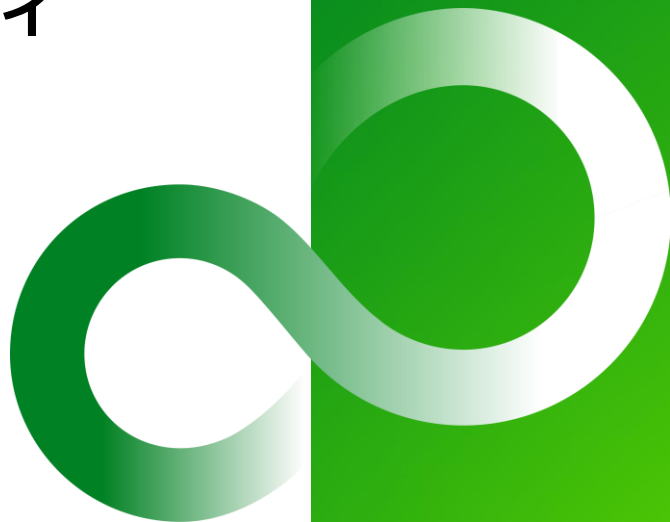


サーバー向けクラウド型セキュリティ (Trend Micro Cloud One – Workload Security) ご紹介資料

富士通クラウドテクノロジーズ株式会社(FJCT)

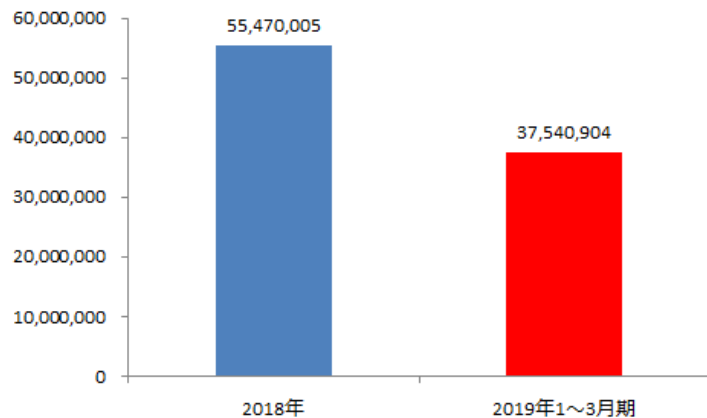


会社名	トレンドマイクロ株式会社
所在地	東京（日経225に選出） 〒151-0053 東京都渋谷区代々木2-1-1 新宿マインズタワー
事業内容	コンピュータ及びインターネット用セキュリティ関連製品・サービスの開発・販売
創業	1988年
従業員数 (全世界)	6,562名（2018年時点）
代表取締役社長 兼 CEO	エバ・チェン
取締役副社長	大三川 彰彦



最新脅威動向

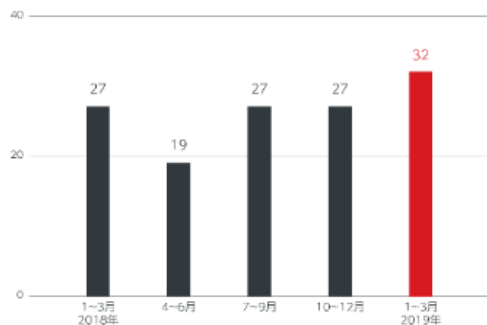
2019年ランサムウェア攻撃が増加傾向



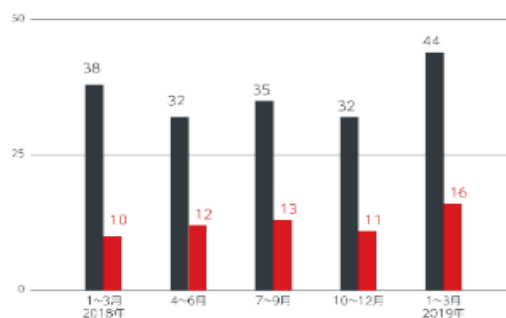
ランサムウェアとは

感染したPCをロックしたり、ファイルを暗号化したりすることによって使用不能にしたのち、元に戻すことと引き換えに「身代金」を要求する不正プログラムです。身代金要求型不正プログラムとも呼ばれます。

2018年に急減したランサムウェア攻撃の件数が2019年に入り増加傾向にあります。



図：主に英語圏の法人でのランサムウェア被害報道件数推移
(発生日もしくは公表日に
基づきトレンドマイクロが独自
に作成)



図：国内法人からのランサムウェア関連問い合わせ件数（黒）とそのうちの被害報告件数（赤）の推移（トレンドマイクロ調べ）

標的型の攻撃手法が確認されたランサムウェア被害事例

○ノルウェーの大手製造業

- 「LockerGoga」の破壊的な活動で複数工場が一時操業停止
- 感染前の攻撃段階でPsExecの使用を確認
- ランサムノートに「Your Company」の文言

○米国製造会社での被害（トレンドマイクロ調査）

- PowerShell RAT「Empire」による管理者権限の奪取とPsExecを利用した「BitPaymer」の遠隔感染の流れを確認
- ランサムノートと暗号化ファイルの拡張子に被害企業名を使用

サーバ攻撃によるシステムへの影響

データの改ざんや持ち出し、破壊



コンピュータ上に保存してあるデータの持ち出しや破壊が行われます。
経理データや顧客データに対しての改ざんが行われた＆気づかなかった場合、取り返しのつかない事態に陥りかねません。

OSやプログラムの改ざん、破壊



踏み台攻撃、データの盗聴、不正アクセスの痕跡を消し去るなどが目的。
攻撃の踏み台になってしまった場合は、被害者側から賠償請求される可能性もあります。

コンピュータリソースの無断使用



コンピュータ上のリソースを無断使用して利益を生み出そうとします。
近年では乗っ取ったサーバ上でビットコインの製造などを行い、換金する手法なども流行しています。

運営の妨害



DDoS攻撃などによる業務妨害を受け、正規の顧客へのサービス提供ができなくなります。
数日間にわたりネットワークがマヒしてしまったISPが復旧を断念してサービス撤退してしまったこともあります。

サーバ攻撃の手法とその対策



<標的型攻撃のフローについて>

攻撃者は、金銭的利益につながる情報を持ち出すことを目的に、入念な準備を行い、侵入・情報探索・情報送出を行います。

標的型攻撃の被害を防ぐためには、情報送出に至るまでのいずれかのステップで阻止することが必要です。

しかし、攻撃者の手口も巧妙化しており、どこか1つのステップで100%攻撃を防ぐことは困難です。

標的型攻撃を未然に防ぐためには、『多層防御』の考え方を取り入れ、各ステップ“ごと”にセキュリティ対策を施すことが重要です。

<（上図に沿った）サーバに対する攻撃と対策>

攻撃者	<div>1 新規侵入</div> <div>2 脆弱性を悪用して不正アクセス</div> <div>「何のOS/アプリケーション/ミドルウェアが動作しているのか?」「待ち受けているポートは?」などサーバの情報を収集します。 システムの情報をもとに、攻撃の穴（脆弱性）を利用して、外部からコマンド操作などを行います。</div>	<div>3 サーバ制御</div> <div>外部からリモートコントロールするためにバックドア設置</div> <div>外部から任意にサーバを操れるようにするため、バックドアを設置します。実行型ファイルを用いたり、Webshellを設置したり、その手法は多岐に渡ります。 侵入を拡大されないよう、攻撃者との通信を切断するなどの対策が必要です。</div>	<div>4 情報探索・集約</div> <div>社内LAN内の感染端末からサーバーへのファイル転送・リモート実行など</div> <div>STEP3で設置したバックドアを利用して、別の端末へ感染を拡大します。サーバを乗っ取るため、パスワードクラッキングや機密データ収集の痕跡が見られます。ログデータの不審な動きを見落とさないことが重要です。</div>	<div>6 情報送出・改ざん</div> <div>攻撃者が使用するサーバーへ情報送出・Webサーバに不正プログラム配置など</div> <div>STEP4,5で収集した機密情報を外部へ送出します。 外部公開サーバの場合はコンテンツの改ざんなどが行われることもあります。改ざんにより、ECサイトの停止（売上損害）、不正プログラムの設置（ユーザーへの被害）などが行われます。</div>
必要な対策	脆弱性を突く攻撃をブロック	C&Cサーバーへの接続をブロック	サーバに対する不審な通信をブロック	犯罪に利用されているサーバーへの接続をブロック

Trend Micro Cloud One – Workload Security(※ 1)は、サーバセキュリティに必要な複数の機能を1つの保護モジュールに実装した総合サーバセキュリティ対策製品です。

複数のセキュリティ機能を統合的に提供します。
(右図)

