

**kaspersky**

**拡張テクニカルサポートプログラム**

MSA Start

## 1. 一般条件

**MSA Start** レベルの拡張テクニカルサポートの証明書の所有者に対して **Kaspersky Lab** が提供する支援に関連するテクニカルサポートについて示します。

**MSA Start** サポートプログラムは、エンドユーザーによるソフトウェア製品の使用条件を定めた **Kaspersky Lab** の使用許諾契約に従って実施される標準のテクニカルサポートと比較して、高品質のテクニカルサポートをエンドユーザーに提供することを目的としています。

## 2. 定義

「**カンパニアアカウント**」とは、Web ベースによる **Kaspersky Lab** のテクニカルサポートのリクエスト処理システムを指します。

「**製品**」とは、**Kaspersky Lab** とお客様との間の使用許諾契約書の条件に従って、お客様が購入、導入、インストールし、かつ使用許諾契約を結んだ **Kaspersky Lab** のソフトウェア製品を指します。

「**エンドユーザー**」、「**ユーザー**」、「**お客様**」とは、本プログラムに従ってサポートされる製品のライセンスを所有している組織を指します。

「**インシデント**」とは、製品の標準動作ではなく、製品が提供するサービスの質を妨げたり低下させるもの（もしくはその恐れのあるもの）として、お客様から報告されたイベントを指します。

「**現地時間**」とは、指名されたテクニカルアカウントマネージャー（TAM）が存在する、**Kaspersky Lab** のローカルオフィスのタイムゾーンを指します。

「**問題**」とは、1つ以上のインシデントの特定できていない根本原因を指します。根本原因と一時的な回避策または恒久的な代替策が特定された場合は、既知のエラーとなります。

「**既知のエラー**」とは、根本原因が解明され、一時的な回避策または恒久的な代替策が特定されている問題を指します。

「**製品のエラー**」とは、断定されていない製品の動作を指します。

「**サービスリクエスト**」とは、サポート、配信、情報、アドバイス、ドキュメントについてのお客様からのリクエストを指します。ただし、このリクエストは、製品の動作不良とは関係ありません。

「**ウイルスアウトブレイク**」とは、最新の定義データベースがインストールされている製品でウイルスが検出されず、ウイルスによりビジネスの継続性やお客様の多数のエンドユーザーに影響を与えている、危機的な状況を指します。ウイルスアウトブレイクは、製品に関連するインシデントです。

「**マルウェア関連のインシデント / ウイルスインシデント**」とは、製品に関連するインシデントではなく、特定のマルウェアの削除、マルウェアの説明、特別なマルウェア削除ツールに関して、**Kaspersky Lab** が助言を行う必要があるインシデントを指します。

「**インシデントのセバリティレベル / 緊急度**」とは、お客様のビジネスニーズに基づくインシデントや問題が事業体に与える影響の大きさの指標を指します。詳細は、付録 1 を参照してください。

「**応答時間**」とは、インシデント情報を受け付けてから、（サポートシステム、メールまたは電話にて）お客様に適切な回答が提供されるまでの経過時間を指します。

「**アップデート**」とは、新しいウイルスシグネチャや製品の実行モジュールの修正が含まれた、**Kaspersky Lab** が発行する定義データベースを指します。製品モジュールのパフォーマンスの向上や機能の拡張が行われます。

「**アップグレード**」とは、新しいバージョン番号の割り当てを伴う、製品のアップデートを指します。

「**回避策**」とは、インシデントに対して一時的な解決策となる可能性がある手段を指します。

「**誤検知**」とは、製品が安全なファイルをウイルスに感染したファイルと誤って検知する状況を指します。

## 3. MSA Start サポートプログラムの説明

製品の運用および事後メンテナンスのリクエストの受け付けに関するテクニカルサポートは、次の手段により実施します：

- Kaspersky Lab のテクニカルサポートの Web ポータル - 24 時間、年中無休でリクエストを受け付け
- 優先電話回線：業務時間は、Kaspersky Lab 各ローカルオフィスの現地時間の営業日によって異なります（詳細は、証明書を参照してください）。
- メール（Company Account にアクセスできない場合のみ） - 24 時間、年中無休でリクエストを受け付け

### インシデントの処理

#### Company Account の Web パネルによるインシデントの処理

Web ベースによる Kaspersky Lab のテクニカルサポートのリクエスト処理システムは、<https://companyaccount.kaspersky.com> でご利用いただけます。

