話　題

パソコンセキュリティ，はじめの一歩

橋本　清治[*1]・金子　敏明[*2]・村上　直[*3]・中村　貞次[*4]・湯浅　富久子[*5]

Personal Computer Security: The First Step

Kiyoharu HASHIMOTO[*1], Toshiaki KANEKO[*2],
Tadashi MURAKAMI[*3], Teiji NAKAMURA[*4] and Fukuko YUASA[*5]

Abstract

We present some tips to protect a personal computer showing examples of security incidents experienced in KEK.

1. はじめに

大学共同利用機関法人，高エネルギー加速器研究機構（以下，KEK）は，つくば研究学園都市の北に位置する研究所です．職員数は 800 人程度ですが，加速器科学のさまざまな分野の研究が進められており，来訪者の数は年間１万人を超えます．著者らが属する計算科学センターは，計算機ネットワークのインフラを運用管理していますが，研究・業務がスムーズに継続していくようコンピュータ・ネットワークに関わるセキュリティを維持していくことも求められています．これは，インターネットを通して私たちが向かい合う人々のなかに，普段接している普通の人だけではなく，世界中のどこにいるかわからない，プロの犯罪組織もまじってきているからです．犯罪組織のターゲットは，世界中の一般の人で，少しでもすきがあればつけ込み利用しようと攻撃してきます．具体的には，私たちが毎日パソコンで行っている，メールを読む，Web ページを見る，情報を交換する，サーバへログインするなどの操作が狙われています．ここでは，KEK で実際におこったセキュリティ事例をあげ，それに対応するための方法を紹介します．

2. メールを読むときに

KEK にもフィッシングメール，詐欺のメール，ウィルス付きのメール，スパムメール，差出人が嘘のメールなどが毎日数多く送られてきています．これらのあやしいメールの多くはメールサーバやパソコンのメールソフトである程度は除去されますが，それでもいくつかは個々の人のメールフォルダまで届きます．あやしいメールは無視することが一番の対策ですが，なかには判断を誤ってひっかかってしまうことがあります．

2.1 フィッシングメール

フィッシングメールとは，実在する銀行，クレジットカード会社，大学の計算センターなどインターネットでさまざまなサービスを提供しているところを装い，パスワードなどの重要な情報を盗み取ろうとするメールです．「フィッシング」は，英語では「phishing[†1]」と書きます．2010 年の夏，KEK では計算科学センターが恒例の年度更新作業をほぼすませた頃にこんなフィッシングメールが KEK のメールサーバの利用者にだされました（**図 1**）．

図 1 に示したように，フィッシングメールは，あなたがサービスを継続して利用したいのなら

- ユーザ名やパスワードをメールに書いていますぐ返信しなさい
- メールにある URL[†2] にアクセスしてユーザ名とパスワードをいれなさい

などと誘いかけてきます．メールにパスワードを書くように要求することは，まともなサービスならばもはやあり得ないことです．こんなメールを受け取ったら，

[*1] 高エネルギー加速器研究機構・計算科学センター（E-mail: kiyoharu.hashimoto@kek.jp）
[*2] 高エネルギー加速器研究機構・計算科学センター（E-mail: toshiaki.kaneko@kek.jp）
[*3] 高エネルギー加速器研究機構・計算科学センター（E-mail: tadashi.murakami@kek.jp）
[*4] 高エネルギー加速器研究機構・計算科学センター（E-mail: teiji.nakamura@kek.jp）
[*5] 高エネルギー加速器研究機構・計算科学センター（E-mail: fukuko.yuasa@kek.jp）

```
差出人: KEK Active! mail <00002010@att.net>
日時: 2010 年 8 月 10 日 7:55:59:JST
宛先: undisclosed recipients: ;
件名: Spam?* E-Mail Account Maintenance

We would like to inform you that we are currently carrying
out scheduled maintenance and upgrade of our account
service and as a result of this your accounts have to be upgraded.

We are sorry for any inconvenience caused.

To maintain your account, you must reply to this email immediately
and enter information below:

USER ID:::.....................
Password:: ....................

Failure to do this within 48 hours will immediately render your
account deactivated from our database.

Thank you for using our Services!

"WEBMAIL SUPPORT WEBMAIL ACCOUNT
ABN 31 088 377 860 All Rights Reserved.
E-Mail Account Maintenance
```

