情報漏洩防止対策セキュリティソフト

セキュリティプラットフォーム(SeP)

セキュリティプラットフォーム (SeP) コンセプト

一本で全局面に対応できる唯一の純国産セキュリティソフトウェア

情報漏洩対策・エンドポイントセキュリティ・内部統制ソリューション

SeP は、あらゆる経路からの情報漏洩や様々な不正から企業を守ります。社内ルールを変えず、自動的に行われるセキュリティのため、社員に意識させることなく確実に情報を守ります。最強の網羅性で業務を監視・制御・記録できる SeP の特長が時代の要請に応えます。

SeP の４つの機能

自動暗号化機能（エンドポイントセキュリティ）

社外へデータを持ち出す操作を全て検知し、自動的に暗号化＆復号。USB メモリや外付け HDD、CD-R、スマートフォンのような外部媒体や、インターネット、メールなどのネットワーク経由でも同じように暗号化処理を施します。

ディフェンス機能（サイバー攻撃対策）

既知のウイルス、未知のウイルス、マルウェア、標的型攻撃、フィッシングなどの、あらゆるサイバー攻撃から PC を完全に防御します。

Write 制限機能（エンドポイントセキュリティ）

あらゆるアプリケーションによる、インターネットなどの通信や、全てのファイルに対しての「書き込み・通信（Write）」を完全にシャットアウトします。

履歴機能（エンドポイントセキュリティ・サイバー攻撃対策）

全 PC の全操作・プログラムの動きを記録します。イベントログ収集のような不可解なものではありません。全業務のトレーサビリティを完全に確保します。

企業・官公庁を不正から守るトータルソリューション

最新AI搭載セキュリティでクラウド、仮想環境、メール、周辺機器、盗難や印刷対策まで全リスクに対応

クラウドやメールなどのインターネット、DVD、CD、USBメモリなどの周辺機器、盗難・置き忘れ、社外PC持ち込み、印刷などの物理的なセキュリティまで、外部へ情報が流出し得る全ての経路をAIが自動で監視・記録・防止するエンドポイントセキュリティ対策ソリューションです。

持ち出し対策・漏洩対策

evolution /SV
- 短期間にスムーズな導入
- 使い慣れたユーザ環境を維持
- 特別なユーザ教育は不要
- 周辺機器への持ち出し対策
- データの自走式暗号化・カプセル化
- あらゆるメディアへの持出制限
  CD、DVD、BD、MO、USBメモリ、外部接続のHDD、スマートフォン、デジタルカメラ、音楽プレイヤーなどあらゆる外部媒体へのあらゆる経路による持ち出しを制限・自動暗号化し、操作履歴を記録

Write制限機能
- DOSコマンドをはじめ、全てのアプリケーションへ情報漏洩につながるファイルの書き込み・メール送信を禁止

イントラネットオプション
- インターネットへの持ち出し操作制限
  クラウド、Webメールなどの持ち出し操作も暗号化

履歴収集・分析

evolution /SV
- 網羅的な履歴の取得
  印刷・メール添付・メール送信・クリップボード・ファイル名変更・ファイル移動・別名保存・オブジェクトの挿入・オブジェクトの出力・プロセスの起動・終了・Windowsの起動・終了・セキュリティの変更など
- ファイル・メール・webなどに対する動作を監視
- 情報資産の活用状況を把握
- 未使用システム・データの破棄・刷新・改良
- 内存リスクの事前洗い出し
- 内部統制・日本版SOX法にも対応
- 外部持出の際は原本を別途保存

セキュア印刷オプション
- 印刷出力時は出力内容をJPEGで保存

トレーサオプション
- 履歴を収集し、CSV形式ファイルに出力

編集履歴オプション
- キーボード操作も記録

スーパーサーチエンジン(SSE)
- 国内最高レベルのスピードで操作履歴を分析

サイバー攻撃対策

ディフェンスオプション(Defense Platform)
- ホワイトリスト型のサイバー攻撃対策
- パソコン上の全動作を把握するためあらゆる攻撃を捕捉
- 標的型攻撃対応
- 未知のウイルス、最新のウイルス対応

※別冊参照

印刷

evolution /SV
- 外部出力操作の制限

セキュア印刷オプション
- セキュリティ機能を持つプリンタへの印刷制限
- JPEG出力機能
  あらゆるプリンタから出力されるすべての印刷物の内容をJPEG形式で保存

アクセス権

evolution /SV
- 外部出力操作の制限
  印刷・別名保存・クリップボード・キャプチャー・ファイル複製などを許可・禁止し、操作履歴を記録
- CD、DVD、BD、USBメモリなどへの持出制限
  コピー・別名保存を禁止し、操作履歴を記録
- 不正な持出を制限

イントラネットオプション
- イントラネットや業務システムにアクセス権設定

二次漏洩対策

ファイルセーフカプセルオプション
- データの暗号化
- 情報提供先から第三者への持出制限
  印刷・別名保存・クリップボード・キャプチャー・ファイル複製の禁止

盗難・置き忘れ対策

エンクリプションオプション
ストレージエンクリプションオプション
- ファイルを常時または任意に暗号化
- PC、CD、DVD、BD、USBメモリなどの盗難・置き忘れ
- PC破棄時の残データ

リアルタイム履歴通知

リアルタイム履歴通知オプション
- リアルタイムに履歴を通知
  印刷・保存・クリップボード・フォルダ・メール添付・コピー・ファイル閲覧・ファイル名変更・移動・ファイル作成・削除・更新・参照・キャプチャー・カプセル化・メール送信・メール受信など

社外PCの持ち込み使用禁止

非SeP拒否オプション
- 不正接続PCの監視
- SeP未導入PCからのアクセス監視
  外出先からのアクセスをセキュアに
- SeP端末なら、外出先からでも自社内ネットワークへ接続可

グループウェア対策

メールオプション
- メールによる情報の持出操作の制限
  ファイル添付・印刷・別名保存・クリップボード・キャプチャー・ファイル複製などを許可・禁止

GW Domino サーバオプション
GW Exchange サーバオプション
- グループウェアによる情報の持出操作の制限

Active Directory

ベーシック+AD evolution /SV
- Active Directoryと連動して、グループ、ドメインなど、細やかな単位でクライアントにSePポリシーを配信可能
- 複雑な権限や部署がある組織であっても管理が容易
- 部署ごとの履歴も収集できる

仮想環境対応

evolution /SV
evolution /SV for TS/MF
- SePのすべての機能を仮想端末環境で実現し、情報の持ち出しを制限
- RDS、Hyper-V、Azure、Xen、VMware、Aws環境下でもオンプレミス版と同様に全てのSePの機能が動作可能

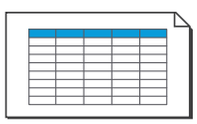
最新環境対応

- Windows 10対応
- Windows 11対応
- Microsoft 365 (旧名：Office 365) 対応
- Device Guard対応
  - IE、Edge、Firefox、Chromeなどのブラウザもバージョン更新ごとに品質テストを行い、都度対応

あらゆる局面を想定したセキュリティ対策でテレワークもバッチリ

理想的なテレワークを実現

Wi-Fiがあれば企業内・役所内と
同レベルの業務環境！公衆Wi-Fiすら安全



詳細な業務履歴・通信履歴で
業務管理がらくらく

ストレスフリーな個人利用と業務での
セキュリティを両立

ワークスペースフォルダ機能の特長

「ワークスペースフォルダ機能」は、端末におけるローカルでの保存先を常に指定のフォルダ「ワークスペースフォルダ」に制限する機能です。保存先が制限されるため、ローカルのデータはすべてワークスペースフォルダ以下に存在することになります。またワークスペースフォルダに保存されたファイルは様々な機能で保護されるため、社外 / 庁外でも安心して業務を行うことができます。

管理者の任意のタイミングで自動削除される

ワークスペースフォルダ内のファイルは、管理者が指定したタイミングで自動削除されます。削除タイミングで端末が起動していなかった場合は、次に起動した時に削除されます。
指定可能な削除タイミング：Windows 起動時、Windows 終了時、ログオン時、ログオフ時、毎日〇時、毎週〇曜日〇時、ファイル最終更新日から〇日経過時、SeP サーバ切断後〇時間経過時

ストレージ暗号がかかっている

ワークスペースフォルダはストレージ暗号化をかけることができます。そのため持ち出し端末が紛失、あるいは盗難された際、ストレージを強引に抜き取って、別の端末に接続して情報を盗み出そうとしても、暗号化されているためデータをみることができません。

盗難紛失対策・遠隔からの削除ができ、削除された際に位置情報も把握できる

設定された任意のタイミングで自動的に全削除するのとは別に、管理者側からデータ削除の命令を出すことができます。命令を受信した端末は、即時にワークスペースフォルダ自体を削除します。動作管理ツールで盗難·紛失した PC の詳細な状況を確認することができます。また盗難·紛失対策完了後に SeP 履歴をアップロードします。

SeP 導入即テレワーク導入完了！テレワークの様々な課題を SeP が解決

以前から労働力確保などの面でテレワークの導入は進められていましたが、2020 年以降の世界情勢に伴い、テレワークの促進は加速度的になっています。しかし急に進められたテレワークにはセキュリティの課題などが多数あります。セキュリティプラットフォームとテレワーク向けに新たに開発された「ワークスペースフォルダ機能」ならば、ただ導入するだけでテレワークの課題を一挙解決。さらに高度なセキュリティを維持したまま、業務を妨げません。組織内で行っていた業務を、まったく手順やルールを変えずに安全なまま外部でも行うことができます。

テレワークのリスクも安心

持ち帰り端末の紛失・盗難

ストレージ（HDD・SSD）暗号化とワークスペースフォルダの自動暗号化・遠隔削除で解決できる

不正アクセス

限られた端末からのみ、アクセスを許可してそれ以外の端末を遮断して解決できる

USBメモリ、メール、Webなどからの漏えい

経路・操作に依らず、ルールや手順なしでファイルを自動的に暗号化して解決できる

始業・終業が良く見える履歴でテレワークの業務管理をサポート

SeP は、PC で行われたあらゆる操作を、詳細にわたって記録する「履歴機能」を持っています。もちろんテレワーク中でも、操作履歴が詳細に取得されるため、業務管理などを行う上で非常に有用です。テレワークに際してはワークスペースフォルダ機能による指定フォルダへの書き込み・持ち出し・自動削除・遠隔削除などの履歴も下記の様に記録されます。

ワークスペースフォルダへの出し入れ、書き込み制限

マシン名	ファイル名	フォルダ名	アプリ名	ウィンドウタイトル	操作名	ユーザ名	操作時間	そのほか
Local	ドキュメント .docx	C:¥HHWorkspaceFolder	explorer.exe		ファイルコピー（ワークスペースフォルダ OUT）	User01	2020/4/8 09:42	¥¥ ファイルサーバ ¥ 資料 ¥ ドキュメント .docx
Local	ドキュメント .docx	¥¥ ファイルサーバ ¥ 資料 ¥ ドキュメント .docx	explorer.exe		ファイルコピー（ワークスペースフォルダ IN）	User01	2020/4/8 09:45	C:¥HHWorkspaceFolder¥ ドキュメント .docx
Local	ドキュメント .docx	C:¥Users¥test¥Desktop¥資料	WINWORD.exe	L<Local>	拒否 - ファイル書き込み（ワークスペースフォルダ機能）	User01	2020/4/8 11:37	C:¥Program Files (x86)¥Microsoft Office¥root¥Office16¥WINWORD.EXE

ワークスペースフォルダ内の自動削除

マシン名	ファイル名	フォルダ名	アプリ名	ウィンドウタイトル	操作名	ユーザ名	操作時間	そのほか
Local		C:¥HHWorkspaceFolder	BKTask.exe		ファイル自動削除（ワークスペースフォルダ機能）	User01	2020/4/8 10:53	2020/4/8 9:10 Windows 起動

ワークスペースフォルダ内の遠隔削除

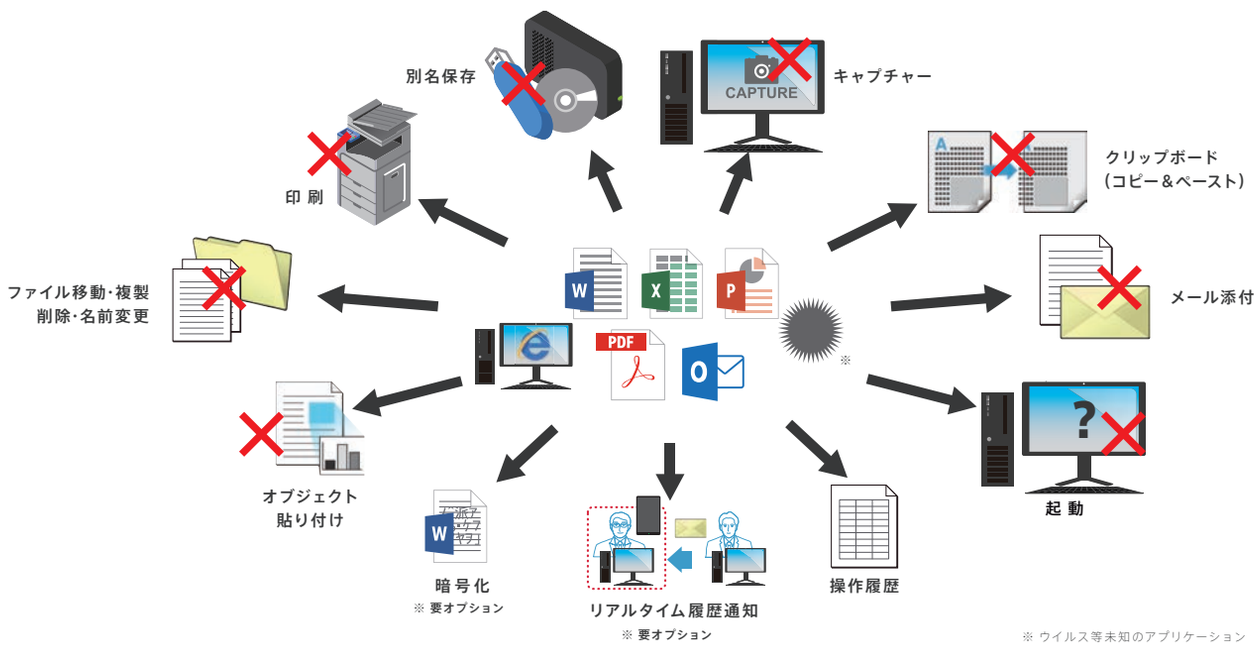
マシン名	社内 / 社外	マシン GUID,OS	アプリ名	位置情報（緯度経度）	操作名	ユーザ名	操作時間	MAC アドレス
Local	社内	233ba5b8-4b91-46e2-c0e3-591fe435b321, Windows 10 version 1909 Build 18363.592	BKTask.exe	35.661037-139.871160	盗難紛失対策実行済み	User01	2020/5/8 18:21	[00-31-58-C0-00-01/192.168.297.9/fe32::150c:cb92:30n1:0220%8] [*00-66-B8-68-9M-45/192.168.291.369/]

防止機能

情報漏洩につながるあらゆる操作を防止

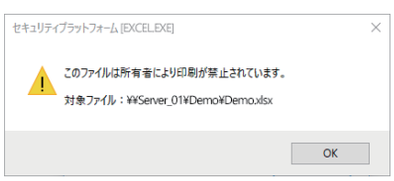
ファイルコピー、印刷、保存、コピー＆ペースト、メール添付などを網羅的に防止

お使いのアプリケーションに対して、情報漏洩につながる操作を網羅的に防止します。一般的な持ち出し操作には、以下の図のような操作があり、セキュリティプラットフォームでは、Windows アクセス権の設定を利用することで、フォルダ・ファイル・メール・インターネットに対してグループ・ユーザ単位で、情報漏洩につながる操作を防止できます。既存環境を変えることなく、ユーザ教育などを行わず、運用できます。業務プロセスの大幅な変更もなく、セキュリティを強化します。この機能により、企業内のあらゆる情報を安全に有効活用できます。

