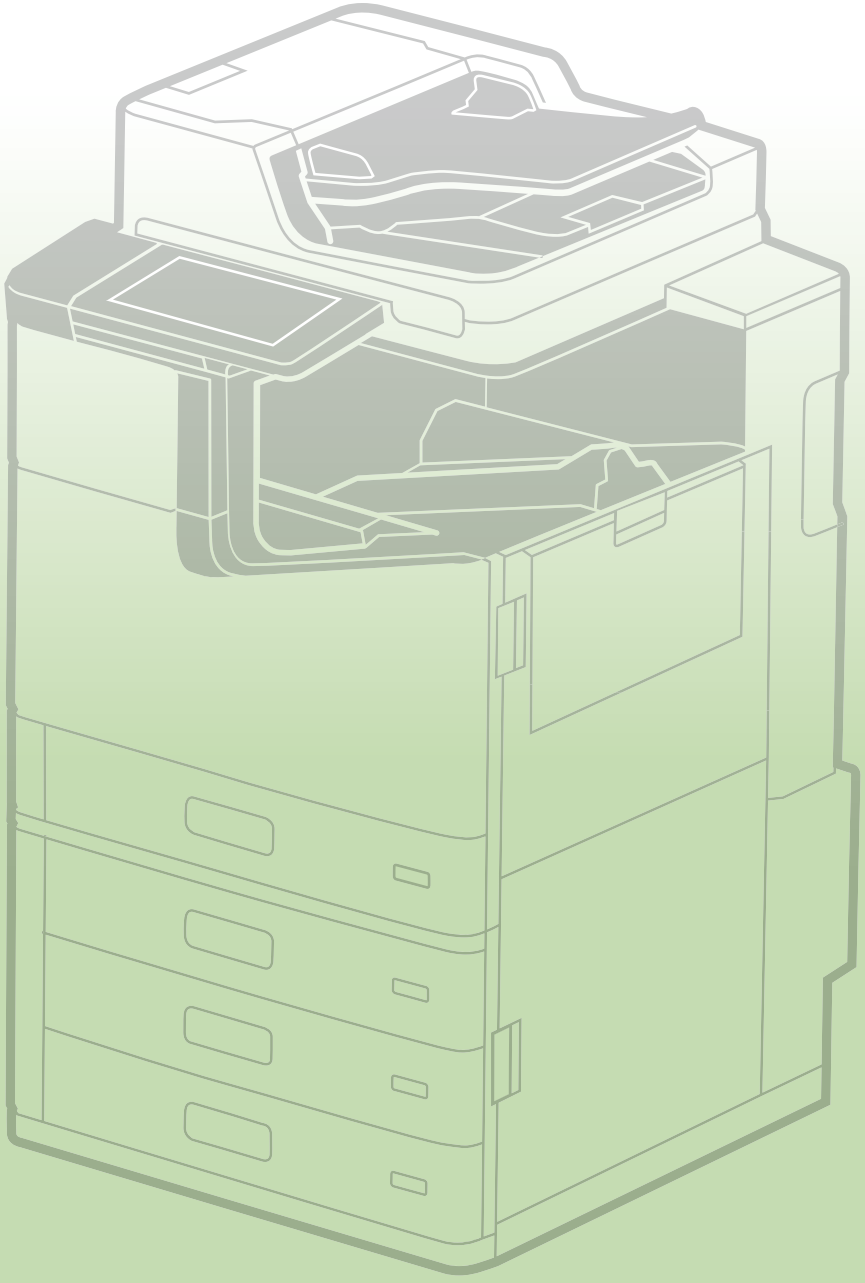
EPSON

보안 가이드북



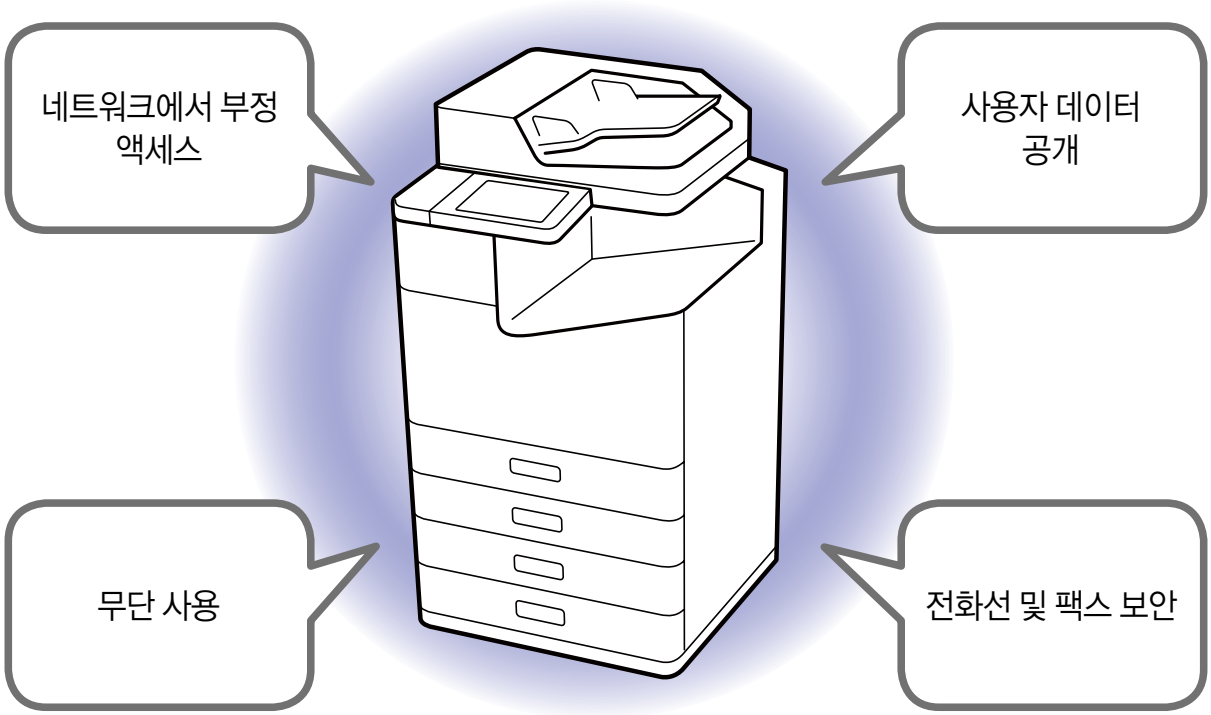
목차

1. 소개

Epson 에서는 고객의 편의성을 개선하기 위해 제품의 네트워크 호환 기능을 강화해 왔습니다 .

한편 , 악의적인 제 3 자의 사이버 공격이 점점 더 정교해지고 복잡해지면서 네트워크에 연결된 기기에 대한 위협이 커져 보안 대책에 대한 우려가 커지고 있습니다 .

Epson 의 제품에는 다양한 기능이 탑재되어 있기 때문에 , 특히 컴퓨터와 서버와 같이 네트워크에 연결된 경우 보안에 대한 적절한 고려가 필요합니다 .



본 가이드북은 보안에 대한 Epson 의 액세스 방식과 고객을 위한 조언을 소개하고 , 사용 가능한 보안 기능을 안내합니다 .

텍스트에서 각 기능 옆에 있는 아이콘은 다음과 같은 의미를 갖습니다 .

: **이 표시가 있는 보안 기능은 관리자가 수행해야 하는 최소 설정입니다 .**

: **이 표시가 있는 보안 기능은 관리자만 구성할 수 있으며 구성된 보안 환경에서 사용자가 사용할 수 있습니다 .**

: **이 표시가 있는 보안 기능은 관리자와 사용자가 설정하고 사용할 수 있습니다 .**

: **기타 보안 기능입니다 . 사양의 일부로 제품에 내장된 보안 기능에 적용됩니다 .**

보안 설정 방법은 제품 설명서를 확인하십시오 .

본 가이드북에 설명된 보안 기능 및 보안 표준 준수 여부는 사용되는 제품에 따라 다릅니다 . 일부 제품에는 이러한 기능이 없거나 해당 보안 표준을 준수하지 않을 수 있습니다 . 따라서 각 제품의 호환성은 별도의 보안 가이드북에 있는 기능 목록을 참조하십시오 .

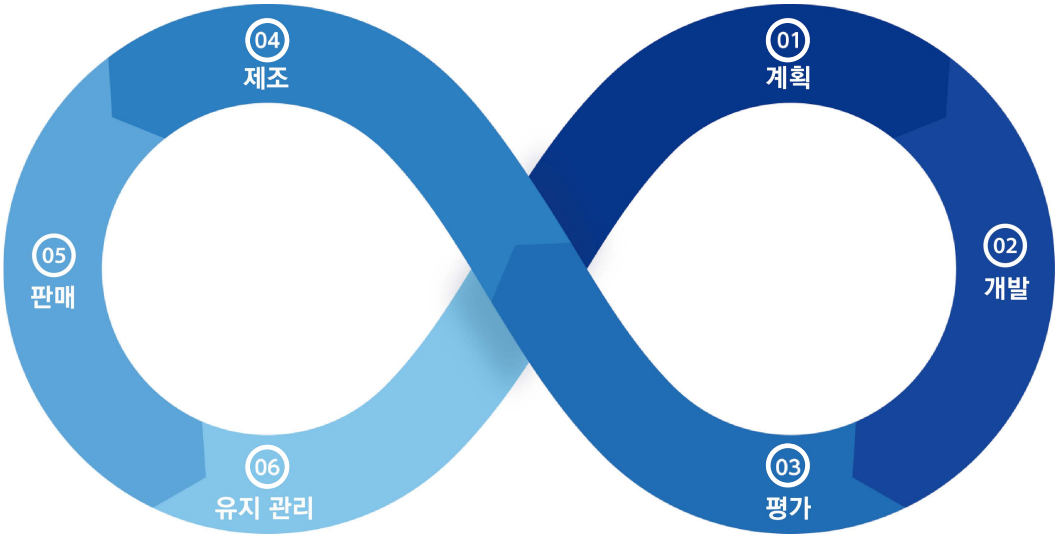
2. EPSON 의 보안 기본 정책

Epson 은 고객이 안전하고 쉽게 제품을 사용할 수 있도록 보안과 관련하여 다음과 같은 액세스 방식을 취하고 있습니다 .

2-1. 기본 정책

Epson 은 제품 보안을 제품 품질의 초석으로 보고 있습니다 .

제품 장르별로 다양한 사용 환경을 면밀히 검토하여 고객이 보다 안전한 조건에서 제품을 사용할 수 있도록 계획 , 개발 , 평가 , 제조 , 판매 , 유지보수에 이르는 전 라이프사이클에 걸쳐 제품 (엔드포인트) 보안을 실천하고 있습니다 .



① 계획

제품 계획 단계에서는 최신 보안 동향과 잠재적인 취약점을 지속적으로 모니터링합니다 . 또한 고객의 요청에 귀를 기울이고 보안 관련 요구 사항을 식별하고 분석합니다 . 이런 식으로 위험이 실현되기 전에 제품의 잠재적인 문제를 제거합니다 .

