EC-CUBEだからこそ言える OSSとセキュリティの話

2020年4月24日

EC-CUBEユーザーコミュニティ 梶原 直樹

#eccube #osc20on

株式会社イーシーキューブが提供するサイト構築パッケージ「EC-CUBE」の脆弱性等について（注意喚起）

2019年12月20日

▶ 安全・安心

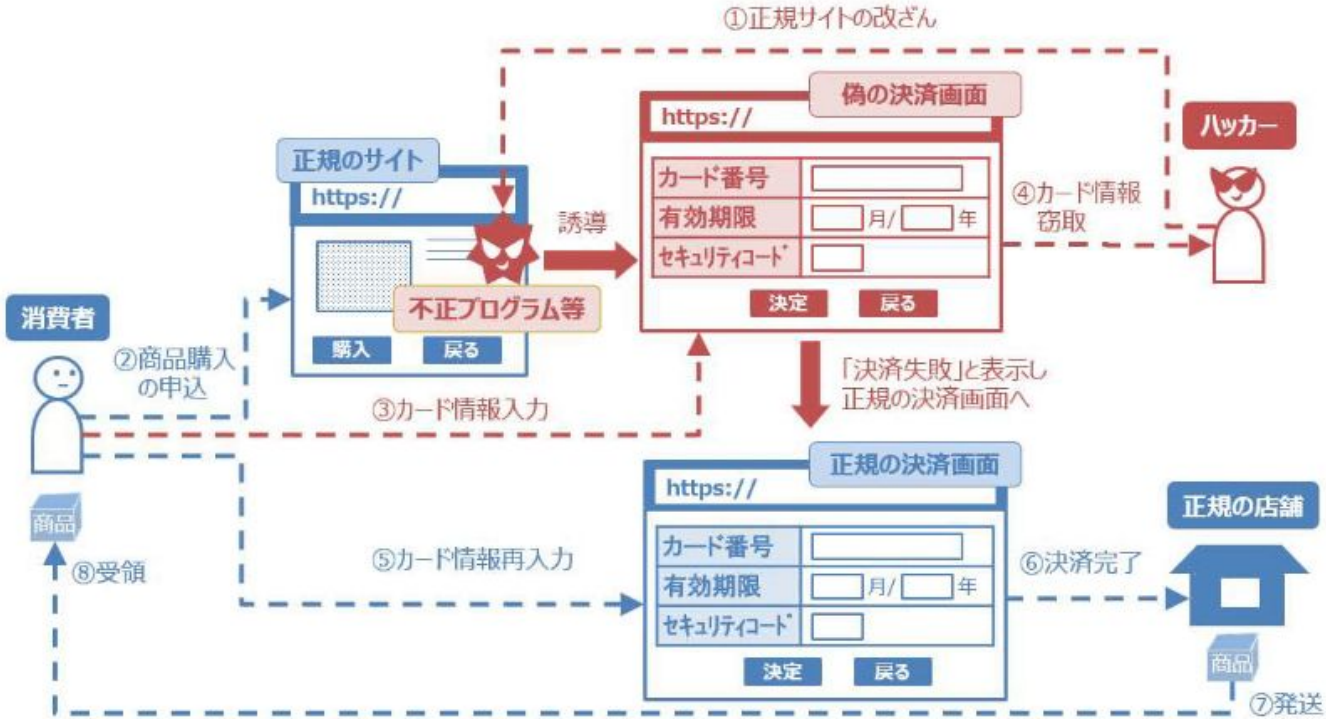
「EC-CUBE」の一部のバージョンには、クレジットカード番号等の漏えいの原因となる脆弱性等があることから、「EC-CUBE」を利用されているインターネットショップの皆様におかれましては、以下の点にご注意いただきますようお願いいたします。

本件概要

- 株式会社イーシーキューブが開発・提供するインターネットサイト構築パッケージ「EC-CUBE」の脆弱性等を突いたインターネットショップのサイトの改ざん等により、クレジットカード番号等が窃取されるといった被害が多発しております。

経済産業省サイトより

フォームジャッキングにより、「偽の決済画面」でクレジット情報を入力させて情報を取得する



消費者庁サイトより

本日のアジェンダ

- 自己紹介
- EC-CUBEとは？
- EC-CUBEで起こったセキュリティ事案と
  運営として対応してきたこと
- OSSを「安心して」利用するためには

梶原 直樹

株式会社イーシーキューブ
取締役 CCO
（チーフ・コミュニティ・オフィサー）

2008年 株式会社ロックオン（現イルグルム）に入社
　　広報担当を間に挟むも、これまでずっとEC-CUBE事業に従事

2018年 株式会社イーシーキューブ 取締役 に就任

EC-CUBEとは？

ECに色を

EC構築オープンソース 国内No1シェア

独立行政法人情報処理推進機構の「第3回オープンソースソフトウェア活用ビジネス実態調査」において、EC構築オープンソースとして国内 No.1シェアを獲得しました。

推定稼働店舗数

3万5千店舗

ダウンロード数

180万DL

プラグイン数

1千件以上

開発コミュニティ登録数

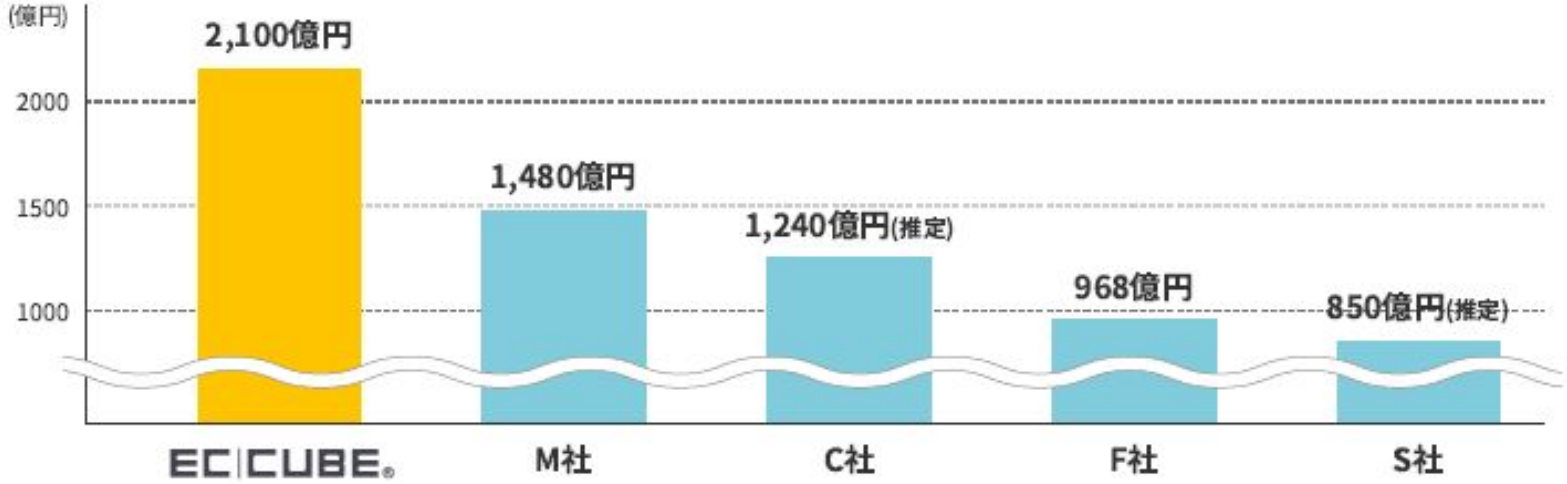
4万6千名

2019年8月時点

オープンなテクノロジーとコミュニティで
みんながワクワクするショッピング体験を創り出す

EC流通総額ランキング

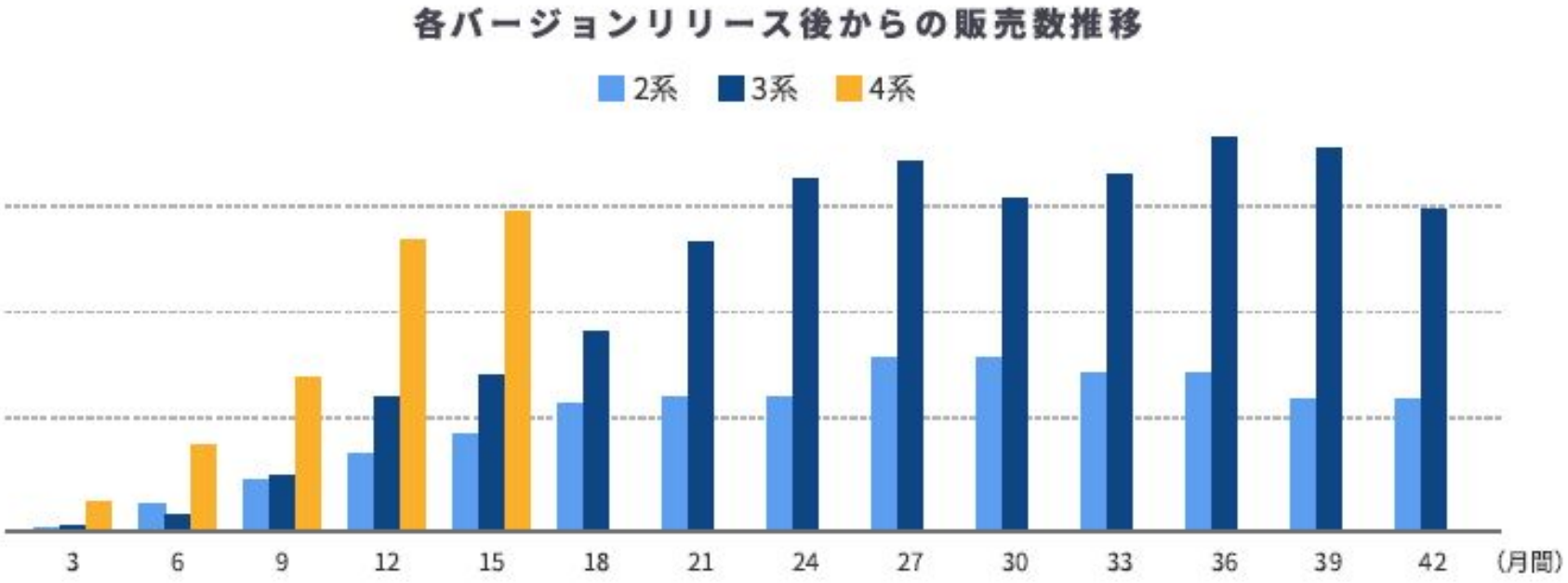
決済加盟店の報告を元に推計した**EC-CUBE利用店舗全体の年間流通総額は少なくとも2,100億以上**とみており
国内のECプラットフォームでもTOP7、自社サイトとしては1位となる規模と推定されています。



参考：国内13・海外18のECモール・カート・アプリの流通総額から見る市場トレンドならびに各社発表資料
https://ecclab.empowershop.co.jp/archives/50308

最新版EC-CUBE4系の立ち上がりも順調

2018年10月リリースのEC-CUBE4も順調に伸びており、公式プラグインストアの各バージョンリリース後のプラグイン数は3系の1/2(約200件)ながらも、販売数推移では、3系リリース時より半年以上早い立ち上がりを見せています。



EC-CUBEで起こったセキュリティ事案と運営として対応してきたこと

2019年12月 経済産業省から「EC-CUBE」に関する注意喚起

2019年

2019年12月

2020年

経済産業省
Ministry of Economy, Trade and Industry

申請・お問合せ | English | サイトマップ | 本文へ | 文字サイズ変更 小 中 大

ニュースリリース | 会見・談話 | 審議会・研究会 | 統計 | 政策に

ホーム ▶ ニュースリリース ▶ ニュースリリースアーカイブ ▶ 2019年度12月一覧 ▶ 株式会社イーシーキューブが提供するサイト構築パッケージ「EC-CUBE」の脆弱性等について（注意喚起）

株式会社イーシーキューブが提供するサイト構築パッケージ「EC-CUBE」の脆弱性等について（注意喚起）

2019年12月20日

▶ 安全・安心

「EC-CUBE」の一部のバージョンには、クレジットカード番号等の漏えいの原因となる脆弱性等があることから、「EC-CUBE」を利用されているインターネットショップの皆様におかれましては、以下の点にご注意いただきますようお願いいたします。

本件概要

- 株式会社イーシーキューブが開発・提供するインターネットサイト構築パッケージ「EC-CUBE」の脆弱性等を突いたインターネットショップのサイトの改ざん等により、クレジットカード番号等が窃取されるといった被害が多発しております。

2018年

NISC内閣サイバーセキュリティセンター
の方々と一緒に調査開始/啓蒙実施

EC-CUBE2系
管理画面のURLが/admin
管理画面のアクセス制限なし

2019年

2019年5月

・EC-CUBEよりセキュリティに関する注意喚起
・セキュリティ専門企業2社による無料診断開始

【重要】サイト改ざんによるクレジットカード流出被害が増加しています（2019/05/09）

Tweet いいね！ 441

※本件について、最新の情報は「【重要】クレジットカード流出被害が増加しています。EC-CUBEご利用店舗のセキュリティチェックをお願いいたします。」をご覧ください。(2019/12/23)

