安全にプログラムを動かすには？

PerlのTaintモードについて
-- 壱 --

AzureStone（あーじゅ・すとーん）
http://www.azurestone.org/

Copyright(C)　Digital Thoth Revolution - AzureStone All Right Reserved.

Taintモードとは

- Perlでは、標準でTaintモード（汚染モード）という機能が内包されている。
- ソースコードのシェバングに -T とつけることにより機能の使用できる。

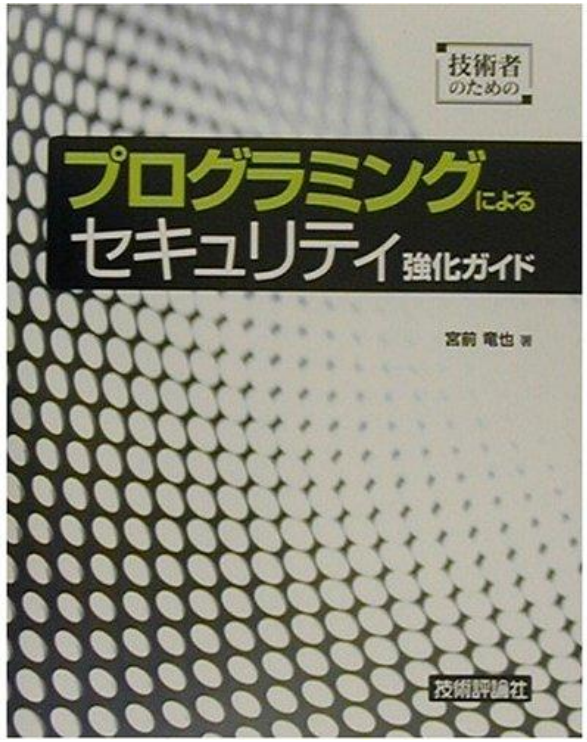
```
#!/usr/bin/perl -T

~~  snip  ~~
```

- 該当プログラムの外部から来たデータは全て汚染されていると判断し処理する。

Copyright(C) Digital Thoth Revolution – AzureStone All Right Reserved.

Taintモードをどこで知ったか

- 初めて知ったのは、書籍からです。
  - 「プログラミングによるセキュリティ強化ガイド」
  - 今から6年前の書籍



Copyright(C)　Digital Thoth Revolution – AzureStone All Right Reserved.

入力ってクエリーだけ？

- Webアプリケーションとかだと、CGIのクエリーストリングだけ？
- 違う。

Copyright(C)　Digital Thoth Revolution – AzureStone All Right Reserved.

汚染って何が汚染されている？

- その実行プログラム以外から入力されてくるデータ全て。
  - クエリーストリング
  - 環境変数
  - ファイルハンドル
  - system関数に渡す引数
  - use hogehoge; → @INC:
  - 特殊変数

Copyright(C) Digital Thoth Revolution – AzureStone All Right Reserved.

汚染って何が汚染されている？

- たとえばこんなプログラムがあったとします。

```
#!/usr/bin/perl -T

use CGI;
my $mail = CGI::param('mail');
print "Content-Type: text/html; charset=euc-jp¥n¥n";
open(MAIL, "|/usr/sbin/sendmail $mail");

print MAIL "Subject: registered¥n";
print MAIL "From: registered@azurestone.org";
print MAIL "ご登録ありがとうございました¥n";

print <<_END;
<HTML>
<HEAD>
<TITLE>登録完了</TITLE>
</HEAD>
<BODY>
<H1>登録完了</H1>
<P>登録ありがとうございます。確認メールを送信しました。</P>
</BODY>
</HTML>

1;
```

※注意　今時こんな実装しません！
「プログラミングによるセキュリティ強化ガイド」から引用してきました。
もしかしたら、TripletailLとかで書いた方がよかったのかな？

Copyright(C)　Digital Thoth Revolution – AzureStone All Right Reserved.

汚染文字列を除去する！

- 汚染されているなら除去せよ！

```
If  ($mail =~ /^([-_¥@¥d¥w¥.]+)$¥) {
    $mail = $1;
} else {
    print “入力エラー¥n”;
    exit;
}
```

  - 引用：技術者のためのプログラミングによるセキュリティ強化ガイドのP．63から

Copyright(C)　Digital Thoth Revolution – AzureStone All Right Reserved.

汚染文字列を除去する！

- 汚染されているなら除去せよ！

```
delete $ENV{PATH}

$ENV{PATH} = '/bin:/usr/bin';
```

  - 引用：技術者のためのプログラミングによるセキュリティ強化ガイドのP．63から

Copyright(C)　Digital Thoth Revolution – AzureStone All Right Reserved.

