금융권 클라우드 가이드라인을 통한 클라우드 보안 전략

2019. 2. 21.

금융혁신지원팀장 김성웅 (swkim@fsec.or.kr)

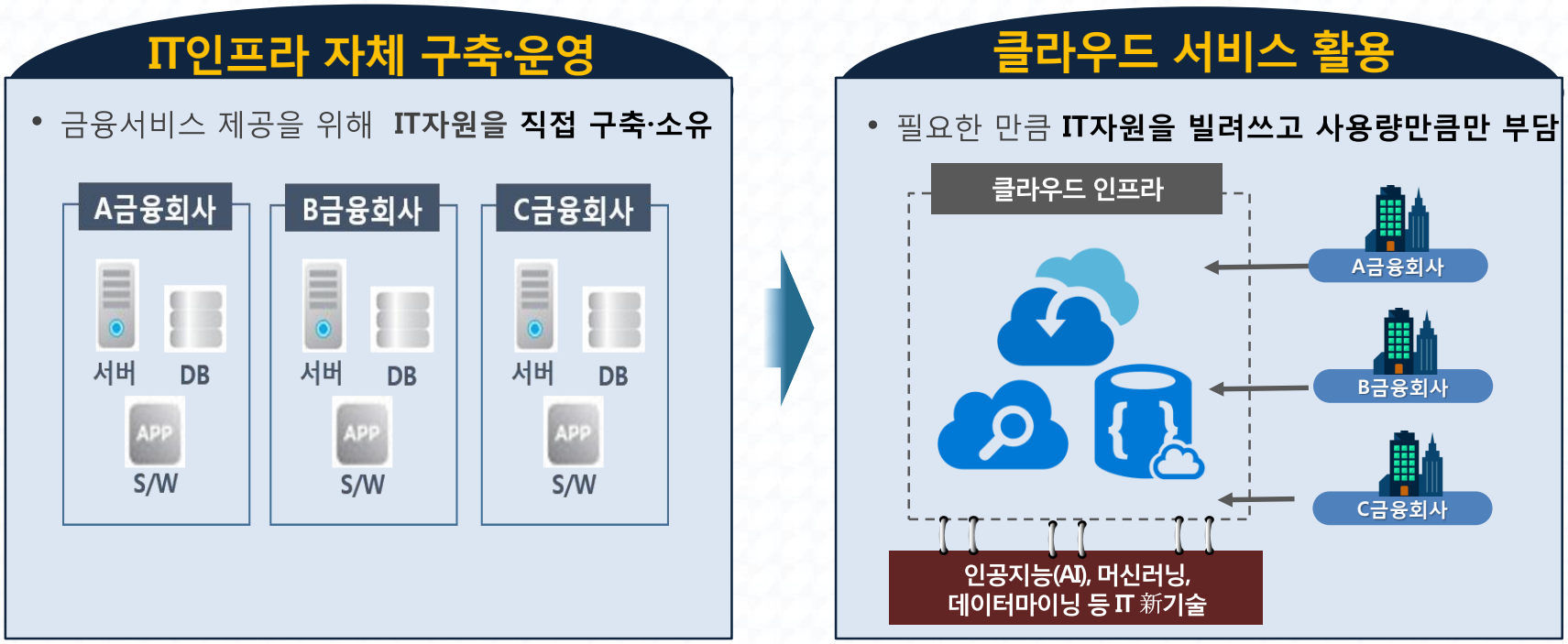
금융보안원
FINANCIAL SECURITY INSTITUTE

목 차

Ⅰ. 클라우드 컴퓨팅

Ⅰ. 클라우드 컴퓨팅

전산설비를 직접 구축하지 않고 전문업체로부터 인터넷(“the cloud”)을 통해 필요한 IT자원을 탄력적으로 제공받아 사용하는 컴퓨팅 환경



Ⅰ. 클라우드 컴퓨팅

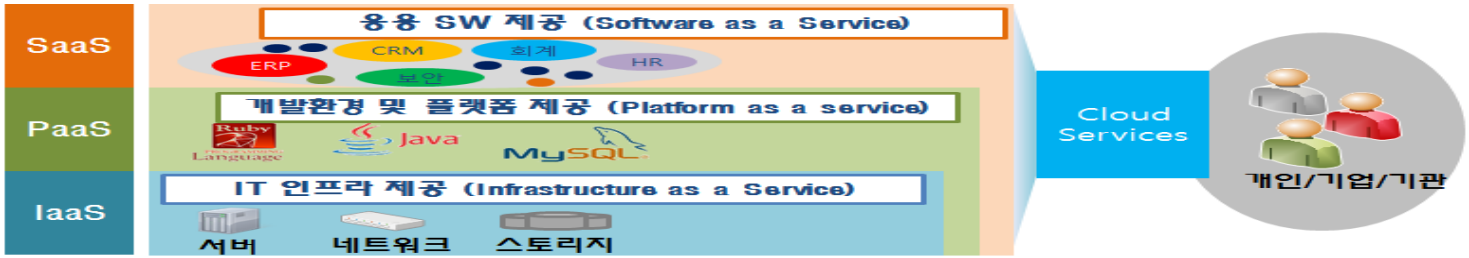
서비스 공유 범위, 제공하는 IT자원의 범위에 따라 서비스 구분

1) 서비스 공유 범위 기준, 3가지 배치 모델

- ① Public(불특정 다수), ②Private(특정회사), ③ Hybrid 클라우드로 구분

2) 제공하는 IT자원의 범위 기준, 3가지 서비스 모델

- ①서버 등 전산 인프라(IaaS) ②응용프로그램 개발환경(PaaS) ③ 응용프로그램(SaaS)으로 구분



Ⅰ. 클라우드 컴퓨팅

신속성(On-demand Self-service)

