効果的な Antivirus の設定と運用
(第一部　用語説明)

--ドラフト版--

AntiVirus Configuration
第 0.1 版

SIOS

サイオステクノロジー株式会社

Copyright©SIOS Technology, Inc. All Rights Reserved

目次

はじめに.....4
I.　一般的な **AntiVirus** ソフトウェアの構成について.....5
I – 1　　集中管理コンソールと管理エージェント.....6
I – 2　　定義ファイルアップデートエージェント.....8
II.　**AntiVirus** ソフトウェアのスキャンタイプについて.....10
II – 1　オンデマンドスキャン.....10
II – 2　オンアクセススキャン.....10
II – 2 -1 linux-2.6.22 以前でのオンアクセススキャンの実装.....10
II – 2 -1 fanotify.....12
II – 3 オンデマンドスキャンとオンアクセススキャンの比較.....13

Copyright©SIOS Technology, Inc. All Rights Reserved

はじめに

2015 年から、マルウェアの一種であるランサムウェアが脅威として注目されています。これは、悪意のある攻撃者が、ユーザのデータを勝手に暗号化や改変を行い、復旧するために身代金を要求してくるというものです。特に昨今、ビットコインなど犯罪者にとっても足のつきにくい仮想通貨が実用化されたため、この仮想通貨を利用した身代金要求ということで被害件数が増加しています。

このようなランサムウェアを含むマルウェアに対応するには、やはり昔からある「AntiVirus ソフト」を利用することが最も効果的です。サイオステクノロジーでは、この AntiVirus の効果的な設定方法に関して、特に実際の日々の運用を行う上で、いわゆるウィルススキャンの種類や効果的な設計・設定方法、スキャン対象などの点について記載していきたいと思います。

第一弾の本書では、多くの AntiVirus で採用されているウィルススキャンの種類や用語に関しての説明をしてきたいと思います。

< サイオステクノロジーについて >
1997 年創業(旧社名:株式会社テンアートニー)で Java の開発、オープンソース分野で強みを持つ会社であり、サイオス（SIOS）という名前は、「SIOS is Innovative Open Solutions」の頭文字を取ったもので、"革新的な技術を活用して、オープンソリューションを提供していく"という思いが込められています。

Copyright©SIOS Technology, Inc. All Rights Reserved

I. 一般的な AntiVirus ソフトウェアの構成について

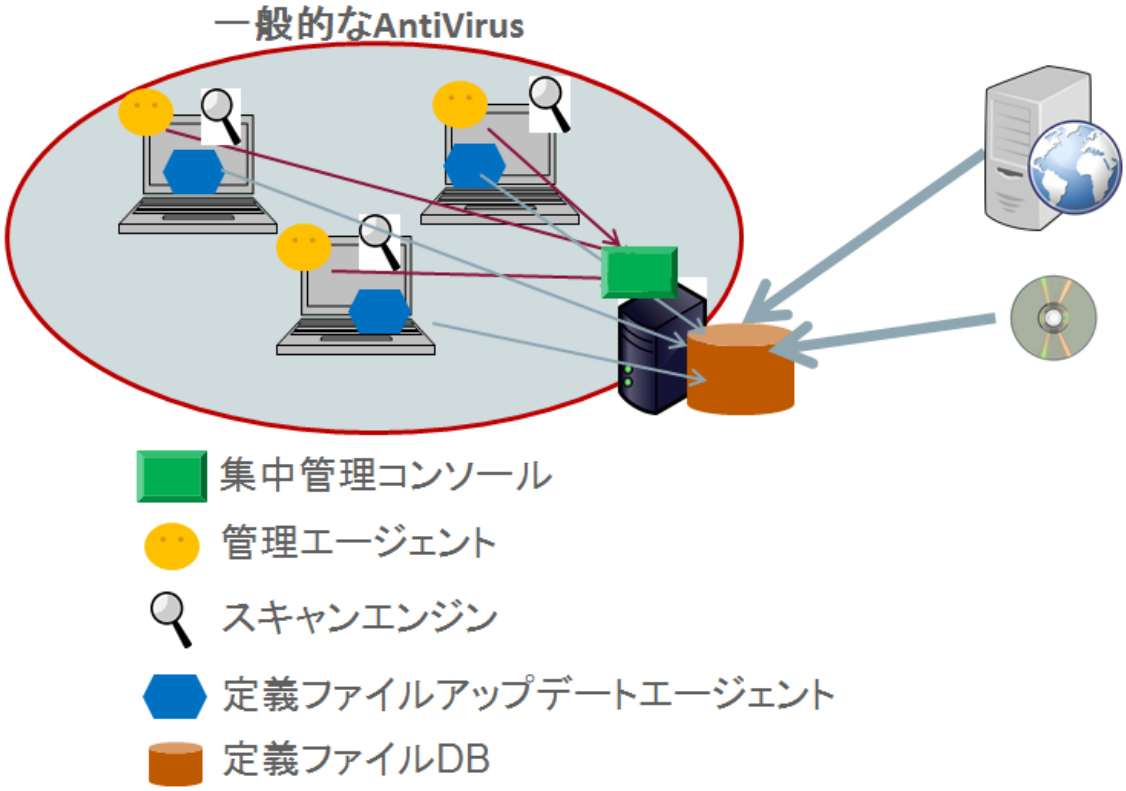
一般的なエンタープライズ向けの AntiVirus ソフトウェアは、概ね以下の５つのコンポーネントから構成されています。

