Dr.Web製品紹介

法人向け
エンドポイントセキュリティ

Dr.Web
Desktop
Security
Suite
(DSS)

株式会社Doctor Web Pacific

www.drweb.com

Dr.WEB®
Anti-virus

今回のテーマ

- 製品コンセプト
- 集中管理 Dr.Webサーバ構成
- 脅威からの保護機能
- 運用管理機能

Dr.WEB®
Anti-virus

製品コンセプト

株式会社Doctor Web Pacific

www.drweb.com

法人組織を取り巻くサイバーセキュリティの課題

課題①ランサムウェア被害 ランサムウェアの侵入経路	● ネットワークへの直接侵入 ● ダークウェブサイト
課題②進化するマルウェア EMOTET（マルウェア）	● ダークウェブサイトによる 亜種マルウェア開発
課題③新生活のマルウェア フィッシング詐欺	● テレワークが狙われている ● メールやサイトの対策

課題①　ランサムウェア被害

「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など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

課題①　ランサムウェア被害

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）】

WebサイトやITサービスへのリモートアクセスを販売するビジネスモデル

【Ransomware-as-a-Service（RaaS）】

ランサムウェアによる攻撃をサービスとして提供・実行するビジネスモデル

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②　進化するマルウェア

「EMOTET」とは？

EMOTET＝偽装メール経由で拡散するマルウェア

- 感染の手法：
  - **返信型 偽装（攻撃）メール**
  - WordなどOffice文書ファイルの**不正マクロ**
- 想定される被害：
  - 感染端末情報の盗難
  - 利用者の認証情報、メールクライアントの認証や受信メール情報など

    ⇒**更なる攻撃の踏み台化**
  - 他のマルウェアの感染

    ランサムウェア や**バンキング型トロイの木馬**など

    ⇒**アクセス権売買（Access-as-a-Service)**の可能性

2014年から存在し、
日々形を変え
進化しているマルウェアの1つ

課題②　進化するマルウェア

日々進化し、攻撃してくるマルウェアから負の連鎖を打ち切るには

EMOTETのように古くから存在するマルウェアの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マルウェア検知だけでは、亜種のマル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。

また一度EMOTETに感染すると、そこで盗まれた情報がダークウェブで売買され、二次的に複数のマルウェアを仕掛けられる恐れがあります。
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。

課題③　新生活のマルウェア

新型コロナウイルス流行以降、フィッシングサイト誘導数は過去最大

正規サイトに偽装したフィッシングサイトで、利用者を騙し、個人情報を詐取する

フィッシングサイト事例：

- 給付金や、賞品当選に便乗し当たサイト
- 公的機関を装ったサイト
- SNS上での不正な投稿

想定される被害：

- **IDやパスワードの詐取**（テレワークによるVPN接続IDなど）
- **口座情報・クレジットカード番号の詐取**（銀行口座やクレジットカード番号など）

課題③　新生活のマルウェア

テレワークで利用する端末を狙った攻撃

ビデオ会議アプリのインストーラーを偽装したマルウェアが多発

攻撃型メールを利用した事例：

- EMOTETを利用（発展型のマルウェア**「IcedID」**なども）
- ビジネスメール詐欺を利用

想定される被害：

- **IDやパスワードの詐取**（テレワークによるVPN接続IDなど）
- 端末乗っ取り（踏み台）による、**機密データ詐取**

課題③　新生活のマルウェア

持出端末をマルウェアから守るには・・・

テレワークのように、社外からアクセスすることが当たり前になりつつ
ある社会で、利用者個人個人のマルウェア対策の認識の向上が不可欠。
その上で、**不正サイト、不正メールへの対策**、ネットワーク内外における
脆弱性対策が必要となります。

そのような環境構築を**情報システム部門の皆様が手軽に運用できる**
各種対策が取れたアンチウイルスソフトが必要不可欠になります。

Dr.Webのコンセプト

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 • エクスプロイド防止

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 XP Service Pack 2以降 •Windows Vista　•Windows 7　•Windows 8 •Windows 8.1　•Windows 10 21H1以前 64ビットプラットフォーム： •Windows Vista Service Pack 2以降 •Windows 7　•Windows 8　•Windows 8.1 •Windows 10 21H1以前　•Windows 11
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

2023年7月現在
対応OS

システム要件 macOS

パラメータ	要件
端末	Mac running macOS operating system
ディスクの空き容量	2GB
OS	【Mac】 •macOS 10.12 Sierra •macOS 10.13 High Sierra •macOS 10.14 Mojave •macOS 10.15 Catalina •macOS 11.0 Big Sur •macOS 12.0 Monterey •macOS 13.0 Ventura

