効果的な Antivirus の設定と運用
(第三部　効果的な運用方法例)

--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

目次

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。

第三部の本書では、Linux 用/Windows 用の AntiVirus ソフトウェアがシステムに及ぼす影響を考慮した、効果的な設置方法・設定方法に関して議論していきたいと思います。第一部・第二部で AntiVirus ソフトウェアの基本的な動作と性能に及ぼす影響を議論していきましたが、それらを踏まえて通常の運用環境でどのような設置・設定・運用方法を行えば、セキュリティレベルを保ちながらシステムに及ぼす影響を少なくしていけるのかを議論していくことで、お客様に、より安定したシステムを設計・運用していいただく手助けになるのではないかと考えています。

＜　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。

I. AntiVirus ソフトウェアの構成・設定・運用に関して

第一弾で AntiVirus ソフトウェアの用語説明と代表的な構成例を説明し、第二弾で AntiVirus ソフトウェアがシステムに及ぼす影響を測定・公開しました。

AntiVirus ソフトウェアはセキュリティを一定レベルに担保しつつも、システムのパフォーマンスに少なからず影響を及ぼします。システムのパフォーマンス劣化により通常業務に支障をきたしてしまうことは本末転倒であるため、なるべくセキュリティレベルを落とさずにパフォーマンスへの影響を少なくしたり耐障害性を高めていく構成・設定・運用が必要になります。

今回は、AntiVirus の効果的な運用を行うキーポイントとして大きく
- システム構成
- スキャン対象
- スキャン方法

に分けて、説明していきます。

II. システム構成について

II－1 オンアクセススキャンとオンデマンドスキャンを使い分ける

一般的な企業では、やはり未だに Windows や MacOS がクライアントであり、Linux や Unix はサーバ用途として使われていると思われます。

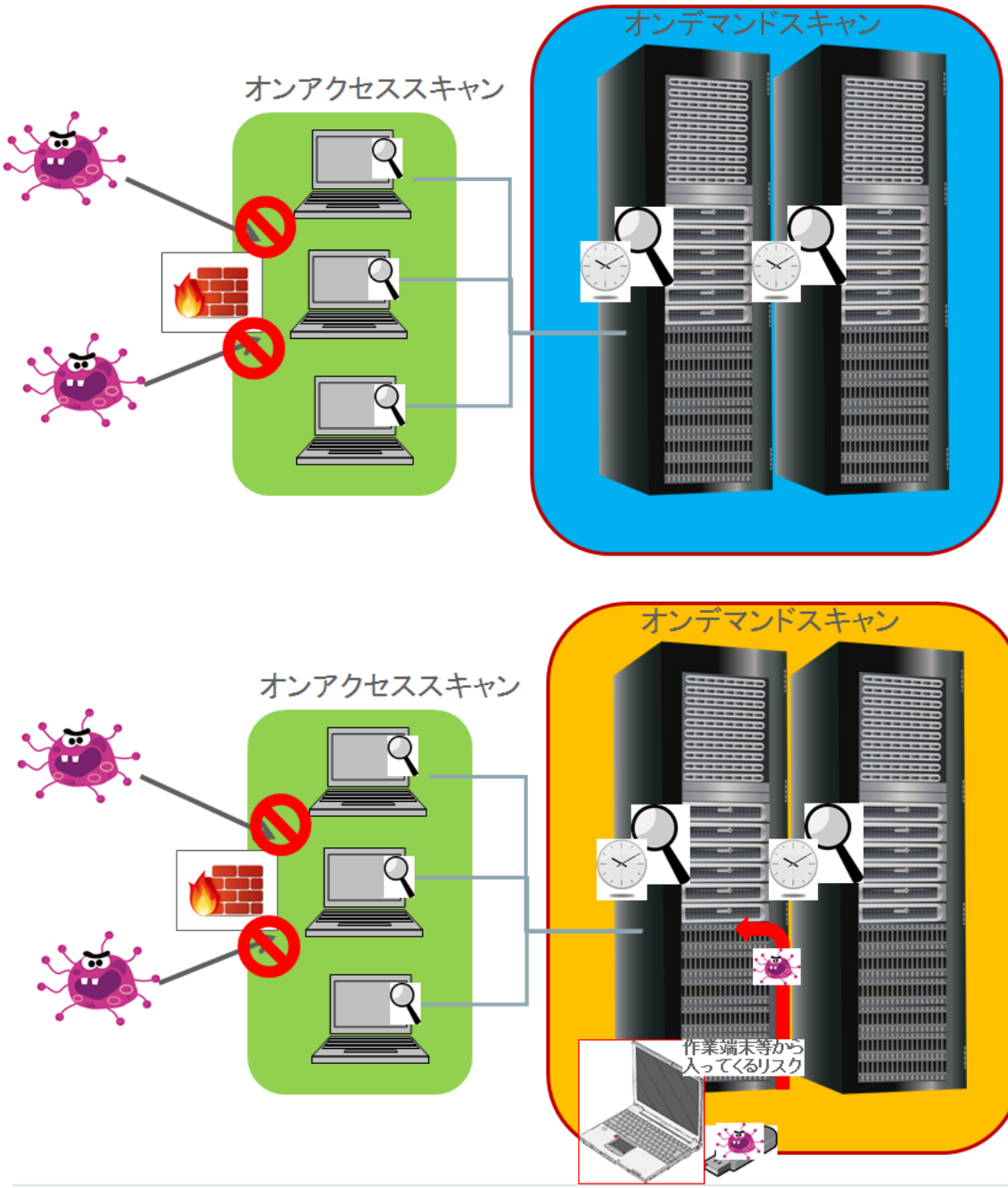
第一弾でも説明しましたが、Linux でのオンアクセススキャンはやはりシステム的にはシステムコールの書き換えを行ったりしているため、どうしても各 AntiVirus ソフトウェアメーカー独自の実装に依存せざるを得ません。

fanotify のような、Linux Kernel で用意しているファイル変更通知を元にしてスキャンを行っている場合には別ですが、古い Kernel を使用しているディストリビューション（例えば Red Hat Enterprise 6 や CentOS 6 など）をサーバ系として使用する場合には、オンアクセススキャンを行うために各社独自のモジュールを読み込ませる必要があるため、別のシステムコールをフックするようなカーネルモジュールを使う監査製品を Linux サーバ上で動作させる場合を考えると、不安定になる要因が増えてしまいます。

