# 항공관제에서 비행자료 보호 관리 시스템에 관한 연구1)

이덕규*, 한종욱*
*한국전자통신연구원
e-mail:deokgyulee@etri.re.kr

# A Study on Flight Data Protection System Data in Flight Control

Deok Gyu Lee*, Jong-Wook Han*
*Electronics & Telecommunications Research Institute

요 약

본 논문은 내부 혹은 외부의 바이러스의 피해 및 비행자료 변조 및 수정 등의 해킹 발생에서 비행자료 시스템의 가용성, 신뢰성 및 무결성을 강화시켜 비행자료시스템 운영 시 관제 서비스를 마비시키는 다양한 사이버 테레에 대응하여 실시간으로 자동으로 재해를 복구하는 시스템 및 그 방법에 대한 것이다. 비행자료시스템 실시간 자동재해복구시스템은 임베디드 시스템을 제공하며, EWF(Enhanced Write Filter)를 이용하며 OS(Operating System)을 보호하여 시스템을 안전하게 운용할 수 있는 장점을 갖는다.

## 1. 서론

비행자료처리시스템은 다양한 국가와 다양한 비행자료를 통해 처리해야하는 자료가 방대하며, 비행관제에 있어 핵심이 되고 있다. 특정 다수에 의해 사용되는데 비해 내/외부의 공격은 다양화, 지능화되어 응용계층 특히, 비행자료처리 시스템 전체에 대해 위협을 증대되고 있는 실정이다. 특히 기존 시스템인 방화벽, SSL, IDS/IPS, VPN, 보안 OS등을 이용하여 네트워크 계층에서의 방어를 한다 하더라도 내부위협자로부터 자료 위/변조에 대해 자유롭지 못하며, 위와 같은 네트워크 계층의 보안이라 할지라도 어플리케이션 계층에서의 위협은 산재되어 있는 실정이다. 이러한 위협은 비행자료처리 시스템 전체 마비에 따른 관제 서비스 중단, 비행사고와 같은 인명 피해, 막대한 비용의 손실, 국가 공신력 및 신뢰성 실추, 피해복구에의 손실 등과 같이 많은 피해가 발생할 수 있다.

시스템 취약의 다양성과 해킹 등 다양한 사이버테러 및 내부 공격자들로 인해 비행자료처리시스템을 보호할 수 없다. 현재 비행망이 폐쇄망이라 할지라도 각 국가가 모두 동일한 보안수준을 갖추고 있지 못하며, 동일한 보안 수준이라 할지라도 내부 위협자들 및 외부 해킹으로부터 자유로울 수 없다.[1-3]

본 논문은 비행자료처리시스템에서 운영되는 비행자료 서버의 가용성, 무결성 및 신뢰성을 위한 실시간 자동 재해 복구 시스템 및 그 방법에 관한 것으로, 내부 혹은 외부로 비행자료의 전송과 같은 관제 서비스를 제공하는데 있어 가용성, 신뢰성 및 무결성을 높여 비행자료처리시스템 운영을 방해하는 다양한 사이버테러에 대응하여 비행자료의 위/변조 등을 감시하고 자동으로 재해복구를 하는 방법에 관한 것이다. [4, 7, 8][10]

본 논문은 위와 같은 문제점을 인식하고 이를 해결하고자 제안한 것으로, 목적은 네트워크상에 설치되어있는 비행자료처리시스템이 다양한 해킹 및 사이버테러에 대하여 실시간으로 지능적 보증 에이전트(IAA: Intelligent Assurance Agent)를 이용하여 비행자료처리시스템의 변조 및 수정이 발생할 경우 자동으로 재해 복구하여 관제 서비스를 중단 없이 제공하는 것을 목적으로 한다.

## 2. 비행자료 자동복구 시스템

본 논문은 서론에서의 문제점을 해결하기 위해 구성을 살펴본 후 세부 제안방식에 대해 설명한다.

그림 1을 보면, 해커의 침입 혹은 사이버 테러로 인해 비행자료처리시스템에서 서비스 또는 비행자료를 삭제하거나 변조 혹은 수정을 하면 실시간으로 자동 재해복구시스템에게 비행자료처리시스템의 변화를 통보하여 복구가 자동으로 진행된다.[5, 6, 9]

그림 2는 실시간 비행자료 자동재해복구시스템(RFRS: Real-time Flight data Recovery System)과 비행자료 시스템으로 나눈다. 실시간 비행자료 자동재해복구 시스템은 다음과 같은 모듈로 구성된다.

임베디드 시스템 모듈(Embedded System Module), 비행

1) 본 연구는 건설교통부 항공선진화사업의 연구비 지원(과제번호# 07항공-항행-03)에 의해 수행되었습니다.

자료 저장소 모듈(Flight data Storage Module), OS저장소 모듈(OS Storage Module), 비행자료 정보사전 모듈(Flight data Information Dictionary Module), 비행자료 복구관리자 모듈(Flight data Recovery Management Module), 호스트 메시지 감시데몬 모듈(Host Message Monitoring Demon Module)로 구성되어 있다. 외부 망 혹은 네트워크를 통해 시스템 메시지가 전송되며, 각 상황에 따라 복구를 위한 비행자료 전송 및 시스템의 데몬과 호스트의 에이전트 연결 매개체가 된다.