最近、ECサイトにおいて、決済画面を改ざんされてクレジットカード情報が抜き取られる手法(フォームジャッキング)による被害が日本国内で増加しています。

詳しくは、こちらの資料をご確認ください。

セキュリティ専門企業
・SHIFT SECURITY
・EG Secure Solutions

2020年

2018年

NISC内閣サイバーセキュリティセンター
の方々と一緒に調査開始/啓蒙実施

2019年

2019年5月

・EC-CUBEよりセキュリティに関する注意喚起
・セキュリティ専門企業2社による無料診断開始

- 警察庁 経済産業省 と連携

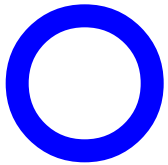
2019年12月

・EC-CUBE運営側からだけでは啓蒙等限界がある
・セキュリティ事案が減らない

経済産業省からの注意喚起で周知

【課題①】OSSパッケージ運営として分からないことがある

・ソフトウェアの脆弱性



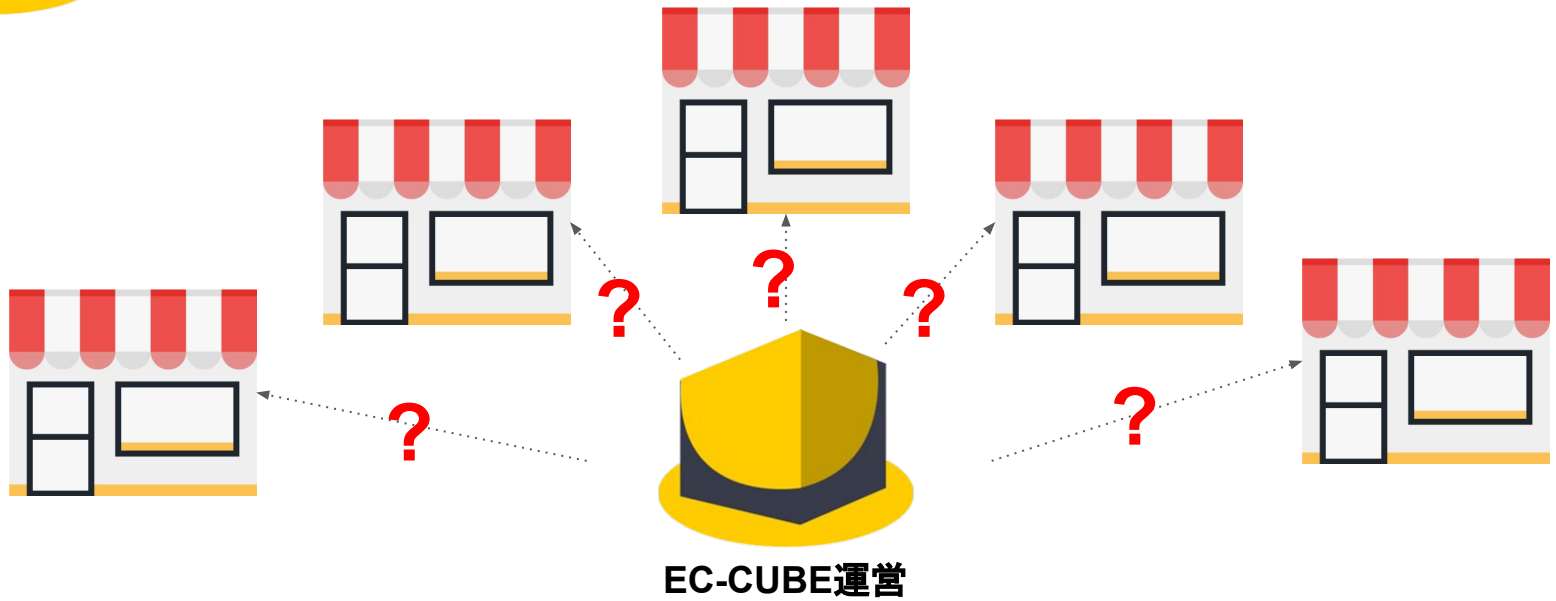
・情報漏洩の原因

セキュリティ事案報告の流れ

■OSS脆弱性報告の流れ

■実際に情報漏洩が起こった場合の 報告の流れ

【課題②】利用者（SHOP）に情報が届きにくい



- 利用者が分からない
- 直接情報をお届けできない

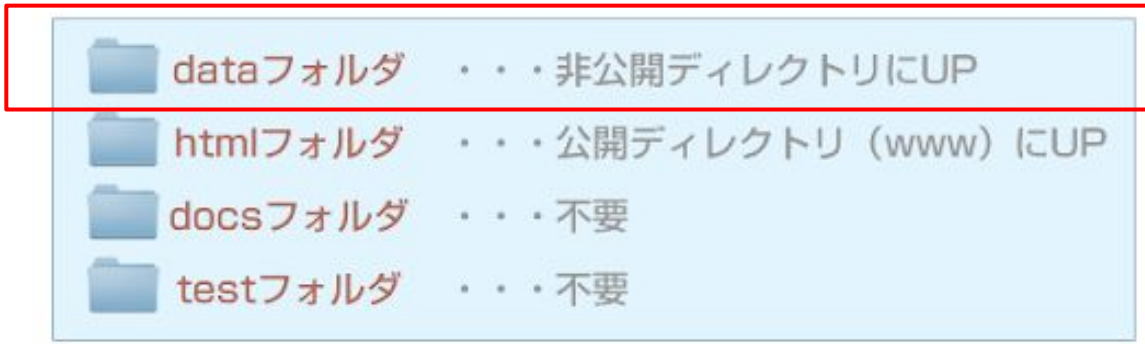
▪
▪
▪

2019年12月
クレジットカード情報漏洩の主な原因が判明

クレジットカード情報漏洩の主な原因
「誤った環境設定・インストール方法で運用」

