

Deep Discovery™ Inspector Basic Service サービスガイドブック Ver. 1.0

トレンドマイクロ株式会社

TRENDMICRO, TREND MICRO, ウイルスバスター, ウイルスバスター On-Line Scan, PC-cillin, InterScan, INTERSCAN VIRUSWALL, ISVW, InterScanWebManager, ISWM, InterScan Web Security Suite, IWSS, TRENDMICRO SERVERPROTECT, PortalProtect, Trend Micro Control Manager, Trend Micro MobileSecurity, VSAPI, トrendマイクロ・プレミアム・サポート・プログラム, License for Enterprise Information Security, LEISec, Trend Park, Trend Labs, InterScan Gateway Security Appliance, Trend Micro Network VirusWall, Network VirusWall Enforcer, Trend Flex Security, LEAKPROOF, Trend プロテクト, Expert on Guard, InterScan Messaging Security Appliance, InterScan Web Security Appliance, InterScan Messaging Hosted Security, DataDNA, Trend Micro Threat Management Solution, Trend Micro Threat Management Services, Trend Micro Threat Management Agent, Trend Micro Threat Mitigator, Trend Micro Threat Discovery Appliance, Trend Micro USB Security, InterScan Web Security Virtual Appliance, InterScan Messaging Security Virtual Appliance, Trend Micro Reliable Security License, TRSL, Trend Micro Smart Protection Network, Smart Protection Network, SPN, SMARTSCAN, Trend Micro Kids Safety, Trend Micro Web Security, Trend Micro IM Security, Trend Micro Email Encryption, Trend Micro Email Encryption Client, Trend Micro Email Encryption Gateway, Trend Micro Collaboration Security, Trend Micro Portable Security, Portable Security, Trend Micro Standard Web Security, トrendマイクロ アグレッシブスキャナー, Trend Micro Hosted Email Security, Hosted Email Security, Trend Micro Deep Security, ウイルスバスタークラウド, ウイルスバスターCLOUD, Smart Surfing, スマートスキャン, Trend Micro Instant Security, Trend Micro Enterprise Security for Gateways, Enterprise Security for Gateways, Trend Micro Email Security Platform, Trend Smart Protection, Vulnerability Management Services, Trend Micro Vulnerability Management Services, Trend Micro PCI Scanning Service, Trend Micro Titanium, Trend Micro Titanium AntiVirus Plus, Smart Protection Server, Deep Security, Worry Free Remote Manager, ウイルスバスター ビジネスセキュリティサービス, HOUSECALL, SafeSync, トrendマイクロ オンラインストレージ SafeSync, Trend Micro InterScan WebManager SCC, Trend Micro NAS Security, Trend Micro Data Loss Prevention, TREND MICRO ENDPOINT ENCRYPTION, Securing Your Journey to the Cloud, Trend Micro オンラインスキャン, Trend Micro Deep Security Anti Virus for VDI, Trend Micro Deep Security Virtual Patch, Trend Micro Threat Discovery Software Appliance, SECURE CLOUD, Trend Micro VDI オプション, おまかせ不正請求クリーンアップサービス, Trend Micro Deep Security あんしんバック, こどもモード, Deep Discovery, TCSE, おまかせインストール・バージョンアップ, トrendマイクロ バッテリーエイド, Trend Micro Safe Lock, トrendマイクロ セーフバックアップ, Deep Discovery Advisor, Deep Discovery Inspector, Trend Micro Mobile App Reputation, あんしんブラウザ, Jewelry Box, カスタム ディフェンス, InterScan Messaging Security Suite Plus, おもいでバックアップサービス, おまかせ！スマホお探しサポート, プライバシースキャナー, 保険&デジタルライフサポート, LiveWedding, おまかせ！迷惑ソフトクリーンアップサービス, Smart Protection Integration Framework, および InterScan Web Security as a Service は、トレンドマイクロ株式会社の登録商標です。本書に記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。Copyright © 2016 Trend Micro Incorporated. All rights reserved.

| | |
|---|-------|
| 1. サービス概要 | - 3 - |
| 2. 本契約をご利用いただくためのお客さまの準備 | - 3 - |
| • DDI のご契約 | - 3 - |
| • コンタクトパーソンの任命 | - 3 - |
| • サービス提供に必要な各種お客さま情報の提供 | - 3 - |
| • DDI ログを当社指定システムに送信するためのお客さま側 DDI 設定 | - 3 - |
| • 当社の技術支援への協力 | - 4 - |
| 3. サービスメニュー | - 4 - |
| 4. 注意事項 | - 5 - |
| • 本サービスガイドブックについて | - 5 - |
| • DDI のバージョンについて | - 5 - |
| • DDI の台数について | - 5 - |
| • DDI の稼働確認 | - 5 - |
| • 本サービスにおける通知およびレポートについて | - 5 - |
| • 当社スタンダードサポートでのサポート範囲について | - 6 - |

