



プロダクト概要説明資料

Dr.Web Server Security Suite

株式会社Doctor Web Pacific



© Doctor Web,
2021

www.drweb.com

● 本資料について

- 本資料は、Dr.Web Enterprise Security Suite（以下ESS）シリーズの1製品である、Dr.Web Server Security Suite（以下SSS）の機能説明資料（集中管理版）です。
- 本資料は、すべての機能や制限事項を記載した資料ではありませんので、あらかじめご了承ください。
- システム要件や制限事項などは、Dr.Web 製品マニュアルページ（<http://download.drweb.co.jp/doc/>）にて公開されている資料をご参照ください。
- 本資料は、2020年10月時点で公開されている製品を元に作成されております。今後のバージョンアップや機能追加などによって内容は予告なく変更される場合がありますので、あらかじめご了承ください。

● 本資料で用いられる略称

- Dr.Web Enterprise Security Suite・・・ESS
- Dr.Web Server Security Suite・・・SSS
- Control Center・・・CC
- ネットワーク・・・NW

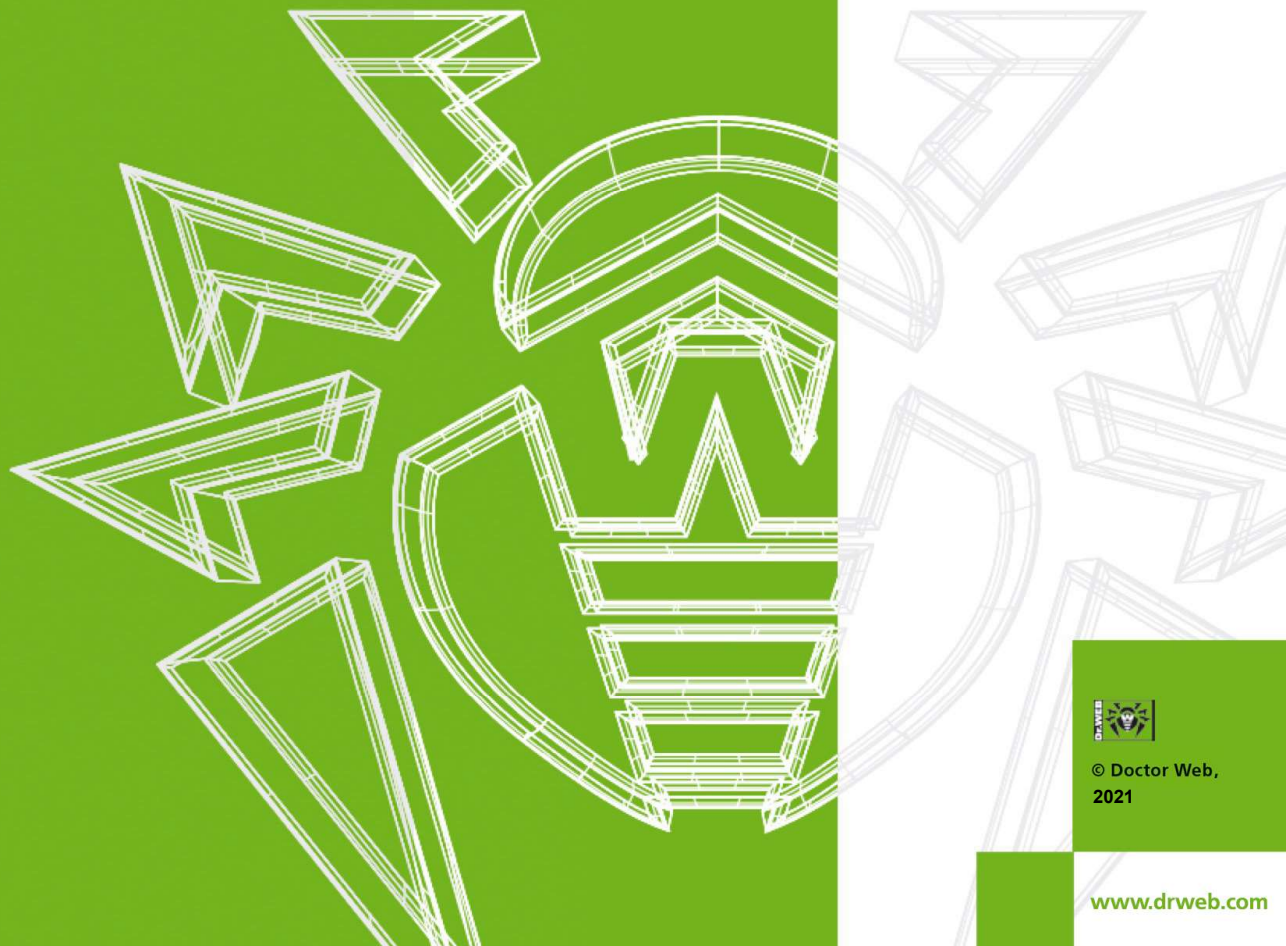
版数	改訂日	内容
第1版	2020/10/30	第1版として公開



SSS

製品コンセプト

株式会社Doctor Web Pacific



© Doctor Web,
2021

www.drweb.com

課題①ランサムウェアの侵入経路

ランサムウェア

- ネットワークへの直接侵入
- ダークウェブサイト

「ランサムウェア」とは？

ランサムウェア＝ファイルを暗号化するなどして身代金を要求するもの

- 感染の手法：

- メール経由ばらまき型（2016年頃の傾向）
- 法人ネットワークへの**直接侵入**（2019年以降の傾向）

Emotetに感染することにより、アクセス権を詐取され

Access-as-a-Service（AaaS）などを利用して侵入してくる。

- 想定される被害：

- 身代金(ビットコインなどの仮想通貨) の請求
- データのロックによる、業務停止
- 情報暴露

ダークウェブサイトによる亜種マルウェア開発

ダークウェブ → マルウェアの作成用ポータルが存在

- ダークウェブとは

- 匿名性保持や追跡回避の技術が資料されており、専用ソフトを使用しないとアクセスできないWebサイト。
- 違法な取引などが行われている。

認証情報

メールアドレス

銀行口座番号

運転免許証番号、パスポート番号

マルウェア⇒ランサムウェアを直接侵入させるためのマルウェアの開発

ダークウェブサイト内にある 【Access-as-a-Service (AaaS)】

サイバー犯罪者が侵入したネットワークで構築したバックドアのアクセス権を他のサイバー犯罪者に販売、レンタルする仕組み。バックドアからに侵入し、新たなマルウェア、ランサムウェアを侵入させる。

プログラムを知らない人間でもダークウェブで、マルウェアを購入することが可能な世の中！

課題① ランサムウェアの侵入経路

日々進化し、攻撃してくるランサムウェアから負の連鎖を打ち切るには

