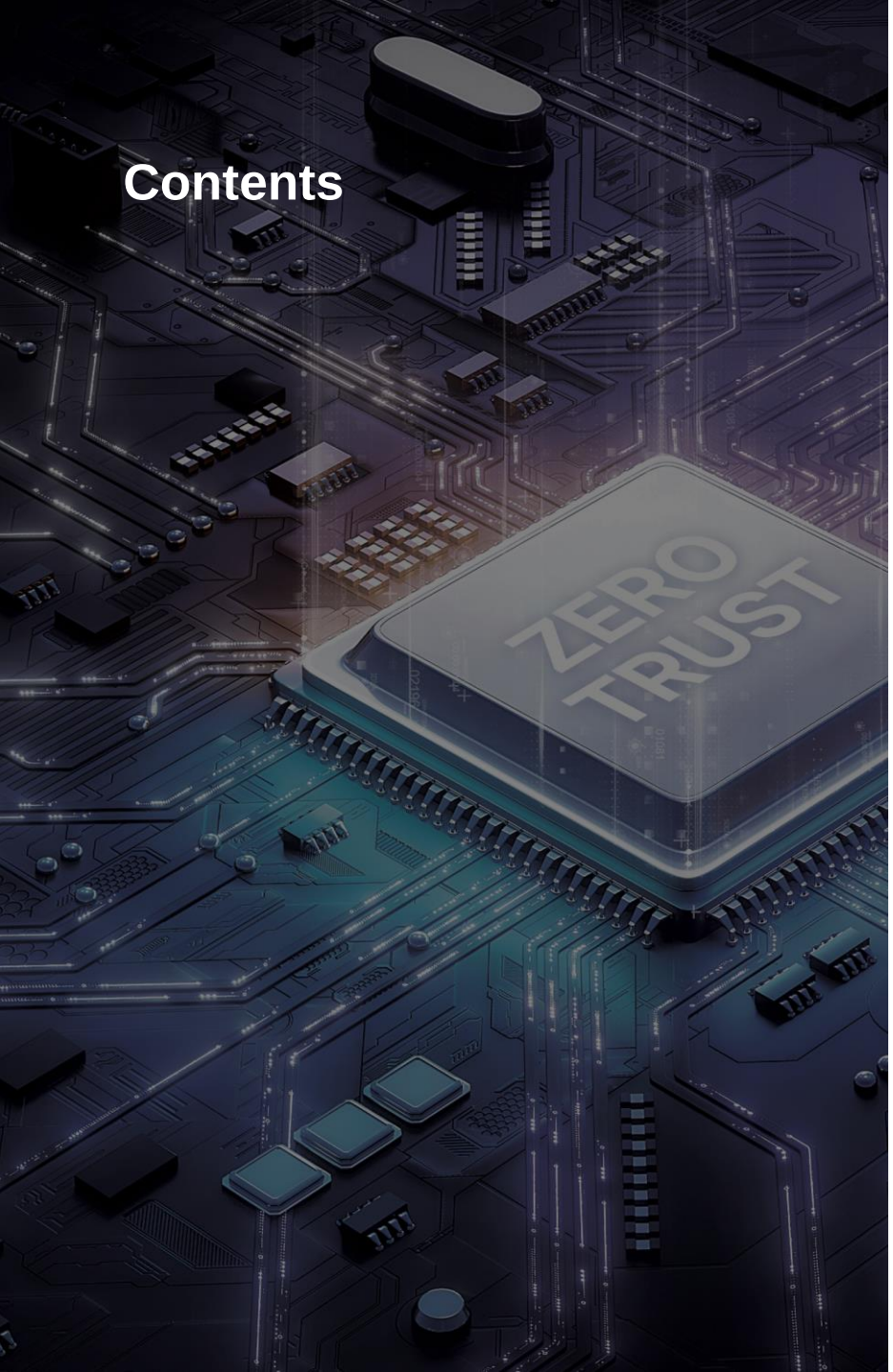
제로트러스트 시대,
의료 기관에서의 내부 통제 강화 방안

라온시큐어 김태진 전무

2024.05.21



Contents

01

배경 및 현황

1.1 인증 체계 변화 인식

보안에 취약한 인증수단은 언제 터질지 모르는 시한폭탄으로 기업과 기관을 위협

現 패스워드 기반 인증 체계 변화 및 **사용자 인증 강화** 필요성 증가

해킹 등 위협/공격에 대한
보안 취약

사용자의 패스워드
이용 불편

패스워드에 대한
관리 비용 발생

업무/시스템
접근 통제 어려움

관리(운영)자 측면 문제점

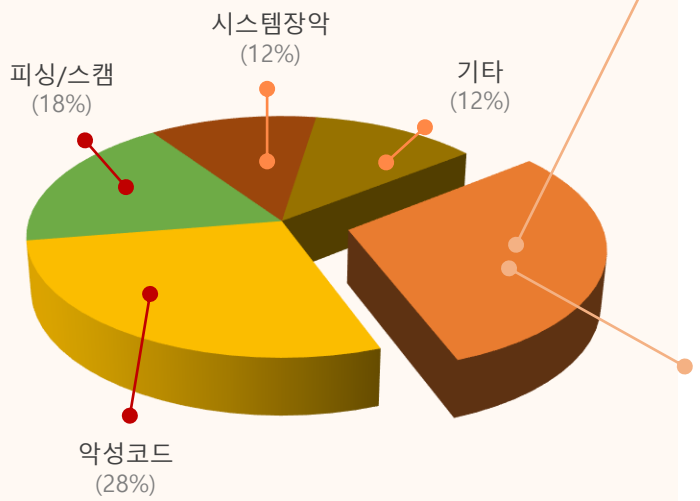
- 패스워드 관리 어려움 및 보호를 위한 지속적인 관리 발생
- 패스워드 공유, 훔쳐보기 등의 취약점으로 내부 통제 어려움
- 해킹 사고로 인한 대규모 개인정보 및 비밀번호 유출 위험

