標準価格（Windows版）

売り切りタイプ

	製品名	標準価格（税別）
管理用サーバ	JP1/秘文 Server 基本ライセンス	1,000,000円
	JP1/秘文 Server ファイルサーバライセンス	100,000円
出さない	JP1/秘文 Device Control	10,000円
見せない	JP1/秘文 Data Encryption	10,000円

※ 別途、製品プログラムの費用として、製品ごとに1,000円［標準価格（税別）］が必要です。
ただし、「JP1/秘文 Server ファイルサーバライセンス」の媒体は「JP1/秘文 Server 基本ライセンス」に同梱されています。

サブスクリプションタイプ

1年ごとに契約の更新が必要なサブスクリプションタイプの商品です。

	製品名	標準価格（税別）
出さない	JP1/秘文 Device Control - Subscription Type*1*4	5,040円
	JP1/秘文 Device Control - Subscription Type - 24 Hours Support*1*5	7,080円
見せない	JP1/秘文 Data Encryption - Subscription Type*2*4	5,040円
	JP1/秘文 Data Encryption - Subscription Type - 24 Hours Support*2*5	7,080円
放さない	JP1/秘文 Data Protection - Subscription Type*3*4	5,040円
	JP1/秘文 Data Protection - Subscription Type - 24 Hours Support*3*5	7,080円

＊1 JP1/秘文 Device Controlの1年間のプログラムプロダクトの使用権、およびサポートサービスの利用権を提供します。JP1/秘文 Server 基本ライセンスの1年間のプログラムプロダクトの使用権、およびサポートサービスの利用権も含まれます。
＊2 JP1/秘文 Data Encryptionの1年間のプログラムプロダクトの使用権、およびサポートサービスの利用権を提供します。JP1/秘文 Server 基本ライセンスとJP1/秘文 Server ファイルサーバライセンスの1年間のプログラムプロダクトの使用権、およびそれぞれの製品のサポートサービスの利用権も含まれます。
＊3 JP1/秘文 Data Protectionの1年間のサービスの使用権、およびサポートサービスの利用権を提供します。JP1/秘文 Data Protectionを管理するサーバ機能は、クラウドによるサービスとして提供します。
＊4 サポートサービスが平日8:00～19:00の商品です。
＊5 サポートサービスが24時間週7日対応の商品です。

●本カタログに記載している価格は、2017年4月現在の日本で販売する場合の標準価格です。
●カタログに記載の仕様は、製品の改良などのため予告なく変更することがあります。
●製品の色は印刷されたものですので、実際の製品の色調と異なる場合があります。
●動作環境や対応状況については、JP1ホームページ（製品情報サイト）で最新情報をご確認ください。
●本製品を輸出される場合には、外国為替及び外国貿易法の規制ならびに米国の輸出管理規則など外国の輸出関連法規をご確認のうえ、必要な手続きをお取りください。
なお、ご不明な場合は、弊社担当営業にお問い合わせください。

JMI-0231 CM009

製品に関する詳細・お問い合わせは下記へ

■製品情報サイト
http://www.hitachi.co.jp/jp1/

■インターネットでのお問い合わせ
http://www.hitachi.co.jp/soft/ask/

■電話でのお問い合わせはHCAセンターへ
0120-55-0504 受付時間 9:00～12:00、13:00～17:00（土・日・祝日・弊社休日を除く）
携帯電話、PHS、一部のIP電話などフリーダイヤルがご利用いただけない場合は、ダイヤルイン：045-762-3059
（通話料金はお客さまのご負担となります）