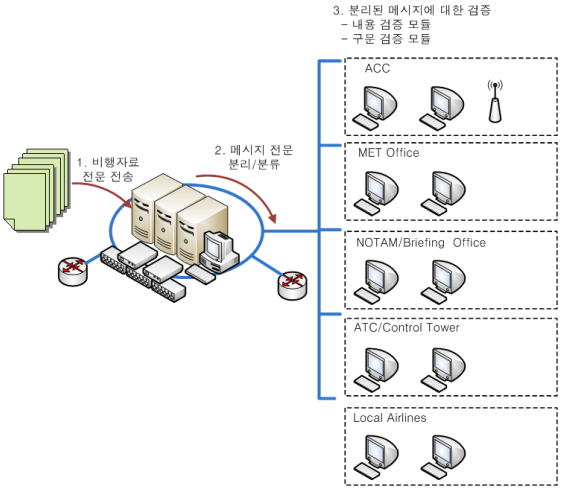


그림 1 비행자료 보호 시스템 개요

재해복구시스템의 모듈 중 임베디드 시스템 모듈, 비행자료 저장소 모듈, OS저장소 모듈, 비행자료 정보사전 모듈은 EWF(Enhanced Write Filter)로 쓰기 방지를 하여 시스템을 보호하며, 이를 통해 시스템의 가용성, 신뢰성 및 무결성을 높일 수 있다. 비행자료처리시스템에서 비행자료 감시 에이전트(Flight data Monitoring Module)가 데몬 형태로 상주하여 비행자료의 이상 여부를 비행자료처리시스템에서 감사한다.

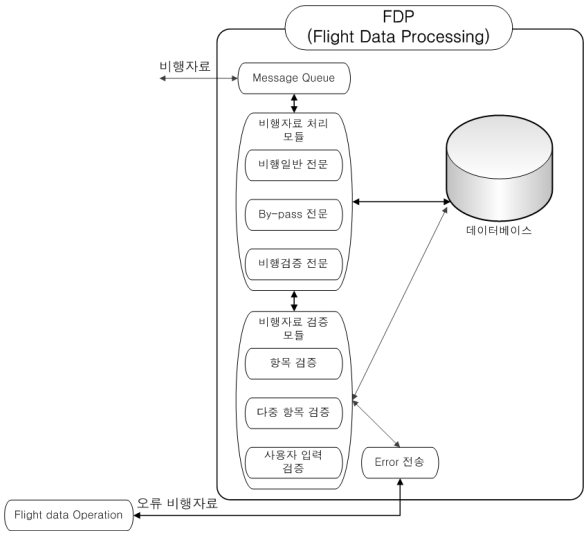


그림 2 비행자료 보호 시스템 상세 모듈

비행자료처리시스템 실시간 자동 재해복구시스템은 비행자료 정보사전을 호스트로부터 정보를 얻어서 진행하며, 호스트의 비행자료 감시 에이전트는 시스템 이벤트 발생 시 파일을 후킹(Hooking)하여 파일의 삭제, 위조, 변조 또는 시스템에 새로운 비행자료가 생성되면 호스트 감시 데몬에 비행자료를 전달하여 복구모듈을 작동시켜 각 상황에 맞도록 처리 후, 이벤트 로그를 저장하고 처리상황을 복구관리자에게 상황을 알려준다. (e-mail, SMS 등)

비행자료 정보 사전을 생성하는 과정으로 본 과정은 비행자료의 원본을 보관하는 것이다. 최초 AFTN을 통해 들어온 비행자료, 혹은 입력된 비행자료에 대해 데이터를 저장한다. 이때 저장할 수 있는 권한은 정적으로 관리자에게 있으며, 저장된 비행자료는 실시간 자동 재해복구시스템의 비행자료저장소에 복제 혹은 복사한다.

