Journal of the Korea Academia-Industrial cooperation Society
Vol. 17, No. 11 pp. 248-255, 2016

http://dx.doi.org/10.5762/KAIS.2016.17.11.248
ISSN 1975-4701 / eISSN 2288-4688

보안성을 강화한 정보연계 프레임워크 및 아키텍처 설계에 관한 연구 - 국방 분야를 중심으로

강민정
국방기술품질원

A Study on Designing of Information Integration Framework and Architecture with Enhanced Security Focused on defense field

Min-Jung Kang
Defense Agency for Technology and Quality

요 약 정보화 시대의 도래로 각 기관에서 생성되는 정보의 종류와 양이 점차 증가하고 있으며, 또한 관련 기관 간 데이터를 연계하는 정보연계 역시 증가되고 있다. 국방 분야에서는 군수품의 품질을 담당하는 국방기술품질원에서 군수품의 품질 향상을 위해 품질관련 정보를 수집·분석하려는 노력을 지속하고 있으며, 정보연계 대상 또한 국방 분야의 기관뿐만 아니라 민간기관의 데이터까지 확대하고자 노력하고 있다. 서로 다른 환경의 정보체계 데이터를 연계하는 방법으로 여러 가지 방법들이 사용되는데, 높은 보안성이 요구되는 국방 분야에는 보안측면을 더욱 강화한 연계방안의 수립 및 적용이 필요하다. 본 논문에서는 다양한 정보화 환경의 기관 간 업무처리를 위하여 필요한 업무요건과 보안 고려요소를 고찰하고, 이에 적합한 연계 아키텍처 및 표준 연계 프레임워크를 제시하였다. 그리고 제시된 프레임워크를 4개 연구기관의 정보체계에 시범적으로 적용하여 기관 간 데이터 연계로 업무처리가 이루어질 수 있음을 확인하였다. 본 연구 결과를 토대로 국방 분야에도 안전하게 적용할 수 있는 정보연계 아키텍처가 제시되었으며, 특히 보안성이 강화된 표준 연계 프레임워크를 적용함에 따라 수집된 데이터는 군수품 품질향상을 위한 정보로 유용하게 활용될 것으로 기대한다.

Abstract The amount and diversity of information is increasing, as is the information integration connecting data among the related institutions. In the defense field, DTAQ, which is in charge of the quality of military supplies, is attempting to collect and analyze the information which is related with it. In addition, the object of information integration is to expand civil data as well as defense data. There are many ways to integrate data in various environments. In the defense field, which needs enhanced security, it is necessary to establish and apply the information integration methods which are enhanced with more security. In this study, the framework and architecture of information integration was designed by considering task requirements and security conditions. As a result of example application of this framework for information systems to the selected 4 institutions, it was confirmed that the task can be performed through data connections. From the study result, integration architecture which can be applied securely in defense field was suggested. The data accumulated by using this framework with strengthened security are expected to be utilized for the quality improvement of military supplies.

Keywords : Framework connected information, Information integration, Information Security, Information Sharing, Military supplies, National defense data

*Corresponding Author : Min-Jung Kang(Defense Agency for Technology and Quality)
Tel: +82-55-751-5314 email: mjkang@dtaq.re.kr
Received October 17, 2016 Revised (1st November 8, 2016, 2nd November 9, 2016)
Accepted November 10, 2016 Published November 30, 2016

1. 서론

정보화 시대의 도래에 따라 정보공유의 중요성이 날로 높아지고, 공유된 정보의 활용도 증대되고 있다. 정부에서는 공공과 민간의 데이터를 공유/활용하기 위해 “공공데이터의 제공 및 이용 활성화에 관한 법률”을 제정하였고[1], 정부3.0 추진 전략에서도 정보공유 정책의 개념이 협의의 정보공유를 포함해 시스템 연계 및 통합을 포함하는 광의의 개념으로 확대되고 있으며, 정책의 목적 역시 범정부적 차원의 스마트 정부 구현을 위한 핵심동력으로 초점을 맞추고 있다[2].