古くから存在するランサムウェアも、亜種のマルウェアがダークウェブで売買され、たびたび攻撃に使われます。

パターンファイルによる既知のランサムウェア検知だけでは、亜種のランサムウェアをブロックすることは難しくなり、ヒューリスティックエンジンが搭載されたアンチウイルスソフトが必要になります。

挙動不審の動きを検知し、ブロックするためにも未知の脅威を検出する機能を搭載したアンチウイルスソフトが必要になります。



シンプルかつ最適化されたテクノロジー

**信頼性の高いテクノロジー
があれば余計なものは
必要ありません。**

最適化された技術だけを使うことで、
コンピュータ環境の安定を維持し、
安全と快適を両立させます。

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

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

機械学習を応用した マルウェア検出技術

予防的保護の テクノロジー

Dr.Webが提供する多層コンポーネント

シグニチャーデータベース	非シグニチャー型テクノロジー
• SpIDer Guard リアルタイム保護 • Scanner 手動スキャン • SpIDer Gate HTTPモニター • SpIDer Mail メールスキャン	• Origins Tracing • ヒューリスティック解析 • クラウドベースの脅威検出テクノロジー
機械学習を応用したマルウェア検出技術	予防的保護のテクノロジー
• Injection Protection • Dr.Web ShellGuard • Dr.Web Process Dumper	• 動作解析 • ランサムウェア保護 • エクスプロイト防止



Dr.Web SSS システム要件 Windows

パラメータ	要件
CPU	i686互換プロセッサ
OS	32ビットプラットフォーム : •Windows Server 2003 with Service Pack 1 以降 •Windows Server 2008 64ビットプラットフォーム : •Windows Server 2008 with Service Pack 2 以降 •Windows Server 2008 R2 •Windows Server 2012 •Windows Server 2012 R2 •Windows Server 2016 •Windows Server 2019
RAM	512 MB以上
画面の解像度	1024x768以上 (推奨)
クラウドおよび仮想化環境のサポート	プログラムは以下の環境での動作が保証されています。 •VMware •Hyper-V •Xen •KVM

パラメータ	要件
プラットフォーム	下のアーキテクチャおよびコマンドシステムのプロセッサがサポートされています。 •Intel/AMD : 32ビット (IA-32、x86) 64ビット (x86_64、x64、amd64) •ARM64
RAM	500MbのRAM空き容量 (1Gb以上を推奨)
ハードディスク容量	512 MB以上
OS	•GNU/Linux カーネルバージョン2.6.37以降glibcライブラリ2.13以降を使用 •FreeBSD バージョン10.3以降



集中管理 サーバ構成 (Control Center)

