비금전형 사이버 협박의 위협 모델과 통합 대응 프로토콜 : 대응 지연과 청소년 표적 시나리오를 중심으로

박민수*, 한승재*, 황성민*, 이하늘*, 김창훈**

대구대학교 (학부생, 교신저자**)

A Threat Model and Integrated Response Protocol for Non-Monetary Cyber Extortion : Focusing on the Response-Latency Gap and Youth-Targeting Scenarios

Min-Su Park*, Seung-Jae Han*, Seong-min Hwang*, Ha-neul Lee*, Chang-Hoon Kim**

*Daegu University(Undergraduate Student, **Corresponding Author)

요 약

본 연구는 금전이 아니라 행위적·심리적 복종을 요구하는 '비금전형 사이버 협박'을 지렛대와 복종 요구의 결합으로 정의하고, 문헌과 대응 지침에서 위협 요소를 추출해 공격 과정을 유인·수집·협박·실행의 네 단계로 구조화한다. 주된 취약점은 개별 방어 기술의 부재보다 대응 착수가 지연되는 절차적 공백과 대응 수단이 단계별로 연계되지 못하는 통합의 공백에 있다. 이에 수사 착수에 의존하지 않고 초기 보호를 전면화하는 통합 대응 프로토콜－비처벌·정보 최소화 기반 안심 접수와 단계별 초동 대응 순서－을 제안한다. 본 연구는 효과를 실증한 것이 아니라 문헌에 근거한 탐색적·방어적 위협 모델링이라는 한계를 갖는다.

I. 서론

사이버 협박 연구와 대응 체계는 오랫동안 금전 갈취 동기와 성인 피해자를 중심으로 축적되어 왔다. 그러나 실무에서는 금전이 아니라 특정 행위·자해·타인 유인·콘텐츠 생성·관계 훼손 등 행위적·심리적 복종을 요구하는 사례가 관찰되며, 이러한 비금전형 협박은 기존 성착취·금전 갈취 정의의 바깥에 있어 개념적·제도적으로 충분히 포착되지 못하였다.

여기에 두 변화가 결합될 수 있다. 대규모 언어모델과 자동화의 성숙으로 협박의 개인화 비용이 낮아질 수 있고, 청소년이 구조적으로 취약한 표적이 된다는 점이다. 디지털 성범죄 피해자 중 10대 비중 상승과 청소년 사이버폭력 경험률(2025년 42.3%) 등은 청소년 대상 온라인 위해의 저변을 보여주는 배경 지표이다[1][2]. 국외 연구는 비금전형 강요의 실재를 뒷받침한다. Wolak 등[3]은 미성년 피해 표본(n=572)에서 가해자 요구가 성적 이미지·특정 행위·자해 등으로 나타난 반면 금전 요구는 4.0%에 그쳐 요구가 금전에 국한되지 않음을 보고하였고(비확률 표본이므로 정성적 근거로만 인용), Europol[4]은 아동 대상 온라인 성적 강요를 기존 범죄 기록 체계가 충분히 포착하지 못한다고 지적하였다. 다만 이들 근거는 성적 강요에 한정되며, 비성적 강요는 본 연구가 개념적으로 확장한 영역이다.

제도적으로 국내 사이버범죄는 대응이 지연될 수 있는 구조에 있다. 검거율 하락 추세[5]와 수사 인력 부담[6]은 착수 속도를 직접 측정한 것은 아니나 대응 역량의 구조적 압박을 시사하는 정황 자료로, 방어 설계가 감당할 제약 조건으로 취급한다.

본 연구는 개별 구성요소의 존재와 결합 가능성에 근거한 탐색적·방어적 위협 모델링이다. 연구 질문은 (RQ1) 비금전형 협박은 금전형 협박·사이버불링과 어떤 구조적 차이를 갖는가, (RQ2) AI 자동화·익명화는 그 비용·규모·개인

화를 어떻게 바꿀 수 있는가, (RQ3) 대응 지연 조건에서 기존 수단을 어떤 순서와 책임 구조로 통합해야 하는가이다.

본 연구는 비금전형 사이버 협박을 조작적으로 정의하고, 네 단계로 위협 과정을 구조화하여 대응 지연 공백을 규명하며, 판정 4요건·지렛대 영향력 3차원(접근·확산·심리)·수사 독립 초기 보호 개시 원칙을 통해 통합 대응의 설계 원리를 도출한다.

II. 선행연구 및 개념 정의

2.1 유사 개념과의 구분

비금전형 협박은 인접 개념과 부분적으로 겹치지만 동일하지 않다. 여기서 지렛대란 가해자가 확보하였거나 확보했다고 주장하는 정보·이미지·계정 접근권·사회적 관계 등, 피해자를 압박하는 수단을 말한다. <표 1>은 지렛대 필요 여부·요구 내용·관계 형성·금전 요구를 기준으로 인접 개념을 방어자 관점에서 정리한 것이다.

