금융감독원	**보 도 자 료**	금융은 튼튼하게 소비자는 행복하게

보도	2023.11.8.(수) 14:00	배포	2023.11.8.(수)

담당부서	IT검사국 검사기획팀	책임자	국 장	장성옥	(02-3145-7420)
		담당자	팀 장	이성욱	(02-3145-7415)

「금융IT 안전성 강화를 위한 가이드라인」을 마련하였습니다.

Ⅰ. 추진 배경

□ 금융권 전반에 디지털 금융이 확대됨에 따라 **서비스 중단**이 **발생**하는 경우 심각한 **금융소비자 불편** 및 **사회적 혼란**이 발생할 수 있음에 따라

○ 금융업계 **IT내부통제 수준**을 **일정 부분 향상**시키고 IT부문 **개발·운영상**의 **문제점**을 **금융회사**가 **자율적·근본적**으로 **개선**할 수 있는 **환경**을 조성할 **필요성**이 **제기**되었음

□ 이에 금융감독원은 지난 3월부터 7개 협회·중앙회와 공동으로 **'금융IT 안전성 강화를 위한 가이드라인'** 마련을 위한 **T/F**를 **구성·운영**하여

○ 전산사고의 주요 원인인 **프로그램 오류, 비상대책, 성능관리** 부분에 대해 **최소한**의 **기준**을 **마련**하여 **제시**하고자

○ **IT검사 사례** 및 **모범사례**(Best Practice)를 **기반**으로 **작성**한 **초안**을 **바탕**으로 **각 협회 주도 하**에 **금융회사 의견**을 **수렴**하여 **가이드라인**의 **세부 내용**을 **마련**하였음

Ⅱ. 가이드라인 주요 내용 및 기대효과

▣ **(주요내용)** IPO 등 **대형이벤트 사전 대비**, 비상대응 **훈련 범위 확대**, 프로그램 **테스트·검증·배포 통제 강화** 등 **기준 제시**

▣ **(기대효과)** IT운영능력 제고 및 복원력 향상 등 **IT 안전성 강화**로 증권사 MTS·HTS 접속 지연 등 **서비스 중단 사고**가 크게 **감소**할 것으로 **기대**

1 전산시스템 성능 관리

○ **(목적)** 전산시스템 성능을 초과하는 이용자 집중으로 **증권사 MTS·HTS 등**이 **지연, 중지**되는 사고 예방

○ **(주요 내용)** 전산자원별 **임계치**를 **세분화**하여 대응토록 하는 등 금융회사 **IT 운영 능력 제고**

- **전산자원 사용량** 임계치를 **4단계**(정상→주의→경계→심각)로 **구분**하고 경계 및 심각 징후 발생시 **즉각 설비 증설 추진**

- IPO 등 **대형이벤트**는 **기획 단계**부터 **고객수요**를 **예측**하고 시스템 **처리능력**을 **검증**하도록 하여 **사용량**이 **집중**되어 **발생**하는 **사고**를 **사전**에 **대비**

> ※ **<참고> 시스템 성능관리 관련 사고 사례**
>
> ◈ A증권사는 전산자원 증설 기준과 대응방안을 수립하지 않아, '23.6월 경계 수준의 사용량(CPU 사용량 65%↑)에 도달하였음에도 조치 없이 운영하다 '23.7월 MTS 중단
>
> ◈ '23.7월 B증권사는 공모주 청약 마감일에 집중된 청약 증거금 이체 신청을 제대로 처리하지 못해 청약 마감시간을 30분 연장(16:00 → 16:30)

2 IT부문 비상대책 수립 · 운용

○ **(목적) 화재 등 비상상황 발생**시 전자금융서비스가 **장기간 중단**되는 사고 **예방**

○ **(주요내용)** 비상대응훈련 범위 확대 및 재해복구센터 인프라 확충 등을 통해 **IT복원력 향상**

- **주전산센터 마비**시에도 **핵심업무**를 **수행**할 수 있도록 **재해복구센터 인프라**(DB·서버·통신망 등)를 충분히 확보

- 실제 **비상상황 발생**시에도 **전자금융서비스**가 신속하게 **복구 가능**하도록 **비상대응 훈련**의 **범위 확대**

> ※ **<참고> IT부문 비상대책 미흡 사례**
>
> ◈ '22.10월 A전자금융업자는 인증기능을 제공하는 대외기관과의 연계훈련을 실시하지 않고 대체 수단도 마련하지 않아 대외기관 중단에 따라 간편결제 서비스가 중단
>
> ◈ '23.4월 금융권 비상대책 점검 결과 B증권사는 재해복구센터의 전산자원(CPU, 메모리 등)의 가용성능이 주전산센터 대비 25% 수준으로 확인됨

