MPIS 2021
2021 의료기관 개인정보보호&정보보안 컨퍼런스

K-Hospital 정보보안의 이슈와 대안

2021년 7월 6일

대한병원정보협회 한기태
(kthan@kuh.ac.kr)

목 차

[Issue 1] 전자의무기록시스템 인증기준 변경
(인증기준 : 보안성 S014 클라우드 서비스 사용 보안 인증)

[참조] (재)한국보건의료정보원 인증위원회 회의자료

[Issue 1] 전자의무기록시스템 인증기준 변경

[현행] 인증기준 : 보안성 S014 클라우드 서비스 사용 보안 인증

중분류	인증기준	번호	인증기준 설명	유형 1	유형 2	유형 3
6.1 계정관리	계정 관리	S001	1. 책임추적성을 관리할 수 있도록 사용자별로 필요 계정이 발급되어야 한다. 2. 사용자 계정 삭제(사용중지) 시 기록을 유지할 수 있어야 한다.	필수	필수	필수
6.1 계정관리	비밀번호 관리	S002	사용자 비밀번호를 관리할 수 있어야 한다. - 사용자 비밀번호 관리는 비밀번호 작성규칙 통제, 비밀번호 일정주기 변경, 비밀번호 초기화 후 강제 변경을 포함한다.	필수	필수	필수
6.2 접근권한	권한 관리	S003	1. 직종 및 업무별 권한 부여 기능을 갖추어야 한다. 2. 사용자 변경 또는 퇴직 시 권한을 변경하거나 말소할 수 있어야 한다.	필수	필수	필수
6.2 접근권한	권한 이력 관리	S004	사용자 권한 부여 및 회수에 대한 이력을 관리할 수 있어야 한다.	필수	필수	필수
6.2 접근권한	로그인 실패 횟수 제한	S005	로그인 실패 횟수를 제한할 수 있어야 한다.	필수	필수	필수
6.2 접근권한	세션 종료	S006	시스템을 일정 시간 동안 사용하지 않을 시 자동으로 세션이 종료되어야 한다. - 전자의무기록시스템 사용자가 일정 시간 이상 업무처리를 하지 않아 시스템에 접속이 차단된 이후, 다시 접속하고자 할 때에도 최초의 로그인과 동일한 방법으로 접속하여야 한다.	필수	필수	필수
6.3 감사	감사기록 생성 및 관리	S007	1. 감사기록을 생성하고 관리할 수 있어야 한다. - 사용자 감사기록 관리를 사용자 인터페이스로 구현하여 수행하고 있지 않은 경우 데이터베이스에 로그 기록의 저장 여부를 확인하여야 한다. - 감사기록은 로그인에 관한 기록(성공 및 실패), 전자의무기록 기록/수정(전자서명 대체 가능), 조회/출력, 접근불가 환자 조회 시 생성되어야 한다. 2. (시범)전자의무기록시스템 화면을 통해 감사기록을 조회할 수 있다.	필수	필수	필수
6.3 감사	시간 동기화	S008	시간 동기화 기능을 갖추어야 한다.	필수	필수	필수
6.4 비식별 조치	고유식별정보 마스킹 표시	S009	전자의무기록시스템에서 한 화면상에 두 건 이상의 환자 고유식별정보가 목록화되어 보여지는 경우, 이에 대한 선별적 마스킹을 할 수 있어야 한다.	필수	필수	필수
6.5 암호화	비밀번호 일방향 암호화 저장	S010	비밀번호를 일방향 암호화 방식을 사용하여 저장할 수 있어야 한다.	필수	필수	필수
6.5 암호화	고유식별정보 암호화 저장	S011	고유식별정보를 대칭키 암호화 방식을 사용하여 저장할 수 있어야 한다. - 단, 암호화 솔루션 등을 별도의 제품으로 사용하는 전자의무기록시스템의 경우 시스템에서 연계가 가능한 제품을 명시해야 한다.	필수	필수	필수
6.6 전자인증	전자서명	S012	1. 전자서명 기능을 갖추어야 한다. 2. 전자서명한 의무기록은 사용자를 식별할 수 있는 계정, 서명, 서명 일시 등을 포함해야 한다.	필수	필수	필수
6.7 백업 및 복구	백업	S013	1. 백업 기능 구현이 가능한 시스템 구조로 설계되어야 한다. - 백업은 전자의무기록시스템의 데이터로 제한하며 이를 위한 시설과 장비를 갖추어야 한다. 2. (시범)매뉴얼을 관리해야 하며 관련 법령 및 시스템의 변화에 따라 갱신할 수 있다. 3. (시범)백업 정책에 따라 월 1회 이상 등 일정한 주기로 백업을 수행할 수 있다.	필수	필수	필수
6.8 외부보관	**클라우드 서비스 사용 보안 인증**	S014	**1. 한국인터넷진흥원의 클라우드 보안인증(CSAP) 인증을 받아야 한다.** **2. (시범) 의료데이터 이외의 데이터와 혼재되지 않도록 별도 분리된 의료 데이터전용의 독립 네트워크를 구성할 수 있다.** **3. 단, 클라우드 서비스를 사용하지 않은 외부보관의 경우 보건복지부 고시 “전자의무기록의 관리 보존에 필요한 시설과 장비에 관한 기준” 에 따라야 한다.** **[해당 기관] 클라우드 서비스를 사용하여 전자의무기록을 보관하는 기관** **[관련 법령] 보건복지부 고시 「전자의무기록의 관리 보존에 필요한 시설과 장비에 관한 기준」의 [별표] 의료기관 외의 장소에 전자의무기록 보관시 필요한 추가적인 조치**	필수	필수	필수

