA라는 개념을 다음과 같이 정의한다[14]-[17].

- 서비스 제공자와 사용자간에 제공되는 서비스에 관련된 여러 조건들에 대한 서로의 책임과 의무사항을 기술해 놓은 상호협약(SLA)에서 정보보호에 대한 항목을 포함한 SLA

2.2 필요성

정부(방송통신위원회)는 이미 통신사의 초고속인터넷서비스 SLA에서 최저속도 보장을 유도하여 해당 서비스의 품질 및 사용자 권익보호가 크게 개선된 바 있다. 그러나, 국내 사업자들은 초고속인터넷서비스, VoIP 서비스, 보안 서비스 등에서 S-SLA 지표 정의를 통한 체계적인 품질관리가 미흡하여 국외 선진국에

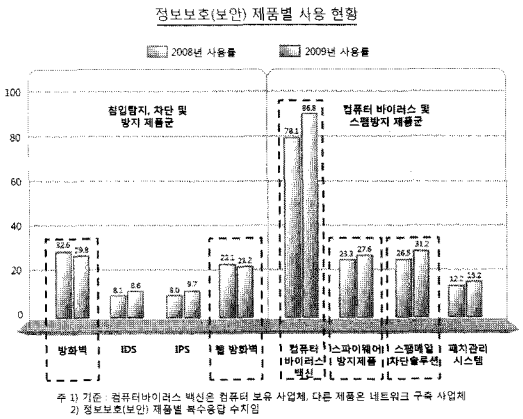
비해 보안품질이 떨어지는 실정이다. S-SLA 도입을 통한 품질관리는 서비스의 보안품질을 제고하는 것을 목적으로 하고 있어, SLA에서 보안지표 항목 관리는 정보보호 서비스 품질제고를 통한 경쟁력 강화 및 서비스 제공자의 신속한 침해사고 대응을 유도하여 국내 인터넷 망의 안전성 강화를 기대할 수 있다. 또한, 유비쿼터스 및 융·복합 서비스에서 망간 연계가 늘어나고 서비스 구조가 복합해지는 등 점점 고도화 되고 있어 사이버 침해공격에 서비스 품질의 악영향도 커질 수 밖에 없어 신규 서비스들에서 보안 품질 관리는 더욱 더 중요해지고 있다.

〔표 2〕 S-SLA 운영에 따른 주체별 이득

구분	설명
국가	- 네트워크 악성코드 및 침해공격 등의 확산 방지
사용자	- 서비스의 안전한 이용 - 서비스에 대한 합당한 가격 지불 및 보상, 제공받는 서비스의 안전성 요구 충족
제공자	- 침해사고 등에 기인하는 통신망 관련 비용요소 경감 및 사업 경쟁력(비교 우위) 강화 - 통신망의 가용성, 접속 실패율 등의 객관적 기준치를 관리함으로써 서비스 실패로 인한 고객 이탈 등의 손실 조기 차단

III. S-SLA 등급화 지표 개발 대상

SLA는 서비스 단위로 구성되기 때문에 서비스의 특성 파악이 중요하다. 현재 단계에서 제공되는 모든 서비스를 종류별로 S-SLA 지표를 개발하는 것은 서비스 특성 분석이 우선 진행되어야 하고 해당 서비스에서 보안항목을 SLA로 관리하는 것이 얼마나 중요한지 또는 의미가 있는지 분석이 선행되어야 하기 때문에 현실적으로 어려운 실정이다. 따라서, 현재 S-SLA는 보안지표 항목이 보안 서비스에서 가장 의미 있게 다루어질 필요가 있고, 서비스 특성이 잘 알려져 있기 때문에 정보보호 관련 서비스에서 우선적으로 적용할 필요가 있다. S-SLA 지표 개발을 위한 정보보호 관련 서비스 선정은 전체 보안제품 및 서비스 중에서 가장 많이 활용되는 주요 보안 서비스에 대해 우선적으로 도출하는 방향으로 설정하였다. 이를 위해 정보보호 제품 및 서비스의 이용빈도와 매출액을 분석하여 가장 많이 사용되는 제품 및 서비스를 S-SLA 지표 개발 대상으로 선정하였다.



〔그림 1〕 정보보호 제품별 사용 현황

3.1 S-SLA 지표 대상 선정

한국정보화진흥원(NIA)에서 발행한 2010년 정보화 통계 결과에 의하면 컴퓨터를 보유한 약 1,764,000개 사업체 가운데 컴퓨터 바이러스 및 스팸 방지 제품으로 컴퓨터 바이러스 백신을 사용하는 사업체는 86.8%(약 1,531,000개)인 것으로 추정하고 있다.

정보보호 제품 이용율은 ① 컴퓨터 바이러스 백신, ② 스팸메일 차단 솔루션, ③ 방화벽, ④ 스파이웨어 방지 제품, ⑤ 웹 방화벽 순으로 나타나고 있다[7].

이용율 순위를 기준으로 S-SLA 지표 개발대상을 우선 선정하면 컴퓨터 바이러스 백신 제품에 속하는 안티바이러스가 해당되므로 관련 시스템을 S-SLA 지표개발 대상으로 선정하였다.

3.2 안티바이러스 시스템

안티바이러스 시스템은 컴퓨터 바이러스를 예방, 진단, 치료하기 위해서 만들어진 프로그램을 의미한다.

