トレンドマイクロ社製品の利用申請手順書

第三版

北里大学情報基盤センター

・・・・・ 目　次 ・・・・・

・・・・・ 目　次 ・・・・・

1.トレンドマイクロ社製品の全学的な導入について

1-1.導入目的

情報基盤センターで一括購入・管理を行うことにより、各部門等の教職員による購入・更新及びライセンス管理に係る負担を軽減し、適切な使用によるコンプライアンスの強化を目的としています。また、製品及びライセンスを纏めることによりウイルス対策ソフトに要する費用の軽減を図ります。

1-2.導入製品

メーカー：トレンドマイクロ株式会社
製 品 名：Client/Server Suite Premium（略称：C/SS Premium）

1-3.使用可能な製品群

C/SS Premiumのライセンスを保有することにより、様々な製品を使用することができます。ライセンス契約上では、以下の製品以外にも利用可能なものがありますが、現時点では運用を考慮して以下の製品のみを利用可能としています。

・WindowsOS（クライアント／サーバ）対応製品
ウイルスバスターコーポレートエディション（略称：ウイルスバスターCorp.）

・MacOS対応製品
Trend Micro Security (for Mac)

・その他
Webレピュテーション
ダメージクリーンナップサービス（DCS）
仮想デスクトップ（VDI）対策用AC

1-4.製品別の機能比較

製品比較 / 主な機能	Client/Server Suite Premium	Client/Server Suite	ｳｲﾙｽﾊﾞｽﾀｰCorp. Client
1.クライアントウイルス対策	●	●	●
2.サーバウイルス対策	●	●	
3.ボット対策(*)	●	●	●
4.ルートキット対策(*)	●	●	●
5.メール対策	●	●	●
6.スパイウェア対策(*)	●		
7.不正サイトへのアクセスブロック(*)	●		
8.ダメージクリーンナップ(*)	●		
9.検疫（ＮＡＣ）対応	●	●	●

※用語集をご確認下さい

1-5.利用上の注意

トレンドマイクロ社製品や他のウイルス対策ソフトウェアを導入することにより、ウイルス感染しないことを保証するものではありません。ウイルス対策ソフトウェアの導入目的はウイルスを早期に発見して感染を未然に防ぐこと、感染した場合であっても被害を最小限にすることです。

ウイルス対策ソフトウェアは出現したウイルスに対応するものであるため、未知のウイルスが発見されてからウイルス対策ソフトウェアの各メーカーが、そのウイルスに対応できるパターンファイルや検索エンジンなどツールを提供できるようになるまでに時間的な「差」が生じます。そして、対応されたツールが私たちのパソコンに反映し機能するまでに更なる「差」が生まれます。この「差」の中で感染被害が拡大することになります。

未知のウイルスは、誰かのパソコンに感染し何らかの被害が起こってから初めて見つかり、その被害の内容がウイルス対策ソフトウェアメーカーに提供されることによって、初めて「既知」のウイルスとなるのです。

情報基盤センターは、パソコンへのインストール（またはアンインストール）や管理サーバの構築や運用について、技術的な問い合わせには対応しておりません。

「インストール時にエラーとなってインストールすることができない・・」
「ウイルスに感染したファイルが見つかったがどのように対応すればよいかわからない・・」

このような場合はトレンドマイクロ社のホームページ等を参考にして各自またはパソコンを管理されている方で対応を行って下さい。それでも、対応できないような場合は情報基盤センターまでお問い合わせ下さい。情報基盤センターがトレンドマイクロ社等に問い合わせを行い、対応方法についてお伝えいたします。

なお、現在はトレンドマイクロ社とのサポート契約は締結しておりませんが、ウイルスの大規模感染や深刻な被害への対応、ウイルス対策環境の構築や整備に関する提案を受けることができるようサポート契約の締結を検討しております。
サポート契約を締結した場合は、そのサポート範囲や内容について改めてお知らせいたします。

情報基盤センター職員が問題の発生しているパソコン等に対して直接操作して対応するようなことは行いませんので、予めご了承下さい。

重複となりますが、トレンドマイクロ社製品であるウイルスバスターCorp.やTrend Micro Securityをインストールしても、ウイルス感染しないことを保証するものではありません。どんなウイルス対策ソフトウェアを導入しても、常に感染のリスクがあることをご認識下さい。

