もっと豊かな情報未来へ
アルシー・ソリューション

情報漏洩対策シリーズ

InterSafe ILP ver.8.2

「インターセーフ アイエルピー」

ファイル自動暗号化 ―― InterSafe FileProtection
デバイス制御 ―― InterSafe DeviceControl
ファイル転送 ―― InterSafe FileTransporter
簡易インターネット分離 ―― InterSafe SecureSwitch
セキュリティUSBメモリ作成 ―― InterSafe SecureDevice
申請・承認ワークフロー ―― InterSafe WorkFlow
ファイル無害化 ―― InterSafe FileSanitizer
Powered by OPSWAT
個人情報検出 ―― InterSafe PIS

- 自治体セキュリティ強靭化対応
- 教育情報セキュリティガイドライン対応
- ネットワーク分離対応
- テレワーク対応
- クラウド対応
- 仮想化（VDI/SBC）対応

https://www.alsi.co.jp/

情報漏洩の脅威が拡大するなか、個人情報管理の強化はすべての組織において最重要課題となっています。

ランサムウェア攻撃による被害の増加、高まる個人情報管理の必要性

ランサムウェアは、民間企業だけでなく、医療や金融、自治体など、あらゆる業界が標的となり被害が増加。働く場所や利用端末が多様化し感染リスクが高まっている今、情報を保護することは重要課題です。しかし一方、個人データのセキュリティ問題は、2022年4月より施行された「改正個人情報保護法」や2018年5月に施行された「EU一般データ保護規則（GDPR）」など、国内外で厳しい規制と罰則が策定。対策の必要性はますます高まっています。

■情報セキュリティ10大脅威 2023

順位	「組織」向け脅威	昨年順位
1	**ランサムウェアによる被害**	1
2	サプライチェーンの弱点を悪用した攻撃	3
3	**標的型攻撃による機密情報の窃取**	2
4	**内部不正による情報漏えい**	5
5	**テレワーク等のニューノーマルな働き方を狙った攻撃**	4
6	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	7
7	ビジネスメール詐欺による金銭被害	8
8	脆弱性対策情報の公開に伴う悪用増加	6
9	**不注意による情報漏えい等の被害**	10
10	犯罪のビジネス化（アンダーグラウンドサービス）	NEW!

出典：独立行政法人情報処理推進機構「情報セキュリティ10大脅威 2023」

■改正個人情報保護法

個人情報を取り扱う**すべての企業が対象**。特に、漏洩時報告義務化や罰則規定が強化されたため、**大きな損害や企業の信頼低下を生まないためにも**適切な対応が求められる。

本人の権利保護強化	・短期保有データの保有個人データ化 ・保有個人データの開示請求のデジタル化 ・利用停止・消去請求権、三者への提供禁止請求権の要件緩和 ・個人データの授受についての第三者提供記録の開示請求権
事業者の責務追加	・**漏洩時の報告義務（個人情報保護委員会・本人）** ・不適正な利用の禁止
企業の特定分野を対象とする認定団体制度の新設	・「事業の種類その他業務の範囲」に限定した個人情報との取扱いを対象とする団体を認定
データの利活用を促進	・「仮名加工情報」について事業者の義務を緩和 ・提供先で個人データとなることが想定される場合の確認義務を新設
法令違反に対するペナルティ強化	・措置命令・報告義務違反の罰則について法定刑を引き上げ **→ 行為者に対して1年以下の懲役又は100万円以下の罰金** ・法人に対する罰金刑を引き上げ **→ 法人に対して1億円以下の罰金**
外国の事業者に対する罰則追加	・日本国内にある者に係る個人情報などを取り扱う外国の事業者も、罰則によって担保された報告徴収・命令および立入検査などの対象

■EU一般データ保護規則（GDPR）

日本企業がGDPRの適用対象となるケース
①EEAに子会社、支店、営業所がある企業
②日本からEEAに商品、サービスを提供している企業
③EEAから個人データの処理について委託を受けている企業

制裁金の上限額	業務違反の一例
企業の**全世界年間売上高の2%**または**1,000万ユーロ**のいずれか高い方　［第83条（4）］	リスクに対する適切なセキュリティレベルを保証する適切な技術的・組織的な対策を実施しなかった場合　［第32条］
企業の**全世界年間売上高の4%**または**2,000万ユーロ**のいずれか高い方　［第83条（5）］	適法に個人データを処理しなかった場合　［第6条］

※EU:EU加盟国及び欧州経済領域（EEA）の一部であるアイスランド、ノルウェー、リヒテンシュタイン ※GDPR:General Data Protection Regulation

INTERSAFE ILP

約900,000ライセンスの導入実績

CLOUD マークの製品は、クラウド版もご用意しています

InterSafe ILPは、「情報の持出し・持込み制御」と「持出し後の安全の担保」ができる、多層的な情報漏洩対策のためのソリューション。以下の機能を、単体でも組み合わせでも、自社のセキュリティポリシーにあわせて自由に導入できます。

基本機能（選択）

InterSafe FileProtection
［ファイル自動暗号化］
ストレージ等、多様な環境に対応。
ドライバレベルでの高い運用性。SBC仮想環境に対応。

InterSafe DeviceControl
［デバイス制御］
多様なデバイスのきめ細かな利用制御。
ワークフローやセキュアデバイスと連携。

InterSafe FileTransporter
［ファイル転送］
異なるネットワーク間でのファイル転送。
ファイル転送時の申請／承認・暗号化・無害化。

InterSafe SecureSwitch
［簡易インターネット分離］
簡易的なネットワーク分離環境を実現。
デスクトップ毎のネットワーク接続切替。

InterSafe SecureDevice Ultimate
［セキュリティUSBメモリ作成］
汎用USBメモリをセキュアなUSBメモリに変換。
ソフトウェアによる柔軟な制御。

拡張機能

InterSafe WorkFlow
［申請・承認ワークフロー］
書出し／持込み／ファイル暗号解除・テンプレート変更。
申請・承認履歴の保存と原本管理ファイル書出し時の自動暗号化。

InterSafe FileSanitizer Powered by OPSWAT
［ファイル無害化］
持込みファイルをCDR（コンテンツ非武装化／再構築）技術で無害化。
30種類以上のアンチマルウェアエンジンを搭載。

InterSafe PIS
［個人情報検出］
サーバーやクライアントPC内の個人情報・マイナンバー情報を検出し暗号化。
暗号化ファイル内の情報も検出可能。

共通機能

管理サーバー機能
共通コンソールでの一元管理
リアルタイムでのポリシー適用

クライアント機能
共通エージェントで各種機能提供
オフラインでの制御を実現
自己復号型暗号、パスワードzip作成

ログ管理機能
操作ログのリアルタイム収集
外部利用USBメモリの操作ログ
不正操作のアラート通知

※InterSafe ILPは上記製品の総称です。※InterSafe SecureSwitchにはInterSafe DeviceControlの機能が含まれています。

情報漏洩対策に合わせ、単一製品での使用はもちろん、製品を組み合わせて使用することができます。

製品の追加はライセンスの入力のみで完了。クライアントソフトを追加インストールする必要はありません。

■例えばこんなデータ管理 1

デバイスへの書出しを制御。書出す場合はWebで申請、上長が承認した場合のみ書出し可能に。

DeviceControl ＋ WorkFlow

■例えばこんなデータ管理 2

デバイスへの書出しを制御。書出す際は、ファイルを自動暗号化。書出したファイルはサーバーにアーカイブ。

DeviceControl ＋ WorkFlow ＋ クイック書出し

■例えばこんなデータ管理 3

デバイスへの書出しを制御。書出す場合はセキュリティが確保されたUSBメモリのみ可能に。

DeviceControl ＋ SecureDevice Ultimate

■例えばこんなデータ管理 4

ファイルを暗号化して情報を保護。外部に送信する場合はWebで申請、上長が承認した場合のみ暗号解除、セキュアファイルに変換。

FileProtection ＋ WorkFlow

InterSafe FileProtection CLOUD

「インターセーフ ファイルプロテクション」

ファイルを保存した時点で自動的に暗号化&アクセス制御。
不正に持出されても解読できないため、情報が漏洩しません。

ユーザーへ負担をかけない2つの自動暗号化方式

■ファイル保存時に自動暗号化

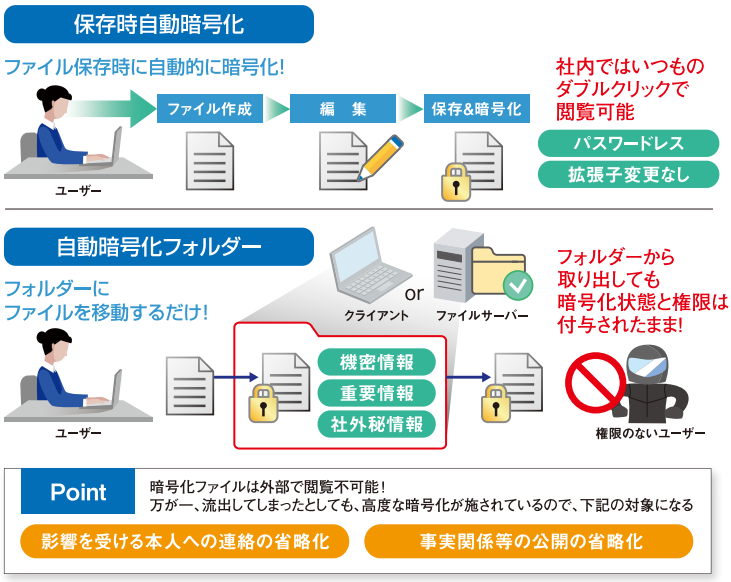
あらかじめ設定したアプリケーションでは、暗号化されていないファイルを開いたり、保存した際に自動的に暗号化します。特別な操作が不要で、ファイル名・ファイル形式もそのまま。ユーザー、管理者ともに従来と操作が一切変わりません。自動暗号化の設定をしていない場合でも右クリックで簡単に暗号化可能です。

