정 보 보 호 학 회 지
제26권 제3호, 2016. 6

금융권 망분리 현황과 망분리 정책 개선에 대한 고찰

박 지 윤*, 정 윤 선**, 이 재 우***

요 약

최근 금융IT를 대상으로 한 사이버 공격이 지속적으로 증가되고 있어 금융 정보와 관련된 개인정보유출 및 금융전산망의 마비에 대한 우려의 목소리가 커지고 있다. 이에 따라 금융위원회에서는 「금융전산 보안강화 종합대책」을 발표하며 금융IT에 대한 보안대책의 일환으로 금융전산망에 대한 분리를 의무화시켰다. 하지만, 망분리 정책 실시 이후 금융회사들은 업무 환경과 맞지 않은 일부 규정들로 주요 업무 처리에 대한 어려움을 호소하였다. 이에 금융위원회에서는 금융회사의 업무의 연속성과 투명성을 보장하기 위해 망분리 예외기준을 마련하였다. 본 논문에서는 금융권 망분리의 동향을 살펴보고 망분리 예외기준과 관련하여 신설·개정된 전자금융감독규정 및 전자금융감독규정 시행세칙에 대해 소개하고자 한다.

Ⅰ. 서 론

2013년 시중은행 5곳의 전산시스템이 마비되었던 '3·20 사이버테러' 발생 이후 금융위원회는 재발 방지를 위해 「금융전산 보안강화 종합대책」을 발표하며 2014년 말까지 금융회사의 전산망 분리를 의무화하였다. 금융회사의 내부 업무망과 외부 인터넷망을 분리하여 해킹 등의 사이버 위협을 방지하고자 하는 의도였다.[3] 하지만 제도 시행 이후 금융회사들은 금융거래상 필수 업무(타행 이체, 신원 및 신용 정보를 확인하기 위한 행정시스템 접속 등) 수행 시 인터넷 접속이 불가피하기 때문에 전면적인 망분리는 현실적이지 않다고 주장하였다.[4]

이에 따라 2015년 금융위원회는 망분리 예외 상황에 대한 기준을 세우고, 기존의 모호했던 망분리 적용범위의 세부기준을 명확히 하는 등의 내용들을 「전자금융감독규정(2015.6.24. 일부개정)」 및 「전자금융감독규정 시행세칙(2015.9.17. 일부개정)」에 반영시켜 개정하였다.

본 고에서는 개정된 금융전산 보안강화 종합대책에 따라 신설·보완된 망분리 예외기준 및 적용범위에 대해 살펴보고 전자금융감독규정의 주요 개정 내용을 소개하고자 한다.

Ⅱ. 금융권 망분리 관련 연구

2.1. 금융권 망분리 제도의 목적

국내에서 발생한 전자금융 관련 주요 보안 사고를 살펴보면 인터넷망에서 접근 가능한 관리 서버 등을 통해 악성코드에 시스템이 감염되거나, 사회공학 공격 방식을 이용하여 특정 이메일 등을 내부 직원에게 유포하여

〔표 1〕 주요 금융권 보안사고 내역〔6〕

발생시기	사고내역
2014.01	- K사 및 N사, L사의 외주업체직원에 의하여 고객정보 유출
2013.05	- M사 내부직원에 의한 고객정보 유출
2013.03	- N사 및 S사 등 패치관리 시스템을 통해 패치파일을 가장한 악성코드가 내부 업무 PC로 유포되어 데이터 삭제 등 서비스 장애 발생
2012.02	- S사 외주업체직원에 의하여 고객정보 유출
2011.12	- I사 내부직원에 의하여 고객정보 유출
2011.05	- L사 홈페이지 관리 서버의 개인정보 DB 관리 소홀로 인해 개인정보 유출
2011.04	- H사 서버 취약점 해킹 공격을 통한 고객 정보와 고객 신용등급 정보 유출

* 동국대학교 국제정보보호대학원 사이버모바일보안학과 (jiyun15@dongguk.edu)
** 동국대학교 국제정보보호대학원 사이버모바일보안학과 (alice_ys@dongguk.edu)
*** 동국대학교 국제정보보호대학원

이메일 열람 시 내부 직원의 PC를 통해 내부 업무망에 침투 또는 시스템 파괴 등과 같은 공격 방식이 증가하였다. 하지만, 현재 상용되고 있는 보안 솔루션인 방화벽, 침입차단시스템, 유해 사이트 차단 시스템, 안티바이러스 등으로는 고도의 APT 공격 대응에 한계가 있다.

