



# USBポートからのデータ漏洩の防止

Pointsec Protectorによるプラグアンドプレイ周辺機器のアクセス  
およびデータの制御

# Contents

本書の内容

概要	3
データ漏洩の新たな経路になったUSBポート	4
USBによって増大するエンドポイントでのデータ漏洩リスク	5
データを簡単に移動できるUSBストレージ	5
ポッド・スラーピングを始めとするテクニック	6
Pointsec Protector: USBポートを保護するためのシンプルなソリューション	6
企業全体のポート制御	6
デバイス管理、コンテンツ・フィルタリング、暗号化(オプション)	7
集中管理	7
詳細について	8

## 概要

デジタル形式で保管されている情報の電子的な流れを統制することは、これまでにない困難になっています。ほとんどの組織では、ファイアウォール、侵入防御、認証、アクセス制御などによって、サーバやネットワークからデータが漏洩するリスクを軽減しようとしてきました。また、モバイル化の進展によってリモートおよびモバイル利用のノートPCが広く普及した結果、暗号化ソリューションでデータを保護してデバイスの紛失や盗難に備える企業も急増しています。しかし、最近になって、これらの対策では軽減できない新たなリスクが浮上してきました。保護対象のネットワークの外にデータが持ち出されても検知できない、というリスクです。そしてその元凶となっているのが、デスクトップPCやノートPCのUSBポートに接続できるすべてのプラグアンドプレイのストレージ・デバイスです。

USBポートには、USBメモリーやリムーバブル・ハードディスクなどのストレージ・デバイスを始め、さまざまな周辺装置を接続できます。デジタル・ミュージック・プレイヤーには、大量のMP3ファイルに加え、Docファイル、PDF、スプレッドシート、データベース、写真、映像など、さまざまな形式のファイルを格納できます。USBフラッシュ・メモリは、格納したマルチメディアを再生する機能はないものの、さまざまな種類のファイルを格納できる点はミュージック・プレイヤーと同じです。デジタル・カメラ、携帯電話、外付けハード・ディスク、PDAなどのモバイル・デバイスも同様です。

ほとんどのオペレーティング・システムでは、USB接続のストレージ・デバイスをエンドポイントのPCに接続すると、即座にデバイスが認識されて自動で使用できるようにされますが、これが一番の泣き所であり、すべてのエンドポイントでのデータ漏洩を可能にしている最大の要因です。また、これとは反対方向の危険性もあります。ウイルスに感染したファイルや悪意のあるアプリケーションが、新たに接続されたストレージ・デバイスからエンドポイントのPCにコピーされ感染し、企業ネットワーク全体に広がることも考えられるからです。

データが漏洩すれば、企業の信用は著しく低下し、往々にして消費者の不買運動、規制当局による厳しい調査、金融マーケットからの制裁などにつながります。HIPAA (Health Insurance Portability and Accountability Act)、GLBA (Gramm-Leach-Bliley Act)、Basel IIなどの法律が適用されれば、組織においてデータ漏洩が発生しかねない状況を放置した責任者個人が、民事訴訟や刑事訴訟で有罪判決を受けるおそれもあります。

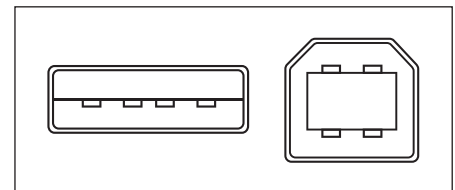
企業全体にわたってモバイル・デバイスの物理ポートを保護するチェック・ポイントの戦略を「データ漏洩保護」といいます。この戦略では、企業のデータ・セキュリティに影響するさまざまなリスクに対処します。この技術白書では、USBポートだけでなく、Bluetooth、FireWire、WiFi、シリアル・ポート、およびパラレル・ポートなど、あらゆるプラグアンドプレイ・ポートに接続されたストレージ・デバイスによるデータ漏洩を、いかに簡単に防止できるかについて説明します。また、リスク要因について分析し、Pointsec Protectorソリューションを使用することで、PCに接続されたストレージ・デバイスのアクセスおよびデータをいかに簡単に統制できるかについても説明します。

## データ漏洩の新たな経路になったUSBポート

すべての組織は、企業データや個人データをいかに厳重に保護できるかという大きなプレッシャーにさらされています。データ漏洩事件に関するニュースは絶えることがありません。Privacy Rights Clearinghouseによると、2005年のChoicePointの大規模なデータ漏洩以降、紛失または盗難によって漏洩した個人情報データは1億件以上にのぼります<sup>(1)</sup>。データ漏洩やサイバー・セキュリティ関連の問題を企業が隠蔽している可能性を加味すれば、実際の数字はもっと大きくなります。

