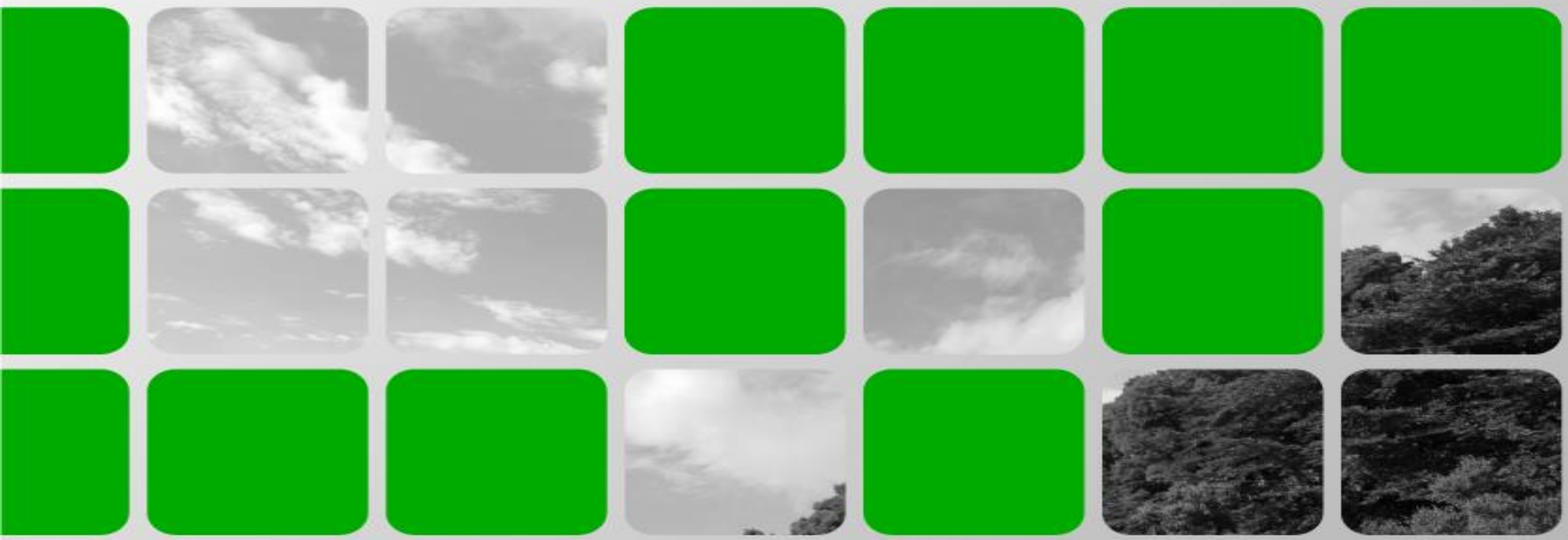
第39回スクエアfreeセミナー　ライトニングトーク

SSLアクセラレータとは何？　必要なの？

株式会社OPENスクエア　　田中昭造



Copyright OPENSQUARE. All rights reserved

SSL色々なこと

- SSL（Secure Sockets Layer）

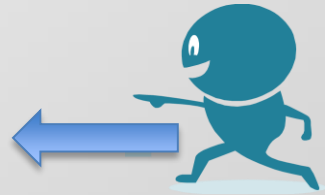
Netscape Communications社が開発した、インターネット上で情報を暗号化して送受信できる仕組み。

個人情報・クレジットカード情報などの大切なデータを安全にやりとりできます。

- SSL証明書

Webサイト所有者の情報、送信情報の暗号化に必要な鍵、証明書発行者の署名データ（ネット上の実印のようなもの）を持った電子証明書です。

  - サイト所有者の証明
  - 情報の暗号化通信



- 常時SSL

全てのページをSSLで暗号化して通信する手法です。常時SSLによってCookieやURLパラメータで保管されることが多いユーザ識別子（セッションIDなど）が常に暗号化され、サイトの信頼性を高めることができます。