이에 금융회사는 전자금융기반시설의 보안강화를 위해 업무망과 외부 인터넷망을 완전히 분리하여 인터넷망을 통한 악성코드 감염을 차단하고, 나아가 알려지지 않는 APT 공격 위협을 사전에 차단하기 위함에 목적을 두고 있다. 아래의 [표 1]은 최근 발생한 주요 보안 사고를 나타낸 내용이다.

2.2. 금융권 망분리 현황

망분리 제도는 사이버 위협으로부터 정보를 안전하게 지키기 위해 정부 주도 하에 2006년부터 시행되었다.[2] 초기의 망분리 사업은 지자체, 공단, 공기업 등 공공기관 위주로 진행되었으나, 정부에서는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령(2015.12.22. 일부개정)[이하: 정보통신망법 시행령]」을 2012년에 개정하면서 정보통신망법 시행령 제15조에서 제시한 기준에 해당하는 민간 기업도 사업장의 망을 분리하도록 의무화시켰다. [표 2]는 정보통신망법 시행령 제15조 2항의 내용으로써, 개인정보 보호조치를 취해야 하는 정보통신서비스 제공자의 기준을 지정하고 해당 제공자가 망분리를 포함하여 어떠한 보호조치를 취해야 하는지 명시하고 있다.

〔표 2〕 정보통신망법 시행령

제15조(개인정보의 보호조치) ② 법 제28조제1항제2호에 따라 정보통신서비스 제공자 등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 다음 각 호의 조치를 하여야 한다. 다만, 제3호의 조치는 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 정보통신서비스 제공자등만 해당한다. 〈개정 2012.8.17.〉 - 생략 - 3. 개인정보처리시스템에 접속하는 개인정보취급자 컴퓨터 등에 대한 외부 인터넷망 차단 - 생략 - 〔전문개정 2009.1.28.〕

'3·20 사이버테러' 발생 이후 정부에서는 금융 전산의 중요성을 인지하여 2013년 7월 망분리 의무화 지침을 발표하였다. 지침에 따라 금융회사는 전산센터의 물리적 망분리를 2014년 말까지, 각 은행의 본점과 영업점에 대해서는 2015년 말까지, 그 외 금융기관은 2016년 말까지 단계적으로 논리적 또는 물리적 망분리를 실시해야 한다.[2]

2014년 「금융전산 보안강화 종합대책」에 따라 금융권에서 망분리 사업을 진행하였으나 수많은 애로사항이 발생되었다. 예로 인터넷 망에 포함된 PC 또는 가상화 서버로 접근하여 업무 환경을 이용할 수 있는 논리적 망분리 환경에서 USB를 이용하여 업무 환경 자료를 로컬 PC로 옮길 수 있는 취약점이 발견되었다. 또한, 업무 PC에 설치된 보안 솔루션이 사용자에게 할당된 특정 네트워크 드라이브를 검사하지 못하는 등 보안 솔루션과 기존 시스템 간의 호환성 문제에 따른 보안 취약점이 발견되기도 하였다. 심지어 일부 기업에서는 자료의 중요성과 상관없이 자료 반·출입을 모두 허용하거나 중요 자료에 대한 승인절차를 구성하지 않는 등 자료전송에 대한 통제가 제대로 이루어지고 있다.

금융위원회에서는 금융전산의 망분리 의무화와 관련하여 발생한 취약점 및 불편사항 등을 개선하기 위해, 2015년 「전자금융감독규정」과 「전자금융감독규정 시행세칙」을 개정하며 규제합리화를 하였다. 전자금융감독규정의 망분리에 대해 명시한 내용은 [표 3]과 같고, 금융회사 또는 전자금융업자가 업무용시스템 및 정보처리시스템의 망을 분리하여 사이버 침해행위에 대한 대책으로 수립해야 한다는 내용과 망분리 시 예외 상황을 함께 명시하고 있다. 망분리 적용 예외 기준과 규정을 이행할 수 있는 조건은 전자금융감독규정 시행세칙에서 다루고 있으며 해당 내용은 [표 4]과 같다.

