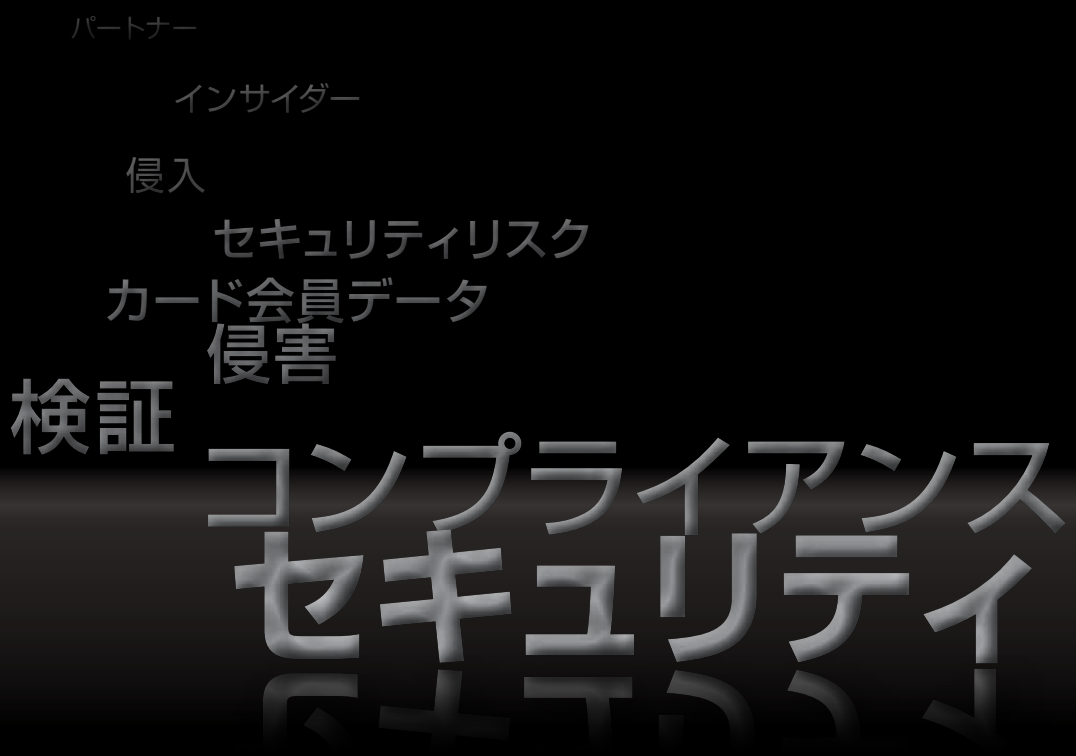
ベライゾン 2010 年ペイメントカード業界コンプライアンス調査報告書

ベライゾン ビジネス PCI チームおよび RISK インテリジェンスチームによる調査



verizon

ベライゾン 2010 年ペイメントカード業界コンプライアンス調査報告書

執筆および協力：

Wade Baker
Michael Dahn
Tabitha Greiner
Alex Hutton
C. David Hylender
Peter Lindstrom
Jennifer Mack
Christopher Porter
Denson Todd
PCI チームおよび RISK チームのその他のメンバー

目次

ベライゾン 2010 年ペイメントカード業界コンプライアンス調査報告書

ベライゾン ビジネス PCI チームおよび RISK インテリジェンスチームによる調査

要約

『ベライゾン 2010 年ペイメントカード業界コンプライアンス調査報告書』は、ベライゾンの認定セキュリティ審査員（QSA）チームが実施した実際のペイメントカード業界データセキュリティ基準（PCI DSS）のアセスメント結果を分析した報告書です。本報告書では、コンプライアンスの目標達成に向けた企業・機関の進捗状況を検証し、他の企業・機関よりも対応に苦慮している企業・機関の状況やその原因などのトピックを取り上げています。さらに、PCI DSS の要件およびサブ要件のうち、評価プロセスにおいて実施が確認された（あるいは、代替管理策の対象となる）頻度が最も多いものと最も少ないものに関する統計も提示しています。最後に、PCI 評価データをベライゾンの調査対応サービスによる発見事項と照合し、リスクを重視した独自のコンプライアンスプロセスに対する観点を提供しています。主な分析結果には、次のようなものがあります。

- 企業・機関の 22% は、初期コンプライアンスレポート（IROC）の時点で検証により PCI DSS に準拠していると判定されました。これらの企業・機関は、毎年繰り返し弊社のサービスを利用する傾向がありました。
- 平均では、企業・機関は IROC の段階で PCI DSS が定める全テスト手順の 81% で準拠と判定されていました。当然ながらこの数字には多少の変動がありましたが、準拠と判定されたテスト手順が全体の 50% 未満であった企業・機関は多くありませんでした（クライアントの11%）。
- 企業・機関が最も対応に苦慮していた要件は、要件10（アクセスの追跡と監視）、要件 11（システムとプロセスの定期的なテスト）、要件 3（保存されるカード会員データの保護）でした。
- 実施率が最も高かった要件は、要件 9（物理アクセスの制限）、要件 7（アクセスを業務上必要な範囲のみに制限する）、要件 5（アンチウィルスソフトウェアの使用と更新）でした。
- PCI DSSの要件のうち、代替管理策を通して準拠を実現した事例が他よりもはるかに多いのはサブ要件 3.4（プライマリアカウント番号（PAN）を読み取り不可能にする）でした。
- PCI セキュリティ基準審議会が公表した 『PCI DSS 優先アプローチ（PCI DSS Prioritized Approach）』に基づいて準拠に向けた取り組みの優先順位付けを行っていると思われる企業・機関はありませんでした。
- 全体として、データ漏洩/侵害の被害を受けた企業・機関が PCI DSSに準拠していた可能性は、弊社 PCI チームのクライアントの正常集団を 50% 下回っていました。
- ペイメントカードデータの漏洩/侵害につながる脅威アクション上位 10 件のすべてが、 PCI DSS の対象範囲内でした。それらの大半については、該当する脅威アクションが課すリスクを緩和するために定められた基準全体にわたって複数の階層の関連管理策が存在しています。

はじめに

規制コンプライアンスの歴史と自動車の交通パターンの歴史には、当初明らかであった以上に多くの共通点があるようです。自動車交通は、ビジネスと同様に、自由に流れるパターンのときに最も順調に機能しますが、1 件でもイベントが発生すると自動車の流れが中断され、交通渋滞が生じます。自動車交通の場合、考えられるイベントには、大きな事故、追い越し車線をゆっくり走る車、道路の合流や交差といった運転環境の変化などがあります。それゆえに、互いに連結している道路では特に、通行する人と車の安全を守りながら、最大の流れを実現するには、交通規則が必要なのです。

そうした複雑な輸送ネットワークは、情報ネットワーク上で互いに通信を行うよう設計された電子システムの相互接続状態に似ています。交通網やシステムの相互接続状態を中断させたり、危険にさらす無数のイベントについては、誰もが嫌というほど詳しく知っています。そのため、相互接続されたシステムのための「交通規則」がさまざまなかたちで出現し、その多くは、安全でセキュリティが確保された状態においてビジネスを運営できるよう、その運営方法を調整するコンプライアンスガイドラインの形式をとっています。ペイメントカード情報の処理、保存または送信を行うすべての企業・機関にとって、このコンプライアンスガイドラインの役割を果たしているのがペイメントカード業界データセキュリティ基準 (PCI DSS) です。

ペイメントカードのデータを保護するための業界基準が必要であるとの認識は、2001 年に VISA がカード会員情報セキュリティプログラム (CISP) とアカウント情報セキュリティプログラム (AIS) を、 MasterCard がサイトデータ保護プログラム (SDP) を導入するなど、ペイメントカード会社がそれぞれ固有のコンプライアンスプログラムを発足させたことから生まれました。2003 年には、CISP の対象範囲がペイメントカードの決済業者と発行会社から大規模小売店とサービスプロバイダーに拡大されました。次に、2006 年には、各ペイメントカード会社がコンプライアンスプログラムを履行する状態を維持しながら、それまでの複数のコンプライアンス基準を 1 つのイニシアティブによって統一するPCI DSS を、ペイメントカード会社 5 社が共同で開発しました。

それ以来、PCI DSS は大きな注目を集めるとともに議論の的になっています。多くの人は PCI DSS がペイメントカード業界にとってカード会員データの保護に向けた大きな一歩になると考えていますが、懐疑的な見方を続ける人もいます。懐疑的な見方の人からは、「PCI DSS が有効であることをどのように確認するのか」「PCI DSS は管理策の最善のミックスなのか」「どの管理策が他の管理策よりも有効か」「基準は十分に高く設定されているのか」「基準が低すぎるのではないか」「投資する価値があるか」「企業・機関の間の違いを適切に考慮しているか」「脅威環境の変化に対処できるか」などの質問が提示されています。これらはどれも良い質問であり、あらゆる指示的な行動規範について問われるべきものです。

本報告書は (あるいは他のどの単一のリサーチであっても)、PCI DSS を支持する人を正当化したり、懐疑的な見方を検証したりするものではなく、支持する人と懐疑的な見方の人の双方に必要なもの、つまり「データ」を提供することによって、懐疑的な見方を検証する方向で必要な基礎作りをするものです。そのために、本報告書では、ベライゾンの認定セキュリティ審査員 (QSA) チームが実施した実際の PCI DSS 評価の結果を分析しています。本報告書では、コンプライアンスの目標達成に向けた企業・機関の進捗状況を検証し、他の企業・機関よりも対応に苦慮している企業・機関の状況やその原因などのトピックを取り上げています。さらに、PCI DSS の要件およびサブ要件のうち、評価プロセスにおいて実施が確認された (あるいは、代替管理策の対象となる) 頻度が最も多いものと最も少ないものに関する統計も提示しています。最後に、PCI 評価データをベライゾンの調査対応サービスによる発見事項 (『データ漏洩/侵害調査報告書 (DBIR)』の情報源) と照合しています。この照合作業により、PCI DSS に関するリスクを重視した独自の分析が実現するとともに、企業・機関の正常集団 (弊社 PCI サービスが評価したクライアント) のプラクティスと既知のセキュリティインシデントの被害を受けた企業・機関 (弊社の調査対応 (IR) サービスが調査したクライアント) のプラクティスの比較を世界で初めて公表することが可能になりました。

予備的ではありますが、弊社では、本報告書の分析結果および関連する論考が、企業・機関がより十分な情報に基づいて (および、より十分に準備を整えて) PCI コンプライアンスに取り組む際に役立つことを願っています。プログラムの開始、改善、継続を問わず、他の企業・機関の現状と努力への理解を深めることによって、企業・機関が今後の評価において「準拠している」と判定されるような取り組みを調整する手がかりになると考えられます。最も重要なことですが、弊社では、本報告書 (および後続のその他のリサーチ) が最終的にペイメントカードに関するデータ漏洩の減少につながり、現代の経済に不可欠な金融取引のセキュリティの測定可能な改善に寄与することを願っています。

メソドロジー

本報告書の大部分は、ベライゾンの認定セキュリティ審査員 (QSA) が実施した PCI DSS 評価に基づいており、残りはベライゾンの調査対応チームが作成したペイメントカードセキュリティ侵害事例から直接引用していたものです[1]。QSA は、オンサイトでの業務中に、クライアントによる PCI DSS の準拠状況を検証するために、スタッフへのインタビュー、ポリシーのレビュー、文書の確認、管理策の評価を行います。オンサイト評価から 6 週間以内に、ベライゾンは初期コンプライアンスレポート (IROC) をクライアントに対して発行します。IROC は、クライアント (およびベライゾン) に、クリーンで完全な最終コンプライアンスレポート (ROC または FROC) に向けた要処置事項のリストを提供します。本報告書に使用したすべての評価結果は、有償業務の一環としてクライアントに提供した IROC と FROC から直接選び抜かれたものです。

ベライゾンの QSA チームは、毎年数百件の PCI アセスメントを実施しています。ただしいくつかの理由から、本報告書にはそのすべてが収録されているのではありません。代わりに、シンプルな選択プロセスを使って、この調査において取り上げる IROC や FROC のサンプルを作成しました。このプロセスにより、QSA、さまざまなタイプと規模の企業・機関、IROC、FROC などのミックスを含む十分にバランスのとれたサンプルになりました。その結果、本報告書において使用した最終データセットを構成する約 200 件の評価サンプルが選定されました。それらの大部分は、2008 年から 2009 年に米国で実施されたものです。

本報告書は、PCI DSS を支持する人を正当化したり、懐疑的な見方を検証するためのものではありません。支持する人と懐疑的な見方の人の双方にとって必要なものであるデータを提供することによって、懐疑的な見方を検証する方向で必要な基礎作りをするものです。

このデータセットには、PCI DSS 1.1 および 1.2 に基づいて作成されたIROC/FROCが含まれます。両バージョンの相違点は、分析プロセス中に (可能な限り) 考慮し、本報告書における具体的な要件、サブ要件、テスト手順への参照には、別途の記載がない限り、v1.2 での指定を使用しています。データと所見を IROC と FROC の両方から採用しているため、さまざまな統計がどのデータセットに基づいているのか判断するのが困難である可能性があります。明確化するため、すべての図表に出所を記載してあります。IROC と FROC のどちらを使用すべきかを判断する際には、該当するリサーチ上の質問に最適なものを単純に選択しました。本調査において企業・機関にとって多少なりとも困難を課す DSS の側面を分析するときに最も多くの情報を提供するものであるため、評価からの発見事項のほぼすべてを IROC から採用しました。その一方で、代替管理策に関連する発見事項は、評価の正式な最終結果に相当する FROC から採用しました。これらの一次統計に関する一般的な所見とコメントは、評価プロセス全体に基づいています。

