붙 임

금융IT부문 자율보안체계 확립 방안

금융위원회 · 금융감독원

목 차

Ⅰ. 추진경과

□ 금융위·금감원은 사이버공격 방어 및 정보유출사고 방지 등 **금융권 IT보안 강화**를 위하여

○ 그 동안 금융회사 및 전자금융업자*에게 특정 보안·인증기술의 사용 의무 등 보안 관련 규정을 항목별로 세세하게 규제해왔음

* 이하 '금융회사'는 전자금융거래법상 금융회사 또는 전자금융업자를 지칭

□ 최근 핀테크 산업 활성화를 위해 **IT보안규제**의 패러다임을 사전규제에서 **사후규제로의 전환**을 추진함에 따라,

➡ 금융회사 스스로 정보보안 및 내부통제를 강화하고 핀테크 시대에 부응하는 **민간 중심의 자율적 보안체계를 확립**할 수 있는 기반을 조성할 필요

□ **「금융IT부문 자율보안체계 확립방안」**은

○ **금융협회***, **핀테크업체, 금융보안원, 학계 전문가** 등의 의견수렴을 통해 마련되었으며,

* 은행·금투·생보·손보·여전협회

○ 동 방안은 **금융개혁 자문단 회의**('15.6.10)의 논의를 거쳐 **금융개혁회의**('15.6.18)에 보고되었음

<최근 전자금융 관련 규제 완화 내용>

규정 개정 내용	시행일	비고
매체분리 원칙 폐지	'15.2월	
보안프로그램 설치 의무 폐지	'15.2월	
공인인증서 사용의무 폐지	'15.3월	
인증방법평가위원회 폐지	'15.3월	
국가기관 인증 정보보호제품 사용의무 폐지	'15.3월	
금감원 보안성심의 의무 폐지	**'15.6월말 예정**	**규정개정 추진 중**

Ⅱ. 자율보안체계 확립을 위한 기관별 역할 정립

□ 금융보안 규제 패러다임이 타율적 규제에서 **원칙중심의 자율규제로 변화**함에 따라

○ **보안관리 주체별*** **역할**을 **재정립**하여 **규제공백 발생 우려 해소** 및 금융권 **자율보안체계**** **조기 안착**을 도모할 필요

* 금융위원회, 금융감독원, 금융회사, 금융협회, 금융보안원

** 시장 참가자들이 원칙적 규제의 틀 안에서 스스로 세부규율을 정하고, 이를 이행하기 위해 자율적으로 점검하는 자율규제 하의 보안체계

□ 주체별 역할

○ **(금융위·금감원) 전자금융거래법규** 등을 원칙중심으로 **정비**하고, 상시감시 및 검사 강화 등 금융권 **자율보안 기반 마련**

○ **(금융회사)** 자체 **보안 점검·관리체계 구축** 및 보안역량 강화

○ **(금융협회) 금융업권별**로 보안 관련 협의체 활성화 및 가이드 마련 등을 통해 **자율보안체계 기반 조성 지원**

○ **(금보원)** 금융회사 **자체 보안성 검토시 기술 지원,** 보안 **가이드 마련** 등 자율보안을 지원하는 **금융보안 전문기관**으로서 역할 수행

금융위·금감원	금융회사	금융협회	금융보안원*
▪ 금융보안 법규 정비(원칙 중심) ▪ 사후 검사·감독 및 책임 강화 ▪ 자율보안체계 기반 조성 등	▪ CEO 책임하에 실질적 보안역량 향상 ▪ 자율보안체계 확립 ▪ IT보안투자 확대, 자체점검, 내부통제 강화 등	▪ 업권별 특성을 반영한 민간자율 가이드 마련 ▪ 협의체 활성화 기반 조성 등	▪ 자율보안체계 확립 지원 기능 강화 ▪ FDS 정보공유 ▪ 금융 IT보안 정책 및 기술, 교육 지원 등

* 금융정보공유·분석센터(정보통신기반보호법 §16)
침해사고대응기관(전자금융거래법 §21의6)

