Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.6, Dec. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.6.1225

정보 유출 방지를 위한 보안 컨테이너의 효과성 연구

이 종 식,† 이 경 호‡
고려대학교 정보보호대학원

A Study on Security Container to Prevent Data Leaks

Jong-shik Lee,† Kyeong-ho Lee‡
Korea University, Graduate School of Information Security

요 약

고객정보 유출 방지를 위해 금융기관은 DLP(Data Leaks Prevention) 관련 정보보호 제품을 도입하고 내부통제 정책을 강화하고 있다. 그러나 정보의 수집, 제공, 이용, 저장 과정의 핵심적 역할을 담당하는 응용프로그램에 대한 관리 및 기술적 통제는 매우 미흡한 실정이며, 응용프로그램을 통한 정보유출 사고를 예방하거나 대책 마련을 위한 내부통제 정책의 이행에 어려움을 겪고 있다. 본 논문에서는 금융기관의 개인정보 취급 및 주요 유통 경로 현황 분석을 통해 문제점을 제기하고 정보유출 방지를 위한 효율적인 내부통제 보안기술의 필요성을 제시하였다. 이에 따라 가상화 및 모바일 분야에서 부분적으로 사용되고 있는 컨테이너 기술을 응용하여 클라이언트 PC 응용프로그램의 보안 취약점을 보완하고 정보유출 방지 기능을 제공하는 새로운 보안 컨테이너를 설계 구현하였으며, 실제 금융기관 업무시스템에 적용하여 정보유출 방지 및 IT 컴플라이언스 내부통제와 관련된 정책 수행능력의 효과성을 검증하였다. 또한 정책 설정을 통해 보안 컨테이너에 추가 보안 기능을 제공하고 보안 컨테이너를 재사용함으로써 보안 취약점 대응 비용 및 시간을 줄여 IT 컴플라이언스 규제 준수를 위한 보안 컨테이너의 효용 가치를 높였다.

ABSTRACT

Recently, Financial companies implement DLP(Data Leaks Prevention) security products and enforce internal controls to prevent customer information leaks. Accidental data leaks in financial business increase more and more because internal controls are insufficient. Security officials and IT operation staffs struggle to plan countermeasures to respond to all kinds of accidental data leaks. It is difficult to prevent data leaks and to control information flow in business without research applications that handle business and privacy information. Therefore this paper describes business and privacy information flow on applications and how to plan and deploy security container based OS-level and Hypervisor virtualization technology to enforce internal controls for applications. After building security container, it was verified to implement internal controls and to prevent customer information leaks. With security policies additional security functions was implemented in security container and With recycling security container costs and time of response to security vulnerabilities was reduced.

Keywords: Data Leaks, Container, Security Container, Virtualization, Internal Controls, IT Compliance

I. 서 론

1.1 연구 배경 및 목적

2014년 국내 은행 및 카드사의 대규모 고객정보 유출사고로 인해 위험관리와 내부통제에 대한 중요성

접수일(2014년 11월 4일), 수정일(2014년 11월 28일), 게재확정일(2014년 12월 1일)
† 주저자, warning0@korea.ac.kr
‡ 교신저자, kevinlee@korea.ac.kr(Corresponding author)

이 증가하고 있다. 금융기관은 2011년 3월 금융감독원이 권고한 「금융회사의 정보통신 수단 등 전산장비 이용관련 내부통제 모범규준」을 참고하여 근무여건, 영업환경 등 제반사항을 감안하여 내부통제 수단을 자율적으로 마련하여 시행해왔다. 그러나 금융감독원은 최근의 고객정보 유출사고가 금융기관의 내부 보안통제 미흡에 기인한 것으로 판단하고 그 동안 권고에 머물렀던 금융권 정보보호 강화 대책을 법제화하여 법적 구속력을 강화시키고 있다. 이에 따라 금융기관은 정보보호 강화를 위해 정보보호 시스템 및 포인트 보안 솔루션을 구축하고 정보보호 운영을 체계적이고 지속적으로 유지하기 위한 정보보호관리체계(ISMS) 인증 제도를 도입하여 IT 인프라의 안전성과 신뢰성을 확보하고자 노력하고 있다. 이러한 노력의 일환으로 네트워크 보안, 시스템 보안, 컨텐츠/정보유출 방지 등의 정보보호 시스템에 대한 투자가 꾸준하게 이루어지고 있지만 내부자에 의한 정보 유출 사고는 지속적으로 증가하고 있는 추세이다[1].

Table 1.은 기업 내 중요 기밀 정보 유출사고의 90% 이상이 내부자가 관여되어 있다는 연구 조사를 정리한 것이다[2].

기존 정보보호 인프라의 보안 사각지대로 알려져 있는 내부자 또는 권한을 가진 사용자들에 의한 정보 유출을 효과적으로 통제하려면 정보를 수집, 제공, 이용, 저장하는 응용프로그램 및 데이터 중심의 보안 기능을 강화해야 하며, 비즈니스 업무처리 효율성과 편의성을 손상시키지 않는 IT 기술의 도입을 고려해야 한다[3].

가트너(Gartner)는 CMF&DLP (Contents Monitoring and Filtering & Data Loss Provention)로, IDC(Internet Data Center)는 SCM(Supply Chain Management)으로 내부정보 유출방지 시장을 규정하고 있으며 응용프로그램 및 데이터 중심의 새로운 보안 제어 기술의 필요성을 제기하여 왔다. 2013년 2월 가트너는 '기업 데이터 관리 및 보안을 위한 모바일 응용프로그램 컨테이너 기술 개요(Technology Overview of Mobile Application Containers for Enterprise Data Management and Security)' 라는 보고서를 통해 응용프로그램 및 데이터를 격리시키는 보안 컨테이너의 필요성을 제시하고 있다[4].

Table 1. The Persons concerned Business and Privacy Information(Allow Multi-answer)

Retired Employees	Employees	Partner's Employees	Competitor's Employees	etc
62.9 %	23.5 %	23.5 %	9.9 %	3.8 %

본 논문에서는 가상화 및 모바일 분야에서 활용되기 시작한 컨테이너 기술을 이용하여 클라이언트 PC에서 실행되는 업무용 응용프로그램을 격리시키고 IT 컴플라이언스 규제준수 및 내부통제의 효율적인 이행과 정보유출을 사전에 방지할 수 있는 클라이언트 보안 기술을 제안하고 리얼 테스트를 통해 효과성을 검증하였다. 또한 내부정보 유출방지를 위해 보안 컨테이너를 다른 응용프로그램에 재사용하고, 일관성 있는 정책 기반 운영 및 중앙 관리 기능을 구현하여 취약점 발견 시 신속한 대응 능력으로 정보유출 위험을 줄이고자 한다.

1.2 논문 구성 및 리얼 테스트 환경

본 논문의 서론에서는 연구 배경 및 목적, 논문의 구성 및 리얼 테스트 환경을 다루었으며, II 장에서는 A금융기관의 사용자 PC 내에 보관되어 유통되고 있는 개인정보 현황을 조사하고, 주요 유통 경로 분석을 통해 정보 유출 취약점을 제시하였다. 또한 실제 적용중인 IT 내부통제(ITGC: IT General Control) 항목과 정보보호관리체계(ISMS)와의 통제 항목 매핑을 통해 IT 내부통제 범위의 특징과 자율적이고 지속적인 통제 항목 추가와 준수를 위한 기술적 통제의 필요성을 제시하였다. III장에서는 보안 컨테이너의 필요 기술요소를 제시하고, 보안 컨테이너의 설계 및 구현 모델을 제안하였다. 또한 보안 담당자와 시스템 운영자 및 관리자를 대상으로 FGI(Focus Group Interview)를 통해 A금융기관의 보안 컨테이너 관련 보안 요구사항의 우선순위를 분석하고, 보안 컨테이너 재사용을 통한 정보유출 방지 대응 비용편익을 분석하였다. 마지막으로 IV 장에서는 결론 및 향후 연구 방향에 대하여 기술하였다.

본 논문에서 사용된 "보안 컨테이너" 용어는 클라이언트 PC에서 실행되는 응용프로그램을 격리시키기 위해 사용된 "가상화 컨테이너"와 정보유출 방지 기능과 같이 데이터를 안전하게 관리하기 위해 적용시킨 보안 모듈들의 집합을 가리킨다.

