

PCI コンプライアンス対応をサポートする  
フォーティネットのソリューション

**~PCI DSS 2.0 を理解する~**  
採用された9つの変更点

## PCI DSS 2.0 を理解する

PCI SSC (Payment Card Industry's Security Standards Council : ペイメント カード業界セキュリティ基準協議会) は、新しいセキュリティ基準である PCI DSS 2.0 についての変更点を「[Summary of Changes – Highlights](#) (変更点の概要 - ハイライト)」と題して文書にまとめ、公開しました。このドキュメントには、カード取扱会社におけるセキュリティのインフラ、運用、コンプライアンスおよび基本ガイダンスに対する潜在的影響という観点から、PCI SSC によって提案された 9 つの変更点<sup>1</sup>が列挙されています。この 9 つの変更点は、PCI DSS 2.0 に盛り込まれた変更内容だけでなく、カード会員データの保護をさらに強化する上で PCI SSC がどのような展望を持っているかについても示唆しています。

### はじめに

本ホワイトペーパーでは、PCI DSS 2.0 で提案された変更点について説明し、それぞれの変更点がペイメントカード業界の業務にどのように影響するかについても解説します。PCI DSS 2.0 の新基準では、PCI DSS の各セクションに対する変更点の一覧が示されていますが、これよりも最も重要なことは、新 DSS の実装とスケジュール要件に関して更なる期間延長が発表されたことです。

PCI DSS 2.0 で提案された 9 つの変更点のうち 6 つは、「Clarification (明確化)」、つまり、PCI DSS の当初の目的をより明確に表すためのものと分類されています。これ以外の 3 つの変更点は、脆弱性の仮想化、範囲およびリスクベースの優先度設定に関するものです。本ホワイトペーパーでは、主に序文と各セクションに対するこの 3 つの変更点にフォーカスし、実際の業務に影響しないと考えられる「Clarification (明確化)」項目については取り上げません。提案された 9 つの変更点の要旨は、下表に示すとおりです。

PCI SSC は、業務上の理由から PCI の基準を準拠しなければならない会社に対して大きな影響力を持っていることを、公的ではない業界規制機関として、明確に認識しています。PCI SSC は、PCI DSS 2.0 で新たな考え方の移行を選択しています。これは、カード取扱会社に運用やインフラの変更を強いる方法では実装に数十億ドルもの費用がかかる可能性がある<sup>2</sup>と判断した結果、リスクベースの情報保証 (アシュアランス) という新たな考え方を PCI DSS 2.0 では持ち込んでいます。今回提案された変更点の初期の分析段階では、カード会員データの情報保証 (アシュアランス) を強化する★「を強化」になっていたのを「を強化する」に変更★には不十分であると指摘されています。一方で、提案された細かい変更点の一部については、十分に効果があると判断されています。重要なのは、“なぜ” または “どのように” これらの新しい要件がカード取扱会社によるセンシティブ情報やネットワークの保護方法を抜本的に変えるかを理解することです。

### 提案された 9 つの変更点

ここでは、今回提案された 9 つの変更点のそれぞれが組織に与える可能性がある影響に言及し★「可能性がある影響について言及し」にしたらどうでしょうか？★、PCI SSC の新しい方向性という観点から、その意味を考察します。PCI SSC によって「Additional Guidance (追加のガイダンス)」または「Evolving Requirement (発展型要件)」に分類された変更点は、主としてオリジナルの基準についての説明の意味を理解するのに苦労していた人に影響するものであり、オリジナルの基準からの要件を変更することを意図するものではないため、ここでは、これらの一部だけを取り上げ、これらのすべてを考察対象とはしていません。

次ページの表 (PCI SSC の “Summary of Changes” (変更点の概要) から抜粋) に、1.2.1 仕様と同じ順番で、それぞれの変更点の説明を記載します。この表の後に、今回提案された変更点の一部を、影響の可能性が高い順に分析します。

---

<sup>1</sup> PCI SSC のドキュメントは 3 つの Payment Application Data Security Standard (ペイメント アプリケーション データ セキュリティ標準) にも言及していますが、これらについては、PCI DSS には適用されないため、このホワイトペーパーでは取り上げていません。

