PSR

2021 決済システムのセキュリティに関するレポートにおけるインサイト

PCI DSS v4.0
ホワイト
ペーパー

Verizon Cyber
Security Consulting

業界における特に重要な基準の1つであるPCI DSS（Payment Card Industry Data Security Standard）が新しくなりました。この最新のバージョンアップにより、組織は、セキュリティを取り巻く環境が絶えず変化する状況においても、データのセキュリティコントロールを最新の状態に維持し、その実効性を高めることができます。これは、2004年に最初のバージョンが発表されて以来の大掛かりな内容の変更です。PCI DSS v4.0のもたらす影響を理解するために整理しなければならない情報の量が多過ぎると感じていて、要点を整理してまとめた最良の資料で内容を簡素化して理解することを望んでいるのであれば、ベライゾンのPSR（Payment Security Report：決済システムのセキュリティに関するレポート）が必須のドキュメントになります。

数十年にわたる綿密な調査に基づくPSRは、クレジットカード業界において革新的な優れたセキュリティ/コンプライアンスアプローチを実現するためのガイドの決定版です。2010年から公開を始めた一連のレポートは、役員会やセキュリティ運営委員会のほか、現場の最前線で働くセキュリティ/コンプライアンス運用チームも含め、セキュリティ確保のためのあらゆるチームに最適なリソースです。

PSRを活用すれば、決済システムのセキュリティに関する数々の大きな疑問の答えが見つかります。的確な情報やアドバイスが提供されるので、霧が晴れていくように疑問が解消し、以下のような問いに答えを出すことができます。

- 優先すべき事柄や時間をかけて取り組むべき事柄をどう選択すればよいか？
- 目標や目的をどう選択するのか？
- 求められる要件を満たし、制約を取り払うには何をすればよいか？

業績が好調な組織には通常、その理由となる特徴があります。そのような組織では、従業員が高い生産性を維持しながら業務に取り組んでおり、組織が向かう方向を、従業員が明確に理解しているのです。データのセキュリティとコンプライアンスの取り組みにおいても同じことが当てはまります。組織全体として、また、個々の従業員単位でも、高いパフォーマンスを保つことができるよう一致団結した取り組みを行った場合にのみ、組織は成果を上げることができるのです。

皆さんにお尋ねしたいことがあります。セキュリティやコンプライアンスの取り組みで目指す目標や目的をしっかりと把握、認識している従業員が皆さんの組織にはどのくらいいますか？どのような基準を用いて、セキュリティチームの限られたリソースを有効活用していますか？目標、目的、戦略について、あるいは、制約と向き合う方法について、的確な意思決定ができていますか？

クレジットカード業界におけるセキュリティ要件の遵守に努力している組織の多くは、自身が思っているよりも戦略目標の達成に近づいています。PSRが提供する既知のインサイトや入念に構成された手順に従っている組織であればなおさらです。

信頼性の高い革新的なセキュリティプログラムや実践的なフレームワーク、斬新なアドバイスが利用できるので、PSRは、非常に多くの組織が将来に向けた方向性を見出すのに役立っています。PSRが提供する実践的なハンズオンフレームワークは、革新的かつ強力なセキュリティビジネスモデル、業務モデル、戦略を立案し、実現するうえでセキュリティ業務に携わる実務者を支援します。

PCI DSS v4.0は、10番目のバージョンに当たるPCIの基準であり、その遵守では、これまでと比較して特に難しい課題に直面することが予想されます。今回のレポートでは、このPCI基準の内容と基準への対応方法に関して価値の高いアドバイスを提供します。今後予想される変化に備えるうえで、ベライゾンのサポートをぜひご活用ください。

PCI DSS v4.0のリリースで、さまざまな組織が大きな影響を受けるものと予想されます。このリリースに伴い、組織における目的、目標、施策、責任の所在、戦略、その他の手続きが変わります。時間をかけ、適切な手順を踏んで、これらを最新の状態にする必要があります。

目次

PCI DSS v4.0に備える

各バージョンのこれまでのリリースの状況

PCI DSS v4.0は、PCI DSSの10番目のバージョンになります。2022年3月にリリース予定のPCI DSS v4.0は、前回のメジャーアップデート（バージョン3.0）から約9年ぶりのメジャーアップデートになり、2018年のマイナーアップデート（バージョン3.2.1）からは、4年ぶりのアップデートになります。

