2020 年 7 月 2 日

報道関係者各位
ニュースリリース

fjconsulting, INC.

ｆｊコンサルティング株式会社

PCI DSS に対応した「インシデント対応演習サービス」の提供を開始

ｆｊコンサルティング株式会社（本社：東京都千代田区　代表取締役 CEO　瀬田陽介）は、2020 年 7 月より、「PCI DSS インシデント対応演習サービス」の提供を開始いたします。ペイメントカードのデータセキュリティの国際基準である PCI データセキュリティ基準（以下、PCI DSS（※））では、クレジットカード情報の流出を想定したセキュリティインシデントの対応演習（年 1 回）と対応担当者のトレーニングを実施することが求められています。本サービスでは、PCI DSS 準拠を維持または今後新規に準拠する企業向けに、具体的なカード情報流出の演習シナリオを策定します。机上演習の結果、システムや体制面の課題や実際の対応に必要な費用、損害賠償額をシミュレーションすることが可能です。

●サービスの特徴

弊社がクレジットカード情報流出を伴うセキュリティインシデント対応の演習シナリオを策定し、お客様のインシデント対応ポリシーや手順に沿って机上演習と記録作成を行います。演習の記録は PCI DSS の要件 12.10.2、12.10.4 の対応証跡として利用することも可能です。

●提供内容

1. 演習シナリオの作成
   貴社のシステムや体制についてヒアリングした上で、最新の攻撃手段などの事例を取り入れた、貴社業種・業態に応じたセキュリティインシデント対応の演習シナリオを策定いたします。
2. 机上演習の実施
   お客様のインシデント対応ポリシーや手順を使用し、シナリオに沿った机上演習（2～4 時間程度）を実施します。
3. インシデント演習記録の作成
   当日のインシデント演習記録を作成し、後日提出します。

●提供形態

- Web 会議形式もしくは対面による机上演習（2～4 時間）
- インシデント演習記録
  - 時系列のインシデント対応結果
  - カード会社からの損害賠償を含む想定被害額
  - インシデント対応に要する費用

- システムや体制面の課題

●料金

300,000 円～（税別）

●サービス詳細

https://www.fjconsulting.jp/consulting/incident_response_exercise/

【ｆｊコンサルティング株式会社　会社概要】

社名　　：ｆｊコンサルティング株式会社

本社所在地：東京都千代田区神田駿河台 4-3　新お茶の水ビルディング 3F

設立　　：2013 年 4 月

代表者　　：代表取締役 CEO　瀬田　陽介

事業内容　：キャッシュレスセキュリティ分野におけるコンサルティングおよび教育

URL　　：https://www.fjconsulting.jp/

グループ会社：ユナイトアンドグロウ株式会社

【ユナイトアンドグロウ株式会社 会社概要】

社名　　：ユナイトアンドグロウ株式会社（東京証券取引所マザーズ市場　証券コード：4486）

本社所在地：東京都千代田区神田駿河台 4-3　新お茶の水ビルディング 3F

設立　　：2005 年 2 月

代表者　　：代表取締役社長　須田騎一朗

事業内容　：中堅・中小企業の情報システム部門を対象とした会員制支援サービス

URL　　：https://www.ug-inc.net/

【お問い合わせ先】

ｆｊコンサルティング株式会社

広報担当　：板垣　朝子

E-mail　　：info@fjconsulting.jp

※ PCI DSS（Payment Card Industry Data Security Standard）

国際カードブランド 5 社(American Express、Discover、JCB、MasterCard、VISA)が共同で策定したクレジットカードやデビットカードなどのペイメントカードデータ保護のための国際的なセキュリティ基準

＜参考＞PCI DSS におけるインシデント対応計画

PCI DSS 要件 12.10 では、カード情報流出を伴うシステム侵害に対するインシデント対応計画の策定と、定期的なレビュー・テスト及びトレーニングを要求しています。（以下 PCI DSS v3.2.1 より抜粋）

要件 12.10.1

システム侵害が発生した場合に実施されるインシデント対応計画を作成する。

計画では、最低限、以下に対応する。

- ペイメントブランドへの通知を最低限含む、侵害が発生した場合の役割、責任、および伝達と連絡に関する戦略
- 具体的なインシデント対応手順
- ビジネスの復旧および継続手順
- データバックアッププロセス
- 侵害の報告に関する法的要件の分析
- すべての重要なシステムコンポーネントを対象とした対応

要件 12.10.2

少なくとも年に一度、要件 12.10.1 にあげられたすべての要素を含め、計画をレビューおよびテストする。

要件 12.10.4

セキュリティ侵害への対応を担当するスタッフに適切なトレーニングを提供する。