要件の影響	提案された変更点	変更理由	分類
PCI DSS の序文	PCI DSS 要件 3.3 および 3.4 が PAN だけを対象とするものであることを明確にする。 説明を PTS Secure Reading and Exchange of Data (SRED) モジュールに合わせる。	PCI DSS とカード会員データの範囲を明確にする。	明確化
評価の範囲	カード会員データ環境の範囲を正確に規定するためには、カード会員データのすべての場所とフローを特定し、文書化する必要があることを明確にする。	カード会員データのすべての場所が PCI DSS 評価の範囲に含まれるようにする。	追加のガイダンス
PCI DSS の序文と各種要件	システム コンポーネントの定義を広げ、仮想コンポーネントも含まれるようにした。 2.2.1 要件を改訂し、「サーバーごとに 1 つの主機能」と仮想化の使用の主旨を明確にした。	仮想化に関するガイダンスを提示する。	追加のガイダンス
PCI DSS 要件 1	インターネットとカード会員データ環境の間の安全な境界を明確にする。	DMZ のさらなる明確化。	明確化
PCI DSS 要件 3.2	業務上の正当な理由がある場合に限り、カード発行会社はセンシティブ認証データを保存できることとする。	カード発行会社またはカード発行会社のプロセッサ（処理システム）に対する PCI DSS の適用範囲を明確にする。	明確化
PCI DSS 要件 3.6	暗号化キーの変更、暗号化キーの破棄または取替え、および暗号化キーの知識分割と二重管理の手順を明確にし、柔軟性を高める。	暗号化キー管理手順を明確にする。	明確化
PCI DSS 要件 6.2	リスクをランク分けすることで、脆弱性を格付けし、優先順を設定できるように、要件を改訂する。	リスクベースの手法を適用して、脆弱性に対処する。	発展型要件
PCI DSS 要件 6.5	要件 6.3.1 を 6.5 に編入することで、内部および Web 対応のアプリケーションの安全なコーディングに関する冗長性を排除する。 安全なコーディング基準の例に、CWE や CERT などの例を追加する。	要件をまとめることで、冗長性を排除する。また、安全なコーディング基準の例を増やし、OWASP 以外の例も取り上げる。	明確化
PCI DSS 要件 12.3.10	リモート アクセス時のカード会員データのコピー、移動および保存を業務上の正当な理由に合わせて調整できるように、要件を改訂する。	リモート アクセス テクノロジー経由のカード会員データのコピー、移動および保存を明確にする。	明確化

## 変更される要件: PCI DSS 要件 6.2

**変更理由:** 脆弱性を検出するために、リスクベースの手法を適用する。

**提案された変更点:** リスクをランク付けすることで、脆弱性を格付けし、優先順を設定できるように、要件を改訂する。

一部の会社がデータの保護に向けて採用している「基本」アプローチが、この変更の影響を受けることになると考えられます。リスクベースのアプローチでは、すべての脆弱性の影響度や発生の可能性は同じではないと想定しています。影響度が高いものを回避するために時間と労力をかけ、影響度が高くて発生の可能性が

高いものを優先すべきです。情報セキュリティにおいては、このことが基本になっているようですが、PCI DSS においてはこれまで、この点が認識されていませんでした。

リスクベースのアプローチを PCI のコンプライアンスの取り組みに常に使用していた会社にとっては、この変更の影響はそれ程大きくないかもしれません。コンプライアンスを主たる目標とする（つまり、コンプライアンス違反によって生じる影響度に関係なく、できるだけ多くのチェック項目をクリアできるようにすることを目標とする）アプローチを採用している場合は、この変更によって、これまでの手法が大きく変わる可能性があります。今回の提案変更点の説明を実際に読んでみなければ、PCI SSC がリスクベースのアプローチを推奨することを推測するのは困難です。リスクベースのアプローチを採用することは、コンプライアンス違反の一部のカテゴリが他のカテゴリよりも代償が高くなることを考えれば、妥当であると言えます。

リスクベースの分析の本質に関して言えば、どんな事故でも（たとえば、プライマリ アカウント番号（PAN）ではなく、顧客の個人識別情報（PII）の漏洩）、カード取扱会社にとってのリスクとカード発行会社にとってのリスクには大きな違いがあると言えます。PCI DSS の目的からすれば、このリスク分析で重点を置かれるのは、カード取扱会社ではなく、カード発行会社にとってのリスクとなります。

