FORTRA™

ホワイトペーパー

PCI DSS 4.0のコンプライアンス要件

土壇場でのパニックを回避するためのヒント

コンプライアンスを遵守し続けることは、その適用範囲および実際の適用方法という両側面において難しい任務です。組織は膨大な数の規制に準拠することを強いられており、その数は着実に増えています。コンプライアンスは常に厳格化されており、新しいPCIデータセキュリティ基準（PCI DSS）4.0の実装期限が2024年と迫るなか、企業や金融機関は、その要件について学び、対応する必要性に迫られています。

新しい基準や改変された基準に準拠することは、ときに「言うは易く行うは難し」となります。現実には、企業はサイバーセキュリティへの対応に日々追われており、コンプライアンスへの対応は、切迫した状態に陥るまで後回しにされる傾向にあります。このような傾向は特に、堅牢なセキュリティとコンプライアンス準拠を達成するために、より多くのリソース、時間、人材、そして包括的戦略を必要としている企業において顕著です。

人材のスキルギャップと人手不足は、あらゆるセクターにおいて現実の懸念事項となっています。その結果、時間と人材が不足し、企業は長期的なプロジェクトよりも、喫緊の課題に注目することとなります。このような状況では、コンプライアンスの対応期限間際にパニックが生じることがよくあります。

それでも、小売業者や金融機関は、日々のセキュリティオペレーションや要件に対応しながら、PCI DSS 4.0に向けたコンプライアンス体制を構築することができるのです。2つのタスクを1つのアクションで解決する「Touch it once」戦略を採用することにより、日常的な優先課題を満たしながら、PCI DSS 4.0に効率的に移行することが可能になります。

それはつまり、「後で見直す必要がないように物事を行う」ことを意味します。新しいビジネスプロセスを作成する際には、「これにより、どのようにセキュリティが強化され、PCI DSS 4.0基準をより遵守できるようになるか」ということを必ず意識して取り組まなければなりません。

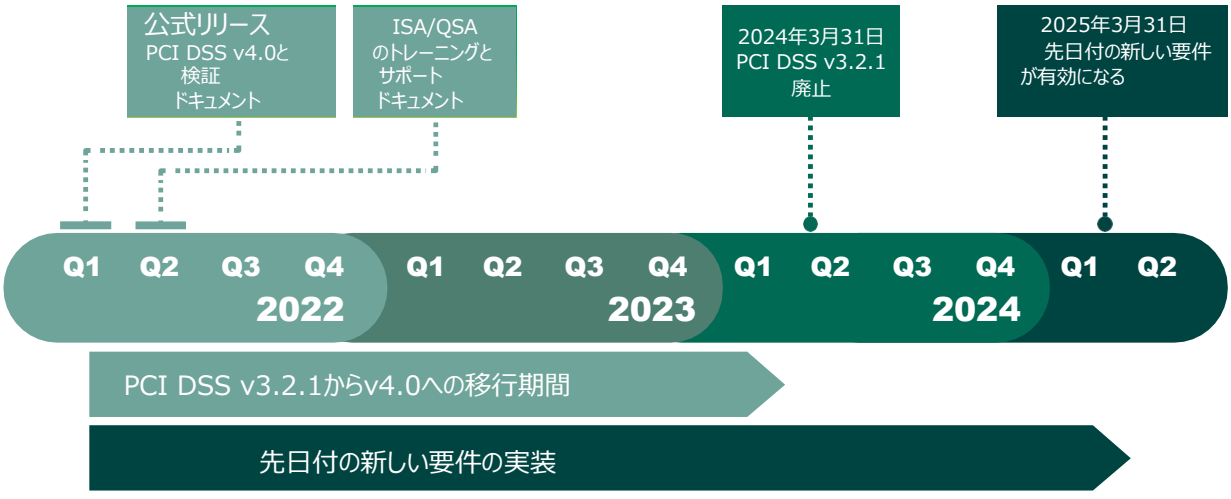
このガイドは、PCI DSS 4.0への準拠に関連する課題を理解していただくことに加え、日常的なサイバーリスクや脅威から企業を保護しながら、準拠を実現するためのロードマップを優先順位を設けて提供することを目的としています。

PCI DSS 4.0：その変更点とは？

PCI DSSは、ペイメントカードのデータを処理、保管、送受信する事業者が、カード会員データの盗難を阻止できるようにする目的のもと、2006年に策定されました。ペイメントカードアカウントのデータに特化して設計されたPCI DSSですが、ペイメントエコシステム内のその他の要素に対する脅威からも保護することができます。

PCI DSS 4.0の適用にあたり、PCI DSSバージョン 3.2.1の廃止までには重複期間が設けられており、バージョン間の移行を円滑に行えるようにしています。この重複期間に、組織は新しいバージョンに慣れ、必要な変更を計画および実装することができます。PCIセキュリティ基準審議会（SSC）提供の以下の図は、PCI DSS 4.0の実装スケジュールの概要を示しています。

PCI DSS v4.0実装タイムライン



PCI DSS v3.2.1は、v4.0 が公開されてから2年間有効です。これにより、組織は新しいバージョンに慣れ、必要な変更を計画して実装するための時間を得ることができます。

バージョン4.0での変更は、主に次の4つの目的で行われています。

- 基準がデジタル決済業界のセキュリティニーズに対応できるようにすること
- セキュリティを継続的な動的プロセスとして促進すること
- 検証手順をより強固なものにすること
- セキュリティ目標を達成するための追加の手段をサポートすること

さらに、新バージョンでは、「カスタマイズされたアプローチ」という概念も導入されています。これは、「すべてのセキュリティアプローチが同じである必要はなく、1つのセキュリティ上の目的を達成するためには、数多くの方法があってよい」という考え方です。バージョン4.0では、このアプローチに対応すべく、要件とテスト手順をカスタマイズできるようになります。

多くの企業が、要件のセキュリティ目標を満たすセキュリティソリューションを採用しています。カスタマイズアプローチにより、企業は採用しているソリューションが、どのようにセキュリティ上の目的を満たし、リスクに対処しているかを示し、要件を満たすための代替方法を提示することができます。

ペイメントカードデータの保護における重要な基盤である「PCI DSSの12の中核的な要件」については、PCI DSS v4.0での変更は基本的にありません。ただし、現在の要件は、セキュリティコントロールの実施に焦点を当てた成果に基づく文言として記述されています。多くの要件においては、単に「実施すべきこと」の記述を「結果として得られるセキュリティ上の成果」という文言に入れ替えるだけで達成できます。

最も広範囲に及ぶ変更は、認証とデータの暗号化に関するものです。決済業界が徐々にクラウドへと移行する中、PCI DSSは、決済およびコントロールプロセスへのアクセスの際のログインに対し、より強固な認証基準を適用することに注力しています。新しい要件には、カード会員データ環境にアクセスする管理者のみならず、「カード会員データへのすべてのアクセスに多要素認証を適用すること」が追加されました。PCI DSS 4.0ではさらに、カード会員データの暗号化の対象に信頼できるネットワークが追加され、より広い範囲への適用が求められます。すべての変更点のリストは、『変更点のまとめ』ガイドにて参照することができます。

PCI DSS 4.0準拠に向けた優先的なアプローチ

PCI DSSは、その包括的な性質上、膨大な量のセキュリティ情報を提供しています。そのため、ペイメントアカウントデータのセキュリティ担当者の中には、どこから手をつければよいのかと悩む人もいます。PCIセキュリティ基準審議会（SSC）は、PCI DSS準拠の初期段階からリスクを軽減する方法について組織が理解できるよう、準拠に向けた優先的アプローチを策定しました。

このガイドには、「優先的アプローチは、すべてのPCI DSSの要件を6つのリスクベースのセキュリティマイルストーンにマッピングします。これは、組織がPCI DSS準拠への取り組みを進めながら、最も高いリスク要因や増大する脅威から段階的に保護できるようにすることを目的としています」と記載されています。

PCI DSSの優先的アプローチには次の6つのマイルストーンが盛り込まれています。

1. **不要な機密認証データを保存せず、カード会員データの保持を制限する。**機密認証データやその他のアカウントデータを保存しないことによって、企業は侵害の影響を軽減することができます。
2. **システムやネットワークへのアクセスポイントを保護し、侵害に対応できるように準備する。**
3. **安全なペイメントアプリケーションを使用する。**このようなアプリの脆弱性が、システムへの侵入や、カード会員データへの不正アクセスなどに悪用されるケースがよくあります。
4. **システムへのアクセスを監視および制御する。**カード会員データ環境に対し、誰が、何に、いつ、どのようにアクセスしたかを明確に把握できるようにします。
5. **保存されたカード会員データを保護する。**カード会員データの保存が業務上必要である場合には、管理策を講じて、そのデータを保護します。
6. **残りの準拠活動の取り組みを完了し、すべての管理が整っていることを確認する。**

これらのマイルストーンは、組織がPCI DSS 4.0準拠への取り組みを進めながら、最も高いリスク要因や脅威から段階的に保護できるようにすることを目的とするものです。

優先的アプローチとそのマイルストーンは、あらゆる企業に、次の利点を提供します。

- リスクに対処するための構造的なアプローチを優先順位を設けて提供
- サイバーセキュリティとPCI DSS 4.0準拠に向けた現実的なアプローチがもたらす「即効性」
- 財務上および運用上の計画のサポート
- 客観的で測定可能な進捗指標

PCI DSS 4.0準拠のための日常的なベストプラクティス

PCI DSS 4.0への準拠は容易ではないでしょう。しかし、攻撃者らが用いる高度な手口に対抗するための強力な方策が獲得できます。まずは、PCI DSS 4.0基準を読んで、コンプライアンスプロセスに影響を与える可能性のある重要な変更点についてよく理解してください。その後、PCI DSS 4.0準拠に向けて、サイバーセキュリティプロセスに変更を実装する計画を策定します。

以下の段落では、標準的な12の要件について説明し、日常的な脅威から組織を保護しつつ、PCI DSS 4.0への準拠を進めるうえでの日常的なベストプラクティスを提供します。さらに詳しい情報については、PCI DSS関連リソースを参照してください。

要件1：ネットワークセキュリティコントロールの導入と維持

ネットワークファイアウォールは、セキュリティにおいて不可欠です。しかし、セキュリティを確保するには、単に組織のネットワーク境界にファイアウォールを設置するだけでは不十分です。

1. **ファイアウォール構成のベースラインを作成する：**ファイアウォールの設定を行う前に、ハードウェアのセキュリティ設定と業務に必要なポートやサービスのルールに加え、これらのルールの正当性に関するドキュメントを作成し、インバウンド、アウトバウンドの両方のトラフィックについて検討します。
2. **すべての設定をテストする：**ファイアウォールの設定が完了したら、ファイアウォールを外部および内部からテストし、設定が適切であることを確認します。
3. **アウトバウンドトラフィックを制限する（インバウンドトラフィックだけでなく）：**私たちはインバウンドポートのブロックにばかり気を取られがちですが、ネットワーク内からのアウトバウンドトラフィックを必要なものだけに制限することも忘れてはなりません。そうすることで、攻撃者によるデータ流出の経路を制限できます。
4. **個人のモバイルデバイス上にファイアウォールを設定する：**モバイル・コンピューティング・プラットフォーム上にパーソナルファイアウォールを設定することにより、攻撃対象領域を制限し、安全ではないネットワークに接続した際のマルウェアの拡散を最小限に抑えます。
5. **外部からのファイアウォールの管理を無効化する：**ファイアウォールの管理は必ずネットワーク内から行うようにします。安全なマネージド・ファイアウォール・インフラストラクチャの一部でない限り、外部の管理サービスは無効化します。

要件2：すべてのコンポーネントにセキュアな設定の適用

1. **デフォルト設定を変更し、内在する弱点を減らす：**デバイスには工場出荷時のデフォルト値（ユーザー名やパスワードなど）が設定されています。デフォルト設定により、デバイスのインストールとサポートを簡単にしていますが、それはすべてのモデルで同じユーザー名とパスワードが使われることを意味します。デフォルト値を変更せずに使用していると、攻撃者にあなたの組織のエコシステムへの侵入経路を与えてしまうことになります。カード会員データにアクセスするすべてのシステムにおいて、ベンダー設定のデフォルト値を変更しておくことが極めて重要です。
2. **業界のベストプラクティスに従ってカード会員データ環境（CDE）を強化する：**CDE内で使用するシステムは、本番稼動前に堅牢化しておく必要があります。システムの堅牢化の目的は、不要な機能を削除して、必要な機能を安全に構成することです。システムに接続されるあらゆるアプリケーションやデバイスが脆弱性をもたらします。PCI DSS要件2.2では、「すべての既知のセキュリティ脆弱性に対処し、業界で認められているシステム堅牢化の標準と整合している」ことを要求しています。
3. **一貫性を保ち、インベントリを最新の状態に保つ：**システムの堅牢化を実行し、文書化されたら、その設定を環境内のすべてのシステムに一貫して適用しなければなりません。ドメイン内の各システムとデバイスに適切な設定を行ったら、インベントリを最新の状態に保つ責任の所在を特定する必要があります。このようにすることで、使用が認められていないアプリケーションやシステムを特定し、排除することができます。

要件3：保存されたアカウントデータの保護

1. **データが存在する場所を把握する：**データ検出ツールを使用して、暗号化されていないデータが存在する場所を特定し、それらを削除または暗号化します。このようなツールは、修正が必要なプロセスやフローの特定にも役立ちます。不適切なプロセスや設定が原因で、カード会員データが簡単に流出してしまうことがあります。データがあると思われる場所を探すことから始め、データがあるべきでない場所もすべて調査します。
2. **すべての保存データを暗号化する：**保存するカードデータは、業界で認められたアルゴリズムを使用して暗号化する必要があります。多くの組織が、暗号化されていないプライマリアカウントナンバー（PAN）を気づかぬうちに保有しています。企業はカードデータを暗号化することに加え、暗号化キーも保護しなければなりません。「堅牢な管理プロセスを用いた暗号化キーの保護」が行われていない状況は、家の鍵を玄関前に吊るしているようなものです。
3. **保持するデータを最小限にする：**不必要なデータは保管しないようにしましょう。PCI DSSの対象範囲を最小限にし、データレコードが本当に必要なのか自分に問いかけましょう。

要件4：オープンな公共ネットワークでの送信時に、強力な暗号化技術でカード会員データを保護する

1. **オープンな公共ネットワーク経由で伝送されるデータを保護する：**カード会員データの送信先を特定します。オープンな公共ネットワーク上を移動中のデータも暗号化する必要があります。
2. **旧バージョンのSSL/TLSを使用しない：**旧バージョンのSSLやTLSには、セキュリティ上の脆弱性があることが知られています。安全なバージョンのTLSをサポートしないPOSハードウェアを使用している場合など、業務上の理由で後方互換性の維持が必要である場合を除き、このような非推奨の暗号化プロトコルの使用は中止しなければなりません。

要件5：悪意のあるソフトウェアからシステムおよびネットワークを保護する

1. **アンチウイルスソリューションを定期的に更新する：**攻撃者がシステムに侵入して重要なデータを盗み出す機会を大幅に縮小し、侵害の可能性を積極的に減らすには、周到な脆弱性管理を実施することが最も効果的です。脆弱性管理戦略の一環として、アンチウイルスソフトウェアの更新を行いましょう。

要件6：安全なシステムおよびソフトウェアの開発と維持

1. **システムの更新とパッチの適用を定期的に行う：**セキュリティ態勢を維持するには、セキュリティアップデートを適時実行することが非常に重要です。ブラウザ、ファイアウォール、アプリケーション、データベース、POS端末、オペレーティングシステムなど、環境内のすべての重要なコンポーネントにパッチを適用します。PCI DSS要件6.3.3の「重要なパッチはリリース後1か月以内にインストールする」に準拠するように、ソフトウェアを継続的に更新します。クレジットカード決済アプリケーションやモバイル機器などの、重要なソフトウェアのインストールを忘れないようにします。脆弱性を低減するもう一つの方法として、脆弱性スキャンがあります。脆弱性スキャンは、サイバー犯罪者が組織へのアクセスや侵害に悪用可能な既知のセキュリティギャップを発見できる最良の方法です。
2. **安全なソフトウェア開発プロセスを確立する：**決済アプリケーションを社内で開発する場合は、厳格な開発プロセスと安全なコーディングガイドラインに従う必要があります。OWASPのような、業界で認められた基準に従ってアプリケーションの開発・テストを行うようにしましょう。
3. **Webアプリケーションファイアウォールをインストールする：**PCI DSS要件6.4では、Webアプリケーションファイアウォール（WAF）を使用して、一般公開されているWebアプリケーションを保護することにより、Webベースの攻撃を定期的に監視、検出、防止することを義務付けています。このようなソリューションは、Webベースの悪質なトラフィックを監視・ブロックすることに特化するものです。

要件7：システムコンポーネントおよびカード会員データへのアクセスを制限する

1. **データおよびシステムへのアクセスを制限する：**ロールベースアクセス制御（RBAC）システムを導入し、ロールリストを定義して最新の状態に保つことにより、カード会員データへのアクセスをNeed-to-now（業務上必要な適用範囲）の原則に則って許可する必要があります。アクセスを制限することで、機密データが権限のない人物の手に渡ることを防止できます。

要件8：ユーザーの識別とアクセスの認証

1. **強力な一意のパスワードを使用するポリシーを確立し、パスワードマネージャを導入する：**長さ、一意性、複雑さの要件を満たしていないユーザー名やパスワードは脆弱性となります。

人間の性質がもたらす限界とリスクに対処するため、企業向けのパスワード管理ソフトウェアの導入を検討し、複雑なパスワードによってユーザーエクスペリエンスが損なわれないようにしましょう。

2. **堅牢なアカウント管理機能：**PCI DSSでは、デフォルトのアカウントを無効にし、一意のユーザー名と管理者アカウント名を設定することを義務付けています。攻撃ルートにさらに多くの防御壁を設けることにより、企業の安全性を高めることができます。

3. **多要素認証を実行する：**単一のパスワードは、どれほど強力であっても、それだけではセキュリティ対策とはなり得ません。多要素認証（MFA）は、安全なリモートアクセスを実現する最も効果的な手段であり、PCI DSS 4.0では新しい要件となっています。認証手段は、アウトオブバンドでそれぞれ独立した経路を使用する必要があります。認証要素を物理的に分離し、ある認証要素へのアクセスによって、別の要素へのアクセスが許可されないようにしなければなりません。たとえ1つの要素が侵害されたとしても、他の要素の完全性および機密性に影響は及びません。さらに、PCI DSSは「事業体のネットワーク外から発信されるすべてのリモートネットワークアクセスに対して、多要素認証を行う」ことを要求しています

（これには、ユーザーと管理者の両方、およびサポートまたは保守を目的とするサードパーティからのアクセスが対象とされます）。

要件9：物理アクセスの制限

1. **組織の環境への物理アクセスを制御する：**重要な資産やデータのオンプレミスでの安全性を維持するための物理的なセキュリティポリシーを導入し、物理的なセキュリティリスクを軽減します。たとえば、これらの重要資産を堅牢な施設で保護することができます。また、部外者の出入りを1箇所の監視付きの入口のみに制限し、外部からの人物には訪問者用バッジの着用を義務付けることもできます。

2. **POS端末を追跡する：**POSシステムやモバイル決済デバイスを使用する事業者は、すべてのデバイスの最新リストを維持し、これらのデバイスを定期的に検査しなければなりません。また、カード提示デバイスを日々扱う従業員に対し、意識向上トレーニングを実施する必要があります。

要件10：すべてのアクセスをログに記録し、監視する

1. **システムログとアラートを定期的に確認する：**ログを追跡するシステムは、ネットワークアクティビティの監視、システムイベントの調査、不審なアクティビティの警告を行い、組織の環境内で実行されるユーザーのアクションを記録します。ログを収集し、一元管理システムやオンサイトのロギングサーバー、あるいはインターネットサービスに送信することが求められます。ミスや不正、通常とは異なる不審な行動を見つけるために、企業は毎日記録を分析しなければなりません。ログを入念に監視することにより、セキュリティプログラムの効果が向上し、セキュリティイベントに迅速に対応できるようになります。ログの分析と定期的な監視は、PCI DSSルールを遵守する姿勢を示せるだけでなく、インバウンドおよびアウトバウンドの脅威を阻止するうえでも有効です。

要件11：システムおよびネットワークのセキュリティを定期的にテストする

1. **組織の環境を理解し、脆弱性の検知とペネトレーションテストを定期的に実行する：**攻撃者は、ブラウザ、電子メールクライアント、POSソフトウェア、OS、およびサーバーインターフェイスの欠陥を通じて環境内にアクセスする可能性があります。最近発見された欠陥や脆弱性の多くは、カード会員データや機密データを扱う環境内のシステムにセキュリティ更新プログラムやパッチをインストールすることで、攻撃者に悪用される前に修正することができます。脆弱性を発見し、修復するには、脆弱性スキャン機能が役立ちます。カスタマイズされた内部アプリケーションの場合、コードテストやサードパーティによるペネトレーションテストを実行することにより、アプリケーションコードによく見られる欠陥の多くを発見することができます。ペネトレーションテストと脆弱性スキャンを互いに補完させることで、最高レベルのネットワークセキュリティを実現できます。これらのスキャンおよびテストによって脆弱な箇所を特定し、デプロイ前に修正することができるため、最善の防御策と言えます。

要件12：プロセスを文書化し、リスクアセスメントを実施する

1. **企業におけるすべてのセキュリティ対策を文書化し定期的に更新する：**すべての従業員は、文書化されたポリシーに簡単にアクセスできる必要があります。文書化しておくことで、情報漏えいが発生した場合にも、企業を潜在的な法的責任から守れる可能性があります。セキュリティポリシーと手順が完全かつ正確に記録されていれば、フォレンジック調査の担当者が企業のセキュリティ対策を確認しやすくなり、企業がセキュリティに対して積極的かつ真摯に取り組んでいることを示すことができます。企業は、PCI DSS 4.0に準拠するために、セキュリティへの対策およびアクションに関する文書を定期的に更新する必要があります。

2. **リスクアセスメントの手順を確立する：**PCIは、すべての事業体に対して、主要なリソース、脅威、弱点、および危険性を特定するためのリスクアセスメントを毎年実施することを義務付けています。それにより組織は、情報セキュリティ上の脅威を特定、体系化、および管理することができます。特定された脅威に対してランク付けやスコアリングを行うことも、リスクアセスメントの一部です。これにより、どの脆弱性に最初に対処すべきかの指針が得られ、優先順位の判断に役立てることができます。リスクを体系的に分類・評価し、軽減することにより、攻撃者がシステムにアクセスして損害を与える機会を奪い、最終的に攻撃を阻止することができます。

3. **インシデント対応計画を策定およびテストする：**データの漏えいがもたらす影響に備えなければなりません。企業には、継続的なインシデントの制御、顧客への被害の最小化、データ漏えいに関連するコストの低減、各種基準や規則に従った関係当局との適切なコミュニケーション、および企業の安全確保に対する責任があります。効果的なインシデント対応戦略は、情報漏えいの影響を軽減し、罰金を引き下げ、悪評を減らし、通常業務への迅速な復帰を可能にします。

4. **すべての従業員に意識向上のためのトレーニングを提供する：**ほとんどの侵害は、人為的なミスに起因します。多くの従業員は、悪意がなくても、セキュリティのベストプラクティスを忘れたり、自分がどのように行動すべきかを正確に把握していません。残念ながら、多くの犯罪者は、人為的ミスを利用して個人情報を入手しようとします。従業員には、具体的なガイドラインを示すとともに、継続的なトレーニングを受講させる必要があります。従業員には、セキュリティ意識向上プログラムを通じて、セキュリティの価値を再認識してもらいましょう。そして、頻繁にトレーニングを実施し、特に新しいセキュリティポリシーや手順についての情報を提供します。

最後に

2024年のPCI DSS 4.0準拠の期限までには、まだ十分な時間があります。早期に開始すれば、移行に向けた正しい道を進むことができます。PCI DSS 4.0への移行開始を2024年まで待つ必要はありません。PCI DSS 4.0へのアップグレードを、適宜進めてください。将来のニーズを検討し、それを組織の戦略とセキュリティプログラムに織り込むことにより、時間を効果的に使えるようにします。長期目線で、組織にとって幅広く利益をもたらすことに注目するようにしましょう。

Fortraができること

Fortraが提供するサイバーセキュリティおよびコンプライアンス対策用ポートフォリオでは、PCI DSS 4.0の要件を遵守し、リスクや脅威から組織を守るという企業の日常的な要求を満たすべく、広範なソリューションとサービスを提供します。以下はPCI DSS 4.0の要件とFortraのソリューションの対応を表にまとめたものです。

PCI DSS 4.0の要件	Fortraのソリューション
要件1 ネットワークセキュリティコントロールの導入と維持	
要件2 セキュアな設定の適用	FortraのTripwire Enterpriseセキュリティコンフィギュレーション管理機能により、企業はネットワーク、サーバー、ファイアウォールなどのあらゆるコンポーネントの設定を監視できます。
要件3 保存されたアカウントデータの保護	FortraのDigital Guardian Enterprise DLPでは、事前に定義されたPCIポリシーを使用して、一般的な各出口ポイントにおけるクレジット情報の流出を監視およびブロックすることができます。 FortraのDigital Guardian Network DLP アプライアンスは、すべてのネットワークトラフィックを検査して、PCIやその他のコンプライアンス要件に対して事前設定されたポリシーを適用し、データを保護します。
要件4 オープンな公共ネットワークでの送信時に、強力な暗号化技術でカード会員データを保護する	FortraのGoAnywhere MFTは、PCI DSSに準拠した機密データの転送を可能にするセキュアなマネージドファイル転送ソリューションです。 FortraのVeraは、PIIやPCIなどの機密データを含むファイルを、それが共有される場所、方法を問わず保護します。組織は、カード会員データを暗号化して、アクセスを制御するだけでなく、データを追跡・監査し、そこへのアクセスを無効にすることができます。
要件5 悪意のあるソフトウェアから システムおよびネットワークを保護する	FortraのPowertech Antivirusは、各種ウイルス、マルウェア、ランサムウェアなどから御社のサーバーを保護します。
要件6 安全なシステムおよびソフトウェアの 開発と維持	FortraのBeyond Security製品では、動的アプリケーションセキュリティテスト（DAST）および静的アプリケーションセキュリティテスト（SAST）ソリューションを用いて、開発プロセスの初期にアプリケーションの脆弱性を検出します。 Fortraの脆弱性管理ソリューションは、企業環境における脆弱性の特定と優先順位付けを支援し、攻撃者に発見される前にセキュリティギャップを解消します。 Fortra Tripwire Enterpriseのコンフィギュレーション管理機能は、企業環境における計画外の変更を検出し、システムの完全性を高めます。 FortraのAlert Logic MDR Essentialsは、エクスポージャーアセスメント機能および管理ツールを含み、外部スキャンおよびネットワーク/エージェントベースのスキャンを実行して、オンプレミスやクラウド上のIT環境におけるエクスポージャーの360度ビューを提供します。FortraのAlert Logicは、PCI認定スキャンベンダーとして承認されています。 FortraのAlert Logic Managed WAFは、Webベースの攻撃を継続的に検知・防御することによりWebアプリケーションを保護します。
要件7 システムコンポーネントおよびカード会員データへのアクセスを制限する	FortraのCore Security Access Assurance Suiteにより、単一のインターフェイスから組織全体におけるアクセスを識別および管理できるようになります。Core Privileged Access Manager（BoKS）は、重要なシステムや情報へのアクセスおよび権限の管理を支援します。
要件8 ユーザーの識別と アクセスの認証	Fortra's Core Passwordは、セキュアなセルフサービス型パスワード管理のリーディングソリューションです。複数のアクセスオプションや堅牢なサービスデスクインテグレーションに対応し、あらゆるシステム、アプリケーション、Webポータルに一貫したパスワードポリシーを適用する機能を備えています。
要件9 物理アクセスを制限する	

PCI DSS 4.0の要件	Fortraのソリューション
要件10 すべてのアクセスをログに記録し、監視する	FortraのTripwire LogCenterは、ログの収集、分析、配信を一元的に行う相関エンジンです。 FortraのAlert Logic MDR Professionalサービスには、ログの管理、保存、およびインジェスト時における不審あるいは悪質なアクティビティの分析が含まれます。これには、UBAD (User Behavior Anomaly Detection)などの高度な分析が用いられ、必要に応じてSOCアナリストによるトリアージが行われます。 FortraのAlert Logic Health Console および Network Health Viewは、Alert Logicセキュリティアプライアンスの健全性を監視および通知します。
要件11 システムおよびネットワークのセキュリティを定期的にテストする	FortraのTripwire Enterpriseの整合性管理機能により、いつ、どこで変更が発生したかを明確に把握することができます。 PCIの認定スキャニングベンダー（ASV）であるFortraの脆弱性管理ソリューションは、包括的なセキュリティ評価の実施を支援し、組織にとって最も重大なリスクに優先順位をつけることを可能にします。 FortraのAlert Logic MDR Essentialsは、エクスポージャーアセスメント機能および管理ツールを含み、外部スキャンおよびネットワーク/エージェントベースのスキャンを実行して、オンプレミスやクラウド上のIT環境におけるエクスポージャーの360度ビューを提供します。FortraのAlert Logicは、PCI認定スキャンベンダーとして承認されています。 FortraのCore Security Core Impactは、高度なペネトレーションテストを効率的に実施するうえで役立ちます。ガイド付きの自動化機能と、認証済みのエクスプロイトを使用すれば、今日の攻撃者らと同様の技術を用いて組織の環境を安全にテストすることができます。
要件12 組織の方針とプログラムによって情報セキュリティをサポートする	FortraのTerranova Securityは、人物中心のアプローチを用い、ターゲットを絞り興味をそそる内容の実用的なセキュリティ意識向上トレーニングを提供します。また、PCI DSSに特化したトレーニングモジュールも用意しています。

これらすべての対応を自社で実施できないという場合には、TripwireおよびAlertLogicのマネージドサービスチームが御社の外部チームとして、セキュリティリスクを低減し、PCI DSS 4.0への準拠を容易に実現します。

御社のPCI DSS 4.0の準拠達成に向けて、Fortraがどのように支援できるかを詳しくお知りになりたい場合には、追加のPCI関連リソースをご覧になるか、当社までお問合せください。お話を伺い、どのようなお手伝いができるかご説明いたします。

FORTRA™

Fortra.com

Fortraについて

Fortraは、他に類を見ないサイバーセキュリティ企業です。私たちは、よりシンプルでより強固な未来をお客様のために創造しています。当社の信頼のおける専門家と、包括的で拡張可能なソリューションのポートフォリオが、世界中の組織にバランスとコントロールをもたらします。常にお客様の味方であり、積極的な変革者である当社は、サイバーセキュリティの旅におけるすべてのステップを通じて安心を提供いたします。詳細については fortra.com.をご覧ください。