



パートナー様総合窓口 PC、サーバーに関するお問い合わせは、こちらで対応しています。

☎ **0120-498-170** 受付時間: 9:00~12:00 / 13:00~18:00
(土、日、祝日、5月1日、12月30日~1月3日を除く)

✉ **L_pitch@lenovo.com**

●レノボジャパン オプション ●レノボジャパン サービス

NECパーソナルコンピュータ サービス ランサム ディフェンダーに関するお問い合わせは、こちらで対応しています。

☎ **03-6316-3305** 受付時間: 9:00~12:00 / 13:00~17:00
(土、日、祝日、5月1日、12月30日~1月3日を除く)

✉ **-NECPC-le1sal@lenovo.com**

●NECパーソナルコンピュータ サービス

●このカタログで使用されている製品の写真は、出荷時のものと一部異なる場合があります。また、仕様は事前の予告なしに変更する場合があります。●表示画面および印刷物の出力例のうち、特に断り書きのない出力例のデータ部分はすべて架空のもので、画面ははめ込み合成で実際の表示とは異なります。●このカタログの情報は2017年7月現在のものです。●製品、サービス等詳細については、弊社もしくはビジネス・パートナーの営業担当にご相談ください。●このカタログに掲載されている標準価格および料金は、2017年7月現在のものと事前の予告なしに変更する場合があります。最新の価格に関しては、弊社ホームページをご参照ください。●「ダイレクト価格」は、直販による提供価格であり、ビジネス・パートナーなど再販者の販売価格を拘束するものではありません。弊社ホームページでは供給状況などの事情により一部の製品を掲載しており、「ダイレクト価格」製品すべてが弊社ホームページで購入できることを意味するものではありません。●当カタログ記載の製品にインストールあるいは添付されているソフトウェア製品につきましては、その梱包方法および内容物に関し、市販されているものとは異なる場合があります。

Microsoft、Windows、Windowsロゴ、Windows Vista start button、Windows Aero、Windows BitLocker、Windows HotStart、Windows Live、Windows Media、Windows ReadyBoost、Windows ReadyDrive、Windows Server、Windows SideShow、Windows SuperFetch、Windows Vista、DirectX、Internet Explorer、Xbox 360、Excel、InfoPath、OneNote、Outlook、PowerPoint、Visio、Officeロゴ、IntelliMouse は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。他の会社名、製品名、サービス名等は、それぞれ各社の商標または登録商標。

レノボ・ジャパン株式会社 / レノボ・エンタープライズ・ソリューションズ株式会社
〒101-0021 東京都千代田区外神田四丁目14番1号 秋葉原UDX
<http://www.lenovo.jp/business/>

