2002-10-1

H．P．Report

第57号

発行責任者 稲崎義明

セキュリティと暗号（１４）

暗号の安全性を定量的に評価するものに、証明可能安全性があります。個々の暗号の安全性を特定の解読法でその鍵を推定されてしまう確率で表現するもので、この確率が小さいほど解読の難しい暗号ということができます。これが前回書いた線形解読法の「線形特性確率」や「平均線形確率」などですが、ＤＥＳなど多くの暗号アルゴリズムが、平均線形確率などの値を求めることが極めて困難であったために、これまでは評価されていませんでした。しかし、数値的に安全度を評価できないということは、本当に安全なのかが証明できないことになります。確かにＤＥＳなどは20年も解読されなかったのですが。そこで、数学的に安全性を証明できる暗号として作り出されたのが「ＭＩＳＴＹ」です。平均差分確率や平均線形確率を元にしてアルゴリズムを組み立て、その確率値をいかに小さくするかで構造を検討していくという方法で「ＭＩＳＴＹ」のアルゴリズムはつくられています。また、暗号は数学ですから、ハードウェアへの実装も念頭に入れて検討されています。実際に実装する際には、1つの回路を何度でも使いまわす方法、例えば、同一の動作をデータやパラメータを入れ替えて8回繰り返すことによって暗号化しています。それぞれの動作は、唯一の暗号鍵を基に一時的に使う拡大鍵を生成する「鍵スケジュール部」とそれを用いてデータを変換・撹拌する「データ・ランダム化部」に分かれていますが、この拡大鍵を生成する回路と、データを撹拌する回路を1つだけ用意して8回処理すれば、回路規模を1／8にすることができるわけで、「ＭＩＳＴＹ」の回路ではさらにこの二つの部分の処理の一部を共通化することによって、更なる回路規模の縮小を進めてあります。

さて、今回の特集では、セキュリティの必要性から盗聴、暗号化までをいろいろと書いてみました。いろいろ調べてみるとこれまでスパイ映画であったようなことが、インターネットのネットワーク環境を使っていく上で、誰でもか必要なものであることが少しでもご理解いただけたらと考えています。初めのほうにも書いたと思いますが、ＡＤＳＬやＣＡＴＶなどの普及によって、常時接続が一般化した現在では、家庭で使っているパソコンですら外部からの侵入が考えられ、また、ウィルスの侵入による友人知人への迷惑メールの発信、他のＷｅｂサーバへの侵入の踏み台にもなりかねません。確かに、クレジットカードによる被害もあるでしょうが、個人的な問題よりも他の人に対する加害者ともなりかねないのが現状です。その中で、このセキュリティにどの程度注意が払われているかとなると怪しいものがあります。ウィルスやインターネットによる犯罪などは対岸の火事ではないのです。十分に個人のパソコンであってもセキュリティに対して対応を考えている必要があります。無線ＬＡＮを使う際にも、スピードが多少遅くなるからといって、暗号化をしないで利用するのは会社などでは行うべきではありません。究極的には、すべてを安心できるように暗号化するということなのかもしれませんが、いろいろな犯罪集団やテロ集団もこの便利なインターネットを使って、それこそ全世界的に24時間活動していることを考えると、メールを暗号化する事によって各国の諜報機関といっても、なかなか情報収集ができないという別の面も出てきています（情報管理されてしまうことも問題ですが）。いろいろな情報がネット上に流れていますが、完全に安全ということはありません。システムとして安全性が高くても人間がかかわってしまえば安全性は絶対に下がってしまいます。絶対に罪を犯さない人だけの集まりはないわけですから。これからもネット上の安全性、セキュリティについて考えてみたいと思います。　　（連載終了）

(情報誌トピックス)

○日経エレクトロニクス　９月２３日号
特集　ＪＰＥＧ特許でアレも売れないコレも売れない
→ＪＰＥＧは国際標準規格ではあるが、この圧縮技術の特許についての権利主張がＦｏｒｇｅｎ社から各社に出されている。まずはデジカメからだが他にもいろいろなものに使われているためどうするかが問題となってきている。既にソニーと三洋は契約が済んでいる。
解説　街頭テレビの復権
→銀行やコンビニ、ホテルなどにブロードバンドでつながった平面ディスプレイが、これまでのポスターに替わって増えてきている。あたかも、テレビ創生期の街頭テレビのようだが、次々と情報が表示される。

