



Dr.Web Enterprise Security Suite (ESS) 説明資料

Doctor Web について



- 1992年 創業者 Igor Danilovが、Dr.WEBという名のアンチウイルスソフトを初めて開発
- 1999年 **世界初のふるまい検知**テクノロジーSplDer Nettingを開発
- 2003年 法人格「Doctor Web Ltd.」を設立

280人の従業員のうち、160人が開発および解析作業に従事。
全世界の個人ユーザから大手企業まで利用され、
世界的なアンチウイルスソフトウェアに成長。



インターネットに潜む害虫(マルウェア)から
Spiderweb(クモの巣)が守ります。



Doctor Web Pacific（日本法人）について

Doctor Web Pacificは、2010年12月に設立された「Doctor Web Ltd.」の子会社です。

Doctor Web Pacificは、アンチウイルス『Dr.WEB』の製品とサービスを約5,000を超える団体に販売。

警察機関、金融機関、サイバーセキュリティ会社と連携しながら国内のコンピュータ環境を保護しております。

マルウェアの検出・駆除能力および感染されたシステムを回復する能力を高く評価いただき、

日本国内においても5,000を超える団体で利用されております。

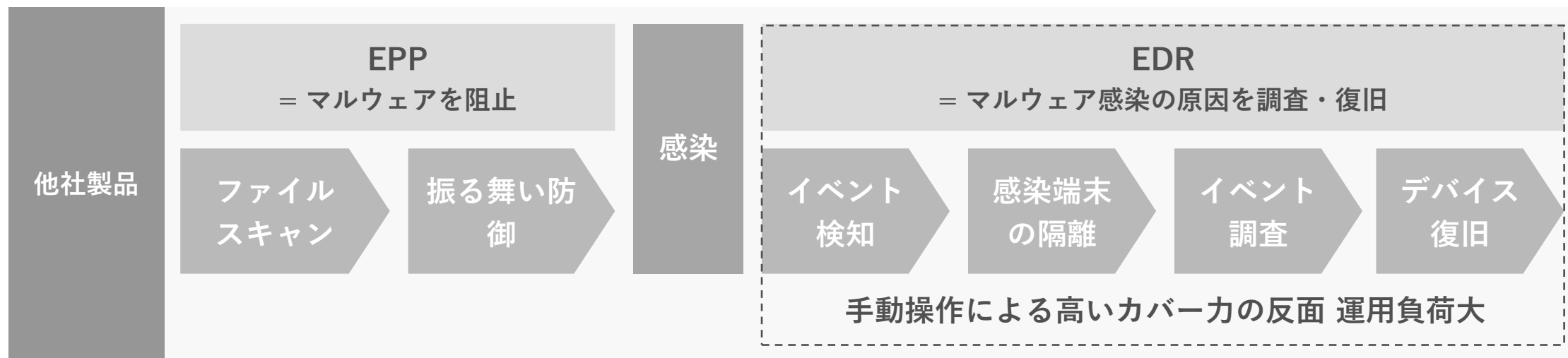
会社名	株式会社Doctor Web Pacific
英文表記	Doctor Web Pacific, Inc
所在地	東京都港区西新橋1-14-10西新橋スタービル 2F
代表者	森 周
TEL/FAX	03-6550-8770 / FAX : 03-6550-8771
業務開始日	2010/12/14
資本金	7300万円（Doctor Web, Ltd. 100%出資）