대부분의 안티바이러스 시스템들은 인터넷을 통해 받은 데이터를 실시간으로 검사하고, 주기적인 업데이트로 새로운 바이러스, 웜, 트로이목마 프로그램의 정보를 유지하며, 검사를 통해 감염된 시스템을 치료하는 기능을 가지고 있다. 기존의 안티바이러스 시스템은 바이러스 치료가 목적이지만, 최근의 안티바이러스 시스템은 취약점을 미리 알려주고 의심스러운 파일을 차단하는 기능까지 포함하고 있다.

〔표 3〕 안티바이러스 시스템의 보안기능

구분	시스템 A(EAL3)	시스템 B(EAL3)	시스템 C(EAL3)	시스템 D(EAL3)
보안 경보	×	×	○	×
감사 데이터 생성	○	○	○	○
사용자 신원 연관	○	○	○	○
잠재적인 위반 분석	×	×	○	×
감사 검토	○	○	○	○
선택 가능한 감사 검토	○	○	○	○
감사 증적 저장소 보호	○	×	○	○
감사 데이터 손실 예측시 대응행동	○	○	○	○
감사 데이터의 손실 방지	○	×	○	○
인증 실패 처리	○	○	○	○
인증	×	×	○	○
비밀정보의 검증	○	○	○	○
모든 행동 이전에 사용자 인증	○	○	×	×
인증 피드백 보호	○	×	×	○
식별	×	×	○	×
모든 행동 이전에 사용자 식별	○	○	×	×
보안기능 관리	○	○	○	○
보안기능 데이터 관리	○	○	○	○
데이터 한계치의 관리	×	×	×	○
관리기능 명세	○	○	○	○
보안 역할	○	○	○	○
외부 전송 데이터의 변경 탐지	○	○	×	○
내부 전송 데이터의 기본적인 보호	○	○	×	×
외부 실체 시험	×	○	×	×
자체 시험	○	○	○	○
사용자에 의한 세션 잠금	×	○	○	×
악성코드 경고	○	○	○	○
악성코드 탐지	○	○	○	○
악성코드 대응	○	○	○	○

※ ○ : 제공, × : 제공하지 않음

3.3 안티바이러스 시스템의 보안기능 분석

S-SLA 지표 도출을 위해 분석한 안티바이러스 시스템은 대표성 및 공정성을 위하여 IT인증사무국에 등록된 CC 인증 제품을 기준으로 분석 하였다. 안티바이러스 시스템 인증 제품은 EAL3 제품으로 총 4개 제품이며, 각 제품의 보안목표명세서(ST : Security Target)의 보안기능요구사항을 기반으로 분석하였다[3]-[6].

다음은 각 보안기능에 대해서 설명한다.

- **보안 경보** : 잠재적인 보안 위반을 탐지한 경우 사전에 정의된 방법으로 인가된 관리자에게 경보
- **감사 데이터 생성** : 감사 기능의 시동과 종료, 감사 수준에 따른 감사대상 사건에 대해 레코드를 생성해야 하고 사건에 대한 정보를 각 감사 레코드에 기록
- **사용자 신원 연관** : 사건을 발생시킨 사용자의 신원과 감사대상 사건을 연관
- **잠재적인 위반 분석** : 관리자가 알려진 잠재적인 보안 위반의 규칙 집합을 적용하여 보안기능의 수행에 대한 잠재적 위반을 지적
- **감사 검토** : 인가된 관리자에게 모든 감사 데이터를 읽을 수 있도록 함
- **선택 가능한 감사 검토** : 감사 데이터의 유형에 따라 감사 데이터를 검색, 정렬 등의 기능 제공
- **감사 증적 저장소 보호** : 인가되지 않은 삭제로부터 감사 종적 내에 저장된 감사 레코드를 보호
- **감사 데이터 손실 예측시 대응행동** : 감사 데이터의 저장소에서 인가된 관리자가 설정한 값을 초과하는 경우, 이를 관리자가 설정해 둔 메일주소로 메일을 발송하고 저장소 확보를 위해 감사 데이터를 백업하거나 오래된 감사 데이터부터 삭제
- **감사 데이터의 손실 방지** : 감사 저장소가 포화된 경우 특별한 경우를 제외하고는 감사 저장소에 대해 덮어쓰기 등의 조치를 취하고 관리자에게 경보
- **인증 실패 처리** : 관리자 및 일반 사용자가 인증을 하려고 할 때, 인증 시도 횟수가 관리자가 구성한 인증 실패 허용 한계치 이상시 1~60분간 인증을 방지
- **인증** : 관리자 및 사용자가 안티바이러스 기능을 사용하기 전에 해당 관리자 및 사용자에 대한 인증을 수행
- **비밀정보의 검증** : 안티바이러스에 접근하기 위한 패스워드를 검증하는 메커니즘
- **모든 행동 이전에 사용자 인증** : 사용자를 대신하여 보안기능이 제공하는 모든 기능을 허용되기 전에 사용자는 성공적인 인증을 수행
- **인증 피드백 보호** : 인증이 진행되는 동안 인가된 관리자에게 모조 패스워드만을 제공
- **식별** : 관리자 및 사용자가 안티바이러스 기능을 사용하기 전에 해당 관리자 및 사용자에 대한 식별을 수행
- **모든 행동 이전에 사용자 식별** : 사용자를 대신하여 보안기능이 제공하는 모든 기능을 허용되기 전에 사용자는 성공적인 식별을 수행
- **보안기능 관리** : 예약 검사, 실시간 검사, 보안 검사, 수동검사 등의 환경에 대해 행동을 결정, 중지, 개시하는 능력을 인가된 관리자로 제한
- **보안기능 데이터 관리** : 관리자에게 예약검사 대상 목록, 예약검사 주기, 실시간 검사 대상 목록, 압축 파일의 검사 깊이 등을 관리하는 능력을 제공하고 사용자에게 수동검사 대상 목록, 예약검사 대상 목록, 예약검사 주기, 실시간 검사 대상 목록, 압축 파일의 검사 깊이 등을 관리하는 능력을 제공
- **데이터 한계치의 관리** : 모든 감사 로그 데이터, 검역소 데이터에 관해 한계치를 정하고 초과하는 경우 경고를 전송
- **관리기능 명세** : 안티바이러스가 보안속성, 보안기능 데이터, 보안기능 등의 관리기능을 제공
- **보안 역할** : 보안기능이 인식 가능한 보안과 관련된 역할을 제공
- **외부 전송 데이터의 변경 탐지** : 보안기능과 원격의 신뢰된 IT제품간 전송되는 모든 데이터의 변경을 탐지
- **내부 전송 데이터의 기본적인 보호** : 보안기능의 분리된 부분간에 보안기능 데이터가 전송될 때 변경으로부터 데이터를 보호
- **외부 실체 시험** : 네트워크 주소의 이상을 점검하기 위해 업데이트시 일련의 테스트를 하고 실패시 연결 재시도를 수행
- **자체시험** : 보안기능의 정확한 운영을 위하여 자체시험을 보장하고 실행 코드의 무결성을 보장
- **세션 잠금** : 사용자가 설정한 일정 시간이 지난 후 상호작용 세션을 잠가야 하며 해제시 재인증을 수행
- **악성코드 경고** : 안티바이러스는 사용자의 화면에 탐지된 악성코드의 정보목록을 표시
- **악성코드 탐지** : 부트 기반, 파일 기반, 메모리 기반 악성코드들을 탐지하기 위해 여러 검사 기능을 제공
- **악성코드 대응** : 부트 기반, 파일 기반, 메모리 기반 악성코드들을 탐지하기 위해 경고, 악성코드 제거, 파일 삭제, 격리 등의 대응행동