複数のセキュリティ製品を組み合わせる必要がなく、コストと運用負荷を最小化しつつ、社内サーバのセキュリティポリシーの統一化を図ります。

多様なサーバ環境や標的型サイバー攻撃対策といったセキュリティ課題をシンプルに解決します。

クラウド環境の
セキュリティ対策

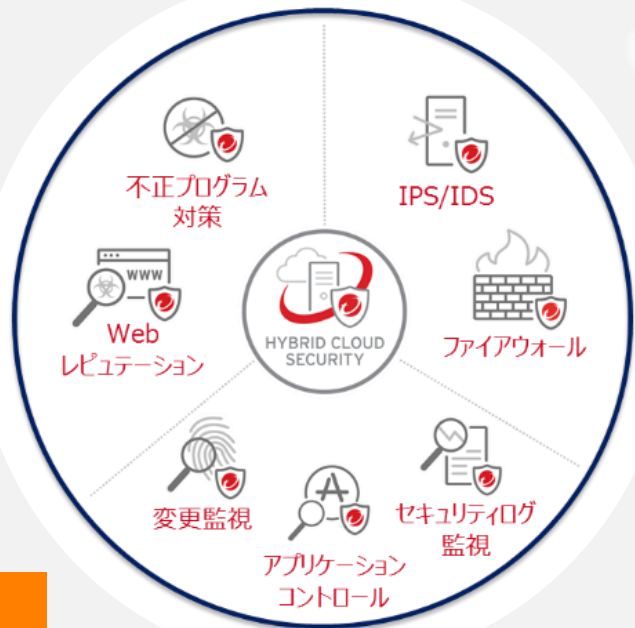
サーバ仮想環境の
セキュリティ対策

VDI環境の
セキュリティ対策

コンテナ環境の
セキュリティ対策

レガシーOS
延命利用対策

PCI DSS
準拠支援



vmware

aws

クラウドとの連携

- ・ Auto Scaling対応
- ・ コンソール連携

IBM

Microsoft Azure

NIFCLOUD
ニフクラ

※ 1 「Trend Micro Cloud One – Workload Security」について、本ページ以降「Workload Security」と呼称させていただきます。

ハイブリッドなサーバー環境に対応

- 「ハイブリッドな環境」
- 「マルチプラットフォーム」
- 「マルチクラウド」を一括管理

サポート対象OS*

Windows

Windows
Server

Red Hat

CentOS

SUSE

等



物理サーバ



仮想サーバ

※ Workload Securityでは
Agent型のみ



クラウド上の
サーバ

対応クラウド



Microsoft Azure

等

*サポート対象OSの詳細については、Webページをご参照ください。

▶ www.go-tm.jp/tmdsaas



全部まとめて、ひとつのコンソールで管理可能！

コンソール画面から一括管理が可能なため**管理負荷の軽減を実現**

サーバを保護する機能

不正プログラム対策
アンチウィルス機能
CTD機能(検出)
CTD機能(防御)
ランサムウェア対策
機械学習型検索機能
Webレピュテーション
ファイアウォール
侵入防御
概要説明
仮想パッチとは
推奨設定について
変更監視
概要説明
その他機能について
セキュリティログ監視
アプリケーションコントロール

トレンドマイクロの**Smart Protection Network(SPN)**を活用することで最新の脅威情報を用いて不正プログラムを検知/防御することが可能です。



SPN :

世界各地から検知された脅威情報が蓄積される、
トレンドマイクロのデータベース

- ・世界各地の**2.5億**の脅威検知デバイス
- ・年間で**3兆件以上**の情報を処理
- ・年間で**650億件以上**の脅威をブロック

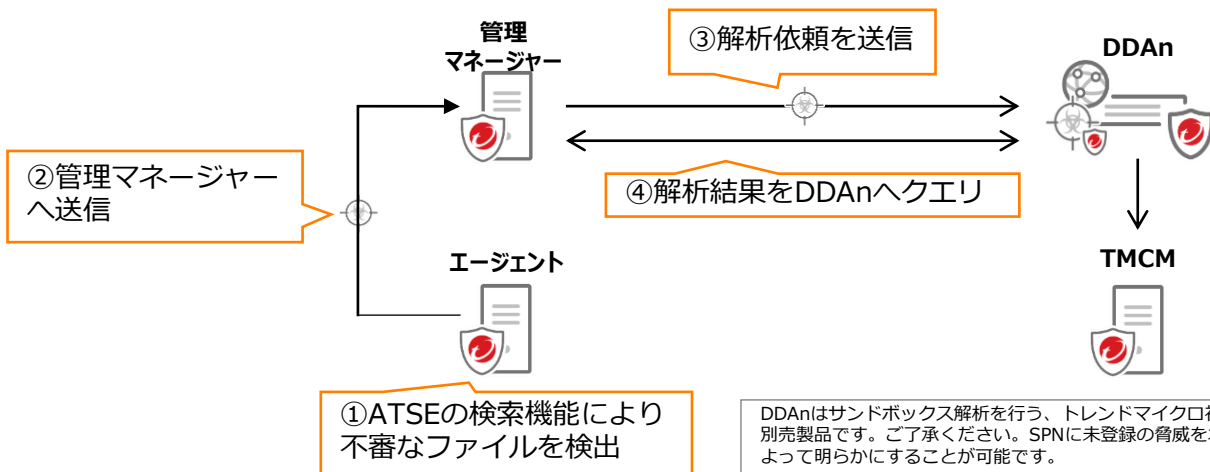
*2018年トレンドマイクロ調べ

SPNから最新の脅威情報を取得し、
その情報に一致する不正プログラムを検知

不正プログラム対策：CTD機能(検出)

不正プログラム対策
アンチウイルス機能
CTD機能(検出)
CTD機能(防御)
ランサムウェア対策
機械学習型検索機能
Webレピュテーション
ファイアウォール
侵入防御
概要説明
仮想パッチとは
推奨設定について
変更監視
概要説明
その他機能について
セキュリティログ監視
アプリケーションコントロール

他製品と連携して未知の脅威を防御する**Connected Threat Defense(CTD)**に対応しています。Workload Security側で不審なファイルを検出し、**DDAn**へ解析依頼を送信します。**ATSE**と呼ばれる高度な脅威検索機能を用いることで、エージェントは**不審なファイル**を検出し、それを管理マネージャー経由で**DDAn**へ**サンドボックス解析依頼**を送信します。そこで脅威と判断されたものは後述の**TCCM**へと共有されます。



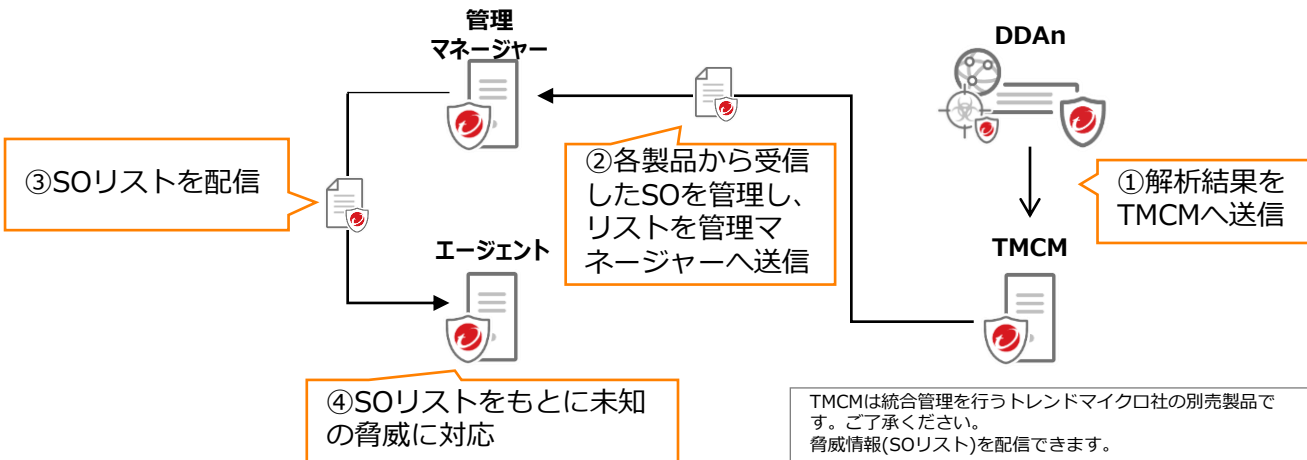
不正プログラム対策：CTD機能(防御)

不正プログラム対策
アンチウイルス機能
CTD機能(検出)
CTD機能(防御)
ランサムウェア対策
機械学習型検索機能
Webレピュテーション
ファイアウォール
侵入防御
概要説明
仮想パッチとは
推奨設定について
変更監視
概要説明
その他機能について
セキュリティログ監視
アプリケーションコントロール

TMCMで管理されている不審オブジェクトリスト(SOリスト)を定期的を取得し、それを未知な脅威の判断根拠とします。

TMCMは製品の統合管理を行い、同時にDDAn等から、脅威と判断されたSOリストを取得および保持しています。本リストを定期的を取得し、リスト上の脅威と同じハッシュ値をもつファイルを検出した場合に防御します。

