http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.24, No.4, November 2019, pp.79-107
https://doi.org/10.7838/jsebs.2019.24.4.079

개정된 유럽연합 지급결제서비스지침의 보안위험에 대한 제도적인 대응과 관련 국내 전자금융 규제와의 비교 연구

Comparison Study between Institutional Response to Security Risks of the EU's Revised Payment Services Directive and Domestic Electronic Finance Regulation

김현부(Hyun Boo Kim)*, 김인석(In Seok Kim)**

초 록

전통적으로 은행 등 금융기관은 자신이 관리하는 고객의 계좌와 정보를 이용하여 지배적인 위치에서 금융서비스를 제공하여 왔다. 최근 유럽연합은 지급결제서비스지침을 개정하여 고객 계좌에 대한 접근과 계좌 관련 정보의 제공을 제3자에게도 허용하는 것을 제도적으로 보장하여, 금융시장에서 경쟁을 촉진하고 혁신을 도모하고 있다. 그렇지만 이러한 변화는 잠재적인 보안위험을 증가시킬 수 있으며, 따라서 신·구 시장참여자 모두가 금융시장에서 보안위험에 적합하게 대응할 수 있도록 금융당국의 제도적인 대응이 요구된다. 본 연구에서는 유럽연합의 새로운 지급결제서비스지침(Payment Service Directive, PSD2)에서 확인할 수 있는 보안위험에 대한 제도적 대응을 분석하고 이를 국내의 전자금융규제와 비교·분석하여 시사점을 도출함으로써 국내 전자금융규제의 개선 방향을 제안하고자 한다.

ABSTRACT

Traditionally banks and other financial institutions use customers' accounts and information managed by them and provide payment services in dominant positions. Recently, EU amends Payment Services Directive to institutionally guarantee access to customers' accounts and use of account-related information even to third parties, which facilitates competition in financial markets and promotes innovation. However, this kind of change can increase potential security risks and therefore institutional responses from financial authorities are required so that all participants in financial markets can properly respond to security risks. In this study institutional responses to the security risks in the EU's new Payment Services Directive (PSD2) are analyzed, comparisons between this and domestic electronic financial regulations are analyzed, and implications for the direction of improving domestic electronic financial regulations will be suggested.

키워드 : 전자금융규제, 지급결제지침, PSD2, 보안위험, 위험평가
Electronic Finance Regulation, Payment Service Directive, PSD2, Security Risk, Risk Assessment

* First Author, Graduate School of Information Security, Korea University(wagamichi@hanmail.net)
** Corresponding Author, Graduate School of Information Security, Korea University(iskim11@korea.ac.kr)
Received: 2019-10-02, Review completed: 2019-10-30, Accepted: 2019-11-12

1. 서 론

인터넷의 발전과 스마트폰의 확산 등 정보기술(Information Technology, 이하 IT)의 발전으로 인터넷뱅킹이나 모바일뱅킹과 같은 새로운 유형의 금융서비스를 제공하는 것이 가능해졌으며, 그 규모도 지속적으로 확대되고 있다. 한국은행에 따르면 인터넷뱅킹과 모바일뱅킹 모두 이용 고객과 이용량이 크게 증가하였는데, 이용 고객은 2001년 약 113만 명에서 2017년 약 1,350만 명으로, 같은 기간 동안 이용 건수는 약 100만 건에서 약 3,464만 건으로 증가하였다[1]. 이와 같은 금융시장에서 IT의 영향력 증가에 대하여, Ju[21]은 한국 금융생태계의 경쟁력 유지를 위해 요구되는 생산성, 강건성, 기회 창조성, 민첩성의 지속적인 향상에는 IT의 역할이 핵심적이라고 주장하여 금융시장에서 IT의 역할을 강조하였다.

최근에는 금융회사가 IT를 이용하여 서비스를 제공하는 수준을 넘어 금융과 IT를 융합한 새로운 금융서비스인 핀테크(fintech)로 IT기업 등 새로운 유형의 시장참여자가 금융시장에 경쟁을 통한 혁신을 가져오고 있는데, 실제로 한국은행에 따르면 간편결제와 간편송금 등 신종전자지급서비스의 이용 건수와 금액이 2017년 기준 전년 대비 각각 175.6%, 212.0% 증가하는 높은 성장세를 보여주고 있다[1].

이런 IT와 핀테크를 통한 금융시장의 혁신에 대해, Park et al.[35]은 IT의 급속한 확산, 모바일 중심의 전자상거래 증가, 글로벌 금융위기 이후 새로운 금융의 모색 및 산업발전을 위한 규제 해제 등 각국 정부의 정책적인 핀테크 지원 등을 발전 배경으로 제시하고, 향후 금융서비스와 금융회사의 분리로 금융업의 독점적인 성격이 약해지고 자본보다 정보가 중요해지는 등 핀테크가 금융시장에 혁신적인 변화를 가져올 것이라고 분석하였다.

유럽연합(European Union, EU)이 2015년에 개정한 지급결제서비스지침(Payment Service Directive2, 이하 PSD2)[37]은 IT라는 기술과 규제라는 정책 수단을 이용하여 시장의 혁신을 도모한 대표적인 사례이다. PSD2는 계좌를 관리하는 금융기관이 지배적인 위치에서 활용하였던 고객 계좌와 관련 정보 등을 오픈API(Open Application Programming Interface, 이하 오픈API)라는 IT를 이용하여 핀테크 기업 등 제3자도 비차별적으로 접근할 수 있도록 제도화하고, 이를 통해 금융서비스 이용자에게 기존과 다른 새로운 유형의 서비스를 제공하는 것이 가능하도록 하였다. 국내 금융당국도 PSD2와 유사한 방식으로 금융시장의 혁신을 추진하고 있는데, 소관 부처인 금융위원회는 2018년 3월에 핀테크 시장의 확대를 위한 금융시장의 오픈API 활성화[15], 2018년 7월에는 금융회사가 고객의 금융정보를 제3자인 마이데이타 사업자에게 API를 통해 제공하도록 의무화하는 금융 분야 마이데이터 산업 도입[11], 2019년 2월에는 은행에 대한 자금이체 기능 등의 API 제공 의무화 및 오픈뱅킹 법제도화 추진[16] 등을 발표하였다.

본 연구는 PSD2와 관련 선행연구 등을 분석하여 법규와 제도의 변화 및 그 배경을 확인하였다. 그리고 금융기관이 계좌를 폐쇄적으로 보호하던 기존과 달리, 다양한 기관에게 오픈API를 통한 계좌 접근과 정보이용을 보장하여 상대적으로 보안위험이 높아진 환경에서 금융시장의 경쟁 촉진과 혁신 도모라는 정책 목표를 훼손하지 않으면서도 보안위험으로부터 계

좌와 정보를 안전하게 보호하기 위한 PSD2의 제도적인 대응을 분석하였다. 마지막으로 PSD2의 보안위험에 대한 제도적인 대응과 전자금융감독규정 등 국내 전자금융의 보안위험 대응 관련 규제를 비교·분석하여 유의미한 시사점을 도출하고 국내의 관련 법규와 제도에 대한 개선방안을 제시하였다.

2. PSD2의 특징과 오픈 API의 이용

2.1 PSD2의 개요와 목적

PSD2는 유럽연합에서 이루어지는 지급결제서비스를 규제하는 기존 지침(Payment Service Directive, PSD)을 2015년에 전면 개정한 것으로, 유럽연합 의회에서 공표한 지침(Directive)에 대해서는 회원국들이 지정된 기일까지 자국의 법규를 마련해야 하므로[23], 유럽연합에서는 PSD2에서 규정하고 있는 제3자의 계좌에 대한 접근 확대가 제도화된다고 할 수 있다.

유럽연합 의회는 PSD2 서문에서 인터넷과 모바일의 발전 등으로 기존 지침의 규제 범위를 넘어서는 새로운 유형의 혁신적인 금융서비스가 등장하여 법적 불확실성과 잠재적인 보안위험 및 소비자 보호의 취약성이 높아지고 금융서비스의 안전한 제공을 어렵게 한다고 배경을 설명하고, 이용자의 요청에 근거하여 이용자의 계좌와 다른 서비스 제공자의 계좌 사이의 지급결제를 개시하는 지급결제지시서비스(Payment Initiation Service, PIS), 복수의 서비스 제공자가 보유한 이용자의 계좌 관련 정보를 통합하여 온라인으로 이용자에게 제공하는 계좌정보서비스(Account Information Service, AIS) 등 새로운 유형의 금융서비스를 규제체계에 포함하였다고 제시하였다[37]. 이는 IT의 발전과 핀테크의 확산에 따른 새롭고 혁신적인 서비스의 도입이 금융시장에서 긍정적인 요인으로 작용하기 위해서는, 기존 규제체계에서 발생하는 규제공백이라는 부작용을 해소하여 서비스와 시장에 대한 신뢰와 안정의 확보가 필요하기 때문이다.

이처럼 IT의 발전과 핀테크의 확산은 금융시장에 대한 규제에 많은 영향을 미치고 있는데, 미국의 경우에는 2018년 7월에 통화감독청(Office of the Comptroller of the Currency, OCC)이 핀테크 기업에 대하여 제한적인 업무범위와 영업수단으로 금융시장에 참여할 수 있는 특수목적연방은행(Special purpose national bank)의 인가 신청을 허용하여[34], 금융시장에서 확산되는 IT 기반의 새로운 금융서비스도 기존 규제체계에 포함될 수 있도록 하였다.

PSD2 제66조와 제67조에서는 지급결제지시서비스와 계좌정보서비스 등 새로운 유형의 금융서비스를 규제체계에 포함하면서, 동시에 계좌를 관리하는 금융기관이 아닌 제3가 제공하는 이러한 서비스를 이용하는 것이 계좌 소유주인 이용자의 권리임을 명시하였으며, 동시에 계좌 관리 금융기관(Account Servicing Payment Service Provider, ASPSP)에 대해서는 이러한 이용자의 권리를 보장하기 위하여 계약 관계 등과 무관하게 제3자가 서비스를 제공하는데 필요한 정보와 기능을 제공할 의무를 부과하고 계좌 관리 금융기관과 제3자가 제공하는 동일한 서비스 간에 성능이나 요금 등의 불합리한 차별을 금지하여, 제3자의 계좌 접근과 정보이용을 비차별적으로 보장함을 명확히 하였다.

또한, 서문에서 제3자는 지급결제지시서비스와 계좌정보서비스의 제공을 위해서 계좌 관리 금융기관의 비즈니스 모델에 종속되지 않으며, 계좌 관리 금융기관은 제3자의 서비스 제공을 위해 제공하는 기능에 대하여 다양한 통신 기술에 대한 호환성을 확보해야 하고, 이용자가 제3자의 서비스를 이용할 때에는 이용자와 계좌 관리 금융기관 간의 통신 없이 제3자와의 통신만으로 서비스를 이용할 수 있어야 한다고 제시하여, 제3자가 서비스를 제공하는 데 있어 계좌 관리 금융기관이 부정적인 영향을 미칠 수 있는 요소를 억제하고 제3자의 독립적인 서비스 제공을 용이하게 하였다.

이처럼 PSD2는 IT에 기반한 새로운 유형의 혁신적인 서비스를 규제 범위에 포함하는 동시에, 규제 범위 안에서는 제3자가 자신이 관리하지 않는 계좌와 정보라는 자원을 사용하여 기존 금융기관에 종속되지 않고 서비스를 제공할 수 있도록 규제라는 수단을 이용하여 제도적・기술적 환경을 보장하고 있다. 이에 대해 Wolters et al.[39]은 PSD2가 보안을 강화하는 내용을 제시하고는 있지만, 위험이 증가할 수 있음에도 불구하고 제3자를 포함하여 서비스 제공기회를 확대하는 원칙을 고수하고 있으며, 이를 통한 금융시장의 발전을 계좌와 관련 정보의 보호보다 우선시하고 있다고 분석하였다.