最後に、重要なことですが、ベライゾンでは、クライアントのプライバシーと匿名性の維持を約束していることにご注意ください。クライアントの名称その他の識別情報は、集計したデータセットを分析する前に評価から除外されています。データの収集と分析は、『データ漏洩/侵害調査報告書 (DBIR)』 シリーズに使用する機密性の高い匿名情報の取り扱いに長年の経験を持つRISK インテリジェンスチームと共同で実施されました。さらに、本報告書に含まれる発見事項は、総括的に提示され、企業・機関を特定するようには、決して使用されていません。

1 ベライゾンの調査対応 (IR) チームは、よく知られているデータ漏洩/侵害調査報告書シリーズの情報源です。

PCI DSS 評価結果

規制コンプライアンス、検証、セキュリティの概念には相互関連性があるため、企業・機関が混乱することも少なくありません。この混乱の原因は、主に 2 つの基本的な思い違いにあります。第 1 に、多くの人がコンプライアンスを「安全な状態」とイコールであると考えています。この論理は成立しません。なぜなら、セキュリティは 「100 %かゼロか」という二元的な状態ではなく、「絶対に安全」から「絶対に脆弱」に至る分布のなかの任意の範囲にすぎないからです (ただし、実際にはこれらの両極の状態は存在しません)。つまり、ある企業・機関がある基準に準拠していると言うときは、ある企業・機関の「セキュリティの程度」がその基準が実現すべく設計されているセキュリティの程度と同様であることを意味するだけです。

第 2 に、規制コンプライアンスは情報セキュリティの多元的な性質に対処するための 1 つの試みです。したがって、特定の基準が実現すべく設計されているセキュリティレベルは、企業・機関が固守すべきベースラインとなります。 このベースラインは、経済活動に関わる人たち全員に突き付けられている業界規模のリスクに対処するために、企業・機関がその役割を果たしていることを保証するものです。ペイメントカード業界の場合は、このベースラインを定めるのが PCI DSS 基準であり、企業・機関によるこの基準の準拠レベルを測定するのが QSA です。

QSA が準拠レベルをどのように測定するのかについて理解を深めるためには、「準拠」という言葉と「検証」という言葉をさらに明確に区別しなければなりません。準拠は、規制団体の基準に従う継続的なプロセスです。PCI DSS の場合、「準拠」と呼ばれる継続的な状態を維持するために企業・機関が実施しなければならない要件が、日単位 (ログのレビュー)、週単位 (ファイル整合性モニタリング)、四半期単位 (脆弱性スキャン)、年単位 (侵入テスト) で定められています。

PCI DSS 基準が実現すべく設計されているセキュリティレベルは、企業・機関が固守すべきベースラインとなります。このベースラインは、活動に関わる人たち全員に突き付けられている業界規模のリスクに対処するために、企業・機関がその役割を果たしていることを保証するものです。

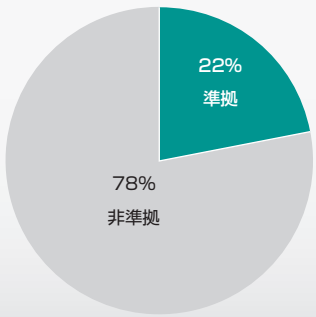
その一方で、検証とは一定時点のイベントであり、基準の準拠レベルを測定し、記述することを目的とした、現状分析に相当します。企業・機関は、「準拠状態を実現する」ために検証によって準拠という判定を得ることはできても、その後 (QSA が検証を終えて立ち去った後) は、時間の経過とともに、基準が実現すべく設計されたセキュリティの程度を維持することがおろそかになるかもしれません。したがって、すべての企業・機関は、PCI DSS 基準が定める最小限のベースラインコンプライアンス要件に準拠しているセキュリティ状態を維持することを目標とすべきなのです。

これは、企業・機関が PCI DSS の最小要件を履行するだけでよいと言っているのではありません。確かに、多くの企業・機関が PCI DSS の要件を上回るレベルや範囲のセキュリティを実現しています。しかし、本報告書は、企業・機関による PCI DSS 自体の準拠状況と、さらに、QSA が企業・機関それぞれの環境における一定時点での検証において行った準拠レベルの測定結果に関する分析に重点を置いています。状況の記述や分析結果を論じるにあたっては、トップダウン方式のアプローチを採用し、総合的な準拠状況の評価結果を紹介した後で、個別の要件とサブ要件の準拠状況について説明します。

総合的なアセスメント結果:

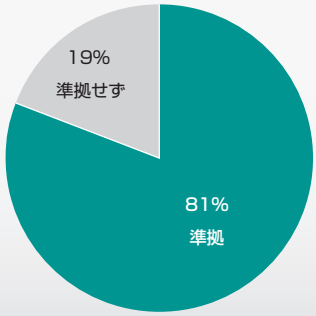
本調査の対象範囲内においてベライゾンの QSA チームがアセスメントを行った企業・機関のうち、22% が IROC の時点で検証により PCI DSS に準拠していると判定されました。この結果に対して、読者がさまざまな反応を示すであろうことは間違いありません。この数字が予想以上に低いと考える人もいれば、自身の経験やデータからこの数字が高すぎるのではないかと疑う人もいることでしょう。どのような立場をとるにせよ、この結果は議論に値します。

図1: IROC の時点で準拠と判定された企業・機関の割合



検証によって準拠していると判定された 22% の企業・機関を精査したところ、その過半数には共通する 3つの特徴が見られました。多くの企業・機関は、初期のオンサイトアセスメント中に特定された問題をIROC の完成前に修正することができました。その他の企業・機関は、検証プロセスを経験している (IROC の時点で検証により準拠していると判定された企業・機関の大半は 2009 年にも検 証を受けていました) か、または PCI DSS に含まれる要件の大多数が「該当せず」とみなされたかのいずれかでした。PCI DSS について経験を重ねている企業・機関が、初めて検証を受けた企業・機関よりも良い成績を残しているのは当然です (ただし、サンプルとした企業・機関の少数派 (22%) の話であることを忘れてはなりません。2008 年に ROC の時点で検証により準拠していると判定されたその他多くの企業・機関は、2009 年の IROC では準拠していると判定されませんでした)。同様に、評価の対象となる管理策要件のセットが小さい企業・機関の方が準拠状態の維持と検証が容易である理由を理解するのは難しいことではありません。

図2: IROC の時点で準拠と判定されたテスト手順の割合



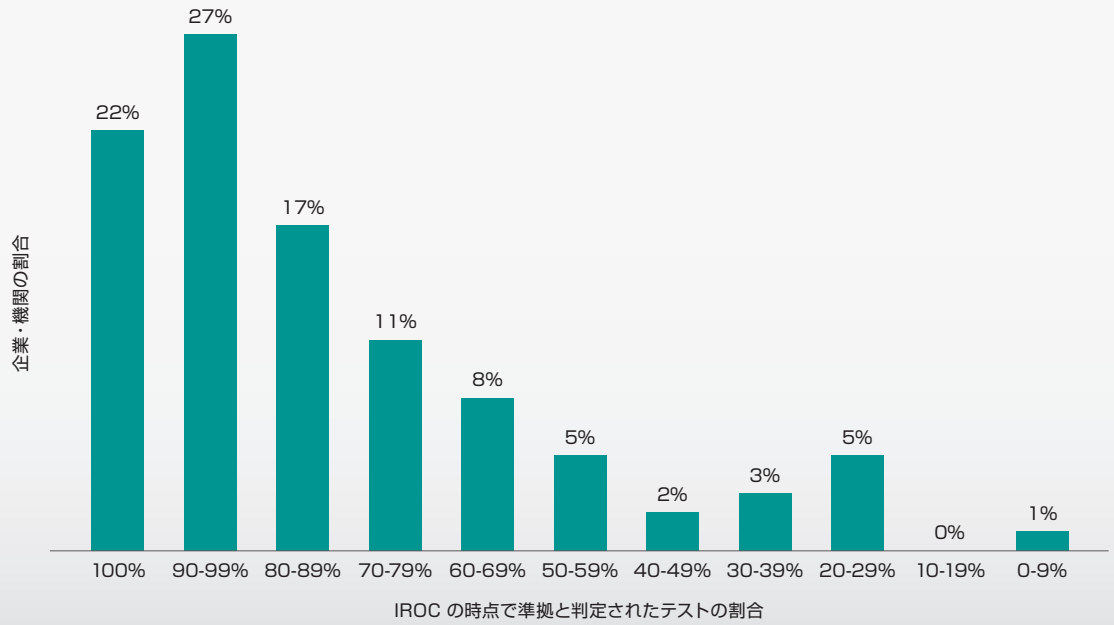
この結果についておそらく最も興味深いのは、IROC の時点で検証により準拠していると判定された企業・機関は、残りの3四半期は準拠していなくても、検証プロセスにおいては準拠しているという判定を少なくともある程度は期待していたということです。この点を検討することは特に重要です。というのは、IROC の時点で検証により準拠していると判定された企業・機関の大半は、コンプライアンスプロセスを初めて経験するのではなく、多くは前回の評価中に検証により PCI DSS に準拠していると判定されていたからです。では、残りの多くの企業が毎年コンプライアンスを維持するのに苦労しているという事実をどのように解釈すべきでしょうか。基準が過度に多くを要求しているのか、それとも過度にあいまいなのでしょうか。検証プロセスがあまりにも困難であるかまたは一貫性がないのでしょうか。IROC の時点で検証により準拠していると判定されなかった企業・機関は、単に準備不足だったのか、あるいは間違った情報に基づいて対処していたのでしょうか。こうした疑問に対する回答は、当然ながら 1 つではなく、単純なものでもありません。こうした結果の背後にあるそれぞれさまざまな理由があり、それらの一部または全部が有効か、あるいはそのすべてが無効であると考えられます。決定的な回答が存在しない (および、決定的な回答を期待しない) が、それでもより深く理解したいと望むのであれば、IROC の時点で検証により準拠していると判定されなかった企業・機関の非準拠の実態を調査することが役立ちます。言い換えると、そうした企業・機関は目標をわずかに外したのか、それとも大きく外したのでしょうか。

弊社の調査結果によれば、平均すると、クライアントは IROC の時点でPCI DSSにおいて定められたすべてのテスト手順の 81% で準拠と判定されていました[2]。この結果には、2 つの見方があります。テストを受けた (あるいは現在受けている) 側とすれば、平均を上回る準拠率として自慢できると思うかもしれません。直前に詰め込み勉強した末に実現したのであれば、特にそう思うことでしょう。その一方で、企業・機関は、PCI DSS に準拠していると判定されることが基準に 100% 準拠することであると理解しています。準拠と判定されるものと期待していたにもかかわらず、検証プロセスを開始した企業・機関はテスト手順の 5 件に 1 件が準拠と判定されませんでした。PCI DSS 要件とセキュリティ評価手順に約 250 件 (数え方によって異なります) のテスト手順が定められていることを考えると、1 つの企業・機関で準拠と判定されなかったテスト手順が約 50 件存在することになります。これは小さな数字ではありません。

2 PCI DSS の構造に詳しくない読者のために説明すると、 12 の主要な要件にそれぞれ複数のサブ要件があります。このそれぞれについて、セキュリティ・アセスメントプロセスは QSA による検証の対象とすべきものを指定する 1 件以上のテスト手順 (弊社では「テスト」と呼ぶ場合があります) を定めています。このテストは、評価中に「実施されている」または「実施されていない」と実際にマークされた測定項目のユニットです。

平均を示すだけではその前後のばらつきを示すことができないため、図 3 はサンプルに含まれる企業･機関が準拠と判定されたテスト手順の割合の分布図を示しています。前述したように、 22% が 企業･機関の予想通り100% 準拠と判定され (すなわち「優等生」)、 27% が 90% 以上などとなっています。この分布が右に偏っているという事実は、良い兆候です。企業･機関の 4 分の 3 がテスト手順の少なくとも 70% で準拠と判定されたということは、あと少し努力していれば適切なタイミングで検証をクリアできたことを意味します。準拠と判定されたテストが半数以下だったのは、約 10% にすぎません。こうした事実はすべて、通信ネットワークの「ラストマイル(交換局と一般家庭を結ぶ通信手段)」に相当する問題がPCI DSS にも存在していることを示唆しています。その原因が、最後の 20% のテスト手順が最も準拠が困難なコントロールに相当するからなのか、それとも企業･機関が最もメリットが大きいと感じる過半数のコントロールに集中しているからなのかは不明です。

図3：IROC の時点で準拠と判定されたテスト手順の分布



企業･機関のコンプライアンスをめぐる上記の統計からは、いくつかの推論を導き出すことができます。何よりもまず、PCI DSS は一般的なセキュリティプログラムにすでに内在する単純で容易な管理策のグループであるとは言えません。大半の企業･機関は、検証によって準拠と判定されるために、それまで実施していなかった (あるいは、維持していなかった) ことを実施 (または維持) しなければなりません。ここで、それらを実施することが正しいことであるか否かは別の問題であり、それについては、後で本報告書の「調査対応データの分析」の項で取り上げます。

さらに、上記の発見事項は基準に対する外部からの検証の重要性を実証しています。大半の企業は、セキュリティプラクティスの状態を評価するときに自信過剰であるように見受けられます。データは、セキュリティプラクティスの大部分が時間の経過とともに陳腐化することや、コンプライアンスに対する継続的なアプローチの維持が不可欠であることを示唆しています。

次に、企業･機関は独力で PCI DSS 要件に準拠、あるいは、準拠の状態を継続的に維持しているのではないため、セキュリティプログラムの成熟度による企業･機関のリスク許容度が、ベースラインとして要求されるリスク許容度 (DSS の特性によって示されるリスク許容度) を上回ると推定することができます。このリスク許容度の差異を解消するためには、変更の必要性に関するコミュニケーションを上級管理職 (支持を求めるため) と残りの従業員層 (ポリシーの表現として) の双方に対して行う必要があります。

最後に、調査対象の企業・機関のコンプライアンスプログラムに関して、それらの企業・機関の 80% が準拠する必要のある項目の 20% で一貫して準拠と判定されていないという事実は、以下の状況のどれか 1 つを示唆しています。