17-07 Printed in Japan

レノボが提供する安心のセキュリティ。

Lenovo Security Catalog

Different is better

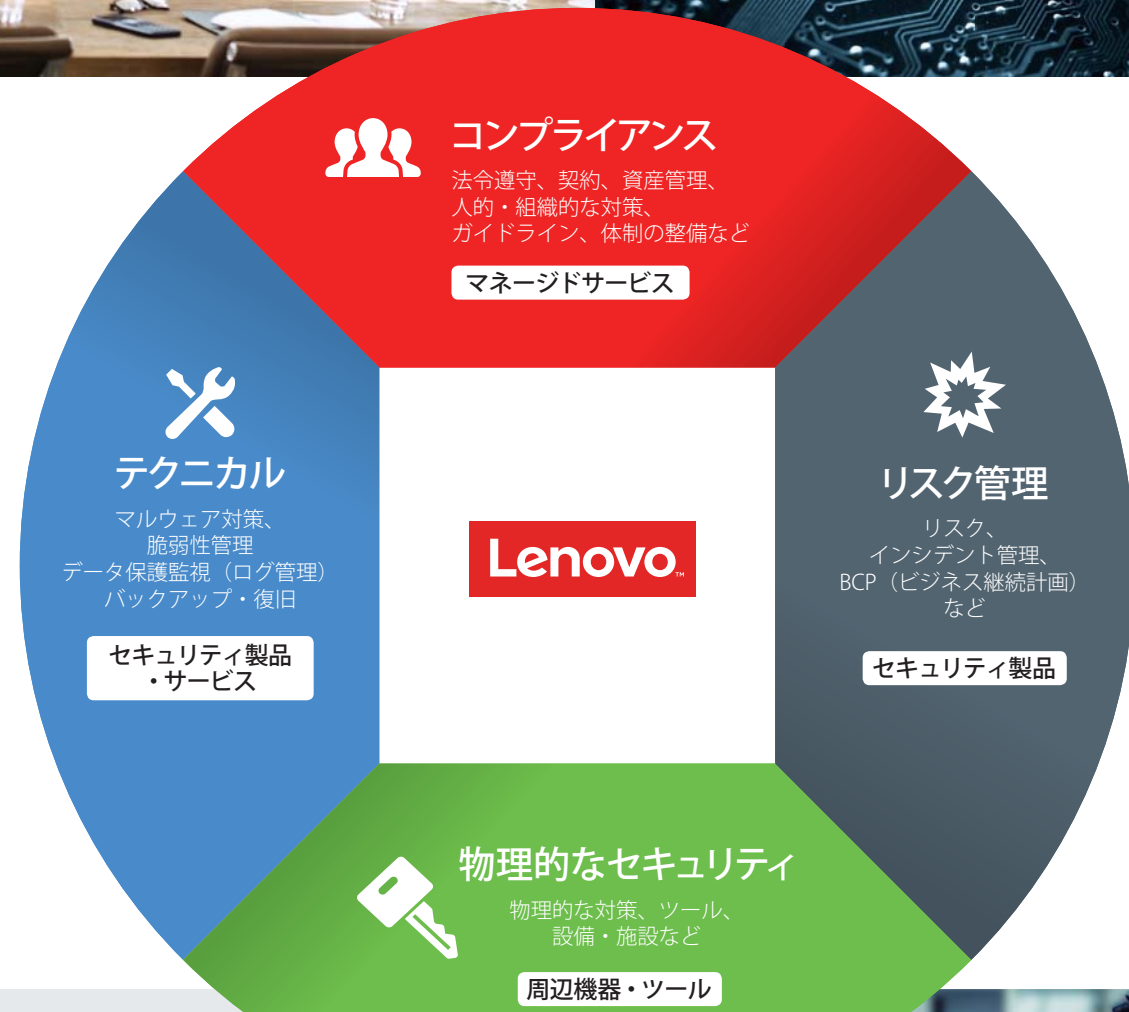
Lenovo™

標的になってからでは遅い。
「もしも」に備えた万全のセキュリティを。



レノボがオススメするセキュリティ対策のフレームワーク

私たちが目指すのは、常に、お客様の成功を「Productivity～生産性向上」によって支えること、その礎を築くための、セキュリティ・ソリューションをご提案します。



レノボが提案する具体的なセキュリティ対策とマッピング

		防御	検出	対応
テクニカル	マルウェア対策	マルウェアの把握・防御 Windows Defender SOTI ランサム ディフェンダー	早期侵入検知 Windows Defender ATP	攻撃後の対策 Windows Defender ATP SOTI Microsoft Intune
	脆弱性管理	パッチ管理 Microsoft Intune 修正アプリの配布 SOTI	早期侵入検知 Windows Defender ATP	攻撃後の対策 Windows Defender ATP SOTI Microsoft Intune
	データ保護	暗号化・認証 BitLocker / Windows 10 SecureDoc Absolute DDS	個人情報・マイナンバー検出 Absolute DDS 個人情報・マイナンバー検出ソフト	機器回収サービス Absolute DDS 遠隔データ消去サービス オンサイト記憶メディアデータ消去・物理破壊サービス
	監視		位置情報トラッキング SOTI Absolute DDS	リモートワイプ・ロック SOTI Absolute DDS SecureDoc 遠隔データ消去サービス
	バックアップ			バックアップ・事後復旧 シンクライアント ランサム ディフェンダー
	物理的なセキュリティ	暗号化・認証 セキュア ハードドライブ 盗難防止ワイヤー Kensington ケーブル・ロック 盗難（覗き見）防止 プライバシーフィルター		

CONTENTS

●レノボジャパン オプション ●レノボジャパン サービス ●NEC/パーソナルコンピュータ サービス

	ページ	オプション	サービス
Windows 10 のセキュリティ	4		●
モビリティ・マネジメント	6	●	
デバイスのセキュリティ強化	8	●	
暗号化ソリューション	10	●	
レノボのマネージドサービス	13		●
	13		●
	14		●
レノボのセキュリティ製品	15	●	
	15	●	
	15	●	

一般的なセキュリティをさらに強化したい!

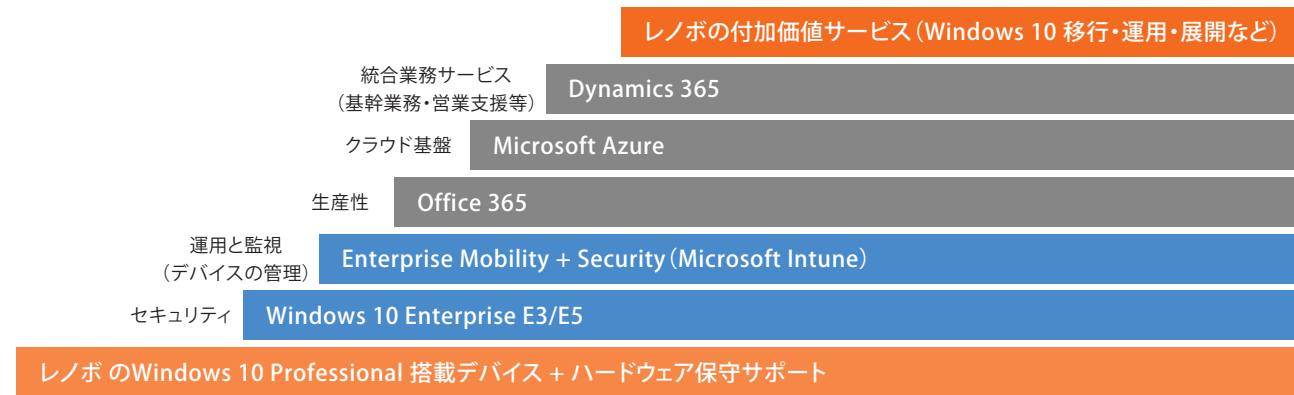
Windows 10 Enterpriseでさらに
安全で生産性の高い企業を作ります。

一般のインターネットユーザーと、セキュリティのエキスパートではこんなにセキュリティ対策が違う!

