



WORKS MOBILE

웍스모바일 주식회사

System and Organization Controls 3 Report

**NAVER WORKS 서비스의 보안성, 가용성, 처리무결성, 기밀성, 개인정보보호에 대한
독립된 감사인의 보고서**

2020 년 1 월 1 일 - 2020 년 12 월 31 일

목차

Section I: 독립된 감사인의 보고서	2
범위	2
서비스조직의 책임.....	2
서비스감사인의 책임	2
고유한계	3
의견	3
Section II: 경영진의 주장.....	4
웹스모바일 경영진의 주장.....	4
Section III: NAVER WORKS 서비스 시스템의 범위에 대한 기술서.....	5
1. 개요	5
회사 소개	5
서비스.....	5
보고서의 적용 범위.....	5
2. 서비스 구성요소	6
인프라스트럭처	6
소프트웨어	6
인력	6
데이터.....	6
절차	7
Section IV: 주요 서비스 책임과 시스템 요구사항	8

Section I: 독립된 감사인의 보고서

웍스모바일 주식회사 귀중

경기도 성남시 분당구 분당내곡로 117

크라프트톤 타워 10F

범위

딜로이트 안진회계법인(이하 '서비스 감사인' 또는 '우리')은 웍스모바일 주식회사(이하 '서비스조직' 또는 '회사')의 NAVER WORKS 서비스 환경(이하 '시스템')에 대한 통제가 미국공인회계사회가 제정한 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*)의 TSP Section 100 에서 제시한 보안성, 가용성, 처리무결성, 기밀성 및 개인정보보호와 관련된 트러스트 서비스 준거기준 (이하 '해당 트러스트 서비스 준거기준')에 따라 회사의 서비스 책임과 시스템 요구사항이 달성되었다는 합리적인 확신을 제공하기 위해 2020년 1월 1일부터 2020년 12월 31일까지의 기간 동안 효과적으로 운영되었다는 "Section II: 경영진의 주장"(이하 '경영진의 주장')을 감사하였습니다.

서비스조직의 책임

회사는 서비스 책임과 시스템 요구사항, 그리고 이들이 달성되었다는 합리적인 확신을 제공하기 위해 시스템 내에 통제를 효과적으로 설계 및 구현하고 운영할 책임이 있습니다. 또한 회사는 시스템 내 통제의 효과성에 대해 첨부 Section II 에서 경영진의 주장을 제시하였습니다. 경영진의 주장을 작성함에 있어 회사는 해당 트러스트 서비스 준거기준을 선정하고 이를 경영진의 주장에 표시할 책임이 있으며, 시스템 내 통제의 효과성을 평가하여 경영진의 주장에 대한 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 효과적으로 운영되었다는 경영진의 주장에 대하여 의견을 표명하는 것입니다. 우리는 미국공인회계사회가 제정한 인증업무기준(AICPA attestation standards)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.

우리가 수행한 감사업무에는 다음의 절차가 포함되었습니다.

- 시스템, 회사의 서비스 책임과 시스템 요구사항에 대한 이해
- 통제가 효과적이지 아니하여 해당 트러스트 서비스 준거기준에 따라 회사의 서비스 책임과 시스템 요구사항이 달성되지 않을 위험에 대한 평가

- 해당 트러스트 서비스 준거기준에 따라 회사의 서비스 책임과 시스템 요구사항이 달성되도록 시스템 내 통제가 효과적이었는지에 대한 증거를 입수하기 위한 절차의 수행

우리는 상황에 따라 필요하다고 인정되는 기타의 절차로도 평가를 수행하였습니다.

고유한계

모든 내부통제 체계는 사람의 실수, 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 요구사항들이 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 저하되는 위험을 수반합니다.

의견

우리의 의견으로는 NAVER WORKS 서비스 환경 내 통제가 해당 트러스트 서비스 준거기준에 따라 회사의 서비스 책임과 시스템 요구사항이 달성되었다는 합리적인 확신을 제공할 수 있도록 2020년 1월 1일부터 2020년 12월 31일의 기간 동안 효과적으로 운영되었다는 경영진의 주장은 중요성의 관점에서 공정하게 표시되어 있습니다.

Deloitte Anjin LLC.

2021년 4월 23일
대한민국, 서울

Section II: 경영진의 주장

웍스모바일 경영진의 주장

우리(이하 '웍스모바일' 또는 '회사')는 NAVER WORKS 서비스의 보안성, 가용성, 처리무결성, 기밀성, 개인정보보호와 관련된 서비스 책임과 시스템 요구사항을 달성하였다는 합리적인 확신을 제공하기 위해 2020년 1월 1일부터 2020년 12월 31일까지의 기간에 대하여 시스템 내 통제를 효과적으로 설계, 구현, 운영 및 유지할 책임이 있습니다. 우리는 우리의 주장이 다루는 시스템의 범위에 대하여 "Section III: NAVER WORKS 서비스 시스템의 범위에 대한 기술서"(이하 '기술서')에 표시하였습니다.

우리는 미국공인회계사회가 제정한 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 웍스모바일의 서비스 책임과 시스템 요구사항이 달성되었다는 합리적인 확신을 제공하기 위해 2020년 1월 1일부터 2020년 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.

모든 내부통제 체계는 인적 오류, 통제를 우회할 가능성 등을 포함하여, 효과성에 대한 본질적인 한계(이하 '고유한계')를 지니고 있습니다. 이러한 고유한계로 인해, 회사는 서비스 책임과 시스템 요구사항이 달성되었다는 절대적인 확신이 아닌 합리적인 확신을 달성할 수 있습니다.

우리는 웍스모바일의 서비스 책임과 시스템 요구사항이 해당 트러스트 서비스 준거기준에 따라 달성되었다는 합리적인 확신을 제공할 수 있도록 시스템 내 통제가 2020년 1월 1일부터 2020년 12월 31일까지의 기간 동안 효과적이었다고 주장합니다.

Section III: NAVER WORKS 서비스 시스템의 범위에 대한 기술서

1. 개요

회사 소개

웹스모바일 주식회사(이하 '웹스모바일' 또는 회사)는 2011년 출시된 네이버 메일 개인 도메인서비스를 기반으로 2012년 "네이버웍스" 서비스를 제공하기 시작하였습니다. 회사는 2015년 4월 글로벌 기업형 서비스 시장으로 본격 진출을 위해 네이버로부터 분사하였으며, 일본 시장 진출을 위해 2015년 6월 일본 법인(WORKS MOBILE Japan Corp)을 설립하였습니다.

회사로는 기업형 메신저, 음성/영상통화, 메일, 드라이브, 캘린더, 홈(게시판), 설문, 주소록, 모니터링 등 다양한 기능으로 구성된 기업형 협업/커뮤니케이션 서비스인 NAVER WORKS 를 주요 서비스로 제공하고 있습니다. 기업이나 단체들은 클라우드(Cloud)환경으로 제공되는 회사의 서비스를 통해 스마트 오피스를 구현할 수 있습니다. NAVER WORKS 서비스는 PC, 스마트폰, 태블릿 등 다양한 디바이스로 접근 및 이용이 가능하며, 기업 내 임직원의 협업/커뮤니케이션 서비스 외에도 기업 내 관리자들을 위한 구성원 관리, 보안 설정, 서비스 통계, 감사, 메일 송수신 모니터링 등의 관리자 기능을 제공합니다.

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 시스템기술서에서 포함하는 서비스는 다음과 같습니다.

- NAVER WORKS - 기업형 메신저, 메일, 드라이브, 캘린더, 주소록 등 다양한 기능으로 구성된 기업 내 임직원의 협업/커뮤니케이션 서비스 외에도 기업 내 관리자들을 위한 구성원 관리, 보안 설정, 서비스 통계, 감사, 메일 송수신 모니터링 등의 관리자 기능을 제공합니다.

서비스 이용자는 회사의 서비스를 안전하고 올바르게 이용하기 위하여, 서비스 이용약관의 '회원의 의무'를 준수해야만 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 NAVER WORKS 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 데이터센터는 화재, 지진, 홍수 등 재해로부터 보호하기 위하여 화재감지기, 소화설비, 무정전 전원장치(UPS), 항온항습기, 누수탐지기 등 보호설비를 운영하고 있습니다.

소프트웨어

서비스를 제공하기 위한 어플리케이션을 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.

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.

절차

회사는 보안성, 가용성, 처리 무결성, 기밀성 그리고 개인정보보호 원칙을 준수하기 위하여 정책, 지침, 가이드라인 등 정보보호 규정을 마련하고 있으며, 각 규정은 관련 법령의 요구사항 변화에 따라 주기적으로 모니터링되고, 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.

Section IV: 주요 서비스 책임과 시스템 요구사항

회사는 이용자에게 NAVER WORKS 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 사용자에게 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 NAVER WORKS 서비스와 관련된 시스템을 운영하거나 개발하는데 있어 필요한 수작업 및 자동화된 세부 절차의 수행 방법을 표준 운영 절차에 명시하고 있습니다.