Dr.Web Mobile Security Suite（MoSS）
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SpIDer 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、アンチウィルス『Dr.WEB』の製品とサービスを約5,000を超す団体に販売。
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。
マルウエアの検出・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を超す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

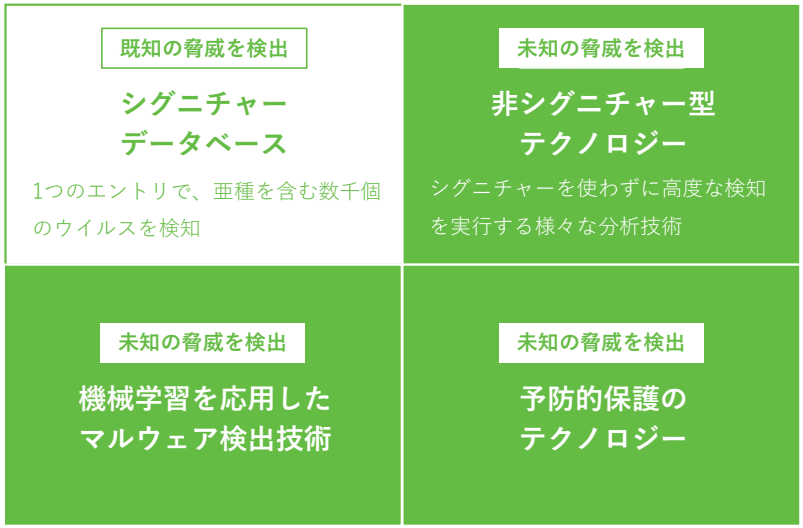
Dr.Webで 快適
最適化された機能群。
使いやすさによる運用コストを低減

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 Androidに特化した製品

point 2 全世界で1億6千万ダウンロード

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



MoSS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

コンポーネント	説明
Anti-virus機能 SplDer Guard	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。
Anti-virus機能 Scanner	ユーザが任意タイミングでスキャンを行います。
Anti-theft	紛失や盗難された場合にモバイルデバイスを探し出し、必要な場合にはリモートから機密情報を消去することができます。
URL フィルター	ウイルスデータベースの状態を問わずに望ましくないWebサイトへのアクセスを制御します。
Security Auditor	デバイスのセキュリティ上の問題を検出し、問題および脆弱性に対応するソリューションを提供します。
Parental Control	不正アクセスからアプリケーションを守るほか、アンチウイルス設定の第三者による変更を防止します。
通話およびSMSフィルター	不要な通話やSMSをブロックします。
Firewall	アプリケーションのネットワークアクティビティを監視します。

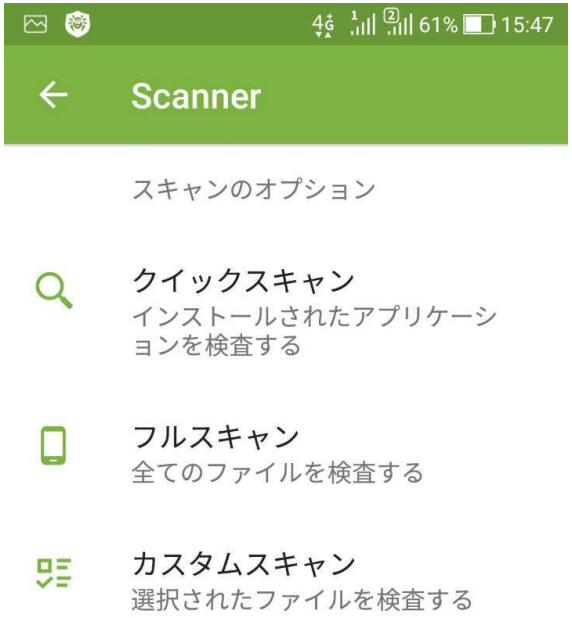
保護機能「Anti-virus機能SpIDer Guard 」：リアルタイム保護

