Dr.WEB®
Anti-virus

プロダクト概要説明資料

Dr.Web Mail Security Suite (MSS)
Dr.Web Gateway Security Suite (GSS)

株式会社Doctor Web Pacific

www.drweb.com

はじめに

- **本資料について**
  - 本資料は、Dr.Web Enterprise Security Suite（以下ESS）シリーズの製品である、Dr.Web Mail Security SuiteとDr.Web Gateway Security Suiteの機能説明資料です。
  - 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、2022年1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 Mail Security Suite・・・MSS
  - Dr.Web Gateway Security Suite・・・GSS
  - Control Center・・・CC
  - ネットワーク・・・NW

改訂履歴

版数	改訂日	内容
第1版	2021/04/01	第1版として公開
第2版	2022/10/01	Dr.Web Premium サブスプリクション サービスへの名称変更対応

MSS/GSS

製品コンセプト

株式会社Doctor Web Pacific

www.drweb.com

マルウェアの侵入経路をブロック

課題①標的型攻撃メール	● 添付ファイルなどの開封時に感染 ● 情報漏洩元や遠隔操作される端末になる危険
悪意のあるメール	

Dr.Web Mail Security Suiteで、メールサーバ内で攻撃メールの駆除が可能です。

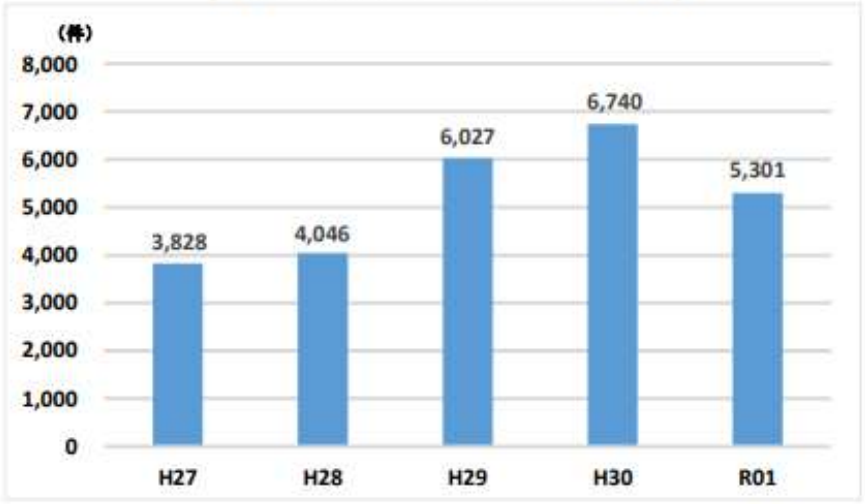
課題②フィッシングサイト	● 本物そっくりの偽サイトへ誘導 ● IDやパスワードなどの情報を詐取
詐欺サイト	

Dr.Web Gateway Security Suiteで、プロキシサーバ上でフィッシングサイトをブロックします。

課題①　標的型攻撃メール

多くのマルウェア感染はメールから！！

【図表４　標的型メール攻撃の件数の推移】



引用：警視庁「令和元年におけるサイバー空間をめぐる脅威の情勢等について」

2020年は標的型攻撃メールの「Emotet」が再流行し、

猛威を振いました。

課題②フィッシングサイト

知らず知らずにのうちに、企業の情報を搾取！！

ICAP
各種プロキシー製品と連携するプロトコル。
URLフィルター製品などプロキシーサーバがサポートしています。

※C&C（Command&Control）サーバとは※
マルウェアに感染してボットと化したコンピュータ群（ボットネット）に指令（command）を送り、制御（control）の中心となるサーバーのことである。

2020年は、テレワークなどの働き方に関する変革期になる年でした。
それに伴い、犯罪者は機密情報（IDおよびパスワードなど）を搾取するため、不正なサイトへ誘導します。

