# 차세대 웹 환경에서 다중요소 MFA (Multi-Factor) 사용자 인증 동향 분석

이재형 (옥타코(주)), 강민구 (한신대학교)

## 1. 서 론

최근, 차세대 웹 환경에서 사이버 보안은 사용자와 네트워크를 통제하기 위한 접근통제, 데이터 비밀번호 암호화 기반의 데이터 통제 형태로 보안을 제공하고 있다. 이러한 환경에서 다양한 디바이스가 플랫폼에 접근하는 클라우드 업무 환경이 이루어지고 있다.

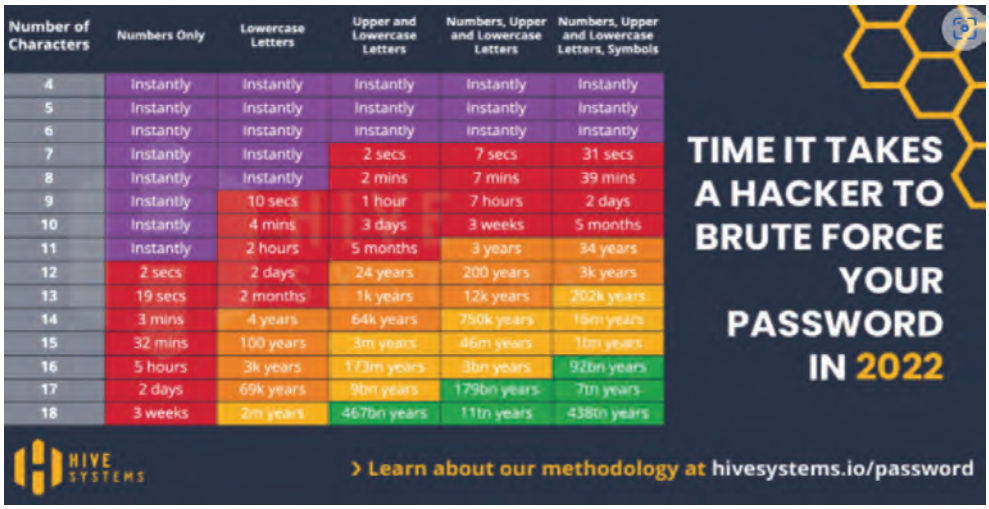
코로나 19이후 디지털 전환에 의한 재택근무, 원격근무 환경 구축 등이 가속화되고, 언제 어디서나 업무를 수행할 수 있는 클라우드 환경에서 차세대 웹의 보안 취약성이 더욱 증가로 인한 사이버 공격 방법도 빠르게 진화하고 있다.

또한, 미국과 중국의 대립으로 잦은 사이버 공격에 유연하게 대응할 수 있도록 사용자 환경을 인지한 인공지능 기반 적응형 다중요소 사용자 보안 인증으로 신원을 증명하는 제로 트러스트 기반 적응형 보안 인증 접근 관리(IAM, Identity and Access Management)의 필요성이 대두하고 있다.

이로서, 본 연구에서는 사용자 환경 변화에 따른 다양한 적응형 다중요소 MFA (Multi-Factor) 보안 인증이 내부 자산 보호를 위해 클라우드 보안 플랫폼에 대한 접근 권한을 부여하는 활용분석으로 차세대 웹3.0의 지능형 MFA 사용자 인증의 활성화를 기대한다.

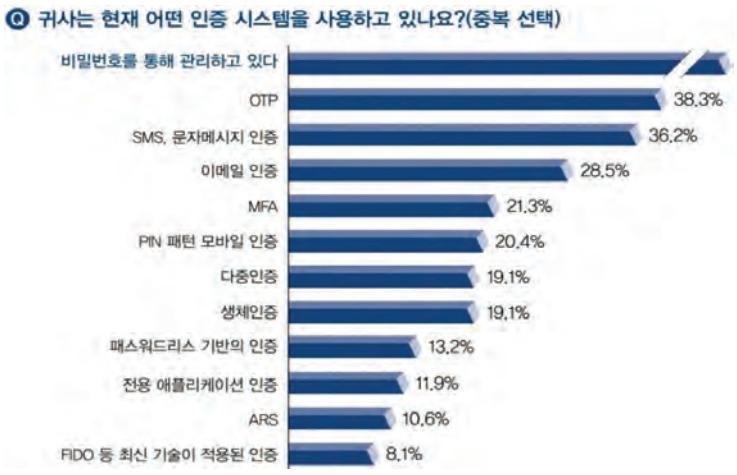
## 2. 웹3.0 환경에서 제로트러스트 사용자 인증

'시한폭탄'된 비밀번호는 보안성에 편리성 높인 차세대 인증 기반의 웹3.0 환경에서 타인도용과 유출사고를 방지하기 위한 필요성이 급증하고 있다. 보안뉴스의 [설문조사] 결과로 비밀번호 72.8%, OTP 38.3%, SMS 및 문자메시지 36.2% 순으로 인증 플랫폼을 사용하고 있다. 그 동안 인증방식으로 1세대 비밀번호이고, 2세대는 PKI 기반의 공인인증서와 OTP, 3세대는 다중요소 MFA 인증과 Passwordless FIDO(Fast ID Online) 통합 인증 등이 있다[2].

