SKYARCH
あなたの側で、あなた以上に考える。

マネージドセキュリティサービス

for Deep Security

サービス仕様書

－第 1 版－

株式会社スカイアーチネットワークス

目次

1.　定義

「マネージド セキュリティ サービス for Deep Security」（以下、本サービス）は、株式会社スカイアーチネットワークス（以下、当社）が提供するサービスの総称です。本仕様書にて本サービスの仕様を定義します。

2.　サービス概要

本サービスは Trendmicro 社が提供する「Trend Micro Deep Security as a Service」（以下、DSaaS）の以下の機能を使用して提供します。

- 不正プログラム対策
  不正プログラム、ウイルス、トロイの木馬、スパイウェア等の脅威からシステムをリアルタイムに保護します。

- 侵入防御 / 侵入検知
  既知もしくは未知の脆弱性への攻撃、SQL インジェクション、クロスサイトスクリプティング、およびその他の脆弱性からシステムを保護（防御モード）または監視（検知モード）します。また、ネットワークへのアクセスを監視することで不正プログラムを特定します。

- ファイアウォール
  双方向のステートフルファイアウォールであり、許可されていない送信元からの通信がホスト上のアプリケーションに到達することをブロックします。

- web レピュテーション機能
  システムから不正プログラムが仕込まれたサイトへのアクセスをブロックします。適用されている Web レピュテーションのセキュリティ基準と照合し、web サイトへのアクセスをブロックまたは許可の判定を行います。

- 変更監視
  システム上で、あらかじめ指定された領域に関する変更を監視します。実行中のサービス、プロセス、ファイル、ディレクトリ、ポート、レジストリが対象となります。ベースラインを用いた検索を定期的に実行することで、変更箇所を検出します。

- セキュリティログ監視
  各種セキュリティログを監視し、事前に設定した閾値を超えた場合に管理者にアラートを発報します。

3. 用語説明

DSaaS
Trendmicro 社が提供するサービス「Trend Micro Deep Security as a Service」の名称

DSM（Trend Micro Deep Security Manager）
Trend Micro Deep Security を一元管理する管理画面。

DSA（Trend Micro Deep Security Agent）
DSM が管理するサーバに配置するエージェントプログラム。

AWS（Amazon Web Services）
Amazon.com により提供されているクラウドコンピューティングサービスの総称。

S3（Simple Storage Service）
Amazon.com により提供されているインターネット用のストレージサービスの総称。

Azure
Microsoft 社により提供されているクラウドコンピューティングサービスの総称。

アラート
DSM ルールにて検出されたイベントにより発生する警告メッセージ。

IDS（Intrusion Detection System）
外部からの不正アクセスを検知するシステム。

IPS（Intrusion Prevention System）
外部からの不正アクセスを検知・ブロックするシステム。

４．　サービス提供条件

（１）DSM

・　DSM と DSA 間の通信が確保されている環境でご利用いただけます。
・　Trendmicro 社による推奨設定かつ重要度「高」以上のルールを適用するものとします。
・　お客様による DSM の管理は不要です。
・　DSaaS における「アプリケーションコントロール」機能は本サービスの対象外とします。

（２）DSA

・　システム要件は、Trendmicro 社の下記情報を参照するものとします。
　http://www.trendmicro.co.jp/jp/business/products/tmds/index.html#requirement
・　DSA をインストールするサーバにおいて、ネットワークの一時的な切断、または OS のネットワークドライバーが他のプログラムによってロックされている場合、OS の再起動が求められる場合があります。
・　DSaaS で提供される機能の一部は日本国内ではサポートされていないものが含まれます。
・　DSaaS で使用されているシステムのバージョンアップおよびプログラム修正、ならびにカスタマーが使用中の本ソフトウェアに対するバージョンアップ版および修正プログラムの配信は、事前通知なく、自動的に行われる可能性があります。
・　本サービスを適用するサーバには、別途、当社が提供するフルマネージドサービスの基本サービス及び運用サポート「ゴールド」もしくは「プラチナ」契約が必要となります。
・　本サービスを導入するサーバの最小ノード数は２とします。