製品コンセプト



Dr.Webが考えるエンドポイントセキュリティ



Dr.Webひとつでエンドポイントセキュリティを全てカバー



Dr.Webの製品コンセプト

使いやすさを追求したシンプルなアンチウイルスソフト

Dr.Webで
安心

あらゆる潜んだ未知の
マルウェアを検知

Dr.Webで
快適

最適化された機能群。
使いやすさによる運用コストを低減

安全・快適に特化することで下記メリットを提供いたします。

point 1 ランサムウェアの検知力

point 2 PCのリソースの大幅な削減

信頼性の高いテクノロジーで
快適なセキュリティ運用を実現します

既知の脅威を検出

シグニチャー
データベース

1つのエントリで、亜種を含む数千個
のウイルスを検知

未知の脅威を検出

非シグニチャー型
テクノロジー

シグニチャーを使わずに高度な検知
を実行する様々な分析技術

未知の脅威を検出

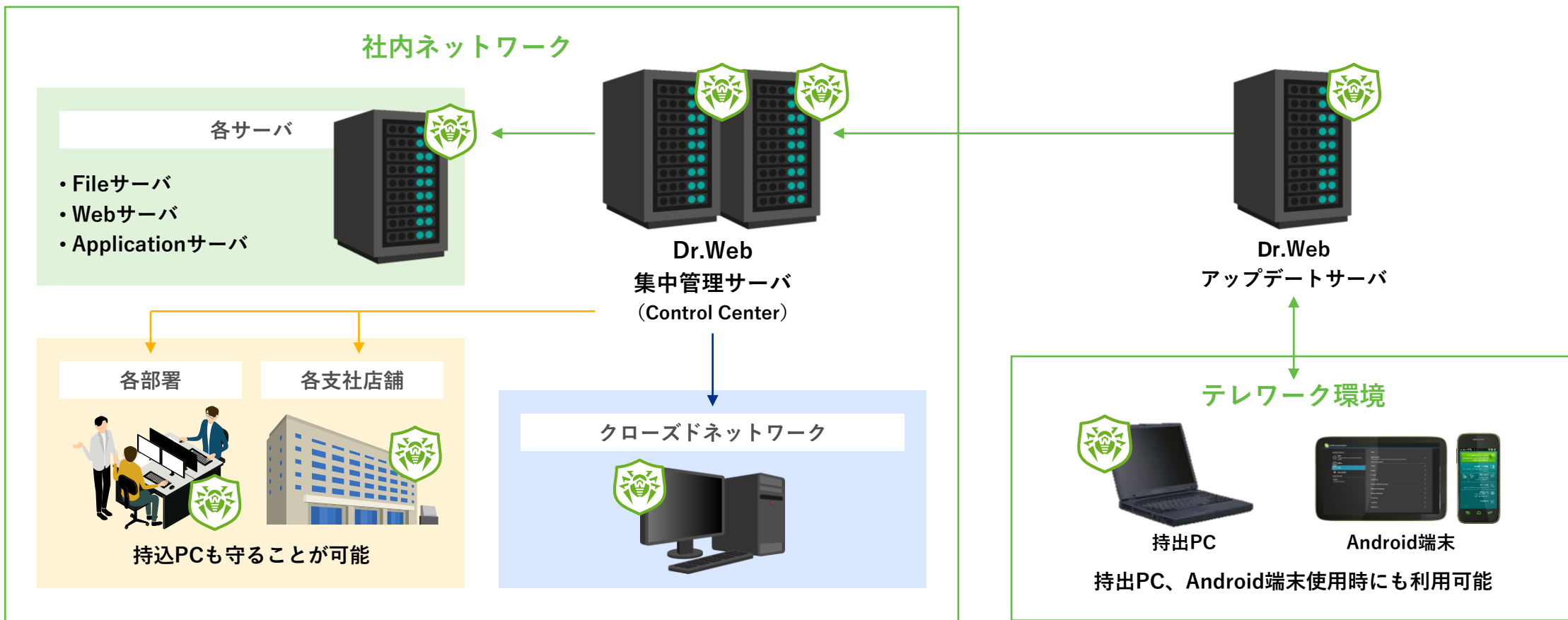
機械学習を応用した
マルウェア検出技術

未知の脅威を検出

予防的保護の
テクノロジー

Dr.Webの利用イメージ

様々なクライアント OS、サーバー OSに対応した製品でエンドポイントを守る





ESSが提供する 脅威からの保護機能と 運用管理機能



保護コンポーネント

DSS : Desktop Security Suite (クライアントOS向け製品)

SSS : Server Security Suite (サーバーOS向け製品)

コンポーネント	DSS	SSS	説明
SplDer Guard : リアルタイムスキャン	○	○	メモリに常駐し、プロセスとファイルの起動と作成に対して、悪意のあるアクティビティを検出します。
SplDer Guard for SMB : リアルタイムスキャン	-	○	Samba共有ディレクトリ内のファイルに適用されたアクションをモニタリングします。常駐モニターとして機能し、保護対象のファイルシステム内の基本的なアクション（作成、開く、閉じる、読み取り、書き込みの操作）を制御します。
SplDer Gate : トラフィックスキャン	○	-	アクセス先のURLが危険か判断し、ブロックします。
SplDer Mail : メールスキャン	○	-	送受信時のメールウイルスを検出駆除。
Dr.Web Firewall	○	-	不正アクセスから保護し、重要なデータがネットワークを通じて漏洩するのを防ぐパーソナルファイアーウォール。
Office Control	○	-	Webサイト、ファイル、フォルダへのアクセス制限や、利用デバイスの制限、インターネット接続時間制限などの設定ができます。
動作解析 : ふるまい検知機能 (Behavior Analysis)	○	○	HOSTSファイルや重要なシステムレジストリキーの変更などを監視し、ブロックします。
ランサムウェア保護 : ふるまい検知機能 (Ransomware Protection)	○	○	ランサムウェアをブロックします。
エクスプロイト防止 : ふるまい検知機能 (Exploit Prevention)	○	○	アプリケーションの脆弱性を利用する悪意のあるオブジェクトをブロックします。
Scanner : 手動スキャン	○	○	ユーザが任意タイミングでスキャンを行います。
Application Control	○	-	業務に関係ないアプリケーションの利用をブロックすることができます。



保護機能「SpIDer Guard」：ファイルシステムのリアルタイム保護

メインメモリ内に常駐し、リアルタイムで端末を監視し脅威を検出します。

SpIDer Guard はOS起動時に自動的に起動され、プロセス・ファイル・メモリへのアクションが行われたタイミングでスキャンを実行します。

Security Center > ファイルとネットワーク > SpIDer Guard

← ファイルとネットワーク

SpIDer Guard
システムをリアルタイムでスキャンします。

スキャンのオプション

リムーバブルメディアをスキャンする
 オン

リムーバブルメディアのオートランをブロックする
 オン

アクション

感染した
修復、修復不可能な場合は隔離(推奨)

