석사학위논문

GMP Data Integrity 완결 증대를 위한 AI 바이오메트릭 활용 전자서명 적용 연구

Research on the application of electronic signatures using AI biometrics to increase GMP Data Integrity

2025년 2월

인천대학교 정보기술대학원

컴퓨터 전공

안 상 훈

석사학위청구논문

GMP Data Integrity 완결 증대를 위한 AI 바이오메트릭 활용 전자서명 적용 연구

Research on the application of electronic signatures using AI biometrics to increase GMP Data Integrity

지도교수 김 우 일

이 논문을 석사학위논문으로 제출함

2024년 12월

인천대학교 정보기술대학원

컴퓨터전공

안 상 훈

이 논문을 안상훈의 공학 석사학위 논문으로 인준함

2025년 2월

심사 위원장 이 장 호 (인)

심사 위원 홍 윤 식 (인)

심사 위원 김 우 일 (인)

국문초록

GMP Data Integrity 완결 증대를 위한 AI 바이오메트릭 활용 전자서명 적용 연구

최근 FDA와 EMA 등 규제기관에서 데이터 무결성(Data Integrity)에 대한 요구사항이 점차 강화되고 있다. 이러한 배경 속에서 의약품 제조 및 품질 관리 기준(GMP)에서 데이터 무결성을 보장하는 것은 필수적이다. 본 연구는 Azure Face API를 활용한 안면인식 기술을 통해 GMP 환경에서 데이터 무결성을 높이는 방안을 탐구한다. AI 기반의 안면인식 기술은 사용자 신원 확인 절차를 강화하며, 전자서명 절차에 포함시켜 적용하면 인증의 신뢰성과 보안을 향상시킬 수 있을 것으로 전망한다. 본 논문에서는 Azure Face API를 이용해 안면인식 기술을 테스트하고, 이를 GMP 전자서명 절차에 보완할 수 있는 방법을 제시하였다. 또한, AI 기반 생체인식 기술이 데이터 무결성 문제를 해결하는 데 효과적인 도구가 될 수 있음을 입증하였다. 이를 통해, 기존 서명 방식의 한계를 상호 보완하여 극복하고 규제기관의 지적 사항에 대응할 수 있는 해결책을 제안한다.

주제어 : GMP, Data Integrity, 바이오메트릭, GAMP5, 전자서명, 안면인식

목 차

표 목차

그림 목차

용어

GMP	Good Manufacturing Practice
cGMP	Current GMP
FDA	Food and Drug Administration
EMA	European Medicines Agency
PIC/S	Pharmaceutical Inspection Co-operation Scheme (의약품 제조 및 품질 관리 분야에서 국제적 협력을 위한 중요한 기구)
ISPE	International society for Pharmaceutical Engineering (국제제약엔지니어링협회 GMP분야의 국제기관 임. 미국 내 소재하며 FDA와 긴밀한 협력 하에 제약 산업분야에 필요한 가이드라인을 확립하여 기준을 제시함)
DI	Data Integrity(데이터 무결성 데이터는 완전하고 일관되며 정확하여야 하고, 출처를 확인할 수 있으며, 판독이 가능하고, 발생과 동시에 기록된 원본이거나 사본을 말한다.)
CSV	Computer System Validation (컴퓨터화 된 시스템이 미리 정의된 규격에 따라서 일관되게 운영 된다는 것을 높은 수준으로 증명하여 문서화된 증거를 확립하는 과정)

[1]

1 장　서론

1.1 연구 배경

GMP(Good Manufacturing Practice)는 제약, 생명공학, 식품 및 기타 규제 산업에서 제품의 품질과 안전성을 보장하기 위해 필수적으로 준수해야 하는 규제 표준이다. GMP 환경에서 데이터 무결성(Data Integrity, 이하 DI)은 제품의 전 과정에서 발생하는 데이터가 정확하고 일관되며 변경되지 않았음을 보장하는 중요한 개념이다.

이는 제품의 제조-생산부터 완제-포장까지 모든 과정에서 데이터의 투명성과 신뢰성을 유지하기 위한 필수적인 요구사항이다.

데이터의 손상이나 왜곡은 제품의 품질 및 소비자 안전에 심각한 영향을 미칠 수 있다. FDA, EMA, 식약처 등의 감사 기관에서는 현장 감사를 통해, 결과를 통보한다. 결과에 따라 제품 허가 여부가 결정되기 때문에 기업 입장에서는 해당 결과가 중요하다.

기존의 전자서명 시스템은 주로 사용자 ID와 비밀번호를 기반으로 운영되며, GMP 준수에 있어 중요한 역할을 하고 있다. 그러나 이러한 전통적인 인증 방식은 사용자의 인증 정보가 도용되거나 유출될 가능성이 높아 데이터 무결성을 위협할 수 있는 잠재적 위험을 내포하고 있다. 이로 인해 GMP 환경에서 더욱 강력하고 신뢰할 수 있는 인증 방법의 필요성이 대두되고 있다.

최근 인공지능(AI) 기술의 발전과 함께, 바이오메트릭(생체인식) 기술이 보안 및 인

증 분야에서 주목받고 있다. 안면인식, 음성인식, 지문인식 등 바이오메트릭 기술은 사용자의 고유 생체 정보를 활용하여 인증의 정확성과 신뢰성을 크게 높일 수 있다. 이러한 기술은 사용자 ID와 비밀번호의 한계를 극복하고, GMP 환경에서 데이터 무결성을 더욱 강화하는 데 중요한 역할을 할 수 있다.

본 연구는 이러한 배경에서 출발하여, AI 기반 바이오메트릭 기술을 GMP 환경의 전자서명 절차에 도입함으로써 데이터 무결성을 강화하는 방안을 탐색하고자 한다. 이를 통해 기존 인증 방식의 문제점을 해결하고, GMP 준수와 데이터 관리의 효율성을 향상시키는 데 기여할 수 있는 새로운 접근법을 제시한다.

1.2 연구 목적

본 연구의 목적은 Good Manufacturing Practice(GMP) 환경에서 데이터 무결성을 강화하기 위한 새로운 전자서명 방안을 제시하는 것이다. 특히, 기존의 ID와 비밀번호 기반 전자서명 방식이 가지는 보안적 한계를 극복하고, 데이터의 신뢰성과 정확성을 높이기 위해 인공지능(AI) 기반 바이오메트릭 기술을 도입하고자 한다. 본 연구에서는 안면인식과 음성인식과 같은 고도화된 바이오메트릭 인증 방법을 활용하여, GMP 환경에서의 사용자 인증 절차를 개선하고 데이터 무결성을 확보하는 방안을 모색한다.

이를 통해, 데이터 도용이나 위 변조의 가능성을 줄이고, GMP 준수에 필요한 데이터 관리 및 품질 관리 시스템의 효율성을 향상시키는 데 기여하는 것이 본 연구의 주된 목적이다. 아울러, AI 기반 바이오메트릭 기술을 전자서명 절차에

적용할 때 고려해야 할 법적, 기술적 과제를 분석하고, 이러한 기술 도입이 GMP 환경에서 어떠한 이점을 제공할 수 있는지를 실증적으로 평가하고자 한다.

결국, 본 연구는 GMP 환경에서 데이터 무결성 강화와 관련된 새로운 표준을 마련하고, 이를 통해 Data Integrity 측면에서 기업들이 보다 신뢰할 수 있는 인증 체계를 갖출 수 있도록 하는 데 기여하는 것을 목표로 한다.

1.3 연구의 중요성 및 필요성

Good Manufacturing Practice(GMP) 환경에서 데이터 무결성(Data Integrity)은 제품의 품질과 안전성을 보장하기 위한 필수 요소로서, 전 세계의 규제 기관과 산업계에서 점점 더 중요하게 다루어지고 있다. 데이터 무결성의 손상은 제품의 품질 저하, 소비자 안전 위협, 심각한 법적 제재로 이어질 수 있어 기업의 신뢰성과 지속 가능성에 중대한 영향을 미친다. 특히, 제약, 생명공학, 의료기기와 같은 고위험 산업에서는 GMP 준수와 데이터 무결성이 그 어느 때보다도 중요한 요소로 부각되고 있다.

그러나 현재 GMP 환경에서 널리 사용되는 전자서명 시스템은 주로 사용자 ID와 비밀번호를 기반으로 하고 있으며, 이는 데이터 위변조, 불법적인 접근, 도용 등 다양한 보안 문제에 취약하다. 이러한 전통적인 인증 방식의 한계는 데이터 무결성을 위협하는 주요 원인으로 작용하고 있으며, 이를 보완하기 위한 새로운 보안 기술의 도입이 시급한 실정이다.

최근 인공지능(AI)과 바이오메트릭(생체인식) 기술의 급속한 발전은 사용자 인증

방법의 신뢰성과 정확성을 획기적으로 향상시킬 수 있는 기회를 제공하고 있다. 안면인식, 음성인식 등 고도화된 바이오메트릭 기술은 사용자 고유의 생체 특성을 기반으로 하여, 기존의 ID/비밀번호 방식에서 발생할 수 있는 보안 취약점을 극복할 수 있다. 이러한 기술은 데이터 무결성을 강화하고, GMP 환경에서의 규정 준수와 품질 관리 시스템의 신뢰성을 크게 향상시킬 잠재력을 가지고 있다.

본 연구의 필요성은 이러한 배경에서 더욱 명확해 진다. GMP 환경에서 데이터 무결성을 유지하기 위한 보다 강력하고 신뢰할 수 있는 인증 시스템의 개발은 필수적이며, 이를 통해 기업은 규제 요구사항을 보다 효과적으로 준수할 수 있을 뿐만 아니라, 제품의 품질과 안전성을 한층 더 높일 수 있을 것이다. 따라서, AI 기반 바이오메트릭 기술을 활용한 전자서명 시스템의 도입은 GMP 환경에서 데이터 무결성을 보장하고, 전반적인 품질 관리 시스템의 효율성을 극대화하는 데 중요한 기여를 할 것으로 예상된다.

2 장 GMP 환경에서의 데이터 무결성

2.1 데이터 무결성(Data Integrity) 정의 및 중요성

데이터 무결성(Data Integrity)이란 데이터가 정확하고, 일관되며, 변경되지 않았음을 보장하는 개념으로, 데이터가 생성되고 수집된 순간부터 삭제 또는 보관될 때까지의 모든 상태에서 그 완전성과 신뢰성을 유지하는 것을 의미한다. 즉, 데이터 무결성은 데이터가 손상되거나 왜곡되지 않고, 의도된 대로 사용될 수 있는지를 보증하는 중요한 요소이다. 이는 데이터가 올바르게 기록되고, 인증된 사용자만이 접근하거나 수정할 수 있으며, 데이터 변경 이력이 추적 가능하도록 하는 다양한 기술적, 관리적 조치를 포함한다.

2.2 ALCOA 란?

데이터 완전성을 "데이터가 완전하고, 일관되고, 정확하고, 신뢰할 수 있고, 신뢰할 수 있는 정도와 데이터의 이러한 특성이 데이터 全주기 동안 유지되는 정도"로 정의하고 있다. 데이터는 귀속 가능하고, 읽을 수 있고, 동시에 기록되고, 원본(또는 정본)이며 정확 해야 하게 안정적인 방식으로 수집되고 유지가 되어야 한다. 데이터 완전성은 과학적 원리와 우수 문서화 기반을 통한 품질 및 위험관리 시스템이 필요하며, ALCOA++ 원칙을 준수해야 한다. ALCOA++는 각 귀속성, 가독성, 동시성 등 데이터 무결성 필수 용어의 앞자리를 추려 만들어 부르는 명칭이다.

