通信情報保護學會誌
第3卷 第3號, 1993.9

정보시스템 보안과 감사증적 메카니즘

김영철* · 남길현**

1. 서 론

정보통신기술의 발전과 컴퓨터 이용의 증가로 정보화사회가 가속화되면서 정보시스템의 보안문제(security)가 대두되고 이와 관련한 규정과 절차의 중요성이 증대되고 있다. 이는 정보시스템의 유용성에 비해 보유자원의 불법적인 복제·절취·변경·침해등의 컴퓨터 범죄와 오류발생의 가능성이 증가하기 때문이다.

미국, 유럽 등 주요 선진국에서는 정보시스템 보안을 위한 법적, 제도적 및 기술적 연구개발을 오랫동안 추진해 왔으며 최근에는 TCSEC(85년), ITSEC(91년)등 정보시스템 보안평가기준을 설정·발표하고 국제표준화를 주도하고 있다.

우리나라에서도 80년대 중반부터 5대 국가기간전산망사업이 추진되면서 국가·기업등 조직의 기밀, 중요자원 및 프라이버시의 보호 필요성을 그 어느 때보다 강조하고 있으며 근래에는 정부기관 및 산·학·연이 연계하여 정보보호 및 기술표준화를 위한 연구 발표를 활발히 추진하고 있으나 아직은 법적, 제도적 및 기술적 장치가 미진한 실정이다. 특히, 정보시스템과 관련한 보안 메카니즘의 국내개발은 극히 미미한 수준이다.

정보시스템 보안은 단순히 물리적 수단만으로 해결하려는 문서 중심의 정보보호체계와는 다르다. 우선, 접근가능한 정보량이 많고 범위가 광역화되어 있으며, 일단 보안 사고가 일어나면 파급이 크고 사고 추적이 매우 난해하다는 점이 특징이다. 기존의 전산망 개념은 주로 작업효율 향상에 치중하여 보안상의 취약점을 간과하고 있다. 즉, 정보에 대한 불법적 접근허용, 편의성만을 위한 보안수칙생략, 보안에 대한 책임과 한계의 불분명 등이 그것이다. 또한, 보안시스템이 기술적으로 아무리 잘 구성되어 있더라도 완벽할 수는 없다.

따라서, 정보시스템에는 정보의 불법유출을 예방하고 통제원칙의 준수의 불법행위의 추적을 위한 감사능력(auditability)이 확보되어야 하며 정보시스템 관계자의 책임을 명확히 하고 사용자의 행위를 가시화할 수 있는 감사증적(audit trail) 메카니즘이 요청된다. 감사증적은 누가, 무슨 자원(resource)을, 언제, 어떤 순서로 이용했는가를 추적하는 회계측면의 기록성(accountability)에서 출발하여 사용료청구, 통계유지, 백업 등의 수단으로 이용되었으나 최근에는 시스템 자원 사용에 대한 부적합성을 감시하고 기록(log)하는 보안개념이 추가되면서 정보시스템에 대한 불법적 접근을 어떻게 추적하느냐가 중요한 관심사로 등장하고 있다.

본 고에서는 정보시스템의 목적, 보안 목표 및

* 통신정보보호학회 정회원, 국방대학원
** 통신정보보호학회 종신회원, 국방대학원

각종 위험을 살펴보고 정보 시스템에 대한 보안 감사의 필요성, 목적 및 범위를 고찰하며, 감사증적의 배경, 목적 및 주요 요구기능을 살펴보고 기존의 감사증적 메카니즘을 비교, 분석하여 감사증적과 관련한 개괄적인 보안대책을 제시하고자 한다.

2. 정보시스템 보안감사의 특성

2.1. 정보시스템 보안

정보시스템이 "컴퓨터, 자료 및 통신망을 축으로 하여 법, 제도, 조직, 시설, 인원 등이 유기적으로 결합된 개념"으로 확장되면서 정보시스템 보안의 범위도 넓어지고 있다. 이는 정보순환체계가 문서중심에서 컴퓨터와 통신중심으로 변모, 발전하고 있기 때문이다.

가. 정보시스템의 목적 및 속성

정보시스템은 완전하고 정확하게 승인된 정보를 적합한 사용자에게 원하는 시간에 일관성 있게 제공함을 목적으로 하며 효과성(effectiveness), 효율성(efficiency) 및 보안성(security)을 기본 속성으로 한다. 효과성은 목적의 달성정도에 관계되며 효율성은 목표달성을 위해 투입된 자원의 수량에 관련된다. 보안성은 효율성과 효과성을 저해하는 제반 위협으로부터의 보호측면이다.

나. 보안목표

정보시스템 보안의 기본 목표는 중요정보, 시설 및 장비, 프라이버시에 대한 보호와 가용성의 향상에 있다. 즉, 비밀성(confidentiality), 무결성(integrity) 및 가용성(availability)이 만족되어야 한다[남길 91].

① 비밀성은 정보가 외부로 노출되지 않는 상태를 의미하며 권한이 없는 비인가자가 시스템자원을 이용할 수 없도록 제어하여야 한다.

② 무결성은 불법적인 자료변경을 막는 것을 말한다. 무결성을 위한 메카니즘으로는 물리적 통제와 접근제어 등이 있으나, 이미 변경되었거나 변경될 위험이 있는 경우 탐지 및 복구를 위한 메카니즘이 요구된다.

③ 가용성은 적법한 사용자가 적시에 필요한 정보를 효율적으로 사용하는 것을 말하며 실용성(practicability)과는 다른 의미를 갖고 있다. 가용성유지를 위한 요소로는 중복성(redundency), 백업, 물리적 위험 요소로부터 보호 등이다. 또한, 지나친 보안의 강조는 가용성을 저하시킬 수 있다.

다. 위협과 위험요소

위협(threats)은 위험(risks)을 발생시킬 수 있는 조건, 상황 및 원인이다. 위험은 위협으로부터 연유하며 노출(exposure), 손실 및 부정적 영향을 초래하는 결과이다.

기존의 일괄처리(batch processing) 시스템에서는 시설, 인원 등 물리적 보안측면이 주요 관심사였으나 최근들어 분산처리, 근거리통신망(LAN) 등이 구축되면서 위협요소는 확산되고 불법적 정보이용 등 역기능 또한 증가추세에 있다. 정보시스템의 위협요소는 표 1과 같이 분류될 수 있으며, 특히 정보의 입력, 처리 및 출력 과정에서의 인위적 위협과 조직, 절차상의 위협에 대한 우려가 높아지고 있다. 일반적으로 인위적 위협은 외부위협(10%) 보다 내부위협(90%)에 기인하며 내부위협중 비관리층(17%)보다 관리층(83%)에 의한 위협이 높은 것으로 알려져 있다[TDO 92].

