ネチケット
（Netiquette；ネットワーク・エチケット）

2016年1月12日

KEK 共通基盤研究施設 計算科学センター
八代 茂夫

ネット利用の心構え

- ネット犯罪の被害に会わないようにする
- 相手に対する思いやり
  - 意思の疎通
  - 誤解を生まない、不快にさせない、余計なことでわずらわせない
- 個人情報を守る

今回の内容

- 電子メイルの作法
- パスワードの管理
- Webの注意点と作法
- 個人情報
  - 以下のURLからダウンロードできます。
    - http://research.kek.jp/people/yashiro/html/gijyutsu.html

文章を書く心がけ

- **「結城浩の心がけ」を一読することをお勧めします。**
  - **言葉づかい、表現方法、**
  - **http://www.hyuki.com/writing/**
- **特に、**
  - **技術系メーリングリストで質問するときのパターン・ランゲージ**
  - **メールを書く心がけ**
  - **Webページを作る心がけ**
  - **文章を書く心がけ**

パスワード

KEKのシステムのアカウント(1)

入所後の早い時期に入手するであろうアカウントを羅列します。
その他所属する研究グループのシステムもあります。
J-parc勤務の場合は更に増える?

- メイルアカウント
  - post.kek.jp
  - post.j-parc.jp
- Webアカウント(事務)
  - 統合認証システム　物品購入、出張の手続き
    https://personsweb.kek.jp/
  - 給与明細 &諸手当申請システム
    https://hrap.kek.jp/package/auth/view/Login.html
  - 研究職員総覧　自分の情報の更新用

このページはKEK固有の情報を記載しています

KEKのシステムのアカウント(2)

- Webアカウント(研究・開発活動用)
  - 研究情報web research.kek.jp
  - 会議支援システム　kds.kek.jp
  - Wikiシステム wiki.kek.jp
- ネットワーク
  - LAS　ネットワーク登録申請システム
  - VPN　自宅などからKEK内のシステムにアクセス
  - TV会議システム
- 計算機システム
  - 中央計算機システム

このページはKEK固有の情報を記載しています

パスワードの役割

- 大雑把に言えば、
  ネットワークにつながっているシステムは、日本中の何処からでも誰でも、また世界中の何処からでも誰でも接続できる。
- 自分のアカウントで、自分だけが読んだり、作成や変更をできるようにするのがパスワード

何故パスワード管理が必要か

- パスワードが他の人に知れると
  - データが見られる
  - データをコピーされる
  - ファイルを書き換えられる
  - 他のシステムのパスワードが類推される
  - 自分になりすまされる
- 不正利用された結果、責任を取らなければならないことになったり、経済的損失の可能性があります
- 他人に絶対に知られないようにする

どのようにして盗られるか

- 典型的なパターンで試行して探す
  - 生年月日、電話番号、車のナンバー、家族の名前、辞書の単語
- 総当たりでの検索して探す
  - 全ての文字を試行
- 洩れたパスワードから他のシステムのパスワードを類推
  - クラックされたサイトから流出
  - 「システム管理者」からの問合せに回答
  - ウイルス感染によるパスワードを含む情報流出
- 偽装webページに入力してしまう

上記の攻撃に対する対策をとる

パスワード扱いの基本

- 解読されにくいパスワードをつける
- 複数のアカウントに同一のパスワードをつけない
  - 1つのパスワードが流出すると他のシステムにも入られる
  - 流用しない
    - でも、どうやって数10のパスワードを覚えておくのか？
- パスワードを他人と共有しない、貸さない
  - 誰も真剣に責任を持たなくなり、扱いがぞんざいになる
- 「システム管理者」から尋ねられたら?
  - 管理者がパスワードを尋ねることは、どのような場合でも絶対にない

解読されにくいパスワードの選択

- 最悪のパスワード
  - アカウント名=パスワード、姓名、生年月日
  - 辞書に載っている単語
- 作り方の一例
  - 小文字、大文字、数字、特殊文字の2種以上を使う
  - sunshine → Sun#shinE
  - yahoo → Ya#hoO → Ya#hoO12
- 文字数は適度に長く
  - 総当たり検索で解読されにくいように
  - 少なくとも8文字以上、自分で覚えられるもの
- しかし
  - 複数アカウントに同じロジックで作ると、類推されやすい。

