2023. 2.

본인확인업무와 다른 인터넷서비스와의 분리 심사기준 안내서

방송통신위원회
Korea Communications Commission

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

2023. 2.

본인확인업무와 다른 인터넷서비스와의 분리 심사기준 안내서

방송통신위원회
Korea Communications Commission

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

CONTENTS

표목차

그림목차

본인확인업무와
다른 인터넷서비스와의 분리
심사기준 안내서

I

개요

1. 작성 목적
2. 정보시스템 분리 목적

Ⅰ 개요

1 작성 목적

- 본서는 본인확인기관 및 본인확인기관 지정 신청기관을 대상으로 다음의 사항을 안내하기 위하여 작성됨
  - 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 정보통신망법)」제23조의3제1항 및 영 제9조의3에 따른 「본인확인기관 지정 등에 관한 기준」[별표 3] 제1장 9-2에서 요구하는 본인확인업무와 다른 인터넷 서비스와의 정보시스템 분리 목적에 대하여 안내함
  - 법률에서 정한 '본인확인업무'의 정의에 따라 본인확인업무 및 본인확인업무를 처리하는 정보시스템을 분류하고, 본인확인업무와 다른 인터넷 서비스와의 정보시스템 분리 대상에 대하여 안내함
  - 본인확인업무와 다른 인터넷 서비스와의 정보시스템 분리 구성 및 운영을 위하여 분리 기준 및 방법에 대하여 안내함

[표 1-1] 본인확인업무 정보시스템 분리 법적 근거

정보통신망법	본문
법률	**제23조의3(본인확인기관의 지정 등)** ① 방송통신위원회는 다음 각 호의 사항을 심사하여 대체수단의 개발·제공·관리 업무(이하 "본인확인업무"라 한다)를 안전하고 신뢰성 있게 수행할 능력이 있다고 인정되는 자를 본인확인기관으로 지정할 수 있다. 1. 본인확인업무의 안전성 확보를 위한 물리적·기술적·관리적 조치계획 2. 본인확인업무의 수행을 위한 기술적·재정적 능력 3. 본인확인업무 관련 설비규모의 적정성

정보통신망법	본문
시행령	**제9조의3(심사사항별 세부 심사기준)** ① 법 제23조의3제1항에 따른 심사사항별 세부 심사기준은 다음 각 호와 같다. 1. 물리적·기술적·관리적 조치계획: 다음 각 목의 사항에 대한 조치계획을 마련할 것 가. 법 제23조의3제1항에 따른 본인확인업무(이하 “본인확인업무”라 한다) 관련 설비의 관리 및 운영에 관한 사항 나. 정보통신망 침해행위의 방지에 관한 사항 다. 시스템 및 네트워크의 운영·보안 및 관리에 관한 사항 라. 이용자 보호 및 불만처리에 관한 사항 마. 긴급상황 및 비상상태의 대응에 관한 사항 바. 본인확인업무를 위한 내부 규정의 수립 및 시행에 관한 사항 사. 법 제23조의2제2항에 따른 대체수단(이하 “대체수단”이라 한다)의 안전성 확보에 관한 사항 아. 접속정보의 위조·변조 방지에 관한 사항 자. 그 밖에 본인확인업무를 위하여 방송통신위원회가 정하여 고시하는 사항 ② 제1항에 따른 심사사항별 세부 심사기준의 평가기준 및 평가방법 등에 관하여 필요한 사항은 방송통신위원회가 정하여 고시한다.
고시	**제7조(심사기준)** ① 지정심사는 본인확인서비스의 안전성과 신뢰성을 보장하기 위한 물리적·기술적·관리적 보호조치와 정보통신설비 관련 시설 및 장비를 대상으로 한다. ② 영 제9조의3제2항에 따른 심사사항별 세부심사기준의 평가기준은 별표 3과 같다. **[별표 3] 심사사항별 세부심사기준의 평가기준** Ⅰ. 물리적·기술적·관리적 조치계획 9. 본인확인업무와 다른 인터넷 서비스와의 분리 9-2. 본인확인서비스 제공을 위한 시스템 및 개인정보 DB를 물리적 또는 논리적으로 다른 서비스와 분리하여 운영하여야 함

2 정보시스템 분리 목적

● 본인확인서비스 안전성 보장

- 본인확인서비스는 대국민 서비스로서 이용자에게 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법(유일성을 보장하는 대체수단)을 제공하고,
- 본인확인입력정보(대체수단 및 이용자가 입력하는 부가정보)를 이용하여 이용자를 안전하게 식별·인증할 수 있도록 보장하여야 함
- 이를 위하여 본인확인업무 관련 내부 규정 및 정보보호 관리체계를 수립하고 본인확인업무와 다른 인터넷 서비스의 정보시스템을 분리·운영하여, 보안 취약점 및 위협으로부터 서로 영향을 미칠 수 있는 위험을 최소화하기 위함

● 본인확인서비스 신뢰성 보장

- 정부 및 각 지방자치단체의 전자정부서비스 활성화와 정보통신서비스 제공자간의 사업 다각화 및 연계 서비스 활성화로 인하여 본인확인서비스에 대한 수요가 증가함에 따라,
- 본인확인서비스를 중단 없이 적시에 안정적으로 제공하여 이용자의 신뢰를 확보하여야 함
- 이를 위하여 본인확인업무 관련 내부 규정을 수립하고 본인확인업무와 다른 인터넷 서비스의 정보시스템을 분리·운영하여, 성능·장애·재해복구 등에서 본인확인서비스의 가용성을 확보하고 운영 전반에 미칠 수 있는 시스템적 영향을 최소화하기 위함

● 본인확인서비스 이용자 개인정보 보호

- 본인확인기관은 본인확인업무를 처리하기 위하여 이용자의 고유식별정보와 연계정보·중복가입확인정보 등 정보주체를 특정하여 식별할 가능성이 높은 개인정보를 수집·보유·이용·제공함에 따라,
- 개인정보가 분실·도난·유출·위조·변조·훼손 또는 오용·남용되지 아니하도록 보호하여야 함
- 이를 위하여 본인확인업무 관련 개인정보보호 규정 및 개인정보보호 관리체계를 수립하고 본인확인업무와 다른 인터넷 서비스의 정보시스템을 분리·운영하여,
- 본인확인기관이 준용하여야 하는 법적 요구사항을 준수하고 본인확인업무에서 처리하는 개인정보를 높은 수준으로 관리하여 개인정보 유출 방지 및 피해를 최소화하기 위함

