CIAM의 필요성과 필수기술

이슈N뉴스

금융IT 분야에서 **이슈가 되고 있는 뉴스**들을 살펴봅니다.

글. 김선애 기자(데이터넷)

넷플릭스 계정 공유가 불가하게 될 것으로 보인다. 넷플릭스는 그동안 계정 공유를 통제하지 않았는데, 후발주자들이 빠르게 성장하면서 신규 가입자 증가세가 둔화된 것도 중요한 요인이지만, 고객들의 계정정보 보안을 위해서 계정공유를 제한해야 한다는 고민이 있었던 것으로 분석된다.

계정 공유는 많은 보안 사고를 일으킬 수 있다. 공유되는 계정은 유출 가능성이 높다. 사이버 범죄자들은 수집한 계정으로 웹 서비스에 접속해 상품 주문 등 서비스를 이용하는 한편, 사용자의 개인정보를 추가로 수집해 다른 공격에 이용할 수 있다.

크리덴셜 스터핑(Credential Stuffing)의 예를 들어보면, 공격자가 미리 입수한 계정정보를 이용해 웹서비스에 로그인해 악의적인 활동을 할 뿐 아니라, 추가 개인정보를 입수해 지하세계에 비싼 가격으로 판매하거나 지능적인 피싱이나 스피어피싱 공격에 사용한다.

보안에 취약한 *ID/PW*

코로나19로 사용자들이 이용하는 애플리케이션이 늘어나면서 고객 계정정보를 관리하는 것이 더 어려워졌다. 사용자들은 업무용 애플리케이션 뿐만 아니라 금융거래, SNS, 전자상거래, 게임, 온라인 스트리밍 등 다양한 애플리케이션을 이용하는데, 대부분 하나의 ID/PW를 이용해 로그인한다. 그래서 개인정보 유출사고가 발생하면 다른 애플리케이션으로 의심스러운 로그인 시도가 집중된다.

보안을 강화하기 위해 서비스 기업은 고객에게 ID와 비밀번호를 웹 서비스마다 다르게 설정할 것을 권고한다. 특히 비밀번호는 대·소문자, 숫자, 특수기호까지 섞어 길고 복잡하게 설정하며, 일정기간마다 바꾸도록 한다. 길고 복잡한 문자와 숫자의 조합은 결코 보안을 강화하지 못한다. 공격자는 사용자 기기에 악성코드를 심어 사용자가 키보드에 입력하는 값을 탈취한다. 자동화 봇을 이용하기 때문에 길고 복잡한 비밀번호는 아무 소용이 없다.

사용자들이 자동로그인을 사용하거나 SNS 계정을 이용해 간편로그인을 한다. 자동로그인은 악성코드 감염 시 모든 계정정보가 유출될 가능성이 있고, SNS 간편로그인 역시 SNS 계정 정보가 탈취되면 연동된 모든 웹서비스의 정보가 위험하다.

사용자 계정을 보호하기 위해 고객들에게 몇 단계에 걸친 강력한 인증을 요구하는 것도 옳은 방법은 아니다. 액센츄어 조사에 따르면 63%의 고객이 온라인 경험이 좋지 않으면 그 서비스에서 떠날 것이라고 답했다. 사용자와 서비스가 처음 만나는 단계인 '회원가입'과 '로그인'이 불편하면 사용자는 더 편리하고 안전한 서비스를 찾아 떠나게 마련이다.

고객경험 개선·보안 향상 위한 *CIAM*

사용자의 온라인 활동이 다각화되면서 서비스 채널과 기기, 플랫폼, 터치 포인트가 증가하고 있어 고객을 보호하는 것이 더 어려워졌다. 그래서 고객의 계정과 접근을 관리하는 CIAM(Customer Identity and Access Management)에 관심이 모이고 있다.