ユーザ登録のパスワード

- クラウドサービス(メイルアカウント、Web、SNSなど)
  - パスワードを暗号化して保存するのが普通。
    - まれに暗号化せずに保存するサイトがある
    - メイルでパスワードを送ってくるサイトもある
  - 暗号化しないサイト、メイルで送ってくるサイトは利用を止めたほうが良い
- 暗号化の有無の見分け方
  - のっけから「パスワードを忘れたとき」の操作を試す
    - パスワードを教えてくれるのは暗号化していない証拠
    - 新しいパスワードを設定するWebページに誘導するようになっていれば、ほぼ合格

2016/1/14 13/40 ネチケット

多数のパスワード管理の一例

- うまい方法がない。次善の策をとる。
- 複数アカウントを関連性、重要性で分類
  - 同一レベルには同一ロジックで、異レベルには別ロジックでつける
    - 例えば、職場の計算機、無料アカウント、銀行関係、メルマガ、など
  - 漏洩したら同一ロジック全てのパスワードが取られたとみなす必要あり
    - →同一ロジック全てのパスワードを変更する

2016/1/14 14/40 ネチケット

多数のパスワード管理の一例

- パスワード一覧表のファイルを暗号化して保存する
  - 暗号化せずにファイルに置くのは、言語同断。流出したら全滅。
  - 必要なときだけ開き、見たらすぐに閉じる。
  - 暗号化の方法
    - 手軽には MS word あるいは MS excelで、「ファイル」「情報」「アクセス許可」とたどってパスワードを設定する
    - 古いバージョンでは「ツール」「オプション」「セキュリティ」
- Webサイトのパスワードをブラウザに記憶させる
  - パスワード一覧を暗号化できることが前提
    - 良：Firefox(「マスターパスワードを使用」と設定変更する必要あり)
    - 可：chrome, Opera, Internet Explorer, safari (マスターパスワード入力なしで使える)
  - PCのアカウントを複数の人で使う場合には利用できない。
    - パスワードが見えることはないが、全ての人が登録したパスワードでアクセスできる

2016/1/14 15/40 ネチケット

電子メイルの作法

2016/1/14 16/40 ネチケット

KEKには2つのメイルシステム

- post.kek.jpはKEK職員+共同利用者用、post.j-parc.jpはJ-PARC関係者用
  - 両方のアドレスを貰う人もいる
- 使いこなし
  - 転送設定で、どちらか一箇所に受信メイルをまとめるのが良い。
  - 外部に教えるメイルアドレスは、統一メイルアドレスだけにするのがセキュリティ上ベター。

このページはKEK固有の情報を記載しています

2016/1/14 17/40 ネチケット

おまけ：転送の一例

統一メイルアドレス shigeo.yashiro@kek.jp
↓
yashiro@post.kek.jp
↓
「PostKEKユーザ情報ページ」で転送設定してあると
↓
yashiro@post.j-parc.jp
↓
Webメイル https://post.j-parc.jp/ を利用
メイルはサーバに保存、どのPCからでも同じに見える

このページはKEK固有の情報を記載しています

2016/1/14 18/40 ネチケット

電子メイル返信の作法(1)

- 携帯電話と同じ使い方をすると失敗する
  - 返信は「全員に返信」を習慣にする
- 受け取ったメイルが個人宛なのか、複数人宛なのかを確認する
  - 宛先の種類
    - 個人宛
      - 特別な注意点なし
    - メイルングリスト(ML)への送付
      - 返信の宛先に注意
    - 複数人宛
      - 返信の宛先に注意
    - その他
      - 特別な注意点なし
  - メイルヘッダには本文に劣らない大事な情報がある

2016/1/14 19/40 ネチケット

電子メイル返信の作法(2)

- ML宛メイルへの返信
  - MLが返信先に設定されている場合
    - 原則は宛先を変えずにMLに返信
    - 個人的な内容は、返信先を差出人宛に変更
      - 参加申し込みへの返事など
      - 受け取ったメイルの記述ミス指摘は、返信先を差出人にする配慮
  - 差出人が返信先になる場合
    - 原則は「全員に返信」、宛先をMLに書きかえる
    - 差出人だけに返信して、全員に届いていると勘違いすることがないよう確認する
  - 送信前には、必ず宛先を確認

