nurit

정보자산의 보안강화를 위하여 사용자 식별.인증을 위한

본인 인증이란?

2025. 7.

별첨. 본인 인증

1. 본인인증의 현주소

nurit

별첨. 본인 인증

2. 본인인증 요소

본인인증은 크게 지식기반 인증(What I know), 소유기반 인증(What I have), 속성기반 인증(What I am), 행위기반 인증(What I do), 장소기반 인증(Where you are) 등 5가지 요소로 구분할 수 있습니다.

지식기반 인증 (What I know)	소유기반 인증 (What I have)	속성기반 인증 (What I am)	행위기반 인증 (What I do)	장소기반 인증 (Where you are)
흔히 사용하는 ID와 비밀번호 등을 들 수 있으며, 계정정보 수정 시 '어릴 때 키우던 강아지 이름은' 등의 질문을 설정하는 것 역시 지식기반 인증에 해당함.	사용자가 가진 OTP, 스마트폰, 보안카드, 보안 토큰 등을 들 수 있으며, 오늘날 스마트폰과 전용 애플리케이션을 흔히 사용함.	지문이나 안면, 정맥, 홍채 같은 사람의 고유한 특징을 통해 인증하는 방식으로, 다른 인증과 함께 복합적으로 쓰임.	어떤 인물의 반복된 행동이나 기기 사용 방식 등을 통해 인증하는 것으로, 수기서명 등 다양한 방식이 연구 및 실증되고 있음.	자신이 가진 기기가 특정 네트워크에 연결됐을 때 인증되는 방식. 스마트폰이 집에서 사용하는 공유기에 연결될 경우 화면 잠금을 풀지 않고 바로 사용할 수 있게 설정하는 것을 예로 들 수 있으며, GPS나 이동통신 등을 이용하면 특정 장소에서만 시스템에 접근하도록 구성하는 것도 가능함.

별첨. 본인 인증

3. 본인인증 방식

본인인증은 크게 IP 접속제한, 공인인증서, 일회용 인증키(OTA, One-Time Authentication 또는 일회용 비밀번호), 생체인식 방식 등 4가지 방식으로 구분할 수 있습니다.

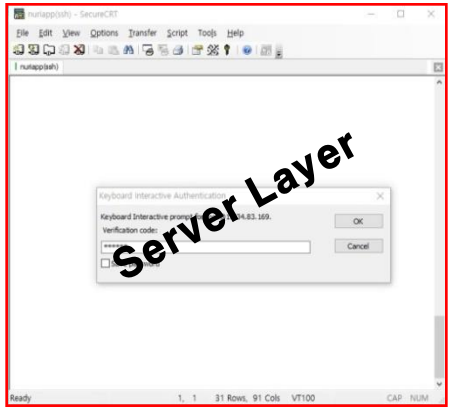
IP 접속 제한	공인 인증서	일회용 인증키 [일회용 비밀번호]	생체인식
IP 접속 제한 방식은 정보 자산(Windows, MacOS, Linux, Unix, Database, 네트워크 장비, 보안장비, 저장장치 등)에 고정된 IP가 필요하기 때문에 IP가 변하는 유동 IP를 사용한다면 접속 제한에 의미가 없음.	공인 인증서 방식은 솔루션 비용이 비싸며, 공인 인증서 인증 모듈의 불편함 때문에 사용하기가 힘들고, 공인 인증서 의무화가 폐지되어 대체할 대안이 필요함.	일회용 인증키 방식은 누구나 사용하기 쉽고, 시간과 장소의 제약을 받지 않으며, 본인이 소유하고 있는 스마트 폰에서 인증키를 생성하기 때문에 간편한 인증 방법인 동시에 한번 사용된 인증키는 재사용할 수 없으며, 인증키 유추가 어려워 다양한 해킹 공격에도 강력한 보안성을 제공함.	요즘 각광 받고 있는 생체 인식 방식은 개인의 신체 특성을 활용하여 개인별로 유일하기 때문에 강력한 보안성을 제공하지만 솔루션 비용이 비싸며, 비밀번호는 해킹을 당할 경우 변경하면 그만이지만, 생체 정보를 해킹 당할 경우에는 변경이 거의 불가능하다. 따라서 최악의 경우 영구적인 피해로 이어질 수도 있음.

별첨. 본인 인증

4. 다계층 인증 체계란?

