通信情報保護學會誌
第 11 券 第 1 號, 2001. 2

초고속망 안전 · 보안의 주요 이슈

이 병 만*, 윤 정 원*, 신 순 자*, 원 동 호**

요 약

초고속국가망을 이용하는 기관은 국가 및 지방자치단체 등 공공기관이 대부분으로 정보시스템에 보안사고 발생시 정보 유출, 파괴, 서비스 마비 등이 발생하여 해당기관의 생존뿐만 아니라 나아가 국가의 안위까지도 위협될 수 있음에 따라 초고속망 안전 · 보안이 주요 이슈로 등장하고 있다. 이에 따라 본 논문은 초고속국가망 이용기관 측면에서, 체계적인 보안관리를 가능케 하는 정보기술 보안관리 일반모델을 소개하고 통신사업자 측면에서, 비상시에도 안정적으로 초고속국가망 서비스를 제공하는 방안에 대해서도 소개한다.

Ⅰ. 서 론

오늘날 정보시스템은 빌딩이나 지역에 국한되어 사용하던 과거와 달리 초고속망으로 전국적, 전세계적으로 상호 연결되어 온라인으로 서비스되고, 많은 사람들이 이용함에 따라 이제 비즈니스를 비롯한 사회 각 분야에 그 중요성은 점점 더 커지고 있으며 의존도 또한 심화되고 있다.

이러한 정보시스템에 보안사고 발생시 정보 유출, 파괴, 서비스 마비 등이 우려되고 있으며, 그 피해는 금전적인 손실뿐만 아니라 경우에 따라서는 조직의 운명을 좌우할 정도의 커다란 문제로 부각될 수 있다.

이에 따라 이러한 문제를 사전에 방지하기 위한 여러 가지 방법이 제안되어 왔으며, 본 논문에서는 초고속망 이용기관의 보안관리 이슈중의 하나이며, 국제표준화기구(ISO)의 SC 27 분과위원회에서 처음으로 제시된 정보기술 보안관리의 일반모델을 소개한다.

이중에서 보안관리의 핵심인 위험분석은 서비스중인 정보시스템의 운영상황과 정보시스템의 가용성, 무결성, 비밀성에 관한 다양한 위협을 파악하여 취약성수준과 기대 손실액을 측정, 분석하여 비용효과적인 대응책을 제시하는 일련의 과정으로 조직의 경영자가 안전하고 경제적인 대응책을 수립할 수 있도록 의사결정 기준을 제공한다.

이러한 보안모델과 위험분석은 조직의 규모가 작을 경우는 불필요할 수 있으나 정보시스템에 의존하는 비율이 크고 규모가 방대한 조직의 경우는 반드시 도입해야 보안사고 발생시의 커다란 문제를 사전에 차단할 수 있다.

아울러, 초고속국가망과 관련하여 재난이나 재해 발생시에도 안정적으로 국가망 서비스를 제공할 수 있는 방안에 대해서도 소개한다.

Ⅱ. 위험분석 개념

2.1 보안관리 모델

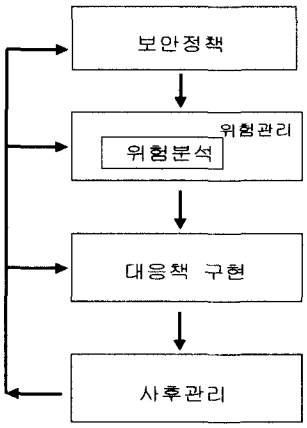


그림 1. 정보기술 보안관리 모델

* 한국전산원
** 성균관대학교

어떤 조직의 보안관리를 체계적으로 하기 위해서는 그림 1에 나타난 바와 같이 크게 4단계로 구분하여 수행해야 한다. 시스템의 위험을 평가하고 비용효과적인 대응책을 제시하여 시스템 보안정책과 보안대응책 구현 계획을 수립하는 위험관리가 보안관리에 있어서 가장 핵심이 되는 과정이다. 위험관리 과정 중 80% 이상을 위험분석 과정이 차지하고 있어 실질적으로 보안관리 과정 중 가장 핵심은 위험분석 과정이라고 할 수 있다.

