기록물 보안관리 방안

2010. 10. 8

중부대학교 정보보호학과
이 병 천 교수

차 례

1. 기록물 관리의 역사

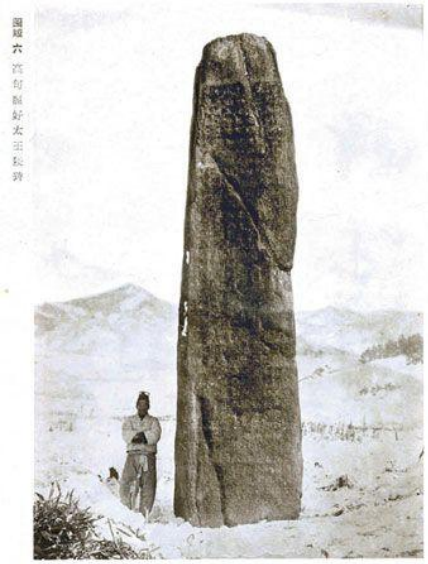
- 우리 민족은 역사의 기록과 보존에 많은 노력을 기울여 온 민족
  - 최초의 금속활자 발명
  - 조선왕조실록
  - 족보 기록 문화

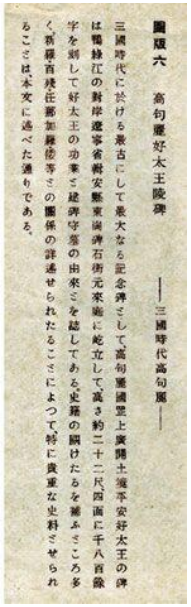
RT @daesabu RT @MikyCho 고구려:유기100권,신집5권/백제:서기(고흥)/신라:국사(거칠부)/고려:구삼국사,단군본기,고구려본기,백제본기,편년통재,속편년통제,편년통록,고려실록,단기고사(대야발) 이상은 사라진 우리 사서입니다. #역사당_

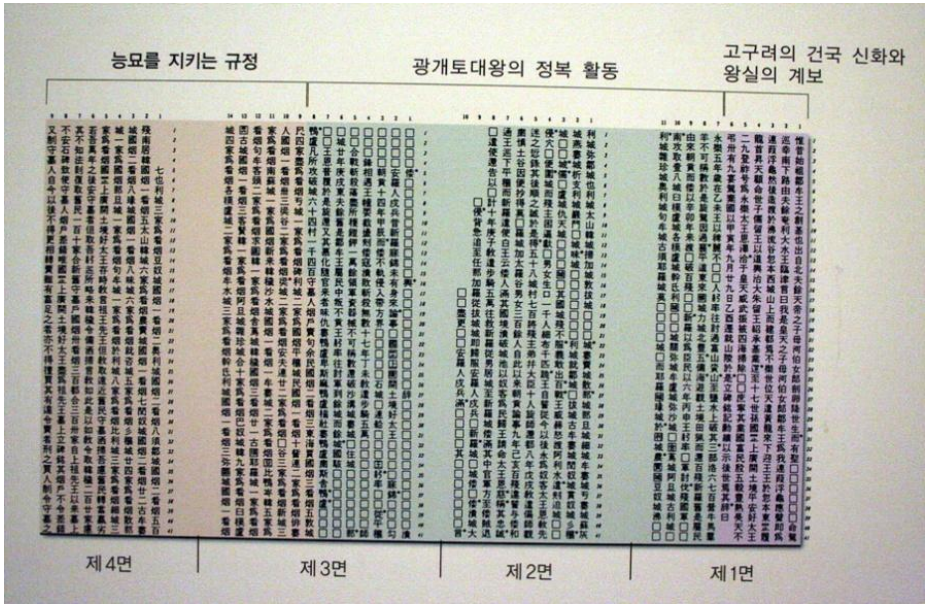
- 일제시대 국권 상실로 기록물의 대량 유실
- 기록물 관리상 드러난 문제점들
  - 유실 - 고대 역사서의 유실, 일제시대 기록물의 대량 유실
  - 파괴 - 정복에 의해 역사가 파괴되고 승자의 기록만 남음
  - 변조 - 일제의 광개토대왕비 변조, 조선시대 소중화 사상에 의한 자체 변조