참고사항

본인확인서비스의 전체 또는 일부가 다른 법률에 함께 근거하는 경우,

- 「본인확인기관 지정 등에 관한 기준」 [별표 3] 제1장 9-2에서 요구하는 본인확인서비스와 다른 서비스와의 정보시스템 분리 목적을 기준으로 판단하여,
- 다른 법률의 물리적·기술적·관리적 보안요구사항이 더 높은 경우에는 그 기준을 준용하여 정보시스템을 구성 및 운영할 수 있음

본인확인업무와
다른 인터넷서비스와의 분리
심사기준 안내서

Ⅱ

정보시스템 분리 대상

1. 본인확인업무 정의 및 분류
2. 정보시스템 정의 및 분류
3. 정보시스템 분리 대상

Ⅱ 정보시스템 분리 대상

1 본인확인업무 정의 및 분류

● 본인확인업무 정의

– 본인확인업무는「정보통신망법」제23조의3제1항과 영 제9조의3 및「본인확인기관 지정 등에 관한 기준」제12조의2에서 다음과 같이 정의되어 있음

1. 대체수단을 제공하기 위해 이용자 신원의 진위여부를 확인하는 업무
2. 연계정보 등 본인확인결과정보 제공 및 관리 업무
3. 그 밖에 대체수단의 개발·제공·관리 등에 관한 업무

[표 2-1] 본인확인업무 정의 법적 근거

정보통신망법	본문
법률	**제23조의3(본인확인기관의 지정 등)** ① 방송통신위원회는 다음 각 호의 사항을 심사하여 대체수단의 개발·제공·관리 업무(이하 "본인확인업무"라 한다)를 안전하고 신뢰성 있게 수행할 능력이 있다고 인정되는 자를 본인확인기관으로 지정할 수 있다. 1. 본인확인업무의 안전성 확보를 위한 물리적·기술적·관리적 조치계획 2. 본인확인업무의 수행을 위한 기술적·재정적 능력 3. 본인확인업무 관련 설비규모의 적정성
시행령	**제9조의3(심사사항별 세부 심사기준)** ① 법 제23조의3제1항에 따른 심사사항별 세부 심사기준은 다음 각 호와 같다. 1. 물리적·기술적·관리적 조치계획: 다음 각 목의 사항에 대한 조치계획을 마련할 것

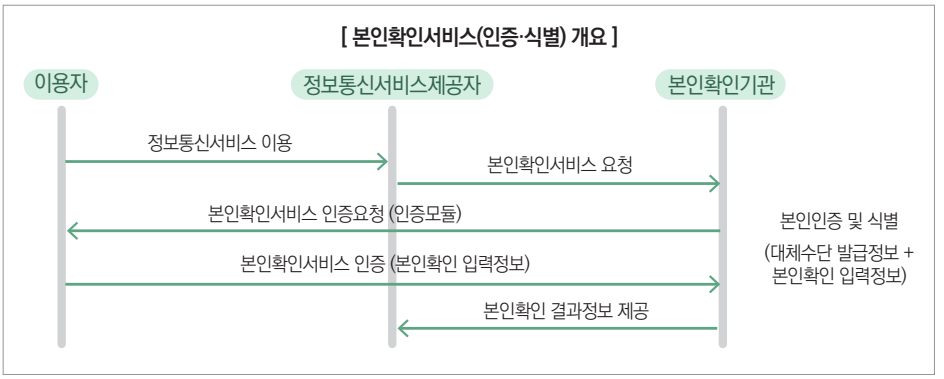
정보통신망법	본문
시행령	가. 법 제23조의3제1항에 따른 본인확인업무(이하 “본인확인업무”라 한다) 관련 설비의 관리 및 운영에 관한 사항 나. 정보통신망 침해행위의 방지에 관한 사항 다. 시스템 및 네트워크의 운영·보안 및 관리에 관한 사항 라. 이용자 보호 및 불만처리에 관한 사항 마. 긴급상황 및 비상상태의 대응에 관한 사항 바. 본인확인업무를 위한 내부 규정의 수립 및 시행에 관한 사항 사. 법 제23조의2제2항에 따른 대체수단(이하 “대체수단”이라 한다)의 안전성 확보에 관한 사항 아. 접속정보의 위조 · 변조 방지에 관한 사항 자. 그 밖에 본인확인업무를 위하여 방송통신위원회가 정하여 고시하는 사항
고시	**제12조의2(본인확인업무)** ① 법 제23조의3제1항에 따라 지정된 본인확인기관은 다음 각 호의 본인확인업무를 수행할 수 있다. 1. 대체수단을 제공하기 위해 이용자 신원의 진위여부를 확인하는 업무 2. 연계정보 등 본인확인결과정보 제공 및 관리 업무 3. 그 밖에 대체수단의 개발·제공·관리 등에 관한 업무

● 본인확인업무 분류

- 본인확인업무 정의에 따라 본인확인업무를 대체수단 및 본인확인서비스의 개발·제공·관리 관점에서 세부적으로 분류함

[표 2-2] 본인확인업무 분류

업무	세부 내용
대체수단 발급	- 대체수단을 발급하려는 이용자의 본인확인 및 신원확인 - 대체수단 관련 정보를 생명주기(신청, 등록, 생성, 발급, 변경·관리, 저장·백업, 폐기)에 따라 처리 ※ 본인확인기관이 모든 업무를 자체적으로 하거나 일부 업무를 등록대행기관을 통해 대면 또는 비대면으로 처리