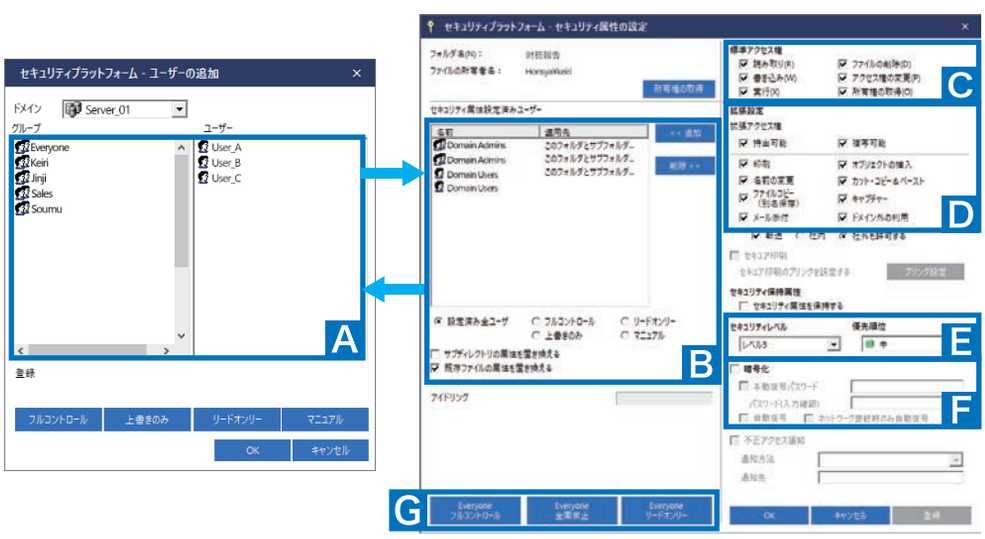


※ ウイルス等未知のアプリケーション

不正操作の際には即座に警告を送ります。



強固なセキュリティを簡単に設定する



A ユーザの追加
グループやユーザを選択（複数可）して登録用ボタンを押すための専用パネルです。

B セキュリティ設定済みユーザ
Windows NT のドメイン管理をそのまま利用しているので、改めてユーザを登録し直す必要はありません。

C 標準アクセス権
Windows NTFS アクセス権を継承します。

D 拡張設定
社内のセキュリティポリシーに合わせたアクセス権の設定ができます。

E セキュリティレベル・優先順位
セキュリティレベルを段階的に設定できます。

F 暗号化（オプション）
自動暗号や手動暗号（パスワード）の管理が設定できます。

G 一括設定ボタン
管理者を除くすべてのユーザに同一の設定ができるので、設定の手間が省けます。

履歴機能

ファイルコピー、印刷、保存、コピー＆ペースト、メール添付などの操作を網羅的に取得

最強の履歴機能

セキュリティプラットフォームは PC 上で行われたあらゆる操作を、AI 技術によりユーザの操作感覚に近い履歴として解釈し、網羅的に記録します。履歴はユーザにわかりやすい書式で記録されています。ファイル･フォルダ･メール･インターネットへの操作に対しては、マシン名･ファイル名･フォルダ名･アプリケーション名･アプリケーションタイトル･操作名･ユーザ名･アクセス日時･備考のように記録された履歴は、管理者に収集されるまで外部に情報が漏れないよう暗号化して保存します。Microsoft 365（旧名：Office 365）の履歴に関しても出力ファイル・別名保存・メールに添付したファイル名・メール送受信・インターネットにアップロードなどの内容を記録します。

取得可能な履歴例

操作内容	操作履歴に記録される操作名
ファイル操作	ファイル作成
	ファイル削除
	ファイル参照
	ファイル更新
	オブジェクトとして出力
	オブジェクトの挿入
	クリップボード
	ファイル名変更
	ファイルコピー
	ファイル移動
	別名保存
	ZIPファイル化
	ドキュメントプロパティ削除
	編集履歴(ファイル)
	編集履歴(ペースト)
	拒否-ファイル書き込み(SV-Write制限)
	拒否-ファイル削除(SV-Write制限)
	拒否-ファイル名変更(SV-Write制限)

操作内容	操作履歴に記録される操作名
フォルダ操作	ディレクトリ作成
	ディレクトリ削除
印刷操作	印刷
	プリントジョブ
	拒否-印刷(SV-Write制限)
メール操作	受信
	送信
	メール添付
	編集履歴(メール)
Web操作	接続
	アップロード
	編集履歴(インターネット)
	拒否-HTTPリクエスト
IP通信	拒否-ファイル転送(SV-Write 制限)
MTP通信	拒否-ファイル転送(SV-Write 制限)
Bluetooth通信	拒否-ファイル転送(SV-Write 制限)
USB 外部記憶媒体操作	USB 接続
	USB 切断
	拒否-USB接続

操作内容	操作履歴に記録される操作名
申請・承認操作	承認
	申請
	申請取り下げ
	否認
アプリケーション操作	アクティブウィンドウ
	編集履歴(プロセス)
	サインイン
	サインアウト
	アカウント切り替え
Windows操作	Windows 起動
	Windows 終了
	ログオン
	ログオフ
	ネットワーク切り替え
SePに対する操作	SeP インストール
	SeP アンインストール
	SeP アップデート
SePの自己保護	拒否-SePモジュール保護
	拒否-SePレジストリ保護
	拒否-不正パケット
	拒否-非SePアクセス

網羅的な履歴

SeP は他社製品と比較しても圧倒的に詳細な履歴を取得できます。ある操作を行うには何通りかの方法がありますが、SeP は全て網羅します。ファイルコピーや、クリップボード（コピー＆ペースト）、メール添付など、方法は様々です。SeP は、**あらゆる操作方法に対して防止**することができ、履歴を残すことが可能です。

例：ファイルコピーの操作例

1. マウスでドラッグ＆ドロップによるファイルコピー
2. ショートカットキーによるファイルコピー（Ctrl＋C→Ctrl＋V）
3. 右クリックメニューによるファイルコピー（コピー→貼り付け）
4. メニューによるファイルコピー（コピー→貼り付け）
5. ファイルをアプリケーションで開いて別名保存

SeP 操作履歴サンプル

	A	B	C	D	E	F	G	H	I
1	マシン	ファイル	フォルダパス	アプリケーション	ファイルサイズ	操作	ユーザ	日時	備考（持出し先　等）
2		メール件名	送信元、送信先メールアドレス		ウィンドウタイトル				備考（添付ファイル　等）
3		接続URL（ドメイン以降）	接続URL（ドメイン）						備考（アップロードファイル　等）
4	DEMO-PC					Windows起動	SYSTEM	2020/7/1 09:01:59	02-00-4C-4F-4F-50
5	DEMO-PC					ログオン	user01	2020/7/1 09:02:39	[192.168.0.1]
6	DEMO-PC		Wireless LAN adapter Wi-Fi		35.661037-139.871160	ネットワーク切り替え	user01	2020/7/1 09:03:52	[02-00-4C-4F-4F-50/192.168.5.61/ fe80::e907:de44:2243:5b5%1]
7	DEMO-PC			EXCEL.EXE		プロセス起動	user01	2020/7/1 09:28:43	14.0.6112.5000
8	DEMO-PC	自治体別人口･PC台数一覧.xlsx	¥¥FileSrv¥営業¥共有情報¥自治体関連	EXCEL.EXE	Size<2132496>L<NetworkDrive>Microsoft Excel – 自治体別人口･PC台数一覧.xlsx	別名保存	user01	2020/7/1 09:30:30	C:¥Users¥user1¥Desktop¥自治体別人口･PC台数一覧.xlsx
9	DEMO-PC	自治体別人口･PC台数一覧.xlsx	¥¥FileSrv¥営業¥共有情報¥自治体関連	EXCEL.EXE	Size<2132496>L<NetworkDrive>	ファイル参照	user01	2020/7/1 09:30:30	107
10	DEMO-PC	自治体別人口･PC台数一覧.xlsx	C:¥Users¥user1¥Desktop	EXCEL.EXE	Size<2132496>L<Local>	ファイル更新	user01	2020/7/1 09:30:30	5
11	DEMO-PC	自治体別人口･PC台数一覧.xlsx	C:¥Users¥user1¥Desktop	EXCEL.EXE	L<Local>	編集履歴(ファイル)	user01	2020/7/1 09:30:30	kom¥BS¥BS¥BS¥BS¥KN¥BS米¥BS※メ¥BS2017/2/3時点の情報¥RE¥RE
12	DEMO-PC			EXCEL.EXE		プロセス終了	user01	2020/7/1 09:30:34	
13	DEMO-PC	自治体別人口･PC台数一覧.xlsx	C:¥Users¥user1¥Desktop	Explorer.EXE	Size<2132496>L<Local to Local>	ファイル名変更	user01	2020/7/1 09:31:10	C:¥Users¥user1¥Desktop¥【参考資料】自治体別人口･PC台数一覧.xlsx
14	DEMO-PC		G:			USB接続	user01	2020/7/1 10:21:16	USB¥HUM_0123&HED_4567¥HH0123456789012[Humming USB device][メモリ]
15	DEMO-PC	報告書.docx	C:¥Users¥user01¥Desktop¥デモファイル	Explorer.EXE	Size<13204>L<Local to USB>	ファイルコピー(SV-暗号)	user01	2020/7/1 10:21:31	G:¥報告書.docx.sve
16	DEMO-PC	報告書.docx.sve	G:	Explorer.EXE	Size<13953>L<USB to Local>	ファイルコピー	user01	2020/7/1 10:21:36	C:¥Users¥user01¥Desktop¥報告書.docx
17	DEMO-PC	報告書.docx.sve	G:	Explorer.EXE	Size<13953>L<USB>	ファイル削除	user01	2020/7/1 10:21:59	
18	DEMO-PC		G:			USB切断	user01	2020/7/1 10:22:06	USB¥HUM_0123&HED_4567¥HH0123456789012[Humming USB device][メモリ]
19	DEMO-PC			OUTLOOK.EXE		プロセス起動	user01	2020/7/1 14:00:09	12.0.667.10000
20	DEMO-PC	SeP提案書.pptx	C:¥Users¥user01¥Desktop¥デモファイル	OUTLOOK.EXE	Size<13122>L<Local>提案書のレビュー依頼 - メッセージ (HTML 形式)	メール添付(SV-暗号)	user01	2020/7/1 14:00:42	SeP提案書.pptx.sve
21	DEMO-PC	提案書のレビュー依頼	user01@hummingheads.co.jp → demo@hummingheads.co.jp; shonin@hummingheads.co.jp	OUTLOOK.EXE	提案書のレビュー依頼 - メッセージ (テキスト形式)	送信	user01	2020/7/1 14:00:46	SeP提案書.pptx.sve
22	DEMO-PC	提案書のレビュー依頼	user01@hummingheads.co.jp → demo@hummingheads.co.jp; shonin@hummingheads.co.jp	OUTLOOK.EXE	提案書のレビュー依頼 - メッセージ (テキスト形式)	編集履歴(メール)	user01	2020/7/1 14:00:46	ファイルを送付します。¥RE¥RE宜しくお願い致します。¥RE¥RE
23	DEMO-PC	提案書のレビュー依頼	user01@hummingheads.co.jp → demo@hummingheads.co.jp; shonin@hummingheads.co.jp	OUTLOOK.EXE	Outlook 送受信の進捗度	受信	user01	2020/7/1 14:01:04	
24	DEMO-PC			OUTLOOK.EXE		プロセス終了	user01	2020/7/1 14:01:43	
25	DEMO-PC					拒否-USB接続	user01	2020/7/1 14:44:33	USB¥Vid_9876&Pid_00000&5432&1&0
26	DEMO-PC		G:			USB接続	user01	2020/7/1 14:45:02	USB¥HUM_0123&HED_4567¥HH0123456789012[Humming USB device][メモリ]
27	DEMO-PC	報告書01.docx	C:¥Users¥user01¥Desktop¥デモファイル	Explorer.EXE	Size<13204>L<Local to NetworkDrive>	ファイルコピー(SV-リリース固定平文IN)	user01	2020/7/1 14:45:14	¥¥RelSrv¥リリースフォルダ¥user01¥報告書01.docx
28	DEMO-PC	報告書01.docx	¥¥RelSrv¥リリースフォルダ¥user01	Explorer.EXE	Size<13204>L<NetworkDrive to CD/DVD/BD>	ファイルコピー(SV-リリース固定平文OUT)	user01	2020/7/1 14:45:17	E:¥報告書01.docx
29	DEMO-PC	報告書02.docx	C:¥Users¥user01¥Desktop¥デモファイル	Explorer.EXE	Size<28160>L<Local to	ファイルコピー(SV-リリース選択IN)	user01	2020/7/1 14:45:24	¥¥RelSrv¥リリース形式選択フォルダ¥user01¥報告書02.docx

社内操作

社内流通（SV暗号･復号）

社外持ち出し（リリースフォルダ）
外部媒体

29	DEMO-PC	報告書02.docx	C:¥Users¥user01¥Desktop¥デモファイル	Explorer.EXE	Size<28160>L<Local to NetworkDrive>	ファイルコピー(SV-リリース選択IN)	user01	2020/7/1 14:45:24	¥¥RelSrv¥リリース形式選択フォルダ¥user01¥報告書02.docx
30	DEMO-PC	報告書02.docx	¥¥RelSrv¥リリース形式選択フォルダ¥user01	Explorer.EXE	Size<28160>L<NetworkDrive to USB>	ファイルコピー(SV-リリース選択ZIP OUT)	user01	2020/7/1 14:46:33	G:¥報告書02.docx
31	DEMO-PC	打ち合わせ議事録.docx	C:¥Users¥user01¥Desktop¥デモファイル	Explorer.EXE	Size<18367>L<Local to NetworkDrive>	ファイルコピー(SV-リリース選択IN)	user01	2020/7/1 14:46:38	¥¥RelSrv¥リリース形式選択フォルダ¥user01¥打ち合わせ議事録.docx
32	DEMO-PC	打ち合わせ議事録.docx	¥¥RelSrv¥リリース形式選択フォルダ¥user01	Explorer.EXE	Size<18367>L<NetworkDrive to FD>	ファイルコピー(SV-リリース選択自走式暗号OUT)	user01	2020/7/1 14:46:51	A:¥打ち合わせ議事録.docx
33	DEMO-PC	SeP提案書.pptx	C:¥Users¥user01¥Desktop¥デモファイル	Explorer.EXE	Size<30283>L<Local to NetworkDrive>	ファイルコピー(SV-リリース選択IN)	user01	2020/7/1 14:47:15	¥¥RelSrv¥リリース形式選択フォルダ¥user01¥SeP提案書.pptx
34	DEMO-PC	SeP提案書.pptx	¥¥RelSrv¥リリース形式選択フォルダ¥user01	Explorer.EXE	Size<30283>L<NetworkDrive to MO>	ファイルコピー(SV-リリース選択カプセルOUT)	user01	2020/7/1 14:47:31	F:¥SeP提案書.pptx
35	DEMO-PC		G:			USB切断	user01	2020/7/1 14:47:45	USB¥HUM_0123&HED_4567¥HH0123456789012[Humming USB device][メモリ]
36	DEMO-PC			OUTLOOK.EXE		プロセス起動	user01	2020/7/1 14:56:55	12.0.667.10000
37	DEMO-PC	提案資料一式.zip	¥¥RelSrv¥リリース形式選択フォルダ¥user01	OUTLOOK.EXE		パスワード自動生成	user01	2020/7/1 14:57:46	w4c?z+i9FN5@
38	DEMO-PC	提案資料一式.zip	¥¥RelSrv¥リリース形式選択フォルダ¥user01	OUTLOOK.EXE	Size<31696>L<NetworkDrive>	メール添付(SV-リリース選択ZIP OUT)	user01	2020/7/1 14:57:47	提案資料一式.zip
39	DEMO-PC	提案書01.docx	¥¥RelSrv¥リリース形式選択フォルダ¥user01¥提案資料一式.zip	OUTLOOK.EXE	Size<31696>L<NetworkDrive>	メール添付(SV-リリース選択ZIP OUT)	user01	2020/7/1 14:57:47	提案資料一式.zip
40	DEMO-PC	提案書02.docx	¥¥RelSrv¥リリース形式選択フォルダ¥user01¥提案資料一式.zip	OUTLOOK.EXE	Size<31696>L<NetworkDrive>	メール添付(SV-リリース選択ZIP OUT)	user01	2020/7/1 14:57:47	提案資料一式.zip
41	DEMO-PC	提案書の送付	user01@hummingheads.co.jp → customer01@corp01.co.jp; customer02@corp02.co.jp	OUTLOOK.EXE	提案書の送付 - メッセージ (テキスト形式)	送信	user01	2020/7/1 14:57:52	提案資料一式.zip
42	DEMO-PC	提案書の送付	user01@hummingheads.co.jp → customer01@corp01.co.jp; customer02@corp02.co.jp	OUTLOOK.EXE	提案書の送付 - メッセージ (テキスト形式)	編集履歴(メール)	user01	2020/7/1 14:57:52	提案資料一式を送付致します。¥RE¥RE
43	DEMO-PC			OUTLOOK.EXE		プロセス終了	user01	2020/7/1 14:58:59	
44	DEMO-PC	/mail/?hl=ja&shva=1#inbox	mail.google.com	iexplore.exe		アップロード	user01	2020/7/1 15:33:13	
45	DEMO-PC	/mail/?hl=ja&shva=1#inbox	mail.google.com	iexplore.exe	Gmail - 受信トレイ - user01@gmail.com - Windows Internet Explorer	アクティブウィンドウ	user01	2020/7/1 15:33:21	12
46	DEMO-PC	/mail/?hl=ja&shva=1#compos	mail.google.com	iexplore.exe		アップロード	user01	2020/7/1 15:33:22	
47	DEMO-PC	/mail/?hl=ja&shva=1#compose	mail.google.com	iexplore.exe	L<URL>Gmail - メールを作成 - user01@gmail.com - Windows Internet Explorer	アクティブウィンドウ	user01	2020/7/1 15:33:30	8
48	DEMO-PC	/mail/?hl=ja&shva=1#compose	mail.google.com	iexplore.exe	Size<18367>L<NetworkDrive to URL>	アップロード(SV-リリース選択自走式暗号OUT)	user01	2020/7/1 15:33:58	¥¥RelSrv¥リリース形式選択フォルダ¥user01¥打ち合わせ議事録.docx
49	DEMO-PC	/mail/?hl=ja&shva=1#compose	mail.google.com	iexplore.exe	L<URL>Gmail - メールを作成 - user01@gmail.com - Windows Internet Explorer	アクティブウィンドウ	user01	2020/7/1 15:33:31	69
50	DEMO-PC	/mail/?hl=ja&shva=1#compos	mail.google.com	iexplore.exe		アップロード	user01	2020/7/1 15:35:32	
51	DEMO-PC	/mail/?hl=ja&shva=1#inbox	mail.google.com	iexplore.exe	L<URL>Gmail - 受信トレイ (1) - user01@gmail.com - Windows Internet Explorer	アクティブウィンドウ	user01	2020/7/1 15:35:43	10
52	DEMO-PC			AcroRd32.exe		プロセス起動	user01	2020/7/1 17:18:28	10.1.7
53	DEMO-PC	経済産業省_中小企業白書2010_概要.pdf	¥¥FileSrv¥営業企画¥共有情報¥参考資料¥経済産業省	AcroRd32.exe	Size<2712250>L<NetworkDrive>	印刷	user01	2020/7/1 17:19:10	user01@DEMO-PC-20170203-171910509
54	DEMO-PC	経済産業省_中小企業白書2010_概要.pdf	Canon iR C3200	splwow64.exe	35	プリントジョブ	user01	2020/7/1 17:20:08	14Bytes,2部,A4,user01@DEMO-PC-20170203-171910509
55	DEMO-PC	経済産業省_中小企業白書2010_概要.pdf	¥¥FileSrv¥営業企画¥共有情報¥参考資料¥経済産業省	AcroRd32.exe	Size<2712250>L<NetworkDrive>	ファイル参照	user01	2020/7/1 17:20:17	106
56	DEMO-PC					ログオフ	user01	2020/7/1 18:22:23	[192.168.0.1]
57	DEMO-PC					Windows終了	SYSTEM	2020/7/1 18:22:30	02-00-4C-4F-4F-50

