□사례발표□

포항종합제철(주)의 정보보안시스템 적용사례

이 상 대† 이 일 수†† 김 성 수†††

◈ 목 차 ◈

1. 서 론

포항종합제철(주)(이하 POSCO라 약칭함)는 1994년도에 포항공대 정보통신연구소와 "포항제철 전산망보안 종합대책"이라는 과제를 시작하면서 정보보안에 신경을 쓰기 시작했다. 그 당시는 대학에서조차 인터넷을 잘 모르는 시기였으므로 몇몇 타기업의 입장에서 보면 필요없는 투자라고 생각되어질 수 있었으나, 1995년도 6월에 대기업의 CO 도메인에서는 거의 최초로 기업의 내부 LAN이 인터넷과 연결되면서 그 투자효과가 나타났다. 본 연구과제는 다음과 같은 일정계획을 가지고 오는 1997년 10월을 최종목표로 추진되고 있으며, 현재는 방화벽시스템과 디지털 서명이 개발완료되어 사용되고있는 단계이다.

① 1994년도 : POSCO 전산망 위험분석
② 1995년도 : 방화벽시스템, 디지털 서명시스템 개발
③ 1996년도 : 방화벽시스템, 디지털 서명시스템 현장적용
암호화 알고리즘, 암호화 통신을 위한 통합보안시스템 설계
④ 1997년도 : 암호화 알고리즘 및 통합보안시스템 구현 및 현장적용

또한 본 연구과제는 기업에서 필요한 모든 보안요소를 포함하고 있으며 최종적으로 연구과제가 완료되면 전자상거래에 사용될 수 있는 보안 모듈을 소유할 수 있게 된다.

한편 POSCO의 전산망 위험분석과 방화벽시스템 개발기간동안 별도로 POSCO 전산시스템에 대한 통합보안정책을 수립하였는데, 이는 국내에서 사례를 찾아보기 어려우며 그 중요성이 점점 더해가므로 본 고에서 언급하고자 한다.

2. POSCO의 정보보안사상

POSCO는 인터넷을 기업정보공유의 인프라로 생각하고 이것을 이용하여 안전하고 경제적으로 전세계에 있는 사무소, 출장자 및 수요가들에게 정보를 제공한다는 목표를 가지고 인터넷을 기업

† 정 회 원 : 포스데이타(주) SM본부 차장
†† 정 회 원 . 포스데이타(주) SM본부 과장
††† 종신회원 : 포스데이타(주) 기술대학원 교수

경영의 도구로 활용하고 있다. 이러한 사상이 1996년 8월에 방화벽시스템 "STEELMASK"를 설치하면서 일부 이루어져 현재는 방화벽시스템 뒤에 "Secured Zone"을 두어 외국의 지사에 정보를 제공하고 있다. 이는 정당한 권한을 가지고 있는 사용자만이 들어와 정보를 접근할 수 있도록 One-Time Password가 적용되고 있다. POSCO의 특성상 Server별로 보안을 담당하기에는 한계가 있고 또 투자측면에서 처음부터 투자하기에는 무리가 있다고 판단되어 기업의 보안정책을 가장 확실하고 경제적으로 구축할 수 있는 시스템인 방화벽시스템을 구축한 것이다. 그리고 그것이 외산이어서는 안된다는 생각에 자체의 기술력으로 개발됐다. 그 결과 Windows95에서 우려하고 현재 Netscape에서 우려되고있는 트랩도어의 우려사항을 잠식시킬 수 있었다.

이러한 면을 고려할 때 POSCO의 인터넷 활용방향을 살펴보면 다음과 같다.

① 인터넷을 기업정보공유의 인프라로 이용
② 인터넷을 이용시 확실한 정보보안시스템 적용 및 정책을 설정
③ 인터넷 이용기술인 인트라넷(Intranet)과 익스트라넷(Extranet)은 별도의 스템으로 보지 않고 동시적용

이와 함께 정보보안의 추진방향을 보면 다음과 같다.

