

Trend Micro Premium Service for Enterprise Threat Management Option 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、トレンドマイクロ・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、トレンドマイクロ 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、トレンドマイクロ 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ナップサービス、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、トレンドマイクロ バッテリーエイド、Trend Micro Safe Lock、トレンドマイクロ 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ナップサービス、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 -
・ TPS for Enterprise および DDI のご契約	- 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 -
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 -

※ 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

Trend Micro Premium Service for Enterprise（以下、「TPS for Enterprise」という）を保有するお客さまは、TPS for Enterprise の追加オプションとして TPS for Enterprise Threat Management Option（以下、「本サービス」という）をご契約いただけます。

本サービスでは、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、確認された脅威の詳細についての問い合わせ対応、一定期間の監視によりインシデント発生の推移や傾向の把握に加えて、詳細な分析に基づく今後の強化ポイントや課題の可視化を行い、ご報告する等のサービスをオプションとして提供します。

2. 本サービスをご利用いただくためのお客さまの準備

■ TPS for Enterprise および DDI のご契約

お客さまが本サービスをご利用いただくには、TPS for Enterprise の契約が必要となります。本サービスは TPS for Enterprise の追加オプションとなりますので、契約条件はお客さまが保有する TPS for Enterprise に準拠します。また、本サービスの提供先は、お客さまが保有する TPS for Enterprise でお客さまが任命されたコンタクトパーソンになります。

また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。

■ 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になるサービスをご利用のお客さまは、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。

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。サービスメニューの一部は、サービスチケットをご利用いただくことで提供可能になります。サービスチケットは TPS for Enterprise でお客さまに付与されたものをご利用頂けますが、本サービスをご契約いただいたお客さまには年間 30 サービスチケットが追加付与されます。

サービスメニュー	提供内容
<p>Critical Incident Notification Service</p> <p>サービスチケット不要</p>	<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ので、ご注意ください)</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. バンキングマルウェア 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のログ送信はおおよそ 1 時間程度毎に行われ、上記検出が含まれる場合はその都度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> <p>尚、通知に対するお問い合わせ対応および、通知を起点としたインシデント対応の支援は TPS for Enterprise で行います。その際の対応条件および支援内容は TPS for Enterprise サービスガイドブック内容に準拠いたします。</p>
<p>DDI Assessment Report</p> <p>15 サービスチケット でご利用可能</p>	<p>お客さま先に設置された DDI から当社指定システムに送信された DDI ログ (お客様任意指定で最大 4 週間分) を精査し、該当期間の傾向分析と注意すべき課題についてまとめ、レポートとして提供します。レポートは監視期間終了後、10 営業日を目途に提供されます。</p> <p>提供されるレポートには、以下のような内容が含まれます。</p> <ul style="list-style-type: none"> ・ 検知傾向の分析 ・ 脅威の発生推移 ・ 検知された脅威の集計 ・ 脅威が検知されたクライアントの集計 ・ 専門家によるアドバイザリ <p>レポートは本サービスをご契約頂いたお客さまが 15 サービスチケットをご利用いただくことで、1 レポート/年 1 回提供することが可能です。複数のレポート提供 (お客さまの拠点/セグメント毎などに分割したレポート作成や、年 2 回以上のレポート作成など) は、対応しておりません。</p> <p>本レポートに関する報告会をご希望の場合は、TPS for Enterprise のオンサイト対応 (要サービスチケット) で対応することが可能です。</p>
<p>DDI Monthly Summary Report</p> <p>20 サービスチケット/年 でご利用可能</p>	<p>お客さま先に設置された DDI から当社指定システムに送信された DDI ログを月次単位で集計し、セキュリティ運用の管理を目的とした毎月の検出傾向集計 (パターンファイル検出数、既知検出の種別、時系列の検出数推移など、端末情報は含まない) に関するサマリーレポートを提供します。レポートは毎月一日より 5 営業日以内を目途に提供されます。但し、提供予定日が祝祭日、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) の場合は、翌営業日に提供いたします。</p> <p>レポートは本サービスをご契約頂いたお客さまが 20 サービスチケットをご利用いただくことで、契約期間内において毎月提供することが可能です。契約期間途中でお申し込みいただく事も可能ですが、契約期間終了日以降のレポート提供は行われません。</p>
<p>通知およびレポートに関するお問い合わせ対応</p> <p>TPS for Enterprise で対応</p>	<p>本サービスで提供される通知およびレポートに関するお問い合わせは、TPS for Enterprise で対応します。お問い合わせ条件は TPS for Enterprise サービスガイドブック内容に準拠します。</p>

※ 「Critical Incident Notification Service」「DDI Assessment Report」「DDI Monthly Report」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。

4. 注意事項

■ 本サービスガイドブックについて

本サービスガイドブックは、TPS for Enterprise の追加オプションとして提供される本サービスについて記載されています。本サービスで提供される支援内容は本サービスガイドブックに記載されている内容のみとなります。また、本サービス提供に付随するお客さまの準備・お問い合わせ方法・注意事項等の諸条件で本サービスガイドブックに記載されていない内容および定義は、TPS for Enterprise サービスガイドブックに準拠します。また、本サービスガイドブック内容と、TPS for Enterprise サービスガイドブック内容に相違がある場合は、本サービスガイドブック内容が優先されます。

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、ご契約内容およびサービスチケット数が増える場合がございますので、事前にご相談ください。

■ 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、レポートの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、その際は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およびレポートについて

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およびレポートを提供しますが、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、提供されるレポートフォーマットは、お客さまにとってわかり易く、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、PSC 経由でお問い合わせください。

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。
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。

※ 本定義に記載されていない項目は、最新の TPS for Enterprise サービスガイドブックに準拠します。

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) ・ 電話窓口 : 03-5334-3862 <ul style="list-style-type: none"> ➢ 電話窓口は、緊急時のみ、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 (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)
運用開始後	DDI のレポートに関するお問い合わせ 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"> ・ TPS for Enterprise サービスガイドブックに記載されたお問い合わせ方法にてお問い合わせ下さい。

※ 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。

※ 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