- 集中管理コンソール
- 管理エージェント
- スキャンエンジン
- 定義ファイルアップデートエージェント
- 定義ファイル DB

また、通信は以下のようなものがあります。

- 管理用通信
- 定義ファイルアップデート用の通信

それぞれのコンポーネントは独立しており、万が一接続に問題が発生しても大丈夫なようになっています。



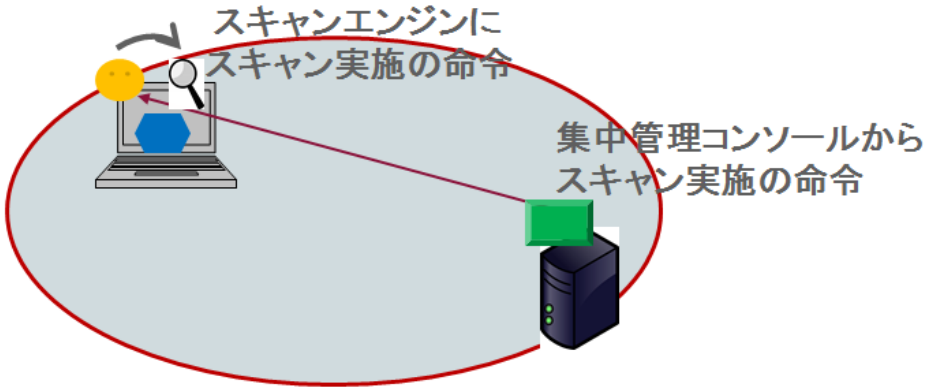
Copyright©SIOS Technology, Inc. All Rights Reserved

I - 1 　集中管理コンソールと管理エージェント

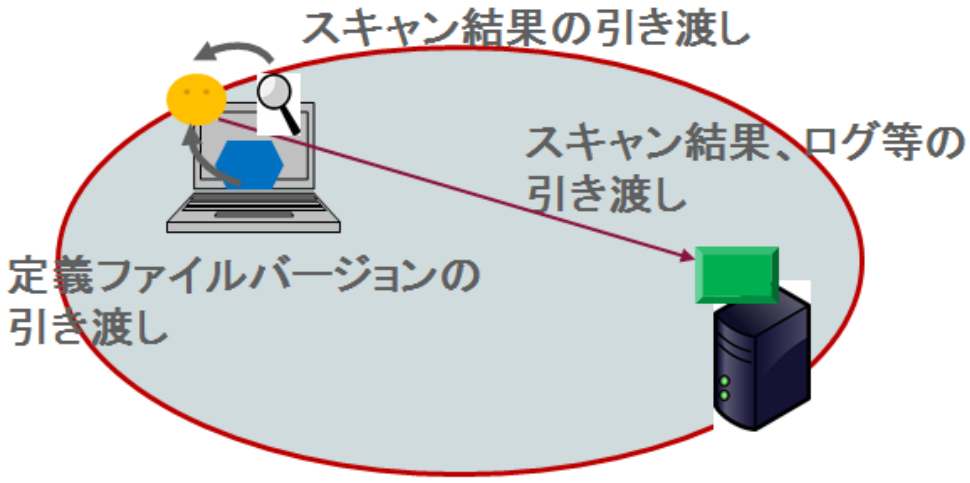
管理エージェントは各スキャン対象端末にインストールされるもので、集中管理コンソール（多くの場合 Windows が OS として使われる）と通信を行います。役割は