図 1　フィッシングメールの例

返信せずに無視してください．もし判断に迷う場合には「メールでパスワードを本当に要求しているのか」ということを，サービスを提供している人や団体などに電話や FAX などで問い合わせします．決してそのメールに返信してはいけません．返信すれば，相手に自分の情報を与えてしまうことになります．

フィッシングでは，メールにある URL が一見正しそうに見えても，クリックすると書いてある URL とは別の偽装サイトに誘導されることもあります．メールに書いてある URL は安易にクリックせず，ブラウザのアドレス欄に自分で URL を入力してアクセスするようにします．できればそのサイトの URL を下から削っていったり，トップから探してメールと同じ内容の案内を探すことも有効です．

2.2　詐欺メール

詐欺メールの内容は非常に巧妙になってきています．現実の世界でも多くの人がだまされている「振り込め詐欺」を，電話でなくメールを使って行おうとする犯罪者もいます．たとえ，親しい人からであってもこんな内容のメールはあやしいです．

- 出張先で財布をスリにすられた．幸いパスポートは盗られなかったけれど，クレジットカードを盗られてしまった．
- ホテルに宿泊代を払うのにお金が足りない．
- 戻ったらすぐ返すので，お金を貸してもらいたい．
- このメールを読んだらすぐ返信してほしい．

こんなメールを受け取ったときは，差出人に口頭，電話，FAX で直接連絡して確認します．たとえ，差出人が上司や重要な取引先の担当者であってもです．このように人の心理の裏をかくような方法を，セキュリティ用語では，ソーシャルエンジニアリング[†3] と言います．急いでいるときなどに引っかかりやすいので，あやしいメールを受け取ったら少し間をあけて考えるなど落ち着いて対応しましょう．

2.3　あやしいメールの見分け方

これまで，あやしいメールの例を紹介しました．あやしいメールはたいてい嘘の差出人から出されます．差出人を偽ってメールをだすのは簡単で，多くの人がインチキ差出人からのメールをそれとは知らずに受け取っているのではないでしょうか．自分が差出人になっている，送った覚えのないメールがエラーとして返って来ることがありますが，それも誰かが自分を装っているせいです．残念ながら，これを止めさせることはできません．宛先についても同様で自分宛のメールでないのにどうしてメールがくるのか，と思ったことはありませんか．

[†1] fishing（釣り）のハッカー的なスラングといわれているが諸説あるらしい（ja.wikipedia.org より）．
[†2] Unified Resource Locator の略．HTTP プロトコルでは，http:// あるいは https:// で始まり Web ページの場所を表す．
[†3] ソーシャルハッキングとも言う．

すぐに差出人を嘘と見破れる場合もありますが，なかにはむずかしい場合もあります．こんなときに助けになるのがメールヘッダです．メールは，本文とメールヘッダから構成されています．メールヘッダをみるとメールがどのようにして運ばれてきたのかある程度わかります．多くのメールソフトの通常の設定では，宛先，差出人，件名，日時と本文しか見ませんので，メールヘッダの全てをみるには，操作が必要になります．その操作はメールソフトによって異なりますが，Thunderbird の場合のメールヘッダの表示方法を紹介します（**図 2**）．メールのメッセージのすべてを表示させると普段はみえないメールヘッダをみることができます．**図 3** には**図 1** のメールのメールヘッダを示しました．**図 3** をみると，本当にメールをだしたのは，KEK の計算科学センターではないことがわかります．ただし，攻撃者はメールヘッダを書き換えることもしますので，迷うような場合には自分一人で判断せずにメールヘッダを添えて専門家に相談することをお勧めします．

