

情報収集について ～脅威や攻撃の手口を知る～

# 情報収集について ～脅威や攻撃の手口を知る～

Part1: 基本的対策 — No. 5

## 導入



取引先や関係者と偽ってウイルス付きのメールや偽の取引メールを送ってきたり、正規のウェブサイトに見せた偽のウェブサイトを立ち上げて、IDやパスワードを盗もうとする巧妙な手口が増えています。

## 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

## 導入

こうした手口の存在を知らずに、攻撃に遭遇してしまうと、焦ってしまって適切な対応が取れない事が考えられます。

## 導入

予め脅威や手口を把握しておくことで、適切な対応を取り被害を予防できます。そのためには、報道やセキュリティ関連機関、利用中のインターネットバンキングなどの注意喚起等の情報源から、セキュリティに関する脅威や犯罪の手口を知る事が重要です。



## 事例



おや？オギノ建設からメールだ。

## 事例

A man in a dark suit, white shirt, and pink tie is sitting at a desk in an office. He has a distressed expression, with his right hand pressed against his temple and his mouth slightly open as if speaking or reacting. In front of him is a computer monitor. To his right, there are several colorful file folders (blue, yellow, green) standing upright. On the desk, there are various office supplies like pens, pencils, and a stapler. The background shows a typical office environment with a window and some plants.

えーと何々…、え！？急な話だな。

## 事例

原田さん、何か問題でも起こったのか？

いえ、問題ではないんですけど…  
今、オギノ建設からメールが送られてきて、  
今回の依頼に関する支払いの銀行口座を  
変えてくれと言ってきたんです。




## 事例



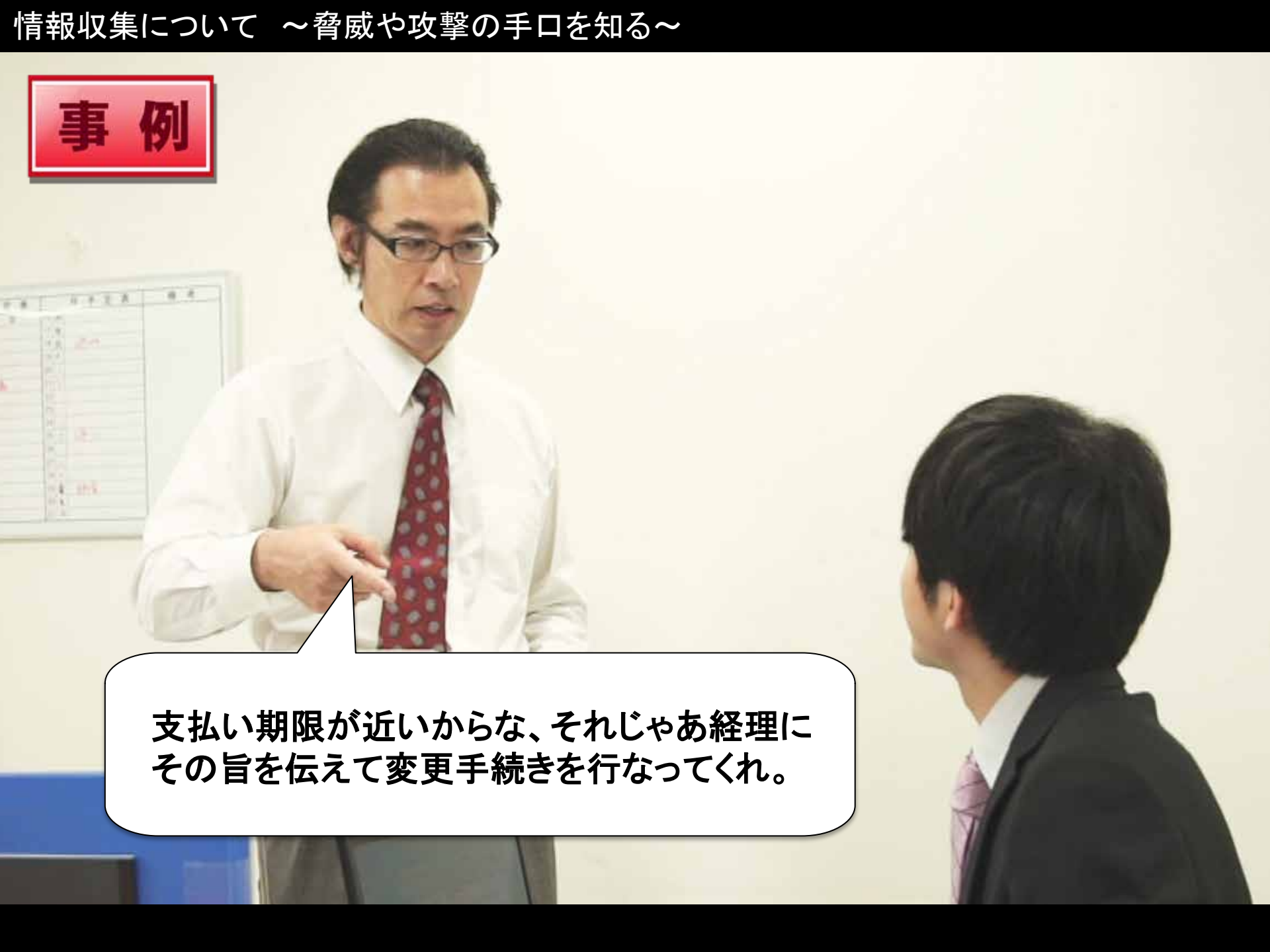
それはまた唐突だな、  
それまで普通に使っていた口座なんだろう？  
変更理由はなんて言ってるんだ？