2016/1/14 20/40 ネチケット

電子メイル返信の作法(3)

- 複数人宛メイルへの返信
  - 同一宛先への返信が原則
    - 「全員に返信」、「reply all」を使用
      - 「返信」、「reply」では差出人にのみ返信
  - 宛先の追加あるいは削除は原則行わない
    - 追加する場合には以下の例のように明記する

皆様 (CC に　鈴木様を追加)

  - 宛先の追加あるいは削除
    - 話の食い違いの原因
    - 人間関係のトラブルの元

電子メイル返信の作法(4)

- 返信時にSubject を書き換えない
  - たとえ誤字が気になっても
  - 過去のメイルを探すキーワードに利用されるので
- 返信で別件を話題にするのは避ける
  - 同一Subjectで話題が続いた後に、別件を話題にする場合には、新しいSubjectにするのが良い
- 繰り返しだが
  - 返事を送る前に、返信のあて先を再確認

電子メイル送信の作法 (1)

- 送信ボタンを押す前に
  - 宛先を確認する
    - 似た名前には特に注意
  - 添付ファイルを付け忘れていないか
- 「高優先度」「高重要度」としない
  - 自分にとっては重要であっても、相手にとっては重要でない。たとえ上司から重要なことだと言い付かっても。
  - マークしてよいのは、相手にとって大きな利益があるとき
    - 例えば予算の追加配分を行なうときなど

電子メイル送信の作法 (2)

- 10人程度以上に同時送信をする場合
  - あて先アドレスを羅列するのでなく、MLにするのが好ましい
    - 書き間違い、書き漏らし、
    - アドレス流出を防ぐ

電子メイル転送の作法

- 第三者への転送
  - メイルを送ってきた人に転送の許可をとるのが原則。場合によっては受取人の許可もとる
  - 記載されている差出人と受取人のメイルアドレスも転送されることを考慮する必要
    - メイルアドレスを削って転送するなら、一部でなく全部を削る
- 他人のメイルアドレスを第三者に教える場合には、本人の許可を得る
  - Webや名刺で公開されていれば暗黙の了承

2016/1/14 25/40 ネチケット

電子メイルとプライバシー

- 封書のように他人に見られないと思わないこと
  - 電子メイルのプライバシーは葉書程度と思うべし
- 送ったメイルが、第3者に転送される可能性が無きにしもあらず
  - 書く内容や、言葉遣いに気配り
- 非公開情報をメイルで送るのは要注意
  - 入札関係、特許関係など。他人の悪口も
  - 一度送られた情報は、どこかのサーバに残っている可能性あり。削除は事実上不可能。

2016/1/14 26/40 ネチケット

電子メイルとセキュリティ

- スパムメイルへの返信
  - 自分の情報を提供することになるので返信しない。放置する。
- 自分が差出人になっているスパムメイル
  - 不愉快でも対処は不可能。反応することは情報提供になり相手を利するのみ。放置する。
- ウイルススキャンは万全でない
  - 新種のウイルスはすり抜ける
  - 怪しいメイル、添付ファイルは絶対に開かない
    - ➔ 情報流出、他の計算機への攻撃、偽装Webページへの誘導

2016/1/14 27/40 ネチケット

電子メイルの作法　その他

- 受け取る立場で読み直す
  - 節度を持った敬語、丁寧語
  - 挑発的な表現
  - 同じ言い方でも、人によって受け取り方が違うことにも配慮する
- いたずらに発信を増やさない
  - 些細な記載ミスは訂正メイルを出さない
  - 用件が片付いたときのお礼は不要の場合もある
- 相手に届くとは限らない
  - 受け取った相手の、見落とし、誤削除もある
  - 担当者は確実なシステムとするよう努力している
  - 規格として完全性を保障しているわけでない

2016/1/14 28/40 ネチケット

Webの注意点と作法

Webの世界

- 情報の宝庫
- 危険がいっぱい
  - 危険を察知するための知識を増やすこと

Web閲覧：不正アクセスの標的

- 不正アクセスの手法の主流
  - 偽メイルで偽装Webページや不正に書き換えられたWebページへの誘導
    - 違法行為があったので訴えるなど、脅しの偽メイル
    - 問題が発見されたのでパスワードを変更するようになどの、銀行などを装った偽メイル
  - 不正プログラムを埋め込む「怪しい」Webページを参照すると
    - PC内のファイルを取得される
    - クレジット番号、パスワードの入力を待ち、取得される
    - 入力することなく、閲覧するだけでも危険なページもある

