한국사이버안보학회 2025 학술연구사업

제 안 요 청 서

2025. 3.

한국사이버안보학회
KACS

1. 사업 개요

가. 사업명: 한국사이버안보학회 2025 학술연구사업

나. 사업목적: 사이버안보 강화를 위한 전략·법·정책·기술 연구 수행

다. 사업기간: 계약체결일로부터 7개월

라. 사업내용: 하기 참조

마. 계약방법: 경쟁입찰(협상에 의한 계약)

2. 입찰 관련 사항

가. 입찰참가자격

본 사업 수행을 제안하는 자는 학회에 소속된 자에 한함

나. 사업자 선정방법

(1) 협상대상자 선정 및 계약체결 등은 협상에 의한 계약체결 기준 '기획재정부 계약예규'를 적용

(2) 제출된 제안서 평가를 위해 평가위원회를 구성하고 평가기준에 따라 평가 실시

(3) 제안서 평가위원의 명단과 점수는 공개하지 않으며, 제안자는 이에 대하여 이의를 제기할 수 없음

(4) 제안서 평가는 기술평가 기준에 의거 제안사항 전반을 종합적으로 고려하여 평가하되 세부 평가방법은 자체계획에 의함

(5) 기술평가 점수가 배점한도의 80% 이상인 제안 중 종합평점 1위부터 순위별로 협상을 진행하여 낙찰자를 선정. 단, 우선협상대상자와 협상이 성립될 경우 차순위 제안자와의 협상은 생략

(6) 평가위원들의 심사 결과를 산술평균하여 최종 점수에 반영

(7) 평점이 동일한 경우, 세부 평가 항목 중 배점이 큰 항목에서 더 높은 점수를 얻은 제안자를 선순위자로 선정

(8) 협상대상자가 제안한 제안서 내용을 대상으로 협상하고, 협상을 통하여 그 내용의 일부를 조정할 수 있으며, 협상완료 후 계약체결은 '협상에 의한 계약체결 기준' 제15조의 규정을 따름

3. 제안서 제출 안내 및 평가

가. 제출기한: 2025년 3월 27일(목) 23:59

나. 제출서류: 제안서(HWP 파일과 PDF 파일)

다. 제출방법: kacs@kacs.ne.kr

라. 평가기간: 2025년 3월 31일(월) ~ 2025년 4월 2일(수)
※ 제안서 평가가 지연될 경우, 협상을 연기할 수 있으며 해당 제안자에게 별도로 통보

마. 평가항목 및 배점: 기술평가(100점)

4. 제안요청 사항

가. 과업명: 한국사이버안보학회 2025 학술연구사업

나. 과업 주제: 총 20개

[전략연구분야]

(1) AI안보 거버넌스 체계 구축 방안

(2) 트럼프 2기 미국의 사이버안보 전략 및 대응 방안

(3) 디지털 전환과 한미일 사이버안보 협력

(4) 사이버 복합 넥서스: 최신 동향 파악과 대응 전략 모색

(5) 중견국의 사이버-AI 국가책략

(6) 한국형 사이버 3축체계 전략과 역량 구축 방향

(7) 미중경쟁시대의 사이버-AI 글로벌 안보 규범

[기술정책연구분야]

(1) N^2SF 기반 보안통제 기술 고도화

(2) 정보보호제품 암호 키 관리 적용사례 조사 및 보안 강화 기준 개발

(3) ICT·SW 제품 도입·운영 등에 관한 공급망 보안 실무안내서

(4) 양자내성암호 등 新기술 암호사용 촉진을 위한 암호모듈 검증방안 연구

(5) MITRE ATT&CK 기반 위협 분석 및 D3FEND 기반 대응 전략 연구

(6) 국가 망 보안체계(N^2SF) 구축시 보안대책 수립 적절성 평가 지표(안) 제시

(7) 국가망 보안체계(N^2SF)에 적용할 관리적 보안대책(안) 연구

(8) 클라우드 인프라 및 클라우드 네이티브 환경의 관리·운용 기술에 대한 보안 평가지표 개발

[법제도연구분야]