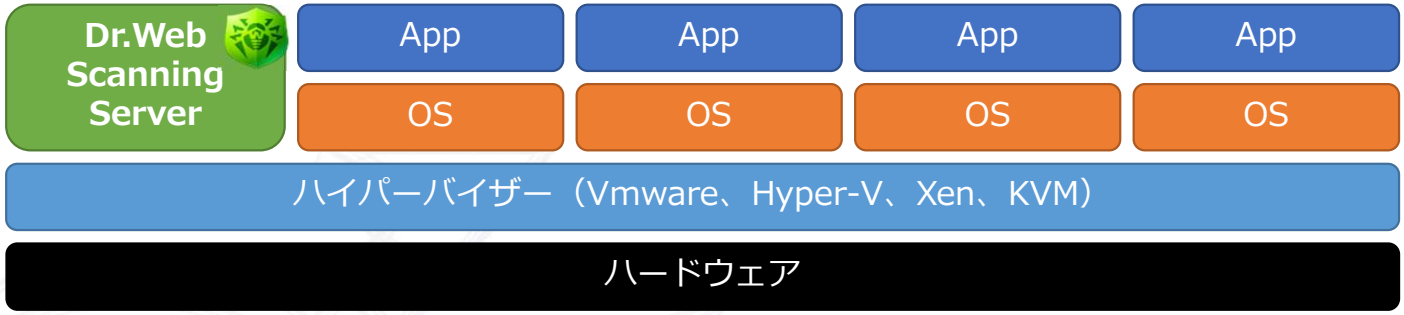
2023年7月現在
対応OS

システム要件 Linux

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ー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	PAM および glibc ライブラリのバージョン2.13以降を使用する、kernel バージョン2.6.37以降の Linux。

2023年7月現在
対応OS

仮想環境下でのスキャニング機能



Dr.Web Scanning Server　仕様	
OS	Linux、FreeBSD
CPU	•Intel／AMD 32ビット（IA-32、x86）および64ビット（x86_64、x64、amd64）
RAM	500 MB以上の空き容量（1 GB以上を推奨）
HDD	1 GB以上

- ファイルスキャンは全てScanning Server上で実行され、仮想環境下での各端末の負荷を軽減します。
- 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。

