항공기반시설의 보안사고 대응을 위한 보안체계 네트워크 모델에 관한 연구

정창화○ 신동렬
성균관대학교 이동통신공학과 대학원
grandprx@gmail.com, drshin@skku.edu

Security System Network Models for Security Accident Coping of Aviation infrastructure

Chang Hwa Jeong○ Dong Ryeol Shin
Department of Mobile Communications Eng., The Graduate School of Sungkyunkwan University

요 약

항공기반시설(공항, 기상 서비스, 항로 항행시설)에 대한 보안사고 대응을 위한 보안체계는 수립단계에서부터 착수하여 분석이 진행됨에 따라 세부적인 평가가 수행되어야하며, 시설변경이 발생하는 경우 변경된 시설에 대하여 재평가를 하여야 한다. 또한 항공기 운용과정에서 발생 가능한 각종 사고에 대한 사전 예방 및 정비를 위해서도 체계적인 보안성 평가가 필수적이다. 보안성 평가에는 계획(Plan), 활동(Do), 그리고 평가(Check), 조치(Action)업무가 네트워크 구조로 통합되어 적용되며, 과거의 사용 또는 경험에 따라 세분화된 보안성 평가 요구조건을 구분하여 적용한다. 특히 항공기반시설에 대한 보안성 입증과 안전한 운항을 보장하기 위하여 실시간 지원체계와 국가 차원에서 이를 관리하여야 한다. 이는 공공의 안전을 확보하기 위한 것으로서, 민간항공업체는 해당 법규, 표준서 및 지침 등에 따라 최소한의 보안성을 입증하여야 한다. 따라서 본 논문에서는 항공기반시설에 대한 보안사고 대응을 위한 보안체계를 위해 설정된 보안의 목표를 충족하고 있는지를 확인 평가하고, 분석 등을 고려하여 종합적인 보안성 평가기법을 적용할 수 있도록 하는 보안체계 네트워크 모델에 대해 제시하고자 한다.

1. 서 론

항공에 대한 보안활동은 2001년 9.11 테러사건 이전까지는 주로 승객과 항공기를 보호하기 위한 목적으로 수행되어 항공사 책임 중심으로 보안활동이 이루어져왔다. 그러나 현재에는 항공보안 활동이 단순히 항공기나 항공여객만을 보호하는 목적뿐만 아니라 항공기반시설(공항, 기상 서비스, 항로 항행시설)로 확대 적용되고 있으며, 규제와 그 시설들의 표준에 관한 권고사항이 강화되었다[1,2,3].

기술적 규제를 위한 규정은 영국의 Air Navigation Order, 미국의 Federal Aviation Regulations 등, 각 국가별로 차이가 있지만, 대체적으로 ICAC의 18개 부속서에서 규정하는 '국제표준과 권고실천안(International Standards and Recommended Practices)에 근거하여 제정되고 있다. 항공기는 공간을 운항하는 비행체로서 초고속 운송수단으로 사용되는데, 사고가 발생하게 되면 수많은 인명피해와 재산손실을 초래하게 되므로 높은 수준의 신뢰성과 안전성에 따른 보안성이 요구된다. 또한 항공기의 안전한 운항을 위해서는 항공기 시스템은 물론이고, 항공기반시설에 대한 안전성 평가 및 안전관리가 필수적이다. 여기서 보안성(Security)이란 항공기반시설이 위험상태에 이르지 않는 상태 또는 정도를 의미하는 것으로서, 본 논문에서는 항공기반시설의 모든 대상을 고려하였다. 항공기반시설은 공항, 기상 서비스, 항로 항행시설에 대해 보안기술과 임무수행을 위한 성능은 물론이고, 고도의 안전성 및 신뢰성이 요구된다. 따라서 대상 시설의 보안성을 입증하기 위한 보안 평가가 수행되어야 한다[4,5].

즉 보안성 평가는 보안의 핵심사항으로 수립단계에서부터 착수하여 분석이 진행됨에 따라 세부적인 평가가 수행되어야하며, 시설변경이 발생하는 경우 변경된 시설에 대하여 재평가를 하여야 한다. 또한 항공기 운용과정에서 발생 가능한 각종 사고에 대한 사전 예방 및 정비를 위해서도 체계적인 보안성 평가가 필수적이며 각 단

계는 상호 네트워크 구조를 가지고 있어야 한다.

