Tya-net Newsletter

富山大学
総合情報基盤センター

No.47

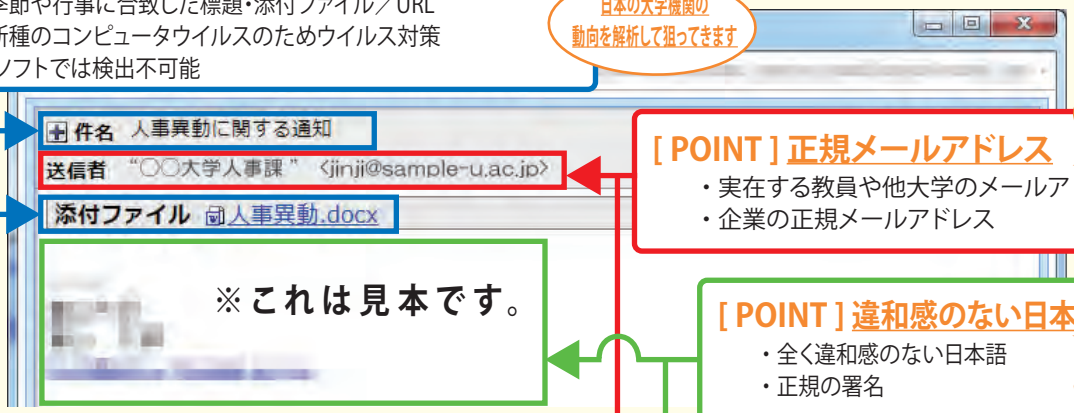
セキュリティ対策情報

緊急告知

こんなメールには要注意!

[POINT] 関連性が高い標題や添付ファイル／URL
- 業務／研究内容に関連性が高い標題・添付ファイル／URL
- 季節や行事に合致した標題・添付ファイル／URL
- 新種のコンピュータウイルスのためウイルス対策ソフトでは検出不可能