データ漏洩に対しては、世間からの厳しい監視、信用の低下、金融マーケットおよび司法による制裁などがあり、企業がセキュリティを継続的に強化することへの動機付けとなっています。CSI (Computer Security Institute) がFBI (Federal Bureau of Investigation : 連邦捜査局) のコンピュータ侵入対応部隊 (Computer Intrusion Squad) との協力のもと最近実施した調査では、「最も重要な問題」としてデータ保護、法令遵守、データ漏洩、ウイルスやワーム、およびアクセス制御が挙げられています<sup>(2)</sup>。企業がこれらの問題に対処するためには、ネットワーク化された情報システムのレイヤごとに、特定の脆弱性を解決するソリューションを個別に導入する必要があります。セキュリティ技術として最も一般的なのは、境界とデスクトップのファイアウォール、アンチウイルス/アンチスパイウェア・ソフトウェア、VPN、侵入検出/防止 (IDS/IPS)、暗号化、ネットワーク・アクセス制御 (NAC)、認証などです。

しかし企業は、これまでのようなレイヤ化されたセキュリティ技術では検知できない、データ漏洩の新たな経路が存在することに気づき始めています。それが、一見無害なエンドポイント・デバイス上のUSBポートなのです。



USB (タイプAおよびB) コネクタ

USB (Universal Serial Bus) は、Microsoft Windows、Macintosh OS X、Linuxなど、一般的なオペレーティング・システムでネイティブにサポートされるインタフェース標準です。USB標準は、PCと周辺デバイスを簡単に相互接続できるようにするためのものです。USBの最大の特長は、USBポートに接続されたあらゆるデバイスを、ユーザの介入 (マウスやキーボードによる操作) なしで自動的に認識できる点です。USBは、キーボード、プリンタ、テレビ、コンポ、ゲーム機のコントローラ、ストレージ関連デバイスなど、さまざまな機器で使用されています。しかし、残念なことに、相互接続を容易にするための技術が、セキュリティ管理者の注意を必要とする重要なポイントにもなってしまったのです。



USBシリーズAプラグ

USBには、データ・セキュリティ上の弱点になっているという側面もあります。従業員は仕事用のPCに個人所有のストレージ・デバイスをひっきりなしに接続し、音楽や壁紙用の画像をアップロードしたり、インターネット経由でデジタル写真を転送したりしています。彼らに悪意はないかもしれませんが、しかし、企業データをUSBポート経由でエンドポイントからポータブル・デバイスに転送できるという事実が、検知できないデータ漏洩や悪意あるファイルの混入という重大なリスクを企業に負わせているのです。

USBには、データ・セキュリティ上の弱点になっているという側面もあります。従業員は仕事用のPCに個人所有のストレージ・デバイスをひっきりなしに接続し、音楽や壁紙用の画像をアップロードしたり、インターネット経由でデジタル写真を転送したりしています。彼らに悪意はないかもしれませんが、しかし、企業データをUSBポート経由でエンドポイントからポータブル・デバイスに転送できるという事実が、検知できないデータ漏洩や悪意あるファイルの混入という重大なリスクを企業に負わせているのです。

(1) 過去に発生したデータ漏洩の記録については、[www.privacyrights.org/ar/ChronDataBreaches.htm](http://www.privacyrights.org/ar/ChronDataBreaches.htm)を参照。

(2) 「2006 CSI/FBI Computer Crime and Security Survey」  
([http://i.cmpnet.com/gocsi/db\\_area/pdfs/fbi/FBI2006.pdf](http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf)) の24ページの表2を参照。

## USBによって増大するエンドポイントでのデータ漏洩リスク

企業向けの一般的なデスクトップPCには、最大で8個ほどのUSBポートが付いています。キーボード、セキュリティトークン・リーダなど、さまざまな周辺機器の接続に使用しますが、使用されていないポートが少なくとも1つはあるのが一般的です。USBポートは、接続されたUSB対応デバイスをいつでも認識できるよう、デフォルトで「常にアクティブ」になっています。

Windowsのグループ・ポリシーやADMテンプレートを使用して、USBを無効にすることも可能です。しかし、残念ながらこの機能はきめ細かな制御には適していません。USBポートを個別に制御できないため、エンドポイント・コンピュータのすべてのUSBポートを有効にするか無効にするかしか選択できないのです。ほとんどのエンドポイントで、不可欠な周辺機器がUSBで接続されている点を考えると、この制御機能はほとんど役に立ちません。