컴퓨팅 기능을 사람의 중재 없이 필요한 만큼 자동적으로 확보하여 사용

효율성(Resource Pooling)

컴퓨팅 자원은 다중 임대(multi-tenant) 방식으로 다중 사용자에 제공되기 위해 풀 형태로 관리

경제성(Measured Service)

적절한 미터링 기능을 이용하여 자원의 사용을 자동적으로 통제하고 최적화

이용편의성(Broad Network Access)

클라우드 컴퓨팅 기능은 네트워크(인터넷)를 통해 이용할 수 있으며, 서로 다른 클라이언트 플랫폼(모바일, PC 등)을 통해 이용 가능

유연성(Rapid Elasticity)

IT자원이 탄력적으로 제공되며, 일부 경우 신속한 확장과 축소를 위해 자동적으로 제공

직접 투자 부담, 미사용 자원에 대한 비용 절감, 스토리지 공간 확장성, 다양한 IT자원 활용 등

기업 운영의 효율성, 유연성, 경제성 등을 극대화

Ⅱ. 클라우드 컴퓨팅 주요 리스크

Ⅱ. 클라우드 컴퓨팅 주요 리스크

공급자(CSP) 관련

가용성 리스크

공급자 리스크

CSP 서비스 제공 중단

- 시스템 장애, 파산 등으로 서비스 중단
- 서비스 중단에 대비한 대응 전략 부재

보안 리스크

해킹, 정보유출 등 보안사고

- 사이버 공격 등으로 인한 침해사고
- CSP의 부주의로 인한 정보유출

집중 리스크

주요 CSP 의존 심화

- 다수의 금융사가 특정 CSP에 의존

가용성 리스크

보안 리스크

금융회사 관리 과실

- 권한관리 미흡 등으로 시스템 장애 및 사고
- 클라우드 환경에 대한 이해 부족

컴플라이언스 리스크

국외 업무 위탁

- 대상 국가 정치 사회 문제로 업무중단
- 수사기관 등에 주요정보 제출 가능성

컴플라이언스 리스크

관리감독 한계

- 사고 조사, 현장방문 등에 비협조적

Ⅱ. 클라우드 컴퓨팅 주요 리스크

CSP 서비스 제공 중단

시스템 장애, 파산 등으로 서비스 중단
서비스 중단에 대비한 대응 전략 부재

- CSP의 파산, 비즈니스 중단 등으로 서비스 제공이 영구적으로 중단되거나 기술적 오류 및 물리적 재해 등으로 시스템 장애가 발생하여 서비스 제공이 일시적으로 중단

사례 및 시나리오

- **(사례1)** A사 DNS 설정 오류로 2시간 이상 서비스 불가('18년)
- **(사례2)** M사 유럽 데이터 센터에서 물리적 관리 시스템 에러로 온도가 상승하여 시스템 중단, 주요 클라우드 서비스 상당기간 중단('17년)
- **(사례3)** N사 의 파산으로, 다수 기업이 짧은 기간안에 데이터 이전 등 업무 연속성 확보에 어려움을 겪음('13.10월)

대응방안

- 출구전략을 수립(계약서에 출구전략 관련 내용 반영)
- 재해복구훈련을 주기적 수행/이중화, 백업 및 복구절차를 수립
- 계약 이행보증보험 가입 요구 등 보장 장치 마련
- 시스템 장애 시 통지, 원인 조사 및 복구 절차 등 CSP 의무사항 및 미이행시에 대한 패널티 조항 명시

해킹, 정보유출 등 보안 사고

사이버 공격 등으로 인한 침해사고
CSP의 의무 불이행으로 인한 정보유출

- 클라우드 시스템을 대상으로 악의적인 내부자 공격, 제로데이 공격 등 사이버 침해사고가 발생하거나 주요정보가 유출 또는 변조

사례 및 시나리오

- **(사례 1)** C사 시스템에서 보안 취약점이 발견되어, 동 클라우드 이용 웹사이트 약 3,400여개가 취약점에 노출됨('17년)
- **(사례2)** 클라우드 DNS 서버가 DDoS 공격을 받아 다수 서비스 영향('16년)

대응방안

- 안전성 확보조치 방안 및 리스크 관리체계 마련
- 침해사고 예방 및 대응 활동 관련 CSP 협조사항 및 미이행 패널티를 계약서에 명시

Ⅱ. 클라우드 컴퓨팅 주요 리스크

주요 CSP 의존 심화

다수의 금융사가 특정 CSP에 의존

- 금융회사의 전략 유연성 감소, 서비스 가용성 확보 어려움 등 발생
- 시스템 장애, 침해사고 발생 등으로 인한 피해가 금융권 전반으로 확산될 가능성

사례 및 시나리오

- **(시나리오1)** 대형 시중은행 5개사가 A사 클라우드를 이용하여 인터넷 뱅킹 웹페이지를 구축, A사에 장애 사고가 발생하여, 뱅킹 서비스 이용 불가
- **(시나리오2)** 금융회사 A가 모든 개발 플랫폼을 CSP B사의 PaaS 기반으로 이전하고 추후 신규 서비스를 구축하려고 했으나, B사에서 해당 플랫폼을 제공하지 않아 구축 대상 서비스 모델을 불가피하게 변경함

대응방안

- 중요도가 높은 정보처리시스템에 대해서는 특정 CSP에 대한 의존도가 과다하지 않게 관리

금융회사 관리 과실

권한관리 미흡 등 관리 실수

클라우드 환경에 대한 이해 부족

- 계정별 권한 및 암호키 관리 미흡, 멀티 팩터 미사용 등으로 시스템 장애, 보안 사고 등 발생 가능
- 시스템 사용량에 따른 요금체계 등 클라우드 환경에 대한 이해 부족으로 예상외 비용 발생