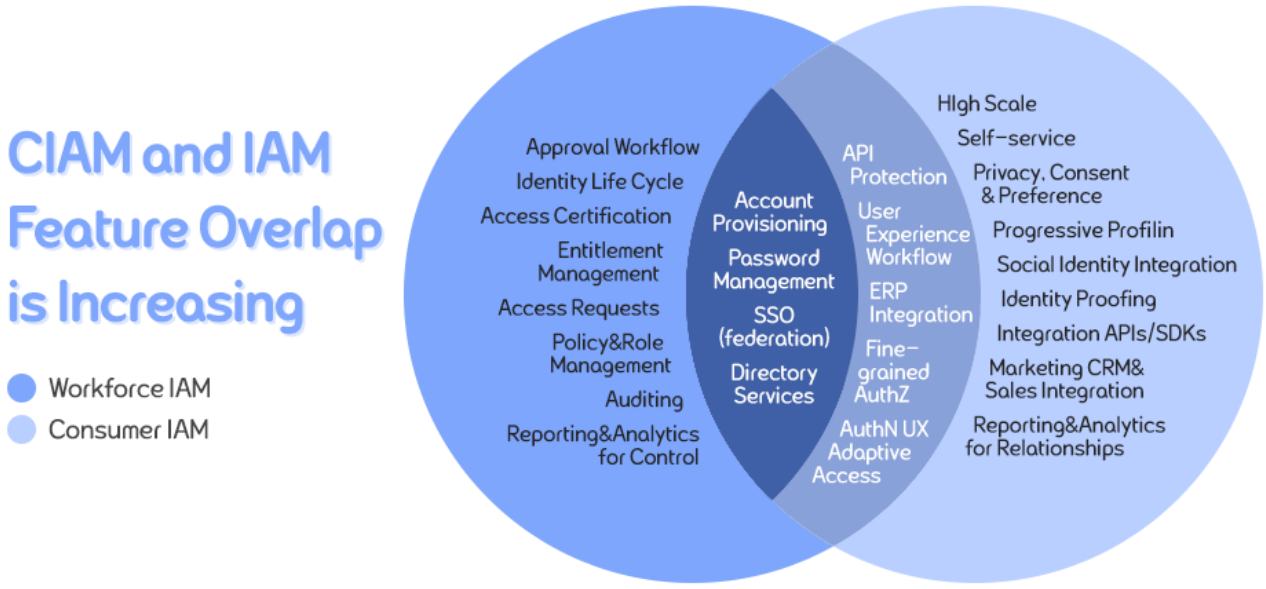
CIAM이 새로운 개념은 아니지만, 최근 보안과 고객경험(CX)이 부상하면서 집중 조명을 받고 있다. 시장조사기관 마켓앤마켓(Markets and Markets)에 따르면 CIAM이 고객 커뮤니케이션을 개인화하는데 도움이 되며, 안전하고 끊김 없는 CX를 제공해 고객과 더 나은 관계를 구축할 것이라고 내다봤으며, 이 시장이 연평균 15.1% 성장, 2020년 76억달러에서 2025년 153억달러로 성장할 것으로 예상했다.

포레스터는 기업이 고객을 확보하고 유지하는 프로세스가 빠르게 진화하고 개인정보보호 요구사항

을 충족할 수 있는 진보한 CIAM이 필요하다고 설명하며 “포괄적인 동의와 관리, ID 확인과 제품화된 통합, 확장성을 제공할 수 있으며, 사용자 경험을 개선할 수 있어야 한다”고 강조했다.

CIAM을 ‘엔터프라이즈에서 사용하는 IAM(Identity and Access Management)을 일반 사용자에게 적용한 것’이라고 이해하는 시각도 있는데, 이는 고객 계정 보호라는 제한적인 측면에서만 바라본 것이다. CIAM은 고객의 서비스 접근을 통제하는 것뿐만 아니라 고객 맞춤형 서비스 제안, 고객 판매주기 관리 등 고객관리 측면으로도 확장하고 있다.

CIAM과 IAM의 공통점과 차이점



출처: 가트너

CRM·컴플라이언스 등 다양한 역할 통합

포레스터의 「포레스터 웨이브: CIAM, 2020년 4분기」 보고서에서는 CIAM이 인증과 권한부여 뿐 아니라 CRM(Customer relationship management), 웹 분석, 개인정보 관리 등 다양한 솔루션이 통합되고 있다고 설명한다. 또 각 지역·국가 및 산업마다 다른 개인정보 보호 규제 등 컴플라이언스를 만족할 수 있도록 사용자 약관과 개인정보 보호 및 동의 관리가 포함되어 있어야 한다고 소개했다.

