

Contribution

Marathon

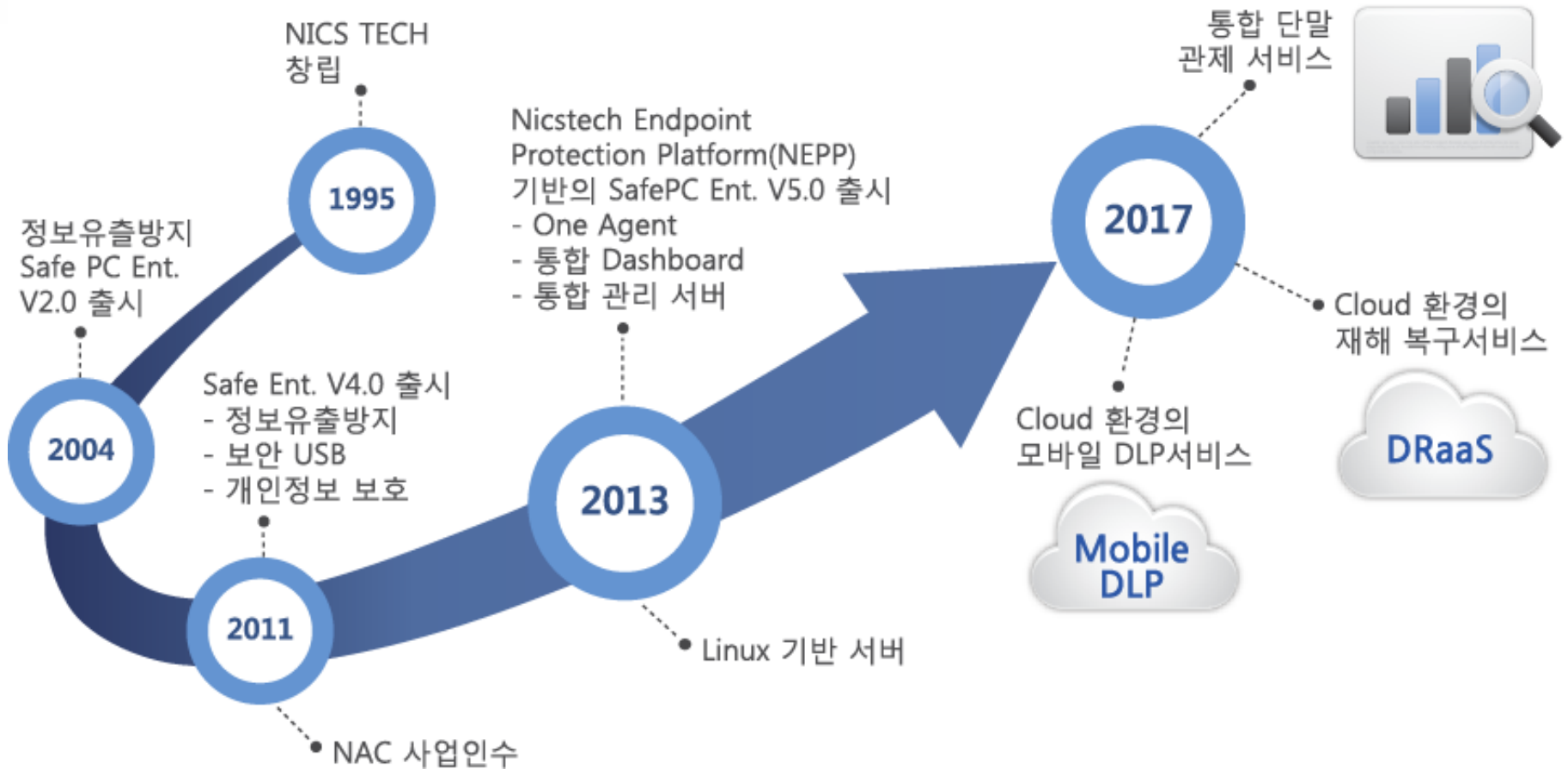
Innovation

# 기업환경 변화에 따른 Endpoint 보안의 변화

---

2015 . 04

# 닉스테크 성장



# 닉스테크 솔루션



**PC 보안**




**보안 USB**




**개인정보**



**1,400+**  
Sites and Services



# 1. 기업의 환경 변화

1

업무 SW → 보편화 클라우드 서비스



2

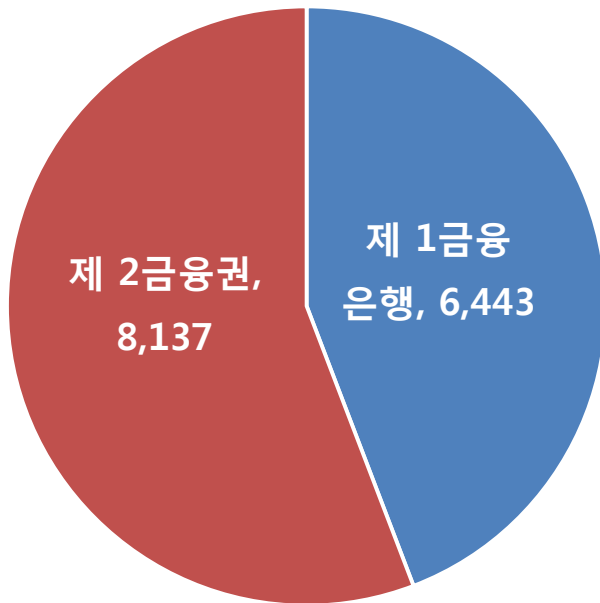
업무 연속성 → BYOD (모바일 단말 사용)

3

HW 운영 → 가상화 환경 (망분리 등)