- 準拠と判定されなかった項目を準拠する必要のある項目として認識していなかった。
- 準拠と判定されなかった項目を準拠する必要のある項目として認識していたが、実施済みであると思い込んでいた。
- 準拠と判定されなかった項目を準拠する必要のある項目として認識していたが、代替管理策を実施済みであると思い込んでいた。
- 準拠と判定されなかった項目を準拠する必要のある項目として認識していたが、実施していないことが検証プロセスで明らかになるとは思っていなかった
- 準拠と判定されなかった項目を認識しており、したがって IROC が発行される時点で準拠と判定されるとは実際に予想していなかった。

これらの推論のすべてが、該当する企業・機関の内部にさまざまな問題が潜んでいることをうかがわせます。それらの問題に対応するには、さまざまなソリューションが必要であることもうかがえます。準拠 (または検証) に関する各企業・機関特有のスタンスや課題を理解することも、重要な作業です。その点に関して追加的な支援を提供するために、弊社では PCI DSS において定められている 12 の要件の準拠状況をさらに詳しく調べています。

PCI DSS 要件別の評価結果

ここまでの部分で、企業・機関の過半数が初期評価において 100% のコンプライアンスという目標を達成していないことを明らかにしました。達成していない企業・機関が、どれほど的を外していたかについても取り上げました。この情報は概要のレベルで十分に興味深いものですが、詳細を追加することによってさらに価値が高くなり、それに基づいて行動することが可能になります。特に、企業・機関がすぐに準拠を達成できた要件と、達成が困難であることが判明した要件は何でしょうか。この質問には、12 の要件それぞれについて検証によって準拠と判定された企業・機関の割合を特定するか、または各要件について定められたテスト手順 (テスト) のうち IROC の時点で準拠と判定されたテスト手順の割合の平均を特定するという 2 つのアプローチが可能です。表 1 は、この 2 種類の手法による統計を両方とも描き出しています[3]。

表 1 からは、大半の企業・機関にとって要件 4 (データ伝送時の暗号化)、要件 5 (アンチウィルスソフトウェア)、要件 7 (論理アクセス)、要件 9 (物理アクセス) の準拠が他の要件ほど困難ではないことをかなり容易に推測できます。これは意外なことではありません。要件 7 (論理アクセス) の「業務上必要な範囲」の正確な意味についてある程度の解釈と説得の余地があることを忘れなければ、なおさらです。企業・機関は、カード会員データを保護するために必要な範囲をはるかに超える物理セキュリティ管理策 (要件 9) の実施を経験しています。トラフィックの暗号化 (要件 4) は、インターネットの興隆とともによく知られるようになり、アンチウェイルスソフトウェアを最新の状態に維持する (要件 5) のはサブスクリプション料金の支払いと自動更新機能の実行というよく知られた定型作業になっています。

達成が難しい要件では、要件 3 (保存されたデータ)、要件 10 (追跡と監視)、要件 11 (定期的なテスト) の準拠率が低いことが判明しています。これも、多くのセキュリティプロフェッショナルに衝撃を与える結果であるとは思えません。レガシーシステム、データ追跡の課題、キー管理の課題などを考えると、保存されるカード会員データの保護 (要件 3) は厄介です。定期的なテスト (要件 11) と監視 (要件 10) はセキュリティのさまざまな側面のなかで最も重要でありながら過小評価され、最も理解されていません。さらに、こうした活動に必要な諸経費と労力も、コンプライアンスを難しくしています。

こうした結果は要求の内容の困難さよりも件数の多さに関係があると考える読者もいるかもしれません。別の言い方をすれば、12 の要件の間で準拠率にばらつきがあるのは、各要件によって定義されているテスト手順の数が 1 つの要因となっているのではないでしょうか。単純な作業量指向の関係を評価するために、弊社は各要件のテスト手順の合計数と表 1 に示した 2 つの列のデータとの相関関係を計算しました。テストの数と準拠と判定したテストの割合の間にはほとんど関係がない (r= -.025) 一方で、テストの数と各要件に準拠していた企業・機関の割合には合理的に強い負の関係がありました (r= -0.61)。これは、指定されているテスト手順が多い要件ほど、準拠と判定される可能性が低くなることを意味しています。それは当然です。

3 注：表 1 には、IROC の時点で検証により準拠していると判定された 22% の企業・機関のデータが含まれています。

表 1：PCI DSS 要件別の IROC の時点での評価結果

PCI DSS 要件	企業・機関の割合 (%)*	テストの割合 (%)**
1: カード会員データを保護するために、ファイアウォールをインストールして構成を維持する	46%	82%
2: システムパスワードおよびその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値を使用しない	48%	77%
3: 保存されるカード会員データを保護する	43%	75%
4: オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する	**63%**	83%
5: アンチウィルスソフトウェアを使用し、定期的に更新する	**70%**	**86%**
6: 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	48%	83%
7: カード会員データへのアクセスを、業務上必要な範囲内に制限する	**69%**	**87%**
8: コンピュータにアクセスできる各ユーザーに一意の ID を割り当てる	44%	82%
9: カード会員データへの物理アクセスを制限する	59%	**91%**
10: ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する	39%	75%
11: セキュリティシステムおよびプロセスを定期的にテストする	38%	70%
12: 情報セキュリティポリシーを整備する	44%	83%

3 つの最も低い値を赤で、最も高い値を太字で表記してあります。

* 言い換えると、企業・機関の 46% はIROC の時点で要件 1 に完全に準拠していました。
** 言い換えると、企業・機関は IROC の時点で要件 1 が定めるテストの平均 82% で準拠と判定されていました。

しかし、要件 11 にはこの傾向への強い反発が見られ、そのことがさらにこの要件の準拠に伴う困難を浮き彫りにしています (要件 11 は相対的にテストの数が少なく、準拠と判定された企業・機関の割合が低いため)。

相関関係に注目して表 1 の列を比較すると、他にもいくつか興味深い事実が明らかになります。関係の大部分は予想通りであり、ある要件に準拠している企業・機関の割合とその要件に関して準拠と判定されたテストの割合の間には強い相関関係 (r=.742) が存在します。しかし、このセットにおいて最も興味深いデータは、相関関係が見られない項目です。要件 12 (セキュリティポリシー) と要件 8 (一意の ID) はデータの差が最も大きく、他にも同様の不一致が見られる要件がいくつかあります。この事実は、これらの要件に定められている少数のテストが、多くの企業・機関にとってその要件全体の準拠に対する障害となっていることを示唆しています。

各要件を詳細に分析する前に、こうした分析結果を検討するために不可欠な大局的な所見を最後に 1 つ紹介します。大半のビジネスプロセスと同様に、セキュリティは繰り返し実施される「計画-実行-評価-改善」 (PDCA) サイクルとみなすことができます。計画フェーズは、リスクの評価とリスク許容度の設定、設定されたリスク許容度を反映するポリシー、手順、プログラムの作成と更新、およびそれ以外に企業・機関がセキュリティに関して何をしたいと考えているかを特定する作業から構成されます。それが終わったら、企業・機関は計画を実際の業務慣行 (プラクティス) に変える作業を実行 (実施) します。次に、賢明な企業・

機関はそうしたプラクティスが順調に計画に従って実施され、想定された機能を正しく果たしていることを確認（検証）します。この確認が行われない場合（多くの場合は行われていません）、計画とプラクティスのずれを修正し計画を正しく実施するためにさまざまな措置が必要になります。PCI DSS に関しては、計画-実行-評価-改善の各フェーズを次のように考えることができます。

- **計画：**要件12
- **実行：**要件 1、2、3、4、5、6、7、8、9
- **評価：**要件 10、 11（ただし要件 1-9 にも「評価」が含まれる）
- **改善：**必要に応じてすべての要件、特に「実行」フェーズに記載されたもの

この内訳を表 1 を踏まえて検討すると、重要なことが 1 つ明らかになります。それは、「企業・機関は評価よりも計画と実行に優れている」という事実です。評価は改善の前提条件であるため、そのことを理解するのは重要です。評価フェーズが破綻している場合、企業・機関はイベントに対応できず、不備を修正できず、時間の経過とともにセキュリティプラクティスの状態を維持できなくなります。弊社が『データ漏洩/侵害調査報告書（DBIR）』において毎年指摘しているように、データ（特にカード会員データの）漏洩/侵害の大多数は、計画されたことが実践されなかったことに帰着します。ほぼすべての事例で、適切な評価が実施されていれば、こうした事態が発見され（多額の費用を要することなく）修正されたはずです。

企業・機関は評価よりも計画と実行に優れています。評価フェーズが破綻している場合、企業・機関は時間の経過とともにセキュリティプラクティスの状態を維持できなくなります。

PCI DSS 要件別の詳細な評価結果

前項で説明した全体像を念頭に置いたまま、PCI DSS 要件をさらに詳細に調べることによって初期評価結果の分析を続けます。各要件には、検証によって準拠と判定されるために準拠しなければならないさまざまなサブ要件とテスト手順が指定されています。以下において、企業・機関による準拠の実現に大きなプラスの影響またはマイナスの影響を与えた具体的な項目に特に注意しながら、12 の要件を評価します。また、該当しないことが多いサブ要件や代替管理策によって満たされることが多いサブ要件を特定します。

要件 1（ファイアウォールの構成）

企業・機関の約 46% は初期評価で要件 1 を満たしており、平均すると関連テスト手順の 82% で準拠と判定されていました。ファイアウォールはセキュリティプロフェッショナルにとって標準的なセキュリティ対策ですが、たえずチェックしていなければ急増する可能性があり、ファイアウォール規則セットが増える一方なのはとてもよくあることです。

この分野の最も困難なテストでは、ファイアウォール規則セットが少なくとも 6 カ月に 1 回レビューされていることを確認します（サブ要件 1.1.6）。さらに具体的には、ファイアウォールとルーターに関する規定をレビューするプラクティスと、レビューが行われたことを裏付け、文書で提示することに一貫性がなかったのです。同じことは、セキュアでないサービス、プロトコル、FTP または TELNET などのポートに関する文書と業務上の正当性を対象とする管理策 1.1.5b にもあてはまります。書類作成作業が十分に機能していないことが多いものの、少なくとも実際のトラフィックは十分に制限されているというのが現状のようです。その理由のひとつは、ファイアウォールの規定を管理するために使われているツールに原因があると弊社では考えています。グラフィカルユーザーインターフェイス（GUI）を表現するツールは、一般的に規則と変更を記録する機能をより多く（およびより使いやすいかたちで）備えています。詳細なコメントを作成できる数少ないテキストベースの管理インターフェイスは、ファイアウォールの外側に文書を保持する必要が生じます。

加えて、インバウンドおよびアウトバウンドのトラフィックに関するテスト手順によって判定された準拠率は、企業・機関によって差がありました。結果を見ると、企業・機関は、インバウンドトラフィックの制限は、十分、合理的に実施していますが、アウトバウンドトラフィックの規則となるとかなり寛容です（すべてのデスクトップに SSH、FTP、Telnet to ANY を許可するなど）。出口フィルタリングはしばらく前から使用されていますが、企業・機関は、アウトバウンドアクセスを制限するときに、予想されるビジネス生産性の向上と低下のバランスの確保に苦慮しているように見受けられます。

要件 2 (ベンダーのデフォルト値を使用しない)

デフォルトのパスワード、設定、構成は、たやすく攻撃できることからハッカーにとって共通の攻撃ポイントになっています。初期評価で要件 2 に準拠していた企業・機関が 48% であったことからもわかるように、多くの企業・機関はそうした攻撃を排除するのが困難です。ベライゾン ビジネスのクライアントが要件 2 のテストによって準拠と判定されなかった理由は、大きく 3 つあります。第1 に、不要なサービスの無効化 (サブ要件 2.2.2) と不要な機能の無効化 (サブ要件2.2.4) によるシステムの十分な強化が実施されていませんでした。第 2 に、特定のサービスと機能をビジネス上の理由により削除できない経緯について (サブ要件 2.2.2 とサブ要件 2.2.4 によって要求されている) 文書化を行っていませんでした。第 3 に、すべての非コンソール管理トラフィックを暗号化していませんでした (サブ要件 2.3)。

サブ要件 2.3 に関しては、問題の多くは今も本稼働中のレガシーシステムとレガシー設備に関連しています。例えば、多くの企業は (新しいデバイスの一部は SSH をサポートしているにもかかわらず) 古いネットワーク機器のために TELNET を使い続けています。これは、企業・機関全体で同じ管理方法を使用する方が運用上容易であることを多くの企業・機関が知っているからです。加えて、一部のレガシーシステムは、管理のために端末エミュレーションセッションを利用していますが、これは暗号化されていません。サブ要件 2.3 は、レガシーシステムや旧来の運用方法を刷新するためには多額の費用が必要であるため、代替管理策によって準拠と判定される例が最も多いサブ要件の 1 つです。

要件 2 には、弊社のサンプルに含まれる企業・機関に関して「該当せず」と言及されることが多い 2 つのサブ要件があります。1 つは、無線ネットワークの構成を対象とするサブ要件 2.1.1 です。環境内に無線ネットワークが存在しない場合は、このサブ要件を気にする必要はありません。同様に、共有ホスティングプロバイダーではない場合は、サブ要件 2.4 について心配する必要はありません。

要件 3 (保存されるカード会員データの保護)

ペイメントカードデータの処理と伝送を行う企業・機関の多くは、データの保存も行っています。そうしたデータストアはハッカーの主な標的であり、したがって要件3 によって定義されている特定の保護を必要とします。しかし、経験豊富なセキュリティプロフェッショナルは、保存されているデータのための強力な暗号化プログラムを作成するのは容易ではないことを知っており、弊社の評価結果はそれを裏付けています。要件 3 に準拠していた企業・機関はわずか43% であり (12 の要件のうち最も準拠率が低いグループ)、要件 3 において定められているテストの 75% で準拠と判定されていました (これも最も準拠率が低いグループ)。

