2012년도 공동학술대회 논문집 pp. 529~532

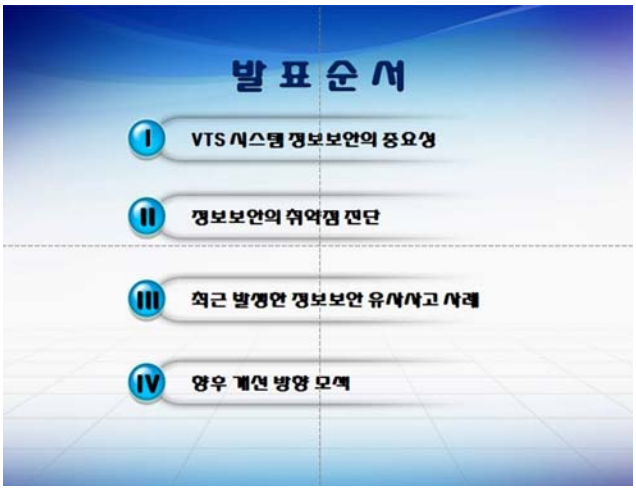
VTS 시스템의 정보보안의 중요성과 방향

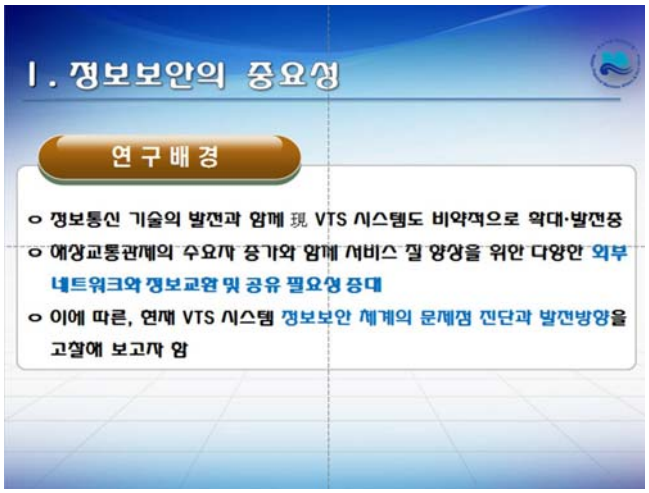
† 정 병우 · 김 효진 · 김 성윤

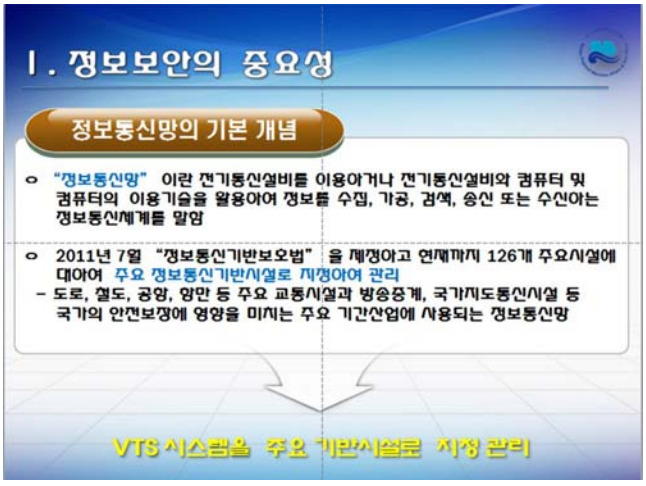
† 국토해양부 목포지방해양항만청

요 약 : 정보통신 기술 발전과 함께 VTS시스템도 비약적으로 발전하고 있다. 특히 해상교통관제의 수요자 증가와 서비스 질 향상을 위해 외부 네트워크의 연계를 통한 정보공유와 교환의 필요성이 지속 증가하고 있다. 따라서 VTS 시스템 간 및 외부 시스템과의 연계와 관련 정보보안의 취약점이 드러날 개연성이 높아졌다. 따라서 본 연구에서는 국가 주요 기반 시설로서의 VTS 시스템의 정보보안의 중요성과 현 취약점을 살펴보고 앞으로 개선해야 할 점을 고찰해 보았다.

