Headline

안전한 클라우드 환경을 위한 하이브리드 본인인증 아키텍처 적용 전략

EQST 금융사업팀 허청일 수석

■ 개요

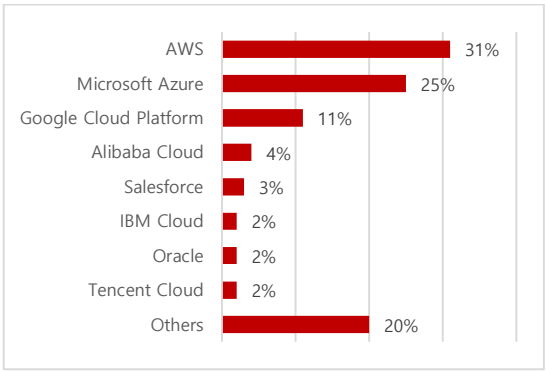
일반적으로 온프레미스(On-Premise) 기업망을 위한 본인인증 아키텍처는 액티브 디렉터리(Active Directory)와 같은 서비스를 통해 처리한다. 그러나 기업이 온프레미스와 클라우드 환경을 결합한 하이브리드 환경으로 전환하려고 할 때, 본인인증 관리는 상당히 복잡해질 수 있다. 이러한 상황에서는 On-Premise 본인인증 관리 아키텍처를 클라우드 시스템과 안전하고 효율적으로 통합하여 상호운용이 가능하도록 해야한다.

2024 년 3 월, 미국 사이버 보안 및 인프라 보안국(CISA)에서는 기업이 안전한 클라우드 기업 애플리케이션(SCuBA, Secure Cloud Business Application)을 위한 가이드를 공개했다. 이 가이드는 하이브리드 환경에서의 본인인증 관리를 위해 페더레이션(Federation), 패스스루 인증(Pass-Through Authentication), 비밀번호 동기화(Password Synchronization), 클라우드 기본 인증(Cloud Primary Authentication(Passwordless)) 총 네 가지의 아키텍처를 제안하고 있다.

이번 Headline 리포트에서는 기업이 On-Premise 와 클라우드 시스템 간의 상호운용성을 확보하기 위해 적절한 본인인증 아키텍처를 적용하는 방안에 대해 다룬다. 각 아키텍처의 장단점과 고려 사항 등을 제시해 기업이 최적의 본인인증 솔루션을 선택할 수 있도록 제언한다.

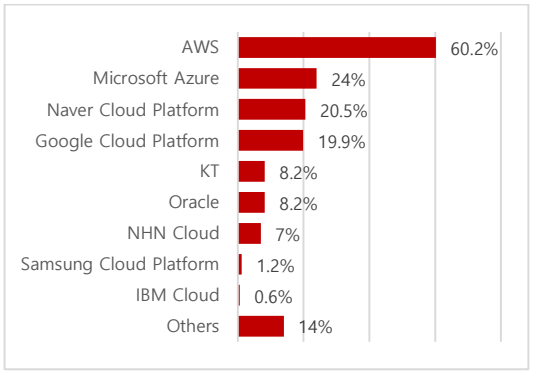
■ 국내외 클라우드 이용 실태 및 자격증명(Credential) 피해 현황

2006 년 AWS 클라우드 컴퓨팅 서비스가 제공된 지 18 년이 지난 지금, 국내외 수많은 기업이 클라우드 컴퓨팅을 사용하고 있다. 2024 년도 1 분기 기준 전세계 클라우드 컴퓨팅 점유율과 2023 년도 국내 클라우드 컴퓨팅 점유율은 아래와 같다.



* 출처: Synergy Research Group

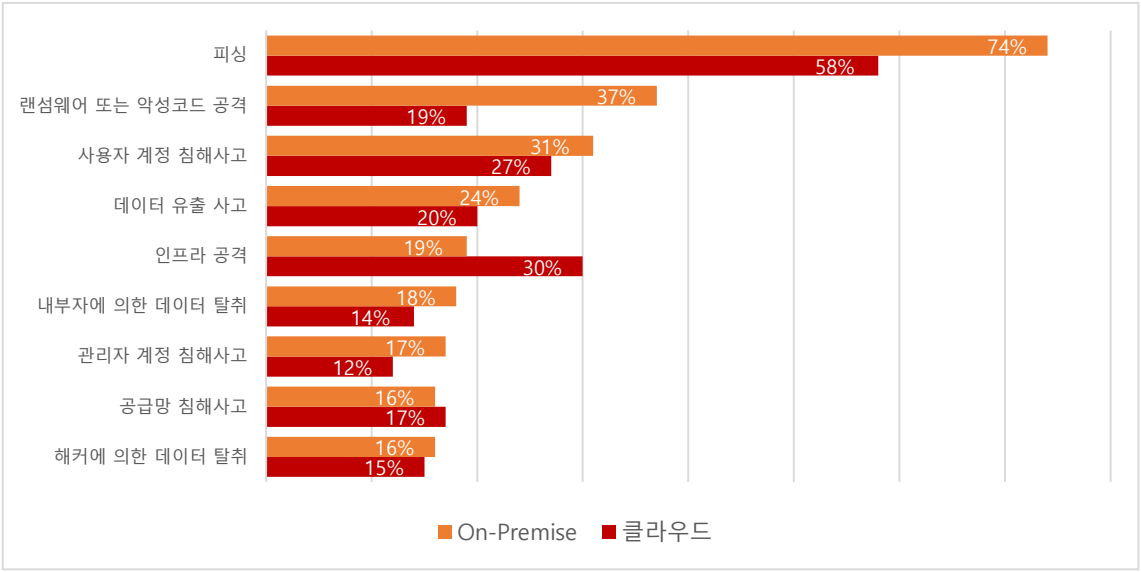
그림 1. '24 년도 1 분기 전세계 클라우드 컴퓨팅 점유율



* 출처: 과학기술정보통신부

그림 2. '23 년도 국내 클라우드 컴퓨팅 점유율

영국 정보보안 컨설팅업체인 StationX 가 올해 발표한 2023 년도 On-Premise vs. 클라우드 보안사고 통계 자료에 따르면, 일부 보안사고 유형을 제외하면 클라우드 환경보다는 On-Premise 환경에서 보안사고가 많이 발생했음을 알 수 있다. 그 중에서도 피싱 공격이 각각 74%, 58%로 1 위를 차지했다.

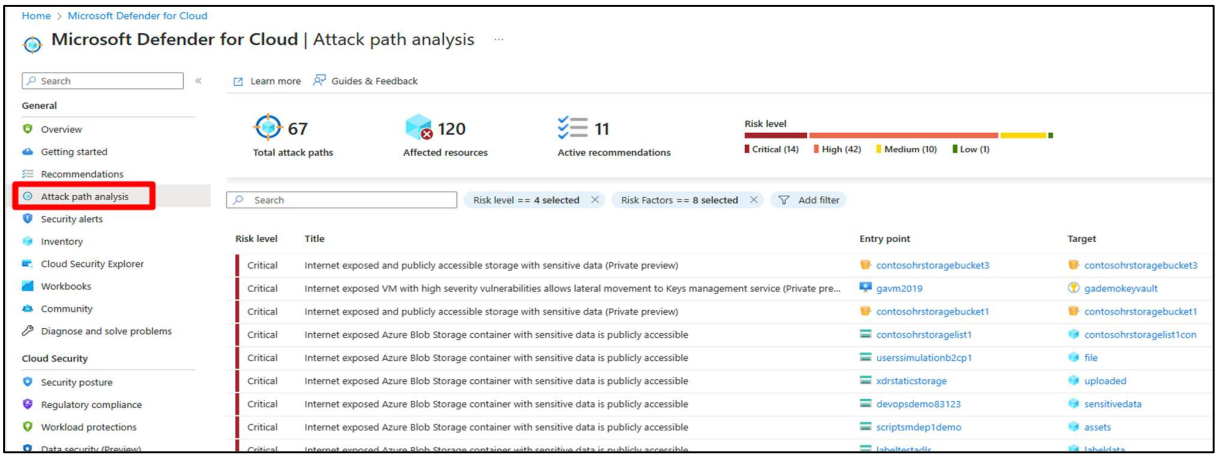


* 출처: StationX

그림 3. '23 년도 On-Premise vs. 클라우드 보안사고통계

클라우드 환경의 보편화로 보안 취약점이나 해킹 공격이 지속적으로 발생하고 있다. 2024 년 4 월 Microsoft 자료에 따르면, 공격경로 전체 대상 중 20%가 취약한 비밀번호나 키와 같은 자격증명(Credential)의 노출로 인해 발생한다. 공격경로란 공격자가 클라우드 내 중요 또는 민감정보에 접근 및 유출하는 데 사용할 수 있는 경로를 의미한다. 이러한 공격경로를 제거하기 위해서는 사전에 '공격경로분석'을 수행해야 한다.