정보시스템이 취약하고 위협이 가중되면 여러가지 유형의 위험이 발생될 수 있으며 주요 위험요소로는 정보누출(disclosure), 변조(modification), 파괴

표 1. 정보시스템의 위협요소

물리적 위협	- 자연재해(홍수, 지진, 번개, 태풍 등) - 환경재해(화재, 정전기, 먼지, 오염물질 등)
인위적 위협	- 내부/외부인의 고의, 과실, 실수 등
기술적 위협	- 하드웨어, 소프트웨어 및 통신망의 결함
조직, 절차상의 위협	- 잘못된 정보화 정책 - 사보타지, 태업 - 책임과 권한의 집중화 현상 - 불합리한 업무분장 - 부서간의 마찰 - 부적절한 인사관리 - 절차나 규정에 대한 이해부족 및 오용

(destruction) 및 오용(misuse)등이 있다.

① 정보누출은 정보시스템이 비밀성을 제공하지 못할 때 정보가 비인가자에게 전파되는 현상이다. 그러나 사용자가 비밀자료의 내용 일부를 임의로 변경하여 보안메카니즘을 회피할 수 있기 때문에 비밀정책을 위반하지 않고도 비밀성을 잃을 수 있다.

② 변조는 정보의 내용을 바꾸는 행위를 말하며 무결성정책의 결함을 의미한다. 이는 정보를 노출시키지 않고도 비밀성을 위협할 수 있다. 즉, 변조행위가 발견되지 않으면 계속 올바른 정보로 여겨질 수 있다.

③ 파괴는 정보의 형태나 내용을 못알아보게 하는 행위로서 가용성과 대응된다.

④ 오용은 사용자가 정보를 잘못 사용하여 비밀성을 위협함으로써 정당한 사용자까지도 사용할 수 없는 경우이다.

2. 정보시스템의 보안감사

감사(auditing)는 특정조직의 자원처리와 보안이 정해진 규정에 따라 올바르게 수행되는가를 조사하는 제3자의 독립된 활동이며 정보시스템 감사는 정보시스템의 활용기술과 운영을 감사대상으로 한다[감사 90].

정보시스템 보안감사는 정보 시스템의 취약요소를 종합적으로 점검, 평가하여 관계자에게 조언, 권고함으로써 보안측면의 피해를 최소화하는 등 건전한 시스템을 도모하는 특징을 보인다.

가. 필요성

컴퓨터에 대한 의존도가 높아지면서 정보시스템의 신뢰성, 안전성 및 효과성의 점검은 조직내부와 사회적 요청이 되고 있다. 조직내부의 요청으로는 오류발생 컴퓨터범죄, 재해피해 등의 극소화와 긴급복구, 기밀보호, 효율성의 추구 등이 있으며 사회적 요청으로는 프라이버시보호, 범죄방지 등이 포함된다.

감사인(auditor)의 입장에서는 내부통제의 신뢰성, 효과성 및 감사증거의 확보가 필요하다. 감사인의 감사활동을 통해 보안침해의 기록을 분석함으로써 침입자를 추적해 내거나 공격 방법 등을 알아낼 수 있으며 침입자에게 사후 발견가능성을 예고함으로써 사전 예방효과를 얻을 수 있다.

나. 목 적

정보시스템은 자연재해, 불법접근 등 물리적, 인위적 위험으로 부터 안전하게 보호되고 관리되어야 한다. 이를 위해 다음과 같은 사항에 대한 조사, 평가 및 보고가 보안감사의 목적에 포함되어야 한다.

① 시스템개발, 운용 및 유지보수의 기준과 절차에 관한 신뢰성을 구축하고 있는가?

② 규정된 기준과 표준절차를 준수하고 있는가?

③ 데이타의 보안과 긴급시 대책은 어느 정도인가?

④ 하드웨어/소프트웨어 취득에 관한 요구는 타당성이 있는가?

⑤ 자원의 보호수준은 어느 정도인가?

다. 보안감사의 범위와 감사인의 역할

정보시스템의 보안감사는 내부감사(internal auditing)와 업무감사로 구분된다. 내부감사는 내부통제(internal control)와 시스템 보안의 유효성을 평가하며 업무감사는 직무수행, 보고서 등의 적법성을 대상으로 한다. 내부통제는 감사인이 전산부서에서 시행하는 물리적 통제기법이며 조직환경에 따른 접근권한의 통제와 시스템개발, 변경, 유지, 회복 등을 대상으로 완전한 문서화와 정확한 보고능력을 갖추도록 한다.

종래의 보안감사는 정보시스템 처리결과를 조사, 분석하는 사후 평가로 인식되었으나 최근에는 시스템의 기획, 개발, 운용 등 전체적인 측면을 범위로 하고 있다. 또한, 감사인의 관점에서는 시스템의 유효성과 효율성 측면보다 보안대책을 강조하는 경향을 보인다. 미국 EDP 감사인협회는 정보시스템 보안감사의 범위를 표 2와 같이 정하고 있다.

감사인(auditor)은 기본적으로 자원보호(resource secruity)와 내부통제의 유효성과 타당성을 검토하고 시스템의 변경관리(change management)와 개발과정에 참여하며 보안메카니즘을 평가한다.

① 시스템의 변경관리는 응용 S/W의 개발과 유지,

표 2. 정보시스템 보안감사의 범위

일반 통제	- 일반적 조작절차의 통제 및 보안성 검토
운영시스템	- 응용시스템(application system)통제 검토 - 데이타완전성 및 시스템 S/W 검토
H/W 및 자원	- 획득 및 자원 검토
S/W개발 및 변경	- S/W개발 및 유지관리 검토

S/W와 H/W 제품의 도입 및 운영체제의 개선 등을 포함한다[Paan 90].

② 시스템 개발과정의 감사관점은 다음과 같다[Morr 90].

▷ 사용자의 요구에 맞게 작동되는가?

▷ 시스템통제/사용자 요구를 제한하는 객관적 근거가 있는가?

▷ 전체 개발과정의 구조가 갖추어져 있는가?

▷ 시스템개발은 시스템통제와 명확히 구분되고 있는가?

그림 1은 시스템 개발주기(SDLC : System Development Life Cycle)와 감사인의 관계를 나타낸다.