■フォルダーに移動で自動暗号化

自動暗号化フォルダーは、ファイルを特定のフォルダーに移動するだけで自動で暗号化することができます。

※共有フォルダーのみオプション

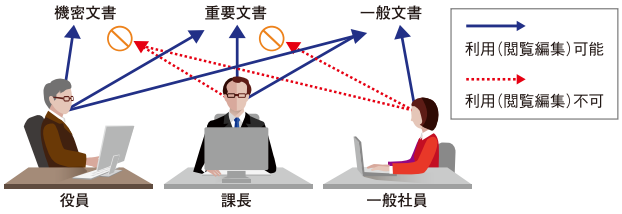
動作確認済み 暗号化対象 アプリケーション	Microsoft Word / Excel / PowerPoint （2016, 2019, 2021） Microsoft メモ帳 / ワードパッド / ペイント Adobe Acrobat Reader DC 一太郎Pro4 AutoCAD / Windows Media Player （2023年2月現在）



※「個人データの漏えい等の事案が発生した場合等の対応について」（平成29年個人情報保護委員会告示第1号）

アクセス権限設定

InterSafe FileProtectionでは独自にユーザー属性を利用者に設定し、ユーザー属性とアクセス権限を紐づけてファイルを暗号化します。



ユーザー属性とアクセス権を紐づけた閲覧権限（テンプレート）が、暗号化の際にファイル毎に適用されます。

機密文書 | 重要文書 | 一般文書

ユーザー属性	閲覧	編集	暗号解除	コピー	印刷	権限変更
役員	許可	許可	許可	許可	許可	許可
管理職	許可	許可	不可	不可	不可	不可
社員	不可	不可	不可	不可	不可	不可

※クライアント端末にて有効期限の設定も可能　　テンプレート例

暗号化したままウイルス検知・全文検索

業界初、暗号化されたファイルは復号することなくウイルスの検閲・駆除、隔離を行うことができます。また、Windows Searchによるコンテンツ検索も可能です。

ウイルス検知イメージ

コンテンツ検索イメージ

【ウイルス検知動作確認済みアプリ】
※Trend Micro Apex One Ver 14.0.11136　※Symantec Endpoint Protection Ver 14.3.9205.6000　※ESET PROTECT Entry Ver 9.1.2060.1
※McAfee MVISION（McAfeeSmart）Ver 5.7.8.262　※Windows Defender Ver 4.18.2211.5
※お客様環境における全ての正常動作を保証するものではありません。またサーバーOSは動作対象外となります。

自動バックアップによるランサムウェア対策

ファイルを保存（暗号化）した時点で自動的にセキュリティフォルダーにバックアップファイルを保存します。セキュリティフォルダーに保存されたファイルは、専用ツールを利用しないとアクセスができないため、**万一ランサムウェアに感染した場合でも、バックアップファイルを安全に保護し、確実に感染前の状態に復元することができます。**

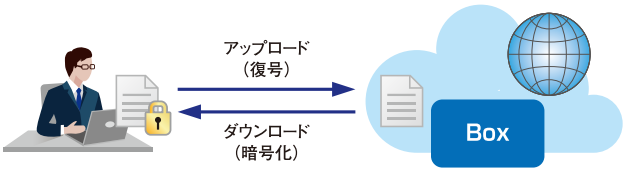
次世代型暗号化エンジンで高速処理化

フィルターモジュール内でオリジナル／暗号ファイルデータを分離して管理・処理することで、多様な環境に対応。SBC環境や大規模ストレージ、様々な資産管理／総合ログ管理製品との高い親和性により、幅広い環境でのセキュリティ強化を実現します。

［動作確認済ストレージ/HCI 環境］
- Microsoft Windows Server
- Microsoft Windows Storage Server
- NetApp FASシリーズ（ONTAP）
- QNAP NAS（QTS／QES）
- Nutanix NXシリーズ

クラウドストレージからダウンロードしたファイルを自動暗号化

ファイル共有サービスのBoxと連携し、ファイルをダウンロード時に自動暗号化することで、社内環境に持込んだタイミングで安全性を確保することが可能です。ダウンロード／アップロードでの暗号化／復号は設定変更可能で、故意の漏洩、不正アクセス、共有リンク通知の誤送信にも対応することができます。



INTERSAFE DeviceControl

InterSafe DeviceControl CLOUD

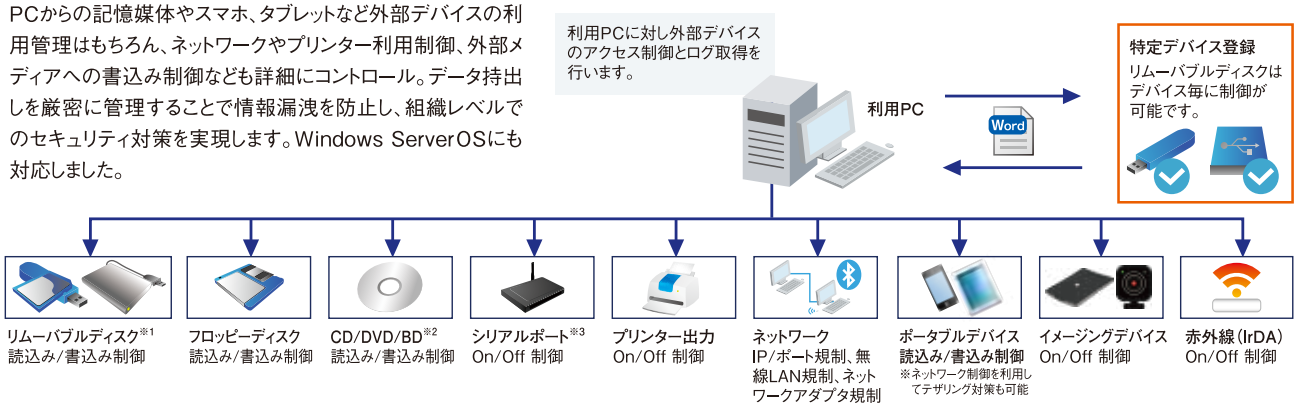
「インターセーフ デバイスコントロール」

業界最多の制御デバイス数!
2022年9月現在

PCから外部デバイスへのアクセス制御とログ取得を実現。
メディアへのコピーやプリントアウトによる不正持出しを防ぎます。

デバイスの制御

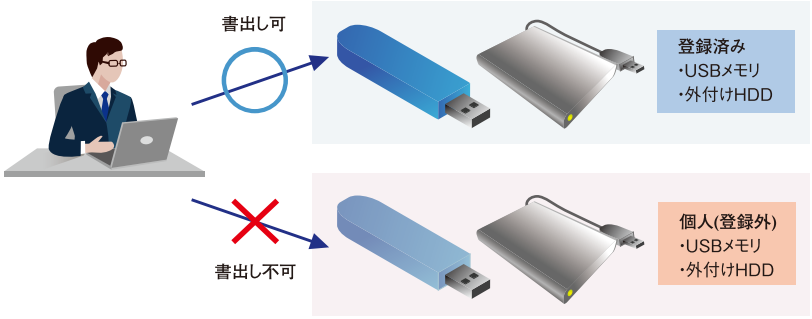
PCからの記憶媒体やスマホ、タブレットなど外部デバイスの利用管理はもちろん、ネットワークやプリンター利用制御、外部メディアへの書込み制御なども詳細にコントロール。データ持出しを厳密に管理することで情報漏洩を防止し、組織レベルでのセキュリティ対策を実現します。Windows ServerOSにも対応しました。



※1:USBメモリやHDD、SDカード、MOなどWindowsがリムーバブルディスクとして認識するメディア。　※2:Blu-ray Disc　※3:モデム等の利用に使われます。

