通信情報保護學會誌
第9券 第2號, 1999. 06

보호공학 방법론에 관한 연구

이 영화*, 이 남용**

요 약

최근 발생한 많은 정보 시스템 침해 사고로 인해 특정 목적·환경에 맞게 개발된 상용 보호 제품의 추가만으로는 시스템을 효과적으로 보호할 수 없다는 것이 실증되었다. 따라서, 조직의 정보 시스템 환경에 보다 뛰어난 보호를 제공하기 위한 보호 관련 활동을 시스템 개발 과정과 통합하여 초기단계부터 중요하게 고려해야 한다는 주장이 널리 제기되었다. 이를 위해 시스템 개발 초기단계부터 운용유지에 이르는 전 단계에 걸쳐 안전한 시스템 구축을 위한 체계적인 보호공학 방법론이 필요하게 되었다. 본 논문에서는 획득자를 대상으로 시스템 수명 주기 전반에 걸쳐 단계별로 고려해야할 보호 고려사항과 수행활동을 체계화한 시스템 개발 기반 보호공학 방법론을 소개한다.

Ⅰ. 서 론

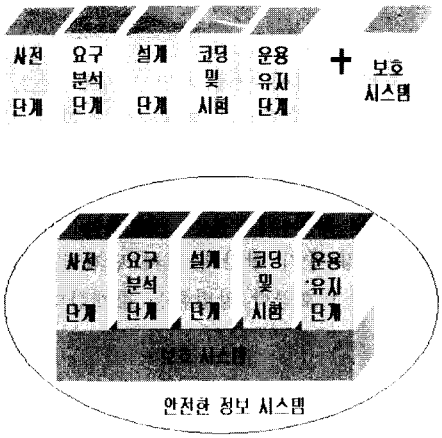
일상적인 조직의 업무가 정보 시스템에 크게 의존하게 되었음에도 불구하고 과거 각 조직에서는 정보 시스템 침해 위협을 심각하게 고려하지 않았으며, 보호 기능의 추가로 인한 시스템 성능 손실, 시스템 수행 활동에 대한 유연성 훼손, 보호 요구사항의 분석, 시스템 명세의 설계와 구현 및 운용유지 등에 상당한 비용 소요 등을 이유로 대개 시스템 개발 완료 후 상용 보호 제품을 추가하는 방식을 선호하였다. 그러나, 최근 발생한 많은 침해 사고로 인해 특정 목적·환경에 맞게 개발된 상용 보호 제품의 추가만으로는 정보 시스템을 효과적으로 보호할 수 없다는 것이 실증되었다. 따라서 조직의 정보 시스템 환경에 맞는 보다 뛰어난 보호 서비스를 제공하기 위해 보호 시스템의 도입을 시스템 개발 과정과 통합하여 초기단계부터 중요하게 고려해야 한다는 주장이 널리 제기되었다.[1,2] 그러나, 다음과 같은 이유로 아직까지 보호 시스템을 정보 시스템에 효과적·효율적으로 통합하는 체계화된 방법론이 제시되지 못하였다.

● 현재의 시스템 개발 방법론에서는 보호 시스템을 시스템 개발 과정의 일부분으로서 고려하지 않는다. 따라서, 현재 정보 시스템 개발시에 보호 시스템은 단지 기반 플랫폼의 보호 기능에 의존하거나 시스템 개발 후에 별도의 상용 보호체계를 추가(Add-on)하는 방식으로 도입되고 있다.[3] 그러나, 상용 보안 제품은 특정한 환경에서 운영되도록 설계된 특수 보호 기능과 인터페이스를 갖고 있기 때문에 각 정보 시스템 고유의 보호 요구사항을 완벽히 충족시키지 못한다는 문제점을 갖고 있다.[4] 또한, 기존의 시스템에 특정 보안 제품을 추가하는 경우 네트워크에 엄청난 로드를 초래하여 통신 두절 문제를 발생시키거나, 원래의 시스템 기능에 영향을 미쳐 초기 사용자 요구사항과 상이한 시스템을 초래할 수 있다.[5]

● 추가 방식의 보호 시스템 도입은 그 효과와 비용면에서 많은 비효율성을 초래한다. 최근 여러 연구에서는 기존 시스템에 보호 시스템을 추가하는 것은 시스템 개발 과정 초기부터 보호 시스템을 고려하는 것

* 국방과학연구소 yhnjy@unitel.co.kr ** 국방과학연구소 nylee@sunam.kreonet.re.kr

보다 10배 이상의 비용을 초래하며, 동시에 시스템 개발 초기부터 보호를 고려하는 것이 보다 뛰어난 보안성을 갖는 시스템을 구축한다는 연구 결과를 제시하였다.[6,7] 〈그림 1〉의 좌측은 보호 시스템을 시스템 개발 과정과 통합할 때 보다 안전한 정보 시스템이 구축된다는 것을, 우측은 보호 시스템을 시스템 개발 초기부터 고려하는 것이 비용 및 효과측면에서 뛰어나다는 것을 도시한다.



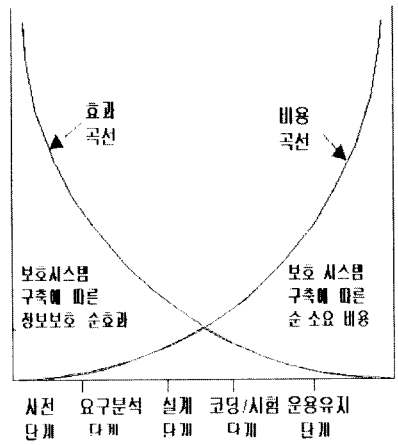


그림 1. 초기 개발 단계부터 보호 고려시 비용 대 효과 측면의 개선 효과

● 전체 시스템 개발 과정을 대상으로 한 체계적인 시스템 개발 기반 보호공학 방법론이 부재하였다. 즉, 현재까지의 보호공학 관련 연구는 주로 상용제품에 대한 평가·인증시 고려사항들을 체계화한 TCSEC[8],ITSEC[9],CC[10] 등 제품 중심의 보호 방법론 연구와, 시스템 개발 단계별로 수행해야할 보호 매카니즘에 대한 부분적인 연구만이 수행되었을 뿐 시스템 개발 전단계를 대상으로 한 보호공학 방법론에 대한 연구는 거의 수행되지 않았다.[3,4,11,12,13,14]

● 개발자 중심 혹은 특정 개발 방법론을 대상으로 한 보호공학 방법론만이 연구 제시되었다.[3,4,14] 즉, 과거의 보호공학 방법론은 시스템 개발자들이 시스템 개발 과정 각 단계에서 수행해야 할 보호 관련 활동들을 대상으로 하였다. 그러나, 이 경우 시스템 개발 전 단계에 걸쳐 요구된 대로 보호 시스템이 적절히 구현되고 있는지를 감독·평가하는 획득자 관점에서의 보호공학 활동 및 고려 사항들을 포함하지 못하였다.

