Dr.Webを活用した
「新しいランサムウェア対策」

株式会社Doctor Web Pacific

www.drweb.com

ランサムウェア対策のポイント

複数のアンチウイルスで検知　→　セカンドオピニオンの活用

静的スキャンでは不十分。動的スキャン（ふるまい検知）で検知

古いOSの脆弱性対策

万が一の場合の救済手段は？

アンチウイルス自体が脆弱性にならないか？

アンチウイルスにおけるセカンドオピニオン

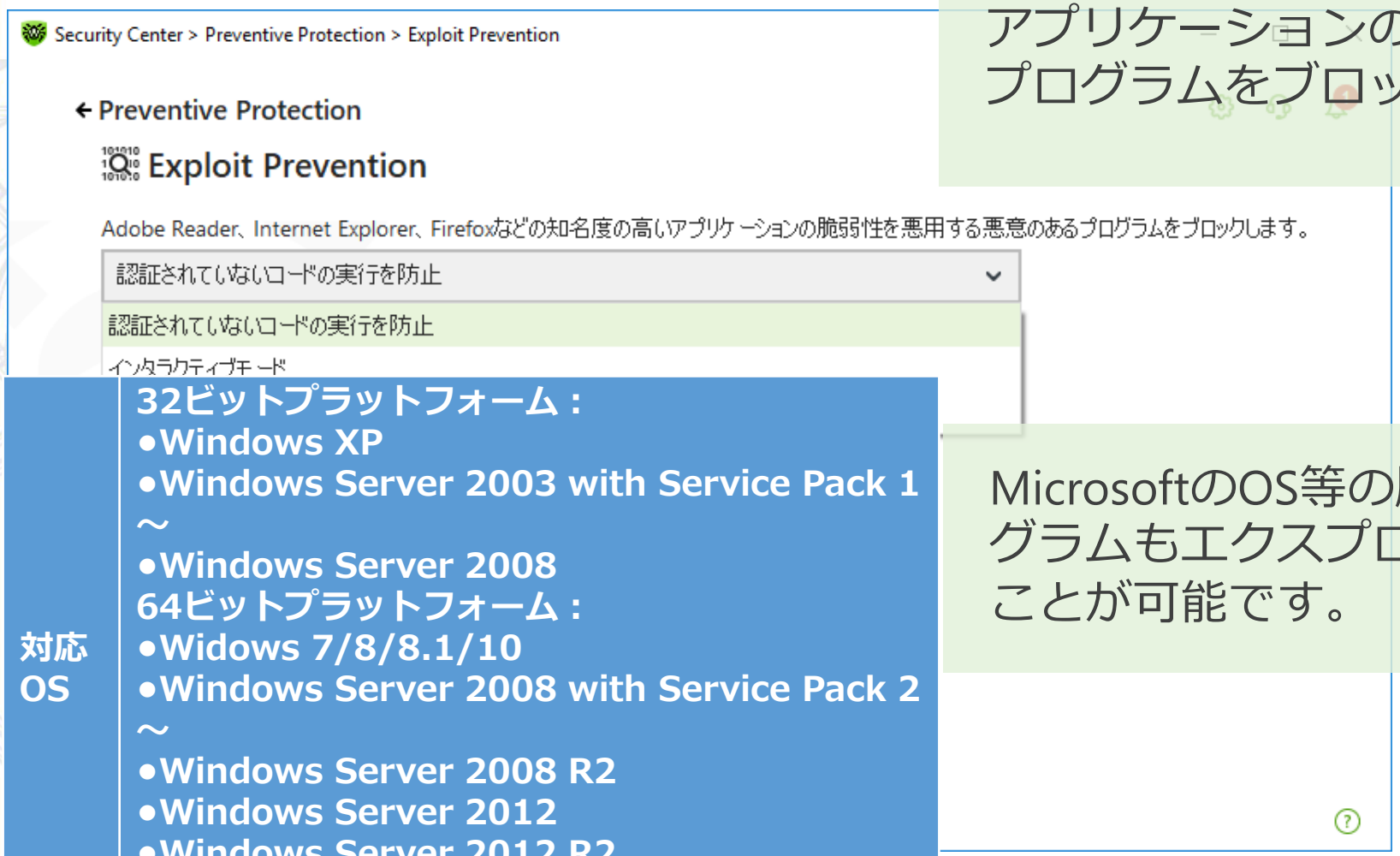
Dr.Web CureIt! / CureNet!