明るい面を挙げれば、90% を超える企業・機関が、認証およびトラックデータまたはカード確認コードを保存しないことによって、重要性の高いサブ要件の 1 つであるサブ要件 3.2 に準拠していました。あまり明るくない面を挙げれば、要件 3 に関して求められる基準に達していない要素があまりにも多いため、いくつかに絞り込むのは困難です (30 件以上のテストの 3 分の 1 以上は、準拠と判定された企業・機関の割合が 70%を下回っていました)。問題の大半は、強力な暗号化技術の使用 (サブ要件 3.4) とキー管理 (サブ要件3.6) という2つの重要な要素に関するものでした。

サブ要件 3.4 は、 ハッシュ、トランケーション、インデックストークン、または強力な暗号技術を用いて、少なくともプライマリアカウント番号 (PAN) を読み取り不可能にすることを義務付けています。トラブルの大半は PAN の暗号化に集中しているため、その点に注目して説明を続けます。PAN の暗号化に使用される手段そのもの (複数の選択肢があります) は、その結果 (暗号化されたデータ) ほど重要ではありません。PAN の暗号化に特有の難しさを理解するためのカギの 1 つは、ペイメントカードデータのさまざまな保存形式を思い出すことにあります。データベースエントリ、デジタル画像、フラットファイル、音声録音、バッチ決済ファイルはほんの一部です。企業・機関はネイティブデータベース暗号化ツールまたはサードパーティツールを使用してそのエントリを暗号化することを選択するかもしれませんが、1 台のファイルサーバー上の共通アクセスフォルダーに保存された頻繁にアクセスされるフラットファイルを暗号化しようとすると問題が大きくなります。代わりにファイルレベルの暗号化を利用しようとする人もいますが、これはミッドレンジシステムやメインフレームシステムでは必ずしも選択肢の 1 つではありません。カスタムビルドの支払いアプリケーション (それぞれが個別のデータストアを持つ) が使われている場合は、複雑性とコストがさらに高くなります。上記とその他のすべての理由から、サブ要件 3.4.a とサブ要件 3.4.b はPCI DSS の他のどのテストよりも代替管理策による準拠が多くなっています。

要件 3 のもう 1 つの大きな障害は、キー管理と定期的な変更に関するものです。Adi Shamir (RSA 暗号の「S」の由来となった開発者) の第 3 の法則は、「暗号化は破られるよりも無視されることが多い」ことを私たちに告げています。キー管理が適切に行われていない場合は、その不適切なキー管理がセキュリティ侵害の原因であることが少なくありません。サブ要件 3.6 に定められたすべてのテストで準拠と判定された企業・機関の割合が低く、特にサブ要件 3.6.3、サブ要件3.6.4、サブ要

件3.6.5は 70% を下回りました。サブ要件 3.6.4 (なかでも最も実施率が低かったもの) は、暗号化キーを少なくとも年 1 回変更することを義務付けています。この場合の課題は、強力な暗号化に関する課題と同様です。例えば、ハードウェアセキュリティモジュール (HSM) はデータベースのカラムの暗号化が比較的容易であり、1 レコードごとにキーを変更することができます。キーの定期的な変更には完全な抽出、復号化、新しいキーによる再暗号化が実際に必要になるため、この同じ機能をフラットファイルまたはトランザクションログに移植するのはかなり困難です。加えて、正式なキー保管形式とサインオフ手順が一般的なプラクティスではないため、ドキュメンテーションはサブ要件 3.6.8 に関する問題があることを裏付けています。

要件 3 には、弊社のサンプルにおいて一般に「該当せず」と評価された分野が 2 つありました。その 1 つであるサブ要件 3.6b (キー管理プロセス) は、サービスプロバイダーのみを対象としているため、容易に説明がつきます。もう 1 つは、ディスク全体の暗号化が実施されているか否かをテストするサブ要件 3.4.1 です。ペイメントカード番号の取得とリアルタイム検索に依存するビジネスモデルを主な理由として、多くの場合はディスク全体の暗号化よりも迅速に実施できる選択肢が好まれます。

要件 4 (データ伝送時の暗号化)

多くのエンドユーザーは、これがセンシティブなトランザクションの最も重要なセキュリティ要素であると考えています。データ伝送を暗号化するプラクティスは、セキュリティに関する不安を軽減しながら IT の利用を奨励するために IT プロフェッショナルによって主に導入されました。パブリックインターネットに暗号化されたデータ伝送が必要か否かは疑わしいものの、過去の重大なセキュリティ侵害が示しているように、データ伝送時には送信側と受信側の双方で危険な状態になる可能性があります。企業・機関のほぼ 3 分の 2 は初回評価の時点でこのことを正しく理解しており、それに対応して、テストが示す準拠率は 83% と高くなっています。

すべての企業・機関が無線ネットワークを利用しているのではないため、サブ要件 4.1.1 はつねに「該当せず」のリストに含まれています。無線ネットワークを使用している企業・機関については、Wired Equivalent Privacy (WEP) の使用禁止に向けた適用猶予期限 (2010年6月) が経過したために、サブ要件 4.1.1 に準拠している企業・機関の割合が今後減少すると考えられます。

他に比較すると、サブ要件 4.2 はかなり頻繁に見落とされています。サブ要件 4.2 は、暗号化されていない支払いアカウント番号 (PAN) をエンドユーザーメッセージング技術を使用して送信することを禁止しています。企業・機関は、セキュリティの懸念に実際に対処しないまま電子メール経由でペイメントカードのデータを送信することが少なくありません (e-fax、カスタマーサービス担当者、会計担当者など)。電子メール (特に社内から社内あてのもの) は、多くの場合私的なものとみなされ、センシティブなデータの保護に関する情報セキュリティチームの検査から除外されます。

要件 5 (アンチウィルスソフトウェア)

70% の企業・機関が準拠と判定され、アンチウィルスソフトウェアのインストールと更新は12 の要件のうち初期評価において準拠率が最も高い要件でした。準拠と判定されたテスト手順の割合に関しても、ほぼトップに近い数字です (86%)。それでも、これらの数字はアンチソフトウェアの実装に関する業界調査においてしばしば報告される 90% 台という高い水準を下回っています。しかし以前の調査によれば、アンチウィルスソフトウェアに関する具体的なプラクティスの質を分析する (例えば単にアンチウィルスソフトウェアを使用しているかと質問するのではなく) と、本報告書に示す結果に似た低い採用率であることが明らかになっています[4]。いずれにせよ、アンチウィルスソフトウェアが現在のペイメントカード業界において最も一般的に使用されているセキュリティソリューションの 1 つであることはほとんど疑問の余地がありません。

アンチウィルスソフトウェア (およびその他のアンチウィルス管理策) が幅広く採用されている理由の少なくとも一部は、一連の大規模かつ広範に宣伝された2000年代初頭のマルウェア大発生 (ILOVEYOU、Code Red、Nimda、SQL Slammer、Blaster など) にあります。加えて、企業の業務に十分に対応できる最新のアンチウィルスソリューションは、ほとんどターンキー式のオペレーションになっています。こうしたソリューションに不備がないと言うつもりはありません。マルウェアの変種、カスタム化、パッキングツールが劇的に増加しているため、シグネチャベースのツールの妥当性に関する最近の疑問について激しい議論が続いています。

要件 6 (開発と保守)

要件 6 の領域に含まれる要素をすべて考えると、企業・機関のほぼ半数が IROC の時点で要件 6 に準拠していると判定されたことはまったく驚くべき事実です。(それ以上でないならば) 同じように意外だったのはすべてのテスト手順で準拠と判定され

4 Baker, W. および Wallace, L. 『Is Information Security Under Control? Investigating Quality in Information Security Management.』 IEEE Security and Privacy 第 5 巻第 1 号 36-44 ページ (2007年)。

た企業･機関の割合が 83% であったことです。この事実は、問題の大半を引き起こしている少数の厄介なサブ要件の存在を示唆しています。企業･機関は、脆弱性の特定 (サブ要件 6.2)、従来型の開発 (サブ要件6.3)、変更管理 (サブ要件6.4) には比較的成功しているように見受けられます。しかし、パッチ適用 (サブ要件6.1) とアプリケーション開発 (サブ要件6.5) には準拠できていません。

サブ要件 6.1 に関しては、月 1 回のパッチ適用は一般的なプラクティスではないことがわかっています。多くの企業･機関は、さまざまな理由から四半期に 1 回のパッチ適用スケジュールを維持しています。リスク管理の観点からは、四半期に 1 回のパッチ適用に対する月 1 回のパッチ適用のメリットは大半の状況においてごくわずかですが、それでも四半期に 1 回の場合は多額の追加コストが発生する可能性があります。テストされていないかまたは急いで展開したパッチに関係する自ら招いたサービス拒否インシデントの規則的な発生も、防ぐことができます。企業･機関は時には「テスト段階にある」ものを敬遠することがあり、パッチ適用は多くの人が「現在の状態」でよいと感じている分野の 1 つです。最後に、アプリケーションとネットワーク機器は障害/修正の状況かまたは重要なアップグレードの時だけパッチ適用されることが少なくありません。それを考えると、サブ要件 6.1 が代替管理策に委ねられることが最も多いサブ要件の 1 つである理由が理解できます。

弊社のサンプルに含まれる企業･機関にとってもう 1 つ問題のあるスポットは、安全なウェブアプリケーションの開発 (サブ要件 6.5) です。ウェブアプリケーションの複雑性、公開性、性質、役割によって、この作業は本質的に困難な作業になっています。どれほど課題が大きいのであっても、関連する攻撃に関する大量のデータは、必要な行動への動機付けとなるには十分なほど気がかりなものです。こうしたトレンドを理由の一部として、一部の企業･機関は代わりに開発をアウトソースする選択を行うことが予想されます(その結果、サブ要件 6.5 に関して「該当せず」という回答の数が増える)。

要件 7 (論理アクセス)

率直に言って、アクセスを業務上必要な範囲に制限する要件 7 が 12 の要件のうち2番めに高い準拠率 (企業･機関の 69%、テストの 87%) であったことは、 PCI DSS 評価よりもセキュリティ侵害の調査に精通している者にとっては予想外でした。しかし、チーム内で少し話し合った結果、「見かけは当てにならない」という人生で最も時の試練を経た教訓の 1 つが提起されました。

多くの企業･機関の目標は基準への準拠を実現することであり、したがって多くの企業･機関がその目標への最短距離を選んでいることを思い出してください。

多くの企業･機関の目標は基準への準拠を実現することであり、したがって多くの企業･機関がその目標への最短距離を選んでいることを思い出してください。「業務上必要な範囲」という概念 (および、それよりも重要なことですが、何がそれを構成するのかという判断) は、白か黒かというような二元的な問題ではありません。QSA が要件 7 の準拠状況を評価するときは、アクセス権限が業務上の責任を果たすために真に必要性のある人に実際に限られていることを確認しようと努力します。すべてのシステムに対するすべてのユーザーの権限を詳細に分析する作業に関係するすべての人にとっては途方もないコストが発生するため、この取り組みは、一般に、企業･機関が原則に従っているか否かを確認することと、その証拠を収集することを目指します。ビジネスニーズに基づいて何が必要であるかをすべて知っているのはクライアントだけであるため、目にあまる違反が起きた場合を除いて、(PCI DSSの境界の範囲内で) QSA がこの件について議論するのは多くの場合困難です。

言い換えると、準拠率を押し上げるに足るほどの曖昧性が、「業務上必要な範囲」という概念、PCI DSS 基準、検証プロセスに存在するように思われます。ここで重要なことは (監査するのが困難なこと)、 企業･機関が「これは本当に必要か?」という難しい質問を実際に自問し、その回答が「ノー」であったときに何か対策をとっているかどうかです。

要件 8 (一意の ID)

この要件は一意の ID から認証、パスワード、タイムアウト、ルックアウト、 使用廃止に至るユーザーアカウント管理の多くの要素を対象としているため、「一意の ID」というタイトルはいささか誤解を招くおそれがあります。要件 8 は準拠率に関しては中央集団に含まれますが、環境と状況によっては骨の折れる課題になります。

サブ要件のうち、サブ要件 8.5 (ユーザー認証とパスワード管理) に定義されているものは、比較的準拠率が低くなっています。パスワードの長さ (サブ要件 8.5.10、準拠率 68%) とパスワードの変更 (サブ要件 8.5.9、準拠率 68%) は、なかでも最も準拠率が低くなっています。パスワードの長さや変更に関するサブ要件はユーザーにとってはいらいらさせられるものかもしれませんが、導入と施行は普通は恐ろしく困難なものではありません。おそらく企業･機関は、7 文字のパスワードと 90 日ごとの変更によって、余計な管理負担と使いやすさへの影響を相殺するほど十分なリスク軽減が実現するか否かについて懐疑的な見方をしています。

要件 8 による複数のテスト手順は、代替管理策を通して準拠を実現する割合がPCI DSS のテスト手順のなかでも最も高いものの 1 つです。代替管理策による準拠に関しても、主な原因はサブ要件 8.5 です。その主な理由になっているのは、必要な機能や一元化された管理および認証メカニズムを欠いたレガシーシステム（またはそれ以外）です。一元的に管理されていない場合は、特定のネットワーク機器、UNIX、POS システム上で数百件のローカル個人アカウントを維持する作業は手に負えなくなります。

要件 9 (物理アクセス)

要件 9 によって定義されているテスト手順は、12 の要件のうち準拠と判定された企業・機関の割合が最も高いものでした。PCI DSS 全体のテスト手順のうち、「準拠率上位 10 件」のリストに含まれるものの半数以上が、要件 9 に定められたテスト手順でした。これらのテストは、主にデータセンター、ワイヤレスデバイス、バックアップテープを含む支払いインフラストラクチャに関する物理的な管理策の確認に重点を置いています。