공공기관을 비롯하여 대부분의 조직에서는 정보(Information)를 처리(Processing)하기 위하여 정보시스템(Information Technology and Systems)에 대한 의존도가 매우 높다. 그러나 정보의 비밀성, 무결성, 인증성, 가용성, 책임추적성, 신뢰성에 대한 위협이 증가하여 조직의 정보시스템 보안의 필요성이 매우 중요해지고 있다. 정보기술 보안관리(IT 보안관리 : Information Technology and Systems Security Management)는 정보의 비밀성, 무결성, 인증성, 가용성, 책임추적성, 신뢰성을 확보하고 유지하는 일련의 과정이다.

그림 1에서 나타난 바와 같이 정보시스템 보안관리는 크게 4단계의 과정으로 이루어져 있다. 물론 세부적인 부문은 조직의 문화, 성격, 업무종류에 따라 조금씩 다를 수도 있으나 상기 4단계의 과정은 반드시 포함하여야 한다.

2.2 보안정책

정보시스템 보안정책은 조직의 환경과 업무성격에 맞게 조직의 정보자산을 어떻게 관리, 보호할 것인가에 대해 기본적으로 무엇이 수행되어야 하는가를 일목요연하게 기술한 지침과 규약이다. 조직의 보안정책은 정보자산을 안전하게 보호하기 위해 우선적으로 수립해야 하며, 그림 2와 같이 여러 단계로 계층화될 수 있다.

o 일반 보안정책

우선 그림 2에 나타난 바와 같이 조직의 환경과 성격에 따라 전체적인 관점에서 보안의 원칙과 방향을 기술한 일반 보안정책(General Security Policy)이 있다. 일반 보안정책에는 전체적인 관점에서 조직의 목적과 요구사항, 제약조건들을 반영한 보안목적, 보안전략, 보안지침, 보안규약 등이 기술되어야 한다.

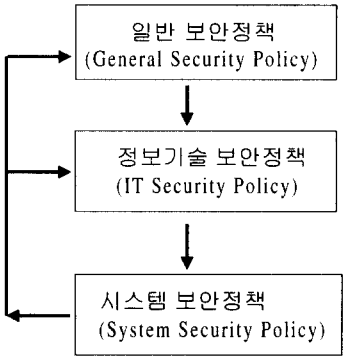


그림 2. 정보시스템 보안정책의 계층구조와 흐름

o 정보기술 보안정책

정보기술 보안정책(IT Security Policy)은 일반 보안정책의 내용과 범위를 벗어나지 않는 한도내에서 정보시스템의 효과적인 보안을 위해 필요한 각종 절차 및 규약을 정보기술 보안관리의 전반적인 시각에서 작성한다. 정보기술 보안정책을 통하여 보안관리의 다음단계에서 시행될 위험관리의 범위가 결정되기 때문에 조직의 환경을 고려하여 작성해야 한다.

기본적으로 정보기술 보안정책은 다음과 같은 항목을 포함하여야 한다.

o 정보기술 보안정책에 포함되어야 할 기본 항목

- 정보기술 보안목적
- 정보기술 보안조직 및 구조
- 정보기술 보안조직의 역할
- 위험관리
- 보안정책 관리 및 변경
- 대응책 선택 기준 및 구현 절차
- 비상계획 및 재해복구 계획
- 보안교육
- 기타(관련 규정)

o 시스템 보안정책

시스템 보안정책(System Security Policy)은 위험분석을 통하여 얻은 결과를 바탕으로 작성된다. 시스템 보안정책은 특정 시스템이나 특정 그룹의 시스템을 대상으로 구현되어야할 보안 요구사항과 대응책들에 대해 좀 더 자세한 내용을 포함해야 한다. 따라서 조직에서 사용하는 시스템이 다수일 경우 여러 개의 시스템 보안정책이 존재할 수 있다. 시스템

보안정책에는 보안 대응책들의 필요성과 이들 보안 대응책들을 어떻게 구현하고 이용해야 하는가를 자세히 기술해야 한다.

