KISA-2017-0034



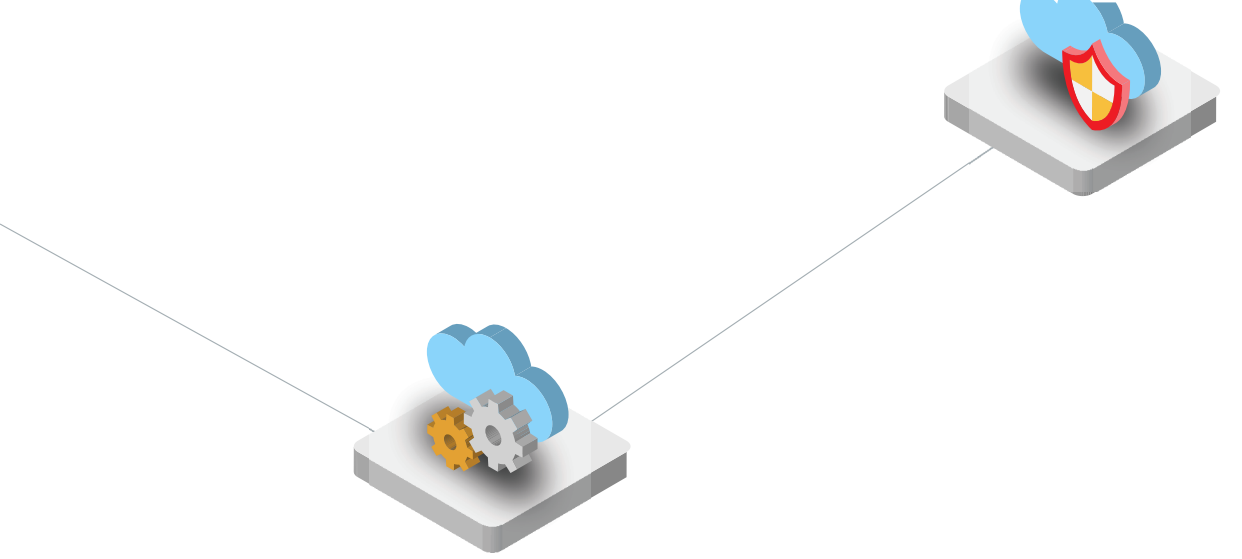
클라우드 서비스를 이용하는 기업 IT담당자 위한

클라우드 정보보호 안내서

2017. 12.

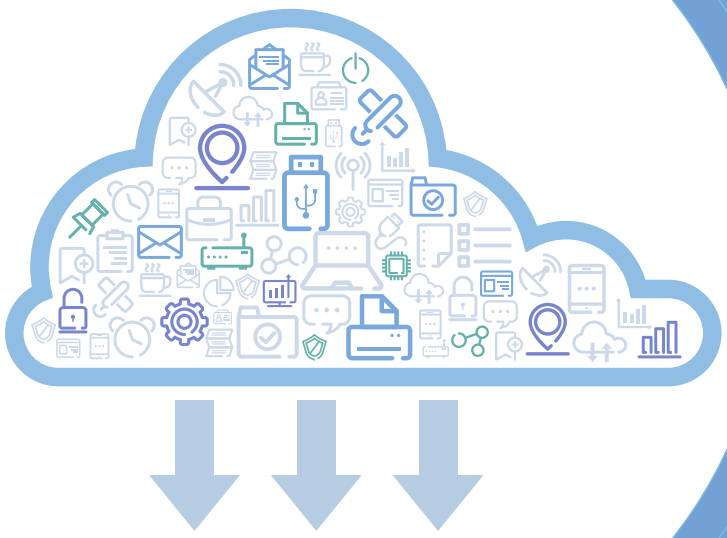
KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

Contents



클라우드 서비스를 이용하는 기업 IT담당자 위한

클라우드 정보보호 안내서



Ⅰ. 개 요

1. 발간배경
2. 구성 및 목적
3. 용어정의

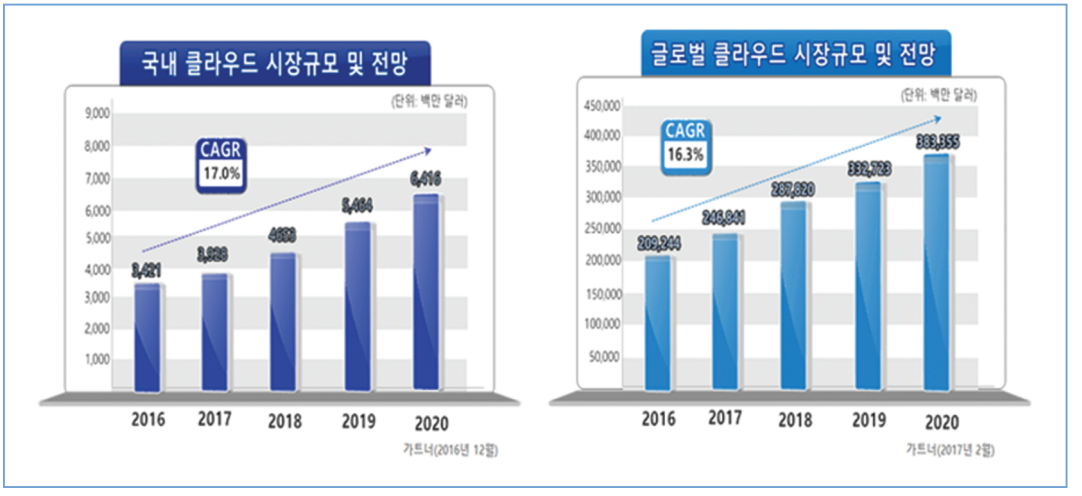
I 개요

1 발간배경

클라우드 컴퓨팅은 비용절감, 업무 효율성 및 생산성 향상 효과 등으로 클라우드 데이터 트래픽[1]은 2018년까지 4배 이상 증가할 것이며, 세계 퍼블릭 클라우드 시장[2]은 2018년까지 전체 IT시장의 6배가 넘는 성장이 전망되고 있다.

1) 클라우드 트래픽 : 1.6 ZB('13년)에서 6.5 ZB('18년)로, 전세계 데이터센터 트래픽 중 54% ('13년)에서 76%('18년)까지 점유할 것으로 예상(출처 : 시스코 클라우드 인덱스)

2) 클라우드 시장 : 세계시장은 '16년 2,092억달러에서 '20년 3,834억달러(연평균 16.3%) 성장이 예상되며, 국내는 '16년 34억 달러→'20년 64억달러(연평균 17.0%) 성장(출처 : Gartner)



또한 성장속도가 말해주듯이 최근 클라우드 내에 중요데이터를 저장하고 있는 기업들도 늘고 있는 추세이다. 하지만 클라우드 컴퓨팅은 자원공유, 가상화 등의 특성으로 IT자원 및 사용자들의 정보가 집적되어 있기 때문에 해커들의 DDoS 공격, 해킹 공격의 표적이 되기 쉽고, 사고 발생 시 대규모 피해가 발생할 수 있는 보안 위협이 내재되어 있다.

※ 전 세계 대기업의 IT 보안 전문가를 대상으로 조사한 결과, 85%의 기업이 클라우드에 민감 데이터를 저장하고 있어 70%가 이를 우려가 있다고 밝힘(출처 : 보메트릭, '16.3)

이에 기존 IT 인프라를 이용한 온프레미스 방식에서 클라우드 환경으로 전환(또는 신규구축) 시 클라우드의 특성을 이해하고 안전하게 도입 할 수 있도록 클라우드 도입방법, 절차, 보안위협 대응 방법 등을 안내하여 기업 스스로 안전한 클라우드 환경을 구축하고 이용할 수 있도록 하는데 도움을 주고자 한다. 또한, 클라우드는 4차 산업의 기본 IT 인프라로 활용되는 만큼 4차산업의 IT 안전망을 갖추는데 기여할 것으로 기대한다.

2 구성 및 목적

본 안내서는 기존 온프레미스 환경에서 클라우드 컴퓨팅 환경으로 전환하고자 하는 클라우드 서비스를 이용하는 기업의 정보유출, 해킹사고 등의 보안위협을 해결하는데 도움을 주고자 작성된 것이다.

클라우드 컴퓨팅 서비스와 관련된 보안위협은 사용되는 정보의 기밀성, 무결성, 가용성 보장에 대한 인식 부족과 이를 사용하는 이용자의 특정 서비스에 대한 의존도 증가(Lock-in)에서 발생하는 문제들과 관련성이 깊다. 이에, 우리보다 앞서 클라우드 컴퓨팅 서비스를 도입한 해외사례를 바탕으로 다양한 환경에서 발생할 수 있는 보안위협에 대해서 알아보고 이를 대처하기 위한 핵심 보안요구사항 등을 제시하여 클라우드 서비스 이용기업이 클라우드를 도입하여 운영하는데 있어서 막연한 두려움 등을 해소하고자 한다.

클라우드 서비스 이용 기업은 서비스 도입 계획 시 정보자산, 서비스 제공 모델과 구축 유형에 따라 보안 위험 요소를 사전에 식별, 평가 후 관리대책을 고려해야 하며, 클라우드 서비스 상에서 정보 자산은 데이터, 응용 프로그램 및 프로세스로 분류 할 수 있다. 인프라 요소는 클라우드 서비스 제공자의 관리 및 책임 영역으로 이용기업 입장에서는 관리 대상에서 제외됨으로 본 안내서에서는 클라우드 인프라 제공 사업자(IaaS) 영역인 클라우드 인프라 보안에 대해서는 다루지 않는다.

본 안내서 구성은 2장에서 클라우드 개념, 클라우드 구성 및 분류, 기술 등 클라우드 컴퓨팅에 대한 이해를 돕는 내용을 담았으며, 3장에서는 해외 CSA(Cloud Security Alliance)에서 발표한 보안위협 영역을 중심으로 클라우드 서비스 환경에서 발생 할 수 있는 보안위협을 관리적, 기술적 측면으로 구성하여 기술하였다. 마지막 4장은 기존 온프레미스에서 클라우드 서비스 환경으로 변화함에 따라 안전한 클라우드 보안관리체계를 갖추는데 필요한 보안요구사항과 보안실무자들이 보안실무 측면에서 클라우드 서비스 환경에서 고려해야 하는 내용을 기술하였다.

따라서, 본 안내서는 클라우드 서비스 이용 기업의 IT 담당자 및 보안담당자가 클라우드 인프라 환경에 자사의 서비스를 안전하게 구축 · 이용하는데 필요한 관리적, 기술적 정보보호요구사항을 이해하고 갖추는데 안내자의 역할을 할 것으로 기대한다.

3 용어정의

1. “클라우드컴퓨팅(Cloud Computing)”이란 집적·공유된 정보통신기기, 정보통신설비, 소프트웨어 등 정보통신자원(이하 “정보통신자원”이라 한다)을 이용자의 요구나 수요 변화에 따라 정보통신망을 통하여 신축적으로 이용할 수 있도록 하는 정보처리체계를 말한다.
2. “클라우드컴퓨팅기술”이란 가상화 기술, 분산처리 기술 등 클라우드컴퓨팅의 구축 및 이용에 관한 정보통신기술을 말한다.
3. “클라우드컴퓨팅서비스”란 클라우드컴퓨팅을 활용하여 상용(商用)으로 타인에게 정보통신자원을 제공하는 서비스를 말한다.
4. “이용자”란 클라우드서비스 제공자가 제공하는 클라우드 서비스를 이용하는 개인 또는 법인 고객을 말한다.
5. “IaaS”란 Infrastructure as a Service의 약자로서 서버, 스토리지, 네트워크를 가상화 환경으로 만들어, 필요에 따라 인프라 자원을 사용할 수 있게 제공하는 클라우드 서비스를 말한다.
6. “PaaS”란 Platform as a Service의 약자로서 애플리케이션의 개발 및 시작과 관련된 인프라를 만들고 유지보수하는 복잡함 없이 이용자가 애플리케이션을 개발, 실행, 관리할 수 있게 하는 플랫폼을 제공하는 클라우드 서비스를 말한다.
7. “SaaS”란 Software as a Service의 약자로서 소프트웨어의 기능 중 이용자가 필요로 하는 것만을 서비스로 배포해 이용이 가능하도록 한 클라우드 서비스를 말한다.
8. “하이퍼바이저”란 단일 컴퓨팅시스템에서 서로 다른 다수의 운영체제를 동시에 실행하기 위한 플랫폼 또는 소프트웨어를 말한다.
9. “가상머신(VM:Virtual Machine)”이란 가상화 기술에 의해 논리적 시스템 자원(CPU, 메모리, 디스크, 네트워크 등)을 이용, 독립적으로 OS 운영환경이 실행되는 시스템을 말한다.
10. “가상 인프라”란 가상환경을 제공하기 위해 필요한 하이퍼바이저, 가상 머신, 가상자원 인터페이스 등으로 구성된 인프라를 말한다.
11. “정보보호 활동”이란 정보의 생성, 저장, 처리, 전달 과정에서 발생할 수 있는 정보의 훼손, 변조, 유출 등의 보안 위험을 통제하고 정보에 대해 기밀성, 무결성, 가용성을 확보하는 일련의 활동을 말한다.
12. “정보자산”이란 데이터베이스, 데이터 파일, 문서 등 정보시스템에서 입력, 송·수신, 보관 및 출력되는 모든 형태의 정보자료와 이를 처리하기 위한 정보시스템, 물리적 설비 및 인적 자원 등 정보가치를 지닌 회사의 모든 유·무형 자산을 말한다.
13. “정보시스템”이란 개인용 컴퓨터, 모바일기기, 서버, 네트워크 장비, 정보보호시스템, 통신설비 및 해당 기기의 기능 수행과 관련된 소프트웨어를 말한다.
14. “정보통신망”이란 지리적으로 떨어져 있는 다른 위치에 있는 장치 간에 정보를 교환할 수 있도록 상호 접속을 위해 사용되는 전기 통신 기기와 장치 전송로의 결합을 말한다.
15. “데이터베이스(DB)”란 구조화된 데이터 등의 집합체 및 그 관리 소프트웨어를 말한다.
16. “정보보호시스템”이란 침입차단시스템, 침입탐지시스템 등 정보의 훼손, 변조 및 유출 등을 방지하기

위해 구축된 하드웨어 및 소프트웨어를 말한다.

17. “기밀성”이란 정보자산이 비인가된 개체에 누설되거나 공개되지 않아야 하는 정보보호의 특성을 말한다.
18. “무결성”이란 정보자산이 파손되거나 고의로 변조되지 않고 완전하게 전송되고 보관되어야 하는 정보보호의 특성을 말한다.
19. “가용성”이란 정당한 권한을 가진 개체가 정보자산을 필요로 할 때 지체없이 접근 및 사용할 수 있어야 하는 정보보호의 특성을 말한다.
26. “위협”이란 바이러스, 해킹, 장애 및 내부유출 등 원하지 않은 사건이 발생하여 정보자산에 손실을 줄 수 있는 잠재성을 가진 일체의 것을 말한다.
22. “취약점”이란 정보자산이 가지고 있는 약점으로 위협에 의해 정보자산이 손실을 입을 수 있는 요소 및 환경을 말한다.
23. “위험”이란 정보자산과 취약점, 위협에 의해 정보보호를 실패하게 할 수 있는 잠재요소를 말한다.
24. “개인정보”란 생존하는 개인에 관한 정보로서 성명, 주민등록번호 등에 의해 특정한 개인을 알아볼 수 있는 부호, 문자, 음성, 음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합해 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다.
25. “장애”란 IDC, 서버실 및 장비실의 정보시스템, 통신회선 등이 그 본래의 기능을 상실하여 더 이상 IT서비스를 제공할 수 없는 상태를 말한다.
26. “침해사고”란 해킹, 컴퓨터 바이러스, 논리폭탄, 메일폭탄 및 서비스거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다.
27. “책임추적성”이란 정보시스템 내에서 개인의 행위를 기록하고 추적하는 것을 말한다.
28. “암호키”란 암호화 및 복호화를 위해 암호화 기법 및 프로그램에서 사용하는 키를 말한다.
29. “암호화”란 기밀성 또는 무결성을 보장하기 위해 암호알고리즘으로 평문을 암호문으로 바꾸는 과정을 말한다.
30. “복호화”란 암호화의 반대되는 개념으로 암호화된 데이터를 다시 평문으로 바꾸는 과정을 말한다.
31. “백업”이란 정보시스템의 장애나, 화재와 같은 재해로 인해 저장해 둔 정보가 소실되거나 손상될 경우에 대비하여 일정한 시간 차이를 두고 데이터를 복사하여 별도의 매체(디스크 혹은 테이프 등)에 예비로 저장해두는 행위를 말한다.
32. “자산”정보(데이터), 소프트웨어(컴퓨터 소프트웨어 등), 물리적 자산(서버 등), 서비스, 인력 등 조직에서 보유하고 있는 가치가 있는 모든 것을 말한다.
33. “클라우드 서비스 제공자(관리자)”클라우드 인프라 해당 되는 클라우드 시스템의 서버, 스토리지 등의 IT자원을 관리하는 자를 말한다.
34. “클라우드 서비스 이용자”란 기업에 속한 임직원 또는 해당 기업에서 업무를 외주 위탁한 외주인력 등으로서 기업 업무를 처리하는 자를 말한다.
35. “클라우드 서비스 기업 관리자”란 클라우드 서비스 제공자로부터 할당받은 VM을 해당 기업 내부적으로 분배 등 해당 기업의 클라우드 시스템 등을 관리하는 자를 말한다.
36. “가상화 기술”이란 물리적으로 구분되는 여러 개의 다른 컴퓨터를 논리적으로 통합하여 1개의 컴퓨터로

구성하거나 1개의 시스템을 논리적으로 분할하여 컴퓨팅 자원을 효율적으로 사용하게 하는 기술을 말한다.

37. “컨테이너”란 시스템을 가상화 하는 것이 아닌 어플리케이션을 구동할 수 있는 환경을 가상화 하는 기술을 말한다.
38. “서비스 수준 협약서(SLA)”란 클라우드 기반 서비스의 서비스 품질(QoS : Quality-of-Service) 특성이나 행동양식, 제약사항, 프로비저닝 등을 명시한 클라우드 공급자와 사용자간의 서비스 목표 수준 계약서를 말한다.
39. “온프레미스”란 소프트웨어 등 솔루션을 클라우드 같이 원격 환경이 아닌 자체적으로 보유한 전산실 서버에 직접 설치해 운영하는 방식을 말한다.
40. “시큐어 코딩”이란 안전한 소프트웨어 개발을 위해 소스 코드 등에 존재할 수 있는 잠재적인 보안 취약점을 제거하고, 보안을 고려하여 기능을 설계 및 구현하는 등 소프트웨어 개발 과정에서 지켜야 할 일련의 보안 활동을 말한다.

II. 클라우드 컴퓨팅 기술

1. 클라우드 컴퓨팅 개념
2. 클라우드 컴퓨팅 구성 및 분류
3. 클라우드 컴퓨팅 가상화 기술
4. 클라우드 컴퓨팅 컨테이너 기술

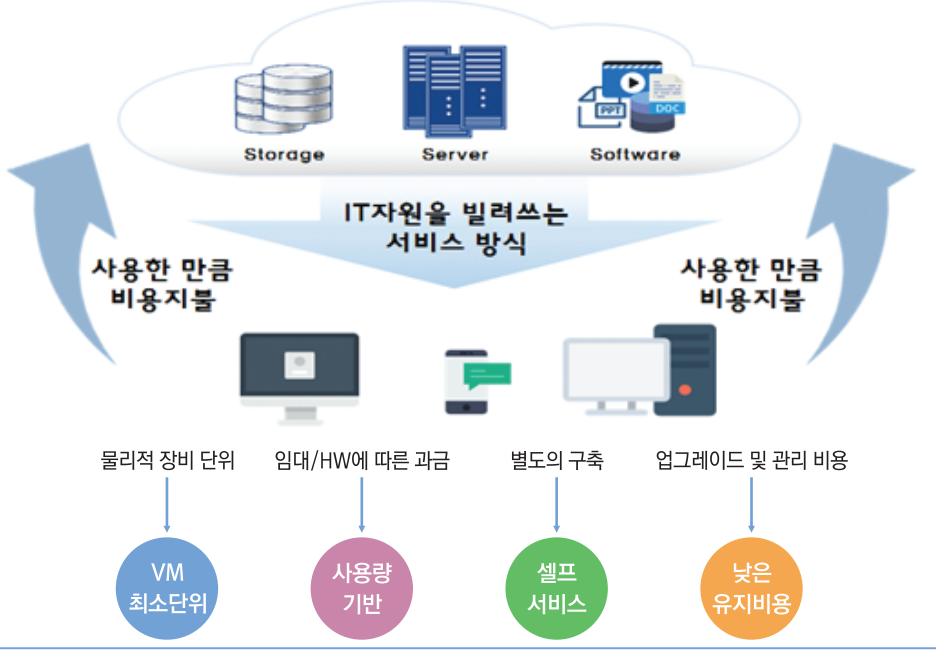
Ⅱ 클라우드 컴퓨팅 기술

1 클라우드 컴퓨팅 개념

클라우드 컴퓨팅이란 '집적 · 공유된 정보통신기기, 정보통신설비, 소프트웨어 등 정보통신자원을 이용자의 요구나 수요 변화에 따라 정보통신망을 통하여 유동적으로 이용할 수 있도록 하는 정보처리체계'를 의미한다. 즉 클라우드 컴퓨팅은 이용자가 IT자원(소프트웨어, 스토리지, 서버, 네트워크)을 필요한 만큼 빌려서 사용하고 서비스 부하에 따라서 실시간 확장성을 지원받으며, 사용한 만큼 비용을 지불하는 컴퓨팅 환경을 말한다.

