サイバートラスト WAF Plus 初期設定手順書

サイバートラスト株式会社

はじめに

【！】本手順書をご利用の前に必ずお読みください

1. 本ドキュメントは、サイバートラスト WAF Plus サービスのトライアルおよび製品版の導入にあたり、Imperva CloudWAF Incapsula（以下、Incapsula）の初期設定およびサイバートラストのSSLサーバー証明書の設定について解説するドキュメントです。
2. このドキュメントは予告なく変更される場合があり、サイバートラスト株式会社はその内容に対して責任を負うものではありません。また、このドキュメント内に誤りがあった場合、サイバートラスト株式会社は一切の責任を負いません。
3. このドキュメントで説明するソフトウェアはライセンスに基づいて配布されるものであり、ライセンスの条項に従った使用のみ許可されます。このドキュメントは、本来の使用目的のために発行され、公に発行されるものではありません。
4. このドキュメントの一部または全部を複製することは禁じられており、提供または製造を目的として使用することはできません。ただし、サイバートラスト株式会社との契約または同意文書で定められている場合に限り、この注記の添付を条件として複製することができます。
5. サイバートラスト株式会社から事前に書面による合意を得ない限り、このドキュメントまたはその一部から直接的または間接的に知り得た内容または主題に関して、個々の企業やその従業員などの第三者に対し、口頭、文書、またはその他のいかなる手段によっても伝達することはできません。

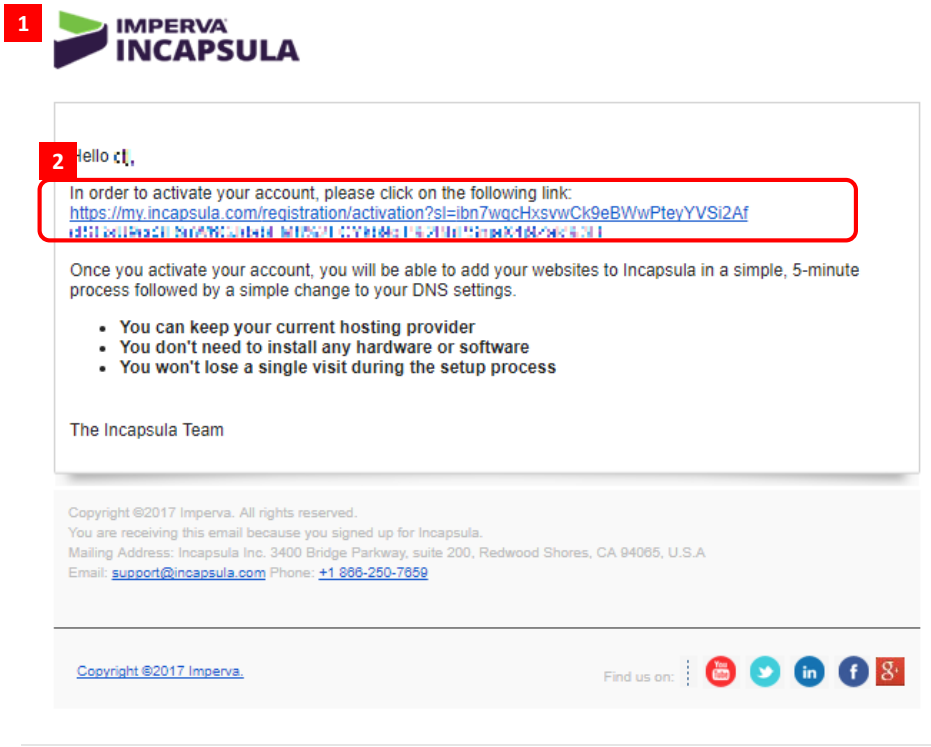
目次

1. アカウントアクティベーション　1/4

アカウントのアクティベーションを行います。

1. お客様用のアカウントが登録されましたら、Incapsulaのメールアドレス（no_reply@incapsula.com）からお客様のメールアドレスへ「Account Activation – 法人名」という件名のメールが届きます。

2. メール内のリンク（右図の赤枠内）をクリックします。
ブラウザが起動し、アカウント登録画面に遷移します。



1. アカウントアクティベーション　2/4

3. 以下の必要事項を入力します。
   - ■First name（名前）
   - ■Last name（名字）
   - ■Company（法人名）
   - ■Role（役職名）
   - ■Email address（メールアドレス）
   - ■Password（パスワード）
   - ■Confirm Password（確認用パスワード）

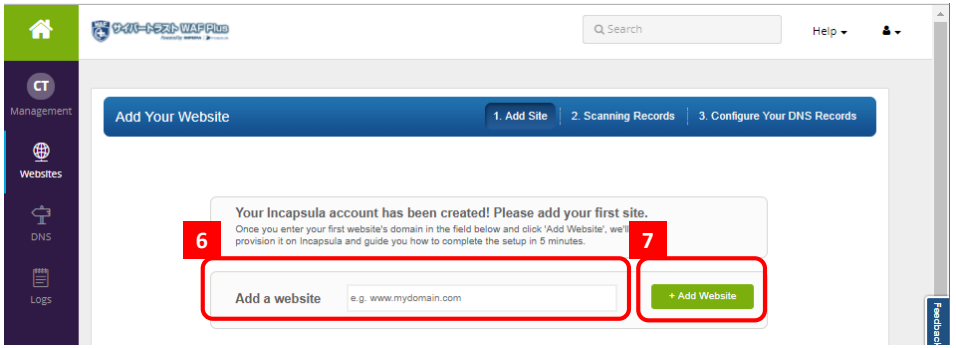
   ※Company（法人名）とRole（役職名）以外の項目は後から変更可能です。

4. 「I agree to the Terms of use」にチェックを入れます。
   ※ Terms of use をご確認ください。

5. 「CREATE MY ACCOUNT」をクリックします。

1. アカウントアクティベーション　3/4

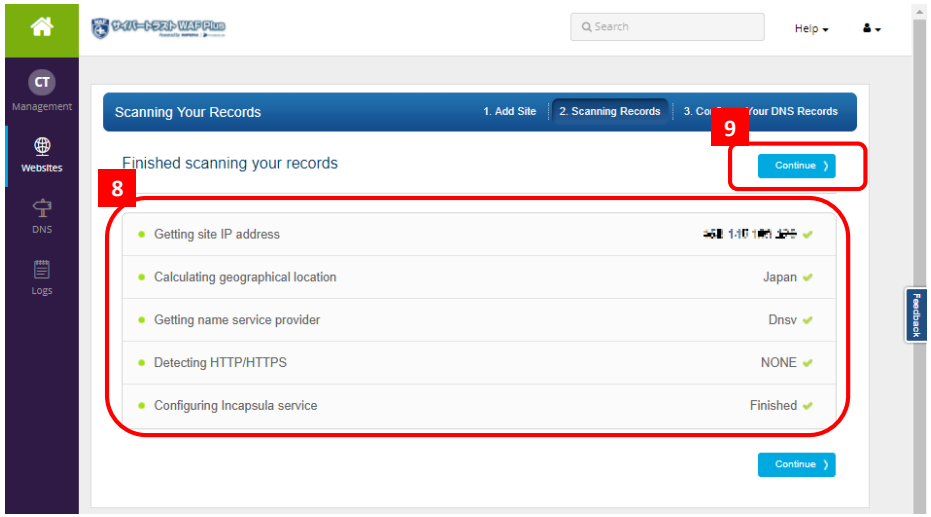
6. 「Add a website」に設定を行うWEBサイトのFQDNを入力します。
   ※FQDN入力例
   URL：https://**www.cybertrust.ne.jp**/index.html
   ⇒　www.cybertrust.ne.jp を入力



