



제433회국회(임시회)
제1차 정무위원회

전자금융거래법 일부개정법률안

검 토 보 고

〈 악성코드 투입 행위 금지 명시 〉

■ 김정호의원 대표발의(의안번호 제2213815호)

2026. 3.

정 무 위 원 회
수석전문위원 정 명 호

목 차

I . 제안경위	1
II . 제안이유 및 주요내용	1
III . 검토의견: 악성코드 투입 행위 금지 명시	3

I. 제안경위

1. 제 안 자 : 김정호의원 등 13인
2. 제 안 일 : 2025. 10. 30.
3. 회 부 일 : 2025. 10. 31.

II. 제안이유 및 주요내용

현행법은 금융회사 및 전자금융업자(이하 “금융회사등”이라 한다)가 전자적 침해행위로 인하여 전자금융기반시설이 교란·마비되는 등의 사고(이하 “침해사고”라 한다)가 발생한 경우 금융위원회에 이를 지체 없이 통지하고, 침해사고 발생 시 원인분석 및 피해 확산 방지 조치를 하도록 하고 있음.

그런데 현행법 규정은 침해사고 발생 유형에 악성코드 감염 여부를 포함하지 않고 있어 금융회사등은 고객정보 유출이나 서비스 장애가 발생하지 않았다는 이유로 악성코드 감염에 대하여 보고하지 않고 있음. 현재 금융회사등은 1만 명 이상 고객 신용정보 유출, 전산장애 등 가시적 피해가 발생하고 나서야 비로소 금융위원회에 보고를 실시하고 있으며 이는 악성코드 감염 사고에 대한 조기 대응의 어려움으로

이어지고 있음. 해외의 경우 미국은 CISA를 통해 전파되는 악성코드를 조기 발견하고 시스템 침투 등 발생 가능한 중대한 위험에 대해 대응하도록 권고하고 있으며, EU는 GDPR 배포를 통해 악성코드 대응 대책을 제시하고 있음.

이에 전자금융업무의 안전성에 중대한 영향을 미칠 수 있는 악성코드 감염을 침해사고의 유형으로 명시함으로써 악성코드 감염에 신속하게 대응하고 전자금융거래 이용자를 보호할 수 있도록 하고자 함(안 제21조의4 및 제49조).

Ⅲ. 검토의견: 악성코드 투입 행위 금지 명시

□ 개정안은 법 제21조의4에 따라 금지되는 행위에 전자금융기반시설에 대하여 데이터를 파괴하거나 전자금융기반시설의 운영을 방해할 목적으로 컴퓨터 바이러스, 논리폭탄 또는 메일폭탄 등의 프로그램을 투입하는 행위 외에 ‘악성코드’를 투입하는 행위도 포함하도록 명시하려는 것임(안 제21조의4제2호 등).

현행	개정안
제21조의4(전자적 침해행위 등의 금지) 누구든지 다음 각 호의 어느 하나에 해당하는 행위를 하여서는 아니 된다.	제21조의4(전자적 침해행위 등의 금지)
1. (생략)	----- ----- --.
2. 전자금융기반시설에 대하여 데이터를 파괴하거나 전자금융기반시설의 운영을 방해할 목적으로 <u>컴퓨터 바이러스</u> , 논리폭탄 또는 메일폭탄 등의 프로그램을 투입하는 행위	1. (현행과 같음) 2. ----- ----- ----- <u>악성코드, 컴퓨터 바이러스</u> ----- ----- -----
3. (생략)	3. (현행과 같음)
제49조(벌칙) ① 다음 각 호의 어느 하나에 해당하는 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다.	제49조(벌칙) ① ----- ----- ----- -.
1. (생략)	1. (현행과 같음)
2. 제21조의4제2호를 위반하여 데이	2. -----

현행	개정안
터를 파괴하거나 <u>컴퓨터 바이러스</u>, 논리폭탄 또는 메일폭탄 등의 프 로그램을 투입한 자 3. 4. (생략) ② ~ ⑧ (생략)	-----<u>악성코드</u>, <u>컴퓨터</u> <u>바이러스</u>----- ----- 3. 4. (현행과 같음) ② ~ ⑧ (현행과 같음)

- 악성코드(Malware)는 컴퓨터에 악영향을 끼칠 수 있는 모든 소프트웨어를 총칭하는 용어로, 악성코드의 종류로 컴퓨터바이러스, 논리폭탄, 메일폭탄, 랜섬웨어, 트로이목마 등이 있음.

