UMEDA SOGO NEWS LETTER

2015.5.29　第13号　発行 梅田総合法律事務所

従業員の私有端末（スマートフォン等）の業務利用（BYOD）に関する法務

梅田総合法律事務所　弁護士　沢田篤志
弁護士　中村昭喜

▶ POINT

❶ 会社が従業員私有のスマートフォン、タブレット等の端末の業務利用を認める仕組みが広がっており、BYOD（Bring Your Own Device）と呼ばれています。

❷ BYOD の導入にあたっては、情報セキュリティ対策が重要です。営業秘密、個人情報等の安全管理についても十分考慮する必要があります。

❸ 従業員のプライバシー保護や、時間外労働に留意した適切な労務管理も必要です。

1　私有端末の業務利用（BYOD）

（1）モバイル端末の業務使用

今日、スマートフォン、タブレット等のモバイル端末（以下「端末」といいます）を業務で使用することが広く行われています。

業務に使用される端末については、①会社が端末を支給しているケース、②従業員の私有端末の業務使用を会社が認めているケース、③会社の許可を得ずに従業員が私有端末を業務使用しているケースがありえます。

（2）BYOD とは

本ニュースレターで取り上げるのは前記②のケース（一定の使用ルールの下、私有端末の業

務使用を会社が認めるケース）で、「BYOD」と呼ばれ、増加傾向にあります。

その背景には、プライベートでスマートフォン等を使いこなす人が増えるとともに、従業員の側には、使いたい端末を自由に選びたい、業務用とプライベート用の「2 台持ち」を避けたい等のニーズがあり、会社の側にも、生産性の向上、費用（端末購入費用や通信料）負担の軽減等のニーズがあるためだと思われます。

（3）無許可の端末の業務使用のリスク

ここで会社として注意しておくべきことは、従業員の側にスマートフォン等で業務を処理したいというニーズが存在するにもかかわらず、前記①（会社による端末の支給）や前記②（BYOD の導入）の対応をしておらず、また、何のルール作りもしなかった場合の影響です。この場合、従業員が自己判断で無許可のまま私有端末の業務使用をする前記③のケースが発生しやすくなり（いわば「隠れた BYOD」）、しかも、適切なセキュリティ対策がされていない状態になりがちです。

このような状態が生じているならば、会社として適切な情報セキュリティ対策ができているとはいえませんから、早急に改善策を検討する必要があります。

2　BYOD 導入と情報セキュリティ対策

（1）情報セキュリティ対策の重要性

近年、ベネッセにおける個人情報流出事件や外国企業への技術流出事件が大きく報道されています。

企業の情報管理に関しては、営業秘密保護に関する不正競争防止法、個人情報保護法等のほか、（従業員、取引先、委託先等との間の）契約に基づく秘密保持義務、民法に基づく損害賠償請求権等が、検討すべき法的なルールとして存在しています。

企業は、自社の有用な情報の社外流出を防止するためにも、また、情報漏洩によって顧客や取引先に被害を与えないためにも、適切な水準の情報管理が必要です。情報管理に不備があると、万一、個人情報や営業秘密の流出等の不祥事が発生した場合、企業にとって経営上の大きなリスクが生じます。

企業にとって、適切な情報管理は、コンプライアンス上の重要課題です。

（2）モバイル端末と情報セキュリティ

統計的に見ると、企業の情報漏洩の事故原因で最も多いのは「紛失・盗難」であり、「第三者による不正アクセス」がそれに続きます。

モバイル端末は、性質上、紛失のリスクが高いため、特に重点的に情報セキュリティ対策の対象にすべきです。

BYOD を導入する場合には、端末上に情報が残ることによるリスク、業務上の情報と従業員のプライベートな情報とが同一端末に混在すること、会社が全従業員に同じ端末を支給する場合とは異なり企業内の IT 部門の管理業務の負担が増加すること等の課題にどう対処するか検討する必要があります。

（3）情報の秘密管理のポイント

情報セキュリティ対策には、組織的管理、人的管理、物理的管理、技術的管理という多面的な対策が必要とされています。

① 組織的管理

担当部署の決定、責任の所在の明確化、安全管理措置の評価・改善の仕組み作り等、継続的な改善の取り組みを可能にする社内体制づくりが必要です。

② 人的管理

従業員教育や、就業規則・営業秘密管理規程・秘密保持契約書等の整備が必要です。

さらに、具体的な運用として、BYOD 対象者への丁寧な教育、BYOD に関する規程・申請書・誓約書等の作成が特に重要です。業務の効率性を保ちつつ情報セキュリティ対策を機能させるため、制度・運用を常にアップデートしていくことが求められます。

