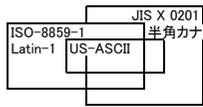


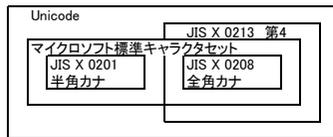
## 6. 文字コードとセキュリティ

### 文字集合

1バイト文字集合の包含関係



マルチバイト文字集合の包含関係



#### Unicode

当初16ビットですべての文字を表現する予定だったが、不十分で21ビットに拡張された。元の16ビット範囲をBMPと呼ぶ。(U+XXXX or XXXXXX)

文字集合間の文字割り当ての違い

文字集合	0x5C	0xA5
ASCII	\	%
JIS X 0201	¥	・
ISO-8859-1	\	¥
Unicode	\	¥

¥ (U+0045) の状態で、エスケープ処理が行われた後で、バックスラッシュ(\)に変換されると、エスケープ処理をすり抜けることになります。

### 文字エンコーディング

#### Shift-JIS

ラリルレロの2バイト目が「宴」にマッチする

Shift-JISの各バイトの分布

	0	#	#	#	#	A0	C0	E0	FF
1バイト文字									
2バイト文字の先行バイト									
2バイト文字の後続バイト									

#### 不正なShift-JIS

Shift-JISの先行バイトの後にデータがない場合(例:0x81)  
Shift-JISの先行バイトに続くバイトが、後続バイトの範囲にない場合(例:0x81 0x21)

#### EUC-JP

ラリルレロの4バイト目が「蛭」にマッチする

EUC-JPの各バイトの分布

	0	#	#	#	#	A0	C0	E0	FF
1バイト文字									
2バイト文字の先行バイト									
2バイト文字の後続バイト									

#### ISO-2022-JP

「ESC \$ B」でJIS X 0208に切り替え、「ESC (B)」でUS-ASCIIに切り替える。  
「インターネットでは半角カナを使うな」というのは、ISO-2022-JPが半角カナ(JIS X 0201)をサポートしないことに由来します。

#### UTF-16

もともと16ビット内で設計されていたが、21ビットに拡張された。

UCS-2 は16ビットのスカラ値を扱う。

BMP外の文字をサポートする符号化方式が**UTF-16**

UTF-16でBMPをサポートするのが、サロゲートペアで、(0xD800~0xDBFF)、(0xDC00~0xDFFF)の2つの領域を予約し、組み合わせて2の20乗文字を表現する。

## UTF-8

### UTF-8のビットパターン

スカラー値の範囲	UTF-8ビットパターン				ビット長
0~7F	0xxxxxxx				7ビット
80~7FF	110 xxxxx	10 xxxxxx			11ビット
800~FFFF	1110 xxxx	10 xxxxxx	10 xxxxxx		16ビット
10000~10FFFF	11110 xxx	10 xxxxxx	10 xxxxxx	10 xxxxxx	21ビット

### UTF-8の各バイトの配置

	0	#	#	#	#	A0	C0	E0	FF
1バイト文字									
2バイト文字の先行バイト									
2バイト文字の後続バイト									

文字の途中に別の文字がマッチする問題は起きません。

UTF-8の非最短形式の問題 U+007F までの文字は、2バイト以上のビットパターンを当てはめて符号化できる。

### 「/」の非最短形式による脆弱性

1バイト	0x2F								
2バイト	0xC0	0xAF							
3バイト	0xE0	0x80	0xAF						
4バイト	0xF0	0x80	0x80	0xAF					

最短形式  
非最短形式

### UTF-8の非最短形式による脆弱性

- セキュリティチェックで、非最短形式 0xC0 0xAF がスラッシュ 0x2F でないと見なされる
- ファイル名などとして、非最短形式 0xC0 0xAF を使うと、スラッシュと見なされる
- ※ UTF-8の最新規格では、UTF-8の非最短形式は処理してはならないとされています