バージョン4.0以前で最もバージョンアップの間が空いたのは、2010年10月リリースのバージョン2.0と、2013年11月リリースのバージョン3.0の間です。

PCI DSSのこれまでのバージョン

リリース		バージョン
2004年	12月	1.0
2006年	9月	1.1
2008年	10月	1.2
2009年	7月	1.2.1
2010年	10月	2.0
2013年	11月	3.0
2015年	4月	3.1
2016年	4月	3.2
2018年	5月	3.2.1
2022年	3月	4.0

決済システムのセキュリティが絶えず変化を続ける業界を対象にして、過去10年にわたり、ベライゾンはコンプライアンスのトレンドをレポートにまとめてきました。PSRでは、決済システムのセキュリティテクノロジーの変化を正確に把握しながら、コンプライアンスの動向を追跡しています。この10年間に、消費者も企業も、インターネット上での活動を大幅に増やしてきました。そしてその結果、クレジットカードでの取引も増加しました。一方、ハッカーの攻撃能力は進化を続け、大幅に強化されており、過去の脅威や新しい脅威を巧妙に利用した攻撃や、決済システムと決済プロセスの弱点を巧みに突いた攻撃が仕掛けられるようになっています。これと同時に、デジタルトランスフォーメーションがクラウドテクノロジーと密接に関連するようになったことから、決済システムのセキュリティを扱う業界に影響を与える新たな要因が生じています。この結果、CISOなどのセキュリティ責任者、セキュリティ担当者が担う役割がさらに複雑になりました。

上記のような状況に対応するために、PCI DSS v4.0のリリースが強く望まれていたのです。これは、2004年にバージョン1.0のPCI DSSがリリースされて以来となる、17年ぶりの大幅な内容の変更です。一見しただけで、PCI DSS v4.0にはいくつかの大きな変更点があることがわかります。バージョン4.0でもPCI基準の基本的な体系は変わっておらず、2006年に導入されたお馴染みのコントロール目標と12の主要要件はそのまま残っています。しかし、バージョン4.0では、目標や要件を強化する目的で、複数の変更が加えられており、多数の文言が変更されたり、既存の要件が改定されたり、いくつかの新しい要件と将来適用される予定の要件が追加されたりしています。

2016年にリリースされたバージョン3.2のPCI DSSで完全に成熟した基準が実現したと考えられていたのに、PCI Councilがメジャーバージョンアップに踏み切ったのはなぜなのでしょうか？

クレジットカード業界で、さまざまな大きな変化が生じていることや、複雑さを増し絶えず変化しているサイバーセキュリティ環境でリスクが増大していることを反映していると考えられます。これに関係するテクノロジー領域での変化を受けて、PCI DSS v4.0では、コントロール環境とコンプライアンス環境全体で組織が持続性のある効果的な管理を実現できるよう、指針となるいくつかの新たなポイントを提示しています。

PCI DSS v4.0は、クラウドやサーバーレスコンピューティングなどの主要なテクノロジーの使用を明確にサポートしています。PCI DSSの要件に対応するうえで代替コントロールを適用している組織は、現在、新しいPCI DSSのカスタマイズ実装手法が自社固有のセキュリティニーズを満たすのに適しているかどうかを判断することで、メリットを得られる可能性があります。

また、PCI DSS v4.0では、要件の記述にこれまでよりも柔軟性を持たせており、要件の意図の説明があります。このホワイトペーパーの6ページと7ページでは、継続的な評価とカスタマイズされたコントロールの環境という、PCI DSS v4.0における2つの非常に重要な変更ポイントについて確認します。

今回のバージョンアップは非常に重要なバージョンアップと考えられており、そのため、Payment Card Industry Security Standards Council（PCI SSC）は2019年から2021年の中頃に、PCI DSS v4.0のドラフトに関するフィードバックを前例のない規模で募集しました。過去のバージョンアップにおいては、PCI SSCのメンバーが加わっていた組織や評価機関からのフィードバックだけを一定の期間に限り受け付けていました。一方で、PCI DSS v4.0の場合は、広くフィードバックを募り、外部からの協力と利害関係者の関与ができるだけ得られるようにしました1。

1 PCI Security Standards Council、『PCI DSS v4.0:Anticipated Timelines and Latest Updates』を参照。
https://blog.pcisecuritystandards.org/pci-dss-v4-0-anticipated-timelines-and-latest-updates
https://www.pcisecuritystandards.org/about_us/press_releases/pr_10242019
https://www.pcisecuritystandards.org/get_involved/request_for_comments