外部媒体

社外持ち出し（リリースフォルダ）
Eメール

社外持ち出し（リリースフォルダ）
Webブラウザ

印刷

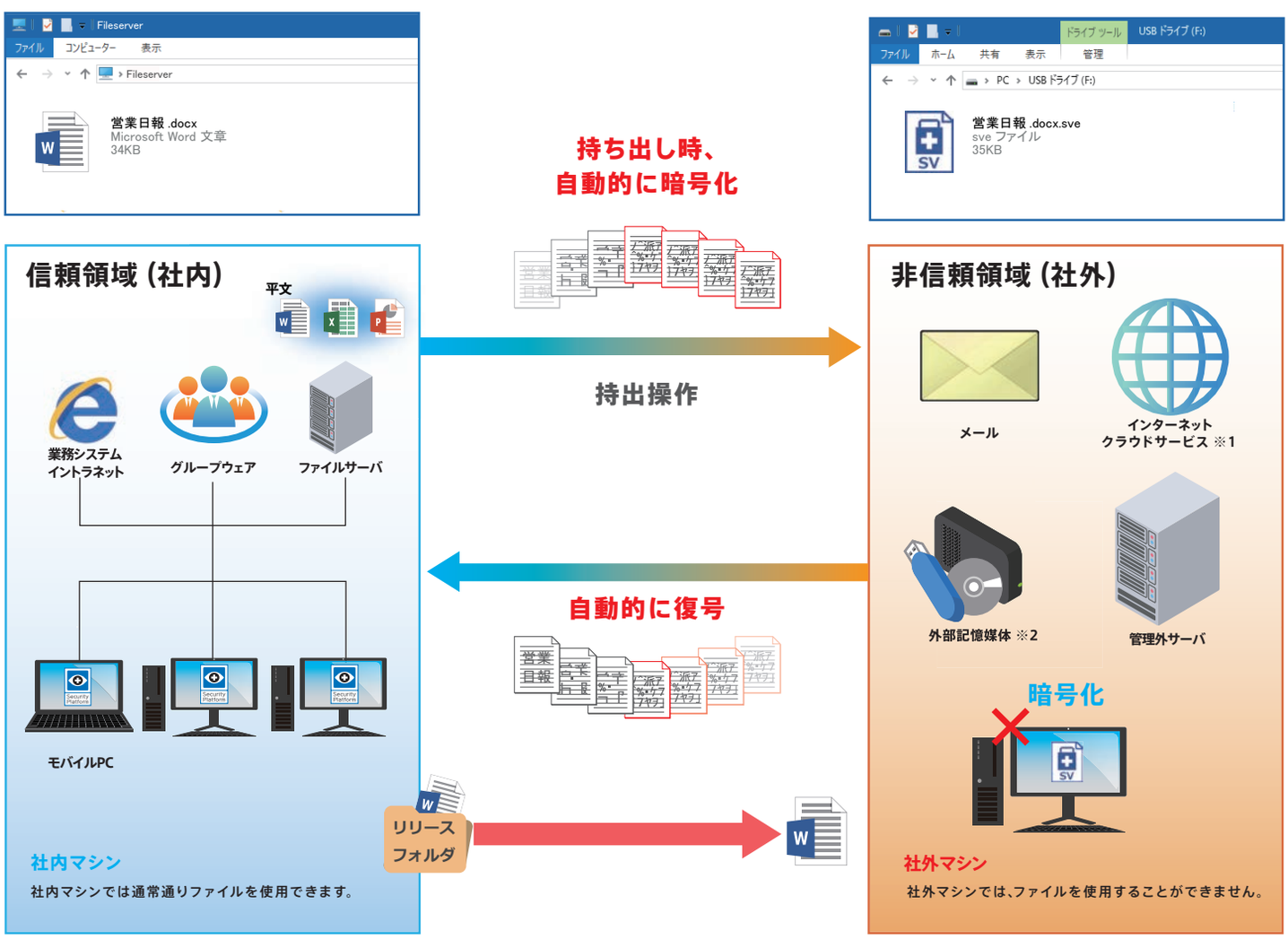
evolution /SV 機能

細かいルールが不要で、PC の使い勝手を変えることなくセキュリティを強靭化

データを社外へ持ち出す際、必ず自動的に暗号化します。
ほぼ全てのセキュリティプラットフォームユーザが利用しています。

evolution /SV 機能ではユーザが定義した信頼領域（社内）から、それ以外の非信頼領域（社外）へファイルを持ち出す際に SV 暗号化（ワンタイムパス、社内暗号キーでのみ復号可）を行い、社外ではファイルを一切使用できないように制限します。SV 暗号化ファイルを社内に戻す時にも自動で復号が行われます。

操作が信頼領域と非信頼領域のどちらに対するものであるかは SeP の AI が自動的に判定します。そのため、ユーザは一切意識することなく、この機能を使うことができます。故意の持ち出しはもちろん、操作ミスによる情報漏洩、USB メモリや SD カードなどの外部媒体による持ち出し、CD、DVD、BD などの各記録媒体の紛失や盗難にも対応し、企業・官公庁内にある情報の安全を徹底的に強化します。さらに evolution /SV 機能を導入しても既存のファイルサーバやクライアント PC では、ファイルは平文で保存されます。そのため、導入後もユーザ環境の変更が少なく、スムーズな環境移行が可能です。



リリースフォルダ

社内で閲覧可能な形式でのファイル持ち出しを許可できます。
※設定によってパスワード付与を強制するという運用も可能です。

※1　ブラウザに対するevolution/SV機能を有効にするには、イントラネットオプションが必要です。
※2　USBメモリ、SDカード等の独自フォーマットは不要です。

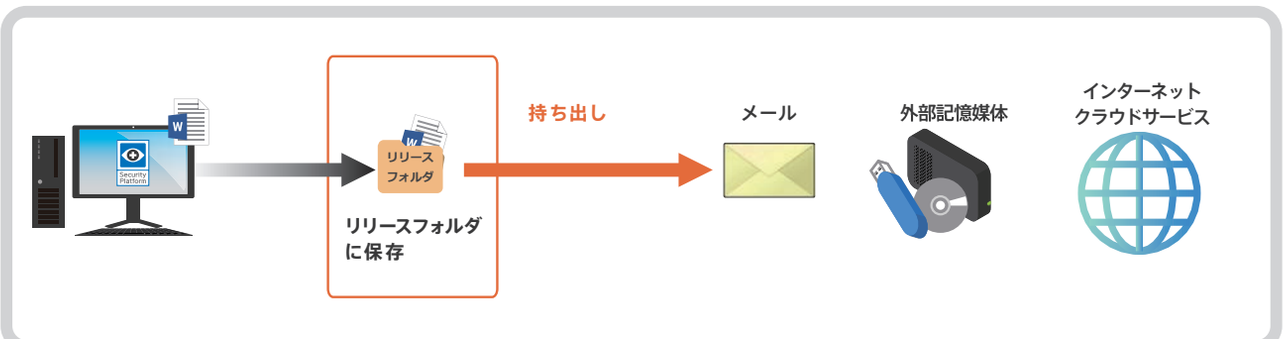
※　Explorer、Internet ExplorerなどのSV化対象アプリケーションから非信頼領域への持ち出しはファイルの種類に制限なく自動で暗号化します。それ以外のアプリケーションによる書き込みは、Write制限機能で禁止されます。

evolution /SV 機能

リリースフォルダ

evolution /SV 機能により、情報を持ち出す操作時には、全て暗号化が行われます。暗号化されたファイルは社外では復号できません。社外で情報を利用したい場合は、リリースフォルダを一旦経由することで、ファイルを平文のまま社外へ持ち出すことができるようになります。リリースフォルダから持ち出す際のファイル形式は 4 種類あります。カプセル化形式、自走式暗号ファイル化形式、パスワード付き ZIP ファイル化形式、平文形式です。「ファイルを社外に持ち出す時には、必ずリリースフォルダを使わなければならない」ということを意識させることで、ユーザのセキュリティ意識の向上にも一役買います。

リリースフォルダとは　社内情報を社外へ持ち出す時、必ず経由しなければならないフォルダです。

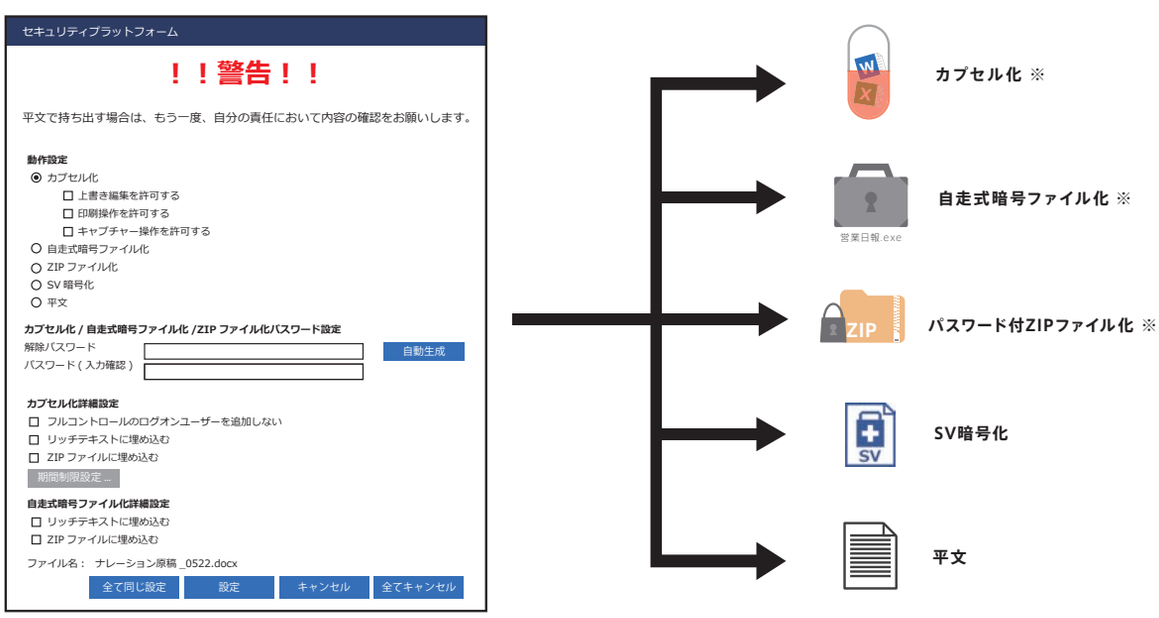


リリースフォルダの特長

リリースフォルダへの操作は全て記録されます。その履歴から、社外へ持ち出されたファイルを把握できます。また、リリースフォルダからファイルが持ち出された時にリアルタイムで通知する設定もできます。また、原本管理機能により、持ち出されたファイルの元ファイルを原本として保護し、原本ファイルの削除・移動・上書き・名前の変更などを禁止できます。

リリース形式選択フォルダ

リリース形式選択フォルダにファイルをコピーすると、リリース形式選択パネルが表示されます。データを持ち出す際のファイル形式は「カプセル化」「自走式暗号ファイル化」「ZIP ファイル化」「SV 暗号化」「平文」から選択できます。さらに、ファイルを持ち出す先により、異なるファイルの持ち出し形式を指定することができます。例えば、「持ち出し形式を「パスワード付 ZIP ファイル化」に強制する」という運用や、「外部媒体へのファイル持ち出し形式のみ平文選択を不可にする (パスワード付与を強制する)」という運用が可能です。また、本フォルダからファイルをアップロードできる URL を限定することもできます。



※別途オプションが必要です。

リリース承認フォルダ

申請から承認、持ち出しをスムーズに

アプリ制限は一切なし。安全で誰でもかんたんに使える

リリース承認フォルダは、非信頼領域へファイルを持ち出す際の申請・承認フローを簡単にわかりやすく、便利にしたものです。承認者へ申請を行い、承認者が承認したファイルを申請者のみが持ち出すことができるようにします。リリース承認フォルダにファイルを保存すると、自動的に申請者の UI が立ち上がり、申請を簡単にできます。申請すると承認者に自動で通知が行き、承認と否認を行うことができます。承認·否認を行うと申請者に連絡が行きます。あらゆる形式のファイルでも使用でき、申請から持ち出しまでを記録に残し、手続きを踏ませつつ、極限まで簡単にした画期的な機能です。

申請者以外は持ち出し不可

リリース承認フォルダは、申請者以外持ち出すことができません。第三者はもちろん、承認者もファイルの持ち出しはできません。申請のない不正な持ち出しを一切できないようにします。

持ち出しまでのフローも履歴に

申請から承認までのフローはすべて履歴に記録されます。申請理由や承認者コメントも記録されるため、いつ、だれが、どのようなファイルを、だれに承認されて、どのような理由で持ち出したのか記録に残ります。

承認者・申請者の管理が容易に

承認者と申請者の組み合わせは任意に指定でき、それぞれ複数のユーザを登録することができます。ご利用の AD におけるユーザ名·グループ名で定義することも可能です。さらに、自己承認を禁止する設定ができるなど柔軟な運用ができます。

リリース承認時の履歴

●申請者

	端末名	ファイル名	フォルダパス	アプリケーション	申請 ID 等	操作	ユーザ名	日時	備考（持ち出し先等）
1	PC01	報告書 01.pdf	¥¥SePSrv¥ リリース承認フォルダ	HHRelMng.exe	5300000B_1C2C293A	申請	user01	2019/4/1 21:20	[○○社に××の報告書を提出いたします。承認お願いします]
2	PC01	報告書 01.pdf	C:¥Biz¥SeP¥ デモファイル	HHRelMng.exe	L<Local to NetworkDrive>	ファイルコピー (SV- リリース承認 IN)	user01	2019/4/1 21:20	¥¥SePSrv¥ リリース承認フォルダ¥報告書 01.pdf

●承認者

3	PC02	報告書 01.pdf	¥¥SePSrv¥ リリース承認フォルダ	HHRelMng.exe	L<NetworkDrive> 開く	ファイル参照	manager01	2019/4/1 21:21	[○○社に××の報告書を提出いたします。承認お願いします]
4	PC02	報告書 01.pdf	¥¥SePSrv¥ リリース承認フォルダ	HHRelMng.exe	5300000B_1C2C293A	承認	manager01	2019/4/1 21:21	[AD¥user01][承認しました]

●申請者

5	PC01	報告書 01.pdf	¥¥SePSrv¥ リリース承認フォルダ	Explorer.EXE	L<NetworkDrive to USB>	ファイルコピー (SV- リリース承認 ZIP OUT)	user01	2019/4/1 21:29	E:¥ 報告書 01.pdf

