セキュリティ分野における安全神話とその崩壊

ー永遠のビギナー対策から標準化まで，穴だらけのセキュリティ？ー

第１７回サイバー犯罪に関する白浜シンポジウム

2013年5月24日

森井昌克

morii@eedept.kobe-u.ac.jp

（**神戸大学大学院　工学研究科**）

要旨

- セキュリティの第一歩はパスワードの設定に始まる「永遠のビギナー」対策だと言われる．実はその対極にあるセキュリティシステムおよびそれらの製品自体に脆弱性を抱えている．ブラウザやOS等の脆弱性がよく問題にされるが，それだけではない．無線LANにおけるWEPの脆弱性は周知のとおりであり，WPAにも脆弱性がないとは言えない．また，最近では認証局の運用における脆弱性が問題となっているが，根本的なSSL／TLSでの脆弱性も指摘され，脆弱性を超えた機能不全状態もまじかに迫っている．本講演ではこれらのいくつかのシステム上の問題点を上げ，その対策について議論する．

安全神話とその崩壊

- キーセンテンス（その1）
  - 時は昔、20世紀の話
    - 昔からセキュリティの問題は変わらない
  - だから暗号は理解されていない！
    - 暗号とは何か、何であるべきか
  - 暗号は破られるもの！？
    - RSA暗号が解かれた？
    - AESが解かれた？

安全神話とその崩壊

- キーセンテンス（その2）
  - WEP/WPA-TKIPの現状
    - WEPは終わった！？は本当か？
    - WPAは安全か？
  - SSL/TLSは終わった！？
    - BEAST,Racky13とは何だったのか？
    - そして、SSL/TLSの終焉　…　Google涙目？
  - 暗号から見たセキュリティの本道
    - 暗号は強いが、暗号システムは弱い！？
    - 「AES128ビットよりAES256ビットが安全」は大間違い！

時は昔、20世紀の話

- セキュリティは昔から深刻な問題
  - 1990年代の私、紹介
    - 私の初めての論文
      - A Theorem that GF (2^{4m}) has no Self-Complementary Normal Bases over GF (2) for Odd m *（1984）*
      - *抽象数学？？？*
    - 学位論文
      - Efficient Algorithm Over Finite Fields And Their Applications To Coding Theory And Cryptography(1989)
  - 現在までのハッキングとの関わり？
  - 現在までのマルウェアとの関わり

時は昔、20世紀の話

- パスワードという古からの問題
  - ユーザに管理させるのは所詮無理！
    - 30年間の実績？
  - ワンタイムパスワード(OTP)
    - 本当のOTPは理解されていない？
    - 利便性の問題、再び
  - パスワード管理システム
    - 解決法として有望、だけど…

だから暗号は理解されていない

- 暗号は、格闘技に例えれば「相撲」のようなもの？
  - 暗号には暗号の世界のルールが有る
  - 同じ土俵の上で議論する
    - 条件や仮定が決まっている。
  - 絶対的ルールが「評価」できること！
    - 全てを公開して、「鍵」だけで守る
- 対して、暗号システムは異種格闘技
  - ルール無用？

だから暗号は理解されていない

- 暗号の強さは鍵の長さに依存しない！
  - AES128ビット鍵よりAES256ビット鍵のほうが安全（ウソ）
  - 一般、鍵が長くなれば処理速度は極めて遅くなる

暗号は破られるもの！？

- 暗号自体は破られない！
  - 1994年RSAが破られた（ニューヨークタイムス）
    - 誤報、なぜ
  - 1996年RSAが破られた(PGPでのRSA)
    - 誤報、なぜ
  - 2011年AESが破られた（CRYPTO2011で）
    - 本当、なぜ？？？
- 暗号システムには脆弱性がある
  - 暗号が理解されていない

WEP/WPA-TKIPの現状

- 無線LAN標準暗号化システム
  - WEPは解読されたは本当か？
    - 2008年、我々（森井ら）が一般的な攻撃法を開発
      - 3万パケットで50%の確率で104ビット鍵を1秒で得る
      - PTW攻撃（2007）はARPパケットが必要、しかも4万パケット
    - 現在、改良が進み19,800パケットで解読(FSE2013)
  - WEPは滅んだか？
    - 生かさなければならない理由
      - その方法は？

WEP/WPA-TKIPの現状

- WPA2, WPA-TKIPはWEP以降の暗号システム
  - 特にWPA-TKIPはWEP環境化で実装可能
    - 当面の代替処置として期待
    - WEPを改良
  - WPA-TKIPは安全か？
    - 我々が2009年に脆弱性を指摘、さらに2010年に深刻な脆弱性を発見。
    - 何が問題だったのか？