疑わしい
隔離(推奨)

Security Center > ファイルとネットワーク > SpIDer Guard

← ファイルとネットワーク

SpIDer Guard
システムをリアルタイムでスキャンします。

アクション

感染した
修復、修復不可能な場合は隔離(推奨)

修復、修復不可能な場合は隔離(推奨)

修復、修復不可能な場合は削除

隔離

削除

隔離(推奨)

ダイアラー
隔離(推奨)

ジョークプログラム

※初期では各端末での設定は出来ません。管理サーバ（Control Center）にて、設定が行えます。

保護機能「SpIDer Gate」：Webトラフィックをチェック

受信するHTTPトラフィックを検査し悪意のあるオブジェクトを全てブロックします。

SpIDer Gateは、HTTPSなどの暗号化プロトコルで送信されたデータもチェックできます。

Security Center > ファイルとネットワーク > SpIDer Gate

← ファイルとネットワーク

SpIDer Gate
受信トラフィックと送信トラフィックをリアルタイムで監視します。

スキャンのオプション

IMクライアントのトラフィックとURLをスキャンする

オン

Mail@RU Agent、ICQ、Jabberなどのインスタントメッセージクライアントによって送られたデータやURLをスキャンします

ブロックパラメータ

著作権者からの申し立てによってリストに登録されたURLをブロックする

オン

非推奨サイトをブロックする

オン

Security Center > 除外 > Webサイト

← 除外

Webサイト

Dr.Webによって非推奨とされているWebサイトへのアクセスを許可することができます。これらのサイトに対するウイルススキャンは引き続き実行されます。

+

✎

🗑️

⋮

ファイル名	SplDer Gate



保護機能「SpIDer Mail」：メールスキャン

メールクライアントとメールサーバー間の通信を監視します。**メールの送受信においてもマルウェアを検出し駆除します。**

Dr.Web Anti-spamを使用して、スパム（迷惑メール）をスキャンすることもできます。



保護機能「Dr.Web Firewall」：パーソナルファイアウォール

不正アクセスからパソコンを守り、重要なデータがネットワーク経由で漏洩することを防ぎます。

アプリケーションレベルおよびネットワークレベルで疑わしい接続をブロックします。

Dr.Web Firewallは、ホワイトリストに登録されているものを除き、全てのアプリケーションによる通信とポートを監視します。

Security Center > ファイルとネットワーク > Firewall

← ファイルとネットワーク

Firewall

ネットワークとアプリケーションレベルで接続設定とデータ転送を監視します。

動作モード

未知の接続を許可

ループバックインターフェイスを許可

オン

アプリケーション

アプリケーションのフィルタリングルールを指定

アプリケーションルール [変更](#)

Security Center > ファイルとネットワーク > Firewall > ネットワーク

Firewall

ネットワーク

現在のフィルタリングルールを確認・編集、または新しいルールを追加することができます。

[ルールセット](#)

特定のネットワークインターフェイス経由で送信されるパケットのフィルタリングに使用するルールセットを選択してください。

ネットワークインターフェイス	アダプター	ルールセット
Ethernet	Realtek PCIe GBE Family Controller	Default Rule
VirtualBox Host-Only Network	VirtualBox Host-Only Ethernet Adapt...	Default Rule

※初期では各端末での設定は出来ません。管理サーバ（Control Center）にて、設定が行えます。

保護機能「Office Control」：簡易フィルタリング機能

ユーザーが不適切なWebサイト（暴力、ギャンブルなど）にアクセスすることを制限したり、特定のWebサイトのみにアクセスを許可することができます。

Security Center > Office Control > user > インターネット

← Office Control

user

インターネット 時間 ファイルとフォルダ

Webサイトへのアクセスを設定し、ブラックリストとホワイトリストを作成する。

カテゴリ別にアクセスを制限する

制限なし

カテゴリ別にアクセスを制限する

ホワイトリスト上のWebサイトに対するアクセスのみを許可

ブラックリストとホワイトリスト

リストは空です 変更

セーフサーチ

検索エンジンに対して自動的にセーフサーチを有効にする

オン

Security Center > Office Control > インターネット > user > カテゴリ別にアクセスを制限する

← user

Webサイトの 카테고리

アクセスを制限するカテゴリを選択できます。

アダルトコンテンツ

暴力

武器

ギャンブル

麻薬

オンラインゲーム

仮想通貨マイニングプール

テロリズム

卑猥な表現

チャット

メール

ソーシャルネットワーク

アノマイザー

求人情報

保護機能「動作解析」：ふるまい検知（予防的保護）機能

従来の検出手法を回避することができる未知の悪意のあるプログラムからシステムを保護します。お使いのコンピューターを感染させる可能性のある信頼されていないアプリケーションの動作に対するDr.Webの対応を設定することができます。


保護するオブジェクト	許可	ユーザーに確認	ブロック
実行中のアプリケーションの整合性	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
HOSTS ファイル	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
ディスクへの低レベルアクセス	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
ドライバのロード	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
イメージ実行オプション	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

