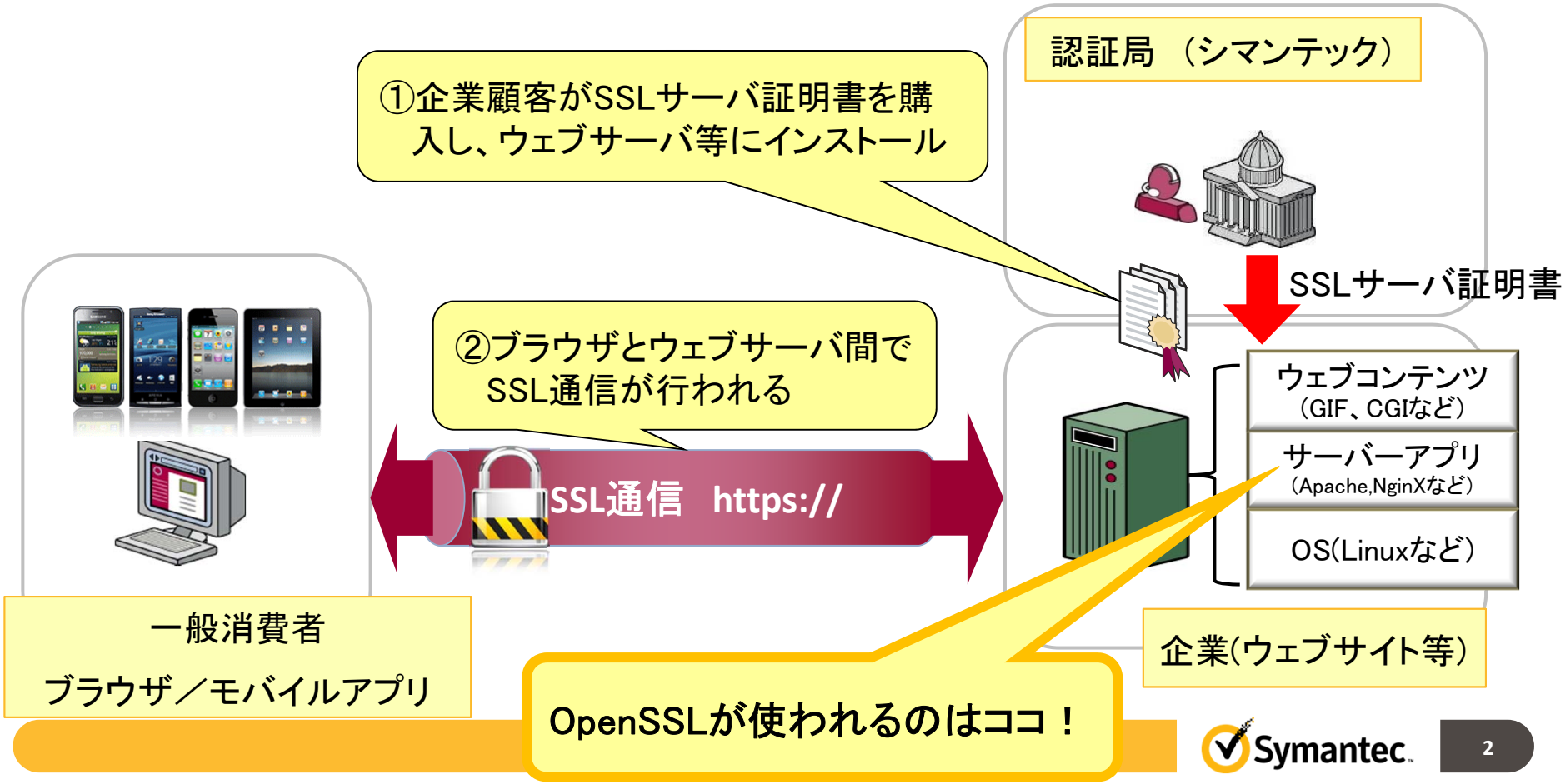
Heartbleed
～OpenSSLの脆弱性～

株式会社シマンテック

4月16日現在の情報で作成されています。内容は変更されることがあります。

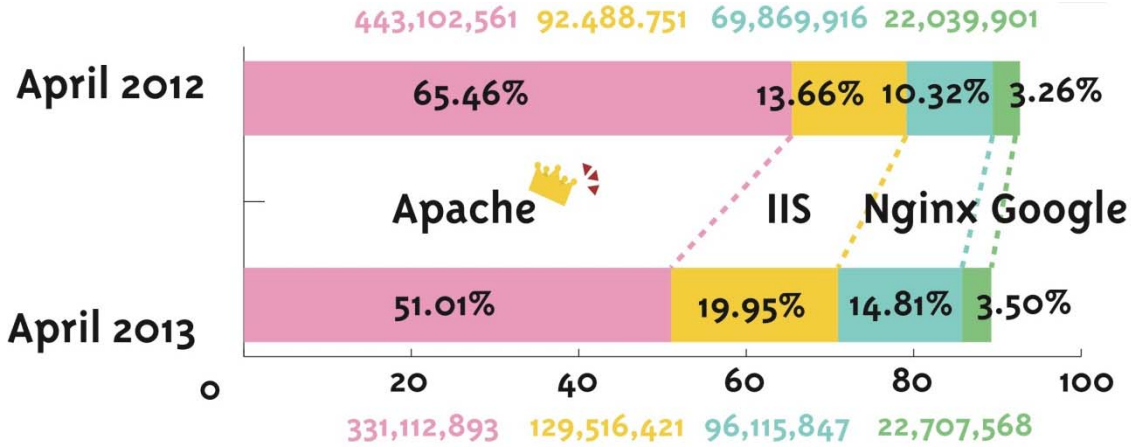
OpenSSL とは？

- OpenSSLとは、オープンソースの暗号ソフトウェアライブラリで、サーバーなどがSSL/TLSと呼ばれる暗号方式を利用するために使用されます。



OpenSSL とは？

- OpenSSLは、ApacheやNginxといったウェブサーバーに使われており、他にもSSL通信を行うアプリケーションなどに広く使われています。



参照：Netcraft　http://news.netcraft.com/archives/2013/04/02/april-2013-web-server-survey.html

※Heartbleedは、以下の条件で問題が発生します。

- SSL暗号通信を行うサーバー
- OpenSSLの特定のバージョン（1.0.1 から 1.0.1f）
- OpenSSLの拡張機能“Heartbeat”の利用

- OpenSSL と「SSLサーバ証明書」は、別物です。
- 今回のHeartbleedは、OpenSSLがその拡張機能Heartbeatを利用している場合にSSL通信を行うためのチェック機能を果たしていないバグを突いた攻撃です。
- SSL/TLSの問題でも、SSLサーバ証明書の危殆化という話でもありません。