・集中管理コンソールからの指示を受けてスキャン対象端末で様々な動作を行う
・スキャン対象端末の情報を収集して、集中管理コンソールに送信する
となります。

動作に関しては、例えば、定期的なウィルススキャンジョブを登録したり、一回限りでスキャンを行ったり、スキャン時のオプション（除外フォルダやファイル、アクションなど）を指定したりするものです。

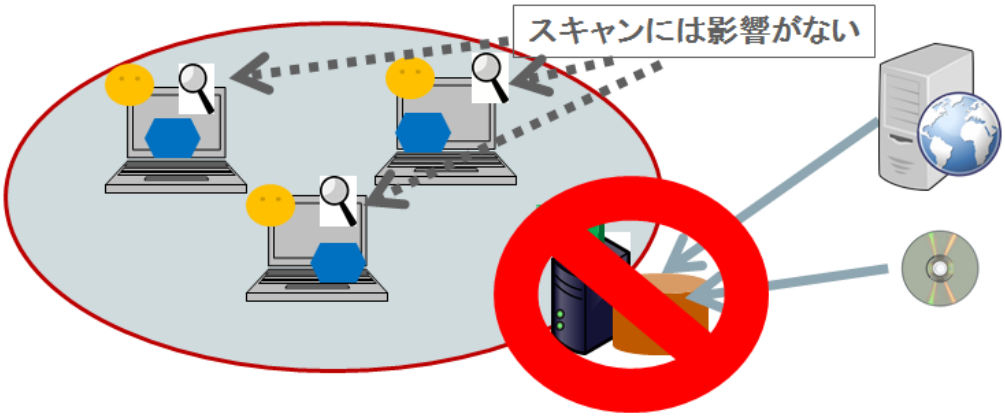


情報収集に関しては、例えばスキャンエンジンや定義ファイルのバージョン、過去のスキャンログなどを収集し、集中管理コンソールに送っています。これら送られた情報を整理・利用するため、集中管理コンソールでは DB(MS-SQL や Oracle、MySQL など)を利用してログのレポート・管理などを行っています。



Copyright©SIOS Technology, Inc. All Rights Reserved

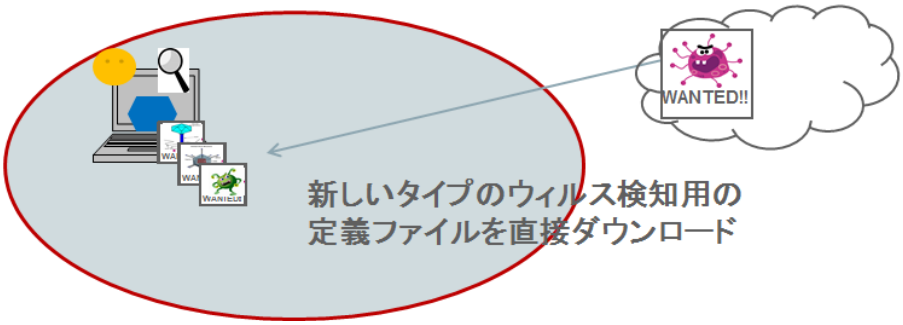
前述したように、各コンポーネントは独立しているため、スキャンを実施するスキャンエンジンと、管理エージェント・管理コンソールによる管理機構は（ジョブを受け取りますが）独立しており、管理機構に問題が発生してもスキャンエンジンは直接的影響を受けません。例えば、集中管理コンソールの方に問題が発生し、集中管理コンソールと管理エージェントが通信できなくなったとしても、スキャンエンジンは独立して動いているため、万が一インストールされているサーバにウィルスが侵入した場合でも問題なく検知ができるようになっています。
（もちろん、通信が出来ないため、ウィルスの有無は集中管理コンソールには送れませんが、ローカルにもあるログファイルに書き出しています。



