

@Solomon Virus check plug-in / SPA-PRO Mail @Solomon Enterprise カスペルスキーアンチウイルスチェックエンジン (Ver.7) アップデートプログラム適用によるプログラム変更内容と注意点

2008.10.03

@Solomon Virus check plug-in シリーズのユーザー様各位 SPA-PRO Mail @Solomon Enterprise

現在、ご利用中のアンチウイルス機能のプラグインを組み込んだ SPA-PRO Mail @Solomon シリ ーズに対して、カスペルスキーアンチウイルスチェックエンジン(Ver.7)アップデートプログラ ムを適用した結果のプログラム変更内容と注意点は次の通りです。

#### 1. アップデートプログラムの年内適用作業をお願いします

アンチウイルス機能のプラグインを組み込んだ SPA-PRO Mail @Solomon シリーズをご利用 中の場合、アップデートプログラムの適用は 2008 年 12 月末までに必ず行ってください。変更 されることになった理由と概要は次の2をご覧ください。また、変更しなかった場合にどのよ うな状態になるのかは、下の5をご覧ください。

#### 2. アンチウイルスエンジンが Ver.4 から Ver.7 へ変更されます

SPA-PRO Mail @Solomon シリーズに組み込んだプラグインの「アンチウイルス機能」が変更になります。アンチウイルス機能は、ウイルススキャン機能とパターンファイル更新機能に 大別されます。

変更されることになったきっかけは、カスペルスキー社から提供されているアンチウイルスエ ンジンのライブラリ Ver.4 サポート終了と Ver.4 が利用しているパターンファイルのデータベ ース更新が 2008 年 12 月末までと、告知された事情に起因します。そのため、アンチウイルス エンジンについて、Ver.4 から Ver.7 を利用したエンジンに変更する作業を施しました。今回提 供されるアップデートプログラムをユーザー様が適用することによって、Ver.7 を利用したエ ンジンに差し替わります。

### 3. ウイルススキャンの仕組みも見直し約2倍の高速化がされています

この機会に合わせてウイルススキャンの仕組みも根本から見直し、Ver.4 のアンチウイルスエ ンジンを使った(2008年9月までにリリースされている)@Solomon Virus check plug-in を 組み込んだ SPA-PRO Mail @Solomon と比較すると、約2倍の高速化をはかりました。なお、 アンチウイルス機能利用時のメモリ消費量は、従来バージョンとほぼ同等です。

### 4. パターンファイルダウンロードサイトも変更されます

Ver.7 を利用したエンジンに変更したことと連動して、カスペルスキー社のパターンファイル をダウンロードするサイトが変更されました(※1)。それにともない、@Solomon Virus check plug-inを組み込んだSPA-PRO Mail @Solomon シリーズ側でもウイルスパターンファイルを ダウンロード・格納するフォルダ名を変更しました(※2)。また、パターンファイルダウンロ



ードの記録ログの内容が簡素化されました。

5. Ver.4 用のパターンファイル更新は 2008 年 12 月末までです

カスペルスキー社提供のウイルスパターンファイルダウンロードサイトについては、<u>Ver.4 の</u> アンチウイルスエンジンを利用した従来版では、2008 年 12 月末まで更新が保証されています が、それ以降は保証されなくなります。 そのため、できるだけ早めにアップデートプログラム を適用くださるようお願い申し上げます。

万が一、Ver.4 のアンチウイルスエンジンを利用した従来版 @Solomon Virus check plug-in を組み込んだ SPA-PRO Mail @Solomon シリーズのご利用を続けられた場合、2009 年 1 月以 <u>降、パターンファイルの更新がされなくなる見込みです。</u>パターンファイルの更新が止まる前 に、アップデートプログラムをできるだけ早い時期に適用してください。アップデートプログ ラムを適用すれば、Ver.7 へのアンチウイルスエンジンが組み込まれ、合わせてパターンファ イルダウンロードサイトも下記の(※1)の通り、自動的に変更されます。

(※1)新しいダウンロードサイトは、次の通りです。ただし、このサイトは、カスペルスキー社が将 来的に変更しないことを保証しているものではありません。また、ダウンロードサイトは予告な しに変更されることがあります。

dnl-00.geo.kaspersky.com

dnl-19.geo.kaspersky.com (連番部分 00-19 のうち、20 カ所からランダムに選択)