別の方法として、使用されていないポートの使用を物理的に制限することも可能です。IT業界には「使用されていないUSBポートを接着剤で埋めた」という逸話もありますが、高価なオフィス機器にこのような永久的な損傷を与える方法はお勧めできません。使用されていないUSBポートを物理的に保護する差し込み式のUSBロックも販売されていますが、本当に悪意のあるユーザであれば、単純に他のUSBデバイスを外したうえで認可されていないストレージ・デバイスを接続するでしょう。その意味では、物理的にブロックする戦術が効果的とは言えません。

## データを簡単に移動できるUSBストレージ

このタイプのデバイスの代表格が、NANDタイプのフラッシュ・メモリにデジタル・ファイルを格納するUSBフラッシュ・ドライブです(下の写真を参照)。フラッシュ・ドライブは、「USBキー」、「ペン・ドライブ」、「サム・ドライブ」、「チップ・スティック」などとも呼ばれます。フラッシュ・ドライブをエンドポイントのUSBポートに差し込むと、エンドポイント・コンピュータのOSが自動的にデバイスを認識してデバイス・ドライバをロードするため、Windowsエクスプローラなどのアプリケーションを使ったファイル転送が可能になります。エンドポイント・コンピュータの設定によっては、フラッシュ・ドライブに格納されているプログラムを実行することも可能です。

フラッシュ・ドライブの現時点でのストレージ容量は最大で16GBもあります。接続は、USBマスストレージ・デバイス・クラスという一連の標準に基づいて実装されています。USBは本来、エンドポイントの内部ストレージ(SCSIなど)のプライマリ・バスとして機能することを意図して設計されたものではありませんが、アプリケーションからの要求がそれほど厳しくない状況であればプライマリ・バスとして十分に機能します。USB標準では、以下の3つのデータ転送速度がサポートされます。

- LS (Low Speed) - 1.5Mbit/秒 (187.5KB/秒)。  
ヒューマン・インタフェース・デバイス  
(マウス、キーボード)に使用します。
- FS (Full Speed) - 12Mbit/秒 (1.5MB/秒)。
- HS (High Speed) - 480Mbit/秒 (60MB/秒)。



USBフラッシュ・ドライブ

USBフラッシュ・ドライブは、エンドポイント・コンピュータ上では他の内部ドライブとまったく同じように表示されます。プラグアンドプレイ機能とその小さなサイズを考え合わせれば、企業から機密情報を盗み出すうえで理想的なデバイスといえます。人目に付かず素早くデータを盗み出すことのできるUSBデバイスはフラッシュ・ドライブだけではありません。既に説明したさまざまなUSBストレージ・デバイスも、すべて同じ用途に使用できます。

### ポッド・スラーピングを始めとするテクニック

USBストレージでデータを盗み出すのに、長いスクリプトを記述する必要はありません。USBストレージ・デバイスをUSBポートに接続し、Windowsエクスプローラで目的のファイルをストレージ・デバイスにドラッグするだけです。この操作は、悪意ある内部関係者だけでなく、善意の内部関係者（つまり、データ漏洩防止のためのセキュリティ方針を知らず、仕事のためにデータを持ち出そうとする人）によって実行される可能性もあります。

最も普及しているUSBストレージ・デバイスは、アップル・コンピュータのiPodです。ファイルをUSBストレージ・デバイスに転送することを表す言葉として「ポッド・スラーピング (pod slurping)」という造語が生まれたほどです。

似たような言葉に「カムスナッフing (camsnuffing)」があります。これは、デジタル・カメラで文書などを撮影し、認可されていない受信者に転送する行為を表します。同様に「ブルースナーフing (bluesnarfing)」は、Bluetooth接続を利用して無線デバイスからデータを盗み出すことを意味します。

どのような言葉で表すにせよ、エンドポイントからUSBストレージ・デバイスにデジタル・ファイルを転送するのは非常に簡単だということです。これらのデータ転送は、通常のセキュリティ制御では検出できません。そのうえ、小さなストレージ・デバイスにいったん転送されたデータは、権限のない人物が悪用を目的として簡単に企業の外に持ち出すことができます。

