共通鍵暗号（例：AES）

AESとは、無線LANなどの通信データの暗号化に用いられる暗号化アルゴリズムです。「Advanced Encryption Standard」の略で、日本語に訳すと「先進的暗号化標準」となります。NIST（米国国立標準技術研究所）が公募の結果採用した暗号化技術で、2001年に承認されて以来、現在に至るまで標準的に使われ続けています。

AESは共通鍵暗号です。

共通鍵暗号では、データの送信者と受信者が同じ暗号鍵を用いて、暗号化と復号を実行します。AES以前にはDESという共通鍵暗号が広く使われていました。

しかし、鍵長が短いなどの難点があり、時代とともに新しい暗号化アルゴリズムが求められるようになりました。そして選ばれたのがAESで、DES以上の強度を持ちます。

３種類の鍵長を利用できる

DESの難点の１つは、鍵長が56bitと短く総当たり攻撃に弱いことでした。この弱点を補うために２DESや３DESが登場しましたが、これらには別の攻撃に弱いなどの弱点が見つかったのです。そのため、鍵長が長く、根本的に問題を取り除ける方法が求められました。

DESの後継的存在として、AESは登場しました。AESでは128・192・256bitの中から鍵長を選んで利用可能です。

また、最大の特徴として４種類の変換を行う点があります。

- ■SubBytes
- ■ShiftRows
- ■MixColumns
- ■AddRoundKey

以上４つの処理を経て、最終的に「128・192・256bit」いずれかの鍵長に合わせた暗号鍵に変換されます。

この工程を複数回繰り返すことで、暗号セキュリティの強度は高まります。

主にWPA２などの通信で使われている

WPA２とは無線LANの通信を保護するための規格です。この規格では、最大256bitの鍵長を利用できる強固な暗号化アルゴリズムとしてAESが採用されています。

そのほか、AESはSSL/TLS化通信やファイルの暗号化など、身近なところで使われています。

AESとほかの暗号アルゴリズムの違い

AESは、DESやRC４といったほかの暗号アルゴリズムとどう違うのでしょうか。

AES通信データを区切り、置き換え・並べ替えのセットを複数回繰り返すアルゴリズム。最もセキュリティが強固。DES/３DES一定量のデータをブロック単位で暗号化するアルゴリズム。一つのブロックの長さ（鍵長）は56bitと短く、安易に傍受されてしまう。RC４ブロックの長さ（鍵長）を自由に設定できるアルゴリズム。逐次暗号化するストリーム暗号。簡単にセキュリティを突破されてしまう。

詳しくはリンク元で。

https://it-trend.jp/encryption/article/64-0070

AESを使う方法

AESは無線LANやSSL通信、ファイル暗号化などで使われています。ここではファイル暗号化におけるAESの使い方を見ていきましょう。

AESによるファイルの暗号化は、暗号化ソフトを使うことで可能です。ファイル単位で暗号化するものもあれば、ストレージやHDDを丸ごと暗号化できる製品もあります。

無料の暗号化ソフトにも、AESで簡単にファイルを暗号化できるものがあります。

たとえば、Web上でテキストを入力するだけで、暗号化テキストファイルとして出力するソフトが存在します。メールに添付したりUSBなどの携帯メディアに保存したりする前に暗号化すれば、安全性が高まるでしょう。

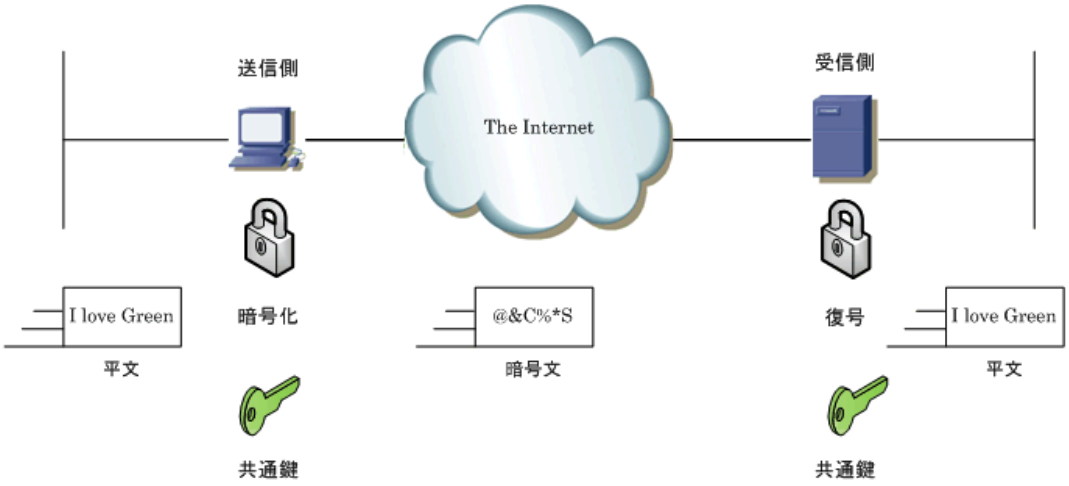
一方、企業ではストレージやHDDを暗号化するソフトが導入されるケースも多いです。専用の鍵がなければ中のファイルを閲覧できないため、物理的な盗難や不正アクセス対策として利用されています。

