IBM i向けウィルス対策ツール

SAVi（セイヴィー）

Security AntiVirus for i

◆「ウィルス」「トロイの木馬」の脅威

IFS上のディレクトリに共有をかけて、社員にその共有ディレクトリ上のファイルを公開している．．．

IBM i上のWebアプリケーション・サーバーを使って、インターネット取引を行っている．．．

IFS上の頻繁に参照／更新するファイルがある（EDTFコマンドなどの使用）．．．

．．．その他、IFS上のファイルを使用されるお客様はウィルス対策を行うことをお勧めします

◆背景

数年前まで、IBM iは閉鎖的な（OPENではない）環境であり、OS/400は安全なデータシステムおよびセキュリティ機能を提供してくれていました。

しかし、分散型データベース、インターネット、ウェブのテクノロジーの発展によって、IBM i においてもそれらの需要が高まってきています。

これらの技術はビジネスチャンスを広げる一方で、IBM i においてもウィルス感染などのセキュリティ・リスクがさらに高まる状況となってしまいました。

IFS（IBM iのディレクトリ構造ファイルシステム）上のファイルを通してクライアントPCにウィルスが感染する、といったことが例として挙げられます。

◆ SAVi はウィルスの脅威からあなたを守ってくれます

IFSオブジェクト・スキャン

IFS(PCファイルが保存できる領域)上に「ウィルス」「トロイの木馬」「悪質コード」などが存在していないかを検索し、発見しだいそれらを隔離します。
スキャン完了後、スキャン結果(サマリー情報)をログとして確認することができます。

