2025年8月25日

加盟店各位

ヤマト運輸株式会社

クロネコwebコレクト(リンク方式／メール方式)・クロネコ クレカ払い PCI DSS4.0要件準拠および不正アクセス対策実施のご案内

平素は格別のご高配を賜り、厚く御礼申し上げます。
表記の件、クロネコwebコレクト(リンク方式／メール方式)、クロネコ クレカ払いのご利用につきまして、クレジットカード会員情報の保護を目的とした国際統一基準であるPCI DSS4.0要件準拠および不正アクセス対策実施のため、9月16日より下記の変更をいたしますのでご案内いたします。

記

1. 対象の決済方式と画面

＜クロネコwebコレクト＞
・リンク方式／メール方式
・クレジットカード決済画面(PC画面／スマホ画面)
・継続課金のクレジットカード決済画面(PC画面／スマホ画面)
＜クロネコ クレカ払い＞
・カード登録・更新・削除画面(PC画面／スマホ画面)

※トークン発行(組込型・モーダルウィンドウ型)はWebページではないため対象外
※クロネコwebコレクト加盟店テスト環境も対象外

2. 変更点

PCI DSSバージョン4.0で求められている別紙の要件に準拠すべく、当社ではCSP機能(Client-Side Protection)を用いて対応します。

Client-Side Protectionは、購入者様ブラウザ側のJavaScriptを可視化、監視(改ざん検知含む)、制御するツールです。「ホスト名」と「ドメイン名」で構成されるFQDN単位で適用されます。本機能適用後に改ざんが検知された場合、クレジットカード決済画面においてJavaScriptがブロックされてページが正常に動作(次ページへの遷移など)しなくなります。

■対象のFQDN
・payment.kuronekoyamato.co.jp
・idpayment.kuronekoyamato.co.jp

3. リリース予定日時(24時間表記)

2025年9月16日(火)10:30頃、上記ツールを適用モード※に変更します。
システム中断等は発生いたしません。

※適用モードとは、監視モードで作成したルールに基づき、許可していない通信やスクリプトを「実際にブロック」する防御モードです。
Webサイトの応答に強制力のある指示書(Content-Security-Policyヘッダ)を付けて送る仕様となります。
この指示書には、管理者が事前に「安全である」と許可したドメインやスクリプトの「許可リスト(ホワイトリスト)」が記載されています。
ブラウザは、このリストに載っていないスクリプトなどの読み込みや実行をすべてブロックします。

4. 本件に関する問い合わせ先

ヤマト運輸株式会社
決済サービス カスタマーサービスセンター
フリーダイヤル:0120-69-5090 (受付時間:9:00 - 18:00)
E-mail:payment@kuronekoyamato.co.jp

以上

別紙1：PCI DSS　バージョン3.2から4.0の変更について

要件	求められている内容	対応状況
6.4.3	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。	9/16より対応
8.3.6	ユーザアカウントのパスワードは最低限、以下の要件を満たす必要がある。 ・12文字以上であること。 ・数字と英字の両方を含む。	2024年11月11日 対応済み
11.6.1	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。 ・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。 ・メカニズムの機能は、以下のように実行される。 　少なくとも7日に1回または-定期的に（要件12.3.1に規定されたすべての要素に従って実施される事業体のターゲットリスク分析で定義された頻度で）	9/16より対応