セキュリティ プランにおいて、コンプライアンスの意味を誤解しないようにしてください。PCI のような情報セキュリティの妥当なガイドラインへのコンプライアンスと各社での情報資産の保護との間には、大きな隔たりが生じることは事実です。この一方で、どの会社にも、その会社特有の環境のさまざまな側面があることも事実です。したがって、汎用的なルールでは、コンプライアンスを越えて、業務要件を考慮した包括的な現場のセキュリティ プランを置き換えることはできません。

**要点:** 一般的に、リスクベースのアプローチによる脆弱性対策は、セキュリティ事故による損失を抑える最良の戦略であると考えられています。法規制の領域や金融業界では、これ以外のモデルは事実上使用されておらず、このモデルを社内の他のプラクティスとうまく調整しておく必要があります。PCI DSS 2.0 で定義されたリスクと自社にとってのリスクの両方を特定し、分類するにあたっては、注意が必要です。たとえば、カード取扱会社が個人識別情報（PII）だけを収集していてプライマリ アカウント番号（PAN）を収集していなければ、カード発行会社に対するリスクはほとんどありません。ところが、漏洩したレコードに対するレコードあたりの通知のコストが大きいため、カード取扱会社にとって影響がある可能性があります。

## 変更される要件: 評価の範囲

**変更理由:** カード会員データのすべての場所が PCI DSS 評価の範囲に含まれるようにする。

**提案された変更点:** カード会員データ環境の範囲を正確に規定するためには、カード会員データのすべての場所とカード会員データの流れを特定し、文書化する必要があることを明確にする。

この提案変更点は、この変更点の説明が「追加のガイダンス」ではなく、「明確化」として分類されるべきであることを示す「Clarify（明確化）」で始まっていなければ、変更点のリストではるかに上位に位置付けられることになるでしょう。説明の内容から判断すると、この変更点は、「カード会員データ環境には、カード会員データが保存されている場所に加えて、カード会員データが通過するあらゆる場所が含まれる」という現実を明確にしようとするものであると考えられます。

この変更点のほとんどの部分については、PCI DSS の範囲で監査対象にならないリモートの場所にある（たとえば）テープ保管庫や POS システムを含まないことを正当化していた会社だけに影響するものと考えられます。ただし、クラウドベースの仮想化のような状況では、カード会員データ環境の境界線が実際にはどこであるのかが明確でなく、カード会員データの保管場所やカード会員データの流れに関する本当に明確な何らかのガイドラインが示されることで、今日の環境でのコンプライアンスに沿ったネットワークの設計が容易になると考えられます。

**要点:** カード会員データ環境の範囲を最小限に設定している会社であれば、この変更による影響はないと思われれます。ただし、カード会員データ環境の範囲は限定されていると楽天的に考えている場合は、範囲を広

げて検討する必要があるかもしれません。監査を適切に進めるためには、カード会員データ環境の範囲を的捉えることを常に心掛けることです。このガイダンスの影響が大きい場合には、PCI DSS の QSA（認定セキュリティ評価機関）との面談の機会を設け、QSA の当初の範囲に照らし合わせて、提案修正案について話し合ってください。

## 変更される要件: PCI DSS の序文と各種要件

**変更理由:** 仮想化に関するガイダンスを提示する。

**提案された変更点:** システム コンポーネントの定義を広げ、仮想コンポーネントも含まれるようにした。2.2.1 要件を改訂し、「サーバーごとに1つの主機能」と仮想化の使用の主旨を明確にした。

この変更点は、今回の重要な変更点の中でも、実際の変更内容が最も分かりにくいものです。仮想化はかねてより論議の多い話題ですが、その主な理由は、要件バージョン 1.2 のセクション 1.2 にある「サーバーあたり 1 つの主機能だけを実装する」という記述によるものです。仮想環境においては、サーバーそのものによって基底となる仮想マシンの動作が実装されるため、技術的にはコンプライアンス違反とも言えます。さらに面倒なことに、高可用性の一部の状況での仮想マシンの自動マイグレーションにより、どの時点においても、どの機能がハードウェアのどの部分で実行中であるのかを正確に突き止めるのが困難である可能性があります。

もちろん、PCI DSS 2.0 でも、仮想化と仮想化のすべての利点が PCI DSS 2.0 コンプライアンスに沿った形で達成できるような方法で、この点を解決しなければならないでしょう。どのような方法でこの件が解決されるのかについては、残念ながら、次回の詳細発表まで分かりません。可能性が高いのは、ファイアウォール境界の共存する仮想マシン上での一定の制限付きの仮想化が認められ、データベース ストレージと仮想イメージストレージの両方に関する追加要件が設けられるという方法です。