※ 記載 URL は予告なく変更される場合がありますのでご了承ください。

1. サービス概要

Deep Discovery™ Inspector Basic Service (以下、「本サービス」という)では、Deep Discovery™ Inspector (以下「DDI」)によって確認された脅威に関する情報提供および、提供した情報についての問い合わせ対応を提供します。

2. 本契約をご利用いただくためのお客さまの準備

■ DDI のご契約

本サービスはお客さまが使用权を有する DDI に対して提供されます。本サービスに DDI そのものは含まれませんので、別途ご契約ください。

■ コンタクトパーソンの任命

お客さまは、本サービスに対して「コンタクトパーソン」を 4 名まで任命し、さらにその中から代表者として「コンタクトパーソン代表者」を必ず 1 名任命します。任命したコンタクトパーソンは、本サービスの新規ご契約時に、右記 URL から登録願います。⇒ <http://www.go-tm.jp/ddibs/cp>

- コンタクトパーソン代表者は、以下の調整を行うものとします。
 - ① 本サービスの「監視対象」範囲の決定
 - ② 問い合わせ内容に応じた優先順位付け
 - ③ 当社への依頼内容の管理
 - ④ お客さまの社内情報の取りまとめ
 - ⑤ コンタクトパーソン間での情報共有
- コンタクトパーソンとして、お客さまの部署名やグループ（チーム）名およびメーリングリストを登録することはできません。
- コンタクトパーソンは、制限人数内であれば契約期間中に変更することができます。ただし、変更にあたっては、「コンタクトパーソン変更届」により当社への連絡が必要です。詳細は当社担当営業、または、本サービスのお問い合わせ窓口までお問い合わせください。
- 4 名以上のコンタクトパーソン登録をご希望の場合は、「追加コンタクトパーソン」の購入により最大 8 名までの登録が可能です。詳細は当社担当営業、もしくは本サービスを購入した販売店にお問い合わせください。

■ サービス提供に必要な各種お客さま情報の提供

お客さまは、本サービスのお申し込み時に、本サービス開始に必要な情報を当社が指定する申込書別紙に記載の上、当社に提出が必要です。また、記載情報に不足があった場合、サービスが開始できない場合がありますのでご注意ください。ご提供いただく情報は、以下内容となります。

| ご提供いただく情報 | ご提供いただくタイミングと方法 |
|------------------------------|--|
| ① DDI ログの送信元となるグローバル IP アドレス | 本サービスのご発注時に、本サービス申込書類に記載して提出願います。 |
| ② 監視対象となる端末台数 | |
| ③ お客さま先に設置された DDI の GUID | お客さま側での DDI 設定時に、本ガイドブックに記載されたお問い合わせ窓口（E-mail 窓口）にご連絡ください。 |
| ④ その他、当社が本サービス提供に必要と判断した情報 | 当社から都度ご連絡させていただきます。 |

■ DDI ログを当社指定システムに送信するためのお客さま側 DDI 設定

お客さまは、お客さま側の DDI から当社指定システムに DDI ログを送信するための設定作業を行っていただく必要があります。

お客さま側での DDI 設定概要は以下の通りです。(詳細は「請書」に同梱される案内文書をご参照ください。)

- ① お客さま先 DDI の Web コンソールから確認できる「GUID」をご確認頂き、当社へ連絡
- ② お客さまから頂いた「GUID」情報に基づき、当社側での登録作業を実施 (5~6 営業日)
- ③ 当社からお客さまへ、登録作業完了を連絡
- ④ 当社指定システムに関する接続先情報に基づき、お客さま側で DDI 設定を実施

DDI および本サービスは、当社指定システムへのログデータ送信を行わなくてもご利用可能ですが、この場合は本サービスの一部について提供ができませんのでご注意ください。

DDI が当社指定システムに対してログデータを送信することで提供可能なサービスをご利用のお客様は、DDI から当社指定システムへデータが送信できる状態にあることを、継続的にご確認ください。