SSL/TLSは終わった！

- SSLはネットワークセキュリティ最後の砦
  - 暗号は信じていなくても、SSLは信じている！？
    - HTTPS
  - SSLは安全というセキュリティ神話
    - 確かにブラウザ実装以降、最近まで致命的な脆弱性はなかった！
  - 2011年、BEAST攻撃
    - SSL/TLSの暗号CBCモードの脆弱性を利用
  - 2013年、Lucky13攻撃
    - SSL/TLSにおけるパディングオラクル攻撃

SSL/TLSは終わった！

- BEASTとLucky13でSSL/TLSは終わったか？
  - BEASTはCBCモードのみ有効、Lucky13はブロック暗号のみ有効
  - 大本命のSSL/TLS on RC4が健在！
    - Googleも使っているSSL/TLS on RC4へのシフトを推奨
    - SSL/TLS on RC4は高速、軽実装

SSL/TLSは終わった！

- 2012年12月、CRYPTREC（日本政府暗号評価機関）に、五十部、大東、森井がRC4の脆弱性（解読法）を報告
  - 結果的に、SSL/TLS on RC4の解読法
  - 暗号文から平文を直接解読する事が出来る。
    - Takanori Isobe, Toshihiro Ohigashi, Yuhei Watanabe, and Masakatu Morii, "Full Plaintext Recovery Attack on Broadcast RC4," 20th Int. Workshop on Fast Software Encryption (FSE2013)

SSL/TLSは終わった！

- SSL/TLS on RC4は安全（無傷）か？
  - RC4自体は古い世代の暗号であり、いくつかの脆弱性が指摘されている。
    - たとえば、最初の暗号文出力バイトは鍵と極めて高い。
    - 最初の256バイトの一部は鍵との相関が小さくない等
  - しかし、致命的な脆弱性は無く、その高速性および軽実装ゆえに、SSL/TLSだけでなく、PDF等様々な場面で利用されている。

SSL/TLSは終わった！

Full Plaintext Recovery Attack on Broadcast RC4

- 実際には、暗号文を2^{24}個集めれば、ほとんど解ける。
  - 2^{35}個集めれば全て解ける
  - プロトコルの制限から、実際の平文空間は小さい（英数字だとか）ので、2^{20}個以下

- どうすればよい？
  - CBCモードでないブロック暗号タイプのSSL/TLSを当分使うしか無い？

まとめに代えて

- セキュリティの評価
  - 暗号の評価とシステムの脆弱性
    - 評価出来る事は一番の信頼！
    - 評価出来ない事は一番の不安！
  - なぜ脆弱性が…
    - なぜWEPは解かれたのか？
    - なぜSSL/TLSは解かれたのか？
      - なぜシステムはこうも脆弱なのか？
    - ついでに
      - SSL/TLSの本当の現状？
      - AESの本当の現状？

無線 LAN 暗号の脆弱性

–WEP の解読と WPA-TKIP の脆弱性、そして暗号を解くとは–

森井昌克（神戸大学大学院工学研究科）

１．はじめに　–暗号を解く（解読）という意味–

昨年 8 月，米国サンタバーバラで開催されていた，暗号に関する権威ある国際会議 CRYPTO2011 のランプセッション（正式な発表ではなく飛び込みの発表，成果報告）にて，事実上の国際標準暗号である AES が解読されたという発表がなされました．このニュースは大きな話題として世界中を駆け抜けました．ほとんどすべての暗号に関わるシステムが，この AES を採用していると言っても過言ではないからです．では 1 年以上たった今，AES は暗号として役に立たず，一瞬にして解読可能になったのでしょうか．決して，そういうわけではありません．やはり以前と同様，AES を解読することは難しいのです．では，CRYPTO2011 での AES 解読成功の発表は間違っていたのでしょうか．これも決して間違っていたわけではありません．解読に成功しているのです．解読に成功したにも関わらず，解読できない？とはどういうことでしょうか．これは暗号の解読と言う意味が暗号研究者，あるいは開発者と，一般の暗号利用者が理解している意味と異なるからです．

無線 LAN 暗号，すなわち WEP，それに WPA/TKIP および WPA2/PSK について，特にその安全性や解読について必ずしも正確に理解されていないことが多いようです．本稿では暗号が解けるということの意味について，特に無線 LAN 暗号の安全性について易しく解説します．

２．暗号解読の意味

現在では，鍵（暗号化するためのそれぞれ利用者、あるいは暗号化するコンテンツ固有のパスワード）以外のすべて，特に暗号化の方法である暗号アルゴリズムは公開し，その安全性を鍵のみに依存させることを前提としています．さらに「選択暗号文攻撃」と言って，どのような暗号文も平文に戻せるという仮定でも安全性を保たなければなりません．しかし，どのような暗号文も平文に戻るのであれば暗号が解けていると言っても過言ではありません．このような強い条件のもとでも，鍵の情報が少しでも漏れないことが暗号の安全性の条件なのです．この安全性が少しでも脅かされた時，暗号の研究者，開発者は暗号が解読されたと宣言するのです．具体的には，上記のような暗号設計者にとって厳しい条件のもとで鍵の情報が 1 ビットでも漏れた場合，その暗号は解読されたと言われるのです．