**要点:** 仮想化を検討している会社にとっては、この変更点が、PCI DSS コンプライアンスを維持しつつ目標を達成するゲートウェイとなるでしょう。新たなルールが仮想化の取り組みの足枷となって仮想化環境本来の利点が失われないことを願います。最も望ましいのは、新たなルールがオンデマンドでの処理時間とストレージをサポートする次の論理ステップとなり、クラウドベースの仮想化環境のアプローチが明確になることです。共有環境によって、テクノロジーによる対応が始まったばかりの PCI の問題が浮き彫りになるでしょう。

## 変更される要件: PCI 標準のライフサイクル

**変更理由:** 関係者が意見やフィードバックを送る機会を増やし、フィードバックを受け付ける期間を延長し、カード取扱会社にとって望ましい開始日を設定する。

**提案された変更点:** PCI DSS 基準のライフサイクルを1年間、延長する。開始日を2011年1月1日に変更する。

この変更点は変更点の表には記載されませんでした。実際には PCI SCC ドキュメントで検討された最初の大幅変更であり、コンプライアンスの取り組みと関連費用への影響の可能性のリストでは先頭に記載されるべきものです。意見やフィードバックを受け付ける期間が長くなれば求める結果を得られるはずであり、基準受け入れの開始日が2009年末から2011年1月1日に変更されたことは、予算の観点からみて納得できることです。しかしながら、これらのいずれについても、この変更点がリストの先頭に記載されるべき理由ではありません。

この変更によって、各社の PCI インフラ投資のために想定される最短ライフサイクルが50%延長されます。PCI 基準のライフサイクルの満了時には、ルールが変更され、現行の PCI インフラでは新しい要件に対応できなくなる可能性があります。この変更によって、24カ月のライフサイクルがさらに12カ月延長されるため、現在のインフラに対する投資のROIが向上します。財務上の観点から良い方向へと大きく前進した変更であると言えます。

情報セキュリティの分野では、3年間というのは長い期間ですが、柔軟性の低いルールはライフサイクル満了時までには陳腐化し、その時々新たな脅威が反映されなくなる恐れがあります。そのため、[新ライフサイクルドキュメント \(英文\)](#) では、「ライフサイクルの半ばに変更する、あるいは補足ガイダンスを提出する」権利が確保されています。