リアルタイムで端末を監視し脅威を検出します

SpIDer Guard は、アプリケーションを閉じてもファイルシステムを保護し続けます。

保護機能「Anti-virus機能Scanner」：手動スキャン

ファイルシステムのオンデマンドスキャンを行うことができます



【スキャナ機能】

「クイックスキャン」

▶ インストールされたアプリをチェック

「フルスキャン」

▶ 全てのファイルをチェック

「カスタムスキャン」

▶ ユーザー指定のオブジェクトをチェック

保護機能「Anti-theft」：紛失、盗難時にデバイスをロック

紛失、盗難にあった場合にデバイスの機能をロックしたり位置情報を検出りすることが可能です

「再起動後ロック」

▶ デバイスを再起動するたびにDr.Web Anti-theftでデバイスをロックします。

「SIMカード変更時ロック」

▶ 信頼するリストにないSIMカードを検出するとデバイスをロックします。

また、登録されているお友達にSMSメッセージを送信することも可能です。

「データ削除」

▶ パスワードを10回間違えると、すべてのアプリケーションをアンインストールし、連絡先、メッセージ、写真、動画などの個人情報を削除します。

保護機能「URL フィルター」：Webサイトへのアクセス管理

望ましくないインターネットサイトへのアクセスを制御します

「Webサイトのカテゴリー」

▶ アクセスを制限する特定のWebサイトのカテゴリーを選択できます。

「ブラックリストとホワイトリスト」

▶ アクセスを制限または許可するWebサイトのリストを設定できます。

制限されるカテゴリー

- 非推奨サイト
- 暴力
- ギャンブル
- 卑猥な表現
- テロリズム
- ソーシャルネットワーク
- 著作権者からの申し立てにより追加されたURL
- 仮想通貨マイニングプール
- アダルトサイト
- 武器
- 麻薬
- オンラインゲーム
- Eメール
- チャット
- アノニマイザー