2. ご利用の前に必ずご確認下さい・・・

2-1. 管理者への確認

既にパソコンには何らかのウイルス対策ソフトウェア（以下、ソフトウェア）がインストールされていると思われます。そのソフトウェアを個人でインストールされた方は、ご自身でご案内している製品の利用可否を判断できると思います。しかし、部門や研究室等にソフトウェアの管理者がおり、その管理者がインストール作業や導入可否の判断、パソコンの管理を行われている場合は、必ずその管理者へ導入についてご確認下さい。

2-2. 業者への確認

上記2-1と同様に、ウイルス対策ソフトウェアやパソコンの管理を業者に委託している場合は、導入可否について必ず当該業者へ確認して下さい。

2-3. 業務系システムや他ソフトウェアとの共存

パソコンに業務系システムや他のソフトウェアがインストールされている場合は、そのシステムやソフトウェアの動作に支障をきたす恐れがありますので、導入前に必ずシステムや他のソフトウェアとの共存が可能であるかをメーカー等にご確認下さい。

2-4. 他のウイルス対策ソフトウェアとの併用

既にパソコンには何らかのウイルス対策ソフトウェアがインストールされていると思われます。トレンドマイクロ社製品も他メーカーのウイルス対策ソフトウェアとの併用について制限がある場合があります。また、同じトレンドマイクロ社製品であっても併用できない場合があります。他のウイルス対策ソフトウェアとの併用を望まれる場合は、その可否について必ずご確認下さい。

既存ウイルス対策ソフトウェアの併用を必要としない場合や併用について不明な場合は、必ず、既存ウイルス対策ソフトウェアのアンインストール（削除）を行ってから、ウイルスバスターCorpやTrend Micro Securityをインストールして下さい。

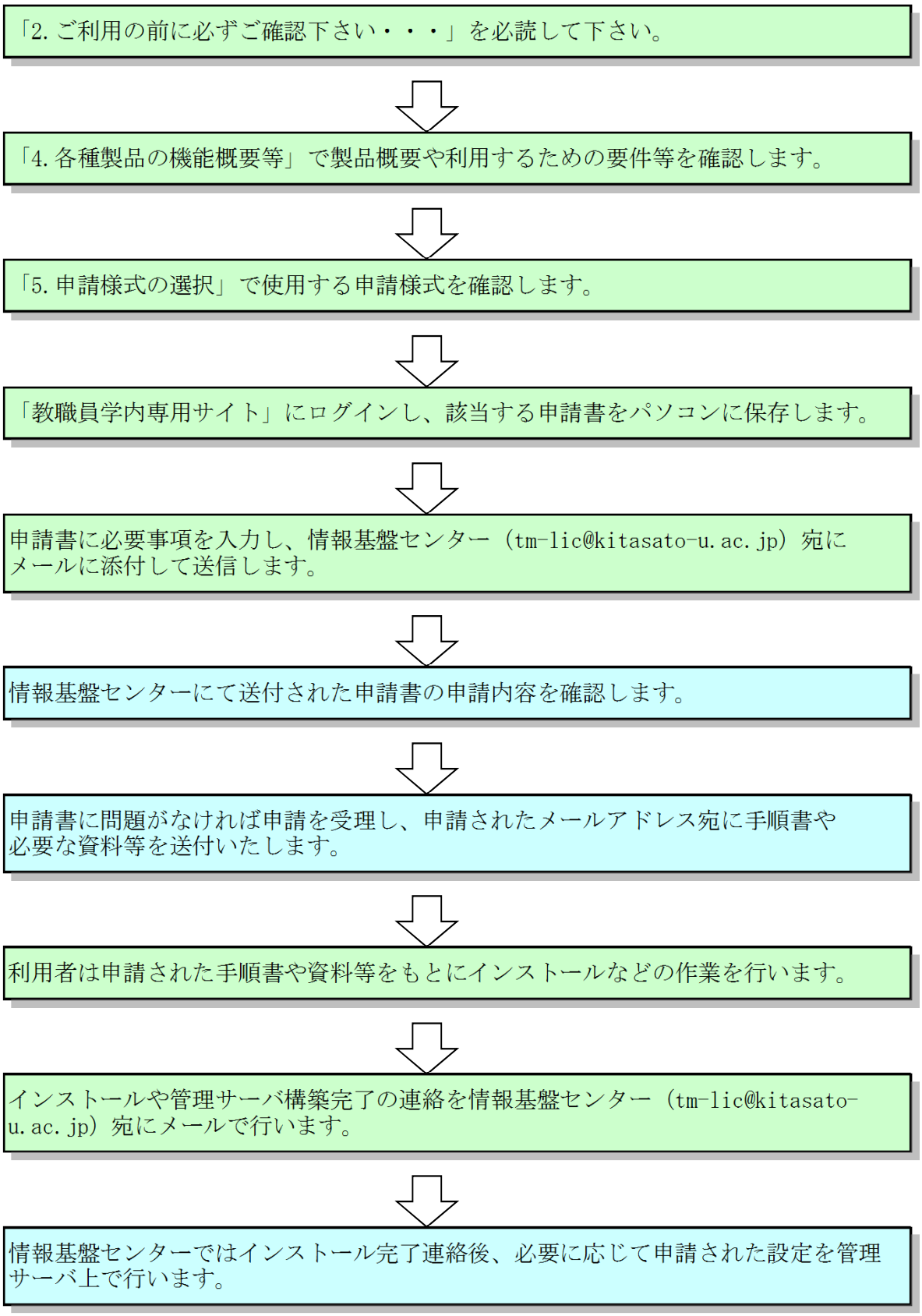
併用が認められていない条件で併用をした場合、パソコンが正常に起動しなくなる恐れがありますので、双方のシステム要件等にて必ずご確認下さい。