② 개발

사무실 / 가정용 프린터에서 상업 / 산업용 소형 및 대형 프린터에 이르기까지 광범위한 제품을 개발하는 동안 개발된 원래의 공통 플랫폼과 기술을 사용하여 보안 위험에 대한 보호를 강화하기 위해 노력합니다 .

③ 평가

철저한 사내 테스트 외에도 객관적인 보안 평가를 위해 제 3 자 기관을 참여시킵니다 . 엄격한 보안 검증 시스템을 통해 제품의 높은 보안을 보장하기 위해 다양한 각도에서 평가를 수행합니다 .

④ **제조**

제조 작업의 최고 품질을 보장하기 위해 당사는 공장에 철저한 정보 자산 관리 시스템을 구현했으며 , 여기에는 당사 제품의 기능을 가능하게 하는 소프트웨어를 설치합니다 .

⑤ **판매**

우리는 사용 환경 및 운영 조건에 따라 보안 위험을 최소화하기 위한 솔루션을 제안하고 구현하여 고객을 지원하기 위해 최선을 다하고 있습니다 . 또한 제품 설치 후 발생할 수 있는 모든 취약점을 신속하게 해결합니다 .

제품을 교체하고 폐기해야 하는 경우 기밀 정보 유출을 방지하기 위해 장치를 공장 기본 설정으로 재설정합니다 .

⑥ **유지 관리**

우리는 제품을 구매한 고객이 보고한 보안 관련 문제 및 우려 사항에 신속하게 대응합니다 .

2-2. 정보 제공

우리는 고객에게 적극적으로 정보를 제공하고 보안에 대해 적극적으로 알립니다 .

2-3. 취약점 대응 지원

저희는 지속적으로 취약점을 해결하고 있습니다 .

- 저희는 업계 표준 도구를 사용하여 취약점을 테스트하고 취약점이 없는 제품을 제공하기 위해 노력합니다 .
- 당사는 우리 제품의 펌웨어에 사용되는 오픈 소스 소프트웨어의 취약점에 대한 정보를 정기적으로 모니터링합니다 .
- 새로운 취약점이 발견되면 즉시 이를 분석하여 정보와 대응책을 제공합니다 .

2-4. 규정 및 표준 준수

우리는 보안 표준을 준수하고 이를 획득하기 위해 노력합니다 .

3. 제품 설치 시 해야 할 일

최적의 보안을 위해 설치 시 다음 사항을 읽고 사용 환경에 따라 필요한 설정을 구성하십시오 .

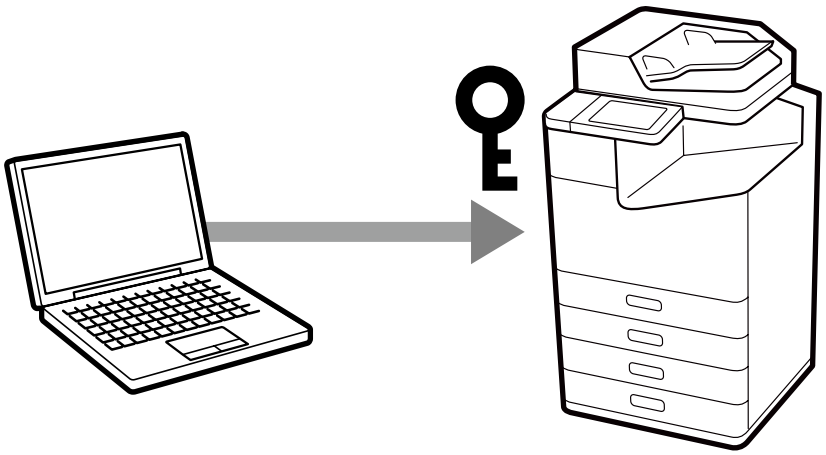
3-1. 관리자 비밀번호

각 제품을 설치하는 동안 관리자 비밀번호 설정을 강력히 권장합니다 .

관리자 비밀번호가 설정되어 있지 않거나 제품이 공장 출하 상태로 남아 있는 경우 , 제품에 저장된 일반 설정 및 네트워크 설정에 불법적으로 액세스되거나 변경할 수 있습니다 . 주소록 , ID, 비밀번호 등 개인정보 및 기밀정보를 보호하지 못할 위험도 있습니다 .

관리자 비밀번호는 다른 사용자가 추측하기 어려운 복잡한 문자열이어야 합니다 . 영문자뿐만 아니라 기호 , 숫자를 포함하여 8 자 이상으로 구성되어야 합니다 . 관리자 비밀번호는 제품 제어판 설정에서 직접 설정하거나 네트워크를 통해 설정할 수 있습니다 .

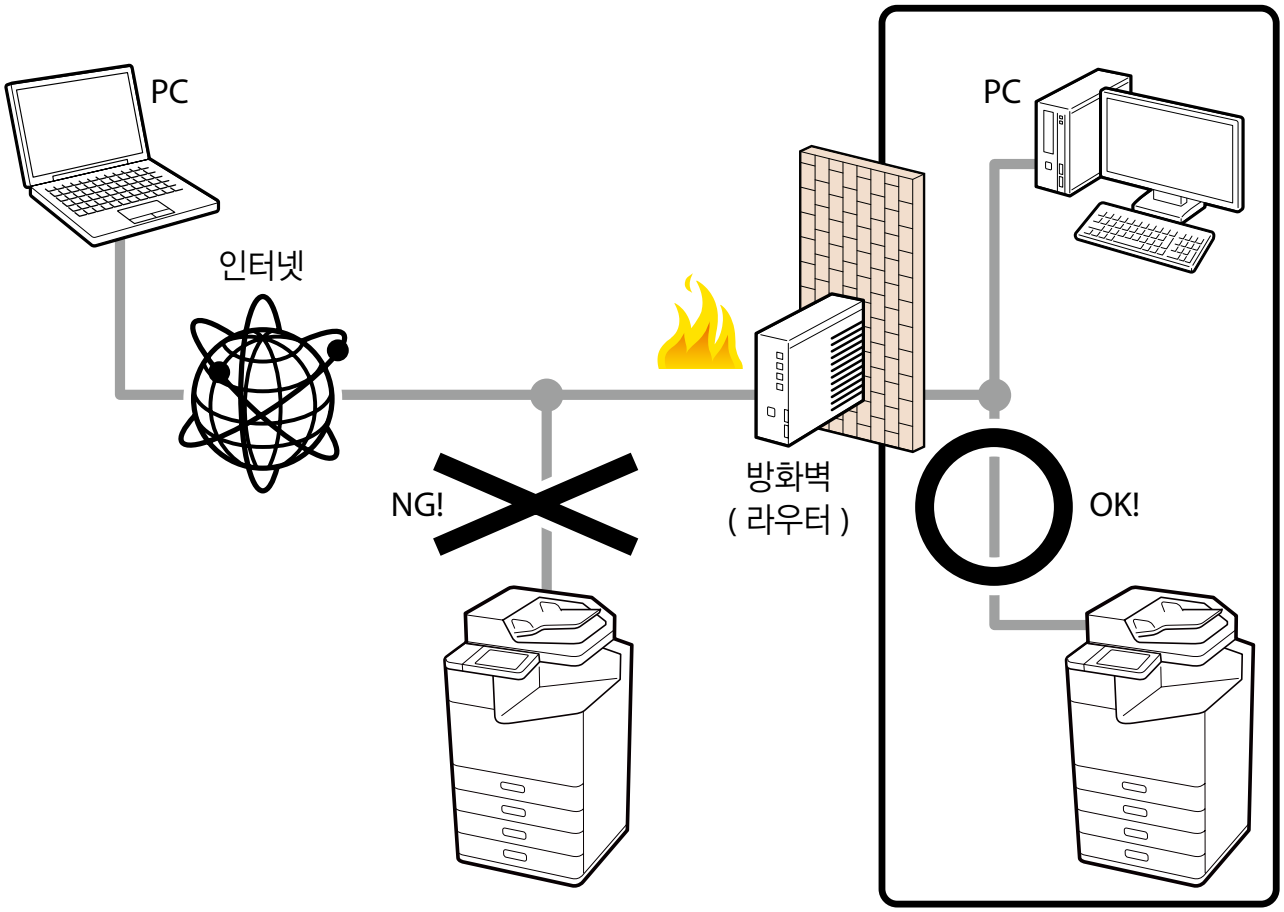
따라서 , 일부 제품은 보안을 강화하기 위해 공장에서 개별 비밀번호가 설정되어 있습니다 .



3-2. 인터넷 연결

인터넷에 직접 연결하지 않고도 방화벽으로 보호되는 네트워크에 제품을 설치할 수 있습니다 . 이 경우 개인 IP 주소를 설정하고 활용하는 것이 좋습니다 .

IPv6 환경에서 제품을 사용하는 경우에도 방화벽이나 기타 수단을 사용하여 인터넷에서 제품에 직접 액세스하지 못하도록 제품에 대한 액세스를 제한하십시오 .



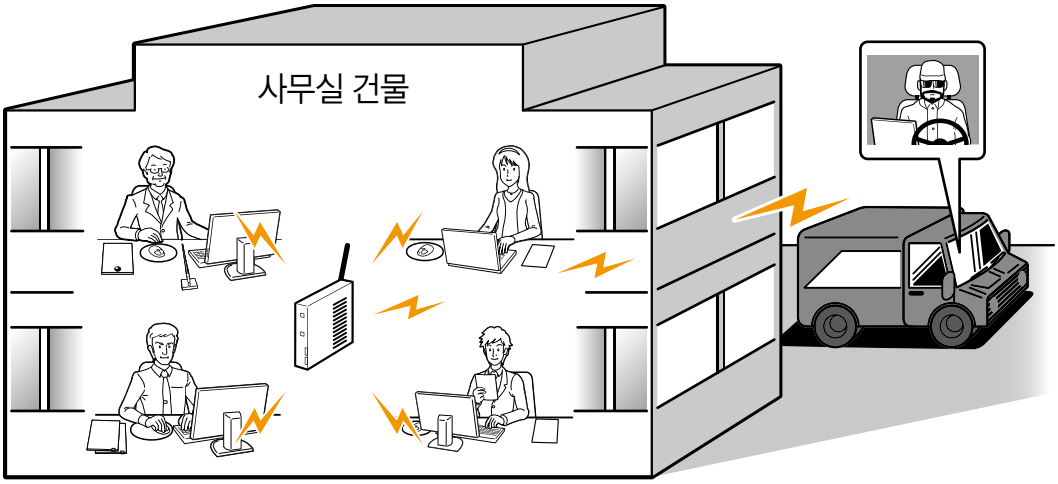
제품의 네트워크 기능과 인쇄를 위한 웹 관리 화면 등의 관리 인터페이스가 포함되어 있습니다 . Epson 은 취약성 테스트를 수행하고 취약성이 없는 제품을 제공하기 위해 노력하고 있으나 , 인터넷에 직접 연결할 경우 고객의 네트워크와 네트워크에 연결된 장치에 무단 작동 및 정보 유출과 같은 예상치 못한 보안 위험이 발생할 수 있습니다 .

3-3. 무선 LAN 네트워크

무선 LAN 네트워크를 사용하는 경우 무선 LAN 의 보안을 적절하게 설정하십시오 .