Write 制限機能

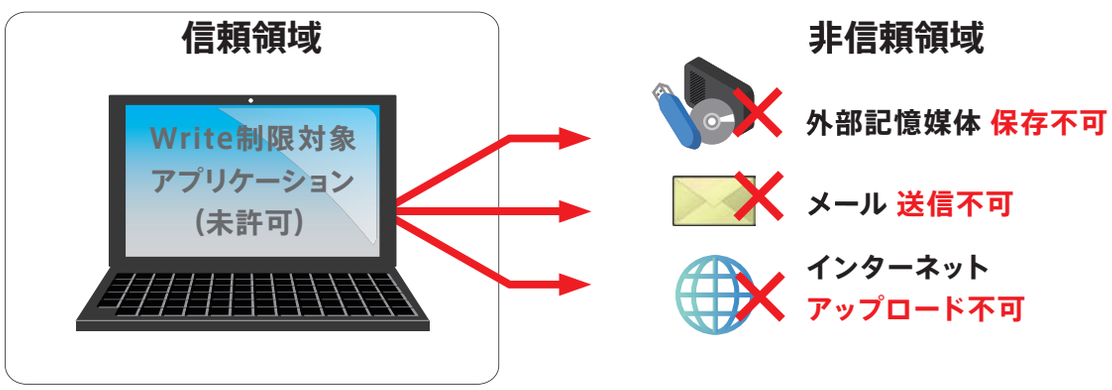
全てのアプリケーションのファイル書き込み・送信を制限（禁止）する

Write 制限とは

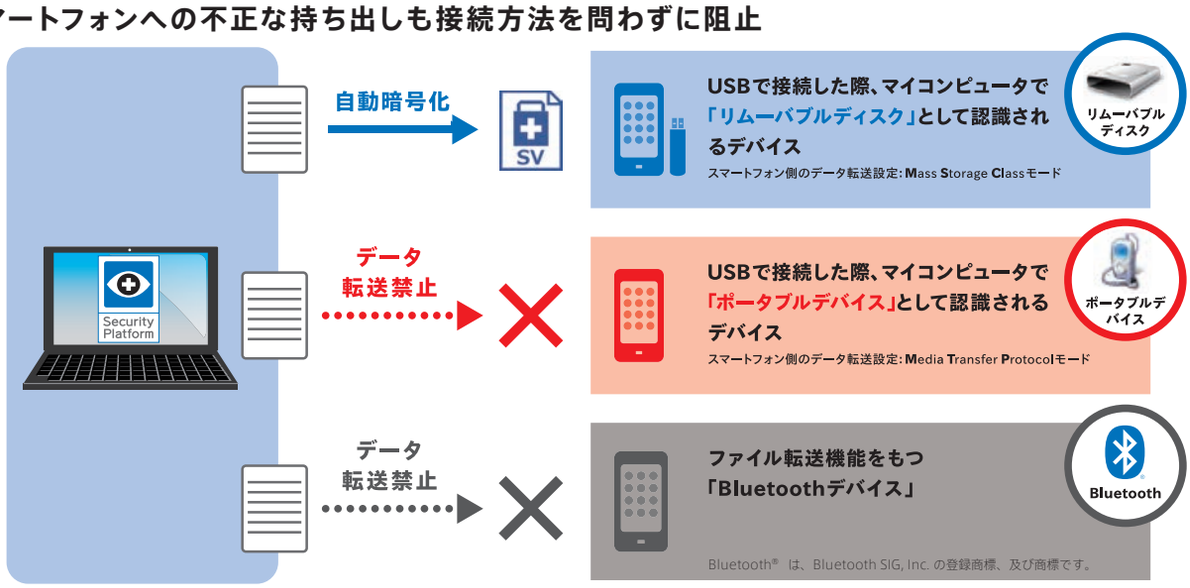
Write 制限機能は、全てのアプリケーションに対して書き込み (ファイルコピー･移動･別名保存･上書き保存など) や通信 (メール送信や転送、Web アップロードなど) を禁止する機能です。尚、信頼領域においては、従来通り書き込み・通信を行うことができます。特定のアプリケーションが行う書き込み･通信を許可したい場合には、許可指定も可能です。Write 制限機能を使うことで、業務を妨げずに万全のセキュリティを実現できます。

書き込み・通信の制限

指定アプリケーション全てに対してファイルコピー･ファイル移動･別名保存･上書き保存などの社外への持ち出し操作を完全に禁止。
また、メール送信や転送、Web 上へのアップロードなども禁止します。



スマートフォンへの不正な持ち出しも接続方法を問わずに阻止



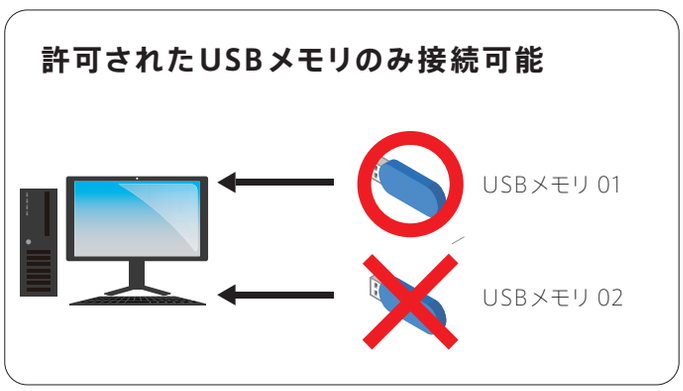
ファイル操作の Write 制限　対象ファイル操作：ファイルコピー、ファイル移動、別名保存、上書保存
通信の Write 制限　対象通信：メール送信（SMTP プロトコル）、ファイル転送（FTP プロトコル）、プロトコルによらず接続制限ができます。
Web アップロードの Write 制限　対象通信：インターネットへのアップロード（HTTP/HTTPS プロトコル）

USB の接続制限機能 /USB の接続・切断履歴出力機能

メーカー名、型式、個体番号、ユーザ名、マシン名を条件に USB メモリ（外部媒体）の接続を許可・不許可

あらゆる USB メモリに対して接続を制限。接続が許可された・禁止された、という履歴を出力

USB メモリなどの外部媒体からの情報漏洩対策を急務とする企業が増加する中、個人用 USB メモリの持ち込みに対する防止策や、セキュリティ機能付き USB メモリ導入にかかる高いコストなど、乗り越えるべき課題が多いのが現状です。また、情報漏洩リスクを回避するために USB メモリ自体の使用を禁止する企業も少なくありません。それでは、業務効率を低下させかねません。



SeP では、インターフェースに USB を使用したあらゆる USB メモリ・HDD・CD/DVD/BD に対して「メーカー名」「型式」「個体番号」「ユーザ名」「マシン名」などを条件に接続を制限します。
また、接続が許可された外部媒体に関しては接続 / 切断の履歴を出力し、接続が制限された場合は禁止操作履歴を出力。同時に「マシン名」「ドライブ名」「日時」「操作名」「ユーザ名」「デバイスの種別」を履歴として出力することで、情報がどの外部媒体から持ち出されたか、もしくは持ち込まれたかを特定することができます。

取得可能な履歴例 - USB メモリ接続時

マシン名	PC-003
ドライブ名	F:¥
操作名	USBメモリ接続
ユーザ名	Suzuki
操作日時	2019/4/1　13:21
デバイス情報	USB¥HUM_0123&HED_4567¥HH0123456789012[Humming USB device][HDD] ①　②　③　④　⑤ デバイスインスタンスID【①メーカーID ②型式ID ③個体ID番号】④外部記憶媒体名 ⑤媒体種別

※外部媒体とは外部記憶媒体のことです。

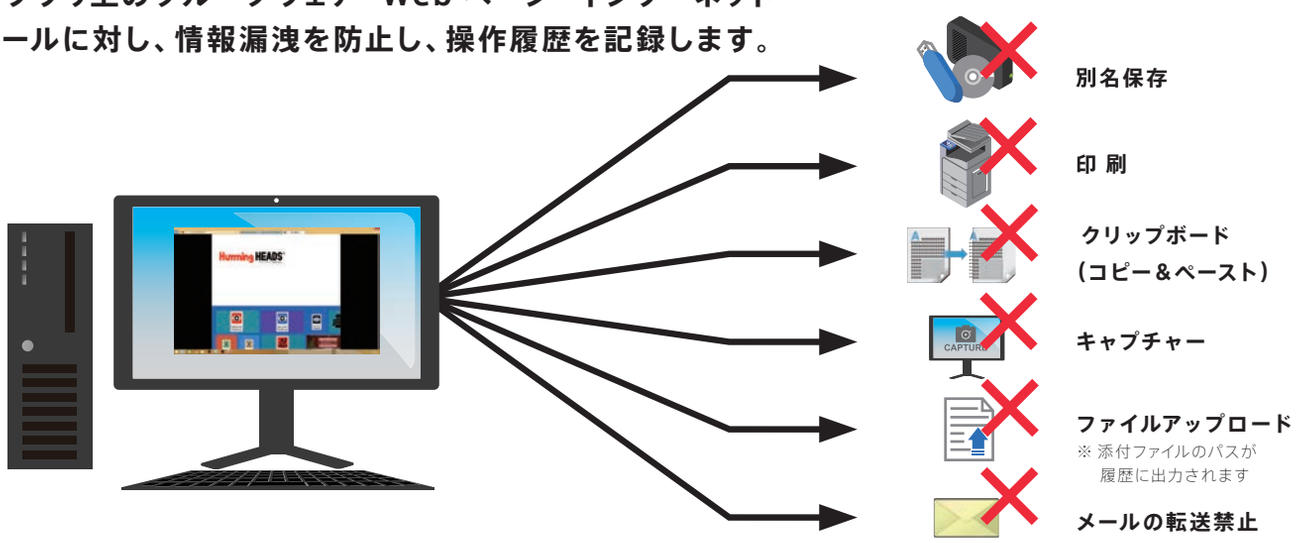
イントラネットオプション

インターネット・イントラネットのセキュリティ強化

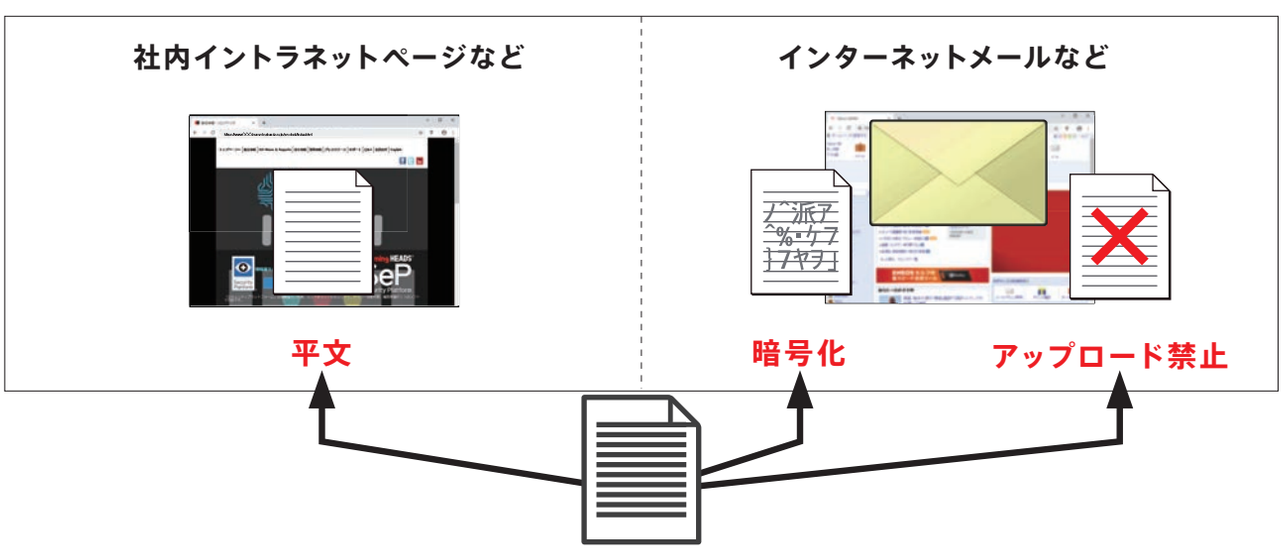
イントラネットオプションは、インターネット・イントラネットなどのブラウザ上で利用するアプリケーションに対して、情報漏洩につながる操作を AI が判定して、防止·暗号化·記録をおこないます。ブラウザ上のグループウェアメール·掲示板やインターネットメール·ホームページ上のブリーフケース・インターネット掲示板などへの、ファイルアップロード・別名保存・コピー＆ペースト・印刷・キャプチャー・メール転送などの操作はすべて防止・暗号化・記録の対象です。evolution/SV などを併用することで、インターネット・イントラネット上へ情報をアップロードする時、自動的に暗号化・復号することができます。インターネット環境でも社内環境と同様のセキュアな運用が可能になります。もちろん、最新の Azure や Microsoft 365（旧名：Office 365）にも対応しています。

対応環境　ブラウザ:Internet Explorer/Firefox ESR/Google Chrome/Edge　プロトコル:HTTP/HTTPS/WebDAV プロトコル(SharePoint環境)

ブラウザ上のグループウェア・Web ページ・インターネットメールに対し、情報漏洩を防止し、操作履歴を記録します。



evolution /SV 併用時
アップロード先 URL ごとにアップロードの方式 (平文・暗号化・禁止) を指定できます。



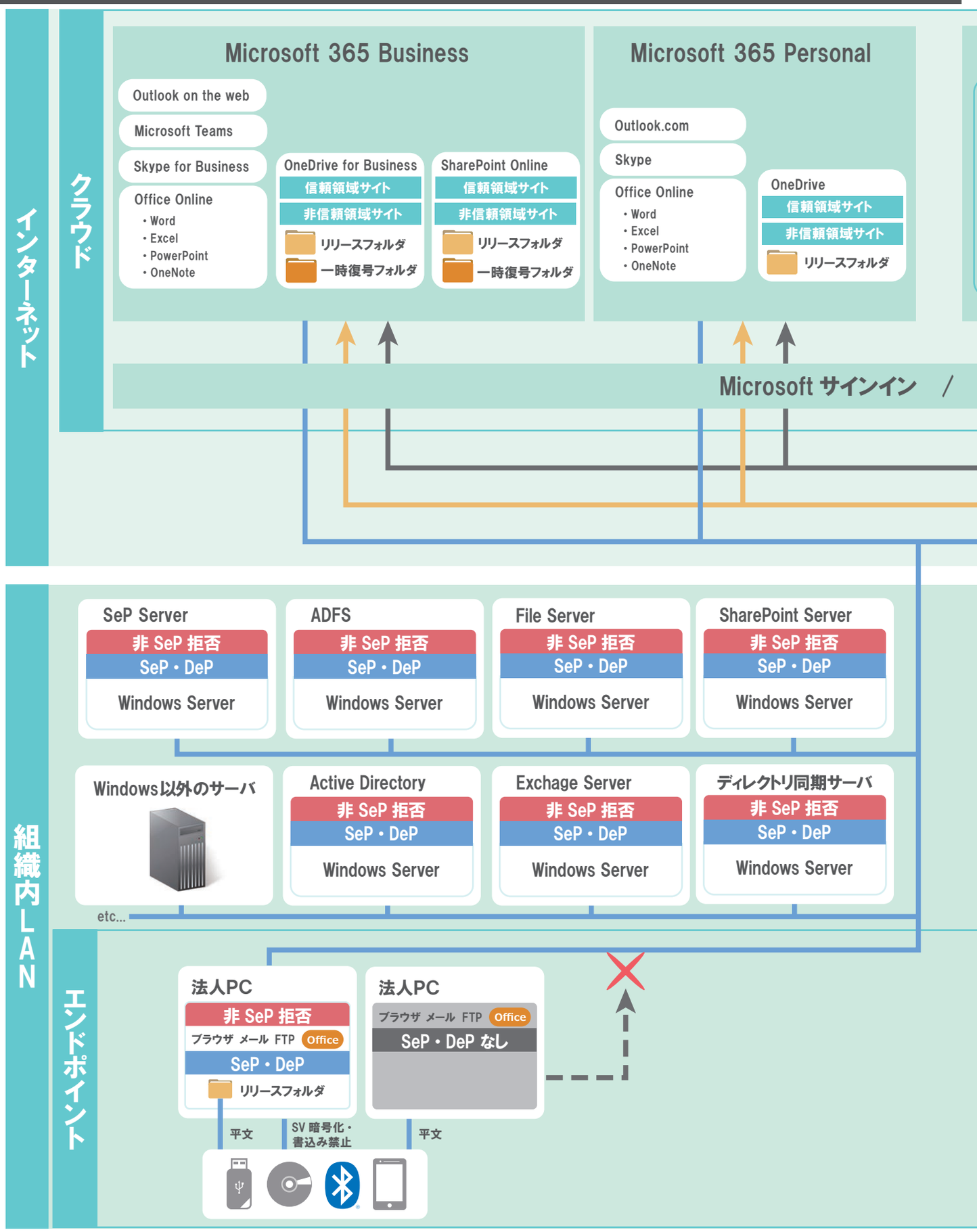
※業務アプリケーションなどユーザ様固有の環境については、運用検証の上ご利用ください。

イントラネットオプション（Microsoft 365※・Azure 対応）

オプション

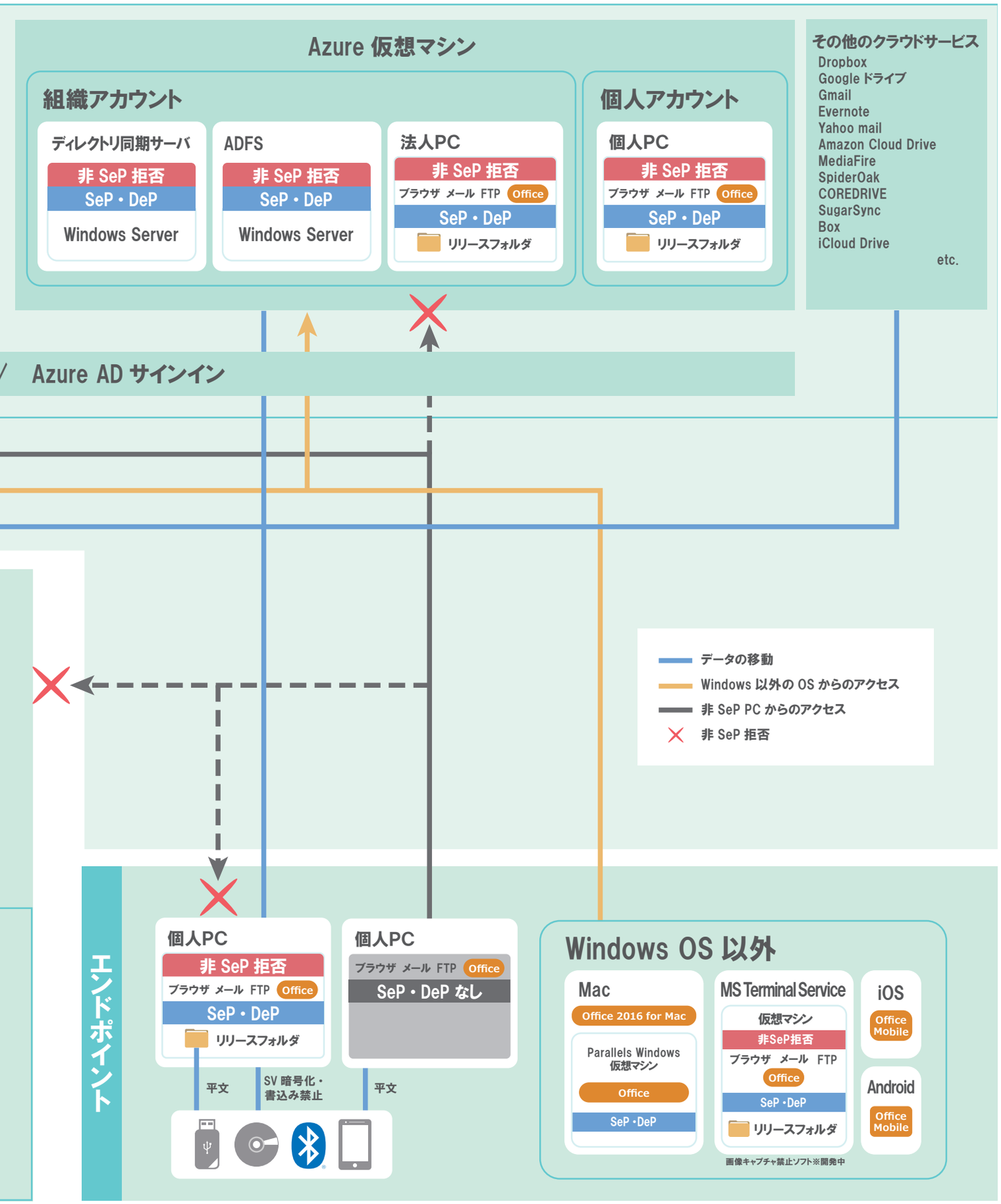
※旧名：Office 365

Microsoft 365・Azure の利用を想定したあらゆるシーンで情報を守る



Microsoft 365・Azure 利用で想定される情報の全経路図

会社の情報をまるごとクラウドに移動しても、セキュリティプラットフォーム・ディフェンスプラットフォームがインストールしてあれば、使い勝手を変えることなく、情報漏洩を完璧に防ぐことができます。社外の個人 PC からのアクセスや Azure、OneDrive 環境まで、あらゆる経路において網羅的にセキュアな環境を築きます。