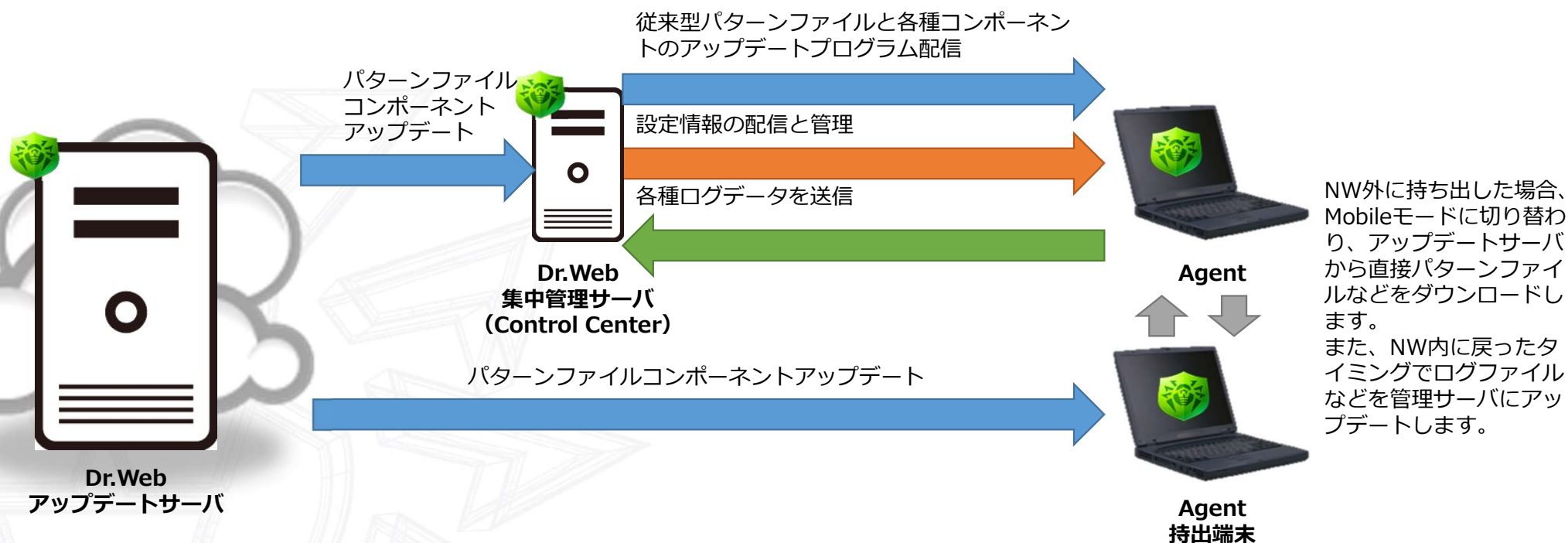
株式会社Doctor Web Pacific



© Doctor Web,
2021

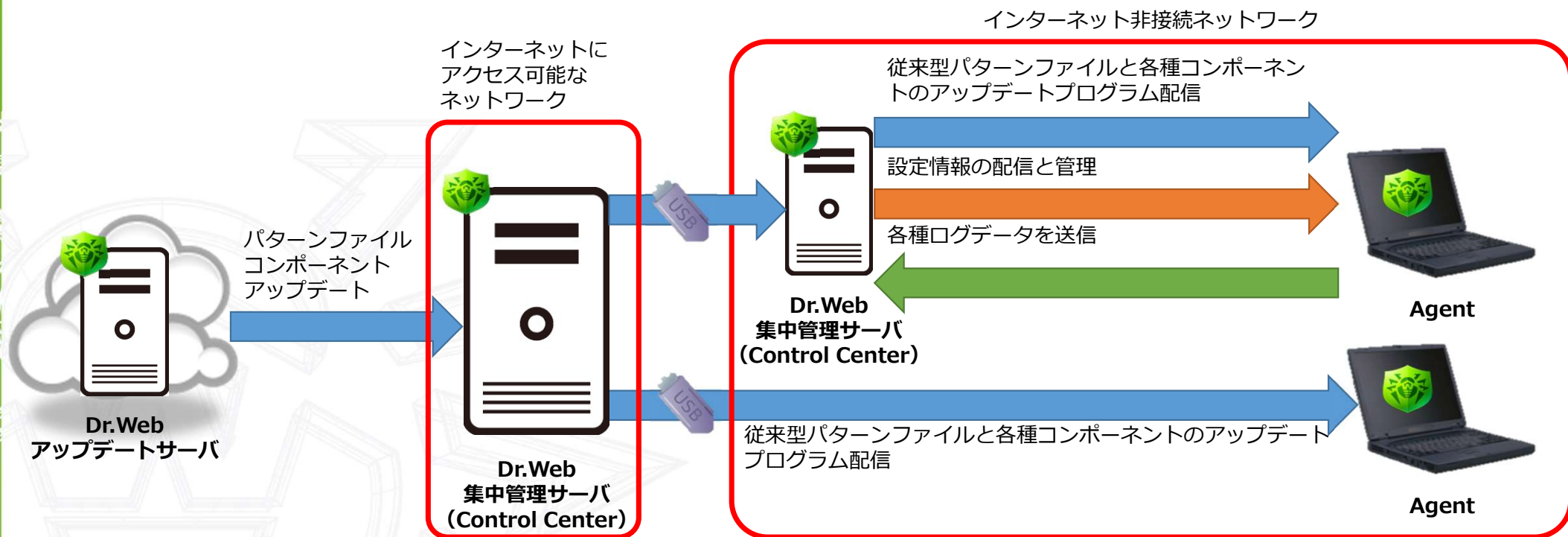
www.drweb.com

基本構成



- 基本的なサーバ構成になります。
 - 集中管理サーバのデータベースは、管理するAgent数でご用意して頂くものが異なります。300Agent以下の場合、Dr.Web内にあるデータベースで対応可能です。
- ※301Agent以上になる場合は、お問い合わせください。