- (※2) パターンファイルのダウンロード時に、従来バージョンで利用されていたフォルダ、および新 バージョンで利用するフォルダは次の通りです。
  - (旧) [プラグインインストールフォルダ] ¥data
     [プラグインインストールフォルダ] ¥modified-date
     ↓
     (新) [プラグインインストールフォルダ] ¥Bases



# カスペルスキーアンチウイルスチェックエンジン (Ver.7) アップデートプログラム適 用方法について

従来の差分アップデート適用方法とほぼ同等です。

(SPA-PRO Mail @Solomon シリーズ)

- (1). "SPA-PRO Mail Control"画面を開き、[サービス制御] タブにある"SPA-RS","VMCS"サービス(※)を停止。
  - (※) @Solomon Virus check plug-in を組み込んでいるときは、"VMCS"サービスはこの画面に なく、「@Solomon Virus check plug-in」-「プラグイン管理」を開いて表示される画面の最 下部分にある「サービス制御」でサービスを停止してください。
- (2). "SPA-PRO Mail Control"および" SPA-PRO Account Manager"を閉じる。
- (3). ダウンロードした zip ファイル "Vengine2B@Solomon-7.0.3.33a.zip"を解凍し、アップデートプログラム "E-POST Virus Engine Changer 2B for Solomon.msi"を実行。
- (4). プラグインインストール済みのドライブ・フォルダを事前に確認しておき、上書き更新される ように、インストール先フォルダを指定して実行。
- (5). "SPA-PRO Mail Control"を開き、停止したサービスを再開する。
- (6). 別記指定された方法やパターンファイルダウンロード記録ログなどでバージョンを確認する。 ちなみに、今回のアップデート適用をしても、[バージョン情報] タブに表示されるバージョン 表記は変わりません。



## アップデートプログラム適用後の動作確認

アップデート適用を行った後は、「バージョン情報」タブでのバージョン表記は変わりませんが、 下記の部分で違いが出てまいりますので、問題なくアップデートが適用されたかどうかを確認する 方法として確かめてください。

 タスクマネージャを起動し、「全ユーザーのプロセスを表示する」状態にすると、従来バージョンにはなかった "epostavs.exe" というプログラムが稼働していることを確認できます。 この "epostavs.exe" は、サービスプログラムではありませんが、パターンファイル更新のサ ービスプログラムである VMCS( "modifys.exe")の従属プログラムとして動作しているものです。

イメージ名	1-1	ザー名	CPU	X刊使用。	
ctfmon.exe	Adm	inistrator inistrator	00	484 K 1 620 K	
epstavs.exe	SYS	TEM	00	736 K	
EpstControlexe	Adm	Administrator		6,272 K	
EPSTIM <sup>*</sup> 1.EXE	SYS	TEM	00	3,692 K 3,524 K	
EPSTPO"1.EXE	SYS	SYSTEM		3,884 K	
Epstralexe	SYS	SYSTEM		4,852 K	
explorer.exe	Adm	Administrator Administrator		4,464 K	
explorer.exe	MOM			0,044 N	
Inetinitation	100	AL CEDUTOE	00	1 006 V	
learn ave	SVS	TEM	00	9748 K	
Manager eve	Adm	inistrator	00	6594 K	
modifysiere	SYS	TEM	00	1.840 K	
mediciexe	NET	NETWORK SERV		4 756 K	
mysald-intexe	SYS	TEM	0D	6,280 K	
namediexe	SYS	TEM	0D	5.456 K	
dsendexe SYSTEM		TEM	00	0440 1/	-

(画面は E-Post シリーズの場合)

 パターンファイルダウンロード時に動作するプログラム "autoupdate.exe" が 1.07 から 2.10 にアップしました。パターンファイルダウンロード記録ログを確認すると、"autoupdate.exe" のバージョン表記を確認することができます。パターンファイルダウンロード記録ログは、従 来通り、[プラグインインストールフォルダ (既定値が C:¥plug-in-Kasp)] ¥log に保管され ます。