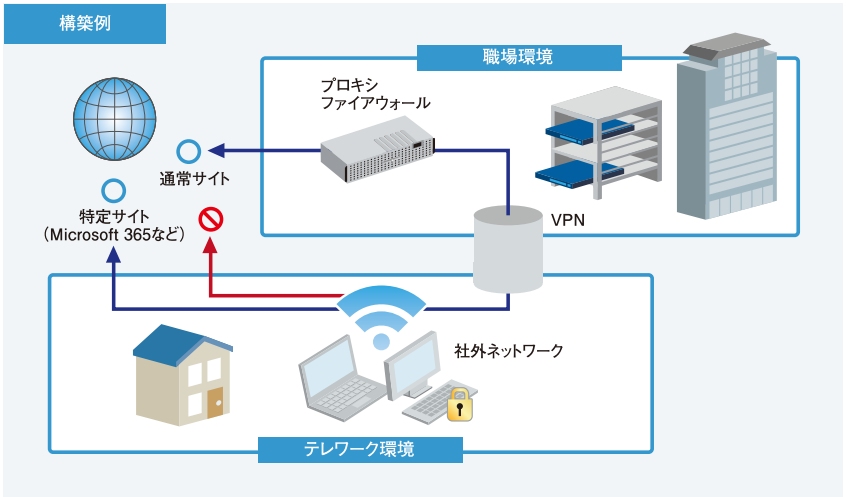
私物USBメモリや外付けハードディスクの利用禁止

あらかじめ登録したUSBメモリ、外付けハードディスク(HDD)のみ書出しを許可する、といった設定が可能。**個人で持込んだUSBメモリや外付けハードディスクを使用させない運用ができます。**
また、業務上必要な、取引先などから持込まれた社外のUSBメモリをILPシステムに登録したうえで、読み取り専用モードで利用することもできます。



社外ネットワーク接続環境でVPN利用を強制

社外ネットワーク接続環境ではVPN利用を強制。VPNスプリットトンネリングの技術などを用いて、特定のサイトのみ直接インターネットへ接続させることができます。テレワーク等の社外環境でのネットワークセキュリティを強化します。



INTERSAFE WorkFlow

InterSafe WorkFlow

「インターセーフ ワークフロー」

データを書出す、持込む場合は、Web上で簡単申請・承認。
厳格な管理と運用負荷の低減を両立します。

外部デバイス利用申請・承認

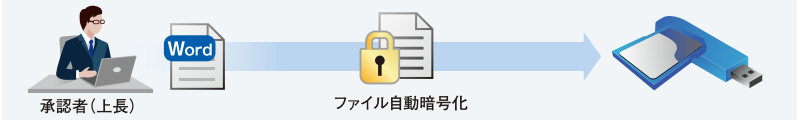
InterSafe DeviceControlで制御されている外部デバイスを、本機能により一時的に利用することができます。
申請時に利用期間を設定すると、**期間終了時には自動的にデバイス制御が再開されるため、システム管理者の手を煩わすことのない運用が可能です。**

ファイル書出し／持込みの申請・承認

InterSafe DeviceControlで外部デバイスが制御されている場合でも、申請し承認が得られればファイル単位での書出しが可能となります。申請者は書出したいファイルを右クリックし申請、上長はファイルの中身を確認した上で承認・却下の判断を行います。承認されたファイルのみ書出し可能で、光学メディアへの書出し時もライティングソフトに依存することなく、ファイル単位に制御します。書出し可能な期間や回数を設定することも可能。承認者が自ら書出す場合は、申請・承認プロセスを簡素化することもできます（クイック書出し）。
ファイルの持込み申請・承認にも対応。USBメモリや外部ネットワークからの不正なファイル持込みを防ぐことができます。

■通常のファイル書出し申請・承認

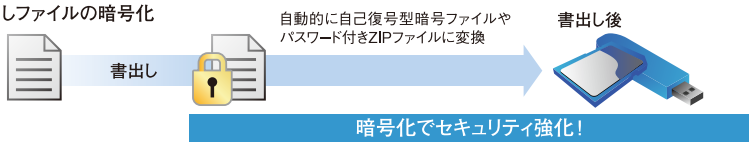
■クイック書出し時（オプション）



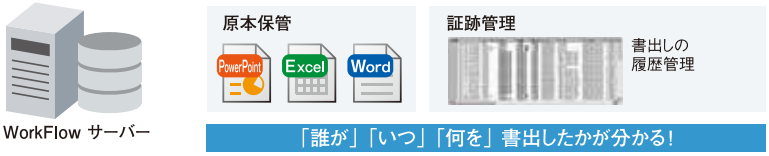
ファイル書出し後のセキュリティ

承認されたファイルをリムーバブルディスクなどに保存するタイミングで、**自動的に自己復号型暗号ファイルやパスワード付きZIPファイルに変換**。書出し後のセキュリティを強化します。
書出したファイルの履歴（ログ）管理だけでなく、書出したファイル自体もサーバー上に保存されるため、「誰が」「いつ」「何を」書出したか、履歴の確認が可能です。

■書出しファイルの暗号化

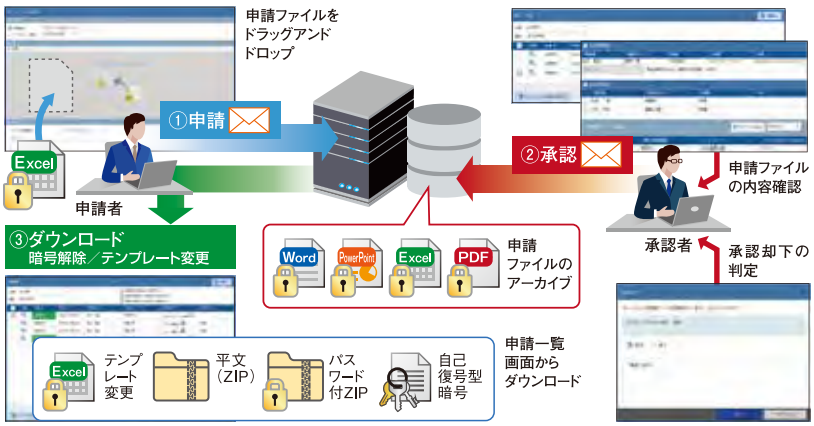


■書出しファイルの原本保管と履歴管理



ファイル暗号解除の申請・承認

InterSafe FileProtectionで暗号解除権限を付与されていない場合でも、申請し承認が得られれば、ファイル単位で暗号解除やテンプレート変更が可能となります。申請・承認したファイルの履歴や原本は保存されるため、一時的に取引先にファイルを送信したい場合にも安全かつ柔軟な対応を実現します。



INTERSAFE FileTransporter

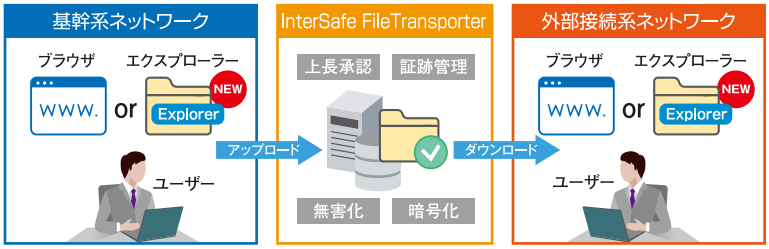
InterSafe FileTransporter

「インターセーフ ファイルトランスポーター」

異なるネットワーク間でファイル授受。
上長承認や暗号化で安全性を強固にします。

ファイル転送

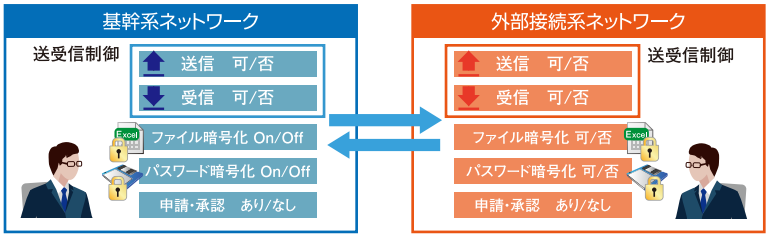
ネットワーク間でのファイル転送をブラウザからエージェントレスに実施。上長承認や暗号化機能を搭載し、ファイル無害化製品やデバイス制御製品と組み合わせることで利便性と安全性をさらに強化します。
また、「自動無害化フォルダー」機能により、指定のフォルダーにファイルを保管するだけで、ファイルを無害化し転送できます。ユーザーはアップロードやダウンロード、申請承認の操作を省け、個人からグループへの転送も容易にできます。



※基幹系ネットワーク⇔外部接続系ネットワークの双方向でご利用可能です。

ユーザー毎・ネットワーク別の柔軟なポリシー

グループ・ユーザー毎にデータ受渡しの方向性指定、暗号化、申請・承認等、柔軟なポリシー制御が可能です。またそれぞれのネットワークで異なる設定を付与することもできます。



他製品と組み合わせ

■ファイル持込み時のウイルス感染を防止

InterSafe FileSanitizer Powered by OPSWATと連携することで、外部からのファイル持込み時に自動で無害化・マルチスキャンを実施。申請時にルール選択可能で、通常のルールでは承認まで自動化。「マクロを削除しないルール」では、マクロを残したまま無害化・マルチスキャンを実施し、承認者チェックを行います。(図1)

