2001년 한국정보처리학회 추계 학술발표논문집 제8권 제2호

전자정부 구현을 위한 정보공유 분석센터 구축에 관한 연구

장홍종*, 박인재*, 이정현**
*행정자치부 정부전산정보관리소
**인하대학교 전자계산공학과
e-mail : realking@gcc.go.kr

A Study on Implementation of Information Sharing and Analysis Center for E-Government

Hong-Jong Chang*, In-Jae Park**, Jung-Hyun Lee**
*Dept of Government Computer Center, MOGAHA
**Dept of Computer Science & Engineering, Inha University

요약

사이버테러는 전세계적으로 시공간을 초월하여 동시다발적 공격이 가능하고 발생시각, 발원지, 침입자 추적 등이 어려우며, 한 곳의 피해가 다른 곳으로 대규모 확산이 우려되고 효율적인 차단 및 복구에도 어려움이 가중되고 있다 이에 본 논문에서는 행정정보인프라의 불법침입에 대한 즉각적인 대응체계와 사이버테러의 사전 예방을 위한 정부고속망의 연결기관에 대한 보안정보제공 및 침해사고 공동대응 체제를 갖춘 정부차원의 정부정보공유분석센터의 효율적인 구축 방안을 제안한다.

1. 서론

오늘날 정보통신기반의 급속한 확산은 인터넷이란 새로운 가상환경을 통해 세계를 하나로 연결하였으며, 국방·통신·금융·전력 등 주요사회기반시설들이 정보시스템에 대한 의존도를 심화시키게 하였다.

이러한 환경의 변화로 탄생한 전자정부도 범정부적인 정보기술 공유기반을 통해 하나로 연결된 정부의 각종 정보와 행정서비스를 정부와 국민이 공유할 수 있도록 90년대 중반부터 지속적인 투자와 노력을 기울여 왔다.

그러나 사이버테러의 지능화, 첨단화되고 대규모 합동공격의 양상으로 발전되고 있어 21세기 국가 경쟁력의 핵심이라 할 수 있는 전자정부의 구현, 전자상거래 등 인터넷 비즈니스의 활성화를 저해하는 가장 큰 걸림돌이 되고 있어 이에 대한 대응이 시급한 실정이다.

이러한 사이버테러는 전세계적으로 시공간을 초월하여 동시다발적 공격이 가능하고 발생시각, 발원지, 침입자 추적 등이 어려우며, 한 곳의 피해가 다른 곳으로 대규모 확산이 우려되고 효율적인 차단 및 복구에도 어려움이 가중되고 있다.

이에 본 논문에서는 행정인프라에 대한 사이버테러를 사전에 차단 및 예방할 수 있는 정부차원의 정보공유 분석센터의 효율적 구축 방안을 제안한다.

2. 국내·외 추진 동향

사이버테러에 대한 문제의식으로 인해 미국 등 선진국에서는 주요정보통신기반에 대한 보호대책을 마련해가고 있으며, 특히 미국은 1996년 국가정보기반보호법을 제정하고 주요정보통신기반에 대한 국가차원의 보호대책(국가정보시스템보호대책 ; 2000 National Plan)을 수립하여 추진 중에 있다[1].

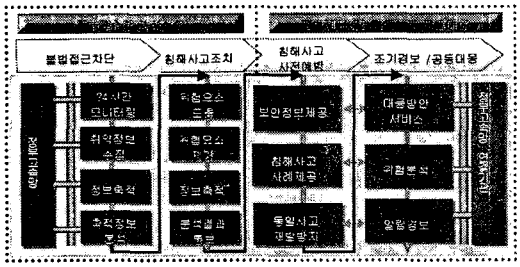
우리정부도 국가차원의 정보보호기반강화를 위해 정보통신부 등을 중심으로 2001년 1월 정보통신기반보호법을 제정·공포하였으며, 동 법에 의거하여 각 정보기반의 취약성분석·평가 등을 대통령령이 정하는 기준에 준 하는 자체 전담기관(정보공유·분석센

터)을 구성·운영하도록 하였다.

이 전담기관의 장은 그 분석 결과를 관할 중앙행정기관의 장에게 제출하고, 당해 행정기관의 장은 제출 받은 보호대책을 종합·조정하여 기반시설보호계획을 수립하고 정보통신기반보호위원회의 심의를 거쳐 추진하도록 하였다[2].

3. GISAC의 기반 기술

정부정보공유분석센터는 행정정보인프라의 불법침입에 대한 즉각적인 대응체계와 사이버테러의 사전 예방을 위한 정부인트라넷의 연결기관에 대한 보안정보제공 및 침해사고 공동대응 체제 구축을 기반으로 하며 [그림 1]과 같은 구성을 갖는다.