汚染文字列を除去する！

- Taintモードは万能？
  - 万能ではない。
  - 出力側でも対応するようにしよう。
- Taintモードで実行すると関連モジュールが、動かない場合があった。
  - use IO::Handle;
  - use POE;

Copyright(C)　Digital Thoth Revolution – AzureStone All Right Reserved.

さてみんなでやってみましょう！

- VMwareだけど。。
- 次回からは、LAN用意しておきますね！

Copyright(C)　Digital Thoth Revolution – AzureStone All Right Reserved.

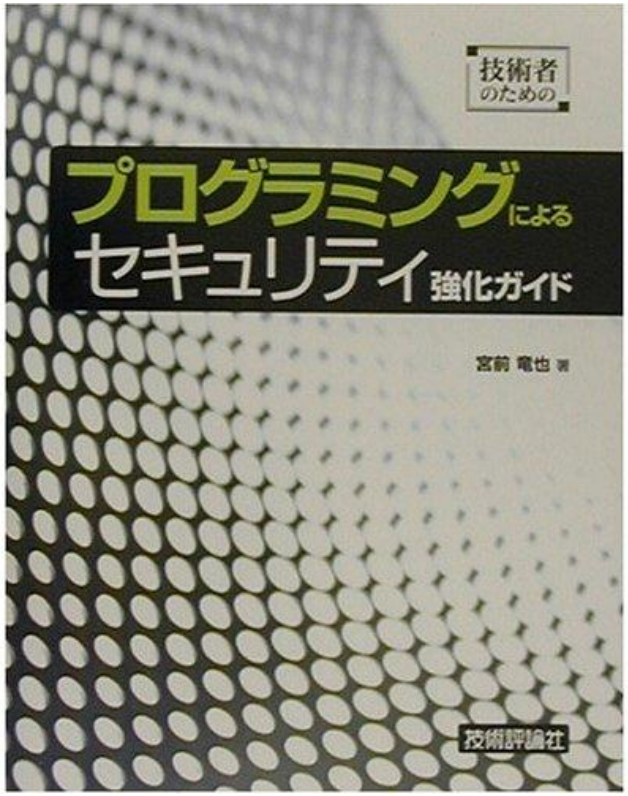
参考にしたURL

- http://blog.livedoor.jp/dankogai/archives/50749873.html
- http://harapeko.asablo.jp/blog/2007/02/12/178733
- http://harapeko.asablo.jp/blog/2007/01/29/148931
- http://www.ipa.go.jp/security/awareness/vendor/programming/a04_03.html

Copyright(C) Digital Thoth Revolution – AzureStone All Right Reserved.

参考にした書籍：壱

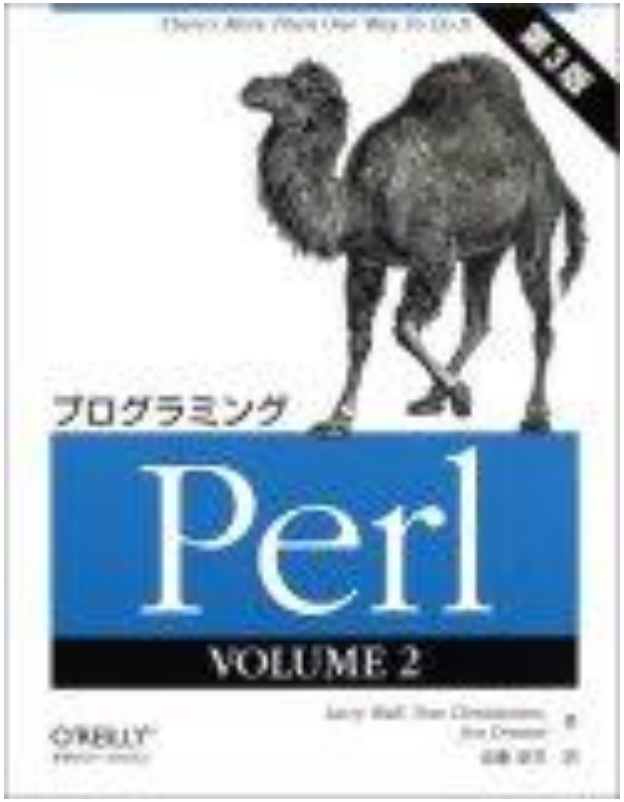
- 技術者のためのプログラミングによるセキュリティ強化ガイド
- 初版：平成14年12月25日



Copyright(C)　Digital Thoth Revolution – AzureStone All Right Reserved.

参考にした書籍：弐

- プログラミングPerl〈VOLUME2〉



Copyright(C)　Digital Thoth Revolution – AzureStone All Right Reserved.

ご参加ありがとうございました

- 平日の夜で忙しい中皆さんお集まり戴きありがとうございました。

Copyright(C)　Digital Thoth Revolution – AzureStone All Right Reserved.