2-5. ライセンスの確認

ご案内している製品については、ライセンスの更新・管理を情報基盤センターで行います。現在使用されているパソコンのウイルス対策ソフトウェアを削除（アンインストール）して不要となった場合は、次年度以降更新する必要がなくなります。不要な費用を支払わないためにも、ウイルス対策ソフトウェアの更新時期や保有しているライセンス数などについてご確認下さい。

3. 申請手順

申請から運用開始までは以下のような手順になります。



4.各種製品の機能概要等

4-1.ウイルスバスターCorp.【バージョン10.5（現時点での最新）】

4-1-1.機能概要

特徴としてスマートスキャンという機能があります。これは、ウイルスチェックに必要となるパターンファイルをすべてクライアントに配信するのではなく、大半をSmart Protection Server（構築する管理サーバ）に配置します。

そして、クライアント上で動作する「ウイルスバスターCopr.クライアント」が不正な疑いのあるファイルを見つけた場合には、クライアントにあるパターンなどに該当するものが無い時に限り、Smart Protection Serverに問い合わせをさせるというものです。

この機能によって、どのクライアントマシンも常に最新のセキュリティレベルを提供できるとともに、アンチウイルスの運用におけるネットワークへの負荷、そしてメモリやCPU使用量などのシステム負荷を長期的に削減、抑制することができます。

4-1-2.システム要件

システム要件については以下のＨＰを参考に、利用される機器で適用可能であるかをご確認下さい。
以下のＨＰはバージョン10.5のシステム要件となります。提供するソフトウェアのバージョンアップやアップグレードを行った場合は、改めてご案内いたします。

http://jp.trendmicro.com/jp/products/enterprise/corp10_5/requirements/index.html

4-1-3.管理サーバを構築される（されている）管理者の方へ

ウイルスバスターCorp.管理サーバの構築を検討されている方、現在使用されている管理サーバのアップグレードを検討されている方は、必ず以下のＨＰにてシステム要件や制限事項などをご確認下さい。

・Readme
http://www.trendmicro.com/ftp/jp/ucmodule/corp/win/105/readme_r8.htm

・インストールガイド
http://www.trendmicro.com/ftp/jp/ucmodule/corp/win/105/OSCE105_InstallGuide_r1.pdf

・管理者ガイド
http://www.trendmicro.com/ftp/jp/ucmodule/corp/win/105/OSCE_105_AdminGuide.pdf

・既知の制限事項
http://esupport.trendmicro.co.jp/Pages/JP-2077937.aspx

4-2.Trend Micro Security（for Mac）【バージョン1.5 SP3（現時点での最新）】

4-2-1.機能概要

MacOS環境では見逃されがちなウイルスやスパイウェア対策を提供します。また、Webから侵入する脅威についても、Webレピュテーション機能により高い防御力を発揮します。セキュリティ設定やライセンス更新を一元的に管理して、Windowsとの混在環境でセキュリティ対策レベルを統一できます。

この製品はウイルスバスターCorp.のプラグイン製品となります。情報基盤センター設置の管理サーバを利用しないでこの製品を使用される場合は、ウイルスバスターCorp.管理サーバを構築する必要があります。