업무	세부 내용
본인확인 서비스 (인증·식별)	– 본인확인서비스 이용기관(정보통신서비스 제공자)의 요청에 따른 본인확인서비스의 직접 또는 대외기관(인증 대행기관 등) 연계를 통한 제공 – 연계정보 및 중복가입확인정보 등 본인확인결과정보 생성·제공 – 다른 본인확인기관과의 연계를 통한 본인확인서비스 제공 
본인확인 서비스 (개발·운영)	– 본인확인서비스 관련 소스코드 및 실행코드 개발·관리 – 본인확인서비스 이용기관(정보통신서비스 제공자) 정보 등록·관리 – 본인확인 인증 대행(또는 중계)기관 정보 등록·관리 – 대체수단의 부정사용 모니터링 시스템(FDS) 관리 – 대체수단 및 본인확인서비스 이용자에 대한 허무인 정보 관리 – 본인확인서비스 이용자의 본인확인서비스 신청·해지 이력 관리 – 본인확인서비스 이용자의 본인확인 인증 이력 관리 – 본인확인서비스 전체 흐름상의 처리 로그(전문연동 로그, 트랜잭션 로그 등) 관리
민원 관리	– 본인확인서비스 이용자 불만 및 상담 처리 – 법원·수사기관 등 본인확인서비스 관련 요청정보 처리
개인정보 관리	– 본인확인서비스 이용자의 개인정보를 생명주기(수집, 보유, 이용, 제공, 파기)에 따라 처리

2 정보시스템 정의 및 분류

● 본인확인업무 처리 정보시스템 정의

- 「본인확인기관 지정 등에 관한 기준」[별표 3]의 요구사항을 준수하기 위한 정보시스템 범위는 대체수단의 종류 및 본인확인기관의 정보시스템 구성 방식 등에 따라 가변적임
- 본서에서는 작성 목적에 따라 본인확인업무를 처리하는 정보시스템 범위를 [표 2-3]과 같이 정의함

[표 2-3] 본인확인업무 처리 정보시스템 정의

구분	세부 내용
구성 환경	- 운영 환경, 개발·테스트 환경, 재해복구(이하 DR) 환경
정보시스템	- 서버, 미들웨어, 데이터베이스(이하 DB), 애플리케이션(웹·앱) - 네트워크 장비, 보안시스템, 스토리지

● 본인확인업무 처리 정보시스템 분류

- [표 2-2] 본인확인업무 분류표에서 식별된 본인확인업무별 처리 흐름을 세분화하여 처리 단계별로 본인확인업무 전용 정보시스템과 전사 공용 정보시스템으로 구분함

[표 2-4] 본인확인업무 처리 정보시스템 분류

구분	세부 내용
본인확인업무 전용 정보시스템	1. 대체수단 발급 정보 및 이용자 정보 관리 정보시스템 2. 대체수단 발급 정보 및 본인확인입력정보를 통한 이용자 인증·식별 처리 정보시스템 3. 본인확인결과정보 생성 및 본인확인 인증 이력 관리 정보시스템
전사 공용 정보시스템	1. 이용자 채널 정보시스템 - 전사 공용 이용자 웹·앱(대표 홈페이지, 어플리케이션 등)에서 본인확인서비스 처리 등 2. 이용자 본인확인 및 신원확인 정보시스템 - 대체수단 발급을 위한 이용자 본인확인(아이핀·휴대폰·인증서·신용카드), 계좌인증, 신분증 진위확인, 영상통화 처리 등

구분	세부 내용
전사 공용 정보시스템	3. 대내·외 업무 연계 정보시스템 – 본인확인업무 전용 정보시스템과 연계하여 본인확인서비스를 처리하는 API, MCI, MCA, EAI, FEP 등 4. 본인확인서비스 전체 흐름상의 처리 로그(전문연동 로그, 트랜잭션 로그 등) 관리 정보시스템 5. 본인확인서비스 민원(이용자, 사법기관 등) 관리 정보시스템

3 정보시스템 분리 대상

● 본인확인업무와 다른 인터넷 서비스와의 정보시스템 분리 대상

- 본인확인업무와 다른 인터넷 서비스 간 분리하여야 하는 정보시스템은 운영 환경에 구성한 본인확인업무 전용 정보시스템 중 서버, 미들웨어, DB에 해당함
- 본인확인업무 전용 정보시스템이라 할지라도 서버, 미들웨어, DB가 아니거나 다른 환경(개발·테스트, DR)에 구성한 정보시스템은 필수적으로 분리하여야 하는 대상이 아님
- 그 외 본인확인업무를 처리하기는 하나, 전사 공용 정보시스템인 경우에도 필수적으로 분리하여야 하는 대상이 아님
- 필수 분리 대상이 아닌 정보시스템은 본인확인서비스 운영 방침 및 내부 규정, 정보보호 및 개인정보보호 관리체계에 따라 본인확인서비스에 영향을 미치지 않도록 구성하고 관리하여야 함

[표 2-5] 본인확인업무와 다른 인터넷 서비스와의 정보시스템 분리 대상

구분	운영 환경	개발·테스트 및 DR 환경
분리 대상	- 본인확인업무 전용 정보시스템 (서버, 미들웨어, DB에 한함)	- 없음
미분리 대상	- 본인확인업무 전용 정보시스템 (분리 대상 외 정보시스템) - 본인확인업무 처리 전사 공용 정보 시스템	- 본인확인업무 전용 정보시스템 - 본인확인업무 처리 전사 공용 정보시스템

[표 2-6] 본인확인 대체수단별 정보시스템 분리 대상 예시

대체수단	본인확인업무 전용 정보시스템
아이핀	- 일반인증, 간편인증(아이핀앱) WEB/WAS(AP)/DB 등
휴대폰	- 일반인증, 간편인증(PASS앱) WEB/WAS(AP)/DB 등
인증서	- CA, RA, OCSP, Directory WEB/WAS(AP)/DB 등 - 본인확인서버 AP/DB 등 (본인확인결과정보 생성 및 본인확인 인증 이력 관리)
신용카드	- 일반인증, 간편인증(앱카드), 홈페이지인증 WEB/WAS(AP)/DB 등

본인확인업무와
다른 인터넷서비스와의 분리
심사기준 안내서

Ⅲ

정보시스템 분리 기준

1. 분리 기준 및 방법
2. 서버 분리
3. 미들웨어 분리
4. DB 분리

Ⅲ 정보시스템 분리 기준

1 분리 기준 및 방법

- **본인확인업무와 다른 인터넷 서비스와의 정보시스템 분리 기준 및 방법을 서버, 미들웨어, DB로 나누어 안내함**
  - [표 2-4]와 [표 2-5]에 따라 본인확인업무와 다른 인터넷 서비스와의 정보시스템 분리 대상은 운영환경에 위치한 본인확인업무 전용 정보시스템 중 서버, 미들웨어, DB로 한정함
  - [표 2-4]와 [표 2-5]에서 본인확인업무를 처리하는 전사 정보시스템의 경우, 다른 인터넷 서비스와는 분리 대상이 아니나, 본인확인업무 전용 정보시스템과는 다른 인터넷 서비스와 동일하게 분리 기준을 적용해야 함
  - 서버, 미들웨어, DB를 물리적 또는 논리적으로 분리할 수 있으나 '물리적' 또는 '논리적' 분리에 대한 판단 기준이 상이할 수 있어,
  - 정보시스템 분리 목적 및 본인확인서비스에 적용 적합성 등을 종합적으로 고려하여 본인확인서비스 정보시스템 구성 시 참고하여야 하는 분리 기준과 방법에 대하여 안내함