7. 「+ Add Website」をクリックします。

8. Incapsulaが入力したFQDNの情報を正しく取得できた場合、WEBサーバの情報が表示されます。

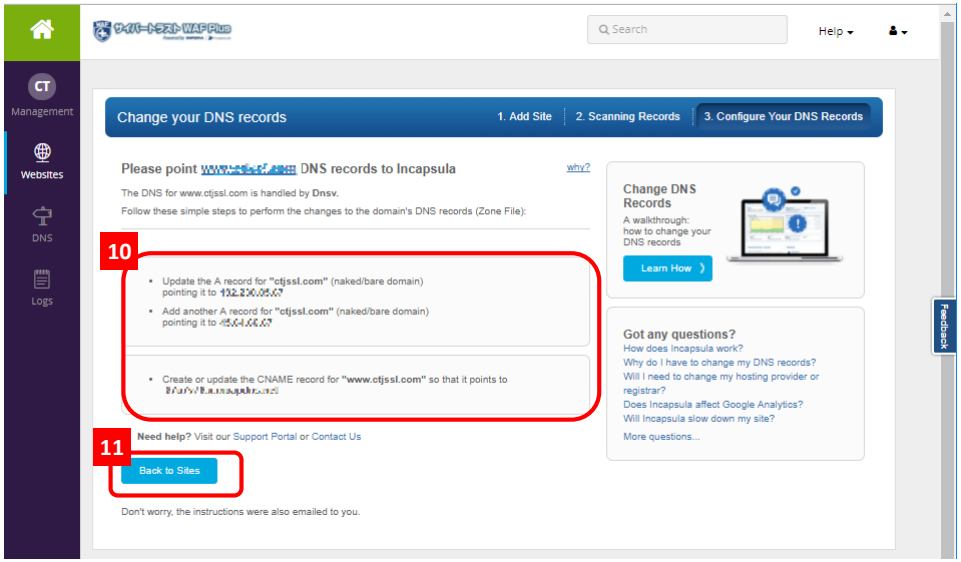
9. 「Continue」をクリックします。



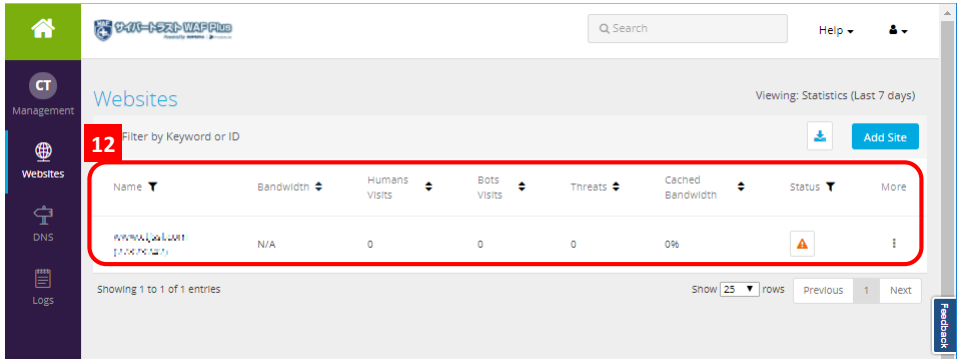
1. アカウントアクティベーション　4/4

10. DNSレコードの変更に関するメッセージが表示されます。
※Incapsulaのメールアドレス（no_reply@incapsula.com）からお客様のメールアドレスへ「Incapsula Service Setup for FQDN」という同内容のメールが届きます。

11. 「Back to Sites」をクリックします。



12. アカウントの登録が完了します。



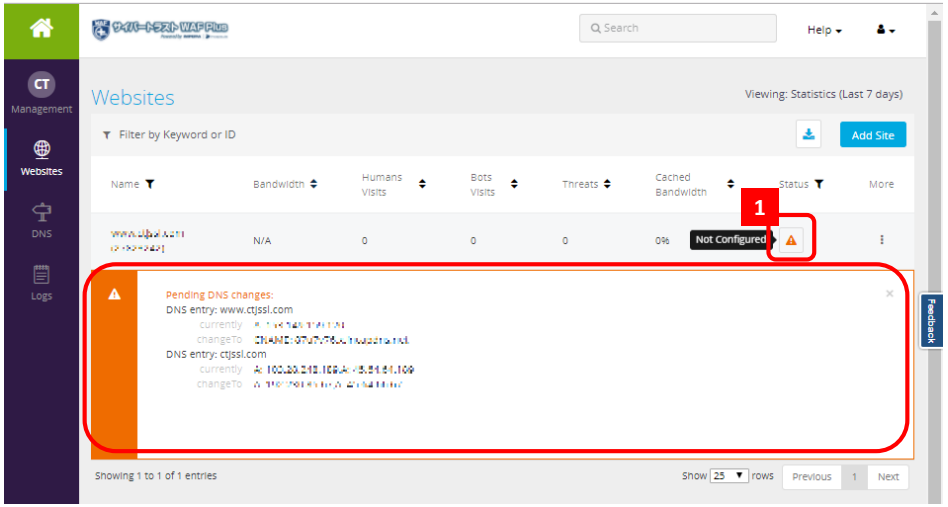
以上で、アカウントのアクティベーションは完了です。
※DNS設定の変更前に、動作確認される場合には「（ご参考4）事前確認方法」をご参照ください。

2. DNSの設定

※管理ポータルへログインした際に Status が「Not Configured」と表示されている場合のみ、本手順を行ってください。

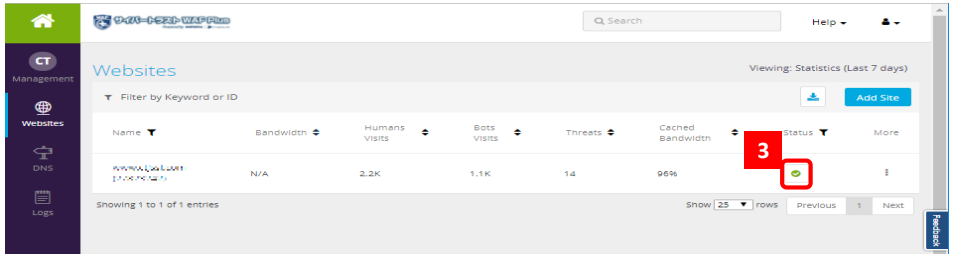
※CNAMEレコードを登録済みでIncapsulaが参照可能な場合、本手順は不要です。
※設定が完了した場合、Incapsulaのメールアドレス（no_reply@incapsula.com）からお客様のメールアドレスへ「DNS changes for “FQDN” were performed successfully」というメールが届きます。

1. Incapsulaの管理ポータルへログイン後、Statusのアイコンをクリックし、表示された値を確認し、DNSサーバーの設定を変更します。
   ※Aレコードが登録されている場合は、Aレコードを削除のうえ、CNAMEレコードとして登録します。



2. Incapsulaに情報が反映されるまで数分待ちます。

3. Statusが「Fully Configured」に表示が変わりましたら、設定完了です。



以上で、DNS レコードの設定は完了です。

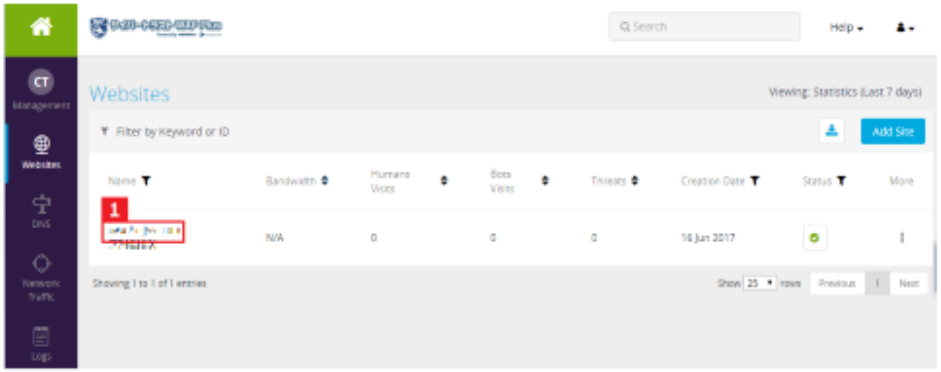
3. SSLサーバー証明書の設定　1/6

サイバートラストのSSLサーバー証明書を設定します。

※アップロードするファイル形式は、「PKCS#12形式」もしくは「PEM形式」のいずれかである必要があります。

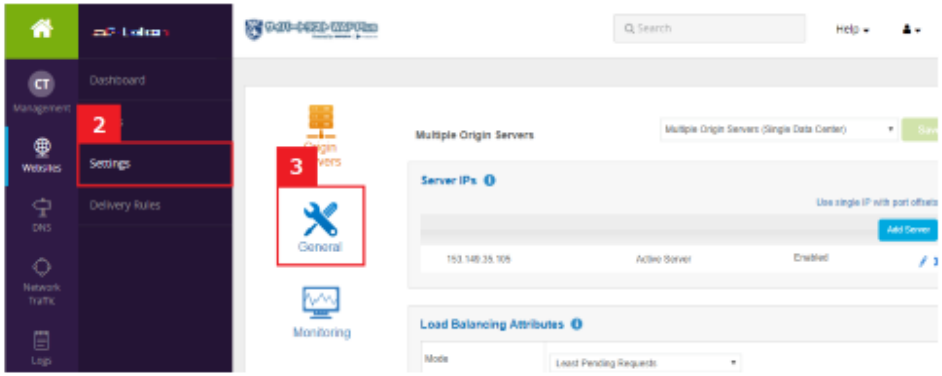
※オリジンサーバーと同じ証明書を設定する場合は、P22以降で記載の手順でも設定可能です。

