과학기술정보통신부

디지털뉴딜 한국판뉴딜

민간분야 주요정보통신기반시설 클라우드 이용 가이드라인

2021. 4.

과학기술정보통신부

1 목적

o 민간분야 주요정보통신기반시설이 클라우드를 안전하고 효율적으로 이용할 수 있도록 절차와 기준을 정함.

2 적용 대상

o 본 가이드라인 적용대상은 「정보통신기반 보호법」 제8조 1항에 의해 지정된 **민간분야 주요정보통신기반시설**임.

> **제8조(주요정보통신기반시설의 지정 등)**
> ① 중앙행정기관의 장은 소관분야의 정보통신기반시설중 다음 각호의 사항을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다.
> 1. 해당 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성
> 2. 제1호에 따른 기관이 수행하는 업무의 정보통신기반시설에 대한 의존도
> 3. 다른 정보통신기반시설과의 상호연계성
> 4. 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위
> 5. 침해사고의 발생가능성 또는 그 복구의 용이성

3 기본 방향

o **(기본 방향)** 주요정보통기반시설은 국가·사회적으로 중요한 정보통신시설로서, 기반시설 관리기관은 클라우드 이용 시 주의가 필요

※ 클라우드 서비스 특성(정보의 외부위탁, 자원의 공유 등) 상 사고파급력 및 전파력이 높아 클라우드 이용 시 주의가 필요

o **(이용 방침)** 기반시설 관리기관은 주요정보통신기반시설을 클라우드 서비스로 이용하고자 하는 경우,

- 국내에 클라우드 서비스 시설이 구축되고 국내에서 데이터*가 처리·저장되어야 하며, 정보보호관리체계인증(ISMS) 또는 이에 준하는 인증(국내·외 클라우드 인증 등)**을 받은 클라우드 서비스를 이용하여야 함.

* 여기서 말하는 데이터는 주요정보통신기반시설의 데이터를 의미함.

** 기반시설이 사용 예정인 서비스 및 데이터센터 등 이용 영역이 인증 대상에 반드시 포함되어 있어야 함.

- 또한, 클라우드 이용 시에도 기존 주요정보통신기반시설과 동일하게 기반보호법 內 보호가 가능 함을 보장*하여야 함.

* 클라우드 이용 계약 시 기반보호법 책임(취약점 분석평가 수행, 보호대책 이행점검 수검 등) 이행 가능 및 감독권한 확보 등

- 기반시설 관리기관은 관계 중앙행정기관(소관 부처)과 검토하여 기반시설의 클라우드 이용에 관한 종합적인 판단 및 결정을 하여야 함.

4 클라우드 서비스 이용

□ 클라우드 서비스 이용 방법

o **(이용 계획 수립 및 제출)** 기반시설 관리기관은 클라우드를 이용하고자 하는 경우 클라우드 이용계획서를 작성하여 90일 이전에 중앙행정기관(소관부처)에 보고하여야 함.

※ **클라우드 이용계획서** : 이용하고자 하는 클라우드 사업자 정보, 기반시설 장비 현황, 기반시설의 중요도, 이용 필요성, 전환일정 등이 포함 (붙임 1 참조)

o **(이용 계획 검토 및 통보)** 클라우드 이용계획서를 받은 관계 중앙행정기관(소관부처)는 해당 기반시설의 중요성, 필요성 등을 검토하여 클라우드 이용가능 여부를 관리기관에게 통보하여야 함.

※ 중앙행정기관은 소관 기반시설의 클라우드 이용 검토결과 및 현황을 「주요정보통신기반시설보호계획」반영하여 정보통신기반보호위원회 보고하여야 함

o **(이용 계약)** 이용가능 통보를 받은 기반시설 관리기관은 클라우드 사업자과 이용 계약을 체결 후 기존 기반시설을 클라우드로 전환

□ 클라우드 서비스 이용 시 보호조치

o **(취약점 분석·평가)** 기반시설이 클라우드로 전환되는 경우, 「정보통신기반보호법」 제9조 2항의 2에 따라 주요정보통신기반시설의 중대한 변화로 판단하고,

- **중앙행정기관(소관부처)은 관리기관에게 기반시설의 취약점 분석·평가를 하도록 명령**하고 관리기관은 취약점 분석·평가를 수행하여 **차년도 「주요정보통신기반시설보호대책」에 반영**하여야 함.