PSD2는 새로운 유형의 서비스를 제공하는 신규 시장 참여자를 통해 계좌에 대한 기존 금융기관의 독점을 해소하고, 금융시장의 혁신을 도모한다는 정책 목적을 설정하고, 이 목적의 달성을 위하여 필요한 이용자의 신뢰와 시장의 안정성 확보를 위하여 예상되는 보안위험에 대응한 것으로 볼 수 있다. 즉, 기존 금융기관이 인터넷뱅킹과 모바일뱅킹 등 IT를 적극적으로 활용하여 서비스를 제공하고 있지만, 계좌에 대한 접근과 관련 정보를 지배적으로 이용하는 환경에서는 혁신을 위한 동기부여가 부족할 수밖에 없으며, 따라서 정부가 PSD2라는 규제를 수단으로 계좌와 정보를 제3자에게 개방한 것이다.

이에 대해 Milne[27]은 혁신을 위해서는 경쟁 관계인 은행 간에 협조가 필요한 금융시장의 네트워크 구조 때문에 은행이 기존 IT시스템을 업그레이드하는 비용과 위험이 혁신에 따른 상업적인 이익을 상회하여, 금융서비스 이용자에게 이익이 된다고 하여도 은행이 적극적으로 혁신적인 서비스를 도입하기 어렵게 만든다고 분석하고, 이것이 금융시장에서 경쟁과 혁신을 촉진하기 위해 유럽연합이 PSD2와 같은 정책 수단을 이용한 원인이라고 제시하였다.

그리고, Cortet et al.[2]은 금융시장에서 혁신적인 서비스를 제공하는 주체가 주로 은행이 아닌 IT기업이나 핀테크기업과 같은 제3자인 점 등을 근거로, 유럽연합이 금융시장에서 경쟁과 혁신을 제한하는 원인이 은행의 높은 지배력이라고 판단하고 다양한 규제 수단을 도입하였으며, PSD2에서는 이런 지배력 문제를 해소하기 위해 금융기관이 아닌 제3의 시장참여자를 통한 경쟁과 혁신을 도모한 것이라고 분석하였다.

2.2 제3자에 대한 계좌 접근 허용과 오픈 API

앞서 확인한 것처럼 PSD2는 계좌 관리 금융기관에 대하여 제3자에 대한 계좌 접근 수단의

제공을 의무화하면서 동시에 기술・성능・비용・계약관계 등에 대하여 비차별적으로 제공하도록 규정하고 있는데, 이러한 요건을 충족하기 위한 기술적 수단으로 제시되고 있는 것이 오픈에이피아이(Open Application Programming Interfaces, 이하 오픈API)이다.

API는 시스템 사이의 연계를 위한 대표적인 프로그래밍 기법으로, API 이용자는 기능의 구조・원리 등에 대한 이해 없이도 원하는 결과를 용이하게 획득할 수 있고, API 제공자는 내부 시스템에 대한 노출을 제한하면서도 규정된 기능을 제공할 수 있다. 오픈API는 API의 제공범위를 기관 외부까지 확대한 것으로, 이를 통해 은행 등 계좌 관리 금융기관이 폐쇄적인 환경에서 관리하는 계좌에 관한 정보와 기능을 온라인을 통해 제3자에게 비차별적으로 제공하는 것이 가능해진다. 유럽은행연합(Euro Banking Association)은 API가 정보시스템 간의 통신을 위한 표준화된 요구사항의 집합이며 서로 다른 조직의 정보시스템 간 연계에 있어 비용과 시간을 절감하고 혁신을 용이하게 하는 기술수단이라고 설명하고 있다[3].

다만, PSD2에서는 계좌 관리 금융기관에 대하여 제3자에 대한 계좌 접근을 허용하도록 규정하면서 동시에 허용 대상에 제한을 두었는데, 제11조에 따라 지급결제지시서비스와 계좌정보서비스 등 모든 규정된 서비스는 금융당국의 허가를 받았거나 등록한 기관만 제공할 수 있으며, 제66조와 제67조에서 계좌 관리 금융기관이 계좌에 대한 접근과 정보를 제공하는 대상도 불특정 다수가 아닌 허가를 받았거나 또는 등록된 기관만으로 제한하였다. 이에 대해 유럽은행연합 역시 향후 계좌 관리 금융기관 등이 PSD2를 준수하기 위해 제공하는 오픈API의 개방수준은 <Table 1>과 같은 4단계 중 사전에 정의된 자격을 충족한 기관만이 API를 이용할 수 있는 맴버(Member) 수준에 해당할 것이라고 분석하였다[3].

이처럼 PSD2에서 은행 등 계좌 관리 금융기관이 제공하는 오픈API를 이용하여 이용자의 계좌에 접근할 수 있는 제3자의 범위를 제한하는 것은, 계좌 접근 대상이 확대됨에 따라 기존의 폐쇄적인 환경에서 계좌를 보호하는 것과 비교하여 보안위험이 증가하고 사고 발생 가능성이 커질 수 있으므로, 제3자에 대해서도 금융서비스를 제공하는 기관으로서 보안위험을 관리하고 사고에 대응할 수 있도록 자격 요건을 설정한 것이다. Gozman et al.[20]은 PSD2에서 오픈API를 통해 제3자에게 계좌 접근이 확대되어 은행 등 계좌 관리 금융기관에 대한 침해사고, 이용자 정보의 부정한 이용, 프라이버시 침해 등의 위험이 커지므로, 보안위험 대응이 금융시장에 대한 이용자의 신뢰 유지에 중요하다고 분석하였다.

〈Table 1〉 Levels of API Openness (Reconstruction of References [3]'s 〈Figure 2〉)

Type	Openness Level	Accessibility
Closed API	Private	banks only.
Open API	Partner	banks' prefererred partners.
	Member	members belonging to a community.
	Acquaintance	anyone complying with a predefined set of requirements.(e.g. contract)
	Public	anyone

금융시장은 금융기관이 이용자의 자금과 정보를 안전하게 보호할 것이라는 신뢰 없이는 유지되기 어려우므로, PSD2에서는 시장에서 경쟁을 촉진하고 혁신을 도모한다는 정책 목표를 달성하기 위한 계좌 접근 대상의 확대뿐만 아니라, 기관이 보안위험을 평가·관리하고 대처할 수 있도록 하기 위한 제도적 대응도 함께 포함하고 있다.

본 연구에서는 PSD2에서 확인할 수 있는 보안위험에 대한 제도적 대응과 이에 대응하는 국내의 전자금융 규제를 시장 진입을 위한 허가 또는 등록 단계와 시장 진입 이후 서비스를 제공하는 단계를 중심으로 비교·분석하여, PSD2와 같은 오픈API를 이용한 계좌 접근 확대와 새로운 금융서비스의 도입을 통해 금융시장의 혁신을 도모하는 상황에서 국내 전자금융 규제의 개선을 위한 의미 있는 시사점을 도출하고자 한다.

3. PSD2의 보안위험에 대한 제도적 대응 분석

PSD2는 지급결제지시서비스와 계좌정보서비스 등 계좌를 관리하지 않는 제3자가 제공할 수 있는 금융서비스를 새롭게 규제 대상으로 포함하고, 보안위험 대응을 포함한 자격 요건을 충족한 기관만 서비스의 제공이 가능하도록 명시하였기 때문에, 이러한 서비스가 규제 범위에서 벗어나 있던 개정 이전보다 보안 수준이 향상되었다고 평가할 수 있다.

그러나 앞서 확인한 것처럼 은행 등 계좌 관리 금융기관으로서는 이용자의 계좌에 대한 제3자의 접근이 제도적으로 보장되는 것은 자신의 통제 범위 외부에서 계좌에 접근할 수 있는 대상이 지속해서 증가한다는 것을 의미하며, 이는 잠재적인 보안위험을 높일 수 있다. 유럽연합은 PSD2의 서문에서 최근 전자금융거래에 대한 보안위험이 증가하고 있으며, 이러한 보안위험으로부터 소비자를 보호하고 안전성을 확보하는 것을 시장이 올바르게 작동하는데 있어 핵심적인 요건으로 제시하였고, 동시에 새롭게 규제 범위에 포함한 계좌정보서비스와 지급결제지시서비스에 대해서도 서비스 이용자의 정보를 보호하고 기존 규제체계에서 발생했던 보안 문제에 대응 하는 것이 중요하다는 것을 명확히 하였다[37].

그리고 Noctor[33]이 언급한 것처럼 은행과 같은 기존 금융기관은 보안이 기관의 평판에 미치는 영향 등을 고려하여 보안에 많은 관심을 두고 투자하지만, 금융기관이 아니면서 금융서비스를 제공하는 제3자는 보안에 높은 우선순위를 두지 않는 경향이 있기 때문에, 은행 등 기존 규제 대상도 잠재적 보안위험에 충실히 대응할 수 있고 새롭게 금융시장에 진입하는 기관도 금융시장에 적합한 적정 수준의 보안체계를 보유하도록 규제할 필요가 있다.

위와 같은 상황을 반영하여 PSD2에서는 지급결제지시서비스와 계좌정보서비스 등을 제공하려는 제3자를 포함한 지급결제기관의 허가 또는 등록 요건으로 보안위험 대응·관리에 관한 요건을 새롭게 포함하였으며, 금융시장에서 실제 서비스를 제공하는 과정에서도 보안위험관리체계의 일관성 있는 운용과 지속적인 개선을 요구하고 있다.

3.1 허가 또는 등록 단계에서의 제도적 대응

지급결제지시서비스나 계좌정보서비스를 제공하려는 제3자를 비롯하여 지급결제서비스 제공을 희망하는 기관은 PSD2 제5조에서 지정한 요건을 충족하여 소관 금융당국의 허가를 받거나 등록을 하여야 하며, 이 때 다른 서비스는 제공하지 않고 계좌정보서비스만 제공하는 경우는 등록 대상이며 그 외의 경우는 허가 대상이다.

제5조 제1항에서는 허가 또는 등록 시에 충족해야 하는 17개의 요건을 제시하고 있으며, 이 중 ① 보안사고와 이용자 불만 등에 관한 처리절차 및 금융당국에 대한 사고보고 체계(f호), ② 민감한 지급결제 정보(Sensitive payment data, PSD2에서는 이상금융거래(fraud)에 이용될 수 있는 개인보안자격증명(personalised security credentials)이 포함된 데이터로 정의)의 저장, 감시, 추적 및 접근통제 절차(g호), ③ 핵심 업무의 정의와 비상계획(Contingency plans)의 수립 및 비상계획에 대한 주기적인 타당성・효율성 평가(h호), ④ 상세한 위험평가(Risk assessment) 및 보안위험으로부터 서비스와 중요 정보를 보호하기 위한 보안수단(j호) 등 4개 요건이 보안위험 대응에 관한 요건이다.

동 요건에서는 금융서비스를 제공하려는 신청 기관에 대하여 적정한 보안위험 대응수준을 확보하도록 요구하고 있는데, 특히, (j)호에서는 위험평가에 근거하여 위험에 대응하는 보안수단을 보유하도록 명시하여 기관의 특성에 적합한 보안위험 대응이 가능하도록 하였고, 동시에 제95조의 서비스 제공 시 보안위험관리를 위한 보안수단을 포함하고 이에 대한 유럽은행감독청(European Banking Authority, 이하 EBA)의 관련 가이드라인을 준수하도록 규정하여, 허가 또는 등록 단계부터 서비스 제공 시까지 일관된 보안위험관리체계를 적용하도록 하고 있다.