## Pointsec Protector: USBポートを保護するためのシンプルなソリューション

チェック・ポイント・ソフトウェア・テクノロジーズが提供するPointsec® Protector™製品は、USBなどの入出力ポートに接続されたストレージ・デバイスからのアクセスと、それらの接続を介して転送されるデータの流れを、企業全体にわたって制御するためのシンプルなソフトウェアベース・ソリューションです。ポリシー方式のポート・セキュリティ・システムにより、エンドポイントでのUSBアクセスをきめ細かく制御できます。例えば、すべてのアクセスを拒否（ブラックリスト機能）したり、読み取り専用のアクセスのみを許可したり、フル・アクセスを認可（ホワイトリスト機能）したりできます。セキュリティとコストのバランスに直接影響する制御レベルは、セキュリティ管理者が構成できます。状況によっては、厳格なセキュリティ・ポリシーを実装した結果、エンドユーザが業務パターンを変えなければならない場合もあるかもしれません。しかし、チェック・ポイントが目標としているのは、エンドユーザの業務パターンの変更を最小限に抑えつつ、セキュリティ・ポリシーにおいて最も重要な問題を解決できるよう、カスタマイズされたポート管理ソリューションを提供することです。

Pointsec Protectorはクライアント/サーバ・ソリューションです。したがって、管理ソフトウェアはサーバに導入し、各エンドポイントにはメモリー使用量の少ないクライアント・ソフトウェアのみをインストールします。ホワイトリストおよびブラックリスト機能は、カーネル・モード・フィルタ・ドライバを使用してクライアント側で有効にします。Pointsec Protectorのリムーバブル・メディア・マネージャを使用すると、ネットワーク上の各デバイスをデジタル・シグネチャに基づいて一意に特定できます。クライアント・ソフトウェアは、既存のMSI (Microsoft Windows Installer) またはコマンドライン対応のソフトウェア配布パッケージを使用して、ユーザ操作なしで導入できます。Pointsec Protectorには、製品を配布および管理するための導入サーバも用意されています。また、Pointsec Protectorは、既存のネットワーク・インフラストラクチャに透過的に統合できます。

### 企業全体のポート制御

Pointsec Protectorは、USB、FireWire、IDE、Bluetoothなど、あらゆるポート上のリムーバブル・メディアおよび入出力デバイスを、ホワイトリストとブラックリストの両方で制御できる唯一のソリューションです。システム管理者は、既知および未知のすべてのデバイスへのアクセスを一元的に管理できます。

ホワイトリスト機能を使用すると、リストに指定されたデバイスを除くすべてのデバイスへのアクセスを拒否できます。ブラックリスト機能を使用すると、リストに指定されたデバイスを除くすべてのデバイスへのアクセスを許可できます。デバイス制御は、グローバルなデバイス・タイプごとに設定したり、デバイスの特定のモデルやメーカーごとに設定したりできます。

Pointsec Protectorでサポートされる操作モードは以下のとおりです。

- アクセス拒否
- 読み取り専用アクセス
- シグネチャの提示による読み取り専用アクセス
- フル・アクセス
- 暗号化フル・アクセス (暗号化ポリシー・マネージャを使用)
- オフラインでのデータ・アクセスが可能な暗号化フル・アクセス

すべてのUSBデバイス・アクセスは、デバイスのタイプ、モデル、メーカー別に制御できます。

### デバイス管理、コンテンツ・フィルタリング、暗号化(オプション)

Pointsec Protectorには、独自のメディア認可システムが含まれており、コンテンツに基づいてデジタル・タグを付けたり承認したりすることができます。デバイスごとにデジタル・シグネチャが生成され、そのデバイスが「承認済み」かどうかマークされます。保護されている環境内でデバイスに情報が格納されると、デジタル・シグネチャが自動的に更新されます。組織の外でメディアに変更を加えることが許可されている場合(例えば、ビジネス・パートナーとデータを共有している場合)は、そのデバイスを保護された環境内で再び使用する前に認可を受け直す必要があります。

また、ユーザによる操作をさらに簡略化するため、プラグアンドプレイ対応のストレージ・デバイスに書き込まれているコンテンツを、ファイル名やファイル形式(Excelスプレッドシート、PDFなど)でフィルタできます。Pointsec Protectorでは、デバイスごとのデジタル・シグネチャでアクセス制御できるため、コンテンツに対するデバイス固有のセキュリティ権限を付与することも可能です。このような権限を付与することにより、過失か故意かに関係なく、保護されているファイルが無認可のポータブル・ストレージ・デバイスに転送されるのを防ぐことができます。

Pointsec Protectorでは、悪意あるコンテンツを含むファイルが、ストレージ・デバイスから組織のエンドポイントに転送されるのを防ぐこともできます。管理者が定義したファイル形式を、ユーザ別やグループ別に制御できます。新しいソフトウェア・パッケージのインストールは、信頼できるユーザおよびアプリケーションにのみ許可されます。