冒頭の AES については，計算量を $2^{126.2}$ とする鍵導出アルゴリズムが開発され，解読に成功したと報告されたのです．したがって，実際に鍵を求めるためには $2^{126.2}$ の計算量が必要

であり，ブルートフォースアタックに比較して約 $1/3$ の時間で済むことが分かりました．もともと鍵を導出するためには，世界最速のスーパーコンピュータを用いたとしても，数十兆年以上の時間が必要でしたから，その１/３としてもほとんど変わることはありません．実際に鍵を導出すると言う意味ではあまり効果がなかったと言わざる得ないのです．ではなぜ暗号研究者らは解読と言う言葉を使うかと言うと，暗号とは鍵の全数探索よりも効果的な鍵導出アルゴリズムが存在しないものとして考えているからであり，それが暗号の安全性の大前提としているからです．AES は鍵の全数探索よりも効率的なアルゴリズムが発見されたことで解読されたと言われるのです．言わば，今までどのような攻撃に対しても無傷であったのが，今回初めて傷を付けられたことになり，致命傷でないにしても，どのような攻撃にも耐え得る強力な暗号ではない可能性が指摘されたことになります．この数年で AES が無力になる可能性は大きくないですが，数年後には新しい暗号に取って代わることでしょう．

３．WEP に用いられる RC4

【ストリーム暗号】

ストリーム暗号では，暗号化鍵（復号鍵）や初期化ベクトル（IV: Initialization Vector）をシード（初期値）としてキーストリームと呼ばれる任意長の擬似乱数系列を生成します．鍵だけをシードに選ばない理由は，シードが同じならば，同一の擬似乱数系列を発生することとなり，鍵を毎回変更しなければ容易に平文が推定されるからです．つまり同じ平文でも毎回暗号文が変わるような仕組みを作っているのです. このキーストリーム Z と平文 P の排他的論理和をとることで暗号文 C を導出します．また復号の際には暗号文 C とキーストリーム Z の排他的論理和をとることで元の平文 P を得ることができます．ストリーム暗号の擬似乱数生成アルゴリズムは一般に二つの機能から構成されます．一つは暗号化鍵や初期化ベクトルを用いて擬似乱数生成器の内部状態を初期化するアルゴリズム，もう一つは内部状態を更新しながらキーストリームを生成するアルゴリズムです．前者は鍵スケジューリングアルゴリズム（KSA：Key Scheduling Algorithm），後者は擬似乱数生成アルゴリズム（PRGA：Pseudo-Random Generation Algorithm）と呼ばれます．

【RC4】

ストリーム暗号では KSA に共有の秘密とする暗号化鍵，および通常，公開されている IV を入力することで内部状態を初期化します．またその初期化された内部状態を PRGA に入力することでキーストリームを出力します．RC4 は 1987 年に RSA Security 社の Ron Rivest によって開発されたストリーム暗号です．RC4 は開発当初からそのアルゴリズムは非公開とされてきました．しかし 1994 年にインターネット上に RC4 と等価な処理を行うアルゴリズムが RSA Security 社の承諾なく公開されました．RSA Security 社は RC4 のアルゴリズムを現在でも公開していません．この RC4 と等価な暗号化処理を行うストリーム暗号を正式

には Arcfour（Alleged RC4）と呼ぶのですが，混乱を避けるため Arcfour を RC4 と呼ぶことにします．

RC4 の特長として非常に短いコードで記述できる点，ソフトウェア上で非常に高速に動作する点等が挙げられます．WEP だけでなく，サーバ・ブラウザ間通信の標準プロトコルである Secure Sockets Layer（SSL）/Transport Layer Security（TLS）等，様々な標準規格に採用されています．今でも事実上 AES と並んで，よく利用される暗号の一つです．

RC4 の内部状態 2^n 個の要素を持つ配列と 2 個のポインタから構成されています．n は可変の値であり，一般的に $n = 8$ が採用されます．したがって，一般には，1 バイトの配列を 256 個有し，2 個のポインタを用いて，その配列要素を入れ替えていくアルゴリズムになっています．つまり，RC4 の KSA，PRGA はスワップ処理を中心としたアルゴリズムなのです．