SeP 操作履歴サンプル (Microsoft 365※ 操作)

※旧名：Office 365

	A	B	C	D	E	F	G	H	I
1	マシン	ファイル	フォルダパス	アプリケーション	ファイルサイズ	操作	ユーザ	日時	備考（持出し先　等）
2		メール件名	送信元、送信先メールアドレス		ウィンドウタイトル				備考（添付ファイル　等）
3		接続URL（ドメイン以降）	接続URL（ドメイン）						備考（アップロードファイル　等）
4	DEMO-PC			IEXPLORE.EXE(Outlook on the web)		Webアプリ起動(Web)	user01	2019/4/1 13:50:55	
5	DEMO-PC	/owa/?realm=hummingheads.co.jp#exsvurl=1&ll-cc=1041&modurl=0	outlook.office365.com	IEXPLORE.EXE	L<URL>メール - user01@hummingheads.co.jp - Internet Explorer	アクティブウィンドウ	user01	2019/4/1 13:51:18	23
6	DEMO-PC	報告書01.docx	C:¥Users¥user01¥Desktop¥デモファイル	IEXPLORE.EXE(Outlook on the web)	L<Local>Drag	メール添付(Web)(SV-暗号)	user01	2019/4/1 13:51:29	報告書01.docx.sve
7	DEMO-PC	/owa/?realm=hummingheads.co.jp#exsvurl=1&ll-cc=1041&modurl=0	outlook.office365.com	IEXPLORE.EXE	Size<13122>L<Local to URL>Drag	アップロード	user01	2019/4/1 13:51:29	C:¥Users¥user01¥Desktop¥デモファイル¥報告書01.docx
8	DEMO-PC	報告書の提出	user01@hummingheads.co.jp→hhdemo@gmail.com	IEXPLORE.EXE(Outlook on the web)		送信(Web)	user01	2019/4/1 13:52:47	報告書01.docx.sve
9	DEMO-PC	/Autodiscover/XFrame/XFrame.html	webdirjp1.online.lync.com	IEXPLORE.EXE		接続	user01	2019/4/1 13:52:50	86
10	DEMO-PC	/Autodiscover/XFrame/XFrame.html	webdirjp1.online.lync.com	IEXPLORE.EXE	L<Unknown>	編集履歴(インターネット)	user01	2019/4/1 13:52:50	報告書の提出¥TBメールを送信します。¥REご確認よろしくお願い致します。¥RE以上。
11	DEMO-PC			IEXPLORE.EXE(Outlook on the web)		Webアプリ終了(Web)	user01	2019/4/1 13:52:51	
12	DEMO-PC			IEXPLORE.EXE(SharePoint)		Webアプリ起動(Web)	user01	2019/4/1 14:10:18	
13	DEMO-PC	/sites/SharePoint-SVURL	saleshhdemo.sharepoint.com	IEXPLORE.EXE		接続	user01	2019/4/1 14:10:18	
14	DEMO-PC	/sites/SharePoint-SVURL	onhummingheads.sharepoint.com	IEXPLORE.EXE	L<URL>SharePoint - SV化URL - ホーム - Internet Explorer	アクティブウィンドウ	user01	2019/4/1 14:10:22	10
15	DEMO-PC	/sites/SharePoint-SVURL/Shared%20Documents/Forms/AllItems.aspx	saleshhdemo.sharepoint.com	IEXPLORE.EXE	L<URL>SharePoint - SV化URL - ドキュメント - すべてのドキュメント - Internet Explorer	アクティブウィンドウ	user01	2019/4/1 14:10:26	8
16	DEMO-PC	報告書01.docx	C:¥Users¥user01¥Desktop¥デモファイル	IEXPLORE.EXE(SharePoint)	L<Local to URL>	ファイルコピー(アップロード)(Web)(SV-暗号)	user01	2019/4/1 14:10:29	https://onhummingheads.sharepoint.com/sites/SharePoint-SVURL/Shared Documents/報告書01.docx.sve
17	DEMO-PC	/sites/SharePoint-SVURL/Shared%20Documents/Forms/AllItems.aspx	onhummingheads.sharepoint.com	IEXPLORE.EXE	L<URL>SharePoint - SV化URL - ドキュメント - すべてのドキュメント - Internet Explorer	アクティブウィンドウ	user01	2019/4/1 14:10:43	8
18	DEMO-PC	/sites/SharePoint-SVURL/Shared Documents/報告書01.docx.sve	onhummingheads.sharepoint.com	IEXPLORE.EXE(SharePoint)	L<URL to URL>	ファイル移動(Web)(SV-暗号)	user01	2019/4/1 14:12:02	https://onhummingheads.sharepoint.com/sites/SharePoint-SVURL/Shared Documents/Shared Documents/報告書01.docx.sve
19	DEMO-PC			IEXPLORE.EXE	L<Unknown>SharePoint - SV化URL - ドキュメント - すべてのドキュメント - Internet Explorer	アクティブウィンドウ	user01	2019/4/1 14:12:09	86
20	DEMO-PC	/sites/SharePoint-SVURL/Shared Documents/Shared Documents/報告書01.docx.sve	onhummingheads.sharepoint.com	IEXPLORE.EXE(SharePoint)	L<URL to URL>	ファイル名変更(Web)	user01	2019/4/1 14:12:36	https://onhummingheads.sharepoint.com/sites/SharePoint-SVURL/Shared Documents/Shared Documents/報告書A.sve.docx
21	DEMO-PC	/sites/SharePoint-SVURL/Shared Documents/Shared Documents/報告書A.docx.sve	onhummingheads.sharepoint.com	IEXPLORE.EXE(SharePoint)	L<URL>	ファイル削除(Web)	user01	2019/4/1 14:12:44	
22	DEMO-PC	/sites/SharePoint-SVURL/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2FSharePoint%2DSVURL%2FShared%20Documents%2FShared%20Documents	onhummingheads.sharepoint.com	IEXPLORE.EXE	L<URL>SharePoint - SV化URL - Shared Documents - すべてのドキュメント - Internet Explorer	アクティブウィンドウ	user01	2019/4/1 14:12:49	39
23	DEMO-PC	/sites/SharePoint-URL	onhummingheads.sharepoint.com	IEXPLORE.EXE	L<URL>SharePoint - 信頼URL - ホーム - Internet Explorer	アクティブウィンドウ	user01	2019/4/1 14:13:05	10
24	DEMO-PC	/sites/SharePoint-URL/Shared%20Documents/Forms/AllItems.aspx	saleshhdemo.sharepoint.com	IEXPLORE.EXE	L<URL>SharePoint - 信頼URL - ドキュメント - すべてのドキュメント - Internet Explorer	アクティブウィンドウ	user01	2019/4/1 14:13:10	8
25	DEMO-PC	報告書02.docx	C:¥Users¥user01¥Desktop¥デモファイル	IEXPLORE.EXE(SharePoint)	L<Local to URL>	ファイルコピー(アップロード)(Web)	user01	2019/4/1 14:13:15	https://onhummingheads.sharepoint.com/sites/SharePoint-URL/Shared Documents/報告書02.docx
26	DEMO-PC			IEXPLORE.EXE(SharePoint)		Webアプリ終了(Web)	user01	2019/4/1 14:13:30	

Microsoft 365
Outlook on the web

Microsoft 365
Share Point
非信頼領域

Microsoft 365
Share Point
信頼領域

27	DEMO-PC			IEXPLORE.EXE(OneDrive)		Webアプリ起動(Web)	user01	2019/4/1 14:10:51	
28	DEMO-PC	/_layouts/15/MySite.aspx?MySiteRedirect=AllDocuments	saleshhdemo-my.sharepoint.com	IEXPLORE.EXE		接続	user01	2019/4/1 14:10:51	
29	DEMO-PC	/personal/demo_saleshhdemo_onmicrosoft_com/_layouts/15/onedrive.aspx	saleshhdemo-my.sharepoint.com	IEXPLORE.EXE	L<URL>ファイル - OneDrive - Internet Explorer	アクティブウィンドウ	user01	2019/4/1 14:10:58	8
30	DEMO-PC	報告書03.docx	C:¥Users¥user01¥Desktop¥デモファイル	IEXPLORE.EXE(OneDrive)	L<Local to URL>	ファイルコピー(アップロード)(Web)(SV-暗号)	user01	2019/4/1 14:11:37	https://onhummingheads-my.sharepoint.com/personal/hummingheads_co_jp/Documents/ドキュメント/報告書03.docx.sve
31	DEMO-PC			IEXPLORE.EXE(OneDrive)		Webアプリ終了(Web)	user01	2019/4/1 14:11:50	

Microsoft 365 OneDrive

32	DEMO-PC			IEXPLORE.EXE(Word Online)		Webアプリ起動(Web)	user01	2019/4/1 14:20:36	
33	DEMO-PC	/personal/hummingheads_co_jp/Documents/報告書04.docx.sve	onhummingheads-my.sharepoint.com	IEXPLORE.EXE(Word Online)	L<URL>	ファイル参照(Web)	user01	2019/4/1 14:20:36	
34	DEMO-PC	/personal/demo_saleshhdemo_onmicrosoft_com/_layouts/WopiFrame.aspx?sourcedoc=%2Fpersonal%2Fdemo_saleshhdemo_onmicrosoft_com%2FDocuments%2F%E5%A0%B1%E5%91%8A%E6%9B%B802.docx.sve&action=default&CT=1553755920843&OR=DocLib	saleshhdemo-my.sharepoint.com	IEXPLORE.EXE	L<URL>報告書02.docx - Internet Explorer	アクティブウィンドウ	user01	2019/4/1 14:20:36	8
35	DEMO-PC	/personal/hummingheads_co_jp/Documents/報告書04.docx.sve	onhummingheads-my.sharepoint.com	IEXPLORE.EXE(Word Online)	L<URL to Local>	別名保存(ダウンロード)(Web)	user01	2019/4/1 14:20:40	C:¥Users¥user01¥Downloads¥報告書04 .docx
36	DEMO-PC	報告書04.docx	C:¥Users¥user01¥Downloads	IEXPLORE.EXE	Size<21239>L<Local>	ファイル参照	user01	2019/4/1 14:20:55	15
37	DEMO-PC	/personal/hummingheads_co_jp/Documents/報告書04.docx.sve	onhummingheads-my.sharepoint.com	IEXPLORE.EXE(Word Online)	L<URL>	印刷(Web)	user01	2019/4/1 14:21:45	user01@DEMO-PC-20190327-142145564
38	DEMO-PC	/personal/hummingheads_co_jp/_layouts/WopiFrame.aspx?sourcedoc=%2Fpersonal%2Fhummingheads_co_jp%2FDocuments%2F%E5%A0%B1%E5%91%8A%E6%9B%B802.docx.sve&action=default&CT=1553663944606&OR=DocLib	onhummingheads-my.sharepoint.com	IEXPLORE.EXE	L<URL>報告書02.docx - Internet Explorer	アクティブウィンドウ	user01	2019/4/1 14:21:47	70
39	DEMO-PC	/personal/hummingheads_co_jp/Documents/報告書04.docx.sve	onhummingheads-my.sharepoint.com	IEXPLORE.EXE(Word Online)	L<URL>	ファイル更新(Web)(SV-暗号)	user01	2019/4/1 14:22:42	
40	DEMO-PC			IEXPLORE.EXE(Word Online)		Webアプリ終了(Web)	user01	2019/4/1 14:22:43	

Microsoft 365 Word

41	DEMO-PC			lync.exe		プロセス起動	user01	2019/4/1 15:33:45	16.0.6001.1078
42	DEMO-PC	user01@hummingheads.co.jp	Skype for Business	lync.exe	Skype for Business	サインイン	user01	2019/4/1 15:33:45	user01
43	DEMO-PC	報告書03.docx	C:¥Users¥user01¥Desktop¥デモファイル	lync.exe	自宅用Skype for Business	ファイルアップロード(SV-暗号)	user01	2019/4/1 15:33:56	zitaku@hhdemo1.onmicrosoft.com
44	DEMO-PC	受信したファイル	C:Users¥demo¥Documents	lync.exe	自宅用Skype for Business	ディレクトリ作成	user01	2019/4/1 15:34:10	
45	DEMO-PC	zitaku@hhdemo1.onmicrosoft.com		lync.exe	自宅用Skype for Business	ファイルダウンロード	user01	2019/4/1 15:34:17	C:¥Users¥demo¥Documents¥受信したファイル¥報告書04.doc
46	DEMO-PC	報告書05.docx	C:¥リリースフォルダ	lync.exe	自宅用Skype for Business	ファイルアップロード(SV-リリース固定平文OUT)	user01	2019/4/1 15:34:25	zitaku@hhdemo1.onmicrosoft.com
47	DEMO-PC			lync.exe	自宅用Skype for Business	アクティブウィンドウ	user01	2019/4/1 15:34:25	11
48	DEMO-PC			lync.exe	PowerPoint を表示	アクティブウィンドウ	user01	2019/4/1 15:34:37	11
49	DEMO-PC	製品紹介資料.pptx	C:¥Users¥demo¥Desktop	lync.exe	自宅用Skype for Business	拒否-ファイルアップロード(SV-暗号)	user01	2019/4/1 15:34:35	Skype for Business
50	DEMO-PC			lync.exe	自宅用Skype for Business	アクティブウィンドウ	user01	2019/4/1 15:34:52	10
51	DEMO-PC			lync.exe	PowerPoint を表示	アクティブウィンドウ	user01	2019/4/1 15:35:04	9
52	DEMO-PC	製品紹介資料.pptx	C:¥リリースフォルダ	lync.exe	自宅用Skype for Business	ファイルアップロード(SV-リリース固定平文OUT)	user01	2019/4/1 15:35:16	Skype for Business

Microsoft 365 Skype for Business

エンクリプションオプション（自走式暗号ファイル化機能）

オプション

輸送経路を保護する

エンクリプションオプションの自走式暗号ファイル化機能は、ファイルまたはフォルダごと暗号化し、他者へファイルを渡す際のセキュリティを強化する機能です。暗号方式は 3DES・AES です。ファイルやフォルダを自走式暗号ファイル化するには対象をアクティブにし、マウス右クリックメニューより実行します。自走式暗号ファイルは、暗号化時に設定したパスワードを入力することによって復号されます。また、evolution /SV 機能を利用している場合は、リリース形式選択フォルダやリリース形式固定自走式暗号フォルダを利用することにより、メールや外部媒体にファイルを持ち出す際に自走式暗号ファイル化を確実に行う運用が可能です。

自走式暗号ファイル化

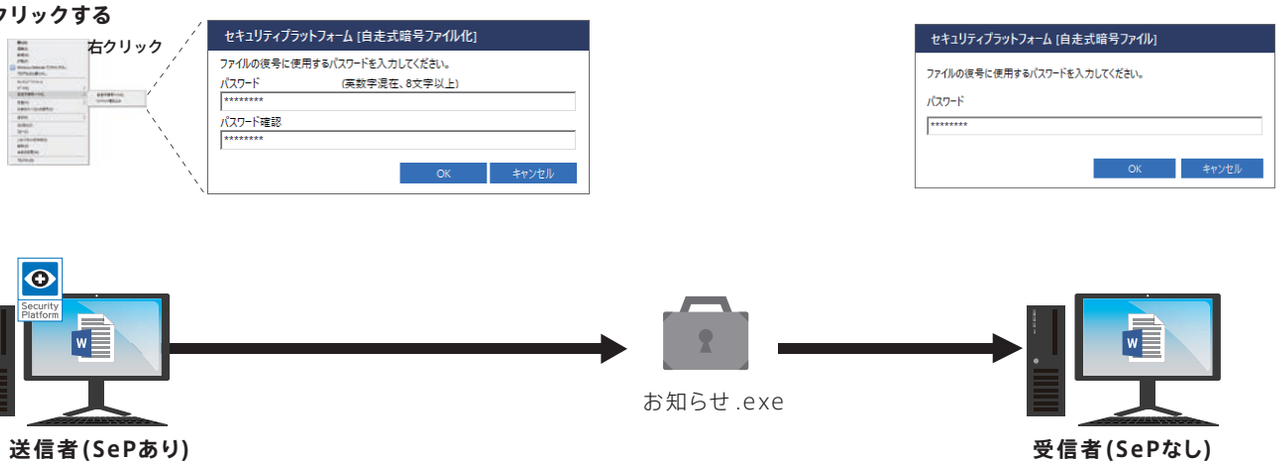
ファイルを選択し、「右クリック」→「自走式暗号ファイル化」→「自走式暗号ファイル化」メニューより作成します。

