

NAVER FINANCIAL

네이버파이낸셜 주식회사

System and Organization Controls 3 Report

네이버페이 서비스의 보안성, 가용성, 처리무결성, 기밀성 및
개인정보보호 관련 독립된 감사인의 보고서

2023년 1월 1일 - 2023년 12월 31일

목차

Section I: 독립된 감사인의 보고서.....	2
Section II: 경영진의 주장	4
Section II: 경영진의 주장 (하위서비스조직)	5
Section III: 네이버페이 서비스 시스템의 범위에 관한 기술서	6
1. 개요	6
회사 소개	6
서비스.....	6
보고서의 적용 범위.....	7
2. 서비스 구성요소	7
인프라스트럭처	7
소프트웨어	7
인력.....	7
절차.....	7
데이터.....	8
Section IV: 주요 서비스 책임과 시스템 요구사항.....	9

Section I: 독립된 감사인의 보고서

네이버파이낸셜 주식회사 귀중

경기도 성남시 분당구 정자일로 95

NAVER 1784

업무의 범위

딜로이트 안진회계법인(이하 '서비스감사인' 또는 '우리')은 네이버파이낸셜 주식회사('네이버파이낸셜', '서비스조직' 또는 '회사')의 네이버페이 서비스 (이하 '시스템')에 대한 통제와 네이버클라우드 주식회사('네이버클라우드' 또는 '하위서비스조직')의 네이버파이낸셜이 설계하고 네이버클라우드가 운영하는 통제가 미국공인회계사회(AICPA)가 제정한 "보안성, 가용성, 처리무결성, 기밀성 및 개인정보보호를 위한 2017 트러스트 서비스 준거기준(2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy)"의 TSP Section 100 에서 제시한 보안성, 가용성, 처리무결성, 기밀성 및 개인정보보호와 관련된 트러스트 서비스 준거기준 (이하 '해당 트러스트 서비스 준거기준')에 따라 네이버파이낸셜의 서비스 책임과 시스템 요구사항이 달성되었다는 합리적인 확신을 제공할 수 있도록 2023년 1월 1일부터 2023년 12월 31일까지의 기간 동안 효과적이었다는 "Section II: 경영진의 주장"(이하 '경영진의 주장') 및 "Section II: 경영진의 주장(하위서비스조직)"(이하 '경영진의 주장(하위서비스조직)')을 감사하였습니다.

서비스조직의 책임

네이버파이낸셜은 서비스 책임과 시스템 요구사항을 준수하고, 서비스 책임과 시스템 요구사항이 달성되었다는 합리적인 확신을 제공할 수 있도록 시스템 내에서 효과적인 통제를 설계, 구현 및 운영할 책임이 있습니다. 네이버파이낸셜은 시스템 내에 통제의 효과성에 대해 첨부 경영진의 주장을 제시하였습니다. 경영진의 주장을 작성함에 있어 네이버파이낸셜은 해당 트러스트 서비스 준거기준을 선정 및 식별하고, 시스템 내 통제의 효과성을 평가하여 경영진의 주장에 대한 합리적인 근거를 확보하고 책임이 있습니다.

하위서비스조직의 책임

네이버클라우드는 네이버파이낸셜이 설계하고 네이버클라우드가 운영하는 통제의 효과성에 대해 경영진의 주장을 제시하였습니다. 경영진의 주장을 작성함에 있어 네이버클라우드는 네이버파이낸셜이 설계한 통제의 효과성을 평가하여 네이버파이낸셜이 서비스 책임과 시스템 요구사항을 달성할 수 있도록 경영진의 주장에 대해 합리적인 근거를 확보할 책임이 있습니다.