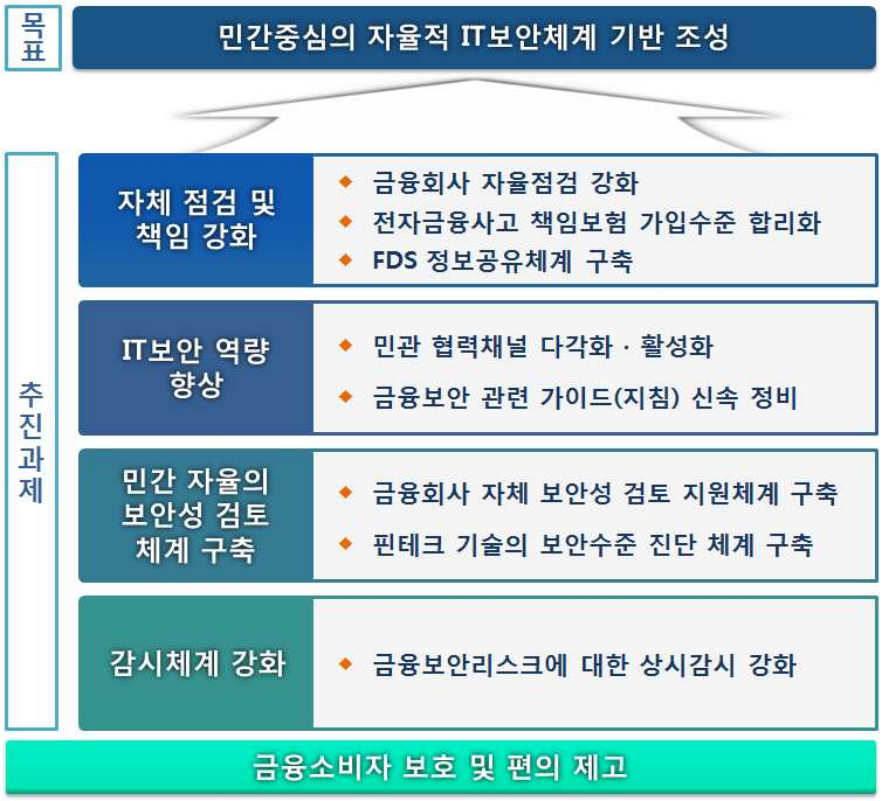
Ⅲ. 추진 목표 및 과제

< 기본 방향 >

◈ 금융회사의 **자체 점검 및 책임**을 강화하고 **IT보안 역량 향상** 도모

◈ 보안성심의 폐지 등에 따라 **민간 자율의 보안성 검토 체계**를 구축하고, 금융보안 리스크에 대한 **상시 감시체계 강화**

➡ 금융회사가 **자율적인 IT보안체계**를 **확립**할 수 있는 기반을 조성함으로써 **금융소비자 보호 및 편의성** 제고



Ⅳ. 세부 추진방안 및 기대효과

1 자체 점검 및 책임 강화

1-① 금융회사 자율점검 강화

가. 현황 및 문제점

□ 금융회사의 IT보안상 **취약점은 해당 금융회사가 가장 잘 파악**할 수 있으나,

○ **IT감사 전문인력이 부족**한 중소형 금융회사는 IT부문에 대한 위규사항 자체 감사·점검에 어려움

□ 규정상 **정보보안 및 외부주문보안 점검 의무***는 점검주기에 비해 점검항목이 많아 금융회사가 **형식적으로 이행할 가능성** 상존

* 정보보안 점검(전자금융감독규정 §37조의5) : 매월 점검(34개 항목), CEO에 보고
외부주문 보안점검(규정 §60①14) : 중요 점검사항 매일 점검(12개 항목)

나. 개선방안

□ IT감사 역량이 부족한 금융회사 지원을 위해 **IT 내부감사 가이드라인** 및 IT 내부감사요원 **교육프로그램**을 마련하고,

○ 상시적인 내부통제 강화를 위해 감사부서 내 IT감사 전담 인력을 배치토록 권고

□ 기 시행중인 **'IT부문 금융회사 내부감사 협의제도***'**의 대상 금융회사 및 점검항목**을 확대하여 **내실화 도모**

* 금융회사가 자체감사를 통해 IT보안관련 미흡사항을 발굴·개선하고 금감원은 이행결과 확인 및 사후 관리('15년 38개 금융회사 대상으로 실시 중)
** 현재 외부주문, 전자금융사고 책임이행보험 등 6개 분야 13개 항목

