외부용역사업 보안관리 시행세칙

제정 : 2016.11.01
개정 : 2018.09.13
개정 : 2020.03.01
개정 : 2021.12.01
개정 : 2022.10.01
개정 : 2023.10.16

제 1 장 총 칙

제1조(목적) 이 세칙은 「정보보안 · 관리규정」 제33조에 의거 외부 용역사업 수행시 용역사업 전반에 걸친 보안사항의 시행기준을 수립하는 것에 목적이 있다. <개정 2021. 12.01.>

제 2 장 용역사업 보안관리

제2조(용역사업 보안관리) ① 미래전략처장은 정보화·정보보호사업 및 보안컨설팅 수행 등을 외부용역으로 추진할 경우 사업 관리책임자로 하여금 미래전략처장이 보안관리가 필요하다고 판단하는 사항 등의 보안대책을 수립·시행할 수 있다. <개정 2018. 09.13., 2021.12.01., 2022.10.01., 2023.10.16.>

①의2 용역사업 계약 시 참가직원의 보안준수 사항과 위반 시 손해배상 책임 등을 계약서에 명시한다. <개정 2021.12.01.>

①의3 용역사업 수행 관련 보안교육·점검 및 용역기간 중 참여인력의 임의교체를 금지한다. <개정 2021.12.01.>

①의4 정보통신망도·IP현황 등 용역업체에 제공할 자료는 자료 인계인수대장을 비치, 보안조치 후 인계·인수하고 무단 복사 및 외부반출을 금지한다. <개정 2021. 12. 01.>

①의5 사업 종료 시 외부업체의 노트북·휴대용 저장매체 등을 통해 비공개 자료가 유출되는 것을 방지하기 위해 복구가 불가능하도록 완전삭제 한다. <개정 2021.12.01.>

①의6 용역업체로부터 용역 결과물을 전량 회수하고 비인가자에게 제공·열람을 금지한다. <개정 2021.12.01.>

①의7 용역업체의 노트북 등 관련 장비를 반입·반출시마다 악성코드 감염여부, 자료 무단반출 여부를 확인하고 반입시 『정보보안·관리규정』의 용역업체 보안관리 점검사항(별지 서식 18호)을 작성하고 반출시 반출신청 및 확인서(별표 1)를 작성하고 사용한다. <개정 2021.12.01.>

①의8 용역업체 서버 점검시 인터넷 연결을 금지하고, 부득이한 경우 대원대학교 보안정책이 적용 되는 기기를 별도 지정하여 보안통제 하에 제한적으로 이용한다. 용역업체가 외부 인터넷을 사용 시에는 용역업체 인터넷 접근 허용 요청(별표 2)을 작성하고 사용한다. <개정 2020.03.01., 2021.12.01.>

② 정보보안담당자는 비밀 및 중요 외주 용역사업을 수행할 경우 외부인원에 대한 신원조사·비밀취급인가, 보안교육 및 외부유출 방지 등 보안조치를 수행할 수 있다.

③ 사업 관리책임자는 보안대책의 시행과 관련한 이행 실태를 주기적으로 점검하고 미비점 발견 시 사업담당자로 하여금 보완토록 조치시키고 정보보안담당자에게 보고해야 한다.

제3조(용역사업 입찰시 보안관리) ① 용역사업 입찰 시 용역사업에 대한 보안관리 계획을 수립 및 평가할 수 있다. <개정 2021.12.01.>

② 입찰공고 이전에 투입이 예상되는 자료 · 장비 가운데 보안관리가 필요한 사항에 대하여 관련법규에 따라 등급을 분류하고 필요한 보안요구기준을 마련할 수 있다. <개정 2021.12.01.>

③ 입찰공고 시에 용역사업 보안위규 처리기준(별표 3), 보안 위약금 부과기준(별표 4), 누출금지 대상정보(별표 5) 등을 공지할 수 있다. <개정 2021.12.01.>

④ 제안서 평가요소에 자료 · 장비 · 네트워크 보안대책, 누출금지 대상정보(별표 5), 관리방안 등 보안관리 계획의 평가항목 및 배점기준을 마련할 수 있다. <개정 2021.12.01.>

⑤ 업체가 입찰제안서에 제시한 용역사업 전반에 대한 보안관리 계획이 타당한지를 검토하여 사업자 선정 시 이를 반영할 수 있다. <개정 2021.12.01.>

