不審メール受信時の対応の参考

- 昨今、政府機関や、実在する事業者等をかたる「不審な電子メール」が送信される事案が多数発生しております。
- これらの不審な電子メールは、貴組織が保有する重要情報を窃取する等の不正行為を目的として送信されている可能性があります。
- ご利用の情報システムでは、ウイルス対策ソフトの定義ファイルを常に最新の状態にする等、ウイルス対策に必要な措置がとられていることと存じますが、インターネットの世界では、ウイルス対策ソフトでは検知できない新種のコンピュータウイルスが日々確認されております。
- 不審な電子メールを受信した場合には、メールを開かず、本資料を参考にして、適切なご対応を御願いいたします。
- また、不審な電子メールに限らず、インターネット閲覧によるコンピュータウイルスの感染もありますので、ご注意ください。

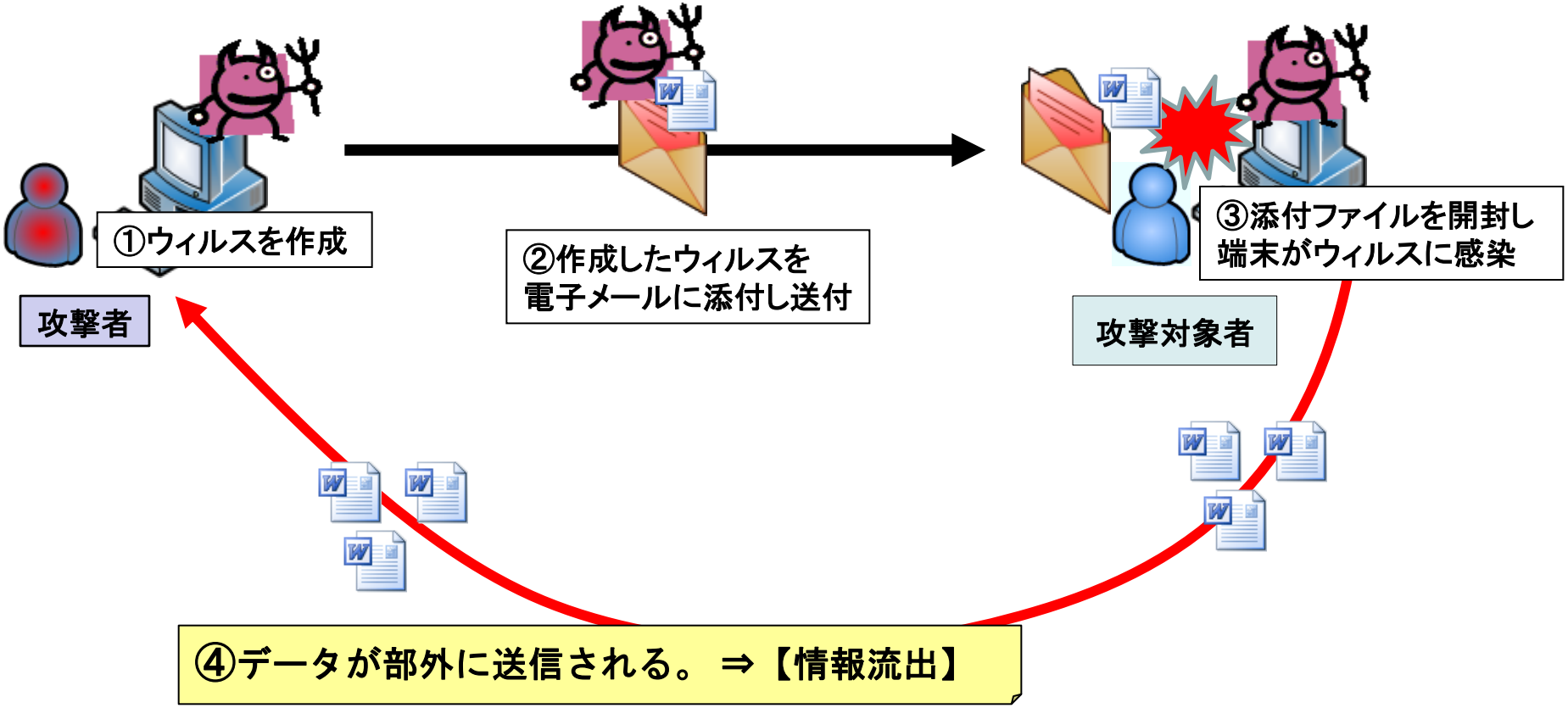
不審な電子メールを受信した時のご対応について

- 不審な電子メールを受信したことに気が付いた場合は、開封せず、貴組織の情報システム担当者へ連絡し、指示に従ってください。

- 不審な電子メールを受信した時の注意点
  - 添付ファイルは開封しない！
  - 電子メールの本文に記載されたリンク（URL）をクリックしない

不審な電子メールとは

- 政府機関の職員や、業務で関係する事業者等をかたり、重要情報等を窃取する等の不正行為を目的として送信された電子メールのこと。
- 不審な電子メールには、コンピュータ・ウイルス付きのファイルが添付されていることが多い。



