개인정보보호를 위한 의료기관의 기술적 보안 방안

2008. 4. 25.

정보보호연구본부 김신효

ETRI

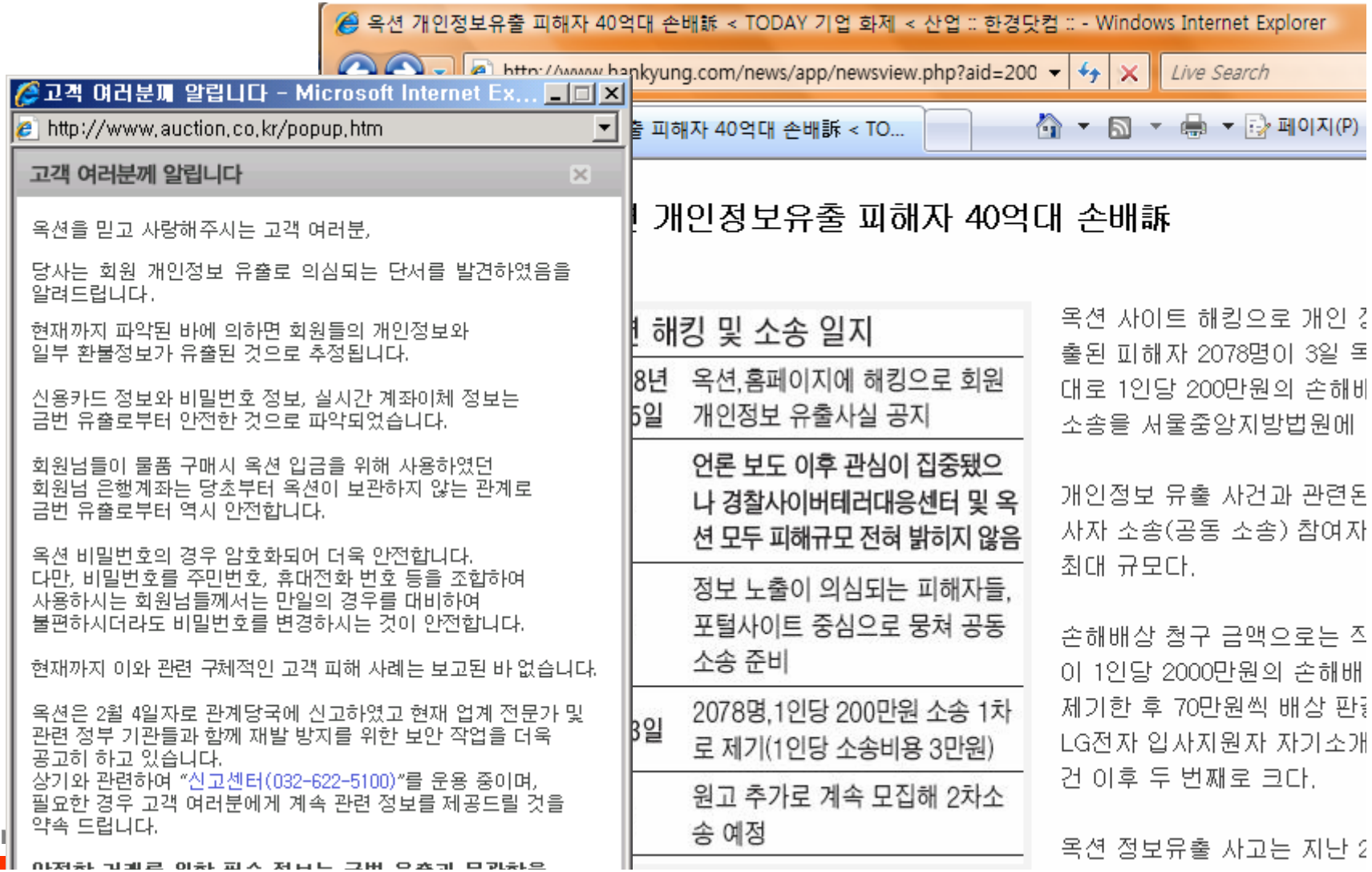
목 차

- 개인정보(프라이버시) 보호
  - 개인정보 유출 사례
  - 개인 의료정보 보호 이슈
- 기술적 보안 방안
- 의료기관 보안 현황 분석 및 시사점
  - 정보자산 보호의 필요성
  - 의료기관의 보안현황 분석
  - 시사점
- 의료정보보호 표준화
- 결론

개인정보 (프라이버시) 보호

개인정보 유출 사례

서비스사업자의 DB 개인정보 유출 사례



인터넷뱅킹-개인정보 유출 사례

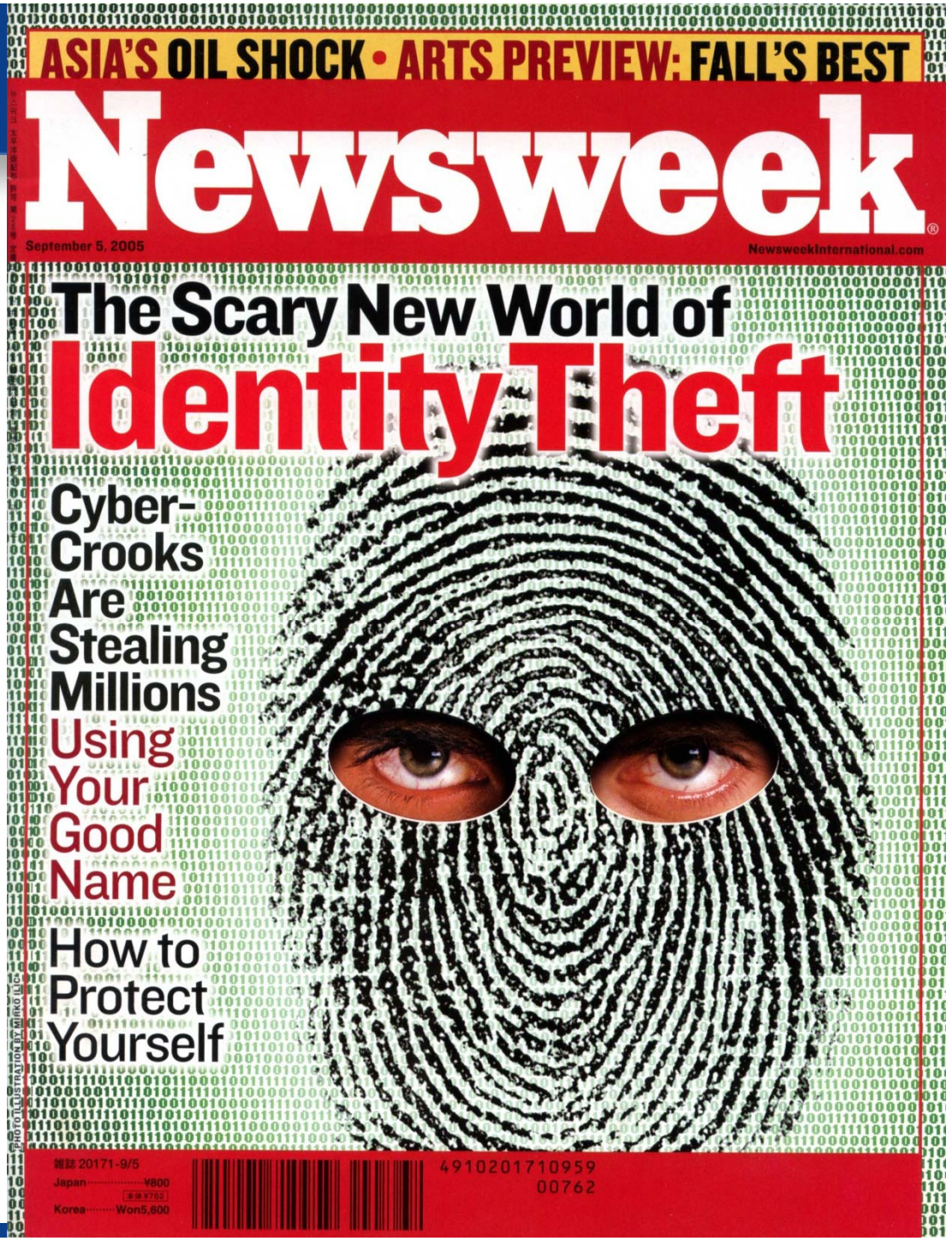
http://hani.co.kr/section-005000000/2005/06/005000000200506031909279.html

