금융감독원	보 도 자 료	금융은 튼튼하게 소비자는 행복하게

보도	2023.9.6.(수) 석간	배포	2023.9.5.(화)
담당부서	IT검사국 상시감시팀	책임자	팀 장 이 수 인 (02-3145-7425)
		담당자	선 임 이 윤 기 (02-3145-7427)

2023년 상반기 전자금융사고 발생 현황 및 대응방안

Ⅰ. 전자금융사고 발생 현황 및 평가

□ **2023년 상반기** 중 **발생**하여 금융감독원에 보고된 **전자금융사고**는 **총 197건**으로

○ **프로그램 오류 등**으로 **10분 이상** 전산업무가 중단·지연된 **장애**는 **194건**이고, **DDoS*** **공격 피해 등** 전자적 **침해**는 **3건**

* DDoS(Distributed Denial of Service, 분산서비스거부 공격) : 여러 대의 PC가 동시에 특정 시스템을 공격하여 시스템 가동을 중단시키는 공격

반기별 전자금융사고 발생 건수

구 분	'22년 상반기	'22년 하반기(a)	'23년 상반기(b)	증감(b-a)
장애사고	197	216	194	△22
침해사고	4	3	3	-
합 계	201	219	197	△22

□ **작년 하반기**와 **비교**하면 **10.0%**가 **감소**(22건↓)하였으며, **전산센터 화재·누수**로 인한 시스템 중단 등과 같은 **대형 사고**는 **없었음**

○ 그러나, **충분한 용량**의 **설비**를 갖추지 않아 **증권사**의 **HTS 및 MTS**가 **중단·지연**되거나, **프로그램 오류**로 인해 **환전, 보험료 출금 등**에서 **일부 소비자**가 **불편**을 겪는 등의 **사례**가 발생

□ **다양한 유형**의 **전자금융사고 발생원인**을 분석한 결과 향후 **타 금융회사**에서도 **동일**하게 **발생**할 **가능성**이 있는 사고가 다수 있어 **사례**를 **공유**하고 **사고 예방활동**을 **강화**할 필요

Ⅱ. 주요 전자금융사고 사례

1 DDoS 공격으로 인한 서비스 영향

□ 일부 **DNS*** **업체**가 **DDoS 공격**을 받아 **서비스**가 **중단**되면서 이를 이용 중인 **금융회사**의 **전자금융업무**가 사실상 **중단**되는 **사고**가 발생

* DNS(Domain Name System) : 사람이 기억하는 도메인 이름을 인터넷 주소(IP)로 변환해주는 시스템 (예시 : www.fss.or.kr → 61.73.100.30)

○ 또한, 보안 수준이 **상대적**으로 **취약**한 **일부 중소 금융회사**가 **DDoS 공격을 받아** 간헐적으로 **서비스**가 **지연**된 사례도 발생

※ **금융회사**를 **대상**으로 한 다양한 **사이버 공격**은 **지속적**으로 **발생**하고 있으나, 그간 구축한 **방어체계**(보안 장비 및 관제, 금융보안원 DDoS 대피소 운영 등)로 **장시간 서비스 중단** 등의 **피해**는 **없었음**

주요 사례

◇ **(다수 카드사)** 결제 서비스를 대상으로 **DDoS 일제 공격**(최대 14Gbps, 약 1분간 집중)이 발생하였으나, **금융보안원**과의 **공조** 등을 통해 **비상상황**에 대해 **신속히 대응**함으로써 서비스가 지연되거나 중단되는 **피해**는 **없었음**

◇ **(A저축은행 등) 외부업체**가 **운영**하는 **DNS**를 대상으로 **DDoS 공격**이 발생하였고, 이에 따라 **이용자**가 서비스 이용시 필요한 **IP주소**를 **획득**하지 못하여 **인터넷·스마트뱅킹** 등 **사용 불가**

2 프로그램 오류로 인한 중복거래 발생 등

□ **전자금융업무**를 처리하는 **프로그램**의 **설계·구현·테스트** 과정에서 오류로 인하여 **소비자 피해**로 이어지는 사고가 다수 발생

○ **주식매매 정산 오류, 환율·금리 산출 오류, 보험료 할인 미적용** 등의 **금전사고** 및 **고객정보 관리 오류** 등의 **사고 발생**

주요 사례

◇ **(B증권사)** 주식매매 프로그램 오류로 **이미 매도된 주식**이 **계좌**에 남은 것으로 **잘못 표시**되면서 고객 착오로 **중복 거래**(주식 추가매도) 등이 발생

◇ **(C보험사) 전산시스템**을 **전면 개편**하면서 보험료 관련 **설정**을 **누락**하여 **보험료**가 **할인**이 **적용**되지 **않은 채 과다 청구**

◇ **(D은행) 환율 고시** 관련 **프로세스**를 **변경**하면서 프로그램 오류로 인해 현재 시점의 환율이 아닌 **전일자 최종 환율**로 **환전 처리**가 됨