공격경로분석은 공격자가 멀티 클라우드 환경에 어떻게 침투하고 이동할 수 있는지를 클라우드 내 보안 위험의 상관관계를 분석해 예상 공격경로를 가시적으로 확인하는 침해사고 사전예방 기법이다. 공격경로분석을 수행하지 않을 경우, 공격자는 취약한 구성이나 리소스를 악용하여 중요 또는 민감정보에 접근하기 위한 또 다른 경로를 활용할 수 있다. 따라서 기업은 공격경로분석을 통해 잠재적인 보안 위협을 사전에 식별하고 차단하는 것이 중요하다.



* 출처: Microsoft

그림 4. 공격경로분석 예시

다음으로 자격증명 피해 통계 현황에 대해 알아보도록 한다. 미국 통신업체 중 하나인 Verizon 의 2024 년도 통계는 다음과 같다.

공격 빈도	3,032/3,661 (82.8%)
공격자 비율	외부자 (100%)
공격 동기	금전탈취(95%), 정보탈취(5%)
유출된 정보	자격증명 (50%), 개인정보 (41%), 내부정보 (20%), 기타 (14%)
공격 기법	프리텍스팅, 피싱, 협박

* 출처: Verizon

표 1. 사회적 공학기법 공격 통계

공격 빈도	881/1,997 (44.1%)
공격자 비율	외부자 (100%), 내부자(1%), 둘 다(1%)
공격 동기	금전탈취(85%), 정보탈취(15%)
유출된 정보	계정정보 (71%), 개인정보 (58%), 기타 (29%), 내부정보 (17%)
공격 기법	크리덴셜 스터핑, Brute-force, 취약점 악용

* 출처: Verizon

표 2. 기본적인 웹 애플리케이션 공격 통계

위 내용에서 생소한 공격기법이 있는데, 바로 프리텍스팅이다. 프리텍스팅은 꾸며낸 이야기를 이용해 피해자를 속여 금전 지출을 유도하는 사회적 공학기법이다. 비즈니스 이메일 침해 사기, 계정 업데이트 사기, 조부모 사기, 로맨스 사기, 암호화폐 사기, 정부기관 사기 등이 이에 해당한다.

또한, 크리덴셜 스터핑은 다른 곳에서 유출된 자격증명(ID 를 포함한 비밀번호 또는 키 등 인증정보)을 여러 웹사이트나 웹에 대입해 계정을 탈취하는 기법이다. F5 에 따르면, 인증 트래픽의 20%가 크리덴셜 스터핑에 해당하며, 이 공격은 자동화 봇을 이용해 무차별 대입을 시도하고 보안 솔루션을 우회할 정도로 발전하고 있어 경각심을 가져야 한다.

Verizon 보고서에 따르면, 위에 언급한 다양한 공격기법에 대한 보호대책으로 MFA(다중 인증) 적용을 권고하고 있다.

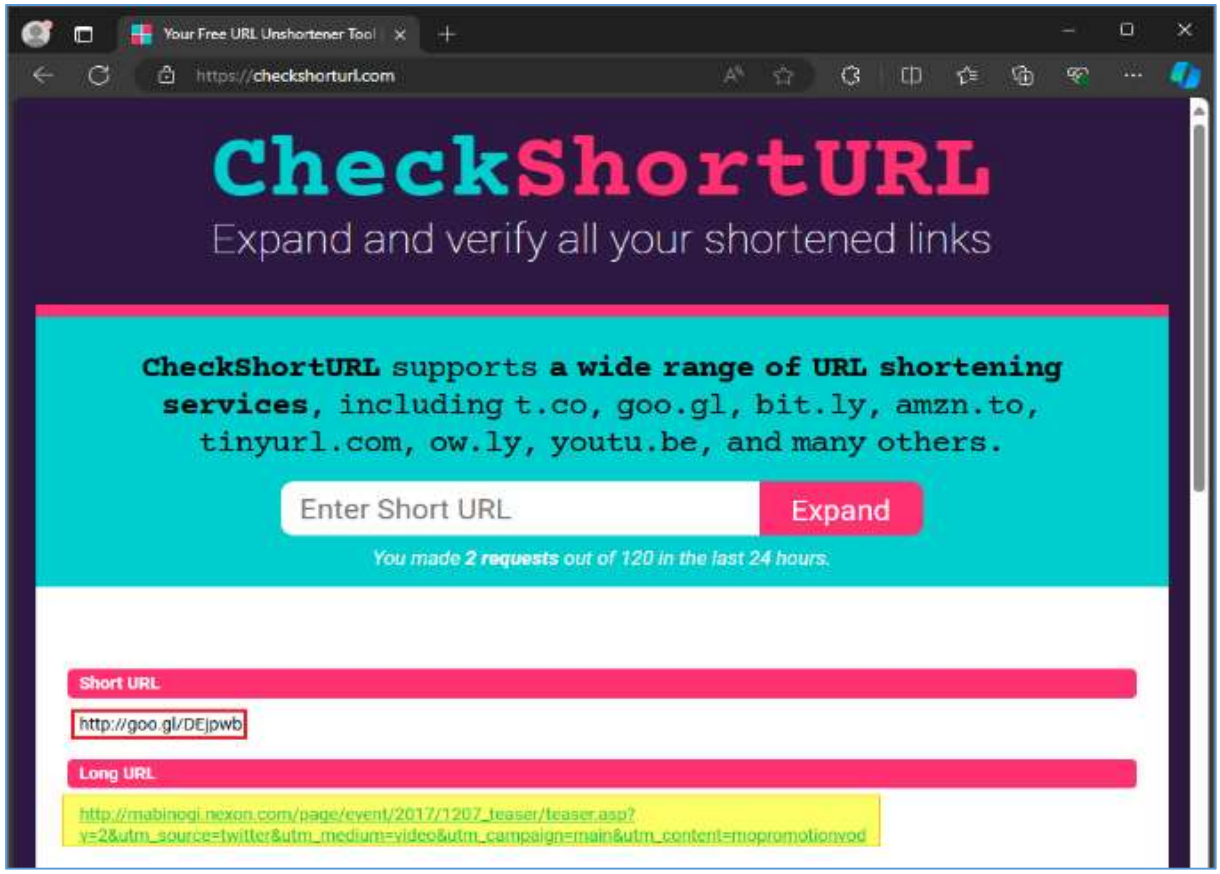
■ MFA(다중 인증)의 보안위협

우리 생활에 사용하는 MFA 는 SMS, ARS, 이메일, OTP 등이 있다. 그러나 이 중 아무거나 MFA 를 적용한다고 해서 무조건 안전해지는 것은 아니다. 미국 CISA 에 따르면, 현재 존재하는 MFA 의 위협은 크게 4 가지가 있다.

1) 피싱(Phishing)

피싱은 공격자가 정보를 획득하기위해 이메일 또는 악성 웹사이트를 사용하는 사회적 공학기법 공격이다. 예를 들어, 공격자가 피해자가 사용하는 웹사이트를 합법적인 로그인 페이지로 속여 방문을 유도하는 이메일을 전송할 수 있다. 이때 피해자는 악성 웹사이트를 방문해 ID, 비밀번호, 2 차인증코드(6 자리) 등을 입력하게 된다.

만약 일반 URL 이라면, 오탈자 여부를 공식 웹 사이트를 방문하여 미리 검증하면 사전예방이 가능하다. 하지만 URL 단축이 적용된 URL 인 경우, 정상 URL 여부를 확인하기 어렵다. 이 경우에는 아래의 그림처럼 축약 URL 의 정상 URL 여부 확인을 진행해 사전예방이 가능하다.



* 출처: CheckShortURL

그림 5. CheckShortURL 에서 URL 단축이 적용된 URL 의 기존 URL 확인 기능 제공

2) 푸시 폭탄(Push Bombing) 또는 푸시 피로(Push Fatigue)

푸시 폭탄은 피해자가 '승인' 버튼을 누를 때까지 푸시 알림을 반복적으로 보내는 공격이다. 이는 피해자의 실수로 승인 버튼을 클릭하게 해 공격 대상 서비스를 이용하게 할 수 있게 한다.

첫 번째 경우는 공격자가 탈취한 비밀번호로 1 차인증을 성공한 후 푸시 알림을 통해 2 차인증을 허용하게 해 계정을 탈취한다. 1 차 비밀번호가 탈취된 경우, 즉시 비밀번호를 변경할 것을 권고한다.