이 같은 요구를 만족하는 CIAM은 고객 데이터를 수집하고 사용하는 과정을 투명하게 관리해 GDPR과 같은 개인정보 보호 규제의 요구사항을 만족한다. 중앙집중화 되고 단순화된 데이터 거버넌스와 오케스트레이션을 통해 디지털 ID와 동의·인증·권한관리를 관리하며, 비용과 IT 복잡성을 줄

일 수 있다. 더불어 고객은 자신이 선택한 방법으로 쉽게 로그인하고 최소한의 개인정보만을 제공해 개인정보에 대한 자기결정권을 강화할 수 있다.

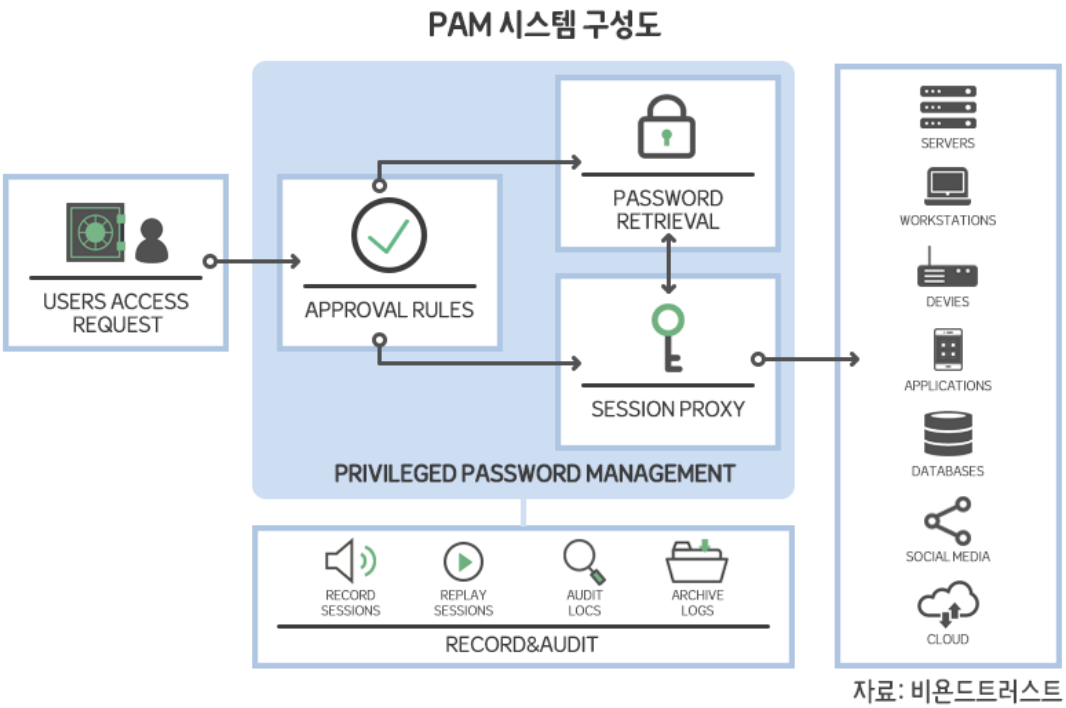
CIAM은 B2C뿐 아니라 B2B2C, B2B까지 확장되고 있다. 기존 CIAM은 일반 사용자 고객을 대상으로 했지만, 디지털 트랜스포메이션이 진행되면서 B2B2C, B2C 모델도 '고객(Customer)'이 일반 사용자 뿐 아니라 기업 사용자나 파트너 직원, 대고객 서비스를 위한 직원이 될 수도 있다. 따라서 일반 사용자 환경뿐 아니라 각 산업군 별로 특화된 인증 및 접근제어 요건, 사용자 환경 등에 맞춤형으로 적용될 수 있는 유연성이 필요하다.