그리고 계좌정보서비스만 제공하려는 기관에 대해서는 제33조에서 17개의 요건 중 초기자본보유수준, 자금세탁방지, 테러자금지원방지에 관한 요건 등을 제외한 11개만 적용하도록 등록요건을 완화하였지만, 보안위험 대응에 관한 4개 요건은 모두 동일하게 적용하도록 규정하고 있다.

개정 이전의 기존 PSD의 허가 또는 등록 요건과 비교해 보면, 위에서 확인한 보안위험 대응에 관한 4개 요건은 모두 기존 PSD에서는 제시되지 않았던 것으로, 유럽연합 집행위원회(European Commission)도 팩트시트(Fact Sheet)에서 PSD2의 허가 또는 등록 요건은 기존 PSD와 대체로 동일하지만, 보안에 관해서는 대상기관의 수준 향상을 위한 변화가 있었다고 언급하였다[7].

이러한 허가 또는 등록 시 보안 관련 요건의 강화는 보안위험의 증가에 대한 기관의 전반적인 대응 능력 향상을 도모하는 것과 동시에 계좌 접근 대상의 확대에 따라 새롭게 금융시장에 참여하는 기관에 대해서도 서비스 제공을 위해서는 사전에 금융시장에 적합한 보안수준과 업무연속성을 확보하도록 요구한다고 분석할 수 있다.

또한 PSD2는 제5조 제5항에서 허가 또는 등록에 대하여 EBA가 추가적인 가이드라인을 제시하도록 규정하고 있으며, EBA는 2017년 7월에 발표한 해당 가이드라인[5]에서 앞서 분석한 보안위험 대응에 관한 4개의 요건에 해당하는

〈Table 2〉 Guidelines on the Authorisation: Response to Security Risks

PSD2 Article 5(1)	Guidelines(Title)
(f)	Procedure for monitoring, handling and following up on security incidents and security-related customer complaints(a~f)
(g)	Process for filing, monitoring, tracking and restricting access to sensitive payment data(a~j)
(h)	Business continuity arrangements(a~e)
(j)	Security policy document(a~i)

내용을 <Table 2>와 같이 제시하고 있으며, 가이드라인은 지급결제지시서비스 포함 지급결제기관의 허가와 계좌정보서비스만 제공하는 경우의 등록에 대한 가이드를 구분하고 있으나 보안위험에 관한 4개 요건에서 내용에 실제적인 차이는 없다.

첫 번째로, 보안사고와 이용자 불만 등에 관한 처리절차 및 금융당국에 대한 사고보고 체계(f호)에 관해서는 이상금융거래 방지 수단을 보유하고, 실제로 이상금융거래나 기술문제 등이 발생하였을 때 이를 처리하는 조직과 내부보고체계를 구축하며, 보안위험의 완화를 위한 위험 모니터링 수단 및 식별한 위험에 대응할 수 있는 보안수단과 통제절차를 보유하고, 주요 사고에 대한 금융당국 보고체계를 구축하는 등 6가지 가이드를 제시하고 있다.

두 번째로, 민감한 지급결제 정보의 저장, 감시, 추적 및 접근통제 절차(g호)에 대해서는 서비스를 제공하는 과정에서 민감한 지급결제 정보의 흐름과 정보를 이용하는 대상 등을 정확히 파악하고, 모니터링・접근통제・암호화 등 보호 수단을 보유하며, 정보의 유출을 탐지하고 조치할 수 있는 방안을 확보하는 등 10개의 가이드를 제시하고 있다. 다만, 지급결제지시서비스만 제공하는 기관에 대해서는 동 요건 중 민감한 지급결제 정보의 저장 체계와 정보의 내・외부 이용 대상에 대한 요건은 적용하지 않도록 제시(가이드라인 10.1(e), (f))하고 있는데, 이는 PSD2 제66조 제e호에서 지급결제지시서비스 제공자는 민감한 지급결제 정보를 저장하지 못하도록 규정하였기 때문이다.

세 번째로, 핵심 업무의 정의와 비상계획의 수립 및 비상계획에 대한 주기적인 타당성・효율성 평가(h호)에 대해서는 서비스 제공 중에 재난 등 비상 상황에서 업무 연속성을 확보하는 것에 관한 5개의 가이드를 제시하고 있으며, 업무 영향 분석(business impact analysis)을 근거로 복구시간 등 목표 수준을 설정하고 필요한 IT인프라를 확보하며, 핵심 시스템에 대한 조치 계획을 수립하고, 재난 대응 및 복구계획 등의 지속적인 평가・개선 체계를 보유하도록 요구하고 있다.

네 번째로, 상세한 위험평가 및 보안위험으로부터 서비스와 중요 정보를 보호하기 위한 보안수단(j호)에 대해서는, 제공하려는 서비스에 대한 위험평가를 실시하고, 이상금융거래 등 식별된 위험에 대한 보안통제 및 위험 완화 수단을 보유하며, 정보시스템과 네트워크 등 IT인프라를 확보하고 물리적 보안체계를 구축하며, 내・외부로부터의 접속에 대한 통제・보안 체계 등을 보유하도록 요구하고 있다. 즉, 위험평가에 기반하여 금융서비스 제공 시 기관

이 직면할 수 있는 내·외부의 보안위험으로부터 자산과 이용자를 보호할 수 있는 논리적·물리적·관리적 보안체계를 보유하도록 요구한 것이다.

3.2 서비스 제공 시에 관한 제도적 대응

유럽연합은 PSD2 제95조 제1항과 제2항에서 지급결제지시서비스 제공자와 계좌정보서비스 제공자를 포함한 서비스 제공기관에 대하여 제공하는 서비스와 관련한 보안위험을 통제하고 관련 사고에 대응할 수 있는 체계를 구축할 의무를 부과하고 있으며, 연 1회 이상 종합적인 위험평가 결과와 식별된 위험에 대한 대응체계를 금융당국에 보고하도록 하여, 보안위험 대응체계의 지속적인 개선과 효율성 확보 등을 도모하고 있다.

그리고 제95조 제3항에서는 EBA에 대하여 추가적인 가이드라인을 제시하도록 규정하고 있는데, 이에 따라 EBA는 2017년 12월에 해당 가이드라인[6]을 발표하였다. 가이드라인은 <Table 3>과 같이 전체 8개의 내용을 세 가지로 분류하여 ① 보안위험관리프레임워크에 관한 5개 내용, ② 보안위험관리프레임워크의 평가·개선에 대한 2개 내용, 그리고 ③ 이용자 관계 관리를 통한 보안위험의 완화에 관한 1개 내용을 제시하였고[4], 이는 금융시장에서 이용자가 신뢰할 수 있는 서비스를 제공하는데 필요한 보안위험 대응체계와 업무 연속성을 확보하고 조직 차원에서 이를 지속적으로 향상시킬 수 있는 절차를 보유하도록 하기 위한 내용으로 해석할 수 있다.

특히 위험평가 요건을 보안위험관리프레임워크에 별도 항목으로 포함하고 있으며, 이후 다른 항목에서 접근통제 대상의 중요도 판단, 업무 연속성 확보를 위한 핵심 대상 선정, 보안수단 시험을 위한 핵심 시스템 선정 등을 동 위험평가 항목에 근거하도록 명시적으로 제시하고 있는 등 대상 기관이 위험평가에 기반하여 보안위험 대응체계를 구축하도록 하고 있다.

3.2.1 보안위험관리프레임워크의 요건

가이드라인은 보안위험관리프레임워크의 하위요건으로 ① 거버넌스, ② 위험평가, ③ 보호, ④ 탐지, ⑤ 업무 연속성을 제시하고 있으며 항목별 내용은 <Table 4>와 같다.

〈Table 3〉 Guidelines on the Response to Security Risks Related to the Provision of Services

Subjects	Guidelines
Risk management framework	Governance
	Risk assessment
	Protection
	Detection
	Business continuity
Testing situational awareness and continuous learning	Testing of security measures
	Situational awareness and continuous learning
Payment Service User relationship management	

〈Table 4〉 Guidelines on the Risk Management Framework

Guidelines	Subjects	No.
Governance	Operational and security risk management framework	2.1~2.4
	Risk management and control models	2.5~2.6
	Outsourcing	2.7~2.8
Risk assessment	Identification of functions, processes and assets	3.1~3.2
	Classification of functions, processes and assets	3.3
	Risk assessments of functions, processes and assets	3.4~3.5
Protection		4.1~4.5
	Data and systems integrity and confidentiality	4.6~4.7
	Physical security	4.8
	Access control	4.9~4.13
Detection	Continuous monitoring and detection	5.1~5.3
	Monitoring and reporting of operational or security incidents	5.4~5.6
Business continuity		6.1~6.3
	Scenario-based business continuity planning	6.4~6.5
	Testing of business continuity plans	6.6~6.9
	Crisis communication	6.10

첫 번째로 거버넌스에 대해서는, 지침 제5조에서 허가 또는 등록 단계의 요건으로 규정한 위험평가 등의 보안 정책 문서를 보안위험관리 프레임워크의 요건으로 포함하여 시장진입 시점부터 서비스 제공 시까지 위험관리체계의 통일성을 확보하고, 보안수단 적용 시 역할과 책임을 정의・할당하며, 위험관리에 필요한 통제 절차와 시스템을 구축할 것 등을 제시하였다. 또한 위험관리체계의 효율성 유지를 위하여 연 1회 이상 기관의 경영진이 위험관리체계를 검토・승인하는 절차를 기관의 공식 절차로 보유하도록 규정하여 경영진의 보안위험 관리 참여를 제도화하고, 프레임워크의 충실한 문서화와 지속적인 보완, 그리고 자산이나 업무절차의 변화 또는 사고 발생 시 이를 반영한 프레임워크의 개선 등을 요건으로 제시하였다.

그리고 업무 수행 조직 차원의 통제를 1차 방어선, 전사적 조직 차원의 통제를 2차 방어선, 그리고 독립적인 내부감사를 3차 방어선으로 하는 내부통제 모델[38]인 '3선방어체계(Three lines of defence)'를 위험관리와 통제 모델의 기준으로 제시하고 권한・독립성・자원・경영진에 대한 직접 보고체계 등을 확보하도록 하였으며 실제 보안수단에 대해서는 관련 분야 전문가와 독립적인 감사 조직이 주기적으로 감사하도록 하였다. 여기에 아웃소싱이 이루어진 시스템이나 기능에 대해서도 조직이 설정한 보안목표를 달성하는데 필요한 보안수단을 적용하고 서비스 수준 협약(Service Level Agreement, SLA)에 이를 반영하여 지속적으로 유지될 수 있도록 요구하고 있다.

두 번째로 위험평가에 대해서는, 먼저 조직이 보유한 기능・절차・자산 등을 정확하게 파악하고 중요도에 따라 분류하며, 이에 대한 위협과 취약점을 식별하여 효과적으로 대응할 수 있는 보안수단을 채용토록 하고 있다. 그리고 새로운

취약점을 확인하거나 제공하는 서비스의 보안 수준에 영향을 미칠 수 있는 IT인프라의 변경 등이 이루어지는 경우에는 이를 분석하여 기존에 채용하였던 보안수단을 변경하도록 요구하고 있다.