전자정부 사업관점에서의 전자정부 발전단계 에 따르면, 개별부처 전산화, 대국민 서비스, 범부처간 연계 순으로 발전단계를 정의하여, 관련 부처 간 연계·통합의 개념은 3단계로 정의하고 있다[3]. 정보공유 및 시스템 연계·통합의 개념을 다시 세분화 하면, 협의의 정보공유(Information Sharing), 시스템 연계(Connectivity of Information System) 그리고 시스템 통합(Integration of Information System)의 세 가지 개념으로 분류된다[4].

또한, 정보시스템 통합을 활성화하기 위한 기술적 방안으로는, 이용자 편의성 제고, 데이터 및 정보시스템의 표준화, 정보보안 및 시스템의 안정성, 그리고 데이터의 신뢰성 확보가 필요하다[5].

국방 분야 역시 임무, 기능 등에 따른 기관 간 해당 정보의 공유 중요성 및 범위가 점차 확대되어 가고 있다. 특히 군수품의 경우에는 품질개선과 생산기술 향상 등을 위하여 품질관련 정보를 수명주기별로 관련 기관으로부터 수집하고 분석·관리하도록 하고 있다[6].

이에 따라 국방 분야 내 관련기관 간의 정보공유는 활발하게 이루어지고 있으나, 민간 분야와의 정보의 수집 및 공유는 보안성 등의 이유로 다소 부족한 실정이다. 특히 군수품의 여러 가지 품질정보 중 시험기관에서 실시하는 군수품의 시험분석 정보는 군수품의 품질 수준으로 판단하는 가장 기본적인 자료로 활용할 수 있다는 관점에서 체계적인 정보의 수집 및 분석이 필요하다[7].

군수품에 대한 정부품질보증을 담당하는 국방기술품질원에서는 시험성적서를 시험기관과 공유하기 위한 정보체계(Test Report Information Service for Military Supplies : TRIS)를 운영하고 있다[8]. 군수품 시험성적서의 위변조 방지를 위해 개발된 이 정보체계는 시험성적서 파일을 관련 기관과 공유하는 기능을 제공하지만, 각 기관에서 독립적으로 운영 중인 정보시스템 내의 데이터까지 연계가 되지 않아 필요한 정보를 별도로 입력하거나, 활용하지 못하는 한계가 존재한다. 따라서 현재의 정보공유의 한계를 극복하고, 관련기관의 데이터를 정보시스템에서 활용하기 위한 국방기술품질원의 TRIS와 시험기관 정보시스템 간 데이터 연계체계가 필요하다[9].

그런데 국방 분야는 민간보다 보안 요구수준이 높으므로 다양한 보안 요구수준 하에서 타 기관과의 시스템 연계 또는 시스템 통합을 해야 하는 한계가 있고, 이에 따라 해결해야 할 기술적인 과제들이 존재한다.

본 논문에서는 정보공유(Information Sharing)에서 시스템 연계(Connectivity and Integration of Information System)로 발전하기 위하여, 국방과 민간 분야 간에 적용할 수 있는 연계모델을 제시하고자 하였다.

연계체계 설계에는 다양한 정보체계 환경에 적용할 수 있는 표준 프레임워크를 설계하는 것과 보안성에 가장 중점을 두었다. 국방 분야에서 외부와의 정보연계 시에는 특히 더 높은 수준의 보안성이 요구되기 때문이다.

본 논문의 구성은 다음과 같다. 2장에서는 데이터 연계에 관련된 이론과 사례를 조사하고, 기관 간 연계의 보안측면의 고려요소를 고찰하였다. 3장에서는 보안성을 강화한 연계 방식과 프레임워크를 설계한 내용을 설명하고, 4장에서는 연계 프레임워크를 국방기술품질원과 시험기관에 실제로 적용한 결과에 대해 설명하였다. 마지막으로 5장에서는 결론 및 향후 연구방향에 대하여 언급하였다.

2. 관련연구

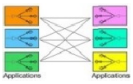
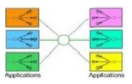
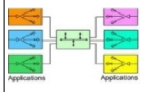
2.1 연계 기술

시스템 통합을 위한 기술로 일반적으로 P2P (Point-to-point), EAI(Enterprise Application Integration), ESB(Enterprise Service Bus) 가 사용된다. 각각의 개념과 특징을 살펴보면 Table 1과 같다[10].