※SOリストは、URL（SPSクエリ）などにも対応しています。詳細は別資料を参照ください。



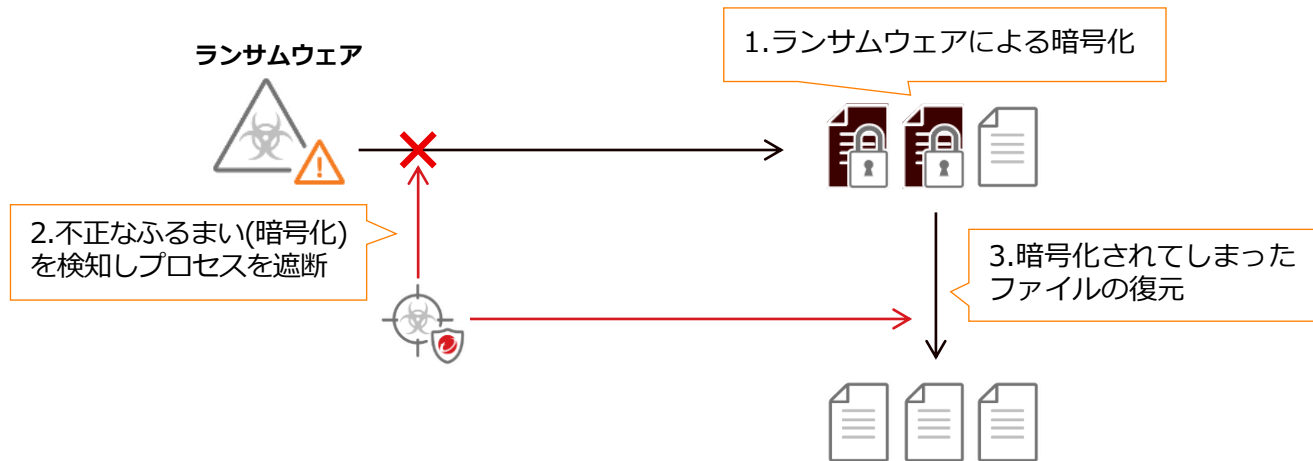
不正プログラム対策：ランサムウェア対策

不正プログラム対策	
アンチウイルス機能	
CTD機能(検出)	
CTD機能(防御)	
ランサムウェア対策	
機械学習型検索機能	
Webレピュテーション	
ファイアウォール	
侵入防御	
概要説明	
仮想パッチとは	
推奨設定について	
変更監視	
概要説明	
その他機能について	
セキュリティログ監視	
アプリケーションコントロール	

ランサムウェアがファイルの暗号化を始めた際に、そのふるまいを検知してプロセスを止めることができます。また、暗号化されてしまったファイルを復元することも可能です。

前述のパターンマッチングによる検知だけではなく、ふるまい監視による不正なプロセスの検知も可能です。

※本機能はDSVAでは未対応です。本機能はWindowsにのみ対応しています。



不正プログラム対策：機械学習型検索機能

不正プログラム対策
アンチウイルス機能
CTD機能(検出)
CTD機能(防御)
ランサムウェア対策
機械学習型検索機能
Webレピュテーション
ファイアウォール
侵入防御
概要説明
仮想パッチとは
推奨設定について
変更監視
概要説明
その他機能について
セキュリティログ監視
アプリケーションコントロール

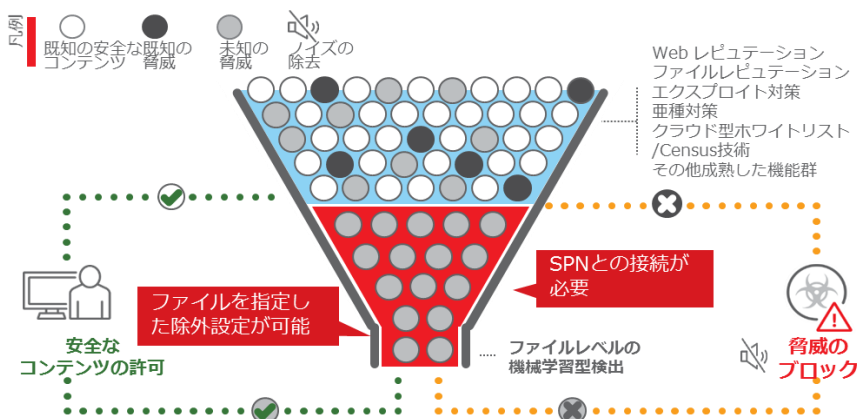
標的型攻撃など高度な不正プログラムに対して、**未知の脅威**を検出する**次世代型の脅威対策**、**機械学習型検索機能**を提供します。

※本機能はWindows版エージェントおよびDSVAが対応しています。

※Workload Security10.2から有効になります。

※SPS経由でなく、SPNと直接接続できる必要があります。

AI技術を導入することで
パターン更新前のウイルスの亜種や未知の脅威に対する検知力を向上します。

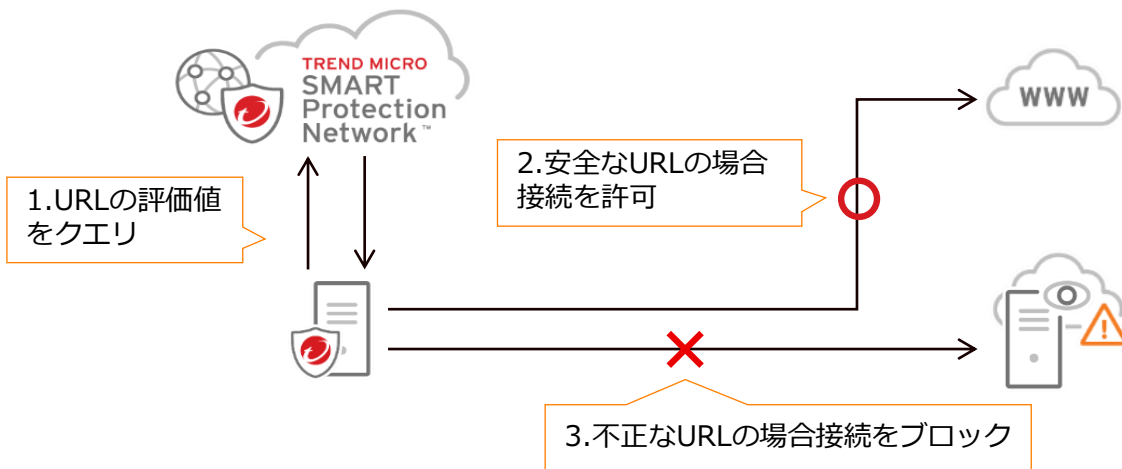


不正プログラム対策
アンチウイルス機能
CTD機能(検出)
CTD機能(防御)
ランサムウェア対策
機械学習型検索機能
Webレピュテーション
ファイアウォール
侵入防御
概要説明
仮想パッチとは
推奨設定について
変更監視
概要説明
その他機能について
セキュリティログ監視
アプリケーションコントロール

サーバからWebアクセスを行った場合、当該URLの安全性を確認し、それが不正であった場合は、接続をブロックすることができます。

※本機能はhttpのみに対応しています。httpsは非対応です。

通常、ユーザがサーバから故意にインターネットへ接続することはありませんが、**不正プログラムによってC&Cサーバ等と接続されるケースがあります。**
その場合、本Webレピュテーション機能によって不正な接続をブロックする必要があります。





レイヤ2-4をカバーする詳細なポリシー設定が可能です。ホスト型であるため、ネットワーク外からの攻撃だけでなく、感染端末による社内ネットワークからサーバへの通信の防御を実現することができます。

本機能のポリシーには
TCP/UDP/ICMPに関してはステートフルインスペクション機能を設定することも可能です。

対応フレーム種別

IP / ARP / REVARP / 任意指定のフレーム番号

通信元/通信先指定方法

単一 IP アドレス / サブネット指定 / アドレス範囲 / 複数 IP アドレス / 予め定義した IP アドレスリスト / 単一 MAC アドレス / 複数 MAC アドレス /
予め定義した MAC アドレスリスト、通信方向として Incoming / Outgoing を選択

対応プロトコル

ICMP / IGMP / GGP / TCP / PUP / UDP / IDP / ND / RAW / 任意指定のプロトコル番号
※ICMP / TCP についてはフラグ指定可能

フィルタアクション

Allow / Bypass / Deny / Force Allow / Log Only
Priority:4-0で定義

通信失敗時の挙動

初期設定は「フェイルクローズ」、Workload Security10.2から「フェイルオープン」に変更可能

不正プログラム対策
アンチウイルス機能
CTD機能(検出)
CTD機能(防御)
ランサムウェア対策
機械学習型検索機能
Webレピュテーション
ファイアウォール
侵入防衛
概要説明
仮想パッチとは
推奨設定について
変更監視
概要説明
その他機能について
セキュリティログ監視
アプリケーションコントロール

脆弱性が発覚してから正規パッチがリリースされるまでの間、**仮想パッチ**により、本脆弱性を衝く**ゼロデイ攻撃**のリスクを軽減することが可能です。

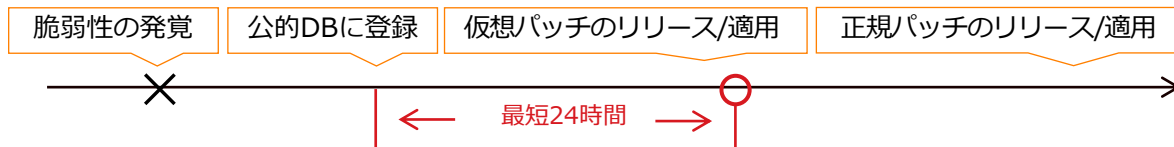
通常、脆弱性が発覚してから正規パッチがリリースされるまでに数週間かかり、その間は本脆弱性をつく攻撃に対して無防備になります。トレンドマイクロでは、脆弱性発見から**最短24時間※**でこのような攻撃に対する対処を仮想パッチという形で提供します。

※対応期間はスコアリングの結果(脆弱性の重要度等)によって異なります

従来の流れ



仮想パッチを用いた流れ

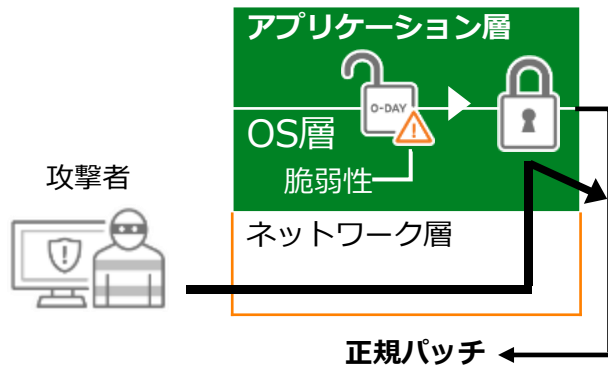


不正プログラム対策
アンチウイルス機能
CTD機能(検出)
CTD機能(防御)
ランサムウェア対策
機械学習型検索機能
Webレピュテーション
ファイアウォール
侵入防御
概要説明
仮想パッチとは
推奨設定について
変更監視
概要説明
その他機能について
セキュリティログ監視
アプリケーションコントロール