사례 및 시나리오

- **(사례1)** A사의 클라우드 저장소 서비스 이용 중 이용자 설정 미흡으로 B기업 회원정보 300만건 노출(보안업체 발견, `15년)
- **(사례2)** 1억2,300만개 이상의 개인정보 노출(보안업체 발견, `17년)
- **(사례3)** 고객 220만명의 개인정보 노출(보안업체 발견, `17년)

대응방안

- 클라우드 서비스 관련 전문성 확보(교육)

Ⅱ. 클라우드 컴퓨팅 주요 리스크

국외 업무 위탁

대상 국가 정치 사회 문제로 업무중단
수사기관 등에 주요정보 제출 가능성

- 전쟁, 당국에 의한 업무정지, 자연재해 등 클라우드 시스템이 위치한 국가 문제로 인해 서비스 중단 발생
- 금융회사의 주요 정보를 수사기관 등 관계당국에 제공

사례 및 시나리오

- **(시나리오1)** 금융회사 A가 B 국가의 데이터센터를 이용하던 중 B 국가에 전쟁이 발생, 해당 데이터센터의 갑작스러운 파손으로 데이터 손실 발생
- **(시나리오2)** 미국 클라우드법(CLOUD ACT)에 따라 국내 금융회사의 주요 정보를 미국 수사기관에 제공

대응방안

- 계약 시, 국외 클라우드 이용에 따른 적용 법규, 재판관할권 등 계약서 반영 여부 등을 점검(국내법원을 관할법원으로 하도록 명시)
- 국외 위탁에 따른 리스크를 식별하고, 별도 대응체계 마련

관리감독 한계

사고 조사, 현장방문 등에 CSP가 비협조적

- 계약 미흡 등으로 현장방문, 사고조사 등에 비협조적으로 대응하는 등 금융회사의 CSP 관리감독에 어려움 존재

사례 및 시나리오

- **(사례)** A사의 국내 리전에 장애 발생 시 금융회사에서 사고 대응을 위한 관련 정보의 수집 및 분석 등에 어려움을 호소(18.11월)
- **(시나리오)** 클라우드 서버에 사고가 발생 하여 포렌식 수행 및 당국 검사가 필요하나, CSP가 다른 이용자에 대한 권리 주장을 바탕으로 현장조사를 거부

대응방안

- 금융당국의 현장접근 및 조사 권한을 계약서에 반영

Ⅲ. 국내 금융권 클라우드 이용 범위 확대

Ⅲ. 국내 금융권 클라우드 이용 범위 확대

전자금융감독규정 개정('19.1월)

개정 배경

클라우드 이용 확대와 관련한 **추가 규제 완화 필요성**이 지속적으로 제기됨에 따라, 클라우드 활용 범위를 개신용정보까지 확대하되 **금융권 보안수준 및 관리감독 체계를 강화**