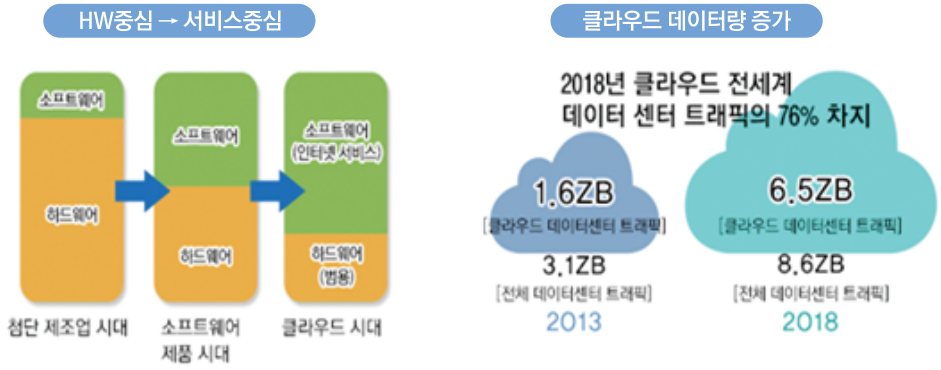
※ 1965년 미국의 전산학자 존 매카시(John McCarthy)의 '앞으로의 컴퓨팅 환경은 공공 서비스(Public Utility)를 사용하는 것과도 같을 것' 이라는 개념에서 시작되었으며, 구글의 전 최고경영자(CEO) 에릭 슈미트(Eric Schmid)가 2016년 미국 산호세에서 열린 검색엔진전략 컨퍼런스에서 '클라우드 컴퓨팅' 용어를 사용하면서 대중에게 널리 알려졌다.

[클라우드 컴퓨팅 개념]



2006년부터 확산된 클라우드 컴퓨팅의 변화는 HW중심→설치형SW→ HW · SW를 서비스 형태로 사용하는 클라우드 시대로 ICT 패러다임이 변화하고 있다. 특히, IoT와 빅데이터, 모바일 등이 성장하면서 데이터양이 비약적으로 폭증하고 있는데, 그 중 클라우드가 데이터 트래픽의 76%를 차지한다. 또한 클라우드

시장규모도 전세계 연평균 16.9%, 국내 17.7%로 급성장하고 있다. 이는 비용절감, 업무혁신을 위해 정보시스템을 자체 구축하는 방식에서 정보자원을 빌려 쓰는 클라우드 컴퓨팅 방식으로 패러다임이 변화하고 있다는 것을 말해준다.



* 클라우드 컴퓨팅 활성화 계획('15, 과학기술정보통신부)/클라우드혁신센터

사용한 만큼의 비용을 지불하는 클라우드는 기존 구축형 시스템에 비해 비용, 기간 등의 측면에서 여러 가지 장점을 가지고 있다. 특히, 인프라를 직접 구축하기 어려운 사업자들은 클라우드 서비스 도입을 긍정적으로 생각하고 있다. 이러한 클라우드 도입의 패러다임은 IT자원이 소유의 개념에서 공유의 개념으로 변화하면서 이루어졌다. 기존 소유개념의 구축형 컴퓨팅 방식과 공유개념의 클라우드 컴퓨팅 방식의 차이는 다음과 같다.

[구축형 환경 vs 클라우드 환경]

구축형(소유형) 환경	클라우드(공유형) 환경
많은 초기 구매 비용(HW임대 및 구축)	초기 투자비용 없음
인력, 패치 및 업그레이드 등 높은 유지비용	낮은 유지비용
고정 용량 및 정해진 자원 할당	유연한 용량 및 효율적인 자원 할당
구매 및 설치	신청 후 빠른 서비스 이용 가능
지리적 한정	지리적 한정 없음
한정된 트래픽 처리	대규모의 트래픽 수용가능

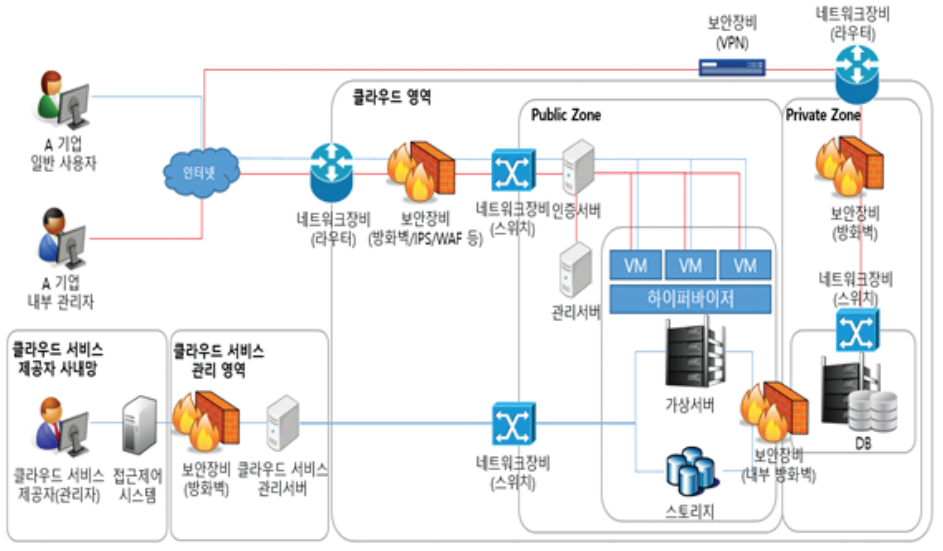
여러 장점들 중 클라우드는 기존 컴퓨팅 환경과 달리 가상화 기술을 적용하여 할당하였던 자원을 회수, 다른 사용자에게 재할당 등의 효율적인 자원 관리가 용이하고, 물리적 자원을 논리적으로 분할하고 다수의 가상머신 운용이 가능하여 서버 또는 PC 구입비용 등의 비용 절감이 가능해 진다. 다만, 데이터가 클라우드 서버로 집중되어 있어 해킹(또는 장애)시 그 안에 저장되어 있는 정보 등의 자료 유출, 손실 등의 보안 위협 증가되는 것에 대한 대책마련이 필요하다.

2 클라우드 컴퓨팅 구성 및 분류

일반적인 클라우드 컴퓨팅의 주요 구성요소로는 보안장비, 서브넷 분리 또는 부하분산을 위한 네트워크 장비, 클라우드 자원을 관리하는 클라우드 인프라 관리서버, 가상 머신이 구동되는 가상서버, 클라우드 사용자가 가상서버를 통해 생성한 데이터를 저장하는 공간인 스토리지 등이 있다.

클라우드 컴퓨팅 구성원에는 클라우드 서비스를 이용하는 기업의 일반 사용자, 클라우드 서비스 제공자로부터 할당받은 VM을 내부적으로 분배하는 기업 내부 관리자, 클라우드 시스템의 서버, 스토리지 등의 자원과 전체 클라우드 영역의 자원 사용률을 관리하는 클라우드 서비스 제공자(관리자)가 있다. 클라우드 컴퓨팅 구성도는 다음과 같다.

[클라우드 컴퓨팅 구성도]



[클라우드 컴퓨팅 구성요소 별 역할]

구성요소	내용
보안장비	방화벽, IDS, IPS, DDoS 장비, VPN 등이 있으며, 외부 공격 대응 및 안전한 통신을 위한 장비
네트워크장비	라우터, 스위치 등이 있으며, 트래픽 부하분산 및 서브넷 분리 위한 장비
접근제어시스템	클라우드 서비스 관리 영역에 대한 접근 감사, 허용, 차단
클라우드인프라 관리서버	클라우드 환경의 서버, 스토리지 등 IT 자원과 전체 클라우드 서비스 사용자의 자원 사용률 등을 관리
인증서버	클라우드 환경에 접근이 허용된 사용자를 등록 · 관리하며, VM에 접근하는 사용자 인증

구성요소	내용
관리서버	클라우드 서비스 제공자로부터 할당받은 VM을 기업 내부적으로 할당
가상서버	하이퍼바이저 기술을 이용해 다수의 가상머신을 구동
스토리지	클라우드 사용자가 가상서버를 활용하여 생성한 데이터를 저장하는 공간
DB	사용자 정보, 금융정보 등 민감 정보를 저장 ※ DB는 주로 외부망과 분리되어있는 Private Zone에 구축

클라우드 컴퓨팅은 이용자가 클라우드 컴퓨팅 서비스에 접근할 수 있는 형태에 따른 분류인 서비스 모델(Delivery Model)과 구현방식에 따른 분류인 배치모델(Deployment Model)로 구분할 수 있다.

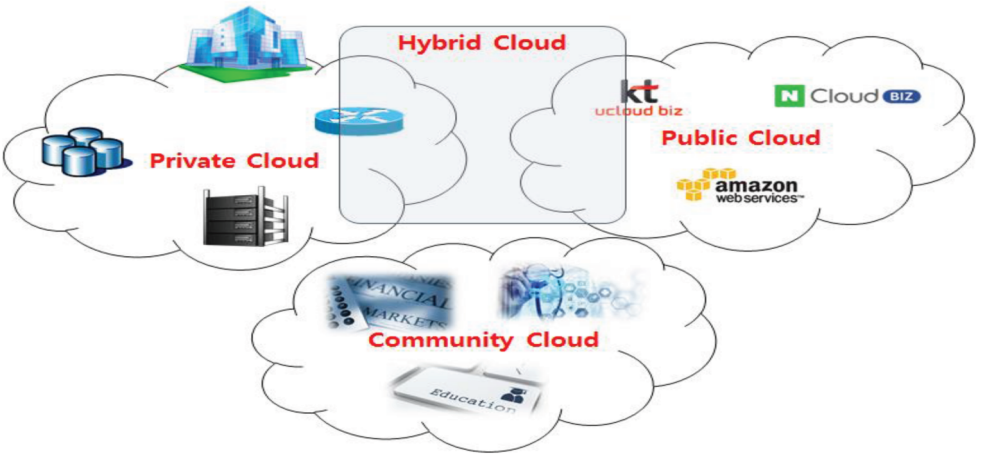
먼저 서비스 모델에 따른 분류는 응용SW를 서비스 제공하는 SaaS (Software -as-a-Service), SW 개발환경(플랫폼) 서비스를 제공하는 PaaS (Platform-as -a-Service), IT인프라(서버, 스토리지 등) 서비스를 제공하는 IaaS (Infrastructure -as-a-Service)로 분류된다.

[클라우드 서비스 모델에 따른 분류]

- SaaS : **소프트웨어/어플리케이션을 제공하는 목적으로 만들어진 모델, 표준화된 어플리케이션 프로세스 제공 (웹메일 서비스,** iCloud, Dropbox, Google Docs, One note **등)**
- PaaS : **개발자가 자신의 어플리케이션을 개발, 테스트, 실행 할 수 있는 컴퓨팅 플랫폼을 제공 제공하는 서비스** (Linux, Apache, PHP, MySQL, MS Azure, Google Apps **등)**
- IaaS : **서버, 스토리지, 네트워크 등 인프라 자원을 사용량 기반으로 제공, 기본 스토리지와 컴퓨팅 능력을 제공**(CPU, Disk **등)**(Amazon EC2, S3 **등)**

구현방식에 따른 분류는 ①기관 내부적으로 구축·이용하는 프라이빗 클라우드(Private cloud), ②외부 사업자의 서비스를 활용하는 퍼블릭 클라우드(Public cloud), ③프라이빗·퍼블릭을 조합한 하이브리드 클라우드(Hybrid cloud)로 분류된다.

[클라우드 구현 방식에 따른 분류]



①퍼블릭 클라우드에서는 클라우드 사업자가 클라우드 서비스와 사용자들을 위한 접근제어 기능을 제공한다. 이 모델은 비용 면에서는 사용자에게 장점을 제공하지만, 각 클라우드 사용자를 위하여 클라우드 컴퓨팅 환경을 커스터마이징 할 수 있는 유연성 면에서는 제한점을 가진다.

②프라이빗 클라우드에서는 클라우드의 사용자 혹은 기관이 스스로 전용의 클라우드 인프라를 구축 및 관리함으로써, 데이터의 저장 및 처리도 해당 조직 내에서 처리할 수 있다는 특징이 있다. 이 모델에서는 사용기관의 목적에 맞게 커스터마이징 할 수 있는 유연성은 높지만, 초기 도입 비용이 비싸고 구축에도 시간이 걸리는 단점을 가진다.

③하이브리드 클라우드 하이브리드 모델은 비용 면에서의 효율성을 높이기 위해, 이들 두 가지 모델을 조합하여 구축하는 모델이다.

구분	장점	단점
퍼블릭 클라우드	• 초기 투자비용 없음 • 융통성 있는 사용량 조절	• 서비스 제공자 기업의 의존도가 높음
프라이빗 클라우드	• 기존 IT 자원을 활용 가능 • 행위추적 용이	• 초기 투자비용이 많이 소요
하이브리드 클라우드	• 기존 IT 자원을 활용 가능 • 서비스 구성변경 용이	• 운용비와 도입비용 증가
커뮤니티 클라우드	• 초기 투자비용 없음 • 융통성 있는 사용량 조절	• 서비스 제공자 기업의 의존도가 높음
공통정보보호 요구사항	외부에서 내부(클라우드) 시스템 접속이 이루어져 함에 따라 통신구간 암호화, 내부 시스템 보호를 위한 방화벽, 침입방지 시스템 구축 등 주요 보호조치 필요	

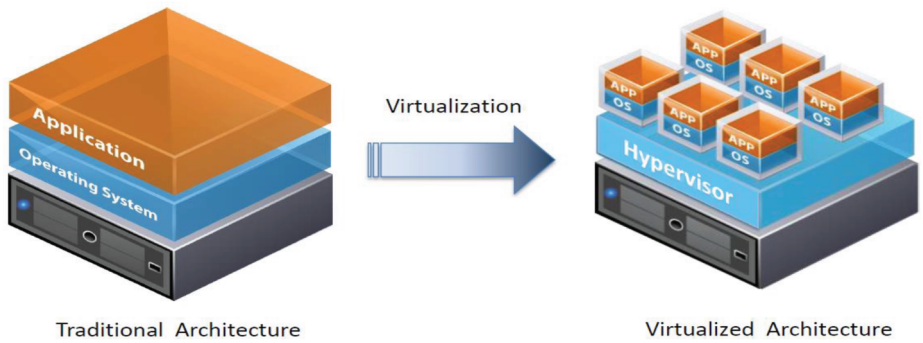
세 가지 클라우드 배치 모델에 추가적으로 커뮤니티 클라우드 모델이 있다. ④커뮤니티 클라우드 모델은 특수한 보안 요구사항이나 협업 등과 같은 공통의 목적을 가지고 클라우드 IT 인프라를 운용하는 모델이다.

3 클라우드 컴퓨팅 가상화 기술

클라우드 개념에서 살펴보았듯이 클라우드의 핵심기술은 가상화 개념을 컴퓨터상에 적용하고 이를 이용할 수 있도록 환경을 구성했다는 것이다. 따라서 본 절에서는 클라우드의 핵심기술인 가상화 기술에 대해 살펴보겠다. 먼저 가상화의 개념에 대해서 알아보고 가상화의 종류와 기술에 대해 살펴본다.

가상화는 단일의 물리적인 IT자원을 동시에 논리적인 다수의 IT자원으로 사용할 수 있도록 해주는 기술이다. 기존의 컴퓨터 환경에서는 단일의 하드웨어에서 단일의 운영체제가 수행될 수밖에 없고, 해당 운영체제가 하드웨어를 독점한다. 그러나, 가상화 기술을 적용하면 단일의 하드웨어 상에서 복수개의 논리적인 가상머신을 동시에 구동할 수 있으며, 각각의 가상머신에 서로 다른 종류의 운영체제를 독립적으로 구동시켜 사용할 수 있다.

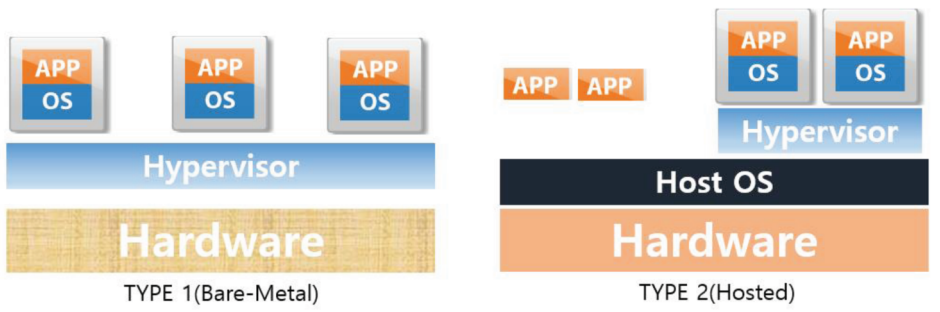
[가상화 아키텍처]



하이퍼바이저는 가상머신과 하드웨어 사이에 위치하여 다수의 가상머신들이 각각의 운영체제가 구동될 수 있도록 논리적으로 독립된 가상머신 환경을 제공해 주며, 주 기능은 CPU, 메모리 등 하드웨어 자원을 각 가상머신에 논리적으로 분할 할당 · 스케줄링을 담당한다. 하이퍼바이저는 2가지 타입으로 나뉜다. 첫 번째인 TYPE 1은 bare-metal 타입이라고 불리며, 하드웨어 상에서 직접 동작하며 그 상부에 가상머신들이 동작할 수 있는 환경을 제공 한다. 두 번째인 TYPE 2는 hosted 타입으로 하드웨어 상에 직접 동작하는 것이 아니라 호스트 운영체제 위에 하이퍼바이저가 위치하는 구조로 동작한다.

TYPE 1은 하드웨어 상에서 바로 동작하는 형태로 고성능의 가상화를 제공하는 것이 특징이며, 오픈소스인 Xen(Citrix, 2014)과 KVM, VMware ESXi와 MS Hyper-V 등 대표적이다. TYPE 2는 개인 컴퓨터의 운영체제 상에 응용프로그램의 형태로 인스톨되어 가상머신을 구동할 수 있는 환경으로 설치 및 사용상의 편의성 좋으며, VMware Workstation, VMware Fusion, Parallels Desktop, Oracle VirtualBox 등이 대표적이다.

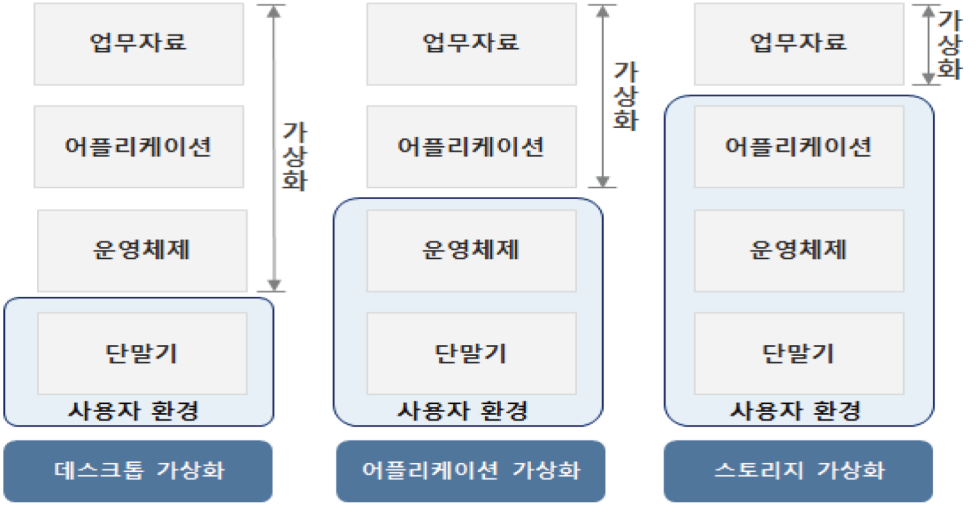
[하이퍼바이저 타입]



기존의 IT인프라 환경에서는 필요한 물리적 IT 자원(서버, 네트워크 장비 등)을 도입하는 데에 일반적으로 수개월이 소요된다. 하지만, 가상머신의 경우 생성, 중단, 재시작, 복사, 종료, 제거 하는 등의 설치 및 관리 과정이 수 분 내에 이루어 질 수 있는 등 자원들의 설치 및 관리가 용이하다는 게 특징이다.

가상화의 종류는 가상화 대상과 가상화 범위를 기준으로 나뉜다. 가상화에는 데스크탑, 어플리케이션 가상화, 스토리지 가상화, 서버 가상화, 네트워크 가상화 등이 있다.