⑥ 웹 호스팅 등 정보시스템의 위탁운영 시에는 해킹에 대비해 웹 방화벽 등 보안시스템 구비 여부와 단순 운영 이외 보안관리가 가능한지 여부를 검토할 수 있다. <개정 2021.12.01.>

제4조(용역사업 계약 시의 보안관리) ① 용역사업에 투입되는 자료 · 장비 등에 대한 대외보안이 필요한 경우 보안의 범위 · 책임을 명확히 하기 위해 사업수행 계약서와는 별도로 보안서약서(별표 6)를 작성할 수 있다. <개정 2021.12.01.>

② 용역사업 참여인원은 용역업체 임의로 교체할 수 없도록 명시하고 신상변동 (해외여행 포함) 사항발생 시 보안담당관에게 즉시 보고해야 한다. <개정 2021.12.01.>

③ 대원대학교의 요구사항을 사업자에게 명확히 전달키 위하여 작성하는 과업지시서 · 계약서(입찰공고 포함)에 인원 · 장비 · 자료 등에 대한 보안조치 사항과 용역사업 보안위규 처리기준(별표 3) 및 누출금지 대상정보(별표 5) 를 기술할 수 있다. <개정 2020.03.01., 2021.12.01.>

④ 용역업체가 사업에 대한 하도급 계약을 체결할 경우 본 사업계약 수준의 비밀유지 조항을 포함토록 조치 할 수 있다. <개정 2021.12.01.>

제5조(용역사업 수행시 보안관리) ① 용역사업 수행 전 참여인원에 대해 용역사업 보안위규 처리기준(별표 3), 보안 위약금 부과기준(별표 4), 누출금지 대상정보(별표 5)에 대한 보안교육을 실시할 수 있다.
② 정보보안담당관은 사업 수행 중 업체 인력에 대한 보안점검 실시, 누출금지 대상정보(별표 5) 외부 누출여부를 확인할 수 있다.
③ 비밀관련 사업을 수행할 경우 참여인원에 대한 비밀취급인가 등 보안조치를 수행할 수 있다.
<전문개정 2021.12.01.>

제5조의2(용역사업 수행시 자료에 대한 보안관리) ① 계약서 등에 명시한 누출금지 대상정보(별표 5)를 업체에 제공할 경우 자료관리 대장(별표 7)을 작성, 인계자 · 인수자가 직접 서명한 후 제공하고 사업완료시 관련 자료를 업체는 완전 삭제해야 한다.
② 용역사업 관련자료 및 사업과정에서 생산된 모든 산출물은 보안담당관이 지정한 PC에 저장 · 관리한다.
③ 용역사업 관련 자료는 인터넷 웹하드 · P2P 등 인터넷 자료공유사이트 및 개인메일함에 저장을 금지하고 대원대학교와 용역업체간 전자우편을 이용해 자료전송이 필요한 경우에는 자체 전자우편을 이용, 첨부자료 암호화 후 수·발신한다. 다만, 대외비 이상의 비밀은 전자우편으로 수·발신을 금지한다. <개정 2020.03.01.>
④ 대원대학교가 제공한 사무실에서 용역사업을 수행할 경우 제공한 비공개자료는 매일 퇴근 시 반납토록 하며 비밀문서를 제외한 일반문서는 용역업체에 제공된 사무실에 시건장치가 된 보관함이 있을 경우 이에 보관 가능하다. <개정 2020.03.01.>
⑤ 용역사업 수행으로 생산되는 산출물 및 기록은 보안담당관이 인가하지 않은 비인가자에게 제공 · 대여 · 열람을 금지한다.
<전문개정 2021.12.01.>

제5조의3(용역사업 수행시 사무실·장비에 대한 보안관리) ① 용역사업 수행 장소는 대원대학교 내 시건장치와 통제가 가능한 공간을 제공하거나 CCTV · 시건장치 등 비인가자 출입통제 대책이 마련된 외부 사무실을 사용 한다. <개정 2020.03.01.>
② 용역업체 사무실 또는 용역 업무를 수행하는 공간에 대한 보안점검을 정기적으로 실시할 수 있다.
③ 대원대학교 내부에서 용역사업을 수행할 경우 용역 참여직원은 노트북 등 관련 장비를 외부에 반출 · 입시마다 악성코드 감염여부 및 자료 무단반출 여부 확인해야 한다. <개정 2020.03.01.>

