2016. 1. 6.
전명훈

# HTTP/HTTPS 및 공인인증서

## HTTP / HTTPS - HTTP와 HTTPS는 무엇이며 그 차이는?

HTTP는 Hyper Text Transfer Protocol의 약자이며 WWW상에서 정보를 주고받는 규약이다. 웹에서는 주로 HTML문서를 사용하므로, HTTP도 주로 HTML 문서를 주고 받는데 사용된다. TCP/IP를 주로 사용하는데, 포트 번호는 80번이다.

HTTP는 클라이언트와 서버 사이에 이루어지는 요청/응답(request/response)에 대한 규약이다. 요청 방법으로는 GET(URL에 해당하는 자료의 전송을 요청)/POST(서버가 처리할 수 있는 자료를 보냄)/PUT(해당 URL에 자료를 저장)/DELETE(해당 URL의 자료를 삭제) 등이 있다.

HTTPS(Hypertext Transfer Protocol over Secure Socket Layer)는 HTTP의 보안상의 약점을 보완한 통신 프로토콜로, 소켓 통신에서 일반 텍스트의 형식으로 데이터를 주고 받는 것이 아니라, SSL이나 TLS 프로토콜을 통해 세션 데이터를 암호화해 통신한다. 기본 TCP/IP 포트는 443이다.

## 공인인증서 - 국내에 공인인증서가 생긴 배경과 그 이유는?

공인인증서란 쉽게 말해 전자 인감도장이다. 우리나라에는 '이 도장이 내 도장이다'고 관공서를 통해 정식으로 인증받는 '인감(印鑑)'이라는 독특한 제도가 있다. 공인인증서는 이 인감을 웹으로 옮겨둔 제도다. 사용자가 인터넷 상에서 한 거래를 '이 거래는 내가 승인한 거래다'고 인증해주는 기술이다.

공인인증서 역시 초창기 열악한 인터넷 환경에서 어떻게든 인터넷뱅킹과 전자상거래를 구현하기 위해 고안해낸 기술이다. 플러그인과 비슷하다.

초기 웹 브라우저는 암호화 능력이 부족해 해커가 중간에서 데이터를 가로채기 쉬웠다. 암호화 전송기술 자체가 없는 것은 아니었다. 넷스케이프 그룹이 95년 고안해낸 SSL(Secure Socket Layer, https)라는 기술이 암호화 전송기술 표준으로 각광받았다. 하지만 미국 정부의 기술유출불가방침 탓에 인터넷뱅킹을 구현하기엔 암호화 수준이 모자랐다. 때문에 독자적인 암호화 기술인 SEED[1]을 적용한 공인인증서를 개발해냈다. 그리고 플러그인인 active X를 사용해 공인인증서를 웹 브라우저에 적용하기 시작했다.

## 위 내용을 조사하며 느낀 점

인터넷뱅킹 구현에는 암호화 전송기술/사용자 인증/OTP 사용이 필요하다. 해외에서는 SSL로 암호화(=https)되어 있는 웹 페이지에서 제3자 인증을 통해 쉽게 보안과 암호화 정도를 브라우저로 확인가능하다. 웹 표준 기술이기 때문인데 우리나라에서는 웹 표준 규정을 지키는 곳이 드물어 공인인증서라는 번거롭고, 보안성이 떨어지는 방식(3자인증의 부족으로 피싱등의 사기에 취약함)을 채택하고 있다는 점이 아쉽다.

[1] 1회차 과제 중 active X 및 SEED 관련 부분 참고. http://it.donga.com/17704/ 기사 참고

2016. 1. 6.
전명훈