표 2.1 ALCOA++ 설명표

데이터 완전성 속성		ALCOA	ALCOA+	ALCOA++
Attributable	귀속성	V	V	V
Legible	가독성	V	V	V
Contemporaneous	동시성	V	V	V
Original	원본성	V	V	V
Accurate	정확성	V	V	V
Complete	완전성		V	V
Consistent	지속성		V	V
Enduring	일관성		V	V
Available	가용성		V	V
Traceable	추적성			V

GMP IT 시스템에서는 해당 시스템의 ALCOA ++ 에 적용되었음을 증명하기 위해 CSV(Computer System Validation)를 진행한다.[1]

FDA에서는 전자 시스템에서 다뤄야 할 기본 규정을 제정하여 발표하였다. 전자기록 (Electronic Record)과 전자서명(Electronic Signature)이 신뢰할 수 있고, 종이 기록과 동등한 것으로 간주한다고 하였고, 이를 지킬 수 있는 적용 기준을 제시하였다. 그 적용 기준이 Title CFR-Part11이다[2][3]

2.3 FDA Title 21 CFR-Part 11

CFR-Part11은 미국 식품의약국(FDA)이 제정한 전자 기록 및 전자 서명에 관한 규정이다. 전자 기록과 전자서명의 신뢰성, 진실성, 기밀성을 증명하는 기준을

제시한다.[2] 제시된 기준은 현실적이지 않은 부분과 혼돈을 줄 수 있는 부분이 있어, 지속적으로 개정되어 지금(24년 2월)버전까지 오게 되었다. [3]

다루는 내용의 목차는 아래와 같다 [2, 3]

표 2.2 CFR Part 11 Audit Table

큰 제목	상세 제목
Subpart-A **– 일반 조항**	• 범위 • 이행 • 정의
Subpart-B **– 전자 기록**	• 폐쇄형 시스템을 위한 제어 장치 • 개방형 시스템을 위한 제어 장치 • 서명 표현 • 서명/레코드 연결
Subpart-C **– 전자 서명**	• 일반 요구 사항 • 전자 서명 및 제어 • 식별 코드/비밀번호에 대한 제어

CFR-Part 11에서 주로 다루는 영역은 아래와 같이 정리된다. [4, 5]

표 2.3 CFR Part 11 주요 요소

구분	설명

Paperless	- 데이터는 종이를 대신하여, 기록이 전자화 되어야 한다 - 전자 기록은 변질의 우려가 없어야 하며, 데이터 신뢰성을 증명해야 한다
Audit Trail	- 변질의 우려가 없음을 증명하기 위해, 모든 데이터의 생성 변경에는 기록자가 누구인지를 식별할 수 있도록 로그화가 되어야 한다. - 삭제는 안되며, 데이터 비활성화는 가능하다. 권한을 가진 관리자만 가능하여야 하며, 비활성화시에도 사유를 기록하여야 한다. 모든 데이터는 백업이 되어야 한다.[6]
e-Signature	- 전자서명은 서명자의 신원과 데이터 무결성을 검증할 수 있는 일련의 규칙과 일련의 매개변수를 사용하여 계산된, 작성자 인증의 암호화 방법을 기반으로 하는 수행되어야 한다.

2.4 GAMP5 란?

GAMP 5(Good Automated Manufacturing Practice 5)는 제약 및 바이오 제약 산업에서 컴퓨터화 된 시스템의 검증과 품질 관리를 위한 중요한 프레임워크이자 전산시스템 검증 방법론이다. 여기서 숫자는 버전이라고 이해하면 된다.

최초 GAMP Life Cycle V Model이었다. 1990년대 초에 처음 만들어진 이래로 GAMP 가이드에는 [그림 1 GAMP5 Basic V Model]과 같이 항상 수명 주기 모델로 시작되었다는 것이 중요하다. 그러나 실험실의 관점에서 볼 때 문제는 GAMP 가이드의 원래 목표가 제약 산업에 제조 생산 장비 공급 업체를 통제하는 것이 있었다는 것이다. 따라서 1994년부터 2008년 초까지 GAMP 가이드의 처음 4개 버전에 사용된 V 모델은 주로 제조 장비를 위한 것이었다. 원래 의도대로 이 V

모델은 엔지니어링 회사에서 제공하는 일부 컴퓨터 제어 요소가 있는 장비로 주로 구성된 장비 및 시스템을 제조하는데 적합하다. 이러한 시스템 중 다수는 기본 장비 구성을 가지고 있으며, 이러한 구성은 개별 시설 또는 제조 라인에 맞게 맞춤화가 된다. [7-10]

따라서 소프트웨어 응용 프로그램에 맞는 카테고리가 추가되고 정리되면서 지금의 GAMP5로 발전하게 되었다.[11]

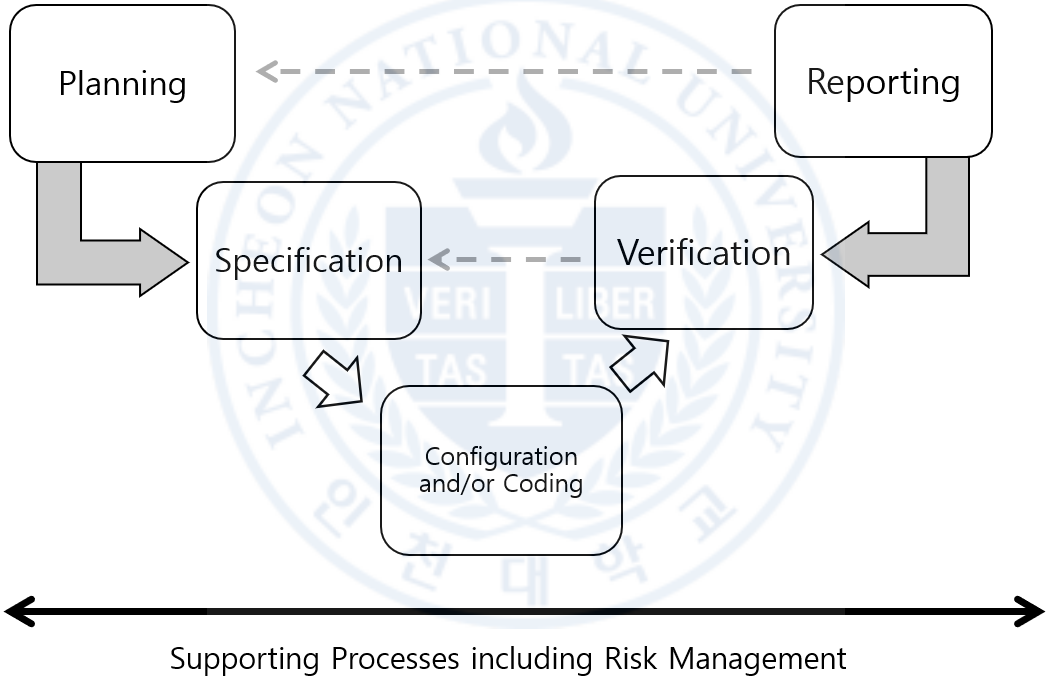


그림 2.1 GAMP5 Basic V Model

표 2.4 GAMP5 Category 구분

Category	GAMP4	GAMP5
1	Operating System	Infrastructure, Software (OS, middleware, DB Manager, etc)

2	Firmware	No longer used – Firmware is no longer functionally distinguishable
3	Standard Software	Non-configured software – Includes default configurable SW
4	Configurable Software	Configurable Software – configured to satisfy business process
5	Custom Software	Custom Software

GAMP에서 제시하는 Category Model은 Software와 응용프로그램이 만들어진 목적과 활용범위에 따라 지정하여 CSV 검증 레벨 수위가 달라짐을 명시함. 검증 절차를 동등하게 적용하게 되면, 어떤 응용프로그램은 부실해질 수 있고, 어떤 응용프로그램은 비효율이 될 수 있기 때문이다.

위험도 평가는 심각도와 확률, 리스크 유형과 탐지가능성 조합으로 등급을 유추한다. 이 결과는 Category 레벨 평가에 가중치로 사용하기도 하고, 유지보수 측면에서 변경관리가 이루어질 때 CSV 레벨에 적용하기도 한다.[10, 12]

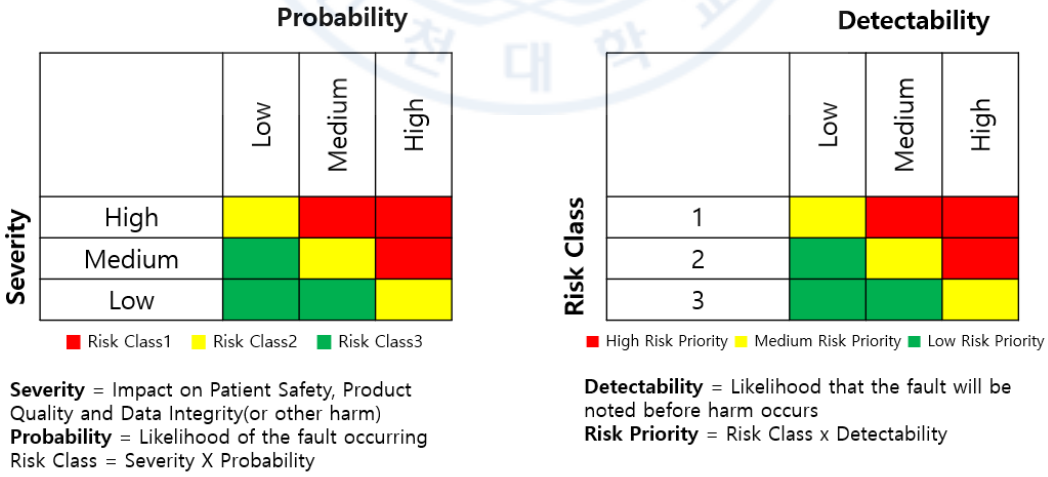


그림 2.2 GAMP5 위험도 평가 접근법 [10]

2.4.1 GMP System 기본 생애주기

제약 바이오 연구, 생산, 품질 관리 등에 Paperless, 데이터 중앙화, 업무혁신을 위해 소프트웨어 응용 프로그램이나 컴퓨터 시스템은 개발되어지고, 점차 고도화되고 있다. 해당 프로그램과 시스템은 치료제 개발과 생산에 직, 간접적으로 관여되기 때문에 GMP 통제 규정에 포함되어진다.[6, 13-15]

GMP 통제 규정에 포함되어진다는 것은 응용프로그램, 시스템이 Data Integrity 측면에서 보증할 수 있어야 하며, 이를 위해 지속적으로 무결정을 검증하고 증명해야 한다. GMP 응용프로그램, 시스템들의 생애 주기는 크게는 Concept-Project-Operation-Retirement로 구분되어진다. 실질적인 구현 단계인 Project 단계에서는 Planning-Specification-Configuration and/or coding-Verification-Reporting 절차로 진행되어진다.[10, 11]

표 2.5 GAMP5 프로젝트 방법론 단계별 설명

단계	설명
Planning	- 작업을 수행하기 위한 청사진 또는 로드맵을 구상하는 단계. 시스템이 올바르게 구축되고 필요에 따라 작동할 수 있도록 준비한다.
Specification	- 앞서 기획했던 계획을 구체적으로 표현하는 단계. 구현과 개발 예정인 응용프로그램, 시스템에 맞는 상황을 구체적으로 기술하고 개발될 수 있도록 한다. 현 단계에서 작성된 문서나 기록들이 향후 확장성 여부를 가늠한다.