(1) 민간 보안진단 전문인력 자격제도 도입 법제 심화연구

(2) 한미일 사이버안보법제 비교분석

(3) 보안관리 수준 측정 등 민간 업무위탁 법제 검토

(4) 공공부문 사이버보안 강화를 위한 안전성 검증제도 설계 방안 (ICT/SW 안정성 & AI 안전성) 수요 통합

(5) 사이버전략과 공세적 대응 개념의 제도적 기반 조성방안

다. 세부 요청내용(20개 주제 중 택일하여 제안)

[전략연구분야]

	과제명 및 내용	예상 결과물
1	**AI안보 거버넌스 체계 구축 방안** - 現 사이버안보 거버넌스 체계하에서 AI안보 위협을 예방·대응하기 위한 법·제도 정비사항 식별 * 해외 주요국의 AI안보 거버넌스 체계 비교 - 향후 AI의 전방위적 확산 등 AI안보 패러다임 변화 예측을 토대로 국내 실정에 맞는 거버넌스 구축 방안 - AI 산업 경쟁력·AI 안전성·AI 신뢰성 개념과 비교하여 한국 실정에 맞는 AI 안보 개념 정립	연구보고서 - 現 사이버안보 거버넌스 체계에 AI안보 측면에서 고려해야 할 사항 분석 * 국내외 AI안보 거버넌스 현황 포함 - AI안보 패러다임 변화에 따른 거버넌스 구축방안 * 법·제도 정비사항 및 기관별 업무분장 등 포함
2	**트럼프 2기 미국의 사이버안보 전략 및 대응 방안** - 트럼프 2기 출범에 따른 △사이버안보 전략 및 정책 방향 분석 △각국의 대응 동향 파악 - 정치·경제·외교·국방 등 각 분야의 관점에서 미국의 사이버안보 정책이 미치는 영향 분석	연구보고서 - 트럼프 2기 행정부의 외교 및 국방 기조·對中전략·경제 정책 등을 중심으로 분석
3	**디지털 전환과 한미일 사이버안보 협력** - 한미일 3국은 은 북한 핵·WMD 개발에 자금을 조달하는 사이버 활동을 차단하고 국가배후 해킹 조직의 위협에 대응하는 방향으로 협력을 지속중 - 제4차 산업혁명이 국가안보전략의 수정·국가간 협력 방식의 변화 등 다양한 방식의 파급력을 발휘하는 디지털 전환 환경하에서 향후 한미일 사이버안보 협력 방안 모색	연구보고서 - 한미일 3국간 양자·다자 사이버협력 방식 고찰

4	**사이버 복합 넥서스 : 최신 동향 파악과 대응 전략 모색** - 사이버안보의 산업, 안보, 경제, 군사, 외교 분야와의 넥서스화에 대한 구체적 분석	연구보고서 - AI·공급망·암호화폐 등 사이버안보의 다양한 층위에서 발생하는 분야간 유기적 결합 및 연쇄작용에 초점을 둔 접근
5	**중견국의 사이버-AI 국가책략** - 각국의 사이버안보 정책에서 AI 관련 이슈의 비중이 커진 것을 계기로, 사이버와 AI를 망라한 국가별 대응 전략을 파악 - 이를 통해 우리 사이버안보 정책에 주는 시사점을 발견하고, 향후 국가사이버안보 전략 수립 참고 자료로도 활용	연구보고서 - 사이버-AI 정책에 대한 이론적 접근 - 美·日·中·러 등 주변국을 비롯한 해외 사례 연구 - 국가·권력·구조·규범 등 개념을 중심으로 한 전략 연구
6	**한국형 사이버 3축체계 전략과 역량 구축 방향** - 국제 및 국가 배후 해킹조직 등 국가사이버안보 위협 요인에 대응, △정책 수립 △민관협력 등 다양한 방면에서 공세적 방어 전략 수립 및 역량 강화 방안 모색	연구보고서 - 북한 등 위협행위자들의 국가사이버안보 위협행위를 능동적으로 확인·견제·차단하는 한국형 모델 제시
7	**미중경쟁시대의 사이버-AI 글로벌 안보 규범** - 美·中의 사이버 패권경쟁 속에서 세계 각국은 국제기구·지역협력체 등을 중심으로 공조·협력하여 사이버 위협에 대응하는 역량을 결집 - 사이버안보의 큰 틀 안에서 AI라는 새로운 화두의 등장으로 발생한 변화 양상을 진단하고, 향후 글로벌 거버넌스 모델에 미칠 영향력 분석	연구보고서 - 사이버안보라는 공동의 목표를 두고 세계 각국이 결집 또는 경쟁하는 상황에서 '안보 규범'의 변화 양상 연구