□ **정보보안 및 외부주문 관련 보안 점검**의 실효성 제고를 위해 지나치게 세세한 점검항목을 **필수항목 위주로 개편**

1-② 전자금융사고 책임보험 가입수준 합리화

가. 현황 및 문제점

□ 최근 전자금융사기에 의한 사고는 지속 증가하는 추세이며,

○ 전자금융거래법 제정('06년) 당시 설정된 **전자금융사고 책임이행 보험 가입 최저한도***가 전자금융거래 **규모에 비해 낮은 것**으로 평가됨

* (시중은행) 20억원, (지방은행, 카드사) 10억원, (금투업자) 5억원, (자금이체업자, 직불업자) 2억원, (기타 전자금융업자) 1억원 등

○ 최근 일부 금융회사의 경우 사고 증가로 인해 보험을 추가 가입하여 **보상한도를 증액**(20억→30억)한 사례

<최근 3년간 전자금융사기 등 사고건수>

연도	'12	'13	'14
전자금융사기 등 사고건수*	147건	2,703건	2,867건

* 전자금융사기에 의한 접근매체 위변조 등 전자금융거래법 제9조제1항 관련 사고로 인해 이용자에게 손해가 발생한 경우

나. 개선방안

□ 전자금융사고 빈발 금융회사에 대해서는 책임보험 가입금액을 **적정수준 이상으로 증액**토록 권고

○ 금융회사 스스로 **전자금융거래 규모, 사고발생 추이, 보안투자규모 등**을 종합 검토하여 **적정 보험가입 금액 산정**

* 예시 : 법규상 기준금액과 적정 보험가입 금액 산정 결과 중 큰 값으로 산정

- 동 산정 내용은 금융회사가 매년 제출하는 'IT부문 계획서'에 기재하여 **금감원이 사후 점검**하고 현장검사시 **보험가입 이행실태 확인**

1-③ FDS* 정보공유체계 구축

* 이상금융거래탐지시스템(Fraud Detection System) : 전자금융거래 접속정보, 거래내역 등을 종합적으로 분석하여 이상금융거래를 탐지 및 차단하는 시스템

가. 현황

□ 금감원은 **이상금융거래에 대한 공동대응**을 위해 '금융권 **FDS 추진협의체**'(은행 16개, 증권 14개, 금보원)를 구성·운영* 중이나

* 「금융권 FDS 고도화 로드맵('14.12월)」
: (1단계) FDS 도입 → (2단계) FDS 확대 → (3단계) 금융권 공동대응

○ 이상금융거래 정보의 전파·공유를 통해 FDS 대응수준을 보다 향상시키기 위해서는 全 금융권으로 협의체를 확대 구성할 필요

나. 개선방안

□ 이상금융거래 정보공유를 위한 **공통 기준을 마련**하고 금융 정보공유·분석센터(ISAC)를 운영하는 **금보원에 FDS 정보공유시스템을 구축**

○ 기존 FDS의 고도화가 필요한 **카드사 및 PG사** 등으로 FDS **협의체를 확대**하여 **정보공유 효과를 극대화**

기대효과

- 금융회사 스스로 IT보안 위규사항 발굴·보완하는 내부감사 일상화로 **자체 보안수준 향상**
- 전자금융사고 발생을 억제하고 **능동적인 책임이행 도모**
- 全 금융권 공동대응 체계 구축으로 **이상금융거래 대응수준 대폭 향상**

2 IT보안 역량 향상

2-① 민관 협력채널 다각화·활성화

가. 현황 및 문제점

□ 금융IT 관련 협의체로 금융정보보호협의회, CISO협의회 등이 운영되고 있으나 일부 소통 채널의 경우 활동이 저조

○ **전자금융업자**의 경우 협회나 협의체가 구성되지 않아 타 권역에 비해 **상호 교류가 미비**

○ 금융회사의 자율성이 보장되는 현 상황에서 금융보안 우수·사고사례 등의 양적·질적 축적을 위한 **정보공유·협업이 무엇보다 중요**

나. 개선방안

□ 공공-민간 협력과 금융업권별 교류 활성화를 위해 **협의체를 다각도로 구성**하고 **전자금융업자의 협의체 구성을 독려**

○ 금융위·금감원-금융회사, 금융회사간, 권역간, 직급별(관리자, 실무자) 등으로 협의체를 다각화하고 **협의체별 모임을 정례화**

- 금융보안 **우수·사고사례 전파**, 금융ISAC(금보원)의 침해 위협 및 사고 분석결과 공유*, **규제 개선사항 발굴** 등의 창구로 활용