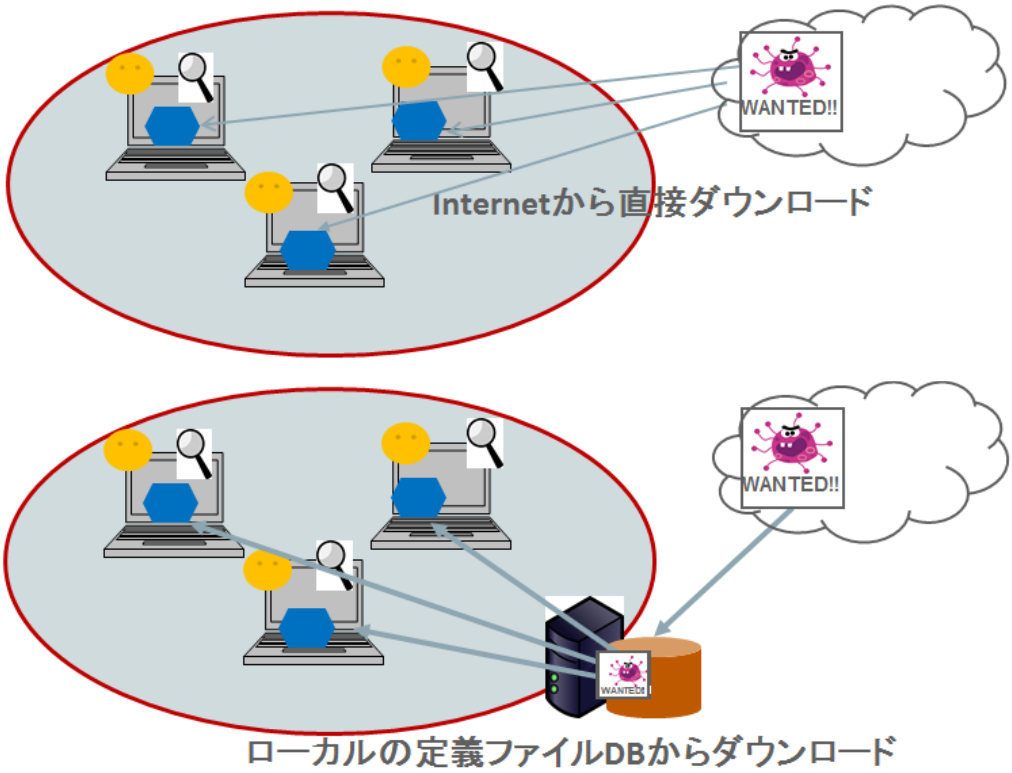
Copyright©SIOS Technology, Inc. All Rights Reserved

I - 2 □　定義ファイルアップデートエージェント

Antivirus ソフトの「定義ファイル」とは、各ウィルスのパターンが登録されたファイルであり、通常は複数の定義ファイル群から構成されています(定義ファイル DB)。新しいタイプのウィルスが確認された場合には、定義ファイル DB の中に「新しいタイプのウィルス検知用の定義ファイル」が追加され、これを更新します。また、以前配布されたウィルス検知用の定義ファイルに誤りがあった場合には、その修正されたファイルも更新されます。このように一般的には差分で提供されるため、定義ファイルのダウンロード時間はなるべく短くなるようになっています(製品によっては全体の定義ファイルを都度更新するものもあります)。