사용자 측면 문제점

- 다수의 업무/시스템별 패스워드 관리 및 이용의 어려움
- 주기적인 패스워드 변경으로 인한 피로도 누적
- 사용자 계정 정보를 노린 다양한 해킹 위험 존재

국내 보안 침해사고 유형별 발생 통계

2023년 상반기
유형별 침해사고 발생 통계

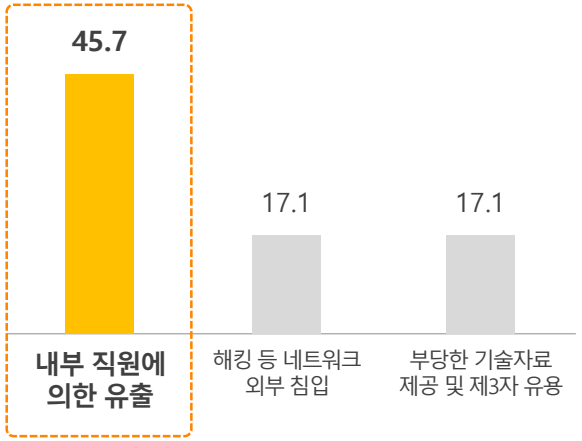


출처 : EQST 2023 상반기 보안 트렌드, SK쉴더스

중요정보유출(30%)

- 취약점을 이용한 정보 탈취 후, 다크웹이나 블랙마켓 등을 통해 판매
- 최근 텔레그램, 디스코드와 같은 암호화 채널을 활용하여 거래하는 추세
- 해킹 그룹 랩서스의 국내외 대기업 기밀정보 탈취 사례 有

기업 내 중요정보 유출/탈취 피해 유형



내부 직원에 의한 중요 정보 유출 사고 다수 발생

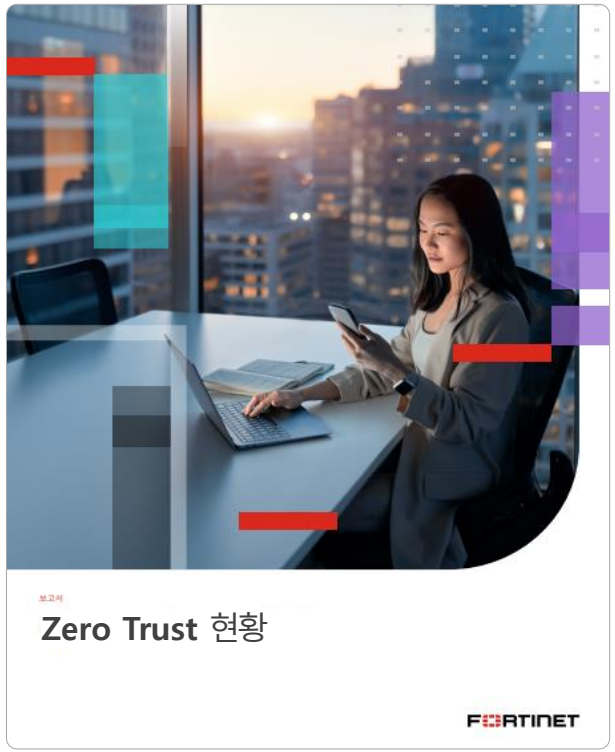
재택/원격근무자로 인한 내부 정보 유출 위험 증대

통제 정책 및 시스템 미비로 인한 유출 피해 확산

02

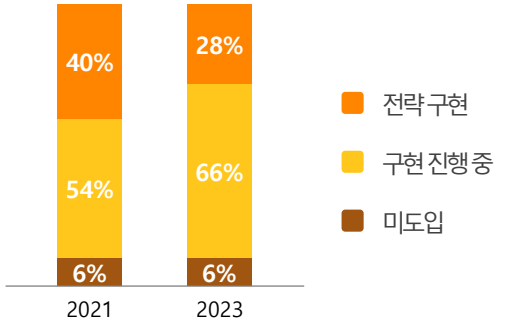
사용자 인증 트렌드

“경계 중심의 통제 정책에서 인증 중심의 통제 정책으로의 변화 필요성 증가”

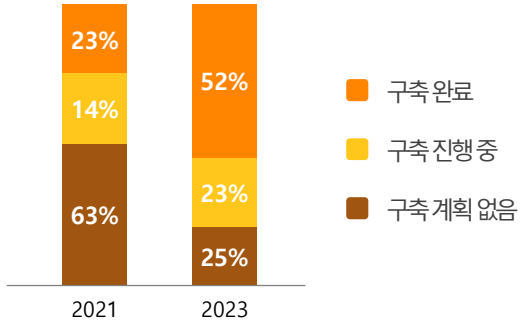


Zero Trust 성숙도 모델

Zero Trust 구현 현황 변화



Zero Trust 중, MFA 부문 투자/구축 계획



출처 : 2023 Zero Trust 현황, FORTINET

2023년도 Zero Trust 현황 요약

규모에 상관없이 거의 모든 조직에서
Zero Trust 전략을 적극적으로 구현

기업들은 보안 침해의 영향을 최소화하기 위해
모든 요소에 Zero Trust를 구현하고자 노력

2차인증, MFA 등 **Zero Trust** 기반
사용자 인증을 위한 투자/구축 계획 확대

다수의 기업에서 **Zero Trust** 전략을
구현하고 있지만 **통합과 관련된 문제에 직면**

“ **인증 후 접속** 및 **보호 자원에 접속**할 때마다 인증 처리(동적 인증) ”

Zero Trust 가이드라인 1.0 주요 내용

Zero Trust의 기본개념과 보안원리, Zero Trust 보안모델의 핵심원칙 및 접근제어 원리,
도입계획 수립을 위한 세부절차 및 도입 참조모델 등을 제시하고 있다.