EC-CUBE2系

EC-CUBEインストールファイルの構成



dataディレクトリをアクセス制限もかけずに、htmlディレクトリに入れてインストール。

data内の設定ファイルやキャッシュファイル閲覧
⇒　管理画面のログインID、PASSが漏れる
⇒　管理画面からページ改ざん

2020年からの対策一覧

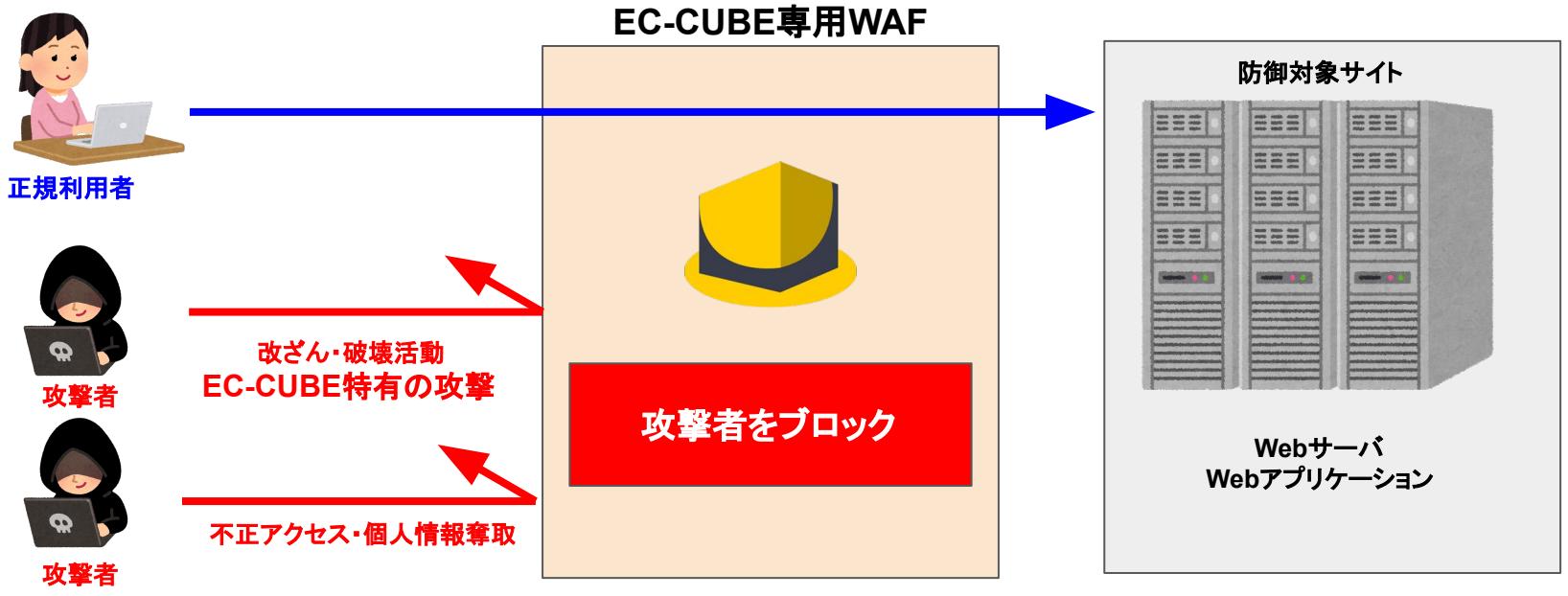
2020年

- セキュリティチェックリストを提供開始
- 自動セキュリティチェックツール
  （2系・3系・4系）を開発し、提供開始

- 決済代行会社と連携し、SHOPへ直接アプローチ

今後の予定

EC-CUBE 専用のWAF　提供予定



Webのセキュリティを守るならWAFは有効

ECのミカタ の記事より

OSSを「安心して」利用するためには

OSSは自由に使える
ただし利用は自己責任

- ダウンロード、インストール
- 環境設定
- カスタマイズ
- 利用
- メンテナンス（バージョンアップ）
- 状態監視
- セキュリティ保守　　等々

OSSの良さ

- カスタマイズ自由
- 利用も自由
- データ利用も自由

運用もナレッジもデータも自分たちのモノ

⇔

赤字以外を全て任せることができる**SaaS**

ec-cube.co

すぐに始めて成長できる、クラウド版「EC-CUBE」

まずはミニマムスタート！クラウド版なら、**メンテナンスフリー**
自動アップデートで常に最新状態のEC-CUBEをご利用いただけます。
規模に合わせオープンソース版への移行も可能！！