## 事例



それが、理由は特に書いてなくて…  
ただ急いでいるのはたしかです。

## 事例

A man in a white shirt and red tie is speaking to another man in a suit. The man in the white shirt is gesturing with his hands while speaking. The man in the suit is listening attentively. A speech bubble is present at the bottom of the image containing Japanese text.

支払い期限が近いからな、それじゃあ經理に  
その旨を伝えて変更手続きを行なってくれ。

## 事例

はい、わかりました。





## 事例

ちょっと待ってください。  
変更手続きを行なう前に、  
一度先方に確認してみては？

## 事例

このメールか・・・  
たしかに今までのメールのやり取りが  
履歴として残っているメールだね、  
でも・・・。



## 事例

送り主のメールアドレス、  
本物と少し違うかい？

あれ！？メールアドレスのスペルが違うぞ！！  
I（アイ）とl（エル）の位置が逆になっている。

## 事例



それによく見ると、先方の関係者のメールアドレスも少しずつ違ってるとぞ！

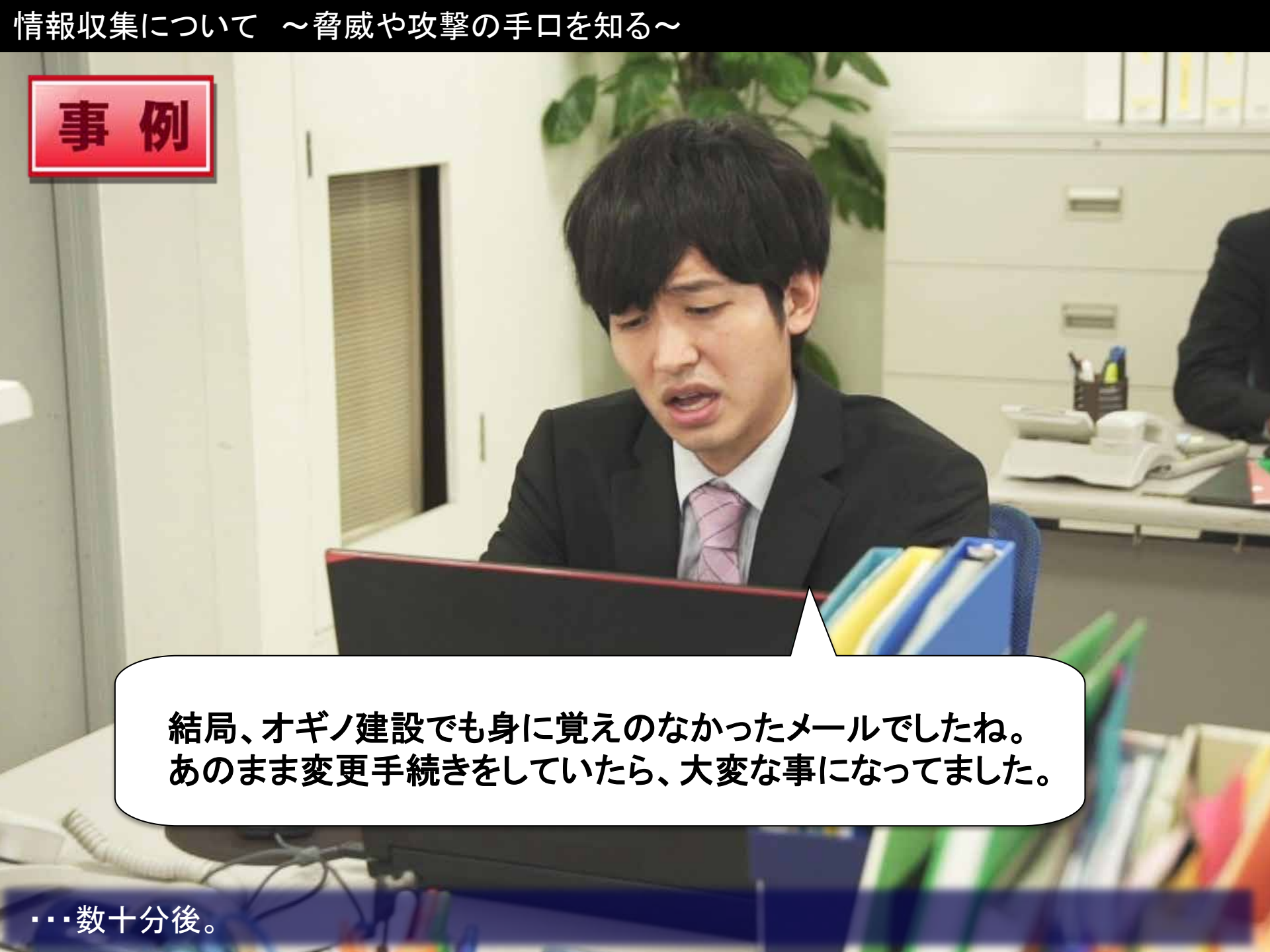


## 事例

やっぱり・・・これは詐欺メールだね。  
先方の関係者には誰にも返信されないように  
細工もされている。  
念のために先方にも確認してみよう。



## 事例

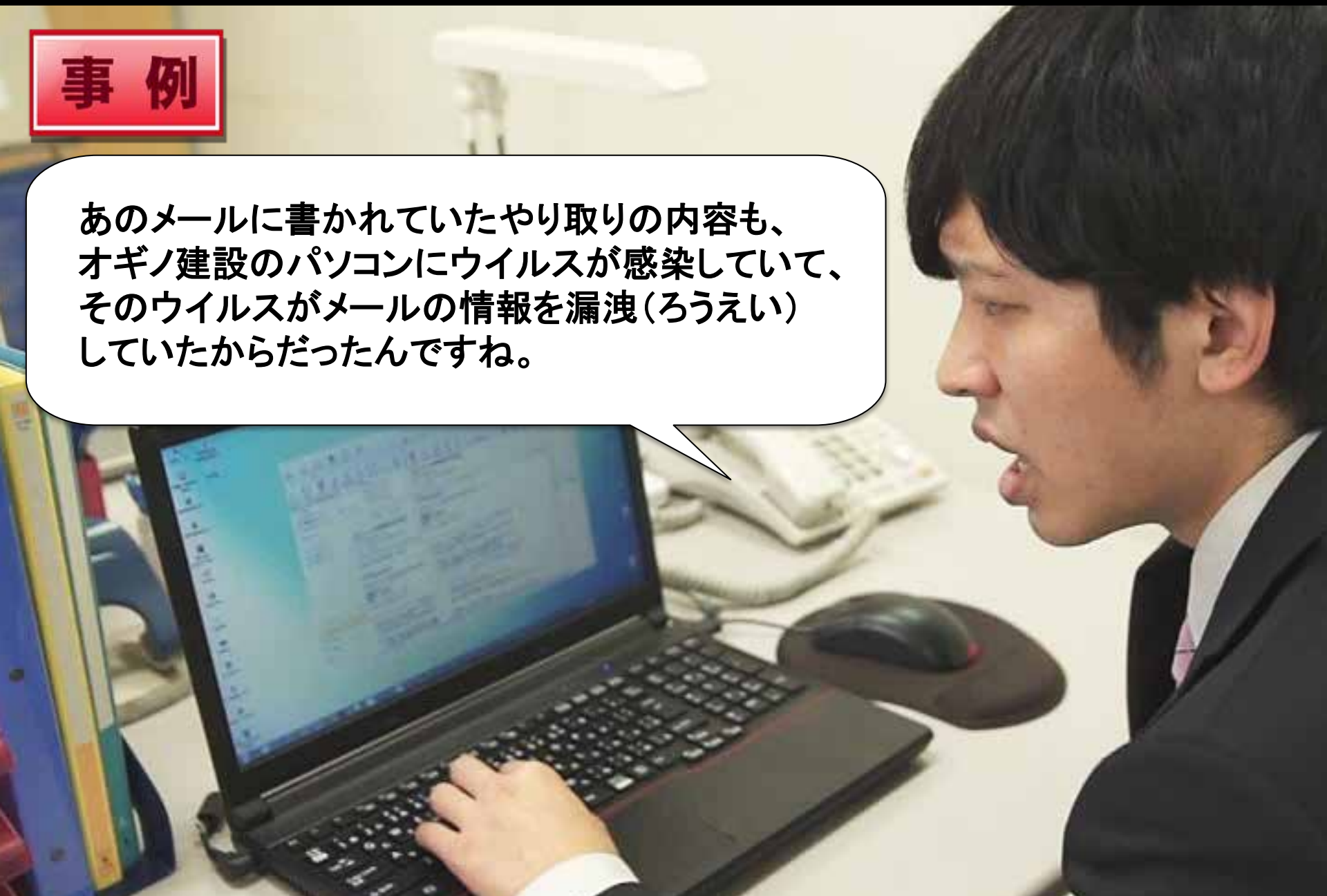
A man with dark hair, wearing a black suit, white shirt, and a pink patterned tie, is sitting at a desk in an office. He is looking down at a laptop screen with a concerned expression. In the background, there are office shelves with binders, a potted plant, and another desk with a printer and papers. A speech bubble is positioned in front of him.

