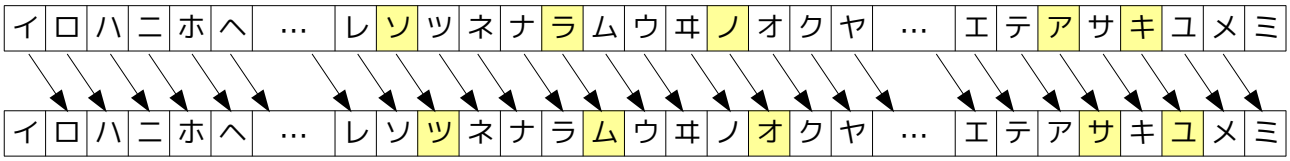
暗号

はじめに、言葉をいくつか決めておきましょう。

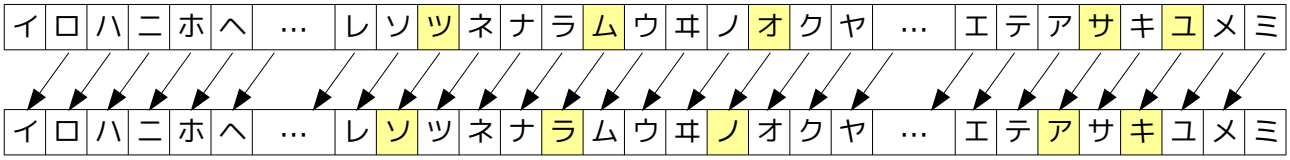
暗号は、相手にだけ内容が伝わり、他の人には内容が分からないようにする工夫です。たくさんの工夫がありますが、よく使われるのは文字を置き換えるやりかたです。

そのような暗号の一つの例として、**アキノソラ**という通信文を 1 文字ずつ、イロハニホヘトの順序でひとつ後の仮名に置き換えてみます。最初の**ア**は**サ**に置き換えます。次の**キ**は**ユ**に置き換えます。



その結果の暗号文は**サユオツム**になりました。これを相手に送ります。

相手は届いた**サユオツム**をイロハの順序でひとつ前の仮名に置き換えると**アキノソラ**に戻ります。



ここでアキノソラのことを**平文**（ひらぶん）といいます。人間が読んでもわからないサユオツムを**暗号文**といいます。平文を暗号文に変える操作を**暗号化**、暗号文を平文に戻す操作を**復号**といいます。

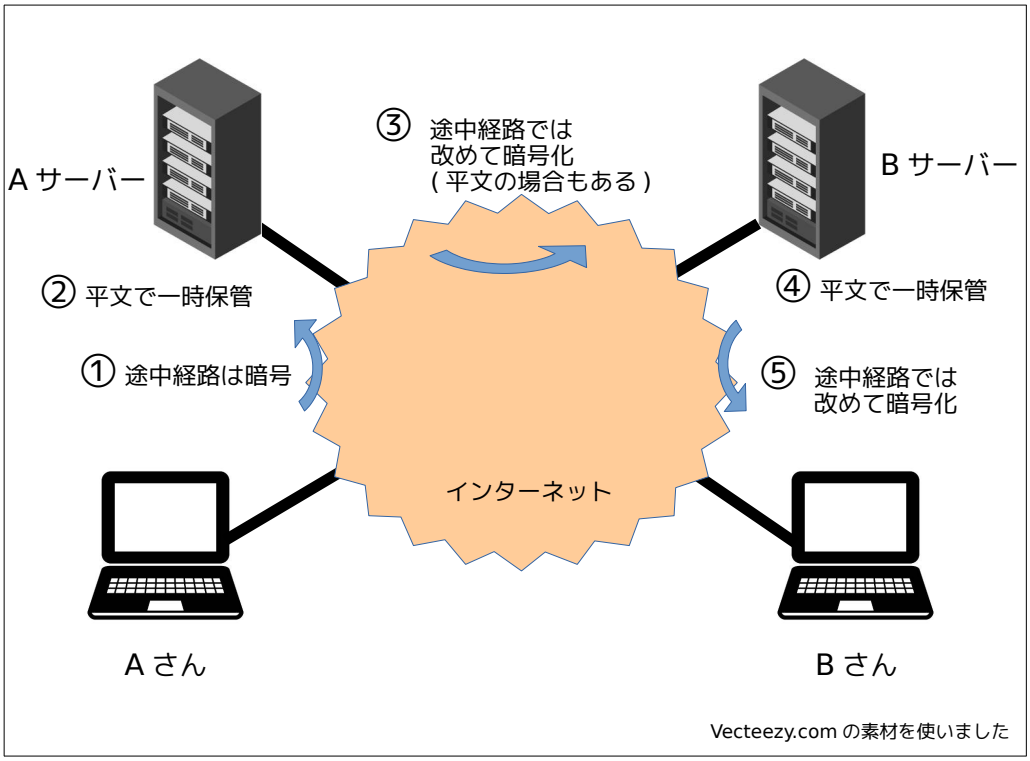
イロハ暗号が役に立つためには、送る人と受ける人とで「イロハで 1 文字あとへ」という約束をしておく必要があります。「イロハで」のことをここでは**暗号方式**とでも呼びましょう。「1 文字あとへ」のことを**鍵**（かぎ）と呼びます。