무선 LAN 의 장점은 신호 범위 내에 있으면 네트워크를 통해 제품에 자유롭게 연결해 컴퓨터 , 스마트폰 단말기와 통신할 수 있다는 점입니다 . 반면 , 보안이 제대로 설정되지 않은 경우에는 악의적인 제 3 자에 의해 다음과 같은 문제가 발생할 수 있습니다 .

- 귀하의 인쇄 데이터 , 스캔 데이터 , ID, 비밀번호 등의 개인정보가 타인에게 공개될 수 있습니다 .
- 통신 내용이 부정하게 재작성 (위조) 될 수 있습니다 .
- 특정인이나 장치를 사칭 (신원 도용) 하여 통신에 사용할 수 있습니다 .



무선 LAN 설정 절차는 제품 설명서를 참조하십시오 .

3-4. 미사용 프로토콜 및 기능 비활성화

사용하지 않는 프로토콜 및 기능을 비활성화합니다 .

각 프로토콜 및 기능은 개별적으로 허용하거나 , 금지할 수 있으므로 의도치 않게 사용되어 보안 위험이 발생하지 않습니다 .

3-5. 최신 펌웨어 및 소프트웨어로 업데이트

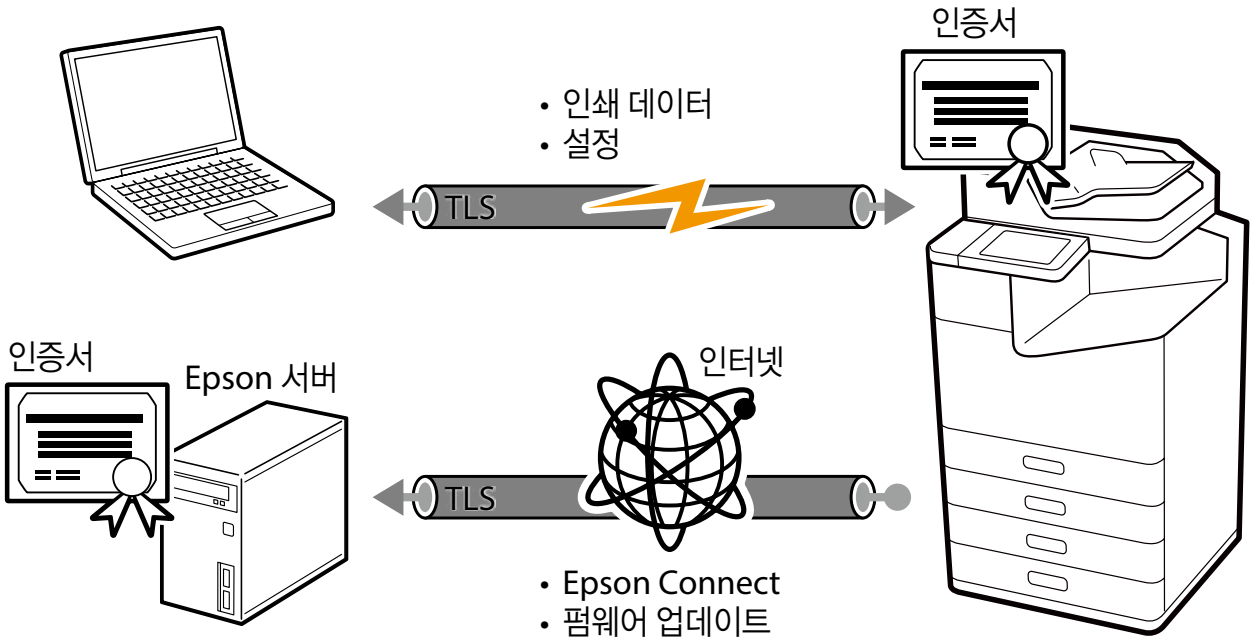
필요에 따라 최신 펌웨어 및 소프트웨어를 제공합니다 . 제품을 사용하려면 반드시 최신 펌웨어로 업데이트하십시오 .

최신 펌웨어 및 소프트웨어에는 추가 기능 뿐만 아니라 결함 및 취약성에 대한 수정 사항도 포함되어 있습니다 . 펌웨어 또는 소프트웨어에 대한 자세한 내용은 펌웨어 또는 소프트웨어의 수정 내역을 참조하십시오 .

4. 네트워크 보안

4-1. TLS 통신

전송은 TLS 로 보호되므로 브라우저를 통해 제품을 인쇄하고 구성하는 IPPS 프로토콜을 사용하여 설정 정보 및 인쇄 데이터의 내용이 노출되는 것을 방지할 수 있습니다 . 또한 , 서버 유효성 검사 기능을 사용하고 CA 서명된 인증서를 가져와 사내 PKI(Public Key Infrastructure) 와 함께 작업하여 승인되지 않은 장치로 정보가 전송되는 것을 방지할 수 있습니다 . 훨씬 안전한 암호화 알고리즘을 사용하도록 암호화 강도를 구성할 수 있습니다 . Epson Connect 및 펌웨어 업데이트용 제품을 통해 인터넷에서 Epson 서버에 액세스하는 경우에도 TLS 로 보호됩니다 .



사용할 TLS 의 버전과 암호화 강도를 선택할 수 있습니다 .

지원되는 TLS 버전과 암호화 강도는 다음과 같습니다 .

TLS 버전

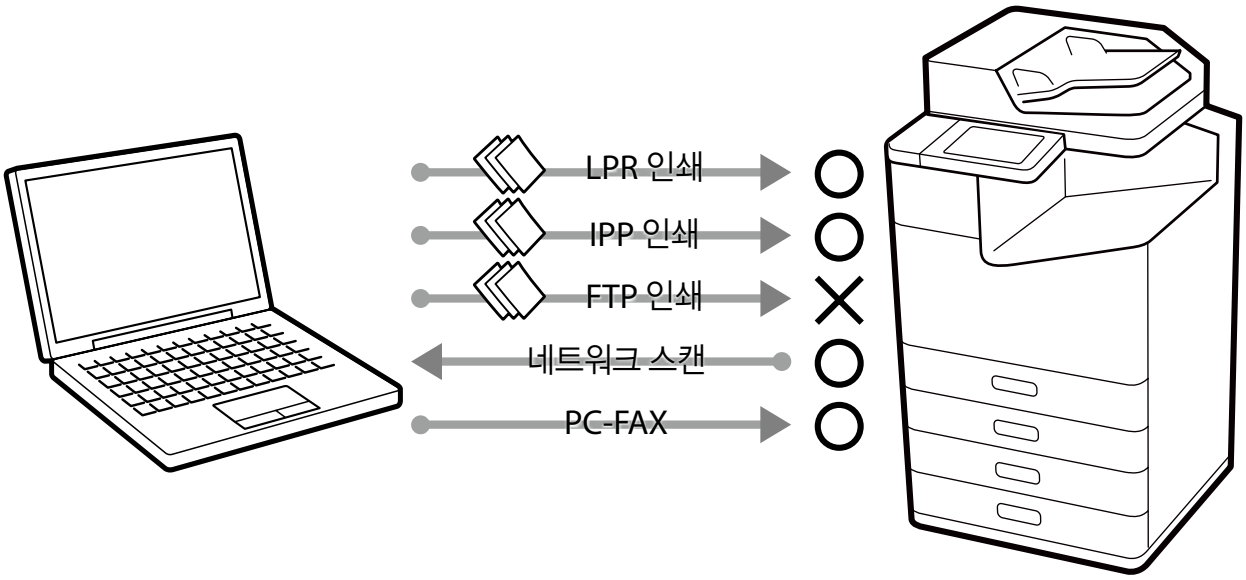
- TLS1.1
- TLS1.2
- TLS1.3

암호화 강도

- 80bit
- 112bit
- 128bit
- 192bit
- 256bit

4-2. 프로토콜 권한 및 제외 제어

제품은 인쇄 , 스캔 , PC-FAX 전송 시 다양한 프로토콜을 통해 통신합니다 . 각 프로토콜에 대해 개별 권한 및 금지 사항을 설정하여 보안 위험이 발생하기 전에 의도하지 않은 사용을 방지할 수 있습니다 .



프로토콜과 기능이 활성화될 때의 보안 위험과 비활성화될 때의 제한 사항은 부록을 참조하십시오 .

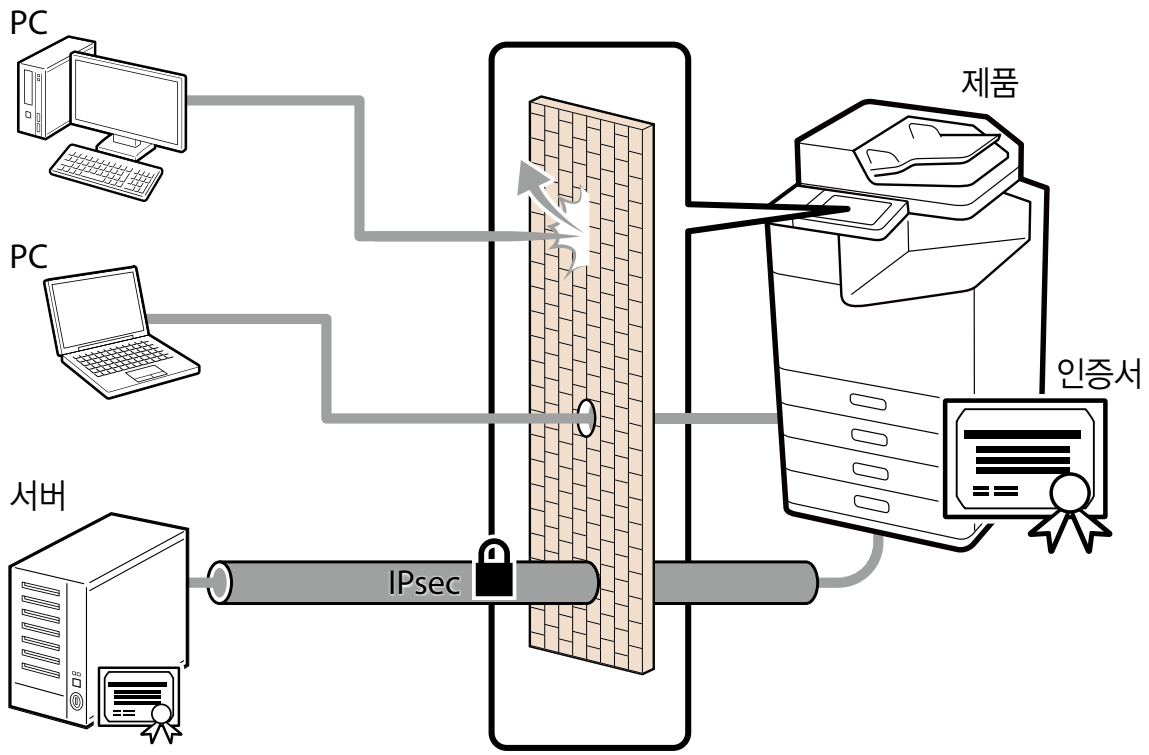
허용 또는 금지될 수 있는 프로토콜과 기능은 다음과 같습니다 .