Configuration and/or Coding	- Specification에서 설계한 대로 구현하는 단계이다. 각 어플리케이션에서 제공하는 기능에 따라 설정기능으로 구현하거나 직접 개발언어를 통해 구현하기도 한다.
Verification	- URS를 기반으로 Configuration 하거나 개발되어진 결과물을 검증한다. 설계 문서에 쓰여진 대로 작동하는지, 변질될 우려나 오작동이 없는지를 체크하여 해당 결과물에 이상이 없음을 증명한다.
Reporting	- URS에 기술된 요청 사항에 대해, 적절하게 구현되었고, CSV 결과 문제없음을 최종적으로 정리한다. 향후, 여기에서 정리된 결과를 감사기관에 제출하기도 한다.

2.4.2 GMP System 단계별 생애주기

ISPE에서 말하는 GAMP5에서 GMP 시스템은 Concept – Project – Operation – Retirement 의 단계를 가진다.[11]

위에 언급된 기본 생애 주기는 단계별 생애주기에서 Project에 해당된다.

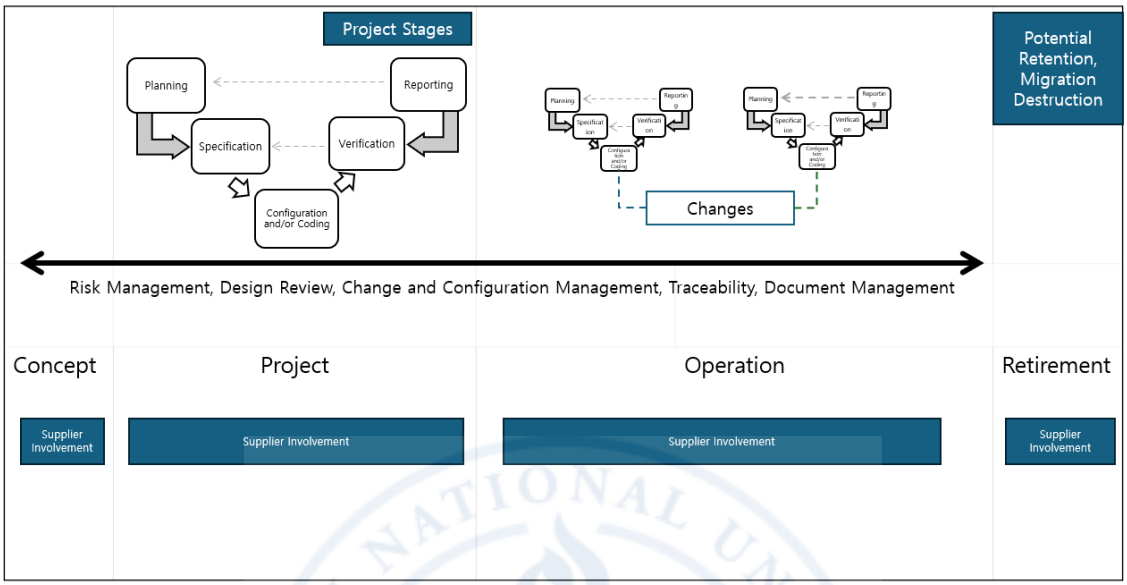


그림 2.3 GAMP5 프로그램 단계별 생애 주기 기본 [10]

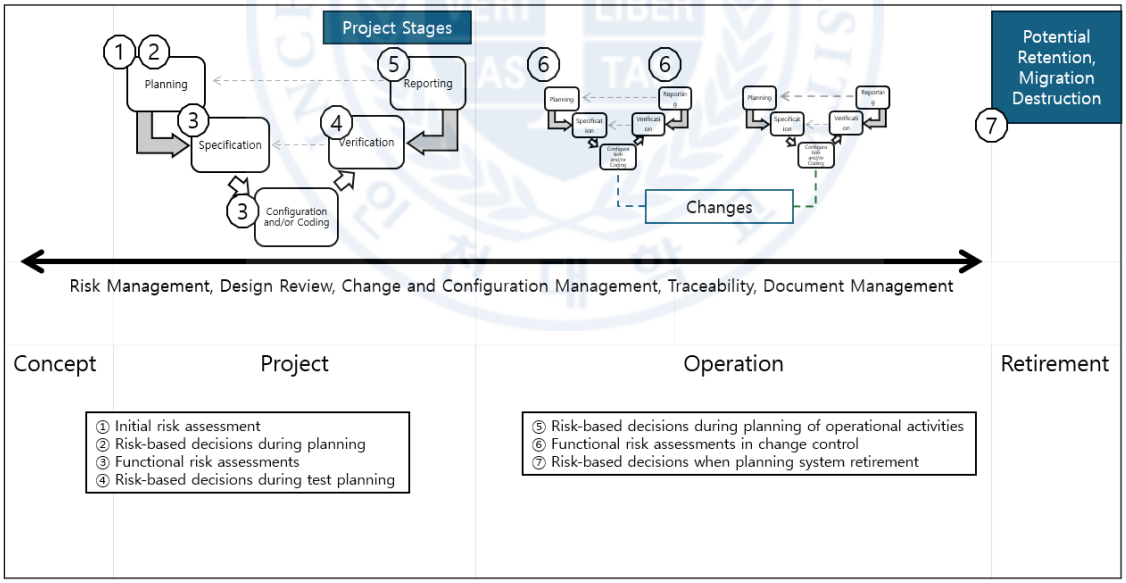


그림 2.4 GAMP5 프로그램 단계별 생애 주기 상세설명[10]

2.4.2.1 Concept 단계

- 시스템의 개념을 정립하는 단계
- 사용자 요구사항(User Requirements)을 수립
- 시스템의 목적과 의도된 사용(intended use)을 정의
- 적합한 외부 솔루션을 도입할지, 내부 개발을 할지를 결정하는 단계

2.4.2.2 Project 단계

- 명세(Specification): 기능 및 기술 설계 명세를 문서화하여 구체화
- 구성 및 코딩(Configuration and Coding): 시스템 개발 또는 구성 작업 실질적인 수행
- 검증(Verification): IQ, OQ, PQ 등 다양한 수준의 테스트 수행 단계
- 보고(Reporting): 프로젝트 활동 결과를 요약하고 시스템 검증 완료 단계

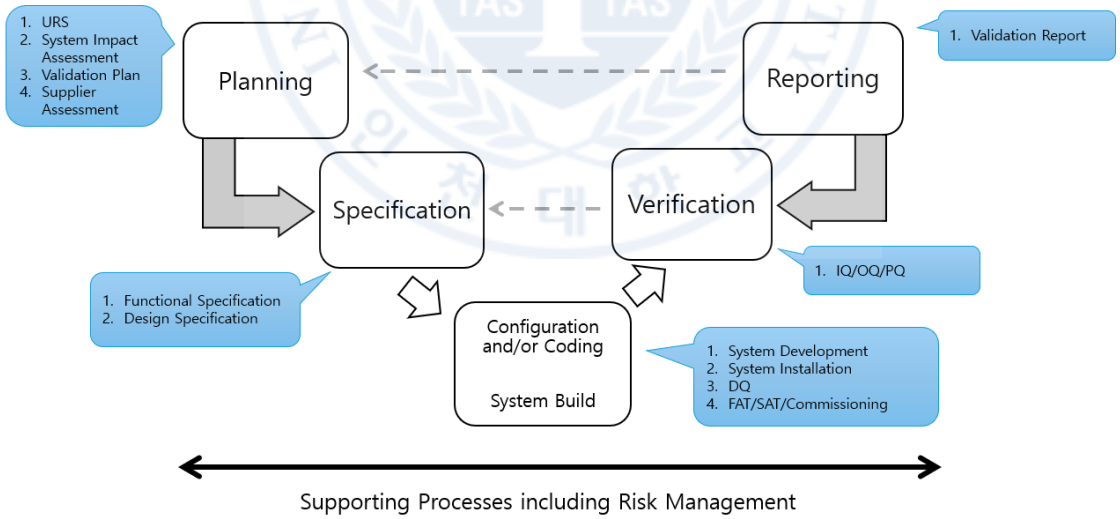


그림 2.5 Life Cycle Approach(Project) [10]

2.4.2.3 Operation 단계

GMP 시스템이 운영되는 단계를 의미하며, 상세 활동은 아래와 같다

- 인시던트 및 문제 관리
- 시스템 백업 및 복구
- 시스템 관리
- 변경 및 구성 관리
- 접근 제어
- 주기적 검토

위 활동에서 조금이라도 이상 증상이 발생되어 사고로 이어지면 일탈이 되는 것이며, 일탈을 방지하기 위해 지속적인 검증과 검토가 수시로 이루어져야 한다.[11]

2.4.2.4 Retirement

GMP 시스템의 퇴역이 결정되었을 때, 행해지는 단계이다. 주로 목적에 맞는 용도가 실종되거나 새로운 GMP 시스템으로 변경이 결정되어졌을 때 행해지게 된다.

- 시스템 폐기 계획 수립
- 중요 비즈니스 데이터의 마이그레이션 또는 보관
- 회사 정책 및 규제 요구사항에 맞는 데이터 보존

표 2.6 GAMP5 Project-Operation Action

Phase	Action
Project	① Initial risk assessment

	② Risk-based decisions during planning ③ Functional risk assessments ④ Risk-based decisions during test planning
Operation	⑤ Risk-based decisions during planning of operational activities ⑥ Functional risk assessments in change control ⑦ Risk-based decisions when planning system retirement

소프트웨어 응용 프로그램이나 컴퓨터 시스템은 갑자기 구체화되지 않는다. 각각을 계획하고 구현해야 한다. 따라서 시스템 수명 주기의 사용은 컴퓨터화 된 시스템의 구현 또는 구축을 위한 기초로 사용할 계획을 제공하기 때문에 중요하다. [7][11]

GMP(Good Manufacturing Practice) 환경에서 데이터 무결성은 제품의 품질과 안전성을 보장하는 데 필수적인 역할을 한다. 제약, 생명공학, 의료기기와 같은 고위험 산업에서는 제품의 제조와 품질 관리 과정에서 생성되는 데이터의 신뢰성과 정확성이 매우 중요하다. 데이터 무결성이 손상될 경우, 잘못된 데이터에 기반한 결정을 내릴 수 있으며, 이는 제품 품질 저하, 안전성 문제, 심각한 법적 제재로 이어질 수 있다. 예를 들어, 제약 제품의 제조 공정에서 중요한 데이터가 손상되거나 조작될 경우, 그 결과물은 효과가 없거나, 심지어 소비자에게 해를 끼칠 수 있는 제품이 될 수 있다.

또한, 규제 당국은 GMP 준수 여부를 판단하기 위해 데이터 무결성을 중요하게 평가한다. 데이터 무결성의 훼손은 규제 당국의 신뢰를 잃게 하고, 이는 곧 기업의

평판 손상, 제품 승인 지연, 또는 시장에서의 퇴출로 이어질 수 있다. 따라서, 데이터 무결성을 유지하는 것은 단순히 규제 준수를 위한 요구사항일 뿐만 아니라, 기업의 지속 가능성과 직결되는 중요한 요소이다.