# 1. 기업의 환경 변화

## 망분리 지점 규모

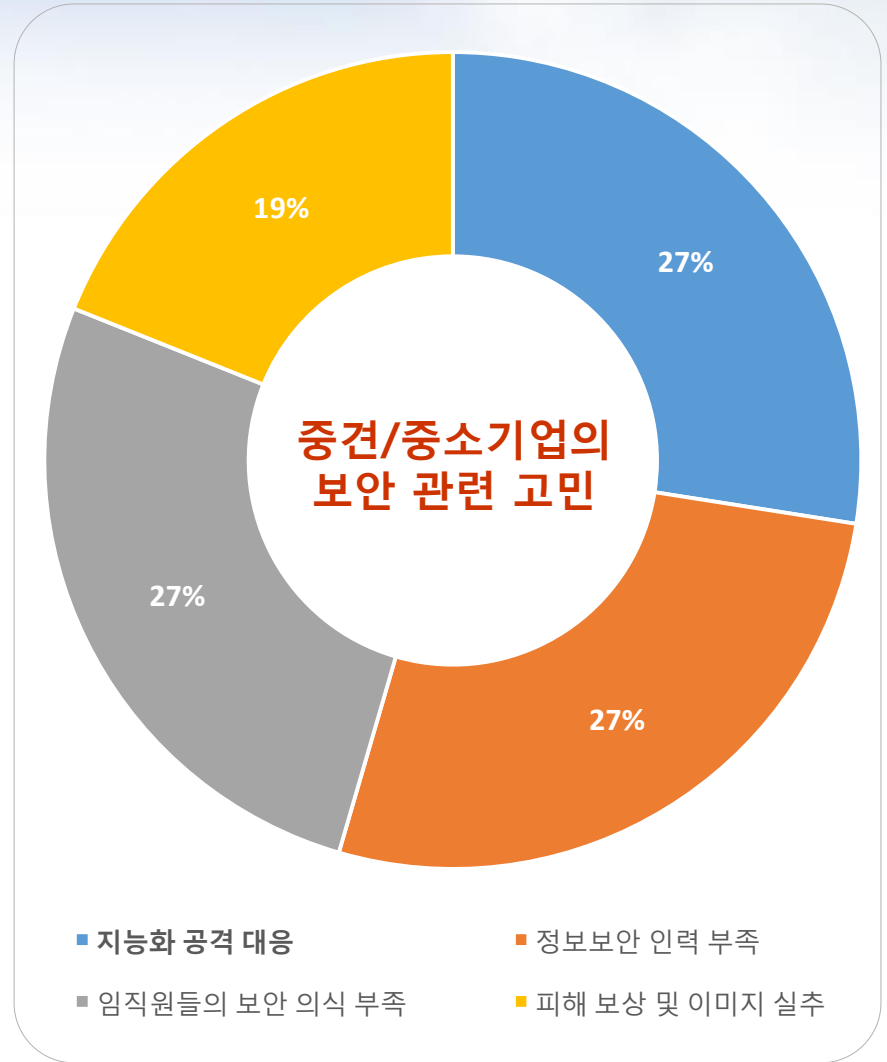
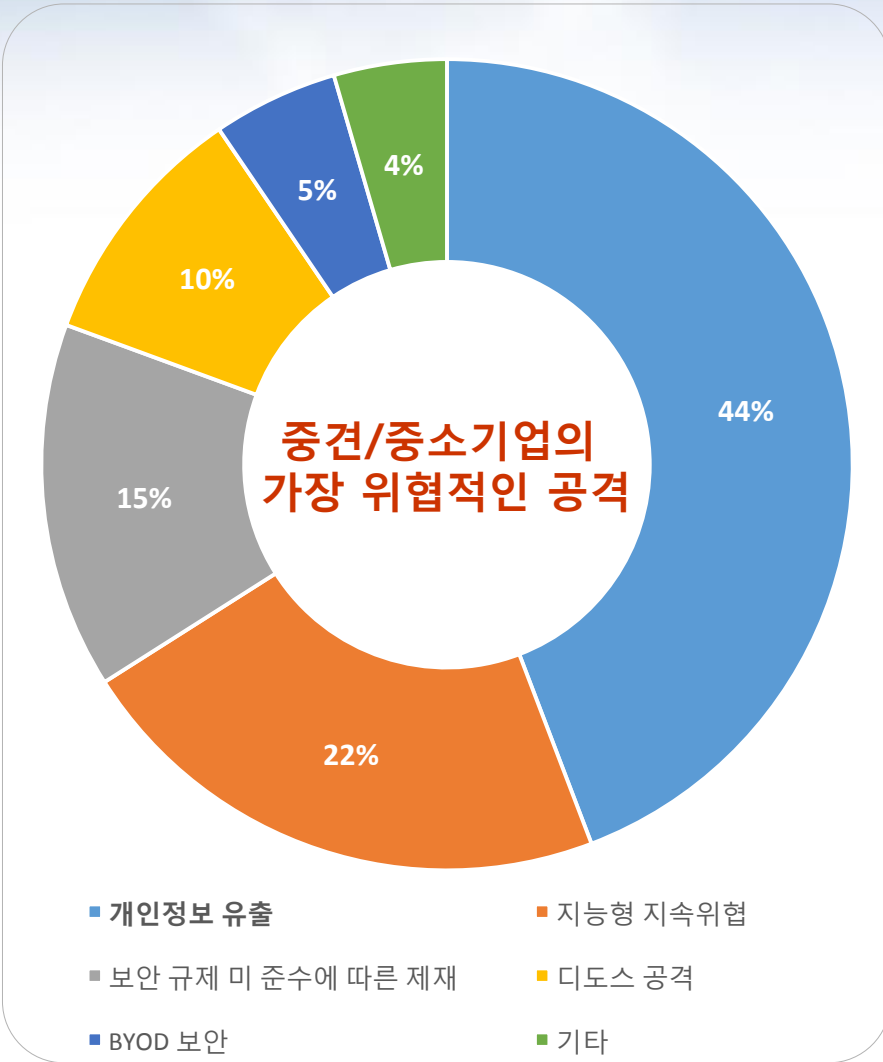


단위 : 기관 지점 수

출처 : 금융감독원, 금융통계 정보시스템  
(2014년 9월 기준)