保護機能「Security Auditor」：デバイスのセキュリティの問題を検出

デバイスのセキュリティを診断し、検出された問題と脆弱性を解決します

「脆弱性」

▶ 検出された脆弱性を表示します。

「システム設定」

▶ デバイスのセキュリティに影響する次のシステム設定を検出し、表示します。

❶USBデバッグが有効

❷未知のソースからのアプリケーションのインストールが有効

❸Dr.Web通知がブロック

❹ユーザーのルート証明書がインストール

保護機能「Parental Control」：アクセス制限機能

デバイスにインストールされている全てのアプリケーションのアクセスを制限できます

「アプリケーション」

▶ デバイスにインストールされている全てのアプリケーションへのアクセスを制限が設定できます。

「コンポーネント」

▶ アクセスを制限できるDr.Webコンポーネントの設定ができます。

保護機能「通話およびSMSフィルター」：通話、SMSのブロック機能

不要な通話やSMSメッセージをブロックすることができます

「ブラックリスト」

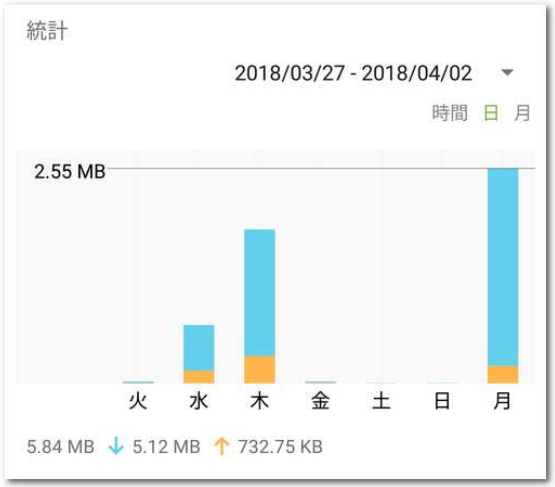
▶ 通話やSMSメッセージを受信しない電話番号のリスト登録できます。

「プロファイル」

▶ 通話とSMSメッセージをフィルタリングするカスタムプロファイルを作成できます。

保護機能「Firewall」：パーソナルファイアウォール

不正アクセスからデバイスを守り、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



「トラフィック」

▶ 現在のインターネット接続に関する情報を表示します。

「アプリケーション」

▶ ネットワークでやり取りされたデータ量の合計や送受信データ量を表示します。

「アプリケーション設定」

▶ インターネットトラフィックの統計をグラフ表示

運用管理機能：統計情報の確認

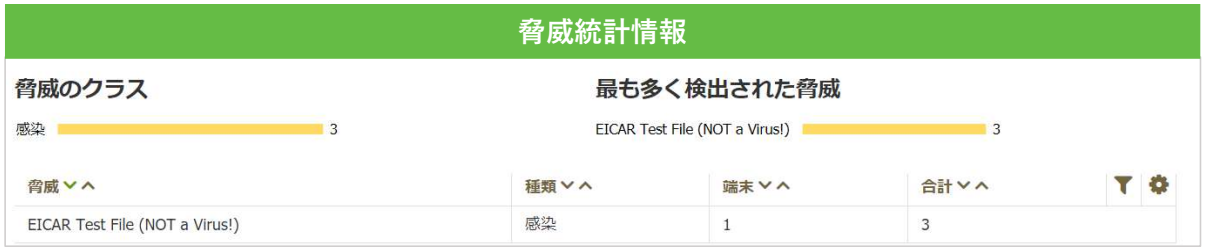
各端末のマルウェア検出情報をControl Center（集中管理サーバ）で確認することが可能です。

➢ 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。



運用管理機能：端末ステータスの確認

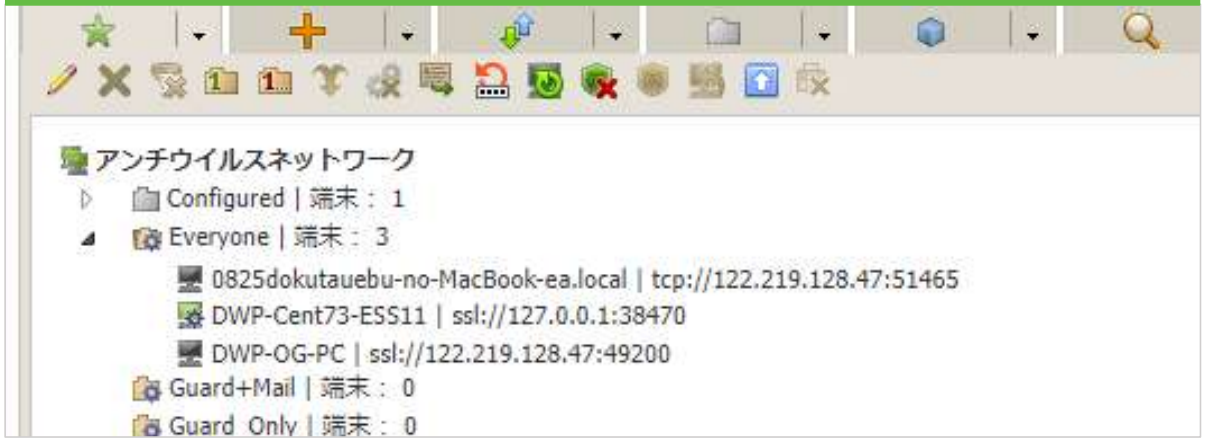
各端末のステータスは、リアルタイムにControl Center（集中管理サーバ）で視覚的に表示することが可能です。