HeartBleedの問題点

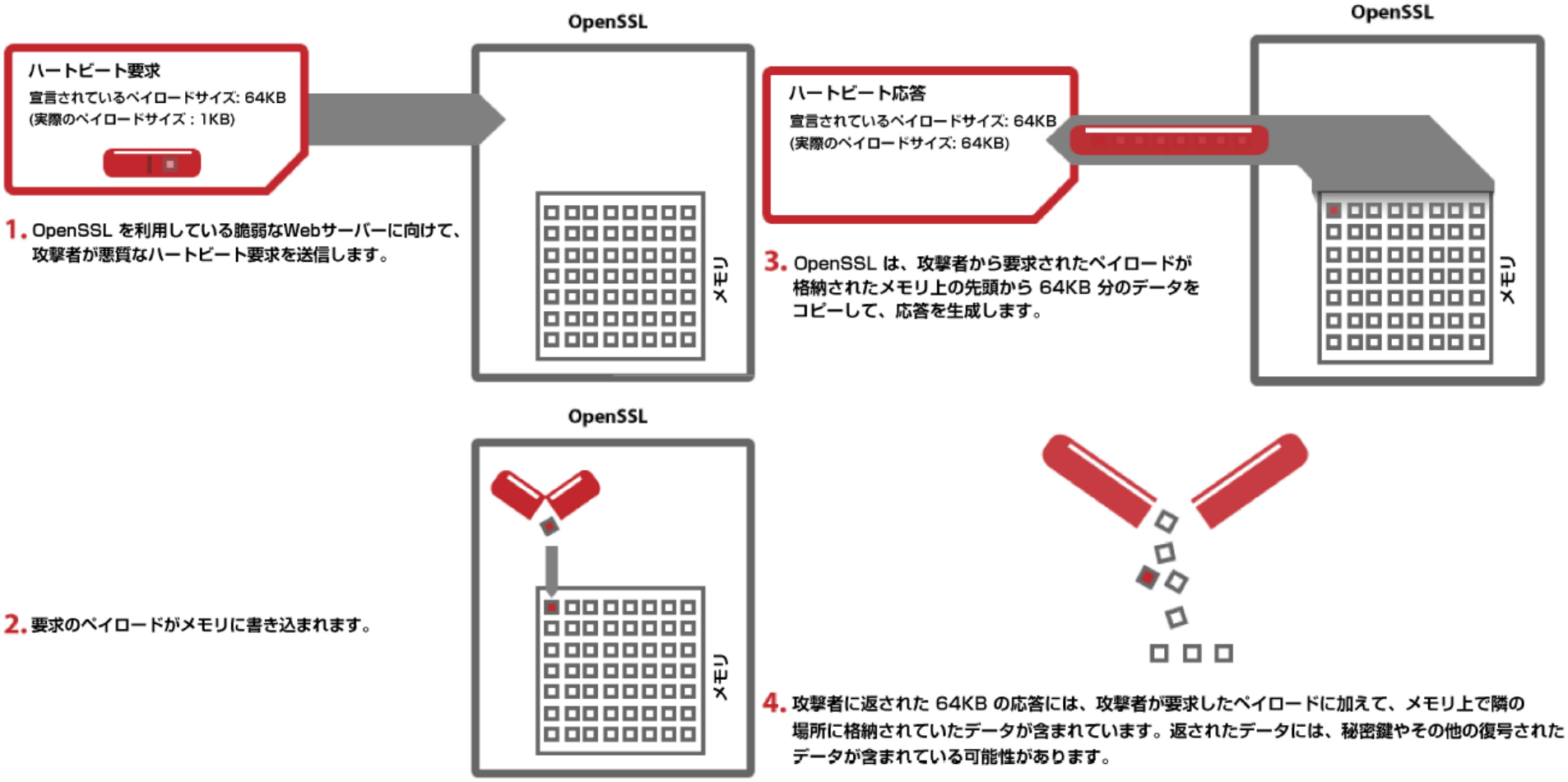
- HeartBleedの脆弱性を狙われることで、以下の情報が漏えいします。
  - パスワードやクレジットカード番号などの個人情報
  - サーバーの秘密鍵

1. ウェブサーバーの鍵ペア(公開鍵+秘密鍵)を生成
2. 公開鍵を、CSR(証明書署名要求)として認証局へ提出
3. 秘密鍵はサーバ管理者が厳重に保管
4. 認証局は、申請情報および申請者の認証を行う
5. 認証OKの場合、認証済み証明書（公開鍵）を発行

- それでは秘密鍵の漏えいで何が起こるのか？
  - SSL暗号通信が、秘密鍵を盗んだ人から解読されます。
  - 偽のサイトのコピーが作られてしまいます。

「Heartbleed」による攻撃の仕組み

Heartbeat は、実際の通信が発生していない間でも TLS セッションの接続を維持する、TLS プロトコルの拡張機能です。この機能によって、双方のコンピュータがまだ接続状態にあり、通信可能であることが確認されます。最初の接続が切断された場合でも、もう一度セキュア接続を確立するときに資格情報を再入力する手間も省けます。



