

# セキュリティ診断事例から学ぶ EC-CUBEセキュリティ

EGセキュアソリューションズ株式会社



# アジェンダ

- 自己紹介
- EC-CUBE向け診断サービス
- EC-CUBE診断で検出した脆弱性
- 脆弱性の対策例
- まとめ
- お知らせ

# 自己紹介

# 自己紹介

## 松本 隆則 (@nilfigo)

- コミュニティ
  - 脆弱性診断研究会
  - OWASP Japan Promotion Team
  - Burp Suite Japan
- 資格
  - 情報処理安全確保支援士



# EC-CUBE向け診断サービスのご紹介

## EC-CUBEセキュリティ診断

- スタンダードパック
- リピーターパック



[https://www.ec-cube.net/products/detail.php?product\\_id=1319](https://www.ec-cube.net/products/detail.php?product_id=1319)

- EC-CUBEで構築したECサイトの脆弱性を検出
- 手動診断による高精度診断
- 詳細な診断レポート

# EC-CUBEセキュリティ診断で検出した 脆弱性の例



# EC-CUBEセキュリティ診断で検出した脆弱性の例

- クロスサイト・スクリプティング
- クッキーのSecure属性欠落
- クッキーのHttpOnly属性欠落
- 不要なファイルの公開
- クリックジャッキング
- アカウントロック機能の欠落
- オープンリダイレクト
- 認可制御の不備
- 重要な情報のクッキーへの保存
- 暗号化通信の強制不足
- セッションIDの固定化
- パスワード再発行の実装不備
- スタックトレース表示
- JSONのContent-Type指定不備

## EC-CUBEセキュリティ診断で検出した脆弱性の例

- 原則、カスタマイズ部分に脆弱性の検出が集中
- EC-CUBEで検出しがちな脆弱性もいくつか存在

# EC-CUBEセキュリティ診断で検出した脆弱性の例

- クロスサイト・スクリプティング
- クッキーのSecure属性欠落
- クッキーのHttpOnly属性欠落
- 不要なファイルの公開
- クリックジャッキング
- アカウントロック機能の欠落
- オープンリダイレクト
- 認可制御の不備
- 重要な情報のクッキーへの保存
- 暗号化通信の強制不足
- セッションIDの固定化
- パスワード再発行の実装不備
- スタックトレース表示
- JSONのContent-Type指定不備

- クッキーのSecure属性欠落
- クッキーのHttpOnly属性欠落

EC-CUBEの2系では自力で対策が必要

脆弱性の対策例

「クッキーのSecure/HttpOnly属性」の  
場合

## 脆弱性の対策例の例：クッキーのSecure/HttpOnly属性

■セッションID（ECSESSID）の場合

PHPの設定（php.ini）を確認&修正します。

```
session.cookie_secure    = 0n  
session.cookie_httponly = 0n
```

# 脆弱性の対策例の例：クッキーのSecure/HttpOnly属性

## ■セッションID以外のクッキーの場合

- ① SC\_Cookie\_Exクラスでsetcookie関数をオーバーライド
- ② オーバーライドした関数でSecure/HttpOnly属性を付与

```
class SC_Cookie_Ex extends SC_Cookie
{
    public function setCookie($key, $val)
    {
        setcookie($key, $val, $this->expire, ROOT_URLPATH, DOMAIN_NAME, TRUE, TRUE);
    }
}
```

# 脆弱性の対策例の例：クッキーのSecure/HttpOnly属性

## ■ 実際の報告書の例

- ECSESSID

php.ini の以下設定を書き換えます。

```
session.cookie_secure = On
```

- その他のクッキー

EC-CUBE 2.17.0-alpha の SC\_Cookie\_Ex クラスにて、以下の通り setCookie 関数をオーバーライドします。setcookie 関数の第 6 引数に TRUE を指定することでクッキーに Secure 属性を付与します。

[https://github.com/EC-CUBE/eccube-2\\_13/blob/improve/php7/data/class\\_extends/SC\\_Cookie\\_Ex.php](https://github.com/EC-CUBE/eccube-2_13/blob/improve/php7/data/class_extends/SC_Cookie_Ex.php)

```
class SC_Cookie_Ex extends SC_Cookie
{
    public function setCookie($key, $val)
    {
        setcookie($key, $val, $this->expire, ROOT_URLPATH, DOMAIN_NAME, TRUE);
    }
}
```



まとめ

- デフォルトの設定がセキュアじゃない  
EC-CUBEのバージョンが存在
- サイト運用の都合を優先して、セキュアじゃないインストール手順や運用方法を解説している書籍やサイトが存在するので注意が必要

お知らせ

# セキュリティ診断事例に学ぶ EC-CUBEセキュリティセミナー



**EC|CUBE**  
セキュリティ診断

powered by



**EG** Secure Solutions

2019年9月19日 25,000円(税別) ※ EC-CUBE DAY 2019 出展記念価格

[https://www.eg-secure.co.jp/news/201909\\_eccube\\_seminar/](https://www.eg-secure.co.jp/news/201909_eccube_seminar/)

## 対象者

- EC-CUBEでのサイト制作を請け負う制作会社の方
- EC-CUBEサイトのセキュリティ診断をお考えの方
- クレジットカード情報漏洩の手口と対策を知りたい方

## Chapter.1 90分

### クレジットカード情報漏洩の手口と対策のポイント

講師

**徳丸 浩**（EGセキュアソリューションズ代表）

Chapter.2 90分

## セキュリティ診断事例に学ぶEC-CUBEセキュリティ

講師

松本 隆則