- Bonjour
- SLP
- WSD
- LLTD
- LLMNR
- LPR
- RAW (Port9100/ 사용자 포트)
- IPP/IPPS
- FTP
- SNMP
- SSL/TLS
- Microsoft 네트워크 공유
- 네트워크 스캔 (EPSON Scan)
- PC-FAX

4-3. IPsec/IP 필터링

IPsec/IP 필터링 기능을 사용하여 IP 주소 , 서비스 유형 , 수신 및 전송 포트 번호 등을 필터링할 수 있습니다 . 이러한 필터의 조합에 따라 특정 클라이언트의 데이터를 허용할지 차단할지 , 특정 유형의 데이터를 허용할지 차단할지 설정할 수 있습니다 . 마찬가지로 IPsec 을 이용해 보호 기능을 결합해 더욱 강력한 보안으로 통신할 수 있습니다 .

IPsec 을 사용한 보호에는 IP 패킷 단위의 보호 (암호화 및 인증) 가 포함되어 있으므로 안전하지 않은 인쇄 프로토콜 및 스캔 프로토콜도 보호 대상이 됩니다 . 인증 방법에서는 미리 공유한 키와 인증서가 지원됩니다 .



지원되는 알고리즘 및 키 교환 방법은 다음과 같습니다 .

키 교환 방법

- IKEv1
- IKEv2

ESP 암호화 알고리즘

- AES-CBC-128
- AES-CBC-192
- AES-CBC-256
- AES-GCM-128
- AES-GCM-192
- AES-GCM-256
- 3DES

ESP/AH 인증 알고리즘

- SHA-1
- SHA-256
- SHA-384
- SHA-512
- MD5

기본 정책은 제품에 액세스하는 모든 사용자에게 영향을 미칩니다 . 특정 요구 사항에 따라 액세스를 제어하려면 개별 정책을 설정하십시오 .

4-4. IEEE802.1X 인증

IEEE802.1X 는 네트워크 장치의 각 포트에 대한 액세스를 제어하기 위한 표준입니다 . IEEE802.1X 네트워크는 RADIUS 서버 (인증 서버) 와 인증 기능이 있는 스위칭 허브로 구성됩니다 .

Epson 제품은 IEEE802.1x 에 호환되며 일부 기밀 정보가 포함된 네트워크 환경에 연결할 수 있습니다 .

다음 인증 방법 및 암호화 알고리즘이 지원됩니다 .

인증 방법

- EAP-TLS
- PEAP-TLS
- PEAP/MSCHAPv2
- EAP-TTLS

암호화 알고리즘

- AES128
- AES256
- 3DES
- RC4

4-5. SNMP

SNMP 는 지원되는 장비 및 관리 도구의 상태를 모니터링하고 설정을 변경하기 위한 프로토콜입니다 .

SNMPv1 및 SNMPv2c 는 통신 암호화를 지원하지 않으며 방화벽 또는 이와 유사한 것으로 보호되는 네트워크 내에서 사용해야 합니다 . 또한 SNMP 통신을 사용하려면 커뮤니티 이름을 기본값에서 변경합니다 .

SNMPv3 는 SNMP 통신 (패킷) 을 인증하고 암호화하여 상태를 모니터링하고 호환되는 장치 관리 도구로 변경 사항을 구성할 수 있습니다 . 이를 통해 네트워크를 통해 설정을 변경하거나 상태를 모니터링할 때 기밀성을 보장할 수 있습니다 .

SNMPv3 는 다음 인증 및 암호화 알고리즘을 지원합니다 .

SNMPv3 인증 알고리즘

- MD5
- SHA-1

SNMPv3 암호화 알고리즘

- DES
- AES128

4-6. SMB

SMB 는 네트워크를 통해 파일을 공유하기 위한 프로토콜입니다 .

SMB1.0 및 SMB2.0 은 통신 암호화를 지원하지 않으며 방화벽 또는 이와 유사한 것으로 보호되는 네트워크 내에서 사용해야 합니다 .

SMB3.0 은 호환 장치와의 SMB 통신 (패킷) 을 인증하고 암호화하는 데 사용할 수 있습니다 . 이를 통해 네트워크를 통한 파일 공유의 기밀성을 보장할 수 있습니다 .

4-7. WPA3

이 제품은 Wi-Fi(무선랜) 용 최신 인증 및 암호화 기술인 WPA3 를 지원합니다 . WPA3 는 무선 네트워크를 통해 데이터를 보호하기 위해 보다 강력하고 강력한 보호 기능을 제공합니다 .

4-8. 인터페이스 간 분리

제품에는 USB 인터페이스 , 표준 유선 LAN 인터페이스 , 추가 유선 LAN 인터페이스 , 무선 LAN 인터페이스 및 팩스 인터페이스가 포함되어 있습니다 . 각 인터페이스는 독립적이므로 해당 인터페이스에서 처리할 수 있는 프로토콜에만 액세스할 수 있으며 직접 전송 또는 라우팅 기능을 제공하지 않습니다 . 구체적인 예로 , 공중 전화선 (팩스선) 에서의 액세스는 팩스 통신 절차에 따른 처리로 제한됩니다 . 해당 절차를 벗어나면 오류로 통신이 끊어지므로 무단 액세스의 위험이 없습니다 . 또한 , 수신된 팩스 데이터는 가져오기 전에 이미지 데이터로 정확성을 확인합니다 . 제품을 통한 전송 기능을 통해 바이러스 감염 또는 무단 액세스로 이어질 수 있는 악성 멀웨어가 심어질 위험이 없습니다 . 권한이 있는 사용자만 전송 기능을 실행할 수 있습니다 . 예를 들어 , 제품을 통해 공중 전화 회선의 네트워크 침입 , 무선 LAN 에서 유선 LAN 으로의 액세스 , USB 를 통해 컴퓨터에 연결된 제품에 대한 인터넷의 무단 액세스 등의 행위를 말합니다 .

5. 제품 보호

5-1. 컴퓨터에서 USB 연결 차단

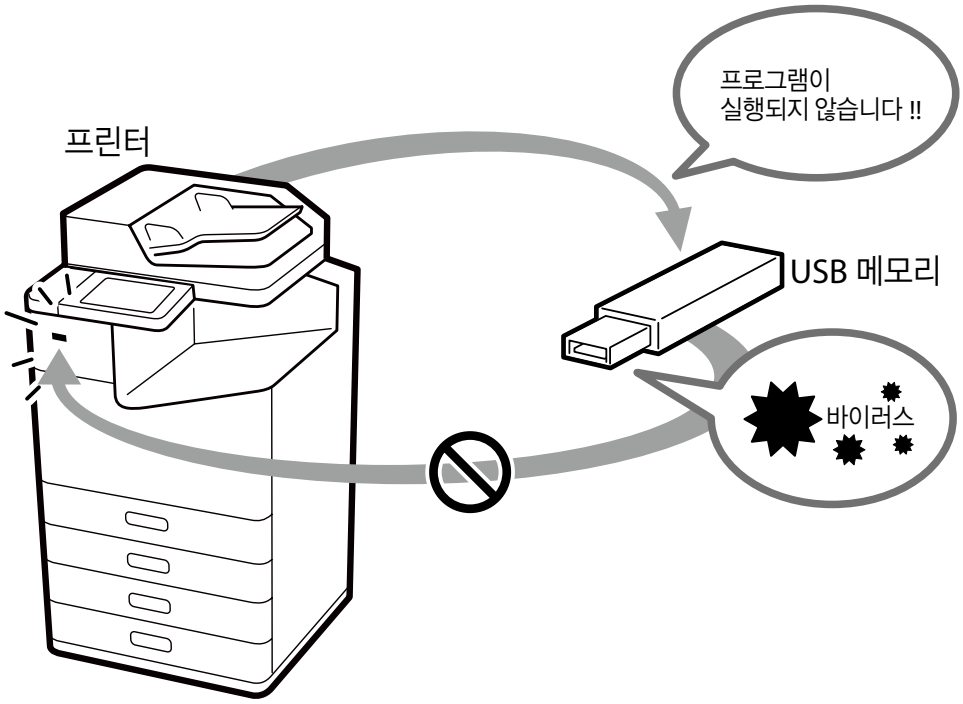
컴퓨터에서 USB 연결을 통해 제품에 대한 액세스를 비활성화할 수 있습니다 . 이 옵션을 설정하면 USB 케이블로 컴퓨터에 직접 연결하여 인쇄하거나 스캔하는 것을 금지합니다 .

5-2. 외부 인터페이스 비활성화

메모리 카드와 USB 메모리 인터페이스를 비활성화할 수 있습니다 . 이를 통해 사무실 내 기밀 문서를 무단으로 스캔하여 데이터의 불법 복제를 방지할 수 있습니다 .

5-3. USB 메모리로 인해 발생하는 바이러스 처리

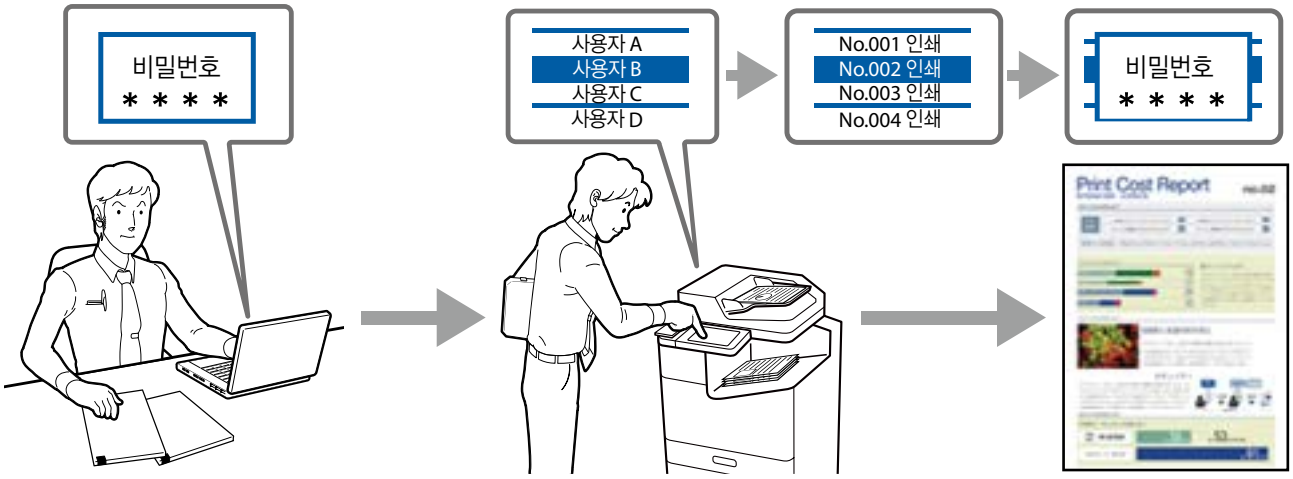
Epson 제품의 USB 메모리에는 실행 가능한 기능이 없기 때문에 USB 메모리를 통해 제품이 바이러스에 감염될 위험이 없습니다 .



6. 인쇄 / 스캔 보안

6-1. 기밀 작업

문서를 " 기밀 작업 " 으로 제출하여 문서의 개인 정보 보호 / 기밀성을 보장하고 승인되지 않은 사람이 장치에서 무인 출력을 볼 수 없도록 합니다 .