3. Web ページを見るときに

KEK で発生したウィルス感染の被害は 2008 年くらいには沈静化していましたが，2009 年くらいから再び感染件数がふえてきました（**図 4**）．以前はメールに添付されているファイルをクリックしたり，パソコンの OS の弱点を放置しておいたためにウィルスに感染してしまうことがよくありました．最近は，Windows アップデートを自動で行いアンチウィルスソフトを動作させている人が増えたため，ウィルスに感染させる手口がかわってきました．たとえば KEK では，次のようなことがありました．

- チャットをしていてそこについていた URL をクリックしたら突然おかしなウィンドウが現れ，ウィルスに感染した．
- Web をみていたらアンチウィルスソフトウェアを導入しなさい，というウィンドウがでて従ったら感染した．
- 国際会議に出席するため，おすすめのホテルのホームページを見ようとしたらパソコンの動作が変になった．

ウィルスを配る攻撃者は，昔ながらの方法の効果が減ってきていることを心得ていて，弱点をもつ Web サイトを乗っ取り，そこにウィルスを潜ませておくように手口をかえてきています．アクセスにきた人にクリックさせてウィルスをダウンロードさせたり，**Web ページを見ただけでも**パソコンにウィルスを送り込み

図 2 Thunderbird でのメールヘッダの表示方法：「表示」をプルダウン→ヘッダ→すべて

感染させてしまうようにもなってきています．代表的な攻撃として，「ガンブラー」というのがあります．2009 年末から現在にかけて日本では，「ガンブラー」による被害が数多く報告されています．KEK も例外ではありませんでした．「ガンブラー」の攻撃は，

1. 攻撃者は，なんらかの方法で Web サイトを管理する人のパスワードを盗む．
2. 盗んだパスワードで Web サーバに不正ログインする．
3. Web ページを改ざんし，仕掛けをつくる．
4. Web ページを見た人が，悪意のある Web サイトへ飛ばされる．
5. 悪意あるサイトからウィルスを送り込まれる．パソコンに弱点があれば感染する．
6. 感染したパソコンからパスワードなどの重要な情報を盗み取り利用する．

を繰り返し，被害を拡大していきます．「ガンブラー」には多くの変種があり，この連鎖を断ち切るのは困難です．

3.1 Web サイトに仕掛けられた攻撃への対応

パソコンで最新のウィルス定義ファイルを用いてアンチウィルスソフトを動かしていて，Windows アップデートも自動設定になっているのになぜ感染してしまうのでしょうか．それは，Web ブラウザと連動して動く JAVA，Adobe Reader，Adobe Flash Player，Web ブラウザ自身などの弱点が狙われて，パソコンを勝手に操作されウィルスを送り込まれてしまうからです．

このような攻撃には，パソコンで動くアプリケー

```
 1: 差出人:  00002010@att.net
 2: 件名:  Spam?*E-Mail Account Maintenance
 3: 日時:  2010 年 8 月 10 日 7:55:59:JST
 4: 宛先:  undisclosed recipients: ;
 5: 返信先:  XXX@ml.post.kek.jp
 6: Return-Path:  <YYY@ml.post.kek.jp>
 7: Delivered-To:  ZZZ@post.kek.jp
 8: Delivered-To:  XXX@ml.post.kek.jp
 9: Received:  from mls01 (mls01 [130.87.45.147]) by mbx00 (Postfix)
    with ESMTP id 9113720EE; Tue, 10 Aug 2010 07:56:01 +0900 (JST)
10: Received:  from ml.post.kek.jp (loopback [127.0.0.1]) by mls01
    (Postfix) with ESMTP id 3B555117B; Tue, 10 Aug 2010 07:56:01 +0900
    (JST)
11: Received:  from mip01.post.kek.jp (mip01 [130.87.45.173]) by mls01
    (Postfix) with ESMTP id AAAB3115F for <XXX@ml.post.kek.jp>;
    Tue, 10 Aug 2010 07:56:00 +0900 (JST)
12: Received:  from n2-vm1.bullet.mail.gq1.yahoo.com ([67.195.23.155])
    by mip01.post.kek.jp with SMTP; 10 Aug 2010 07:55:59 +0900
13: Received:  from [67.195.9.81] by n2.bullet.mail.gq1.yahoo.com with
    NNFMP; 09 Aug 2010 22:55:59 -0000
14: Received:  from [98.137.27.218] by t1.bullet.mail.gq1.yahoo.com
    with NNFMP; 09 Aug 2010 22:55:59 -0000
15: Received:  from [127.0.0.1] by omp128.mail.gq1.yahoo.com with
    NNFMP; 09 Aug 2010 22:55:59 -0000
16: Received:  (qmail 43607 invoked by uid 60001); 9 Aug 2010
    22:55:59 - 0000
17: Received:  from [82.128.61.231] by web180204.mail.gq1.yahoo.com
    via HTTP; Mon, 09 Aug 2010 15:55:59 PDT
18: Message-Id:  <114353.43021.qm@web180204.mail.gq1.yahoo.com>
```