〔표 4〕 안티바이러스 시스템의 공통보안기능

구분	시스템 A(EAL3)	시스템 B(EAL3)	시스템 C(EAL3)	시스템 D(EAL3)
보안 감사 영역	감사 데이터 생성			
	사용자 신원 연관			
	감사 검토			
	선택 가능한 감사 검토			
	감사 데이터 손실 예측시 대응행동			
식별 및 인증 영역	인증 실패 처리			
	비밀정보의 검증			
보안 관리 영역	보안기능 관리			
	보안기능 데이터 관리			
	관리기능 명세			
	보안 역할			
보안기능 보호 영역	자체 시험			
악성 코드 차단 영역	바이러스 경고			
	바이러스 탐지			
	바이러스 대응			

〔표 5〕 안티바이러스 시스템의 개별보안기능

구분	시스템 A(EAL3)	시스템 B(EAL3)	시스템 C(EAL3)	시스템 D(EAL3)
보안 감사 영역	-	-	보안 경보	-
	-	-	잠재적인 위반 분석	-
	감사 증적 보호	-	감사 증적 저장소 보호	
	감사 데이터의 손실 방지	-	감사 데이터의 손실 방지	
식별 및 인증 영역	-	-	인증	인증
	모든 행동 이전에 사용자 인증		-	-
	인증 피드백 보호	-		인증 피드백 보호
	-	-	식별	-
	모든 행동 이전에 사용자 식별		-	-
보안 관리 영역	-	-	-	데이터 한계치의 관리
보안기능 보호 영역	외부 전송 데이터의 변경 탐지		-	외부 전송 데이터의 변경 탐지
	내부 전송 데이터의 기본적인 보호		-	-
	-	외부 실체 시험	-	-
제품 기능 접근 영역	-	사용자에 의한 세션 잠금		-

〔표 6〕 안티바이러스 시스템 S-SLA 지표

대분류	보안기능	세부기능	카테고리
보안 감사 및 대응	감사 데이터 관리 기능	감사 데이터 생성	I
		사용자 신원 연관	I
		감사 검토	I
		선택 가능한 감사 검토	I
		감사 데이터 손실 예측시 대응행동	I
	감사 데이터 보호 기능	감사 증적 저장소 보호	II
		감사 데이터의 손실 방지	II
	보안 위반 탐지 및 대응 가능	보안 경보	IV
		잠재적인 위반 분석	IV
인증 및 인증 정보 보호	인증 보안기능	인증 실패 처리	I
		비밀정보의 검증	I
	인증 및 식별 기능	인증	III
		식별	IV
	사전 인증 및 식별	모든 행동 이전에 사용자 인증	III
		인증 피드백 보호	III
		모든 행동 이전에 사용자 식별	III
보안 관리 및 권한 설정	권한 설정 기능	보안기능 관리	I
		보안기능 데이터 관리	I
		관리기능 명세	I
		보안 역할	I
	데이터 포화 경보 기능	데이터 한계치의 관리	IV
	무결성 검증 기능	자체시험	I
	데이터 위·변조 탐지 기능	외부 전송 데이터의 변경 탐지	II
		내부 전송 데이터의 기본적인 보호	III
	시스템 시험 기능	외부 실체 시험	IV
세션 보호	세션 보호 기능	세션 잠금	III
악성코드 차단	악성코드 관리 기능	악성코드 경고	I
		악성코드 탐지	I
		악성코드 대응	I

