



Network & Security Solution Provider

HP Quarantine System 情報提供サービス

Vol.2.2

2008/8/19

ジェイズ・コミュニケーション株式会社

情報提供サービス担当

Hpqu-info@jscom.co.jp

J's Communication Co.,Ltd.

目次

目次

1. 「情報提供サービス」とは
2. 情報提供サービスの内容
 2. 1. 情報提供サービスの内容 (Basicサービス)
 2. 2. 情報提供サービスの内容 (Advancedサービス)
 2. 3. 情報提供サービスの内容 (Advanced Plusサービス)
3. 情報提供サービスのご提供形態
4. サービス選択

1. 1. 情報提供サービスとは

「情報提供サービス」とは・・

HP Quarantine Systemの検疫ポリシー作成において、迅速にかつ正確にセキュリティ更新情報を入力するため、ポリシー作成フォーマット(CSV)にて提供される最新の情報提供データです。

- 毎日更新されるアンチウィルスのパターンファイル情報を管理者にいち早く提供することを目的とします。
- Microsoft更新プログラムの更新情報を提供し、ポリシーマスターの作成をお手伝いします。

- ① 「情報提供サービス」の提供形式
データ提供サービスASP形式でのCSVデータの提供(ポリシー作成フォーマット)
年間定額制でのサービス課金
- ② 情報提供サービスのご提供形態
2. 「情報提供サービスのご提供形態」をご覧ください。

【ご注意】

この情報提供サービスには、HP Quarantine Systemの設定・操作・運用支援などの保守サービスは含んでおりません。

日本ヒューレット・パッカード株式会社の提供する「製品保守サービス」をご契約のお客様のみの限定サービスです。

1. 2. 情報提供サービスの利用シーン

「情報提供サービス」が活用されるシーン…



「情報提供サービス」を利用すると自動的にポリシーの元になるデータを作成できます

アンチウィルスパターンファイル情報 (Basicサービス)

- CSVでQuManagerに自動取り込み (ポリシーマスター)
- 必要なポリシーを設定して有効化
- シマンテック、トレンドマイクロ、マカフィーの複数を設定可能

Microsoft更新プログラム情報 (Advancedサービス)

- CSVでQuManagerに自動取り込み (ポリシーマスター)
- 必要なポリシーを設定して有効化
- WSUSに提供される更新情報をそのまま活用

Microsoft更新プログラム情報 (Advanced Plusサービス)

- Microsoftの更新プログラムをOSのセキュリティ更新のみ選択
- 必要なポリシーを設定して有効化
- 最低限必要なセキュリティ更新情報のみを適用可能

1. 3. 情報提供サービスの利用シーン(アンチウイルス)

「情報提供サービス」が活用されるシーン…



「情報提供サービス」を利用すると自動的にポリシーの元になるデータを作成できます

アンチウイルスパターンファイル情報 (Basicサービス)

- CSVでQuManagerに自動取り込み(ポリシーマスター)
- 必要なポリシーを設定して有効化
- シマンテック、トレンドマイクロ、マカフィーの複数を設定可能

【ご注意】

- 情報提供サービスでは、Web情報に公開されるパターンファイル情報を自動取得しておりますが、各アンチウイルス製品のバージョンにより適用されるシグネチャが異なる場合があります。詳しくは、各メーカーのWebサイトを参照してください。

シマンテック

Web情報【日次更新】に対応
(【日次複数回更新】【週次更新】には対応していません。)

トレンドマイクロ

Web情報【最新パターンファイル】に対応

マカフィー

Web情報【企業向け製品の定義ファイル・エンジンのバージョン】に対応

運用パターンの参考例

- アンチウイルスのシグネチャ(パターンファイル)を日付指定で検疫制御する。
例)1週間以上古いパターンなどを排除
 - 大型連休後に最新のシグネチャ(パターンファイル)を強制的にダウンロードさせるポリシーにする
例)最新パターンファイルをHP Quarantine System側で自動有効化する設定にして強制的にUpdateさせる。
 - 更新履歴のないメーカーの更新履歴を独自に作成して運用する
例)シマンテック、マカフィー
(トレンドマイクロ社は最新10パターンのみ公開)
- など運用ができます。