それらのテスト手順の大部分については、予想と一致する高い準拠率でした。多くの企業・機関は、電子データのセキュリティよりも物理セキュリティの方が概念化しやすいと考えています。物理セキュリティはよく知られており、目に見えるものです。物理管理策は、データセンターに関しては以前から強力なものが採用され、一元管理されている物理デバイスやメディアへの適用が比較的容易であり、評価を義務付ける規制や基準が無数に存在するため頻繁に評価されています。さらに、物理管理策は、一般に、複雑性が高く動的なジャンル（ログの監視とレビューなど）が有効性と正しい秩序を維持するために必要とするほど多くの日常的な注意と資金や労力の投入を必要としません。

多数の企業・機関の足をすくった要件 9 の 1 つの項目は、センシティブなエリアへの物理アクセスを監視するビデオカメラその他メカニズムを義務付けるサブ要件 9.1.1です。これはおそらく、設置、設定、3 カ月分のデータを保存できる記憶媒体の容量のコストに関係があります。展開されカード会員環境を対象範囲と定められた後は、企業・機関が準拠状態を維持するのは実際に難しいことではありません。

要件 10 (追跡と監視)

要件 9 の準拠率の高さを論じた際に、その理由の一部は物理的制御の固定的な性質に起因すると考えました。要件 10 は、数千台にもなる可能性がある分散したデバイス全部にわたって複雑でたえず変化する一連の状況をたえず監視する作業を伴うため、多くの意味で要件 9 とは対照的です。さらに、監査の記録と監視は、その意図された目的が (1) 疑わしい活動について警告すること、および (2) フォレンジック調査を円滑化することであるため、多くの場合は報われない作業です。「悪いこと」が起きているのを知らされたり、「悪いこと」について調べたりするのを楽しいと思う人はほとんどいません。それがおそらく初期評価の時点で要件10 に準拠していた企業・機関の割合の低さ (39%) と、準拠と判定されたテスト手順の割合の低さ (75%) のもう 1 つの要因です。

要件 10 の構造を理解すると、この要件が提示している課題を理解する上で役に立ちます。要件 10 のサブ要件は論理的な順序に従って定められ、それぞれ次のサブ要件に依存しています。サブ要件 10.1 とサブ要件 10.2 は、監査ログによって対象範囲内の全システム上でユーザー活動を追跡可能であることを要求し、サブ要件 10.3 はそうした監査ログに記載されていなければならない内容を定めています。サブ要件 10.4 はイベントを再現するためにログの時間を同期することを要求し、サブ要件 10.5 は監査ログを不正な変更から保護するためのさまざまな要素を取り上げています。サブ要件 10.6 に準拠するためには異常に関するレビュープロセスが導入されていなければならず、最後にサブ要件 10.7 は監査ログの保管スケジュールに関するパラメータを定めています。これは簡単なことでしょうか。いいえ、違います。企業・機関は、上記の分野のすべてで苦労する傾向があり、それが最も顕著なのは監査ログの生成 (サブ要件 10.1 およびサブ要件 10.2)、保護 (サブ要件10.5)、レビュー (サブ要件 10.6)、そして苦労の跡が最も目立たないのはアーカイブ (サブ要件 10.7) です。

サブ要件 10.1 とサブ要件 10.2 に準拠するには、ネットワーク全体にわたって、カード会員データにアクセスするユーザーが残す痕跡をすべて記録する必要があります。これらのサブ要件に関する主な問題は、関連する情報資産の途方もない幅の広さと数です。企業・機関は、一般に、ネットワーク機器とオペレーティングシステムに関するログの実装には大きな問題はありませんが、アプリケーションに関してはそれができていません。多数のカスタム構築されたレガシーの支払いアプリケーションがあり、それらは多くの場合PCI DSS に準拠するために必要なログ機能を備えていないからです。そうした状況では、多くの場合、アプリケーションレイヤにおける監査ログの欠如を補正するために、オペレーティングシステムレイヤかデータベースレイヤのいずれかにログを追加する必要があります。当然ですが、企業・機関のすべてのシステムがログをサポートしている場合であっても、ログ機能が有効になっているとは限りません。

監査ログの変更からの保護に関しては、次の2つの要因が影響しています。この 2 つの要因とは、1) 大半の企業・機関の標準的な運用手順は、デフォルトで有効になっているあらゆるログにデフォルト設定/ディスクスペースに応じてローカルな書き込みと上書きを許可していること、および 2) ファイル整合性監視 (FIM) が導入されていないことです。ログがつねに新たなログによって上書きされている (自己変更している) 場合、その企業・機関はサブ要件 10.7 (監査履歴の維持) に準拠しているとは期待できません。この問題は、企業・機関がストレージの制約からログが上書きされる前に古いログを他のメディアへ解放する集中管理型ログソリューションを導入していないときに表面化します。サブ要件 10.5.5、またはファイル整合性監視の要件は複雑性と難易度が高く、導入には多額のコストを必要とします。大半の企業・機関にとっては、動的ログファイルのハッシュが困難であり、そのためサブ要件 10.5.5 については代替管理策を追求しています。

ログの監視とレビューを効果的に実行しようとする際に直面するジレンマは、セキュリティ業界特有かもしれませんが、その根本的な問題は現代社会全体に影響します。利用可能な情報の量は、そこから意味を見つけ出す我々の能力をはるかに超えています。リモートでのログ監視に精通している人でも、この概念は理解しています。人の目だけで監視するのは不可能であるため、ログの解析を自動化するためにさまざまな分析ツールが使用されています。これは確かに大きなメリットがありますが、他のあらゆるツールと同様に、干し草の山から針を探す (または、弊社が『2010年データ漏洩/侵害調査報告書』において推奨しているように、少なくとも干し草の山を見つける) には解析ツールをチューニングしなければなりません。問題がすでに十分に困難なものではないかのように、多くの企業・機関は、支払い環境のコンテキストにおいて必要であるかまたは有用であるものだけを特定し、優先順位付けし、有効化するための時間を確保するのではなく、何もかもすべてを記録することによって、問題を自らさらに困難なものにしています。

たいして苦労せずに何もかもすべて記録できる場合は、それに加えて、生成された大量のログファイルをどこかに保存しなければなりません。サブ要件 10.7 は、企業・機関にフォレンジック調査を支援するため過去 1 年間のログのアーカイブを要求し、そのうち直近 3 カ月分についてはただちに分析できる状態にしておくことを義務付けています。ストレージの価格は日ごとに低下していますが、ログファイルの数とサイズ、それらの維持に伴う運用上の頭の痛い問題によって、ストレージのコスト削減効果が相殺されます。

要件 11 (定期的なテスト)

セキュリティプロフェッショナルの多くは、『ブラインド・サイド アメフトがもたらした奇蹟 (The Blind Side) 』を読んでいないようです。さもなければ、セキュリティに関する職業に付随するありふれた管理策をもっと高く評価しているはずです。この本にはさまざまなサイドストーリーが含まれますが、その 1 つは、アメリカンフットボールの左タックルのポジションについて説明しています。左タックルは、点を取りに行くクォーターバックを守るためのかなりありふれた「管理策」に相当します。フィールドではクォーターバックなどの高得点を獲得する派手なタイプの選手が脚光を浴びるのが普通ですが、実は最も重要性が高く最も高額の報酬が与えられる役割は左タックルです。この本では、なぜそうなっているのかについて説明しています。この本は、おそらく新規採用されたセキュリティスタッフ全員の必読書です。いずれにしても、システムとセキュリティプラクティスの定期的なテストを実施していない企業・機関は、大変な被害を自ら招く運命にあります。要件 11 の初期評価での準拠率が最も低い (企業・機関の 38%) ことと、一般的に準拠と判定されたテスト手順の割合 (70%) を考えると、この分野は被害が発生しやすいように見えます。

要件 11 によるテスト手順の準拠率はどれも見るに堪えない数字ですが、なかでも 49% というおそらく PCI DSS 全体にわたって最も低い実施率であることが判明したのは、サブ要件 11.5 (ファイル整合性監視) です。このサブ要件が骨の折れる課題を突き付けているのは疑問の余地がありません。事実、監査ログのファイル整合性監視 (サブ要件10.5.5) に関する要件 10 の準拠率を考えあわせると、実現するのが最も困難なプラクティスに属します。かつては、この要件は最も重量な資産または高リスク資産を保護するためにのみ必要だと考えられていました。しかし現在では、 PCI DSS によってカード会員データ環境内のすべてのシステムが適用対象とされています。そのため、ファイル整合性管理をネイティブサポートしていないいくつかのレガシーシステムとメインフレームシステム (Tandem、AS400、MS DOS その他) が、このサブ要件 11.5 の対象範囲が含まれるようになりました。こうした事情から、サブ要件 11.5 は代替管理策によって達成される場合があります。

本報告書では、要件 11 の問題が多い分野のすべてを取り上げることはできませんが、準拠率が最も低かった 3 件のサブ要件の残り 2 件はサブ要件 11.3 とサブ要件 11.2 でした。サブ要件 11.3 は、認定資格を保有する内部または外部の当事者によって年 1 回の侵入テストを実施することを定めており、その目的は現行の管理策が熟練した確信犯的な攻撃者を撃退可能であるか否かをチェックすることにあります。例えば、企業・機関はシステムのセッティングを構成し (サブ要件2.2)、正しいセキュリティパッチを適用し (サブ要件6.1)、ウェブアプリケーションの脆弱性のテスト (サブ要件 6.5) を行っているかもしれま

せんが、侵入テストでは、こうしたポイント管理策のすべてを結合して、支払いインフラストラクチャを保護するために連携して機能するかどうかを判断します。一般に、侵入テストを 1 回実施した企業・機関は、再度実施する前に、修正が必要な事項のリストを作成します。侵入テストでは発見できなかった問題のなかには単純な構成を通して対処可能（NTP をオンにするかまたは SSL を有効化する）なものがある一方で、調査と修正に長時間を要するものもあります。例えば、多くのテストツールは、アプリケーションのバナーグラビングを行い、システムが攻撃の影響を受けやすい場合は「最も有力な推測」を判断します。ツールに限界があるため、侵入テストの実施担当者がテスト結果を全面的に検証するのはきわめて困難になりますが、それにもかかわらず厳密な調査をさらに行うことによってテストが行われた資産のセキュリティ特性に悪影響が生じる可能性があります。これは、修正とフォローアップにさらに時間を必要とする多くの誤認例や回答が得られない問題の原因になる可能性があります。この理由から、侵入テスト（および修正作業のきっかけとなるその他のテスト）は検証プロセスの早い段階で実施すべきです。

サブ要件 11.2 には、ネットワーク脆弱性スキャンが含まれ、検証の誤認例に関して侵入テストと同様の問題が存在します。しかし、企業・機関にとって、サブ要件 11.2 に関する主な課題は、ネットワーク脆弱性スキャンを四半期に 1 回実施しなければならないことです。繰り返し実施するプロセス（とそれが実施されたことを裏付ける証拠）を維持することは、弊社のサンプルに含まれる多くの企業・機関にとって困難であることが判明しました。さらに、四半期に 1 回のスキャンを実施していない（または実施した証拠を提示できない）企業・機関は、将来において実施するのがさらに困難であることに気づくはずです。これは、評価機関が多くの場合それ以後さらに厳しいプロセスが実施されていることを示す追加の証拠を要求するからです。

全般的に見て、多くの企業・機関が要件 11 の準拠に苦慮しているのは、それがありふれたことと考えられ、定型作業を必要とするためです。これは、システム。プラクティス、手順を展開するときに最初は熱心に取り組むが展開後は忘れるという多くの企業・機関の自然な傾向に反します。残念なことに、それではセキュリティがうまく機能するとは期待できません。

要件 12（セキュリティポリシー）

初期評価の時点で要件 12 に準拠していた企業・機関の割合は 44% と低い数字でしたが、（平均すると）この要件に定められたテスト手順によって判定された準拠率は 83% という妥当な数字でした。セキュリティポリシーは、通常は作成や検証は困難ではありませんが、真の実効性となると、作成にかけた時間、コスト、労力に見合ったものになります。本当に重要なのは、セキュリティポリシーの内容の質、周知状況、および順守状況です。すでに述べたように、成文化されたポリシーと実際のプラクティスの間には大きな違いがあることも少なくありません。そのため、ポリシーにはほとんど価値がないと考える人もいますが、そうした考え方は「赤ん坊をおふろの水と一緒に捨てる」という慣用句と同じように疑わしく聞こえます。

要件 12 に定められた大半のテストは高い準拠率を示していますが、改善の機会がいくつかあります。サブ要件 12.9 の「インシデント対応計画の実施」はそうした機会の 1 つであり、その範囲内には最も多くの作業を必要とする 2 つの項目（サブ要件12.9.2 とサブ要件 12.9.4）があります。1件めの サブ要件 12.9.2 は、インシデント対応計画のドキュメンテーションについて定めており、（とても意外ですが）多くの企業・機関がインシデント対応計画を作成していると思われる一方で、その更新またはレビューはまれにしか行われていません。企業・機関はインシデント発生時の役割と責任についてインシデント対応担当者に適切なトレーニングを行う（サブ要件12.9.4）ことができていないため、それが、2つめの障害になっています。この 2 つのサブ要件がなぜともに支障をもたらすのかについて説明することは可能ですが、それは先日発行した『2010年データ漏洩/侵害報告書』の「発見から封じ込め（拡大防止）まで」の項（47 ページ）で多数の図表を用いて説明しています。こうした基本的なことを忘れてはなりません。

PCI DSS マイルストーン分析

PCI DSS の準拠状況を分析するもう 1 つの方法では、PCI セキュリティ基準審議会が「ステークホルダーが準拠プロセスの早い段階においてリスクを軽減するために行動できる分野を理解できるよう支援する[5]」ために開発した『PCI DSS 優先アプローチ (Prioritized Approach)』の観点から分析を行います。このアプローチは、順序付けされた6 つのマイルストーンを中心として活動のロードマップを定義しており、その目的は早い順序のマイルストーンで最も重要なリスクに対処することにあります。これらのマイルストーン（表 2 を参照）は、12 の要件を中心として編成されているのではなく、要件を取り出して 6 つのマイルストーンを中心として編成したものです。『PCI DSS 優先アプローチ』 は比較的新しいため（2009年に作成）、企業・機関が準拠に向けた取り組みをこの 6 つのマイルストーンを中心として順序付けする作業に着手しているかどうかを疑問視する人がいるかもしれません。表 2 は、このトピックに関するデータを提供しています。