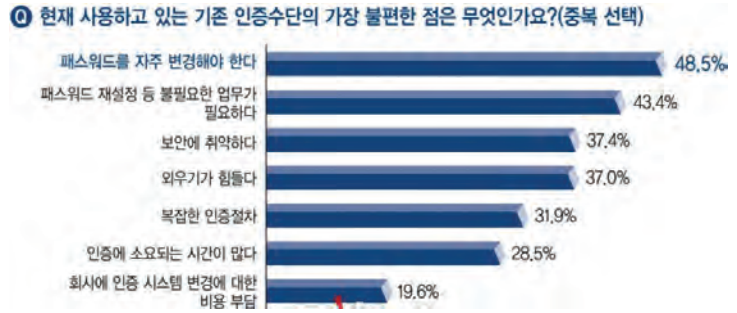



〈그림 1〉 비밀번호 조합별 해독에 걸리는 시간(문자 등의 숫자) 비교분석

출처: Hivesystems




〈그림 2〉 차세대 인증인식 및 선택기준에 대한 설문조사 중 현재 사용 중인 인증 플랫폼 설문 [2]




〈그림 3〉 기존 인증 플랫폼에서 가장 불편한 점은 무엇인지에 대한 설문조사 결과[2]

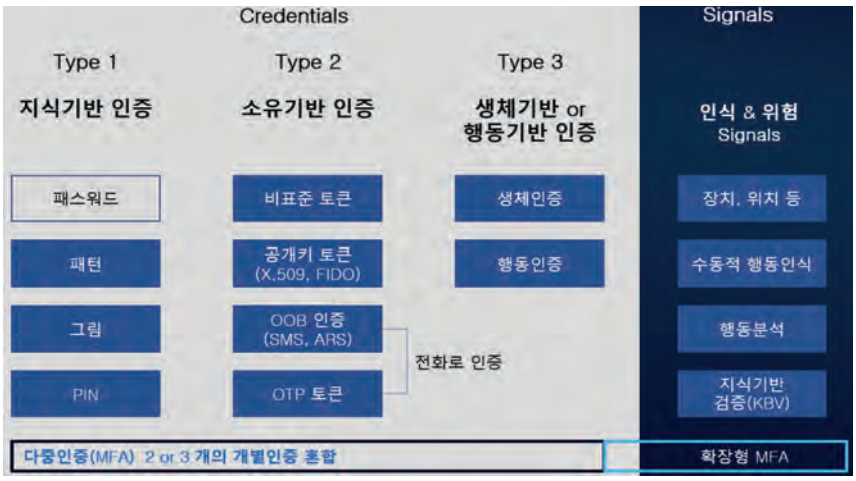
1세대: 1970년대 등장한 비밀번호, '시한폭탄'[2]
(비밀번호는 4자리 숫자 조합에서 영문, 특수문자로 확대, 자릿수는 8자리, 10자리 이상)

2세대: 공인인증서 & OTP(일회용 비밀번호, One Time Password) '양대 산맥'[2]
(공인인증서, '전자서명법'에 '전성시대 맞이', 그러나 액티브엑스가 '보안 홀')
(OTP, 사용자 불편과 번거로움돠 취약점 이슈)

## 2.1 차세대 사용자 인증 제로트러스트와 Passwordless FIDO 국제표준 연계

3세대 사용자 인증은 단일요소 인증(SFA, Single Factor Authentication)보다 사용자 환경과 중요도에 따라 여러 인증수단을 혼용하는 다중요소 인증 MFA가 대세로 발전되고 있다.

〈그림 4〉처럼 사용자 인증은 신호 기반과 크레덴셜 기반의 방법이 있다. 크레델셜 기반은 지식기반(Password, PIN 코드 등)과 소유기반(휴대폰 SMS,




〈그림 4〉 사용자 환경과 중요도에 따라 여러 인증수단을 혼용하는 다중요소 인증 MFA 비교[3]

| 공격 유형 | 패스워드 | SMS | 이메일SMS인증 | OTP | 모바일 FIDO 생체인증 | PC FIDO 생체인증 | H/W FIDO 지문 보안키 |
|---|---|---|---|---|---|---|---|
| 비밀공유 | X | X | X | X | O | O | O |
| 비밀 중앙저장 | X | O | O | O | O | O | O |
| 중간자공격 | X | X | X | X | O | O | O |
| 스미싱 | X | X | X | O | O | O | O |
| 스푸핑 | X | X | X | O | O | O | O |
| 피싱 | X | X | X | O | O | O | O |

* 다양한 해킹 공격 방법 조합으로 OTP 인증 방어력에 대한 일부 다른 의견이 있을 수 있습니다.

〈그림 5〉 보안을 위해 설계되지 않은 인증 수단(Phishable vs Phishing resistance MFA) 비교[3]

보안카드, OTP, 인증서 등), 신체적 특징기반(지문, 얼굴, 홍채 등) 및 신체적 행위기반(수기 서명, 위치・시간・행위 패턴, 키보드 입력 등) 등 사용자의 신원을 인증하는 방법이 있다[2].

차세대 대표적 기술인 FIDO(Fast Identity Online)는 국제표준 기술로 비밀번호를 대체 하는 여러 인증수단을 하나의 플랫폼에서 사용할 수 있는 통합인증 MFA 기술이다. FIDO2는 WebAuthen과 CTAP(Client To Authentication Protocol)로 구성된 최신 표준이다.

생체인증기술 국제표준화기구는 FIDO 규격 외에 'ISO/IEC JTC1 SC37'이 있다. 국내에서 '바이오인식플랫폼 성능 시험인증'은 한국인터넷진흥원(KISA)과 TTA 등이 시험 기준을 수행하고 있다. 또한, Passwordless FIDO 등의 다중요소 인증 MFA는 차세대 웹과 연동하여 IoT 보안, 5/6G, 스마트카 자율주행・메타버스 등 제로트러스트 정보보호 정책 및 제도에 따라 차세대 '사용자 인증'이 등장과 활용 범위 및 기술이 확대될 것이다[2].

