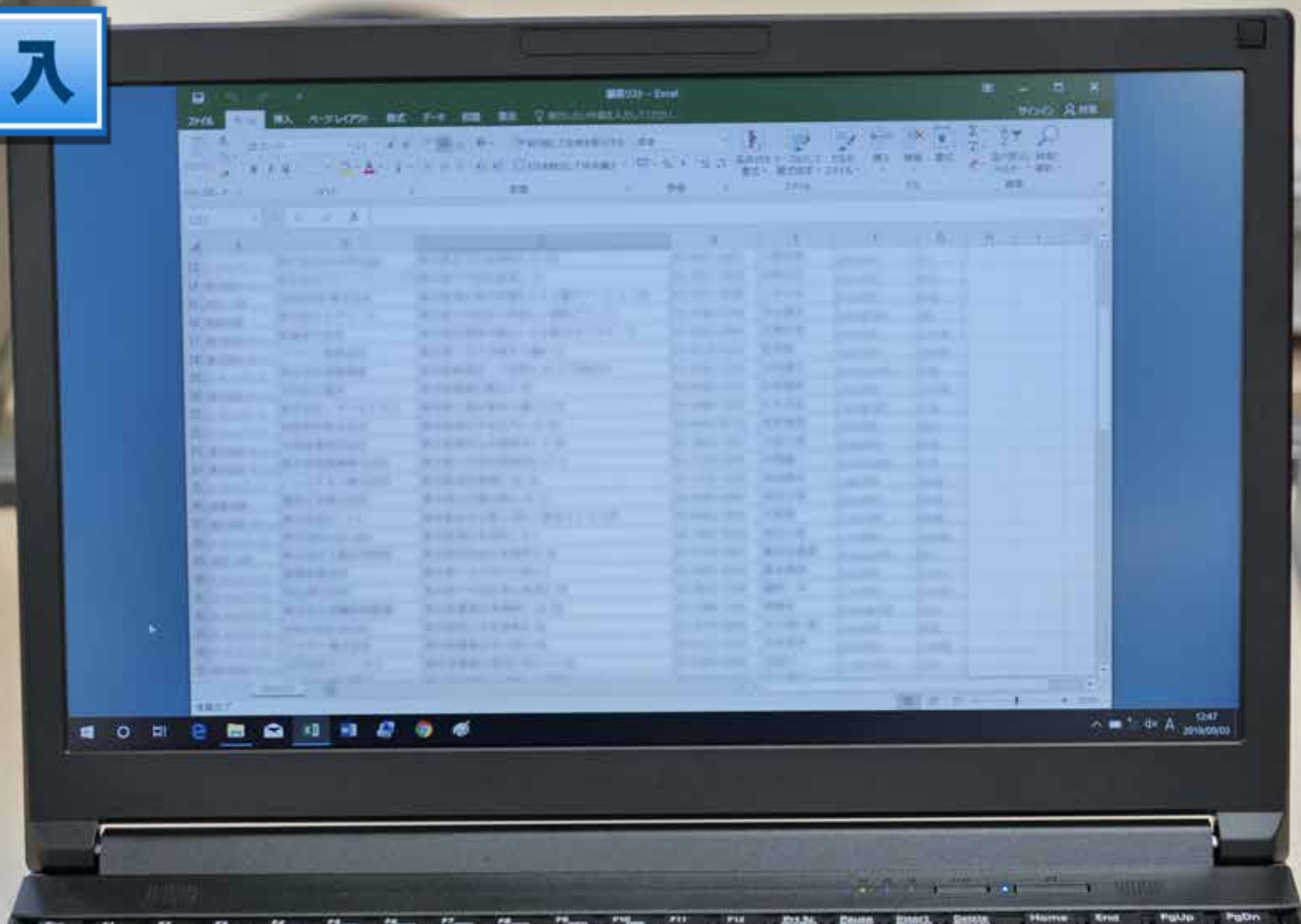


取引先や委託先を含めたセキュリティ対策

～ ビジネスパートナーも含めたセキュリティ対策の重要性 ～

経営者・管理者向けコース — No.6

導入



多くの悪意ある攻撃者は、攻撃対象の企業から個人情報等を盗もうとした場合、直接対象企業に攻撃を仕掛けますが、最近では対象企業の関連企業や取引先企業、委託先企業やビジネスパートナーなどの、比較的セキュリティ対策が不十分な関連企業を探し出して攻撃を行ない、攻撃が成功した関連企業を踏み台にして、対象企業に迫っていく攻撃が見受けられます。

