インターネット大学SOIで学ぶデジタルリテラシー

【村井純教授のインターネット基礎講座】

ダイジェスト

第4回：セキュリティーとプライバシー

日常でインターネットを使っていても、技術の基本はよくわからない、ホントの意味を知っておきたいというみなさんに、テクノロジーとしてのインターネットがどのような原理や仕組みで動いているかを正しく理解していただくことを目的に、インターネット大学SOIの「インターネット概論」の授業の一部をダイジェストとして紹介しています。今回はインターネット上のセキュリティーとプライバシーを守る公開鍵暗号を考えましょう。

URL http://www.soi.wide.ad.jp/class/20020002/

村井純 むらい・じゅん

慶應義塾大学環境情報学部教授。日本のインターネット第一号となったWIDEプロジェクトを設立。インターネットでの日本語の取り扱い方の取り決めの開発、IAB委員、インターネット協会（ISOC）理事など国際的なインターネット組織の役員を歴任するなど、インターネットの技術と社会の発展に尽力している。

今回の授業はこちらを参照

SOI「インターネット概論」（第7回「セキュリティーとプライバシー」）へ

URL http://www.soi.wide.ad.jp/class/20020002/slides/07/

◎パイプの安全とポリシーコントロール

政府関係者や企業の人と話をしても、セキュリティーとプライバシーの問題については、みなさん非常に混乱しています。とても大切なことなので、セキュリティーとは何か、プライバシーとは何かということをしっかり理解してほしいですね。

たとえばメールのやり取りをする、ボイスメールでも何でもいいんですが、インターネットを使ってコミュニケーションをするときに、セキュリティーについて2つに分けて考えてほしいんです。

1つは、みなさんが出すメッセージが、みなさんから出て相手に届くまでの間にきちんと守られているかどうか。データの受け渡しのときの安全性、その間に人に盗まれるとか壊されるとか、すり替えられてしまったりするのは、通信のパイプの安全性の問題です。これがセキュリティーの1つの側面です。運ぶときの安全性が確保されなくてはなりません。

そしてもう1つの問題は、何かデータにアクセスするときに発生します。自分にきたメールをみんなに公開する人は誰もいないでしょうが、親しい数人には見せるかもしれません。この人とこの人には見せてもいいなという判断基準、これが個人のプライバシーポリシーです。「この情報にアクセスしていいのは私が許可した人だけ」という、このプライバシーポリシーをコントロールできなくてはいけません。

インターネット上の大学SOI

この連載の内容はSOI（School of Internet）でストリーミング映像によって公開しています。 URL http://www.soi.wide.ad.jp

SOIとは、世界中の学ぶ意欲を持つ人々にインターネットを基盤とした高等教育と研究機会を提供することを目的として1997年に開始したインターネット大学です。
希望者はインターネットから入学を登録し、学生認証を受けることができます。詳細はホームページをご覧ください。

レッスン1

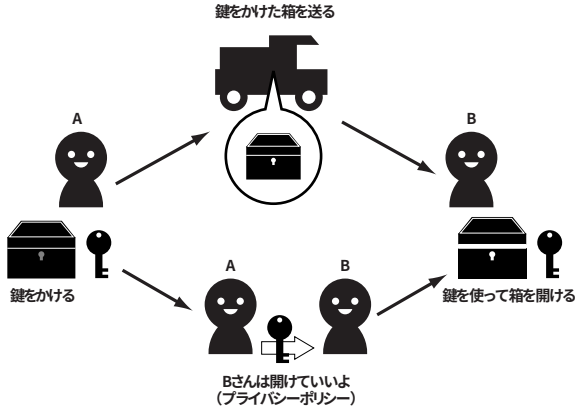
公開鍵暗号でセキュリティーを実現

図1　2つの視点から見たセキュリティー

●データ受け渡し時の安全性
身の周りの例　→　郵便の現金書留
本当に正しいデータ？　データを送る途中で盗み見られたりしていない？
中身が替えられたりしていない？

●データのアクセス権のコントロール
身の周りの例　→　電話のナンバーディスプレイ
アクセスしてきたのは許可した人？
アクセス者が特定できる？
匿名のアクセス者ではない？