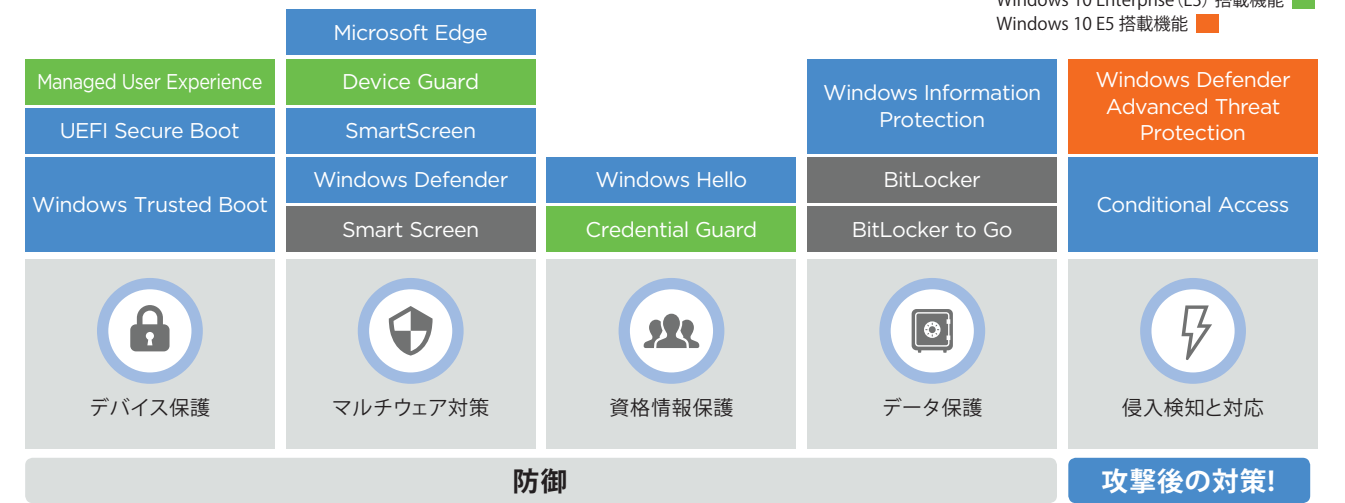
一般インターネットユーザーが行っている と答えたセキュリティ対策	VS	セキュリティのエキスパートが 行っていると答えたセキュリティ対策
1. アンチウイルスソフトを使う		1. ソフトウェアアップデートをインストールする
2. 強固なパスワードを使う		2. サービスなどにユニークなパスワードを使う
3. 頻りにパスワードを変える		3. 二段階認証を利用する
4. 知っているウェブサイトしか利用しない		4. 強固なパスワードを使う
5. 個人情報公開しない		5. パスワード管理ツールを使う

レノボがマイクロソフトのクラウドサービスで提供する価値

レノボはマイクロソフトのソリューション・プロバイダー (CSP) として、レノボ独自の付加価値サービスを提供します。



Windows 10 セキュリティの多層防御



セキュリティをさらに強化 Windows 10 Enterprise E3

E3は、大規模および中規模の組織のニーズに対応するための高度な機能を追加することで、Windows 10 Pro上に構築されています。最新のセキュリティ脅威に対する先進的な防御、OSの展開と更新に関する幅広いオプション、包括的なデバイスとアプリケーションの管理などがあります。



早期侵入検知サービス

Windows 10 Enterprise E5 Windows Defender Advanced Threat Protection (ATP)

Windows Defender ATPは、Windows 10が提供する既存のセキュリティ機能とサービス (Pre-Breach) をベースに、Windows 10セキュリティスタックに対する新しいポスト侵害防止レイヤーを提供します。これにより、顧客はネットワーク上の高度な攻撃やデータ侵害を検出、調査、修復することができます。



汎用のモバイルデバイスを業務用にできるか不安!

モビリティ管理を容易にすることで、企業のモビリティに無限の可能性をもたらします。

2017年5月、SOTIは複数の製品を緊密に統合した新しいソリューションプラットフォーム、SOTI ONEを市場投入しました。SOTI ONEプラットフォームは、企業がビジネス成功の鍵とすべくモビリティやIoTをオペレーションやプロセスに有効利用しようと試みたときに直面する根本的な問題に焦点を当て、解決するための比類ない機能を提供します。

このようなお客さまにお勧めします

- 汎用デバイスを業務専用として利用したい
- さまざまなOSのデバイスを一元管理したい
- デバイスにアプリをサイレント配布したい
- デバイスをリモートコントロールしたい
- デバイスの物理的なボタンを遠隔操作したい
- コンテンツを管理したい
- デバイスの資産管理もしたい

デバイスのライフサイクル管理

- デバイス登録
- デバイスプロビジョニング
- デバイスセキュリティ
- デバイス管理
- アプリケーション管理
- コンテンツ管理
- デバイスリプレイス

事例 様々な形態のデバイス管理

キオスクモード、レノボ製品の物理的ボタンの遠隔操作 在宅ホームケアサービス

- ケアワーカー400名
- キオスクモードで業務効率を大幅にアップ
- 正確な位置情報サービスやリモート
- 端末の位置情報でケアワーカーの管理
- 遠隔操作で通知や端末の問題を解決

Windowsタブレット及び業務アプリのリモート管理を実現 大手ビジネスマーケット調査会社

- 毎年50,000人をインタビュー
- アプリケーションの無料配布
- トラブルシューティングのためのリモート管理制限
- 過失/盗難デバイスの位置情報

医療系事例の共通点

汎用デバイスを医療現場で使用するのに色々と不安

- 汎用デバイスをキオスクにて業務デバイス化
- 不安を未然に防ぎ、業務効率、セキュリティのアップ!

デバイスの知識がなく不安

- 物理ボタンまで操作できる遠隔操作で、丁寧に細かな遠隔によるサポートが可能!