2 서버 분리

- **서버 분리 기준**
  - [표 2-4]와 [표 2-5]에서 정한 본인확인업무와 다른 인터넷 서비스와의 정보시스템 분리 대상에 따라 본인확인업무 전용 정보시스템은 물리적 또는 논리적으로 서버를 분리하여야 함

- 본인확인업무 전용 서버는 ▲물리적 하드웨어에 단일 운영체제를 설치하여 물리적으로 분리하는 방법 ▲서버 가상화 기술과 컨테이너 기술을 적용하여 논리적으로 분리하는 방법으로 구성할 수 있음

● 서버 물리적 분리

- 물리적으로 별도인 하나의 하드웨어에 하나의 운영체제(이하 OS)를 설치하여 단독(Stand-Alone)으로 본인확인업무를 수행하도록 구성하여 운영할 수 있음
- 물리적으로 같은 하드웨어에 하나의 OS에서 본인확인업무 이외의 다른 인터넷 서비스를 함께 운영하는 구성은 적절하지 않음

[그림 3-1] 서버 물리적 분리 구성 예시

● 서버 논리적 분리(서버 가상화)

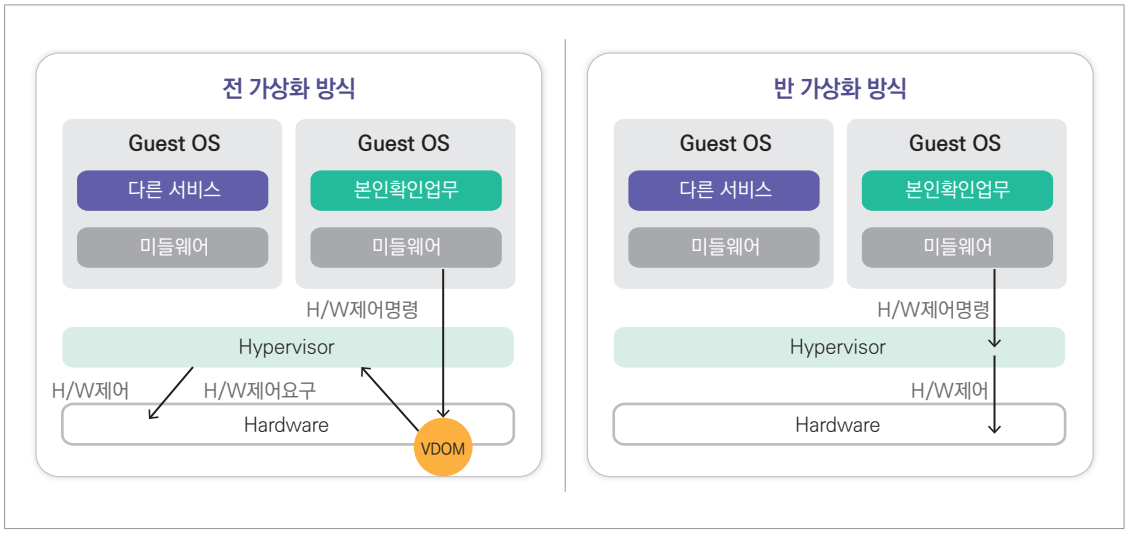
- 하드웨어의 물리적인 자원들을 통합 및 논리적으로 재구성하고 자원을 배분하여 사용하는 가상화 기술 적용을 통한 분리 방식임
- 하나의 물리적 하드웨어를 여러 개의 가상머신(VM)으로 나누어 사용하는 방식과 분산된 2개 이상의 하드웨어를 클러스터링하여 본인확인업무만을 수행하는 통합(Consolidation) 기법 등이 있음
- 서버 가상화 구성 시 전제조건은 본인확인기관이 서버를 직접 구매하여(클라우드 서비스를 통한 하드웨어 임대 등은 불가) 설치·운영 및 유지보수를 수행하여야 함
- 서버 가상화 종류는 Guest OS(VM) 수정 여부 및 하드웨어 가상화 정도에 따라 ▲전 가상화(Full Virtualization) ▲반 가상화(Para Virtualization), 하이퍼바이저의 위치와 역할에 따라 ▲TYPE 1(Bare-Metal) ▲TYPE 2(Hosted) 등으로 구분할 수 있음

[표 3-1] 서버 가상화 종류

구분		세부 내용
가상화 운영 방식에 따른 분류	전 가상화 방식	- 하드웨어 전체를 가상화하는 방식 - Hardware Virtual Machine - 하드웨어를 완전히 가상화하므로 Guest OS 커널 수정 불필요 - 유사 방식인 하드웨어 에뮬레이션 기법도 포함
	반 가상화 방식	- 하드웨어 절반만 가상화하고 나머지 절반은 실제 하드웨어를 사용하는 방식 - 전 가상화의 성능 문제를 개선하기 위한 방식 - 하드웨어 접근 시 별도의 특정 명령(HyperCall)이 사용되기 위하여 반드시 Guest OS 수정 필요
하이퍼바이저 위치 및 역할에 따른 분류	TYPE 1 방식	- Bare Metal형, Native 하이퍼바이저형 - 아무것도 설치되어 있지 않은 하나의 물리적 하드웨어에 하이퍼바이저를 설치하여, 하드웨어 자원을 제어하는 OS 역할과 가상머신을 관리하는 역할을 하이퍼바이저가 모두 담당하는 방식 ※ VMWare ESXi, Citrix-Xen, KVM, MS Hyper-V 등
	TYPE 2 방식	- Hosted 하이퍼바이저형 - 하나의 물리적 하드웨어에 Host OS를 설치하고 그 위에 하이퍼바이저를 설치하여, 하드웨어에 대한 OS 역할은 Host OS가 담당하고 가상머신 관리는 하이퍼바이저가 담당하는 방식 ※ VMworkstation, Oracle-VirtulBox 등