> **제9조(취약점의 분석·평가)**
> ① 관리기관의 장은 대통령령으로 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석·평가하여야 한다.
> ② 중앙행정기관의 장은 다음 각 호의 어느 하나에 해당하는 경우 해당 관리기관의 장에게 주요정보통신기반시설의 취약점을 분석·평가하도록 명령할 수 있다.
> 1. 새로운 형태의 전자적 침해행위로부터 주요정보통신기반시설을 보호하기 위하여 필요한 경우
> 2. 주요정보통신기반시설에 중대한 변화가 발생하여 별도의 취약점 분석·평가가 필요한 경우

o **(추진과제 수립)** 클라우드 서비스를 이용하는 경우 「주요정보통신기반시설보호대책」에 **추진과제로 클라우드 이용에 따른 계약→운영→종료 단계에서의 보호대책**을 마련하여야 함.

- **(계약단계)** 기반시설 관리기관은 클라우드 사업자와 이용 계약체결 시 아래 사항 고려하여 계약하고, 추가 요구사항*은 각 기반시설에 특성에 맞게 관리기관과 중앙행정기관(소관부처)이 판단하여 추가

* 위수탁 관련 사항, 데이터 소유권, 출구 전략, 책임소재, 정보보호 및 서비스 연속성 확보 등 요구사항, 관련 법률 준수 등에 관한 사항 등

기반시설 관리기관 ↔ 클라우드 서비스 제공자 간 클라우드 이용 계약 시 권장사항
① **(물리적 위치)** 클라우드서비스를 이용하는 업무, 처리되는 데이터, 데이터가 처리되는 물리적 위치(시·군 단위까지 기재하고, 소관부처 및 관리기관 요청 시 세부 위치 별도 제출) 명시 및 위치 이동 시 협의사항

⇒ **(참고)** 주요정보통신기반시설은 국가·사회적으로 중요시설로 기반시설이 클라우드 이용 시 기반시설 데이터 및 데이터를 처리하는 시스템은 국내에 위치하여함.

② **(장애 및 침해사고 통지)** 이용하는 클라우드 서비스의 장애 및 침해사고 인지 시 이용자(관리기관) 통지 의무 및 해당 법 준수의무에 관한 사항

⇒ **(참고)** 클라우드서비스 제공자는「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」제25조에 따라 서비스 장애 및 침해사고 시 이용자에게 통지의무를 가지며, 주요정보통신기반시설은「정보통신기반 보호법」제13조, 시행령 제21조에 의해 기반시설의 침해사고 시 관계기관에 통지의무를 가지고 있기 때문에 계약 시 통지 의무 및 해당법 준수 의무에 관한 사항을 명시하여야 함.

③ **(감독 수용)** 서비스 장애 및 침해사고 시 정부 감독 또는 내, 외부 감사인의 조사.접근(현장방문 포함) 수용 의무

⇒ **(참고)**「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」제30조,「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제48조의4에 의해 법위반 사실 및 침해사고 원인 분석 등을 위해 클라우드 사업자에 출입하여 조사 할 수 있음. 이에 기반시설 관리기관은 클라우드 사업자에게 사전에 외부조사에 수용 의무를 계약서에 명시하여야 함.