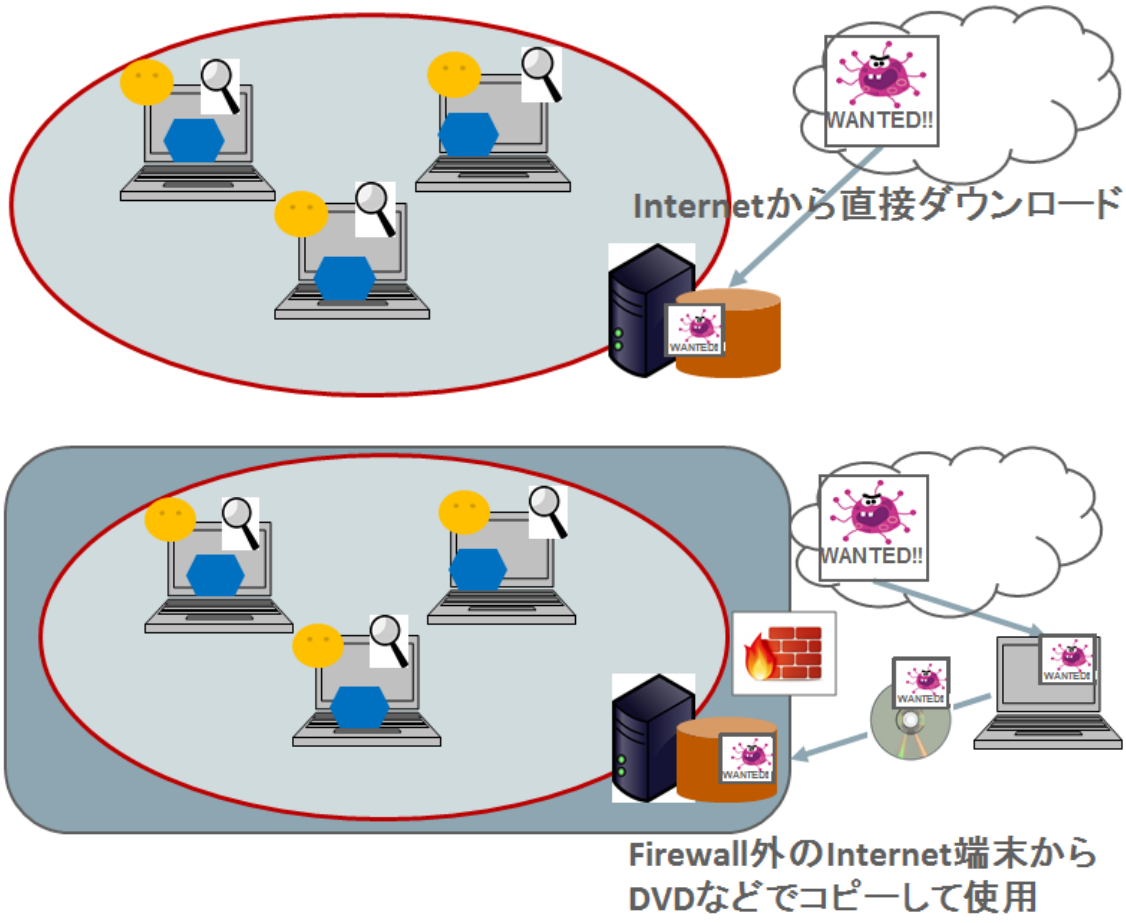


各端末上の定義ファイルアップデートエージェントは、設定により各端末が Internet 上に個別に定義ファイルを取得しに行く方法や、ローカルに置かれた定義ファイル DB から取得する方法など選ぶことが可能です。通常は、Internet への通信の流量を抑えるために、ローカルに定義ファイル DB を置くことが一般的です。



Copyright©SIOS Technology, Inc. All Rights Reserved

また、ローカルの定義ファイル DB が定義ファイルを取得する方法としては、Internet から直接ダウンロードする方法や、システム外（通常 Firewall で遮断されている外）に置かれた端末で定義ファイルをダウンロードしておき、DVD/USB などに定義ファイルを保存して、それを定義ファイル DB に入れる方法があります。後者のケースは、特に Internet から隔絶されている重要インフラ（金融系のシステムや政府のシステム、工場・研究所など、Internet に直接つなげないことでセキュリティ上のリスクを軽減する方法を取っているもの）に使われます。



Copyright©SIOS Technology, Inc. All Rights Reserved

II. AntiVirus ソフトウェアのスキャンタイプについて

AntiVirus ソフトウェアには、大きく分けて下記の 2 種類のスキャンタイプがあります。

- オンデマンドスキャン(手動スキャン、定時スキャン等とも呼ばれる)
- オンアクセススキャン（リアルタイムスキャン等とも呼ばれる）

それぞれの特徴について説明します。

II – 1 オンデマンドスキャン

スキャン対象（デバイスやディレクトリ、ファイル）を指定してスキャンエンジン等が Virus スキャンを実行するものです。オンデマンドスキャンの中でも、一度だけ手動で実行する「マニュアルスキャン（手動スキャン）」と、エージェントがＯＳのスケジューラや、自身のスケジューラを利用して実施する「定時スキャン」があります。