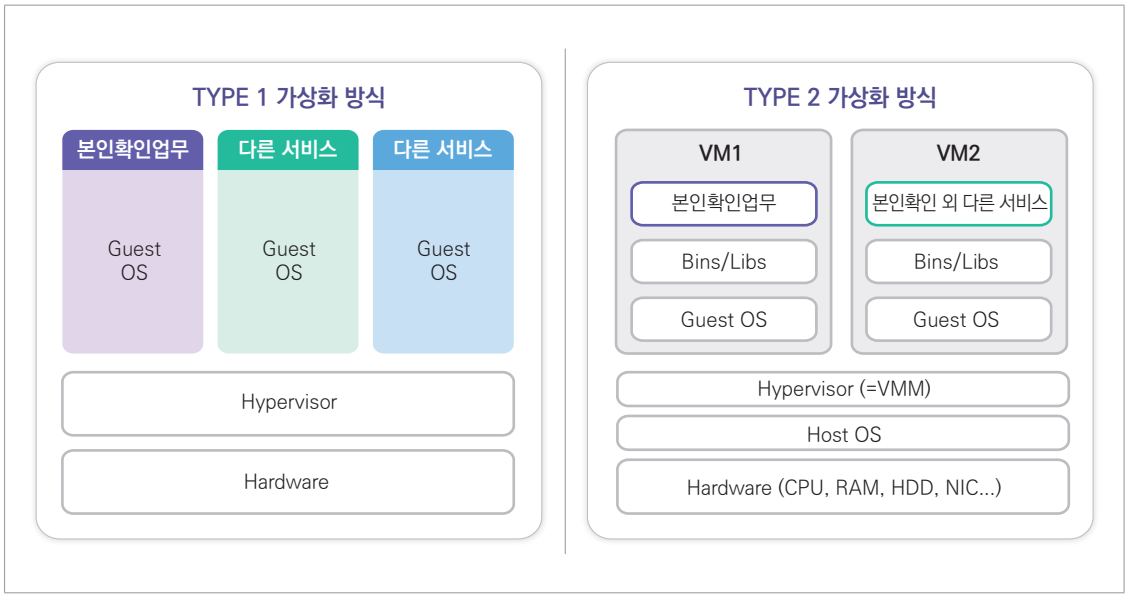
- 전 가상화 및 반 가상화 방식은 별도의 서로 다른 Guest OS가 존재하여 본인확인업무를 위한 자원 할당도 논리적으로 분리됨

[그림 3-2] 서버 논리적 분리 구성 예시(전 가상화, 반 가상화)



- TYPE 1, 2 방식도 별도의 가상머신을 구성하여 서로 다른 Guest OS가 존재하고 자원 할당 역시 논리적으로 분리되며, 특정 가상머신의 문제가 다른 가상머신의 문제로 전이될 가능성이 낮음
- 본인확인업무 전용 서버를 단독 가상머신으로 구성하는 경우에는 TYPE 1, 2 방식 모두 서버 분리 기준에서 논리적 분리 방법으로 적용할 수 있음

[그림 3-3] 서버 논리적 분리 구성 예시(TYPE 1, TYPE 2)



- 서버 논리적 분리(컨테이너 가상화)

  - 컨테이너 런타임 프레임워크(Docker, CRI-O, Containerd, rkt 등)를 통하여 서로 격리된 컨테이너로 본인확인업무를 수행하는 방식임
  - 컨테이너 런타임 프레임워크 위에 컨테이너 오케스트레이션 플랫폼(쿠버네티스, 오픈쉬프트 등)을 적용하여 운영하기도 함
  - Host OS 공유 방식으로서 물리적인 하드웨어에 영향을 받지 않고 설치된 OS에서 프로그램별로 자원을 할당하고 관리함
  - 본인확인업무 전용 컨테이너와 다른 인터넷 서비스 컨테이너는 프로그램 실행환경이 격리되지만 서로 공유하는 OS 환경으로 인하여 영향을 받을 수 있으므로,
  - 복수 개의 본인확인업무 전용 컨테이너 유지 및 자동 TakeOver 정책 적용 등 무중단 서비스를 위한 아키텍처가 수립되어야 함

[그림 3-4] 서버 논리적 분리 구성 예시(컨테이너 가상화)

[표 3-2] 가상머신과 컨테이너 가상화 비교

비교 항목	가상머신(TYPE 1, TYPE 2)	컨테이너
하드웨어 플랫폼	- 물리적인 하드웨어 1대에 다수의 가상머신 존재	- 하드웨어 플랫폼에 영향받지 않음
운영체제	- 물리적인 하드웨어 HOST OS에 다수 가상머신 Guest OS를 설치함	- 하드웨어 플랫폼과 관련 없이 설치된 OS는 1개임
자원 할당	- 하이퍼바이저를 통해 가상머신별로 개별적 자원을 할당함	- OS에서 프로그램별로 자원을 할당하고 관리함
논리적 분리 (격리 수준)	- 가상머신별로 완전하게 격리됨	- 본인확인업무 컨테이너 실행환경은 격리되지만, OS 환경은 서로 공유됨
충돌 및 문제 전이 위험성	- 특정 가상머신의 문제가 다른 가상머신의 문제로 전이 및 확장될 가능성이 매우 적음	- 본인확인업무와 다른 서비스 컨테이너 간에 충돌 및 간섭을 일으키지 않지만, 특정 프로그램이 서로 공유하는 OS에게 문제를 유발하여 시스템 중단 가능성은 존재함

- 컨테이너 가상화 방식 도입 시 필수 고려사항은 다음과 같음

1. 컨테이너 가상화 방식은 현재 존재하는 클라우드 서비스와 매우 유사하며, AWS(아마존 웹 서비스) 등 기존 클라우드 환경과 연계하여 사용하는 것이 일반적이지만, 본인확인업무 전용 서버 구성에 적용할 경우에는 [표 3-3]에 제시한 전제조건을 준수하여야 함
2. 본인확인기관이 서버를 직접 구매하여 MSP(Managed Service Provider) 또는 CSB(Cloud Service Brokerage), CSP(Cloud Service Provider) 등을 통한 대리 운영이 아닌 기관 스스로 컨테이너 가상화에 대한 설치 및 운영, 유지보수를 수행하여야 함