導入



これでは、せっかく自分たちが適切なセキュリティ対策を行なっている、周りの影響によって攻撃にさらされる危険があると言えるでしょう。

導入



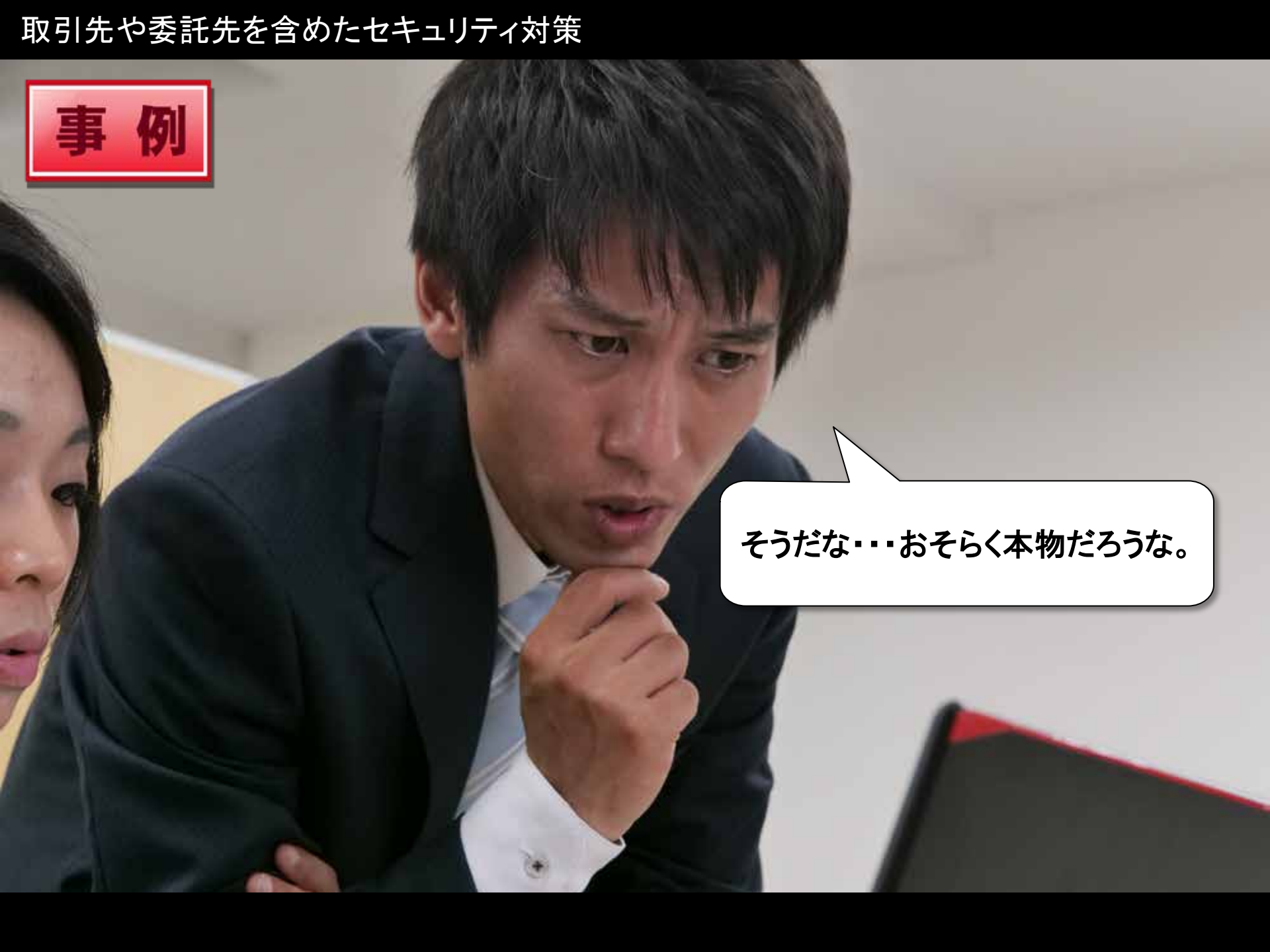
これからは自社のセキュリティ対策の強化だけでなく、関連企業はもとより、取引先企業や委託先企業、ビジネスパートナーも含めたセキュリティ対策の強化が求められています。

事例

田端さん、
この情報って本物ですか？


広瀬洋子 【株式会社シックハック／総務部社員】
田端健一 【株式会社シックハック／転職して間もないシステム管理者】

事例



そうだな・・・おそらく本物だろうな。

事例

A woman with short dark hair, wearing a black blazer over a white collared shirt, is pointing her right index finger upwards. She is looking towards a man whose back is partially visible on the right side of the frame. The background consists of light-colored horizontal blinds.