- 피싱(phishing)
  - 개인 정보(private data)를 낚시질(fishing)하듯이 빼냄
  - ’ 패스워드를 변경해주십시오. …. 응답하지 않으면 계좌가 정지됩니다. 첨부내역을 확인해주십시오’ 등의 메시지와 실제 사이트와 똑같은 모습으로 위장된 홈페이지 링크를 보내서 사용자가 클릭하도록 유도
- 파밍(pharming)
  - 사용자 컴퓨터에 트로이목마 해킹 프로그램을 심어서 은행의 공식 사이트가 아닌 해커가 만든 위장 사이트로 이동하도록 유도
- 웹 메일에 공인인증서를 올려두는 경우
  - 대부분의 사람이 포털과 메일 등 각종 사이트의 ID와 비밀번호를 동일하게 사용한다는 점을 이용

ID Theft:
A National
Security
Threat

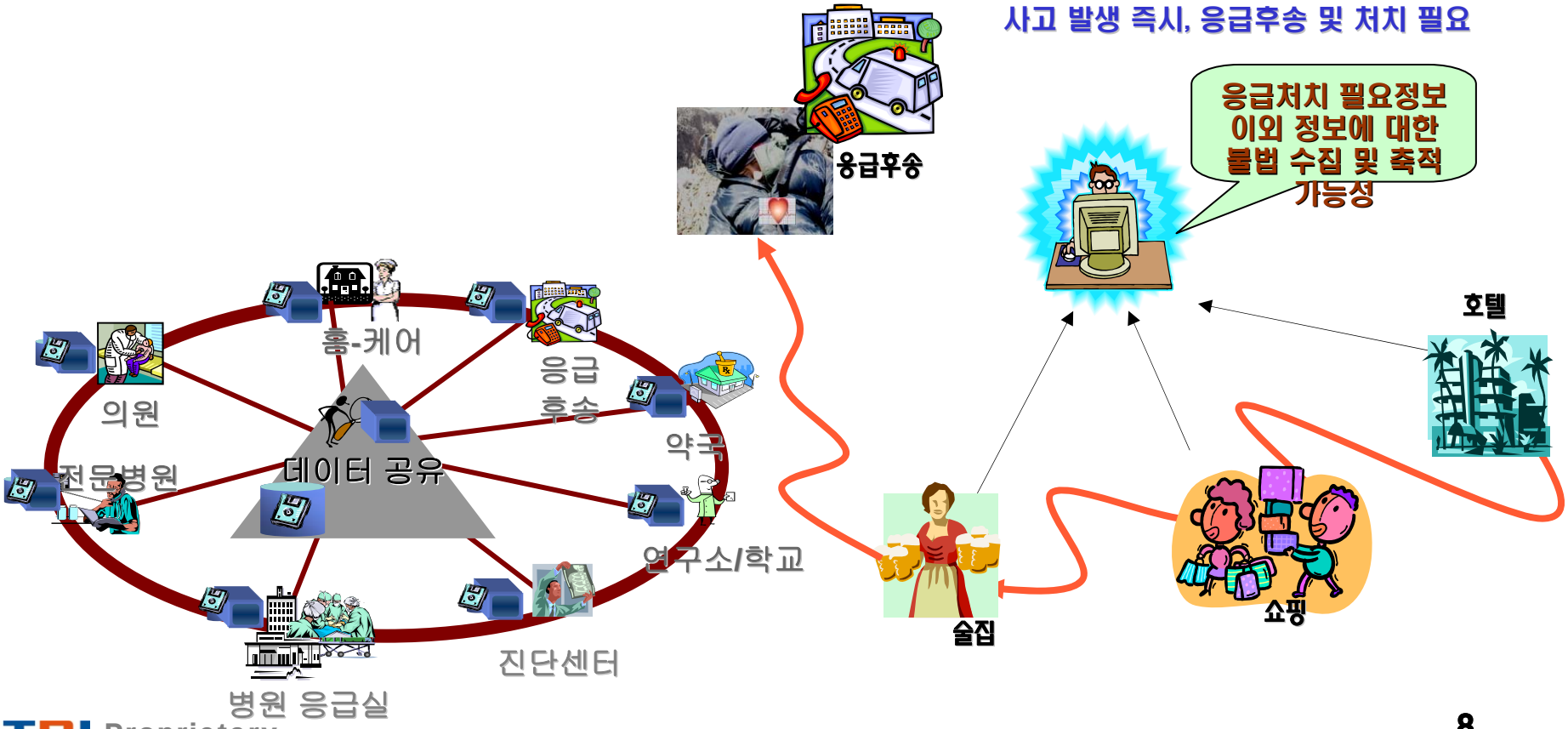
FBI-2006

Bigger problem than drugs…



개인 의료정보 보호 이슈

- 진단에 필요한 특정 기록에 대한 공유만 이루어져야 이상적임
- 불법적 정보 접근 및 활용 가능성



내가 복용하고 있는 약물/처치내용에 대하여 누군가가 알고 있다면??

'의료 정보 활용' vs '개인 정보 보호'

- 의료 정보의 활용
  - 환자 건강정보에 대한 알 권리(Need-to-Know)
  - 위급 상황 및 보다 나은 의료 서비스를 위에서는 개인 정보(신원확인)를 제공하여야 한다.
- 개인 정보 보호
  - 극히 개인적인 정보에 대하여 알려주고 싶지 않다.
  - 정보 공유가 목적에 맞게 이루어지고 있는지 개인(공유정보 대상자)은 알 수 없다

HIPAA PHI

- **보호 대상 건강 정보**(Protected Health Information)
  - **의료기록와 함께 보호되어야 할 모든 개인 정보**
  - **직.간접적으로 특정 개인을 인지 할 수 있는 정보**
    - **과거, 현재 또는 미래의 육체적, 정신적 건강 또는 상태 및 해당 의료 보건 서비스**
    - **이름이나 번호 등 개인의 신분을 밝힐 수 있는 정보, 신상정보**
    - **의료정보, 치료비**
    - **환자가 우리 병원에서 치료를 받는다는 사실**
  - Privacy Rule's De-identification
    - **이름, 거주지, 지역, 전화, 팩스 번호, 이메일, 웹 페이지 주소,** IP **주소,** Social Security Number, **계좌번호, 의료기록부 번호, 건강보험번호, 증명서/자격증 번호, 자동차 번호, 기계 등록 번호, 얼굴전체 이미지나 사진, 생물 측정 인식사항 (예:** DNA), **다른 어떤 개인만의 특이사항 (예: 점, 상처..) 등의 개인인식 사항을 제거하도록 조치함.**