株式会社 日立製作所 サービスプラットフォーム事業本部

SP-831-30 2017.4

HITACHI Inspire the Next

情報漏えいを未然に防ぐセキュリティ対策で
安全に情報を利用したい

JP1/秘文

**JP1/秘文は、情報の不正な持ち出しや、人的ミスによる情報漏えいを未然に防ぎ、
安全な方法で情報を利用するためのセキュリティ対策製品です。**

社内にある機密情報の不正な持ち出しや、組織内外の関係者間での情報共有時に起こりうる情報流出を「出さない」「見せない」「放さない」の3つの視点で対策することで、さまざまな情報漏えいリスクを見据えた着実なセキュリティ対策を実現できます。利用者の判断に任せない管理者主導のセキュリティ対策が可能なため、不正利用を意図した情報漏えいを回避するだけでなく、データの送受信や組織外へのデータの持ち出しなど、さまざまな業務で起こりうる過失的な情報漏えいのリスクも低減できます。

「出さない」「見せない」「放さない」で情報漏えいを防止

漏えいしてはいけない情報を社外に「出さない」ために、スマートフォンやUSBメモリーなどのデバイスの利用や接続先ネットワークを制御して、機密情報が社外に流出することを防ぎます。また、情報が社外に出ても中身を「見せない」ように、PCや記録メディア、ファイルサーバのデータを暗号化することができます。さらに、情報を社外に渡しても手を「放さない」ことで、万一、情報が流出してもファイルの閲覧停止（IRM）により、社外に渡した情報の不正利用や流出・拡散を防止します。

社内でも社外でも安全にデータを利用

社内では、PCの内蔵ハードディスクをドライブごと暗号化し、リムーバブルメディアや外付けハードディスク、ファイルサーバの共有フォルダも強制的・自動的に暗号化します。暗号化や復号を利用者が意識する必要はありません。一方、リムーバブルメディアやメール添付などで社外にデータを持ち出す場合は、パスワード入力により復号可能な形式でデータを暗号化できます。万一、紛失や盗難、誤送信が起きても、パスワードを知らない第三者は情報の中身を見ることができません。

