2013년도 추계학술대회 논문집 pp. 353~355

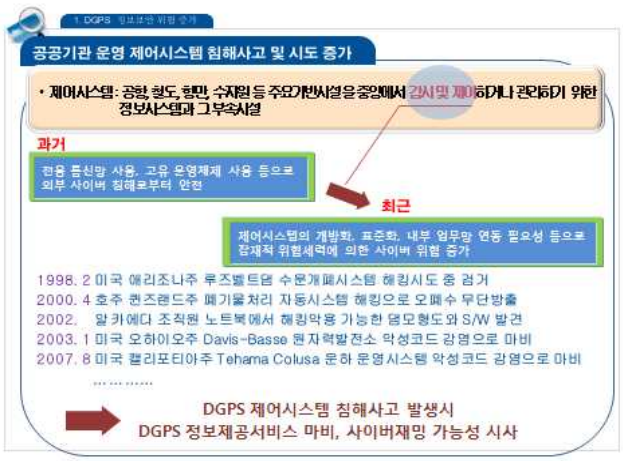
DGPS 정보보안에 관한 연구

† 최 대영 · 김 희태* · 구 자헌**

† 해양수산부 위성항법중앙사무소, *, ** 해양수산부 위성항법중앙사무소

요 약 : 최근의 사이버공격으로 각 국가기관에서 운영하는 제어시스템의 보안위협이 증가하고 있다. DGPS의 경우도 DGPS 정보시스템을 대상으로 새로운 유형의 공격이 제시되었다. 이에 사전 방어를 위해 체계적으로 정보보호관리체계(G-IMS)를 수립을 제시하였고 이로부터 안전하고 신뢰성 있는 DGPS 서비스를 제공하고자 한다.

핵심용어 : 정보보안, DGPS, ISMS, 제어시스템



† 교신저자 : chdy5@korea.kr 042)824-0941

* kht0704@korea.kr, ** jhgoo@korea.kr 042)824-0941

새로운 유형의 GPS 공격유형 제시(2012. 12. 14)

- 미국 카네기멜론 대학과 코히런트 네비게이션社에서 발표
- 기존의 GPS 공격유형 : 재밍이나 스푸핑과 같은 전파교란형태
- 새로운 유형의 GPS 공격유형 : 해킹을 통한 GPS수신기 소프트웨어 공격

최근의 GPS 수신기는 TCP/IP 기반의 네트워크 방식으로 작동됨

GPS 수신기도 컴퓨터처럼 작동되어 소프트웨어 공격이 가능해짐
- OS(윈도우 CE, Linux 등)
- 어플리케이션 지원(FTP서버, WEB서버 등)

- 위치계산 불가 또는 잘못된 보정정보 전송이 가능함
  (SW 접근 후 GPS 항법메세지 Parameter 변조, GPS Week Number 변조 등)
- 어플리케이션 취약점 공격시 관리, 제어불가 가능성 있음

.....

CONTENTS

2. DGPS 정보보안 관리체계 분석

안전하고 신뢰성 있는 DGPS 정보보안 관리체계 필요

전자정부 정보보호관리체계(G-ISMS) 도입
* G-ISMS : Government Information Security Management System

- 안전행정부 산하 한국인터넷진흥원(KISA)에서 전담(現 51건의 인증서 발급)
- 정부기관 조직 및 서비스의 특성에 적합하게 수립된 종합적인 정보보호 관리 체계
- 정보보안 법규 및 보안감사에 지속적인 대응 필요
- 보안전담 부서 부재에 따른 보안사각지대 발견 필요
- 신청 전 G-ISMS인증심사기준에 따라 자체점검 후 3개월간 시행하여야 함

