httpと https

JJ1SXA/池

Web サイトの URL の最初の文字は、ほとんどが、http か https だ、http は、「Hyper Text Transfer Protocol」の略で、今やインターネットの代名詞となった WWW(World Wide Web)上で Web サーバとクライアントが、html で書かれた文書などの情報をやりとりする時に使われるプロトコル(通信手順)を意味します、html は「Hyper Text Markup Language で Web ページを記述するための言語」です。

http ではデータが暗号化されていないため、 通信経路のどこかで内容を知られる可能性があります、 第三者に知られたくない情報をやりとりする時は、別途暗号化を行うか、 暗号化された https という通信手順を使う必要があります。

https は、「Hyper Text Transfer Protocol Secure(ハイパーテキスト トランスファープロトコル セキュア)」で、http に Secure(セキュア)の「S」を追加したものです。

https は、データのやりとりをセキュア(暗号化)な状態で通信していますよ、ということで、URL の前に「鍵マーク」がついて、次のように表示されます、「🔒 “https:…”」、一方、http の場合は、URL の前に Edge では「⚠ セキュリティ保護なし “http:…”」というように表示されます、Chrome では、「⚠ 保護されていない通信 “http:…”」と表示されます、ちなみに 240 のホームページは、「🔒 https://240sxa.net/…」と、暗号化された表示をされています、余り知られていないようですが…

SSL(Secure Sockets Layer)と TLS(Transport Layer Security)は、いずれもインターネット上でデータを暗号化して送受信する仕組み(プロトコル)で、個人情報やクレジットカード情報などの重要なデータを暗号化して、サーバと PC 間での通信を安全に行なうことができますということです。(共通鍵暗号方式と公開鍵暗号方式の両方を用いて、データの暗号化と復号を実施)

SSL でデータを暗号化することで、「盗聴」、「改ざん」、「なりすまし」等のサイバー攻撃を防げますとのこと。

現在は「TLS1.3」までリリースされていますが、SSL3.0 と TLS1.0 は、仕様の違いもごくわずかで仕組みがほぼ同じですが、TLS が登場した段階では既に SSL という名称が広く使われていたため、現在では「TLS のことも含めて SSL と呼ぶ」又は「SSL/TLS」、「TLS/SSL」のような併記で使われる事が多いようです。

SSL/TLS のこれまでの歩みですが、SSL1.0 はリリース前に脆弱性が発見され公開されず、SSL2.0 が 1994 年リリース、SSL3.0 が 1995 年リリース、TLS1.0 が 1999 年リリース TLS1.1 が 2006 年リリース、TLS1.2 が 2008 年リリース、TLS1.3 が 2018 年リリースと、バージョンアップされました。 (2024 年 9 月記)

注:この記事は、TWO-FORTY 誌第 120 号に投稿するべく、昨年 9 月に書いたものですが、PCの不調で、一時行方不明になっていたものです。