③ 物理的管理・技術的管理

ID・パスワードによる情報のアクセス制限、情報の種類や重要性に応じた段階的なアクセス制限、端末紛失時に備えた遠隔ロックやデータの遠隔消去の準備、不正アプリ対策等が必要です。

情報セキュリティ対策の物理的管理・技術的管理のための専用の製品・サービス（仮想デスクトップ、モバイルデバイス管理、モバイルコンテンツ管理等）が多数提供されていますので、最新情報の収集が重要です。

（4）営業秘密（不正競争防止法）との関係

不正競争防止法は「営業秘密」を保護していますが、「営業秘密」として認められるためには、①秘密管理性、②有用性、③非公知性の 3 要件を満たす必要があります。その中でも、①秘密管理性の要件該当性が、しばしば問題になります。

そこで、企業としては、自社の「営業秘密」保護のために、スマートフォン等の端末の業務使用のルールを整備するにあたっても、営業秘密保護の要件に関する法的問題[1]も念頭におくことが望ましいと思われます。具体的には、例えば、ID・パスワードによる管理や秘密情報である旨の表示の徹底等が必要になると思われます。

---

[1] 2015 年1月に全面改訂された経済産業省の「営業秘密管理指針」では、秘密管理性の要件に関し、企業の当該情報についての秘密管理の意思が「秘密管理措置」によって従業員に明確に示され従業員の認識可能性が確保されることが必要であること、営業秘密と一般情報とが「合理的に区分」されていることが必要であること等が解説されています。ただし、秘密管理性の要件の判断基準が今後どうなるかについては、裁判例の集積を待つ必要があります。

3　従業員の権利保護

BYOD 導入においては、従業員個人のプライバシー保護についての考慮が必要です。

特に、紛失等の緊急事態において、端末内に保存されている従業員の私的なデータも含めて全部消去せざるをえない場合が生じることに留意が必要です。BYOD を希望する従業員から、予めその承諾を得ておくことが必要でしょう。

4　適切な労務管理

私有端末で業務を行うようになると、従業員が業務時間外に仕事をすることが増加ないし常態化するおそれがあります。また、労働時間の正確な把握が難しくなることがありえます。

言うまでもなく、時間外の労働時間については、残業代が発生します。一般的に、従業員が使用者の「指揮命令下」にあると評価される状態にあれば、労働時間であると認定されます。企業としては、従業員やその上司に対して、業務時間外に端末を使用した場合、どのような場合は時間外労働にあたることになるのか、適切な教育を行い、適切な労務管理を行うことが必要です。

5　会社のサポート

企業は、BYOD を導入するにあたっては、従業員に対する費用面及び技術面のサポートについて検討する必要があります。

なお、仮に労働者に費用の負担をさせる定めをする場合、就業規則への規定を要すること（労働基準法 89 条 5 号）に注意を要します。

6　まとめ

以上のように、スマートフォン等の端末の業務使用に関しては、法的側面からの各種検討が必要です。具体的な制度作り（営業秘密管理規程・秘密保持契約書・BYOD に関する規程・申請書・誓約書の作成）等については、当事務所にご相談ください。

COLUMN

先日、スペインのバルセロナを訪れる機会がありました。大阪弁護士会国際委員会のメンバーとして、バルセロナ弁護士会の主催するシンポジウム等に参加するためです。シンポジウムでは、実に40を超える国・地域から弁護士が集まり、白熱した議論と活発な情報交換が行われました。

また、バルセロナ弁護士会の公式行事の後、夜は盛大なカクテルパーティーが開催されるのですが、そのパーティーが夜9時半ごろから始まって深夜まで延々と続くなど、スペイン人のパワフルさにも驚かされました(もっとも、睡眠不足はシエスタと呼ばれる昼寝で補っているのかもしれません)。

ヨーロッパは近年、不況のイメージが強かったかもしれませんが、力を取り戻しつつあり、元々非常に魅力のある地域でもありますので、グローバル化の進む今日、日本企業にとってもますます重要な投資先・取引先となっていくのではないか、そのように改めて感じたバルセロナ訪問でした。　（弁護士　西口健太）

梅田総合法律事務所

〒530-0004 大阪市北区堂島浜1丁目1番5号　大阪三菱ビル6階
TEL：06-6348-5566(代)　FAX：06-6348-5516
http://www.umedasogo-law.jp