P2P는 개별 시스템 간 1:1 연계로 복잡하지 않은 환경에서 빠른 적용을 할 수 있으나 연계되는 어플리케이션이 추가될 때 마다 개발이 필요하다. EAI는 Hub&Spoke 방식이라고도 하며 중앙허브에서 개별 어플리케이션을 어댑터로 연결하는 형식으로 신규 어플리케이션 추가 시 확장이 용이하나 중앙서버에 부하가 생

길 수 있고, 어댑터 추가에 따른 비용이 발생된다. 마지막으로 ESB는 Bus방식이라고도 하며, 중앙서버에 부하가 없고 표준 통합기술을 이용하여 확장 또한 매우 용이하다.

Table 1. Comparison of Information Integration Technology

Function	Point To Point	EAI (Hub&Spoke)	ESB
Diagram			
Concept	correspondence of multi applications	System integration using adaptors attached each system	bus method to integrate dynamic task process
Feature	difficult to change and reuse	easy to expand and maintain various application	loose coupling using standard integration technology

2.2 연계방식

정보연계 시 데이터 수집의 주체에 따른 연계방식을 Push 방식과 Polling 방식으로 나누어 볼 수 있다.

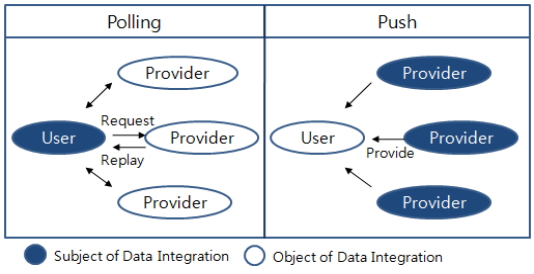


Fig. 1. Comparison of Information Integration Method

Push방식은 정보제공자(Provider)가 정보수요자(User)에게 데이터를 넘겨주는 방식으로 연계의 주체는 정보제공자가 된다. 이 방식은 정보제공자가 연계방식을 주도하기 때문에 제공자 시스템의 성능, 안정성, 보안성이 높다. 그러나 정보수요자 측에서는 정보의 수집/통합이 어렵고, 시스템의 확장성이 떨어지며, 정보수요자 측의 보안성이 떨어지는 문제가 있다.

Polling 방식은 정보수요자가 필요한 시기에 정보제공자에게 요청(접근)하여 데이터를 받아오는(가져오는) 방식으로 연계의 주체는 정보수요자가 된다. 이 방식은 정보수요자가 연계방식을 주도하기 때문에 정보수집이 용이하고 데이터의 즉시성이 보장되지만, 외부에서 정보소스에 직접 접근하는 방식으로 정보제공자 측면에서는 내부 시스템의 운영과 보안을 이유로 선호하지 않는 방식이다[11].

2.3 기관 간 정보연계시스템 사례

기관 간 정보연계시스템의 사례로 국방기술품질원과 타 기관과의 연계시스템을 살펴보았다.

① 국방부는 국방관련 여러 기관들 간의 정보를 효율적으로 연계하기 위하여 P2P 방식의 연계를 사용하며, 각 기관 간에는 데이터 양방향 송신·수신이 모두 지원된다. P2P 방식의 한계인 개별 연계에 따른 통합관리가 어려운 문제를 해결하기 위해, 각 기관 간 데이터 연계현황과 결과를 중앙관리서버에서 통합 관리하여 모니터링 한다[12-13].

② 방위사업청은 국방기술품질원과의 데이터 연계를 위해 ESB Bus방식을 사용한다. 양 기관간 정보시스템의 데이터 연계 요구가 M:N으로 발생되기 때문에 중앙집중형 연계보다는 각 시스템간 연계를 공통 환경으로 지원하는 Bus방식으로 구성되어 있다[14].

③ 조달청은 수십 개의 기관들이 나라장터로부터 정보연계(수신)를 필요로 하기 때문에, 각 기관에 연계용 Agent를 설치하여 나라장터 중앙서버로부터 데이터를 수신하는 Hub&Spoke 기반의 정보제공자 Push 방식의 연계방식을 사용하고 있다.