[기술정책연구분야]

	과제명 및 내용	예상 결과물
1	**N²SF 기반 보안통제 기술 고도화** o 위협분석 기법 추가 연구에 따른 위협 정의 및 보안대책 도출 - 위협분석 기법에 따른 보안위협 재정립 - 보안대책 정립에 따른 N2SF 보안통제 항목 추가 도출 o C/S/O 등급에 따른 영역 구분 및 관련 보안통제 항목 세분화 - 물리(L1·2)·논리적 분리(L3~7) 기반 보안통제 - 마이크로 세그멘테이션 기반 보안통제 - 트래픽 제어 기반 보안통제 - 제로트러스트 아키텍처 기반 보안 도메인간 보안통제 등	o 연구보고서 - 보안위협 목록 및 이에 따른 보안대책 - 등급별 영역 구분 방식에 따른 기술적 보안통제 항목
2	**정보보호제품 암호 키 관리 적용사례 조사 및 보안강화 기준 개발** o 정보보호제품의 암호 키 관리 적용사례 조사 - 부적절한 암호 키 관리 및 사용실태 분석 - 고수준 암호모듈 등 국내·외 암호 키 관리 전용 제품 기능 분석 o 암호 키 관리 강화를 위한 보안기준 개발 - 정보보호제품의 암호 키 관리 개선방안 도출 - 암호 키 관리 보안기준(案) 마련	o 연구보고서 - 국내·외 정보보호 제품 암호 키 관리 적용기술 현황 분석 - 제품·시스템의 암호 키 관리 보안기준(案)
3	**ICT·SW 제품 도입·운영 등에 관한 공급망 보안 실무안내서** o ICT·SW 제품 도입·운영(유지보수 등) 단계에서의 위협을 식별하고 위험관리 주체의 역할별로 필요한 공급망보안 요소를 도출 - ICT·SW 제품 도입시 공급망 위험평가·관리 요소 - 도입후 ICT·SW 제품이 조직내에서 안전하게 운영될 수 있도록 수행되어야 하는 공급망 위험관리 요소	o 연구보고서 - 공급망보안 실무안내서(案)

4	**양자내성암호 등 新기술 암호사용 촉진을 위한 암호모듈 검증방안 연구** o 주요국 양자내성암호 검증 정책 조사 및 세부 검증방안 도출 - 美·日·EU 등 양자내성암호 탑재 정보보호 제품에 대한 검증 정책 및 관련 제도 조사 - 양자내성암호 및 하이브리드 방식에 대한 세부 검증방안 연구 - 양자내성암호 도입을 활성화 하기 위한 제도적 지원방안 조사 o 속성·응용기반 암호 등 신규 암호기술 검증 필요성 연구 - 주요국의 신규 암호기술에 대한 도입·검증정책 조사 - 신규 암호기술 검증 필요성 및 제한 사항에 대한 연구	o 연구보고서 - 양자컴퓨터 등 新 ICT 환경을 고려한 암호모듈 검증정책 운용案
5	**MITRE ATT&CK 기반 위협 분석 및 D3FEND 기반 대응 전략 연구** o ATT&CK 기반 위협 시나리오 도출 연구 - 최신 사이버 공격 트렌드 및 위협 동향 조사 - ATT&CK 매트릭스를 활용한 주요 공격 기법 식별 및 사례 분석 - ATT&CK 기반 특정 조직(또는 시스템) 대상 위협 시나리오 도출 o D3FEND 기반 보안 대응 전략 연구 - ATT&CK 매핑을 활용한 D3FEND 보안 대응 기법 연구 - 주요 공격 기법에 대한 방어 기법 분석 및 효과성 검토 - 위협 시나리오별 대응 프로세스 연구 및 적용 방안 검토 o ATT&CK 위협 및 D3FEND 매핑 시각화 도구 개발 및 실제공격·대응사례 적용 - ATT&CK 및 D3FEND 매트릭스 기반 공격·방어 관계 매핑 기능 구현 - 공격 기법과 방어 기법 간의 상관관계를 시각적으로 표현하는 도구 개발 - 실제 해킹사례와 대응체계를 매핑하여 도구의 효율성 검증	o 연구보고서 및 SW

