セキュリティについて考えてみよう

プログラマから見たセキュリティ

Yasuo Ohgaki / yohgaki@ohgaki.net

セキュリティとは何か？

バグ・脆弱性・

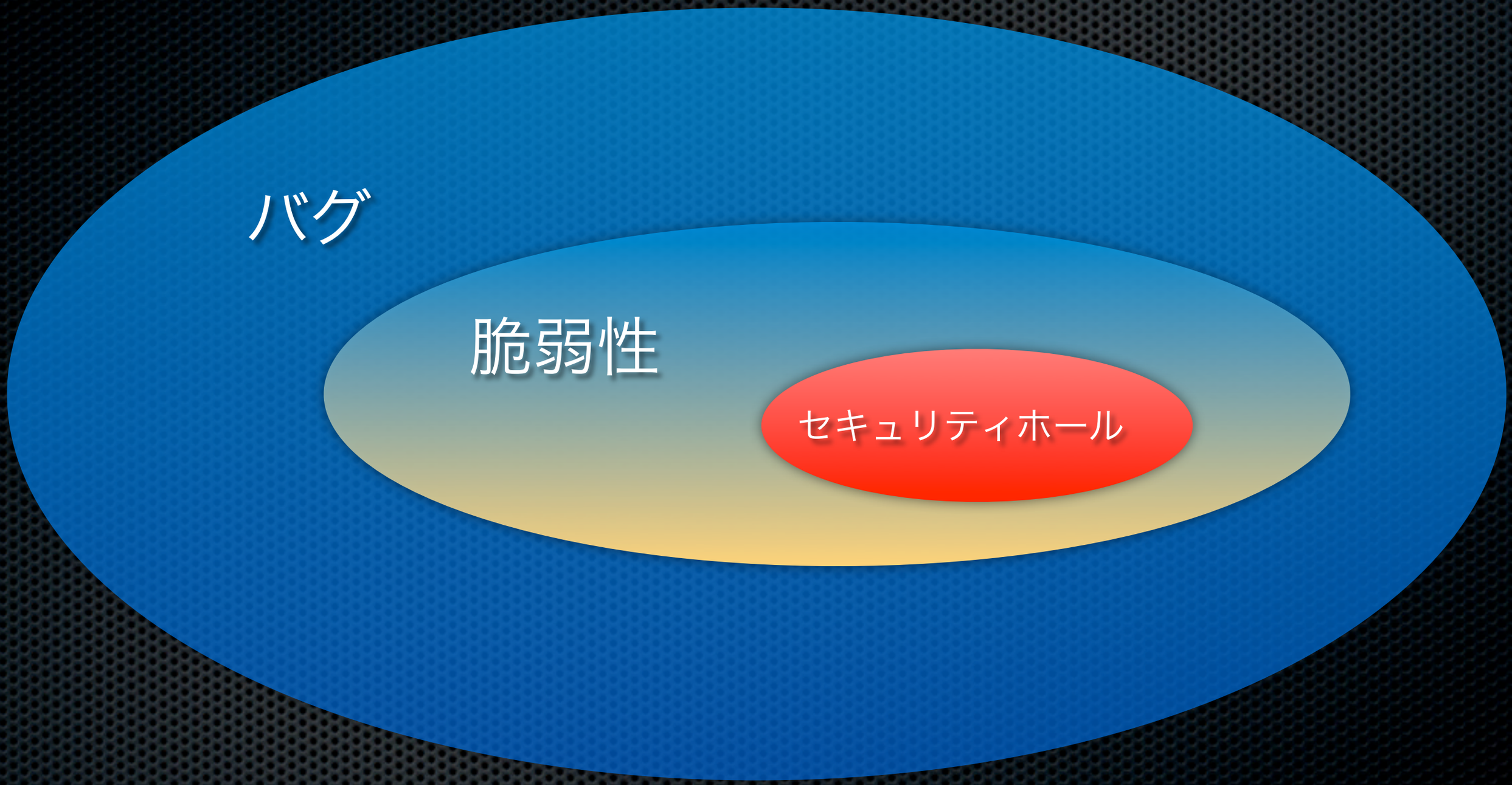
セキュリティホール

バグとは何か？

脆弱性とは何か？

セキュリティホールとは？

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

セキュリティとは？

アプリが正常に動作する様に作ること

アプリが正常に動作する為に必要なこと？

リスクを知り、対応する

リスクは何か？

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

すべてバリデーション

処理

処理はベストプラクティス