개인정보보호 취급단계 및 침해요소

*KISA 발표자료 참조

개인 의료 정보 보호 규정

국내 의료 정보보호 관련 규정

조항	내용
개인보건의료정보의 수집, 처리, 이용 및 제공 등	동의에 의한 수집, 수집 시 고지의무, 개인보건의료정보 수집의 제한, 개인보건의료정보의 처리, 이용 및 제공, 연구목적에 의한 개인보건의료정보의 처리, 이용 및 제공, 개인보건의료정보의 파기
정보주체의 권리	자기결정권, 개인보건의료정보에 대한 접근 권리, 개인보건의료정보에 대한 수정 요청의 권리, 제3자 제공 내역서를 받을 권리, 제한 요청의 권리, 비밀 의사소통 요청의 권리, 동의철회의 권리
보건의료정보취급자의 의무	보건의료정보취급자의 책임, 개인보건의료정보관리책임자의 지정,개인보건의료정보의 보호조치, 비밀유지, 요청 및 불만의 처리
전자의무기록	전자의무기록의 보존, 전자의무기록의 관리, 보존에 필요한 장비,전자의무기록의 타 기관 전송 등
전자처방전	전자처방전 등의 공개제한
원격의료	비밀누설금지

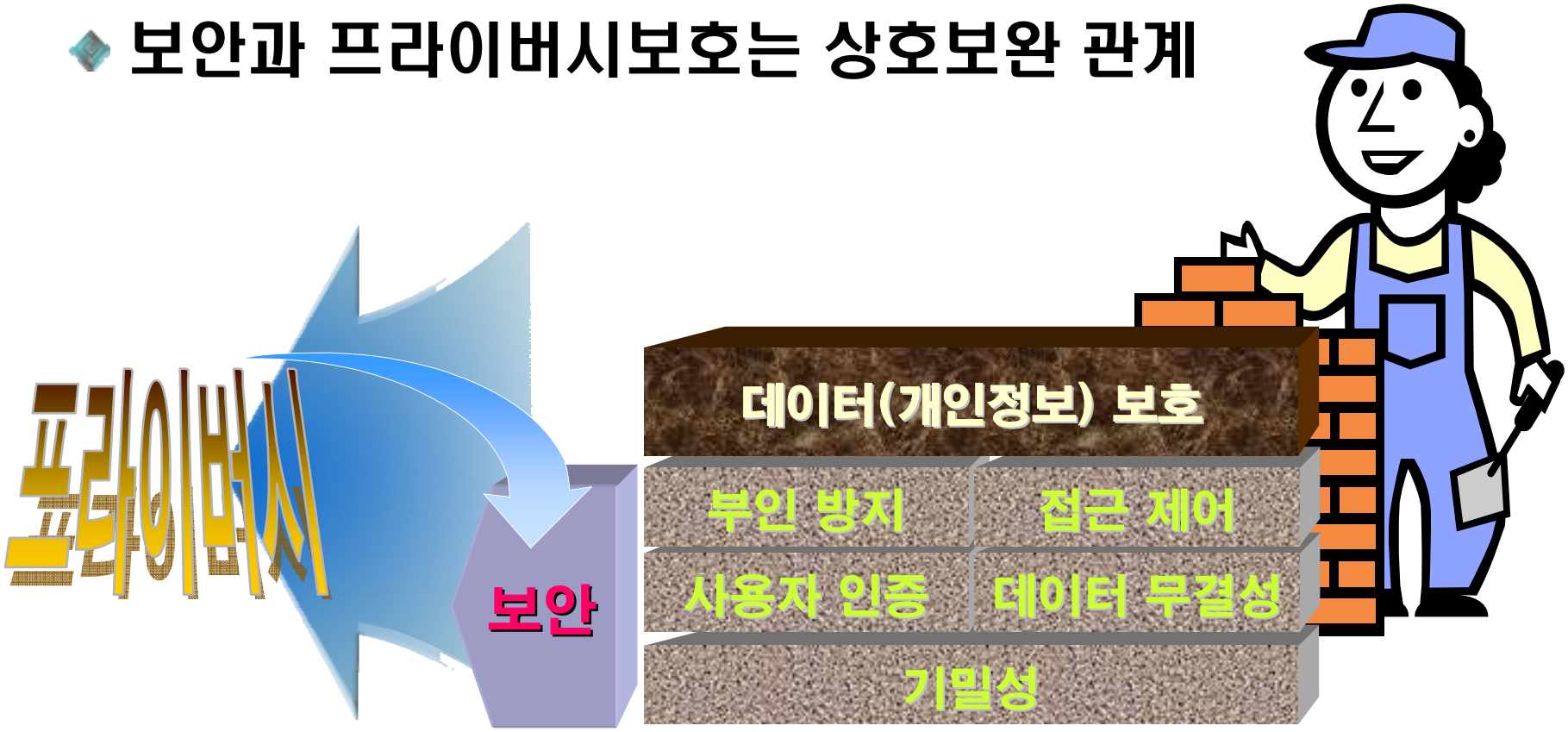
* 국내 e-Health 발전에 따른 정책대응방안 연구 -한국보건사회연구원,2005 자료

건강 정보보호 및 관리 운영에 관한 법률

- 제정 중???
- 반대의견
  - 환자 인권침해의 요소가 있고 현행 의료법과 일부 상충됨
  - Big brother의 등장 -의료정보가 정부 주도로 수집, 정리될 경우

프라이버시와 보안

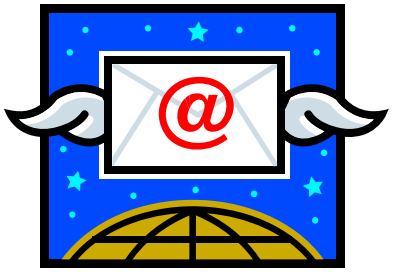
- 프라이버시보호는 보안보다 더 광범위한 의미
- 보안 기술을 바탕으로 프라이버시 실현
- 보안과 프라이버시보호는 상호보완 관계



기술적 보안 방안

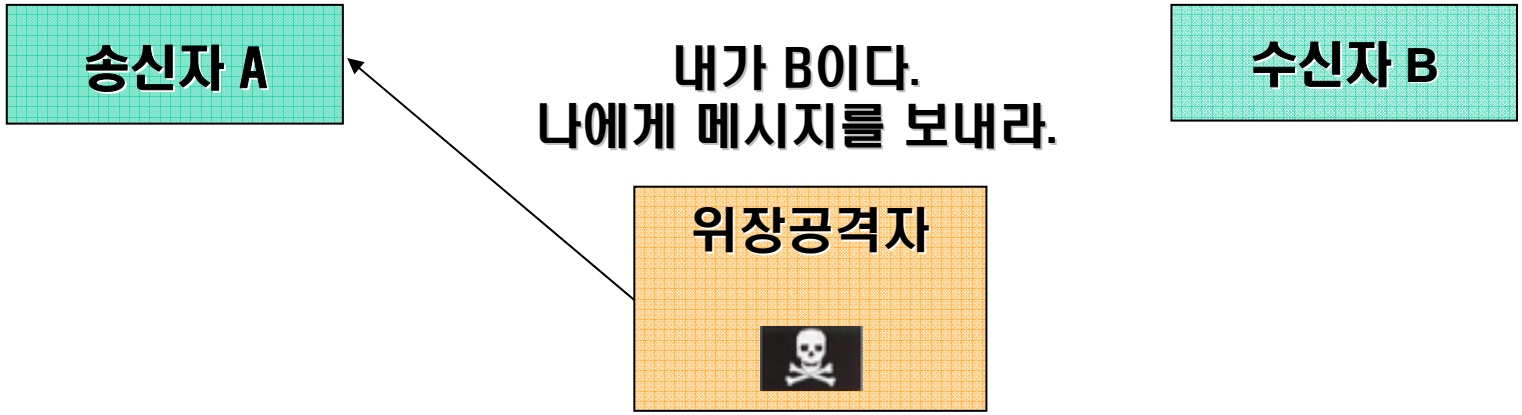
보안 필요성

- 온라인상에서 만난 A와 B 사이의 신뢰 문제?
  - 다른 사람이 내용을 보지 않았는가? (기밀)
  - A가 보낸것은 확실한가? (인증)
  - 내용이 변조되지 않았는가? (무결성)
  - A가 보낸 사실을 부인하지 않을까? (송(수)신 부인)