図 3　メールヘッダの例：行 17 から web180204.mail.gq1.yahoo.com でメールが受け付けられたこと，続いて omp128.mail.gq1.yahoo.com（行 15）→・・・→ ml.post.kek.jp（行 10）→ mls01（行 9）と順に中継されたことがわかる

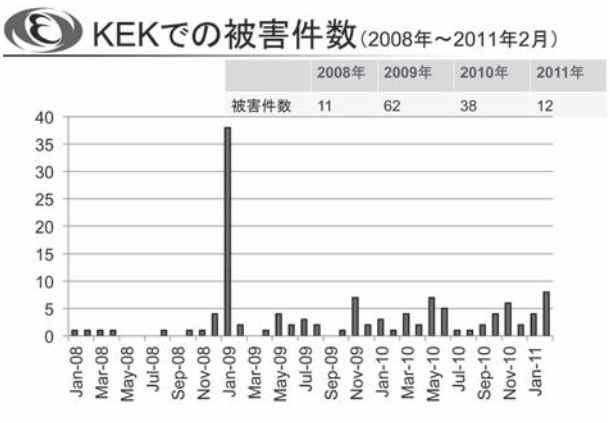

図 4　KEK でのセキュリティ被害発生状況

ションソフトウェアを常に最新にしておくことが有効です．たくさんあるアプリケーションのそれぞれについて最新かどうか判断するのは，手間がかかります．そんな時には，IPA 情報処理推進機構が提供している**「MyJVN 脆弱性対策情報収集ツール」**を利用すると便利です．これは，パソコン上にインストールされたソフトウェア製品のバージョンを容易にチェックする等の機能を提供する仕組み（フレームワーク）です．Web ブラウザで http://jvndb.jvn.jp/apis/myjvn/ にアクセスして使います．

また，アンチウィルスソフトの設定で，ダウンロードされてくるファイルを動的にチェックするようにするのも一定の効果があります．

4.　USB メモリで情報交換

2008 年 10 月 20 日から 23 日にかけてインドのニューデリーで開催された加速器の会議のあと，会議主催者から「会議中に使用された USB メモリにウィルス感染があったので確認して欲しい」という注意喚起のメールが参加者にだされたことがありました．ある参加者がこの会議でだけ使用した USB メモリを大学にもちかえったところ，感染活動が発見されたので，会議の主催者に連絡したというのが経緯です．

この会議にかぎらず USB メモリを媒介とする次のような事例が KEK でも頻繁に報告されています．

- 国際会議の会場で発表用のパソコンに持参した USB メモリを差し込んでプレゼンテーションのファイルをコピーした後，USB メモリを自分のパソコンに差し込んだらパソコンの様子がおかしくなった．
- 実験ビームラインに設置されているパソコンが動作