に従う

出力

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

セキュリティとは何か？

アプリケーションが正しく
動作する事を担保する

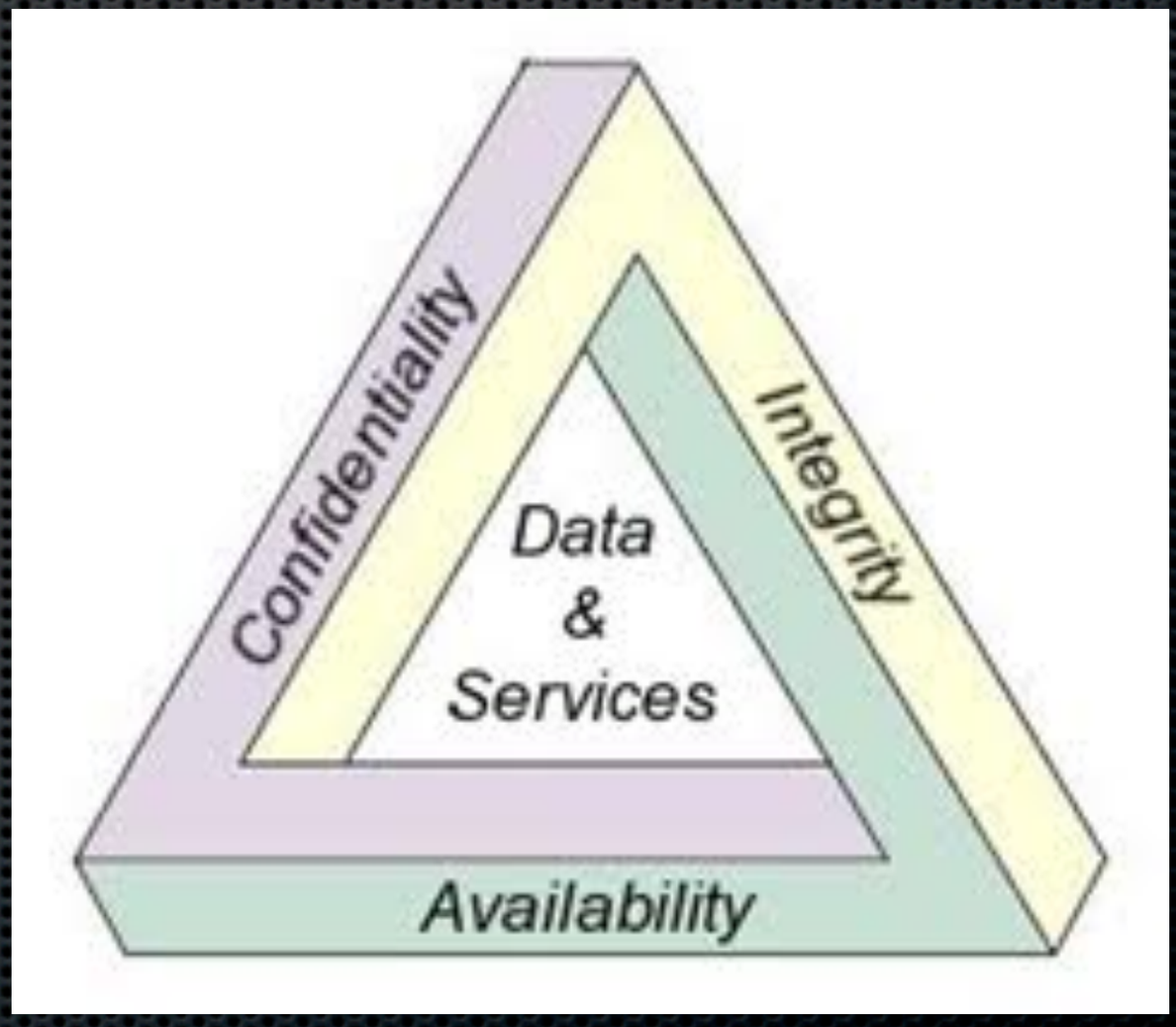
特にセキュリティに特化し

た場合

CIAを保証する


CIA
Clearance A1 required for access to Top Secret documentation
A3 - B6 clearance required for all other access
Unauthorized access prohibited
USE OF DEADLY FORCE TO PROTECT THE NATIONAL INTEREST IS AUTHORIZED