Dr.WEB®
Anti-virus

MSS/GSS

メリット

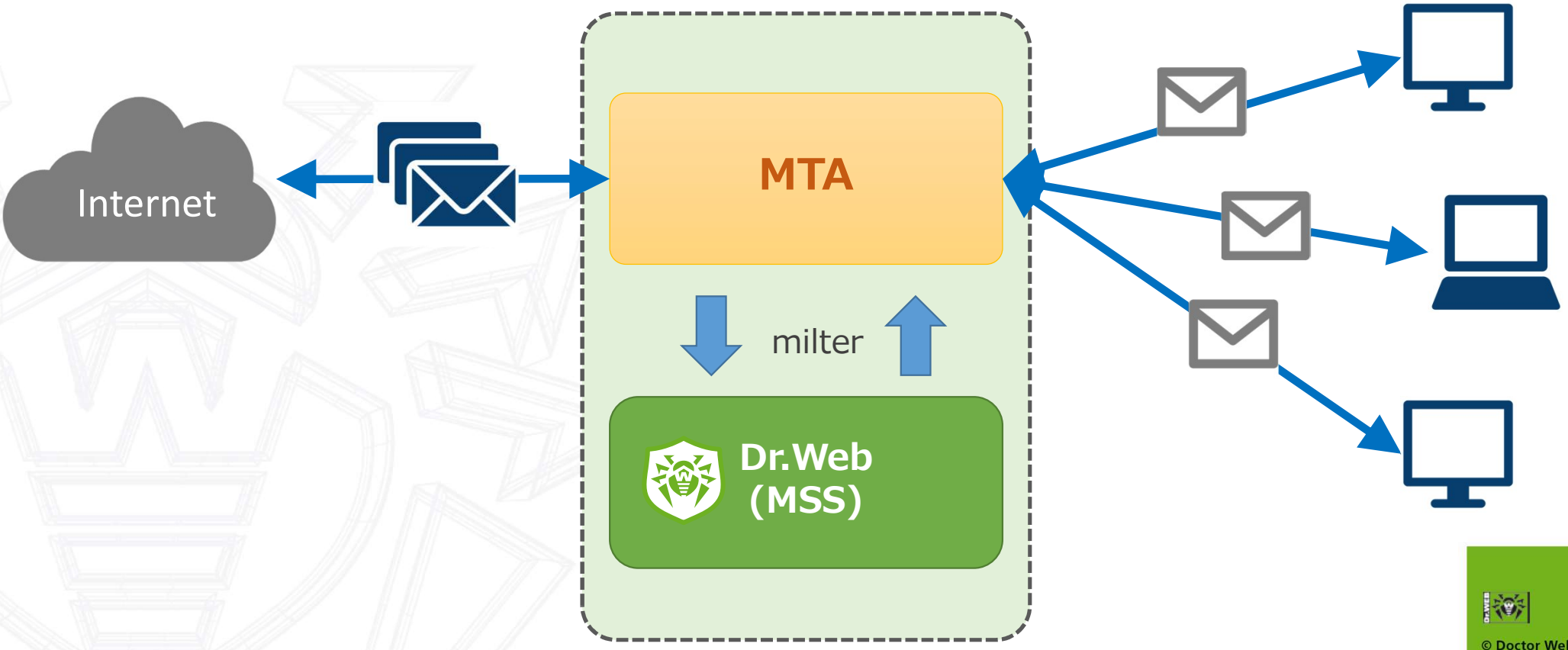
株式会社Doctor Web Pacific

www.drweb.com

MSS のメイン機能

No.	メイン機能	内　　容
1	脅威の検出と駆除	悪意のあるプログラムや不要なソフトウェアを検索します。 脅威の検出方法： ①シグネチャ解析 ②ヒューリスティック解析 ③クラウドベースの脅威検出テクノロジー
2	メールメッセージのスキャン	メールサーバー（MTA）とMilterを介して接続し、送受信されるメールをスキャンします。
3	スクリプトを使用した脅威等を含むメールへの処理の指定	以下のような設定ができます。 ・脅威を含むメールに対する処理の指定(拒否、圧縮、許可) ・メール本文内のURL(の該当するカテゴリ)を元にした処理の指定(拒否、圧縮、許可) ・スパムに該当するメールに対する処理の指定(拒否、圧縮、許可) ・スパムの閾値の設定 ・無条件で受信を拒否(許可)する送信元メールアドレスの指定 など。
4	データベースの自動更新	スキャンエンジン、ウイルスデータベース、Webリソースカテゴリーのデータベース、メールスパムフィルタリングのルールなどのデータベースを自動更新(初期設定では30分毎に実施)します。