今回のアップデートに至った特に重要な理由を以下にまとめます。

- このデータセキュリティ基準が決済業界のセキュリティニーズに常に対応できるように確実に維持する必要がある
- セキュリティを確保するための新たな手法に対する柔軟性とサポートを確立する
- 決済システムやモバイル、クラウドなどにおけるテクノロジーの進化に対応できなければならない
- 脅威の現状に対応して、検証に関係するプロトコルや手法を強化するなどの変更を絶えず実施しなければならない
- セキュリティの強化とコンプライアンスの確保を継続的に推進しなければならない

> **「PCI DSS v4.0への移行に備えるためには、どのような対応を始める必要があるのでしょうか？」**
>
> **今こそ、最も重要なこの質問を問い始める必要があります。**

移行期間に関する指針

PCI DSS v4.0の運用が始まるのは2024年ですが、それまでに残されている時間はわずかしかありません。PCI DSS v4.0のリリースは2022年3月ですが、その時点から2年以内に、このバージョンを遵守できるようにしなければなりません。PCI DSS v4.0がリリースされた後は、3.2.1の延長サポート期間を利用して、移行の準備を行います。PCI DSS v4.0のマテリアルがリリースされてから18か月の間は、3.2.1のバージョンが有効です。この移行期間が終了すると、PCI DSS v3.2.1は無効になり、PCI DSS v4.0だけが有効になります。バージョン3.2.1とバージョン4.0が共に有効になる18か月間に加え、さらに別の移行期間も設けられています。PCI DSS v4.0では、リリースがさらに遅くなる新たな要件がいくつかあり、これらの要件を段階的にリリースする期間が別に設定されています。

コンプライアンス環境の移行に取り組んでいる組織の中には、コントロールの内容を変更するための時間が十分にあると考えている組織もあるかもしれませんが、カスタマイズされたアプローチのオプションなどのような大きな変更があることを考慮すると、今準備を始めても早すぎるということはありません。

適切な目標設定によりデータのセキュリティを確保

PCI SSCでは、組織がデータセキュリティのベストプラクティスの活用を習慣付けられるよう、さまざまな要件を策定しています。要件が継続的に遵守されることで、目標の調整、設定、優先順位付け、導入、維持がスムーズになり、それによって、コントロール環境の実効性と持続性が維持されることを、PCI DSSでは意図しています。PCI DSS v4.0ではこのような意図が、これまでのバージョンよりもさらに明示的に示されることが予想されます。

2004年にPCI DSS v1.0がリリースされて以降、ほとんどの組織がクレジットカード情報のセキュリティを実効性と持続性の高い方法で維持しようと努めています。毎年の審査を通過するために継続的に更新作業を行うようなことはせず、年間を通してすべてのPCI DSSの要件を満たすことに成功している組織は、適切に設定された持続性のある目標をベースにした戦略と設計を取り入れています。目標を明確にできれば、独自のコントロールや検証設計の導入が容易になります。

これを念頭に置いている組織の中には、セキュリティの確保を通常業務の中に取り込むことに成功している組織もあります。残念なことに、ベライゾンの2020年のPSRにおけるコンプライアンス調査の結果を見ると、約4分の3（72%）の組織が、PCI DSSのコンプライアンス審査を通過することを重視しており、コントロール環境の実効性や持続性の維持には目を向けていないことがわかります。一方で、コントロール環境の実効性を高めている組織でもコントロールに不備が生じる可能性はありますが、そのような組織では、不具合が発生している期間は短く、問題はすぐに検出され、修正されます。これを実現するには、ほとんどの組織のコントロール環境には組み込まれていないある機能が必要です。

PCI DSS v4.0では、セキュリティの確保を通常業務の中に取り込むことをこれまでよりも重視しており、検証情報を一定の期間収集してセキュリティプロセスの継続的な強化につなげるなどの取り組みを促しています。

持続性のあるコントロールの設計ソリューションの構築

目標が明確でなかったり、セキュリティプランの戦略性が乏しかったりすると、セキュリティの設計に穴が生じてしまいます。慌てて新しい要件を取り入れず、まずは組織特有のニーズや問題解決のためのソリューションを時間をかけて検討することが、CISOやセキュリティ責任者には求められます。新たに加わった要件や内容が変更になった要件を、1つひとつ注意深く確認していく必要があります。プロジェクトマネージャーは、リソースにタスクを割り当てる前にまず、目標と制約の両面から、プロジェクトの範囲を把握しておく必要があります。

