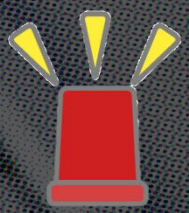
CORE
CORE GROUP

IT資産の完全な把握、コスト削減の実現
信頼と安心、そして未来を共にするパートナー

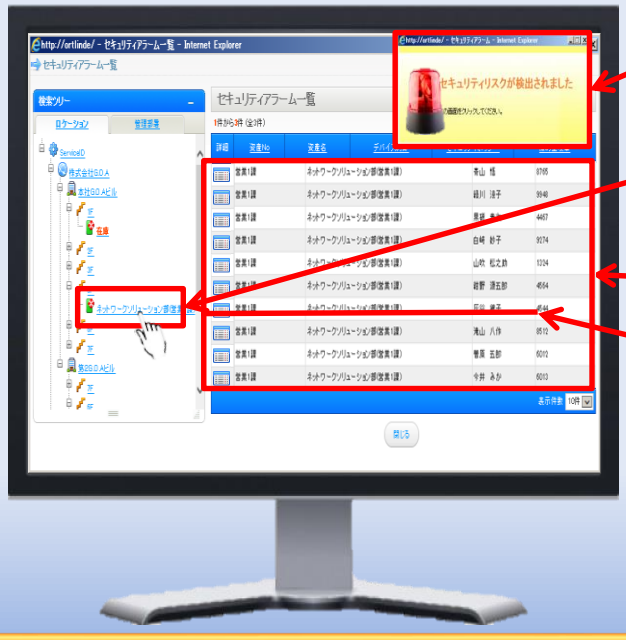
「今のマルウェア対策 安心ですか？」



日本初!
国産 !!

インシデントレスポンスといえば「マルウェアバスター」

市場を賑わしている標的型攻撃、マルウェア攻撃を素早く検知
防御・対策・分析・予防までワンストップで実現！



①パトランプ発報
※音声によるアラートも可能

②組織ツリー表示
該当組織にⓍを表示

③感染資産表示

④利用者へ連絡
もしくは現地に急行

防御のポイント　発病したマルウェアの駆除に加え、発病前のマルウェアがどこに存在するのか把握

1 **端末の特定**
- 感染端末のIPアドレスの把握
- 端末の管理状況の把握（設置場所・管理者）

2 **侵入検知**
- 既知のマルウェアの検知・防御
- 未知のマルウェアの検知・防御

3 **感染経路分析**
- 感染経路の確認
- 感染した可能性のある端末のIPアドレスの把握
- 組織内の端末情報の把握（OS情報・ソフトウェア情報）

検知だけではない
マルウェア対策を
提案致します！

特徴　ITAMの機能を生かしたメリットにより、組織のインシデント発生を抑止

1 **迅速な初動対応**
感染資産の設置場所や利用者情報を参照し、
素早い初動対応が可能

2 **組織内の脆弱性把握**
エンドポイントの標的型攻撃対策製品の導入状況を把握し、
未導入のエンドポイントへ導入の促進が可能

3 **予防策の実施**
配布機能を用いてインシデントに対するパッチの配布が可能
資産情報を用いてHW/SWの置換時のデータ活用が可能

CORE
CORE GROUP

IT資産の完全な把握、コスト削減の実現
信頼と安心、そして未来を共にするパートナー

「マルウェアバスター」

①端末の特定
検知した端末、マルウェア潜伏の可能性がある端末の管理者・管理場所を把握

②侵入検知・隔離マルウェアを検知したタイミングで端末を防御

③感染経路分析
侵入経路と共に、マルウェアが他の端末に潜んでいる可能性を分析

1 端末の特定

ITA

1. 感染、及び感染の可能性のある端末を組織ツリーで一覧表示
2. 対象端末の利用者（責任者）へ連絡
3. 原因となった脆弱性の高いソフトウェアの削除、もしくはバージョンアップ

