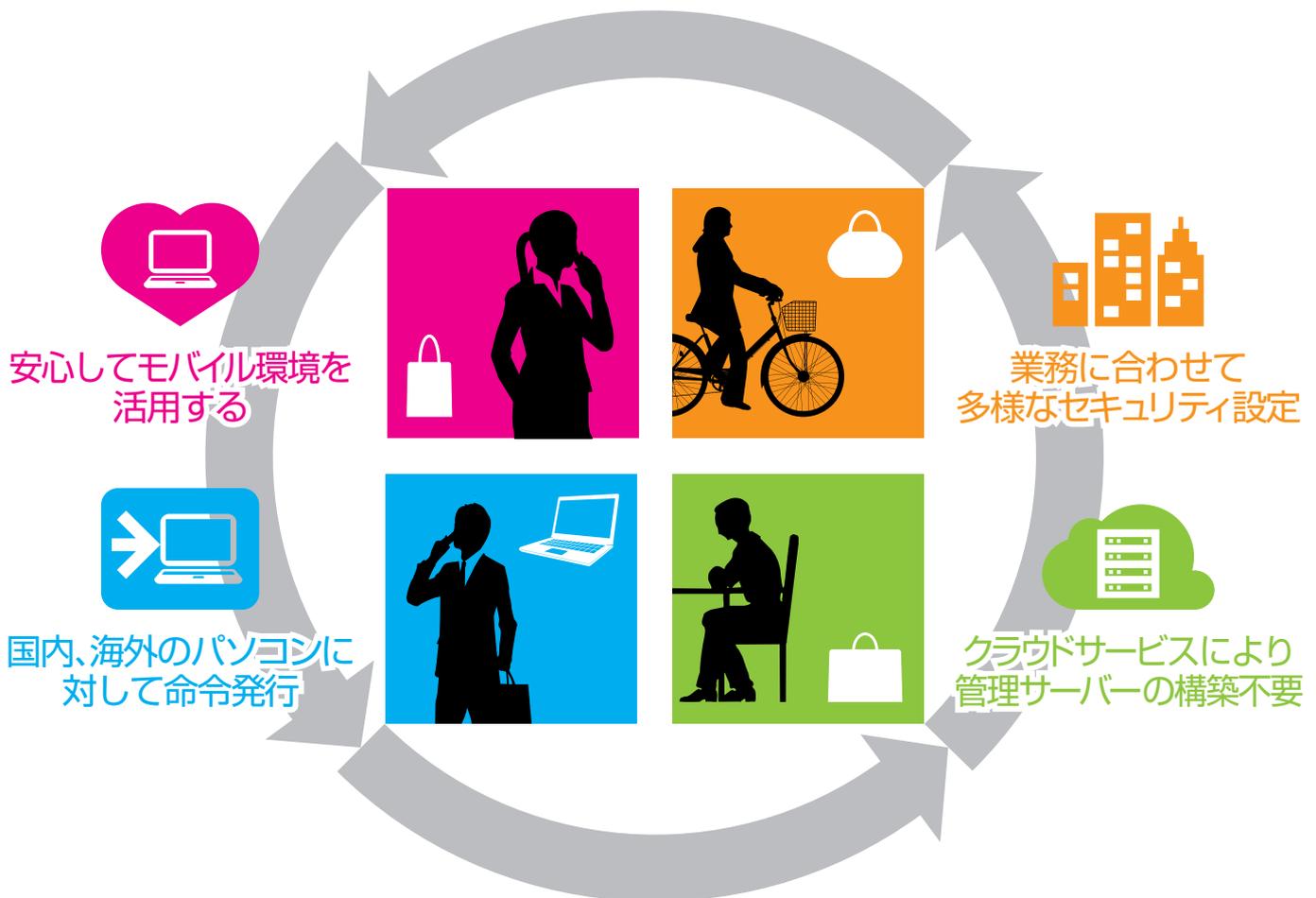


モバイル/パソコンを安心して活用するリモートワイプソリューション

TRUSTDELETE Biz

「TRUST DELETE Biz」は、盗難・紛失してしまったタブレットやノートパソコンに保存されている個人情報や機密データを、遠隔から消去できる情報漏えい対策ソリューションです。