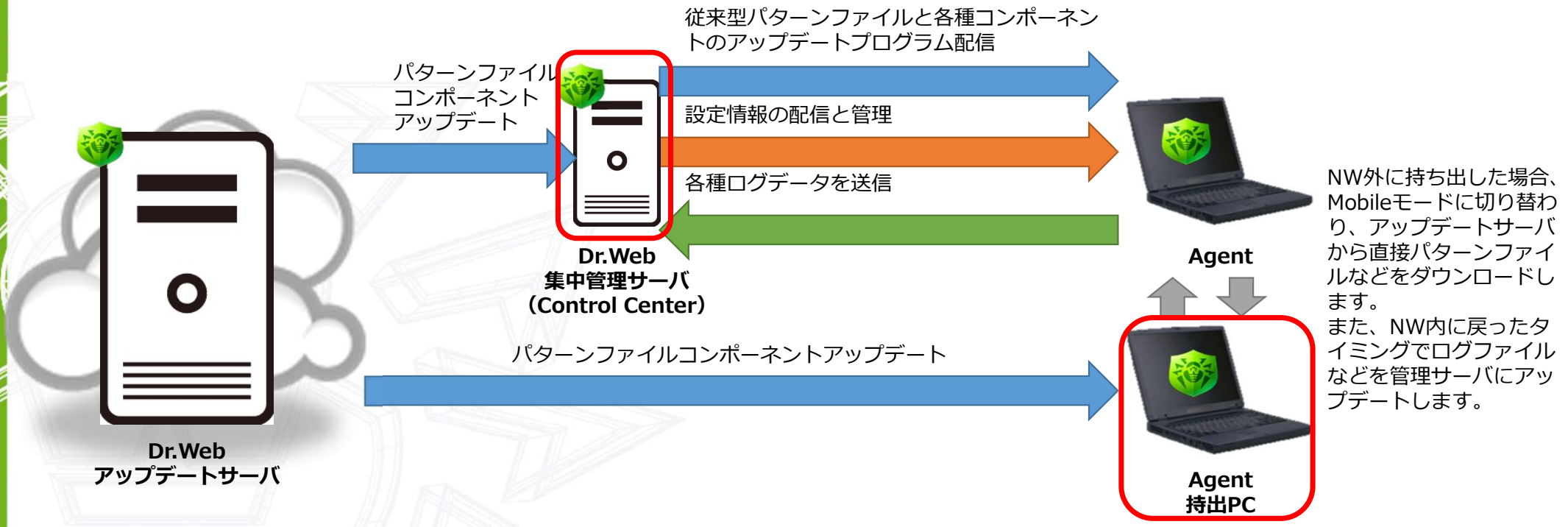
Dr.Web 集中管理サーバ構成

（Control Center）

株式会社Doctor Web Pacific

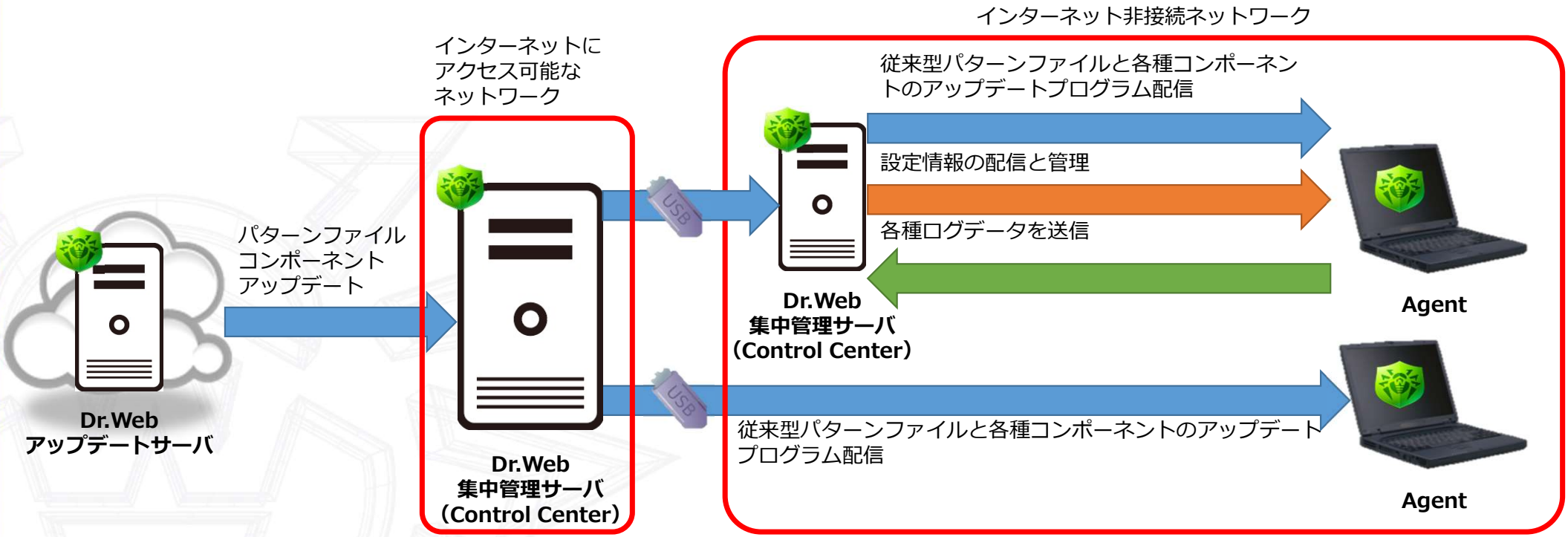
www.drweb.com

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ーベースは、管理するAgent数でご用意して頂くものが異なります。300Agent以下の場合は、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。

Dr.WEB®
Anti-virus

脅威からの保護機能

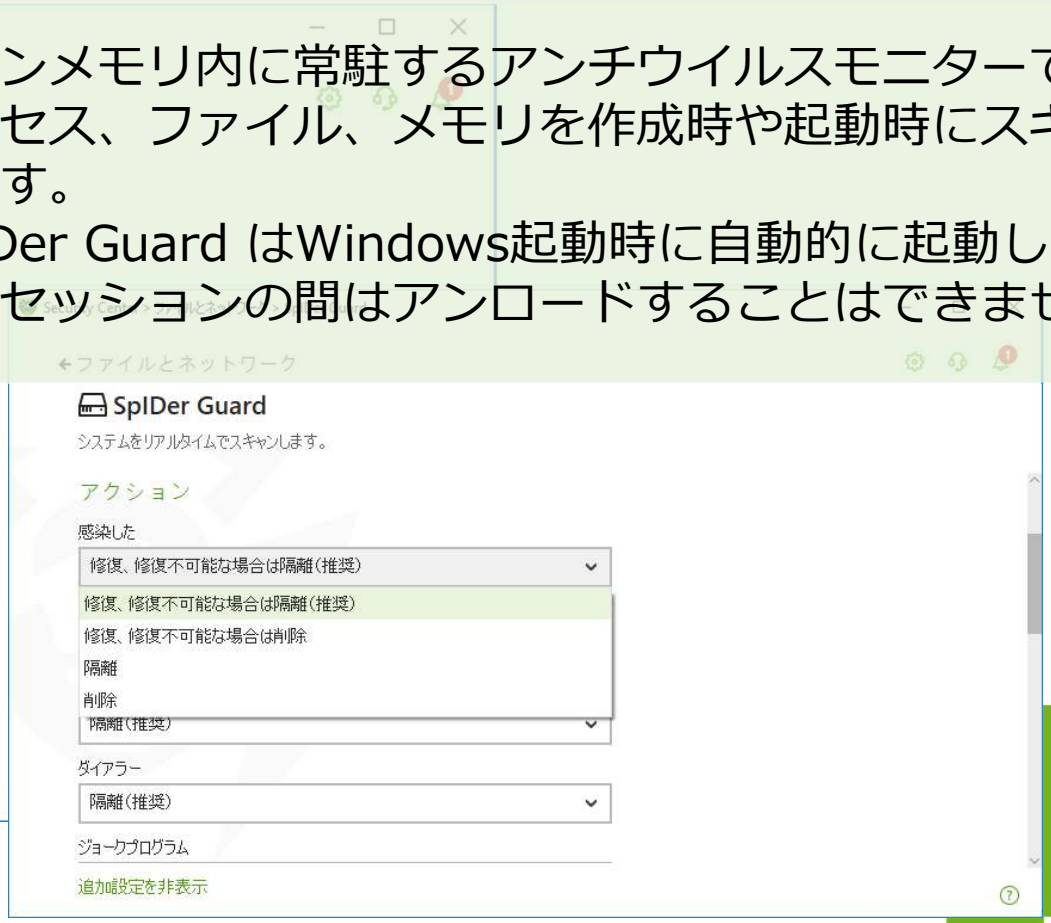
株式会社Doctor Web Pacific

www.drweb.com

保護コンポーネント

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 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。
SpIDer 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。