④ **(훈련·평가 등 협조)** 비상대응훈련(침해사고, 재해복구 등), 취약점 분석·평가(결과보고서 제출, 조치요청 등) 등의 협조에 관한 사항

※ 가이드 內 클라우드 이용 시 취약점 분석·평가 방법을 참고하고 책임을 구체적으로 명시

⇒ **(참고)** 주요정보통신기반시설은「정보통신기반 보호법」시행령 제8조에 의해 매년 주요정보통신기반시설보호대책을 수립·제출하고, 제17조에 의해 매년 또는 중대한 변화 시 취약점 분석·평가를 수행하여야 함. 클라우드 특성 상 침해사고 및 재해복구, 취약점 분석·평가 시 클라우드 서비스 제공자의 협조가 필요.

- **(이용 단계)** 위탁한 기반시설에 해당하는 가상환경에 대하여 주기적으로 취약점 점검, 보안 모니터링 실시 등 보호대책 마련

※ KISA 클라우드 정보보호 안내서를 참조하여 기반시설 관리기관에 맞는 보호체계 마련

- **(종료 단계)** 클라우드 내 기반시설 관련 데이터의 반환(이전) 확인 및 복구 불가능한 방법으로 파기함 됨을 확인

※ 데이터 파기 확인에 관한 사항은 클라우드 서비스 특성을 고려하여 기반시설 관리기관이 확인 방안(파기 확인서 등)을 마련

o **(보호대책 이행절차)** 클라우드 서비스 이용 시 관리기관의 주요정보통신기반시설의 **보호대책 이행 절차는 기존 절차와 동일**함.

- 단, 「주요정보통신기반시설보호대책」 수립 시 클라우드 서비스 부분(클라우드 서비스 제공자의 취약점 분석·평가 결과) 추가, 클라우드 이용 시 보호대책을 추진과제로 도출 등 작성내용 일부 변경

< 주요정보통신기반시설 보호대책 이행절차>

보호계획·대책 수립지침 배포 (과기부·국정원 → 중앙행정기관)	과기정통부와 국정원은 중앙행정기관이 수립해야 하는 보호계획의 수립지침을 개발·배포(매년 5.31)
보호대책 수립지침 배포 (중앙행정기관 → 관리기관)	중앙행정기관은 보호계획 수립지침을 기반으로 소관 관리기관이 수립해야 하는 보호대책 수립지침을 개발·배포
취약점 분석·평가 실시 (관리기관)	관리기관은 보호·관리하는 기반시설에 대하여 취약점 분석·평가를 실시
보호대책 수립·제출 (관리기관 → 중앙행정기관)	관리기관은 취약점에 대한 조치계획 등을 반영한 보호대책을 수립하여 중앙행정기관에 제출(매년 8.31)
보호계획 수립·제출 (중앙행정기관 → 기반보호위원회)	중앙행정기관은 보호대책을 종합·조정하여 보호계획을 수립, 정보통신기반보호위원회(국무조정실)에 제출(매년 10.31)
보호계획 심의 (실무위원회·기반보호위원회	공공·민간 실무위원회와 정보통신기반보호위원회를 통해 각 중앙행정기관의 보호계획을 심의·확정
보호대책·보호계획 이행 (중앙행정기관, 관리기관)	각 중앙행정기관과 관리기관은 각각 수립한 다음 연도 보호계획 및 보호대책을 이행

□ 클라우드 서비스 이용 시 취약점 분석 · 평가 방법

o **(취약점 분석·평가 기준)** 기존 주요정보통신기반시설 취약점 분석·평가 기준 고시 내용을 준용하고, **클라우드 서비스와 관련된 기준(하이퍼바이저, 가상화 플랫폼, 도커 등)은 추가**(붙임 2 참조)

o **(취약점 분석·평가 주체)** 기반시설이 클라우드를 이용하는 경우, 제공받는 **서비스 범위에 따라 관리기관과 제공자가 구분하여 취약점 분석·평가를 수행**하여야 하나, **취약점 분석·평가 결과에 대한 관리·책임은 기반시설 관리기관**에 있음.

