

SGAV および SGAV Domino 技術ガイドブック



StandGuard Anti-Virus—Technical Packet

StandGuard Anti-Virusの紹介	5
ソリューション概要: IBM Power Systemに対する脅威とリスク	
なぜ、IBM Power Systemをスキャンする必要がありますか？	7
IBM Power Systemは、ウィルスの脅威が無いですか？	7
IBM Power Systemへの脅威は何ですか？	8
IBM Power Systemの何がリスクにさらされていますか？	8
何で IBM Power Systemとそのデータがリスクにさらされていますか？	9
IBM Power Systemを保護する方法: StandGuard Anti-Virusの主な特徴	
システムをスキャンしない限り、ウィルスは発見できません	11
IBM i 向けネイティブMcAfeeスキャン・エンジンは、どうシステムを保護しますか	12
IBM i スキャン機能のサポート	13
オン・アクセス・スキャン	13
オン・デマンド・スキャン	13
IBM i SMTPメールのスキャン	13
オブジェクト統合スキャン	14
ゲストオペレーティングシステムのスキャン	14
IBM i ロータスドミノのスキャン	15
自動更新	15
スケジューリング機能	16
ネットワーク起動	16
レポートとログ	16
モニタリングとアラート	17


StandGuard Anti-Virusは、どのようにウィルスを検出して、 IBM Power Systemを保護しますか

IBM Power System向けベスト・スキャンング・エンジン	19
オブジェクト・タイプを確認する	19
オブジェクトを解読する	19
ウィルスを探す	19
暗号化	20
ポリモフィズム(多形性)	20
帰納的(ヒューリスティック)な分析を使う	20
チェックサムを行う	20
クリーン(ウィルスの除去)	20
法令順守の規定、会社重役、および監査の要望	
COBITオブジェクティブ DS5.17: セキュリティ機能の保護	21
COBITオブジェクティブ DS5.19: 悪意のあるソフトウェアの防止、発見と訂正	21
COBITオブジェクティブ DS9.5: 未許可のソフトウェア	21
IBM i ロータスドミノ向けStandGuard Anti-Virus	
メールスキャンング	23
データベーススキャンング	23
隔離・検疫	23
リアルタイム・アラート	23
自動更新	24
スケジューリング	24
ロギング	24
管理の容易さ	24
連絡先	25

StandGuard Anti-Virusは、IBM i(別名OS/400またはi5/OS)、AIX、LinuxとDominoを稼動しているIBM Power System(別名AS/400、iSeries、システムi)のセキュリティ部門で金賞を受賞しております。この章では、サーバーとオペレーティングシステムの過去と現在のバージョンを表すために、「IBM Power System」と「IBM i」用語を使います。

StandGuard Anti-Virusは、IBM Power System のセキュリティ必要条件を満たし、ウイルス、バグとハッカーソフトからデータを保護し、安心して使用可能なツールを提供いたします。





IBM Power Systemに対する脅威とリスク

IBM Power Systemのスキャンを行う必要がありますか？ はい。

IBM Power Systemは感染したストリーム・ファイル(PCファイル)をサーバーとして、リモートPCと他のサーバと共に常に共有することができます。IBMマーケティングとして、IBM Power Systemは「ウィルスに頑強である」とオブジェクト指向を強調しています。「ウィルスが生じた」ことがあると一度も主張したことはありません。「ウィルスに強いシステムである」と言うことは、伝統的なファイルシステム、プログラム、および CLP、RPG、COBOL プログラムはウィルスに強いということです。つまり実行前にコンパイルされ、オブジェクト指向制御されているためです。一旦コンパイルされたら、簡単に変えることができません。

IBMサーバの革新は、ウィルスの被害を受けにくいことです。今日のIBM Power SystemはUNIXバイナリー・コードを実行して、POSIXとX/Open規格に従って、UNIXファイルシステム上で、リモートコマンド、シェルスクリプト、およびJavaを実行します。感染したHTMLとPHPファイルが存在するウェブサーバーとして稼動しています。それは今日のウィルスと悪質なコードを防ぐ環境と言えます。

なぜ、IBM Power Systemは、ウィルスに強いホストなのですか？

IBM Power Systemは、ネットワーク上でいろいろなタイプのコンピュータとして、稼動することが出来ます。感染したファイルがこれらのコンピュータのいずれかで実行された場合、そのコンピュータは感染してしまい、次々に残りのネットワークへの新しい攻撃を開始することができます。IBM Power System自身にも攻撃します。これらの攻撃は、コンピュータとネットワークを実行不可能にすることができます。このウィルスは、次々に感染を他のマシンへ広げます。

ウィルスは、IBM i ファイル、プログラム、ライブラリーに対してコマンドを変更、コピー、削除、実行することができます。IBM Power Systemに関するウィルスは、ネットワーク共有のある区画またはIntegrated File System(IFS)を経由して広がります。