핵심용어 : 정보통신망, 국가 주요 기반시설, 정보보안, 보안장비, IVEF 서비스, 정보보안시스템, 방화벽







Ⅰ. 정보보안의 중요성

정보통신망 발전의 역효과

- 국가나 민간이 제공하는 주요 사회 기반시설 대부분은 정보통신망 기반으로서 의존도 심화
  - 네트워크의 확대보급에 따라 정보교환 및 공유로 정보에 대한 불법접근 문제점 등
- 해킹 또는 웜·바이러스 감염 등의 전자적 침해로 엄청난 피해를 줄 가능성 상존
  - 예를 들어 국토해양부에서 관할하는 SOC분야 제어시스템이 해킹을 입게 된다면 철도사고, 해상선박충돌, 도로교통 마비, 수문조작으로 용수대란 발생 가능

정보통신망 불안감 사회 의존도 심화는
국가적 안보차원에서 위협이 될 수 있음

Ⅰ. 정보보안의 중요성

최근 국가기반시설 정보보안 사고사례

- 2003년 1. 25 인터넷 대란 사고
  - KT전화국 DNS서버를 공격에 큰 혼란
- 2009년 7. 7, 2011년 3. 4 DDOS 사태
  - 청와대 및 정부공공기관, 주요포털 및 금융사 웹사이트 등이 DDOS의 공격을 받음

* DDOS(Distibuted Denial of Service) : 인터넷 사용이 대용량화되면서 분산되어 있는 대량의 컴퓨터가 일제히 특정서버에 패킷을 송출하여 통신로에 과다 통신량을 발생시켜 네트워크 및 서버의 장애를 유발

기존 국가차원의 정보보안이 정보화 보급에 비해
중요도가 낮았던 것이 시발점

Ⅱ. 정보보안의 취약점 진단

정보보안 관련 법률

- 국가 사이버 안전관리 규정(2005년 제정), 정보통신기반 보호법(2001년 제정) 등
- 주요 정보통신 기반시설 보호는 행정안전부 주관, 그 외 부분의 공공부분은 국가정보원, 민간부분은 방송통신위원회가 각각 주관

→ 국내의 사이버 위기관리체계를 국가적 차원에서 총체적으로 대응할 수 있는 기관이 불투명, 전문적이면서 일관성 있는 대응이 어려운 구조를 가짐.

→ 법제의 대부분이 정보화를 다루는 부분에서 정보화의 역기능에 대비한 처벌 또는 정보보안 업무의 운영 측면을 언급하고 있을 뿐 기술의 연구 및 개발에 관련된 내용을 담고 있지 못함

Ⅱ. 정보보안의 취약점 진단

주요 국가 기반시설 점검결과

- 국가정보원이 최근 수도, 철도, 항만 등 국내 주요 기반시설의 정보보안 실태를 점검한 결과, 일부를 제외한 다수의 기반시설이 낮은 정보보호 수준을 보임
  - 정보보호 정책 설정, 실질적인 장비 운영, 내부 보안 운영 등
- 정보통신기반시설 대부분이 S/W방식의 정보보안(방화벽, 네트워크 보안) 에 의존
  - 통신포트 물리보안 설비를 갖추지 못하면 내·외부직원이 악의적으로 USB로 바이러스를 유포하거나, 해킹하고 정보를 유출할 가능성이 상존

* 스턱스넷(Stuxnet) : USB를 통해 전파되며 주요산업 기간시설의 제어시스템에 침투 해, 오작동을 일으키는 악성코드를 입력해 시스템을 마비시킬 수 있는 강력한 바이러스 웜