- **(기반시설 관리기관)** 이용하는 가상머신 위에 구성된 시스템(서버, PC, DBMS, 웹 등)은 기존 기반시설 취약점 분석·평가와 동일하게 관리기관에서 수행

※ 일부 클라우드 서비스 제공자의 협조가 필요해 조치 기간이 걸리는 취약점에 대해서는 보호대책에 일정 및 사유를 명시하고, 조치를 위해 노력하여야 함

- **(클라우드 서비스 제공자)** 제공하는 물리적·논리적 장비(보안장비, 네트워크 장비, DBMS 등)나, 클라우드 서비스 구성 시 중요 구성요소(하이퍼바이저, 가상화 플랫폼, 도커 등)에 대해서는 클라우드 서비스 제공자가 취약점 분석·평가 수행 후 결과를 관리기관에 제공(붙임 2 참조)

※ 이용자가 운영·관리하는 가상머신에 대한 취약점에 대해서도 클라우드 서비스 제공자의 조치가 필요한 경우 적극 협조하여야 함.

※ 제공자는 해당 물리적·논리적 장비에 대해 매년 「정보통신기반 보호법」 제9조(취약점의 분석·평가) 제4항에 해당하는 기관에게 취약점 분석·평가를 받고 해당 결과를 클라우드 이용하는 기반시설 관리기관들에게 공통으로 제공 가능함.

제9조(취약점의 분석·평가)

④ 관리기관의 장은 제1항 또는 제2항에 따라 취약점을 분석·평가하고자 하는 경우에는 다음 각호의 1에 해당하는 기관으로 하여금 소관 주요정보통신기반시설의 취약점을 분석·평가하게 할 수 있다. 다만, 이 경우 제3항에 따른 전담반을 구성하지 아니할 수 있다.

1. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조의 규정에 의한 한국인터넷진흥원(이하 "인터넷진흥원"이라 한다)
2. 제16조의 규정에 의한 정보공유·분석센터(대통령령이 정하는 기준을 충족하는 정보공유·분석센터에 한한다)
3. 「정보보호산업의 진흥에 관한 법률」 제23조에 따라 지정된 정보보호 전문서비스 기업
4. 「정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조의 규정에 의한 한국전자통신연구원

붙임1. 클라우드 이용계획서

클라우드 서비스 이용계획서

기반시설 관리기관	관리기관명			이용예정일	0000년 00월 00일	
	담당자	성명		부서명		
		연락처		이메일		
	기반시설명	장비현황				
		PC·서버	네트워크 장비	보안장비	기타	계
	000	00개	00개	00개	00개	00개
	기반시설 중요도	※ 신규지정평가 기준 가이드라인을 참고하여 작성				
	클라우드 이용 필요성 (간략히)					
클라우드 서비스	서비스명		서비스 구분	IaaS[ ], PaaS[ ], SaaS[ ]		
	보안인증현황					

2020년 월 일

신 청 인 : (인)

*신청인 제출 서류 : 개인정보 수집·이용 동의서 1부

개인정보 수집 · 이용 동의서

일자 2020년 월 일

관리기관명			
소속 부서			
직 위		성 명	(서명)
연락처	(유선☎) (메일주소)		

<개인정보 수집 · 이용 고지사항>

o 개인정보 수집·이용 목적 : 클라우드 서비스 이용 계획 확인을 위한 수집

o 수집하는 개인정보 항목 : 관기기관명, 소속부서, 직위, 성명, 서명, 연락처(유선 연락처 및 메일주소)

o 보유 및 이용기간 : 담당 업무 미수행 통지 시 또는 1년(공공기록물관리법시행령 제26조①항)

o 개인정보의 수집·이용을 거부할 수 있으며, 다만, 이 경우 클라우드 서비스 이용 신청시 제한될 수 있음을 알려드립니다.