위의 사례들을 살펴보면, 기관 간 정보 수신의 요구가 양쪽에 모두 있는 경우 P2P 또는 ESB방식이 사용되며, 단방향 송신인 경우 Hub방식이 사용된 것을 알 수 있다.

2.4 보안 고려요소

본 절에서는 국방 분야에 안전하게 적용할 수 있는 연계체계의 설계를 위해 보안측면의 고려요소를 점검하였다. 국방정보체계의 보안 점검요소는 크게 네트워크, 서버/ 데이터베이스, 웹/응용체계, 정보보호체계, 단말기/콘솔 등의 분야로 나누어볼 수 있는데, 이중 기관간 연계체계 운용과 관련된 부분은 DMZ의 설정/운용에 대한 부분을 확인해볼 필요가 있다.

DMZ는 내부 네트워크와 외부 네트워크 사이에 위치

한 부분 망으로 DMZ 내에는 외부 네트워크에 서비스를 제공하는 호스트만 배치하여 외부에서 내부 네트워크 접근 및 공격을 방지하기 위해 설정한다. 외부 서비스를 제공하는 경우 내부 자원을 보호하기 위해 내/외부 서비스 영역 사이에 DMZ를 둔다. 내부 네트워크를 보호하기 위한 설정 및 설치가 올바르지 않으면 내부 네트워크를 보호할 수 없게 된다. 따라서 방화벽 정책설정으로 내부와 외부 영역 사이에 필요한 IP만 접근할 수 있도록 통제함으로써 내부 자원을 외부 침입으로부터 보호하는 것이다[15].

일반적으로 공용영역인 DMZ(Public Zone)에는 외부 서비스를 처리하기 위한 WEB서버를 두고, Private 영역에는 WAS와 DB서버를 두며, 외부 사용자는 공용영역인 DMZ에 있는 WEB서버까지만 접근하고, 서비스는 WEB서버와 WAS간의 통신으로만 제공됨으로서 외부 사용자가 내부서버에 접근할 수 없도록 차단한다.

3. 설계

본 장에서는 정보연계를 위해 일반적으로 사용되는 연계방식의 문제점과 국방 기관에서 민간 기관과의 정보연계시 보안상의 문제점을 살펴보고 이를 개선한 연계방식과 이를 구현한 프레임워크를 설계하였다.

3.1 일반적인 연계방식의 보안 문제점

2.2절에서 살펴본 것처럼, 정보제공자 Push 방식은 정보제공자가 선호하는 방식으로[16] 정보의 수집에 대한 협조가 쉽지만, 이 방식으로 연계할 경우 반대로 정보수요자 측에 보안 취약성 문제가 발생된다. 정보제공자 Push 방식에서 정보수요자 측의 보안 취약성은 정보연계의 객체 측은 정보연계의 주체 서버로부터의 접근을 항상 열어놓아야 한다는 데 기인한다.

또한, 내부와 외부 네트워크가 분리되어 있는 환경에서 일반적으로 정보연계서버는 외부 서버와의 데이터 통신을 위해 DMZ(Public Zone)에 배치되는데, 이러한 경우 정보연계서버가 외부에 노출됨에 따른 보안 위험이 있으며, 이것은 국방 분야에서 권고하는 외부 네트워크 연동통제에 대한 규정에 위배되는 사항이기도 하다[15].

만약 연계기술로 ESB를 사용한다면, 이는 웹서비스 방식을 따르기 때문에 OWASP의 발표[17]에서 보듯이 연계 프로그램이 여러 웹취약점에 노출될 수 있는 위험에 놓여진다. 그리고 웹서비스 메시지의 검증을 수행하는 과정에서도 메시지 내 정보가 노출될 위험도 존재한다[18].

3.2 보안성을 강화한 정보연계 아키텍처

정보제공자 Push 방식에서 나타나는 정보수요자의 보안문제, 그리고 정보연계 서버가 Public Zone에 있을 경우의 보안 문제를 해결하기 위해,본 연구에서는 일반적으로 하나의 서버로 운영되는 연계서버를 외부서비스를 담당하는 서버와 정보연계 처리기능을 담당하는 서버의 두 개로 분리하였다.