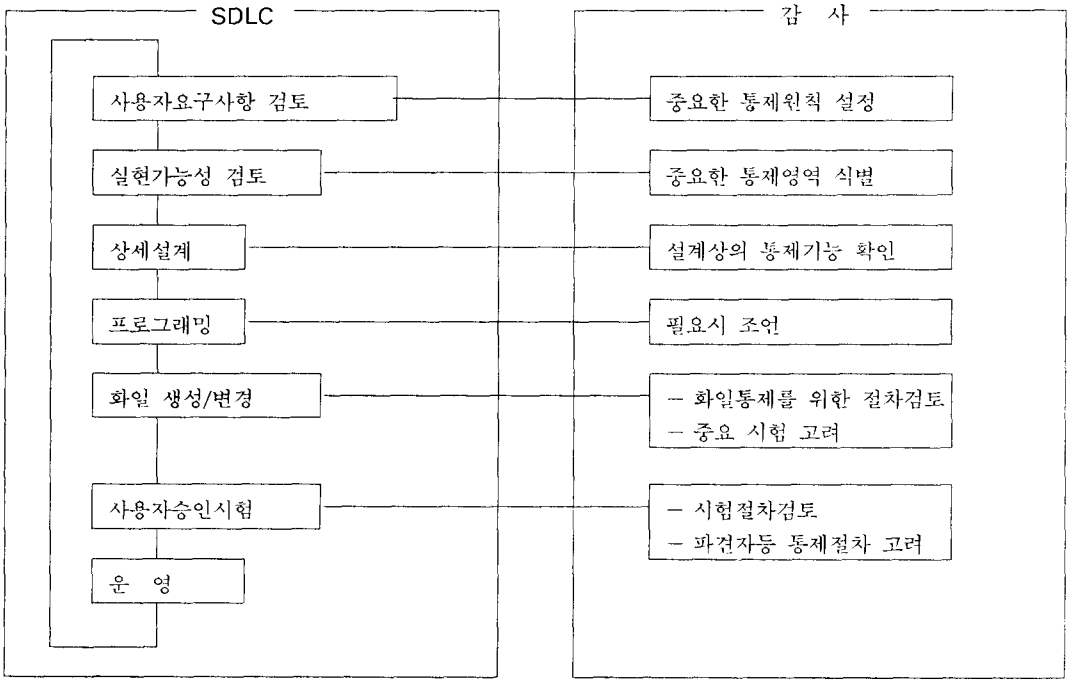

그림 1. 시스템 개발주기와 감사인의 역할

③ 감사인은 보안메카니즘의 평가지침과 기준을 설정하고 보안기능을 평가하며 다음사항을 검토한다[GISA 89].

▷ 보안정책 중 어느 부분이 구현되어 있는가?

▷ 어떤 취약성이 있으며 다른 메카니즘에 어떤 영향을 주는가?

▷ 취약성방지를 위해 어떤 수단이 필요한가?

3. 전산업무 보안관리 지침

우리나라는 국가기간전산망 사업이 추진되면서 정보시스템의 안전성 및 신뢰성 확보를 위한 노력이 가중되고 있다. 86년 전산망보급확장과 이용촉진에 관한 법률을 기반으로 「전산망조정위원회」가 발족되어 법령정비와 제도의 개선을 추진하는 한편,

표 3. 「전산업무보안관리지침」의 주요 내용

구 분	주 요 내 용
전산실	- 통제구역설정 및 출입인가자명부 비치 - 비밀자료입력용 보조기억장치 별도지정 및 출력시 비밀등급, 장비번호, 면수, 일시등 자동표시 - 보조기억장치별 입출력관리대장 유지 - 관리책임자는 주전산기에 내장된 작업기록과 입출력관리대장을 월1회이상 대조, 확인 및 점검
단말기	- 단말기별 관리책임자 지정, 운용 - 비밀자료입출력시 입출력관리대장 기록 - 비밀번호(password), 단말기사용설명서, 디스켓 관리 - 비밀번호는 단말기, 취급자 및 화일별로 구분하여 분기 1회이상 변경사용 - 비밀자료전송시 암호화 및 인가된 보안장비운용
워드프로세서	- 관리책임자지정 및 비밀번호사용 - 비밀자료입출력시 비밀등급표시, 소자처리 및 입출력관리대장 자동기록유지
기타	- 전산출력된 비밀자료수령자는 비밀관리기록부 유지 및 관리번호부여

한국전산원이 설립되어 전산망의 역기능 예방을 위한 안전·신뢰성을 검토하고 감리기능을 수행하고 있다.

한편 「국가정보자료관리규정」을 기반으로 88년에 「전산업무보안관리지침」을 제정하여 표 3과 개괄적인 보안요구사항을 규정하였다.

과학기술처에서는 89년 「컴퓨터시스템 안전관리기준」을 발표하는 한편, 「전자계산조직위」를 설치하여 안전대책을 심의하도록 하였다. 체신부에서는 90년 「정보통신설비에 관한 안전신뢰성기준」을 제정하여 전산망의 안전성, 신뢰성 및 장애대책을 규정하고 있으며, 총무처에서는 「개인정보의 보호에 관한 법률」을 입법화할 예정이다.

3. 감사증적 메카니즘과 보안대책

1. 감사증적의 이론적 배경 및 목적

감사증적은 원래 회계(accounting) 감사에서 사용한 용어로서 어떤 사용자가 무슨 자원을 얼마나 사용했는가를 기록하는 logging 개념에서 출발하였으나, 정보시스템의 보안개념이 추가되면서 최근에는 정보시스템에 대한 불법적 접근을 어떻게 추적하느냐가 중요한 관심사로 등장하고 있다. 따라서 감사증적은 회계 및 보안감사에 필요한 정보를 적절한 시간내에 추출하여 제3자에게 합리적으로 설명가능하도록 추적할 수 있는 능력으로 정의된다 [감사 90]. 그러나 본 연구에서는 정보시스템 감사증적의 목적을 다음과 같은 범위로 제한한다.

① 사용자/프로세스가 객체에 대해 접근하는 상황을 검사한다.

② 보안메카니즘을 우회하려는 불법적 시도를 기록한다.

③ 중요한 객체의 접근상황을 기록하여 관계자에게 제공한다.

2. 주요 요구기능

정보시스템 감사 증적의 목적을 실현하기 위해서는 불법적 접근시도에 의해 침해되지 않도록 감사기록을 안전하게 관리하여야 한다. 이를 위해 비밀성, 무결성 및 가용성을 만족하는 메카니즘이 요구되며 이러한 메카니즘을 관리하는 보안담당자가 지정되어야 한다.

가. 메카니즘

감사기록에는 불법적인 login시도, 사용자의 시스템사용/종료시간, 객체의 식별자(identifier), 사용시간 등의 필요한 사항들이 포함되어야 한다. 이를 위해 정보시스템은 정확한 날짜와 시간을 제공하여야 하며 다음의 요구사항을 충족하여야 한다.

① 감사증적과 관련한 자원보호를 위해 패스워드의 불법적 사용/변경, 지정된 사용자의 행위, 시스템 명령어의 부당한 사용 등을 감시하는 메카니즘을 갖추어야 한다.