두 번째 경우는 공격자가 푸시 폭탄 공격으로 피해자의 계정 비밀번호 초기화를 시도해 계정을 탈취한다. 이 경우 피해자는 당황하지 말고 모두 '거부' 처리해야 한다.

* 출처: Bitdefender

그림 6. Push Bombing 의 예시

3) 3G(SS7 프로토콜), LTE(Diameter 프로토콜) 취약점 악용

ACM Queue 에 따르면, 공격자는 통신사 인프라에서 사용하는 3G(SS7 프로토콜[1]), LTE(Diameter 프로토콜[2]) 취약점을 악용하여 SMS 내 2 차인증 코드를 탈취할 수 있다. Diameter 가 SS7 로부터 개량한 프로토콜이기 때문에, SS7 과 동일한 취약점이 존재한다.

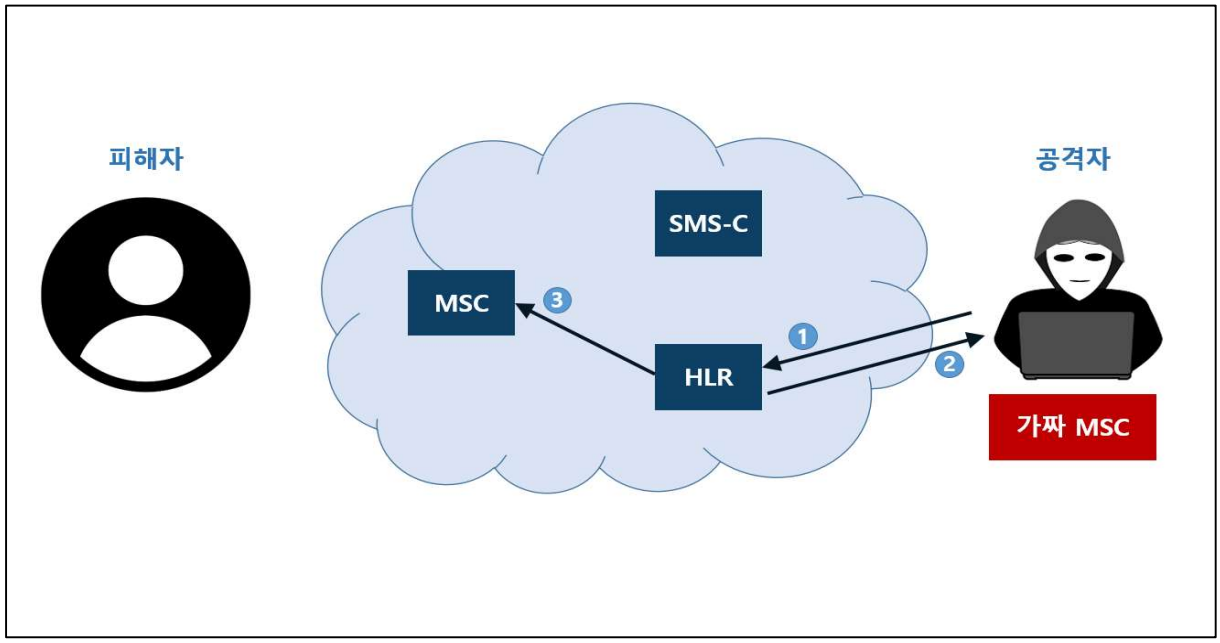
따라서 공격자는 SS7/Diameter 프토토콜 취약점을 악용해, 사용자가 받는 SMS 을 해외로 전송할 수 있으며 이는 SMS 내 2 차인증 코드 탈취로 이어질 수 있다. 해당 공격을 근본적으로 방지하기 위해서는 5G 단독모드를 도입해야 한다.

5G 는 NSA(비단독모드)와 SA(단독모드)가 있다. 비단독모드는 LTE + 5G 와 함께 사용하지만, 단독모드는 5G 만 사용한다. 5G 단독모드를 사용하면 LTE 의 Diameter 프로토콜 취약점으로 인한 SMS 내 2 차 인증 코드 탈취를 방지할 수 있다.

[1] SS7 프로토콜: 음성통신의 호출정보와 데이터통신의 접속정보 등을 통합적으로 관리하기 위한 개방 신호 처리 프로토콜. 통화설정, 요금청구, 통화 라우팅 지원 기능 제공

[2] Diameter 프로토콜: 이동 인터넷 및 모바일 IP 가입자에게 로밍 서비스를 제공하기 위해서 요구되는 인증, 인가, 과금을 지원하는 프로토콜. 로밍에 필요한 도메인 간 이동성 지원, 강화된 보안 제공

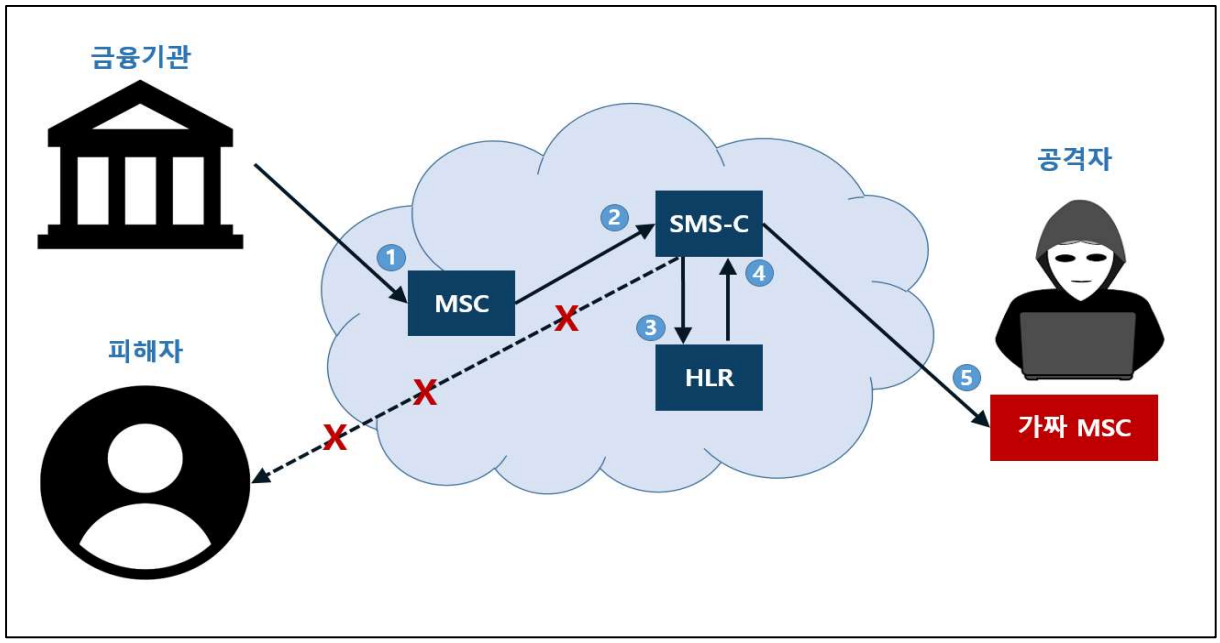
SS7 프로토콜 취약점을 악용한 SMS 탈취 취약점의 시나리오는 다음과 같다.



* 출처: FirstPoint

그림 7. 절차 1 – SMS 탈취공격 사전준비

① 공격자가 만든 가짜 이동전화교환국(MSC)에 피해자의 휴대전화번호 등록
② 가입자위치등록기(HLR)에 피해자의 휴대전화번호의 위치 설정
③ 가입자위치등록기(HLR)가 실제 이동전화교환국(MSC)의 기존 값 초기화 요청