* 최근 금융ISAC 운영주체 변경(금결원·코스콤→금보원) 및 보안관제 대상 금융회사의 확대로 **조직적 침해대응 능력 향상** 기대

<금융IT부문 협의체 다각화(예시)>

	현행(금융정보보호협의회)	➡	개편(예시)
자문단	—		금융위, 금감원, 학계·산업계·유관기관 등 전문가
임원급	협의회, 소협의회		**CISO협의회**(매분기)
부서장급	—		**부서장협의회**(매분기)
실무자급	실무협의회		**실무협의회**(매월)

※ 사무국 : 금융보안원

<금융IT부문 협의체별 활동(예시)>

- (금융위·금감원-금융회사) 최근 사고사례 전파, 규제 개선사항 의견 수렴 등
- (CISO) 금융보안 거버넌스 사례 공유 등
- (실무자) 금융보안 조사·연구결과 공유 등
- (권역간) 금융권 공동 대응 논의 등

2-② 금융보안 관련 가이드(지침) 신속 정비

가. 현황

□ 규제 완화 및 다양한 핀테크 적용제품 출시 등으로 금융회사가 **보안정책 수립 및 의사결정시 참고**할 민간자율의 **가이드 수요 증가**

○ 또한, 최근 법규 개정사항 반영 등 금융회사 **자체 내규의 현행화** 필요

나. 개선방안

□ 신규 보안기술·인증수단 등의 도입, 법규준수를 위한 실무 지침 등 **가이드라인**을 민간자율로 **적기 제정 유도***

* 또 다른 규제가 되지 않도록 **민간자율 제정**을 원칙으로 하되, 필요시 감독기관이 T/F 구성 등 협의 기반 조성

○ 아울러 최근 법규 개정사항을 기존 금융보안 관련 가이드라인*에 반영하고 현 실정에 맞지 않는 과거 가이드라인을 정비

* 금융전산보안 표준지침(내규 예시)('14.12월, 협회, 금보원) 등

기대효과

- IT보안 정보공유 및 협업의 활성화로 **금융권 전반의 보안수준 및 침해대응 능력 향상**
- 민간 주도의 가이드 마련을 통해 **자율규제 풍토 조성** 및 **개별 금융회사의 자율성 보장**

3 민간 자율의 보안성 검토 체계 구축

3-① 금융회사 자체 보안성 검토 지원체계 구축

가. 현황

□ 금융회사의 부담을 완화하고 자율적인 보안수준 확보 노력을 유도하고자 보안성심의 제도를 폐지함에 따라('15.6월 예정)

○ 금융회사 **자체 보안성 검토의 실효성 확보를 지원**할 필요

나. 개선방안

□ 금융회사가 자체 보안성 검토시 활용할 수 있도록 금감원의 **보안성심의 주요 사례를 분석·제공**하고,

○ 금융회사가 **객관적인 전문가 진단 필요시** 금융보안 전문기관(금보원 등)에 **보안성 검토를 의뢰**할 수 있는 **프로세스 구축**

3-② 핀테크 기술의 보안수준 진단 체계 구축

가. 현황

□ 핀테크 기술에 대한 **객관적인 보안성 검증 체계가 미비**하여 금융회사와 핀테크 업체가 기술 도입 및 보급에 어려움

나. 개선방안

□ **핀테크 업체**가 자신이 보유한 기술에 대해 금융보안 전문기관에게 **보안수준 진단을 의뢰**할 수 있도록 **세부 절차 및 운영환경을 마련**하고

○ **핀테크 지원센터**가 핀테크 기업의 **보안수준 진단의뢰** 및 보안진단 후 **금융회사 제휴 알선** 등을 **지원**

기대효과

▶ 객관적인 전문기관의 보안수준 진단을 통해 **전자금융서비스의 안전성 확보** 및 **정보보안을 전제**로 한 금융회사-핀테크 업체간 **협업 활성화 도모**