そのため、

- Windows や MacOS でオンアクセススキャンを行う。
- Fanotify をサポートする以前の Linux や Unix サーバ上ではオンデマンドスキャンを行う
- 最新の Linux ではオンアクセススキャンとオンデマンドスキャンの双方を走らせる。
- オンアクセススキャンは除外フォルダなどを考慮する（後の章で後述）。

という構成が一番安定した構成となります。
ただし、この場合には Linux サーバへの出入り口で全て AntiVirus ソフトウェアが動作するようにしておかないと、Linux サーバ上でオンデマンドスキャンが実施されるまでの間に Virus に感染するリスクが存在するため、対処する必要があることを忘れてはいけません。



II – 2 AntiVirus ソフトウェア各クライアントは集中管理し、社内で予め用意している専用の定義ファイル DB から更新する（個別に更新をかけさせない）。

こういう構成にするメリットは大きく二つあります。

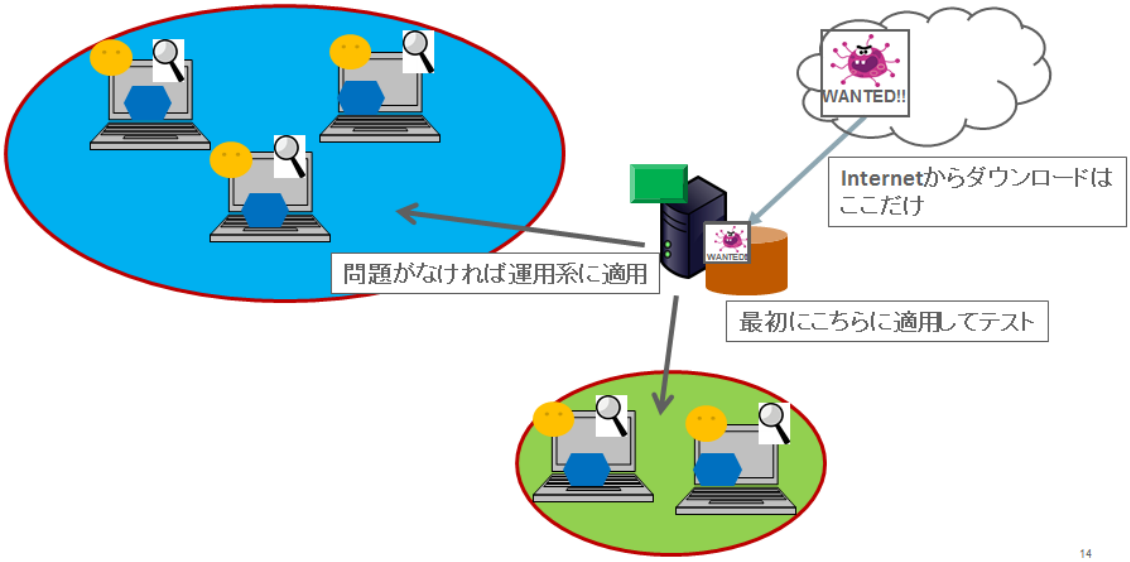
1. Network 帯域の確保
2. 更新させたいタイミングを自分で選べる

まず、1.の「Network 帯域の確保」は比較的わかりやすいと思います。現在はほとんどの企業での Network 帯域は潤沢なものが提供されているため、あまり問題にならないケースもあると思います。しかし、一定の時間（例えば、毎時間置き等）に各々のサーバが勝手にベンダーが提供している Internet 上のサーバに接続に行くのは、特定タイミングでネットワーク帯域を一定量占有することになるため、ほかの業務を圧迫する可能性があります。また、そもそも AntiVirus ソフトウェアを集中管理していないと、どのマシンがどのタイミングで更新に行くのかがわからないため、Network 帯域に一気に負荷が来るのか、バラバラに負荷が来るのかなどの予測が立てられず、対処もできません。そのため、更新は集中管理したうえで社内に予め用意しておいた DB を使うように設定しておく必要があります。

2. のメリットは一見わかりにくいと思います。しかし、AntiVirus をある程度管理したり製品に携わっていると、特定の定義ファイル・エンジンにバグが入っていることが（年に一度くらいは）発生する事が経験上わかります。勿論、AntiVirus ベンダーとしては『定義ファイル・エンジンは綿密に QA を行い、顧客に障害が発生しないようにする』と言ってはいますが、現実には年に一度くらいのトラブルは発生しています。誤検知で済む場合もありますが、アプリやサービスの停止、システムダウンにつながるケースもあります。

・ Mcafee では、2016 年 6 月に配布された DAT 8183 を適用すると、VSE Mcshield サービスが予期せず動作を停止する問題や、以降の DAT が更新できなくなる問題が発生しました。
https://kc.mcafee.com/corporate/index?page=content&id=KB87253&actp=DETAIL&viewlocale=ja_JP
・ Symantec では 2015 年 2 月に Norton の IPS 定義パッケージ 20150220.001 に欠陥があり、32bit 版 IE が使えなくなるという不具合が発生しました。
https://www.symantec.com/connect/ja/blogs/corrupt-ips-definition-package-impacted-32-bit-versions-internet-explorer
・ TrendMicro では 2015 年 8 月に、Trend Micro Deep Security でウイルスパターンファイル 11.877.00 へ更新すると、CPU が定常的に高騰したり ds_am プロセスが定期的にクラッシュする不具合が発生しました。。
https://app.trendmicro.co.jp/SupportNews/NewsDetail.aspx?id=2436
・ OSS の ClamAV では 2016/09/16 に更新された Signature22213 を使うと PDF ファイルをウィルスと誤検知するという問題が発生しました。
http://www.gossamer-threads.com/lists/clamav/virusdb/67293）

