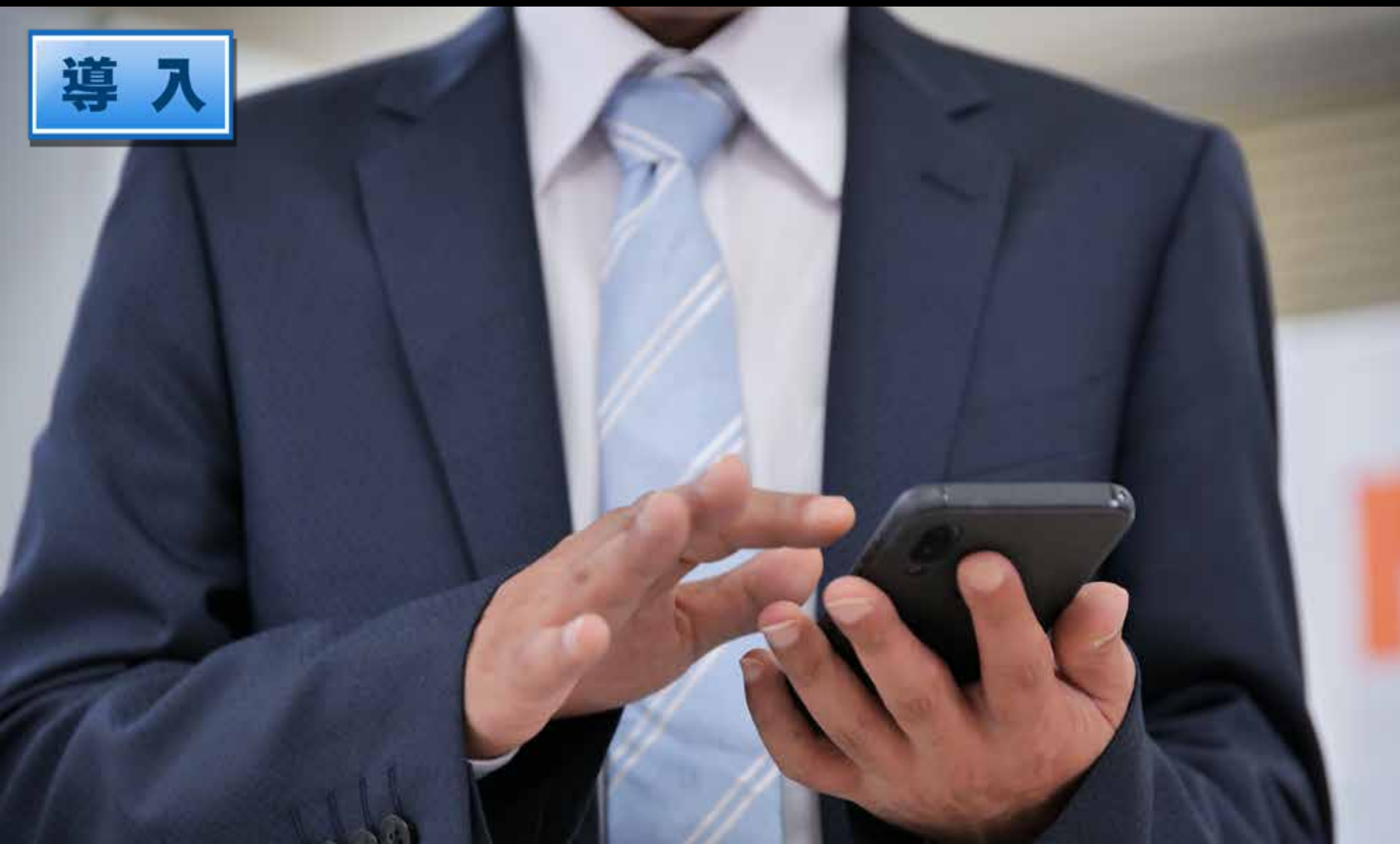


スマートフォンの職場使用

～ 個人のスマートフォンを職場で使わせる メリットとデメリットとは ～

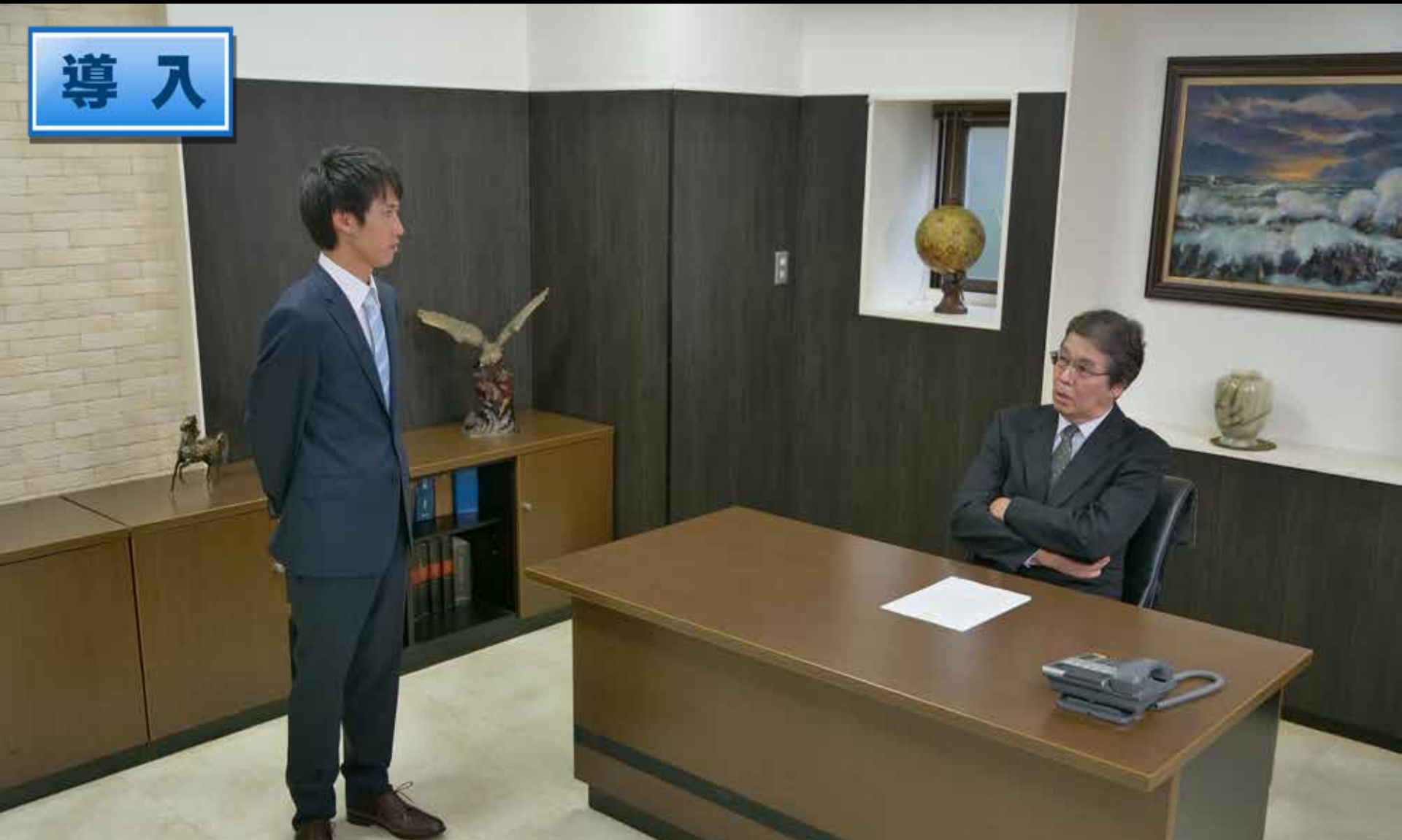
経営者・管理者向けコース — No.4

導入