脅威とは、何ですか？

現代の脅威と悪性コード(例えばウィルス、スパイウェア、爆弾(ボム)、マルウェアソフト、ネットワークパスワード検知、アドウェア、疑わしいプログラム、ルートキット等)は、会社におけるコンピュータ・データとセキュリティーに大きなリスクを提示しています。今日広まっている432,000以上の既存の脅威、毎週起こっている100以上の新しい脅威が企業を目標とするようになっています。今日の脅威は、単に馬鹿げた事だけでなく、本当の脅威となります。 EXE感染とマクロウィルスと一緒に、インターネットワーム、トロイの木馬とバックドアは今では増殖している脅威です。これらの混合された脅威は、今後の新しいウィルスとなります。 コンピュータ利用率を上げている最近の傾向は、信頼の無いソースからコンパイルされたプログラム、システム・リソースを使う、盗む、またはデータを破壊する不確かな機能によって起こります。

何がリスクにさらされていますか？

Integrated File System(IFS)は、ほとんどのIBM iビジネス(業務アプリケーション)から見落としがちな領域です。ますます多くのオペレーティングシステム機能がIFSのルートファイルシステムのファイルに保存された情報とコードを使用するようになって来ています。 残念ながら、まだIFSが使用されていないという誤解があります。より多くのオペレーティングシステムコードとデータがQSYS.LIB以外のIFSに存在します。 システムの重要なデータの多くがIFSに保存されています。(TCP/IP構成ファイル、ウェブサーバー構成ファイル、ターミナルサービス構成ファイル等)。

WebSphere Application Server(WAS), IBM Power SystemとApacheウェブサーバは、Root上に実行可能なコードとデータを保存しています。 IBM iを含むあらゆるシステムで稼動するPHP(アプリケーションプログラムまたはデータを読むか、変更が出来る)のアプリケーションが、IBM iで稼動するとウィルスの脅威にさらされます。

スキャンされていないIFSに保存されたPCデータまたはアプリケーションは、IBM i システムをリスクにさらします。 IFSにある一度もスキャンされず、クリーンになっていない感染したファイルは、再度PCクライアントを感染し続けます。 そして、IFS上に残っています。 おそらく、上記のアプリケーションは、WAS、ポータルServer、ApacheまたはPHPと関連したアプリケーションプログラムやデータはWindowsウィルスにより攻撃される恐れがあります。

IBM i システム全体の安定と統合は、IFSのセキュリティーと統合を行わない限り、IBM i は脆弱と言えます。


何が、IBM Power Systemとそのデータをリスクにさらしますか？

ウィルスと悪質なコードは、さまざまなツール(例えば、ルートキット、トロイの木馬、パケット盗聴プログラム)を使用して、データに感染したり、盗んだりして、ホストに感染する一般的な技術を利用しています。これらの技術はFTP、Telnet、およびODBCを含んで、すべてが通常のIBM i 環境で毎日のように使われています。これらの技術で、ウィルス、悪意のあるコードは、他のタイプのサービス妨害(DoS)攻撃や、マン・イン・ザ・ミドル(MIM)攻撃や、Floodingや、Sniffingや、Spoofingや、アルプや、DHCP攻撃や、バッファオーバーフローなどの攻撃の一部として使用されていることがあります。

実行しているウィルスはIBM Power Systemにマウントされたネットワークドライブに対してDELコマンドと他のリスクあるシステム・コマンドを実行できます。重大な被害を引き起こして、IPLによる回復があれば、これらの攻撃のいくつかはシステムTCP/IPスタックから消えてしまいます。

IBM i 上のドメイン名解決機能(BINDプログラム)は、Portable Application System Environment (PASE)が稼動する実行可能なAIX環境で可能となります。パブリック・ドメイン上の多くの異なったタイプのシステムは、全く同じコードを使用します。この特定のプログラムは、いくつかのセキュリティ上の問題があります。少なくともその1つで、AIXの「スーパーユーザー」やIBM iのQTCPなどは、攻撃者に任意のコードの実行を可能にしています。これは他のIFSファイルとNative環境のIBM i リソースさえ攻撃するのに使われるルートファイルシステムに挿入される凶暴で、ウィルスのようなコードがどう使われるかが、1つの例です。

規定の法律はセキュリティ取り組みに重大な挑戦をしています。ソフトウェアソリューションは組織を法令順守に運び込む計画を築き、実装する際に重要な役割を果たします。悪質なコードの脅威と戦うことに関する特定の方向性に関して、SOX法と他の規定の法律に従う取り組みにCOBITガイドラインを使用できます。