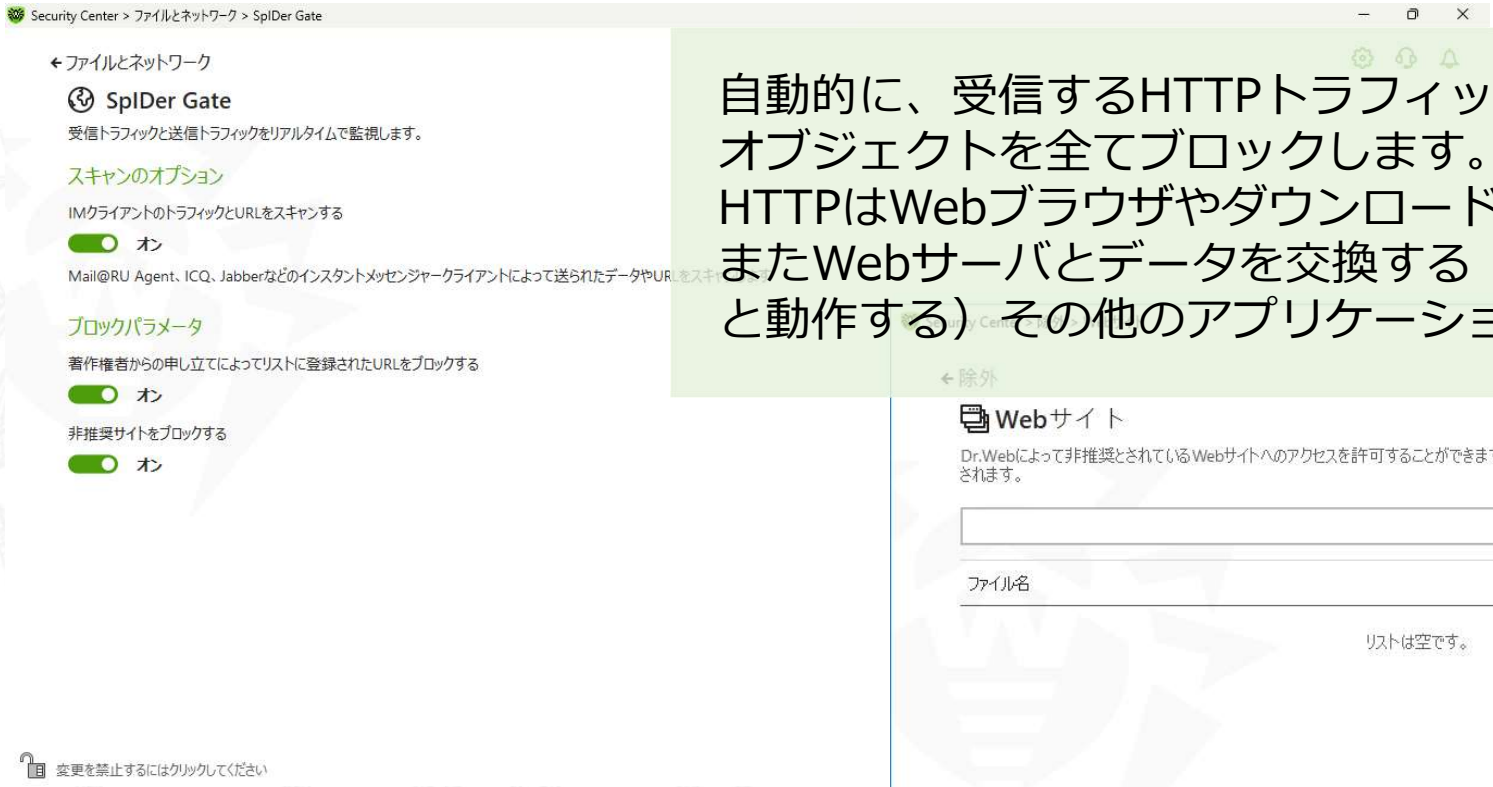
ファイルシステムのリアルタイム保護 SpIDer Guard



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。

Webトラフィックをチェックする SpIDer Gate



自動的に、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。
HTTPはWebブラウザやダウンロードマネージャによって、またWebサーバとデータを交換する（すなわちインターネットと動作する）その他のアプリケーションによって使用されます。