そうですか・・・と言うことは外部の通報者からの言うとおりに、
ウチの系列企業でもあるシックハック物流から、
顧客情報が漏洩(ろうえい)したということですね？

事例

まだ調査中だがほぼ間違いないだろう・・・
わが社も同じ情報を持っているが、
わが社からの漏洩ではないと確認できたからね。

でもこの状況だと、わが社にも少なからず影響は出そうだ。

事例

うちの顧客からのお叱り電話やメールですか・・・
考えるだけで嫌になりますね、ウチが漏らした訳ではないのに。

事例

まあそう言わずに、そのような連絡があったらしっかり対応しておいてくれ。
これからの対応も含めて、
わが社の系列企業全体で協議することになってるから。

はい、わかりました。

事例

でもわが社の系列会社が何かしらの攻撃を受けていたということは、わが社もその攻撃を受けていたと考えられるな。

そういうものなんですか？
ウチも攻撃を受けていたってことは、
ウチが漏らしていたかもってことですか？




事例

その可能性もあったってことさ。

最近では攻撃対象の企業を直接狙うのではなく、対象企業の系列企業や、仕事上での関連企業、ビジネスパートナーや委託先企業、と言うところから攻撃を行ない、攻撃が成功してそこで得た情報を元に対象企業に攻撃を移していく、と言う手口が多いと聞くよ。

事例



そんな、わざわざ遠回りするような攻撃が流行っているんですか？

事例

確かに遠回りだな。

しかしセキュリティ対策がおろそかな企業や組織があれば、そこから情報を窃取するのはたやすくなるだろう？

事例

そうされないためにも、
自社も含めた企業や組織のセキュリティ対策はもちろん、
仕事を委託しているところなどは、委託先のセキュリティ対策管理も
怠らなく行なうことが重要と言えるな。



学習の意図



自社が起こした**インシデント**ではないにしても、関連企業や委託先企業などから発生したインシデントから、自社が攻撃されることもあります。その結果、思わぬ2次被害を誘発してしまい、自社が加害者となる恐れもあります。

用語解説

●インシデント (incident)