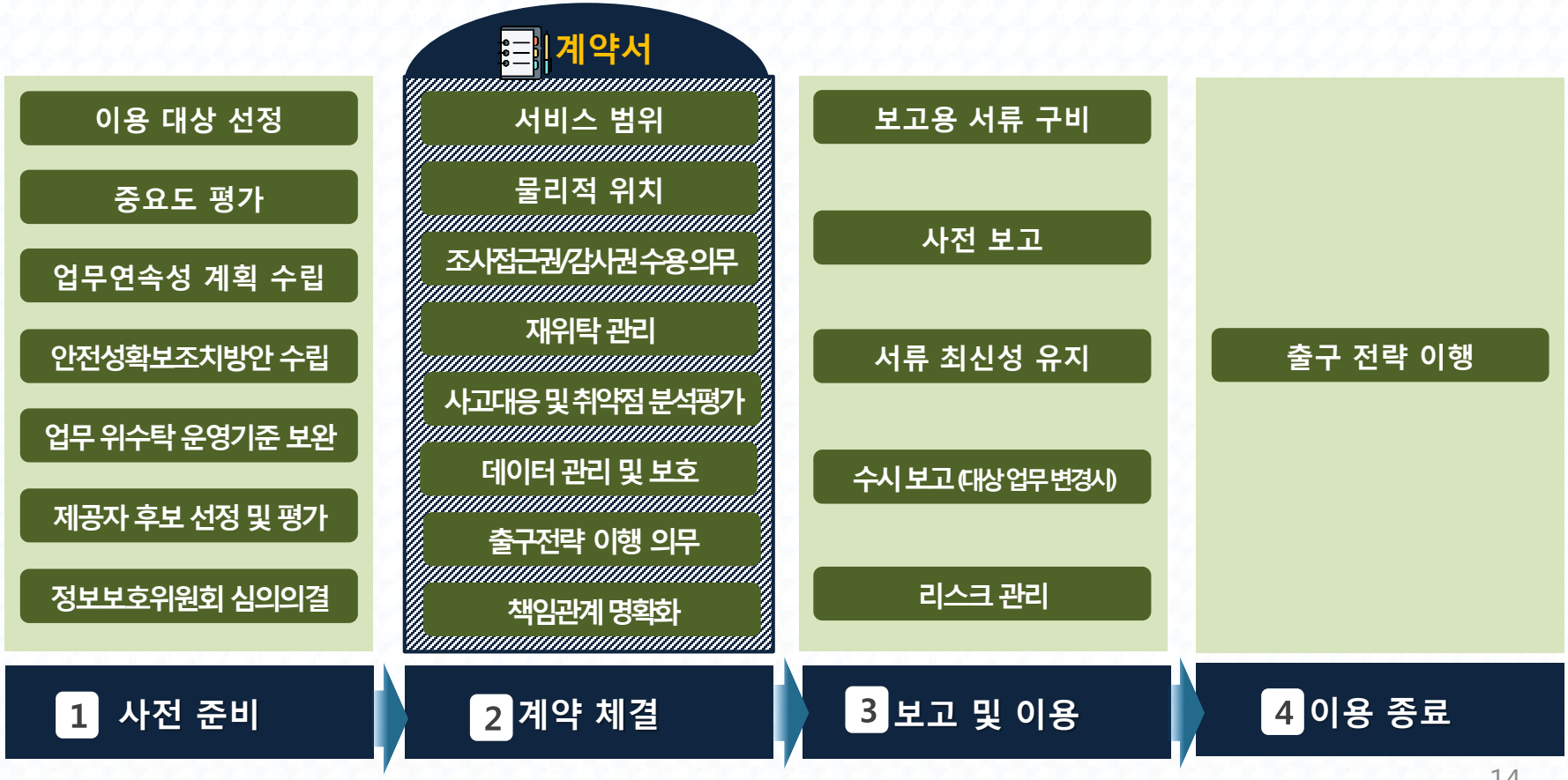
주요 내용

- 클라우드 서비스 이용범위 확대 (비중요정보限 → 개인신용정보·고유식별정보)
- 클라우드에 대한 내부통제 강화(클라우드 서비스의 안전성 평가, 자체 정보보호위원회 심의 의결)
- 클라우드 이용 관련 보고의무 등 감독 강화 (클라우드 이용 현황 보고, 법적책임 등을 계약서에 명시)
- 국내 소재 클라우드 운영 (개인신용정보 처리는 국내 소재 클라우드에 한해 우선 허용)

Ⅲ. 국내 금융권 클라우드 이용 범위 확대

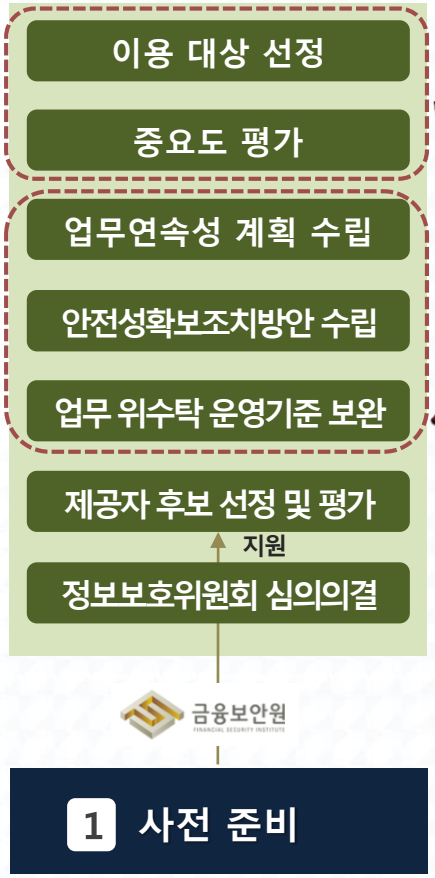
금융권 클라우드컴퓨팅서비스 이용 가이드 개정('18.12월)

금융회사 또는 전자금융업자가 클라우드 서비스를 이용하고자 할 경우 요구되는 세부절차를 안내하고 금융시스템 및 금융소비자 보호를 위해 필요한 보안사항을 권고



Ⅲ. 국내 금융권 클라우드 이용 범위 확대

금융권 클라우드컴퓨팅서비스 이용 가이드 주요내용(1)



1.업무 선정 및 평가

(이용대상 선정) 클라우드 서비스 이용에 따른 **효율성** 등을 감안하되 **핵심업무의 경우** 효율성 외에도 **업무 중요도, 취급 정보의 민감도, 경영 전략** 등을 **복합적으로 고려**

*(예) 신기술 활용, 파일럿 서비스, 시스템 사용량 변동이 큰 경우 등

(중요도 평가) 고유식별정보 또는 개인신용정보 처리 시 중요 업무로 취급, 그 외 **전자금융거래의 안전성 및 신뢰성에 중대한 영향**을 미칠 경우 **중요 업무로 취급**

2.계획 수립

(업무 위수탁 운영 기준) 중요도가 높은 업무 위탁 시 관련 규정에 따라 기 수립 운영 중인 자체 업무위수탁 운영기준에 **감독규정에서 정하고 있는 업무위탁 운영기준 보완사항을 반영 준수**

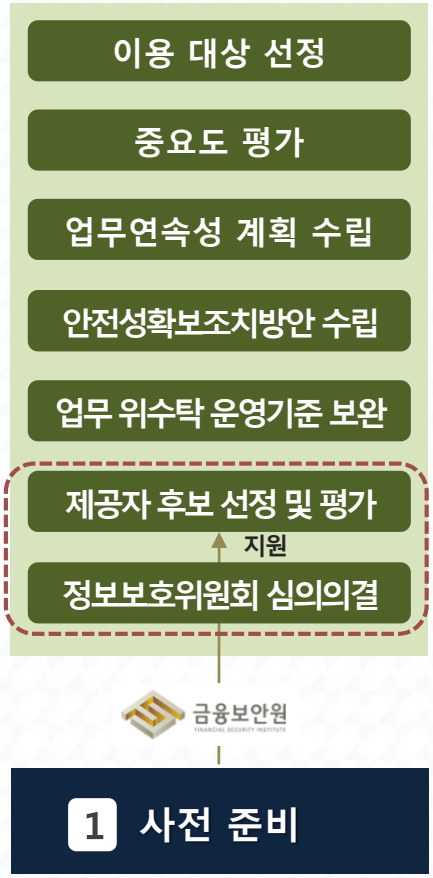
(안전성 확보조치 방안) 계정관리, 접근통제 등 **필수 보안 통제사항**을 포함한 안전성 확보조치 방안 수립 이행 (*클라우드 관련 보안사고 중 **이용자 보안 관리 미흡으로 인한 사고 비중 매우 높음**)