본 논문의 보안 컨테이너 구성에 사용된 보안 모듈은 A금융기관의 클라이언트 표준 PC 환경에 맞추어 Microsoft Windows 7 32 bit용으로 제작되어 운영 중인 기존 보안 응용프로그램을 일부 수정하여 재

Table 2. Security Components in Security Container

Categories	Components	Dev.
Identification and Authentication	Kerberos Clients Module	Reuse
	NTLM Client Module	Reuse
	Certificate Client Module	Reuse
Encryption and Decryption	AES 128 Module	New
	AES 256 Module	New
	DES Module	New
	3-DES Module	New
Logging and Monitoring	Logging Module	New
	Monitoring Agent Module	Reuse
ETC	Anti-Virus Client/Server Module	Reuse
	Client Information Detection Client/Server Module	Reuse
	DRM Client/Server Module	Reuse

사용하였다. Table 2.는 실증적 테스트 환경 구현을 위해 보안 컨테이너 설계 및 개발 시 사용된 보안 모듈 목록이다. 보안 컨테이너 운영 정책에 따라 변경되어야 하는 암호화 및 로깅 모듈은 새롭게 구현되었으며, 인증 모듈 및 안티-바이러스 모듈, 고객 정보 검출 모듈, DRM(Digital Rights Management) 모듈은 기 도입되어 사용되고 있는 보안 응용프로그램을 사용하였다.

A금융기관의 리얼 테스트 환경을 위해 보안 컨테이너를 구성하고 응용프로그램의 리소스 사용을 제어하기위해 "OS-레벨 가상화"를 의미하는 협의적 컨테이너 기술과 "하이퍼바이저" 기반의 가상화를 의미하는 광의적 컨테이너 기술을 함께 연구하였다. OS-레벨 가상화 컨테이너 기술은 Docker라는 이름으로 Linux 운영체제 전용 솔루션으로 제공되고 있으며,

Table 3. Client SW for Container's prototype

Virtualization	Component	Product
Container Based Hypervisor	Guest OS	Microsoft Windows 7 32 bit
	Virtualization S/W	Virtual Box
	Host OS	Microsoft Windows 7 32 bit

Microsoft는 2014년 10월에 Windows를 위한 Docker의 공식 지원을 선언했다[5]. 따라서, 본 논문의 실증을 위해 A금융기관의 표준 업무환경인 Windows 환경을 고려하여 하이퍼바이저 기반의 광의적 컨테이너 운영 환경을 구성하였다.

Table 3.은 컨테이너의 프로토타입 설계 및 개발을 통해 실증적 테스트를 위해 사용된 소프트웨어 목록이다. 호스트 OS와 게스트 OS에는 Microsoft Windows 7 32 bit가 사용되었으며 가상화 응용프로그램에는 Virtual Box가 사용되었다.

1.3 선행 연구

내부 정보유출방지와 관련된 선행 연구자료를 조사한 결과 가상화 솔루션의 보안 취약점 및 대응 방안, 가상화 솔루션의 효율적 자원 활용 및 성능 부문의 연구, 정보유출방지와 관련된 다양한 기술에 대하여 연구된 사례는 다수가 있으나, 본 논문처럼 가상화 기술을 이용한 가상화 컨테이너를 구성하여 응용프로그램을 격리시키고, 보안 솔루션(또는 기능)을 융합하여 IT 컴플라이언스 및 다양한 보안 요구사항에 대응한 선행 연구 사례는 존재하지 않는다. 따라서 본 논문의 기반이 되는 가상화 및 컨테이너, 정보유출방지와 관련된 주요 기술의 특징 및 차이점을 설명하였다.

1.3.1 가상화와 컨테이너

Fig.1.은 전통적인 가상화 솔루션의 기반 기술을 제공하는 하이퍼바이저 기술을 사용한 컨테이너 구성도이다. 하이퍼바이저 기술은 CPU, 메모리, 스토리지 등 모든 컴퓨팅 스택을 가상화하고, 여러 하드웨어를 추상화하여 거대한 자원으로 만든 뒤 용도별로 공간을 분할하는 방식을 사용한다. 일반적인 하이퍼바이저 가상화 솔루션은 서버상의 운영체제 및 응용프로그램 운영 환경을 가상화한다. 컨테이너는 서버에서 실행되는 것이 아니라 클라이언트 PC에서 실행되므로 네트워크를 통해 컨테이너 서버에서 컨테이너 클라이언트로 컨테이너 전체 이미지를 이동시킬 때 네트워크 트래픽 및 시스템 자원이 과다 사용되는 문제가 발생할 수 있다[6].

Fig.2.의 OS-Level 가상화는 전통적인 하이퍼바이저와 달리 운영체제 커널 공간을 공유하고 사용자 프로세스를 실행하는 사용자 공간의 리소스를 분할

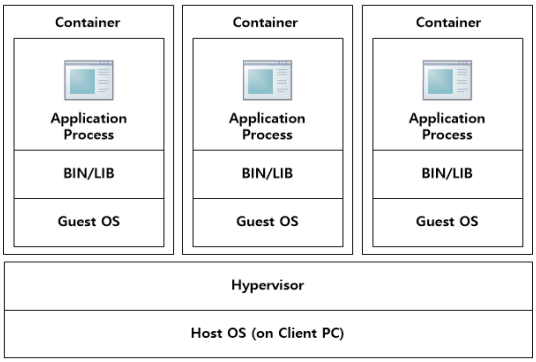

Fig. 1. Traditional virtualization and paravirtualization require a full operating system image for each instance.

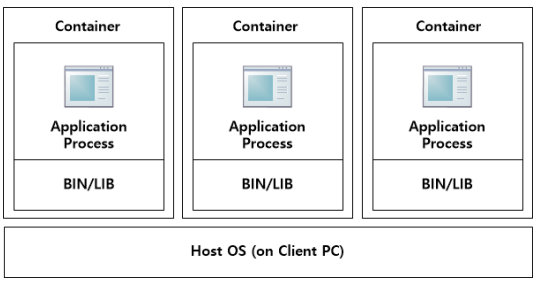

Fig. 2. Containers can share a single operating system and, optionally, other binary and library resources.

격리시켜준다. OS-Level 가상화 기술을 이용한 컨테이너는 CPU, 메모리, 스토리지, 네트워크 등의 자원을 가상으로 할당받으며 다른 컨테이너에 할당된 자원과 철저히 격리된다[6]. 컨테이너는 네트워크를 통해 서버에서 서버, 서버에서 클라이언트로 전달될 수 있다.

응용프로그램을 위한 컨테이너는 서버에서 작성되고 클라이언트로 배포되어 실행되기 때문에 컨테이너의 크기를 줄일 수 있는 OS-Level 가상화가 최적의 솔루션으로 평가받고 있다. 그러나 현재 OS-Level 가상화 컨테이너 기술(Docker)은 Linux 전용 솔루션으로써 Windows 응용프로그램에 적용시킬 수 없다는 문제가 있다. 따라서, Windows 응용프로그램을 위한 컨테이너를 구성할 때는 Hypervisor 가상화를 이용하여야 하므로 컨테이너의 경량화에 따른 클라이언트 시스템 자원(CPU, 메모리, 네트워크) 배분 및 사용에 주의해야 한다.

1.3.2 정보 유출 방지 기술

내부정보 유출 방지를 위해 사용하고 있는 기술은 Data in Motion, Data at Rest, Data at Endpoint, Database Security로 구분할 수 있다[7].

Data in Motion 보안은 네트워크를 통해 유출되는 정보 보안 기술로서 NDLP(Network Data Loss Prevention)라고도 한다. 일반적으로 침입탐지시스템(IDS)과 침입방지시스템(IPS)처럼 스니핑 또는 인라인 방식으로 동작하며, 감사기능, 관리자의 정책에 따라 통신을 허용 또는 차단하는 기능을 제공한다. Data in Motion 보안 기술은 투자 비용에 비해 그 효율이 떨어진다는 평가를 받고 있다. 랜덤 포트를 사용하거나 포트를 변경하는 프로토콜을 사용하는 서비스나 RFC를 따르지 않는 비표준 프로토콜을 사용하는 서비스의 경우는 리버스 엔지니어링을 수행해야한다. 또한 서비스에 따라 전송방식과 유출 경로가 다양하며 대부분의 서비스가 우회 포트로 80 포트를 사용하고 있기 때문에 대응에 어려움이 있다.

Data at Rest는 PC나 서버에 저장되어 있는 정보에 대한 보안을 의미하며, 정보에 대한 식별, 중앙관리, 필요에 따라 데이터 암호화 기능을 제공한다. 지원 파일 포맷이 다양해야 하며 패턴/키워드 추가 및 편집 기능, 메일 분석 기능, 암호화 강제 기능, 강제 삭제 기능, 중앙 관리 기능 등이 제공된다[8].

Data at Endpoint는 네트워크 이외의 유출 경로에 대한 보안을 의미한다. 일반적으로 USB/CD 등 외부 저장 매체와 프린터를 통한 유출 방지 기술이 이 부류에 속한다.

Database Security는 주요 정보를 대량으로 저장 관리하는 데이터베이스와 관련된 것이다. 개인정보 마스킹 기능, 작업 전후 정보 비교 기능, 중요정보 조회시 결재 기능 등이 있다.

본 논문에서 제안한 보안 컨테이너는 Table 4.와 같이 정보 유출 방지 기능을 제공하는 다양한 보안 모듈의 탑재가 가능하다.