6	**국가 망 보안체계(N²SF) 구축시 보안대책 수립 적절성 평가지표(안) 제시** o 국가 망 보안체계 보안가이드라인에 정보서비스 모델이 공개되었으나 보안통제 선정·구현에 대한 적절성 평가 절차만 공개 중 - 이에 등급분류, 위협식별, 보안통제 선택에 대한 평가 방법론을 수립하여 보안 적절성 평가 세부 기준(체크리스트) 개발을 목표로 과제 진행 o 각급기관이 보안가이드라인 활용시 담당자의 이해를 돕고 자율적으로 정보서비스 모델 구축 및 보안대책 수립·평가할 수 있도록 방안 제시 * 평가 기준과 자가 점검표 등 제공 o 보안가이드라인의 단계별 적절성 평가(NSF-A-1) 항목을 토대로 단계별 산출물과 적절성 평가항목에 대한 점검지표 제안	o 연구보고서 - 좌측의 내용을 산출물에 포함
7	**국가망 보안체계(N²SF)에 적용할 관리적 보안대책(안) 연구** o C·S·O 등급별 정보시스템에 권고하는 관리적 보안대책 방안을 연구 제시하여 국가망 보안체계(N² SF)에 맞는 국가정보보안기본지침 개정에 활용토로 지원 - 기밀시스템상 온라인 개발 및 유지보수 등 유지보수 관리적 방안, 기밀/민감 시스템의 서버, 단말기 등에 비밀번호 관리, 시스템 운영체제 패치보안 관리 - C·S·O 등급별 시스템 위협 탐지 및 보안관제, 인공지능시스템 개발 운용시 보안관리, 등급별 암호사용 관리방안 등 강구	o 연구보고서

8	**클라우드 인프라 및 클라우드 네이티브 환경의 관리·운용 기술에 대한 보안 평가지표 개발** o 클라우드를 구축·사용·평가하는 기관이 클라우드 인프라 및 네이티브 환경의 관리·운영기술에 대해 안전성을 확인할 수 있도록 세부 평가지표 개발 o 클라우드 관리·운영플랫폼 보안기능 분석 - 국·내외 주요 클라우드사 제품 또는 오픈소스로 제공되는 CMP(Cloud Managemet Platform)·컨트롤러 등 대상 보안기능 분석 - 클라우드 관리·운영에 대한 공통 보안기능 도출 o 관리·운영플랫폼 보안기능을 활용한 보안대책 수립 및 평가지표 개발 -「국가 클라우드 컴퓨팅 보안 가이드라인」上 클라우드 인프라 및 클라우드 네이티브 환경의 관리·운영 관련 보안기준을 준수하기 위한 보안대책을 CMP·컨트롤러 등의 보안기능을 활용하여 수립 - 보안대책 이행을 위한 세부 설정법 등 사례 제시 - 보안대책 적용여부 확인을 위한 자체검진표 및 평가지표 개발	o 연구보고서 - CMP·콘트롤러 보안기능 분석 자료 - 가이드라인 통제항목 준수를 위한 세부 보안대책 - 보안대책 자체검진표 - 보안 평가지표

[법제도연구분야]