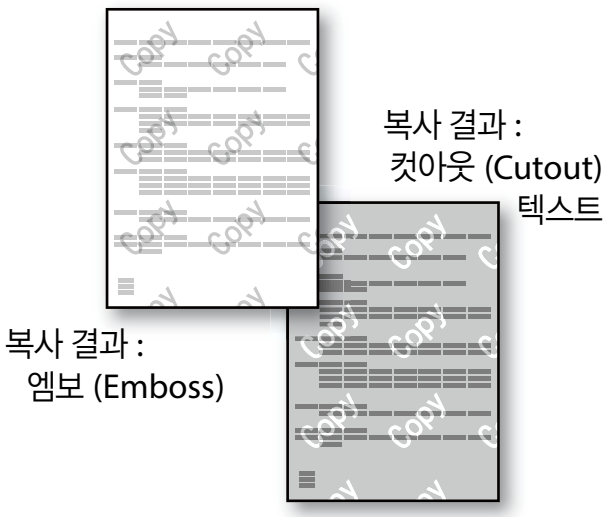
인쇄하려면 비밀번호를 입력하십시오 .

제품에서 인쇄 작업을 선택하고 비밀번호를 입력하십시오 .

인쇄가 완료되었습니다 .

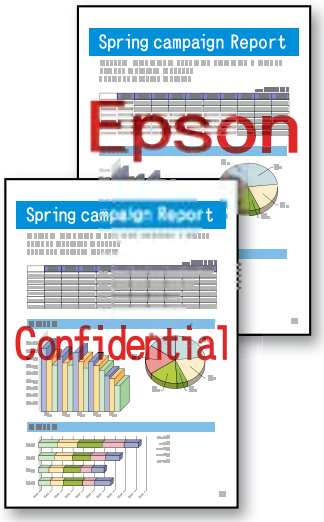
6-2. 복사 방지 패턴

원본 출력물에 투명한 워터마크 패턴을 생성하는 복사 방지 워터마크 인쇄로 문서의 독창성을 보호할 수 있습니다 . 원본 출력을 사용하여 복사본을 만들면 투명 워터마크가 표시됩니다 .



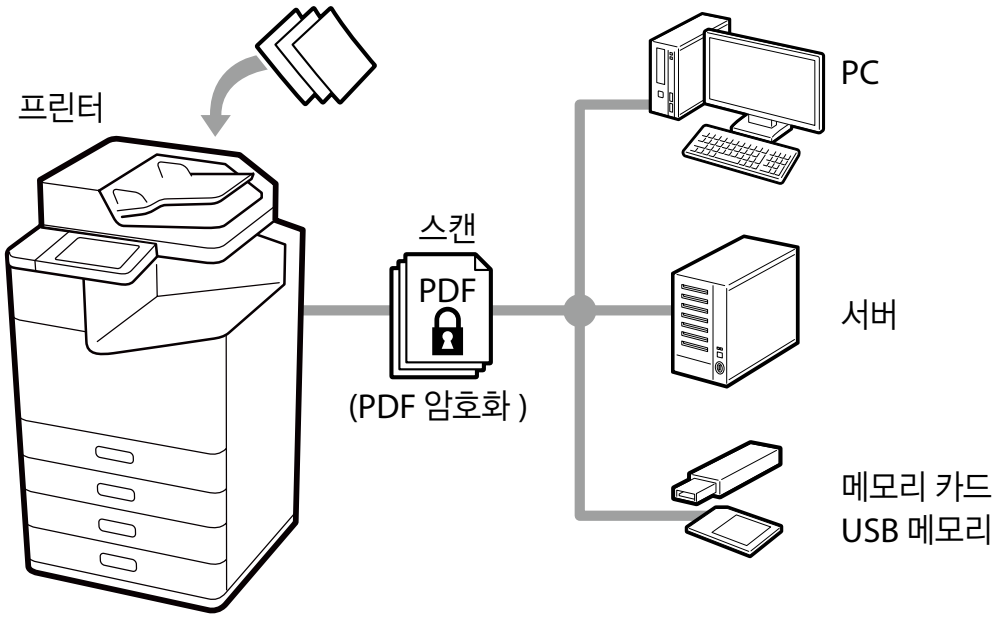
6-3. 워터마크

기밀 및 중요 (텍스트 또는 BMP 형식) 와 같은 워터마크를 문서에 중첩할 수 있습니다 . 또한 " 사용자 이름 " 또는 " 컴퓨터 이름 " 을 선택할 수도 있습니다 . 수신자에게 문서를 주의 깊게 처리하도록 상기시키면 무단 사용을 방지할 수 있습니다 .



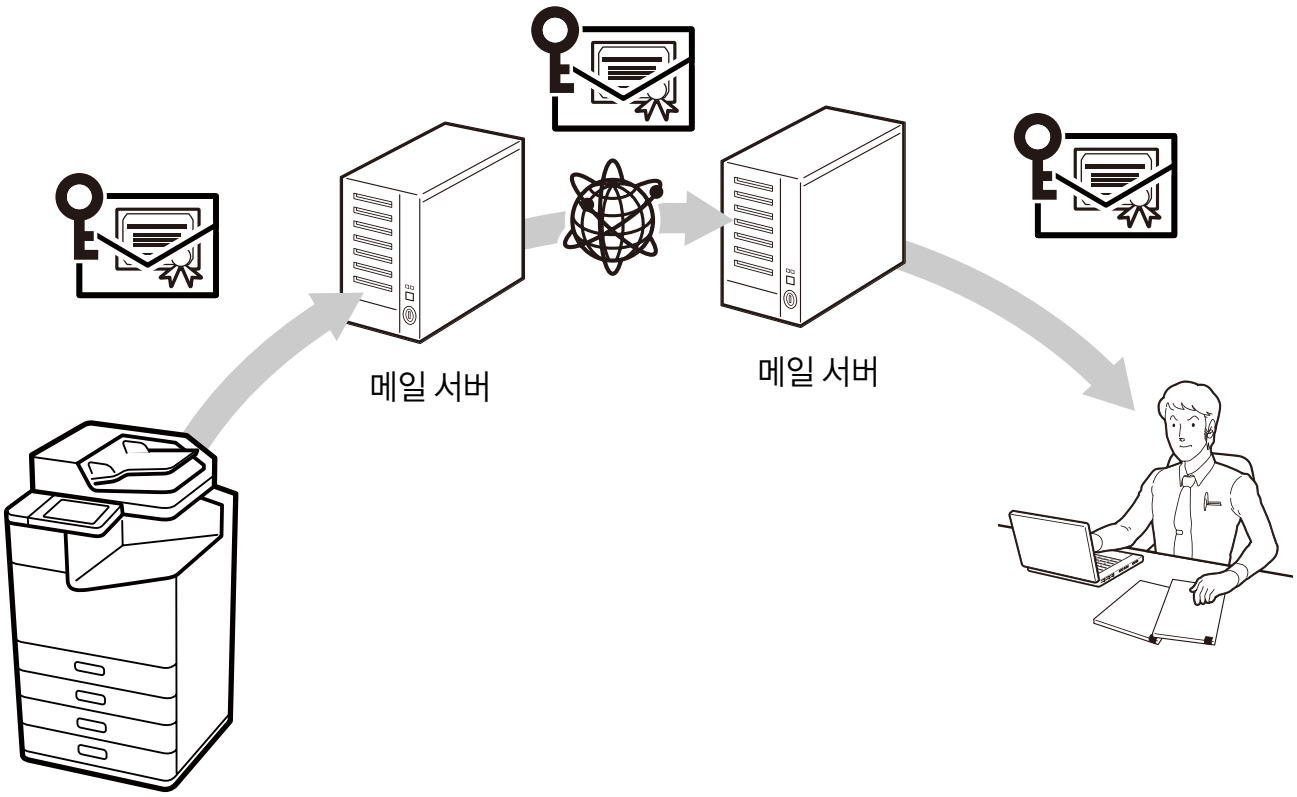
6-4. PDF 암호화

문서를 비밀번호로 보호된 PDF 파일로 스캔할 수 있습니다 . 이를 통해 제 3 자가 허가 없이 문서를 보는 것을 방지할 수 있습니다 .



6-5. S/MIME

S/MIME 을 사용하면 스캔 후 이메일로 전송 및 이메일로 팩스 송수신을 위해 디지털 서명을 추가하거나 이메일을 암호화할 수 있습니다 . 이메일이 여러 이메일 서버를 통과하더라도 이메일이 위조 , 감청 , 변조되지 않도록 보호할 수 있습니다 . S/MINE 은 메시지의 진정성과 무결성을 보호하는 동시에 데이터 보안을 보호하고 거부를 방지합니다 .



지원되는 알고리즘은 다음과 같습니다 .

암호화 알고리즘

- AES-128
- AES-192
- AES-256
- 3DES

디지털 서명 해시 알고리즘

- SHA-1
- SHA-256
- SHA-384
- SHA-512
- MD5

6-6. 도메인 제한

이메일 주소의 도메인 이름에 제한 규칙을 적용하면 메일로 스캔 및 팩스 전달 이메일 기능에 대한 잘못된 전송 및 정보 유출 위험을 줄일 수 있습니다 .

6-7. 길이가 긴 인증 비밀번호 지원

최근에는 비밀번호 보안을 강화하기 위해 긴 비밀번호를 설정하는 것을 권장합니다 . 스캔 후 네트워크 폴더 /FTP 로 전송 , 스캔 후 이메일로 전송 , 이메일 알림에 사용되는 인증 비밀번호를 최대 70 자까지 설정할 수 있습니다 . 파일 서버와 메일 서버에 긴 비밀번호에 대한 비밀번호 정책을 설정할 수 있습니다 .

6-8. PDL 에서 파일 액세스 제한

PDL(Page Description Language) 에서 파일 액세스를 비활성화하면 프린터 내부에서 파일을 훔치는 악성 인쇄 데이터로 인한 정보 유출 위험을 방지할 수 있습니다 . 악성 인쇄 데이터가 전송되더라도 파일을 읽지 않고 안전하게 제품을 사용할 수 있습니다 .

6-9. 보안 인쇄

인쇄 전송 경로의 보안을 보호하려면 TLS 를 통해 암호화된 IPPS 를 사용할 수 있습니다 .

7. 팩스 보안

7-1. 직접 전화 걸기 제한

숫자 키패드를 사용하여 직접 팩스 번호를 입력하려는 경우, 수신인을 두 번 정확하게 입력한 경우에만 팩스가 전송되도록 설정할 수 있습니다 . 숫자 키패드를 사용하여 전화번호를 직접 입력하는 것을 금지하고 , 원터치 다이얼링과 주소록에 등록된 주소로만 팩스가 전송되도록 설정할 수도 있습니다 . 이를 통해 전화번호 입력 오류로 인해 잘못된 전송으로 정보가 유출될 위험을 줄일 수 있습니다 .

7-2. 주소 목록 확인

팩스를 보내기 전에 선택한 주소를 확인할 수 있습니다 . 이를 통해 주소 지정 시 오류로 인한 잘못된 전송에서 정보가 노출될 위험을 줄일 수 있습니다 .

7-3. 신호음 감지

신호음 감지를 확인한 후 팩스를 보내면 잘못된 전송을 방지할 수 있습니다 .

국가 또는 지역에 따라 신호음 감지가 불가능할 수 있습니다 .