CIAを保証する



Confidentiality

気密性

Integrity

完全性

Availability

可用性

セキュリティ対策に役立たない

セキュリティ対策は無い

セキュリティ対策とは

リスクマネジメント

リスクを許容できれば

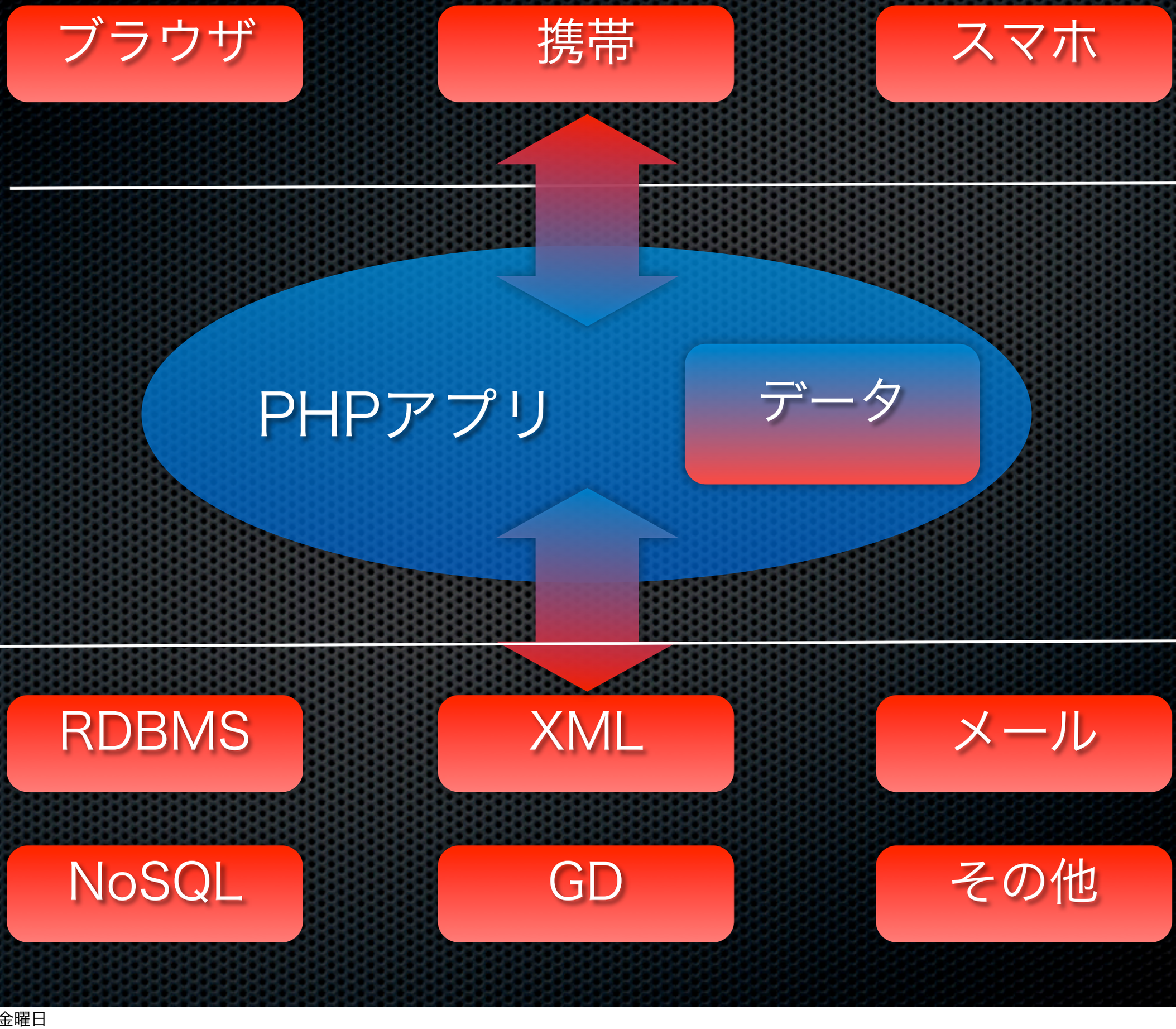
どんな対策でも構わない

ただし、他人に

迷惑はかけない

リスクマネジメントの例

例えば、文字エンコーディングのバリデーション


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

セキュリティは簡単！

プログラマから見れば

「入力・処理・出力」だけ

もちろん適切な設計も重要

リスクを知ることが重要

どれが優れたセキュリティ

対策か？よりも

どれが**必要な**セキュリティ

対策か？が重要

ご意見・ご質問などは

yohgaki まで