5 『PCI DSS 優先アプローチ』（https://www.pcisecuritystandards.org/education/docs/Prioritized_Approach_PCI_DSS_1_2.pdf）を参照

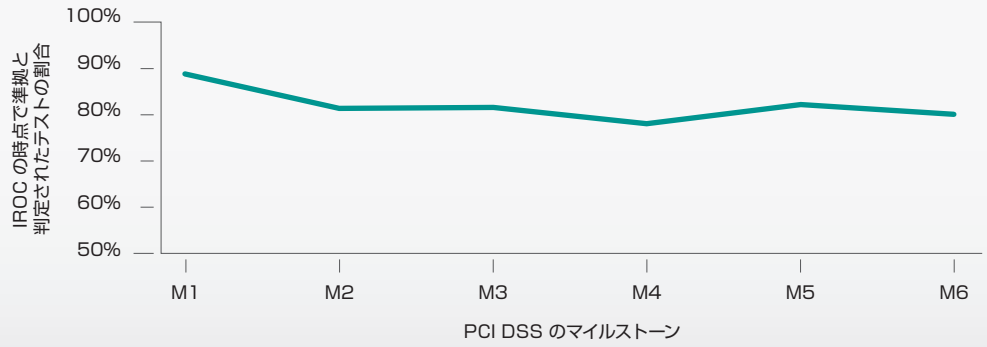
図2：IROC の時点で準拠と判定されたテスト手順の「優先マイルストーン*」別の割合

マイルストーン	目標	実施済み
1	センシティブ認証データを削除し、データの保持を制限する。	88%
2	境界、内部、無線ネットワークを保護する。	81%
3	ペイメントカードアプリケーションを保護する。	81%
4	システムへのアクセスを監視し、制御する。	79%
5	保存されたカード会員データを保護する。	83%
6	残りの準拠への取り組みを完了し、すべての管理策が実施されていることを確認する。	80%

* PCI セキュリティ基準審議会の『PCI DSS 優先アプローチ』に基づく。

検証によって PCI DSS に準拠していると判定されるためには、マイルストーンでの分類とは関係なく、すべてのテスト手順で準拠と判定されなければならないことを忘れてはなりません。とは言うものの、企業・機関が 『PCI DSS 優先アプローチ』を活用すれば、順序の早いマイルストーンについては IROC（ご存知のように不完全である場合が少なくありません）で高い準拠率を期待できます。マイルストーン 1 が最も重要なリスクに最初に対処するという目標を達成しているとすれば、実際に最も高い実施率を示しているのは喜ばしいことです。しかしそれ以降は、残りのマイルストーンは管理策の実施率がほぼ同じになっています。図 4 の比較的フラットな折れ線グラフは、この傾向をよく表しています。

図4：IROC の時点で準拠と判定されたテスト手順の「優先マイルストーン*」別の割合



*. PCI セキュリティ基準審議会の『PCI DSS 優先アプローチ』に基づく。

このグラフによれば、弊社のサンプルに含まれる企業・機関の間では『PCI DSS 優先アプローチ』の普及率が高いようには見受けられません。ただし、弊社のサンプルが 2008 年と 2009 年の評価から構成されていることに留意しなければなりません。『PCI DSS 優先アプローチ』は 2009 年に公表されたため、企業・機関が実施する十分な時間を確保できなかったとしてもまったく不思議ではありません。さらに、弊社では PCI DSS 優先アプローチへ移行した証拠が評価結果に表れるまでにはしばらく時間がかかると予想しています。

調査対応データの分析

ベライゾンは、数年前から調査対応 (IR) チームが実施したフォレンジック業務に関する一連の報告書を発行しています。『データ漏洩/侵害調査報告書』は、企業・機関のデータ漏洩/侵害の 5W1H (誰が、何を、いつ、どこで、どのように、なぜ) を徹底的に調査し、その結果を公開しています。『データ漏洩/侵害調査報告書 (DBIR)』は 6 年間分の漏洩/侵害事件を網羅し、事例数は 900 件以上、被害を受けたレコード数は9億件を超えます。それらのデータ漏洩の多くはペイメントカード情報が関係しているため、この大量のデータセットに基づいて PCI DSS に関する 2 種類の興味深いユニークな分析を行いました。最初の分析では、弊社の QSA が評価した企業・機関を弊社 IR チームが調査したペイメントカードデータ漏洩/侵害の被害者と比較します。2 つめの分析は、過去 2 年間に弊社 IR チームが調査を行った調査対応事例においてカード会員データに被害をもたらした最も重要な脅威アクションを列挙するものです。

表 3: PCI DSS 要件に準拠している企業・機関の割合.IR データはデータ漏洩/侵害発生後のレビューに基づく。PCI データはIROC の時点での QSA による評価に基づく。

PCI DSS 要件	PCI データ	IR データ
1: カード会員データを保護するために、ファイアウォールをインストールして構成を維持する	46%	32%
2: システムパスワードおよびその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値を使用しない	48%	41%
3: 保存されるカード会員データを保護する	43%	19%
4: オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する	**63%**	**77%**
5: アンチウィルスソフトウェアを使用し、定期的に更新する	**70%**	**58%**
6: 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	48%	12%
7: カード会員データへのアクセスを、業務上必要な範囲内に制限する	**69%**	27%
8: コンピュータにアクセスできる各ユーザーに一意の ID を割り当てる	44%	26%
9: カード会員データへの物理アクセスを制限する	59%	**49%**
10: ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する	39%	15%
11: セキュリティシステムおよびプロセスを定期的にテストする	38%	19%
12: 情報セキュリティポリシーを整備する	44%	25%

3 つの最も低い値を赤で、最も高い値を太字で表記してあります。

PCI DSS に懐疑的な見方をする人々に共通する主張の 1 つは、有効性を裏付ける証拠が比較的少ないというものです。

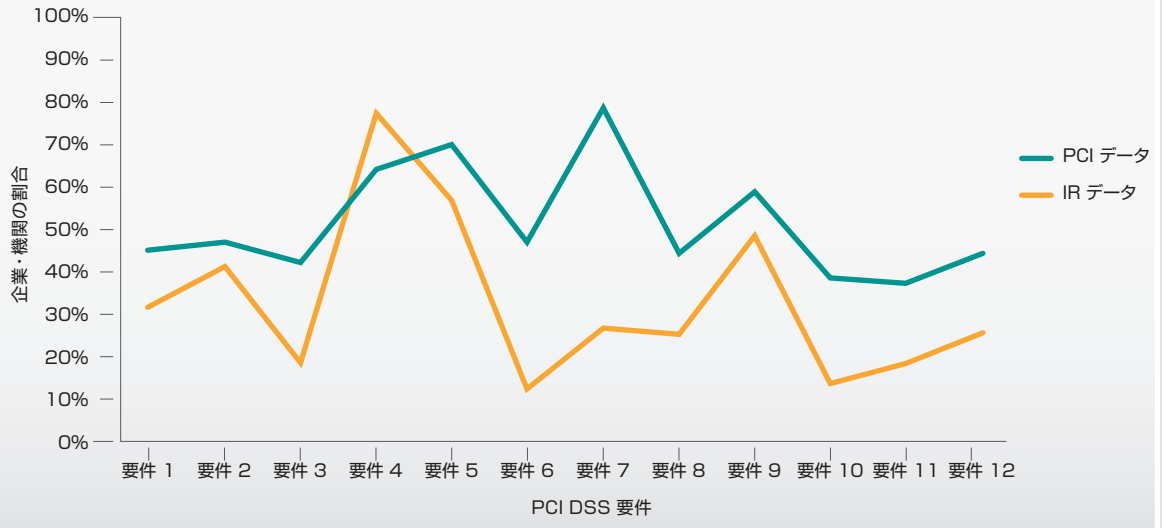
PCI DSS に懐疑的な見方をする人々に共通する主張の 1 つは、有効性を裏付ける証拠が比較的少ないというものです。PCI DSS の準拠状況を調べた結果に基づく調査は少ないため、反対するのは少なくとも理解できます (根拠が真実であるか否かにかかわらず)。PCI DSS に高度に準拠している企業・機関のセキュリティ障害/データ漏洩を準拠していない企業・機関のそれと比較する網羅的で管理された調査が実施されるならば、この論争に決着をつける (あるいは、少なくとも実証的な議論の材料を提供する) 上で大いに役立つことでしょう。

網羅的でも管理されたものでもありませんが、ベライゾンの PCI チームと IR チームが実施した評価に基づいて、PCI DSS への準拠とセキュリティに関する結果の少なくとも一部が知られている企業・機関同士を比較することは可能です。フォレンジック業務では、その頂点において、主任調査スタッフが PCI DSS 要件のレビューを実施し、その結果を関連するペイメントカード会社に伝達します。このレビューは正式な評価ではありませんが、データ漏洩/侵害の被害者の間で不備がある傾向の強い要件に関する知見を得ることができます。

表 3 は、2 つのグループの企業・機関について PCI DSS の準拠結果を示しています。第 1 のグループには、本報告書を通して取り上げている PCI DSS に関する評価の対象となったクライアントが含まれます (表 1のデータを使用)。第 2 のグループは、2008 年から 2009 年にかけて弊社 IR チームが調査した確認済みのデータ漏洩/侵害の被害者である企業・機関から構成されています。

図 5 は表 3 と同じデータを示していますが、メッセージははるかに鮮明です。IR チームのクライアントが PCI DSS 要件に準拠している可能性は、PCI チームのクライアントほど高くはありません。別の言い方をすれば、データ漏洩/侵害の被害者の準拠率は、企業・機関の正常 6 集団を下回っています。これは、要件 4 (データ伝送時の暗号化) を除くすべての要件にあてはまります。次の項で取り上げるように、公共ネットワークを流れるデータの侵害を試みる手法は、弊社が取り扱う事例全体にわたる共通の脅威アクションではありません。IR チームのクライアントと PCI チームのクライアントでは、準拠率が要件ごとに異なりますが、平均すると、PCI チームのクライアントの準拠率はデータ漏洩/侵害の被害を受けた企業・機関を 50 % 上回っています[7]。したがって、この場合「実証」という言葉を使うのは強引ですが、上記の結果は、データ漏洩/侵害を回避したい企業・機関はPCI DSS を完全に避けるのではなく追求する方が良い結果が得られることを示唆しています。

表 5: PCI DSS 要件に準拠している企業・機関の割合IR データはデータ漏洩/侵害発生後のレビューに基づく。
PCI データはIROC の時点での QSA による評価に基づく。



6 「正常」はこの場合は統計上の意味で使用したのではありません。PCI チームのクライアントのグループが、全員 弊社の PCI 評価サービスを利用しているという以外に既知の非定型な特徴が見られない企業・機関に相当するという事実に言及しているにすぎません。

7 これらの結果が IROC を代表していることも考慮すべきです。PCI データセットに含まれる企業・機関の大半は、この結果に示された不備に対応済みであり、最終的に検証により完全に準拠していると判定されました。この点において、IR データセットと PCI データセットの差はさらに大きいと言えます。

最重要脅威アクション

前項までに取り上げた分析はすべて、脆弱性を重視する（または、制御を重視する）ものでした。PCI DSS の最終目的は、一連の要件を定めることだけではなく、カード会員データの漏洩を減らすことであり、したがってリスクを重視する観点はこの調査に関連性があり、有用です。このリスクを重視する観点を取り入れるために、ベライゾンの IR チームが行ったデータ漏洩/侵害調査を利用します。表 4 は、2008 年から2009 年にペイメントカードデータの被害につながった最も重要な 10 件の脅威アクションのリストです。脅威アクションとは、何らかの脅威因子による行為または活動であり、セキュリティインシデントを引き起こし、もしくはセキュリティインシデントの発生に寄与するような行為または活動（攻撃手法）です。VERIS では脅威アクションの 7 つのカテゴリ 8 を確認していますが、上位 10 件のリストに含まれるのはそのうち 3 つだけです（3 件のうちの 1 件は VERIS において 1 回しか言及されていません）。表 4 に示した割合を合計すると 100% を超えますが、これは大半のデータ漏洩/侵害に複数の脅威アクションが関係しているためです。本項の残りの部分では、これらの脅威アクションと、脅威アクションの阻止、回避、検出を可能にする PCI DSS 要件を取り上げます。

VERISについて

表 4 に記載されている脅威アクションは、ベライゾンエンタープライズリスク/インシデントシェアリング（VERIS）フレームワークに基づいています。VERISは、共通言語を使ってセキュリティインシデントに関する情報を記録するためのフレームワークであり、構造化された反復可能な形式で情報を入力することができます。「誰が、何にまたは誰かに。どのようなことをして、結果はどうなったか」という物語風に情報を入力すると一定形式のデータ（『データ漏洩/侵害調査報告書』に記載されているようなデータ）に変換されます。このフレームワークは誰でも無償で利用でき、VERIS コミュニティ wiki 9 からアクセス可能です。

表 4：ベライゾンの IR チームが調査した2008 - 2009 年のペイメントカードデータ漏洩/侵害事例に基づく最重要脅威アクション

カテゴリ	脅威アクション	データ漏洩/侵害件数（%）
マルウェア	バックドア	25%
ハッキング	SQLインジェクション	24%
ハッキング	バックドアまたはコマンド&コントロールチャンネルの不正使用	21%
ハッキング	デフォルトまたは推測可能な認証情報の悪用	21%
不正使用	システムアクセス権/権限の不正使用	17%
ハッキング	盗んだログイン情報の使用	14%
マルウェア	RAMスクレーパー	13%
ハッキング	不十分な認証の悪用	13%
マルウェア	パケットスニファー	13%
マルウェア	キーロガー/スパイウェア	13%