(업무연속성 계획) 기존에 감독규정에 따라 수립 운영 중인 업무연속성 계획에 클라우드 시스템 추가, 특히 **데이터 백업 관리, 훈련 및 사고 관리, 출구 전략**이 중요

(출구 전략) CSP 파산 등으로 클라우드 서비스 이용 전환 또는 종료 시 대응 방안으로, 출구 전략 이행에 필요한 상황을 지표로 설정/모니터링하고 조직별 역할 및 책임을 포함한 세부 이행 절차를 정의

Ⅲ. 국내 금융권 클라우드 이용 범위 확대

금융권 클라우드컴퓨팅서비스 이용 가이드 주요내용(2)



3.계약 준비

(제공자 평가) 가이드 부록 "**금융분야 클라우드컴퓨팅 서비스 제공 기준**"에 따라 **CSP를 평가**, 그 결과에 따라 계약 추진 및 이용 여부를 최종 결정

- **고유식별정보 또는 개인 신용정보 처리 업무**의 경우, 해당 정보를 처리하는 **모든 시스템을 국내에 설치**하고, 해당 전산실 내에 **무선통신망이 설치되지 않아야 한다**는 점 고려

  * 일시적으로 처리되는 시스템은 모두 포함되며, 해당 정보가 처리되는 경우 관리시스템도 포함

(평가대상) 금융회사가 제3자로부터 상용(商用)으로 제공받는 모든 유형의 클라우드 제공자

(절차 및 방법) 최초 이용시 종합평가, 이용 중 보안수준 유지여부를 확인하는 정기평가로 구분

1 종합평가 : 특정 CSP를 최초 이용 시 실시

CSP 자가점검 및 제출 → 금융회사가 현장평가 및 검증 → 미흡사항 보완 및 확인

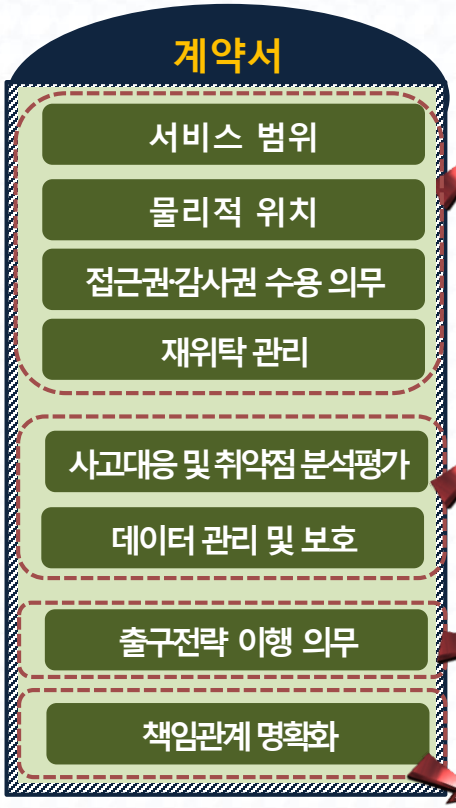
2 정기평가 : 종합평가 종료 후 매 1년마다 실시

점검 절차는 종합평가와 동일(단, 자가점검 결과 서면 검증 원칙, 매 3년 현장평가)

(정보보호위원회 심의의결) 중요도 평가 결과, 자체 업무 위수탁 운영기준 및 CSP 평가 결과에 대해 정보보호위원회를 개최하여 심의의결

Ⅲ. 국내 금융권 클라우드 이용 범위 확대

금융권 클라우드컴퓨팅서비스 이용 가이드 주요내용(3)



2 계약 체결

1. 서비스 위탁 관련

(서비스 범위 및 물리적 위치) 데이터가 처리되는 물리적 위치의 시 군 단위까지 기재 (고유식별정도 또는 개인신용정보 처리 시 모든 시스템 국내 설치, 해당 전산실 내 무선통신망 금지)