핵심원칙

Never Trust, Always Verify
'절대 믿지말고, 계속 검증하라'

접근제어 원리

안전하고 지속적인 접근 제어 수행

핵심요소 식별관리

6가지의 핵심 요소에 대한
보안 수준 성숙도 단계별 기능 정의

도입 참조모델

네트워크 모델과 **Zero Trust** 보안
모델 적용 사례를 참조 모델로 제시

참고. 23년도 키워드 10

01 생성형 **AI 보안**

02 **CPO 지정** 의무화

03 개인정보 보호법 위반 **과징금 제도 변경**

04 의료기관 **ISMS_P 인증**

05 의료분야 **공급망 공격**

06 **다중 인증**
의료정보시스템을 중심으로 ID와 패스워드를 입력하는 전통적인 지식 기반 인증 방식을 사용했으나 사용자 인증에 대한 다양한 문제가 발생해 새로운 인증 체계가 요구됨.
ID 공유로 나타나는 오남용과 보안 취약점을 해결하기 위한 **FIDO(Fast Identity Online)** 등이 해결책으로 떠오름

07 **망 분리**

08 **원격의료 보안**

09 **업무연속성**과 **회복탄력성**

10 **Never Trust & Always verify**

참고. 23년도 키워드 10

- 업무연속성 계획(BCP)
- 의료 마이데이터 보안
- 스마트 의료기기 IoT 보안
- 수술실 CCTV 보안
- 보건의료 데이터 가명 처리
- 클라우드 의료정보시스템 보안
- 제로 트러스트 (Zero Trust)
- 타켓형 랜섬웨어
- 의무기록 무단 열람 방지 프로세스
- 의료기관 정보보호 공시

생체정보 관련 법률 및 지침

법제처 국가법령정보센터

- 생체정보를 활용한 사업의 확산과 안정적 운용을 위한 관련 법률/규정/지침 제정

전자서명법

- **제6조(다양한 전자서명수단의 이용 활성화)**
- 국가는 생체인증, 블록체인 등 다양한 전자서명수단의 이용 활성화를 위하여 노력하여야 한다.

개인정보의 안정성 확보조치 기준

- **7조(개인정보의 암호화)**
- 개인정보처리자는…(중략)…**생체인식 정보**를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 **암호화**하여야 한다.

보안제품 내 '생체인증' 기본 탑재

국가정보원(NIS) 국가보안요구사항 V3.0 배포 (2021.9)

1장 서버 공통보안요구사항

- 추가적인 식별 및 인증 기능 제공을 위해 **△FIDO 표준을 준수한 2FA 지원기기△인증서 △일회용 비밀번호 생성기(OTP)** 등을 활용할 수 있다.
- 제품·운용환경에서 지원할 경우 'FIDO 표준을 준수한 2FA 지원기기'를 권고한다.