8 VERIS によって定義された 7 つの脅威アクションカテゴリは、マルウェア、ハッキング、ソーシャルエンジニアリング、不正使用、物理的窃盗、エラー、環境です。
9 https://verisframework.wiki.zoho.com

バックドア

表 4 の脅威アクションを詳しく調べるには、脅威アクションをいくつかの論理的なグループに分類し、それらのグループを中心として議論を整理するのが便利です。バックドア（マルウェア）とそれらの悪用（ハッキング）は、いずれも脅威アクションの上位 3 件に数えられ、適切な出発点に相当します[10]。バックドアは、通常の認証メカニズムやその他のセキュリティコントロールを迂回することによって、感染したシステムへのリモートアクセスを提供するツールです。バックドアはいくつもの感染経路または感染媒体を経由してシステムに感染しますが、ベライゾンが調査した事例で最も一般的だったのはリモートの攻撃者が直接インストールまたは注入する手口です。バックドアが設定されている場合、攻撃者はそれを利用して自在にシステムにアクセスし、あらゆる不正な活動を行うことができます。バックドアは、継続してアクセスし、しかも発見されないようにするという犯人の狙いを達成しやすくするため、好んで使われるツールです。被害者の環境からペイメントカードデータをこっそり引き出す手段としても一般的です。

バックドアのインストールと悪用に関連する PCI DSS 要件に関しては、要件 5（アンチウィルスソフトウェア）が該当するのは明らかです。管理策の実施率が最も高い分野の 1 つが最も頻度の高い脅威アクションと関係しているというのは、直観と相いれないように思えます。しかし『データ漏洩/侵害調査報告書（DBIR)』で論じたように、最新のマルウェアは高度にカスタマイズされており（DBIR によれば半数以上)、アンチウィルスソフトウェアを巧みに回避する感染経路や幹線媒体を通してインストールされます。これはアンチウィルスソフトウェアが役に立たないと言っているのではありません。攻撃者がアンチウィルスに適応していることと、他の管理策も同様に必要であることを意味しています。バックドアはシグネチャベースではないため、ファイル整合性監視（要件 11）はバックドアその他のマルウェアに対する効果的な対策として期待されます（「期待される」はこの場合は効力発生文言です。企業・機関はこのことを正しく理解するために苦労しています)。PCI DSS の他の複数の分野も役に立ちますが、要件 1（ファイアウォールの構成）と要件 10（追跡と監視）は特に関連性が高い要件です。残念なことに、それらは実施率が最も低い要件に含まれています。バックドアは通常とは異なるポート、プロトコル、サービスを介してデータが送信されることが多いため、それらを封じるためには入口フィルタリングと出口フィルタリングがとても効果的です。入口フィルタリングと出口フィルタリングは、既知のシグネチャに依存する必要がありません。ネットワークアクセスの監視と(実際に監視している場合は) 記録は、別の防御のレイヤーを提供し、バックドアの存在を示す不審なトラフィックの検出に役立ちます。

現時点までのすべての分析は脆弱性を重視したものですが、
リスクを重視する観点はこの調査に関連性があり、有用です。

SQLインジェクション

バックドアの次に頻度が高い脅威アクション（ペイメントカードデータ漏洩/侵害事例の 24%）は SQL インジェクションです。SQLインジェクションは、ウェブページとバックエンドデータベースとの間の通信を利用する手法です。かなり高度な処理も可能で、ウェブサーバーを介してアプリケーションにSQL文を挿入し、その応答を取得したり別のSQL文を実行したりといった事例も見られます。つまり、ユーザーによる入力をアプリケーションが信頼し、しかもサーバーで入力の検証が行われない場合、SQLインジェクションにさらされる確率が大きくなります。クロスサイトスクリプティングなど、入力検証の脆弱性を利用する攻撃についても同様のことが言えます。データ漏洩/侵害事例の場合、SQLインジェクションの主な目的は、(1) データベースのデータに対する照会、(2) データベースに保存されているデータの修正、(3) システムへのマルウェアの挿入の3つです。SQLインジェクションは柔軟性と実効性が高いため、サイバー犯罪では、いわば多目的ツールとして広く利用されています。

入力検証機能が弱い場合は SQL インジェクション攻撃を受ける可能性が非常に高くなるため、阻止するには要件 6（開発と維持）が不可欠です。安全なアプリケーションを作成するには、アプリケーションが完成するまで待つのではなく、開発サイクルを通してセキュリティの問題を検討することが最も重要です。開発した後は、一定の間隔で定期的にアプリケーションをテストし、管理策が実施され基準を満たしているか確認すべきです（要件 11)。その間ずっとアプリケーションのログ作成機能を有効化し、SQL インジェクション攻撃を発生時または発生直後に特定できるよう監視すべきです（要件 10)。当然ですが、表 3 によって示される多くの企業・機関のように関連する要件をまったく無視する企業・機関では、このすべては役に立ちません。

10 この 2 つの脅威アクションを分けて取り上げるのは奇妙に思われるかもしれませんが、それには理由があります。VERIS では、インシデントを一連の独立しているが関連しているイベントとして分類します。したがって、バックドアを開くマルウェアをシステムに導入するのは、そのバックドアを利用して不正アクセスを取得する脅威因子とは別のイベントであるとみなされています（マルウェアを利用したハッキングはマルウェアに依存しますが、確実に発生するとは限りません)。

認証と権限付与に関する攻撃

次の脅威アクションのグループは、認証 (アクセスしたのは誰か) と権限付与 (どの操作を実行できるか) メカニズムをターゲットとしています。デフォルトまたは推測可能な認証情報の悪用、盗んだログイン情報の使用、不十分な認証の悪用は、カード会員データに対する最も一般的で大きな損害をもたらす攻撃につねに含まれています。多くのシステムやデバイスは、初期設定ができるよう標準的なユーザー名とパスワードが事前設定された状態で出荷されます。これらのユーザー名やパスワードはサイバー犯罪者に広く知られているため (およびそれらは単純なものである例が多いため)、それらを頻繁に変更しない場合は不正アクセスを許す結果になります。販売時点管理 (POS) システムを第三者が管理する宿泊飲食サービス業や小売業では、ユーザー名やパスワードを頻繁に変更していない例が多く見られます。攻撃者が有効なユーザー認証情報を盗み出すことに成功した場合、それに続く行動は、正規のユーザーによるものであるかのように見えるため、さまざまな検出メカニズムを導入していても、悪意のあるものとしてタグ付けされる可能性がはるかに低くなります。さらに、足跡を残さずに企業などのデータを窃取することも容易です。アクセス制御リスト （ACL） は、どのユーザーがどのオブジェクトにアクセスでき、どのような操作を行えるかを定義することを目的としています。ACL などの認証メカニズムが定義されていなかったり、定義されていても脆弱だったり、権限の範囲や設定が不適当だった場合は、リソースにアクセスして不正行為を実施する機会を攻撃者に与えることになります。

こうした脅威アクションを軽減するために、複数の要件が定められています。その 1 つである要件 2 の主な目的は、デフォルトの認証情報や推測可能な認証情報を排除することにあります。企業・機関がセキュリティに関するシステムとプロセスを要件 11 に従って定期的にテストしていれば、見過ごされたものがあったとしても発見され、修正されるはずです。マルウェアは認証情報を盗むためによく使われるため、要件 5 (アンチウィルスソフトウェア) は既知のパスワード窃取用マルウェアの感染予防と検出に役立ちます。制限の厳しいファイアウォール規則とネットワークのセグメンテーション (要件 1) は、不十分な認証をネットワークのレベルで補強し、その一方で業務上必要な範囲にアクセスを制限する (要件 7) 措置はアプリケーションやシステムのレベルで有効です。要件 7に関して PCI チームのクライアントと IR チームのクライアントの準拠率に大きな差がある (表 3 または図 5 を参照) のは、興味深い事実です。セキュリティプロフェッショナルは「付与する権限を最小限に抑える」という考え方を熟知していますが、ビジネス部門からの要求が厳しくなり、複雑性が高くなるにつれて、実際の業務においてその考え方を固守する際の管理上の課題も大きくなります。このことに関してデータ漏洩/侵害の被害者が他の企業・機関よりもはるかに苦戦しているのは明らかであり、見る人の注意を引きます。要件 8 (一意の ID) と要件 10 (記録と監視) は認証および権限付与メカニズムへの攻撃の一部を防止できるかもしれませんが (大部分は依然として正規の活動に見えるものの)、特定の資産に対する特定の行動を特定の因子と結びつけることができるため、説明責任が強化されます。これが、ひいては対応、封じ込め、復旧プロセスに大きく役立ちます。

データ捕捉マルウェア

表 4 にはペイメントカードデータを窃取する手法のうち最も頻度の高いものを掲載しているため、RAM スクレーパー、パケットスニファー、キーロガー/スパイウェア (すべてデータの捕捉を目的としたツール) がリストを構成しているのは意外ではありません。最近の数年間に流行し始めた RAM スクレーパーは、コンピュータ内のメモリ (RAM) のデータを捕捉するという機能を持っています。パケットスニファー (ネットワークスニファーまたはパケットアナライザーとも呼ばれます) は、ネットワーク方を流れるデータを監視し、捕捉するマルウェアであり、サイバー犯罪者の昔からのお気に入りです。最後のキーロガーとスパイウェアは、ユーザーが行う操作の監視と記録を専門に行います。キーロガーは、大規模な攻撃に先立ち、ユーザー名やパスワードの収集に使用されるのが普通です。

一見すると、要件 4 (データ伝送時の暗号化) は幅広く実施され、データ捕捉マルウェアに対する明らかな対策であるように見受けられます。しかし、「公共ネットワーク上で」という重要な違いがあります。これまでに説明したマルウェアは、ネットワーク内のシステム上で機能するものです。内部ネットワークは暗号化される可能性が低く (暗号化は一般的になってきていますが)、パケットスニファーはその事実を利用します。内部のトラフィックをすべて暗号化している企業・機関にとってさえ、キーロガー、スパイウェア、RAM スクレーパーは、システム内で処理されたデータを犯罪者が捕捉できるようにすることによって、防御の弱点を利用します。これは、攻撃者と防御者のイタチごっこと、セキュリティプラクティスが防御の弱点に対する脅威とともに進化しなければならないことを思い起こさせます。

これは、ファイル整合性監視などの要件 11 (定期的なテスト) に含まれる管理策の重要性につながります。データ捕捉マルウェアなどのアプリケーションは、コンピュータの設定を観察し、特定のシステムファイルやアプリケーションファイルを監視します。IDS/IPS の場合と同様に、チューニングにはある程度の労力が必要であり、誤認例が多いために多くの人が監視のレベルを引き下げたり管理策をまとめて無視したりする原因になっています。マルウェアが前述の防御を巧みに逃れてシステムに感染した場合、厳格な出口フィルタリング (要件 1によって定められた対策) がそれを封じ込め、要件 10 (記録と監視) が (例えば、バックドア経由で) データの取得またはネットワーク外への送信の試みを検出する機会をもたらします。

システムアクセス権/権限の不正使用

本項で取り上げる最後の脅威アクションは、 1 つの重要な点でこれまでに取り上げたものと異なっています。上位 10 件の脅威アクションのリストに含まれるその他すべての脅威アクションは、ほぼすべてが外部の脅威因子によって実行されています。しかし、権限を不正使用するためには権限が与えられていなければならず、その対象は部内者やビジネスパートナーなどの信頼された当事者だけです。不正使用のカテゴリには、「軽微な」ポリシー違反からあからさまな悪意ある行動まで、脅威アクションが幅広く収集されています。特にこの点は、IT システムへのアクセス権や特権の意図的な不正使用をさします。システム管理者が不正に手を染めるのは、今に始まったことではありません。この脅威アクションは、アクセス権や権限の不正使用が目的であり、したがって関連する攻撃手法がなく、回避するのはとても困難です。すでに特権的なアクセス権を与えられている場合は、現在のアクセス権以上のアクセス権を求めたり、制限を回避する必要はありません。

こうした結果から、PCI DSS がカード会員データに対する最も一般的な脅威に対応できていないとは言えません。これは、上記のリストに含まれる重要な脅威アクションのうち、PCI DSSに定められた 12 の要件の対象外に該当するものはひとつもないからです。

部内者による不正使用を制御するために常用される優れた対策は、「慎重な配慮-指示-制限-監督」という流れにまとめることができます。権限の不正使用の抑止は、不正使用することが予想される既知の犯罪者やその他の疑わしい人物を権限に近づけないことから始まります (慎重な*配慮*を示す)。権限を与えられた人は、期待されていることと禁止されていることを知っていなければなりません (対象者に*指示*を与える)。こうして、要件 12 (セキュリティポリシー) は悪意ある部内者を管理するための基礎を提供します。次の防衛線は、高レベルの権限を持つユーザーの数を限定することと、どのような権限であれ職務を遂行するために必要な最小限の権限に制限することです (*制限*)。要件 7 による「業務上必要な範囲」という考え方を厳密に従う (容易なことではありませんが) と、この制限を実現しやすくなります。こうした対策にもかかわらず、部内者が不適切な活動に従事している場合は (それは必ず起こります)、要件 8 (一意の ID) と要件 10 (記録と監視) が不適切な活動の検出と、責任を負うべき者への関連付けに役立ちます。信頼できる人物を採用するのは良いことです。しかし、信頼できる人物であることを継続的に確認するのも良いことです (「信頼せよ、されど確認せよ」)。