IBM Power Systemとそのデータを保護する方法

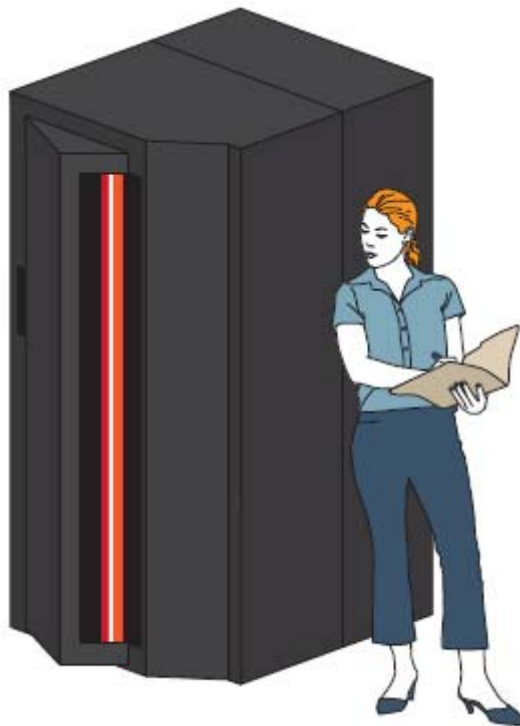
IBM i をスキャンしないと、ウィルスは決して発見されません

ネイティブのソリューションが脅威を検出して、クリーンするように設計されている状態でシステムをスキャンしていない場合、脅威がIBM Power Systemにあるかどうかを知る方法が全くありません。そして、絶えず脅威が進化し、システムは定期的に信頼できるスキャン対策を使ってファイルサーバスキャンをしなければならない以上に発展しました。StandGuard Anti-VirusはMcAfeeのスキャンエンジンの最新の技術を取り入れます。StandGuard Anti-Virusは、古くからある製品で、ウィルス対策ツールとして多くのテストがなされ、高度な帰納的分析、一般の検出、クリーンが可能です。StandGuard Anti-VirusでIBM Power Systemをスキャンしていないと、システムで脅威がないかがわかりません。これらのパワー機能を使って、潜在的な脅威を制御して、排除してください。

・マクロおよびスクリプト
ウィルスを検出して、ク
リーンにします。

・暗号化されて多形ウィル
スを検出して、クリーンに
します。

・帰納的な分析を使って未
知のウィルスを見つけま
す。



・トロイの木馬、ワーム、マル
ウェアを見つけて、取り除き
ます。

・圧縮、パックされた、OLEファ
イルをスキャンします。

・IBM i上のビルト・イン・スキャ
ンをサポートします。



IBM i 向け、ネイティブ McAfee スキャンはどう IBM i を保護しますか？

ウィルス・スキャンの主要メーカーの McAfee とのパートナーにより、Bytware 社は IBM i 向けの Anti-Virus スキャン対策を提供しています。McAfee のエンジンは業界で非常に優れたエンジンを提供しています。

・マクロおよびスクリプトウィルスを検出して、クリーンにします

マクロウィルスは悪意のあるマクロです。マクロウィルスは、マクロプログラミング言語で書かれていて、マクロをサポートするドキュメントに付けられています、Word やエクセルファイルのようなマクロウィルスを含むドキュメントかテンプレートがターゲット・アプリケーションで開かれるとき、ウィルスは稼働していて、損害を与え、他のドキュメントにそれ自体をコピーすることがあります。プログラムの継続使用はウィルスの増殖をもたらします。

・暗号化された多形ウィルスを検出して、クリーンにします

暗号化されたウィルスのコードは、残りのウィルスのために復号化アルゴリズムで始まって、スクランブルが掛かっているか暗号化されたコードを続行します。毎回感染され、自動的にそれ自体をエンコードします。コードは決して同じにはなりません。このメソッドで、ウィルスはウィルス除去ソフトによって検出を避けようとしています。

多形性ウィルスはウィルス除去ソフトで検出を避ける方法として様々な(完全に機能的ですが)自分自身のコピーを作ります。いくつかの多形性ウィルスが、異なった暗号化体系を使用して、異なった復号化ルーチンを必要とします。したがって、同じウィルスは異なるシステム、または、異なったファイルの中でさえ完全に異なるように見えるかもしれません。他の多形性ウィルスは、ウィルス除去ソフトを阻む試みに指示系列を変えて、誤ったコマンドを使用します。最も高度な多形性ウィルスの1つは、ウィルスコードとその復号化ルーチンを変えるのに変異エンジンや乱数発生を使用します。

・高度なヒューリスティック分析を使用することで未知の新しいウィルスを検出します

ヒューリスティックな分析は潜在的ウィルスを特定する Anti-Virus ソフトによるコンピュータ・プログラムのオブジェクトの動きにそった分析を意味します。

・トロイの木馬、ワーム、および他の多くのタイプの悪意のあるソフトウェアを検出して、取り除きます

トロイの木馬は有益なアプリケーションのふりをする不正プログラムです。それは故意にユーザが予想しない動きをします。複製しないので、トロイの木馬はウイルスではありませんが、それらはオブジェクトを破壊することも考えられます。トロイの木馬は、攻撃の前触れとしてハッカーによってシステムにダウンロードされ、リモートサイトへのパスを提供してしまうということに繋がります。

ワームは複製を許す寄生的なコンピュータ・プログラムですが、ウイルスと異なって、それらは他のプログラムファイルに感染しません。ワームは、同じコンピュータでコピーを作成できるか、またはネットワークを通して他のコンピュータにコピーを送ることができます。ワームはインターネットRelay Chat(IRC)を通して広がります。

・圧縮、パックされたOLEファイルをスキャンします

ZIPファイルは圧縮されたファイルの集合としてのアーカイブです。ZIPファイルはインターネットではよく利用され、ユーザが単一のコンテナで複数のファイルをいっしょに送ることができます。そして、ZIPファイルはディスクスペースおよびダウンロード時間を節約します。パッケージされたファイルのどれかがウイルスを含んでいるなら、ZIPファイルはウイルスを含むことになりますが、ZIPファイル自体は直接のリスクではありません。他のアーカイブファイルタイプはRAR、SIT、およびLHAファイル等です。