기록물 관리의 역사

- 기록물 관리를 위한 제도
  - 조선왕조실록-현재의 왕은 자신에 대한 기록을 볼 수 없음. 4대사고 운영으로 백업체계를 갖춤
  - 광개토대왕비- 능묘를 지키는 엄격한 규정을 마련







전자문서 시대의 기록 보존

- 전자기록물 보안요구사항 – ISO 15489
  - 진본성 (authenticity)
  - 신뢰성 (reliability)
  - 무결성 (integrity)
  - 가용성 (usability)

- 전자문서 시대의 기록 보존 노력
  - 국가기록원 운영
  - 각종 기록관리 표준, 지침 마련
  - 전자기록물 생성, 관리 체계 운영
  - 기록물정보서비스
  - 안전한 보안관리-물리적 보안, 백업체계, 시스템/네트워크 보안

2. 최근의 정보보안 동향

- 정보통신 환경의 변화
  - 스마트폰, 스마트TV, 태블릿컴퓨터 등 모바일 컴퓨팅의 발전, 모바일 사용자의 급격한 증가
  - 광대역통합망, 유비쿼터스 환경으로 발전
  - 클라우드컴퓨팅 확대로 개인정보가 클라우드에 저장
  - 위치기반서비스의 확대
  - 소셜네트워킹 서비스의 급격한 발전
  - 그린 IT, 스마트그리드
  - 익스플로러의 퇴조 및 브라우저의 다변화
  - ActiveX 기반한 전자상거래에 대한 비판과 대안 마련을 위한 노력

정보보호 10대 이슈

- 2009년 정보보호 10대 이슈 (2010국가정보보호백서)
  1) 7.7 DDOS 침해사고 발생
  2) 소셜 메시징 인프라 기반 피싱 기승
  3) 허위 보안제품 등장
  4) 온라인 게임 해킹 급증
  5) 성적 조작을 위한 대학 전산망 해킹
  6) 개인정보유출 피해자 집단소송 판결
  7) 정보보호 관련 법 제개정 활발
  8) 새로운 IT기술과 정보보호: 스마트그리드, 클라우드 서비스
  9) 아이폰 등장으로 스마트폰 보안 관심 증가
  10) 응용프로그램 제로데이 공격 증가

사이버침해 위협 동향

- 2009년 사이버침해 위협 동향(2010국가정보보호백서)
  - 응용프로그램 취약점을 노리는 홈페이지 은닉 악성코드
  - 금전적 이득을 취득할 목적의 악성코드
  - 사회적 이슈, 이벤트를 악용한 악성코드
  - 분석지연을 위한 고도의 분석방해 기술의 접목
  - 악성코드 대량생산을 위한 자동화된 도구의 이용

최근 해킹 공격의 특징

- 다기능 악성코드 출현
- 웜•바이러스 전파속도 고속화
- 스팸 메일의 지능화
- 공격도구 자동화 및 신속성 증가
- 공격도구 다양화 및 지능화
- 시스템의 취약점을 이용한 공격 증가
- 기간망에 대한 공격 증가