セキュリティ担当者やセキュリティ技術者が、セキュリティスタッフの人材不足の問題への対処や、大量のメールアラートの処理に追われています。そのため、データのセキュリティやコンプライアンスのソリューションを適切に策定することが後回しになっており、そのようなケースがあまりにも多く見受けられます。毎年行われる検証プロジェクトにおいて、年1回発行される最終のDSSレポート（ROC：Report on Compliance）を、コントロールの問題を修正することで取得できれば良いとする考え方がありますが、そのようなアプローチでは、PCI DSSの意図をまったく満たせません。

検証手法と検証手続きの強化

PCI DSS v4.0ではいくつかの大幅な内容変更が行われていますが、検証手法と検証手続きの強化もその1つです。そして、この変更では、事前定義済みのアプローチに加え、目的ベースのカスタムアプローチが追加されています。このような検証手法の強化をPCI DSS v4.0に盛り込むことを、PCI SSCは2019年にCommunityの会議の場で明らかにしました。

従来の事前定義済みのアプローチは広く利用されていますが、このアプローチでは、適宜、必要なセキュリティコントロールの導入が必要になります。この検証手法はバージョン4.0でも残されています。事前定義済みのアプローチでは、非常に具体的なかたちで要件を満たすことが求められたり、対象のコントロールシステムが実効性や持続性を有しているかどうかといったような実際の成果とは切り離された検証が求められたりすることもあります。新しく導入されたカスタマイズされたアプローチでは、対応するPCI DSSの要件の意図をコントロールが満たし、その有効性を示せることを条件として、従来のPCI DSSとは異なるセキュリティアプローチが利用できます。

PCI DSSのコンプライアンス評価では、どの主要要件に関しても、いずれのアプローチも選択可能です。たとえば、PCI DSS v4.0では、ハイブリッドのアプローチが可能です。ある要件には事前定義済みのアプローチで対応し、別の要件には、カスタマイズされたアプローチで対応するといったことが許されます。また、要件が1つの場合でも、要件の目的を満たしていれば、事前定義済みのアプローチとカスタマイズされたアプローチで要件の内容を分担して対応することが可能です。ただし、要件によってはカスタマイズされたアプローチでは対応できないものがあるため、その点は注意が必要です。

カスタマイズされたアプローチと代替コントロール

事前定義済みのアプローチ

事前定義済みの実装では、セキュリティコントロールの実装やコンプライアンスの検証で従来型の既存アプローチを用います。これは、PCIの基準の導入時点から存在するものです。要件、コントロール、テスト手順のセットがあらかじめ完全に決められています。導入が必要なコントロールの説明や、対応すべき検証テストの手順の説明が、PCIの基準に記載されています。

事前定義済みのアプローチでは、PCI DSSに記述されている現行（従来）の要件とテスト手順に従うことが求められます。このアプローチは今後も有効です。目的を達成するのにあらかじめ決められた方針に従うやり方は、依然としてどの組織にもメリットをもたらします。コントロールの目的を達成するうえでカスタマイズされたアプローチを採用する必要があると考えている組織の数はあまり多くはありません。

カスタマイズされたアプローチ

カスタマイズ型の実装を活用すれば、カスタムのプロセスを通じて、セキュリティコントロールを個別に設計したり、一般的な事前定義済みのコントロールとは異なるコントロールを導入したりできます。PCI DSSのコントロールを評価するための新しいアプローチであるカスタマイズされたアプローチでは、実装要求ベースのアプローチよりも、成果ベースのアプローチを重視しています。すでに述べたように、カスタマイズされたコントロールではいずれの場合も、要件ごとに定められたセキュリティ上の目的も満たす必要があります。

PCI DSS v4.0の要件と検証オプションは、セキュリティ上の目的に重点を置くように、また、PCI DSSの要件の意図を満たすために組織がさまざまな手法を利用できるように再設計されています。このPCIの基準では、要件の意図が説明されているため、カスタムの実装で達成すべきセキュリティ上の成果が明確にわかります。コントロールの意図の説明では、何を達成することが求められているのかを明示しています。達成する方法は問われないので、目指す成果を達成するための方法を組織はきわめて柔軟に選択できます。