Ⅱ. 정보보안의 취약점 진단

❑ 전국 VTS시스템 보안장비 설치 현황

장비명	설치목적	설치년도	설치개소
방화벽	VTS-GICOMS 간 접근통제	2010~2011년	13곳
방화벽	인근 VTS간 접근통제	2011~2012년	7곳
방화벽	CCTV 서버 통제	2011년	3곳
보안USB	허가된 USB만 접근	2011년	2곳

→ 단순 PC 및 내부망 데이터 송수신 보호를 목적으로 방화벽같은 보안 1세대 장비를 주로 설치하고 있음

Ⅱ. 정보보안의 취약점 진단

❑ 보안장비의 발전 동향

구분	설치 목적	주요 장비
1세대	○ PC 및 내부망의 데이터 송수신 보호 목적	○ DOS백신, 네트워크 방화벽
2세대	○ 네트워크 보안 목적	○ 방화벽, 가상사설망(VPN) 침입탐지시스템(IDS), 침입방지시스템(IPS)
3세대	○ 조직에 맞춤형 및 유기적인 관리체계를 구축할 수 있는 정보보호 서비스	○ 조직 구성원의 정보보호인식 제고를 위한 교육, 전문인력에 의한 위탁관리인 아웃소싱, 컨설팅 등

Ⅱ. 정보보안의 취약점 진단

주요 문제점

- 정보보호 관련 법률상 국가 관리기관의 이원화 체계와 주요 기반시설 지정은 오이려 각 지방청 VTS 시설담당자의 업무 가중으로 나타남
- 現 보안담당자의 정보보안 분야 전문지식 부족과 전담인력의 부재
- 각 센터별 설치 보안장비의 원시성과 포맷 통일의 결여
- 국제적인 추세에 따른 인접VTS간 시스템 정보공유는 향후 보안문제가 따를 것으로 예상

* IVEF 서비스 : IVEF는 VTS에서 수집된 선박의 항적(Track) 정보를 인접 VTS 센터와 공유하기 위한 데이터 표준 프로토콜

Ⅲ. 최근 발생한 정보보안 유사사고

VTS시스템 정보보안 유사사고 사례

- 완도와 진도 VTS 센터의 관제구역이 인접해 있어 효율적인 선박운항관리 및 일부 음영구역 (어란진, 어령도 부근) 해소를 위해 2007년부터 양호 시스템을 연계 운영 추진
- 2010년 7월 이후 진도VTS 운영권이 해양경찰청으로 이관 되고 2011년 양 VTS 시스템의 외부 유지보수 용역업체가 달라 선정됨
- 2011. 3월경 발생한 진도VTS 시스템 장애 원인에 대해, 단순한 부품파손, 외부 해킹 등 수사
  - 당시 로그기록 확인시 진도VTS 시스템 서버에 접속한 IP 주소가 완도VTS 시스템 서버와 일치
- 양 업체간 사건은 당시 완도VTS에서 진도VTS로 원격접속한 사항은 진도VTS 시스템 장애 연장과 무관한 "혐의없음" 으로 종료됨