더불어 서비스 기업이 CIAM에 대한 전문성이 없어도 빠르고 편리하게 CIAM을 적용할 수 있어야 한다는 점도 중요 고려사항이다. 애플리케이션 시대로 접어들면서 고객의 변화에 따라 애플리케이션이 신속하게 개발·개선·수정돼 배포되어야 하는데, CIAM에 대한 전문적인 지식이 없는 개발자들도 서비스에 쉽게 적용하고 다양한 애플리케이션과 연동할 수 있도록 해야 한다.

CIAM 필수 기술

권한관리 실패로 인한 보안 사고는 셀 수 없이 많이 발생한다. 가트너는 IaaS·PaaS 보안을 위해 클라우드 액세스 관리 권한을 보호해야 하며, 민감 데이터에 대해 최소 권한을 부여해야 한다고 조언한다. 「안전한 IaaS 및 PaaS를 위해 꼭 알아야 할 5가지」 보고서에서 가트너는 ID관리(IM)와 액세스 관리(AM), ID·거버넌스 관리(IGA)를 사용해 클라우드 사용 권한을 모니터링 해야 하는데, 세분화 된 역할 기반 액세스 제어(RBAC), 속성 기반 액세스 제어(ABAC) 모델은 모든 워크로드에서 과도한 권한이 제거되도록 최소 권한 원칙에 따라 설계돼야 한다고 조언했다. 또한 특권권한관리(PAM) 도구를 사용해 관리자 계정을 보호하고, 권한을 정기적으로 검토하며 조정해야 한다고 조언했다.

이러한 요구는 클라우드에만 해당하는 것이 결코 아니다. 온프레미스와 멀티·하이브리드 클라우드 모두 공통으로 통용되는 것으로, 특히 특권권한 관리는 대규모 보안사고를 막기 위해 필수라고 할 수 있다. 데브옵스의 권한관리를 예로 들어보면, 데브옵스의 빠른 개발·운영 환경에서 어떤 사람이 어떤 프로세스에 개입해 개발·테스트·운영하는지 정하는 과정이 필요하다. 다수의 개발·운영자들은 하루에도 수십만개의 서비스를 개발하게 되는데, 모든 서비스마다 접근 가능한 개발자와 운영자를 수동으로 배치하는 것은 불가능한 일이다. 자동화된 권한관리 솔루션으로 허가된 사람만 허용된 절차에 배정돼 CI/CD 프로세스를 완성도 있게 운영할 수 있게 한다.



PAM 솔루션은 국내에서 시스템 접근제어, 패스워드 관리, 시큐어OS(서버보안) 등으로 불리기도 하지만, 실제 PAM은 이러한 포인트 솔루션보다는 광범위한 영역에서 특권권한을 관리한다. 온프레미스와 멀티·하이브리드 클라우드, IT·OT·IoT 전 영역에서 특권권한을 관리하고 제로 트러스트 기반 접근이 가능하게 된다.

앞서 설명한 요구사항을 만족하기 위해 CIAM 솔루션은 ▲사용자 인증과 접근관리 ▲고객 경험 개선 ▲광범위한 API 지원과 API 보안 ▲쉽고 편리한 개발과 운영, 확장성과 유연성 ▲보안과 컴플라이언스 등의 요건을 갖추고 있어야 한다.

- **사용자 인증과 접근관리**

사용자 인증과 접근관리는 CIAM의 기본이 되는 요소다. 사용자 본인이, 정상 상황에서, 사용자 스스로의 의지로, 주어진 권한 내의 서비스로 접근한다는 것을 인증한다. 사용자가 원하는 방법의 본인확인 절차를 거칠 수 있도록 선택 가능한 다양한 옵션을 제공하는 것이 좋다.

적응형 인증을 적용해 정상 상황에서 중요도가 낮은 서비스로 인증할 때는 자동로그인·간편인증 등을 통해 쉽게 접속하도록 하며, 중요도가 높은 서비스 접속을 요구할 때 보안 수준이 높은 추가 인증을 거치도록 한다.