がおかしい．調べてみたらウィルスに感染していた．どうも前にこのパソコンを使っていた人が差し込んだUSBメモリ[†4]がウィルス付きだった様子．

残念ながら，現状ではウィルス感染を完全に防ぐことはできません．アンチウィルスソフトの製造会社は発見されたウィルスを解読して，ウィルスを判定するため「ウィルス定義ファイル」を作ります．アンチウィルスソフトはこの「ウィルス定義ファイル」を取り込んだあとに，ウィルスと判定することになります．ウィルスが作られてから一定の時間がたたないとパソコンには免疫力ができません．特にUSBメモリを通して感染するウィルスの場合，「ウィルス定義ファイル」が間に合わなかった事例が多く報告されています．時間がたって「ウィルス定義ファイル」が更新されたあとウィルス感染がわかることもよくありますので，定期的なウィルススキャンは欠かせません．すぐできる予防として，USBメモリを差し込んだときに勝手にウィルスが活動しないよう自動実行の機能を停止することがあります．人にファイルを渡すだけなら書き込み禁止にする（書き込み禁止のスイッチのついたUSBメモリもあります）とか，人にUSBメモリを貸した後にLinuxなどの別のOSから正常かどうか見てみるのは有効です．

Windowsパソコンでの自動実行を禁止する方法は，Microsoftのサポートオンラインページ`http://support.microsoft.com/kb/971029/ja`に掲載されています．

5. パスワードについて

KEKでは，研究グループが運用するSSH[†5]サーバのパスワードがとられてサーバを不正に利用されるということが毎年発生しています．インターネットのどこからもSSHログインを受け付けるようにしているサーバは，何万，何十万回という規模でSSH辞書攻撃を受けています．SSH辞書攻撃は，システムにありそうなユーザ名とパスワードの組を機械的に次から次へと試します（日本人名の辞書も出回っています）．うまくログインできたら不正なツールキット（裏口をつくる，コマンドを置き換える，不正な行動の指令を受けるためのソフトなどの一式）をもってきます．このような攻撃が成功する原因は，パスワードがユーザ名と同じだったり，せいぜいユーザ名に1文字加えただけだったりすることがほとんどです．

現在は，SSHサーバへのログインパスワード，Webアプリケーション利用時のパスワード，パソコンのパスワードなどなど多くのパスワードを管理していかなければならないのですが，いずれも推測されにくいものとし，安全に保管していかなければなりません．なぜなら，パスワードは他人から自分の情報を守るための唯一の手段だからです．キャッシュカードにたとえるなら，カード本体は銀行に預けておいて暗証番号だけで現金を引き出しているようなものです．自分以外の誰かが利用したような気がするなど変だと思ったら，すぐパスワードを変え，管理者に連絡します．きちんとしたシステムならば，いつでもパスワードは自分で変えることができて，管理者も知ることができません．

一部繰り返しになりますが，まとめます．

- 暗号化されていないものにパスワードは書かない．特にメールには書かない．
- Webで入力するときはURLの先頭に注意します．URLの先頭が`https://`ならば暗号化されていますが，`http://`なら暗号化されていません．
- ユーザ名とパスワードは同じにしない．ユーザ名に2，3文字だけ変えたり加えたりするのも危険です．辞書にあるような普通の単語（英語でも日本語でも）だけのパスワードは使わない．
- あやしいと思ったらパスワードを変えます．
- 人にパスワードは教えない．どうしても教える必要があるときは，普段使っているものを別のものに変えてから使ってもらい，用事が終わったら元に戻します．

6. フリーサービスの利用

インターネットからの攻撃によるセキュリティ被害とは別の話ですが，Google，Yahoo，Microsoftなどがアプリケーションサービスプロバイダとして提供する最近話題のフリーサービスについて触れます．

これらのサービスでは，使い勝手のよいWebメール，大容量ファイルの保存，スケジュール管理など便利な機能が使えます．世界中を飛び回っている研究者，技術者には大変魅力的なサービスです．しかし，これらのサービスはクラウド技術を用いて実現されていることが多く，やりとりした情報がどこに保存されているのか，どのように扱われるのかなどを特定しにくいという問題点があります．電子データは容易にコピー

