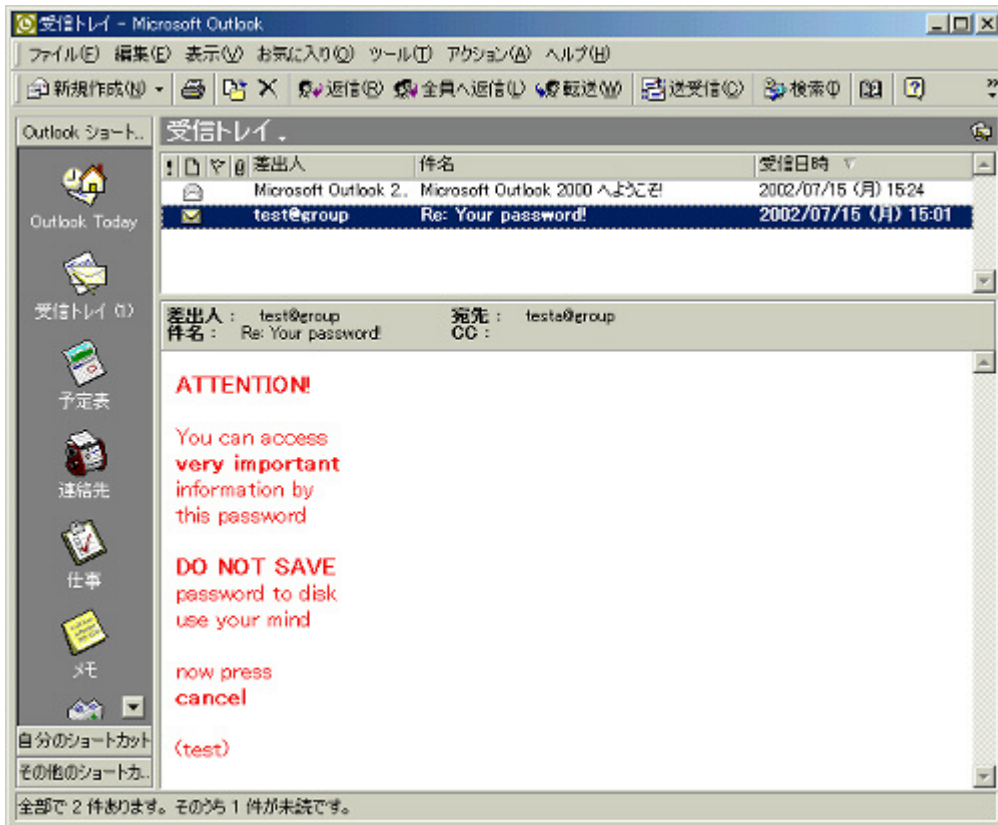


## ウイルス解析報告書

ウイルス名	W32/Frethem.K (WORM_FRETHEM.K)
プログラム名及び容量 (添付ファイル名)	decrypt-password.exe (48,640バイト)
種別	ワーム
プログラム言語:	Visual C++
発症環境	Windows95/98/ME/NT/2000/XP (32ビットWindows環境)
発見日時	2002年7月15日
発見場所(発信地)	発信地不詳であるが日本国内でも流通している
危険性	低い(感染力は高い)
発症条件	発病は認められない
ウイルスの活動、 影響	<p>このワームはWindows95/98/ME/NT/2000/XPで動作する。</p> <p>InternetExplorer5.0/5.5にセキュリティホール(「不適切な MIME ヘッダーが原因で Internet Explorer が電子メールの添付ファイルを実行する」)が存在する場合は、Outlook/OutlookExpressでメールを表示/プレビューしただけでワームが自動実行され、ワームに感染する。</p> <p>ワームが実行されると、OutlookExpressが標準で使用するSMTPサーバと送信者のメールアドレスを取得する。</p> <p>コンピュータの内部カレンダーが7月12日から16日であるとき、ワームはHDDにあるファイルからメールアドレスを取得し、このすべてのアドレスにメールを送信する。</p> <p>ワームはメールの送信のためにSMTPサーバに直接接続するので、メーラーの送信済みトレイにはワームが送信したメールは残らない。</p> <p>ワームが送信するメールの送信者(From)はOutlookExpressの設定に拠る。 添付ファイルは常に「decrypt-password.exe」と「password.txt」である。 decrypt-password.exeはBASE64でエンコードされたワーム本体である。</p> <p>ワームが送信するメールの件名は「Re: Your password!」で本文は下記の通り。</p> <p>ATTENTION!</p> <p>You can access very important information by this password</p> <p>DO NOT SAVE password to disk use your mind</p> <p>now press cancel</p> <p>(送信者名)</p>



なお、このワームに発病は確認されていない。

被害の規模	日本国内で150件の相談・報告がある (IPA、7月15日16:00現在の数字)
亜種、変種の有無	A型からK型までが確認されている

ワームはWindowsフォルダにワーム自身をtaskbar.exeという名前でコピーする。  
ワームはコピーしたファイルへのフルパスをレジストリの  
HKEY\_CURRENT\_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Runに  
Task Barというキーで登録する。

ワームはミュテックスオブジェクト「IEXPLORE\_MUTEX\_AABBCCDDEEFF」を作る。  
これが既にあるときには、既にワームが起動していると判断して、ワームは終了する。(2重起動を防ぐ)

ワームは下記のレジストリの値を取得する。  
Software¥Microsoft¥Internet Account Manager¥Accounts¥00000001¥SMTP Server  
Software¥Microsoft¥Internet Account Manager¥Accounts¥00000001¥SMTP Email Address  
Software¥Microsoft¥Internet Account Manager¥Accounts¥00000001¥SMTP Display Name

ワームはCドライブを再帰的に検索して拡張子が.dbx.wab.mbx.eml.mdbのいずれかならば、そのファイルからメールアドレスを取得する。

システム日付が7/12～7/16なら、ワームはメールを送信する。内容は下記の通り。

```
From: %s
To: %s
Subject: Re: Your password!
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary=L1db82sd319dm2ns0f4383dhG
```

```
--L1db82sd319dm2ns0f4383dhG
Content-Type: text/html;
Content-Transfer-Encoding: quoted-printable
```

```
<HTML><HEAD></HEAD><BODY>
<FONT COLOR=#FF0000>
```

ウイルス動作概要	<pre> &lt;b&gt;ATTENTION!&lt;/b&gt;&lt;br&gt;&lt;br&gt; You can access&lt;br&gt; &lt;b&gt;very important&lt;/b&gt;&lt;br&gt; information by&lt;br&gt; this password&lt;br&gt;&lt;br&gt; &lt;b&gt;DO NOT SAVE&lt;/b&gt;&lt;br&gt; password to disk&lt;br&gt; use your mind&lt;br&gt;&lt;br&gt; now press&lt;br&gt; &lt;b&gt;cancel&lt;/b&gt;&lt;br&gt;&lt;br&gt; (%s)&lt;/font&gt;&lt;/BODY&gt;&lt;/HTML&gt; &lt;iframe src=3Dcid:W8dqwg8q918213 height=3D0 width=3D0&gt;&lt;/iframe&gt;  --L1db82sd319dm2ns0f4383dhG Content-Type: audio/x-midi; name=decrypt-password.exe Content-Transfer-Encoding: base64 Content-ID: &lt;W8dqwg8q918213&gt;  (BASE64でエンコードされたワーム本体) --L1db82sd319dm2ns0f4383dhG  --L1db82sd319dm2ns0f4383dhG Content-Type: application/octet-stream; name=password.txt Content-ID: &lt;W8dqwg8q918213&gt;  Your password is W8dqwg8q918213 --L1db82sd319dm2ns0f4383dhG--  添付ファイルとしてdecrypt-password.exeとpassword.txtがある。 decrypt-password.exeはワーム本体で、IEの脆弱性があるとプレビューただけで実行される。%sはそれぞれ先頭からSMTP Email Address(レジストリから取得)、送信先のメールアドレス、SMTP Display Name(レジストリから取得)となる。 (W32/Klezのような送信者の偽装はしない) ワームはSMTPサーバに独自に接続してメールを送信する。(メーラーの送信済みトレイに残らない)  ワームはWindowsフォルダにwinstat.iniとnotepad.iniというファイルを作成する。 これらはデータファイル(無害)。  ワームは環境変数USERPROFILEがあるときにはその値以下の ¥Start Menu¥Programs¥Startup¥setup.exeにワーム自身をコピーする。 環境変数USERPROFILEがなければWindowsフォルダ以下の ¥Start Menu¥Programs¥Startup¥setup.exeにワーム自身をコピーする。 このフォルダがなければコピーは失敗する。(通常、日本語環境ではフォルダはない)  ワーム内部にはいくつかのIPアドレスが含まれており、ワームはスレッドを作成してそこにHTTPプロトコルで接続する。  ワーム内部には下記のメッセージが含まれている。 thAnks tO AntlvlrUs cOmpAnIEs fOr dEScribIng thE IdEA! nO AnY dEstrUctIvE ActIOns! dOnt wArrY, bE hAppY! </pre>
感染・発症防止方法	<p>・件名が「Re: Your password!」で添付ファイルが「decrypt-password.exe」と「password.txt」の電子メールを受け取った場合、この添付ファイルを開かないこと。</p> <p>・InternetExplorer5.0/5.5にセキュリティホール(「不適切な MIME ヘッダーが原因で Internet Explorer が電子メールの添付ファイルを実行する」)が存在する場合は、Outlook/OutlookExpressでメールを表示/プレビューただけでワームが自動実行される。これを避けるために、InternetExplorer5.0/5.5SP2またはInternetExplorer6にアップデートしてセキュリティホールをふさぐこと。</p>
ウイルスの駆除方法	<p>&lt; 確認 &gt;</p> <p>Windowsフォルダにtaskbar.exeがあるか、環境変数USERPROFILEの値以下に¥Start Menu¥Programs¥Startup¥setup.exeがあるかWindowsフォルダに¥Start Menu¥Programs¥Startup¥setup.exeがあれば感染している。</p> <p>レジストリのHKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥RunにTask Barというキーがあれば感染している。</p> <p>&lt; 駆除 &gt;</p>

	Windowsフォルダのtaskbar.exeとwinstat.ini、notepad.ini、環境変数USERPROFILEの値以下の ¥Start Menu¥Programs¥Startup¥setup.exe、Windowsフォルダの ¥Start Menu¥Programs¥Startup¥setup.exeを削除する。 レジストリのHKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥RunにあるTask Barも削除する。
その他	報告書作成 : 2002年7月18日現在

# W32/Frethem.K フローチャート