〔표 3〕 전자금융감독규정

제15조(해킹 등 방지대책) ① 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운용하여야 한다. - 생략 - 3. 내부통신망과 연결된 내부 업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속 금지(단, 업무상 불가피하여 금융감독원장의 확인을 받은 경우에는 그러하지 아니하다) 〈개정 2013.12.3.〉 4. 내부통신망에서의 파일 배포기능은 통합 및 최소화하

여 운영하고, 이를 배포할 경우에는 무결성 검증을 수행할 것 〈신설 2013.12.3.〉
5. 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리할 것(단, 업무 특성상 분리하기 어렵다고 금융감독원장이 인정하는 경우에는 분리하지 아니하여도 된다.) 〈신설 2013.12.3., 개정 2015.2.3.〉
⑥ 금융회사 또는 전자금융업자는 무선통신망을 설치·운용할 때에는 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013.12.3.〉
- 생략 -
3. 금융회사 내부망에 연결된 정보처리 시스템이 지정된 업무 용도와 사용 지역(zone) 이외의 무선통신망에 접속하는 것을 차단하기 위한 차단시스템을 구축하고 실시간 모니터링체계를 운영할 것 〈개정 2015.2.3.〉
- 후략 -

〔표 4〕 전자금융감독규정 시행세칙

제2조의2 (망분리 적용 예외) ① 규정 제15조제1항제3호에서 금융감독원장의 확인을 받은 경우란 내부 업무용시스템을(규정 제12조의 중요단말기는 제외한다) 업무상 필수적으로 특정 외부기관과 연결해야 하는 경우를 말한다(다만, 이 경우 필요한 서비스번호(port)에 한하여 특정 외부기관과 연결할 수 있다).
② 규정 제15조제1항제5호에서 금융감독원장이 인정하는 경우란 다음 각 호와 같다.
1. 「금융회사의 정보처리 업무 위탁에 관한 규정」에 따라 정보처리 업무를 국외 소재 전산센터에 위탁하여 처리하는 경우(다만, 해당 국외 소재 전산센터에 대해서는 물리적 방식 외의 방법으로 망을 분리하여야 하며, 이 경우에도 국내 소재 전산센터 및 정보처리시스템 등은 물리적으로 망을 분리하여야 한다)
2. 업무상 외부통신망과 연결이 불가피한 다음의 정보처리시스템(다만, 필요한 서비스번호(port)에 한하여 연결할 수 있다)
가. 전자금융업무의 처리를 위하여 특정 외부기관과 데이터를 송수신하는 정보처리시스템
나. DMZ구간 내 정보처리시스템과 실시간으로 데이터를 송수신하는 내부통신망의 정보처리시스템
다. 다른 계열사(「금융회사의 정보처리 업무 위탁에 관한 규정」 제2조 제3항의 "계열사"를 말한다)와 공동으로 사용하는 정보처리시스템
3. 규정 제23조의 비상대책에 따라 원격 접속이 필요한 경우
③ 제1항 및 제2항의 규정은 금융회사 또는 전자금융업자가 자체 위험성 평가를 실시한 후 〈별표 7〉에서 정한 망분리 대체 정보보호통제를 적용하고 정보보호위원회가 승인한 경우에 한하여 적용한다.
〔본조신설 2015.9.17〕

2.3. 금융권 망분리 구축 사례

정보통신망법 시행령에 따르면 전년도말 직전 3개월간 일일 평균 100만 명 이상의 이용자 개인정보를 보유하거나 전년도 정보통신분야 매출액이 100억 원 이상인 정보통신서비스 제공자는 개인정보처리시스템에 접속하는 컴퓨터 등에 대해서 외부 인터넷망과 차단해야 한다. 이에 따라 금융회사들은 전산센터를 대상으로 하는 물리적 망분리 사업은 완료하였으며, 본점과 지점의 망분리는 2016년까지 마무리 지을 예정이다.