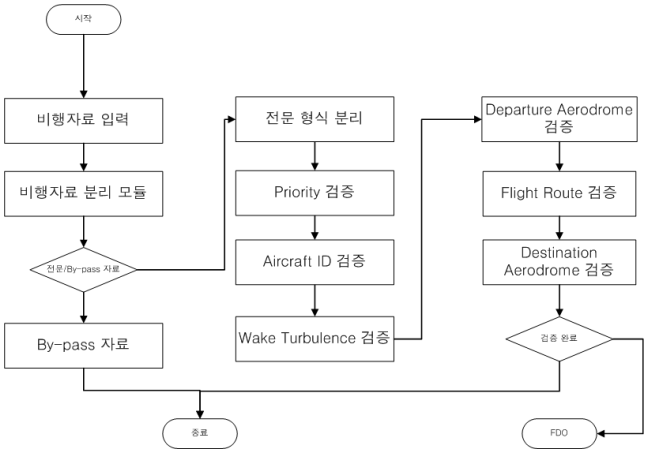


그림 3 비행자료 보호 시스템 흐름도

비행자료감시에이전트 모듈의 처리과정으로 I/O request packet을 감사한다. 비행자료감시에이전트는 기본적으로 filter driver를 이용하며, filter driver는 파일 시스템 드라이버나 디스크 드라이버와 같은 드라이버에 전달되는 I/O요청을 가로채어 기존의 드라이버가 제공하는 기능을 보완하거나 새로운 기능을 추가할 수 있는 형태이다. 비행자료의 요청이나 처리된 비행자료의 요청이 있는 경우, 요청에 대하여 처리된 비행자료를 전송하는 경우 각각 가로채어 정당한 요청과 정당한 처리결과인지 모니터링할 수 있다. 파일 후킹을 진행하여 파일 변조 및 삭제 여부를 확인하고 이상 발생 시 호스트 메시지 감시 데몬에 시스템 메시지를 전송하여 감시 데몬은 각 상황에 맞도록 프로세스를 실행한다. 이때 실행되는 프로세스는 다음과 같은 절차를 따른다. 비행자료 실시간 자동 재해복구시스템에서 데몬 형태로 있으면서 호스트 및 비행자료처리 시스템의 에이전트가 보내는 메시지를 분석하여 각 상황에 맞는 프로세스를 실행한다. 마지막으로 비행자료 정보사전에서 기존 변조가 있는 비행자료와 비교 검색한다. 이때 이상이 발생한 경우 각 상황에 맞춰 복구형태를 결정하며 실시간 비행자료 복구시스템이 복구한다.

마지막으로 복구 모듈에서 처리되는 과정으로 비행자

료에 대해 이상이 발생한 경우 비행자료정보사전과 비교하여 처리를 진행한다. 비행자료의 삭제가 발생한 경우 비행자료 저장소에서 원본복제 파일을 검색하여 장애가 발생된 시점으로 비행자료를 전송하여 복구하며, 불법적인 비행자료 추가가 발생한 경우 비행자료에 대한 삭제를 진행한다. 비행자료 수정 및 변조가 발생한 경우, 이상비행자료는 삭제하고 원본 복사 파일을 전송하여 시스템을 복구한다. 비행자료 첨부 및 비행자료 수정의 경우, 각 상황(이상적인 행위, 비이상적인 행위)에 대처하고 각 비행자료를 검역소에 저장하여 차후의 문제를 동일 패턴에 대해 처리하도록 한다.

## 3. 결론

비행자료처리스템에서 발생하는 사이버테러 혹은 악성변화에 대해 비행자료처리시스템의 가용성을 최대화 시키고 비행자료처리시스템의 정지시간 동안 안정적으로 관제서비스를 제공할 수 있다. 다양한 공격(사이버테러, 내부자 공격, 파일 위/변조 등)에 대해 비행자료에 대한 처리 및 복구가 가능하며, 이벤트 로그를 이용하여 추후 이에 대한 분석을 통해 동일한 공격 형태를 예방할 수 있다. 비행자료 변조로부터 복구가 수동이나 갑작스런 초기상태로의 복구가 아닌 자동으로 실시간 복구되어 복구비용 측면뿐 아니라 국가 신뢰도 및 인명피해를 사전에 예방할 수 있다.

## 참고문헌

[1] Dr.Jae Sug Ki. Study on Developing a Flight Data Visualization. 산업경영시스템학회지 Vol. 25, Sep 2003

[2] Chris, Mitchell. & Walter, Gekelman. Real-time physics data-visualization system using Performer. Computers in Physic, Vol.12, No. 4, July/August 1998, pp 371-379

[3] Dennig, James, Clark, Nicholas, Korthuis, David, Prince, Michale. & Kim, Hyun-Soo. Bid Document: F/A-18 Memory unit data visualization project. Http://wonderwoman.cse.msu.edu

[4] Ronald, L. Small, Stephen, D. Lakowske, Jerry, Bresee. & Gerry, Callejo. A future direction in pilot training. Specific Applications in Pilot Training, September 1999, pp 281-285.

[5] Roth, S. A, Lucas, P, Senn, J. A, Gomberg, C. C, Burks, M. B, Stroffolino, P, J., Kolojejchick, J. A, & Dunmire, C. "Visage: A user interface environment for exploring information." Proceedings of Information Visualization, IEEE, San Francisco, October 1996, pp. 3-12.

[6] Rouff, Christopher. & Robbert, Mary Ann. Developing the cooperative mission development environment. ACM International Conference on Supporting Group Work, Phoenix, AZ, November 1997

[7] SimAuthors Inc, FlightViz, www.simauthor.com

[8] Spirent Systems, GRAF-VISION Flight Data Animator, www.spirent-systems.com

[9] SystemWare Incorporated, FDAS, www.sysware.com

[10] 이덕규, 한종욱 "항공관제에서 비행자료 자동복구 시스템에 관한 연구", 2011년도 한국정보처리학회 추계학술대회