盗難・紛失による企業のリスクを軽減



社員への罰則で情報漏えいを防ぐのではなく

紛失したら、“**データを消去**”して守る

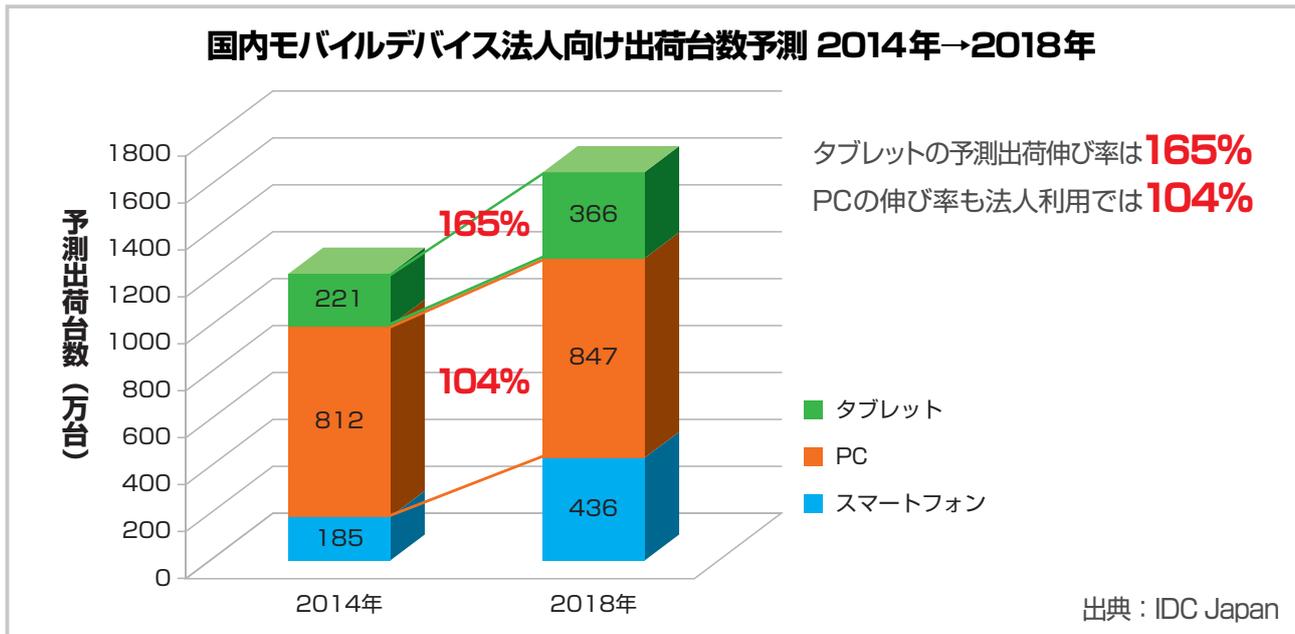
ソリューションで企業リスクを軽減する



タブレットやノートパソコンを活用しながら 安心のワークスタイルを実現

2005年の個人情報保護法の施行を機に個人情報の漏えいが大きなリスクとなり、多くの企業は個人情報を保存したパソコンの持ち出しを禁止するようになりました。しかし、多様化するビジネスへの素早い対応やモバイルネットワークの整備に伴い、改めて社外でパソコンを使用する機運が高まっています。

パソコンやタブレットの社外利用によって社員とデータのリソースを最大限に活用し、効率的なビジネスを実現するためにはモバイルのセキュリティの確保が重要課題です。



「TRUST DELETE Biz」のご利用者様の声

・ 利用目的 1 安心感をご提供する顧客満足向上

「個人情報や企業秘密を取り扱うことへのお客様の抵抗感や不安感が増していると考えております。過剰反応な面はあると思いますが、こうしたお客様の意識に対して「暗号化」という専門的な言葉での説明だけではなく、「何かあったら消せますよ」というシンプルな説明の方が圧倒的に分かりやすく、お客様の納得感も高いと感じているためデータ消去製品を探していました。お客様と接する場合には、保存したデータが暗号化されていることとあわせて、何かあったら消せるということを説明させるようにしています。」