機能

MobiControl エンタープライズモビリティ管理

- 統一されたエンドポイント管理-iOS、Android、Windows、プリンター及びLinux
- レノボとの提携による独自のAndroid+テクノロジー
- カスタマイズ可能なキオスク技術で汎用的なデバイスを業務専用デバイス化
- デバイスの位置情報に基づいたジオフェンスによるデバイス管理と制御
- 基本的なリモートロック・ワイプはもちろん、ログやファイルの取得
- リモートコントロールによる遠隔地のデバイスをトラブルシューティング
- アプリケーションやコンテンツの管理、配布と回収

SOTI Snap 迅速なアプリケーション開発

- アプリの作成と配布を数分で完了
- プログラミング無しのドラッグアンドドロップでのアプリ作成
- エンジニアのような知識がなくてもアプリ作成可能
- スマホやタブレットのサイズに自動調整
- MobiControlのiOS SDKと連携しiOSアプリは作成したアプリからリモートビューが可能

SOTI Assist モバイルファーストなヘルプデスク

- MobiControlでのリモートコントロール、分析を統合したモバイルファーストのヘルプデスク
- スクリーンショットやデバイス、ユーザー情報をサポートケースへ自動的に添付
- サポートケースのためのトラブルシューティングの文書化にかかる時間を短縮
- MobiControlとの統合で必要な管理・制御をリアルタイムに実行
- やりとりの高度な監査記録

随時リリース予定

- SOTI Insight **ビジネスインテリジェンス**
- SOTI Connect **IoTゲートウェイ**
- SOTI Collaborate **お客様&パートナー様のBtoBtoC コラボレーション**

SOTI MobiControlの販売に関する情報

製品名	製品内容	参考価格 (税別)
MobiControl On-Premise SaaS	プライベートクラウドまたはオンプレのデバイスライセンス	¥4,500 / 1年(1台)
MobiControl Cloud SaaS	SOTIのクラウドのデバイスライセンス	¥5,500 / 1年(1台)
MobiControl JumpStart Implementation	管理コンソール設定支援サービス	¥203,400

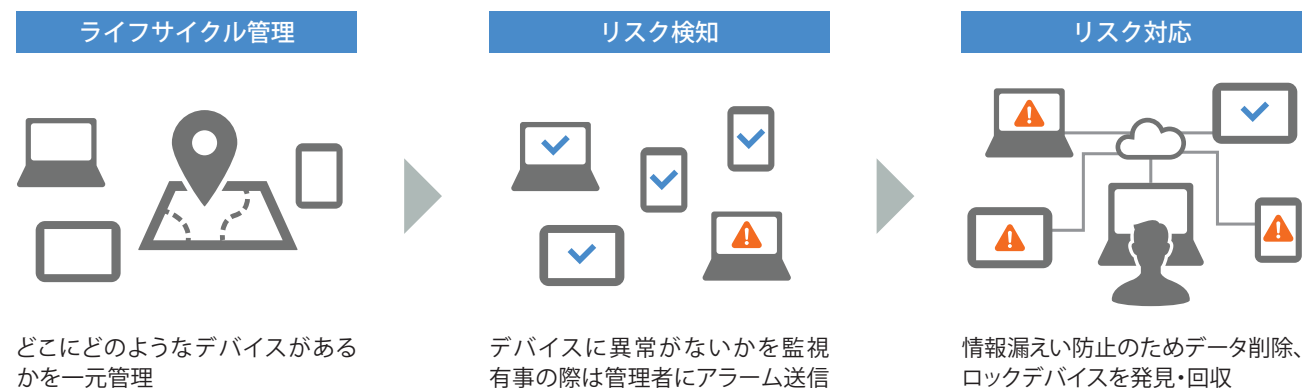
持ち出すデバイスの盗難や紛失、データの悪用が不安!

モバイルデバイスに対する盗難対策、
情報漏えい対策ソリューションを提供します!!

Absolute® Data & Device Security (DDS) は、パソコンやタブレット、スマートフォンなどのモバイルデバイスに対し、盗難・紛失時の情報漏えい防止と資産保護を提供します。Absolute DDSは、万が一、お客様のデバイスが盗難や紛失に遭った場合に、リモートからデータを削除して情報漏えいを防止したり、ロックして悪用を防ぐことができます。また、警察と協力しながら盗まれたデバイスを取り戻すお手伝いをします。

このようなお客さまにお勧めします

ノートPCを持ち出したいけど、情報漏えいが心配	シンクライアントを導入したいが、コストが高すぎる
社内にあるデバイスが、どこでどんな構成で使われているか把握したい	暗号化しているけど、パスワードを見破られたり、スリープモードのまま盗まれた時に心配
日本国内だけでなく、海外出張が頻繁にある	ノートPCやスマートデバイスに異変があったらすぐに検知したい



事例 持ち出し用デバイスの盗難・紛失対策

<p>保険外交員用 タブレットの情報漏えい対策</p> <ul style="list-style-type: none"> ●暗号化ソフトと機能補完 ●デバイスの位置情報把握 	<p>製薬会社MR用 PCの資産保護</p> <ul style="list-style-type: none"> ●車上荒らしによる盗難対策 ●新薬データなど機密情報の保護 	<p>店頭用タブレットの 盗難対策</p> <ul style="list-style-type: none"> ●店舗設置タブレットの盗難対策 ●棚卸補助 ●ジオフェンシング
---	--	--