そのため、例えば『定義ファイル・エンジンはリリースされた直後は社内の情シス部門等だけに限定して適用してテストを行い、一定時間（24 時間など）経って問題が発生しない場合には運用系のネットワークに展開する』というような運用を行うことで、最新の定義ファイル・エンジンが不具合を抱えていた際のリスクを軽減し、かつ比較的新しい脅威にも対処することが出来ます。



II－3 ヘテロな環境にする

前章でも述べている通り、AntiVirus 製品は時々バグが発生します。誤検知が発生する場合から、サービスダウンにつながる状態まで様々です。そのため、万が一の事を考えて、ある程度ヘテロな（複数のベンダーの AntiVirus 製品を使っておく）環境を用意しておいた方が、誤検知やサービスダウンのリスクを減らすことに繋がります。

また、AntiVirus 製品ベンダーにはそれぞれ（製品の歴史的にも）OS による得手不得手が存在します。例えば、Windows 向けの製品と Linux 向けの製品は、検知エンジンやシグネチャの構成は同じだとしても、OS の仕組み上の違いがあります。そのため、例えば Windows 製品は A 社製品、Linux 製品は B 社製品といった風に分けるというのも一つの考え方です。

仮に予算の都合上、一種類のベンダー製品のみに統一せざるを得ない状態の時でも、少なくとも情シス部門では別ベンダーの（たとえフリーのものでも）AntiVirus 製品を用意しておいた方が無難でしょう。前述のように、運用環境で誤検知の問題が発生した場合には、その別ベンダーの製品を用いてスキャンする事で、誤検知か否かの判断が付きます。

III. スキャン対象について

III – 1 DB と DB に関係するファイルはスキャン対象から外す

- トレンドマイクロ「検索除外を推奨するフォルダやファイル」
  http://esupport.trendmicro.com/solution/ja-jp/1313316.aspx
- シマンテック「Scan exclusions for Oracle database servers running Symantec Endpoint Protection」
  https://support.symantec.com/en_US/article.TECH134383.html
- Microsoft「SQL Server を実行しているコンピューター上で実行するウイルス対策ソフトウェアを選択する方法」
  https://support.microsoft.com/ja-jp/kb/309422

などにも記載がありますが、Linux/Windows 問わず DB サーバ(Oracle, Microsoft SQL, PostgreSQL, MySQL 等)上に AntiVirus ソフトウェアをインストールしてスキャンを行う場合には、DB 及び DB に関係するファイルはオンアクセススキャン・オンデマンドスキャンの両方で、スキャン対象から除外する事を検討してください。

これには三つの大きな理由があります。

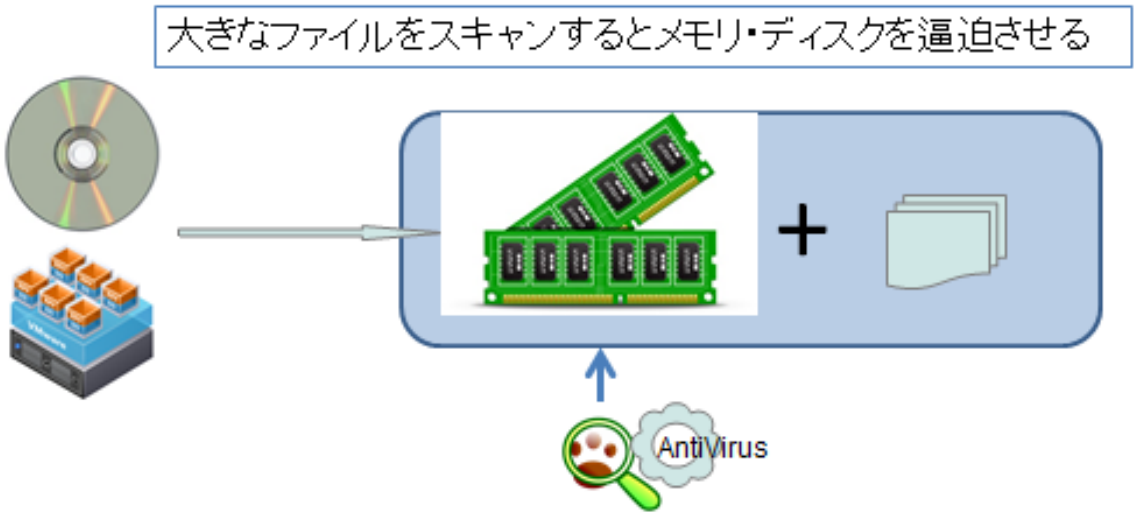
1. DB は頻繁に更新されるため、オンアクセススキャンを DB ファイルに対して有効にしていた場合には DB ファイルに対してのスキャンが頻繁に行われます。これにより、サーバのパフォーマンスが著しく劣化します。
2. 巨大な DB ファイルや Redo ログファイルなどをスキャンしてしまうと、スキャン終了までに時間がかかってしまいます。スキャン中は他のプロセスがアクセスできないようにロックしてしまうものもあるため、スキャンが終了するまで DB や Redo ログの更新が出来ず、結果的に DB が破損してしまう可能性があります。
3. 前項でも触れていますが、AntiVirus のエンジンには（頻繁ではないですが）バグが発生します。このバグにより、スキャンが異常終了してスキャン中のファイルを壊してしまうことも発生し得ます。DB や Redo ログファイルなどが破損してしまうと DB が破損してしまいます。

そもそも DB ファイルや Redo ログファイルが何らかのマルウェアに改変されてしまうと、その時点で正しい DB として起動できなくなってしまうため、マルウェア感染に使用されるということはあり得ません。そのため、DB 及び DB に関係するファイルはスキャンの種類によらず、スキャン対象から除外する事を検討してください。