## 2.2 FIDO 기술 기반 국제표준 차세대 인증과 제로트러스트 메타버스 적용

기존 인증수단은 차세대 웹 3.0에서 주요 보안 위협 문제로 부실한 비밀번호 관리와 보안에 취약한 공인인증서의 보안 대책으로 국내외 사용자 인증 기업 들의 인증수단에서 보안의 취약점과 보안 위협 대책 및 기업 들의 인식을 고취하는 방안으로 제시되고 있다.

### (1) 비밀번호와 OTP 인증, 타인 도용 및 유출 위험 요소 파악[2~4]

현재 인증수단인 비밀번호와 OTP 인증은 비밀번호를 공유하는 구조로 한쪽이 보안을 잘해도 다른 한쪽이 해킹될 가능성이 있다. 아이디・비밀번호 및 OTP는 숫자 또는 코드이며, 인증할 때도 코드 등 단일요소만 인증한다. 이때, 비밀번호만 알면 누구나 인증이 가능해져서 관리자의 인증정보가 유출되는 해킹의 피해가 될 수 있다.

### (2) 인증수단 탈취・공유와 OTP 유실 및 크리덴셜 스터핑 등 보안 위협의 대책[2][5]

### (3) 메타버스 아바타와 연동하는 생체기반 다중요소 MFA 및 제로트러스트 인증

차세대 웹3.0의 메타버스 환경에서 아바타의 본인 인증방식은 아바타 보안의 경우 정당하지 않은 자가 타인 행세를 할 경우 금융과 물품 거래의 피해를 예방하기 위해서는 메타버스 속 사용자 인증은 분산화되고, 다양한 이종의 플랫폼을 초월한 생체인증 중심의 차세대 사용자 인증방식이 도입되어야 한다.


〈그림 6〉 사용자 인증 보안을 위한 다양한 인증 수단 MFA 요소분석[3]

〈표 1〉 기존 인증수단의 보안 취약점과 위협, 기업 문제점 및 대책

| 보안 위협 | 보안 대책 |
|---|---|
| 사용자 인증의 시작인 로그인에서 인증수단 탈취 및 공유, OTP 기기 유실, 크리덴셜 스터핑(Credential Stuffing) 보안 위협 | 생체 정보 기반 사용자 인증 기반 탈취 및 유실을 방지, 사용자 개입을 최소화하고, 패스워드리스 정책 준수 |
| 보안 업무 플랫폼 접근의 경우 휴면계정, 이상 행위, 만료 계정 미관리, 정책 설정 오류, 과도한 권한 부여 등 보안 위협 | 통합 계정관리 및 접근제어를 통해 계정 라이프사이클 관리, 이기종 계정 동기화, 최소 권한 설정으로 계정 관리 |
| 작업수행 시 데이터베이스 관리자인 DBA(Database Administrator), 개발자의 고의 · 실수 발생으로 연결 세션으로 단말 조작 및 권한 탈취, 작업 화면 유출 위험 | 사용자 행위 검증/차단, 명령어 단위 권한 제어, 외부자 해킹 시도를 차단, 카메라 촬영/훔쳐보기 공격인 Shoulder Surfing Attack 등 비주얼해킹차단 |
| ID · PW 기반 인증의 접속자가 인가자인지 판단불가, 중요 · 금지 명령어 실행 시 재인증 절차없어 제3자접속, 기기 조작사고 | ID 인증 체계 구현 솔루션, 핵심적인 보안 전략 '패스워드리스', '제로 트러스트'(FaceLocker,Unified-IAM) |

출처 : https://pnpsecure.com/


〈그림 7〉 노출된 사용자 인증과정에서 해킹 사례분석[3]

탈중앙화 신원인증 기반의 메타버스 속 사용자 인증에서도 사용될 것이다. 메타버스는 스마트폰과 이기종 디바이스 기반의 클라우드, 네트워크, 플랫폼 등이 융합된 구조로 종류 별로 다양한 인증기술의 차이를 극복하기 위한 상호인증이 가능한 공동 플랫폼이 필요하다.

이때, 메타버스 사용자가 아바타와 연동하게 되는 모션이 'Man-Machine/Brain-Computer 접속'하는 사용자 인증이 기존 지식기반 인증이나 소유기반 인증보다 생체기반 다중요소 MFA인 차세대 인증방식으로 구성해야 보안성이 강화된다.

## 3. 다중요소(MFA) 사용자 인증과 활용

다중요소 인증 MFA은 사용자가 인증 요소를 두 가지 이상 사용해 자신의 사용자 인증을 확인으로 서로 다른 인증 요소를 2가지 이상 혼용해야 한다. 하나는 일반적으로 알고 있는 사용자 이름과 비밀번호이고,


〈그림 8〉 메타버스 연동형 다중요소 MFA 인증설계 위한 고려사항 사례분석[3][11]


〈그림 9〉 차세대 다중요소 MFA인증과 연동하는 앱 구성도 사례 분석[3]

나머지 하나는 가지고 있는 것 또는 신체(생체) 정보를 활용한다.

이러한 사용자 이름과 비밀번호 조합 및 두 번째 다중인증 요소를 추가하는 제로트러스트 (ZeroTrust) 기반의 사용자 확인 등으로 개인정보를 보호하게 된다[8].

* 가지고 있는 것 : 휴대 전화, 키 카드, USB 등이 모두 사용자 신원을 확인함
* 신체 정보 : 지문, 홍채 스캔, 기타 생체인식 데이터가 사용자 신원을 확인함

### 3.1 차세대 MFA 사용자 인증 운영과 Passwordless 통합계정의 인증관리 플랫폼

국내외 인증(Authentication)방식에서 해킹을 탐지하는 Cloud Native Continuous Adaptive Trust 기반의 Passwordless 통합계정의 인증관리 플랫폼은 접근관리 서비스와 사용자 환경에 따른 인공지능 기능을 탑재하게 된다. 이러한 사용자 인증 플랫폼은 국제표준 보안인증 프로토콜 기반의 지능형 MFA를 적용하여 차세대 사용자 인증의 Identity and Access Management 서비스의 중요한 구성요소로 작용한다.