カスタムのアプローチでは通常、以下の点に関するドキュメントの整備が必要です。

- コントロールの設計（コントロールの目的や意図を満たしていることを証明するエビデンスが必要）
- 内部コントロールテスト
- コントロールリスク
- コントロールのパフォーマンス
- コントロールの有効性
- コントロールのメンテナンス
- 外部の機関による、コントロールのコンプライアンス検証テストの手順

カスタマイズされたアプローチは高い柔軟性を有しているため、PCI DSSがまだ言及していないセキュリティソリューションやセキュリティテクノロジーも、PCI DSSが取り上げるのを待つことなく導入できます。検証の手法では具体的な成果をより重視しているので、組織特有の手法が意図する成果を達成できる手法であるかどうかを証明する機会が組織には与えられます。

この代替アプローチでは、いくつかの基準を満たすことで、セキュリティコントロールの個別設計や個別開発が可能です。

- 個々のセキュリティ上の目標を達成するためのコントロールを定める
- コンプライアンスを遵守するために採用するアプローチを説明した詳細なドキュメントを、認定セキュリティ評価機関（QSA：Qualified Security Assessor）に提出し、アプローチの有効性を明らかにする
- QSAはエビデンスを確認し、提出されたドキュメントを審査した結果に基づき、コントロールの有効性の最終判断を行う

カスタマイズされたアプローチがもたらす影響

セキュリティコントロールをカスタマイズするには、評価、予測可能な結果を生み出せる、体系化を徹底した手法が必要です。成熟したコントロール環境を有する組織の場合は、カスタマイズ型の新しい検証アプローチを問題なく導入できる可能性が高くなります。PCI DSSの最新の要件をシステムがどの程度満たしているのかをテストできるようにシステムを改修する場合も、比較的容易に作業を進められます。

新しい評価手法の導入では最初に、ドキュメントの作成やコントロールの設計、診断を準備、実施したり、QSAによる評価で求められるリスク評価データを用意したりする必要がありますが、それらの作業も最小限で済みます。

この新しい評価アプローチの場合、PCI DSSの12の主要要件を満たす際に柔軟な対応が可能になりますが、組織特有の個々の要件は、PCI DSSのコントロールの目的と意図に沿ってカスタマイズされていることが、組織には明示的に求められます。

そのため、カスタマイズされたアプローチでは、セキュリティコントロールの設計および管理と、コントロール環境のメンテナンスで、万全の手法を用意する必要があります。コントロールの設計やコントロールリスクの評価、コントロールの実装および監視で、より高いレベルのプロセスや、より成熟度の高い能力も求められます。

カスタマイズされたアプローチを選択したものの、十分な成熟度のあるコンプライアンス管理プロセスや管理機能に支えられた信頼できるコントロール環境を有していない場合は、成熟度のレベルの向上を図り、段階的かつ小規模に変更を取り入れていくことをお勧めします。そうすれば、コントロール環境に広く変更を加えたことで予期せぬ事態に見舞われるのを避けられます。

QSAや内部監査人（ISA：Internal Security Assessor）の協力を得ながら、カスタムのテスト手順に関して合意を形成し、手順をまとめることが、組織には求められます。組織によっては、カスタマイズしたコントロールの設計や実装に伴い、予期しない結果に遭遇する可能性があります。見落としている点があることに気付き、コントロール、コントロールシステム、コントロール環境の間に存在する因果関係を探し出すことも必要です。

要件の意図に基づき、独自のコントロールを設計して実装する場合には、新たなリスクが生じる可能性があります。さまざま影響を受ける可能性があることや、責任が増えることを組織は理解する必要があります。また、カスタマイズされたコントロールを設計、実装、メンテナンス、監視するための能力およびコンピテンシーの有無と、自社のアプローチに関連のあるすべての要件を満たすことのできる能力の有無を判断することも必要です。この新たな代替アプローチは、どの組織にとっても有用であるわけではありませんが、セキュリティ、コンプライアンス、リスク評価プロセスの観点で成熟したスキルを保有している組織には、最も適したアプローチです。

能力、成熟度、指標の概要については、2019年版PSRの、21ページと29ページの記述を参考にしてください。

意図しない結果について

ある意図のある行動の意図しない、あるいは予想しない結果を表現する言葉として、社会学者のRobert K. Merton氏が初めて、意図しない結果または予想外の結果という概念を打ち出しました。自身の業績の基盤となる著書、『The Unintended Consequences of Purposive Social Action』の中でMerton氏は、以下の3つの種類に意図しない結果を定義しました。

- **予期しない利益：**予想外の利益（偶発利益やセレンディピティと呼ばれることもある）
- **予想外の不利益：**プラスの利益を伴う、望ましくない結果
- **意図に反した結果：**利益を伴わない、望ましくない結果[2]

2 『Unintended consequences』、Wikipedia。 https://en.wikipedia.org/wiki/Unintended_consequences

増大するコントロールリスク：エバーギブン号の座礁事故に学ぶ

安全対策で意図しない結果の存在を見逃すのは大変危険ですが、この危険は容易に見過ごされてしまう可能性があります。複雑なシステムでは、わずかな変化が生じただけでも予想外の結果につながることがあります。望ましくない結果につながるあらゆる可能性を設計の段階で予測して備えることが不可欠ですが、複雑な相互依存関係が存在する場合は、結果を予測するのが困難です。決済システムのセキュリティで、意図しない結果によるダメージのリスクを回避するためには、十分なリサーチに基づく包括的な設計アプローチが必要です。5Gや非接触型決済、ブロックチェーン、人工知能、機械学習など、デジタルトランスフォーメーションの原動力となる複数の要素と、PCI DSS v4.0の新たなアプローチである、カスタマイズされたアプローチを組み合わせるときには特に、このことが当てはまります。

設計や、戦略の立案、計画の策定で先を見据えて調整を図ることを怠った場合に何が起きるのかを、2021年3月にスエズ運河で発生した、コンテナ船、エバーギブン号の大惨事は物語っています。複数の要素が重なり合い、6日間にわたり船が座礁するという最悪の事態が発生したのです。

1 2000年以降、コンテナ船はその規模が2倍以上に拡大しており、特に船幅が広くなっています。事故当時、これを規制する法令には限界があり、海運業界とスエズ運河の関係者の連携にも問題がありました[3]。

2 現役のコンテナ船の中でも最長の部類に入るエバーギブン号が横向きに座礁した海域は、スエズ運河において、その水路が狭まっている場所でした。エジプト政府による2015年の運河改修プロジェクトでは、運河の他の部分とは異なり、その箇所が拡張されることはありませんでした。

3 水深が浅く幅の狭い運河の海域を船幅の広いコンテナ船が航行すると、流体力学の原理から、船体が岸に近づいてしまい、スクワット効果やバンク効果が増し、船舶の操縦性が低下します[4]。事故当時に発生していた強風や砂嵐も、船の操縦を難しくしていたものと思われます。

> 「ネズミの場合も人の場合も、計画の多くは、入念に準備してもうまくいかない。」
>
> — Robert Burns[5]

設計の変更を行う場合、CISOやセキュリティ責任者は、「予防原則[6]」という概念を考慮する必要があります。この概念では、害があることを証明する能力ではなく、害のないことを証明できる能力を証明責任で重視します。何らかの確証が得られないときや、方針の変更あるいは意思決定の結果として悪い結果が予想されるときに、政策立案者たちに度々用いられる手法です。

「予防原則」では、リスクの性質や不確実性、可能性、政府や倫理の役割に関する多くの難しい質問に答えを出すことを強いられます。また、Farnam Streetのブログ記事[7]によれば、特定の状況での適切な意思決定には直感に頼ることも、「予防原則」では求められる場合があるといいます。設計の変更を行う場合に、この点を考慮しておくと、多大な損害を招くデータ侵害のリスクを回避するうえで役立ちます。

3 『The Impact of Mega-Ships』、The Organisation for Economic Co-operation and Development (OECD)、International Transport Forum、2015年。 https://www.itf-oecd.org/sites/default/files/docs/15cspa_mega-ships.pdf

4 Marc Vantorreほか、『Maneuvering in Shallow and Confined Water』、Encyclopedia of Maritime and Offshore Engineering、2017年4月20日。 https://doi.org/10.1002/9781118476406.emoe006