IV. S-SLA 지표 개발

4.1 보안기능 분류

안티바이러스 시스템은 공통평가기준에 따라 IT보안인증사무국 인증 제품 목록에 등록된 4개 시스템의 보안기능요구사항을 분석하였다.

이 중에서 동일하게 제공되는 보안기능은 안티바이러스 시스템을 구성하기 위한 기본적인 보안기능으로 분류 할 수 있으며, 각 시스템에 따라 달리 제공되는

보안기능은 제품에 따라 추가적인 보안기능으로 분류할 수 있다.

• 공통보안기능

분석한 4개의 안티바이러스 시스템에서 동일하게 제공되는 기능은 안티바이러스 시스템을 구성하기 위한 기본적인 기능으로 분류할 수 있으며, 이를 '공통보안기능'으로 정의한다.

• 개별보안기능

분석한 4개의 안티바이러스 시스템에서 각 시스템에 따라 달리 제공되는 기능은 시스템에 따라 추가적인 기능으로 사용될 수 있으며, 이를 '개별보안기능'으로 정의한다.

4.2 S-SLA 지표 도출

보안기능 영역은 동일한 보안목적을 가지므로, 해당 시스템에 유사한 기능들이 함께 분류되어 있다. 따라서 본 기능들의 유사성에 따라 지표를 선정하고, 지표에 해당하는 기능을 설정할 수 있다.

안티바이러스 시스템의 공통보안기능은 기본적으로 안티바이러스 시스템이 제공해야 하는 보안기능으로 모든 안티바이러스 시스템에 포함된 공통적인 보안기능을 나타낸다.

안티바이러스 시스템의 개별보안기능은 각 시스템에서 추가적으로 제공하고 있는 보안기능을 나타낸다.

카테고리 Ⅰ(공통보안기능)은 모든 안티바이러스 시스템이 공통적으로 제공하고 있는 보안기능을 나타낸다.

카테고리 Ⅱ(개별보안기능)는 4개의 시스템 중 3개의 시스템이 지원하고 있는 보안기능의 분류이다. 하지만 예외 상황으로 보안 관리 및 권한 설정의 데이터 위·변조 탐지 기능에서 내부 전송 데이터의 기본적인 보호기능은 외부 전송 데이터의 변경 탐지와 동일한 맥락으로 시스템에서 전송되는 데이터의 변경을 탐지하고 보호하는 내용이므로 카테고리 Ⅱ에 포함이 되었다.

카테고리 Ⅲ(개별보안기능)은 2개의 안티바이러스 시스템에서 제공하고 있는 보안기능을 말한다. 예외 상황으로 인증 및 인증 정보보호의 인증 및 식별 기능에서 식별은 카테고리 Ⅳ에 포함되지만, 안티바이러스 시스템의 기능을 사용하기 전에 인증 및 식별이 동시에 제공되기 때문에 카테고리 Ⅲ에 포함이 되었다.

카테고리 Ⅳ(개별보안기능)는 안티바이러스 시스템 중에 한 개의 시스템에서만 제공하고 있는 기능이다.

다음 표는 안티바이러스 시스템의 기능에 따른 S-SLA 지표를 도출한 것이다.

4.3 S-SLA 지표 등급화

4.3.1 등급화 기준

본 절에서는 보안기능별로 도출된 S-SLA 지표에 따라 각 제품군의 등급화 기준을 제시한다. 등급화된 S-SLA 지표는 사용자가 보안서비스에 대한 수준 협약시 자신이 요구하는 보안기능의 질적 수준을 결정하는 요소로서 활용된다.

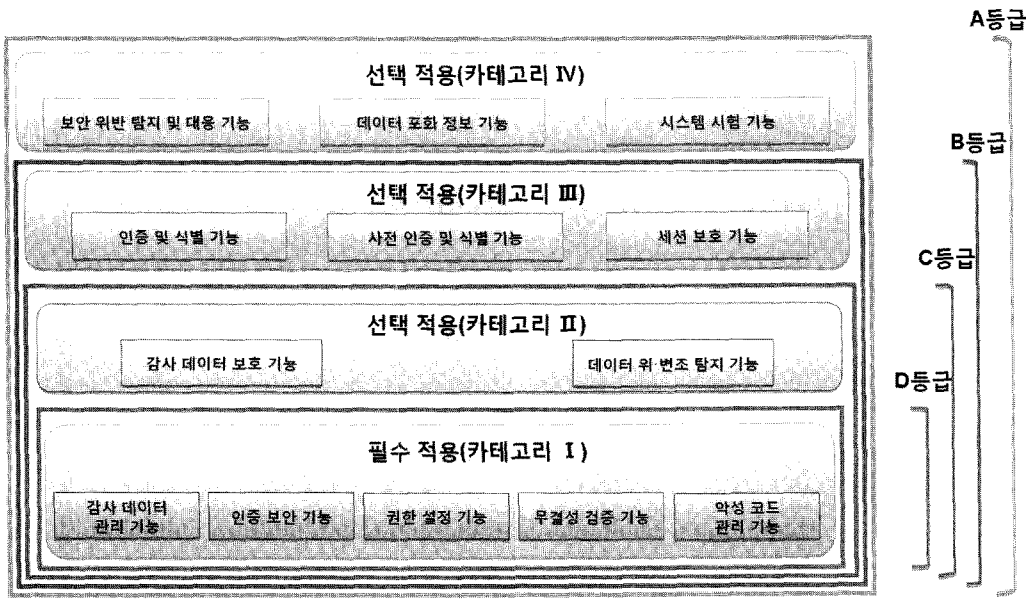
S-SLA 지표의 등급 분류에는 필수 적용 및 선택 적용으로 구분하고 있다.