② 지정된 자원에 대한 접근, 침해 및 변경의 실패/성공 등을 감사기록하고 보관하며 보관된 감사기록에 대하여 사용자의 신분 또는 객체의 비밀수준 등을 key로 하여 조회할 수 있어야 한다.

③ 보안침해에 대한 대응조치가 구비되어야 한다.

④ covert 채널의 비인가된 정보흐름에 대한 감사기록이 요구된다. 여기에서 covert 채널이라하은

프로그래머 자신만이 알 수 있는 은밀한 표시를 통해 중요 정보를 파악할 수 있는 비밀통로를 의미한다.

위의 요구사항이 만족되기 위해서는 감사증적 메카니즘과 감사기록 자체에 대한 불법적인 접근, 변조, 우회침투 등을 방지할 수 있는 대책이 강구되어야 한다[Glig 86].

나. 보안담당자(Security Officer)

조직의 책임자는 정보시스템 자원의 보호의 보안메카니즘의 적절성을 평가할 수 있는 보안담당자를 정하여야 한다. 보안담당자는 정보시스템의 overhead를 고려하여 다음과 같은 감사증적의 관리기능을 수행한다.

① 정보시스템의 보호대상자원을 설정하고 보호수준을 정의하며 사용자의 접근 권한을 관리한다.

② 보호대상자원의 접근을 감시하는 접근제어 메카니즘을 검사한다.

③ 기록성(accountability), 감사능력(auditability), 무결성(integrity), 유용성(usability) 등의 보안요구기능이 어떻게 수행되는지를 평가한다. 기록성은 인가된 사용자가 가용자원에 접근할 때의 감사기록을 의미하며 보안 목적 보다는 회계목적에 치중한다[Perr 84]. 감사능력은 불법적인 접근시도, 보안침해 등 보안목적의 감사기록을 생성하며, 감사 기록은 보안담당자에게 제공되어야 한다. 무결성은 시스템 전체의 일관성 및 완전성을 확보하기 위해 시스템을 감시/보호하는 활동이다. 유용성은 사용자에게 무리한 제약을 가하지 않고 기록성, 감사능력 및 무결성을 제공할 수 있는 기능이다.

④ 보안 소프트웨어(S/W)의 특징을 검토하고 적합성을 확인한다. 보안담당자는 사용자별 보안책임을 정의하고 보안요구사항을 기록, 확인하여야 하며 보안 S/W에는 다음과 같은 사항이 만족되는지를 검토한다.

- ▷ 요구된 보호수준
- ▷ 시스템 overhead의 수용수준
- ▷ 기록성, 감사기능, 무결성 및 유용성 등의 요구사항

이를 위해 보안담당자는 조직의 보안요구사항과 보안 S/W의 능력에 대한 교차참조(cross-referencing) checklist를 이용한다[Perr 84].

⑤ 보안 S/W의 특징을 시험한다. 이는 보안 S/W를 취득하기 전에 보안 S/W가 바람직하게 작동되는지를 시험하여 보안 S/W의 적절성에 관한 의견을 제시한다. 의견의 제시는 구입의 권고가 아니라 보안통제의 적절성에 대한 판단이며 관리자가 결정하기 전에 통제중심(control-oriented)의 정보를 제공하여야 한다.

3. 기존의 감사증적 메카니즘

감사증적 메카니즘은 IBM등의 메인프레임(mainframe)과 UNIX등의 워크스테이션 환경에서 운영되는 보안패키지(security package)를 중심으로 발전하는 추세를 보인다.

IBM 메인프레임과 관련한 감사증적 메카니즘은 GUARDIAN, RACF, ACF2, SECURE, SAC, TOP SECRET등이 있으며, UNIX와 관련된 메카니즘은 Trusted DG/UX, CMW(Compartmented Mode Workstation)등이 있다.

가. GUARDIAN

GUARDIAN은 IBM CICS(Customer Information Control System) 환경에서 보안, 감사 및 통제능력의 제고를 위해 개발된 패키지이다. 이는 기존의 CICS가 통제보다는 생산성에 치중하며 시스템기록(CICS Journal)은 단순히 백업기능만을 제공한다는 보안상의 취약성(vulnerability)을 개선한 OSI(Online Software International) 제품이다[Moll 84].

① 기밀로 분류된 각 기능별 자원을 보호하기 위한 보안기능을 제공한다.

② 사용자의 권한(authorization)은 시스템에 저장된 정보에 따라 감시되고 변경된다. CICS의 효율적인 통제는 시스템의 모든 접근과 생성을 완벽하게 감시하여야 하고 알기쉬운 감사기록이 있어야 한다. 그림 2는 보안 및 감사기능이 통제에 미치는 영향을 설명하고 있다.

한편, GUARDIAN은 정보누출을 방지 하기 위해 프로세스를 검사하고 CICS 활동을 감시하며 기록하는 한편, 식별된 에러, 보호자원 및 보안정책에

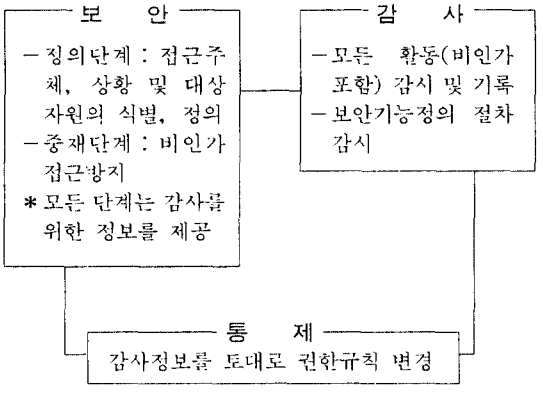

그림 2. CICS에서의 GUARDIAN cycle

관한 리스트와 감사증적의 자동생성을 포함하여 여러가지 표준레포트를 제공한다. 각 레포트에는 시간, 단말기, 트랜잭션, 사용자(last singed-on user), 활동 내용 등이 포함된다. 감사인은 원거리 단말기를 통해 의심나는 단말기의 활동을 감시하고 시험할 수 있다.

나. RACF(Resource Access Control Facility)

RACF는 IBM OS/MVS(Multiple Vertual Storage)의 확장개념으로 작동하며 자원보호를 위한 접근제어와 접근시도에 대한 감사기록 기능을 갖추고 있는 패키지이다[Perr 84]. 이는 시스템자원에 대한 각 사용자의 접근권한을 토대로 사용자의 식별, 권한의 검사 및 감사기록을 수행한다.

① 사용자의 식별을 위해 사용자 id와 패스워드를 사용하며 패스워드는 사용자의 보안등급에 따라 정기적으로 보안담당자 또는 당사자에 의해 변경되도록 한다.