세 번째로 보호에 대해서는, 하나의 보안위험에 대하여 다수의 보호수단을 적용하는 '심층방어(defence-in-depth)'를 원칙으로 대상 기관이 보유 자산과 민감한 지급결제 정보 등의 기밀성・무결성・가용성을 보호할 수 있는 보안수단을 구축하고, 보안수단 변경관리를 공식 업무절차에 포함하여 보안수단의 효용을 지속적으로 유지할 수 있도록 하고 있다.

그리고 '직무 분리(segregation of duties)'와 '최소 권한(least privilege)'의 원칙을 적용한 내부통제절차를 수립하고 '알 필요성(need to know)' 원칙에 근거하여 IT시스템에 대한 접근통제를 적용하도록 하고 있는데, 여기서 시스템의 중요도를 위험평가 항목에 근거하여 판단하도록 명시하고 있다. 또한, 민감한 지급결제 정보에 이용자의 개인정보가 포함되어있다면, 유럽연합의 개인정보보호 규정(Regulation(EU) 2016/679, General Data Protection Regulation, GDPR)에서 제시하는 보안 요건을 준수하도록 관련 법규와의 관계를 규정하고 있다.

네 번째로 탐지에 대해서는, 논리적・물리적 침입과 정보・자산의 침해 등을 지속적으로 모니터링・탐지할 수 있는 수단을 보유하고 그 대상은 업무와 IT기능 및 기관 내・외부의 잠재적인 위협 등을 포괄하도록 하고 있으며, 부정한 접근을 탐지하기 위한 감시 대상을 서비스 제공자뿐만 아니라 관련자까지 확대하고 있다. 또한, 보안사고에 대해서는 그 범주・정도에 관한 판단 기준과 지표를 수립하고, 사고의 탐지・처리 및 고위 경영진 보고 관련 절차와 조직을 보유하도록 하고 있다.

마지막 다섯 번째로 업무 연속성에 대해서는, 복구 대상과 중요도 식별, 재난 시나리오와 대응계획의 수립, 대응계획 등의 지속적인 개선으로 순환되는 일련의 체계를 구축하여 견실한 업무 연속성 관리가 가능하도록 하고 있는데, 여기서도 앞서 제시한 위험평가 항목에 근거하여 서비스 제공 시 핵심 업무를 분류하고 이에 대한 업무 연속성 계획(Business Continuity Plan, BCP)을 수립하도록 명시하여 일관되게 위험평가에 기반한 관리체계를 구축하도록 하고 있으며, 서비스의 연속성을 유지하는데 필요한 보안・통신수단을 도입하고, 다양한 재난 시나리오에 대하여 대응・복구 절차를 마련하며, 연1회 이상 업무 연속성 계획과 재난 시나리오를 평가・개선하도록 하고 있다.

3.2.2 보안위험관리프레임워크의 평가·개선 및 이용자 관계 관리를 통한 보안위험의 완화에 관한 요건

먼저, 보안위험관리프레임워크의 평가・개선의 하위요건으로는 ① 보안수단에 대한 평가,

〈Table 5〉 Guidelines on the Testing and Improvement of Risk Management Framework

Guidelines	Subjects	No.
Testing of security measures	-	7.1~7.6
Situational awareness and continuous learning	Threat landscape and situational awareness	8.1~8.3
	Training and security awareness programmes	8.4~8.6

② 상황 인식과 지속적인 학습 등을 제시하고 있으며, 각 항목별 내용은 <Table 5>와 같다.

첫 번째로 보안수단의 평가에 관해서는 기관의 보안위험관리체계를 구성하고 있는 보안수단이 새로운 보안위험에도 효과적으로 대응할 수 있도록 지속적인 평가를 수행할 것과 평가의 대상・요건・주기 등을 규정하고 있다.

평가대상은 서비스 제공을 위한 장비, 이용자의 인증에 사용되는 기기, 이용자가 인증 코드를 생성하거나 수신하는데 이용하는 기기와 소프트웨어 등으로 정의하고 있으며, 평가요건에 대해서는 보안수단 평가절차를 기관의 공식 절차로 수립하고 보안수단의 구축에 관여하지 않은 독립적인 인력이 평가하되 취약점 스캔(vulnerability scans)과 침입 시험(penetration test)을 포함하도록 하고 있다.

평가주기는 핵심 시스템에 대해서는 연1회, 그 외의 시스템에 대해선 3년에 1회 이상 주기적으로 평가하되 중요한 사고가 발생하거나 인프라와 업무절차에 중대한 변경 시에는 수시로 실시하도록 하고 있으며, 평가주기를 구분하기 위한 핵심 시스템의 분류 근거를 앞서 보안위험관리프레임워크에 관한 요건으로 제시되었던 위험평가에 근거하도록 명시하여 의사결정을 위한 중요도의 판단 기준이 위험평가에 근거하여 통일되도록 하고 있다.

두 번째로 상황 인식과 지속적인 학습에 대해서는 보유하고 있는 보안수단을 지속적으로 개선하기 위하여 서비스 제공 환경을 모니터링・분석하는 조직 요건 및 임직원 등에 대한 교육 활동과 보안인식(security awareness) 제고 활동에 대한 요건을 제시하고 있다.

보다 구체적으로는, 기술 변화와 신규 보안위험을 지속적으로 모니터링하고 발생한 보안사고를 사고를 분석하여 기관의 보안수단에 반영하는 조직과 체계를 구축하도록 하였다. 그리고 소속 직원의 보안인식 향상을 위한 프로그램을 수립하여 시행하고, 임직원이 기관의 보안 정책・절차를 명확히 인지하고 부여된 역할을 수행하는데 필요한 교육을 실시하도록 규정하고 있는데, 특히 앞서 위험평가에서 식별한 핵심 역할에 대해서는 보다 특화된 교육을 실시하도록 하여 일관되게 위험평가에 기반한 위험관리체계를 적용하도록 규정하고 있다.

이용자와의 관계 관리를 통한 보안위험의 완화에 관한 요건으로는 <Table 6>과 같이 이용자의 보안위험에 대한 인식 제고와 위험 완화를 위한 조치 관련 7개의 가이드를 제시하고 있는데, 이에 대해 EBA는 이용자 관계 관리는 위험관리체계에서 구축한 보안수단과 보안위험에 대한 이용자의 이해도를 높여 서비스의 보안 수준을 전반적으로 향상시키고 위험을 완화하기 위한 활동으로, 서비스 제공 기관은 이용자에 대해서도 보안수단을 구축할 책임이 있다고 설명하고 있다[4].

보다 구체적으로는 이용자를 대상으로 보안

〈Table 6〉 Guidelines on the User Relationship Management to Mitigate Security Risks

Guidelines	Subjects	No.
Payment service user relationship management	Payment service user awareness on security risks and risk-mitigating actions	9.1~9.7

인식 수준 향상을 위한 상세한 가이드를 제공하되 보안 환경의 변화에 맞춰 그 내용을 지속적으로 개선토록 하였고, 이용자가 보안절차의 변경이나 보안 취약점 등에 관한 정보와 지원을 적시에 편리하게 이용할 수 있도록 하며, 필요한 경우에는 이용자가 보안상의 목적을 위해 서비스의 기능을 중지하거나 지정한 기기에서 금액 한도를 조정할 수 있도록 지원하게 하고 있다.

3.3 지급결제지시서비스와 계좌정보 서비스의 정보이용 등에 관한 추가적인 제한요건

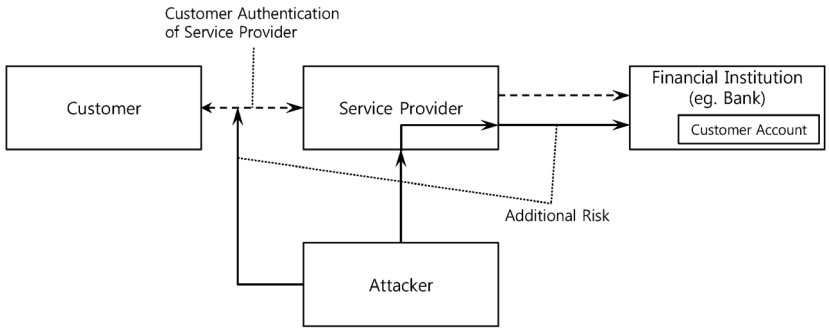
PSD2 제66조, 제67조는 제3자가 지급결제지시서비스나 계좌정보서비스를 제공하기 위하여, 계좌 관리 금융기관이 보유한 이용자 계좌에 접근할 수 있는 권한을 보장함과 동시에 계좌와 정보의 이용 범위와 보관 여부 등을 제한하고 있으며, 이는 지침의 개정에 따라 계좌 관리 금융기관의 통제 범위 외에서 다수의 서비스 제공자가 계좌에 접근할 수 있게 됨에 따라 중요 정보의 부정한 사용 등 서비스와 관련하여 새롭게 발생할 수 있는 보안위험에 대응하기 위함이라 할 수 있다.

두 서비스에 대한 제한요건의 구체적인 내용에 일부 차이는 있으나, 공통적으로 제3자인 서비스 제공자가 서비스 제공을 위해 계좌에 접근하기 위해서는 이용자의 명시적 동의를 받도록 요구하고, 서비스 제공에 불필요한 정보에 대한 접근 또는 민감한 지급결제정보 등에 대한 요청・저장 등을 제한하고 있다. 또한, 이용자인증의 기술적인 요건과 예외사항, 개인보안자격증명의 보호 방안, 서비스 관련자 간의 안전한 통신을 위한 공개 공통 표준 등을 제시하는 PSD2의 인증과 통신에 대한 규제기술표준(Regulatory Technical Standards, RTS)[36]에 따라 서비스 이용자의 개인보안자격증명을 보호하고 통신의 안전성을 확보할 의무를 부여하고 있다.

4. PSD2와 국내법규의 보안 위험에 대한 제도적 대응 비교・분석

유럽연합의 PSD2는 국내 금융시장에도 변화를 가져오고 있는데, 이는 국내에서도 금융기관이 아닌 제3자에게 계좌 접근과 관련 정보의 이용을 허용하는 제도의 변화와 법규의 개정을 금융당국이 적극적으로 추진하는 것으로 나타나고 있으며 이에 대해서는 앞서 1장에서도 확인하였다. 국내 금융시장에서도 금융회사가 아닌 제3자에 대한 계좌 접근과 정보 제공이 의무화 된다면, 먼저 새롭게 금융시장에 진입하려는 기관에 대해서는 이용자의 자금을 안전하게 보호하고 이용자의 신뢰를 확보할 수 있도록 금융시장에 적합한 수준의 보안위험 대응체계를 보유하도록 하여야 한다.

또한 Wolters et al.[39]이 제3자의 이용자 인증에 기반한 서비스 제공은 계좌 관리 금융기관이 계좌 접근의 적정성 등을 서비스 제공자에게 전적으로 의존할 수밖에 없다는 것이며, 이는 PSD2에서 인증의 강화 등에도 불구하고 <Figure 1>과 같이 공격의 대상과 기회의 증가를 의미하고 보안 위험을 증가시킨다고 분석한 것처럼, 기존 시장 참여자의 보안위험 대응 수준 향상도 요구된다고 할 수 있다.



〈Figure 1〉 Additional Risks (Reconstruction of References[39]'s 〈Figure 4〉)

앞서 확인한 것처럼 PSD2에서는 이러한 보안위험에 대한 제도적 대응으로 제3자를 포함한 신규 참여자가 시장에 진입하기 위해서는 적정 수준의 보안위험 관리체계를 보유하도록 규정하였으며, 서비스 제공 단계에서도 관리체계를 유지・개선하도록 요건을 제시하고 있다. 국내의 경우 지급결제서비스 등 전자금융의 보안위험에 대한 대응은 '전자금융거래법[13]'으로 규제하고 있으며 규제의 상세한 내용은 동 법의 하위 규정인 '전자금융감독규정[18]'에서 주로 제시하고 있으므로, 본 연구에서는 향후 국내 금융시장의 변화에 대비한 제도 개선의 시사점 도출을 위해 동 법규와 규정에서 제시하고 있는 허가 또는 등록과 서비스 제공 단계의 보안위험에 대한 제도적 대응을 중심으로 비교・분석하였다.