7-4. 확인이 완료된 팩스 서류에 대한 조치

수신된 팩스를 받은 편지함에 저장 (메모리 수신) 하고 제어판에서 확인한 후 인쇄하도록 " 보기 후 팩스 인쇄 " 를 설정할 수 있습니다 . 이렇게 하면 인쇄된 팩스가 방치되어 정보가 노출되고 수신된 팩스에서 인쇄된 자료가 손실되는 것을 방지할 수 있습니다 .

또한 , 받은 편지함에 액세스하려면 비밀번호가 필요하도록 설정하여 인증되지 않은 사용자가 임의로 인쇄하고 삭제하는 것을 방지할 수 있습니다 .

7-5. 전송 확인 보고서

결과 보고서 전송 , 결과 보고서 전송 , 관리 보고서 전송 등 전송 세부 사항을 확인하는 보고서를 인쇄하여 팩스가 올바른 주소로 확실히 전송되었는지 확인할 수 있습니다 .

7-6. 수신된 팩스의 백업 데이터 삭제

수신된 팩스의 백업 데이터 * 는 제어판에서 삭제할 수 있습니다 . 백업 데이터가 자동으로 삭제되도록 설정하여 수신된 팩스의 데이터를 무단으로 다시 인쇄하는 것도 방지할 수 있습니다 .

* 수신된 팩스의 백업 데이터는 제품 (공장 기본 설정) 에 저장되므로 인쇄 결과가 불분명하거나 인쇄 결과가 손실된 경우 팩스를 다시 인쇄할 수 있습니다 .

7-7. 여러 수신자에게 전송 제한

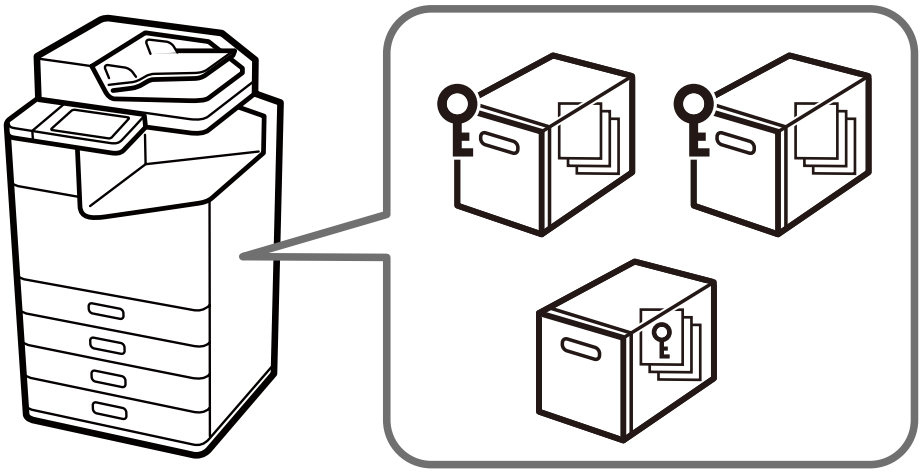
수신자를 1 명만 선택할 수 있도록 제품을 설정할 수 있습니다 .

여러 수신자를 지정할 수 없게 함으로써 의도하지 않은 수신자에게 팩스를 보내고 정보가 노출될 위험을 줄일 수 있습니다 .

8. 사용자 데이터 보호

8-1. 저장 보안

공유 폴더가 있는 모델에서는 공유 폴더와 문서에 대해 고유한 비밀번호를 설정할 수 있습니다 . 비밀번호는 정보 노출 , 손실 및 무단 변조를 방지할 수 있습니다 . 또한 저장 작업은 액세스 제어의 대상이 될 수 있습니다 . 공유 폴더를 사용하지 않는 경우 공유 폴더 기능 사용을 금지할 수도 있습니다 .



8-2. 사용자의 주소록 보호

제품에 저장된 주소록을 일괄 편집하려면 관리자 비밀번호가 필요하므로 주소록 정보의 유출 및 무단 변경을 방지할 수 있습니다 . (관리자 비밀번호가 설정된 경우) 또한 , 주소록을 암호화된 파일로 내보낼 수 있으므로 제품 교체나 백업 시 팩스 번호 , 이메일 주소 등 개인정보가 노출되는 것을 방지할 수 있습니다 .

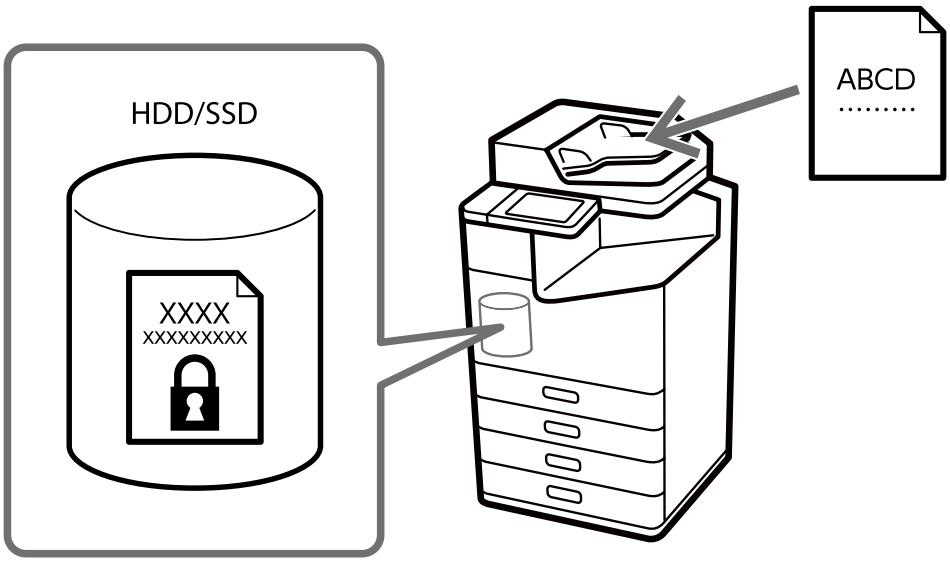
8-3. 제품별로 처리되는 데이터 처리

인쇄 , 복사 , 스캔 기능의 데이터는 제품에 일시적으로 저장되었다가 작업이 완료되거나 , 제품을 끄면 삭제됩니다 . 팩스를 보내거나 받을 때 팩스 데이터는 완전히 삭제됩니다 . 수신된 팩스는 데이터로 저장되고 백업 기능에 의해 유지되지만 , 설정을 변경하여 데이터가 자동으로 지워지도록 할 수 있습니다 . (7-6 참조)

8-4. HDD/SSD 에 저장된 데이터의 암호화

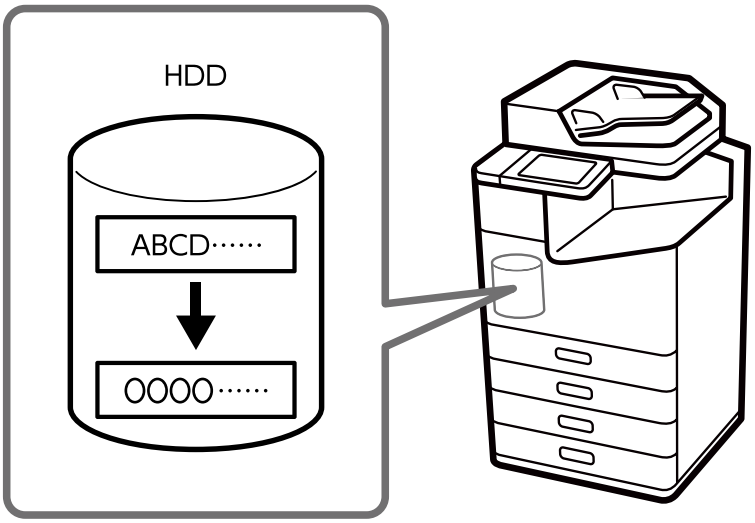
제품 내부 HDD/SSD 에 데이터를 저장할 때 고객 데이터를 항상 암호화하여 보호합니다 . 악의적인 제 3 자의 공격이 발생할 가능성이 낮지만 , 저장된 데이터의 내용은 보이지 않습니다 . HDD/SSD 에는 자체 암호화 드라이브가 제공되며 , 문서 데이터는 AES-256 으로 암호화됩니다 .

데이터를 암호화하면 HDD/SSD 를 도난당한 경우 개인 데이터에 대한 무단 액세스나 악의적인 공격을 방지할 수 있습니다 .



8-5. 작업 데이터의 순차적 삭제

이 기능을 활성화하면 장치의 HDD 에 일시적으로 저장된 작업 데이터가 특수 패턴으로 덮어쓴 후 자동으로 지워집니다 . 이렇게 하면 제 3 자가 악의적으로 잔여 작업 데이터에서 데이터를 복구하는 것을 방지할 수 있습니다 .



8-6. 비밀번호 암호화

제품에 저장된 비밀번호를 암호화할 수 있습니다 . 암호화되는 정보는 다음과 같습니다 .

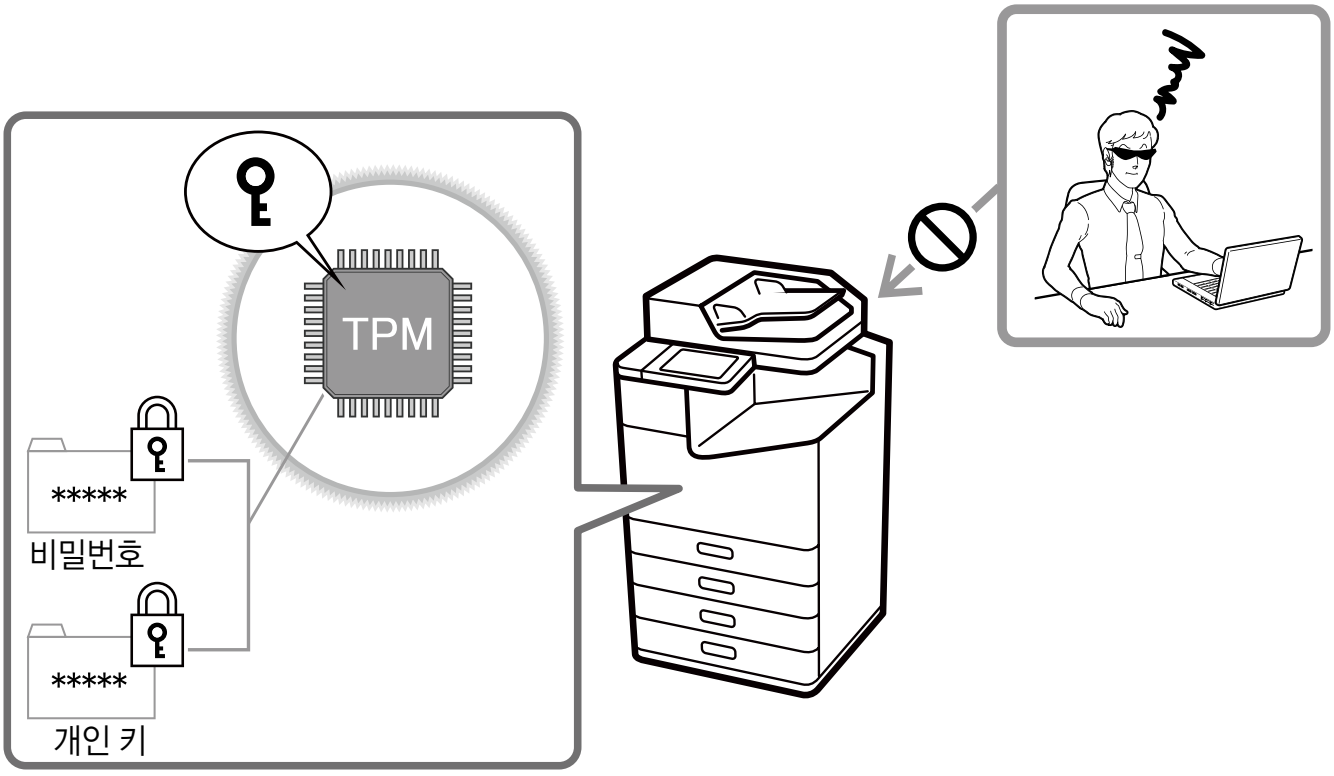
- 관리자 비밀번호
- 액세스 제어를 위한 사용자 비밀번호
- 하드 디스크 인증 키 , 인증서 개인 키 등 네트워크 폴더 /FTP 로 스캔에 액세스하기 위한 비밀번호

8-7. TPM

TPM(Trusted Platform Module) 이 장착된 모델의 경우 암호화된 비밀번호와 개인 키 정보를 복원하기 위한 암호화 키는 TPM 칩에 저장됩니다 . TPM 칩은 프린터 외부에서 액세스할 수 없으므로 하드웨어 수준에서 무단 분석으로부터 보호됩니다 .