ことばの紹介はこのぐらいにしておきましょう。

> **共通鍵暗号・公開鍵暗号**
>
> 共通鍵暗号と公開鍵暗号はとりあえず別物です。さきほどの「イロハ 1 文字あとへ」は、暗号化する時の鍵「1 文字あとへ」と解読するときの鍵「1 文字前へ」とが（ほとんど）同じものなので、**共通鍵**暗号と言ってよさそうです。たとえほとんど同じとまでいえなくても、片方から他方を簡単に作れる（計算できる）なら、共通鍵暗号と呼ぶようです。
>
> **公開鍵**暗号は、みんなが知っている公開鍵と、1 人だけが知っている**秘密鍵**とを、うまく使い分けて暗号化が行われます。公開鍵と秘密鍵とは 1 つずつのセットになっているので、みんなが知っている公開鍵は 1 個だけではなく、対応する秘密鍵の数だけあります。A さんの秘密鍵に対応する A さんの公開鍵があって、A さんは公開鍵の方をみんなに知らせておきます。
>
> さて、A さんから B さんに暗号文を送ろうとするとき、A さんは **B さんの公開鍵**を使って暗号化します。この暗号文はもうだれの公開鍵を使っても復号できません。暗号化に使った **B さんの公開鍵**でも復号できないのです。暗号メールを受け取った B さんは**自分の秘密鍵**を使って暗号を解読します。
>
> **OpenPGP** (オープン・ピー・ジー・ピー) は公開鍵暗号のいろいろな処理をするうえでの決まりごと（通信プロトコル）のひとつです。同じ目的に使える S/MIME (エス・マイム) というプロトコルもあります。

メールの暗号化

古い時代のインターネットでは、メールが平文のままでサーバー間やメーラーとの間で転送されていました。これはあまりにも無防備だというので、今では暗号化された状態で転送される方が普通です。つまり通信途中を盗聴しても暗号化されていて中身はわからないのです。しかしメールがサーバー内で次の転送を待っている間は平文で保存されるので、ここから情報が漏れる恐れはあります。



メールを送る・受ける　（非暗号）

ところがメールをエンド・ツー・エンド暗号化する場合は、送信者のメーラーは受信者に合わせてメールを暗号化します。このため通信途中はもちろん、転送途中のメールがサーバーに一時保存されているときも暗号化されたままです。どこから漏洩しても内容は暗号文になっていて、盗聴者が平文に戻すことはできません。（次のページの絵をご覧ください。）