분산서비스거부(DDoS) 공격의 위협

- 7.7 DDoS 공격 – 2009.7.7

웹해킹

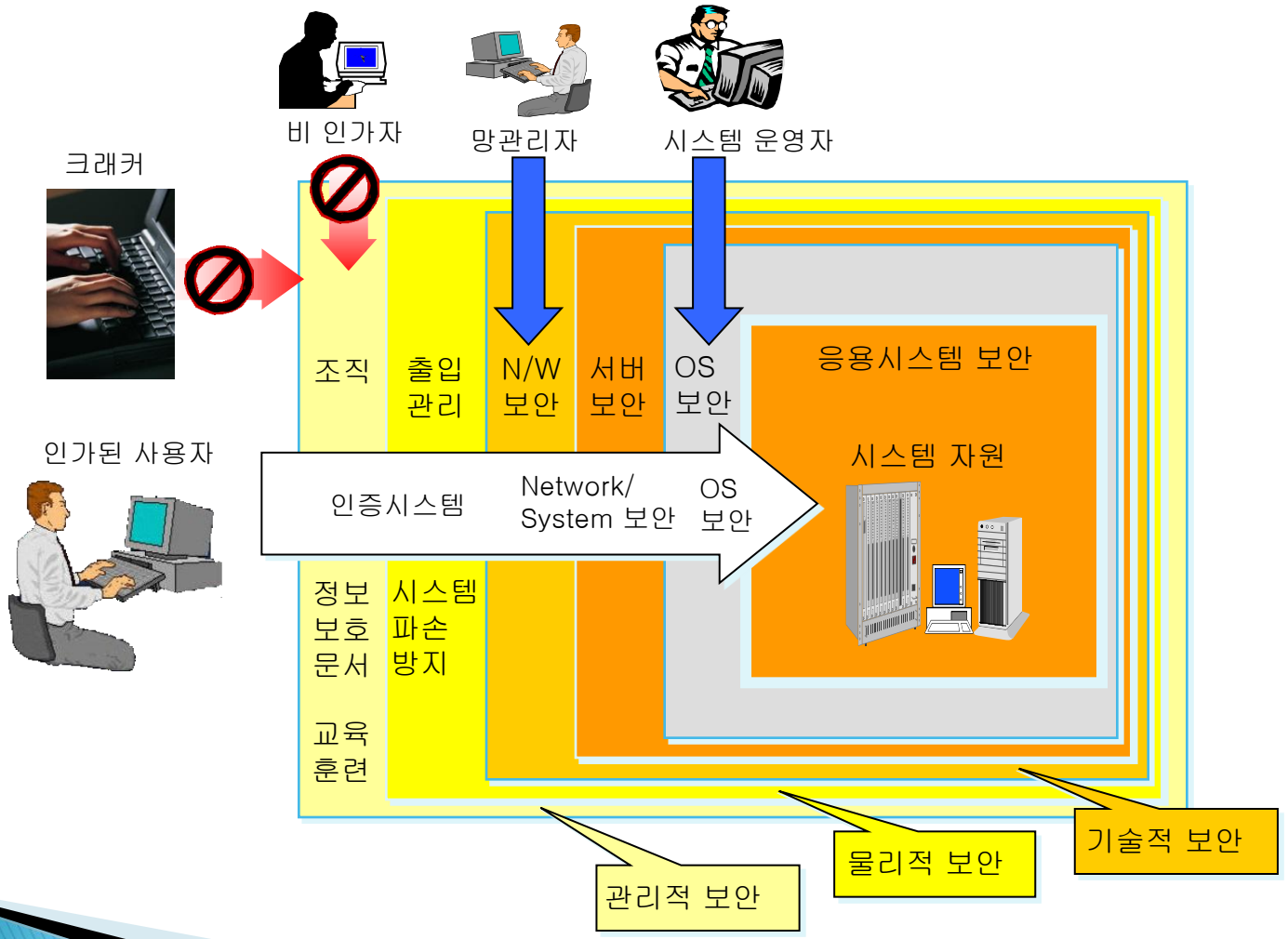
- 위협 요소
  - 현재 대부분의 정보서비스들이 웹서비스 형태로 제공
  - 방화벽에서 웹서비스는 통과를 허용
  - 웹서버가 아닌 웹프로그래머의 오류 가능성
  - 특별한 도구 없이 웹브라우저만으로 공격이 가능
- 공격 기법
  - SQL 삽입
  - 크로스사이트스크립팅 (XSS)
  - 세션 하이재킹
  - 파일 업로드
  - 디렉토리 탐색
  - 악성코드 배포

OWASP Top 10 – 2010년

- A1 – 인젝션(Injection)
- A2 – 크로스사이트 스크립팅(XSS)
- A3 – 취약한 인증과 세션관리
- A4 – 안전하지 않은 직접객체참조
- A5 – 크로스사이트 요청 변조(CSRF)
- A6 – 보안상 잘못된 구성
- A7 – 안전하지 않은 암호 저장
- A8 – URL 접근제한 실패
- A9 – 불충분한 전송계층 보호
- A10–검증되지 않은 리다이렉트와 포워드