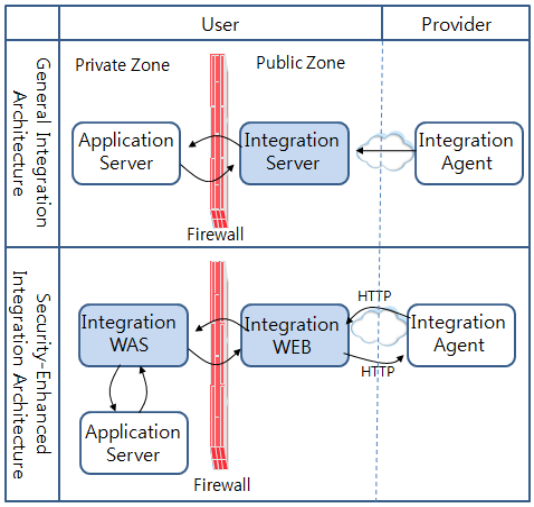


Fig. 2. General and Security-Enhanced Integration Architecture

정보수요자의 Public Zone에는 외부 서비스를 위한 연계용 WEB서버를 배치하고, Private Zone에는 연계용 WAS서버를 배치하며, WEB과 WAS 서버 간에는 방화벽으로 분리된 제한된 통신만을 허용한다. 정보제공자 측에는 정보연계용 Agent를 설치하여 정보수요자의 정보연계WEB서버와 정보를 송수신하도록 하였다. 정보연계용 WEB서버는 연계WAS에 서비스를 전달하는 역할만 수행하고 정보연계 처리 기능은 하지 않는다. 따라서 일반적인 정보연계 프로그램과 같은 데이터 통신기능을 수행할 수 없으므로, 정보연계용 WEB서버가 처리 가능한 HTTP 프로토콜을 이용하여 정보를 전달하도록 설계

하였다.

또한 정보연계용 WEB서버가 정보수요자 측에만 존재하므로, 정보제공자가 정보수요자 쪽으로 단방향 접근 방식으로도 정보연계 서비스를 처리할 수 있도록 하였다.

개선된 아키텍처에서는 외부에 노출되는 프로그램이 최소화되어 보안 위험성을 낮출 수 있게 된다. 일반적 정보연계시스템이 Public Zone에서 수행하던 웹서비스 메시지의 검증 또한, 개선된 아키텍처에서는 Private Zone에서 수행하여 정보노출의 위험을 방지할 수 있다.

송수신 구간의 데이터를 보호하는 방법은 데이터 암호화 또는 SSL(Secure Socket Layer)을 이용한 구간암호화 방법이 있다. 구간암호화 방식은 각 기관에 인증서를 지속적으로 갱신/유지해야 하는 부담이 있으므로, 본 연구에서는 시스템의 운영관리가 편리한 데이터 암복호화 방식으로 설계하였다.

데이터 암호화 알고리즘은 ARIA를 이용하였다. ARIA는 경량 환경 구현을 위해 최적화된 국가표준 블록암호 알고리즘으로[19], 본 연구에서와 같은 경량 연계 프레임워크에 적용하기에 적합하다.

웹서비스의 보안 취약점은 취약점 진단툴을 이용하여 진단하여, 검출된 취약점에 대한 프로그램을 수정보완한다.

새로운 연계방식은 Private Zone에 정보제공자의 접근이 허용되지 않아 국방 분야의 외부 네트워크 연동통제에 대한 보안 요구사항을 충족시키며, 정보수요자 측의 보안성이 유지될 수 있다. 따라서 이 연계방식은 국방분야에서 민간과의 정보연계체계를 구축하는 경우 유용하게 적용될 수 있으며, 특히 보안성의 문제로 정보연계를 기피하는 기관에도 안전하게 적용될 수 있을 것이다.

3.3 데이터 연계 절차

3.2절의 연계 아키텍처에 따른 데이터 연계절차는 Fig. 3과 같다.

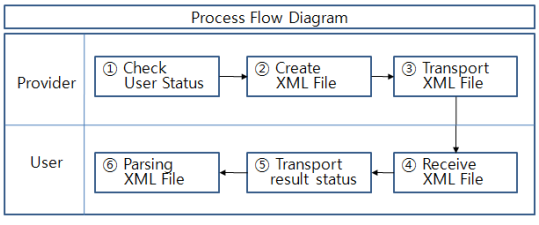


Fig. 3. Process Flow Diagram

① Live 상태 Check : 먼저 수신기관 서버의 상태를 체크한다. 작업시작을 알리는 메시지를 송신하여 수신여부를 회신 받음으로써 수신서버의 Live 상태를 알 수 있게 된다.