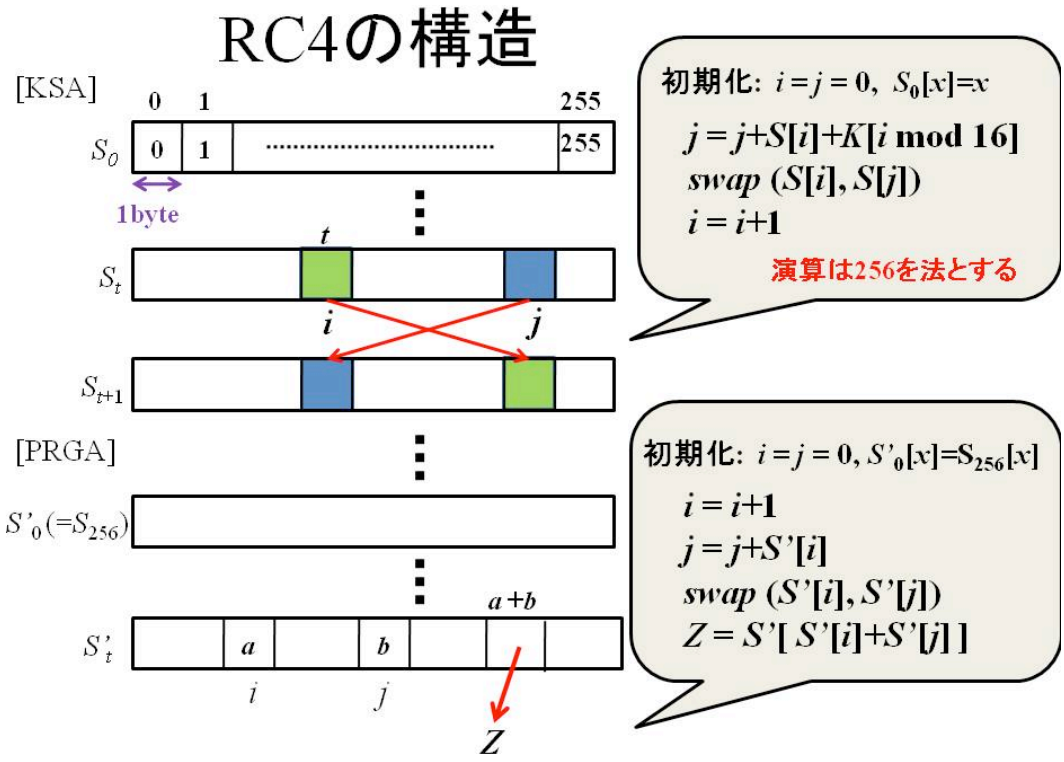

図 1．RC4 の構造

【RC4 の安全性】

RC4 自体の解読法に関しては，鍵の全数探索よりも効率的な鍵導出法が知られているものの，現実的な時間で鍵を導出する方法は与えられていません．RC4 の開発から四半世紀，傷つきながらも十分な安全性を保っているということは大きな評価となっています．我々の研究グループも RC4 の解読に取り組み，キーストリームから内部状態（初期値）を推定する方法，さらに鍵を推定する方法を提案しています．前者では，内部状態である 256 バイトの配列のうち，70 バイト程度が既知であれば，他の 186 バイトを現実的な計算量であ

る2^{30}程度で推定する方法であって，後者は鍵の全数探索よりも効率的な鍵導出方法（計算量は2^{96})を与えています．しかしながら，我々を含めて，RC4 に関しては，キーストリームが既知であるという理想的な条件であったとしても，現実的な計算量（例えば2^{64}程度）で鍵を導出できるところまでは至っていません．RC4 の最大の欠点は鍵と KSA での処理を行った後での初期値との相関性，さらに初期値とキーストリームとの相関性にある．特に初期値とキーストリームの初期の時刻での相関が高いことが問題となっています，

【無線 LAN 暗号方式 WEP】

無線 LAN の性質上，空間を伝搬している信号を誰にも気づかせることなく盗聴することが可能です．特に伝搬範囲を正確に制限することが難しく，利用を想定している範囲外（室外）に信号が伝搬することからその対策が必須となります．信号電力を制御することや電波を遮蔽することは事実上不可能であることから，物理的ではなく，いわゆる論理的に信号を処理する必要があります．暗号化を行って，利用を制限する必要があるのです．このため，提案された暗号化の規格が WEP です．無線 LAN においては当初から数 Mbps という高速な通信を仮定していたことから，暗号化においてオーバーヘッドが許されない，高速に処理可能な暗号方式が望まれました．AES をはじめとするブロック暗号では高速処理という面において十分な性能が得られず，高速処理可能なストリーム暗号の適用が考えられ，当時においてすでに様々な分野で実用化に具されており，特にソフトウェア実装において実績もある RC4 を用いた方式が採用されることとなったのです．