不審な電子メールの特徴

① 実在の組織や個人を装っているが、メールアドレスがフリーメールアドレスから送信されている。

差出人のメールアドレスとメール本文の署名に記載されたメールアドレスが異なる。

② 受信者に興味を持たせる件名

③ zip圧縮ファイル、ワードファイル等が添付されている。

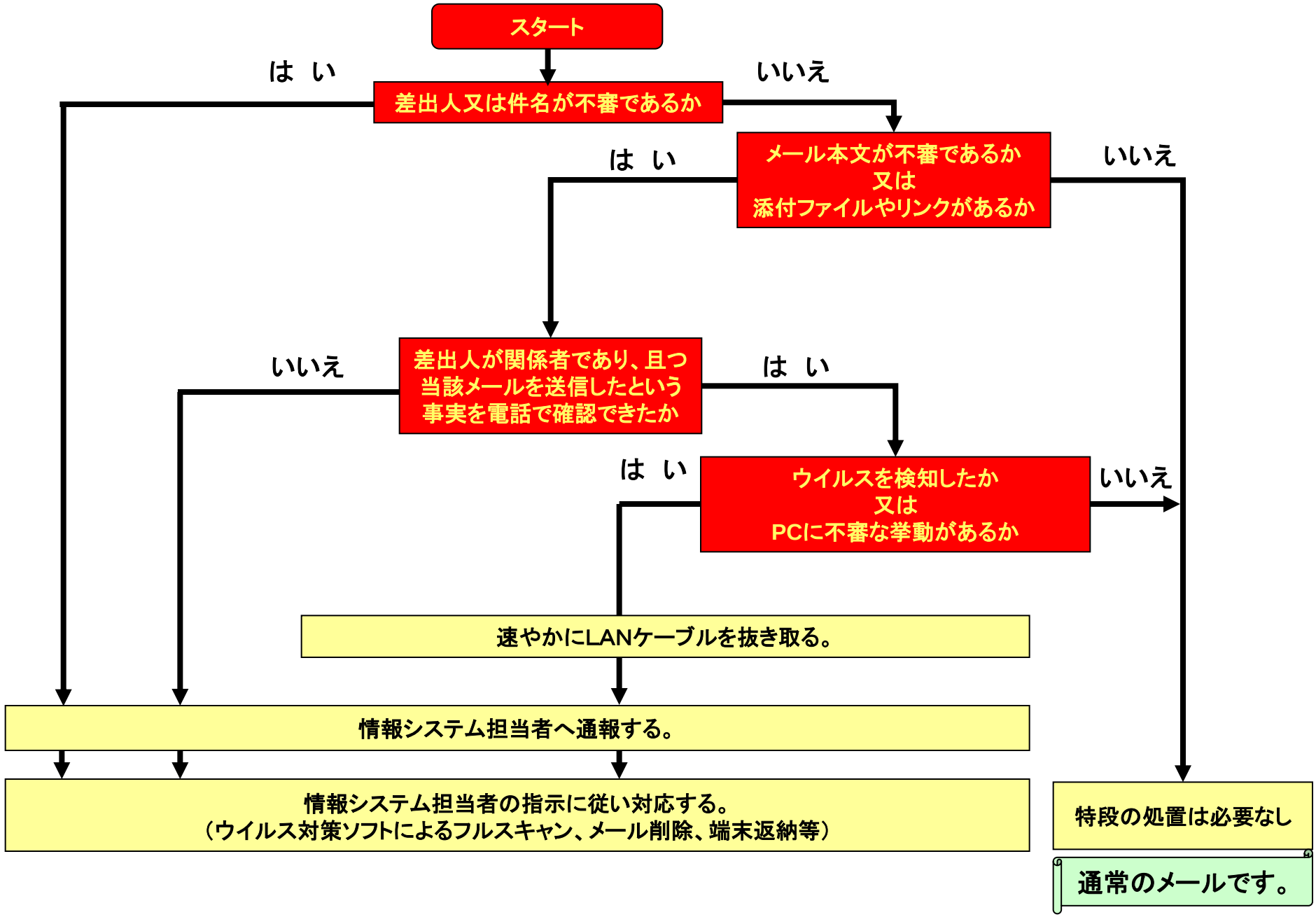
④ 件名に関わる本文が記載されている。

⑤ 本文の内容に合ったリンク(URL)が記載されている。

⑥ 実在の組織名や個人名などを含む署名が記載されている。

- **電子メールの添付ファイルは、不用意に開かない。**
  - 見ず知らずの相手からの電子メールの添付ファイルは開封しないようにしましょう。ウイルスに感染し、情報を窃取される可能性があります。
  - よく知った相手からの電子メールも、添付ファイルはウイルスチェックを行ってから開くようにしましょう。
- **メール本文のリンク(URL)は安易にクリックしない。**
  - 見ず知らずの相手からの電子メール本文に記載されたリンク(URL)をクリックしてはいけません。クリックすると、危険なウェブサイトに接続し、ウイルス感染や情報を窃取される可能性があります。