情報セキュリティ分野において、情報セキュリティリスクが発現・現実化した事象のこと。

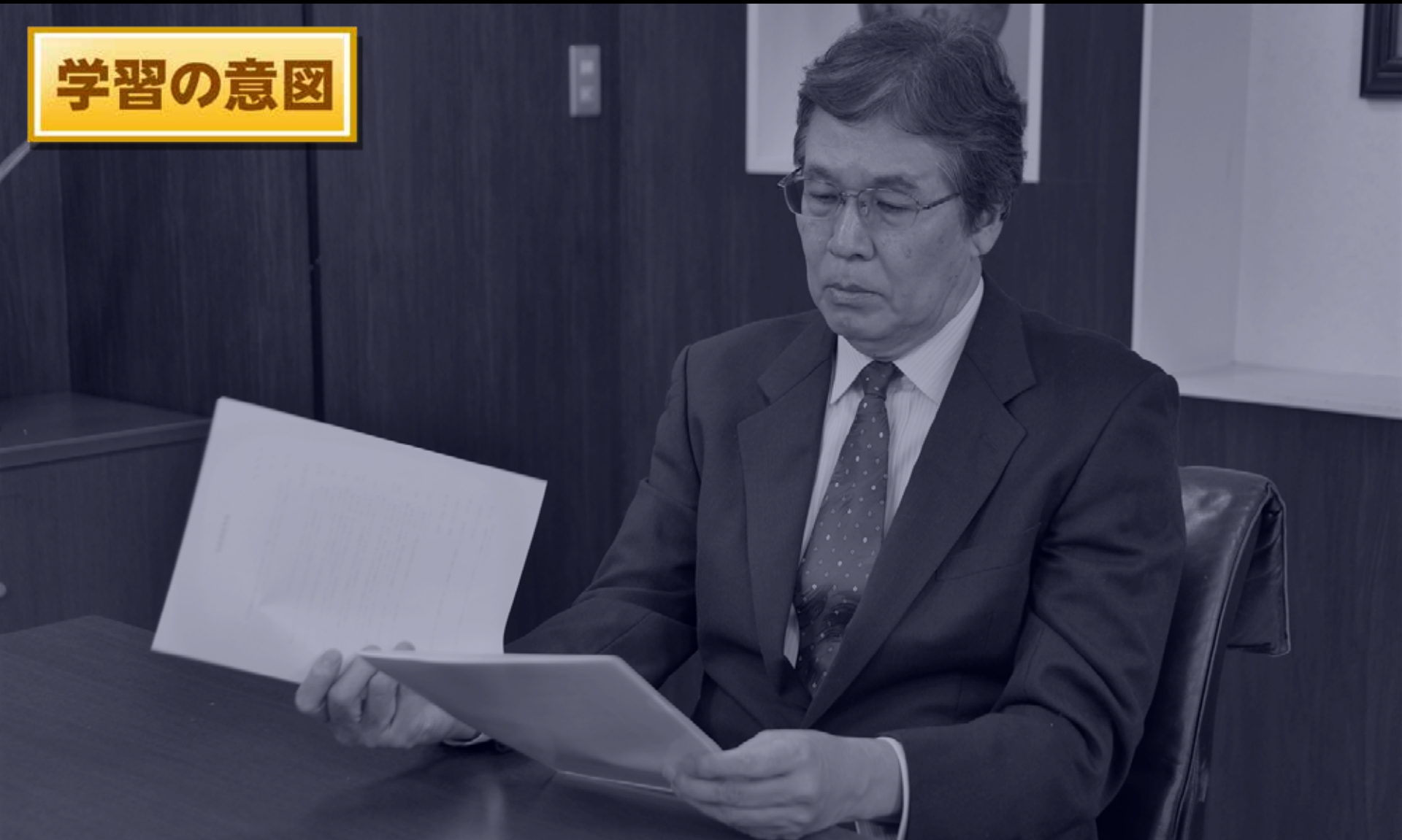
【出典】

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



そのため、関連企業や取引先企業、委託先があれば、再委託先やさらにその先の委託先の企業を含めたセキュリティ対策が必要となります。

学習の意図

「取引先や委託先を含めたセキュリティ対策」について、
以下を学習しましょう。

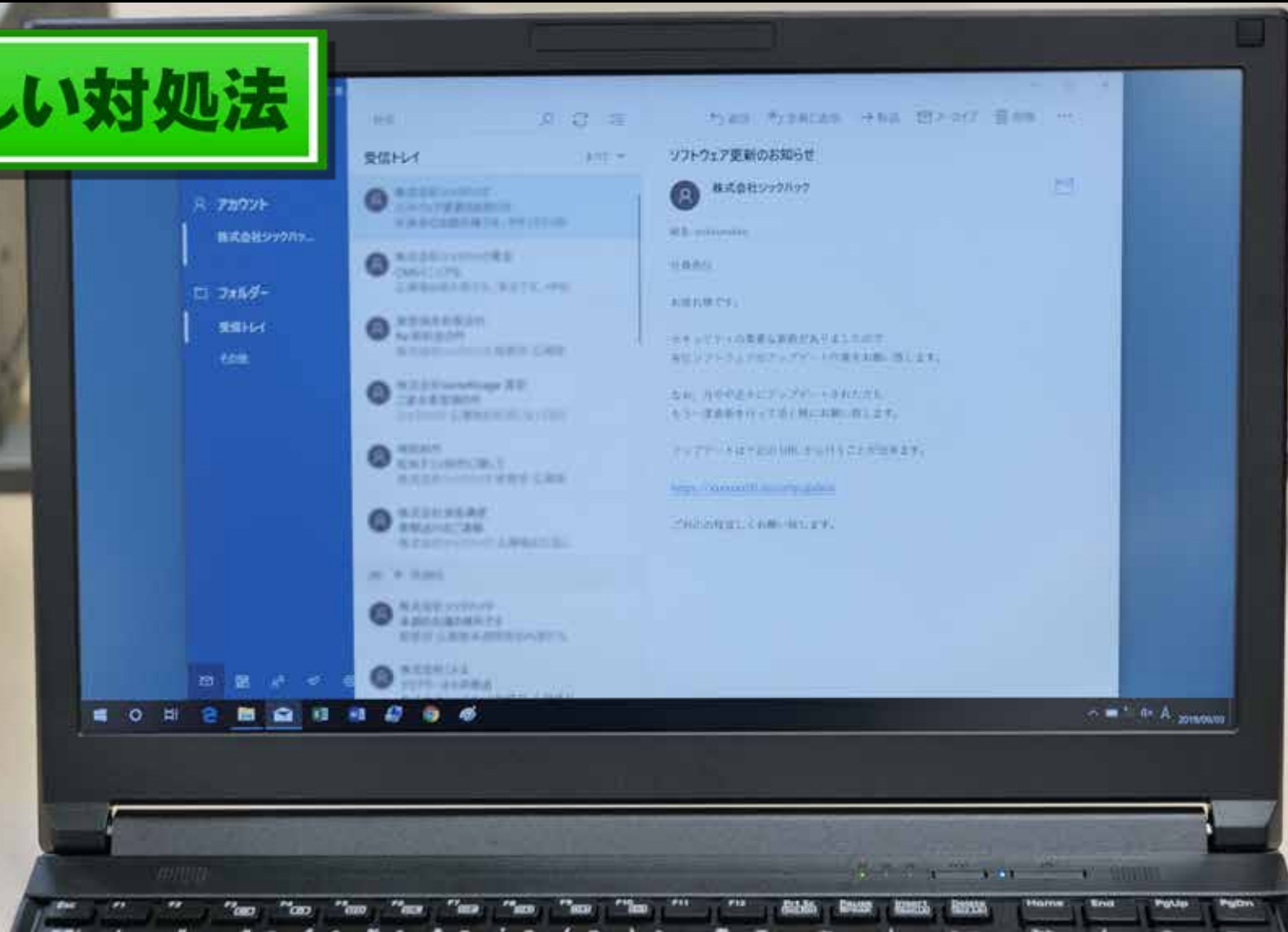
1. 関連企業や取引先企業、委託先企業を含めたセキュリティ対策の重要性

正しい対処法



情報セキュリティ上何らかのトラブルが発生した場合、委託元委託先双方で対応する部分の境界をあいまいにしていると、対応や対策の漏れが生じることが予想されます。双方とも情報セキュリティ上の責任範囲と賠償による負担について、契約の内容も含めて明確化しておきましょう。これは、関連企業や取引先企業でも言えることです。

正しい対処法



また、普段から情報セキュリティに関するコミュニケーションを取っておくことをお勧めします。これは、セキュリティ対策に関するお互いの信頼を高めるだけではなく、**ビジネスメール詐欺**などのいわゆる**標的型攻撃**などに対しても、日頃から連絡を取り合っていることで怪しいと気づきやすく、被害予防にもなるでしょう。

用語解説

●ビジネスメール詐欺（Business E-mail Compromise : BEC）

巧妙な騙しの手口を駆使した、偽の電子メールを組織・企業に送り付け、従業員を騙して送金取引に係る資金を詐取するといった、金銭的な被害をもたらすサイバー攻撃です。詐欺行為の準備として、企業内の従業員などの情報が狙われたり、情報を窃取するウイルスが悪用されることもあります。

【参考】

IPA [ビジネスメール詐欺（BEC）対策特設ページ](#)

●標的型攻撃

主に電子メールを用いて特定の組織や個人を狙う攻撃。攻撃対象の組織や個人に合わせてメールの内容がカスタマイズされているので、怪しいメールとの区別がしにくい。また、不特定多数を攻撃対象としていないため、攻撃サンプルの入手が難しく、ウイルス対策ソフトウェアへの反映が困難になる。