インターネット非接続環境の場合



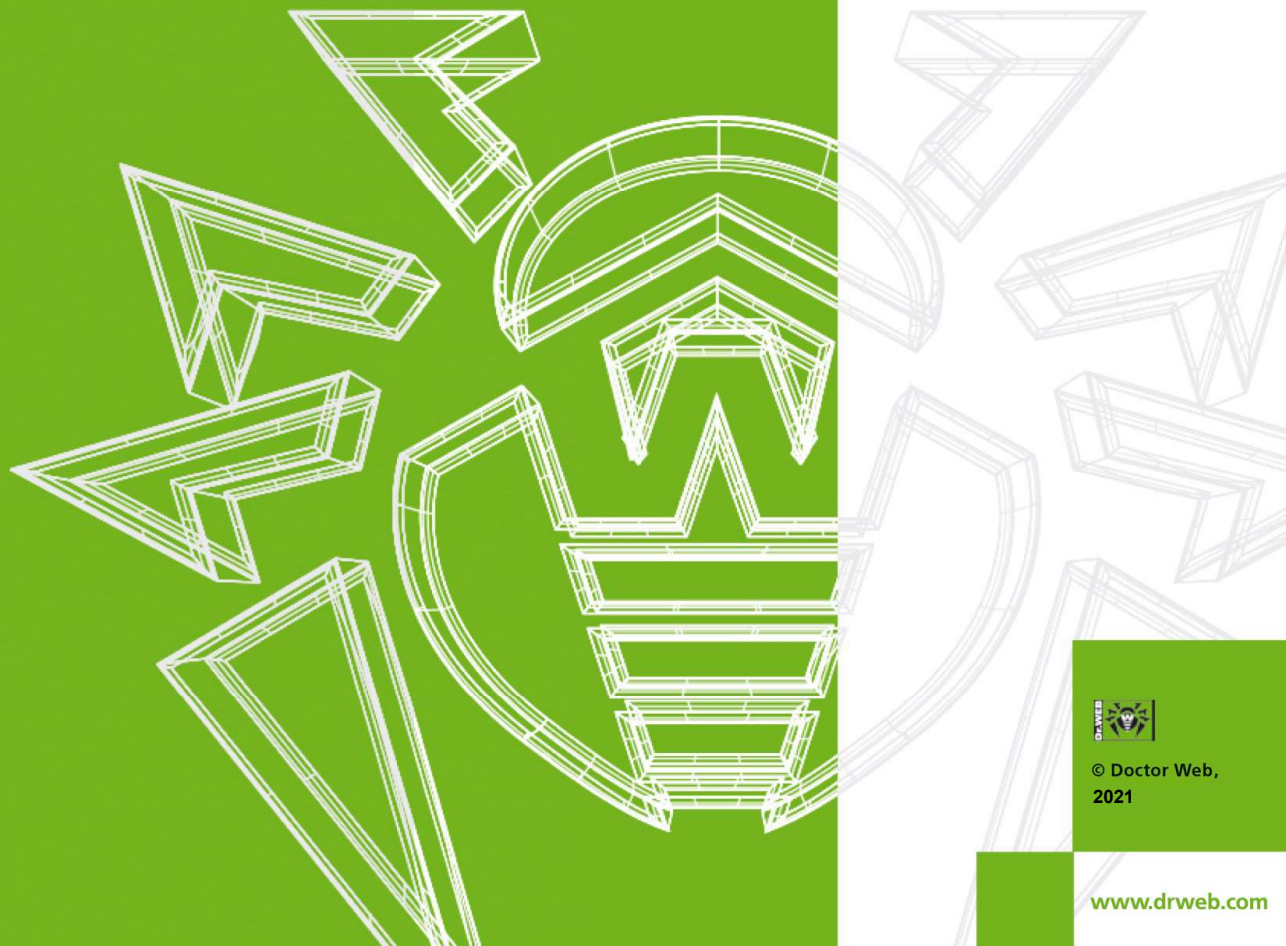
- 集中管理サーバを2台用意し、パターンファイルやコンポーネントをインターネットにアクセスできるNWの集中管理サーバから、できないNWの集中管理サーバにコピーすることが可能です。
- 病院の電子カルテ用NWや、工場などの業務用スタンドアロン端末などでの運用事例がございます。



SSSが提供する

脅威からの保護機能

株式会社Doctor Web Pacific



© Doctor Web,
2021

www.drweb.com

コンポーネント	説明
SpIDer 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。
SpIDer 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。
SpIDer Guard for NSS : リアルタイムスキャン	NSS（Novell Storage Services）ファイルシステムボリューム上のファイルアクティビティを監視します。
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。



メインメモリ内に常駐するアンチウイルスモニターです。プロセス、ファイル、メモリを作成時や起動時にスキャンします。

SpIDer Guard はWindows起動時に自動的に起動し、そのセッションの間はアンロードすることはできません。



※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。

感染させる可能性のあるサードパーティ製アプリケーションの動作（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）への対応を設定することができます。システムオブジェクトの自動変更が、OSに対する悪意のある試みであることや悪影響を与えるものであるかどうか判断し、それらの変更をブロックします。

Security Center > Preventive Protection > Behavior Analysis > 保護レベル

← Preventive Protection

Behavior Analysis

保護レベル アプリケーションアクセス

保護されているオブジェクトへのアクセスを試みるアプリケーションに対するDr.Webのアクションを決定する保護レベルを選択します。カスタムオプションが設定されている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。

最適 (推奨)

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	☐	☐	☒
HOSTS ファイル	☐	☐	☒
ディスクへの低レベルアクセス	☐	☐	☒
ドライバのロード	☒	☐	☐
イメージ実行オプション	☒	☐	☐
Windowsマルチメディアドライバ	☒	☐	☐

← Preventive Protection

Behavior Analysis

保護レベル アプリケーションアクセス

Dr.Webによって保護するオブジェクトごとのアクセスパラメータを設定します。パラメータが設定されていないアプリケーションには、選択された保護レベルが適用されます。

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。

ふるまい検知（予防的保護）ランサムウェア保護

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。これらのハフメータは、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。

ブロック

ブロック

ユーザーに確認

許可

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

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。これらのハフメータは、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

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。

ふるまい検知（予防的保護）エクスプロイト防止

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。

MicrosoftのOS等の脆弱性を突いた悪意あるプログラムも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。