◇ **(E증권사)** 회사가 보유한 **고객정보**와 **CI**(Connecting Information)의 **관리 프로그램 오류**로 **일부 고객**의 **정보 중복** 발생

3 하드웨어 결함으로 인한 전자금융거래 지연·중단

□ **하드웨어**(서버, 통신장비, 저장장치 등)의 **노후화** 등으로 **이상 동작**이 발생하여 **서비스**가 **지연·중단**되는 **사고** 다수 발생

○ 이상 동작시 **이중화 예비 장비**로의 **전환**도 **실패**함에 따라 **자금 이체** 및 **해외주식 주문 장애** 등의 사고 발생

주요 사례

◇ **(F증권사)** 보안장비(방화벽)에 **과부하**가 **발생**하여 고객의 거래요청을 즉시 처리하지 못하면서 **이체** 및 **해외주식 매매 서비스** 등의 **지연 발생**

◇ **(G은행) 서버·통신장비** 등을 **다중화**하여 장애상황에 대비하였으나, **통신장비**에서 **유량제어 신호 처리** 중 **이상동작**이 발생하였고 **백업장비**로 **전환**도 **원활치 않아 대외계 서비스 장애** 발생

4 전자금융보조업자 등의 장애로 인한 서비스 영향

□ **전자금융보조업자**의 **서비스**(본인인증, 카드결제 대행 등)를 **이용**하는 경우 **외부 서비스**의 **장애**가 **금융회사**에 **직접적**으로 **영향**

○ **비대면 계좌개설 등**의 **거래**가 중단되거나 보험료 등의 **카드 정기 자동결제**가 **중복**으로 **발생**하는 등의 사고 발생

주요 사례

◇ **(H은행 등) 휴대폰 본인인증 대행업체**의 **시스템 장애**로 인하여 은행·저축은행 등에서 **비대면 계좌개설** 등의 **거래 불가**

◇ **(I보험사)** 보험료 결제 요청시 **VAN사**의 **업무처리 오류**로 인하여 **정상 결제건**을 **카드사**에 **재요청함**에 따라 **보험료**가 **중복 결제**

5 인적 요인에 의한 장애

□ 전산시스템 변경 등의 **통제 절차**가 일부 **미흡**하여 **작업자 실수**로 인한 **서비스 지연·중단 사고** 발생

○ **프로그램**을 **이관**하는 과정에서 **일부**를 **누락**하거나, **네트워크 장비** 등의 **설정 오류**가 **서비스**에 **영향**을 미치는 **사고** 발생

주요 사례

◇ **(J은행)** 프로그램을 **운영환경**에 **배포**시 **일부 소스코드** 등을 **누락**하거나 **DB 변경사항**을 **반영**하지 **않고 프로그램만 배포**하여 **대출·오픈뱅킹 업무 중단**

◇ **(K카드사) 개발이 완료되지 않은 소스코드**가 **운영환경**에 **이관**됨에 따라 **모바일 앱 접속 장애 발생**

◇ **(L전금업자) 보안장비**의 **탐지 규칙**을 정비하면서 **정상적**인 **통신**을 **차단**토록 **잘못 설정**함에 따라 이용자가 **전자고지서 열람 불가**

6 기타

□ 전산시스템을 **장기간 운영**하면서 **거래량 증가** 등에 **선제적**으로 **대응**하지 **않아 서비스**가 **중단**되는 사고도 발생

주요 사례

◇ **(M은행 등)** 거래번호 채번시 **거래량 증가**로 인하여 **최대값**(예 : 7자리 숫자)을 **초과**하여 **오픈뱅킹 이체거래**가 **중단**되거나 **기업뱅킹 로그인**이 **불가능**한 상황 발생

Ⅲ. 전자금융사고 예방 활동 및 향후계획

□ ’23.9.6. **금융감독원**은 **총 269개 금융회사**를 대상으로 **’23.3분기 IT상시협의체 회의**를 개최하여 **전자금융사고 사례**를 **전파**하고 전자금융 **안전성 확보방안** 등을 **논의**하였으며,

○ 금융회사가 기존 사고 **사례 및 발생 원인**을 충분히 **숙지**하고, **CIO 및 CISO 등 경영진**이 **주도**하여 **IT 업무 프로세스 전반**을 **재점검**하고 **사고**를 **예방**할 필요가 있다고 **강조**하였음

□ 금융감독원은 앞으로도 **동일·유사**한 유형의 **장애** 사고 **재발 방지**를 위해 금융IT 안전성 강화를 위한 **가이드라인**을 **배포**할 예정이며, 이를 통해 **전반적인 금융IT 내부통제 수준 상향**을 유도하는 한편,

○ 금융보안원 등 **유관기관**과의 **공조**체계 강화 등을 통해 **사이버 공격**에도 **철저히 대비**하겠음

□ 또한, 전자금융사고 **보고**를 **소홀**히 하거나 **안전성 확보 의무**를 **준수**하지 **않아서 사고**가 **발생**한 경우 **엄중 조치**할 계획임