Virus スキャンを実行する際には、（特に圧縮ファイルなどがある場合）メモリと CPU、HDD 等のリソースをかなり使用します。そのため、一般のジョブに影響を及ぼしてしまうため、通常は業務外の時間帯（業後や休日）にスキャンを行います。

II – 2 オンアクセススキャン

プロセスからファイルを開く(open)、読む(read)、書き込む・保存(write)など、アクションが起こった際に、自動的にそれらアクセス先のファイルをスキャンエンジンがスキャンします。対象のファイルはディレクトリ単位やデバイス単位などで指定します。また、デフォルトで有効になっていて、除外フォルダを指定する製品もあります。

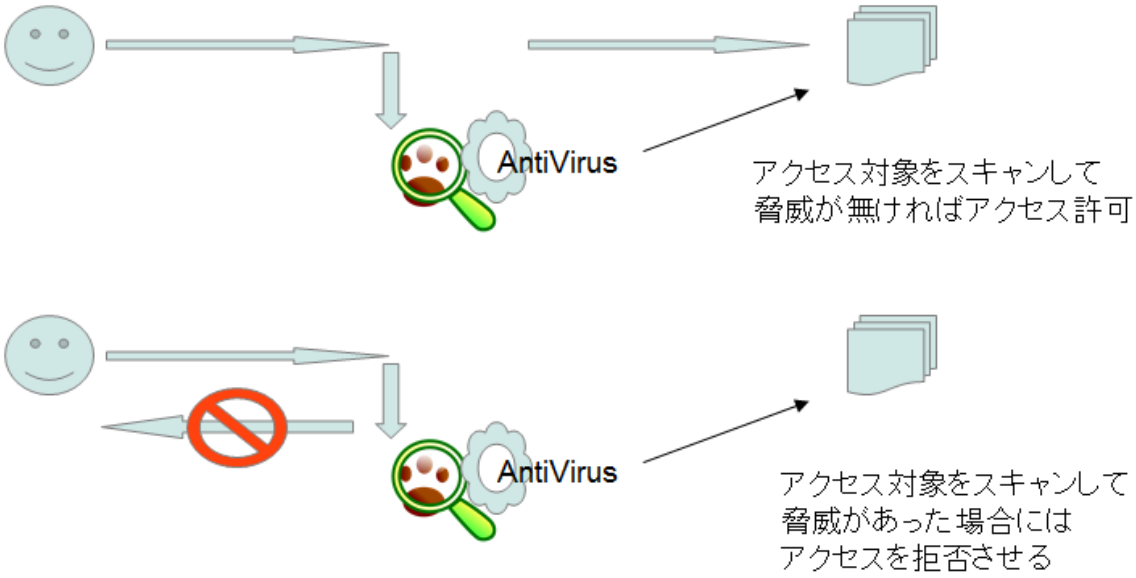
ファイルに対してのアクションをつかむために、通常 OS のシステムコールをフックして割り込みを行い、スキャンエンジンの検知結果によって対象ファイルへのアクセスを許可・拒否するアクションを行います。これにより、ウィルスを検知した際に、感染を未然に防ぐことが出来ます。

II – 2 -1 linux-2.6.22 以前でのオンアクセススキャンの実装

カーネル 2.6.22 以前の linux では、オンアクセススキャンを行うために、各アンチウィルスベンダーは LKM 形式のモジュールを使用していました。これは、Syscall Table のアドレスを上書きして、自身の処理を挟み込むことにより、ウィルススキャ

Copyright©SIOS Technology, Inc. All Rights Reserved

ンエンジンによるアクセスの可否判断に従って、アクセスしてきているプロセスに対してアクセスの許可・拒否をさせるものです。スキャンエンジンがアクセス対象ファイルをスキャンしている間は、アクセス元のプロセスは wait になっています。