(접근권/감사권 수용 의무) 금융당국, 침해사고대응기관 등의 현장 조사 수행에 적극 협조

(재위탁관리) 중요 변경 사항 발생시 금융회사에 사전 동의를 받을 것

2. 보안 관련

(사고대응 및 취약점 분석 평가) 사고 인지 즉시 금융회사와 침해사고대응기관에 통지,사고 조사복구에 적극 협조

(데이터 관리 및 보호) 제3자 제공 관련 의무 및 실제 제공 여부는 금융당국 및 금융회사에 통지 및 사전 동의 필요

3. 출구전략 관련

(전환 종료 시 데이터 이전 및 삭제) 금융회사에 반환 및 이전. 복구 불가능한 방법으로 완전 파기 및 확인

(모의훈련 협조) 전환 및 종료 절차에 대한 모의훈련을 주기적으로 실시

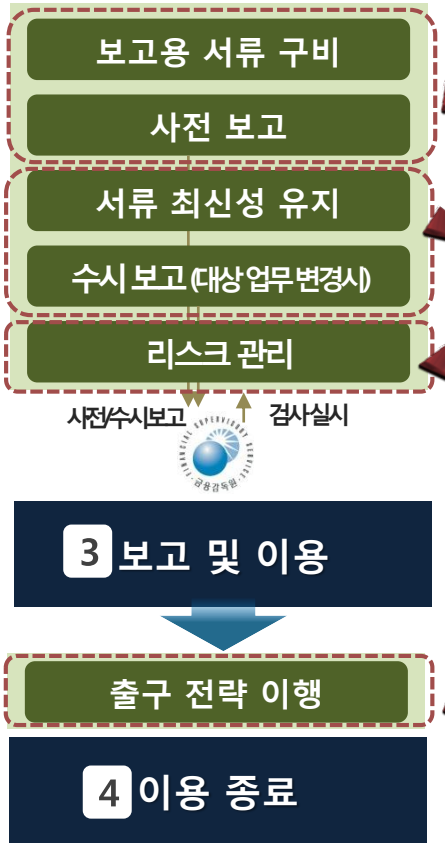
4. 책임관계 명확화

(대외적 책임) CSP가 금융관련 법령 위반으로 발생한 손해에 대해서는 연대 배상책임 부담

(계약 당사자 간 책임관계) CSP 귀책 사유로 손해(간접 손해 포함) 발생시 손해배상 책임 청구 가능

Ⅲ. 국내 금융권 클라우드 이용 범위 확대

금융권 클라우드컴퓨팅서비스 이용 가이드 주요내용(4)



(서류구비 및 사전보고) 클라우드 서비스 이용 전 **관련 서류*를 구비**하고 **중요 업무의 경우** 실제 이용날 **7영업일 이전에 금융감독원에 보고**

* 업무 위탁 관련 서류, 자체 중요도 평가 기준 및 결과, 업무연속성 계획 및 안전성 확보조치 관련 사항 등

(서류 최신성 유지 및 수시보고) 구비한 각 서류를 **최신상태로 유지, 주요 변경사항 발생시** 발생사유, 관련 자료 및 대응 계획을 **7영업일 내 금융감독원장에 보고**

(리스크 관리) 기 수립된 업무 연속성 계획 및 안전성 확보조치 방안을 준수하여 서비스 중단 및 보안 관련 리스크를 관리하고 **집중리스크, 재위탁 관련 리스크** 등을 **중점적으로 관리**

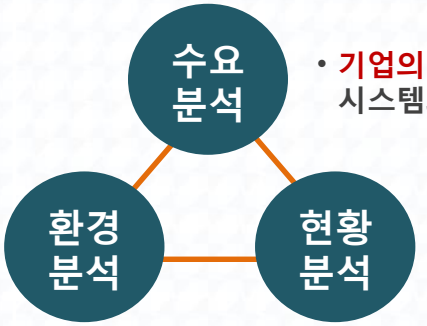
클라우드서비스 전환 및 종료 시 기 수립한 **출구 전략에 의거**하여 **데이터 이전 및 파기 등 실시**

Ⅳ. 클라우드 추진 시 고려사항

Ⅳ. 클라우드 추진 시 고려사항

1 사전 고려사항

대상 사업 및 서비스 종류, 클라우드 이용에 따른 효율성·안전성, 대내외 영향 요인을 파악



- 국내외 시장에 출현하는 클라우드 서비스/제품, 벤더, 이용사례 등 **기술, 산업, 시장의 최신동향을 심층 분석**

- **기업의 경영전략 달성**을 위해 필요한 경영프로세스·정보시스템의 **혁신(변경) 및 IT현대화 요구** 파악

- 클라우드 도입 성공에 필요한 **기업 내부환경 조성 여부 점검**
- **법/규제 제한, IT자원의 외부호스팅 정책, 관련 내부 프로세스 성숙**도 등 클라우드 도입 성공 요건 점검

(참고) 데이터 센터를 퍼블릭 클라우드 IaaS로 이전하지 않아야 할 주요 이유

환경적 제약

- IT 민첩성의 중요도가 낮고 변화가 거의 없음
- 메인프레임 기반 또는 non-x86 서버 기반으로 운영
- 리눅스 또는 윈도우 외의 OS 기반
- 하드웨어 리프레시 사이클이 5년 이상
- 새로운 하드웨어를 이제 막 도입

물리적 제약

- 주요 퍼블릭 클라우드 서비스가 제공하지 않는 지역
- WAN 네트워크가 비약한 지역
- 기타 보안상의 이유로 온프레미스 운영이 필요한 상황

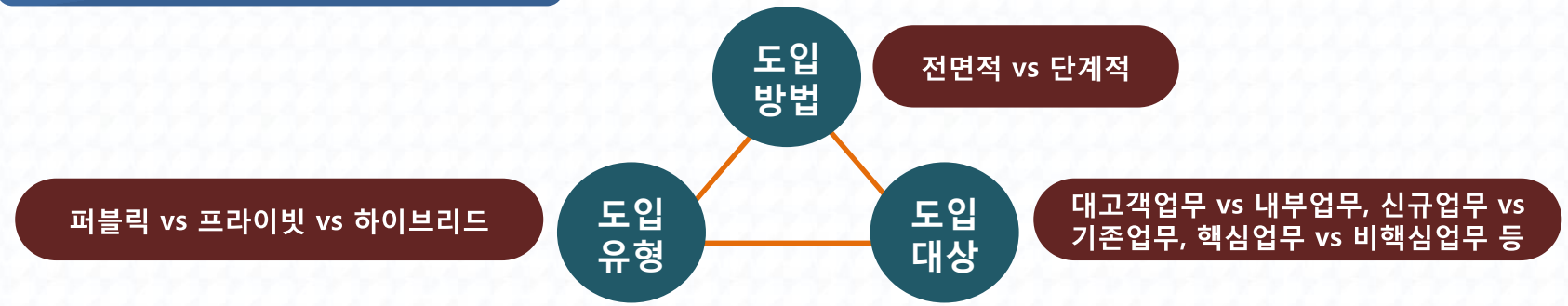
경영진의 지원 미흡

- IT 혁신 의지에 대한 지원이나 투자 미비

* 가트너, 15 reasons not to migrate your data center to public cloud infrastructure as a services