・IBM iのスキャン機能をサポートします。

V5R3から始まって、IBMはウィルススキャンサポートをオペレーティングシステムに統合しました。StandGuard Anti-Virusはこれらの機能を完全にサポートします。結果として、他のプラットフォームとファイルシステムと比べて、より良いセキュリティと実質的に低いオーバーヘッドとなります。

・オン・アクセス・スキャンニング

StandGuard Anti-Virusはスキャンファイルに対して、ダイナミックにウィルスの脅威に対するリアルタイムの保護を提供します。ファイルサーバーアクセス(NetServerはドライブ,FTPをマップします)と5250の環境(Java、Websphereなどのようなホストベースのアプリケーション)のために別々にスキャンすることができます。

・オン・デマンド・スキャンニング

StandGuard Anti-Virusはオン・デマンド・スキャンニングを提供します。(スケジュールごとにシステムのすべてか一部をスキャンできます。) どのディレクトリをスキャンしたらよいか、またスキャンを実行するスケジュールを構成できます。つまり、他のアプリケーションにCPUの影響を減少させるためにオフピークの間にスキャンを実行できます。

●IBM i SMTPメールをスキャンします

StandGuard Anti-Virusは、IBM i メール・サーバー・フレームワーク経由で受信、送信メールをスキャンできます。メールを送るか、または受け取るのにIBM Power Systemを使用し、StandGuard Anti-VirusはPCクライアント、ネットワークにおける他のサーバに達する前にメールをスキャンし、ウィルス確認を実行できます。

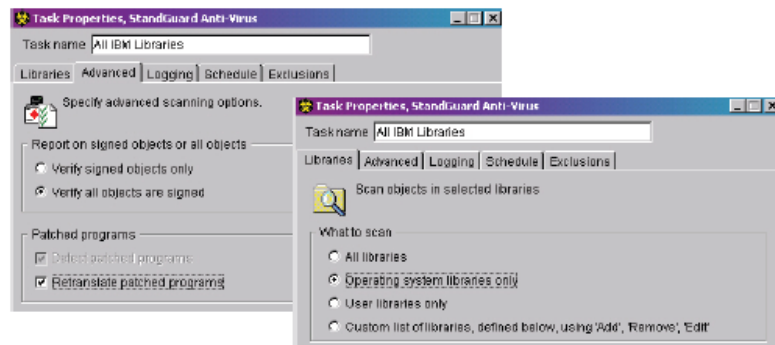


変更されたオブジェクト、パッチを受けたプログラム等見出すObject Integrity Scanning:

IBM iにしかないオブジェクト統合機能に関して、StandGuard Anti-Virus は、重大なリスクをオペレーティングシステムに引き起こすか、またはすべてのセキュリティを迂回させてしまう可能性を誘発するオブジェクトが存在するユーザライブラリーをスキャンします。

システムセキュリティ管理者は、権限のない機能を実行するプログラムに関して考慮する必要があります。新しいサーバー機能がオープンな環境で利用可能になるとき、サーバのオブジェクトベース保護機能のいくつかがもう機能しません。例えば、IFS上で、ユーザはストリーム・ファイルなどのディレクトリ内のいくつかのオブジェクトを直接操作できます。ファイルサーバーとして、サーバは多くのPCユーザーが共有するプログラムを保管できます。ハッカーと他の悪意あるユーザーはすばやく先進技術に追いつくことができるので、唯一の効果的なセキュリティー対策はシステムにウィルスプログラムが検出されるのを助けるために常に最新ウィルスファイルをアップデートすることが重要となります。

IBMと他の多くのベンダーがそれらのオブジェクトにデジタル署名をすることもこの理由のひとつです。つまりスキャンがすべてのサーバーでとても重要であるためです。オブジェクトをスキャンしないなら、オブジェクトが変更されたかどうかを確かに知ることはできません。StandGuard Anti-Virus は、変更されたオブジェクト、パッチされたプログラム等をスキャンして検出します。



StandGuard Anti-Virusで、望まれないオブジェクト変更からIBM iを保護します。IBMのデジタル署名をスキャンすることにより、オブジェクトがいつ変更されたかがわかります。

•区画上のゲストオペレーティングシステムをスキャンします。

StandGuard Anti-Virusは、ネットワークファイルシステム(NFS)を使用することでLINUXとAIXゲスト区画のスキャンとクリーン機能をサポートします。ゲスト区画上のNFSがマウントされたボリュームをスキャンするためにスケジュールされたスキャンタスクを作成することによって、各区画の複数のスタンドアロンのAnti-Virusアプリケーションをインストールして、構成する時間、取り組み、およびコストを削減できます。ホスト区画にStandGuard Anti-Virusを一つ導入することにより、LINUXとAIX区画のすべてのウィルス、トロイの木馬、ワーム、マルウェア、およびスパイウェアを取り除くことができます。
(付加ライセンスが必要となります。)

•IBM i ロータスドミノをスキャンします。

DominoサーバをIBM Power Systemで実行しているなら、StandGuard Anti-Virusは、Dominoサーバをスキャンするためにアドオン機能が必要となります。StandGuard Anti-Virus は、ウィルスチェックを、Dominoメールとデータベースに対してスキャンします。そしてセントラル管理サーバより、リモートDominoサーバを構成、管理します。詳しい情報は、Dominoに関するAnti-Virus の章を見てください。