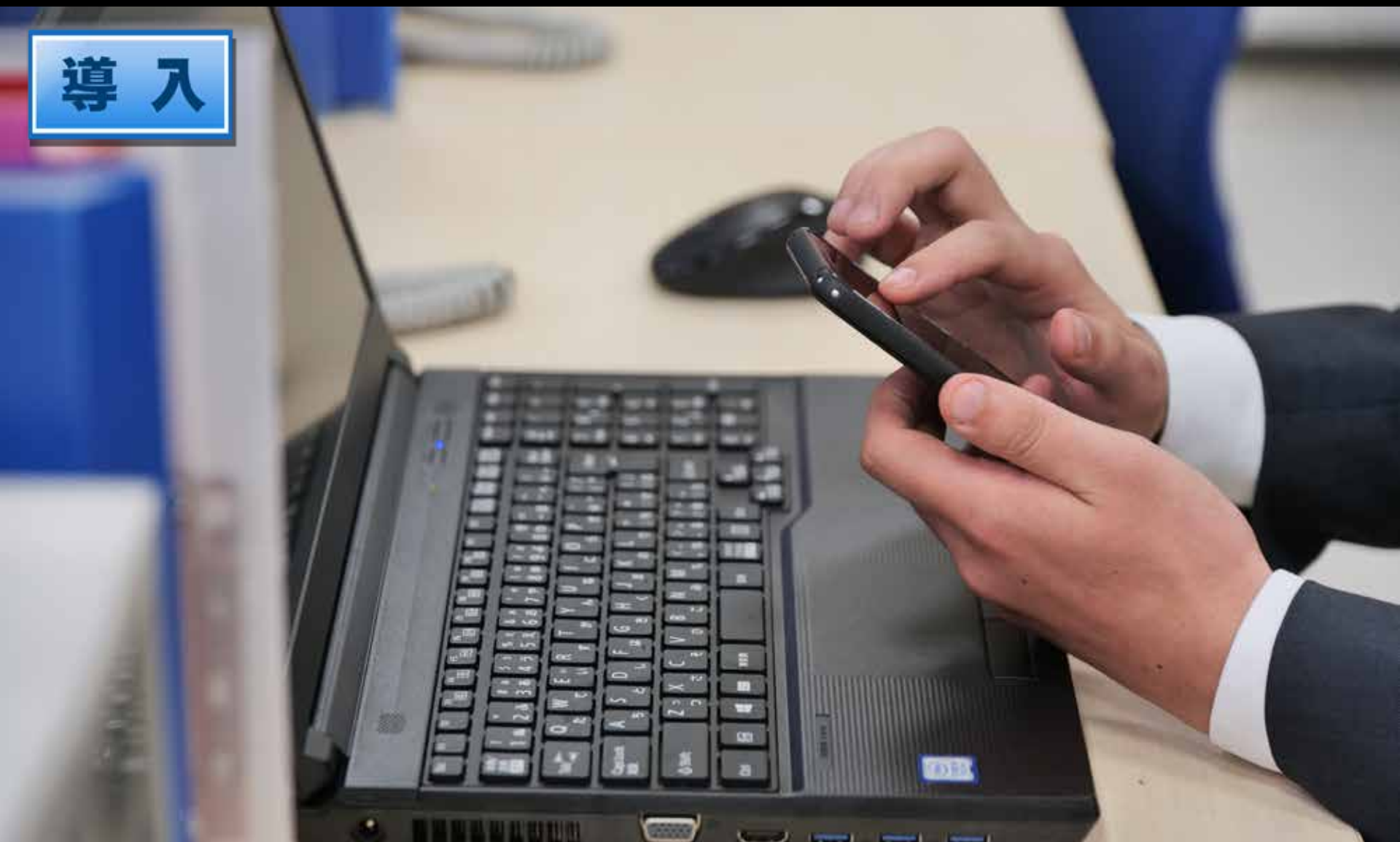
皆さんの職場では、個人のスマートフォンの使用を認めていますか？認めている場合、明確な利用ルールの下で管理されていますか？

導入



「個人のスマートフォンまで管理するのはちょっと気が引けるな・・・」という思いから、無制約で利用を許している経営者や管理者の方もいると思います。しかし、そうした状況下での利用は、会社にとって危険であると言えます。

導入



業務で利用しない場合でも、スマートフォンを職場に持ち込んだ場合のルール等は必要と言えます。そこで、個人のスマートフォンを職場で使わせる場合について、今一度考えてみてはいかがでしょうか。

