(PHP)セキュリティの基礎

Yasuo Ohgaki / yohgaki@ohgaki.net

http://www.ohgaki.net/

Electronic Service Initiative, Ltd.

http://www.es-i.jp

自己紹介

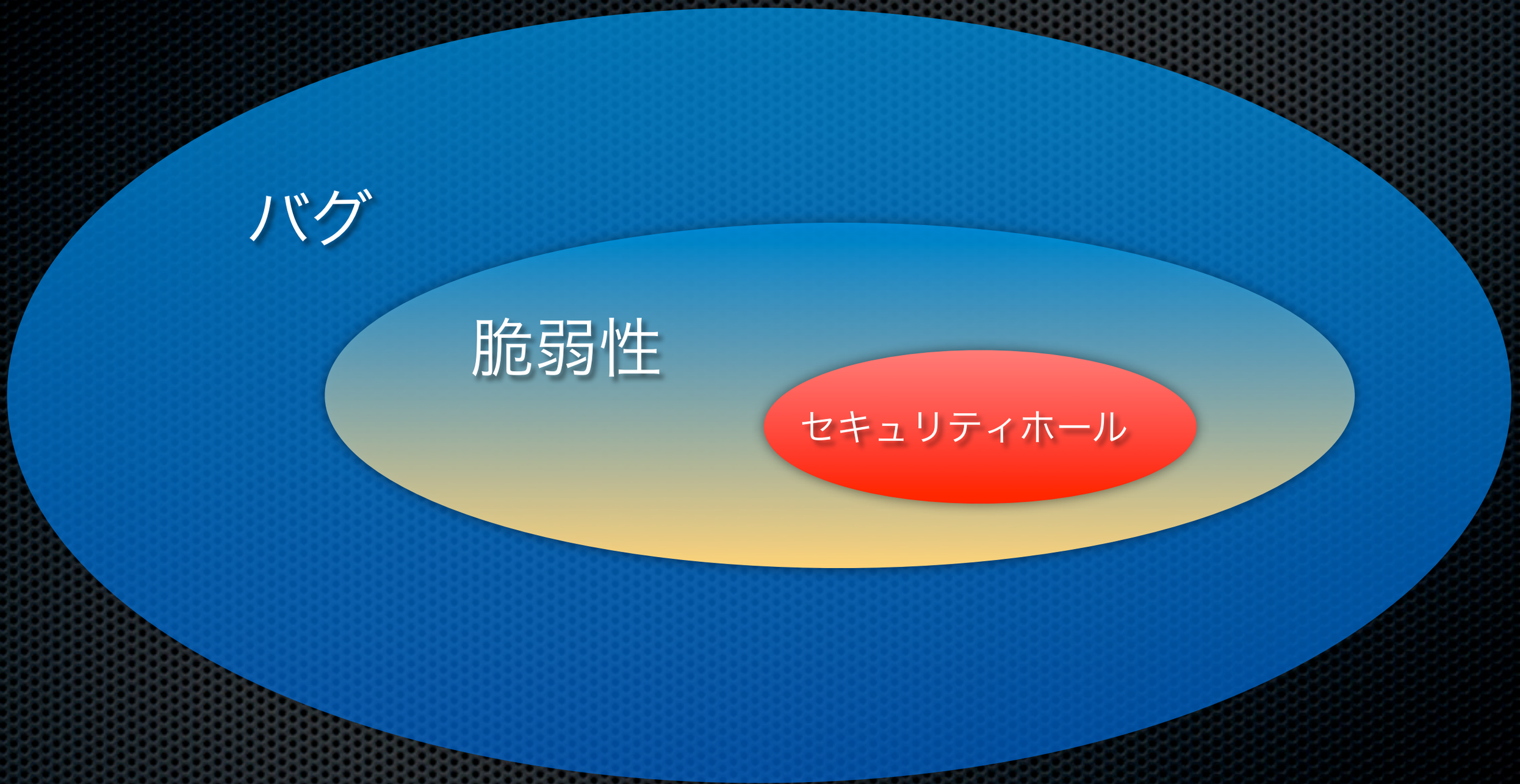
yohgaki

Momonga Linux Project
PostgreSQLユーザ会
日本PHPユーザ会
PHP Group
PHP技術者認定機構
岡山大学大学院 非常勤講師
エレクトロニック・サービス・イニシアチブ