【出典】

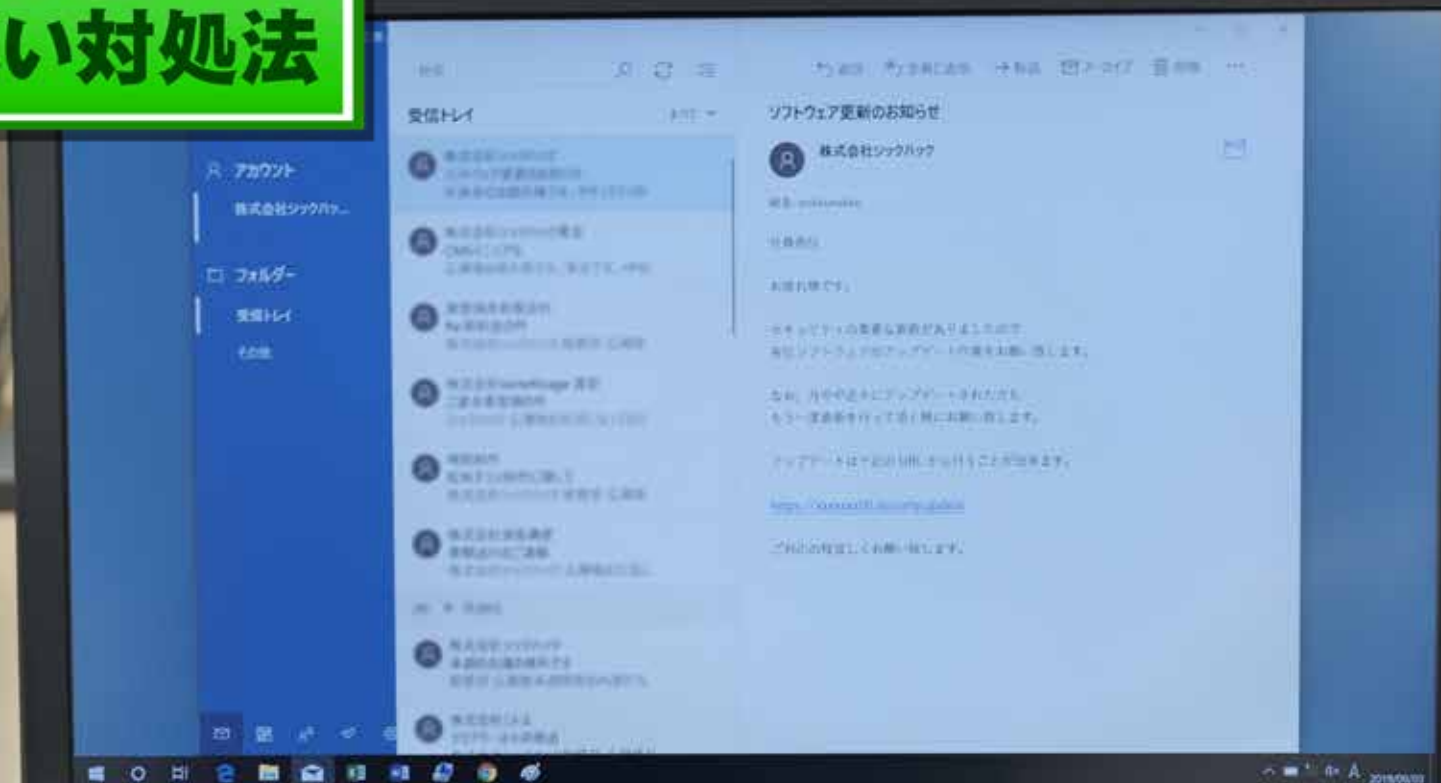
情報セキュリティ読本 I T時代の危機管理入門（六訂版）

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

取引先や委託先を含めたセキュリティ対策

正しい対処法



委託先と取引先を行なっている企業は、責任をもって委託先のセキュリティ対策状況の実態を、定期的に確認することが重要です。もちろんですが、自社のセキュリティ対策の状況も忘れずに把握しておきましょう。

確認テスト 問題

No.6 取引先や委託先を含めたセキュリティ対策 ～ビジネスパートナーも含めたセキュリティ対策の重要性～

Q1

取引先や委託先を含めたセキュリティ対策について、適切なものはどれか。

選択肢

- | | |
|--|---|
| | 1. 情報セキュリティ対策は、委託元、委託先がそれぞれ自社に合った対策を行なうのが望ましい。 |
| | 2. 情報セキュリティ上何らかのトラブルが発生した場合は、委託元、委託先それぞれで対応や対策を行なう。 |
| | 3. 委託元、委託先共に、日頃から情報セキュリティに関するコミュニケーションを取っておく。 |

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

取引先や委託先を含めたセキュリティ対策について、適切なものはどれか。

正解	選択肢
	1. 情報セキュリティ対策は、委託元、委託先がそれぞれ自社に合った対策を行なうのが望ましい。
	2. 情報セキュリティ上何らかのトラブルが発生した場合は、委託元、委託先それぞれで対応や対策を行なう。
●	3. 委託元、委託先共に、日頃から情報セキュリティに関するコミュニケーションを取っておく。

【解説】

日頃から情報セキュリティに関する事故報道などを共有し、連絡などのコミュニケーションを取り合うことで、標的型攻撃メールなどの怪しいメールにも気づきやすく、被害予防につながります。