② 권한검사를 수행하는 GACF(Global Access Checking Facility)를 호출하며 GACF는 내장된 테이블을 통해 자원접근의 허용여부를 결정한다. 사용자/그룹의 권한과 자원에 대한 접근수준을 계층별로 분류하고 있다.

③ 사용자/그룹별, 일자/접근권한별 통계정보를 옵션으로 제공하는 한편, multiple group membership, 프로그램의 제어, Masking/치환, migration 등의 관리를 위해 사용자 복귀(user exit)에 강하게 의존한다.

RACF는 운영체제의 부품인 SMF(System Management Facility)를 통해 정보시스템에서 일어나는 profile변경, RACF명령어수행, RACF옵션사용, 보호자원접근, 비인가된 접근시도 등의 사건을 기록하고 보안콘솔에 표시한다.

다. ACF2(Access Control Facility 2)

ACF2는 70년대말 메인프레임, 테이프화일 등의 접근제어를 위해 CA(Computer Associates)가 상품화하여 은행, 기업 등에서 광범위하게 활용되고 있다[Perr 84]. 이는 IBM MVS, VS1등의 운영체제와 호환성이 있는 패키지로서 시스템 자원에 대한 비인가된 접근을 검사하며 보호된 명령어에 대한 접근규칙(access rules)을 제공하여 보안환경에 맞는 data-set을 구성하도록 하는 융통성(flexibility)을 갖추고 있다.

① MVS의 무결성 유지와 자동보호(default protection) 기능을 제공하고 운영체제의 변경없이 공유(sharing) 자원의 접근권한을 검사하며 기존의 운영체제가 가진 무결성 결함을 해결한다. 또한, 보안담당자가 보호대상자원과 사용자의 관계성(relationship)을 TSO(Time-Sharing Option)를 통해 정의하면 자동보호기능이 작동된다. 이는 사용자에 대한 교육기능과 유용성(usability)을 향상시킬 수 있다.

② 식별자의 관리를 위해 Uid(User identification) string과 표시(Masking)를 사용한다[CAI 88]. Uid string은 사용자와 group의 식별을 위한 일종의 접합문자(concatenation character)이며 조직의 계층구조에 따라 그림 3과 같이 구성 할 수 있다. 이러한 string은 사용자의 부서변경 또는 grouping 등에 효율적으로 이용된다.

표시는 data-set에 대한 접근규칙을 간소화하는데

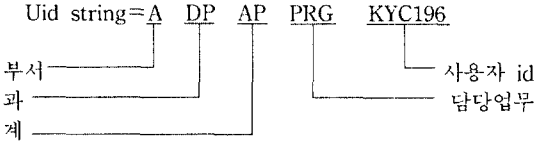

그림 3. Uid string의 구조

모든 프로그래머	*****PRG
모든 응용프로그래머	***APPRG
A부서의 응용관리자	A**AP
A부서 DP과의 모든 분석가	ADP**AST
DP과의 모든 직원	*DP
사용자 KYC196	********KYC196

그림 4. Uid string을 표시하는 예

목적이 있다. 그림 4는 특정 data-set에 대한 접근권한의 검사를 위해 사용되는 Uid string을 표시하는 예를 보이고 있다.

③ ACF2의 자원(resource)은 data-set과 시스템 자원으로 구분되며 융통성과 성능개선을 위해 시스템 접근제어, data-set 접근제어, 시스템자원 접근제어 등 3가지 유형의 접근제어 방법을 제공한다.

④ 보안관리(security administration) 기능의 분리이다. 이는 사용자의 관리권한(administrative authority)과 처리범위를 제한한다[CAI 88]. 보안담당자는 시스템관리자, 오퍼레이터, 일반사용자 등의 권리권한을 시스템 환경에 따라 분산(decentralization) 시킬 수 있다.

라. SECURE, SAC(Security Access Controls) 및 TOP SECRET

IBM 메인프레임의 감사증적 메카니즘은 GUARDIAN, RACF 및 ACF2 외에도 조직의 보안요구수준에 따라 여러 종류로 개발, 발전되고 있다.

SECURE는 IBM OS/VS1, MVS등 운영체제에 보안기능을 추가, 수정한 Sunnyvale CA 제품이며 다음과 같은 특징을 갖는다[Perr 84].

① JCL(Job Control Language) 중심이다. 즉, JCL의 변경에 따른 융통성이 떨어질 수 있다.

② 보호된 자원접근시 모든 접근시도에 대한 내부기록능력을 갖춘다.

③ 시스템의 overhead는 1% 미만이지만 enrty 수가 증가하면 패스워드 data-set이 커져 성능하락의 요인이 된다.

SAC은 IBM OS/VS1, MVS, DOS/VSE등 운영체제의 능력을 개선하기 위해 개발된 미국의 Goal Systems 제품이며 ACF2와 같이 사용자가 정의한 접근규칙을 통해 자원을 보호한다[Perr 84]. 이는 업체제공 S/W 등 모든 시스템자원의 보안통제가 가능하고 CICS, IMS등을 지원한다.

TOP SECRET는 CGA Software Products Group의 제품으로 다음과 같은 접근자중심(accessor oriented)의 특성을 갖는다.

① 모든 사용자는 개인/그룹중 하나로 정해지며 모든 권한규칙은 전체규칙(global rules)과 공유규칙(shared rules)으로 정해진다. 전체규칙은 모든 사용자레코드에 유지되고 공유규칙은 사용자 profile에 정의된다.

② data-set은 DSCB(Data Set Control Block)를 통해 선택적(optional) 또는 자동으로(by default) 보호된다.

③ 기록(logging)은 SMF 또는 온라인 감사화일에서 수행되거나 두가지 모두 가능하다. 시스템이 운영되는 도중에도 내장된 레코드생성자(record generator)를 통해 무리없이 감사레코드에 접근할 수 있다.

마. Trusted DG/UX

미국 DGC(Data General Corporation)에서는 DoD/NSA의 요구수준을 만족하고 편의성(easy-of-use), POSIX(Portable Operating System Interface for computer environment)등의 표준을 유지하며 성능하락을 8% 이하의 보증을 목표로 TCSEC의 C2와 B1 등급을 만족하는 두 종류의 UNIX를 개발하였다[TDO 92].