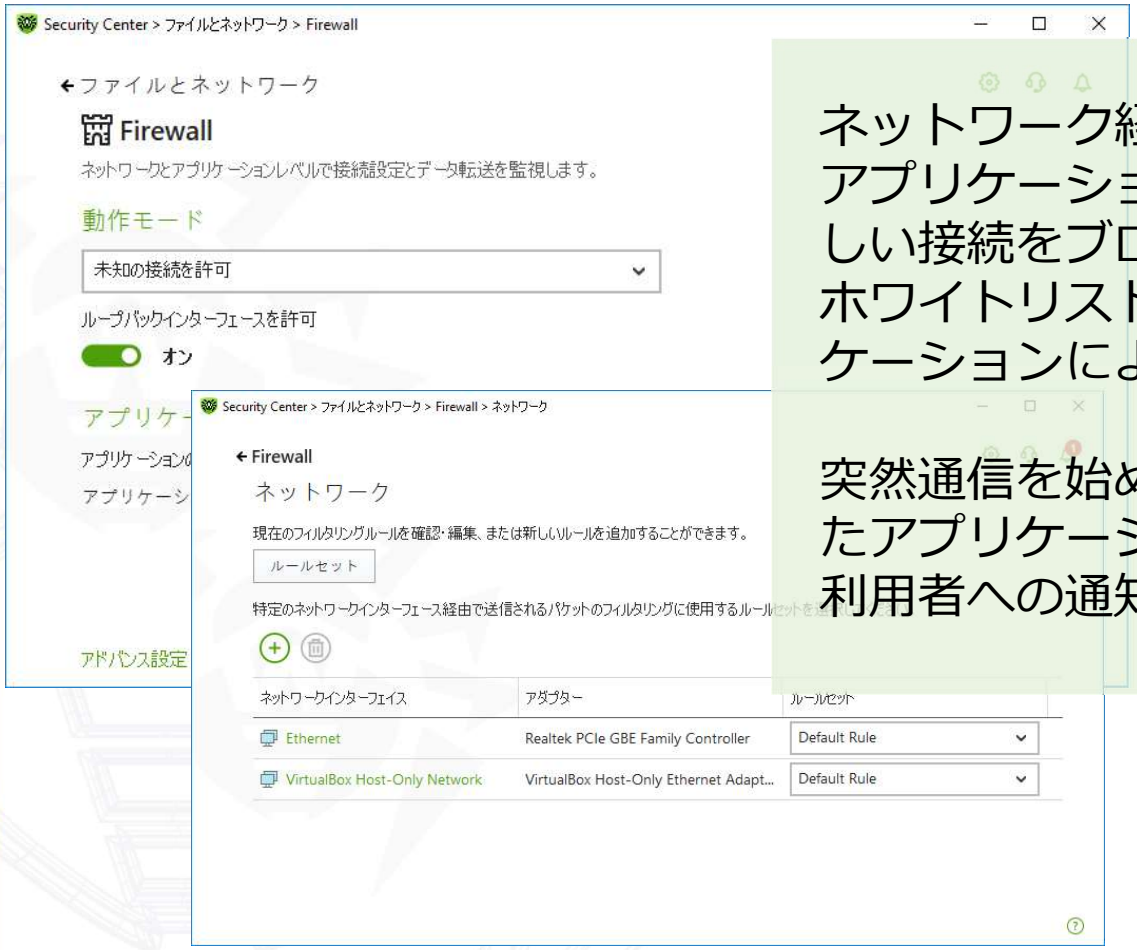
※初期では各端末での設定は出来ません。
管理サーバ（Control Center）にて、設定が行えます。

メールスキャン SpIDer Mail

デフォルトでインストールされるアンチウイルスメールスキャナ。システムの起動と同時に自動的に起動。
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。

※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。

パーソナルファイアウォール Dr.Web Firewall



ネットワーク経由で重要なデータが漏洩するのを防ぎます。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。
ホワイトリストへ登録されている物を除き、全てのアプリケーションによる通信と利用ポートを監視します。

