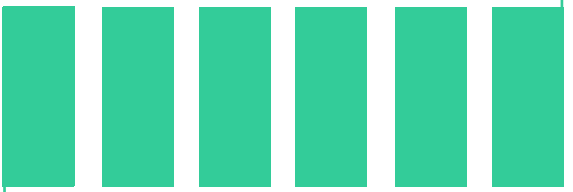
이슈 미니
써머리

핀테크 기업의 망분리

고려대학교 정보보호대학원 김승주 교수 감수



2020년 2월

STARTUP ALLIANCE

vol 1.

‘이슈 미니 써머리’ 시리즈

스타트업얼라이언스는 대한민국 스타트업 생태계를 활성화하고 다양한 이해관계자에게 스타트업의 목소리를 전하기 위해 2014년 개소한 비영리기관입니다.

스타트업얼라이언스는 지난 6년간 스타트업 생태계가 빠르게 변화하고 성장해 나가는 걸 보았습니다. 2019년 하반기, 한국의 유니콘 기업의 수는 전 세계에서 다섯 손가락 안에 들 만큼 많습니다. 10개가 되었으며, 스타트업에 대한 투자는 매년 사상 최대 규모를 갱신합니다. 전 세계적인 추세가 그러하듯, 스타트업들은 기존 산업군의 경계를 넘어, 기존 기업들을 무섭게 따라잡고 있으며, 스타트업의 성장세는 앞으로 더욱 거셀 겁니다. 우리 경제에서의 스타트업 비중은 이렇게 조금씩 높아지고 있습니다.

하루가 다르게 성장해 나가는 한국의 스타트업의 발목을 잡는 것은 규제입니다. 스타트업얼라이언스가 매년 진행하는 ‘스타트업트렌드리포트'에서는 항상 가장 먼저 풀어야 할 숙제로 ‘규제완화'가 6년째 1, 2등을 차지합니다. 정부, 정치권에서도 스타트업의 의견을 듣고 문제를 해결하고자 노력합니다. 하지만 법, 규제 환경을 살필 여력이 있는 스타트업은 소수이며, 다양한 산업군, 제도에 걸쳐 있는 데다 빠르게 변화해 정부/정치권에서도 다루기 어려운 이슈가 많습니다.

그래서 ‘미니 이슈 써머리’가 탄생하게 되었습니다. 우리 스타트업 생태계가 겪는 법/규제/정책 이슈, 혹은 우리도 참고해 볼 만한 사례들을 조망해 보려 합니다. 이슈가 무엇인지, 어떻게 흘러왔는지, 다양한 이해당사자들은 지금 어떻게 생각하는지 다양한 방식으로 조명해 보려 합니다. 빠른 이해가 필요하다면 앞의 요약 정리를, 자세한 이해가 필요하다면 뒤의 상세 내용을 참고할 수 있게 작성했습니다. 좀 더 많은 분들이 스타트업의 법/규제/정책 이슈에 접근하고, 함께 고민하는 데 도움이 된다면 더할 나위 없이 좋겠습니다.

목차

— 이슈 미니 써머리 첫번째 챕터 —

쉽게 보는 이슈

한 눈에 보는 망분리 이슈

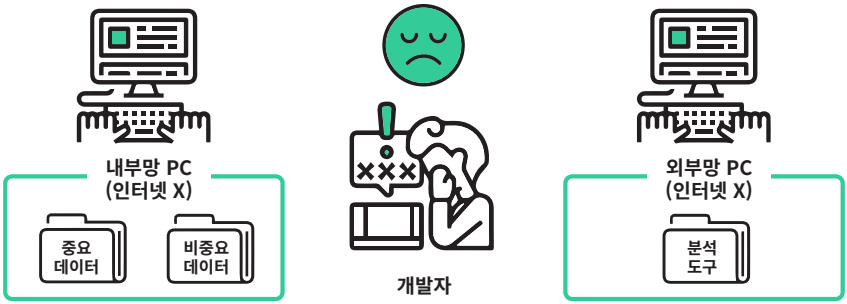
국내 핀테크 기업들은
‘전자금융감독규정’의
망분리 규제 개정을 원합니다.
이유는 이렇습니다.

1

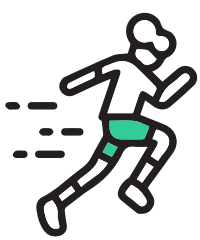
개발현장과 괴리
생산성 저하와 과도한 비용

2

보안에도 악영향
모호한 적용범위와 특정 보안방법 강제



개발자 생산성 50% ⬇
개발자 인건비 30% ⬆
망분리 비용 약 5억원 ⬆ (25인 기준)



1. 개발현장과 괴리

생산성 저하와 과도한 비용

데이터와 분석/개발도구가 물리적으로 분리되어 있어
개발자는 소스코드 하나하나 반입/반출허가를 받습니다.

업계의 추산에 따르면, 규제로 인해
개발자 생산성은 **50%**이하,
개발자 인건비는 **30%** 더 지출하며,
망분리 비용은 **약 5억원** 정도 더 지출합니다.

2. 보안에도 악영향

모호한 적용범위와 특정 보안방법 강제

‘내부통신망과 연결된 내부 업무용시스템’이라는
모호한 범위는 업무 현장에 적용이 어렵습니다.

해킹과 보안 기법의 빠른 변화를 따라가지 못하는 점도
문제로 지적됩니다.

국내 핀테크 기업들은
망분리 규제가
이렇게 개정되길 원합니다.

해외에서는 이미
이런 방식이 일반적입니다.

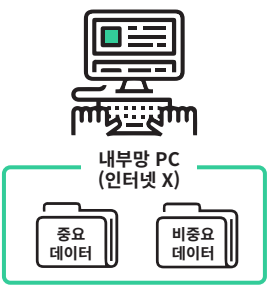
전문가들 역시
'망분리'로 대표되는
현재의 '도메인 중심' 보안정책을
재고해야 한다고 합니다.

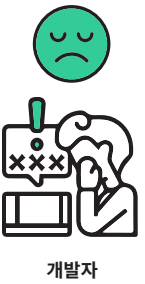
1

‘데이터 단위’ 보안정책

2

기업이 책임지는 자율규제, 사후규제


내부망 PC
(인터넷 X)
중요
데이터
비중요
데이터

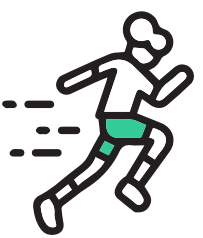

개발자


외부망 PC
(인터넷 X)
분석
도구


중요정보 PC
(인터넷 X)
중요
데이터


개발자


비중요정보 PC
(인터넷 O)
비중요
데이터
분석
도구



1. '데이터 단위' 보안정책

핀테크 기업들은 정보통신망법 시행령처럼
'개인정보' 등 데이터 단위로 보안 정책을 적용했으면 합니다.

수많은 보안 전문가들 역시
정보를 중요도 기준으로 분류하는
'데이터 중심' 보안 패러다임으로 전환해
기밀은 안전하게 보관하고,
정보는 더욱 활발히 유통해야 한다고 말합니다

2. 기업이 책임지는 자율규제, 사후규제

기업 전체의 보안을 가장 빠르게 진단하는 것도,
가장 올바른 해결책을 빠르게 도입하는 것도 기업입니다.

해외에서는 이런 방식이 일반적입니다.
표준, 가이드라인을 참고해
최신 보안 기술을 자율적으로 적용하되,
사고발생 시 강력한 책임을 지는 사후규제를 받습니다.

핀테크 기업의
현업 환경을 고려해도,

해외 표준, 가이드라인
권고사항을 따라도,

초연결시대를 대비하는
전문가들의 의견도,

망분리 규제 개정은
‘4차산업혁명’을 위한
‘새로운 보안
패러다임’의
시작점입니다.

규제 ‘내부업무망’이라는 모호한 적용범위에 ‘망분리’라는 강력한 기술 적용 의무, 심지어 사전규제

o 관련규정 : 전자금융감독규정 제15조 제1항 제3호, 제5호

· 빠르게 변하는 현업 환경 반영하지 못하는 ‘사전규제’ 방식
· 기술은 쏟아져 나오는데 하필 특정 기술, ‘망분리’ 적용 의무
· 대체 어디까지가 내부 업무망? 적용범위 모호한 ‘도메인 중심 보안 정책’

o 관련표준 : PCI DSS* 범위 설정 및 망분할 가이드 등

· 표준/가이드라인 바탕으로 기업이 자율성, 책임 갖는 ‘사후규제’ 방식
· ‘망분리’ 등 특정 기술 적용 의무 없으며, 기업 상황 맞게 기술 도입해 ‘전사적 보안 체계 강화’ 우선시
· 중요한 데이터를 기업이 판단해 확실히 보호, 훨씬 체계적이고 안전한 ‘데이터 중심 보안’

*** PCI DSS** : 비자, 마스터카드 등 카드사 업계에서 보안 강화를 위해 자체적으로 만든 민간 표준

망분리를 둘러싼 각자의 주장은?

