제12회 정보보호의 날 기념 세미나
기조연설 (7.19일)

디지털 금융혁신 시대의 금융보안 정책 방향

2023. 7.

금 융 위 원 회 위 원 장

김 주 현

I. 인사 말씀

안녕하십니까?
금융위원장 김주현입니다.

먼저 **제12회 정보보호의 날**을 맞이하여
이번 세미나를 주최하신
금융보안원 김철웅 원장님과 관계자 여러분,

그리고 이 자리에 참석하여 주신
금융회사, 핀테크사, 유관기관 대표자와

정보보호 최고책임자*(CISO)분을 비롯한
관련 **업무 종사자 여러분**들께
깊이 감사드립니다.

* CISO: Chief Information Security Officer
→「전자금융거래법」에 따라 **IT부문 보안 총괄 책임자**로 지정된 임원

오늘 **정보보호 유공 표창**을 받으시는
다섯 분께는 특별한
축하의 말씀을 드립니다.

Ⅱ. 디지털 금융혁신을 위한 노력

귀빈 여러분,

코로나19 이후 **전 산업에서**
비대면 거래가 가속화되면서
디지털 역량이
기업의 경쟁력을 좌우하는
핵심 기능이 되고 있습니다.

금융위원회는
금융권의 **디지털 전환 노력을 지원**하고
금융회사간 경쟁을 촉진하기 위해

민·관 합동의 혁신 TF 등
현장의견 수렴을 통한 **규제 개선,**
인공지능(AI) 활용 활성화 등을 위한 인프라 정비,
핀테크 산업 활성화를 위한
「K-Fintech 30」 선정 등
다양한 노력을 기울이고 있습니다.

Ⅲ. 디지털 금융의 위험요인

금융의 디지털 전환은
금융의 **효율성**과 소비자에 대한 **편리성 제고**라는
장점이 있는 반면,

금융보안 측면에서는
새로운 도전과제를 제시하고 있습니다.

여러 국제금융기구들은
이구동성(異口同聲)으로
디지털 위협요인에 대한 대응 강화를
주문하고 있습니다.

금융안정위원회(FSB)는
사이버 사고(Cyber Incident)의 **발생빈도**가
빠르게 증가할 뿐만 아니라
점차 **복잡한 형태로 변모**하고 있어
금융시스템의 위협요인이 되고 있다고 하면서,

금융의 디지털화와 **제3자 위탁**이
증가하고 있는 상황에서
사이버 위협에 대한 **효과적인 정보수집** 및
대응태세 마련의 필요성을 강조하였습니다.

* 「Achieving greater convergence in cyber-incident reporting」(22.10월)

그러나 디지털 금융의 **복잡성·다양성 등**으로 인해
사이버 사고를 사전적으로 원천봉쇄하는 것은
쉽지 않습니다.

사이버 보안이 강화되고 있지만
그에 대응한 **사이버 공격도 더욱**
고도화·지능화*되고 있기 때문입니다.

* 지능형 지속 공격(Advanced Persistent Threat) : 기술발전을 반영하여 새로운 전술과 기술을 이용하여 다양하게 장시간에 걸쳐 진행되는 사이버 공격

최근 **국제결제은행**(BIS)은
금융분야에서의 **보안 정책**이
리스크의 접근과 통제에 집중했던 **1세대 규제**에서
복원력 확보를 우선으로 하는 **2세대 규제**로
진화하고 있다고 분석했습니다.

* 「Bank's cyber security-a 2nd generation of regulatory approaches」(23.6월)

해외 선진사례 등을 **참고**하여
금융부문이 **사이버 위협**에 굳건히 버틸 수 있도록
금융시스템의 **사이버 복원력**(Cyber Resilience)을
강화해 나가야 하겠습니다.

국민의 재산과 개인정보 등이
안전하게 지켜지지 않는다면,
디지털 금융혁신은
사상누각(沙上樓閣)에 불과할 것이기 때문입니다.

Ⅳ. 금융보안 정책 추진방향

정부는 이러한 사이버 위협에 대응하기 위해
다음 3가지 측면에서 방점을 두면서
금융보안 정책을
추진해 나가고자 합니다.

첫째, 시시각각 변화하는 사이버 위협에
능동적으로 대응할 수 있도록
규칙중심의 경직적인 보안 규율체계를
'자율-책임'기반의 탄력적이고 유연한
원칙중심(Principle-based) 규율체계로
전환해 나가겠습니다.

이를 통해 금융회사 등이
스스로 보안 리스크를 분석·평가하고
리스크에 비례한 보안 방안을 수립할 수 있도록
자율적인 보안체계 구축을 지원하겠습니다.

둘째, 금융보안을 기업의 핵심가치로 인식하고
현업·IT·준법감시 부서 등
전사적 차원에서 준수할 수 있도록
보안 거버넌스 체계를 구축하겠습니다.

정보보호최고책임자(CISO)의 **권한 확대**,
중요 보안사항의 **이사회 보고 의무화** 등을 통해
금융보안을 기업경영전략의 핵심으로
자리잡도록 하여

여러분들이 **자부심을 갖고 금융보안 업무를**
수행할 수 있도록 하겠습니다.

셋째, 고도화되는 보안 위협에 따른
관리 사각지대를 해소하고
금융회사 등의 **보안관리 역량 강화**를
지원해 나가겠습니다.

클라우드 기반의 소프트웨어 서비스* 등
제3자 서비스 이용에 따른 리스크 관리 방안과
보안사고 후 **운영복원력****(Operational Resilience) **강화 방안 등**
그간의 관리 사각지대 해소방안을
모색하겠습니다.

* 서비스형 소프트웨어(Software as a Service): 인터넷을 통해 전문IT업체에서 제공하는 클라우드 기반 소프트웨어(문서관리, 화상회의 등)를 이용하는 서비스

** 사이버 공격으로부터 데이터·시스템을 보호하고, 신속히 운영을 재개할 수 있는 복구 능력

금융보안 전문기관 등을 통해
보안기술 공유 및 컨설팅, 보안인력 양성교육 등의
서비스를 제공하여 금융회사 등의
보안역량 강화를 지원하겠습니다.

V. 마무리 말씀

금융서비스의 디지털 전환에 대한
국민의 기대가 큽니다.

그러나 **견고한 보안 관리**를 통한
고객의 신뢰 확보 없이는
성공적인 디지털 전환이 불가능할 것입니다.

오늘 세미나가
디지털 혁신시대에
보안의 중요성을 되새기고

금융혁신과 정보보호의
선순환적 발전 방향을 모색하는
의미있는 장이 되기를 기대합니다.

감사합니다.