アプリケーション	パス
notepad.exe	C:\Windows\notepad.exe

※初期では各端末での設定は出来ません。管理サーバ（Control Center）にて、設定が行えます。

保護機能「ランサムウェア保護」：ふるまい検知（予防的保護）機能

既知のアルゴリズムを使用してユーザーファイルを暗号化しようとするプロセスをセキュリティ上の脅威として検出することができます。



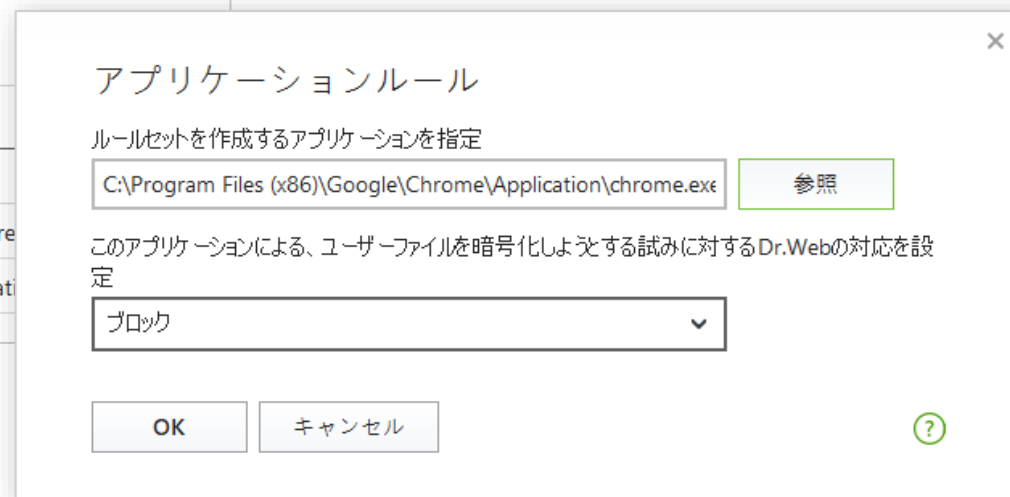
Security Center > Preventive Protection > Ransomware Protection

← Preventive Protection

Ransomware Protection

ユーザーのファイルの暗号化を試みるアプリケーションに対するDr.Webのアクションを設定してください。これらのパラメータは、以下のアプリケーションには適用されませんのでご注意ください。

アプリケーション	ルール	パス
notepad.exe	ブロック	C:\Windows\notepad.exe
iexplore.exe	ユーザーに確認	C:\Program Files (x86)\Internet Explorer\iexplore.exe
chrome.exe	許可	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe



アプリケーションルール

ルールセットを作成するアプリケーションを指定

C:\Program Files (x86)\Google\Chrome\Application\chrome.exe 参照

このアプリケーションによる、ユーザーファイルを暗号化しようとする試みに対するDr.Webの対応を設定

ブロック

OK キャンセル

※初期では各端末での設定は出来ません。管理サーバ（Control Center）にて、設定が行えます。

保護機能「エクスプロイト防止」：ふるまい検知（予防的保護）機能

- ✓ アプリケーションの脆弱性を使用する悪意のあるプログラムをブロックできます。
- ✓ Windows OS等の脆弱性を突いた悪意あるプログラムをエクスプロイト防止機能でブロックすることが可能です。
- ✓ Dr.Web クラウドサービスのデータを活用し、既知の脆弱性を悪用するプログラムをブロックします。



保護機能「Scanner」：手動スキャン

ブートセクター、メモリー、複合オブジェクト（アーカイブ、コンテナ、メール）内にある個別のファイルやオブジェクトを検査します。**手動または、予め設定したスケジュールに沿って実行します。**

Security Center > 設定 > Scanner

← 戻る

- 一般
- 通知
- Self-Protection
- Scanner**
- Server

スキャンのオプション

バッテリー駆動時にスキャンを一時停止する
 オフ

警告音を有効にする
 オフ

コンピューターリソースの使用

最適 (推奨)

アクション

感染した

修復、修復不可能な場合は隔離 (推奨)

疑わしい

隔離 (推奨)

