

Optimal Biz ホワイトペーパー

Optimal Biz:スマートフォンなどの USB 接続機能 経路による情報漏えい対策

本ホワイトペーパーに記載された内容は情報の提供のみを目的としており、お客様ご自身の責任において情報の利用を行うものとし、明示、黙示または法律の規定にかかわらず記載情報について株式会社オプティムはいかなる責任を負わないものとします。

2014 年 10 月 29 日発行

目次

Optimal Biz:USB の情報漏えい対策	3
Windows の USB 機器の接続、利用の仕組み	3
Optimal Biz の USB 使用制限の機能拡張	4
各設定選択項目の説明	5
USB 使用制限の機能の注意点	6

Optimal Biz : USB の情報漏えい対策

近年、携帯情報機器の進化によりスマートフォンや大容量のデジタルメディアプレーヤーなどが登場し多くの方が日常的にそれらの機器を利用しています。企業においても従業員が個人所有の情報機器を所持したまま職場に来て仕事に従事している状況が特殊なことではなくなっています。従来の企業の情報漏えい対策では USB メモリーによる業務データや顧客リストのコピーに主眼が置かれていましたが、現在では前述の携帯情報機器などを業務 PC へ接続することで USB メモリーと同様に大量のデータのコピーが可能となることへの対応が必要となっています。

Optimal Biz ではかねてより Windows 端末の使用制限機能として管理端末の USB 利用の禁止機能を提供してきました。従来の禁止対象として、USB メモリー、ポータブル HDD などを対象とした USB(ストレージ)の禁止、また USB 接続全体の禁止、またそれらの選択と組み合わせで禁止から除外する USB 機器を個別指定するホワイトリスト機能の設定の機能が提供されていました。

前述した携帯情報機器の利用禁止には USB 接続全体の禁止機能の設定が必要でしたが、Optimal Biz 7.1 では従来までの禁止設定項目に新たにスマートフォンやデジタルメディアプレーヤー、デジタルカメラを対象とした Windows ポータブル デバイス(WPD)の接続禁止の項目を追加しました。

本ホワイトペーパーでは新たに加えられた Windows ポータブルデバイスの禁止設定の詳細および Windows 端末向けの USB 禁止機能の効果的ご利用方法について記します。Optimal Biz における端末管理の情報漏えい対策設定の参考資料としてご活用ください。

Windows の USB 機器の接続、利用の仕組み

Windows では PC に備わっている USB ポートに外部機器が接続されると、機器に対応したドライバと呼ばれる情報機器操作の基盤となるソフトウェアがインストールされます。ドライバは一般的に接続する機器の機能ごとに種別分けがされており、その種別は「デバイスクラス」または「デバイスセットアップクラス」と呼ばれて管理されています。

USB メモリーや USB 接続のポータブル HDD などは一般的に「USB ストレージ」クラスのドライバを使用して接続されます。また、スマートフォンやデジタルメディアプレーヤー、デジタルカメラは主に「Windows ポータブルデバイス」クラスのドライバが使用されます。

※ Windows ポータブル デバイスが OS 標準でサポートされるのは Windows Vista 以降です。Windows XP の場合、同じ USB 情報機器を接続しても Vista 以降の OS と異なるクラスのドライバで接続、認識されます。

Optimal Biz の USB 使用制限の機能拡張

Optimal Biz では USB ストレージの使用禁止を従来から提供している「禁止(ストレージのみ)」を選択することで使用制限が行えます。また、Windows ポータブル デバイスについては USB 利用全体を禁止する「禁止」を選択して使用を許可する機器を個別にリスト指定設定を行う必要がありました。そのため、Optimal Biz 7.1 では Windows ポータブルデバイスとして接続される情報機器を簡単に接続制限できるように新たに「禁止(ストレージおよびポータブルデバイス)」選択項目を追加しています。



各設定選択項目の説明

The screenshot shows a settings window titled '設定 - 編集' (Settings - Edit). At the top, there is a '設定名' (Setting Name) input field. Below it, the 'USBデバイス' (USB Device) section is active, with three radio button options: '許可' (Allow), '禁止(ストレージのみ)' (Prohibit (Storage only)), and '禁止(ストレージおよびポータブルデバイス)' (Prohibit (Storage and Portable Devices)). The '許可' option is selected. Below these options are two tables for specifying allowed devices. The first table is titled '許可USBデバイス(ハードウェアID)' (Allowed USB Devices (Hardware ID)) and has a header 'ハードウェアID' (Hardware ID) and a note '(+ボタンで追加: 300件まで)' (+ button to add: up to 300 items). The second table is titled '許可USBデバイス(インスタンスパスまたはシリアルID)' (Allowed USB Devices (Instance Path or Serial ID)) and has a header 'インスタンスパスまたはシリアルID' (Instance Path or Serial ID) and the same note. At the bottom left, there is a '保存' (Save) button with a checkmark icon.