Trusted DG/UX는 TCB(Trusted Computing Base)를 통해 모든 보안정책과 시스템자원의 사용 및 소유권한(possess privilege)을 제어한다. TCB는 보안정책 Subsystem, SM(Session Monitor), RM(Reference Monitor), 인증(Authentication) 및 권한(Authorization) Subsystem, UFIA(User File Information Area), 감사 Subsystem 등과 관련된다. UFIA는 기존 시스템과의 호환성이 있으며 할당된 디스크 i-node의 비사용공간을 이용하여 화일의 보안속성(security attributes)을 저장한다. 감사 Subsystem은 보안정책의 위반사항을 검사, 보고하며 내부/외부의 위협을 기록, 탐지 및 격리(isolate)

시키기 위하여 병렬처리기법의 일종인 fine-grained 기능을 사용한다. 또한 주체/객체의 표시를 위한 감사 mask를 이용한다. 보안관련 사건(event)은 이러한 mask를 통해 감사되며 사건은 객체에 대한 주체의 접근 또는 보안상태(security state)의 변경을 의미한다. 예를 들어, log-in 및 패스워드의 변경 등이 사건이 될 수 있으며 이러한 사건은 type과 원인코드로 정의되어 감사의 대상이 된다.

바. CMW(Compartemnted Mode Workstation)

CMW는 미국 DIA(Defense Intelligence Agency)의 의해 첨단수준의 보안기능과 상업성을 목적으로 MITRE에서 개발되었으며 TCSEC의 B1 등급을 요구하는 CMWRESQ(DIA Document DRS-2600-5502-86)를 수용하여 SUN 2/120의 UNIX 4.2 BSD (Berkeley Software Distribution) 환경에서 구현된 프로토타입이다[Cumm 87].

CMW는 독자적인 보안기능을 갖춘 프로그램의 조정(accommodation), DAC, 객체재사용, Labeling, MAC, 사용자의 식별 및 인증, trusted path, 시스템의 무결성, TFM(Trusted Facility Management)등의 기능을 제공한다.

CMW의 감사 Subsystem은 사건의 type과 사용자를 기반으로 감사대상을 정하고 정해진 사건이 발생하면 감사자료를 수집하여 저장하는 절차를 거친다. 저장된 감사자료는 보안담당자에게 감사목적으로 제공된다[Cumm 87]. 또한, 사용자 편의성과 유연성을 제공하며 감사기능을 사용자 인터페이스 수준, 응용(application)수준, 사용자/운영체제 인터페이스수준 및 운영체제 내부수준으로 구분하고 있다[Picc 87].

4. 특성비교 및 분석

가. IBM 메인프레임 환경의 감사증적 메카니즘

RACF, ACF2, SECURE, SEC 및 TOP SECRET는 IBM 메인프레임 환경에서의 보안정책, 감사능력(auditability), 무결성(integrity) 및 유용성(usability) 측면의 향상을 도모하는 특성을 갖고 있다.

① RACF는 data-set의 보호를 위해 DSCB에 bit를 세우는 방법으로 시스템 테이블을 정의한다. 이는 방대한 data-set을 생성할 수 있으나 전체적인 보안정책을 세우기 어렵다. RACF의 보안정책은 전체적인 규칙정의가 아니라 요구수준에 따라 변경되는 사용자복귀(user exit) 수준에서 구현되며 이러한 사용자 복귀는 사용자의 요구변화에 민감하여 보안상의 취약요소로 작용한다.

② ACF2는 모든 자원이 자동보호되고 사용자가 정한 수준에 따라 모든 접근이 감시된다. 이는 정해진 변수범위에서 시스템의 개입없이 새로운 보안정책을 구현할 수 있으며 일단, ACF2가 보호하는 자원을 풀기 위해서는 특별한 절차를 필요로 한다.

③ SECURE는 DSCB에 bit를 설정하는 등 많은 시스템지원을 요구하며 감시기능은 AIS(Access Identification String)와 보호코드의 작용으로 이루어진다. 이러한 알고리즘적 과정은 JCL 데이타에 기초함에 따라 보안기능 설정을 위해서는 많은 JCL 변경을 수반한다.

④ SAC은 시스템 테이블에 정의된 모드(mode), 단말기 id, 패스워드 등 변수를 근거로 사용자를 검증(verification)하고 사용자의 권한에 따라 트랜잭션을 검사한다. 또한 화일에 대한 접근은 사용자의 권한수준에 의거하여 검사된다. 이러한 전체적인 규칙(universal rules) 정의는 보안패키지의 수정없이도 융통성을 제공한다.

⑤ TOP SECRET에서는 모든 사용자의 권한을 다음 3가지 접근규칙 중 하나와 연결되도록 한다.

- ▷ 레코드의 일부 항목(item)만을 허용하는 규칙
- ▷ profile로 참조되는 공유규칙(shared rules)
- ▷ 모든 레코드에 적용되는 일반규칙 (common rules)

이러한 구조는 모든 사용자의 권한을 구획화(compartmentalized)하며 시스템관리자들의 월권행위를 방지할 수 있다.

감사능력은 시스템에 대한 접근, 접근시도, 사용, 보안침해 등의 감사증적을 생성하고 보고하는 능력으로서 IBM 계열의 마카니즘은 data-set의 접근, 침해 및 변경을 식별하는 사건기록(event logging)을 이용하며 시스템관리자에게 보안사건을 보고하는

도구(tool)를 제공한다. 한편, ACF2의 기록자료(documentation)는 양이 많고 비체계적이며 감사목적에 맞는 보고기능이 미흡하다는 지적이다 [Perr 84].

대부분의 메카니즘은 사용자에게 투명성(transparency)을 제공하지만 보안정책을 수정하는 경우에는 메카니즘에 따라 다른 면모를 보이며 ACF2, SECURE 및 SAC은 시스템 overhead가 1% 미만으로 평가된다.

나. UNIX 워크스테이션 환경

UNIX 워크스테이션 환경에서 운영되는 Trusted DG/UX와 CMW는 보안정책측면에서 매우 유사한 특성을 보이는 반면, 감사능력 측면에서 다른 면모를 보인다.

① Trusted DG/UX는 POSIX 표준에 준용하는 접근제어 수단을 제공하고 모든 보안정책은 kernel 수준에서 구현된다. 또한, TCB를 매개로 하여 보안정책을 제어하며 시스템에서 일어나는 사건의 type과 원인코드를 시스템 테이블에 mapping하여 감사레코드를 생성하고 감사증적에 기록하며 감사기록(audit log)은 감사증적과 다른 개념으로 인식한다.

② CMW에서는 보안담당자와 일반사용자를 엄격히 구분하여 kernel 수준에서 보안정책을 실행하며 TFM을 매개로 보안담당자, 시스템 관리자 및 오퍼레이터의 권한을 제한하고 상호간에 견제하도록 한다. 또한, 시스템에서 일어나는 사건을 기반으로 감사레코드를 생성하는 관점은 Trusted DG/UX와 비슷하나 저장과정에서 차이를 보인다. 생선된 감사레코드는 임시기억장치에 기록되고 기록된 감사레코드는 background 모듈에 의해 축약(compression) 되어 감사증적 화일에 저장된다.