■ファイル持出し時の個人情報漏洩を防止

InterSafe PISと連携することで、内部からのファイル持出し時に対象ファイル内の個人情報やマイナンバー情報の有無を自動チェック。ファイルに個人情報やマイナンバー情報が含まれていない場合は自動で承認され、含まれていた場合には申請を自動で却下、または、承認者によるチェックを行います。(図2)

その他にも、InterSafe DeviceControl・InterSafe WorkFlowと併用することで、ユーザーはファイル転送と外部デバイスによるファイル受渡しの双方を利用可能となり、申請／承認履歴を1つの管理画面から確認できます。
InterSafe FileProtectionと連携することで、基幹系ネットワークではファイルを暗号化した状態で保持し、外部接続系ネットワークへ転送する場合に自動で復号可能です。万が一、別の方法で外部接続系ネットワークへ持出しされても、閲覧することができません。(図3)

図1

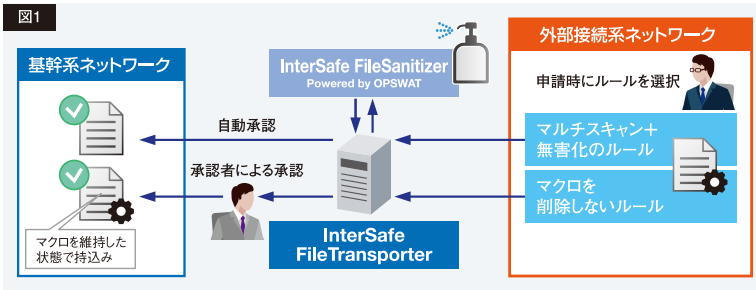


図2

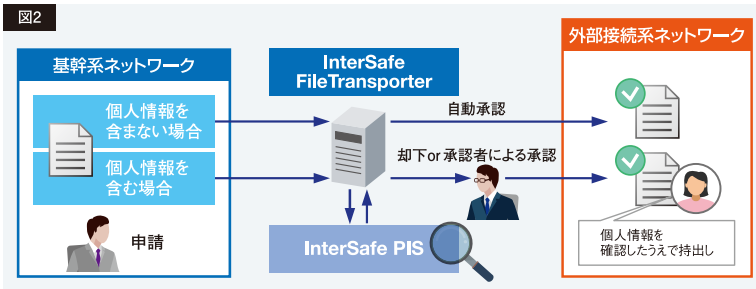
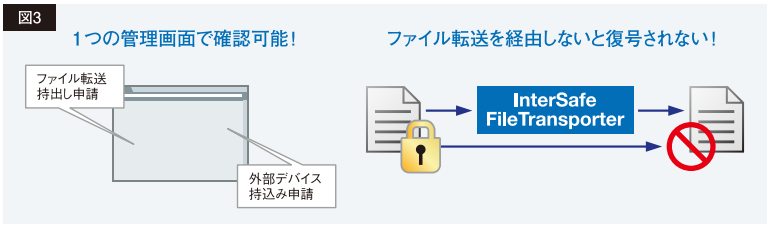


図3



INTERSAFE FileSanitizer Powered by OPSWAT

InterSafe FileSanitizer Powered by OPSWAT

「インターセーフ ファイルサニタイザー パワード バイ オプスワット」

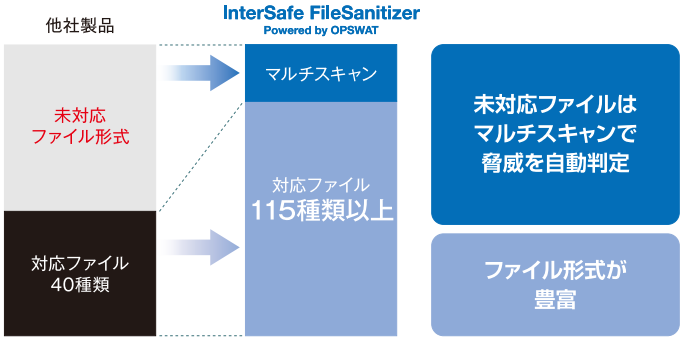
多様なファイル形式に対応したファイル無害化と、複数のアンチマルウェアエンジンを搭載。
外部ファイル経由の脅威を防御します。

複数の防御機能を搭載

■ファイル無害化（Deep CDR）

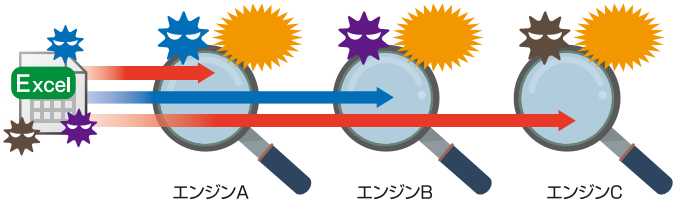
ファイル内の脅威となり得るマクロやリンクを削除・無効化したうえで、安全なコンテンツを再構築。ユーザビリティを損なうことなくファイルを無害化できます。他のファイル無害化製品は対応ファイルが40種類程度と言われていますが、本製品は、Officeファイルだけでなく、画像ファイルなど115種類以上※のファイル形式に対応可能です。また未対応ファイルについては下記マルチスキャン機能を使って複数のアンチウイルスエンジンでチェックをかけることで、脅威の有無を自動判定します。

※2022年4月現在

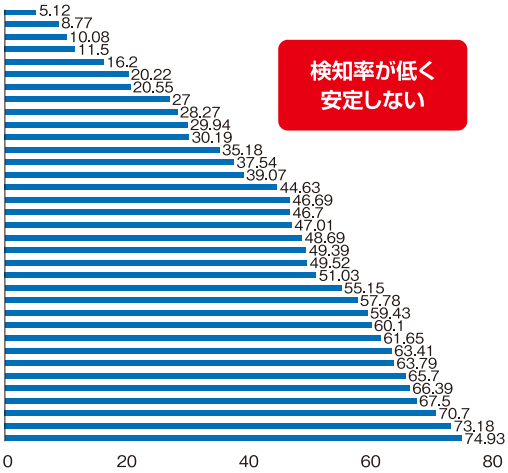


■マルチスキャン

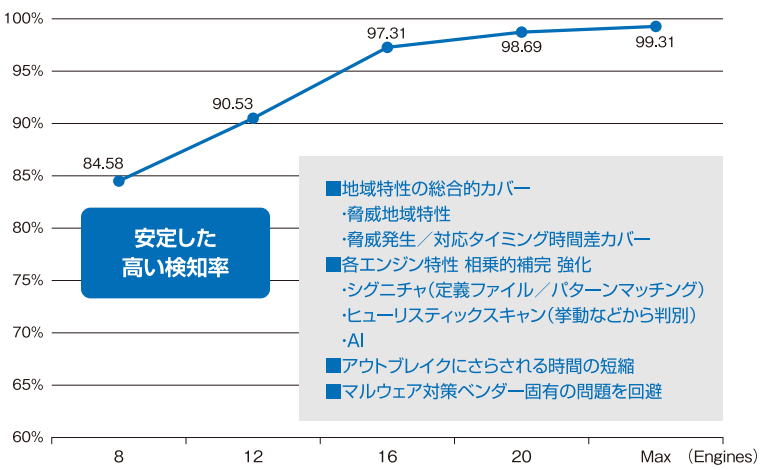
単一エンジンでのスキャンでは、高くても約75%ほどしか脅威を検知することができません。しかし、本製品なら30種類を超える実績あるアンチマルウェアエンジンのシグネチャ、ヒューリスティック、機械学習によって、マルウェアの99%※以上を検知。既知・未知の外部脅威から徹底的に防御します。利用するエンジンは柔軟なパッケージオプションから選択いただけます。



■単一エンジン検知率



■Top 10,000脅威 検知率



※任意の80個の脅威をスキャンを行い、各エンジンの単一検知結果を表しています。※OPSWAT社調べ。

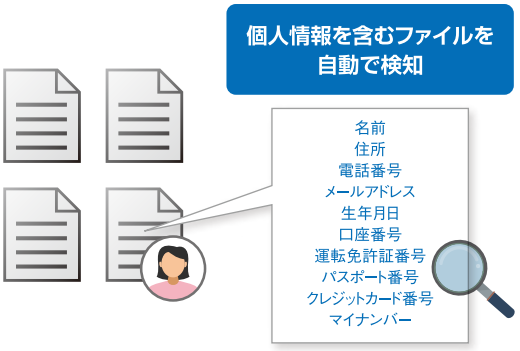
InterSafe PIS (Personal Information Search)