이와 같은 이유로, 데이터 무결성은 GMP 환경에서 필수적인 요소로 자리 잡고 있으며, 이를 보장하기 위한 다양한 기술적 및 관리적 조치들이 필요하다. 특히, 디지털 전환과 더불어 데이터 관리의 중요성이 더욱 커지고 있는 현대 산업 환경에서는 데이터 무결성을 보장하는 것이 그 어느 때보다 중요하다.

2.5 GMP에서의 데이터 무결성 요구사항

FDA 에서는 모든 제조과정에서 발생하는 데이터는 신뢰할 수 있고 정확하기를 기대한다고 했다[16]

데이터 무결성은 품질 및 안정성을 보장하며, 제품의 일관성 여부를 판단할 수 있다. 이러한 정황들은 생산 제조 포장 과정에서의 신뢰를 보증하게 된다.

각 기관은 자신의 GMP기준을 만들어 해당 사항이 지켜지는가를 감사한다.

표 2.7 기관별 국가별 GMP 기준에 따른 구분

기관관	소속
cGMP	FDA가 만든 높은 수준의 GMP
EU GMP	유럽의약품청(EMA)에서 정한 가이드라인
WHO GMP	WHO 가 지정한 백신, 생물학 제제 제조관리 기준
PIC/S GMP	의약품 상호실사협력기구의 GMP 가이드라인, 회원국간

	의약품 실사정보를 공유해 의약품 허가 등록시 필요한 GMP 실사를 면제 또는 간호화 할 수 있음

각 기관의 감사 기준을 통해, 감사 결과를 전달해 주는데, FDA의 감사 결과는 아래와 같이 구분되어진다 [17]

표 2.8 FDA Inspection classification

구분	설명
No Action Indicated (NAI)	which means no objectionable conditions or practices were found during the inspection. 검사 중에 불쾌한 조건이나 관행이 발견되지 않았음을 의미
Voluntary Action Indicated (VAI)	which means objectionable conditions or practices were found, but the agency is not prepared to take or recommend any administrative or regulatory action or 불쾌한 조건이나 관행이 발견되었지만 기관이 행정 또는 규제 조치를 취하거나 권고할 준비가 되어 있지 않음을 의미
Official Action Indicated (OAI)	which means regulatory and/or administrative actions are recommended 규제 및/또는 행정 조치가 권장됨을 의미

Warning Letter : *FDA 감사결과 중 심각한 시정이 필요한 경우 발간한다. Form 483 형태의 경고 서한은 FDA승인과 밀접한 관련을 가지고 있고, 시정조치가 부족한 경우 승인 취소, 거절을 할 수 있다.* [18]

(2010~2020) 10년간 FDA에서 발행한 Warning Letter를 분석한 보고서에 따르면, Data Integrity 미준수에 대한 경고가 꾸준히 20~25%에 달한다고 분석했다. [18]

표 2.9 FDA 산하 연구센터 구분

용어	설명
CDER(Center for Drug Evaluation and Research)	의약품평가연구센터, 제너릭, 바이오 치료제등 의약품을 규제하고 평가함
CDRH(Center for Devices and Radiological Health)	의료기기·방사선보건센터 : 치료에 필요한 의료기기와 방사선 방출제품의 안전성과 유효성을 평가함

23년도 FDA Warning Letter를 분석하여도 DI와 관련된 지적사항은 상당부분(27%) 차지함을 알 수 있다. [19, 20]

표 2.10 23년도 FDA Warning Letter 분석표

점유율	Instances	규정구분	규정 설명
19.3%	**98 instances**	**21 CFR 211.22(d)**	**Procedures not in writing, fully followed**
14.0%	71 instances	21 CFR 211.192	Investigations of discrepancies, failures
10.8%	- 55 instances	21 CFR 211.100(a)	Absence of written procedures
10.2%	52 instances	21 CFR 211.160(b)	Scientifically sound lab controls
9.4%	48 instances	21 CFR 312.60	1572 Protocol compliance
9.1%	46 instances	21 CFR 211.67(a)	Cleaning/sanitizing/maintenance
7.7%	39 instances	211 CFR 211.63	Equipment design, size, and location

7.3%	37 instances	21 CFR 211.68(b)	Computer control of master formula records
6.7%	34 instances	21 CFR 1271.75(a)(1)	Human tissue for transplantation, risk factors, clinical evidence
5.5%	28 instances	21 CFR 211.113(b)	Procedures for sterile drug products

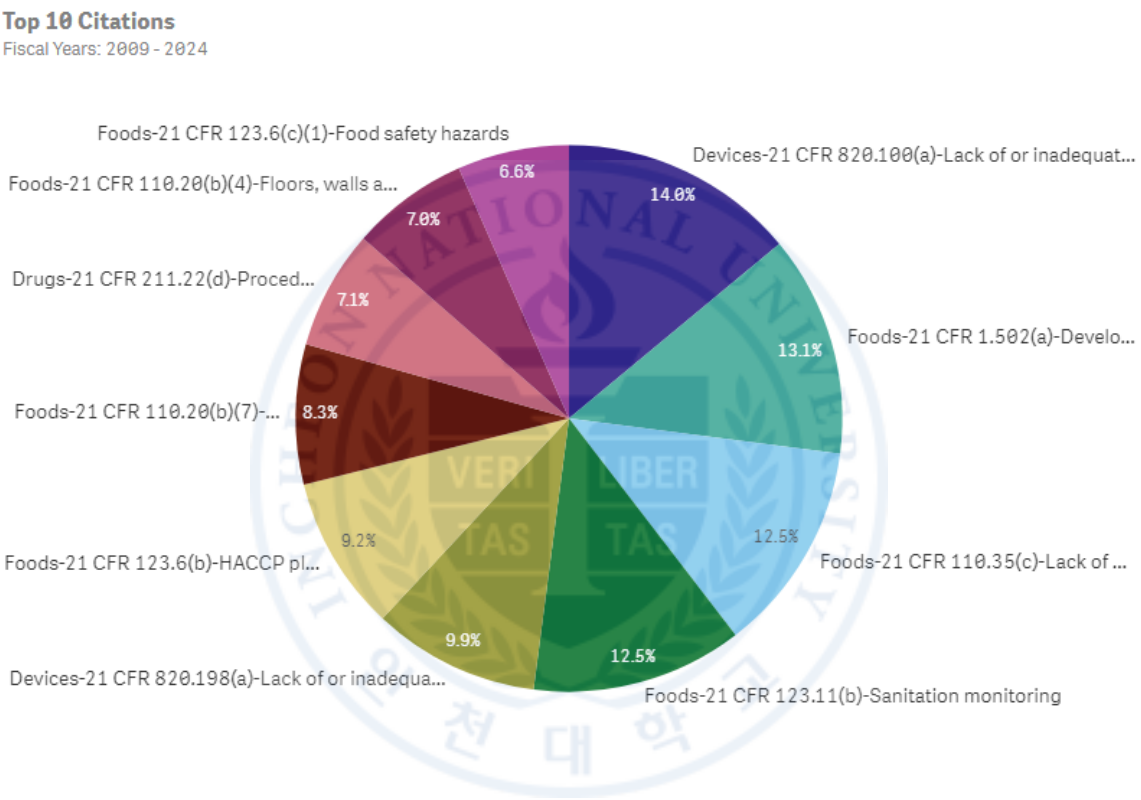


그림 2.6 2009-2024 Top 10 Citations [21]

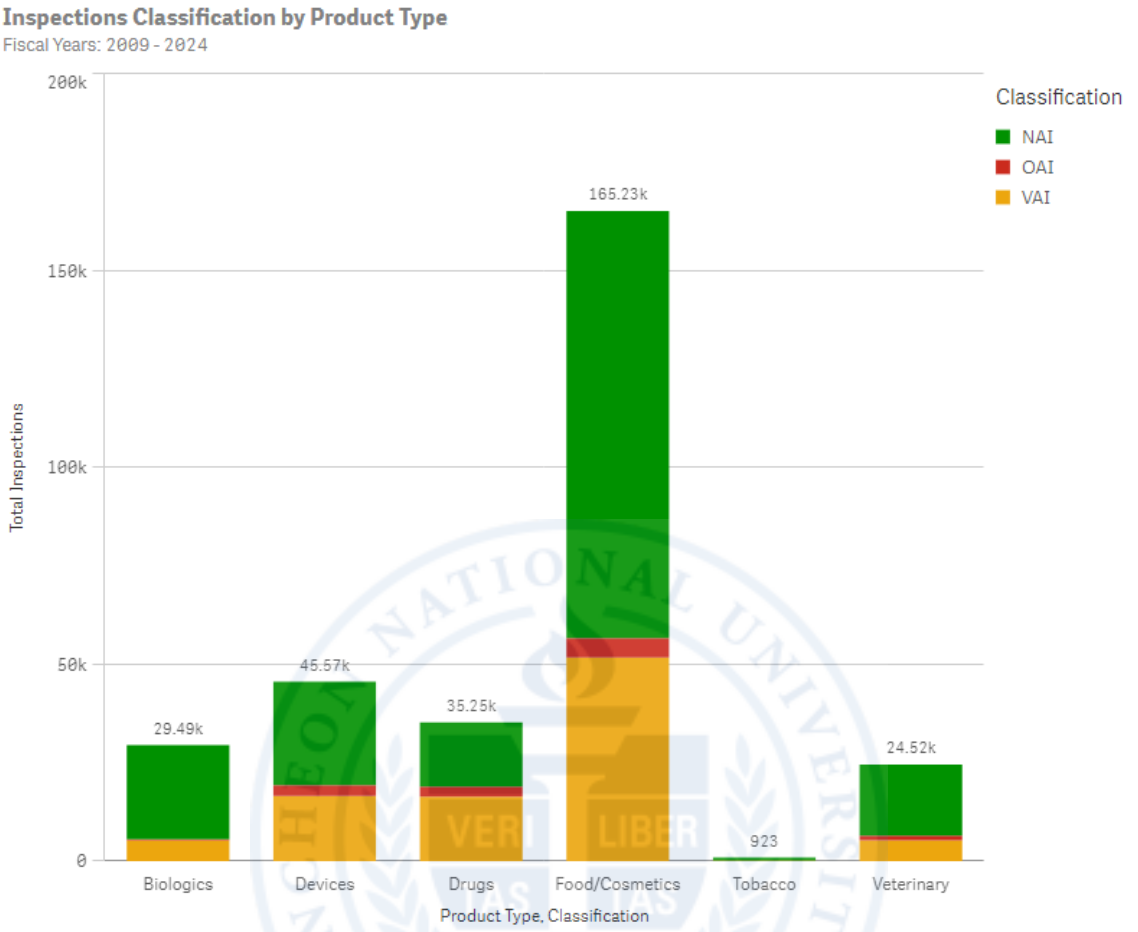


그림 2.7 2009-2024 Inspections Classification by Product Type [21]

24년 이후 감사결과를 예상한바, OAI같은 부정적 의견은 점차 감소되면, 시정될 수 있도록 유도하는 VAI가 증가할 것이라고 내다봤다.[19]

FDA의 감사결과를 토대로 주관적인 견해로는 제약 바이오 산업에 점차 많은 GMP System들이 도입되고, 실험 장비에서 나오는 데이터나 품질관리에서 활용되는 여러 IT시스템등을 DI 관점에서 무결한지를 감사자들은 세심하게 살피고 이를

중심으로 감사결과를 내고 있는 추세이다. 그리고 감사자들은 DI관점에서 검토하는 폭이 앞으로 더욱 커질 것으로 예상된다.