出さない

デバイス制御

漏えいしてはいけない情報を、社外に「出さない」

スマートフォンやUSBメモリーなどのデバイスの利用をコントロール。機密情報が社外に出ることを防ぎます。

- デバイス制御
- ネットワーク制御
- ログ取得・管理

見せない

暗号化

情報が社外に出ても、中身を「見せない」

PCや記録メディア、ファイルサーバのデータを暗号化。第三者に情報の中身を見せません。

- ドライブ・メディア暗号化
- ファイルサーバ暗号化
- ファイル保護

放さない

閲覧停止

情報を社外に渡しても、手を「放さない」

ファイルの閲覧停止（IRM）で、相手に渡した情報の不正利用や流出・拡散を防止します。

- IRM
- 不正流出対策
- 予兆検知・可視化

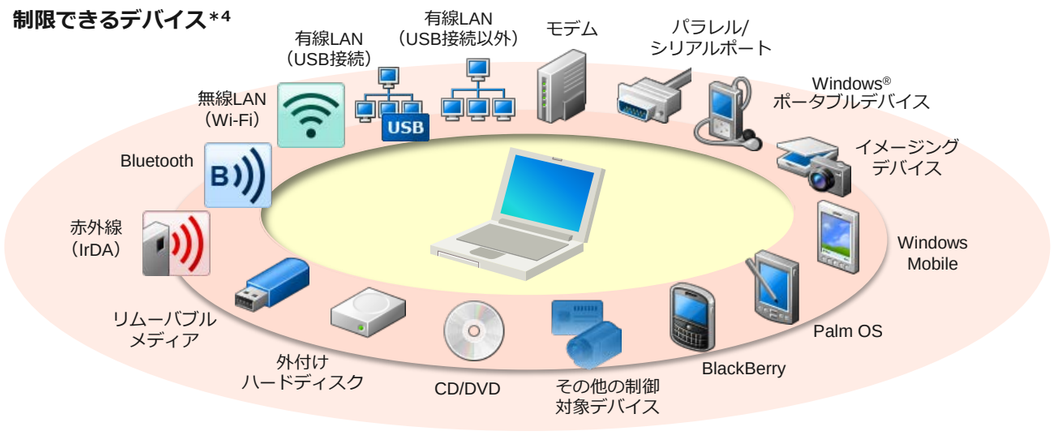
IRM：Information Rights Management

漏えいしてはいけない情報を、社外に「出さない」

デバイスの利用を制限

スマートフォン*1、USBメモリーなどのリムーバブルメディア、有線LAN、無線LAN、赤外線（IrDA）やBluetoothなどを利用した通信など、さまざまなデバイス（PCの周辺機器）を利用したデータのやりとりを制限できます。利用できるデバイスを制限することで、不正なデータコピーによる情報漏えいを防止できます。

また、利用を禁止したデバイスの中で、特定の機種のみ利用を許可することができるため、お客さまの利用環境にあわせた柔軟な運用が可能です。さらに、部署や利用者ごとに外部メディア*2へのデータコピーや印刷、ネットワーク利用*3などの許可・禁止を設定できます。



*1 スマートフォンは、OS、製造メーカー、接続方法などの違いによって、さまざまなデバイスとして認識されます。JP1/秘文はこれらのすべてのデバイスを利用禁止にすることで、スマートフォンへのデータコピーを防止します。

*2 リムーバブルメディア、外付けハードディスク、CD/DVDが対象です。

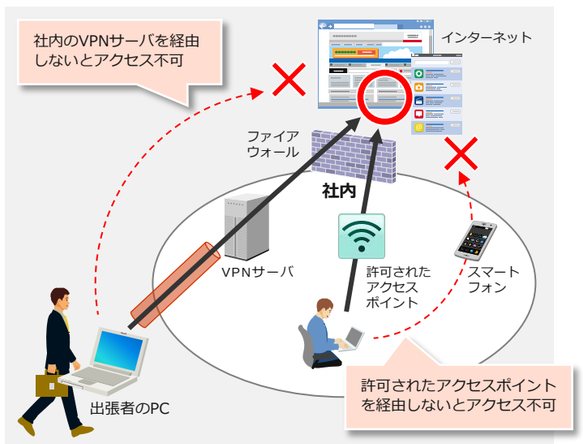
*3 ネットワークドライブやネットワーク上の共有フォルダが対象です。

*4 キーボード、マウスなどのヒューマンインタフェースデバイスは対象外です。

接続先ネットワークを制御

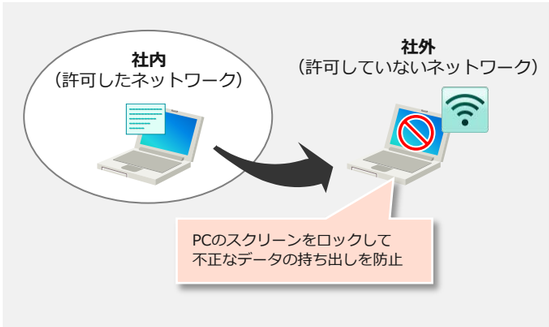
管理者が許可していないアクセスポイントはPCに表示しないようにできるため、スマートフォンやモバイルルーターなどのテザリング機能や不正に持ち込んだルーターなどを利用したインターネット接続を禁止できます。許可したアクセスポイントを使用する場合でも、社内のネットワーク以外には接続させないようにできます。また、社外でインターネットに接続するときには強制的に社内のVPNサーバを経由させることで、情報漏えいのリスクを低減できます。

VPN：Virtual Private Network



ネットワーク識別によるスクリーンロック

ノートPCなどにデータをコピーして社外に持ち出されても、管理者が許可したネットワークとの接続が切れると、PCのスクリーンをロックして操作を禁止し、不正なデータの持ち出しを防止できます。



ログの取得・管理

PCへのデバイスの接続ログや、リムーバブルメディアなどへのデータのコピーといった利用者の持ち出しログだけでなく、ネットワークへの接続や通信先ログも取得できます。ログを参照することで、不正な操作や社外への通信が行われていないかどうかの確認や通知ができます。また、ログ管理を周知することで不正行為の抑止効果も期待できます。