II. 보호대상 정보의 취급 현황 및 분석

2.1 개인정보의 보관 및 유통 현황

금융기관의 대부분 업무는 개인정보를 매개로 하여 운영되고 있으며 고객에게 제공하고 있는 금융 서비

Table 4. Security Container's DLP Technologies

Category	Function	Security Container Module
Data in Motion	Prevention data leakage on network (NDLP) - uditing packet - grant/prohibit communication with policies	- Host Firewall - Network Monitor (Sniffing Tool)
Data at Rest	- support various file format - add and edit pattern/keyword - analysis mail - force encryption - force delete - analysis encrypted file - central admin	- DRM - Privacy Detector - Encrypt & Decrypt - Anti Virus
Data at Endpoint	- prohibit USB/CD and external mass storage - prevention data leak with printer	- Remove or disconnect external mass storage - Remove or disconnect printer
Database Security	- masking about privacy - compare result after work and before - approvals access on important information	- Control or approval database access

스의 특성상 신용 및 금융거래에 수많은 개인정보를 취급 및 활용하고 있다. 따라서 금융기관의 정규직, 비정규직, 하도급, 시간제 등의 근로 형태를 불문하고 금융기관 임직원 모두 개인정보 취급자라고 할 수 있다. Table 5.는 망분리, 고객정보탐색 솔루션, DRM(Digital Rights Management), NAC (Network Access Control), Anti Virus 등이 적용된 A금융기관의 특정 부서를 대상으로 개인정보 보관 현황을 조사한 것이다. 직접식별 개인정보인 주민번호 1개 이상 또는 모바일 번호 2개 이상 포함된 파일을 탐색 대상으로 설정한 결과이다.

Table 6.는 Table 5.에서 검출된 파일내용을 분석하여 주요 패턴별 분류한 정보 건수이다

Table 5. Customer Informations in Client PC

Month	Number of Files (ea)		
	Customer Info. (Plain Text)	Customer Info. (Cipher Text)	Total
2014.4	16	2,485	2,501
2014.5	68	2,271	2,339
2014.6	6	2,100	2,106
2014.7	0	924	924
2014.8	4	323	327
2014.9	18	322	340

Table 6. Customer Informations Pattern

Month	Pattern (ea)		
	Korean SSN	Mobile Phone	Total
2014.4	1,256	10,389	11,645
2014.5	9,313	12,651	21,964
2014.6	3,563	14,278	17,841
2014.7	1,167	18,255	19,422
2014.8	2,179	48,230	50,409
2014.9	4,389	11,902	16,291

Table 7. Customer Information Flow Channel

Channel	Pattern (ea)		
	Korean SSN	Mobile Phone	Account Number
Web Mail	4,239	34,083	7,198
Internal Mail	107,930	59,239	44,509
Messenger	256,045	3,851,164	548,562
Total	368,214	3,945,006	600,269

Table 7.은 2014.4.1.~2014.09.30 까지 임직원이 주로 사용하는 응용프로그램을 대상으로 개인정보 유통 현황을 조사한 결과이다.

본 조사결과에 의하면 메일, 메신저 등을 이용하여 개인정보가 유통되고 있음을 확인 할 수 있었다. 이와 같은 조사결과는 임직원 PC 내에 보관 중인 개인정보가 메일, 메신저와 같은 응용프로그램들을 이용하여 유출될 가능성이 높다는 것을 시사한다.

2.2 IT 내부통제 현황

A금융기관은 개인정보 유출을 방지하고 정보보호

부분에 대한 내부통제 강화요구를 만족시키기 위해 “정보통신망 이용촉진 및 정보보호 등에 관한 법률” 제47조(정보보호관리체계의 인증)에 따라 2013년 2월에 의무화된 ISMS(정보보호관리체계) 인증을 획득했다.

A금융기관의 SOX ITGC(전산부문 통제절차)는 업무 프로세스 중심의 통제절차에 초점을 맞추고 있으며, 전사적 수준 통제절차 34개 항목과 전산일반통제 33개 프로세스, 293개 통제절차 항목으로 구성되어 있다. 이에 비해 ISMS는 정보보호 부문별 필수 점검사항과 관련하여 정보보호 관리 5개 과정, 12개 부문, 28개 통제절차와 정보보호 대책 13개 과정, 92개 부문, 225개 통제절차로 구성되어 있다. 결과적으로 A금융기관은 ISMS 보다 더 많은 통제 항목으로 SOX ITGC 기반의 내부통제를 시행하고 있음에도 불구하고 내부정보 유출과 관련된 크고 작은 보안 사고를 겪고 있는 상황이다.

Table 8.과 같이 A금융기관이 운영 중인 COSO Framework의 SOX ITGC 중 약 66%에 해당하는 통제절차가 ISMS의 통제 항목과 중복 및 대체 가능하며 금융기관 자체적으로 지속적인 통제 항목을 선정하여 제도화를 통해 IT 컴플라이언스 준수를 강화할 필요가 있다.

Table 8. SOX ITGS and ISMS

Classific-ation	Secu-rity	Oper-ating	Cha-nge	Deve-lop	Total
SOX ITGC	104	106	34	49	293
ISMS Replac-eable controls	95% (99)	64% (68)	35% (12)	30% (15)	66% (194)

2.3 내부정보 유출 취약점 대응 현황

Table 7.에서 조사된 것처럼 A금융기관의 내부정보 유통에 가장 많이 사용되고 있는 응용프로그램은 다양한 운영 환경의 솔루션 및 장비들이 결합되어 운영되고 있는 통합 커뮤니케이션 시스템이다[9][10]. Table 9.는 A금융기관에서 사용하고 있던 통합 커뮤니케이션 시스템의 메일 및 메신저 관련 업무시스템 보안 점검 결과 중에서 정보 유출 사건을 유발할 수 있는 보안 취약점을 정리한 것으로 보안

Table 9. Unified Communication System Security Vulnerability Corresponding Case

Asset	Vulnerability Item	Day	M/M
Internal mail	Attachment file (malware)	169	4
	SQL syntax inject exist	15	1
Messen-ger	Employee personal information exposed through a network packet	332~	3
	Possibility of data collection of organization chart information and employee information	332~	4
	Leakage of password authentication	332~	3
	accessible when ID/PW exposed	332~	1
	Can be connected using a long-term leave of absence administrator account	332~	2
	Due to insufficient external personnel management, retirement accounts exist	155	1
	Personal information / customer information distribution through the messenger	332~	2
	Encryption is not applied of when Transmission attachment file between internal and affiliates	155~	3
	Possibility of malware distribution when the note is sent	332~	3
	Abuse of the remote function of messenger	332~	3
	Note and File transfer function encryption transmission insufficient	332~	4

취약점 대응을 위한 실제 소요일수 및 개발인력을 산출한 것이다. 정보 유출 보안 사고를 유발할 수 있는 대부분의 보안 취약점은 정보의 유통 채널 보다는 서비스 별 서버 및 클라이언트 응용프로그램에서 발견되고 있다는 것을 알 수 있다. 일부 보안 취약점은 기술적 문제 및 소요예산 등으로 취약점 발견 후 1년 가까이 대응하지 못하고 있는 상황이다.

2.4 현황 분석을 통한 취약점 분석 결과

2.1, 2.2, 2.3의 현황 조사결과를 살펴보면 정보 유출 방지를 위한 포인트 솔루션만으로 정당한 인가

자에 의한 정보유출 보안 취약점을 제거하는 것은 한계가 있다. 특히 금융기관의 지주사 및 계열사, 공공기관 및 일반기관, 협력사가 함께 사용하는 응용프로그램을 통한 자료 유출 위험은 상존 및 증가하고 있는 상황이다.

A금융기관이 가지고 있는 정보유출 관련 취약점을 정리한 결과는 다음과 같다. 첫째, 응용프로그램을 통한 개인정보 취급 통제가 방치되어 있어 내부 자 및 보안 수준이 낮은 계열사 및 관계사를 통한 유출 가능성이 존재한다. 둘째, 응용프로그램을 통해 유통된 파일은 보호되지 않고 있으며, 유통 경로 추적이 어렵다. 셋째, 정보보호관리체계(ISMS) 인증 획득이 IT 컴플라이언스의 보안 부문과 95% 매핑 되지만 IT 컴플라이언스 준수를 위한 내부통제 부문은 기업의 운영환경에 적합하도록 자율적인 통제 정책을 강화할 필요가 있다. 넷째, 응용프로그램에 대한 보안 취약점 발견 후 소요예산 및 개발 난이도에 따라 대응기간이 길어져 정보유출 위험이 증가하고 있다. 다섯째, 응용프로그램의 본문 또는 첨부파일을 통한 악성코드가 유입될 경우 APT 공격 및 사회공학적 공격의 기반이 될 수 있다.