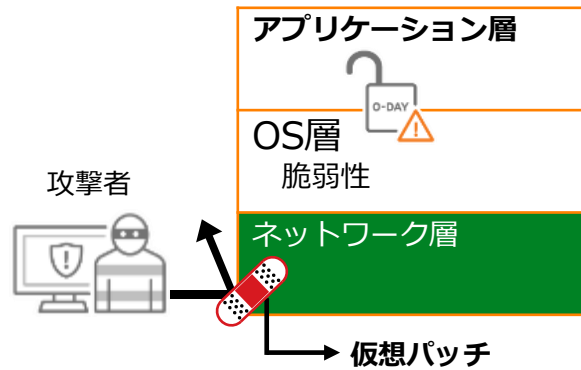
仮想パッチとは、**脆弱性**そのものを修正する正規パッチとは異なり、脆弱性を突く攻撃をネットワークレイヤで検知およびブロックするものです。

OSやアプリケーションの脆弱性を衝いた攻撃コードをネットワーク上を流れるパケットレベルで照合し、**ルールにマッチする攻撃パケットをブロックする技術**です。
正規パッチとは異なりソフトウェアのコードレベルでの修正は行わないので、**動作中のシステムへの影響が少ない**特徴があります。

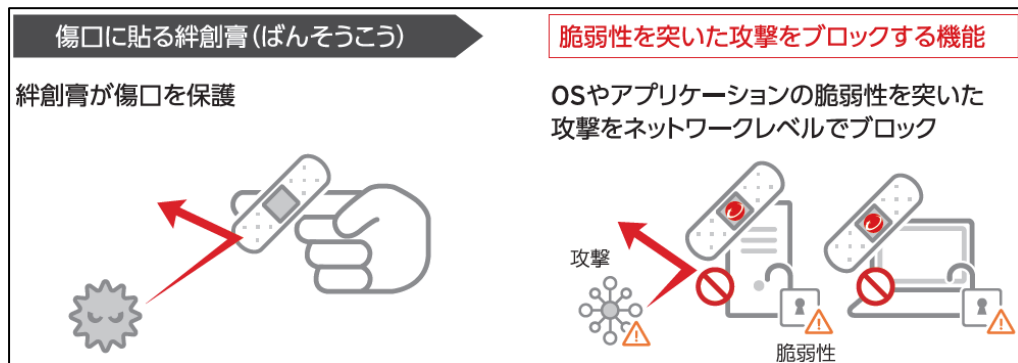
正規パッチによる防御



仮想パッチによる防御



- 仮想パッチとは
 - 脆弱性を狙う攻撃コードを、IPS/IDSルールでブロック
 - 脆弱性に対して**仮想的に**パッチが当たっている状態にすること



イメージは絆創膏

「絆創膏」

- × 傷を治す
- 外部から細菌の侵入を防ぐ

「仮想パッチ」

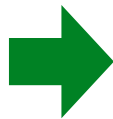
- × 脆弱性を直す
- 脆弱性に対する攻撃を防ぐ

仮想パッチ適用に伴う検証が不要なため、迅速に脆弱性を保護

近年の重大な脆弱性に対する仮想パッチの対応

脆弱性 攻撃コード公開

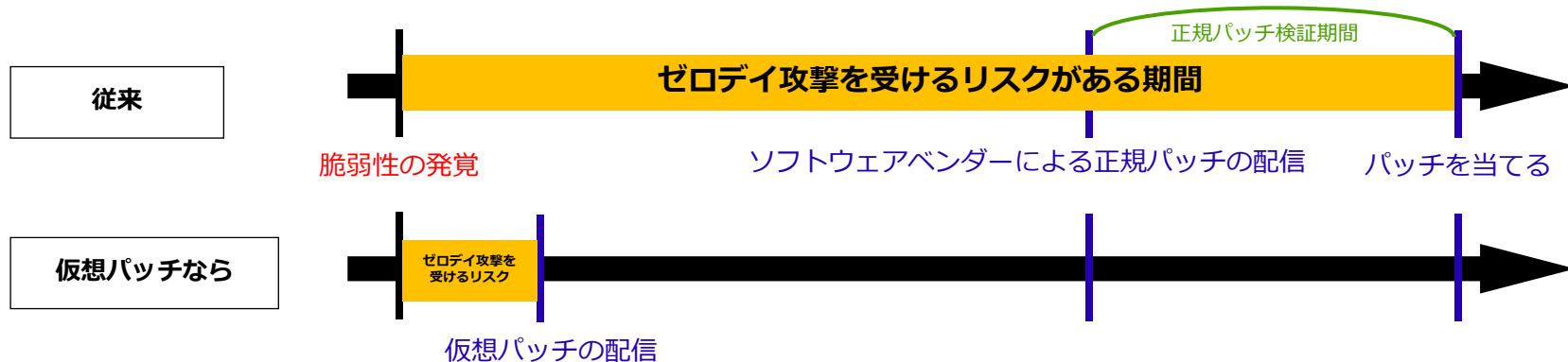
WordPress 2月3日公開
Apache Struts2 3月8日公開



仮想パッチ（IPSルール）の配信

対応IPSルール 2月3日配信
対応IPSルール 3月8日配信

仮想パッチは多くの場合、正規パッチよりも早く配信されます。



ゼロデイ攻撃とは：脆弱性の発見後から正規パッチが配布されるまでの間に脆弱性を狙った攻撃をすること

「ゼロデイ攻撃を受けるリスクがある期間」を最小限に。



対象サーバに「どの仮想パッチが必要か/不要か」を自動で判断し、適用と取り外しを行うことができます。（推奨設定の検索）

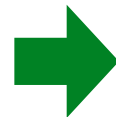
エージェントのインストールされている対象サーバに推奨設定の検索をかけることで、下記処理を自動で実行することができます。

1. 内在する脆弱性を検知し、対応する仮想パッチを適用する
2. 正規パッチの適用後、不要な仮想パッチを検知し、取り外す

推奨検索の実行



- アプリケーション情報
- 環境変数
- ファイル情報
- 空いているポート
- 実行されているプロセス
- レジストリ(Windowsのみ)
- サービス(Windowsのみ)



パッチの適用/取り外し



正規パッチがリリースされるまでの保護を自動化できるため、システム管理者の方は、**正規パッチの適用作業スケジュール**を計画的に行うことができます。

侵入防御：仮想パッチの推奨検索について

～CVEベースの脆弱性対応が可能～

コンピュータ: SN-SV071WIN2016

概要 一般 詳細 侵入防御イベント

侵入防御

設定: オン

ステータス: オン, 防御, ルールなし

侵入防御の動作

● 防御

○ 検出

コンテナの保護

コンテナのネットワークトラフィックの検索:

現在許可されている侵入防御ルール

すべて

許可/拒否/許可/拒否解除... 一括適用... エクスポート... アプリケーションの種類... 印刷

名前 説明

推奨設定

現在のステータス:

前回の推奨設定の検索:

未解決の推奨設定:

侵入防御の推奨設定を自動的に適用 (可能な場合): 初期設定 (いいえ)

推奨設定の検索 推奨設定の検索のキャンセル 推奨設定をクリア

適用されれば
ここに適用済み仮想パッチの一覧が出ます

推奨検索結果の
自動適用可否: はい・いいえ

推奨検索開始ボタン
* タスク実行も可能

推奨検索結果 = リスクがあるためあてたほうがいい仮想パッチの一覧

前回の推奨設定の検索以降にDeep Securityルールアップデートが実行されました。現在の推奨設定は古い可能性があります。最新の検索については、新しい推奨設定の検索を実行してください。

侵入防御ルール: すべて 許可/拒否/許可/拒否解除... アプリケーションの種類...