「インターセーフ ピーアイエス」

サーバーやクライアントPC内から個人情報・マイナンバー情報を含むファイルを検出。
機密情報を漏れなく保護します。

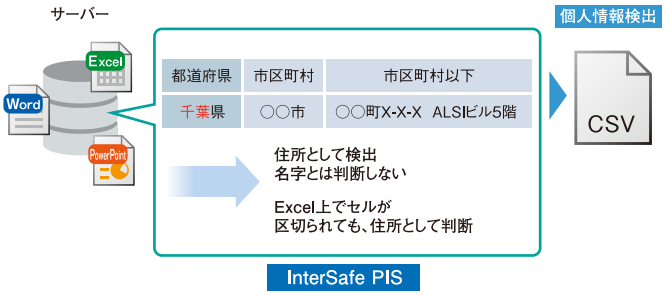
個人情報を含むファイルを検出

InterSafe PISは個人情報や機密情報をファイルの中身までくまなくチェックします。住所や名前だけでなくマイナンバー情報も自動で検出。InterSafe FileProtectionやInterSafe FileTransporterなどと連携することで、外部への流出を未然に防ぎ、内部の情報を常に暗号化で保護することができます。



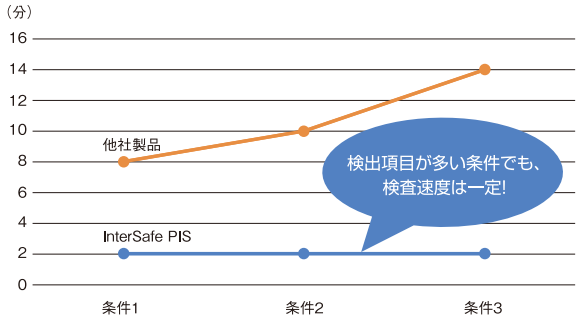
高い検査精度

24種類のデータベースを元に個人情報を検出。特に名字と住所の検出精度が高く、例えば、「千葉県」のように「千葉」という名字が含まれる住所でも、住所と名字は区別して判断します。また、Excelで住所が県、市区町村などで区切られている場合でも、住所として正確に検出できます。



圧倒的な速さで個人情報を検出

ファイルサーバー内の個人情報を含むファイルの検出までをスピーディーに行うことができます。また、検出項目を増やしても検査速度が変わることはありません。



ビジネスで多用されるファイル形式に対応

Officeファイルや PDFなどビジネスシーンで欠かせないファイル形式に対応しています。

■検査可能なファイル形式

Windows 版 Microsoft Word 97 / 98 / 2000 / 2002(XP) / 2003 / 2007 / 2010 / 2013 / 2016 / 2019 / 2021
Windows 版 Microsoft Excel 97 / 2000 / 2002(XP) / 2003 / 2007 / 2010 / 2013 / 2016 / 2019 / 2021
Windows 版 Microsoft PowerPoint 97 / 2000 / 2002(XP) / 2003 / 2007 / 2010 / 2013 / 2016 / 2019 / 2021
Adobe Systems Acrobat (PDF) 4.0 / 5.0 / 6.0 / 7.0 / 8.0 / 9.0 / X / XI / DC / 2017
ODF 1.1 / 1.2(ワープロ、表計算、プレゼンテーション)※
一太郎　V7-V13 / 2004-2021(JFWファイル、JTDファイル)
圧縮ファイル(zip, lha, tar, tgz, 7z)　通常10階層まで展開して検査
eml(Outlook、Thunderbirdのメールファイル)※

※InterSafe FileProtecitonサポート外(連携対象外)アプリケーションです。InterSafe FileProtectionのサポート対象バージョンは別途ご確認ください。

INTERSAFE ILP

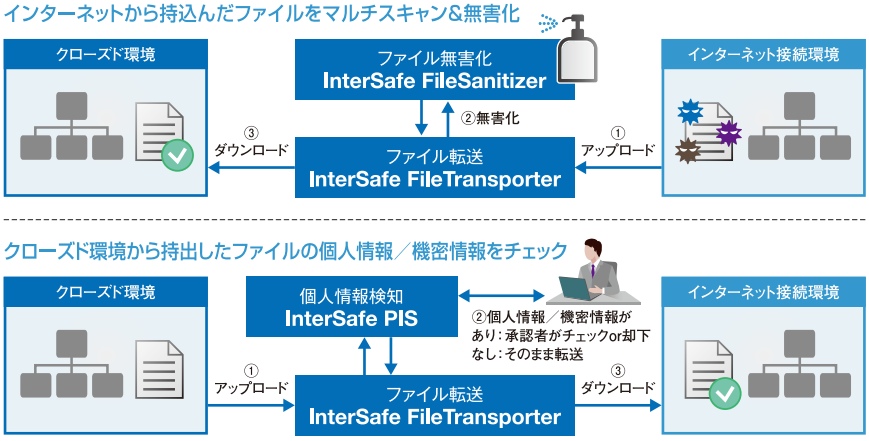
おすすめパッケージ

自社のセキュリティポリシーにあわせて様々な組み合わせが可能なInterSafe ILP。
目的別に、3つのおすすめパッケージをご用意しています。

ファイル転送を利用した受渡しなら…

ファイル無害化転送パック

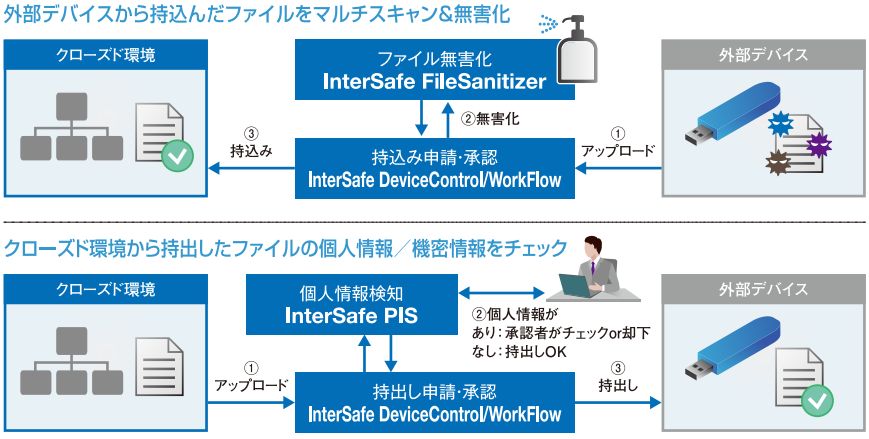
ネットワーク間のファイル転送時に、ファイル無害化や個人情報検出と連携。クローズド環境へ持込むファイルに脅威が含まれていても、無害化することで安全に持込むことができます。反対にインターネット接続環境に持出すファイルに個人情報が含まれていても、個人情報検出後に承認者のチェック、または申請を却下することで情報漏洩を未然に防ぎます。



外部デバイスを利用した持出し／持込みなら…

デバイス無害化管理パック

外部デバイスを利用したファイル書出し申請の際に、ファイル無害化や個人情報検出と連携。外部からの資料をUSBメモリを利用して持込む際に、無害化することで安全に持込むことができます。反対に内部の資料を外部へ持出す際、個人情報検出後に承認者のチェック、または申請を却下することで情報漏洩を未然に防ぎます。

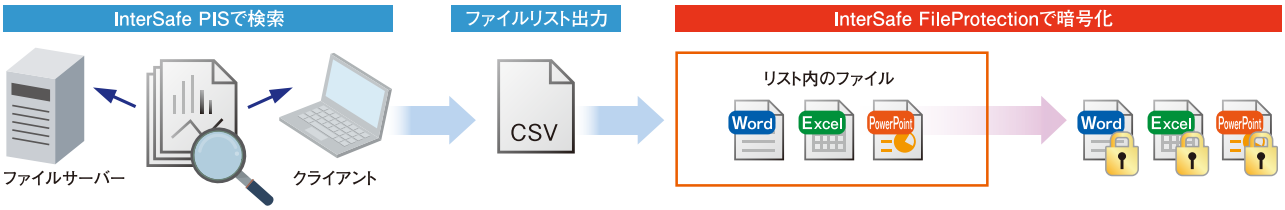


個人情報やマイナンバー情報を強固に守りたいなら…

個人情報暗号化パック

ファイルサーバーやクライアントPCの中に保存されたファイルに、個人情報が含まれていないか一つ一つ確認するのは現実的ではありません。個人情報検出オプションとファイル暗号化が連携することで、簡単かつ強固なセキュリティを実現します。検索対象エリアのファイルの中身までチェック。個人情報やマイナンバーが含まれるファイルを検出し、一括で暗号化することができます。