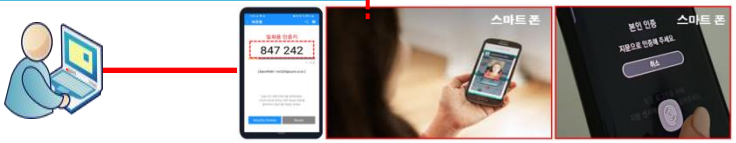
다계층 인증 체계(Multi-layer authentication system)는 중앙 집중식에서 벗어나 탈중앙화로 촘촘한 그물망처럼 보안의 위험을 분산하여 시스템의 모든 계층에 걸쳐 보안을 강화하여 잠재적인 공격으로부터 전체 IT 인프라를 보호하는 포괄적인 보안 전략입니다.

Desktop/PC	Application	Server / Network 장비	Database / Storage
로그인-ID, 비밀번호 이외의 추가 인증(2차 인증) (일회용 인증키)	비밀번호 대체 또는 추가 인증(2차 인증) (일회용 인증키)	로그인-ID, 비밀번호 이외의 추가 인증(2차 인증) (일회용 인증키)	로그인-ID, 비밀번호 이외의 추가 인증(2차 인증) (일회용 인증키)




```
$ sqlplus baropam/baropam

Verification code: 613045

SQL*Plus: Release 11.2.0.1.0 Production on
금 11월 30 09:38:50 2018

Copyright (c) 1982, 2009, Oracle.  All
rights reserved.

SQL> exec twofactor.authenticate(691199);

PL/SQL procedure successfully completed

SQL> exec enable_role('APPOBJACCESS');
PL/SQL procedure successfully completed.
```

Storage Layer



※다계층 인증 체계는 제로 트러스트 모델의 핵심 요소 중 하나이며, 각 레이어별로 인증을 강화하여 네트워크 보안을 혁신하는 안전한 해결책.

nurit

별첨. 본인 인증

5. 다계층 인증 체계의 필요성

조직의 민감한 자산을 보호하고, 규제 준수를 보장하며, 궁극적으로 사용자에게 더욱 안전하고 신뢰할 수 있는 서비스를 제공하는 데 핵심적인 역할을 수행합니다.

보안 강화 및 무단 접근 방지	진화하는 사이버 위협에 대한 대응	규제 준수 및 신뢰도 향상	비즈니스 연속성 확보 및 비용 절감 효과
보안을 획기적으로 강화하여 해커나 무단 사용자의 접근을 차단. ▶단일 인증의 취약성 극복 ▶비밀번호 유출/도용 시 보호 ▶심층 방어(Defense in Depth) 전략	오늘날 사이버 공격은 점점 더 지능적이고 정교해지는 위협에 대한 필수적인 방어선 역할. ▶다양한 공격 방식 방어 ▶다양한 정보 자산 보호	단순히 보안 기술을 넘어 조직의 신뢰도를 높이고 법적, 규제적 요구사항을 충족. ▶법적 및 규제 요구사항 충족 ▶고객 및 사용자 신뢰도 향상	사고 발생 위험을 줄여 비즈니스 연속성을 확보하고 장기적인 비용 절감에 기여. ▶사고 대응 비용 절감 ▶운영 효율성 증대

※다계층 인증 체계는 제로 트러스트 모델의 핵심 요소 중 하나이며, 각 레이어별로 인증을 강화하여 네트워크 보안을 혁신하고 있다.

별첨. 본인 인증

6. 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.

nurit

별첨. 본인 인증

7. 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(Hard 인증)

- ❖ 인증서버 방식(SHA-I), Gateway(+Proxy) 방식, 통합인증
- ❖ 중앙 집중 방식, 단일 지점 공격 방어에 취약
- ❖ 토큰, 카드 위주(인증키 생성기)
- ❖ 개인별 HMac Key 발급 및 관리
- ❖ 정적 HMac Key 방식
- ❖ 일괄 인증키 생성주기(30, 60초) 적용
- ❖ 비영구적 사용 / 추가 비용 발생
- ❖ 2차 인증(추가 인증)
- ❖ 고가, 제한적 적용, 관리가 복잡하고 운영비용 증가
- ❖ 사용자 정보 동기화 필요
- ❖ 인증폭주 시 인증속도 저하
- ❖ 통신망 및 인증서버 장애 시 서비스 중단 발생(장애 취약)
- ❖ 인증 절차 시 인증 데이터 위변조, 우회/원격접속, 중간자공격, 우회기술, 피로공격 등 사이버 보안에 취약
- ❖ 간단(느슨)한 구성에서 시작해 더 복잡(견고)한 보안 시스템으로 진화 불가능