推奨のマーク

優先度・重要度

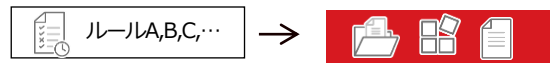
名前	CVE	前回のアップデート	優先度	重要度	モード	種類	カテゴリ	TIPPINGPOINT	MICROSOFT
✓ DCERPC Services (2)	CVE番号								
1010900 - Microsoft Windows SMB Information Disclosure Vulnerability (CVE-2021-28325)	CVE-2021-28325	2021-06-16	2 - 標準	● 重大	検出のみ	スマート	脆弱性と攻撃コード	なし	MSCVE-2021-28325
1007596 - Identified Possible Ransomware File Extension Rename Activity (T)	なし	2021-02-23	2 - 標準	● 重大	検出のみ	スマート	不審なネットワークアクティ	なし	なし
1007913 - Identified Possible Ransomware File Extension Rename Activity (T)	なし	2020-12-09	2 - 標準	● 重大	検出のみ	スマート	不審なネットワークアクティ	なし	なし
1009717 - Microsoft Windows PowerShell EXE Filename Parsing Remote Code (M)	なし	2019-05-08	2 - 標準	● 重大	防御	脆弱性	脆弱性と攻撃コード	なし	なし
1011079 - Microsoft Windows Services NFS ONCRPC XDR Driver Remote Code (M)	CVE-2021-26432	2021-08-18	2 - 標準	● 重大	防御	攻撃コード	脆弱性と攻撃コード	なし	MSCVE-2021-26432
1006740 - Identified SSL/TLS Diffie-Hellman Key Exchange Using Weak Para...	CVE-2015-4000...	2021-08-11	2 - 標準	● 中	検出のみ	スマート	脆弱性と攻撃コード	16986, 16987	MS15-055
1006591 - Identified Usage Of TLS/SSL_EXPORT Cipher Suite In Response (Ex)	CVE-2015-4000...	2021-08-04	2 - 標準	● 中	防御	スマート	脆弱性と攻撃コード	16986, 16959	MS15-031
✓ Web Client Common (10)	←アプリケーション種別								
1011126 - Microsoft MDHTML Remote Code Execution Vulnerability (CVE-2...	CVE-2021-40444	2021-09-29	2 - 標準	● 重大	防御	脆弱性	脆弱性と攻撃コード	なし	なし
1011005 - Microsoft Windows MDHTML Platform Remote Code Execution Vul...	CVE-2021-33742	2021-08-04	2 - 標準	● 重大	防御	攻撃コード	脆弱性と攻撃コード	なし	MSCVE-2021-33742
1010700 - Microsoft Windows Defender Remote Code Execution Vulnerabilit...	CVE-2021-1647	2021-01-13	2 - 標準	● 重大	防御	攻撃コード	脆弱性と攻撃コード	なし	MSCVE-2021-1647
1004715 - HTTP Web Client Decoding	なし	2020-08-12	1 - 低	● 重大	防御	スマート	脆弱性と攻撃コード	なし	なし
1009489 - Microsoft Windows Vot And Contact File Insufficient UI Warning R...	なし	2019-06-26	2 - 標準	● 重大	防御	攻撃コード	脆弱性と攻撃コード	なし	なし
1009714 - Microsoft Windows PowerShell EXE Filename Parsing Remote Code (M)	なし	2019-05-08	2 - 標準	● 重大	防御	脆弱性	脆弱性と攻撃コード	なし	なし

不正プログラム対策
アンチウイルス機能
CTD機能(検出)
CTD機能(防御)
ランサムウェア対策
機械学習型検索機能
Webレピュテーション
ファイアウォール
侵入防御
概要説明
仮想パッチとは
推奨設定について
変更監視
概要説明
その他機能について
セキュリティログ監視
アプリケーションコントロール

ファイルやディレクトリ、レジストリ等を監視し、
不正な変更が加わった場合にいち早く検知します。

「どこ(監視対象)の何(監視属性)を監視するか」が定義されているルールを選択し、それに基づいて、ベースラインと呼ばれるその時点での監視対象のリストを作成します。
ベースラインから変更がかった場合にそれを検知し、管理者はログから詳細を確認することが可能です。

ベースラインの作成



[監視対象]

- ファイル/ディレクトリ
- レジストリ(キー/値)¹
- サービス/プロセス
- ソフトウェア
- Listenポート
- ユーザ/グループ

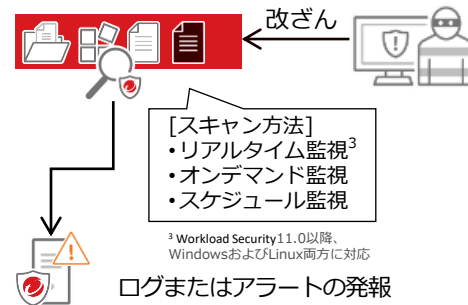
[監視属性]

- 作成/更新日時
- 所有者/グループ/権限
- サイズ/Hash
- Flags¹
- シンボリックリンク²
- i-node/デバイスナンバー²

¹ Windowsのみ対応 ² Linux/Unixのみ対応



変更の検出



³ Workload Security 11.0以降、
WindowsおよびLinux両方に対応

不正プログラム対策
アンチウイルス機能
CTD機能(検出)
CTD機能(防御)
ランサムウェア対策
機械学習型検索機能
Webレピュテーション
ファイアウォール
侵入防御
概要説明
仮想パッチとは
推奨設定について
変更監視
概要説明
その他機能について
セキュリティログ監視
アプリケーションコントロール

対象サーバに適切なルールを自動で割り当てる推奨設定の検索、また、スキャン中のパフォーマンス低下を防止する機能があります。

推奨設定の検索を使用することで、**対象サーバに適切な監視ルールを自動で検出/割り当てる**ことが可能です。
※ルールの種類によっては、別途設定が必要な場合があります。



ベースラインからの変更のスキャン中、パフォーマンスに影響を出したくない場合、**スキャンによるCPU負荷の設定**することが可能です。

制限のタイプ (CPU負荷)	詳細
高	ウェイト処理を挟まない
中	定期的にウェイト処理を挟むことでCPU負荷を下げる
低	頻繁にウェイト処理を挟むことでCPU負荷を下げる



OSやアプリケーションからの膨大なログエントリに埋もれて見逃しがちな**重大なセキュリティインシデント**を効率的に発見することが可能です。

特定ログのエントリを監視するルールを作成します。ルールに合致したログエントリを発見した場合に、どの重要度のアラートを上げるかを設定することができます。

また、サーバ別に適したルールを、推奨検索により自動で適用することも可能です。

※各ルールのパラメータ設定が別途必要な場合もあります。

監視ルールの作成

ルールA,B,C,...

「どのログファイル」に
「どのメッセージ」が含まれていると
「どの重要度²」でアラートを上げる

¹対応ログの種類は下記の通り:

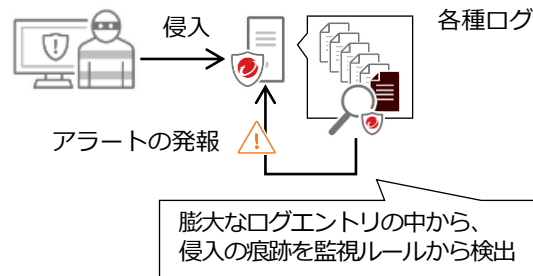
syslog, snort-full, snort-fast, apache, iis, squid,
nmapg, mysql_log, postgresql_log djb-multilog,
eventlog, single-line-text-log

²重要度設定は下記の通り:

低(0-3),中(4-7),高(8-11),重大(12-15)



ルールに合致したログエントリの検出





ソフトウェアを監視し、承認されていないソフトウェアを検知し、当該ソフトウェアの実行を許可/ブロックできます。

本機能¹を有効化した時点で、対象サーバ内に存在する実行ファイルを全て一覧化し、ホワイトリストとして登録します。ホワイトリストにない実行ファイルを検知した場合、管理者は当該ファイルの実行を許可するかブロックするか選択することができます。

¹本機能はWorkload Security10.1以降、LinuxおよびWindows両方に対応しています

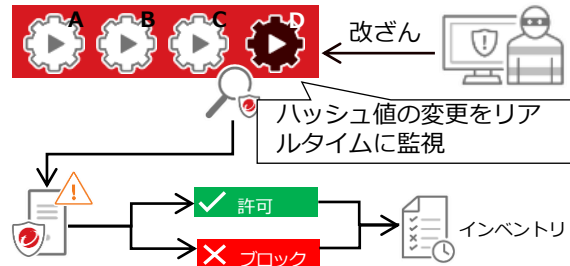
ホワイトリストの作成



[ホワイトリスト作成の条件]

- コンパイル済みのバイナリやライブラリ (.exe/.class/...)
- 実行権限または特定の拡張子を持つテキストファイル (.sh/.jar/.php/.py/...)

承認されていない実行ファイルの検出



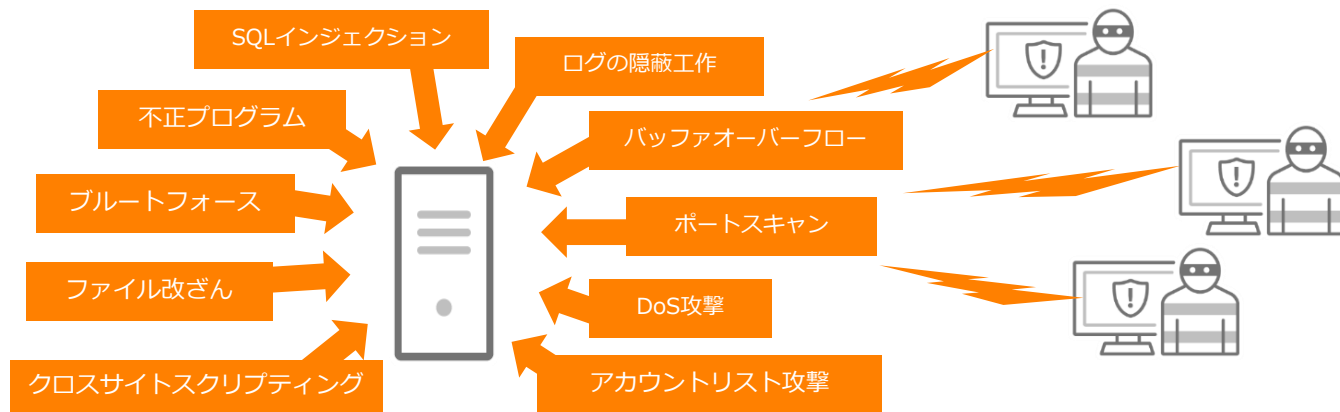
許可またはブロックされた実行ファイルはインベントリに追加され、同ファイルを再度検知した際に参照されます。