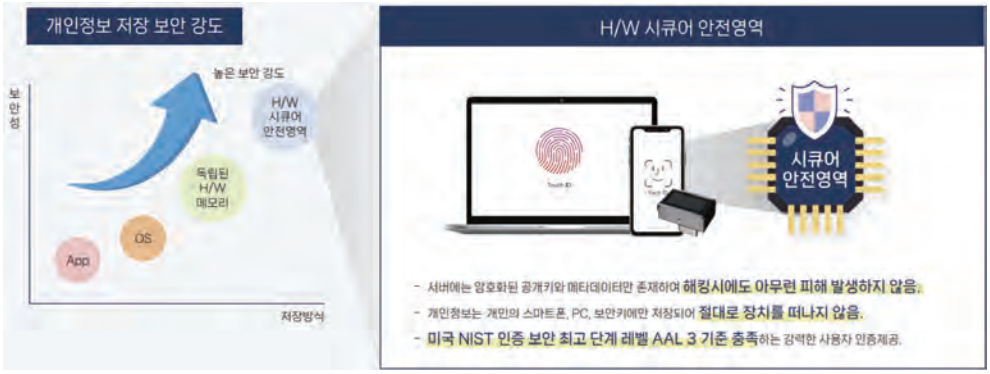
웹3.0 환경에서 차세대 MFA 플랫폼은 사용자 이름과 강력한 인증 수단을 제공하며, 지속적으로 인증 방법을 추가하여 계층화된 권한을 가진 사람만 액세스를 허용하고 공격자를 차단할 수 있게 된다. 이때, 다중요소 MFA에 의한 사용자 인증 절차는 다음과 같다[8].

① 등록 : 사용자가 휴대 전화 등 하드웨어를 플랫폼에 연결하고 사용자 등록
② 로그인 : 사용자가 사용자 이름과 Passwordless 기반 인증으로 플랫폼 로그인 시도
③ 확인 : 다중요소 MFA 플랫폼에 등록된 하드웨어 연결 후, 생체인증과 디바이스 동시 확인
④ 대응 : 사용자가 확인된 하드웨어로 사용자 생체 인증 완료

### 3.2 제로 트러스트 기반의 MFA 사용자 인증 연동 활용

2021년 5월에 바이든 대통령은 정부 컴퓨팅 플랫폼에 제로 트러스트를 의무화하는 행정명령 으로 연방


〈그림 10〉 제로트러스 기반 다중요소 MFA 사용자 인증 사례 분석[3]

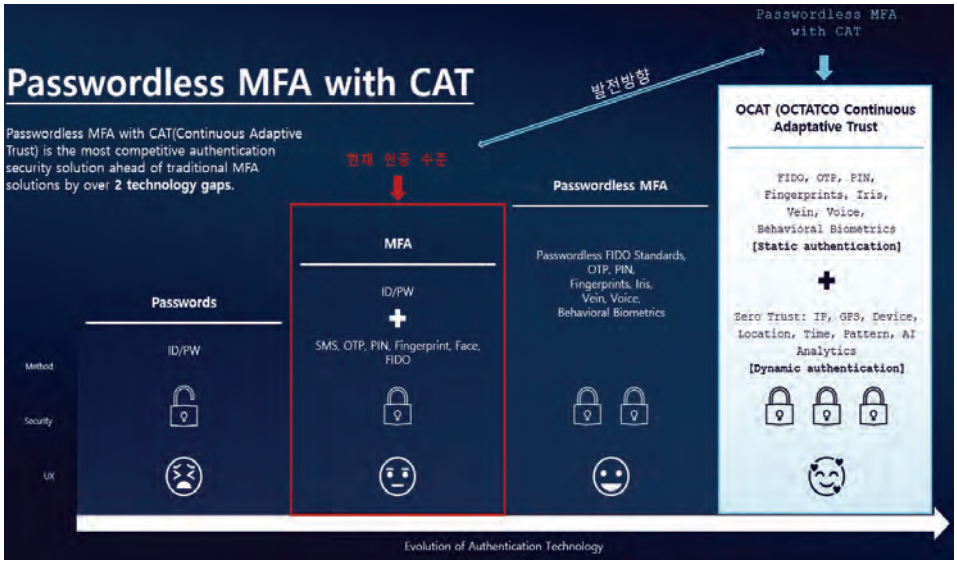



〈그림 11〉 HW 안전(Secure)영역에 다중요소 MFA 사용자 인증 정보저장 사례 분석[3]

기관들은 NIST 권고 사항에 기반으로 제로 트러스트 아키텍처를 도입하였다. 또한, 보안 침입의 사례에 따라 안전위원회는 일부 소비자 제품에 사이버 보안 경고 라벨을 부착하는 프로그램 등을 추가하였다. 이로서 제로 트러스트가 사이버 보안의 핵심으로 자리잡게 되었다.

사용자 인증에 따라 단일 네트워크는 최소 권한 접근 정책으로 네트워크 보안에는 각각의 엔드포인트는 초세분화(microsegmentation) 네트워크 세분화를 해야 한다. 제로 트러스트 사용자들은 보호 중인 각각의 리소스에 대한 접근을 별도로 요청하고, 이때 컴퓨터 디바이스에 암호키를 제공하고 스마트폰으로 암호키를 보내는 등의 다중 인증 MFA 방식이 적용해야 한다.

