nurit

정보자산의 보안강화를 위하여 3단계 인증을 위한

BaroPAM과 타 인증 솔루션 비교

2024. 3.

인증 솔루션 비교

1. 2차 인증이란?

2차 인증은 정보자산의 보안 강화를 위하여 로그인-ID 및 비밀번호(지식기반 인증) 이외에 별도의 추가인증(소유기반/속성기반/행위기반/장소기반 인증)절차를 의미하며, 2 Factor 인증과 2 Channel 인증으로 구분합니다.

2 Factor 인증

2 Factor 인증의 개념도

"지식기반 인증"인 로그인-ID/비밀번호 인증에 다른 요소 즉 소유기반 인증 및 생체인증 요소를 추가한 인증 기법으로 서비스 채널과 인증 채널이 하나로 결합된 형태.

- 다양하고 광범위한 적용, 관리가 단순하고 운영비용 절감.
- 통신망을 사용하지 않기 때문에 보안지역이나 통신장애에 영향을 받지 않아 서비스 보장.
- 모듈인증 방식은 사용자 정보 동기화가 필요 없으며, 통신 및 인증서버 미사용으로 서비스 보장.
- 인증폭주 시 부하분산으로 인증속도 보장.

2 Channel 인증

2 Channel 인증의 개념

2 Factor 인증을 포함한다고 보는 것이 일반적이며, 인증과 서비스를 수행하는 통신망을 서비스 채널과 인증채널로 물리적으로 분리한 형태.

- 구현복잡, 제한적 적용, 관리가 복잡하고 운영비용 증가
- 통신망을 사용하기 때문에 보안지역이나 통신장애에 영향을 받아서 서비스 중단.
- 인증서버 방식으로 사용자 정보 동기화가 필요하며, 인증서버 장애 시 서비스 중단 및 인증 폭주 시 인증속도 저하.
- 우회기술 및 피로공격으로 사이버 범죄에 악용 (삼성전자, MS, 우버, 레딧 등)

※ **다중 인증(MFA)은 최소 두 가지 이상의 본인인증 요소를 이용하여 본인 여부를 인증하는 것으로 2차 인증은 다중 인증의 일종.**

Copyright © Nurit Corp. All rights reserved.

인증 솔루션 비교

2. 2차 인증 구분 및 특징

2차 인증은 별도의 인증서버가 필요한 Hard 방식의 1st 인증 (1세대 인증) 와 별도의 인증서버가 존재하지 않아 관리가 필요 없고, 손쉽게 적용할 수 있는 소프트웨어 방식(jar, so, dll 등의 인증모듈 호출)의 2nd 인증 (2세대 인증) 로 구분합니다.

1st 인증(타사)	2nd 인증(BaroPAM)
❖ 인증서버 방식(SHA-I, SHA-Ⅱ:SHA-512), Gateway(+Proxy) 방식, 통합인증	❖ 모듈인증 방식(SHA-Ⅱ:SHA-512), PAM방식, 분산(개별)인증
❖ 제로 트러스트(Zero trust) 보안 모델 불가	❖ 제로 트러스트(Zero trust) 보안 모델 적용
❖ 개인별 HMac Key 발급 및 관리	❖ 개인별 HMac Key 발급 및 관리하지 않음
❖ 정적 HMac Key 방식	❖ 동적 HMac Key 방식
❖ 일괄 인증키 생성주기(30, 60초) 적용	❖ 개별 인증키 생성주기(3~60초) 적용
❖ 비영구적 사용 / 추가 비용 발생	❖ 영구적 사용 / 비용 절감
❖ 2차 인증(추가 인증)	❖ 2차 인증(추가 인증), 생체인식 적용
❖ 고가, 제한적 적용, 관리가 복잡하고 운영비용 증가	❖ 저가,다양하고 광범위한 적용, 관리가 단순하고 운영비용 절감
❖ 사용자 정보 동기화 필요	❖ 사용자 정보 동기화 필요하지 않음
❖ 인증폭주 시 인증속도 저하	❖ 인증폭주 시 부하분산으로 인증속도 보장
❖ 통신망 및 인증서버 장애 시 서비스 중단 발생(장애 취약)	❖ 통신망 및 인증서버 미사용, 장애가 발생하지 않음(서비스 보장)
❖ 우회접속, 원격접속, 중간자공격 등 사이버 보안에 취약	❖ 우회접속, 원격접속, 중간자공격 등 사이버 보안에 강함
❖ 간단(느슨)한 구성에서 시작해 더 복잡(견고)한 보안 시스템으로 진화 불가능	❖ 간단(느슨)한 구성에서 시작해 더 복잡(견고)한 보안 시스템으로 진화 가능

Copyright © Nurit Corp. All rights reserved.