III – 2 大きなファイル（ISO ファイルや仮想ディスクのイメージファイルなど）はオンアクセススキャン対象から外す

AntiVirus がファイルをスキャンする場合には、一般には予約してあるメモリ上にファイルを展開してスキャンを行い、それでも足りない場合にはテンポラリフォルダ（Linux/Unix 系であれば/tmp など）を用いて展開して後にスキャンを行います。
ここで、ISO ファイルなど 4GB を超えるようなファイルや、仮想ディスクのイメージファイルなど数十 GB を超えるようなファイルがスキャン対象に入ってしまっている場合には、テンポラリディレクトリの急激な逼迫が発生し、その他のアプリケーション・サービスに影響を与えます。また、tmpfs のようにメモリを仮想ディスクとして/tmp にマウントして使用している場合には、メモリを大幅に使用してしまい、システム全体として満足なサービスが提供できない状態にもなり得ます。

そのため、例えば ISO ファイルや仮想ディスク関連ファイルなどの大きなファイルは一定のフォルダ・ディレクトリに格納しておき、それらのフォルダ・ディレクトリ単位でオンアクセススキャンから除外し、オンデマンドスキャンで定期的なスキャンで対応するのは、システムへの影響を考えると検討する価値があります。

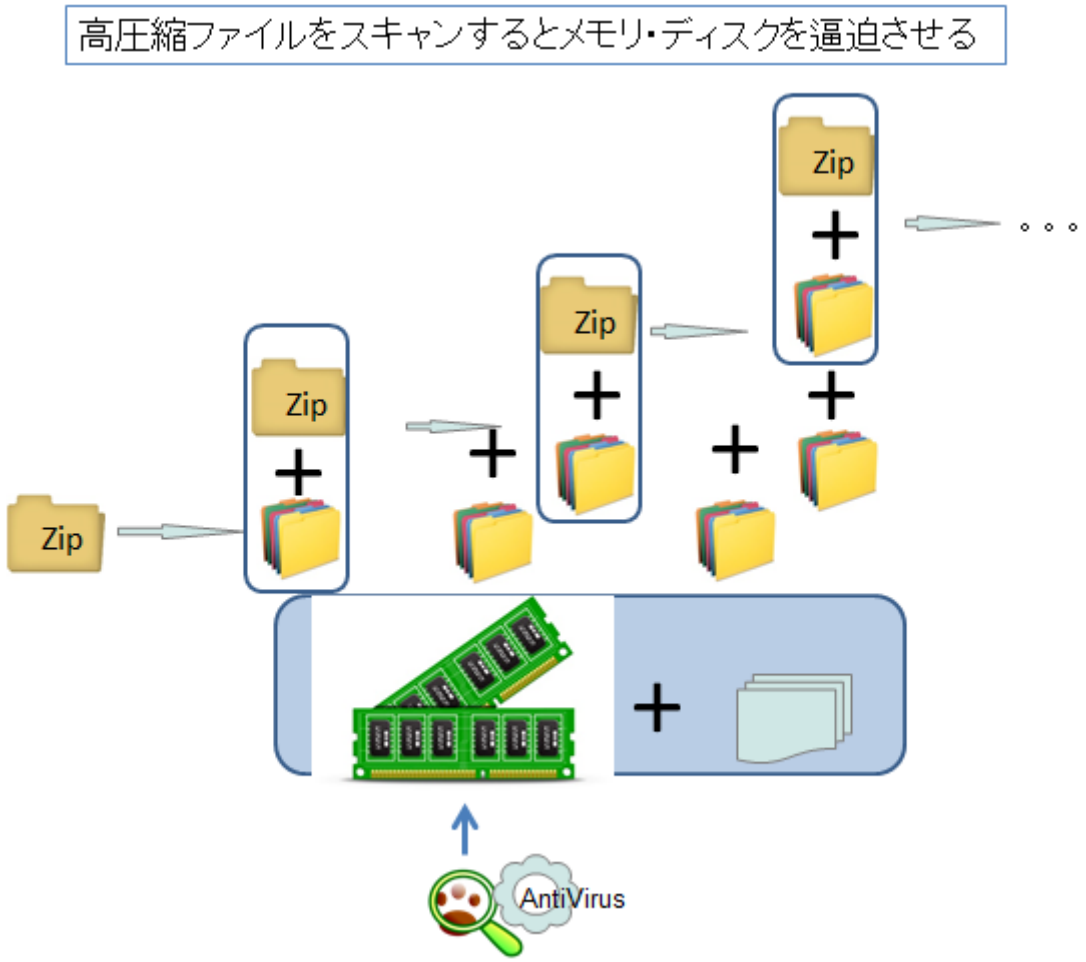


II I– 3 圧縮されたファイのスキャンは必要かどうかを考える。
第一弾の用語説明でも説明したとおり、AntiVirus ソフトウェアは圧縮ファイルをスキャンする際にメモリ上（足りなければテンポラリ領域を追加）にファイルを展開してスキャンを行います。その際、大きな圧縮ファイルであれば前項のようにファイルサイズによってオンアクセススキャンから外すということも考えられますが、その他にファイルが「高圧縮」されている場合にもメモリやディスクの残量を逼迫させる原因になります。

「高圧縮」とは、圧縮ファイルの中にさらに圧縮ファイルが入っている状態（入れ子状態）を指します。この場合には、最初の圧縮ファイルをメモリ上で展開したのちに、それを保持した上でさらに内部の圧縮ファイルを展開する為、余計にメモリを使うことになります。これが更に三階層目、四階層目、となっていけば行くほど、メモリを多く使うことになります。

実際、これを利用して「zip 爆弾（Zip Bomb）」という高圧縮ファイルを添付ファイルとして送り込み、AntiVirus でスキャンしようとしたマシンを使用不可能にしてしまう攻撃があります。例えば、”45.1 zip”と呼ばれる圧縮ファイルは見た目上 45.1kbytes しかありませんが、内部が 9 段階の多段構造でそれぞれ 1.3GB の圧縮ファイルを含む構造になっており、全て解凍すると 1.3 エクサバイトのファイルをスキャンする事になります。

この様な攻撃を避けるために、一般的な AntiVirus ソフトウェアでは
・スキャンサイズの上限
・圧縮ファイル階層の上限
が設定されています。例えば、という高圧縮ファイルを添付ファイルとして送り込み、AntiVirus でスキャンしようとしたマシンを使用不可能にしてしまう攻撃があります。
(参考) https://en.wikipedia.org/wiki/Zip_bomb