<표 1> 인접 개념과 비금전형 사이버 협박의 비교

개념	지렛대 필요	요구 내용	관계 형성	금전 요구	본 연구와의 관계
금전형 사이버 협박	필요	금전 지급	필수 아님	중심	요구 목적에서 구분
성착취 협박	필요	금전·추가 이미지·성적 행위 등	필수 아님	선택적	비금전형 협박의 하위 사례가 될 수 있음
그루밍	필요 (형성 단계)	신뢰 형성 후 착취	필수	선택적	유인·수집 단계과 중첩
강압적 통제	필요	관계 내 지속적 복종	필수	드묾	요구 지속성에서 유사, 범위에서 구별
사이버 불링(cyberbullying)	불요	괴롭힘·평판 훼손	선택적	없음	지렛대 없이 성립하여 구분
비금전형 협박 (본 연구)	필요	금전 이외 행위적·심리적 복종	선택적	없음	지렛대와 비금전 복종 요구의 결합

2.2 조작적 정의와 판정 규칙

본 연구에서 비금전형 사이버 협박은 위와 같은 지렛대를 이용해 금전 지급 이외의 행위적·심리적 복종을 요구하는 행위를 의미하며, 핵심 구조는 지렛대와 복종 요구의 결합이다. 다음 네 요건을 모두 충족하는 경우를 비금전형 협박으로 분류한다. (i) 공격자가 실제 또는 주장된 지렛대를 제시하고, (ii) 그 공개·악용·확산 가능성을 명시적·묵시적으로 전달하며, (iii) 금전 이외의 특정 행위·부작위 또는 심리적 복종을 요구하고, (iv) 요구와 불이익 사이에 조건적 연결이 존재한다. '심리적 복종'은 이 조건적 연결이 성립하는 경우로 한정하며, 연결이 없는 정서적 괴롭힘이나 일반적 스토킹은 제외한다. 금전 요구와 비금전 요구가 병존·전환되는 경우는 혼합형, 자료가 없음에도 보유를 허위 주장하는 경우는 허위형으로 구분한다.

2.3 복종 요구의 유형

복종 요구는 행위 요구, 부작위 요구, 자기 위해 요구, 관계적 복종, 표현적 복종으로 구분되며, 유해 행위의 세부 실행 절차는 연구 윤리상 범주 수준에서만 기술한다.

III. 연구방법

3.1 연구 설계와 자료 범위

본 연구는 실증 분석이 아니라 공개 문헌과 대응 지침의 위협 요소를 방어자 관점에서 재구성하는 탐색적·방어적 위협 모델링이다. 분석 자료는 (i) 성착취 협박·그루밍 등 인접 현상에 관한 학술 문헌[3][4], (ii) 공공기관의 침해사고 대응 및 디지털 성범죄·아동 보호 지침[1][7], (iii) 대규모 언어모델·자동화 위협에 관한 산업·기관 자료[8]로 한정하였다. 자료 선정은 체계적 문헌고찰이 아니라 목적표집(purposive sampling)으로, 정부·국제기구·표준·동료심사 등 공신력 있는 1차 자료를 포함하고 언론 보도·2차 요약은 배경 확인 용도 외에는 제외하였다.

3.2 분석 절차와 기존 지침과의 대조

문헌에서 위협 요소와 대응 수단을 추출하여 '지렛대 - 복종 요구' 구조로 범주화하고, 공격 진행에 따라 네 단계로 배열한 뒤 기존 대응 수단을 연결하여 대응 지연 공백을 식별하였다. 도출된 단계 별 구조와 통제는 NIST 침해사고 대응 권고[7] 등 기존 지침과 개념적으로 대조하였으며, 항목별 형식적 대응표 작성은 향후 과제로 남긴다.

3.3 연구 윤리와 범위 제한

공격 재현에 이용될 수 있는 세부 절차(표적 선정, 자동화 구성, 지속·은닉 기법, 구체적 강요 지시 등)는 서술에서 배제하고, 각 단계는 관찰 가능한 신호와 대응 지점 수준에서만 기술하였다.