TPM 의 순수 난수는 브라우저 (Web Config) 세션을 통한 구성에 사용되는 난수에 사용됩니다 . TPM 의 순수 난수는 암호화된 HDD/SSD 의 인증 키를 생성하는 데에도 사용됩니다 .

이러한 모델에는 TPM2.0 사양 칩이 장착되어 있습니다 .



8-8. HDD 미러링

추가 HDD 옵션을 설치하면 하나의 HDD 가 오작동하더라도 저장된 데이터를 잃지 않고 다른 HDD 로 모든 기능을 계속 사용할 수 있습니다 .

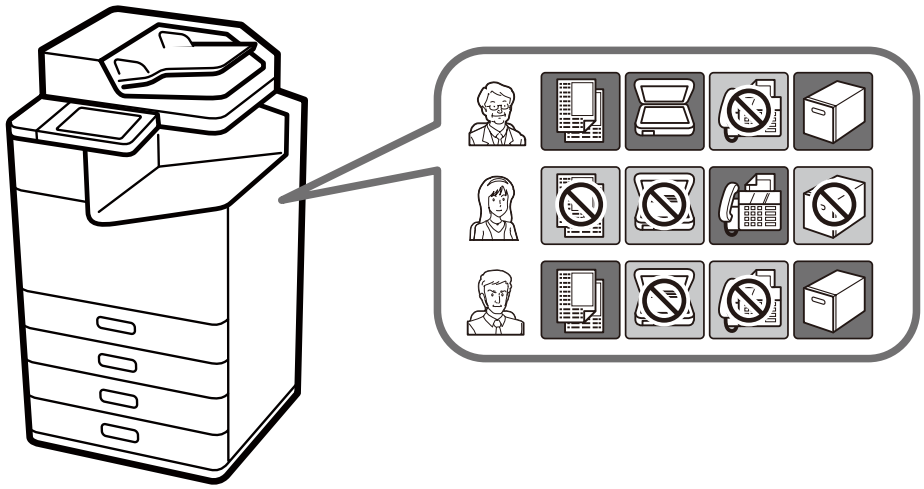
9. 작동 제한

9-1. 패널 잠금

패널 잠금을 사용할 때 제어판에 접근하려면 관리자 비밀번호를 입력해야 합니다 . 공개된 사무실 , 공공시설 등의 장소에서 관리자 비밀번호로 패널을 보호하는 경우 사용자가 설정을 변경하는 것을 방지할 수 있습니다 .

9-2. 액세스 제어

개별 사용자의 인쇄 , 스캔 , 복사 , 팩스 * 및 보관함 기능 사용을 제한하여 역할 및 직무에 따라 보안 위험을 최소화할 수 있습니다 . 또한 사용자가 지정된 기간 이후 제어판을 조작하지 않으면 자동으로 로그아웃됩니다 .



* 팩스 전송 제한만 가능합니다 .

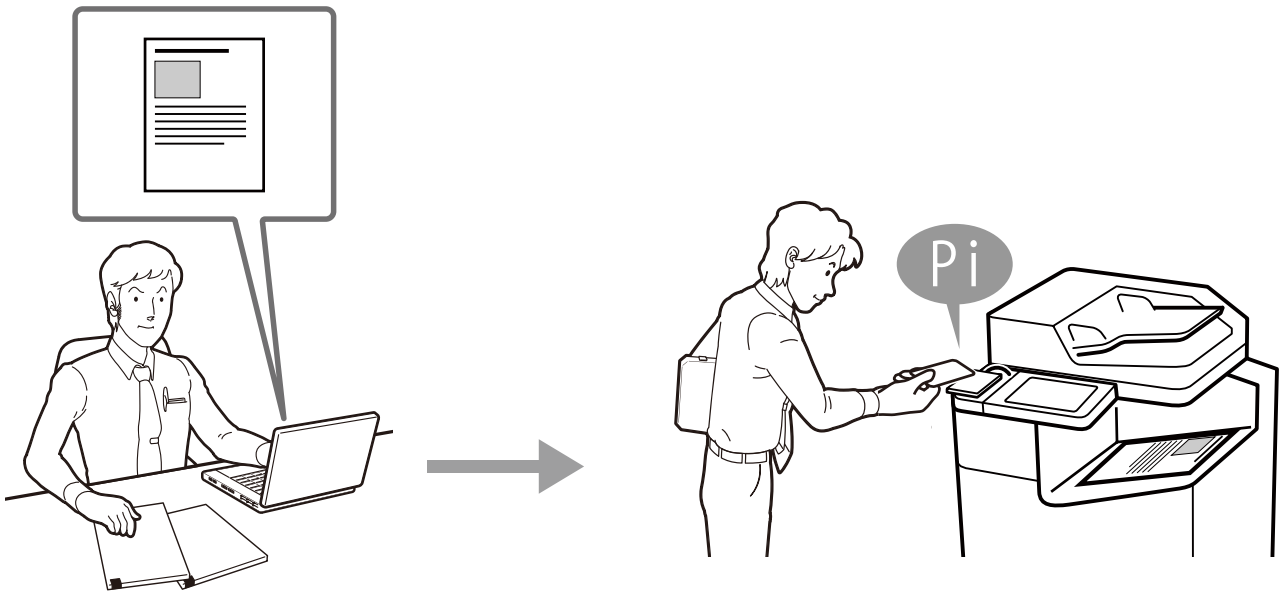
9-3. 인증 인쇄 / 스캐닝

옵션인 Epson Print Admin 또는 Epson Print Admin Serverless 를 설치하면 ID/ 암호 인증 및 IC 카드 리더와 같은 인증 장치를 사용하여 인쇄 또는 스캔하는 사용자를 인증할 수 있습니다 . 사용자가 제품 앞에서 인증 및 작업을 수행하면 사람들이 실수로 집어 올린 인쇄물이나 무인 문서에서 정보가 유출되는 것을 방지할 수 있습니다 .

LDAP 로 연결되어 프린터에 등록된 사용자는 이를 인증 방법으로 사용할 수 있습니다 .

또한 일부 독립형 스캐너의 경우 메인 유닛 인증 또는 Document Capture Pro Server Authentication Edition 을 사용하여 ID/ 암호 인증 또는 IC 카드 리더와 같은 인증 장치로 스캔을 인증할 수 있습니다 .

LDAP 로 연결되어 프린터에 등록된 사용자는 이를 인증 방법으로 사용할 수 있습니다 .



9-4. 비밀번호 정책

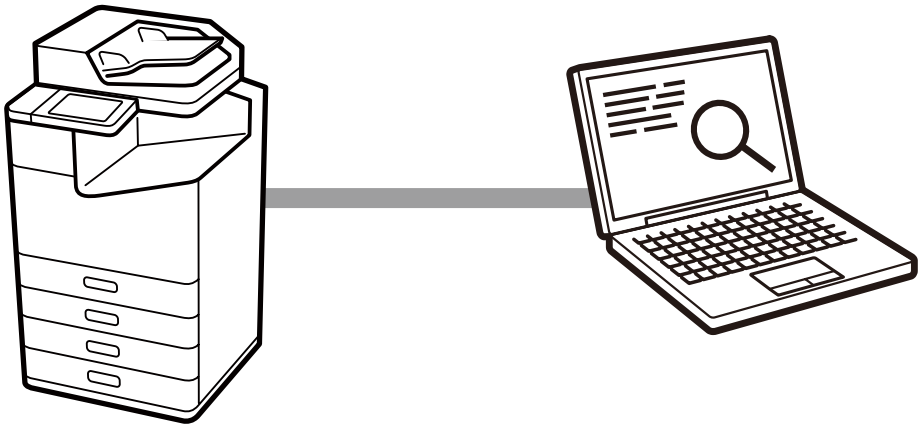
관리자 비밀번호 , 액세스 제어 , 팩스에 비밀번호 정책을 적용할 수 있습니다 . 다음과 같이 여러 조건을 요구하는 강력한 비밀번호는 악의적인 공격자에 의한 비밀번호 크래킹을 방지하는 데 도움이 될 수 있습니다 .

- 비밀번호의 최소 문자 수
- 비밀번호에 영문 대문자 포함 / 포함 안 함
- 비밀번호에 영문소문자 포함 / 포함 안 함
- 비밀번호에 숫자 포함 / 포함 안 함
- 비밀번호에 기호 포함 / 포함 안 함

9-5. 감사 로그

감사 로그 기능은 감사 목적으로 인쇄 , 복사 , 스캔 , 팩스 및 설정 변경 내역을 기록할 수 있습니다 . 이 로그를 주기적으로 확인하면 잘못된 사용에 대한 조기 발견 및 보안 문제 추적에 도움이 될 수 있습니다 .

최대 20,000 개의 감사 로그 (일부 모델의 경우 최대 5,000 개) 가 보관됩니다 .



10. 제품 보안

10-1. 자동 펌웨어 업데이트

자동 펌웨어 업데이트가 활성화되면 지정된 시간에 펌웨어가 자동으로 업데이트될 수 있습니다 . 업데이트는 지정된 시간에 진행되기 때문에 작업을 중단하지 않고 항상 최신 펌웨어를 사용할 수 있습니다 .

10-2. 불법 펌웨어 업데이트로부터 보호

펌웨어 업데이트 중에 관리자 비밀번호를 통한 인증이 수행됩니다 . 또한 제품과의 데이터 통신은 HTTPS 로 보호되며 제품 자체로 전송된 펌웨어는 펌웨어를 다시 쓰기 전에 서명으로 합법적인지 확인합니다 . 이를 통해 악의적인 제 3 자에 의한 무단 펌웨어 수정을 방지할 수 있습니다 .