2nd 인증(Soft 인증)

- ❖ 모듈인증 방식(SHA-II), PAM 방식, 다계층 인증
- ❖ 탈중앙화 방식, 단일 지점 공격 방어에 강함
- ❖ 스마트폰 위주(인증키 생성기)
- ❖ 개인별 HMac Key 발급 및 관리하지 않음
- ❖ 동적 HMac Key 방식
- ❖ 개별 인증키 생성주기(3~60초) 적용
- ❖ 영구적 사용 / 비용 절감
- ❖ 2차 인증(추가 인증), 생체인식 적용
- ❖ 저가,다양하고 광범위한 적용, 관리가 단순하고 운영비용 절감
- ❖ 사용자 정보 동기화 필요하지 않음
- ❖ 인증폭주 시 부하분산으로 인증속도 보장
- ❖ 통신망 및 인증서버 미사용, 장애가 발생하지 않음(서비스 보장)
- ❖ 인증 절차 시 인증 정보 위변조 불가능, 우회/원격접속, 중간자공격, 우회기술, 피로공격 등 사이버 보안에 강함
- ❖ 간단(느슨)한 구성에서 시작해 더 복잡(견고)한 보안 시스템으로 진화 가능

별첨. 본인 인증

8. 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 다계층 인증 체계로 구분합니다.

SMS, 이메일 등 문자 기반의 2차 인증	모듈인증 방식의 2차 인증
❖ 인증서버 방식(SHA-I), Gateway(+Proxy) 방식, 통합인증	❖ 모듈인증 방식(SHA-II), PAM 방식, 다계층 인증
❖ 중앙 집중 방식, 단일 지점 공격 방어에 취약	❖ 탈중앙화 방식, 단일 지점 공격 방어에 강함
❖ 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
❖ 우회/원격접속, 중간자공격, 우회기술, 피로공격 등 사이버 보안에 취약	❖ 우회/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

nurit

별첨. 본인 인증

9. 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

- ❖ Gateway 방식, 복잡한 아키텍처 구조, 통합인증
- ❖ Public-Key Cryptography(공개키 암호기술) 사용
- ❖ 스마트폰에서 생체인증 후 PKI를 생성하여 전송하는 구조
- ❖ 비밀번호, 지문, 홍채, 안면 등과 같이 고정된 정적인 보안 (보안에 취약)
- ❖ 중앙 집중 방식, 단일 지점 공격 방어에 취약
- ❖ 다양한 환경의 정보자산 등에 손쉽게 적용하기 힘듬
- ❖ 도입 시 별도의 서버와 DB가 필요함(최소 서버 3대 필요)
- ❖ 고가, 관리가 복잡하고 운영비용 증가
- ❖ 사용자 정보 동기화 필요
- ❖ 인증폭주 시 인증속도 저하(인증속도 느림)
- ❖ 통신망 및 인증서버 장애 시 서비스 중단 발생(장애 취약)
- ❖ 보안구역에서 사용 불가, 임베디드 시스템 적용 불가
- ❖ 사용자 Device가 변경되면, 모든 서비스 재등록
- ❖ Device가 고장 나거나 분실되면 서비스 불가

모듈인증 방식의 2차 인증

- ❖ 모듈인증 방식, 단순한 아키텍처 구조, 다계층 인증
- ❖ 스마트폰에서 생체인증 후 OTP를 생성하는 구조(Time Sync)
- ❖ 매번 변하거나 한번 사용하고 버리는 일회성/휘발성 같은 동적인 보안(보안에 강함)
- ❖ 탈중앙화 방식, 단일 지점 공격 방어에 강함
- ❖ 다양한 환경의 정보자산 등에 손쉽게 적용 가능
- ❖ 도입 시 별도의 서버나 DB가 필요하지 않음
- ❖ 저가, 관리가 단순하고 운영비용 절감
- ❖ 사용자 정보 동기화 필요하지 않음
- ❖ 인증폭주 시 부하분산으로 인증속도 보장(인증속도 빠름)
- ❖ 통신망 및 인증서버 미사용, 장애가 발생하지 않음(서비스 보장)
- ❖ 보안구역에서도 사용 가능, 임베디드 시스템에 적용 가능
- ❖ 사용자 Device가 변경되면, 모든 서비스 등록하지 않음
- ❖ Device가 고장 나거나 분실되어도 대체 방안 제공 (WebOTP, 응급 일회용 인증키)

nurit

별첨. 본인 인증

10. 2차 인증 적용 순서

기본 보안부터 철저히 해야, 주요 인프라 공격의 85%가 패치, 2차 인증(추가 인증), 최소 권한 원칙 등 기본적인 수준의 보안을 지키지 않아서 발생한 것으로 기본 보안 정책만 지켜도 대부분의 공격은 막을 수 있습니다.