① 정보보안시스템은 모두 국산화한다.
② 기업에서 사용하는 모든 정보보안기술을 보유한다.
③ 향후 사용될 EDI, 철강 CALS에서 필요한 정보보안기술을 보유한다.
④ 국가 기반기술인 정보보안기술의 선구자적 역할을 한다.

이러한 사상을 가지고 시작한 정보보안 기술개발은 지금 4년째 접어들면서 확실한 자체 기술력을 가질 수 있었고 현재 보안시장의 추세인 "맞춤보안"에 누구보다도 앞서 있다고 자체 평가한다.

3. POSCO의 정보보안 발전방향

POSCO의 정보보안 발전방향은 인터넷의 사용측면과 맞물려 다음과 같이 3단계로 구분될 수 있으며, 현재 2단계에 와있다. 이것은 이용자 측면에서 생각한 적용단계로서, 추가로 필요한 기술들은 오는 1997년 10월에 완성되어 현장에 적용하게 될 것이다.

① 1 단계(단순 이용단계)

1 단계는 보통의 정보공유단계로서 인터넷을 이용하여 기업의 홍보 및 채용 그리고 수요가에게 간단한 정보를 제공하는 단계이다. 여기에서의 보안은 단순하게 Router의 Packet Filtering을 가지고 정보보안을 하며 정보보안정책의 순환단계를 가지지 못하는 단계이다. 각 사무소와의 정보공유는 전용선과 Frame Relay 기술을 사용하여 이루어지고 원격지와 정보공유시 상대적으로 많은 비용이 필요한 단계이다.

② 2 단계(정보공유의 과도기적 단계)

2 단계는 보통의 이용단계에서 약간 발전해 인터넷을 기업정보공유의 도구로 사용하기 시작하는 단계로서 기업의 보안은 방화벽시스템을 이용한 네트워크 보안에 역점을 두고 그 뒷단에 인가된 사용자만이 사용할 수 있는 "Secured Zone"을 두어 원격지간에 정보를 공유하는 단계이다. 여기서는 정보의 암호화 통신을 이용해 중요한 정보를 송수신할수는 없지만, 기업의 경제적인 정보공유 인프라 기술의 적용이라는 큰 의미를 가지는 단계이다. 즉 점점 전용선을 인터넷과 같은 공중망으로 변경하는 단계이다. 현재 우리나라의 법률상 공중망을 이용한 암호화 통신은 허용되고있지 않아 그것을 기업이 사용하기에도 약간 어려운 단계이다.

③ 3 단계(암호화 통신을 이용한 가상사설망의 확립단계)

3 단계에서는 실제적인 통합보안기술을 가지고 업무에 적용하는 단계로서 기업의 EDI/CALS, EC에 필요한 모든 보안시스템이 현장에 적용되는 시기이다. 이제까지의 모든 전용선은 인터넷과 같은 공중망으로 전환되고 기업의 정보보호도 인증 프로토콜, 암호화 통신과 방화벽시스템을 연계한 안전한 보안시스템이 적용된다. 기존의 정보공유를 위해 필요한 경비의 약 1/3로 구축할 수 있으며, 이것은 다시 기업의 경영활동에 큰 영향을줄 수 있다. 그 이유는 전세계 어느 곳에서도 시공간을 초월하여 안전하게 기업의 비밀자료를 송수신할 수 있고, 여기서 사용되어지는 모든 보안시스템이 자체적으로 개발된 것이며, 보안선진국이 가지고 있는 보안제품의 수출 규제에 대해 매우 근본적인 대응책이 될 수 있을 것이다.

4. 정보보안정책

POSCO의 정보보안정책은 기업의 정보보호에 필요한 기술개발과 병행되어 작성된 것으로서 기업에서 필요한 모든 정보보호기술 및 내용을 포함한다. 이는 지난 1994년 말에 작업을 시작으로 약 1년여에 걸쳐 작업이 이루어졌으며 지난 1996년 6월에 초안이 완성되었다.