〈그림 12〉는 연속적인 적응형 트러스트(continuous adaptive trust, CAT) 보안 전략인 디바이스 ID와 네트워크 ID, 지리 위치 등의 맥락 데이터를 사용자 인증을 실행하게 된다. 〈그림 13〉은 원격 사용자 인증을 위한 MFA와 AM(Access Management) 연동방식을 분석하고 있다.

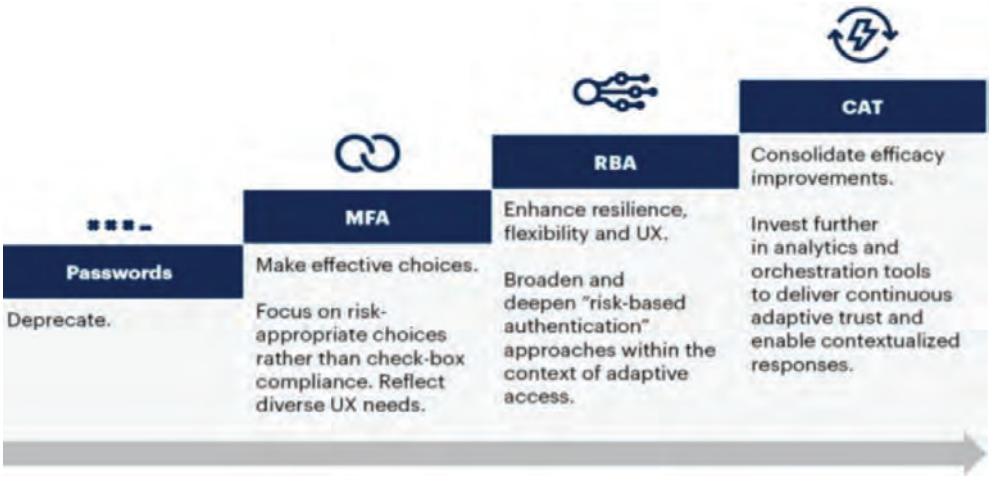



〈그림 12〉 연속적인 적응형 트러스트(CAT, Continuous Adaptive Trust) MFA인증 사례 분석[3]

〈표 2〉 글로벌 통합인증 서비스 제공 업체의 사용자 인증 비교표

| 업체명 | 특징 | 차이점 |
|---|---|---|
| Microsoft | -글로벌 IAM(Identity and Access Management) 1위<br>-Office365, Azure cloud 등 연계한 IAM솔루션 제공 | -Office365, Azure 서비스와 연계된 인증 보안솔루션 및 접근제어서비스 제공<br>-별도 H/W통합서비스를 제공하지 않지만 MS서비스에서 보안을 위해 사용 가능한 FIDO2 보안키 벤더사 등록 제공<br>-통합인증서비스로 타 서비스 이용 어려움 |
| OKTA | -IAM 솔루션 전문업체<br>-SSO, MFA 등 클라우드 기반 보안솔루션 제공 | -소프트웨어 솔루션 기반 양자기술 등을 포함한 H/W폼팩터 미보유 |

출처 : Gartner, IAM Leader's guide to access management, 2022, April, 27, Abhyuday Data, Michael Kelly, Henrique Teixeira.




〈그림 13〉 사용자 인증 MFA와 연속적인 적응형 트러스트 CAT 인증 발전단계 분석[3]

출처 : Gartner

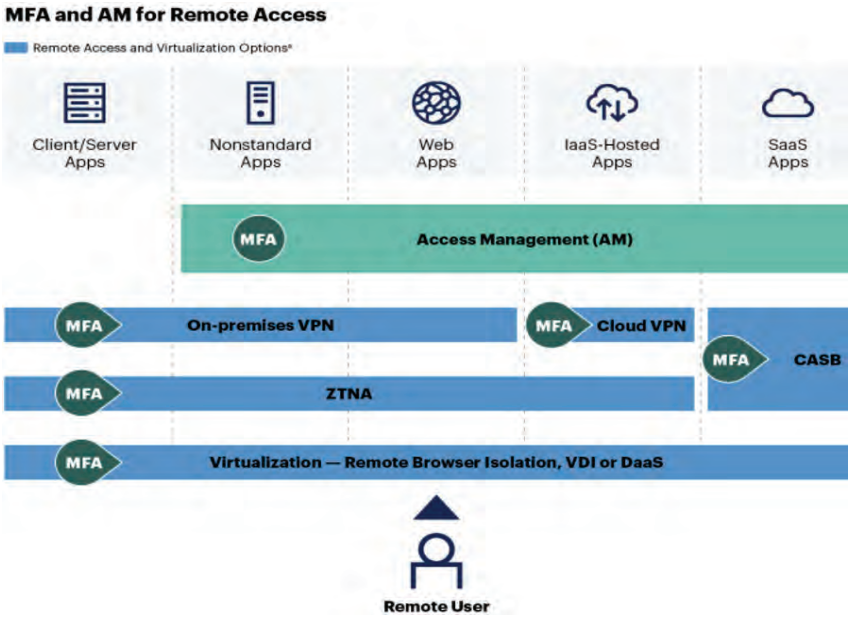
## 4. 사용자 환경을 고려한 지능형 MFA 적용[8]

웹3.0의 사용자가 다양한 환경에서 접근하는 다중요소 MFA 인증은 로그인 할 때마다 인증을 요구하거나 디바이스가 기억하는 플랫폼이 존재할 수 있다. 하지만, 새로운 디바이스가 평소와 다른 시간에 로그인을 한다면 인증이 필요할 수 있다. 항상 동일한 디바이스를 사용한 로그인이면, 로그인할 때마다 인증할 필요가 없을 수 있다.