カスタムスキャンが完了しました

← Scanner

スキャンが完了しました

スキャン済みのオブジェクト: 2645 検出された脅威: 3 駆除された脅威: 0

検出された全ての脅威を直ちに駆除することを推奨します。
Dr.Web Scannerは設定に応じてアクションを適用します。

駆除

ファイル名	脅威	アクション	パス
▶ 感染した	2	修復、修復不可...	
▶ アーカイブ	1	隔離	

運用管理機能：統計情報の確認

各端末のマルウェア検出情報をControl Center（集中管理サーバ）で確認することが可能です。

➤ 脅威情報

どの端末で、いつ、どのような脅威が検出されたか等を確認できます。

➤ 脅威統計情報

どのような脅威が検出されたかを確認できます。

脅威情報									
脅威					最も多く検出された脅威				
最も多く攻撃を受けた端末					最も多く検出された脅威				
DWP-Cent73-ESS11  3					EICAR Test File (NOT a Virus!) 				
<input type="checkbox"/>	時刻	ID	端末	端末アドレス	種類	脅威	アクション	コンポーネント	オブジェクト
<input type="checkbox"/>	20-10-2020 01:13:02	096b0ef9-d6be-443d-a99c-bfc1893b5232	DWP-Cent73-ESS11	ssl://127.0.0.1:38470	感染	EICAR Test File (NOT a Virus!)	隔離	SpIDer Guard for UNIX	/root/eicar.com.txt
<input type="checkbox"/>	20-10-2020 07:13:02	096b0ef9-d6be-443d-a99c-bfc1893b5232	DWP-Cent73-ESS11	ssl://127.0.0.1:38470	感染	EICAR Test File (NOT a Virus!)	隔離	SpIDer Guard for UNIX	/root/eicar.com.txt
<input type="checkbox"/>	20-10-2020 13:13:01	096b0ef9-d6be-443d-a99c-bfc1893b5232	DWP-Cent73-ESS11	ssl://127.0.0.1:38470	感染	EICAR Test File (NOT a Virus!)	隔離	SpIDer Guard for UNIX	/root/eicar.com.txt

脅威統計情報			
脅威のクラス		最も多く検出された脅威	
感染  3	EICAR Test File (NOT a Virus!)  3		
脅威	種類	端末	合計
EICAR Test File (NOT a Virus!)	感染	1	3

運用管理機能：端末ステータスの確認

各端末のステータスは、リアルタイムにControl Center（集中管理サーバ）で視覚的に表示することが可能です。

※端末アイコンの色により確認可。

また、詳細情報も確認することができます。

コンポーネントが最新であれば、
ふるまい検知で多くの未知の脅威を
検知可能

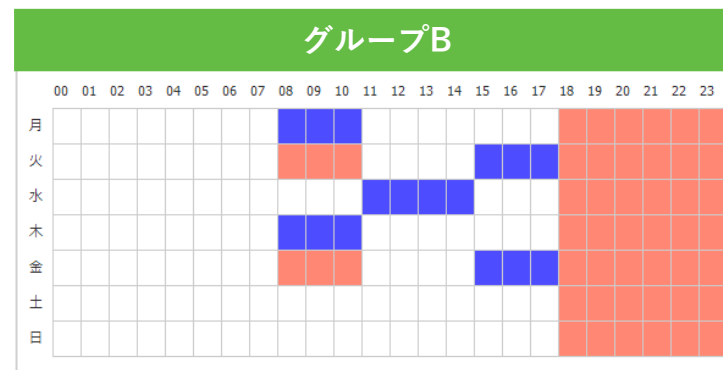
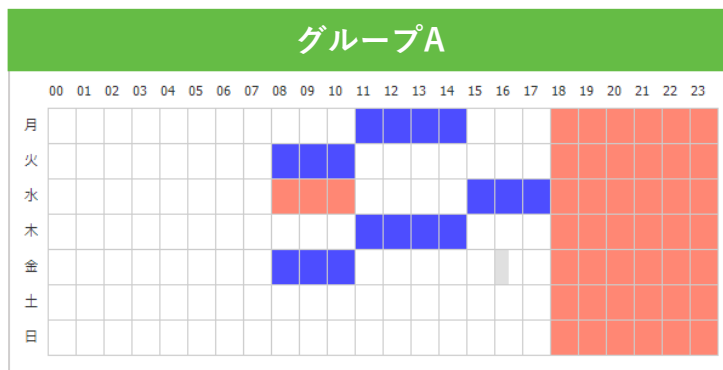
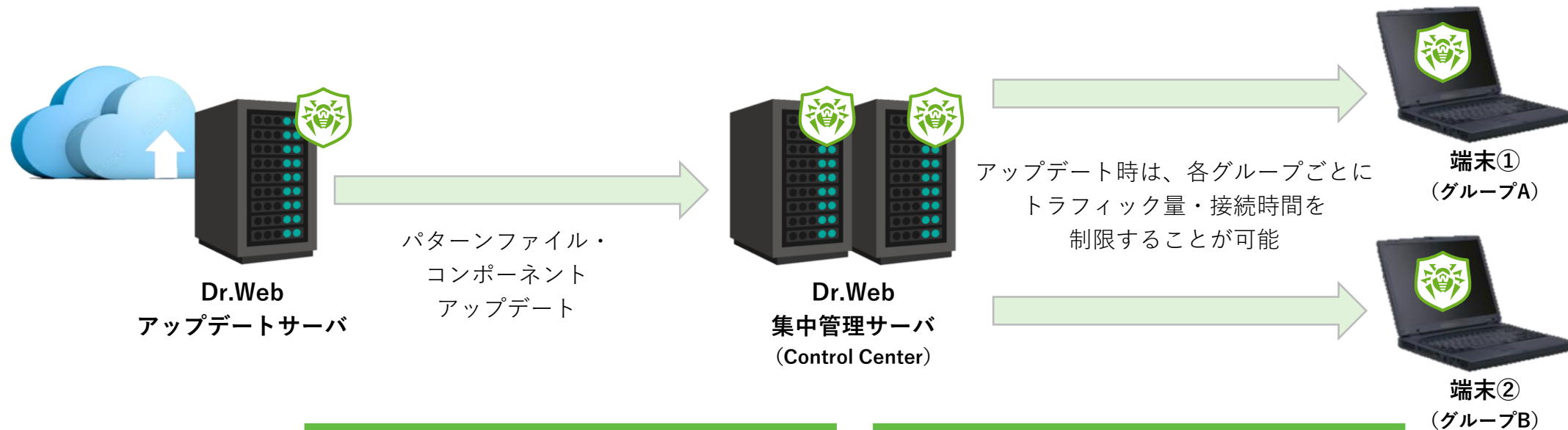
端末の一覧