Ⅳ. 클라우드 추진 시 고려사항

2 단계적 • 맞춤형 도입



해외 금융권 클라우드 활용 현황

영국

Oaknorth Bank 모든 시스템을 AWS 가상 사설 클라우드로 이전
ClearBank MS Azure 하이브리드 클라우드 기반으로 시스템 구축

홍콩

HSBC 구글 클라우드 이용, 위험분석 및 자금세탁감시시스템 구축추진

싱가포르

DBS은행 AWS 기반 하이브리드 클라우드로 데이터 센터 구축, 금융상품 추천 및 금융 가치 측정 업무 등에 활용

미국

BoA ERP 시스템을 클라우드 기반으로 구축

해외는 핵심시스템도 확장성이 우수한 퍼블릭 클라우드로 전환이 활발해질 것으로 예상

국내 금융권 클라우드 도입의 경우..

U2L 이슈 등 기존 코어뱅킹시스템의 전면적인 클라우드 이전에 **선결과제 존재 → 초기비용 多, 보안 위협 등 우려** 高

비핵심업무, 신규 업무를 중심으로 우선 추진 後 핵심 업무 등으로 단계적 도입 필요

Ⅳ. 클라우드 추진 시 고려사항

3 멀티 클라우드

10개 중 8개 기업이 클라우드 핵심 전략을 멀티 클라우드라고 응답

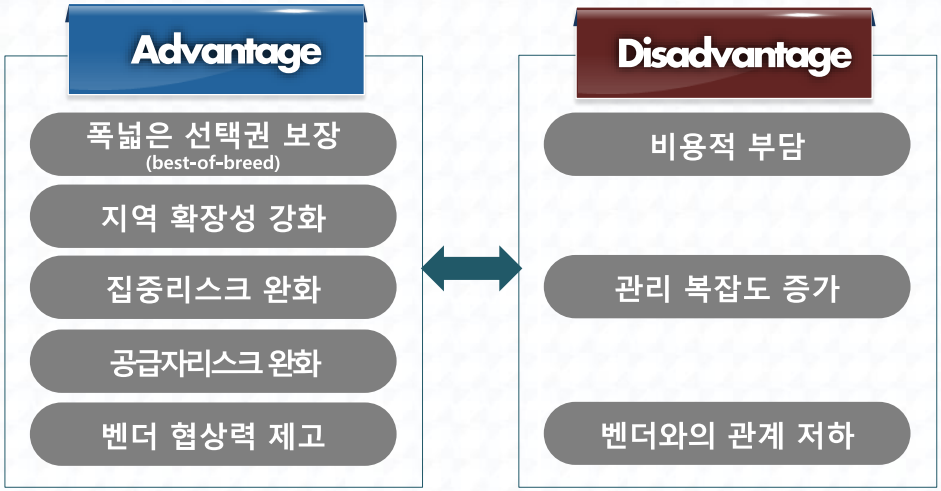
* 2018 Forrester survey

멀티클라우드

두가지 이상의 클라우드(클라우드 사업자)를 사용하는 것

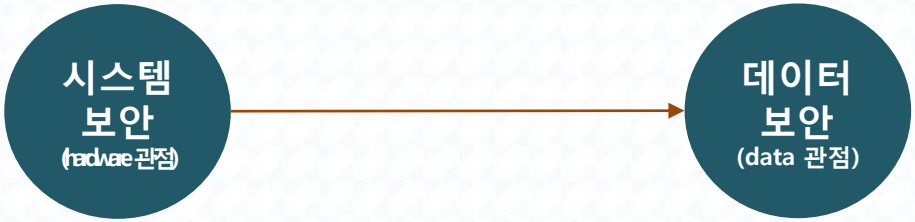
예) 서로 다른 워크로드에 프라이빗이나 퍼블릭을 선택적으로 사용,
동일한 워크로드에 둘 이상의 퍼블릭 클라우드를 동시에 사용 등