① ファイルまたはフォルダを右クリックする

② パスワードを入力する

③ 自走式暗号ファイル化

④ パスワードを入力し、復号する



パスワード付き ZIP ファイル化

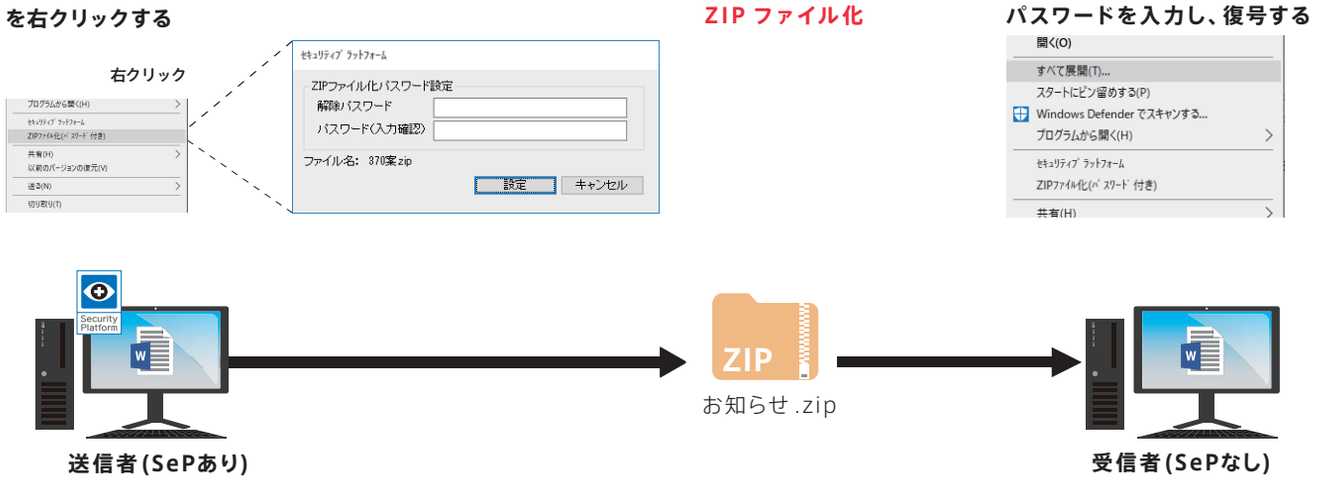
ファイルを選択し、「右クリック」→「ZIP ファイル化（パスワード付き）」メニューより作成します。

① ファイルまたはフォルダを右クリックする

② パスワードを入力する

③ パスワード付き ZIP ファイル化

④ ZIPファイル通常の復号方法でパスワードを入力し、復号する



ファイルセーフカプセルオプション

提携先からの二次情報漏洩を対策する

セキュリティを付与して、情報を外部へ提供することが可能になります

ファイルセーフカプセルオプションは、二次漏洩対策機能です。ファイルをカプセル化することで、社外のセキュリティプラットフォームがインストールされていない環境でも、印刷·保存·コピー＆ペースト·キャプチャーなどを禁止することができます。さらに起動条件として、ネットワークアドレス・メールアドレスなどの環境固有条件や、起動回数・期間などを設定でき、条件が合わない場合はファイルが削除されます。持ち出し時にはもちろん暗号化されるため、セキュリティが保たれます。

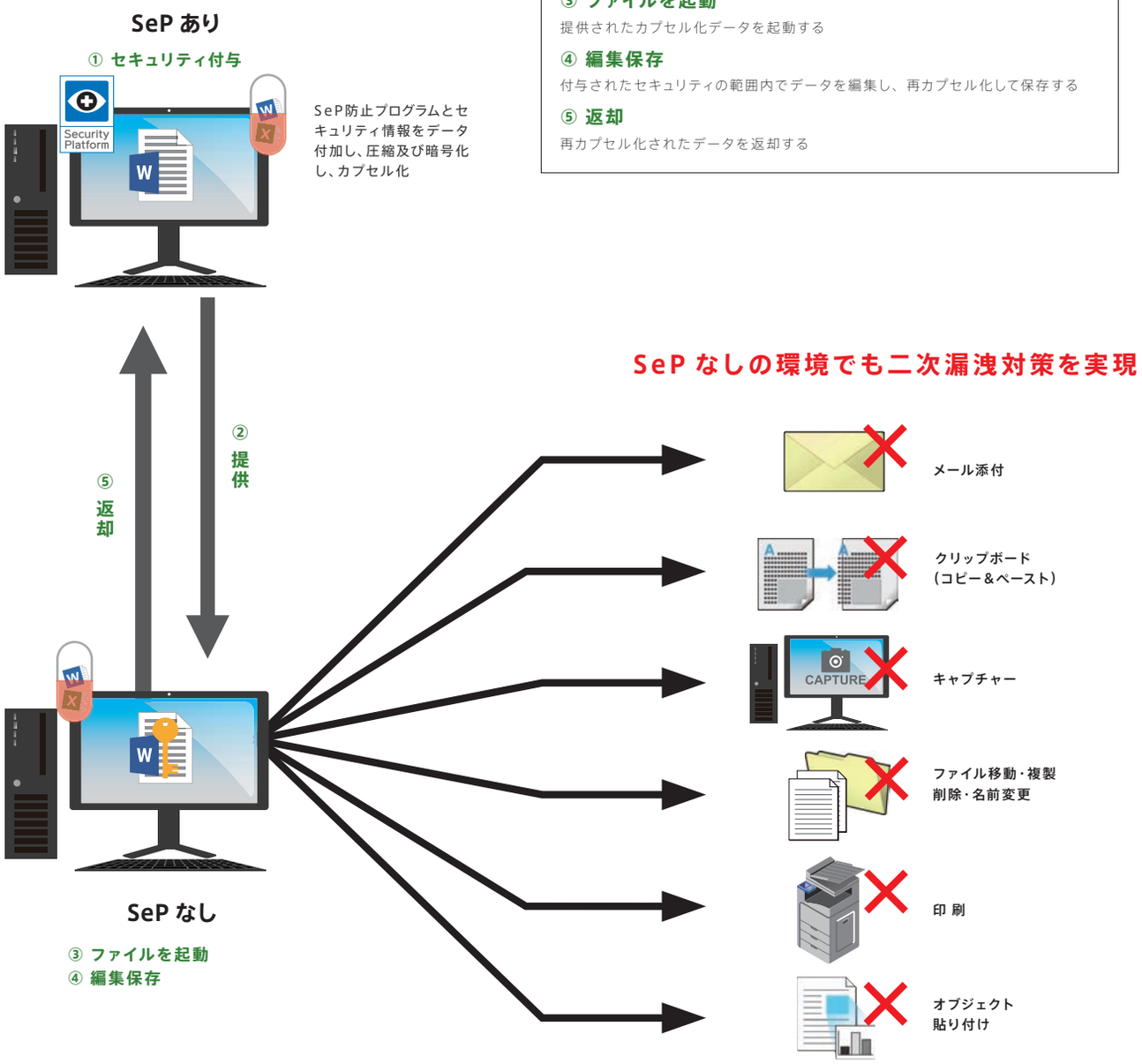
① セキュリティ付与
データファイルに対しセキュリティを付与し、カプセル化する

② 提供
メール及び外部媒体を利用してカプセル化されたデータを提供する

③ ファイルを起動
提供されたカプセル化データを起動する

④ 編集保存
付与されたセキュリティの範囲内でデータを編集し、再カプセル化して保存する

⑤ 返却
再カプセル化されたデータを返却する



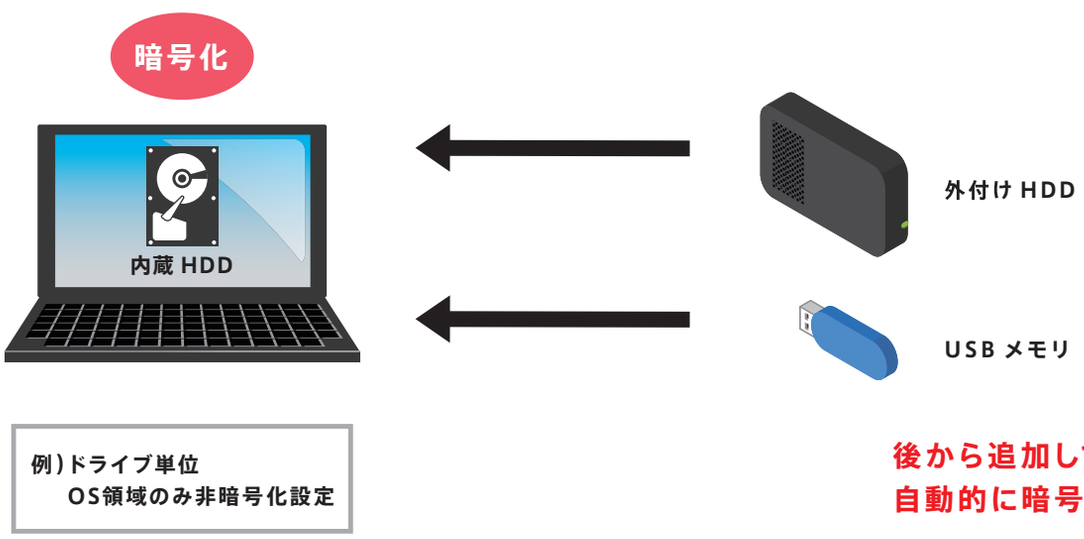
ストレージエンクリプションオプション

HDD・USBkey など 究極の暗号化

HDD・USBkey などのディスク全てを暗号化し、PC や外部媒体の置き忘れ・紛失・盗難に備えます。Windows の NTFS や FAT フォーマットされた記憶媒体を 3DES または AES で暗号化します。使用領域のみハード暗号化するため、高速な暗号化を実現しています。導入負荷を可能な限り軽減します。

PC 内の HDD を全て暗号化
PC 内の指定したドライブ領域を暗号化
USB メモリ・外付け HDD を暗号化

全体を暗号化した後で USB や外付け HDD を追加した場合でも、
外部媒体を認識すると、自動的に暗号化を行います。



詳細

暗号方式
3DES（168bit 相当）
AES（128bit、192bit、256bit）
記憶媒体（ストレージ）
HDD（IDE、SCSI、USB）
USB メモリ
フォーマット
FAT（16、32）
NTFS

認証
Windows ログオン認証
Windows 起動前パスワード認証
SeP サーバ認証
その他特長
Windows 領域暗号・非暗号可能
使用領域のみハード暗号
外部媒体に対する plug&play 対応
クライアント・サーバ型ポリシー設定
導入時、バックグランド暗号化対応

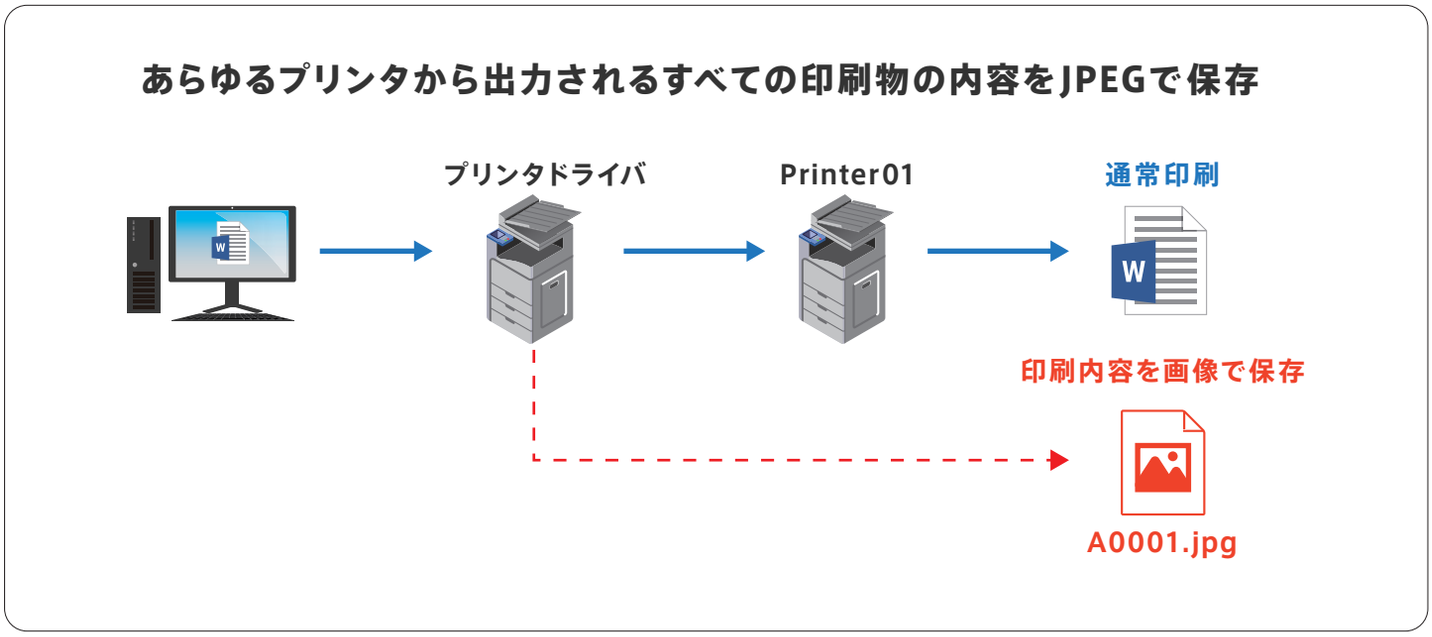
対応 Windows（クライアント）
Windows NT、Windows 2000、
Windows XP、Windows 7、
Windows 8、Windows 8.1、
Windows 10、Windows 11
※ サーバOSにも対応予定です。

セキュア印刷オプション

印刷物の統制をエンドポイントで強化

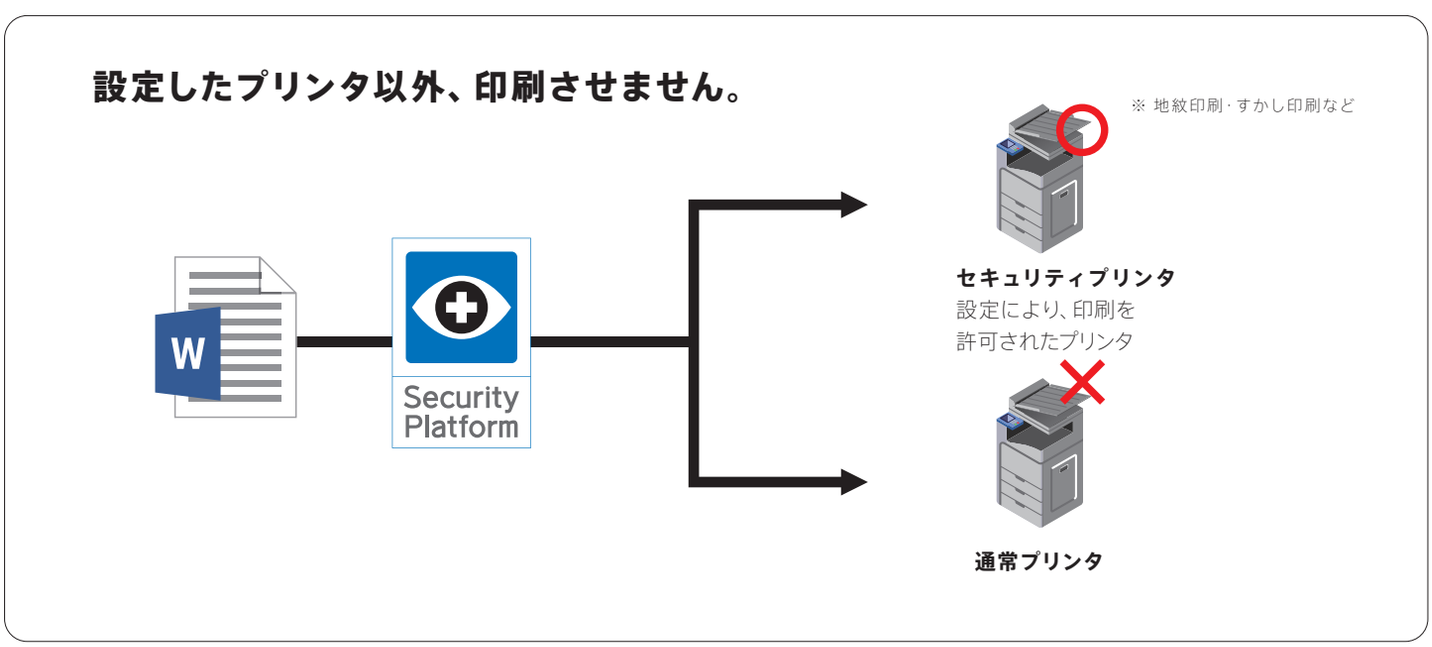
印刷物の内容を JPEG で保存

セキュア印刷オプションは、あらゆるプリンタから出力されるすべての印刷物に対して、印刷した内容を JPEG 形式の画像ファイルとして保存することができるようにする機能です。