4-2-2.システム要件

システム要件については以下のＨＰを参考に、利用される機器で適用可能であるかをご確認下さい。
以下のＨＰはウイルスバスターCorp.のシステム要件ですが、ＨＰの下段にTrend Micro Securityのシステム要件があります。提供するソフトウェアのバージョンアップやアップグレードを行った場合は、改めてご案内いたします。

http://jp.trendmicro.com/jp/products/enterprise/corp10_5/requirements/index.html

4-3.Webレピュテーション

4-3-1.機能概要

ウイルスに感染する可能性のある危険な不正サイトや改竄サイト、フィッシングサイトなどへのWebアクセスを未然に防ぎ、運用するネットワークの安全を守るのに有効なのがWebレピュテーションサービスです。

トレンドマイクロが提供するWebレピュテーションは、同社の脅威情報収集ネットワークによって収集した様々な情報を基に行います。膨大なWeb評価データベースには、ドメイン・ＩＰアドレスなどの登録変更履歴やフィッシングサイトやスパム送信元としてデータベースへの登録があるか、不正プログラムの検出履歴など、多面的にそのWebサイトの危険度を採点化したものが蓄積・更新されています。

WebレピュテーションはユーザがWebサイトにアクセスするなどの通信が発生する際にTrend Micro Smart Protection Networkに自動的に問い合わせを行い、接続先ドメイン、Webサイト、Webページが不正な場合にはアクセス自体をブロックすることによって不正プログラムによる感染、フィッシング詐欺サイトへのアクセスを防ぐことができます。

4-3-2.メリット

Webからのウイルス感染の防止
・ガンブラーなどのウイルス感染Webサイトへのアクセス防止
・トロイの木馬が仕掛けられたWebサイトへのアクセス防止

ファーミング詐欺、フィッシング詐欺の防止
・偽サイト、フィッシングサイトへのアクセス防止

4-3-3.URLフィルターとの違い

Webレピュテーションがチェックするもの
コンテンツ内容を問わず、セキュリティ脅威が高いと思われるサイト
・ウイルス感染や改竄履歴
・フィッシング・ファーミングサイトかどうか
・スパム送信元か
・変更履歴などその他もろもろ

URLフィルターがチェックするもの
コンテンツ内容がどのカテゴリ(掲示板、アダルト、旅行、ブログ/SNS等々)に属するか
・どのカテゴリに該当するか

２つのWebセキュリティ対策は相互に補完しあう関係です。

Webレピュテーションの目的
・ウイルスや詐欺サイトなど、Webからの脅威をブロック
・ダウンローダー（ウイルスの一種）による多重感染をブロック
※ダウンローダーとはインターネット上のサイトから他の不正プログラムをダウンロードし、インストールする活動を行う不正プログラムのこと。

URLフィルターの目的
・効果的なWebアクセス管理実現による、業務効率の向上
・不適切Webサイト閲覧のブロック

4-3-4.利用方法

Webレピュテーションサービスは単体で使用できるものではありません。「ウイルスバスターCorp.」や「Trend Micro Sucurity (for Mac)」に付随して利用するものです。また、利用を強制するものではなく、例えば、「ウイルスバスターCorp.」の利用者がWebレピュテーションサービスを利用する／しないを選択することができます。

4-3-5.利用可能製品

情報基盤センターが提供する「ウイルスバスターCorp.」および「Trend Micro Sucurity (for Mac)」はWebレピュテーションサービスを利用することができます。これ以外の製品での利用可否を確認する場合は、以下のＨＰを参考にして下さい。

http://www.trendmicro.co.jp/spn/features/web/

4-4.ダメージクリーンナップ【バージョン3.2（現時点での最新）】

4-4-1.機能概要

トレンドマイクロ　ダメージクリーンナップサービス（以下、DCS）は、システムのダメージを診断しクリーンナップする包括的なサービスです。ネットワークを繰り返し攻撃する可能性のあるスパイウェア、ウイルス、トロイの木馬、不正プログラムを自動的に削除し、改変されたレジストリとメモリを復旧します。また、最新版にはルートキットの検出及び削除用の新しいコンポーネントが含まれています。

4-4-2.利用方法

DCSは「ウイルスバスターCorp.」のオプション機能として動作するのとは別に、単体で使用するための環境を構築できます。その場合、クライアント単体で利用することはできず、必ず管理するためのサーバを構築する必要があります。
また、単体で使用するばあいの最新版3.2はプログラム及び管理者ガイドが英語版のみの提供となっています。