(新バージョンの記録ログ)(画面は E-Post シリーズの場合)

🚺 080910.log - メモ株	
ファイルの 厚美田 書式図 表示の ヘルブロ	
[08:49:0] E-Post Autoupdate v2.10 Copyright 2004-2008 E-POST Inc. All rights reserved.	-
[08:49:08] Key check., success. [D8:49:08] mPath = C:YPROGRA IYEPOSTYMS [08:49:08] mKaysBase = C:YPROGRA IYEPOSTYMSYbases [D8:49:08] mProxy = [] [08:49:08] connect	
[08:49:28] Download Ok.	-

(従来バージョンの記録ログ)(画面は E-Post シリーズの場合)

D80910.log	- ¥ŧŧ	
77-11(E)		
[17:45:2] Copyright 2	E-Post Autoupdate v1.07 004-2006 E-POST Inc. All right	s reserved.
[17:45:29] [17:45:29] [17:45:29] Shared File [17:45:29] [17:45:29]	Key check success. mPath = C:YPROGRA IYEPOSTYMS mKavsBase = C:YProgram Files¥C sYBases mProxy = [] connetct Site 4 (updates).	⊐ Common Files¥KAV
[17:45:40] ¥EPOST¥MS¥c [17:45:40]	Download C:¥PROGRA~1 lata¥avomhk5.mhk.\$\$\$ Ok. →XML Sign	1.1.1.1.1.1.1.1.1
] [17:45:40]	+DB Sign	
[17:47:12] ¥EPOST¥MS¥c [17:47:12]	Download C:¥PROGRA~1 ata¥base004.avc.\$\$\$ Ok. →XML Sign	
] [17:47:12]	+OB Sign	
] [17:47:12] Ok.	Copy C:¥PROGRA~1¥EPOST¥MS¥data	¥base004.avc.\$\$\$

 ダウンロードされたパターンファイルは、[プラグインインストールフォルダ(既定値が C:¥plug-in-Kasp)] ¥Bases に格納されます。(画面は E-Post シリーズの場合) 従来バージョンでは、[同] ¥data、[同] ¥modified-date というフォルダを利用していました が、それらのフォルダは使わなくなります。

2 million	CAProgram Files/EPOSTIN	ISVBases					
Image:	ファイル田 編集田 表示心 :	お知じ入り後 クール田 へい	UTU UT				2
PH-0.00     C+Program FilestEPCSTWEWBase       2mk3     X       2mk3     X       3     C are:       3     Second       3 <th>Q R6 - 0 - 7 P HR</th> <th>0 7+115 - × ×</th> <th>D.</th> <th></th> <th></th> <th></th> <th></th>	Q R6 - 0 - 7 P HR	0 7+115 - × ×	D.				
Tech         x         connec         base/01/cone         base/01/	PHUR CAProgram FilestE	POSTVMSVBater					· 🔁 6540
	7el.65	Carro Carro	M baseli % are to baseli 1% are baseli 1% are baseli 1% are baseli 2% are	barn034c.rvc B barn034c.rvc B barn010c.rvc B barn010c.rvc B barn010c.rvc B barn040c.rvc B barn040c.rvc	I barn (50c are II) barn (50c are III) barn	base070c ave base070c ave base070c ave base070c ave base070c ave base110c ave	The base 120c are to base 120c are base 126c are base 126c are base 126c are base 126c are base 120c are



 ウイルスチェックのテストは、コマンドプロンプトを開き、カレントフォルダを「プラグイン インストールフォルダ」に移動してから、次のコマンドを入力します。最後に表示された "nResult=1"のコード番号は、「ウイルスが見つからなかった」ことを意味します。

```
C:¥plug-in-Kasp > kasp arj.ppl
[arj] argv[1] = arj.ppl
[arj] Source = arj.ppl
[arj] Start Virus scan.
[arj] End Virus scan.(arj.ppl,)
[arj] nResult = 1 ()
```

(※) Windows Server 2008、Windows Vista の環境では、「コマンドプロンプト」を必ず「管理者として実行する」必要があります。管理者としてコマンドプロンプトを開いていない場合、kasp プログラムを実行するとパイプエラーの表示がされますので注意してください。