ただし、この LKM 方式の場合には、いくつか問題がありました。同様の機構（ファイルシステムに何かイベントが発生した際の通知機構）を利用するアプリケーションを、同一サーバ上で使用している場合等です。例えば、Software A と Software B が同様に syscall table のアドレスをコピーして上書きしていた場合には、ソフトウェアの起動と停止を、起動順に行っていくと Syscall Table（Syscall_Table とする）が

Software Aを起動	→	Syscall_Table_A (Software AがSyscall Tableを上書き)
Software Bを起動	→	Syscall_Table_A_B (Software BがSyscall Tableを更に上書き)
Software Bを停止	→	Syscall_Table_A (Software BがSyscall Tableを開放し、自身が起動する直前の物に上書き)
Software Aを停止	→	Syscall_Table

となるため特に問題は生じないが、システムの運用上の理由など、なんらかの理由で停止順序が狂い、Software A を先に停止してしまった場合には

Copyright©SIOS Technology, Inc. All Rights Reserved

Software Aを起動	→	Syscall_Table_A (Software AがSyscall Tableを上書き)
Software Bを起動	→	Syscall_Table_A_B (Software BがSyscall Tableを更に上書き)
Software Aを停止	→	Syscall_Table (Software AがSyscall Tableを開放し、自身が起動する直前の物に上書き)

となり、Software B が上書きしていた Syscall_Table ではなく、最初の Syscall_Table に戻ってしまうため、Software A や Software B がクラッシュしてしまうことがありました。

このような、ファイルシステムにイベントが発生した際に何かを行う機構は、例えばシステム監査の目的でアクセスログを取得するようなソフトウェアが使用しています。そのようなソフトウェアがインストールされるシステムでは、セキュリティの観点上、Anti Virus ソフトウェアもインストールされているケースが多いため、実運用の際に上述のようなトラブルになるケースが起きていました。

II – 2 -1 fanotify

カーネル 2.6.23 以降では、fanotify という通知機能がカーネルに取り込まれました。これは、inotify/fsnotify の拡張で、特定の inode(つまりファイル)に対して変更が加えられた場合、ユーザ空間に通知する機構です。カーネルに取りこまれている機構によりイベントを掴むようになるため、前述のようなトラブルも起きることは無く、実運用上でより安定したシステムが提供されることになります。

Copyright©SIOS Technology, Inc. All Rights Reserved

II – 3 オンデマンドスキャンとオンアクセススキャンの比較

オンデマンドスキャンとオンアクセススキャンは、それぞれ特徴があります。下に、それぞれの比較表を示します。

	オンデマンドスキャン	オンアクセススキャン
ウィルス検知のタイミング	ウィルス感染後	ウィルス感染直前
プロセスとの衝突率	下げる方にコントロール可能	コントロール不可能
スキャン対象	特定ディレクトリ以下を漏れなく	アクセスしたもののみスキャン
安定度	安定	不安定（他のプロセスに影響する）

上記比較表の中で、特に「他のタスクに影響する」という点が注目すべき点です。これは、オンアクセススキャンがプロセスにどう影響を及ぼすかという点を理解していただければわかります。

オンアクセススキャンで通常は対象ファイルのスキャンには時間がかからないため、特に問題は起きません。しかし、

- 対象ファイルが大きく、スキャンに時間がかかる
- 対象ファイルが多段圧縮されており、展開に時間がかかる
- スキャンエンジンに問題があり、プロセスの応答が遅くなる

などがあった際には、スキャンに時間がかかってしまい、スキャンエンジン内のタイムアウトが発生します。この際には、wait しているアクセス元プロセスにはエラー（アクセス拒否）が返るため、結果としてプロセスはファイルの READ や WRITE に

