

メールについて ～身に覚えのない電子メールの対応～

メールについて ～身に覚えのない電子メールの対応～

Part2: 従業員としての対策 — No. 6

導入



パソコンを使っている人であれば、誰もがコンピュータ**ウイルス**の脅威について、一度は耳にしたことがあるでしょう。パソコンに感染してOSの動作を遅くしたり・・・データを破壊したり・・・悪質なものになると、個人や会社の**重要情報**を盗み出すなど、大きな被害をもたらす困った存在です。

用語解説

●ウイルス

他のファイルやプログラムに寄生し、不正な行為を行うプログラム。

「コンピュータウイルス対策基準」（平成12年 経済産業省告示）によると、「第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、自己伝染機能、潜伏機能、発病機能の各機能を一つ以上有するもの」と定義されている。

最近では、ウイルス、スパイウェア、ボットなどの不正プログラムを総称して「マルウェア」と呼んでいる。

【出典】

情報セキュリティ読本 I T時代の危機管理入門（六訂版）

著作：独立行政法人情報処理推進機構

発行：実教出版株式会社

用語解説

●重要情報【じゅうようじょうほう】

- ・ お客様や取引先の連絡先
 - ・ 社員の住所や給与情報
 - ・ 会社の経理情報
 - ・ 取引先毎の仕切り額の一覧表や取引実績
 - ・ 競合相手に見られては困る新製品情報
 - ・ 取引先から取り扱い注意と言われた情報
- 等

事業活動に有用な技術上又は営業上の情報は営業秘密として管理しておく必要があります。

- (1) 秘密として管理されていること（秘密管理性）
- (2) 事業活動に有用な技術上又は営業上の情報であること（有用性）
- (3) 公然と知られていないこと（非公知性）

以上、3つの条件を満たすことにより、営業秘密として法的に認められます。各種ファイルが不正競争防止法で定義される営業秘密の要件を満たすために、社内でそのルールを決めたマニュアルを作成しましょう。営業秘密かそうでないかをきちんと分けしないと、何でもかんでも「秘密」にしていたずらに業務を煩雑化する恐れがあります。

導入



ウイルスを感染させる手口として、電子メールを使った攻撃は今でも多く、メール本文や添付ファイルの確認時は、とりわけ注意が必要です。

用語解説

●ウイルス

他のファイルやプログラムに寄生し、不正な行為を行うプログラム。

「コンピュータウイルス対策基準」（平成12年 経済産業省告示）によると、「第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、自己伝染機能、潜伏機能、発病機能の各機能を一つ以上有するもの」と定義されている。