生命保険会社 営業担当者

・ 利用目的 2 紛失で重要なデータの流出食い止める

「これまでは紛失したとしても暗号化されているから漏えいしないだろう、というところで妥協せざるを得なかった。これは、紛失後に継続して行う対策が無いと思っていたためです。」

その結果、紛失などの事案が発生した場合は善意の第三者が警察に届けてくれることを待つしかなかったため、事案をクローズすることが出来にくかった。

一方で他の業務で使用している iPad では MDM を利用することによりリモートワイプと位置情報を特定する機能があるため、完全ではないが位置を特定できた場合は回収が可能で、回収ができない場合も端末をリモートで初期化するという、待つ以外の継続した対策が取れていた。iPad では可能なことが Windows では出来ないということはセキュリティポリシー上説明がつかないため、Windows 用のリモートワイプ製品を探していた。」

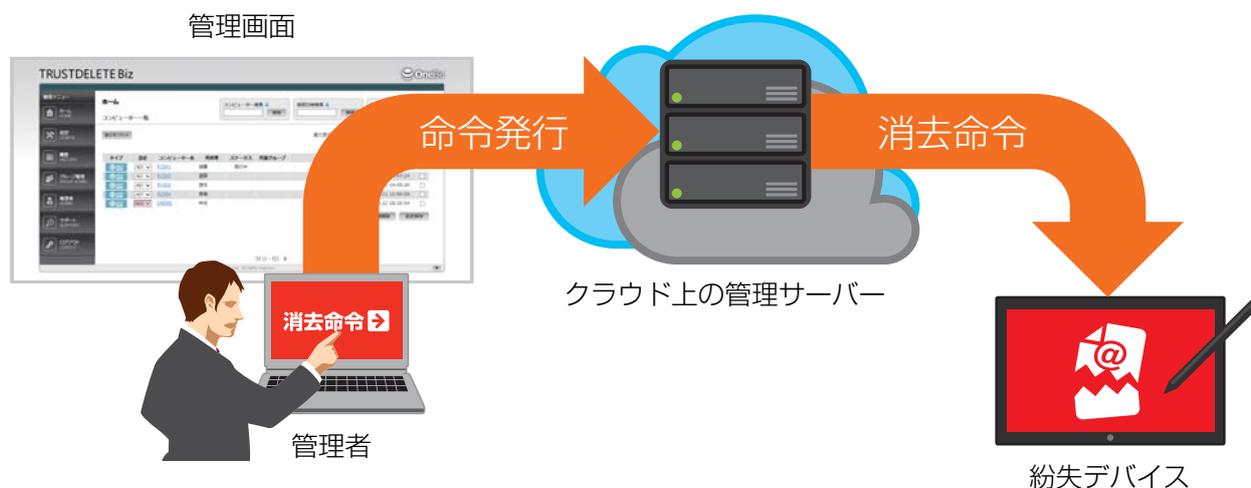
製造会社 セキュリティ担当者

Windowsパソコン用リモートワイプ クラウドサービス