② 연계자료 생성 : 송신할 데이터를 DB로부터 추출하고 첨부파일 자료를 합쳐 하나의 XML파일로 구성한다. 데이터는 송신하기 전 암호화 하여 전달한다.

③ 연계자료 송신 : XML파일을 송신기관에서 수신기관으로 전송한다.

④ 연계자료 수신 : 수신기관에서는 송신기관에서 전송한 XML파일을 전달받는다.

⑤ 수신 처리결과 전달 : 데이터 수신처리 결과를 수신기관에서 송신기관으로 전달한다.

⑥ 연계자료 파싱 : 수신된 파일을 복호화 후 XML파일을 파싱하여 DB해당 파일에 입력하고, 첨부파일은 분리하여 응용체계의 해당 위치에 업로드한다.

데이터 연계 중 발생되는 오류는 정보제공자, 정보수요자 양쪽에서 발생될 수 있는 오류를 각각 저장한 후 정보수요자의 서버에 전달하여 오류에 대한 통합관리를 한다. 또한 네트워크 일시단절 등에 대비하여 자동으로 재처리될 수 있도록 하였다.

3.4 연계 프레임워크

3.2의 연계 아키텍처를 구현하기 위한 프레임워크를 설계하였다. 연계 아키텍처의 확장성을 위해, 전달되는 데이터는 공통 포맷인 XML을 사용하였고, 구현하는 프로그램은 JAVA 기반으로 구현하여, 다양한 시험기관의 정보체계 환경에도 적용할 수 있도록 표준화된 시스템을 설계하였다.

프레임워크는 일반적인 EAI 프레임워크의 구조로 구성하였는데, 데이터를 어플리케이션으로부터 데이터를 추출하는 Adapter, 표준 형식으로 가공하는 Broker, 데이터를 수신측으로 전송하는 Messaging과 이를 전체적으로 관리하는 Control&Monitoring으로 이루어진다.

연계 프레임워크 컴포넌트의 구성 및 처리내용은 Table 2와 같다. Adapter 모듈은 응용시스템으로부터 DB와 파일 데이터를 추출하거나, 수신된 데이터를 응용시스템으로 입력하는 기능을 한다. Broker 모듈은 DB 데이터를 XML 포맷으로 변환하고 데이터를 암/복호화하며, DB와 파일 데이터를 XML 파일로 묶어 구성한다.

Table 2. Framework contents of Process

Category		Contents of Process
Adapter	Job Manager	Extract of DB and File Data from Application
		Input of DB and File Data to Application
Broker	XML Manager	DB To XML, XML To DB
		Data Encrypt and Decrypt
		Create XML File from DB and File Data
Messaging	Queue Manager	Create Message Queue Data
	Data Manager	Transport XML File
		Transport repeat of error data
		Transport Result status
Control & Monitor	Scheduler	JOB Scheduler Demon
	Monitoring	List of transported data
		Log of transported data
		List of error data and details of error
		Statistics of transportation result
	Error Check	authentication Error, XML validation check, transportation error, check of Server status
	Controller	Certification of users (create and verify authentication key)
		User Management (Registratiob and update users)

Messaging 모듈은 Queue Manager와 Data Manager로 구성된다. Queue Manager는 전송용 Message Queue를 생성하고 관리한다. Data Manager는 데이터를 송/수신하고 전송결과를 서버로 전송하는 기능을 한다.

Control&Monitoring 모듈은 Scheduler, Monitoring, Error Check, Controller로 구성된다. Scheduler는 송신측에서 일정한 주기로 데이터 송신 처리를 시작시키는 역할을 한다. Monitoring은 전송 데이터, 전송 결과, 전송 이력, 오류내역을 저장하여 사용자가 확인할 수 있도록 한다. Error Check는 송수신 상대의 인증시 오류, 수신된 XML 파일의 유효성, 서버 상태를 체크한다. Controller는 송수신 상대의 인증과 사용자 관리를 한다.