PC及びサーバーのウィルス検知・修復。既存アンチウィルスソフトでは検知出来ないマルウェアを炙り出す非常駐型スキャナ。**他社アンチウィルスと共存可。**
インストール不要。

Dr.Web Katana

振る舞い検知機能 DPH（Dr.Web Process Heuristic）のみを実装した、ノンシグニチャー型アンチウィルス製品
他社アンチウィルスと共存しながら未知の脅威を検知

古いOSも保護



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。

対応OS

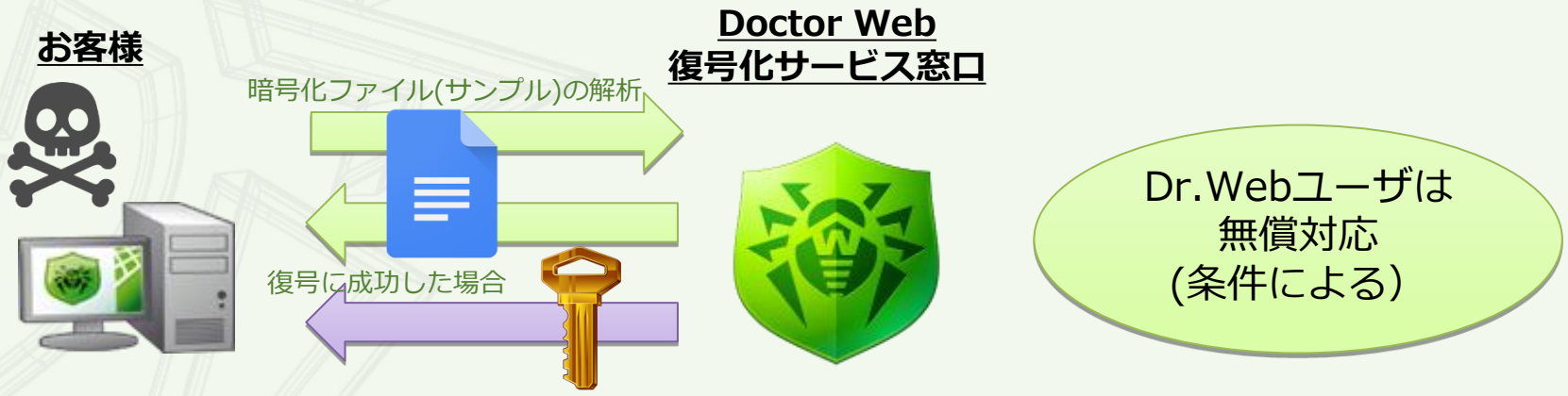
32ビットプラットフォーム：
- **Windows XP**
- **Windows Server 2003 with Service Pack 1 ～**
- **Windows Server 2008**

64ビットプラットフォーム：
- **Widows 7/8/8.1/10**
- **Windows Server 2008 with Service Pack 2 ～**
- **Windows Server 2008 R2**
- **Windows Server 2012**
- **Windows Server 2012 R2**
- **Windows Server 2016**
- **Windows Server 2019**

万が一暗号化されてしまった場合

ランサムウェア被害救済サービス

お使いのAVを問わずどなたでもご利用頂けるランサムウェアによる暗号化被害ファイルの復号化サービスです。
Doctor Webウイルスラボでは2014年からファイル復号化ルーチンを徹底的に研究しております。マルウェアインテリジェンスで得られる情報を掛け合わせ高い確率で多くの暗号化ファイルを救済しております。



アンチウイルス自体が脆弱性にならないか？

総合電機メーカM社	国内 総合病院	Windows Defender
大手アンチウイルスソフトの管理サーバの脆弱性を突かれ、機密情報や個人情報のファイルが流出。ランサムウェア被害に（2020年）	標的型攻撃によりOSおよび大手アンチウイルスの脆弱性を突かれ、さらにADの管理者権限を奪取される。電子カルテ情報が漏洩（2019年）	Windws7から10の間の長期間にわたり存在した脆弱性が判明。実際も攻撃も確認されている。（2021年）
アンチウイルスの無力化が最も危険	**実被害が大きい**	**アンチウイルスの脆弱性が狙われる**

著名なセキュリティーソフトほど脆弱性を突かれ、攻撃の拠点とされます。

Doctor Webは、「アンチウイルス自体を保護するセルフプロテクション」に注力。

著名になることよりも、顧客のコンピュータ資産を守ることを優先します。

アンチウイルスにとって知名度は必ずしもメリットではありません。

新しいランサムウェア対策（まとめ）

古いOSに対応したエンドポイントセキュリティー

単一のアンチウイルスではなくセカンドオピニオンを積極利用

万が一ランサム感染の場合の手立てを整理しておく

アンチウイルス選びは「自己防衛」機能がポイント

Dr.WEB®

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