４．WEP とその解読法

【WEP とその脆弱性】

WEP は暗号アルゴリズムとして RC4 を用いているものの，RC4 とまったく同じというわけではありません．WEP では IP レイヤで生成されるパケット毎に生成される鍵（パケット鍵）K を 40 ビット，あるいは 104 ビットの秘密鍵（WEP 鍵）K ’と 24 ビットの初期化ベクトル IV を用いて，その連結 K = IV || K ’として生成します．WEP における IV の役割は以下のとおりです．通常，WEP 鍵は頻繁に更新することはなく，WEP 鍵だけで暗号化した場合，キーストリームは常に同じものとなります．暗号文は平文との排他的論理和で得られることから，キーストリーム自体が類推される可能性が高くなります．特に平文であるパケットでは，IP アドレス等，部分的に固定値を取ることがあり，特にキーストリームの推定からパケット全体を推定することが容易になる可能性があります．したがって，IV を変化させることによって，キーストリームを変化させているのです．IV は平文として，暗号化されたパケットに加えて伝送されます．

WEP と RC4 との相違は秘密鍵の設定方法にあります．WEP は秘密鍵の設定を制限した RC4 なのです．RC4 の脆弱性は WEP の脆弱性そのものになりますが，RC4 に対して運用を脅かす致命的な欠陥は発見されておらず，キーストリームが既知としても現実的には RC4

を解読する，すなわち秘密鍵を導出することはできません．他方，WEP では秘密鍵の先頭 24 ビットが既知であり，かつ 24 ビットという短い IV ゆえ，望みの IV に対するキーストリームを得ることも可能となります．結果的にこの相違点が WEP の脆弱性となり，WEP の致命的な欠陥に結びつくこととなったのです．

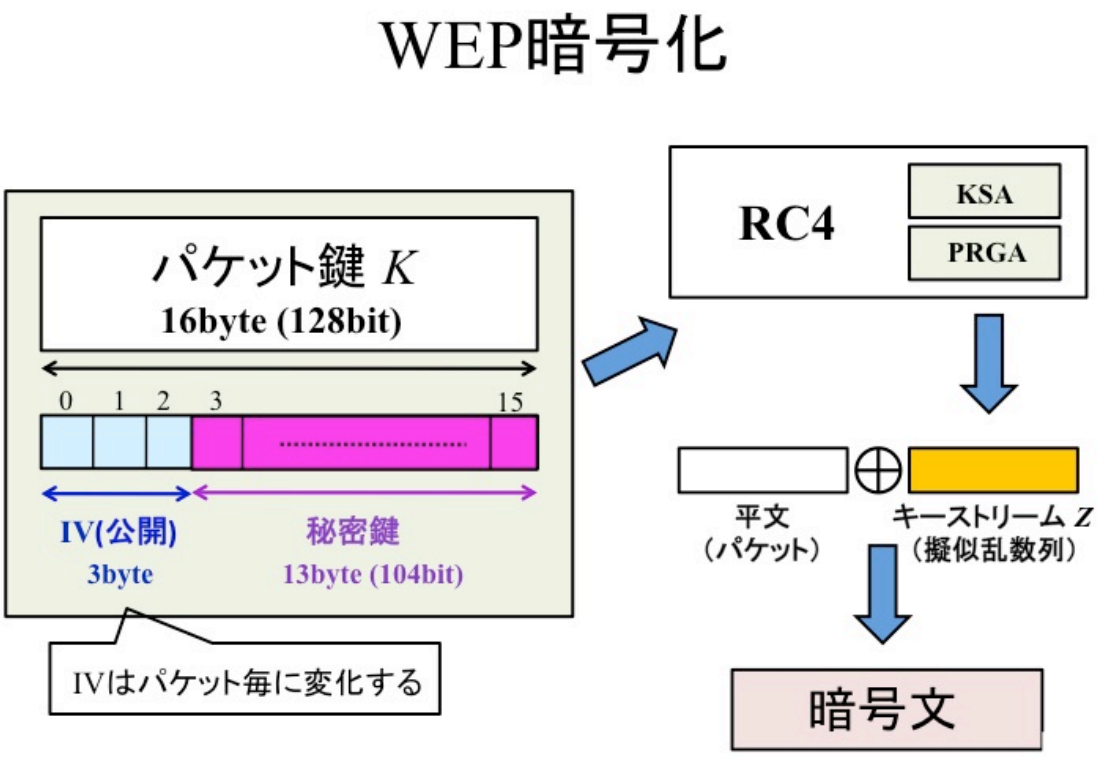

図２．WEP

【PTW 攻撃】

2007 年，ダルムシュタット大学の Tews らによって（このとき，Tews は大学院修士課程の学生），高速に 104 ビットの WEP 鍵が導出できる方法を提案し，実際に解読ツールを作成し実証しました．この攻撃は PTW 攻撃と呼ばれます．PTW 攻撃の原理は，2006 年に Klein によって発表されたキーストリームから鍵を推定するという鍵回復攻撃を発展させたものです．Klein 攻撃は RC4 の内部状態とキーストリームの間の若干の相関を利用するものです．この若干の相関をどのように利用するかによって，攻撃性能が異なります．PTW 攻撃はこの性能を極めて高く上げることに成功したのです．

