情報セキュリティ担当者説明会

2018　8/1-8/7

附属総合情報センター

Agenda

基本的な情報セキュリティ対策

1　情報セキュリティの動向

2　日々のメンテナンス

3　個人情報・機密情報の取扱い

4　OS・ソフトウェアのサポート期限について

１　情報セキュリティ動向
（２）世界を取り巻く状況

①ランサムウェア被害の深刻化

・2017年5月Microsoft社のファイル共有プロトコルの脆弱性を悪用した自己増殖するランサムウェア「Wanna Cryptor」が世界を席巻。ランサムウエアによる攻撃は巧妙化を続けている。

②新たな脅威となった不正マイニング

・Bitcoin等の仮想通貨の価値が急騰した結果、セキュリティに問題のあるパソコン等を乗っ取り、仮想通貨マイニングソフトウェアを仕掛けて計算機パワーを不正に使ったマイクングを行うサイバー犯罪が急増。

③巧妙化するビジネスメール詐欺

・2014年以降、被害が増加傾向にあり、2017年には本格的に広がる傾向が出てきた。2017年12月には、JALがビジネスメール詐欺により、3億8,400万円の被害を発表。

１　情報セキュリティ動向
（３）札幌医科大学を取り巻く状況

①フィッシングの巧妙化

「フィッシング」とは実在する企業をかたったメールを送り、個人情報を詐取するWebページ（フィッシングサイト）に誘導し、個人情報を入力させて詐取する手口

- 「Appleアカウントの停止」、「楽天ショッピングの利用」、「Amazonアカウント」などをかたる精巧なフィッシングメール受信を確認。

- 送信元（差出人）アドレスは詐称されており、本物のメールアドレスが使用されている場合がある。

- フィッシングサイトとして使用されているページも作り込まれており、本物のWebサイトの情報を完璧にコピーして使用する。

・フィッシングサイトへ誘導するメール本文の巧妙化

相手にされなかった

英語やその他言語で記載されたメール本文

すぐに見分けがつく

幼稚・誤字が多い日本語で記載されたメール本文

今ココ→ほぼ見分けがつかない

実在する企業等が使用するメール本文をコピーして使用

・フィッシングによる被害への対策

・メールに記載されたリンクを利用せず、googleやYahooなどの検索サイトから本物のWebサイトを探しアクセスする。

→検索サイトの検索結果を詐称するのは非常に困難であり、また、本物のWebサイトにフィッシングメールが出回っている事実を周知している場合もある。

・怪しいと感じたら、所属内の詳しい人物に問い合わせるか、総合情報センターまで問い合わせを行う。

【問い合わせ先】
附属総合情報センター総務・システム係
内　線：22390・22490
メール：icccj@sapmed.ac.jp

【平成２９年度～】
学内における情報セキュリティインシデントについて

１　ウイルス対策ソフトの有効期限切れによるウイルス感染

２　個人情報（学生情報）を保存したパソコンの紛失

３　一斉同報メールの誤配信

1　ウイルス対策ソフトの有効期限切れによるウイルス感染

対策

学内統一ウイルス対策ソフトの導入を行う

・平成３０年４月より学内ネットワークに接続する際には、導入が必要。公有PC（台数無制限）、教職員私有PC（３台）、学生私有PC（１台）に導入可能。

OSのセキュリティアップデートを行う

・Windowであれば自動アップデートを有効とする。
・Apple macOSXも自動アップデートを有効とする。

2　個人情報（学生情報）を保存したパソコンの紛失

対策

不必要なデータの持ち出しを行わない

- 持出ルール・管理体制の確認
- 本当に必要な持出か？許される持出か？確認を行う
- 他のより安全な方法の検討

万が一の紛失・盗難に備えた対策を行う。

やむを得ず持ち出す場合には、
パスワード設定・暗号化・匿名化を。

3　一斉同報メールの誤配信

対策


重要な情報は暗号化した添付ファイルに


送信前に宛先と内容の再確認


同時に多くの宛先に送信する場合（同報メール）は、
TO,CC,BCCの正確な判断を

２　日々のメンテナンス（１）

学内統一ウイルス対策ソフトの導入

常に最新の状態に保つ

＊平成３０年４月より、トレンドマイクロ社ウイルスバスターコーポレートエディションを大学包括契約により導入。公用PC（台数無制限）、教職員私用PC（３台まで）、学生私用PC（１台まで）に導入可能。対応OSは、Windows7・8.1・10、Apple macOSX 10.9以降、Linux系OS、マイクロソフトサーバ系OS（詳細は情報センターまで問い合わせください。）