https://www.infraexpert.com/study/security4.html

共通鍵暗号

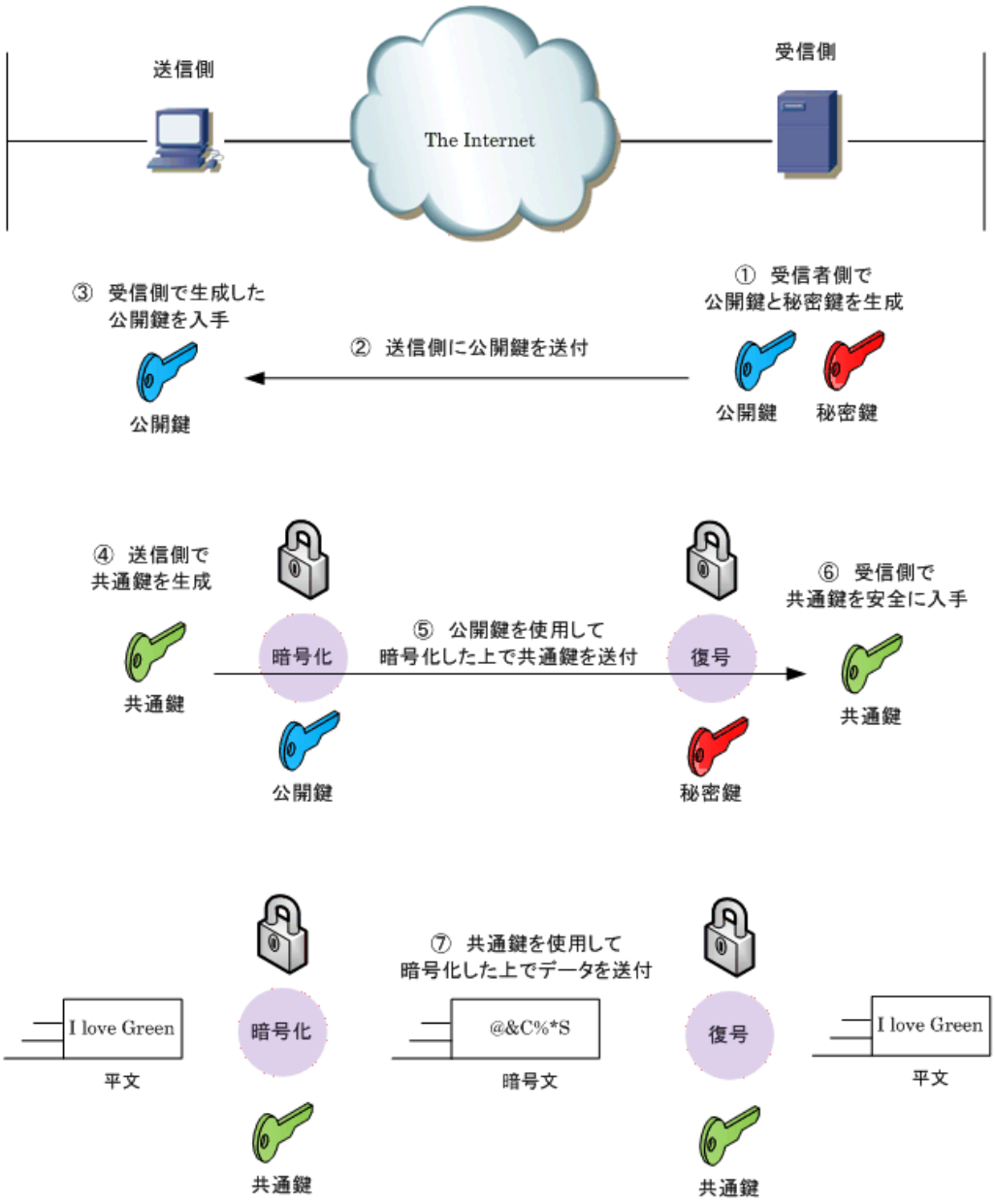
共通鍵暗号では、暗号化と復号に同じ鍵を使用します。共通鍵暗号で使用するアルゴリズムには「RC4、DES、3DES、AES」などがあります。

共通鍵暗号では通信接続先ごとに共通鍵を生成する必要があり、また、鍵交換を盗聴されないよう安全に行う必要があります。



共通鍵は安全に渡さないと行けないので、安全に行うためにハイブリッド方式が用いられる。

ハイブリッド方式


送信側
The Internet
受信側
③ 受信側で生成した
公開鍵を入手
② 送信側に公開鍵を送付
① 受信者側で
公開鍵と秘密鍵を生成
公開鍵
公開鍵
秘密鍵
④ 送信側で
共通鍵を生成
暗号化
⑤ 公開鍵を使用して
暗号化した上で共通鍵を送付
復号
⑥ 受信側で
共通鍵を安全に入手
共通鍵
公開鍵
秘密鍵
共通鍵
⑦ 共通鍵を使用して
暗号化した上でデータを送付
I love Green
暗号化
@&C%*S
復号
I love Green
平文
暗号文
平文
共通鍵
共通鍵

暗号化方式	共通鍵暗号	公開鍵暗号
暗号化アルゴリズム	RC4、DES、3DES、AES	RSA、ElGamal
使用する暗号鍵	共通鍵	公開鍵、秘密鍵
鍵の管理	通信接続先ごとに作成	通信接続先の数に関係なく１つだけ作成
鍵の交換	第三者に知られないよう安全に交換	作成した公開鍵を一般に公開
データの処理時間	速い	遅い

※　共通鍵暗号の共通鍵と、IPsec-VPNで使用するPre-shared key（事前共有鍵）は全くの別ものです。混同しないように！

引用元

https://it-trend.jp/encryption/article/64-0070

https://www.infraexpert.com/study/security4.html