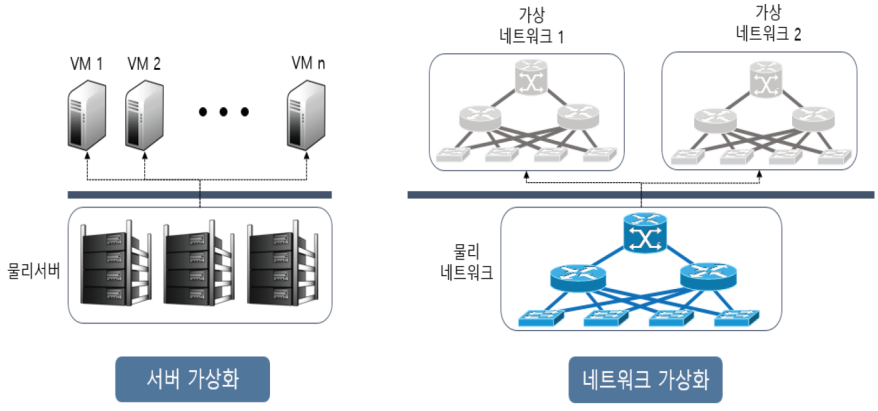
[가상화 종류(데스크톱, 어플리케이션, 스토리지]



구분	내용	
데스크톱 가상화	사용자의 데스크톱에서 Vista, Window7 등 이기종의 OS 사용 가능	
	장점	• PC에 두 종류 이상의 OS 설치가 가능하여 업무 효율화 • 가상머신 재구축 및 삭제 용이
	단점	• 데스크톱보다는 성능 및 속도가 느려 고성능 시스템자원 제공 미흡

구분	내용	
어플리케이션 가상화	어플리케이션을 가상화하여 사용자 컴퓨터에 설치하지 않고 중앙의 가상화 서버에 설치/구동하는 방식	
	장점	• 일괄 배포 및 업데이트를 통한 어플리케이션 관리 용이 • 중앙서버에서 모든 자료를 처리/저장 하므로 정보유출 방지
	단점	• 사전에 공동으로 사용하도록 구성된 어플리케이션만 사용가능 • 네트워크 환경에 따라 처리 및 응답속도 지연 가능성 존재
스토리지 가상화	개별 스토리지를 통합하여 저장 용량이 하나로 통합된 가상 스토리지를 만들고 재할당하는 방식	
	장점	• 웹 오피스, 업무포털 등과의 연동으로 여러 용도로 활용 가능
	단점	• OS, SW 설치 및 업데이트 등의 개별 관리 필요

[가상화 종류(서버, 네트워크)]

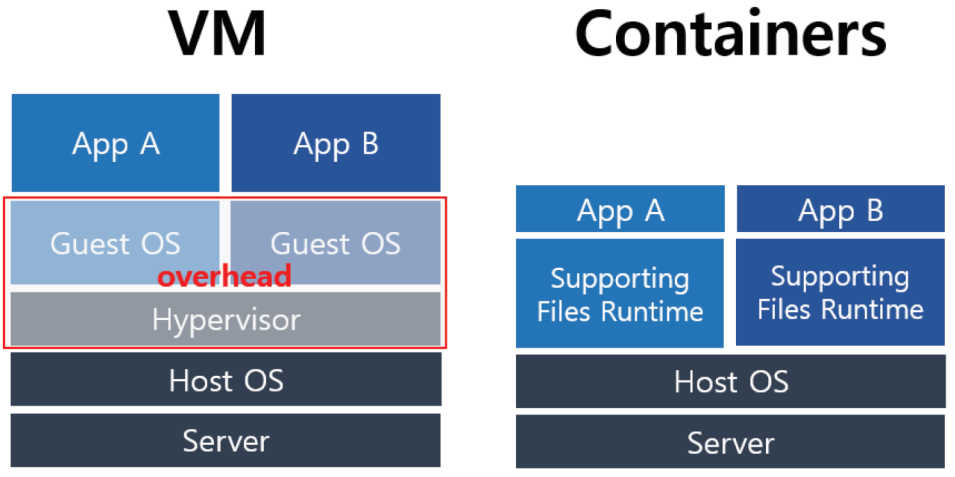


구분	내용	
서버 가상화	물리적 서버 수 십대를 가상 서버로 통합하여 필요한 서버로 재생성하고 할당하여 전체 관리비용을 감소시키는 방식	
	장점	• 유동적 IT 자원 구축 및 확장 가능
	단점	• 자료의 중앙 집중화로 인해 해킹에 의한 자료 유출 위험성 존재 • 장애 발생 시 원활한 업무 진행 차질
네트워크 가상화	네트워크 리소스(하드웨어 및 소프트웨어)를 물리적 요소가 아니라 논리적 요소로 구축하고 관리하는 기술로 여러 개의 물리적 네트워크를 논리적 네트워크 하나로 통합하거나 물리적 네트워크 하나를 각각 구분되는 여러 개의 논리적 네트워크로 세분화하는 방식	
	장점	• 네트워크 장비들의 통합 관리가 가능하며 보안 배치 작업 용이
	단점	• 물리적인 네트워크에 비해 복잡한 구성

4 클라우드 컨테이너 기술

앞서 살펴본 것과 같이 가상머신을 이용한 가상화 기술은 하이퍼바이저를 통해 다양한 OS 환경을 구축할 수 있다는 이점이 있다. 하지만 가상머신마다 OS가 설치되기 때문에 하이퍼바이저와 OS 운영으로 인한 오버헤드가 발생하며, 개발자는 운영체제 및 커널의 버전을 고려해 개발환경을 구축해야 한다는 부담이 있다. 이런 문제를 해결할 수 있는 기술로 컨테이너가 등장했다. 본 절에서는 컨테이너의 핵심 개념과 컨테이너를 사용했을 때 개발자 혹은 클라우드 서비스를 이용하려는 기업이 얻을 수 있는 이점에 관해 살펴본다.

[가상머신과 컨테이너]



위 그림은 가상화와 컨테이너의 차이를 보여주고 있다. 단일 시스템에서 여러 운영체제가 동시에 실행될 수 있도록 하는 가상화와 달리, 컨테이너는 리눅스 커널의 기능인 cgroup[1]과 namespace[2]을 통해 서로 다른 어플리케이션 프로세스별로 공간을 격리한다. 또한, 컨테이너가 호스트 OS 자원을 공유하기 때문에 격리된 공간마다 게스트 OS를 설치할 필요가 없다. 따라서 가상머신 환경에 비해 오버헤드가 적으며, 가상 하드디스크 용량이 GB 단위인 가상머신에 비해 이미지 용량이 수백 MB로 작고 설치가 빠르다는 이점을 지닌다.

1) cgroup : 프로세스들의 CPU, 메모리 등의 자원 사용을 제어하고 격리시키는 리눅스 커널 기능

2) namespace : 하나의 시스템에서 수행되지만, 각각 별개의 독립된 공간인 것처럼 격리된 환경을 제공하는 가상화 기술

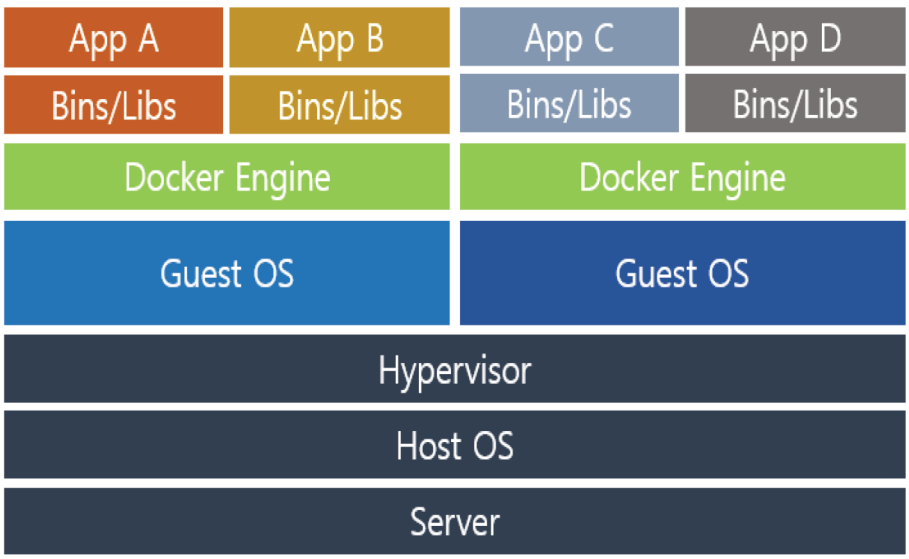
최근 가장 주목받는 컨테이너 기반의 오픈소스 가상화 플랫폼으로 도커를 꼽을 수 있다. 도커는 이미지와 컨테이너로 구성되어 있는데 이미지는 서비스 운영에 필요한 프로그램, 라이브러리를 포함한 파일이고 컨테이너는 이미지를 실행한 상태를 말한다. 즉, 이미지는 운영체제의 실행 파일과 유사하며, 컨테이너는 프로세스로 볼 수 있다. 이미지는 개발자 개인이 생성하여 실행하거나 도커 허브라는 이미지 공유 저장소에서 다운받아 실행할 수 있어, 하이퍼바이저와 게스트 OS를 설치해야 하는 가상머신보다 간편하게 환경

구성이 가능하다.

도커는 이미지 형태로 배포가 가능하기 때문에 하나의 이미지로 여러 개의 컨테이너를 생성할 수 있다는 특징을 지닌다. 이는 클라우드 환경에서 사용되는 Auto Scaling1) 기능과 시너지 효과를 낼 수 있다. 서비스 운영 환경을 이미지로 만들어 서버에 배포한 후, 서버에서 해당 이미지를 실행하여 간편하게 서비스를 확장할 수 있다.

1) Auto Scaling : 클라우드 컴퓨팅 서비스에서 서비스의 부하량과 사용량에 맞게 탄력적으로 컴퓨팅 자원을 늘리거나 줄이는 기능

[가상머신과 도커의 공존]



클라우드 시스템을 이용하려는 기업이 컨테이너를 사용해서 얻을 수 있는 가장 큰 이점은 비용절감이다. 클라우드 인프라 제공자는 클라우드 인프라를 임대하여 사용하는 기업이 생성한 가상머신 수를 기반으로 요금을 부과한다. 즉, 가상머신을 추가할수록 기업이 지불해야 하는 요금이 증가하는 구조이다. 기업입장에서 비용절감을 위해 서비스 하나를 생성할 때마다 가상머신을 추가하는 대신, 위 그림과 같이 한 가상머신에 여러 개의 컨테이너를 생성하여 서비스 환경을 구축하는 것이 합리적이다.

클라우드 서비스를 이용하는 기업 IT담당자 위한

클라우드 정보보호 안내서

III. 클라우드 컴퓨팅 보안위협

1. 클라우드 컴퓨팅 보안위협 개요
2. 클라우드 컴퓨팅 관리적 보안위협
3. 클라우드 컴퓨팅 기술적 보안위협

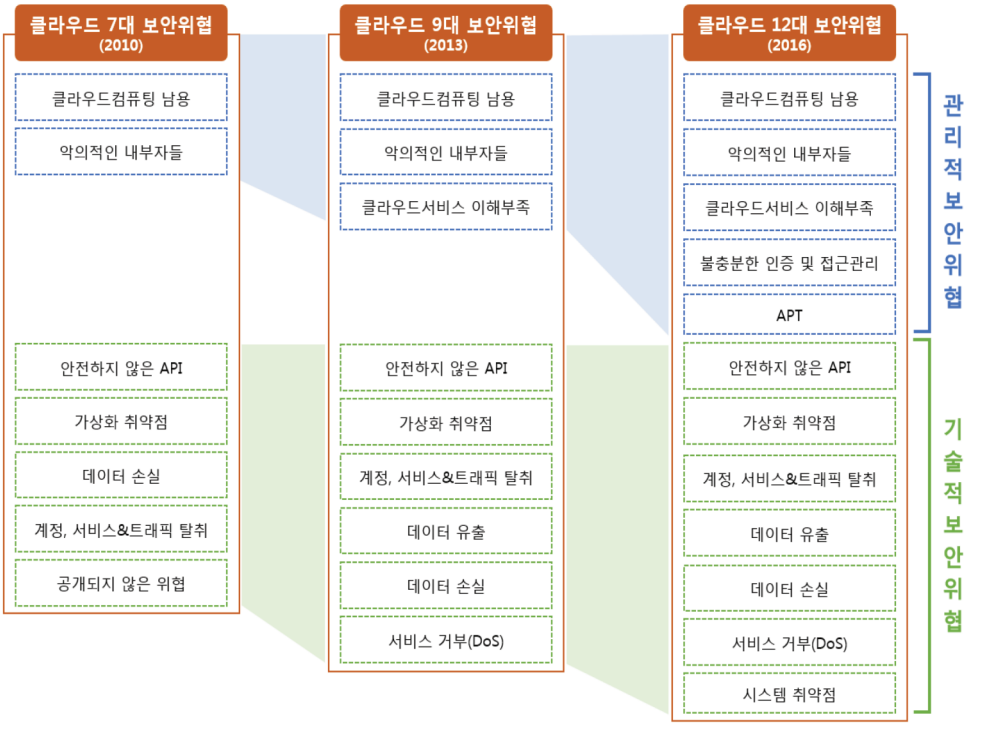
Ⅲ 클라우드 컴퓨팅 보안위협

1 클라우드 컴퓨팅 보안위협 개요

클라우드 컴퓨팅은 가상화(하이퍼바이저 등) 기술 적용, 정보의 외부위탁, 자원의 공유, 다양한 단말기의 접속이라는 특징을 가지고 있다. 이러한 특징에 따라 클라우드 컴퓨팅에 대한 보안위협도 다양하게 발생할 수 있어, 클라우드서비스의 제공자와 이용자는 보안위협을 정확히 인식하여 이러한 위협들을 최소화할 수 있도록 주의가 반드시 요구된다.

클라우드 컴퓨팅 보안위협에 대한 연구는 CSA(Cloud Security Alliance)를 중심으로 클라우드 환경에서 발생할 수 있는 보안위협들을 2010년, 2013년, 2016년 지속적으로 발표하고 있다. 2010년 클라우드 컴퓨팅 7대 위협, 2013년 클라우드 컴퓨팅 9대 위협, 2016년 클라우드 컴퓨팅 12대 위협과 같이 클라우드서비스의 도입 및 이용이 활성화됨에 따라 클라우드 컴퓨팅 보안위협도 관리적, 기술적 범위에서 점진적으로 늘어나고 있다.

[CSA 클라우드서비스의 보안위협 현황]



2 클라우드 컴퓨팅 관리적 보안위협

클라우드 컴퓨팅은 수많은 이용자들이 대용량의 인프라를 공유하며, 데이터 역시 중앙집중식으로 관리하여 접근할 수 있는 "멀티테넌트(multi-tenant)" 환경이다. 이러한 멀티테넌트 환경은 다수의 이용자가 하나의 서비스를 공유함에 따라, 관리적 측면에서 보안 위험성에 대한 우려가 높다. 주요 클라우드 컴퓨팅의 관리적 보안 위협으로는 클라우드 컴퓨팅 남용, 악의적인 내부자들, 공개되지 않은 위협, 클라우드 서비스 이해 부족, 불충분한 식별자, 권한 및 접근관리 그리고 APT공격이 있다.

1. 클라우드 컴퓨팅 남용

클라우드 컴퓨팅의 장점은 대용량의 컴퓨팅(CPU, 메모리 등), 네트워크 그리고 저장 공간을 손쉽게 구매하여 이용할 수 있다는 점이다. 이러한 컴퓨팅 자원은 일반 기업 또는 이용자가 원활하게 업무를 수행하는데 유용한 도구가 되지만, 한편 해커들에게도 악의적인 행위(암호 해독, 패스워드 크래킹 등)를 위한 도구로도 제공될 수 있다. 달리 말하면 해커도 같은 가상공간에 입주하여 다양한 악의적인 행위(스팸, 악성코드 유포 등)를 할 수도 있으며, 이는 공유된 모든 이용자에게 대규모의 피해를 발생시킬 우려가 높다는 뜻으로도 해석할 수 있다.

클라우드 컴퓨팅의 남용을 막는 것은 쉬운 일이 아니다. 기술적으로 기존 대부분의 네트워크 보안 장비들은 가상머신 간 네트워크 트래픽을 확인할 수 없으며, 동일한 호스트 상의 가상머신에서 발생한 공격도 탐지하거나 차단하지 못하는 것이 현재 상황이다. 따라서 기술적인 방법보다는 클라우드 컴퓨팅 서비스를 최초로 가입 · 등록 시 사용자의 신원을 철저하게 검증하는 절차를 도입하고, 주기적으로 이용자 모니터링 등의 관리적 · 정책적 방법이 좀 더 우선되어야 할 것이다.

2. 악의적인 내부자들

클라우드 컴퓨팅에 기반을 둔 서비스는 많은 사용자들이 동시에 사용하도록 운영되는 것이 보통이다. 그래서 기업의 클라우드 서비스는 기업 내 사용자 뿐만 아니라 협력사의 사용자들도 사용하는 경우가 많다. 퇴사한 직원의 계정이 즉시 삭제되지 않았거나, 직무의 조정으로 인해 접근할 수 없어야 하는 권한이 아직 유효한 것을 악용하는 것이 대표적인 사례이다. 악의적인 내부 사용을 막기 위해서는 사용자의 계정과 권한에 대해서 지속적인 관리와 감사가 이루어져야 한다. 특정한 사용자에게 많은 권한이 집중되는 것을 막기 위해 권한을 분산시키는 것도 좋은 방법이다.

[다양한 유형의 내부자 위협]

3. 공개되지 않은 위협

클라우드 컴퓨팅이 제대로 자리 잡기 전까지 클라우드 컴퓨팅 환경에서 발생할 잠재적인 보안 위협은 분명하게 드러나지 않을지도 모른다. 이에 따라 일부 클라우드 컴퓨팅을 도입하기 원하는 기업들은 여전히 클라우드 컴퓨팅의 보안 위협을 제대로 인식하지 못한 채 클라우드 컴퓨팅이 주는 장점들에만 주목할 수 있다. 또한 클라우드 서비스 제공업체들의 투명성도 떨어지게 되어 이용 고객들은 자신이 이용하는 클라우드 컴퓨팅 시스템의 구성이나 소프트웨어 설치 및 실행에 많은 어려움을 겪을 수 있다. 이러한 알 수 없는 잠재적 위협을 줄이기 위해서는 클라우드 서비스 이용 고객이 위협으로부터 대응 및 조치를 할 수 있도록 관련된 정보(해당 로그, 데이터 그리고 인프라의 세부 정보)를 공개하고, 보안위협에 대한 모니터링 및 경고를 보강하여야 한다.

[ZERO DAY 공격 위협]

4. 클라우드서비스 이해 부족

존의 서버 기반 환경에서 가상화를 채용한 클라우드 기반으로 전환하는 것은 자원의 운영 효율성과 가용성의 증대에서 매력적으로 보일 수 있다. 그러나 기존의 업무시스템을 가상화하여 가상머신으로

동작하게 되면 하드웨어나 네트워크를 직접적으로 제어하는 등의 일은 불가능해진다. 업무시스템이 클라우드의 가상화 환경에서 안전성을 충분히 확보할 수 있는지의 여부를 미리 충분하게 검토할 필요가 있다. 클라우드 환경에 대한 이해의 부족은 가상화된 후의 시스템에 치명적인 취약점을 야기할 수 있기 때문이다.

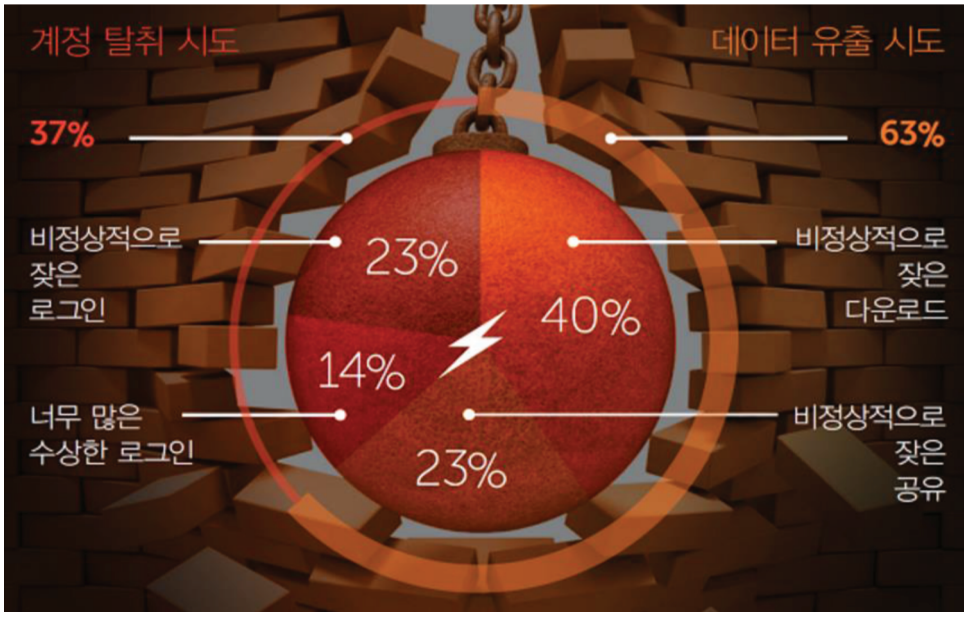
5. 불충분한 식별자, 권한 및 접근관리

다수의 이용자가 접근할 수 있는 클라우드컴퓨팅 환경은 이용자에 대한 식별 및 접근제어가 쉽지 않다. 또한 분산 파일시스템을 통해 대용량 데이터가 다수의 서버들에 혼재되어 저장 · 관리됨에 따라 데이터 접근제어에 대한 어려움이 증가하고 있으며, 다양한 이종의 클라우드와 온프레미스 시스템을 함께 관리해야 하이브리드 클라우드 환경의 계정관리는 더욱 쉽지 않다.

또한 「2016년 하반기 섀도(Shadow) 데이터 리포트 (2016, 시만텍)」에 따르면, 기업 클라우드에 저장된 1억7300만개의 문서 중 23%가 광범위하게 공유되고 있는 것으로 조사됐다. 이 중 3%는 개인정보 등 기밀 정보를 포함하고 있으며, 공유 대상도 전체 기업 조직뿐 아니라 제3자, 일반 대중까지 공유하고 있다. 기업의 클라우드 서비스 담당자도 자신이 쓰는 클라우드 애플리케이션(평균 928개) 중 극히 일부(5% 수준인 30~40개)만 인지하고 있을 정도로, 관리의 사각지대에 있는 '섀도 데이터'도 늘고 있다.

따라서 클라우드서비스 이용에 있어 보안의 핵심은 사용자 인증 및 권한 관리가 되어야 하며, 다양한 규모와 환경에 적용 가능한 통합인증기술(SSO, OpenID 등)이 선결되어야 할 것이다.