２　日々のメンテナンス（２）

OS、アプリケーションのアップデート

脆弱性（セキュリティホール）を残さない

＊平成３０年４月に実施されたWindows１０の「機能更新プログラム」の適用により学内統一ウイルス対策ソフトであるトレンドマイクロ社ウイルスバスターコーポレートエディションに不具合が生じました。今後も年２回の機能更新プログラムの実施がアナウンスされえいる為、別紙手順書のとおり機能更新プログラムの配信遅延設定を行ってください。

３　個人情報・機密情報の取扱い（１）

①データへのパスワード設定

・フリーウェアのLhaplusを用いたzipファイルへのPW設定など

②データの暗号化

・一般的には暗号化の際に自動的に共通鍵とパスワード生成する方式の
　メール暗号化ソフトを利用
※MS-Office製品の暗号化機能もある

③データの匿名化

・データから個人識別情報を取り除く（仮名化）
・他の情報と組み合わせても個人を特定できないように

３　個人情報・機密情報の取扱い（２）

管理ルールの明確化

- 情報の保存先を限定・特定する
  （場所の明確化）
- 情報にアクセスできる者を限定・特定する
  （人の明確化）

物理的対策

- 無人の場所に放置しない・無人状態を作らない
- 施錠管理の徹底
  （管理の継続性確保）

＊ハードディスクを搭載したPCやサーバ、NAS、USBメモリを廃棄する際は、専用ソフトウェアを使用したデータ削除か、物理的な破損を実施した後廃棄を行う。

＊総合情報センターではハードディスク破壊機器を所有しております。ハードディスクの廃棄を行う際は、そのまま廃棄せず、上記処理を行った後に廃棄を行うか、ハードディスクを総合情報センターまでお持ちください。

３　個人情報・機密情報の取扱い（３）

なくした！落とした！盗まれた！

情報の持ち出し
持出ルール・管理体制は明確か？

本当に必要な持出か？許される持出か？

他のより安全な方法はないか？

やむを得ず持ち出す場合には、パスワード設定・暗号化・匿名化を。

４　OS・ソフトウェアのサポート期限について

OSやソフトウェアにはサポート期限が設定されており、**期限が終了すると、脆弱性の対応がなされなくなる**。

↓

コンピュータウイルス等、悪意のあるソフトウェアは**脆弱性を狙って攻撃を行う**。

↓

学内の**ネットワーク環境全体が危険**に。

Microsoft Windows　サポート期限

製品名	サポート終了日
Windows　XP	すでに終了
Windows　Vista	すでに終了
Windows　7	2020年1月14日
Windows　8/8.1	2023年1月10日
Windows　10	2025年10月13日

Apple macOSX　サポート期限

Apple社はサポート期限を公開していないが、トレンドマイクロ社ウイルスバスターについて、macOS10.9以降対応（2018年8月現在）となっている。

製品名	最終バージョン更新
OSX 10.9 Mavericks	2014年09月17日
OSX 10.10 Yosemite	2015年08月18日
OSX 10.11 El Capitan	2016年07月18日
MacOS 10.12 Sierra	2017年07月19日
MacOS 10.13 High Sierra	最新版

その他主要ソフトウェアのサポート期限

製品名	サポート終了日
Windows　Liveメール	2017年1月10日【すでに終了】
Windows　Office 2007	2017年10月10日【すでに終了】
Office for Mac 2011	2017年10月10日【すでに終了】
Windows　Office 2010	2020年1月14日
Windows　Office 2013	2023年4月11日