다만, 금융위원회는 PSD2와 같은 오픈 API를 이용한 제3자 제공 서비스(지급결제지시서비스, 계좌정보서비스) 도입 등의 추진을 발표하면서, 지급결제지시서비스에 해당하는 지급지시서비스업(마이 페이먼트 산업)은 전자금융거래법에 따라 추진하기로 하였지만[11], 계좌정보서비스에 해당하는 본인 신용정보 관리업(마이 데이터 산업)은 '신용정보의 이용 및 보호에 관한 법률[12](이하 '신용정보법')'에 따라 추진하기로 하였다[16]. 그러나 현재 신용정보법에 따른 신용정보회사 등도 전자금융거래법 제3조와 제5조에 따라 금융회사로서 전자금융업무를 수행하는 경우 전자금융거래법의 적용을 받으며, PSD2에서 두 서비스 모두 이용자에게 전자적 수단을 통해 온라인으로 제공하는 것을 전제하므로, 본 연구에서는 전자금융거래법을 중심으로 분석하되 허가 또는 등록 등 필요한 경우 신용정보법을 추가로 분석하였다.

4.1 허가 또는 등록 단계의 제도적 대응 비교

전자금융거래법은 제31조에서 전자금융업의 허가 또는 등록 요건을 제시하면서 동 조항 제2호에서 이용자 보호와 업무 수행을 위해 필요한 전산설비 등 물적 요건의 충족을 요구하고 있으며, 이를 전자금융감독규정 제50조 제1항과 금융당국이 제공하는 '금융회사 인허가 매뉴얼[19]'의 물적 시설 설비 현황 제출 자료 항목에서 ① 서버, 통신망 구축 등에 관한 '전자금융업의 원활한 영위를 위한 전산기기 보유', ② 백업・소산 및 비상대책 등에 대한 '전산 장애에 대비한 백업장치 구비', ③ 업무용 프로그램 구비와 변경통제에 관련한 '전자금융업의 원활

〈Table 7〉 Requirements for Information Processing and Communications Facilities Necessary for Issuing Permission to Conduct Credit Inquiry Business and to Operate Credit Information Collection Agency

Configuration	Detailed Requirements
Systems configuration	1. Communications section encryption systems, Web server, Storage device, Other peripheral devices 2. Backup and recovery system 3. Security management systems including the system security and facility security
Systems performance	1. The system shall provide performance that can appropriately process information held 2. The system shall provide performance that can appropriately collect and provide information through online services or public telecommunications networks 3. Backup and recovery work shall be completed within the shortest amount of time
Security system	1. Firewall 2. Security system that can detect, warn and interrupt intrusions 3. Internal network independent from the credit inquiry network 4. Information user verification system 5. Data encryption system 6. Measures taken for the prevention of intrusions 7. Measures taken for backup and vaulting
Operating capability	1. The credit information collection agency shall have the capability to operate the system 2. The credit information collection agency shall have the capability to develop programs

한 영위를 위한 프로그램 보유', ④ 접근통제, 보안장비 등 각종 논리적・관리적 보안수단의 확보를 규정한 '전산자료 보호 등을 위한 시스템 관리방안 마련 및 정보보호시스템 등 감시 운영체제 구축', ⑤ 재해대비와 물리적 보안수단에 관한 '전산실 등의 안전성 확보' 등 5개로 분류하여 제시하고 있다.

신용정보법도 전자금융거래법과 유사하게 법규에서 신용정보업 중 신용조회업의 허가를 위해서는 업무 수행을 위해 필요한 전산설비 등 물적 요건의 충족을 요구하고, 하위 규정에서 그 구체적인 내용을 제시하고 있는데, 구체적으로는 신용정보법 제6조 제1항 제1호와 동법 시행령 제6조 제1항 제1호에서 금융위원회가 고시하는 정보처리・정보통신설비 등 전산설비 관련 요건을 충족하도록 규정하고, 하위 규정인 '신용정보업감독규정[17]'의 별표 2에서 <Table 7>과 같이 동 요건을 4개 항목 15개의 세부 사항으로 제시하고 있다.

이처럼 전자금융거래법과 신용정보법의 허가 또는 등록 요건 중 보안위험 대응을 포함한 물적 요건에 관한 항목은 유사한 구성을 보여주고 있는데, 먼저 전산장비와 소프트웨어 등 업무수행을 위해 필요한 전산자원을 확보하고, 이렇게 확보한 전산자원을 보호하기 위한 물리적・논리적・관리적 보안수단을 도입하며, 금융정보나 신용정보와 같은 중요정보의 보호체계를 구축하고, 유사시에 대비한 백업 및 복구체계를 구축하도록 규정하고 있다.

이에 관한 앞에서 분석한 PSD2의 허가 또는 등록 단계의 보안위험 대응에 관한 가이드라인과 이에 해당하는 국내법규인 전자금융감독규정과 신용정보업감독규정의 요건을 비교한 내용을 <Table 8>에 제시하였다.

〈Table 8〉 Comparison of response to security risks in PSD2 and domestic laws: Authorisation

PSD2 : Guideline for authorisation
Regulation on Supervision of Electronic Financial Transactions(Article50(1))
Regulation on Supervision of Credit Information Business(Table 2)
9. Procedure for monitoring, handling and following up on security incidents and security related customer complaints
N/A
10. Process for filing, monitoring, tracking and restricting access to sensitive payment data
5. Developing an information processing system management plan appropriate to protect computer data, and establishing a monitoring and operating system, such as an information protection system
Security system
11.Business continuity arrangements
3. Having the backup devices to prevent the loss of computer data from any computer system failure
Systems configuration, Systems performance, Security system
13.Security policy document
2. Having computer equipment necessary to efficiently perform the electronic financial affairs 4. Having various programs necessary to efficiently perform the electronic financial affairs 5. Developing an information processing system management plan appropriate to protect computer data, and establishing a monitoring and operating system, such as an information protection system 6. Ensuring the safety of the structure, interior materials, facilities, etc. of the IT room and developing a proper security plan
Systems configuration, Systems performance, Security system, Operating capability

먼저 PSD2의 보안사고와 고객 불만 등에 관한 처리절차 및 금융당국에 대한 사고보고 체계에 대해서는 국내법규의 허가 또는 등록 단계의 요건에서는 직접 대응하는 내용을 확인하기 어렵지만, 서비스 제공시의 요건에서는 전자금융감독규정 제73조에서 금융당국에 대한 사고보고에 관한 요건을 제시하고 있는 등 관련 내용을 확인할 수 있다.

다음으로, 민감한 지급결제 정보의 저장, 감시, 추적 및 접근통제에 관한 절차에 대해서는 국내법규에서도 전산자료의 보호를 위한 보안수단과 통제절차를 요건으로 제시하고 있어 대응하는 내용을 확인할 수 있다. 그리고 핵심 업무의 정의와 비상계획의 수립 및 주기적인 비상계획의 타당성과 효율성 평가에 대해서는 국내법규에서 재해에 대비한 비상대책의 수립과 백업과 복구에 필요한 장비・절차 등의 요건이 대응하였다.

마지막으로 상세한 위험평가 및 보안위험으로부터 서비스와 중요 정보를 보호하기 위한 보안수단에 대해서는 식별된 보안위험에 대한 논리적・물리적・관리적 보안체계에 대해서는 국내법규에서도 대응 요건을 확인할 수 있으나, PSD2의 위험평가와 관련한 요건은 대응하는 내용을 확인하기 어려웠다.

이처럼 PSD2에서 허가 또는 등록 단계에서 보유하도록 요구하는 구체적인 보안수단과 통제절차에 대해서는 국내법규에서도 대부분 대응하는 요건을 제시하고 있으나, PSD2에서 위험을 파악하고 대응 수준과 방법을 판단하기 위한 위험평가에 대한 요건에 관해서는 국내법

규와 분명한 차이가 발생하고 있다.

4.2 서비스 제공 시에 관한 제도적 대응 비교

전자금융거래법은 제21조에서 전자금융거래의 안전성과 신뢰성을 확보하기 위한 금융위원회의 기준을 준수하도록 규정하고 하위 규정인 전자금융감독규정 제7조부터 제37조까지에서 이에 대한 상세한 요건을 제시하고 있으며, 아웃소싱(제60조)과 금융당국에 대한 사고보고(제73조) 등 일부 사항은 그 외의 조항에서 대응하는 내용을 규정하고 있다.

4.2.1 보안위험관리프레임워크에 해당하는 요건

PSD2는 서비스 제공 기관이 보유해야 하는 보안위험관리프레임워크에 대하여 거버넌스,

〈Table 9〉 Comparison of Response to Security Risk in PSD2 and Domestic Laws: Risk Management Framework

PSD2 Guideline	Regulation on Supervision of Electronic Financial Transactions
Governance	8. Personnel, Organization and Budget 8-2. Operation of Information Security Committee 19. Procedures, etc. for Submitting Plans for IT Sector 20. Building Information Processing System and Promoting Projects Related to Electronic Financial Transactions 21. Contracts for Building of Information Processing System and Electronic Financial Transactions 22. Supervision of Information Processing System 37-2. Cycle, Content, etc. of Analysis and Evaluation of Weak Points of Electronic Network for Financial Transactions 37-5. Duties of Chief Information Security Officer 60. Standards for Outsourcing, etc.
Risk assessment	N/A
Protection	9. Matters Relating to Buildings 10. Matters Relating to Facilities, such as Power Supply System and Air Conditioning System
Detection	11. Matters Relating to IT Room, etc. 12. Measures to Protect Terminals 13. Measures to Protect Computer Data 14. Measures to Protect Information Processing System 15. Anti-Hacking Measures, etc 16. Measures to Prevent Malicious Code Infections 17. Measures to Manage Open Source Web Servers, Including Home Pages 18. Measures to Manage IP Addresses 26. Division of Duties 27. Control of Electronic Ledger 28. Control, etc. of Transactions 29. Control of Program 30. Control of Batch Processing 31. Control of Encryption Programs and Key Management 32. Management of Internal User Passwords 33. User Password Management 34. Compliances in Electronic Financial Transactions 73. Reports on Accidents in IT Sector and Electronic Financial Transactions
Business continuity	23. Establishment and Implementation of Emergency Measures, etc. 24. Conducting Emergency Response Training

위험평가, 보호, 탐지, 업무 연속성 등 다섯 가지 하위요건을 제시하고 있는데, 이 중 위험평가 항목은 전자금융거래법과 전자금융감독규정에서 직접적으로 대응하는 내용을 확인하기 어렵지만, 나머지 4개 요건은 <Table 9>와 같이 대응하는 내용을 확인할 수 있다.

