やさしいネットワーク・セキュリティ（1）
通信データの盗聴への対策技術

連載 IT技術

村山　純一
MURAYAMA　Junichi
東海大学大学院情報通信学研究科
情報通信学専攻主任教授

インターネットとセキュリティ

現代社会は高度情報化社会である。これを支えるインターネットの発展には目を見張るものがある。現在では，スマートフォンなどを介して，世界中の人々が繋がっている。この結果，我々の生活に欠くことの出来ない，インフラストラクチャとなっている。

一方で，インターネットを利用した犯罪が後を絶たない。当初は，コンピュータの技術者が技術力を誇示するための事件が大半であった。しかし，現在は，事件の悪質化が進んでいる。ビジネス社会にも大きな金銭的な損害を与えている。最近では，毎日のように新聞やTVで，インターネットに関わる事件がニュース報道されている。高度情報化社会においては，インターネットを使わないという選択はありえない。このような背景から，インターネット上で安心・安全を実現するためのネットワーク・セキュリティ技術への関心が高まっている。

そこで，今回から全4回にわたり，ネットワーク・セキュリティの考え方について，できるだけわかりやすく紹介させて戴くことにする。

盗聴されるインターネット

ニュース報道などでご存知の方も多いと思うが，インターネットでは，盗聴が日常茶飯事である。通信の秘密が守られる固定電話に比べると大違いである。これは，通信網の設計思想の違いも影響していると考えられる。

固定電話網は，国家並みに信頼できる通信キャリア（通信事業者）同士が相互接続されることで構成されている。従量課金を行うために，誰と誰がいつからいつまで通信したかについても，通信事業者が詳細を把握している。

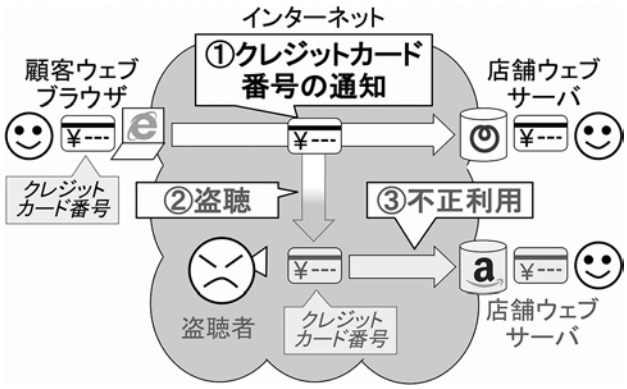
一方，インターネットでは，多種多様なサービス・プロバイダ（通信事業者）同士が複雑に相互接続されている。定額課金が主流のため，誰と誰がいつからいつまで通信したかについては，ほとんど把握されていない。また，通信データが，どのプロバイダを経由して送られるのかも把握されていない。このため，通信データが送られる経路上に，悪質なプロバイダや第三者がいても，利用者がその存在に気づくことは難しい。

インターネット・ショッピング

現在のインターネットは，ショッピングの利便性を飛躍的に高めている。顧客がインターネット上で商品を選択した後に，クレジットカードで料金支払いを行うことで，後は宅配業者が顧客へ現物の商品を配送してくれる。クレジットカード決済時は，その場でカード番号（とセキュリティコード）を通知するだけで良く大変便利である。

しかし，図－1に示すように，インターネットには盗聴者が潜んでいる。①クレジットカード番号は，顧客のウェブブラウザから店舗のウェブサーバへ，インターネットを利用して，通知される。②この際に，ク

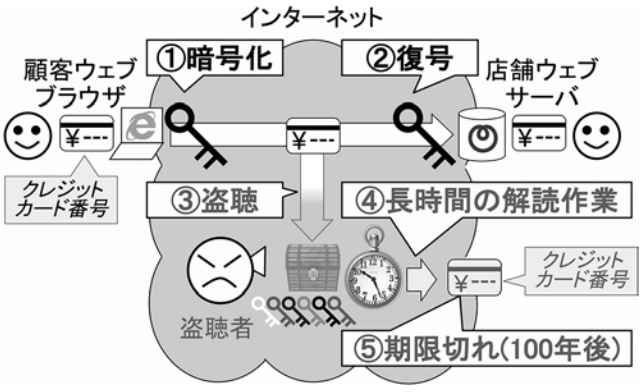
レジットカード番号が盗聴される確率が高い。③盗聴者は，クレジットカード番号を入手すると，これを別の店舗のウェブサーバなどで不正利用する。クレジットカードで購入された商品の最終的な支払いは，クレジットカードの所有者に請求されることとなる。



図－1　通信データの盗聴

暗号通信による盗聴対策

盗聴自体を防げない状況で，クレジットカードの不正利用を防止するためには，図－2に示すように，暗号通信の利用が魅力的である。①顧客のウェブブラウザは，暗号鍵を利用してクレジットカード番号を暗号化する。生成された暗号データは，インターネット上を転送され，店舗のウェブサーバに届けられる。②サーバは，暗号鍵を利用して暗号データを復号し，クレジットカード番号を読み取る。③一方，暗号データは盗聴者にも届いてしまう。しかし，盗聴者は暗号鍵を持たない。このため，暗号データを復号できない。④仮に暗号データの解読を試みようとしても，クレジットカード番号を読み取るまでに，多大な試行錯誤が要求される。通常は，天文学的に長期の時間を費やすこととなる。⑤暗号解読時にクレジットカードの期限が切れていれば，そのカードの不正利用が行えない。このため，安全が確保されたことになる。