※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。

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。

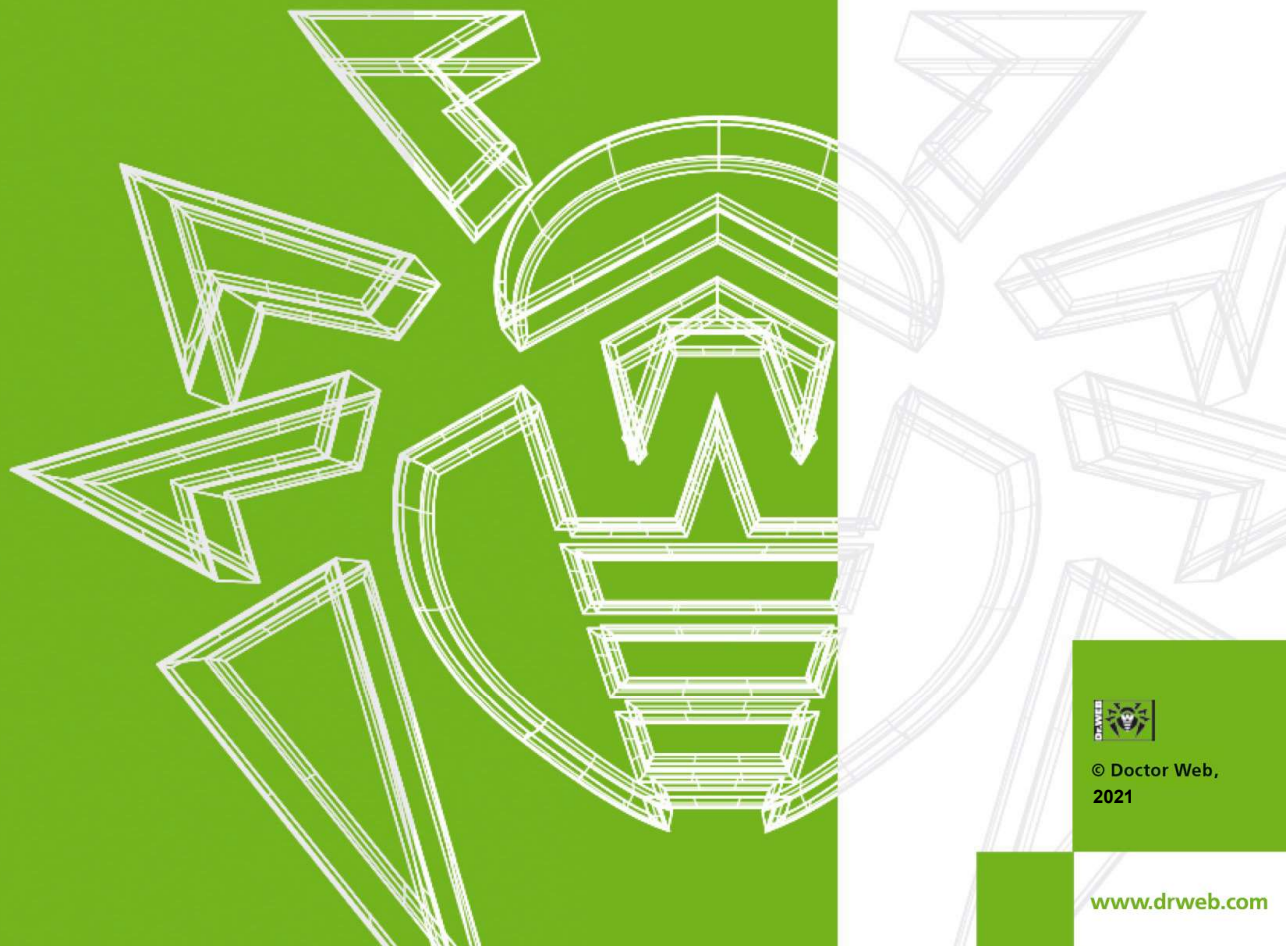


※初期では各端末での設定は出来ません。
管理サーバ（Control Center）にて、設定が行えます。



運用管理機能

株式会社Doctor Web Pacific



© Doctor Web,
2021

www.drweb.com

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					EICAR Test File (NOT a Virus!)				
DWP-Cent73-ESS11 3									
☐ 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	
☐ 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	
☐ 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	
☐ 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		

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。

端末の一覧



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

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	0825dokutaeubu-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	0825dokutaeubu-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