먼저 PSD2의 거버넌스 항목에서는 보안위험관리프레임워크의 요건, 위험관리 및 통제모델의 기준, 아웃소싱 부문에 대한 요건 등을 제시하고 있으며, 전자금융감독규정에서는 이에 대응하는 내용으로 정보보호최고책임자의 직무와 정보보호위원회의 구성 등의 항목을 통해 조직 구성과 수행 업무에 대한 구체적인 요건을 직접 규정하고 있으며 별도 항목으로 정보보호 인력・예산 보유 기준을 구체적으로 제시하고 있다. 그리고 정보기술부문계획서의 검토 의무를 부과하여 보안체계에 대한 주기적인 평가・개선이 이루어지도록 규정하고 있다. 여기에 PSD2는 먼저 통제모델의 기준으로 '3선방어체계'를 제시하고 추가 요건을 규정하였다면, 전자금융감독규정은 금융당국이 효과적인 보안 통제체계에 필요하다고 판단한 조직의 구성・업무・역할 등을 분야별로 비교적 상세하게 제시하고 규제 대상 기관이 이를 준수하여 보안체계를 확보하도록 하는 특징이 있으며, 아웃소싱에 대해서도 외부주문과 계약 항목을 통해 요건을 상세하게 제시하고 있다.

다음으로 PSD2는 보호와 탐지를 분리하여 보호에 대해서는 보안위험에 대한 '심층방어' 체계 구성을 원칙으로 시스템과 데이터 보호, 물리적 보안, 접근통제 등의 분야별 요건을 제시하되 보호 대상 업무와 정보자산의 중요도 등은 위험평가 항목에 근거하도록 규정하였으며, 탐지에 대해서는 지속적인 모니터링, 보안사고의 보고 등에 대한 요건을 제시하고 있다.

이와 달리 전자금융감독규정은 각 분야별로 하나의 조항에서 보호와 탐지 요건을 함께 제시하고 있다. 분야별로 규제 대상 기관이 보유해야 할 암호화, 악성코드 대응 등 보안수단과 프로그램 변경통제, 암호키 통제 등 통제절차 및 직무분리 등의 요건을 상세하게 규정하고 있으며, 보안수단과 통제절차에 대한 감시・추적이 필요한 경우 접속기록 보존 등을 분야별 규정에서 추가로 제시하고 있으며, 별도로 중요 사고에 대해서는 금융당국에 대한 보고절차를 규정하고 있다.

마지막으로 PSD2는 업무 연속성 항목에서 위험평가 항목에 근거한 업무 연속성 계획의 수립에 대한 요건을 제시하고 또한 지속적인의 계획의 평가・개선을 위한 관련 요건 등을 제시하고 있다. 이에 대해 전자금융감독규정은 비상대책 수립 시 업무별 중요도의 분석・반영, 대책의 주기적인 점검・개선 등 업무연속성 확보를 위해 기관이 수행할 업무 및 복구목표시간, 인력・장비 수준 등 적정 기준을 구체적으로 제시하여 이를 준수하는 경우 분석・계획・평가・개선으로 이어지는 업무연속성관리체계가 이루어지도록 규정하고 있으나, PSD2와 같이 위험평가에 근거하도록 명시하지 않는다는 차이가 있다.

4.2.2 보안위험관리프레임워크의 평가·개선 및 이용자 관계 관리를 통한 보안위험의 완화에 해당하는 요건

PSD2는 기관이 구축한 보안위험관리프레임워크가 내・외부의 환경변화에도 유효성을 유지할 수 있도록 관련 보안수단을 지속적으로 평가・개선할 수 있는 체계를 구축하고, 서비스 환경의 변화 등을 모니터링・분석하여 프레임워크에 반영하는 조직과 절차를 보유하며, 임직

〈Table 10〉 Comparison of Response to Security Risk in PSD2 and Domestic Laws: Testing and Improvement of Risk Management Framework and User Relationship Management to Mitigate Security Risks

PSD2 Guideline	Regulation on Supervision of Electronic Financial Transactions
Testing situational awareness and continuous learning	8. Personnel, Organization and Budget 8-2. Operation of Information Security Committee 19-2. Formulation and Execution of Educational Plan for Information Security 37-2. Cycle, Content, etc. of Analysis and Evaluation of Weak Points of Electronic Network for Financial Transactions
Payment Service User relationship management	35. Caution Notice for Users

원의 보안인식 제고와 보안 절차・역할에 대한 교육 프로그램을 수립하도록 규정하고 있다.

전자금융감독규정도 취약점 분석・평가 및 관련한 경영진 참여의 요건, 규정 시간 이상의 임직원 대상 보안교육 실시 등 PSD2에 대응하는 내용을 <Table 10>과 같이 규정하고 있지만, PSD2는 평가와 교육에 있어 핵심 시스템과 중요 직무의 판단 기준을 위험평가 항목에 근거토록 규정하고 있으나, 전자금융감독규정은 직접 위험평가에 근거토록 제시하지는 않으며 기관이 수행해야 하는 업무와 준수해야 하는 기준을 상세하게 제시하는 방식을 취하고 있다.

먼저, 전자금융감독규정은 일정 규모 이상의 기관은 주기적인 취약점 분석・평가를 실시하고 취약점 개선 등 조치사항의 이행에는 경영진이 참여토록 하고 있다. 다만, 이는 지속적으로 보안 취약점의 존재 여부를 점검하고 개선하도록 하는 목적이 강하며, PSD2에서 제시하는 보안위험관리프레임워크를 평가・개선하는 체계를 보유하도록 하는 것과는 차이가 있다.

다음으로, 교육에 관해서는 임직원의 정보보호역량 강화를 위한 정보보호 교육의 실시를 규정하고, 인력 및 조직 운용요건에 관한 별도의 항목으로 교육・연수 프로그램의 수립을 포함하는 등 대응하는 내용을 확인할 수 있으나, 다만, PSD2는 평가와 교육에 있어 핵심 시스템과 중요 직무의 판단을 위험평가 항목에 근거토록 하지만 전자금융감독규정은 직접 위험평가에 근거토록 제시하지는 않으며 대상 기관의 의무와 준수 기준을 상세하게 제시하는 방식을 취하고 있다.

마지막으로 PSD2는 이용자가 대상이거나 원인인 보안위험의 완화를 위하여 이용자에게 서비스 관련 보안위험 가이드와 공지 등을 제공하는 지원 절차를 보유하도록 규정하고 있는데, 전자금융감독규정도 역시 안전한 서비스 제공을 위하여 이용자에게 비밀번호 유출, 해킹・피싱 등 보안위험과 기관의 이용자 보호제도 등을 공지하도록 규정하고 있다.

5. 보안위험에 대한 국내 전자금융 관련 법규의 제도적 대응에 대한 제언

5.1 위험평가에 기반한 보안위험관리를 통한 제도적 대응

PSD2는 제도적으로 지급결제지시서비스와 계좌정보서비스 등 새로운 서비스를 금융시장에 도입하고 금융기관이 독점적으로 통제하던 계좌와 관련 정보를 제3자에게도 비차별적으

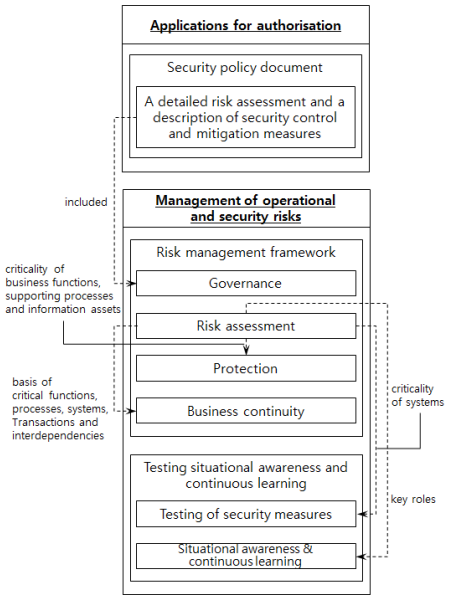
로 제공함으로써 시장의 혁신을 도모하고 있다. 그러나 이는 계좌와 정보의 보호를 보다 어렵게 하고, 새롭게 계좌 접근을 보장받은 IT기업 등 제3자는 기존 금융기관과 다른 특성과 보안 수준을 가지며 신뢰와 평판 등을 중시하여 보안투자에 적극적인 금융기관과 달리 자율적인 투자에 소극적일 수 있다.

실제 과학기술정보통신부가 실시한 2017년 기업부문 정보보호실태조사에서는 금융 및 보험업종과 비교한 정보서비스업의 보안역량·인식 수준은 정보보호정책 수립 비율(82.8% : 41.6%), 정보보호와 개인정보보호 조직 공동운영 비율(33.1% : 14.5%), IT예산 중 정보보호예산 편성 비율(92.2% : 61.3%), 경영진의 정보보호 중요성 인식 비율(75.9% : 54.6%, 5단계 평가 중 가장 높은 '매우 중요하다' 선택 비율 기준) 등에서 차이를 보여주고 있다[28].

서두에 제시한 것과 같이 국내에서 IT에 기반한 서비스와 새로운 유형의 신종전자지급서비스의 규모는 지속적으로 확대되고 있으며, PSD2와 같은 제도가 본격적으로 도입된다면, 기존 금융기관과는 규모·특성·보안인식·투자수준 등이 상이한 다양한 조직의 금융시장 참여를 보다 촉진할 것이다. 금융시장은 본질적으로 금융기관에 대한 이용자의 신뢰가 시장을 유지하고 발전시키는 기반이 되며, 따라서 이러한 신뢰와 안정을 해칠 수 있는 보안위험에 대한 대응·관리와 이용자 보호는 시장의 혁신이라는 제도 도입의 목적 달성을 위해서도 중요한 요소이다.

앞서 분석한 것과 같이 유럽연합은 이런 관점에서 금융시장 참여 기관이 자체적으로 보안위험을 관리할 수 있도록 PSD2에서 시장진입을 위한 허가 또는 등록 단계의 규제를 통해 위험평가에 기반한 보안수단과 통제절차 등을 보유하도록 하고 있으며, 서비스 제공 단계에서도 위험평가에 근거한 보안위험관리체계를 지속적으로 유지·개선하도록 요구하고 있다.

유럽연합의 이러한 규제 방향은 서비스 제공 단계의 요건에서 위험평가를 위험관리프레임워크의 독립항목으로 규정하고 있는 점에서도 명확하게 확인할 수 있었으며, 보안위험 대응에 관한 다른 항목에서도 시스템과 업무 등의 중요도 분석, 핵심 역할을 수행하는 임직원의 식별, 업무 연속성 확보를 위한 기능과 절차의 확인 등을 위험평가에 근거하도록 명시하여 규제 대상 기관이 보안위험관리를 일관성 있게 위험평가에 근거토록 하고 있는 것에서도 또한 확인할 수 있었다. 이와 같이 PSD2에서 보안위험에 대한 제도적 대응을 위험평가에 근거하도록 규정한 내용을 분석하여 <Figure 2>로 제시하였다.



〈Figure 2〉 Institutional Response to Security risks in Accordance with Risk Assessment Specified in PSD2

또한 유럽연합은 2016년에 유럽연합의 전반적인 정보보호 수준향상을 위하여 범 유럽 차원의 사이버보안 관련 규제 지침인 네트워크와 정보시스템의 보안에 대한 지침(The Directive on security of network and information systems, NIS Directive)을 제정하고 2018년까지 소속 국가에 대해서 동 지침에 대응하는 자국 법규를 수립하도록 규정하였다[8]. 그리고 이에 대해 유럽연합 사이버보안청(European Union Agency for Cybersecurity)이 각국 금융당국과 규제 대상 기관이 PSD2와 동 보안규제기준과의 일관성을 유지할 수 있도록 제공한 맵핑 가이드[9]에서 <Table 11>과 같이 두 지침이 공통적으로 위험평가와 위험관리 관련 항목을 포함하는 것을 확인할 수 있으며, 이는 유럽연합이 보안위험에 대한 제도적 대응에 있어서 각 기관이 위험평가에 기반하여 적정 위험관리체계를 확보하도록 일관되게 대응하고 있음을 보여준다.