* 출처: FirstPoint

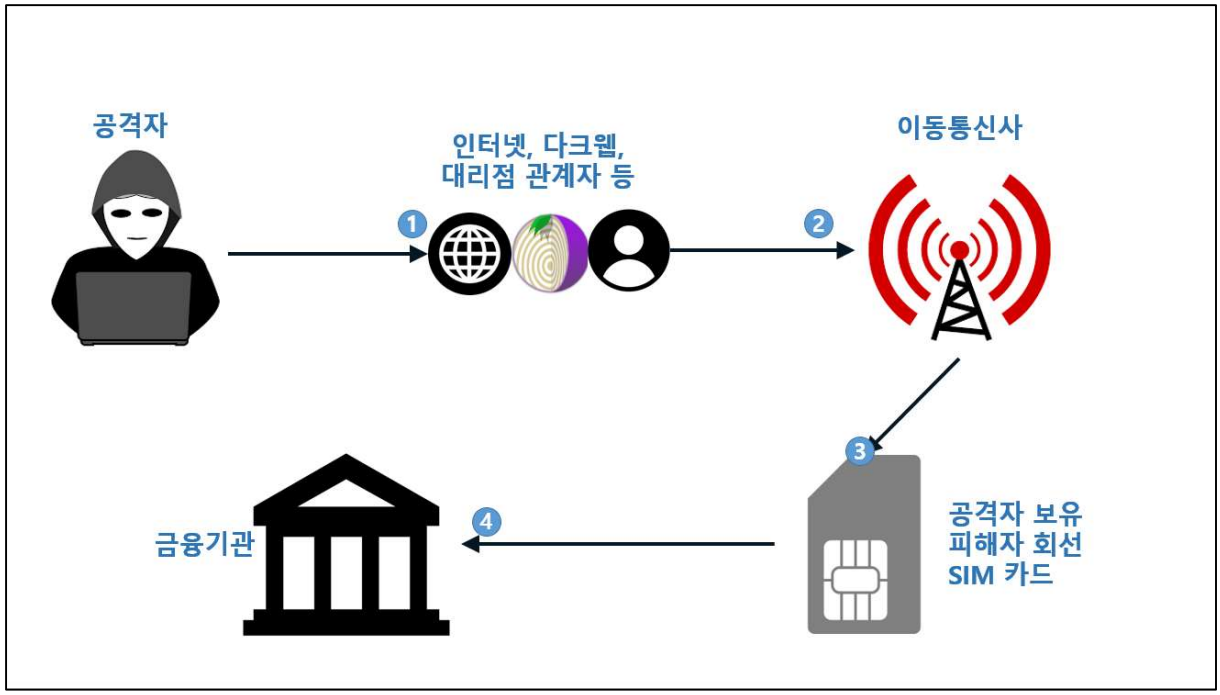
그림 8. 절차 2 – SMS 탈취공격 수행

① 금융기관이 피해자에게 SMS 전송 시도 (예: 피해자가 요청한 2 차인증코드)
② 실제 이동전화교환국(MSC)이 SMS 를 SMS 센터로 전송
③ SMS 센터가 피해자의 위치를 가입자위치등록기(HLR)에 확인 요청
④ 가입자위치등록기(HLR)는 공격자가 등록한 가짜 MSC 주소로 응답
⑤ SMS 센터는 가짜 이동전화교환국(MSC)인 공격자에게 SMS 전송

4) SIM 스와핑

SIM 스와핑 공격은 공격자가 이동통신사를 속여 피해자 가입자회선정보를 공격자의 SIM 카드로 이전한 후, 이 SIM 카드를 이용하여 공격자가 피해자 가입자회선을 사용할 수 있도록 하는 일종의 사회적 공학적기법이다.

SIM 스와핑 공격 시나리오는 다음과 같다.



* 출처: SEON Technologies

그림 9. 절차 – SIM 스와핑 공격 수행

① 공격자가 공격대상 특정된 피해자 개인정보 획득	**<피해자 개인정보 수집경로 예시>** - 이동통신사 고객에 대한 피싱 - 이동통신사 직원에 대한 피싱 - 이동통신사 직원에 뇌물공여 또는 협박 - 이동통신사 인프라에 대한 사이버공격 - 이동통신사 대리점 또는 지점에 사기꾼 잠입 - 인터넷, 딥웹, 다크웹 등 활용
② 공격자가 획득한 개인정보를 이용하여 피해자로 위장하여 이동통신사에 접촉 시도	**<피해자 SIM 부정발급을 위한 사회적 공학기법 예시>** - 공격자가 대리점에 위조한 신분증 제시 - 공격자가 고객센터 전화를 통해 인증 관련 질문에 성공적으로 응답 - 피해자의 이동통신사 계정을 탈취하여 SIM 개통 서비스 신청
③ 공격자에게 이동통신사로부터 피해자 가입자회선 SIM 카드 발급 완료	
④ 피해자 가입자회선으로 SMS 인증을 통해 피해자 정보로 금융기관 계좌 탈취 가능	

* 출처: SEON Technologies

표 3. SIM 스와핑 공격 시나리오 절차

■ 앱 기반 MFA 보안위협

만약 Phishing-resistant MFA 를 적용하기 현실적으로 어렵거나 불가능한 상황이라면, 앱 기반 MFA 로 대체할 수 있다. 앱 기반 인증의 유형은 다음과 같다. 그러나 앱 기반 MFA 는 기본적으로 피싱 공격에 취약하기 때문에 유의해야 한다. 앱 기반 인증의 유형은 다음과 같다.

앱 기반 인증 유형	설명	취약여부
OTP	앱 기반 인증기가 OTP 코드를 생성하거나 모바일 앱으로 '푸시' 팝업 알림을 전송하여 사용자의 본인여부를 확인하는 기술	취약(피싱)
사용자전화번호 일치여부 검증하는 모바일 푸시 알림	모바일 앱 푸시 알림 인증시작 및 인증종료 사이에, 사용자가 서비스에 미리 등록한 사용자전화번호와 실제 요청 중인 단말기의 USIM 전화번호의 일치여부 검증하여 본인여부를 확인하는 기술	취약(피싱)
토큰 기반 OTP	토큰 기반 인증기가 사용자가 OTP 를 소지함을 증명목적으로, 해당 토큰이 생성하는 OTP 코드를 입력하여 사용자의 본인여부를 확인하는 기술	취약(피싱)
사용자전화번호 일치여부 미 검증하는 모바일 푸시 알림	모바일 앱 푸시 알림 인증시작 및 인증종료 사이에, 사용자가 서비스에 미리 등록한 사용자전화번호와 실제 요청 중인 단말기의 USIM 전화번호의 일치여부 검증없이 본인여부를 확인하는 기술	취약(피싱, 푸시 폭탄)

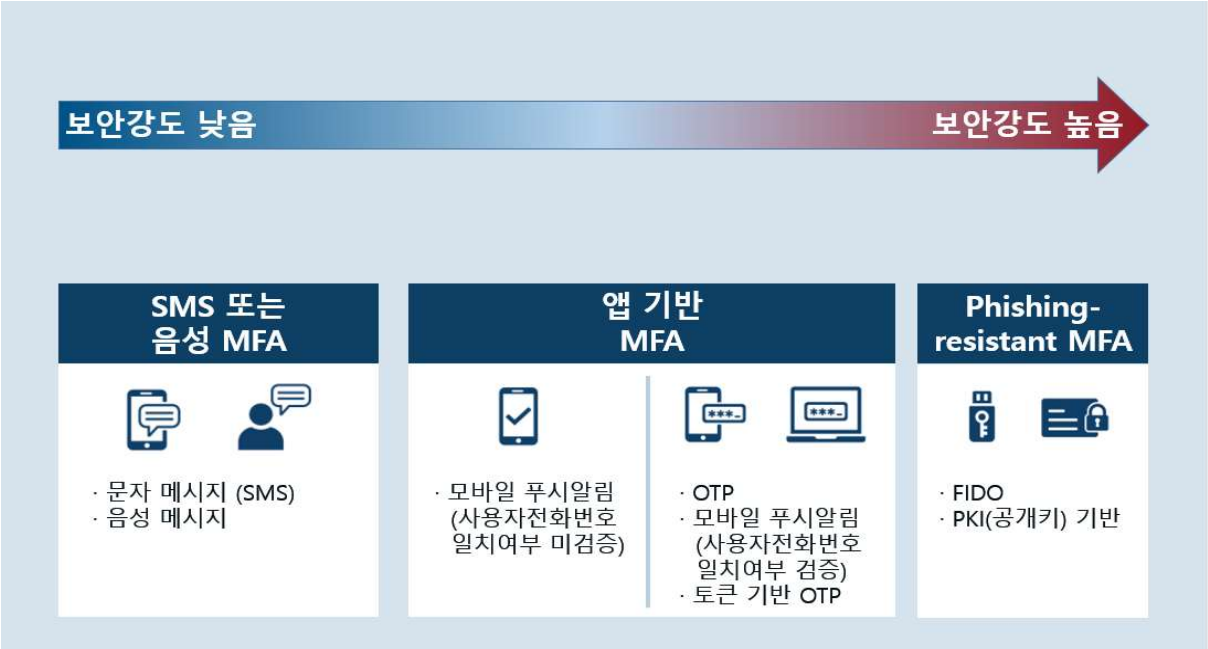
* 출처: CISA

표 4. 앱 기반 MFA 유형에 따른 취약여부

■ Phishing-resistant MFA 사용 필요성

1) 개요

미국 CISA 에서는 2 가지의 MFA 를 사용할 것을 권고하고 있다. 첫 번째는 Phishing-resistant MFA 이고 두 번째는 앱 기반 인증이다. 먼저, Phishing-resistant MFA 는 피싱 공격을 방지할 수 있는 MFA 로 현존하는 MFA 방식 중 가장 안전하다고 평가받는다. 이에 대한 내용은 아래에서 다시 살펴보도록 하겠다.