정보연계 프레임워크에는 Spring 경량 컨테이너 프레임워크와 전자정부프레임워크의 라이브러리 중 필요기능들을 활용하여 설계하였다.

4. 구현

본 장에서는 국방과 민간 분야 간 정보연계의 보안성 향상을 위하여 설계한 프레임워크의 구현결과에 대해 설명한다. 연계 프레임워크는 국방기술품질원과 3곳의 시험기관 정보시스템에 적용하였다.

4.1 구현화면

기관 간 데이터 연계결과는 모니터링 시스템을 통하여 확인해 볼 수 있다. 모니터링 시스템은 시스템 관리자를 위한 화면으로, ID와 IP확인을 통해 승인된 사용자만 접근할 수 있도록 하였다. 관리자 모니터링 화면은 사용자 등록/로그인 외 데이터 연계결과, 서버상태 현황, 메시지 연동통계, 성적서 연동통계, 접근이력 메뉴로 구성된다. 관리자 기능의 주요화면들은 그림과 같다. Fig. 4의 화면은 시험기관의 시험성적서 데이터가 연계된 결과를 보여주는 화면으로, 각 기관에서 연동 처리된 결과는 중앙서버에 저장되어, 관리자 화면에서 통합조회해 볼 수 있다. Fig. 5는 상대 서버의 상태를 체크하는 화면으로 버튼을 클릭할 때마다 실시간으로 서버상태 체크결과를 보여준다. Fig. 6은 시험성적서 데이터가 전송된 결과를 일별 통계 그래프로 보여주는 화면이다.

4.2 구현결과

국방기술품질원은 군수품 시험성적서의 위변조 방지를 위해 시험기관과 시험성적서 파일을 공유하는 TRIS 정보체계를 운용하고 있으며, 현재 30여개의 시험기관이 TRIS를 사용하고 있다. 본 연계 시스템은 3개 시험기관에 시범적으로 적용하였는데, 이 시험기관 사용자들은 시험성적서 정보를 자체 정보시스템과 국방기술품질원 TRIS에 두 번 입력하지 않고, 자체 정보시스템에 한번만 입력하는 것으로 작업이 완료되어, 업무 간소화의 효과도 얻을 수 있었다.

5. 결론 및 향후 연구

정보화 시대에 정보공유에 대한 요구증대에 따라, 국방 분야에서도 관련기관과의 정보공유의 중요성 및 범위가 점차 확대되어 가고 있으며, 군수품의 품질개선을 위하여 품질관련 정보를 외부로부터 수집할 필요성이 높아지고 있다.

Fig. 4. The Screen of Transported Data List

Fig. 5. The Screen of Transporting Statistics of Data

Fig. 6. The Screen of Server Status

그러나 국방 분야에서는 민간분야와의 정보연계가 보안상의 이유로 어려움을 겪고 있어, 이에 대한 해결방안이 필요하였다.

본 연구에서는 정보연계와 관련된 연구내용과 기존 운영 중인 사례를 조사하고, 보안 고려요소를 고찰하였다. 또한 기관 간 정보연계시스템에서 가지고 있는 보안성과 확장성의 문제를 개선하여, 안전하고 표준화된 정보연계 방식과, 아키텍처, 그리고 이를 위한 프레임워크를 제시하였다. 그리고 설계된 프레임워크를 국방기술품질원 및 3개 민간 시험기관의 정보체계에 시범적으로 적용하여 기관 간 데이터 연계가 이루어짐을 확인하였다.

본 연구결과로 국방 분야에 안전하게 적용할 수 있는 연계 아키텍처가 제시되었으며, 보안성이 향상된 아키텍처 및 프레임워크는 민간분야에도 활용될 수 있을 것으로 사료된다.

또한 연계 시스템을 적용한 3개 시험기관에서는 중복업무가 방지되는 업무 간소화 효과를 얻을 수 있었으며, 기품원에서는 연계 프레임워크 적용에 따라 수집된 데이터를 군수품 품질향상을 위한 정보로 유용하게 활용할 수 있을 것으로 기대된다.