1. 4. 情報提供サービスの利用シーン (Microsoft更新情報)

「情報提供サービス」が活用されるシーン…



運用パターンの参考例

- 社内PCのバージョンが多岐にわたるため、検疫ポリシーが作れない。
例) Windows OSのサービスパックごとに【OSのセキュリティ更新】のみをポリシー化
 - 社内のWSUSの更新ポリシーをHP Quarantine System検疫ポリシーで活用
例) WSUSで管理された更新情報を【OSのセキュリティ更新】のみ抽出しHP Quarantine System検疫ポリシーとして作成
- など運用ができます。

「情報提供サービス」を利用すると自動的にポリシーの元になるデータを作成できます

Microsoft更新プログラム情報 (Advanced Plusサービス)

- Microsoftの更新プログラムをOSのセキュリティ更新のみ選択
- 必要なポリシーを設定して有効化
- 最低限必要なセキュリティ更新情報のみを適用可能

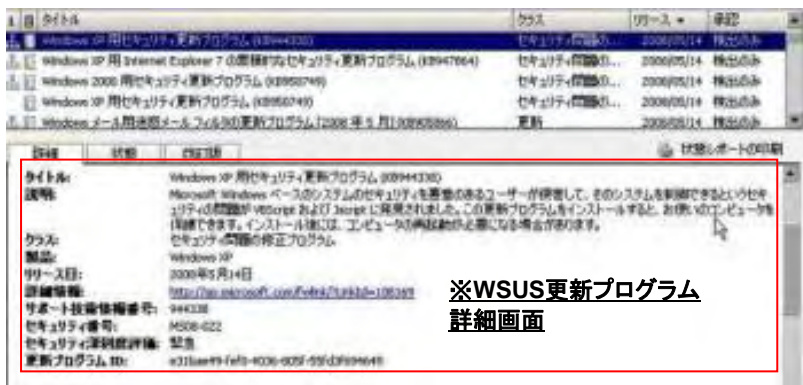
【ご注意】

- Advanced Plusサービスでは、WSUS (Windows Server Update Services) を元にしたMicrosoft更新プログラム情報を独自のロジックにより【OSのセキュリティ更新】を抽出してご提供しております。
- 【OSのセキュリティ更新】のロジックは、Microsoft社より唯一提供されている定義フォーマットを元に判定しております。
(詳しくは、Advanced Plusサービスの項をご参照ください)
<http://www.microsoft.com/japan/technet/security/bulletin/revsbwp.mspx>
- Advanced Plusサービスのお申し込み時には、Advancedサービスを含みます。(『サービス選択』の項をご参照ください)

1. 5. 情報提供サービスの利用シーン(WSUS利用ユーザー)

「情報提供サービス」が活用されるシーン・・・(WSUSを利用している企業ユーザー)

WSUSで更新される「更新プログラム」リストを「検疫ポリシー」に活用できます



Microsoft更新プログラム情報 (Advancedサービス)

- CSVでQuManagerに自動取り込み(ポリシーマスター)
- 必要なポリシーを設定して有効化
- WSUSに提供される更新情報をそのまま活用

情報提供サービスAdvancedサービスに含まれる情報

- WSUSにダウンロードされる更新プログラムの詳細情報(製品(OS)にサービスパック情報を付加)

Microsoft WSUSの「更新プログラム」情報にサービスパック情報を付加してご提供

- Microsoft WSUSでは、製品(OS)にサービスパック情報がありません。そのため、更新プログラムの適否が検疫ポリシーとして判断できない。

【Advanced サービス】の情報を参考にWSUSの更新プログラムを検疫ポリシーとして適用可能

※WSUS(Windows Server Update Services)2.0 Sp1に対応

1. 6. 情報提供サービスの利用シーン(WSUS利用ユーザー)