（３）留意事項

下記の条件に該当する場合、DSaaS が正常に機能しないことがあります。

・　システムにストレージ領域（AWS S3 等）をマウントしている場合
・　DSA が稼働するシステムのスペックが低い場合
　http://www.trendmicro.co.jp/jp/business/products/tmds/index.html#requirement
・　変更監視対象ファイル数が多い場合、システムのリソースに影響を与える場合があります。
　https://help.deepsecurity.trendmicro.com/ja-jp/Protection-Modules/Integrity-Monitoring/create-integrity-monitoring-rules.html

その他、動作環境は DSaaS の仕様に準拠します

5. ご契約プランとサービス概要

分類	サービス内容	スタンダード	アドバンスド	ハイエンド
ライセンス	DsaaS ご利用ライセンス設定	○	○	○
基本オペレーション	・ 環境構築・初期設定 ・ プロセス監視 ・ ライセンス更新 ・ ヘルプデスク	○	○	○
設定変更	基本的な設定変更	○	○	○
アラート対応	DSaaS アラート/セキュリティインシデント対応	×	○ 翌営業日 10-18 時	◎ 24 時間 365 日
各種レポート	週次レポート	×	○	○
	月次レポート	×	有償	○
	定期報告会	×	有償	○ （年 4 回）
コンサルティング	各種チューニング・カスタムルール作成	×	有償	○

6.　ご利用までの流れ

ご契約から利用開始までの流れを下記に示します。

手順	担当	概要	詳細
1	お客様	ご契約	弊社所定の注文書、およびヒアリングシートにご記入いただきます。
2	スカイアーチ	ライセンス発行	DSaaS アカウントの発行、初期設定および契約内容に準拠した通知先設定を実施します。
3	スカイアーチ	DSA インストール	対象ホストへの DSA インストールを行います。
4	スカイアーチ	ルール適用	DSM より、対象ホスト上で稼働する DSA にルールの適用を行います。
5	お客様	ご利用開始	

7. 各サービスの詳細

（1） 基本オペレーション（環境設定・初期構築）

お客様から依頼された下記の作業を弊社エンジニアが実施します。

- DSaaS アカウント発行
  DSaaS にて、お客様専用アカウントを登録します。登録後、初期設定および契約内容に準拠した通知先を設定します。
- DSA インストール
  弊社エンジニアが対象サーバにログインし、DSA のインストールを行います。また弊社監視サーバにてエージェントプロセスの監視設定を行います。
- ルール適用
  ヒアリングシートに基づいた各種設定およびルールを適用します。

（2） 基本オペレーション（プロセス監視）

- 弊社が運用する監視システムよりお客様サーバ上で稼働する DSA の死活監視を行います。（24 時間 365 日）
- アラート検知後、設定されたフローに基づき障害対応及びお客様への連絡を行います。
- メンテナンス作業等による DSA の停止、もしくは通信に影響が発生する場合は事前に弊社までお知らせください。

（3） 基本オペレーション（ライセンス更新）

弊社エンジニアがライセンス更新作業を行います。

（4） 基本オペレーション（ヘルプデスク）

DeepSecurity に関連する技術的なお問い合わせを受け付けます。受付後、3 営業日以内に一次回答を行います。

受付時間	弊社営業日 10:00～18:00 ※
受付方法	電話、電子メール

※ 弊社営業日とは、平日月曜から金曜までのことをいい、土曜・日曜・祝祭日・年末年始（12/30～1/3）は含みません。

（5） 設定変更

お客様から依頼された以下作業を弊社エンジニアが実施します。

・ポリシー変更
・アラート通知先変更
・防御モード/検知モード切替（コンピュータ単位）
・除外設定
・予約タスク設定
・エージェントアップデート

受付時間	弊社営業日 10:00～18:00 ※
受付方法	電話、電子メール

※ 弊社営業日とは、平日月曜から金曜までのことをいい、土曜・日曜・祝祭日・年末年始（12/30～1/3）は含みません。

（6） アラート対応（スタンダードプラン）

・ DSM ルールにより検出したイベントに関するアラートメールを、ご契約時にご登録いただいた電子メールアドレスに送信します。(24 時間 365 日)
・ アラートメールに関するお問い合わせを、ヘルプデスクにて受け付けます。