이상과 같이 3단계의 보안정책은 위험분석 등 보안관리의 과정을 통하여 얻어진 결과를 바탕으로 수정될 수 있다. 물론 수정의 절차는 보안정책에 기술되어 있는 보안정책 변경 규정에 의하여 수행되어야 한다. 보안정책을 수정하는 이유는 여러 가지가 있을 수 있다. 새로운 시스템이 구축되어 기존의 보안정책이 제 기능을 발휘하지 못할 경우나 보안사고 등으로 인하여 기존 대응책에 문제점이 발견될 수도 있다. 그러나 어떠한 경우에도 보안관리 과정에 나타난 바와 같이 적정 수준의 위험분석 실시 후 그 결과를 근거로 보안정책에 대한 수정이 이루어져야 한다. 그러나 보안정책을 수정해야만 하는 충분한 근거에도 불구하고 보안조직의 구성원들이나 최고책임자가 수정에 대해 여러 가지 이유로 동의하지 않을 경우 보안정책을 수정할 수 없는 것이 원칙이다.

o 보안조직

조직의 규모에 따라 조금씩 틀릴 수도 있지만 보안정책과 함께 꼭 필요한 부분이 전담 보안조직을 구성하는 것이다. 보안조직이 성공적으로 구성되고 운영되어야만 조직에 알맞은 보안정책의 개발과 활용이 이루어질 수 있다. 조직의 규모가 작다 하더라도 전담 보안조직을 구성하여 담당 부서와 담당자의 책임 및 역할을 명확히 하여야 한다.

보안조직의 역할은 여러 기능이 있다. 그 중에서 가장 기본적인 역할을 나열해 보면 아래와 같다.

o 보안조직의 기본 역할

- 보안정책 수립
- 보안 사고 대응(IRC : Incident Response Capability)
- 보안 대응책 구현 및 지원
- 비상계획 수립
- 보안예산의 계획 및 집행

일반적으로 필요한 보안조직 인력은 조직 규모에 따라 달라질 수 있지만 기본적으로 아래와 같다. 조직의 환경과 예산에 따라 보안조직을 구성하는 인력의 역할이 달라질 수 있고 규모가 작은 조직일 경우 보안조직 인력의 역할이 축소될 수 있다. 또한 조직의 규모가 매우 큰 경우 부서별로 보안 담당자를 지정할 수도 있다.

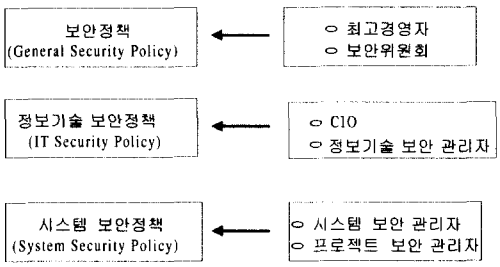


그림 3. 보안정책과 보안조직간의 관계

그림 3은 보안정책과 보안조직과의 관계를 나타낸 것이다. 조직의 일반 보안정책(General Security Policy)은 주로 최고관리자와 보안위원회에 의해서 전략과 목적이 조직의 역할에 맞게 정해지게 된다. 또한 최고경영진과 보안위원회는 정보시스템 보안을 포함하여 조직의 전반적인 보안의 수준과 방향을 결정하여 보안정책에 반영한다. 이러한 보안정책에 의거하여 CIO(정보화책임관), 정보시스템 보안책임자 및 정보시스템 감사 담당자들은 시스템 보안정책을 수립하게 된다. 시스템 보안관리자나 프로젝트 보안관리자들은 위험분석 결과에 따라 각 시스템별로 세부적인 시스템 보안정책 수립에 참여하게 된다.