* 출처: CISA

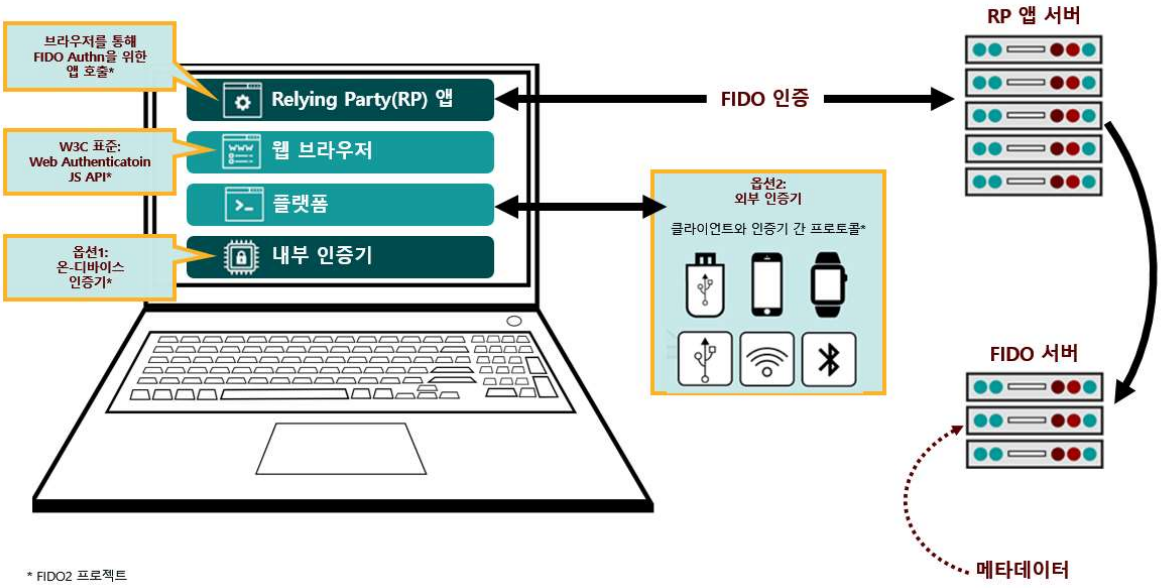
그림 10. MFA 보안강도 비교

2) Phishing-resistant MFA – FIDO/WebAuthn[3] 인증

MFA 는 현재 피싱 공격을 방지하는 목적으로 널리 사용할 수 있는 방식이다. FIDO 얼라이언스가 원래 FIDO2 표준의 일부분으로서 WebAuthn API 를 개발했지만, 지금은 W3C 표준으로 발행됐다. WebAuthn 은 주요 웹 브라우저, 운영체제 및 스마트폰에서 지원한다. WebAuthn 은 Phishing-resistant 인증기를 제공해 FIDO2 표준과 함께 동작한다.

WebAuthn 인증기는 아래의 내용을 모두 처리할 수 있다.

- USB 또는 NFC 등을 통해 장치와 연결된 물리적인 토큰을 분리할 수 있음
- '플랫폼' 인증기로서 노트북 또는 모바일 단말기에 내장될 수 있음



* 출처: FIDO Alliance

그림 11. FIDO2 구성 예시

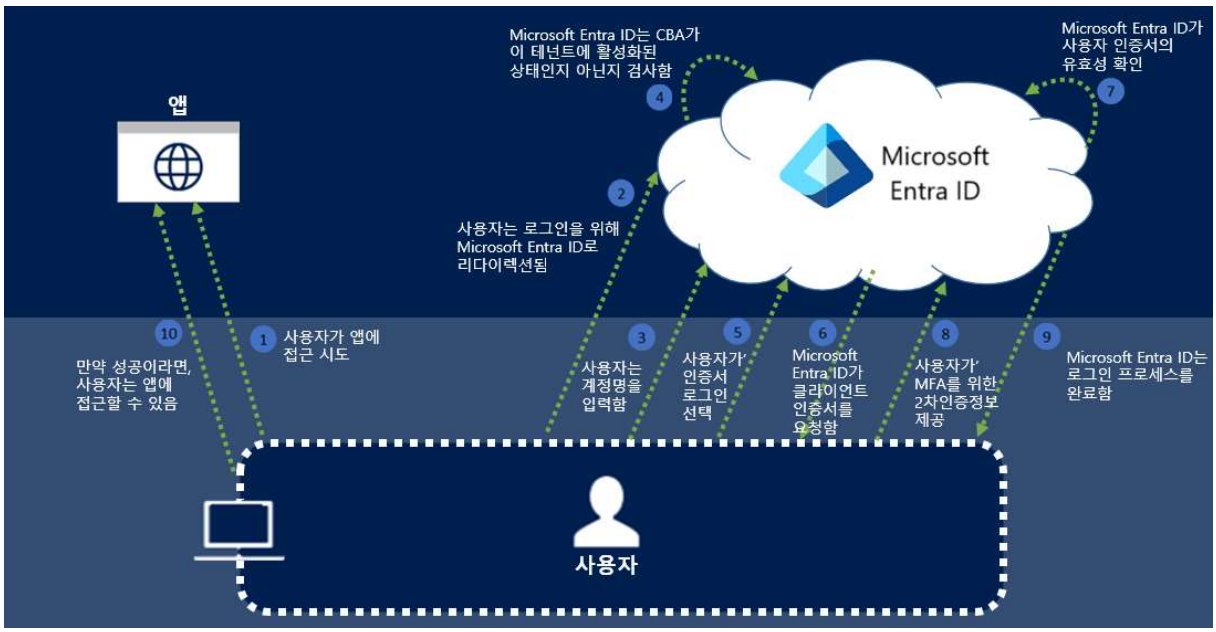
[3] WebAuthn: 비밀번호, SMS 대신 공개키를 이용하여, 서버가 사용자 등록 및 인증하기 위한 API. WebAuthn 을 활용한 Passkey 를 이용해 다양한 플랫폼, 웹 브라우저에 Passwordless 인증 로그인 가능

3) Phishing-resistant MFA - PKI(공개키) 기반 MFA

Phishing-resistant MFA 는 널리 사용하기 어려운 방식으로 기업의 PKI 인증서와 결합이 필요하다. PKI 기반 MFA 에 사용할 수 있는 인증기의 예로는 스마트카드, IC 칩 내장된 신분증 등이 있다. PKI 기반 MFA 는 어려운 방식을 요하는 만큼 대규모 기업 및 조직에 강력한 보안을 제공한다.

그러나, PKI 기반 MFA 를 성공적으로 이용하려면 매우 성숙한 본인인증 관리 문화가 필요하다. 특히, SSO 가 구축되지 않은 서비스 및 인프라에서는 폭넓게 지원하지 않는다. 대부분의 PKI 기반 MFA 활용 시, 사용자 자격증명은 스마트카드 내 보안칩 내에 있다. 해당 카드를 이용해 사용자가 시스템에 로그인 시 반드시 장치에 직접 연결되어야만 한다. 이 때 비밀번호 또는 PIN 입력을 동시에 요구한다.

디지털적으로 PKI 인증서 탈취가 불가능한 스마트카드 또는 IC 칩 내장된 신분증을 통해 로그인 하도록 시스템을 구축해야 한다는 점을 유의해야 한다.