MSS の動作イメージ



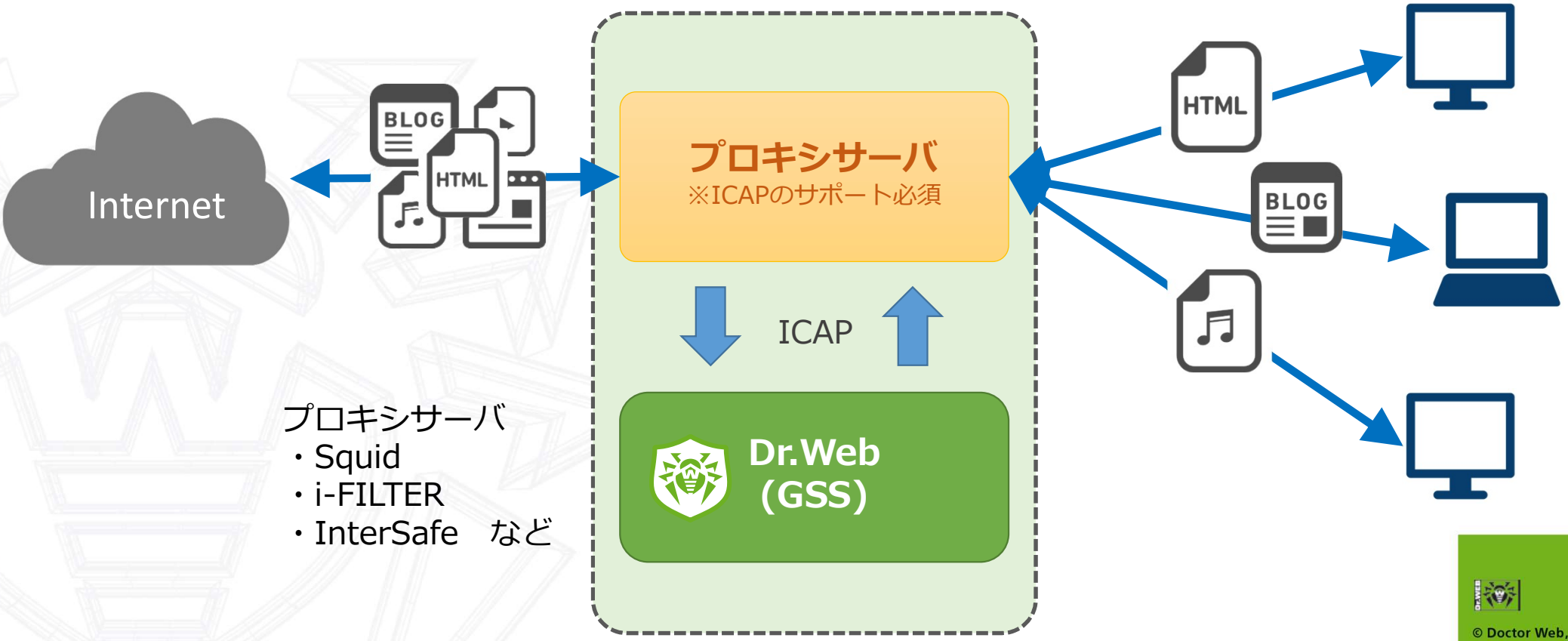
UNIXメールサーバ
※MTAとDr.Web(MSS)が動作

GSS のメイン機能

No.	メイン機能	内容
1	脅威の検出と駆除	悪意のあるプログラムや不要なソフトウェアを検索します。 脅威の検出方法： ①シグネチャ解析 ②ヒューリスティック解析 ③クラウドベースの脅威検出テクノロジー
2	インターネットに送信されたデータの分析	ユーザーから送信されるリクエストおよびリクエストに対するサーバーのレスポンスを監視します。送受信されるデータを分析するために、ICAPプロトコル経由でプロキシサーバの外部フィルターとして接続し、ローカルネットワークユーザーのHTTP接続を処理します。さらに、Webリソースカテゴリーのデータベースを使用したURLフィルタリングを利用できます。
3	データベースの自動更新	スキャンエンジン、ウイルスデータベース、Webリソースカテゴリーのデータベース、メールスパムフィルタリングのルールなどのデータベースを自動更新(初期設定では30分毎に実施)します。
4	集中管理モードでの動作	Windows10等のクライアントPCと同様に集中管理サーバーに接続した運用が可能です。 複数のGSSを運用する場合、保護されたネットワーク内のコンピューターに統一されたセキュリティポリシーを実装することができます。

