Dr.WEB®
sinse 1992


# 従業員が私物のモバイル端末/コンピュータを業務で利用するについてのガイドライン(BYOD)


## #1

お勤め先の企業で私物のデバイスを業務で利用するにあたる規定されているルールを学び、遵守してください。


## #2

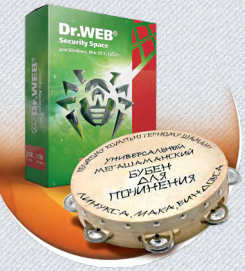
可能であれば、OSの機能を利用して端末上には個人用及び業務用と二つのアカウントを作成してください。その際には、Guestアカウント名、及びプログラムのオートラン機能を無効にする必要があります。

## #3

アカウントにログオンするために、出来るだけ複雑なパスワードを設定してください。

## #4

Playストアなど公式な管理アプリやリソースを使って、インストールされている全てのアプリのアップデート、最新版のインストールを適宜行ってください。ソフトウェアは正式にライセンスされたもののみでなければなりません。企業内セキュリティシステムが採用される場合、インストールされているアプリのアップデートは集中管理されます




## #5

お持ちのPC/ノート型パソコンまたはスマートフォンを保護するアンチウイルスの選択については、お勤め先企業のシステム管理者の決定に準ずる必要があります

## #6

利用するアンチウイルスは、集中管理ができるように、企業セキュリティシステムへの組み入れが可能なものでなければなりません。

## #7

現在のウイルス対策はアンチウイルスだけでは不十分であるため、包括的保護を活用することが必要不可欠になります。


犯罪者がスマートフォンやSIMカード対応タブレット型PC上にある情報を盗み取れないように、アンチシフトを使って遠隔からデバイスをロックし、デバイス上のデータを削除することができます。

これらの保護コンポーネントは、絶対に無効にしないでください！なお、セキュリティを集中管理している場合、コンポーネントの無効化はできません。

## #8

以下のケースでは特殊なツールを使って企業情報を完全に削除する必要があります。

- 端末のファームウェアを書き換える場合、或いは修理のために端末を社外スタッフ（サービスセンター）に出す場合
- 退社する場合
- 端末の持ち主が変わる場合

情報削除については、必ずお勤め先企業のシステム管理者に問い合わせることを推奨します。また、情報削除が実行されたことについての記録を取ることが望ましいです。万が一、退社後にデータ漏洩が発生した場合にクレームの対象になりません

## #9

端末のシリアル番号（IMEI番号）のメモを取り、安全な場所に保管してください。端末が紛失されたら、必要になります。

# 注意事項

- ファームウェアがメーカー製のものから改造ファームウェアに書き換えられた端末、または第三者に作成されたOS版を搭載している端末の利用は控えてください。
- 製造元が不明であったり、非常に安価なスマートフォンやタブレット型PCは安全性と品質の面で疑問があるため、利用は控えてください。
- Google Play及びプログラム開発会社の公式なwebサイト以外のリソースからAndroid対応アプリのダウンロード/インストールはしないでください。
- 他人にご利用中の端末の利用は許可しないでください。
- 業務用アカウントを使って個人目的でインターネットにアクセスしないでください。
- アンチウイルスの自動更新を無効にしてはいけません。
- 企業内セキュリティシステムが採用されている場合、更新又は定期スキャンの無効化について、システム管理者にお問い合わせはしないでください。
- オンラインバンキングにて支払う目的で端末を使用する場合、この端末は絶対に他の目的で使用しないでください。



株式会社Doctor Web Pacific〒210-0005
神奈川県川崎市川崎区東田町1-2NKF川崎ビル 2F
TEL 044-201-7711
FAX 044-201-7712

www.drweb.co.jp | www.drweb-curenet.com | www.av-desk.com
http://freedrweb.com | http://mobi.drweb.com