突然通信を始めた登録外のアプリケーションや、登録されたアプリケーションの通信ポートが変更した場合などに、利用者への通知や通信の制御を行います。

※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。

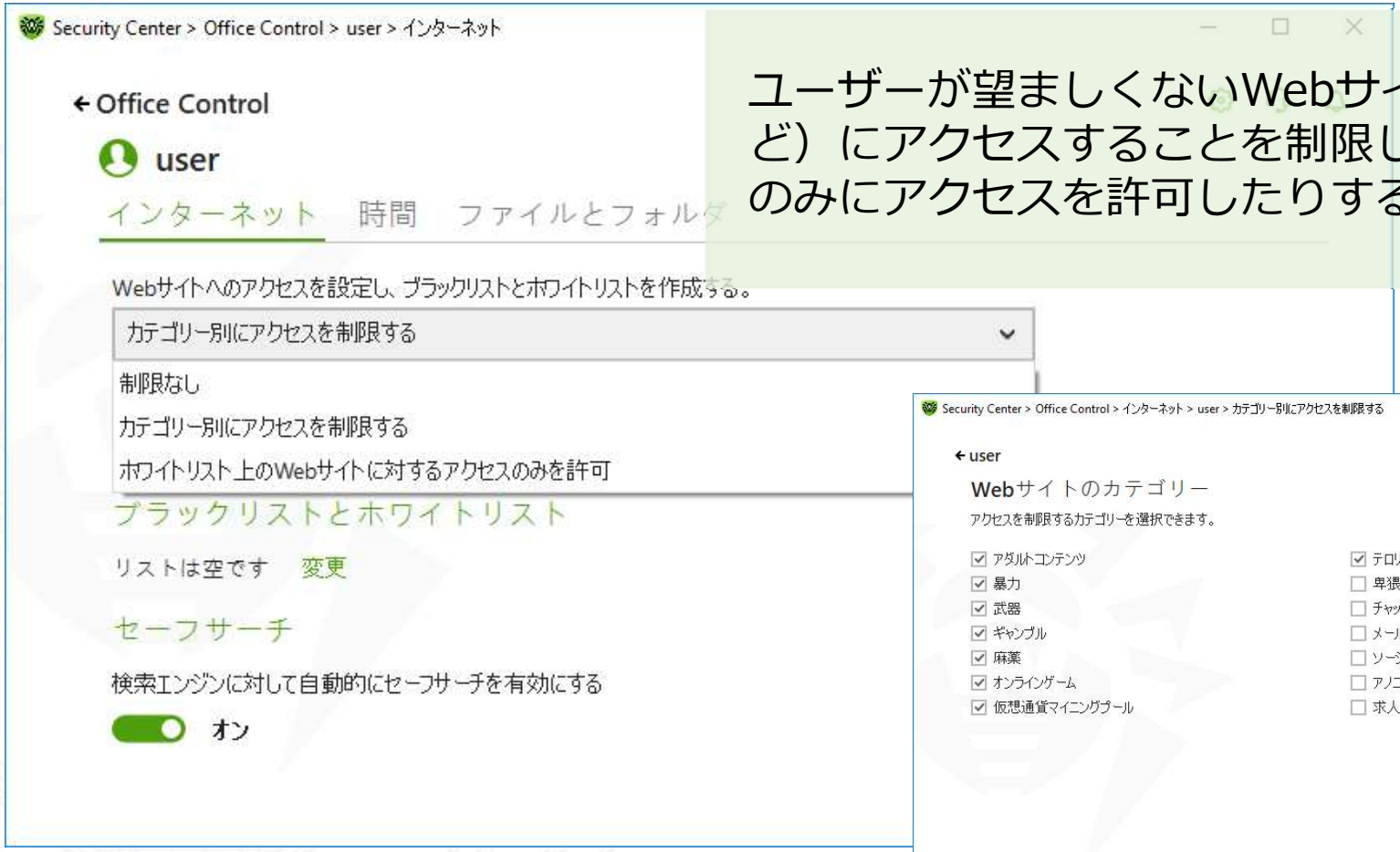
デバイスコントール Office Control

データの流出を防ぐ機能（Windows）

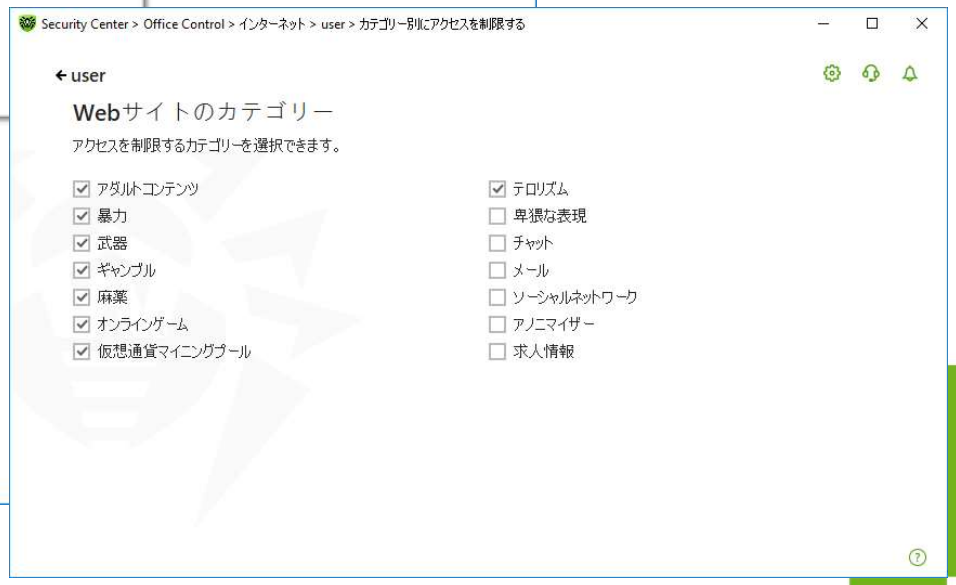
PC単位やグループ単位で、PCに接続する外部デバイスの利用を制限します。
特定のデバイスのみ利用可能といったホワイトリスト運用も可能です。
接続デバイスを経由した情報漏えいを防止することが可能です。