※HTTPSの場合は、アクセス先URLのカテゴリに基づくフィルタリングが可能です。

GSS の動作イメージ



プロキシサーバ
・Squid
・i-FILTER
・InterSafe　など

UNIXプロキシサーバ
※Dr.Web(GSS)が動作

Dr.Webのゲートウェイ(MSS/GSS)対策を行うと…

ゲートウェイ全体	・端末に到着する前にマルウエアを検知・駆除 ・入口対策の強化
MSS	・メールサーバ内でメールアドレスごとに標的型メールを駆除 ・意図しない送信メールに添付されたマルウエアを駆除
GSS	フィッシングサイトへのアクセスをプロキシサーバー上でブロック

多層防御で未知のマルウエアをシャットアウト！

Dr.WEB®
Anti-virus

MSS/GSSが提供する

脅威からの保護機能

株式会社Doctor Web Pacific

www.drweb.com

MSS/GSS 基本アンチウイルスコンポーネント

コンポーネント	説明
Dr.Web Virus-Finding Engine	ウイルスと悪意のあるプログラムを検出するアルゴリズムを実装したスキャンエンジンです。
Dr.Web Scanning Engine	ファイルやブートレコード内のウイルスやその他の悪意のあるオブジェクトをスキャンします。
Dr.Web File Checker	ファイルとディレクトリをスキャンします。
Dr.Web Ctl	OSのコマンドラインからMSSやGSSの設定・管理を行うユーティリティです。
Dr.Web HTTPD	MSSやGSSを設定・管理するWebインターフェースです。
Dr.Web ES Agent	集中管理サーバーとの接続を行います。集中管理サーバーに接続すると、集中管理サーバー上で設定等を管理できるようになります。

MSS 脅威検索コンポーネント

コンポーネント	説明
Dr.Web MailD	メールのスキャンを行い、悪意のあるコンテンツの検出（添付ファイルだけでなく望ましくないWebサイトへのリンクも含む）を行えます。 スクリプトを使用して、悪意のあるコンテンツを含むメールに対する処理やDr.Web Anti-Spamにより算出されるスパムスコアに基づく処理の指定等ができます。
Dr.Web Anti-Spam	メールにスパムメールによくみられる特徴が含まれるかを解析しスコア化するコンポーネントです。
SpIDer Gate	ネットワークトラフィックとURLを監視するためのコンポーネントになります。

GSS 脅威検索コンポーネント

コンポーネント	説明
Dr.Web ICAPD	ICAPサーバ機能を提供するコンポーネントです。ICAPクライアントであるHTTPプロキシサーバー(Squidなど)と接続します。 Dr.Web ICAPDは、プロキシサーバーの外部フィルターとして使用され、ユーザーのリクエストとこれらのリクエストに対するサーバーのレスポンスを解析します。
SpIDer Gate	ネットワークトラフィックとURLを監視するためのコンポーネントです。

MSS/GSS 設定方法

株式会社Doctor Web Pacific

www.drweb.com

設定・管理の方法

MSS/GSSは以下の方法で、設定・管理を行うことができます。

1. コマンドラインユーティリティ(drweb-ctl)

2. 専用Webインターフェース

3. Control Center

尚、Webインターフェースは、MSS/GSSと共にインストールされ、Webmin等のアプリケーションを追加する必要はありません。また、Control Centerを使用する場合には、別途集中管理サーバを構築する必要があります。
※集中管理モードでは、3のみ利用可能です。

Dr.Web MSS/GSS システム要件

コンポーネント	要件
プラットフォーム	以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	1GB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

※OSによっては、利用できない機能が有ります。

Dr.WEB®
Anti-virus

その他 ESS 製品群

株式会社Doctor Web Pacific

www.drweb.com

Dr.Web ソリューションマップ

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 Premium サブスプリクション 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）

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プロキシー	**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 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 サブスプリクションサービス**	Windows Linux macOS	欧州・ロシア初のクラウド型 アンチウイルス

Dr.WEB®
Anti-virus

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