【PTW 攻撃の改良】

PTW 攻撃には ARP パケットという特殊なパケットを大量に収集する必要があります．したがって一般の通信を短時間の盗聴によって鍵を導出することは難しく，現実的な方法ではありません．PTW 攻撃を改良し，ARP パケットではなく，一般の IP パケットを用い，し

かも収集するパケット数を大幅に減少させる攻撃方法が提案されました．この攻撃法は開発者らの頭文字をとって, TeAM-OK(TeramuraAsakuraMorii-OhigashiKuwakado)攻撃と称されています．攻撃対象のネットワーク環境に寄らず，また相手の IP アドレス等の固有情報を事前に知ることなく，単に WEP によって暗号化された IP パケットを 3 万パケット程度観測することにより，104 ビット WEP 鍵を導出することが可能です．さらに，攻撃対象の IP アドレス等のサイト情報や, WEP 鍵に使用されるパスフレーズが任意の英数字 13 文字に限定される場合は 2 万パケット以下で，104 ビット鍵を導出することが可能です．

【TeAM-OK 攻撃の効果】

TeAM-OK 攻撃によって，IP パケットを 3 万個程度，観測するだけで 104 ビット WEP 鍵を導出することが可能となります．実際，3 万パケット程度であれば，一般家庭で使われる無線 LAN において，動画データ等をダウンロードする場合，十数秒から数十秒です．また，盗聴したパケットに基づく TeAM-OK 攻撃において，計算の中枢は単純な統計処理であり，かつ計算量的に規模も小さく，通常，数秒とかかりません．したがって，パケットを収集し終わってからのオフライン攻撃としては一瞬であり，オンライン攻撃としても現実的な時間で終了します．このように，TeAM-OK 攻撃は実際にも十分現実的な攻撃法であり，もはや WEP は暗号と言えないのです．現在、この鍵導出に必要なパケット数を減らす研究も続けられており、1 万パケット以下でも導出可能という報告もあります。

【WEP はなぜ解読されたのか】

WEP は無線 LAN の標準規格として開発された無線 LAN 暗号化システムです．十分に検討された規格であるはずですが，実際，数年も経たないうちに脆弱性が指摘され，それから間もなく，WPA という新しい暗号システムへの変更が暫定的に推奨されるに至りました．なぜ，WEP は十分な安全性をもった暗号システムとならなかったのでしょうか．暗号の利用方法に脆弱性を有していたからなのです．鍵の運用やアルゴリズムの実装を含めて，暗号システムであり, 実際に利用される暗号となるのです. 無線 LAN の規格である IEEE802.11 を定める際に，高速な通信を求めるあまりに，その実装にとって負担とならない暗号システムとなるだけでなく，暗号アルゴリズムにも高速化，軽装化が望まれたのです．その結果が RC4 の採用だったのです．当時から非常に高速かつプログラムサイズ等を含めて軽量な暗号として多くの通信システムおよびデータの秘匿に用いられ実績がありました．しかし，RC4 に対しては 128 ビット鍵が推奨され，鍵の冒頭 24 ビットを公開，かつ残りの 104 ビットを固定して，キーストリームを発生させることを想定していません．つまり，RC4 を利用するといいつつ，結果的に不正に改良した暗号となっていたのです．暗号システムを構築する場合，利用する暗号に対して変更を加えることなく，また鍵の運用や実装に関しても安全性を脅かすことのないように十分に考慮して設計する必要があるのです．たとえば，米国商務省が選定し，現在でも米国標準暗号である AES に関しても，その暗号を利

用しているからといって，必ずしも安全，すなわち解読困難な暗号システムとは限らないのです．AES の暗号アルゴリズムに変更を加えていないか，推測可能な鍵を設定する仕様になっていないか，あるいはハードウェアおよびソフトウェアでの実装において，鍵の情報が漏えいする仕様になっていないかを十分検討する必要があるのです．近年では，暗号アルゴリズム上の脆弱性だけでなく，それをハードウェア実装した場合での脆弱性について盛んに研究が進められています．例えば電力解析攻撃や故障利用攻撃（fault-based attack）という攻撃方法です．ソフトウェア実装した場合でも，キャッシュ攻撃等が存在し，安易な実装は暗号システムの強度を著しく弱める結果となることが報告されています．