このような攻撃から防ぐため、一般的な AntiVirus ソフトウェアでは下記のような対処をしています：

・圧縮ファイルの展開するサイズの上限がパラメータなどで決められており、それ以上のサイズになる場合にはアラートを出してスキャンを中止します。

（参考）TrendMicro ServerProtect

http://esupport.trendmicro.com/solution/ja-jp/1306343.aspx

・圧縮ファイルを展開する階層の上限がパラメータなどで決められており、それ以上の階層が圧縮ファイル中にある場合には「Zip Bomb 攻撃」とアラートを出してスキャンを中止します。

(参考) Sophos Antivirus for Linux

http://sophos.usask.ca/sophos/current/docs/eng/os2_men.pdf

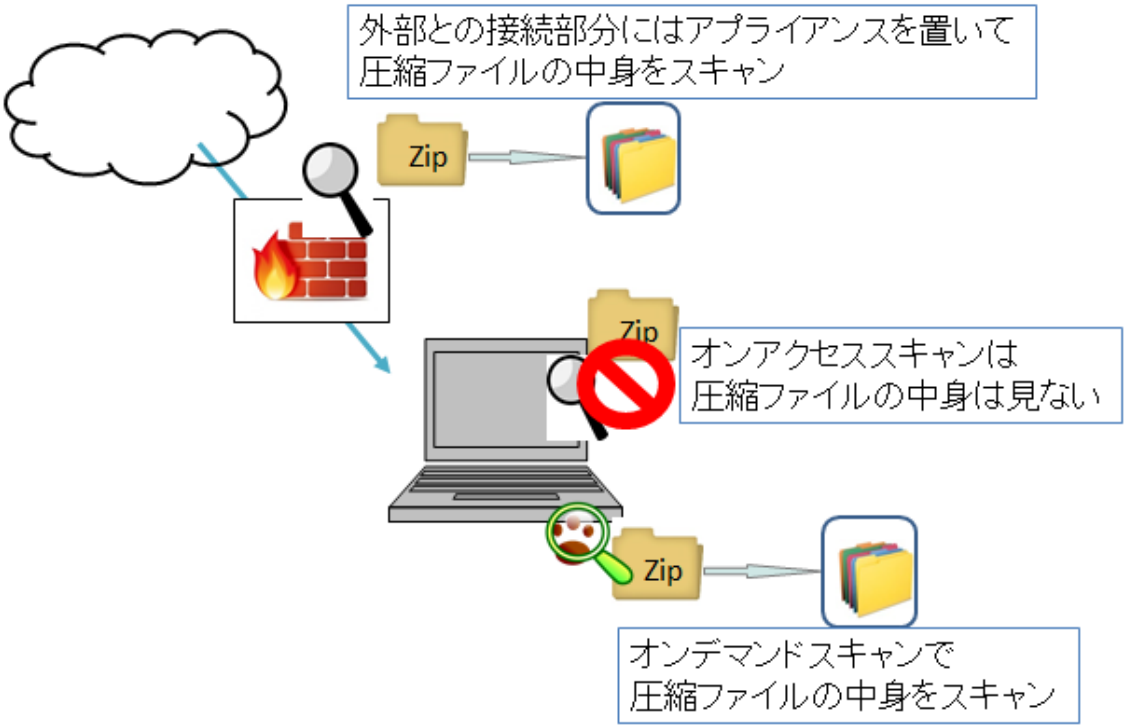
「Maximum Archive Depth」で調整（デフォルト： 16）

これらの数値は AntiVirus ソフトウェア各社のベストプラクティス値が使用されていますので、なるべく変更はしない方がベターですが、システムへの負荷が大きい場合には変更

を検討するのも一つです。

また、圧縮ファイルは中身をわざわざ展開して予めスキャンしておかなくとも、そのファイルを（スキャンのためではなく）実際に使用する際に展開を行いますので、その展開時にオンアクセススキャンが有効になっているシステム上では即座にスキャンされますので、いちいちスキャン時に中身を展開して検査しなくても良いという考え方もあります。ただ、圧縮ファイルそのものをスキャン対象外にしてしまうと、圧縮ファイル形式そのものの脆弱性を付いたような攻撃を用いたウィルス（ZIP や RAR などが近年にありました）には対処できなくなってしまいます。また、ウィルスが混入されている圧縮ファイルの多くはメールや Web のダウンロードなどを通して入ってきますので、それらの中身は専用のアプライアンスでスキャンする事でリスクをかなり減らすことが出来ます。

そこで、例えば
・オンアクセススキャンに関しては、圧縮ファイルの中身はスキャンしないことにする。
・オンデマンドスキャンに関しては、圧縮ファイルを展開してスキャンする。この際、スキャン時間やリソースとの兼ね合いから、必要であれば、圧縮ファイルサイズ上限や階層上限の値を調整する
・外部との接続部分（メールや Web）にアプライアンス型のウィルススキャン製品を置いて、圧縮ファイルのスキャン等もそちらの製品でカバーする
といった使い方を検討していただくのが良いと思われます。