10-3. 보안 부트

시작 시 시스템은 서명을 통해 제품 펌웨어가 합법적인지 확인합니다 . 펌웨어가 다시 읽히며 , 승인되지 않은 펌웨어임을 감지하면 부팅을 중지하고 , 사용자에게 펌웨어를 업데이트하라는 메시지를 표시합니다 .

10-4. 멀웨어 침투 감지

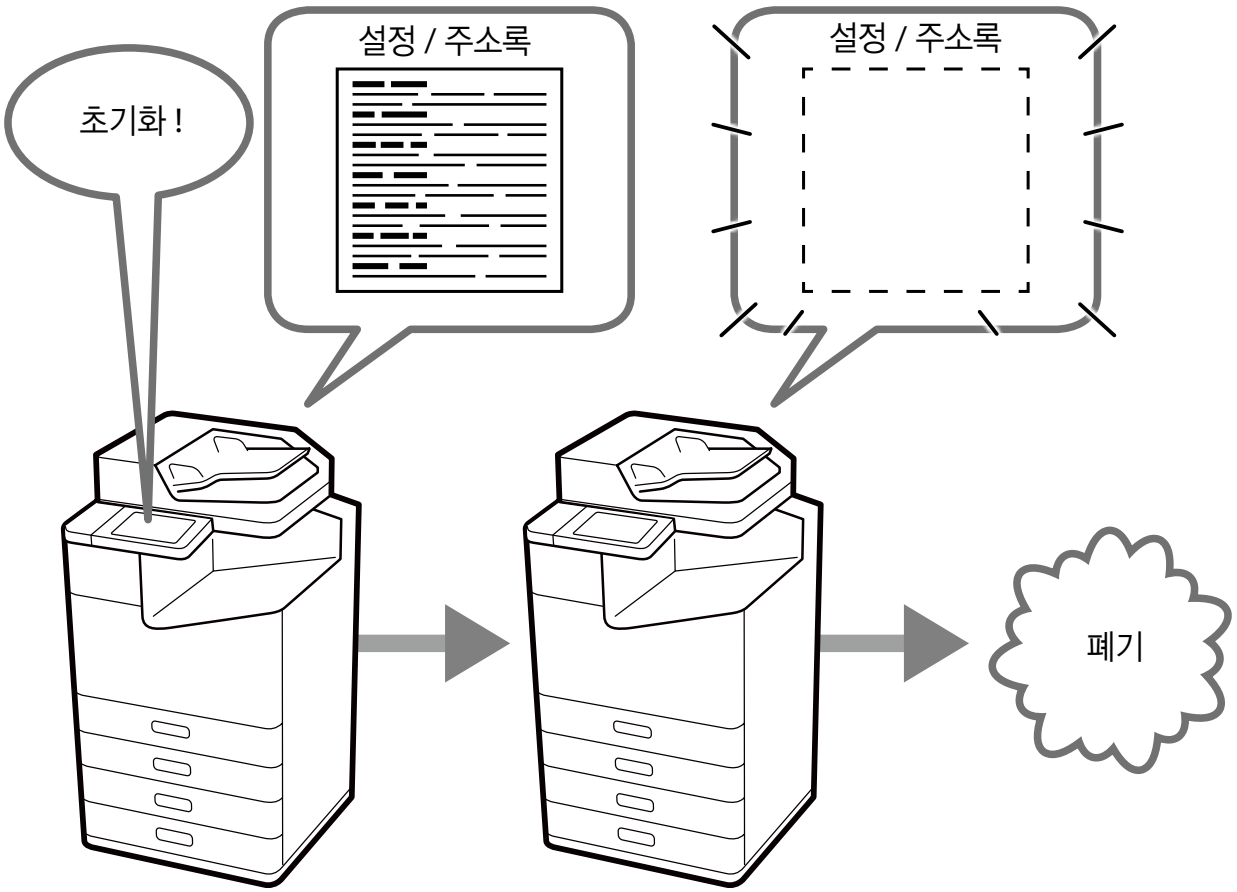
제품이 실행되는 동안 펌웨어에 악성 소프트웨어가 침투하는지 지속적으로 모니터링됩니다 . 악성 소프트웨어가 감지되면 해당 악성 소프트웨어를 제거하기 위해 제품을 재부팅합니다 .

11. 제품 폐기 시 보안 조치

11-1. 공장 기본값 복원

제품을 양도하거나 폐기할 때 모든 설정 (내장 HDD/SSD 포함) 을 공장 출하 상태 (초기화) 로 되돌려 기밀 정보가 유출되는 것을 방지할 수 있습니다 .

또한 HDD/SSD 는 " 자체 암호화 드라이브 내부에서 암호화 키를 변경하여 삭제 (고속)" 또는 " 암호화 키를 변경하고 특수 패턴으로 덮어쓰기 (덮어쓰기 , 트리플 덮어쓰기) 하여 삭제 " 할 수 있습니다 .



12. 보안 인증 및 표준

12-1. ISO15408/IEEE2600.2™

본 제품은 IEEE Std. 규격 준수를 위한 ISO/IEC 15408 인증을 획득하였습니다 . 2600.2™-2009[*1], 정보 보안을 위한 국제 표준입니다 .

IEEE Std. 2600.2™

IEEE Std. 2600.2™ 은 MFP 에 대한 정보 보안 기준을 지정하는 국제 표준입니다 . 사용자 식별 및 인증 , 액세스 제어 , 데이터 덮어쓰기 , 네트워크 보호 , 보안 관리 , 자체 테스트 , 감사 로그 등 표준을 준수하는 보안 기능을 제공하여 MFP 보안을 종합적으로 강화할 수 있습니다 .

ISO/IEC 15408

공통 기준 (CC, Common Criteria) 이라고도 불리는 ISO/IEC 15408 은 IT 제품 및 시스템의 보안 조치를 독립적이고 객관적으로 평가하여 해당 조치가 적절하게 설계 및 구현되었는지 여부를 판단하기 위한 국제 표준입니다 .

지정된 버전의 펌웨어 , 매뉴얼 및 기타 구성 요소는 ISO/IEC 15408 인증을 위해 평가됩니다 . 구입한 제품의 펌웨어 버전은 인증된 버전과 다를 수 있습니다 .

인증된 버전을 사용하는 경우 제품 기능에 일부 제한이 있을 수 있습니다 .

CCRA 인증 로고는 제품이 일본 정보기술 보안 평가 및 인증 제도 (JISEC[*2]) 에 따라 평가 및 인증되었음을 나타냅니다 .
이는 제품에 취약점이 전혀 없음을 보장하는 것은 아닙니다 .
또한 , 제품이 모든 운영 환경에서 필요한 모든 보안 기능을 갖추고 있음을 의미하지는 않습니다 .

*1 미국 정부 승인 보호 프로필 - 하드카피 장치용 미국 정부 보호 프로필 버전 1.0 (IEEE Std. 2600.2™-2009)

*2 JISEC (일본 정보기술 보안 평가 및 인증 제도)

프로토콜 기능이 활성화될 때의 보안 위험과 비활성화될 때의 제한

프로토콜 / 보안 기능	활성화될 때의 보안 위험	비활성화될 때의 제한
Bonjour	제 3 자가 네트워크의 장치에 대한 정보를 읽을 가능성이 있습니다 .	컴퓨터에서 Bonjour 로 검색할 수 없습니다 .
SLP	발신자가 인증되지 않았기 때문에 발신자가 스푸핑되면 서비스를 비활성화하는 공격에 악용될 수 있습니다 .	컴퓨터는 SLP 를 사용하여 장치에 대한 정보를 검색하거나 탐색할 수 없습니다 .
WSD	통신이 암호화되지 않았으므로 제 3 자가 인쇄된 데이터를 읽을 가능성이 있습니다 .	WSD 를 사용하여 인쇄 및 스캔할 수 없습니다 .
LLTD	제 3 자가 네트워크의 장치에 대한 정보를 읽을 가능성이 있습니다 .	Windows 의 " 장치 및 프린터 " 에 장치가 표시되지 않습니다 .
LLMNR	제 3 자가 네트워크의 장치에 대한 정보를 읽을 가능성이 있습니다 .	컴퓨터에서 LLMNR 로 검색할 수 없습니다 .
LPR	통신이 암호화되지 않았으므로 제 3 자가 인쇄된 데이터를 읽을 가능성이 있습니다 .	LPR 을 사용한 인쇄는 불가능합니다 .
RAW (포트 9100/ 모든 포트)	통신이 암호화되지 않았으므로 제 3 자가 인쇄된 데이터를 읽을 가능성이 있습니다 .	RAW 포트를 사용한 인쇄는 불가능합니다 .
IPP/IPPS	IPP 의 경우 통신이 암호화되지 않으므로 제 3 자가 인쇄된 데이터를 읽을 가능성이 있습니다 . IPPS 의 경우 보안 위험이 없습니다 .	AirPrint 또는 Mac OS 에서 인쇄하는 것과 같이 IPP/IPPS 를 사용한 인쇄는 불가능합니다 .
FTP	통신이 암호화되지 않았으므로 제 3 자가 인쇄된 데이터를 읽을 가능성이 있습니다 .	FTP 를 사용하여 파일을 인쇄하거나 전송할 수 없습니다 .
SNMP	SNMPv1 및 v2c 의 경우 통신이 암호화되지 않으므로 제 3 자가 장치 정보 및 설정 데이터를 읽을 가능성이 있습니다 . SNMPv3 의 경우 보안 위험이 없습니다 .	SNMP 를 사용하는 관리 도구를 사용할 수 없습니다 . 또한 Epson 에서 제공하는 관리 도구 및 애플리케이션을 사용할 수 없습니다 .
SSL/TLS	설정한 TLS 버전 및 키 길이에 따라 암호화 강도가 약하고 암호가 해독될 수 있습니다 .	브라우저에서 HTTPS 를 통한 연결이 불가능합니다 .
Microsoft Network Sharing	스캔된 데이터 또는 파일 공유 데이터를 제 3 자가 읽을 가능성이 있습니다 .	SMB 를 사용하여 파일을 전송하고 네트워크 파일을 공유할 수 없습니다 .
네트워크 스캔 (EPSON Scan)	통신이 암호화되지 않으므로 제 3 자가 스캔된 데이터를 읽을 가능성이 있습니다 .	네트워크를 통한 스캔이 불가능합니다 .
PC-FAX	통신이 암호화되지 않았기 때문에 네트워크의 팩스 데이터를 제 3 자가 읽을 가능성이 있습니다 .	PC-FAX 기능을 사용할 수 없습니다 .

EPSON

주의

- 본 문서의 일부 또는 전부를 복제하는 것은 금지되어 있습니다 .
- 본 문서의 내용은 향후 예고 없이 변경될 수 있습니다 .
- 이 문서는 정보 제공 목적으로만 제공됩니다 . 자세한 활용 방법은 각 제품의 매뉴얼을 확인해주십시오 .

상표

- Microsoft is trademark of the Microsoft group of companies.
- Wi-Fi is trademarks of Wi-Fi Alliance.
- Other product names are the trademarks or registered trademarks of their respective companies.

NPD6296-05 KO
©2024 Seiko Epson Corporation