➔ 합리적인 비용과 성능, 관리 효율성 등을 고려하여 워크로드를 배치시키는 것이 중요



77%가 클라우드 보안이 과제라고 응답, 29%는 중대한 과제라고 응답

*라이트스케일(RightScale) "2018 클라우드 현황 보고서"/ 응답자의 81%가 멀티클라우드 전략을 채택



멀티클라우드 환경에서 클라우드 사업자(간)의 데이터 처리 과정 및 절차에 대한 세밀한 분석과 대응 필요

Ⅳ. 클라우드 추진 시 고려사항

4 데이터 보안 관리 강화

데이터 분산

관련 모든 국가 또는 지역의 규정 준수에 따른 통제 수단 및 매커니즘 변화

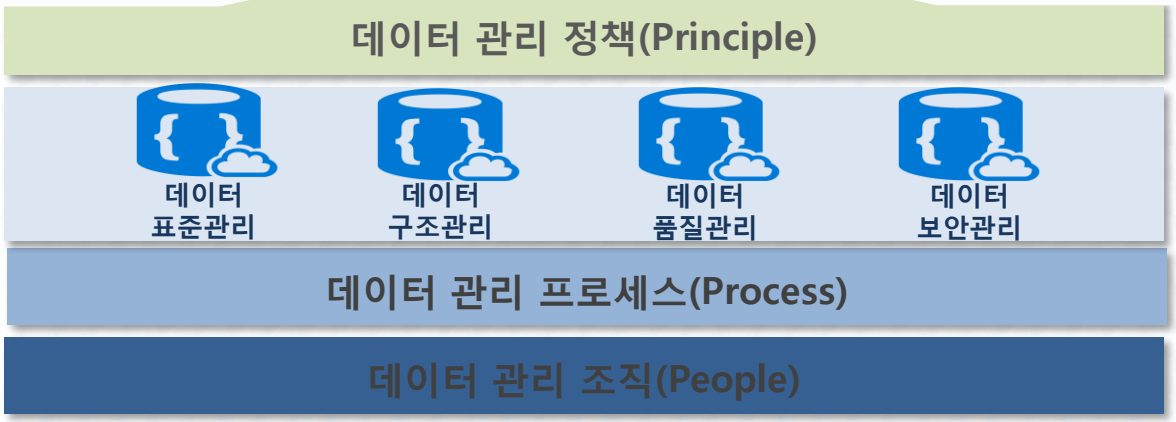
가시성 부재

데이터의 위치, 처리 방법 및 과정이 명확하게 보이지 않음

새로운 위협

멀티클라우드 환경을 타켓으로 한 신규 취약점 등장 우려

데이터 거버넌스 체계 수립



Ⅴ. 안전한 클라우드 이용을 위한 제언

Ⅴ. 안전한 클라우드 이용을 위한 제언

경영진의 관심과 책임(필수)

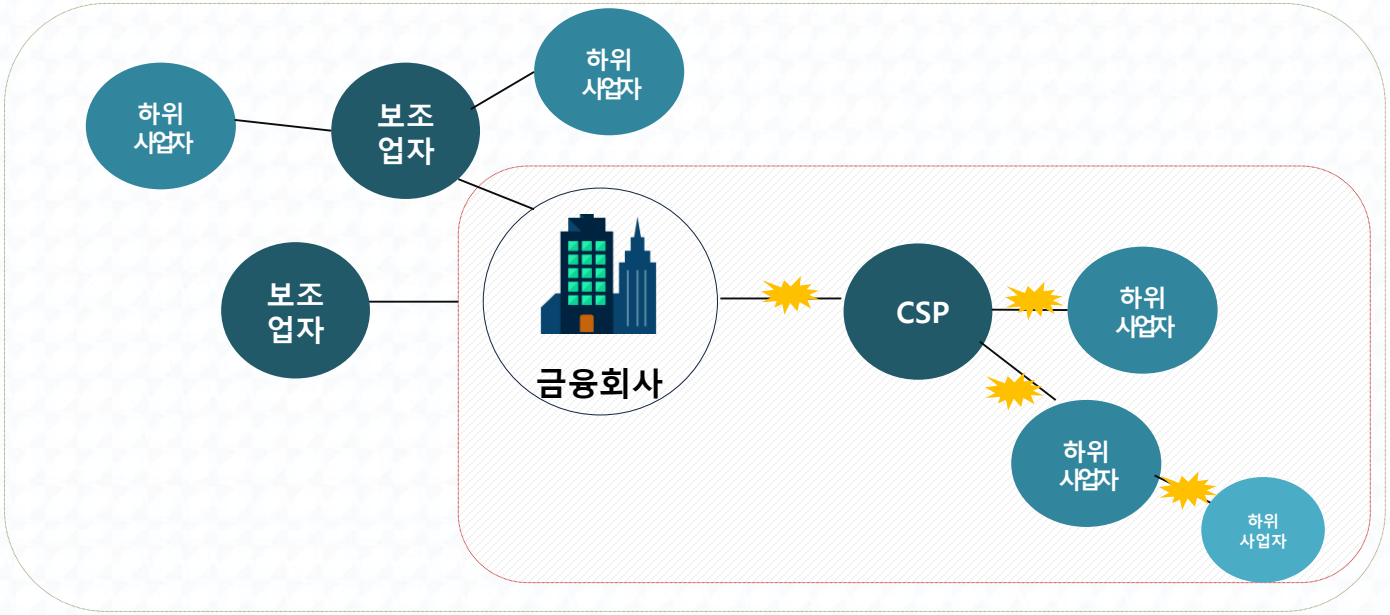
디지털 금융 확산 | 글로벌 사업 확대 | 규제 환경 개선 등

유연한 엔터프라이즈 관리 중요성 증대,
클라우드 도입을 고려하는 금융회사 증가

경영진이 기업의 리스크 관리를 위한 전략 및 대응계획 등을
이해하고 확인하는 적극적 리더십 필요

Ⅴ. 안전한 클라우드 이용을 위한 제언

공급망 관리 강화



클라우드 사업자를 비롯한 전체 공급망에 대한
보호대책 수립 및 통제, 모니터링 등 관리 강화 필요

Ⅴ. 안전한 클라우드 이용을 위한 제언

출구전략의 중요성

CSP의 파산, 서비스 제공 중단, 서비스 품질 저하, 규제 환경의 변화 또는 기타 금융회사의 필요에 따른 이용 중단 가능성 존재

➔ **Risk Mitigation 전략 필요**

출구 전략 (Exit Strategy)

출구전략 이행 지표 설정

- 출구 전략이 필요한 상황
- 출구 전략 성공 기준

출구 전략 이행 절차 정의

- 전사적인 기본방향 수립
- 조직별 역할 및 책임
- 개별시스템별 세부이행 절차 마련

<참고> 출구전략 수립 관련 고려사항

- 중요도가 높은 정보처리시스템은 **출구전략을 보다 정밀하게 수립**할 것
- 중요도가 높은 정보처리시스템은 **출구전략 이행이 용이한 구현 방식*을 고려**할 것

*** 구현 방식에 따른 출구 전략 이행 용이성**

- (IaaS) 컨테이너 방식 유리, CSP 의존도를 낮출 것
- (PaaS, SaaS) CSP가 제3자의 IaaS 인프라를 이용하여 서비스 제공 시 유리

감 사 합 니 다.

금융보안원
FINANCIAL SECURITY INSTITUTE