다. 우리나라 현실에서의 전망

IBM계열의 운영체제는 성능(performance)과 효율성(efficiency) 측면에서 인정을 받고 있으나 IBM 고유의 폐쇄적 속성으로 인하여 운영체제에 대한 분석적 접근이 어려운 반면, UNIX 계열은 고유의 개방적 속성으로 인하여 조직환경에 따라 여러가지 수준으로 변형/발전되고 있다. 최근에는, UNIX계열이 특정 단체나 기업에 의해 발전되는 수준을 벗어나고 있으며 X/Open, USL(UNIX System Laboratories), OSF(Open Software Foundation) 등에 의해 표준안들이 제정되기에 이르렀다. 표준안에는 XPG3(X/Open Portability Guide)와 IEEE가 제정한 POSIX등이 있다. 또한, 개방시스템(open system)이 대두되면서 IBM까지도 OSF에 가입하는 등 UNIX에 접근하는 경향을 보인다.

우리나라에서도 국가기간전산망 사업이 추진되면서 190여대의 주전산기 I 이 보급되어 운영중에 있으며 주전산기 I 은 UNIX system V와 BSD를 기반으로 고장허용기능(fault tolerancy)과 다중처리기능을 추가하여 TX운영체제를 구축하고 있는 한편, 주전산기II에는 POSIX, 주전산기III에는 분산운영체제(DCE/ONC)를 표준화 목표로 채택하고 있다.

또한, 국산 주전산기 활용을 촉진하기 위해 정보통신전문리스회사의 설립을 추진하는 등 UNIX와 관련된 제품의 보급에 주력하고 있다.

1) 보안정책측면

RACF, SECURE, SAC등의 IBM 패케지는 독자적인 보안정책을 설정/운영함에 따라 객관적인 평가가 어렵고 운영체제 수준의 중재가 없이 사용자복귀(user exit) 또는 JCL 수준에서 보안정책이 변경되거나 실행됨으로써 무결성보호에 위협이 되고 있는 한편, UNIX 계열에서는 모든 보안정책이 공인된 평가기준에 의거, kernel 수준에서 변경되고 실행됨에 따라 IBM계열 보다는 효율적인 보안정책 수행이 가능한 것으로 보인다.

우리나라의 경우에도 기술적 보안정책에 대한 공인된 평가기준이 정립되어야 하며 이러한 평가기준에 따라 조직환경에 맞는 보안정책을 수행하고 변경할 수 있는 절차가 마련되어야 할 것이다. 또한, 감사증적 메카니즘은 보안정책의 변경에 대한 영향을 최소화하는 유연성을 갖추어야 하며 보안정책을 전담관리하는 보안담당자가 지정되지 않으면 안 될 것이다.

2) 감사능력수준

앞서 고찰된 모든 감사증적 메카니즘은 시스템에서 일어나는 사건을 시스템 테이블에 내장된 사건유형과 mapping함으로써 감사기록을 생성하고 저장하여 보안담당자/감사인에게 제공하는 공통점을 갖는다.

따라서, 우리나라도 사건유형에 따른 감사능력이 운영체제 수준에서 이루어지도록 하며 감사기록은 보안담당자에게 효과적으로 제공되도록 하는 기술적 장치가 마련되어야 할 것이다.

5. 정보시스템의 보안대책

정보시스템은 각종 위협에 대한 보안대책이 수립되어야 하며 보안대책은 물리적, 관리적 및 기술적 측면으로 분류될 수 있다.

가. 물리적 보안대책

물리적 보안대책은 자연재해와 불순세력에 의한 피해를 최소화하기 위해 경비원을 배치하거나 경보장치를 부착하는 등의 시설물 보호차원이다.

지역적 특성으로 야기되는 위협을 최소화하기 위해 장소선택과 건물설계시 예상되는 위협에 대비하여야 하며 비상계획을 수립하여야 하며, 각종 위협에 대해 시설물이 노출되었을 때 예상되는 손실의 정도를 예측하여 위협별 보안대책 순위를 산출하고 손실을 객관적으로 평가한다.

나. 관리적 보안대책

관리적 보안대책은 내부/외부 인원에 의한 오용을 방지하기 이해 정보시스템의 법제도적 운용절차를 규정하고 인원관리 및 교육을 포함한다.

① 정보시스템 보안을 위한 적절한 관리조직이 구축되어야 한다. 조직의 구성은 현재의 보안관련 기술, 개발수준, 법규 등의 환경변수와 조직규모, 경영전략, 위험정도 등 조직내부의 변수를 고려하여야 한다.

② 정보시스템 운용절차의 확인을 위해 보안담당자가 지정되어야 하며 보안 담당자는 표 4와 같이 내부통제의 목표설정, 확인, 수정 및 보완작업을 수행한다.

③ 보안정책의 지속적 추진을 위한 보안조사전략이 구축되어야 한다[Buur 84].

표 4. 보안담당자의 임무[Wood 87]

- 취약성 평가 및 통제방법 권고
- 비상계획 참여
- 보안규정의 준수성검사 및 교육
- 사용자 패스워드 관리
- 보안정책의 개발
- 사용자책임 결정 및 유지
- 시스템 침해의 조사
- 보안환경관리 및 제품평가

④ 횡령(Embezzlement), 사기(Fraud) 및 강탈(Extortion) 등의 범죄에 대한 조사계획이 수립되어야 한다. 이를 위해 감사인, 보안담당자, 시스템분석가, 하드웨어전문가 및 법률고문 등의 팀구성이 필요하다[Nasu 85].

⑤ 정보시스템의 위협분석과 예방조치의 강구를 위해 제조업자의 신뢰성, 제품의 시험 등 공인된 평가기준이 제정되어야 한다. 보안정책의 구현을 위한 메카니즘은 다음과 같은 취약성을 내포할 수 있다[GISA 89].

- ▷ 보안정책의 완전한 실행이 안된다. 이는 보안정책과 하위수준(low level) 명세의 mapping으로 평가된다.
- ▷ 잘 구현되었더라도 보안정책을 침해하는 취약성을 안고 있다. 이는 취약성의 식별과 평가를 위한 지침이 요구된다.
- ▷ 취약성이 발견되지 않더라도 부정확하게 구현된다. 이는 구현과정에서 검사되어야 한다.

⑥ 정보시스템의 가용성(availability)이 아무리 좋아도 내부통제와 보안기능의 약화에 따른 충격을 방지하지 못한다. 이러한 충격은 주로 임무편중 및 전문가 부재에 기인하며 이를 식별하기 위해서는 변경관리에 대한 명확한 절차가 구축되어야 한다.