❶ 망분리 정책 데이터 중심으로 개정
(‘개인정보’ 등 데이터 단위 적용범위)
❷ 해외처럼 기업의 자율규제 도입
(사후규제방식 도입)

핀테크 기업

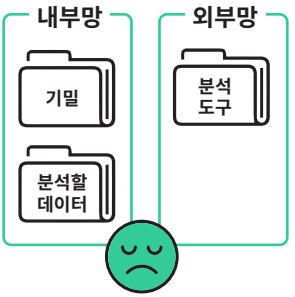
❶ 망분리 정책 데이터
(망분리 정책 시행 이
❷ 해외처럼 기업의 자
(금융분야의 특수성 고

금
당

적용 망분리 규제 적용받은 국내 핀테크 회사는 '내부망'에서 인터넷 안 됨, 신기술 활용에 지장

한국

도메인 중심 보안 정책



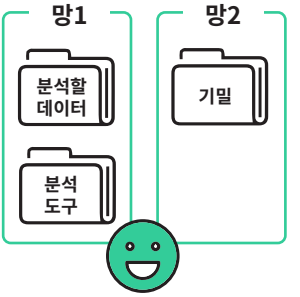
❶ 데이터와 분석도구가 분리되어 데이터 활용에서 비효율

❷ 기밀과 데이터를 같은 공간에 둬서 취약

❸ 클라우드, 스마트워크, 오픈소스 활용 등 신기술 활용 불가

해외

데이터 중심 보안 정책



❶ 데이터와 분석도구가 같은 공간에 있어 효율적 데이터 활용

❷ 기밀과 데이터를 분리 보관해 안전

❸ 클라우드, 스마트워크, 오픈소스 활용 등 신기술 활용 가능

---

❶ 망분리 정책 데이터 중심으로 개정
(데이터 활용, 보안성 강화에 적합)

❷ 정부, 데이터 분류 체계 시급히 마련해야
(기밀 아닐 경우 유통 활용 최대한 장려)

보안 전문가

		논리적 망분리 완화 (15조 1항 3호)
 핀테크 기업	오픈소스, 클라우드 때문에 논리/물리적 망분리 필요. 자율규제 도입된다면 사후규제 감수 데이터 중심 보안체계가 현장에 적합	YES
 금융사/공공	오픈소스, 클라우드 때문에 논리/물리적 망분리 필요. 비조치의견서 등 받아가며 조심스러운 움직임	-
 금융당국	금융분야의 특수성, 망분리 도입 후 사고 감소 효과로 망분리 규제 변화는 조심스럽게 접근	NO
 전문가/학계	현재의 도메인 중심 정책, 4차산업혁명에 맞지 않아 데이터 중심 보안정책으로 이행해야	YES
 해외	데이터 중심 보안 정책 이미 추진 기업들에게 기술선택, 도입범위 자율권 주되 표준, 가이드라인 통해 안내, 사고 발생 시 기업에 책임	YES

물리적 망분리 완화 (15조 1항 5호)	자율규제 /사후규제	데이터 중심 보안체계 이행
YES	YES	YES
YES	-	-
NO	NO	-
YES	-	YES
YES	YES	YES

한 눈에 보는 망분리 Q&A

Q1. 망분리, 왜 갑자기 문제가 된 건가요?

'4차산업혁명' 시대에 맞는 신기술 활용과 장기적 보안성 제고를 위해서입니다. '내부 업무용 시스템의 망분리'라는 규정은 업무에 인터넷이 제한적으로 사용되던 2006년, 혹은 원자력 발전 시설 등 민감한 시설에는 적합한 정책일 수 있습니다. 하지만 현업에서 어디까지가 '내부 업무용 시스템'인지 알기는 정말 어렵기에 현업에서 완전히 준수하기도 어려우며, 오픈소스, 클라우드 등 신기술을 유연하게 활용하는 데 장애물이 되기 일쑤입니다.

디도스 (DDoS, Distributed Denial of Service)
: 여러 공격자가 동시에 서비스에서 제공하는 것 이상의 것을 요청해 (예, 과도한 접속 시도) 시스템이 정상적 서비스를 제공할 수 없도록 만드는 해킹 방식

내-외부망 등 도메인 중심으로, 기술을 명시한 현재 망분리 정책은 장기적으로 보안성 제고에도 악영향을 끼칠 수 있습니다. **해외에서는 업무영역 단위가 아닌 데이터 중요도를 기준으로 보안정책을 세웁니다. 업무 효율성이 증가하는 것은 물론, 보안성 역시 제고되기 때문입니다.** 해외에서는 표준, 가이드라인 등을 통해 기업이 도입할 수 있는 효과적인 기술, 기준을 알려주고, 기업이 전사적으로 보안 수준을 제고하도록 돕고 지속적인 모니터링을 실시하고, 강한 사후규제를 적용하는 것이 일반적입니다. 빠르게 변화하는 기술의 발전속도를 따라가려면, 특정 기술을 사전규제로 처방하는 것보다 기업이 내부 사정에 맞게 정보보호를 위한 기준, 기술을 채택하고 최선의 노력을 다하도록 하는 것이 현실적이기 때문입니다.

Q2. 망분리가 뭔가요?

망분리는 네트워크 보안 기법의 일종입니다. 외부의 공격으로부터 내부의 자료를 보호하기 위해 **망을 분리(separate)하는 것을 의미합니다.** 직원 입장에서 업무용 컴퓨터에 망분리를 적용한다는 것은, 업무용 컴퓨터에서는 인터넷 연결이 안 된다는 의미입니다. 그렇기에 다른 컴퓨터 등 하드웨어를 사서 인터넷을 쓰기도 하고(물리적 망분리), 소프트웨어적으로 다른 가상의 컴퓨터를 구현해서 인터넷을 쓰기도 합니다(논리적 망분리).

망분리를 하는 방법은 다양합니다. '전자금융감독규정'처럼 업무망과 아닌 망을 구분할 수도, '정보통신망법' 처럼 개인정보를 다루는 망과 아닌 망을 구분할 수도 있습니다. 망을 두 개로만 쪼개야 하는 것도 아닙니다. 자원만 충분하다면 3개든 그 이상이든 마음껏 나눌 수 있습니다. 같은 목적을 달성하기 위해 라우터, 방화벽 등을 이용해 망을 다수의 서브네트워크로 나누는 '망 세분화(segmentation, zoning)' 방식을 사용하기도 합니다.

망이 분리되면 상대적으로 더 안전해지겠지만, 효율성은 그만큼 저하되므로, 이 상충관계를 잘 조절한 보안정책이 필요합니다.

-> 자세한 내용은 32페이지 참고!

Q3.
망분리 규제는 왜 생겼죠?

국내의 망분리 정책은 **2006년, 중앙정부에 물리적 망분리를 도입하는 것에서 시작됩니다.** 2009년 7.7 디도스 , 2011년 3.4 디도스, 2013년 3.20 디도스 등 다양한 사이버 공격을 겪으며 보안 향상에 대한 필요성이 대두됩니다. 이에 대한 해답으로 '망분리'가 제시되었고, 지자체, 공공기관을 거쳐 민간부문까지 확산됩니다. 2012년 정보통신망법 시행령 개정, 2013년에는 전자금융감독규정 개정 등이 그 예입니다.

-> 자세한 내용은 34페이지 참고!

Q4.
망분리 관련해 지금은 어떤 규제가 있죠?

공공부문은 ‘국가정보보호기본지침'에 따라, 민간부문은 ‘정보통신망법 시행령'에 따라, ‘금융기업’은 ‘전자금융감독규정'에 따라 망분리를 적용합니다. 공공부문은 내부망(업무망)과 외부망(인터넷망)을 나누고 있습니다. 일반 민간부문의 경우 100만건 이상의 개인정보를 보유한 기업에서는 개인정보가 있는 PC를 분리시킬 것을 명시합니다. **금융부문의 경우 업무용PC의 인터넷이 차단되어야 하고(15항 3조), 시스템 운영/개발/보안용 PC는 물리적으로 분리되어야(15항 5조) 합니다.**

-> 자세한 내용은 37페이지 참고!

Q5.
지금의 망분리 규제를 지키면 안전한가요?

100% 안전한 금고란 없듯, 100% 안전한 사이버 보안 방법도 없습니다. 망분리 역시 같은 맥락에서 봐야 합니다. 정부와 금융당국의 발표에 의하면 망분리 규제 이후 보안사고가 많이 줄어들었습니다. 하지만 물리적 망분리가 되어 있어도 공격당한 사례는 많습니다. 2010년 스턱스넷 악성코드가 이란의 핵 시설을 공격했고, 2014년에는 한국수력원자력이, 2016년에는 국방부가 해킹당했습니다. 망분리는 하나의 보안 수단일 뿐이며, 다른 보안 요소 중 취약한 부분이 있다면 망분리가 되어 있어도 공격당할 수 있습니다. 올바른 자원 배분을 통해 전반적인 보안 수준을 올리는 것이 우선입니다.

-> 자세한 내용은 33페이지 참고!

Q6.
지금 망분리 규제가 바뀌면 보안성이 떨어지는 것 아닌가요?

규제부문에서는 망분리 규제 이후 보안사고가 줄어든 것을 근거로 망분리 규제를 유지하고 있습니다. 국민들의 재산이 달려 있고, 상호 연계되어 있는 금융업의 특수성 때문에 사전규제가 불가피하지만, 금융기업의 성장 촉진을 위해 현장 목소리 역시 청취하겠다는 입장입니다. 하지만 보안을 투자가 아닌 비용으로 생각하는 금융기업들의 행태를 지적하며 날을 세우기도 합니다.

-> 자세한 내용은 52페이지 참고!

Q7. 핀테크 업계에서는 왜 망분리 규제 개선을 원하나요? 어떻게 바꾸고 싶어하나요?

핀테크 기업들은 전자금융감독규정의 망분리 규정이, **망법처럼 중요한 정보를 지정해 분리하는 방식으로 바뀌길 원합니다.** 망법에서는 개인정보 취급 PC만 물리적으로 분리하고 있습니다. 이런 방식으로 개인정보의 중요도에 준하는 금융정보를 지정해 별도로 관리한다면 보안성도 해치지 않고, 기업의 효율성은 제고됩니다. 현재의 감독규정, 특히 5호는 오픈소스 활용을 통한 스타트업의 빠른 개발 사이클과 유리되어 있으며, 망분리에 의한 추가비용 역시 스타트업에게는 부담스럽습니다.

장기적으로는 사전규제 완화, 사후규제 강화를 통해 기업이 보안에 대한 책임과 권한을 갖길 바랍니다. 특정 기업에게 가장 효율적이면서도 안전한 보안 유지 방안은 그 기업이 가장 잘 알 수 있기 때문입니다. 그렇기에 사전규제 완화가 가능하다면 징벌적 손해배상 등도 불사하겠다는 입장입니다.

-> 자세한 내용은 47페이지 참고!

Q8.
기존 금융부문은 망분리 규제에 어떤 입장을 취하나요? 어떻게 대응하고 있나요?

기존 금융기업 역시 현재의 망분리 조항은 과도하다고 생각하나, 스타트업에게만 규제를 완화를 완화해 주는 건 불공정하다고 생각합니다. 최근에는 망분리 규제 중에서도 클라우드 도입을 위한 물리적 망분리 조항(5조)의 완화를 주목하고 있습니다. 금융당국에서는 19년 1월 중요시스템 역시 클라우드에 저장이 가능하도록 조치하는 문서를 내놓았지만, 금융회사들은 금융당국으로부터 '비조치의견서'를 받아가며 망분리에 신중한 행보를 보이고 있습니다.

-> 자세한 내용은 50페이지 참고!

Q9. 공공 부문은 망분리 규제에 어떤 입장을 취하나요? 어떻게 대응하고 있나요?

공공부문 역시 현재의 망분리 규정을 바꿔 나가고 있습니다. 정부는 물리적 망분리 도입의 선구자지만, **높은 비용 문제를 해소하고, 공무원의 컴퓨터 이용환경을 개선하기 위해 논리적 망분리를 추진 중입니다.** 행안부와 과기정통부가 선도부처로 우선 적용 후 타부처로 점차 확산할 계획이라고 합니다.