- アンチウイルスネットワーク
 - Configured | 端末：1
 - Everyone | 端末：3
 - 0825dokutaebu-no-MacBook-ea.local | tcp://122.219.128.47:51465
 - DWP-Cent73-ESS11 | ssl://127.0.0.1:38470
 - DWP-OG-PC | ssl://122.219.128.47:49200
 - Guard+Mail | 端末：0
 - Guard Only | 端末：0

ステータス情報							
時刻	ID	端末	端末アドレス	重要度	ソース	メッセージ	
20-10-2020 15:29:04	096b0ef9-d6be-443d-a99c-bfc1893b5232	DWP-Cent73-ESS11	ssl://127.0.0.1:38470	非常に低い	Agent	OK	
04-09-2020 14:36:38	ca94ab81-9227-47e3-aadc-79f5b0df4a0c	0825dokutaebu-no-MacBook-ea.local	tcp://122.219.128.47:51465	高い	Server	Dr.Webウイルスデータベース製品は古くなっています	
04-09-2020 14:36:38	ca94ab81-9227-47e3-aadc-79f5b0df4a0c	0825dokutaebu-no-MacBook-ea.local	tcp://122.219.128.47:51465	高い	Server	Dr.Web Agent for UNIX製品は古くなっています	
25-08-2020 12:29:18	60819363-d21d-b211-928c-f40742dbfce1	DWP-OG-PC	ssl://122.219.128.47:49200	非常に低い	Agent	端末がオフラインか、Agentが動作していません	

運用管理機能：アップデートの仕組み

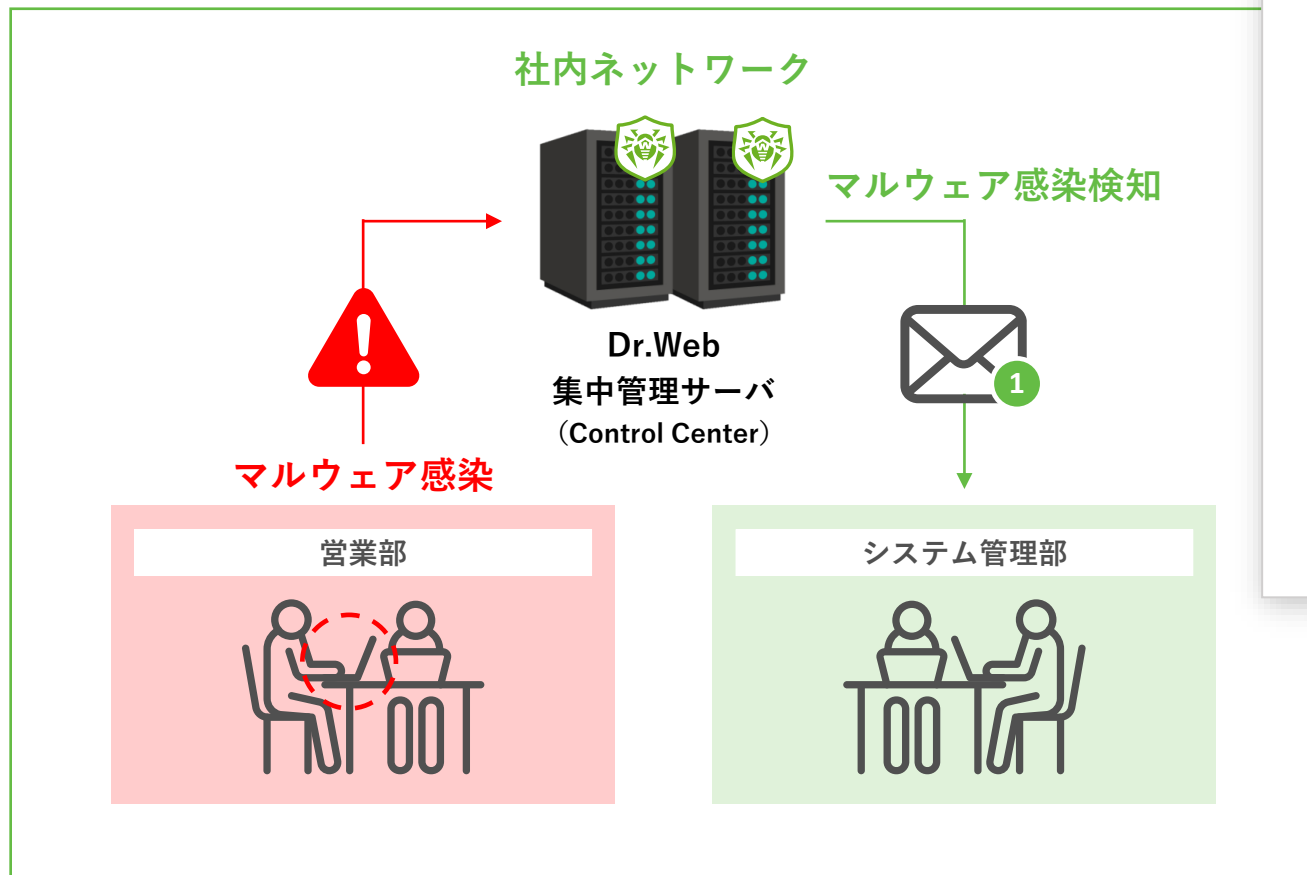
集中管理サーバから、各Agentへのアップデート送信は、グループごとに帯域や対応時間を設定することが可能です。
このことにより、社内ネットワーク帯域への負荷を分散させることが可能です。