이상에서와 문제점을 해결하기 위해 시스템 개발 초기단계부터 운용유지단계에 이르는 전 단계에 걸쳐 안전한 정보 시스템 구축을 위한 체계적인 보호공학 방법론에 대한 필요가 제기되었다.[2][11] 따라서, 본 논문에서는 시스템 수명 주기 전반에 걸쳐 단계별로 고려해야할 보호 고려사항과 수행활동을 체계화한 보호공학 방법론을 소개한다. 특히 본 논문은 획득자 중심의 보호공학 방법론에 초점을 맞춘다. 본 논문의 2장에서는 보호공학 방법론의 프레임워크를 제시하며, 3장에서는 보호공학 방법론의 세부 구성요소들에 대해 설명한다. 마지막으로 4장에서는 보호공학 방법론 적용시 중요 고려 사항들을 제시한다.

II. 보호공학방법론

보호공학 방법론은 시스템 개발 전 단계에 걸친 보호 고려 사항 및 수행활동들을 체계화한 프레임워크로서 개발 전 제안 요청서 작성 단계에서부터 시스템 유지 보수 및 폐기에 이르는 전 단계를 포괄한다. 보호공학 방법론은 크게 사전단계, 요구분석단계, 설계단계, 코딩/시험단계 및 운용유지단계로 구성되며, 각 단계별 보호공학 구성요소는 다음과 같다.

● 사전 단계 : 최고 경영층 및 조직 구성원의 지원 확보, 제안 요청서 작성 및 제안서 평가, 보호 전담 조직 구성, 사용자 교육

● 요구분석단계 : 보안 정책 수립, 초기 보안 요구사항 분석, 보안 운영 개념 설정, 위험 분석 실시, 보호 시나리오 작성, 최종 보안 요구사항 결정

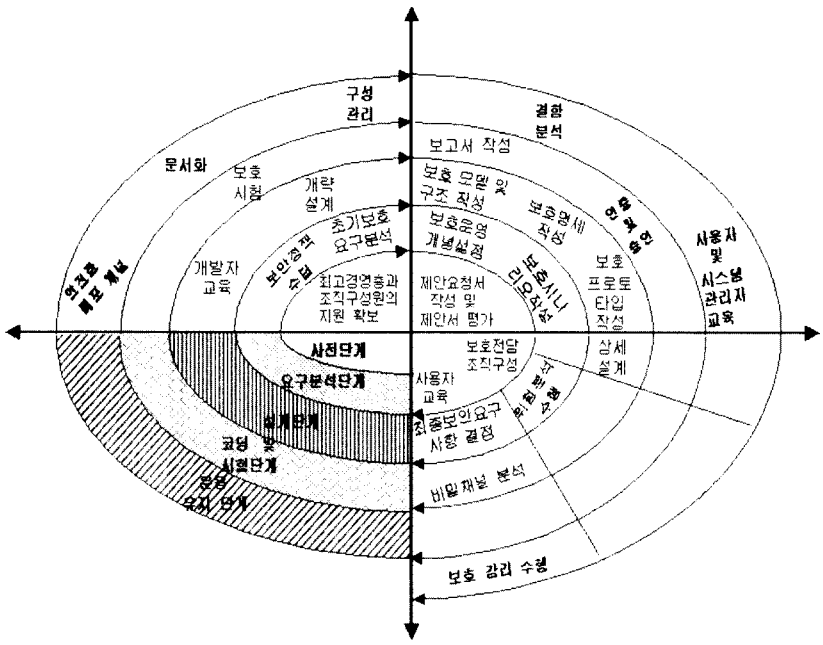


그림 2. 보호공학 방법론 프레임워크

● 설계단계 : 개발자 교육, 개략 설계, 보호 모델 및 구조 작성, 보호 명세 작성 및 프로토타입 개발, 상세 설계 수행, 비밀채널 분석

● 코딩 및 시험단계 : 보호 시험, 보고서 작성, 인증 및 승인 실시

● 운용유지단계 : 안전한 배포 채널 수립, 문서화, 구성 관리, 결함 분석, 사용자 및 시스템 관리자 교육, 보호 감리 수행

이상의 세부 구성요소를 갖는 보호공학 방법론 프레임워크는 <그림 2>와 같다.

보호공학 방법론은 계속적으로 변화하는 시스템 환경에 유연하게 대처할 수 있는 개방적·동적 구조로 작성되어야 한다. 따라서, 시스템 개발 과정에서 발생하는 요구사항 및 기술 변화, 환경 변화 등을 예측 및 관찰하고 이를 쉽게 수용할 수 있어야 하며, 피드백 과정을 통해 즉각적으로 대처할 수 있어야 한다. 보호공학 방법론은 시스템의 무결성, 기밀성 및 가용성과 관련된 모든 보호활동, 보호 관련 관리적, 물리적, 기술적 행위, 경제적, 법적 및 인적 측면 등을 모두 포괄하여야 하며, 보호에 간접적인 영향을 미칠 수 있는 비보호 관련 요소들도 수용하여야 한다.

Ⅲ. 세부구성요소

본 장에서는 보호공학 방법론의 세부 구성요소를 사전단계, 요구분석 단계, 설계단계, 코딩 및 시험단계, 운용유지단계로 분류하고 각 단계별 고려사항 및 수행 활동을 제시한다.

1. 사전 단계

시스템 개발 사전 단계에서는 최고 경영자 및 조직 구성원의 지원 확보, 보호 요구사항이 반영된 제안요청서 작성 및 제안서 평가, 프로젝트 수행 중 보호 활동을 조정·통제·평가할 보호 전담 조직 편성 등을 수행한다.

● 최고경영층 및 조직구성원 지원 확보

일반 조직에서 최고 경영층은 보호 시스템 구축에 대한 여러 가지 부정적 선입관을 갖고 있다. 즉, 정보 보호 시스템은 불필요한 관료주의 도입, 창조성 및 유연성의 제약, 막대한 비용 발생 및 낮은 생산성을 초래하며, 상용 시스

템 도입만으로도 충분히 보호 문제를 해결할 수 있다는 견해를 갖고 있다. 또한, 조직구성원들도 보호 시스템 도입이 개인의 자유와 조직의 일반 업무 절차의 유연성을 제약한다는 점에서 부정적인 시각을 갖고 있다. 따라서, 보호 관리자는 시스템 개발 활동에 앞서 최고 경영층 및 조직 구성원을 대상으로 보호 시스템의 필요성 및 도입 효과 등을 설득하는데 많은 노력과 시간을 기울여야 하며, 이를 통해 적극적인 지원을 확보할 수 있어야 한다.[15,16]

● 제안 요청서 작성 및 제안서 평가

제안 요청서 작성시 보호 관련 사항은 보호 관리자에 의해서 작성되며 기존에 시스템 개발 과정에서 축적한 경험, 유사한 업종 또는 시스템에서의 보호 활동, 국내·외 전문기관에서 제시한 Baseline Controls[17,18], Code of Practice[19] 등 일반 보호관련 기준, 보호 전문가 자문, 개발 비용 대 효과의 상충 관계 등에 대한 분석을 토대로 하여 작성하여야 한다. 제안 요청서 내에서 해당 시스템에 대한 보호 요구사항을 정확히 기술하는 것은 시스템 개발 단계에서의 추가적인 노력과 비용을 절감시켜주며, 개발자에 의한 적절한 자원할당을 유도할 수 있어 매우 중요하다.

각 개발기관에서 제출된 제안서에 대한 평가는 제안요청서의 요구조건 충족 여부, 구현 방법의 기술적·경제적 타당성, 해당 개발기관의 수행 능력 등을 전반적으로 평가하여야 하며, 필요시 이를 조직 내·외부의 전문가들로 구성된 평가기관에 의뢰하여 검증을 받아야 한다. 제안 요청서 작성시 고려하지 못했던 보호 요구사항이나, 환경 변화로 인해 추가될 요구사항들은 최종 개발업체 선정 및 계약 체결시까지 관련 업체와의 협의를 통해서 반영할 수 있다.

● 보호 전담 조직의 구성

보호 시스템 구축과 관련된 보호 전담 조직은 개발자측과 사용자측으로 분류할 수 있다. 개발자 측은 보호 시스템의 설계를 담당하는 시스템 건축가(System Architect)와 보호 시스템을 구현하고, 실용화하는 시스템 구현가(System Builder) 등으로 구성된 보호 전담팀이 있다. 사용자측은 보호 정책을 수립하고 보호관련 업무/예산/인력을 조정·통제할 책임을 갖는 보호조정 위원회(Security Coordination Committee), 보호 관리자(Security Officer)를 책임자로 하며 프

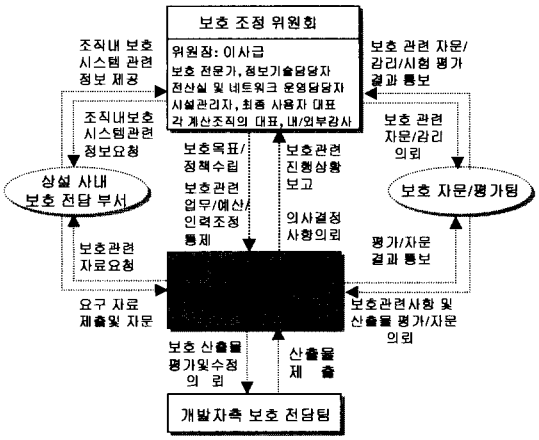


그림 3. 보호 전담 조직의 구성

로젝트 전 과정에서 개발자와 지속적 의사소통을 통해 보호 요구사항이 적절히 구현되었는지를 시험·평가하는 보호 전담팀, 시스템 운영 및 관리를 담당하는 시스템 관리자와 시스템을 직접 이용할 최종 사용자로 분류할 수 있다. 이 밖에도 조직 내·외부의 전문가로 구성된 보호 자문/평가팀이 참여할 수 있다. Badenhorst[13]는 보호조정 위원회의 구성을 Peter Fagan[20]와 D. Bailey[21]는 보호 관리자의 수행 기능 및 역할에 대해 상세히 제시하고 있다. <그림 3>은 조직들 간의 관계를 도시하고 있다.

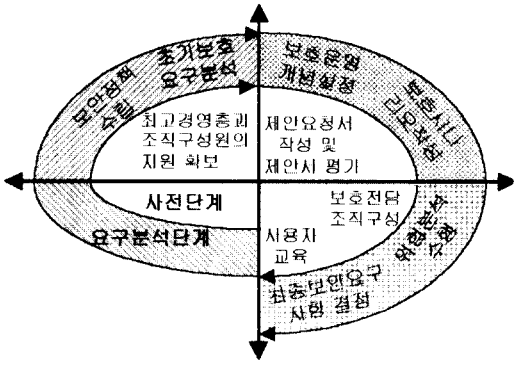
이 밖에도 사전 단계에서는 설명서, 비디오 등을 이용한 보호교육을 수행하여 보호관련 지식 및 마인드 확산을 통한 다양한 보호 요구사항을 정확하게 식별할 수 있도록 하여야 한다.

2. 요구분석 단계

요구 분석 단계는 조직의 정책, 환경 요소, 예산 제약, 사용자 요구사항 등을 고려하여 최종 보호 요구사항을 도출하는 과정으로 보호 정책 수립, 초기 보호 요구분석, 보호 운영개념 설정, 보호 시나리오 작성, 위험분석 실시 및 최종보호 요구사항 선택 등의 활동을 수행하게 된다.

● 보호 정책 수립

보호 정책은 "중요한 정보를 포함한 조직의 자산이 사용자 조직에 의해 관리되고, 보호되며 분배되는 방법을 통제하는 법, 규칙 및 관행의 집합"이라고 정의된다.[9,22] 보호 정책은 시스템



개발전에 제안된 시스템에 대한 기초적인 보호 요구사항을 기술하는 시스템 보호 정책, TCSEC, ITSEC, CC 등 개발된 보호 제품의 평가·인증을 위한 명세를 기술하는 제품 보호 정책, 특정 조직간에서 정보 시스템을 활용할 때 공통으로 적용하는 조직간 보호 정책과, 일반 조직에서 자신의 운영 환경에 맞게 작성한 조직내 보호 정책으로 분류할 수 있다.[23] 또한 보호 정책은 그 수준에 따라 최고 경영층에 의해 결정되는 상위 수준의 보호 정책과 시스템 건축가 및 구현가를 대상으로 하는 하위 수준 보호 정책으로 분류할 수 있다. 시스템 개발과 관련된 모든 활동은 보호 정책에 근거하고 있으므로, 성공적 보호 시스템 구축을 위해서는 모든 보호 관련 사항들을 완벽하게 포괄할 수 있는 정책 설정이 무엇보다 중요시 된다.[24] 따라서, 개발 대상 시스템의 보호 정책은 내부적으로는 조직내 정책과의 일관성 유지, 시스템에 대한 보호 요구사항 충족 등을 반영하여야 하고, 외부적으로는 법적, 제도적 문제, 제품 보호 정책 및 조직간 보호정책 등을 포괄하여야 한다. 또한 초기에 고려하지 못했거나, 신규로 추가될 보호 정책들은 관련 조직의 검토를 거쳐 신속히 반영될 수 있어야 한다.