■ 当社の技術支援への協力

- 当社が本サービスを提供するにあたり、コンタクトパーソンは、当社が円滑に、そして効果的にサービス提供できるよう、環境整備や技術情報の提供に積極的に協力する必要があります。
- コンタクトパーソンは、当社が適切にサービス提供できるように社内外の調整を行う必要があります。そして、当社が提供するサービスに必要な協議の機会を準備する必要があります。
当社が必要とする協力が得られない場合、本サービスガイドブックに記載されるサービスが提供できない場合があります。

3. サービスメニュー

本サービスでは、以下に記載されたサービスメニューを提供いたします。

| サービスメニュー | 提供内容 |
|--|--|
| Critical Incident Notification Service | <p>お客さま先に設置された DDI 検出イベントを当社指定システムに取り込み、優先的に対応すべき以下疑いのある検出時にコンタクトパーソン宛にメール通知を行います。(全ての脅威を完全に通知できることをお約束するものではありません。また、脅威傾向の変化に伴い、通知対象が変更される場合がございます。)</p> <ol style="list-style-type: none">1. 持続的標的型攻撃 (APT 攻撃)2. ランサムウェア3. オンライン銀行詐欺ツール4. その他 (1.~3.いずれかの可能性が高いが断定できない検出および、お客さまネットワーク内部での他端末への感染拡大) <p>お客さま先の DDI から当社指定システムへ送信されたログの確認はおおよそ 1 時間程度毎に行われ、上記検出が含まれる場合はコンタクトパーソン宛にメール通知が行われます。メール通知の対応時間は 24 時間 365 日です。</p> |
| 通知およびレポートに関するお問い合わせ対応 | <p>お客さまは、専用の E-MAIL アドレスに連絡することによって、本サービスで提供される「Critical Incident Notification Service」の内容、DDI が生成するレポート (日次・週次・月次)、DDI に記録された各種イベントの内容について、当社へ問い合わせを行うことができます。</p> <p>但し、「Critical Incident Notification Service」および DDI の検知・レポートを起点としたインシデント対応に関するお問い合わせは、本サービス対象外です。</p> <p>但し、レポート提供が正しく行われないなど、本サービスの提供に影響を及ぼすような緊急を要すると判断される状況が発生した場合、お客さまは電話を通じた問い合わせを行うことができます。電話を通じた問い合わせは、土日、祝祭日、年末年始 (12 月 30 日~1 月 4 日)、その他に当社が指定する休日 (創立記念日など) を除く、平日 9:00~17:30 となります。</p> |

※ 「Critical Incident Notification Service」は、当社指定システムに送信された DDI ログに基づき提供されるため、当社指定システムに対して情報を送付できない環境の場合 (「お客さま」のご都合等の理由も含む)、サービスを提供することができませんのでご注意ください。

※ DDI の製品に関するご質問 (機能・仕様確認、製品不具合など)、ならびに不正プログラム関連のご質問 (不正プログラム感染が疑われる端末の調査、調査用ログの調査など) は、本サービスに含まれません。お客さまが使用权を有する DDI に同封される弊社スタンダードサポートメニュー、または別途有償でご契約いただく弊社有償サポートサービスメニューをご利用ください。

4. 注意事項

■ 本サービスガイドブックについて

お客さまは、当社で提供する本サービス以外のサービスを利用する権利がある場合、それらのサービスで定める方法を利用して問い合わせることもできますが、その場合、本サービスガイドブックに記載されるサービス内容は適用されません。

■ DDI のバージョンについて

本サービスでは、サポートサービスを終了させて頂いたバージョンの DDI に対するサービス提供は対象外とさせていただきます。サポートサービス終了製品のご案内および関連情報は、以下のページにてご確認ください。

- サポートサービス終了製品のご案内
 - <http://jp.trendmicro.com/jp/support/lifecycle/old-versions/index.html>
- サポートライフサイクル
 - <http://jp.trendmicro.com/jp/support/lifecycle/index.html>
- 製品 Q&A
 - <http://esupport.trendmicro.com/ja-jp/default.aspx>

また本サービスで提供される「Critical Incident Notification Service」は、DDI 3.8 SP1 以上のバージョンのみに提供されます。本バージョンに該当しないバージョンの DDI をご利用中のお客さまには、該当バージョンへのバージョンアップを推奨いたしますが、バージョンアップ不可の場合は「Critical Incident Notification Service」は提供出来かねますのでご注意ください。

■ DDI の台数について

本サービスでは、単一の契約でお客さまが使用权を有する DDI の台数 = 10 台までに対するサービス提供が可能です。DDI 台数が 11 台を超過する場合、DDI 台数 = 10 台毎に本サービスの契約が必要です。