3 프로그램 통제 가이드라인

○ **(목적)** 금융회사가 프로그램 변경 과정에서 **모바일 뱅킹** 등 **전자금융서비스**가 **중단**되는 **사고**를 **예방**

○ **(주요내용)** **제3자 검증·통제 기능**을 구축 및 전산프로그램 **테스트역량 강화**를 도모 등

- 프로그램 변경시 **충분한 테스트**를 실시하고, 개발·변경 내용 **검증**을 위한 **별도 조직 구성**

- 프로그램을 신규로 개발하여 적용하는 경우 **고객접속**이 적은 **시간**에 **수행**토록 하여 **오류가 발생**하더라도 **피해**를 **최소화**

※ <참고> 프로그램 오류 관련 사고 사례

◈ '22.5월 A은행은 체크카드 사용이 활발한 21시경에 변경 프로그램을 배포하던 중 오류가 발생하여 약 20분 동안 8.7천명 이상의 체크카드 고객이 불편을 겪음

◈ '23.7월 B증권사는 MTS내 수익률 및 평가손익금액 계산 프로그램 변경시 충분한 테스트를 수행하지 않아 수익률 및 평가손익금액 표기 오류 발생

Ⅲ. 최종 점검 및 향후 계획

□ 11월 8일 **금융협회·중앙회 간담회**를 **통해 시행시기**를 조율하고 **시행시 예상되는 문제점**을 최종 **점검**하였으며,

○ 금번 **가이드라인**의 경우 IT운영 안정성을 위한 **최소한**의 **기준**이기에 **세부 구현 방식**에 있어 **각 회사별 상황**에 따라 **취지를 벗어나지 않는 범위내**에서 **조정 가능함**을 **논의**하였음

[간담회 개요]

- **일시 :** '23.11.8.(수) 14:00 ~ 15:00
- **장소 :** 금융감독원 9층 회의실
- **참석자** : (금감원) 김병칠 부원장보, IT검사국장
  (협회·중앙회) 금융투자협회, 생명보험협회, 손해보험협회, 여신금융협회, 은행연합회, 저축은행중앙회, 핀테크산업협회

□ 수립된 가이드라인은 7개 금융 협회·중앙회별 **자체심의, 보고** 등의 **내부 절차**를 거친 후 **연내 시행할 예정**이며,

○ **11월 하순**부터 **금융업권별 릴레이 설명회**(협회·중앙회 주관)를 통해 **가이드라인 제정 취지**를 **설명**하고 **협조**를 **당부할 계획임**

□ 향후에도「금융IT 안전성 강화를 위한 가이드라인」에 대해 **업계**의 **피드백을 반영**하고 **부족한 부분**은 협회·중앙회와 협의하여 **지속 개선**할 예정임

붙임1 가이드라인 주요 내용(요약)

전산시스템 성능관리 가이드라인 주요 내용

1. 임계치 설정 및 대응전략 수립

○ 전산자원별 임계치를 **4단계**(정상→주의→경계→심각)로 **관리**하고 **주의 단계**에서는 **증설 필요성**을 **검토**, **경계·심각 단계**에서는 **즉각적인 증설** 추진

2. 대형이벤트 유입량 분석 및 예측

○ 금융회사별 **대형이벤트 기준을 마련**하여 이벤트 **기획 단계**에서 **고객수요 예측**과 **처리능력 검증** 결과를 CIO에게 보고하고 예비장비 확보 및 **긴급증설체계 점검** 등 **이벤트**에 대비