사용자 인증

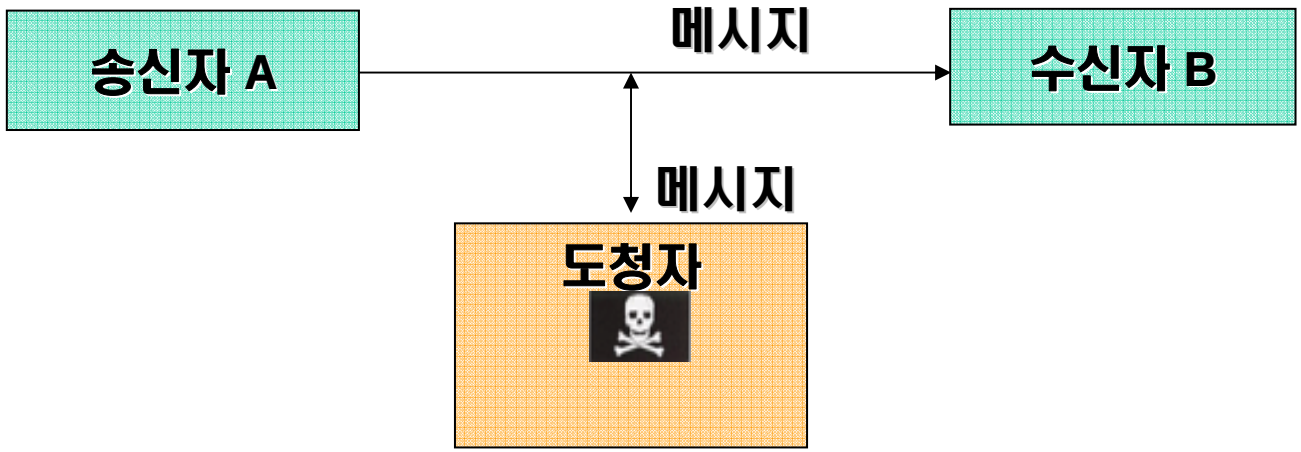
- 내가 B이니 나에게 A의 영상의무기록을 보내라? 진짜 B라는 것을 어떻게 확인하지?
- 위장 방지



➲B임을 증명할 수 있는 증표(인증서, 디지털 서명)를 제시

데이터 기밀성

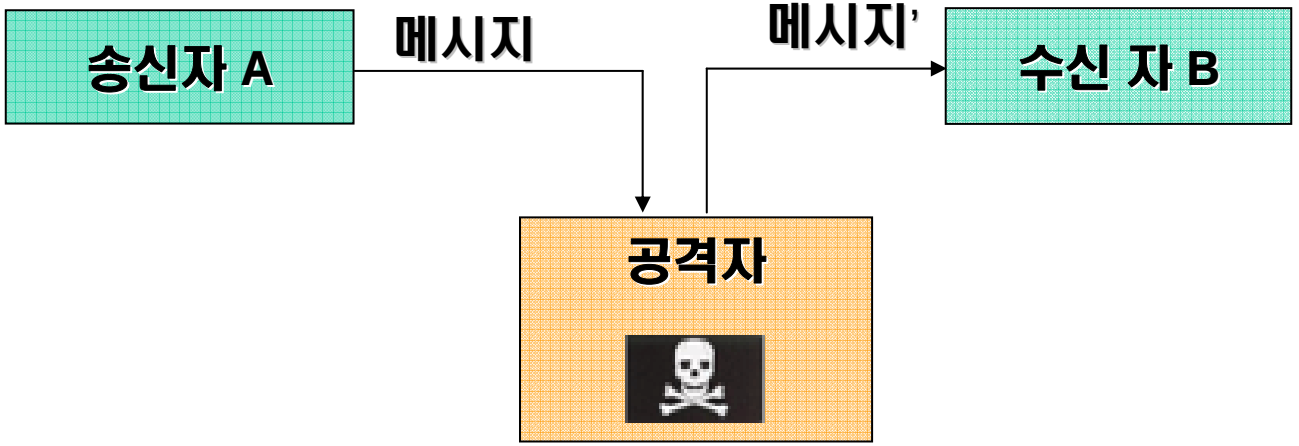
- 누군가가 비밀번호를 엿듣는다면?
- 관리자가 내 비밀번호를 알고 있다면?



- A와 B가 공유하는 값(비밀키)으로 메시지를 암호

데이터 무결성

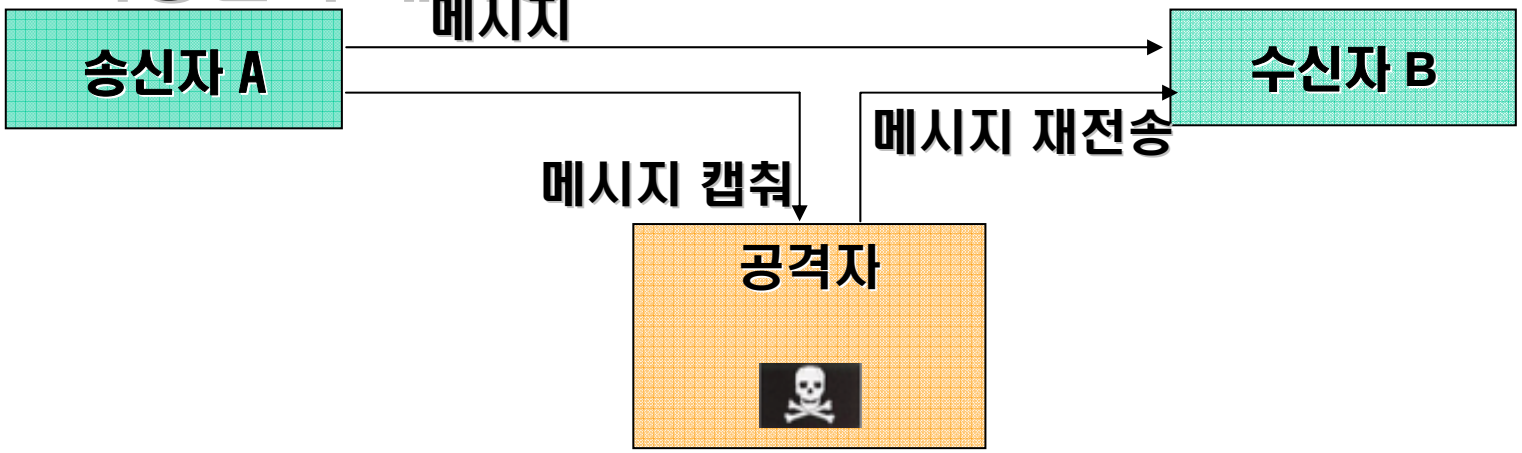
- 영상의무기록이 변경되어 오른쪽 다리에 수술이 필요한 환자에게 왼쪽다리 수술을 한다면?
- 변조 방지



- A는 메시지 변조를 막기 위해 B만 해석가능한 특수값(디지털 서명) 전달
- B는 메지지와 특수값이 일치하는지 확인(서명 검증)

부인 방지 및 재사용(replay) 방지

- A는 투약지시서를 보냈는데 B는 안받았다고 한다면?
- 한번 보낸 투약지시서를 중복으로 재사용된다면?
- 처방전의 재사용?