1. Incapsulaの管理ポータルへログイン後、WEBサイトのFQDNをクリックします。



2. 「Settings」をクリックします。

3. 左側のメニューより「General」をクリックします。



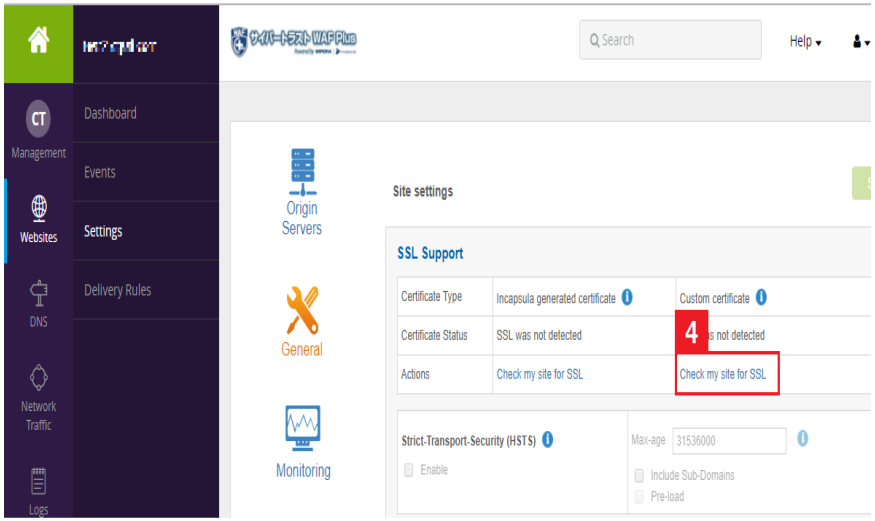
3. SSLサーバー証明書の設定　2/6

4. 「SSL Support」内の
「Check my site for SSL」をクリックします。

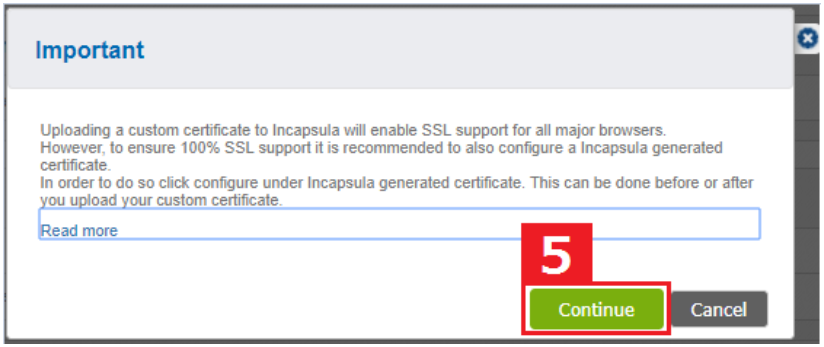
※PEM形式のファイルをアップロードする場合は、
「A)PEM形式（.cerや.PEM）の場合」を参照ください。

※PKCS#12形式のファイルをアップロードする場合は、
「B)PKCS#12形式（.pfx）の場合」を参照ください。

※オリジンサーバーと同じ証明書を設定する場合は、
P23に記載の手順でも設定可能です。



5. 「Continue」をクリックします。



3. SSLサーバー証明書の設定　3/6

A) PEM形式（.cerや.pem）の場合

a. お客様証明書と中間CA証明書を以下の順序で1つのファイルに連結します。

1. お客様証明書
2. 中間CA証明書
3. クロスルート証明書（必要な場合）

※中間CA証明書は、以下弊社ホームページからダウンロードしてください。

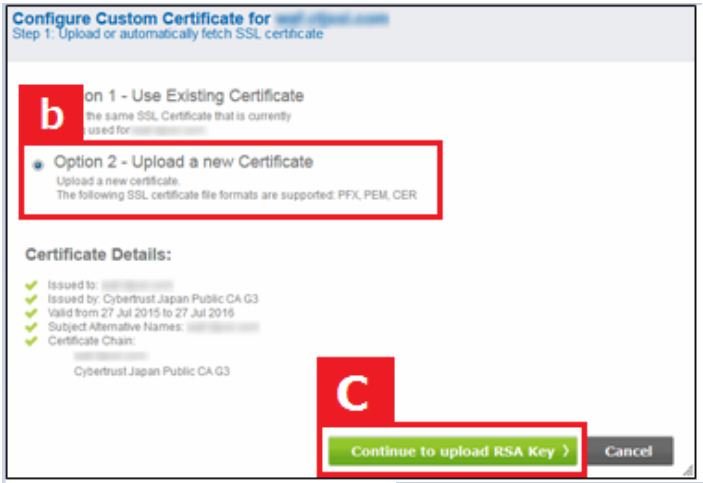
▼ルート・中間CA証明書のダウンロード
https://www.cybertrust.ne.jp/sureserver/support/download_ca.html

```
a
----BEGIN CERTIFICATE-----
お客様証明書
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
中間証明書
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
クロスルート証明書
-----END CERTIFICATE-----
```

b. 「Option 2 – Upload a new Certificate」にチェックをいれ、設定する証明書ファイルを指定します。

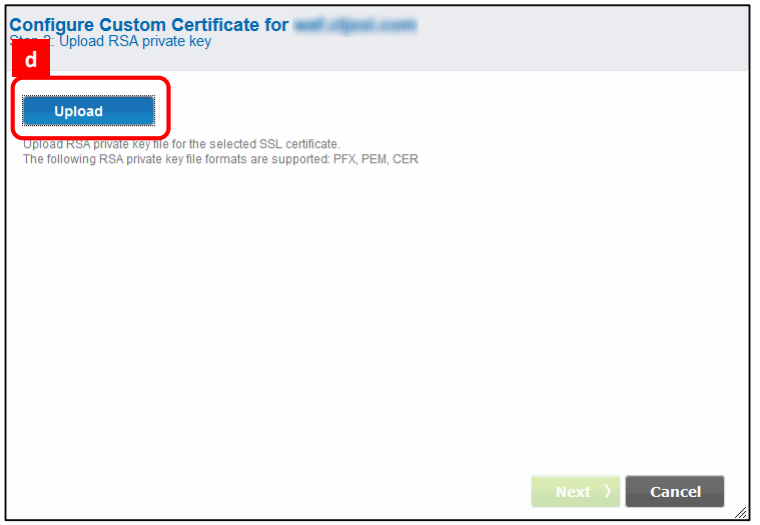
※証明書の連結順序に誤りがある場合、「Certificate Details」に「×（バツ）」が表示されます。

c. 「Continue to upload RSA Key」をクリックします。

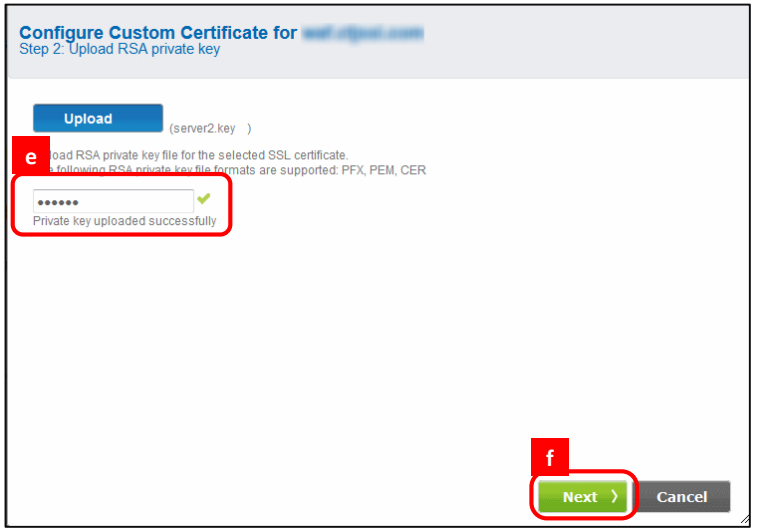


3. SSLサーバー証明書の設定　4/6

d.　「Upload」をクリックし、秘密鍵ファイルをアップロードします。



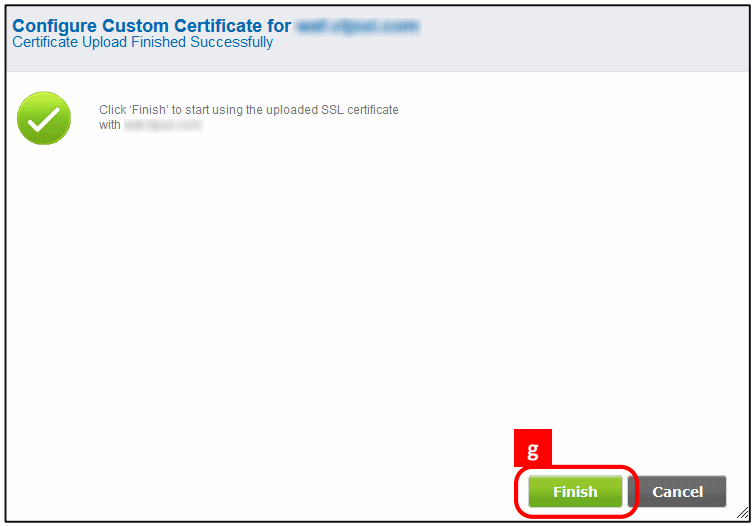
e.　秘密鍵にパスフレーズを設定している場合は、パスフレーズ入力用のテキストボックスが表示されますので、パスフレーズを入力します。



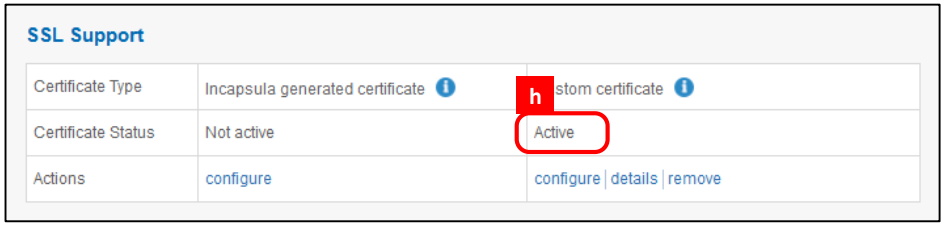
f .　「Next」をクリックします。

3. SSLサーバー証明書の設定　5/6

g.　「Finish」をクリックします。



h.　SSL設定の完了後、
「Certificate Status」が「Active」に変わります。



3. SSLサーバー証明書の設定　6/6

B）PKCS#12形式（.pfx)の場合

a. お客様証明書と秘密鍵ファイルを含む「.pfx」ファイルをあらかじめ作成します。pfxファイルには中間CA証明書、クロスルート証明書を含めます。

※中間CA証明書は、以下弊社ホームページからダウンロードしてください。

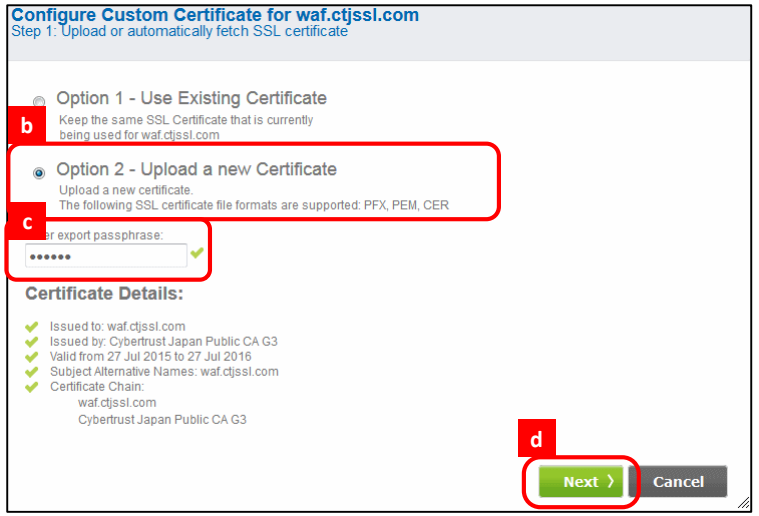
▼ルート・中間CA証明書のダウンロード
https://www.cybertrust.ne.jp/sureserver/support/download_ca.html

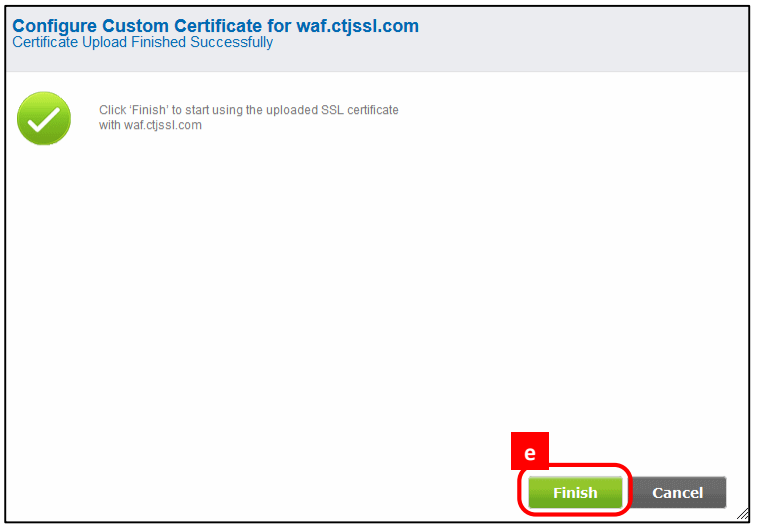
b. 「Option 2 – Upload a new Certificate」にチェックをいれ、設定するpfxファイルを指定します。

c. パスフレーズの入力欄が表示されるため、ファイルをエクスポートした際に設定したパスフレーズを入力します。

d. 「Next」をクリックします。

e. 「Finish」をクリックします。





3. SSLサーバー証明書の設定　5/6

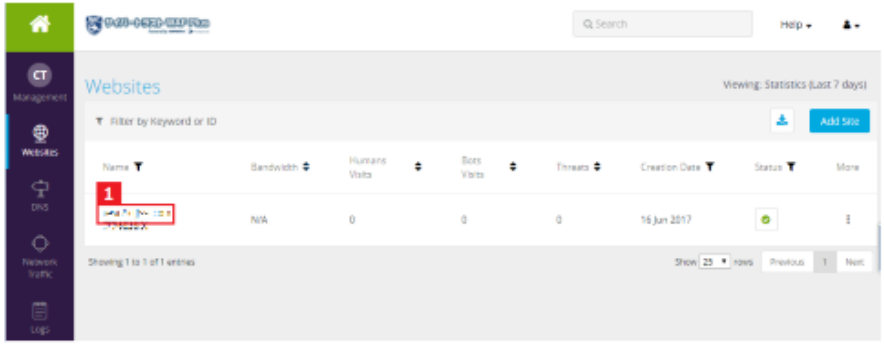
f.　SSL設定の完了後、
「Certificate Status」が「Active」に変わります。

以上で、 SSLサーバー証明書の設定は完了です。

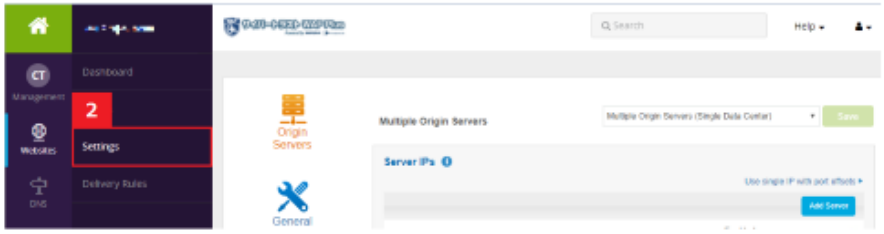
4. WAF機能の初期設定　1/2

WAF機能の初期設定を行います。

1. Incapsulaの管理ポータルへログイン後、WEBサイトのFQDNをクリックします。



2. 「Settings」をクリックします。



3. 左側のメニューより「WAF」をクリックします。

4. WAF機能の初期設定　2/2

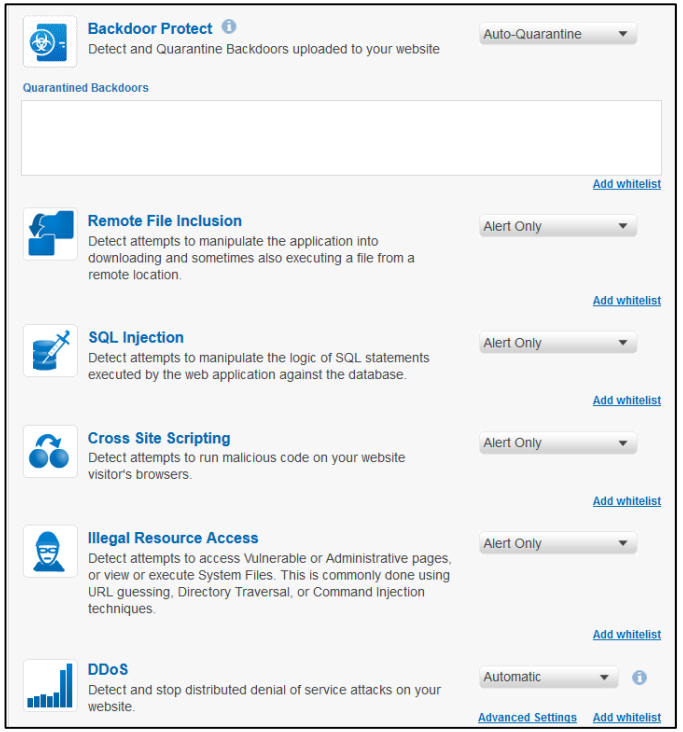
4. 各脅威について保護レベルを任意で設定します。

   ※初期設定は、「Alert Only（警告のみ）」攻撃をブロックするには、「Block Request」以上に設定してください。

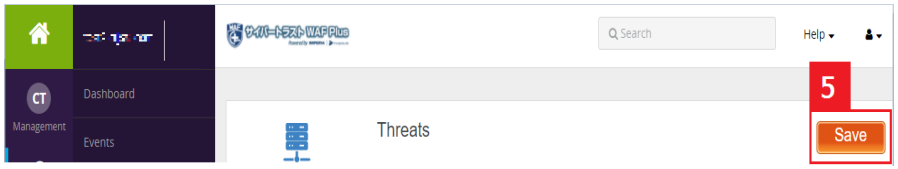
   ※設定値は以下の5つから選択可能です。

   a. Alert Only（警告のみ）
   b. Block Request（リクエストのブロック）
      脅威をあたえるリクエストが確認された場合にブロック
   c. Block User（ユーザーのブロック）
      上記に加え、当該ユーザからのリクエストを全てブロック （Cookie値によってユーザを識別）
   d. Block IP（IPアドレスのブロック）
      上記に加え、該当IPからのリクエストを10分間ブロック
   e. Ignore（無視）