このシステムを通じてお客様がご利用になれるサービスは、次の通りです：

- インシデントの作成、更新、監視を行うための、個人アカウントへのアクセス
- 製品のインストール時、設定時、動作時に発生する可能性があるインシデントに関連するテクニカルサポートおよびコンサルティング
- マルウェアによって改竄されたファイルの駆除、および最新の定義データベースがインストールされた製品によって保護されているお客様のコンピューターからのマルウェアの削除に関連するテクニカルサポート

#### 電話によるインシデントの処理

電話によるテクニカルサポートをご利用になれるのは、権限を与えられたお客様側の窓口担当者のみです。

#### メールによるインシデントの処理

メールによるインシデントの処理は、カンパニーアカウントにアクセスできない場合に、ご利用いただけます。この処理は、権限を与えられたお客様側のすべての窓口担当者をご利用になれます。

メールを通じてお客様がご利用になれるサービスは、次の通りです：

- 製品のインストール時、設定時、動作時に発生する可能性があるインシデントに関連するテクニカルサポートおよびコンサルティング
- マルウェアによって改竄されたファイルの駆除、および最新の定義データベースがインストールされた製品によって保護されているお客様のコンピューターからのマルウェアの削除に関連するテクニカルサポート

### 応答時間

お客様のリクエストの緊急度に応じて、Kaspersky Lab が保証する応答時間は、次の通りです：

セバリティレベル	応答時間
レベル 1	6 営業時間

MSA Start のお客様からのリクエストは、標準サポートパッケージで対応するリクエストより高い優先順位が割り当てられます。

緊急度のレベルは、テクニカルサポートに問い合わせる際にお客様が選択するカテゴリ（カンパニーアカウントのドロップダウンリストを使用）とインシデントの内容によって決まります。お客様が指定された案件のセキュリティレベルを確定していない場合、Kaspersky Lab はリクエストの緊急度のレベルを変更する権利を有します。緊急度のレベルのリストについての説明は、付録 1 を参照してください。

## インシデントの解決の管理

どのような場合でも、インシデントはお客様側または Kaspersky Lab 側のどちらかに存在します。Kaspersky Lab さんから問題の解決を促す連絡を行い実施いただいているときは、インシデントはお客様側に存在します。Kaspersky Lab がお客様に情報の提供をご依頼した時も、インシデントはお客様側に存在します。必要な情報をお客様が Kaspersky Lab に提供した時に、インシデントは、Kaspersky Lab 側に存在すると見なされます。インシデントがお客様側に存在する期間の上限は、1か月とします。期限内にお客様からの回答がなかった場合、インシデントはタイムアウトとなりクローズされます。

Kaspersky Lab の責任は、インシデントが Kaspersky Lab 側にある期間に限られます。

## マルウェアインシデントまたは誤検知に関するお客様のリクエストに対応した定義データベースのリリース

最新の定義データベースを使用している状態で誤検知（感染したファイルが安全と判定されたり、反対に安全なファイルが危険と判断されたりすること）が発生した場合、お客様は、製品のアンチウイルスシグネチャを修正するように要求することができます。Kaspersky Lab は、ファイルを正確に検知する製品のアップデートをお客様に提供いたします。

Kaspersky Lab が行うことは、次の通りです：

- 定義データベースのリリースに関するリクエストの処理（専任のスペシャリストグループが 24 時間、年中無休で対応します）
- MSA Start の契約者を対象とした優先度の高いアップデートのリリース

## サポートの追加条件

お客様は、Kaspersky Lab のテクニカルサポートのリクエストを開始する権限を付与された担当者を 1 名まで指名できます。権限を与えられた担当者のリストは、Kaspersky MSA Start 証明書に明記する必要があります。担当者のリストを変更する場合は、お客様はカンパニーアカウントから依頼書を送付してください。Kaspersky Lab は、最新版の Kaspersky MSA Start 証明書をお客様に提供いたします。

Kaspersky MSA Start 証明書に別段の定めがある場合を除き、お客様は、この証明書の有効期間中に 6 件のインシデントを登録できます。

インシデントによっては、ウイルスの感染や製品のエラーをテストおよび検証する目的で、Kaspersky Lab 側で再現する必要があります。

インシデントが再発する条件を再現して調査するために必要なすべての情報および特定のソフトウェアやハードウェアを、お客様から提供していただく場合があります。これは、必要なソフトウェアまたはハードウェアが Kaspersky Lab にない場合に必要になります。

必要なすべての情報と、ソフトウェアやハードウェアが提供された時点で、Kaspersky Lab はインシデントを再現します。

インシデントが再現できない場合、正しく機能していないお客様のシステムに、Kaspersky Lab のスペシャリストがリモートでアクセスする権限を与えていただく必要があります。