（7） アラート対応（アドバンスドプラン）

弊社にて前日分の稼働データを集計し、下記のアラートメールの確認を行います。処置が必要と判断したものは、ご登録いただいた連絡先へエスカレーションを行います。

確認対象	・ 変更監視 ・ セキュリティログ監視 ・ 不正プログラム ・ DeepSecurity アラート
対象外	・ 正常に削除や防御などの対応が完了したアラート ・ エージェントとの一時的な疎通不可 ・ 予定された作業に起因して発生したアラート

（8） アラート対応（ハイエンドプラン）

弊社及び提携 SOC（SecureWorks 社)にてアラートメールを 24 時間 365 日体制で検知し、内容の確認を行います。

下記のような重大なアラートを検知した際は、弊社エンジニアが提携 SOC と連携し、お客様に相談の上、必要な処置を行います。

アラートの例	処置
マルウェア感染	対象サーバの停止・隔離
断続的な攻撃	攻撃元の遮断や対象サーバの停止・隔離、等

（9） 各種レポート（週次レポート）

ご契約プランに応じて、毎週、DSM の下記運用レポートを発行します。

報告日	5 営業日以内に提出
集計期間	毎週　月曜日 00 時 00 分　～　日曜日 23 時 59 分
報告対象	・攻撃レポート ・Web レピュテーション ・ファイアウォール ・侵入防御 / 侵入検知
報告方法	電子メールにて、ご契約時にご登録いただいた電子メールアドレスにレポートを送付
報告元	アドバンスドプラン　：弊社 ハイエンドプラン　：SOC

（１０）各種レポート（月次レポート）

ご契約プランに応じて、毎月、DSM の下記運用レポートを発行します。

報告日	毎週第 1 営業日を含めた 5 営業日以内に提出
集計期間	毎月　1 日 00 時 00 分　～　月末 23 時 59 分
報告対象	（1）現在の設定情報 ・適用ポリシー一覧 ・有効サービス名 ・ネットワークエンジンモード （2）お問い合わせへの対応結果（サマリー） ・当月内の変更作業概要 （3）インシデント対応

	・検知内容 ・検知日 ・対応内容
報告方法	弊社より電子メールにて、ご契約時にご登録いただいた電子メールアドレスに PDF 形式のレポートファイルを送付

（１１）各種レポート（定期報告会）

弊社エンジニアが訪問し、DSM 運用状況の報告、およびご質問にお答えします。

開催日時	年 4 回（開催日の 2 週間前までに調整いただく必要があります）
開催条件	・ハイエンドプランのご契約 ・訪問先は都内に限定（遠隔地への訪問は有償となります） ・TV 会議方式での報告会も対応可能です
報告資料	報告対象期間の月次レポートサマリー

（１２）コンサルティングサービス

お客様から依頼された各種チューニング/カスタムルール作成を弊社エンジニアが実施します。

受付時間	弊社営業日 10:00～18:00 ※
受付方法	電話、電子メール

※ 弊社営業日とは、平日月曜から金曜までのことをいい、土曜・日曜・祝祭日・年末年始（12/30～1/3）は含みません。

8. 免責事項

（1） 当社は、第三者がお客様の端末設備に、ログイン名等を不正使用する等の方法で不正アクセスを行い、お客様又は第三者に損害を与えた場合においてもその損害について一切の責任を負わないものとします。

（2） 本サービスの使用により、お客様が他のお客様又は第三者に損害を与えた場合、お客様の責任と費用において解決するものとし、当社に損害を被らせないものとします。

（3） 当社は、本サービスに起因した以下の事項についていかなる保証も行わず、いかなる担保責任も負いません。

- 第三者からの不正アクセス等を検知もしくは遮断できなかった場合
- システムの動作、通信等に障害が生じた場合
- システム上のデータの破損、消失、等が発生した場合
- その他、本サービスに起因してお客様システムに障害が発生した場合

（4） 設定変更は、DSaaS の仕様に準拠した範囲に限定させていただきます。

株式会社スカイアーチネットワークス

〒105-0001 東京都港区虎ノ門 3-8-21

虎ノ門 33 森ビル 6 階

TEL(代表)：03-6743-1100　FAX：03-6743-1101