   ※上記はBackdoor ProtectとDDoSを除きます。



5. 設定変更を行った場合は、画面右上の「Save」をクリックします。

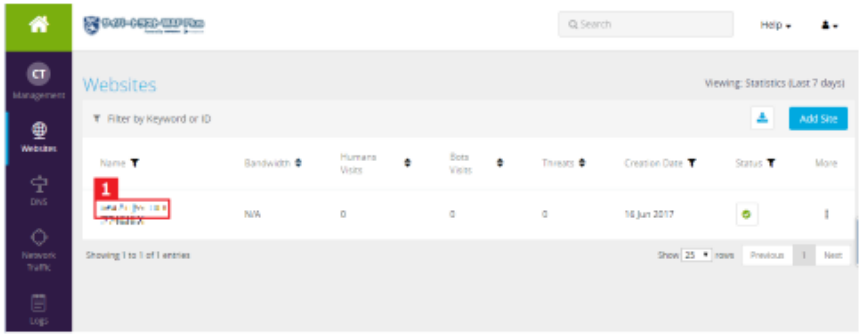


以上で、WAF機能の初期設定は完了です。

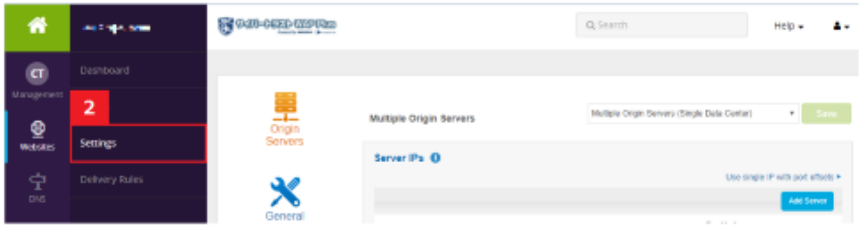
5. 通知機能の設定　1/2

PCI Compliance Reportの配信方法および各脅威ごとのアラートやブロックの通知有無を設定します。

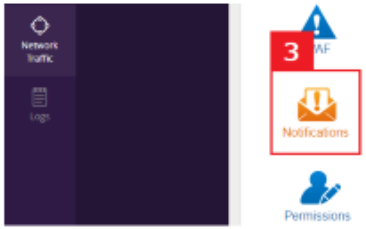
1. Incapsulaの管理ポータルへログイン後、WEBサイトのFQDNをクリックします。



2. 「Settings」をクリックします。



3. 左側のメニューより「Notifications」をクリックします。



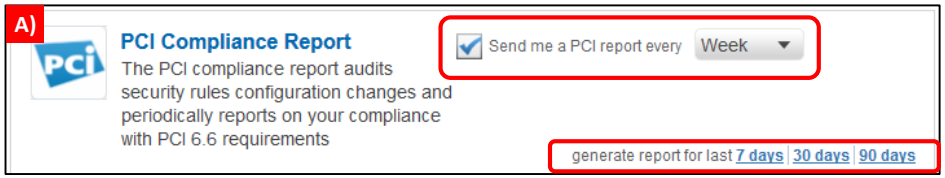
5. 通知機能の設定　2/2

A) PCI Compliance Report

「Send me a PCI report every」にチェックを入れ、プルダウンからレポートの作成期間を以下より選択します。設定期間に応じてレポートが自動で発行、配信されます。

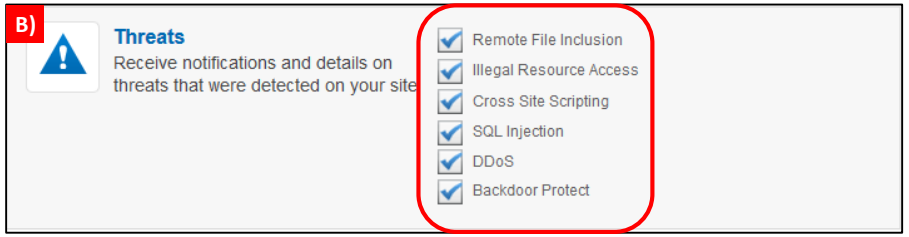
・Week（週ごと＝7日）
・Month（月ごと＝30日）
・Quarter（四半期ごと＝90日）

「generate report for last」の日数をクリックすると、それぞれの日数に合わせたレポートが即時発行されます。

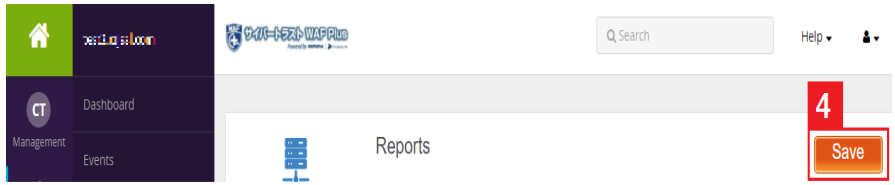


B) Threats

各脅威にチェックを入れると、Incapsulaが検知したアラートやブロックについてメールにて通知されます。



4. 設定変更を行った場合は、画面右上の「Save」をクリックします。

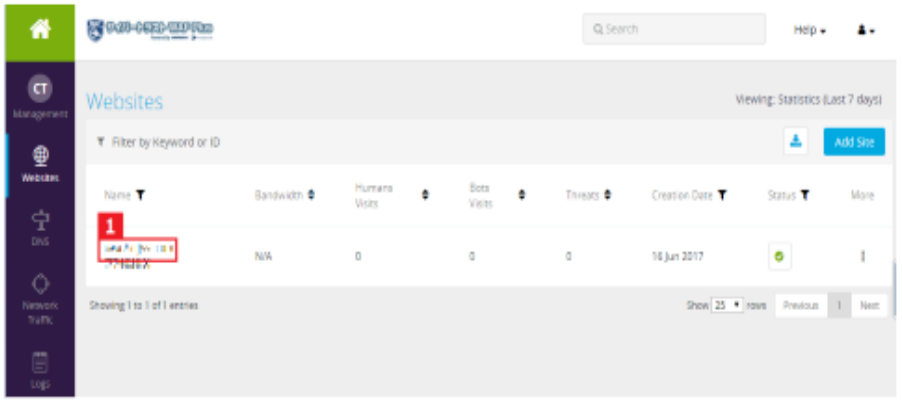


以上で、通知機能の設定は完了です。

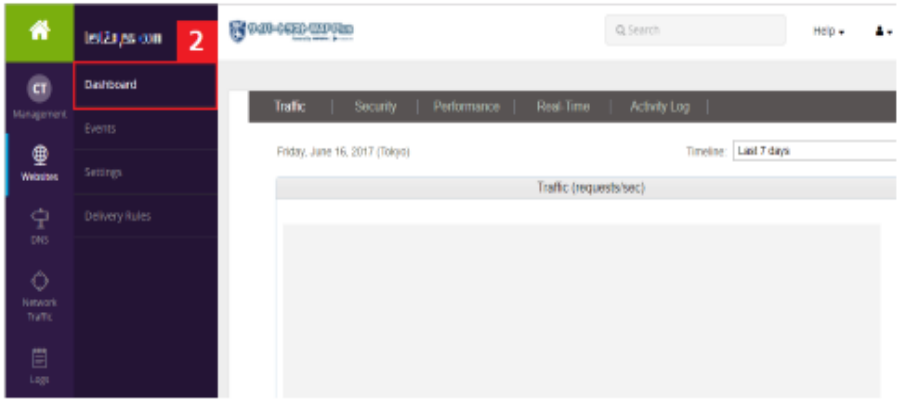
6. Trafficの確認手順　1/3

TrafficはDashboardで確認できます。

1. Incapsulaの管理ポータルへログイン後、WEBサイトのFQDNをクリックします。



2. 「Dashboard」をクリックします。



6. Trafficの確認手順　2/3

「Traffic」タブ

①Traffic…トラフィック

サイト訪問者によるIncapsulaへのトラフィックを表示します。

※IncapsulaからWEBサーバーへの通信は含まれません。

②Visits by client…アプリケーション単位の訪問割合

サイト訪問者が接続時に使用したアプリケーションを表示します。

③Visit by country…国別の訪問割合

接続元の国を表示します。

④Total Visits…合計訪問数

サイトへの訪問者数（オリジナルIPアドレス数）を表示します。

⑤Total Hits…合計ヒット数

WEBコンテンツに対する接続数の合計を表示します。WEBページ、画像ファイル、CSSファイルなどに対する各リクエストを1つとします。

⑥Bits per second(95 percentile）…BPS（ビット毎秒）

1秒間の送信データのビット数を表示します。95パーセンタイルで計算（上位5%を排除）します。リクエストとレスポンスの両方が含まれます。　※ WAF利用帯域の確認が行えます。