우선 (그림 1)과 같이 POSCO의 전산망 보안정책의 목차를 살펴보면 다음과 같다.

이 목차에는 우선 보안정책의 목표가 먼저 설정되어 있고, 다음으로 기업에서 필요한 정보보호 서비스가 규정되어 있다. 이것은 각 기업마다 보안의 필요범위에 따라 달라질 수 있으며 필요시 추가 삭제될 수 있다.

다음으로 전산망 보안정책의 대원칙이 규정되어 있어, 모든 정책은 여기에 따라 규정된다. 다음으로는 실제 보안정책이 구현되는 보안정책 적용범위가 결정되어져야 한다. 물리적인 면과 기능적인 면이 별도로 규정되어져 있고 보안사고의 유형에 따른 대책 또한 강구되어져야 함은 물론이다. 이 보안대상을 결정하는 것과 같이 그 대상에 대한 보안등급을 결정하기 위하여 자원 및 정보에 대해서 보안등급 결정기준이 설정되어 있다. 이는 정보보안의 구현 및 위반시 법적근거를 제공하는 부분으로 기업의 내부 사용자에 의한 보안사고가 전체 보안사고의 70%를 차지하고 있다는 보고를 고려한다면 보안정책의 핵심이 되는 부분이다. 다음으로 실제 정보보안 정책이 구현되고 운영되어지는 기준이 결정되어 있다. 여기에는 관리적인 보안대책과 기술적인 보안대책으로 구분되어져 있으며 POSCO의 경우 기술적인 보안대책에서 Network 보안, Server 보안, Database 보안, Host 보안, Client 보안, Application 보안, Internet 보안, 사용자계정 관리방안 등으로 규정되어 있다. 여기서 Host 보안과 Server 보안의 차이는 POSCO의 내부특성상 Workstation급은 Server라고 부르고, Mainframe은 Host라고 부른다. 또한 Application 보안은 POSCO 내부시스템으로 개발되어지는 시스템들에 대한 보안을 의미한다. 여기에는 보안정책을 구현하는 실행단계까지를 포함하고 있다.

또한 POSCO의 특성상 모든 POSCO의 계열사가 동일 네트워크에 물려있다는 점이 보안상의 큰 헛점일 수 있다는 생각에 대외보안정책이라는 큰 항목으로 이것에 대한 보안정책을 규정하고 있다. 이는 현재 각 계열사들을 같이 운영하고 있는 국내 대기업들에서도 모두 같은 고민을 가지고 있을 것이다. 이 부분의 보안정책 의사결정은 관계되는 당사자간에 서로 협의에 의해 이루어지거나 그룹의 책임감있는 단일 조직에 의해 의사결정되어지고 그 결정에 따라 실현될 수 있다. 다음으로 정보보안을 담당하는 조직의 책임과 역할

POSCO 전산망 보안정책

목 차

포스데이타

(그림 1) POSCO의 전산망 보안정책

에 대해 규정되어 있고 보안사고의 처리 및 일반 직원의 보안의무에 대해 기술되어져 있다. 이것은 쉽게 간과되어질 수 있는 항목으로 구분되기 쉬우나 실제로는 가장 실천하기 어렵고 가장 많은 보안적 위험이 존재하는 부분이다. 그 이유는 아무리 좋은 정책을 가지고 있을지라도 역시 그 지

침을 실천하는 주체는 기업의 각 개인이라는 점에서 충분히 고려되어지고 교육되어져야 한다.

5. 정보보안시스템 구축

인터넷과 연계되어 해커가 극성을 부리고 있는 시점에 외부의 인가되지 않은 사용자들로 부터 내부시스템을 보호하는 방화벽시스템이 기업의 통합보안시스템의 최종목표로 지난 1996년 8월에 구축되어져 현재까지 운영되고 있다. 이 방화벽의 구축으로 POSCO는 인터넷을 통한 비인가자로 부터 내부 전산자원에 대한 보호 뿐만 아니라 사외의 인가된 사용자(해외사무소 주재원등)에게 POSCO의 사내 정보를 안전하고 신속하게 전달할 수 있게 되었다.