IV. 위협 모델

4.1 공격 전개의 네 단계

위협 과정은 <표 2>와 같이 유인·수집·협박·실행의 네 단계로 구분한다. 이 구조는 시스템 침투 단계를 분해하는 사이버 킬체인과 달리 공격 목적이 피해자의 복종 행동으로 실현되는 과정을 방어 지점 중심으로 재구성한 것이다. 킬체인이 정찰·초기 접근·자료 수집·목적 실행으로 이어지는 데 비해 본 모델의 축은 지렛대 확보와 복종 요구의 결합이며 이에 대응되는 킬체인 단계는 존재하지 않는다. STRIDE나 공격 트리 같은 형식적 기법을 적용한 것은 아니며, 방어 지점을 조직화하기 위한 경량의 위협 모델이다. 다만 이는 선형 모형이 아니라 일부 단계가 생략·반복·병합되거나 금전형 요구로 전환될 수 있는 분석적 구조이다. 실행 단계의 위해는 대인 피해에 국한되지 않고 기물·표현물 훼손과 같은 파괴적 행위로 확장될 수 있으며, 이 경우 개별 피해가 저강도로 분산되어 위해도 판정에서 과소평가되기 쉽다.

<표 2> 네 단계와 예상되는 대응 공백

단계	대표적 위협 징후	예상되는 탐지·대응 공백
1. 유인	청소년 관심사와 결합된 위장 접근(게임 관련 비인가 프로그램 위장 등)	행위의 위험성을 기기·계정 침해와 연결하지 못함
2. 수집	개인정보에서 가족·직장 정보로의 점진적 확장	장기·저용량 접근이 단발 이벤트로 포착되지 않아 계정 단위 연계 탐지가 필요함
3. 협박	지렛대 제시와 금전 이외 복종 요구의 전달	비금전·비성적 요구가 기존 협박 범주에 포착되지 않음
4. 실행	요구 이행 또는 위해 실현 (대인 피해 및 기물·표현물 훼손 등)	가시적 금전·성적 피해가 없어 위해도 판정에서 과소평가되기 쉬움

4.2 AI 개입의 수준

AI 자동화의 함의는 '24시간 반복 발신'이라는 양적 확대에 국한되지 않는다. 반복 발신·규칙 응답은 전통적 스크립트로도 가능하며, 질적 변화의 핵심은 개인화된 압박의 비용을 낮출 수 있다는 우려에 있다[8]. 본 연구는 AI 개입을규칙 기반 자동화, AI 보조, 개인화, 최적화의 네 수준으로 구분한다. 규칙 기반 자동화와 AI 보조는 문헌에서 우려가 제기된 수준이고 개인화는 그 연장선이며, 완전 자율형 최적화는 공개된 실증이 부족하므로 미검증 고위험 가정으로 취급한다. 한편 익명화 수단은 가해자 귀속을 어렵게 하여 수사 착수를 지연시키며, 이는 대응 지연 공백을 심화한다.

4.3 대응 지연 공백

비금전형 협박은 즉시 가시화되지 않아 가시적 피해가 큰 사건에 밀려 후순위가 되기 쉽다. 검거율 하락[5]·수사 인력 부담[6]의 제약 아래 방어 프로토콜은 신속한 수사 착수를 전제할 수 없으므로, 초기 보호는 수사와 독립적으로 신고 즉시 개시되도록 설계되어야 한다. 이 원칙은 제Ⅵ장 통합 대응 프로토콜의 설계 근거가 된다.

V. 청소년 표적의 구조적 취약성

청소년이 비금전형 협박의 표적이 되는 이유는 세 가지다. 또래 평가 민감성과 보상·결과 형량의 한계로 유인·강요에 취약하고[9][10][11], 노출 공포가 신고를 억제해 피해 청소년의 상당수가 피해를 알리지 않으며[2] 2차 피해 우려[12]가 이를 강화하고, 보호자 고지는 부모의 기기·계정·직장 정보를 추가 지렛대로 편입시키는 한편 지원 체계 인지도 낮다[13]. 이 세 요인은 각각 유인·협박·실행 단계의 표적화·신고 지연·지렛대 확보에 대응하므로, 초기 지원은 비처벌 응대와 정보 최소화를 전제하고 보호자 고지와 분리 가능하게 설계되어야 한다.

VI. 통합 대응 프로토콜 및 결론

본 장은 새로운 단일 기술이 아니라 기존 수단을 조합·체계화하되 초기 보호를 수사와 독립적으로 개시하도록 설계한다. 새로 제시하는 요소는 지렛대 영향력의 세 차원 축소(접근·확산·심리), 수사 독립 초기 보호 개시, 비처벌 안심

접수의 단계별 배열이다. 여기서 지렛대 영향력의 세 차원은 다음과 같다. 접근(access)은 공격자가 확보한 계정·기기·정보에 대한 접근 경로로 계정 보호와 기기 침해 차단으로 축소하고, 확산(diffusion)은 지렛대가 제3자에게 노출·유포될 가능성으로 삭제 지원과 플랫폼 조치로 축소하며, 심리(psychological)는 피해자가 지각하는 압박의 강도로 비처벌 응대와 허위형 판별로 축소한다. 초동 대응 순서는 이 세 차원을 동시에 낮추도록 수단을 배열한 것으로 기존 수단의 단순 나열과 구별된다.