*Windows Updateによるノイズが10.2以降では軽減される

*変更監視機能が利用可能なライセンスを保有していれば、本機能用に追加購入の必要はありません

*管理マネージャー12.0以上+エージェント11.0以上、あるいは管理マネージャー11.1以上+Workload Security11.1以上の場合にはハッシュ値のみが監視対象になります。

- サーバへの攻撃はますます巧妙化しています。
- 近年相次ぐサーバへの攻撃は、**様々な攻撃手法を複数組み合わせ**て実行されることが多いのが特徴です。



従来の不正プログラム対策にプラスした多段での対策が必要

複数機能でサーバの多層防御を実現

予

従来型は予防的な対策が中心

- ・パッチの適用
- ・パスワードポリシーの強化 など

ゼロデイ・攻撃早期化・運用不備・リスト型

完璧な予防は困難

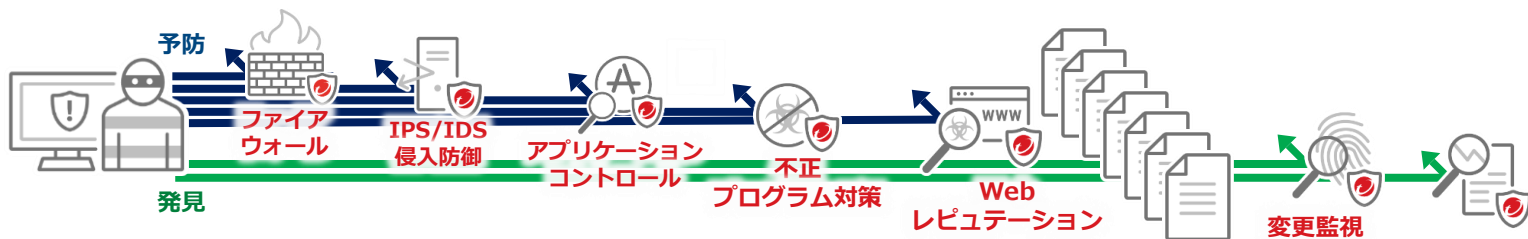
発

今後は発見的な対策を強化

- ・不正侵入、改ざんの検知
- ・大量の認証試行の検知 など

攻撃に「気づく」

被害を最小限に留める



予防はもちろんのこと、万が一侵入された場合も、
早期発見で被害を最小限に留めます。

サーバの管理機能

- Workload Securityの管理を行う際は、Webブラウザを経由してWeb管理コンソールに接続します。

管理用のソフトウェアをインストールする必要はありません。

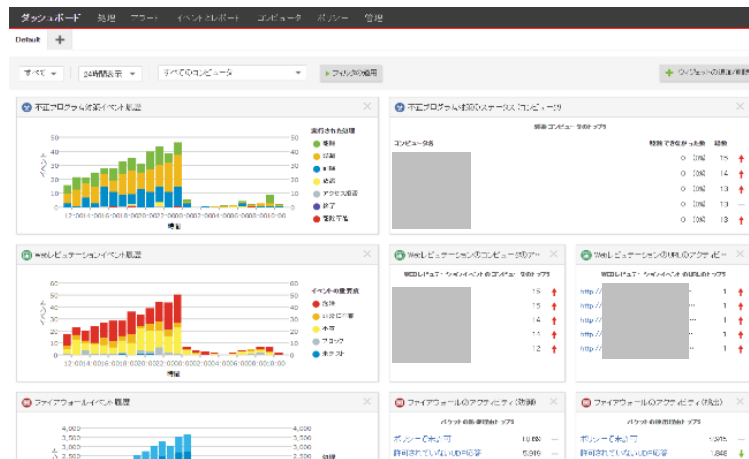
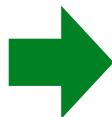
ログオン

ユーザー名

パスワード

☐ 多要素認証を使用する

ログオン



- ・ ユーザ名・パスワードはManagerインストール時に設定したものを入力ください。
- ・ デフォルトのポート番号は4119（可変）です。

管理コンソールのメニューについて

【ダッシュボード】
コンピュータの管理状況、セキュリティ検知状況などをグラフ形式で表示します。

【処理】
アプリケーションコントロールの検知結果の表示と、それに対するアクション（許可・ブロックリストへの追加）が可能です。

【アラート】
アラート通知の一覧とその詳細を確認することが可能です。

【ヘルプセンター】
オンラインWebヘルプ情報を検索することが可能です。



【管理】
マネージャーに関するシステム設定、コンポーネントのアップデートなどが可能です。

【イベントとレポート】
各コンピュータで検知されたセキュリティログや、システムログを確認できます。

【コンピュータ】
管理対象のサーバを確認することができます。また、Agentの追加/削除、ステータスの確認、ポリシーの付け替えなどの操作が可能です。

【ポリシー】
Agentの処理動作を決めるセキュリティポリシーの作成・編集が可能です。

Agentサーバの管理について (1/3)

- Agentサーバの追加・削除、その他の管理については「コンピュータ」メニューから行います。

The screenshot displays the MasterAdmin web interface. The top navigation bar includes 'ダッシュボード', '処理', 'アラート', 'イベントとレポート', 'コンピュータ', 'ポリシー', and '管理'. The 'コンピュータ' menu is active, showing a list of computers. On the left, the 'スマートフォルダ' (Smart Folders) tree is expanded, showing 'All Factory', 'OKINAWA', 'DC', '工場', 'OSAKA', and '工場'. In the center, the '追加' (Add) dropdown menu is open, showing options like 'コンピュータの追加...', 'Active Directoryの追加...', 'VMware vCenterの追加...', 'AWSアカウントの追加...', 'Azureアカウントの追加...', and 'vCloudアカウントの追加...'. On the right, the 'インストールスクリプト' (Install Scripts) dropdown menu is open, showing 'サポート情報', '新機能', and 'バージョン情報'. Three callout boxes provide additional information: 1. '【インストールスクリプト】 Agentのインストール用のスクリプトを作成することができます。' (Install Scripts: You can create scripts for installing the Agent.) 2. '【クラウドコネクタ】 各種パブリッククラウド上、VMware vCenter上で管理されるマシン情報を同期できます。' (Cloud Connectors: You can synchronize machine information managed on various public clouds and VMware vCenter.) 3. '【スマートフォルダ】 登録されているコンピュータを動的にグループ化できます。' (Smart Folders: You can dynamically group registered computers.)

MasterAdmin | ヘルプ | サポート情報 | ヘルプセンターの検索

ダッシュボード 処理 アラート イベントとレポート コンピュータ ポリシー 管理

インストールスクリプト

サポート情報
新機能
バージョン情報

【インストールスクリプト】
Agentのインストール用のスクリプト
を作成することができます。

【クラウドコネクタ】
各種パブリッククラウド上、
VMware vCenter上で管理されるマシン情報を
同期できます。

【スマートフォルダ】
登録されているコンピュータを動的に
グループ化できます。

コンピュータ サブグループを含む グループ別

追加 削除... 詳細... 処理 イベント

コンピュータの追加...
Active Directoryの追加...
VMware vCenterの追加...
AWSアカウントの追加...
Azureアカウントの追加...
vCloudアカウントの追加...

プラットフォーム ポリシー ステータス

操作	プラットフォーム	ポリシー	ステータス	メンテナンス...	ポリシーの選...
スマートフォルダの作成...	Microsoft Windows...	なし	● 管理対象 (オンライン)	なし	なし
グループの作成...	Microsoft Windows...	なし	● 管理対象 (オンライン)	なし	なし
			● 管理対象 (オンライン)	なし	なし
			● 管理対象 (オンライン)	なし	なし
			● 管理対象 (オンライン)	なし	なし
			● 管理対象 (オンライン)	なし	なし

アラート 0 0

○ Agentのインストールについて

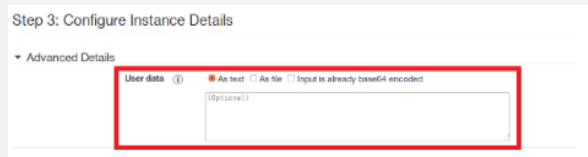
対象のサーバにAgentをインストールする事で、各種保護を提供します。

Agentのインストールは、2つの方法が用意されています。

- OSに対応したエージェントインストーラを利用
- インストールスクリプトを利用

インストールスクリプトを利用することで、クラウドサービスを利用したAuto Scaling時、インストール～有効化までを自動化させることができます。

<AWS上で設定する時の例>



Auto-Scaling対象のインスタンスのAMIイメージにインストールスクリプトを貼り付けることで、新規インスタンス起動時に自動的にスクリプトが走ります。

<インストールスクリプトについて>

インストール用のスクリプトを自動生成させることで、インストーラを利用することなく、Agentをインストールさせることが可能になります。



「サポート情報」から
インストールスクリプト
を選択します

※9.6以前は「ヘルプ」
→「インストールスクリプト」



Agentサーバの管理について (3/3)

○ スマートフォルダ

- 「スマートフォルダ」は登録されているコンピュータを動的にグループ化する機能
- スマートフォルダにアクセスしたタイミングで最新の情報を取得し、コンピュータの一覧から検索クエリの条件に沿ったコンピュータのみを表示