보안기능별 등급화는 특성 분류를 통해 필수 적용 S-SLA 지표와 선택 적용 S-SLA 지표를 분류하고, 선택한 지표에 따라 등급을 분류한다. 가장 기본이 되는 기본 등급(D등급)은 보안서비스의 필수 적용 S-SLA 지표를 적용한 것이며, 선택 적용 S-SLA 지표의 추가 선택 수에 따라 상위 등급을 부여받게 된다. 선택 적용 S-SLA 지표는 모두 동일한 등급을 가지며, 포함되는 각 분야에 따라 등급이 상향된다. 보안 등급은 A등급이 가장 높은 등급이며, D등급은 기본 등급을 나타낸다.

4.3.2 보안기능별 등급화

안티바이러스 시스템의 등급화는 총 4등급(A, B, C, D)으로 분류된다. 제공되는 보안기능의 시스템 적용 정도에 따라 차등적으로 등급을 분류한다. D 등급은 필수 적용 - 카테고리 Ⅰ을 포함하는 등급이며, C 등급은 필수 적용 - 카테고리 Ⅰ에 선택 적용 - 카테고리 Ⅱ를 추가한 등급이다. 또한 B 등급은 필수 적용 - 카테고리 Ⅰ과 선택 적용 - 카테고리 Ⅱ·Ⅲ 모두를 포함한 등급이며, A 등급은 필수 적용 - 카테고리 Ⅰ과 선택 적용 - 카테고리 Ⅱ·Ⅲ·Ⅳ 모두를 포함한 등급이다.

보안서비스를 제공하기 위해서는 필수적으로 제공해야 하는 보안기능이 있으며, 이를 모든 제품들에서 제공하는 기능들의 집합으로 구분할 수 있다. 안티바이러스 시스템의 4개 제품에 대한 보안기능을 분석하였을 때, 모든 제품이 공통적으로 제공하는 보안기능과 개별적으로 제공하는 보안기능을 분류할 수 있다. 이와 같이 모든 제품에서 공통적으로 제공하는 보안기능은 보안서비스 자체가 성립되기 위한 필수 기능으로



〔그림 2〕 안티바이러스 시스템에 대한 등급화

써 제공되어야 하므로, 이와 맵핑되는 S-SLA 지표에 '필수 적용'을 부여할 수 있다.

선택 적용의 경우에는 제품들에 포함되는 보안기능의 출현 빈도수에 따라 구분할 수 있다. 보안SLA 지표에 맵핑되는 보안기능이 모든 제품에 포함되지 않고 특정 제품에만 포함된 경우, 이는 보안서비스를 제공하는데 있어서 필수적 특성이 아닌 선택적인 부가기능으로 분류할 수 있다. 안티바이러스 시스템의 개별보안기능과 같이 제품에 따라 적용되는 보안기능과 적용되지 않는 보안기능은 부가기능이라고 분석할 수 있다. 따라서 필수 적용에 해당하는 경우를 제외한 특정 제품에 포함된 보안기능과 맵핑되는 S-SLA 지표에 '선택 적용'을 부여하였다.

V. 파급 효과

S-SLA는 서비스를 이용함에 있어서 사업자와 사용자가 상호 서비스 품질에 대한 협약을 통해 보다 효율적이고 안전한 서비스를 제공받을 수 있도록 한다. 이와 같은 S-SLA는 관련 서비스의 증가와 함께 수요증가 및 다양한 파급효과를 가져올 것으로 분석된다.

특정 서비스를 제공하는 사업자 측면에서는 사용자의 증가가 결국 사업의 성공 및 이윤의 창출로 이어진다. 이는 기업이 추구하는 가장 기본 목적이 되며, 이를 위하여 다양한 방안을 적용하고 있다. 그 중에서도 서비스의 보안성을 향상시키는 방안들이 증가하고 있으며, 사용자의 보안의식이 향상된 결과를 반증한다고 할 수 있다.

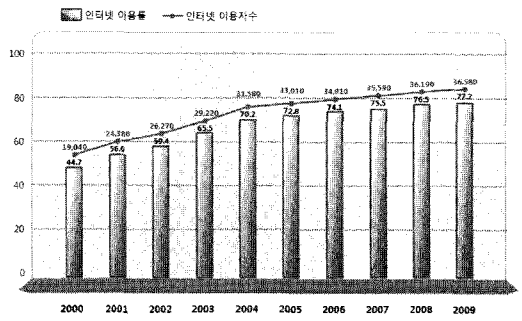
S-SLA의 적용은 사업자의 목적 달성을 위한 다양한 방안 중 기업의 신뢰도 향상과 함께 사용자 증가의 효과를 가져 올 수 있을 것으로 분석된다.