５．むすび

現在，公開されている Backtrack5 での無線 LAN 暗号解読ツールには PTW 攻撃の改良版が搭載され，容易に実装･運用可能です．したがって，WEP については容易に鍵を導出することが可能です. WEP は名実共に, 理論的にも現実的にも解読可能な暗号システムなのです. WEP の後継として，WPA/TKIP や WPA2/PSK 等が推奨されています．WPA/TKIP は WEP を改良した方式であり，無線ルータ等の大幅な変更なく利用できる暫定的な無線 LAN 暗号方式です．この WPA/TKIP については鍵を導出するという意味での解読方法は知られていません．しかしながら不正なパケット（たとえばシャットダウンさせるような）を受け取る等の脆弱性が知られており，必ずしも安全ではありません．WPA2/PSK については AES を利用する等，大幅な改良が加えられており，十分安全性を保て得る無線 LAN 暗号方式となっています．しかしながら WPA2/PSK を利用しているからといって無条件で安全であるとは言えません，例えばマスターキーと呼ばれる，初期設定用の鍵を類推されやすい文字列や数字のみ，もしくは英単語のみに設定されている場合は容易に鍵を導出される可能性があります．それは WPA2/PSK の安全性の問題ではなく，運用の問題です．ブルートフォースアタックと呼ばれる鍵の全数探索手法で解かれる可能性があるのです．GPU（画像処理プロセッサ）の演算機能を利用して、高速に WPA2/PSK のブルートフォースアタックを行うシステム Pyrit が公開され話題となりました。しかしながら Pyrit を用いたとしても、高々毎秒、10 万個から 100 万個の鍵しか確かめることはできません。そのような GPU を搭載したコンピュータをたとえ 100 万台同時に使ったとしても、注意深く設定した 128 ビットの鍵を求めるためには、1,000 京 (10^{19}) 年以上かかるのです。無線 LAN に限らず，その安全性を十分に確保するためには，どのような暗号化手法が用いられ，どのような条件が必要かを理解しなくてはなりません．

マルウェアの脅威　--PC 遠隔操作の波紋と恐怖--

神戸大学大学院工学研究科　教授　森井昌克

PC 遠隔操作ウイルスの波紋

昨年８月と９月，インターネットの掲示板を利用し，飛行機爆破等の犯行予告を行ったとして，それぞれ大阪府と三重県の男性が逮捕，起訴された．それまで掲示板を利用しての犯行予告自体は珍しい事件ではなく，事件性が疑われる件を含めれば年間百件以上あり，その内，数十件は立件され，ほとんどが逮捕，起訴に及んでいる．しかしながら，１０月になって驚くべき展開を迎えたのである．その２人が利用したパソコンを精査した結果，本人の意思による犯行予告の書き込みではなく，そのパソコンが遠隔から操作され，第三者がそれらの書き込みを行った可能性が高いことが判明し，釈放されたのである．更にその後，真犯人を名乗る人物から犯行声明があり，立件されていない事件を含め，合わせて１３件の犯行予告が，パソコンの遠隔操作によるものであると明らかになった．上記の２人以外にも，更に２人，合わせて４人の誤認逮捕が明確になったのである．この遠隔操作にはウイルスと称されるマルウェア（不正なプログラム）が使われた．人体に感染するウイルスと同様，パソコンがそのウイルスに感染すると，すなわち不正なプログラムを意図せず組み込まれると，異常な動作を引き起こす事になる．その一つの異常動作が遠隔操作なのである．遠隔操作ウイルスによって，誰でもが無実の罪を着せられる可能性が現実のものとなったのである．また，農林水産省のパソコンが外部からサイバー攻撃と呼ばれる不正アクセスを受け，機密文書が外部に流出した可能性があると今年になって報じられた．このようなサイバー攻撃は今年に始まったことではなく，一昨年の９月，三菱重工に対するサイバー攻撃が報じられ，やはり企業秘密が外部に漏えいした可能性が報じられている．その後，三菱重工だけでなく，国内の主要企業や総務省，参院議員会館，さらに JAXA 等でもサイバー攻撃を受け，パソコンに侵入し，情報改ざんや情報漏えいが行われた可能性が報告されている．

サイバー攻撃には一般にマルウェアが利用される．このマルウェアの歴史は古く少なくとも約３０年前から存在し，２０年以上前から，国産化とその感染が

報告されている．本稿ではこのマルウェア，特に遠隔操作を可能にするコンピュータウイルスとその脅威について述べる．

コンピュータウイルスとは

マルウェア，特にコンピュータウイルスの歴史は古く，その対策も十分考慮されている．しかし，個人のパソコンもウイルス対策ソフトが導入され，サーバにおいても対策が取られているものの，現在でもその脅威はいささかも衰えていない．

そもそもコンピュータウイルスとは何なのか．自然界のウイルスと根本的に違うところは，例外なく人の意志で作られているということである．これが恐らく永遠に脅威となる原因であろう．１９９０年に当時の通商産業省がコンピュータウイルス基準を定めている．