항공기반시설 보안성 평가에는 계획(Plan), 활동(Do), 그리고 평가(Check), 조치(Action)업무가 네트워크 구조로 통합되어 적용되며, 과거의 사용 또는 경험에 따라 세분화된 보안성 평가 요구조건을 구분하여 적용한다. 특히 항공기반시설에 대한 보안성 입증과 안전한 운항을 보장하기 위하여 국가 차원에서 이를 관리하여야 한다. 이는 공공의 안전을 확보하기 위한 것으로서, 민간항공업체는 해당 법규, 표준서 및 지침 등에 따라 최소한의 보안성을 입증하여야 한다.

따라서 본 논문에서는 항공기반시설에 대한 보안성이 설정된 목표를 충족하고 있는지를 확인 평가하고, 분석 등을 고려하여 종합적인 보안성 평가기법을 적용할 수 있도록 하는 보안체계 네트워크 모델에 대해 제시하고자 한다.

2. 관련연구

항공기반시설은 매우 복잡하고, 다양한 시설에 대한 유지비용이 매우 많이 소요되고, 사고가 발생하면 이의 파급효과가 매우 커서 고도의 신뢰성과 안전성을 확보하기 위한 활동이 필수적이며, 안전성을 입증하기 위해 체계적이고 매우 엄격한 평가가 수행되어야 한다. 또한 항공기반시설은 항공기나 항공여객만을 보호하는 목적뿐만 아니라 공항, 기상 서비스, 항로 항행시설로 확대 적용되고 있는 만큼, 안정성과 신뢰성을 부여하기 위하여 보안체계 수립이 우선시 되어야 한다. 또한 안전성과 신뢰성의 확보를 목표로 수립되는 항공기반시설의 보안체계를 위하여 요구되는 보안성 평가는 군용기 또는 항공교통관제(ATC, Air Traffic Control) 시설 등의 획득 및 조달에 적용되는 안전성 평가와는 다소 차이가 있다[5,6,7,8].

항공기반시설에 대한 보안성 평가와 입증에 대한 법적 요구조건은 두 가지 목표에 따른 활동으로 구분된다. 첫째는 잠재적 위험요소 자체를 제거하는 것이고, 둘째는 제거가 불가능한 위험요소의 경우 잔존하는 위험수준을 허용할 수 있는 수준 이하로 낮추기 위한 활동이다. 두 가지 모두 시설의 보안성을 확보하기 위하여 여러 가지의 기술과 기법을 응용하게 되며 이 중 하나가 보안성 평가(Security Assessment)이다. 보안성 평가에서는 고장이나 재해의 발생확률을 평가하는 방법을 이용하며, 보안성을 확보하기 위한 종합적이고 균형적인 노력을 PDCA 사이클에 걸쳐서 검토하고 적절한 조치를 취하여야 한다. 이 과정에서 보안성을 입증하는 것은 보안담당자의 의무사항으로서, 다음과 같은 사항을 기본적으로 고려하여 적용하여야 한다[9.10,11,12].

① 허용할 수 있는 위험요소의 수준
② 위험수준을 낮추기 위한 활동의 범위
③ 위험수준을 낮추기 위한 활동의 효율성
④ 해당 법규 및 기준의 만족 여부

1960년대에서부터 최근까지 전 세계적으로 발생한 항공기 사고율을 보면 1970년대 이전까지 높았던 사고율이 기술과 시스템의 발전으로 인하여 1970년대 들어 급격히 감소되었으나, 1970년대 중반 이후부터 항공기 사고율은 더 이상 낮아지지 않고 30여년 동안 정체상태에 머물러 있다. 그러나 항공 운송량은 해마다 증가하고 있어 전체 사고 발생 횟수는 오히려 늘어나고 있으며 이 같은 추세가 지속된다면 2012년에는 현재보다 4배 이상 증가할 것으로 예상된다. 이에 따라 세계 각 국의 공항당국을 비롯한 국제민간항공기구 등 항공안전과 관련된 조직은 다음과 같은 목표를 설정하고, 항공기반시설에 대한 사고예방을 위한 보안성 평가 기법 개발하여 보호체계를 수립하고 있으며, 평가를 위한 규정, 기준 또는 표준 제정에 대한 체계적 관리를 수행하기 위한 연구를 진행하고 있다[5,7,9,10,13].