-> 자세한 내용은 50페이지 참고!

Q10. 해외에서는 망분리 규제 사례가 있나요?

해외에서도 망분리는 합니다. 하지만 해외의 금융/보안당국이 **민간에 일괄적으로 망분리를 의무화한 사례는 없으며, 일반적으로 망분리 채택 여부 및 범위 설정은 기업 자율에 맡기고 있습니다.** 해외 금융/보안당국은 강제성이 없는 가이드라인을 통해 기업의 환경에 맞게 망 세분화(segmentation)를 보안성 제고를 권유하는 것이 일반적이며, 망분리는 치명적이고 민감한 정보를 담고 있는 시스템에 적용할 수 있는 선택지 중 하나로 제시됩니다. 특히, 미국에서는 기업들이 중요도에 따라 데이터를 분류하는 많은 민간 표준을 참고해 어떤 기준으로, 어떤 방식으로 세분화하는 것이 기업의 자율적으로 선택합니다. **자율규제긴 하지만, 법정 분쟁 발생 시 표준의 준수 여부는 엄격하게 따진다는 점에서 구속력은 충분**합니다. 기업이 정보보호를 위한 최대의 노력을 기울이지 않았다는 점이 입증되면, 징벌적 손해배상 제도 등 사후규제로 인해 기업에 타격이 있을 정도로 휘청일 수 있기 때문에 보안에 대한 투자가 활발히 일어나게 됩니다.

-> 자세한 내용은 39페이지 참고!

Q11. 현재의 망분리 정책, 어떻게 바꾸면 가장 이상적일까요?

4차위 등 전문가집단에서는 현재의 업무망/인터넷망과 같은 **도메인 중심의 보안 정책은 데이터 중심으로 변경되어야 한다고 권고**합니다. 현재의 이분법적인 방식으로 오픈소스 활용, 클라우드 도입은 요원하기에, 4차산업혁명 시기에 부적합한 정책이기 때문입니다. 공공/민간/군사, 업무용/외부용 등 도메인 중심이 아니라 데이터를 보유한 기관들이 보유하고 있는 데이터들을 민감도, 치명도 등으로 분류해 관리하는 것은 쉽지 않은 과제지만, 장기적으로 데이터 활용에도, 보호에도 더 적합한 방식입니다.

-> 자세한 내용은 53페이지 참고!


Lan Cable

— 이슈미니 써머리 두번째 챕터 —

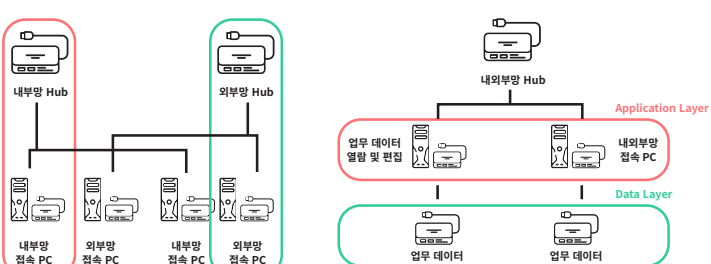
자세히 보는 이슈

망분리란?

망분리는 보안 기법의 일종으로, 외부의 공격으로부터 내부의 중요한 자료를 보호하기 위해 망을 연결하지 않고 분리(separate, isolate)해 두는 것을 의미합니다. 비슷한 개념으로 망 세분화/구역 설정(segmentation, zoning)이 있는데요, 라우터 등 네트워크 장비를 통해 하위 망을 구성하고 접근을 통제하나, 망 간 연결성이 유지된다는 점에서는 개념적으로 망분리와 다릅니다.

'망분리'는 어떻게 이해하면 될까요? '내부의 중요한 자료'를 다른 소중한 것, 예를 들면 비상금 같은 걸로 생각하시면 이해가 간편합니다. 보통 비상금은 현관에 팽개쳐 두는 게 아니라 아무도 모르는 곳에 어떤 곳에 따로 떨어져 숨겨져 있죠. 이렇게 다 열린 현관같은 인터넷 망도 필요하지만, 비상금을 숨길 땐 안방 옷장이라든가, 다른 사람들이 드나들지 못하게 자물쇠를 채워 둔 별도의 공간을 따로 마련하는 것이 좋겠죠. 비상금을 숨길 때 목적에 따라 하나는 장판 밑, 사전 속, 가방 안주머니 등등에 각각 나눠서 보관할 수 있는 것처럼, 정보의 중요도에 따라 망을 나눠서 사용할 수 있습니다. 미세먼지 경보처럼 널리 퍼져도 아무런 해가 없는 정보는 다들 볼 수 있는 곳에 두고, 원자력 발전소 시설 정보처럼 외부에 유출되면 큰일나는 정보는 따로 모아서 분리해 두는 방식입니다.

그렇다면 망분리는 어떻게 구현할까요? 기술적으로는 '물리적 망분리'와 '논리적 망분리' 두 가지 구현 방식이 있습니다. 물리적 망분리는 개인 당 여러 PC를 사용하는 방식입니다. 논리적 망분리는 소프트웨어를 통해 하나의 PC에서 여러 대의 PC를 구현합니다.



[그림 1] 물리적 망분리와 논리적 망분리

두 가지 방식에는 장단점이 명확합니다. '물리적 망분리'의 경우 물리적으로 다른 망을 사용하기 때문에 보안성이 높아지나 비싸고 업무 효율성 역시 저하됩니다. 중요정보의 경우 외부 인터넷이 차단된 망 내에서만 유통된다는 점에서 훨씬 안전하며, 이 자료를 다른 망으로 옮기기 위해서는 망연결 프로그램을 활용해야 하기 때문에 기록이 남아 관리에도 적합합니다. 하지만 일단 최소 PC 두 대에 연결 프로그램 등 각종 장비를 갖춰야 한다는 점에서 비싸고, 두 PC를 계속 오가야 한다는 점에서 업무 효율성이 저하됩니다.

망분리는 중요한 정보가 인터넷망에서 유통되지 않게 막는 효과적인 보안 방법이지만, 100% 안전한 방법이 될 순 없습니다. 물리적 망분리를 통해 망을 폐쇄해 놓아도 공격당한 사례는 많습니다. 2010년 스턱스넷 악성코드는 폐쇄망이었던 이란의 핵 시설을 공격했습니다. 직원이 무심코 주운 USB 저장장치를 들고 핵시설 안으로 들어갔고, 안에 있던 악성코드가 제어시스템에 설치됩니다 . 2 원전 제어시설을 감염시킨 스턱스넷은 원심분리기를 조작했고, 약 천개 이상의 원심분리기가 파괴되었습니다.

국내에도 망분리를 했음에도 해킹을 당하는 사례가 나타납니다. 2014년에는 한국수력원자력이 해킹당합니다. 당시 한수원을 공격한 해커는 메일에 악성코드가 포함된 한글파일을 첨부하고, 업무와 관련된 것처럼 메일 내용을 위장해 직원들이 이를 실행하도록 유도했습니다. 2016년에는 국방부도 해킹당합니다. 군사비밀을 포함한 일부 군사 정보가 유출되었으며, 북한 소행으로 추정된다고 밝혔습니다. 국방부는 이전까지 물리적 망분리를 통해 내부망을 엄격하게 관리했다며 해킹 가능성을 일축했지만, 공격으로 감염된 컴퓨터는 3200여 대인 것으로 알려졌습니다 . 3

이렇듯, 망분리는 하나의 보안 수단일 뿐이며, 절대적인 보안 대책으로 사용될 수 없습니다. 정당한 접근권을 가진 사람을 속여 암호를 해독하는 '사회공학적 해킹', 혹은 소요시간, 전력, 전자기파, 소리 등 암호체계의 구현과정 정보를 기반으로 공격하는 '부채널 공격(Side Channel Attack) 등 다양한 공격 가능성을 배제할 수 없습니다. 망분리가 되어 있어도 연결된 사용자와 기기가 점점 더 많아지며 공격 채널이 다양화된다는 점을 염두에 둬야 합니다. 보안에 있어서는 100% 안전을 장담하는 해법이 없으며, 가능한 위험성을 줄일 수 있도록 자원 배분을 통해 전반적인 보안 수준을 올리는 것이 보다 효과적입니다.

2 망분리 맹신 '큰 코 다친다' … 인터넷 연결 안돼도 PC 스피커로 자료 샌다
http://www.etnews.com/20150720000153

3 망분리 기술의 가장 큰 취약점은 사용자
http://www.cctvnews.co.kr/news/articleView.html?idxno=142992

망분리 정책의 경과

2006년 | 국가사이버안전전략회의, 망분리 최초 보고
2007년 | 망분리 시범사업(국무총리실, 통일부)
2008년 | 정부부처 중심 1차 망분리 사업
2009년 | 기재부 업무망 해킹(4월), 7.7 DDoS, 국가사이버위기종합대책(9월)
2010년 | 정부부처 중심 2차 망분리 사업

2011년 | 3.4 DDoS(일주일간 금융거래 마비)
2012년 | 정보통신망법 시행령 개정(개인정보 보유 PC 망 별도 분리)
2013년 | 3.20 사이버테러(2시간 동안 금융업무 중단)
2013년 | 금융전산 보안 강화 종합대책(7월), 전자금융감독규정 개정(업무망/인터넷망 분리)
2014년 | 금융회사 전산센터 망분리 완료
2015년 | 은행 본점, 영업점 망분리 완료
2016년 | 보험, 카드, 증권, 제2금융권 망분리 완료

2016년 | 전자금융감독규정 개정
(영업점 PC 논리적망분리, '비중요정보처리시스템'을 클라우드로 이관 가능, 이 경우 물리적 망분리 예외 적용)
2017년 | ATM 이용자 정보 유출
2018년 | 금융위 '금융권 클라우드 확대 방안'
2019년 | 전자금융감독규정 개정('중요시스템' 클라우드로 이관 가능)

[그림 1] 망분리 정책의 경과

1) 공공부문 중심의 망분리 도입

망분리 정책의 본격적인 시작점은 2006년입니다. 2006년 5월 국가사이버안전전략 회의가 열리고, 다음 달인 6월, '해외발 국가기관 해킹 실태 및 대처방안'이라는 문서가 발표됩니다. 이 문서에서 최초로 국가기관 업무전산망과 인터넷 분리 보고 방침이 언급되었고, 대통령께 보고됩니다.[4]

4 사용자가 고통 받는 망분리 의무화 개선사항은? https://www.boannews.com/media/view.asp?idx=37490&kind=1

2007년에는 망분리 시범사업이 시작됩니다. 1월에 국가정보보안기본지침이 발표되고 4월에는 국가/공공기관 업무전산망 분리 실무 매뉴얼이 배포됩니다. 5월에는 국가사이버안전대책회의에서 인터넷/업무망 분리대상 기관이 확정됩니다. 이를 근거로 국무총리실, 통일부가 국가기관 망분리 시범 사업을 추진합니다.