本オプションツールによって、ファイル検出→暗号化完了までシームレスに実行されます。



INTERSAFE SecureSwitch

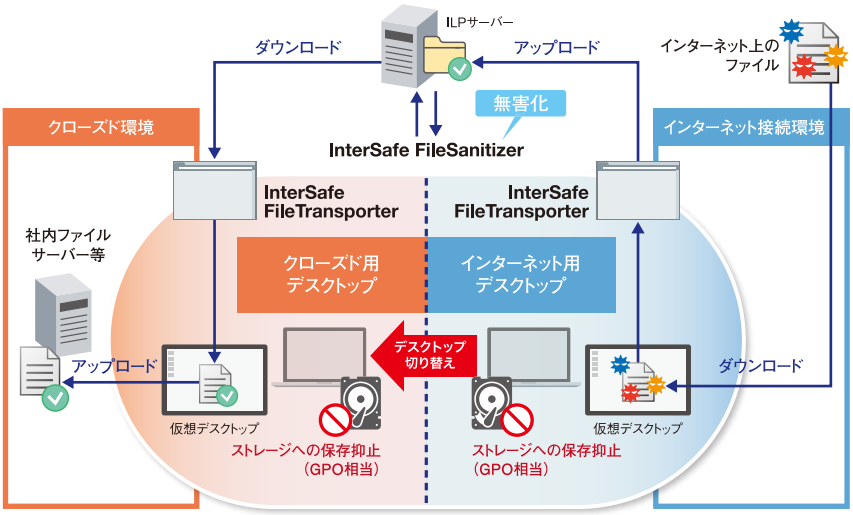
InterSafe SecureSwitch CLOUD

「インターセーフ セキュアスイッチ」

デスクトップをワンタッチで切替。
簡易にネットワークを分離します。

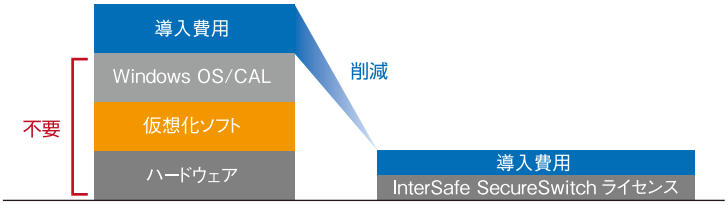
デスクトップ切替でネットワークを分離

インターネット用デスクトップとクローズド用デスクトップを作成し、ワンタッチでネットワークを切り替えできます。ローカルドライブへの保存抑止やUSBメモリ制御、ネットワーク制御の機能を標準搭載しているため、1台のPCでネットワーク分離を簡易に実現します。また、デスクトップ切り替え時に任意のスクリプトを実行できるため、プロキシ・IPアドレス設定の変更や、ファイルサーバーのマウントなどのネットワーク関連の設定も実施できます。
InterSafe FileTransporterと連携し、一時作業領域を利用することで、ローカルドライブへの保存抑止をしていても、インターネットからのダウンロードファイルをクローズド環境へ転送可能です。ファイル無害化やマルチスキャン、個人情報チェックとも連携することで、安全なファイル受渡し環境を実現します。



低コストでネットワークセキュリティを強化

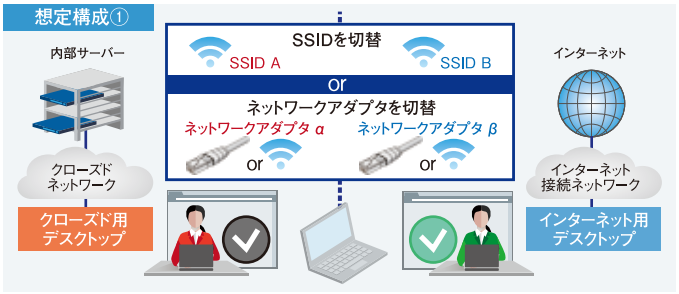
VDIや物理分離によるネットワーク分離は導入費用に加えて、Windows OS／CALや仮想化ソフト、ハードウェアなどが必要ですが、InterSafe SecureSwitchは導入費用とライセンス費用のみで導入いただくことが可能です。



ネットワーク環境に応じた構成

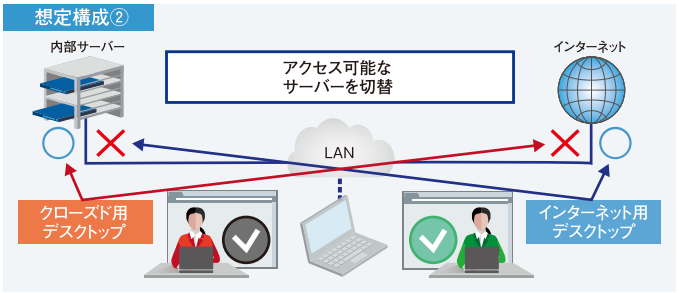
■ネットワークが物理的に分かれている場合の構成

ネットワークが物理的に分かれている場合、SSIDまたはネットワークアダプタを切り替えることで、接続先ネットワークを制御します。



■ネットワークが物理的につながっている場合の構成

ネットワークが物理的につながっている場合、アクセス可能なサーバーを切り替えることで、アクセス先を制御します。



※InterSafe SecureSwitchにはInterSafe DeviceControlの機能が含まれています。

INTERSAFE SecureDevice

InterSafe SecureDevice Ultimate CLOUD

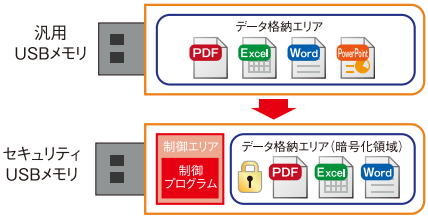
「インターセーフ セキュアデバイス アルティメイト」

現在使用中のUSBメモリをセキュリティUSBメモリに変換。
小さなコストで大きなセキュリティを実現します。

多彩なセキュリティ機能

汎用USBメモリをセキュリティUSBメモリに変換できるだけでなく、変換時に、セキュリティモードを選択できます。セキュリティモードは5種類（オリジナルの設定も可能）。使用目的やポリシーに応じて、最適なセキュリティUSBメモリが作成できます。
ハードウェアタイプのセキュリティUSBメモリと違い、普通のUSBメモリに戻したり、ライセンスを他のUSBメモリに再利用したりすることも可能です。

USBメモリの有効期限の設定も可能
有効期限後はデータの解読不能

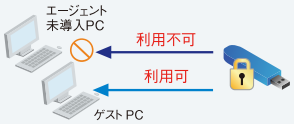


パスワードモード

盗難、紛失時にもパスワードによる認証でデータを保護します。

社外利用禁止モード

InterSafe Clientが未導入の社外のPCでは、暗号化USBメモリを利用させません。



ウイルス対策モード

自宅等に持ち帰った場合にも、自宅PCへデータのコピー、移動ができないため情報漏洩を防ぐことが可能です。さらに、PCからUSBメモリへのデータコピー、移動も不可のため、ウイルスの侵入を防止します。

USBメモリ内で編集・保存は可能

情報漏洩対策モード

自宅等に持ち帰った場合にも、自宅PCへデータのコピー、移動ができないため情報漏洩を防ぐことが可能です。

USBメモリ内で編集・保存は可能

読み取り専用モード

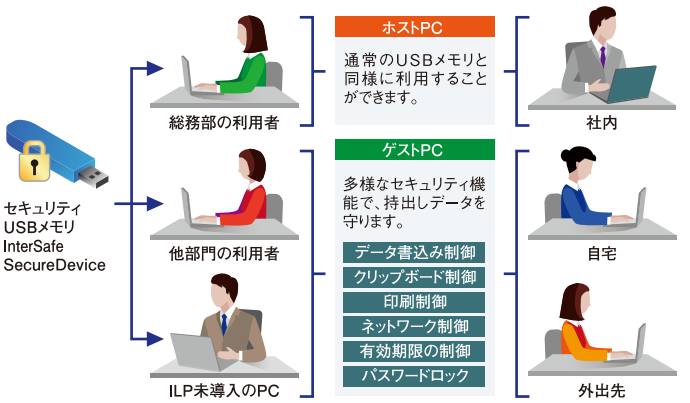
USBメモリへの書込み不可のためウイルスの侵入を防止します。また、USBメモリ内のファイル編集も不可のため、原本が変更されることはありません。

ホストPCとゲストPC

セキュリティUSBメモリに変換時、USBメモリごとに使用するユーザーやグループを登録できます。登録したユーザーやグループが使用する場合には「ホストPC」として動作。通常のUSBメモリと同様に利用できます。**登録ユーザー／グループ以外の人が使用する場合は「ゲストPC」として動作、セキュリティUSBメモリとして、設定されたセキュリティモードでの使用に制限**されます※。
また、**クライアントソフト未導入PCでは、セキュリティUSBメモリの利用自体を禁止することも可能**です。

※ユーザー権限では動作しません。事前にドライバーソフトをAdmin権限でインストールする必要があります。暗号化されたUSBメモリには、アプリケーションを問わず保存できますが、動作確認済みのアプリケーションは、下記の通りです。

動作確認済み アプリケーション	Microsoft Word / Excel / PowerPoint（2016, 2019, 2021） Microsoft メモ帳 / ペイント Adobe Acrobat Reader DC 一太郎Pro4 （2023年2月現在）