2.5 기존 전자서명 방식의 한계

기존의 ID와 비밀번호를 기반으로 한 전자서명 방식은 오랫동안 다양한 산업에서 사용자 인증의 표준 방법으로 사용되어 왔으나, 이 방식에는 여러 가지 한계가 존재하며, 특히 GMP(Good Manufacturing Practice) 환경에서 데이터 무결성을 위협하는 잠재적 위험을 안고 있다.[22, 23]

표 2.11 ID/비밀번호 방식의 문제점

구분	상세 내용
보안 취약성	ID와 비밀번호 기반 인증 시스템은 사용자 정보 도용, 해킹, 피싱 등의 보안 위협에 취약하다. 비밀번호는 상대적으로 쉽게 추측되거나 탈취될 수 있으며, 이는 데이터의 무결성을 심각하게 위협할 수 있다. 예를 들어, 불법적으로 접근 권한을 획득한 사용자가 의도적으로 데이터를 조작하거나 삭제할 경우, 제품의 품질과 안전성에 치명적인 영향을 미칠 수 있다.
인증 정보의 공유 및 도용	여러 사용자가 동일한 ID와 비밀번호를 공유하거나, 인증 정보를 타인에게 의도적으로 또는 무의식적으로 넘겨줄 가능성이 존재한다. 이는 실제로 인증을 수행한 사람이 누구인지 정확히 식별할 수 없게 만들어, 책임 소재를 명확히 하기 어렵게 한다. 이러한 상황은 데이터 변경 이력의 신뢰성을 저하시키고, 규제 기관의 감사에서 문제를 일으킬 수 있다.

사용자 행동 패턴과의 불일치	ID와 비밀번호는 사용자 행동 패턴이나 위치와 같은 맥락 정보를 반영하지 않기 때문에, 평소와 다른 방식으로 시스템에 접근하더라도 이상 징후를 감지하기 어렵다. 이는 내부자 위협(예: 권한을 가진 사용자가 의도적으로 데이터를 조작하는 경우)이나 외부 공격자의 침입을 효과적으로 방지하지 못하는 원인이 된다.
비밀번호 관리의 어려움	사용자는 강력한 비밀번호를 설정하고 이를 주기적으로 변경해야 하지만, 이는 실제로 많은 사용자에게 불편을 초래하며, 결과적으로 비밀번호를 재사용하거나 쉽게 추측할 수 있는 약한 비밀번호를 설정하게 된다. 또한, 여러 시스템에서 다양한 비밀번호를 관리해야 하는 경우, 이를 메모하거나 저장해 두어야 하는 상황이 발생할 수 있는데, 이는 추가적인 보안 위험을 초래한다.
감사 추적(Audit Trail)과 책임성의 결여	ID와 비밀번호를 기반으로 한 전자서명 방식은 전자 기록에서 특정 작업을 수행한 사용자를 명확히 식별하는 데 한계가 있다. 만약 여러 사용자가 동일한 자격 증명을 사용하거나 타인의 계정을 이용해 작업을 수행한다면, 감사 추적이 복잡해지고, 데이터 조작의 책임을 명확히 하기 어려워진다. 이는 규제 기관의 검토 과정에서 중대한 문제로 이어질 수 있다.
인증 방법의 고정성	기존의 ID와 비밀번호 방식은 고정된 인증 요소를 사용하기 때문에, 상황에 따라 다중 요소 인증(MFA)이나 추가적인 보안 층을 적용하는 데 한계가 있다. 이는 더 높은 보안 수준이 요구되는 GMP 환경에서 필요한 유연성과 적응성을 제공하지 못한다.

이러한 한계로 인해, 기존 ID 방식의 전자서명은 GMP 환경에서 데이터 무결성 요구사항을 충분히 충족시키지 못하며, 더욱 강력하고 신뢰할 수 있는 인증 방법의

필요성이 강조되고 있다. 이를 해결하기 위해, AI 기반 바이오메트릭 기술과 같은 새로운 인증 방식을 도입하는 것이 데이터 보안과 무결성을 유지하는 데 중요한 전략으로 부상할 것으로 예상해 본다.[22, 24-26]

3 장 AI 기반 바이오메트릭 기술

3.1 바이오메트릭 기술의 개요

생체 인식은 개인의 신체적 인식(지문인식, 얼굴인식, 홍채인식, 정맥인식) 또는 행동적 특성(음성인식, 걸음걸이 인식, 행동인식)을 사용하여 신뢰할 수 있는 액세스 제어를 제공하는 일련의 고급 기술이다. 정보 통신 기술의 급속한 발전으로 생체 인식은 특히 인공 지능(AI)의 통합으로 점점 더 중요한 분야가 되었다. 지문 및 얼굴 인식 기술은 AI를 사용하여 크게 향상되었다.[27] AI로 학습된 인증 알고리즘을 통해 생체 인식이 본인임을 증명할 수 있는 결과를 신뢰성 있게 나타내고 있다.

AI 알고리즘은 고급 패턴 인식 및 적응형 의사 결정을 가능하게 하여 IoT 애플리케이션에서 생체 인식 시스템을 개선하는 데 필수적이다. 또한 생체 인식과 AI 및 IoT의 통합은 보안 위험을 완화하여 데이터 및 사용자 개인 정보를 보호하는 데 도움이 될 수 있다.[27]

표 3.1 바이오메트릭 인증 방식 구분

구분	바이오메트릭 인증 방식
신체적 인식	지문 인식, 얼굴인식, 홍채인식, 정맥인식
행동적 특성	음성인식, 걸음걸이 인식, 행동인식

전문 AI 서비스를 준비하는 IT회사가 아닌 이상, AI 인프라를 구성하여, 서비스를 모색하기에는 한계가 있다. 그런 부분을 우린 클라우드로 제공하는 회사로 통해 적은 비용과 빠른 도입을 모색해 볼 수 있다. 최근 전통적인 클라우드 기반의

인공지능 서비스(AI as a Service, AIaaS)가 크게 주목받고 있다.[28]

대표적인 AIaaS 회사이면서 안면인식 서비스로는 AWS(Amazon Web Services)의 Rekognition, GCP(Google Cloud Platform)의 Google Cloud Vision API, Microsoft의 Azure Face API서비스를 대표로 꼽을 수 있다. 이들은 사전 학습된 모델과 도구를 API 형태로 제공한다. [29]

클라우드 서비스를 이용하면 최소한의 인프라 오버헤드로 얼굴 인식 시스템을 배포하고 최적화 시킬 수 있게 된다. [28]

클라우드 AI 서비스를 도입하기 위해서는 서비스. 효율성, 정확성 및 비용에 대해 심도 있게 고민하여 채택을 고민해야 한다.

3.2 안면인식 기술과 인권 문제

AI 안면인식 서비스를 위해서는 사전에 지정된 안면 데이터를 토대로 학습된 데이터를 가지고 있어야 한다. 이는 개인정보 취급에 대한 논란의 여지가 있어 신중하게 접근하여야 한다. 개인정보 활용에 대한 동의가 있어도 해킹사고나 내부직원의 악의적 접근으로 인해 유출 사고가 발생하면 사회적 문제가 발생할 가능성이 높은 기술이 된다. 이외에도 내재된 불안감은 수도 없이 많다.[25, 26, 30]

표 3.2 안면인식기술의 논란 요소

구분	세부 내용
편향성 및	- 인공지능이 학습한 수많은 데이터는 이미 역사적으로 형성된 인종별,

차별성	성별 등 차별적 요소가 내재되어 있어서 근원적으로 편향성 문제를 지님. - 이를 제거하지 못한 채 활용된다면 근거 없는 차별적 요소로 작동할 가능성이 있음. 즉, 안면인식기술은 발전했지만, 여전히 불완전함
	- 안면인식기술을 공공장소에서 사용하는 것은 개인의 사생활을 해할 여지가 높음 - 특히, 민간에서 사용할 경우는 본인의 동의 아래 제한적으로 동의 분야 에서만 사용되어야 하며, 다른 용도로 사용되어서는 안 됨 - 수집 정보 및 저장장치에 대한 관리·보안 책임 주체 명시 필요함

AIaaS를 수행하는 기업들은 이 부분을 해결하기 위해 많은 노력과 비용을 들이고 있으면, Microsoft Azure Face의 경우는 사진을 저장하는 방식 대신, 얼굴을 감지하고 특성을 저장하는 형태로 개인정보를 최소화 시키며 인지를 강화 시키는 노력을 하고 있다.

Azure Face landmarks는 눈동자나 코끝과 같이 얼굴에서 찾기 쉬운 지점을 수집한다. 기본적으로 27개의 이정표 지점이 사전 정의되어진다. 다음 그림8은 Azure Face landmarks에서 활용하는 27개의 기본 이정표를 나타낸다.[31]

이 지점들은 좌표로 기록되어 Detection Master 기준점으로 활용되어, 인지가 필요한 상황에서 명도, 각도, 표정, 안경 등의 특징에 맞게 인식률을 제공해준다.

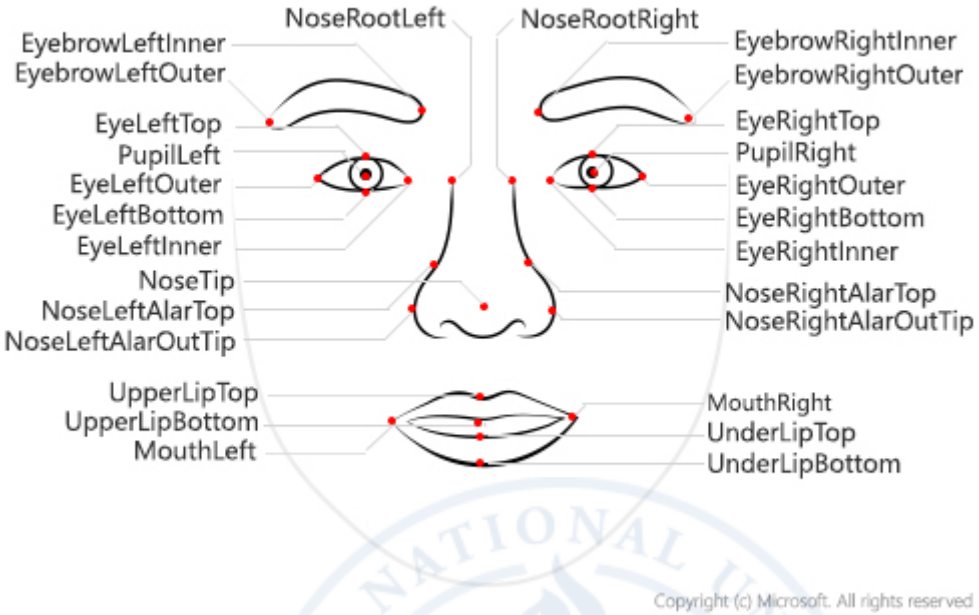


그림 3.1 Azure Face landmarks [31]

4 장 GMP 환경에서의 바이오메트릭 인증

GMP 환경이라 하면, 외부 공기를 차단하여 무균상태를 일정하게 유지하고, 최적의 제조과정을 거칠 수 있는 곳이어야 한다. 오인/잘못된 라벨링, 불순물, 대체제 및 중금속/살충제/미생물 오염과 같은 품질 위험은 제조 공정의 적절한 품질 관리 조치를 통해 충분히 최소화되어야 한다.[4]

따라서, 위한 방법으로 가우닝과 같은 방진복 착용은 필수이며, 출입제한 및 엄격한 통제가 이루어져야 한다.