Web発信

- 以下のWebシステムにアカウントを作れば、簡単に国内外に発信できる
  - 研究情報web research.kek.jp
  - Wikiシステム wiki.kek.jp

← KEK固有の情報です

- 自由に発信できる分、責任を持ってページを作成すること
  - 自分の研究・開発の成果や業績を発信するのが基本
  - その他の情報の場合には熟慮すること
    - 発信することが許容範囲の情報か
    - 権利侵害やプライバシーの問題（次ページ）

Web発信時の作法 (1)

- 他人の権利を侵害しないよう注意
  - プライバシー
    - 氏名などは、せめてイニシャルや仮名にする
  - 著作権
    - ダウンロードしたファイルの掲載はしない。
  - 肖像権
    - 顔の写っているスナップ写真の掲載は、せめてパスワード付きにするのが無難
- 自分の情報の発信
  - 顔写真、自宅の情報、は覚悟を決めた上で
  - 写真は GPS情報が含まれていないことを確認
    - 特にスマートフォンの写真、GPS設定したデジカメの写真には注意
- 一度公開された情報は、ネット上から簡単には消えない
  - どこかの検索サイトに残っている可能性あり
  - 転用されている可能性

個人情報

ネット社会は便利

- フリーメイル、スケジュール調整、グーグルマップ
  - これらはタダ?
    - 誰かが経費を負担している
    - 篤志家が寄付している訳ではない
- ファイル転送サービス、クラウドストレージ
  - データは実際にどこにあるの?
    - 自分のパソコンの中でない
    - 日本のどこか? 外国?

考えるべきこと

- タダにはワケあり
  - 情報は収集され、売買されていると思うべき
  - 最近注目されている「ビッグデータ」とは、収集した情報から、嗜好や動向をを分析して商売に利用すること
  - ネット上に置いたデータは外国に置かれることもあると思うべき
- 情報流出もたびたび
  - クラッカーによる搾取
  - 米国家安全保障局(NSA)による盗聴
    - CIA元職員エドワード・スノーデンによる告発

個人情報の公開は慎重に

- 自分自身の情報や写真、他人の情報
  - 必要以上の情報や写真を公開しない
  - 仲間内で利用するサイトであっても、流出がありうると考えて掲載
    - 事故による流出
    - 仲たがいからくる嫌がらせ
    - 関係が薄い人の仲間入り
  - 場合によっては、パスワードを付けたPDFファイルを掲載する
  - 一度流出したら限りなく転写されるので、消し去ることは不可能

2016/1/14 37/40 ネチケット

個人情報保護か、利便性か

- 利便性を得るために、個人情報をどこまで提供するのだろうか？
- 無料アカウントの利用
  - 職場のPCでの利用、自宅のPCでの利用、スマートフォンでの利用
    - 同一アカウントを使うことにより、一日の行動が読み取れる
    - スマートフォンの GPS 情報から、現在地が読み取れる
    - ネット検索などと結び付けて、関心事、趣味、冠婚葬祭の状況、健康の状況が付加できる
- ジョージ・オーウェルのSF小説『1984年』の到来

2016/1/14 38/40 ネチケット

まとめ

- パスワードを取られないように
- メイルのトラブルで人間関係を悪くしないように
- 情報を流出させないように
  - メイル、Web

2016/1/14 39/40 ネチケット

謝辞

- この原稿は、2010～2015の「高エネルギー加速器研究機構初任者研修」で使用した資料に加筆修正したものです。
- 2010年の初任者研修で講演する機会をKEK素核研の山野井豊氏が設定してくださいました。講演テーマは彼と共に検討しました。
- 2011年4月の書き換えに当たっては、元KEK計算科学センターの押久保智子氏にコメントを頂きました。
- 2012年4月の書き換えに当たっては、大阪大学レーザーエネルギー学研究センター高性能計算機室の福田優子氏に頂いたコメントを参考に修正しました。

2016/1/14 40/40 ネチケット