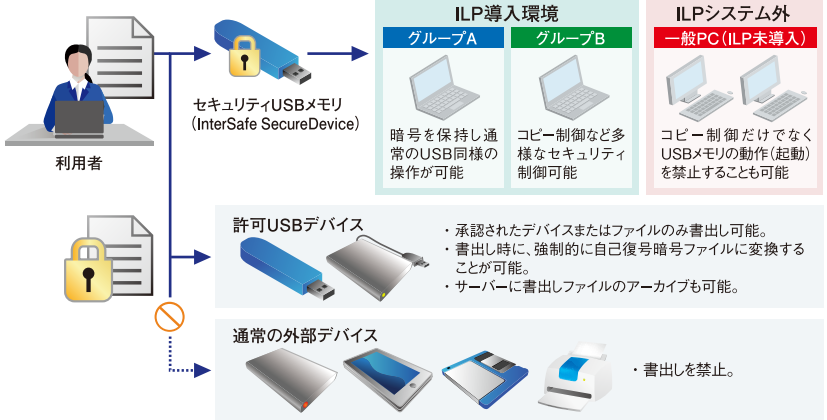
・総務部では通常のUSBメモリと同等に動作。
・他部門ではセキュリティUSBメモリとして動作。

<利用例>

・社内のPCでは通常のUSBメモリと同様に動作。
・自宅や社外PCではセキュリティUSBメモリとして動作。

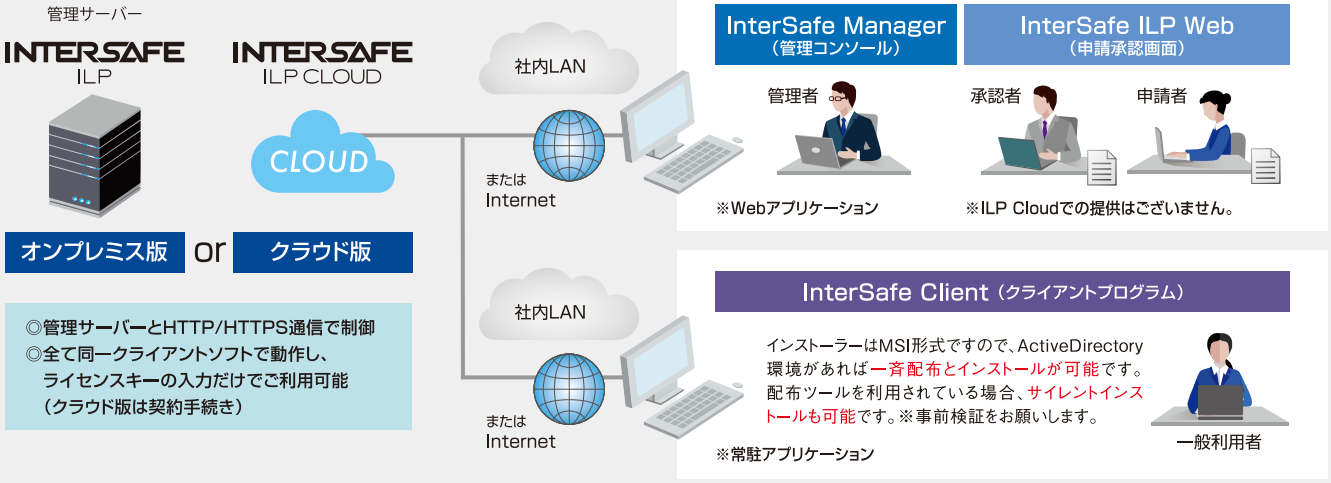
持出し対策の強化

InterSafe DeviceControl、InterSafe WorkFlowと組み合わせてご利用いただくことで、さらなる持出し対策強化が可能です。
通常の外部デバイスへの書出しを禁止し、**InterSafe SecureDevice Ultimateで暗号化したUSBメモリであれば、書出しが可能です。**
その他のデバイスの場合、承認されたデバイス、ファイルのみ書出すことができます。

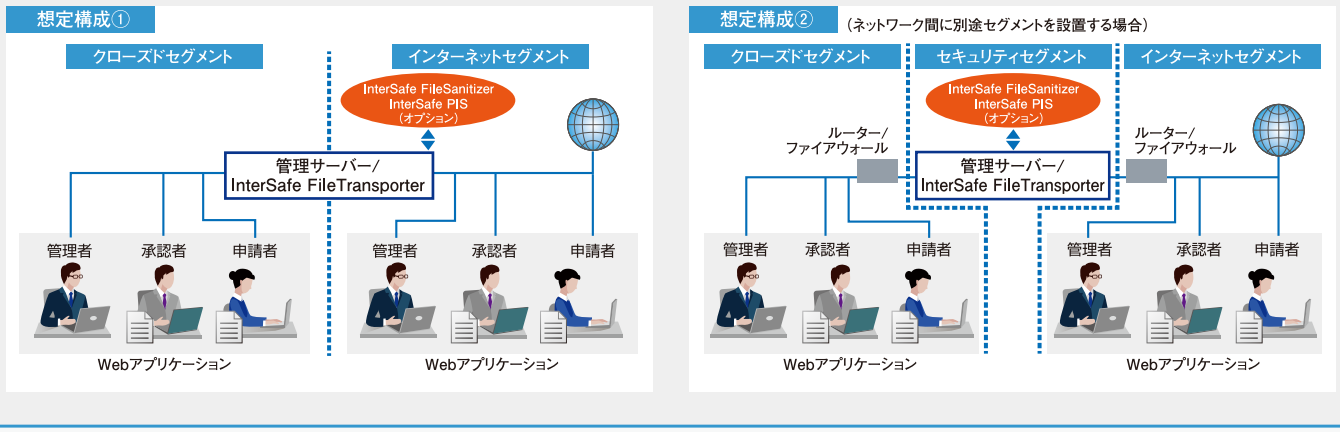


InterSafe ILPのシステム構成

InterSafe ILPは、自社システムに合わせて、オンプレミス版、クラウド版をお選びいただけます。



InterSafe FileTransporterのシステム構成



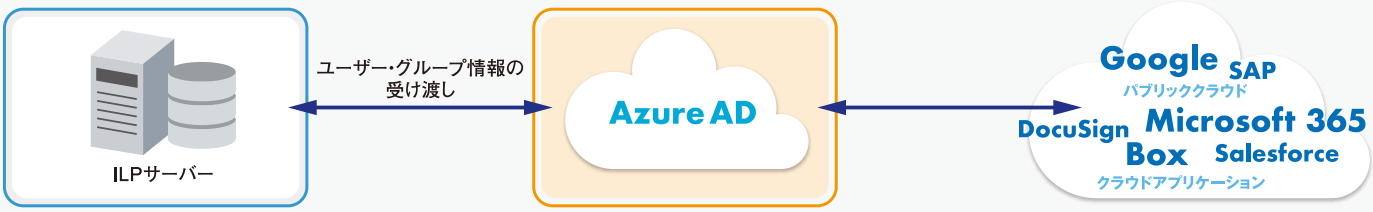
スタンドアロン管理

サーバーに接続できない環境（スタンドアロン）にあるPCに対しても、クライアントソフト／専用ツールを導入し、サーバーに接続しているPCと同様にポリシー適用やログ収集が可能です。

InterSafe FileProtection
InterSafe DeviceControl
InterSafe SecureDevice Ultimate

InterSafe ILPをクラウド環境へ。セキュリティ向上、導入期間も大幅に短縮。

AWS（Amazon Web Service）やWindows Azureなどのクラウドプラットフォームに対応。
Azure ADと連携し、各種クラウドアプリケーションとILPとでユーザー情報を一元管理することが可能です。



※Azure ADとの連携はILPサーバーをAzure等のクラウド基盤上に構築する場合を想定しています。

■こんな企業・法人様におすすめ！

○Web環境の安全性を向上させながら、脆弱性対策コストを軽減したい
○クラウドへのシステム移行を検討中

■ILPお試しクラウドで、まずは簡単・安全の実感を！

面倒な準備なしにすぐに試用、30日間の「ILPお試しクラウド」をご利用ください。

ILPお試しクラウド　検 索

機能概要一覧

機能概要		
情報漏洩対策	ファイル作成	自己復号型暗号ファイル / パスワード付き ZIPファイル作成
	デバイス制御	外部デバイス規制（リムーバブルディスク、光学メディアなど）
	DeviceControl	ポータブルデバイス制御
		イメージングデバイス制御
		イメージングデバイスの例外設定（USB カメラ、Web スキャナー）
		例外 USB の読み取り専用利用
		登録済み USB メモリ制御
		プリンター出力制御
		ネットワーク規制
		ユーザー / グループ単位の制御
		FireEyeとの連携による感染端末の隔離（自動 / 手動）
	申請・承認ワークフロー WorkFlow	申請・承認（デバイス利用 / ファイル書出し・持込み / ファイル暗号解除・テンプレート変更）
		ファイル書出し時の暗号化と原本保存
		ファイル書出し強制暗号（クイック書出し）※オプション
	セキュリティ USB メモリ作成 SecureDevice Ultimate	汎用 USB メモリをセキュリティ USB メモリへ変換
		USB メモリの暗号化
		USB メモリのパスワード設定
		USB メモリのコピーガード機能設定
		USB メモリ利用時の印刷規制、クリップボード制御
		USB メモリへのウイルス侵入防止機能
	ファイル自動暗号化	パスワード不要なファイル単位の暗号化
		暗号化ファイルへのウイルススキャン・全文検索対応
		セキュリティフォルダーへの自動バックアップ
	FileProtection	ファイル単位のアクセス制御 （閲覧、編集、暗号解除、コピー、印刷、 権限変更、有効期限）
		暗号化対象外フォルダーの設定
		自動暗号化フォルダー機能 （ローカルフォルダー / 共有フォルダー） ※共有フォルダーのみオプション