● USB デバイスの利用制限の選択項目

➤ 許可

USB デバイスに対する使用制限(接続制限)は行われません。

➤ 禁止(ストレージのみ)

USB メモリーやポータブル HDD など、USB ストレージとして Windows に認識される機器の利用を禁止します。

➤ 禁止(ストレージおよびポータブルデバイス)

上記、USB ストレージに加え、スマートフォンやデジタルメディアプレーヤー、デジタルカメラなど Windows で Windows ポータブルデバイスとして認識される機器の利用を禁止します。

➤ 禁止

上記、USB ストレージおよび Windows ポータブルデバイスを含んですべての USB 接続機器の利用を禁止します。

● 利用制限から除外する機器の指定

機器の「ハードウェア ID」、「インスタンスパス」または「シリアル ID」を指定することで利用可能にします。(各 300 件まで指定可能)

➤ 許可 USB デバイス(ハードウェア ID)

➤ 許可 USB デバイス(インスタンスパスまたはシリアル ID)

※ 接続を許可する機器の「ハードウェア ID」、「インスタンスパス」または「シリアル ID」を確認するには、実際に対象となる機器を管理対象の Windows 機器に接続し、Windows のコントロールパネルからデバイスマネージャーを起動して確認します。デバイスマネージャーでは Windows で管理されているデバイス一覧が表示されるので目的の機器を探して選択、右クリックしてプロパティを表示、プロパティの詳細タブを開きプロパティの選択肢から「ハードウェア ID」、「インスタンスパス」(※対象の Windows OS バージョンによりプロパティ名が「デバイスインスタンスパス」または「デバイスインスタンス ID」と表記されています。)または「シリアル ID」を選択することにより値の欄にその機器の値が表示されます。複数の値が表示される場合がありますが、そのうちの一つを許可する USB デバイスのリストに追加します。

USB 使用制限の機能の注意点

- Windows のバージョンなどにより同じ情報機器でも接続に使用されるドライバが異なる場合があります。またその外部機器が別のクラスとして認識される場合があります。

例: デジタルカメラを USB 接続した場合、Windows Vista 以降では Windows ポータブルデバイスとして認識されるが、Windows XP の場合イメージングデバイスとして認識される。その場合、USB ストレージおよびポータブルデバイスの禁止では使用制限が行えません。(Windows ポータブルデバイスは Vista 以降でサポートされます。)

- iPhone、iPad などの iOS 端末を USB 接続し、iTunes ソフトウェアをインストールした場合、ポータブルデバイスとしてだけでなく、独自のドライバで接続され iTunes ソフトウェアの利用が禁止されません。また、一部のアプリケーションでも iTunes ソフトウェアが提供しているドライバを利用してファイルの転送などの機能を行えるものがあり、ポータブルデバイスの禁止ではこれらの使用に制限を行えません。管理対象にこれらのケースが含まれる場合、iTunes ソフトウェアおよびそれらのファイル転送ソフトをアプリケーション起動禁止機能で指定するか、USB 使用制限においてすべての USB 禁止機能の設定を検討してください。
- USB 使用制限で「禁止」を指定することによりすべての USB 接続機器の利用が禁止されます。一部の Windows タブレット端末やノート、デスクトップ型 PC などではネットワークや操作パネル機能、ハードディスクなどを USB 接続で提供している場合があります。その場合、すべての USB 接続機器の設定を行うとこれらの機能が停止し、以後の機器の使用が一切行えなくなる場合があります。(機能の利用禁止により再設定の同期も行えません。)すべての USB 機器の使用制限の設定を行う場合は、管理対象の機器のデバイス構成を確認し、端末の基本機能およびネットワーク機能が禁止されないように除外(許可)設定をしたうえでご利用ください。

OPTiM[®] オプティムについて

オプティムは、ネットを空気のように快適で、息をするように無意識に使えるサービス・インフラを提供する会社です。急速なインターネット普及に伴い、これまでネットを利用したことのないユーザーがネットを利用する機会が増えており、このユーザー層にとって現状のネットは必ずしも使いやすいものではありません。オプティムのオプティマル事業では、誰もがネットを意識せずに利用できる環境の実現を目指しています。オプティムおよびオプティマル事業の詳細については <http://www.optim.co.jp> をご覧ください。

©2014 OPTiM Corporation All rights reserved.

本ホワイトペーパーで記載される会社名・商品名などは、オプティムまたは各社の商標および登録商標です。また、記載されているシステム名、製品などには、必ずしも商標表示（®、™）を付記していません。

OPOB00001J