結局、オギノ建設でも身に覚えのなかったメールでしたね。  
あのまま変更手続きをしていたら、大変な事になってました。

…数十分後。

## 事例

あのメールに書かれていたやり取りの内容も、オギノ建設のパソコンにウイルスが感染していて、そのウイルスがメールの情報を漏洩（ろうえい）していたからだったんですね。



## 事例

それにしても、  
名取さんよく気が付いたね。





## 事例

インターネットのセキュリティニュースで  
読んだ事のある事例でしたので。  
入金直前に口座を変更してくる手口が  
ちょっと気になったので。



## 事例

でも、まさか自分の会社でそうした事が  
起こるなんて思ってもみませんでしたよ。  
こんな小さな設計事務所も狙われるのだから、  
業種や会社の規模は関係ないようですね。



**事例**

名取さん、「小さな」は余計じゃないかね。

あっ！ すいません…。





## 学習の意図



巧妙に細工されたメールのやりとりにより、企業の担当者を騙し、攻撃者の用意した口座へ送金させる手口のビジネスメール詐欺。こうした詐欺メールの手口は、技術的な対策による防止が難しく、一人ひとりが手口を理解し、“怪しさ”を見抜くことが重要です。



## 学習の意図



不審なメールに担当者が気づけることは重要ですが、それと同時に、その情報を社内で共有することで、他の担当者に届いた詐欺メールに気づくことができ、被害を未然に防ぐことも可能です。

## 学習の意図



また、ビジネスメール詐欺に限らず、新たな脅威や攻撃の手口について、普段から情報セキュリティに関するニュースや注意喚起の内容等をインターネット上から情報収集しておき、社内で共有しておくことも対策の一つになります。

## 学習の意図

「情報収集」について、以下を学習しましょう。

1. 新たな脅威や攻撃の手口を知り、対策を社内で共有する。

## 正しい対処法

ビジネスメール詐欺の様な攻撃は、どの従業員がいつ攻撃の対象となるかは分かりません。このような攻撃に対抗するため、こうした攻撃手口を理解するとともに、不審なメールなどへの意識を高めておくことが重要です。



## 正しい対処法

不審なメールなどの情報は、集約して社内で共有できる体制を作っておきましょう。  
そうすることで、他の担当者に届いた詐欺メールに気づくことができ、被害を未然に防ぐことも可能です。

## 正しい対処法



日頃から、IPAのウェブサイトやメールマガジン、利用中のSNSやインターネットバンキングなどが提供する注意喚起等を利用して情報収集を行ない、最新の脅威や攻撃手口の情報を社内で共有しておきましょう。

## 確認テスト 問題

### No.5 情報収集について ～脅威や攻撃の手口を知る～

#### Q1

次のセキュリティ対策について、適切なのはどれか答えなさい。

#### 選択肢

- |  |   |
|--|---|
|  | 1. テレビニュースなどで注意喚起していた詐欺メールが、会社のメールアドレスに届いたので、直ぐに削除した。           |
|  | 2. 取引先から添付ファイル付きのメールが届いたが、身に覚えがないので、メール内に書かれていた連絡先に確認のメールを送った。  |
|  | 3. 利用しているインターネットバンキングから、新たな詐欺メールの注意喚起メールが届いたので、会社内や家族内で情報を共有した。 |

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

次のセキュリティ対策について、適切なのはどれか答えなさい。

正解	選択肢
	1. テレビニュースなどで注意喚起していた詐欺メールが、会社のメールアドレスに届いたので、直ぐに削除した。
	2. 取引先から添付ファイル付きのメールが届いたが、身に覚えがないので、メール内に書かれていた連絡先に確認のメールを送った。
●	3. 利用しているインターネットバンキングから、新たな詐欺メールの注意喚起メールが届いたので、会社内や家族内で情報を共有した。

### 【解説】

詐欺メールなどの攻撃や犯罪の手口を事前に知っていることで、被害に遭いづらくなります。情報の収集元として、IPA が公開している「安心相談窓口だより」や、官公庁やセキュリティ企業が公表しているレポートが参考になります。定期的に情報を収集し、社内や家族、知り合いの中で情報を共有し、被害に遭わないように備えておきましょう。もしその様なメールが届いたら、勝手に削除したり、送り主に連絡をするのではなく、システム管理者の指示に従い、適切に対処しましょう。