본 연구에서는 정보시스템 통합을 활성화하기 위한 기술적 방안 중 보안성에 대한 부분을 연구하였다. 향후 연구과제로는 본 연구에서 다루지 않은 시스템의 안정성 측면에서 성능개선을 위한 연구가 필요할 것이다. 현재는 3개 기관과의 연계만 이루어지고 있지만, 향후 연계기관 수가 늘어날 것에 대비하여 시스템 처리 속도 개선과 서버부하 감소를 위한 쓰레드 처리기술 적용 등의 대비가 필요하며, 또한 대용량 자료 전송시 전송중단 문제를 해결하기 위해 전송파일의 압축이나 스트리밍 방식 적용 등에 대한 연구가 필요하다.

References

[1] Ministry of the Interior(Public Service Policy Bureau), “Act on promotion of the provision and user public data”, Act no. 13723, 2016.

[2] Ministry of the Interior(Cooperation of relevant ministries), “Government 3.0 Master Plan”, 2013.

[3] G. H. Wang, “Next generation e-Government created by service users : UCG(User Created Government)”, e-Government Focus [2007], Korean Association for Information Society, no. 07, pp. 69-73, 2007.

[4] M. H. Lee, “Exploring the Influencing Factors on the Effectiveness of Government Information Sharing, Information System Connection, and Information System Integration”, Korean society and public administration 26(2), pp. 25-28, 2015.

[5] M. H. Lee, “Vitalizations of Government Information Sharing, System Connection, and System Integration”, pp. 339-343, Korea Institute of Administration, 2014.

[6] Defense Acquisition Program Administration (Aquisition Policy Division), “Instruction of DAPA No.366”, 2016.

[7] S. Y. Jeon, “A Study on the Application Method of Munition’s Quality Information based on Big Data”, Journal of the Korea Academia-Industrial cooperation Society Vol. 17, No. 6, pp. 315-325, 2016.
DOI: http://dx.doi.org/10.5762/KAIS.2016.17.6.315

[8] Defense Agency for Technology and Quality(IT Planning Department), “TRIS Usage Guide”, 2014.

[9] D. H. Lee, “Study on Test Report Information Service Architecture for Preventing Forgery and Alteration in Defense Industry”, Journal of the Korea Academia-Industrial cooperation Society, vol. 17, no. 4, pp. 43-51, 2016.
DOI: http://dx.doi.org/10.5762/KAIS.2016.17.4.43

[10] S. M. Lee, “University Textbook, Management Information System”, Infodream, 2013.

[11] D. O. Kim, “A Study on the Information Integration Model Based on Standard Integration Framework”, Journal of Korea Institute of Information and Communication Engineering. vol. 18, no. 4, pp. 861-866, 2014.
DOI: https://doi.org/10.6109/jkiice.2014.18.4.861

[12] Ministry of National Defense(Defense Computing Information Agency), “The Standard for Defense Data Integration”, MND, pp. 4-6, 2008.

[13] Korea Institute for Defense Analysis(Defense Information System Management Group), “The Instructions for users of Defense Data Integration Program”, MND, pp. 13-17, 2016.

[14] Defense Agency for Technology and Quality (Technology Intelligence Division), “Methods for upgrading data integration DTAQ and DAPA”, pp. 9-13, 2015.

[15] Ministry of National Defense(Cyber Command), “General Guideline for weakness analysis and evaluation in National defense Information System”, 2016.

[16] H. S. Choi, “Design of a NTIS Information Integration Model based on a Standard Integration Platform”, Journal of KIISE : Computing and Letters 18(6), pp. 484-488, 2012.

[17] The Open Web Application Security Project, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project, 2016.

[18] S. H. Lee, “A Security Enhancement Method for Web Service”, The Journal of Digital Policy & Management 11(12) : 361-366, 2014.

[19] Korea Internet and Security Agency, Domestic Code Dissemination : ARIA : https://seed.kisa.or.kr/iwt/ko/sup/EgovAriaInfo.do, 2016.

강 민 정(Min-Jung Kang) **[정회원]**

- 1993년 2월 : 덕성여자대학교 전산학과 (이학사)
- 2014년 2월 : 한성대학교 국방과학대학원 국방경영학과 (경영학석사)
- 1993년 4월 ~ 현재 : 국방기술품질원 선임연구원

<관심분야>
정보경영, 정보통합, 품질정보