1. 운영체제(OS)

최우선적으로 Windows, Windows server, Linux, Unix, MacOS 등의 다양한 운영체제(OS)와 VPN이다.

해커들은 2차 인증이 적용되어 있지 않은 OS의 원격접속에 주로 사용되는 RDP나 SSH 등을 이용하여 서버에 침투하여 서버를 장악한 후 불능 상태로 만든다.

또한, VPN은 사용자와 전체 네트워크로 접근 권한을 부여하기 때문에 내부 시스템에 보안 경계를 설정하기 어려워 해커들의 집중 공략 대상이다.

2. 관리자 계정이나 관리 콘솔

다양한 애플리케이션, WAS, 가상화, 클라우드 등의 관리자 계정이나 관리 콘솔에 대한 2차 인증 설정이다.

계정 정보를 유출하여 도용 및 악용하거나, 관리콘솔에 악성코드 삽입 또는 계정정보 또는 VM을 삭제한 후 시스템을 무력화시켜 서비스를 불능 상태로 만든다. 이는 기업에 커다란 피해를 준다.

3. 일반 사용자 계정

회사 내에서 업무를 위해 사용하는 애플리케이션(ERP, 포탈, 그룹웨어, 웹메일), 가상화, 클라우드 등의 일반 사용자 계정에 대한 2차 인증 설정이다.

특히, 외부에서 접속할 수 있는 시스템에 2차 인증을 설정해 보안을 강화할 수 있도록 해야 한다.

11. 보안 솔루션 적용 방식

보안 솔루션의 적용 방식은 크게 Gateway(+Proxy), Sniffing, Agent, LKM(Loadable Kernel Module), PAM(Pluggable Authentication Module) 방식 등 5가지 방식으로 구분할 수 있습니다.

Gateway(+Proxy) 방식	Sniffing 방식	Agent 방식	LKM 방식	PAM 방식
접속하기 위한 통로를 별도로 설치한 후 사용자가 해당 통로를 통해서만 서버나 네트워크, DB에 접속, 로그인하거나 로그인 한 후에 프로세스를 수행하기 위해서는 반드시 Gateway를 거치도록 구성하여 모든 로그인과 철저하게 통제하는 방식이다. 해커들이 너무도 좋아하는 우회접속 및 원격 접속이 가능한 솔루션으로 보안 전문가들은 이런 분류의 솔루션은 보안 솔루션으로 취급하지도 않는다.	사용자와 서버 간에 주고받는 패킷을 복사하여 서버에 전달하는 방식이다. 남들이 이것 설치했다고 좋은 게 아니고 반드시 임베디드 테스트나 사전 도입 검토를 충분히 거쳐야 한다. 보안솔루션은 한번 설치되면 빼내기 무척 어렵고 제 기능 발휘하지 못해도 그대로 방치하는 경우가 발생할 수도 있다.	서버에 접근제어를 설치하는 방식이다. 솔루션에 따라서 Agent만으로 접근이 가능하도록 설계되거나 어떤 솔루션은 별도로 외부에 서버를 설치한 후에 내부 패킷을 외부 서버로 전송하여 접근을 제어하기도 한다.	커널 재컴파일 없이 작동중인 운영 체제 커널에 실행 기능을 모듈로 추가하기 위한 기법이다. 현재 리눅스, 솔라리스, FreeBSD를 포함한 많은 운영체제에서 사용되고 있다. 트로이목마에 감염된 모듈이 LKM에 있으면 시스템을 리부팅한다해도 부팅 과정에서 다른 커널 모듈들과 마찬가지로 감염된 LKM 모듈을 다시 적재하게 된다. 전형적인 서버 접근제어에 사용한 방식으로 Secure OS가 이 방식을 채택하여 사용하고 있다.	Linux/Unix 시스템에서 중앙집중적인 인증 매커니즘을 지원하는 방식이다.PAM의 기본 원리는 응용 프로그램이 password 파일을 읽어 오는 대신 PAM이 직접 인증을 수행 하도록 하는 것이다. PAM은 시스템 관리자가 원하는 인증 매커니즘이 무엇이든 상관하지 않는다. Library로 프로그램이 어떤 사용자에 대한 인증을 수행하려면 PAM Library가 있는 함수를 호출한다. PAM은 해당 함수의 Library를 제공하여 응용 프로그램이 특정 사용자를 인증하도록 요청할 수 있다.