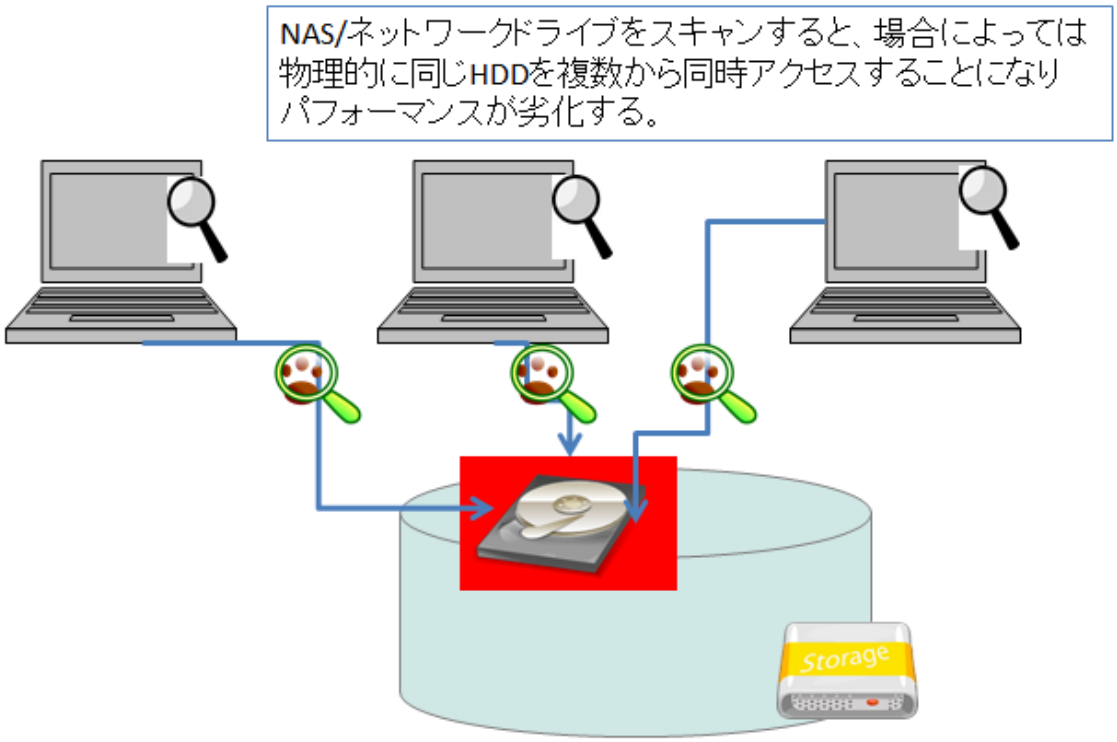


IV. スキャン方法について

IV – 1 NAS などのファイルサーバはスキャン方法を工夫する

昨今の AntiVirus ソフトウェアでは、NAS などのファイルサーバや、それをマウントしたネットワークドライブのスキャンはデフォルトで行わないようになっていますが、稀にネットワークドライブまでスキャンを行ってしまうものがあります。

この場合の問題として、例えばネットワークマウントしている端末側から見ると個別のディレクトリに見えるのですが、現実には、物理的には同じ HDD を複数から同時アクセスしていることがあります。こういう構成になってしまっている場合には、複数のマシンから同時にスキャンを行った場合に、物理的 HDD に同時に負荷が集中してしまって HDD のパフォーマンスが著しく劣化することがあります（現実としては外部ストレージも HW/SW レベルでストライピング化されたり仮想化されているため、パフォーマンス劣化は単独の HDD に比べて低いですが、やはり少なからずパフォーマンス劣化は発生します）。また、各端末には「スキャンに失敗した」旨のエラーが溜まっていくため、管理上も宜しくありません。