미연방항공청(FAA)은 2007년까지 1994~1996년 당시 사고율의 80% 수준으로 낮추고, 이를 지속시키는 것을 목표로 보안성 확보를 위한 활동을 진행 중이다. 유럽연합은 항공기반시설의 보안 수준을 향상시키고, 유럽 각국에 동일한 체제를 유지하기 위하여 2002년에 유럽 연합공항당국(EASA, European Aviation Safety Agency)을 구성하였으며, 민간 항공기에 대한 업무를 비롯하여 보안성 확보를 위한 활동을 공동으로 수행중이다. 특히 유럽의 항공산업체간 과도한 경쟁으로 인한 손실을 방지하고, 공동 개발 및 연구를 통해 보안성 향상에 기여하기 위한 목표도 가지고 있으며, 최근에는 비유럽 국가의 공항당국과도 협력체계를 확대해 나가고 있다.

3. 항공기반시설 보안체계 프로세스

항공기반시설 보안체계 네트워크구조의 주요 목표는 해당 보안요구조건에 부합하는지 확인하고 최소한의 보안성을 보장하기 위한 것이다. 이러한 시설 중에서 공항, 기상 서비스, 항로 항행시설이 보안성 평가의 개념이 적용되는 프로세스에는 관리적보안, 기술적보안, 물리적보안 검증 등이 있으며, 이와 같은 프로세스에는 예상 환경조건에서 점검 결과가 지속적으로 유지된다는 것을 입증하기 위한 점검 방법 및 적합성 입증을 위한 세부 기법들이 포함된다. 각 프로세스는 서로 다른 분야에 초점

을 맞추어 진행되지만, 궁극적인 목표는 항공기반시설의 보호체계를 위한 것으로서 이러한 프로세스들은 항공기반시설 프로세스 내에서 상관관계를 갖고 있으며 상호중복 되기도 한다. 프로세스가 간단하여 직접적인 방법으로 보호체계 수립이 가능한 경우에는 몇 가지 기본적인 보안성 평가 기법을 적용하는 것만으로도 보안성을 입증할 수 있지만, 복잡한 경우에는 개별 세부시설에 대한 세부항목을 적용하여 전체 프로세스에 대한 평가를 수행하여야 한다. 또한, 보안성에 대한 목표를 수립하고, 설정된 목표를 충족하고 있는지를 평가하며, 항공기반시설의 사고 발생을 방지하거나 사고가 발생하였을 때 이로 인한 영향(손실)을 최소화하기 위한 노력이 체계적으로 이루어져야 한다. 이러한 프로세스의 최종 단계는 더 이상의 점검 또는 분석이 필요하지 않을 정도로 검토, 검사 또는 기타 조치 등을 수행하여 보안 조치사항에 대하여 입증하기 위한 조사 및 관련 활동이 완결되는 시점이다.

(1) 보호체계 수립

보호체계 수립 승인에는 대상 시설의 보안성 확인을 위해 적용되는 문서화 및 점검 등의 프로세스가 포함되며, 주요 목표는 항공기반시설에 설정된 범위에서 운용되는 경우, 요구되는 보안기능을 안전하게 수행할 수 있다는 것을 입증하기 위한 것이다. 또한 기반시설이 적절하게 통합될 수 있다는 것을 입증하기 위해서도 보호체계 승인이 필요하며, 항공기반시설의 운용에 있어서 모든 위험성이 최소화되었다는 것을 입증하기 위하여 수행된다. 즉, 보호체계 승인은 보호체계 요구조건에 적합하다는 것을 검증하기 위해서, 시설의 대상 수준에 대하여 수행되는 평가 프로세스이다. 예상 운용 범위 결정, 설정된 운용 범위 내에서의 점검 및 조치의 운용을 보증하기 위한 제한사항 설정을 포함한 보호체계 수립 승인의 기초사항이 이 프로세스의 범위이며, 공학적 분석, 검사, 설계 검토, 안전성 평가, 공급업체 승인 및 시험 등이 이 프로세스에 포함된다. 보호체계 승인 계획서 작성 단계에서 보호체계 수립 요구조건이 개발되어야 한다.

(2) 보안성 검증

보안성 검증은 대상 시설이 설정된 요구조건을 만족하는지 판단하기 위하여 적용되는 프로세스로서, 검사, 분석, 실증 및 시험을 통해 모든 계약 보안 규격 요구조건을 만족한다는 것을 입증하기 위한 것이다. 보안성 검증은 계약업체가 계약 요구조건을 만족시켰는지를 확인하기 위하여 적용되는 프로세스이지만, 이 프로세스를 통해 도출된 대부분 시설의 보호체계 입증을 위해 사용되기도 한다. 보안성 검증은 시설이 보안 요구조건에 적합하게 작동하는지 포괄적으로 평가하기 위한 프로세스로서, 주로 안전성에 중점을 두고 진행되며, 시설의 보안 보안성 보증 부분에 대한 규칙에는 설정된 개별 규칙 항목에 대하여 보안성을 입증하기 위한 보안성매트릭스가 포함된다. 보안성 검증의 범위는 이러한 보안 요구조건을 만족시키는 것으로서, 예를 들어 세부시설 수준에 대한 보안성 검증 프로세스에서는 세부시설 수준에 대한 보안 요구조건을 규정하여야 한다.

(3) 보호체계 프로세스

보호체계 프로세스는 보안담당자에 의해 전반적 시설에 도출된 보안 요구조건에 적합한지 판단하기 위하여 사용되는 프로세스로 정의한다. 여기서 초기평가는 현 수립되어 있는 보호체계를 기반으로 하는 개념으로서, 통상적으로 첫 단계에서는 문서를 대상으로 하는 반면, 현장점검 단계에서는 세부시설을 대상으로 하게 된다. 평가의 목표는 기존 수립된 보호체계를 통하여 이전에 승인된 체계를 수행하고 있는지를 확인하기 위한 것이다. 초도프로세스는 통상적으로 계획 단계에 착수한 이후에 적용된다. 이러한 프로세스 승인은 수립 방법 및 프로세스가 승인된 보안의 특성을 변경시키지 않는다는 것을 입증하기 위해서도 적용된다.
승인된 프로세스는 대상 시설이 해당 프로세스 및 절차에 따라 수립되었는지 확인하고, 수립된 프로세스가 규정된 운용 조건에서 보안 요구조건에 부합하는지 확인하는 과정으로 구성된다. 이러한 프로세스의 중요한 측면은 초기 계획 및 승인 절차에서 검증된 수준과 동등한 보안성이 검증되도록 절차와 수행을 설정하고 이를 확인하여야 한다는 것이다. 프로세스 승인을 위한 검증 및 점검 범위는 보안성 재확인을 위한 이전의 승인과정을 재수행하고 프로세스에 대한 승인을 위한 추가 점검을 수행하는 것이다.

(4) 조치사항 확인

조치사항은 평가를 기반으로 기반시설 중 보안성이 취약한 부분에 대해 재점검을 운용하는 과정이다. 이러한 조치사항의 확인에 대하여 집중적으로 계획, 활동, 평가 및 조치하는 프로세스로 정의하며, 다음과 같은 두 가지 목표에 따라 수행한다. 첫째는 항공기반시설의 보안 강화일환으로 기반시설이 적절하게 보안사고에 대한 대응력이 갖춰졌는지 확인하기 위한 것이고, 둘째는 기반시설의 중요한 특성을 사전에 파악하여, 세부적인 사항까지의 모든 과정에 대하여 관리해야 할 사항을 설정하고

이를 안정화시키기 위한 것이다. 이러한 기반시설에 대한 조치확인은 대상 시설에 대한 관리 수준과 기술적 세부 요건의 수준에 있어서, 기타일반 시설에 대한 프로세스와 차이가 있다. 기반시설 보안 프로세스에서 요구되는 점검 및 분석의 범위는 안전한 비행조건 유지를 위해 중요한 시설에 대한 보안의 특성을 설정하고, 이러한 특성에 대한 세부내용을 설정하는 것이다. 기반시설에 대한 보안 활동에는 비행 안전 특성에 대한 수준에서의 조치, 그리고 점검활동 범위와 추적 요구조건을 설정하는 활동이 포함된다.