< 악성코드의 정의 및 종류 >

① 정의 (한국정보통신기술협회 표준)		컴퓨터에 악영향을 끼칠 수 있는 모든 소프트웨어의 총칭
②종류	바이러스	다른 프로그램이나 파일에 악성코드를 삽입하여 실행 시 복제·전파
	논리폭탄	특정 조건이 만족되면 특정형태에 공격을 하는 코드
	메일폭탄	메시지 수신방해를 목적으로 일시에 대량의 메일을 발송
	랜섬웨어	시스템/데이터에 암호화하고 복구하는 대가로 금전을 요구
	트로이 목마	합법적인 SW로 가장하여 실행토록 유도하는 악성코드

*자료: 금융위원회

- 현행법은 ① 전자금융기반시설에 대한 불법적 접근이나, 데이터의 조작·파괴·은닉 또는 유출 행위, ② 금융위반시설의 데이터 파괴, 컴퓨터 바이러스, 논리폭탄 또는 메일폭탄 등의 방법으로 전자금융기반시설 공격 행위, ③ 대량의 신호 송출 등의 방법으로 전자금융기반시설에 오류나 장애를 발생하게 하는 행위를 전자적 침해행위¹⁾ 등으로 보아

1) 「전자금융거래법」

제2조(정의)

22. “전자적 침해행위”란 해킹, 컴퓨터 바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파

금지하고 있으며(법 제21조의4²⁾),

○ 이를 위반하는 경우 10년 이하의 징역 또는 1억원 이하의 벌금에 처하도록 하여(법 제49조제1항제1호부터 제3호까지)³⁾ 전자금융거래의 안전성 및 신뢰성을 확보하기 위한 조치를 마련하고 있음.

○ 한편, 현행법은 ‘전자적 침해행위’를 별도로 정의하고 있으며⁴⁾, 법 제21조의5⁵⁾에서는 ‘전자적 침해행위’로 인하여 전자금융기반시설이 교란·마비되는 등의 사고(이하 “침해사고”)가 발생한 때에는 금융위

등의 방법으로 전자금융기반시설을 공격하는 행위를 말한다.

2) 「전자금융거래법」

제21조의4(전자적 침해행위 등의 금지) 누구든지 다음 각 호의 어느 하나에 해당하는 행위를 하여서는 아니 된다.

1. 접근권한을 가지지 아니하는 자가 전자금융기반시설에 접근하거나 접근권한을 가진 자가 그 권한을 넘어서 저장된 데이터를 조작·파괴·은닉 또는 유출하는 행위
2. 전자금융기반시설에 대하여 데이터를 파괴하거나 전자금융기반시설의 운영을 방해할 목적으로 컴퓨터 바이러스, 논리폭탄 또는 메일폭탄 등의 프로그램을 투입하는 행위
3. 전자금융기반시설의 안정적 운영을 방해할 목적으로 일시에 대량의 신호, 고출력 전자기파 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 전자금융기반시설에 오류 또는 장애를 발생하게 하는 행위

3) 「전자금융거래법」

제49조(벌칙) ① 다음 각 호의 어느 하나에 해당하는 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다.

1. 제21조의4제1호를 위반하여 전자금융기반시설에 접근하거나 저장된 데이터를 조작·파괴·은닉 또는 유출한 자
2. 제21조의4제2호를 위반하여 데이터를 파괴하거나 컴퓨터 바이러스, 논리폭탄 또는 메일폭탄 등의 프로그램을 투입한 자
3. 제21조의4제3호를 위반하여 일시에 대량의 신호, 고출력 전자기파 또는 데이터를 보내거나 전자금융기반시설에 오류 또는 장애를 발생시킨 자(이하 생략)

4) 「전자금융거래법」

제2조(정의)

22. “전자적 침해행위”란 해킹, 컴퓨터 바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 전자금융기반시설을 공격하는 행위를 말한다.

5) 「전자금융거래법」

제21조의5(침해사고의 통지 등) ① 금융회사 및 전자금융업자는 전자적 침해행위로 인하여 전자금융기반시설이 교란·마비되는 등의 사고(이하 “침해사고”라 한다)가 발생한 때에는 금융위원회에 지체 없이 이를 알려야 한다.

② 금융회사 및 전자금융업자는 침해사고가 발생하면 그 원인을 분석하고 피해의 확산을 방지하기 위하여 필요한 조치를 하여야 한다.