	과제명 및 내용	예상 결과물
1	**민간 보안진단 전문인력 자격제도 도입 법제 심화연구** - 제도 시행·운영을 위한 △법적근거 마련 방안 △산·학·연·관 각계 역할 정립 △예상 소요 판단 및 운영 방향 등 추가연구 필요 - 유사례 비교, 산·학·연·관 각계의 예상 입장 분석 및 협업방안 도출등을 통해 자격제도 시행을 위한 구체적인 액션 플랜을 마련 필요	연구보고서 - 자격제도 시행을 위한 △법적근거 방안 △산·학·연·관 각계 역할 및 지원 방안 △단·중장기 제도 운영 방안 등 구체적 액션 플랜 마련
2	**한미일 사이버안보법제 비교분석** - 일본 '사이버공격에 대한 능동적 대응' 을 위한 관계 법령안 발의 계기, 한미일 사이버안보법제 비교·분석 및 우리나라 법제 개선방향에 대한 제언 * 우리나라의 경우 사법경찰과 행정경찰 기능이 구별되는 점을 고려하여 금번 제개정되는 일본 법안의 경찰의 통신조치를 국내에서 벤치마킹하여 법제화할 경우 수사경찰 조직이 아닌 보안기관이 수행토록 하는 방안에 대한 타당성 연구 필요	연구보고서 - 일본에서 발의된 법안에 대한 상세한 분석, 일본의 금번 법제도 정비에 따른 미국과의 협력 체계의 예상되는 변화 및 이에 따른 우리나라에도 필요한 법제 정비 등
3	**보안관리 수준 측정 등 민간 업무위탁 법제 검토** - 사이버안보 업무규정 제9조 제5항에 따른 보안관리 수준 측정 업무와 관련하여 아래와 같은 업무 수행 형태간 비교 연구 * (일부 민간위탁) 정보통신기반보호법에 따른 정보보호 전문서비스 기업이 참여하는 취약점 분석·평가 형태로 일부 업무를 위탁하고 국가정보원이 추후 확인하는 형태 * (협회) 산업기술보호법에 근거한 산업기술보호협회 대상 실태조사 등 업무 위탁 방식 * (출연기관) 방산기술보호법에 따라 전담기관을 지정하여 사이버 취약점 점검 업무 위탁 방식 * 기타 미국·유럽 등 해외 사례	연구보고서 - 국내·해외 사례 및 제도별 장·단점 및 관련 정책·법제화 추진 방안 등

4	**공공부문 사이버보안 강화를 위한 안전성 검증제도 설계 방안(ICT/SW 안정성 & AI 안전성) 수요 통합** **o ICT/SW 안정성 부분** - 美·日·유럽 등 사이버보안 주요국의 공공분야 ICT·SW 제품 도입을 위한 적합성 인증·검증 제도 및 관련 법을 분석하고, 국내 실태와 비교 - 공공분야 ICT·SW 제품 조달 관련 법·규정을 면밀 분석하고, 안전성이 검증된 제품을 도입·운영하도록 제한하는 법적 근거 도출 - 공급망 보안 측면에서 국내 ICT·SW 제품 안전성 인증·검증을 통합하는 체계 제안 **o AI 안전성 부분** - 국가·공공기관이 도입·운용하는 AI 시스템·서비스 대상 안전성 확인 방법·절차·법제정비 등 방안수립	**o ICT/SW 안정성 부분** - 연구보고서 : 공공분야에 도입(조달)·운영되는 ICT·SW 제품 대상 적합성 검증 관련 국내외 既 시행 법·제도를 분석하고, 공급망보안 등 급변하는 사이버안보 환경에 맞춰 효율적으로 통합·운영할 수 있는 법·제도 기반 마련 **o AI 안정성 부분** - 연구보고서 : AI 시스템 안전성 확인 절차·법제정비 방안 등 - 체크리스트 : AI 시스템 안전성 확인 시 물리·관리·기술적 방법 체크리스트
5	**사이버전략과 공세적 대응 개념의 제도적 기반 조성방안** - 공세적 대응의 개념 범주를 정립하고, 주체별/유형별 수행 절차를 분석하며, 이를 수행하기 위한 우리나라·주요국의 법적 근거를 조사 및 비교·분석하여 입법 체계 정비 방안 마련 * 공세적 대응 후 행위자의 행위가 정당행위에 해당하여 면책될 수 있는지 등도 포함	연구보고서 - 공세적 대응의 이론적 개념화 및 유형 분류, 수행절차 및 면책 방안 수립 및 입법 제언 등