* 출처: Microsoft

그림 12. Entra ID 를 활용한 PKI 기반 MFA 예시

■ 하이브리드 본인인증 아키텍처 소개 및 비교

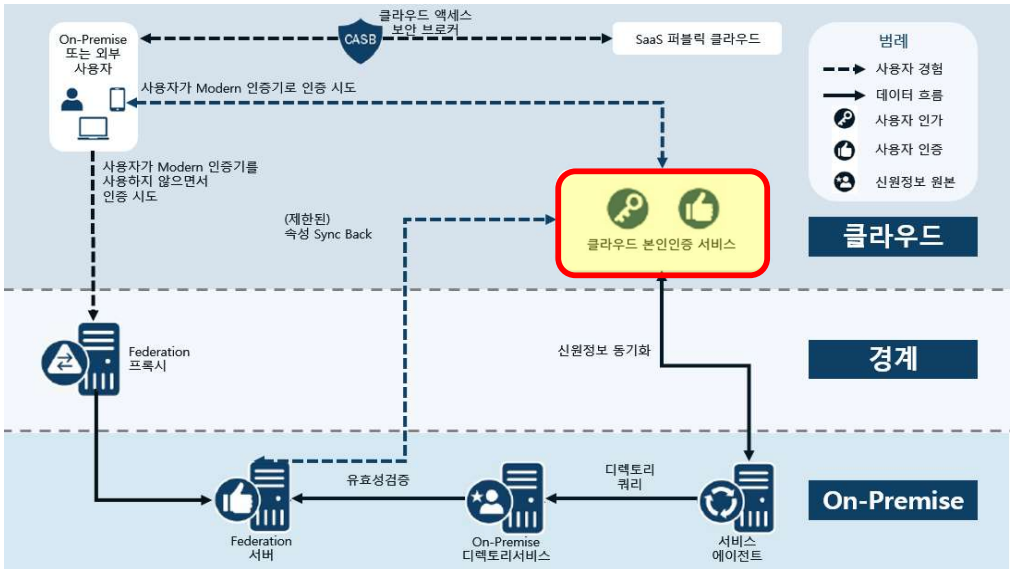
지금부터 하이브리드 본인인증 아키텍처에서 사용할 페더레이션, 패스스루 인증, 비밀번호 동기화, 클라우드 기본 인증에 대해 설명하고 이후, 하이브리드 본인인증 아키텍처 4 종류에 대해 비교 및 정리한다.

1) 페더레이션

페더레이션은 클라우드 본인인증 서비스와 기업 On-Premise 디렉토리 서비스를 연동해 On-Premise 에서 기업의 사용자 인증 프로세스 수행할 수 있도록 하는 아키텍처다. 이 아키텍처는 클라우드 관련 도메인을 사전에 정책상으로 허용하므로 On-Premise 본인인증은 클라우드 서비스에 대한 본인인증을 승인할 수 있다. 따라서, 사용자가 한 번 로그인하면 On-Premise 와 클라우드 기반 리소스에 모두 접근할 수 있다.

페더레이션은 기업이 모든 인증을 On-Premise 에서 처리하기 원하거나 클라우드 등 외부에서 인증을 원하지 않을 경우에 장점이 지닌다. On-Premise 에서 모든 인증 트랜잭션을 처리해 각 계정은 하나의 레코드만 필요로 한다. 모든 인증 시도를 중앙에서 관리하고 로깅도 수행한다. 반면, 페더레이션이 아닌 본인인증 아키텍처는 사용자 접근을 인증하기 위해 로그온 데이터 호스팅을 요구하며, 여러 곳으로 인증 로그를 분산 저장한다.

이처럼 페더레이션은 모든 인증을 중앙처리 하므로 보안에 장점이 있지만, 기업은 원격 사용자에 대한 지연시간 증가와 이에 따른 잠재적인 서비스 영향 및 지속적인 On-Premise 디렉토리 서비스 운영비용 지출을 고려해야 한다. 또한 디렉토리, 페더레이션 서버 등 On-Premise 디렉토리 서비스는 가장 민감한 자산으로서 높은 수준의 보안을 유지해야 한다. 따라서, 기업은 시간이 지남에 따라 페더레이션 아키텍처에서 클라우드 기본 인증 아키텍처로 전환할 수도 있음을 인지해야 한다.



* 출처: CISA

그림 13. 페더레이션 아키텍처 구조

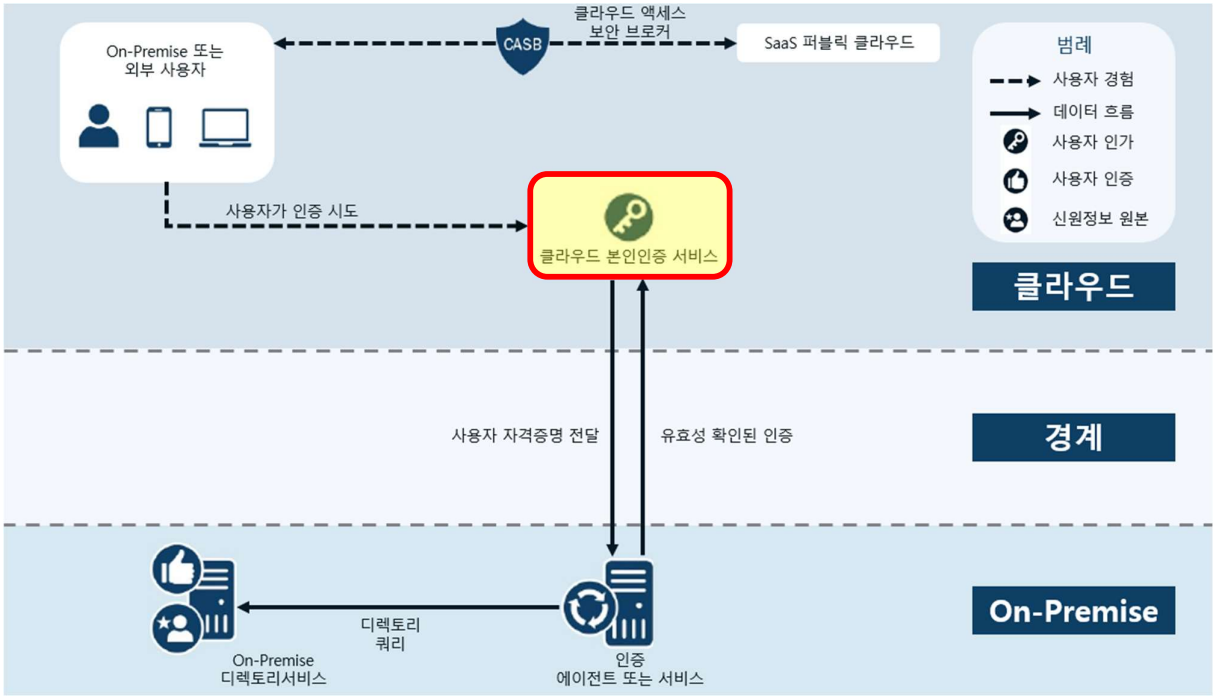
2) 패스스루 인증

패스스루 인증은 On-Premise 디렉토리 서비스에서 인증을 수행한 후, 클라우드 본인인증 서비스를 통해 리소스를 사용하도록 인가하는 방식이다.

일반적으로 클라우드 본인인증 서비스를 On-Premise 과 연동하기 위해, On-Premise 에 인증 에이전트 또는 서비스 구축 및 연동한다. 이를 통해 기업이 On-Premise 에서의 인증을 유지하고 보안정책을 강제할 수 있다.

기업은 클라우드 서비스 제공자(Cloud Service Provider, CSP)와 기업의 특정 니즈를 최적으로 충족시키는 옵션을 선택할 수 있다. 예를 들면, 기업은 On-Premise 디렉토리 서비스(예: 도메인 컨트롤러, LDAP)에서 직접 소프트웨어 설치를 제한 및 금지하는 보안 요구사항에 대한 준수가 필요할 수 있다. 이 경우, On-Premise 디렉토리 서비스와 함께 인증요청 및 인터페이스를 처리할 수 있는 부가서비스 또는 제안 때문에 클라우드 서비스 제공자에 더 의존하게 된다.

이와 별도로, 인증은 On-Premise 에서 수행하지만, 인가는 클라우드에서 수행한다.