機能概要		
情報漏洩対策	ファイル転送 FileTransporter	ネットワーク間のファイル転送
		ファイル転送時の申請・承認
		ファイル転送時の暗号化 （別途FileProtectionのライセンスが必要です）
		ファイル転送時の無害化 （別途FileSanitizerのライセンスが必要です）
		ファイル転送時の個人情報検出 （別途PISのライセンスが必要です）
		自動無害化フォルダー機能
	簡易インターネット分離 SecureSwitch	接続ネットワークの切替
		外部デバイス利用制御
		HDDへの保存禁止
		一時作業領域の利用
		許可プロセスの指定
	ファイル無害化 FileSanitizer	ファイルの無害化（Deep CDR）
		マルチスキャン
	個人情報検出 PIS	個人情報を含むファイルの検出
運用管理支援	管理機能 全製品	ポリシー管理機能
		グループ管理者設定
		クライアントモジュールのバージョン管理機能
		ログ管理機能（検索・アラートなど）
		Windows Update 制御機能
		人事連携
		クライアントインストーラーの不正利用防止機能
	FileProtection DeviceControl SecureDevice Ultimate	サーバーに接続できない環境（スタンドアロン）にある PCに対するポリシー適用やログ収集※オプション
	WorkFlow FileTransporter	InterSafe Client未導入端末からの承認管理画面 ログイン（マルチデバイスでの承認操作） ログインパスワード / ID、アクセスURLのメール一括配信 ダウンロード期限切れファイルの自動削除 ファイル保護機能

ライセンス料金

■オンプレミス版

※InterSafe FileSanitizer Powered by OPSWATはオープン価格です。

ライセンス数 ＼ 製品名	InterSafe FileProtection ※SBC版を含む	InterSafe SecureDevice Ultimate	InterSafe DeviceControl	InterSafe WorkFlow	InterSafe FileTransporter（クライアントライセンス）
5-99	¥8,040	¥3,840	¥2,400	¥1,440	¥3,000
100-499	¥7,440	¥3,720	¥2,160	¥1,380	¥2,160
500-999	¥7,440	¥3,480	¥1,920	¥1,260	¥1,560
1000 以上	別途お問い合わせください				

ライセンス数 ＼ 製品名	InterSafe SecureSwitch	InterSafe PIS（クライアントライセンス）	クイック書出しオプション	自動暗号化フォルダーオプション		自動無害化フォルダーオプション
				共有フォルダー	for NetApp	
5-99	¥4,200	¥3,960	¥660	¥80,400	¥264,000	¥264,000
100-499	¥3,840	¥3,840	¥660			
500-999	¥3,600	¥3,180	¥600			
1000 以上	別途お問い合わせください					

■クラウド版

ライセンス数 ＼ サービス名	InterSafe DeviceControl Cloud	InterSafe SecureDevice Cloud	InterSafe FileProtection Cloud ※SBC版含む	InterSafe SecureSwitch Cloud
Basic Pack	¥300,000	¥300,000	¥600,000	¥420,000
51-（クライアント）	¥6,000	¥6,000	¥12,000	¥8,400

※記載の価格は1端末あたりの税抜き価格（年額）です。月額ライセンスについては別途お問い合わせください。※FAT端末においては、インストールした物理端末数でカウントします。クライアント仮想化（VDI方式／SBC方式）においては、インストールした仮想化クライアント環境へアクセスする物理端末数の総数にてカウントします。

オンプレミス版

※新規ご購入時の最低購入数は5ライセンス（InterSafe PISのみ20ライセンス）です。追加のご購入は1ライセンスから可能です。※同一の管理サーバーにて複数の製品をご利用の場合、クライアントライセンスは全製品同数の購入が必要です。※ガバメントライセンス、アカデミックライセンスもご用意しています。詳細は、別途お問い合わせください。

クラウド版

※BasicPackは50クライアントまでご利用可能な一律価格となります。51クライアント以上でご利用の場合は、ライセンス単価×クライアント数の購入が必要です。※InterSafe ILP Cloudには、セットライセンス、ガバメントライセンス、アカデミックライセンスはございません。※オンプレミス版にて提供されているInterSafe WorkFlow、FileTransporter、PIS、FileSanitizer Powered by OPSWAT、クイック書出しオプションは本クラウド版ではご利用になれません。※InterSafe FileProtection Cloudを購入いただくと、自動暗号化フォルダー・SDK機能、スタンドアロン管理オプションをご利用になれます。

動作環境

	OS	CPU	メモリ	ブラウザ
ILPサーバー （オンプレミス版）	・Microsoft Windows Server 2016 Standard / Datacenter Edition ・Microsoft Windows Server 2019 Standard / Datacenter Edition ・Microsoft Windows Server 2022 Standard / Datacenter Edition ※日本語 OS のみ対応	Intel Xeon 2.1GHz（4Core）以上 ※Intel Xeon 2.5GHz（6Core）以上推奨	4GB 以上 ※8GB 以上推奨	
クライアント導入PC※1 （InterSafe Client導入PC）	・Microsoft Windows 10 Pro / Enterprise LTSC1809 / LTSC21H2 / SAC21H1 / SAC21H2 / SAC22H2 ・Microsoft Windows 11 Pro / Enterprise SAC21H2 / SAC22H2 ※日本語 / 英語 / 中国語（簡体）［多言語は Client OS のみ］	Intel Core i3 2.0GHz 以上	2GB 以上 ※4GB 以上推奨	Microsoft Edge / Google Chrome
FileProtection for SBC	・Microsoft Windows Server 2016 Standard / Datacenter Edition（LTSC） ・Microsoft Windows Server 2019 Standard / Datacenter Edition（LTSC） ・Microsoft Windows Server 2022 Standard / Datacenter Edition（LTSC） ※日本語 OS のみ対応	Intel Xeon 2.1GHz（4Core）以上 ※Intel Xeon 2.5GHz（6Core）以上推奨	32GB 以上 ※64GB 以上推奨	
クライアント未導入PC	・Microsoft Windows 10 Home / Pro / Enterprise ・Microsoft Windows 11 Home / Pro / Enterprise ※32 / 64bit 対応 ※日本語 / 英語 / 中国語（簡体）OS 対応	Intel Core i3 2.0GHz以上	2GB 以上 ※4GB 以上推奨	

	VMware	Citrix
仮想環境（VDI）	VMware Horizon View ※2	Citrix Virtual Desktops ※2

	Windows
仮想環境（SBC）	Remote Desktop Services ※3

※1：InterSafe Client（常駐型プログラム）をインストールしたPC。
※2：対応バージョンおよび制限事項等は別途お問い合わせください。
※3：InterSafe FileProtection for SBCが対象です。
※自己復号型暗号ファイルの動作環境については、クライアント導入PCの動作環境に準じます。
※Windows10およびWindows11サービシングモデルの対応状況は、弊社FAQサイトをご確認ください。 https://alsifaq.dga.jp/
※InterSafe SecureSwitch / DeviceControlは、すべてのデバイスに対する制御を保証するものではありません。
※InterSafe SecureDevice UltimateをゲストPCでご利用になる場合は、事前にドライバソフトをAdmin権限でインストールする必要があります。
※InterSafe ILP のご利用には、Microsoft .NET Framework 4.8およびMicrosoft Visual C++ 2015-2019 Redistributable Package 14.32.30135 以降が必要です。
※Windows 10 / 11のストアアプリ、タブレットモードには対応しておりません。
※仮想環境（SBC）は、MicrosoftのRemote Desktop Servicesが稼働する環境で利用します。
※利用される際は目安としてメーカーリリース後3年以内のハードウェア（HW）をご利用ください。旧式のHWをご利用される際は十分なパフォーマンスが得られない可能性がありますので、予めご注意ください。
※InterSafe FileTransporterについては、上記OS以外でも転送・承認等のブラウザで操作する機能はご利用になれます。

注意：本製品は暗号化機能を実装しているため、中国等、日本国外でご利用になる場合は、利用申請・許可が必要な場合があります。ご利用にあたっては、予め各国の法規制をご確認ください。

製品に関するお問い合わせは各営業所までお願いいたします。

アルプス システム インテグレーション株式会社

本　　社　〒145-0067　東京都大田区雪谷大塚町1-7
TEL：03-5499-8045　FAX：03-5499-0357
東京営業所・古川営業所・仙台営業所・いわき営業所・
名古屋営業所・大阪営業所・福岡営業所・白金台オフィス

https://www.alsi.co.jp/　E-mail：ssg@alsi.co.jp
※ALSI（アルシー）はアルプス システム インテグレーション株式会社のコミュニケーションブランドです

お問い合わせ、ご用命は下記へお申し付けください

23.02.ILP.2500