인증 솔루션 비교

3. 문자 기반과 모듈인증 방식의 2차 인증

SMS, 이메일 등 문자 기반의 2차 인증은 별도의 인증서버가 존재하는 방식의 통합 인증과 별도의 인증서버가 존재하지 않아 관리가 필요 없고, 손쉽게 적용할 수 있는 모듈 인증 방식의 분산 인증으로 구분합니다.

SMS, 이메일 등 문자 기반의 2차 인증 [타사]	모듈인증 방식의 2차 인증 (BaroPAM)
❖ 인증서버 방식(SHA-I), Gateway(+Proxy) 방식, 통합인증	❖ 모듈인증 방식(SHA-Ⅱ), PAM방식, 분산(개별)인증
❖ 제로 트러스트(Zero trust) 보안 모델 불가	❖ 제로 트러스트(Zero trust) 보안 모델 적용
❖ 1st 인증 (1세대 인증), 사이버 범죄의 1순위	❖ 2nd 인증 (2세대 인증), 생체인식 적용
❖ 개인별 HMac Key 발급 및 관리	❖ 개인별 HMac Key 발급 및 관리하지 않음
❖ 정적 HMac Key 방식	❖ 동적 HMac Key 방식
❖ 일괄 인증키 생성주기(30, 60초) 적용	❖ 개별 인증키 생성주기(3~60초) 적용
❖ 제한적 적용, 관리가 복잡하고 운영 비용증가	❖ 다양하고 광범위한 적용, 관리가 단순하고 운영비용 절감
❖ 사용자 정보 동기화 필요	❖ 사용자 정보 동기화 필요하지 않음
❖ 인증폭주 시 인증속도 저하	❖ 인증폭주 시 부하분산으로 인증속도 보장
❖ 통신망 및 인증서버 장애 시 서비스 중단 발생(장애 취약)	❖ 통신망 및 인증서버 미사용, 장애가 발생하지 않음(서비스 보장)
❖ 보안구역에서 사용 불가	❖ 보안구역에서도 사용 가능
❖ 우회접속, 원격접속, 중간자공격, 우회기술, 피로공격 등 사이버 보안에 취약	❖ 우회접속, 원격접속, 중간자공격, 우회기술, 피로골격 등 사이버 보안에 강함
❖ 간단(느슨)한 구성에서 시작해 더 복잡(견고)한 보안 시스템으로 진화 불가능	❖ 간단(느슨)한 구성에서 시작해 더 복잡(견고)한 보안 시스템으로 진화 가능

Copyright © Nurit Corp. All rights reserved.

인증 솔루션 비교

4. FIDO 인증과 모듈인증 방식의 2차 인증

FIDO(Fast Identity Online)는 Password를 서로 공유하여 인증하는, 공유방식 인증 방식 대신, 사람의 생체정보(지문, 얼굴모양, 홍채 등)나 외부 인증장치(Yubikey, Titan Security key 등)을 사용하여, "Public-Key Cryptography(공개키 암호기술)" 방식으로 보다 편리하고 안전하게 인증 기능을 제공하는 인증 프로토콜 표준입니다.

FIDO 인증 (타사)	모듈인증 방식의 2차 인증 (BaroPAM)
❖ Gateway 방식, 복잡한 아키텍처 구조로 2단계 인증, 통합인증	❖ 모듈인증 방식, 단순한 아키텍처 구조로 3단계 인증, 분산인증
❖ Public-Key Cryptography(공개키 암호기술) 사용	❖ 전세계적으로 인정된 512Bit 표준 Hash 함수 사용
❖ 스마트폰에서 생체인증 후 PKI를 생성하여 전송하는 구조	❖ 스마트폰에서 생체인증 후 OTP를 생성하는 구조(Time Sync)
❖ 비밀번호, 지문, 홍채, 안면 등과 같이 고정된 정적인 보안 (보안에 취약)	❖ 매번 변하거나 한번 사용하고 버리는 일회성/휘발성 같은 동적인 보안(보안에 강함)
❖ 다양한 환경의 정보자산 등에 손쉽게 적용하기 힘듬	❖ 다양한 환경의 정보자산 등에 손쉽게 적용 가능
❖ 도입 시 별도의 서버와 DB가 필요함(최소 서버 3대 필요)	❖ 도입 시 별도의 서버나 DB가 필요하지 않음
❖ 고가, 관리가 복잡하고 운영비용 증가	❖ 저가, 관리가 단순하고 운영비용 절감
❖ 사용자 정보 동기화 필요	❖ 사용자 정보 동기화 필요하지 않음
❖ 인증폭주 시 인증속도 저하(인증속도 느림)	❖ 인증폭주 시 부하분산으로 인증속도 보장(인증속도 빠름)
❖ 통신망 및 인증서버 장애 시 서비스 중단 발생(장애 취약)	❖ 통신망 및 인증서버 미사용, 장애가 발생하지 않음(서비스 보장)
❖ 보안구역에서 사용 불가, 임베디드 시스템 적용 불가	❖ 보안구역에서도 사용 가능, 임베디드 시스템에 적용 가능
❖ 사용자 Device가 변경되면, 모든 서비스 재등록	❖ 사용자 Device가 변경되면, 모든 서비스 등록하지 않음
❖ Device가 고장 나거나 분실되면 서비스 불가	❖ Device가 고장 나거나 분실되어도 대체 방안 제공 (WebOTP, 응급 일회용 인증키)

Copyright © Nurit Corp. All rights reserved.