情報システムにおいて「不審な電子メール」を認知した場合の手順



サイバー攻撃等に関する相談窓口①

【警視庁】サイバー犯罪にかかる電話相談窓口

サイバー犯罪に係る電話相談窓口

ミヨミライ　ハイテク

電話相談　03－3431－8109

平日午前8時30分から午後5時15分まで

情報提供はこちらから

警視庁　サイバー犯罪対策課

出典：警視庁ホームページ

サイバー攻撃等に関する相談窓口②

【IPA】情報セキュリティ安心相談窓口

ウイルスおよび不正アクセスに関する技術的なご相談を受け付ける窓口

電話でのご相談

次の注意事項をご確認の上、下記の電話番号までお願いいたします。

なお、受付時間は平日の10:00～12:00および13:30～17:00とさせていただいています。

注意事項

- 上記の整理していただきたい情報について説明願います。
- 対応の品質向上のため、通話内容（音声）は記録させていただいています。
- 相談は無料ですが、通話料はご負担いただくことになります。

電話番号：03-5978-7509

メールでのご相談

次の注意事項をご確認の上、下記のメールアドレスまでお願いいたします。

注意事項

- 上記の整理していただきたい情報について明記願います。
- メールを受信後、5営業日以内を目処に返信、回答いたします。
- 大量または大きなサイズ（目安として3MB以上）のファイルを添付したメールを送信しないでください。
- フィルタリング設定をしている場合「ipa.go.jp」ドメインのメールを受信できるようしてください。
- 特定電子メール（いわゆる迷惑メール）の転送、送信はしないでください。

E-mail：anshin@ipa.go.jp

出典：IPAホームページ

サイバー攻撃等に関する相談窓口③

【 JPCERT/CC 】インシデント報告

【JPCERT/CCでお受けしている相談の例】

- Web サイト改ざんに関する相談
  サイトの改ざん箇所の特定や、改ざんされた際の復旧手順について
- 不正アクセスに関する相談
  サーバへの侵入やDoS 攻撃が発生した際の対処について
- マルウエア感染の相談
  マルウエアに感染した際の駆除方法、復旧方法について

連絡先	
電子メール	info@jpcert.or.jp（PGP 公開鍵） (*) JPCERT/CC PGP 鍵が更新されました。詳細はリンク先をご覧下さい。
FAX	03-3518-2177 （インシデント報告以外のものは 03-3518-4602 宛にお願いします）
電 話	03-3518-4600（夜間: 留守番電話）

出典：JPCERT/CCホームページ

（参考）パスワード管理の徹底

- パスワードは、情報システムやデータの不正使用を防止し、情報流出を防ぐために重要な情報です。
- パスワードは、情報システム（パソコンや業務で使用するソフトウェア）に限らず、スマートフォン・携帯電話でも用いられています。
  - パスワードは、初期設定のままにせず、パスワードは容易に推測されない複雑なものを設定し、他者に知られないよう、厳重に管理しましょう。
  - パスワードの使い回しをしないようにしましょう。

米SplashData社が発表した「最悪なパスワード　トップ25（2015年版）」

第1位	123456 （1）	第14位	111111 （15）
第2位	password （2）	第15位	1qaz2wsx（New）
第3位	12345678 （4）	第16位	dragon （9）
第4位	qwerty （5）	第17位	master （19）
第5位	12345 （3）	第18位	monkey （12）
第6位	123456789（6）	第19位	letmein （13）
第7位	football （10）	第20位	login （New）
第8位	1234 （7）	第21位	princess（New）
第9位	1234567 （11）	第22位	qwertyuiop （New）
第10位	baseball（8）	第23位	solo （New）
第11位	welcome （New）	第24位	passw0rd （New）
第12位	1234567890 （New）	第25位	starwars （New）
第13位	abc123 （14）		

（ ）内は前年順位

出典：米SplashData社ホームページ

（参考）ウェブサイト閲覧時の注意事項

- 標的とされた対象者がよく利用するウェブサイトにウイルスを仕掛け、標的とされた対象者が閲覧したときのみウイルスに感染させ、情報の窃取を行う「水飲み場型攻撃」があります。
  - パソコンのOS（Windows等）やソフトウェアの更新プログラムは、定期的に適用しましょう。