[그림 1] GISAC의 구성도

이러한 사이버테러대응기술을 정리하면 <표 1>과 같으며, 국가 주요정보기반의 안전을 위해 필수적인 전략분야로서 지식정보화 실현에 있어 핵심적인 인프라로 자리잡을 것이다.

<표 1> 사이버테러 대응기술

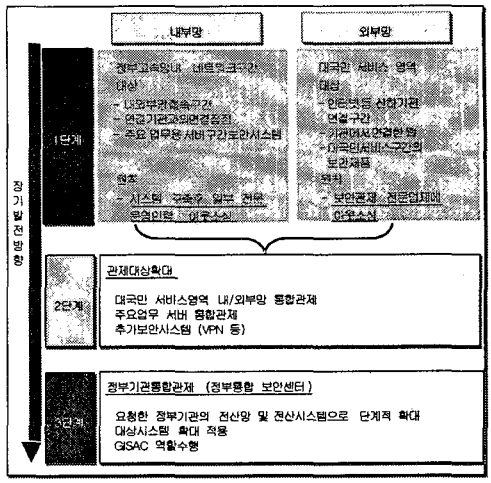
대응기술	주요내용
취약성분석	주요기반의 보안성취약성, 공격에 대한 피해 파급효과, 기존 보안대책의 적절성 등을 분석·진단
침입탐지·대응·복구	사이버테러 발생시 실시간 침입탐지 및 정보를 통지하고, 탐지된 침입에 대한 대응복구
네트웍공격 방어및예방	대규모 네트웍에 대한 효율적 보안관리를 위한 보안정책 서버, 보안게이트웨이 등을 통한 공격의 조기차단 및 방어
안전·신뢰성 강화	Secure OS/DBMS, 네트웍 프로토콜 취약성탐지·제거 등 정보통신기반의 취약성 제거를 통한 보안성 강화

가. 통합관제시스템

정부고속망의 통합관제시스템은 고속망의 주요 업무서버 및 네트워크 구간을 24시간 모니터링하며, 침해사고 및 이상징후 발생 시 즉각적인 대응을 할 수 있는 체제를 필요로 한다.

(1) 보안관제 대상

정부고속망 보안관제의 대상은 [그림 2]와 같이 단계별로 추진한다.



[그림 3] 보안관제의 대상

고속망 네트워크 구간에 대한 보안관제의 대상은 다음과 같다[3].

- 외부망과의 연결접점의 보안 시스템(침입차단시스템, 침입탐지시스템)
- 주요 업무서버 구간의 보안시스템(침입차단시스템, 침입탐지시스템)
- 청사내 기관과의 연결구간, 단독청사와의 연결구간, 지자체 망 연결구간의 보안시스템 (침입차단시스템, 침입탐지시스템)
- 향후 도입될 VPN 등의 보안시스템

(2) 보안관제 대상 구성방안

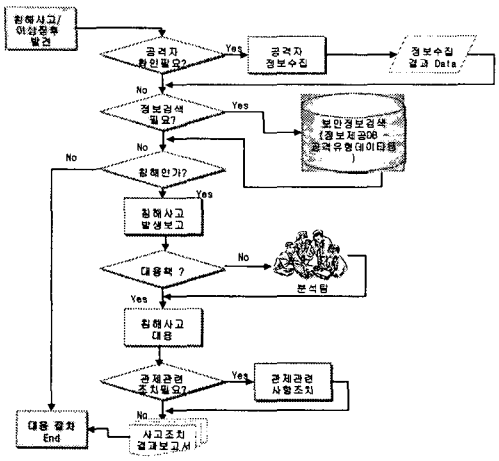
현황분석자료를 토대로 정부고속망 연결기관을 보안수준, 인프라성숙도, 시급성의 관점에서 A, B, C, D그룹으로 나누어서 이행 우선순위를 적용한다.

(3) 주요 기능

기본기능으로써는 중요 시스템 및 네트워크 구간에 대한 24시간 모니터링(보완관제)과 보안로그의 중앙집중관리, 정부고속망 침해사고에 대한 즉각적 대응의 기능이며 추가적인 기능으로써는 주기적인 시스템, 네트워크 취약성 진단 및 방역과 보안시스템 중앙집중통제 및 관리 기능이 있다.