[클라우드에서 발생하는 보안사고]



※ [출처] 2016 상반기 섀도 데이터 보고서 (시만텍)

6. APT(Advanced Persistent Threat)

APT 공격은 이제까지의 악성코드, 해킹 기법들과는 다른 형태의 위협이다. 잠복 기간이 길고, 다양한 패턴의 공격 방식이 복합적으로 적용되기 때문에 일반적인 보안 정책으로는 예방과 대응이 어려운 것이 현실이다. 물론 현재 출시된 다양한 보안 솔루션들과 기법들을 통해 APT 공격에 일부 대응하고 있으나 대부분이 기술적 대응 방안에만 치중하고 있으며, 다양한 공격 기법이 복합적으로 활용될 경우에는 종합적으로 대응할 수 없다. 최근 클라우드 서비스로의 전환이 대규모로 이루어지고 있는 상황을 고려할 때, 클라우드 환경은 큰 돈벌이가 될 수 있는 매력적인 공격 목표물이 되고 있다. 특히, 클라우드 환경의 특징인 다양한 단말의 원격 접속, 데이터의 중앙 집중 관리 등으로 APT 공격의 침투 경로가 매우 용이하다고 볼 수 있다.

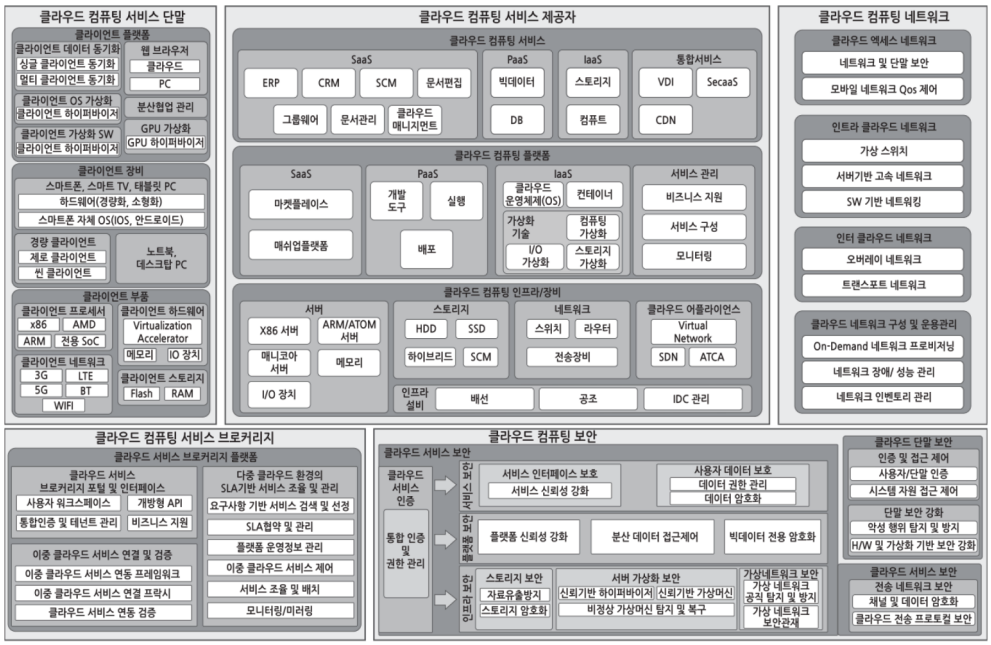
"2017년 10대 보안 전망 보고서(시만텍)"에 따르면, 2017년 주목해야 할 10가지 보안 이슈 중 클라우드컴퓨팅 확산에 따라 보안이 새로운 전환점을 맞이할 것이라고 발표했다. 즉, 웨어러블, 가상현실, IoT 등 새로운 IT기술의 기반이 되는 클라우드컴퓨팅 환경이 확산되면서 기존의 엔드포인트 보안에서 애플리케이션과 서비스 전반에서 사용자와 관련 정보를 보호하는 방향으로 보안 활동의 초점이 옮겨가게 될 것이다. 따라서 APT 공격에 보다 효과적으로 대응하기 위해서는 효율적인 악성코드 탐지 등의 기술적 대응뿐만 아니라 서비스 보호를 위해 기술적/관리적 대응 방안을 함께 고려할 필요가 있다.

3 클라우드 컴퓨팅 기술적 보안위협

클라우드 서비스가 이용자에게 언제 어디서나 인터넷 접속을 통해 다양한 서비스를 제공하고 있지만, 그 이면에는 아래 그림과 같이 이용자가 모르는 복잡한 인프라 구조와 다양한 최신 기술이 집약된 형태를 가지고 있다. 이렇게 최신 기술이 복합적으로 집약된 클라우드 컴퓨팅 환경에서는 기술적으로 보안에 취약해지는 역설적인 상황이 발생할 우려가 높다.

주요 클라우드 컴퓨팅의 기술적 보안 위협으로는 안전하지 않은 API, 가상화 취약점, 계정, 서비스 및 트래픽 탈취, 데이터 유·손실, 서비스 거부공격(DDoS) 그리고 시스템 취약점이 있다.

[클라우드 컴퓨팅 통합 스택]



※ [출처] 2015 클라우드 컴퓨팅 기술 스택(2016년 1월, 클라우드컴퓨팅연구조합)

1. 안전하지 않은 API (Application Programming Interface)

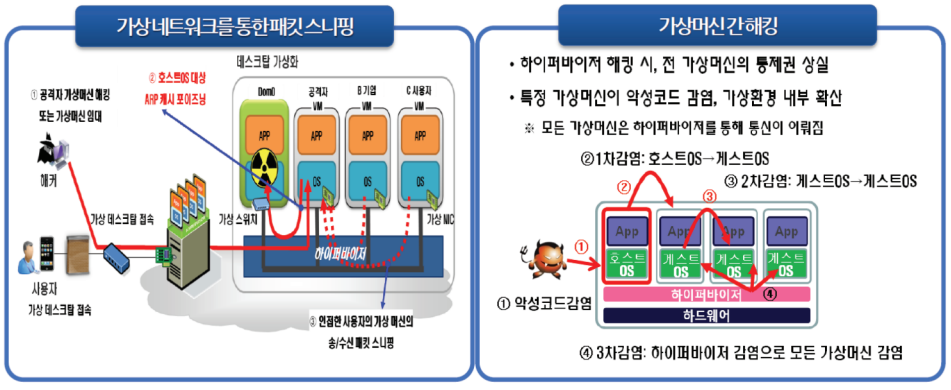
클라우드 서비스 제공업체는 서비스 모델(IaaS, PaaS, SaaS)에 따라 다수의 어플리케이션을 이용하거나 대용량의 데이터에 접근할 수 있도록 다양한 API(권한설정, 서비스모니터링 등)를 제공하고 있다. 하지만, 안전하지 않은 API의 취약점을 통해서 등의 보안 사고가 발생할 수 있다. 안전한지 않은 API를 공개하여 다양한 기능을 활용할 수 있는 반면, 악의적인 클라우드서비스 이용자에게 노출된 API로 인해 기밀 데이터 유출, 악의적인 시스템 제어 등으로 금전적 손실이 발생한 우려도 매우 높다.

또한 안전하지 않은 API의 취약점을 통해서 사용자의 인증을 우회한다거나 정상적인 경로로는 접근할 수 없는 데이터에 대해서 접근할 수 있는 등의 보안 사고가 발생할 수 있다. 이 취약점은 클라우드를 제공하는 사업자가 안전한 API를 설계하고 제공하여야 하는 것이지만, 운영의 과정에서 응용계층의 보안(클라우드 웹 방화벽 등)을 채용함으로써, 최소한의 보안을 확보할 수 있다.

2. 가상화 취약점

클라우드 기술은 하나의 기술로 구성되는 것이 아니라 그 내부에는 엄청나게 많은 요소기술들이 존재하고 있다. 하드웨어의 측면에도 CPU, 메모리, 저장장치 등의 많은 요소들이 대량으로 서로 연결되어 있다. 클라우드 서비스는 여러 전산 자원이 여러 요소기술들의 조합에 의해서 IaaS, PaaS, SaaS 등의 서비스 모델 형태로 제공한다. 이러한 가상화 기술로 인해서 내부의 요소기술이나 하드웨어에서 발견되는 취약점이 클라우드컴퓨팅 환경의 전체 취약점으로 연결될 수 있다.

[가상화 취약점]



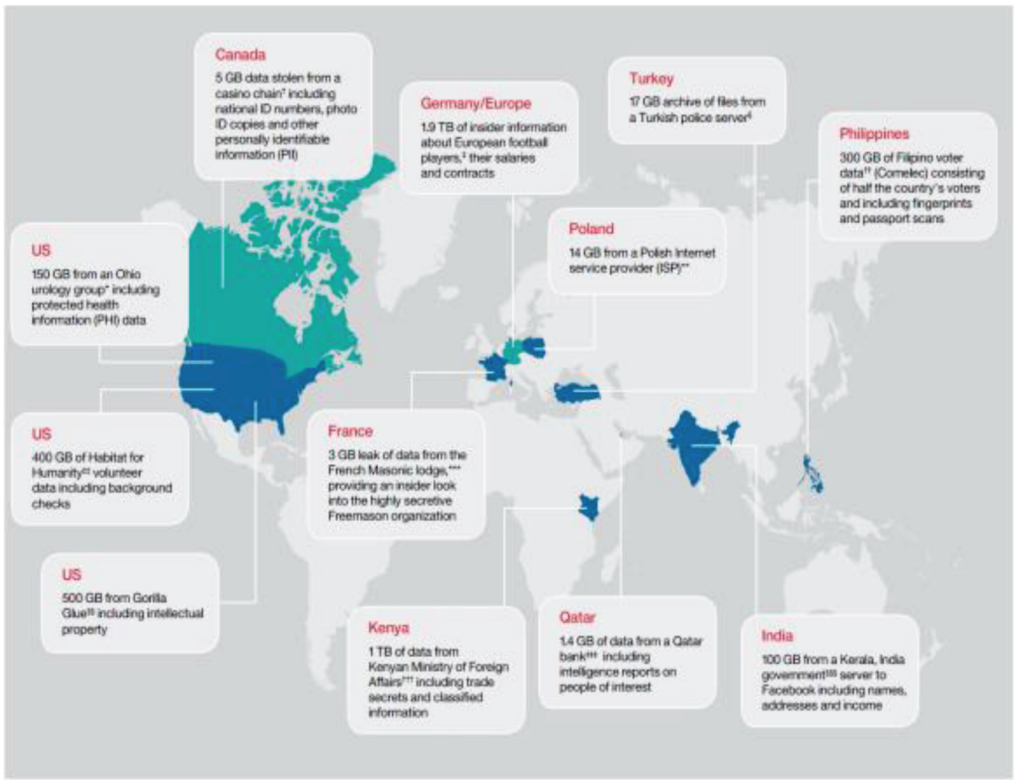
3. 계정, 서비스 및 트래픽 탈취

사용자가 클라우드 서비스를 이용할 때 가장 기본이 되는 것은 계정정보이다. 사용자의 계정정보에 기반을 둔 클라우드 서비스는 사용자를 인식하고 사용자가 원하는 정보를 제공해주기 때문이다. 사용자의 계정정보가 탈취되면 어떤 일이 일어날지를 상상하는 것은 쉬운 일이다. 특정 기업의 기밀 정보를 엿볼 수 있고, 관리자로서 다른 사용자의 계정을 삭제하거나 기업의 클라우드 서비스 계약 정보를 변경할 수도 있다. OWASP에서 발표하는 10대 취약점 중 매년 3위안에 포함되는 XSS(Cross-Site Scripting) 취약점이 대표적이며, 해당 취약점을 활용하여 계정정보를 탈취한 공격이다. 이를 해결하기 위해서는, 입 · 출력값 검증, 보안 라이브러리(AntiXSS, OWASP ESAPI) 사용, Two-factor 인증 등의 적용이 필요하다.

4. 데이터 유출 (Data Breaches)

클라우드를 기업의 업무시스템으로 사용하는 기업에게 가장 두려운 일은 데이터와 정보가 유출되는 것이다. 클라우드는 기존의 서버 기반 환경보다 네트워크 접근성을 확대하기 때문에, 해커들에게는 그만큼 다양한 공격 경로가 열려있는 것을 의미한다. 특히 퍼블릭 클라우드(Public Cloud)의 경우에는 여러 기업들이 클라우드를 사용하기 때문에, 특정 기업의 클라우드 서비스에 대한 공격이 이루어졌을 때 동일한 클라우드를 이용하는 다른 기업의 클라우드 서비스에도 동일한 공격이 이루어질 가능성이 매우 높다. 클라우드의 데이터 저장과 관리는 이러한 관점의 기술적 해결방안이 고려되어야 한다.

[2016년 주요 데이터 유출 사고]



※ [출처] IBM X-Force 보안 동향 및 위험 보고서 (IBM)

5. 데이터 손실 (Data Loss)

클라우드의 장점은 언제, 어디서나 클라우드에 접속하면 원하는 데이터에 접근할 수 있다는 것이다. 특정 데이터는 여러 채널과 경로를 통해서 여러 사람이 동시에 접속할 수 있다. 이러한 편리함이 갖는 장점은 엄청나지만, 누군가 삭제를 하거나 수정해버린 데이터는 영원한 시간의 저편으로 사라져 버린다.

삭제나 수정은 새로운 데이터로의 갱신으로 이해할 수도 있지만 기존 데이터의 손실로도 이해할 수 있으며, 또한 데이터의 손실은 해커나 어느 성실한 직원의 성실한 업무 수행 과정에서 고의적으로 행해질 수도 있지만, 실수에 의해서 우연히 발생할 수도 있다. 데이터 손실을 막을 수 있는 방법은 데이터를 수정하거나 삭제할 수 있는 권한을 잘 관리하는 것이고, 수정과 삭제에 대해서 이전 데이터를 백업해두는 것뿐이다. 앞에서 언급한 데이터 유출은 데이터를 읽는(reading) 과정에서 발생하지만, 데이터 손실은 데이터를 쓰는(writing) 과정에서 발생한다.

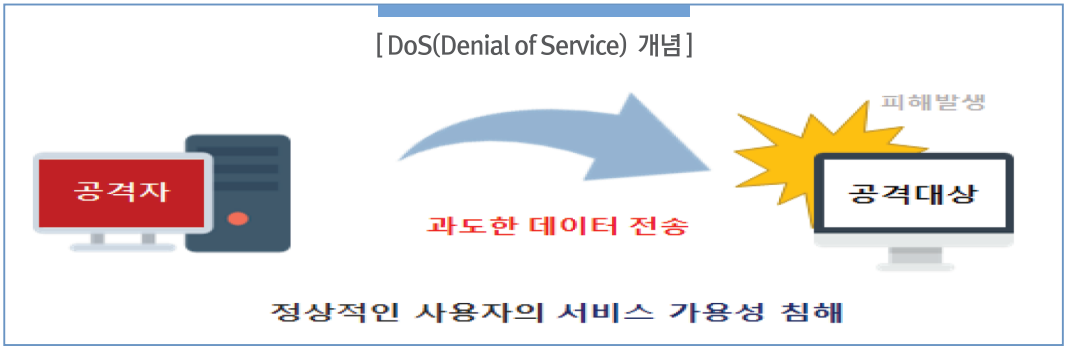
[데이터 손실로 인한 손해 비용]

※ [출처] EMC 글로벌 데이터 보호 인덱스 보고서 (EMC, 2016)

6. 서비스거부 (DoS: Denial of Service)

서비스 거부 공격은 서버의 자원을 소진함으로써 서비스의 가용성(availability)을 없애는 형태의 공격으로서, 클라우드 환경에서도 여전히 유효한 공격 방법이다. 클라우드 서비스에서는 클라우드를 구성하는 하드웨어 자원의 가용성을 소진하고, 나아가서는 클라우드 서비스를 이용하는 기업의 업무가 원활히 이루어지는 것을 방해하게 된다.

[DoS(Denial of Service) 개념]

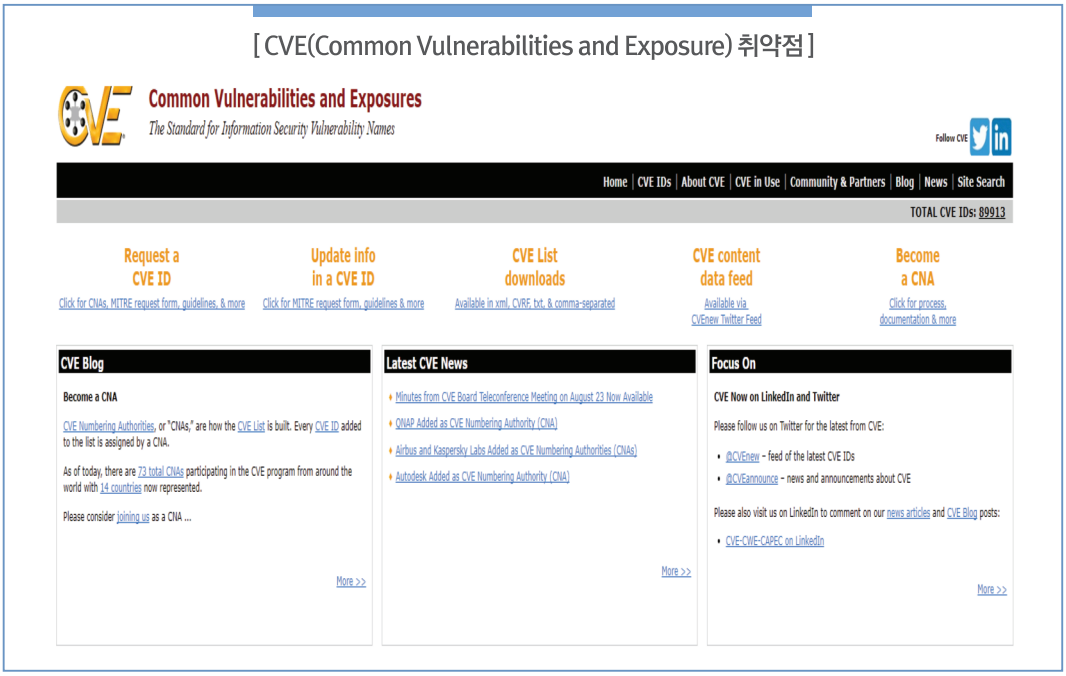


7. 시스템 취약점

클라우드컴퓨팅 환경에서의 시스템 취약점은 새로운 유형의 위협은 아니다. 일반적인 시스템 취약점은 크게 시스템 자체의 소프트웨어 취약점(CVE; Common Vulnerabilities and Exposure)과 환경 설정 미흡에 따른 취약점(CCE; Common Configuration Enumeration)이 존재하며, 클라우드 환경에서도 동일한 취약점이 발견되고 있다.

클라우드컴퓨팅 환경에 특화된 CVE 취약점은 오픈소스 플랫폼(CloudStack, Openstack 등)과 오픈소스 하이퍼바이저(Xen, KVM 등)에 대한 취약점이 대표적이며, 공격자는 이러한 CVE 취약점을 통해 시스템 운영중단 또는 장애를 유발하는 DoS 공격을 발생시키거나, 가상화 소프트웨어(QEMU 등)의 보안취약점을 이용해 사용자 권한획득을 목적으로 공격한다. 또한, 클라우드컴퓨팅 환경은 시스템 규모가 크고 보안관리 및 보안정책 적용이 복잡한 관계로, 환경 설정 미흡에 따른 관리자/사용자 계정의 권한 오남용, 취약한 패스워드 사용, 시스템/중요 파일의 권한 오남용, 불필요한 서비스(DNS, SNMP, FTP, SSH 등) 활성화 등 CCE 취약점에 상대적으로 노출될 가능성이 높다.

[CVE(Common Vulnerabilities and Exposure) 취약점]



클라우드 서비스를 이용하는 기업 IT담당자 위한

클라우드 정보보호 안내서

Ⅳ. 클라우드 컴퓨팅 보안

1. 클라우드 컴퓨팅 보안 개요
2. 클라우드 컴퓨팅 도입 보안
3. 클라우드 컴퓨팅 운영 보안
4. 클라우드 컴퓨팅 실무 보안

Ⅳ 클라우드 컴퓨팅 보안

1 클라우드 컴퓨팅 보안 개요

본 장에서는 앞장에서 살펴본 클라우드 보안위협을 최소하기 위해 갖추어야 하는 사항에 대해서 다루도록 하겠다. 클라우드 환경은 기존 온프레미스 인프라 환경과 동일한 보안업무로 수행할 수 있는 부분도 존재하나 클라우드 서비스 환경 특성으로 인해 기존의 보안업무의 변경 및 새로운 보안업무를 추가해야 할 것이다.

본 장에서는 먼저 기존 온프레미스 환경에서 클라우드 도입 시 보안 관점에서 달라지는 사항, 클라우드 도입 후 운영관점에서 갖추어야 하는 보안관리체계, 마지막으로 클라우드 특성을 고려한 보안실무 관점에서 적용하면 좋은 사항에 대해서 다루도록 한다.

먼저, 2절에서는 기업이 클라우드 서비스 도입에 따른 변화를 효율적이고 안정적으로 적용하는 데에 반드시 고려해야 하는 ①조직, ②정책, ③기술 관점에서 필요한 사항을 다루고,

3절은 클라우드 인프라를 체계적이고 안전하게 운영하는데 필요한 보안관체계 관점에서 정보보호정책 수립, 보안조직 구성, 자산식별 및 통제, 침해사고관리, 서비스 연속성, 가상화 보안 등 클라우드 서비스 환경에서의 보안관리체계 갖추는데 필요한 사항을 기술한다.

마지막 4절은 클라우드 환경변화에 따라 달라지는 사항 중심으로 보안 실무 수행 시 어떤 사항들을 고려하여 적용해야 하는지를 알아보기 위해 아키텍처 설계, 네트워크 접근통제, 보안솔루션 구축, 보안관제 등 클라우드 서비스 환경에서의 보안실무에 필요한 사항을 다룬다. 또한 클라우드 제공업자가 제안하는 솔루션이나 이용자 관점에서 업무에 적용했던 일부 사례를 들어 관련 이해를 돕고자 하였다.