○日経パソコン　９月３０日号
特集　それでも気になるパソコンのスペック
→普通のアプリケーションを使うのなら、今のパソコンならどれでも性能は十分のはず。しかし、実際に買うとなったらスペックにはどうしても目がいってしまう。宣伝に惑わされずにパソコンを選ぶために、どうスペックを読んだらいいかをそれぞれのパーツに分けて解説。
特集　Ｗｉｎｄｏｗｓ玄人志向テクニック
→レジストリの設定変更などに出てくる呪文のような言葉の意味を理解し、Ｗｉｎｄｏｗｓを使いやすく作り替えるには。
ﾚﾎﾟｰﾄ 古いパソコンをサーバにする
→パソコンの買い替えでててくるこれまで使っていたパソコン。捨てるには忍びない。複数台のパソコンを家で使っているならサーバにしてしまうための設定は。また、思い切ってＷｅｂサーバを立ち上げるには。

○日経バイト　１０月号
特集　プログラミング言語の明日
→現在プログラミング言語としては、ＶｉｓｕａｌＢａｓｉｃ（ＶＢ）、Ｃ言語のほかに、Ｊａｖａなどがあるが、現在のＶＢ６の後継であるＶＢ．ＮＥＴはＶＢとの互換性がない。明日のプログラミング言語は．ＮＥＴがいいのかＪａｖａ、Ｃの後継の新しいＣ＃がいいのか選択を迫られている。
特集　ＩＥとスクリプトの“危険な関係”
→メジャーなブラウザであるＩＥ、いろいろとセキュリティホールが指摘されるがいまだに使われている。一方いろいろなサイトにアクセスすることによってパソコン側で動作するスクリプトは危険な毒にもなるが薬にもなる。特に危ないサイトにＩＥでアクセスすると危険がいっぱい。ＩＥがローカルのＡｃｔｉｖｅＸを利用できる仕様になっているため注意が必要。危ないサイトにアクセスしないほうがいい。

○日経オープンシステム　１０月号
特集　データベース構築の新常識
→データベースの機能アップするために、これまでは事前準備として検索頻度の高いテーブルを設定したりしていたが、ハードの力でデータベースの機能向上が図られている。但し、正しい増強の仕方があり、最適な

アーキテクチャを見極める必要はある。

選択　メールソフトの安全な使い方

→メールはウィルスマ感染や情報漏洩の窓口。アンチウィルスソフトの活用に加えて、ＩＥ以外のソフトの利用や設定に気をつけたい。

○Ｎ＋Ｉ　ＮＥＴＷＯＲＫ Ｇｕｉｄｅ　１０月号

特集　内部セキュリティをスイッチで守れ！！

→スイッチの機能を使い、ネットワークの分割などを行うことによって、ネットワークの接続そのものに認証を施すなどによって早い段階でのセキュリティ対策が可能となる。スイッチの重要性を見直してみる。

特集　ＡｃｔｉｖｅＤｉｒｅｃｔｒｙ導入と運用のポイント

→サーバやクライアントを階層的に管理するディレクトリサービス。Ｗｉｎ２０００をベースにしたＡｃｔｉｖｅＤｉｒｅｃｔｒｙの導入と運用のポイント。

○ＡＳＣＩＩ　１０月号

特集　ＵＳＢ２．０　ｖｓ　ＩＥＥＥ１３９４ハイスピード頂上対決

→２．０で転送速度が４８０ＭｂｐｓとなったＵＳＢ。一方ＳＣＳＩの代わりとなる高速インターフェース規格ＩＥＥＥ１３９４。これからのインターフェースとしてどちらが使える規格か。

特集　ホームデータセンター大構築

→家庭用サーバが商品化されてきている。パソコンでホームデータセンターとなるサーバを構築するには。ホームデータサーバとして何が必要か。

○ＤＯＳ／Ｖｍａｇａｚｉｎｅ　１０月１５日号

特集　完全検証！ＤＸ９世代ビデオカード

→パソコン上で３Ｄ処理を行うＤｉｒｅｃｔＸ(ＤＸ)の第９世代のＤＸ９に対応したハードウェアが、ＤＸ９の正式発表を前に製品化されつつある。３Ｄ処理の現状と、新世代のビデオカードの性能の紹介。

特集　売れ筋電源ユニット徹底チェック

→パソコンに絶対必要な電源。性能面であまり話題にならないが、電源容量や静音性などチェックする点はある。売れ筋電源ユニットを比較してベストチョイスを探る。