

PCI DSS v4.0 ベストプラクティス要件への効率的対応を実現 WAF/オンラインスキミング対策サービスを提供開始

—PCI DSS 要件 6.4.2、6.4.3、11.6.1 に対し、2025年3月末までにスムーズに対応—

PCI DSS 準拠を促進するクラウドサービス「PCI DSS Ready Cloud」 「BIZTEL コールセンター PCI DSS」 や、店舗向けのサブスクリプション（継続課金）決済端末およびゲートウェイサービス「Smart TG」を展開する株式会社リンク（本社：東京都港区、代表取締役社長：岡田 元治、以下リンク）は、PCI DSS（※）バージョン 4.0 のベストプラクティス対応（※）を支援する WAF/オンラインスキミング対策サービスの提供を開始します。

（※）PCI データセキュリティ基準（PCI DSS）：クレジットカードなどペイメント会員データを安全に取り扱う事を目的として策定された、国際セキュリティ基準。Payment Card Industry Data Security Standard の頭文字をとったもので、国際ブランド5社（American Express・Discover・JCB・MasterCard・VISA）が共同で設立した PCI SSC（Payment Card Industry Security Standards Council）によって策定・管理されています。

（※）ベストプラクティス要件：バージョンアップによって企業に大きな負担がかかるような要件に対しては、特定の期日までの猶予期間を設ける措置。期限までは対応していなくても不適合にならないが、その期日以降は正式な要件になるという考え方。V4.0 のベストプラクティス要件は、2025年3月末までに対応が必要です。

リンクが提供する PCI DSS Ready Cloud 「マネージドモデル」は、60社超の導入実績を有する PCI DSS 準拠促進クラウドサービスです。Amazon Web Services・Microsoft Azure・オンプレミス環境など、幅広くお客さまの PCI DSS インフラ環境への対応が可能で、PCI DSS の維持・運用にかかるコストと工数を削減するさまざまなサービスをパッケージ化しています。

今回の追加オプションは、ユーザからの要望や問い合わせの多かった PCI DSS バージョン 4.0 ベストプラクティスへの対応を支援します。概要は以下の通りです。

■WAF/オンラインスキミング対策

1. サービス概要

WAF（Web Application Firewall）やオンラインスキミングへの対策を、低コストかつ運用負荷を軽減可能なサービスとしてパッケージ化しました。

WAF	オンラインスキミング対策
<ul style="list-style-type: none"> ・マネージドルールによるサービス提供 ・オンプレミス/AWS いずれの環境にも提供可 ・HTTP ヘッダーの不正な変更を防御・検知可能 ※要件 6.4.2 と 11.6.1 に対応 	<ul style="list-style-type: none"> ・決済ページなど入力フォームの監視 ・入力フォームに紐づくスクリプトの監視 ・スクリプトに紐づくデータ送信先サイトの監視 ※要件 6.4.3 と要件 11.6.1 に対応