サポート期限が終了したOS、ソフトウェアは早急に削除

使用を続ける場合は、学内ネットワークから取り外す

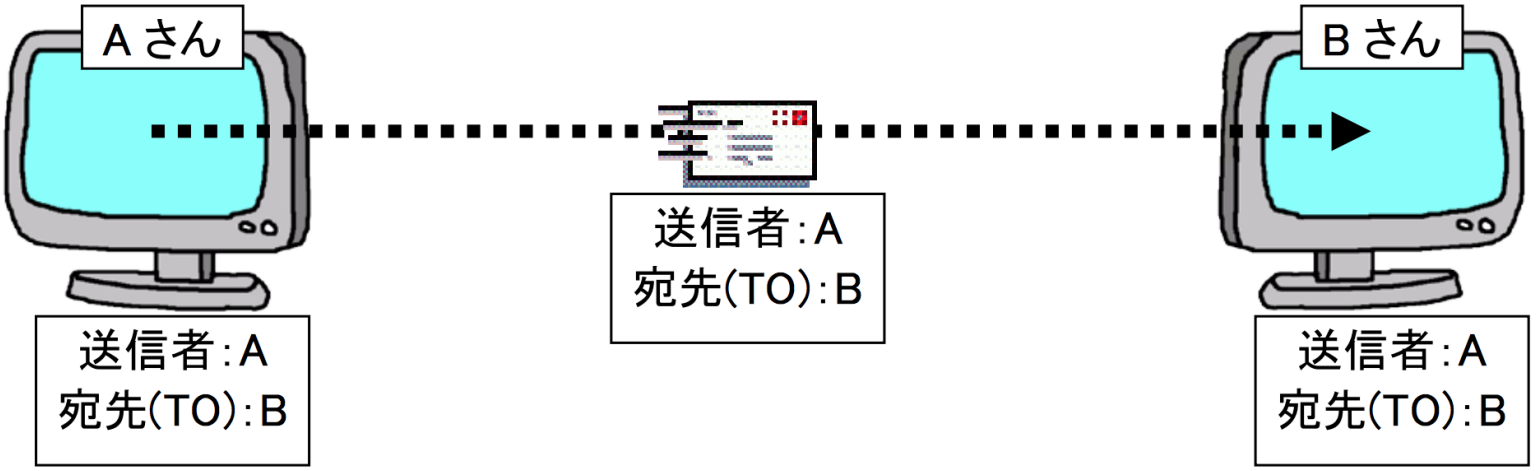
【資料】

電子メールの利用方法

TO、CCおよびBCCの使い方

TO

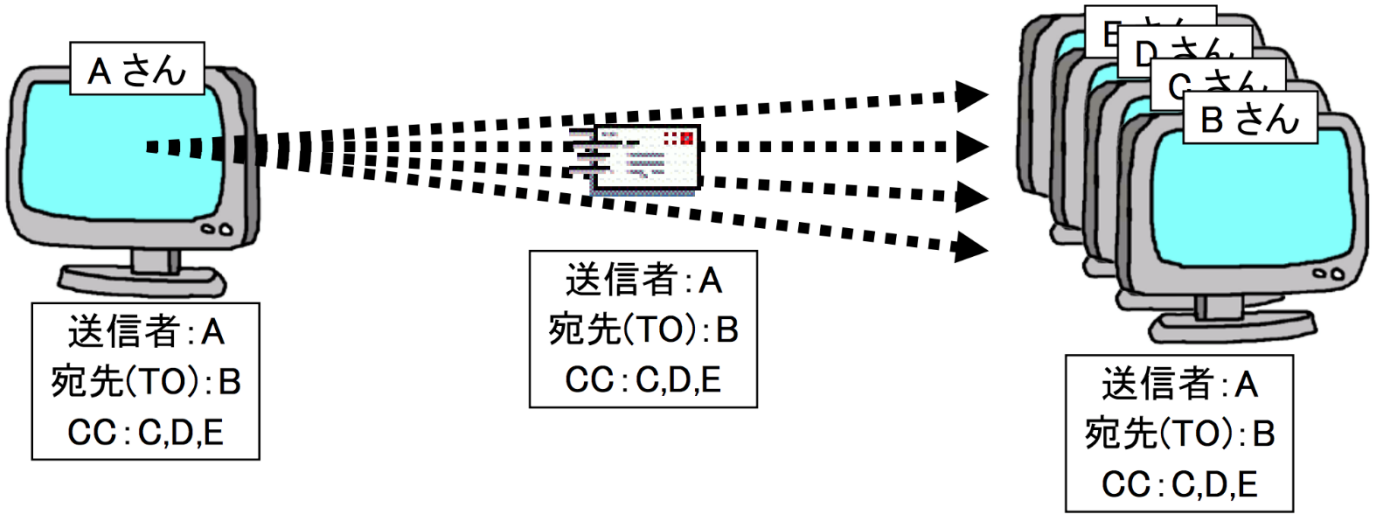
TO による宛先指定は、電子メールの主宛先を指定するのが一般的にです。特定の一人の宛先を指定する場合は、TOを使います。