•ウィルス定義ファイル(DATファイル)の自動ダウンロード

StandGuard Anti-Virusの自動ダウンロードは、McAfeeサイトからウィルス定義ファイルを自動的にダウンロードすることによって最新のウィルスの脅威から保護されています。自動的にウィルス定義を最新に保つことによって、StandGuard Anti-Virusは毎週のように起こる100+以上の新種のウィルス脅威から保護されます。StandGuard Anti-Virusにインタラクティブにファイルをダウンロードするか、夜間のバッチ処理でダウンロードするメニュー/コマンドを用意しています。または、IBM i にプラグインされた機能により、アップデートを自動的に処理させることができます。

•ソフトウェアアップデートとフィックスの自動ダウンロード

StandGuard Anti-Virus はBytwareサイトから最新の機能、フィックス、および拡張機能をダウンロードします。

```
Change AVUPDATE Attributes (AVCHGUPDA)

Type choices, press Enter.

Transfer method . . . . . =FTP          +PATH, +FTP
FTP Location . . . . . =DFT
_____
_____
FTP Password . . . . . _____
_____
_____
Schedule . . . . . =DAILY          +DAILY, +WEEKLY, +MONTHLY...
Days . . . . . =ALL              +SAME, +ALL, +SUN, +MON...
      + for more values
Time . . . . . 053100          Time, +SAME
Output . . . . . =LOGFILE        +LOGFILE, +PRINT
Back up files before update . . =YES          +NO, +YES
Retrieve files only . . . . . =NO            +NO, +YES
More...

F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
```

製品とウィルス定義両方の自動アップデートを最新に保ち、保護することが出来ます。直接McAfeeとBytwareサーバから更新が可能です。あるいは、プログラム更新とDAT更新をダウンロード後、ローカルシステムから更新することもできます。

•スキャンとアップデートのための内蔵スケジューリング機能

StandGuard Anti-Virus は、ウィルス定義、製品の拡張機能、およびスキャンタスクの自動アップデートをスケジュールできるように、IBM i ジョブ・スケジューラと他のジョブスケジューラを統合しています。IBM i ツールを使用することで、タスクを自動化することによって、24時間StandGuard Anti-Virus がIBM iを守ります。

・ネットワーク対応

StandGuard Anti-Virus はFTPサーバか共有されたローカル・ネットワーク・パスのいずれかからウィルス定義とプログラム最新版を検索できます。パスは別のIBM Power System、区画、Windowsファイルサーバー、またはサポートされたネットワーク・パスにも配置できます。ウィルス定義をダウンロードするには、McAfeeのFTPサーバから、または共有されたネットワーク・フォルダーから取ることができます。また、同一ネットワークダウンロード機能を使って、StandGuard Anti-Virus製品を最新の状態に保つことが可能です。

・レポーティングとログ機能

StandGuard Anti-Virus はモニターとレポートを使用したログ機能を提供します。

- ・スキャンレポートはスキャンされたディレクトリ、感染結果、クリーン/検疫処理の詳細な情報を提供します。
- ・ウィルススキャン処理はシステム監査ジャーナルに記録されます、システム内のウィルス処理監査証跡を提供します。
- ・StandGuard Anti-Virusの実行によるすべての変更はAVJRNジャーナルに記録されて、だれが変更したか、いつ実施されたかをAVJRNジャーナルに記録されます。
- ・スキャン関連のメッセージはAVMSGQにログされます。必要に応じて手動でメッセージキューを見るか、パッケージのモニター・ツール(Bytware Messengerなど)を使用して、またはメール、携帯電話、またはポケットベルを通してウィルスと失敗したダウンロードについて警告を出します。

・インターフェースは、5250画面またはIBM i Navigatorプラグインとなります

・モニタリングと警報

Bytwareは、進行中の問題ができるだけ早く処理され、解決策が行われたことを検地するためにAVMSGQにログされたStandGuard Anti-Virus メッセージをモニターすることを強く勧めます。



StandGuard Anti-Virus はシステムの状態に関して最新に保つことができます。自動化されたモニターと通知機能を持ったStandGuard Anti-Virus のウィルス保護機能によって、いつクリティカル・イベントが起こったか、操作継続が出来ないか等を知ることが可能です。

たとえば、こうすることができます：


- ・手動でAVMSGQメッセージキューをモニターしてください。
- ・Bytware Messenger等のパッケージで、モニターを自動化してください。
- ・メール、ポケットベル、携帯電話、スマート電話等タイムリーな通知をしてください。

サーバにanti-virus保護をインストールするのと同様に、問題がいつ起こったかを知るのは重要です。モニターする必要がある重大項目は以下の通りです。

- StandGuard Anti-Virusがウィルスを検出して、取り出したとき
- ウィルス定義ファイルが検索されない場合。
- AVSVRジョブが終わるか、走っていない場合。
- スキャンが異常に終わる場合。
- スキャンがまったく実行されなかった場合。

StandGuard Anti-Virus はウィルス・スキャンすること以上のことをします。
IBM Power System を良好状態に保って、ネットワークの他の領域かシステムの外でウィルスの蔓延を防いで、規定の必要条件を満たします。