별첨. 본인 인증

12. 로그인의 현주소

기업 및 개인의 정보 유출에 대한 해킹 피해보도는 잊혀질 만 하면 계속 발생되고 있으며, 이에 대한 피해는 심각한 수준입니다. 보다 근본적으로 해킹에 안전한 **추가 인증(2차 인증)**를 사용하여 대응하여야 한다는 인식이 사회적으로 확산되고 있습니다.

- 추측 가능한 비밀번호 사용 (기념일, 전화번호 등)
- 기억하기 쉬운 ID/ PW 한 두 개 일원화
- 유출 시 사용자가 유출여부 파악하기 어려움
- 내 컴퓨터는 항상 Virus / 해킹에 노출
- 너무 많은 비밀번호 때문에 사용하기 불편 (비밀번호 / 리셋 증후군)

- 온라인 뱅킹 사고
- 정보자산 해킹
- 정보 노출 / 유출
- 명의 도용
- 불법 이용 / 침입 / 통과
- 불법 접속 / 사용 / 승인
- 무단 접속

❖ 비밀번호 만으로는 결코 안전하지 않으며,
매번 사용할 때마다 **비밀번호를 대체** 또는 **추가 인증(2차 인증)**이 필요.

nurit

별첨. 본인 인증

13. 규정 및 언론 보도

과기정통부, 제로트러스트 가이드라인1.0 발표(2023.7.10)

핵심원칙: 제로트러스트 보안은 '절대 믿지 말고, 계속 검증하라'는 기본철학을 구현하기 위한 ① 강화된 인증(아이디/패스워드 외에도 다양한 인증정보를 활용한 다중인증 등 지속적인 인증을 포함), ② 마이크로 세그멘테이션(서버 · 컴퓨팅 서비스 등을 중심으로 하는 작은 단위로 분리), ③ 소프트웨어 정의 경계(소프트웨어 기반으로 보호 대상을 분리 · 보호할 수 있는 경계를 만들 수 있어야 함)를 말한다.

정보보호시스템 및 네트워크 장비에 대한 '**국가용 보안요구사항 우선 적용**' 원칙에 따라 '**적용하지 않는다**'고 명시한 경우를 제외하고 제품 단위로는 국가용 보안요구사항에 정의된 동일 기능을 우선 식별하여 적용해야 합니다.

1.1.2 제품은 사용자 식별 및 인증을 위해 1.1.1과 병행하여 추가적인 식별 및 인증 기능을 자체 또는 외부 IT실체와 연동하여 제공해야 한다.

① 추가적인 식별 및 인증 기능 제공을 위해 **△FIDO 표준을 준수한 2FA 지원 기기 △인증서 △일회용 비밀번호 생성기(OTP) 등**을 활용할 수 있다.

인증실패 대응은 1.2.1 제품에서 **사용자 인증이 설정된 횟수만큼 연속적으로 실패하면, 식별 및 인증 기능이 비활성화** 되어야 한다.

2013년 12월에 공지된 금융감독원의 전자금융감독규정을 보면, 제14조 9항 신설

"9. 정보처리시스템의 운영체제(Operating System) 계정으로 로그인(Log in)할 경우 계정 및 비밀번호 이외에 별도의 **추가인증** 절차를 의무적으로 시행할 것."

2020년 11월에 공지된 재택근무 관련 금융감독원의 전자금융감독규정 시행세칙을 보면, 제2조의2 제1, 2항 개정안(<별표 7> 망분리 대체 정보보호 통제)

원격접속에 대한 인증은 **이중 인증 적용(예: ID/PW + OTP), 일정 횟수(예: 5회) 이상 인증 실패 시 접속 차단**
인증수단을 특정하지는 않고 있으나, **지식기반.소유기반.특정기반** 인증 수단 중 **서로 다른 방식에 속하는 인증수단 2개를 조합**

미국립표준기술연구소(NIST)가 최근 발표한 비밀번호 가이드라인에 따르면 **주기적으로 비밀번호를 변경하는 것이 온라인 해킹 침해를 결코 막지 못한다**고 한다. **주기적인 비밀번호 변경은 약한 비밀번호를 생성시킬 가능성이 높을 뿐만 아니라 사용자는 수십 개의 비밀번호를 기억하지 못해서 결국 어디엔 가는 써 놓게 된다는 것**이다. NIST는 비밀번호 가이드라인 개정을 통해 **비밀번호를 특수문자를 포함한 여러 문자로 조합하고 일정 기간마다 바꾸도록 하라는 강제요건을 삭제**했다.