* 출처: CISA

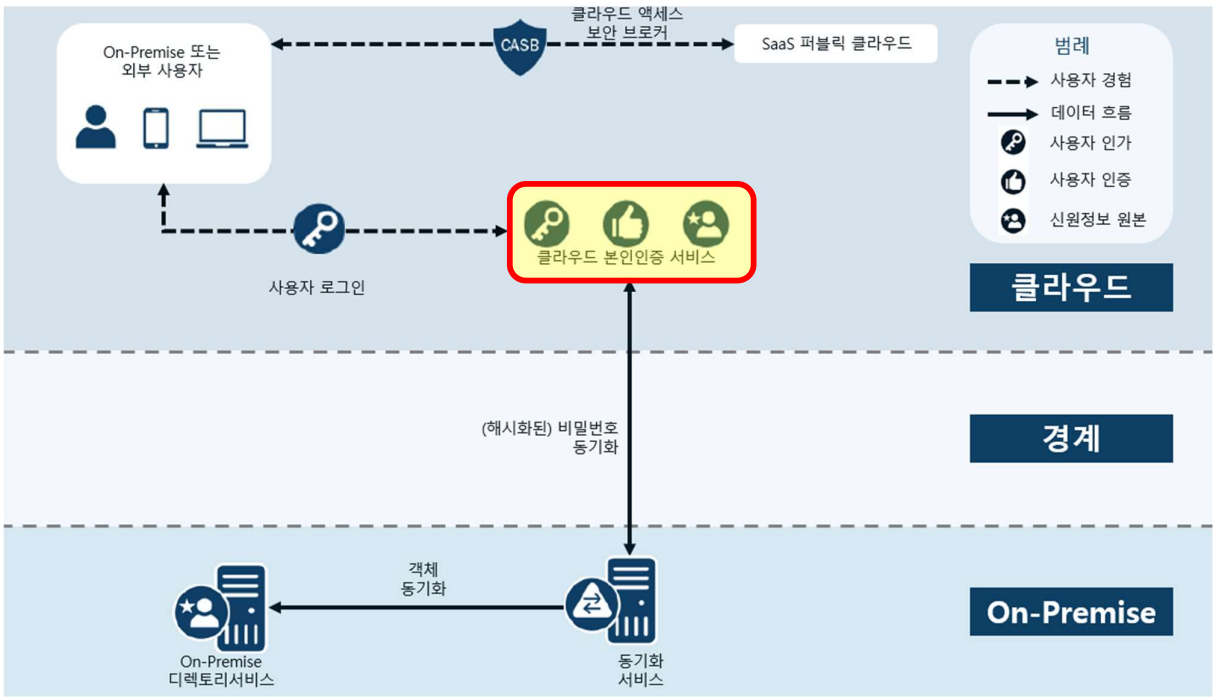
그림 14. 패스스루 아키텍처 구조

3) 비밀번호 동기화

비밀번호 동기화 아키텍처는 사용자가 Cloud 리소스 또는 On-Premise 리소스에 접근하기 위해 하나의 계정만 유지하도록 한다.

이는, 비밀번호 분실 시 대응을 줄이는 데 도움을 준다. 네트워크 내 위치와 관련없이 모든 사용자의 행위는 동일한 계정 및 인증이 사용자에 가장 가까운 지점에서 발생하는 것에 기인한다.

비밀번호를 동기화할 때, 해시 메커니즘 및 암호화를 사용하는 것은 계정 자격증명의 기밀성 및 무결성을 보존하기 위해 가장 중요하다. 활성화된 클라우드 세션을 지닌 사용자는 비밀번호 갱신 이후에도 세션이 중단되지 않지만, 다음 인증 시에 반드시 새로운 비밀번호로 인증해야만 한다.



* 출처: CISA

그림 15. 비밀번호 동기화 아키텍처 구조

4) 클라우드 기본 인증(Passwordless)

클리우드 기본 인증 아키텍처는 사용자가 하이브리드 환경(On-Premise+클라우드)에서 클라우드 기반 본인인증 서비스를 통해 인증할 수 있도록 한다.

클라우드 기본 인증 아키텍처는 “사용자가 클라우드 기반 본인인증 서비스를 통해 인증을 수행하지만” 클라우드 네이티브 아키텍처는 클라우드 애플리케이션만 접근할 수 있다.

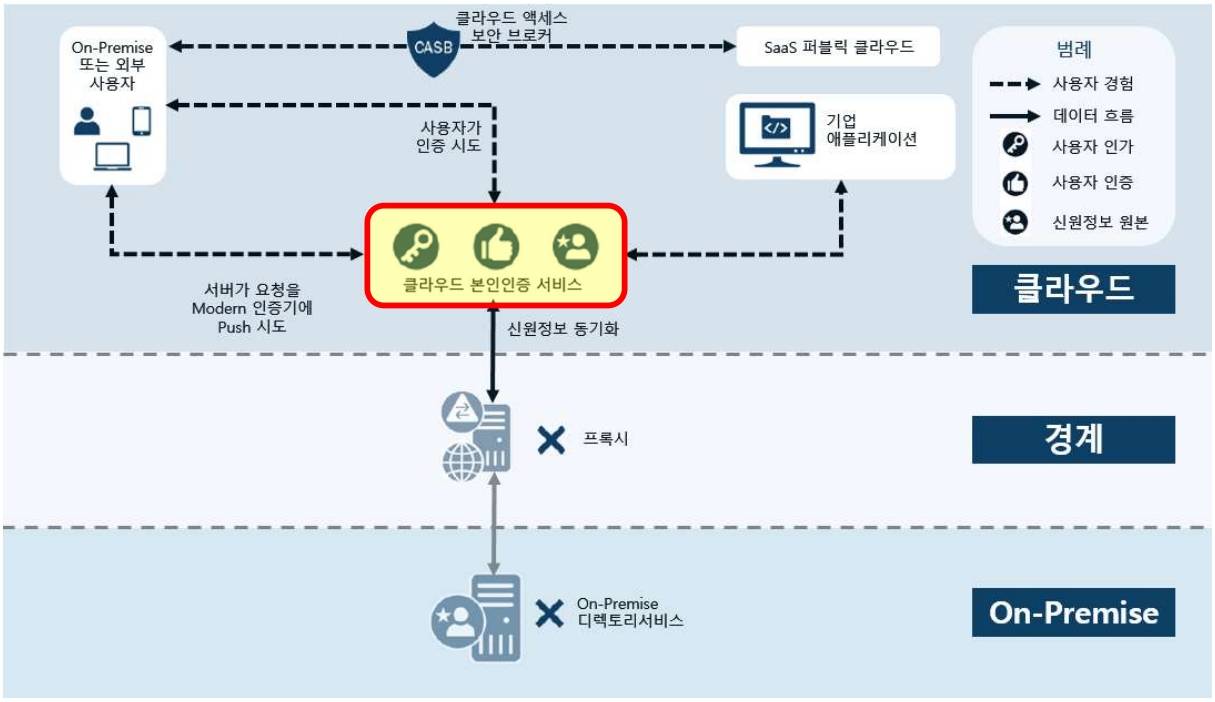
클라우드 기본 인증 아키텍처와 클라우드 네이티브 아키텍처 모두 On-Premise 디렉토리 서비스에 의존없이 본인인증의 모든 부분을 처리한다. 그러나 클라우드 환경과 On-Premise 환경 모두 지원하는 클라우드 기본 인증 아키텍처와 달리 네이티브 아키텍처는 클라우드 환경만 지원하는 차이점을 지닌다.

기업은 클라우드 기본 인증 아키텍처로 전환할 때 고려할 많은 옵션이 지닌다. 예를 들면 다양한 클라우드 서비스 업체, 지속적으로 확장되는 서비스 그리고 기업의 요구사항을 반영해야 한다. Modern 인증기를 활용하고 Passwordless 인증 메커니즘을 지원하며, On-Premise 애플리케이션에 대한 접근을 허용하는 일반적인 클라우드 기본 인증 아키텍처를 소개한다.

클라우드 기본 인증 아키텍처는 관련 법률 또는 컴플라이언스 문제가 없다면 대부분의 기업에 적용할 수 있다. 기업은 전환을 위해 기존 사용 중인 On-Premise 리소스 및 인프라를 활용해야 한다.

예를 들면 기업은 더 많은 시스템과 애플리케이션, 프로세스, 사용자, 장치 및 기타 리소스 등을 클라우드 기본 인증 아키텍처로 활용하기 위해 점진적으로 구성할 수 있다. 이러한 맥락에서 이전에 도입한 본인인증 아키텍처 중 하나를 채택한 기업은 클라우드 기본 인증 아키텍처를 새로운 기본 또는 보조 인증 요소로 처음에 사용하여 마이그레이션을 용이하게 할 수 있다.

다만 이 아키텍처를 채택하기 위해 요구되는 계획, 리소스 및 노력의 양이 상당할 수 있다. 일부 기능에 기업의 클라우드 본인인증 서비스를 내장하도록 구현하는 것 보다는 기업에서 제공하는 대부분의 서비스를 IAM 요구사항을 준수하면서 대부분의 클라우드 서비스와 원활하게 서로 상호작용하도록 구현하는 것이 어렵기 때문이다. 이 아키텍처를 위해 Modern 인증 프로토콜을 포함하여 클라우드로 애플리케이션을 마이그레이션하고 운영중인 서비스(예: 티켓팅 서비스, 안티바이러스)를 업데이트하는 것은 클라우드 본인인증 서비스에 대한 의존성을 더 높일 수 있다.



* 출처: CISA

그림 16. 클라우드 기본 인증 아키텍처 구조

5) 하이브리드 본인인증 아키텍처 4 가지 비교

지금까지 언급한 본인인증 아키텍처 4 가지를 비교한 결과는 다음과 같다.