### 4.1 제로 트러스트 기반의 사용자 환경 연동형 MFA과 패스키(Passkey) 활용

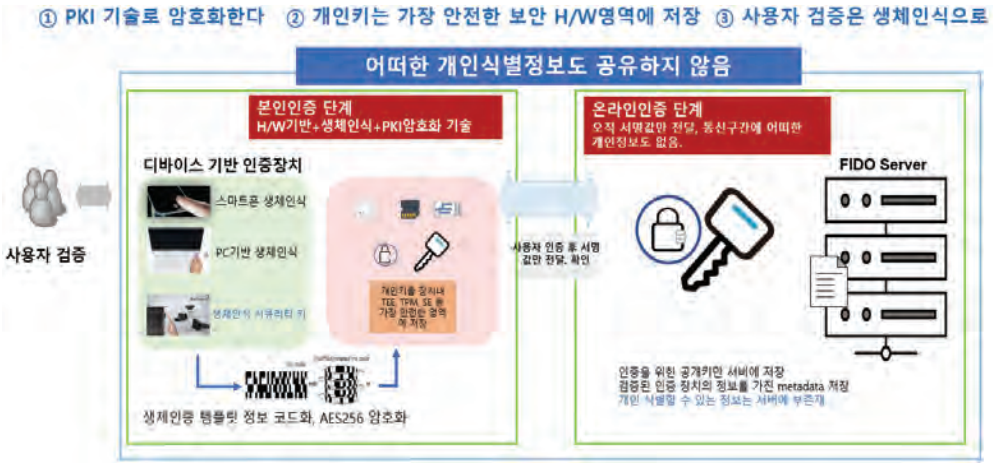
안전한 웹3.0 환경을 지원하는 통합계정관리 서비스는 사용자 환경을 고려할 때 인공지능 기반 차세대 사용자 인증 플랫폼은 취약한 비밀번호 인증을 대체하고 모바일 기반 푸시, 생체인식 및 OTP 등을 기반으로 하는 MFA 사용자 2차 인증을 지원해야 된다.

다중요소 인증 MFA는 복수로 사용자를 인증하는 방법으로 다중요소 인증은 인증을 2차례에 걸쳐서 진행하는 2차 인증(2FA, Two-factor authentication)을 포함한다. 구글, 네이버, 카카오의 포털 웹사이트에 접속할 때 2차 인증을 설정하면, 비밀번호 이외에 추가 인증으로 해커가 계정 비밀번호를 획득해도, 로그인할 수 없




〈그림 14〉 원격 사용자 인증을 위한 MFA와 AM(Access Management) 연동분석

출처 : Gartner




〈그림 15〉 공유하지 않는 개인식별 정보 기반의 사용자 인증 단계[3]

도록 하여 추가적인 정보보호 방안이 필요하다[10].

또한, 웹3.0 환경에서 패스키는 글로벌 보안기술표준화단체인 FIDO 얼라이언스(FIDO Alliance)가 주도한 로그인 방식으로 비밀번호 입력 없이 로그인한다. 암호화 처리로 계정 보안 능력도 뛰어나며, 패스키를 발급받으면 암호화된 '공개키'와 '개인키'가 생성된다. 공개키는 FIDO 서버에, 개인키는 사용자 디바이스 또는 클라우드에 저장된다.

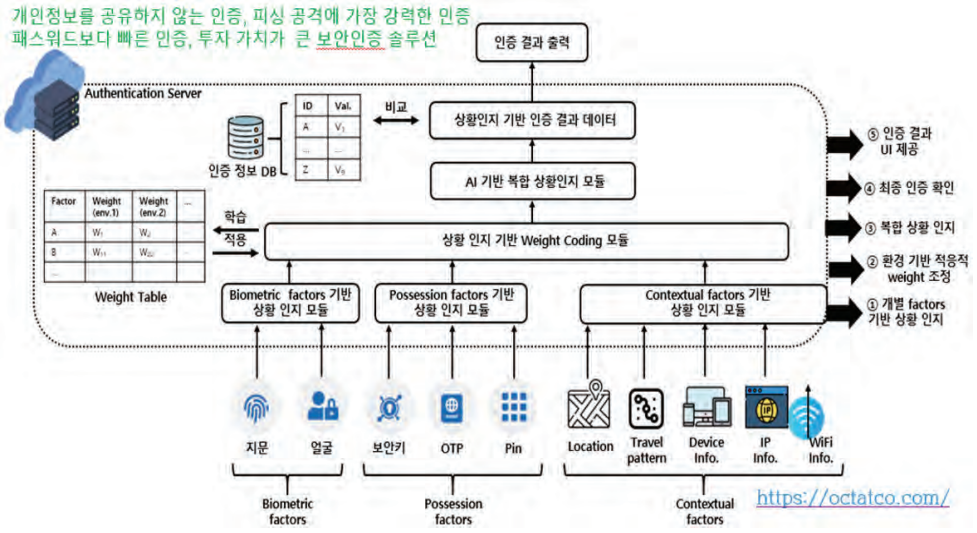
사용자 인증을 위한 로그인 과정에 공개키와 개인키다 필요하며, 로그인할 때, 서버는 사용자 본인이 맞는지 확인하기 위해 디지털 서명을 요구한다. 사용자가 개인 키를 보내면, 서버는 비공개키로 암호를 해독하는 과정에서 암호화 처리로 사용자 인증과 거래인증이 가능하다.