※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

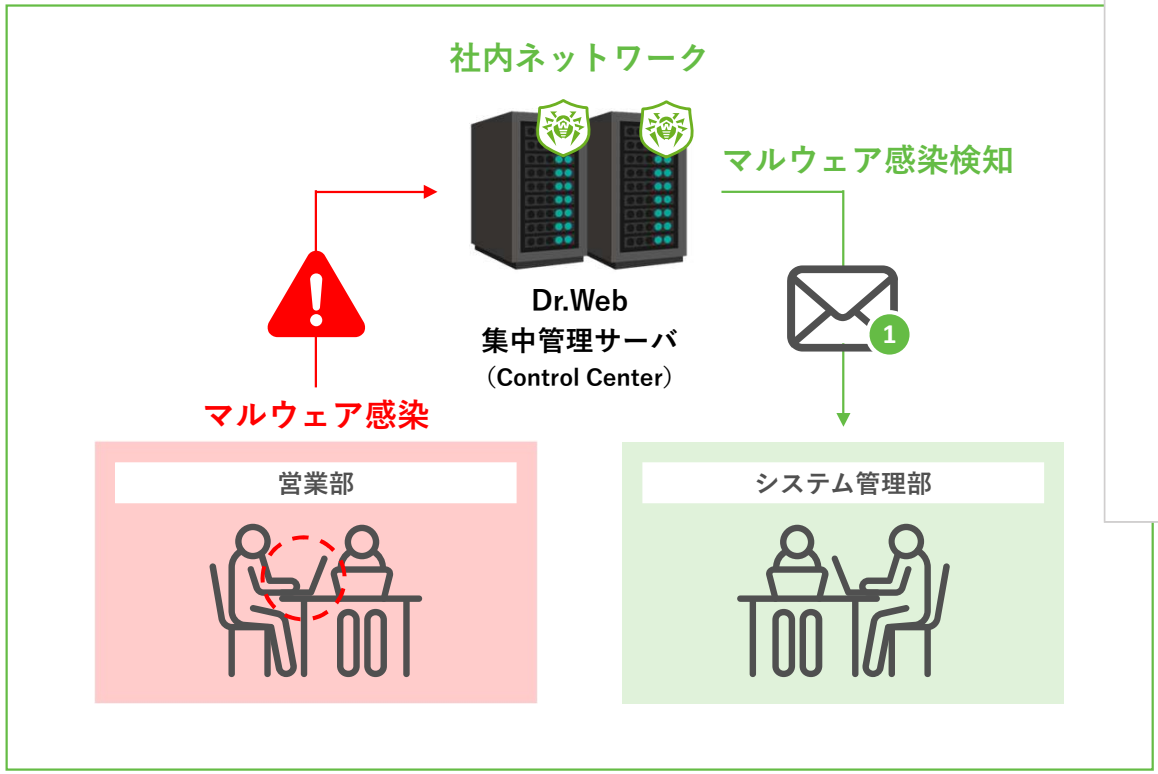


ステータス情報

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

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！○○端末上で脅威が駆除されました**
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 Android
(t350＼ t350:t350＼None)
オブジェクト：storage/emulated/aaaaa.tmp(未知)
脅威：EICAR Test File(NOT a virus!)
アクション：駆除

システム要件と導入事例

システム要件

パラメータ	要件
オペレーティングシステム	Androidバージョン4.4～ Android TV（TVセット、メディアプレーヤー、ゲームコンソール）
CPU	x86/x86-64/ARM7/ARM8
RAM空き容量	512 MB以上
デバイスの空き容量	45 MB以上（データストレージ用）
画面解像度	800×480以上
その他	インターネット接続（ウイルスデータベースの更新用） Android TVを実行しているデバイスでは、集中管理モードを使用することはできません

導入事例①

NX情報システム株式会社 様

Android端末数	15,000台

日通の宅配ドライバーが利用するモバイル端末に、Dr.Web Mobile Security Suiteを採用。
アンチウィルスだけでなく、盗難・紛失対策や、Webフィルタリングなどのセキュリティ機能が搭載されていることが重要な要件であった。全世界のAndroid向けアンチウィルスにおいて豊富な導入実績を持っていることが採用の決め手となった。

point 1

充実した機能

盗難した際のロック機能、マルウェアにより端末ロックされた際の解除機能、Webフィルタリング等必要な機能が漏れなく搭載されており、
カスタマイズ不要であった。

point 2

安定稼働

長く培ったAndroid向け製品のノウハウが活かされ、機種固有の問題や他社アプリとの競合がなく、
安定した稼働を実現出来た。

導入事例②

さつき株式会社 様

Android端末数	23,112台

（2024年5月末現在）

インクルーシブ電子黒板”MIRAI TOUCH” にDr.Web Mobile Security Suiteを採用。
全国の教育機関向けに電子黒板”MIRAI TOUCH”提供されています。GIGAスクール構想以降、ネットワークが整備された。同時に各自治体においてセキュリティ対策も重要視されるようになり、安心してご利用いただけるよう、今回の採用に至りました。

point 1

稼働実績

Android OSでの稼働実績が高く、Google Playで1億6000万ダウンロードの実績が採用理由になりました。

point 2

技術支援体制

プリインストール及び標準搭載を前提に協業でき、デバイスやOSの特性に応じて、ソフトウェアを柔軟にチューニングできる支援体制を提供いただけた。

今後とも宜しくお願い致します。

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