事例

以上が今回この二人が起こした、
個人所有のスマートフォンによる情報漏洩の顛末になります。

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】
南雲直樹 【株式会社シックハック／社長】

事例

そうかわかった、よく報告してくれた。
二人は業務に戻ってくれ。

はい、すいませんでした。
失礼します。

広瀬洋子 【株式会社シックハック／総務部社員】
太田幸一 【株式会社シックハック／総務部社員】

事例

さて田端さん、
この後の対応は先ほど話した通りで進めてくれ。

はい、承知しました。




事例

ところで社長、今回の件で、
改めて個人のスマートフォンの職場利用について
考えなければいけませんね。

そうだな、使わせるにしろ使わせないにしろ、
明確な利用ルールは必要だな。

事例



でも田端さん、私は基本的に使わせるのに反対ではないが、
本当はどちらが良いのだろうか。

事例

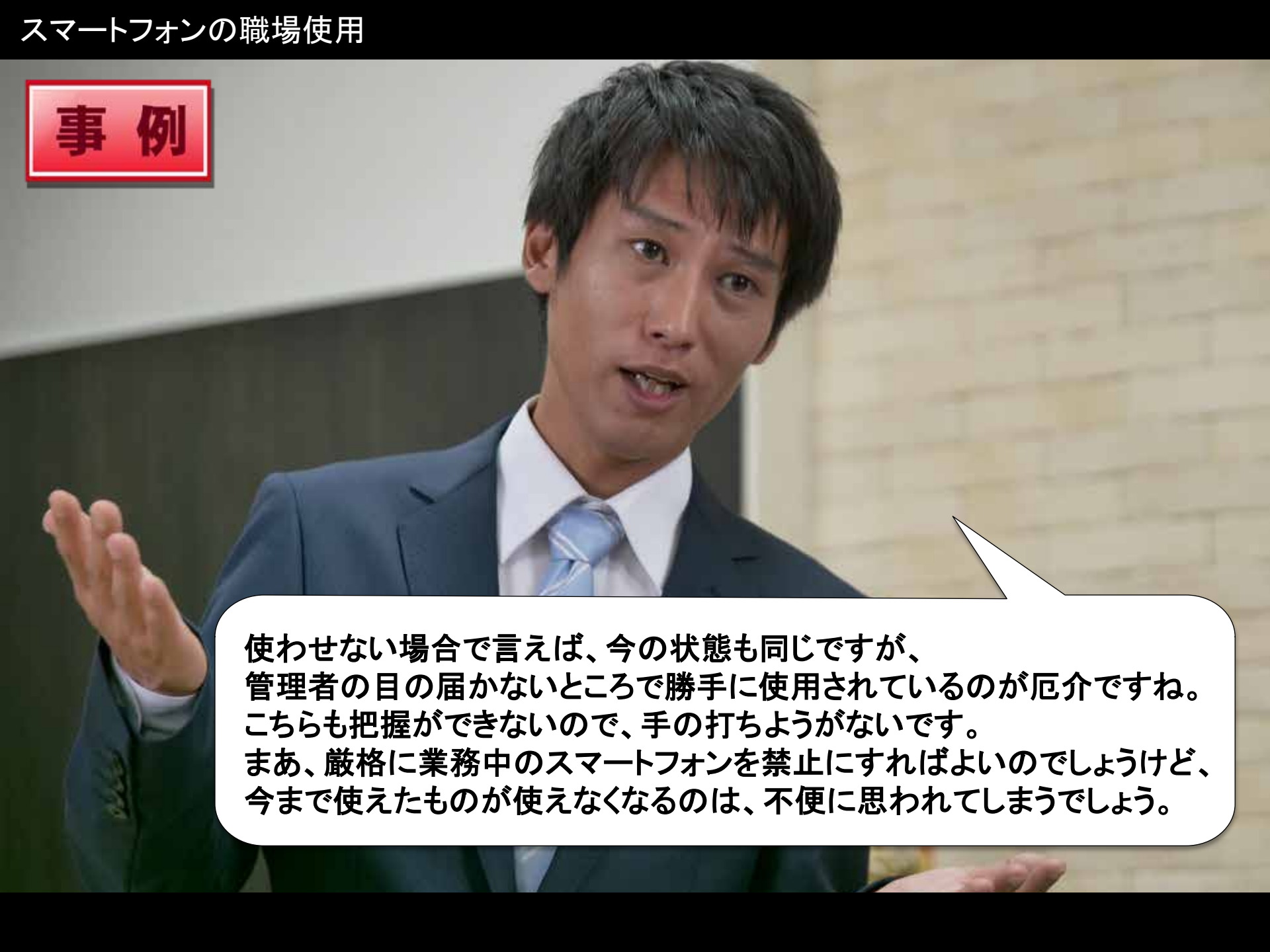
そうですね、使わせる場合の心配事は、
今回の件のように関係のない者にうっかり個人情報を送ってしまったり、
不正なアプリをインストールして情報が漏洩してしまうことですね。
ここが一番気になるところですね。