影響範囲と対策

- ウェブサイトの管理者は以下の対策を行う必要があります。

ウェブサイト管理者

- OpenSSL を修正版（1.0.1g）に更新 （またはHeartbeat 拡張機能を使わない）

※この脆弱性が自社サーバーに存在するかを確認するにはページ下部の確認方法を参照ください。

- OpenSSL の更新後、SSL サーバ証明書を再発行 （シマンテックとジオトラストは、無償で再発行）
- 「SSL サーバ証明書」の入れ替えが完了したら、古い証明書は失効(リボーク)
- エンドユーザーのパスワードをリセットすることも検討

脆弱性の有無の確認方法

- SSL ToolboxでOpenSSL の脆弱性があるかを確認することが出来ます。

SSL Toolboxはhttp://www.symantec.com/jp/ssltools **へアクセスして使用方法をご確認ください。**

- SSL Toolbox で確認できるサイトは、SSL暗号通信を行うサイトのみです。HTTPでアクセスするサイトは脆弱性が無いので調べる必要がありません。
- SSL Toolboxに入力するURLはFQDNです。(以下の赤字部分がFQDNです。
<https://www.symantec.com/ja/jp/outbreak/?id=heartbleed >)

影響範囲と対策

- ウェブサイトの利用者は以下の対策・注意を行う必要があります。

消費者（ウェブサイト利用者）

- 利用するウェブサイトが安全であるか確認

※確認方法はページ下部の確認方法を参照ください。

- 利用しているウェブサイトからのパスワード変更を喚起されたら速やかに実施
- ソフトウェアもハードウェアも、ベンダーからパッチが公開されたら速やかに更新
- 公共ネットワークでは、Heartbleed に対して脆弱でないVPNクライアントを使用
- パスワード更新メールはURLに注意。（公式サイトのドメインであることなど）
- 銀行口座やクレジットカードの明細で不審な取引がないか確認

安全なウェブの確認方法

- 利用しようとしているウェブサイトの安全性を確認するウェブサイトを作成しました。

Norton Safe Webは http://safeweb.norton.com/heartbleed へアクセスして、ご利用するサイトのURLを入力ください。(入力方法は、以下をご確認ください。)

- Norton Safe Web で確認できるサイトは、SSL暗号通信を行う（URLがhttps://で始まる)サイトです。HTTPでアクセスするサイトは脆弱性が無いので調べる必要がありません。
- Norton Safe Webに入力するURLは、以下の赤字部分です。
  <https://www.symantec.com/ja/jp/outbreak/?id=heartbleed >

現時点での対応状況など

- 現時点（日本時間4/16日0時時点）での対応状況
  - Alexa ※による上位 1,000 の Web サイトはすべて、この脆弱性に対応済み
  - Alexa の上位 50,000 の Web サイトのうちHeartbleed に対して脆弱なのは 1.8%

※webサイト情報や利用状況に関するデータを集め、どれだけの人に見られているかを調査する機関

- 攻撃の状況
  - 脆弱な Web サイトに対するスキャンは広く行われていますが、そのスキャンのほとんどは研究者によるものです。
  - Heartbleed 脆弱性に関して、攻撃者が実行している大量スキャンは比較的少数しか確認されていません。（人気のあるサイトは現時点で影響を受けていません。）

- 攻撃の遮断
  - シマンテックの IPS シグネチャ 27517「Attack: OpenSSL Heartbleed CVE-2014-0160 3」がリリースされたので、脆弱なサーバーに対して Heartbleed を悪用する試みは検出され遮断されます。詳しくは、IPSベンダーにお問い合わせ下さい。
  - シマンテック クラウド型WAFの利用ユーザーは、Heartbleedの脆弱性を突いた攻撃の影響を受けません。