最近では、ウイルス、スパイウェア、ボットなどの不正プログラムを総称して「マルウェア」と呼んでいる。

【出典】

情報セキュリティ読本 IT時代の危機管理入門（六訂版）

著作：独立行政法人情報処理推進機構

発行：実教出版株式会社

導入

身に覚えのない電子メールであれば、なおさら軽率にクリックしないよう慎重にならなければいけません。
こうしたことにならないように・・・。

事例


もしもし、橘建築設計事務所です。
いつもお世話様です。
はい、おります。
少しお待ちください。

事例

原田さん、電話。
施主のシロガネ不動産さんから。

シロガネ不動産？なんだろう。
今、取り急ぎの用件は無いんだけどな。

事例



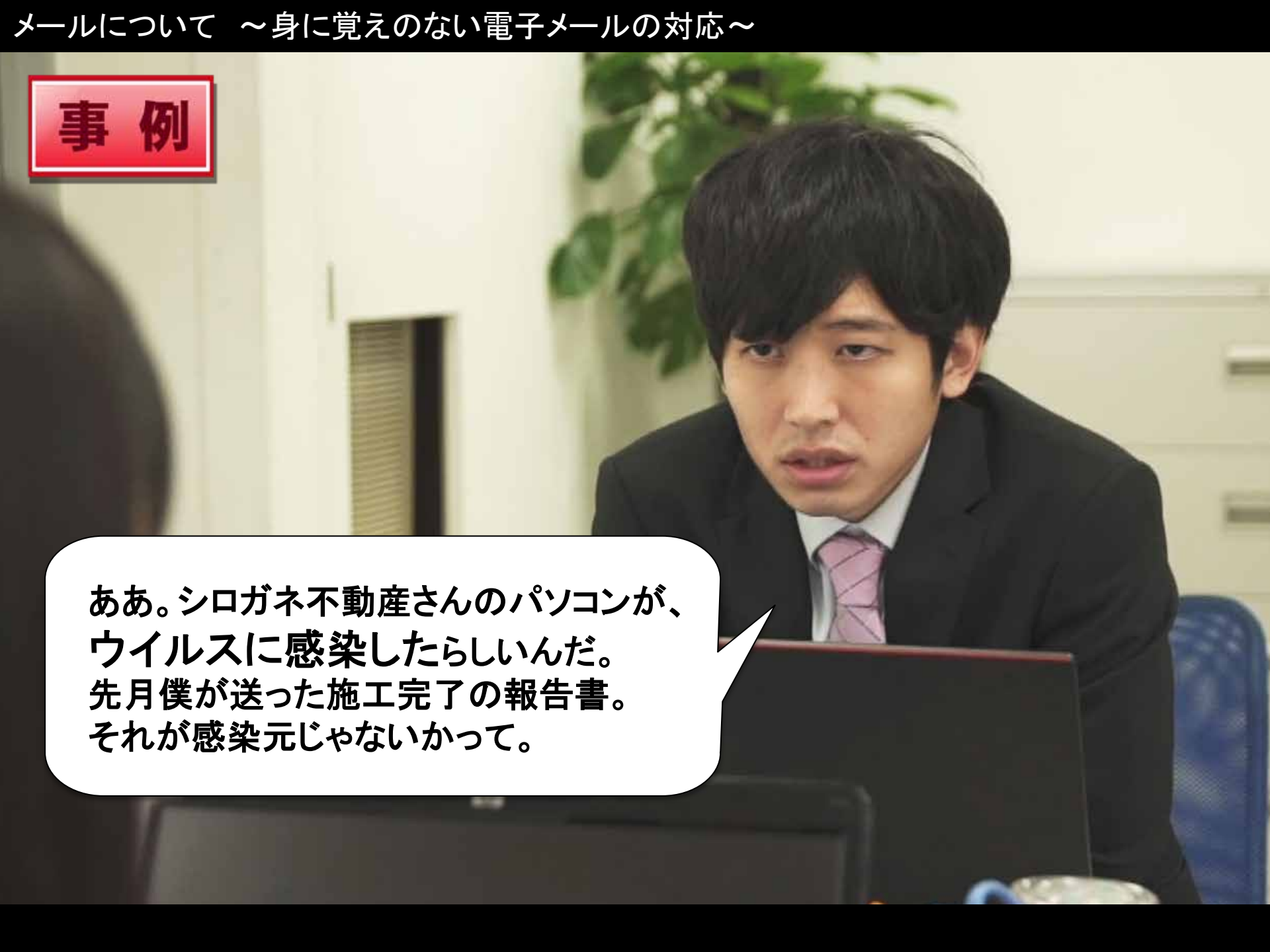
はい、代わりました。
はい、はい。エー！！
そうですけど、いやー、
そういうことは無いと思うんですが…、
はい。はい。