Microsoft가 기업의 보안 관리자에게 권장하는 내용(보안기준)은 **주기적인 비밀번호 변경이 보안에 실질적으로 도움이 되지 않는다**는 주장이 힘을 얻은 상황에서 PC 운영체계인 Windows 10과 Windows 서버의 보안 기준에서 **비밀번호를 주기적으로 변경해야 한다는 조항을 삭제**했다.

구글이 지난 해(2021년) 자사 서비스에 자동 활성화 시킨 **2단계 인증을 통해 계정 해킹을 50% 줄였다**고 구글 블로그를 통해 밝혔다.

2024.2 금융당국, '전자금융감독규정' 개정안 규정 변경 예고
사용자 비밀번호 설정 방식을 구체적으로 특정하던 규정을 삭제하고 **금융회사 스스로 안전하다고 판단되는 비밀번호와 인증수단 관리 방식을 도입할 수 있도록 허용**했다.

제로 트러스트(Zero Trust)는 아주 믿을만한 직원의 계정이라도 시스템마다 접근 권한을 달리 부여하고, **실제 접근이 이뤄질 때마다 상대를 검증하는 보안 모델로 날로 지능화된 사이버 공격에 대응하기 위한 최적의 보안 대책**으로 꼽히고 있다.

"절대 믿지 말고, 계속 검증하라(Never Trust, Always Verify)"

별첨. 본인 인증

13. 규정 및 언론 보도

미국 국립표준기술연구소(NIST)는 지난달(2024.9) 공개한 '디지털 신원 지침(가이드라인)' 개정안

NIST는 이번 개정안의 비밀번호 요건에서

△여러 문자유형을 혼합하도록 요구하는 등 사용자에게 추가적인 비밀번호 규칙을 부과하는 행위
△정기적으로 비밀번호 변경을 요구하는 행위를 금지의무(SHALL NOT) 항목으로 격상했다.

두 행위는 2017년 지침에서 금지권고(SHOULD NOT) 항목이었다.

NIST는 "유출된 비밀번호 데이터베이스를 분석한 결과 숫자 · 문자 · 기호를 혼합해 구성한 비밀번호를 선택하는 규칙의 이점이 당초 생각보다 크지 않고, 사용성과 기억력에 미치는 영향이 심각한 것으로 나타났다"며 "이 때문에 비밀번호 길이를 바탕으로 좀 더 간단한 접근방식을 제시했다"고 밝혔다.

NIST는 2017년에 이어 이번 개정안에서도

△비밀번호를 8자 이상으로 설정하도록 요구하라
△모든 유니코드 문자를 '비밀번호 1자'로 취급하라
△비밀번호가 탈취된 흔적이 있다면 사용자에게 변경을 요구하라

는 조항을 의무(SHALL) 항목으로 유지했다.

이 밖에

△**비밀번호 최소 길이를 15자 이상으로 요구하고 64자 이상의 비밀번호도 설정할 수 있도록 허용하라**
△알파벳 · 숫자 외 모든 유니코드 글자를 비밀번호로 입력할 수 있도록 허용하라

는 조항은 2017년에 이어 이번 개정안에서도 권고(SHOULD) 항목으로 이름을 올렸다.

NIST는 '의무' · '금지의무'를 반드시 따라야 하고 위반을 허용하지 않는 행위, '권고'를 적합하다고 권장하는 행위, '금지권고'를 권장하지 않지만 금지도 하지 않는 행위로 규정했다. 지침의 적용대상은 웹사이트 등 인터넷 신원인증서비스제공자(CSP)와 검증기관(Verifier) 등이다.

NIST가 10여년 뒤 이 같은 조건들을 금지 항목으로 전환하면서 세계 각국은 비밀번호 설정기준을 완화하고 비밀번호를 보완할 '**2FA(2단계 인증)**' 등 추가 인증수단과 암호화 기술을 법제화하고 있다. 국내에서 '패스워드 선택 및 이용 안내서'를 발간하는 한국인터넷진흥원(KISA)은 2019년 '안전한 비밀번호'의 기준을 '두 종류 이상 문자로 구성된 8자리 이상의 문자열' 혹은 '10자리 이상 문자열'로 완화하고 비밀번호 변경주기를 삭제한 상태다.