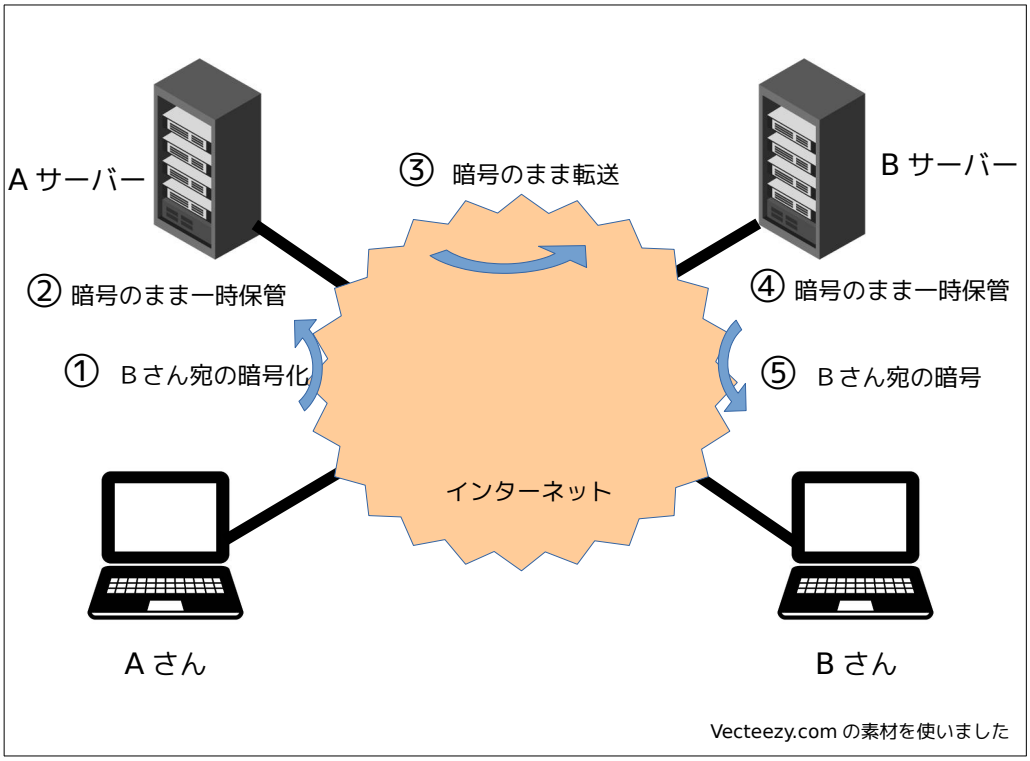
エンド・ツー・エンド

「入口から出口まで」とか「こっちからあっちまで」といった意味です。(「終わりから終わりまで」ではありません。)

> 英語でも end-to-end は少々長いので E2E と略したりします。もちろん イー・ツー・イー と読んでください。イー・に・イー ではワケが分かりません。

メールの場合、E2E 暗号化（E2EE と書いたりもします）は送信する人が thunderbird など自分のメーラーで暗号化を行ない、その暗号文を普通のメールと同じ方法で受信する人へ向けて送ります。インターネットの中を暗号文のままでサーバーからサーバーへ転送されていきます。

受信する B さんは暗号文を受けとると、あらかじめ A さんと申し合わせてあった鍵を使って復号します。



メールを送る・受ける （E2E 暗号）

A さんのところで暗号化したり、B さんのところで解読したりする手順は、メーラーが自動的に済ませてくれます。鍵を作ったり、相手と申し合わせるところも、完全自動ではありませんが手伝ってくれるメーラーもあります。