セキュリティプリンタのみ印刷を許可

またほかにもセキュア印刷オプションは、指定したプリンタのみから印刷できるようにする機能も備えています。地紋や透かし、隠し印刷などが行なえるセキュリティ機能を搭載したプリンタのみを選択できるようにすることで、印刷に関するセキュリティを向上できます。



編集履歴オプション

ファイル、Web、メールでの入力文字の履歴を出力

入力した文字を丸ごとキャッチ すべてのアプリケーションの履歴を出力

編集履歴オプションは、従来 SeP が出力する履歴に加え、ファイル、メールの編集やインターネットへのアップロードなどの際に必要なキーボードストロークを履歴として出力する機能です。プロセス単位で、全てのアプリケーションについて履歴を取得するオプションです。
インターネット上の掲示板へのアップロードも、書き込んだ文字すべてが履歴として記録されるので、「いつ」「誰が」「どの PC から」「どこのサイトへアクセスしたか」だけではなく、「どのような内容を書き込んだか」が一目瞭然です。
また、プロセス単位ですべてのアプリケーションについて履歴を取得するため、強力な証跡としても有効活用することができます。個人が最新ファイルを探したい場合には、履歴から検索することですぐに見つけることができるので、ファイル管理にも効果を発揮します。
この特長により、自社業務の正当性を容易に証明し、内部統制も強化できます。編集履歴オプションは、SeP サーバ編集履歴オプションと SeP クライアント編集履歴オプションを併せて使用することで、ユーザが行った編集内容等の操作履歴を出力します。

特長

- **PC単位ではなく、ファイル単位でのキー入力の履歴取得が可能。**
- **Webページへのキー入力の履歴取得が可能。**
- **送信したメール本文の編集内容を履歴として取得可能。**
- **英数字だけではなく、日本語入力での履歴取得が可能。**

機能

ユーザ操作履歴出力機能

ユーザが行うファイル、メール、またはインターネット上でのキー操作履歴を出力する機能です。この履歴では、CSV出力できないキー(タブキー等)も対象とすることができます。

プロセス単位の履歴出力機能

コマンドの入力履歴などをプロセス単位で取得可能。プロセス単位の履歴はあらゆるアプリケーションについて取得することができます。
※ 一部のアプリケーションについては詳細に動作を確認しております。

クリップボード詳細履歴出力機能

コピーまたはカットしたテキストデータを、クリップボード経由でペーストした際、そのテキストデータを履歴に出力することができます。

履歴出力対象指定機能

編集履歴を出力する対象、または出力を除外する対象として、ユーザ、PC、アプリケーションを指定することができます。

サーバ設定機能

サーバにおいて、機能の設定を行うことができます。
※ サーバ設定機能は、SePサーバ編集履歴オプションのみの機能です。

履歴上限サイズ指定機能

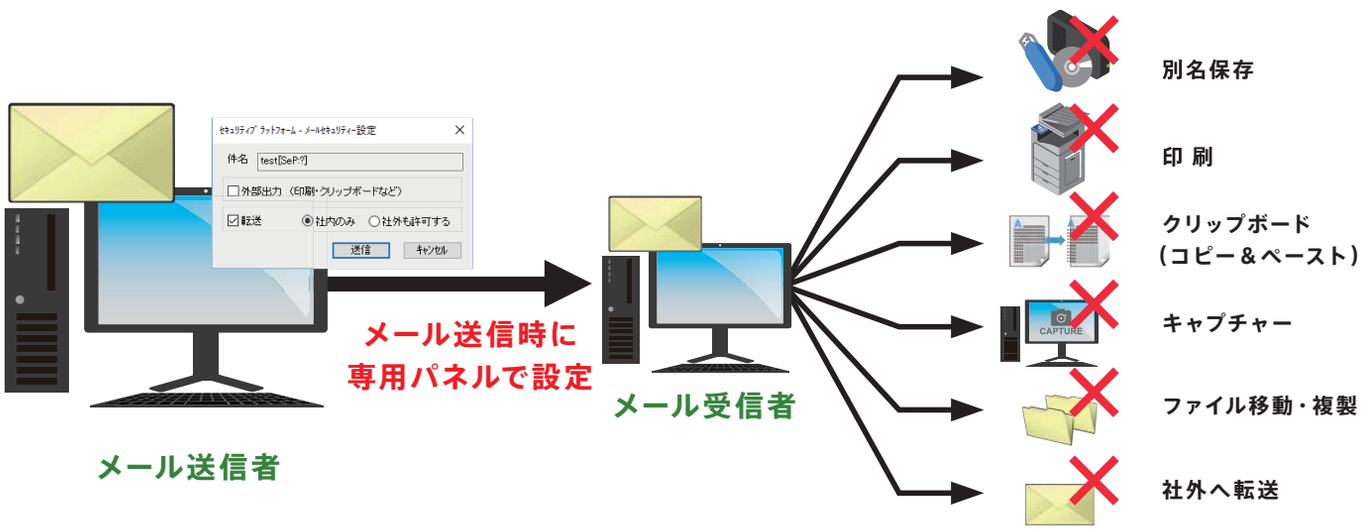
ユーザ操作履歴やクリップボード詳細履歴について、出力する編集内容の上限サイズを設定することが可能。履歴データ量が多い場合、すべてのデータを出力させず、指定した編集内容のサイズまで出力させることができます。

メールオプション

オプション

送信者が受信者の操作を制限する

メールオプションは、メール本文からの情報漏洩を防止するための機能です。メール送信者は、送信時に表示されるパネルにより、メールへの印刷や保存、転送などの制限設定を行ないます。この設定により、受信者の操作は制限され、外部出力や社外への転送が禁止されます。



セキュリティ設定：メールセキュリティ設定パネルの文言を変更することができます。
※ 文言は ini ファイルに記述

※ 添付ファイルや転送したメールにも、設定が継承されます。

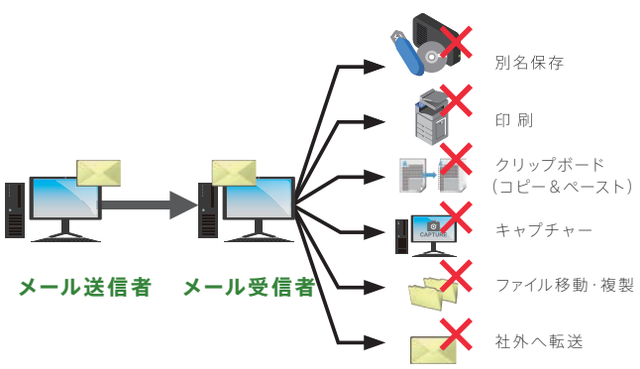
グループウェア用オプション

オプション

グループウェア上の共有文書に対するセキュリティを強化する

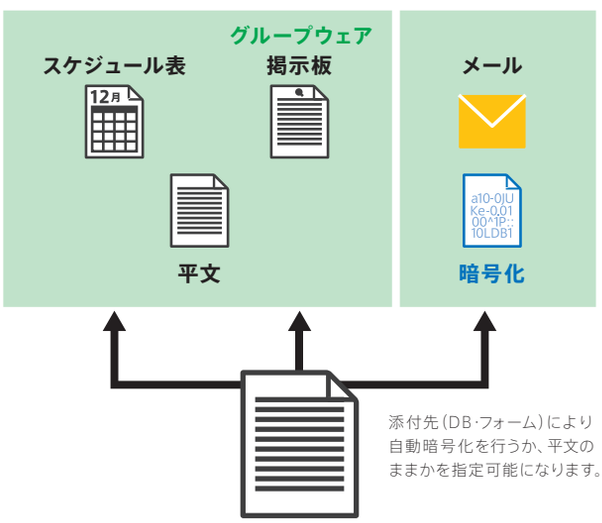
GW Domino サーバオプションおよび GW Exchange サーバオプションは、メールオプションに機能を追加するオプションです。対応しているグループウェアはそれぞれ Domino と Exchange です。グループウェアメールや掲示板などの共有している文書に対してセキュリティを付与し防止することができます。また、evolution /SV 機能を利用している場合は、本オプションを導入することによってデータベースやフォームごとにファイル添付時に SV 暗号化を行うか否かを選択できるようになります。

グループウェアメールに対する防止機能を提供します。



※本製品はメールオプションと共に使用するオプションです。ご利用になるためには、メールオプションが必要です。
※対応グループウェア…Domino、Exchange　※GWはゲートウェイの略称です。

evolution /SV使用時の機能



添付先（DB・フォーム）により自動暗号化を行うか、平文のままかを指定可能になります。

トレーサオプション

オプション

クライアントＰＣの操作履歴を収集する

SeP の履歴は、操作が行われた PC 内に暗号化して一時保管後、設定したタイミング（ユーザログオン時、Windows 起動・終了時、指定した時間間隔など）で、クライアントから指定した SeP サーバへ送信の上、保管されます。トレーサオプションは、その SeP サーバに集積された操作履歴を収集・復号し、CSV 形式のファイルとして出力します。トレーサオプション起動時には、パスワード認証が必要です。尚、リアルタイムで操作履歴を扱いたい場合は、リアルタイム履歴通知オプションが必要です。詳しくは、下記のリアルタイム履歴通知オプションをご参照下さい。

履歴集積のタイミング

1. クライアントログオン時
2. Windows起動時・終了時
3. 指定時間毎
4. 履歴サイズが一定量に達した時
5. クライアントアンインストール時

Step1：集積

SePクライアント

クライアントに記録された履歴が、サーバに集積（送信）されます。その後クライアントの履歴は削除されます。

Step2：収集

SePサーバ

クライアントから集積した履歴や、サーバ自身の操作履歴が、履歴管理用PCへ収集されます。

Step3：出力

履歴管理用PC

トレーサオプションで各サーバから収集した履歴を復号し、CSV形式ファイルで出力します。

CSV形式

※履歴が集積されるサーバを指定することができます。
※スタンドアロン PC はサーバに接続し、履歴が集積されるまでローカルに蓄積され続けます。

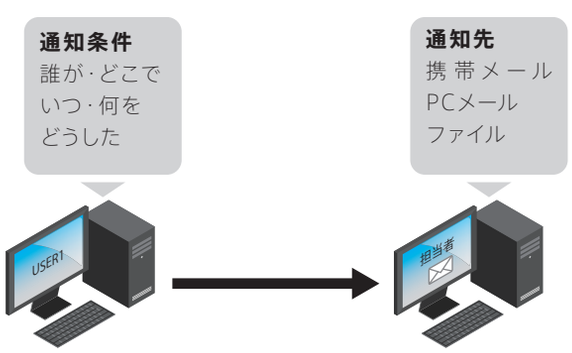
リアルタイム履歴通知オプション

オプション

クライアントＰＣの操作履歴をリアルタイムに通知する

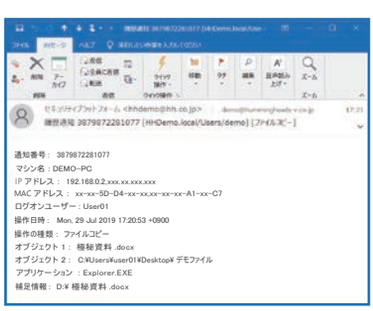
SeP はお使いのアプリケーションに対して、全ての操作を網羅的に記録します。その履歴をリアルタイムで管理者へ通知する機能です。「誰が（ログオンユーザ）」「いつ（マシン Date：Time）」「何処で（PC 名・MAC アドレス・IP アドレス）」「何を（ファイル・URL）」「どの様に（操作）」などが通知条件として指定できます。
通知形式は E メール・携帯メール・指定したファイルへの書き込みです。

条件に一致するとリアルタイムに通知

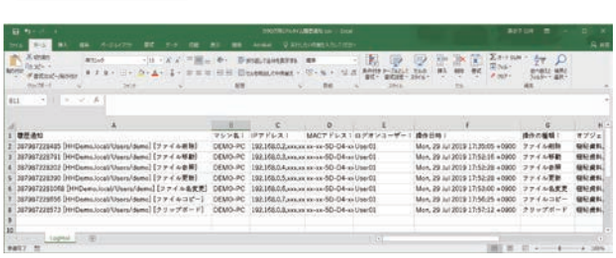


通知例

Eメール



ファイル

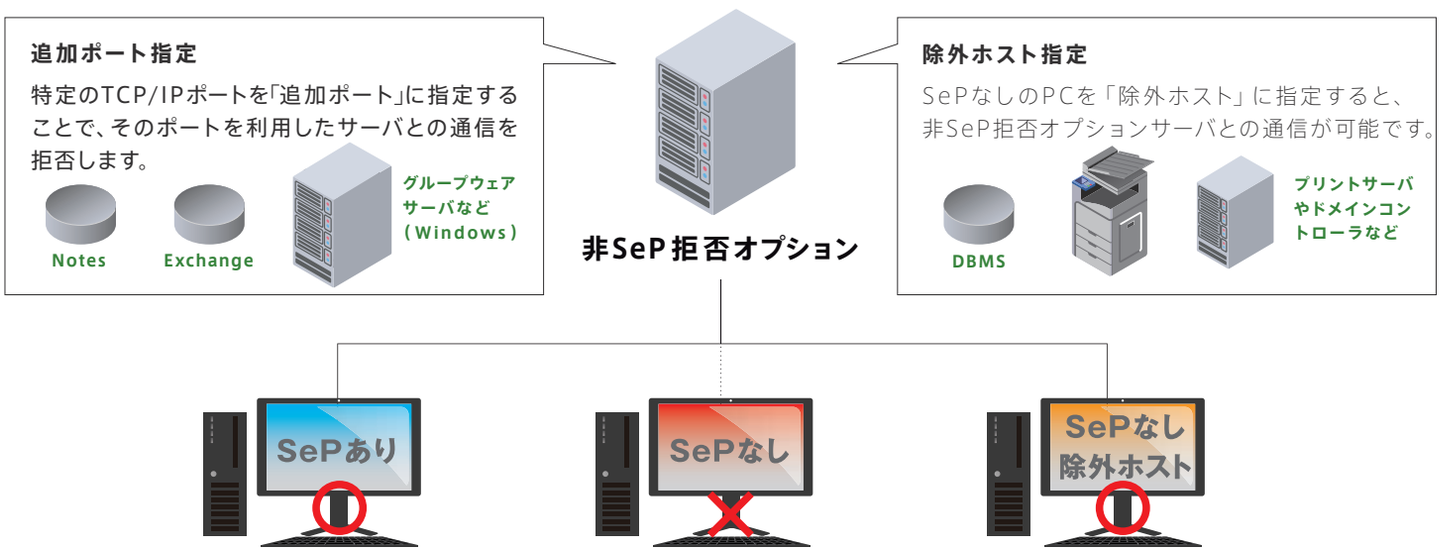


非 SeP 拒否オプション

オプション

SeP 未搭載の PC からのアクセスを拒否

非 SeP 拒否オプションは、SeP 未搭載の PC から SeP 搭載済の PC へのアクセスを拒否する機能です。このオプションはサーバにインストールして使用します。SeP 未搭載の、プリントサーバやドメインコントローラなどといったマシンで、非 SeP 拒否オプションが導入された SeP サーバと通信する必要がある場合には、これらを“除外ホスト”として設定することができます。



監視除外アプリケーション機能

基本製品・機能

監視が不要なアプリケーションを指定してスムーズな運用

監視除外アプリケーションとは、SeP の防止機能や履歴出力機能のための監視を行わないアプリケーションのことです。
通常、システムプログラムやウイルス対策ソフトなど、情報漏洩対策のために監視を行う必要がないアプリケーションを指定します。この機能により、環境に応じたスムーズな運用が可能になります。また、防止は行わず、履歴のみを取得するアプリケーションを指定することも可能です。

監視対象および監視除外アプリケーションに対する防止と履歴

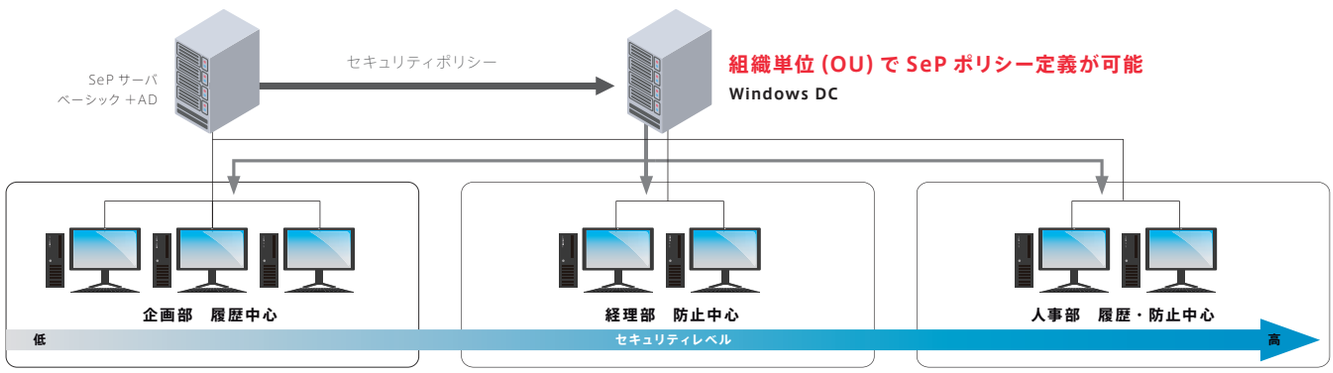
対象アプリケーションの組み合わせ		防止機能	履歴機能
監視しているアプリケーション		○	○
監視除外しているアプリケーション	履歴を出力する除外アプリケーション	×	○
	履歴を出力しない除外アプリケーション	×	×

