웹기반 시스템의 보안감리프로세스 모델에 관한 연구

윤상현, 장은정, 권호열

강원대학교 전기전자정보통신공학부

A Study on Security Auditing Process Model for Web-Based Information System

Sanghyun Youn, Eunjeong Chang, Ho Yeol Kwon

Dept. Electrical and Computer Engr., Kangwon National University

E-mail : hykwon@kangwon.ac.kr

요 약

인터넷 기술을 기반으로 하는 웹기반 시스템은 웹 브라우저를 이용한 편리한 사용성과 하이퍼링크를 이용한 효과적인 연결성을 TCP/IP 네트워크 위에서 경제적으로 제공함으로서 최근 급속히 개발이 증가하고 있다. 그러나 운영환경에서 서버 측의 다양한 플랫폼과 운영체제, 그리고 클라이언트 측의 다양한 웹 브라우저가 혼재되어 존재하는 웹기반 정보시스템의 특성은 정보시스템의 개발 뿐 만 아니라 감리에서도 기존의 메인프레임 및 클라이언트/서버 시스템의 경우와 다른 특성을 갖는다. 본 논문에서는 웹기반 정보시스템의 특성과 보안감리 규격인 SSE-CMM의 프로세스 모델에 대하여 분석한 후 웹기반 정보시스템의 보안감리를 위한 새로운 프로세스 모델에 대하여 논하였다.

1. 서론

인터넷 기술을 기반으로 하는 웹기반 시스템은 웹 브라우저를 이용한 편리한 사용성과 하이퍼링크를 이용한 효과적인 연결성을 TCP/IP 네트워크 위에서 경제적으로 제공함으로서 최근 개발이 증가하고 있으며, 이들 웹기반 정보시스템은 운영환경에서 서버 측의 다양한 플랫폼과 운영체제, 그리고 클라이언트 측의 다양한 웹 브라우저가 혼재되어 존재하는 아키텍처 상의 특성 때문에 기존의 메인프레임 및 클라이언트/서버 시스템의 경우와 구별된다.

이들 정보시스템은 초기의 단순한 기술적인 현안 해결수준에서 벗어나 조직과 사회의 경쟁력 및 생산성을 좌우하는 핵심 기반시설의 일부로 인식되기 시작하면서, 정보시스템의 안전성, 효율성 및 효과성 향상을 위하여 정보시스템의 구축과 운영에 관한 사항을 종합적으로 점검 및 평가하고 감리의뢰인 및 피감리인에게 개선이 필요한 사항을 권고하는 정보시스템 감리의 중요성이 커지고 있다.[1]

정보시스템의 개발 및 구축에 대한 감리는 보통 프로젝트 관리, 시스템 아키텍처, 데이터베이스, 응용시스템, 보안 등 5개 분야로 나뉘어 진행되는데, 이 중에서 보안 감리는 정보시스템의 보안상 취약점 및 위협요소를 식별하고 개선함으로써 정보시스템의 안전성을 보증하는 역할을 수행한다.

보안감리에 대한 연구는 ISO/IEC 12207, ISO/IEC TR 15504 (SPICE), ISO/IEC TR 13335 (GMITS), BS7799/ISO17799, SSE-CMM 등의 국제적으로 인정되는 표준규격을 중심으로 이루어져 왔으며, 이 가운데 SSE-CMM은 보안 감리 프로세스의 능력 수준을 5단계로 결정하고 프로세스 개선의 방향을 제시한다는 점에서 주목받고 있다.

본 연구는 정보통신부와 한국소프트웨어공학협회의 "한•카네기멜론 S/W 전문인력교육 국내보급사업"의 지원으로 수행되었음.

본 논문에서는 웹기반 정보시스템의 특성과 보안감리 규격인 SSE-CMM의 프로세스 모델에 대하여 분석한 후 웹기반 정보시스템의 보안감리를 위한 새로운 프로세스 모델에 대하여 논하였다.