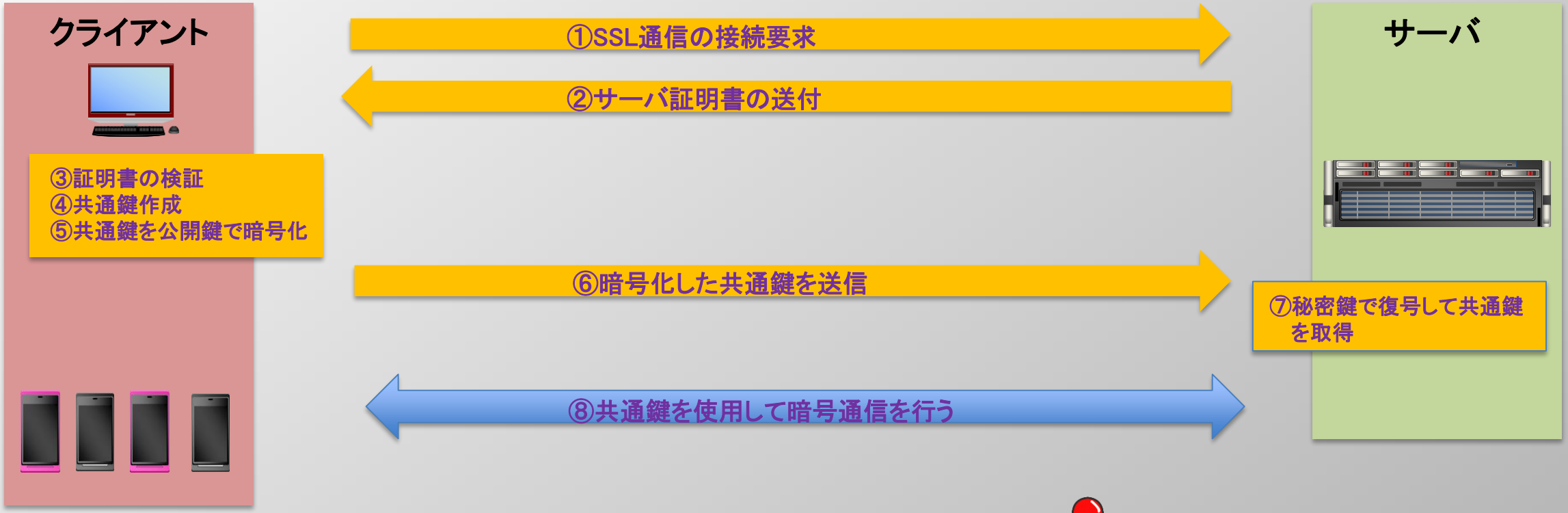
既にFacebook、Google、Twitterといった非常に成功しているウェブサイトで広く利用されています。

Wi-Fiが普及した事も一つの要因です。

日本の銀行でも導入が進んでいます。

Copyright OPENSQUARE. All rights reserved

SSL通信の仕組み概要



①から⑥が公開鍵暗号化方式【SSLセッションの確立】（1024ビット、2048ビット）
⑧は共通鍵暗号化方式【データの暗号/復号】（56ビット～256ビット）

鍵長が長くなれば CPU負荷が増加します

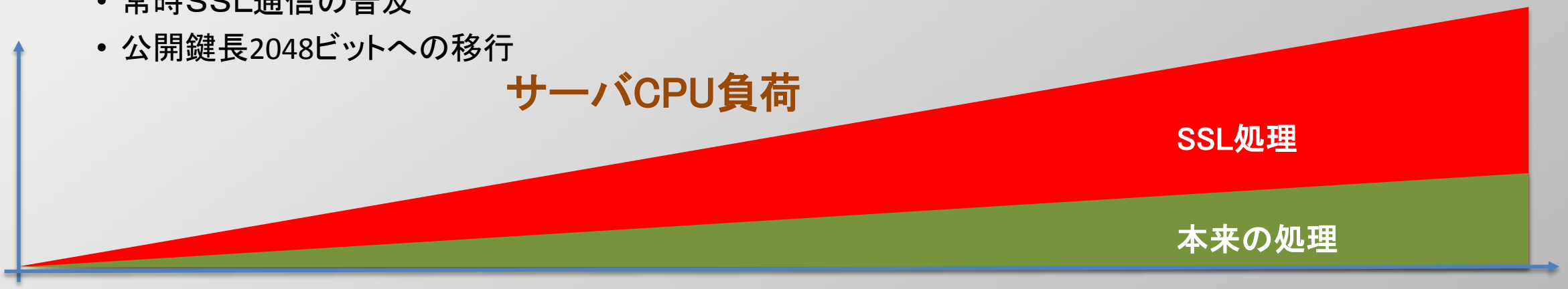
Copyright OPENSQUARE. All rights reserved