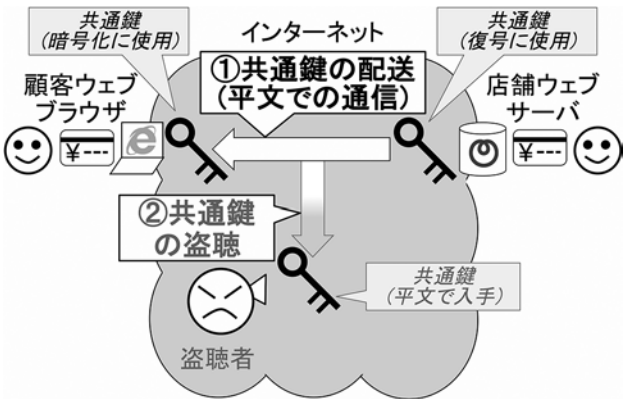


図－2　盗聴対策としての暗号通信

共通鍵の配送は危険

インターネット・ショッピングで暗号通信を行うためには，図－3に示すように，顧客のウェブブラウザと店舗のウェブサーバの双方が暗号鍵を持つ必要がある。基礎的な暗号通信方式では，暗号化と復号で同じ鍵を使用する。この鍵は共通鍵と呼ばれる。①共通鍵は，通信の初期段階で，店舗のウェブサーバから顧客のウェブブラウザへオンラインで送り届けられる必要がある。しかし，この段階では，まだ暗号通信路が設定されていない。②このため，この鍵自身が盗聴される危険性が高い。

盗聴者は，あらかじめ共通鍵を入手しておくことで，その後に盗聴した暗号データを瞬間的に復号できる。すなわち，クレジットカードが不正利用されてしまう。このことは，インターネット・ショッピングを実現する上で，大きな問題となっていた。



図－3　暗号鍵の配送問題

2つの鍵を使う暗号通信

暗号鍵の盗聴対策として，2つの鍵を使う暗号通信方式が，Diffie氏とHellman氏によって提唱された。1976年のことである。この方式では，暗号化専用の鍵と復号専用の鍵を使用する。暗号化専用の鍵で暗号化したデータを，同じ鍵で復号することはできない。一方で，復号専用の鍵では復号することができる。こ

のように，とても不思議な性質を持った鍵を使用する。

盗聴が前提の公開鍵

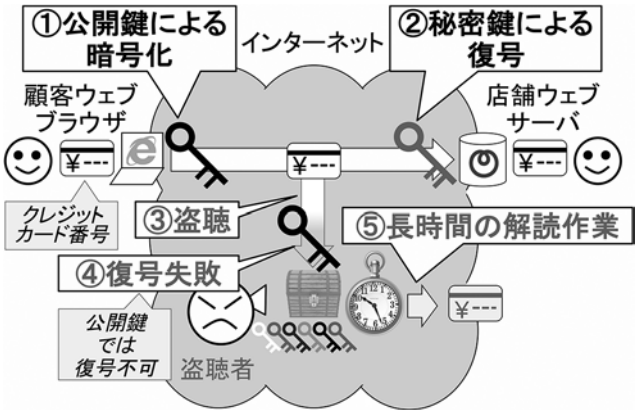
暗号化専用の鍵は「公開鍵」，復号専用の鍵は「秘密鍵」と呼ばれる。通信の初期段階には，店舗のウェブサーバが，顧客のウェブブラウザへ，公開鍵を送り届ける。この公開鍵も盗聴される危険性が高い。一方，店舗のウェブサーバは，秘密鍵も保有する。こちらは，他者に晒されないよう，サーバ内部で厳重に保管される。

秘密鍵だけが復号可能

2つの鍵を使う暗号通信方式では，図－4に示すように，クレジットカード番号が秘匿される。①顧客のウェブブラウザは，公開鍵を利用してクレジットカード番号を暗号化する。生成された暗号データは，インターネット上を転送され，店舗のウェブサーバに届けられる。②サーバは，秘密鍵を利用して暗号データを復号し，クレジットカード番号を読み取る。

③暗号データは公開鍵を事前入手した盗聴者にも届いてしまう。④しかし，暗号データの復号には失敗する。公開鍵で暗号化された通信データは，公開鍵では復号できないためである。⑤この結果，盗聴者は長期間の解読作業を強いられることになる。

この公開鍵/秘密鍵・暗号方式は，インターネット・ショッピングを実現する画期的なアイデアとされた。しかし，このアイデアが提唱された時点では，これらの鍵を実現することができなかった。まさに，絵に描いた餅のようなアイデアだった。