● 초기 보호 요구사항 수집

초기 보호 요구사항 수집은 개발될 시스템을 직접 이용할 사용자들을 대상으로 보호 요구사항을 식별하는 활동으로 보호 전담팀이 주관하여 수행한다. 효과적인 요구사항 수집을 위해 보호 전담팀에서는 시스템의 운영 환경, 보호 시스템 구축에 따른 조직 업무 절차의 변형 등에 대한 정보를 요구분석 수행 전에 미리 사용자에게 전달하여야 한다.[25] 과거 요구 분석시에는 상위 수준의 추상적인 분석을 수행하고 이를 토대로 보호 시스템을 구축하였기 때문에 조직 각 부문 구성원들의 세부적이며 실제적인 요구사항을 반영하지 못한다는 비판을 받았다. 따라서, 보다 세부적인 변수들을 고려하여 정확한 요구사항을 도출할 수 있어야 한다.[20] Mostert와 von Solms은 보호 관리자를 통해 보호 요구사항을 효과적으로 추출하는 방법을 제시하였다.[6]

● 보호 운영 개념 설정

정확한 보호 요구사항을 식별하기 위해서는 이를 구현한 시스템이 실제 어떻게 운영될 지를 제시하는 보호 운영 개념을 파악하여야 한다.[12] 이를 위해서는 정보의 원천지, 수신처 및 수신 방법, 보호등급, 보호 운영 모드, 모드들간 변환 및 사용자 신뢰수준 그리고 외부 인터페이스 관련 특징 등과 같은 일련의 정보 흐름을 분석하여야 한다. 또한 시스템의 현재 상태와 시스템 구축 후의 기대 상태간의 차이로 정의되는 보호 목표도 설정하여야 한다. 보호 운영 개념은 초기에 식별될 경우 계약 인도 품목의 일부로 활용될 수 있고, 사용자, 개발자, 평가자, 인증 및 승인팀 등을 위한 기반자료로서 활용될 수도 있다.

● 보호 시나리오 작성

보호 시나리오는 개발 대상 시스템에서 발생할 수 있는 다양한 위협 및 침해 가능성을 스토리로 체계화한 것으로서, 요구사항 분석단계, 시험평가단계 등에서 활용할 수 있다.[12] 우선 요구분석 단계에서는 발생할 수 있는 위협 시나리오를 사용자에게 제시하여 보호에 관한 직관적인 이해를 제공함으로써 보다 정확한 보호 요구사항을 식별할 수 있게 된다. 시험평가단계에서는 개발된 시스템이 요구된 보호 기능을 완벽히 구현하였는지를 평가하기 위해 활용된다. 보호 시나리오는 평가 타당성을 위해 반드시 개발자와 독립된 주체에 의해 작성되어야 한다.

● 위험 분석 수행

위험 분석이란 구축 대상 시스템에 영향을 미칠 수 있는 다양한 위협, 취약점을 식별하고, 이로 인해 예상되는 손실 및 영향을 분석하여, 목표 보호 수준에 도달하기 위한 적절한 보호 매카니즘을 선택하는 과정이다.[26,27] 위험 분석은 과대한 보호 시스템 구축에 따른 비용 낭비

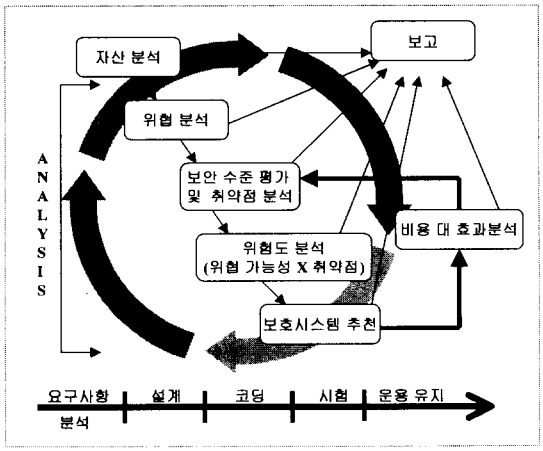


그림 4. 위험 분석 수행 절차

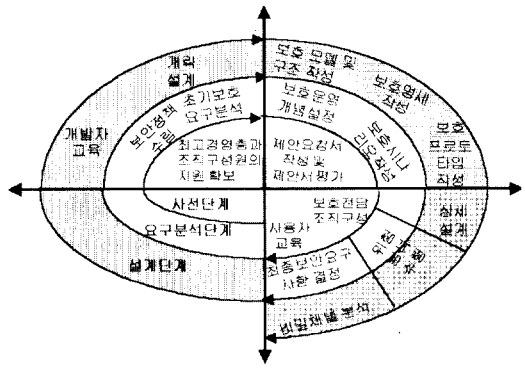
혹은 과소한 보호 시스템 구축에 따른 보호 사고 발생 위험간에 상충관계를 고려하여 최적의 보호 시스템을 결정하는 것을 목적으로 한다. 현재까지 효율적인 위험분석 수행을 위한 위험분석방법론에 대한 연구가 국 내·외에서 활발히 수행되고 있다.[26,27,28,29,30] 위험분석은 일반적으로 <그림 4>에서와 같은 7가지 활동 즉, 자산분석, 위협 분석, 취약점 분석, 위험도 분석, 보호 시스템 추천, 비용대효과 분석 및 최적 보호 대책의 선정으로 구성된다. 위험분석은 요구분석 단계에서 수행되는 일회적인 것이 아니라, 시스템 개발 전단계에 걸쳐 수행되는 지속적, 반복적인 과정으로 시스템 개발 초기부터 수행하는 것이 훨씬 경제적이며, 보다 뛰어난 효과를 발휘하게 된다.[31] 위험분석은 요구사항분석 단계에서 적절한 요구사항 도출과 최적 보호 시스템 구성요소의 식별을 위해, 설계단계에서 보호시스템의 구현에 대한 감독과 안전성 변화를 관찰하기 위해, 그리고 운용유지단계에서 환경 변화에 따른 보안성 변화를 분석하고 시스템의 수정 및 변경 등을 위해 수행된다.

● 최종 보호 요구사항 결정

위험분석과 초기 보호요구사항 수집을 통해 획득된 보호 요구사항은 전체 조직적 측면의 검토를 거쳐 최종 보호 요구사항으로 결정되어야 한다. 즉, 수집된 보호 요구사항들을 일반 조직 정책과의 비교, 예산 및 시간 제약, 상대적 중요도, 개발 능력, 생산성 감소, 운영 환경 특성, 법적 규제 등을 고려하여 최종 요구사항으로 결정하여야 한다.[32,33] 최종 요구사항 결정 시에는 요구사항의 완벽성(Completeness), 실현 가능성(Realism), 시험가능성(Testability)과 추적 가능성(Traceability) 등이 반영되어야 하며, CAM(Constraints Acquistion Methodology) 등 체계적인 방법론을 활용하여야 한다.[15,34,35] 요구분석 과정에서 미처 발견하지 못했거나, 시스템 개발 과정 중 새롭게 추가된 요구사항들은 시스템 개발 주체들이 참여하는 회의를 통해 반영 여부 및 수준 등을 결정하여야 한다.

3. 설계 단계

설계 단계에서는 요구분석 단계에서 식별된 최종 보호 요구사항을 구체화하는 단계로 개략 보호 설계, 보호 모델 및 구조 작성, 보호 명세



작성 및 프로토타입 개발, 상세 보호 설계, 비밀 채널 분석 등을 수행한다. 이에 앞서 요구분석 과정에 참여했던 보호 전담팀에서는 시스템 설계 및 개발을 수행할 시스템 건축가 및 구현가를 대상으로 개발 대상 시스템에서 제공해야 할 보안 요구사항에 대해 상세히 교육하여야 한다.

3.1 개략 보호 설계

개략 설계는 자연어로 기술된 보호 요구사항을 공식적인 시스템 지향적(System-oriented) 명세로 번역하는 작업으로 상세 설계의 기초가 된다. 개략 설계에서는 보호 요구사항을 구현 가능한 형태로 변형하며, 시스템 내부의 상호작용, 흐름, 통제 형태와 외부 인터페이스와의 관계 등을 다이아그램 등을 통해 구체적으로 도시하여야 한다. 개략 설계시에는 다음과 같은

원칙을 충족시켜야 한다.[36]

· 일관성(Directiveness) : 조직의 보호 정책, 운영 절차, 생산성 감소와의 상충관계 등을 설계에 반영하여야 한다.

· 보호성(Prevention) : 신뢰할 수 있는 시스템을 생성 및 관리할 수 있게 설계되어야 한다.

· 탐지가능성(detectiveness) : 정보 시스템에서 발생한 시도된 또는 실제 발생한 침해를 식별할 수 있도록 설계되어야 한다.

· 수정용이성(correctiveness) : 침해 또는 시스템 오류로부터 복구가 쉽도록 설계되어야 한다.

C. Wood는 이와 같은 원칙을 충족시키기 위해 비용 효과성(Cost-Effectiveness),간결성(Simplicity), 명확한 설계 및 오퍼레이션(Overt Design and Operation), 최소 특권(Least Priviledge) 등 개략 설계시 고려해야 할 22가지 사항을 제시하고 있다.[7,16]

● 보호 모델 및 구조 작성

보호 모델은 최상위 수준에서의 시스템에 대한 개관을 제공하기 위해 다양한 다이아그램을 통해 시스템을 가시화한 것으로 객체를 분류하고, 이들 간의 상호작용을 도시화하며, 객체들 간에 존재하는 상호의존성을 구체화하여 정보 흐름 분석을 가능케 한다. 예를 들어, 데이터플로우 다이아그램은 프로세스, 엔티티, 데이터 저장소 및 흐름간 관계를 도시함으로서 객체 민감도 수준(Sensitivity Level)의 식별을 용이하게 한다.

보호 구조는 보호 요구사항들을 계층화된 컴포넌트들로 명세화하는 것으로 계층구조의 최상위 부분은 시스템 건축가에 의한 논리적인 컴포넌트가 되고, 최하위수준은 실제 구현가능한 컴포넌트가 된다. 잘 설계된 보호 구조는 보호 요구사항 및 보호 환경이 변경되었을 때 이에 대한 추적을 가능하게 하며, 부적절한 보호 구조의 경우에 발생할 수 있는 재설계 등의 비용을 절감할 수 있다. 보호 구조는 각 정보 시스템별로 새롭게 작성할 필요는 없으며, ISO 7498-2[37]나 ECMA[38] 등에서 제시하는 공개 시스템 보호 구조 등을 활용할 수 있다.

● 보호 명세 작성

작성된 보호 구조를 토대로 개략적 설계를 위해서는 보호 명세를 작성하여야 한다. TCSEC에서는 개략적 설계를 위한 보호 명세로 DTLS(Descriptive Top-Level Specification)와 FTLS(Formal Top-Level Specification)를 제안하고 있다.[8] DTLS는 자연어, 비공식적인 프로그램 설계 표기법 또는 이 둘을 결합한 형태로 작성된 최상위 수준의 명세이다. 최상위 수준 명세란 가장 추상적인 수준으로 시스템의 행위를 표현하는 비절차화된 명세로서 대개 구현 세부사항은 생략하게 된다. FTLS는 시스템 명세가 요구사항과 일치한다는 것을 증명하는 이론을 가설검증하기 위해 공식적인 수리 언어로 기술한 최상위 명세이다. 공식적 검증은 시스템의 공식 명세와 보호 정책 모델간의 일관성(설계 검증) 또는 공식 명세와 프로그램 구현간의 일관성(구현 검증)을 증명하기 위한 공식적인 검증 절차이다.

3.2 상세 보호 설계

상세 설계는 개략 설계를 직접 프로그래밍이 가능한 상세 수준으로 구체화하는 활동이다. 상세 설계 수행시에는 보호 시스템 성능의 최적화, 재사용성에 대한 고려, 공식 언어를 이용한 투명성 보장 등이 고려되어야 하며, 코드 혼합 기법 등 보호 모듈 부분이 쉽게 노출 및 수정될 수 없는 방안을 강구하여야 한다. 또한, 시스템의 실패 또는 기타 사고 발생시 보호 매카니즘의 가용성을 보장할 수 있는 복구 절차 등 비상 대책(Contingency Planning)[39]도 고려하여야 한다.

● 보호 프로토타입 개발

보호 프로토타입은 추후 본격적인 시스템 개발에 앞서 최종적으로 보호 요구사항 및 이들에 대한 설계의 적절성을 검증하기 위해 작성된다.[3] 즉, 가시화된 프로토타입을 살펴봄으로써 보호 기능 추가에 따른 시스템의 성능 저하 등을 보다 정확히 예측할 수 있으며, 추가 보호 요구사항의 필요를 식별할 수 있다. 또한, 설계자는 효율적인 보호 시스템 설계 방안을 고안할 수 있으며, 프로그래머는 전체적인 보호시스템 구조에 대한 인식하에 시스템 개발에 착수할 수 있게 된다.

● 비밀 채널 분석

비밀 채널은 시스템의 보호 정책을 위반하여 정보를 전달할 수 있는 통신 채널로서 크게 비밀 저장 채널(Covert Storage Channel)과 비밀 시간 채널(Covert Timing Chennel)이 있다. 비밀 저

장 채널은 일반적으로 상이한 보호 수준을 갖는 두 주체들간에 공유되는 한정된 자원의 직·간접적인 읽기·쓰기와 관련된 비밀 채널이며, 비밀 시간 채널은 한 프로세스가 자신의 시스템 자원 사용을 변조하여 다른 프로세스에 정보를 전송하는 비밀 채널이다.[40] 시스템 구현시 대역과 시스템 성능간에는 상충관계가 발생하게 되고, 신뢰할 수 있는 대역인 1bps이하로 낮추는 데 많은 노력이 필요하게 되어, 일반 시스템내에서는 비밀 채널이 존재할 가능성을 갖게 된다. 비밀 채널 분석은 공유 자원 매트릭스(Shared Resource Metrix)[41], 정보 흐름 방법(Information Flow Method)[42] 등을 통한 직접적인 비밀 채널의 존재 가능성 분석과 특정 bps이상의 대역을 갖는 비밀 채널 매카니즘 사용 감사를 위한 능력(Capability)의 도입 등을 통해 수행된다.

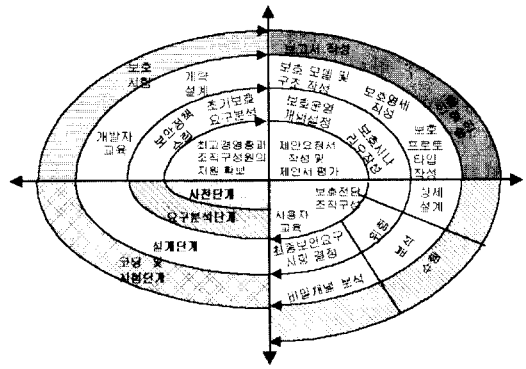
4. 코딩 및 시험

코딩은 상세설계를 구현하는 과정이며, 시험은 코딩 완료된 시스템이 적절히 운용되는지를 검증하는 과정이다. 코딩은 공식 언어를 이용하여 작성하며, 상세한 주석을 첨부하여 추후에 발생할 수 있는 수정 및 재사용에 대비할 수 있어야 하고, 시험은 시스템 개발 과정에 참여하지 않았던 별도의 전문가들에 의해 보호 시나리오 및 시험 절차 등을 기반으로 수행되어야 한다. 코딩 및 시험 단계에서의 보호공학 구성요소로는 보호시험, 보고서 작성, 인증 및 승인이 있다.

● 보호 시험

보호 시험은 구현된 시스템이 초기 보호 요구사항대로 설계 및 구현되었는지 그리고 실제 운영 환경에 적절히 기능을 수행하는 지를 평가하는 절차이다. 보호 시험시에는 설계 문서, 소스 코드, 목적 코드 등 모든 코드에 대해 분석을 수행하며, FTLS와 소스 코드간 매핑 관계도 분석한다. 대표적인 보호 시험으로는 기능시험(Functional Testing), 운영 시험(Operational Testing), 검증(Verification) 및 침투 시험(Penetration Testing)이 있다.[43]

이 중 침투 시험은 침투자가 시스템의 보호 기능에 대한 방해를 시도할 수 있는지를 분석하는 것으로서 다른 유형의 시험이 모두 완료



된 후에 수행된다. 침투 시험은 시스템의 보호 매카니즘을 파괴하기 위한 시도로서 그리고 다른 유형의 시험에서 발견되지 않은 시스템의 취약점을 식별하기 위해서 수행된다. 침투 시험의 수행 주체는 시스템의 보호 기능 및 다른 관련 시험의 수행 결과에 대한 사전 지식을 갖추어야 한다. Neumann[44]은 침투 시험을 수행하기 위한 4단계 모델을 제시하였으며, TPEP에서는 A1등급의 보호 제품을 시험할 때 최소한 3명이상(전산 전공 석사급 2명, 학부졸업 1명)이 25가지 이상의 침투 시험을 3개월~6개월 동안 수행하도록 권고하고 있다.[45]

이상의 시험 결과는 보호 보고서로 작성되어야 한다. 보호 보고서는 시험 결과 및 발견사항을 문서화하기 위해 사용되며, 선택된 보호수단의 결함, 이를 개선하기 위해 필요한 행위들 그리고, 이러한 행위의 수행 결과 등이 포함된다.

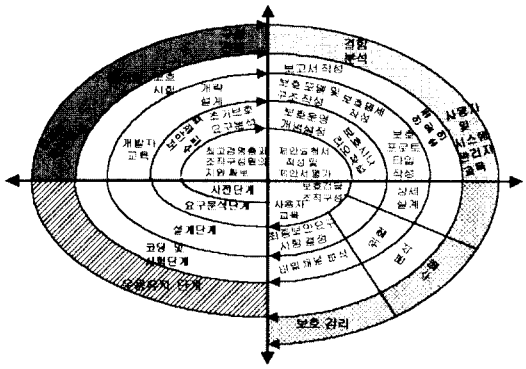
● 인증 및 승인

구현 및 시험이 완료된 시스템에 대해서는 필요한 경우 시스템의 보호 요구사항 충족 여부에 대한 공식적인 인증 및 승인 절차를 거치게 된다. 인증은 시스템의 보호 기능의 적절성에 대한 기술적 평가 결과인 반면, 승인은 실제 운영될 환경에서 시스템이 데이터를 안전하게 처리할 수 있는 정도의 안전성을 갖는가에 관한 관리적 측면에서의 공식적인 평가이다.[46,47] ITSEC에서는 인증 및 승인을 수행하기 위해서 처리될 데이터의 중요도, 사용자의 신뢰수준, 운영모드 및 개념, 시스템에 의해 제공될 기술적 보호에 대한 보증, 보호 관리 책임 소재의 확인, 보호 관련 기술 및 법규, 비기술적 보호

수단의 적절성 등을 고려하도록 하고 있다.[9]

5. 운용 유지 단계

개발 및 시험 평가가 완료된 시스템은 각 사용자 사이트에 배포되어 활용되어야 한다. 운용 유지 단계에서의 보호공학 구성요소에는 시스템의 인도 후에 발생할 수 있는 다양한 보안 관련 사항들 즉, 안전한 배포 채널 수립, 문서화, 구성 관리, 결함분석, 사용자 및 시스템 관리자 교육, 보호 감리 수행 등이 포함된다.



● 안전한 배포

개발된 시스템은 물리적, 관리적, 인적 수단 등을 통해 각 사이트에 안전하게 배포되어야 한다. 즉, 현장 배치가 결정된 시스템은 각 조직 환경에 적합한 안전한 경로를 통해 배포되어야 한다. 이 때 마스터 프로그램과 현장 배치 프로그램간에 무결성을 보장하기 위한 방안이 강구되어야 하며, 사후 시스템 변경 발생시에도 계속적으로 활용될 수 있도록 신뢰성 있는 배포 경로가 운용 및 관리되어야 한다.

● 문서화

문서화는 소프트웨어 개발 절차동안 발생한 모든 보호 관련 사항들을 기록하여 추후 시스템 변경 등에 활용하기 위한 것으로 특히 보호 관련 코드를 위해서 필요하다. 보호 코드 문서는 개발 문서와 별도로 작성하며 정보의 비밀 등급별로 분류하여 문서화하는 것이 권고된다. 이 밖에 보호 관련 문서에는 보호 기능 사용자 매뉴얼, 관리자 매뉴얼(Trusted Facility Manual), 시험 문서(Test Documentation), 설계 문서

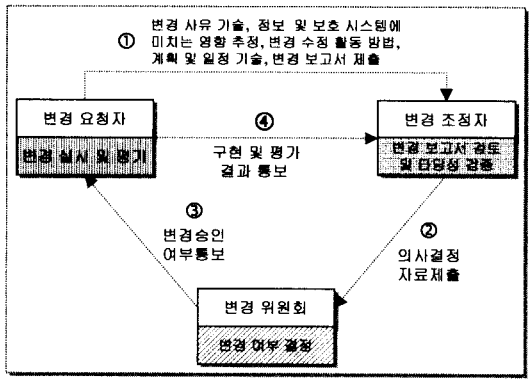


그림 5. 구성관리 수행절차

(Design Documentation)가 있다.[8,12]

보호 기능 사용자 가이드는 보호 시스템에 의해 제공되는 보호 매카니즘에 대해 기술하고, 사용 방법 및 그들간의 상호작용 방식을 포함하는 문서이다. 관리자 매뉴얼은 시스템 관리자를 대상으로 시스템의 보호 기능을 실행시킬 때 통제되어야 하는 기능, 특권 등과 같은 사항들을 기술한 문서이다. 시험 문서는 시험 계획, 시험 절차 및 기능, 시험 결과를 포함하는 문서로 시스템 개발자가 평가자에게 제공하는 문서이다. 마지막으로, 설계 문서는 개발자의 보호 시스템 개발 철학, 이 철학을 시스템으로 변환한 매카니즘에 대한 설명을 기술한 문서이다.