2008년~2009년에는 망분리가 정부부처 중심으로 확산됩니다. 5월에는 외교안보정책조정회의에서 국가기관 망분리 방안이 대통령 보고 후 확정되고, 2008년 9월에는 18개 국가기관 대상으로 1차 국가기관 망분리 사업이 시작됩니다. 2009년 4월에는 기획재정부 내부 업무망이 해킹당한 사건이 있어, 정부 부처 보안 강화를 위한 망분리 정책은 더욱 탄력을 받게 됩니다. 2010년에는 27개 기관 대상 국가기관 망분리 사업이 실시되고, 국가/공공기관 업무망과 인터넷 간 안전한 자료 전송 보안 가이드라인이 만들어집니다.

망분리 정책이 중앙정부을 넘어 지자체/공공기관으로 본격적으로 확장 적용된 계기는 2009년 7.7 DDoS 사건입니다. 미국 독립기념일을 겨냥해 전세계적으로 악성코드가 배포되었고, 국내 역시 주요 사이트들이 공격을 받고, 좀비 PC의 데이터가 파괴되는 등 큰 영향을 받았습니다. 이를 계기로 정부는 9월 '국가사이버위기종합대책'을 수립했으며, 중앙행정기관과 지자체에도 같은 망분리 정책이 확장됩니다.

2) 민간, 금융기관으로의 망분리 확산

연이은 대형 해킹사건으로 민간, 금융기관으로까지 보안을 강화해야 할 필요성이 확산됩니다. 2011년에는 3.4 DDoS라는 굵직한 사건이 터집니다. 청와대, 국민은행 등 40개 기관이 공격받아 약 820여대의 PC가 마비되고, 4월 12일 농협 전산망의 내부서버가 파괴되고, 일주일간 금융거래가 마비되었습니다. 2013년에는 3.20 사이버테러가 일어나 KBS, YTN, MBC 등 언론사는 물론 NH농협은행, 신한은행, 제주은행 등 금융사가 커다란 손상을 입고 약 두 시간 동안 금융업무가 중단됩니다.[5] 이 사태의 여파로 일반 민간 분야에도 망분리가 도입됩니다. 2012년 8월부터 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령에 의해 개인정보 보유 PC는 별도로 분리된 망을 사용하게 됩니다.

5 경찰, 3.4 디도스 공격 北소행 간주 https://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=105&oid=001&aid=0004996845

금융회사에도 망분리가 도입됩니다. 2013년 금감위는 7월 '금융전산 보안 강화

종합대책'을 수립하고, '전자금융감독규정'을 개정합니다 . 6 이에 따라 내부업무용 시스템은 망분리가 이뤄져야 하며(3조), 개발용 시스템은 물리적으로도 분리하게(5조) 됩니다. 금융회사 전산센터는 2014년, 은행의 본점과 영업점은 2015년, 보험, 카드, 증권, 제2금융권은 2016년까지 망분리가 이뤄지도록 했습니다.

3) 4차 산업혁명과 망분리 정책의 보완

망분리 논의가 본격적으로 시작한 지 10년이 지난 2016년부터는 변화하고 있는 산업 현장에 맞게 망분리 정책이 일부 개정됩니다. 2016년에 금융권의 망분리 규정이 일부 완화된 것이 대표적입니다. 영업점 PC의 경우 물리적 망분리 정책의 대상이었으나, 논리적 망분리로 충분해졌습니다. 신산업 활성화를 위해서도 망분리 정책이 보완되었습니다. 금융분야의 디지털화가 확산되며, 금융회사에서 클라우드 서비스의 도입에 대한 필요성을 외치는 목소리가 커집니다. 하지만 원격에서 서버에 접속하는 것을 전제로 하는 클라우드 서비스는 물리적 망분리 환경에서는 원천적으로 사용이 불가능합니다. 이에 2016년 금융위는 '비중요업무'에 한해 클라우드를 사용할 수 있게 했으며, 이렇게 클라우드를 사용할 경우 물리적 망분리에 대한 예외를 인정했습니다 . 7

6 **금융전산 망분리 의무화, 공동백업센터 구축한다** http://www.wowtv.co.kr/NewsCenter/News/Read?articleId=A2013071100087&resource=

7 **'클라우드 격동' 시작된 금융권… IT혁신과 보안 과제, 어떻게 극복할까** http://www.ddaily.co.kr/news/article/?no=183816

현재의 망분리 정책

1) 국내의 망분리 정책 : 정부 정책에 따라 망분리 일괄 채택, 사전규제 방식

국내에서 현재 망분리를 의무화하는 규정은 크게 3가지입니다. 공공영역에서는 국가정보보호기본지침, 민간에서는 정보통신망법, 금융부문에서는 전자금융감독규정을 준수해야 합니다.

> 3. "인터넷서비스망" (이하 "인터넷망"이라 한다)이란 진흥원의 네트워크 중에서 인터넷을 사용할 수 있도록 연결되어 있는 인터넷 전용망을 말한다.
>
> 4. "업무전산망"(이하 "내부망"이라 한다)이란 진흥원의 네트워크 중에서 내부 업무를 수행할 수 있도록 연결되어 있는 전산망을 말한다.

[그림 2] 공공영역의 망분리 사례
(한국콘텐츠진흥원 정보보안기본지침 발췌)

공공기관은 국가정보보호기본지침을 준용해 내부망과 외부망을 분리해 운영합니다.

> 제15조(개인정보의 보호조치) ② 법 제28조제1항제2호에 따라 정보통신서비스 제공자등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 다음 각 호의 조치를 하여야 한다. 다만, 제3호의 조치는 전년도 말 기준 직전 3개월간 그 개인정보가 저장ㆍ관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 정보통신서비스 제공자등만 해당한다. <개정 2012. 8. 17.>
> 3. 개인정보처리시스템에 접속하는 개인정보취급자 컴퓨터 등에 대한 외부 인터넷망 차단

[그림 3] 정보통신망법 시행령 15조

민간기업을 대상으로 하는 정보통신망법은 시행령에서 망분리를 언급합니다. 개인정보 유출사고를 방지하려는 목적이며, 파급력이 큰 기업, '이용자 수가 일일평균 100만명 이상'이거나 '전년도 매출액이 100억원 이상'인 정보통신서비스 제공자에 한해 적용됩니다. 이들 기업은 개인정보처리시스템에 접속하는 개인정보취급자 컴퓨터 등에 대한 외부 인터넷망 차단을 해야 하지만, 물리적인 방법과 논리적인 방법 중 선택이 가능합니다. 개인정보를 다루지 않는 컴퓨터라면 망분리를 하지 않아도 된다는 이야기입니다.

전자금융감독규정 15조

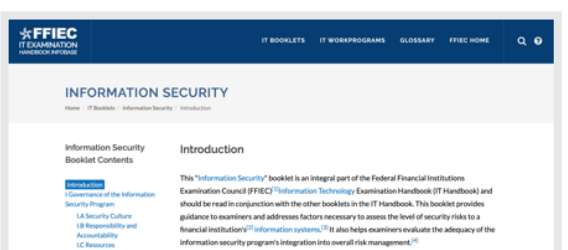
제15조(해킹 등 방지대책) ① 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운용하여야 한다.
3. 내부통신망과 연결된 내부 업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속 금지(단, 업무상 불가피하여 금융감독원장의 확인을 받은 경우에는 그러하지 아니하다)
<개정 2013. 12. 3.>
5. 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리할 것(단, 업무 특성상 분리하기 어렵다고 금융감독원장이 인정하는 경우에는 분리하지 아니하여도 된다.)
<신설 2013. 12. 3., 개정 2015. 2. 3.>

[그림 4] 전자금융감독규정 제 15조 제1항 제3호, 제5호

하지만 금융거래 정보유출, 금융서비스 마비, 금융사고 방지 등 좀 더 넓은 목표를 가진 전자금융감독규정은 좀 더 복잡합니다. 금융회사·전자금융업자는 감독규정 제15조 제1항 제3호와 제5호 의해 망분리를 해야 합니다. 3호는 '내부 업무용시스템은 인터넷과 분리·차단 및 접속을 금지'한다는 내용이며, 5호는 '전산실 내 단말기 또는 데이터센터 내 서버에 직접 접속하는 단말기는 인터넷 등 외부통신망으로부터 물리적으로 분리'해야 한다는 내용입니다. 이에 따르면, 영업점 등의 단말기는 논리적 망분리로도 충분하지만, 개발/운영을 위한 단말기는 무조건 물리적 망분리를 해야 합니다.

2) 해외의 망분리 정책 : 데이터 중요도 따라 민간이 결정, 사후규제 방식

해외에서도 망분리는 흔히 사용되는 보안 수단이지만 망분리 도입 여부와 적용범위는 기관, 기업이 결정하는 것이 일반적입니다. 데이터의 중요도에 따른 데이터 분류에 관한 표준이나 가이드라인이 많으며 쉽게 나와 있어, 기업이 이를 참고해 자발적으로 보안 정책을 설정하게끔 조치하는 것입니다. 자율적으로 규제하지만, 정보보호 수준은 도리어 높습니다. 집단소송제, 징벌적 손해배상제 등 강력한 사후처방으로 인해 정보유출을 한 기업에게는 소송의 부담, 영업이익에 차질이 생길 만큼의 과징금이 부과되기 때문입니다. 이 때 개인정보유출 등 법정 분쟁 발생시 표준의 준수 여부를 중요하게 검토하므로, 표준 자체에 강제성은 없지만 기업 입장에서 표준에 따른 정보보안 정책 설정은 필수입니다.



[그림 5] 미연방금융기관 검사협의회 홈페이지

8 **미연방금융기관 검사협의회**(Federal Financial Institutions Examination Council, FFIEC) : 5개의 은행 규제 기관으로 구성된 미국의 정부간 기관으로, 금융관 간 원칙, 표준, 보고서 양식 간 균일성 확보 등이 목적

미국의 연방금융기관 검사협의회(FFIEC) 8 는 망분리 방식을 우리나라처럼 강제하지 않습니다. 기업과 감사역이 정보시스템의 보안 수준을 측정하는 데 필요한 요소를 제시하고, 정보보안 프로그램의 전반적인 리스크 관리 수준의 적합도를 측정할 수 있게 도와주는 '정보보안 소책자(Information Secu-rity Booklet) '9 의 네트워크 통제(Network Controls)부분을 살펴 보겠습니다.