## 4.2 상황인지 기반의 지능형 MFA 사용자 인증 활용 설계

〈그림 18〉은 다양한 생체인증 수단과 위험 요소를 파악하는 사용자 인증을 제공하는 클라우드 네이티브 제로트러스트 기반 동적인지 보안인증 플랫폼으로 사용자 환경을 고려한 인공지능 제로트러스트 클라우드


〈그림 16〉 SSO 기반의 클라우드/온프레미스/하이브리드 통합 사용자 인증 협업[3]


〈그림 17〉 국내 포털 네이버, 카카오 등 2차 인증 요청 화면 분석




〈그림 18〉 클라우드 네이티브 제로트러스트 기반 동적인지 사용자 보안인증 플랫폼

네이티브 기반 보안인증 및 접근제어 서비스 모델을 제시하고 있다.

〈그림 19〉처럼 차세대 사용자 인증은 클라우드 네이티브 기반아래 모바일, PC, 기타 표준 FIDO 기술을 지원하는 지능형 인증 방법이다. 이러한, 크레덴셜 기반의 인증 방법과 Contextual 기반의 상황인지 요소, 즉 위치, 시간, 장치, IP 주소, 네트워크, 행동 패턴 등과 같은 인증을 결합한 사용자 환경과 맥락을 활용하는 인공지능 분석 요소는 아래와 같다.

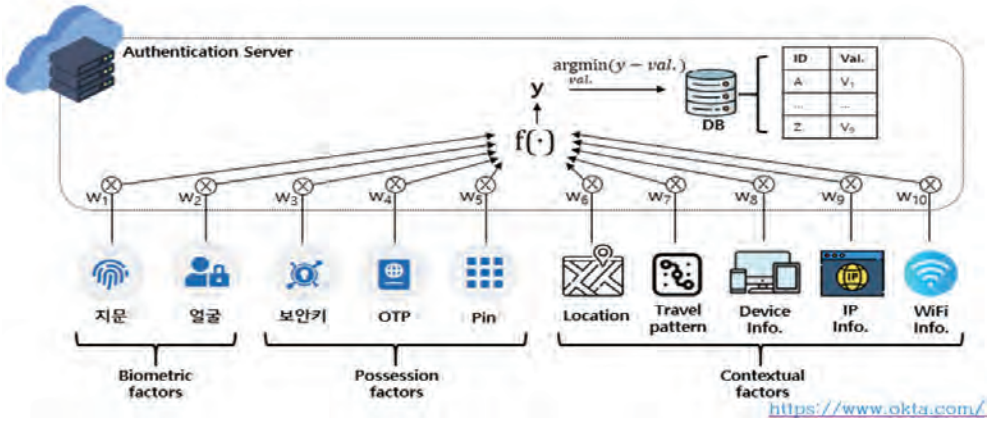
① 개별 인증 요소 기반의 상황인지
② 상황인지 기반의 Weight Configuration 조정
③ 복합 상황 인지
④ 최종 인증 확인
⑤ 인증 결과 UI 제공

〈그림 19〉는 웹3.0의 차세대 웹 환경에서 언제, 어디서, 어떠한 디바이스를 통해 사용자가 플랫폼에 접속하는 서비스와 PC 로그인 및 원격접속에서 사용자 다중요소 MFA 인증하도록 데이터베이스와 네트워크 장비의 특수 권한을 인증할 수 있다. 이러한, 사용자 상황인지 기반의 인공지능으로 지속적인 적응형 인증 등 다중요소 MFA를 활용한 보안 신뢰성을 지속적으로 향상할 수 있다.

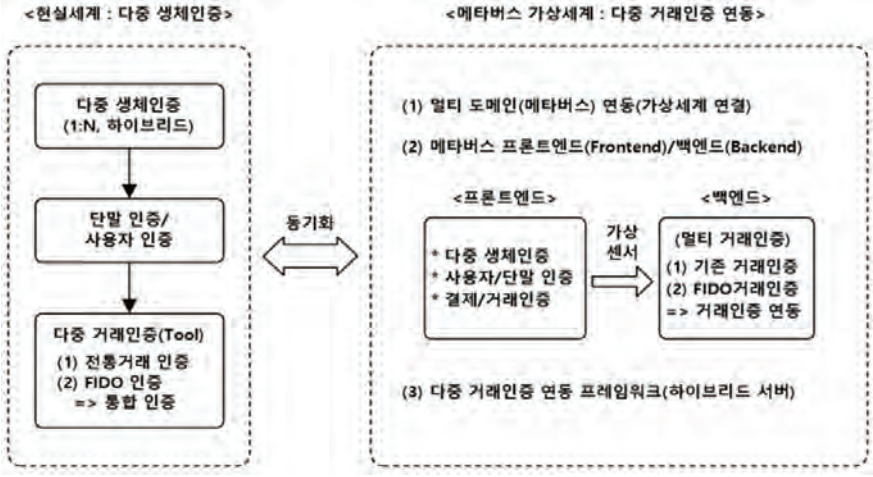
## 5. 결론

본 연구에서는 차세대 웹3.0 환경에서 생체인증 기반으로 가상세계와 사용자 인증 및 거래인증을 연동하는 메타버스 플랫폼을 제시하고자 하였다. 현실 세계에서 이루어지는 단말 인증과 사용자 인증에 연계하며, 메타버스 가상세계에서 멀티도메인에 대한 다중요소 MFA 인증을 구성할 수 있다.