평소와 다른 기기를 이용하거나 장소에서 접속했을 때, 서울에서 로그인하고 5분 후 싱가포르에서 로그인을 시도하는 등 의심스러운 상황이 발생했을 때, 로그인 후 정상 사용자의 행위로 볼 수 없을 만큼 빠른 속도로 서비스 페이지를 호핑하거나 정상 거래 프로세스를 따르지 않을 때 등 이상 정황

으로 의심될 때는 접근 요청을 중단하고 상황을 파악하도록 한다.

- **고객 경험 개선**

CIAM은 고객경험(CX)을 반드시 고려해야 한다. CX를 통해 고객 접근성을 높이며, 웹·모바일 등 다양한 채널에서 접근할 수 있도록 지원한다. 회원가입과 로그인 시 번거로운 등록 양식을 작성하도록 요청하는 대신 SNS, 이메일 로그인 등 다양한 방법을 선택할 수 있도록 한다.

패스워드 없는(Passwordless) 로그인은 CX 개선에 도움이 된다. 패스워드리스는 실제로 비밀번호를 없애는 것이 아니라 사용자가 비밀번호를 입력하는 대신 대체 인증 수단을 사용할 수 있도록 하는 것을 말하며, 생체인증, QR인증이 주로 많이 사용된다.

SSO(Single Sign On)를 통해 한 번 인증으로 다른 서비스에 별도 인증 없이 이용할 수 있도록 사용자 편의성을 제공하는 것이 필수다. 또 개인화를 통해 다른 채널에서 수집한 선호도를 활용해 모든 채널에서 더 나은 경험을 교차 판매하고 홍보할 수 있도록 하는 것도 좋은 방안이다.

서비스에서 사용자 경험을 고도화할 때, MFA(Multi-factor Authentication)는 반드시 필요하다. 결제 혹은 민감한 개인정보 입력 등 보안 수준이 높은 접속을 시도할 때, 혹은 평소와 다른 접속 정황이 나타났을 때 보안 수준이 높은 추가 인증 수단을 요구해야 한다. OTP, SMS·SNS 인증, ARS 인증, 생체인증 등 MFA를 이용할 수 있다. MFA를 위한 인증수단은 보안 수준에 따라 고객이 선택할 수 있어야 한다.

- **광범위한 API 지원과 API 보안**

고객이 사용하는 다양한 애플리케이션과 연동해 사용자 경험을 개선하기 위해 광범위한 API 지원과 보안이 필요하다. API 액세스 관리를 위한 표준 기술을 사용해야 하며, API에 대한 무단 접근이

나 API 계정 탈취, API의 논리적인 결함으로 인한 취약점 등을 관리할 수 있는 보안 대책도 마련돼야 한다.

- **쉽고 편리한 개발과 운영**

현대 애플리케이션은 수명이 매우 짧다. 빠르게 개발해 배포하고 소비자의 반응을 수집해 수정하는 과정을 거쳐야 하며, 소비자의 요구가 달라졌을 때 이에 맞는 앱을 신속하게 개발하고 서비스해야 한다. 더불어 사용자가 폭증했을 때에도 문제없이 지원할 수 있도록 높은 확장성이 요구된다.

다양한 요구 조건에서 CX와 컴플라이언스, 보안 등 다양한 문제를 감안하면서 앱을 적용하기 어렵다. 대다수의 개발자들은 이 분야에 대한 전문성을 갖지 못하며, 하루가 급한 서비스 출시에 있어 다양한 고려사항을 충분히 검토할 시간도 없다.

IAM 전문기업 옥타(okta)가 제품·엔지니어링 리더를 대상으로 조사한 결과, 응답자의 80%가 CIAM을 새로운 애플리케이션과 통합하는데 한 달 이상 걸려 시장의 변화에 신속하게 적응할 수 없다고 답했다. 조직의 41%는 CIAM 전담 팀이 없으며, 개발자의 34%는 CIAM 솔루션이 새로운 애플리케이션을 시작하거나 이전 애플리케이션을 업데이트할 때, 원하는 기능을 개발하지 못했다고 답했다.

이 같은 문제를 해결하기 위해 CIAM은 보다 쉽게 개발 단계에 적용될 수 있도록 개발자 친화적이어야 한다. 또한 다양한 개발환경에 최적화될 수 있도록 유연성을 높여야 하며, 중소기업이나 스타트업도 CIAM을 이용해 CX 개선과 고객보호 요건을 만족시킬 수 있도록 합리적인 가격으로 제안되어야 한다.