[표 3-3] 컨테이너 및 이미지 생성 전제조건

구분	세부 내용
Public 클라우드 사용 불가	- 어떤 경우에도 Public 클라우드 사용은 불가하며, 컨테이너를 직접 관리하여야 함
본인확인업무 컨테이너 및 이미지 자산 식별	- 본인확인업무 컨테이너·이미지 자산목록을 작성·관리하여야 함 ※ 필수 필드 : 해당 Node, Namespace, Name, Ready, Status, Age, IP주소, 위치 등

구분	세부 내용
외부 레지스트리 사용 불가	- 베이스 이미지 또는 컨테이너 생성 시 외부 인터넷으로 접속 후 Docker Hub 사용은 불가함
최소한의 베이스 이미지 사용	- 운영체제가 포함된 이미지 등은 알 수 없는 취약점이 존재할 수 있으므로, 이미지 스캐너 등을 통한 안전성 확인 절차를 마련하여야 함
최신 상태의 이미지 확인	- 구성요소 버전 확인 업데이트 등을 통해 최신 상태를 확인하여야 함

3 미들웨어 분리

- 미들웨어 분리 기준
  - [표 2-4]와 [표 2-5]에서 정한 본인확인업무와 다른 인터넷 서비스와의 정보시스템 분리 대상에 따라 본인확인업무 전용 정보시스템은 물리적으로 미들웨어를 분리하여야 함
  - 미들웨어 종류는 [표 3-4]와 같이 분류할 수 있으며, 본서에서 미들웨어는 범용 미들웨어를 의미함

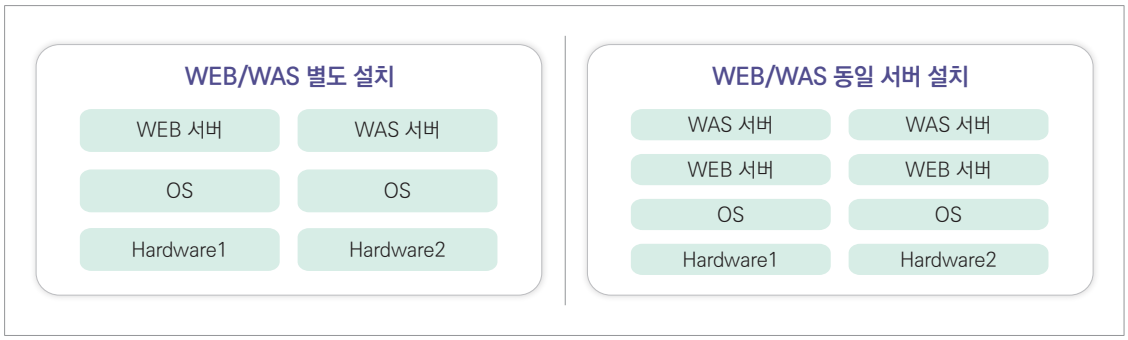
[표 3-4] 미들웨어 종류

구분	세부 내용
범용	- 데이터베이스나 서버에 종속되지 않고 다양한 데이터베이스를 접속하거나 애플리케이션을 개발할 수 있도록 지원
벤더 전용	- 벤더가 자사의 데이터베이스를 연결하기 위하여 제공
특수 목적용	- 벤더가 자사의 데이터베이스와 다른 벤더의 데이터베이스를 연결하기 위하여 제공

● 미들웨어 물리적 분리

- 미들웨어 영역에는 WEB/WAS/AP(Application) 서버 등이 존재하며, 물리적 분리는 각각 하나의 하드웨어에 하나의 WEB/WAS/AP 서버를 설치하여 본인확인업무를 단독으로 수행하는 형태를 의미함
- WEB 서버와 WAS 서버를 각각 별도의 다른 하드웨어에 설치하거나, 사용하는 WAS 서버 성격상 기능적으로 WEB과 WAS가 결합 되어 있는 경우에 WEB 서버와 WAS 서버를 동일한 하드웨어에 설치하는 구성도 가능할 수 있음
- 단, 서버가 처리하는 업무 목적에 따라 적절한 미들웨어 구성 방식을 적용하여야 하며, 장애 처리를 위한 이중화 구성도 고려하여야 함
- 기본적으로 WAS 서버가 WEB 서버의 정적 콘텐츠를 모두 처리할 수 있으나 많은 부하가 발생하므로, WAS 서버는 WEB 서버와 분리하여 설치하는 것을 권고함