5.1 시스템 구성 및 기능개요

POSCO 구축된 방화벽시스템은 (그림 2)와 같이 방화벽시스템내에 5개의 단위기능으로 나눠지고, 그것은 실제 적용되는 사업장이나 조직의 인터넷을 포함한 전산망 보안정책위에 위치하여 실제 구현을 담당한다.

또한 POSCO에 적용된 방화벽시스템의 구조는 (그림 3)과 같다.

각각의 기능해설은 다음과 같다.

가) Protocol proxy부

사외로부터 인가된 사용자가 사용하는 Protocol에 대하여 사용권한을 부여하기전에 해당 사용자가 인가된 사용자인지를 사용자 인증부와 연결되어 확인하고 인가된 사용자의 경우 실제 내부시스템으로 연결 시켜주는 기능.

나) 사용자 인증부

Protocol proxy부로부터의 사용자 인증요구에 대하여 사용자의 인가여부를 결정하는 기능.

사용자의 접속단말과 One-Time Password를 이용하여 인증을 행한다.

다) Log, 감시 기능부

사외로부터의 접속시도에 대하여 일별, 주별, 월별로 접근실적을 로깅관리하는 기능.

라) Alarm 기능부

비인가자의 접속시도에 대해 보안관리자에게 실시간으로 알리는 기능

마) 사용자 접속부

방화벽시스템의 운영관리자가 인터넷을 포함한 정보보안정책을 구현하기 쉽게 할 수 있도록 도와주는 기능.

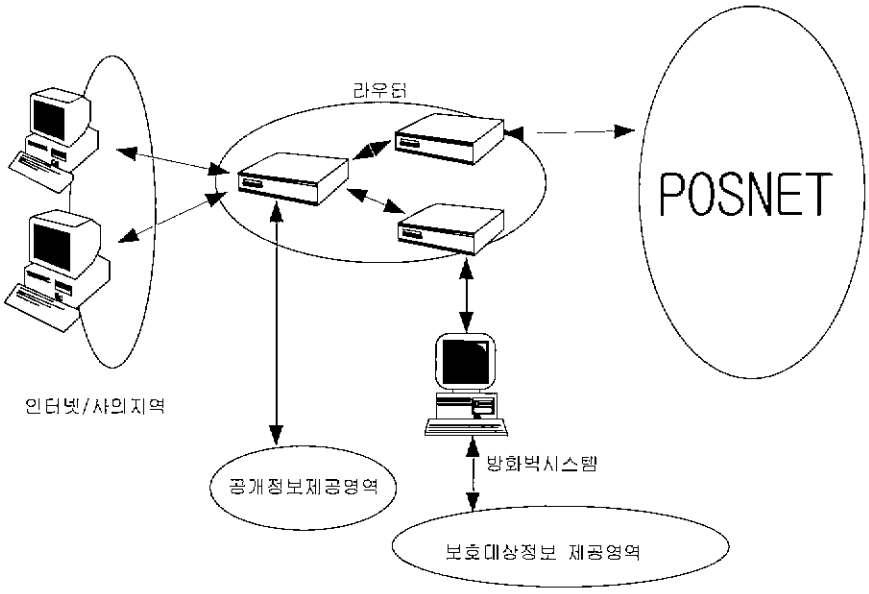
(그림 2) POSCO의 방화벽시스템 기능구성도

5.2 시스템기능 특징

POSCO에 구축되어 운영중인 방화벽시스템의 특징은 다음과 같은 사항들이 있는데, 이는 Screened subnet 형태의 방화벽시스템이며 방화벽시스템 뒷단에 "Secured Zone"을 두어 인가된 사용자들에게 정보를 제공하고 있다.

5.2.1 일반적인 특징

- Application level gateway
- Dual homed
- Screened subnet을 포함한 모든 형태의 방화벽 수용.



