금융위원회 보도 자료 금융감독원

보도시점 2026.11.18.(수) 석간 배포 2026.11.17.(화) 16:00

# 全금융권이 상시적으로 철저하게 보안 관리에 임하도록 IT자산 식별·관리를 의무화하고 취약점 점검·평가 제도를 내실화하겠습니다.

**- 「전자금융감독규정」 개정안 규정변경예고(11.18~30) -**
**- 시급히 추진 필요한 과제는 행정지도를 통해 11월 중 실시 -**

- **IT자산 식별·관리체계 수립·운영 및 최신화**
- 대형 금융사 **취약점 분석·평가 점검주기 단축**(연1회 → 2회)
- 긴급한 취약점 점검 필요 발생시 **금융당국의 수시점검 요청근거 신설**
- 전자금융기반시설에 직·간접 연결된 **모든 시스템 점검 의무화**

금융위원회는 **「전자금융감독규정」 일부개정안 규정변경예고**('26.11.18~11.30일)**를 실시**한다. 이번 개정안은 지난 '26.11.5일 발표한 「全금융권 보안체계 혁신방안」의 후속조치로서, ▲全금융권이 각 회사가 보유한 **IT자산을 스스로 면밀히 식별·관리**하는 의무를 부과하는 한편, **▲대형 금융회사의 취약점 분석·평가 주기를 연 1회에서 연 2회로 확대**하고 ▲긴급한 취약점 점검 필요 발생시 **금융당국이 수시점검을 요청**하는 근거를 마련하며, **▲전자금융기반시설에 직·간접적으로 연결된 모든 시스템을 점검대상으로 명시**하는 등 **취약점 분석·평가를 내실화**하는 내용을 담고 있다.

금번 「전자금융감독규정」 개정안은 규정변경예고와 법제처·규개위 심사, 금융위 의결 등을 거쳐 **'27년 1분기 중 시행**을 목표로 추진한다. 다만, 규정 개정 내용 중 시급한 추진이 필요한 ▲대형 금융사의 취약점 분석·평가 주기 단축(연 1회→2회)과 ▲전자금융기반시설과 연결된 모든 시스템 점검대상 포함 과제는 **행정지도를 통해 11월부터 신속히 추진**할 예정이다.

## < 전자금융감독규정 개정안 주요 내용 >

### 1 IT자산 식별·관리체계 수립·운영 및 최신화 (안 제14조)

전금법 대상 모든 금융회사 및 전자금융업자는 ▲정보처리시스템, 통신장비, 정보보호시스템 등 각 회사가 보유하고 있는 **모든 정보기술자산을 식별**하고, **▲중요도에 따라 분류**하고 **책임자를 지정**하며 **▲해당 자산목록을 최신상태로 관리**하여야 한다.

최근 벌어지고 있는 금융권 해킹 사고는 보안관리가 철저한 핵심 시스템이 아니라 상대적으로 보안이 허술한 업무지원관리 등 주변부 시스템에서 주로 발생하고 있다. AI를 활용한 해킹의 특성상 이러한 “약한 고리”를 빠르고 치밀하게 공격하는 침해공격이 앞으로 지속될 것으로 예상되는 바, 전 금융권과 전자금융업자들이 스스로 보유한 IT 자산목록을 명확히 파악하고, 주변부 시스템까지 꼼꼼히 점검·관리토록 하는 조치이다.

### 2 대형 금융사 취약점 분석·평가 주기 단축(연 1회→2회)(안 제37조의2제1항)

총자산 규모 2조원 이상, 상시 종업원 수 300명 이상인 **대형 금융회사**는 기존 연 1회 실시하던 취약점 분석·평가를, **두 배 확대된 연 2회**(반기 당 1회) **실시하는 것이 의무화**된다.

취약점 분석·평가는 금융회사·전자금융업자의 상시적인 보안관리·취약점 점검을 위한 제도로서, 금융보안원·민간 보안업체 등으로부터 IT 자산 전반의 취약점 여부 등을 점검받고, 그 결과와 보완계획을 금융당국에 제출토록 하는 제도이다. (전자금융거래법 제21조의3)

AI를 통한 침해위협이 빠르게 진화·발전하고 있으며, 전산자원의 취약점도 과거와 비교할 수 없이 빈번히 나타나고 있는 상황에서, 보다 밀도있고 신속하게 전산 시스템의 취약점을 확인하고 조치하기 위한 제도 개선이다.

우선 점검여력이 있는 대형 금융사부터 연 2회 점검을 의무화하되, **금융권 준비상황 등**을 보아가며 **적용범위를 신속히 확대**해 나갈 예정이다.

### 3 긴급한 점검 필요시 금융당국의 수시점검 요청 신설(안 제37조의2제7항)

다수의 금융회사에 유사한 침해사고가 연달아 발생하는 등 긴급한 취약점 확인 및 신속한 조치가 필요한 경우에는 **금융위원회가 해당 금융회사·전자금융업자 등에 대해 수시로 취약점 분석·평가를 요청**할 수 있는 근거도 마련된다.