⑦Bandwidth…帯域幅

総通信量（WEBサーバーへのリクエスト、およびWEBサーバーからのレスポンス）を示します。

6. Trafficの確認手順　3/3

「Traffic」タブ

⑧Visits…訪問数

サイトへの訪問者数（オリジナルIPアドレス数）を表示します。

⑨Hits per second…ヒット毎秒

1秒間のWEBコンテンツに対する接続数を表示します。

⑩Accumulated bandwidth…累積帯域幅

DN機能によってIncapsulaのネットワーク内にコンテンツをキャッシュし、 CDNで削減したWEBサーバーに到達するはずであったトラフィックの累積帯域幅を表示します。

⑪Bits per second…BPS（ビット毎秒）

1秒間の送信データのビット数で、WAF帯域幅を表示します。

※ WAFの利用帯域の詳細を確認できます。

⑫Daily hits…ヒット数/日

1日のサイト訪問者数（オリジナルIPアドレス数）を表示します。

⑬HTTP versions…HTTP Versionの割合

HTTP/1.1 及び HTTP/2.0 の接続の割合を表示します。

Trafficの確認手順は以上です。

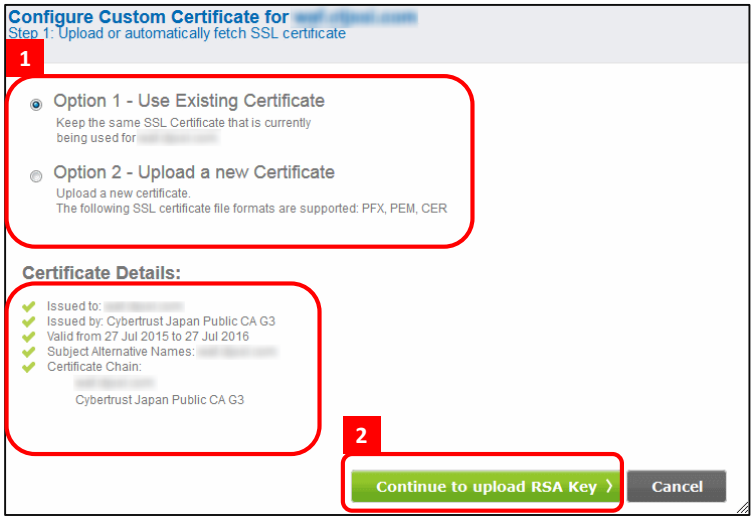
(ご参考1) SSLサーバー証明書の設定

オリジンサーバーの証明書と同じ証明書を使用する場合の手順です。

1. 「Option 1- Use Existing Certificate」が自動選択されます。また、Incapsulaが自動取得したオリジンサーバーの証明書情報が表示されます。
   ※オリジンサーバーの証明書設定が完了している必要があります。

2. 「Certificate Details」の表示情報に誤りがなければ、「Continue to upload RSA Key」をクリックします。

3. P13「5. SSLサーバー証明書の設定」の「d.」以降の手順を行います。



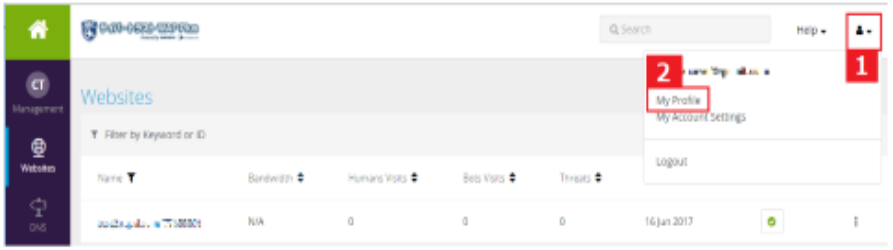
(ご参考2) アカウントパスワードの変更手順

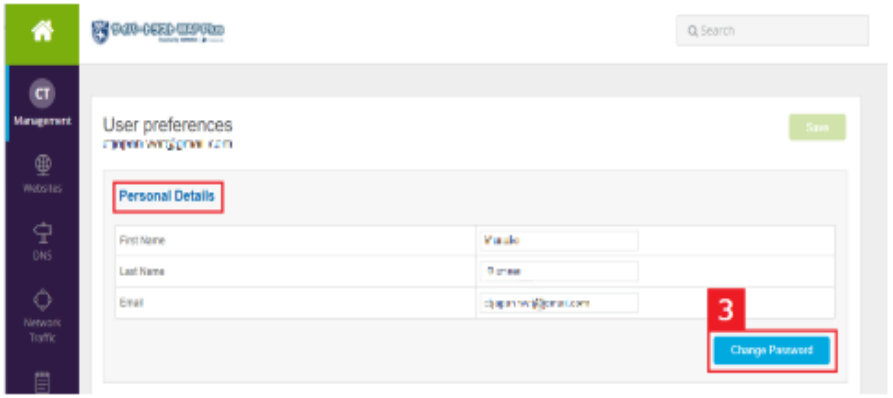
P5「1. アカウントアクティベーション」の「3.」で登録したアカウントのパスワードを変更する場合の手順です。

1. Incapsulaの管理ポータルへログイン後、右上の人型のアイコンをクリックします。

2. 「My Profile」をクリックします。

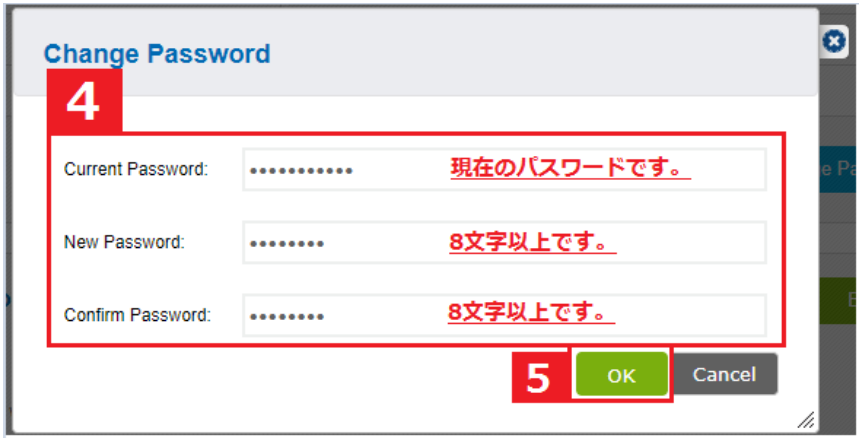
3. 「Personal Details」の「Change Password」をクリックします。





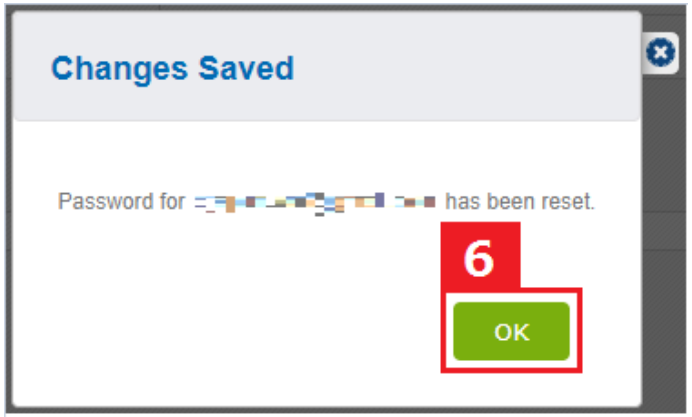
(ご参考2) アカウントパスワードの変更手順

4. 以下の項目を入力します。
   - ■Current Password（現在のパスワード）
   - ■New Password（新しいパスワード）
   - ■Confirm Password（確認用パスワード）