데이터의 중요도에 따라 망을 나누고 접근을 통제하는 세분화(zoning)에 대해 설명하고 있을 뿐, '인터넷을 차단한다'는 의미에서의 망분리에 대한 언급은 찾을 수 없습니다. 치명적이거나 민감한 정보를 기준으로 망을 나누거나 접근을 제한한다는 일반적인 원칙을 제시하면서도, 각 회사의 사정에 맞게 이를 달리 적용하도록 유연하게 접근합니다.

[Action Summary]

Management should secure access to computer networks through multiple layers of access controls by doing the following:

- Establishing zones (e.g., trusted and untrusted) according to the risk profile and criticality of assets contained within the zones and appropriate access requirements
  within and between each security zone.
- Maintaining accurate network diagrams and data flow charts.
- Implementing appropriate controls over wired and wireless networks.

[조치 요약]

경영진은 다음을 시행함으로써 다양한 층위의 접근 통제를 통해 컴퓨터 네트워크로의 접근을 보호해야 한다

- 구역 내 위험 수준과 자산의 치명도에 따라 (신뢰와 비신뢰구간 등)의 구역을 설정하고 각각의 보안 구역 사이와 내부에 적절한 접근 요건을 설정한다.
- 정확한 네트워크 구성도와 데이터 흐름도를 유지해야 한다

[그림 6] **FFIEC Information Security Booklet, II.C.9 Network Controls**

9 **FFIEC**(미연방금융기관 검사협의회 IT 핸드북 정보보안 부분)
https://ithandbook.ffiec.gov/it-booklets/information-security/introduction.aspx

[그림 7] 호주 사이버보안센터, '망 세분화와 망분리 도입하기 (Implementing Network Segmentation and Segregation)'

호주 보안당국 역시 망분리를 의무화하지 않으며, '민감한 환경', 즉 데이터가 중요할 경우에 기업이 망분리 도입을 고려해 볼 수 있다고 언급합니다. 호주 사이버보안센터(Australian Cyber Security Center, ACSC)는 2019년 4월, 기업에게 다양한 망분리 정책들을 제시해 기업의 보안성을 향상시키는 것을 돕기 위해 '망 세분화와 망분리 도입하기(Implementing Network Segmentation and Segrega-tion) '라는 문서를 배포합니다. 이 문서의 목적은 기업이 망 세분화와 망분리 정책을 세우도록 도움으로써, 단 한번의 침입으로 모든 정보에 대한 접근이 열리는 상황을 방지하는 것입니다. 기업은 라우터나 방화벽을 활용하는 등 다양한 방법을 선택해 망 세분화를 한다는 강제성 없는 권고가 주 내용이며, '망분리'는 특히 민감한 환경에서 기업이 선택할 수 있는 강력한 수단으로 언급됩니다.

Apply technologies at more than just the network layer. Each host and network should be segmented and segregated, where possible, at the lowest level that can be practically managed. In most cases, this ap-plies from the data link layer up to and including the application layer; however, in particularly sensitive environments, physical isolation may be appropriate. Host-based and network-wide measures should be deployed in a complementary manner and be centrally monitored. It is not sufficient to simply implement a firewall or security appliance as the only security measure.

네트워크 계층 외의 다른 곳에도 기술을 적용하라. 각각의 호스트와 네트워크는 실용적으로 관리될 수 있는 가능한 가장 작은 단위로 세분화되어야 한다. 대부분, 데이터링크 계층부터 어플리케이션 계층까지 적용이 가능하다. 하지만, 특별히 민감한 환경에서는, 물리적 망분리가 적당할 수 있다. 호스트 기반 방법, 네트워크 전반에 적용되는 방법이 보완적으로 적용되어야 하며, 이를 중심에서 감독해야 한다. 유일한 보안 방법으로 방화벽이나 보안 프로그램을 적용하는 것은 충분치 않다.

[그림 8] 호주 사이버보안센터, '망 세분화와 망분리 도입하기 (Implementing Network Segmentation and Segregation)' 중

[그림 9] PCI-DSS 범위 설정(scoping) 및 망분할 가이드(Guidance for PCI DSS Scoping and Net-work Segmentation)

기업들이 자발적으로 지키는 민간 표준에서도 망분리의 위상은 비슷합니다. 신용카드업계의 민간표준인 PCI DSS 에서도 카드사용자정보를 다루는 등 특수한 상황에 적용할 수 있는 선택지로서 망분리가 언급됩니다. PCI-DSS는 전체적인 데이터 흐름의 파악과 사용자 권한 통제를 통해 위험도를 낮춘다는 목적을 달성하는 데 초점을 맞추기 때문에, 망분리, 망세분화 도입 시 기업이 어떤 이점을 누릴 수 있는지, 어떤 기준으로 도입하면 좋을지 설명합니다.

Network Segmentation

Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of an entity's network is not a PCI DSS requirement. However, it is strongly recommended as a method that may reduce:

- The scope of the PCI DSS assessment
- The cost of the PCI DSS assessment
- The cost and difficulty of implementing and maintaining PCI DSS controls
- The risk to an organization (reduced by consolidating cardholder data into fewer, more controlled locations) Without adequate

망 세분화

카드사용자 데이터 환경을 한 조직의 다른 네트워크와 세분화, 혹은 분리하는 것은 PCI DSS 요구사항이 아니다. 하지만 다음의 사항을 줄일 수 있는 방법으로 강력히 추천된다.

- PCI DSS 평가 범위
- PCI DSS 평가 비용
- PCI DSS 제어방식을 도입하고 설계하는 난이도와 비용

[그림 10] PCI-DSS 범위 설정(scoping) 및 망분할 가이드 (Guidance for PCI DSS Scoping and Net-work Segmentation) 중

한편, '망 세분화' 등 하나의 조치만으로 모든 위험을 해결하려는 방법론을 경계하는 문구도 보입니다. 이렇게 PCI DSS는 강력한 수단을 어떻게 하면 잘 활용할 수 있는지 알려주는 동시에, 단 하나의 수단에만 의존하는 것을 경계하고 가능한 모든 수단을 동원할 수 있도록 돕습니다. 전사적으로 인프라의 보안 수준을 끌어올리고 위험도를 줄인다는 목적에 집중하고 있기 때문입니다.

While segmentation may help reduce the number of exposure points to the cardholder data environment (CDE), it is not a silver bullet; implementing segmentation is no replacement for a holistic approach to securing an organization's infrastructure.

망 세분화는 '카드소유자의 데이터 환경(CDE)' 접근 경로 수를 줄이는 데 도움이 될 수 있지만, 만능은 아니다. 망 세분화는 한 조직의 인프라를 안전하게 하기 위한 전사적 접근의 대안이 될 수 없다.

[그림 11] PCI-DSS 범위 설정(scoping) 및 망분할 가이드(Guidance for PCI DSS Scoping and Net-work Segmentation) 중

NIST Special Publication 800-53 (Rev. 4)

Security and Privacy Controls for Federal Information Systems and Organizations

[그림 12] NIST Special Publication 800-53 (Rev. 4)

규제기관이 아닌 미국 국립표준기술연구소(NIST, National Institute of Standards and Technology)이 공공기관을 대상으로 발행한 가이드라인이 취하는 입장 역시 비슷합니다. '연방정부 정보시스템과 기관을 위한 보안, 개인정보 통제(Security and Privacy Control for Federal Infor-mation Systems and Organization)이라는 부제를 달고 있는

특별간행물(Special Publication) 800-53을 보겠습니다. 이 문서는 국방 외 전 분야의 미 연방 정보 시스템이 정보보안 관련 법규를 보다 확실히, 효율적으로 지킬 수 있도록 돕는 것을 목적으로 합니다.총 18개로 나눈 제어범위 중 '시스템과 커뮤니케이션 보호(System and Communications Protection) 부분 발췌를 보면, 해당 가이드라인은 공공부문에 망분리/망세분화 도입을 권고하면서도 '어떤 정보를, 어떤 목적 혹은 기능을 위해' 분리할지는 각 기관의 재량에 맡기고 있습니다.

SC-7(21) BOUNDARY PROTECTION | ISOLATION OF INFORMATION SYSTEM COMPONENTS

The organization employs boundary protection mechanisms to separate [Assignment: organization-defined information system components] supporting [Assignment: organization-defined missions and/or business functions].

Supplemental Guidance: Organizations can isolate information system components performing different missions and/or business functions. Such isolation limits unauthorized information flows among system components and also provides the opportunity to deploy greater levels of protection for selected components. Separating system components with boundary protection mechanisms provides the capability for increased protection of individual components and to more effectively control information flows between those components. This type of enhanced protection limits the potential harm from cyber attacks and errors. The degree of separation provided varies depending upon the mechanisms chosen. Boundary protection mechanisms include, for example, routers, gateways, and firewalls separating system components into physically separate networks or subnetworks, cross-domain devices separating subnetworks, virtualization techniques, and encrypting information flows among system components using distinct encryption keys.

경계 보호 | 정보시스템 요소 분리

기관은 [과제 : 기관이 정의한 미션 혹은 업무 기능]을 지원하는 [과제 : 기관이 정의한 정보시스템 요소]를 분리하는 경계 보호 메커니즘을 도입한다.

보조 가이드 : 기관은 각기 다른 미션과(혹은) 업무 기능을 수행하는 정보 시스템 요소를 분리할 수 있다. 이렇게 분리함으로써 시스템 요소 간 허가되지 않은 정보의 흐름을 제한할 수 있으며, 특정 요소에 대한 보호를 강화할 수 있다. 경계 보호 매커니즘을 통해 시스템 요소를 분리함으로써 각 요소의 보호 수준이 올라가고, 이러한 요소 간 정보의 흐름을 효과적으로 통제할 수 있게 된다. 이렇게 보안이 강화되면 사이버 공격과 오류로 인해 입을 수 있는 피해가 제한된다. 분리 정도는 선택된 메커니즘에 따라 다양하다. 경계 보호 메커니즘에는 시스템 요소를 물리적으로 분리된 네트워크 혹은 서브네트워크로 나누는 라우터, 게이트웨이, 방화벽, 서브네트워크를 나누는 교차 도메인 장비나, 가상화 기법, 구별되는 보안 키를 활용한 시스템 요소 간 정보 흐름 암호화 등이 있다.