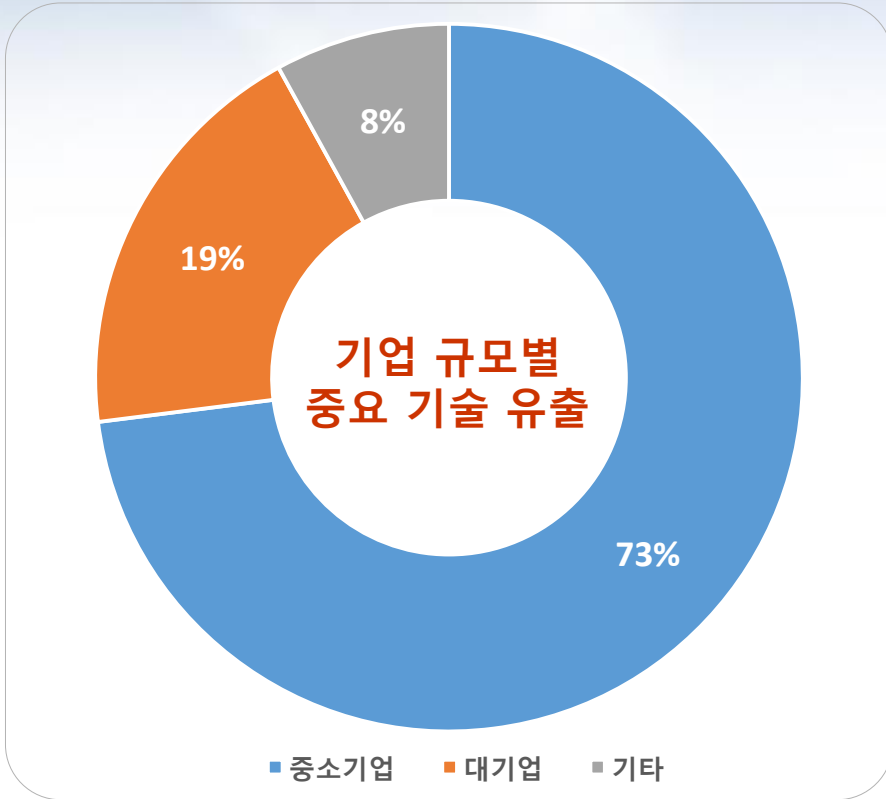
- 정보통신망법 : 15조 2항 3호 (개인정보 취급자 컴퓨터 외부 인터넷 차단)
- 개인정보보호법 : 30조 1항 2호 (개인정보 접근 통제 및 권한 제한)
- 금융위원회 금융전산 보안 강화 종합 대책(2013)
  - 금융전산 망분리 가이드 : 2015년 말까지 은행 본점 및 영업점 망분리(증권사 포함), 2016년 말까지 제 2금융권 망분리
  - 금융전산 망분리 가이드 내용 中 : PC보안 및 보안 USB, NAC 도입에 대한 필요성 포함.
  - 기존 금융권 고객 및 신규 고객 시장 활성화 (단말의 증가에 따른 추가 시장)

## 2. 2015년 중견/중소기업의 보안



출처 : IBM, 국내 "중견중소기업을 위한 보안 솔루션 구매 가이드" 내용 중

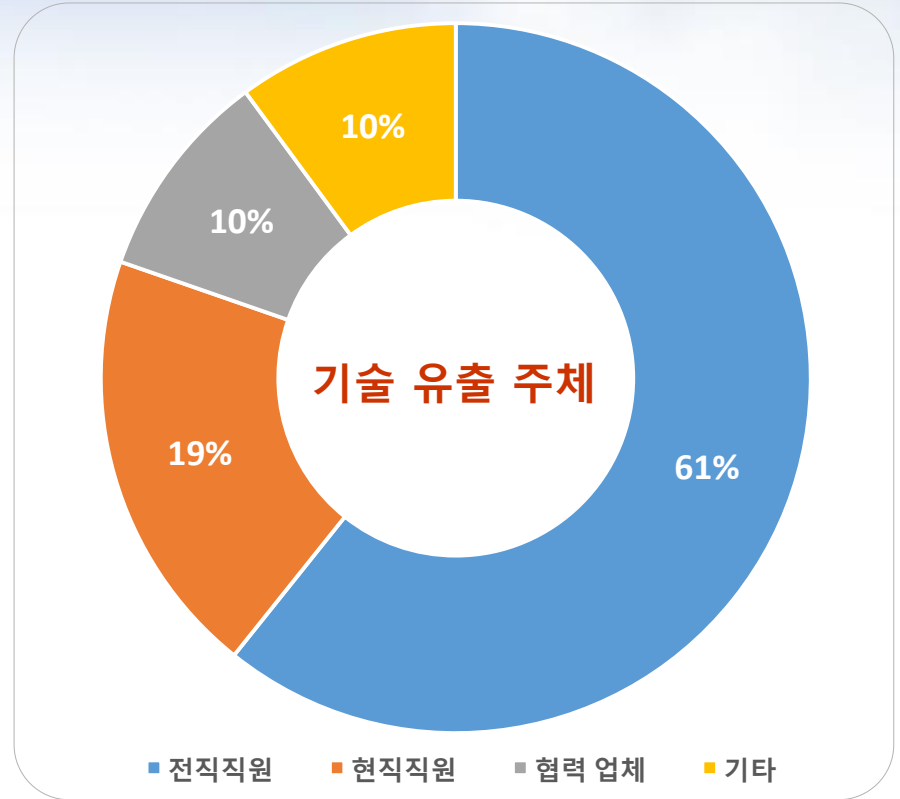
## 2. 2015년 중견/중소기업의 보안



[자료 출처 : E-Journal, 11/01/2014]

### 규모별 기술 유출 이슈

- 중소기업의 높은 유출율 → 보안 관리 및 기술 투자 필요
- 대기업의 경우 유출에 따른 피해도가 높음.



[자료 출처 : E-Journal, 11/01/2014]

### 기술 유출 주체 이슈

- 정보 유출 주체는 기업 인원 및 관계자가 90% 임.
- 기업의 내부 정보의 관리 및 보안 기술 투자 필요.