※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。

簡易フィルタリング機能 Office Control



ユーザーが望ましくない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したりすることができます。



※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。

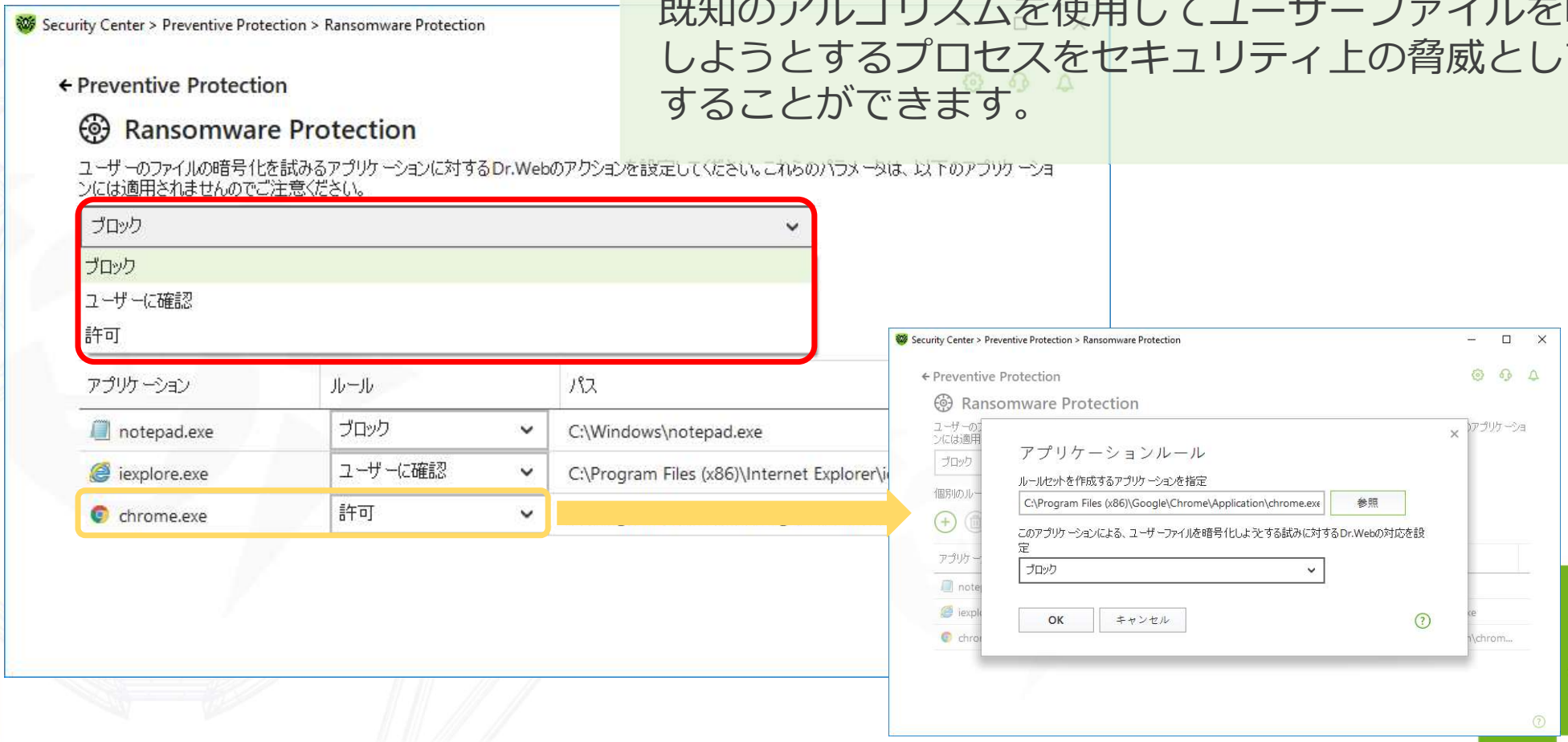
ふるまい検知（予防的保護）動作解析

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。

※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。

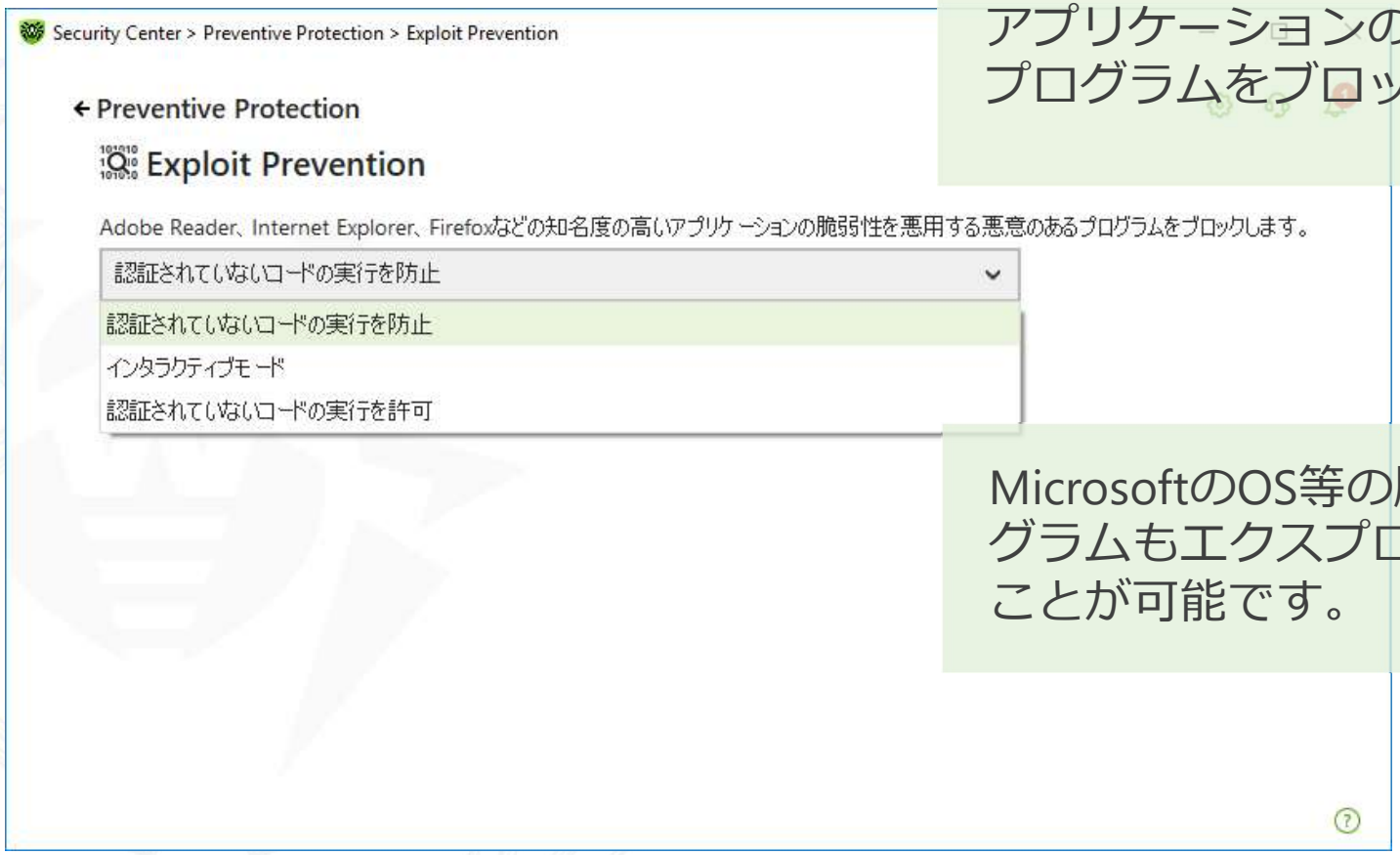
ふるまい検知（予防的保護）ランサムウェア保護

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。



※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。

手動スキャン Scanner

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。

Dr.WEB®
Anti-virus

運用管理機能

株式会社Doctor Web Pacific

www.drweb.com

統計情報の確認

脅威情報

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	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。