원회에 지체 없이 이를 알리도록 하고, 법 제51조⁶⁾에서는 이를 위반하여 침해사고를 알리지 아니한 자에 대해서는 1천만원 이하의 과태료를 부과하도록 하고 있음. 이에 대응하여 금융위원회는 침해사고에 대한 긴급조치 등의 업무를 수행함(법 제21조의6)⁷⁾.

□ 그런데 현행법이 침해사고 발생 유형에 악성코드 감염 여부를 포함하지 않아 금융회사 등이 고객정보 유출이나 서비스 장애가 발생하지 않았다는 이유로 악성코드 감염에 대하여 보고하지 않고 있다가 고객 신용정보 유출, 전산장애 등 가시적 피해가 발생한 후에 금융위원회에 보고하고 있어서 악성코드 감염 사고에 대한 조기 대응이 어려운 상황이 발생하고 있으므로, 이를 해소하기 위한 방안이 마련될 필요가 있다는 지적이 있음.

□ 이에 개정안은 데이터를 파괴하거나 전자금융기반시설의 운영을 방해할 목적으로 전자금융기반시설에 ‘악성코드’를 감염시키는 행위를 전자적 침해행위의 한 유형으로 법률에 명시하려는 것으로,

6) 「전자금융거래법」

제51조(과태료) ③ 다음 각 호의 어느 하나에 해당하는 자(제1호, 제6호부터 제8호까지 및 제10호의 경우에는 제28조제4항에 따라 해당 규정을 준용하는 선불전자지급수단을 발행하는 자를 포함한다)에게는 1천만원 이하의 과태료를 부과한다.

6. 제21조의5제1항을 위반하여 침해사고를 알리지 아니한 자

7) 「전자금융거래법」

제21조의6(침해사고의 대응) ① 금융위원회는 침해사고에 대응하기 위하여 다음 각 호의 업무를 수행한다.

1. 침해사고에 관한 정보의 수집·전파

2. 침해사고의 예보·경보

3. 침해사고에 대한 긴급조치

4. 그 밖에 침해사고 대응을 위하여 대통령령으로 정하는 사항

② 제1항에 따른 업무를 수행하는 데 필요한 절차·방법 등은 대통령령으로 정한다.

○ 악성코드 감염 등이 발생한 경우 금융위원회 보고가 이루어지도록 함으로써 악성코드에 감염된 경우 신속한 초동조치가 취해질 수 있도록 하려는 취지임.

□ 다만, 개정안에 대해서는 다음과 같은 점을 고려하여 논의될 필요가 있어 보임.

○ 첫째, 현행법 제21조의4제2호에서는 “전자금융기반시설에 대하여 데이터를 파괴하거나 전자금융기반시설의 운영을 방해할 목적으로 컴퓨터 바이러스, 논리폭탄 또는 메일폭탄 등의 프로그램을 투입하는 행위”를 전자적 침해행위로 규정하고 있는데,

컴퓨터 바이러스, 논리폭탄 등의 프로그램은 악성코드의 여러 유형 중 일부를 예시하고 있는 것이어서 “악성코드”라는 용어를 명시할 실익이 크지 않아 보임. 「전자금융거래법」 및 동법 시행령에서 위임한 사항을 규정하고 있는 「전자금융감독규정」⁸⁾에 따른 침해사고 신고 양식을 보면, 침해사고 발생 정보 중 공격방법에 악성코드⁹⁾를 포함하고 있고, 악성코드로 인해 전자금융기반시설의 장애가 발생하면 금융회사 등은 현재도 금융위원회에 보고하여야 함.

8) 「전자금융감독규정」 (금융위원회고시)

제37조의4(침해사고 통지의 방법) 금융회사 및 전자금융업자는 법 제21조의5에 따른 침해사고가 발생한 사실을 안 때에는 지체 없이 사고 내용, 사고에 따른 영향 등을 <별지 7호 서식>에 기재하여 금융위원회에 보고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여서는 아니된다.

9) 「전자금융감독규정」 (금융위원회고시)

제2조(정의) 8. "컴퓨터악성코드"(이하 "악성코드"라 한다)라 함은 컴퓨터에서 이용자의 허락 없이 스스로를 복사하거나 변형한 뒤 정보유출, 시스템 파괴 등의 작업을 수행하여 이용자에게 피해를 주는 프로그램을 말한다.