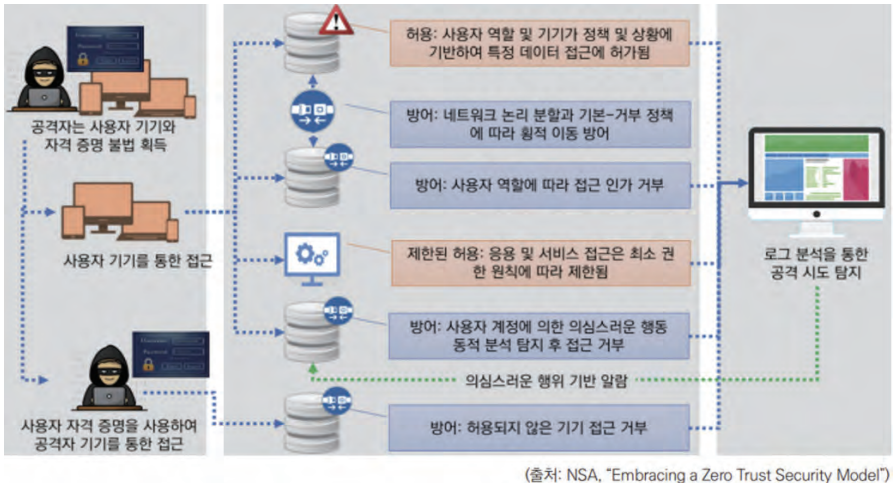
〈그림 20〉은 메타버스 가상세계에서 멀티도메인에 의한 다중요소 MFA 기반의 사용자 인증과 거래인증을 현실 세계의 다중 생체인증과 연동함에 따라 메타




〈그림 19〉 사용자 환경 적응형 MFA 기반의 복합 사용자 인증 AI 가중치 조정 설계




〈그림 20〉 메타버스 활용 다중요소 MFA 생체인식 연동 플랫폼 설계제안 사례[11]




〈그림 21〉 제로 트러스트를 위한 다중요소 MFA 기반의 사용자 인증 사례와 활용

버스에서 보안을 강화하고 안정성으로 거래의 편리함을 개선할 수 있다[11].

아울러, 차세대 웹 환경에서 사이버 공격의 증가로 다중요소 MFA 생체인식 연동 플랫폼은 클라우드 기반 플랫폼 기술과 인공지능 보안기술의 융합으로 보안 서비스를 강화하고 있다. 인공지능 및 암호화 기술 등은 아이디 패스워드 없이 안전하고 편리한 인증이 가능함에 따라, 고령자의 인터넷 이용에 대한 진입 장벽을 해소할 것으로 기대된다.

또한, 온라인 경제 활성화로 사이버 보안 수요는 보안 시장의 확대로 보안 침해 위험 증가와 디지털 ID 증가로 인한 보안인증 시장을 견인하고 있다.

이에 따라, 〈그림 21〉은 제로 트러스트를 위한 다중요소 MFA 기반의 사용자 인증 사례와 활용되고 있다. 웹3.0 서비스에서 다중요소에 의한 2차 사용자 인증은 이메일, 문자 메시지, 앱 확인, OTP 등으로 패스키 기반으로 보안성과 편의성을 제공한다. 이에 따라, △구글 △마이크로소프트 △네이버 △다음 △삼성전자 △애플 △아마존 등이 2차 인증을 지원하게 될 것이다.

또한, FIDO 얼라이언스는 차세대 웹사이트를 지원하게 되어 △마이크로소프트 △구글 △아마존 △이베이 △디스코드 △페이스북 등이 패스워드를 사용하지 않는 차세대 인증으로 전환하고 있다.

## 참고문헌

[1] 한국인터넷진흥원(KISA), "제로트러스트 가이드라인," 2023. 7. 11. https://www.kisa.or.kr
[2] 보안뉴스, "[2023 차세대 인증 분석 리포트] '시한폭탄'된 비밀번호, 보안성에 편리성 높인 차세대 인증 적용해야,", 2023.11.30. https://m.boannews.com/html/\detail.html?idx=124252
[3] 옥타코, "Passwordless 인증 도입에 대한 연구," PASCON 2022, https://octatco.com/
[4] 듀얼오스, "기존 사용자 인증, 서비스 제공자 진짜 or 가짜 확인할 수 없어," 전자신문 2023.11.30.

https://www.dualauth.com/
[5] 피앤피시큐어, “비전 AI 기술로 비밀번호리스・제로 트러스트 보안 모델 구현,” 전자신문 2023.11.30. https://pnpsecure.com/
[6] 이찬희 외, “사용자 인증 기술 동향과 메타버스에서의 적용 방향 연구,” 한국정보처리학회 추계학술발표대회 2022.10.12. https://www.manuscriptlink.com/society/kips/conference/ack2022
[7] 강민구, “암호 없는 사용자의 2차 인증용 복합생체 기반의 FIDO 플랫폼,” 인터넷정보학회논문지 Vol.23 No.4 2022.8.31. https://doi.org/10.7472/jksii.2022.23.4. 65
[8] 옥타, “다중요소 인증 MFA이 중요한 이유,” https://www.okta.com/
[9] 남상엽, 강민구 외, “디지털 자산과 보안,” 상학당, 2022.01.25.
[10] 전자신문, “털리기 쉬운 내 계정, 귀찮아도 이것만은 꼭,” 2024.03.01. https://n.news.naver.com/article/030/ 0003185580
[11] 이재형 외, “다중 생체인증 기반의 통합 거래인증 연동 메타버스 플랫폼 플랫폼,” 대한민국특허 등록번호 10-2521684, 2023년04월10일

## 저자약력

**이 재 형**

fimori@octatco.com

2003 충남대학교 국제경영(학사)
2023 서울과학종합대학원 AI 융합공학(공학석사)
2018년–현재 옥타코 대표이사
2021년–현재 FIDO Alliance 글로벌 개발자대회 심사위원
관심분야 접근관리, FIDO, 생체인증, AI

**강 민 구**

kangmg@hs.ac.kr

1986 연세대학교 전자공학과(공학사)
1989 연세대학교 전자공학과(공학석사)
1994년–현재 연세대학교 전자공학과(공학박사)
1985년–87 삼성전자 통신연구소 연구원
2000년–현재 한신대학교 AI,SW계열 교수
관심분야 정보통신, 스마트 모바일, IT영상콘텐츠