다. 과업 예산

분야	주제	예산 (단위 : 만원)
국가 전략	① AI안보 거버넌스 체계 구축 방안	3,000
	② 트럼프 2기 미국의 사이버안보 전략 및 대응 방안	3,600
	③ 디지털 전환과 한미일 사이버안보 협력	2,000
	④ 사이버 복합 넥서스 : 최신 동향 파악과 대응 전략 모색	2,750
	⑤ 중견국의 사이버-AI 국가책략	3,950
	⑥ 한국형 사이버 3축체계 전략과 역량 구축 방향	2,000
	⑦ 미중경쟁시대의 사이버-AI 글로벌 안보 규범	2,000
기술 정책	① N^2SF 기반 보안통제 기술 고도화	4,000
	② 정보보호제품 암호 키 관리 적용사례 조사 및 보안강화 기준 개발	4,000
	③ ICT·SW 제품 도입·운영 등에 관한 공급망 보안 실무 안내서	4,000
	④ 양자내성암호 등 新기술 암호사용 촉진을 위한 암호모듈 검증방안 연구	4,000
	⑤ MITRE ATT&CK 기반 위협 분석 및 D3FEND 기반 대응 전략 연구	4,000
	⑥ 국가 망 보안체계(N^2SF) 구축시 보안대책 수립 적절성 평가지표(案) 제시	4,000
	⑦ 국가망 보안체계(N^2SF)에 적용할 관리적 보안대책(案) 연구	4,000
	⑧ 클라우드 인프라 및 클라우드 네이티브 환경의 관리·운용 기술에 대한 보안 평가지표 개발	4,000
법제도	① 민간 보안진단 전문인력 자격제도 도입 법제 심화연구	5,000
	② 한미일 사이버안보법제 비교분석	3,000
	③ 보안관리 수준 측정 등 민간 업무위탁 법제 검토	5,000
	④ 공공부문 사이버보안 강화를 위한 안전성 검증제도 설계 방안(ICT/SW 안정성 & AI 안전성) 수요 통합	6,000
	⑤ 사이버전략과 공세적 대응 개념의 제도적 기반 조성방안	4,000

5. 제안서 작성 지침

가. 제안서 작성일반

(1) 제안자는 제안요청서에 제시된 제안서 목차와 제안서 작성방법을 준용하여 작성

(2) 제안서는 한글 작성이 원칙임

(3) 제안서의 모든 내용은 객관적으로 입증될 수 있어야 하며, 그 내용이 허위로 확인될 경우 또는 발주처의 입증 요구를 충족하지 못하는 경우는 평가대상에서 제외됨

(4) 제출된 제안서의 내용은 발주처가 요청하지 않는 한 변경할 수 없으며, 계약체결 시의 계약조건의 일부로 간주함

(5) 발주처는 필요시 입찰참가자에 대하여 추가제안이나 추가자료를 요청할 수 있으며, 이에 따라 제출된 자료는 제안서와 동일한 효력을 가짐

(6) 계약 후 제안서의 내용이 허위로 작성한 사실이 발견되거나 제안된 내용을 충족시키지 못할 경우 제안자는 일체의 손해배상 책임을 져야 함

나. 제안서 작성요령

(1) 제안서 목차

I. 연구과제 개요

1. 연구목적 및 내용

2. 연구수행 일정 및 주요 사항

II. 참여연구진

1. 연구수행책임자

가. 인적사항

나. 연구수행 실적

다. 연구논문 발표실적

2. 연구원

III. 예산내역서

(2) 제안서 작성방법

작성항목	작성방법
I. 연구과제 개요	
1. 연구목적 및 내용	본 사업의 제안 내용을 명확하게 이해하고, 본 제안의 목적과 연구의 주요 내용을 기술
2. 연구수행 일정 및 주요 사항	연구수행 기간, 주요 활동, 연구진 구성, 연구수행 일정을 제시
II. 참여연구진	
1. 연구수행책임자	
가. 인적사항	소속, 직위, 연락처, 학력, 경력 등을 제시
나. 연구수행 실적	지난 3년간 수행한 연구수행 실적
다. 연구논문 발표실적	지난 3년간 발표한 연구논문 실적
2. 연구원	소속, 직위, 학력, 연락처 등
III. 예산내역서	
1. 인건비	2024년 학술연구용역 인건비 기준단가에 준하여 참여율 계상
2. 경비	항목별 경비 예산액과 산출 근거 제시