- **보안과 컴플라이언스**

보안과 컴플라이언스는 CIAM의 핵심 중 핵심이라고 할 수 있다. 보안에 실패하면 기업의 존폐를 걱정할 수준의 심각한 피해가 발생할 수 있기 때문이다. 고객의 개인정보는 법에 정해진 최소한의 범위로 수집하고, 안전하게 암호화해 보관하며, 고객정보 활용에 대한 기록을 반드시 남겨 고객이 열람을 요청했을 때 즉시 제공할 수 있어야 한다. 고객 계정정보는 반드시 암호화하고 키는 HSM 등을 통해 안전하게 보호해야 하며, 암호화 데이터와 키 관리 시스템에 대한 강력한 접근 통제를 적용해야 한다.

CIAM를 설계할 때, 컴플라이언스는 매우 복잡한 여러 사항을 고려해야 한다. 각 지역별, 국가별로, 혹은 산업별로 개인정보를 수집할 수 있는 범위와 수단, 보호 및 활용 방법 등이 다를 수 있다. 따라서 개인정보 제공 동의를 받을 때 해당 지역·국가·산업의 컴플라이언스를 고려해야 하며, 그에 맞는 관리 체계를 자동으로 적용할 수 있어야 한다.

보안과 컴플라이언스에 실패했을 때 과징금·소송비용 등 금전적인 문제만 발생하는 것이 아니다.

핑아이덴티티 조사에 따르면 55%의 데이터 유출 등의 사고를 일으키는 것 보다 허가 없이 개인 데이터를 공유하는 기업에 더 실망하고 다시 그 회사의 제품을 사용하지 않을 가능성이 높다고 답했다. 또 63%는 회사가 고객의 데이터를 보호할 책임이 있다고 답했으며, 계정을 탈취한 공격자로 인한 피해를 막기 위해 기업에서 사기거래방지(FDS) 등을 운영해야 한다고 답했다.

편의성·보안 극대화된 *CIAM*

CIAM은 오래 전부터 도입·운영되어오던 솔루션이지만, 고객 경험이나 마케팅, 영업 등 넓은 영역까지 영향을 미치게 된 것은 최근의 일이다. 모바일이 고객 디지털 경험의 중요 수단으로 자리잡으면서 새로운 서비스가 고객에게 더 쉽게 다가갈 수 있게 됐으며, CIAM을 통해 여러 비즈니스 가치를 창출할 수 있게 됐기 때문이다.

그러나 CIAM이 반드시 갖춰야 할 CX 향상이나 보안·컴플라이언스, 개발자 지원 등의 문제는 아직 충분히 성숙됐다고 할 수 없다. 가트너의「2019년 고객경험 혁신 조사」에 따르면 “많은 기업들이 지난 3년 이내에 CX 프로그램에서 위기 상황에 직면했다. 53%이 조직이 CX 개선에 있어 재정적 압력을 받았으며, 60%는 경영진 지원 부족, 59%는 ROI를 입증하는데 어려움을 겪었기 때문”이라고 밝혔다.

CIAM에 대한 소극적인 태도는 애플리케이션 시대로 접어들면서 빠르게 개선되고 있는 것으로 보인다. 특히 우리나라의 경우 편의성이 극대화된 다양한 인증 서비스를 경험하면서 더욱 편리하고 안전한 CIAM을 요구하게 됐다.

고객은 애플리케이션이 어떻게 개발되었으며, 애플리케이션 간 어떤 상호작용을 하는지, 얼마나 많은 사용자를 지원하는지 관심 없다. 고객은 자신이 원하는 서비스가 신속하고 편리하게, 그리고 안전하게 제공되기를 바란다. 이를 위한 필수 솔루션 CIAM이 지속적으로 성장을 이룰 것으로 기대된다.

* 저작권법에 의하여 해당 콘텐츠는 코스콤에 저작권이 있습니다.
* 따라서, 해당 콘텐츠는 사전 동의없이 2차 가공 및 영리적인 이용을 금합니다.