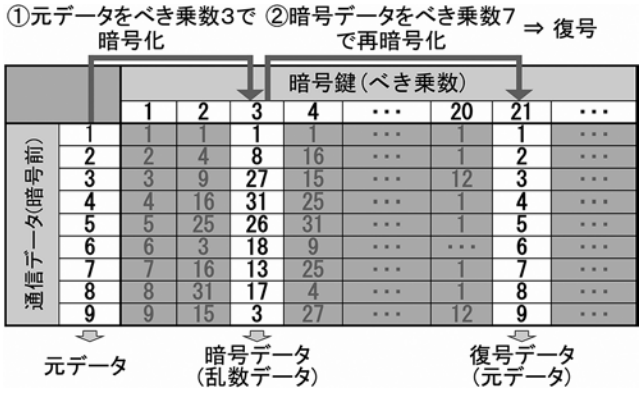
図－4　2種類のカギを使う暗号通信

RSA暗号

公開鍵/秘密鍵・暗号方式の提唱以来，数学的な難問として，その実現が数学者たちの大きな目標となった。一般的には，ある関数で変換した通信データは，逆変換することで元に復元できる。しかし，元に戻せない関数を作り出す必要があった。さらには，何らかの手段で元に復元できる必要もあった。

このような難問は，当面解決できないと思われた。しかし，なんと翌年の1977年に，Rivest氏，Shamir氏，Adleman氏の3氏によって，解決されてしまった。この暗号は，彼らの頭文字を合わせて，RSA暗号と呼ばれている。

RSA暗号の詳細は文献1）にわかりやすく解説されているので参考にされたい。ここでは紙面の都合で詳細の説明を割愛する。ポイントは，通信データを，何乗か「べき乗」した後で，2つの素数の積で割り，その余りを求めることである。



通信データ(暗号前)	1	2	3	4	…	20	21	…
1	1	1	1	1	…	1	1	…
2	2	4	8	16	…	1	2	…
3	3	9	27	15	…	12	3	…
4	4	16	31	25	…	1	4	…
5	5	25	26	31	…	1	5	…
6	6	3	18	9	…	…	6	…
7	7	16	13	25	…	1	7	…
8	8	31	17	4	…	1	8	…
9	9	15	3	27	…	12	9	…

図－5　RSA暗号で使う乱数表

図－5に示すように，元データである通信データを行に，暗号化の鍵に該当するべき乗数を列にした表を作成すると乱数表が出来上がる。表の中身は割算の余りなので，逆変換しても元に復元することはできない。興味深いのは，この乱数表がべき乗数に対して周期性を持つことである。すなわち，暗号化の処理を重ねると元データに復元できるポイントが存在する。逆変換しても元には戻せないが，変換を重ねると元に戻せるということである。

①この表では，べき乗数を3として，通信データを変換することで，暗号データが生成される。（表のべき乗数3の行に，元データと異なる乱数列が並んでい

ることに注目されたい）。②この暗号データを，さらにべき乗数を7として再変換する。べき乗数3とべき乗数7の変換を重ねるので，べき乗数21の変換を行ったことになる。ここで生成されるデータは，元データと等しい。すなわち，暗号データが復元できたことになる。（表のべき乗数21の行に，数字列が元データと同じ順に並んでいることに注目されたい）。

復号鍵を持たない盗聴者が，この復元ポイントを探すためには，2つの素数の積を素因数分解する必要がある。小さな数では簡単にできるが，大きな数だと数学的な難問となる。すなわち，RSA暗号の強度は，大きな数の素因数分解の難しさに支えられている。

数学者たちはホワイトハッカー?

RSA暗号の提案以来，世界中で素因数分解の競争が行われている。文献2）では，NTTの研究所が2010年に世界記録として，232桁の整数の素因数分解に成功したことが報告されている。大きな数が素因数分解されると，RSA暗号では，より大きな素数の積を用いる必要が生じる。数学者たちはホワイトハッカーのような役割を果たすことで，ネットワーク・セキュリティの強化に貢献している。

暗号通信の確認方法

インターネット・ショッピングでクレジットカード番号を通知する際には，暗号通信が行われていることを確認することが重要である。このためには，ウェブブラウザのアドレスバーを見れば良い。このアドレスバーは，図－6に示すように，ウェブブラウザの上部に位置し，アクセス中のウェブサーバのアドレスを常に表示している。このアドレスは，通常httpあるいはhttpsのいずれかで始まる。httpは平文通信，httpsは暗号通信を行うプロトコル（通信方式）を意味する。平文通信の時は，httpの表示自体も省略されることがある。よく注意されたい。

アドレスバーを確認する際には，アクセス中のサーバが本物であるかどうかも併せて見極める必要がある。この方法については，次回解説する。

なお，一般的なインターネット・メールは平文で送られる。このため，情報漏洩を避けることができない。日頃から十分に注意して利用されたい。

図－6　ウェブ・ブラウザーのアドレスバー

【参考文献】

1）RSA暗号の世界
<http://www.maitou.gr.jp/rsa/rsa10.php>
2）公開鍵暗号の安全性の根拠である「素因数分解問題」で世界記録を更新<http://www.ntt.co.jp/news2010/1001/100108a.html>