「情報提供サービス」が活用されるシーン・・・(WSUSを利用している企業ユーザー)

WSUSで更新される「セキュリティ問題の修正プログラム」を「検疫ポリシー」に活用できる分類でのご提供

Microsoft WSUSの運用と検疫ポリシーの違い

●Microsoft WSUSでは、【重要な更新】【セキュリティ問題の修正プログラム】などのクラスを各PC個別にサーバーが自動選別しているため、検疫ポリシーとして共通の更新プログラムが判断できない。

WSUSには【自動インストールの承認】をクラス(【セキュリティ問題の修正プログラム】【重要な更新】など)で分類していますが、各PCの環境が統一されていない場合、検疫ポリシーには利用できない場合が想定されます。

(例:【セキュリティ問題の修正プログラム】には、OS以外のIE、OE、DirectXなども含まれるため、各PC環境によって適用される更新プログラムに違いが出る)



【Advanced Plusサービス】の情報を参考に最低限必要(OSのセキュリティ更新情報)な更新プログラムのみを検疫ポリシーとして適用

Microsoft更新プログラム情報 (Advanced Plusサービス)

- Microsoftの更新プログラムをOSのセキュリティ更新のみ選択
- 必要なポリシーを設定して有効化
- 最低限必要なセキュリティ更新情報のみを適用可能

【ご注意】

- 【OSのセキュリティ更新】のロジックは、Microsoft社より唯一提供されている定義フォーマットを元に判定しております。
<http://www.microsoft.com/japan/technet/security/bulletin/revsbwp.mspx>
(詳しくは、Advanced Plusサービスの項をご参照ください)
- Advanced Plusサービスのお申し込み時には、Advancedサービスを含みます。(『サービス選択』の項をご参照ください。)

※WSUS(Windows Server Update Services)2.0 Sp1に対応

1. 7. 情報提供サービスの利用シーン(WSUS非利用ユーザー)

「情報提供サービス」が活用されるシーン・・・(WSUSを非利用の企業ユーザー)

WU(Windows Update)で検出される内容をAdvanced Plusサービスを使用して活用

WU(Windows Update)の運用にも一部活用可能

- WU(Windows Update)、【重要な更新】を適用。
- 検疫ポリシーにはAdvanced Plusサービスの情報を適用。

WUを採用している企業ユーザーでは、各PCが自動的に判断する更新プログラムがUpdateされます。
その中には【セキュリティ問題の修正プログラム】以外も含まれるため更新プログラム適用の管理ができません。



【Advanced Plus】サービスでは、実際にWindows Updateによってフィルタリングされた更新プログラム(セキュリティ問題の修正プログラム)のみを抽出しているため、共通した更新プログラムのみを検疫ポリシーとして選択することが可能です。

Microsoft更新プログラム情報 (Advanced Plusサービス)