SSLアクセラレータは何故必要？

SSL通信の増加により、、、

– **サーバのCPU負荷が益々増大** → **本来行うべきアプリケーション処理が遅延**

- スマートデバイスの普及によりクライアント数が爆発的に増加
- 常時SSL通信の普及
- 公開鍵長2048ビットへの移行



対策

– SSL処理を別のサーバで処理

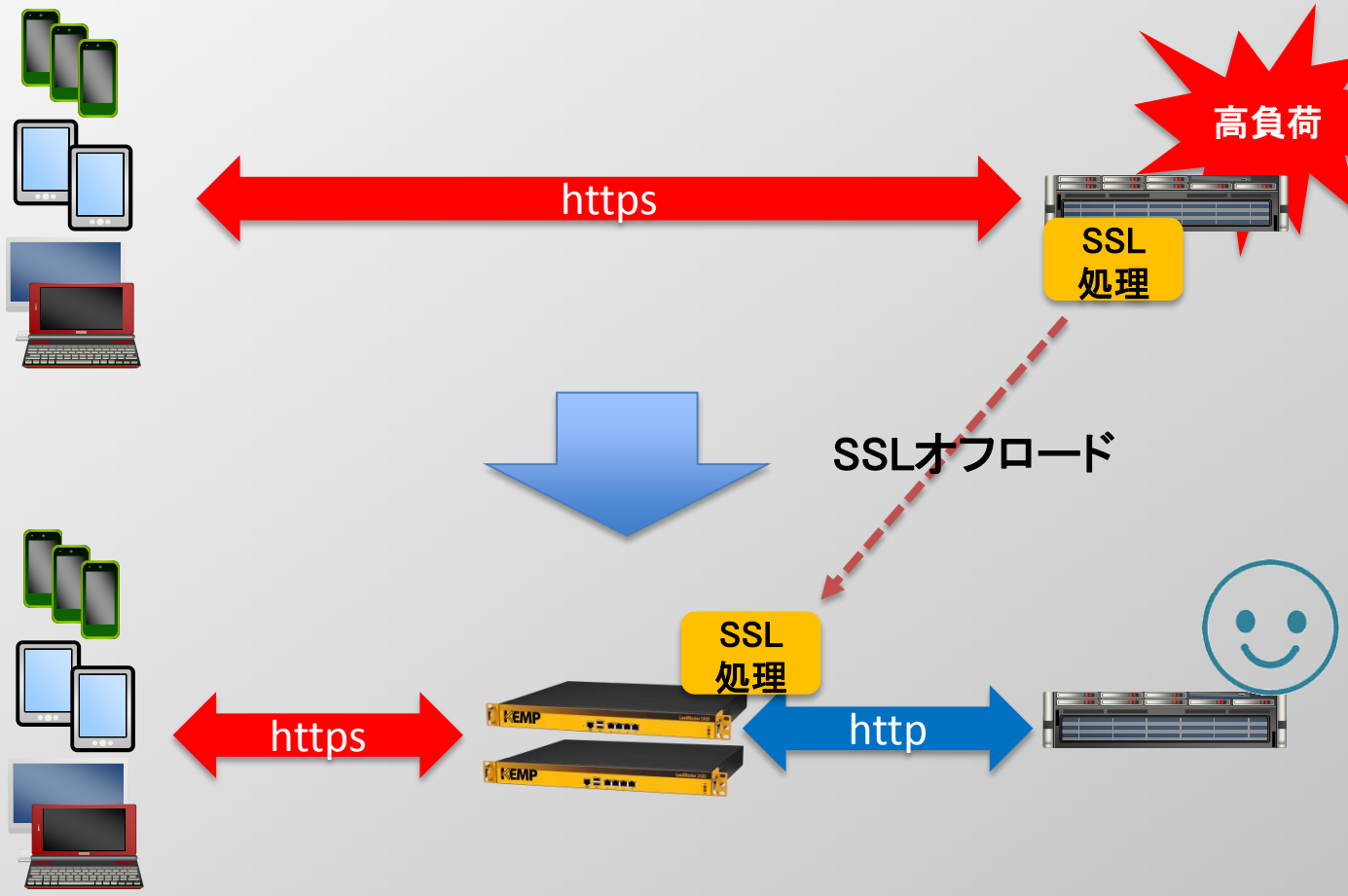
SSLオフローディング

SSL処理を高速に行うSSLアクセラレータを利用

SSL処理専用のASICにより高速処理を実現

Copyright OPENSQUARE. All rights reserved

LoadMaster（SSLアクセラレータ）登場



1. サーバのCPU負荷が高くなりアプリケーションの処理性能が低下します。
2. 公開鍵長を1024ビットから2048ビットに変更するとSSL処理負荷は4～5倍になります。

高性能なサーバへのリプレイスが必要になる場合があります。サーバのリプレイスは高額な（工数と費用）追加投資が必要になります。

廉価なLoadMasterを導入するだけで、

- **サーバは本来の処理に専念できます。**
- **SSL証明書の管理を一元化できます。**
- **サーバのスケールアウトも容易です。**

Copyright OPENSQUARE. All rights reserved

ご清聴、ありがとうございました。

株式会社OPENスクエア

www.opensquare.co.jp

〒101-0035　東京都千代田区神田紺屋町17番地　SIA神田スクエア　2F

電話：03-6413-1840　　E-Mail：sales_os@opensquare.co.jp

担当：田中昭造

END

Copyright OPENSQUARE. All rights reserved