한 당국자는 국내 상당수 웹사이트에서 유지 중인 문자 · 숫자 · 특수문자 혼합과 비밀번호 변경주기 규칙에 대해 "명시적 의무규정이 없다"고 말했다.

제로 트러스트(Zero Trust)는 아주 믿을만한 직원의 계정이라도 시스템마다 접근 권한을 달리 부여하고, **실제 접근이 이뤄질 때마다 상대를 검증하는 보안 모델로 날로 지능화된 사이버 공격에 대응하기 위한 최적의 보안 대책**으로 꼽히고 있다.

"절대 믿지 말고, 계속 검증하라(Never Trust, Always Verify)"

별첨. 본인 인증

14. 2차 인증 도입의 필요성

"정보자산의 로그인-ID/비밀번호가 유출이 되어도 대안이 있느냐?"

1. 보안 강화를 위하여 사용자 식별・인증을 위한 OTP 등을 활용한 2단계 인증 체계 적용

2차 인증 적용(예: ID/PW + OTP), 일정 횟수(예: 5회) 이상 인증 실패 시 접속 차단 및 인증수단을 특정하지는 않고 있으나, 지식기반.소유기반.특정기반 인증 수단 중 서로 다른 방식에 속하는 인증수단 2개를 조합해서 사용해야 함.

2. 중앙 집중식에서 벗어나 탈중앙화 방식의 다계층 인증 체계 적용

중앙 집중화 방식은 해커들의 "**단일 지점 공격**"의 표적이 되어 집중 공격을 받아 서비스가 중단되는데 비해서 탈중앙화된 다계층 인증 체계는 "**단일 지점 공격**"을 없애고, 사용자 식별.인증을 정보자산의 각 레이어별 분산하여 시스템의 보안을 강화시켜, 해커들의 공격으로 부터 서비스가 중단되거나 시스템에 접속하는 상황을 최소시켜 신뢰를 증가시킴.

3. 악의적인 목적으로 만들어진 프로그램인 악성코드에 의한 불법적인 우회/원격접속을 차단

악의적인 목적으로 만들어진 프로그램인 악성코드 프로그램에 의하여 정보자산의 접속정보(Desktop to Application, Desktop to Desktop, Desktop to Server, Desktop to Database, Server to Server 등)를 불법 취득한 뒤 불법적으로 정보자산에 우회/원격으로 접속하는 것을 차단 해야 함.

4. 분실.도용.해킹으로 인한 사용자 비밀번호 초기화에 적용

사용자 본인 스스로 로그인-ID, 특정항목, **일회용 인증키**를 입력하여 맞으면 새로운 비밀번호를 등록하여 사용하게 함.

"정보자산의 보안 강화를 위하여 **비밀번호 대체** 또는 **2차 인증(추가 인증)**은 선택이 아닌 반드시 적용해야 할 솔루션!"

별첨. 본인 인증

15. 도입 시 검토사항

1. 제로 트러스트(Zero Trust) 개념이 적용되어 있는지?

2. 별도의 인증서버 방식인지 또한 클라이언트에 Agent가 존재하는지, 모듈인증 방식인지?

3. 통합인증인지 분산인증인지?

4. 다양한 운영체제/애플리케이션 환경에 손쉽게 적용할 수 있는지?

5. 인증키 생성 및 검증 시 사용되는 키는 정적인지, 동적인지?

6. 제한된 시간 내에 횟수 제한을 할 수 있는지?

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

8. 중앙 집중식에서 벗어나 탈중앙화 방식의 다계층 인증 체계(Multi-Layer authentication system)를 지원하는지?

9. 보안 관점에서 위험을 얼마나 분산 시킬 수 있는지?

10. 인증 폭주 시 인증 속도는 얼마나 저하되는지?

11. 통신망을 사용하는지?

12. 보안시스템의 우회 및 원격접속을 차단할 수 있는지?

13. 보안지역이나 통신장애에 영향을 받는지?

14. 인증절차 시 데이터를 위변조하여 우회 인증절차에 대한 문제는 없는지?

[국가 사이버안전센터 인증 솔루션 보안 취약점]
15. 로그인 계정이나 개인정보의 도난, 스파이 행위, 통신 방해, 데이터 변경 등에 사용되는 중간자 공격(Man-in-the-middle attack)을 방어할 수 있는지?

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

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

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

16. 오픈소스 Google OTP 적용의 위험성

1. 상용화된 인증 솔루션이 아님
Open source로 이미 여러 해킹 사례가 발생하여 피해를 입은 사용자들이 많으며, Google에서는 어떠한 책임도 지지 않음.