日本の大学機関の
動向を解析して狙ってきます

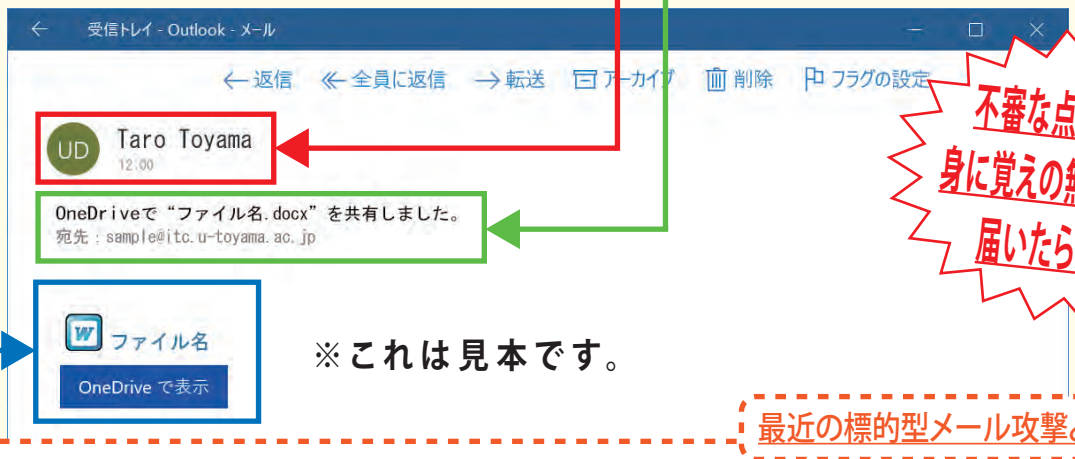


[POINT] 正規メールアドレス
- 実在する教員や他大学のメールアドレス
- 企業の正規メールアドレス

他機関のシステムが
悪用されている可能性あり

[POINT] 違和感のない日本語
- 全く違和感のない日本語
- 正規の署名

他機関で流出した
メールが流用されています



**不審な点が無くても
身に覚えの無いメールが
届いたら要注意!**

最近の標的型メール攻撃とは

- ✓ 正規のメールアドレスやドメインで送付されるため,"見た目"は正規メールと見分けがつきません。
  ⇒ メールの見た目や差出人だけの情報で判断するのはやめましょう。"見た目"は容易に偽装可能です。
- ✓ 業務内容,問い合わせ,社交辞令,冠婚葬祭などあらゆる内容で送付してきます。
  ⇒ 実在する大学や会社からの業務関連／通知メール,学生からの問い合わせ,知人名義での出産／子供の成長報告メールなどありとあらゆる正規メールを偽装して送付してきます。
- ✓ すべての添付ファイルにウイルスを埋め込むことが可能です。
  ⇒ ワード,エクセル,PDF,画像ファイルなど"すべてのファイルにウイルスを埋め込む事が可能"で,その多くが新種(未知)のウイルスです。
- ✓ 本文に記載されたURL(ウェブサイト)は"見ただけ"でウイルス感染する場合があります。
  ⇒ あなたのパソコンやスマートフォンに"一つ"でも脆弱性がある場合,攻撃者によって改ざんされたウェブサイトを"閲覧しただけで"ウイルス感染する可能性があります。攻撃者は,その"穴＝脆弱性"を狙っています。

富山大学 総合情報基盤センター
2017年12月18日
http://www.itc.u-toyama.ac.jp/
内線：6946（五福）

▶ バックナンバー：http://www.itc.u-toyama.ac.jp/cn/

重要

年末年始のセキュリティ対策について

特に年末年始は世界的かつ大規模なサイバー攻撃が発生するため，**個々人が各々適切に対策を実施しなければ甚大な被害が発生するおそれが高まります。**以下にセキュリティ対策方法を簡潔にまとめましたので，年末年始前後には必ず実施願います。

なお，不審な点を発見された場合は，最寄の総合情報基盤センターへ早急にご相談ください。

パソコン編

Check!

- ☐ **OSに修正プログラムを適用する**
  - ☐ Windows → Windows Update
  - ☐ Mac → ソフトウェア・アップデート
- ☐ **導入しているアプリケーションに修正プログラムを適用する**
  - ☐ Adobe製品全般（特にReader/Acrobat）
  - ☐ Java　☐ Flash
  - ☐ JustSystem製品全般（特に一太郎）
- ☐ **ウイルス対策ソフトの定義ファイルを最新の状態に更新し，完全スキャンを行う**　重要!

ネットワーク機器編

Check!

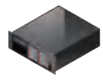
- ☐ **ネットワーク機器（複合機やルータ等）に適切なセキュリティ対策を行う**
  - ☐ 最新のファームウェアを適応する
  - ☐ 管理画面へ適切なパスワード設定する
  - ☐ セキュリティ機能を活用し，適切な設定／管理を行う
    - ☐ アクセス制限機能
    - ☐ MACアドレス制限機能　重要!
  - ☐ 通信／利用記録等のログ（履歴）に不審な点がないか確認する

※機種やメーカーによって対応事項／方法が異なります。メーカーサイトを確認する／メーカーサポートに問い合わせる等，ご自身で適切に対応してください。

サーバ編

Check!

- ☐ **各種修正プログラムを適用する（yum update等）**
  - ☐ 稼動サービス等の脆弱性に関する情報収集に努め，適切に対応する
- ☐ **サーバーの設定や履歴の確認を行う**
  - ☐ 強固なパスワードの設定（8文字以上かつ大文字や数字を組み合わせる）
  - ☐ 稼動サービスの確認（psコマンド）
  - ☐ アクセス制限等の適切な設定／管理
  - ☐ 接続 / ログイン / 操作等履歴の確認（lastコマンド，/var/log配下の確認）　重要!