5. 「OK」をクリックします。

6. 「OK」をクリックします。

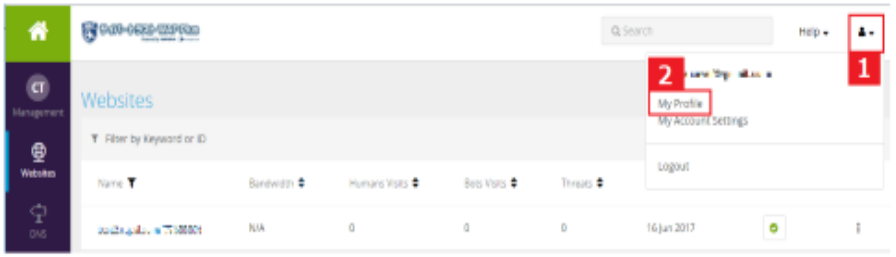


以上で、アカウントパスワードの変更は完了です。

(ご参考3) アカウント情報の変更

P5「1. アカウントアクティベーション」の「3.」で登録したアカウントの情報を変更する場合の手順です。

1. Incapsulaの管理ポータルへログイン後、右上の人型のアイコンをクリックします。
2. 「My Profile」をクリックします。



3. 「Personal Details」の項目に、新しい情報を入力します。
   - ■First name（名前）
   - ■Last name（名字）
   - ■Email address（メールアドレス）
4. 設定変更後、「Save」をクリックします。

以上で、アカウント情報の変更は完了です。

（ご参考4）事前確認方法

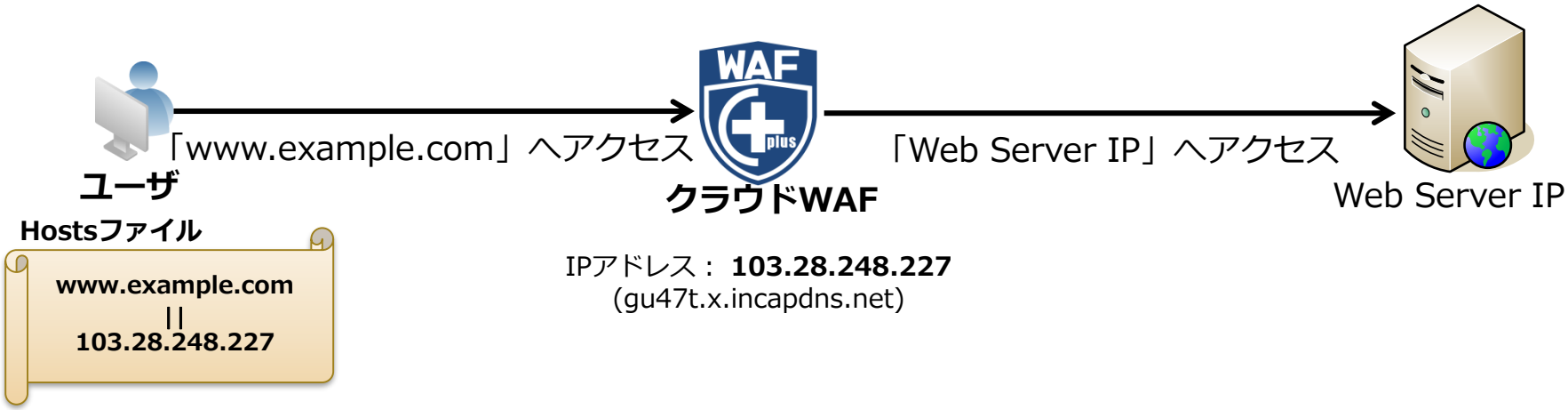
事前確認の方法

はじめに

以下の理由から、トライアル時はクライアントPCのHostsファイルへ設定を追加し、対象サイトへアクセスしていただきます。

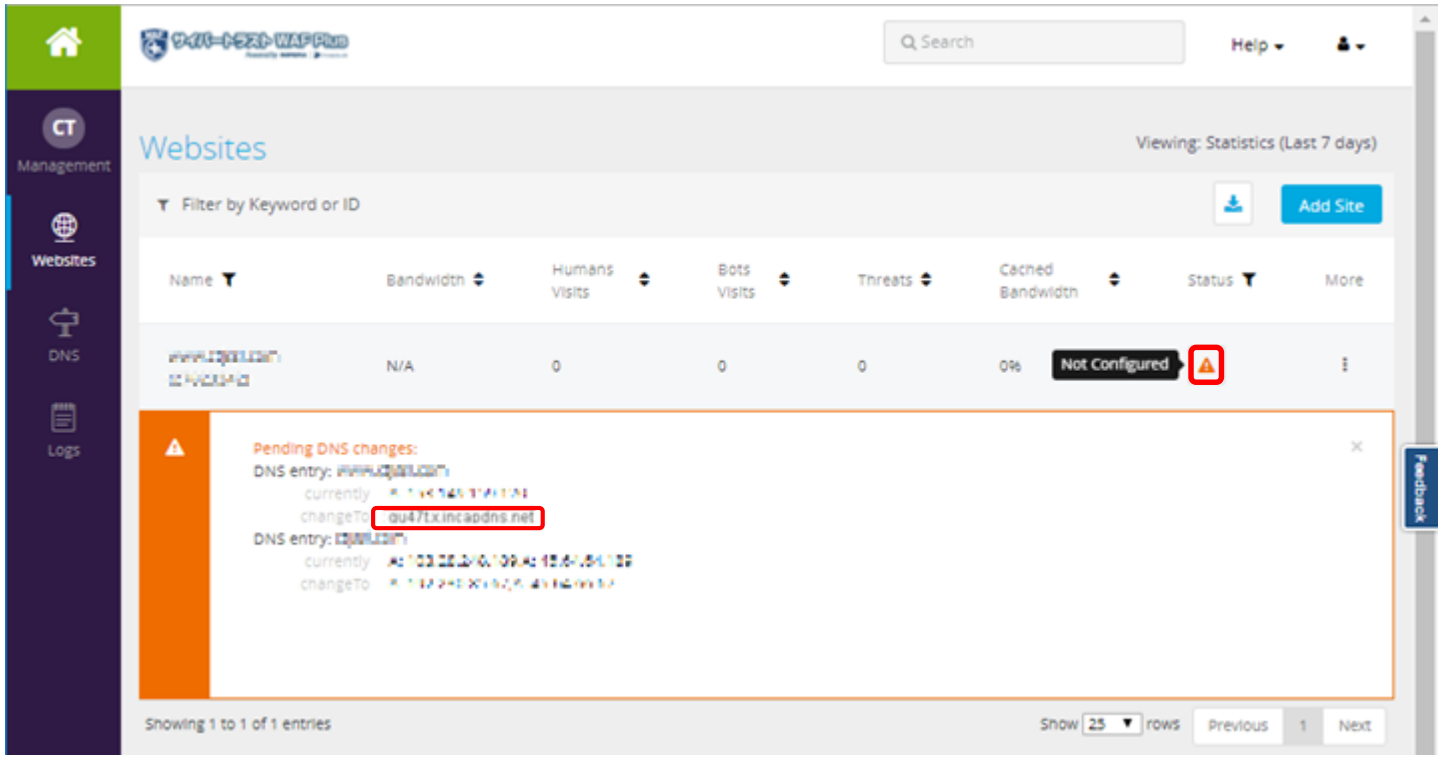
- 本番環境へ影響を与えずにトライアルを行う為
- Webサイトの構成に影響を受けず、トライアルを行う為
- IP直打ちのリクエストをクラウドWAFは拒否する為

アクセスイメージ図



CNAMEの確認

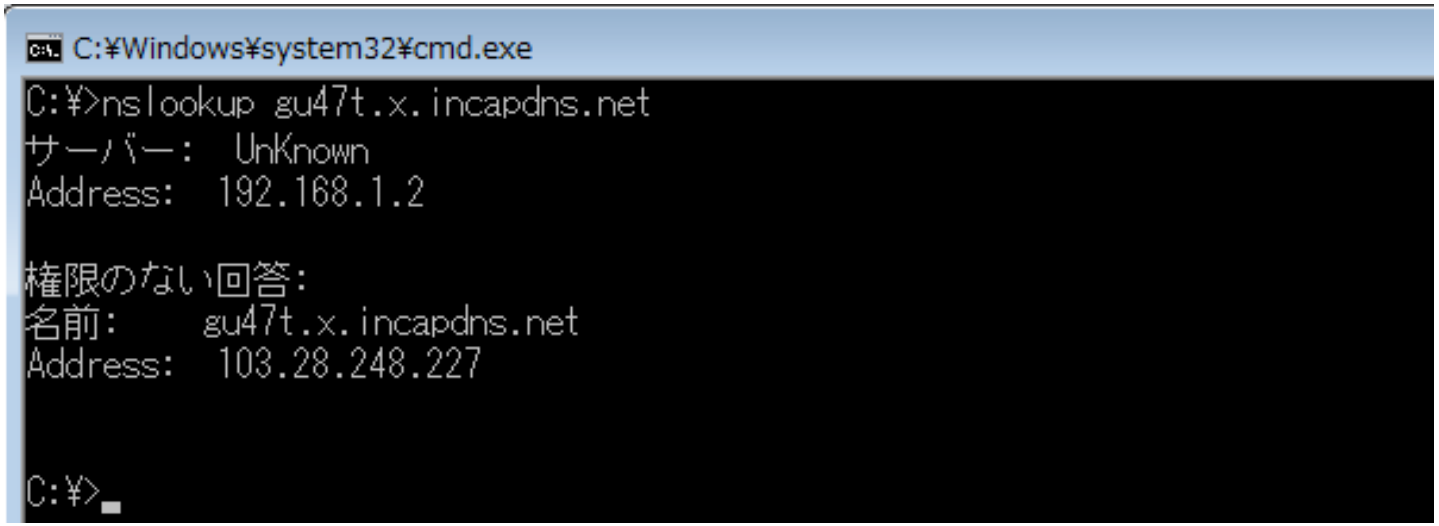
- Hostsへの設定追加
  - まずアカウントアクティベーションの際に、DNS設定変更で指定されたCNAMEのIPアドレスをnslookupで確認します。
    - CNAME先として指定されたFQDNは Status詳細で確認できます。
    - **今回は例として**「gu47t.x.incapdns.net」です。