→ 진도VTS 운영권 이관 당시, 로깅데이터 및 네트워크 공유 등 보안상 문제점 등이 거론되었으나, 정보보안 등의 후속대책이 미흡했음

Ⅲ. 최근 발생한 정보보안 유사사고

❑ 완도-진도VTS 시스템 연계 현황

Ⅲ. 최근 발생한 정보보안 유사사고

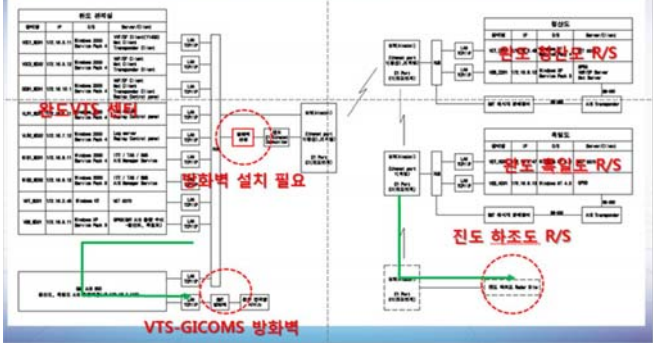
❑ 사이버 공격에 의한 피해 형태

구 분	내 용	유 형
1)경유지 이용	해킹피해를 당한 뒤 다른 사이트를 공격하는 경유지로 활용되는 피해	해킹경유지, 스팸 릴레이
2)웜 바이러스	웜 바이러스 감염시도 및 전이	감염시도, 감염 후 전이
3)홈페이지 변조	취약점 등을 통해 홈페이지 메인 페이지 변조, 타 페이지 삽입	홈페이지 변조, 삽입, 삭제
4)자료훼손/유출	서버 및 PC의 권한이나 공유설정 취약으로 자료 변조 / 삭제	자료삭제, 유출, 변조, 백도어 설치
5)단순침입시도	스캐닝기법이용 시스템이나 네트워크 취약점 조사	패스워드 추측시도, 스캐닝

→ 초기 진도 VTS시스템 장애원인을 외부의 웜 · 바이러스, 네트워크 침입시도 등의 해킹으로 간주하였음

Ⅲ. 최근 발생한 정보보안 유사사고

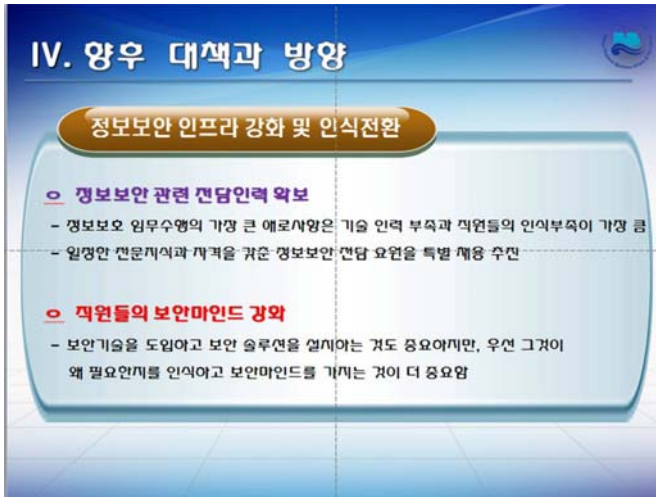
❑ 완도VTS 시스템 네트워크 구성도



Ⅳ. 향후 대책과 방향

보안시스템 포맷 통일과 적극적인 기술개발

- VTS 시스템 분야 정보보호수준 측정 및 지수화를 통해 적합한 정보보호시스템 선정 및 지수모델 개발 필요
  - 현재 각 지방청 관제센터는 제 각각 통일되지 못한 보안장비 설치운영과 일정 예산 미확보로 신규장비 도입의 어려움 발생
- 현재의 보안시스템은 방화벽 장비와 같은 공격탐지에 초점이 맞춰져 있으나, 근원지 역추적과 복구 분야의 장비 도입 검토
  - 시스템을 지속적으로 유지할 수 있도록 피해시간과 복구시간을 최소화
- 시스템 외부 유지보수 용역시 정보보안 분야의 적정 요율산정과 정보보호 대가 기준 마련
  - 정보보안 S/W는 CC인증 획득, 보안 업데이트, 보안정책 지원 등 개선요인이 수시로 발생


IV. 양후 대책과 방양
정보보안 인프라 강화 및 인식전환
○ 정보보안 관련 전담인력 확보
- 정보보호 임무수행의 가장 큰 애로사항은 기술 인력 부족과 직원들의 인식부족이 가장 큼
- 일정한 전문지식과 자격을 갖춘 정보보안 전담 요원을 특별 채용 추진
○ 직원들의 보안마인드 강화
- 보안기술을 도입하고 보안 솔루션을 설치하는 것도 중요하지만, 우선 그것이
왜 필요한지를 인식하고 보안마인드를 가지는 것이 더 중요함