Zero Trust 및 내부통제 접근 제어를 위한

인증통합플랫폼 기반 사용자 인증 체계 강화 필요

Focus 01
내부업무/사용자 접근 통제 등 관련 컴플라이언스 대응

+

Focus 02
개인화된 인증방식 적용을 통한 보안사고 사전 방지

+

Focus 03
생체인증 도입 트렌드에 맞춘 차세대 시스템 도입

금융/공공 등 컴플라이언스 대응

- 최근 내부 직원에 의한 각종 보안 사고 증가로 인한 시스템 접근 등에 강화된 인증 방식 적용 필요

Zero Trust 및 내부 접근 제어를 위한 인증 강화

- 업무/인터넷망 사용자 단말 접근에 대해 고유한 생체정보를 통한 강화된 인증 시스템 도입 필요

기업 내부 업무 시스템 사용성 및 보안성 제고

- Passwordless 체계 도입을 통한 사용자 업무 편의 및 보안 요구 대응 필요

IT 트렌드 변화에 따른 신기술 도입 요구 증대

- 생체인식 정확도 증가에 따른 다양한 유형의 생체 인식 기술 등장 및 상용화

생체인식 및 다양한 추가 인증 수단에 대한 통합 도입과 함께 일원화된 관리 체계 구축을 통한

안정적인 내부 인증 강화 체계 수립 및 효율성 제고

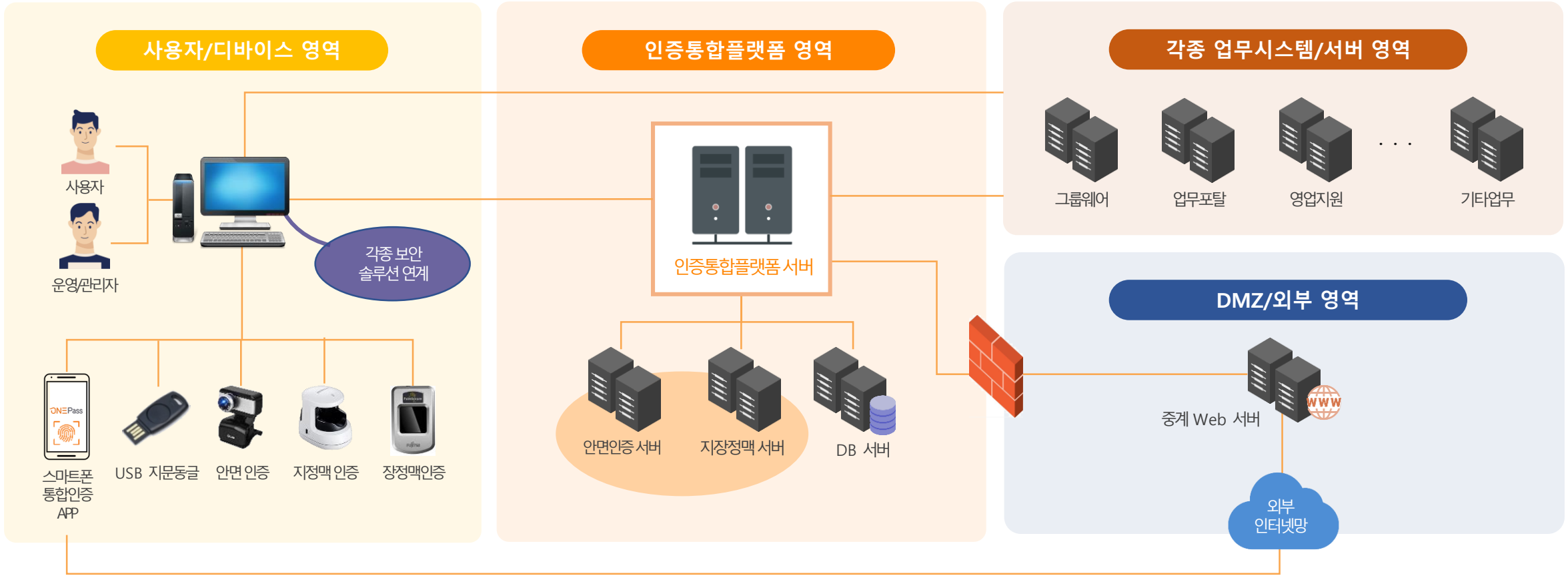
다양한 생체인증 수단에 대한
일원화된 관리 제공

관련 컴플라이언스 및
내부통제 관련 내규 준수

신규 인증수단 도입 시,
유연한 확장성 보장

세분화된 **사용자 인증**
정책 적용 및 관리 지원

인증통합플랫폼 중심의 사용자 및 운영/관리자 측면의 인증 강화 시스템 구성



03

OnePass 인증통합플랫폼

생체인증 및 FIDO 기반 다중요소인증(MFA) 지원 인증통합플랫폼, " OnePass "

OnePass는 FIDO 기반의 인증 수단과 함께 FIDO2, OTP 등 다양한 인증 수단을 제공하는 다중 요소 통합 인증 솔루션으로 안전한 사용자 인증과 함께 효율적인 인증 관리를 위한 정책 설정 기능을 지원하며, On-Premise/Cloud 환경 구분없이 안정적인 구축을 보장합니다.

1. **FIDO Certified 인증**
세계 최초 획득

2. 국내 FIDO 솔루션 분야
점유율 1위

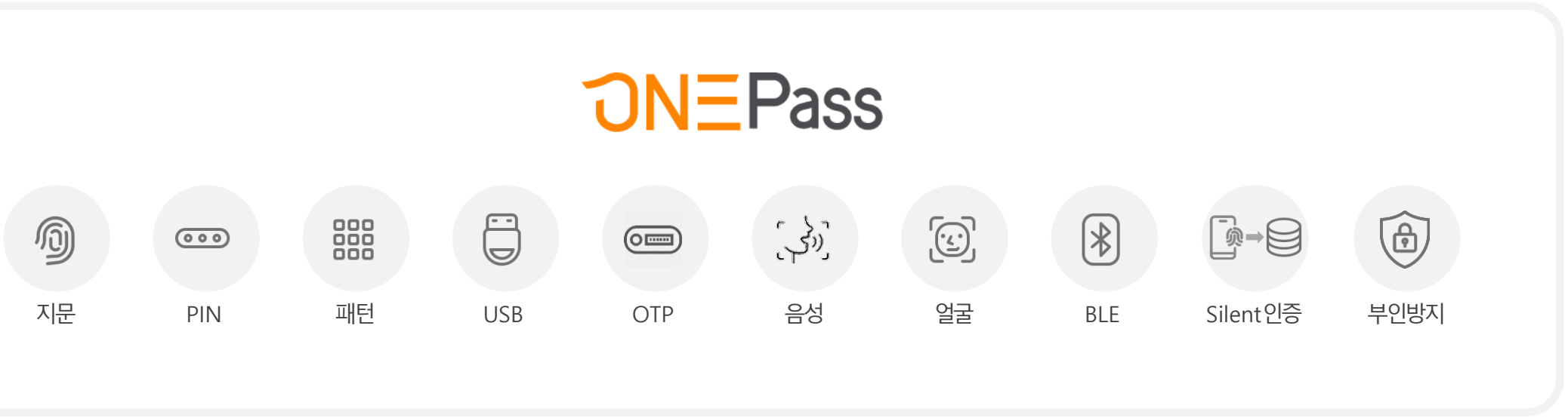
3. **해킹 위협 원천** 차단을
통한 **보안성 강화**

4. 국내 정보보안업체 유일
FIDO 이사회 멤버

국내 고객사
1,000+

OnePass FIDO 기술 사용자
2,000만+

금융결제원 금융권 회원사
180여개
(전체 회원사 중, 80% 수준)