4. 항공기반시설 보안체계 모델 분석

ISO 13335 GMTS, ISO27001, VAF, OCTAVE와 같은 국제표준과 국내기준인 KISA ISMS, 행안부 G-ISMS, 정보통신기반보호법, 안전진단기준에 따라 항공기반시설의 최신 정보보호 환경 분석과 위험분석 과정에서 도출된 취약점에 대해 취약점 분석·평가를 한다.

취약성의 유형을 관리적, 물리적, 기술적으로 구분하여 식별하고 보안수준평가를 한다. 이 보안수준평가를 통해 관리적영역, 물리적영역, 기술적영역(서버, 네트워크, DB, PC, 노트북)으로 대상을 구분하고 취약성에 대한 평가를 GAP분석자료 및 스캐너 점검결과, 체크리스트 점검결과, 로그분석결과, 모의해킹결과를 이용하여 실시한다.

항공기반시설 보안체계의 보안기능은 예방(Protection)과 모니터링(Adit Trail)으로 구분한다. 예방은 유출통제(Responsible Use), 접근통제(Secure Use)로 세분화한다. 세분화한 기능의 유출통제를 위해 메일 및 메신저 등의 보안시스템을 적용한다. 또한 접근통제는 DRM과 DB보안, 네트워크 접근제어(NAC)를 적용한다. 마지막으로 모니터링 보안기능은 보안대상의 모니터링 및 필터링을 적용한다.

이 모델의 항공기반시설의 보안체계를 수립하고 이행, 점검, 개선하기 위한 프로세스를 정립하기 위해 항공시설기반보호관리체계를 수립한다. 이 체계에서 표준서(정책, 지침, 절차)의 개발과 지속적인 개선을 위한 사후관리 프로세스를 정립한다. 표준서의 내용에는 항공기반시설보호위원회를 설치하고 관련 규정을 마련하여 통제 및 모니터링을 주기적으로 이행되도록 제도적으로 마련한다. 또한 기반시설보호규정 등을 문서화 한다.

항공기반시설 보안체계는 국제표준, 자산분석, 위험분석, 취약성분석, 문서화, 정책수립, 관리체계 정립, 사후관리 등의 순으로 순환되는 구조를 가지도록 설계한다.

5. 보호체계 평가 결과의 반영

항공기반시설에 대한 보안성 평가 결과는 지속적으로 보호체계 수립에 반영되어야 하는데, 이러한 변경은 사고 발생 원인을 완전히 제거하는 것이 이상적이지만, 기술수준, 환경 제약조건, 비용 등의 문제로 인하여 불가능할 경우에는 평가 대상의 사고발생 확률 및 심각도 등급을 종합적으로 고려하여 다음과 같은 우선순위에 따라 적용하여야 한다.

(1) 최소 위험성 설계

제거가 불가능한 위험요소의 경우에는 잔존하는 위험성을 허용수준 이하로 낮추기 위한 보호체계 변경이 이루어져야 한다. 여기서 허용 가능한 수준은 보안성평가 대상에 따라 관리적, 기술적, 물리적 판단을 바탕으로 설정되어야 하며, 발생확률을 낮추거나 사고로 인한 영향을 최소화하는 방안이 이에 포함된다.

(2) 보안장치의 추가 설치

위험성을 최소화하기 위한 보호체계 수립이 불가능한 경우에는 보안 환경 특성을 반영하거나 자동으로 동작하는 고정식 보안장치를 추가적으로 설치하는 방안으로서, 설치된 보안장치에 대해서는 주기적인 보안 점검이 요구되며, 이를 해당 절차에 따라 문서화하여야한다.