図2　暗号は鍵と箱の関係



鍵をかけた箱の中身（暗号）を相手に安全に渡すには、鍵と箱を別々に渡し、鍵（暗号の解読法）は、そっと手渡すのが安全だが、インターネットではそれができない。

アクセスしたい人とアクセスされる側の約束事をポリシーというのですが、その約束事がきちんと守られていることもセキュリティーなのです。

この2つのセキュリティーはまったく異なった問題ですね。情報にアクセスするときのコントロールと、情報を運搬するときの安全性。全然違うけど、インターネットのセキュリティーを考える入り口としては、この2つを考えておくことが重要です。この2つを混同してはいけません（図1）。

◎鍵配送問題にけりをつけた
公開鍵暗号という大発明

この2つのセキュリティーを実現するためにどんな技術があるかと言うと、「公開鍵暗号」という技術です。これはどちらのセキュリティーにも使えます。公開鍵暗号は1975年に作られたものだから比較的新しい大発明ですね。これがなくてはインターネットの上で安全なオンラインショッピングはできません。

秘密の通信をしたいときには合い言葉で暗号化します。たとえばこの教室で僕と一番後ろの席の人が、「これから暗号で話すぞ」と言って、ごにょごにょと話している。それを教室中の人がみんな聞いてる、というのがインターネットの状況です。インターネットは途中で情報を盗まれるかもしれないわけだから、みんなが聞いてるところで話すようなものですよね。そこでいきなり僕がわけのわからない言葉で話し出したらそれが暗号ですね。

たとえば「HALって言ったらIBMのことだ」みたいに、アルファベットを一文字足して受け取るというルールを決めて、それが可能な耳を持っていればこれはお互いの暗号方式になる。ただ、ここで一番問題になるのは「一文字足す」という「鍵」をどうやって相手に渡すかということです。これを「鍵配送問題」といいます。こうやってパブリックスペースで話をしているときに暗号の鍵をどうやって渡すか？

暗号の技術自体は大昔から、シーザーの時代からあるわけですが、鍵の受け渡しは難しい問題をはらんでいます。普通は最初から知っている、あらかじめ出会っている人にはそっと鍵を渡し、後でこの鍵で暗号を解読してと頼むことが可能です。これは『共有鍵暗号方式』です（図2）。

しかし、インターネット上ではそうはいきません。たとえばプロバイダーのIDやパスワードは郵便で送ってきますが、これはネットで完結せずにショートカットをしている。そうではなくて、インターネット上で鍵が交換できないか？　この問題にけりをつけたのが「公開鍵暗号」方式で、だから大発明なんです。これがなければ、ショッピングサイトに行って、いきなり秘密でクレジットカード番号を送って買い物なんかできません。公開鍵暗号の偉いところは、もうみなさんが使ってる、広く普及した技術だということです。

