

Cloud Web Application Firewall(旧:Incapsula)における セキュリティインシデントに関するお詫びとご報告

謹啓 貴社ますますご清栄のこととお慶び申し上げます。平素は格別のご高配を賜り厚く御礼申し上げます。

この度、Imperva 社の Cloud Web Application Firewall(旧:Incapsula) (以下、Cloud WAF)においてセキュリティインシデントが発生し、情報流出の可能性が認められました。

お客様および関係者の皆様に多大なるご心配とご迷惑をおかけいたしますこと、深くお詫び申し上げます。

本件につきまして、下記のとおりご報告申し上げます。

謹白

記

1. 本事象の内容

2019年8月20日(米国太平洋時間)に外部よりImperva社のCloud WAFをご契約いただいている一部のお客様の情報が外部より閲覧可能であるという報告を受けました。

現在、本セキュリティインシデントの詳細は調査中ではございますが、対象範囲は以下の情報となります。

- メールアドレス
- ソルトおよび暗号化されたパスワード
- API Key
- お客様が登録された証明書(Custom SSL Certificate)

2. 本事象の影響範囲

現時点で確認ができている本インシデントの影響範囲は以下のとおりです。

- 2017年9月15日までにCloud WAFをご契約いただいたお客様

なお、WAF Gateway(旧:SecureSphere)などImperva社のその他製品及びサービスをご利用いただいているお客様への影響はございません。

3. 本事象の原因

現在調査中につき、原因の詳細が判明いたしましたら改めてご報告申し上げます。

4. Cloud WAF をご利用いただいているお客様へのご依頼

影響範囲に関わらず、Cloud WAF ユーザー様には以下のご対応を推奨いたします。

- Cloud WAF 管理 Web GUI (MY) のログインパスワード変更
MY URL: <https://my.incapsula.com/admin/login>
- 2 要素認証の有効化 / シングルサインオンの利用 (SSO)
- API Key のリセット
- 新しい Custom SSL Certificate の発行/登録

設定方法に関してご不明ございましたら NVC サポート窓口: nvc-tac@nvc.co.jp にお問い合わせください。

5. 今後の対応について

Imperva 社の Cloud WAF 製品開発、情報セキュリティ、運用、サポートの各分野の関連メンバーにより組織された本インシデント特別調査チームにより 24 時間体制で調査を継続しております。また、本インシデントの調査のため、外部のフォレンジック専門会社とも協力し適切な機関への報告も行っております。

今後、メーカからの調査結果の進捗に応じて改めてサポートサイトでご報告いたします。

6. 本件のお問い合わせ先について

本件に関してご質問等ございましたら、お手数ですが下記情報とともに、各窓口までお問い合わせください。

- ご提供いただきたい情報
 - Cloud WAF アカウント管理者様の email アドレス
 - お客様の会社名、お名前
 - サポート証書記載の契約番号もしくは登録番号
- お問い合わせ窓口
 - 現在、Cloud WAF をご契約いただいているお客様
NVC サポート窓口: nvc-tac@nvc.co.jp
 - 過去に Cloud WAF をご契約いただいていたお客様
担当営業、もしくは以下のメールアドレスまでご連絡ください。
NVC 営業部窓口: sales@nvc.co.jp

以上