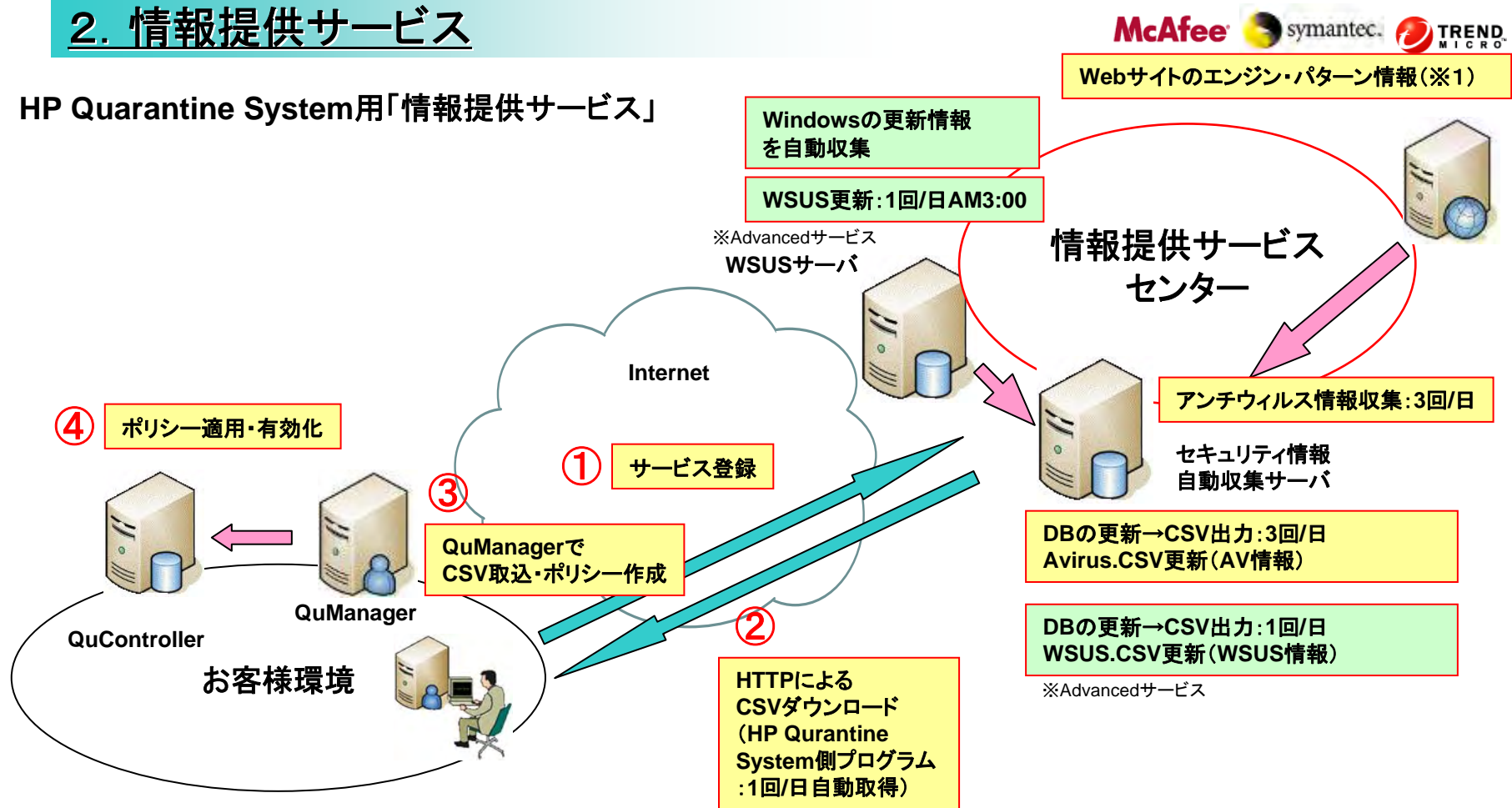
- Microsoftの更新プログラムをOSのセキュリティ更新のみ選択
- 必要なポリシーを設定して有効化
- 最低限必要なセキュリティ更新情報のみを適用可能

【ご注意】

- 【OSのセキュリティ更新】のロジックは、Microsoft社より唯一提供されている定義フォーマットを元に判定しております。
<http://www.microsoft.com/japan/technet/security/bulletin/revsbwp.mspx>
(詳しくは、Advanced Plusサービスの項をご参照ください)
- Advanced Plusサービスお申し込み時には、Advancedサービスの内容を含みます。(『サービス選択』の項をご参照ください)
- Microsoft Update(MU)には対応していません。

2. 情報提供サービス

HP Quarantine System用「情報提供サービス」



※1 : 情報提供サービスの内容(アンチウイルス)参照

2. 1. 情報提供サービスの内容(Basicサービス)

Basic(基本)サービス

1. アンチウイルス・ソフトウェアの更新内容を提供

基本サービス:【選択できる範囲】

アンチウイルス・ソフトウェアの次のメーカーの更新情報(毎日)

- ① シマンテック
- ② トレンドマイクロ
- ③ マカフィー



アンチウイルス情報 取得先Webサイト

シマンテック(日次更新)

- ① URL <http://www.symantec.com/region/jp/avcenter/defs.download.html>
- ② 取得項目

ウイルス定義ファイル作成日
 ウィルス定義ファイルリリース日
 ウィルス定義ファイルバージョン
 シーケンス番号
 拡張バージョン番号
 ウィルス対策済み数

シマンテック(週次更新)について

シマンテックの提供する【週次更新】は、法人向け全製品が【日次更新】に対応するようになったため提供を終了しております。

http://service1.symantec.com/support/inter/japanesecustserv-ent.nsf/jp_docid/20070418220533961?Open&dtype=corp

2. 1. 情報提供サービスの内容 (Basicサービス)



アンチウイルス情報 取得先Webサイト

トレンドマイクロ

① URL <http://jp.trendmicro.com/jp/support/download/pattern/index.html>

② 取得項目

バージョン (パターン)

リリース日



アンチウイルス情報 取得先Webサイト

マカフィー

① URL <http://www.mcafee.com/jp/default.asp>

② 取得項目

定義ファイルバージョン

エンジン番号

2. 2. 情報提供サービスの内容(Advancedサービス)

Advancedサービス

1. Microsoftの更新プログラム(HOTFIX)の更新内容をご提供



Advancedサービス

Microsoft更新プログラム情報の提供(毎日更新)

Windows Server Update Services

- ① 同期スケジュール: 同期時刻AM3:00毎日
- ② 対象OS製品

製品: Windows 2000 Sp4, Windows XP Sp2, Sp3

Windows Vista 初期出荷版, Sp1

注1) サーバー製品およびその他のOS製品については、更新プログラム情報の提供はありません。(Microsoft社のサポート期限終了製品の更新はありません)

- ③ Service Pack情報付加、情報確認のため、マイクロソフトのリリース日より1~2日後に提供。

※Microsoft社のセキュリティ情報は通常、米国日付の毎月第2火曜日に公開。日本では、時差の関係上、毎月第2火曜日の翌日(第2水曜または第3水曜)に公開

<http://www.microsoft.com/japan/security/relsched.msp>

2. 3. 情報提供サービスの内容(Advanced Plusサービス)

Advanced Plusサービス

1. Microsoftの更新プログラム(HOTFIX)更新内容からOSに限定した更新プログラムを抽出して提供

[定義]

- ① Microsoftセキュリティ情報(詳細)の定義された項目(Technetの該当サイトの詳細情報)から下記の条件を「OSに限定したセキュリティ更新」としています。
 - ② セキュリティ情報概要:
「このセキュリティの対象となるユーザー:「Microsoft Windowsをご使用のお客様」
「影響を受けるソフトウェア: (OSのサービスパック名称)」
「影響を受けるコンポーネント: (記載なし またはOSのサービスパック名称)」
 - ③ それ以外の記載(IE、DirectX、WMPなどの各バージョン)がある場合には、OS以外のコンポーネント、アプリケーション用のセキュリティ更新のため採用されません。
 - ④ 情報提供サービス側で実際に更新プログラムのインストールを実施したもののみを抽出
- 参考URL: <http://www.microsoft.com/japan/technet/security/bulletin/revsbwp.mspx>