事 例

どうしたの？
何かあったの？



事例



ああ。シロガネ不動産さんのパソコンが、
ウイルスに感染したらしいんだ。
先月僕が送った施工完了の報告書。
それが感染元じゃないかって。

事例

原田さんの送ったファイルから
ウイルスに感染？
ヤダ！ そんな、ファイル扱ってたの？

じょーだんでしょ！
そんなこと、僕がする訳無いじゃない！

事例

でも。シロガネ不動産さんだって、
根拠の無い指摘をするはずもないし・・・、
何か心当たりでもあるんじゃない？

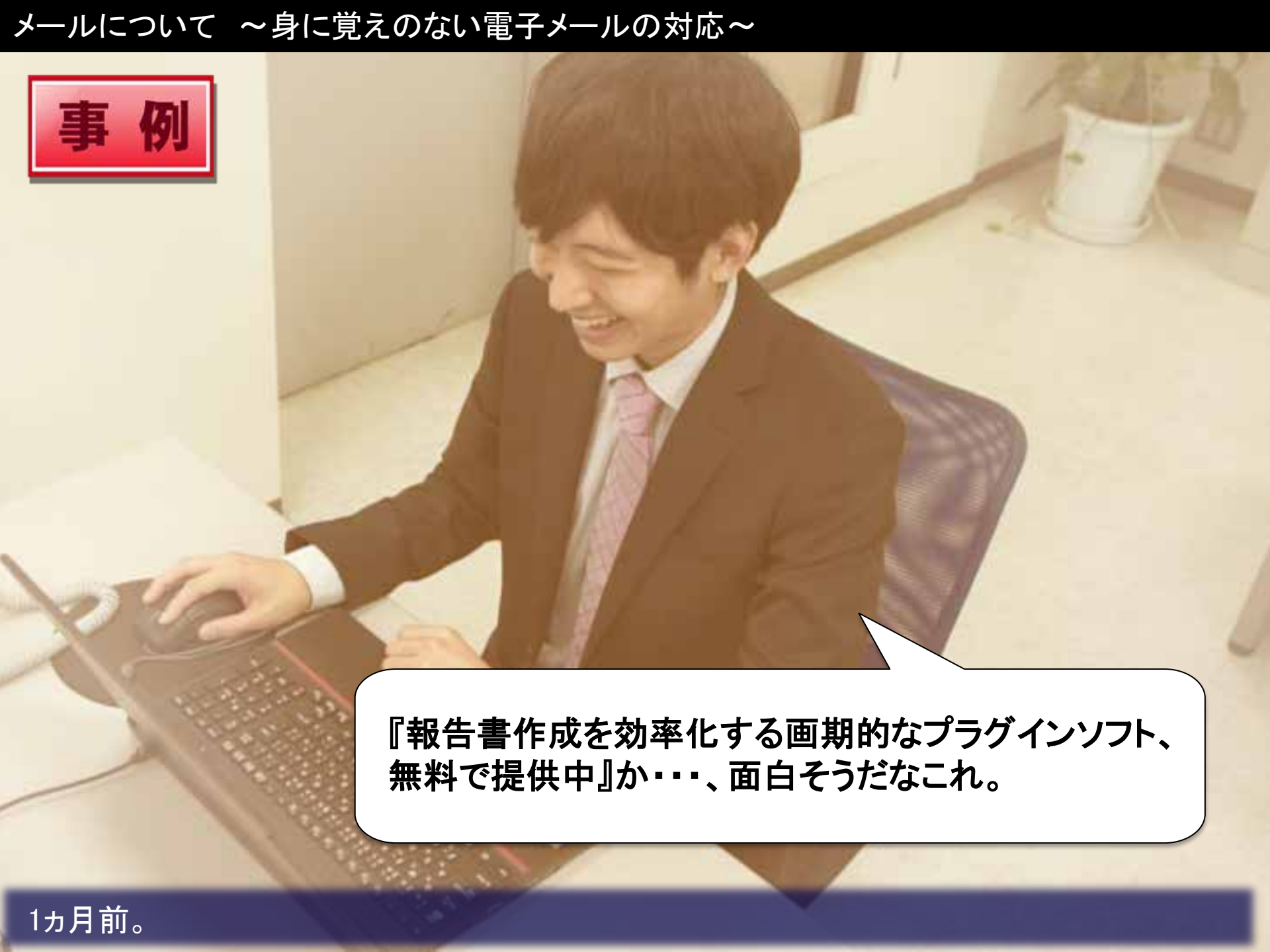


事例

うーん…

そう言えば、身に覚えのない広告メールの中に書かれていたURLをクリックして…。

事例

A man with dark hair, wearing a dark suit, white shirt, and pink tie, is sitting at a desk. He is smiling and looking down at a computer mouse he is holding with his right hand. His left hand is resting on the desk. A keyboard is visible in front of him. The background shows a white wall and a potted plant on the floor.

『報告書作成を効率化する画期的なプラグインソフト、
無料で提供中』か・・・、面白そうだなこれ。

1ヵ月前。

事例

それって、危ないんじゃない！？
身に覚えのないメールに書かれているURLリンク先なんて、
どこのウェブサイトにつながってるかわからないし、
ダウンロードしたソフトも、実はウイルスそのものかも知れないじゃない。

うーん、そうなのかなあ・・・。

学習の意図



このように、自分では気がつかないところでウイルスに感染し、知らずにそれをまき散らしてしまっているということが、インターネット社会では頻繁に発生します。

用語解説

●ウイルス

他のファイルやプログラムに寄生し、不正な行為を行うプログラム。

「コンピュータウイルス対策基準」（平成12年 経済産業省告示）によると、「第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、自己伝染機能、潜伏機能、発病機能の各機能を一つ以上有するもの」と定義されている。

