# 경영유의사항 등 공개안

**1. 금융회사명 :** 유진투자증권㈜

**2. 제재조치일 :** 2022. 11. 30.

**3. 제재조치내용**

| 제재대상 | 제재내용 |
|---|---|
| 기 관 | 경영유의사항 1건, 개선사항 1건 |

**4. 조치대상사실**

**가. 경영유의사항**

⑴ 해킹 등 전자적 침해사고 대비 보안체계 강화 필요

회사는 해킹 등 전자적 침해사고에 대응하기 위해 외부 보안관제 서비스를 이용하고 정보보호시스템을 설치·운영하고 있으나

① 웹방화벽, 방화벽 등 일부 정보보호시스템의 보안정책을 주기적으로 검토·점검하지 않고, 점검결과 및 이행계획을 보고하지 않았으며

② 내부통신망에서 운영 중인 정보보호시스템과 중요 서버팜 등에 추가적인 접근통제 수단을 적용하지 않아 보안위협에 취약한 상태로 운영하였고

③ 금융ISAC 보안관제서비스(금융보안원)에서 제공하는 보안위협

정보에 대한 위험수준 파악 및 보안조치 등 보안관제 업무를 수행할 인력이 부재하여 침해사고 발생 시 적절한 대응이 원활하게 이루어지지 않을 우려가 있으므로

정보보호시스템의 보안정책 등이 적정한지 주기적으로 점검하여 점검결과 및 이행계획을 보고하고, 내부통신망 내 보안위협의 확산을 차단할 수 있도록 방화벽 등 추가적인 접근통제 수단을 적용하며, 보안관제 전문인력을 확보하여 전자적 침해사고에 신속히 대응할 수 있도록 보안체계를 강화할 필요가 있음

## 나. 개선사항

### (1) 해킹사고 관련 피해확인 및 잠재 위협 점검 미흡

회사는 ○○○○.○○.○○.~○○○○.○○.○○. 기간 중 발생한 해킹사고와 관련하여 보안전문업체(◇◇)에 의뢰하여 사고의 원인을 파악하고 내부 시스템에 잠재 위협이 존재하는지를 점검하였으나

공격자가 침입한 시스템(◎◎)과 직·간접적으로 연결된 시스템 중 △△, ▽▽ 등 주요 시스템을 대상으로 정보유출 피해여부 등을 분석하지 않고,

일부 전산기기로만 한정*하여 분석하는 등 주요 시스템의 피해 확인 및 잠재 위협 점검을 미흡하게 수행하였으므로

* 보안업체(◇◇)에게 ■■, ◉◉ 등 총 ○○대 전산기기 분석 의뢰

◎◎ 등 공격자가 침입한 시스템과 연결된 주요 시스템을 대상으로 피해확인 및 잠재 위협 등을 추가 점검할 필요가 있음