<スマートフォルダの利便性>

スマートフォルダ内の対象コンピュータに処理が行えます。

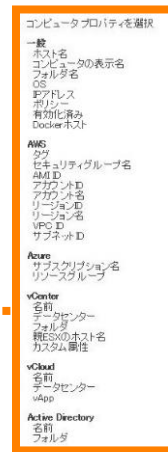
予約タスクでも、スマートフォルダを指定することが出来ます。

<スマートフォルダの作成方法>

各スマートフォルダごとに検索クエリを設定します。
AND/ORの条件を用いて条件を複合的に設定することができます。

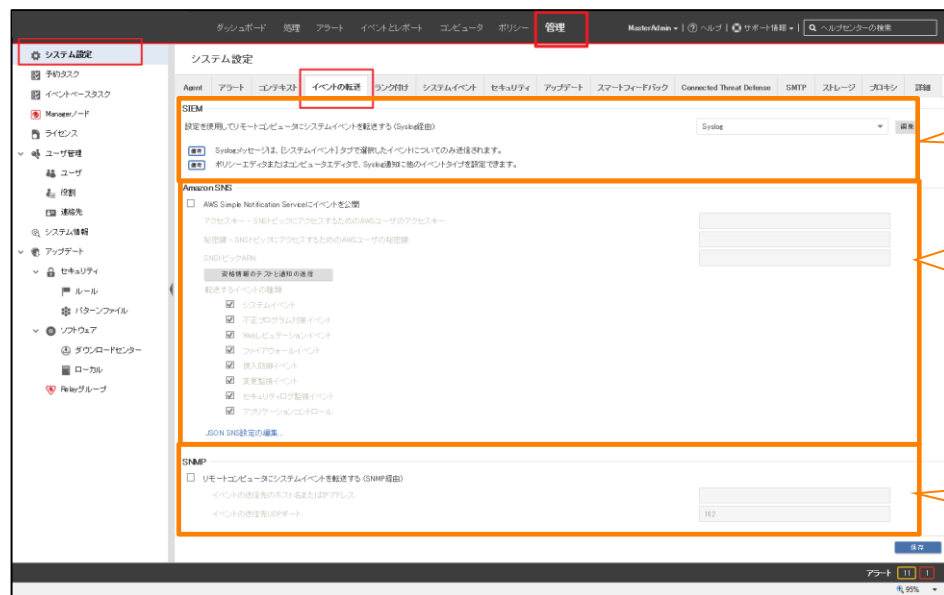


※サブフォルダは各スマートフォルダにつき10個まで作成可能
※正規表現は利用することができません。



イベント転送について (1/2)

- 管理マネージャーはSyslogのSIEM連携機能、Amazon SNS連携機能、またSNMPのイベント転送機能を提供しています。



【SyslogのSIEM連携】

- Syslog経由でリモートコンピュータにシステムイベントの転送は可能
- ※セキュリティイベントの転送方法は次頁に記載。

【Amazon SNSとの連携】

- Amazon SNSにイベント公開可能
 - 転送するイベントの種類を選択可能
 - JSON SNS設定の詳細編集にて通知先のカスタマイズが可能
- 例) セキュリティポリシーやサーバ役割ごとに送信先をカスタマイズ可能。

【SNMP転送】

- SNMP経由でリモートコンピュータにシステムイベントのみ転送は可能。

イベント転送について (2/2)

○ 管理マネージャーは、AgentコンピュータからSyslogサーバまたはSIEMサーバへのセキュリティイベント転送を設定できます。

The screenshot displays the 'Policy' (ポリシー) management interface. On the left sidebar, the 'Policy' (ポリシー) menu is highlighted. Under the 'List' (リスト) section, 'Linux Server' is selected. A callout box with an arrow points to 'Linux Server' with the text 'ポリシーをダブルクリック' (Double-click the policy). The main content area shows the configuration for 'Base Policy > Linux Server'. A callout box with an arrow points to the '設定' (Settings) tab, with the text '特定のポリシーやコンピュータ、特定のイベント種類に対してSyslog/SIEMサーバの設定は可能' (It is possible to set Syslog/SIEM server for specific policies or computers, and for specific event types). The 'Settings' tab shows various configuration options, including 'Event Forwarding Frequency (Agent/Appliance)' set to 'Interval (60 seconds)', and 'Event Forwarding Settings (Agent/Appliance)' where 'Syslog 2' is selected for 'Syslog destination'.

- 管理マネージャーより、アラートのメールを送信できます。

The screenshot displays the 'Management' (管理) section of the Fujitsu Management Manager. The left sidebar contains a 'System Settings' (システム設定) menu item, which is highlighted with a red box. Below it, the 'User Management' (ユーザ管理) menu item is highlighted with an orange box. The main content area shows the 'System Settings' (システム設定) page, with the 'Alerts' (アラート) tab selected and highlighted with a red box. Within the 'Alerts' section, the 'Alert Settings' (アラートの設定) link is highlighted with an orange box. A blue callout box points to this link, stating: 'アラート重要度、送信タイミングなど条件の詳細設定が可能' (Detailed settings for alert importance, sending timing, etc. are possible). Another blue callout box points to the 'Alert Email Address' field, stating: 'メール通知の送信先設定可能' (Email notification destination setting is possible). The 'Alert Email Address' field contains 'admin@example.com'. At the bottom, an orange box contains the text: '宛先を追加する場合には、ユーザを追加し、連絡先情報で設定が可能です。' (When adding a destination, you can add a user and set it in the contact information).

- ご利用になられる前に、 Workload Security体験版をご利用いただくことをおすすめいたします。
- Workload Securityで提供しているエージェントのシステム要件は、こちらを参照してください。
 - <https://www.go-tm.jp/tmdsaas/req>
- エージェントをインストールするサーバから、 Workload Security管理マネージャにアクセスできることをご確認ください。
 - (参考)サポートページ： <https://success.trendmicro.com/jp/product-support/cloud-one-workload-security>
 - プロキシサーバを経由する場合など、設定の詳細についてはWorkload Securityのオンラインヘルプをご参照ください。

- プロキシサーバを経由する際の認証は、Basic認証のみ利用できます。Digest認証とNTLM認証はサポートしていません。
- エージェント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NW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
- Workload SecurityのUIの一部、通知メールなどが英語で表記されております、ご了承ください。
- Workload Securityで提供される機能の一部は日本ではサポートされないものが含まれております。ご了承ください。
- Workload Securityアカウントを作成すると、エージェントがインストールされたデモ用の仮想サーバ（AWSインスタンス）が提供されます。
 - これは30日間利用が可能なデモ用インスタンスです。
 - デモ用仮想サーバのエージェントも、1ユニットとしてカウントされるため、ご利用前にデモ用仮想サーバを削除して利用開始してください。

■ サーバー向けクラウド型セキュリティ（Trend Micro Cloud One – Workload Security）

ニフクラ上のサーバーを、トレンドマイクロ社がクラウド上で提供する管理サーバーから集中管理することにより、管理サーバー構築の工数を削減し、迅速に安全性の高いシステムを構築・運用することが可能になります。 ※Trend Micro Cloud One – Workload Security（以下 Workload Security）

■ 特長

【管理サーバー構築不要】

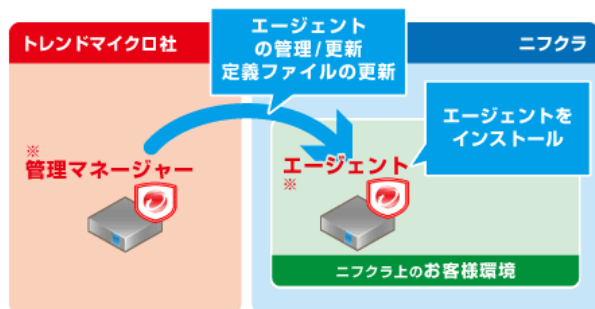
トレンドマイクロ社がクラウド上で提供する管理サーバーから集中管理するため、管理サーバー構築の必要がなく、迅速に手軽に利用開始することができます。

【サーバー増減の考慮が不要】

従来のセキュリティ対策では、サーバーが増えた場合、管理者が都度手動で設定する必要がありました。サーバー向けクラウド型セキュリティ（Workload Security）は、インストールスクリプトを利用することで、サーバーが増えた場合にも、自動的にセキュリティエージェントをインストールし、自動で適切なセキュリティ設定を行うことができます。

【複数のセキュリティ機能を統合】

サーバーセキュリティに必要な複数の機能を実装しているため、セキュリティコストの最適化と複数のセキュリティ機能の統合運用が可能になります。



- ・管理マネージャーの提供
- ・クラウド上のサーバに対しての定義ファイル更新など
- ・月額ライセンス提供
- ・24時間/365日のサポート一次受け
- ・ニフクラとあわせての一括請求

■ 仕様

ウイルス対策 (Webレビュテーション機能付)	サーバーにウイルスが感染することを防止します。 ウイルスがサーバに侵入しようとした時に検出する「リアルタイム検索」や、毎週/毎日など事前に設定した時間に検索を行う「スケジュール検索」によりサーバーをウイルス感染から保護します。
Webアプリケーション保護	SQLインジェクション、クロスサイトスクリプティング（XSS）などからシステムを守ります。
侵入検知・防止 (ホスト型IDS/IPS)	仮想パッチ（脆弱性ルール）によって、脆弱性を突いた攻撃からサーバーを保護します。 対応している脆弱性は、Windows・Linux・Solarisなど、主要なサーバーOSや、Apache・BIND・Microsoft SQL・Oracleなど100以上のアプリケーションに対応しています。
ファイアウォール	ホストベースでのネットワークアイソレーションを実現します。 IPアドレス・MACアドレス・ポートのフィルタリングをサーバーごとに細かく設定できます。ネットワークごとのポリシー作成も可能です。 あらかじめ用意された共通テンプレート（Webサーバー用、DNSサーバー用など）を利用してスピーディに設定することができるので、攻撃を受ける機会を軽減します。
ファイルやレジストリなどの変更監視	あらかじめ指定したファイルやレジストリ、ファイル権限、ポートなどを監視し、変更があった場合に管理者に通知する機能です。 例えば、ファイルのサイズを監視することで、不正な侵入者がアクセスログを隠蔽するためにログの一部を削除するなどの行為を行った際に、すぐに管理者にアラートを上げます。
セキュリティログ監視	Windowsのイベントログやアプリケーションのログを監視し、あらかじめ定められた閾値を超えた場合に管理者にアラートを上げることができます。 例えば、Windowsイベントログに短い間に複数のログイン失敗のイベントが上がった場合などに、管理者に直ちに知らせることができます。