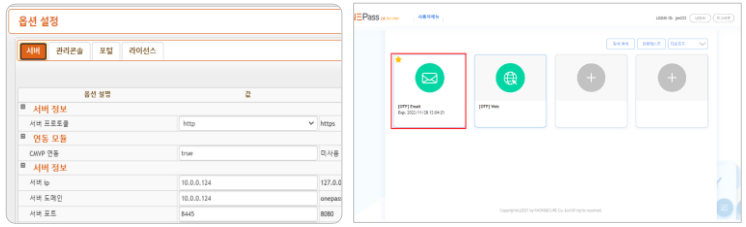
다중 요소 통합인증 환경 구축 지원

사용자 인증 수단 모듈화 설계 및 선택적 적용 지원

비밀번호 관리 대체 편의성 향상 및 관리 비용 감소

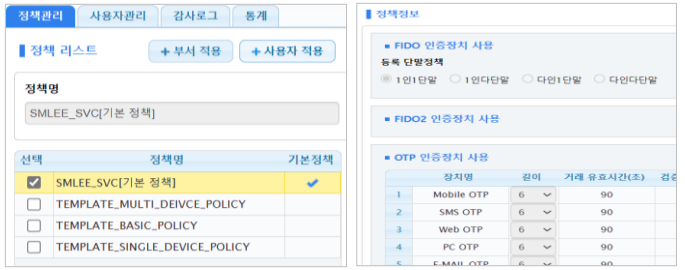
01. 직관적이고 심플한 메뉴 제공

관리 편의성 극대화 및 초기 설치 시 작업 효율성 증대를 위한 안정적 구성 환경 지원
사용자의 다양한 인증수단 관리를 위한 사용자 포털 제공



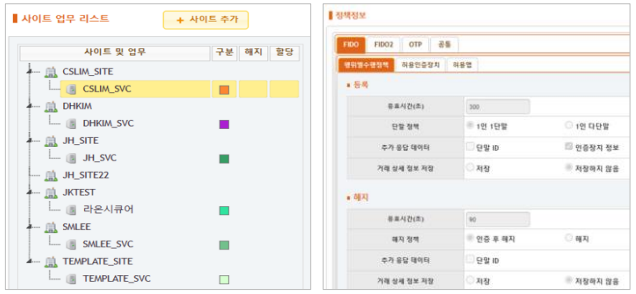
02. 조직/사용자 관리 지원

조직/사용자 정보 동기화 및 정보 관리 기능 제공
조직/사용자별 인증정책 부여를 위한 사용자 포털 관리자 기능 지원



03. B2E 환경 최적 기능 지원

업무/서비스별 사용자에 대한 다양한 인증 정책 수립 지원
인증장치별 세분화된 정책 설정과 정책 적용을 위한 기능 제공

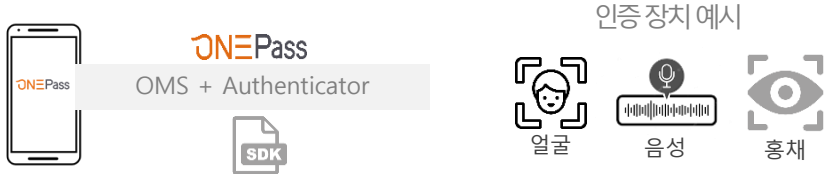


신규 인증수단 및 외부 생체 인증솔루션에 대한 안정적인 연동과 추가 확장을 지원합니다.

FIDO 표준 기반 연계/연동

FIDO 표준을 준수하는 생체인증 솔루션에 대한 추가/확장 시,
OnePass 에서 제공하는 OMS(Open Matcher SDK)를 이용하여
연동 및 연계를 지원합니다.