※ 본 동의서는 개인정보보호법 제15조 ②항에 근거하여 작성되었음

▷ **개인정보 수집 · 이용 동의여부** 동의 □ 동의안함 □

붙임2. 클라우드 취약점 분석·평가 기준(클라우드 서비스 제공자 용)

클라우드 서비스 제공자는 매년 취약점 분석·평가를 수행하고 수행한 결과를 이용자(기반시설 관리기관)에 제공하여야 함

※ 상 : 필수점검 항목, 중, 하 : 선택점검 항목

■ 하이퍼바이저

본 가이드의 하이퍼바이저 관련 취약점 분석·평가 기준은 외부에 공개되고 널리 사용되는 하이퍼바이저 4종(XenServer, VMware vSphere ESXi, KVM, Hyper-V)에 대해 작성되었습니다. 그 외 하이퍼바이저를 이용하는 경우 계정 설정, 접근 제어, 보안 설정, 패치 및 로그 등 아래 기준에 준하는 취약점 분석·평가 결과를 제공하면 됩니다.

1. XenServer 점검 항목

점검분류	항목번호	항목명	항목 중요도
계정 설정	XE-01	일반계정 root 권한 관리	상
	XE-02	사용자 및 그룹 파일 권한 관리	상
	XE-03	계정 잠금 임계값 설정	상
	XE-04	패스워드 사용 규칙 설정	상
	XE-05	su 명령어 사용 제한	하
파일 시스템	XE-06	xsconsole 파일 권한 설정	상
	XE-07	/etc/profile 파일 권한 설정	상
	XE-08	/etc/hosts 파일 권한 설정	상
	XE-09	/etc/service 파일 권한 설정	상
	XE-10	VHD 파일에 대한 umask 구성	중
	XE-11	PATH 환경변수 설정	중
	XE-12	사용자 UMASK 설정	하
	XE-13	사용자 홈 디렉터리 및 파일 관리	하
	XE-14	Crontab 파일 권한 설정 및 관리	하
네트워크 설정	XE-15	root 계정의 ssh 및 sftp 접근 제한	상
	XE-16	불필요한 서비스 제거	상
	XE-17	서비스 Banner 관리	중
	XE-18	XAPI에 대한 암호화되지 않은 연결 제한	중
	XE-19	VM 네트워크 카드에서 promiscuous 모드 비활성화	중
	XE-20	session timeout 설정	하
패치 및 로그	XE-21	로그 설정	상
	XE-22	최신 보안패치 및 벤더 권고사항 적용	상
	XE-23	로그 파일 권한 설정	중

2. VMware vSphere ESXi 점검 항목

점검분류	항목번호	항목명	항목 중요도
계정 설정	ES-01	관리자 계정을 root 이외의 계정으로 설정	상
	ES-02	비밀번호 복잡도 설정	상
	ES-03	비밀번호 변경 시 이전 비밀번호 사용 제한	상
접근 제어	ES-04	유효하지 않은 로그인 시도 제한	상
	ES-05	root 계정 ssh 접속 제한	상
	ES-06	접속 IP 제한 설정	상
	ES-07	방화벽 기본 정책 '차단'으로 설정	상
보안 설정	ES-08	가상 스위치 위조 전송 거부 설정	상
	ES-09	가상 스위치 MAC 주소 변경 거부 설정	상
	ES-10	가상 스위치 Promiscuous 모드 거부 설정	상
	ES-11	Managed Object Browser(MOB) 비활성화	상
	ES-12	SNMP Community String 복잡성 설정	중
	ES-13	ESXi Shell 세션 타임아웃 설정	중
	ES-14	Direct 콘솔 UI 세션 타임아웃 설정	중
	ES-15	웹 콘솔 세션 타임아웃 설정	중
	ES-16	NTP 시간 동기화	중
패치 및 로그	ES-17	ESXi 호스트에 대한 원격 로깅 서버 설정	상
	ES-18	감사 기록 설정	상
	ES-19	로컬에 저장되는 로그 영구 저장	상
	ES-20	최신 보안패치 및 벤더 권고사항 적용	상