事例

情報漏洩か、そうすると盗難や紛失も該当するか・・・
でもこれは個人のものに限らないか。

はい、
でももちろんそういうことも考えていなければいけませんね。

事例



使わせない場合で言えば、今の状態も同じですが、
管理者の目の届かないところで勝手に使用されているのが厄介ですね。
こちらも把握ができないので、手の打ちようがないです。
まあ、厳格に業務中のスマートフォンを禁止にすればよいのかもしれませんが、
今まで使えたものが使えなくなるのは、不便に思われてしまうでしょう。

事例

だろうな、
業務の士気にも関わってくるかも知れないからな。



事例

そうですね、
私もできれば使いたい、使わせたいと思いますので、
もう少し考えてまた提案させていただきます。



事例

大変だが、よろしく頼むよ。



学習の意図



個人のスマートフォンでは、個人が勝手にスマホアプリのインストールが行えるため、気づかずに不正なアプリをインストールしてしまうと、知らない間にスマートフォン内の情報が漏洩(ろうえい)してしまうという危険があります。もし業務関係者の携帯番号やメールアドレスを登録していたら、その情報も漏洩してしまうことになります。

学習の意図



こうした危険が考えられるため、職場で使わせる場合は利用ルールが必要となります。なお利用ルールを作成する際は、今の使用状況や使わせる場合のメリットデメリットも考えてみましょう。

学習の意図

「スマートフォンの職場使用」について、以下を学習しましょう。

1. 個人のスマートフォンを職場で使わせる場合の利用ルールの作成

正しい対処法

個人のスマートフォンを職場で使わせる場合のメリットとして、企業支給の端末を購入する必要がない、業務の効率化、などが考えられます。従業員も自分の好きなスマートフォンを使って、いつでもどこでも作業が可能になることで、業務に対する意識の向上が見込まれることが考えられます。対してデメリットは、スマートフォンの紛失や盗難の被害、情報漏洩(ろうえい)、退職した従業員による情報持ち出し、などが考えられます。

正しい対処法

デメリット部分の対策を考えてみましょう。退職した従業員による情報持ち出しについては、利用ルールで管理が可能と言えます。問題は紛失や盗難、情報漏洩の対策ですが、モバイル端末管理ツール(Mobile Device Management、通称MDM)の利用が望ましいと言えます。

正しい対処法



モバイル端末管理ツールの主な機能として、紛失や盗難時に遠隔操作で、スマートフォン内のデータの削除や操作を一時的に制限する機能、危険と思われるスマホアプリの利用を制限する機能、などがあります。また、遠隔での情報収集が行えるため、スマートフォンが利用ルールに則り正しく利用されているか、の管理も可能です。

正しい対処法



また、“スマートフォンのアップデート”、“スマートフォンの改造行為をしない”、“セキュリティソフトを導入する”、など、スマートフォンの基本的なセキュリティ対策も、使わせる場合の重要事項になります。

正しい対処法



もちろん、職場での利用はさせない選択もありますが、その場合でも利用ルール（職場に持ってこない、職場内のパソコンには接続しない、など）は必要と言えます。しかし、利用させることで業務上のメリットが大きいと感じられる様でしたら、利用ルールを検討されてもよいのではないのでしょうか。

確認テスト 問題

No.4 スマートフォンの職場使用

～個人のスマートフォンを職場で使わせるメリットとデメリットとは～

Q1

個人のスマートフォンの職場利用について、もっとも適切でないものはどれか。

選択肢

- | | |
|--|--|
| | 1. データ転送も可能なUSBケーブルで直接パソコンと接続して充電。 |
| | 2. 業務中に撮った機密性のない写真を、会社のメーリングリストに送信。 |
| | 3. 顧客との打ち合わせで記述したホワイトボードの内容を、議事録の代わりに写真撮影。 |

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

個人のスマートフォンの職場利用について、もっとも適切でないものはどれか。

正解	選択肢
●	1. データ転送も可能なUSBケーブルで直接パソコンと接続して充電。
	2. 業務中に撮った機密性のない写真を、会社のメーリングリストに送信。
	3. 顧客との打ち合わせで記述したホワイトボードの内容を、議事録の代わりに写真撮影。

【解説】

データ転送も行なえるUSBケーブルを使用すると、スマートフォンがウイルスに感染していた場合、パソコンに接続することでパソコンにもウイルスが感染する可能性があります(その逆の可能性もあります)。充電する場合は充電専用のUSBケーブルを使用するか、コンセントから充電する様にしましょう。

※利用ルールによっては全て適切ではない場合があります。