2.3 위험관리와 위험분석

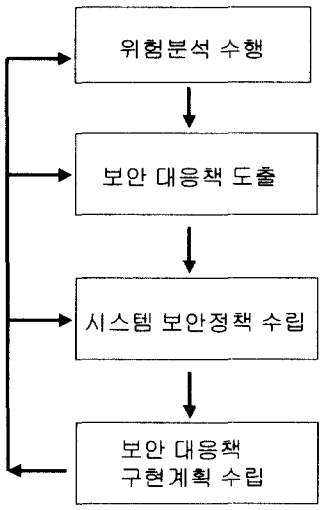


그림 4. 위험관리 모델

위험관리는 시스템의 위험을 평가하고 그 결과에

따라 비용효과적인 대응책을 제시하여 시스템 보안 정책과 보안대응책 구현 계획을 수립하는 일련의 과정이다. 위험관리는 조직의 환경과 능력에 맞추어 대응책을 운영하도록 지원하는데 큰 장점이 있다. 위험관리는 조직의 정보시스템을 설계하는 단계에서 고려될 때 가장 큰 효과를 발휘할 수 있다. 시스템이 구축되기 전에 위험관리를 수행함으로서 시스템이 갖추어야할 비용효과적인 대응책을 사전에 구현할 수 있다. 뿐만 아니라 위험관리는 시스템이 변경되거나 운영되는 과정에도 적용하면 안정된 시스템 운영에 기여할 수 있다. 위험관리는 적정한 주기로 반복되어 실시되어야 한다. 이미 구현된 대응책들도 고유의 취약성을 내포할 수 있기 때문에 적정한 주기를 두고 위험관리 과정을 반복함으로서 새로운 위협을 발견하고 이미 측정된 위험을 재평가하여 새로운 대응책을 보안정책에 반영하는 일련의 과정이 필요하다. 위험관리의 반복주기는 조직의 규모에 따라 매우 다르지만 일반적으로 1년에 1 ~ 2회 정도가 바람직한 것으로 받아들여지고 있다. 잦은 위험관리의 수행은 시간과 인력, 비용 등을 증가시킴으로서 조직의 고유 업무 수행에 부담을 줄 수 있기 때문이다.

2.4 대응책 구현

위험관리 과정을 수행한 뒤 보안대응책 수행계획에 따라 대응책을 구현해야 한다. 대응책 구현과정에서 반드시 지켜야할 사항은 아래와 같다.

- 대응책 구현 비용이 위험관리를 통하여 계획된 비용을 초과하지 않아야 한다.
- 대응책은 보안대응책 수행계획에 따라 정확하게 구현되어야 한다.
- 대응책은 보안대응책 수행계획에 따라 정확하게 운영되고 관리되어야 한다.

대응책은 기술적인 구현 후에도 대응책의 특성상 지속적으로 관리, 운영해야 하는 경우가 많다. 따라서 대응책 구현이 끝난 뒤 대응책이 시스템 보안정책과 대응책 수행계획에 맞게 구현되었는지를 검증하고, 보안관리자가 승인했을 경우에만 대응책이 운영에 들어갈 수 있어야 한다.

2.5 사후관리

사후관리는 보안관리 주기에서 가장 중요한 부문이다. 사후관리는 보안정책 수립에서 위험관리에 이르기까지 수행된 보안관리 단계가 조직의 보안성 향상에 실질적으로 도움이 되었는지 점검하고 관리하는 분야이다. 사후관리는 크게 4가지로 나누어 질 수 있다.

- 대응책 관리분야 : 본 분야는 글자 그대로 모든 대응책들을 관리하는 작업을 말한다. 관리에는 여러 가지 행위가 포함될 수 있다. 우선 관리는 대응책들을 정기적으로 재평가하고 원래 의도대로 보안 기능들이 동작되고 있는지를 점검한다. 또한 시스템의 변경으로 인하여 대응책들에 어떠한 영향이 없는지를 살펴야 한다. 수행되는 대응책들이 특정 조직이나 특정 시스템에 편중되지 않도록 적절한 배분의 기능도 수행해야 한다.
- 감사(Audit)분야 : 적정 수준의 보안이 유지되고 있는지를 측정하고 각종 보안대응책들이 계획대로 유지되고 구현되었는지를 검사하고 평가하는 분야이다.