アップデートの仕組み



パターンファイル・コンポーネント
アップデート



アップデート時は、各グループごとにトラフィック量・接続時間を制限することが可能

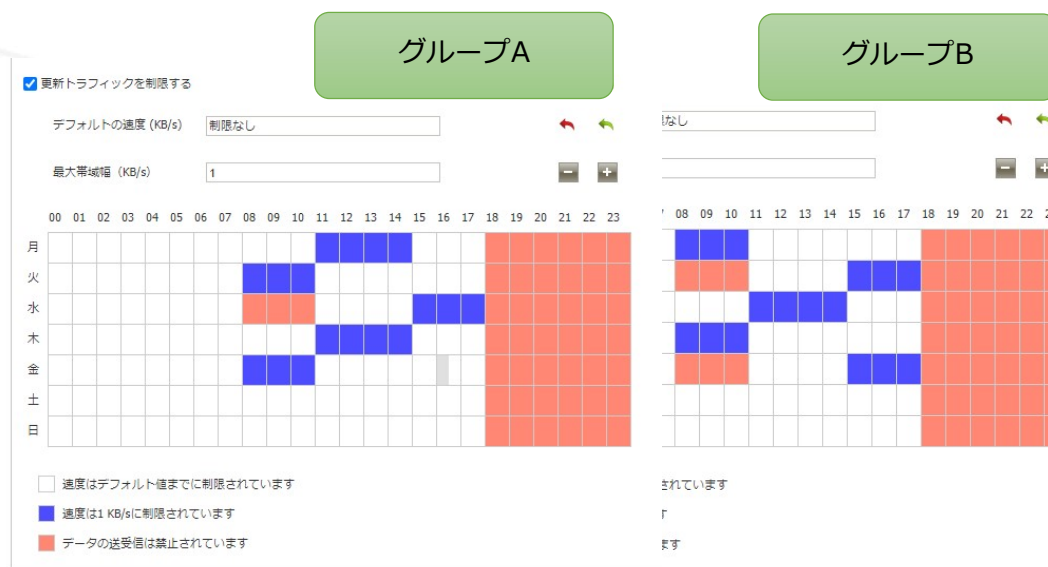


Agent



Agent

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。



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。

- ・ 端末情報
- ・ 時刻情報
- ・ ソース情報
 - ⇒ 検出したコンポーネント
- ・ オブジェクト情報
 - ⇒ 検出されたファイル情報
- ・ 脅威情報
- ・ アクション情報

差出人 [redacted] ☆
件名 注意! [redacted] 端末上で脅威が検出されました。
宛先 yeah@flashcu.be ☆

端末: [redacted] (IPアドレス: [redacted], MACアドレス: 未知, SID: [redacted], 説明: なし)
時刻: 2020-10-08-03:10:40+0300
ソース: SpIDer Guard for Windows workstations (t350-PC\t350:t350-PC\None)
オブジェクト: C:\Users\[redacted]\AppData\Local\Temp\45725770-20201008-031040.tmp (未知)
タイプ: 1
脅威: EICAR Test File (NOT a Virus!)
アクション: 隔離

--
Dr.Web Server 12.00.1-202004130 (Linux 3.10.0-693.17.1.el7.x86_64 x86_64; glibc 2.17)

※別途管理サーバ（Control Center）への設定が必要になります。

Endpointの展開方法

プッシュインストール

集中管理サーバからプッシュインストールを行う方法です。

Active Directory MSI

ADのドメインに参加している端末であればMSIが可能です。

バッチファイルを作成し、 インストーラと展開 (配布ミドルウェアを使って)

IPアドレスの検出が出来ない端末は、バッチファイルと一緒にインストーラを配布頂く方法があります。

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 ESS 製品群

株式会社Doctor Web Pacific



© Doctor Web,
2021

www.drweb.com

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
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 AV-Desk 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)

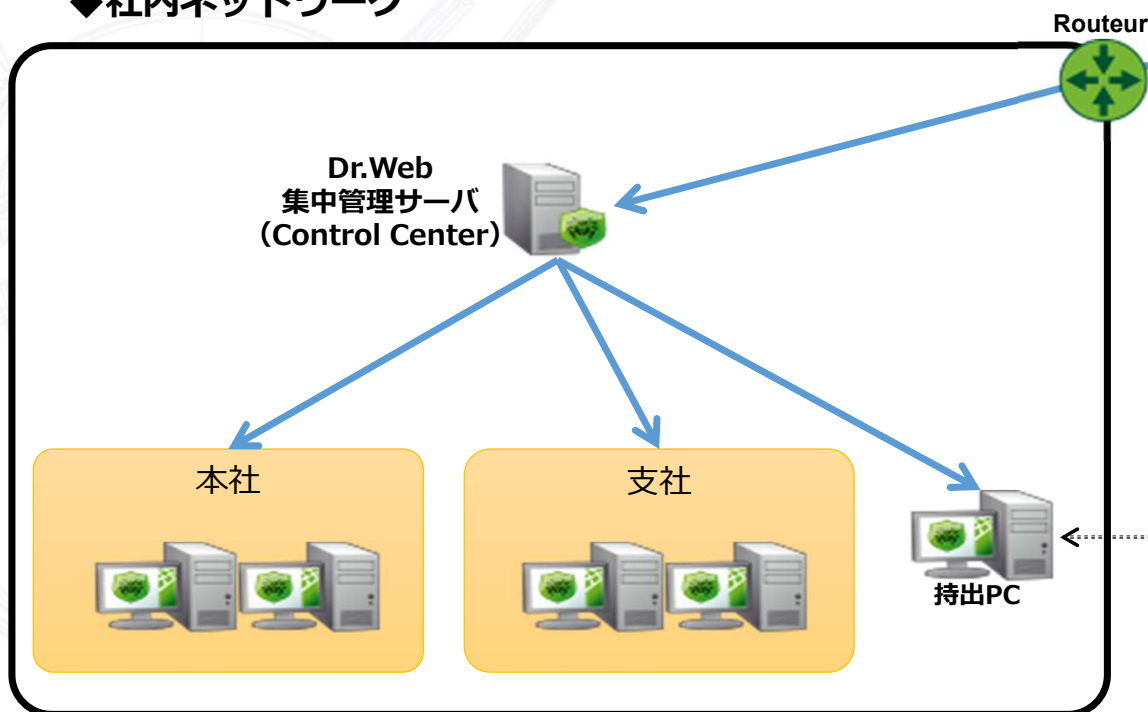
本来のアンチウイルスの役割として、グレーなものも含め検知・駆除し、システム運用者の負担を軽減します。エンドポイント製品では極力コンパクトな設計にすることで挙動の軽さを実現します。運用上負担となりがちな「解析・追跡」の要素は外出しし、クラウド型のオンデマンドサービスとして提供しております。