StandGuard Anti-Virusは、どのようにウィルスを検知しますか。
そして、IBM Power Systemをどのように守りますか。



IBM Power System用ベスト・スキャン・エンジンです

オープンソース、ClamAVのような非商業的に人気のあるスキャンエンジンはビジネスに、有効なソリューションではありません。McAfeeスキャンエンジンとBytwareの StandGuard Anti-Virus は商用のフル機能を提供するソリューションです。

StandGuard Anti-Virusによって包括されたMcAfeeのスキャンエンジンは複雑なデータ分析エンジンです。正確な分析のプロセスはスキャンされるオブジェクトとそのウィルスのタイプによります。

•オブジェクトのタイプを特定すること

このステージは、どのタイプのオブジェクトがスキャンされているかを決定します。例えば実行コードを含むファイルは、スキャンされる必要があります。例えば、マイクロソフトウィンドウズ・オペレーティングシステムにおける、異なったタイプのファイルはそれらのファイル拡張子(EXEや.TXT)が区別されます。

しかしながら、本当の識別に隠れて誤った拡張子を与えることもあります。ファイルの内容は、最初に決定されなければなりません。それぞれのタイプのオブジェクトは特別な処理を必要とします。タイプがウィルスに感染させることができないなら、これ以上のスキャンは必要ありません。例えば、ビットマップ形式(.BMPファイル)で保存された画像は感染されません。

•オブジェクトを解読すること

このステージがオブジェクトのコンテンツを解読するので、ウィルス・スキャナーは、それが何なのかを「理解しています」。例えば、オリジナルコンテンツに展開されるまで、圧縮されたWinZipファイルを解釈できません。同じことが非圧縮されたファイルにも言えます。

例えば、エンジンは、マクロウィルスを見つけるためにマイクロソフトWordドキュメント(.DOC)ファイルを解読しなければなりません。そのファイルがさらにコード化されたファイルが入っていると、ファイル解読はかなり複雑になります。例えば、WinZipアーカイブファイルは他のアーカイブとドキュメントファイルの混合となっている場合等です。オリジナルのWinZipファイルを解読した後に、そのエンジンは、解読して、別々に中のファイルをスキャンしなければなりません。

•ウィルスの検索

この複雑なステージのウィルススキャンはウィルス定義(DAT)ファイルによって制御されます。scan.datファイルは何千もの異なったドライバーを含みます。各ドライバーは、特定のウィルスかウィルスのタイプを見つけるかに関する細かい指示を持っています。ファイルの存在する場所から始められ、次に、ウィルス署名を捜し求めてエンジンは簡単なウィルスを見つけることができます。しばしば、エンジンは、ファイルにはウィルスがないことを知るためにファイルの小さい部分だけを捜す場合があります。ウィルス署名はユニークにウィルスを特定するキャラクタです。ウィルスがスクリーンに表示するかもしれないというメッセージ、またはコンピュータ・コードの断片などのように。クリーンされたファイルの中に間違っしてウィルスを検出するのを避けるためにこれらの署名を選ぶとき、注意します。より複雑なウィルスは、2つのポピュラーなテクニックを使ってスキャンする簡単な署名と共に検出を避けます。

•暗号化

ウィルスを含むデータが暗号化されている場合、anti-virus スキャナーはウィルスのメッセージまたはコンピュータ・コードを見ることができません。ウィルスが活性化された時、暗号化を解いてその時に実行します。

•ポリモフィズム(多形性)

これはウィルスがそれ自体を複製するとき、変形することを除いて、暗号化と同様です。そのようなウィルスを打ち消すために、エンジンはエミュレーションと呼ばれるテクニックを使用します。エンジンは、ファイルがそのようなウィルスを含むと疑うなら、それ自体を解読して、真のフォームが目に見えるようになるまでウィルスが無害に稼働できる人工環境を作成します。そして、エンジンは、ウィルス署名のためにスキャンしながら、ウィルスの身元を確認することができます。

•帰納的な分析を使うこと

ウィルス署名を使用して、署名がまだ知られていないので、エンジンは新しく、以前に未知のウィルスを検出できません。したがって、エンジンは機能的な分析と呼ばれる追加テクニックを使用します。ウィルスを載せるプログラム、ドキュメント、メールメッセージがしばしば顕著な機能を持っています。ファイルの変更を試みるか、メールクライアントを呼び出すか、または自分たちを複製する手段を使用するかもしれません。エンジンは、これらの種類のコンピュータ命令を検出するためにプログラム・コードを分析します。エンジンは、また、アクションの前にユーザにプロンプトを表示、または誤ったアラームを上げることを防ぎながら、正当な動作を捜し求めます。これらのテクニックを使用することによって、エンジンは多くの新種のウィルスを検出できます。

•チェックサムを実施する

このステージはまさにウィルスを特定します。エンジンはユニークな数(チェックサム)を見出すためにウィルスデータの計算をします。エンジンは、正確なウィルスを特定するためにDATファイル(scan.dat)の1つ以前に計算された値に対してこのチェックサムを計算します。

