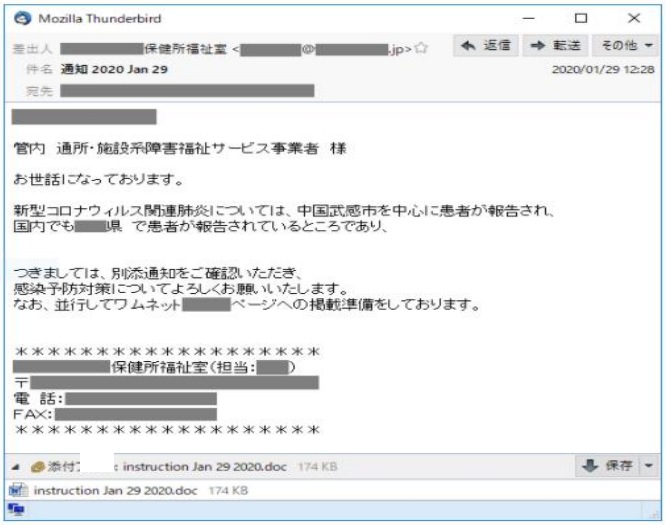
標的型攻撃による機密情報の漏えいに注意！

標的型攻撃（スピア型攻撃）とは、特定の攻撃対象（個人・組織）に対して、知人や取引先等に偽装したメールを利用してPCをウイルスに感染させる手口（標的型攻撃メール）・頻繁に利用するウェブサイトを調査し、そのサイトを閲覧するとウイルスに感染するように改ざんして、ウイルスに感染させる手口（水飲み場型攻撃）等を用い、機密情報を不正に入手したり、システムを破壊する不法な活動です。標的型攻撃は、不特定多数を攻撃対象とするものと比較して、被害者が攻撃されたことに気づきにくいという特徴があります。

○ **攻撃手口**

- メールを利用した手口（標的型攻撃メール）
  - 不正な添付ファイルを開かせる。
  - 不正なウェブサイトへのリンクをクリックさせる。
- ウェブを利用した手口（水飲み場型攻撃）
  - 攻撃対象が頻繁に利用するウェブサイトを調査し、そのサイトを閲覧するとウイルスに感染するように改ざんする。
- 不正アクセスによる手口
  - 組織が利用するクラウドサービスやウェブサーバーの脆弱性を悪用して不正アクセスし、認証情報等を不正に入手する。
  - 不正に入手した認証情報等を悪用して正規に社内システムへ侵入し、PCやサーバーをウイルスに感染させる。



新型コロナウイルスを題材とした攻撃メールの例（2020年1月）

（出典　IPA 独立行政法人情報処理推進機構）

対策

- **ウイルス対策の徹底。**
  OS、ソフトウェア及びウイルス対策ソフトは、頻繁にアップデートし、最新の状態を保つ。
- **不審なメールのリンクや添付ファイルは不用意に開かない。**
  メールのアドレスや本文を確認した上で、必要な場合のみ添付ファイルを開くようにし、少しでも不審点があれば送信元にメールの送信事実を確認してから開く。
  ※　添付ファイルがマイクロソフトオフィスの場合や拡張子が exe、scr、pdf、cpl 等の場合は注意が必要です。
- **セキュリティ意識の向上（職員等への教育）。**
  標的型攻撃の典型的な手口や対策について職員等に啓発することにより、セキュリティ意識の向上を図る。

【参考】　IPA 独立行政法人情報処理推進機構　情報セキュリティ 10 大脅威 2021
「情報セキュリティ 10 大脅威 2021［組織編］」
https://www.ipa.go.jp/files/000089239.pdf

岩手県警察本部サイバー犯罪対策課の公式ツイッターは QR コードから！！サイバー空間を悪用した犯罪の手口やサイバー犯罪の被害に遭わないための情報をお知らせしています。

@Iwate_cyber

岩手県警察本部生活安全部サイバー犯罪対策課

令和3年6月1日発行