④ 인가받지 않은 USB 등의 휴대용 저장매체 사용을 금지하며, 산출물 저장을 위해 휴대용 저장매체가 필요한 경우 정보보안담당관 승인 하에 사용해야 한다.
<전문개정 2021.12.01.>

제5조의4(용역사업 수행시 내·외부망 접근의 보안 관리) ① 용역업체 사용 전산망은 방화벽 등을 활용하여 대원대학교 업무 망과 분리 구성할 수 있으며 업무상 필요한 서버에만 제한적 접근 허용을 할 수 있다. <개정 2020.03.01.>
② 용역사업 수행 시 대원대학교 전산망 이용이 필요한 경우 다음 각 호와 같이 보안관리한다. <개정 2020.03.01.>
1. 사업 참여인원에 대한 사용자 계정(ID) : 하나의 그룹으로 등록하고, 계정별로 정보시스템 접근권한을 차등 부여 할 수 있으며, 기관 내부문서 접근을 금지할 수 있다.
2. 계정별로 부여된 접속권한 : 불필요 시 곧바로 권한을 해지하거나 계정을 폐기할 수 있다.
3. 참여인원에게 부여한 패스워드 : 보안담당관이 관리하고 수시로 해당 계정에 접속하여 저장된 자료와 작업이력을 확인할 수 있다.
4. 보안담당관 : 서버 및 장비 운영자로 하여금 내부서버 및 네트워크 장비에 대한 접근기록을 확인할 수 있다.
③ 용역업체에서 사용하는 PC는 인터넷 연결을 금지 할 수 있으며, 사업수행 상 연결이 필요한 경우에는 보안담당관 보안통제 하에 제한적으로 허용할 수 있다.
<전문개정 2021.12.01.>

제6조(용역 사업 완료시 보안관리) ① 사업 완료 후 생산되는 최종 산출물 중 대외보안이 요구되는 자료는 대외비 이상으로 작성·관리하고 불필요한 자료는 삭제 및 세단 후 폐기한다. <개정 2021.12.01.>
② 용역업체에 제공한 자료, 장비와 중간·최종 산출물 등 용역과 관련된 제반자료는 전량 회수할 수 있으며, 업체는 사본 등별도 보관을 금지해야 한다.
③ 사업 완료 후 업체 소유 PC·서버의 하드디스크·휴대용 저장매체 등 전자기록 저장매체는 국가정보원장이 안전성을 검증한 삭제 S/W로 완전 삭제 후 반출할 수 있다.
④ 용역사업 관련자료 회수 및 삭제조치 후 업체에게 복사본 등 용역사업관련 자료를 보유하고 있지 않다는 대표 명의 확약서(별표 8)를 징구할 수 있다.
⑤ 사이버침해사고 예방을 위한 근본적인 대책으로 보안취약점의 원인이 되는 소프트웨어 결함 및 오류 등을 진단·제거하기 위해 소프트웨어 개발보안(시큐어 코딩) 적용을 하여야 하며, 시큐어 코딩 필수 항목(별표 9)에 대해 만족할 수 있게 개발되어야 한다.

제7조(기타) 정보누출 적발 시모든 책임은 해당용역 업체에서 책임을 지며, 부정당업자 제재 조치를 할 수 있다. <개정 2021.12.01.>

부 칙

이 시행세칙은 규정관리 위원회 심의의결 통과 후 지정일 부터 시행한다.

부 칙

이 시행세칙은 2021년 12월 1일부터 시행한다.

부 칙

이 시행세칙은 2022년 10월 1일부터 시행한다.

부 칙

이 시행세칙은 2023년 10월 16일부터 시행한다.

〔별표 1〕

〔 반출신청 및 확인서 〕

	담당	계장	팀장	처장
확인				

고 유 번 호 :
품 명 :
모 델 :
수 량 :
반 출 부 서 :
설치 장소(호실) :
Data 보안 조치 : □HDD분리 □중요자료삭제(HDD 미분리) □중요자료 없음
반 출 사 유 :

위의 장비를 반출하는 것을 확인하며 장비에 포함된 어떤 정보도 임의로 유출하지 않을 것을 확약합니다. 반출된 장비의 정보 유출로 인해 문제 발생 시 모든 책임을 지겠습니다.