다. 제안서의 효력 및 유의사항

(1) 제안서의 효력

(가) 제안서 제반 내용은 계약서와 동일한 효력을 가진다. 단, 계약서에 명시한 경우는 계약서 사항이 우선함

(나) 제안서 평가시 제안사항에 대한 보조 질문에 응하여야 하고 응하지 않음으로써 발생하는 불이익은 제안자의 책임

(다) 제안자는 필요시 제안사항에 대하여 추가 계획 또는 자료를 요청받을 수 있으며, 이에 따라 제출된 자료는 제안서와 동일한 효력을 가짐

(2) 유의사항

(가) 본 제안과 관련된 일체의 소요비용은 입찰참가자의 부담으로 함

(나) 제안자는 본 사업에 대한 제반사항을 사전에 충분히 숙지하고 제안에 임한 것으로 간주함

(다) 제안내용에 대한 확인을 위하여 추가 자료 요청 또는 현지 실사를 할 수 있으며, 입찰참가자는 이에 응하여야 함

(라) 사업자는 전체적 사업 수행에 대한 권한을 갖고 모든 책임을 짐

(마) 본 사업을 위해 사업자는 전체 인력에 대한 인력 및 구체적인 업무분담 및 활용방안을 제시하여야 함

(바) 과제 수행 완료 후 사업 수행결과가 불량한 경우 향후 당사 추진 사업의 참여에 제한받을 수 있음

(사) 제안자 간 담합하여 제안할 수 없으며, 담합 사실이 발견될 경우 독점규제 및 공정거래에 관한 법률 등 관련 법률에 의거 제재

라. 기타사항

(1) 발주처의 조치나 기타 불가항력적인 환경변화로 본 제안서의 일부 또는 전부가 변경되거나 취소되는 경우라도 제안자는 이의를 제기할 수 없음

(2) 추가 자료 요청시 제안자는 이에 성실히 임하여야 하며, 미제출시 불이익에 대한 책임은 제안자가 짐

(3) 제안서 평가는 발주처의 평가기준에 의하며, 제안사는 결과에 대해 일체의 이의를 제기할 수 없으며 세부적인 평가항목 및 결과는 공개하지 않음

(4) 제안요청서에 대한 문의는 한국사이버안보학회 사무국(kacs@kacs.ne.kr)으로 할 수 있음

5. 제안서 평가 방법

가. 평가 방법

(1) '협상에 의한 계약체결기준'에 의하여 기술평가 점수가 배점한도의 80% 이상인 자를 협상적격자로 선정하며, 협상적격자 중 고득점 순으로 협상에 임함

(2) 평가결과에 대하여 제안업체는 이의를 제기할 수 없으며, 평가항목 및 제안서에 기재되지 않은 사항은 평가하지 아니함

나. 기술 평가

부문	평가 항목	평가요소	배점 기준
기술점수	사업 추진계획	제안서가 본 사업의 성격과 취지에 적합한가?	10점
		제안하는 범위가 사업의 내용과 일치하고 적절한가?	10점
		제안 내용이 실현 가능하게 계획되었는가?	10점
		추진 전략에 창의성이 있고 특징이 있는가?	5점
		필요한 인력 및 시설, 기자재의 투입이 적절하게 계획되었는가?	10점
	수행 및 관리	사업 수행 일정 및 절차가 적절하게 계획되었는가?	10점
		단계별 계획을 구체적으로 제시하였는가?	5점
		일정관리, 산출물 관리 등 사업수행에 필요한 관리 방법론이 구체적으로 제시되었는가?	5점
		목표 산출물 도출과 관련하여 제약조건을 극복하기 위한 방안이 수립되었는가?	5점
	전문성	투입인력이 본 사업 수행에 있어 전문성을 보유하고 있는가?	10점
		투입인력이 본 사업과 유사분야 사업에 참여한 실적이 있는가?	10점
	사후 관리 및 기타	사업 종료 후 협조 및 지원 계획을 적절하게 계획하였는가?	5점
		사업 추진 동안 기밀을 보호하면서 수행의 원활성을 보장하기 위한 대책을 제시하였는가?	5점