감사분야에서는 정보시스템 프로젝트의 경우 계획, 설계, 개발, 운영, 유지보수 등 각 단계에 대한 전반적인 평가가 이루어져야 한다. 감사분야에서 또 하나의 중요한 기능은 준수평가(Compliance Evaluation)와 보안감사(Security Audit) 분야이다. 정보시스템 보안정책을 바탕으로 관련 인력에 대하여 책임과 역할의 적합성에 대한 검사를 수행하게 된다.

- 점검(Monitoring)분야 : 점검분야는 감사분야와는 달리 정보시스템 보안 대응책들이 계획대로 구현되고 있는지의 사실 여부를 파악하여 경영진에게 정확한 정보를 제공하기 위한 것이 목적이다.
- 사고대응분야 : 보안사고는 보안대응책을 적절히 구현하더라도 어떠한 유형으로든 발생한다. 따라서 각 보안사고에 대한 적절한 대응체계 구축이 필요하다. 사고대응의 목적은 크게 2가지로 나눌 수 있다.

우선 사고에 대하여 효과적이고 피해를 최소화시키는 방법으로 대응하는 것이다. 이를 위해서는 각종 사고에 대한 시나리오를 파악하여 사전 대응체계를 구축해 놓아야 한다.

두 번째로 사고의 원인을 파악하여 같은 사고의 재발을 방지하는 것이다. 사고발생 시각과 사고 대처 상황 및 평가 등을 통하여 사고 발생원인을 파악할 수 있고 보안정책부터 사후관리에 이르는 보안관리 전 과정에 유용한 정보를 제공할 수 있다.

Ⅲ. 초고속국가망과 보안

초고속국가망 사업은 2005년까지 공공재원을 선투자하여, 고속·대용량의 정보 전송이 가능한 기간망 및 초고속(ATM)교환망 중심의 초고속정보통신 기반을 구축하는 사업이다. 초고속국가망이란 초고속국가망 사업으로 구축되는 개념적인 통신망으로, 통신사업자가 소유하며 사업 주체인 정보통신부는 국가 및 지방자치단체 등 공공기관이 사용한 이용요금중의 일부를 부담함으로서 통신망 서비스를 저렴하게 이용토록 하여 망의 활용을 활성화하고, 나아가 지식정보사회를 앞당기는데 중요한 역할을 하는 기반망이다.

초고속국가망 이용기관은 이 서비스를 이용하여, 개별 통신망(응용통신망)을 구축·운영 중으로 정부고속망, 지방행정정보망(행정자치부), 체신망(정통부), 국방망(국방부), 교육망(서울대), 연구망 등이 있으며, 이 망은 주로 각 기관만 독점적, 폐쇄적으로 이용하고 있으나, 교육망 (대학), 연구망 (연구기관), 정부고속망 (정부 청사) 등은 다른 기관에도 연결서비스를 제공하고 있다.

초고속국가망을 이용하는 대상이 국가 및 지방자치단체 등 공공기관임에 따라 초고속국가망을 통해 전달되는 정보의 안전한 전송을 위해 망의 구성요소(시설, 전송장비, 교환장비, 정보시스템 등)를 각종 보안 위협요인으로 부터 안전하게 보호하기 위한 대책이 주요 이슈로서 제기 됨에 따라 전쟁, 재난, 재해 시에도 초고속국가망 이용기관에 대해 안정적인 서비스를 제공하기 위해 여러 가지 방안이 구현되어 있다. 95년부터 구축한 모든 광전송로는 지하 매설을 원칙으로 하였으며, 초고속국가망의 특정구간이 비상시 물리적으로 단절되는 경우를 대비해서 우회통신망 구성이 용이하도록 망의 형태를 mesh 형 또는 ring 형으로 구성하였으며 주요 국가기관의 경우 기간망 구간외에 가입자망을 이중화하였다. 또한 우회선로마저 파괴된 경우 마이크로웨이브 또는 위성을 사용하여 임시 응급복구가 가능하도록 구축되어 있다.