➲A가 보낸것을 제3자에게 위탁해 놓는다.(내용증명)

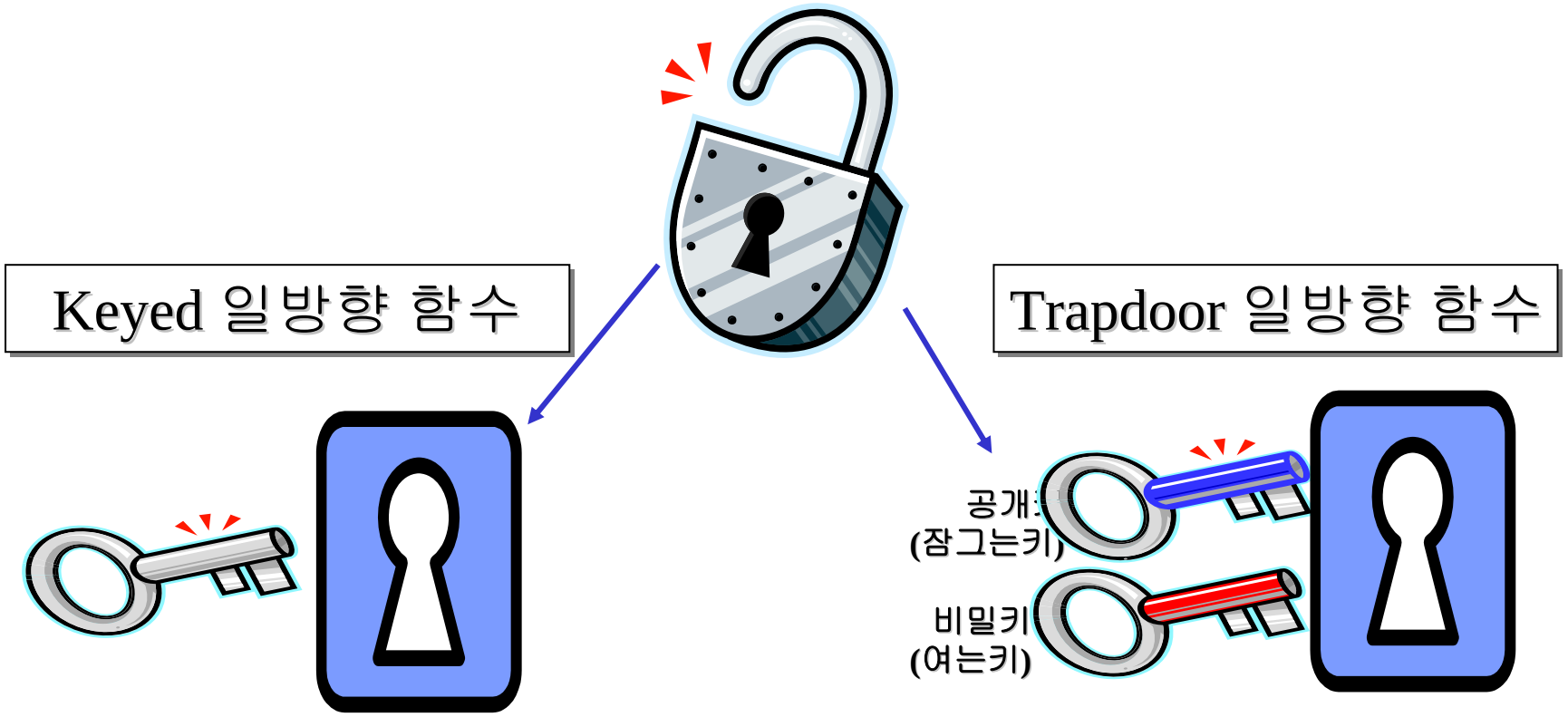
➲메시지 송신 시각(또는 유효기간)까지 보낸다.

암호 알고리즘

- 평문을 뒤섞어서 해석 불가능한 암호문으로(암호화), 또는 암호문을 평문으로(복호화) 변환하는 규칙

- 변환시 사용되는 변수(정보)를 "키"라 함
- 키 공유 방법에 따라 비밀키 암호와 공개키 암호로 구분
  - 비밀키 암호: 송수신자가 별도의 안전한 방법으로 암호키를 공유
  - 공개키 암호: 암호화는 상대방의 공개키를 사용하고, 복호화는 자신의 비밀키를 사용

비밀키 vs. 공개키 암호 (1)



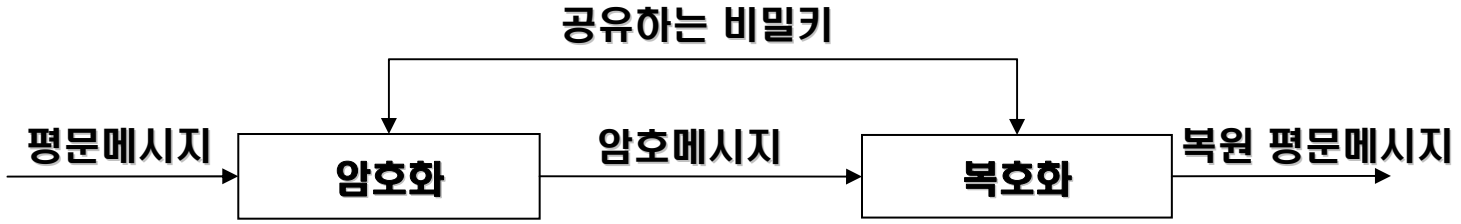
(비밀키 암호)

공개키 암호

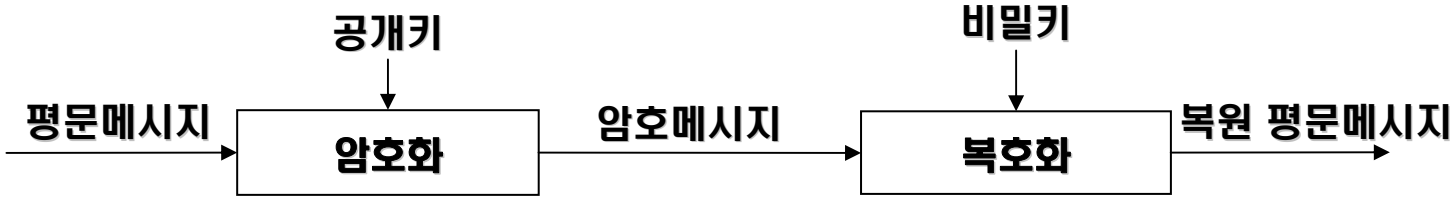
- **수학적으로 증명된 일방향 함수** (one-way function)
  A -> B and B->A
  A(평문)에 대해, B(암호문)를 계산하는 것은 용이하나
  이미 주어진 B로 부터 A를 계산하는 것은 계산상 불가능한 함수

비밀키 vs. 공개키 암호 (2)