[†4] USBハードディスクの場合もあります．
[†5] Secure SHellのこと．通信が暗号化されたリモートログインサービス．SSHでは，パスワード認証，公開鍵認証などが選択できる．

でき劣化しないという特徴があります．一旦預けた情報は，バックアップなどを含めて完全に消去することは不可能です．

特に，サービスがフリー（無料またはきわめて低価格）の場合には，情報を渡してサービスを買っていると考える必要があります．フリーサービスの利用を始める前には，利用規約をよく読んで慎重に検討する必要があります．フリーサービスを研究や業務で利用する場合には，次のことを確認してください．

- ライセンス上，使い方に問題はありませんか．
- 機密性のある内容（例えば，契約にかかわる内容など）をやりとりしていませんか．
- 個人情報を含んでいるファイル（例えば，学生の成績など）をやりとりしていませんか．
- 知的財産権を侵害するおそれのあるファイル（例えば，製作図面など）をやりとりしていませんか．
- サービスを利用するときのパスワード入力は，暗号化通信になっていますか．
- サービス提供者への連絡方法，パスワードのリセットの手続き方法，データ削除についての取り扱いなどの手続きはどうなっていますか．

7. ま と め

これまで，KEK で発生したセキュリティ事例を紹介しそれにどのように対応したらよいのか述べてきました．攻撃者は，インターネットを利用するすべての人をねらっていますので，KEK で発生するセキュリティの問題は，すべての組織に発生する可能性があります．ここで紹介した方法が，読者のパソコンセキュリティのはじめの一歩として参考になれば幸いです．

パソコンを守る方法は時とともにかわるのでやっかいですが，現時点での被害をへらすための５つの心がけと役に立つ Web サイトの URL を示し，この文章のまとめとします．

被害をへらすための５つの心がけ

1. あやしいメールの本文中にある URL はクリックしない．あやしいメールを受け取り判断にまよったら相談をする．
2. パソコンの状態を安全に保つ．
   （Windows アップデートの自動設定，アンチウィルスソフトの導入と「ウィルス定義ファイル」の自動アップデート，JAVA，Adobe Reader，Adobe Flash Player，MS Office などの広く使われているソフトを最新にします）．
3. USB メモリの自動実行を禁止する．
4. 定期的にウィルススキャンをする．
5. パスワードは推測されにくいものとする．

参考となる Web サイト

- **JPCERT/CC：**`http://www.jpcert.or.jp/`
  JPCERT コーディネーションセンター（JPCERT/CC）は，インターネットを介して発生する侵入やサービス妨害などのコンピュータセキュリティインシデントについて，日本国内のサイトに関する報告の受け付け，対応の支援，発生状況の把握，手口の分析，再発防止のための対策の検討や助言などを，技術的な立場から行なっています（上記サイトより部分的に抜粋）．
- **IPA 情報処理推進機構：**`http://www.ipa.go.jp/`
  IPA（独立行政法人情報処理推進機構）は，1970 年に設立された特別認可法人「情報処理振興事業協会」を前身として，2004 年に発足．現在の活動は，「情報セキュリティ対策」「ソフトウェア・エンジニアリング」「IT 人材の発掘・育成」「オープンソフトウェア」の 4 つのカテゴリーを重要領域としてとらえ，事業の柱にしています（上記サイトより部分的に抜粋）．
- **サイバークリーンセンター：**`https://www.ccc.go.jp/`
  サイバークリーンセンターは，インターネットにおける脅威となっているボット（上記サイトの「ボットとは」を参照してください）の特徴を解析するとともに，ユーザのコンピュータからボットを駆除するために必要な情報をユーザに提供する活動を行っています（上記サイトより部分的に抜粋）．
- **総務省「国民のための情報セキュリティサイト」：**
  `http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.htm`
  総務省が提供する情報セキュリティのための Web サイト．役割に応じた対策と実践をダウンロードできる．