2. 본론

2.1 웹기반 시스템

기존의 메인프레임 또는 클라이언트/서버 스타일의 정보시스템에 비교할 때 웹기반 시스템은 다양성 및 복잡성이 크게 증가한 특징을 갖는다. 예를 들어 그림 1와 같은 아키텍처를 갖는 웹기반 시스템은 다양한 운영체제(Linux, Unix, Windows), 웹 서버(MS IIS, Apache), 응용 서버(WebLogic, ASP, WebSphere), 미들웨어(Tuxedo, CORBA, DCOM), 전자상거래 서버(Ariba, BroadVision), DB 서버(SQL, Informix, Oracle, Sybase), ERP(PeopleSoft, Oracle, Seibel, SAP) 등 주요 백오피스 서버, 방화벽, 브라우저(AOL, Explorer, Mosaic, WebTV) 등으로 구성되며, 웹서비스를 구현하는 프로그래밍 언어(HTML, Java, EJB, Java Script, PHP, CGI) 및 프로토콜(HTTP, HTTPS, SSL, FTP, ADO, ODBC)도 매우 다양하여 서로 이질적인 구성요소들이 통합 및 상호연동되어 정보서비스를 제공한다.[2]

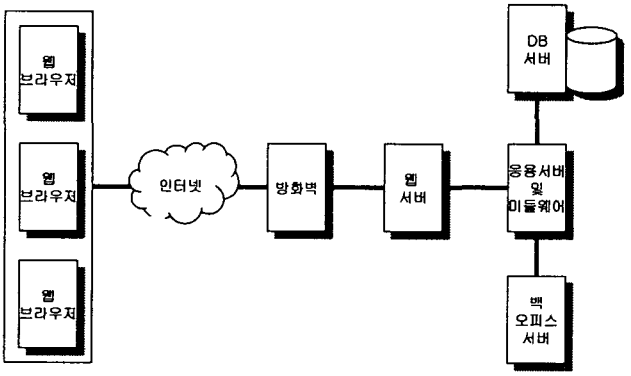

그림 1. 웹기반 시스템의 아키텍처

웹기반 정보시스템에서는 이질적인 구성요소들을 효과적으로 통합하고 소프트웨어 재사용성을 극대화할 수 있도록 공통된 프레임워크와 표준화된 인터페이스를 갖는 컴포넌트 기반 개발 방법을 사용하는 것이 일반적이다. 그림 2 는 전형적인 웹기반 정보시스템의 아키텍처를 위한 프레임워크의 예를 보여준다.[3]

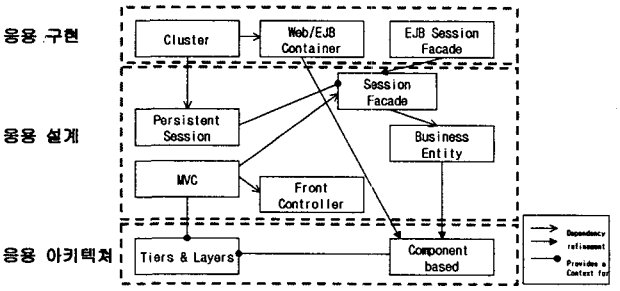

그림 2. 웹기반 시스템의 패턴 프레임워크

웹기반 정보시스템의 개발에 있어서 만족되어야 할 주요 품질 속성은 목표 서비스를 제공하는 기능성 외에도 신뢰성, 사용성, 보안성, 가용성, 확장성/호환성, 유지보수성, 성능 및 개발기간 등이다.[4] 특히 보안성은 웹기반 시스템에 대한 의도적 및 비의도적인 공격에 대하여 전반적인 보안 방어 시스템이 효과적으로 운영되고 있다는 것을 보증하는 것으로서 시스템의 취약점 분석, 위협의 평가, 보안대책의 설계 및 구축 등의 프로세스를 통하여 구현된다.

2.2 SSE-CMM 프로세스 모델

소프트웨어 능력성숙도 모델(SW-CMM)[5]과 유사한 프레임워크를 갖는 SSE-CMM[6]은 정보시스템 보안의 설계 및 개발 프로세스의 능력성숙도모델로서 보안공학 프로세스의 개선, 보안공학 능력평가, 프로세스 기반의 보증의 제공 등을 목표로 1993년부터 미국정부 및 산업계가 참여하여 개발하기 시작하였으며, 1999년에 SSE-CMM V2.0 이 발표되어 현재 사용되고 있다.

SSE-CMM 모델은 능력수준(Capability Level)과 프로세스 영역(Domain)의 2개 차원을 갖는다. SSE-CMM 의 능력 수준은 그림 3 에 나타낸 것과 같이 미실행(수준 0), 비정형적 실행(수준 1), 계획 및 추적(수준 2), 우수한 정의(수준 3), 정량적 통제(수준 4), 지속적 개선(수준 5) 등의 6 가지 수준으로 표현되며, 각 수준마다 공통특징(CF)과 이를 달성하기 위한 일반활동(GP)이 존재한다.

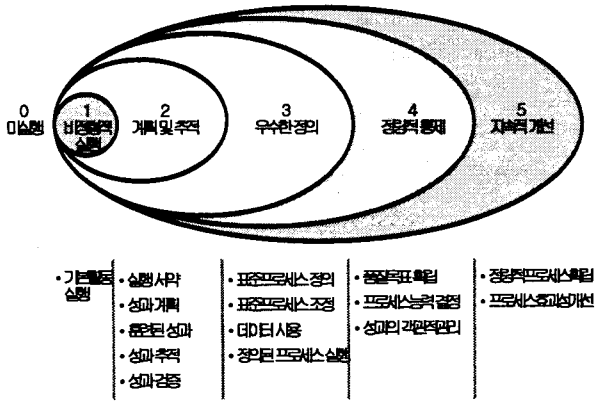

그림 3. SSE-CMM 능력 성숙도 모델

SSE-CMM의 프로세스영역(PA)은 보안공학 프로세스 (PA01-PA11), 프로젝트 프로세스(PA12-PA16), 조직 프로세스 (PA17-PA22) 등 3개의 프로세스 범주로 이루어져 있으며, 이들 프로세스 범주는 22개 프로세스 영역, 128개 프로세스로 구성되어 있다. 각 프로세스 영역에 대한 목표(Goal)와 기본활동(BP)은 표 1 에 나타낸 바와 같다.

표 1. SSE-CMM의 프로세스: 보안공학 범주

PA01 행정적 보안 통제	*Goal 1*	보안통제가 적절하게 배치되어 사용됨
	BP.01.01	보안통제의 책임자가 확립되고 이들이 조직내 인원과 의사소통
	BP.01.02	시스템 보안 통제의 형상을 관리
	BP.01.03	사용자 및 관리자를 위한 보안 경고, 훈련, 및 교육 프로그램 관리
	BP.01.04	보안서비스 및 통제기구의 주기적인 유지보수 및 관리
PA02 영향도 평가	*Goal 1*	시스템의 위험에 대한 보안의 영향을 식별하고 특성을 분석함
	BP.02.01	시스템에 의한 운영/사업 또는 미션 능력을 식별, 분석 및 우선순위화
	BP.02.02	주요 보안목적을 지원하는 시스템 자산의 식별 및 특성분석
	BP.02.03	평가에 사용될 영향도 메트릭의 선정
	BP.02.04	선정된 평가용 메트릭과 메트릭 변환인자 간의 관계를 식별
	BP.02.05	영향도의 식별 및 특성분석
	BP.02.06	영향도의 변화를 감시
PA03 보안 위험의 평가	*Goal 1*	정의된 환경에서 운영되는 시스템의 보안 위험을 이해
	Goal 2	정의된 방법론에 따라 위험을 우선순위화
	BP.03.01	보안위험 평가대상 시스템을 위한 방법론, 기법, 평가기준을 선정
	BP.03.02	위협/취약점/영향도의 식별
	BP.03.03	노출 발생과 관련된 위험의 평가
	BP.03.04	노출된 위험과 관련된 불확실성 평가
	BP.03.05	위험의 우선순위화
	BP.03.06	위험의 종류 및 특성의 변화를 감시
PA04 위협의 평가	*Goal 1*	시스템의 보안 위협을 식별하고 특성을 분석함
	BP.04.01	자연적 원인에 의해 발생하는 위협을 식별
	BP.04.02	인공적 원인에 의해 발생하는 의도적/비의도적 위협을 식별
	BP.04.03	특정 환경에서 적용되는 범위 및 측정 단위를 식별
	BP.04.04	인공적 원인의 위협의 대리자 능력 및 동기 평가
	BP.04.05	위협 사건의 발생 가능성을 평가
	BP.04.06	위협의 종류 및 특성의 변화를 감시
PA05 취약점 평가	*Goal 1*	정의된 환경의 시스템 보안 취약점을 이해함
	BP.05.01	보안시스템 취약점 분석을 위한 방법론, 기법, 평가기준의 선정
	BP.05.02	시스템 보안 취약점의 식별
	BP.05.03	취약점 관련 데이터의 수집
	BP.05.04	시스템 취약점의 평가 및 특정 취약성들의 결합에 의한 취약점 종합
	BP.05.05	발생가능한 취약점의 종류 및 특성의 변화를 감시
PA06 보증 논의의 구축	*Goal 1*	작업산출물과 프로세스가 고객의 보안요구를 충족하는 증거를 제공
	BP.06.01	보안 보증 목표의 식별
	BP.06.02	모든 보증 목표에 대한 보안보증 전략의 정의
	BP.06.03	보안 보증 증거의 식별 및 통제
	BP.06.04	보안 보증 증거의 분석 실행
	BP.06.05	고객의 보안요구를 충족하는 보안 보증 논의의 제공
PA07 보안의 조정	*Goal 1*	모든 프로젝트 팀원이 필요한 만큼 보안공학 활동에 참여함
	Goal 2	보안관련 결정 및 권고가 전달되고 조정됨
	BP.07.01	보안공학 조정에 대한 목표와 관계의 정의
	BP.07.02	보안공학을 위한 조정기구의 식별
	BP.07.03	보안공학 조정의 제공
	BP.07.04	식별된 기구를 보안관련 결정 및 권고에 사용
PA08 보안 사태의 감시	*Goal 1*	내외부 보안관련 사건의 검출 및 추적
	Goal 2	정책에 따라 보안사고에 대응
	Goal 3	운영보안 사태의 변화를 식별하고 보안목적에 따라 처리
	BP.08.01	사건 및 잠재적 사건의 원인 결정을 위한 사건기록의 분석
	BP.08.02	위협, 취약점, 영향, 위험, 및 환경의 변화를 감시
	BP.08.03	보안관련 사고의 식별
	BP.08.04	보안 보호장치의 성능 및 기능 효과성의 감시
	BP.08.05	필요한 변화를 식별하기 위한 보안 사태의 검토
	BP.08.06	보안관련 사고의 대응을 관리
	BP.08.07	보안감시 관련 장치가 적절히 보호되는지 보증
PA09 보안 입력의 제공	*Goal 1*	모든 시스템 이슈를 보안관점에서 검토하고 보안목적에 따라 해결
	Goal 2	모든 프로젝트팀원이 자신의 기능을 수행하도록 보안을 이해
	Goal 3	보안 솔루션은 제공된 보안입력사항을 반영
	BP.09.01	보안입력요구의 공통이해를 위해 설계자, 개발자, 사용자와 작업
	BP.09.02	개발방법 선택에 필요한 보안 제약 및 고려사항의 결정
	BP.09.03	보안관련개발문제의 대안적 솔루션 식별
	BP.09.04	보안 제약 및 고려사항을 이용한 공학대안의 분석 및 우선순위화
	BP.09.05	다른 공학그룹에게 보안관련 지침을 제공
	BP.09.06	운영시스템사용자 및 관리자에게 보안관련지침을 제공

PA10 보안 요구의 지정	*Goal 1*	고객을 포함한 관련자 모두가 보안요구사항을 공통적으로 이해
	BP.10.01	고객의 보안요구사항을 이해함
	BP.10.02	시스템을 지배하는 법규, 정책, 표준, 외부영향 및 제약을 식별
	BP.10.03	보안 배경을 결정하기 위한 시스템 목적을 식별
	BP.10.04	시스템운영관점에서 본 고수준 보안의 획득
	BP.10.05	시스템 보안을 정의하는 고수준 목표의 획득
	BP.10.06	시스템에 구현된 보호를 정의하는 일관된 기술문 정의
	BP.10.07	특정 보안이 고객요구를 만족한다는 계약의
PA11 보안의 검증 및 확인	*Goal 1*	솔루션이 보안 요구사항을 만족함
	Goal 2	솔루션이 고객의 운영 보안 요구를 만족함
	BP.11.01	검증되고 확인될 솔루션을 식별
	BP.11.02	각 솔루션의 검증 및 확인을 위한 접근방법 및 엄밀성의 수준 정의
	BP.11.03	솔루션이 이전 추상화수준에 관련된 요구사항을 구현하는 지 검증
	BP.11.04	솔루션이 이전 추상화수준 및 궁극적인 고객의 운영 보안요구를 만족하는 지 확인
	BP.11.05	다른 공학그룹을 위한 검증 및 확인 결과를 획득

표 2. SSE-CMM의 프로세스: 프로젝트 범주

PA11 보안의 검증 및 확인	*Goal 1*	솔루션이 보안 요구사항을 만족함
	Goal 2	솔루션이 고객의 운영 보안 요구를 만족함
	BP.11.01	검증되고 확인될 솔루션을 식별
	BP.11.02	각 솔루션의 검증 및 확인을 위한 접근방법 및 엄밀성의 수준 정의
	BP.11.03	솔루션이 이전 추상화수준에 관련된 요구사항을 구현하는 지 검증
	BP.11.04	솔루션이 이전 추상화수준 및 궁극적인 고객의 운영 보안요구를 만족하는 지 확인
	BP.11.05	다른 공학그룹을 위한 검증 및 확인 결과를 획득
PA12 품질 보증	*Goal 1*	프로세스 품질의 정의 및 측정
	Goal 2	기대된 작업 산출물 품질의 달성
	BP.12.01	정의된 프로세스에 대한 적합성 감사
	BP.12.02	작업 산출물 품질의 측정
	BP.12.03	프로세스 품질의 측정
	BP.12.04	품질 측정치의 분석
	BP.12.05	참여의 획득
	BP.12.06	품질 개선 활동의 개시
	BP.12.07	시정 조치의 필요 검출
PA13 형상 관리	*Goal 1*	작업산출물 형상에 대한 통제의 유지
	BP.13.01	형상관리 방법론의 확립
	BP.13.02	형상단위의 식별
	BP.13.03	작업 산출물 기준선의 유지
	BP.13.04	변경 통제
	BP.13.05	형상 상태에 대한 의사소통
PA14 프로젝트 위험 관리	*Goal 1*	프로그램에 대한 위험의 식별, 이해, 및 완화
	BP.14.01	위험관리 접근방법의 개발
	BP.14.02	위험식별
	BP.14.03	위험평가
	BP.14.04	위험평가 검토
	BP.14.05	위험완화 실행
	BP.14.06	위험완화 추적
PA15 기술 인력의 감시 및 통제	*Goal 1*	기술 인력의 감시 및 통제
	BP.15.01	직접적인 기술적 인력
	BP.15.02	프로젝트 자원의 추적
	BP.15.03	기술 파라미터의 추적
	BP.15.04	프로젝트 성능의 검토
	BP.15.05	프로젝트 이슈의 분석
	BP.15.06	시정조치 실시
PA16 기술 인력의 계획	*Goal 1*	모든 측면의 기술 인력의 계획
	BP.16.01	핵심 자원의 식별
	BP.16.02	프로젝트 범위 산정
	BP.16.03	비용 산정치의 개발
	BP.16.04	프로젝트의 프로세스 결정
	BP.16.05	기술적 활동의 식별
	BP.16.06	프로젝트 인터페이스의 정의
	BP.16.07	프로젝트 일정의 개발
	BP.16.08	기술적 파라미터의 확립
	BP.16.09	기술적 관리 계획의 개발
	BP.16.10	프로젝트 계획의 검토 및 승인

표 3. SSE-CMM의 프로세스: 조직 범주

PA17 조직의 보안공학프로세스	*Goal 1*	조직을 위한 표준 시스템 공학 프로세스의 정의
	BP.17.01	프로세스 목표의 확립
	BP.17.02	프로세스 자산의 수집
	BP.17.03	조직을 위한 보안공학 프로세스의 개발
	BP.17.04	프로세스 재단 지침의 정의
PA18 조직의 보안공학프로세스 개선	*Goal 1*	표준 시스템 공학 프로세스의 개선이 계획되고 구현됨
	BP.18.01	프로세스의 심사
	BP.18.02	프로세스 개선의 계획
	BP.18.03	표준 프로세스의 변경
	BP.18.04	프로세스 개선사항의 의사소통
PA19 제품 라인 진화의 관리	*Goal 1*	제품라인이 자신의 궁극적인 목표를 향해 진화함
	BP.19.01	제품의 진화를 정의
	BP.19.02	새로운 제품기술의 식별
	BP.19.03	개발 프로세스에 적용
	BP.19.04	핵심 구성요소의 가용성을 보증
	BP.19.05	제품 기술에 삽입
PA20 시스템 공학 지원 환경의 관리	*Goal 1*	시스템공학 지원환경이 프로세스 효과성을 극대화함
	BP.20.01	기술적 주의상태 유지
	BP.20.02	지원 요구사항 결정
	BP.20.03	공학 지원환경 획득
	BP.20.04	공학 지원환경의 재단
	BP.20.05	신기술의 삽입
	BP.20.06	환경의 유지
	BP.20.07	공학 지원환경의 감시
PA21 현재 기법 및 지식의 제공	*Goal 1*	조직이 프로젝트 및 조직의 목표 달성에 필요한 기법을 보유함
	BP.21.01	훈련 수요의 식별
	BP.21.02	지식 또는 기법 획득 모드의 선정
	BP.21.03	기법 및 지식의 가용성 보증
	BP.21.04	훈련자료의 준비
	BP.21.05	인력 훈련
	BP.21.06	훈련의 효과성 평가
	BP.21.07	훈련 기록의 유지
	BP.21.08	훈련 자료의 유지
PA22 공급자와 조정	*Goal 1*	효과적인 공급자의 선정 및 이용
	BP.2201	시스템 구성요소 또는 서비스의 식별
	BP.22.02	우수한 공급자 또는 판매자의 식별
	BP.22.03	공급자 또는 판매자의 선택
	BP.22.04	기대치의 제공
	BP.22.05	의사소통의 유지

2.3 제안된 보안감리 프로세스

정보시스템 감리에서 자주 참조되는 ISO 12207은 소프트웨어 개발 생명주기(SDLC)는 모두 17개의 프로세스를 이루어져 있으며, 이들은 그림 4와 같이 주요 프로세스, 지원프로세스, 조직프로세스의 3개 프로세스 범주로 구분된다.[7]

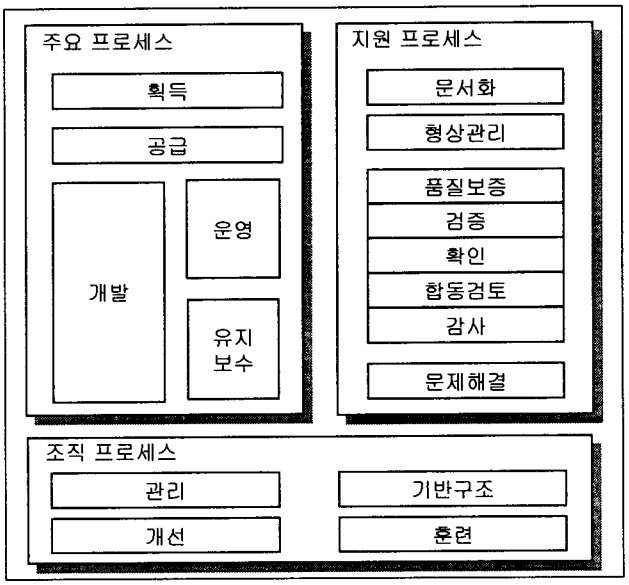

그림 4. ISO 12207 소프트웨어 생명주기

SSE-CMM 모델은 보안시스템의 개발 프로세스를 보안공학, 프로젝트, 조직의 3개 범주로 구분하며, 이들 범주에 속한 프로세스 영역과 ISO 12207 SDLC 프로세스 사이의 매핑은 표 4와 같다.

표 4에서 보는 바와 같이 SSE-CMM의 보안 프로세스는 주로 위험의 평가를 비롯한 개발(분석)프로세스에 집중되어 있으며, 개발 단계의 설계/구현