いずれの当事者もインシデントを再現できない場合、インシデントが再現できうるネットワーク環境へのアクセスをお客様が許可しない場合、またはインシデントの原因が製品以外にあることが判明した場合、インシデントはこのサポートプログラム内で分類することはできません。

## 拡張テクニカルサポートプログラム MSA Start の制限事項

MSA Start プログラムに定められているテクニカルサポートは、次のインシデントには適用されません。

- すでに解決済みのインシデント（インシデントが解決された後にインストールされた同じ製品で発生した同じインシデント）。
- すでに解決済みの問題と類似しているか、同じようなすべての問題（Kaspersky Lab から追加の情報を得ずに、以前に適用された解決策を適用できるインシデント）のトラブルシューティング。
- お客様のハードウェアの誤動作に起因するインシデント。
- ソフトウェアプラットフォームの不適合（ベータソフトウェアや、Kaspersky Lab により製品との互換性がまだ確認されていないサービスパックや追加機能を含む新しいバージョン、ただしこれらに限定しない）に起因するインシデント。
- サードパーティ製のアプリケーション（ガイドに公開されている、サポートされないまたは競合するアプリケーションのリストを含む、ただしこれらに限定しない）をインストールして実行したことを起因とするインシデント。
- インシデントの再現、調査、解決のために、Kaspersky Lab が合理的に要求した正確な情報がお客様から提供されないインシデント。
- Kaspersky Lab の指示に従わずに使用したか、誤って使用したために生じたインシデント（正しく使用していれば、明らかに防げたインシデント）。

## 4. 付録

### 付録 1 製品インシデントのセベリティレベル

「レベル 1」（重要）とは、重大な製品の問題を指します。製品の正常な機能の中断によってお客様のビジネスの継続性に影響を与え、製品やオペレーティングシステムのクラッシュを引き起こします。またはデータを消失させたり、既定の設定を安全でない値へ変更したりします。あるいは、有効な回避策のないセキュリティの問題を指します。

レベル 1 の製品に関連するインシデントには、次の問題が含まれます。ただし、これらに限定されるものではありません：

- すべてのローカルネットワーク（またはその重要な部分）が動作不能で、中核となるビジネスプロセスの妨害や中断を発生させる問題。

「レベル 2」（高）とは、製品の機能に影響はあるが、データの破損や消失またはソフトウェアクラッシュを引き起こさない問題を指します。回避策が利用できる場合、レベル 1 はレベル 2 に再分類されます。

レベル 2 の製品に関連するインシデントには、次の問題が含まれます。ただし、これらに限定されるものではありません：

- 製品が正しく機能しないが、中核となるビジネスプロセスの継続性が中断されることはない。

「レベル 3」（中）とは、製品の機能に影響しない、重大ではない問題またはサービスリクエストを指します。レベル 3 のインシデントには、次の問題が含まれます。ただし、これらに限定されるものではありません：

- 製品が部分的に使用できない状態（機能不全）ではあるが、お客様が使用している他のアプリケーションは関与していない。

「レベル 4」（低）とは、重大ではない問題またはサービスリクエストを指します。上記の基準と一致しないすべてのインシデントには、このレベルが適用されます。

### 付録 2 ウイルスインシデントのセベリティレベル

「レベル 1」（重要）とは、ウイルスアウトブレイクを指します。製品の正常な機能の中断によってお客様のビジネスの継続性に影響を与え、製品やオペレーティングシステムのクラッシュを引き起こします。またはデータの消失を引き起こし、そして有効な回避策がない場合です。



レベル 1 のマルウェアに関連するインシデントには、次の問題が含まれます。ただし、これらに限定されるものではありません：

- すべてのローカルネットワーク（またはその重要な部分）が動作不能な状態
- ウイルスアウトブレイク
- 業務に不可欠なシステムを参照するファイルの誤検知

「レベル 2」（高）とは、製品の機能に影響はあるが、データの破損や消失またはソフトウェアクラッシュを引き起こさない問題を指します。回避策が利用できる場合、レベル 1 はレベル 2 に再分類されます。

レベル 2 のマルウェアに関連するインシデントには、次の問題が含まれます。ただし、これらに限定されるものではありません：

- 重要でないネットワークノードの感染
- 業務に不可欠なシステムを参照しないファイルの誤検知



[www.kaspersky.co.jp](http://www.kaspersky.co.jp)  
[www.securelist.com](http://www.securelist.com)