[그림]13 NIST Special Publication 800-53 (Rev. 4), Security and Privacy Controls for Federal Information Systems and Organizations SC-7 BOUNDARY PROTECTION

이렇듯, 해외에서 일반적으로 망분리 도입 여부와 범위 설정은 기업/기관 단위 자율이며 의무사항이 아닙니다. 하지만. 수많은 표준 기관이 권고했듯, 기업 역시 망분리/망세분화가 강력한 보안 수단임을 알고 자체적으로 망분리 도입을 결정하기도 합니다. 다만, 데이터를 자체적으로 중요도에 따라 나눈후, 그 중요도 등급별로 망분리가 이뤄집니다. 심한 경우, 비밀을 다루는 직원의 경우 책상에 6~7대의 PC를 놓아 두기도 합니다. 각 등급별로 망이 분리되어 있고 각 망에 PC가 한대씩 연결돼 있다는 얘기입니다. 이때 기밀이 아닌 일반 업무 데이터 망은 인터넷과 연결되어 있습니다. 이렇게 PC가 6~7대나 있어도 불편함을 못 느끼는 이유는 기밀자료에 접속하는 일이 극도로 드물기 때문입니다. 그러나 우리나라는 업무망과 안터넷망을 분리시켰기 때문에 필요할때마다 복잡한 절차를 거쳐 망을 다시 연결시켜야 하고, 그러다가 해킹 사고가 발생할 경우 피해가 커지게 됩니다.

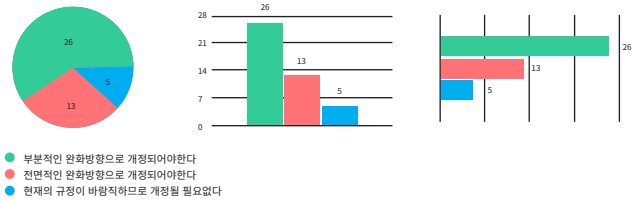
이렇게 미국 금융회사의 경우 사전규제를 유연하게 적용받고 있지만 보안사고가 일어날 경우 집단소송과 징벌적 손해배상으로 혹독한 대가를 치를 수 있기에 보안에 대한 투자를 게을리하지 않습니다. 대표적인 사례가 19년 7월에 있었던 캐피털원 해킹 사고입니다. 해킹으로 인한 모든 처리 비용을 더하면 최대 1억5000만달러(1773억원)에 이른다고 합니다. 사전에 규제를 적용받지 않아도 치명적인 결과가 있을 수 있다는 점에서 미국 금융회사들은 보안에 점점 더 많은 투자를 하고 있습니다. 비트디펜더 백서에 의하면, 미국 금융회사의 보안 투자가 점점 증가하고 있으며 많게는 보안 비용을 1조원 이상(1 Billion USD) 지출하는 회사까지 나타났다고 합니다 .

이해당사자별 입장

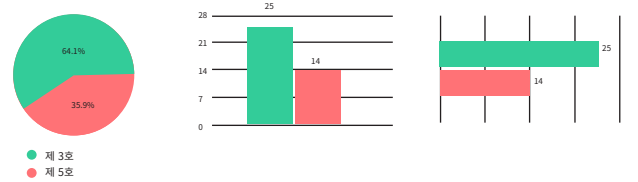
1)[핀테크 스타트업] 망분리 적용 범위가 명확했으면… 장기적으로는 자율규제 희망

핀테크 기업들은 전자금융감독규정의 망분리 규정이, 망법처럼 중요한 정보를 지정해 분리하는 방식으로 바뀌길 원합니다. 대부분의 핀테크 기업들은 금융인프라의 특수성과 소비자 보호를 고려해 치명적이거나 민감한 정보에 대해 현재의 망분리 규제가 적용될 수 있다는 점을 이해합니다. 하지만 '전자금융업자'라는 이유만으로 개발용 단말마저 망분리를 적용 대상이라는 점에 이의를 제기합니다. '내부 업무용 시스템'이'라는 현재의 모호한 법령은 준수하기도 어렵기에, 정보통신망법처럼, 지켜야 하는 중요한 정보를 명시하는 방식으로 바뀌었으면 하는 겁니다.

9. 전자금융감독규정의 망분리 관련 조항에 대해 다음과 같은 의견이 있는데, 이러한 의견에 대해 어떻게 생각하십니까?



10. 전자금융감독규정의 망분리 관련 조항에 대해 전면적 또는 부분적 개정/완화에 찬성하시는 경우, 어떤 조항이 우선적으로 검토될 필요가 있다고 생각하십니까? 전자금융감독규정 제 15조제1항제3호 "내부통신망과 연결된 내부업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리, 차단 및 접속 금지" 전자금융감독규정 제 15제1항제5호 "전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등외부통신망으로부터 물리적으로 분리할 것"



[그림 14] 한국핀테크산업협회 전자금융감독규정 망분리 관련 설문 결과

핀테크산업협회가 실시한 설문의 응답에 따르면, 전자금융감독규정의 망분리 규정을 개정해야 하는 가장 큰 이유는 업무생산성 저하입니다. 2019년 6월 10일부터 19일까지 한국핀테크산업협회, 오픈서베이가 함께 실시한 조사 결과, 설문에 응답한 44개 회원사 중 88.6%가 망분리 완화 의견에 찬성하였고, 11.4%는 유지하자는 의견을 보였습니다. 핀테크 스타트업이 감독규정의 망분리 규제완화를 희망하는 이유는 첫 번째로 업무생산성의 저하, 두 번째로 비용 부담이 꼽혔습니다. 또한 망분리 조항 중에서도 제3호 개정의 필요성이 64.1%로 제5호 개정 의견(35.9%)보다 두 배 가까이 높게 나왔습니다.

현재 전자금융감독규정의 망분리 규정의 어떤 점이 현재 핀테크 업체의 운영 현황과 유리된 걸까요? 핀테크 기업들은 현재의 망분리 정책은 기업 문화와 일하는 방식, 업무환경과 조직구조를 고려하지 않은 방식이며, 특히 개발환경에 있어서 큰 비효율이 발생한다고 이야기합니다. 지금의 방식으로는 최근 개발 환경의 필수요소인 오픈소스, API 등 라이브러리 활용이 어렵습니다. github, stack over-flow 등의 대표적인 오픈소스 개발자 커뮤니티에는 수십조의 연구개발비로도 못 해내던 프로젝트들의 소스코드가 무료로 개방되어 있습니다. 개발자는 이를 활용해 빠르고 유연하게 새로운 제품과 서비스를 만들고, 이를 이용한 결과물을 외부에 공개함으로써 다시 개발자 커뮤니티에 기여합니다. 망분리 환경으로 이렇게 자원 활용을 어렵게 하는 것은 스타트업들의 주무기인 속도와 유연성을 빼앗는 것과 마찬가지입니다. 업무생산성이 많게는 50% 이하로 떨어진 사례도 있습니다. 개발속도 저하를 상쇄하기 위해 개발부문 인건비 역시 30%정도 더 많이 지출합니다. 가뜩이나 스타트업에서 개발자 채용은 쉽지 않은데, 이마저도 인터넷이 차단된 환경에서 개발환경을 마련하고 견디는 스트레스 때문에 개발자들이 핀테크 분야를 기피하거나 이탈한다는 얘기마저 나오고 있습니다.

망분리를 위한 추가적인 투자 비용 역시 핀테크 스타트업에게는 부담입니다. 망을 분리해야 하므로 기본적으로 네트워크 장비, PC, 보안시스템, 소프트웨어 라이선스 등에 2배의 비용이 들어가며, 분리된 망 사이의 정보교환을 위한 망연계시스템을 도입하는 데에도 대략 1억원의 비용이 수반됩니다. 최근 사례를 보면 25명 규모의 스타트업에게 망분리를 위한 추가비용이 대략 5억원

수준입니다. ISMS 인증과 컨설팅 등 기본적인 정보보안관리체계 수립에 필수적인 보안투자는 상대적으로 비용이 적게 들지만 전자금융감독규정의 망분리 규정 때문에 오히려 후순위로 밀리는 경향도 있습니다.

장기적으로 자발적인 보안 강화 문화를 구축하는 데도 악영향을 끼칩니다. 위험평가에 근거한 보안관리가 아니라 체크리스트 기반의 보안통제문화가 조성되기 때문입니다. 체크리스트, 즉 규제에 해당하지 않은 사항에 대해서는 소극적으로 투자하게 되어 결과적으로는 정보보안수준의 저하로 이어질 위험성이 늘어납니다. 정보보호가 제대로 이뤄지기 위해서는 각 기업의 상황에 맞게 예방, 탐지, 대응, 복구의 연관성을 종합적으로 고려해 보안통제를 적용하고 관리프로세스를 정립해야 합니다. 그런데, 인터넷 연결을 차단하는 접근방법은 예방에만 치중하고 있는 방식입니다.

하지만 현재의 전자금융감독규정의 망분리를 하지 않게 되면 보안이 훨씬 약해지는 건 아닐까요? 망분리 시행 이후 사고가 줄었다며 망분리 유지를 주장하는 규제당국의 논리에도 핀테크 업체들은 반론을 제시합니다. 실제로 보안사고가 줄어든 건 맞지만, 전자금융감독규정을 받는 금융기업보다, 정보통신망법의 적용을 받는 일반 기업들이 훨씬 많다는 점을 감안해 결과를 해석해야 한다는 것입니다. 전체적으로 사고가 줄었다는 것은, 정보통신망법 수준의 망분리(개인정보를 보유한 PC만 분리) 역시 충분한 효과가 있다는 증거입니다. 그렇기에 전자금융감독규정의 강도 높은 망분리 수준은 불필요하며, 정보통신망법과 같은 방식의 망분리로 완화해도 위험도가 대폭 증가하지 않는다는 겁니다.

이에 그치지 않고, 핀테크 스타트업들은 보안에 대한 책임 역시 강하게 지겠다는 입장입니다. 앞선 핀테크산업협회의 조사에서 핀테크 스타트업의 70%는 “필요하다면 특정 분야에서 금융회사들보다 더 높은 수준의 보안통제를 적용하겠다”고 응답하며, 보안투자에 적극적인 의사도 동시에 표현했습니다. 실제로 핀테크 기업들은 고객이 가진 보안에 대한 우려를 불식하기 위해 큰 노력을 기울이고 있습니다. 특히, 12개 회원사의 경우 이미 신용카드업계의 민간표준인 PCI-DSS 인증을 취득해 은행, 증권 등 다른 금융회사에 비해 월등하게 높은 수준임을 보여주고 있습니다. 그럼에도 불구하고 망분리 규정

위반이라는 일부 사안으로 제재를 받을 경우, 핀테크 산업 전반의 보안수준에 대한 고객의 불신이 초래되고, 산업에 치명타가 될 수 있다는 점을 우려하고 있습니다.