レッスン2

鍵をどうやって相手に渡すかが問題だ

図3　共有鍵暗号方式の仕組み

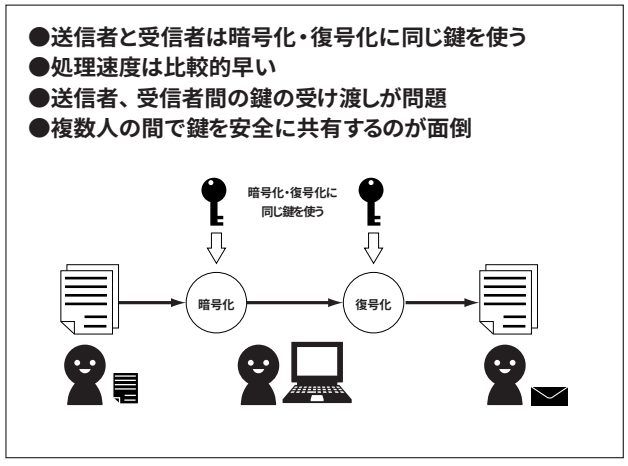
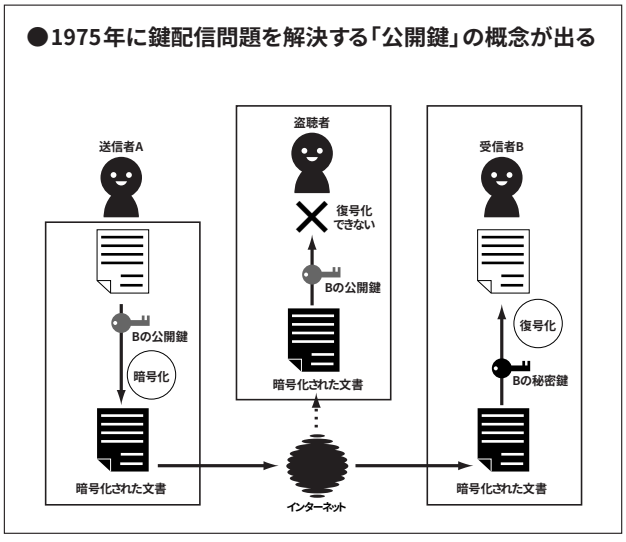


図4　公開鍵暗号方式の仕組み



◎公開鍵暗号で安全にショッピング

インターネットで使われているのはデジタルすなわち数字なので、数学の魔法が使えます。公開鍵にはその数学の魔法が使われています。アルゴリズムを説明するのは難しいのですが、基本的に行っていることは、鍵をかけた箱を送るということなのです。

鍵をかけた箱を小包で送る場合、相手が鍵を持っていないと開けられません。ところが、開けてもらうために鍵を先に送ると途中で鍵をコピーされてしまう危険があるので鍵をかけた意味がない。さて、どうしよう。公開鍵暗号方式はこの箱と鍵の関係を変えたのです。普通は閉めた鍵と同じ鍵で開けていたのを、公開鍵暗号では、閉めたのとは別の鍵で開けるようにしたのです。

鍵を作るときに閉めるのと開けるのと別々の2つの鍵ができる仕組みを作ったのです。このことを覚えておくと公開鍵暗号はすごくわかりやすくなります。2つの鍵のどちらで閉めてもいいのですが、つまりどちらかでかければもう1つで開けられる、AとBというペアの鍵ができます。1つが秘密にしまっておく秘密鍵、もう1つは誰にでも手の届くところに置いておく公開鍵です。

公開鍵はだいたいホームページに置いてあります。たとえば伊勢丹のオンラインショッピングの公開鍵は伊勢丹のホームページに置いてあります。伊勢丹のホームページで買い物をするときは、この公開鍵を持ってきて、送る情報を暗号化する。そうするとそのペアのもう1つの鍵は伊勢丹だけが持っているから、送った暗号を開けるのは伊勢丹の秘密鍵を持っている人だけです。このメカニズムが公開鍵暗号です（図4）。

これによって、インターネット上で初対面の人にも暗号化した秘密のメッセージを送れるようになり、これを使って安全にオンラインショッピングができているわけです。これは先ほど話したパイプの暗号化で、送るときに人に見られてもかまわないようにメッセージを暗号化したわけです。

◎公開鍵を電子判子として使う

では、今度はこれを逆に使ってみましょう。さきほど買い物をしたので、伊勢丹が領収書を送ってきます。このときに、秘密鍵で暗号化して送ってくるとこれを僕が税理士のところに持っていきます。「伊勢丹で本当に買い物したんで、領収書を送ってきたんですよ」と。税理士は本当に伊勢丹が送ってきたのかわからないじゃないかと言いますが、これを伊勢丹の公開鍵で開くと領収書が出てきたとしたら、ペアの秘密鍵で暗号化できる可能性があるのはそれを持っている伊勢丹だけだから、という証明ができるわけです。

