참고 7.

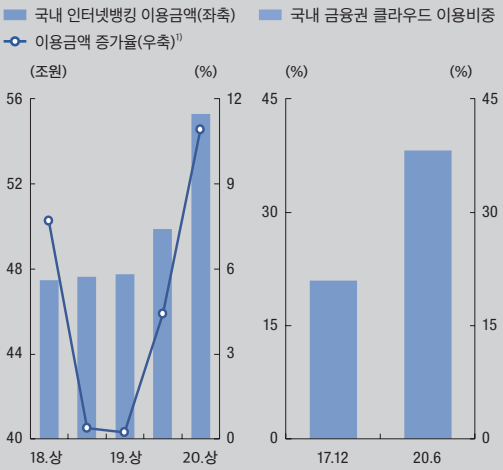
코로나19 이후 주요국 사이버 리스크 대응현황 및 시사점

코로나19 확산에 따른 재택근무 실시 확대, 금융의 디지털 전환 가속화 등으로 사이버공격 발생 가능성이 높아지고 있다. 사이버리스크[1]는 주요 데이터 손실로 인한 금융거래 안정성 저하, 금융시스템 전반에 대한 신뢰 손상 등 다양한 경로를 통해 금융안정에 영향[2]을 미칠 수 있다. 이에 코로나19 발생 이후 사이버리스크에 대한 관심[3]이 높아졌으며, 각국 금융감독당국은 관련 상황을 점검하고 대응조치를 취하였다. 이하에서는 코로나19 이후 주요국의 사이버리스크 대응현황을 살펴보고 시사점을 도출해 보았다.

코로나19 이후 사이버리스크 관련 현황

코로나19 확산에 따른 비대면 거래 선호, 재택근무 실시 등으로 인해 이전부터 진행되어 온 금융의 디지털화 및 제3자[4] 서비스 이용 추세가 가속화되고 있다. 금년중 온라인 거래 증가 등에 힘입어 전자결제, 인터넷뱅킹을 통한 자금이체, 대출신청 등의 디지털 기반 금융서비스 이용이 증가한 것으로 나타났다.[5] 아울러 제3자 서비스 이용이 재택근무를 위한 클라우드 컴퓨팅 활용 등으로 더욱 늘어났다.[6]

인터넷뱅킹 서비스 이용 **금융권 클라우드 이용[2]**



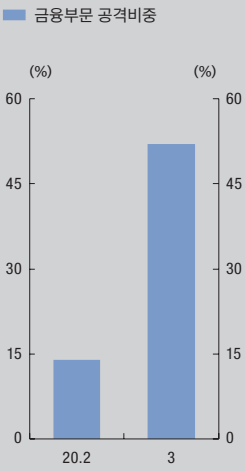
주: 1) 전기대비
2) 주요 금융기관(은행, 증권, 보험 등) 110개사 대상 이용현황 조사
자료: 한국은행, 금융감독원

이러한 상황에서 금융부문에 대한 사이버공격은 지속적으로 증가해 왔으며 특히 코로나19 발생 이후 더욱 확산되었다. 세계적으로 보면 금년초 확진자 수가 늘어나면서 코로나19를 키워드로 한 악성의심 메일 등 사이버공격이 크게 증가한 것으로 나타

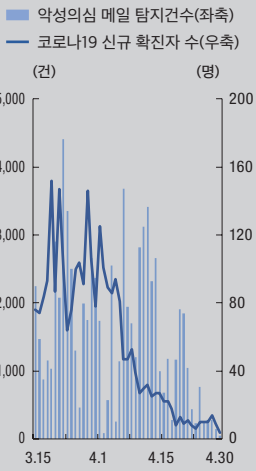
1) 일반적으로 합의된 정의는 없으나 IT시스템 장애로 인한 금융손실(financial loss), 운영장애(disruption) 또는 평판 손실(reputational damage)을 초래하는 리스크를 포괄한다고 볼 수 있다("Financial Stability Review", 호주중앙은행, 18년 등).
2) 영란은행은 사이버리스크가 시스템 리스크의 특성(외부 충격에 의해 촉발, 점진적 누증, 금융시스템 전부 또는 일부에 영향, 기관간 상호연계성에 의해 파급 및 확대, 금융부문 신뢰도 저하에 따른 시장참가자 행태변화가 충격을 확대, 금융서비스 공급 실패에 따른 실물경제에 대한 악영향 등)을 가질 수 있다고 분석하였다("Quarterly Bulletin", 영란은행, 18년 4/4분기).
3) 캐나다 중앙은행, ECB 등은 금융안정보고서 등을 통해 코로나19 발생 이후 사이버리스크 증대 가능성을 언급하였으며 영란은행 금융정책위원회(FPC)는 코로나19 이후 운영복원력 증진을 위한 두 가지 우선순위로 사이버부문과 지급결제를 언급하였다.
4) 클라우드 컴퓨팅 서비스 제공자, 컨설턴트 등 금융기관과 업무 협약을 맺고 있는 외부기관을 의미한다.
5) 글로벌 현황을 보면 McKinsey의 유럽 소비자 대상 서베이 결과 코로나19 이후 은행(banking) 부문에서 디지털 서비스 이용률(77%)이 가장 높았으며 이 중 23%는 코로나19 이후 처음으로 은행 부문 디지털 서비스를 이용한 것으로 나타났다.
6) 글로벌 현황을 보면 글로벌 보안소프트웨어기업 McAfee의 보안플랫폼 이용기업(약 3천만 개) 데이터를 토대로 재택근무 확산에 따른 클라우드 사용 현황을 파악한 결과, 1월 대비 4월중 전산업 평균은 50%, 금융서비스부문은 36% 증가하였다.

났다. 국내 금융부문에서도 마스크 판매 위장, WHO 사칭 기부 요청 등의 형태로 악성코드나 피싱사이트를 유포하는 코로나19 관련 악성의심 메일이 일평균 1,500여건(3월 15일~4월 30일중) 발생하였다.

글로벌 금융부문 사이버공격[1]



국내 금융부문 코로나19 관련 악성의심 메일[2]



주: 1) VMware Carbon Black 보안플랫폼 데이터 분석 결과 전체 사이버공격에서 금융서비스부문에 대한 공격이 차지하는 비중
2) 금융보안원 금융보안관제센터에서 탐지한 악성의심 메일 건수
자료: 금융보안원, VMware Carbon Black, 보건복지부

사이버공격은 금융기관 시스템 정보 및 금융이용자 정보 유출, 자금 편취 등의 피해로 이어지기도 하였으나 국내의 경우 심각한 금전적 손실로 이어진 사례는 없었다.

국내외 사이버리스크 발생 사례

국내	• 가짜 증권회사 홈트레이딩시스템(HTS)으로 이용자에게 조작된 주가를 보여주고 추가 투자금액을 입금하도록 하여 자금을 편취(20년 11월)
	• 국내 핀테크 기업(카카오페이, 토스 등)에서 1,000만원 상당의 부정결제가 발생(20년 6~9월)
	• 코로나19 관련 소상공인 정부지원대출을 빙자한 사기범이 피해자의 휴대폰에 원격 프로그램 설치를 유도한 후 자금을 편취(20년 4월)
해외	• 금융기관 대상 운영서비스를 제공하는 American Bank System(ABS)에서는 랜섬웨어 공격으로 금융기관 및 이용고객 정보가 유출(20년 10월)
	• 미국 인터넷은행 Dave에서는 제3자 서비스 제공자에 대한 사이버사고로 고객정보가 일부 유출(20년 7월)
	• 미국에서는 코로나19 관련 지원금을 지급한다는 내용의 국세청을 사칭한 가짜 문자를 통해 개인정보 입력을 요구하여 자금을 편취(20년 6월)
	• 영국에서는 인터넷·모바일뱅킹을 이용한 사기가 2019년중 0.6조원에 달하였음(19년)

자료: 금융감독원, 각국 중앙은행 등

주요국 및 국제기구 대응현황

주요국 및 국제기구는 코로나19 이후 사이버리스크에 대응하여 사이버복원력을 제고하기 위한 다양한 조치를 취하였다.