(4) 기능별 프로세스

정부고속망 불법침입 발견 시 통합관제요원의 대

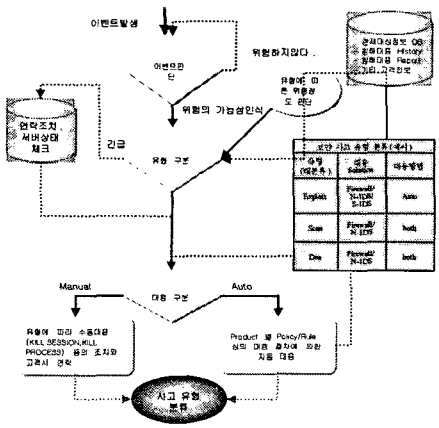


[그림 3] 침해사고 대응 프로세스

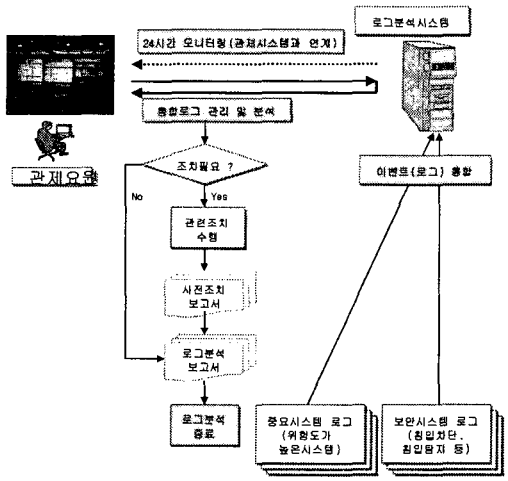
응 프로세스로서, 구축된 정보DB에 없는 새로운 기법의 침입인 경우 분석팀과 연계하여 대응하며, 분석팀의 경우는 정보보호 전문인원으로 구성된 팀으로, 국정원, 경찰청 등의 관련기관과 연계 방안을 고려해야 한다. 침해사고에 따른 대응프로세스는 [그림 3]과 같다.

이벤트 발생 시에는 관제대상 데이터베이스에서 그 유형에 따른 위험정도를 판단하여 보안사고 침해정도에 따른 대응절차를 밟게 되며 [그림 4]와 같은 관리프로세스를 갖는다.

중요 시스템, 네트워크에서 발생하는 로그는 취합/통합하여 [그림 5]와 같이 관리하며, 로그분석을 통해 침입흔적, 시스템/네트워크의 접근 유형 등을 분석하여 보안정책 및 시스템에 조치한다. 정부고속망의 경우 트래픽을 고려할 때 로그의 크기가 기하



[그림 4] 이벤트 관리 프로세스

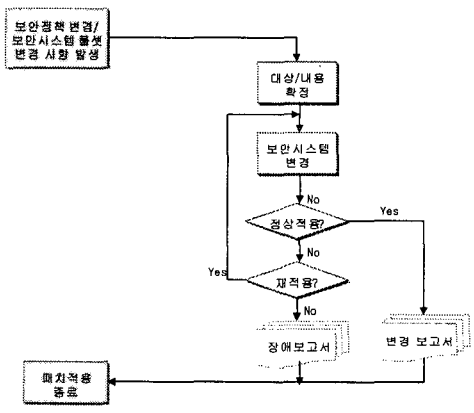


[그림 5] 이벤트로그 관리 프로세스

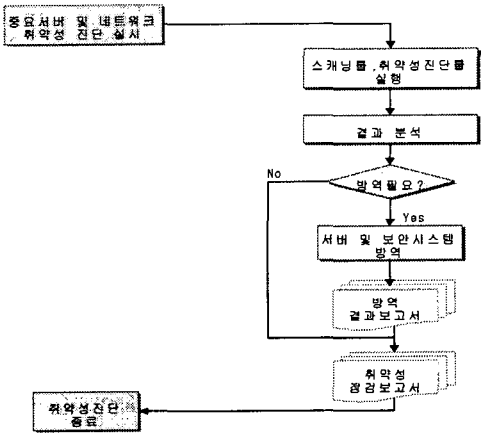
급수적으로 증가할 가능성이 높으므로, 통합관리 할 로그패턴을 선정하는 것을 고려해야만 한다. 보안정책이 바뀌거나, 보안시스템에 새로운 룰 변경사항 발생 시에는 전체 또는 일부의 보안시스템의 룰셋을 변경해야 한다. 관제요원에 의해서 일괄 변경하거나, 중요 보안시스템의 경우는 관리자의 승인을 득 한 후 조치하여야 한다. 이에 따른 보안시스템 관리프로세스는 [그림 6]과 같다.