오픈웹어플리케이션보안프로젝트

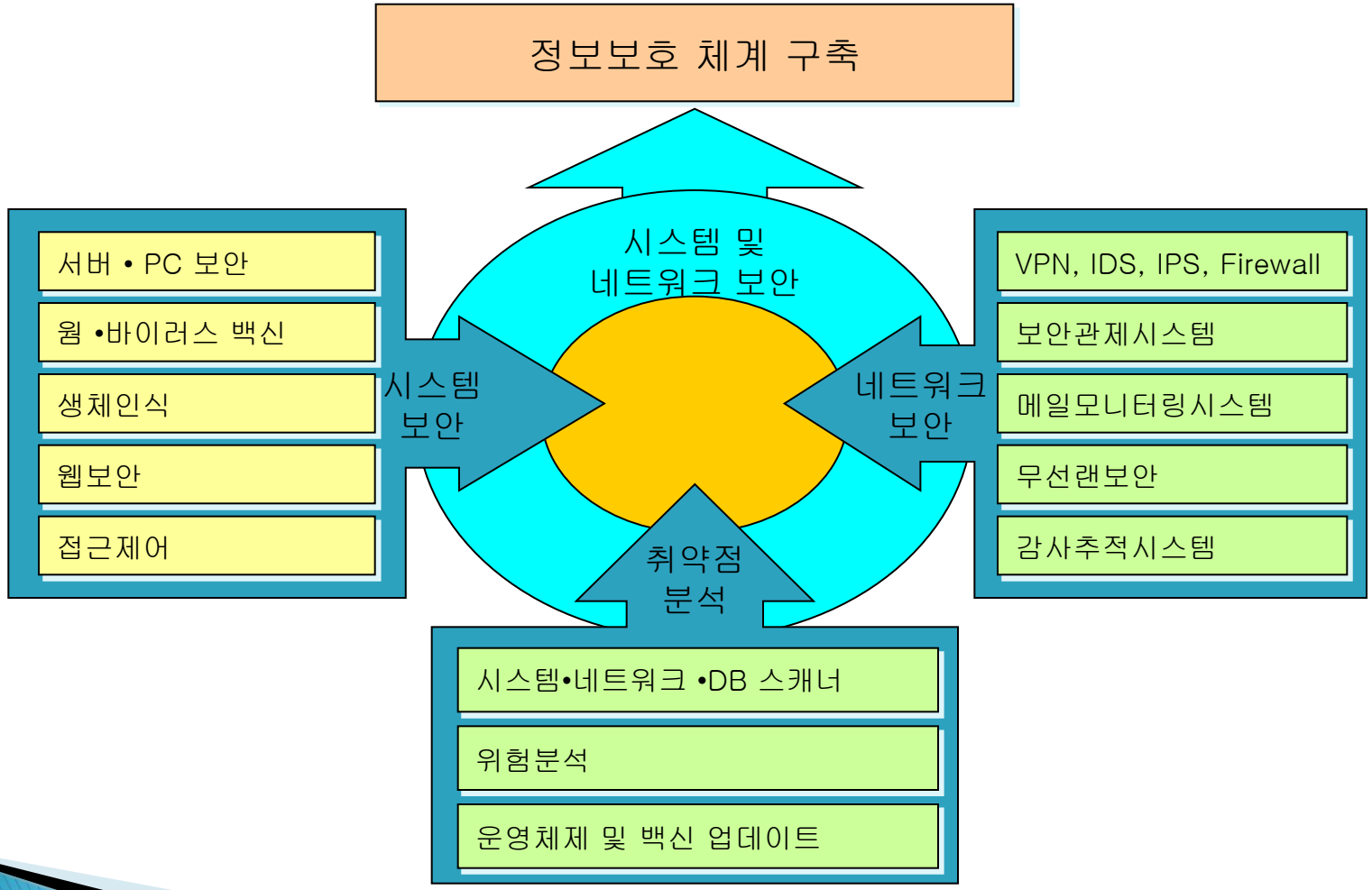
정보보호의 계층적 구조


비 인가자
망관리자
시스템 운영자
크래커
조직
출입 관리
N/W 보안
서버 보안
OS 보안
응용시스템 보안
시스템 자원
인가된 사용자
인증시스템
Network/ System 보안
OS 보안
정보 보호 문서
시스템 파손 방지
교육 훈련
관리적 보안
물리적 보안
기술적 보안

