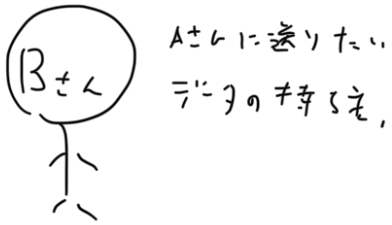
暗号化方式

① Secret key と Public key

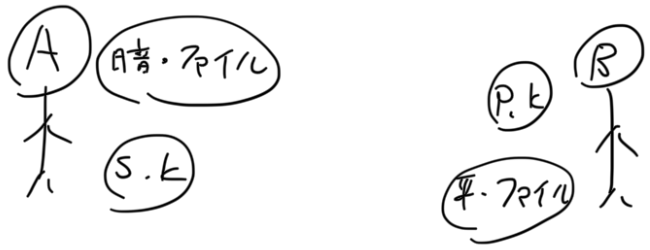


Step 1: Aさんが Secret key (S.k) を使って Public key (P.k) を生成

Step 2: Bさんが Aさんの P.k を取得

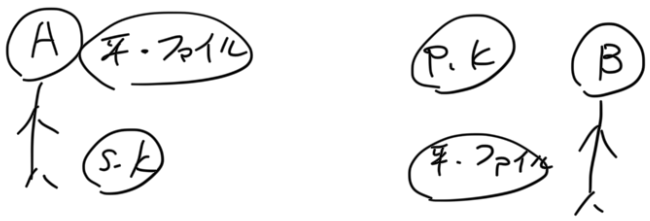
Step 3 : Bさんが 取得した P.k で ファイルを 暗号化

Step4 : Bさんが暗号化されたファイルをAさんに送る。



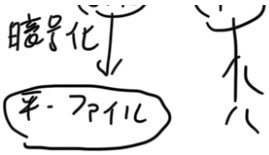
Step5 : Aさんが S.K で 暗号化されたファイルを 平文化する

Step6 : Aさんは Bさんのファイルの平文を確認できる

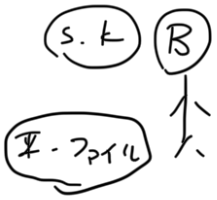


② Shared key

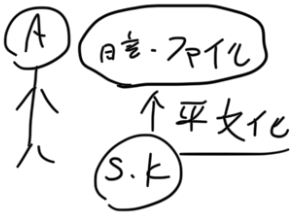
Step1 : Bさんは shared key (S.K) でファイルを暗号化する

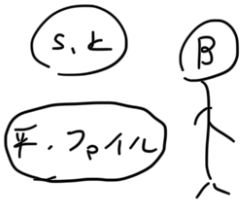


Step2：Bさんは暗号化したファイルをAさんに送る

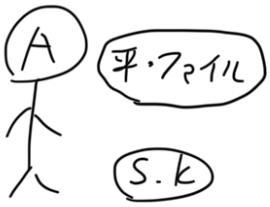


Step3：Aさんは S.K で暗号化されたファイルを平文化する





Step4：Aさんは平文化されたファイルにアクセスできる



☆ 各暗号化方式の pros & cons

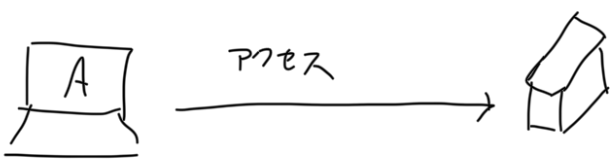
Secret	

	Public key	Shared key
Pros	・安全性が高い Secret key を持つ人だけが平文化できるため、	・安全性が低い ⇒ shared key が流出したら誰でも暗号化されたファイルを平文化できてしまう。
Cons	・暗号化/復号化の処理に時間がかかる	・処理に時間がかからない

③ SSL (Secure Sockets Layer)