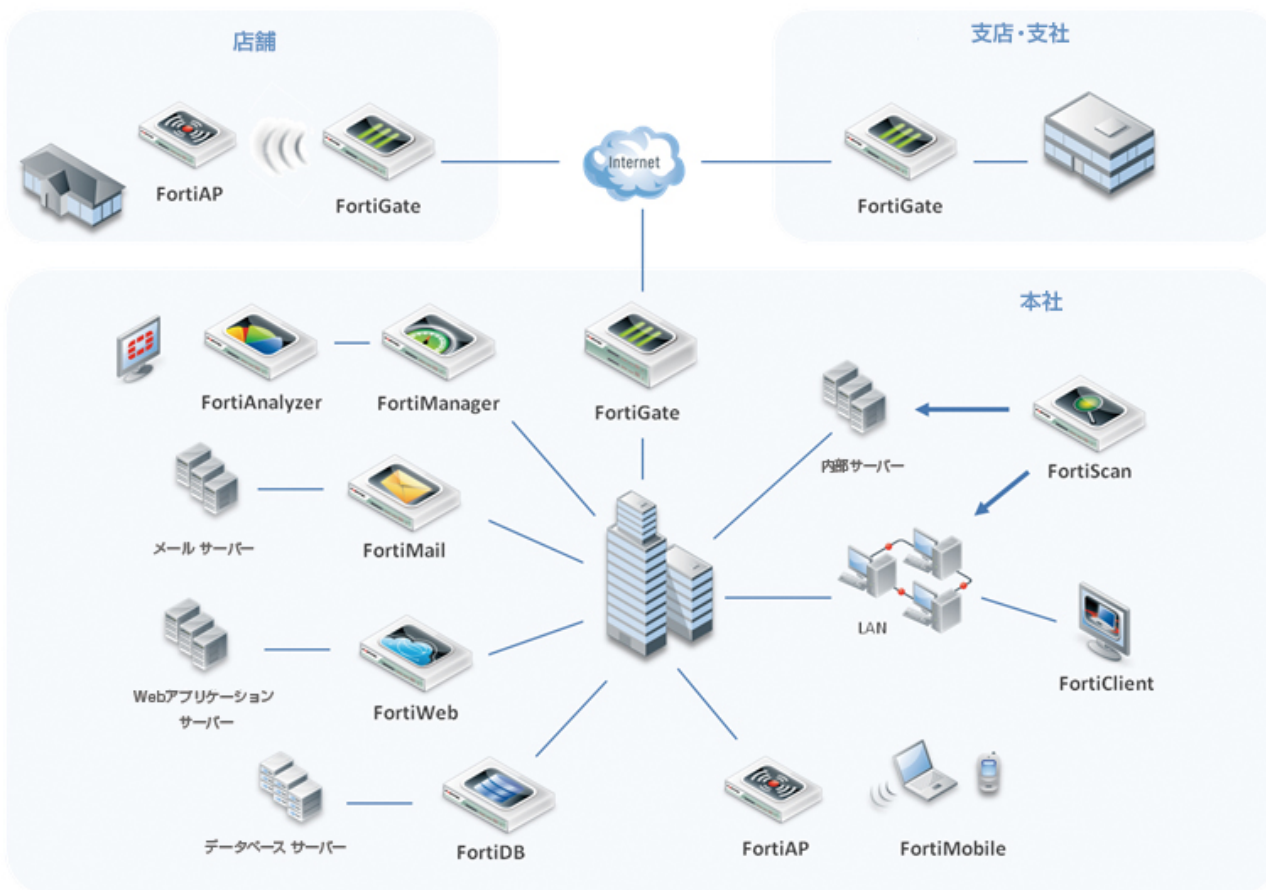
**要点:** ルールの有効期間が長くなれば、ライフサイクルの半ばでの変更を頻繁に PCI SSC が決定しない限り、情報セキュリティの ROI の数値が改善されるはずで、柔軟性をもって投資できるようになります。

## フォーティネットのソリューション: いかに、フォーティネットは皆さんを支援できるか

フォーティネットの FortiGate® 統合セキュリティ システムにより、小売業や PCI コンプライアンス基準に関係する会社は、地理的に分散する複数のサイトやミッションクリティカルなアプリケーション（在庫管理システム、POS システム、予約システムなど）のセキュリティを確保すると同時に、IT の予算や人員を増やすことなく、PCI-DSS 基準に準拠できます。コンテンツとネットワーク処理という目的に特化して設計された FortiASIC™ プロセッサを採用した FortiGate システムは、リモート オフィス アプライアンス、モバイル POS アプリケーションやキオスク端末から、マルチギガビットのコア ネットワークやデータセンターのプラットフォームまで、さまざまな規模の環境に、マルチレイヤの完全なセキュリティを提供します。FortiGate システムは、ファイアウォール、侵入防止システム (IPS)、アプリケーション制御、VPN、トラフィックシェーピング、アンチウィルス、アンチスパイウェア、アンチスパム、コンテンツ フィルタリング、脆弱性管理などをひとつに統合した単一ソリューションで、脅威からの完全な保護を可能にします。FortiManager™ および FortiAnalyzer™ 管理/レポートアプライアンスは、あらゆる規模の環境で、脆弱性管理や規制へのコンプライアンスのためのログ/アーカイブ機能を始めとする一元的制御を可能にします。フォーティネットのデータベース セキュリティおよびコンプライアンス製品は、集中管理によるデータベース強化、高速で包括的なポリシー コンプライアンス、脆弱性評価 (VA) などの機能を提供し、組織全体のデータセキュリティの強化に貢献します。