2. OTP 등록 키 값(Secret 값) 노출
Secret 값의 유출 가능성으로, TOTP 생성의 매개변수가 되는 Secret 값이 유출되면 제3자가 OTP를 알아내 2단계 인증이 무력화될 수 있음. 보통 TOTP를 인증기에 등록할 때 QR코드를 스캔하거나 Secret 문자열을 입력하는데, 이것이 안전한 방법으로 전달되는 것이 아니라 보통은 웹 페이지에 그대로 출력하는 방식이기 때문에 유출의 위험이 있다고 볼 수 있음. 더군다나 이 값을 토대로 OTP를 생성하기 때문에 Secret 값을 암호화하여 제공하는 것은 불가능.

해당 Secret 문자열 내지는 QR코드를 가지고 있는 한 인증기에 무한정 등록할 수 있다는 것. 물론 RFC 6238 표준에서는 하나의 Secret은 하나의 기기에만 등록해야 한다고 하고 있지만, 그것을 강제할 방법이 없다는 것이 문제.

또한, 앱을 삭제할 경우 키 값을 어딘가에 보관하지 않으면 등록된 OTP 등록 키 값을 새로이 받아서 키 값을 변경해야 함.

3. 해킹에 대단히 취약
Open source 기반의 무상 서비스이기에 소스 공개로 알고리즘 유출, 앱 위변조 방지 등의 기본적인 보안장치들이 전혀 없음.

4. 구성원의 Google 계정 해킹 시 대비책 없음
계정이 해킹 당하면 Google OTP가 적용된 업무서비스를 일정기간 사용하지 못함.

5. 낮은 Hash 함수 사용
SHA-1을 사용하고 있음(국정원에서 최소 SHA-256 이상, 미국NSA에서는 VPN에 SHA-384 이상을 사용할 것을 권고)
미국 NIST는 SHA-1을 2030년 12월 31일까지 완전히 단계적으로 중단하므로 SHA-2 또는 SHA-3로 마이그레이션 할 것을 권장

6. Secure key(Seed key) 문제
Secure key가 암호화 및 난독화 되지 않고, Hex로만 변환되어 있음.
SHA 함수별 Seed key가 다름에 따라 업그레이드 시 혼선(SHA-1, 224, 256: 20Byte, SHA-384: 32Byte, SHA-512: 64Byte)

7. 기술지원 문제(Technical support)
Open source이기 때문에 문제 발생 시 본인이 해결해야 함.
미국과 중국의 무역 전쟁으로 인하여 중국은 Android 업데이트에 액세스 할 수 없으며, Google Play store를 사용할 수 없음.

8. Google OTP가 SaaS 형태의 유료 버전으로 전환되어 무료 버전은 더 이상 버그 패치나 업그레이드를 지원하지 않음.

무료 Google OTP는 소규모 Linux나 애플리케이션에 적합할지는 모르나 대규모 Linux나 애플리케이션에는 부적합.

별첨. 본인 인증

17. 맺는 말

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
▶보안 관점에서 위험을 얼마나 분산 시킬 것인지?
▶인증 절차 시 데이터 위변조를 어떻게 방어할 것인지?
▶계정 정보 도용 및 악용은 어떻게 차단할 것인지?
▶권한상승은 어떻게 차단할 것인지?
▶브라우저 자동 로그인은 어떻게 방어할 것인지?
▶단일 지점 공격을 어떻게 방어할 것인지?
▶우회/원격접속을 어떻게 차단할 것인지?
▶중간자 공격을 어떻게 방어할 것인지?
▶다중 인증(MFA)의 우회기술/피로공격을 어떻게 방어할 것인지?

무엇보다도 인증키는 본인이 소유하고 있는 인증키 생성매체를 사용해서 본인이 직접 인증키를 생성하여 본인이 접근하고자 하는 정보자산에 직접 입력 및 검증해야 그나마 정보보안 사고를 예방할 수 있는 최선책.

결론은 "2차 인증을 도입했다"는 것이 아니라 기술 및 보안성 등 "어떤 2차 인증을 도입했느냐"가 관건.
"절대 믿지 말고, 계속 검증하라(Never Trust, Always Verify)"

nurit

기억할 필요가 없는 비밀번호!
BaroPAM이 함께 합니다.

감사합니다!

www.nurit.co.kr

서울시 강서구 마곡중앙2로 15, 913호(마곡동, 마곡테크노타워2)
주식회사 누리아이티 대표전화 : 02-2665-0119