- 速度はデフォルト値までに制限されています
- 速度は1 KB/sに制限されています
- データの送受信は禁止されています

運用管理機能：マルウェア検知時の管理者通知

Control Center で、登録された管理者メールアドレスに対して、
Dr.Webをインストールされた端末で発見されたマルウェア情報を通知



差出人 bbb@bbbb.jp

件名 **注意！** ○○端末上で脅威が検出されました

宛先 yeah@flashcu.be

端末 : aaaaa@aaaaa.jp

時刻 : 2024 4.1 13:00 10.021

ソース : Spider Guard for windows workstations
(t350-pc\ t350:t350-pc\None)

オブジェクト : C: \ Users \ aaaaaaaa.tmp(未知)

脅威 : EICAR Test File(NOT a virus!)

アクション : 隔離



運用管理機能：その他

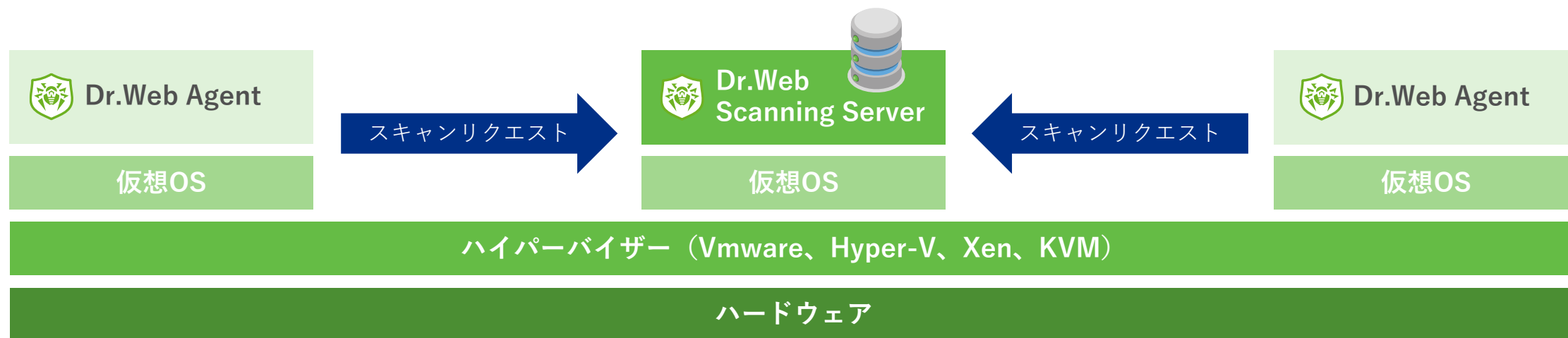
No.	タイトル	概要
1	Agentグループの管理	Control Center で、各種端末を階層分けして管理することが可能です。 階層分けされたフォルダ毎に、各種設定を保存することが出来ます。
2	複数シリアルナンバーの管理	追加の購入や、部署ごとの管理などでシリアルナンバーを複数で運用される場合も1つのControl Center 上で管理ができます。 シリアルナンバー毎に、Control Center をご用意して頂く必要はございません。
3	異なるOS端末の管理	WindowsやMacなどの異なるOSでも1つのControl Center 上で管理ができます。異なるOS毎に、Control Center をご用意して頂く必要はございません。
4	ライセンスのアップデート	シリアルナンバーの更新処理は、Control Center 上で一括で更新することが可能です。 ※スタンドアロン版は、各端末でシリアルナンバーの更新が必要になります。
5	インストール製品情報	インストールされている製品、シリアルナンバー、残ライセンス数をControl Center 情報で確認することが出来ます。



その他機能と対応OS

仮想環境下でのスキャン機能

多数のマシンが存在する仮想化環境において、各マシン上で稼働するアンチウイルスがファイルスキャンやパターンファイルの更新を実行した場合、膨大な負荷が発生します。この課題を解決し、仮想化ホストの負荷を軽減します。



- ファイルスキャンは全てScanning Server上で集約して実行されます。
- パターンファイルは、Dr.Web Scanning Server にのみアップデートされ、**更新にかかるトラフィックの負荷を軽減**します。

稼働条件

ハイパーバイザー: VMware、Hyper-V、Xen、KVM OS: Linux、FreeBSD (対応OSの一覧はUNIX用アンチウイルスパッケージ向けと同様)