フォーティネットのソリューションの主な利点は次のとおりです。

- FortiGate システムは、重要なアプリケーションのパフォーマンスやネットワークの可用性やアップタイムを損なうことなく、ネットワークレベルおよびコンテンツレベルの脅威からのスケーラブルで包括的な保護を可能にします。
- 管理が容易なプラットフォームに複数の脅威からの保護が統合されているため、面倒な管理作業は必要なく、導入費用も低く抑えられ、低 TCO を実現します。
- FortiClient™ エンドポイント セキュリティ エージェントは、3G のサポートによって有線のブロードバンドがないリモートの場所にも対応し、リモートのパソコンやラップトップ パソコンのための、包括的な一元管理によるセキュリティを提供します。
- FortiAP™ 無線アクセス ポイントは、高速の 802.11n 無線をサポートしており、FortiGate プラットフォームを無線コントローラとして使用することで、エンタープライズ環境への導入に対応し、無線ネットワークのコスト削減に貢献します。
- FortiManager と FortiAnalyzer は、複数サイトの管理を容易にするアプライアンスで、広範なロギング/アーカイブ機能によって顧客や訪問客による安全なクレジットカードの使用をサポートすることで、コンプライアンスの維持を支援します。
- FortiDB™ データベースセキュリティ コンプライアンス製品は、プリインストールされたポリシーによって、重要なデータベース リソースを保護します。数百に及びプリインストールされたポリシーは、PCI-DSS を始めとする重要な規定のコンプライアンス レポートを含む業界および公的な標準の要件やベスト プラクティスを網羅しています。
- 仮想ドメインやセキュリティ ゾーンの幅広い機能により、広範囲に分散する複数のサイトのネットワークやアプリケーションのきめ細かいアクセス制御が可能です。
- どのシステムでも複数のセキュリティ機能を利用でき、既存のソリューションに簡単に追加できます。さらに、ハードウェアやソフトウェアに対する追加投資なしに、機能を強化できます。



図：小売業でのフォーティネット PCI DSS ソリューション導入例

フォーティネットの幅広い製品ポートフォリオは、PCI コンプライアンスの多くの局面に対応します。下表は、フォーティネットのどの製品がどの PCI 標準に対応するかを示したものです。

PCI DSS	説明	フォーティネットのソリューション
安全なネットワークの構築・維持	1. データを保護するためにファイアウォールを導入し、最適な設定を維持すること。  1. システム パスワードと他のセキュリティ パラメータに、ベンダー提供のデフォルトを使用しないこと。	FortiGate 統合ファイアウォール機能  FortiDB 脆弱性の評価と監査  FortiWeb Web アプリケーションのパスワード・チェック  FortiScan OS の脆弱性の管理
カード会員データの保護	3. 保存されたカード会員データを保護すること。  4. 公衆ネットワーク上でカード会員データや機密情報を送信する場合、暗号化すること。	FortiDB 脆弱性の評価と監視  FortiWeb Web アプリケーションのファイアウォール  FortiGate IPSec VPN
脆弱性を管理するプログラムの整備	5. アンチウイルス ソフトウェアを利用し、定期的に更新すること。	FortiGate 統合アンチウイルス  FortiClient および FortiMobile 統合アンチウイルス  FortiMail 統合アンチウイルス

	5. 安全性の高いシステムとアプリケーションを開発し、保守すること。	<p>FortiGuard 自動アンチウイルス更新</p> <p>FortiGate 脆弱性の管理</p> <p>FortiDB 脆弱性の評価、監査、監視</p> <p>FortiWeb Web アプリケーションのセキュリティ</p> <p>FortiScan OS の脆弱性の管理</p> <p>FortiAnalyzer ネットワークの脆弱性のスキャン</p>
強固なアクセス制御手法の導入	<p>7. データへのアクセスを業務上の必要範囲内に制限すること。</p> <p>7. コンピュータにアクセスする利用者毎に個別の ID を割り当てること。</p> <p>7. カード会員データへの物理アクセスを制限すること。</p>	<p>FortiDB 脆弱性の評価、監査、監視</p> <p>FortiGate アクティブ ディレクトリの統合データベースまたはフック</p> <p>FortiPartner VAR ソリューションとのパートナーシップによる、フォーティネットのプロフェッショナルサービス</p>
定期的なネットワークの監視およびテスト	<p>10. ネットワーク資源およびカード会員データに対するすべてのアクセスを追跡し、監視すること。</p> <p>10. セキュリティ システムおよび管理手順を定期的にテストすること。</p>	<p>FortiDB 監査と監視</p> <p>FortiAnalyzer イベントのレポート、脆弱性のスキャン</p> <p>FortiDB 脆弱性の評価</p> <p>FortiScan OS の脆弱性の管理</p> <p>FortiGate 脆弱性の管理</p>
情報セキュリティ ポリシーの整備	12. 情報セキュリティに関するポリシーを整備すること。	<p>FortiManager セキュリティポリシー管理アプライアンス</p> <p>FortiScan OS の脆弱性の管理</p>