Dr.Web ESS 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 総合アンチウィルス
	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
Webプロキシ	Dr.Web Gateway Security Suite	Unix	Proxyと連携
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
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）

社内におけるすべてのPC、サーバに対して無制限でインストールできます。（マルチOS対応）

◆社内ネットワーク



ユーザー数で価格提示

Internet

Dr.Web
アップデートサーバ

<対応Product>

- ・ Dr.Web Desktop Security Suite
- ・ Dr.Web Server Security Suite
- ・ Dr.Web Mobile Security Suite



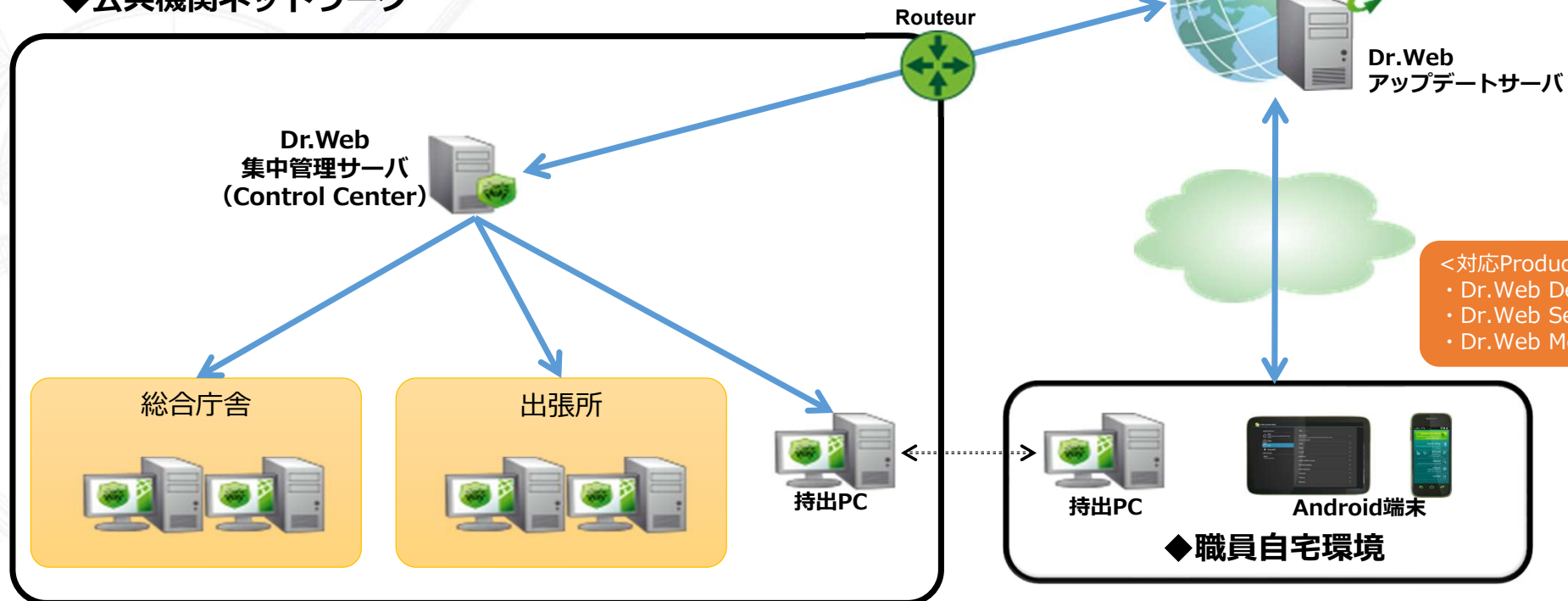
社員皆様の自宅PC、Android端末でも利用できます。



© Doctor Web,
2021

公共機関におけるすべてのPC、サーバに対して無制限でインストールできます。（マルチOS対応）

◆公共機関ネットワーク



ユーザー数で価格提示

<対応Product>

- ・ Dr.Web Desktop Security Suite
- ・ Dr.Web Server Security Suite
- ・ Dr.Web Mobile Security Suite