다. 기술적 보안대책

기술적 보안대책은 컴퓨터 기술을 통해 정보 시스템을 보호하는 정책으로서 시스템 환경에 따라 다음과 같은 기본적 보안기능을 갖추어야 한다.

① 주체(subject)와 객체(object)는 유일하게 식별되어야 하며, 보안정책은 필요한 식별(identifica-

tion)과 인증(authentication)을 위해 주체와 객체를 정의하며 식별만 필요한 경우와 인증까지 포함하는 경우를 구분하여야 한다. 또한, 식별과 인증이 수행되는 환경과 수행이 실패될 때의 대응조치가 고려되어야 한다.

② 식별된 주체는 정해진 권한(rights)을 가지며 이러한 권한은 보안정책에 의해 관리되어야 한다. 일반적으로 주체가 정해진 속성을 갖고 있어야만 실행하도록 하는 방법을 취하며 보안정책은 관리주체, 관리대상, 권한종류, 운영규칙, 우선조건 등을 정한다.

③ 감사기능은 권한실행의 실패/성공에 관한 정보를 기록하여야 하며 보안정책은 기록될 사건유형, 정보내용, 기록장소, 기록의 접근주체·방법·시기, 기록의 평가기준 등을 정한다. 또한, 감사기능의 정확성과 완전성이 평가되어야 한다.

④ 오류(error)는 시스템 영향을 줄이기 위해 가능한 쉽게 식별되어야 한다. 보안정책은 회복될 오류의 종류, 회복방법 및 손실내용 등을 정한다.

⑤ 위험분석과 보안관리를 자동화하는 도구의 개발이다. 자동화 도구로는 영국 CCTA(Central Computer and Telecommunications Agency)의 CRAMM(CCTA'S Risk Analysis and Management Methodology)등이 있다.

4. 결 론

본 연구에서는 우리나라에서 표방하는 개방형 시스템과 정부와 공공기관 등의 보안 측면을 고려하고 선진국에서 개발된 감사증적 메카니즘의 주요 기능을 분석하여 우리 실정에 필요한 보안대책을 제시하였다.

앞서 언급한 바와 같이 정보시스템에 아무리 훌륭한 보안체계가 구축되어 있어도 완벽할 수는 없다. 따라서, 기존 응용프로그램 수준의 logging 개념을 탈피하고 보안사건에 대한 추적능력을 확보하기 위해 감사증적 메카니즘의 설계범위에는 다음 사항이 포함되어야 한다.

첫째, 접근시도의 실패를 포함한 모든 보안사건은 kernel 수준에서 기록하고 보호하여야 한다. 보안사건을 탐지/기록하기 위해서는 참조모니터 개념을 사용하며 호출된 프로그램/명령어가 인가된 것인지를 식별하여야 한다.

둘째, 보안담당자는 시스템 환경에 따라 감사기능을 작동/중단하며 감사중인 사건을 변경시키거나 감사증적화일을 교체할 수 있어야 한다.

셋째, 공인된 프로그램은 kernel 수준의 감사기능을 우회하도록 하여 불필요한 감사 레코드의 생성을 방지하고 kernel 수준의 감사기능을 지연/재개할 수 있는 융통성을 갖추어야 한다.

넷째, 사건추적에 필요한 감사레코드를 쉽게 조회/검사할 수 있어야 한다.

본 연구에서 접근한 정보시스템 보안개념과 감사증적 메카니즘은 정보시스템 운영조직의 최고관리자, 보안책임자, 시스템설계 및 운영자에게 참조될 수 있을 것이다.

참 고 문 헌

[Berg 84] B. Berg and H. Leenaars, "Advanced Topics of a Computer Center Audit", Computers & Security, Vol.3, 1984, pp.171-185.

[Buur 84] F. Buurmeijer, "IBM's Data Security Strategy : Some Implementation Aspects", Computers & Security, Vol.3, No.4, 1984.

[CAI 88] Computer Associates International Inc., *CA-ACF2 The Access Control Facility For the MVS Environment*, Computer Associates International Inc., 1988.

[Cumm 87] P.T. Cummings, D.A. Fullam, M.J. Goldstain, M.J. Gosselin, M.J. Picciotto, J.P.L. Woodward and J. Wynn, "Compartemnted Mode Workstation : Results through Prototyping", 1987, IEEE Symposium on Security and Privacy, Oakland California April 1987, pp.2-12.

[DRG 91] Datapro Research Group, *Information Technology Security Evaluation Criteria (ITSEC)*, McGraw-Hill, 1991.1.

[GISA 89] German Information Security Agency, *Criteria for the Evaluation of Trustworthiness*

of Information Technology System, GISA, 1989.

[Glig 86] V.A. Gligor and E.L. Burch, "On the Design and The implementation of Secure XENIX Workstation", Proc. of IEEE Symposium on security and Privacy, Oakland California April 1986, pp.102-117.

[Moll 84] Carol G. Molloy, "Improving CICS Controls with GUARDIAN", AUERBACH, Auerbach Publishers Inc., 1984.

[Morr 90] P.W. Morriss, "The Auditor's, Role in Creating Successful System", COMPSEC '90, 1990.

[Nasu 85] Frank. W. Nasuti, "Devloping a Computer Crime Investigation Plan", AUERBACH, Auerbach Publishers Ins., 1985.

[Paan 90] R. Paans and I.S. Herschberg, "Auditing The Change Management Process", COMSEC'90, Conference, London, 1990.

[Perr 84] William E. Perry, "Reviewing the Selection of Data Security Software", AUERBACH, Auerbach Publishers Ins., 1984.

[Picc 87] J. Picciotto, "The Design of an Effective Auditing subsystem", 1987, IEEE Symposium on Security and Privacy, Okaland California April 1987, pp.13-22.

[TDO 92] *Trusted DG/UX Overview*, Data General Corporation, 1992. 2.

[감사 90] 한국정보시스템감사인협회, 정보시스템 감사론, 법영사, 1990.

[남길 91] 남길현, 선진국 데이타보호 기술동향 분석, 연구보고서, 한국전자통신연구소, 1991.11.

□ 著者紹介

남 길 현(正會員)

陸軍士官學校 卒
서울工大 土木科 卒
美海軍 大學院(電算學 碩士)
위스콘신(메디슨) 州立大(電算學 碩士)
루이지아나州立大(電算學 博士)
陸軍士官學校 教授部 專任講師, 現在 國防大學院 電子計算學科 副教授
관심분야 : 컴퓨터보안, 암호학, 데이타베이스, 알고리즘 분석

金 永 喆

'88년 한국방송통신대학 전자계산학과 졸업(이학사)
'92년 국방대학원 전자계산학과 졸업(이학석사)
'79년~현재 : 국제과학문화연구소
관심분야 : 정보시스템 보안 감사, 분산운영체계