■ DDI の稼働確認

DDI が正常に稼働せずデータが正常に送信されない場合、サービス品質に影響を与える可能性があります。当社にて、DDI に問題があると判断した場合、稼働確認のために簡単な確認作業をお願いする場合がありますので、その際にご対応をお願い致します。

■ DDI の状況に応じた当社への連絡について

DDI で以下の状況が発生する場合、本サービスの提供に一部影響が発生する場合がございますので、必ず当社までご連絡ください。

- DDI の再インストール
- DDI の追加/撤去
- DDI のバージョンアップ

■ 本サービスにおける通知について

本サービスでは、お客さま側の DDI から当社指定システムに送信されたログに基づく通知を提供しますが、全ての脅威情報を完全に網羅することを保証するものではありません。あらかじめご了承ください。また、通知フォーマットは、お客さまにとってわかりやすく、適切な情報をお届けできることを目的に、継続的に改善されます。改善点について不明な場合や改善要望がある場合は、お問い合わせ窓口までご連絡ください。

■ 当社スタンダードサポートでのサポート範囲について

当社スタンダードサポートでのサポート範囲は製品保守関連のお問い合わせ対応となります。詳細は、以下の当社 Q&A ページをご参照ください。

<http://esupport.trendmicro.com/solution/ja-jp/1102160.aspx>

5. 定義

| 項目 | 定義 |
|--------------|---|
| サービス利用規約 | 本契約のご利用にあたり、事前に合意していただく条件を明記した文書。以下「サービス規約」とする。「サービス規約」の内容は、以下リンク先の「トレンドマイクロ製品使用許諾契約」に記載するものとする。 http://www.trendmicro.co.jp/jp/business/buy/permit/index.html |
| サービスガイドブック | 本ドキュメント。以下「本サービスガイドブック」とする。 |
| お客さま | サービス規約上の「乙」に相当するお客さま |
| コンタクトパーソン | 本契約におけるお客さまのご担当者様（お客さまから指定された協力会社のご担当者様を含む）。本契約ではコンタクトパーソン代表者を含め 4 名のコンタクトパーソンを登録できる。また、コンタクトパーソンの追加購入も可能であるが、本サービスで登録可能な最大人数は、8 名とする。 |
| コンタクトパーソン代表者 | コンタクトパーソンの一人であり、その代表者。 |
| 検体 | ウイルスもしくは、ウイルスである可能性のあるファイル。 |
| 請書 | 当社が、お客さまから本サービスを受注した際に、当社からお客さま宛に発行する契約書類。本サービスの契約内容および、お問い合わせ窓口情報を記載。 |

6. お問い合わせ窓口

| | お問い合わせ内容 | お問い合わせ窓口 |
|------------|--|---|
| 運用開始前の事前準備 | DDI⇔当社指定システム 接続作業時の不具合に関するお問い合わせ (DDI の製品不具合を除く) | <ul style="list-style-type: none"> ・ E-mail 窓口 : moc_service@trendmicro.co.jp <ul style="list-style-type: none"> ➢ 受付日時：24 時間 年中無休（回答は電話による受付日時に準じる） |
| 運用開始後 | DDI が生成するレポートおよび検出された脅威に関するお問い合わせ | <ul style="list-style-type: none"> ・ 電話窓口 : 03-5334-3862 <ul style="list-style-type: none"> ➢ 電話窓口は、本ガイドブックに記載された緊急を要すると判断される状況が発生した場合のみ、ご利用いただけます。 ➢ 受付日時：土日・祝祭日・年末年始（12 月 30 日～1 月 4 日）その他に当社が指定する休日（創立記念日など）を除く平日 9:00～17:30 |
| | 製品仕様・不具合に関するお問い合わせおよび、検体の解析依頼 | <ul style="list-style-type: none"> ・ 当社製品の使用許諾に含まれる当社スタンダードサポート、または別途有償の当社サポートサービスをご利用下さい。 |

※ 上記お問い合わせ窓口は、本サービスをご発注頂き新たにご契約を開始されるお客さまおよび、本サービスをご契約中のお客さまに提供されます。恐縮ながら本サービスご発注前のお客さまはご利用になれませんので、あらかじめご了承ください。

※ 電話窓口へのお問い合わせは、レポート提供が正しく行われないなど本サービスの提供に影響を及ぼすような緊急を要すると判断される状況が発生した場合に限ります。

※ DDI⇔当社指定システム 接続作業時の不具合の多くが、接続作業で使用されているお客様・送信元 Global IP アドレスが、申請時のものと異なる事に起因しています。お問い合わせの前に今一度 Global IP アドレスをご確認ください。

以上