Windows アクティブディレクトリ（AD）対応版

セキュリティプラットフォーム クライアント ベーシック +AD evolution /SV　セキュリティプラットフォーム サーバ ベーシック +AD evolution /SV

AD 環境下でも、情報漏洩を防止する

セキュリティプラットフォーム+ADは、WindowsのActive Directory（AD）環境で強固なセキュリティを実現できる情報漏洩対策ソフトウェアです。ネットワーク上のハードウェアを一元管理できるAD環境下で、いままで内部からの情報漏洩を防止する強力なセキュリティソフトウェアはありませんでした。そこで、このセキュリティプラットフォーム+ADは、AD環境下の組織単位（OU）のセキュリティ環境設定を可能にし、部署ごとに異なる段階的セキュリティポリシーを有する組織に対して、柔軟に対応します。主な特長は、AD環境下において組織・グループ単位で管理されたユーザの操作履歴を網羅的に取得することです。これにより、履歴取得の手順が簡素化され、業務分析、効率改善に大きく役立ちます。また、サーバ設定のパラメータでサイト、ドメイン、OUごとの設定ができます。ADとグループポリシーを連携することで、SePのポリシーを社内のポリシーとして適用できます。その際、クライアントPCの設定、管理は一元的に行えます。また、AD環境内に複数のOSが混在していても、1台のサーバで管理できます。



すべての PC 操作を記録し、網羅的な履歴を取得

ユーザによるPC操作のすべてを記録し、履歴を網羅的に取得します。組織・グループ単位で管理されたユーザ名が表示されるので、情報漏洩防止、業務分析などに役立ちます。

操作履歴例

操作履歴のユーザ名欄に組織名が付加されます。

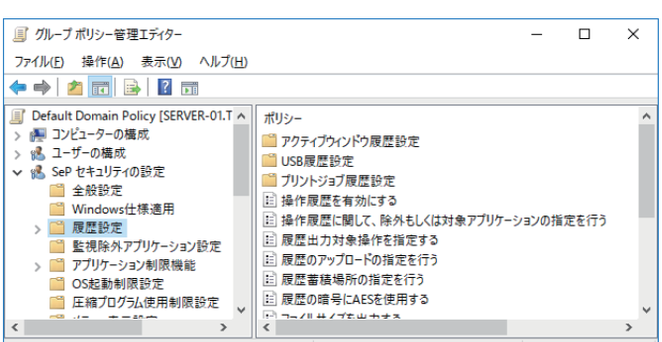
マシン	ファイル メール件名 接続URL（ドメイン以降）	フォルダパス 送信元、送信先メールアドレス 接続URL（ドメイン）	アプリケーション	ファイルサイズ ウィンドウタイトル	操作	ユーザ	日時	備考（持出し先　等） 備考（添付ファイル　等） 備考（アップロードファイル　等）
DEMO-PC	報告書01.docx	C:¥Biz¥リリース形式選択フォルダ	OUTLOOK.EXE	Size<14582>L<Local>	メール添付(SV-リリース選択平文OUT)	Domain.co.jp/営業部/user01	2019/7/29 18:43	報告書01.docx
DEMO-PC	報告書について[SeP:?]	user01@hummingheads.co.jp → customer	OUTLOOK.EXE	報告書について - メッセージ (HTML 形式)	送信	Domain.co.jp/営業部/user01	2019/7/29 18:52	報告書01.docx
DEMO-PC	駅前再開発案.pptx	C:¥Users¥user01¥Desktop	POWERPNT.EXE	Size<932656>L<Local>駅前再開発案	印刷	Domain.co.jp/営業部/user01	2019/7/29 18:59	user01@DEMO-PC-20190729-185906224
DEMO-PC	営業週報.docx	C:¥Users¥user01¥Desktop¥デモファイル	IEXPLORE.EXE	Size<14819>L<Local>	メール添付	Domain.co.jp/営業部/user01	2019/7/29 19:17	営業週報.docx
DEMO-PC	/mail/u/0/#inbox/KtbxLthqD	mail.google.com	IEXPLORE.EXE	Size<14819>L<Local to URL>	アップロード	Domain.co.jp/営業部/user01	2019/7/29 19:17	C:¥Users¥user01¥Desktop¥デモファイル¥営業週報.docx
DEMO-PC	営業月報10月.docx	D:	WINWORD.EXE	L<Unknown to USB>	拒否-ファイル書き込み(SV-Write制限)	Domain.co.jp/営業部/user01	2019/7/30 19:45	
DEMO-PC	2019年8月発注書.xlsx	¥¥FileServer¥2019¥発注書	EXCEL.EXE	Size<9360>L<NetworkDrive>	ファイル参照	Domain.co.jp/営業部/user01	2019/7/31 19:51	31

主な機能

SePサーバ設定がADに対応

サーバ設定ツールのパラメータをサイト、ドメイン、OUごとに設定可能です。ADとグループポリシーを連携させることで、SePのルールを社内のポリシー設定として円滑に適用できます。

階層表示例



セキュリティ設定パネルがADに対応

セキュリティ設定時のユーザ/グループ表示がツリー表示されます。

AD（ネイティブ）のアクセス権追加機能への対応

グループのネストに対してアクセス権が設定できます。

サーバ設定ツールのADへの移行ツール

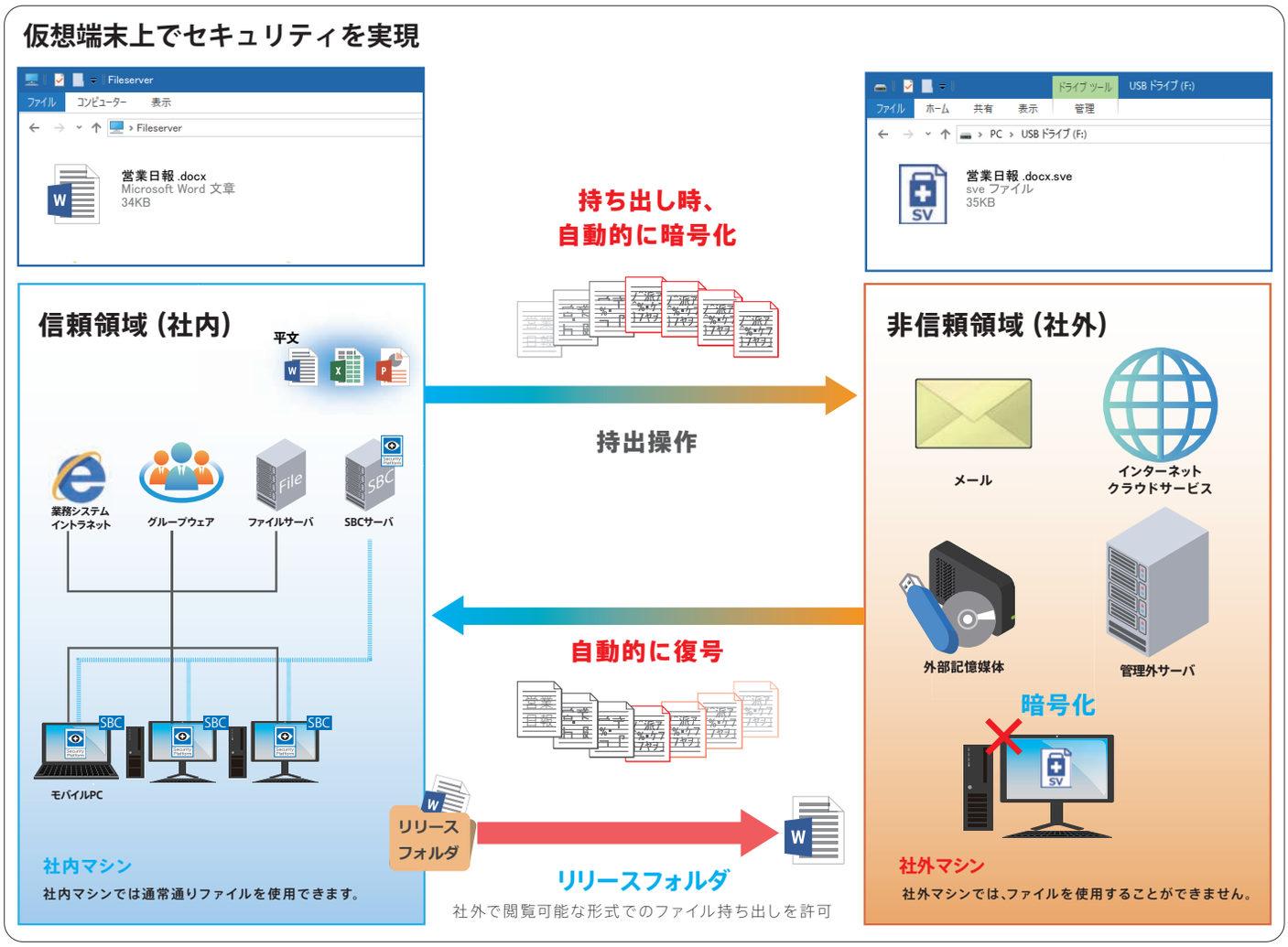
サーバ設定ツールの定義をAD環境へ移行することができます。

SBC 方式仮想環境対応版

セキュリティプラットフォーム サーバ ベーシック evolution /SV for TS/MF　セキュリティプラットフォーム クライアント ベーシック evolution /SV for TS/MF

仮想端末環境でも情報漏洩を防止

SBC（Server Based Computing）方式仮想環境対応版は、リモートデスクトップサービスや XenApp などの仮想端末上で、通常のサーバ・クライアント環境と同様に SeP の機能を利用できます。



仮想端末から物理端末へのファイルコピー禁止または自動暗号化

ファイルコピーが禁止されている場合、仮想端末から物理端末へのファイルコピーを禁止します。社内（ドメイン内もしくは信頼領域）のファイルを仮想端末から社外 (ドメイン外もしくは非信頼領域) の物理端末へコピーすると、暗号化が自動的に行われ、社外（ドメイン外もしくは非信頼領域）では使用できなくなります。

仮想端末からクリップボード経由で物理端末へのカット・コピー & ペースト防止

クリップボードが禁止されている場合、社内（ドメイン内もしくは信頼領域）のファイルをクリップボード経由で仮想端末から社外（ドメイン外もしくは非信頼領域）物理端末へペーストすることを禁止します。

物理端末での仮想端末に対するキャプチャー防止

物理端末から仮想端末に対するキャプチャーを防止します。

鍵生成シードの更新対応

セキュリティプラットフォーム サーバ ベーシック evolution /SV for TS/MF　セキュリティプラットフォーム クライアント ベーシック evolution /SV for TS/MF

鍵生成シードの更新（追加・破棄）が可能に

ニーズにあわせて鍵生成シードを追加・破棄。万が一の事態に備えることが可能

セキュリティプラットフォームによるファイルの暗号化では、ファイルごとに異なる暗号キーが使用されています。したがって、万が一特定のファイルの暗号キーが第三者に解読されても他の暗号化ファイルが復号されることはありません。このように、既にセキュアな環境が実現されていますが、各企業様のセキュリティポリシーに基づいて「暗号キーおよび鍵生成シードを更新したい」というニーズにもお応えします。

※鍵生成シードとは、暗号化を行う際に暗号キーを生成するための元となる値です。
本サービスでは以下の「追加」と「破棄」が可能です。

鍵生成シードの追加

鍵生成シードを追加すると、追加した鍵生成シードが暗号キーを生成するようになります。なお、シードの追加後も、古い鍵生成シードが生成した暗号キーによる暗号化ファイルの復号は可能です。

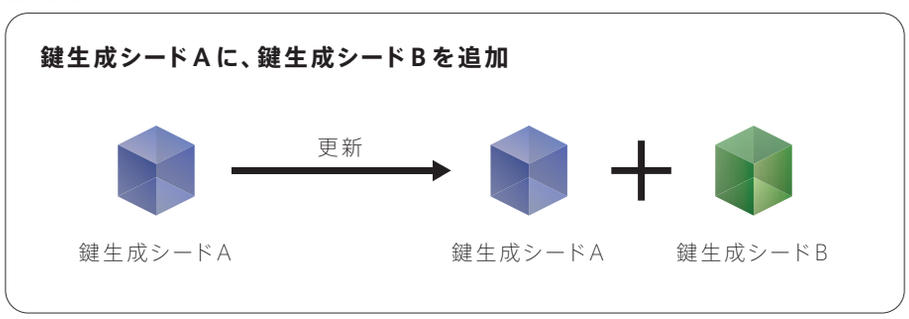
鍵生成シードの破棄

鍵生成シードを破棄すると、そのシードが既に生成した暗号キーを使用しての暗号化されたファイルの復号はできなくなります。

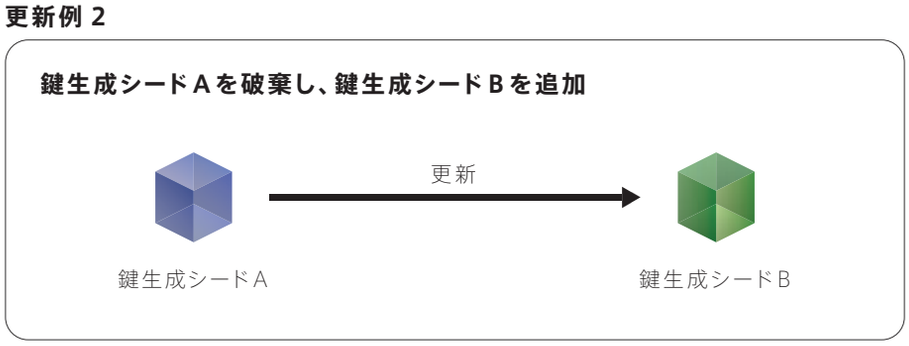
対応する暗号化機能

・evolution /SV 機能による SV 暗号化
・エンクリプションオプション機能による自動暗号化

更新例 1



更新例 2



※本機能は、Ver.1.9.40 以降のベーシック evolution /SV 製品、ベーシック +AD evolution /SV 製品、ベーシック evolution /SV for TS/MF 製品のいずれかが導入されている場合にご使用可能です。

製品名・オプション

様々な環境に対応、ワンランク上の情報漏洩対策へ

基本製品名

サーバ

セキュリティプラットフォーム サーバ ベーシック evolution /SV
セキュリティプラットフォーム サーバ ベーシック +AD evolution /SV
セキュリティプラットフォーム サーバ ベーシック evolution /SV for TS/MF

クライアント

セキュリティプラットフォーム クライアント ベーシック evolution /SV
セキュリティプラットフォーム クライアント ベーシック +AD evolution /SV
セキュリティプラットフォーム クライアント ベーシック evolution /SV for TS/MF

オプション

製品名	機能	サーバ	クライアント
トレーサオプション	サーバに収集された操作履歴を復号化し CSV 形式ファイルに出力する	○	
イントラネットオプション	インターネット、イントラネットに対しての 不正防止機能を強化する	○	○
エンクリプションオプション	ファイル持ち出し時にパスワード付き ZIP、 自走式暗号化を選択可能にする	○	○
ストレージエンクリプションオプション	ハードディスク、外部媒体を暗号化する	○	○
メールオプション	メール本文や添付ファイルに対して 不正防止機能を有効にする	○	○
DWA オプション	iNotes 環境でイントラネットオプション機能を利用可能にする ※イントラネットオプションが必要です		○
リアルタイム履歴通知オプション	クライアント、サーバ PC の指定操作を リアルタイムで通知	○	○
編集履歴オプション	入力した文字を操作履歴として出力	○	○
非 SeP 拒否オプション	SeP 未インストールマシンの接続を拒否	○	
ファイルセーフカプセルオプション	持ち出しファイルに対する二次漏洩対策	○	○
セキュア印刷オプション	印刷内容を画像ファイルで出力し、 プリンター使用を制限する	○	○
認証オプション	特定の操作を行う時に、スマートカードによる 認証を要求する	○	○
サーバ設定オプション	サーバ設定を管理者用クライアントから 遠隔操作する		○
ディフェンスオプション	ホワイトリスト型サイバー攻撃対策の機能を追加し、 関連する履歴を追加で取得する	○	○
セパレートオプション	業務ごとにサーバ設定の内容（ポリシー）を もつことができ、１台の PC 上で切り替えられる	○	○
サイバーハイジーンオプション	アップデート、動作検証、脅威の検知・可視化・防止、 PC 環境最適化を管理者に代わり全て自動的に行う	○	○

※オプション製品の正式名称は、オプション名の前に以下の文字列を追加したものとなります。（トレーサオプションを除く）
サーバ製品→セキュリティプラットフォーム サーバ（例：セキュリティプラットフォーム サーバ イントラネットオプション）
クライアント製品→セキュリティプラットフォーム クライアント（例：セキュリティプラットフォーム クライアント イントラネットオプション）
※ +AD evolution /SV 用のトレーサーオプション、サーバ設定オプションの名称には、末尾に +AD が追加されます。
例：セキュリティプラットフォーム トレーサーオプション +AD

Humming HEADS®
開発・販売元 ハミングヘッズ株式会社

〒134-0083 東京都江戸川区中葛西5-38-8　Tel.03-6808-1300 Fax.03-5679-7720
sales@hummingheads.co.jp　http://www.hummingheads.co.jp/

お問い合わせ先

23081031