### UTF-8の非最短形式を許していた処理系

- Java SE6 Update 10以前のJRE(Java実行環境)
- PHP5.3.1以前の htmlspecialchars関数

### その他の非正規なUTF-8

ISO/IEC 10646 Unicodeよりも広い31ビット空間で、UTF-8符号化後の1文字が最大6バイトだったが、2006年改訂で、実質的にUnicodeと同じものとなり、UTF-8符号化後の1文字も最大4バイトとなった。

### PHPの文字エンコーディング関数 mb\_check\_encoding

- PHP5.3 まではUTF-8の5バイト以上の形式を正しいエンコーディングと判断
- PHP5.4 以上は間違いと判断

### サロゲートペア領域の文字の変換

- 正しい変換 : ①まず、UTF-32に変換 ⇒ 次にUTF-8に変換 ⇒ 結果4バイト
- 機械的にUTF-8に変換すると、3バイトになる ※ このような文字エンコーディングに CESU-8 がある (oracleDBの内部処理で使用)
- PHPの文字エンコーディング関数 mb\_check\_encoding
  - ① PHP5.2 では正しいと判断
  - ② PHP5.3.0 以降では間違いと判断

## 文字コードを正しく扱うために

- Java と ASP.NET は入力時に文字エンコーディングの変換処理が入るので、チェックされ、不正な文字は代替文字(U+FFFD)に変換される。
- Perl (5.8以降) の場合は、decode関数による内部形式への変換時に、不正文字エンコーディングは代替文字に変換されます。
- PHPの場合には、文字エンコーディングが自動的にチェックされないで、mb\_check\_encoding関数により、チェックします。
- マルチバイト文字の扱いは  
Java、.NET、Perl(5.8以降)は問題ないが、PHPはマルチバイト文字に対応していないので、以下に従う必要があります。
  - ① ソースコードはUTF-8で保存
  - ② php.ini の default\_charset (PHP5.6以降) あるいは mbstring.internal\_encoding (PHP5.5以前) を、UTF-8と設定する
  - ③ 文字列処理は原則 mbstring系の関数を使う
  - ④ 関数の引数として、正しく文字エンコーディングを指定する
- HTTPレスポンスの Content-Type を正しく指定する
- データベースの文字エンコーディングを正しく指定する
  - ① MySQLでは、「utf8」は3バイトまでの形式で、BMP外の文字を含む場合は、「utf8mb4」と指定する。
  - ② 「尾紙骨」吉をデータベースに登録して、表示が崩れたら、Unicodeでの一貫した処理ではなく、途中でShift-JIS、EUC-JPの部分がある。

## 63-001:不正な文字エンコーディングによるXSS(正常系)

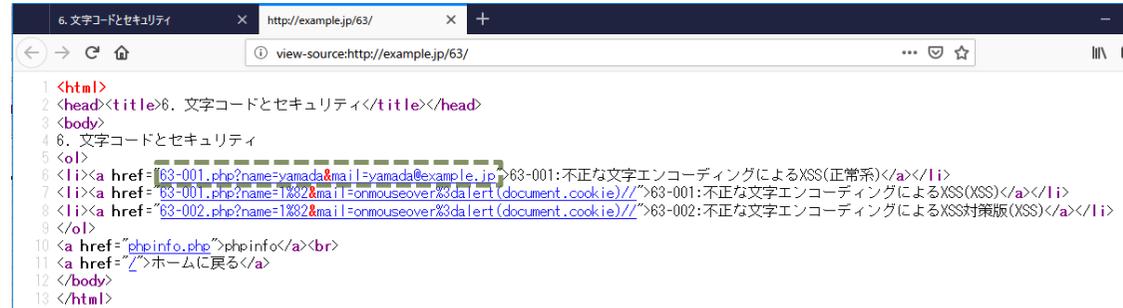
### 【ブラウザ】



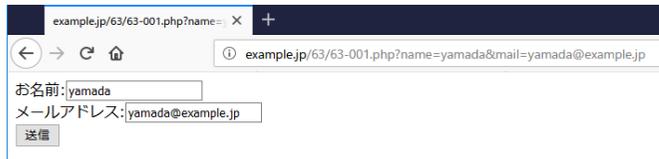
6. 文字コードとセキュリティ

1. [63-001:不正な文字エンコーディングによるXSS\(正常系\)](#)
2. [63-001:不正な文字エンコーディングによるXSS\(XSS\)](#)
3. [63-002:不正な文字エンコーディングによるXSS対策版\(XSS\)](#)

[phpinfo](#)  
[ホームに戻る](#)



```
1 <html>
2 <head><title>6. 文字コードとセキュリティ</title></head>
3 <body>
4 6. 文字コードとセキュリティ
5 <ol>
6 <li><a href="63-001.php?name=yamada&mail=yamada@example.jp">63-001:不正な文字エンコーディングによるXSS(正常系)</a></li>
7 <li><a href="63-001.php?name=1%82&mail=onmouseover%3dalert(document.cookie)//">63-001:不正な文字エンコーディングによるXSS(XSS)</a></li>
8 <li><a href="63-002.php?name=1%82&mail=onmouseover%3dalert(document.cookie)//">63-002:不正な文字エンコーディングによるXSS対策版(XSS)</a></li>
9 </ol>
10 <a href="phpinfo.php">phpinfo</a><br>
11 <a href="/">ホームに戻る</a>
12 </body>
13 </html>
```



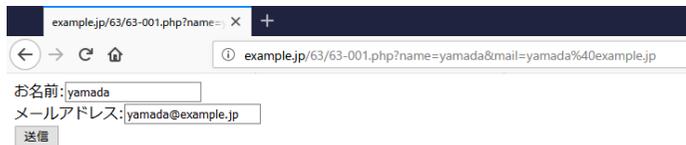
example.jp/63/63-001.php?name= X +

お名前:

メールアドレス:



```
1 <body>
2 <form action="">
3 お名前:<input name=name value="yamada"><BR>
4 メールアドレス:<input name=mail value="yamada@example.jp"><BR>
5 <input type="submit">
6 </form>
7 </body>
```



example.jp/63/63-001.php?name= X +

お名前:

メールアドレス:

### 【サーバ: 63/63-001.php】



```
/var/www/html/63/63-001.php - wasbook@example.jp - エディタ - WinSCP
k?php
  session_start();
  header('Content-Type: text/html; charset=Shift_JIS');
?>
<body>
<form action="">
お名前:<input name=name value=""?php echo htmlspecialchars($_GET['name'], ENT_QUOTES); ?>><BR>
メールアドレス:<input name=mail value=""?php echo htmlspecialchars($_GET['mail'], ENT_QUOTES); ?>><BR>
<input type="submit">
</form>
</body>
```



【ブラウザ→サーバ: リクエスト 63/63-001.php → レスポンス】(送信クリック)

The screenshot displays the OWASP ZAP interface. The top menu includes 'ファイル', '編集', '表示', 'ポリシー', 'レポート', 'ツール', 'オンライン', and 'ヘルプ'. The main window is split into three panes: 'コンテキスト' (Contexts), 'リクエスト' (Request), and 'レスポンス' (Response). The 'リクエスト' pane shows a GET request to 'http://example.jp/63/63-001.php?name=yamada&mail=yamada%40example.jp'. The 'レスポンス' pane shows an HTTP/1.1 200 OK response with headers and an HTML body containing a form with input fields for 'name' (value: 'yamada') and 'mail' (value: 'yamada@example.jp').

```
GET
http://example.jp/63/63-001.php?name=yamada&mail=yamada%40example.jp
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101
Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer:
http://example.jp/63/63-001.php?name=yamada&mail=yamada@example.jp
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=dskvjs6kdbg2180qrrqfg8mm1
Upgrade-Insecure-Requests: 1
Host: example.jp

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Thu, 10 Jan 2019 00:13:25 GMT
Content-Type: text/html; charset=Shift_JIS
Content-Length: 169
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragmas: no-cache
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
<form action="">
お名前:<input name=name value="yamada"><BR>
メールアドレス:<input name=mail value="yamada@example.jp"><BR>
<input type="submit">
</form>
</body>
```

Id	リクエスト日時	メソッド	URL	ステータス	ステータス...	ラウン...	レスポンス...	検出ア...	ノ...	タグ
36	19/01/10 9:12:...	GET	http://example.jp/63/63-001.php?name=yamada&mail=yamada@example.jp	200	OK	131 ms	169 bytes	Me...		Fo...
39	19/01/10 9:13:...	GET	http://example.jp/63/63-001.php?name=yamada&mail=yamada%40example.jp	200	OK	21 ms	169 bytes	Me...		Fo...

アラート: 0 1 3 0

現在のスキャン: 0 0 0 0 0 0

## 63-001:不正な文字エンコーディングによるXSS(XSS)

### 【ブラウザ】



6. 文字コードとセキュリティ

1. 63-001:不正な文字エンコーディングによるXSS(正常系)
2. 63-001:不正な文字エンコーディングによるXSS(XSS)
3. 63-002:不正な文字エンコーディングによるXSS対策版(XSS)

[phpinfo](#)  
[ホームに戻る](#)



```
1 <html>
2 <head><title>6. 文字コードとセキュリティ</title></head>
3 <body>
4 6. 文字コードとセキュリティ
5 <ol>
6 <li><a href="63-001.php?name=yanada&mail=yanada@example.jp">63-001:不正な文字エンコーディングによるXSS(正常系)</a></li>
7 <li><a href="63-001.php?name=%26amp;mail=onmouseover%3Dalert(document.cookie)//">63-001:不正な文字エンコーディングによるXSS(XSS)</a></li>
8 <li><a href="63-002.php?name=%26amp;mail=onmouseover%3Dalert(document.cookie)//">63-002:不正な文字エンコーディングによるXSS対策版(XSS)</a></li>
9 </ol>
10 <a href="phpinfo.php">phpinfo</a><br>
11 <a href="/">ホームに戻る</a>
12 </body>
13 </html>
```



example.jp/63/63-001.php?name= X +

example.jp/63/63-001.php?name=1%82&mail=onmouseover%3Dalert(document.cookie)//

お名前: 1

メールアドレス: onmouseover=alert(doc

送信



```
1 <body>
2 <form action="">
3 お名前:<input name=name value="1"><BR>
4 メールアドレス:<input name=mail value="onmouseover=alert(document.cookie)//"><BR>
5 <input type="submit">
6 </form>
7 </body>
```



example.jp/63/63-001.php?name= X +

example.jp/63/63-001.php?name=1%26%2365533%3B&mail=onmouseover%3Dalert(document.cookie)

お名前: 1&#65533;

メールアドレス: onmouseover=alert(doc

送信



```
1 <body>
2 <form action="">
3 お名前:<input name=name value="1&#65533;"><BR>
4 メールアドレス:<input name=mail value="onmouseover=alert(document.cookie)//"><BR>
5 <input type="submit">
6 </form>
7 </body>
```

### 【サーバ: 63/63-001.php】



```
/var/www/html/63/63-001.php - wasbook@example.jp - エディタ - WinSCP
k?php
session_start();
header('Content-Type: text/html; charset=Shift_JIS');
?>
<body>
<form action="">
お名前:<input name=name value=""?php echo htmlspecialchars($_GET['name'], ENT_QUOTES); ?>><BR>
メールアドレス:<input name=mail value=""?php echo htmlspecialchars($_GET['mail'], ENT_QUOTES); ?>><BR>
<input type="submit">
</form>
</body>
```



【ブラウザ→サーバ: リクエスト 63/63-001.php → レスポンス】(送信クリック)

The screenshot shows the OWASP ZAP interface. The top toolbar includes buttons for 'クイックスタート' (Quick Start), 'リクエスト' (Request), and 'レスポンス' (Response). The main window is divided into three sections: 'リクエスト' (Request), 'レスポンス' (Response), and '履歴' (History).