(3) 기반시설 경보장치 설치

위의 2가지 방안을 적용할 수 없는 경우에는 상태를 감지하여 위험 발생 조건에 대하여 적절한 경보신호를 발생할 수 있는 경보장치를 설치한다. 이러한 경보신호 및 경보장치는 인적요소를 충분히 고려하여 보호체계에 반영하고, 운용상의 오작동 및 부적절한반응이 발생하지 않도록 설치하여야 한다.

(4) 절차 및 훈련과정 개발

위의 모든 대안이 실현 불가능한 경우에 비상절차를 개발하여 이를 숙지할 수 있도록 반복적으로 훈련하는 방안으로서, 심각도가 High level 및 Critical level 등급인 경우 위험성을 감소시키기 위하여 절차 및 훈련과정을 개발하고자 하는 경우에는 해당 공항당국의 승인을 받아야 한다.

6. 결론

항공기반시설의 보호체계 수립을 위해서는 보안성평가를 수행하고, 대상 시설의 세부 요구조건에 대한 보안성

이 입증되어야 한다. 이를 위해서는 보안성 평가를 위한 모든 사고가 설정되고, 이러한 사고를 유발할 수 있는 원인 중 중요사항이 모두 고려되었다는 것을 보장할 수 있도록 계획 및 관리되어야 한다. 특히, 기반시설과 같은 복잡한 프로세스의 경우에는 절차 및 프로세스의 통합으로 인해 야기되는 추가적인 복잡성 및 상호의존성을 고려하여야 하며, 통합시설을 포함한 모든 경우에 대하여 시설의 적절한 보안성 목표를 수립하고, 이 목표의 만족 여부를 판단하기 위한 보안성 평가를 전체 기반시설의 관점에서 수행하여야 한다. 그리고 운용 중 변동사항이 발생할 경우에는 이로 인하여 기반시설의 보안성에 미치는 영향을 다시 평가하여야 하며, 기반시설의 보안성을 수치적 확률분석만으로 입증하여서는 안 되고, 시설 보안성 평가를 위한 공학적 판단이 중심이 되어야 한다. 이러한 공학적 판단의 구조는 보호체계 수립에서 보안성 평가까지 과정을 상위계층 네트워크구조를 취한 프로세스가 되어야 한다. 이를 위해서는 보안성 평가를 위한 지속적인 연구 및 개선활동이 진행되어야 하며, 대상 시설에 따라 세부적으로 적용해야 할 기법의 개발이 필요하다.

참고문헌

[1] SAE ARP 4754, "Certification Considerations for Highly-integrated or Complex Aircraft Systems"

[2] ETRI 정보화기술연구소, "일본의 e-Japan 전략 Ⅱ," 주간기술동향 통권 1103호, 정보통신연구진흥원, 2003.7.

[3] SAE ARP 4761, "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment"

[4] FAA System Safety Handbook, "Practices and Guidelines for Conducting System Safety Engineering and Management"

[5]강자영, 안재형, "항공위협의 역사적 고찰과 항공보안 관리에 관한 연구," 한국항공운항학회지, 제12권 2호, 2004. 9.

[6] Cranfield Univ., 2006, "Safety Assessment of Aircraft Systems"

[7] ADS-51-HDBK Aeronautical Design Standard Handbook, 1996. "Rotorcraft and Aircraft Qualification(RAQ) Handbook

[8] Frank C. Fickeisen, SAE 2001-01-2664, "Improving the Effectiveness of Airplane Certification Analysis Processes"

[9] Y. Papadopoulos, J.A.McDermid, Reliability Engineering and Systems Safety 63, 2007, 47~66, "The Potential for a generic approach to certification of safety critical systems in the transportation sector"

[10] J. Murdoch, J.A. McDermid, P.Wilkinson, International System Safety Conference, 2008. "Failure Modes
and Effects Analysis (FMEA) and Systematic Design"

[11] Safety & Security Measurement White Paper V2.0, 2004. PSM Safety & Security TWG

[12] Junichiro Saito and Kouichi Sakurai, "Privacy Protection Using Re-encryption in RFID
Tags," Technical Report of IEICE ISEC 2008-81, Nov. 2008.

[13] P. Golle, M. Jakobsson, A. Jules, and P. Syverson, "Universal Re-encryption for Mixnets," 2007, http://www.rsasecurity.com.