< 감독규정 별지 제7호 서식 >

1. 기본 사항			
보고자	금융회사명	보고 담당자 (부서명/성명)	연락처 (전화/이메일)
보고일시			
보고형태	☐ 최초 ☐ 중간 ☐ 종결		
2. 침해사고 발생 정보			
공격 대상	☐ 내부망 시스템 ☐ DMZ 구간 시스템 ☐ 기타() ☐ 미상(파악 중)		
공격 방법	☐ 악성코드(웬슬, 랜섬웨어, 바이러스 등) ☐ 서비스 거부 (DDoS 공격 등) ☐ 보안취약점 해킹 ☐ 무단 접속 및 조작 ☐ 공급망 보안 침해(연계기관 해킹 등) ☐ 기타() ☐ 미상(파악 중)		
최초 인지 경로	☐ 금융회사 ☐ 외부() ☐ 고객(민원인) ☐ 기타()		
사고인지 일시		사고발생 일시	
사고 지속시간		사고종료 일시	
사고 발생 업무(시스템 등)		사고 발생 업무 중요도	☐ 높음 ☐ 보통 ☐ 낮음
사고 내용 (현상 및 결과)			
초동 조치사항			
3. 침해사고 영향			
침해사고 결과 (복수 선택)	☐ 시스템 및 서비스 중단(중단시간:) ☐ 정보유출(유출된 정보: / 유출량:) ※ 개인정보, 소스코드, 암호화 키, 인증서 등 ☐ 주요 정보 조작(조작된 정보:) ☐ 금전적 손실(금액:) ☐ 기타 () ☐ 미상 (파악 중)		
	(서식 중간 생략)		
악성코드 정보 (해시 값 등)			
상세내용			

○ 둘째, 개정안에 따르더라도 악성코드 감염에 대한 사전 보고 이행 및 대응 강화라는 당초 개정 취지를 달성하는 데에 한계가 있을 것으로 보임.

현행법 제21조의5¹⁰⁾에서는 ‘전자적 침해행위’로 인하여 전자금융

10) 「전자금융거래법」

제21조의5(침해사고의 통지 등) ① 금융회사 및 전자금융업자는 전자적 침해행위로 인하여 전자금융기반시설이 교란·마비되는 등의 사고(이하 “침해사고”라 한다)가 발생한 때에는 금융위원회에 지체 없이 이를 알려야 한다.

기반시설이 교란·마비되는 등의 사고(침해사고)가 발생한 때에는 금융위원회에 지체 없이 이를 알려야 하고, ‘침해사고’는 전자적 침해행위로 인하여 전자금융기반시설¹¹⁾이 교란·마비되는 결과를 가져온 경우를 말함. 즉, 전자적 침해행위가 있었다 하더라도 전자금융기반시설이 교란 또는 마비되지 않으면 침해사고에 해당되지 않아 금융회사 등은 이를 보고할 의무가 없음. 이는 금융회사 등에 대한 악성코드 침투 등의 시도가 수시로 발생하는 상황에서, 이러한 모든 행위를 보고하도록 할 경우 과도한 행정적 부담이 발생할 수 있음을 고려한 것으로 보임.

이에 따르면, 금융회사 등은 악성코드 침투¹²⁾를 전자적 침해행위로 보지 않아 이를 금융위원회에 보고하지 않은 것이 아니라, 이로 인해 전자금융기반시설의 장애가 발생하지 않은 경우로서 침해사고에 해당하지 않아 보고하지 않은 것으로 볼 수 있음.

즉, 개정안에 따르더라도 전자금융기반시설의 교란 또는 마비가 발생하지 않는 경우에는 금융회사 등이 악성코드 침투 사실을 보고할 의무가 발생하는 것은 아니므로 개정 취지를 실현하기에는 한계가 있을 것으로 보임.

② 금융회사 및 전자금융업자는 침해사고가 발생하면 그 원인을 분석하고 피해의 확산을 방지하기 위하여 필요한 조치를 하여야 한다.

11) 「전자금융거래법」

제2조(정의) 21. “전자금융기반시설”이란 전자금융거래에 이용되는 정보처리시스템 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호에 따른 정보통신망을 말한다.

12) 참고로, 악성코드를 침투시키는 행위는 현행법 제21조의4에 따라 금지되는 전자적 침해행위 등에 해당하므로, 해당 행위를 한 자는 현행법에 따라 형벌 등의 제재를 받음.

- 개정안에 대하여 금융위원회는 현행법에서도 컴퓨터 바이러스, 논리폭탄 등 악성코드의 종류들을 전자적 침해행위의 예시로 제시하고 있어 ‘악성코드’라는 단어를 별도로 추가할 필요성은 낮다는 의견임.

문 의 처

02)6788-5104