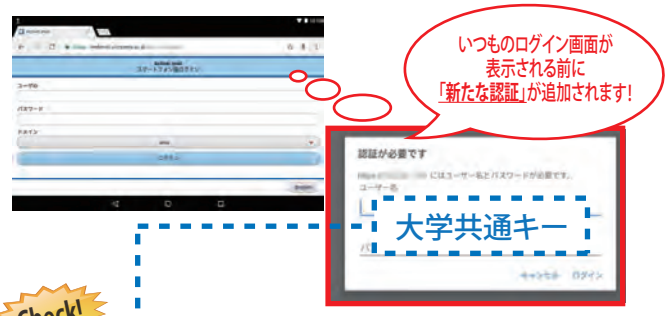


※　記載事項は一般的な必要最低限の対策事項です。機器管理者は管理状況に合わせて適切に対応してください。

[参考] 情報セキュリティ（IPA）
https://www.ipa.go.jp/security/index.html

Active! mailの二段階認証について

このところ，ウェブメール（Active!mail）を介した情報セキュリティ事案が発生しているため，ウェブメール（Active!mail）のセキュリティ強化を図ることを目的に，**12月18日13時より二段階認証（個人のログイン画面を表示する前に大学共通キーによる認証を行う）を導入します。**



Check!

詳細は，センターのウェブサイトをご覧ください。

ITC HOME ＞ Active! mailについて
http://www.itc.u-toyama.ac.jp/activemail/index.html

ウイルス対策ソフトの貸出しについて

センターではウイルス対策ソフトのライセンス貸与サービスを行っています。所定の利用申請手続きを行うことで，ウイルス対策ソフトが利用可能になります。ウイルス対策ソフトは**2種類**から選択可能です。

- ○ Symantec　＝　統合管理型セキュリティ対策ソフト
  （AntiVirus機能に加えて，ファイアウォール等様々な機能を搭載し，機器のセキュリティを総合的に管理）
- ○ ESET　＝　ウイルス対策ソフト
  （AntiVirus機能に特化，機能を厳選しているため動作が軽快）

2つのソフトは"性格"が異なります。お好きな方を！

詳細は，センターのウェブサイトをご覧ください。

ITC HOME ＞ サービス ＞ ソフトウェア・ライセンスの貸与サービス（職員向け）
http://www.itc.u-toyama.ac.jp/service/license.html

【最新バージョン】

- ○ Symantec　Win / Mac : 14.0.1 (RU1)
- ○ ESET　Win / Mac : 6.4～6.5系

macOS 10.13 に対応しました！

おまけのコラム

～ メールの転送設定は慎重に! ～

センターではメール転送サービスを提供しています。多くの方がこのサービスを利用している一方で，トラブルの件数も増加しています。

メール転送は，便利な半面，誤った使い方をすると，他の利用者へ迷惑をかけるだけでなく，情報漏えい等の大きな問題に発展します。

【トラブルケース１】　設定ミスによるメールサーバの停止

キャリア（携帯会社）側でPCメールの拒否設定を有効にした状態でキャリアメールに転送設定のみを行った。確認作業を怠った結果，メール不達のエラーメールに気づかず，無限ループ（大学→キャリア→携帯電話→"不達"→キャリア→エラーメール→大学→・・・）し，メールサーバが過負荷となり緊急停止しました。

【トラブルケース２】　多量のメール転送により，転送先から本学のメールが拒否される

大手のフリーメールサービスへ転送設定を行い，数百通のメールを一度に転送した結果，本学のメールサーバが迷惑メールの発信源としてブラックリスト登録をされてしまった。解除申請の手続きを行ったが，申請が受理されるまで，他の利用者も転送が拒否されたり，遅延する事態になりました。

Check!

- ☐ 本学にはActive!Mailというウェブメールがあります。本当に転送設定が必要ですか？
- ☐ 学外のメールサーバでは，メール内容を解析しているところがあります。そのメール内容は学外へ流出しても問題ありませんか？
- ☐ あなたが設定ミスをした場合，大学のメールサーバが停止する可能性があります。あなたが行ったその転送設定に責任が持てますか？

もう一度設定確認をお願いします

PC，スマホ，タブレット等とインタネット環境があればどこからでも利用可能な，Active!mailも是非ご利用ください。

ITC HOME ＞ マニュアル ＞ 電子メールの設定 ＞ Active! mail (Webmail) の使い方
http://www.itc.u-toyama.ac.jp/inside/start.html#mail

総合情報基盤センター
http://www.itc.u-toyama.ac.jp/