한편, 초고속국가망은 한국통신, 데이콤의 2개 사업자를 지정 각자 독립적인 망으로 구축토록 하여 한 사업자의 망이 파괴되었을 경우 타 사업자망을 보완적으로 사용할 수 있도록 상호연동성을 확보하였으며 비상시에 초고속국가망이외에 초고속공중망 및 하나로통신, 두루넷 등의 민간 통신망을 이용하도록 하여 어떤 상황에서도 안정적인 서비스가 제공되도록 되어 있다.

또한, 통신망이 대량으로 파괴되었을 경우 복구 우선순위를 설정하여 국가 주요기관부터 복구토록 하였으며, 통신사업자와 협력체계를 구축하여 장애 발생시 장애구간에 대해 즉각 조치할 수 있도록 되어 있다.

Ⅴ. 결 론

정보화에 따른 정보 의존도가 심화됨에 따라 여러 위협에 의한 정보시스템의 심각한 피해를 방지하기 위한 정보기술 보안이 주요 이슈로 등장하고 있다. 초고속국가망 보안의 범위는 이용기관측면과 통신사업자 측면의 보안대책으로 크게 구분할 수 있다.

정보시스템 보안에 대한 필요성과 중요성에 대한 인식이 커짐에 따라 정부 및 지방자치단체, 산하기관 등 초고속국가망을 이용기관은 각종 보안 솔루션 도입을 추진하거나 정보시스템 보안을 강화하는 노력을 기울이고 있으나 이들 대부분은 체계적인 보안관리를 하지 못하고 있는 상태로 해킹, 화재, 절도 등 위협 발생시 그 피해결과가 얼마나 큰지, 그리고 이러한 위협을 막기 위해서는 어떻게 해야 하는지를 모른 체로 정보시스템을 운영중에 있는 실정이다. 이에 따라 본 논문에서는 체계적으로 보안관리를 하기 위한 정보기술 보안관리 모델을 소개하였으며, 특히 대규모 조직인 경우 본 모델에 따라 보안관리를 수행하는 것이 필요하다.

체계적인 보안관리를 하기 위해서는 그 조직의 보안정책을 수립하는 것이 선행되어야 한다. 이러한 것을 하기 위한 여러 가지 표준연구가 우리 나라에서도 많이 진행되었으며, 표준지침에 따른 각 이용기관의 지침개발과 적용이 필요하다.

아울러, 본 논문에서는 통신사업자 측면에서 국가비상시에도 안정적으로 통신 서비스를 제공하기 위해 전송로의 지중화 및 이중화, 무선망을 이용한 응급복구, 그리고 타 통신사업자 망을 이용하는 방안 등에 대해 소개하였다. 앞으로, 이용기관의 체계적인 보안관리를 위한 위험분석 모델, 방법론, 그리고

평가 등에 대한 연구가 지속적으로 수행되어야 할 것이다.

참 고 문 헌

[1] 이병만, 윤정원, 박승규 "정보시스템 위험분석 모델에 관한연구", 정보보호 및 암호 학술대회, 1998

[2] 공공정보시스템 보안을 위한 위험분석 표준 - 개념과 모델, TTA, 1998

[3] 공공기관 전산보안정책 수립을 위한 지침서, TTA, 1998

[4] 윤정원, 김홍근, "정성적 위험분석을 위한 버디시스템의 구조분석", 한국통신정보보호학회 종합학술발표논문집, 1995

[5] 윤정원, 신순자, 김기수, 이병만, 송관호, "자동화 위험분석 도구(HAWK) 개발에 관한 연구", 한국통신정보보호학회 종합학술발표논문집, 1996