端末ステータスの確認

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。

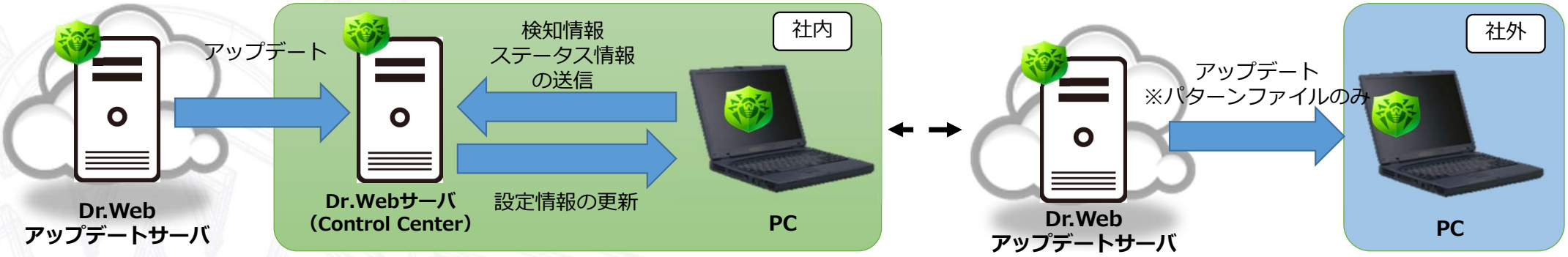
コンポーネントが最新であれば、ふるまい検知で多くの未知の脅威を検知可能

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	0825dokutauebu-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	0825dokutauebu-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

PC持ち出し時の運用

お使いの端末を社外に持ち出し、Dr.Webサーバ（ControlCenter）に接続できない状態の場合、Mobileモードを使用して、Dr.Web アップデートサーバから直接更新(パターンファイルのみ)を受け取ることが出来ます。
また、集中管理サーバに接続した際に、脅威の検知情報等は集中管理サーバに送信され、各種データを管理することが出来ます。

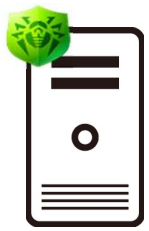


項目	Control Center版	スタンドアロン版
脅威の検知情報等	Control Center にて確認可 ※Control Centerへの接続が必要	各端末で確認
設定の変更	Control Center で設定可 ※Control Centerへの接続が必要	各端末で設定
アップデート	Control Center接続時：Control Centerから取得 Control Center非接続時：Dr.Webアップデートサーバからパターンファイルのみ取得	Dr.Webアップデートサーバから取得
ライセンスの更新	Control Center で更新	各端末で更新

アップデートの仕組み

Dr.Web
アップデートサーバ

パターンファイル・コンポーネント
アップデート



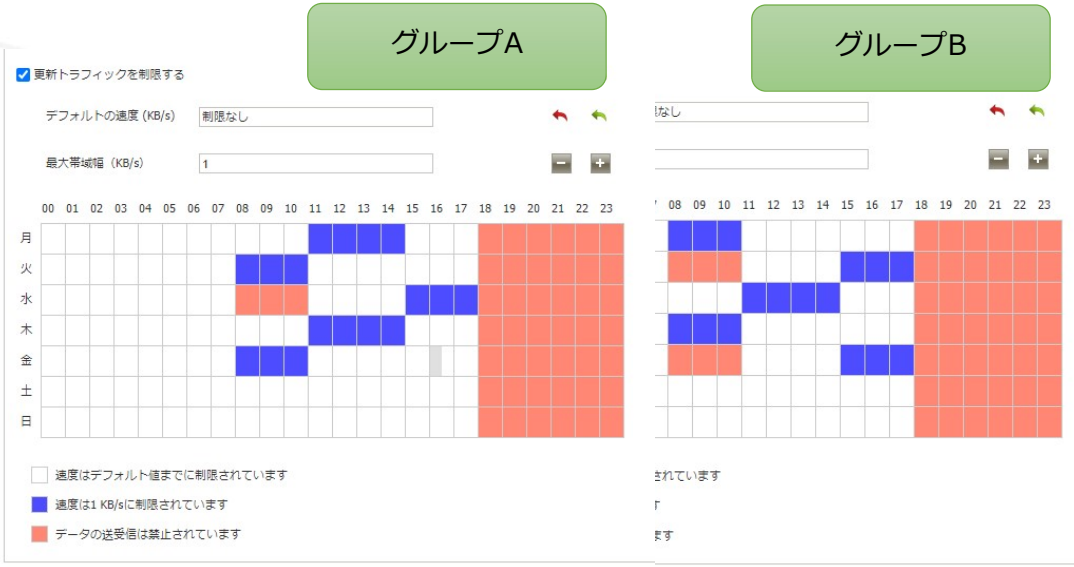
Dr.Web
集中管理サーバ
(Control Center)

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へのアップデータ送信は、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

差出人 [redacted] ☆　　返信　全員に

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 [redacted]

ソース : SpIDer Guard for Windows workstations (t350-PC\t350:t350-PC\None)

オブジェクト : C:\Users\[redacted].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。

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

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インストーラを配布頂く方法があります。

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。

Dr.WEB®
Anti-virus

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