년 월 일

회 사 명 :
직 위 :
연 락 처 :
성 명 : (서명)

상기 품목의 반출을 확인 합니다.

대원대학교 확인자 소속 : 성명 :
(서명)

〔별표 2〕

〔 용역업체 인터넷 접근 허용 요청 〕

순번	사용자		일시		용도	미디어팀 확인
	소속	성명	날짜	시간		

〔별표 3〕

〔 용역사업 보안위규 처리기준 〕

구 분	위 규 사 항	처 리 기 준
심 각 (A급)	1. 비밀 및 대외비 급 정보 유출 및 유출시도 가. 정보시스템에 대한 구조, 데이터베이스 등의 정보 유출 나. 개인정보 · 신상정보 목록 유출 다. 비공개 항공사진 · 공간정보 등 비공개 정보 유출 2. 정보시스템에 대한 불법적 행위 가. 관련 시스템에 대한 해킹 및 해킹시도 나. 시스템 구축 결과물에 대한 외부 유출 다. 시스템 내 인위적인 악성코드 유포	○ 사업참여 제한 ○ 위규자 중징계 ○ 재발 방지를 위한 조치계획 제출 ○ 위규자 대상 특별 보안교육 실시
중 대 (B급)	1. 비공개 정보 관리 소홀 가. 비공개 정보를 책상 위 등에 방치 나. 비공개 정보를 휴지통 · 폐지함 등에 유기 또는 이면지 활용 다. 개인정보·신상정보 목록을 책상 위 등에 방치 라. 기타 비공개 정보에 대한 관리소홀 2. 사무실 · 보호구역 보안관리 허술 가. 통제구역 출입문을 개방한 채 퇴근 등 나. 인가되지 않은 작업자의 내부 시스템 접근 다. 통제구역 내 장비 · 시설 등 무단 사진촬영 3. 전산정보 보호대책 부실 가. 업무망 인터넷망 혼용사용, 보안 USB 사용규정 위반 나. 웹하드 · P2P 등 인터넷 자료공유사이트를 활용하여 용역사업 관련 자료 수발신 다. 개발 · 유지보수 시 원격작업 사용 라. 저장된 비공개 정보 패스워드 미부여 마. 인터넷망 연결 PC 하드디스크에 비공개 정보를 저장 바. 외부용 PC를 업무 망에 무단 연결사용 사. 보안관련 프로그램 강제 삭제 아. 사용자 계정관리 미흡 및 오남용(시스템 불법접근 시도 등)	○ 위규자 중징계 ○ 재발 방지를 위한 조치계획 제출 ○ 위규자 대상 특별 보안교육 실시

구 분	위 규 사 항	처 리 기 준
보 통 (C급)	1. 기관 제공 중요정책 · 민감 자료 관리 소홀 가. 주요 현안 · 보고 자료를 책상위 등에 방치 나. 정책 · 현안자료를 휴지통 · 폐지함 등에 유기 또는 이면지 활용 2. 사무실 보안관리 부실 가. 캐비넷 · 서류함 · 책상 등을 개방한 채 퇴근 나. 출입키를 책상위 등에 방치 3. 보호구역 관리 소홀 가. 통제 · 제한구역 출입문을 개방한 채 근무 나. 보호구역내 비인가자 출입허용 등 통제 미실시 4. 전산정보 보호대책 부실 가. 휴대용저장매체를 서랍 · 책상 위 등에 방치한 채 퇴근 나. 네이트온 등 비인가 메신저 무단 사용 다. PC를 켜 놓거나 보조기억 매체(CD, USB 등)를 꽂아 놓고 퇴근 라. 부팅 · 화면보호 패스워드 미부여 또는 "1111" 등 단순숫자 부여 마. PC 비밀번호를 모니터옆 등 외부에 노출 바. 비인가 보조기억매체 무단 사용	○ 위규자 경징계 ○ 위규자 사유서 / 경위서 징구 ○ 위규자 대상 특별 보안교육 실시
경 미 (D급)	1. 업무 관련서류 관리 소홀 가. 진행 중인 업무자료를 책상 등에 방치, 퇴근 나. 복사기 · 인쇄기 위에 서류 방치 2. 근무자 근무상태 불량 가. 각종 보안장비 운용 미숙 나. 경보 · 보안장치 작동 불량 3. 전산정보 보호대책 부실 가. PC내 보안성이 검증되지 않은 프로그램 사용 나. 보안관련 소프트웨어의 주기적 점검 위반	○ 위규자 서면 · 구두 경고 등 문책 ○ 위규자 사유서 / 경위서 징구