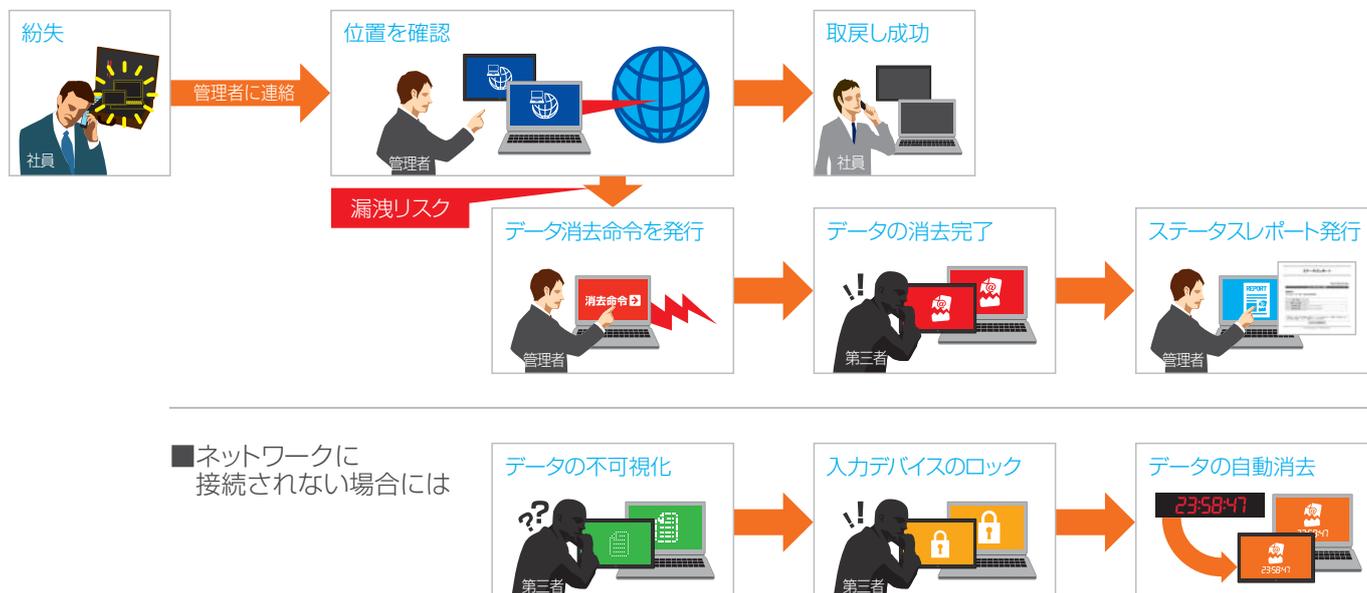
「TRUST DELETE Biz」の運用イメージ

管理サーバーは、クラウドサービスとして提供されるため、お客様側でサーバーを構築する必要はありません。



■ 「TRUST DELETE Biz」の活用方法

デバイスの紛失が発覚した場合、社内の管理者はインターネット経由で TRUST DELETE Biz の管理サーバーにログインします。紛失したデバイスを選択し、位置の確認をして想定外の場所で発見した場合には、直ちに消去命令を発行します。紛失したデバイスがネットワークに接続された時点で、指定したデータを復元不可能な手法で消去します。ネットワークに接続できない場合でも一定時間を経過すると、入力デバイスをロックして不正な操作を防ぐことや、自動的にデータを消去して情報の流出を防ぐことが可能です。

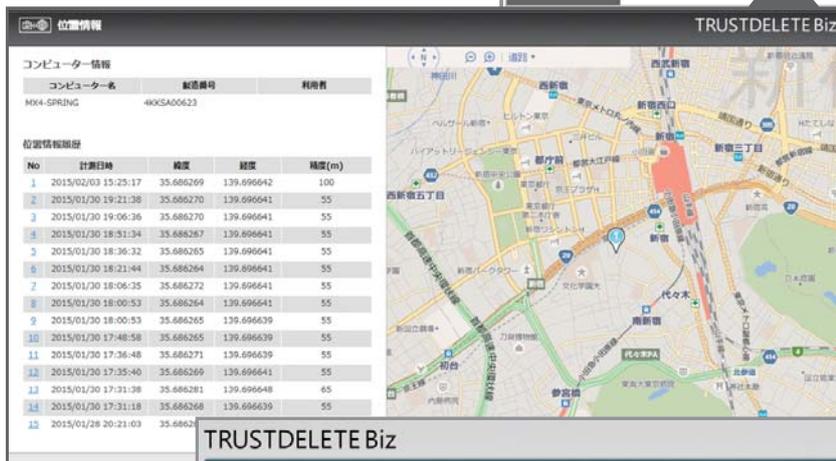
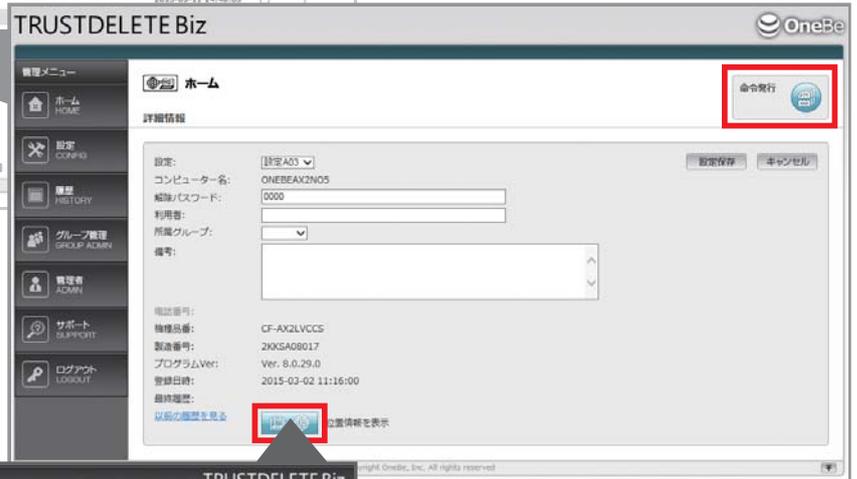