4-4-3.システム要件

システム要件については以下のＨＰを参考に、利用される機器で適用可能であるかをご確認下さい。提供するソフトウェアのバージョンアップやアップグレードを行った場合は、改めてご案内いたします。

http://www.trendmicro.com/ftp/jp/ucmodule/dcs/3.2/DCS32_1023_Repack3_readme_JP.txt

4-5.仮想デスクトップ環境（VDI）対応

4-5-1.機能概要

VDIとは、PC上にあるクライアント環境をサーバ上で稼動させる仕組みであり、仮想マシンは自由に作成することができ、あたかも物理的なPCのように使用することができます。運用コスト削減、PCの長期利用、構成管理の徹底、また「クラウド化」の基礎技術であるといった理由から「VMware View」や「Citrix XenDesktop」に代表されるVDIが注目されています。

「ウイルスバスターCorp.10.5」はVDIに使用される一般的な仮想化ソフト「VMware View」と「Citrix XenDesktop」の双方に最適化されており、これらの環境を保護します。
個々の仮想マシンに対するウイルス検索やパターンファイルをアップデートするタイミングを自動で調整し、過負荷を防止します。さらに、OSやアプリケーションなど、各仮想マシンでリンク元として共有するマスターイメージ部分をホワイトリストとして検索対象から除外登録することにより、 CPUやHDDへの負荷を低減しながら、ウイルス検索時間を大幅に短縮しました。

4-5-2.システム要件

システム要件については以下のＨＰを参考に、利用される機器で適用可能であるかをご確認下さい。
以下のＨＰはバージョン10.5のシステム要件となります。提供するソフトウェアのバージョンアップやアップグレードを行った場合は、改めてご案内いたします。