### 3. Endpoint 보안 관점

1

#### 내부자 위협에 대한 정의

- 내부자 위협이란 권한을 보유하고 있는 보유자 또는 보유 대상의 행위

2

#### 데이터의 흐름에 대한 분석

- 평소 업무에 따른 데이터의 흐름  
→ 부서간 업무 흐름, 직급에 따른 업무 흐름, 업무 패턴 등

3

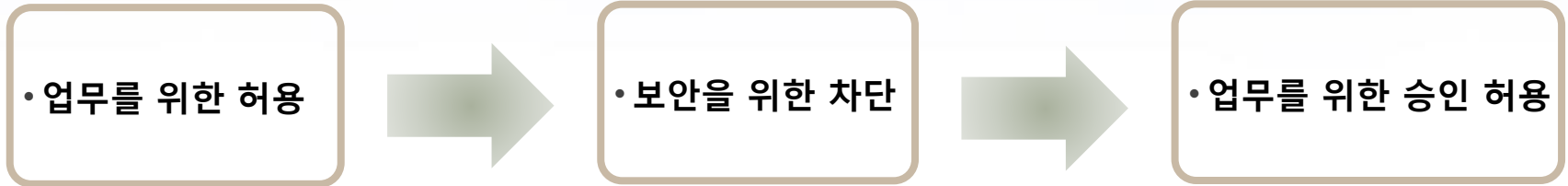
#### 위협의 우선 순위 정의

- 모든 것을 다 막기는 어려움.  
→ 위협에 따른 자산의 리스크 관리가 필요(우선 순위를 통한 자산 보호)



### 3. Endpoint 보안 관점

#### 01 | 업무의 익숙함 → 편리성



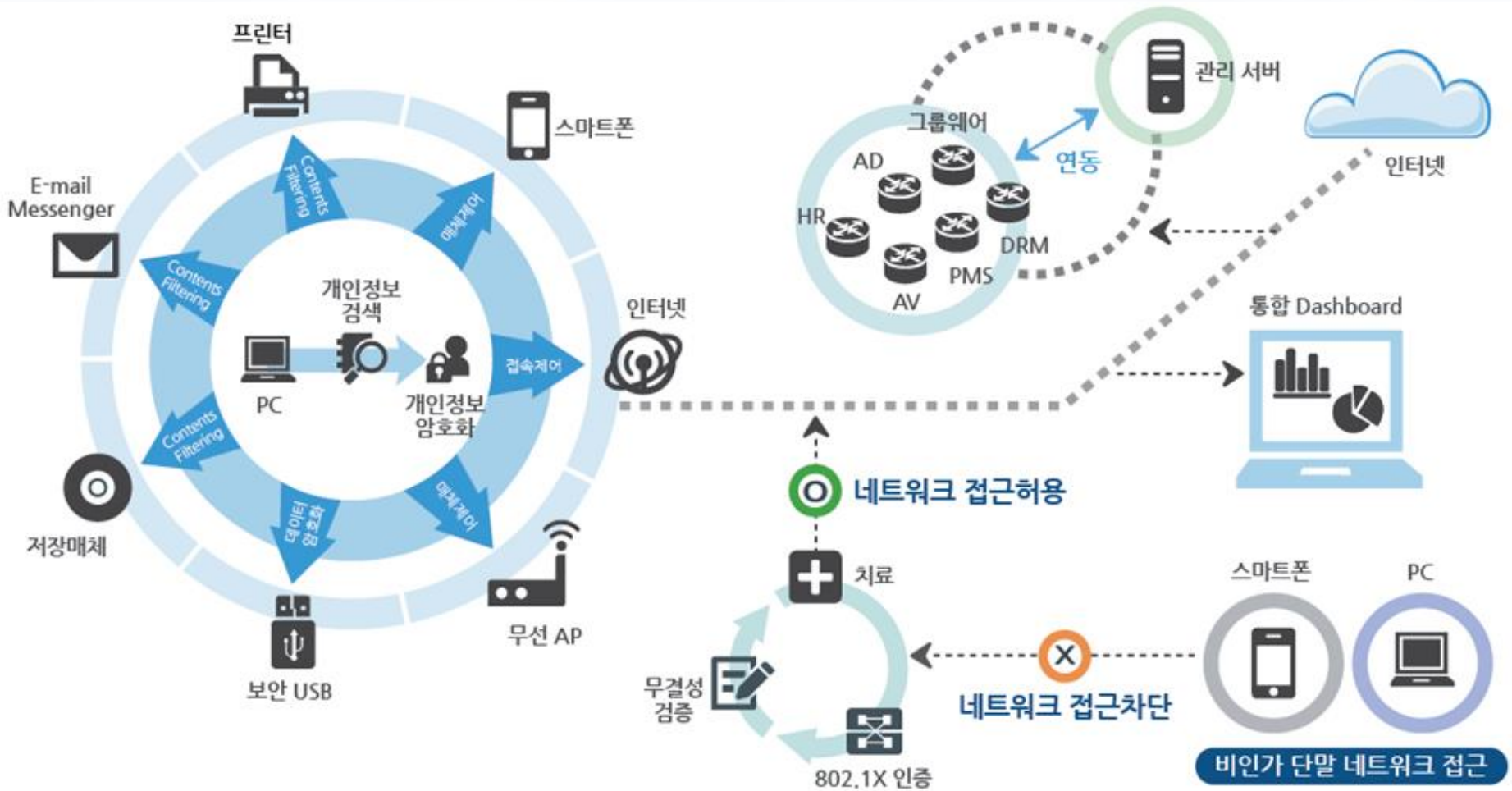
#### 02 | 보안 솔루션 통제 시간

- 보안 정책에 따른 업무 지원에 걸리는 시간  
→ 예) 신청 / 승인에 걸리는 시간

#### 03 | 보안 솔루션 심리적 부담감

- 보안 솔루션의 기능이 동작에 따른 심리적 부담(로그 수집 등), 보안 관리자의 장애 대응
- 해당 결과에 대한 책임(승인권자, 보안 관리자 등)