III. 보안 컨테이너 실증

3.1 컨테이너에서 보안 컨테이너로의 확장 적용

본 연구에서 컨테이너는 통제 대상이 될 응용프로그램의 "격리 환경"만을 제공한다. 격리 환경이란 컨테이너에 등록되는 응용프로그램이 정책적으로 허용된 시스템 자원과 네트워크 기능만을 사용할 수 있다는 것을 의미한다. 응용프로그램들이 송수신하는 모든 데이터들은 컨테이너에 격리되어 저장되며 반출 승인 프로세스를 거쳐야만 컨테이너 외부 환경으로 반출시킬 수 있다.

컨테이너를 보안 컨테이너로 확장시키기 위해서 컨테이너 가상화 표준을 작성하고 기업 내 기사용중인 보안 관련 시스템(인증, 키 관리, 파일 저장, 파일 전송, 암호화/복호화, 동기화 등의 API 제공)의 SDK(Software Development Kit)를 이용하여 보안 구성요소를 준비하여야 한다. 이 응용프로그램은 보안 모듈들과 함께 보안 컨테이너에 담겨져 클라이언트 PC에 배포된다. 기존 업무용 응용프로그램들은 이 SDK를 이용하도록 수정하고 재 컴파일 한다. 금융기관 대부분의 업무용 응용프로그램은 In-House 방식으로 개발되고 있으므로 보안 컨테이너 표준이 정해지면 신규 서비스들은 보안 컨테이너 SDK를 이용해 개발하고, 기 개발되어 사용 중인 업무용 서비스들은 후킹 및 래핑 기술을 통해 호환성을 제공하도록 한다.

3.2 보안 컨테이너 구성 요소

보안 컨테이너는 사용 용도에 따라 다양한 형태로 구성할 수 있다. 본 연구에서는 Table 10.처럼 용도별로 응용프로그램 컨테이너, 데이터 컨테이너, 커넥션 컨테이너로 구성하였다.

사용되는 가상화 솔루션에 따라 클라이언트 PC에서 실행되는 보안 컨테이너를 다양한 형태로 구성할 수 있다. OS-Level 가상화를 사용할 경우는 컨테이너에 하나의 프로세스만을 격리시킬 수 있으므로 Fig.3.처럼 프로세스별 컨테이너를 만들고 컨테이너 사이의 통신과 입출력을 정책으로 제어해야 한다.

Hypervisor 가상화 솔루션을 사용할 경우는

Table 10. Security Container's Type

Type	Role
Application Container	Isolate application (cpu, memory function)
Data Container	Serve data storage (storage function)
Connection Container	Serve connection (network function)

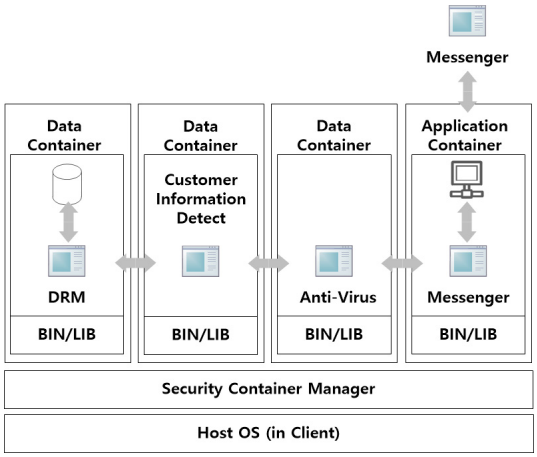

Fig. 3. Security Container with OS Level Virtualization

Fig. 4.처럼 응용프로그램들이 공용으로 사용하는 데이터 컨테이너를 생성하고 데이터 가공, 처리에 필요한 보안 모듈을 적용할 수 있다.

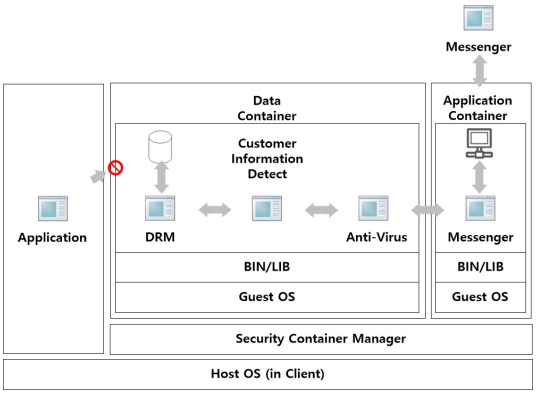

Fig. 4. Security Container with Hypervisor

3.2.1 보안 컨테이너 클라이언트 구성요소

Fig.5.는 본 연구에서 사용된 하이퍼바이저 기반의 보안 컨테이너 클라이언트 구성요소의 도식이다.

① 보안 컨테이너 관리자(Security Container Manager)는 클라이언트 PC에 설치되어 응용프로그램에 격리(isolation) 환경을 제공하며 응용프로그램의 실행 및 관리 역할을 담당한다. 보안 컨테이너 관리자는 보안 정책에 따라 클라이언트 PC에 다운로드된 보안 컨테이너의 운용을 담당한다.

실행 가능한 응용프로그램, 기업 기밀 데이터 및 개인 데이터가 보안 컨테이너 내부에 잠겨 있게 되므로 악성 프로그램이나 개인 응용프로그램의 위험한 상호 작용을 차단시키고 다른 사용자가 응용프로그램

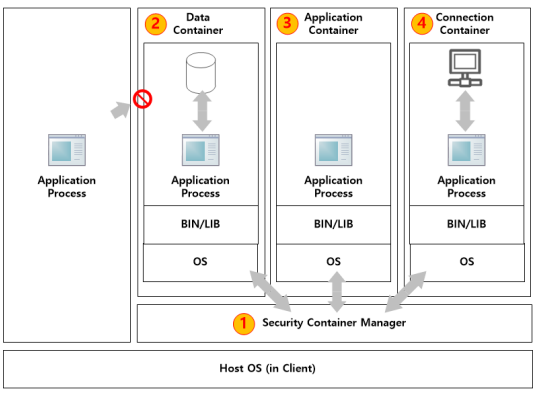

Fig. 5. Client Component of Security Container

및 데이터를 공유하지 못하도록 하는 보안 정책을 적용하였다.

② 데이터 컨테이너(Data Container)를 사용하여 업무용 응용프로그램이 유통하는 민감한 데이터를 안전하게 저장, 관리할 수 있도록 하였다. 데이터 컨테이너에 DRM 클라이언트, 고객정보탐지 클라이언트, 안티바이러스 소프트웨어들을 배치하였다. 컨테이너 정책을 통해 데이터 컨테이너를 구성하는 보안 솔루션의 활성, 비활성 상태를 설정하도록 하였다. 컨테이너 외부에서는 보안 컨테이너의 데이터에 액세스할 수 없으며, 정책적으로 허용된 보안 컨테이너 내의 응용프로그램이 데이터에 액세스하려면 기 구축되어 있는 LDAP, Kerberos, 보안 토큰 기반 또는 인증서 기반의 인증서비스를 통해 사용자 인증을 받도록 하였다. 데이터 컨테이너로 전송되어 온 데이터는 고객정보 탐지 프로세스와 악성코드 및 안티바이러스 검출, DRM 프로세스를 차례로 거친 후, 보안 컨테이너 자체 암호화 프로세스를 통해 AES-256으로 암호화 하였다. 데이터를 암호화할 때 사용된 대칭형 암호화 키는 사용자의 공개키를 이용해 암호화되어 키 관리 서버에 저장되도록 하였다.

③ 응용프로그램 컨테이너(Application Container)에는 전용 SDK를 이용해 개발된 응용프로그램과 기개발되어 운영되고 있는 업무용 응용프로그램이 등록, 저장, 관리되도록 하였다. 전용 SDK를 이용해 개발되어 컨테이너에 저장되어 있는 업무용 응용프로그램은 응용프로그램 컨테이너를 통해서만 실행되며, 사용자 인증, 데이터 암호화, 데이터 백업 제한 등의 컨테이너 사용 정책을 적용하였다. 컨테이너 내의 응용프로그램에서 발생하는 모든 이벤트는 응용프로그램 컨테이너에 기록하고 서버와 동기화하여 관리자 콘솔에서 조회를 통해 보안 위반 사항들을 추적 가능하도록 하였다.

④ 커넥션 컨테이너(Connection Container)는 통합 커뮤니케이션과 같은 다양한 업무 시스템과 인터페이스 역할을 수행하도록 하였다. 사용자들이 커넥션 컨테이너에 등록된 업무시스템에만 접속할 수 있도록 업무시스템 접속정보 및 식별, 인증 정보를 암호화하여 보관, 관리하도록 하였다. 커넥션 컨테이너에 화이트리스트/블랙리스트 정책을 적용하여 사용자의 타 업무시스템 접근을 제어하도록 했다.