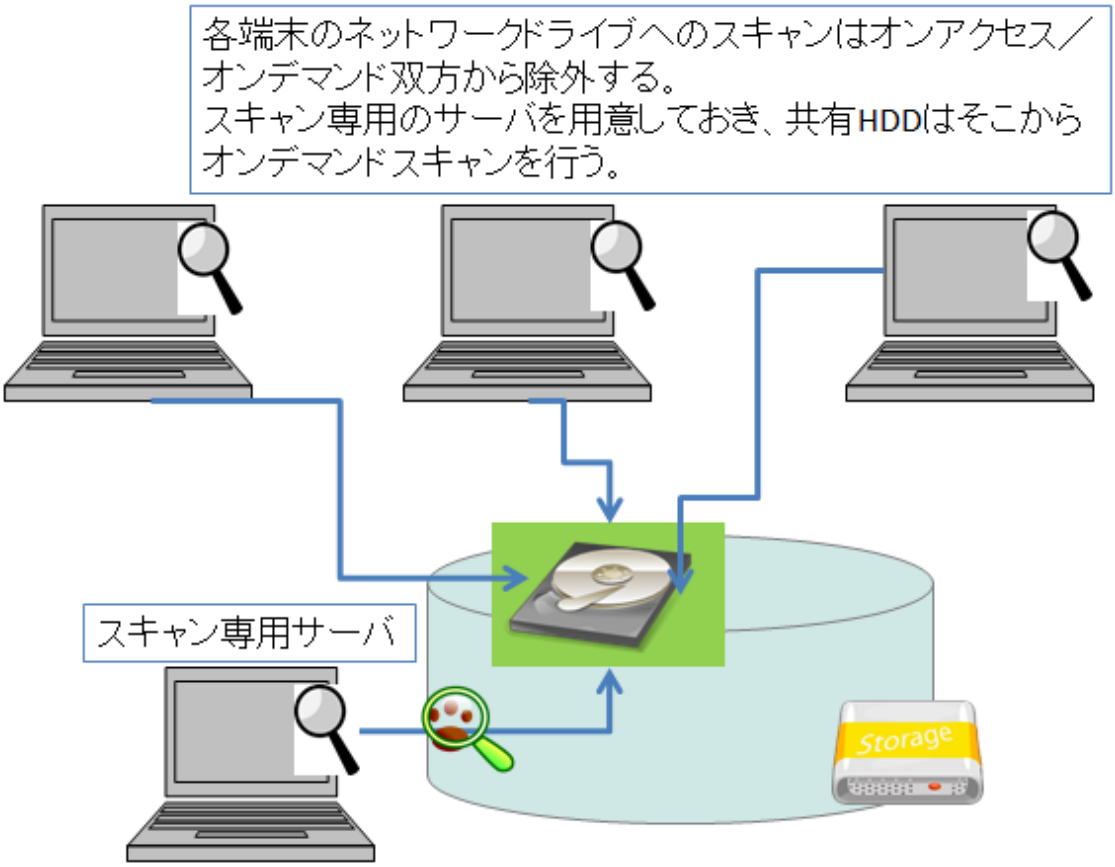


この場合には、次のような工夫でリスクを抑えながらパフォーマンス劣化を防ぐことが出来ます。

IV – 1– 1 スキャン用のサーバを別途用意して起き、オンデマンドスキャンを行う

ネットワークドライブをオンアクセス／オンデマンド双方のスキャン対象から除外しておき、別途用意したスキャン専用サーバ上からオンデマンドスキャンを行います。

長所：NAS のパフォーマンスを増加させることが出来ます。
短所：ウィルス混入時の即時検出が難しくなります（オンデマンドキャンを待つ必要があります）



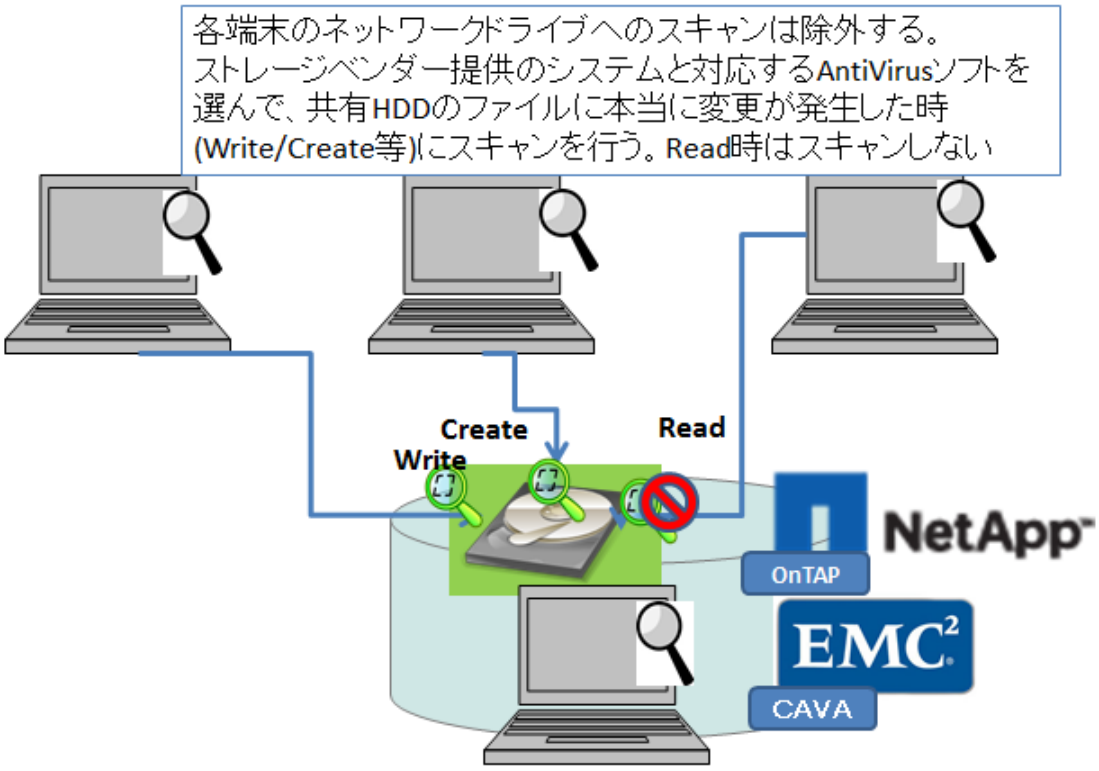
IV – 1– 2 ストレージベンダーが提供する AntiVirus インターフェースを使う

EMC や NetApp などの高価なストレージでは、ストレージベンダーの方で AntiVirus 用にインターフェースを用意してくれているものがあります。例えば NetApp などでは OnTAP、EMC では CAVA という Interface を用意しており、これと（それぞれのストレージベンダーの方でサポートしている）AntiVirus ソフトウェアを組み合わせることで

- ファイルを Open/Read した時にはスキャンせずに
- ファイルを Write/Modify した時に AntiVirus ソフトでスキャンする

という構成を作ることが可能です。

長所：NAS のパフォーマンスを増加させ、共有ディスクにウィルス混入時にも素早く対処することが出来ます。
短所：対応しているストレージベンダー・AntiVirus ソフトが必要になります（多くの場合、高価なソリューションになります。）



IV – 2 NAS のオンデマンドスキャンはスキャン方法を工夫する

NAS をオンデマンドスキャンする際には、サイズが膨大になってしまうため、フルスキャンするとかなりの時間が掛かってしまいます。通常オンデマンドスキャンは、夜間などのメンテナンス時間に行いますが、NAS の場合にはサイズによってはメンテナンス時間をオーバーして業務時間に食い込んでしまい、利便性を下げることにもなりかねません。

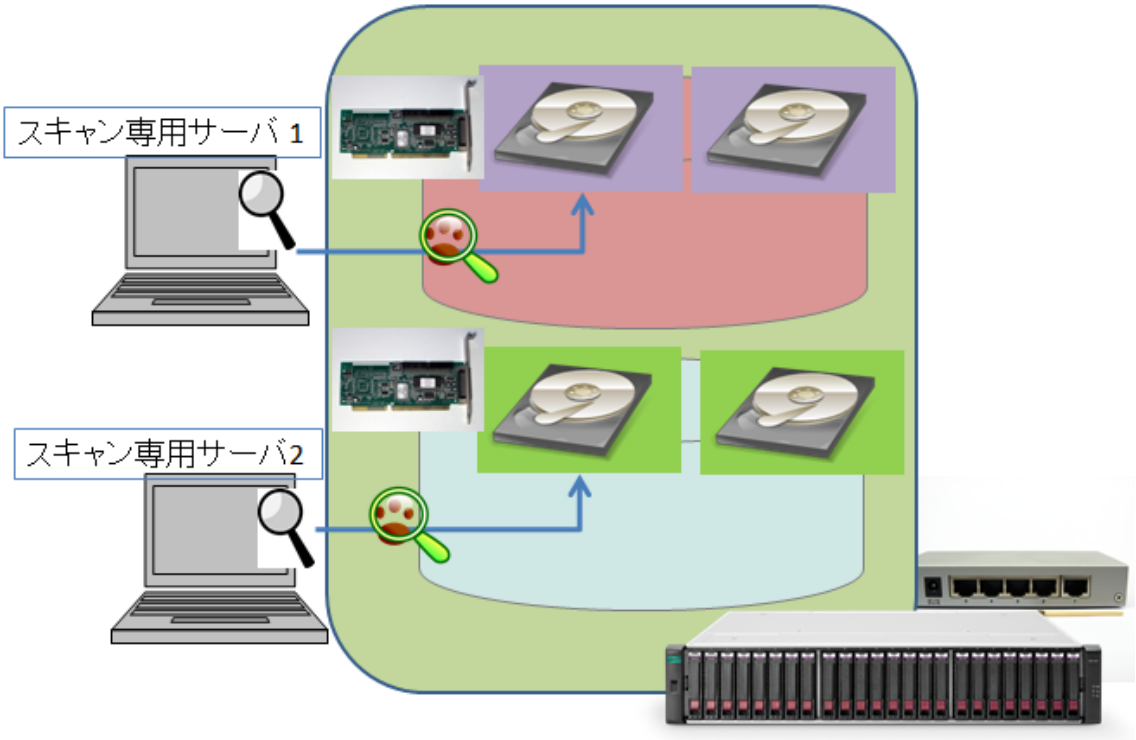
そのため、NAS をオンデマンドスキャンする際には工夫をして、スキャン時間を短縮できるようにします。