3. 성능관리 비상대책 마련

○ **비정상적 트래픽** 발생시 **동시접속자**를 **통제**하고, CPU·메모리 등 **전산자원**을 **즉각 증설**할 수 있는 **체계** 마련

4. 조직 · 내규 등 성능관리 기반 확보

○ 전산시스템 전반의 **성능관리 담당 조직**을 갖추고, **성능 관리 절차**와 담당 **조직**의 **권한** 등의 내용을 포함한 **내규**를 **수립·운용**

5. 성능관리 내부 보고체계 수립

○ 전산 자원의 임계치가 **경계 또는 심각 단계**에 도달하는 경우 **원인 분석**을 실시하고 대응 방안이 포함된 **성능관리보고서**를 **최고정보책임자**(CIO)에게 **지체없이 보고**

IT부문 비상대책 수립·운용 가이드라인 주요 내용

1. 비상훈련 실효성 강화 및 환류체계

○ **핵심업무 전체**에 대하여 **최소 5년에 1회 이상 재해복구모의훈련**이 **시행**될 수 있도록 하고, 훈련 결과 발견된 **미흡 사항**은 **보완 대책**을 마련하여 **업무지속성 확보방안** 등에 **반영**

2. 재해복구센터 인프라 확충

○ **主전산센터 마비**시에도 **재해복구센터**를 통해 **핵심업무**를 **수행**할 수 있도록 **재해복구센터 인프라**(DB·서버 등)를 **확보**하고, **주요 대외기관**과의 **통신 회선** 구축을 의무화

3. 전산센터 화재 예방·대비

○ 전산센터 화재 발생시 **신고***, **초기대응 및 대피 절차**를 **업무지속성 확보방안**의 상황별 대응절차에 **포함**

* 전산센터 화재임을 밝히고 발화원인(전기배터리 여부)과 진입경로를 안내

4. 핵심업무 선정 절차 및 관련 부서별 역할 명확화

○ **핵심업무 선정시** 전사적 운영리스크 또는 **업무영향도 분석 결과**를 반영하고, **핵심업무 선정 절차 내**에 각 단위 업무의 **소관 부서**와의 **합의·검토 절차** 및 **관련 보고 절차**를 포함

5. 업무 지속성 확보 방안 점검 및 관련 시스템 구축

○ **업무지속성 확보방안** 관련 사용자 매뉴얼, 연락처 등을 원활하게 열람할 수 있도록 **책자·서류**를 사전에 **비치**하거나 **자료가 등재된 시스템**에 대한 **재해복구시스템**을 **구축**토록 함

프로그램 통제 가이드라인 주요 내용

1. 제3자 검증 · 통제 기능 강화

○ **등록·변경·폐기** 절차 및 **정당성 검증 절차**를 모두 **내규**에 **반영**하여 **명확화**하고, **IT개발 경력자**로 구성된 **별도 조직**에서 **개발·변경·폐기** 내용의 **정당성**을 **검증**

2. 테스트 역량 강화

○ **운영시스템**과 시스템 환경이 **유사**하면서도 **가용성**(부하) **테스트**가 가능한 **테스트 환경**과 **테스트 담당 조직**을 **준비**토록 하고, **테스트 자동화 솔루션 도입 추진**

3. IT운영 안정성을 위한 배포 전략

○ **고객접속이 적은 시간**에 프로그램 배포를 **수행**토록 하여 **배포된 프로그램**에서 **오류 발생시**에도 **피해**를 **최소화**

4. 프로그램 통제 관리 및 점검 강화

○ 프로그램 등록・변경・폐기 절차 준수 여부 등 개발· 테스트 시 **통제 절차 준수 여부**를 **내부 감사자**가 **분기 1회 이상 점검**

5. 프로그램 통제 절차 내부교육 강화

○ 프로그램 통제 절차 미준수자, 신입 직원 등에게 **연 1회 이상 프로그램 등록·변경·폐기 절차, 프로그램 테스트 절차, 운영시스템 적용·배포 절차** 등 **교육**토록 **규정**

붙임2 가이드라인 관련 질의 및 답변사례(FAQ)

1 「금융IT 안전성 강화를 위한 가이드라인」의 법적 성격은?

