

kaspersky

**カスペルスキーディスク暗
号化サービス**

概要

このドキュメントでは、カスペルスキーのエキスパートが提供するディスク暗号化サービスについて説明します。ディスク暗号化サービスは、合意した作業範囲内で、お客様の環境において効果的なディスクおよびファイルの暗号化の実施を目標としたサービスです。

対象範囲

最大で 20 ディスク または 20 ファイル

サービスタイムライン

注：本サービスでは、前述の目標を達成するための作業時間として最大 8 時間が割り当てられ、最大でディスク 20 台または 20 ファイルを対象とすることができます。すべてが実施され、お客様の了承を得た場合、作業時間が 8 時間未満であっても、プロジェクトは「完了」となります。

サービスには、HDD、ファイル、およびリムーバブルドライブの暗号化が含まれ、以下のステージに分けられます：

初期段階	暗号化サービス	最終段階
キックオフ、暗号化の概念について説明	認証エージェントのオプションの設定およびディスク全体の暗号化モジュールの導入。設定後、コンピューターの再起動が必要です	HDD およびリムーバブルドライブ全体の暗号化、その後の使用に関する説明
必要な環境のチェック（リモートアクセス、FDE テストユーティリティの結果、ネットワーク通信、ライセンス）	以下のデモンストレーションおよび説明： <ul style="list-style-type: none"> タスクを作成して、認証エージェントのアカウントを管理する方法 認証エージェントのアカウントを表示するレポートを設定する方法 チャレンジレスポンス方式 ディスクの復号方法とステータスが表示される場所 ファイル暗号化の運用原則 ポリシーでのファイル暗号化ルール 	
ディスク暗号化の仕様および認証エージェントの仕組みの説明 注：事前に Kaspersky Security Center をバックアップしておく必要があります。このサービスに含まれている作業時間では、セキュリティのエキスパートがお客様に	<ul style="list-style-type: none"> ファイルレベルの暗号化モジュールの導入（コンピューターの再起動が必要な場合があります）。 暗号化されたパッケージの使用に関するデモおよびリムーバブルドライブの暗号化の種類に関する説明。 ファイルの暗号化と、暗号化されたファイルの組織内および組織外への転送方法に関する説明。 	

代わってこの作業を実行する十分な時間を確保できません。

要件および声明

以下に記載された要件が完全に満たされていない場合、カスペルスキーはこのサービスを提供、または提供を試みる義務を負わないことにご注意ください。これらの要件のいずれかが問題となる可能性がある場合は、速やかにご連絡ください。

1. 本サービスはリモートで提供され、各 4 時間の 2 回に分割される場合があります。
2. リモートサポート Zoho Assist ツールで使用される TCP ポート 80 および 443 の解放（要件の詳細については、<https://www.zoho.com/assist/kb/firewall-configuration.html> を参照ください）。
3. サービス提供中は、カスペルスキーのエンジニアからの妥当な要求（権限やアクセス権などを含む）に対応するために、お客様の IT 部門またはセキュリティチームの代表者と常に連絡できる状態であること
4. 環境に Kaspersky Endpoint Security (Advanced 以上のライセンス)、Kaspersky Security Center、および Kaspersky Network Agent がインストールされていること
5. Kaspersky Security Center の最新バージョンの要件を満たしていること
要件は以下を参照ください：（ページ右上でアプリケーションのバージョンを選択してください）
 - a. システム要件：<https://support.kaspersky.com/KSC/14/ja-JP/96255.htm>
 - b. DBMS に使用するアカウント：<https://support.kaspersky.com/KSC/14/ja-JP/156275.htm>
 - c. Kaspersky Security Center で使用するポート：<https://support.kaspersky.com/KSC/14/ja-JP/158830.htm>
6. Kaspersky Security Center がインストールされているサーバーおよび暗号化の対象となる各コンピューターにリモートアクセスを実行できること
7. サービス提供中に、必要に応じて複数回の再起動を行います。常にコンピューターが使用可能な状態になっていること
8. Kaspersky Network Agent が Kaspersky Security Center と制限なく通信できること
9. ディスク全体の暗号化が適用されるデバイスは、FDE テストユーティリティで互換性があると確認されること詳細については、<https://support.kaspersky.co.jp/14328> を参照ください。
10. Kaspersky Security Center がインストールされたサーバーで、バックアップを保存するのに十分な空き容量詳細については、<https://support.kaspersky.com/KSC/13/ja-JP/3673.htm#block3> を参照ください。
11. サービス提供開始前に、インストールされている Kaspersky Security Center のバックアップを実行してください。（本サービスにはお客様に代わってバックアップを実行する時間は含まれません）。
12. 暗号化が適用されるデバイスを制御するポリシーが正しく設定され、適用されていること
13. 暗号化が適用されるコンピューターでは必ず、インストールされている Kaspersky Endpoint Security のバージョンと互換性のある Microsoft Windows オペレーティングシステムが実行されていること
14. すべてのカスペルスキー製品が最新バージョンにアップグレードされていること
「サポート終了」または「限定サポート」のカスペルスキー製品はこのサービスの対象外です。

注：

- ハードディスク暗号化では、デュアルブートおよびマルチ OS の環境はサポートされません
- 導入中に分析が必要なエラーが発生した場合は、サポートサービスでの対応となります。

作業範囲

範囲内

範囲外

- 暗号化の有用性およびカスペルスキー製品に適用可能な暗号化の種類に関する概念的な説明
- プロジェクトタイムラインのセッションで定められたアクティビティでの、HDD ディスク全体、ファイル、およびリムーバブルドライブの暗号化の実施

別途、事前の合意がない限り、カスペルスキーのエンジニアはここに記載された範囲および成果物の定義に従い、カスペルスキーの暗号化サービスの提供と厳密に関連付けられたタスクまたは製品についてのみ作業を実施することになっています。

このサービスの範囲外となるタスクの例は以下の通りです：

- あらゆる種類のポリシーの作成。暗号化に使用されるポリシーは、お客様が保護用に作成済みで使用されているポリシーのコピーとなります
- Kaspersky Security Center と Active Directory の連携
- 保護コンポーネントのインストール。エンドポイント保護がインストール済みで機能している必要があります
- カスタマイズされたレポートの作成
- 暗号化の非互換性に関するトラブルシューティング。この種の問題を解決するには、テクニカルサポートチームにインシデントとして報告してください
- ユーザー、DNS、DHCP、Active Directory またはその他のネットワークサービスの作成
- カスペルスキーが提供している製品以外の製品に関する作業
- プロジェクトに含まれるマシンまたはシステムのバックアップコピーの作成
- オペレーティングシステムのインストール



結果と成果物

お客様のインフラストラクチャにおいて最大 20 のディスクおよびファイルについて暗号化が実行されます。暗号化されたディスクおよびファイルの使用および管理の方法を含め、製品機能の使用方法を理解できます。

注意事項

お客様固有のニーズにお応えするため、必要に応じて付加的な設定や導入、修正を行うこともできます。カスタムプロジェクトにご興味ございましたら、弊社営業へお問い合わせください。

サービス実行開始日は、お客様およびカスペルスキーサービスチームの間で交渉し、希望開始日の 15 日以上前に取り決めます。



www.kaspersky.co.jp

[Kaspersky Professional Services](#)

© 2023 AO Kaspersky Lab.
無断複製禁止。登録商標とサービスマークに関する権利は各所有者に帰属します。