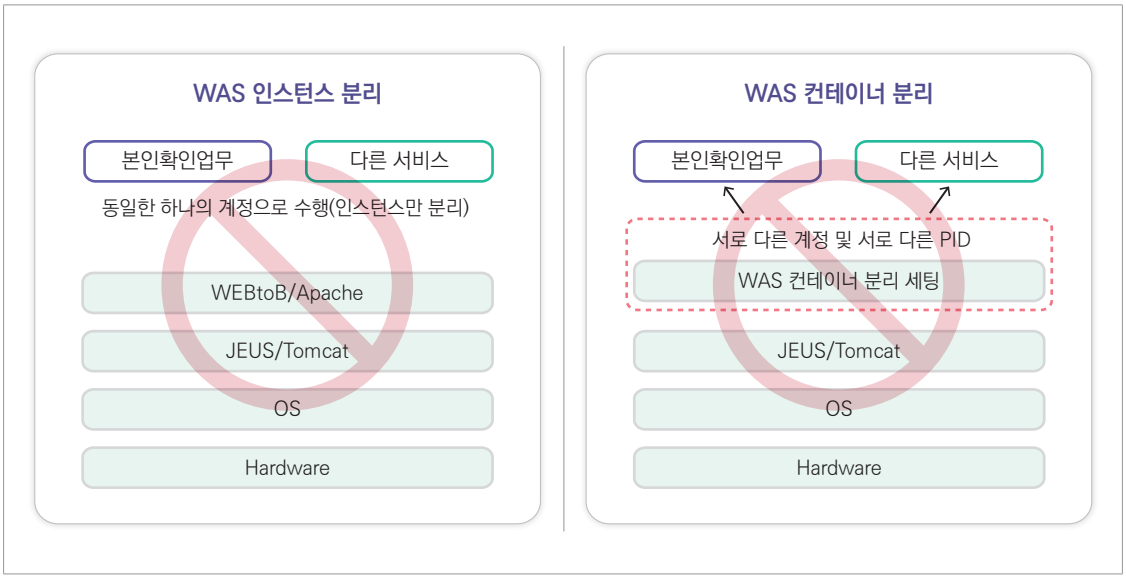
[그림 3-5] 미들웨어 물리적 분리 구성 예시



● 미들웨어 논리적 분리

- 미들웨어 논리적 분리 방법으로 ▲단일 서버 내 WAS 인스턴스 분리 ▲단일 서버 내 WAS 컨테이너 분리 등이 있음
- 단일 서버 내에서 본인확인업무와 다른 인터넷 서비스를 제공하기 위하여 미들웨어의 리소스를 공유하면서 단순히 서비스 포트만 다르게 운영하는 인스턴스(Instance) 분리 방식은 본인확인업무 구성 방식으로 적절하지 않음
- Servlet, JSP, EJB 컨테이너 분리 기술 등을 통하여 단일 서버 내에서 본인확인업무와 다른 인터넷 서비스를 WAS 컨테이너로 계정 및 리소스를 분리하는 방법은 적절하지 않음

[그림 3-6] 미들웨어 논리적 분리 구성 불가 예시



4 DB 분리

- DB 분리 기준
  - [표 2-4]와 [표 2-5]의 분류표에 따른 운영 환경의 본인확인업무 정보시스템은 [표 3-5]와 같은 DB를 구성하고 데이터를 처리함
  - [표 3-5]에서 ▲대체수단 발급 정보 및 대체수단 발급자 정보 ▲본인확인결과정보 생성 이력 및 본인확인 인증 이력이 저장된 운영 환경의 본인확인업무 전용 DB는 다른 인터넷 서비스용 DB와 분리하여야 함
  - 본인확인업무 전용 DB를 분리하는 방법에는 ▲서버 레벨에서 분리하는 방법 ▲DB 레벨에서 분리하는 방법 등이 있으나,
  - 분리 대상 DB에 보관된 데이터의 안전성과 신뢰성, 강화된 개인정보 보호를 위하여 DB 레벨에서의 분리가 아닌 서버 레벨에서 분리하여 본인확인업무 전용 운영 DB서버로 구성하여야 함

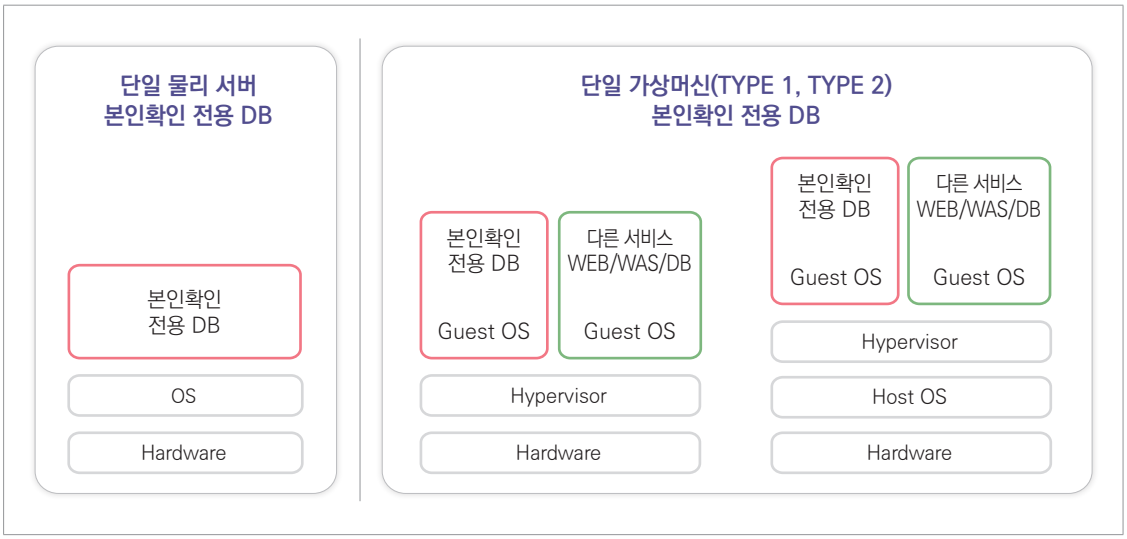
[표 3-5] 본인확인업무와 다른 인터넷 서비스와의 분리 대상 DB 데이터

구분	운영 환경	관련 데이터
분리 대상	본인확인업무 전용 DB	
	– 대체수단 발급 정보 및 이용자 정보 관리 DB – 본인확인결과정보 생성 및 본인확인 인증 이력 관리 DB	– 대체수단 신청·등록·발급·변경·저장·폐기 정보 – 대체수단 발급자 개인정보 – 본인확인결과정보 생성 이력 – 본인확인 인증 이력
미분리 대상	본인확인업무 처리 전사 공용 DB	
	– 이용자 채널 관련 DB – 이용자 본인확인 처리 관련 DB – 이용자 신원확인 처리 관련 DB – 대내·외 업무 연계 DB – 본인확인서비스 전체 흐름상의 처리 로그 관리 DB – 본인확인서비스 민원(이용자 및 대관) 처리 관련 DB	– 본인확인서비스 이용자 웹·앱(전사 공용서비스) 회원가입 정보 – 대체수단 발급을 위한 이용자의 본인확인 인증 및 신원확인 처리 정보 – 본인확인서비스 신청·해제 이력 – 본인확인서비스 이용기관(정보통신서비스 제공자) 관련 정보 – 본인확인 인증 대행(또는 중계) 기관 관련 정보 – 본인확인서비스 처리 로그 (전문연동 로그, 트랜잭션 로그 등) – 본인확인서비스 민원(이용자 및 대관) 처리 정보

● DB 물리적 또는 논리적 분리

- 서버 레벨에서 본인확인업무 전용 운영 DB서버로 분리 구성하는 방법은 ▲단일 물리 서버에 DB 구성 ▲물리 서버에 가상화 기술을 적용하여 단일 가상머신(VM)에 DB 구성으로 구분할 수 있음