機能

- 遠隔データ消去**
 - 遠隔地にあるデバイスのデータを消去
 - 全データ消去、OS以外のデータ消去、フォルダ単位の消去、ファイル単位の消去
 - デバイスに保存されているファイルの一覧を取得可能
 - 消去前にデータのバックアップを取得可能
 - ファイルへの最終アクセス日時を把握
- 位置情報トラッキング**
 - GPSもしくはWi-Fi APから位置情報を取得、地図上に表示
 - 過去の位置情報の履歴も表示可能
 - 地図上に指定された範囲から持ち出された場合、管理者にアラート送信 (ジオフェンシング)
- 遠隔デバイスロック・タイマーロック**
 - 遠隔地にあるデバイスをロック
 - 任意のメッセージを表示することも可能
 - 一定期間、ネット接続がない場合、デバイス側でロックすることが可能
- 盗難デバイスの発見・回収サービス**
 - 盗難に遭ったデバイスを物理的に発見し、警察と協力しながら取り戻し
 - 今までに盗難に遭ったデバイスのうち、4台に3台が回収成功
- 資産管理** レポートと不審デバイスの検出
 - ハードウェア構成情報
 - インストールされているソフトウェア情報
 - ユーザー名やデバイス名が変更になるなど、不審な動きをするデバイスがあったら管理者にアラート送信
 - マイナンバーやクレジットカード番号など、許可されていないデータを保存しているデバイスを抽出
- エージェント自動復活機能**
 - 万が一エージェントが削除された場合、自動的に再インストール
 - レノボ製品のBIOSに、復活用モジュールを組み込み済み

※回収を保証するものではありません

Absolute DDSの販売に関する情報

*1-2,499台まで。2,500台以上はお問い合わせください。

製品名	製品内容	年間参考価格 (税別)
Absolute DDS Premium	資産管理、遠隔データ消去・ロック、位置情報トラッキング、回収サービス	¥6,500 / 1台
Absolute DDS Professional	資産管理、遠隔データ消去・ロック、位置情報トラッキング	¥4,000 / 1台
Absolute DDS Standard	資産管理、遠隔データ消去・ロック ※資産管理はハードウェア情報のみ	¥2,500 / 1台

クライアントPCや散在するデータからの情報漏えいが心配!

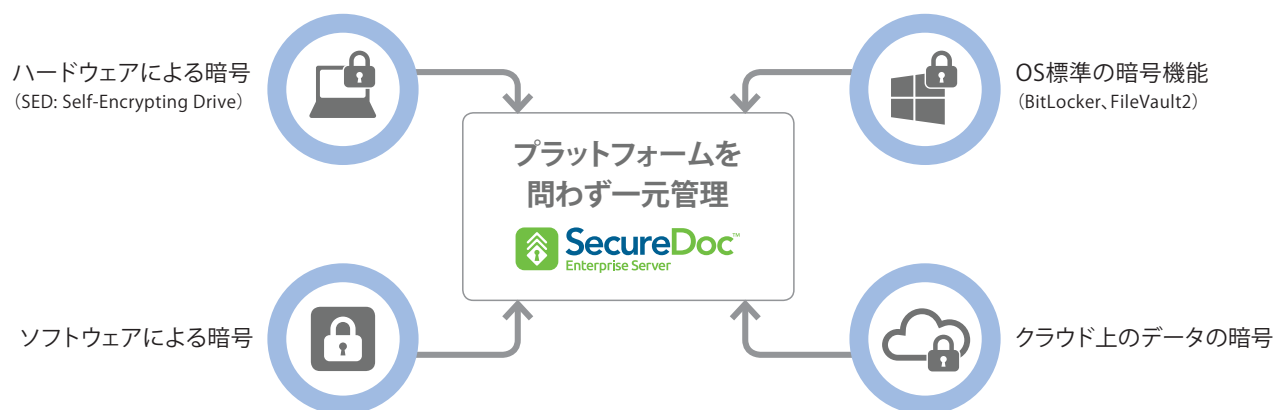
あらゆる場所のデータを暗号化するSecureDocで情報漏えいを防ぐことができます!!

ウィンマジックのSecureDocはノートPC、デスクトップPCのフルディスク暗号を実現するとともに、BitLockerやTCG OPALで暗号化されたパソコンの暗号化状態を管理することができます。厳密に管理された暗号化により、端末を紛失・盗難に遭った場合でも情報漏えいを防ぐことができます。

このようなお客さまにお勧めします

- 情報漏えいを防ぎながらノートPCを持ち出したい!
- 社内だけで使用するデスクトップPCのセキュリティを高めたい!
- TCG OPAL搭載PCのセキュリティを高めたい!
- BitLockerを厳密かつ効率的に運用したい!
- データを安全に持ち運びたい!
- クラウドストレージサービスを安全に利用したい!
- 仮想サーバーのセキュリティを強化したい!

暗号化を行うから暗号化されているものを管理するへ



事例 業務用デバイスの情報漏えい対策

- セキュリティを高めながら、利便性を下げない運用を実現 大学病院**
 - 院内全端末1500台に導入
 - 人の出入りが自由な病院において発生するパソコンの盗難に対してデータを保護
 - 業界唯一の機能:プリブートネットワーク認証により利便性を維持
- 自己暗号化ドライブ (TCG OPAL) の導入効果を最大化 医療機器メーカー**
 - 8000台に導入済+全パソコン20000台に導入予定
 - OPALとの併用によって高パフォーマンスと高セキュリティを両立
 - 暗号化の管理、運用の効率化によりTCOを削減
- 複数の暗号化環境を一元管理 建設業**
 - 持ち出し対象パソコン全1500台へ導入
 - BitLocker暗号/パソコン、OPAL暗号/パソコン、SecureDoc暗号/パソコンを一元管理
 - 暗号化状態の維持、把握により有効な情報漏えい対策を実現