`09년~`16년까지 신문기사를 통해 금융회사의 망분리 구축과 관련한 보도 자료를 게제한 곳은 총 16건인 것을 확인할 수 있다. 다음 [표 5]는 보도 자료를 기반으로 망분리 방식 및 내용에 대한 망분리 구축 사례를 정리한 내용이다.

〔표 5〕 망분리 구축 사례

도입 시기	기관	내용	방식
2015.12	삼성화재	전산센터 및 본사·지점 업무 PC	논리적
2015.12	KDB 산업은행	본점 및 지점 3,000여명 직원 업무 PC	물리적
2015.01	동부화재	전산센터 업무 PC	물리적
2014.12	한국은행	1차 160대, 차후 2,500대	물리적
2014.12	부산은행	3,500명	논리적
2014.12	농협은행	IT본부 540대 물리적 망분리 6,000대 논리적 망분리	Hybrid
2014.12	기업은행	영업점 950대 논리적 망분리 650개 지점 물리적 망분리	Hybrid
2014.11	기술보증기금	전산부서 50명 물리적 망분리 1,200명 논리적 망분리	Hybrid
2014.09	예금보험공사	100대	논리적

도입 시기	기관	내용	방식
2014.03	국민연금공단	본부 800명 논리적 망분리 140개 콜센터 물리적 망분리	Hybrid
2014.02	금융투자협회	업무용 PC	논리적
2014.02	알리안츠생명	250개 지점 3,000대 PC	논리적
2013.12	수출입은행	전산부서 60대	물리적
2013.07	KDB 산업은행	최초 200대, 차후 3,000대	논리적
2013.06	신한은행	15,000대	논리적
2009.12	기업은행	520개 지점 및 영업점과 53개 본부부서 12,000명	논리적

Ⅲ. 금융권 망분리 제도의 주요 개선 내용

금융회사 또는 전자금융업자는 망분리 적용 예외 시 스스로 위험평가를 실시한 후 대체통제를 점검하고 정보보호위원회의 심의를 통하여 보안리스크를 스스로 통제하도록 예외 적용 절차를 마련하였다. 다음 [표 6]은 전자금융감독규정 시행세칙에 신설된 내용으로 금융회사 또는 전자금융업자가 망분리 적용 예외를 택했을 경우, 망분리를 대체할 수 있는 정보보호통제에 관한 내용이다.

〔표 6〕 망분리 대체 정보보호통제(신설 2015.9.21)

대책	세부사항
내부망 보안 강화	- 업무망에 반입되는 전산자료 대상으로 악성코드 감염여부 진단·치료 대책 수립
외부망 보안 강화	- 지능형 해킹(APT)차단 대책 수립 - 외부망을 통해 전산자료 외부전송 시 정보유출 탐지·차단·사후 모니터링 대책 수립
메일시스템 보안 강화	- 본문과 첨부파일 포함하여 메일을 통한 악성코드 감염 예방 대책 수립 - 메일을 통해 전산자료 외부전송 시 정보유출 탐지·차단·사후 모니터링 대책 수립
단말기 보안 강화	- PC 사용자의 관리자 권한 제거 - 승인된 프로그램만 설치·실행토록 대책 수립 - 단말기 전산 자료 암호화 저장
원격 접속 통제 수립	- 원격접속 기준 및 절차가 포함된 보안 정책 수립 - 불법 원격접속을 방지하기 위한 사용자 인증, 암호화 등의 보안대책을 수립 - 원격접속은 책임자의 승인을 받은 사전 등록자에 한하여 허용하며 원격 접속 관리 기록부를 기록·보관 - 원격에서 접속하는 외부 단말기와 내부 업무용 시스템 구간의 암호화 통신 - 원격접속 사용자는 아이디·비밀번호 이외에 추가 인증수단을 적용 - 원격에서 접속하는 외부 단말기의 악성코드 감염 예방 대책 수립·적용 - 원격으로 접속 가능한 내부 업무용 시스템의 접근 통제 수립·적용 - 원격으로 접속하여 수행한 모든 작업 내역을 기록하고 매일 이상여부 점검 실시 및 책임자가 확인

3.1. 전산센터

전산센터의 경우, 국외소재 전산센터의 정보처리 업무, 정보처리시스템의 외부망 연결, 업무의 연속성을 위한 원격접속과 관련된 세부기준이 마련되었다.