職員皆様の自宅PC、Android端末でも利用できます。



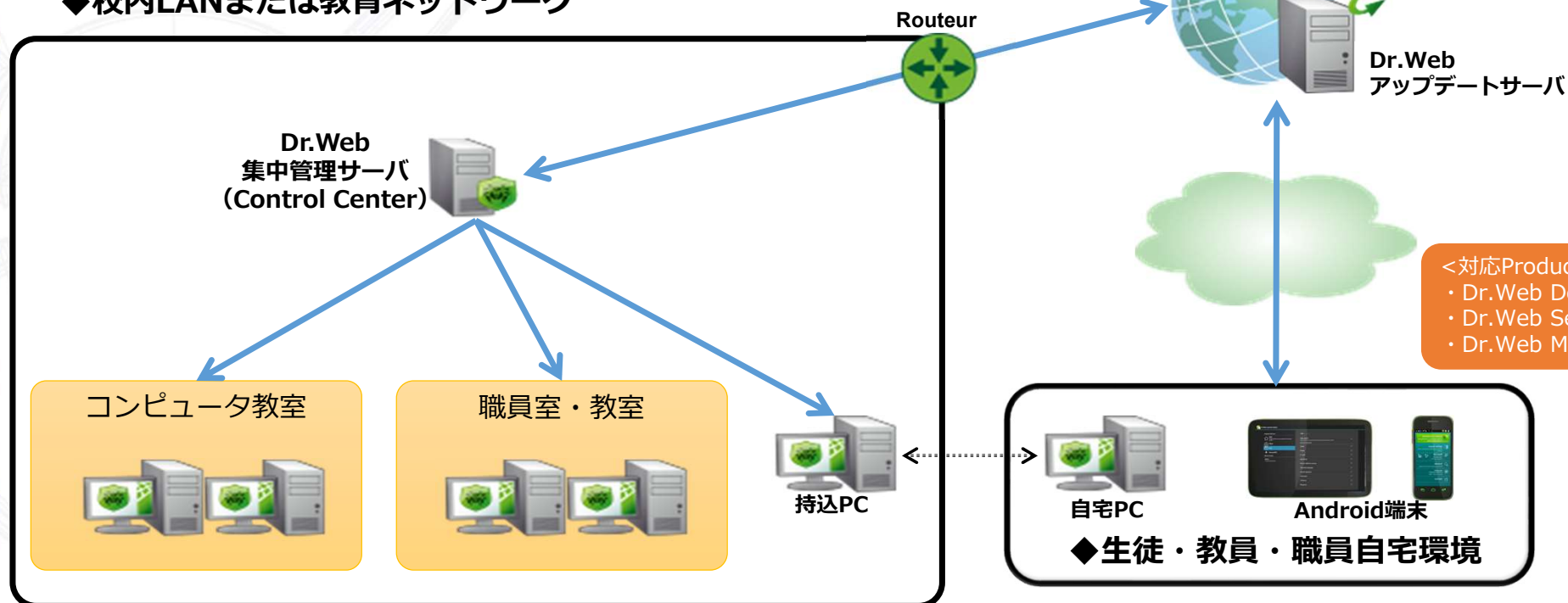
© Doctor Web,
2021

小中高等学校向け無制限ライセンス

学校内すべてのPC、サーバに対して無制限でインストールできます。（マルチOS対応）

学校数で価格提示

◆校内LANまたは教育ネットワーク



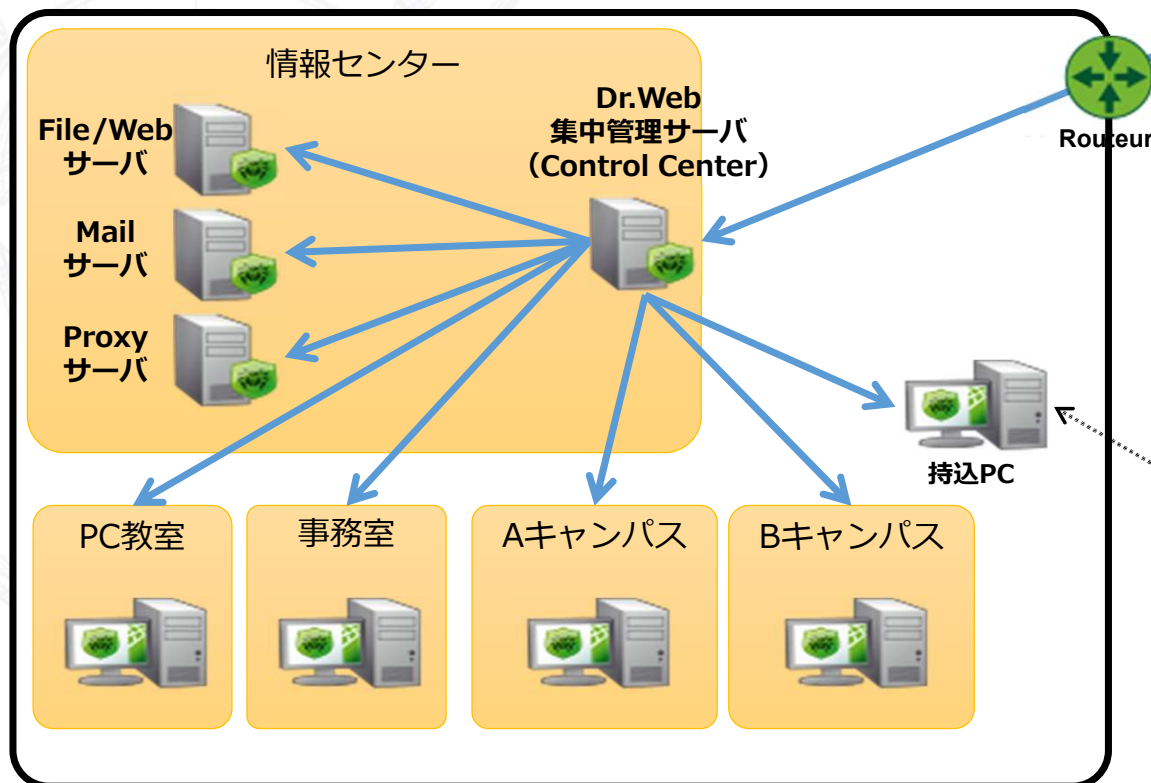
生徒、教員、職員皆様の自宅PC、Android端末でも利用できます。



© Doctor Web,
2021

学内全体のPCやサーバだけでなく、メール、WEBゲートウェイまで対応しています。（マルチOS対応）

◆大学ネットワーク



ユーザー数（学生、教員、職員数）で価格提示



<対応Product>

- ・ Dr.Web Desktop Security Suite
- ・ Dr.Web Server Security Suite
- ・ Dr.Web Mail Security Suite
- ・ Dr.Web Gateway Security Suite
- ・ Dr.Web Mobile Security Suite



学生、教員、職員皆様の自宅PC、Android端末でも利用できます。



www.drweb.com
www.drweb.co.jp



© Doctor Web,
2021

www.drweb.com