機能

- フルディスク暗号 SecureDoc FDE**
 - PCからHDD/SSDを外して、他のPCに外付けで装着してもデータにアクセス不可
 - プリブート認証を通過するまではデータは暗号化状態
 - 正規の手順以外でのクラッキングは不可能
- 暗号化端末管理**
 - BitLocker (Windows 標準の暗号機能)
 - FileVault 2 (Mac OS 標準の暗号機能)
 - TCG OPAL (自己暗号化ドライブ)
- リムーバブルメディア暗号**
 - メディア全体を強制的に暗号化あるいはメディアの一部を暗号化
 - SecureDocがインストールされているPCでファイルを開くことが可能
 - SecureDocがインストールされていないPCでは、パスワードを入力することでファイルを開くことが可能
- 共有ファイル・フォルダ暗号**
 - ユーザーの操作無しに自動的に確実に暗号化
 - SecureDocの有無とSecureDocによる権限管理によって重要なファイルを保護
- クラウドストレージに保存するファイルを暗号化 SecureDoc CloudSync**
 - クラウドストレージに保存するファイルを暗号化
 - 鍵の共有化により、暗号化されたファイルも共有可能
- 仮想マシンをフルディスク暗号化 SecureDoc CloudVM**
 - 暗号化と起動制御でデータがどこにあっても情報漏えいを防止
 - パブリック、プライベート、ハイブリッドいずれのクラウド環境にも対応

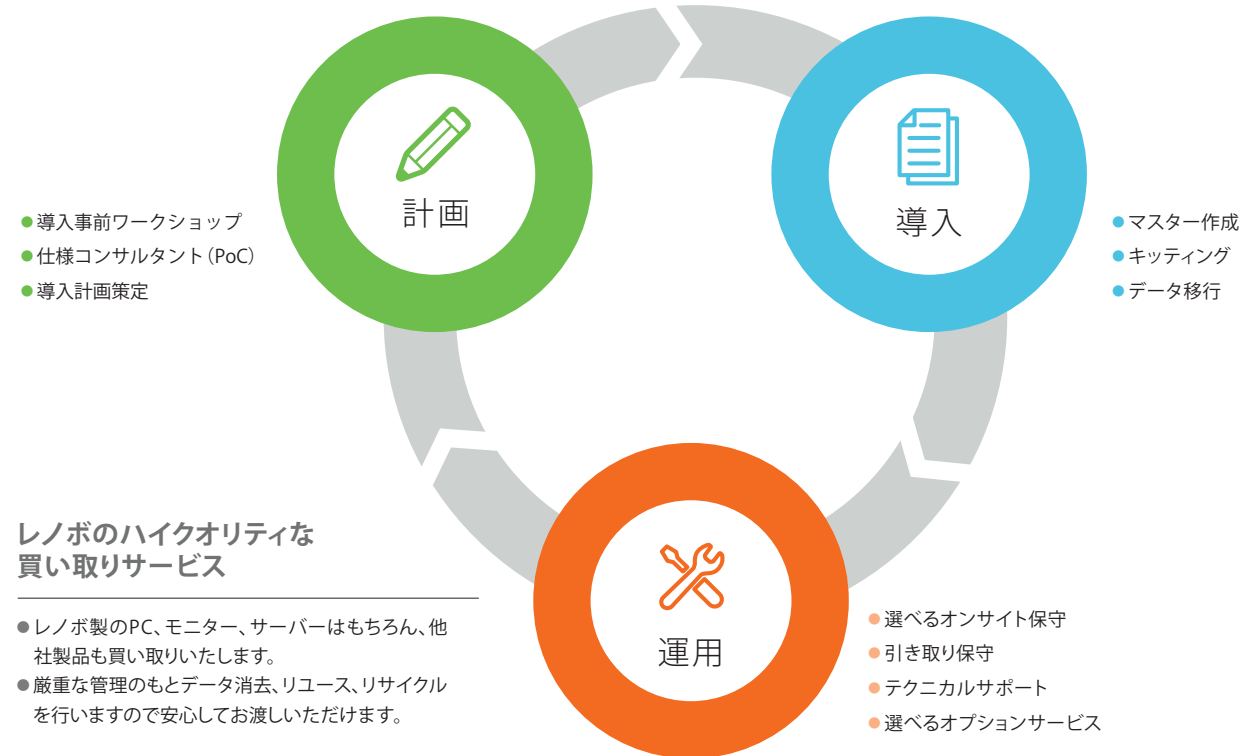
SecureDocの販売に関する情報

製品名	製品内容	ライセンス	年間保守	
SecureDoc Enterprise Lenovo Client	・フルディスク暗号と管理サーバーによる管理 ・リムーバブルメディア暗号	¥ 14,500/1台	¥ 4,000/1台	※初回購入時の最少購入数:10
SecureDoc Standalone For Windows	・スタンドアロンでのフルディスク暗号 ・リムーバブルメディア暗号	¥ 15,500/1台	¥ 4,000/1台	
File Folder Encryption	共有ファイルの暗号化	¥ 7,500/1台	¥ 2,000/1台	※SecureDoc Enterprise Lenovo Client のオプション
SecureDoc CloudSync for Lenovo	クラウドストレージのファイルの暗号化	¥ 2,500/1台	¥ 1,000/1台	※SecureDoc Enterprise Lenovo Client のオプション
SecureDoc CloudVM	仮想マシンのフルディスク暗号	¥ 48,000/1VM		※年間サブスクリプションライセンス
Onsite Installation and Consulting	管理サーバー構築支援サービス (任意)	¥ 400,000/1日		※標準サービス内容は2日間 (¥ 800,000) で提供

導入計画段階からサポートしてほしい!