서비스감사인의 책임

우리의 책임은 우리가 수행한 평가를 근거로, 회사의 서비스 책임과 시스템 요구사항이 해당 트러스트 서비스 준거기준에 따라 달성되었다는 합리적인 확신을 제공하기 위해 시스템 내 통제가 보고기간 동안 효과적이었다는 경영진의 주장에 대하여 의견을 표명하는 것입니다. 우리는 미국공인회계사회(American Institute of Certified Professional Auditors; AICPA)가 제정한

인증업무기준과, 국제감사인증기준위원회(International Auditing and Assurance Standards Board; IAASB)가 제정한 인증업무기준 3000, *역사적 재무정보에 대한 감사 또는 검토 이외의 인증업무기준*(ISAE 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*)에 따라 업무를 수행하였습니다. 이 기준은 경영진의 주장이 중요성의 관점에서 공정하게 표시되었는지에 대해 합리적인 확신을 얻을 수 있도록 감사를 계획하고 수행할 것을 요구하고 있습니다. 우리는 우리가 입수한 증거가 우리의 의견을 위한 근거로서 충분하고 적합하다고 믿습니다.

우리는 인증업무와 관련된 윤리적 요구사항에 따라 독립성을 유지하고 기타 윤리적 책임을 이행할 책임이 있습니다.

우리가 수행한 감사업무에는 다음의 절차가 포함되었습니다.

- 시스템, 회사의 서비스 책임과 시스템 요구사항에 대한 이해
- 통제가 효과적이지 아니하여 해당 트러스트 서비스 준거기준에 따라 네이버파이낸셜의 서비스 책임과 시스템 요구사항이 달성되지 않을 위험에 대한 평가
- 해당 트러스트 서비스 준거기준에 따라 네이버파이낸셜의 서비스 책임과 시스템 요구사항이 달성되도록 시스템 내 통제가 효과적이었는지에 대한 증거를 입수하기 위한 절차의 수행

우리는 상황에 따라 필요하다고 인정되는 기타의 절차로도 평가를 수행하였습니다.

서비스감사인의 독립성 및 품질 관리

우리는 성실, 객관성, 전문가적 적격성과 정당한 주의, 비밀유지 및 전문가적 품위 등의 기본 원칙에 기반한, 미국공인회계사회가 제정한 *전문가행동강령*(Code of Professional Conduct) 내 독립성을 비롯한 기타 윤리적 요구사항들과 국제회계사윤리기준 위원회(International Ethics Standards Board for Accountants; IESBA)의 *회계사윤리강령*(Code of Ethics for Professional Accountants)을 준수하였습니다. 우리는 품질관리에 관한 미국공인회계사회의 기준서들과, 국제품질관리기준 1, *재무제표의 감사나 검토, 또는 기타 인증업무나 관련 서비스를 수행하는 법인의 품질관리*(International Standards on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements*)를 적용하고 있으며, 이에 따라 종합적인 품질관리체계를 유지하고 있습니다.

고유한계

모든 내부통제 체계는 인적 오류나 통제를 우회할 가능성 등으로 인해 그 효과성이 저하될 수 있는 고유 한계를 지니고 있습니다. 이러한 특성으로 인해 통제가 해당 트러스트 준거기준에 따라 회사의 서비스 책임과 시스템 요구사항이 달성되었다는 합리적인 확신을 제공하도록 항상 효과적으로 운영되지는 않을 수 있습니다. 또한, 통제의 효과성에 대한 현재의 평가를 미래의 기간으로 연장하는 것은 환경의 변화로 인해 회사의 통제가 효과적이지 않게 되거나, 정책 또는 절차를 준수하는 정도가 약화되는 위험을 수반합니다.

의견

우리의 의견으로는 네이버페이 서비스 환경 내 통제가 해당 트러스트 서비스 준거기준에 따라 네이버파이낸셜의 서비스 책임과 시스템 요구사항이 달성되었다는 합리적인 확신을 제공할 수 있도록 2023년 1월 1일부터 2023년 12월 31일의 기간 동안 효과적이었던 경영진의 주장은 중요성의 관점에서 공정하게 표시되어 있습니다.

Deloitte Anjin LLC.