통제지역에서 활동하는 사람들은 교육을 통한 자격을 갖추고 소독과 청결을 수시로 하기 때문에 행동에 제약이 있으며, 모든 기록을 남겨야 한다. [30]

모든 활동은 긴장을 요구하게 되며, 이로 인한 피로도 누적은 일탈 위험을 높일 가능성이 있다. GMP 활동을 기록하는 GMP 전자시스템이 있다면 항상 마지막은 전자 서명을 통해, 작업을 마무리하게 된다. 모든 활동을 개선할 수 없지만, 바이오메트릭 인증을 통한 전자서명을 적용하게 되면, 효과적일 수 있다.

그림 4.1 GMP ISO 지역 로그 기록 활동과 전자서명

4.1 데이터 무결성 강화 방안

FDA CFR-Part 11에서 전자서명이란 개인이 실행, 채택 또는 승인한 컴퓨터 데이터 편집물로, 기호 또는 일련의 기호로 구성되며 개인의 수기 서명과 법적으로 동등한 효력을 갖는 것을 의미한다고 정의 내렸다.[2, 3]

ID/ PW 는 전자서명의 수단으로 활용 가치가 높다. 다만, Data Integrity가 점차 강화되도록 요청된다면, ID/PW가 갖는 Data Integrity적 약점을 극복할 수 있는 방안이 마련되어야 할 것이다.

이에 대한 방안으로 AI기술 장점을 활용해 전자서명에 도입해 보면, Data Integrity 기준인 ALCOA++ 측면에서 강화되는 부분은 있을 것으로 예상된다. ID/PW 전자서명 약점이 보완될 것으로 보인다. (그림 4.2 Data Integrity-ALCOA++요소매치

참조)

그림 4.2 Data Integrity – ALCOA++ 요소 매치

4.2 GMP 환경에서 AI기술의 장점

인공 지능(AI)은 최근 몇 년 동안 의료를 포함한 여러 산업을 변화시킨 강력한 도구가 되었다. 복잡하지만 반복적인 일에 도움을 주며, 놓치기 쉬운 일을 챙겨 주며, 사람처럼 학습된 상태에서 응용이 가능한 기술이다.

표 4.1 AI기술 장점

장점 요소	장점 상세
오류 감소	AI를 통해, 인간이 갖고 있는 인간적인 실수를 줄일 수 있음.
매일 적용	AI를 통해, 기계적인 꾸준함과 일상사에 다양한 장르에 적용할 수

	있음
디지털 에이전트	AI를 통해, 기억의 한계를 극복할 수 있음. 서로 유기적인 대화를 통해 부족한 부분을 채워줄 수 있음
반복적인 작업	AI는 명확함에 있어서는 오류가 없음. 무한 반복 활동에 대해서 오차가 거의 없음
기술 성장 가속화	기술이 머물러 있지 않고, AI기술은 지속적으로 진화하고 있음

하지만, 신뢰할 수 없는 AI는 오히려 더 큰 부작용이 생길 수 있으므로 플랫폼 선정에 신중을 기해야 한다. 이번 테스트에 사용할 Azure Face API의 성능을 조사해 보았다.[30]

표 4.2 Azure Face API 성능 비교표

Feature	**Azure Face API**	**Open CV Haar Cascade**	**Dlib Face Detector**	**LSTM**
Platform support	Cloud and Edge	Local	Local	Local
Supported image formats	JPEG, PNG, BMP, GIF	JPEG, PNG, BMP,TIFF	JPEG, PNG , BMP	JPEG , PNG
Accuracy	High	Medium	High	Medium
Speed	High	Medium	Medium	Medium
Age and Gender estimation	Yes	No	Yes	No

Emotion detection	Yes	No	No	No
Eye detection	Yes	Yes	Yes	No
Skin color detection	Yes	No	No	No
Facial hair detection	Yes	No	Yes	No
Scalability	High	Low	Medium	Low
Cost	Free, Pay as you go	Free	Free	Free

[26, 32]

4.3 Azure Face API를 활용한 안면인식을 통한 인증

Azure Face API 서비스는 기능에서 Open소스보다 성능이 좋다. 정확도와 속도, 보안을 동시에 고려하여 설계된 알고리즘을 기반으로 동작하며, 다양한 환경에서도 신뢰도 높은 인증 기능을 제공함. [31, 32]

1. 안면 감지 (Face Detection)

- 입력된 이미지에서 얼굴 영역을 식별
- Bounding box로 얼굴 위치를 정의
- 이미지에서 다수의 얼굴 감지 가능하며 각 얼굴의 고유 ID를 할당
- 안면 감지의 정확도를 위해 조명, 각도, 해상도 등의 품질 요인을 고려

2. 안면 특징 추출 (Feature Extraction)

- 감지된 얼굴에서 주요 특징점(landmarks) 추출.
  - 예: 눈, 코, 입의 위치, 얼굴 윤곽선 등
- 특징점 기반으로 고유한 안면 데이터 벡터(Embedding) 생성
- 이 데이터는 사람의 얼굴을 수학적으로 표현하며 비교의 기준으로 활용

3. 데이터 비교 및 매칭 (Face Matching)

- 추출된 안면 데이터 벡터를 사전 등록된 데이터와 비교
- 유사도 점수(Similarity Score) 계산
- 유사도는 0~1 사이의 값으로 반환되며, 1에 가까울수록 동일 인물로 판정
- 임계값(Threshold) 설정: 특정 점수 이상일 때만 인증 성공으로 처리
  - 기본적으로 Azure는 0.5~0.6 이상의 임계값을 권장

4. 안면 인증 결과 반환 (Authentication Response)

- 비교 결과를 호출 시스템으로 반환
- 성공시 - 인증 성공 여부와 매칭된 사용자 ID 반환
- 실패시 - 인증 실패 원인(예: 낮은 유사도, 얼굴 감지 실패 등) 반환
- 처리 속도 최적화로 실시간 인증 지원

5. 안전 및 보안 관리 (Security Management)

- 모든 데이터는 암호화하여 전송(HTTPS/TLS 사용)
- 안면 데이터는 요청 시점에만 사용되며, 지속적인 저장 또는 재사용 불허
- 호출한 클라이언트의 API 인증 키를 통해 권한 확인

Azure Face API 서비스는 여러 가지 전처리(preprocessing) 기술을 사용하여 얼굴 인식 및 분석 알고리즘의 정확도와 효율성이 개선된다. [31, 32]

표 4.3 Azure Face API 전처리 기술

구분	설명
Basic Algorithm	얼굴감지를 위해 합성신경망(CNN)을 사용함
Detection	이미지 정규화, 이미지 정렬, 조명 정규화를 통해 Detection 된 Master Landmarks와 비교를 객관화 함
Filter	노이즈 감소를 위해 artifacts를 제거하고 Gaussian blur, median filter를 적용함
기타 전처리 기술	Principal Component Analysis (PCA), Local Binary Patterns (LBP), Viola-Jones Algorithm, Support Vector Machines (SVMs) 등의 전처리(preprocessing) 작업을 통해, 인식률을 높이고 있다

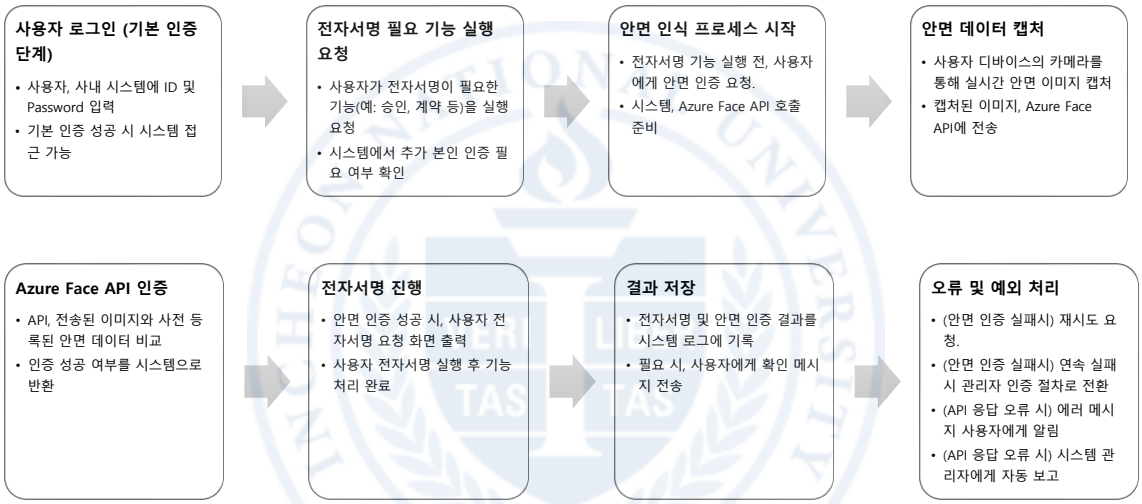
4.4 사례 분석(바이오메트릭 정보를 활용한 공항의 “One ID” 적용)

하나의 사례로 공항에 바이오메트릭 정보를 활용한 “One ID”를 확대하여, 여객 프로세스 뿐만 아니라 공항 면세점 등 쇼핑 결제에 이르기까지 바이오 정보의 이용처가 확대될 전망이다. 이런 움직임은 AI알고리즘에서 나온 결과인 바이오메트릭 정보를 신뢰할 수 있고, 선별 가능하고, 체크인 시간 10%, 탑승시간 40% 정도 절감할 수 있으며, 인력 운영성도 올릴 수 있음을 나타낸다.[33]

4.5 Azure Face API 인증 테스트

4.5.1 전반적인 처리 Flow

사내 시스템에는 기본 인증 체계인 (ID/PW)방식으로 기본 식별을 하고, 전자 서명 필요시, 안면인식을 통해 신뢰도를 높이고자 하는 방식으로 테스트를 진행 하였음



4.5.2 테스트 시나리오

구분	시나리오
CASE 1	① 특정인 홍길동은 ID/PW를 이용해 해당 시스템에 로그인을 한다. ② 로그인 후 자신의 정면 인식 사진을 찍어, 홍길동과 probe 이미지를 마스터로 등록한다. 셋팅을 마친다. ③ 평상시 정면화면 인식율을 확인한다. ④ 마스크를 쓴 정면화면 인식율을 확인한다.
CASE 2	① 특정인 홍길동은 ID/PW를 이용해 해당 시스템에 로그인을 한다. ② 로그인 후 자신의 정면과 상하좌우 5개의 인식 사진을 찍어, 홍길동과

	probe 이미지를 마스터로 등록한다. 셋팅을 마친다. ③ 평상시 정면화면 인식율을 확인한다. ④ 마스크를 쓴 정면화면 인식율을 확인한다.
CASE 3	① 특정인 홍길동은 ID/PW를 이용해 해당 시스템에 로그인을 한다. ② 로그인 후 자신의 정면과 상하좌우 5개의의 인식 사진과 마스크를 쓴 동일 패턴의 사진을 찍어, 홍길동과 probe 이미지를 마스터로 등록한다. 셋팅을 마친다. ③ 평상시 정면화면 인식율을 확인한다. ④ 마스크를 쓴 정면화면 인식율을 확인한다.

4.5.3 Azure Face API 기술적 접근

- Azure Face API 인식 신뢰도 임계치 기준 (Microsoft 제공)

결과치 리턴 기준 값에 따라 나오는 실패 비율이다. 0.1로 설정하면, 구분의 의미가 없을 정도로 신뢰도가 낮아지고, 0.9로 설정하면 신뢰도는 올릴 수 있지만 주변 환경 변수(조명, 각도, 안경, 카메라 품질, 마스크 착용 등)에 따라 효용성이 떨어질 것으로 예상된다.