외국계 금융회사가 아닌 국내 법인이 데이터센터(또는 특정 일부 시스템) 운영을 해외에 위탁하는 경우, 전자금융감독규정 시행세칙 제2조의제2항제1호에 따라 국외로 위탁한 전산센터, 정보처리시스템 및 단말기가 망분리 통제의 대상에서 완전히 제외되는 것은 아니며, 논리적 망분리, 방화벽을 통한 접근 통제 등 물리적 망분리 이외의 다른 방법으로 네트워크를 분리할 수 있도록 허용한다. 단, 국내 소재 정보처리시스템의 운영을 위해 국외 소재 단말기에서 접속하는 경우, 해당 국외 소재 단말기는 전자금융감독규정 시행세칙 제2조의제2항제1호에 따른 예외대상에 포함되어 물리적 망분리 이외 다른 방법으로 망분리가 가능하다. 다만, 수탁자가 국외에 소재하는 경우라 할지라도 정보처리시스템이 국내에 있는 경우, 국내에 위치한 정보처리시스템은 물리적 망분리 대상에 해당된다.

다른 계열사와 공동으로 이메일 시스템을 사용하는 경우 해당 이메일 시스템, 내부망, 외부망, 사용자 단말

기에 '망분리 대체 정보보호통제'를 적용해야 한다. 그룹웨어 등 기타 시스템을 공동으로 사용하는 경우에는 '메일 시스템 보안 강화'를 제외한 나머지 대책을 모두 적용해야 한다. 단, 해당 공용시스템을 사용하는 계열사의 사용자 단말기는 '망분리 대체 정보보호통제'의 '단말기 보안강화' 적용 대상이 아니다.

전산센터의 단말기가 업무상 외부통신망이 필요하더라도 망분리를 적용한 전산센터의 단말기는 모든 외부망 및 인터넷 연결이 불가하다. 다만, 전자금융감독규정 제17조에 따라 안전대책을 운용하는 경우 DMZ 내 정보처리시스템에는 직접 접속이 가능하다.[5]

3.2. 금융회사 본점 및 영업점

본점 및 영업점의 경우, 내부망에 연결된 단말기의 제한적 접속 허용 범위에 관한 세부기준이 마련되었다.

금융회사 내부망에 연결된 모든 단말기는 망분리 대상이므로 외주직원이 소유한 단말기도 망분리를 적용해야 한다. 다만, 외주직원의 단말기가 내부망과 분리된 망(DMZ 등)에 위치한 시스템에만 접속하는 경우에는 해당 단말기는 망분리 대상에 포함되지 않는다.

업무용 단말기에서 특정 외부 기관을 연결하는 경우, 망간 자료전송시스템 등 특정 시스템이나 솔루션 사용이 의무사항은 아니며 방화벽 등을 통해 외부기관과 연결이 가능하다.[5]

Ⅳ. 결 론

오늘날 인터넷 기술의 발달로 인터넷망을 통한 악성코드 유포 및 사회공학 공격 방식과 같은 보안 사고가 계속해서 급증하고 있으며, 이는 사회·경제적 측면에서 큰 문제가 되고 있다. 이러한 문제의 재발 방지를 위해 종합적인 망분리 제도의 구축이 필요하게 되었다. 특히 '3·20 사이버테러' 발생 이후 금융위원회에서는 금융IT 보안의 필요성을 인지하고 「금융전산 보안강화 종합대책」을 발표를 통해 금융회사의 전산망 분리를 의무화하였다. 하지만 금융거래상 필수업무 수행 시 인터넷 접속을 필요로 하는 시스템에 대해서는 망분리 적용이 현실적이지 않았다. 이에 따라, 금융위원회는 망분리 예외상황에 대한 기준을 세우고, 세부기준을 명확히 하는 내용을 반영하여 기존의 모호했던 망분리 적용 기준을 개정하였다.

본 고에서는 과거 금융 전산 망분리 의무화에 대한 내용과 현재 해당 내용이 개정된 이후의 변화에 대해 고찰해 보았다. 금융위원회는 「전자금융감독규정 시행세칙」을 통해 예외기준을 마련하며 망분리 적용 범위의 불명확성을 개선하였다. 또한 업무상 대외기관과 연결이 불가피하거나 업무 연속성을 위한 비상시 업무 처리 등 망분리 예외기준을 명확히 하여 업무의 투명성을 확보하였으며, 규제합리화를 통해 금융산업의 경쟁력 제고에 기여 하였다.[4]

현재 신설된 금융 전산 망분리의 예외 기준이 금융회사의 필수 업무에 대한 연속성을 보장하고 금융업의 능률 제고시킬 대책인 것은 분명하다. 하지만, 현재 개정된 내용에 따르면, 전자금융 사고 발생 시 온전히 금융회사의 책임이 될 가능성이 매우 크다. 일례로 현재 금융당국은 망분리 가이드라인 또는 체크리스트를 제공하지 않고 있다. 이에 따라 금융회사가 필수 업무와 관련하여 망분리를 적용하지 않을 경우 자체적인 위험성 평가를 통하여 자율적으로 망분리 대책을 세우고 망분리 대체정보보호통제 사항을 따를 것을 전자금융감독규정 시행세칙에서 명시하고 있다. 하지만 예외상황에 대한 통제 내용 역시 현실에 맞지 않은 내용이 일부 존재할 뿐만 아니라 예외 상황에서 보안 사고 발생 시의 책임은 금융회사에서 부담해야 한다고 IT·금융정보보호단은 밝혔다.

이제는 3·20 사이버테러 발생 이후 금융당국이 내놓았던 초기 망분리 의무화와 같은 결과론적인 대책보다는 금융 IT 환경에 적합한 현실적인 보안 대책을 제시해야 할 것이다. 향후에는 금융 IT의 현실과 맞는 금융전산 망분리 및 금융 IT와 관련한 보안 대책을 수립하기 위해, 금융당국과 금융회사는 지속적으로 연구하고 관리해야 할 것이다.

참 고 문 헌

[1] 이익준. "금융전산 논리적 망분리 보안정책에 관한 연구" 동국대학교 국제정보대학원 정보보호학 학위논문 February 2014.

[2] 임병하, "정보보안을 위한 망분리 구축에 대한 연구", *전자무역연구*, 제12권 제4호, November 2014.

[3] 조병주, 윤장호, 이경호. “금융회사 망분리 정책의 효과성 연구”, *정보보호학회논문지*, 25(1), February 2015.
[4] IT보안인증사무국, “금융전산 망분리에 대한 세부기준 마련으로 업무투명성 확보”, September 2015
[5] IT·금융정보보호단. “전자금융감독규정 시행세칙 망분리 예외 조항 관련 Q&A”. September 2015
[6] KB금융지주경영연구소. “KB 지식 비타민: 국내외 금융권의 정보보안 최근 동향과 전망”. 15-19호. March 2015.

〈저 자 소 개〉

박 지 윤 (Ji-Yun Park)
학생회원

2014년 8월 : 서울여자대학교 정보보호학과 졸업
2015년 3월~현재 : 동국대학교 사이버모바일보안학과 석사과정
<관심분야> 정보보호 관리체계 인증, 시스템보안, 네트워크보안

정 윤 선 (Yun-Sun Jung)
학생회원

2014년 8월 : 서울여자대학교 정보보호학과 졸업
2015년 3월~현재 : 동국대학교 사이버모바일보안학과 석사과정
<관심분야> 정보보호, 정보보호 관리체계 인증

이 재 우 (Jae-Woo Lee)

동국대학교 국제정보대학원 석좌교수(현)
한국포렌식조사전문가협회 회장(현)
ISC2 Fellow, Asia Board 의장(현)
한국 CSO 협회 자문위원장(현)
한국정보보호진흥원 초대 원장