**Request Section:**

```
GET http://example.jp/63/63-001.php?name=1%26%2365533%3B&mail=onmouseover%3Dalert%28document.cookie%29%2F%2F HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://example.jp/63/63-001.php?name=1%82&mail=onmouseover%3Dalert(document.cookie)//
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=q806end446t12om9b49kd0c46
Upgrade-Insecure-Requests: 1
Host: example.jp
```

**Response Section:**

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Thu, 10 Jan 2019 00:33:27 GMT
Content-Type: text/html; charset=Shift_JIS
Content-Length: 195
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
<form action="">
お名前:<input name=name value="1&#amp;#65533;" ><BR>
メールアドレス:<input name=mail value="onmouseover=alert(document.cookie)" ><BR>
<input type="submit">
</form>
</body>
```

**History Section:**

Id	リクエスト...	メソ...	URL
103	19/01/10 9...	GET	http://example.jp/63/63-001.php?name=1%82&mail=onmouseover%3Dalert(document.cookie)//
105	19/01/10 9...	GET	http://example.jp/63/63-001.php?name=1%26%2365533%3B&mail=onmouseover%3Dalert%28document.cookie...

At the bottom, the status bar shows 'アラート' (Alerts) with 0 counts and '現在のスキャン' (Current Scan) with 0 counts.

## 63-002:不正な文字エンコーディングによるXSS対策版(XSS)

### 【ブラウザ】

6. 文字コードとセキュリティ

1. 63-001:不正な文字エンコーディングによるXSS(正常系)
2. 63-001:不正な文字エンコーディングによるXSS(XSS)
3. 63-002:不正な文字エンコーディングによるXSS対策版(XSS)

[phpinfo](#)  
[ホームに戻る](#)

```
1 <html>
2 <head><title>6. 文字コードとセキュリティ</title></head>
3 <body>
4 6. 文字コードとセキュリティ
5 <ol>
6 <li><a href="63-001.php?name=yamada&mail=yamada@example.jp">63-001:不正な文字エンコーディングによるXSS(正常系)</a></li>
7 <li><a href="63-001.php?name=1%82&mail=onmouseover%3dalert(document.cookie)//">63-001:不正な文字エンコーディングによるXSS(XSS)</a></li>
8 <li><a href="63-002.php?name=1%82&mail=onmouseover%3dalert(document.cookie)//">63-002:不正な文字エンコーディングによるXSS対策版(XSS)</a></li>
9 </ol>
10 <a href="phpinfo.php">phpinfo</a><br>
11 <a href="/">ホームに戻る</a>
12 </body>
13 </html>
```

example.jp/63/63-002.php?name= X +

example.jp/63/63-002.php?name=1%82&mail=onmouseover%3dalert(document.cookie)//

お名前:

メールアドレス:

```
1 <body>
2 <form action="">
3 お名前:<input name=name value=""><BR>
4 メールアドレス:<input name=mail value="onmouseover=alert(document.cookie)//"><BR>
5 <input type="submit">
6 </form>
7 </body>
```

example.jp/63/63-002.php?name= X +

example.jp/63/63-002.php?name=1%82&mail=onmouseover%3dalert(document.cookie)//

お名前:

メールアドレス:

### 【サーバ: 63/63-001.php】