정보보호 기술

구 분	보안대책	용 도	대상
사용자 인증	PKI	•정당한 사용자 인증 (전자서명 인증)	* 인증서버
시스템 보안	Secure OS	•시스템의 불법접근 차단 및 강력한 안티해킹	* 웹서버 등의 24시간 서비스 시스템
	Scanner (S)	•시스템 보안취약성 점검 및 진단	* 웹서버 등의 24시간 서비스 시스템
네트워크 보안	Firewall	•불법적인 네트워크 접속에 대한 접근통제	* F/W 서버
	IDS	•내/외부망으로 부터의 불법침입 탐지 및 차단	* IDS 서버
	E-Mail 보안	•전송메일의 암호화 / 스팸메일 차단	* Mail 서버
	Scanner (N)	•네트워크 보안취약성의 점검 및 진단	• Scanner & VMS 서버
	VMS	•웜 바이러스 및 악성코드 차단	• Scanner & VMS 서버
암호화 통신	VPN	•종단간 메시지/데이터의 비밀성 보장	• 본사 ←→지점통신실, 본사←→인터넷
PC 보안	통합 PC 보안	•개별 PC의 통합보안 관리(바이러스, 방화벽 등)	• 사내 PC
통합보안관리	ESM 솔루션	•각 개별 보안솔루션의 통합보안관리	• ESM 서버

정보보호 체계


정보보호 체계 구축
시스템 및
네트워크 보안
서버 • PC 보안
웜 •바이러스 백신
생체인식
웹보안
접근제어
시스템
보안
네트워크
보안
VPN, IDS, IPS, Firewall
보안관제시스템
메일모니터링시스템
무선랜보안
감사추적시스템
취약점
분석
시스템•네트워크 •DB 스캐너
위험분석
운영체제 및 백신 업데이트

사이버침해 대응 방안

- 사이버침해에 대한 지속적인 관심 및 보안교육
  - 보안 도구 설치, 보안 패치, 정기적인 백신 업데이트
  - 지속적인 보안 교육 실시
- 정보보호용 제품 사용
  - IDS, IPS, VPN, 방화벽, SecureOS 등
- 업무상 필요하고 검증된 소프트웨어만 사용
  - 많은 악성 코드가 프리웨어 또는 불법 복사제품을 통해 전달
- 내부정보의 유출 방지책 강구
  - 망의 구성을 NAT 등을 사용하여 사설 형태로 구성
  - 시스템에 불필요한 서비스 포트 삭제
- 이메일 주의
  - 첨부 파일을 열기 전에 백신 프로그램으로 검사
  - 이메일 서버에 서버용 백신 프로그램 설치 및 주기적 업데이트 수행
- ID와 패스워드 관리 철저
  - 불필요한 사용자 계정 삭제, 추측 어려운 ID와 패스워드 사용

보안 관리자의 역할

- 보안정책/지침 수립
  - 모든 직원이 준수해야 하는 정책 및 지침을 수립
  - 기술적 대책으로 대응하기 힘든 위협으로부터 보호
- 기본원리에 따른 보안시스템 구축•운영
  - 정기적인 보안취약점 점검 및 보완
- 주기적인 인식교육 및 보안기술 교육실시
  - 보안권고문, 보안취약점, 보안정보 등 전파
- 중요 자료에 대한 주기적인 백업 수행
- 보안 프로그램 업그레이드 및 패치를 통한 시스템 취약점 제거
- 불필요한 서비스 중지
- 사고 시스템 및 주변 시스템의 주기적 점검
- 사이버테러 발생 시 즉각적인 신고 및 협조