メタデータ

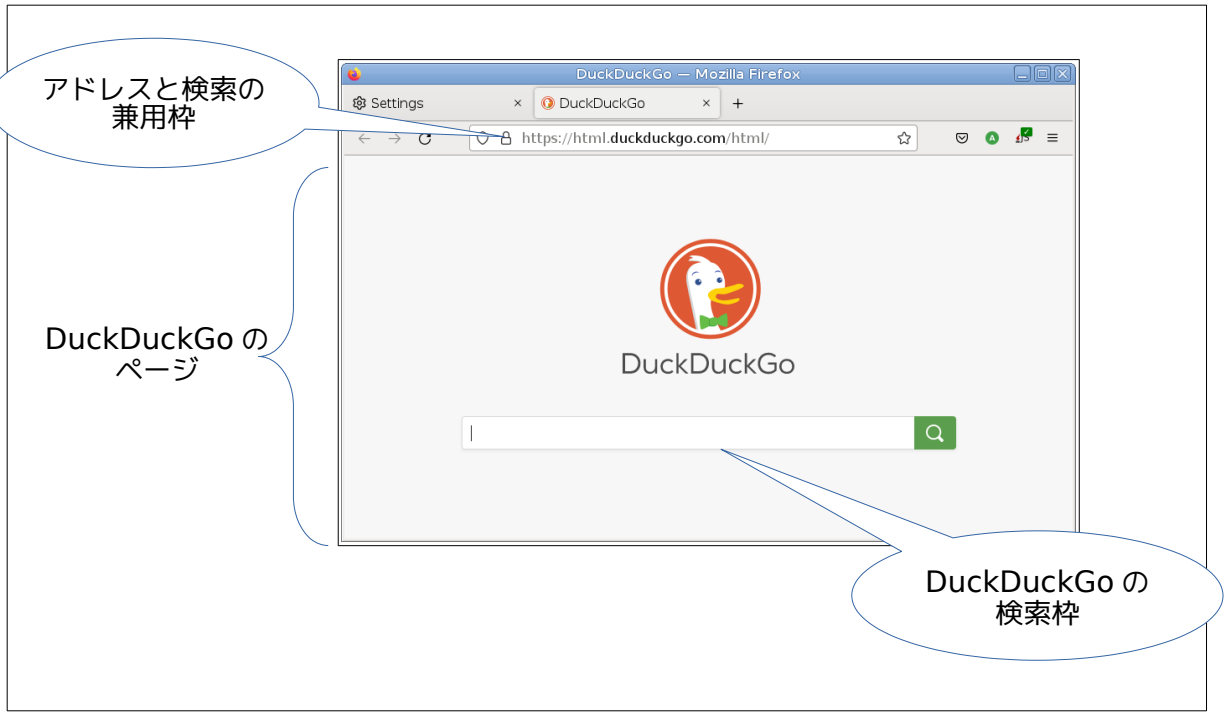
メール本体は暗号化されますが、送信者アドレスや受信者アドレスは、封筒の表書きのようなもので、暗号化されずに扱われます。このメールはいつ、誰が誰に宛てたものかというような中身以外のデータのことを、メタデータと呼びます。中身が暗号化されていてもメタデータだけを大量に集めれば（大量監視）、中身とは別の意味でいろいろな情報が監視者に伝わります。さらにスマホでメールを送受信すれば、どの基地局と通信していたかメタデータとして集められ、ユーザーの所在地がわかります。

数年前までは OpenPGP で暗号メールを送るとき、メールの件名は平文で送られました。今の OpenPGP では件名も暗号で送られます。

ウェブページ（ホームページ）とウェブサーバーとウェブサイト

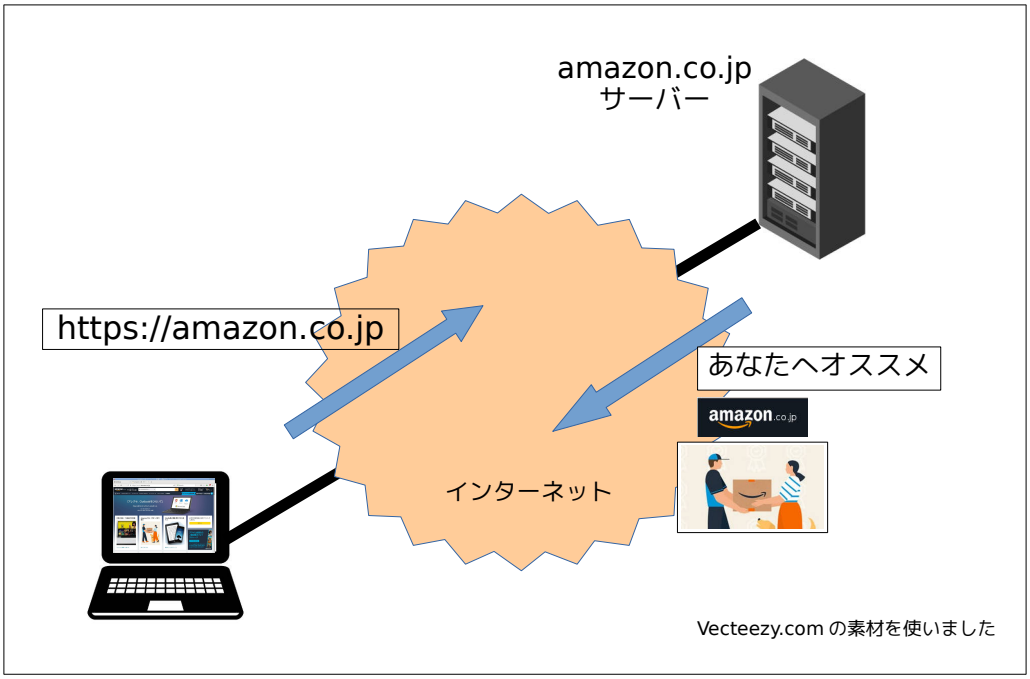
ここでもちょっとだけ用語を整理しておきましょう。

ブラウザ（firefox、Edge、chrome、vivaldi、Safari など）のウィンドウ内に現れるのが**ウェブページ**、あるは略して**ページ**です。ブラウザ窓の上の方には**アドレス枠**や**検索枠**がありますが、下の絵のようにひとつの枠で兼用されることも多いので要注意です。