IV – 2–1 NAS のディスクは、スキャンを分散させる

NAS の共有ディスク構成を明確に（ハードレベルで）知る必要がありますが、スキャンを並列処理にすることでスキャン時間を短縮することが出来ます。

1. 繋がっている NAS で物理的に異なる HDD を使っているパーティション毎に、個別の「スキャン専用サーバ」にマウントします。
2. それぞれの「スキャン専用サーバ」からマウントした領域をスキャンします。

この際、NAS の構成にもよりますが、物理的な HDD ごとで、かつ物理的な（RAID コントローラなど I/O を制御する）コントローラ毎に分けてマウントするようにすると、I/O がうまく分散されて並列でのスキャン処理が可能になり、スキャンの短縮化につながります。

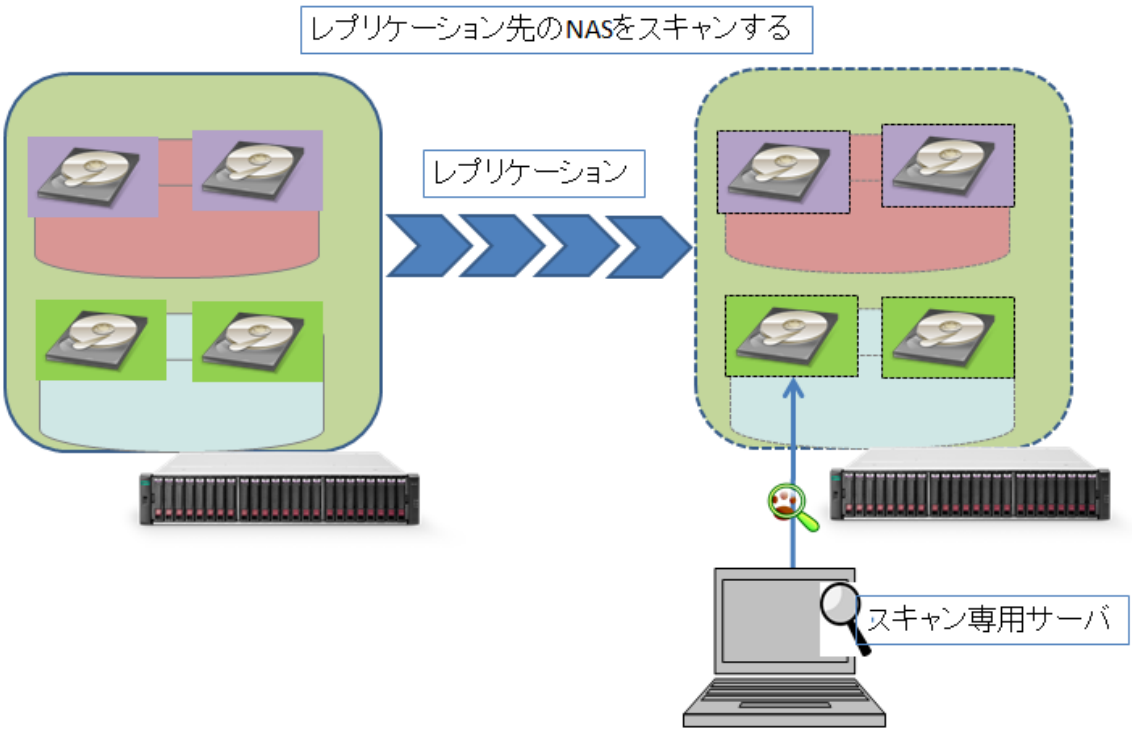


IV – 2– 2 バックアップを用いてスキャンする

これは災害対策などでディスクをレプリケーションしているときに使える方法ですが、通常のオンデマンドスキャンは、運用しているディスクではなく、レプリケーション先のディスクをスキャンするようにするという構成です。これにより

長所：オンデマンドスキャンがメンテナンス時間にとらわれることなく
実施できます。
短所：ウィルス混入時の即時検出が難しくなります（オンデマンドキャンを待つ
必要があるため、検出するまで最大で「ディスクのレプリケーションに
要した時間」＋「オンデマンドスキャン時間」のタイムラグがあります）。

昨今ではディスクの価格も下がっていることから、レプリケーションをバックアップ代わりに使用している場合も多いと思われますが、そのような構成でも使用できます。



結論

本ホワイトペーパーでは、Linux 用/Windows 用の AntiVirus ソフトウェアがシステムに及ぼす影響を考慮した、効果的な設置方法・設定方法に関して紹介してきました。

第一部で説明した構成要素を把握しながら、第二部でテストした AntiVirus ソフトウェアがシステムに及ぼす影響を考慮しつつ、今回の構成例を参考にして、実際の運用環境で AntiVirus を効果的に使用していただければ幸いです。

今後もサイオステクノロジーでは AntiVirus の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検討されている皆様の手助けとなれば幸いです。

サイオステクノロジー株式会社 OSS 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
URL: http://www.sios.com