Advanced Plusサービス

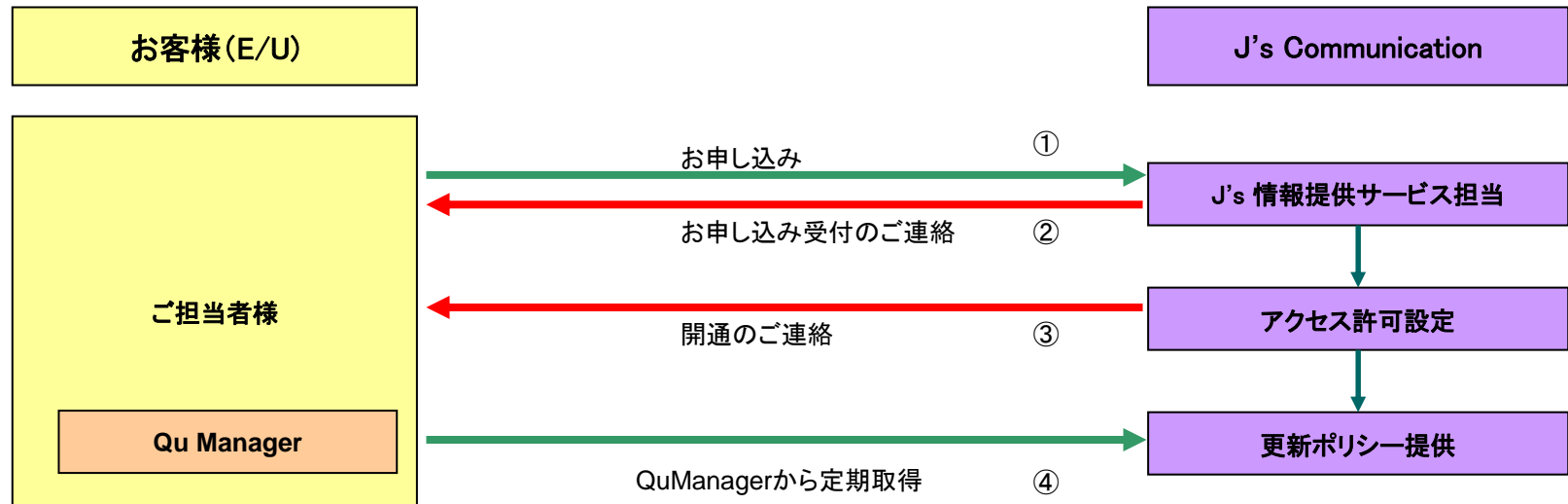
Microsoft更新プログラム情報および「OS限定セキュリティ更新」の提供

Windows Server Update Services

- ① 同期スケジュール: 同期時刻AM3:00毎日
- ② 対象OS製品: マイクロソフト更新サポート対象製品
製品: Windows 2000 Sp4, Windows XP Sp2, Sp3, Windows Vista 初期出荷版およびSp1
注1) サーバー製品およびその他のOS製品については、更新プログラム情報の提供はありません。
(Microsoft社のサポート期限終了製品の新しい更新は提供されません)
- ③ Service Pack情報付加、情報確認のため、マイクロソフトのリリース日より1~2日後に提供。

3. 情報提供サービスのご提供形態

情報提供サービスのご提供形態



4. サービス選択

情報提供サービスの選択

情報提供サービスの選択 (契約ユーザ単位1QuManager)

Basicサービス (アンチウイルス)	Advanceサービス (WSUS)	Advanced Plusサービス (WSUS+Policy)	説明
○	—	—	アンチウイルス更新情報のみ必要な場合
—	○	—	Microsoft更新情報(全件)のみ必要な場合
—	N/A	○	Microsoft更新情報(OSセキュリティ更新)のみ必要な場合 (Advancedサービスを含みます)
○	○	—	アンチウイルス更新+Microsoft更新(全件)のみ必要な場合
○	N/A	○	すべてのサービスを選択

サービス料金につきましては、別途価格表をご参考ください。
お申し込みの際には、別途弊社担当者より見積もりさせていただきます。