## まとめ

多くの評論家が、PCI DSS バージョン 2.0 で提案された変更点が比較的小規模であることから、バージョン 1.3 とすべきだったのではないかという感想を漏らしています。しかしながら、一部の組織では、今回取り上げた変更点によって、コンプライアンスの問題の解決方法やカード会員データ環境のプランニングへの新しいテクノロジーの採用方法が大きく転換することになる可能性があります。ほとんどの部分についてみれば、今回提案された変更点では、業界標準（リスクベースのアプローチ）、新しい IT 標準（仮想化、クラウドなど）、情報セキュリティの投資をできるだけ長く利用したいという当然とも言うべき要望が理解されているようです。情報保護および情報保証に対する現状の考え方からみると、PCI DSS で具体的な内部統制ではなく内部統制の目標を特定することに向かって動き出したことに若干の驚きを感じます。しかしながら、監査プロセスに課されるトータルな負担を考えれば、理解できると言えます。

皆さんが現行の PCI DSS 基準を満たすことだけを目指しているツールに投資しているのではなく、柔軟性の高いハードウェアおよびソフトウェアのインフラに投資しているのであれば、運用やコンプライアンスの手順の大幅な変更は必要ないはずです。これまでも述べたように、今回の変更点はカード取扱会社に対し、直接的な利益をもたらすでしょう。以前に取り上げた、PAN に対するリスクを伴わない PII 違反のリスク分析の例では、法規制（特に、ワシントン州 HB 1149、ネバダ州 SB 227、ミネソタ州 H.F. 1758）に発生した利害は収束しています。ここでは、PCI コンプライアンスの証拠が、PCI に関連しているのであれば、違反に関する法的な根拠になっています。

最後に、ネットワーク攻撃の多様化と急増によって、コンプライアンスへの投資はもはや、「できれば望ましい」というものではなくなったことを指摘したい。クレジットカードや POS の情報を取り扱うすべての企業にとっては、コンプライアンスへの投資は必ず取り組まなければならない待ったなしの最重要要件になったといえることができます。

## 著者紹介

### Michael Simon - Creation Logic 社、最高技術責任者

Mike Simon は 1985 年以来、コンピュータのセキュリティおよびポリシーの開発に携わっています。アイダホ大学在職時には、コンピュータセキュリティの地域のパイオニアとして、また、NSA Centers of Excellence in Information Assurance Education プログラムの一員として、同センターの研究プログラムに使用するネットワーク研究所のインフラストラクチャを構築し、大学の専門課程や大学院のネットワークおよびネットワークトポロジのコースで教鞭をとっていました。

1993 年～2005 年 9 月までは、シアトルに本社を置く著名セキュリティコンサルティング会社のサイエンス担当責任者として、数百社に及ぶ企業のセキュリティ対策の策定とセキュリティ体制の改善に携わりました。医療、バイオテクノロジー、軍事、ストリーミングメディア、電力施設、金融機関、電子商取引、航空などの幅広い分野で、企業を保護するセキュリティのインフラストラクチャやポリシーの設計を指揮しました。

現在は、最高技術責任者として Creation Logic 社で技術面の指揮に当たる傍ら、ワシントン大学でも非常勤講師として教壇に立ち、シアトル大学、アイダホ大学、The Office of the Director of National Intelligence (ワシントン大学の Institute for National Security Education and Research) やさまざまな団体の講座で講師を務めています。また、情報評価認定プログラムの顧問、Goldfish Holdings 社の技術顧問、アイダホ大学のコンピュータサイエンス学部および工学部の顧問を務めており、ワシントン大学情報学部の創立メンバーでもあります。Mike は、アイダホ大学でコンピュータサイエンスの学位を取得しました。



フォーティネットジャパン株式会社

〒106-0032

東京都港区六本木7丁目18-18 住友不動産六本木通ビル8階

TEL:03-6434-8531/8533 FAX:03-6434-8532

購入前のご相談: <http://www.fortinet.co.jp/contact>

※記載された社名、各製品名は各社の登録商標または商標です。  
※記載された内容は、変更する場合がありますのでご了承ください。

お問い合わせ