지금 기본 임계 값은 0.5 (10만분의 1)로 셋팅 되어 있다. 언제든지 임계 기준을 바꿀 수 있다. (이번 테스트에는 기본 값으로 수행 하였음)

표 4.4 신뢰도 임계 기준에 따른 성공 확률 표본

Recognition Confidence Threshold	**거짓 긍정 비율(False Positive Rate)**
0.1	1 / 10
0.2	1 / 100

0.3	1 / 1,000
0.4	1 / 10,000
0.5	**1 / 100,000**
0.6	1 / 1,000,000
0.7	1 / 10,000,000
0.8	1 / 100,000,000
0.9	1 / 1,000,000,000

- **인식 방향성**

사전에 등록된 Probe Landmarks와 대조를 위해서는 현재 시점에서 촬영된 이미지가 중요한데, 얼굴을 대조군과 상하좌우를 정확하게 카메라로 재현해서 인식결과를 올리는 것은 불가능에 가깝다. 35도 이내의 상하좌우 변화에는 인식률에 큰 변동이 없음을 알 수 있다. [34] 검증(Verification)과 인증(Authentication) 과정에서 두 개념의 특성과 차이를 이해 할 필요가 있음. 검증(Verification)은 사전에 등록된 Probe Landmarks 비교 데이터 안에 해당 정보가 있는지 여부를 가리는 것이고, 인증(Authentication)은 검증된 정보가 특정 지을 수 있는지 여부를 가리는 것이다.

표 4.5 Verification과 Authentication 차이점

	Verification	**Authentication**
대상	Lands Marks 정보안에 대상이 있는지 확인	대상이 기존 AD(Active Directory)안에 있는 대상자 특정
목적	Face 정보 매칭 확인	신원 정보 특정
사례	신원 정보 확인, 얼굴 매칭	로그인, 권한 부여

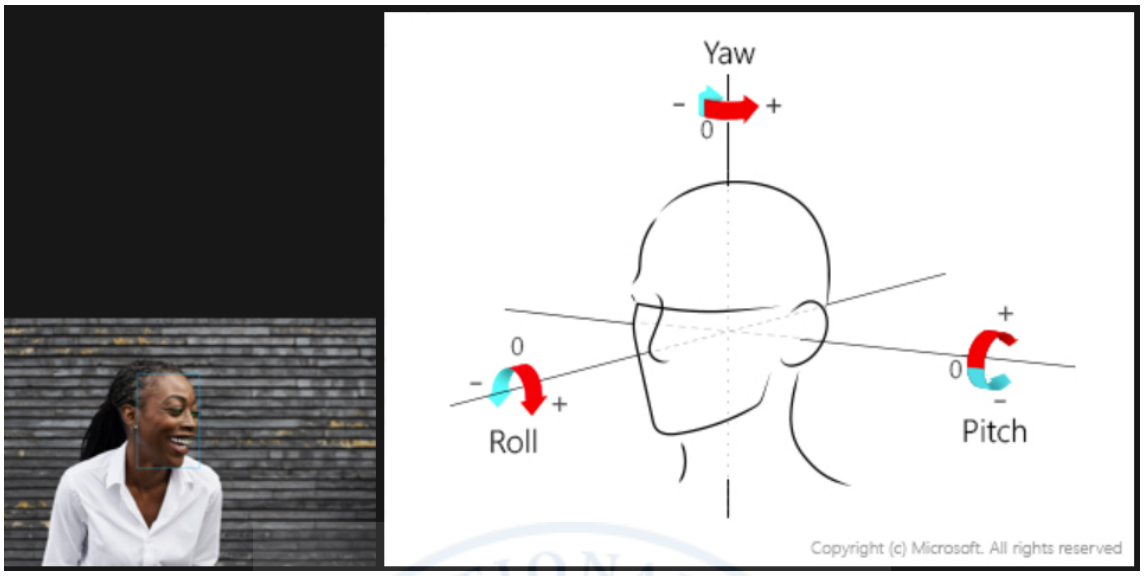
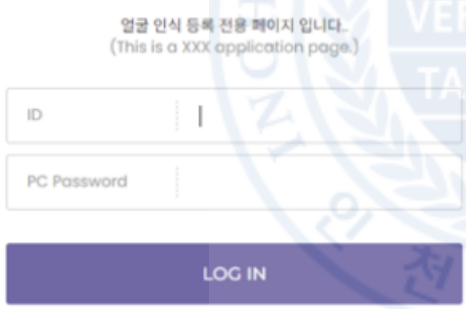
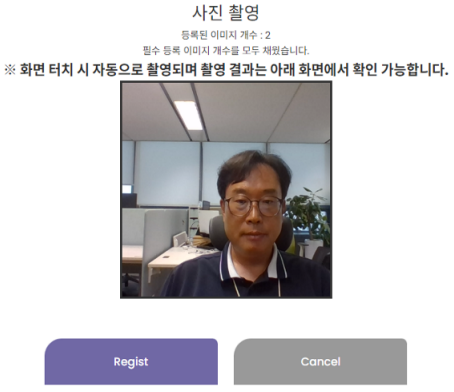
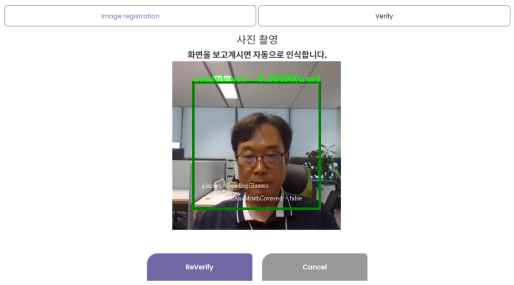
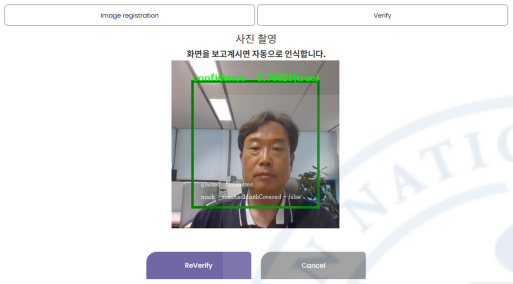


그림 4.3 Azure Face API 각도별 허용 인식률 [31]

4.5.4 실제 테스트 진행

	ID / PW로 로그인 하여, 이미 저장된 기본 정보에 얼굴 정보를 추가한다
	촬영을 진행하고 ID + Face landmarks 정보를 기록한다.

	Verify-Authentication 준비 과정을 통해, 인식률(Facial recognition rate)을 테스트해본다. (정상적인 환경에서 Verify 0.9 이상 일치율을 보임) Verify 후 해당인을 특정 시킬 수 있는 Authentication 매칭을 한다
	안경을 벗은 상태에서 인식률은 0.7 일치율을 보임

위와 같은 절차로 총 8명을 대상으로 테스트를 진행하였다.

동일한 조명과 동일한 노트북 카메라, 안정적인 공간에서 진행하였음.

특징	**구분1**	**구분2**
성별 (8)	남자 : 7	여자 : 1
안경 착용 여부 (8)	착용 : 3명	미착용 : 5명
연령 (8)	30대 : 6명	40대 : 2명

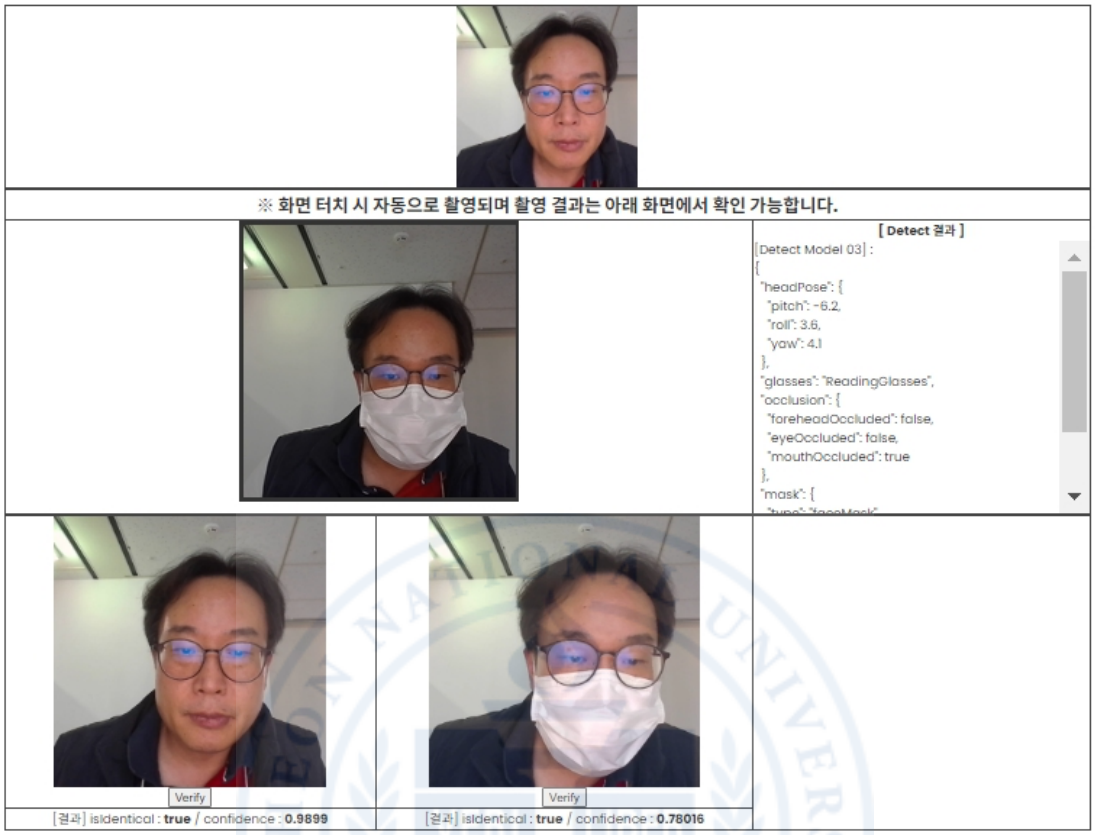


그림 4.4 CASE 1 결과 예시

Face Landmarks 가 1개일 경우,

- 일반적인 인식률은 0.98로 거의 일치하는 결과로 나옴
- 마스크로 코 아래를 가렸을 경우, 0.78의 결과로 임계치인 0.5를 넘어서 True 값을 반환함

그림 4.5 CASE 2 결과 예시

Face Landmarks 가 5개일 경우,

- 일반적인 인식률은 0.95로 결과로 나옴. CASE 1보다 인식률은 근소하게 떨어졌지만 신뢰할 수 있는 범위내에 있음
- 마스크로 코 아래를 가렸을 경우, 0.76의 결과로 임계치인 0.5를 넘어서 True 값을 반환함

그림 4.6 CASE 3 결과 예시

Face Landmarks 가 10개일 경우,

- 일반적인 인식률은 0.95로 결과로 나옴
- 마스크로 코 아래를 가렸을 경우, 0.90의 결과로 CASE2 보다 인식률이 높아졌음

그림 4.7 참여자 CASE 3 결과 화면

표 4.6 실제 테스트 결과표

행 레이블	평균 : NORMAL	평균 : MASK
CASE1	**0.98**	**0.80**
User1	0.98	0.76
User2	0.98	0.87
User3	0.99	0.90
User4	0.97	0.89
User5	0.94	0.67
User6	0.98	0.71
User7	0.99	0.80
User8	0.98	0.78

CASE2	**0.96**	**0.82**
User1	0.97	0.76
User2	0.96	0.90
User3	0.98	0.91
User4	0.97	0.89
User5	0.94	0.62
User6	0.95	0.78
User7	0.98	0.88
User8	0.95	0.78
CASE3	**0.96**	**0.90**
User1	0.96	0.90
User2	0.95	0.93
User3	0.98	0.94
User4	0.97	0.93
User5	0.94	0.75
User6	0.98	0.88
User7	0.97	0.94
User8	0.90	0.95
총합계	**0.97**	**0.84**

8명의 CASE 세가지 평균, 마스크 착용시 0.84, 일반상황 0.97의 일치율을 보임임

시사점 :

- 마스크로 인식해야 하는 경우가 많을 시에는 마스크 착용 Face Landmarks를 보유하는 것이 좋다.
- Face Landmarks를 많이 보유하면 인식율이 오히려 소폭으로 감소하고 상하좌우의 Face Landmarks는 불필요함
- 성별, 연령, 안경 착용여부는 인식률 차이가 없었음
- 감정 표현이나 얼굴 일그러짐은 인식율에 영향을 주지 않음
- FACE 인식으로 ID/PW를 완전 대체는 힘들 수 있으나, 보조 수단으로서 가치는 충분함을 증명함

5 장 결론

5.1 연구 결과

본 연구를 통해 AI 기반 생체인식 전자서명 시스템이 GMP 데이터 무결성 강화에 효과적임을 확인하였음. 주요 결론은 다음과 같음.