심지어 징벌적 손해배상제를 강화하자는 의사를 밝히는 핀테크 기업도 있습니다. 최종책임을 지면서 기업이 가장 안전한다고 여기는 보안기술과 보안통제 방법을 선택하고, 보안에 지속적으로 더 많이 투자하도록 유도해 가는 것이 4차산업혁명 시대에 맞는 선택이라는 겁니다. 미국에서 발생한 1억 명의 신용정보 유출사고를 보더라도 해킹사고를 막는 일은 특정 방식으로 해결할 수 있는 문제가 아닙니다. 기업이 책임을 지고 빠르게 변화하는 환경에 대비해 위협에 대응하는 방식을 스스로 구축해 나가는 것이 합당하다는 것입니다. 대신, 정보보안과 개인정보보호가 미비했을 때 최종적인 책임도 진다는 입장입니다. 전자금융거래법, 정보통신망법, 개인정보보호법 등 국내 법률이 정한 과징금의 수준은 유럽의 개인정보보호법(GDPR)이 정하고 있는 기업 전체 매출액의 4%라는 벌금에 비해서는 매우 작습니다.

2)[금융회사/공공부문] 클라우드 도입을 위한 물리적 망분리 완화부터

금융회사들도 현재의 망분리 규정이 과도하다는 점에는 동의합니다. 하지만 핀테크업체에만 규제를 완화해주는 건 형평성에 어긋난다고 여깁니다 . 또한, 망분리 규제 완화를 주장하는 초점 역시 살짝 다릅니다. 업무 비효율 문제가 아니라, 클라우드 도입을 위해 '물리적 망분리' 조항에 대한 개정이 필요하다는 입장을 주로 취하기 때문입니다. 금융회사는 역시 전자금융감독규정으로 인해 물리적 망분리를 따라야 하기 때문에 자동적으로 클라우드를 도입할 수 없었습니다. 같은 그룹이라고 해도 IT자원(서버, 스토리지, 네트워크 등)이 별도로 필요하기 때문에 IT 운영비가 만만치 않았고, 그룹 내 데이터의 흐름 역시 자유롭지 못했습니다.

하지만 2019년 1월 금융당국이 '금융 클라우드 이용 확대'방안을 발표해 숨통이 트이기 시작합니다. 우리금융그룹은 비조치의견서를 통해 2019년 '그룹 공동 클라우드 구축'을 목적으로 '논리적 망분리'를 할 수 있게 되었습니다. 이로 인해 IT 운영비용 절감은 물론 업무의 효율성 역시 상승할 것으로 전망하고

있습니다. 신한금융그룹, KB금융그룹 등 타 금융회사도 클라우드 도입에 촉각을 기울이고 있었던 만큼, 비조치의견서 결과를 바탕으로 클라우드 도입이 촉진될 것으로 예상됩니다.

비조치의견서로 인해 클라우드 활용을 위한 '물리적 망분리' 제한은 일부 풀린 셈이긴 하지만, 금융당국에서 의견을 얼마나 효율적으로 처리할지는 두고 봐야 할 문제입니다. '비조치의견서'는 금융회사가 금융당국에게 신규사업이 문제가 없는지 미리 확인을 받는, 일종의 '규제샌드박스' 같은 제도입니다. '비조치의견서'는 홈페이지에 공개되어 다른 금융회사들도 확인할 수 있게 되어 있지만, 신중한 금융권의 특성상, 클라우드 전환 시 시스템이 망분리 요건에 해당되는지 여부를 금융당국에 질의하는 빈도수가 높아지고 있다고 합니다. 금융사들의 질의가 많아질수록 금융당국 역시 답변에 시간에 걸립니다.

공공부문은 금융회사와 입장이 비슷합니다. 역시 클라우드 등 IT 기술 도입에 있어 물리적 망분리가 발목을 잡고 있기 때문입니다. 한국은 2010년부터 전자정부평가 1위를 달성한 'IT강국'이지만, 인공지능, 클라우드 중심 디지털 전환에 대한 대처가 늦어지고 있습니다. 기존의 PC 환경을 중심으로 한 규제환경 때문에 모바일 환경 적응이 늦어지고 있기 때문인데, 이에 대한 대표적인 사례가 '물리적 망분리' 규정입니다. 현재도 공공부문에서는 보안을 이유로 물리적 망분리를 의무화하고 있으며, 데스크톱(PC) 두 대를 이용합니다.

4차산업혁명에 대응하기 위해 공공부문에서도 물리적 망분리를 논리적 망분리로 완화하려는 움직임이 생겨나고 있습니다. 행안부는 국가정보원, 과학기술정보통신부 등과 협의를 거쳐 두 대 PC를 한 대 노트북으로 대체하는 논리적 망분리를 내년부터 추진합니다. 이로 인해 공무원 컴퓨터 이용환경이 대폭 개편될 예정입니다. 주요 문서 등을 클라우드에서 관리해 외부에서도 모바일 등으로 시스템에 접속해 업무 처리가 가능해질 예정입니다. 행안부와 과기정통부가 내년 선도부처로 우선 적용 후 타부처로 점차 확산할 계획이라고 합니다.

3) [금융당국] 금융산업의 특수성을 고려한 사전규제는 불가피

금융당국은 금융혁신과 소비자보호를 모두 고려해야 하기에 신중한 입장을 취하고 있습니다. 먼저 금융분야의 특수성을 고려해 일정수준의 사전규제는 불가피하다는 입장입니다. 금융분야의 경우 ICT 분야와 다르게 정보유출 등 피해 발생시 단순 프라이버시 차원의 문제가 아닌 국민의 재산상 피해, 금융안정 등의 치명적인 문제가 생길 수 있기 때문입니다. 더욱이 국내 금융분야는 네트워크 연계성, 상호의존성(Interconnectedness)이 강해 금융사고 발생시 금융 기반시설 전반에 영향을 끼칠 수도 있습니다. 사후규제로 해결하기에는 사안이 심각해질 수 있다는 것입니다. 한편, 개별 기업의 책임 확대로는 해결될 문제가 아니라는 방어적인 입장 역시 취하고 있습니다. 금융회사 등은 보안을 투자가 아닌 비용으로 인식하고, 스스로 금융보안을 강화하는 관행•문화가 아직 미성숙하다는 지적 역시 함께 내놓았기 때문입니다.

하지만 변화하는 금융환경에 발맞춰 현장의 의견 지속적으로 청취하고 수용하겠다는 입장도 함께 내놓았습니다. 대표적인 것이 15년에 일부 물리적 망분리의 예외를 인정해 일부 금융사의 물리적 망분리를 인정한 사례입니다. 업무상 대외 기관과 연결이 불가피(금융공동망 연결, 정부 또는 금융 유관기관과 연결 등)하거나 비상시 업무처리 등의 경우 물리적 망분리를 예외로 인정한다는 내용입니다. 또한 19년 1월에는 '금융 클라우드 이용 확대 방안'을 통해 클라우드 이용시 물리적 망분리 예외를 인정했습니다. 클라우드 이용 범위를 개인신용정보까지 확대해, 인터넷 접속이 필요한 클라우드의 망분리 예외를 인정한 것입니다.

현장의 의견을 수렴하려는 금융당국의 움직임은 점차 빨라지고 있어 2020년에도 핀테크 기업을 위한 전향적인 정책들이 나올 것으로 기대됩니다. 19년 12월 11일 플라자호텔에서 개최한 컨퍼런스에서 금융감독원 IT핀테크전략국 정기영 부국장은 현재 검토되고 있는 2020년 주요 금융 IT감독 개선 방안에 대해 소개했습니다 . 그 중 클라우드 서비스 확대에 따른 망분리 규제의 발전적 개선방안을 모색할 계획이라고 밝혔습니다. 산업 발전을 위한 업계의 의견과 정보보호를 통한 소비자 보호가 조화된 균형점을 찾을 수 있을지 귀추가 주목됩니다.

4) [학계/전문가] 망분리 규제는 역행… 도메인이 아닌 데이터 중심 보안체계 필요

보안업계에서도 망분리 만능론에 대한 회의감이 짙어지고 있습니다. 홈네트워크의 안전을 위해 '세대간 망분리' 규정이 채택된 데 있어 한국정보보호산업협회 관계자는 "망분리만으로는 해킹을 막을 수 없다"면서 "홈네트워크 해킹 사고를 예방하기 위해 추진되고 있는 세대 간 망분리 기술은 만능이 아니며, 특정기술을 지정하면 오히려 보안 취약성을 초래할 수 있다"고 지적했습니다. "안전한 홈네트워크를 자율적으로 구축하도록 한 후 안전 점검이나 사후 검증할 수 있는 체계나 보안 등급제를 실시하는 것이 좋은 방향"이며, 행정규칙 '지능형 홈네트워크 설비 설치 및 기술기준'에 보안성 항목을 넣더라도 특정 기술 명시는 금지해야 한다는 것입니다. 대신 전문가 검증 후 등급만 매겨 시장의 자율적 선택을 보장하고, 만약 사고가 발생하면 주택 및 통신사업자의 책임을 강화하는 방향의 입법이 바람직하다는 의견입니다.

2019년 8월에 있었던 망분리 간담회에서도 현재의 망분리 정책은 산업 발전 현황에 맞지 않는 구시대적 정책이라는 언급이 있었습니다. 망분리 정책이 도입될 당시에는 업무에 제한적으로 컴퓨터가 사용되었기에 도입하는 것이 적절했지만, 지금은 4차산업혁명 시대에 맞는 새로운 보안 정책이 필요하다는 의미입니다. 이석윤 서울대 수리과학부 객원교수는 "현재 금융기관의 정보처리 시스템은 처음부터 옷장의 옷들이 그 가치별로 분류돼 보관된 것이 아니라 그때 그때 필요한 옷들을 구입해 옷장 속에 넣고 사용하고 있어 중요한 옷과 덜 중요한 옷들이 함께 섞여있는 상황"이라면서 "금융기관 물리적 망분리 정책을 전환할 때는 데이터 중요도에 따라 정보 시스템을 분류하고 적정 등급에 따른 다중 보안대책을 마련해야 한다"고 제언했습니다.