第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり， 次の機能を一つ以上有するもの． (1)自己伝染機能：自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより，他のシステムに伝染する機能．(2)潜伏機能：発病するための特定時刻，一定時間，処理回数等の条件を記憶させて，発病するまで症状を出さない機能．(3)発病機能：プログラム，データ等のファイルの破壊を行う，あるいは設計者の意図しない動作をする等の機能．この３つの機能の一つでも当てはまればコンピュータウイルス（以下，ウイルス）と呼ばれる．

２１世紀になって，ウイルスは大きな転換点を向かえる．それは自己伝染機能から発病機能への重点の遷移である．１９８０年代から９０年代にかけては，如何に広範囲に感染させるかによって，その作者の能力，利用者の存在の誇示することを目的とした．発病機能自体は特別なメッセージや画像を画面に表示する，あるいはキー入力ができない等の現象が主であった．感染事実を誇示するという目的から，被害にあったことが明白となり，事後対策を立てることも容易なのである．

最近のウイルスは自己伝染機能においても，ＯＳやソフトウェアのセキュリティホールを巧みに利用し，かつてないほど強力な伝染機能を有しているものの．それ以上に発症機能が脅威となっている．更に発症に対する秘匿機能も有している．つまり感染が容易に検知出来ないのである．その脅威となるべき発症機能が情報の収集，送信であり，後に述べる遠隔操作である．情報収集では，情報が自動的に選別評価され，ネットワークを介して悪意のある第三者に送られる．その事実を隠すために，パソコンや利用する人の状況に合わせて発症をコントロールする機能を有し，容易には感染どころか，情報漏えいの事実も発見出来ないのである．

遠隔操作を可能にするボットとは

ボット(bot)とは外部からの指示に従って，悪意ある動作を行うプログラムを指し，ウイルスの発症後の機能であって，感染を含め，その動作自体を秘匿する機能を有している．昨年の「遠隔操作ウイルス」はこの一種の発症機能であり，必ずしも珍しくはない．またボット自体も１０年近く前から存在し，５年ほど前には国内でも広く感染した事実があり，それを駆除するための対策が進められた．

ボットの目的は感染したパソコンの遠隔操作であるものの，具体的には，そのパソコンから DDoS(Distributed Denial of Service attack)攻撃と呼ばれる，特定のサーバ（Web やメール，さらにデータベースを運用するためのコンピュータ）等にアクセスする事によって，そのサーバの処理能力を超える負荷をかけ，サービス不能にする攻撃を行う．１台のパソコンからだけのアクセスであればサーバにとっては問題にならないものの，数万台，数十万台のパソコンを一度に操る事によって，大量の負荷をかける事が可能となる．ボット機能を有するウイルスに感染したパソコン群をボットネットと称し，遠隔操作を行うもの（羊飼いを意味するハーダーと呼ばれる）はボットネットを自在に操る事ができる．巨大なボットネットはその悪用によって，重要な社会インフラを機能不全におとしめる可能性があり，その対策が国家レベルで行われている．また，世の中で流通しているメール総数の９０％以上が迷惑メールと言われるが，その迷惑メールを大量に発信する手段として，ボットネットが用いられる．すなわち，大量のパソコンを同時に操作し，そのパソコンから迷惑メールを発信するので

ある．このボットネットは以前に比較すれば，幾分減少傾向にあるものの，今なお，密かに巨大なボットネットが運用されている．

むすびに代えて　--サイバーテロの脅威--

ウイルスの作成や感染（流布）の目的は，当初，その誇示が目的であると述べた．現在では不正な利益誘導が目的であり，その手段として，個人の銀行口座情報やカード番号，あるいは企業の機密情報の搾取，更に企業活動の妨害，脅迫，迷惑メールの配送等の犯罪行為への加担が行われている．もはやその影響は重要な社会インフラを脅かすまでに至っていることから，サイバーテロと呼ばれている．遠隔操作ウイルスによる犯行予告では，いとも簡単に，「なりすまし」に成功し，悟られる事無く，無実の罪をなすり付け，誤認逮捕に誘導した．今回，犯人からの犯行声明によって短期間での限られた件数となったものの，ボットネットのように大規模な数のパソコンを操作し，今回以上の社会的混乱を引き起こすことが考えられる．対策の第一歩はウイルス感染を防ぐ事にあり，ウイルス対策ソフトの導入は必須である．しかしながらウイルス対策ソフトですら完璧な対策ではなく，ウイルス感染の可能性は０ではない．自然界のウイルス感染としてなじみ深いインフルエンザに対して，予防接種としてのワクチン投与が有効であるとされる，しかしながら完全に防ぐ事は出来ず，感染した場合，早期発見とその事後処置が重要である．同様に，パソコンやネットワークでも，日頃の管理を十分行い，感染した際の対処法を予め想定して運用すべきである．