[6] 윤정원, 이병만, "보안사고대응기능과 위험분석의 역할", 전산망 기술 및 표준화 심포지움 발표집, 1996

[7] 윤정원, "Approach to the Behavioral Model of IT Risk Analysis Process"

[8] 이성만, 이필중, "해외의 보안위험분석 방법론 현황 및 분석", 한국통신정보보호학회 종합학술발표논문집, 1994

[9] 신동익, "위험관리 체계연구", 한국통신정보보호학회 종합학술발표논문집, 1994

[10] 김기윤, 김정덕, "정보보호를 위한 위험분석 방법: 분류와 선택기준을 중심으로", 한국통신정보보호학회 종합학술발표논문집, 1994

[11] 임채호, 박태완, 이경석, "전산망 보안을 위한 위험관리 기술지원서 개발연구", 한국통신정보보호학회 종합학술발표논문집, 1994

[12] 한국전산원, 정보시스템 보안을 위한 위험분석 소프트웨어 개발연구, 1996

[13] 한국전산원, 전산망 보안을 위한 위협분석 프로그램에 관한 연구, 1995

[14] 한국전산원, 전산망 보안을 위한 위험관리 지침서, 1994

[15] 이병만, 이민구, 송관호"공공기관의 보안대책 수립에 관한 연구", 정보보호 및 암호 학술대회, 1996

[16] ISO/IEC JTC1/SC27, Guidelines for the Management of IT Security, 1996

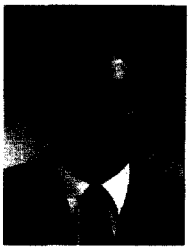
[17] Deborah J. Bodeau, "A Conceptual Model for Computer Security Risk Analysis", in Computer Security Applications Conference, 1992

〈著者紹介〉

이 병 만 (Byeong-Man Lee)
고려대학교 물리학과 졸업
아주대학교 산업대학원 컴퓨터공학과 졸업
성균관대학교 일반대학원 전기전자 및 컴퓨터공학부 박사과정
1982년~1985년 : 금성반도체 컴퓨터기술부 사원
1985년~1992년 : 데이콤 컴퓨터공학연구실 선임연구원
1992년~현재 : 한국전산원 보안기술팀장, 초고속서비스부장/책임연구원
주관심분야 : 네트워 및 컴퓨터 보안, 위험분석, 공개키 기반구조

윤 정 원 (Jung-Won Yoon)
1992년 : Computer Engineering 학사, 캘리포니아주립대
1994년 : Computer Science 석사, 캘리포니아주립대
1995년 3월~현재 : 선임연구원, 한국전산원
2001년 3월~현재 : 초빙연구원, 미국 국립표준기술원(NIST)

신 순 자 (Soon-Ja Shin)
1995년 2월 : 성균관대학교 정보공학과 학사 졸업
1995년 1월~현재 : 한국전산원 주임연구원
주관심분야 : 위험분석, 시스템보안, 전자서명/인증



원 동 호 (Dong-Ho Won)
1976년 : 성균관대학교 전자공학과 졸업
1978년 : 성균관대학교 전자공학과 석사
1988년 : 성균관대학교 전자공학과 박사
1978년~1980년 : 한국전자통신연구소 전임 연구원
1985년~1986년 : 일본 동경공대 객원연구원
1992년~1994년 : 성균관대학교 전산소장
1995년~1997년 : 성균관대학교 교학처장
1996년~1998년 : 국가정보화 추진위원회 자문위원
1990년~1999년 : 한국통신정보보호학회 이사
1998년~1999년 : 성균관대학교 정보통신기술연구소장
1982년~현재 : 성균관대학교 전기전자 및 컴퓨터 공학부 교수
1999년~현재 : 성균관대학교 전기전자 및 컴퓨터 공학부장
(겸)정보통신대학원장, 한국통신정보보호학회 부회장
관심분야 : 암호이론, 부호이론