# 4. Endpoint 보안 솔루션 구성



## 4. Endpoint 보안 솔루션 구성

보안 솔루션 도입 효과

1

통제를 통한 보안 의식 강화

2

중요 정보의 유출 가능성 차단

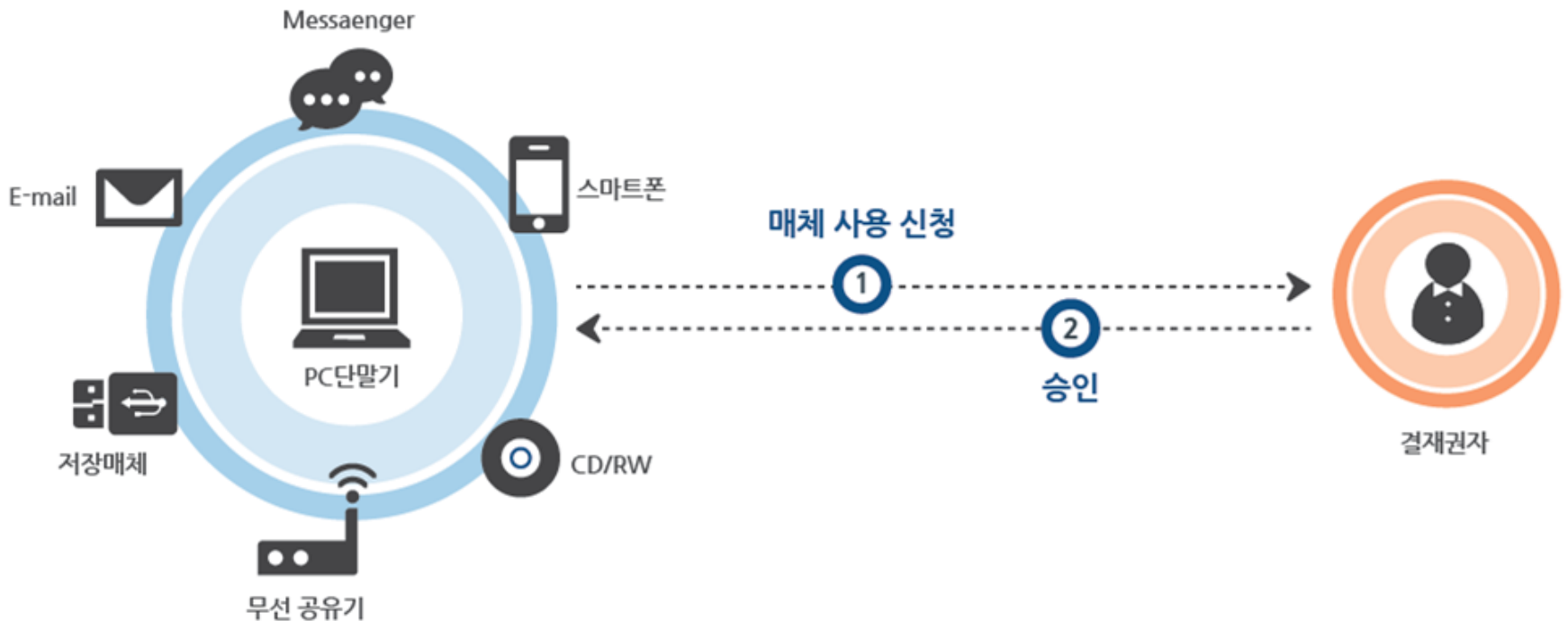
3

감사 로그를 통한 사후 문제점 및 해결 방안 모색

## 5. 효율적인 보안 솔루션 운영 방안

### 가. PC 보안 기능

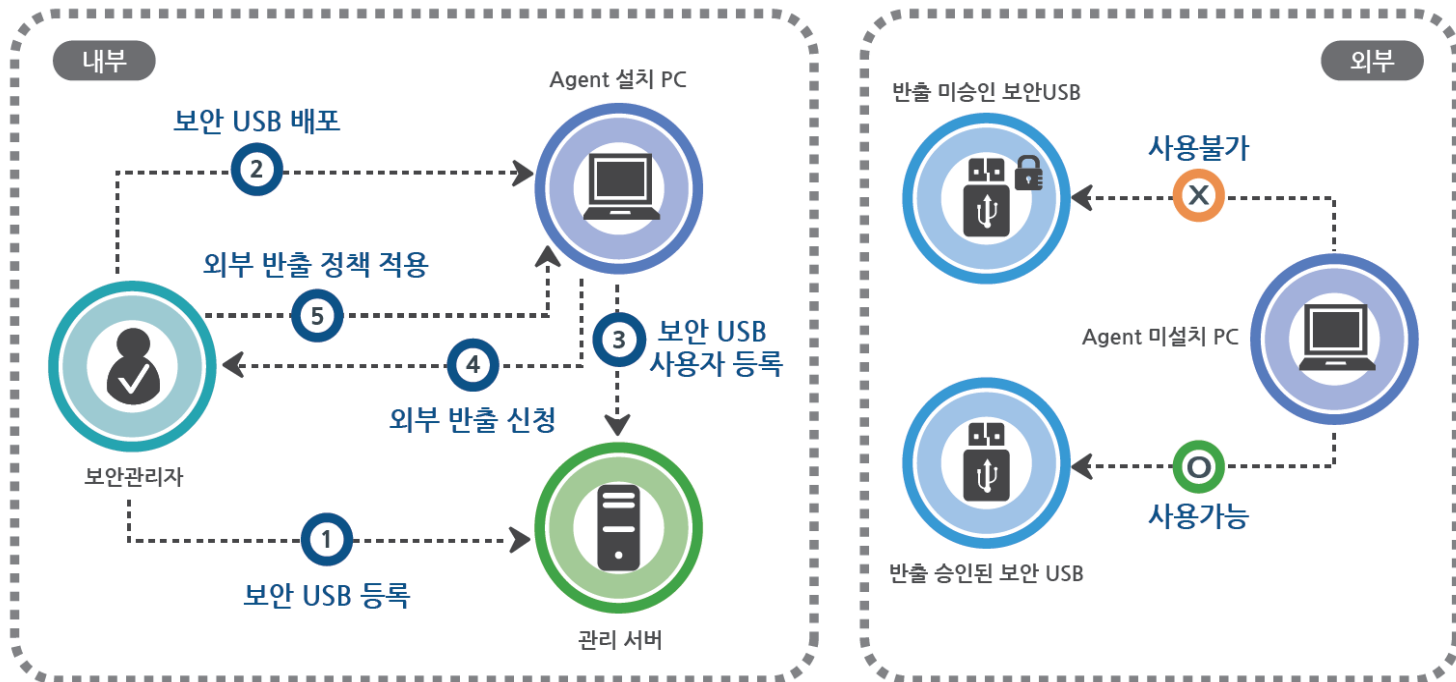
- PC의 매체 통제 (허용 / 차단)
- 매체 사용 신청 프로세스 제공 (기간 / 시간 / 알림 / 위임)
- 해당 프로세스로 매체에 파일 복사를 허용하고 해당 반출 로그 제공