ブラウザのウィンドウ

アドレスを記入したり、あるいは表示されているページやメールの中で**リンク**をクリックすると、ブラウザはそのアドレスの**ウェブサーバー**に問い合わせを送ります。下の例では、amazon.co.jp というアドレスのサーバーへ問い合わせを送り、サーバーから返信が届いたところです。



アマゾンを表示させる

ウェブの暗号

ウェブサイトとの通信に使われる http プロトコル（通信するための約束事）では、ネット通販でも使えるように比較的早くから暗号化できるようになっていました。暗号通信するときは https というプロトコルを使います。https が有効になっているときはブラウザのアドレス枠に南京錠マークが表示されたり、ブラウザのウィンドウの下端付近に南京錠マークが表示されたりします。

Firefox で暗号通信が確立できたところ

メールとは違ってウェブの場合は通信相手がウェブサーバーだけなので、メールのような E2E 暗号化は不必要です。ウェブサーバーと自分のパソコンとの間の通信経路が暗号化されていれば良いので、https が有効になっていることを確かめれば充分です。

実際には接続先が本物のウェブサイトであることも自動的に確認されています。というのは、暗号通信が成立しても相手がフィッシング詐欺のサイトでは意味がないからです。https では内容を秘密にする暗号化だけでなく、相手サイトの**真正性**が確認できたときに南京錠を表示しています。

TLS/SSL

TLS も SSL も、インタネットの通信を暗号化するときに使われるものらしい、と覚えてください。昔は **SSL** という名前で、Secure Socket Layer だだそうです。Secure（確実) はよく「安全」と誤訳されます。安全でもセキュリティでも暗号とは関係ない言葉ですが、当時の流行に従った名称のようです。

TLS は SSL の後継規格で Transport Layer Security の略語です。インターネットの通信は、様々な役割を担ういくつもの仕組みがあたかも地層のように重なって成り立っています。Transport Layer もそのひとつで、「トランスポート層」とも表現されます。

https の末尾の s は Secure の意味です。https では SSL や TLS で暗号化されたデータが送られます。

実際の暗号化の仕組みは公開鍵と共通鍵を組み合わせている（やや立ち入った説明）

暗号化では公開鍵暗号と共通鍵暗号を組み合わせるハイブリッド暗号化が用いられることがあります。たとえば、メーラーへ暗号化を指示するとまず共通鍵が自動的に作られます。それを使って本文を暗号化します。この共通鍵を今度は受信者が公開している公開鍵で暗号化します。2 つできた暗号(公開鍵で暗号化された共通鍵と共通鍵で暗号化されたメッセージ本文)をメールで送信します。受信者は、自分の秘密鍵で暗号化された共通鍵を復号し、この復号化された共通鍵を使ってメッセージ本文を復号します。

このような煩雑な手続きをとるのは、公開鍵暗号の計算は共通鍵より余分に時間がかかるためです。そこで、何十行もあるメール全体や大きな添付ファイルまでもいきなり公開鍵で暗号化するのでなく、ほんの数行に過ぎない共通鍵だけを公開鍵で暗号化するのです。こうすれば、暗号処理に必要となる時間があまり増えずに済みます。しかも、この方法ならメール本体を毎回違う鍵で暗号化するため、暗号が破られにくいようです。

共通鍵暗号はあまり手間をかけずに使うことができて、OpenPGP の他にもウェブサイトとの暗号通信 https で使われていて、利用者が気づかないうちに暗号化も復号できてしまいます。一方、公開鍵は秘密鍵とセットで作っておき、公開鍵をみんなに知らせておく（少なくとも、自分宛にメールを送りそうな人へは知らせておく）という手間がどうしても必要です。