※システム要件詳細についてはマニュアル等をご確認下さい。



対応OS

Dr.Web製品	対応OS
Desktop Security Suite	<p>< Windows ></p> <p>32ビットプラットフォーム：</p> <ul style="list-style-type: none">• Windows XP Service Pack 2以降• Windows Vista Service Pack 2以降• Windows 7 Service Pack 1以降• Windows 8• Windows 8.1• Windows 10 22H2以前 <p>64ビットプラットフォーム：</p> <ul style="list-style-type: none">• Windows Vista Service Pack 2以降• Windows 7 Service Pack 1以降• Windows 8• Windows 8.1• Windows 10 22H2以前• Windows 11 22H2以前 <p>< Mac ></p> <ul style="list-style-type: none">• macOS 10.12 Sierra• macOS 10.13 High Sierra• macOS 10.14 Mojave• macOS 10.15 Catalina• macOS 11 Big Sur• macOS 12 Monterey• macOS 13 Ventura• macOS 14 Sonoma• macOS 15 Sequoia <p>< Linux ></p> <p>法人向けDr.Web製品のマニュアル ワークステーションを保護するDr.Web Desktop Security Suite「Dr.Web for Linux」を確認ください。 https://download.drweb.co.jp/doc/</p>
Server Security Suite	<p>< Windows ></p> <p>32ビットプラットフォーム：</p> <ul style="list-style-type: none">• Windows Server 2003 with Service Pack 1 以降• Windows Server 2008 with Service Pack 2 以降 <p>64ビットプラットフォーム：</p> <ul style="list-style-type: none">• Windows Server 2008 with Service Pack 2 以降• Windows Server 2008 R2 with Service Pack 1 以降• Windows Server 2012• Windows Server 2012 R2• Windows Server 2016• Windows Server 2019• Windows Server 2022 <p>< Mac ></p> <ul style="list-style-type: none">• macOS 10.12 Sierra• macOS 10.13 High Sierra• macOS 10.14 Mojave• macOS 10.15 Catalina• macOS 11 Big Sur• macOS 12 Monterey• macOS 13 Ventura• macOS 14 Sonoma• macOS 15 Sequoia <p>< Unix ></p> <p>法人向けDr.Web製品のマニュアル サーバを保護するDr.Web Server Security Suite「Dr.Web for Unix」を確認ください。 https://download.drweb.co.jp/doc/</p>



Dr.Web アンチウイルス 製品群



Dr.Web ソリューションマップ

エンドポイント / ゲートウェイ アンチウイルス	Dr.Web Enterprise Security Suite PC / Mobile / Server OS / MacOS / Proxy / Mail Server	オンプレミス アンチウイルス
	Dr.Web Premium サブスクリプションサービス PC / Mobile / Server OS / MacOS	クラウド/サブスク型 アンチウイルスサービス
アドオン / セカンドオピニオン	Dr.Web Cure Utilities	インストールレスアドオン
	Dr.Web KATANA	常駐型アドオン (シグニチャーレス)
スレットインテリジェンス	Dr.Web y-Tracker	高度なスレッドポータル
	Dr.Web Threat investigation service	個別調査サービス
EDR-like	Dr.Web vxCube	クラウド型解析

本来のアンチウイルスの役割として、グレーなものも含め検知・駆除し、システム運用者の負担を軽減します。

エンドポイント製品では極力コンパクトな設計にすることで挙動の軽さを実現します。

運用上負担となりがちな「解析・追跡」の要素は外出しし、クラウド型のオンデマンドサービスとして提供しております。



Dr.Web プロダクトラインナップ

用途	製品名	対応OS等	コメント
エンドポイント	Dr.Web Desktop Security Suite	Windows / Linux / macOS	ふるまい検知を搭載したPC端末用 総合アンチウイルス
	Dr.Web Katana	Windows	ふるまい検知のみ提供
モバイル	Dr.Web Mobile Security Suite	Android	世界で1億6000万DLの実績
サーバー	Dr.Web Server Security Suite	Windows / Linux / macOS	Windows向けはふるまい検知搭載 国内ISP/CATVでも実績多数
メールサーバ	Dr.Web Mail Security Suite	Unix	国内ISP/CATVでも実績多数 アンチスパムオプションあり
修復ユーティリティ	Dr.Web CureIt! / Dr.Web CureNet!	Windows	他社AV搭載の環境で簡単スキャン セカンドオピニオン
無制限ライセンス	オフィスマルチパック	Windows / Linux macOS / Android	中小企業向けデバイス無制限パック
	公共マルチパック		公共期間向けデバイス部制限パック
	小中高等学校向け無制限ライセンス		学校向け無制限パック（学校単位）
	大学専門学校向け無制限ライセンス		大学向け無制限パック（人数単位）
インテリジェントアナライザー	Dr.Web vxCube	Windows / Android	オブジェクト解析クラウド 未知の脅威に対するワクチン提供
サブスクリプション	Dr.Web Premiumサブスクリプションサービス	Windows / Linux / macOS	欧州・ロシア初のクラウド型 アンチウイルス



今後とも宜しくお願い致します。

Doctor Web Pacific, Inc
<http://www.drweb.co.jp/>