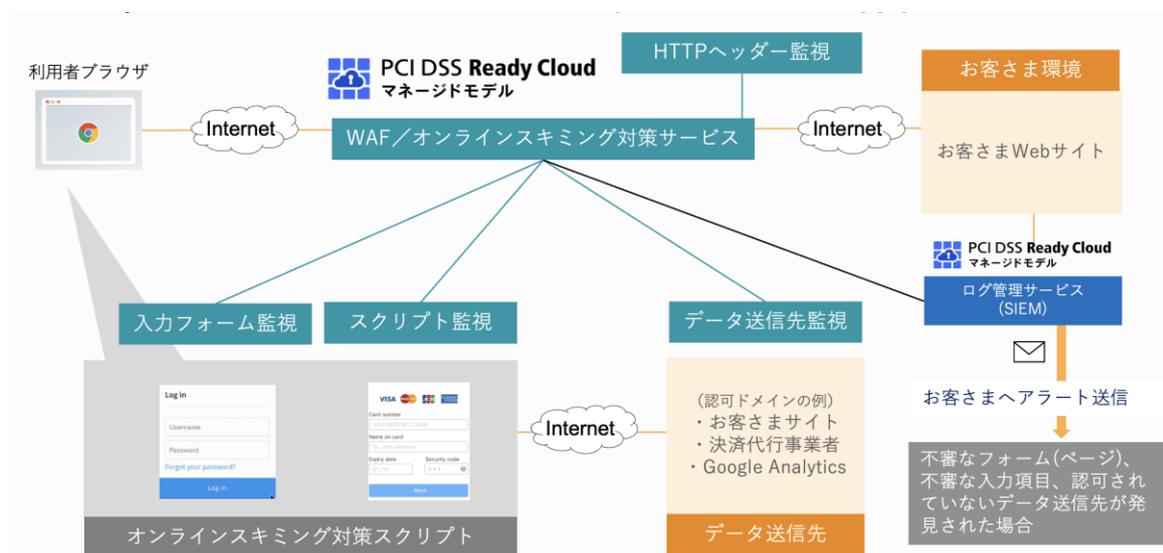
2.本サービスに対応するベストプラクティス要件

本サービスは、難易度が高い要件 6.4.2、6.4.3、11.6.1 に対応するサービスです。なお、PCI DSS バージョン 4.0 のベストプラクティス要件は 2025 年 3 月 31 日までに対応する必要があります。

番号	要件概要
6.4.2	<p>一般公開されているウェブ アプリケーション については、ウェブベースの攻撃を継続的に検知・防止する自動化された技術的ソリューションを 導入しており、少なくとも以下の条件を備えている。</p> <ul style="list-style-type: none"> ・一般公開されているウェブアプリケーションの 前にインストールされ、ウェブベースの攻撃を検知・防止するように設定されている。アクティブに実行され、該当する場合は最新の状態に更新されていること。 監査ログを生成していること。ウェブベースの攻撃をブロックするか、アラートを生成して直ちに調査するように設定されている。
6.4.3	<ul style="list-style-type: none"> ・消費者のブラウザに読み込まれ実行されるすべての決済ページスクリプトは、以下のように管理される。 ・各スクリプトが認可されていることを確認するための方法が実装されている。各スクリプトの整合性を保証するための方法が実装されている。すべてのスクリプトのインベントリが、それぞれのスクリプトが必要な理由を説明した文書とともに維持される。
11.6.1	<p>変更・改ざん検知のメカニズムは、以下のように展開されている。</p> <ul style="list-style-type: none"> ・消費者ブラウザが受信した HTTP ヘッダーと決済ページのコンテンツに対する不正な変更（侵害の指標、変更、追加、および削除を含む）を担当者に警告すること。メカニズムは、受信した HTTP ヘッダーと決済ページを評価するように構成される。（一部抜粋）

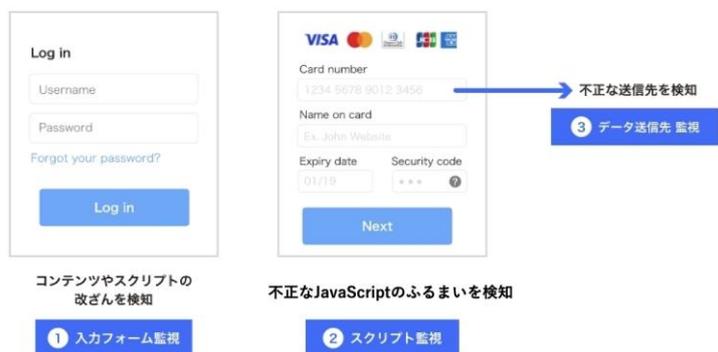
3.WAF/オンラインスキミング対策サービス 提供イメージ

PCI DSS Ready Cloud 「マネージドモデル」との組み合わせによって、要件 6.4.2、6.4.3、11.6.1 に対応し、HTTP ヘッダーの不正な変更、コンテンツやスクリプトの改ざん、不正な JavaScript のふるまいなどを検知し、アラートを送信します。



3.1 オンラインスキミング対策サービス : 3つの機能

サイトに潜む悪意のあるコードを検出&アラート送信します。



今後も PCI DSS Ready Cloud は、ユーザの要望をもとにしたさまざまなサービスの追加によって、PCI DSS 準拠・運用に関する課題解決・効率化を支援してまいります。

株式会社リンクについて

株式会社リンクは、業界最大級の稼働台数を持つ専用ホスティング「at+link」、クラウド型ホスティング「リンク・ベアメタルクラウド」を軸として、6年連続シェア第1位のクラウド型コールセンターシステム「BIZTEL」、セキュリティプラットフォームサービス「PCI DSS Ready Cloud」など、さまざまなサブスクリプション型サービスを提供しています。農系事業にも取り組んでおり、2011年10月からは岩手県岩泉町にある自然放牧酪農場「なかほら牧場」を運営しています。事業の詳細は、<https://www.link.co.jp/> をご覧ください。

★リンクが運営するメディアサイト「最適なサービスで一步先行く組織へ」ビジネスに伴走する課題解決メディア『LINK Watch!』 <https://watch.link.co.jp/>