본 연구에서 사용된 보안 컨테이너 사이의 통신은 Zhiyong Shan의 Facilitating Inter-Application Interactions for OS-level Virtualization 을

참조하여 구현하였다[11]. 응용프로그램 컨테이너(Application Container)는 응용프로그램이 정보를 생성, 가공, 저장할 때는 해당 응용프로그램 컨테이너를 이용하거나 데이터 컨테이너의 저장 공간을 이용하도록 하였다. 본 연구에서는 DRM, 고객정보 탐지, 안티바이러스용 전용 데이터 컨테이너를 구성하고 API를 제공하여 응용프로그램 컨테이너(Application Container)내의 응용프로그램은 이 API를 사용하도록 하였다.

3.2.2 보안 컨테이너 서버 구성요소

본 연구에서 보안 컨테이너의 정보 유통을 통제하기위해 사용된 서버 구성 요소는 Fig.6.와 같다.

① 인증 및 키 관리(Authentication/Key Management) 서비스는 기 도입되어 사용하고 있는 인증 방식을 사용하고, 사용자 인증 및 사용자별 컨테이너 키 관리 기능을 제공하도록 하였다. 사용자는 표준 인증 절차를 거쳐 암호화된 자신의 보안 컨테이너를 열 수 있는 키를 얻는다.

키를 얻은 사용자는 클라이언트 PC에 암호화되어 저장되어 있는 응용프로그램을 실행시키거나 데이터에 액세스할 수 있도록 하였다.

② 컨테이너 서버(Container Server) 서비스는 클라이언트 PC에 생성되어 운영되는 사용자들의 컨테이너와 동기화되는 컨테이너를 서버에 저장, 관리하도록 하였다. 보안 컨테이너에 암호화되어 저장 관리되는 데이터들이 이동되는 경우는 통신 채널의 종류에 상관없이 모든 데이터(사용자들의 대화 내용, 대화상대 정보, 연락처 정보, 업무용 메시지, 메일, 첨부파일 등)가 암호화되어 송수신 된다. 보안 컨테이너 영역에서 보안 컨테이너 외부 영역으로의 데이터 복사가 일어나는 경우는 승인 절차를 거치도록 하였다.

③ 로그 서버(Log Server)는 사용자의 서비스 및 데이터 액세스 행위 이력을 남겨 모니터링 및 감사에 사용하도록 했다. 보안 컨테이너에 등록된 응용프로그램을 통해 유통되는 모든 데이터의 로그 관리 및 통계 기능을 이용하여 보안 감사, 정보 유출, 개인정보의 불필요한 이용 등을 감시하는 기능을 추가하였다. 또한, 데이터 및 사용자와 관련된 이벤트를 일정 기간 축적하여 악성코드의 전파 및 유통 경로를 추적할 수 있는 기능을 제공하도록 하였다.

④ 관리 및 보안정책 서버(Management and Policy Server)는 관리 및 보안 정책을 변경하여 컨테이너 사이의 통신을 제어하고 응용프로그램 서비스 및 보안 모듈을 변경하거나 보안 수준의 조정 등 신속하게 보안정책을 적용할 수 있도록 하였다. 보안정책의 범위는 비즈니스 및 정보보호 부서의 담당자 요구사항을 고려하여 기업의 환경에 적합한 보안 정책을 수립 적용할 수 있는 관리 기능을 제공할 수 있도록 했다. 또한 업무 형태가 서로 다른 계열사 및 부서, 직무, 직책에 따른 보안 정책 설정이 가능하도록 고려했다.

3.3 보안 컨테이너 워크플로우

Fig.7.는 보안 컨테이너의 워크플로우를 시퀀스 다이어그램으로 표시한 것이다.

사용자가 보안 컨테이너 클라이언트를 실행시키면 보안 컨테이너 관리자를 통해 로그인 프로세스가 시작된다. 사용자 인증이 성공하면 사용자에게 할당된 보안 컨테이너(응용프로그램 컨테이너, 데이터 컨테이너, 커넥션 컨테이너)가 클라이언트 PC로 다운로드 된다. 로컬 클라이언트 PC에 컨테이너의 공통 이미지가 존재할 경우는 서버에서 제공하는 이미지와 다른 부분만을 다운로드하게 된다. 컨테이너 전체 이

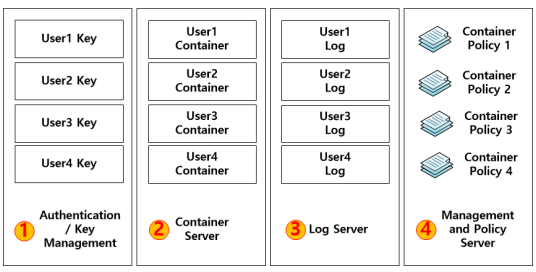

Fig. 6. Server Component of Security Container

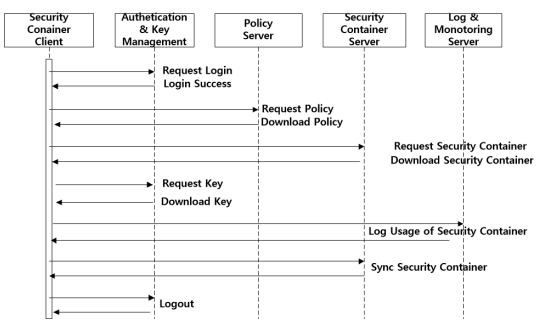

Fig. 7. Summary of Security Container's Workflow

미지가 다운되지 않으므로 네트워크 이동 트래픽은 최소화된다.

컨테이너가 성공적으로 다운로드되면 사용자는 컨테이너 암호화에 사용된 암호화키에 액세스할 수 있다. 이 암호화키는 사용자의 공개키로 암호화되어있으므로 개인키를 이용해 암호화되어있는 컨테이너 암호화키(AES 256 대칭키)를 복호화 한다. 이 키는 보안 컨테이너 복호화에 사용된다.

보안 컨테이너 내의 응용프로그램은 자동 실행되며 보안 컨테이너에 로그인할 때 사용된 인증 정보를 이용해 응용프로그램에 자동 로그인된다. 사용자가 다른 프로세스들과 격리된 공간(컨테이너)에서 응용프로그램을 사용하여 데이터를 등록, 수정, 삭제, 저장하는 액션을 취하면 정책에 따라 자동으로 데이터 컨테이너로 데이터가 넘겨진다. 데이터 컨테이너로 넘겨진 데이터는 정책에 따라 고객정보 검출, 안티바이러스 및 악성코드 체크 등의 절차를 거쳐 데이터 컨테이너에 대칭키로 암호화되어 저장된다. 데이터와 관련된 모든 액션은 정보유통 이력 서버에 기록된다.

사용자가 응용프로그램에서 로그아웃하고 해당 컨테이너를 종료하면 데이터 컨테이너의 컨텐츠 변경사항이 서버로 전송된다. 응용프로그램 컨테이너의 변경사항은 서버로 전송되지 않는다. 또한 정책을 적용시켜 로컬 클라이언트 PC에 저장되어있는 암호화된 컨테이너들을 자동 삭제시킬 수 있다.

3.4 보안 컨테이너의 정책 설정

본 연구의 리얼 테스트를 위해 A금융기관에서 운용중인 통합 커뮤니케이션 도구인 Microsoft Lync 2010을 대상으로 보안 컨테이너를 적용하고 다양한 보안 정책을 설정하였다.

Fig.8.와 Fig.9.는 정책 설정을 통해 업무 시스템 보안 컨테이너와 관련된 응용프로그램의 기능을 제한하는 예이다. 프로토타입 구축 시에는 커넥션 컨테이너 정책에 따라 메신저 응용프로그램 UI 및 기능이 확장, 변경되도록 했다.

Fig.8.은 보안 컨테이너에 담겨져 있는 메신저 응용프로그램과 연동된 다른 응용프로그램(메일, 전자결재, 화상회의, FAX, 쪽지 등) 접속권한과 관련된 정책 설정 화면이다. A금융기관의 경우 계열사별로 커넥션 컨테이너의 정책을 설정했다. 정보유출 방지를 위해 반드시 필요한 기능만을 정책 통제할 수 있도록 하였다.

Fig. 8. Policies for Messenger Client Application Security Container

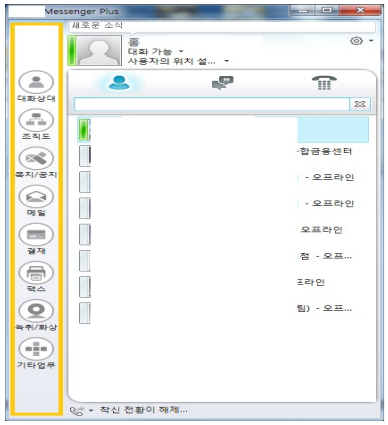

Fig. 9. Example of Security Container(Before apply policy to connection container)

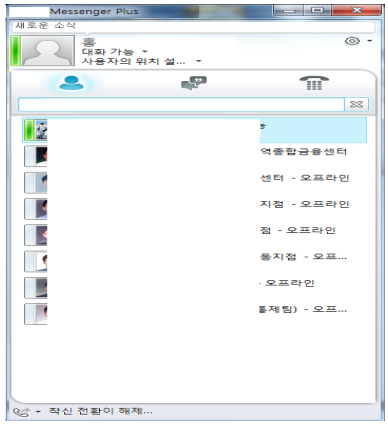

Fig. 10. Example of Security Container(After apply policy to connection container)

Fig.9.와 Fig.10.는 커넥션 컨테이너의 사용권한 설정 정책을 통해 사용자들이 사용하는 응용프로그램의 접근 UI를 통제하는 예이다.