- AI 기반 생체인식 기술을 활용한 전자서명은 기존의 ID/PW 기반 전자서명에 비해 보안성과 신뢰성이 향상될 것으로 예상됨.
- 생체인식 기술은 개인을 고유하게 식별할 수 있어 GMP 규정에서 요구하는 전자서명의 요건을 충족시킬 수 있음.
- 생체인식 기술을 결합한 전자서명 시스템은 작업 효율성을 높이고 안전성을 개선하는 데 기여 가능성 있음.
- AI 기술의 도입으로 생체인식 데이터의 정확성과 신뢰성이 향상되어, Data Integrity 보장에 기여할 것으로 예상함.
- 본 시스템을 GMP에 반영시키기 위한 CSV 방법론으로 GAMP-5 지침을 준수하여 제약 산업의 컴퓨터 시스템 검증 요구사항을 충족시킬 수 있음.

이러한 결과는 제약 산업에서 AI 기반 생체인식 전자서명 시스템의 도입이 GMP 데이터 무결성을 강화하고 규제 준수를 개선하는 데 효과적인 솔루션임을 증명함. 향후 연구에서는 다양한 생체인식 기술의 비교 분석과 장기적인 영향 평가가 필요함.

5.2 향후 연구 방향 및 제언

본 연구에서는 GMP 환경에서 데이터 무결성을 높일 수 있는 방안을 AI

기술과 함께 찾아보았다.

사람을 치료하는 치료제 생산은 안전 보장을 위해 까다로워야 하며, 보수적이어야 한다. 생산 과정에서 산출되는 데이터와 정황들은 객관성이 증명되어야 한다.

가장 안정적인 시스템을 뽑으라고 하면, Paper System을 손 꼽을 수 있다. 서버가 다운될 염려도 없고, 네트워크가 끊겨 전자 시스템을 못쓰는 경우도 없다. 하지만, 효율 저하와 관리 부담이 크기 때문에 전자 시스템으로 상당부분 전환이 되었고, 점차 늘어나는 추세이다. 전자 시스템의 객관성 증명을 위해 전자서명이란 이름으로 ID/PW 방식이 주로 쓰이나 이는 Data Integrity 측면에서 부족한 부분이 존재한다. 앞으로 많은 GMP Process가 전자화가 될 예정이고 이는 지속적인 고민거리가 될 것으로 예상된다.

FDA, EMA등의 국가 허가 기관의 결과에 따라 케미컬 바이오 치료제 회사 주가에 영향을 미친다.[5] 허가 기관들은 Data Integrity에 대한 감시가 강화될 것이고 데이터 객관성 증명 강화를 요구할 것이다. 제조사들은 대응 방안을 모색할 것이다. 그 선택지 중 하나가 AI를 활용하는 것이다. AI를 활용한 바이오메트릭 인증이 ID/PW를 완전 대체하기 힘들 것이다. AI를 활용한 바이오메트릭 인증이 GMP 시스템에서 완전 대체되어 보편화되기 까지는 시간이 걸릴 것이다. 다만, ID/PW를 보완하는 형태로 시작을 해서 점차 확대될 가능성은 있어 보인다.

GMP ISO 지역에서의 Gowning은 안면인식에 큰 장애물이 될 것이다. 그리고 쌍둥이 분별과 변장을 통한 접근을 걸러내는 기술은 안면인식에서 풀어야 할 숙제로 보인다. AI를 통한 바이오메트릭 인증에는 Voice 인식과 홍채인식 등의 대안이 있다. 이를 효과적으로 활용할 수 있는 연구는 지속될 필요가 있다.

참 고 문 헌

[1] 한국식약처, "식약처_첨단바이오의약품+ 데이터+ 완전성+ 안내서_2024." www.mfds.go.kr

[2] FDA Gov, "CFR - Code of Federal Regulations Title 21."

[3] Wikipedia, "Title_21_CFR_Part_11"

[4] 임찬표, 2022, "의약품 제조관리에서의 데이터 완전성 위반 유형 분석", *국내석사학위논문 Thesis*, 성균관대학교 일반대학원, 서울.

[5] He, T., Ung, C. O. L., Hu, H. and Wang, Y. (2015). "Good manufacturing practice (GMP) regulation of herbal medicine in comparative research: China GMP, cGMP, WHO-GMP, PIC/S and EU-GMP." *European Journal of Integrative Medicine*, 7(1), pp. 55-66.

[6] Heejung Lee"미국의 국가식품안전관리체계 평가 사례연구." *Journal of Food Hygiene and Safety*.

[7] McDowall, R. D. (2010). "Understanding and Interpreting the GAMP 5 Life Cycle Models for Software." *Spectroscopy*, 25(4), pp. 22-31.

[8] Martin, K. C. and Perez, A. (2008). "GAMP 5 quality risk management approach." *Pharmaceutical Engineering*, 28(3), pp. 24.

[9] Kevin C. Martin and Dr. Arthur (Randy) and Perez"GAMP5 Quality Risk Management Approach." .

[10] Chris Clark, Heather Watson, et al., “GAMP 5 Guide 2nd Edition”, ISPE.

[11] 임지혜, 2022, "제약회사에서의 Data integrity 준수를 위한 컴퓨터화 시스템 운영 방법 연구", *국내석사학위논문 Thesis*, 연세대학교 대학원, 서울.

[12] 이종현, 2023, "FDA cGMP 평가항목별 지적사항에 관한 연구", *국내석사학위논문 Thesis*, 성균관대학교 일반대학원, 서울.

[13] 지상용, 2017, "GMP 인증의 CSV 수행 방법론에 관한 연구", *국내석사학위논문 Thesis*, 국민대학교 비즈니스 IT 전문대학원, 서울.

[14] FDA Gov(2018). "Data Integrity and Compliance With Drug CGMP."

[15] Anurag S. Rathore, Yuexia Li, Hemlata Chhabra and Akshat Lohiya"FDA Warning Letters: A Retrospective Analysis of Letters Issued to Pharmaceutical Companies from 2010–2020." .

[16] Ben Locwin"FDA Inspections & Compliance Trends(A look back at 2023 and what 2024 will bring)." *https://www.contractpharma.com/*.

[17] Bang, Y., Lee, D., Bae, Y. and Ahn, J. (2012). "Improving information security management: An analysis of ID–password usage and a new login vulnerability measure." *International Journal of Information Management*, 32(5), pp. 409–418.

[18] A. Conklin, G. Dietrich and D. Walz, 2004, "Password-based authentication: a system perspective." *37th Annual Hawaii International Conference on System Sciences*, 2004. Proceedings of the, pp. 10 pp.

[19] Zaware, S., Chachra, M., Hedaoo, K., Pol, R. and Singh, A. (2024). "Face Recognition based Smart Attendance System using Cloud Computing." , pp. 895–900.

[20] Yadav, S., Singh, A., Singhal, R. and Yadav, J. P. (2024). "Revolutionizing drug discovery: The impact of artificial intelligence on advancements in pharmacology and the pharmaceutical industry." *Intelligent Pharmacy*, 2(3), pp. 367–380.

[21] Bagwani, M. K., Tiwari, V. K., Chouhan, D. K. and Jain, A."Optimizing Face Detection Performance with Cloud Machine Learning Services." .

[22] Awad, A. I., Babu, A., Barka, E. and Shuaib, K. (2024). "AI-powered biometrics for Internet of Things security: A review and future vision." *Journal of Information Security and Applications*, 82, pp. 103748.

[23] 이용, 장래영, 박민우, 이상환 and 최명석 (2020). "인공지능 서비스(AIaaS) 기술 동향과 활성화 방안." *정보과학회지*, 38(8), pp. 49–57.

[24] 조병선 (2022). "클라우드와 AIaaS 서비스 동향." .

[25] Microsoft, "Azure Face detection, attributes, and input data." . *learn.microsoft.com*

[26] Lechanteur, C., Briquet, A., Bettonville, V., Baudoux, E. and Beguin, Y. (2021). "MSC manufacturing for academic clinical trials: from a clinical-grade to a full GMP-compliant process." *Cells*, 10(6), pp. 1320.

[27] Y. Duraisamy, S. Priya.S, S. S. Alnuaimi and S. K. R, 2024, "Bringing Them Home: The Role of Azure Face API in Finding Missing Person." *2024 5th International Conference on Mobile Computing and Sustainable Informatics* (ICMCSI), pp. 71-76.

[28] 이수경 (2024). "공항 생체인식기술의 지속이용의도와 프라이버시 염려의 조절효과에 관한 연구 - 후기기술수용모델(Post-Acceptance Model)을 기반으로 -." *한국항공경영학회지*, 22(2), pp. 25-51.

[29] wguyman, eric-urban, kcpitt, PatrickFarley, v-alje, lucia-msft, michaelamoako"Characteristics, limitations, and best practices for improving accuracy." Microsoft.

ABSTRACT

Research on the application of electronic signatures using AI biometrics to increase GMP Data Integrity

SangHoon, Ahn

Department of Computer Engineering

Incheon National University

Lately, the FDA and the EMA, the regulatory organizations, have asked for stronger requirements regarding 'Data Integrity'. In this situation, it is necessary to guarantee 'Data Integrity' in the medicine production and GMP. This research searches for the way to raise Data Integrity through the technology of face recognition utilizing Azure Face API. The technology of face recognition based on AI can reinforce the Internet users' identification process and if it is included in and applied to the electronic signature procedure, credibility and security of the authentication are expected to improve. In this thesis, the technology has been tested by using Azure Face API, and the way to make up for GMP electronic signature process has been suggested. Also, it has been proved that biometric techniques based on AI can be effective tools to work out the Data Integrity problems. Through this treatise, I suggested the solutions to complementing and overcoming the limits of preexisting signature process, and responding to any matters regulatory organizations point out

Key Words : GMP, Data Integrity, Biometrics, GAMP5, Electronic Signature, Facial Recognition