- 비밀키(대칭키) 암호
  - 동일한 비밀키를 송신/수신자가 공유함
  - 별도의 비밀키 전달 경로 필요



- 공개키(비대칭키) 암호
  - 키생성시 공개/비밀키 쌍을 생성
  - 수신자의 공개키로 암호, 수신자의 비밀키로 복호
  - 비밀키가 네트워크로 전송되지 않음



공개키 기반의 전자서명

- 디지털 서명 : 공개키 암호의 역변환, 즉 암호알고리즘으로 암호 및 서명 가능
  - 공개키로 암호화, 비밀키로 복호화

  - 비밀키로 서명, 공개키로 서명 검증

전자서명의 정보보호 기능

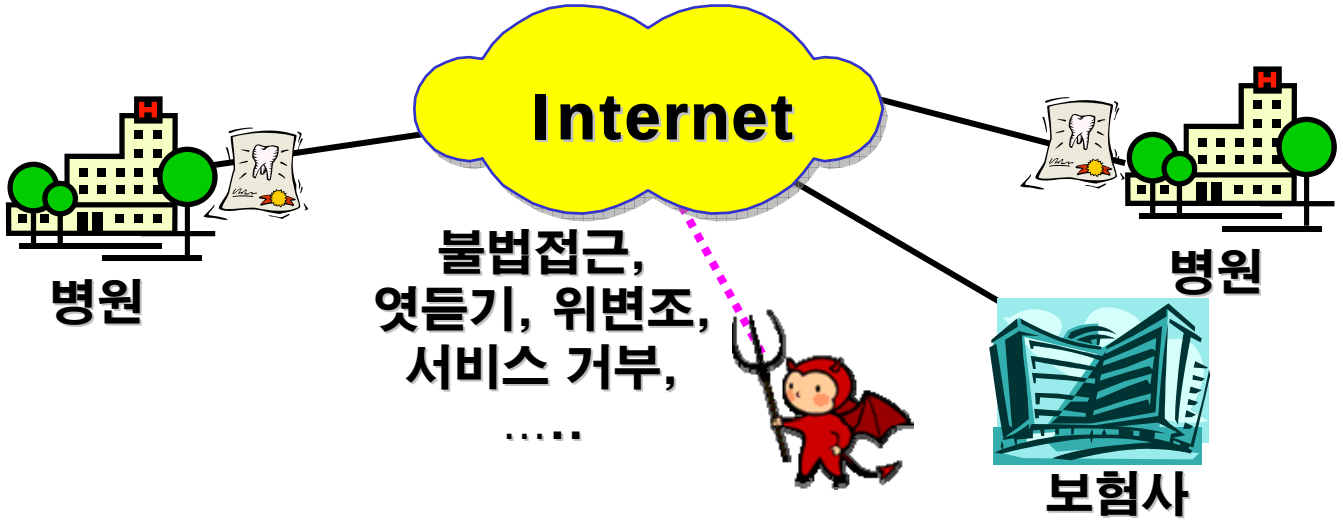
- **무결성 보장 : 위조 및 변경 불가**
- **사용자 인증**
- **재사용 불가**(no reusability)
- **부인 방지**(non-repudiation)

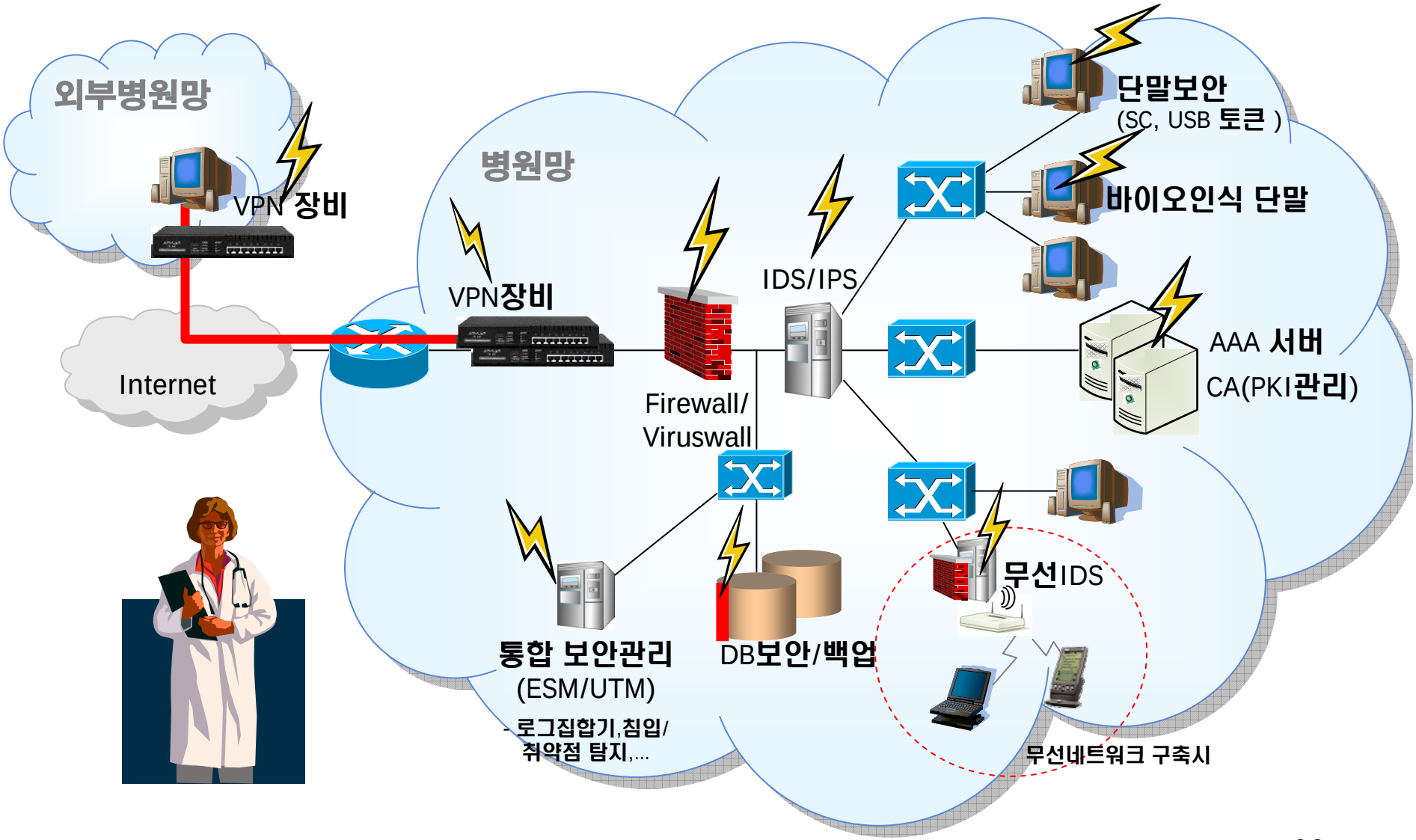
서비스 가용성(신뢰성)

- 2003년 1.25인터넷 대란
  - 서비스 거부(Denial of Service) 공격
  - 슬래머 웜에 감염된 PC들이 대량의 데이터를 생성해 DNS 서버에 인터넷 트래픽을 집중시키면서 마비
    - DNS 서버: 사람이 기억하기쉬운 도메인이름(www.etri.re.kr)을 컴퓨터가 인식할 수 있는 IP주소(129.254.19.28)로 변환, 모든 인터넷 접속은 초기에 DNS서버로 접속이 필요함.
  - 접속 불가에 따른 소송
- 2004년 A병원 전산망 마비
  - 환자의 의료정보를 수기로 기록
  - 무중단 재해복구(DR; Disaster Recovery)시스템을 구축 계기

의료정보화에서의 보안 기술

- 기밀성, 무결성, 사용자 인증, 접근권한 제어, 부인 방지,,....
- 시스템 가용성(또는 신뢰성)
  - 정보의 백업과 DB이중화, 분산배치, ...




외부병원망
VPN 장비
Internet
병원망
VPN장비
Firewall/
Viruswall
IDS/IPS
단말보안
(SC, USB 토큰)
바이오인식 단말
AAA 서버
CA(PKI관리)
무선IDS
통합 보안관리
(ESM/UTM)
- 로그집합기,침입/
취약점 탐지,...
DB보안/백업
무선네트워크 구축시

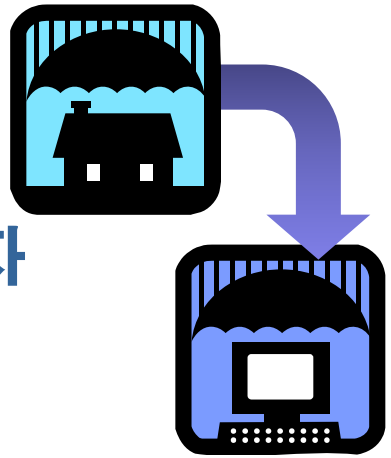
의료 기관 보안 현황 및 시사점

정보 자산 보안의 필요성

- 자산의 변화
  - 의료장비, 약품, 인쇄물(의무기록, X-ray 사진 등)

  → 비용절감, 편리성 추구

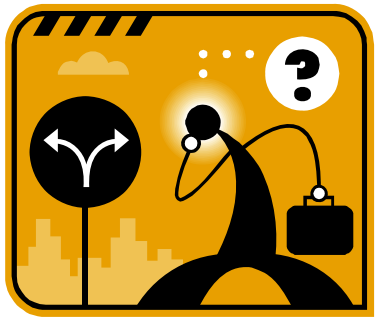
  → 정보자산(EMR, 영상의무기록 등)의 등장



- 보안의 변화
  - 장비가 있는 곳의 출입을 제한하여 보호하자

  →정보자산을 안전하게 지키자
    - 부피가 작다(USB 메모리, CD, 노트북,...)
    - 눈에 보이지 않는다.(원격접속으로 데이터를 옮길 수 있다) …

- '무엇을 보호할 것인가?'



의료기관의 보안 현황 및 시사점

1. 디지털 정보의 저장과 교류
2. 접근 권한 제어
3. DB 정보 암호
4. 재난관리(DB 이중화 등)
5. 문서 위변조 방지 및 출력 관리
6. 디지털 정보의 파기
7. 보안 감사 및 로그
8. 새로운 IT 서비스 기술 등장

1. 디지털 정보의 저장과 교류

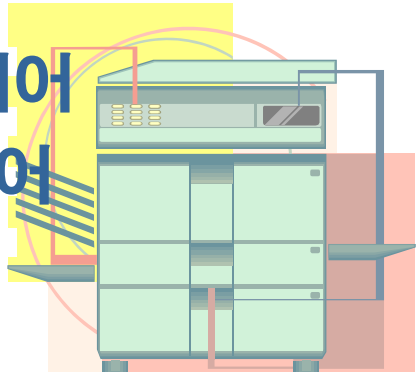
- 의료 정보 저장 및 관리의 복잡도
  - 의료정보는 최신정보 뿐만 아니라 이전 정보도 매우 유용하다.
  - 접근제어 (정보 관련자가 많다, 그룹별로 정보가 공유될 필요가 있다, 다른 많은 정보가 유통된다,,,)
  - 24시간 365일 가동 (타 IT시스템에 비해 가용성 높음)
  - Case by case로 해결
- 의료 정보의 소유권 (환자 vs. 의료진)
- 다중번호 관리
- 의료 정보 교환을 위한 표준화 체계 미비
- 교환 정보의 최소화, 기밀성 및 무결성(위변조에 대한 검증) 유지

2. 접근 권한 제어

- 접근권한 (정보보호 vs. 효율성)
  - 엄격한 접근제어(일정시간 미사용시 시스템 로그오프, 개인의료정보의 접근제한 등)
  - 정확한 진단/치료를 위해서는 간접 의료정보 파악 필요
  - 신속한 의료 서비스 위해 담당의사가 아닌 간호사가 의무 기록에 접속
- 디지털 전자서명
  - 의료 서비스를 지연시키지 않는 수준
  - 서명 시점이나 범위, 빈도 등에 대한 이견
- 의료진이 치료 이외의 목적으로 환자 정보 수집, 축적
- 체계적인 권한 부여, 철회, 위임 등에 대한 규정 미비

3. 문서 오남용 방지 및 출력 방지

- 접근권한 제어, 출력 횟수, 문서 유효기간 제어
- 의료 정보의 화면프린트(PrtScn) 및 촬영 제어
- 보안 감사 수행, 보안 책임 규정 등
  - 필요이상의 문서 출력, 정보 남용시



4. 디지털 정보의 파기

- 복제가 용이하고 원본/사본의 구분이 어려움
- 정보 파기에 관한 보안 책임 명시
- 보안 감사 추적

5. DB 정보 암호화

- 의료 정보 유출, 무단 사용 등의 방지 대책
- 패스워드 암호화
- 의료정보 암호화
  - 비용 대비 효율성이 있는가?
  - 암호키 관리의 어려움
  - 백업 필요

6. 재난관리 (DB 이중화 등)

- 시스템 구축 및 관리 비용의 부담
- 합리적 수준의 DB이중화 시행 권고 등의 방안 모색

7. 보안 감사 및 로그

- 어떤 행위에 대한 단순한 기록 수준(A가 X시간에 로그온하여 의료정보 Y에 대한 조회/수정)
- 체계적인 보안 정책이 부재
  - 기록 정보에 대한 분석과 활용 미미함
  - 보안 감사 대상, 항목, 횟수, 저장 기간, 경보 수준 등
  - 감사 권장 주기, 저장 기간, 보안 감사 활용 등에 대한 가이드라인

8. 새로운 IT 서비스(무선네트워크, RFID, 센서,..) 접목

- 소형, 경량화, 무선 → 분실이나 도난이 용이
- 기기 내부에 저장된 데이터도 함께 유실 가능성
- 유형의 자산 외 기기내에 저장된 무형의 자산(의료 정보 등)에 대한 보안 대책 필요
  - 장비 내 저장 가능한 데이터 제한
  - 유실 경우에 대비한 보안 대책 마련.

→ 새로운 IT 서비스 환경은 기존 기술을 무력화 함.

- (예) 듀얼모니터에서는 화면프린트 제어 기능이 동작하지 않는 경우가 있음.

시사점

분 류	기술적 요소	관리적 요소
디지털 정보의 저장과 교류	AA	AAA
접근 권한 제어	AAA	AAA
DB 정보 암호	AAA	A
재난관리(DB 이중화 등)	AA	AA
문서 위변조 방지 및 출력 관리	AA	AAA
디지털 정보의 파기	AAA	AA
보안 감사 로그	A	AAA
새로운 IT 서비스 기술 등장	AA	AAA

의료 정보보호 요소기술

- 데이터 기밀성, 무결성
  - 의료 정보의 안전한 교환 및 저장
- 인증 및 접근권한 관리
  - 사용자 식별을 통한 진료기록의 접근 제어
  - 접근과 사용 권한에 대한 정의
  - 진료 내용의 분류에 따른 접근 제어 등

기존 네트워크 보안기술 활용 가능

- 보안 감사 및 로그
  - 보안 책임 근거
- 정보 가용성, 신뢰성
  - 데이터 백업 및 복구 시스템
- 개인 프라이버시 보호

CSO & CPO

- CSO(Chief of Security Officer)
  - 임원의 신변, 건물, 시설 등의 유형자산 이외에 컴퓨터 정보 등의 무형 자산을 보호하는 책임
- CPO(Chief of Privacy Officer)
  - 개인의 프라이버시 보호 규정에 위배되는 정책이나 해킹 등의 사이버 범죄로부터 회원정보를 보호하는 책임

- **보안에서 가장 중요한 것은 기술이 아닌 사람!!**

  http://www.zdnet.co.kr/builder/system/security/0,39031673,39148134,00.htm

의료 정보보호 기술 개발 및 적용

- 보안 취약성의 대부분은 개발단계에서 발생
  - 설계 및 구현 시 다양한 보안 취약성이 존재
  - 개발 단계에서 보안이 고려되지 않아 보안 취약성을 내포한 상태로 소프트웨어 출시
  - 비정상적 권한 획득에 의한 정보유출, 조작, 파괴 등이 보안사고의 주요한 발생 원인
- 보안사고의 90%이상이 알려진 보안결함을 악용(출처 : 미국 CMU SEI)

- 설계 단계부터 보안을 염두에 두어야 함.
- 보안기술의 적용/개발시 input을 줄 수 있는 사람

→ CSO or CPO

→ 의무기록사

의료 정보보호 표준화

의료정보보호 표준화 (1/4)

- **공개키 기반 구조**(PKI)-ISO/TS 17090-1/2/3 : Health informatics - Public key infrastructure : part 1/2/3
  - **의료환경에서 PKI를 이용한 보안 서비스(사용자 인증, 무결성, 기밀성, 전자 서명, 인가, 접근제어 등) 제공**
  - **표준에서 제안한 헬스케어 특성을 반영한 전자 인증서 정책 수립, 보안 프로파일 작성, 구현 가이드라인 등은 유용하게 사용될 것임.**
  - **국내 의료 정보 시스템에 인증서 도입 시, 국내 실정과 표준의 상충되는 부분 없는지 분석 필요.**
- **권한 관리 및 접근 제어** (PMAC) - ISO/TS 22600-1/2/3 : Health informatics - Privilege management and access control : part 1/2/3
  - Part 1 : **이질적 헬스케어 도메인간 보안 정책을 합의시, 표준에서 제시한 정책 합의와 관련된 문서 구조와 내용, 정책 합의 문서의 템플릿으로 유용함.**
  - Part2 : **이질적 헬스케어 도메인 간에도 상호호환적인 접근제어 플랫폼을 구현에 참조 가능함.**

의료정보보호 표준화 (2/4)

- ISO/Draft TS 21298 : Health informatics - Functional and structural roles
  - 직업 분류에 따른 의료 서비스의 구조적 역할과 기능적 모델 예제 제시
  - 권한 관리를 위한 Role attribute 생성 및 발급 방법 제시, 역할 명세, 기능적 모델과 구조적 모델간 관계 제시 등은 권한 관리 및 접근제어를 위한 역할 정의 및 분류에 매우 유용하다고 사료됨.
  - 구조적 역할, 기능적 역할의 실제 사용 및 구현 예가 추상적임
  - 구조적 역할과 기능적 역할이 정의되는 상황에 대한 조건 모호.
- **보안 아카이빙**(Secure Archiving)- ISO/WD 21547-1/2 : Health informatics - Security requirements for archiving and backup : part 1/2
  - 일반적인 EHR e아카이브 시스템 구조 및 기능적 특성 뿐 아니라 고려되어야 할 보안 요구사항을 정책 중심으로 기술하였음.
  - 병원 및 운영 환경에 따라 상세화 수준의 차이가 있겠으나 보안 정책 수립 시, 참고할 만한 표준 및 보안 요구사항 제시됨.

의료정보보호 표준화 (3/4)

- **보안 관리**(Security Management)- ISMS
  - ISO/Draft IS 27799, ISO/IEC 17799
    - **의료 정보 시스템의 특성에 기초한 발생 가능한 위협 및 취약점을 분석하고** ISO/IEC 17799(**엄밀히 말하면, 헬스케어 환경에서** ISMS**를 구축, 운영하는 가이드라인)를 구현할 수 있는 가이드라인을 제시하고 있음**.
    - ISO/IEC 17799 **구현 가이드라인은 보안 사고 감소, 시스템 신뢰성 향상 등의 의료 정보 시스템 보안성 강화에 유용한 활용임**.
  - ISO/IEC 27001, Information technology — Security techniques — Information Security Management Systems — Requirements, 2005.
    - **정보 시스템의 계획, 개발, 운영, 유지보수 하는 모든 단계에서** ISO/IEC 17799**를 반영하여 보안수준을 보장하기 위한 프레임워크를 제안하고 있음**.
    - **의료 정보 시스템의** ISMS **체계를 구축하는데 매우 유용**
  - **국내 의료환경에 적합한 ISMS 도입 및 인증기관 필요**

의료정보보호 표준화 (4/4)

- **익명화**(Pseudonymisation)-ISO/Draft TS 25237
  - 데이터 저장 및 비영리적 연구 목적의 개인 의료 정보 활용 시에 익명화를 통하여 개인 식별 가능한 정보의 유출을 방지 가능함.
  - 익명화 공격 모델 및 위험 분석, 익명화 기법 등을 향후, 의료 정보 시스템 구축 시 참고 가능
- **보안 감사**(Audit Trail)-ISO/27789
  - New Work Item Proposal 단계로 국내 보안 감사 시스템에 즉시 반영은 어려우나, 표준에 대한 지속적 follow-up 필요.
  - 보안 감사의 대상, 항목, 횟수, 저장 기간, 로그 트리거 등의 정의가 부족한 상황.
  - 필수 보안 감사 항목, 이벤트에 대한 표준은 유용한 가이드라인이 될 것임.
- **안전성 평가**(Safety Assessment) **및 위험 관리**(Risk Management)- ISO/DTR 27809
  - HW 중심으로 이루어졌던 위험/안전 관리가 SW 측면에서도 이루어져야 함.
  - SW 안전성 측면에서 분류 및 통제 방법, 이에 준하는 국제/사실 표준 기술 등을 분석함으로써 국내에서도 의료 SW의 안전성 평가 기준 및 가이드라인 수립에 참고할 만한 표준임.

결 론

If you

See it

Hear it

Or Speak it

PROTECT IT!

결 론

- 개인프라이버시 보호 vs. 의료서비스 공공성 절충
  - 의료 정보보호 필요성 인식
  - 의료 정보보호 법/제도
  - 보안기능이 내장된 시스템 설계 및 구현
  - 의료 정보 표준 기술과 호환 개발
- 의료서비스 정보보호 기술 개발 방향
  - 의료진
    - 보안현황/서비스 환경에 대한 모니터링
    - 보안요구사항을 기술 개발에 반영
  - 엔지니어
    - 손쉽게 사용할 수 있고 신뢰할 수 있는 의료정보시스템
    - 프라이버시 보호(익명 인증, 조건부 추적 등)형 의료정보시스템
    - IT서비스 발전방향에 따른 보안기술개발 및 적용

Q & A