IP Addressへの返還方法

- Hostsへの設定追加
  - コマンドプロンプトを起動し、nslookupコマンドで「gu47t.x.incapdns.net 」のIPアドレスを確認します。
  - 以下が実行例です。

「gu47t.x.incapdns.net 」のIPアドレスは「103.28.248.227」です。



Hosts ファイル

- Hostsへの設定追加
  - 「gu47t.x.incapdns.net 」のIPアドレスが確認できたので、そのIPとフェーズ01で初めに登録した、保護対象のFQDNを、Hostsファイルで関連付けます。
  - 以下に保存されているHostsファイルをテキストエディタで開き設定を追加し、上書き保存します。

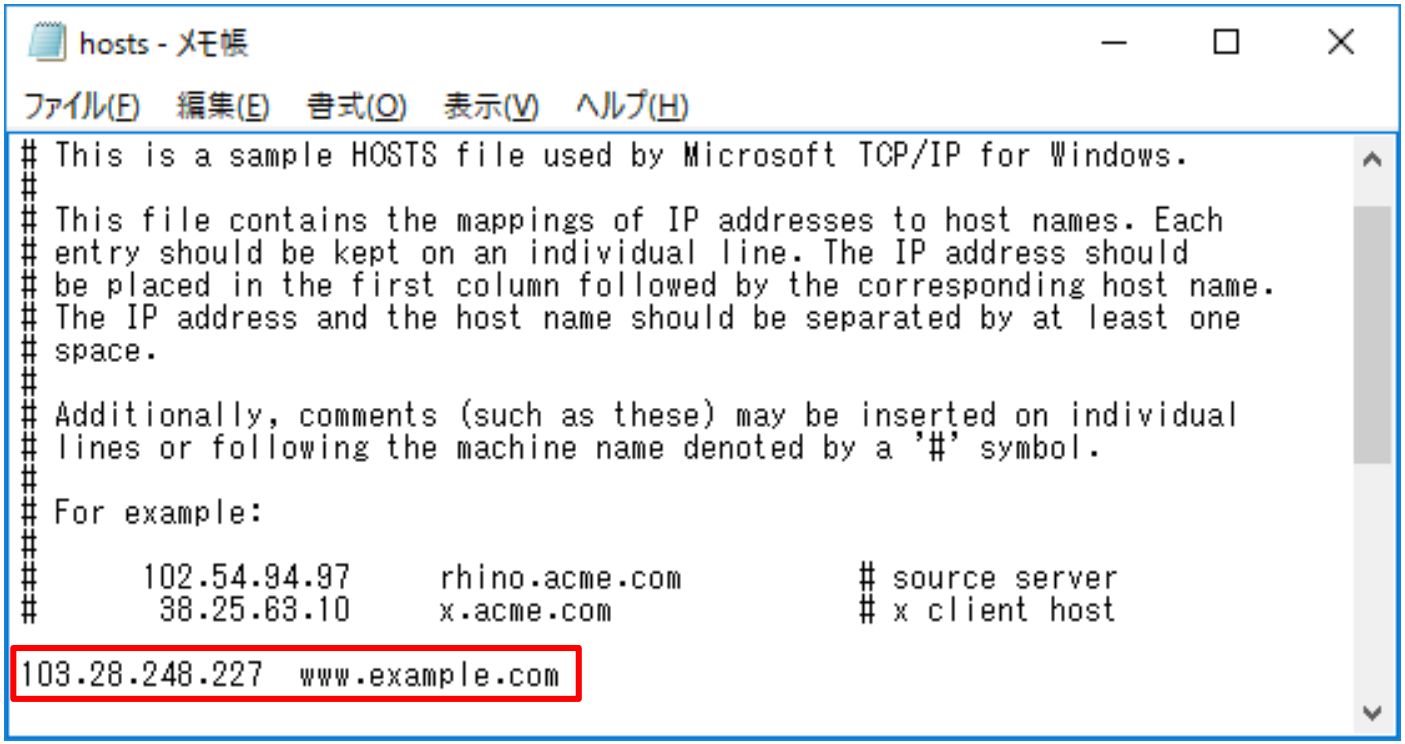
該当 OS	保存先
Windows XP/Vista/7	C:¥Windows¥System32¥drivers¥etc¥hosts
Windows NT/2000	C:¥WinNT¥System32¥drivers¥etc¥hosts
Windows95／98／ME	C:¥Windows

  - 実行例は次のスライドをご確認ください。

Hostsファイルへの変更内容

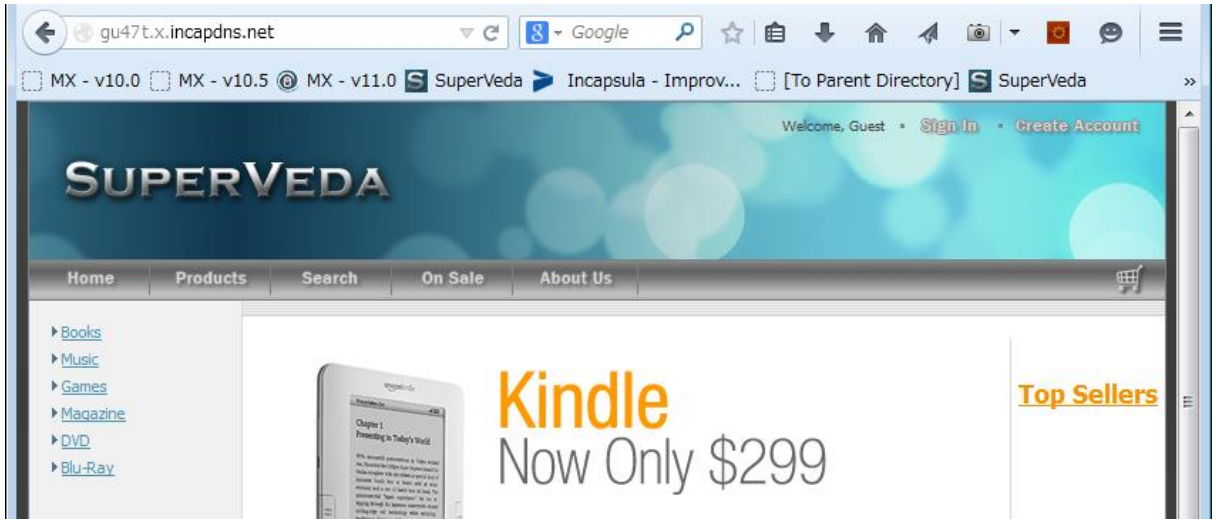
- Hostsへの設定追加
  - 実行例は以下です。

    【設定値】
    - 103.28.248.227　　:クラウドWAFが指定したCNAME先FQDNの**IPアドレスの例**
    - www.example.com　:保護対象WebサーバのFQDN**の例**



アクセス確認方法

- Hostsへの設定追加
  - 以上で、Hostsへの設定追加は完了です。
- アクセス確認①
  - ブラウザで「gu47t.x.incapdns.net」へアクセスし、保護対象サイトが表示されることを確認します。



事前検証の開始

- アクセス確認
  - 以上でアクセス確認が完了です。
  - クラウドWAFのトライアルを行う際は、Hosts設定を変更したクライアントPCから保護対象WebサイトのFQDN（例：www.example.com）へアクセスしてください。

- 注意事項
  - トライアル終了後やトライアル中断時は、追加したHosts設定を無効化する事をお勧めします。
    - 無効化は、「追加した設定の削除」または「追加した設定の行の先頭に#を入れる」を行い保存ことによって可能です。

https://www.cybertrust.ne.jp