さらには、業界トップ・レベルのPointsec暗号化ソリューション全製品を、Pointsec Protectorに活用することも可能です。このオプションの集中管理機能を使用することで、エンドユーザによる特別な操作なしで、外部ストレージ・デバイスに転送されるファイルを自動的に暗号化したり、エンドポイントからそれらのファイルにアクセスするときに自動的に復号化したりできます。これらの機能により、ネットワーク・セキュリティのレイヤ制御の範囲外で発生するデータ・アクセスを完全に保護できます。

### 集中管理

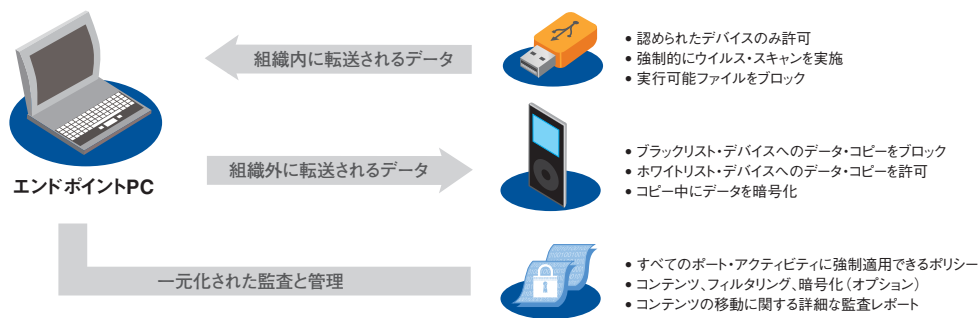
管理は、一般的なMMC(Microsoft Management Console)インタフェースで行います。一元化された監査および警告機能により、セキュリティを侵害する攻撃やデバイスの利用状況がすべて報告されます。監査情報は、クライアント側で暗号化およびフィルタ処理された後、指定の間隔でサーバに転送されます。管理者が定義したイベントについて、電子メールで警告を受信することも可能です。多くの場合、エンドポイント・セキュリティ方針を実装するには、特定のデータ・ファイルや特定のタイプのプラグアンドプレイ・デバイスの動向を、組織内で追跡できるようにするだけで十分です。それ以上の規制によって、ユーザの業務パターンを変更する必要はありません。

「Pointsec Protectorを選んだのは、Allen & Overyに寄せられるビジネス・ニーズの要件を満たすテクノロジーだった、という単純な理由からです。Pointsec Protectorを全社に導入した今では、その詳細な監査機能のおかげで、どのデータがどこに移動したかを完全に把握できるようになりました。しかし、最も重要なのは、データが常に保護されていると我々が確信できていることです。」

マーク・ヒースコート

ITアーキテクト兼設計マネージャ

Allen & Overy (英国の法律事務所)



Pointsec Protectorは、企業データの侵害リスクが最も大きい経路を遮断します。

## 詳細について

Pointsec Protectorの詳細について、ぜひチェック・ポイントまでお問い合わせください。Pointsec Protectorは、企業全体にわたってポートを保護するためのシンプルなソリューションです。導入プロセスが自動化されており、少ない作業負担で素早く導入できます。一元化された管理と操作により、USBポート経由のデータ漏洩を効率的かつ費用対効果の高い方法で制御できます。より詳しい情報については、チェック・ポイントまたはチェック・ポイント製品取り扱い代理店までお問い合わせいただくか、[www.checkpoint.co.jp/products/datasecurity/protector/](http://www.checkpoint.co.jp/products/datasecurity/protector/)をご覧ください。

©2003-2007 Check Point Software Technologies Ltd. All rights reserved.  
 Check Point, Application Intelligence, Check Point Express, Check Point Express CI, Check Pointのロゴ, AlertAdvisor, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, Zone Labs of the... Check Point Software Technologies Ltd. あるいはその関連会社の商標または登録商標です。ZoneAlarm is a Check Point Software Technologies, Inc. Company. その他の企業、製品名は各企業が所有する商標または登録商標です。本書で記載された製品は米国の特許No.5,606,668、5,835,726、6,496,935、6,873,988、および6,850,943により保護されています。その他の米国における特許や他の国における特許で保護されているか、出願中の可能性があります。

Preventing Data Leaks on USB Ports

P/N:502480-J 2007.05

※記載された製品仕様は予告無く変更される場合があります。



**Check Point**<sup>®</sup>  
 SOFTWARE TECHNOLOGIES LTD.

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社  
 〒160-0022 東京都新宿区新宿5-5-3 建成新宿ビル6F  
<http://www.checkpoint.co.jp/> E-mail: info\_jp@checkpoint.com Tel: 03 (5367) 2500