[그림 15] 4차산업혁명 대정부 권고안 권고문

4차산업혁명의 국내 도입을 위한 대통령직속 4차산업혁명위원회의 활동 결과문서인 '대정부 권고안 '에 서도 개선되어야 할 규제로 현재의 '망분리' 정책이 언급되었습니다. 사이버 보안부분의 핵심 내용은 '도메인 중심에서 데이터 중심으로 사이버 보안 정책이 전환되어야 한다는 것이었으며, 현재의 도메인 중심 보안 정책의 대표적인 사례로 지적된 것이 망분리 정책입니다. '모든 것이 네트워크에 연결되어 있고, 데이터는 활발하게 공유•활용되어야 한다'는 4차 산업혁명의 기본철학과 상충되며, 관련 산업 육성에도 걸림돌이 되기 때문입니다.

현재의 '도메인 중심' 망분리 정책은 사용성과 보안성을 동시에 악화시킨다는 점에서 문제가 있습니다. 도메인 중심 분류는 인터넷을 민간/공공/금융, 업무영역/비업무영역 등의 영역으로 구분합니다. 공공업무용 망(내부망), 인터넷망(외부망)으로 나눌 경우, 인터넷을 이용해 업무용 망에 접속할 수 없게 되므로 원격근무 자체가 불가능해집니다. 또한, 각종 보안시스템을 이용해 제한적으로 업무용 데이터에 접근할 수 있게 된다 하더라도 이에 상응하는 고수준, 고사양의 보안시스템이 필요하게 되며, 만에 하나 사용자의 실수나 해킹으로 인해 기관 내부의 기밀 데이터가 외부로 유출될 경우 사회적으로 큰 혼란이 야기됩니다. 게다가, 모든 것이 연결되는 지금의 시점으로 '영역'이라는

개념이 모호해졌다는 점도 고려해야 합니다

그래서 제시되는 대안이 바로 '데이터 중심'의 망분리 정책입니다. '데이터 중심' 망분리 정책을 따르게 되면, 데이터의 중요도에 따라 기밀이 유통되는 망과 기밀이 아닌 일반 데이터가 유통되는 망을 운영하게 됩니다. 일반 데이터 망에서는 인터넷을 통해 외부에서 접속하는 것을 허용함으로써 보안성도 강화하고 업무의 효율성도 극대화할 수 있다는 것입니다. 해외의 경우 보호해야 할 데이터가 기밀인지 아니면 기밀이 아닌 중요(Sensitive but Classified) 데이터인지에 따라 보안정책 및 관할부처를 구분합니다. 우리나라 역시 현재의 정보보호 정책 수립 방향의 근본적 한계를 인식하고, 비기밀 공공 데이터에 대한 유통 및 활용을 촉진할 다양한 세부 방안을 마련해야 한다는 입장입니다.

이슈미니 써머리 세번째 챕터

앞으로의 망분리 정책

데이터 중심의 정보보호정책 마련이 시급하다

앞으로의 망분리 정책은?

김 승 주
(고려대학교 정보보호대학원 교수 / 대통령직속 4차 산업혁명위원회 위원)

공공영역인가, 민간영역인가 또는 금융영역인가? 업무영역인가 아니면 비업무영역인가? 이는 우리나라에서 정보보호정책을 결정짓는 중요한 기준이다. 이에 반해 미국 등 외국에서는 보호해야 할 데이터의 중요도 즉, 보호해야 할 대상이 기밀 데이터인지 아니면 기밀이 아닌 중요(SBU: Sensitive But Unclassified) 데이터인지, 또는 평범한 일반 데이터인지에 따라 정보보호정책을 달리한다. 즉, 영역 중심이 아닌 데이터 중요도 중심의 정보보호정책을 펴고 있는 것이다.

예를 들어, 미국의 경우 기밀 데이터를 암호화 할 때는 정부가 개발한 비공개 암호기술을 사용하고, 기밀이 아닌 SBU 데이터에는 AES라는 민간이 개발한 공개 표준 암호기술을 사용토록 하고 있다. 반면 우리나라의 경우 공공 및 대국민 행정업무 영역에서는 그것이 기밀이 아닌 데이터라 할지라도 정부가 개발한 암호기술인 NES 또는 ARIA를 사용토록 하고 있고, 민간 영역에서는 SEED, AES 등을 사용하도록 의무화하고 있어 민간 • 공공간의 데이터 호환에 있어 문제를 야기하고 있다.

공공영역인가, 민간영역인가 또는 금융영역인가? 업무영역인가 아니면 비업무영역인가? 이는 우리나라에서 정보보호정책을 결정짓는 중요한 기준이다. 이에 반해 미국 등 외국에서는 보호해야 할 데이터의 중요도 즉, 보호해야 할 대상이 기밀 데이터인지 아니면 기밀이 아닌 중요(SBU: Sensitive But Unclassified) 데이터인지, 또는 평범한 일반 데이터인지에 따라 정보보호정책을 달리한다. 즉, 영역 중심이 아닌 데이터 중요도 중심의 정보보호정책을 펴고 있는 것이다.

예를 들어, 미국의 경우 기밀 데이터를 암호화 할 때는 정부가 개발한 비공개 암호기술을 사용하고, 기밀이 아닌 SBU 데이터에는 AES라는 민간이 개발한 공개 표준 암호기술을 사용토록 하고 있다. 반면 우리나라의 경우 공공 및 대국민 행정업무 영역에서는 그것이 기밀이 아닌 데이터라 할지라도 정부가 개발한 암호기술인 NES 또는 ARIA를 사용토록 하고 있고, 민간 영역에서는 SEED, AES 등을 사용하도록 의무화하고 있어 민간□공공간의 데이터 호환에 있어 문제를 야기하고 있다.

이뿐만이 아니다. 지난 2007년부터 우리 정부는 공공 및 금융 기관 내부의 업무용 망(내부망)을 인터넷으로부터 완전히 단절시키는 '망 분리 정책'을 시행해 왔다. 망을 분리시킴으로써 내부의 중요 데이터가 인터넷을 통해 외부로 유출되는 것을 원천적으로 차단하자는 '망 분리 정책'은 일견 그럴듯해 보이기는 하다. 그러나 이렇게 할 경우 유 • 무선 인터넷을 이용해 업무용 망에 접속할 수 없게 되므로 원격근무(일명, 스마트워크)나 클라우드를 이용하는 것이 어려워진다. 각종 보안시스템을 이용해 제한적으로 업무용 데이터에 접근할 수 있게 한다 하더라도 이에 상응하는 고수준 • 고사양의 보안시스템이 필요하며, 만에 하나 관리자의 실수 등으로 인해 해커나 악성코드가 회사 내부로 침투할 경우 일반, 기밀 할 것 없이 내부의 모든 데이터가 유출되므로 큰 피해를 입힐 수 있다. 더욱이 회사 내부 시스템에 문제가 발생했을 경우 이를 신속히 업데이트하는 것 또한 쉽지 않다. 반면, 미국 등 선진국에서는 전산망을 단순히 업무용과 비업무용으로

구분하는 것이 아니라 데이터의 중요도에 따라 기밀 데이터 유통망과 일반 데이터 유통망으로 분리하고, 이중 기밀이 아닌 일반 데이터가 유통되는 망에 대해서는 유 • 무선 인터넷을 이용해 외부에서 접속하는 것을 허용함으로써 보안성도 강화하고 업무의 효율성도 극대화 하고 있다.

앞선 사례에서 봤듯 공공영역이냐 민간영역이냐 또는 업무영역이냐 비업무영역이냐의 여부로 정책을 구분하는 것이 얼핏 단순 • 명쾌해 보이긴 하나 사실 많은 문제점들을 안고 있다. 왜냐하면 인터넷이라는 것의 특성상 그 영역을 정확히 구분하는 것이 쉽지 않으며, 더욱이 "모든 것이 네트워크에 연결(초연결)되어 있고, 데이터는 활발하게 공유 • 활용돼야 한다"는 4차 산업혁명의 기본 철학과도 상충되기 때문이다.

더욱 큰 문제는 현재 우리의 상태를 개선하는 것 또한 쉽지 않다는 것이다. 우리나라는 1978년 이후 행정전산화사업, 국가기간전산망사업 등을 통해 어느 정도 국가 정보화의 기반을 갖추었으며, 특히 2001년부터는 본격적으로 전자정부 사업을 추진해 왔다. 그러나 이 과정에서 너무 전산화에만 몰두한 나머지 보안에는 상대적으로 소홀했으며, 그 결과 현재에는 이미 무차별적으로 입력된 방대한 정부 전산 데이터들을 그 중요도에 따라 다시 분류할 엄두조차 내지 못하고 있는 실정이다.

클라우드 슈밥이 그의 저서, '더 넥스트(THE NEXT)'에서도 밝혔듯 정보보호가 담보되지 못한다면 4차 산업혁명과 관련한 모든 시도들은 모래위에 쌓아올린 성처럼 오래 갈 수 없다. 그러나 그렇다고 해서 보안이 또 다른 규제가 되어서도 곤란하다. 이 두 가지 딜레마 속에서 균형점을 찾을 때 대한민국은 신뢰할 수 있는 초연결 국가로서의 위상을 갖게 될 것이다. 이제 우리 정부도 현재의 정보보호정책 수립 방향의 근본적 한계를 인식하고, 하루빨리 데이터 중요도 중심의 정책으로의 전환을 모색해야 할 때다.

— 이슈 미니 써머리 부록 챕터 —

부록 : 관련 법정 원문

부록 : 관련법령 원문

1) 국가정보보안기본지침

o 성격 : 공공기관 망분리 가이드

o 본문 < 비공개>

2) 전자금융감독규정

o 성격 : 금융기관 망분리 가이드

o 본문

제15조(해킹 등 방지대책) ① 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립•운용하여야 한다.

1. 해킹 등 전자적 침해행위로 인한 사고를 방지하기 위한 정보보호시스템 설치 및 운영
2. 해킹 등 전자적 침해행위에 대비한 시스템프로그램 등의 긴급하고 중요한 보정(patch)사항에 대하여 즉시 보정작업 실시
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 최소화하여 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.>

3) 정보통신망법 시행령

o 성격 : 일반기업 망분리 가이드

o 본문

제15조(개인정보의 보호조치)

② 법 제28조제1항제2호에 따라 정보통신서비스 제공자등은 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.>

1. 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템(이하 "개인정보처리시스템"이라 한다)에 대한 접근권한의 부여 · 변경 · 말소 등에 관한 기준의 수립 · 시행
2. 개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치 · 운영
3. 개인정보처리시스템에 접속하는 개인정보취급자 컴퓨터 등에 대한 외부 인터넷망 차단
4. 비밀번호의 생성 방법 및 변경 주기 등의 기준 설정과 운영
5. 그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치

이슈미니써머리 vol1
2020. 2

STARTUP ALLIANCE