- **Mobile App 환경 + 내장 H/W 장치**



- **PC Web 환경 + CTAP 지원 H/W 장치**

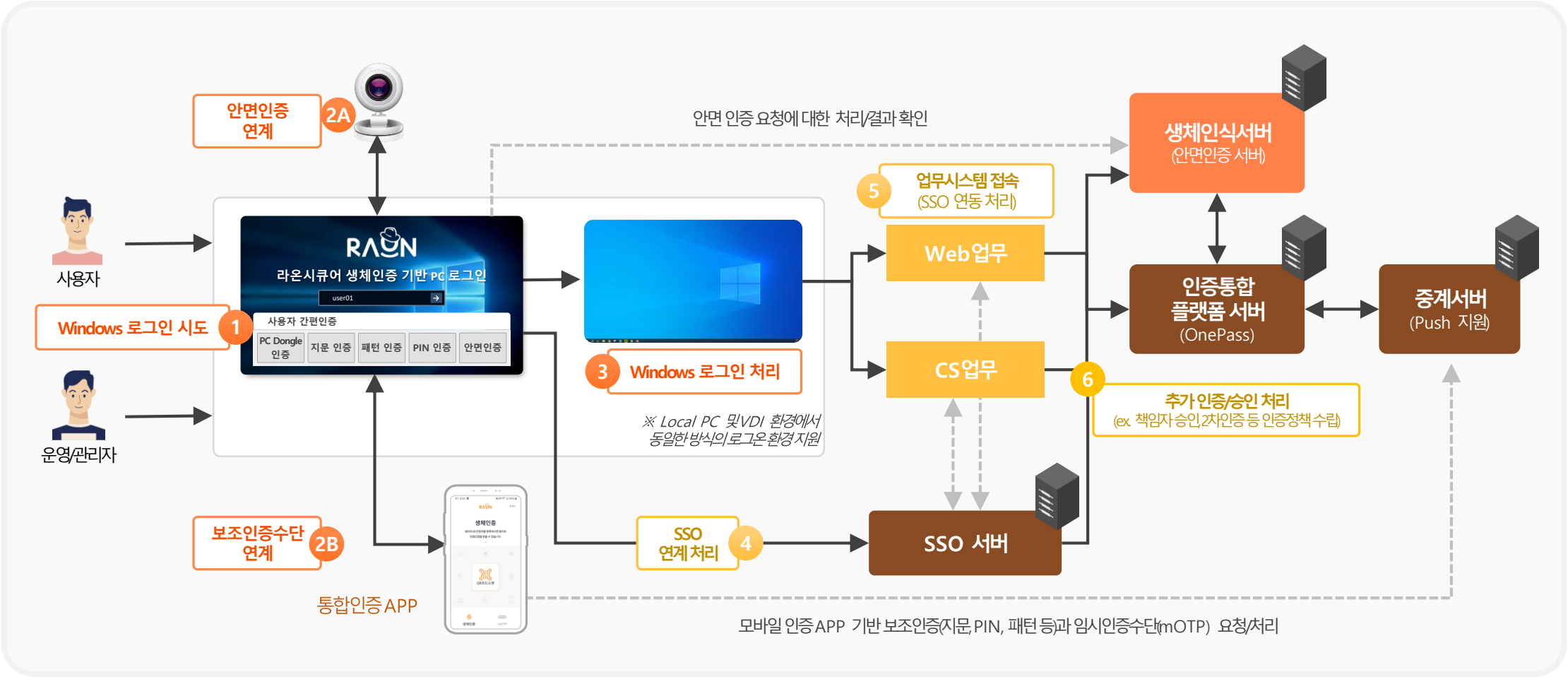
FIDO 비표준 방식 솔루션 연계/연동

FIDO 비표준 생체인증 솔루션의 연계 시,
해당 솔루션 업체와 긴밀한 협력을 통해 안정적인 인증통합플랫폼
연동 환경을 구성합니다.

- **Mobile + 내장 H/W 장치**

- **PC Client + 외장 H/W 장치**

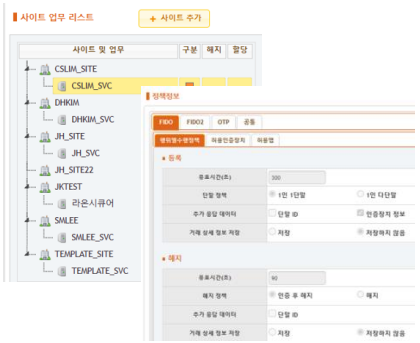
사용자는 PC 로그인 시, **사전에 등록한 인증 수단에 따라 인증을 수행**하며
이에 따라 **다양한 유형의 업무 시스템을 간편하게 인증하여 접근 및 이용**할 수 있습니다.



사이트·업무별 인증 정책과 부서·사용자 별 인증 정책에 근거한 MFA인증으로 조직 내부 사용자에 대한 통제를 강화합니다.

Phase 1
사이트/업무 정책 설정

솔루션 ADMIN 권한을 보유한 관리자가 인증 정책 설정/관리



Phase 2
부서/사용자 별 정책 설정

부서별 관리 담당자가 부서/사용자에 대한 인증 정책 선택적 적용

Phase 3
부여된 인증 정책 기반 MFA 인증 수행

사이트/업무와 부서 정보에 근거한 인증 정책에 따라 사용자 인증 절차 수행

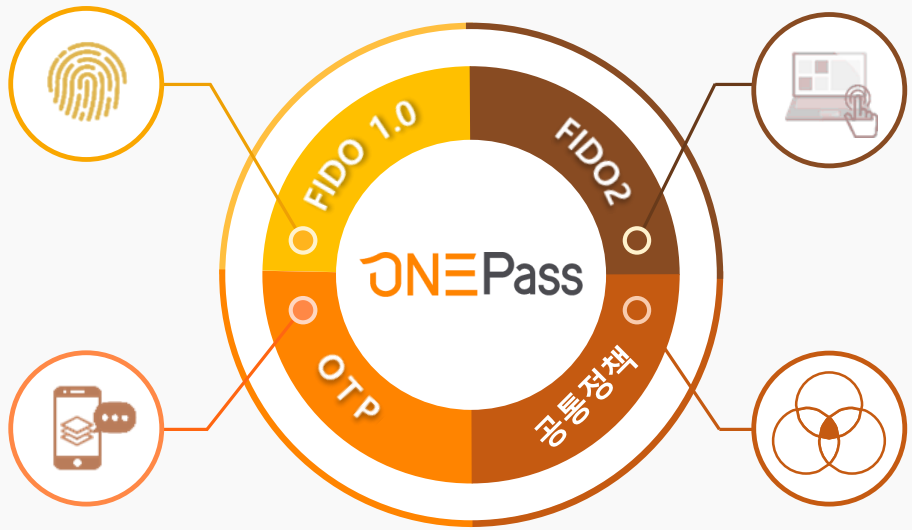
MFA 인증 수단 / 정책 수립 제공

※ Adaptive MFA를 위한 커스터마이징/연계 지원

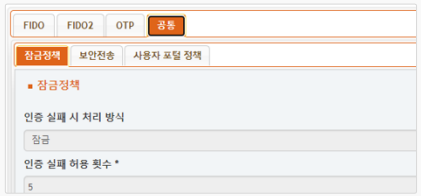
Web 기반의 관리 콘솔을 통한 FIDO1.0과 FIDO2, OTP, 확장인증수단 등 관리기능 통합으로 일원화된 구성/운영 환경을 제공합니다.