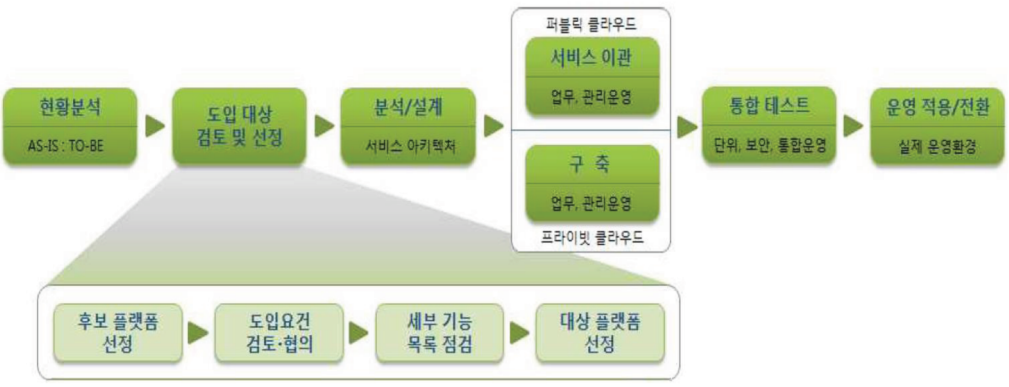
2 클라우드 컴퓨팅 도입 보안

최근 들어 클라우드 컴퓨팅을 도입하는 일부 기업들이 IT비용을 절감하고 시스템의 확장성을 향상시켜 사업의 유연성을 증대하는 등 클라우드 컴퓨팅 도입에 대한 많은 이점들을 인식하고 있다. 이제는 클라우드 컴퓨팅을 도입할지 여부보다는, 클라우드 컴퓨팅을 어떻게 하면 가장 효율적이고 안전한 방식으로 도입할 수 있는지 고민해야 할 시기이다.

2장에서 설명한 것처럼, 현재 클라우드 컴퓨팅은 서비스 유형, 배치 형태에 따라 다양한 기술모델이 존재한다. 클라우드 도입을 고려한 기업은 기업의 필요와 목적에 따라 클라우드 컴퓨팅 기술모델을 선정하고, 관련 기술, 비용, 보안 등을 고려한 전략적인 결정을 선행함으로써, 정보와 경험 부족으로 인한 시간, 투자 비용 손실 등의 시행착오를 최소화할 수 있다.

2012년에 방송통신위원회에서 발간한 「민간 부문의 클라우드 도입 실무 가이드라인」에는 클라우드 컴퓨팅 도입도 아래 그림과 같이 일반적인 정보시스템 구축 절차를 따르며, 각 단계별로 클라우드 환경의 특성을 고려해야 한다고 기술하고 있다.

[일반적인 클라우드 도입 절차]



※ [출처] 민간 부문의 클라우드 도입 실무 가이드라인('12.12월, 방송통신위원회)

클라우드 컴퓨팅 도입 절차에 따라 기업은 ①[현황분석] → ②[도입 대상 검토 및 선정] → ③[분석/설계] 단계를 통해, 클라우드 시스템을 내부에 구축(프라이빗 클라우드)할 것인지, 외부 클라우드 서비스 제공자를 통해 이관(퍼블릭 클라우드)할 것인지 선택하여야 한다.

프라이빗 클라우드는 기존 온프레미스(On-Premise) 환경과 유사하게 물리적, 관리적, 기술적 보안을 유지해야 한다. 따라서 본 안내서에서는 클라우드 전환에 따른 장점을 살린 퍼블릭 클라우드 도입할 경우인 ④[서비스 이관] 단계를 거쳐 외부 클라우드 환경으로 이동하는 방식에 대해 다루도록 하겠다.

기업에서 기존의 IT 시스템을 퍼블릭 클라우드 형태로 운영환경으로 전환을 위해서는 변화를 위한 준비가 필요하다. 클라우드 서비스 도입에 따른 변화를 효율적이고 안정적으로 적용하는 데에 반드시 고려해야 하는 ①조직, ②정책, ③기술에 대한 사항을 ①[현황분석] → ②[도입 대상 검토 및 선정] → ③[분석/설계] → ④[서비스 이관] → ⑤[통합테스트] 단계에서 같이 검토되어야 할 것이다.

1. 조직(Organization) : 조직 및 조직원 역할 수립, 변화관리 준비 필요

기존의 IT 시스템을 운영하는 조직은 업무 변화에 대한 준비를 위해 클라우드 서비스 환경에서의 업무와 역할을 사전에 정의하는 것이 필요하다. 클라우드 환경에서의 IT 조직은 조금 더 비즈니스와 연계된 조직으로서 IT 자원의 운영관리에서 IT 서비스의 공급 관리 관점으로 그 역할이 전환된다. 기존의 IT 시스템 구축 및 운영 중심에서 서비스 운영의 형태로 변화됨에 따라 공급자 역할과 책임을 가지는 IT 조직으로 변화되어야 할 것이다.

클라우드 서비스로의 전환은 IT 조직과 조직원들에 큰 변화를 줄 수 있다. 변화의 단계에서 조직원들의 변화의 저항과 변화에 대한 거부감을 최소화하기 위해 구성원들이 환경변화에 적극적으로 공감하고 동참할 수 있도록 체계적인 지원활동[1]을 해야 할 것이다. 이를 위해 우선적으로 변화를 의도적으로 앞장서서 주도하는 팀을 구성하고 해당 팀이 먼저 클라우드를 적용해 보고 시행착오를 통하여 모범사례를 만드는 것이다. 이를 통해 클라우드 도입에 대한 거부감을 줄일 수 있을 것으로 기대한다.

1) 선행 팀 운용, 모범사례 공유, 전문가 세미나, 내부 연구모임, 전문 교육 등

클라우드 환경에서 IT 자원은 소유가 아닌 사용 또는 이용의 개념으로 바뀌며 온프레미스 환경에서 각 IT 자원에 담당이 클라우드 환경에서는 서비스 담당으로 변화하게 된다. 따라서, 클라우드 환경으로 전환 시 클라우드 공급자 조직에 대한 사전 역할 정의를 통하여 업무 준비도를 향상시키고 서비스에 대한 접근통제 정책을 수립하고 적용해야 할 것이다.

2. 정책 : 표준 운영 모델 수립, 정책 식별 및 개정(법규, 지침, 절차 등)

기존 IT 운영 조직과 함께 어떻게 조화롭게 구성하여 안정적으로 클라우드로 전환 할 것인가가 매우 중요하다. 이에 포괄적인 IT 서비스에 대한 관리 관점으로 클라우드에 접근이 필요하다. 큰 틀의 IT 서비스 제공을 위한 표준 운영 모델을 수립한 후 포괄적인 IT 서비스에 대한 관리 관점으로 클라우드를 접근하여야 한다. 또한 클라우드 서비스 도입 시 영향받는 법규, 정책, 지침 및 절차를 식별하여 개정하는 하는 것이 필요하다. 공공, 금융, 의료, 교육 등 주요 산업분야의 법규 또는 관행이 클라우드 서비스 이용의 장애물 요소가 있는지도 살펴보고 지침 등에 반영해야 할 것이다. 한 번에 완벽하게 수립할 수 없음으로 서비스를 운영하면서 지속적으로 검토하고 반영해야 할 것이다.

[보안 운영 지침 중 일부내용 예시]

통제 항목	내용
1. 네트워크 구성	– 프로덕션 환경과 프리프로덕션 환경은 구분한다. – 대외 · 대내 서비스 영역은 구분한다. – 어플리케이션과 데이터베이스 영역은 구분한다.
2. IP 통제 및 모니터링	– 필요한 IP & Port에 대해서만 연결 허용한다. – 프로덕션 대외서비스 영역 (DMZ, Web)에 대해서 대외 및 인터넷 망에 연결 허용한다. ※ 단, Outbound 허용은 보안팀 검토 후 적용한다. – 대외서비스 영역 (DMZ, Web)에 대해서 Internet Gateway(IGW)에 대한 연결을 허용한다. ※ 보안통제 Rule 통하여 대외 및 인터넷망 연결을 통제한다. – 대외 및 인터넷 망 연결 허용된 서비스는 WAF 또는 이에 준하는 서비스 및 솔루션을 통하여 Blacklist IP를 관리한다. – 보안통제 Rule에 의하여 허용 또는 차단된 히스토리는 로깅한다.
3. 침해 방지 및 모니터링	– 침입탐지 및 차단을 위해 보안솔루션을 통해 보호한다. – 프로덕션 및 프리프로덕션 환경의 아래 네트워크 영역에서 구축되는 모든 서버에는 통합 보안솔루션 에이전트를 설치한다.
4. 암호화	– DB 데이터 암호화 적용시 안전한 알고리즘을 사용하여 암호화 한다.
5. DB 개인 정보접근기록	– 개인정보처리시스템의 DB를 접속할 경우 모든 접근행위는 기록한다.

[클라우드 도입 시 검토가 필요한 법규 예시]

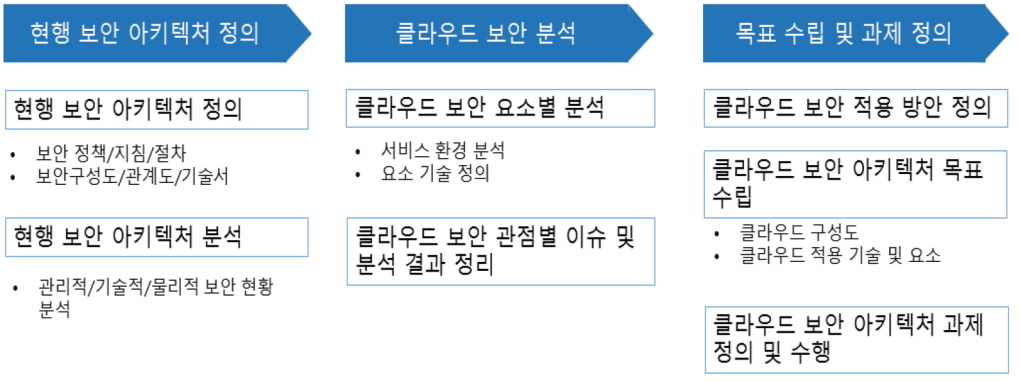
분야	관련 법규
IT	전자문서 및 전자거래기본법(제31조의2) 및 시행령 (제15조의 4) (공인전자문서센터 시설 및 장비 등에 관한 규정)
	전자문서 및 전자거래기본법(제31조의2) 및 시행령(제15조의14)(공인전자문서중계자 인력 · 기술 능력, 시설, 장비규정)
	지능형 홈네트워크 설치 및 기술기준(제 13조)
클라우드 컴퓨팅	클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률
	클라우드컴퓨팅서비스 정보보호에 관한 기준
개인정보 국외이전	정보통신망법제63조제2항
	개인정보보호법 제17조 제3항

3. 보안 기술

클라우드 환경에 필요한 보안 기술 자원을 인식하고, 세부 요소기술에 대한 표준을 설정하고 이에 기반하여 보안 아키텍처 수립이 필요하다. 특히 클라우드 서비스의 도입 및 적용에 대한 전사 아키텍처 검토와 함께, 기업 내 보안 기술 및 솔루션 표준화가 무엇보다도 중요하다. 클라우드 환경에서의 도입 시에는 필요한 보안 요소기술과 현재 적용 솔루션의 클라우드 환경하에서의 적용 여부를 검증하는 단계가 필요하다.

클라우드 서비스의 도입 및 전환 시에 보안 아키텍처 사항이 전사 아키텍처 수립에 반영되어야 한다. 보안 아키텍처 단계에서는 클라우드 환경에 필요한 보안 기술 자원을 인식하고, 세부 보안 요소기술에 대한 표준을 설정하고 이에 기반하여 보안 아키텍처를 수립한다. 특히 다양한 클라우드 서비스 및 클라우드 컴퓨팅 환경에서 보안 기술 필요요소를 식별하고 각 각의 클라우드 서비스간의 기술 관계성을 도출한다. 무엇보다도 클라우드 서비스 운영에 영향을 줄 수 있는 아키텍처 특성, 가용성, 확장성, 성능, 보안 등에 대하여 상세 검토한다. 또한 비즈니스 아키텍처와 정보시스템(어플리케이션, 데이터) 아키텍처에 연계하여, IT 인프라, 기술 및 보안요구사항이 반영되었는지를 확인한다.

[클라우드 보안 아키텍처 수립 절차 예시]



① 클라우드 서비스 도입 시 영향받는 통제항목을 식별하고 통제 방안 수립한다.
② 통제 사항에 대한 필요한 보안기술 식별 및 적용 방안 설계한다.

인프라 보안, 계정 및 접근제어, 취약점 제어, 데이터 보호 및 로깅 모니터링 영역 구분하여 보안 식별 및 적용할 것을 권고한다.

※ 클라우드 서비스 공급사의 마켓에서 제공하는 보안 솔루션 및 공급사에서 이행 되어야 하는 통제 방안 및 보안 활동에 대해 이해하는 것이 필요하다.

③ 현 표준 보안 솔루션이 클라우드 환경에 적용 가능성과 클라우드 서비스에서 제공하는 솔루션이 보안 표준에 부합하는지 검증한다.

※ 솔루션 검증 작업 시 아키텍처 변경, 성능, 가용성, 비용 및 타 시스템과의 연동 등의 필요 요소를 식별하고 진행해야 한다.

[보안 솔루션 검증 방법]

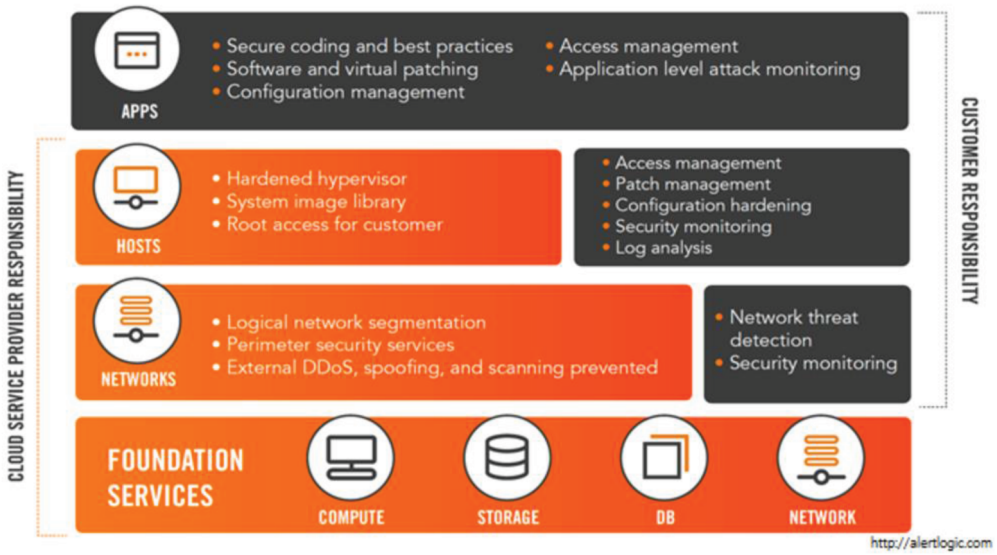
보안 솔루션 검증 절차	보안 솔루션 검증 시 고려 요소
검증 대상 선정 → 요구사항 결정 → 설계 → 구현 → 테스트 → 문제 및 해결방안 도출 → 적용 유무 검토	솔루션 아키텍처 변경 사항, 성능 및 가용성, 타 시스템 연계방법, 클라우드 서비스 비용

그리고, 클라우드 서비스 업체 선정 시 적절한 서비스 도입 비용, 최소한의 서비스 수준 및 보안 요구사항 등의 충족 여부를 비교해 봄으로써, 해당 기업에 적합한 클라우드 서비스 제공업체를 선정해야 한다.

기업은 클라우드 서비스 제공자와 서비스의 안전성 및 보안성, 책임범위를 명확히 정의하기 위해, 클라우드 서비스 제공업체와 서비스 계약과 서비스 수준 계약(SLA)을 체결하게 되는데, 보안성 측면에서 SLA 계약 시 서비스 내용 및 범위, 업무 및 책임 범위, 서비스 수준 지표(서비스 가용성, 서비스 장애, 위약금(손해배상), 데이터 백업 및 복구, 서비스 확장성, 고객지원 등) 설정, 서비스 수준의 평가 등급 및 방법, SLA 개정 및 변경 절차 등에 관한 내용을 포함하여야 한다.

※ [클라우드 서비스를 위한 SLA가이드, 2011년 방송통신위원회], [클라우드 표준계약서(B2B, B2C), 2016, 과학기술정보통신부」가이드 참조하여 클라우드 사업자와 계약 시 요구할 것을 검토한다.

[퍼블릭 클라우드의 책임 분담 모델(Shared Responsibility Model)]



※ [출처] Understanding the shared responsibility of cloud security('15.5월, ALERT LOGIC)

마지막으로 클라우드 서비스로의 이전이 완료되면, 기업은 「통합테스트」 단계에서 서비스 성능, 기능에 대한 테스트 이외에도 서비스 수준, 보안 수준이 사전에 설정된 사항을 충족하는지를 확인해야 할 것이다.

3 클라우드 컴퓨팅 운영보안

관리적 보안은 중요한 정보(자산)를 안전하게 보호하기 위해 지침 · 절차서 등으로 정의하고, 이를 관리적 · 기술적으로 보안 등을 적용하여 클라우드 인프라를 안전하게 운영 · 관리하기 위한 일련의 정보보호 활동을 의미한다.

본 절에서는 클라우드 인프라를 안전하게 운영하는 데 있어 필요한 보안을 요약한 내용으로써, 정보보호정책 수립, 보안조직 구성, 자산식별 및 통제 등 관리적 보안을 위해 갖추기 위해 해야 하는 사항을 기술한다.

정보보호 활동	주요 내용
클라우드 정보보호 정책서 수립	정보시스템 및 자산을 기술적 · 관리적으로 보호하기 위한 절차
보안조직 구성 및 인적보안	정보보호 활동을 수행하기 위하여 책임, 권한, 관계가 정의된 조직, 인원
자산식별 및 통제	물리 자산(정보시스템 등) 및 정보 자산을 식별하고 해당 자산에 대한 관리책임 및 통제방안
침해사고 관리	침해사고 시 신고, 처리 절차
서비스 연속성 관리	서비스 장애 등 서비스 이용문제 발생 시 처리절차
준거성 관리	사내 보안규정, 개인정보보호법, 정보통신망법 등 법적인 의무사항
가상화 및 서버보안	악성코드 방지대책, 가상자원(수정, 이동, 삭제, 복사)관리, 클라우드 서버에 대한 기술적 보안대책 적용
접근통제 보안	접근통제 정책을 수립하고, 사용자 · 관리자 접속 관리 및 제한, 사용자 · 관리자 계정 분할 및 권한 최소화
네트워크 보안	네트워크 분할 또는 이중화 관리, 네트워크 보안관제 체계 구축, 네트워크 가용성 확보
데이터 보호 및 백업	중요 데이터 분류, 데이터 소유권 확립, 데이터 보호를 위한 안전한 암호알고리즘 사용 및 암호키 관리
시스템 개발 및 도입 보안	시스템 개발 시 보안요구사항을 반영한 설계 및 구현, 시스템 도입 시 안전성 테스트 등을 포함한 인수정책 수립

1. 클라우드 정보보호 정책서 수립

정보보호정책은 해당 기관의 클라우드 운영 관련 전반의 신뢰도나 안전성을 판단하는 기초자료로 활용될 수 있음으로 최대한 운영 환경과 이용 주체를 상세히 정의하고 운영하는 것이 좋다. 이는 해당 정책문서와 관련한 이해당사자가 해당 문서를 기반으로 이행하는 것이 무엇보다 중요하다.

클라우드 운영 정보보호정책은 클라우드 인프라를 구축 · 이용하는 환경과 이용 주체의 역할, 기능 등을 규정하고 그와 관련된 보안절차, 의무, 규칙 등의 내용을 포함하여 작성하며, 이러한 정보보호정책은 경영진의 승인을 받고, 이해당사자들에게 공표하고, 대내 · 외적인 주요 변화에 대한 정책의 일관성, 적정성 및 효율성 등의 보장을 위해 주기적으로 감사를 실시하고 감사 결과를 반영하여 개정하도록 한다.

2. 정보보호조직 구성 및 인적보안

조직의 규모와 업무절차 등을 고려한 정보보호전략을 수립하며 정보보호조직을 구성 · 운영하는 것이 필요하다. 1절1항에서 정의한 정보보호정책을 이행하는데 있어 클라우드 인프라 이해당사자(시스템 관리자, 보안관리자(또는 담당자), 이용자 등)의 보안 요구사항을 반영해야 하며, 중요정보(개인정보 등) 암호화 저장과 같은 법 · 규정 등 준거성을 준용하는 보안조치가 적용될 수 있도록 해야 한다. 조직의 정보보호 활동과 업무를 원활히 수행하기 위해서는 조직의 각 부분에서 정보보호에 관련된 역할과 책임을 명확히 정의해야 하며, 조직의 규모에 따라 정보보호 관리자 및 실무자를 지정하여 정보보호활동 업무를 수행하도록 해야 한다. 조직의 규모가 큰 경우에는 정보보호 전담 팀이나 부서가 만들어서 운영하는 것을 권고한다. 정보보호 조직 구성 시 다음을 고려하여 구성하는 것이 필요하다.

정보보호 조직 구성 정보보호 요구사항

① 조직의 규모(크기 및 인력), 조직 관리구조, 조직 수와 위치, 조직간 상호 연결형태, 정보화 및 IT 예산, 시스템 운영 환경 등을 고려한다.

② 조직에서 정보보호활동을 원활히 수행하기 위해서는 보호해야 할 정보자산의 유형, 규모 및 가치 등을 고려하여 이에 적합한 수준으로 인원과 예산을 배정한다.