(사이버복원력 관련 가이드라인 발표)

주요국 금융감독당국과 국제기구는 금융기관의 사이버복원력 관련 가이드라인을 발표하였다.

먼저 팬데믹 상황에서의 업무지속계획(BCP: Business Continuity Plan) 가이드라인을 마련하였다. 미국 연방금융기관검사협의회[7](FFIEC)는 제3자와의 협력 및 임직원 교육 등의 운영장애 예방프로그램, 확산단계별 전략, BCP 테스트 프로그램 마련과

7) 연방준비제도이사회(FRB), 연방예금보험공사(FDIC), 전국신용협동조합감독청(NCUA), 통화감독청(OCC), 소비자금융보호국(CFPB) 및 주 연락위원회(SLC)로 구성되어 있다.

재택근무를 비롯한 내부절차 및 시스템 정비를 주요 내용으로 하는 팬데믹 BCP 가이드라인을 제시하였다.

다음으로 금융기관의 사이버보안 관련 지배구조와 사전·사후 대응 및 복구 방안 등에 관한 가이드라인을 발표하였다. 최근 금융안정위원회(FSB)는 코로나19에 따른 재택근무 환경으로 인해 사이버사고에 유의할 필요성이 높아졌음을 강조하며 금융당국과 금융기관이 활용할 수 있는 사이버사고 대응 및 복구 가이드라인을 발표[8]하였다. 특히 담당 조직 구조와 책임 명확화 등 지배구조 측면에서 상세한 내용이 포함되었다. ECB는 재택근무와 사이버공격 확대 가능성을 감안하여 기존 IT 인프라 역량을 점검하고 고객 및 금융기관 대상의 금융사기 리스크를 평가할 것을 금융기관에 권고하였다.

FSB 금융기관 사이버사고 대응 및 복구(CIRR) 모범규준[1]

부 문	주요 내용
지배구조	• CIRR 관련 이사회, 고위 경영진, 부서의 역할·책임 명확화 및 합리적 보고체계 형성 • CIRR 활동을 위한 충분한 예산 배정
계획·준비	• 시나리오 기반 스트레스 테스트 수행 • 제3자 서비스 제공자, 기술 솔루션 판매사 등 공급체인 전반에 걸친 리스크관리
분 석	• 포렌식 분석 등을 통해 사이버사고의 심각성, 영향, 원인 파악
완화조치	• 사고 유형별 적합한 억제책을 적용 • 핵심운영기능에 대한 업무지속조치
복원·복구	• 우선순위를 정하고 기 승인된 복원절차에 따라 데이터, 시스템 등을 복구
협업·소통	• 조직 내부 및 감독당국에 적시 보고 • 국가간 협업, 미디어 활동 등을 통해 신뢰할 수 있는 정보 공유
개 선	• 사이버사고 사후분석, 모의 훈련 등에서 얻은 교훈을 토대로 CIRR 역량을 개선

주: 1) 7개 부문 49개 방안으로 구성
자료: FSB

한편 금융기관의 대응상황에 대한 감독지침을 제시하기도 하였다. 미국 금융감독당국은 공동 가이드라인을 통해 금융기관 경영실태평가(CAMELS)의 경영관리 적정성 항목에 코로나19 이후 사이버보안 관련 조치에 대한 평가를 포함할 것을 권고하였다.

(정보 공유[9])

주요국은 금융감독당국 및 민간 금융인프라 운영기관 간 협의체를 통해 사이버리스크 관련 정보를 공유하고 있다.

ECB가 의장을 맡고 있는 유로존 사이버복원력이사회(ECRB)는 핵심 금융인프라 운영기관과 사이버보안 유관기관 간 정보교환을 위한 이니셔티브[10]

8) “Effective Practices for Cyber Incident Response and Recovery”, FSB, 2020년 10월
9) 코로나19 발생 이전부터 수행되어 온 국가간 정보공유 이니셔티브로는 지역내 그룹 및 포럼이 있으며 아시아에서는 ASEAN이 일본과 협업하여 사이버역량 개발 프로젝트(19년)를 시작하였고 ASEAN-싱가포르 사이버보안센터(19년)를 설립하였다.
10) 유럽지역의 중앙은행, 청산소, 증권거래소, 지급결제시스템 제공자, 유로폴(Europol) 등으로 구성되어 있다.

(CIISI-EU)를 새롭게 마련하였다. 캐나다 중앙은행 주도로 창설된 금융부문 복원력 그룹[11](CFRG)은 코로나19 이후 격주로 회의를 가지며 사이버위협 관련 정보를 공유하고 있다.

(금융기관의 사이버리스크 테스트)

일부 금융감독당국은 금융기관에 사이버리스크 관련 테스트를 권고하였다.

ECB는 금융기관의 핵심 기능 및 시스템에 대한 사이버공격 시뮬레이션을 통해 금융기관의 대비상황을 점검하는 TIBER-EU[12](Threat Intelligence-Based Ethical Red-teaming)에 은행의 참여를 권고[13]하였다. 동 테스트에 참여한 은행은 실제와 유사한 사이버공격을 받게 되며 예방, 탐지, 대응능력을 평가받는다.

시사점

코로나19 이후 더욱 확산될 디지털금융의 장점을 활용하면서도 금융소비자를 보호하고 금융시스템 안정을 도모하기 위해 사이버리스크 관리의 중요성이 높아졌다. 우리나라는 BCP 수립·운영실태를 점검하고 재택근무 관련 보안대책을 마련하였으나 코로나19 장기화 가능성에 대비하여 사이버보안에 공백이 생기지 않도록 주요국 사례를 참고하여 기존 BCP나 가이드라인들을 지속적으로 보완할 필요가 있다.

아울러 금융감독당국은 금융기관 경영실태평가의 일부로 반영되는 정보기술부문 실태평가[14] 수행 시 코로나19 이후 운영환경 변화로 새롭게 발생할 수 있는 사이버리스크 대응상황을 면밀히 점검하고 필요시 반영비중을 상향 조정하는 등 사전적 리스크 예방을 위한 감독 활동을 수행할 수 있어야 한다.

금융기관의 자체적인 노력도 지속적으로 요구된다. 금융기관은 가이드라인 등을 바탕으로 금융보안과 관련 내부 거버넌스를 강화하는 한편 충분한 수준의 IT 인력 및 예산을 확보하여야 한다. 또한 국가간 리스크 전파 가능성 등을 고려할 때 국제 공조체제에 적극 참여하여 관련 정보 획득에도 노력하여야 할 것이다.

11) 캐나다 중앙은행, 재무부, 금융감독원과 캐나다의 시스템적 중요은행 및 지정된 캐나다 금융시장인프라(지급·결제·청산 시스템 등)로 구성된 금융부문의 운영상 위협에 대응하기 위한 민관협의체이다.

12) ECB가 마련(18년)한 TIBER-EU 테스트는 사전에 알지 못하고 대응능력을 테스트 받는 금융기관 인력(blue team), 금융기관에 발생 가능한 위협을 점검하는 위협 인텔리전스 제공업체, 사이버 공격자를 모방하여 금융기관의 주요기능을 약화시키는 공격 시뮬레이션 수행 업체(red team), 금융기관내 테스트 수행을 알고 있는 소규모 인력(white team)과 테스트 수행 감독 책임을 부여받은 금융당국내 관련 팀(TIBER cyber team)의 참여로 진행된다.

13) "Are Banks Cyber-proof in the Digital World?", ECB, 2020년 10월

14) IT 보안을 포함한 금융기관의 정보기술부문 실태평가 결과는 경영실태평가의 경영관리 또는 위험관리 항목 평가비중(각각 15%)의 최소 20% 이상으로 반영되고 있다.