リアルタイム検知

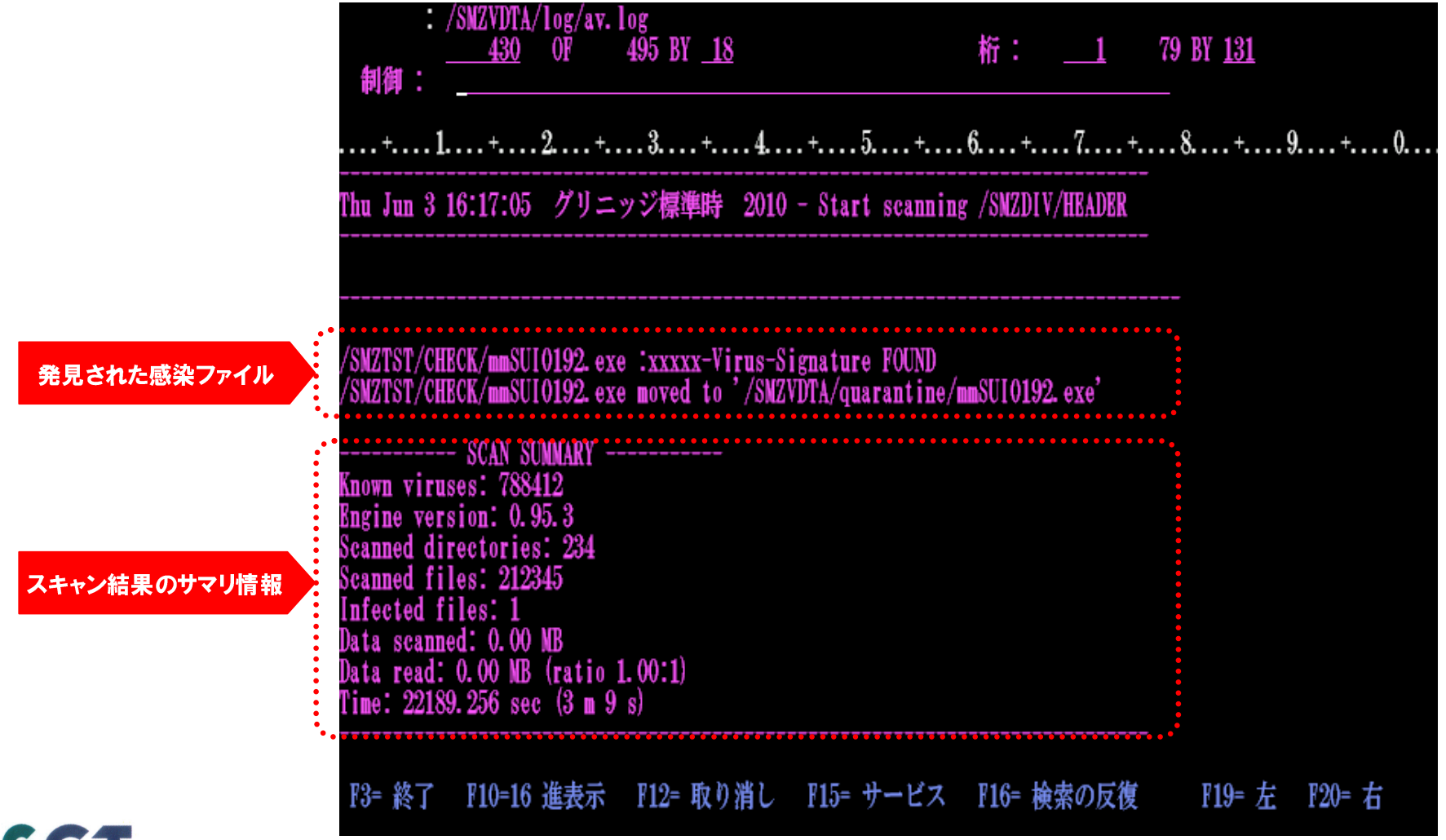
■ IFS上のファイルOPEN時のチェック

IFS上のウィルス感染ファイルをOPENしようとした場合(ファイル共有[Net Server]、EDTF etc...)、それを検知しユーザーのアクセスを拒否します。
ウィルスが検知されたファイルは感染ファイルとしてマークされ、以後OPENできなくなるため、感染の拡大を防ぐことができます。

■ メールのウィルス・チェック

悪質コードを含むメールが送信された場合、受信先に届いてしまう前にSAViが検知するため、感染の拡大を防ぐことができます。

◆スキャン結果はサマリ情報で確認できます



◆リアルタイム検知

◆こんな運用が可能です

スキャンは自動で実行が可能なの？

自動実行機能(スケジュール実行)が用意されています。例えば、毎日2:00にスキャンをかけるといった運用が可能です。

特定のディレクトリだけのスキャンは可能なの？

スキャン対象のディレクトリを指定することができます。また、スキャンしたくないディレクトリがある場合はOMIT(除外)することも可能です。

ウィルスのパターンファイルはどうやって更新するの？

インターネットにつながる環境であれば、パターンファイル(ウィルス定義ファイル)を自動で更新させる機能があります。また、インターネットにつながっていない環境でも、クライアントPCから手動で更新する方法もあります。

◆ 保全性検査

保全性

権限のない者による変更や改ざんからデータを保護することを指します。 権限のない者が情報を勝手に受信したり変更したりするデータ改ざんというセキュリティー上のリスクからシステムを保護できます。

Nativeオブジェクトの保全性チェック

Native(ライブラリ、オブジェクト[*LIB、*CMD、*PGM　etc…])に関して、以下のような保全性をチェックします。

- ◆ コマンドが悪用されている
- ◆ オブジェクトに無効なディジタル署名がある
- ◆ オブジェクトがそのオブジェクト・タイプに対して誤りであるドメイン属性をもっている
- ◆ プログラムまたはモジュール・オブジェクトが改ざんされている
- ◆ ライブラリーの属性が悪用されている

◆ 保全性検査の結果

```
                        Work with Suspicious Objects
                                          Position to library . . .  _________
Type options, press Enter.                Omit confirmed objects  .  *NO
  1=Select  3=Confirm  4=Quarantine  5=Display  8=Recreate pgm  9=Disconfirm

Opt Library     Object       Type       Owner        Violation  Confirmed
 -  SMZ8_25SYS  DSPJOB       *CMD       SECURITY1P   BADSIG     *NO
 _  SMZ8_25SYS  DSPMSG       *CMD       SECURITY1P   BADSIG     *NO
 _  SMZ8_25SYS  ENDRQS       *CMD       SECURITY1P   BADSIG     *NO
 _  SMZ8_25SYS  SIGNOFF      *CMD       SECURITY1P   BADSIG     *NO
 _  SMZ8_25SYS  SNDMSG       *CMD       SECURITY1P   BADSIG     *NO
 _  SMZ8_25SYS  TFRSECJOB    *CMD       SECURITY1P   BADSIG     *NO
 _  SMZ8_25SYS  WRKJOB       *CMD       SECURITY1P   BADSIG     *NO
 _  SMZ8_32SYS  DSPJOB       *CMD       SECURITY1P   BADSIG     *NO
 _  SMZ8_32SYS  DSPMSG       *CMD       SECURITY1P   BADSIG     *NO
 _  SMZ8_32SYS  ENDRQS       *CMD       SECURITY1P   BADSIG     *NO
 _  SMZ8_32SYS  SIGNOFF      *CMD       SECURITY1P   BADSIG     *NO
 _  SMZ8_32SYS  SNDMSG       *CMD       SECURITY1P   BADSIG     *NO
 _  SMZ8_32SYS  TFRSECJOB    *CMD       SECURITY1P   BADSIG     *NO
 _  SMZ8_32SYS  WRKJOB       *CMD       SECURITY1P   BADSIG     *NO
                                                                 続く ...
F3=Exit    F7=Subset    F15=Information
```

BADSIG:

ディジタル署名が正しくありません

※上記は開発中の画面です

ありがとうございました

お問い合わせは、弊社営業部
sales@sct.co.jp まで

http://www.sct.co.jp/