단계별로는 유인에서 위험 경로를 합법적 실습으로 전환하고, 수집에서 초기화보다 연결 차단·조작 최소화 후 전문기관에 인계하며[7], 협박에서 플랫폼 정형 발신 탐지와 계정 보호·삭제 요청·지렛대 축소를 병행하고, 급박한 위해 시 수사기관·긴급보호가 병행 개입해 증거 우선의 보호 지연을 막으며, 안전 확보 후 상담·계정 복구·재접촉 감시로 전환한다. 피해자 지원은 가능한 범위에서 가족 고지와 분리하며, 비처벌 접수는 최소 정보만 수집하고 규정 위반과 피해자 보호를 분리하여 아동·청소년은 신고 없이도 일부 삭제 지원이 개시될 수 있다[1]. 보호자 고지·기업 통보는 관련 법령[14]과 피해자 의사를 검토해 최소 범위로 판단한다.

주된 공백은 방어 기술 부재보다 대응 지연의 절차적 공백과 수단 미연계의 통합 공백에 있으며, 본 연구는 저비용 절차 개선으로 이를 완화하는 설계 원리와 '비금전형 협박 대응 지침' 제도화를 제언한다. 본 연구는 다음의 한계를 갖는다. 첫째, 효과를 실증한 것이 아니라 공개 문헌에 근거한 탐색적·방어적 위협 모델링으로, 체계적 문헌고찰이나 전문가 델파이를 수행하지 않았다. 둘째, 근거의 상당 부분이 성적 그루밍·강요 맥락에서 축적된 것이어서 비성적·비금전형 협박으로의 확장은 유추를 포함하며, AI 개입에 관한 논의 역시 인접 위협에 대한 경고에서 유추한 것으로 비금전형 협박에 대한 직접 관측은 아니다. 셋째, 문헌 기반 연구로서 선택 편향과 규모 미실증의 한계가 있다. 이러한 한계는 향후 신고 시간·계정 회복·분류 일치도·기관 인계 성공률을 지표로 한 실증으로 보완한다.

Acknowledgements

본 논문은 과학기술정보통신부 및 정보통신기획평가원의 'SW중심대학사업'의 지원을 받아 제작되었습니다. (2025-0-00077)

[참고문헌]

[1] 성평등가족부·한국여성인권진흥원, "디지털성범죄 피해자 지원 보고서," 중앙 디지털성범죄피해자 지원센터, 2025.

[2] 방송통신위원회·한국지능정보사회진흥원, "사이버 폭력 실태조사," 2025.

[3] J. Wolak, D. Finkelhor, W. Walsh, and L. Treitman, "Sextortion of Minors: Characteristics and Dynamics," Journal of Adolescent Health, vol. 62, no. 1, pp. 72-79, 2018.

[4] Europol, "Online Sexual Coercion and Extortion as a Form of Crime Affecting Children," 2017.

[5] 경찰청, "사이버범죄 발생 및 검거," 국가지표체계(원자료: 경찰청 사이버범죄통계), 2025.

[6] 정웅, "경찰서 사이버수사팀의 적정 인력 및 업무량 추정," 경찰학논총, 제13권 제2호, pp. 69-95, 2018.

[7] A. Nelson, S. Rekhi, M. Souppaya, and K. Scarfone, "Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile," NIST SP 800-61 Rev. 3, 2025.

[8] Europol Innovation Lab, "ChatGPT: The Impact of Large Language Models on Law Enforcement," 2023.

[9] L. Steinberg, "A Dual Systems Model of Adolescent Risk-Taking," Developmental Psychobiology, vol. 52, no. 3, pp. 216-224, 2010.

[10] L. H. Somerville, "The Teenage Brain: Sensitivity to Social Evaluation," Current Directions in Psychological Science, vol. 22, no. 2, pp. 121-127, 2013.

[11] H. Whittle, C. Hamilton-Giachritsis, A. Beech, and G. Collings, "A Review of Young People's Vulnerabilities to Online Grooming," Aggression and Violent Behavior, vol. 18, no. 1, pp. 135-146, 2013.

[12] 김호겸, "아동·청소년을 대상으로 한 디지털 성범죄의 실태 및 피해자 지원 방안," 법과정책연구, 제23권 제4호, pp. 83-114, 2023.

[13] 장근영, 임지연, "아동·청소년 대상 디지털 성범죄 현황 및 대응방안 연구," 한국청소년정책연구원, 2021.

[14] 개인정보 보호법, 법률 제20897호, 2025. 4. 1. 일부개정, 2025. 10. 2. 시행.