3.5 보안 컨테이너의 효과성

3.5.1 고객정보 유출 탐지 및 통제

보안 컨테이너의 정보유출 방지 효과를 측정하기위해 개인정보를 자주 취급하는 주요 부서 사용자의 메신저와 통합 커뮤니케이션 응용프로그램에 보안 컨테이너를 6개월간 테스트 적용하였다. 보안 컨테이너에 적용된 정책은 Table 11.과 같으며, 리얼 테스트 운영기간 동안 인사발령 등 기타 사유로 정책 적용에 예외가 발생된 사용자의 데이터는 결과에서 제외하였다. Table 12.는 그 결과를 정리한 것이다.

Fig.11.은 리얼 테스트 기간중의 정보 유통 결과를 정리한 것이다. 2014.04.01. ~ 2014.06.30. 까지는 보안 컨테이너 정책을 고객정보 유무 탐지(통제 제외), 고객정보 평문 전송 허용, 악성코드 탐지 정책이 적용되었으며, 2014.07.01. ~ 2014.09.30. 까지는 고객정보유무 탐지(탐지 내용 팝업 표시 및 예외 승인 정책 포함), 고객정보 평문 전송 불가(서버 암호화), 내부 근무자중 외부인력 및 계열사 전송 시 승인 프로세스, 보안 컨테이너에서 외부로의 승인 프로세스 등의 정책을 적용하였다. 정책 적용 전후의 차이점을 정리하면 첫째, 통제 정책으로 고객정보의 유통량이 감소하였다. 둘째, 고객정보의 평문 전송이 제어되었고, 필요시 승인프로세스로 처리되었다. 셋

Table 11. Applied Security Container Policies

Policy	Period	
	Before (2014.04 ~06)	After (2014.07 ~09)
Detect Customer Information on application registration and download	O	O
Encrypt Customer Information		O
Allow Transfer Customer Information with Plain Text	O	
Allow Transfer Customer Information with Approval Process to Partner Employees		O
Allow Transfer Customer Information with Approval Process to Other Companies		O
Allow Transfer Customer Information with Approval Process to External Container		O
Detect Malware and Prohibit Transfer	O	O

Table 12. Customer Information Detection Results

Category	Apr	May	Jun	Jul	Aug	Sep
Customer Information	1195	1254	1220	902	616	614
Customer Information CyperText	1052	1120	1140	902	616	614
Transfer PlainText	143	134	80	7	2	9
Approval Transfer (Allow Exception within Company)	0	0	0	59	50	111
Approval Transfer to Non Employee	0	0	0	140	114	138
Approval Transfer to External Container	0	0	0	7	6	10
Detection Malware	2	2	2	0	0	2

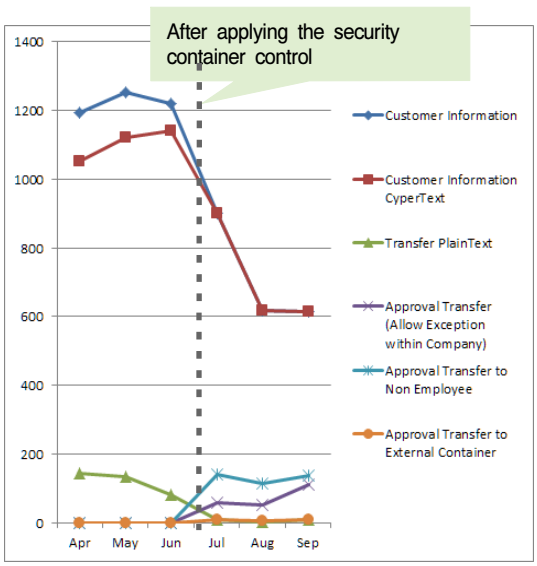

Fig. 11. Security Container's Policies Effective Analysis

째, 고객정보의 승인절차를 통한 정상적인 유통이 증가하였다. 넷째, 보안 컨테이너는 고객정보의 흐름을 실시간으로 탐지할 수 있도록 해주었다. 또한, 개인정보취급자에 대한 보안인식 강화 및 규제 준수에 추가적인 효과가 있음을 확인 할 수 있었다.

3.5.2 FGI(Focus Group Interview)를 통한 보안 컨테이너 적용의 효과 검증

IT 컴플라이언스 준수를 위해서는 비즈니스 활동을 지원하는 정보처리 시스템과 디지털 데이터에 대한 규제가 필수적으로 요구된다. 규제 주체, 적용 범위(지리/산업별)로 다양한 IT 컴플라이언스들이 존재하고 있다. 그러나 IT 컴플라이언스의 규제 준수에 대한 객관성 , 공정성, 정확성을 제공하는 체계적인 평가 지표의 연구는 아직 미흡한 상황이다.

Table 13.은 보안 컨테이너의 고유한 기능이 각 영역의 IT 컴플라이언스 통제 정책 수행 능력을 충족시키는 지를 보안 전문가와 응용프로그램 운영 및 관리자들이 평가한 결과이다. 평가지표 도출 범위는 정보보호 및 개인정보보호 분야를 대상으로 하였으며, 식별 및 인증 항목 총 15개, 기밀성과 무결성 항목 총 9개, 접근제어 항목 총 11개, 악성코드 통제 항목 총 6개의 통제 지표가 선정되었다. 지표에 대한 타당검증은 "기업의 정보보호 및 개인정보보호 컴플라이언스 평가 지표에 관한 연구(김영태)" 연구 자료를 참고하였다.

보안 컨테이너에 대한 평가 참여자는 보안 담당자와 응용프로그램 운영 및 관리자 30명을 대상으로 하였으며, 평가 지표의 항목별 평가 빈도 분석을 통해 항목별 응답율을 추출 하였다. 평가에 참여한 보안 전문가 및 시스템 운영자들은 식별 및 인증 영역에 대해서는 97.1%, 기밀성과 무결성 영역에 대해서는 98.1%, 접근제어 영역에서는 95.3%, 악성코드 및 바이러스 영역에 대해서는 86.7%의 IT 컴플라이언스 통제항목 정책 수행 능력을 충족한다는 평가를 내렸다. 또한, 90.0%의 응답자가 보안 컨테이너를 보안 관련 업무에 적용할 의향이 있다는 긍정적인 반응을 보였다.

보안 컨테이너가 사용자 식별 및 인증을 위한 보안 솔루션이 아니기 때문에 기 도입되어 있는 식별 및 인증 솔루션과의 호환성 및 유연성을 강력하게 요구하였으며, 악성 코드 감염, 전파와 관련된 근본적인 대책(응용프로그램 및 데이터 격리)을 제공하지만 PC에 설치된 안티바이러스 솔루션과 컨테이너에 적용하는 안티바이러스 솔루션은 서로 다른 제품을 사용해야 한다는 권고를 받았다.

3.5.3 보안 컨테이너에 대한 보안요소 우선순위 분석

A금융기관의 보안담당자와 응용프로그램 운영 및 관리자들이 어떤 보안적인 요소에 우선순위를 두고 보안 컨테이너를 평가했는지 분석하기 위해, {식별 및 인증 기능, 기밀 및 무결성 기능, 접근제어 기능, 악성코드 대응 기능}을 독립변수로 지정하고 {보안 컨테이너 적용 우선 순위}를 종속변수로 지정하여 상관관계를 분석하였다. 독립변수와 종속변수의 상관관계를 분석하기위해 IBM SPSS Statistics 21 통계 소프트웨어가 사용되었으며 범주형 회귀분석을 수행하였다.

Fig.12.는 SPSS Statistics 21 범주형 회귀분석 결과의 일부분이며, 중상관계수(=다중 R)과 결정계수(R^2)가 1에 가까우면 가까울수록 회귀식의 적합도가 좋다고 볼 수 있다. FGI(Focus Group Interview)의 결과는 다중 R값과 R 제곱 값이 1이므로, 수정된 R 제곱 값도 1 이 되어 회귀식이 통계적으로 가치가 있음을 의미한다.

분산 분석은 다음의 귀무가설을 검정하고 있다.
"귀무가설 H_0 : 관계식은 예측에 도움이 되지 않는다."