위험평가에 기반한 보안위험관리로 보안위험에 제도적으로 대응하는 것은 미국에서도 확인할 수 있는데, 미국표준기술연구소(National Institute of Standards and Technology, NIST)는 연방정부의 보안위험 관리를 위한 지침[32]에서 공공은 물론 민간 조직도 업무 수행을 정보시스템에 의존하고 있으며, 이에 대한 보안위험은 인지 여부와 관계없이 조직의 기능·자산 등에 큰 위협이라고 정의하였다. 그러므로 정보보호를 조직 차원의 위험관리와 무관한 기술적인 문제로 한정하는 고위 경영진의 경향은 부적절한 보안위험 대응으로 이어지며, 따라서 고위 경영진이 보안위험 관리를 조직의 핵심 기능으로 인식하고 책임지는 것과, 충분한 자원을 투입하여 조직에 적합한 보안위험관리체

〈Table 11〉 Mapping of the PSD2 Security Measures to the NIS Directive (Reconstruction of Table on pp. 18-19 of References[9])

NIS Directive		PSD2 Guideline
Domains	Sub-Domains	
Governance & Ecosystem	- Information System Security Governance & Risk Management	- Governance - Risk assessment
	- Ecosystem Management	N/A
Protection	- IT Security Architecture	- Protection
	- IT Security Administration	
	- Identity & access management	
	- IT Security Maintenance	N/A
	- Physical & environmental security	- Protection
Defence	- Detection	- Detection - Situational awareness & continuous learning
	- Computer Security Incident Management	- Guidelines on major incident reporting
Resilience	- Continuity of operations	- Business continuity - Testing of security measures
	- Crisis management	N/A

계를 구축하는 것이 중요함을 강조하였다.

그리고 동 기관의 위험평가 수행 가이드[31]에서는 보안위험관리체계의 핵심 요소가 바로 위험평가이며, 그 이유를 조직의 기능・자산 등에 대한 위험을 식별・평가하고 우선순위를 부여함으로써 의사결정권자에게 위험수준, 사고발생 가능성, 사고 영향 등의 정보를 제공하고 위험에 대한 의사결정을 지원하기 때문이라고 제시하였다.

또한 Lee[26]은 금융기관과 핀테크기업의 위험관리체계에 대한 미국 금융당국의 관심이 높아지고 있으며, 금융산업규제당국(Financial Industry Regulatory Authority, FINRA)이 2014년의 금융기관 일제 검사에 대하여 작성한 금융기관이 직면한 위험과 대응에 관한 사이버보안 실태 보고서(Report on Cybersecurity Practices, 2015)의 내용을 분석하여 금융기관이 보안위험을 이해하고 대응할 수 있도록 하는 위험평가의 중요성이 다시 한 번 확인되었다고 하였다. 그리고 Kim and Kim[22]은 2017년의 뉴욕금융시장 규제에 관한 주정부의 금융사이버보안규정(Cybersecurity Requirements for Financial Services Companies, 23NYCRR500) 개정 시 규정의 모든 항목이 위험평가에 기반하게 되었다고 분석하였다.

금융시장의 혁신을 위해 정책적으로 시장 참여자를 확대하는 상황에서 목적을 훼손하지 않으면서도 다양한 특성을 가진 기관이 금융시장에서 직면할 보안위험에 적정하게 대응할 수 있도록 전자금융에 대한 규제를 개선할 필요가 있으며, 유럽연합과 미국 등이 제도적으로 위험평가에 기반한 보안위험 관리・대응 체계를 강조하는 것은 의미 있는 시사점을 제시한다.

앞서 분석한 것처럼 국내 규제체계는 금융기관이 보안위험에 대응하기 위하여 보유해야 할 물리적・논리적・관리적 보안수단과 통제절차를 분야별로 상세하게 제시하고 기관은 이를 준수함으로써 보안위험에 대응하도록 하고 있으며, 금융기관에 대하여 위험평가와 위험관리체계 등을 보유하도록 직접적으로 규정하고 있지는 않다.

현재의 규제방식도 대상과 환경에 따라 규정을 지속적으로 변경・확대하여 규제 대상 기관이 보안위험에 적정하게 대응토록 할 수 있지만, 이는 단순히 규정 준수만을 목표하는 경향과 직면한 보안위험과 대응 역량의 차이에 관계없는 동일한 수준의 대응이라는 부작용이 있을 수 있다. 또한 규제 대상이 빠르게 변화・증가하는 상황에서는 대응할 보안위험도 보다 다양해지며, 대상 기관이 잠재적인 위험에 대해서도 자율적으로 판단・대처할 수 있는 능력을 보유토록 할 필요도 있다.

따라서 규제 대상 기관의 자율적인 보안위험 대응능력 향상이 보다 적합한 규제방향이라 할 수 있으며, 앞서 확인한 것과 같이 기관이 위험평가에 기반한 보안위험 관리・대응 체계를 보유하도록 규정하되, 필요한 부문에 대해서는 지금과 같이 보안수단과 통제절차 등을 상세하게 제시하는 규제방식의 개선이 필요하다.

국내 금융당국도 2015년 '금융IT부문 자율보안체계 확립 방안[14]'에서 법규 및 행정지도를 준수하는데 그치는 기존 방식이 아니라 기관의 자율적인 보안능력 향상을 통해 자신의 보안에 대해 스스로 책임지는 자율 보안체계를 강조하였다.

또한, '정보통신망 이용촉진 및 정보보호 등에 관한 법률' 제47조에 근거하여 ISO27001를 기반으로 조직의 정보보호관리체계를 평가하는

정보보호 관리체계 인증(Information Security Management System, 이하 ISMS인증)에서도 [24], 이러한 방향성을 확인할 수 있다. 동 인증은 전기통신 사업자 등은 의무적으로 획득해야 하며 금융 분야에서도 적극 활용하고 있는데, 전체 3개 인증영역 중 관리체계 수립 및 운영 영역의 16개 인증기준에 위험관리 관련 4개 기준을 포함한다[25].

이처럼 금융시장에서 보안위험에 대응하는 정부의 규제는 이미 대상 기관이 적정 보안위험 관리체계를 구축하도록 하는 방향성을 보이고는 있으나, IT기업 등 기존과 다른 유형의 조직에 대한 금융시장 참여를 촉진하는 상황에서는 본 연구에서 확인한 PSD2의 제도적 대응과 같이 서비스 제공자가 시장에 진입하기 전인 허가 또는 등록 단계부터 위험평가에 기반한 보안위험 관리체계를 보유・유지・개선하도록 전자금융감독규정 등 관련 법규에서 보다 적극적으로 반영할 필요가 있다.

다만 앞서 제4장의 PSD2와 국내법규의 보안위험에 대한 제도적 대응의 비교・분석 등에서 확인한 것처럼 규제 대상 기관이 보유해야하는 각 분야별 보안통제와 수단 등에 대한 요건은 이미 국내법에서 높은 수준으로 규정하고 있으므로, 규제 대상 기관의 조직 요건에 위험평가에 기반한 보안위험관리 관련 역할・책임 및 보고체계 등 조직 관련 요건을 반영하고, 실제 각 분야의 보안수단 및 통제절차에 관한 규정 중에서 위험평가에 근거하도록 규정에 명시할 필요가 있는 경우 관련 내용을 추가하는 방식의 개선이 가능할 것이다.

예를 들면, <Table 12>와 같이 현재 규제 대상 기관의 인력・조직・예산 등을 규정하고 있는 전자금융감독규정 제8조와 제8조의2 등에 위험평가에 기반한 보안위험관리에 관한 역할과 책임을 규정하는 등 관련 요건을 명시적으로 규정하고, 앞서 <Figure 2>에서 제시한 PSD2의 구성을 기준으로 보유한 정보 등의 보호와 취약점

〈Table 12〉 An Example of Changes in the Regulation on Supervision of Electronic Financial Transactions

Article	Changes
8. Personnel, Organization and Budget 8-2. Operation of Information Security Committee	Define and assign key roles and responsibilities to manage and assess security risks
12. Measures to Protect Terminals 13. Measures to Protect Computer Data 37-2. Cycle, Content, etc. of Analysis and Evaluation of Weak Points of Electronic Network for Financial Transactions	Identify criticality of business functions and information assets in accordance with risk assessment
23. Establishment and Implementation of Emergency Measures, etc	Identify criticality of functions, processes, systems, transactions and interdependencies in accordance with risk assessment to prioritise business continuity actions
19-2. Formulation and Execution of Educational Plan for Information Security	Identify staff members occupying key roles in accordance with risk assessment to provide targeted security training

분석을 규정하고 있는 전자금융감독규정 제12조, 제13조, 제37조의 2 등은 위험평가에 근거하여 정보자산이나 업무의 중요성을 인식하고 이에 근거하여 보안수단의 적용・평가와 접근기록 관리를 적용하며, 재난 등에 대비한 비상대책 수립을 규정하고 있는 제23조는 복구조치의 우선순위를 위험평가에 근거하도록 규정하고, 소속 임・직원에 대한 보안교육에 관한 제19조의2는 위험평가에 따라 핵심역할을 수행하는 대상자를 선별하고 역할에 보다 특화된 교육을 제공하도록 규정하는 것이 가능할 것이다.

5.2 허가 또는 등록 단계부터 일관된 가이드 제공

새로운 금융시장 참여자가 규제 목적에 적합한 보안 역량을 보유하고 시장에 진입하며, 이후에도 지속적으로 유지・개선하도록 하기 위해 허가 또는 등록 단계부터 대상 기관에게 규제 목적에 부합하는 명확한 기준과 가이드를 제공할 필요가 있다. 영국의 경우 영업행위감독청(Financial Conduct Authority, FCA)이 시장참여를 희망하는 기관 등에 대해 PSD2에 대응하는 자국 법규(The Payment Services Regulations 2017)의 이해를 돕기 위한 가이드 문서[10]를 제공하고 있는데, 여기서 허가 또는 등록 요건의 하나인 보안위험관리를 위한 보안수단의 기준으로 2014년에 영국정부가 중소기업 정보보호 컨소시엄(Information Assurance for Small and Medium Sized Businesses, IASME) 등과 공동으로 개발한 보안인증체계로 사이버 안전 관련 기본적인 공통 필수항목을 제시하는 사이버 에센셜(Cyber Essentials)[30]을 참조하도록 예시하고 있다.

국내에도 PSD2와 같은 제도가 도입된다면 IT기업 등 기존 금융기관과는 다른 새로운 시장 참여자가 금융시장에 적합한 보안체계를 보다 용이하게 확보하여 금융시장의 안정성을 저해하지 않도록, 법규 등에서 보안위험 대응 관련 요건을 적정하게 제시하는 것뿐만 아니라 금융시장에 적합한 보안위험관리체계의 가이드를 제공하는 것이 적절한 지원이 될 수 있다.

이를 위해 앞서 확인한 ISMS인증 제도의 활용을 고려할 수 있는데, 동 인증은 금융보안원이 금융 분야 인증기관으로 금융에 특화된 점검항목 등을 개발・운용하여 왔으며, 2019년부터 기존 '정보보호 관리체계(ISMS)' 인증과 '개인정보보호관리체계(PIMS)' 인증을 '정보보호 및 개인정보보호 관리체계(ISMS-P)' 인증으로 통합하여 수요 기관의 필요에 따라 인증 종류를 선택할 수 있도록 변경된 제도[29]하에서도, 인증기관으로서 동일한 역할을 수행한다.