[별표 4]

〔 보안 위약금 부과기준 〕

구분	위규 수준			
	A급	B급	C급	D급
위규	심각 1건	중대 1건	보통 2건 이상	경미 3건 이상
위약금 비중	부정당업자 등록	5백만 원 이하	3백만 원 이하	1백만 원 이하

〔별표 5〕

〔 누출금지 대상정보 〕

1. 기관 소유 정보시스템의 내·외부 IP주소 현황
2. 세부 정보시스템 구성현황 및 정보통신망 구성도
3. 사용자계정 · 비밀번호 등 정보시스템 접근권한 정보
4. 정보통신망 취약점 분석 · 평가 결과물
5. 용역사업 결과물 및 프로그램 소스코드
6. 국가용 보안시스템 및 정보보호시스템 도입 현황
7. 침입차단시스템 · 방지시스템(IPS) 등 정보보호제품 및 라우터 · 스위치 등 네트워크 장비 설정 정보
8. 「공공기관의 정보공개에 관한 법률」 제9조제1항에 따라 비공개 대상 정보로 분류된 기관의 내부문서
9. 「개인정보보호법」 제2조제1호의 개인정보
10. 「보안업무규정」 제4조의 비밀 및 동 시행규칙 제7조제3항의 대외비
11. 그 밖에 각급기관의 장이 공개가 불가하다고 판단한 자료

〔별표 6〕

〔 보안서약서 〕

1. 본인은 대원대학교(이하 “본 대학교” 이라 함)에서 _____ 용역 관련 업무 중 취득한 모든 정보를 업무에 한해 이용할 것이며, 계약기간, 퇴직 및 계약 종류 후에도 유출 또는 공개하거나 부정한 목적으로 사용하지 않을 것을 서약합니다.
2. 본인은 본 대학교로부터 제공받은 정보자산(서류, 사진, 전자파일, 저장매체, 전산 장비 등의 일체의 자산)을 무단변조, 복사, 훼손, 분실 등으로부터 안전하게 관리하겠습니다.
3. 본인이 알 필요가 없는 자(직원 고객 혹은 계약직 직원 등)에게 본 대학교 소유정보를 누설하지 않을 것이며, 업무상 알게 된 고객의 비밀 및 개인정보를 누설하지 않겠습니다.
4. 본인은 명백히 허가 받지 않은 정보나 시설에 접근하지 않으며, 본 대학교 관련 업무를 수행할 때만 교내 정보시스템을 사용하고, 이 시설에 본인의 사적 정보를 보관하지 않겠습니다.
5. 본인은 본 대학교에서 승인 받지 않은 프로그램, 정보저장 및 처리장치(모뎀, 외장 HDD, USB HDD등)를 본 대학교 내에서 사용하지 않겠습니다.
6. 본인은 본 대학교 소유 정보자산을 외부로 반출할 경우 본 대학교의 통제 절차를 준수할 것이며, 교내 통신망을 통해 수발신 되는 전자문서는 정보자산의 보호를 위하여 본 대학교차원에서 점검(발신통제 및 모니터링)할 수 있음을 인식하겠습니다.
7. 본인에게 할당된 사용자 계정 및 비밀번호, 네트워크 정보를 타인과 공동사용 또는 누설하지 않겠습니다.
8. 본인은 본 대학교의 보안규정 및 정책, 지침을 준수하겠습니다.
9. 본인은 퇴직 및 계약 종료 시 본 대학교에서 제공받은 본 대학교의 비밀과 관련된 모든 자료를 포함하여 본 대학교 소유의 모든 정보자산을 반드시 반납하겠습니다.

본인은 _____년 ___월 ___일부로 _____ 관련 용역사업(업무)을 수행함에 있어 상기 사항을 숙지하고 이를 성실히 준수할 것을 동의하며 비밀 유지 서약의 보안사항을 위반하였을 경우에는 민 · 형사상의 모든 책임 이외에도, 본 대학교의 관련 규정에 따른 징계조치 등 어떠한 불이익도 감수할 것이며 본 대학교에 끼친 손해에 대해 지체 없이 변상 · 복구할 것을 서약합니다.