Model Summary

Multiple R	R Square	Adjusted R Square	Apparent Prediction Error
1.000	1.000	1.000	.000

Dependent Variable: Security_Priorty
Predictors: Identification_Authentication Confidentialty_Integrity Access_Control Protection_Malware

ANOVA

	Sum of Squares	df	Mean Square	F	Sig.
Regression	30.000	8	3.750	806261.349	.000
Residual	.000	21	.000		
Total	30.000	29			

Dependent Variable: Security_Priorty
Predictors: Identification_Authentication Confidentialty_Integrity Access_Control Protection_Malware

Fig. 12. Categorical Regression of FGI(Focus Group Interview) Result

Table 13. FGI(Focus Group Interview) Result on Security Container

Category	Internal Controls		Compliance		
			Good	Normal	Bad
Identification and Authentication	1.	Security Container for Identification and Authentication	15	14	1
	1.1	Authentication(Certification Token, Certificate, ID/PW, OTP etc)	15	14	1
	1.2	Prohibit Multi Login	14	15	1
	1.3	Manage Password	15	14	1
	1.4	Limit Authentication Number	10	18	2
	1.5	Logout After x times	18	10	2
	1.6	Prohibit common account and virtual account	18	12	
	1.7	Prohibit bypass authentication path	15	15	
	1.8	2-Factor Authentication	15	15	
	1.9	Lockout user account	15	10	5
	1.10	Manage external human resource life-cycle	10	20	
	1.11	Manage retired human resource life-cycle	10	20	
	1.12	Manage internal human resource life-cycle	10	20	
	1.13	Manage Mobile Authentication and device	9	21	
	1.14	Manage access log	18	12	
	Response Rate		**46.0%**	**51.1%**	**2.9%**
Confidentiality and Integrity	2	Security Container's Confidentiality and Integrity	27	2	1
	2.1	Encrypt communication	27	3	
	2.2	Encrypt message and attachment file	29		1
	2.3	Encrypt client env. file	29		1
	2.4	Encrypt client application	29	1	
	2.5	Encrypt ID/Password	29		1
	2.6	Use Verified Encryption Algorithm	27	3	
	2.7	Prohibit exposure of client source	28	2	
	2.8	Access control and encrypt to log	20	9	1
	Response Rate		**90.7%**	**7.4%**	**1.9%**
Access Control	3	Security Container's Access Control	28	1	1
	3.1	Service Access Control with user rights	29		1
	3.2	Use stop word and spam flitering	15	10	5
	3.3	Administrator Access Control to Application	28	2	
	3.4	Detection and Control on privacy	26	4	
	3.5	Approval process for privacy information	28	2	
	3.7	Logout after x times	28	2	
	3.8	File transfer control between companies	28	2	
	3.9	Control mess message transfer	27	2	1
	3.10	Manage access log	10	14	6
	Response Rate		**82.3%**	**13.0%**	**4.7%**
Malware	4	Security Container's abilities to malware	17	9	4
	4.1	Prohibit modification of identification information	28	2	
	4.2	Detection mail ware code and script in message body	10	20	
	4.3	Detection mail ware code/ spyware/virus	20	10	
	4.4	cross site scripting(XSS)	9	1	20
	4.5	Monitoring and tracing log	14	16	
	Response Rate		**54.4%**	**32.3%**	**13.3%**
Are you willing to apply security container to work process?			**22**	**5**	**3**
			73.3%	**16.7%**	**10%**

유의확률이 0.000 으로 유의수준 0.05보다 작으며, 검정통계량 (=F)이 자유도 (8, 21)의 F 분포에 대한 기각역에 포함되므로, 귀무가설 H_0는 기각된다.

따라서, Fig.13.과 같이 베타 표준화 계수를 바탕으로 다음 상관 관계식이 통계적으로 의미를 가지게 된다.

보안 컨테이너 적용 우선 순위= 0.312 X (식별 및 인증 기능) + 0.598 X (기밀 및 무결성 기능) + 0.654 X (접근제어 기능) + 0.001 X (악성코드 대응 기능)

Coefficients

	Standardized Coefficients				
	Beta	Bootstrap (1000) Estimate of Std. Error	df	F	Sig.
Identification_Authentication	.312	.186	2	2.821	.082
Confidentialty_Integrity	.598	.324	2	3.410	.052
Access_Control	.654	.202	3	10.452	.000
Protection_Malware	.001	.001	1	.854	.366

Dependent Variable: Security_Priorty

Fig. 13. Categorical Regression Parameters of FGI(Focus Group Interview) Result

A금융기관의 보안 담당자와 응용프로그램 운영 및 관리자들은 보안 관련 업무를 위한 보안 솔루션을 도입할 때 베타 값이 높은 {접근제어 기능} 및 {기밀 및 무결성 기능} 이 우선 순위가 높았다. 즉, FGI 분석 결과에 따르면 {접근제어 기능}, {기밀 및 무결성 기능}, {식별 및 인증 기능} 순으로 보안 컨테이너 적용 우선 순위의 종속변수에 영향을 주는 것으로 나타났다. 이에 비해 {악성코드 대응 기능}은 보안 컨테이너 적용 우선 순위의 종속변수에 별다른 영향을 미치고 있지 못한 것을 알 수 있다.

3.5.4 정보유출 방지 대응 비용편익 분석

본 연구에서 제안한 보안 컨테이너는 다양한 응용프로그램을 위해 사용될 수 있다. 보안 컨테이너의 정보기술 아키텍처는 재사용성이 뛰어나며, 비즈니스 업무처리 목적에 따라 응용프로그램에 적용되어야하는 다양한 보안 정책의 수준을 지원한다. 보안 컨테이너는 간단한 코드 추가 작업을 통해 보안 모듈의 보안강도를 높여 재개발 비용 및 시간을 줄일 수 있다는 장점을 제공한다.

보안 컨테이너의 재사용에 따른 비용 효과 및 개발 시간 절감의 측정 방법은 2003년 한국전산원에서 진행한 '정보기술 아키텍처 사례분석을 통한 효과측정 모델 연구 (A study on the effectiveness measurement model through analyzing the cases of Information Technology Architecture)'의 측정방법을 이용하였다[12].

Table 14.는 A금융기관의 통합 커뮤니케이션 시스템을 위한 보안 컨테이너 개발 시 영역별 소요된 개발 인력을 정리한 것이다. 보안 컨테이너 개발은 기술의 난이도에 따라 평균적으로 고급 개발자 19 M/M 가 참여하여 약 3개월에 걸쳐 개발하였다.

보안 컨테이너 개발을 위해 산정된 비용은 다음과 같다.

- 고급기술자 노임단가(월) : 13,436,136 원 (2013년 기준)
- 총 소요비용: 255,286,584 원
  - 소요비용: 개발소요인력(M/M) * 노임단가(월)
- 재사용 가능한 응용프로그램 : 96개(A금융기관 기준)

재사용성은 보안 컨테이너를 다른 응용프로그램에서 사용함으로써 얻는 근본적인 이익이다. 보안 컨테이너에 대한 재사용 가능 개발비용과 재사용 개발비용 이익은 다음과 같이 산출한다[12].

재사용가능 보안 컨테이너의 개발비용 = 보안 컨테이너의 개발비용 / 보안 컨테이너의의 재사용 갯수

재사용가능 보안 컨테이너의 개발비용 이익 = (보안 컨테이너의 재사용 갯수 - 1) * 보안 컨테이너의 개발비용

- 재사용가능 보안 컨테이너의 개발비용
  - 재사용 개수 96개 기준 : 2,659,235 원
- 재사용 가능 보안 컨테이너의 개발비용 이익
  - 재사용 개수 96개 기준 : 24,252,225,480 원

A금융기관의 재사용 가능한 응용프로그램의 수량은 업무처리시스템을 제외한 관리자에 의한 정보제공유형과 쌍방향 커뮤니케이션 응용프로그램을 모두 산정한 것이다. 위의 산출된 비용은 시스템간이나 플랫폼이 동일한 서비스 수준으로 산정하였으며 부가세 등 기타 부

Table 14. Costs and Men Days of Security Container

Categories	Components	Dev. M/M	Dev. days
Container	Container	2	40
Identification and Authentication	Kerberos Clients Module	2	20
	NTLM Client Module	2	20
	Certificate Client Module	2	20
Encryption and Decryption	AES 128 Module	1	10
	AES 256 Module	1	10
	DES Module	1	10
	3-DES Module	1	10
Logging and Monitoring	Logging Module	2	40
	Monitoring Agent Module	2	40
ETC	Anti-Virus Client Module	1	20
	Client Information Detection Client Module	1	20
	DRM Client Module	1	20
Total		19	280

대비용은 반영하지 않았다.

금융기관마다 다소 플랫폼이나 시스템간의 호환성 문제로 다소 비용적인 차이는 발생할 수 있지만 재사용을 통한 비용편익이 높은 것은 효과성이 매우 크다는 것을 시사한다.