4 감시체계 강화

4-① 금융보안리스크에 대한 상시감시 강화

가. 현황 및 문제점

□ 금융회사는 규정상 IT부문 계획서, 취약점 분석·평가보고서 등 목적에 따라 여러 보고서*를 정기·수시로 금융위·금감원에 제출하고 있으나

* ① 업무보고서, ② 정보기술(IT)부문 계획서, ③ 취약점 분석·평가 결과보고서, ④ 정보기술부문 및 전자금융 사고보고서, ⑤ 자체 보안성심의 결과보고서, ⑥ 전자금융보조업자의 재무건전성 및 서비스 품질수준 평가결과 보고 등

○ 주요 항목을 누락하거나 축약 기재 하는 등 일부 금융회사의 **보고서 품질이 미흡**

나. 개선방안

□ 금융회사가 금융IT 및 정보보안에 대한 **연간계획을 면밀히 수립**하고 이에 대한 내용을 충실히 기재·제출할 수 있도록

○ **IT부문 계획서**, 취약점 분석·평가보고서 등의 **표준양식 제정** 및 이에 대한 **점검 강화**

□ 금융회사의 **신규 전자금융서비스** 관련 **자체 보안성검토 결과 점검** 및 시장 모니터링을 강화하고 취약점 발견 등 **필요시 보완·개선 권고**

□ 금융회사 제출 보고서를 통해 IT인력·예산비율, CISO 지정 및 전자금융사고 책임이행보험, 전자금융업자의 경영지도기준 등 **법규 준수 현황**을 정기적으로 **분석·평가**하고 금융회사 **현장검사시 활용**

기대효과

▶ 금융회사의 IT보안체계 확립을 독려하고 다양한 상시감시 수단을 통한 **사후 점검 및 검사 강화 기반 구축**

Ⅴ. 추진일정

이행과제	주관	일정
〈자체 점검 및 책임 강화〉		
1-① 금융회사 자율점검 강화		
'15년 IT부문 금융회사 내부감사 협의제 결과 확인 및 IT 내부감사 현황 점검	금감원	'15.3/4분기
IT 내부감사 가이드라인 마련	금융협회, 금보원	'15.4/4분기
IT 내부감사요원 양성을 위한 교육프로그램 개발·운영	금보원	'15.4/4분기
정보보안 및 외부주문보안 점검항목 개선 (필요시 가이드라인 마련, 시행세칙 개정)	금감원, (금융협회, 금보원)	'15.4/4분기
1-② 전자금융사고 책임보험 가입수준 합리화		
전자금융사고 책임이행 보험금의 증액방안 마련	금감원	'15.3/4분기
1-③ FDS 정보공유체계 구축		
FDS 추진협의체 확대 운영	금감원, (금보원)	'15.3/4분기
FDS 정보공유시스템 구축	금보원	'15.4/4분기
〈IT보안 역량 향상〉		
2-① 민관 협력채널 다각화·활성화		
금융IT 협의체 다각화 및 정례화	금융위, 금감원, 금보원	'15.3/4분기
금융ISAC 보안관제 대상 금융회사 확대	금보원	연중
2-② 금융보안 관련 가이드(지침) 신속 정비		
금융보안 관련 가이드 제정 및 정비	금융협회, 금보원	연중

이행과제	주관	일정
〈민간 자율의 보안성 검토 체계 구축〉		
3-① 금융회사 자체 보안성 검토 지원체계 구축		
금감원 보안성심의 주요 사례 분석·제공	금감원	'15.6월말
금융회사 자체 보안성 검토 지원을 위한 세부 기준, 절차 및 운영환경 구축	금보원	'15.6월말
3-② 핀테크 기술의 보안수준 진단 체계 구축		
핀테크 보안성진단을 위한 세부 기준, 절차 및 환경 구축	금보원	'15.3/4분기
핀테크 지원센터와 연계방안 마련	금융위, 금감원, 금보원	'15.3/4분기
〈감시체계 강화〉		
4-① 금융보안리스크에 대한 상시감시 강화		
금융보안리스크에 대한 상시감시	금감원	연중
'정보기술부문 계획서', '취약점 분석·평가 결과 보고서' 등 표준양식 제정	금감원	'15.3/4분기