CC(カーボンコピー)

同じ内容の電子メールを複数の宛先に同時に送信(同報メール)する場合に利用します。

Bさん宛の電子メールをCさん、Dさん、Eさんにも送信したことが、
Bさん、Cさん、Dさん、Eさんにもすべて分かる

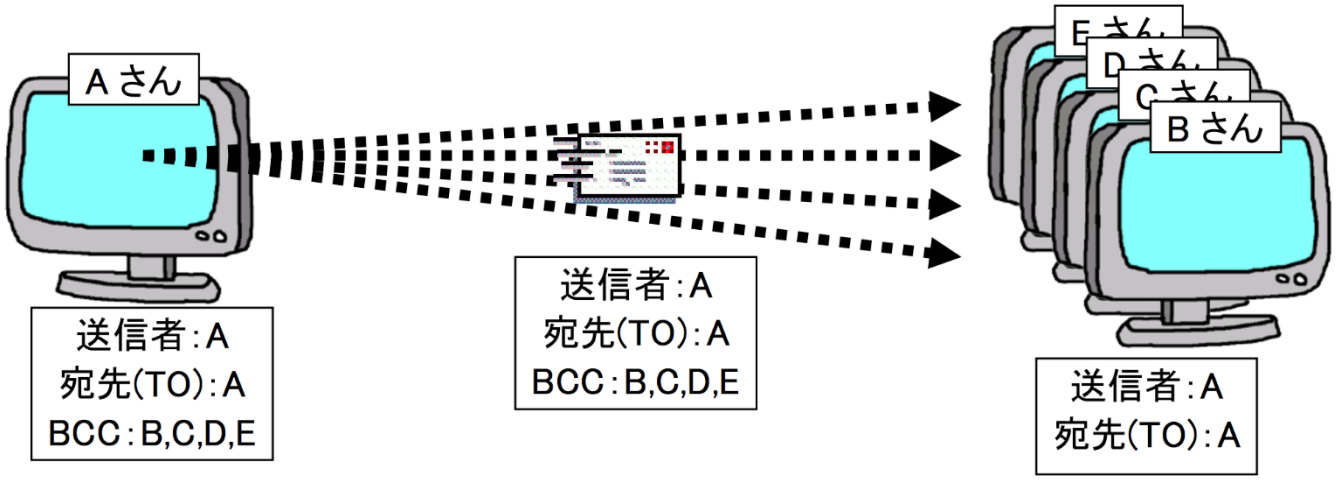


このケースで、Bさん、Cさん、Dさん、Eさんが、それぞれお互いを
知らない場合、メールアドレスが知られてしまい、メールアドレスの漏えい(個人情報の漏えい)となってしまう。

BCC(ブラインドカーボンコピー)

同じ内容の電子メールを複数の宛先に同時に送信(同報メール)する場合に利用します。BCCに指定されたメールアドレスは他の宛先に知られません。

Bさん、Cさん、Dさん、EさんにはAさんの電子メールが送信されますが、Bさん、Cさん、Dさん、Eさんには、この電子メールの宛先が自分以外にあることは通知されません。(自分宛なのかも表示されません。)