③ 조직의 모든 부서에서 해당 업무 수행에 필요한 정보보호 책임이 할당되어야 하며 이를 정보보호 전담조직은 이를 기획 · 조정, 통합하고 이행을 모니터링하며 정보보호 사고 등 위반에 대응하는 역할을 수행한다.

④ 정보보호조직을 구성함에 있어 직무분리의 원칙을 적용해야 한다. 직무분리는 부주의에 의한 또는 고의적인 시스템 오용, 악용의 위험을 감소시키기 위해 필요하며, 직무분리가 어려운 상황에서는 별도의 관리감독 강화 또는 통제대책을 수립한다.

※ 외부 전문업체에 위탁(또는 인력)을 활용하는 경우, 해당인력의 책임 및 역할, 자격요건 등도 문서화하고, 계약된 인력과 실제 업무를 수행하는 인력이 일치하는 지에 대해서도 확인하고 운영하는 것이 필요

기업 입장에서 시설 · 전산 · 문서 등 어느 것 하나 중요하지 않은 것이 없지만, 이러한 모든 것의 관리 · 운영 주체는 사람이다. 즉, 인력에 대한 보안관리가 매우 중요하다. 인적보안은 내부인력, 외부인력 구분할 수 있으며, 다음 아래 사항을 고려하여 운영하여야 한다.

인적보안 정보보호 요구사항

공통	① 모든 임직원 및 외부인력에 대해 연간 정보보호 교육 계획 수립 및 이행하고, 중대한 변경, 보안사고 등 발생 시 추가 교육을 실시한다. ② 계약만료 시 자산반납, 접근권한 회수, 중요정보 파기 등을 해야 하며, 업무 수행 시 알게 된 정보에 대해 비밀 유지서약을 받는다.
내부 인력	① 고용계약서에 정보보호 정책을 준수하도록 하는 조항을 포함한 계약서를 작성한다. ② 보안관리자를 포함하여 클라우드 인프라 운영과 관련된 임직원의 경우 주요 직무자로 지정하고 관리한다.
외부 인력	① 정보자산 접근 등과 관련된 보안요구사항을 계약에 반영한다. ② 보안요구사항 준수여부를 주기적으로 점검하고 위반 시 적절한 조치를 수행한다. ※ 보안요구사항 예시 - 정보보호 관련 법률 준수 - 서비스 수행 인력 대상 주기적인 정보보호 교육 수행 - 서비스 수행 관련 취득한 중요정보 유출 방지 대책 - 비 승인자의 접속 제한 - 물리적 공간의 보호조치 - 서비스 수행 인력의 단말 보안 - 주기적 보안점검 수행 - 유무선 네트워크 통제 - 보안요구사항 계약 위반 시 처벌, 손해배상 책임 - 정보 제3자 제공 시 통지 의무 - 허가된 범위 외에 정보 유용 방지 - 보안사고 발생에 따른 보고 의무 - 정보보호협약서 및 비밀유지서약서 제출 ③ 외부자(공급사)가 계약 만료, 업무 종료, 담당자 변경 시 조직이 외부자에게 제공한 정보 자산의 반납, 정보시스템 접근계정 삭제, 중요정보 파기, 업무 수행 시 알게 된 정보의 비밀유지 서약서 등의 내용을 확인한다.

3. 정보자산 관리

자산을 보호하기 위해서는 발생 가능한 위협요소에 대하여 해당 자산이 가진 취약점을 제거하는 일이 무엇보다 중요하며, 이러한 작업의 궁극적인 목적은 자산의 가치에 따라 부여된 보안등급, 즉 자산을 어떻게 취급하고 보호할 것인지에 대한 대책을 수립하기 위해서다. 자산이 가진 중요도 또는 업무 기여도 등에 따라 자산에 대한 보호수준이 달라질 수 있는데, 자산을 체계적으로 보호하고 관리하기 위해서는 일정 기준과 원칙을 정하는 것이 중요하다.

클라우드 환경에서의 자산관리는 다음 사항을 고려하는 것이 필요하다.

- 가상 자원의 식별정책 수립 및 적용
- Domain Name 기반의 자산 관리
- Role 현황 관리
- 다수의 지역에 분산되어 있을 자산의 통합관리

정보자산 관리 정보보호 요구사항

구분	내용
① 자산 식별	■ 클라우드컴퓨팅서비스에 사용된 정보자산(정보시스템, 정보보호시스템, 정보 등)을 식별하고, 해당 자산을 목록화 하고 관리한다. ※ 자산 – 가상서버 등 이용자가 생성하는 자산 · 정보시스템 : 정보의 수집, 가공, 저장, 검색, 송수신에 필요한 응용 프로그램 · 정보 : 이용자가 생성한 전자적 정보 · 가상자원 : 가상 인프라를 통해 가상화된 가상 머신(CSP 소유의 자산), 가상 스토리지, 가상 소프트웨어(예: 배포 이미지 등) 등을 포함 – 클라우드 업체에서 제공하는 서비스 · 인프라 : 정보보호시스템, 클라우드 플랫폼 등 · 정보보호시스템 : 침입차단시스템, 침입탐지시스템 등 정보의 훼손, 변조 및 유출 등을 방지하기 위해 구축된 하드웨어 및 소프트웨어 ■ 식별된 정보자산(가상자원 포함)에 대해 보안등급 부여하고 자산별 책임자, 관리자 두어 해당 자산에 대한 책임을 부여한다. ※ 정보자산 도입, 변경, 폐기, 반 · 출입 등의 책임을 질 수 있는 책임자 및 정보자산을 관리 · 운영 하는 관리자(또는 담당자)를 지정하여 책임소재 명확히 필요
② 자산 보안 등급 부여 및 취급	■ 자산에 대해 기밀성, 무결성, 가용성, 법적요구사항 등을 고려하여 자산의 중요도에 따라 보안 등급을 부여하고, 보안 등급별 취급 절차(생성, 저장, 이용, 파기) 수립하고 관리한다.
③ 자산 변경관리	■ 클라우드컴퓨팅서비스에 사용된 자산(시설, 장비, 소프트웨어 등)의 변경이 필요한 경우 보안 영향 분석(보안, 성능, 업무 등에 미치는 영향)한 후 변경요청, 책임자 검토 승인 등 공식적인 절차를 수립하고 이행한다. ※ 변경 시 변경 실패에 따른 복구방안을 사전에 고려하고, 클라우드 인프라를 이용하는 이용자에 게 큰 영향을 주는 변경에 대해서는 사전에 공지필요

4. 침해사고 관리

클라우드 환경은 데이터가 분산되어 있지 않고 한 곳에 집중됨에 따라 침해사고 시 큰 피해로 이어질 수 있다. 따라서, 침해사고에 대해 효과적인 대응을 위해 침해사고 대응체계를 구축하고, 신고절차, 사고 처리 절차 등을 담은 침해사고 대응절차를 필수적으로 마련하여 운영하는 것이 필요하다.

다음은 일반적인 침해사고 대응절차를 설명한다. 다음 아래 내용을 참고하여 해당 기업에 맞는 침해사고 대응절차를 마련하고 운영하는 것이 필요하다.

침해사고 관리 보안요구사항

① 침해사고에 대한 효과적인 대처를 위해 침해사고 대응절차를 수립하고 운영한다.

※ 침해사고 대응절차는 일반적으로 [예방] ▶ [탐지/분석] ▶ [대응] ▶ [복구]의 4단계로 구성하며, 각 단계에서 수행해야 할 주요활동은 다음과 같다.

단계	구성	주요활동	역할 및 책임
1	예방	· 정보보호를 위한 평시 활동 · 침해사고 대응팀(CERT) 구성 및 운영 · 정보보호 교육을 통한 인식제고	전체 임직원
2	탐지/분석	· 정보자산 모니터링 · 초기분석	운영담당자 보안담당자
3	대응	· 증거데이터 수집/보호 · 침입유형별 긴급조치	운영담담당자 보안담담당자
4	복구	· 재발방지 조치 · 시스템 통제권 회복 후 재발방지 대책 수립	운영담당자 정보보호담당자 정보보호책임자

② 침해사고 대응절차 각 단계별 관리적/기술적 대응을 할 수 있는 침해사고 대응체계 구축하고 이행한다.

- (관리적) 각 단계별 실시하는 정보보호활동을 수립하고 이행할 수 있도록 조직, 인력, 승인체계 등을 포함한 중앙집중적인 대응체계를 갖춘다.
- (기술적) 단계별 기술적 정보보호 조치를 위해 정보보호시스템을 갖추고 해당 시스템을 기반으로 모니터링, 증거데이터 수집 및 분석, 침입차단 등의 정보보호활동을 수행한다.

③ 침해사고 발생 시 침해사고 대응절차에 따라 이행하고, 법적 통지 및 신고 의무를 준수한다. 또한 클라우드컴퓨팅 서비스 이용자에게 발생 내용, 원인, 조치 현황 등을 신속하게 알린다.

※ 참고 ※

- 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제48조의3(침해사고의 신고 등)
- 개인정보보호법 제34조(개인정보 유출 통지 등)
- 클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제25조(침해사고 등의 통지 등)

5. 서비스연속성 관리

클라우드 서비스는 구성방법에 따라 지리적으로는 분산된 환경에서, 클라우드 사업자가 제공하는 장비에 따라 클라우드 인프라를 구현할 수 있다. 이는 시스템 관리자가 예측하기 어려운 사고로 이어질 가능성이 높다는 것을 의미한다. 그에 따라 발생할 피해와 손실은 해당 기업의 비즈니스, 이미지 등 막대한 손해를

끼칠 수 있다. 따라서 피해 확산을 방지하고 손실을 최소화하기 위해 시스템 가용성 및 서비스 연속성 관리는 필수적으로 대비하여야 한다. 서비스 연속성 보장은 업무 복구 시간을 단축하고, 복구에 소요되는 발생 비용을 최소화할 수 있도록 계획을 수립해야 하며, 신속한 서비스 복구를 위해 주요 대응방안은 중요도에 따라 우선순위를 결정하고 이행하여야 한다.

다음은 서비스연속성 관리를 위해 갖추어야 하는 내용을 기술한 것이며, 해당 내용을 참고하여 해당 기업에 맞는 서비스연속성 관리 방안을 수립하고 운영하는 것이 필요하다.

서비스 연속성 관리 정보보호 요구사항

① 클라우드컴퓨팅서비스의 중단으로부터 업무 연속성을 보장하기 위해 백업, 복구, 재발방지 대책 등을 포함하는 장애 대응 절차를 마련한다.

- 서비스 중요도 따라 가용성 및 연속성 보장을 위한 대책은 일관성 있게 수립하고, 각 대책항목은 우선순위를 정하고, 그에 따라 복구 할 수 있는 절차를 수립한다.
- 시스템 오류나 장애 등에 대비한 복구 조직 및 연락망 구성, 주요시스템 및 네트워크의 이중화 구축방안 등을 포함한다.
- 장애 관련 정보를 활용하여 유사한 서비스 중단이 반복되지 않도록 장애 재발방지 대책을 수립하고, 필요한 경우 장애 대응 절차도 변경한다.

② 가용성 유지를 위해 H/W 및 S/W의 주요 시스템 정보를 저장 · 백업 등 관리가 가능하도록 시스템을 갖추고 해당 주요시스템의 상태를 실시간을 확인할 수 있는 모니터링 체계를 갖춘다.

- 백업대상 선정기준, 백업담당자 지정, 백업대상별 백업 주기 및 보존기한 정의 등 백업정책 수립

※ 필요 시 주요 정보시스템의 경우 IT 재해복구 측면에서 백업정보의 완전성, 정확성 등을 점검하기 위하여 정기적인 복구 테스트 수행

- 백업대상은 중요정보(개인정보, 기밀정보 등), 문서, 각종 로그(클라우드시스템 보안감사로그, 이벤트 로그, 정보보호 시스템 이벤트 로그 등), 환경설정파일 등 대상 정보 및 클라우드시스템의 중요도를 고려하여 선정하여야 하며 정해진 절차에 따라 백업관리를 수행한다.

6. 서비스 공급망 관리

클라우드 서비스 이용하려고 하는 업체는 클라우드 서비스 제공자(IaaS, PaaS, SaaS)를 통해 필요한 클라우드 인프라를 구축하여 이용하게 될 것이다. 이때 해당 클라우드 서비스 제공자 마다 제공하는 수준 등이 상이함에 따라 다음 사항을 고려하여 계약하고 클라우드 서비스를 운영하는 것이 필요하다.

서비스 공급망 관리 정보보호 요구사항

① 서비스에 대한 접근과 서비스 연속성을 저해하는 위험 식별 및 최소화하기 위해 공급망(IaaS 사업자 등)과 관련한 보안 요구사항을 포함하는 공급망 관리 정책을 수립하고 관리한다.

※ 위협식별 요소 예시 : 하위 계약, 정보교환 미 전송유형, 사용하는 네크워크 유형 등

② 공급망 계약 시 클라우드컴퓨팅서비스 범위 및 보안 요구사항을 포함하는 공급망 계약을 체결한다.

※ 보안요구사항 예시 : 식별된 위험을 해결하기 위한 계약 조항, 통제 및 모니터링의 적용범위, 침해사고, 장애, 서비스 연속성 유지를 위한 역할 및 책임, 문제발생 시 대책 및 책임 등

③ 공급망 관련 서비스 수준 협약의 요구사항에 대한 준수 여부를 주기적으로 점검하고, 공급망 상에서 발생하는 기록 및 보고서는 정기적으로 검토한다.

※ 보안요구사항 등 추가가 필요한 한 경우, 계약서 내용을 변경 요청하여 변경 관리 한다.

7. 준거성

국내에서 클라우드 인프라를 구축하여 운영하는 업체는 개인정보보호, 정보통신망법, 클라우드 정보보호 정책 등 정보보호의 의무를 이행하는 것이 필요하다. 법 · 정책에 대한 준거성 확보를 위해 다음과 같은 정보보호 요구사항을 기반으로 대응방안을 마련한다.

준거성 관리 정보보호 요구사항

① 법, 정책적 요구사항

- 정보통신망법, 개인정보보호법, 클라우드 관련 법, 정보보호정책 등에서 기술하고 있는 침해사고, 개인정보 유출 시 관계기관에 신고 등 법적으로 지켜야 하는 사항을 내부 지침에 반영하고 준수한다.

② 정보시스템 보안감사

- 법적 요구사항 및 정보보호 정책 준수 여부를 보증하기 위해 독립적 보안감사 계획을 수립하여 시행하고 개선 조치를 취한다.
- 보안감사 증적(로그)은 식별할 수 있는 형태로 기록 및 모니터링하고, 비인가된 접근 및 변조로부터 보호한다.

8. 가상화 및 서버 보안

클라우드 서비스는 불특정 다수의 이용자가 가상화 기술로 구현된 IT 자원의 공유 기능을 통해 컴퓨팅 자원을 제공한다. 이를 통해 가상화 기술 안에서 IT 자원을 통합 · 재배치하여 활용성을 극대화하기 때문에 운영비용 절감 및 공간 절약의 효과를 기대할 수 있다. 반면, 악성코드의 신속한 전파로 인한 감염 확산이나 하이퍼바이저에 대한 공격 등 새로운 보안위협도 존재한다. 특히, 가상화 시스템 장애 발생 시 신속한 시스템 복구를 위해 가상머신의 구동 이력을 이미지 형태로 저장 · 관리하기에 이미지 저장 시 오류가 생길 경우, 전체 시스템의 완전한 복구가 어려울 수도 있다. 따라서, 클라우드 서비스의 가용성, 지속성, 악성코드 감염예방 등을 위해서는 클라우드 시스템들에 대한 주기적인 보안패치 및 점검을 하고, 데이터를 안전하게 저장 · 관리 목적으로 주기적인 데이터의 무결성 점검 및 백업 등도 이루어져야 한다. 다음은 클라우드 가상화 및 서버 보안에 필요한 사항을 기술한 것으로, 이를 참고하여 관련 보안대책을 적용하여 운영하는 것이 필요하다.

서버 및 가상화 보안 정보보호 요구사항

공통	① 바이러스, 웜, 트로이목마 등의 악성코드 예방을 위해 서버 및 가상환경을 보호하기 위한 악성코드 탐지, 차단 등의 보안기술을 적용한다. 특히, 가상환경의 경우 이상 징후 발견 시 사용 중지 및 격리 조치를 수행할 수 있는 체계를 갖추고 운영한다.
가상화 보안	① 가상자원(가상 머신, 가상 스토리지, 가상 소프트웨어 등)의 생성, 변경, 회수 등에 대한 관리 방안을 수립한다. ② 가상자원에 대한 무결성 보장하기 위한 보호조치 및 가상자원의 변경(수정, 이동, 삭제, 복사)에 대해 모니터링 한다. ③ 호스트 OS 및 하이퍼바이저를 모니터링 하고 악성코드 감염예방을 위해 주기적인 보안패치를 시행한다. ④ 가상화 실행 이력은 스냅샷 등 이미지 형태로 저장 · 관리하는 방안 등 안전한 저장 방법으로 관리한다. ⑤ 가상화 OS의 내 · 외부 데이터 이용에 대한 로그 정보를 관리 한다. ⑥ 가상머신별 자원 사용량 제한하여 특정 가상머신의 자원이 남용되지 않도록 한다. ⑦ 호스트와 가상영역 간의 경계를 명확히 구분하고 운영한다.
서버 보안	① 클라우드 서비스 운영 시 시스템에 대해 기술적 보호대책을 수립하고 적용한다. – 웹서버, DB서버, 클라우드 인프라 관리서버 등 운영 시 다음의 보호대책 적용 · 송 · 수신 시 SSL/TLS 통신 적용, 불필요한 서비스 및 포트 차단 · 접근권한 설정, 백신설치 및 OS 최신 패치 · 불필요한 소프트웨어, 스크립트, 실행파일 등 설치 금지 · 불필요한 페이지(테스트 페이지) 및 에러처리 미흡에 따른 시스템 정보 노출 방지 · 주기적인 보안패치 및 취약점 점검 실시 등 ② 공개서버는 내부 네트워크와 분리된 DMZ(Demilitarized Zone)영역에 설치하고 침입차단시스템 등 보안시스템을 통해 보호한다. **※ 보안솔루션 구축 시 고려사항** 기존 IT 환경에서는 일반적으로 H/W 형태 보안솔루션(Firewall, IPS, IDS, Web Application firewall 등)을 구축하지만, 가상환경에서는 유연한 확장성을 고려하여 S/W 방식으로 구축하는 것이 일반적이다. 따라서, 확장성이 반드시 보장되어야 한다면 호스트 기반의 보안솔루션을 설치하는 것이 적합한 방법이다.

9. 접근통제 보안

클라우드 서비스 이용자의 IT 자원 공유, 다양한 무선 단말기의 원격 접속 등이 보편화됨에 따라 기존 IT 서비스 환경보다 보안성이 강화된 사용자 인증 및 접근 관리가 필요하다. 클라우드 IT 자원에 접근이 허가된 이용자만이 서비스에 접속할 수 있도록 보장해야 하며, 서비스 이용자의 제한된 영역에 대한 접근 시도 등 부적절한 행위에 대해 모니터링하고 차단할 수 있는 기술적 정보보호 대책을 마련해야 한다. 클라우드 서비스는 사용자의 자원에 대한 인증 및 접근 관리를 사용자 계정과 부여된 역할에 따라 접근 가능하도록 관리 · 감독하는 것이 필요하며, 애플리케이션과 시스템에 대한 사용자의 접근 권한에 따른 적절한 통제가 이루어져야 한다. 이에, 서비스를 이용하는 단말기의 원격 접속 제한, 계정의 책임 분할 및 권한 최소화 등 다음과 같은 정보보호 요구사항을 기반으로 적절한 대책을 마련하여야 한다.

접근통제 정보보호 요구사항

접속 관리 및 제한	① 서비스 연결을 승인하기 전에 모든 사용자(또는 단말기)의 접속은 정책에서 규정된 절차에 따라 인증하고, 접속로그를 관리하며 모니터링을 해야 한다. - 인증 시 사용하는 패스워드 조합 규칙 준용 · 세 가지 종류 이상의 문자구성으로 8자리 이상의 길이로 구성된 문자열 · 두 가지 종류 이상의 문자구성으로 10자리 이상의 길이로 구성된 문자열 - 로그인 횟수제한(5회), 잠김해제(120초) 준용 - 하나의 사용자가 동시에 여러 세션을 소유하는 것을 제한 ② 통신 세션의 기밀성을 보장하기 위해 안전한 암호 기술을 적용한다. - 통신세션 기밀성은 SSL/TLS, VPN 등 안전한 보호기술 적용 ③ 내부정책에서 제한하는 모바일 단말기의 통제 대책을 마련한다.
계정 분할 및 권한 최소화	① 서로 다른 이용자 계정의 충돌을 최소화하기 위하여 접근을 허용하는 영역이나 권한 등을 분리한다. ② 사용자에 부여하는 역할 · 권한을 최소한의 범위로 제한해야 한다. ③ 정책서의 계정관리 주기에 따라 점검 및 이용자 변경 사항은 즉시 정책에 반영한다.

10. 네트워크 보안

클라우드 환경은 온프레미스 환경과 달리 물리적으로 구축하고 운영해야 했던 네트워크 구축, 서버 구축 등의 업무를 논리적으로 수행할 수 있게 해준다. 논리적인 접근을 허용한다는 것은 온프레미스 환경에 IDC 출입권한을 제공하는 것과 같다. 비인가자에게 접근이 허용되면 네트워크, 서버를 삭제 하여 서비스를 삭제하여 가용성을 침해당해 연무연속성을 유지 하지 못할 수도 있고 불법으로 정보를 유출하거나 서비스와 무관한 서버를 생성하여 백도어, 좀비PC 등의 악의적인 목적으로 악용될 수 있다.