[그림 3-7] DB서버 레벨 분리 구성 예시



- 서버 레벨에서 본인확인업무 전용 운영 DB서버로 분리 구성 시에는 다음의 사항을 고려하여야 함

1. 분리 대상인 본인확인업무 전용 운영 DB서버는 물리 서버 또는 가상머신 단위로 다른 인터넷 서비스용 서버와 분리하여야 함
2. 분리 대상인 본인확인업무 전용 운영 DB서버를 가상머신으로 구성 시에는 가상화 환경의 관리적·기술적 보안 위협으로부터 안전을 확보하기 위한 보호조치를 적용하여 운영하여야 함
3. 분리 대상인 본인확인업무 전용 운영 DB서버에는 본인확인업무 전용 DB만 설치·운영하여야 함
4. 분리 대상인 본인확인업무 전용 운영 DB에는 본인확인업무 관련 데이터만 저장하여야 함
5. 분리 대상인 본인확인업무 전용 운영 DB에는 다른 인터넷 서비스에서 처리하는 데이터가 저장되지 않도록 구성하여 다른 업무담당자나 다른 서비스 애플리케이션 등에서 접근하지 않도록 하여야 함
6. [표 3-5]에서 본인확인업무 전용 운영 DB 간에는 구성 방법에 별도 제한이 없으나, [표 2-6]과 같이 DB 용도가 상이한 경우에는 서로 간에 안전성, 신뢰성, 개인정보 보호를 확보할 수 있는 물리적 또는 논리적 분리 방법으로 DB를 구성·운영하여야 함

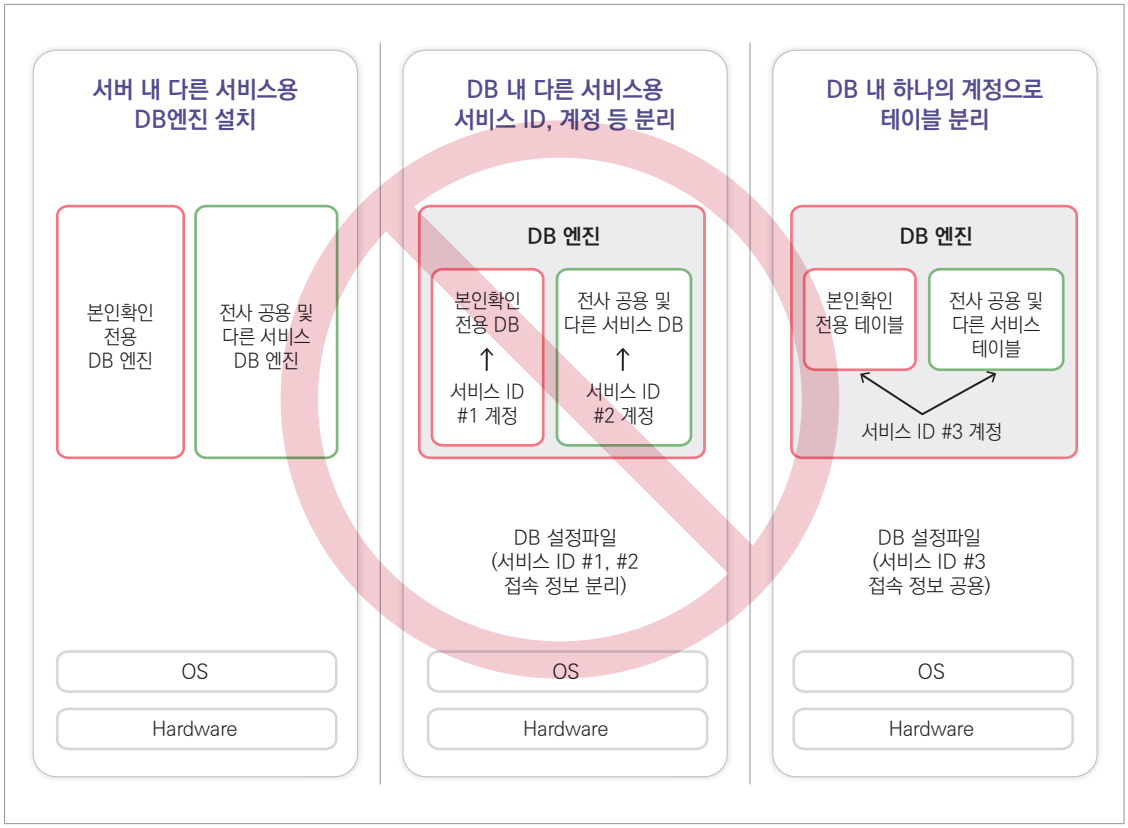
- DB 종류별(Oracle, MySQL, MariaDB, Altibase, PostgreSQL, Redis, Dynamo, MongoDB 등 관계형·비관계형 DB 또는 In-Memory DB)로 DB를 분리 구성하는 다양한 방법이 있으나,

- DB 분리 기준에 따라, DB 레벨에서 본인확인업무 전용 운영 DB와 다른 인터넷 서비스용 DB를 분리하는 것은 적절하지 않음

- [그림 3-8]을 참고하여 다음과 같이 구성하지 않도록 고려하여야 함

1. 본인확인업무 전용 DB서버 내에 다른 인터넷 서비스용 DB 엔진을 설치하여 구성하는 경우
2. 단일 DB서버에 하나의 DB 엔진을 설치하여 본인확인업무 전용 DB와 다른 인터넷 서비스용 DB를 논리적으로 분리(DB 서비스 계정 분리, DB 서비스 ID 분리, 스키마 분리 등 DB 종류별로 다양) 구성하는 경우
3. 단일 DB서버에 하나의 DB 엔진을 설치하고 테이블만 분리하여 하나의 DB 서비스 계정으로 본인확인업무용 테이블과 다른 인터넷 서비스용 테이블에 접근하도록 구성하는 경우

[그림 3-8] DB 레벨 분리 구성 예시



본인확인업무와
다른 인터넷서비스와의 분리
심사기준 안내서

발 행 : 2023년 2월
인 쇄 : 2023년 2월

발행처 : **방송통신위원회**
경기도 관천시 관문로 47, 2동 (TEL : 02-500-9000)
https://www.kcc.go.kr

한국인터넷진흥원
전라남도 나주시 진흥길 9 (TEL : 1433-25)
https://www.kisa.or.kr

인쇄처 : 호정씨앤피(Tel. 02-2277-4718)

본인확인업무와
다른 인터넷서비스와의 분리
심사기준 안내서

방송통신위원회
Korea Communications Commission

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY