오픈마켓 판매자 싸이트 2 차 인증제도 운영방안

송영규
고려대학교 컴퓨터정보통신대학원
svv0708@korea.ac.kr

Operation Plan of 2nd Certification System for Seller Site in Open Market

Song Young Gyu
Korea University Graduate School of Computer & Information Technology

요 약

본 논문에서는 오픈마켓 개인 판매자의 개인정보 취급에 있어 개인정보 보호 강화를 위해 판매자 싸이트 로그인 시 2 차 인증 필요성에 대한 법적 준거성을 분석하고 이에 대한 기술적 방안을 제시한다.

1. 서론

최근 코로나 19 의 영향으로 온라인쇼핑 거래 증가에 따라 오픈마켓의 시장규모도 대폭 상승했다.[1]

(그림 1) 2021 년 1 월 온라인쇼핑 동향[2]

오픈마켓이란 다수의 개인 판매자가 직접 상품을 올려 전자 상거래가 이루어지는 곳을 뜻한다. 오픈마켓에선 다수의 개인 판매자가 고객의 개인정보를 처리하기에 개인정보 해킹, 유출 등 많은 위협에 노출되어 있다.

판매자 전용 싸이트에선 상품 등록, 주문 확인, 배송 등을 처리함과 동시에 많은 개인정보가 처리된다. 따라서 각별한 관리가 필요한 싸이트이며, 그에 대한 방안 중 싸이트 로그인 시 2 차 인증 수행이 있다.

본 연구에서는 오픈마켓 판매자 싸이트 로그인 시 2 차 인증제도 운영방안에 대해 법적 준거성 및 기술적 방안을 소개한다.

2. 법적 준거성

2.1 개인정보 보호법

제 2 조(안전조치의무)개인정보처리자는 개인정보가 분실・도난・유출・위조・변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적・관리적 및 물리적 조치를 하여야 한다.

2.2 개인정보 보호법 시행령

제 48 조 2(개인정보의 안전성확보 조치에 관한 특례)
① 정보통신서비스 제공자와 그로부터 이용자의 개인정보를 법 제 17 조제 1 항제 1 호에 따라 제공받은 자는 이용자의 개인정보를 처리하는 경우에는
제 30 조에도 불구하고 법 제 29 조에 따라 다음 각 호의 안전성 확보 조치를 해야 한다.
③ 제 1 항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

2.3 개인정보의 기술적 · 관리적 보호조치 기준

제 4 조(접근통제) ④ 정보통신서비스 제공자 등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용하여야 한다.

2.4 개인정보의 기술적 · 관리적 보호조치 기준 해설

안전한 인증 수단이란 사용자계정과 비밀번호를 입력하여 사용자 식별. 인증하는 절차 이외에 추가적인 인증 수단의 적용을 말한다.[3]

3. 기술적 방안

사용자 ID 와 비밀번호를 통한 1 차 인증 후 추가적 2 차 인증 수단에 대한 연구를 진행했다.

2.1 전자서명

전자서명이란 HASH 값을 서명자의 개인키로 암호화 작업을 통해 서명한 사람의 신원 및 위변조 사실을 알 수 있는 특수한 형태의 디지털 정보를 말한다. 인증서는 공인인증기관에서 발급 받을 수 있으며, 서명 과정에서 신뢰성 있는 제 3 자를 통한 검증이 이루어 진다는 점에서 명확한 신원 증명이 이루어 진다는 점이 장점이다. 하지만 PC 에 인증서를 설치 해야하며 별도의 발급 과정이 필요하다는 점이 단점이다.

2.2 핸드폰 인증

판매자 회원 가입 당시 본인 인증한 핸드폰으로 임의의 문자를 포함한 SMS 를 송신하여 판매자로부터 해당 문자를 입력 받는 방식이다. 이는 핸드폰이라는 점유 기반의 매체를 통해 본인을 확인하는 방식이며, 진행 방식이 간편하고 누구나 소유하고 있는 휴대폰을 이용하였기에 별도의 기기를 소지할 필요가 없다.

추가적인 별도 과정 없이 사용할 수 있다는 장점이 있지만 핸드폰 분실 및 미 소지에 대한 추가 대체 방안이 필요하다는 단점이 있다.

2.3 일회용 비밀번호(OTP)[5]

일정 시간 동안 1 회에 한해 사용할 수 있는 핀 코드 번호로 타 인증 수단과 달리 유출에 대한 위험이 적은 방안이다. 코드 번호를 만드는 방식으로는 현재 시간을 입력 값으로 하는 시간 동기화 방식, 서버에서 난수를 생성하여 전송해주는 챌린지/응답 방식, 서버와 클라이언트가 카운트 값을 증가시켜 해당 값을 입력 값으로 사용하는 이벤트 동기화 방식 등이 있다.

생성된 코드 번호는 사용자에게 전달하기 위해선 별도의 장치가 필요하다. 스마트폰 앱을 통해 코드 번호를 전달할 수 있으며 추가 비용이 없다는 점이 장점이다. 하지만 다양한 스마트폰 환경에서 해킹의 위험에 노출이 되어 있단 것이 단점이다.

2.4 생체 인증[6]

생체 정보를 사전에 취득하고 추후 인증 할 때 센서를 통해 취득한 정보와 비교를 통해 본인 확인이 이루어진다. 최근 휴대폰 기기에서 홍채, 지문, 얼굴에 대한 인식 기능을 탑재하고 있기에 용이하게 사용될 수 있는 방식이다. 하지만 선천성 결손 등으로 인해 생채 인식이 불가능 한 사람을 위한 대안이 필요하다. 또한 생체 정보는 변경이 불가능하기에 해당 정보가 복제되어 유출 시 안전성을 회복할 수 없다는 것이 단점이다.

4. 결론

통계청의 발표에 따르면 온라인 쇼핑 거래액이 2021 년 1 월 기준 15 조 623 억원으로 작년 1 월 대비 22.4% 늘어났다고 한다. 스마트폰 이용 증가와 비대면 거래에 대한 고객의 만족스러운 경험을 기반으로 향후 더욱 시장 규모가 커질 것으로 예측된다. 이에 따라 오픈마켓의 시장 규모 역시 증가할 것이다. 이러한 흐름에서 개인 판매자의 개인정보 취급에 있어 개인정보 보호는 중요한 의미를 내포한다. 특히 주문을 처리하는 장치들이 전국에 산발적으로 분포하고 있고 각기 다양한 환경에서 업무를 처리함과 주문 정보가 실시간 정보이기에 유출 및 해킹에 대한 위험도가 상당히 높고 중앙 통제의 불가능함은 제 2 의 피해로 이어질 가능성이 높다.

본 논문에서는 오픈마켓 개인 판매자가 사용하는 판매자 싸이트 로그인 시 2 차 인증에 대한 법적 준거성과 그에 대한 기술적 방안을 도출하였다.

먼저 개인정보 보호법에 적용 받아 주문 데이터를 처리하는 판매자 싸이트를 개인정보 처리시스템으로 인식하고 외부에서 판매 회원의 접근 시 안전한 인증 수단을 적용해야 할 의무가 있다.

이러한 관점에서 다음과 같은 기술적 방안을 제시하였다. 첫째, 공인인증기관에서 발급받은 인증서 형태의 전자서명이다. 둘째, 핸드폰에 수신한 SMS 내 임의의 문자를 입력하는 방식이다. 셋째, 스마트폰 앱을 통한 일회용 비밀번호를 입력하는 방식이다. 넷째, 스마트폰 내 생체 인증 기능을 이용한 인증 방식이다. 해당 방안 중 한가지를 채택하여 사용자 계정 및 패스워드 인증과 더불어 2 차 인증 수단으로 사용이 필요하다.

참고문헌

[1] 매일경제, ”네이버 '네이버쇼핑', 스마트스토어 42 만개…거래 폭증”, 2021.4.14 자

[2] 2021 년 1 월 온라인쇼핑 동향, 통계청, 2021.3, 1 쪽

[3] 개인정보의 기술적관리적 보호조치 기준 해설서, 개인정보보호위원회 한국인터넷진흥원, 2020.12, 48 쪽