인증 솔루션 비교

5. 도입 시 검토사항

1. 제로 트러스트(Zero Trust) 개념이 적용되어 있는지?

2. 별도의 인증서버 방식인지, 모듈인증 방식인지?

3. 통합인증인지 분산인증인지?

4. 인증키 생성 및 검증 시 사용되는 키는 정적인지, 동적인지?

5. 제한된 시간 내에 횟수 제한을 할 수 있는지?

6. 다양한 운영체제와 애플리케이션에 손쉽게 적용 및 관리가 단순한지?

7. 간단(느슨)한 구성에서 시작해 더 복잡(견고)한 보안 시스템으로 진화할 수 있는지?

8. 인증 폭주 시 인증 속도는 얼마나 저하되는지?

9. 통신망을 사용하는지?

10. 보안시스템의 우회 및 원격접속을 차단할 수 있는지?

11. 보안지역이나 통신장애에 영향을 받는지?

12. 인증절차 시 데이터를 위변조하여 우회 인증절차에 대한 문제가 없는지?

13. 로그인 계정이나 개인정보의 도난, 스파이 행위, 통신 방해, 데이터 변경 등에 사용되는 중간자 공격(Man-in-the-middle attack)을 방어할 수 있는지?

14. 모바일 문자 메시지로 인증코드를 전송 했을 때 발생하는 심스와핑(SIM-swapping) 공격을 방어할 수 있는지?

15. 리버스 프록시(Reverse Proxy)와 같은 기술을 적용하여 인증을 우회할 수 있는 구조인지?

16. 푸시 알림을 계속 보내 상대방을 지치게 만들어 우발적으로 로그인 승인 버튼을 누르게 만드는 공격인 "MFA 피로 공격(fatigue attacks)"을 방어할 수 있는지?

결론은 "**2차 인증을 도입했다**"는 것이 아니라 기술 및 보안성 등 "**어떤 2차 인증을 도입했느냐**"가 관건.

Copyright © Nurit Corp. All rights reserved.

인증 솔루션 비교

6. 맺는말

망분리로 인한 보안이 강화된다는 것은 어불성설이며, 지금은 정보보안에 대한 인식의 대전환이 필요한 시대.

아직도 보안에 취약한 이런 방식이 사용되고 있다는 현실
▶2차 인증 중 해커들의 가장 좋아하는 적용 방식: Gateway(+Proxy) 방식
▶2차 인증 중 가장 취약한 인증 방식: SMS, 이메일 등 문자기반의 인증
▶2차 인증 중 해커들이 가장 애용하는 우회 기술과 피로공격에 취약한 인증 방식: 2 채널 인증
▶피싱 공격에 잘 속는 링크 방식: QR 코드 방식

정보자산의 보안 강화를 위해서는 가장 중요한 기본 사항
▶인증 절차 시 데이터 위변조를 어떻게 방어할 것인지?
▶계정 정보 도용 및 악용은 어떻게 차단할 것인지?
▶브라우저 자동 로그인은 어떻게 방어할 것인지?
▶우회접속을 어떻게 차단할 것인지?
▶원격접속을 어떻게 차단할 것인지?
▶중간자 공격을 어떻게 방어할 것인지?
▶다중인증(MFA)의 우회기술을 어떻게 차단할 것인지?
▶다중인증(MFA)의 피로공격을 어떻게 방어할 것인지?

무엇보다도 인증키는 본인이 소유하고 있는 인증키 생성매체를 사용해서 본인이 직접 인증키를 생성하여 본인이 직접 입력해야 그나마 정보보안 사고를 예방할 수 있는 최선책.

결론은 "2차 인증을 도입했다"는 것이 아니라 기술 및 보안성 등 "어떤 2차 인증을 도입했느냐"가 관건.
"아무 것도 신뢰하지 않는다" = "아무도 믿지 마라" = "계속 검증하라"

Copyright © Nurit Corp. All rights reserved.

nurit

기억할 필요가 없는 비밀번호!
BaroPAM이 함께 합니다.

감사합니다!

www.nurit.co.kr

서울시 강서구 마곡중앙2로 15, 913호(마곡동, 마곡테크노타워2)
주식회사 누리아이티 대표전화 : 010-2771-4076