ライフサイクルに沿った、
トータルサポートを提供します。

レノボはすべてのお客様が安心して製品をご利用いただけるよう、計画から運用、リサイクルまでのライフサイクルに沿って安心のサポートサービスメニューを揃えています。



レノボのハイクオリティな
買い取りサービス

- レノボ製のPC、モニター、サーバーはもちろん、他社製品も買い取りいたします。
- 厳重な管理のもとデータ消去、リユース、リサイクルを行いますので安心してお渡しいただけます。

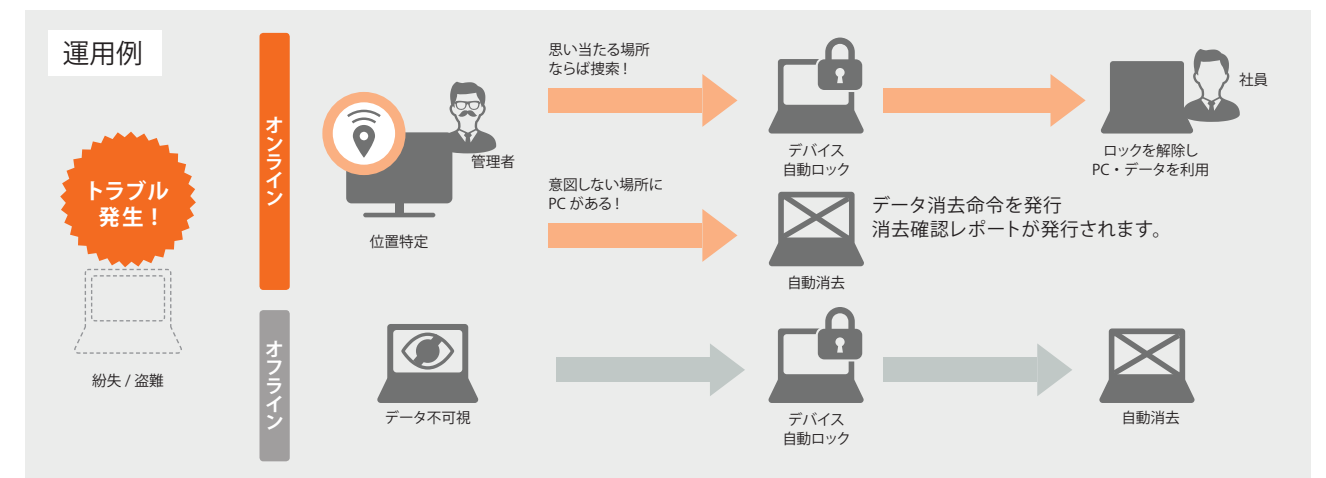
Windows 10 移行サービス詳細

フェイズ	実施項目	内容
計画	導入事前ワークショップ	Windows 10管理の必要知識をご説明します。 ・Windows 10の新機能、Windows as a Service (WaaS) の概念のご説明 ・移行の際の留意事項のご説明
	仕様コンサル(PoC)	お客様の導入後のイメージをヒアリング、要件定義を策定します。 ・Windows 10の導入イメージの摺り合わせ ・導入要件定義
	導入計画策定	要件定義に基づき、導入スケジュールを策定します。 ・展開計画策定 ・更新計画策定
導入	マスター作成	イメージファイルのマスターを作成します。
	キットティング	PC配布後、すぐに使い始められるよう、初期設定を行います。 周辺機器セット、IPアドレス・BIOS・HDDパスワード設定、管理ラベルの作成・貼付なども承ります。
	データ移行	最適なデータの移行方法を提案します。

遠隔データ消去サービス

パソコンの紛失・盗難に備えた情報漏えい対策サービスです。万一、パソコンの盗難や紛失が起きた場合に、サーバーに消去指示を送り、漏えいしたり、見られたら困るデータを遠隔から消去することができます。

遠隔データ消去 PCからサーバーに消去指示を送り、対象データを消去	不可視化 対象PCがインターネットに接続していない場合、データを不可視化	自動データ消去 管理サーバーへの認証が一定期間ない場合、設定していたデータを自動消去	デバイスロック 一定時間インターネットに接続しない場合、入力デバイスなどを無効化	位置情報取得 PCの位置情報をGPSまたは無線LANのアクセス情報を利用して取得可能



オンサイト記憶メディアデータ消去・物理破壊サービス

出張訪問にてデータを消去します。高いセキュリティを求められるお客様に最適です。ソフトを利用したデータ消去から、物理的な破壊まで4種類の対応が提供可能です。

データセキュリティポリシーに合わせた4種類の消去方法

- 1 Blancco社製データ消去ソフト (3回上書き+1 米国防総省規格DoD方式)**
企業や組織で使われる様々なIT資産の消去に対応したデータ消去ソフトです。記憶媒体の全領域に対して、新たな(無意味な)データを上書きすることで記憶媒体に蓄積されたデータを、参照(復元や読み取り)できない状態にすることができます。また、セキュリティ要件に合わせて、最適な消去方式を選択することができます。
- 2 電磁破壊 (18,000 Gauss電磁波)**
- 3 4ピン(HDD)・40ピン(SSD) 加圧穿孔物理破壊 (3t, 5t加圧)**
- 4 シュレッド物理破砕 (2-40mm)**

● お客様立会いのもとデータ破壊作業を実施するため、確実な作業実施が確認可能
● 万が一の輸送中の事故や盗難などによるデータ漏えいリスクが軽減
● データ破壊にともなう証明書もご用意

ランサムウェアとは?