<FIDO 1.0 정책정보 관리 화면>

<OTP 정책정보 관리 화면>



<FIDO 2 정책정보 관리 화면>



<공통 정책 관리 화면>

관리 포인트 감소

- FIDO/FIDO2/OTP 아키텍처 동시 운영 지원
- 관리 페이지의 일원화를 통한 효율적 사용자 / 인증수단 관리

효율적인 운영 정책 관리

- 다양한 인증 수단에 대한 일괄적 / 효율적 정책 수립 지원
- 내부 정책 변화에 대한 유연하고, 신속한 대응 지원

시스템/사용자 이력 관리

- 사용자 인증 및 거래 이력 제공을 통해 이상 발생 시, 거래 이력 추적을 통한 관리
- 관리자 감사 이력 조회 기능 제공

OnePass는 **사용자가 직접 인증 수단을 직접 관리**할 수 있도록 포토갤러리 방식의 **사용자 포탈 페이지를 제공**합니다.

사용자 인증 수단 셀프 관리

- 등록된 인증 수단의 인증 방식, 등록 일자, 만료 일자, 활성화 상태 등 인증수단 정보 조회 및 인증 수단에 대한 삭제 기능 제공

사용자 인증 수단 셀프 등록

- 사용자 본인이 사용할 인증 수단을 직접 선택하고, 이를 등록할 수 있도록 다이얼로그 방식의 인증 수단 등록 기능 제공

사용성 제고 및 관리 편의성 확보

- 사용자가 직접 인증 수단 관리를 수행함에 따라 인증 수단 분실, 손망실 등의 상황에 관리자의 도움없이 능동적인 대처 가능

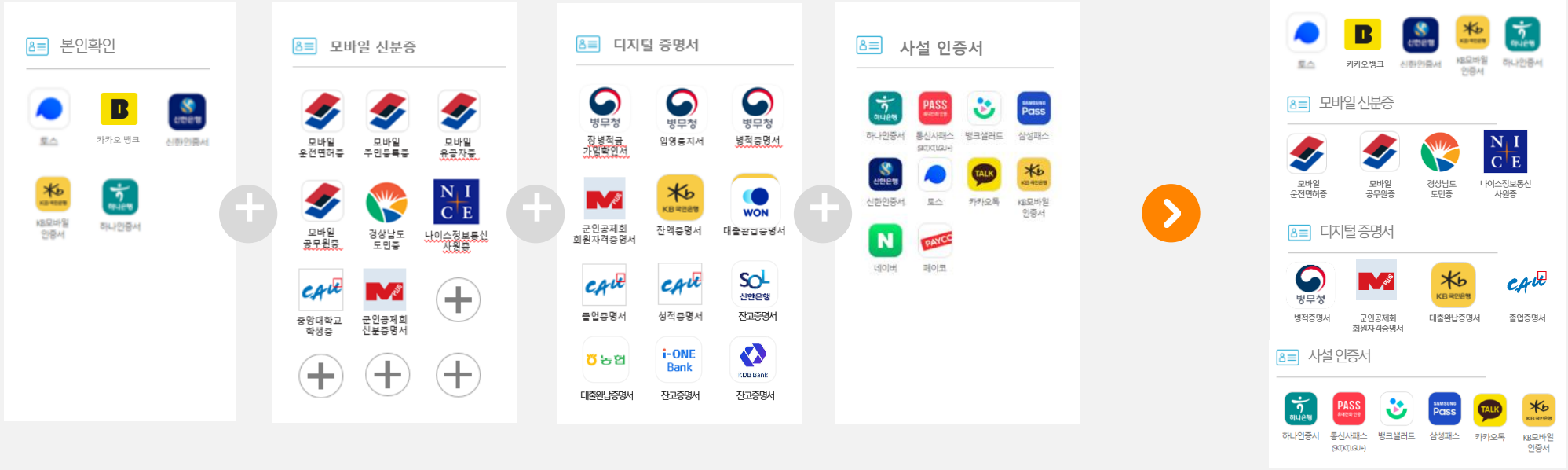
04

OmniOne CX 통합인증

골라 쓰는 재미가 있다!

다양하고 편리한 OmniOne CX 통합인증 서비스

OmniOne CX 통합인증 서비스



인증서 본인확인/모바일 신분증/디지털 증명서/사설 인증서를

한번의 계약을 통해 **하나의 통합 인증창**으로 제공

01. 무한한 서비스 **확장성 및** 시장 변화 **대응성**

- **간편인증, 전자서명, 본인확인, 모바일신분증, 다양한 디지털증명서 활용 가능**
- 정부정책기조와 시장 니즈를 반영하여 업무 다변화시 민첩하게 대응 가능

02. **연동 개발** 및 **유지보수** 용이

- **표준화된 API**를 제공함으로써 쉽고 **빠른 인증서비스 연동** 가능
- 추가되는 인증사업자를 위한 **손쉬운 확장성** 보장
- API 방식 제공하여 고객사에서 원하는 **UI/UX 구성** 가능
- 이용기관에서 원하는 인증서 호출 및 **순서 반영 가능**