일반 사용자의 역할

- 보안수칙을 잘 지키자
  - 백신프로그램 사용, 자동업데이트
  - 안전한 비밀번호 사용
  - 정품소프트웨어 사용
  - 전자메일 사용 주의
  - 중요한 데이터의 백업 생활화
  - 부팅시, 윈도우로그인시, 공유폴더 등 비밀번호 설정
  - OS 및 주요소프트웨어의 보안패치 설치
  - 사용하지 않는 PC는 끄기
  - 정보보호를 위한 유용한 도구들을 사용

사용자PC 보안수칙
스마트폰 보안수칙
인터넷뱅킹 보안수칙
정보보호관리자 보안수칙
사이버안전매뉴얼

3. 기록물 보안관리 방안

- 기록물 보안관리의 특수성
  - 서비스의 지속가능성이 중요 (수백년~수천년?)
  - 자연재해, 전쟁, 관리부실 등으로 인한 유실 가능성
  - 후대에서 선대의 기록을 고의로 변조, 파괴할 가능성

- 각종 기록관리 표준 제정
  - 기록물관리기관 보안 및 재난관리 기준 – 2009년 제정
  - 기록관리시스템 기능요건 – 2007년 제정
  - 전자기록물 장기보존포맷 기술규격 – 2008년 제정

기록물 보안관리 방안

- 사람에 대한 보호
  - 자체보안팀 운영 및 능력향상 도모, 보안관리 인력양성
  - 내부인에 의한 위협 대응, 보안 교육, 처벌규정
- 프로세스 측면
  - 안전한 기술적 대책에 기반한 기록물 관리 시스템 운영
  - 엄격한 법, 제도, 표준, 규정 수립
- 기술 측면
  - 엄격한 신분인증 및 권한에 기반한 운영
  - 로그시스템 운영
  - 안전한 암호기술 적용
  - 장기적 서비스 가능한 체계 구축
  - 지속적인 기술개발이 필요

기록물 관리 방안 – 기타

- **국외 백업**
  - 전자화된 기록에 대해서는 국외에도 백업을 두는 방안
  - 대사관 등 국외소재 국내자산을 이용하여 백업
  - 국가간의 조약을 통해 상호 백업서비스 제공
  - 암호학적 대책으로 보안에 만전
- **외국 소유의 문화유산 이용환경 구축**
  - 국외에 반출되어 외국이 소유하고 있는 우리의 문화유산에 대해 환수 노력과 함께 백업 개념에서 전자화하고 국내에서 사본으로 서비스
- **개인소장 유산들에 대한 보존노력**
  - 국내에 산재하는 사라져가는 개인 소장의 주요 유산들을 수집, 분석, 활용한다는 측면에서 개인의 소유권을 인정하는 수준에서 국가가 수집 및 보관을 대행하고 사본을 제작하여 서비스
- **후대의 역사변조 방지**
  - 우리의 역사에서는 후대에 과거의 역사를 변조하는 행위가 많았음. 이를 근본적으로 방지할 수 있는 암호학적, 기술적, 법적 조치가 필요

기록문화축제(아이디어) – 기타

- **"현재의 기록할만한 사례들을 축제를 통해 발굴하고 역사에 기록하자"**
  - 유명인들의 유익한 강연, 공연, 가치있는 아이디어 등
  - 불굴의 의지로 성공한 사례, 잘 보이지 않는 미담, 기술의 발전
  - 일상적으로는 역사에 기록되기 힘든 가치있는 기록들을 발굴
  - 좋지 않은 역사보다 성공적인 역사를 발굴하여 기록
  - 일반인들에게 기록문화의 중요성을 축제형식으로 홍보
- 행사진행방법
  - 기록할만한 사례들을 강연, 공연 형태로 소개하고 그것을 사진, 동영상, 기록문서 등의 형태로 기록 – TED의 성공사례
  - 모든 행사 내용을 실시간 중계하고 인터넷으로 영구 서비스. 장기보존 포맷으로 역사에 기록하는 것은 국가기록원에서 주관

감사합니다

Q & A