시스템상 유사한 취약점을 노린 침해사고가 빈발하거나, PHP 등 광범위하게 사용되는 소프트웨어에 중요한 취약점이 나타나는 경우에는 위험성이 높은 업권이나 금융회사 등에 정기적인 점검 외에도 시급한 취약점 분석·평가 및 이에 따른 조치가 필요할 수 있다. 금융당국에서 이러한 시급한 경우에 점검대상과 범위 등을 정하여 통보하면, 금융회사·전금업자 등은 지체없이 이를 이행하도록 제도화할 계획이다.

### 4 취약점 분석·평가 시 의무점검 범위 명시(안 제37조의2제8항)

금융회사 및 전자금융업자가 취약점 분석·평가를 실시하는 경우, **전자금융기반시설에 직접 또는 간접적으로 연결되어 사용되는 정보처리시스템**을 **빠짐없이 모두 대상에 포함**하여야 한다.

기존에는 금융회사 등이 취약점 분석·평가를 실시할 경우 의무적으로 포함하여야 하는 범위가 규정화되어 있지 않아 중요하다고 여겨지는 핵심 시스템을 주로 점검하고, 상대적으로 관심도가 떨어지는 주변부 시스템은 점검대상에서 누락하는 경우가 많이 있었다.

AI를 활용한 해킹공격이 주변부 시스템의 허점까지 파고드는 것으로 나타나는만큼, 전자금융기반시설에 직·간접적으로 연결되는 모든 시스템들을 빠짐없이 철저히 관리하기 위한 제도 개선이다.

## < 행정지도 주요 내용 >

IT자산 식별·관리 의무화, 취약점 분석·평가 내실화 등 과제는 「전자금융감독규정」 개정을 통해 최대한 신속히 추진할 계획이나, 규정 개정에 필요한 절차와 이에 소요되는 최소 시한 등을 감안할 때 '27.1분기에 시행이 가능할 것으로 예상된다.

따라서, 「전자금융감독규정」 개정안의 내용 중 **시급한 추진이 필요한 ▲대형 금융사의 취약점 분석·평가 주기 단축**(연 1회→2회)과 **▲전자금융기반 시설과 연결된 모든 시스템 점검대상 포함 과제**는 **행정지도를 통해 우선 시행할 계획**이다. 행정지도의 경우 법적인 강제성은 없으나, 全 금융업권이 AI 침해위협에 대한 긴밀한 대응 필요성에 공감하고 있는 만큼, 제도개선 내용을 우선 명확히 하여 「전자금융감독규정」 개정 전이라도 해당 사항에 대해서는 자발적인 이행이 이뤄질 것으로 기대한다.

## < 향후 일정 >

「전자금융감독규정」 개정안은 국무조정실 규제심사 등 관련 절차를 거쳐 금융위원회 의결에 따라 **'27년 1분기 중 시행되도록 추진**한다.

행정지도는 11.18일에서 11.23일까지(5일간) 의견 청취 후 금융위원회 내 금융행정지도 심의위원회 심의·의결을 거쳐 **11.30일(잠정) 시행**될 예정이며 규정 개정 전까지 효력을 유지한다.

**〈 규정변경예고 관련 안내사항 〉**

■ **예고기간** : 2026.11.18일(수) ~ 2026.11.30일(월), (12일)

■ **입법예고·규정변경예고된 내용에 대해 의견이 있으시면 다음 사항을 기재한 의견서를 아래의 제출처로 제출해 주시기 바랍니다.**

- 예고 사항에 대한 찬성 또는 반대 의견(반대의 경우 이유 명시)
- 성명(기관·단체의 경우 기관·단체명과 대표자명), 주소·전화번호

- 일반우편 : 서울시 종로구 세종대로 209 정부서울청사 금융위원회 금융안전과
- 전자우편 : src0745@korea.kr
- 팩스 : 02-2100-2948

※ **개정안 전문(全文)**은 "금융위 홈페이지(www.fsc.go.kr) › 정책마당 › 법령정보 › 입법예고/규정변경예고"에서 확인 가능합니다.

| | | | |
|---|---|---|---|
| 담당 부서<br><총괄> | 금융위원회<br>금융안전과 | 책임자 | 과 장 김태훈 (02-2100-2970) |
| | | 담당자 | 사무관 최서린 (02-2100-2974) |
| 담당 부서<br><공동> | 금융감독원<br>디지털금융총괄국 | 책임자 | 국 장 이 석 (02-3145-7420) |
| | | 담당자 | 팀 장 이정운 (02-3145-7540) |
| | | | 팀 장 노경록 (02-3145-7130) |

대한민국 정책브리핑
대체불가 대한민국
OPEN 출처표시 공공누리 공공저작물 자유이용허락