㈜클라우드 가상화 보안관리지침은 클라우드컴퓨팅서비스를 제공하기 위한 운영문서로서 검토되고 승인됨	구분	직위	성명	일자	서명
	승인	정보보호 최고책임자	홍길동	2019.01.01	
	검토	정보보호 담당자	장길산	2019.01.01	

㈜클라우드
가상화 보안관리지침

2019. 01. 01

㈜클라우드

문서 제·개정 이력				
번호	날짜	쪽	내용	담당자
1	2019-01-01	-	최초 작성	홍길동

본 문서는 가상화 보안관리지침에 대한 예시이며, 클라우드컴퓨팅서비스 제공자는 자사의 서비스 형태, 운영환경 등을 고려하여 작성하여야 한다.

제1장 총칙

제1조(목적) 이 지침은 ㈜클라우드의 「정보보호정책서」에 의거 구성원의 가상화 보안관리에 필요한 사항을 규정함을 목적으로 한다.

제2조(적용범위) 이 지침은 ㈜클라우드의 클라우드컴퓨팅서비스 업무에 종사하는 임직원 및 ㈜클라우드와 계약을 맺어 클라우드컴퓨팅서비스 업무 외부업체 직원 모두에게 적용된다.

제3조(용어정의) 이 지침에서 사용하는 용어의 정의는 다음과 같다.

1. “악성코드”이라 함은 컴퓨터바이러스와 달리 다른 파일을 감염시키지는 않지만, 악의적인 용도로 사용될 수 있는 유해 프로그램을 말한다.
2. “가상자원”이라 함은 가상화 기술을 활용하여 서버, 네트워크, 스토리지 등 논리적으로 생성된 자원을 말한다.

제2장 가상자원

제4조(가상자원 관리) ① 가상자원(가상 머신, 가상 스토리지, 가상 소프트웨어 등)의 생성, 변경, 회수 등에 대한 관리 방안을 수립하여야 한다.

- 가상자원의 생성, 변경, 회수 등에 대한 관리방안 수립 및 운영
- 가상자원 등을 생성/변경/회수할 때 승인절차 마련
- 가상자원을 관리하기 위한 담당자 지정
- 가상자원의 생성, 변경, 회수 등에 대한 승인 등의 책임추적성 확보
- 가상자원의 생성, 변경, 회수에 대한 주기적(분기 1회) 점검 이행
- 가상자원 관리직무와 가상자원 관리 점검직무 분리

② 가상자원의 생성, 변경, 회수 등에 대한 승인, 책임추적성 확보 방안 및 주기적 점검을 이행하여야 한다.

제5조(공개서버 보안) ① 공개서버(웹서버, 메일서버, 배포 서버 등)를 운영하는 경우 다음과 같은 보호대책을 마련하여야 한다.

- 공개 서버 전용 서버로 운영
- 웹서버를 통한 개인정보 송•수신 시 SSL/TLS 인증서 설치 등 보안서버 구축
- 접근 권한 설정
- 백신 설치 및 OS 최신 패치
- 불필요한 서비스 제거 및 포트 차단
- 불필요한 소프트웨어•스크립트•실행파일 등 설치 금지 등

- 불필요한 페이지(테스트 페이지) 및 에러처리 미흡에 따른 시스템 정보 노출 방지
- 주기적인 취약점 점검 등

② 공개 서버(웹서버, 메일서버, 배포 서버 등)는 DMZ 영역에 설치하고 공개 서버가 침해당하더라도 공개 서버를 통한 내부 네트워크 침입이 불가능하도록 접근통제정책을 적용하여야 한다.

- DMZ의 공개 서버가 내부 네트워크에 위치한 DB, WAS(Web Application Server) 등의 정보시스템과 접속이 필요한 경우 엄격하게 접근통제 정책 적용

③ 웹서버의 경우 최소한 OWASP TOP 10 웹 취약점은 기본적으로 점검하여 취약점이 발견된 경우 신속하게 조치를 하여야 한다.

제6조(악성코드 통제) ① 바이러스, 웜, 트로이목마 등의 악성코드로부터 가상환경을 보호하기 위한 다양한 클라우드 기반 보안서비스(예 : 웹 방화벽, 백신 등)를 도입하여 적용하여야 한다.

② 이상 징후가 발견되는 경우 해당 시스템은 이용하는 이용자에게 통지하고 사용 중지 및 격리 조치를 수행하여야 한다.

③ 바이러스, 웜, 트로이목마 등 악성코드가 다른 시스템에 전파되었는지 점검하여야 한다.

제7조(인터페이스 및 API 보안) ① 클라우드서비스 환경에서 상위 서비스(IaaS, PaaS 등)로 통신하는 인터페이스 및 API 뿐만 아니라 SaaS 이용자가 클라우드서비스 환경으로 접근할 수 있는 인터페이스 및 API를 식별하여야 한다.

② 상위 서비스(IaaS, PaaS 등) 사업자가 제공하는 안전한 인터페이스 및 API를 사용하여야 하며 인터페이스 및 API가 아닌 경우 해당 인터페이스 및 API가의 안전성을 확인하고 사용하여야 한다.

③ 식별된 인터페이스를 통한 중요 데이터 통신 시 암호화 등을 통하여 보호하여야 한다.

제8조(데이터 이전) ① 이용자의 데이터 이전 시 안전한 이전을 위하여 VPN 기능을 제공하여야 한다.

② VPN에서 사용되는 암호알고리즘 및 암호 키는 안전성이 확보된 메커니즘을 적용하여야 한다.

제9조(가상소프트웨어) ① 가상환경 내에 출처, 유통경로 및 제작자가 명확하지 않은 소프트웨어의 설치를 방지하여야 한다.

② 설치된 소프트웨어에 대해서는 주기적으로 보안 패치 및 업데이트가 수행되어야 한다.

③ 불법 소프트웨어 설치 및 사용 여부에 대하여 주기적으로 점검하여야 한다.

④ 가상 환경 내에 허가 받지 않은 소프트웨어 설치가 탐지된 경우 이용자에게 신속히 알려야 한다.

[별지 제1호 서식]가상자원 관리담당자 목록

가상자원 관리담당자 목록				
가상자원명	관리자명	부서명	권한	비고

[별지 제2호 서식]소프트웨어 패치관리대장

소프트웨어 패치관리대장

2019년 2/4분기

패치 적용일	시스템 명	패치내용	서비스 정상여부	패치 미적용 대책	작업자

2019. 07. 01

서버담당자 : (서명)

정보보호관리자 : (서명)