前回のおさらい
「セキュリティについて考えてみる」

アプリが正常に動作する様に作ること

セキュリティホール、脆弱性はバグの一部


バグ
脆弱性
セキュリティホール

入力、処理、出力

ブラウザ

携帯

スマホ

PHPアプリ

データ

RDBMS

XML

メール

NoSQL

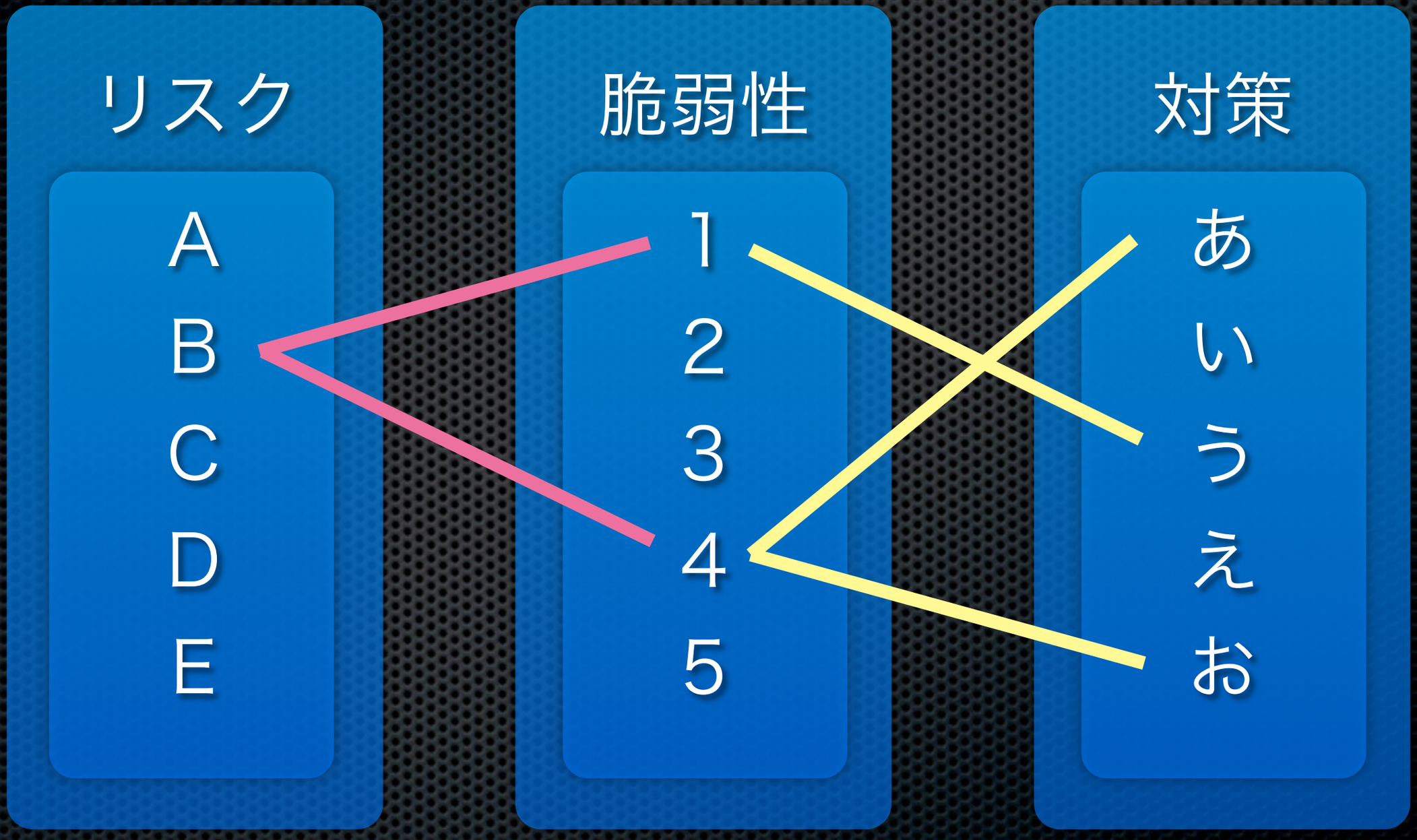
GD

その他

入力：バリデーション
処理：ベストプラクティス
出力：全てエスケープ

1. エスケープを理解し、
エスケープする
2. ヘルパーを理解し、
ヘルパーを使う
3. エスケープもヘルパーも使
えない物はバリデーション

セキュリティ対策とは？



セキュリティ対策は

基本的に普遍

セキュリティ対策が

セキュリティ対策でなくな

る場合はない

PHPセキュリティの基礎

PHPセキュリティ
ー
Webセキュリティ

Webセキュリティ

複数のシステムの組み合わせ

複数の標準の組み合わせ

＋

通常、一般公開

＝

攻撃者のターゲット

新たな脅威

HTML5

セキュリティ対策の基本

管理編

バージョンアップ

バージョンアップ

バージョンアップ

OS
Apache
PHP
フレームワーク
アプリケーション

現実にはバージョンアップ

はかなり難しい。。

php.iniには

php.ini-productionを使う

php.ini

open_basedir

disable_functions

disabl_classes

expose_php=off

default_charset=utf-8

php.iniが変更できる場所

php.ini / php.ini-SAPI名

--with-config-file-scan-dir

環境変数

httpd.conf

.htaccess

コマンド引数（-d）

スクリプトをDocument Rootに配置しない（可能であれば）

ログチェック

パフォーマンスモニタ

負荷テスト

セキュリティ対策の基本
設計編

Webシステムの特徴

ステートレス

つまり

ページさえ表示できればプ

ログラムはいつ終了しても

構わない

Webアプリの基本
不正な入力、異常な状態を
検出したら
「必ず終了」
させる。

PHPの場合、出力バッファを使い、エラーイベントでバッファをクリア、エラーページを表示可能。

当たり前だが
入力エラー処理は
別途実施する。

今ならJavascript、
将来はHTML５

Webアプリの基本
不正な入力、異常な状態を
検出したら
「必ずログを取る」

Webアプリの基本
不正な入力、異常な状態を
続けて検出したら
「ログオフ」
など必要な対処を取る

ログが必要な部分

認証

ユーザアクション

DBアクセス

エラー

DBへのアクセスログは
ユーザ名が必要
＝
アプリケーションからのログが必要

PHPのコードは
error_reporting=E_ALL
でエラーなく動作するよう記述。

@オペレータの利用は控える。

ユーザがアクセスする必要がない
ファイルはドキュメントルートに
配置しない。

ドキュメントルートに不要なファ
イルは再配置可能にする。

セキュリティ対策の基本

コード編

入力のバリデーション

文字エンコーディング

文字種類

長さ

フォーマット

メタ文字（特殊文字）
に注意

できるだけ正規表現
に頼らない

正規表現には
pregまたはmbregex
を利用する

PHPはUnicodeの正規化に注意する必要はない

出力の取り扱い

恐らく時間切れ

質問など？