端末利用者の特定

資産No	資産分類コード	管理部署名	ブロック名	氏名	コンピ
INV_PC0000023	PC	戦略部	戦略部	緋川 遼子	WIN-HT
INV_PC0000004	PC	業務推進部	業務推進部	倉川 忠康	S-190
INV_PC0000001	PC	開発技術課	情報システム部	田中 三郎	N234
INV_PC0000046	PC	営業1課	情報システム部	田中 三郎	N280
INV_PC0000003	サーバー	開発技術課	情報システム部	赤井 真	TKSV00
INV_PC0000168	ゲストOS	戦略部	戦略部	赤井 真	L810

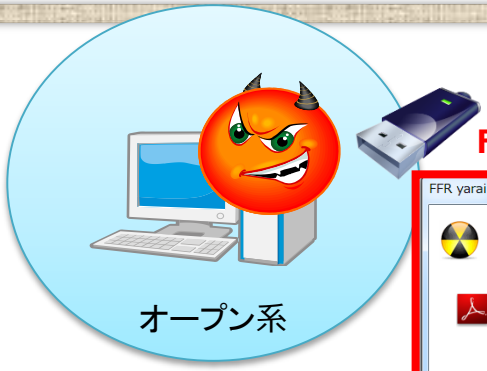
ソフトウェア種別	プロダクトID	パス名	ソフトウェア名	ソフトウェアバージョン
プログラムの追加と削除	none		AuthenTec Fingerprint Software	9.0.8.36
プログラムの追加と削除			Symantec Endpoint Protection	12.1.3001.165
プログラムの追加と削除			Microsoft Visual C++ 2005 Redistributable (x64)	8.0.59192
プログラムの追加と削除	none		TOSHIBA HDD Protection	2.2.0.12
プログラムの追加と削除	none		TOSHIBA PC Health Monitor	1.7.3.64
プログラムの追加と削除			PlayReady PC Runtime amd64	1.3.0
プログラムの追加と削除	{2503-211-4525401-49236		Microsoft Office Professional Plus 2010	14.0.4763.1000
プログラムの追加と削除			Intel(R) Network Connections Drivers	15.4
プログラムの追加と削除			Synaptics Pointing Device Driver	15.2.4.4
プログラムの追加と削除			TOSHIBA Fingerprint Utility	1.0.2.37
プログラムの追加と削除			N-040 USB Driver	1.0.5.0
プログラムの追加と削除	none		Java(TM) 6 Update 20	6.0.200
プログラムの追加と削除			Microsoft Visual C++ 2005 Redistributable	8.0.56336

脆弱性の高いSW抽出

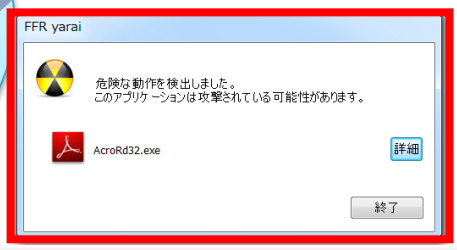
2 侵入検知・隔離

Yarai

1. マルウェアが何かしらの状態で発症
2. FFR yaraiが検知し、マルウェアの実行プロセスの停止等で端末防御
3. 発病とともに隔離実行
   アラートを出して管理者への報告



FFR yarai検知・隔離



3 感染経路分析

SML
SECURITY MANAGEMENT WITH LOGGING

ファイル一括削除

侵入経路の明細 選択解除 ファイル隔離 ファイル復元 ファイル削除

状	日時	ログ種別	プロセス	ファイル名	ファイルパス	ユーザー	その他
1	2014/06/26 16:35:59	ALERT	AcroRd32....	AcroRd32.exe	C:¥Program File...	satou	ZDP: Process was killed.
2	2014/06/26 16:35:04	OPEN	AcroRd32....	機密②.pdf	C:¥Users¥satou...	satou	
	2014/06/11 12:16:28	RENAME	explorer.exe	機密②.pdf	C:¥Users¥satou...		
3	2014/06/11 12:15:56	MOVE	explorer.exe	サンプル.pdf	C:¥Users¥satou...	yonekawa	
	2014/06/11 12:15:47	COPY	explorer.exe	サンプル.pdf	C:¥Users¥yonek...	yonekawa	
4	2014/06/11 12:15:47	DEVICE					

1. 6/26、FFR yaraiで異常検知
2. ファイルがオープンされた
3. ファイルがコピー、移動、リネームされた
4. 6/11に使用された外部デバイスからファイルが持ち込まれた