이러한 행위를 차단하기 위해서는 정교한 접근통제 정책을 수립하여 적용하여야 한다. 접근통제 정책은 아키텍처 설계 단계에서 반드시 같이 검토되고 아키텍처 구축 과정에서 반영하고 모니터링 여부를 확인해야 한다. 다음 아래 사항을 참고하여 네트워크 보안을 강화해야 할 것이다.

네트워크 정보보호요구사항

① 네트워크 접근통제를 H/W 형태, S/W 형태, API 형태 중 어떤 것을 선택할 것인지 고려해야 한다.

※ 클라우드 서비스 업체에서 제공하는 방식에 대해 확인필요

- H/W 형태 : 기존 온프레미스 환경과 동일
- S/W 형태 : 서버에 접근통제 솔루션을 설치하는 방식으로 여러 대를 설치해야 할 수 있음
- API 형태 : 기존의 네트워크 솔루션 기반의 접근통제 방식과는 다른 개념으로 성능 및 네트워크와 무관하게 원하는 방식으로 그룹을 묶어서 접근통제 가능

② 네트워크 트래픽 도청이나 데이터 유출 방지를 위해 통신 암호화를 적용하여 관리한다.

③ 사용자의 네트워크 접속 · 인증을 위한 신분확인 메커니즘을 도입한다.

④ 네트워크 가용성이 침해하는 서비스거부공격(DoS)에 대한 대책을 마련한다.

⑤ 이(異)기종 네트워크의 연동에 따른 보안대책을 고려한다.

⑥ 네트워크 장애에 대비하여 네트워크 분할 또는 이중화하여 관리한다.

⑦ 네트워크 장애에 대비하여 보안관제 체계 구축을 고려한다.

11. 데이터 보호 및 백업

클라우드 서비스에서는 이용자의 대용량 정보, 기업의 중요한 기밀정보 등을 다른 이용자와 공동으로 사용하는 스토리지에 저장하기 때문에 서비스 이용과 관련해 이용자 데이터의 안전한 관리가 선행되어야 한다. 또한, 데이터 전송 중에도 데이터 유출의 위험이 있기 때문에 데이터의 암호화 전송이 필요하다. 특히, 시스템 설정 파일, 시스템 구성 및 관리 문서, 개인 정보 및 계정 정보는 서비스 이용에 필수적인 이용자 데이터로 암호화하여 저장 · 관리가 반드시 이루어져야 한다. 또한, 클라우드 서비스의 기본 전제는 이용자가 항상 서비스를 사용할 수 있는 환경을 제공한다는 것이다. 따라서 장비의 고장이나 예측할 수 없는 사고에 대비하여 다음과 같은 정보보호요구사항 고려하여 이용자 데이터, 서버 접근 로드 등의 저장 · 관리 이중화 및 백업 대책을 마련하고 운영하는 것이 필요하다. 그리고, 클라우드 특성상 가상화로 구현된 인프라 관련 데이터는 백업이 불가능하기 때문에 가상 이미지 파일(스냅샷)과 같은 대체 방안을 고려해야 한다. 따라서, 내부 백업 정책에 따라, 이용자 데이터의 백업을 수행하고, 주기적으로 백업 시스템을 테스트하고 점검하는 것이 필요하다. 따라서, 다음과 같은 정보보호 요구사항 참고하여 데이터 보호를 위한 대책을 마련한다.

데이터 보호 정보보호 요구사항

① 국내에서 권고하는 안전한 암호화 알고리즘 사용한다.

- 주민등록번호 및 계좌번호 등의 정보 저장 시 이용하는 알고리즘

※ AES, SEED, ARIA-128/192/256, 유효기간 : 송신용(2년 이내), 수신용(5년 이내)

- 비밀번호 및 바이오 정보를 저장 시 이용하는 알고리즘

※ SHA-224/256/384/512 ② 암호 알고리즘을 통한 이용자 데이터 암호화 실행에는 안전한 키 분배, 키 관리 메커니즘 등을 적용한다.

③ 이용자 데이터 백업을 위한 별도의 백업 장비 구축, 장비 이중화 등 백업 방안 등을 포함하는 백업정책을 수립하고 해당 정책에 따라 데이터를 주기적으로 백업한다.

④ 백업 장치 신뢰성과 데이터 무결성 검증을 위해 주기적으로 확인하고 점검한다.

12. 시스템 개발 및 도입 보안

기업이 클라우드 시스템을 신규로 개발하거나 기존 시스템을 변경할 경우, 혹은 클라우드 시스템을 새로이 도입하는 경우가 있을 수 있다. 클라우드 시스템 구현 시 안전하지 않은 코딩방법을 사용하거나 비인가자가 소스코드에 접근해 악성코드를 심어 해당 클라우드 시스템 사용자에게 피해를 입힐 수 있다. 따라서 분석 및 설계과정에서 도출한 보안요구사항을 적용했는지 여부를 파악하고 인가된 사용자만 소스 프로그램에게 접근하도록 하는 통제절차를 수립하는 것이 중요하다. 신규 클라우드 시스템 개발 및 기존 시스템 변경 시 (개인)정보 영향 평가 결과, 정보보호 기본요소, 최신 보안취약점 등을 고려한 보안 요구사항을 정의하고, 해당 보안 요구사항을 설계 단계에서부터 구현, 시험, 이관까지 체계적으로 적용하는 것이 필요하다.

시스템 개발 및 도입 정보보호 요구사항

① 신규 시스템 개발 및 기존 시스템 변경 시 정보보호 관련 법적 요구사항(정보통신망법, 개인정보보호법 등), 최신 보안 취약점, 정보보호 기본요소(기밀성, 무결성, 가용성) 등을 고려하여 보안요구사항을 명확히 정의하고 이를 적용한다.

② 클라우드 시스템 설계 시 사용자의 인증, 권한 변경, 중요정보 이용 및 유출 등에 대한 감사증적을 확보할 수 있도록 한다.

③ 시큐어 코딩을 적용하여 시스템을 구현 하고, 분석 및 설계 과정에서 도출한 보안요구사항이 정보시스템에 적용되었는지 확인하기 위한 시험을 수행한다.

④ 개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소하기 위해 원칙적으로 분리하며, 단 분리하여 운영하기 어려운 경우 그 사유와 타당성을 검토하고 안전성 확보 방안을 마련한다.

⑤ 클라우드 시스템 개발을 외주 위탁하는 경우 분석 및 설계단계에서 구현 및 이관까지의 준수해야 할 보안요구사항을 계약서에 명시하고 이행여부를 관리·감독한다.

⑥ 클라우드 시스템의 처리 속도와 용량에 대하여 주기적인 모니터링을 수행하고 안정성의 확보에 필요한 시스템 도입 계획을 수립한다.

⑦ 클라우드 인프라 운영시스템 관련 소스 프로그램에 대한 변경관리를 수행하고 인가된 사용자만이 소스 프로그램에 접근할 수 있도록 통제절차를 수립하여 이행 한다. 또한 소스 프로그램은 운영환경에 보관하지 않는 것을 원칙으로 한다.

⑧ 새로 도입되는 시스템에 대한 인수 기준이 수립하고, 인수전에 테스트를 수행한다.

4 클라우드 컴퓨팅 실무 보안

3절에서는 클라우드 인프라 운영에 하는데 필요한 보안관리체계 관점에서 갖추어야 하는 보안요구사항을 다룬 것이며, 본 절에서는 클라우드 환경변화에 따라 달라지는 사항 중심으로 보안 실무 수행 시 어떤 사항들을 고려하여 적용해야하는지 그리고, 클라우드 제공업자가 제안하는 솔루션이나 이용자 관점에서 업무에 적용했던 일부 사례를 통해 클라우드 환경에서의 보안 실무 수행 방안을 기술한다.

다음 아래 표는 보안 업무를 수행하는 영역별로 클라우드 서비스 환경의 특징이 반영될 경우 어떻게 달라지는지 클라우드 서비스 환경과 기존 온프레미스 환경을 비교한 것이다.

구분	온프레미스 환경	클라우드 환경
1. 서비스 오픈/이관	· 기획, 개발, 배포 단계별 점검	· 클라우드 환경 고려한 기획, 개발, 배포 단계별 점검
2. 아키텍처 설계	· 물리적인 아키텍처 포함한 설계	· 가상환경의 논리적인 아키텍처 설계
3. 네트워크 접근통제	· H/W 형태의 보안솔루션을 통한 접근통제	· S/W형태의 솔루션을 이용한 접근통제 · 클라우드 서비스에서 제공하는 API형태의 접근통제
4. 보안솔루션 구축	· H/W 형태의 네트워크 보안 솔루션 및 Host 보안솔루션 · H/W DDoS 솔루션, ISP 제공 DDoS 차단 서비스	· S/W 형태의 네트워크 보안 솔루션 및 Host 보안솔루션 · S/W 형태 솔루션 및 클라우드 서비스 제공 DDoS 차단 서비스 등
5. 계정 및 권한 관리	· OS 접속에 대한 권한 관리	· 가상 자원 생성 및 사용에 대한 권한 관리 · OS 접속에 대한 권한 관리
6. 서버(OS) 보안	· 설치된 OS, WEB, WAS, DBMS에 대한 Hardening (클라우드는 배포 이미지에 따라 Hardening 범위가 달라짐)	
7. 취약점 점검	· 인프라(H/W Appliance 등), 어플리케이션 취약점 점검	· 어플리케이션, 가상자원 사용권한 취약점 점검 위주
8. 보안관제	· 침입 및 정보유출에 대한 모니터링	· 침입 및 정보유출에 대한 모니터링 · 가상 자원의 생성, 변경, 삭제 등 가용성에 대한 모니터링

1. 서비스 오픈/이관

클라우드 서비스 운영정책, 운영 조직, 컴플라이언스 검토가 완료되었다면 클라우드 서비스로 신규 서비스를 구축하거나 기존에 구축되어 있는 서비스를 이관하는 작업을 수행해야 한다. 그러나 클라우드 환경으로 서비스를 구성하는 경우, 아래와 같은 다양한 문제점으로 인해 원하는 시기에 원하는 수준의 서비스 구성을 진행하지 못할 수 있다. 그렇기 때문에 클라우드 서비스 구성 및 이전에 대한 절차를 마련하여 단계별로 확인하는 것이 필요하다.

클라우드 이관 시 발생할 수 있는 문제점

- 클라우드 서비스에 대한 지식 및 운영 경험 부족으로 인한 문제
- 인프라/네트워크/보안/비지니스 관련 정책의 미적용으로 인한 문제
- 회사의 공통 모듈 미사용으로 인한 호환성, 확장성 문제
- 개별적인 서비스 구성으로 인한 추가 비용 발생

[클라우드 서비스 이관 절차]

서비스 오픈/이관 보안요구사항

① 시작단계 : 서비스 목적, 서비스 구성, 서비스 리스크, 기업의 보안정책 공유 및 준수
- 서비스 목적 : 서비스 식별, 서비스 오픈 ETA, 서비스 담당자, 이해 관계자
- 서비스 구성 : 클라우드 자원 논리적 구성도, 타 서비스 연동 및 영향도, 예상 트래픽, 예상 비용
- 서비스 리스크 : 장애 발생 시 영향도 및 대처 방안, 컴플라이언스 이슈사항(개인정보, 금융정보 처리
- 기업의 보안정책 공유 : 개발 및 배포단계에서 적용할 수 준비하여 제공

② 개발단계 : 시작 단계에서 제공한 정책 및 요구사항이 잘 반영되고 있는지 개발 or 이전 서비스 1차 초안 완료 시 중간 점검을 수행한다.

③ 배포단계 : 시작단계에서 확인된 사항에 변동된 부분은 없는지 변동된 부분이 있다면 보완할 부분은 없는지 확인한다. 또한, 회사의 정책과 표준을 준수했는지를 점검하고 클라우드 서비스 오픈 여부를 결정한다.

** 체크리스트 예시
- 클라우드 리소스를 사용하기 위한 적절한 권한을 부여 받았는가?
- 클라우드 아키텍처에 적합한 서비스 아키텍처를 구성하였는가?
- 회사에서 제공하는 API 표준을 준수하였는가

- 회사에서 지정한 표준 가상OS 이미지를 사용하였는가?
- 서비스의 모든 자원은 회사의 자산 식별 정책을 준수하였는가?
- 회사에서 요구하는 보안솔루션이 구축 및 설치되었는가?
- 회사에서 요구하는 수준의 접근통제 정책이 적용되었는가?
- OS/미들웨어/어플리케이션에 대한 보안 규칙은 적용되었는가?
- 어플리케이션에 대한 보안 취약점 점검은 수행하였는가?
- 개인정보 및 금융 정보 이전 시 컴플라이언스에 대한 이슈 점검은 완료하였는가?

2. 아키텍처 설계

클라우드 서비스는 가상의 공간이기 때문에 기존의 IT 환경과 달리 물리적인 제약이 없어, IDC와 같은 서비스 영역을 여러 개 생성하여 분리할 수도 있고 통합하기 용이하다. 아키텍처 설계는 서비스의 규모, 회사의 개발 문화, 개발 방법론에 따라 구성하지만 클라우드 환경에서는 잘못된 아키텍처 설계로 인해 비인가자가 권한을 획득하거나 접근통제가 이루어지지 않는다면, 중요정보의 유출은 물론이고 논리적인 아키텍처 자체에 손실이 발생하면 업무 연속성에 치명적인 영향을 줄 수 있기 때문에 보안을 최우선으로 반영하여 아키텍처를 설계하는 것이 필요하며, 아키텍처 설계 시 다음을 고려하는 것이 필요하다.

아키텍처 보안요구사항

① 확장성 : 클라우드는 로드밸런싱, 오토스캐일링 기능을 사용하여 리소스 늘리고 축소가 가능
- 기본 서비스에서 최대 사용할 수 있는 IP수(Public/Private IP)
- 클라우드 제공업체와 협의하여 최대 확장할 수 있는 IP수
- Load Balancing, Auto-Scaling 지원여부
- Auto-Scaling 시 과금정책
- 구축된 보안솔루션의 Auto-Scaling 여부

② 지연 또는 대기(latency)시간 : 클라우드는 가상 IDC, 가상 네트워크, 가상 서버, 가상 DBMS 등 모든 환경이 가상으로 구성된다. 또한, 클라우드 환경이라는 특수성 때문에 서로 다른 지역에 Resource가 위치 할 수 있어 기존 온프레미스 환경 보다 속도가 느릴 가능성이 있다. 따라서, 속도가 민감한 서비스의 경우 네트워크 속도, 서버의 성능, DBMS 반응 속도 등 다양한 부분에서 서비스에 적합한 성능과 속도를 제공 받을 수 있는지 확인 필요
- 서비스 특성 파악(속도에 민감 여부 확인)
- 클라우드 네트워크와 온프레미스 네트워크 속도 테스트
- 클라우드 DB와 온프레미스 DB의 반응속도테스트
- Hybrid 구성시 속도 테스트

③ 서비스 구성
- 모놀리틱(Monolithic) 아키텍처 : 서비스 아키텍처를 하나의 일체형으로 구축하는 방법

※ 단일 VPC를 이용할 경우 서비스 구조가 단순하기 때문에 속도가 빠르고, 비용 효율적일 수 있으나 Resource 제한 등으로 인해 확장성이 부족할 수 있다.

- 마아크로서비스(Micro service) 아키텍처 : 단일 응용 프로그램을 나누어 작은 서비스의 조합으로 구축하는 방법

※ 여러 개의 계정을 사용하여 관리하고, 마이크로 서비스를 구현하는 등 확장성이 좋아진다. 그러나 구조가 복잡하기 때문에 latency 이슈, 비용이 증가할 가능성이 높다.

④ 비용

- 각 서비스별 비용 확인 및 미래비용 예측하는 절차를 포함하여 아키텍처 설계

※ 클라우드는 다양한 서비스 제공(독립적 서비스, 공용 서비스, 단일 공간, 다중 공간 등)함에 따라 이용자는 어떤 서비스를 이용하느냐에 따라 비용이 달라짐으로 아키텍처 설계 시 고려필요

⑤ 보안솔루션 구성

- 클라우드 환경의 보안솔루션은 대부분 하드웨어가 아닌 소프트웨어 기반으로 성능, 기능 고려필요

※ 보안솔루션의 구성방식 및 종류에 따라 네트워크 기반(또는 호스트 기반)으로 구성 할지 결정이 필요하며, 솔루션이 제공되지 않을 경우 기업이 고려한 보안구성을 하지 못할 수 도 있음

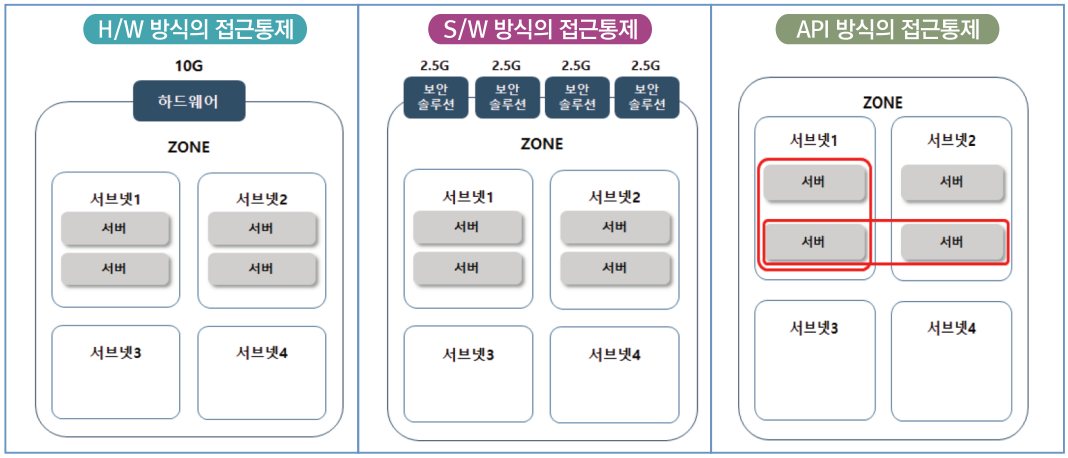
⑥ 클라우드 관리계정의 형태(단일 또는 다수)

- 서비스 특성 파악(속도에 민감 여부 확인)
- 클라우드 네트워크와 온프레미스 네트워크 속도 테스트
- 클라우드 DB와 온프레미스 DB의 반응속도테스트
- Hybrid 구성 시 속도 테스트

⑦ 업무연속성 : 서비스 가용성, 재해 시 신속한 복구를 고려한 아키텍처 설계 필요

3. 네트워크 접근통제

클라우드 서비스에서는 접근통제를 수행 할 수 있도록 접근통제 솔루션을 제공하며 H/W 형태, S/W형태, API 형태로 구분될 수 있다. 접근통제 솔루션의 형태에 아키텍처가 변경될 수 있기 때문에 서비스 이용 검토 시 반드시 클라우드 서비스 업체에서 제공하는 방식을 명확하게 확인하고 수립된 접근통제 정책이 적용 가능한지 충분한 검토가 필요하다. H/W 방식은 기존의 온프라미스 환경에서 사용하는 것과 동일한 appliance 방식으로 동일하게 구성이 가능하지만 클라우드 환경을 이용하는 이점이 없다. S/W 방식은 서버에 접근통제 솔루션을 설치하는 방식으로 서버의 성능에 따라 여러 대를 설치해야 할 수 있는 단점은 있다. API 방식은 기존의 네트워크 솔루션 기반의 접근통제 방식과는 다른 개념으로 성능과 무관하며 네트워크와 무관하게 원하는 방식으로 그룹을 묶어서 접근통제를 할 수 있다. 그러나 생성할 수 있는 룰의 수에 제한이 있을 수 있다.



※ 여기서는 클라우드 장점을 살린 API 방식에 대해서만 다루도록 하겠다.

네크워크 접근통제 보안요구사항

① 네트워크 접근통제를 H/W 형태, S/W 형태, API 형태 중 어떤 것을 선택할 것인지 고려해야 한다.

※ 클라우드 사업자가 제공하는 네트워크 접근통제가 API 방식을 제공하는지 확인한다.

- H/W 형태 : 기존 온프레미스 환경과 동일
- S/W 형태 : 서버에 접근통제 솔루션을 설치하는 방식으로 여러 대를 설치해야 할 수 있음
- API 형태 : 기존의 네트워크 솔루션 기반의 접근통제 방식과는 다른 개념으로 성능 및 네트워크와 무관하게 원하는 방식으로 그룹을 묶어서 접근통제 가능

② 클라우드 사업자가 API 방식의 Security Group 등 이와 유사한 방법으로 네트워크 접근통제 기능을 제공하는지 확인한다.

③ Security Group 기능 등을 이용하여 Inbound, Outbound 트래픽 제어를 해당 기업 네트워크 보안정책에 맞게 설정하고 이를 준용한다.

《 예시 》

㉠ 기본정책 설정

→ Inbound Deny All, Outbound Any Open(또는 Inbound Deny All Outbound 허용대역 Open)

㉡ 모든 트래픽이 Security Group의 규칙을 적용 받을 수 있도록 설정

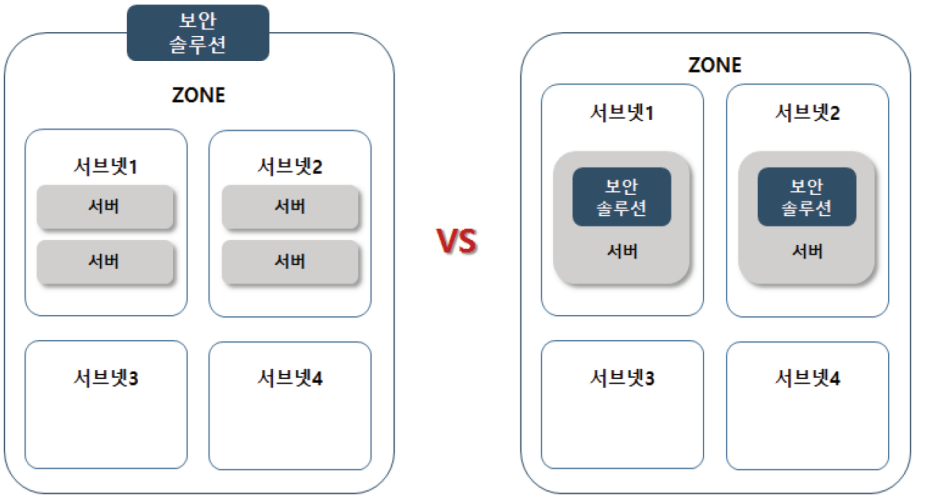
㉢ 새로운 가상서버 생성 시 Security Group의 규칙에 적용받을 수 있도록 설정 등

※ 네트워크 접근통제는 해당 사의 비즈니스(혹은 이용모델)에 따라 필요한 서비스, 포트 등 허용하는 서비스(또는 Port) 등을 화이트리스트 기반으로 설정하여 이용할 것을 권고한다.