최소 3개월 단위로 정부고속망 내의 시스템 및 네트워크 구간에 대한 침해흔적 조사를 포함한 취약성 진단이 필요하다. 이 진단결과에 따라 서버 및 네트워크를 방역을 해야 한다. 관제운영 및 분석팀의 아웃소싱 검토 시 관리요원의 역할에 추가할 수 있다. 취약성 진단 및 방역프로세스는 [그림 7]과 같다.

(5) 관제시스템 기본요건 및 고려사항



[그림 6] 보안시스템 관리 프로세스



[그림 7] 취약성 진단 및 방역 프로세스

관제시스템의 기본적인 요건은 다음과 같다.

- 정부고속망내에서 사용하는 침입차단, 침입탐지시스템을 비롯하여 중요서버에 대한 통합로그관리 및 실시간 모니터링이 가능해야 한다.
- 원격지 모니터링 시스템 및 침입탐지시스템으로부터 발생되는 각종 이벤트를 시스템 운영요원에게 알리거나, 실시간(AAP일, 핸드폰 등)으로 경보하여야 한다.
- 긴급한 사안인 경우 원격에서 각종 보안시스템을 조정할 수 있어야 한다.
- 침해사고시 공격자의 추적이 가능하도록 지원하여야 한다
- 각종 시스템에서 발생하는 로그를 통합해서 관리 및 분석이 가능하여야 한다.
- 로그파일을 분석하여 불법침입자 파악 및 기관별/사용자별 시스템 사용상황 등 다양한 분석 및 통계 기능을 제공하여야 한다.
- 보안정보 DB와 연계하여 추가되는 최신 해킹기법과 연계하여 분석이 가능하여야 한다.

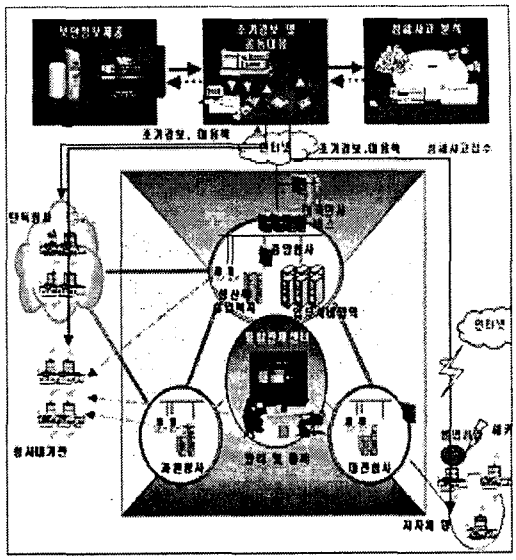
또한, 구축시 고려해야 될 사항은 <표 2>와 같다.

<표 2> 관제시스템 구축시 고려사항

부 문	고 려 사 항
정부고속망 보유 보안제품 통합	정부고속망 보유 보안시스템의 로그형태가 표준화되어 있지 않으므로, 로그의 표준화 검토
로그 필터링	정부고속망의 트래픽을 고려할 때, 일일 로그 사이즈가 기하급수적으로 저장될 가능성이 높음. 로그분석 및 침해사고 대응을 위한 이벤트 및 로그내용 선정필요
로그분석	과거 및 최신 공격정보와 연계한 자동화된 로그분석 기법이 요구됨
보안정보 제공서비스와 연계운영	보안정보제공 및 침해사고대응과 연계/운영하는 방안 검토 필요
분석팀과의 연계	침해사고 대응을 위한 CERT(침해사고대응팀) 보유기관과 연계할 수 있는 협조체계 구축 필요

(6) 구축시스템

본 논문에서 구축하고자 하는 시스템의 구성도는 [그림 8]과 같다.



[그림 8] 구축시스템의 구성도

4. 결론 및 향후 연구과제

행정정보통신기반의 안전한 운영은 전자정부의 전제조건이다. 이에 본 논문에서는 행정정보인프라의 불법침입에 대한 즉각적인 대응체계와 사이버테러의 사전 예방을 위한 정부인트라넷의 연결기관에 대한 보안정보제공 및 침해사고 공동대응 체제를 갖춘 정부차원의 정부정보공유분석센터의 효율적인 구축 방안을 제안한다. 향후 취약점 분석, 평가 및 보호 대책 수립을 할 수 있는 공유데이터베이스에 대한 공학적인 절차 및 방법론의 표준화에 대한 연구가 되어야 하겠다.

참고문헌

[1] Protecting America's Critical Infrastructures : PDD 63 May 22, 1998.
[2] 정보통신부, "정보통신기반보호법", Jan, 2001.
[3] 조태희, "정보통신기반 취약점 분석 평가", SIS2001, Jul, 2001.