(그림 3) POSCO의 방화벽시스템 구조

- Protocol proxy service
- Host & User 인증
- Logging
- 관리용 GUI 환경

5.2.2 STEELMASK 방화벽시스템의 특징

- 강력한 사용자 인증기능 수용(One-Time Password 채용).
- 외부로부터의 Command 별 제어
- http 인증.
- 순수 국내 기술진에 의한 제품.
- Groupware, Intranet, Extranet 적용예정
- 국내 실정에 맞는 전산망 보안정책 구현

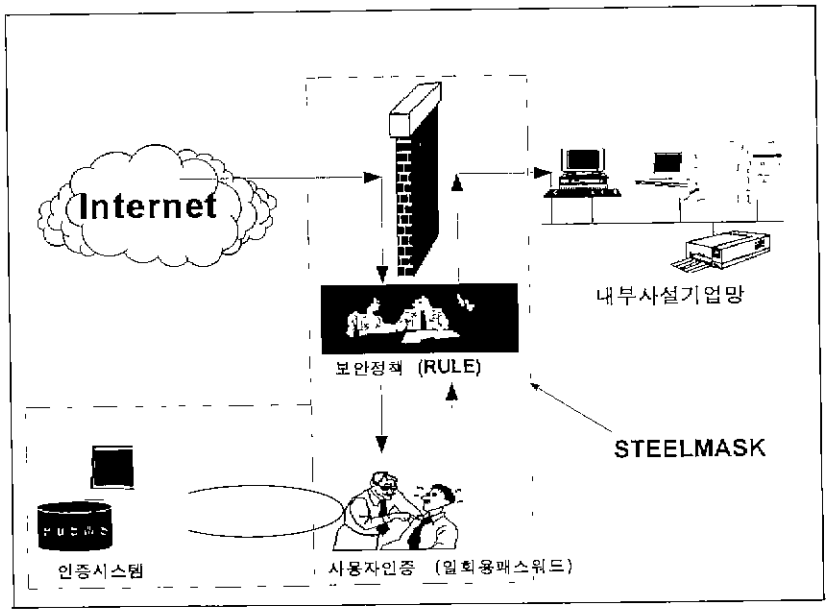
5.3 최종목표

POSCO의 전산망보안에 대한 최종목표는 위에서 언급된 것과 같이 기업에서 필요한 모든 정보보안기술을 집약한 통합정보보안시스템을 구축하는 것이다. 여기에는 현재 개발이 완료된 방화벽시스템, 디지털 서명기술을 비롯하여 암호화 알고리즘, 암호화 통신기법, 인증기법 등을 망라한 시스템이 될 것이다.

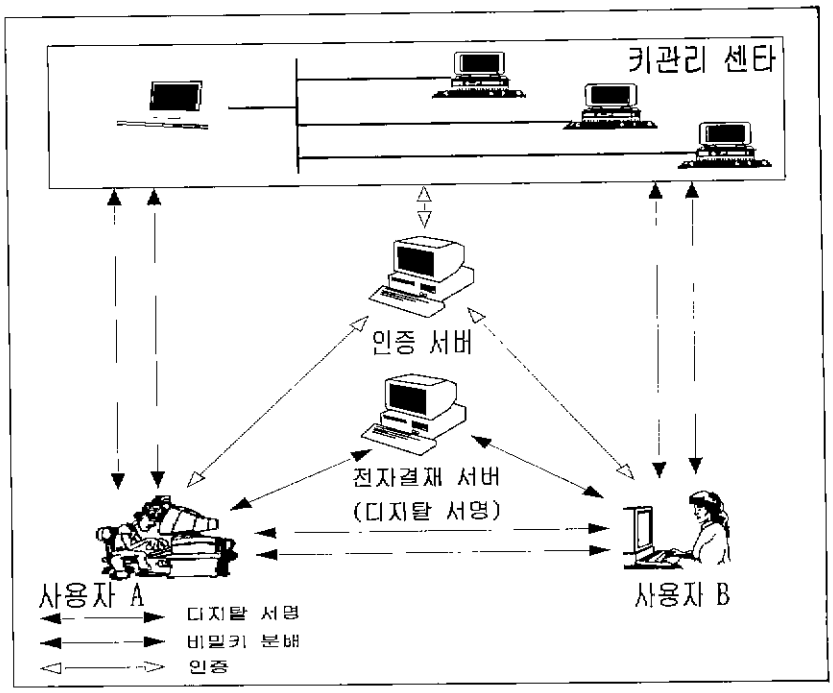
POSCO의 전산망보안을 담당하고 있는 방화벽시스템의 기능구성도는 (그림 4)와 같으며, 인증기법과 암호화 통신을 비롯한 제반기능의 작업도는 (그림 5)와 같다. 그리고 최종적으로는 이러한 모든 정보보안기술들이 통합되어 업무가 이루어질 것이고, 이는 국내 정보보호기술을 한발 앞당기는 것이라 하겠다.