● 구성관리

구성 관리 혹은 변경 통제(Change Control Management)는 정보 시스템의 변경을 지속적으로 관찰하고, 기술 및 조직환경의 변화에 따른 요구사항의 변화, 설계 명세의 변화, 프로그래밍 및 시험 버전 변경 등 변경 요인 발견 즉시 해당 시스템에 수정 등 필요한 조치를 강구하는 활동이다.[48] 일반적으로 시스템 관련 환경은 동적이며, 끊임없이 변화한다. 이러한 변화의 원인은 고용인의 퇴직, 보직 이동 등 예측가능한 변화, EDI를 이용한 타 조직과의 통신시스템 구축 등과 같은 조직 정책의 변경, 새로운 법규의 생성, 기술의 변화 및 경쟁자의 정책 변경 등이 될 수 있다. 구성관리는 시스템 개발 중 또는 시스템 개발 후에 수행할 수 있으며 감리 활동들과 통합될 때 보다 뛰어난 효과를 발휘하게 된다.[49]

● 결함 분석

결함 분석은 시스템을 사용하는 도중에서 불

명확한 절차, 악의적인 침투 및 설계의 결함 등으로 인해 발생하는 여러 가지 시스템 결함을 발견 및 분석하는 일련의 활동이다. 보호와 관련된 모듈에서의 조그만 결함은 특히 그 파급효과가 시스템 전체에 미칠 수 있어 매우 중요하게 고려하여야 한다. 이를 위해 O.Tettero[4]는 보호 관련 부분에서 결함이 발견되는 경우에는 이를 제거하기 위해 최소한 새로운 릴리즈를 개발하는 정도의 작업 수행을 권고하고 있다.

● 사용자및시스템관리자 교육

구현된 정보 시스템을 실제 사용자 환경에서 운용하기 위해서는 여러 가지 추가 보호 활동을 필요로 한다. 이를 위해서는 시스템을 운용하는 과정에서 필요한 보호 활동들을 시스템 관리자 및 사용자에게 교육하여야 한다. 예를 들어 시스템 관리자는 주별 암호키 변경, 일별 사용자 변동사항 변경 등을 수행하여야 한다. 또한 사용자도 정규적인 패스워드 변경, 데이터 파일 전송시 암호화 등을 준수하여야 한다.

● 보호 감리 수행

개발이 완료된 시스템의 운용과정에서 발생할 수 있는 여러 가지 유형의 보호정책 위반 사항들, 즉, 해커에 의한 침투 사실, 내부자의 권한외 행위, 합법적인 권한을 가장한 침투 행위 등을 식별하기 위해서는 보호 감리 시스템이 구축되어야 한다. 보호 감리는 일반 감리증적 시스템, 침입탐지시스템, 방화벽 시스템 등에서 불법적인 행위 탐색의 기반이 되며 추후 책임 소재를 식별하여 제재 조치를 취하는 등에 활용될 수 있다.

마지막으로 이상에서의 보호공학활동을 효과적으로 수행하기 위해서는 시스템 개발 전단계에 걸쳐 자원의 효율적 배분, 시기 적절한 문제해결 및 의사결정 등을 지원하는 보호 관리 활동을 수행하여야 한다.

Ⅳ. 결 론

본 논문에서는 안전한 정보 시스템을 구축하기 위하여 획득자가 시스템 개발 수명 주기 전단계에 걸쳐 수행하는 보호 공학 활동들을 체계화한 보호 공학 방법론을 제안하였다. 보호공학 방법론은 공개적·개방 구조의 프레임워크로서 5단계걸친 총 27가지의 세부 활동으로 구성되며, 프로젝트 개발 방법론과 통합되어 시스템 개발 활동과 함께 수행됨으로써 보다 안전한 정보 시스템을 경제적으로 구현할 수 있다. 이상에서 제시한 보호 공학 방법론의 효과적인 활용을 위해서는 다음과 같은 사항들을 고려하여야 한다.

● 시스템 개발시 각 단계별 보호공학 활동은 일회적으로 완벽하게 수행될 수 없다. 따라서, 시스템 개발 전단계에 걸쳐 발생하는 추가 보호공학 활동 및 이들에 대한 수정을 피드백 과정을 통해 반복적·지속적으로 수행하여야 한다.

● 모든 조직 환경에 적용할 수 있는 최적 보호공학 방법론은 존재할 수 없으므로 조직의 구조, 환경, 예산규모, 전략 목표 및 방향 등을 고려하여 각 조직 환경에 가장 적합한 형태로 보호공학 활동들을 테일러링하는 것이 바람직하다.

● 보호공학 활동은 조직의 보호 정책, 절차, 책임 및 기타 사항들을 체계적으로 관리하는 기반 구조하에서 효과적으로 운용될 수 있으므로 ISO 9000등을 통한 기반구조를 구축하여야 한다.

● 시스템 폐기 시점에서 해당 프로젝트와 관련된 보호 정보들을 체계적으로 데이터베이스화하여 수정, 재사용 및 신규 프로젝트 수행시에 이를 효과적으로 활용할 수 있도록 하여야 한다.

● 안전한 정보 시스템의 효과적인 구축을 위해서는 별도의 보안업무를 전담하는 관련 조직을 구성하여야 한다. 조직의 규모는 각 조직의 과거 경험, 유사 프로젝트의 현황, 시스템의 중요도 등을 고려하여 적정 규모로 결정하여야 한다.

참고문헌

[1] F.G.Tompkins and R.Rice,"Integrating Security Activities into the Software Development Lifecycle and the Software Quality Assurance Process," Computer & Security, Vol. 5, 1986, pp.218-242

[2] Warman, A.R., "Developing Policies,

Procedures, and Information Security Systems," In Information Security-The Next Decade : Proc. of IFIP Information Security, Chapman & Hall, 1995, pp.465-476

[3] H.A.S.Booysen & J.H.P. Eloff, "A Methodology for the Development of Secure Application Systems," In Information Security-The Next Decade:Proc. of IFIP Information Security, Chapman & Hall, 1995, pp.255-269

[4] O.Tettero, D.J.Out, H.M.Franken and J. Schot, "Information Security Embedded in the Design of Telematics Systems," Computers & Security, vol.16, no.2, 1997, pp.145-164

[5] Baskerville R., "Information Systems Security Design Methods:Implications for Information Systems Development,"ACM Comuting Surveys Vol.25 No.4, December, 1993.

[6] D.N.J. Mostert and S.H. von Solms, " A Methodology to Include Computer Security, Safety and Resilience Requirement as Part of the User Requirement," Computers & Security, vol.13, no.4, 1994, pp. 349-364.