最近では、ウイルス、スパイウェア、ボットなどの不正プログラムを総称して「マルウェア」と呼んでいる。

【出典】

情報セキュリティ読本 I T時代の危機管理入門（六訂版）

著作：独立行政法人情報処理推進機構

発行：実教出版株式会社

学習の意図

例えば、電子メールに添付されていたファイルや、インターネットからダウンロードしたソフトウェアなどに、**ウイルス**が混入していることがありますし、電子メールそのものや、電子メールの本文に書かれているURLリンク先のウェブサイトなどの画面に仕込まれていることもあります。

用語解説

●ウイルス

他のファイルやプログラムに寄生し、不正な行為を行うプログラム。

「コンピュータウイルス対策基準」（平成12年 経済産業省告示）によると、「第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、自己伝染機能、潜伏機能、発病機能の各機能を一つ以上有するもの」と定義されている。

最近では、ウイルス、スパイウェア、ボットなどの不正プログラムを総称して「マルウェア」と呼んでいる。

【出典】

情報セキュリティ読本 IT時代の危機管理入門（六訂版）

著作：独立行政法人情報処理推進機構

発行：実教出版株式会社

学習の意図

身に覚えのないメールであれば、なおさら軽率に添付ファイルを開いたり、メール本文内のURLリンク先をクリックしてはいけません。

学習の意図

「身に覚えのない電子メール」について、以下を学習しましょう。

1. 身に覚えのない電子メールに添付されたファイルは開かないようにする
2. メール本文に書かれているURLリンク先を安易にクリックしないようにする
3. 不審なウェブサイトにはアクセスしないようにする
4. ウイルス対策ソフトをパソコンにインストールする

正しい対処法



ウイルスはさまざまな感染ルートから入り込んできます。送り主の不明な電子メールに添付されたファイルや、電子メールの本文に書かれているURLリンク先のウェブサイトなどにも、**ウイルス**が潜んでいることがあるのです。

用語解説

●ウイルス

他のファイルやプログラムに寄生し、不正な行為を行うプログラム。

「コンピュータウイルス対策基準」（平成12年 経済産業省告示）によると、「第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、自己伝染機能、潜伏機能、発病機能の各機能を一つ以上有するもの」と定義されている。

最近では、ウイルス、スパイウェア、ボットなどの不正プログラムを総称して「マルウェア」と呼んでいる。

【出典】

情報セキュリティ読本 IT時代の危機管理入門（六訂版）

著作：独立行政法人情報処理推進機構

発行：実教出版株式会社

正しい対処法



第三者に提供されたファイルにも、**ウイルス**が感染していることがあるので、きちんと安全性が確認できるファイル以外は、軽率に開かないようにしましょう。
もしファイルを開いてしまったら、システム管理者に報告し、対応を指示してもらいましょう。

用語解説

●ウイルス

他のファイルやプログラムに寄生し、不正な行為を行うプログラム。

「コンピュータウイルス対策基準」（平成12年 経済産業省告示）によると、「第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、自己伝染機能、潜伏機能、発病機能の各機能を一つ以上有するもの」と定義されている。

最近では、ウイルス、スパイウェア、ボットなどの不正プログラムを総称して「マルウェア」と呼んでいる。

【出典】

情報セキュリティ読本 IT時代の危機管理入門（六訂版）

著作：独立行政法人情報処理推進機構

発行：実教出版株式会社

確認テスト 問題

No.6 メールについて ～身に覚えのない電子メールの対応～

Q1

身に覚えのない電子メールについて、適切なのはどちらでしょう。

選択肢	
	1. メールの本文に書かれているURLリンク先は、かならずクリックして確認する。
	2. メールの添付ファイルは、安全が確認できるまで軽率に開かない。

次のページで正解と
解説を確認しましょう

確認テスト 正解と解説

Q1

身に覚えのない電子メールについて、適切なのはどちらでしょう。

正解	選択肢
	1. メールの本文に書かれているURLリンク先は、かならずクリックして確認する。
●	2. メールの添付ファイルは、安全が確認できるまで軽率に開かない。

【解説】

メールの添付ファイルや、メール本文に書かれているURLリンク先、インターネットでダウンロードしたファイルを軽率に開くことは、ウイルス感染のリスクが高い行為です。むやみやたらに開いたり、クリックしたりしないようにして下さい。