•クリーニング

このステージはオブジェクトのクリーニングです。エンジンはうまく感染ファイルをクリーンにすることができます。しかしながら、いくつかのウィルスが、変形されるか、またはファイルを修復できない程度までデータを破壊されることがあります。エンジンは感染したドキュメントからマクロを消すことによって、マクロウィルスをクリーンにすることができます。

しかし、実行可能なウィルスは、より複雑です。エンジンはウィルスがアクティブでないプログラム実行の元のパスを回復しなければなりません。例えば、ウィルスは実行可能プログラムファイルの終わりにウィルスを追加するかもしれません。実行時に、ウィルスは元のコードから実行時のパスに変更します。ウィルスがアクティブになった後、そのウィルスはオリジナルのパスから実行時のパスに変更されます。エンジンは、ウィルスコードの進路を除くことにより、このウィルスを無効にすることができます。そして、ファイルをきれいにするために、エンジンはウィルスコードを消します。

法令順守の規定、会社重役、および監査の要望を満たします

Health Insurance PortabilityとAccountability条例(HIPAA)、サーベンス-オックスリー、(GLBA)、FISMA、およびPCI DSS等(データ保護の観点より)を含む、秘密保持規定は何年もの間、遵守されています。これらはすべてが、IT専門家の責任と重要性により遵守されています。いくつかの役に立つガイドラインとして:

・COBITオブジェクトブ DS5.17: セキュリティ機能の保護

最も重要なのは、セキュリティ機能の保護に関するCOBITオブジェクトブです。この目的は、すべてのセキュリティ関連のハードウェアとソフトウェアの保全を維持して、秘密鍵の公開をガードすることを定義しています。StandGuard Anti-Virus は、ウイルスと悪質なコードを、検出して、予防して、取り除くことができます。このことはIBM Power Systemのネイティブの要求処理を満たしています。

・COBITオブジェクトブ DS5.19:悪意のあるソフトウェア防止、検出、および修正

この目的を述べますと、悪意があるソフトウェア(コンピュータウイルスやトロイの木馬)に対して、経営者側は適切な予防薬、発見手段、修正制御方法、応答の繰り返し、および報告等のフレームワークを確立するべきです。ビジネスとIT経営者側は、コンピュータウイルスから情報システムと技術を保護するために組織を通して手順が確立される必要があります。その手順は、ウイルスの防止、検出、応答の繰り返し、および報告を取り入れるべきです。StandGuard Anti-Virusは、ウイルスと悪質なコードを検出して、予防して、取り除くことができます。

・COBITオブジェクトブ DS9.5:権限のないソフトウェア

権限のないソフトウェアに関するCOBITオブジェクトブは、個人で無免許のソフトウェアの使用を制限する明確な方針が決められ、励行されるべきであると言っています。この組織はウイルス検出とそのソフトウェア対策が重要です。ビジネスとIT経営者側は権限のないソフトウェアがないかどうか定期的に組織のパーソナルコンピュータをチェックするべきです。ソフトウェアとハードウェア許諾契約の要件へのコンプライアンスは周期的ベースで見直されるべきです。StandGuard Anti-Virusは、ウイルスと悪質なコードを検出して、予防して、取り除くことができます。



AS/400 ロータスドミノ向け StandGuard Anti-Virus

IBM Power System上のMcAfeeとStandGuard Anti-Virus Domino

サポートがもたらすことは:

StandGuard Anti-Virus Dominoのアドオン機能はロータスDominoメールとIBMPower SystemsにあるDominoデータベースのスキャンとその保護を行います。StandGuard Anti-Virus の機能を提供して、Dominoアドオン機能は、以下の機能を提供いたします:

•メールスキャン

アプリケーションはダイナミックにウィルスと他のタイプの悪質なコードとなるメールメッセージをスキャンし、感染したもの、潜在的に有害なメッセージからDominoメールユーザを保護します。

•Dominoデータベーススキャン

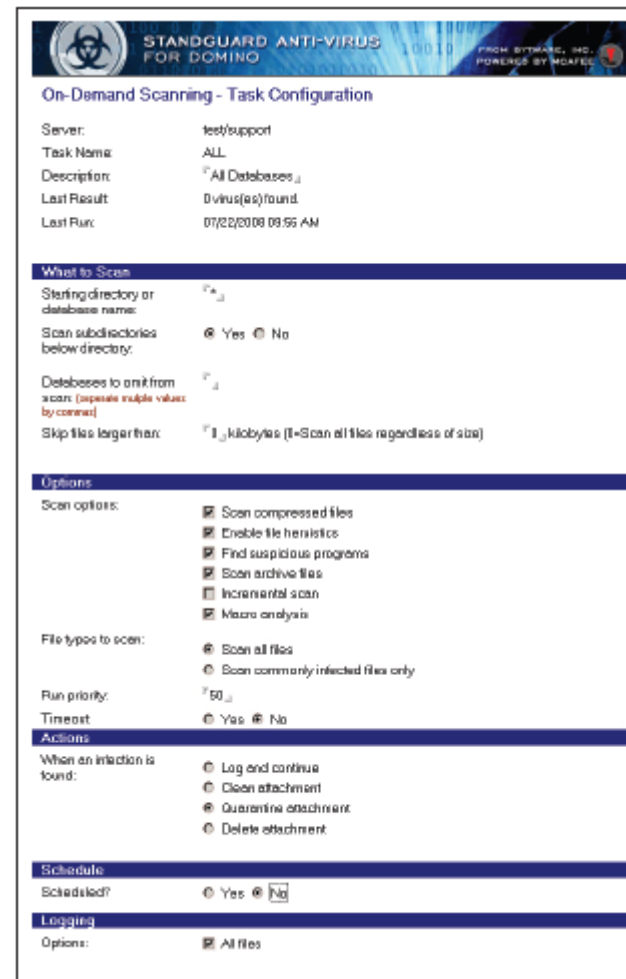
ドキュメントの添付ファイルとOLEオブジェクトの中に埋め込まれたウィルスと悪質なコードを検出して、SGAVはDominoデータベースのオン・デマンド・スキャンを提供します。