これが認証、電子判子の仕組みです。電子判子を自分で押しながら、相手の公開鍵で暗号化して二重化することも可能で、信頼性が増します。セキュリティーで重要なのは公開鍵の技術です。この技術を使って、伝送経路の暗号化と、受け取った場合になりすましを防ぐ、相手の認証を電子的にできる仕組みができています。

レッスン3

暗号化の計算方法――安全性と時間の兼ね合いを秤にかける

図5　公開鍵暗号方式にまつわる3つの誤解

●公開鍵暗号はより安全だ
具体的なシステムによる

●公開鍵暗号は汎用性がある
計算のコストが高いので、秘密鍵の受け渡しや署名が主な応用分野

●公開鍵の受け渡しが簡単だ
公開鍵の信用性は?

図6　暗号化とは元に戻すのが大変な演算のこと

●暗号化の演算
ある数を10乗する
たとえば
17^{10} →がんばれば計算できる

●復号化の演算
9904兆5780億3290万5937は何を10乗したものか?
→計算にとても時間がかかる

この時間差が暗号の解読されにくさ

◎暗号化は行きと戻りの時間の差

いいことずくめの公開鍵暗号ですが、暗号化のコスト面などの問題はあります(図5)。

暗号化とはどんな計算がされているのでしょう?　たとえばすごく大きな数の13乗は、一生懸命計算すれば答えは出ます。しかし、その答えの紙を渡して、「この数字は何を13乗したのか調べろ」と言うと計算はすごく大変になります(図6)。要は素因数分解なのですが、ある数を素数で分解していくのは時間がかかるが、かけ算はもっと短時間で誰でもできます。

暗号化の演算も、行くときは速いが戻るには時間がかかる関数を用意しておきます。この行きと戻りの差が問題で、戻りが天文学的な時間のかかる計算であれば安全性は非常に高いわけですが、結局は差の問題なので、実は安全性の高い公開鍵暗号は行きの計算にも時間がかかるものなのです。安全な暗号はものすごく計算量が多い。これはみなさんのコンピュータで計算をさせると、そのパワーだけでCPUがへたってしまうほどの計算量です。ですから公開鍵暗号も万能ではありません。自分に何が大事なのかを判断し、本当に大事なものは時間のかかる暗号をかければいいわけです。一方、重要性の高くないものは、暗号なんかかけないほうが、処理が 速く進むから気持ちがいいでしょう。

これをどうやって組み合わせるのかを考えていくと、安全性やセキュリティー、さらにプライバシーについて、もっとわがままを言えるように社会全体が成熟していく必要があると思います。

◎技術だけでは解決できない課題

山奥の一軒家だったら、鍵なんかかける必要はないでしょう。昔は東京のど真ん中でも鍵なんかかけずに生活していた人はたくさんいました。ところが、最近物騒になってきてみんな鍵をかけるようになり、より頑丈な鍵も出てきました。

悪いやつがどこにいるかわからないような時代になったら、身の安全というのを考えるようになります。それと同じで、インターネットはどこにでもつながるから、その上で大事なものを扱うのであれば、それなりのセキュリティーリテラシーみたいなものをみなが持っていなくてはなりません。

デジタル情報のいいところは完全な複製が可能な点ですが、いくら暗号化して送っても、開いた後で裸のデータをばらまけば、本来出回るべきでなかったデータが出回ってしまう。これは人為的な問題です。デジタル情報はコピーしても劣化しないので複製されまくる危険性があります。

デジタルテクノロジーをよく理解して、公開鍵とその技術の限界もよく理解して、新しい社会制度なり、文化なり、教育なりをきちんとやらないと、社会全体としてはセキュリティーを実現できません。技術だけですべてを解決することはできない。セキュリティーとプライバシーは技術と人と社会が作らなければなりません。どうプロデュースしていくかはこれからの課題です。

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp