クリプト便

ファイル転送/共有ガイドブック

PCI DSSに準拠した カード情報の 受け渡し方法とは？

クラウドサービスで
FAX/メディア郵送から
脱却！

NRI SECURE

ファイル転送 / 共有ガイドブック

PCI DSS に準拠した カード情報の受け渡し方法とは?

目　次

クリプト便

はじめに

クレジットカード情報を取り扱う事業者は、カード情報の漏えいや不正利用を防ぐため、国際的なセキュリティ基準「**PCI DSS**（Payment Card Industry Data Security Standard）」で求められる要件を満たす必要があります。しかし、多くの事業者は急速に進展するデジタル化の波に乗れずにITシステムでの対応を見送り、依然としてFAXやメディア郵送といったレガシー手法を余儀なくされている現状が見受けられます。

この現状を受けて、NRIセキュアテクノロジーズでは、自社で提供しているファイル交換サービス「**クリプト便**」をカード情報の安全な受け渡しに使っていただこうと考え、2021年4月、「クリプト便」がPCI DSSに準拠したことを示す認証を取得しました。これにより、これまでFAXやメディア郵送などの手法で社外とやり取りしていたクレジットカード番号を含む重要情報も、クリプト便で安心して取り扱えるようになります。

本ガイドブックは、PCI DSS準拠が求められる業務を実施する中でカード会員データの授受に課題を抱えている方を対象として、より安全かつ効率的なカード情報の授受をご紹介するものです。

日々の運用負荷を軽減しつつ、求められるセキュリティレベルを維持していくために、本ガイドブックをお役立てください。

1

カード情報の授受に伴う課題

今、クレジットカード業界全体でPCI DSS対応が求められています。事業者はPCI DSSが定める細かな要件に対応するためにシステムを自社開発するという選択肢もありますが、システム開発費だけでなく、その後のPCI DSSのアップデートに対応していく必要があり、そのための負荷やコストについても考慮しておかないといけません。それならば、いっそのことPCI DSSの要件に対応したクラウドサービスを利用してカード情報の授受を行えば、PCI DSS対応の負荷は軽減します。

ただし、クラウドサービスを利用する場合は、自社のコントロール範囲を大きく超えてしまうため、その選定は慎重に行う必要があります。例えば、技術者不足やコストカットを理由として、業務の一部を海外へ委託する動きが加速していますが、海外に開発・運用を委託したことで、個人情報が守られない状況を生み出してしまったケースもあります。こうなると、企業の管理体制を問われることにもなりかねません。したがって、単に機能だけで判断するのではなく、クラウドサービスのセキュリティが保たれているかどうかという観点から検討を進めることも重要です。

本章では、カード情報の受け渡しに依然としてレガシー手法が使われ続けている理由に着目すると共に、デジタル化を進める上でのクラウドサービスの選び方、外部に委託する際の注意点について解説します。

1-1. 事業者を悩ますPCI DSS準拠

2018年、安全かつ効率的なカード情報の受け渡しを実現するために、改正割賦販売法により、事業者は「PCI DSS準拠」か「クレジットカード情報の非保持化」のいずれかに対応することが義務付けられました。さらに2021年4月から施行された改正割賦販売法で義務対象事業者が拡大され、これまで非保持化で対応してきた決済代行業者においても、非対面取引についてはPCI DSS準拠相当の対応が求められるようになりました。

PCI DSSに準拠すれば、単に不正アクセスから大事な情報資産を保護するだけでなく、企業やブランドの信頼、企業価値が高まるメリットがありますが、その運用は決して簡単ではありません。PCI DSSは一度認証を取得したら終わりではなく、準拠レベルを維持するために毎年監査を行うことが定められているからです。年1回の監査に加え、四半期に1回の診断と対応、日々の脆弱性情報収集やパッチ適用など、日々の業務をこなしながらの運用は非常に負荷が高く、多くの事業者が年中PCI DSS対応に追われているのが実態です。

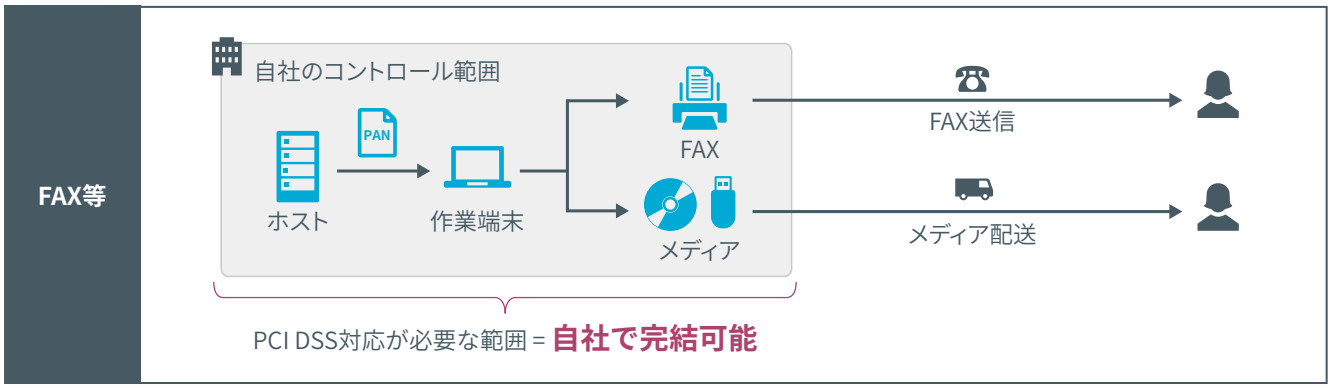
さらに、セキュリティを取り巻く環境は変化し続けているため、認証を取得した後も、常に最新バージョンに追随する必要があります。また、事業が拡大する中で、既存システムはもちろん、追加・更新するシステムについても、同様の対応が求められます。運用が適切に継続されていなかったために、サイバー攻撃による情報漏えいにつながったケースがあるように、**重要なのは、PCI DSS準拠に則したセキュリティ基準を維持し続けること**なのです。

カード情報の受け渡しにデジタル手法を利用する場合、上記の運用負荷の課題が出てきます。しかし、自社開発ではなくクラウドサービスを利用するのであればセキュリティ基準の維持は提供会社が対応することが一般的のため、運用負荷の軽減が期待できます。それにもかかわらず、依然としてレガシー手法での対応が続いているのはなぜでしょうか？ 次項では、クラウドサービスの利用に二の足を踏む理由に着目します。

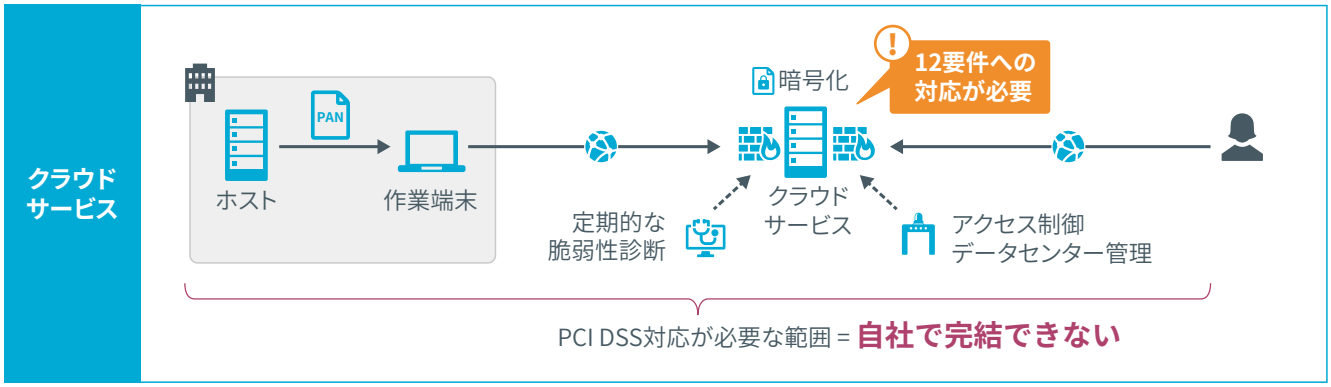
1-2. クラウドサービス利用時の課題

レガシー手法から抜け出せない理由がどこにあるのか、もう少し詳しく探ってみましょう。

例えば、FAXやメディア郵送によりカード情報の受け渡しをする場合を見てみると、PCI DSS対応が必要な業務は自社でコントロールできる範囲で完結しています。つまり、自社で責任を持って受け渡しが行える環境にあります。



では、カード情報の受け渡しにクラウドサービスを利用する場合はどうでしょうか。



この場合は、クラウドサービスに保存されたデータがカード情報であれば適切な取り扱い（保存、伝送方法など）をする必要がありますが、クラウドサービス事業者は保存されたデータ内の情報について通常は関知しません。つまり**利用者側で、暗号化や、定期的な脆弱性診断、アクセス制御、データセンター管理など、PCI DSSが定める12の要件への対応できているかを確認する必要があります。**法律上でも、利用者がクラウドサービス事業者による情報（データ）の取り扱いにも責任を持つことが求められるため、サービスの仕様を把握し、その修正や変更についても追い続けていく必要があるわけです。このようにPCI DSS対応が必要な業務が自社のコントロール範囲を大きく超えてしまう状況はあまりにもリスクが大きく、クラウドサービス利用に二の足を踏んでしまうのも当然でしょう。

1-3. サービス選定のポイント

多くの事業者がレガシー手法から抜け出せない理由を踏まえると、カード情報の受け渡しにクラウドサービスを利用する際は、**PCI DSS に準拠しているサービスかどうか**が重要なポイントになることがわかります。実際、クラウドサービスの中には PCI DSS に準拠しているサービスがあり、そうしたサービスを提供する事業者は、取り扱っている情報がカード情報であるという前提で安全に取り扱えることを保証し、認証を受けています。

このように PCI DSS 準拠の認証を受けているサービスであるという事実を確認することによって、自社のコントール範囲外の部分に対しても PCI DSS に準拠していることを示す根拠とすることができます。最新の PCI DSS への対応はクラウドサービス事業者が責任を持って行うことになるため、PCI DSS 準拠に伴う数多くの監督業務を省略できるメリットがあります。また、実際にクラウドサービスを活用したデータ送付方法が PCI DSS に準拠しているかどうかは QSA（認定セキュリティ評価機関）が判断することになりますが、やり取りを円滑にするためにクラウドサービスが PCI DSS に準拠している証明となる AOC（準拠証明書）を提出することも有効です。

補足として、セキュリティガイドライン 2.0（公表版）では、「その他の留意事項」において、カード情報の取り扱い業務を外部委託する場合の留意点と受託者における必要な対策について次のように言及しています。

カード情報の取扱い業務を外部委託する場合の留意点と受託者における必要な対策

セキュリティ対策の実施主体者である関係事業者（加盟店、カード会社、決済代行業者等、コード決済事業者等）は、カード情報を取り扱う業務を外部委託する場合は、委託者自身が委託先のセキュリティ状況を確認し、責任を持って PCI DSS 準拠等の必要な対策を求める。

特に、複数の委託者からカード情報を取り扱う業務を受託する事業者においては、カード情報が漏えいした場合の影響が大きいため、また、ショッピングカート機能のシステムを提供する事業者においては、ショッピングカート部分の脆弱性からフィッシング等によりカード情報が漏えいする事案が発生していることから自社システムにおけるカード情報の保持状況について確認の上、**PCI DSS 準拠等**の必要なカード情報保護対策等を行う。

* 文字の装飾は本書にて付記

この文面からわかるように、クラウドサービスなどを提供するサービスプロバイダーに対しては、PCI DSS 準拠“等”の対策が必要としており、必ずしも PCI DSS 準拠に限定しているわけではありません。しかし、サービスを利用する際に、当該サービスが PCIDSS 準拠を謳っていない場合、「PCIDSS 準拠相当」の対策を講じていることを利用企業が監査やヒアリングを通して確認する必要があります。これには情報セキュリティ対策について理解度の高い人材が相当時間をかけて確認することが必要となるため、大きな負荷といえるでしょう。そのため、クラウドサービスを利用する際は、「PCI DSS 認証を取得しているサービス」を選定することが望ましいと言えます。

カード情報の授受に利用できるクラウドサービスで PCI DSS 認証を取得している仮想サーバやファイル共有サービスは複数ありますが、多くは国内サービスではなく、海外製のサービスです。

これらのサービスに共通するのは、開発および運用、データの保管が海外で行われていることです。もちろん、データの保管場所として国内を指定できる場合もありますが、PCI DSS 準拠そのものに直接関係はないものの、「**海外で開発および運用をしている**」という点に注意する必要があります。

特に昨今は、技術者不足やコストカットを理由として業務の一部を海外へ委託する動きが加速しつつあります。大手企業が提供するサービスの個人情報管理において、システム開発を委託されていた中国企業の従業員から日本国内のサーバにアクセスがあったことが判明したニュースは記憶に新しいでしょう。クレジットカードの場合も、他の個人情報と容易に照合できる情報を扱うことを念頭に置き、海外への委託に際しては、委託先管理や PCI DSS 準拠の観点から細心の注意が必要になりそうです。

PCI DSS 認証取得済み企業の一覧はある？

PCI DSS 認証取得済み企業のリストは、現在のところ、マスターカードと VISA カードがサービスプロバイダーに限定して公表している英語版リスト以外にはありません。公表することで、準拠していない企業がハッカーの標的になる危険性があるだけでなく、規制をかけようとする動きへの抗議活動として、アノニマスが PCI DSS 準拠済みセキュリティに対してサイバー攻撃をしかける可能性もあり、公表は得策でないという意見があります。これと同じ理由で、PCI SSC が定める PCI DSS 認定マークもありません。

2

「クリプト便」活用のススメ

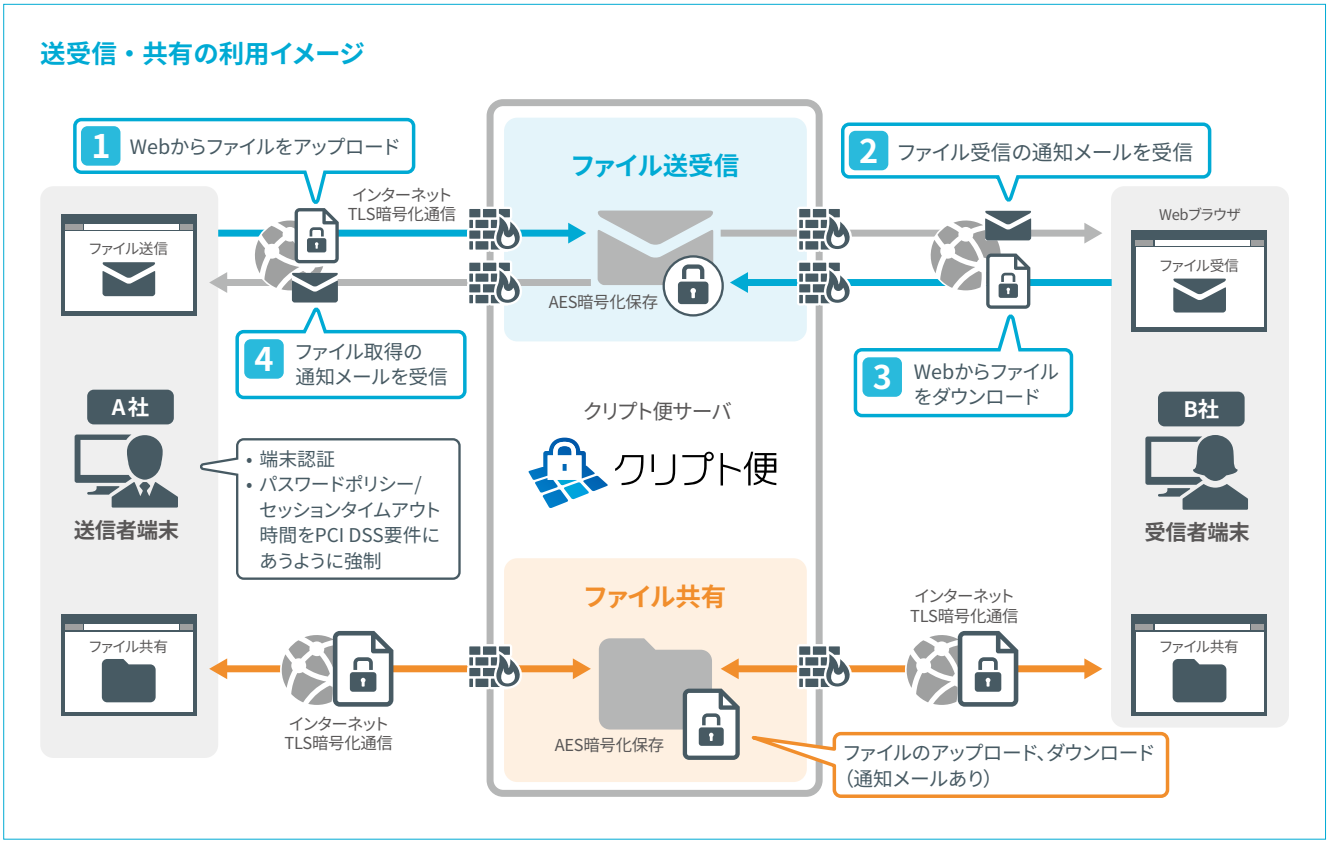
昨今、さまざまな業種でデジタル化の進展と共に業務効率化が求められる中で、カード情報の受け渡しにおいては、FAXの送信、DVDやUSBメモリなどのメディア郵送といったレガシー手法からの脱却が進まない現状があります。

NRIセキュアテクノロジーズは、PCI DSSの要件を満たした環境でカード情報やカード会員データの伝送・保存が行える「**クリプト便**」の提供を通じて、レガシー手法における問題点を解決し、「カード情報の受け渡しを安全かつ効率的に行いたい」という事業者のニーズにお応えします。何より、「開発・運用、データの保管が国内で行われている」ことも大きな強みです。

本章では、レガシー手法における問題点を整理すると共に、解決策としての強力な選択肢となるクリプト便の活用パターン、メリットをお伝えしていきます。

2-1. PCI DSS 認証を取得した「クリプト便」とは

「クリプト便」は、インターネットを介して電子ファイルの転送・共有をするSaaS型クラウドサービスです。堅牢なセキュリティ対策を施したクリプト便サーバを経由してファイル受け渡しを行うため、カード情報などの機密情報を安全かつ確実に受け渡しすることが可能です。Webブラウザを利用するため、新たにシステムを構築する必要がなく、短期間で導入できるのも特徴です。また、**システムの開発・運用、データの保存はすべて日本国内で実施**されています。



このクリプト便が、2021年4月、**PCI DSSに準拠したことを示す認証を取得**しました。PCI DSSの認証を受けたことで、これまで電子記録媒体の郵送やFAXなどで社外とやり取りしていたカード番号やカード会員名、有効期限、サービスコードなどを含む重要情報も、クリプト便で安全に取り扱えるようになっています。実際、多くの企業で「PCI DSS認証取得を実現した数少ない国産サービス」であることが高く評価され、導入の決め手となっています。

参考情報：導入事例 / 情報セキュリティのNRIセキュア | クリプト便（nri-secure.co.jp）

PCI DSS に準拠した環境でクリプト便を利用するための機能例

1. 端末認証
クリプト便にアクセスできる端末を証明書導入済みの端末に制限。証明書とクリプト便 ID による二要素認証が実装可能。

2. 管理者操作ログ取得
管理者が画面で操作した内容をログとして記録。管理者による不適切な利用を、監査・けん制することが可能。

3. セキュリティ強化オプション（PCI DSS）
クリプト便のユーザアカウントに対して、PCI DSS の各要件を満たす処置（アカウントロック、セッションタイムアウト時間、パスワードポリシー）を強制。

2-2. レガシー手法の置き換え例

業界全体でPCI DSS準拠が求められるなか、PCI DSSに準拠していないシステムを利用しにくいことから、多くの事業者が依然としてレガシー手法で業務を続け、クラウド活用に手を伸ばすことができずにいます。そこで、レガシー手法における問題点を確認すると共に、クリプト便による解決策をご紹介していきましょう。

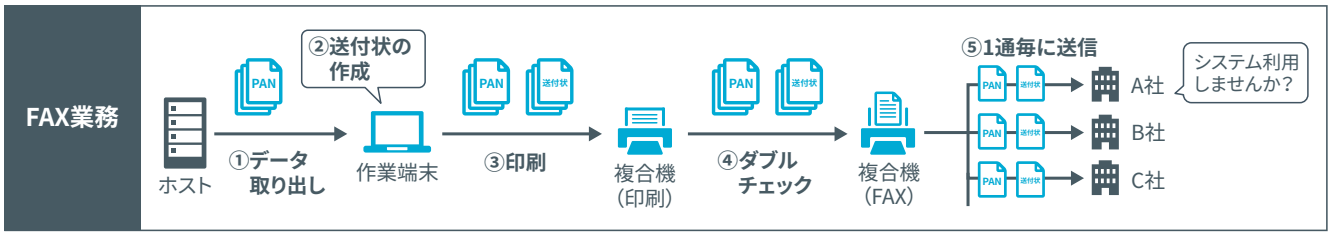
ケース① FAX利用のケース

[業務]

- 特定のカード会社間におけるカード会員データや個人情報の受け渡しをFAXで行う
- 数十名のメンバーが「リトリーバル」「チャージバック」「属性照会」などの情報の受け渡しを毎日複数回行う
- カード会員データを扱えるのは社内の高セキュリティエリアのみで、エリア内ではインターネットは基本的に遮断している

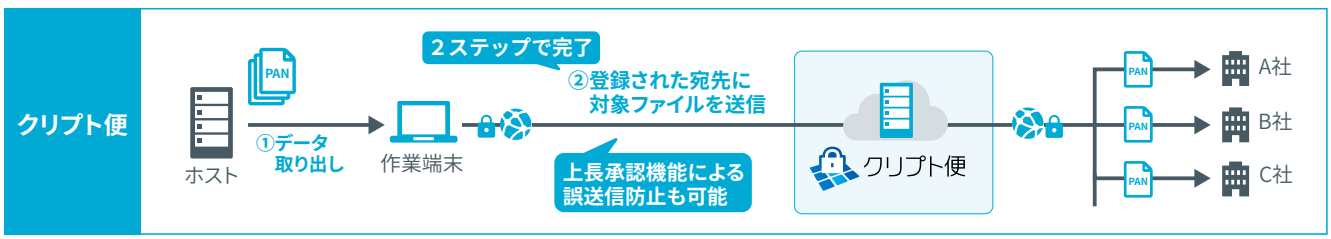
[課題]

- 紙ベースのためデータ入力作業が必要でFAX送受信にかかる作業負荷が大きい
- あるカード会社から、データの受け渡しにクラウドサービスの利用を提案されているが、PCI DSSに準拠していないサービスの利用は認可できない



[解決策]

- クリプト便の利用により電子ファイルを直接送付することでデータ入力やFAX送受信の手間が不要に
- QSA（認定セキュリティ評価機関）に対しては、クリプト便のAOC（準拠証明書）の提出によりPCI DSS準拠を証明



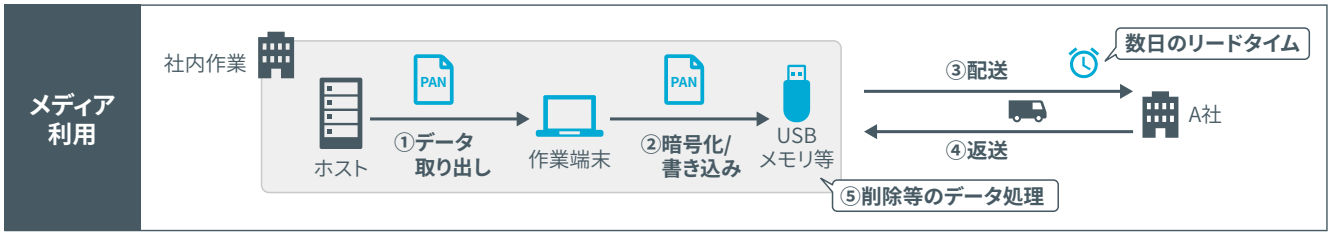
ケース② メディア利用のケース

[業務]

- 決済代行サービスで取り扱っているテキストベースのカード会員データや個人情報をUSBメモリに格納して郵送（カード情報を含むためPCI DSS準拠が必要）
- 受け渡しの方向は、「自社から他社へ送る」、「他社から自社が受け取る」、「社内で受け渡しを行う」の3パターンとなる
- 月1回程度のペースで受け渡しを行う

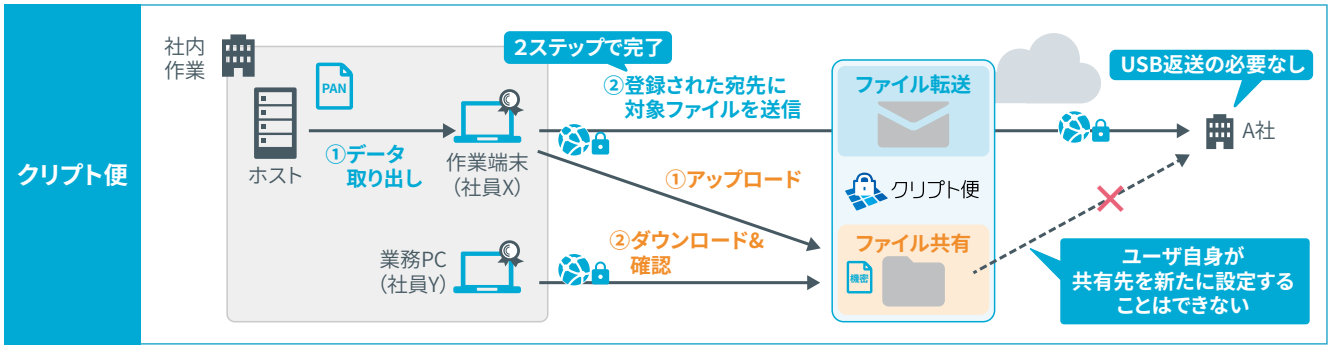
[課題]

- メディアの郵送に伴う作業負荷が大きく、相手に届くまでのリードタイムがある
- メディアの紛失リスクを伴う
- 社内におけるファイルの受け渡しが非効率である
- メディアを廃止しても、代替手段がPCI DSSに準拠していることをQSAに証明する必要がある



[解決策]

- クリプト便から送付することで、郵送作業が不要となり、届くまでのリードタイムも大幅に短縮
- 物理媒体（USBメモリ）の紛失リスクを回避
- 機密データの社内共有にもクリプト便のファイル共有機能が利用でき、効率化を実現
- QSA（認定セキュリティ評価機関）に対しては、クリプト便のAOC（準拠証明書）の提出によりPCI DSS準拠を証明



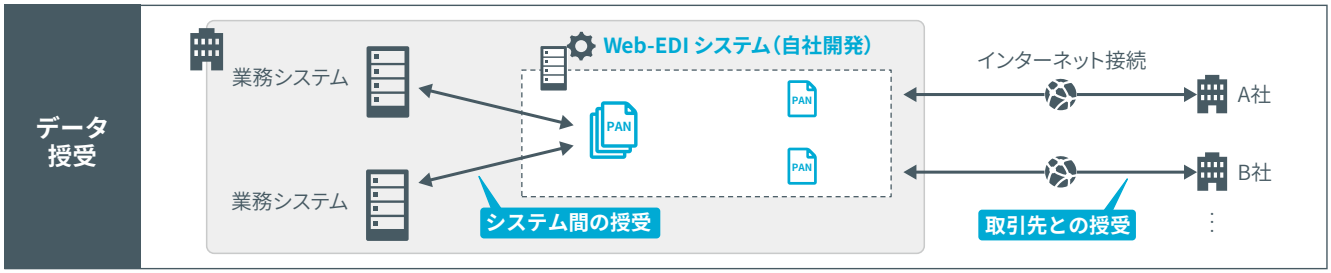
ケース③ システム間でのデータ授受

[業務]

- オンプレミスの自社開発システムで取引先とカード会員データを含むファイルを授受
- ユーザ数は数千規模、データの受け渡し件数は月数万件

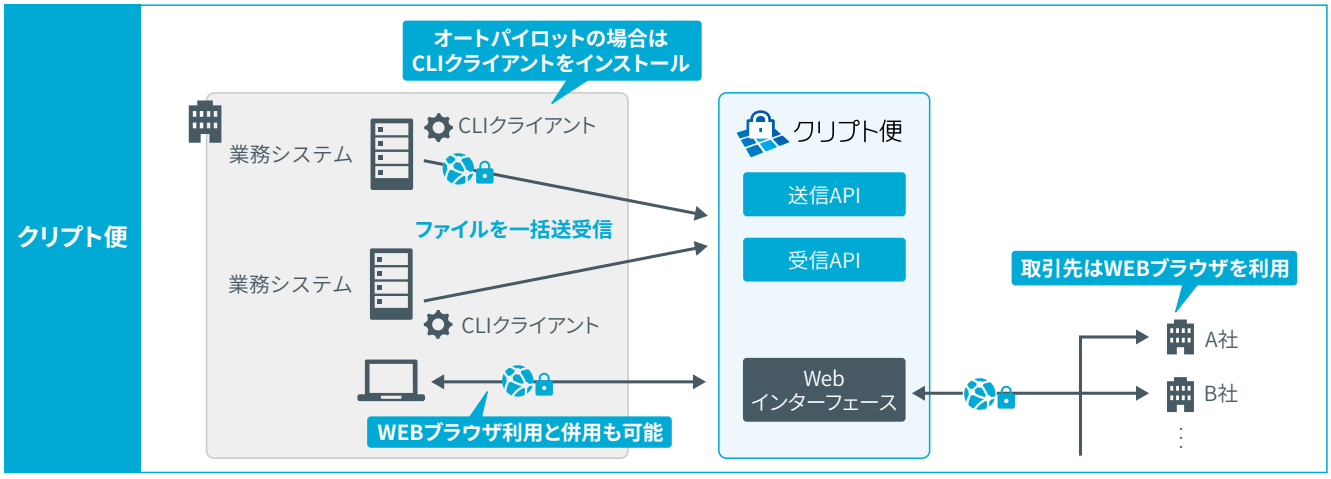
[課題]

- 自社開発システムの老朽化に伴いリプレイスが求められている
- リプレイスにあたり開発・運用コストを最小化したい
- クラウドサービスを利用したいが、PCI DSS に準拠していることを QSA に証明する必要がある



[解決策]

- 送受信 API を使った自動送受信環境を構築できるクリプト便のオートパイロットオプションもしくは API を活用することでリプレイスを実現
- オートパイロットオプションにより開発工数を削減可能もしくは API により個々の要件に柔軟に対応可能
- QSA（認定セキュリティ評価機関）に対しては、クリプト便の AOC（準拠証明書）の提出により PCI DSS 準拠を証明



2-3. クリプト便活用のメリット

クリプト便は、高いセキュリティが求められるビジネスの現場で長年選ばれてきました。ファイル転送市場でシェアNo.1であるだけでなく、顧客の50%以上が、セキュリティを重んじる金融関連企業である点がクリプト便の信頼を物語っています。また、クリプト便の運用拠点やデータセンターは国内にあるため、昨今懸念事項として話題に挙がっている海外に**データを預けた際のリスクを回避できる**ほか、実査など国内企業の細やかな要件にも柔軟に対応できます。

さらにNRIセキュアテクノロジーズでは、単に機能を提供するだけではなく、**PCI DSSに関する各種コンサルティングも提供**しています。また、PCI SSCによるQSA（認定セキュリティ評価機関）の資格を有し、専門審査員による訪問審査も承っています。情報セキュリティに関わる多くの実績・ノウハウや、QSAとしての立場を活かし、PCI DSSが求める12要件を満たすための効果的な対策の実施から訪問審査までワンストップで支援します。

クリプト便のようなクラウドサービスを利用する際は、自社のセキュリティ基準への準拠という観点で厳しい審査が必要となる企業も多く、仕様の調査やチェックシート記入などの審査対応が導入のハードルとなるケースもあるでしょう。NRIセキュアテクノロジーズが提供するクリプト便なら、お客様からの審査・監査にも丁寧に対応するほか、QSAによる審査の際にPCI DSS準拠の証となるAOC（準拠証明書）の提出が可能です。

クリプト便の強み

1. 金融業界で広く使われている実績があり、セキュティの高さを証明している。
2. 国産サービスのため、日本語でのサポートはもちろん、監査対応をはじめとした国内企業のさまざまな事情に配慮し柔軟に対応できる。
3. NRIセキュアはQSA審査機関としての立場を活かし、PCI DSSに関するさまざまな相談に対応可能であるだけでなく、事業者とQSAとの間に立って課題の解決を支援できる。

まとめ

カード情報の受け渡しは、依然としてFAXやメディア郵送といったレガシー手法で行われていることが多く、効率化が思うように進んでいません。多くの事業者が運用負荷の軽減を課題として認識し、効率化の手段を検討されていることでしょう。

こうしたレガシー手法に代わるクラウドサービスを選定する際は、PCI DSSの最新動向に追随しているサービスを選定することに加え、委託先管理や準拠法の観点から開発・運用、データの保存が国内で行われていることを重視すべきです。何を選ぶかによって、導入後、PCI DSS準拠のセキュリティ基準を効率的に維持していけるかどうかが大きく左右されます。選択を誤れば、守るべき情報がリスクにさらされることになります。

レガシー手法に代わるクラウドサービスの有力候補となる「クリプト便」は、PCI DSS認証を取得した国産サービスです。提供元であるNRIセキュアテクノロジーズは、情報セキュリティの専門会社であり、クリプト便のサービス提供だけでなく、PCI DSS準拠に向けたコンサルティングから実際に準拠しているかどうかの審査に至るまでワンストップでの支援が可能です。また、時には事業者とQSAとの間に立ち、PCI DSS準拠への課題解決に尽力します。クリプト便とPCI DSS準拠支援を通じて、お客様のカード情報を守りつつ業務の効率化を実現します。

「安全かつ効率的にクレジットカード情報の受け渡しをしたい」

NRIセキュアテクノロジーズなら、お客様のニーズにお応えできます。まずはお気軽にご相談ください。

クリプト便 PCI DSS　検索

NRI SECURE

ファイル転送 / 共有ガイドブック

PCI DSSに準拠した
カード情報の受け渡し方法とは？

NRIセキュアテクノロジーズ株式会社

〒100-0004 東京都千代田区大手町1-7-2 東京サンケイビル
www.nri-secure.co.jp