2024년 4월 26일
대한민국, 서울

Section II: 경영진의 주장

우리(‘네이버파이낸셜’ 또는 ‘서비스조직’)는 네이버페이 서비스가 미국공인회계사회가 제정한 “보안성, 가용성, 처리무결성, 기밀성 및 개인정보보호를 위한 2017 트러스트 서비스 준거기준 (2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy)”의 TSP Section 100(AICPA, Trust Services Criteria)에서 제시한 보안성, 가용성, 처리무결성, 기밀성 및 개인정보보호와 관련된 트러스트 서비스 준거기준(이하 ‘해당 트러스트 서비스 준거기준’)에 관련된 서비스 책임과 시스템 요구사항을 달성하였다는 합리적인 확신을 제공하기 위해 2023년 1월 1일부터 2023년 12월 31일까지의 기간에 대하여 시스템 내 통제를 효과적으로 설계, 구현, 운영 및 유지할 책임이 있습니다. 해당 시스템의 범위에 대한 기술서는 Section III 에 제시되었으며, 동 기술서에는 우리의 주장에 포함되는 시스템의 측면이 표시되어 있습니다.

우리는 네이버파이낸셜의 서비스 책임과 시스템 요구사항이 관련 트러스트 서비스 준거기준에 따라 달성되었다는 합리적인 확신을 제공하기 위해 2023년 1월 1일부터 2023년 12월 31일까지 기간 동안의 시스템 내 통제의 효과성을 평가하였습니다. 해당 트러스트 서비스 준거기준을 적용하기 위한 시스템의 목적들은 해당 트러스트 서비스 준거기준과 관련된 서비스 책임과 시스템 요구사항에 반영되어 있으며, 해당 트러스트 서비스 준거기준과 관련된 주요 서비스 책임과 시스템 요구사항은 Section IV 에 기술되어 있습니다.

네이버파이낸셜은 네이버페이 서비스와 관련된 IT 인프라스트럭처 운영 서비스에 대해 네이버클라우드를 이용하고 있습니다. 네이버클라우드가 제공하는 서비스는 네이버파이낸셜이 제공하는 서비스의 일부입니다. 해당 트러스트 서비스 기준에 따라 네이버파이낸셜의 서비스 책임과 시스템 요구사항을 달성하는데 네이버파이낸셜이 설계하고 하위서비스조직이 운영하는 통제가 필요합니다.

모든 내부통제체계는 인적 오류와 통제를 우회할 가능성 등을 포함하여, 효과성에 대한 고유한계를 지니고 있습니다. 이러한 고유한계 때문에 서비스조직은 서비스 책임과 시스템 요구사항이 달성되었다는 절대적 확신이 아닌 합리적 확신을 달성할 수 있습니다.

우리는 네이버파이낸셜의 서비스 책임과 시스템 요구사항이 해당 트러스트 서비스 준거기준에 따라 달성되었다는 합리적인 확신을 제공할 수 있도록 네이버파이낸셜의 통제와 네이버파이낸셜이 설계하고 네이버클라우드가 운영하는 시스템 내 통제가 2023년 1월 1일부터 2023년 12월 31일까지의 기간 동안 효과적이었다고 주장합니다.

Section II: 경영진의 주장 (하위서비스조직)

네이버클라우드 주식회사(‘네이버클라우드’ 또는 ‘우리’)는 네이버파이낸셜 주식회사(이하 ‘네이버파이낸셜’)의 네이버페이 서비스 시스템과 관련된 IT 인프라스트럭처 운영 서비스를 제공하고 있습니다. 네이버클라우드가 제공하는 서비스는 네이버페이 서비스 시스템의 일부입니다. 우리는 미국공인회계사회가 제정한 “*보안성, 가용성, 처리무결성, 기밀성 및 개인정보보호를 위한 2017 트러스트 서비스 준거기준 (2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy)*”의 TSP Section 100(AICPA, *Trust Services Criteria*)에서 제시한 보안성, 가용성, 처리무결성, 기밀성 및 개인정보보호와 관련된 트러스트 서비스 준거기준(이하 ‘해당 트러스트 서비스 준거기준’)에 따라 네이버파이낸셜의 서비스 책임과 시스템 요구사항을 달성하였다는 합리적인 확신을 제공하기 위해 2023년 1월 1일부터 2023년 12월 31일까지의 기간에 대해서 네이버파이낸셜이 설계한 네이버페이 서비스 시스템 내의 통제의 운영 효과성에 대한 책임이 있습니다.

우리는 네이버파이낸셜이 설계하고 네이버클라우드가 운영하는 통제들은 2023년 1월 1일부터 2023년 12월 31일까지의 기간 동안 해당 트러스트 서비스 기준에 따라 효과적이었다고 주장합니다.

Section III: 네이버페이 서비스 시스템의 범위에 관한 기술서

1. 개요

회사 소개

네이버파이낸셜 주식회사(이하 '네이버파이낸셜', '회사' 또는 '서비스조직')는 금융사업의 독립성을 강화하고 사업 추진의 속도를 높이기 위해 2019년 11월 1일 네이버 주식회사로부터 분사하여 설립되었으며, NAVER Pay(이하 '네이버페이') 서비스를 제공하고 있습니다.

네이버페이는 2015년 6월, 다양한 가맹점에서 네이버 ID로 쇼핑하고 네이버 뮤직, 영화, e북 등 디지털콘텐츠까지 결제, 충전, 적립, 송금할 수 있는 서비스로 정식 출시되면서 사업의 범위를 간편결제 및 통합결제 서비스까지 확대하고 기존 서비스와의 연계를 통해 시너지 효과를 창출하고 있습니다.

2018년 소상공인의 결제 수수료 부담은 낮추고 소비자의 혜택은 높이는 제로페이 결제를 지원하며, 2019년 라인페이와 함께 일본 오프라인 QR 결제 서비스를 시작하여 오프라인 영역까지 확장하였습니다.

2020년 6월 네이버페이 회원 전용통장 서비스 출시를 시작으로 보험, 대출 서비스 등 이용자가 일상에서 금융서비스를 좀 더 쉽고 편리하게 경험할 수 있도록 다양한 온라인 금융플랫폼 사업을 준비하였습니다.

2021년 그 동안에 축적된 이용자 데이터와 데이터 기반 기술을 활용해 대안신용평가시스템을 고도화하고, 글로벌에서 가장 빠른 정산시스템과 혁신금융서비스로 지정된 후불결제 서비스와 오프라인 결제·주문에 특화된 네이버페이 앱을 출시하였으며, 기존 '내자산 서비스'를 마이데이터 API(Application Programming Interface) 체계로 전환하였습니다.

또한 2022년에는 마이데이터를 기반한 보험통합조회 서비스와 핀테크 최초 사업자대출비교 서비스 출시를 통해 차별화된 서비스를 제공하고, 스마트워치 전용 네이버페이 워치앱과 네이버페이 머니 하나 통장을 출시하였습니다.

2023년 네이버페이 X 삼성페이 MST 기반 현장 결제 서비스를 시작하였고, 해외 65개 지역/국가에서 가능한 현장결제, 그리고 핀테크 최초로 예적금 간편가입/파킹통장 비교서비스를 오픈하며 혁신 금융 서비스로 진화하고 있습니다.

서비스

회사의 서비스는 고객의 편리한 서비스 이용을 위해 PC 웹, 모바일을 통하여 제공됩니다. 이러한 서비스를 제공하기 위하여 다양한 IT 시스템과 보안장비, 그리고 자체적으로 개발한 서비스 관리 시스템들을 사용하고 있습니다. 본 기술서에서 포함하는 서비스는 다음과 같습니다.

- 네이버페이 - 네이버 ID로 다양한 가맹점에서 회원가입 없이 쇼핑, 결제, 배송을 관리할 수 있고 네이버 뮤직, 영화, 웹툰 등 디지털콘텐츠를 결제할 수 있는 서비스입니다.