# 5. 효율적인 보안 솔루션 운영 방안

## 나. 보안 USB 기능

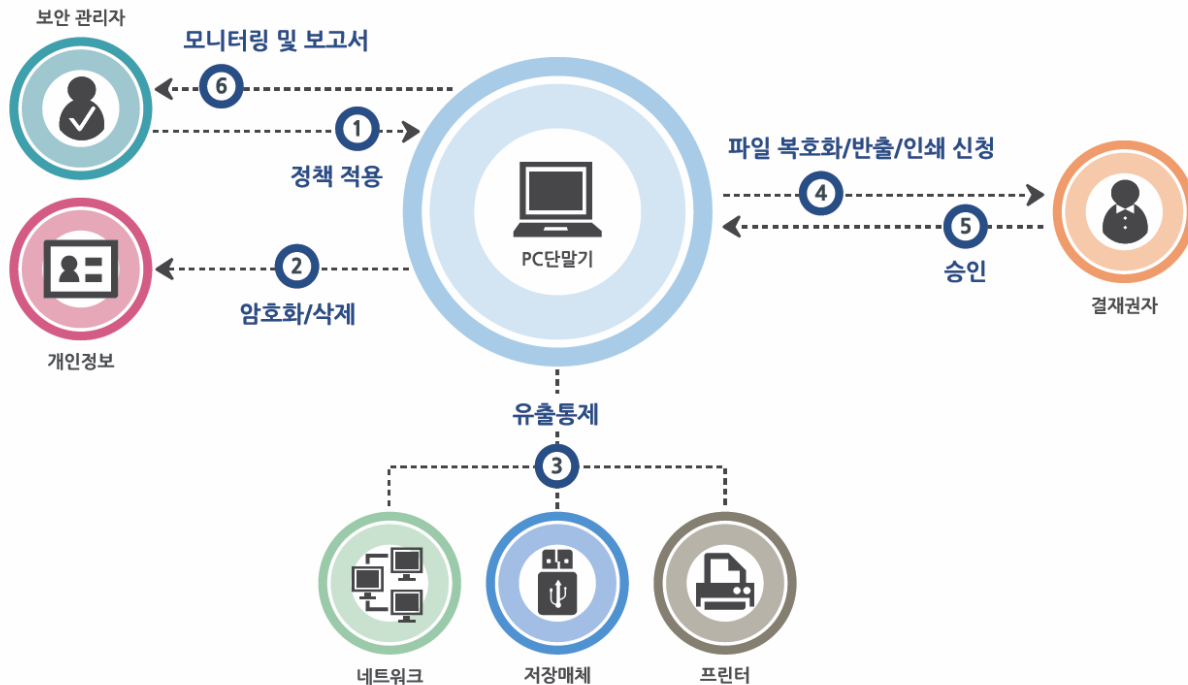
- 일반 USB 메모리 분실에 따른 내부 정보 유출  
→ 분실 및 도난에 대한 보안 정책, 사용자 인증을 통한 접근
- 외부 PC에 연결하여 USB 메모리 내의 정보 복사  
→ 보안 USB 내 데이터 외부 복사 통제, 다른 이름 저장 차단, 출력 차단, 웹 첨부 차단



# 5. 효율적인 보안 솔루션 운영 방안

## 다. 개인정보 파일 반출

- 개인정보 보호법으로 개인정보 파일 관리 방안 필요
- 개인정보 파일과 일반 파일에 따른 반출 방안
  - 일반 파일 반출 가능 / 개인정보 파일 승인 반출
  - 일반 파일 및 개인정보 파일 승인 반출 (승인 라인 별도)
- \* 승인라인 별도 : 개인정보 파일은 개인 정보 관리자 별도로 승인 라인에 포함.



## 5. 효율적인 보안 솔루션 운영 방안

### 라. 보안 강화

	매체 권한 통제	파일 반출 프로세스
기본 정책	읽기/쓰기 차단	모든 파일 차단
승인 요청	읽기 권한만 승인 요청	파일 반출 승인 요청
승인 후	휴대용 저장 장치 데이터만 읽기 가능	승인 받은 파일만 반출