03. **개발기간 단축** 및 고객사 리소스 절약을 통합 **비용 절감**

- **고객사 리소스 절약 가능(구축, 계약 비용 정산 리소스 절약)**
- 통합 인증창, 인증 게이트 플랫폼 적용

04. **사용자 편의성** 및 **보안성** 증대

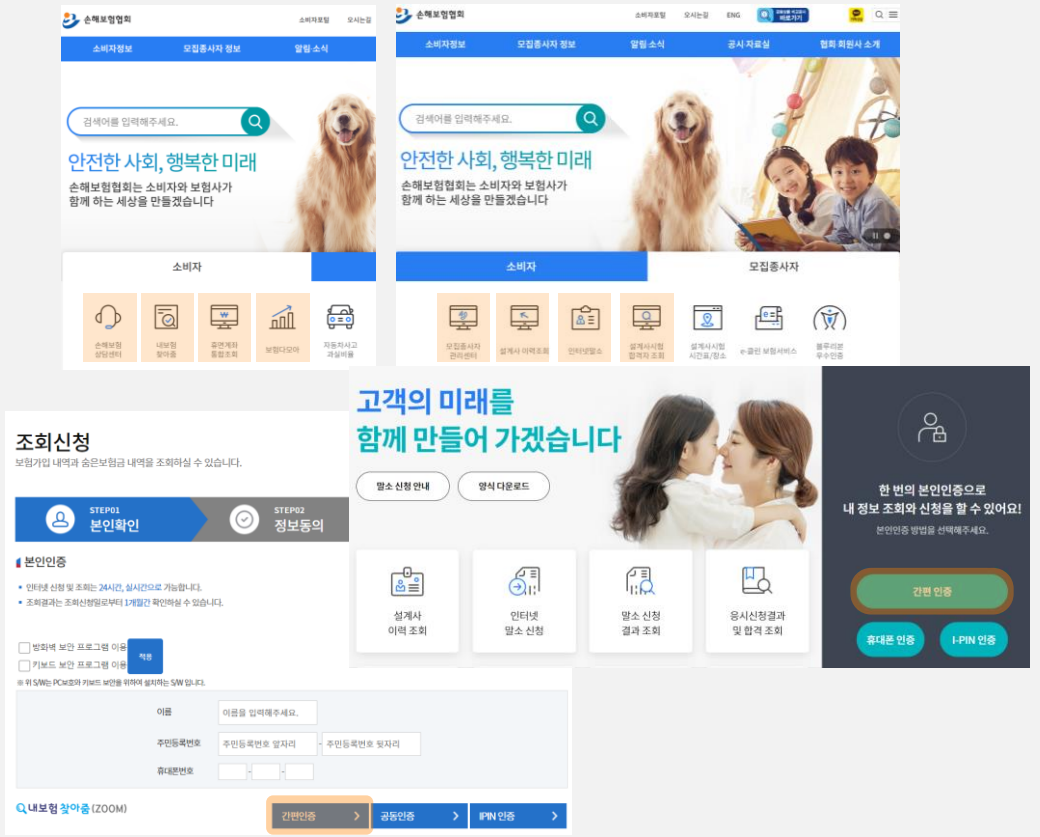
- **별도의 인증서 보관이 필요 없으며, 사용자가 선호하는 전자서명 수단 통합 제공**
- 인증 수단의 선택적 적용을 통한 사용자 인증 편의성 향상과 보안성 강화를 동시 충족

01. 여러 서비스에서 이용하는 본인인증을 대체함으로서 **예산 절감 효과 발생**

02. **이용자들이 선호하는 인증 수단**을 도입함으로서 이용자들의 만족도 제고

03. 시장의 흐름에 따른 편리한 인증 수단 도입에 따라 **인증 트렌드 반영**

04. **한번의 계약으로 협회 내 여러 서비스에 손쉬운 확대**
사례 : 내보험 찾아줌, 보험다모아, 휴면계좌 통합조회 등



성장과 경험의 새로운 디지털 기록 및 증명 'OmniOne Badge'

새로운 디지털 자격증명 수단

학습자의 성과, 스킬을 '인증' 할 수 있는
디지털 수단으로, 블록체인 기반으로
메타데이터를 포함한 자격 증명 제공

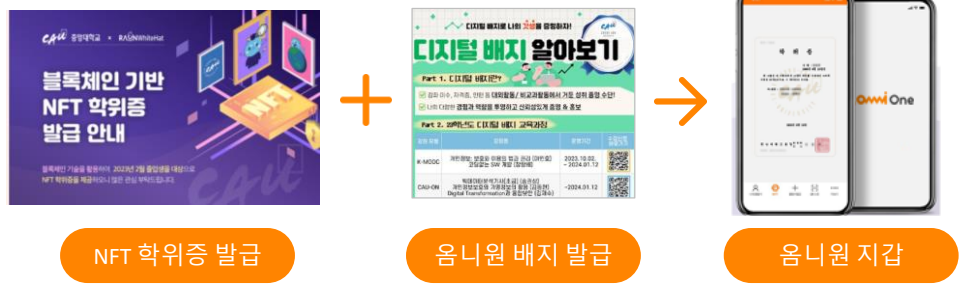
학교(학위증) 국가자격증 민간자격증 스킬과 성과

서비스흐름도

블록체인

디지털 자산에 생명력과 가치를 부여하는 'OmniOne NFT'

하나의 지갑에서 NFT 학위증과 디지털 Badge를 함께 관리



Q&A

감사합니다.

IT 보안·인증
플랫폼 기업
RAON SECURE

간편결제 및 본인인증
솔루션 NO.1 기업
INBIZNET

Trust and Accountability
In the Digital World
digital trust networks

Contact us

서울특별시 영등포구 여의대로 108, 48층(여의도동, 파크원타워2)

02-561-4545 | mkt@raoncorp.com | www.raoncorp.com