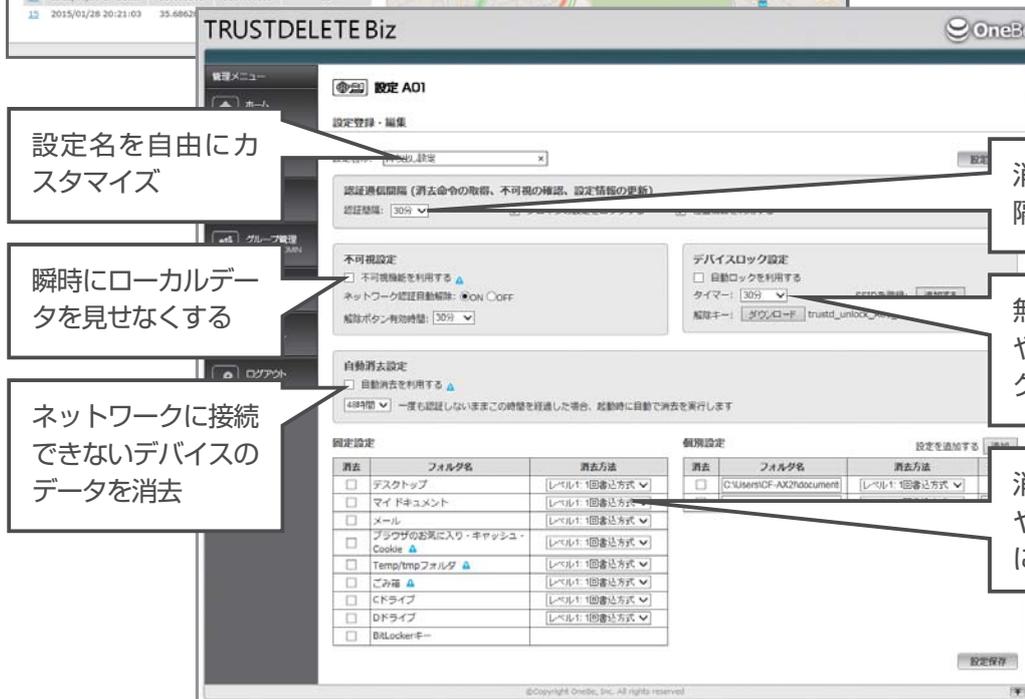
組織の規模や業種に応じて柔軟な運用ポリシーを実現



命令発行ボタンで
遠隔消去



デバイスの位置を特定
GPS または無線 LAN のアクセスポ
イント情報から取得した位置情報を最
大 15 か所まで表示



設定名を自由にカ
スタマイズ

瞬時にローカルデー
タを見せなくする

ネットワークに接続
できないデバイスの
データを消去

消去命令の受信間
隔を設定

無線 LAN の SSID
やUSBメモリでロッ
クの解除

消去するフォルダ
やファイルを任意
に指定

ご利用シーンや職種に
よって、機能ごとに詳細
なカスタマイズが可能



指定した重要なデータや個人情報をリモートワイプ

遠隔データ消去

遠隔からの命令で消去。命令を発行する際に、消去したいデータや消去方式を選択可能。

データ不可視化

インターネットに接続していない場合は一時的にデータを隠す。

自動データ消去

一定時間インターネットに接続しない場合には自動でデータを消去可能。



サイズ: 0 バイト
 ディスク上のサイズ: 0 バイト
 内容: ファイル数: 0, フォルダ数: 0

消去方式は、ゼロ 1 回書き込み式、または NSA 方式(3回書き込み)の 2 種類から選択できます。
 ※NSA 消去方式とは米国国家安全保障局の推奨する消去方式で、乱数を 2 回、0 を 1 回、計 3 回上書きを行う。