4. 보안솔루션 구축

클라우드 환경에서 보안솔루션 구축을 검토할 때 얼마나 서비스 확장성에 맞게 확장될 수 있는지도 고려해야 한다. 구축된 보안솔루션이 서비스 확장성이 영향을 준다면 다른 솔루션으로의 교체나 아키텍처 자체를 다시 설계해야 할 수도 있다. 일반적으로 확장성이 반드시 보장되어야 한다면 호스트 기반의 보안솔루션을 설치하는 것이 적합한 방법이다.

[설치 위치에 따른 보안솔루션 구축]



예를 들어 클라우드 환경을 평소 보다 2배 혹은 10배 정보 가변성이 있는 서비스 특성을 고려해 서버를 Auto Scaling 할 수 있도록 구성해 놓은 환경일 경우, 네트워크 보안솔루션도 서비스 구성에 맞춰 Auto Scaling이 가능해야 할 것이다. 모든 네트워크 기반의 보안솔루션이 아직은 Auto Scaling을 지원하지 않기 때문에 구축 전에 반드시 확인해야 한다.

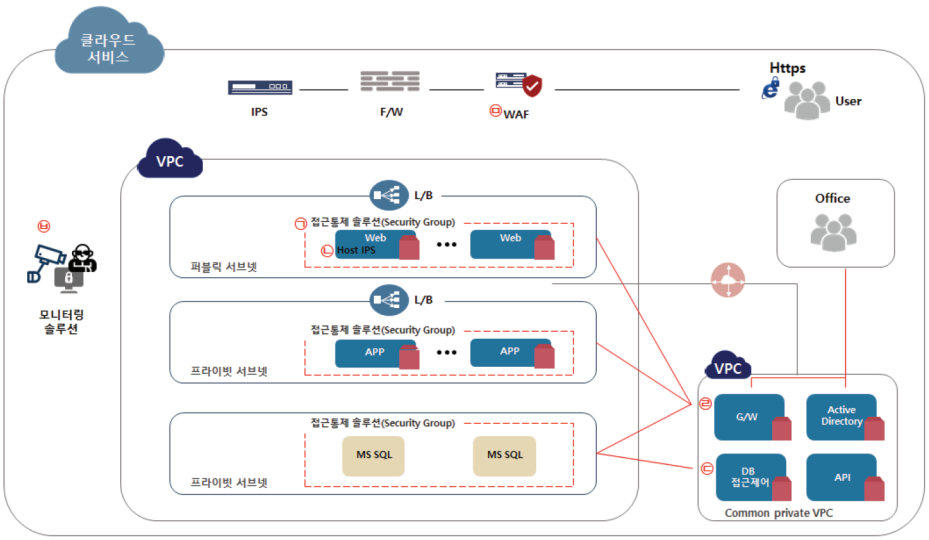
보안솔루션 구축 보안요구사항

① 보안솔루션 구축 시 네트워크 기반으로 구축할지 호스트 기반 구축할지 다음 아래사항과 참고하여 검토하고 선택한다.

[보안솔루션 구축 시 고려사항]

네트워크 기반	호스트 기반
• 서버에 S/W 보안 솔루션을 설치하는 구조로 대량 트래픽을 처리하기 위해 다수의 서버 운영이 필요할 수 있음 • Zone을 다수 운영할 경우 Zone별로 별도도 보안솔루션을 구성해야함 • Auto Scaling, HA 구성이 불가한 솔루션이 많아 반드시 확인해야함	• OS에 설치했을 때 오동작이 없는지 검증 필요함 • 최신 OS 지원여부 확인 필요함(CentOS7, Ubuntu 16.04, CoreOS 등)

[클라우드 환경에서의 보안솔루션 구축 예시]



㉠ 접근통제 솔루션(Security Group) : 온프레미스 환경에서는 접근통제를 위해 Firewall을 사용 하였으나 클라우드 환경에서 API 형태의 접근통제솔루션을 사용할 수 있다. 물론 기존에 사용하던 Firewall을 별도 구매하여 사용할 수 있으나 클라우드 환경에서는 API 방식으로 통제하는 것이 훨씬 더 유연하고 강력하게 접근통제를 수행할 수 있다.

㉡ Host IPS : 클라우드 환경에서도 네트워크 기반의 탐지솔루션을 구축할 수 있으나 Auto Scaling, HA 구성 등의 문제로 인해 Host에 IPS를 설치하여 악성코드를 탐지하고 있다.

㉢ DB Access Control : DB Access Control System은 온프레미스 환경과 동일하게 사용 가능하다. 단, 클라우드 환경에서 서비스 형태로 제공하는 서비스의 경우 Server Agent 방식의 솔루션은 사용할 수 없다.

㉣ Server OS 접근 : Server OS에 대한 접근은 온프레미스 환경과 동일하게 구성할 수 있다. 서버접근 통제 솔루션을 구축하거나 Active Directory나 LDAP을 연동한 Gateway를 구축하여 접근을 통제할 수 있다.

㉤ WAF(Web Application Firewall) : 클라우드 서비스에서 제공하는 WAF를 구성하거나 Third-party 솔루션 구매하여 구축할 수 있다. 클라우드에서 제공하는 서비스로 WAF를 구성할 경우 일부 패턴을 사용자가 직접 제작해야 하는 경우가 존재하기 때문에 원하는 수준의 탐지나 모니터링이 가능한지 충분히 검토해야 한다. Third-party 솔루션을 구매하여 구축하는 경우에서는 Auto Scaling, HA 구성 등이 가능한지 검토해야 한다.

㉥ 모니터링 솔루션 : 클라우드 환경에서 다양한 로그들을 생성하여 제공하지만 원하는 수준의 모니터링을 수행하기에는 한계가 존재한다. 현재 판매되는 모니터링 Third-party 솔루션도 온프레미스 환경과 같은 형태로 제공을 받기에는 부족하기 때문에 기업에서 직접 모니터링 환경(SEIM 솔루션을 통한 연동, Divvy Cloud 등)을 구축해야 할 수도 있다.

5. 계정 및 권한관리

클라우드 환경에서는 다음 아래 2가지 형태의 계정 및 권한관리를 고려하여야 한다.

① 클라우드 서비스 계정 : 클라우드 서비스에 자원을 성생할 수 있는 권한
② VM OS 접근 계정 : 가상서버의 OS에 접근할 수 있는 권한

① 클라우드 서비스 계정

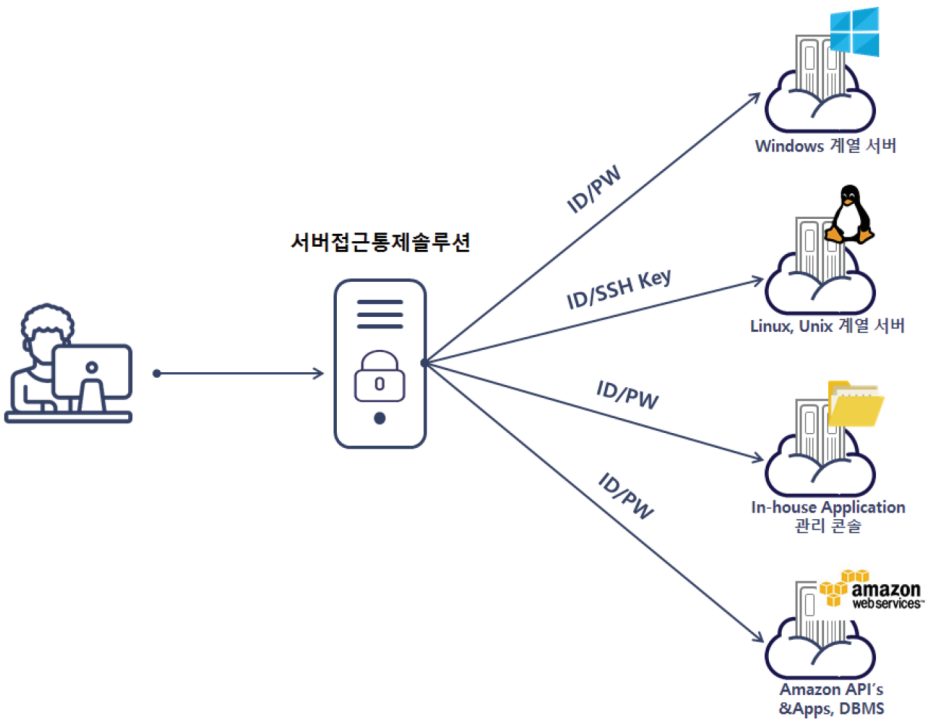
클라우드 자원을 관리하는 기능은 다양하게 존재하지만 계정에 권한을 부여하고 접근통제를 수행하는 것은 기업의 몫이기 때문에 잘못된 권한 설계는 기업 보안의 치명적인 취약점이 될 수 있다. 또한, 계정의 중요도에 따라 중요한 권한을 수행하는 Admin 계정 등에 대해서는 2차 인증 등의 추가 인증수단을 수행하여 보호하는 것이 필요하다. 그리고 클라우드 서비스 관리 콘솔은 회사에서 허용한 IP에서만 접속할 수 있도록 접근통제를 수행하는 것이 필요하며, 관리콘솔을 접속할 수 있는 IP가 통제 되지 않는 것은 외부로 부터의 악의적인 접속시도 및 해킹으로 인해 기업의 서비스가 치명적인 영향을 받을 수도 있음을 명심해야 할 것이다.

② 가상서버 OS의 접근 계정

클라우드 환경에서 가상서버 OS의 접근계정은 기존의 온프레미스 환경과 차이가 없다. 따라서, 서버 접근통제솔루션을 도입하여 계정관리 및 접근통제를 수행하거나 그에 상응 보안기술을 적용하여 접근제어를 해야 한다.

대부분의 접근통제 솔루션들은 클라우드 서비스에서 사용할 수 있기 때문에 서로 다른 클라우드 환경을 사용하는 경우에 유용하게 사용할 수 있다. 다음 아래 그림은 서버접근통제 솔루션을 이용하여 다양한 OS 계열을 관리하는 화면이다.

[서버접근통제 솔루션 사용 예시]



계정 및 권한관리 보안요구사항

① 클라우드 서비스 계정은 해당 사의 VM를 생성 · 삭제 권한을 갖는 것으로 다음 아래 사항을 참고하여 계정 및 권한 관리를 해야 한다.

- 클라우드 서비스 계정은 최소인원으로 한정하고 관리해야 한다.

  ※ 특히, Admin 계정에 대해서는 추가 2차 인증 등의 수단을 적용할 것을 권고 한다.

- 클라우드 서비스 관리 콘솔은 회사에서 허용한 IP에서만 접속할 수 있도록 접근통제를 적용한다.

② VM OS 접근 계정은 가상서버의 OS에 접근할 수 있는 권한을 갖는 것으로 서버 접근통제 솔루션을 도입하여 계정 관리 및 접근통제를 수행할 것을 권고한다. 또는 그에 상응 보안기술을 적용하여 접근제어를 해야 한다.

6. 서버 OS 보안

클라우드 환경에서 자원을 생성할 수 있는 권한을 보유한 사용자는 클라우드 서비스에서 제공하는 다양한 OS를 설치해서 사용할 수 있지만 기업에서 사용할 OS를 선택하기 전에 많은 요소를 고려해야 한다. 가상 서버를 안전하고, 효율성 있게 사용하기 위해서는 기존 시스템과의 호환성, 표준 OS, DB의 사용 등 다음 아래 사항을 고려해야 할 것이다.

가상서버(표준 OS, 호환성 등) 보안요구사항

① 클라우드 서비스 가상서버에서 OS, DB 등 소프트웨어 사용 시 구현 시 다음 아래사항을 고려해야 한다.

- 기존 시스템과의 호환성
- 배포판의 평판
- 상용 지원의 가능성
- 표준 OS, WEB, WAS, DBMS 사용 정책 수립
- 표준으로 채택된 OS 및 Application에 대한 Hardening1)
- Hardening이 적용된 배포 Image 작성

※ 1) Hardening 이란 : 보안 설정으로 공격으로부터 시스템을 안전하게 지키는 방법

예시) 최소 권한 모델(least-privilege model)설정, 부트 프로세스 보안, 할당량과 한계 적용, Telnet 사용금지하고 SSH만 허용 등

- 표준 OS Image 관리 프로세스를 수립하고, 주기적인 서버 취약점 점검 및 보안패치 ※ 부득이 비표준 OS 등 사용 시 해당 OS 모니터링 및 향후 표준 OS로 전환 검토 필요

② 만약, Docker 환경일 경우 OS까지 자동 배포 할 수 있기 때문에 Hardening, 취약점 점검, 신규 취약점 패치 등을 모든 서버에 개별적으로 진행하지 않고 표준 Image만 적용해서 배포가 가능하다. 하지만 이러한 Docker 형태로 구축하여 사용할 경우 다음 아래를 고려해야 한다.

- Docker를 원활히 사용할 수 있는 CentOS7, CoreOS, Ubuntu 16.04, Container(Docker) 등 배포시스템 구축에 대한 Hardening
- Docker 시스템 구조를 이해하고 관련 취약점 최소화 노력

※ Container(Docker)는 기존 가상화(하이퍼바이저) 환경과 달리 별도의 GuestOS를 사용하는 것이 아닌 Host OS에 파일 형태로 설치되어 Host OS의 자원을 공유하여 사용하는 구조로 속도가 빠른 장점이 있으나 HostOS가 보안이 취약하거나 Container(Docker)가 보안에 취약할 경우 영향을 줄 가능성이 존재하며, Docker를 사용할 경우, Docker가 root 기반으로 동작하기 때문에 root 권한을 개발자에게 부여해야 함에 따른 권한관리를 철저히 해야 할 것이다.

7. 취약점 점검

클라우드 서비스 환경에서의 취약점 점검은 기존의 온프레미스 환경에서 수행하는 모든 취약점 점검을 포함하며, 클라우드 환경은 리소스 관리가 가상환경에서 이루어지므로 이러한 가상환경에서 발생할 수 있는 취약점, 클라우드 서비스 이용자가 공용으로 사용하는 공용 서비스에 대한 취약점 점검, 클라우드 서비스의 리소스를 관리하는 계정의 권한 검토 등 클라우드 서비스 환경에서는 추가로 다음 사항을 포함한 취약점 점검을 해야 할 것이다.

취약점 점검 보안요구사항

① 클라우드 서비스 환경에서의 IAM(Identity and Access Management) 권한 점검
- 계정관리 정책 수립 여부
- 계정별 권한 관리 매트릭스 작성 및 시스템 적용 여부
- 계정에 부여된 패스워드 정책수립 및 적용 여부
- Access Key로 인증할 경우 키 관리 방안 수립 여부
- 중요권한을 보유한 계정에 대한 Multi Factor 추가 인증 여부
- 계정 및 패스워드 전송구간 암호화 여부
- 허용된 Network 범위에서만 접근 허용 여부
- 모든 계정 생성/수정/삭제 및 활동 로그 생성 여부
- 계정 및 권한 관리 시스템 자동화 여부

② 클라우드 서비스 환경에서의 네트워크 점검
- **네트워크 아키텍처**
  - Public / Private Network 구성의 적절성 여부
  - 외부 서비스와 연동 시 구성의 적절성 여부
  - 가상서버 접근 Gateway 서버 구성의 적절성 여부
  - 보안솔루션 설치의 적절성 여부
- **접근통제 정책**
  - Any/Any Open으로 설정되어 있는 정책 존재 여부
  - 외부에 불필요하게 오픈되어 있는 서비스 포트 존재 여부
  - 만료된 접근통제 정책 존재 여부

③ 클라우드 서비스 환경에서의 서버 점검
- 클라우드 환경에서 사용할 표준 Image(OS, WEB, WAS 등)만 생성하고 사용하는지 여부
- 표준 Image(OS, WEB, WAS 등)에 대한 취약점 점검이 완료된 것인지 여부

8. 보안관제

클라우드 서비스 환경에서는 매우 다양한 운영 체제, 프로그래밍 언어, 프레임워크, 도구, 데이터베이스 및 장치를 지원하기 때문에 기존 온프레미스 환경 보다 모니터링이 더욱 중요해 진다. 온프레미스 환경에서 수집하고 모니터링 하는 OS 로그, Web application 로그, 보안솔루션 로그에 더해 자원의 생성, 삭제, 변경 할 수 있는 클라우드 서비스 계정 로그, 자원이 생성, 삭제, 변경된 로그 등을 통합해서 모니터링 하는 것이 필요하다. 클라우드 환경에서 보안관제를 수행하기 위해서는 다음 아래사항을 고려해야 한다.

보안관제 보안요구사항

① 클라우드 리소스 생성/변경/삭제 관련 로그 수집 및 모니터링
② 가상서버 등 클라우드 서비스에서 자체적으로 남기는 로그 수집을 통한 모니터링
③ 호스트 레벨의 보안제품(오픈소스)을 통한 시스템 감시 및 로그 모니터링
④ 클라우드 가상 네트워크 상의 패킷 감시 및 로그 모니터링
⑤ 파트너 사의 클라우드 기반의 보안솔루션 사용을 통해 로그 수집 및 모니터링
⑥ 특히, 클라우드 특성을 고려한 모니터링 대상은 다음과 같다. 아래사항을 포함 보안관제가 필요함
- 루트 또는 관리 권한을 가진 개인이 수행한 작업
- 모든 감사 추적에 대한 액세스
- 잘못된 논리적 액세스 시도
- 식별 및 인증 메커니즘 사용
- 감사 로그 초기화
- 시스템 수준의 객체 생성 및 삭제

또한, Splunk, sumologic, QRadar, ArcSight와 같은 로그통합관리 솔루션을 검토하여 활용하는 것을 고려하면 좋을 것으로 기대된다.

[부록 1] 참고자료

[1] '민간 부문의 클라우드 도입 실무 가이드라인', 방송통신위원회, 2012
[2] '클라우드 서비스를 위한 SLA가이드', 방송통신위원회, 2011
[3] '민간 부문의 클라우드 도입 실무 가이드라인', 클라우드컴퓨팅표준화포럼, 2012
[4] '클라우드 서비스 정보보호 안내서', 한국인터넷진흥원, 2011
[5] '클라우드 서비스와 가상화 기술', 한국정보통신기술협회, 2009
[6] '클라우드 도입에 따른 행정환경 변화와 감사시사점', 감사원, 2016
[7] 배유미, 정성재, 소우영, '웹 서버 구성을 통한 가상머신과 컨테이너 방식 비교 분석', 한국정보통신학회 논문지, 2014
[8] '정보보호조직 구성 및 운영 가이드', 한국정보통신기술협회, 2012
[9] '조직의 정보보호를 위한 자산관리 지침', 한국정보통신기술협회, 2010
[10] '알고리즘 및 키 길이 이용 안내서', 한국인터넷진흥원, 2010
[11] '패스워드 선택 및 이용안내서', 한국인터넷진흥원, 2010
[12] '침해사고대응팀(CERT) 구축/운영 안내서', 한국인터넷진흥원, 2010
[13] '가상화 기술의 동향 및 주요 이슈', 정보통신정책연구원, 2013
[14] '클라우드 데스크톱 가상화 기술 동향', 한국전자통신연구원, 2013
[15] '오픈 소스 프로젝트를 위한 도커 기반 버전 관리 기법', 한국산학기술학회 논문지, 2016
[16] '가장 빨리 만나는 Docker', 길벗, 2014
[17] 'IDC white paper' (Cloud Going Mainstream : All Are Trying, Some Are Benefiting; Few Are Maximizing Value), Cisco, 2016
[18] '클라우드 표준계약서(B2B, B2C)', 과학기술정보통신부, 2016
[19] 'Understanding the shared responsibility of cloud security', ALERT LOGIC, 2015
[20] 'The Notorious 9 Cloud Computing Top Threats in 2013', CSA, 2013
[21] 'Treacherous 12 Cloud Computing Top Threats in 2016', CSA, 2016
[22] '클라우드 환경으로 전환하는 최적의 방법: 신뢰성, 경제성, 기능성 간의 균형적 모색', EMC2, 2011
[23] '2016 상반기 섀도 데이터 보고서', 시만텍, 2016
[24] '2017년 10대 보안 전망 보고서', 시만텍, 2016
[25] '2015 클라우드 컴퓨팅 기술 스택', 클라우드컴퓨팅연구조합, 2016
[26] '소프트웨어 개발보안 가이드', 한국인터넷진흥원, 2017
[27] 'K-ICT 클라우드 컴퓨팅 활성화 계획', 관계부처합동, 2015
[28] '공공기관 민간 클라우드 이용 가이드라인', 행정안전부, 2016

클라우드 서비스를 이용하는 기업 IT담당자 위한

클라우드 정보보호 안내서

2017년 12월 인쇄
2017년 12월 발행

발행처 : **한국인터넷진흥원**
전라남도 나주시 진흥길 9(빛가람동 301-2)
Tel : 1544-5118

인쇄처 : ㈜한국장애인상생복지회
Tel: (02) 2644-2911