■ サーバー向けクラウド型セキュリティ（Trend Micro Cloud One – Workload Security）

■ 料金

	月額（税込）
サーバー向けクラウド型セキュリティ （Workload Security）ライセンス	22,000円/台/月

- ※サーバー1台に対して、1ライセンス必要です。必要なライセンス数をお申し込みフォームに記載してください。
- ※ライセンスコード発行の連絡をもちまして、ご利用開始とさせていただきます。
- ※お申し込み後、ご利用開始まで5営業日程度かかります。余裕をもってお申込みください。
- ※利用開始月は、月額料金を無料でご利用いただけます。
- ※利用開始翌月1日からの1カ月間を最低利用期間とします。最低利用期間経過前に解除する場合は、1カ月分の利用料金を請求いたします。
- ※プラン、ライセンスなどご利用内容変更時の新料金は、変更翌月より反映されます。サーバーご利用解除時は、解除月分までの利用について料金が請求されます。
- ※サービスの設定変更・解除について、20日までに申請した場合、申請月当月に設定変更・解除されます。
- ※21日以降月未までに申請した場合、申請月翌月に設定変更・解除されます。
- ※二フクラを解約する場合、解約前までに本サービスの契約を解除いただく必要がございます。
- ※利用開始月・解除月の日割り計算による割り引きはいたしません。
- ※ライセンスの追加・削除は、下記フォームからの申請が必要です。
- サーバー向けクラウド型セキュリティ（Trend Micro Cloud One – Workload Security）各種申請フォーム：
https://inquiry.nifcloud.com/webeg/pub/cloud/dsaas_auth

■ 注意事項

- 本サービスは、二フクラ内での利用に限定されます。
- エージェントのシステム要件は、トレンドマイクロ社のページをご覧ください。
- WEBページを参考に、エージェントをインストールしたサーバーから、管理マネージャーにアクセスできることをご確認ください。
- ※2020/11/23 09:00のタイミングで、その時間以降に作成したアカウントでの仕様に変更がございます。詳細はトレンドマイクロ社の案内をご参照ください。
- プロキシサーバーを経由する場合などの設定については、トレンドマイクロ社のオンラインヘルプをご覧ください。
- 当月中にサービス解除を行う場合は、20日までにご申請ください。21日以降の申請の場合は、翌月分の月額料金が発生します。
- 本サービスは、定期メンテナンスを実施いたします。メンテナンスの実施タイミングやメンテナンス内容の詳細につきましては、トレンドマイクロ社のページをご確認ください。
- 非活性メンテナンスを実施する場合はFJCTから事前にご連絡をいたしますが、終了時のご連絡は実施いたしませんのであらかじめご了承ください。

※本サービスは、2020年6月1日に名称変更しました。
（旧名称：Trend Micro Deep Security as a Service）。
提供機能に変更はございません。詳しくは以下をご確認ください。
<https://success.trendmicro.com/jp/solution/000247822>

■ 制限事項

- エージェントをインストールするサーバーの環境によって、再起動が求められる場合がございます。
- サーバー向けクラウド型セキュリティ（Workload Security）の一部通知メールなど、英語で表記されております。また、提供される機能の一部には日本ではご利用いただけないものが含まれております。あらかじめご了承ください。
- 当社で提供中のサーバー向けクラウド型セキュリティ（Workload Security）では、XDR機能はご利用いただけません。あらかじめご了承くださいませよう、お願い申し上げます。

■ ご利用方法



- 1.お申し込み**
本サービスのお申し込み、設定変更、解除については、下記フォームよりお申し込みください。
※二フクラIDとパスワードの入力が必要です。
※お申し込み時にログインされた二フクラIDでのご登録となります。
■お申込みフォーム：https://inquiry.nifcloud.com/webeg/pub/cloud/dsaas_auth
- 2.サーバー作成**
お申し込み後、お客様にて二フクラのコントロールパネルより、サーバー作成を行ってください。
- 3.ライセンス発行**
当社より、お申し込み時にご入力いただいたご担当者メールアドレスに、ライセンスが記載されたファイルを送付いたします。ライセンス送付後、メールで送付いたします「サービス設定完了のお知らせ」内に、導入手順書などマニュアルのURLを記載しておりますのでダウンロードしてご利用ください。
- 4.エージェントインストール**
管理マネージャーへアクセスし、「インストールガイド」を参考に作成したサーバーにエージェントをインストールしてください。
- 5.ご利用開始**
管理マネージャーへアクセスし、管理マネージャーの管理機能をご利用いただけます。

■ お問い合わせについて

※障害やトラブル時のお問い合わせは、二フクラでも24時間365日承っておりますが、対応時間は下記提供企業窓口に準じることとなりますので、あらかじめご了承ください。

提供企業：トレンドマイクロ株式会社



導入事例

高いスケーラビリティを確保しつつ利便性と安全性のバランスを確保

○ Trend Micro Deep Security™ as a Service 導入事例 / 株式会社富士通ラーニングメディア様



株式会社 富士通ラーニングメディア

業種：情報サービス

地域：東京都、日本

導入製品・ソリューション：

Trend Micro Deep Security™ as a Service
(DSaaS)

導入時期：2016年2月

TREND MICROは、トレンドマイクロ株式会社の登録商標です。
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。
記載内容は2016年2月現在のものです。内容は予告なく変更になる場合がございます。
製品・サービスの導入効果は、ご利用企業・組織の方の声に基づくものであり、
お客様のご利用状況により効果は異なります。
Copyright ©2019 Trend Micro Incorporated. All rights reserved.

お客様の課題

- クラウド上にユーザ企業の個人情報や社外秘の情報を含む教育コンテンツなどを移行するには、万全のセキュリティ対策を取る必要があった
- さまざまな環境からアップロードされるファイルに、悪意のあるプログラムやマルウェアなどが紛れ込む可能性はゼロとは言い切れず、セキュリティリスクを感じていた

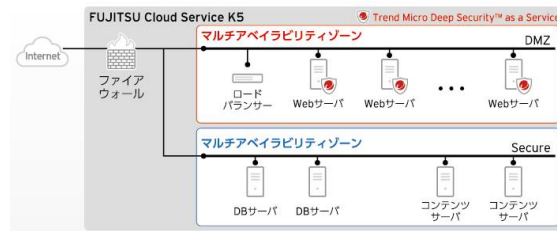
採用理由

- DSaaSは、必要な時に必要なだけ購入できるライセンス体系のため、一定期間だけ利用したり、頻繁に増減するサーバの台数にスケーラブルに対応できた
- 管理サーバ構築が不要で、スタートアップが早いので、クラウドサービスの利点を損なわないソリューションであり、リアルタイムスキャンも可能だった

導入効果

- セキュリティを懸念される顧客に対し、より具体的な対策として明示でき安心感を与えられるようになった
- スケーラビリティが高くサーバリソースの増減計画が容易になった
- 運用コストやスタッフの作業効率が上がった

〈利用環境イメージ〉



※本事例作成時は、Trend Micro Deep Security™ as a Service として導入、作成許可をいただいておりますため、このページでは旧名称を利用いたします。

※2020年6月1日に、DSaaSは名称変更しております。

機能比較

サーバのセキュリティ対策機能比較表

機能名	Workload Security	ウイルスバスターCorp	ServerProtect
ウイルス対策	○	○	△ ※ファイル検索のみ
ファイアウォール	○	○	×
IPS/IDS（侵入防御）	◎	○ ※クライアント向けルールのみ	×
Webレピュテーション	○	○	×
アプリケーションコントロール	○	-	×
変更監視（改ざん検知）	○	-	×
セキュリティログ監視	○	-	×
保護対象サーバ サポートOS	Windows Linux Solaris/HPUX/AIX	Windows	Windows Linux
管理マネージャ	1台で管理可能	1台で管理可能	Win/Lin環境により別々
仮想化対応	ホスト型+仮想アプライアンス型	ホスト型のみ	ホスト型のみ
クラウド対応	◎ 管理マネージャ連携可能	×	○

※ サーバの目的や求められるセキュリティレベルに応じて選択してください。

- 正式利用の前に、トライアル利用を行うことができます。
- 期間：1ヶ月間
- 正式利用の移行（設定引継）：可
- 制限事項
 - 利用可能数（5 OS）まで

■ トライアルのお申し込み

担当営業にご相談の上、以下Webフォームより申請ください

https://inquiry.nifcloud.com/webeq/pub/cloud/dsaas_auth

※申込を選択し、備考欄に担当営業名と調整済の旨をご記入ください。

○お気軽にご相談ください

契約／お申し込みに関する内容、サービス概要、導入にあたっての疑問点や、お見積りなどの依頼など、お電話又はサイトでのお問い合わせをお待ちしております。

ニフクラ導入相談窓口

サイト <https://pfs.nifcloud.com/inquiry/>

電話 0120-22-1200

受付時間：平日9:00～17:45
※携帯電話・PHSからのご利用可能

Thank you