Copyright©SIOS Technology, Inc. All Rights Reserved

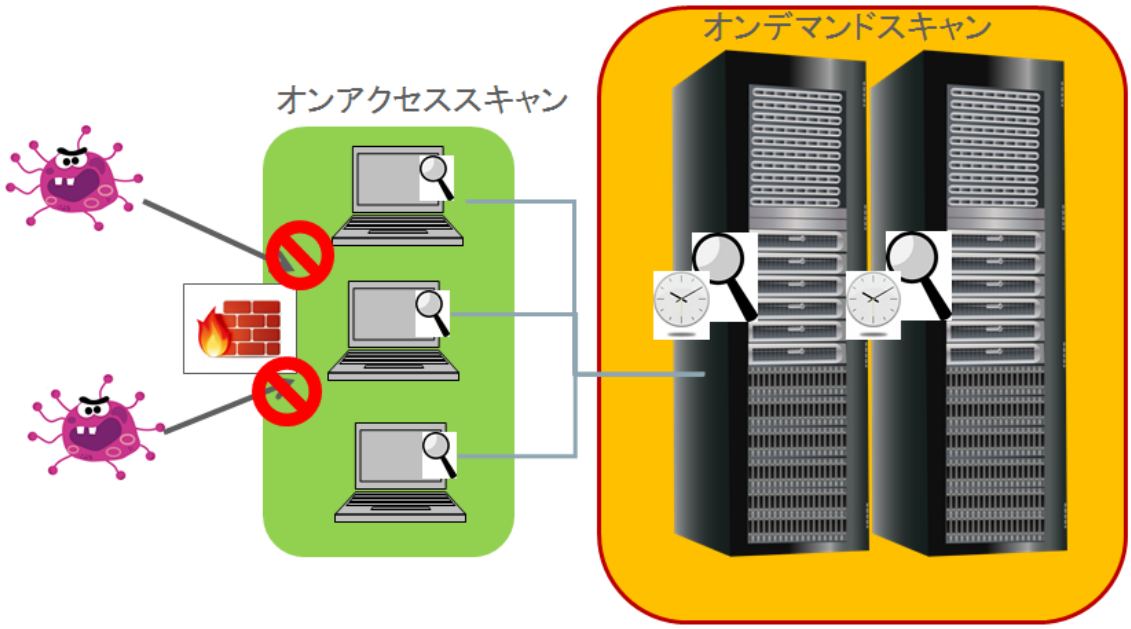
失敗してしまいます。そのため、そのファイルを構成要素としているアプリケーションの正常な動作を破壊してしまう可能性があります。

このようにオンアクセススキャンは、そのシステム上で動作しているアプリケーションの正常な動作を妨げる可能性がありますが、感染は未然に防げます。一方で、オンデマンドスキャンは自由な時間にスキャンをスケジュールできるため、他のアプリケーションが動作していない時間帯でスキャンを行うことにより、他のアプリケーションの破壊は防げますが、感染後のスキャンになってしまいます。したがって、実際のシステムで使用する際には、２つのスキャンの（オンデマンドスキャンとオンアクセススキャン）を組み合わせて使用した方が良いと思われます。

例えば、サーバ上で重要なアプリケーションが動作するようなネットワーク構成の場合には

- クライアントはオンアクセススキャンを有効にする
- Linux サーバは使用頻度が少ない時間帯にオンデマンドスキャンを行う

というシステム設計にすることにより、感染のリスクと既存アプリの破壊のリスクの双方を下げることが出来ます。



＜結論＞

本ホワイトペーパーでは、多くの AntiVirus で採用されているウィルススキャンの種類や用語に関しての説明を行いました。
今後サイオステクノロジーでは AntiVirus の性能試験や効果的な構築のノウハウ、運用方法などの技術資料を公開していきます。安全で安定した環境をご

Copyright©SIOS Technology, Inc. All Rights Reserved

検討されている皆様の手助けとなれば幸いです。

著作権

本書に記載されているコンテンツ（情報・資料・画像等種類を問わず）に関する知的財産権は、サイオステクノロジー株式会社に帰属します。その全部、一部を問わず、サイオステクノロジー株式会社の許可なく本書を複製、転用、転載、公衆への送信、販売、翻案その他の二次利用をすることはいずれも禁止されます。またコンテンツの改変、削除についても一切認められません。本書では、製品名、ロゴなど、他社が保有する商標もしくは登録商標を使用しています。

サイオステクノロジー株式会社 Red Hat 事業企画部
〒106-0047 東京都港区南麻布 2-12-3　サイオスビル
電話: 03-6401-5111
FAX: 03-6401-5112

Copyright©SIOS Technology, Inc. All Rights Reserved

URL: http://www.sios.com

Copyright©SIOS Technology, Inc. All Rights Reserved