耐タンパー性エージェント

エージェントプログラムはパスワードなしにアンインストールすることができず、耐タンパー性仕様により、不正にプログラムを停止することもできません。

複数のパソコンへの導入

管理サーバーへの登録を自動化してインストール作業を軽減するサイレントインストールに対応しています。

※ご利用環境により、対応作業費が必要な場合がございます。



ステータスレポート

遠隔命令が実行された日時や消去したファイルの数をステータスレポートで確認することができます。



ロック機能

一定期間インターネットに接続されない場合には、マウス、キーボード、タッチパネルからの入力を無効化することで、デバイスの操作を一切不可能にします。

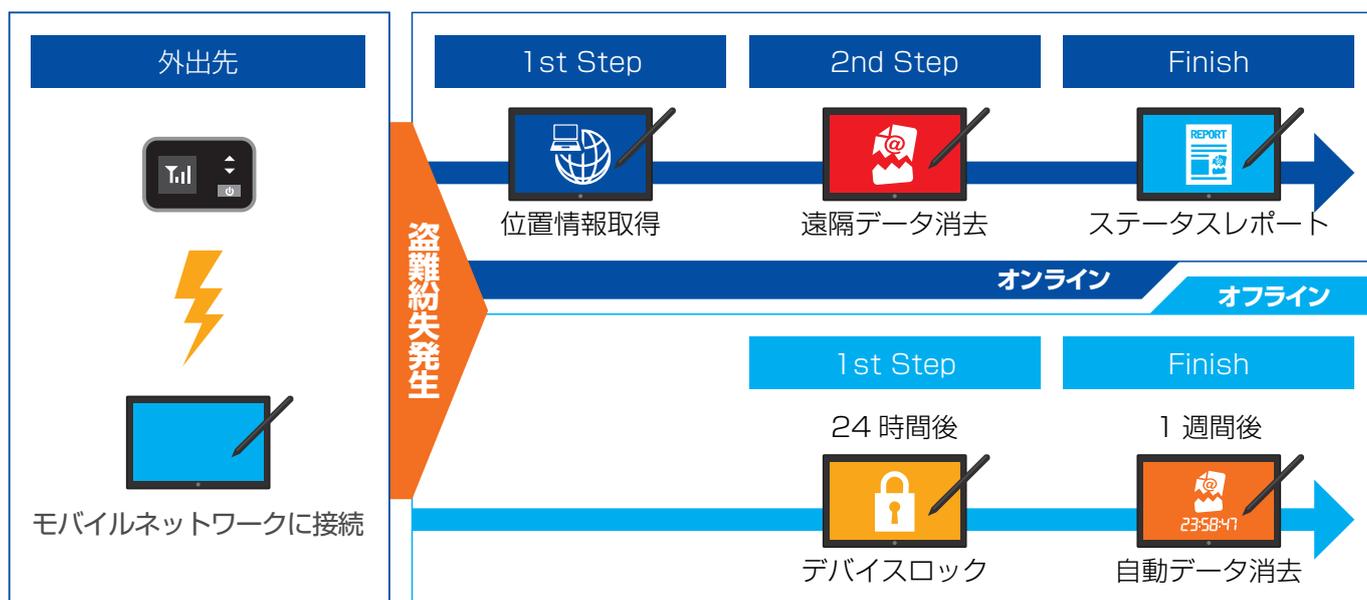


ニーズに合わせた様々なご利用ケース

▶ 持出PC対策 金融業

営業スタッフ持ち出し端末

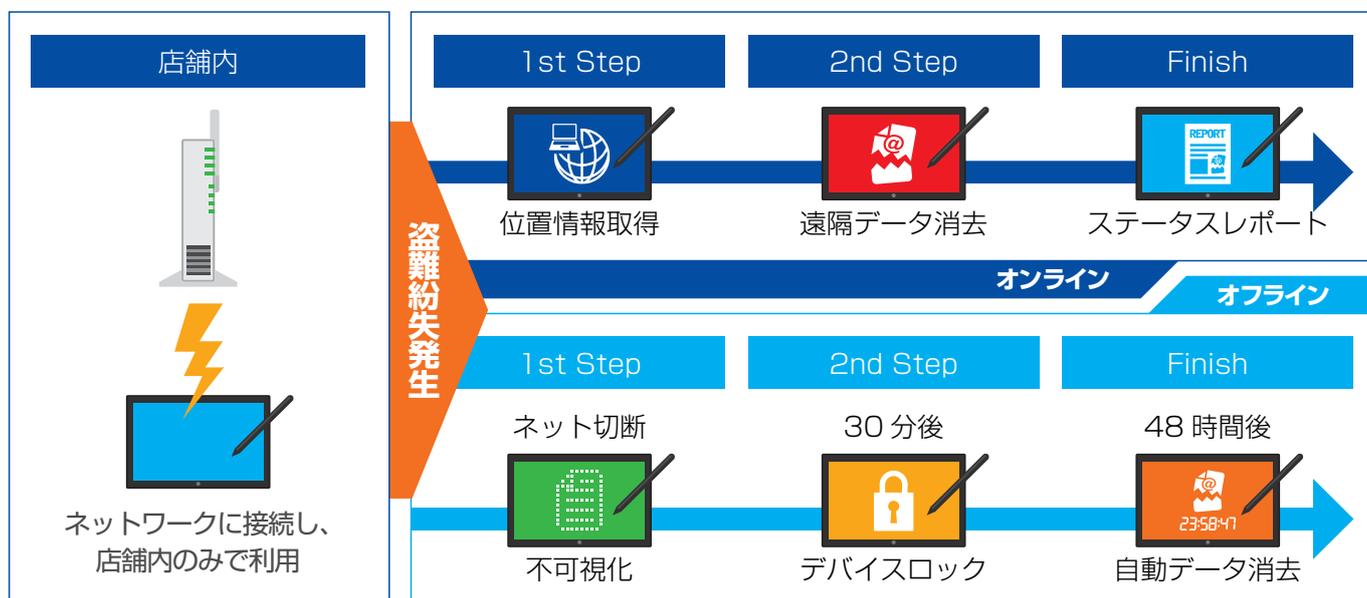
- ・ 端末の持ち出しを一切認めていなかったが、競争力強化の一環として一部の部門にのみテスト導入したい。
- ・ 禁止していたことを許可するにあたり、セキュリティのレベルを現状より高めることが必須。
- ・ 暗号化でデータは守るが、紛失後にも継続して対応できる対策が不足していると感じている。



▶ 持出禁止PC対策 サービス業

店舗・ショールーム用端末

- ・ アルバイトスタッフが多い環境で盗難が度々発生している。
- ・ OS にログインしている状態での盗難のため暗号化が機能していない。
- ・ 不特定多数の人が出入りする環境で盗難が度々発生している。



あらゆる環境に適合するTRUST DELETE Biz

■ 他社リモートワイプ製品に対する優位性

• Open MDM 製品のリモートワイプとは

Microsoft 社の System Center Configuration Manager と Windows Intune を代表とするデバイス管理製品に採用されている OMA-DM 技術を利用したリモートワイプです。これらは、デバイスを工場出荷状態に戻す初期化機能と Active Directory で管理しているワークフォルダ内のデータ削除に対応しています。

• TRUST DELETE Biz の優位性

TRUST DELETE Biz は国際標準規格の消去技術でデータを復元不可能な状態に処理できる上、ディスク上のフォルダー / ディレクトリを自由に指定して消去することが可能です。また、OMA-DM 方式のワイプとの最大の違いは、自動消去機能や不可視機能、ロック機能によってオフライン時にも有効な複数の対策を実装している点です。紛失したパソコンがインターネットや社内ネットワークに再び接続する保証はありません。あらゆるケースを想定した機能、それは TRUST DELETE Biz が盗難・紛失時のデータ流出を防止することを目的としたセキュリティ製品である証です。