따라서 금융당국과 협력하여 동 기준을 기반으로 새로운 시장 참여자를 위한 금융시장 진입 시 보유해야하는 보안체계에 대한 가이드를 수립하기에 용이하며, 앞서 영국의 사례처럼 금융당국이 동 가이드를 규제요건에 대한 참조 예시로 제시하는 방식 등으로 규제 목적과 내용에 대한 이해를 높이는 유용한 수단이 될 수 있다. 또한, 법규에서 모든 보안 요건을 제시하는 것보다 기술 발전과 보안위험 변화에 더 유연하게 대처할 수 있고, 시장 진입 시에 구축한 보안체계의 참조기준과 서비스 제공 시 인증기준에 통일성이 있으므로, 실제 인증 취득 여부와 관계없이 서비스 제공 단계에서도 지속적으로 보안위험 대응에 관한 참조 지침으로 활용하는 것이 가능하다.

6. 결 론

본 연구에서는 PSD2의 내용과 배경을 분석하여 먼저 유럽연합이 오픈API라는 IT를 수단으로 금융기관이 지배적인 위치에서 이용하던 계좌와 정보를 금융기관이 아닌 제3자도 이용할 수 있도록 제도적으로 보장함으로써 새로운 유형의 서비스를 적극적으로 도입하고 금융시장의 혁신을 도모하는 내용을 확인하였으며, 동시에 이와 같은 정책 목적을 달성하기 위해 위험평가에 기반한 보안위험관리체계를 중심으로 보안위험에 대한 제도적인 대응을 강화하였음도 확인하였다.

그리고 IT에 기반한 서비스가 금융시장에서 지속적으로 확대되고 있으며 금융당국에 의해 계좌에 대한 접근과 정보이용에 대한 제도적 변화가 추진되는 상황에서는 국내 전자금융규제의 보안위험에 대한 제도적 대응을 위험평가에 기반한 보안위험관리체계의 구축을 중심으로 개선하여, 준수해야 할 보안수단과 통제절차를 상세하게 규정하는 기존 방식보다 규제대상 기관의 자율적인 대응능력 향상과 다양한 보안위험에 보다 유연하고 적합한 대응을 기대할 수 있음을 제시하였다.

또한, 새로운 시장 참여자에게 보안위험 대응 관련 규제요건에 대한 명확한 지침을 제공하고 이후에도 일관성 있게 보안위험에 대응할 수 있도록, 해외 사례 등을 분석하여 국내 금융분야 ISMS인증 기준을 활용한 가이드 제공을 제안하였다.

IT의 발전과 이를 이용하여 제도적으로 금융시장의 변화를 도모하는 다양한 시도가 이루어지고 있는 상황에서는 국내 전자금융의 보안위험 대응에 관한 규제의 발전을 위한 보다 다양한 논의와 접근이 필요할 것이며, 본 연구는 PSD2의 개정 의도와 내용을 중심으로 국내의 규제에 대한 시사점과 개선 방향을 제시하는데 중점을 두었기 때문에, 향후 본격적으로 제도가 적용된 후 보다 실제적인 사례와 교훈을 확인하고 관련 전문가 그룹과의 충분한 논의 등을 거쳐 국내 금융시장에 적합한 보다 구체적인 규제의 내용을 제시하고, 기존과는 달리 서비스 제공 시 다수의 기관이 관련되어 있는 환경에서 보안사고가 발생하였을 때 이용자를 보호하고 배상과 입증 책임 등을 명확할 수 있는 규정의 변화에 대하여 추가 연구가 필요할 것이다.

References

[1] Bank of Korea, 2017 Financial Informatization Promotion, https://www.bok.or.kr/portal/bbs/P0000272/view.do?nttId=10047572&menuNo=200728&pageIndex=, 2018.

[2] Cortet, M., Rijks, T., and Nijland, S., “PSD2: The digital transformation accelerator for banks,” Journal of Payments Strategy & Systems, Vol. 10, No. 1, pp. 13-27, 2016.

[3] Euro Banking Association, Understanding the business relevance of Open APIs and Open Banking for banks, https://www.abe-eba.eu/publications/, 2016.

[4] European Banking Authority, Consultation Paper on the security measures for operational and security risks of payment

services under PSD2, 2017.

[5] European Banking Authority, Guidelines on the information to be provided for the authorisation of payment institutions and e-money institutions and for the registration of account information service providers under Article 5(5) of Directive (EU) 2015/2366, 2017.

[6] European Banking Authority, Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2), 2018.

[7] European Commission, Fact Sheet - Payment Services Directive: frequently asked questions, https://ec.europa.eu/commission/presscorner/detail/en/memo_15_5793, 2018.

[8] European Commission, The Directive on security of network and information systems (NIS Directive), https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive, August 7, 2019.

[9] European Union Agency for Cybersecurity, Good practices on the implementation of regulatory technical standards MS approaches on PSD 2 implementation: commonalities in risk management and incident reporting, https://www.enisa.europa.eu/publications/good-practices-on-the-implementation-of-regulatory-technical-standards, 2018.

[10] Financial Conduct Authority, [1] Payment Services and Electronic Money - Our Approach, The FCA's role under the Payment Services Regulations 2017 and the Electronic Money Regulations 2011, https://www.fca.org.uk/firms/emi-payment-institutions-key-publications, 2019.

[11] Financial Services Commission, "Press Releases, 2018. 7. 18," http://www.fsc.go.kr/info/ntc_news_view.jsp?bbsid=BBS0030&page=1&sch1=subject&sword=%EB%A7%88%EC%9D%B4%EB%8D%B0%EC%9D%B4%ED%84%B0&r_url=&menu=7210100&no=32579, Aug 15, 2019.

[12] Financial Services Commission, Credit Information Use and Protection Act, No. 16188, 2018.

[13] Financial Services Commission, Electronic Financial Transactions Act, No. 14828, 2017.

[14] Financial Services Commission, Press Releases, 2015. 1. 27, http://www.fsc.go.kr/info/ntc_news_view.jsp?bbsid=BBS0030&page=1&sch1=subject&sword=%EC%9C%B5%ED%95%A9&r_url=&menu=7210100&no=30227, Sep 30, 2019.

[15] Financial Services Commission, Press Releases, 2018. 3. 20, http://www.fsc.go.kr/info/ntc_news_view.jsp?bbsid=BBS0030&page=1&sch1=subject&sword=%ED%95%80%ED%85%8C%ED%81%AC%20%ED%98%81%EC%8B%A0%20%ED%99%9C%EC%84%B1%ED%99%94%20%EB%B0%A9%EC%95%88&r_url=&menu=7210100&no=32368, Aug 15, 2019.

[16] Financial Services Commission, Press

Releases, 2019. 2. 25, http://www.fsc.go.kr/info/ntc_news_view.jsp?bbsid=BBS0030&page=1&sch1=subject&sword=%EA%B8%88%EC%9C%B5%EA%B2%B0%EC%A0%9C&r_url=&menu=7210100&no=32976, Aug 15, 2019.

[17] Financial Services Commission, Regulation on Supervision of Credit Information Business, No. 2019-33, 2019.

[18] Financial Services Commission, Regulation on Supervision of Electronic Financial Transactions, No. 2018-36, 2019.

[19] Financial Supervisory Service, Manual for Authorization of Financial Institutions, http://www.fss.or.kr/fss/kr/bbs/view.jsp?bbsid=1207388946537&url=/fss/kr/1207388946537&idx=1549530368762, 2019.

[20] Gozman, D., Hedman, J., Sylvest, K., and Bank, D., "Open Banking: Emergent Roles, Risks & Opportunities," The 26th European Conference on Information Systems (ECIS), pp. 1-15, 2018.

[21] Ju, Y. S., "The role of IT in Korean financial market from business ecosystem view," Master's Thesis, Korea University, 2008.

[22] Kim, D. C. and Kim, I. S., "A Study on Cybersecurity Regulation for Financial Sector: Policy Suggestion based on New York's Cybersecurity Regulation," The Journal of Society for e-Business Studies, Vol. 23, No. 4, pp. 87-107, 2018.

[23] Kim, E. K., "The Application of Fin-tech industry and Law in European Union," Kangwon Law Review, Vol. 49, pp. 617-654, 2016.

[24] Korea Internet & Security Agency, Information Security Management System[ISMS] Certification, https://isms.kisa.or.kr/main/isms/notice/ (Page3, No.28), Aug 15, 2019.

[25] Korea Internet & Security Agency, Personal Information & Information Security Management System Certification Guidebook, https://isms.kisa.or.kr/main/ispims/notice/ (Page1, No.8), Sep 30, 2019.

[26] Lee, H. K., "A Study on Regulations, Current Status and Implications of Electronic Finance and Financial Security in the U.S.," Business Law Review, Vol. 31, No. 3, pp. 491-529, 2017.

[27] Milne, A., "Competition policy and the financial technology revolution in banking," DigiWorld Economic Journal, Vol. 103, pp. 145-161, 2016.

[28] Ministry of Science and ICT and Korea Internet & Security Agency, 2017 Survey on Information Security : Business, http://www.kisa.or.kr/public/library/etc_View.jsp?regno=0099060&searchType=&searchKeyword=&pageIndex=4, 2018.

[29] Ministry of Science and ICT, Press Releases, 2018. 11. 6, https://www.msit.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=1411436, Aug 15, 2019.

[30] National Information society Agency, NIA Special Report 2018-15, https://www.nia.or.kr/site/nia_kor/ex/bbs/View.do?cbIdx=82618&bcIdx=20329&parentSeq=2032

9, 2018.

[31] National Institute of Standards and Technology, NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments, https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final, 2012.

[32] National Institute of Standards and Technology, NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, https://csrc.nist.gov/publications/detail/sp/800-39/final, 2011.

[33] Noctor, M., "PSD2: Is the banking industry prepared?," Computer Fraud & Security, Vol. 2018, No. 6, pp. 9-11, 2018.

[34] Office of the Comptroller of the Currency, OCC Begins Accepting National Bank Charter Applications From Financial Technology Companies, https://www.occ.gov/news-issuances/news-releases/2018/nr-occ-2018-74.html, Aug 8, 2019.

[35] Park, J. S., Kim, M. J., and Hwang, B. I., "The development background and major trends of fintech," The Journal of The Korean Institute of Communication Sciences, Vol. 33, No. 2, pp. 52-58, 2016.

[36] The European Commission, Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication, OJ L Vol. 69, pp. 23-43, 2018.

[37] The European Parliament and The Conucil of The European Union, Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC OJ L Vol. 337, pp. 35-127, 2015.

[38] The Institute of Internal Auditors, IIA Position Paper: The three lines of defense in effective risk management and control, https://global.theiia.org/standards-guidance/recommended-guidance/Pages/The-Three-Lines-of-Defense-in-Effective-Risk-Management-and-Control.aspx, 2013.

[39] Wolters, P. T. J. and Jacobs, B. P. F., "The security of access to accounts under the PSD2," Computer Law & Security Review, Vol. 35, No. 1, pp. 29-41, 2019.

저 자 소 개

김현부 (E-mail: wagamichi@hanmail.net)
2004년 중앙대학교 컴퓨터공학과 졸업 (학사)
2018년～현재 고려대학교 정보보호대학원 석사과정
2004년～현재 금융감독원 근무
관심분야 정보보호정책, 금융보안

김인석 (E-mail: iskim11@korea.ac.kr)
2008년 고려대학교 정보경영공학과 졸업 (박사)
2009년～현재 고려대학교 정보보호대학원 교수
FDS산업포럼 회장, 한국정보보호학회 운영위원
관심분야 전자금융보안, IT감사, 전자금융법규