S-SLA의 특성상 사업자와 사용자가 서비스 이용에 있어 긴밀한 협의를 거치게 되며, 이는 서비스의 투명도, 신뢰도, 효율성을 제공하게 된다. 서비스의 투명도는 어떠한 서비스를 어느 수준만큼 제공할지에 대해 서비스 사용자가 명확히 알게 되어, 이에 대한 사용자의 평가가 가능하기 때문이다. 또한, 서비스 신뢰도의 향상은 서비스 수준의 공개로 인해 사용자가 자신이 원하는 만큼의 서비스를 기업이 제공할 수 있다는 것을 판단할 수 있기 때문이다. 그리고 원하는 만큼의 서비스를 제공함에 따라 사업자는 보다 효율적인 자원의 분배도 가능하게 된다.

이와 같은 결과는 보안성과 관련된 타 서비스의 사용자 증가 동향을 분석하면 쉽게 유추할 수 있다.

한국인터넷진흥원 인터넷통계정보검색시스템(ISIS)에서 지난 2009년 12월에 발표한 '2009년 인터넷이용실태조사'에 따르면, 만 3세 이상 인구의 인터넷이용률은 77.2%이며, 인터넷 사용자수는 3,658만명(전년 대비 39만명 증가)으로 집계되고 있다[8].

국내 전체 인구가 5,000만명 정도임을 감안할 때,

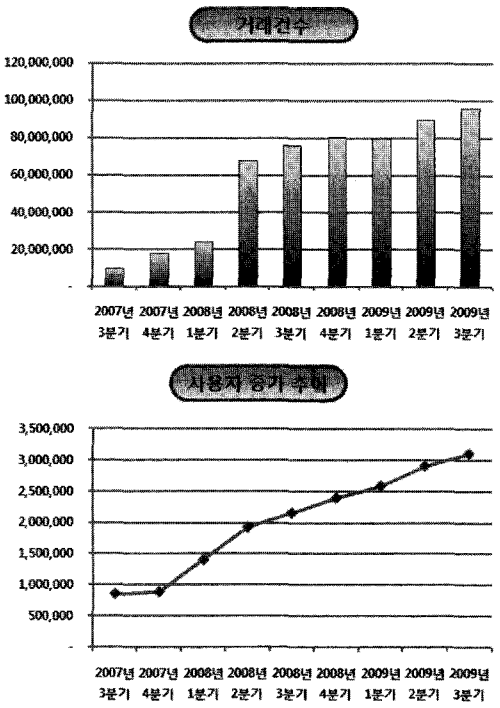


〔그림 3〕 인터넷이용률 및 이용자수 변화추이(%, 천명)

인터넷을 이용할 수 없는 신체적, 정신적 문제와 같은 경우를 제외한 거의 대부분의 국민이 인터넷을 이용하고 있음을 알 수 있다.

이와 같이 대부분의 국민이 인터넷을 이용하게 되면서 인터넷을 이용한 금융거래인 인터넷뱅킹 서비스도 함께 이용하는 경우가 증가하고 있다. 그 중에서도 가장 높은 등급의 보안성을 제공하는 OTP 사용 증가 추이를 보면 다음과 같다[9].

위의 그림은 '07년부터 '09년까지의 분기별 전자금융거래를 위해 이용되는 OTP 사용량의 증가율을 나타낸 그래프이다.



〔그림 4〕 OTP 거래 건수 및 사용자 증가 추이

〔표 7〕 보안서비스 사용자 증가 추이

구분	증가율	추정 가중치	사용자수				
			2009	2010	2011	2012	2013
사용자 증가	44%	90%	2,796,518	3,624,287	4,697,076	6,087,410	7,889,283

※ 당해년도 사용자 수 = (전년도 사용자 수 + (전년도 사용자수 * 증가율)) * 추정 가중치

금융보안연구원 OTP통합인증센터가 발표한 OTP 거래 통계에 따르면, 2009년 3분기 기준 310만 7,243개의 OTP가 금융거래에 이용되고 있으며, 이로 인한 누적 거래건수는 5억 4,354만 5,579건에 이르는 것으로 집계되었다.

2009년 3분기 OTP 사용자 수는 2008년 3분기의 215만 8,730명 대비 44% 증가했고, OTP를 이용한 자금이체 등의 거래건수는 9,596만 6,305건 발생하였다. 2008년 3분기 누적 거래건수가 1억 9,807만 9,875건이었던 것을 감안하면, 1년 사이에 무려 174%나 증가하였다. 이와 같은 결과를 보면 전체 인터넷 사용자 중 8.4%의 인원이 OTP를 활용한 전자금융거래를 이용하고 있다.

전자금융거래의 특성상 OTP를 활용하게 될 경우, 보안상의 이유로 인해 안티바이러스 시스템을 함께 활용하게 된다. 따라서 OTP를 활용한 전자금융거래 사용자들은 보안서비스를 이용하는 사용자라고 가정할 수 있다.