分析結果のサマリー

こうした結果から、PCI DSS がカード会員データへの最も一般的な脅威に対応できていないとは言えません。これは、上記のリストに含まれる重要な脅威アクションのうち、PCI DSSに定められた 12 の要件の対象外に該当するものはひとつもないからです。リストに含まれる脅威アクションの大半には、実際に、関連する管理策の複数のレイヤーがPCI DSS 全体にわたって存在します。PCI DSS の範囲内には、(少なくとも概要レベルでは) 大きな過剰や無駄はありません。本報告書では、要件 3 (保存されるデータの保護)[11]、要件 4 (データ伝送時の暗号化)、要件 9 (物理アクセス) を除いて、12 の要件のそれぞれについて上記の論考で取り上げました。好ましくない兆候について指摘するならば、評価結果が最も悪かった要件 (要件 10、要件 11) は表 4 に示した脅威アクションに最も幅広く該当する要件でもあります。したがって、既知のデータ漏洩/侵害の被害者である企業・機関の PCI DSS の準拠率が高くないのはさして驚くにあたりません。図 5 が明確に示しているように、被害にあった企業・機関は要件 4 (データ伝送時の暗号化) を除いてすべての要件にわたって準拠率が低くなっていました。これは、PCI DSS が完全な基準であり、ペイメントカード関連のデータ漏洩に対する保証であることを意味しているのでしょうか。もちろんそうではありません。しかしこの事実は、PCI DSSの準拠や準拠状態の維持に取り組んでいる企業・機関に努力が無駄ではないという励ましのメッセージを送っています。

11 要件 3 については具体的に言及しませんでしたが、表 3 に示したすべての脅威アクションに一般的に該当することに注意してください。データが存在しなければ、被害を受けることはありません。

結論と推奨事項

弊社では、本報告書において提示した資料が、ペイメントカード業界におけるPCI DSS の準拠に関する全体的な状況をより明確に描き出しているものであってほしいと考えています。読者が属する企業・機関がこの全体的な状況において占める位置の判断に役立ち、目標への到達に有用であることが実証されるならばさらに喜ばしいことです。結局のところ、読者が属する企業・機関が今後 PCI DSS に関する評価や取り組みにおいて成功することを保証する魔法の公式は存在しません。しかし、準拠の達成と維持となると、大きな成功を収めている企業・機関に共通する特定のプラクティスがあります。それらの多くは初歩的な常識に帰着しますが、理由は何であれ、日常的な懸念やビジネスを遂行するという定型作業にまぎれておろそかになることも少なくありません。以下にそうしたプラクティスを列挙しました。

準拠とセキュリティを分裂させてはならない。	「コンプライアンスかセキュリティか」の議論に関するスタンスとは関係なく、準拠とセキュリティを意図的に分けたままにするのは、コンプライアンスの観点からもセキュリティの観点からも意味がないという点については、弊社は読者のみなさんと意見が一致するものと思います。理論上は整合しているはずの 2 つの概念の間に、なぜ偽りの二者択一を無理やり持ち込むのでしょうか。結局は、どちらもデータを守ることを目標としています。確かに、（リスク評価またはリスク許容度に基づいて）セキュリティに関して実行していないことをコンプライアンスのために実行する必要がある（またはその逆）かもしれませんが、一律にどちらか一方を選択する状況ではとてもありません。コンプライアンスの管理の全体的な方向性は、セキュリティ戦略と一致しているべきです。自社のコンプライアンス管理チームは、セキュリティ管理チームと同じですか?違う場合は、可能な時と可能な場所でコラボレーションを行うための協調した取り組みが実施されていますか? それともまったく交流がないまま各チームがそれぞれ独立して業務を行っていますか?自社の状況が後者に近い場合は、おそらくその理由とそうした現状を維持することが最善か否かを問うべきです。
セキュリティをプロセスの上に構築するのではなくプロセスに組み込む。	今では、応急処置的なセキュリティはコストが高く、実効性に乏しいことを大半の企業・機関が学習し知っています。多くの企業・機関が認識していないように思われるのは、そうしたアプローチがコンプライアンスにも影響するという事実です。生データを通して分析するのは困難ですが、経験によれば、セキュリティをコアプロセスに組み込んでいる企業は、準拠状態の検証となると、一般に低いコストで高い準拠率を実現しています。これはおそらく、前の推奨事項と関係があるかもしれません。安全な状態を目指して真に、そして継続的に努力している企業・機関は、準拠を実現するために大きな飛躍を必要としないはずです。
コンプライアンスをイベントではなく継続的なプロセスとして扱う。	プロセス主導型コンプライアンスプログラムとイベント主導型コンプライアンスプログラムの違いを見分けるは、経験豊富なアセスメント担当者にとって比較的容易です。PCI DSS 準拠の達成と維持に継続的に成功している企業・組織は、PCI DSS が定める活動を日常業務に統合している企業・組織です。そうした企業・機関は、他の外部または内部のコンプライアンスに関する取り組みと平行して、 PCI DSS 要件のレビューと要件の準拠に継続的に取り組んでいます。セキュリティプロセスを文書化し、記録を維持し、定期的な内部チェックポイントに対応し、指定された管理策に従っていることを示す証拠をすみやかに提供することができます。次の数年間に関するロードマップを作成し、そのロードマップを定期的に調べて今後どのような課題が待ち受けているか、どのような変化が必要か、さまざまな取り組みを支払いインフラストラクチャとデータを保護するための短期戦略と長期戦略にどのように統合するのが最善であるかを確認します。別の言い方をすれば、PCI DSS 準拠の達成と維持は、年 1 回実施するプロジェクトではなく日常的なプロセスとみなすべきです。

検証の準備をするときは、先延ばしにしない。	この推奨事項は、前の推奨事項に関連しており、前の推奨事項から導き出されたものです。企業・組織がコンプライアンスを期限が迫りつつあるイベントとして扱う場合は、大量の準備をあわててしなければならず、相当にあちこち走り回ることになります。間近に迫る OSA の到着を前に、すさまじい勢いで準備するために多大なエネルギーとリソースが投入されます。1 年分の実施していない変更をあわてて実施し (結局そのツケが回ってきます)、古い文書の埃を払い (それが存在していて見つけることができた場合は)、ガムテープで貼り合わせたり、唾をつけて靴を磨くような小手先の対応で何もかもが堅牢で整然としているかのように見せかける (「立ち止まらないでください、ここには見るものは何もありません」、とでも言うように) のです。これは、PCI DSS 準拠に関する評価でほぼ確実に失敗する運命にある企業・機関の行動です。セキュリティの失敗を招く運命にある企業・機関の行動でもあります。なぜなら、評価によってどうにか準拠と判定されたとしても、すぐにいつもの行動に戻るからです。ガムテープははがれ落ち、光沢は曇り、物事の真の姿が白日の下にさらされます。そうした企業・機関は、コンプライアンスの失敗に対して無駄にした時間と労力という代償を支払い、セキュリティの失敗には損害と処罰で代償を支払うことになります。しかし最悪の部分は、そうした企業・機関の行動に対してカード会員も対価を支払う羽目になることです。
コミュニケーション不足を避ける。	コンプライアンスの取り組みに関係しているにも関わらず、多くの場合で企業・機関はコミュニケーションの重要性を認識していません。評価の準備をしているか、または評価中の企業・機関は、調整不足によって評価プロセスが阻害されることのないよう、全当事者に前もってコミュニケーションを行うべきです。このコミュニケーションが内部当事者に関して重要なのは確かであり、外部当事者との共同作業に関しては特に不可欠です。評価の対象範囲内のシステムを管理するベンダーと連絡がとれる体制を作ると、必要な情報を確実に入手しQSA に提供することができます。企業・機関の側の変更によって準拠期限に対応できない場合、ペイメントカード提携銀行は遅延とそれに付随する状況を把握すべきです。つねに全員で最新情報を共有するのは明白すぎる推奨事項ですが、誰もが満足できる状態を維持するための推奨事項でもあります。この満足感がもう少し多く行き渡っても悪いことは何もありません。
貴社の意思決定がコンプライアンスに与える影響を理解する。	「三つ子の魂百まで」というように、企業・機関は自身に関する特定の物事を (容易に) 変更することはできません。そうした変更不能なことのなかには、コンプライアンスに影響するものがあります。例えば、PCI DSS はサービスプロバイダーに加盟店とは違うことを行うよう要求していますが、それを変更するためにできることは何もありません。これはもちろん、企業・機関が重要な変更を実施できないという意味ではありません。企業・機関による変更はたえず起きることであり、こうした意思決定が企業・機関のコンプライアンスを達成/維持する能力に与える影響を理解することが重要です。例えば、レガシーシステムを堅持するという選択を行う場合は、アクセス制御、監査ログ、暗号化に関する特定のテスト手順で準拠と判定されるのが困難になります。ある機能をアウトソースする選択を下すと、プロバイダーから検証に必要な情報を取得するのがさらに困難になります。最終的には、そうした意思決定はビジネスニーズその他の関連する要因に基づいて行われますが、企業・組織は準拠プロセスへの予想される悪影響を考慮し、それに備えるのが賢明です。

小規模かつ単純な状態に維持する。	意思決定の話の続きですが、企業・組織は多くの場合その IT 環境を根本的に変更することができません。ビジネスプロセスは特定のインフラストラクチャ、アプリケーション、機能、構成を必要とする場合があります。しかし、時には、より複雑な選択肢と単純な選択肢の間で選択が可能です。それ以外のすべてが等しいのであれば、単純な選択肢の方が、セキュリティとコンプライアンスの双方に関してほぼつねに管理しやすくなります。弊社の経験から、管理しやすさは管理の成功と高い相関性があります。したがって、可能な場合はつねにこの修正版 KISS (Keep It Small and Simple) ルールを採用し、小規模かつ単純な状態を維持してください。
自社のデータを検出し追跡する。	カード会員データの現状がわからなくなっていることほど、 PCI DSS 評価の範囲を不必要に拡大するものはありません。間違いなく、データは尋常ならざるペースで増殖し、次々と移行することが可能であり、企業・機関の IT インフラストラクチャにはそのための場が大量に用意されています。PCI DSS 評価の範囲を確定するには、データの流れとデータストアの理解が不可欠です。それを十分に理解していない場合は、評価の対象範囲が過度に大きくなり、その結果、評価のコストと複雑性が増します。これを克服するためには、データの厳格な管理が不可欠です。これは、データの検出から始まる継続的なプロセスです。幸いなことに、その作業を支援する内部ツールや第三者サービスが提供されています。データが管理不能な状態になった場合の問題の大きさと危険性ゆえに、それらは一般に長期的には十分に対価に見合う価値があります。
準拠へのアプローチに優先順位を付ける。	「セキュリティ」への道の途上で、企業・機関は、各自のリスク許容度に基づいて異なる目的地を設定すると考えられます。「準拠」への道はその点に関して「セキュリティ」への道とは異なります (ただしそれらは同じ一般的な方向を目指していなければなりません)。PCI DSS はPCI DSS に支配される企業・機関の目的地 (あるいは少なくとも中間地点) を規定します。これは、企業・機関がその目的地なり中間地点へ至る同じルートをとらなければならないという意味ではなく、すべてのルートが等しいという意味でもありません。そこには 1 つの最適ルートと数多くの準最適ルートがあります。PCI セキュリティ基準審議会はその点を認識しており、準拠を実現するためのガイドとして 『PCI DSS 優先アプローチ』 を公表しました。ペイメントカード業界に最も関連のある脅威に関する信頼できるデータも、ルートの調整に役立ちます。適切に利用すれば、それらのリソースは準拠に向けた安全で採算性が高く順調な取り組みに寄与することでしょう。
自ら窮地に陥る前にセルフチェックする。	古い歌の文句のようなフレーズですが、セキュリティプログラムやコンプライアンスプログラムに関しては賢明なアドバイスです。細心の注意を払っている限りすべて問題ないという発想は、捨ててください。それは危険な考え方です。物事の裏では見かけと実態が一致しているのはまれであるということを理解するのが、健全な考え方です。非の打ちどころがない企業・機関は存在しません。完璧なセキュリティプログラムやコンプライアンスプログラムは存在しません。行動を起こし修正する必要のあることが今この瞬間に存在していても、チェックするまでは決してそのことに気づかないものです。要件 10 と要件 11 の準拠率が見るに堪えないほど低いことを知ってもこのことを納得できない場合は、おそらく本報告書 (および『データ漏洩/侵害調査報告書』) で紹介したデータ漏洩/侵害の被害者に関する分析結果を知れば誰でも納得できるはずです。チェックしない企業・機関は対策をとることができません。対策をとらない企業・機関は長期的には成功を収めることができません。そうした企業・機関にならないでください。

ベライゾン PCI サービスについて

企業の業務分野によっては PCI DSS が適用され、PCI DSS に準拠しなかったり、PCI DSS の理解が不十分だった場合、代償を払わなければならないことがあり、しかも代償は予想以上に多方面に及ぶのが普通です。例えば、処罰や罰金のほか、訴訟が発生したり、加えてカード再発行の費用を負担しなければならないこともあります。また、実際にデータ侵害が発生した場合、金銭的な損害に加え、これまでの信用が失われることもよくあります。

上のようにPCI DSSへの準拠は難しく、結局、準拠のためのソリューションやサービスが必要です。ベライゾン ビジネスでは、このようなソリューションやサービスを提供しています。ベライゾン ビジネスの PCI チームは、毎年数百件の評価を実施し、ローカルおよびグローバル Fortune 500　企業の両方と共同で作業を行っています。世界の6大地域で活動する QSA と PA-QSA から構成され、20 種類以上の言語に対応しています。

この専任チームは、PCI DSS 評価と PA-DSS 評価はもちろん、 PCI DSSに関する即応体制構築サービス、助言サービス、改善サービスにも重点的に取り組んでいます。プロフェッショナルサービスに加えて、ベライゾン ビジネスは加盟店コンプライアンスプログラム (MCP)、オンラインコンプライアンスプログラム (OCP)、パートナーセキュリティプログラム (PSP) などのさまざまなプロダクトプラットフォームを通して PCI チームのお客様を支援しています。

verizonbusiness.com/jp

verizonbusiness.com/jp/socialmedia　verizonbusiness.com/thinkforward（内容英語）