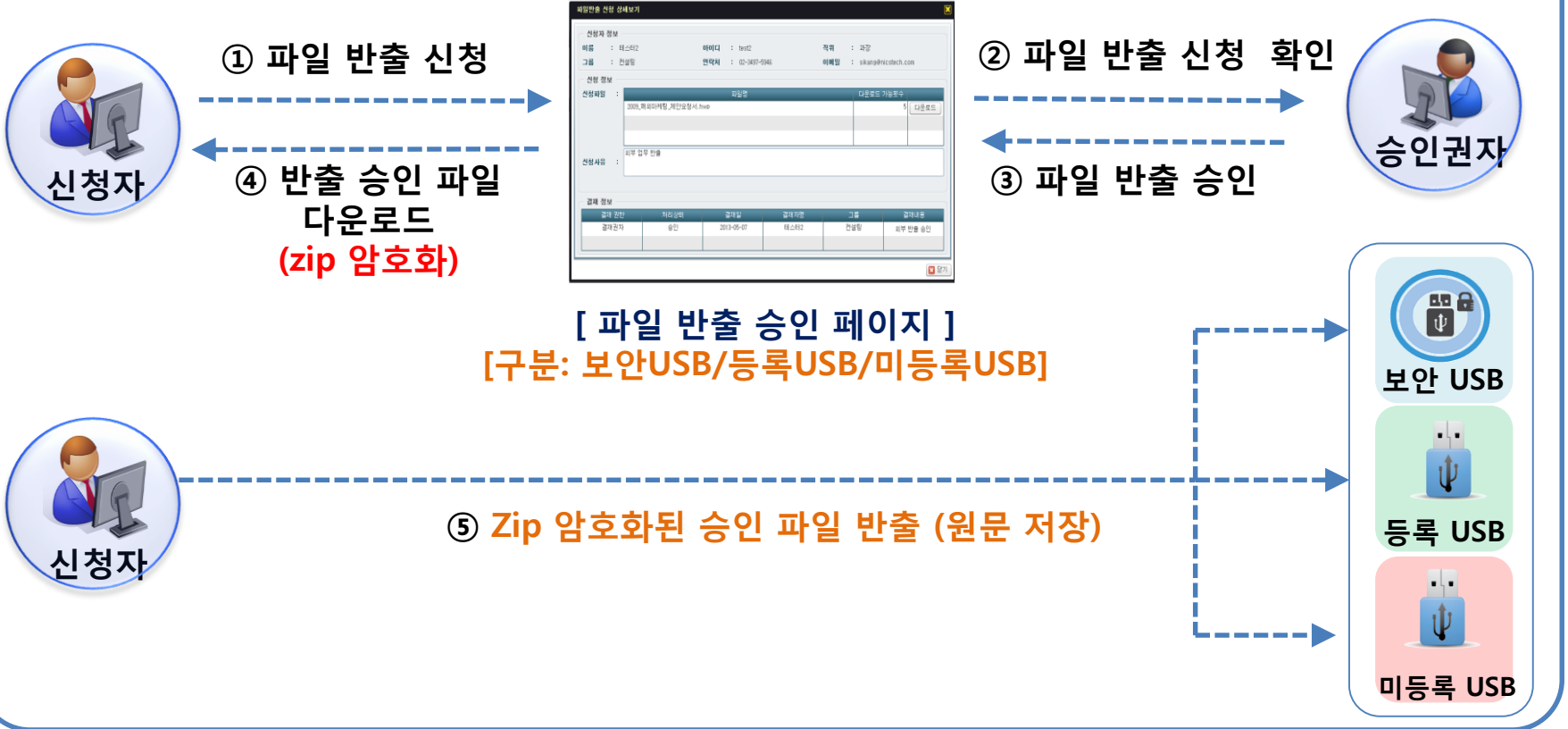
- 보안 USB 반출 프로세스 특화 → 매체 지정 파일 반출 기능  
→ 매체 지정이 가능한 사유 : 보안 USB 시스템은 매체 등록 관리 기능 제공
- 매체 등록 관리를 통해서 보안 USB, 등록 USB, 미등록 USB 구분 가능

# 5. 효율적인 보안 솔루션 운영 방안

## 라. 보안 강화

### 매체 지정 파일 반출 시스템 제공

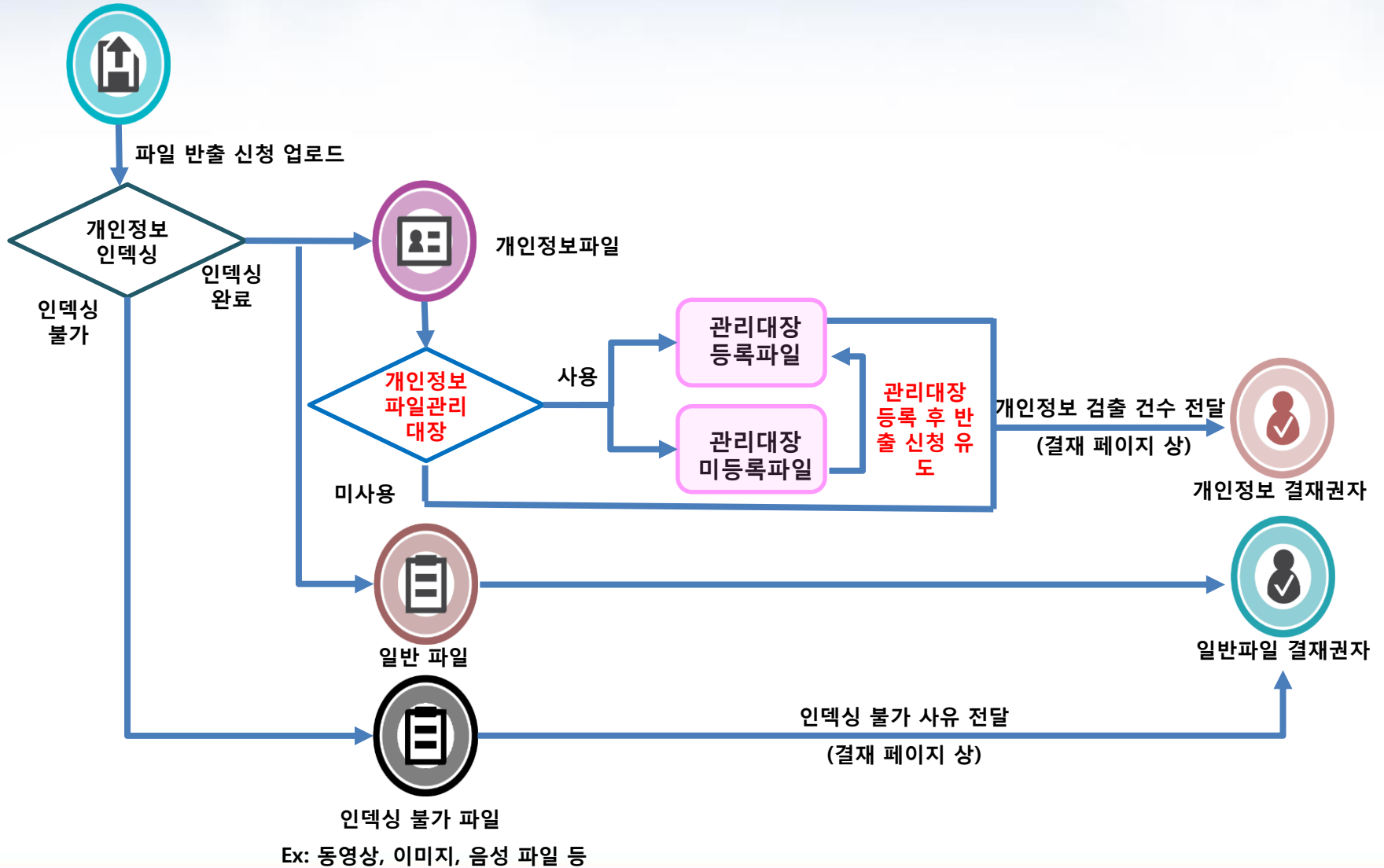
▶ 파일 반출 승인 시 매체를 지정하여 반출 가능함.