위의 자료를 바탕으로 S-SLA 적용 시 특정 서비스의 사용자 증가율을 분석하면 다음과 같다.

사용자 증가와 관련하여 증가율 수치는 앞서 전자금융거래시 OTP를 이용한 사용자의 증가율을 적용하였다. 그러나 보안서비스에서의 증가율은 OTP의 그것과 동일하다고는 할 수 없다. 보안서비스 사용자의 사용 빈도를 고려하였을 때, 모든 사용자가 안티바이러스 시스템을 이용하고 이에 대한 S-SLA를 준수한다고 볼 수 없기 때문에, 90%의 추정 가중치를 부여하였다.

이에 따라 2009년 OTP 이용 전자금융거래 사용자 310만 7,243명의 90%인 279만 6,518명이 보안서비스 사용자의 수치로 추정되며, 이에 증가율과 추정 가중치를 연산하여 2013년까지의 사용자수 추정치를 도출하였다.

VI. 결 론

보안서비스에 대한 S-SLA의 개념은 상대적으로 새롭게 인식되고 있으며, 이에 대한 측정지표 역시 잘 정립되어 있지 않다.

일반적인 SLA에서는 기밀성, 가용성, 무결성 등에 대한 보안사항을 고려하도록 권고하고 있으나, 실제적으로는 각 서비스 특성에 따른 보안특성 분석의 어려움으로 인하여 잘 다루어지지 않고 있다.

이에 따라 서비스 제공자 및 사용자가 보안서비스를 안전하고 효율적으로 이용하기 위해 S-SLA가 어떻게 적용될 수 있는지에 대한 연구가 필요하다.

따라서 본 논문에서는 보안서비스의 품질 제고를 위해 정보보호 서비스 제공자와 사용자 사이의 SLA에서 다루어져야 할 안티바이러스 시스템에 대한 S-SLA 지표를 개발하고, 사용자가 원하는 보안서비스 수준의 다양화를 위한 등급화 방안을 제안하였다.

본 논문에서 제안한 S-SLA의 적용은 사업자와 사용자간의 서비스 수준에 대한 규정화된 협약을 할 수 있게 하며, 사용자의 서비스 이용시 자신이 제공 받는 서비스가 최초 자신이 요구한 수준을 준수하는지에 대한 분명한 평가가 가능하게 한다.

S-SLA의 적용을 통해 서비스 제공 및 이용에 있어서 사업자와 사용자간의 서비스 수준에 대한 명확한 협의를 거치게 된다면, 서비스에 문제가 발생했을 경우, 최초 협의한 수준에서 벗어난 결과인지를 분석하고 책임 소재를 명확하게 구분할 수 있게 된다.

법적 분쟁의 소지를 감소하는 것은 사업자 및 사용자의 불필요한 경제적 시간적 손실을 막고, 사회적으로도 해당 서비스에 대한 불필요한 소모 논쟁 없이 원만한 해결을 가져올 수 있다.

본 논문에서는 보안서비스 제공에 필요하다고 판단되는 SLA 필수 지표항목들 개발하는데 초점이 맞추어져 있어 실제 사업환경에서 이를 적용하기 위해서는 추가적인 연구가 필요하다.

예를 들어, S-SLA 지표항목들을 실제 사업자 환경에 적용하기 위해서는 보안서비스 특성, 보안사업자 특성을 고려하여 서비스 등급을 분류하고 이러한 등급에 따라 S-SLA 지표 항목들을 묶어서 차등 운영하는 방안이나, 각 항목들을 등급화하여 운영하는 방안에 대한 고려가 필요하다.

또한 SLA 지표항목은 측정 가능한 항목들이 도출되어야 하고 측정 방법들이 명확히 제시되어야 하는데, 본 논문의 범위는 S-SLA 지표항목들을 도출하는 것으로 현재 측정방법, 측정기준 및 환경 구성방법 등이 제시되지 않았으므로 향후 이러한 항목들이 제시될 필요가 있다.

제시되는 지표항목들을 실제 사업자 환경에 권고하고 적용하기 위해서는 좀 더 포괄적인 정책입안자, 유관기관, 사업자들의 의견수렴 과정을 도입하여 현실적으로 적용 가능한 지표항목부터 시작하여 좀 더 많은 수의 지표항목을 관리토록 하는 방식으로 점차 수준을 높여가거나, 서비스 특성이나 운영환경 또는 제공되는 서비스 용도에 따라 S-SLA 항목과 그 권고 기준값을 엄밀하게 또는 느슨하게 가져가는 등의 탄력적인 적용방안 고려가 필요하다.

참고문헌

[1] SLA를 강화한 정보시스템 운영계약 참조모델, 한국정보화진흥원, 2006.

[2] 김대웅, 이길행, 김영선, "서비스수준협약(SLA) 기술동향," 전자통신동향분석, 제19권 제6호, pp. 55-65, 2004년 12월.

[3] 이스트소프트, 알약 2.0 and ASM 2.0 보안목표명세서, IT보안인증사무국, 2009년.

[4] 에스지에이, SGA-VC 2.0 Server and SGA-SC 2.0 for Antivirus 보안목표명세서, IT보안인증사무국, 2010년.

[5] 하우리, ViRobot Desktop 5.5 And ViRobot ISMS 3.5 for anti-virus 보안목표명세서 V1.2, IT보안인증사무국, 2009년.