※1オープンソース版に比べ、カスタマイズには制限があります。

安心してOSSを利用するためには（特に重たいセキュリティ問題）

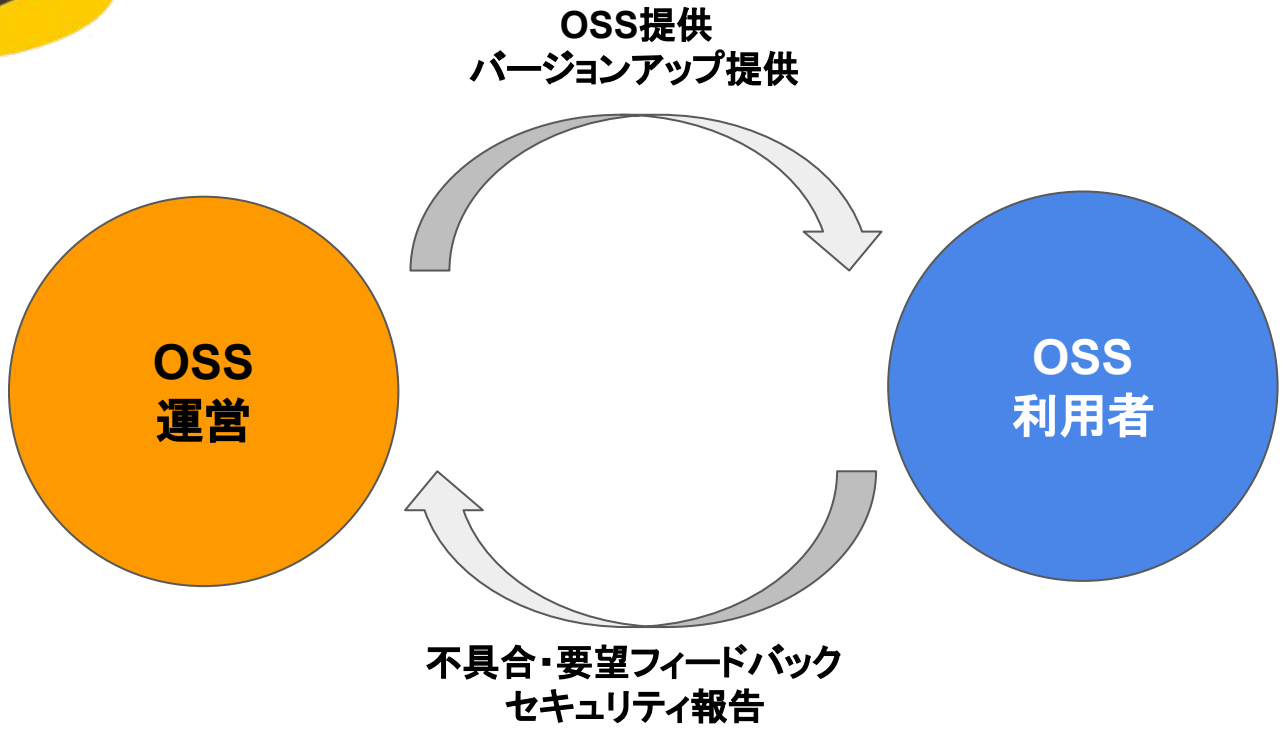
独自でOSS利用は、セキュリティ保守は自分で対応

- **脆弱性診断（自社サービス・サイト公開前）**
- **バージョンアップ or セキュリティパッチ対応**
  ⇒アプリケーション、OS、ミドルウェア
- **アプリケーション監視（改ざん検知、不正アクセス検知 等）**
- **サーバ監視（DDos攻撃対策、不正アクセス検知　等）**