3. KVM 점검 항목

점검분류	항목번호	항목명	항목 중요도
보안 설정	KVM-01	SELinux 활성화	상
	KVM-02	VM 이미지 디렉터리 강화된 보안 정책 적용	상
	KVM-03	권한 없는 사용자 VM 생성 제한	상
	KVM-04	virt samba 비활성화	상
	KVM-05	VNC 포트 접속 IP 제한	상
	KVM-06	불필요한 응용프로그램 실행 금지	중
	KVM-07	NTP 시간 동기화	중
패치 및 로그	KVM-08	최신 보안패치 및 벤더 권고사항 적용	상
	KVM-09	libvirt 감사 활성화	상

※ KVM의 경우, Linux 서버에서 동작하기 때문에 주요정보통신기반시설 취약점 분석·평가 기준 중 Unix 서버 취약점 분석·평가 항목의 상(필수), 중/하(선택) 항목에 대해서도 취약점 분석·평가 결과를 같이 제공

4. Hyper-V 점검 항목

점검분류	항목번호	항목명	항목 중요도
보안 설정	HV-01	hypver-v 관리자 전용 계정 사용	상
	HV-02	접속 IP 제한 설정	상
	HV-03	WMI 원격 실행 제한	상
	HV-04	가상 컴퓨터 기본 경로 변경	중
	HV-05	가상 하드디스크 기본 경로 변경	중
가상 머신 보호	HV-06	가상 OS MAC Address 스푸핑 제한	상
	HV-07	가상 OS DHCP 가드 사용	중
	HV-08	가상 OS 라우터 알람 가드 사용	중
패치 관리	HV-09	최신 보안패치 및 벤더 권고사항 적용	상

※ Hyper-V의 경우, 윈도우즈 서버에서 동작하기 때문에 주요정보통신기반시설 취약점 분석·평가 기준 중 윈도우즈 서버 취약점 분석·평가 항목의 상(필수), 중/하(선택) 항목에 대해서도 취약점 분석·평가 결과를 같이 제공

■ 클라우드 플랫폼

본 가이드의 클라우드 플랫폼 관련 취약점 분석·평가 기준은 외부에 공개되고 널리 사용되는 오픈스택(OpenStack)에 대해 작성되었습니다. 오픈스택 점검 항목은 서비스 별로 구분하여 작성되었으며, 해당 서비스를 이용하지 않을 경우 해당없음(N/A) 처리하여 취약점 분석·평가 수행하시면 됩니다.

1. 오픈스택(OpenStack) 점검 항목

점검분류	항목번호	항목명	항목 중요도
Identity 서비스	OT-01	keystone 설정 파일들의 소유권 설정	상
	OT-02	keystone 설정 파일들의 접근 권한 설정	상
	OT-03	HTTP 서버에서 TLS 활성화	상
	OT-04	admin 토큰 비활성화	상
	OT-05	keystone의 요청 본문 최대 크기 설정	중
Dashboard 서비스	OT-06	horizon 설정 파일의 소유권 설정	상
	OT-07	horizon 설정 파일의 접근 권한 설정	상
	OT-08	Cross-Frame Scripting 방지	상
	OT-09	Cross Site Request Forger 방지	상
	OT-10	세션 쿠키 평문 전송 방지	상
	OT-11	세션 ID 도용 방지 설정	상
	OT-12	암호 자동 입력 방지	상
	OT-13	로그인 없이 비밀번호 변경 방지	상
	OT-14	https redirection 설정	상
	OT-15	비밀번호 재사용 금지 설정	중
Compute 서비스	OT-16	nova 설정 파일들의 소유권 설정	상
	OT-17	nova 설정 파일들의 접근 권한 설정	상
	OT-18	nova 인증시 keystone 사용	상
	OT-19	nova 인증시 암호화 프로토콜 적용	상
	OT-20	nova와 glance 통신시 TLS 사용	상