[7]C.C.Wood, "Principles of Secure Information Systems Design with Groupware Examples," Computers & Security, Vol. 12, 1993 pp.663-678

[8]DoD, *Trusted Computer System Evaluation Criteria*, DoD-Std-5200.28, Dec. 1985

[9]EC, *Information Technology Security Evaluation Criteria(ITSEC)*, Ver.1.2, June 1991.

[10]CCEB, *Common Criteria for Information Technology Security Evaluation*, May,1998.

[11] F.G.Tompkins and R.Rice, "Integrating Security Activities into the Software Development Lifecycle and the Software Quality Assurance Process," Computers & Security, 5(1986), pp.218-242.

[12] Marshall D. Abrams, Sushil Jajodia and Harold J. Podell, *Information Security-Security Engineering*, IEEE Computer Society Press, 1995, pp.330-349

[13] K.P. Badenhorst and Jan H.P. Eloff, "Framework of a Methodology for the LifeCycle of Computer Security in an Organization," Computer & Security, Vol.8, 1989, pp.432-442.

[14]Jean Hitchings, "Achieving an Integrated Design: the Way Forward for Information Security," Proceedings of IFIP Information Security, Chapman & Hall, 1995, pp.369-383.

[15]S.J.Shepherd, P.W. Sanders, and A.Patel, "A Comprehensive Security System-the Concepts, Agents and Protocols," Computers & Security, Vol.9, 1990, pp.631-643.

[16]C.C.Wood,"Principles of Secure Information Systems Design," Computers & Security, Vol.9, 1990, pp.13-24.

[17] SRI, *The Baseline Approach*, 1993

[18]ISO/IEC JTC 1/SC 27/WG 1, *Guidelines for the Management of IT Security*, 1995.5

[19] BSI, *A Code of Practice for Information Security Management*, 1993.

[20] Peter Fagan, "Organizational Issues in IT Security," Computer & Security, Vol.12, 1993, pp.710-715.

[21]D. Bailey, *Information Security-An Integrated Collection of Essays, A Philosophy of Security Management*, IEEE Computer Society Press, 1995, pp.98-111.

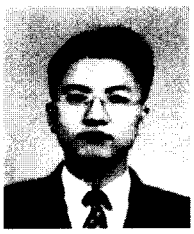
[22]Ford, W., *Computer Communications Security: Principals, Standard Protocols and Techniques*, Prentice Hall, New Jersey, 1994.

[23]Dr. Jan H.P. Eloff, "Computer Security

Policy:Important Issues,"Computers & Security, Vol.7, 1988. pp.559-562.
[24]Kenneth R. Lindup,"A New Model for Information Security Policies," Computers & Security, vol.14, pp.691-695
[25]Jenus Associates, "Information Security Administration Model: A Management Model to Help Identify the Best Practices of the Administration Function Within the Security Group," Computer & Security, Vol. 11, 1992, pp.327-340.
[26]Rex Kelly Rainer, JR., Charles A. Snyder, and H.H. Carr, "Risk Analysis for Information Technology," Journal of MIS, 1991, pp.129-147
[27]강동석, *Risk Analysis and Management in Public Project Selection*, 정보화저널 제5권 제1호, 1998년 7월, pp.62-82
[28]윤정원,신순자,이병만, "국내환경에 적합한 IT 위험분석 표준에 관한 연구," WISC'98, 1998. pp.371-382.
[29]이영화, "확장능력매트릭스를 이용한 위험분석도구 선택 방법론," WISC'95, 1995. pp.189-202.
[30]이성만, 이필중,"해외의 보안위험분석 방법론 현황 및 분석,"한국통신정보보호학회 종합학술발표회 논문집, Vol.4, No.1, 1994, pp.316-323
[31]ARC, *Lifecycle Risk Analysis for Improved System Development*, Dec. 1993.
[32] C.C. Wood, "A Context for Information Systems Security Planning," Computers & Security, Vol.7, 1988, pp.455-465.
[33]Clark, D. D. and Wilson, D.R., "A Comparision of Commercial and Military Computer Security Policies," Proceedings of '87 Symposium on Security and Privacy, 1987.
[34]S.L.Pfleeger, "A Framework for Security Requirements," Computers & Security, Vol.10, 1991, pp.515-523.
[35]W .Fred. de Koning, "A Methodology for the Design of Security Plans," Computers & Security, Vol.14, 1995. pp.633-643.
[36]Belden Menkus, "Control is Fundamental to Successful Information Security," Computers & Security, Vol.10, 1991, pp.293-297.
[37]ISO, *Information Processing Systems -open Systems Interconnection-basic Reference Model-security Architecture*, ISO 7498-2, 1989.
[38]European Computer Manufactors Association(ECMA), *Security in Open Systems, a Security Framework*, , ECMA TR-46, 1988.
[39]Butler, J., *Contingency Planning and Disaster Recovery Strategies*, CTR Corp.; 1994.
[40]C.P.Pfleeger, S.L.Pfleeger and M.F.Theofanos, "A Methodology for Penetration Testing," Computers & Security, vol. 8, 1989, pp.613-620.
[41]Denning,D. "A Lattice Model of Secure Information Flow," Comm ACM, Vol.19, No.5, May, 1976, pp.236-243.
[42] Kemmerer,R. "Shared Resource Matrix Methodology,"ACM Trans Comp Sys, Vol.1, NO.3, Oct 1983, pp.256-277.
[43] Millen, J.,"Covert Channel Capacity," Proc IEE Symp Security & Privacy, IEEE Comp Soc Press 1987, pp.60-66.
[44]P.Neumann, "Computer System Security Evaluation," Proc. AFIPS 1977 Natl. Computer Conf., vol.46, pp.1087-1095
[45] NCSC, *TPEP Procedures*, Jun.1996
[46] Tinto, M., "The Design and Evaluation of INFOSEC Systems:The Computer Security Contribution to the Composition Discussion," C Tech. Report 32-92, NSA, June 1992.
[47] NBS, *Guideline for Computer Security Certification and Accrediation*, FIPS Pub.102, 1983.
[48]DoD, *Defense System Software Development*, DOD-STD-2167A, 1998.

[49]Dr. R. Paans, Prof. Dr. I.S. Herschberg, "Auditing the Change Management Process," Computers & Security, Vol. 9, 1990. pp.161-174.

이 영 화(Lee, Young Hwa)



1991년 2월 : 고려대학교 경영학과 졸업
1993년 2월 : 고려대학교 경영학과 경영정보학 석사
1993년 3월~1998년 12월 : 국방정보체계연구소 선임연구원
1999년 1월~현재:국방과학연구소 선임연구원

〈관심분야〉 위험분석, 보호공학, 프로젝트 관리 등

이 남 용(Lee, Nam Yong)

1979년 2월 : 숭실대학교 전산학과 졸업
1982년 2월 : 고려대학교 대학원 경영정보학 석사
1993년 8월 : 미시시피주립대 경영정보학 박사
1983년 1월~현재:국방과학연구소 선임연구원

〈관심분야〉 객체지향방법론, 보호공학, 프로젝트 관리 등