금융기관이 정보유출 취약점 발견 후 신속한 대응이 반드시 필요하지만 기술적 난이도, 소요예산, 개발 및 도입 시 소요되는 기간에 따라 수개월간 취약점을 안고 있을 수 밖에 없다.

따라서 인지된 취약점을 안고 대응기간이 길어질수록 정보유출 위험은 가중 될 수 있다. 취약점에 대한 신속한 대응은 위험을 제거하거나 감소시킬 수 있으므로 매우 중요하다. 96개의 응용프로그램에 보안 컨테이너를 재사용 시 개발시간 절감효과는 다음과 같이 산출한다[12].

- 재사용 보안 컨테이너 개발시간 : 504 시간
  - 개발 소요 기간 : 3개월
  - 월 근무 일수 : 21일 기준
  - 1일 근무 시간 기준 : 8시간
- 보안 컨테이너 생성을 위한 인스턴스 재사용율
  - 보안 컨테이너 재사용을 위해 인스턴스 프로그램 변경 없이 재사용율을 20% 산정
- 재사용 가능한 응용프로그램 :96개(A금융기관 기준)

$$T = ((D/8) * (1 - R) * N) - D$$

- T : 절약한 시간
- R : 보안 컨테이너 생성을 위한 인스턴스 재사용율(프로그램 변경 없이 보수적으로 계산하여 20% 재사용 기준)
- N : 보안 컨테이너 재사용된 갯수
- D : 재사용 가능한 보안 컨테이너 개발 시간

※ 1 개의 응용프로그램에 한해 8 개의 재사용 가능한 보안 컨테이너(서버 및 클라이언트)를 갖는다고 가정함(리얼 테스트에 적용된 컨테이너 수량임)

- 보안 컨테이너 개발시간 절감 : 4,334 시간
  - 1일 8시간 기준으로 약 541 일 절감

위의 산출된 결과는 응용프로그램 96개에 보안 컨테이너를 재사용 할 경우 실제 개발소요 기간보다 541일을 절감하는 효과를 가져 온다는 의미이다. 응용프로그램이 장기간 보안 취약점을 안고 있는 경우 보안 컨테이너를 재사용함으로써 신속하게 대응할 수 있다. 따라서 새로운 보안 취약점 발견 시 보안 컨테이너에 대한 추가 보안기능과 이를 재사용하여 비용 및 개발 기간을 절감할 수 있다.

IV. 결론 및 향후 계획

금융기관은 정보 유통 단계에서 정보 취급자의 고의 또는 실수에 의해 정보가 유출될 수 있는 보안 위협을 항상 가지고 있다. 또한 IT 컴플라이언스와 관련된 이슈는 지속적으로 증가하는 추세이며, 이에 대한 효과적인 대응책을 마련하지 못하고 있는 실정이다. 특히 정보유출 방지 솔루션 및 정보보호 인프라가 구축되어있다 하더라도 내부자 및 인가자에 의한 개인정보 수집, 제공, 이용, 저장과 관련된 응용프로그램의 통제가 미약한 상태이다.

본 논문에서 제시한 보안 컨테이너의 기술은 응용프로그램 격리를 통해 개인정보를 보호하고, 사용자가 정보 취급 과정 중 개인정보를 탐색하여 이를 사용자에게 경고함으로써 정상적인 승인 프로세스를 통한 정보의 반출 및 반입을 유도한다. 이에 따라 개인정보의 취급 현황이 실시간으로 파악되어 정보유출의 위험을 사전에 예방할 수 있다. 또한 개인정보의 일반 평문 전송을 강제적으로 암호화하고, 계열사 및 관계사에 개인정보 전송 시 사전 승인 프로세스 과정을 추가하여 고의 및 실수에 의한 정보유출을 방지하고 업무용도 외의 개인정보 오남용 여부 등을 판단할 수 있다.

보안 담당자 및 시스템 운영자의 평가를 통해 보안 컨테이너의 기술이 IT 컴플라이언스의 보안 요구사항을 만족시킬 수 있음을 검증하였고, 리얼 테스트 운영을 통해 개인정보 거래 건수가 약 50% 이상 감소되었으며, 정상적인 통제절차에 의한 거래량이 증가되어 보안 컨테이너의 정보 유출 방지 효과를 실증하였다. 또한 상관관계 분석 결과 금융기관에서의 보안 컨테이너 적용 우선 순위는 접근제어 기능, 기밀 및 무결성 기능, 식별 및 인증 기능, 악성코드 대응 기능의 순서로 나타났으며 금융기관의 자율적 내부통제 목표에 따라 비용 편익 및 효과성을 고려하여 적용 순서를 선택할 수 있다. 그리고 정보유출 위험도가 높은 응용프로그램을 대상으로 보안 컨테이너를 재사용하는 경우 개발 비용 편익을 증대시키고 개발 시간을 크게 감소시킬 수 있다는 결론을 얻었다.

보안 컨테이너의 정보유출 방지 기능은 매우 우수하다. 그러나 보안 컨테이너를 실제 업무 환경에 도입하기 위해서는 네트워크 속도, 사용자 PC의 사양, 가상화의 다양한 운영체제 지원 등이 선제적으로 해결되어야 한다. 최근 Docker를 이용한 OS 레벨 가상화를 지원하겠다는 Microsoft의 공식 발표로 인해 컨테이너 기술의 다양한 활용 방안들이 선을 보일 것이다. 향후 보안 컨테이너 기술을 각 금융기관의 플랫폼 환경에 최적화하기 위한 연구와 표준화 노력을 통해 다양한 응용프로그램이 지원되도록 지속적인 연구가 진행되어야 한다. 이러한 노력은 효과적인 금융기관의 IT 컴플라이언스 규제 준수를 강화시키는데 크게 기여할 것이다.

References

〔1〕 Security World, "IT Security Trend for Prevention of Internal Data Leaks," Monthly Security World No. XIV Section 203

〔2〕 Jeong Byeong-Il, "A Study for Preventing Industrial Technology Leakage in Enterprise," The Journal of Korean Association for Industry Security, Vol.1, No.1, pp. 4-5, Dec. 2009.

〔3〕 Jong In Im, "Trend of Information Environment and Countermeasure to Information Leaks," Korea University, pp. 20-31, Oct. 2011.

〔4〕 Gartner, "Technology Overview of Mobile Application Containers for Enterprise Data Management and Security," pp. 1-11, Feb.2013.

〔5〕 Microsoft, "Docker and Microsoft partner to bring container applications across platforms," http://news.microsoft.com/2014/10/15/dockerpr/

〔6〕 Kong Jae Hee, "Secure Full-Virtualization Scheme Using OS-level Virtualization Method," M.S, Sungkyunkwan University Department of Digital Media and Communications Engineering, April. 2013.

〔7〕 CONCERT:CONsortiumCert, "Security Consumer Report - DLP," 2014.

〔8〕 Hangbae Chang, Sang-Soo Yeo, Cilcheol Park and Changhoon Lee, "The Study on Development of Document Security Components," Journal of Security Engineering, Vol.5, No.2, Apr. 2008.

〔9〕 Jin-hyung Kim and Hyung-Jong Kim, "A Study on the way for Handling for Personal Information Protection considering the Scale and Characteristic of Companies Status," Journal of Security Engineering Vol.9, No.1, Feb. 2012.

〔10〕 Jeong Han Kim, In Hyuck Kim and Chang Woo Min, "Trend of Mobile Virtualization Technology," Communications of the Korean Institute of Information Scientists and Engineers, Vol.28, No.6, pp. 35-52,

Jun.2010.
〔11〕 Zhiyong Shan, Xin Wang, Tzi-cker Chiueh and Xiaofeng Meng, "Facilitating Inter-Application Interactions for OS-level Virtualization," Key Laboratory of Data Engineering and Knowledge Engineering (Renmin University of China), MOE, Stony Brook University, Industrial Technology Research Institute
〔12〕 Lee Tae Gong, "A study on the effectiveness measurement model through analyzing the cases of Information Technology Architecture," National Information Society Agency, NCAIV-RER-03061, pp. 119-132, Nov. 2003.

〈저자소개〉

이 종 식 (Jong Shik Lee) 정회원
1992년 2월: 강원대학교 전자공학과 학사
1994년 9월~ 현재: KB국민은행 근무
2013년 3월~ 현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 금융포렌식, 침해사고대응, 보안개발방법론, 정보보호 및 개인정보보호정책

이 경 호 (Kyung Ho Lee) 종신회원
1989년 8월: 서강대학교 수학과 학사
1997년 8월: 서강대학교 정보통신대학원 석사
2009년 8월: 고려대학교 정보보호대학원 박사
1994년 2월~현재: 삼성그룹, 네이버(주), 시큐베이스 등 근무
2011년 9월~현재: 고려대학교 정보보호대학원 조교수
〈관심분야〉 위험관리, 정보보호컨설팅, 정보보호 및 개인정보보호정책