인증 아키텍처	페더레이션	패스스루 인증	비밀번호 동기화	클라우드 기본 인증
신원정보 원본	On-Premise 디렉토리 서비스	On-Premise 디렉토리 서비스	On-Premise 디렉토리 서비스 및(또는) 클라우드 기반 본인인증 서비스	클라우드 기반 본인인증 서비스
데이터 흐름	인증시 사용자 자격증명은 클라우드 본인인증 서비스 또는 페더레이션 서버에서 On-Premise 디렉토리 서비스로 전달됨	인증시 사용자 자격증명은 클라우드 본인인증 서비스에서 On-Premise 디렉토리 서비스로 전달됨	리소스 위치에 따라 사용자 자격증명은 클라우드 본인인증 서비스 또는 On-Premise 디렉토리 서비스에서 인증됨	사용자는 클라우드 본인인증 서비스에 의해 인증됨
장점	- Legacy 인가 및 인증 방법을 지원하며 Legacy 인증기와 Modern 인증기로 점진적으로 전환 가능 - 스마트카드, IC 칩 내장된 신분증을 통한 Passwordless 인증 지원	- 편리한 인증기능 제공 - 하이브리드 환경 (On-Premise+클라우드) 내 SSO 통합	- 편리한 인증기능 제공 - 하이브리드 환경 (On-Premise+클라우드) 내 SSO 통합	- 편리한 Modern 인증 기능 제공 - 클라우드 서비스의 모든 기능 활용 가능 - 클라우드 또는 하이브리드 환경 (On-Premise+클라우드) 에서 모두 구현 가능
보안 고려사항	- On-Premise 디렉토리 서비스에 침해사고 발생시, 비인가 엔티티가 중심이 되어, Cloud 본인인증 서비스에 대한 접근권한 획득 가능 - 권한이 있는 계정을 On-Premise 페더레이션을 신뢰하지 않는 'cloud-only' 계정으로 Cloud Identity 서비스 및 SaaS 퍼블릭 클라우드 애플리케이션에 보관할 것을 권장함. 이렇게 하면 침해사고가 발생한 On-Premise 환경에서 클라우드로 측면 이동(Lateral Movement)이 제한됨	- On-Premise 디렉토리 서비스에 침해사고 발생시, 비인가 엔티티가 중심이 되어, Cloud 본인인증 서비스에 대한 접근권한 획득 가능 - 침해사고 발생한 On-Premise 디렉토리 서비스를 통해 공격자가 사용자 인증하는 행위를 방지하기 위해, 클라우드 본인인증 서비스에서 MFA 를 강제할 수 있음	- 인증을 위해 클라우드 본인인증 서비스의 리소스 및 기능을 사용하므로, Brute-force 또는 비밀번호 암호 스프레이 공격받기 쉬움 - 호환성 문제로 취약한 해시 암호화 알고리즘을 사용하면 공격에 취약하므로, 적용할 수 있는 가장 안전한 해시 암호화 알고리즘을 On-Premise, 클라우드 모두에 적용해야 함	- 비록 전통적인 비밀번호 정책을 지원할 수 있지만, 의도한 구현은 클라우드에 자격증명을 저장하고, 절대 사용자가 계정에 비밀번호를 설정하지 않도록 하는 것 - 각 사용자의 공개키는 클라우드에 저장하고, 각 사용자의 비밀키는 FIDO 지원 단말기, 스마트카드, IC 칩 내장된 신분증에 저장하도록 하기 위함 - FIDO2 에 사용할 Modern 인증기 도입 전 주의 깊게 평가를 해야 하며, 인증기는 안전하게 자격증명을 생성하고, 프롬프트가 발생하면 Assertion 시그니처를 생성해야 함

* 출처: CISA

표 5. 본인인증 아키텍처 4 가지 비교

■ 도입 시 권고사항

1. Passwordless 인증 지원하는 SSO 프로토콜 사용 권고

기업은 SSO 프로토콜을 선택할 때 Passwordless 인증을 지원하는 SAML(Security Assertion Markup Language), OAuth, OIDC(OpenID Connect), Kerberos, 스마트카드/PKI 등을 고려해야 한다. 일반적으로 SAML 과 OIDC 가 많이 사용되지만, 엄격한 보안이 필요한 경우 스마트카드/PKI 방식이 권장된다.

스마트카드/PKI 인증은 사용자를 인증하기 위해 사용하는 스마트카드 또는 IC 칩 내장된 신분증과 같은 물리 장치에 비밀키나 X.509 인증서를 저장한다. 스마트카드는 서버와 클라이언트 인증서 간 mutual 인증을 제공하기 위해 mTLS 를 사용한다. 스마트카드 PIN 은 신원정보 제공자가 한 번 확인한 후, 오프라인 장치를 인증하기 위해 캐시할 수 있으며, 여러 애플리케이션 인증에 사용될 수 있다.

2. Passwordless 인증 미지원 Legacy 시스템에 비밀번호 관리자 사용 권고

Passwordless 인증이 적용되지 않는 Legacy 시스템은 비밀번호 관리자(Password Manager)를 사용해 비밀번호 관련 취약점을 방지할 수 있다.

비밀번호 관리자 사용시의 기본 자격증명이나 자격증명 저장소가 비인가 접근으로 유출될 위험이 존재한다. 또한 비밀번호 관리자가 사용자 단말기의 외부 DB 에 의존할 경우, 공급업체의 서비스 중단으로 서비스 가용성에 영향을 받아 사용자가 접근하지 못하는 문제가 발생할 수 있다.

자격증명 저장 시 암호화를 사용하고, 단말기 또는 캐시된 자격증명 저장소를 지원하는 비밀번호 관리자를 이용하여 단일 장애점(Single Point Of Failure, SPOF) 위험을 줄이고, 보안 수준을 향상시킬 수 있다.

비밀번호 관리자의 유형은 클라우드 기반, On-Premise 기반, 모바일 단말기 기반, 웹 브라우저 기반이 있다. 이러한 비밀번호 관리자는 자동완성, 다크웹 모니터링, 장치 동기화, 저장공간 암호화, MFA, 역할기반 권한, 보안정책 강제, 암호화된 비밀번호 생성기, SSO 통합, Team Sharing 기능 등을 지원한다.

3. 동적 접근 정책 적용을 위한 상황기반접근제어 사용 권고

상황기반접근제어(CBAC)는 역할기반접근제어(RBAC)와 속성기반접근제어(ABAC)를 결합한 접근제어 방식으로, 단말기 수준의 신호를 단서로 사용해 동적 접근 정책을 적용할 수 있다.

상황기반접근제어는 NIST SP 800-207(Zero Trust Architecture)의 제로트러스트 7 가지 기본 원리 4 번째인 '동적 정책으로 리소스에 대한 접근 결정'을 수행한다. 해당 정책에는 클라이언트 식별자, 응용, 요청을 보낸 자산 상태, 행동 및 환경 속성 등이 포함되며 동적으로 리소스 접근 결정이 필요한 게 특징이다. 동적 정책으로 리스스에 대한 접근 권한 부여시, 최소 권한 원칙을 준수해야 한다.

CBAC 솔루션을 도입할 경우, 학습 기반 AI 및 머신러닝을 사용하여 동적 접근 정책을 수립할 수 있다. 학습을 진행할 수록 표준 사용자 행동, 중요자산 또는 특정 리소스에 접근하는 사용자를 구분할 수 있으며, 각 행동에 기반하여 로그인 시도에 맞는 보안대응이 조정되므로 유용하다.

■ 맺음말

지금까지 '안전한 클라우드 환경을 위한 하이브리드 본인인증 아키텍처 적용 전략'에 대해 살펴봤다. 앞에서 다룬 본인인증 아키텍처 4 가지 중에서 실무에서 안전한 본인인증 아키텍처는 Passwordless 를 지원하는 Modern 인증기를 사용하는 페더레이션 아키텍처와 클라우드 기본 인증 아키텍처임을 알 수 있었다.

Passwordless 인증 도입 시, 플랫폼, 운영체제 및 웹 브라우저 버전 지원 여부가 솔루션 별로 상이할 수 있으니 도입 전에 반드시 면밀히 검토해야 한다. SSO, Phishing-resistant MFA, 제로트러스트는 안전한 클라우드 애플리케이션을 위한 하이브리드 본인인증 아키텍처를 적용하는 데 있어서 빠질 수 없는 핵심 개념이다. 페더레이션 아키텍처 또는 클라우드 기본 인증 아키텍처를 적용해 기업이 안전하게 On-Premise 서비스 및 클라우드 서비스를 운용할 수 있기를 기대한다.

SK 쉴더스는 보안 컨설팅부터 맞춤형 솔루션 구축까지 A to Z 클라우드 보안 서비스를 제공하고 있다. 안전한 클라우드 환경 구축과 관련한 보다 자세한 내용은 SK 쉴더스 홈페이지 또는 문의하기를 통해 확인할 수 있다.