上記の、②の暗号化方式を利用した通信のこと。

Step1: PCAが、とあるWebページにアクセス



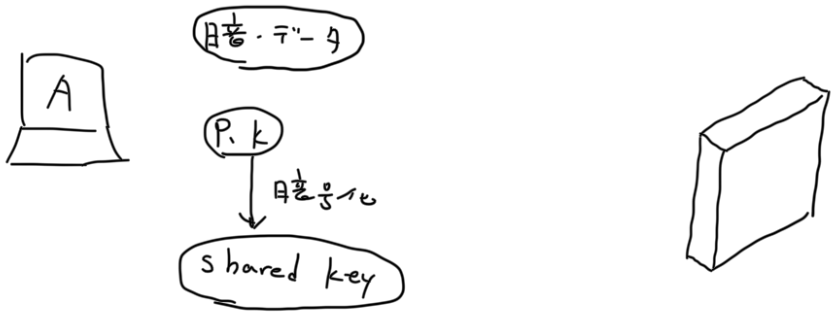
Step 2: サーバーからSSL証明書が送られてくる

Step 3: PC・Aがssl証明書からpublic keyを生成

Step4: PC・Aは shared keyを生成する

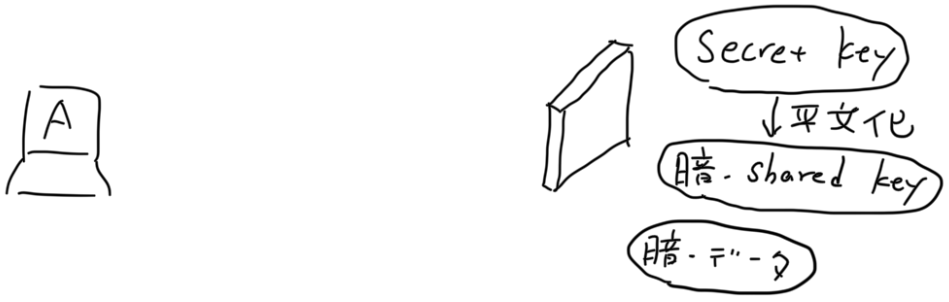
Step5: PC・Aは shared keyでデータを暗号化する。

Step 6 : PC-A は shared key を Public key で暗号化する

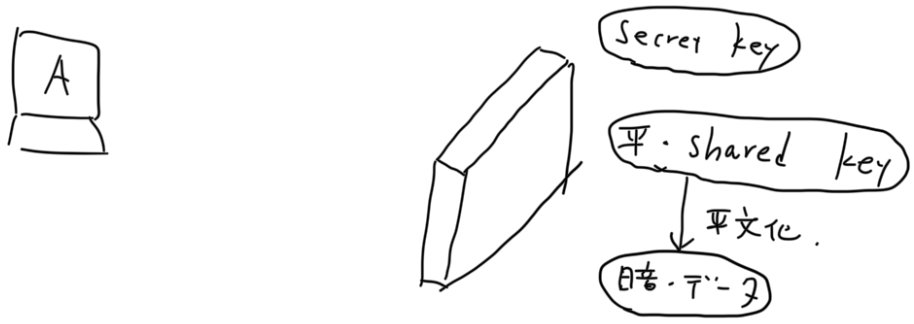


Step 7 : PC-A は 暗号化 された データ と shared key を
サーバー に送る

Step 8 : サーバー 側は、Secret key で 暗号化された shared key
を平文化する



Step 9: サーバー側は、さらに、平文化された Shared key を使って
暗号化されたデータを平文化する。



これで サーバー は、ユーザーのデータにアクセスできる。

ポイント

(i) ユーザーデータを 暗号化/平文化するのは Shared key
→ 暗号化/復号化の処理時間が短かい。

(ii) Public / Secret key で暗号化された Shared key を
暗/復号化する。

→ 安全性が高い。
暗/復号化するのは shared key だけなので、処理時間は短くてすむ。