**FTP와 SFTP의 개요**

**1. FTP (File Transfer Protocol)**

* **정의**: FTP는 파일을 전송하기 위한 통신 규약으로, 주로 인터넷을 통해 파일을 주고받을 때 사용됩니다. 기본적으로 21번 포트를 사용하며, 보안이 취약한 것으로 알려져 있습니다.
* **포트 사용**:
  + 명령어 전송에 21번 포트를 사용하고, 데이터 전송에는 20번 또는 랜덤 포트를 사용합니다.
* **운영 모드**:
  + **액티브 모드**: 클라이언트가 서버에 포트 번호를 전달하여, 서버가 해당 포트를 통해 클라이언트와 데이터를 주고받습니다.
  + **패시브 모드**: 서버가 클라이언트에 포트 번호를 전달하고, 클라이언트가 해당 포트를 통해 서버와 데이터를 주고받습니다.
* **단점**: FTP는 암호화되지 않은 평문(plain text) 통신을 사용하므로, 패킷 캡처 공격에 취약하여 민감한 정보(예: 비밀번호)가 쉽게 노출될 수 있습니다.

**2. SFTP (SSH File Transfer Protocol)**

* **정의**: SFTP는 SSH를 기반으로 한 파일 전송 프로토콜로, FTP의 보안 문제를 개선한 버전입니다. 22번 포트를 사용하며, **모든 데이터가 암호화된 상태로 전송됩니다.**
* **특징**:
  + FTP와는 달리, SFTP는 SSH의 확장 프로토콜로 설계되었으며, 안전한 파일 전송을 보장합니다.
  + 일반적인 FTP와 달리, SFTP는 PC와 서버 간의 데이터 전송을 암호화하여 보안 문제를 방지합니다.
* **장점**: SFTP는 파일 전송 시 데이터가 암호화되므로, 해킹이나 보안상의 문제를 방지할 수 있습니다. 또한, 안전한 호스팅 서비스를 이용할 수 있습니다.

**FTP와 SFTP의 비교**

* **보안성**:
  + **FTP**: 보안이 취약하며, 평문으로 데이터를 전송하므로 패킷 캡처 공격에 민감합니다.
  + **SFTP**: SSH를 기반으로 하여 모든 데이터가 암호화되므로, 해킹에 대한 보호가 가능합니다.
* **사용 사례**: FTP는 주로 보안이 크게 요구되지 않는 환경에서 사용되지만, SFTP는 보안이 중요한 파일 전송에 사용됩니다.
* **프로토콜 설계**:
  + **FTP**: 오랜 전통의 파일 전송 프로토콜로, 보안 기능이 내장되어 있지 않습니다.
  + **SFTP**: SSH 기반의 파일 전송 프로토콜로, 처음부터 보안 기능을 염두에 두고 설계되었습니다.

**기타 관련 프로토콜**

* **FTPS**: FTP가 TLS/SSL 보안 연결에서 동작하는 방식으로, 'implicit'와 'explicit' 모드로 구분됩니다.
* **SecureFTP (FTP/SSH)**: SSH 연결 위에서 일반 FTP로 접속하지만, 데이터는 암호화되지 않는 방식입니다.

**결론**

* **FTP**는 파일 전송에 있어 오래된 표준이지만, 보안상의 취약점이 있습니다.
* **SFTP**는 SSH를 기반으로 하여 보안을 강화한 파일 전송 프로토콜로, 현재는 많은 환경에서 FTP 대신 사용되고 있습니다.
* 보안이 중요한 경우 SFTP를 사용하는 것이 좋습니다.