•隔離・検疫

StandGuard Anti-Virus は感染ファイルが安全な場所に移動される安全な領域を提供します。ファイルが検疫される時、ファイルは削除されず、ファイルへのアクセスを防ぐことができます。そして、McAfee管理者は、McAfeeのAVERT Labs脅威センターにサンプルをもらうことにより、ウィルスの発生源を調査し、ウィルス・ファイルの保全を調査できます。

•リアルタイム・アラート

様々なイベントが起こるときは、アラートが通知されます。たとえば、感染したメッセージとドキュメントがいつ検出されたか、また自動処理がいつ起きたか等。これらのアラートにより、システム管理者は絶えずシステムの監視が出来ます。



SGAV DominoはIFSのスキャンを行うSGAVの追加機能となります

•自動更新処理

McAfeeは毎日ウィルス定義をアップデートします。StandGuard Anti-Virusは直接McAfeeのインターネット・サーバからDATファイルをダウンロードするか、または内部ネットワークで指定されたコンピュータにダウンロードしたDATファイルを使用することによって、自動的にDATファイルのアップデートできます。

•スケジューリング

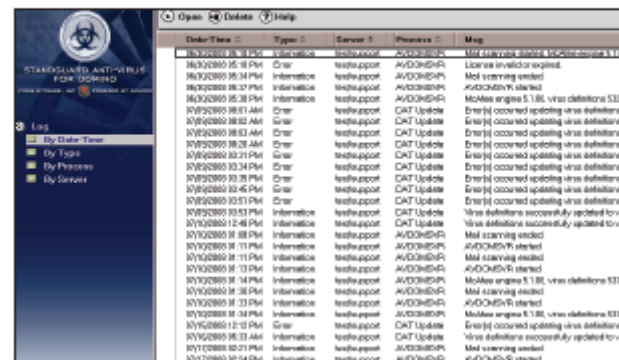
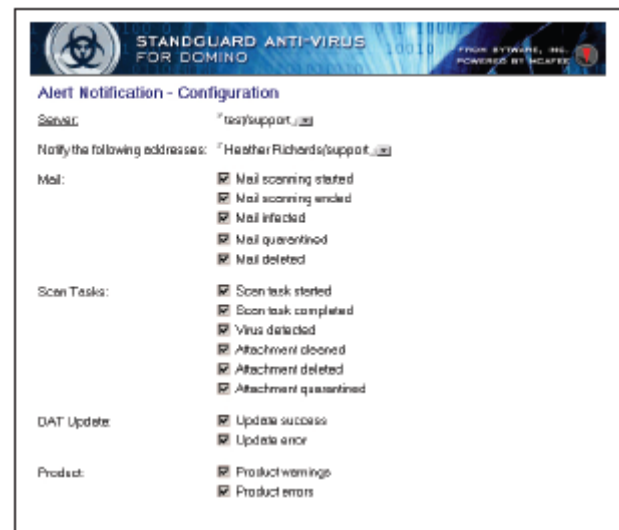
管理者は、ユーザー構成が可能な時間帯であるシステム活動が低い時間帯(夜、週末)に、自動データベーススキャンをスケジュールしたり、自動DATファイル更新を行うことができます。

•ロギング

すべての製品実行状況が、セントラル・データベースにログされます。ログ・データベースはスキャン時の情報、始動、終了、見つけられた感染データ等の情報を持ちます。ログ・データベースの情報保有期間を指定することができます。

•管理の容易さ

セントラル・管理サーバからリモートDominoサーバを構成し、管理することができます。これにより、リモートサーバを管理する時間と取り組みを短縮することに繋がります。ログデータベースは複数のサーバに起こるすべてのイベントの統合しています。従来のNotesユーザーインターフェイスに加えて、SGAV Dominoは複数のリモートサーバすべての活動を監視し、管理するのにウェブブラウザインターフェイスを提供します。





StandGuard Anti-Virusに関する詳しい情報は、株式会社ソルパック 03-3585-4639まで連絡してください。 StandGuard Anti-Virus の追加情報と無料トライアルも <http://www.solpac.co.jp>より可能となっています。

Bytware, Inc. 9440 Double R. Blvd, Suite b, Reno, Nevada 89521 usa
StandGuard® and StandGuard Anti-Virus® are registered trademarks of Bytware, Inc. © 2008 Bytware, Inc.
All Rights Reserved. [AVTP080729]