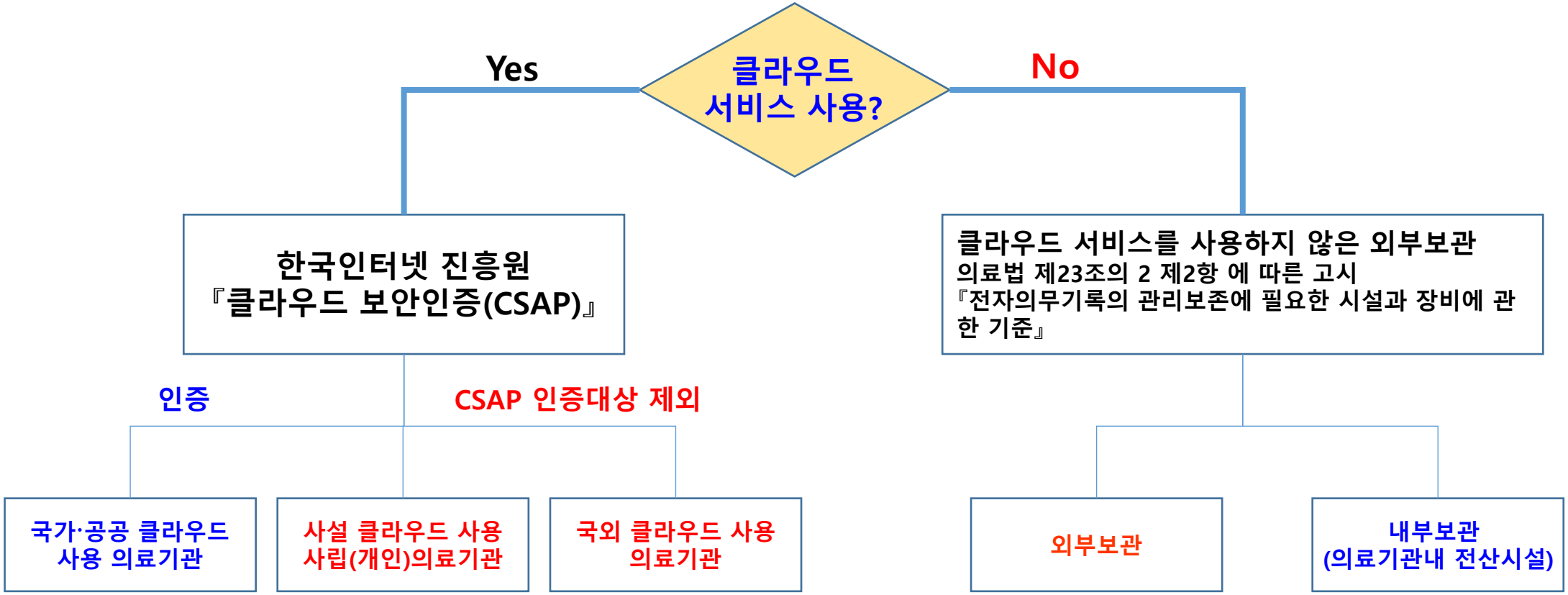
[Issue 1] 전자의무기록시스템 인증기준 변경

[현행] 인증기준 : 보안성 S014 클라우드 서비스 사용 보안 인증

대분류	중분류	번호	인증기준	인증기준 설명	유형 1	유형 2	유형 3
6. 보안성	6.8 외부보관	S014	클라우드 서비스 사용 보안 인증	1. 한국인터넷진흥원의 클라우드 보안인증(CSAP) 인증을 받아야 한다. 2. (시범) 의료데이터 이외의 데이터와 혼재되지 않도록 별도 분리된 의료 데이터전용의 독립 네트워크를 구성할 수 있다. 3. 단, 클라우드 서비스를 사용하지 않은 외부보관의 경우 보건복지부 고시 "전자의무기록의 관리 보존에 필요한 시설과 장비에 관한 기준"에 따라야 한다. [해당 기관] 클라우드 서비스를 사용하여 전자의무기록을 보관하는 기관 [관련 법령] 보건복지부 고시 「전자의무기록의 관리 보존에 필요한 시설과 장비에 관한 기준」의 [별표] 의료기관 외의 장소에 전자의무기록 보관시 필요한 추가적인 조치	필수	필수	필수

[Issue 1] 전자의무기록시스템 인증기준 변경

[문제점] 인증기준 : 보안성 S014 클라우드 서비스 사용 보안 인증)



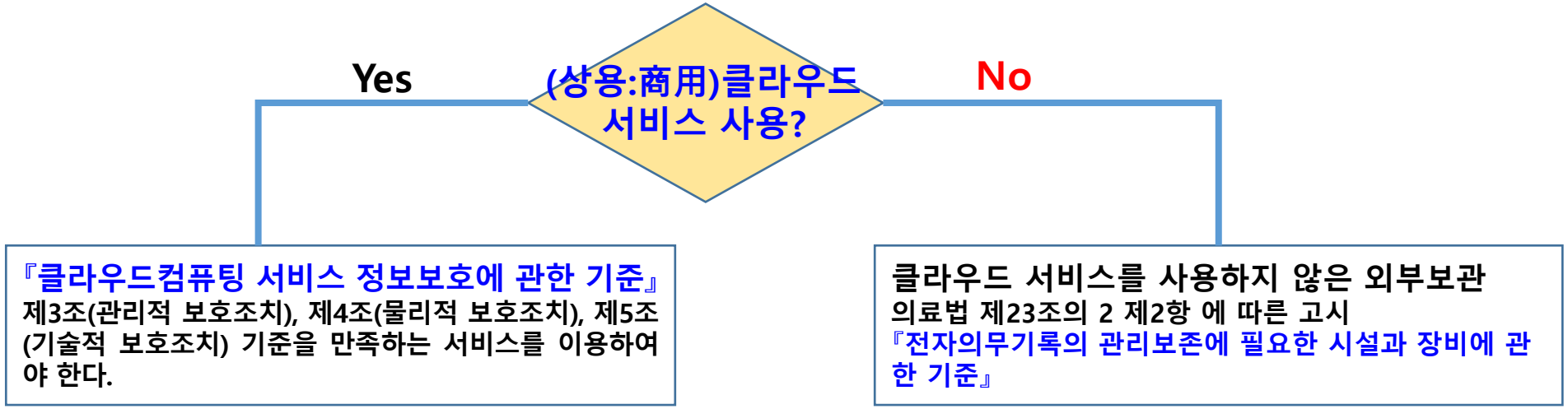
[Issue 1] 전자의무기록시스템 인증기준 변경

[변경] 인증기준 : 보안성 S014 클라우드 서비스 사용 보안 인증

대분류	중분류	번호	인증기준	인증기준 설명	유형 1	유형 2	유형 3
6. 보안성	6.8 외부보관	S014	클라우드 서비스 사용 보안 인증	1.『의료법』 제23조의2(전자의무록의 표준화 등) 제2항에 따른 보건복지부 고시 『전자의무기록의 관리 보존에 필요한 시설과 장비에 관한 기준』과 동 기준 [별표] **『의료기관 외의 장소에 전자의무기록 보관시 필요한 추가적인 조치』**를 준수하는 서비스를 이용하여야 한다. 2.『클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률』 제23조 (신뢰성 향상) 제2항에 따른 과기부 고시 **『클라우드컴퓨팅 서비스 정보보호에 관한 기준』** 제3조(관리적 보호조치), 제4조(물리적 보호조치), 제5조(기술적 보호조치) 기준을 만족하는 서비스를 이용하여야 한다. - **단 국가·공공 의료기관은 한국인터넷진흥원의 CSAP 인증을 받은 서비스를 이용하여야 한다.** 3. (시범) 의료데이터 이외의 데이터와 혼재되지 않도록 별도 분리된 의료 데이터전용의 독립 네트워크를 구성할 수 있다. [관련 법령] 의료법 제23조의2, 같은 조 제4항 및 같은법 시행규칙 제16조, 보건복지부 고시 『전자의무기록의 관리 보존에 필요한 시설과 장비에 관한 기준』 클라우드 컴퓨팅법 제23조 제2항, 과기부 고시 『클라우드컴퓨팅 서비스 정보보호에 관한 기준』	필수	필수	필수

[Issue 1] 전자의무기록시스템 인증기준 변경

[변경] 인증기준 : 보안성 S014 클라우드 서비스 사용 보안 인증)



단) 국가·공공 의료기관은 한국인터넷진흥원의 CSAP 인증을 받은 서비스를 이용하여야 한다.

[S014 심사제외 대상]

내부보관 (의료기관내 전산시설)

① 의료기관내 전산시설 운영
② 의료원 산하 의료기관 서비스
③ 국가, 공공기관 산하 공공의료기관 서비스

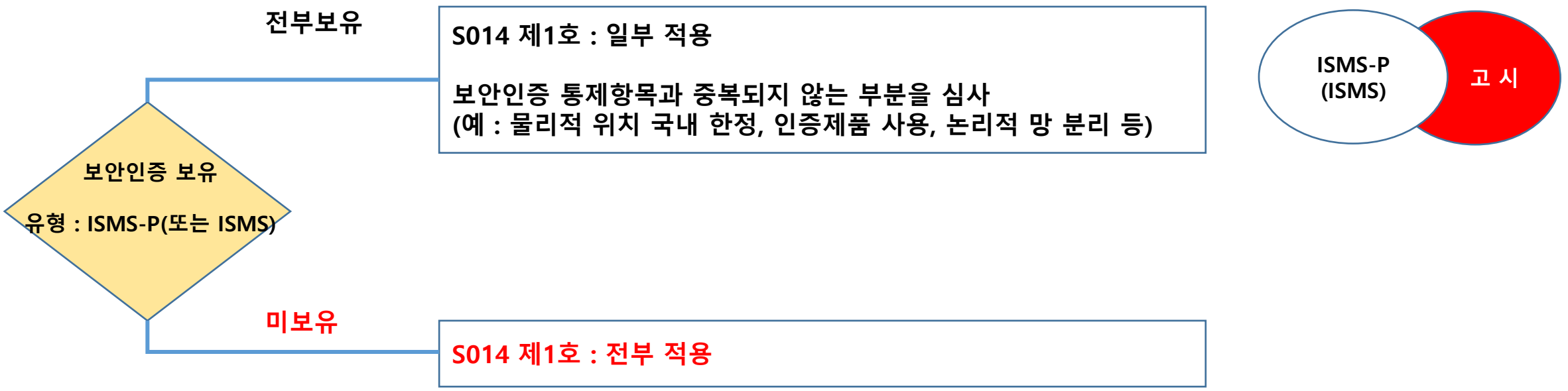
『클라우딩컴퓨팅 발전 및 이용자 보호에 관한 법률』
제2조(정의) 1. "클라우드컴퓨팅"(Cloud Computing)이란 집적·공유된 정보통신기기, 정보통신설비, 소프트웨어 등 정보통신자원(이하 " 정보통신자원"이라 한다)을 통하여 신축적으로 이용할 수 있도록 하는 정보처리체계를 말한다.
3. "클라우드컴퓨팅서비스"란 클라우드컴퓨팅을 활용하여 상용(商用)으로 타인에게 정보통신자원을 제공하는 서비스로서 대통령령으로 정하는 것을 말한다.

[Issue 1] 전자의무기록시스템 인증기준 변경

[EMR 인증심사 "보안인증 별" 적용사항]

① S014 제1호 : 단순 외부보관

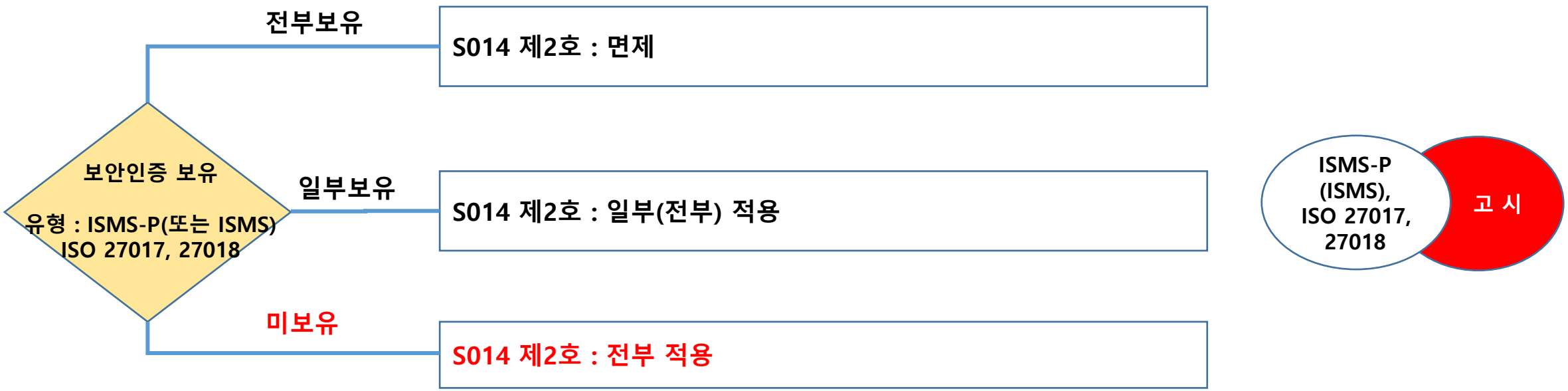
1.『의료법』 제23조의2(전자의무록의 표준화 등) 제2항에 따른 보건복지부 고시 **『전자의무기록의 관리 보존에 필요한 시설과 장비에 관한 기준』**과 동 기준 [별표]『의료기관 외의 장소에 전자의무기록 보관시 필요한 추가적인 조치』를 준수하는 서비스를 이용하여야 한다.



[Issue 1] 전자의무기록시스템 인증기준 변경

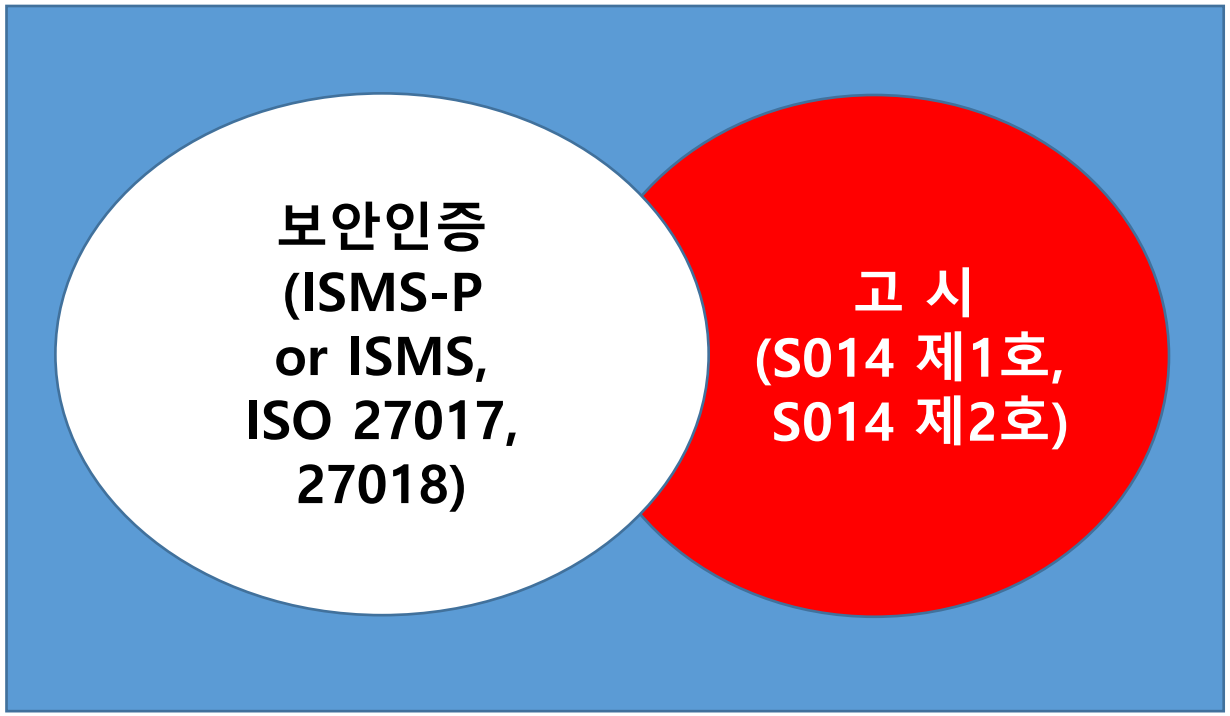
[EMR 인증심사 "보안인증 별" 적용사항]

② S014 제2호 : 클라우드 기반 외부보관
2.『클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률』제23조 (신뢰성 향상) 제2항에 따른 과기부 고시 **『클라우드컴퓨팅 서비스 정보보호에 관한 기준』** 제3조(관리적 보호조치), 제4조(물리적 보호조치), 제5조(기술적 보호조치) 기준을 만족하는 서비스를 이용하여야 한다.
- 단 국가·공공 의료기관은 한국인터넷진흥원의 CSAP 인증을 받은 서비스를 이용하여야 한다.



[Issue 1] 전자의무기록시스템 인증기준 변경

[EMR 인증심사 외부보관 적용사항]



+

취약점 점검

[취약점 점검]

- 자체점검 계획수립
- 취약점 점검
- 모의침투 테스트

⇩

취약점 도출 및 개선

⇩

보완조치 여부 확인

⇩

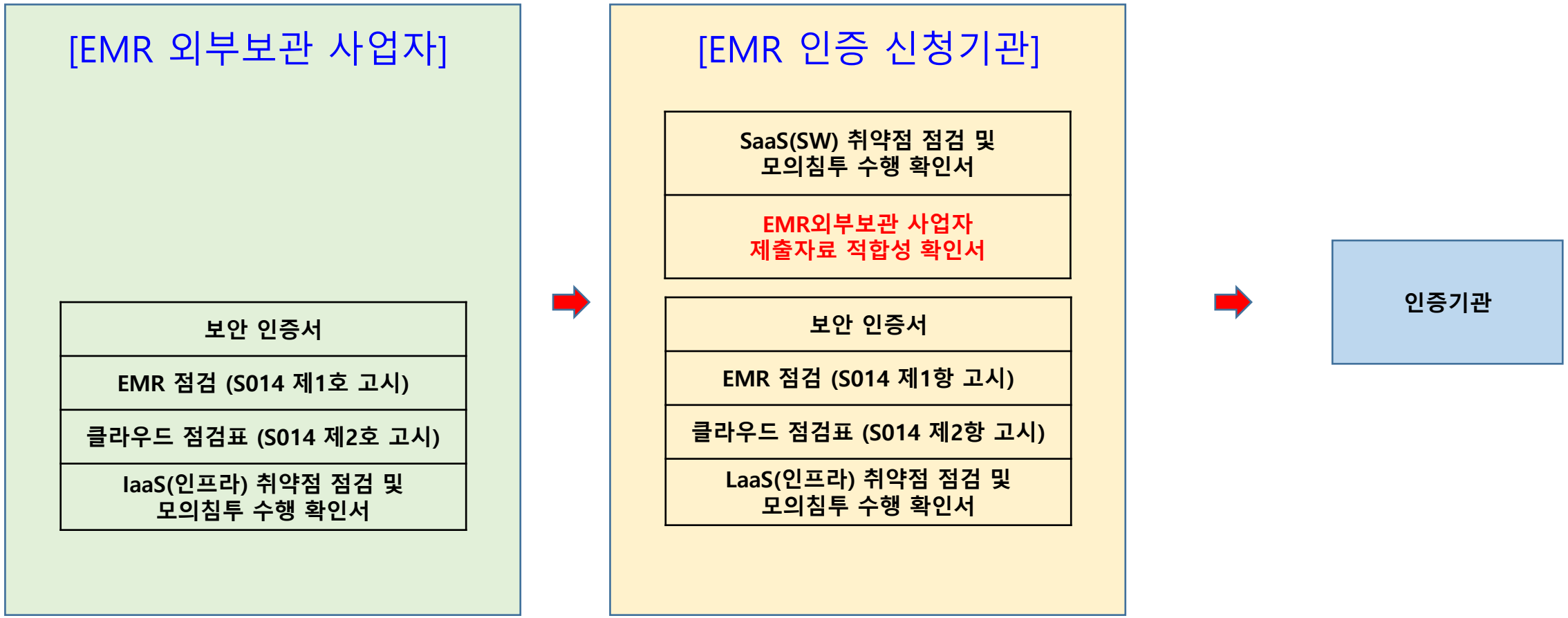
취약점 점검 등
수행 확인서 제출
(점검내역은 미제출)

[취약점 점검 및 모의침투 테스트 도입취지]

『클라우드컴퓨팅서비스 정보보호에 관한 기준 고시』
[별표1] 관리적 보호조치 3.3.2(취약점 점검) 취약점 점검 정책에 따라 주기적으로 기술적 취약점을 점검하고 보완하여야 한다.
"모의침투 테스트"는 한국인터넷진흥원의 클라우드 보안인증(CSAP)에서 준용

[Issue 1] 전자의무기록시스템 인증기준 변경

[신청 기관별 제출자료]



[Issue 1] 전자의무기록시스템 인증기준 변경

[일부 인증기준 항목에 대한 심사 면제]

타 인증제 · 사업			EMR 인증제 (제품인증)	
주관기관	인증 프로그램 · 사업	대상	면제대상	면제 인증기준
사회보장 정보원	진료정보교류사업	의료기관	개발업체, 자체개발 의료기관	I001-I010 상호운영성 인증기준 전체
한국인터넷진흥원	정보보호관리체계(ISMS)	의료기관	자체개발 의료기관	S009,S012,S014를 제외한 보안성 인증기준 전체
	정보보호 및 개인정보보호 관리체계(ISMS-P)	의료기관	자체개발 의료기관	S012,S014를 제외한 보안성 인증기준 전체
	ISMS-P(또는 ISMS), 클라우드서비스 보안인증 (CSAP)	집적정보통신 시설 사업자, 클라우드서비스 제공업체	개발업체	S014 제1호 일부, 제2호 전부
ISO	ISO 27017 (ISO 클라우드 보안인증) ISO 27018 (ISO 클라우드 개인정보보 호인증)			
건강보험 심사평가원	청구소프트웨어 보안기능 검사인증	개발업체, 자체개발 의료기관	개발업체, 자체개발 의료기관	S008,S009,S012,S014를 제외한 보안성 인증기준 전체

[Issue 1] 전자의무기록시스템 인증기준 변경

[국내/국외 클라우드 업체별 정보보안 인증 취득 현황]

클라우드 서비스 제공자 (CSP)	ISMS-P (ISMS)	ISO 27017	ISO 27018
AmaZon	보유	보유	보유
MicroSoFt	보유	보유	보유
Google	보유	보유	보유
Oracle	보유	보유	보유
IBM	보유	보유	보유
네이버	보유	보유	보유
KT	보유	보유	보유
NHN	보유	보유	보유

출처: 각 클라우드 업체별 공식 홈페이지, https://isms.kisa.or.kr/

[Issue 2] 의료장비 데이터 보안

[Issue 2] 의료장비 데이터 보안

1. 랜섬웨어 피해사례

Dailymedi
보건의료문화를 선도하는 데일리메디

전자의무기록(EMR) 병·의원 '랜섬웨어' 공격 빈발

부산·수도권 등 잇따라 발생, 환자 개인정보·상담내용 유출되면 치명적

[2021년 06월 10일 04시 53분]

현재 대다수 병원에 정보시스템이 도입되고 있는 가운데 '랜섬웨어' 공격 등으로 환자 개인정보 및 상담 내역 등이 유출되는 사례가 발생하고 있다.

악성 프로그램인 랜섬웨어는 몸값(Ransom)과 제품(Ware)의 합성어로, 문서·사진 파일 등을 암호화시킨 후 돈을 요구한다고 해서 붙여진 이름이다.

9일 관련 업계에 따르면 최근 부산 소재 某여성의원이 랜섬웨어 공격 피해를 입어 환자들의 개인정보가 유출·공개됐다. 이어 서울·경기 등에 지점을 보유한 某피부과도 개인정보·상담 내용 등 내부 데이터가 유출된 것으로 알려졌다.

지난달에는 강남 유명 성형외과가 이 같은 피해를 입고 해킹 조직이 병원 고객들에게 직접 연락을 취한 사실까지 드러나며 충격을 안겼다.

한국인터넷진흥원(KISA)이 지난해 발표한 '2021년 사이버위협 전망' 보고서에 의하면 랜섬웨어는 국·내외 공통으로 올해 가장 주목해야 할 위협으로 꼽혔다.

앞서 지난해 9월 독일의 한 대학병원에서는 랜섬웨어 공격으로 병원시스템이 일시 마비돼 긴급 이송 중이던 환자가 사망한 사건이 발생하기도 했다.

병원 정보 해킹 피해로 인한 개인정보 유출을 넘어 환자의 생명까지 앗아가는 치명적인 사례도 방심할 수 없게 된 셈이다. 이에 병원 내 EMR 등 보안을 강화해야 한다는 지적이 나온다.

실제 의료기관이 보안사고에 대응시 △상급종합병원 59.5% △300병상 이상 종합병원 53.6% △300병상 미만 종합병원 55.5%△병원 59.6%가 '보안 기술 같은 전문성 미흡' 문제로 어려움을 겪었다.

KISA는 사이버위협 전망 보고서에서 "최신 보안 업데이트 조치, 출처 불명확한 이메일·URL 링크 실행 주의, 백업 체계 구축 및 보안성 강화 등의 관리가 요망된다"고 조언했다.

포용적 복지을 실현하는 정보 플랫폼 선도기관

SSIS 한 국 사 회 보 장 정 보 원

수신 수신자 참조

(경유)

제목 (긴급) 의료기관 랜섬웨어 공격 주의 권고에 따른 정보공유 협조 요청

1. 귀 협회의 무궁한 발전을 기원합니다.

2. 한국사회보장정보원은 보건복지부로부터 의료법 시행규칙 제16조4(진료정보 침해사고의 예방 및 대응을 위한 업무의 위탁)에 의거 진료정보침해대응센터를 위탁 받아 운영하고 있습니다.

3. 최근 국내 의료기관 대상으로 랜섬웨어 공격이 지속적으로 발생하고 있습니다. 인터폴(국제형사경찰기구)에서도 국내 중요시설 및 병원에 대한 랜섬웨어 공격에 주의를 당부하는 권고문이 접수되어 협부로 공지합니다. 귀 협회에서는 회원(회원사) 대상으로 관련 내용을 공지하여 랜섬웨어에 대비할 수 있도록 조치하여 주시기 바랍니다.

가. 요청사항 : 회원(회원사) 공문발송 및 홈페이지 공지글 게시
나. 시행시점 : 긴급사항으로 즉시 시행

붙임 20210623 (긴급)의료기관 랜섬웨어 주의 권고. 끝.

한 국 사 회 보 장 정 보 원 장

수신자 대한병원협회, 대한의사협회, 대한한의사협회, 대한치과의사협회, 대한병원정보협회, 대한병원정보보안협의회

[Issue 2] 의료장비 데이터 보안

2. 랜섬웨어 피해 영역

PC 영역	의료장비 영역	스캔 이미지(파일) : 진료기록, 전자동의서 등
		
- (외장)하드디스크 - 공유폴더 -> 사용자 자료 영향	- (외장)하드디스크 - 공유폴더 - NAS(Network-Attached Storage) -> 사용 진료과에 영향 -> 백업 안함(수년간의 검사자료 날릴 위험 있음)	- 통합 디스크 -> 전체 진료에 직접적 영향
사용부서 : 전 부서 관리부서 : 개인 사용자	사용부서 : 각 진료과 관리부서 : 의공학팀	사용부서 : 전 진료과 관리부서 : 의료정보팀

[Issue 2] 의료장비 데이터 보안

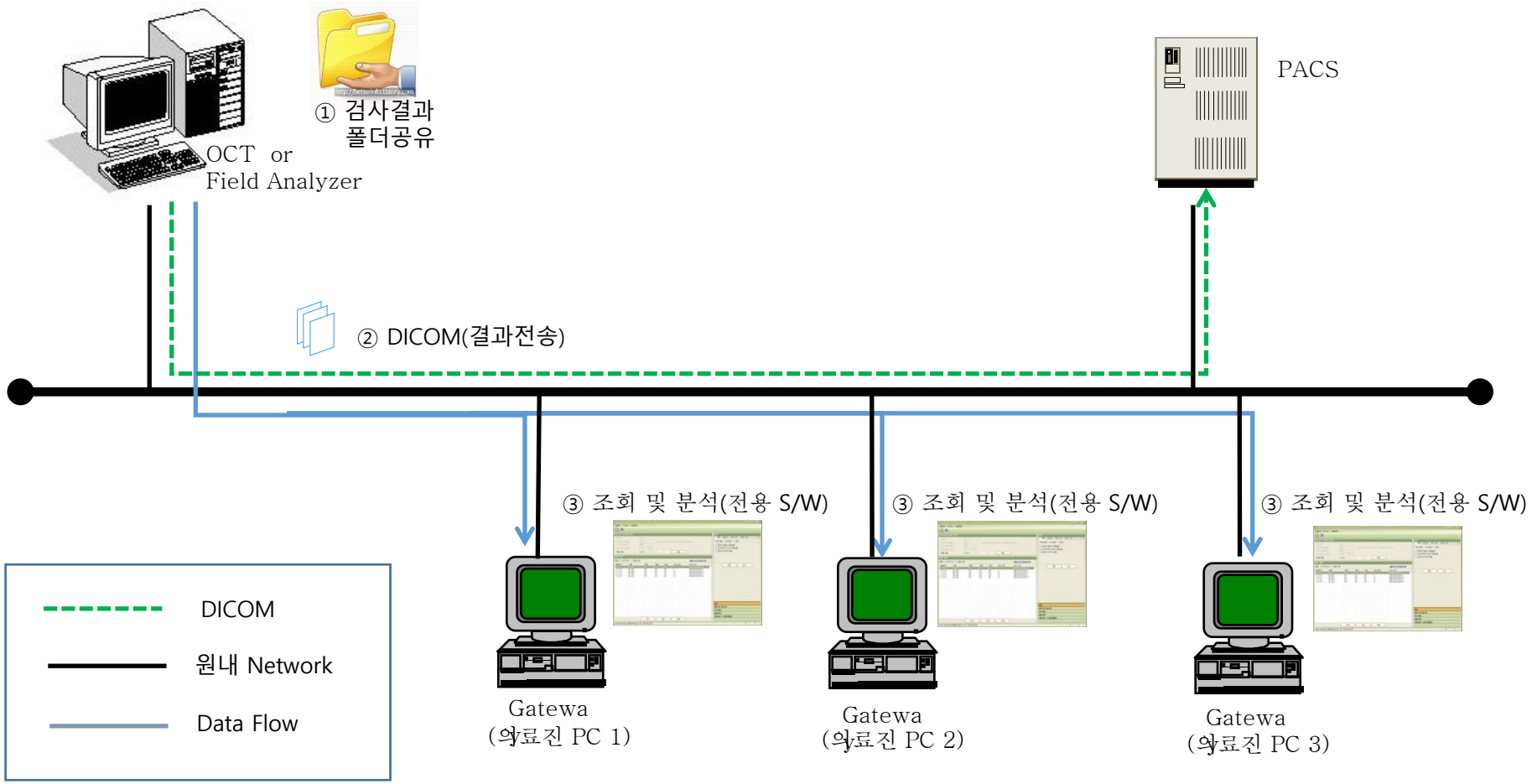
3. 의료장비의 보안 취약점

Case) 안과 OCT & Field Analyzer Data Flow

직접 연결

File 공유 / Data Export

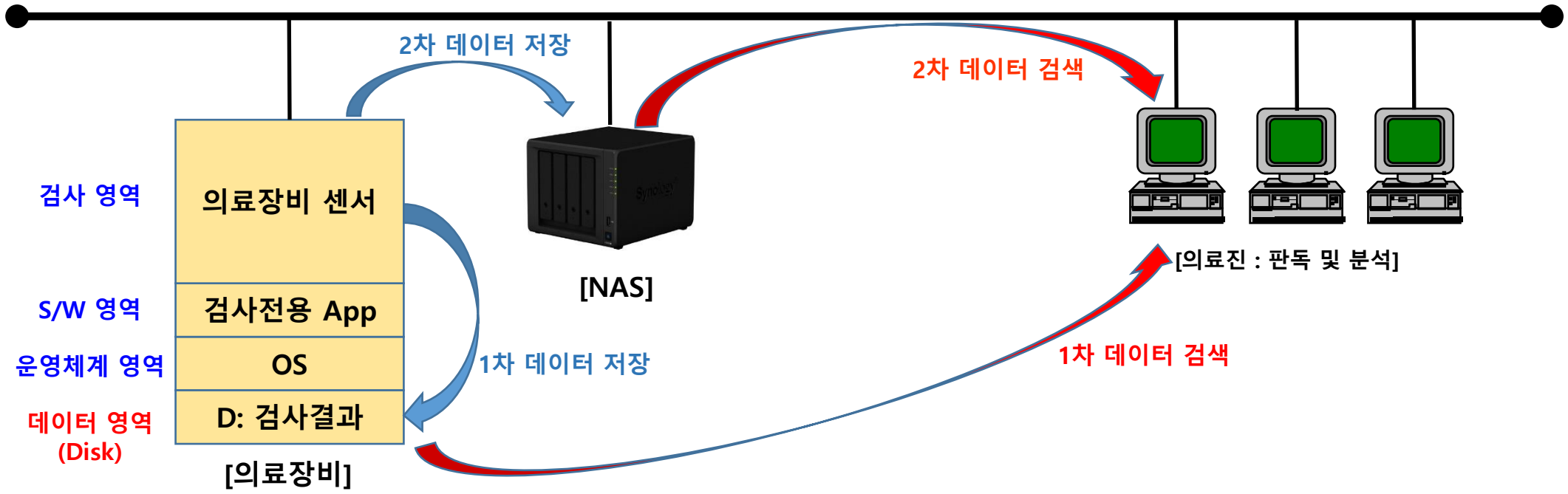
DICOM



[Issue 2] 의료장비 데이터 보안

3. 의료장비의 보안 취약점

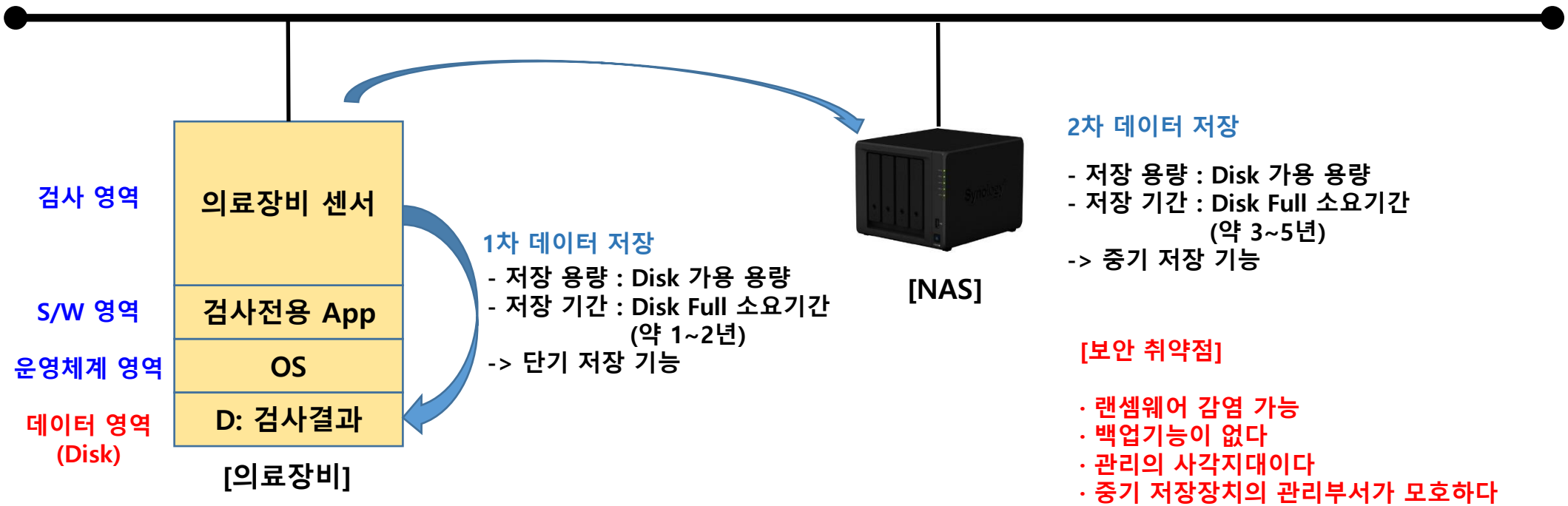
Case) 안과 OCT & Field Analyzer Data Flow : 데이터 저장구조



[Issue 2] 의료장비 데이터 보안

3. 의료장비의 보안 취약점

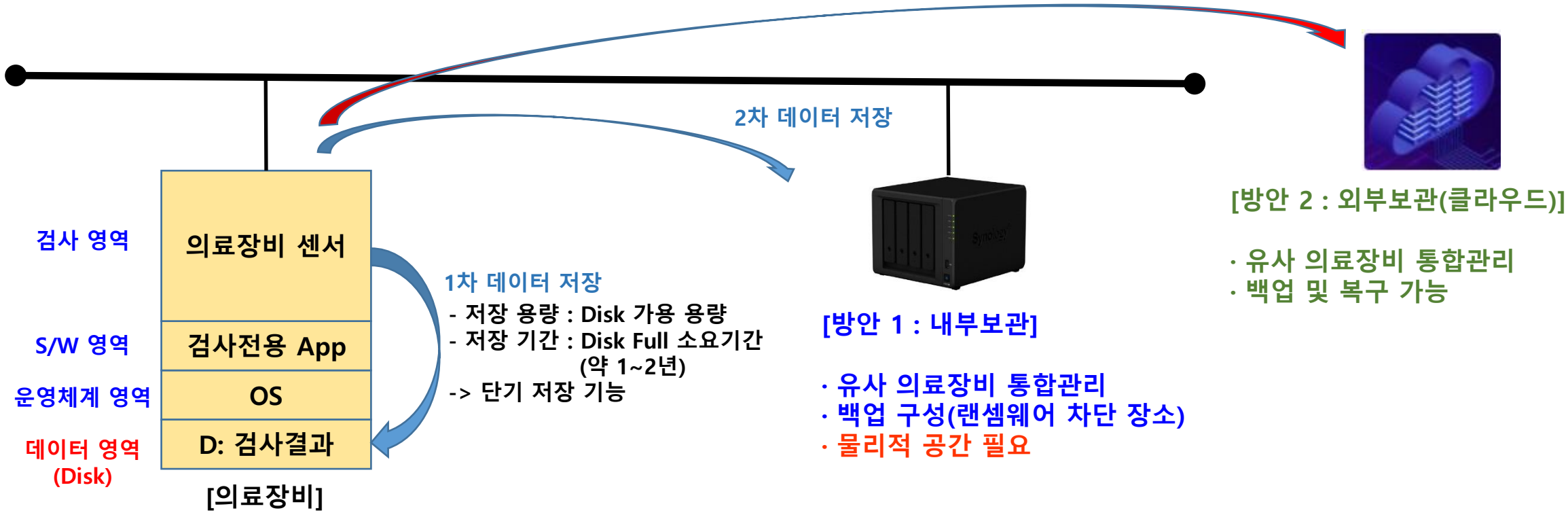
Case) 안과 OCT & Field Analyzer Data Flow : 데이터 저장구조



[Issue 2] 의료장비 데이터 보안

4. 의료장비의 보안의 대안

Case) 안과 OCT & Field Analyzer Data Flow : 데이터 저장구조




Thank
You