6. 결 론

현재 정보보안에 대한 모든 기술들은 보안선진국들이 기술이전을 꺼려하고 있으며, 그들이 제공하는 모든 시스템에 자국에서 사용하는 보안 모듈과 수출되는 제품의 보안 모듈이 상이하다는 것도 모두가 알고 있는 주지의 사실이다. 여기에 우리의 정보를 안전하게 보호하고 송수신하기 위



(그림 4) POSCO 방화벽시스템 기능구성도



(그림 5) POSCO 통합정보보안시스템

한 근본적인 대응책은 정보보호에 대한 우리의 기술을 보유하는 것이다.

POSCO, 포스데이타 그리고 포항공대는 이러한 상황에서 우리의 기술을 확보하기 위해서 연구개발하고 있고, 앞으로 통합정보보안시스템이 완성되면 정보보안에 대한 우리의 기술을 확실하게 확보할 수 있을 것이다.

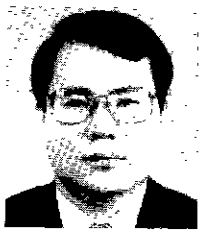
참고문헌

[1] Siyan,K. & Hare,C., Internet Firewalls and Network Security, New Riders Publishing, chapter 3, 1995.

[2] Stallings,W. "Network and Internetwork Security", IEEE Press, pp. 157~197, 1995.

[3] 이필중, POSCO 전산망 Security 종합대책(1), 포항공과대학교 정보통신연구소, pp.26~45, 1994.

[4] 이필중, POSCO 전산망 Security 종합대책(2), 포항공과대학교 정보통신연구소, pp.32~43, 1995.

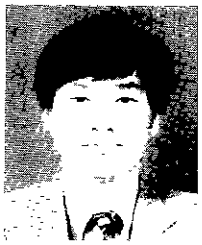


이 상 대

1983년 충남대학교 전산학과 졸업 (이학사)
1985년-1995년 포항제철 전산시스템부
1996년-현재 포스데이타(주) SM본부 차장
관심분야 : 전산망보안, 데이타통신

이 일 수

1987년 인하대학교 금속공학과 졸업 (공학사)
1987년-1996년 포항제철 전산시스템부
1993년-1995년 포항공대 정보통신대학원 컴퓨터통신전공 졸업 (공학석사)
1996년-현재 포스데이타(주) SM본부 과장
관심분야 : 전산망보안, 이동통신보안, 데이타통신



김 성 수

1982년 인하대학교 전자계산학과 졸업 (이학사)
1984년 숭실대학교 대학원 경영학과 MIS 전공 졸업 (경영학석사)
1991년 중앙대학교 대학원 경영학과 MIS 전공 졸업 (경영학박사)
1989년-1993년 경희대학교, 중앙대학교, 숭실대학교 강사
1993년-1994년 포스데이타(주) 컨설팅사업부 책임컨설턴트
1995년-현재 포스데이타(주) 기술대학원 교수
관심분야 : MIS, 소프트웨어공학, 전산감리 및 보안