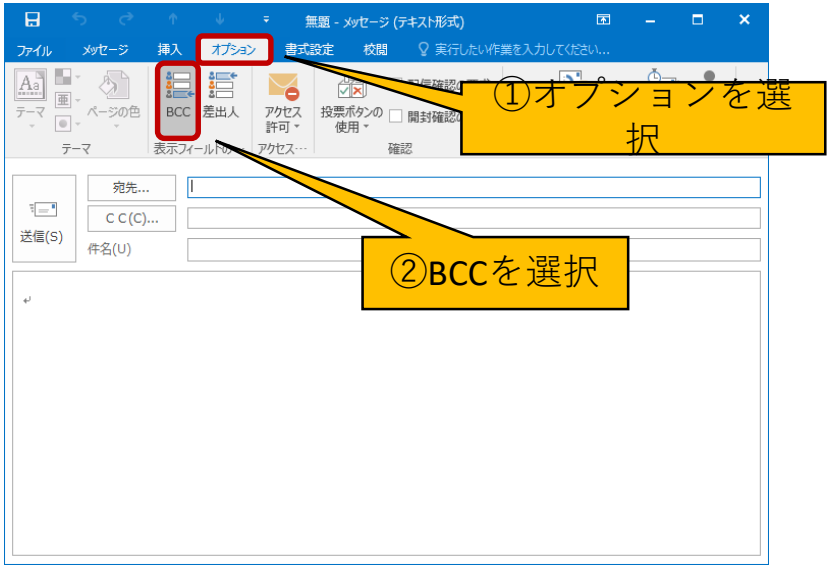
このケースでは、本文や添付ファイルの内容を除いて、TOやCCの時のようなメールアドレスの漏えいは生じません。