표 4. SSE-CMM 과 ISO 12207 의 매핑

범주	ISO 12207 프로세스	SSE-CMM 프로세스 영역	상관도
주요 프로세스	획득	PA22 공급자와 조정	O
	공급	PA22 공급자와 조정	O
	개발(계획)	PA06 보증 논의의 구축	O
	개발(계획)	PA19 제품라인 진화의 관리	O
	개발(분석)	PA02 영향도 평가	O
	개발(분석)	PA03 보안 위험의 평가	O
	개발(분석)	PA04 위협의 평가	O
	개발(분석)	PA05 취약점 평가	O
	개발(분석)	PA10 보안요구의 지정	O
	개발(설계)	PA09 보안 입력의 제공	△
	개발(구현)	PA09 보안 입력의 제공	△
	운영	PA08 보안 사태의 감시	O
	유지보수	PA01 행정적 보안통제	△
지원 프로세스	문서화	PA01 행정적 보안통제	X
	형상관리	PA13 형상 관리	O
	품질보증	PA12 품질 보증	O
	검증	PA11 보안의 검증 및 확인	O
	확인	PA11 보안의 검증 및 확인	O
	합동검토	PA07 보안의 조정	△
	감사	PA18 조직의 보안공학프로세스 개선	O
	문제해결	PA07 보안의 조정	△
조직 프로세스	관리	PA14 프로젝트 위험 관리	O
	관리	PA15 기술 인력의 감시 및 통제	O
	관리	PA16 기술 인력의 계획	O
	관리	PA17 조직의 보안공학프로세스	O
	개선	PA18 조직의 보안공학프로세스 개선	O
	기반구조	PA20 시스템공학 지원환경의 관리	O
	훈련	PA21 현재 기법 및 지식의 제공	O

* 상관도: O: 크다, △: 중간, X: 작다.

프로세스 및 문서화 프로세스는 상대적으로 빈약함을 알 수 있다. 따라서 웹기반 정보시스템을 위한 효과적인 보안감리를 위해서는 SSE-CMM 에 규정된 기존의 프로세스 외에 추가적인 프로세스를 더 정의하여 사용하는 것이 필요하다. 표 5는 SSE-CMM의 'PA09 보안 입력의 제공' 프로세스를 웹기반 시스템의 설계 및 구축을 위한 보안 감리 프로세스인 'PA09+ 보안 입력의 제공'으로 확장한 예이다.

표 5. 수정된 SSE-CMM 프로세스의 예

PA09+ 보안 입력의 제공	*Goal 1*	모든 시스템 이슈를 보안관점에서 검토하고 보안목적에 따라 해결
	Goal 2	모든 프로젝트팀원이 자신의 기능을 수행하도록 보안을 이해
	Goal 3	보안 솔루션은 제공된 보안입력사항을 반영
	Goal 4	보안 솔루션의 아키텍처 설계
	BP.09.01	보안입력요구의 공통이해를 위해 설계자, 개발자, 사용자와 작업
	BP.09.02	개발방법 선택에 필요한 보안 제약 및 고려사항의 결정
	BP.09.03	보안관련개발문제의 대안적 솔루션 식별
	BP.09.04	보안 제약 및 고려사항을 이용한 공학대안의 분석 및 우선순위화
	BP.09.05	다른 공학그룹에게 보안관련 지침을 제공
	BP.09.06	운영시스템사용자 및 관리자에게 보안관련지침을 제공
	BP.09.07	보안 솔루션을 위한 아키텍처 및 패턴프레임워크 선정
	BP.09.08	보안 솔루션을 위한 세부 설계
	BP.09.09	보안 솔루션을 위한 단위 모듈 구현 및 시험
	BP.09.10	보안 솔루션을 위한 시스템 통합 및 시험

3. 결론

본 연구의 주제와 관련하여 향후 연구되어야 할 사항은 ISO 12207 소프트웨어 개발 생명주기의 관점에서 보안감리 관련 규격들의 프로세스간 특성을 비교하는 것과 함께 본 논문에서 제안된 프로세스를 실제로 감리에 적용하여 얻어진 결과를 통하여 검증하는 연구 등이다.

[참고문헌]

[1] 문대원, 장시영, 정보시스템 감리: 사업관리, 시스템 개발 및 감리 실무, 명경사, 1998, pp. 15-37.

[2] H.Q. Nguyen, Testing Applications on the Web, Wiley, 2001, pp. 3-56.

[3] 오찬주, 아키텍처 패턴 프레임워크, 웹기반 소프트웨어공학, 한국소프트웨어공학협회, 2003, pp. 93-178.

[4] J. Offutt, Testing Web Software Applications, 2003 한국정보과학회 소프트웨어공학회 튜토리얼 발표집, 서울, 2003. 6.17., pp.3-43.

[5] M.C. Paulk, B. Curtis, M.B. Chrissis, and C.V. Weber, "Capability Maturity Model for Software, Version 1.1", Software Engineering Institute, CMU/SEI-93-TR-24, Feb. 1993.

[6] Systems Security Engineering CMM (SSE-CMM) Ver. 2.0, Apr. 1999

[7] Information technology - Software life cycle processes, ISO/IEC 12207, Aug. 1995.