서비스 이용자는 회사의 서비스를 안전하고 올바르게 이용하기 위하여, 서비스 이용약관의 '회원의 의무'를 준수해야 합니다. 또한, 서비스 이용자는 본인의 데이터를 보호하기 위하여 패스워드를 주기적으로 변경하며, 타인에게 공개하지 않는 등 일반적으로 서비스 이용자 본인이 개인정보보호를 위해 수행해야 하는 활동을 인식하고 이행해야 합니다.

보고서의 적용 범위

이 보고서의 범위는 네이버페이 서비스로 한정되며, 그 외 다른 서비스에 대한 내용을 포함하고 있지 않습니다.

2. 서비스 구성요소

회사의 서비스 제공을 위해 인프라스트럭처, 소프트웨어, 데이터와 이를 운영하기 위한 절차 및 인력으로 구성하고 있습니다.

인프라스트럭처

회사는 서비스 제공을 위해 서버, 네트워크, 보안시스템 등 인프라를 구축하여 운영하고 있으며, 각 인프라는 독립된 망으로 구성되어 있습니다. 인프라스트럭처에 대한 접근통제 절차를 수립하여 비인가자에 의한 논리적/물리적 접근을 차단하고 있으며, 이상행위 로그를 기록하여 주기적으로 모니터링하고 있습니다.

회사는 또한 인프라스트럭처에서 발생 가능한 취약점을 지속적으로 탐지, 보완하기 위하여 자동화된 취약점 점검 도구를 운영하고 발견된 취약점에 대한 개선조치를 실시하고 있습니다. 인프라스트럭처가 위치하고 있는 데이터센터를 화재, 지진, 홍수 등 재해로부터 보호하기 위하여 화재감지기, 소화설비, 무정전 전원장치(UPS), 항온항습기, 누수탐지기 등의 설비를 운영하고 있습니다.

소프트웨어

서비스를 제공하기 위한 어플리케이션의 개발 운영은 서비스별 담당 부서에서 담당하고 있으며, 이용자에게 제공하는 서비스 품질 향상, 장애 및 성능 개선 등의 사유로 어플리케이션 추가 개발 또는 고도화가 필요한 경우 서비스 기획부서와 개발부서 간 협의를 통해 보안요구사항을 정의하고, 정의된 내용은 인트라넷을 통해 이해관계자에게 공유하고 있습니다.

어플리케이션의 변경사항은 책임자에 의해 사전 승인되며, 변경 후 발생 가능한 장애를 최소화하기 위하여 QA(Quality Assurance) 조직의 검토를 거친 후 자동화된 시스템을 통해 운영환경으로 배포됩니다. 이용자의 개인정보 처리와 관련된 중대한 변경이 포함되는 경우 개인정보 영향평가를 실시하여 그 영향도를 검토하고, 필요한 경우 개선조치를 실시하고 있습니다.

인력

해당 서비스의 안정적인 제공을 위해 회사는 정보보호 및 개인정보보호 담당자, 서비스 기획자, 개발자, 인프라 운영자, CS(Customer Satisfaction) 담당자 등을 지정하여 운영하고 있으며, 각 인력의 정보보호 인식 제고를 위해 매년 정보보호 및 개인정보보호 교육을 실시하고 있습니다.

신규 입사자 및 퇴사자 발생 즉시 정보보호 서약서를 작성, 제출토록 하여 비밀유지 의무에 대한 준수사항을 전달하고 있으며, 전체 임직원은 매년 정보보호 서약서를 작성, 제출하고 있습니다.

절차

회사는 보안성, 가용성, 처리 무결성, 기밀성 및 개인정보보호 원칙을 준수하기 위하여 정책, 지침, 가이드라인 등 정보보호 규정을 마련하고 있으며, 각 규정은 관련 법령의 요구사항 변화에 따라 주기적으로 모니터링되고 필요 시 개정되며, 개정 시 책임자의 승인을 득한 후 인트라넷을 통해 전체 임직원에게 공표하고 있습니다.