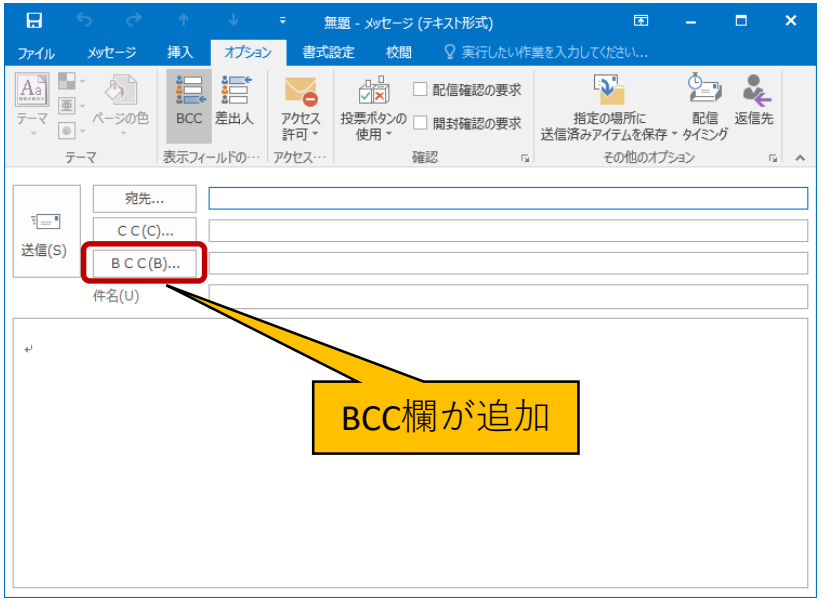
【資料】

BCCが使えない？

OutlookやAppleメールなどでは、初期状態ではBCC欄が表示されていない場合があります。

Outlookの場合、メール送信時に①「オプション」タブを選択、②「BCC」を選択すると宛先入力欄に「BCC」が追加されます。



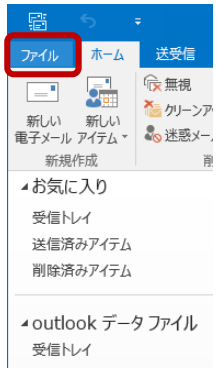


【資料】 HTMLメールからテキストメールへの変更

受信メール（Outlookの例）

初期設定ではHTMLのプログラムが埋め込めるため危険です。特に必要の無い場合はテキストメールに変更しましょう。

①

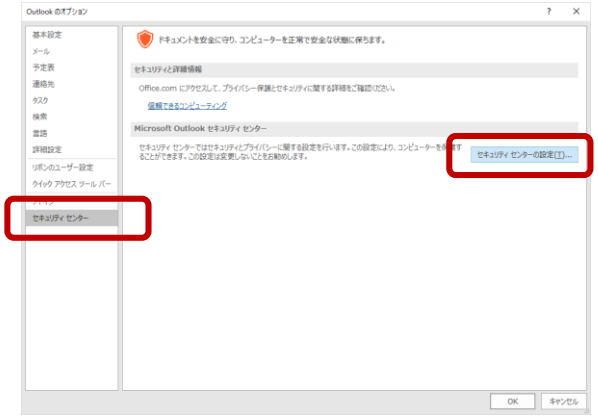


「ファイル」タブを選択します。

②

表示されたメニューから「オプション」を選択します。

③



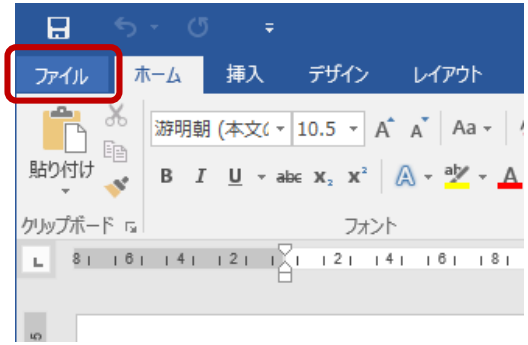
「Outlookオプション」から「セキュリティセンター」を選択し「セキュリティセンターの設定」をクリックします。

④

表示された画面から「電子メールのセキュリティ」を選択し、「テキスト形式で表示」と書かれた項目にチェックをいれて、「OK」をクリックします。

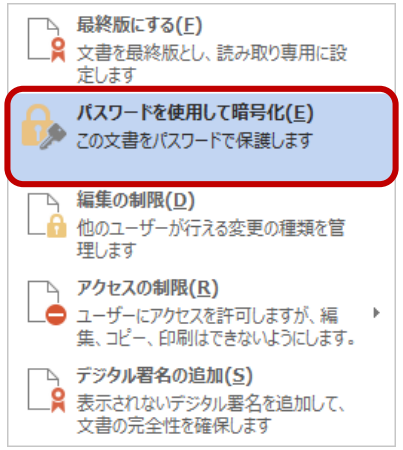
【資料】

データの暗号化（Microsoft Office 2016 Word の例）

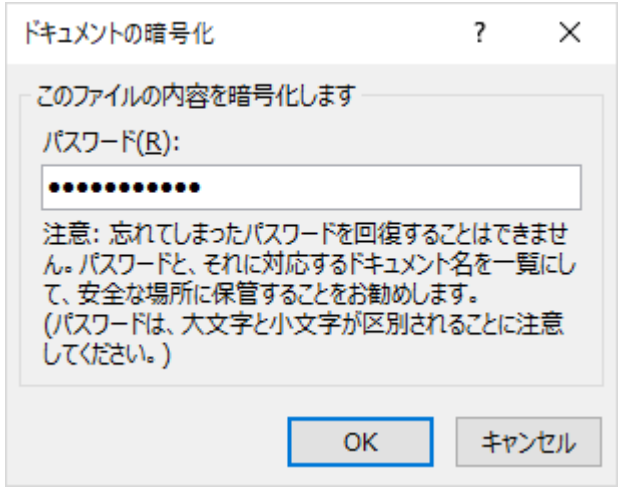


① 「ファイルタ」タブを選択

② 「情報」を選択し「文書の保護」をクリック



③ リストから「パスワードを使用して暗号化」を選択



④パスワードを入力後、OKボタンをクリック