Ransom (身代金)とWare (製品)の合成語で、ユーザーのコンピュータに不正にインストールされて、ユーザーのドキュメントなどを暗号化してお金を要求するマルウェアの一つです。



マルウェアに感染したWebサイトを訪問するか、ランサムウェアが添付されたスパムメールをクリックすると、感染



コンピュータシステムまたはデータファイルを暗号化して、ユーザーのアクセス不可



身代金 (Ransom) を要求するか、ファイルを永久に利用不可にする

ランサム ディフェンダーとは

ランサムディフェンダーは、その名の通りランサムウェア対策専門のセキュリティソフトです。

ランサムウェアの流入→実行→ファイル暗号化などが行われる前に、複数の防御システムで事前に検知して防御します。ウイルスソフトだけでは防ぎきれない未知のランサムウェアも行為の検出時に自動的に元のファイルをバックアップして、データを保護します。ほとんどのウイルス対策ソフトと一緒にパソコン上で使用可能です。



1. マルウェア検査

ファイルのダウンロード・コピー・実行時に検査



2. おとりファイル診断

暗号化やファイル名変更プログラムをおとりファイルで診断



3. ふるまい検知

ウイルスの行動から攻撃を検知



4. 指定フォルダの保護

ソフトも保護フォルダで防御

バックアップと復元でファイルを保護します



自動バックアップ

ランサムウェアの攻撃によりファイルの変更が発生したときに、ファイルが暗号化される前に元のファイルを自動的にバックアップしてデータを保護



自動復元

おとりファイルへのランサムウェア行為を検出したときに、自動的にバックアップした元データとランサムウェアによって書き換えられたデータを照合した後、変更される前のデータに復元可能

問い合わせ先は裏表紙

※こちらに掲載しているサービスは、レノボグループのNECパーソナルコンピュータが販売するサービスです。販売、サービスについてのお問い合わせは、冊子裏にあるNECパーソナルコンピュータへ直接お問い合わせください。

その他の情報漏えい対策サービス



個人情報・マイナンバー 検出ソフト

個人情報が含まれたファイルを検出し、暗号化や抹消することができます。

- PC内に保存された個人情報を含むファイルを検出
- 検出したファイルを暗号化や抹消することが可能
- ゴミ箱から削除したファイルの検出も可能



リモートアクセス サービス

外出先や自宅から、会社PCへカンタン・セキュアにアクセスできます。

- とにかく速い。目の前のPCを操作しているようなスピード感
- 導入も利用もカンタン
- 豊富なセキュリティ対策機能。大手金融機関・官公庁でも活用中なため安心

レノボのセキュリティ製品

Lenovo Security and Privacy

「外出先における情報保護」、「PCやモニターの盗難対策」、「データの保護」に絞って、その課題解決をレノボがご支援させていただきます。

セキュア ハードドライブ



シンプルで安全なポータブルハードドライブが欲しい!

ソフトウェアをインストールする必要がなく、お客様の大切なデータを保護します。



データをすべて暗号化し、保護します。使用にあたりソフトウェアをインストールする必要がなく、企業での大規模データの安全な受け渡しに最適です。USBポートにつなぎ、暗証番号を入力するだけでデータへのアクセスが可能。

ThinkPad USB3.0 500GB
セキュアハードドライブ 0A65619

ThinkPad USB3.0 1TB
セキュアハードドライブ 0A65621

ThinkPad USB3.0 2TB
セキュアハードドライブ 4XB0K83868



Lenovo 4TB
セキュア デスクトップ ハードドライブ
4XB0M13792

Lenovo 8TB
セキュア デスクトップ ハードドライブ
4XB0M13808



Kensington ケーブル・ロック



PCやモニターの紛失・盗難が心配!

盗難に対する抑止力として物理的なケーブル・ロックをお勧めします。



ケーブル・ロックはオフィス、学校や図書館、研究所などでの物理的なセキュリティ・マネージメントを可能にします。ケーブル・ロックによる盗難の減少と、ノートブックパソコンやドッキングステーション、デスクトップやモニター製品の資産保護に役立ちます。また最新のLenovo KensingtonマイクロセーバーDSケーブルロックでは薄型のヘッドを採用、Ultrabookや薄型パソコンにも違和感なくフィットするようにデザインされており、施錠/解錠も容易です。ケーブルは強靱な炭素鋼を用いています。

Lenovo Kensington マイクロセーバーDSケーブルロック 0B47388
Lenovo Kensington ツインヘッド・セキュリティー・ケーブル 45K1620
Kensington コンビネーション ケーブル・ロック 4XE0G97138

※上記以外にも多数ご用意しています。詳細はレノボまでお問い合わせください。



ThinkPad/ThinkVision専用 プライバシーフィルター



のぞき見による情報漏えいが心配!

のぞき込み防止にはプライバシーフィルターの装着が有効です。



個人情報保護法により、プライバシーを取り扱う業務に、情報管理の大きな責任が発生しています。個人データの宝庫で、意外と漏えい源になりやすいパソコン画面の情報もしっかり管理する必要があります。3M独自の内蔵マイクロルーバーの働きにより、正面以外からの視線を遮り、左右からの「のぞき見」を防止。不特定多数が出入りする官公庁や企業、窓口業務などで、画面情報の漏えいを防止します。

タブレット ThinkPad X1 Tablet ノート ThinkPad ディスプレイ ThinkVision デスクトップ All-in-One

※各種画面サイズのフィルターも多数ご用意しています。詳細はレノボまでお問い合わせください。