Webアプリケーションなら**WAF**が外部攻撃から守ってくれる

OSSを長く安心して利用するために
より重要なこと

フィードバックがOSSを発展させ
より安心できる環境になって帰ってくる

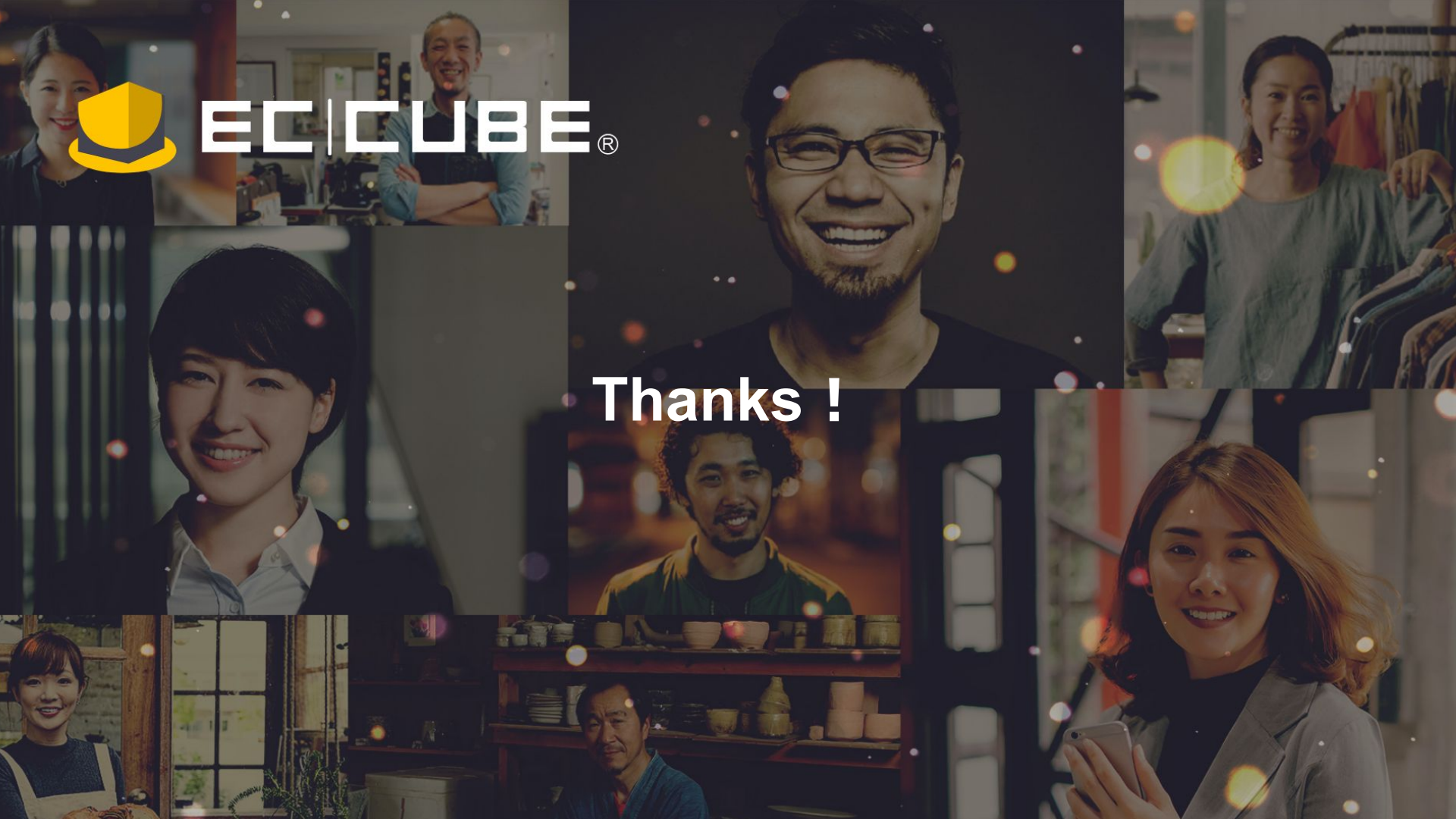


本日のまとめ

- EC-CUBEご利用者様、OSS全体にもご不便おかけしました
  セキュリティ対策、サービス提供随時実施中

- OSS利用・セキュリティ対策はあくまで自己責任
  自ら情報をとりにいき、守る姿勢。WebならWAFは有効

- OSS利用ではフィードバックが重要
  OSSに貢献すれば、更に良い利用環境になって帰ってくる


EC|CUBE®
Thanks !