□ 금번 시행되는 **가이드라인**은 **IT검사 지적사례** 및 업계 **모범사례**(Best Practice) 등을 취합하여 **마련·권고**한 것으로

○ **행정지도** 등 **금융 규제**에 해당하지 않아 **법적 구속력**은 없음

□ 다만, **3개 가이드라인** 모두 각각 **전자금융감독규정**에서 **세부적**으로 **정하고 있지 않은 사항**에 대해 **안내**하고 있어

○ 가이드라인 자체는 법적 구속력이 없다 하더라도 가이드라인 **미준수 상태**가 **규정위반으로 이어질 경우 행정처분**을 받을 수 있음

< **가이드라인 및 관련 전자금융감독규정** >

가이드라인	전자금융감독규정
전산시스템 성능관리 가이드라인	제25조(정보처리시스템의 성능관리)
IT부문 비상대책 수립·운용 가이드라인	제23조(비상대책 등의 수립·운용)
프로그램 통제 가이드라인	제29조(프로그램 통제)

2 성능관리 가이드라인에서 제시하는 임계치 수치를 변경하여 적용할 수 있는지?

예시) CPU 정상 임계치 60% 미만 → 50% 미만, 또는 60% 미만 → 70% 미만

□ 해당 수치는 **금융업권**에서 **운용중**인 **사례**를 **참고**하여 예시로 제시한 것으로,

○ 임계치의 **세부적인 구현 방식**에 있어서는 **금융회사**의 **상황**별, **시스템 별**로 **차등화**하여 **적용**할 수 있으며,

○ 임계치 그 자체보다는 일부 금융회사에서 **CPU 등 전산자원별 임계치**를 초과하는 **경우**에도 **별도 대응방안**을 **마련**하지 않는 **경우**가 있어 **이에 대한 개선**을 **유도**하는 **취지**임

3 성능관리 가이드라인에서 '대형이벤트'의 기준은?

□ 공모주 청약 및 상장, 신규 서비스 개시, 대고객 이벤트 시작 등 **이용자가 단기간 급증할 수 있는 이벤트**에 대해

○ 금융회사가 이벤트 계획 단계에서부터 전산 인프라 측면에서 **처리 능력**을 **준비·검증**하자는 **취지**로

○ 금융회사별로 월간 활성이용자수(MAU), 거래규모, 업무 특성 등을 감안하여 **대형이벤트**의 **기준**을 자율적으로 **내규**에 **마련**토록 **하였음**

4 '대형이벤트'의 기준 등 가이드라인 세부적인 기준을 금융회사가 자율적으로 적용토록 하면, 실효성이 저하 되는 것이 아닌지?

□ '24년중 **서면 점검 등**을 통해 금융회사의 **가이드라인 준수 실태**를 **점검**하여

○ 형식적인 기준으로 **운영하고 있지** 않는지 살펴보는 등 실효성 확보를 위해 지속적으로 **노력**할 **계획**임

□ 아울러, 가이드라인 시행 후 운영 과정에서 확인된 **개선 필요 사항**에 대해서는

○ 협회·중앙회와 협의하여 **지속적**으로 **개선할 계획**임

5 '프로그램 통제 가이드라인' 중 검증 조직 관련, 경력 10년 이상의 개발자의 수가 많지 않고 IT인력이 부족한 회사도 있어 별도 조직을 구성하기 어려울 것으로 예상되는데, 해당 항목 준수가 가능한지?

□ 금융회사 의견 수렴 결과 IT개발 관련 인력이 부족하여 해당 항목 준수가 어렵다는 의견도 많아

○ CIO 등 **개발담당 임원의 승인하**에 기존 조직내 업무 분장 변경을 통해 **검증 담당 인력**을 **지정 가능**토록 **허용**하는 등 **예외 조항**을 **포함**하였음

6 '프로그램 통제 가이드라인'에서 테스트 자동화솔루션을 도입토록 규정하고 있는데, 도입 대상 및 적용 범위는?

□ 테스트 자동화 솔루션을 적용해야 하는 대상 및 범위에 대하여 **각 금융회사**가 **자율적**으로 **판단**하여 **적용**할 수 있음