년 월 일

서 약 자 소 속 회 사 :
직 위 :
성 명 : (서명)
연락처(핸드폰) :
연락처(사무실) :

〔별표 7〕

〔 자료관리 대장 〕

사 업 명 :

사업기간 :

사업회사 :

회사대표 :

연 락 처 :

※ 아래에 제공받은 자료에 대해서는 용역사업이 종료됨과 동시에 모두 삭제 하여야 합니다.

※ 제공받은 자료의 저작권이나 권리는 대원대학교에 있으므로 함부로 외부 유출 또는 본 사업 이외의 타 용도로 사용해서는 안 됩니다.

※ 만일 자료의 유출 또는 본 사업 이외의 타 용도로 사용 중 발생하는 민/형사상 문제는 용역사업 회사에서 일체 책임을 져야 하며 관련하여 대원대학교의 피해에 대해서는 손해배상을 하여야 합니다.

순번	자료명	자료크기(mb) 건수	제공일자 제공방법	수신자 성명 수신자 서명	제공자 성명 제공자 서명
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

〔별표 8〕

〔 확약서 〕

본인은 _____년 ___월 ___일부로 _____ 관련 용역사업(업무)을 완료함에 있어 귀 대원대학교로부터 전달받은 개발에 필요한 모든 자료(시스템 정보, 각종 아이디 / 비밀번호 등)에 대해 삭제 조치를 할 것이며 관련한 복사본이나 어떤 자료도 보관하지 않을 것을 다음과 같이 확약합니다.

1. 용역사업 수행관련 어떠한 자료도 보관하지 않는다.
2. 본인은 하도급업체를 통한 사업 수행에 대해서도 관련 자료를 회수 및 파기하여 문제가 발생하지 않도록 한다.
3. 본인이 위의 사항을 지키지 않아 발생하는 문제에 대해서는 관련 법령 및 계약에 따라 어떠한 처벌 및 불이익도 감수한다.

년 월 일

서 약 자 (업체 대표)
업 체 명 :
직 위 :
성 명 : (서명)
사업자등록번호 :

서 약 자 (작업책임자)
업 체 명 :
직 위 :
성 명 : (서명)
연락처(핸드폰) :
연락처(사무실) :

〔별표 9〕

〔 시큐어 코딩 필수 항목 〕

유형	내용	대표적인보안약점
1. 입력데이터 검증및표현	프로그램 입력 값에 대한 검증 누락 또는 부적절한 검증, 데이터의 잘못된 형식지정으로 인해 발생할 수 있는 보안약점	SQL삽입, 정수오버플로우, 크로스사이트스크립트(XSS)
2. 보안기능	보안기능(인증, 점근제어, 기밀성, 암호화, 권한관리 등)을 부적절하게 구현시 발생할 수 있는 보안약점	부적절한 인가허용, 중요정보 평문저장, 하드코드된 패스워드
3. 시간및상태	멀티 쓰레드 시스템 혹은 하나 이상의 프로세스가 동작되는 환경에서 시간 및 상태를 부적절하게 관리하여 발생할 수 있는 보안약점	경쟁조건, 제어문을 사용 하지 않는 재귀호출
4. 에러처리	에러를 처리하지않거나, 불충분하게 처리하여 에러정보에 중요 정보(시스템, 사용자정보 등)가 포함 될 때 발생할 수 있는 보안약점	오류상황 대응부재, 오류메시지를 통한 정보노출
5. 코드오류	타입 변환오류, 자원(메모리, 파일, 소켓)의 부적절한 반환등과 같이 개발자가 범할 수 있는 코딩오류로 인해 발생할 수 있는 보안약점	널포인터 참조, 부적절한 자원해제
6. 캡슐화	중요한 데이터 또는 기능을 불충분하게 캡슐화하였을 때 인가되지 않은 사용자에게 데이터누출이 가능해지는 보안약점	제거되지 않고 남은 디버거코드, 시스템 데이터 정보노출
7. API오용	의도된 사용에 반하는 방법으로 API를 사용하거나, 보안에 취약한 API를 사용하여 발생할 수 있는 보안약점	DNSlookup에 의존한 보안결정