[6] 2010 정보화통계집, 한국정보화진흥원, 2010년.

[7] 2009년 인터넷이용실태조사, 한국인터넷진흥원, 2009년.

[8] OTP 거래 현황, 금융보안연구원, 2010년.

[9] End-user Multimedia QoS Categories, ITU-T Rec. G.1010, 2001.

[10] Network Performance Objective for IP-based Service, ITU-T Y.1541, 2006.

[11] Guideline for Attributes and Requirements for Interconnection between Public Telecommunication Network Operators and Services Provider involved in Provision of Telecommunication Services, ITU-T Y.140.1, 2004.

[12] Measurements in IP Networks for Inter-domain Performance Assessment,

ITU-T Y.1543, 2007.

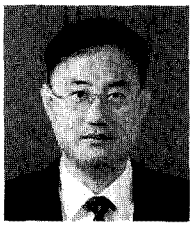
[13] Bill Pepper, "Security Service Level Agreements For Outsourced Security Functions," Information Security Technical Report, Vol. 1, No.3, pp 48-50, 1996.

[14] Ganna Frankova, "Service Level Agreements: Web Services and Security," Proc. of the 7th International Conference on Web Engineering, LNCS 4607, pp. 556-562, 2007.

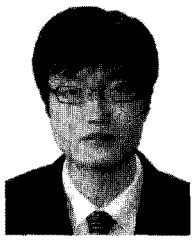
[15] Internal SLA (Service Level Agreements) for Information Security, SANS Institute InfoSec Reading Room, 2001.

[16] SLA Management Handbook, The Open Group, Vol. 4, 2004.

〈著者紹介〉

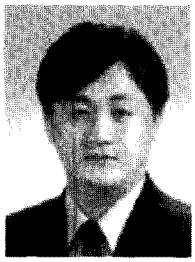


이 완 석 (Wan-Suck Yi) 특별회원
1991년 5월: Va. Tech. 전산과학과 학사 졸업
2001년 2월: 동국대학교 정보보호학과 석사 졸업
2004년 9월~현재: 성균관대학교 전자공학과 박사과정
1994년 7월~96년 6월: 현대정보기술 사원
1996년 7월~현재: 한국정보보호진흥원 인터넷서비스보호팀장
〈관심분야〉 정보보증, 정보보호 제품 평가, 정보통신기반보호, 신규 IT서비스 보호 등



이 동 범 (Dongbum Lee) 학생회원
2008년 2월: 순천향대학교 정보보호학과 학사 졸업
2010년 2월: 순천향대학교 정보보호학과 석사 졸업
2010년 3월~현재: 순천향대학교 정보보호학과 박사과정
〈관심분야〉 정보보호, 보안성 평가, 전자여권 보안 등

원 동 호 (Dongho Won) 평생회원
1976년: 성균관대학교 전자공학과 학사 졸업
1978년: 성균관대학교 전자공학과 석사 졸업
1988년: 성균관대학교 전자공학과 박사 졸업
1978년~1980년: 한국전자통신연구원 전임연구원
1992년~1994년: 성균관대학교 전자계산소 소장
1995년~1997년: 성균관대학교 교학처장
1997년~1998년: 정보화추진위원회 자문위원 (발령 정보화추진위원회 위원장 국무총리)
1999년~2001년: 성균관대학교 정보통신대학원 원장
2002년~2003년: 한국정보보호학회 회장
2002년~2004년: 대검찰청 컴퓨터 범죄 수사 자문위원
2002년~2004년: 성균관대학교 연구처장
2002년~2003년: 감사원 IT 감사 자문위원
2002년~2004년: 산학연 정보보안협의회 회장
2005년~현재: 정보보호인증기술연구소 소장
2005년~2008년: 한국정보보호진흥원 이사
2009년~현재: 성균관대학교 BK21 사업단장
〈관심분야〉 암호이론, 정보이론, 정보보호 등



곽 진 (Jin Kwak) 종신회원
1994~2006년: 성균관대학교 전자공학과(공학사 공학석사, 공학박사)
2006~2006년: 일본 큐슈대학교 방문연구원
2006~2006년: 일본 큐슈시스템 정보기술연구소 특별연구원
2006~2007년: 정보통신부 개인정보보호기획단 개인정보보호팀 통신사무관
2007~2009년: 정보통신연구진흥원 집필위원
2009~2009년: 순천향대학교 공과대학 교학부장
현재: 정보통신산업진흥원 기술평가위원, 디지털아이디관리포럼 기술평가위원, 한국정보통신기술협회 JTC/SC27 분과 기술위원, 한국정보통신기술협회 표준화 로드맵 기술표준기획 전담반 기술위원, 순천향대학교 정보보호학과 학과장, 순천향BIT 창업보육센터 소장, 사)국제정보능력평가원 쇼핑몰 플래너 자격 검정 출제 및 채점위원, 한국인터넷진흥원 미래융합IT서비스 보안연구회 스마트그리드 보안 분과 기술위원, 교육과학기술부 국가기술 수준 평가 전문위원, 한국과학기술정보연구원 충남 과학기술 정보협의회 전문위원, 지식경제부 지식경제기술혁신평가단 평가위원
〈관심분야〉 암호프로토콜, RFID 시스템 응용보안, 개인정보보호, 정보보호제품평가, 클라우드 컴퓨팅보안 등