■ 暗号化製品との併用

暗号化製品の場合、電源 ON で OS がログオンされた状態で盗難されると、セキュリティとして機能を果たさないが、TRUST DELETE Biz を併用することにより、そのような状態でも、位置情報取得やリモートワイプなどで対策が可能です。

デバイスの状態	電源状態	起動中				オフ
	OSログオン状態	ログオン		ログオフ		
	インターネット接続	あり	なし	あり	なし	なし
製品ごとの有効性	暗号化製品	×	×	○	○	○
	TRUSTDELETE Biz	○	○	○	○	×

「他のセキュリティ製品」または「暗号化製品」と組み合わせることで、より一層のセキュリティレベルの向上を図ることができます。

■ シンククライアント製品との併用

安全性の高いシンククライアントにおいても、万一の際にはローカルに残ったキャッシュデータや接続情報を削除することで、更に安全にご利用できます。



■ 閉域網ネットワーク(VPN)での運用

閉域網内に管理サーバーを構築することが可能。パソコンが管理サーバーと通信できない（外部に持ち出された）状況でも、データの不可視化や自動消去によりデータの流出を防ぎます。

動作環境、導入事例について

■ 動作環境

対応OS	CPU	メモリ(RAM)	ハードディスク
Windows 8 / 8.1 (32ビット / 64ビット) Windows 8 / 8.1 Pro (32ビット / 64ビット) Windows 8 / 8.1 Enterprise (32ビット / 64ビット)	1GHz 以上	32 ビットの場合 1GB 以上 64 ビットの場合 2GB 以上	100MB 以上の 空き容量
Windows 7、Windows Vista (32ビット / 64ビット) Ultimate, Professional, Home Premium, Enterprise	800MHz 以上 (1GHz 以上推奨)	32 ビットの場合 1GB 以上 64 ビットの場合 2GB 以上	
動作条件	.NET Framework4 のインストール環境 インターネットへの接続環境		



【導入事例】 約110万人の「メルスプラン」会員情報を守る

会社名 株式会社メニコン
本社所在地 〒460-0006 愛知県名古屋市中区
従業員数 1,089 名 (2014 年 3 月 31 日時点)
事業内容 コンタクトレンズ・ケア用品事業他
導入台数 600 ライセンス



・「コンタクトユーザー」の個人情報を守れ

110 万人もの会員データは、住所や氏名はもとより、診療情報や購入履歴といったセンシティブな情報が記載されているため、**ロックやリモートワイプを行う仕組みを導入することで、万一 PC が盗難されたり紛失したりしても、そこからデータが流出するリスクを最小化**しています。

・国内企業が自社開発した製品だからこそ

TRUST DELETE Biz は、**国内の企業が開発したということ**で、**管理画面もわかりやすく**、特定のデータを吐き出させて管理するといったことも柔軟にできる点や、問い合わせのレスポンスが速く、**特に苦勞もなくスムーズに導入できた点**を評価していただきました。

・持出しPCに加え、直営店舗PCにも

メニコンユーザの会員「メルスプラン」に入会したお客様の個人情報を管理するシステムを自社開発し、それを販売店に提供することで、顧客サービスの向上に役立てており、店舗 PC にも個人情報が保存されています。営業担当者が社外に持ち出して利用していたモバイル PC 200 台に加え、店舗の PC にも TRUST DELETE Biz を導入。現在は約 600 台にまで展開したところです。「今後も、持出し PC や盗難のおそれがある PC を中心に、さらに導入台数を拡大させていく方針」とのことです。

■ お問い合わせ先



ワンビ株式会社

〒151-0053 TEL: 03-6909-0305
東京都渋谷区代々木 2-18-3 WEB: <http://www.onebe.com>
オーチャー第一ビル 2F メール: sales@onebe.co.jp

会社名・製品名などは、各社または各団体の商標もしくは登録商標です。
※製品の仕様は予告なく変更になる場合がございます。

本資料の内容は予告なく変更となる場合がございます。最新情報につきましてはワンビ株式会社の WEB サイトをご確認ください。Rev 1.5

Copyright OneBe, Inc. All Rights Reserved.