情報が社外に出ても、中身を「見せない」

社内利用のデータを自動的に暗号化

社内PCの内蔵ハードディスクをドライブごと暗号化し、PCの盗難や置き忘れなどによる情報漏えいを防止します。PCに保存されたデータは強制的・自動的に暗号化されるため、利用者が暗号化や復号を意識する必要はありません。また、リムーバブルメディアや外付けハードディスク、CD/DVD、ファイルサーバの共有フォルダも暗号化するので、社内でのデータのやりとりを安全に効率よく行えます。

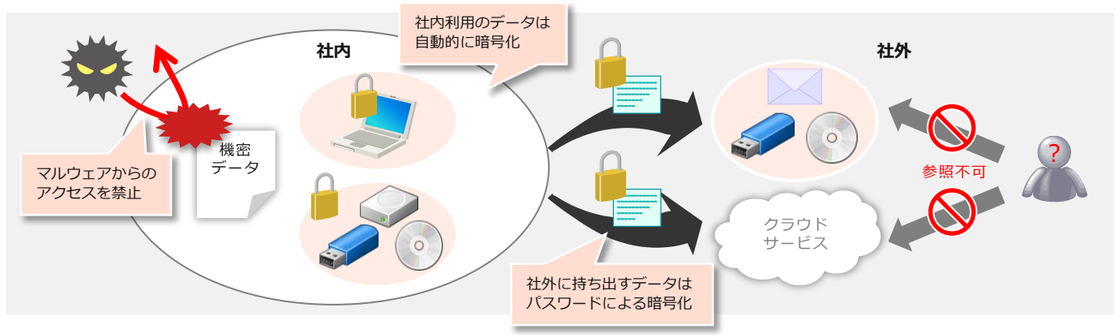
社外に持ち出すデータはパスワードで保護

リムーバブルメディアへの書き出しやメール添付、クラウドサービスの利用などで社外にデータを持ち出す場合は、パスワード入力により復号可能な形式でデータを暗号化*できます。万一、紛失や盗難、誤送信が起きた場合でも、パスワードを知らない第三者による解読を防ぎます。

＊ 暗号化したデータを参照するには機密ファイルビューアが必要です。機密ファイルビューアはWebからダウンロードできます。
http://www.hitachi-solutions.co.jp/hibun/sp/

機密データをマルウェアから保護

許可したプログラムからのみ機密データへアクセスできるようにすることで、データを保護します。マルウェアなどの許可していないプログラムが機密データにアクセスするのを禁止するため、社内の重要なデータを脅威から守ることができます。



情報を社外に渡しても、手を「放さない」

二次利用できない暗号化ファイルの作成

参照以外の操作を禁止した暗号化ファイル（閲覧型機密ファイル*）を作成できます。社外に閲覧型機密ファイルを送信しても参照しかできないため、不正な二次利用（編集、印刷、クリップボードへのコピー、プリントスクリーン）を防止できます。また、閲覧型機密ファイルには有効期限を設定でき、期限を過ぎると自動的に参照できなくなるので、社外に送信した場合でも期限管理や削除依頼の手間が省けます。

＊ ファイルの印刷イメージから閲覧型機密ファイルを作成します。
閲覧型機密ファイルを参照するには機密ファイルビューアが必要です。機密ファイルビューアはWebからダウンロードできます。
http://www.hitachi-solutions.co.jp/hibun/sp/

情報流出の予兆検知と閲覧停止が可能

閲覧型機密ファイルを開くときのパスワード認証を一定回数失敗するなど、情報流出が疑われる操作を検知すると、メールで管理者に自動通知します。また、閲覧型機密ファイルが参照された場所が地図上に表示されるため、利用範囲外で参照されたことを視覚的に確認できます。情報流出が疑われる場合には、すぐに閲覧型機密ファイルを閲覧停止（失効）にすることで、情報の拡散を防止できます。