```
/var/www/html/63/63-002.php - wasbook@example.jp - エディタ - WinSCP
k?php
  session_start();
  header("Content-Type: text/html; charset=Shift_JIS");
?>
<body>
<form action="">
お名前:<input name=name value=""?php echo htmlspecialchars($_GET['name'], ENT_QUOTES, 'Shift_JIS'); ?>><BR>
メールアドレス:<input name=mail value=""?php echo htmlspecialchars($_GET['mail'], ENT_QUOTES, 'Shift_JIS'); ?>><BR>
<input type="submit">
</form>
</body>
```

【ブラウザ→サーバ: リクエスト 63/63-002.php → レスポンス】(初期フォーム表示)

無題セッション - 20190109-100359 - OWASP ZAP 2.7.0

ファイル 編集 表示 ポリシー レポート ツール オンライン ヘルプ

標準モード

サイト クイックスタート リクエスト レスポンス

コンテキスト  
既定コンテキスト  
サイト  
http://example.jp  
http://api.example.ne

デフォルトビュー

```
GET http://example.jp/63/63-002.php?name=1%82&mail=onmouseover%3dalert(document.cookie)// HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://example.jp/63/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp
```

デフォルトビュー

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Thu, 10 Jan 2019 00:47:12 GMT
Content-Type: text/html; charset=Shift_JIS
Content-Length: 182
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: PHPSESSID=5fkinj6pli1ca9e7vohd5eqc2; path=/
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
<form action="">
お名前:<input name=name value=""> <BR>
メールアドレス:<input name=mail value="onmouseover=alert(document.cookie)//" > <BR>
<input type="submit">
</form>
</body>
```

履歴 検索 アラート アウトプット

フィルタ: オフ エクスポート

Id	リクエスト日時	メソッド	URL	ステータス	長さ	タイプ	コメント
110	19/01/10 9:47:12	GET	http://example.jp/63/63-002.php?name=1%82&mail=onmouseover%3dalert(document.cookie)//	200	OK	1...	F...
112	19/01/10 9:51:38	GET	http://example.jp/63/63-002.php?name=miko&mail=onmouseover%3Dalert%28document.cookie%29%2F2F	200	OK	3... 1...	F...

アラート 0 0 0 0 0 0 0 0

現在のスキャン 0 0 0 0 0 0 0 0

【ブラウザ→サーバ: リクエスト 63/63-002.php → レスポンス】(送信クリック)

The screenshot displays the Burp Suite interface with the following components:

- Top Bar:** 無題セッション - 20190109-100359 - OWASP ZAP 2.7.0
- Menu:** ファイル 編集 表示 ポリシー レポート ツール オンライン ヘルプ
- Navigation:** 標準モード, サイト, クイックスタート, リクエスト, レスポンス
- Left Panel (Contexts):** コンテキスト, 既定コンテキスト, サイト (http://example.jp, http://api.example.net)
- Request View (GET http://example.jp/63/63-002.php?name=miko&mail=onmouseover%3Dalert%28document.cookie%29%2F%2F):**

```
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://example.jp/63/63-002.php?name=1%82&mail=onmouseover%3Dalert(document.cookie)//
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=5fkInJ6pl1ca9e7vohd5eqc2
Upgrade-Insecure-Requests: 1
Host: example.jp
```
- Response View (HTTP/1.1 200 OK):**

```
Server: nginx/1.10.3
Date: Thu, 10 Jan 2019 00:51:38 GMT
Content-Type: text/html; charset=Shift_JIS
Content-Length: 186
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
<form action="">
お名前:<input name=name value="miko"><BR>
メールアドレス:<input name=mail value="onmouseover=alert(document.cookie)//"><BR>
<input type="submit">
</form>
</body>
```
- Bottom Panel (Request List Table):**

Id	リクエスト日時	メソッド	URL	ステータス	長さ	長さ	長さ	長さ	タグ
110	19/01/10 9:47:12	GET	http://example.jp/63/63-002.php?name=1%82&mail=onmouseover%3Dalert(document.cookie)//	200 OK	26...	18...			Fo...
112	19/01/10 9:51:38	GET	http://example.jp/63/63-002.php?name=miko&mail=onmouseover%3Dalert%28document.cookie%29%2F%2F	200 OK	31...	18...			Fo...

Alerts: 0 1 3 0 現在のスキャン: 0 0 0 0 0 0