http://jp.trendmicro.com/jp/products/enterprise/corp10_5/requirements/index.html

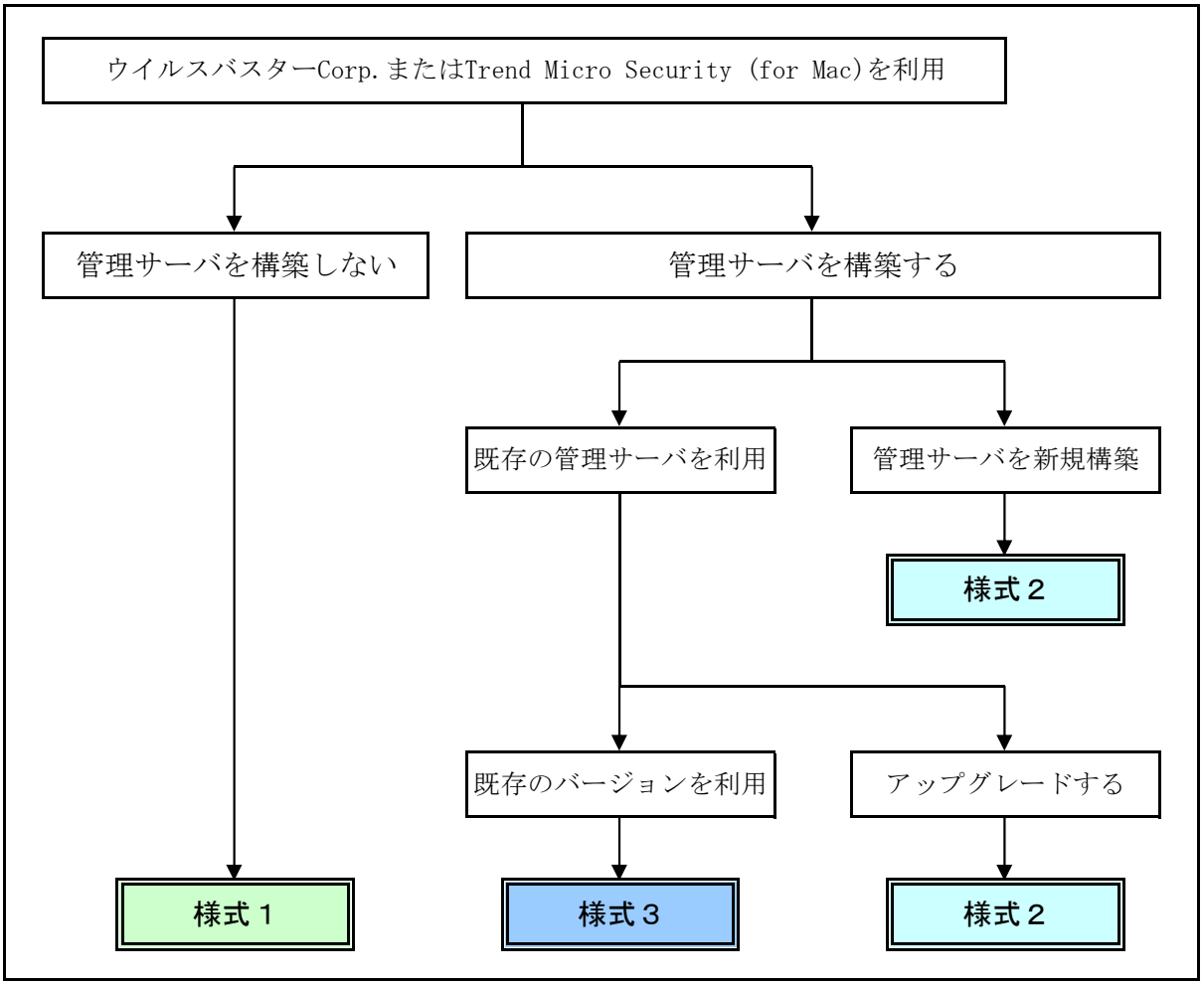
4-5-3.仮想環境上でのサポート対応状況

トレンドマイクロ製品の仮想環境上でのサポート対応状況については以下のＨＰを参考にご確認下さい。

http://esupport.trendmicro.co.jp/Pages/JP-2078573.aspx

5.申請様式の選択

5-1.ウイルスバスターCorp.またはTrend Micro Security (for Mac)を利用



5-2.ダメージクリーンナップサービスを利用

様式４

6.用語集

スパイウェア

主に情報漏洩につながる活動を行うプログラム。コンピュータ内の特定の情報を収集したり、収集した情報を外部に送信するなどの活動がある。

ダメージクリーンナップサービス

ネットワーク上のコンピュータにソフトウェアをインストールせずに、システム ダメージを評価してクリーニングするための包括的なサービスです。ネットワークを繰り返し攻撃する可能性のあるネットワークウイルスを削除して、次の機能を実行します。

- ワームまたはトロイの木馬によって作成された不要なレジストリ エントリを削除する。
- メモリ常駐型のワームまたはトロイの木馬を削除する。
- アクティブなスパイウェアおよびグレーウェアを削除する。
- ルートキットを削除する。
- ウイルスによって投下された不要なファイルおよびウイルス ファイルを削除する。
- システムを評価して感染しているかどうかを判断する。
- システムをクリーンな状態に戻す。
- スパイウェアおよびグレーウェアを検出する。

バックドア型

トロイの木馬の一種。ネットワークを介して被害者のマシンを自由に操ったり、パスワードなど重要な情報を盗んだりすることを目的としている。サーバモジュールをクライアントモジュールから遠隔操作する形式になっており「サーバ＝クライアント型」とも呼ばれる。まず、不正プログラムをターゲットとするコンピュータに侵入させる。それに対応するプログラムをインストールしたコンピュータを使って、ターゲットとしたコンピュータを外部から操作する。ちょうど被害に遭ったコンピュータはバックドア（裏口）が開いたような形になる。

ボットウイルス

ロボット（roBOT）から由来される、バックドア型不正プログラムのこと。コンピュータに感染後、ユーザに気づかれないように活動し、悪意のハッカーからの指示を受けて、コンピュータがロボットのように操作されてしまう。外部操作により、スパムメール送信、サーバ攻撃、などの不正活動に利用されてしまう。

ルートキット

主にファイルやレジストリなどをシステムから隠す活動を行う不正プログラムのこと。元々は悪意のハッカーが不正アクセスなどハッキングの際に使用するツール（群）の呼称だった。WindowsシステムのAPIをフックしてユーザやセキュリティ対策アプリケーションから自身や他の不正プログラムの実体や活動の痕跡にアクセスできないようにする活動を行う。

Webレピュテーション（不正サイトへのアクセスブロック）

レピュテーションとは、評価・評判のことです。つまり、Webレピュテーションとは、クラウドを利用したレピュテーション型のWebサイトの評価技術です。不正ファイルのほとんどはWebサイトから侵入してくるため、それらのサイトへのアクセスをブロックすることで、高いセキュリティを提供できます。HTTP要求を受信するたびに（例えば、インターネットでWebページを閲覧する度に）、不正サイトの情報が格納されているデータベースに照会し、要求された全てのWebサイトのセキュリティリスクを評価して、危険性の高いサイトへの接続を遮断します。

メモとしてご利用下さい