# 5. 효율적인 보안 솔루션 운영 방안

## 라. 보안 강화



## 6. Endpoint 보안 솔루션 운영

### 계층적 방어

네트워크 접근 통제

필수 프로그램 설치

최신 패치 설치

매체 / 프린터 사용 통제

네트워크 사용 통제

Application 사용 통제

개인정보 암호화

개인정보 유출 통제

이동 저장매체 접근 통제

외부 PC 파일 이동 통제

### 솔루션

네트워크 접근통제

PC보안

개인정보보호

보안USB

## 6. Endpoint 보안 솔루션 운영



### ✓ 네트워크 접근 통제

필수 프로그램 설치

최신 패치 설치

매체/프린터 사용 통제

네트워크 사용 통제

Application 사용 통제

개인정보 암호화

개인정보 유출 통제

이동 저장매체 접근 통제

외부 PC 파일 이동 통제

### ❖ 유/무선 네트워크 접근 통제

- 엔드포인트의 내부망 접근 시도 시, 접근이 가능한 자에 대한 사전 정의를 통해 접근 통제

### ❖ 인증 방법

- 사용자 ID/PW/IP/MAC/HDD size
- 국제 표준 IEEE 802.1x

## 6. Endpoint 보안 솔루션 운영



네트워크 접근 통제

✓ 필수 프로그램 설치

✓ 최신 패치 설치

매체/프린터 사용 통제

네트워크 사용 통제

Application 사용 통제

개인정보 암호화

개인정보 유출 통제

이동 저장매체 접근 통제

외부 PC 파일 이동 통제

### ❖ 보안 취약자 접근 통제 및 치료

- Endpoint 보안상태 적절성 및 위협 방어 솔루션 운영 여부 점검 후 패치

### ❖ 보안 정책 준수 여부 체크

- 바이러스 감염 등으로 접근 거부된 Endpoint 단말은 치료 후 접근 허용

## 6. Endpoint 보안 솔루션 운영



네트워크 접근 통제

필수 프로그램 설치

최신 패치 설치

✓ 매체/프린터 사용 통제

✓ 네트워크 사용 통제

✓ Application 사용 통제

개인정보 암호화

개인정보 유출 통제

이동 저장매체 접근 통제

외부 PC 파일 이동 통제

### ❖ 매체 / 프린터 사용 통제

- 허용되지 않은 모든 매체 사용 통제.
- 스마트폰, USB 저장매체, Wi-Fi, CD/RW
- 출력물 워터마킹
- 출력 로깅 및 원문 저장

### ❖ 네트워크 유출 통제

- 비 업무 사이트 접속 차단
- E-mail 통한 파일 유출 차단

### ❖ Application 사용 통제

- 비 업무/불법 Application 사용 제어

## 6. Endpoint 보안 솔루션 운영

네트워크 접근 통제

필수 프로그램 설치

최신 패치 설치

매체/프린터 사용 통제

네트워크 사용 통제

Application 사용 통제

✓ 개인정보 암호화

✓ 개인정보 유출 통제

이동 저장매체 접근 통제

외부 PC 파일 이동 통제



### ❖ 개인정보 암호화

- 내용 기반 개인정보 검색
- 개인정보 암호화 및 중앙 통제
- 개인정보파일관리대장

### ❖ 내용 기반 유출 경로 통제

- USB 저장 매체/E-mail/프린트 유출 통제

### ❖ 파일 반출 승인 프로세스

- 승인된 암호화 파일에 대해서만 외부 반출 통제 및 반출 파일 원문 저장

## 6. Endpoint 보안 솔루션 운영

네트워크 접근 통제

필수 프로그램 설치

최신 패치 설치

매체/프린터 사용 통제

네트워크 사용 통제

Application 사용 통제

개인정보 암호화

개인정보 유출 통제

✓ 이동 저장매체 접근 통제

✓ 외부PC 파일 이동 통제

### ❖ 보안USB 접근 인증

- USB 저장매체 접근 시, 인증 요구
- 인증 실패 시 USB 접근 통제

### ❖ 데이터 자동 암호화

- PC → USB 파일 이동 시, 자동 암호화

### ❖ USB 분실 조치

- 데이터 완전 삭제 및 USB 접근 통제

### ❖ 외부 PC 파일 이동 통제

- USB 외부 반출 승인 프로세스
- 파일 읽기 및 외부 복사 통제



NICS TECH Co., Ltd.

Network Integrated computing Service Provider

Contribution

Marathon

Innovation

감사합니다