G-ISMS 통제사항 및 인증절차

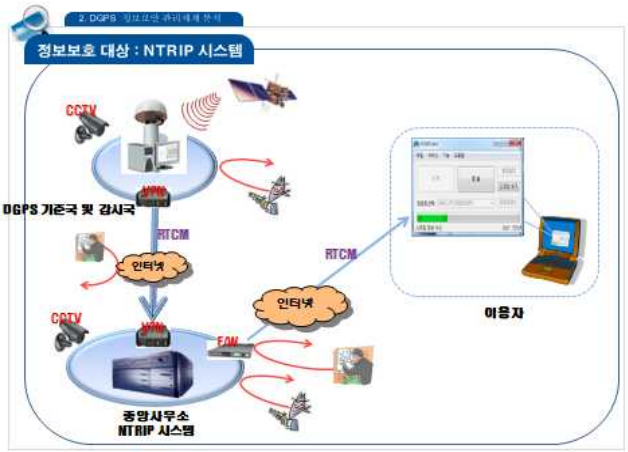
- 12개의 통제분야, 156개의 통제사항으로 구성

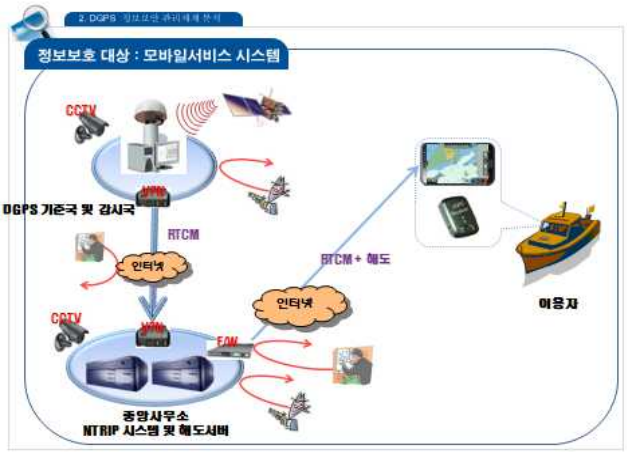
기관의 정보보호 대상·범위 정의
↓
분석 및 점검
↓
허용가능한 위험수준 설정
↓
지속적인 대응 및 관리

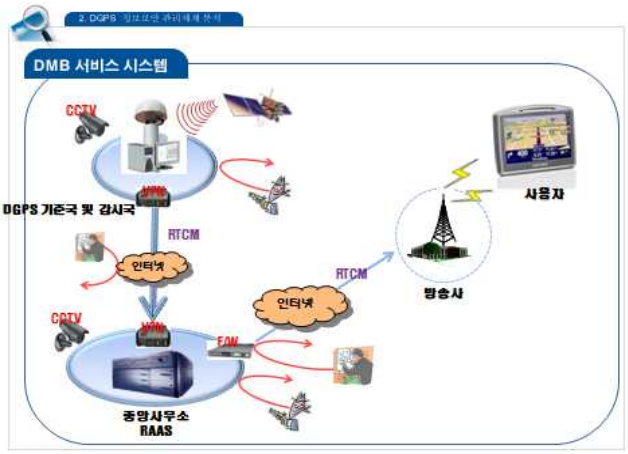
G-ISMS 통제분야 및 항목

통제분야	통제내용		통제분야	통제내용	
1. 정보보호 정책	1.1 정보보호 정책		7. 접근통제	7.1 접근통제에 대한 업무 요구사항 7.3 사용자 책임 7.5 운영시스템 접근통제 7.7 이동 컴퓨팅 및 원격지 근무	7.2 사용자 접근 관리 7.4 네트워크 접근통제 7.6 정보 접근제어
2. 정보보호 조직	2.1 정보보호 조직				
3. 자산관리	3.1 자산에 대한 책임	3.2 정보자산 분류			
4. 인적보안	4.1 해킹사 인적보안 4.3 퇴직 및 직무변경	4.2 위탁사 인적보안 4.4 업무적 보안	8. 정보시스템 요구사항, 개발 및 유지보수	8.1 정보시스템의 보안요구사항 8.3 업무처 통제 8.5 개발 및 지원과정에서의 보안	8.2 응용프로그램의 정확한 처리 8.4 시스템파일의 보안 8.6 기술적 취약성 관리
5. 물리적 보안	5.1 보호구역	5.2 정보처리 시설 및 장비보호	9. 보안사고관리	9.1 보안사고 및 취약점 보고	9.2 보안사고 대응 및 사후 관리
6. 통신 및 운영관리	6.1 운영절차 및 책임 6.3 정보시스템 인수 6.5 백업 6.7 매체관리 6.9 전자상거래서비스	6.2 제3자 서비스 관리 6.4 장애 소프트웨어관리 6.6 네트워크보안 6.8 정보의 교환 6.10 모니터링	10. 업무연속성 관리	10.1 업무연속성 관리	
			11. 준거성	11.1 법적 요구사항 준수 11.3 정보시스템 감사 고려사항	11.2 정보보호정책 준수
			12. 개인정보보호	12.1 개인정보 관리 12.3 개인정보 수집 및 처리 12.5 개인정보의 기술적 보호조치	12.2 CCTV 설치 및 관리 12.4 개인정보 처리의 열람 및 정정

정보보호 대상 : 중파방송 시스템







CONTENTS

03 분석결과 및 향후방향

DGPS 정보보안 분석 및 점검 결과

- 12개의 통제분야에 대한 점검 결과 대체로 양호한 결과를 보였으나,
- 일부 세부통제항목에 대해서는 현실적으로 기준을 적용하기 힘듦
  - 원격접속 접근통제에 관한 문제 : 관리대상이 도서지역에 다수 분포되어 원격접속을 엄격하게 제한하는 것은 DGPS 시스템 유지관리에 큰 영향을 미침(서비스 지연시간, 비용 …)

원격접속관리 정책에 대한 허용가능한 위험수준을 설정

- ☞ 관리대장 엄격히 기록
- ☞ 사전에 허가된 인력만 제한된 IP, Port, 시간으로 접속허가

DGPS 정보보안관리 향후 방향

정보보안관리를 모호한 개념이 아닌 실질적인 구현이 될 수 있도록

행정적인 측면에서의 정책(정보보안 예산수립, 인력양성 등)도 필요