Block Storage 서비스	OT-21	cinder 설정 파일들의 소유권 설정	상
	OT-22	cinder 설정 파일들의 접근 권한 설정	상
	OT-23	cinder 인증시 keystone 사용	상
	OT-24	cinder와 nova 통신시 TLS 사용	상
	OT-25	cinder와 glance 통신시 TLS 사용	상
	OT-26	안전한 NAS 운영 환경 설정	중
	OT-27	cinder의 요청 본문 최대 크기 설정	중
Image Storage 서비스	OT-28	glance 설정 파일들의 소유권 설정	상
	OT-29	glance 설정 파일들의 접근 권한 설정	상
	OT-30	glance 인증시 Keystone 사용	상
	OT-31	glance 인증시 TLS 사용	상
Shared File Systems 서비스	OT-32	manila 설정 파일들의 소유권 설정	상
	OT-33	manila 설정 파일들의 접근 권한 설정	상
	OT-34	manila 인증시 keystone 사용	상
	OT-35	manila 인증시 TLS 사용	상
	OT-36	manila와 nova 통신시 TLS 사용	상
	OT-37	manila와 neutron 통신시 TLS 사용	상
	OT-38	manila와 cinder 통신시 TLS 사용	상
	OT-39	manila의 요청 본문 최대 크기 설정	중
Networking 서비스	OT-40	neutron 설정 파일들의 소유권 설정	상
	OT-41	neutron 설정 파일들의 접근 권한 설정	상
	OT-42	neutron 인증시 keystone 사용	상
	OT-43	neutron 인증시 TLS 사용	상
	OT-44	ARP Spoofing 완화	상
패치 및 로그	OT-45	최신 보안패치 및 벤더 권고사항 적용	상
	OT-46	로그 기록 설정	상

■ 컨테이너

본 가이드의 컨테이너 관련 취약점 분석·평가 기준은 컨테이너 기술에 많이 활용되는 도커(Docker)에 대해 작성되었습니다. 컨테이너 기술을 통해 이용자에게 제공하는 경우에만 취약점 분석·평가를 수행하시면 됩니다.

1. 도커(Docker)

점검분류	항목번호	항목명	항목 중요도
호스트 보안	DO-01	최신 보안패치 및 벤더 권고사항 적용	상
	DO-02	감사 설정	상
	DO-03	도커 그룹에 불필요한 사용자 제거	중
도커 데몬 설정	DO-04	추가 권한 획득으로부터 컨테이너 제한	상
	DO-05	legacy registry v1 비활성화	하
설정 파일 접근 권한	DO-06	docker.service 파일 소유권 설정	상
	DO-07	docker.service 파일 접근 권한 설정	상
	DO-08	docker.socket 파일 소유권 설정	상
	DO-09	docker.socket 파일 접근 권한 설정	상
	DO-10	/etc/docker 디렉터리 소유권 설정	상
	DO-11	/etc/docker 디렉터리 접근 권한 설정	상
	DO-12	/var/run/docker.sock 파일 소유권 설정	상
	DO-13	/var/run/docker.sock 접근 권한 설정	상
	DO-14	daemon.json 파일 소유권 설정	상
	DO-15	daemon.json 파일 접근권한 설정	상
	DO-16	/etc/default/docker 파일 소유권 설정	상
	DO-17	/etc/default/docker 파일 접근 권한 설정	상
컨테이너 이미지 빌드 파일	DO-18	root가 아닌 user로 컨테이너 실행	상
	DO-19	도커를 위한 컨텐츠 신뢰성 활성화	중
컨테이너 런타임	DO-20	컨테이너 SELinux 보안 옵션 설정	상
	DO-21	컨테이너에서 ssh 사용 제한	상
	DO-22	PIDs cgoup 제한	상
	DO-23	기본 브리지 docker0 사용 제한	상
	DO-24	호스트의 user namespaces 공유 제한	하