이용자의 개인정보 및 프라이버시 보호를 위한 관련 규정은 이용자가 언제든지 확인 가능하도록 홈페이지 개인정보처리방침 등을 통해 공개하고 있습니다.

데이터

이용자 개인정보를 포함한 중요 데이터는 정보통신망법, 개인정보보호법 등 관련 법령과 서비스 이용약관 및 회사의 정보보호 규정에서 제시하고 있는 기준에 따라 보호하고 있으며, 관련 업무담당자에 의해서만 처리되도록 관리하고 있습니다.

중요 데이터의 보호를 위해 접근통제, 암호화, 로그기록 등 기술적 보호조치를 적용하고 있습니다.

Section IV: 주요 서비스 책임과 시스템 요구사항

회사는 이용자에게 네이버페이 서비스 이용에 대한 책임을 약속하고, 시스템 요구사항을 확립하였습니다. 이러한 책임 중 일부는 서비스 수행 및 해당 트러스트 서비스 준거기준과 관련이 있습니다. 회사는 서비스 책임과 시스템 요구사항, 그리고 이들이 달성되었다는 합리적인 확신을 제공하기 위해 시스템 내에 통제를 적절히 설계 및 구현하고, 효과적으로 운영할 책임이 있습니다.

고객에게 약속하는 서비스 책임은 이용약관과, 개인정보처리방침, 청소년보호정책, 스팸메일정책, 검색결과 수집에 대한 정책 등으로 문서화하여 고객센터를 통해 고객과 공유하며, 이와 더불어 온라인으로 서비스에 대한 설명을 제공하고 있습니다. 회사의 서비스 책임에는 다음의 내용이 포함되며, 이에 한정되지 않습니다:

- **보안성:** 회사는 암호화, 사용자 인증, 접근통제, 물리적 보안 등의 통제를 통해 고객의 데이터를 인가되지 않은 접근 및 사용으로부터 안전하게 보호하고, 인가된 사용자에 의한 오남용 방지 및 주기적인 모니터링을 수행할 책임이 있습니다.
- **가용성:** 회사는 성능 모니터링, 주기적인 데이터 백업 및 복구 등의 통제를 통해 서비스를 중단없이 지속적으로 제공할 책임이 있습니다.
- **처리무결성:** 회사는 안전한 시스템 개발환경 및 운영환경 구축, 운영환경 이관 시 책임자의 승인 등을 통해 고객의 정보를 완전하고 정확하며, 적시에 처리할 책임이 있습니다.
- **기밀성:** 회사는 중요한 사용자 정보의 전송 및 저장 시 암호화를 비롯한 보안통제를 통해 고객정보의 기밀성을 보호할 책임이 있습니다.
- **개인정보보호:** 회사는 관련 법령 및 회사의 개인정보처리방침에 따른 개인정보의 수집, 저장, 이용, 제공, 위탁 및 파기 절차를 통해 고객의 개인정보를 보호하고, 개인정보의 유출 및 오남용을 예방함으로써 고객의 프라이버시를 보호할 책임이 있습니다.

회사는 서비스 책임, 관련 법규 및 시스템 요구사항을 달성하기 위해 운영 요구사항을 정의하고 있습니다. 이러한 요구사항은 회사의 정책 및 절차, 시스템 설계 문서에 명시하고 있으며, 홈페이지를 통해 고객에게 전달됩니다.

회사의 정보보호 정책은 전사를 대상으로 시스템과 데이터가 어떻게 보호되어야 하는지에 대하여 정의하고 있으며, 여기에는 서비스의 설계 및 개발, 시스템의 운영, 내부 업무 시스템 관리, 네트워크 관리, 및 임직원의 입사와 교육에 대한 정책이 포함됩니다. 이와 더불어 네이버페이 서비스와 관련된 시스템을 운영하거나 개발하는데 있어 필요한 수작업 및 자동화된 세부 절차의 수행 방법을 표준 운영 절차에 명시하고 있습니다.