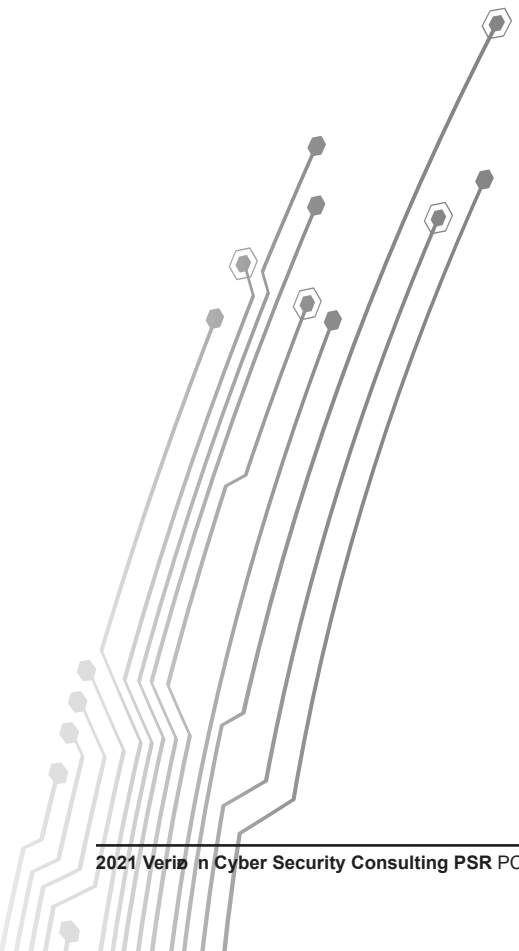
5 「To a Mouse」、Wikipedia。 https://sco.wikipedia.org/wiki/To_a_Mouse

6 「Precautionary Principle」、Wikipedia。 https://en.wikipedia.org/wiki/Precautionary_principle

7 『The Precautionary Principle:Better Safe than Sorry?』、Farnam Street、2021年6月。fs.blog/2021/06/precautionary-principle

目標、要件、および制約のモデル：複雑な問題の解決に向けたアプローチ

持続性の高い設計を実現するには、賢明な戦略と信頼できるビジネスモデルが必要です。PCI DSS v4.0とカスタムのコントロール設計を導入する場合、CISOとマネージャーは、個々の要件に関してプロジェクトの範囲を目標と制約の観点から、明確に把握する必要があります。目標、要件、および制約のモデルと呼ばれ、複雑な問題の解決に使われるこのアプローチが、効率的で持続性の高いカスタムのセキュリティ設計には不可欠なプロセスであるのは間違いありません。2020年版のPSRでは、このモデルについて詳細に説明しています。



論理的思考の活用

本当の意味で実効性と持続性に優れたコントロール環境を設計、実装している組織の数はごくわずかです。戦略プランの立案では、新たな手法を考案したり、実績のあるプロセスを適用したりすることが重要になりますが、それはなぜでしょうか？高い持続性を有する優れた製品や手続きの中には、実績のあるプロセスが取り入れられているものがあります。歯の治療に携わる歯科医師は、ミスの起こらない手順にこだわります。建設業者は家を建てる前に土地の整備を行い、安全が確保される方法で基礎工事を実施します。セキュリティプロフェッショナルも、セキュリティシステムのコントロール設計で同様の手法を採用すべきではないでしょうか？多くの組織に欠けているのは、明確な目標、目的の設定で複雑さを排除できる論理的な手法と、目標、目的を達成できる能力です。論理的な思考を適用すれば、段階的ながら明確かつ予測できるかたちで物事を進める能力を高められます。

エバーギブン号を襲った不幸な出来事を検証すると、先を予測する取り組みを行っていなかったという事実や、戦略目標、規制要件、制約事項という3つの要素の間の調整を怠っていたという事実にたどり着きます。セキュリティマネージャーは、このような3つの要素が相互に関係するモデルを考慮することで大きなメリットを得られます。このモデルにより、設計プロセスでの見落としを回避できるのです。

コンプライアンスの検証評価において、QSAとその顧客が交わしている会話を聞いていると、本当の意味での検証とはかけ離れたところで検証が行われているような印象を受けることが少なくありません。一般にQSAは、評価を実施する際に現状のコントロールの状態を見ずに、過去において検査対象の組織ができていた、あるいはできていなかった判断やアクションに目を向けて評価を実施しており、これでは直接的であれ間接的であれ、マイナスの評価しかできません。そして、会話の内容は組織のセキュリティとコンプライアンスの目的の話に戻らざるを得ません。ほとんどの場合、コントロール環境の管理のエビデンスから、目標、要件、制約に十分な注意払っていない状況が確認できます。これでは、結局のところ、コントロールが機能しなくなってしまいます。

ほとんどのケースでは、コントロールの設計の不備や実装とメンテナンスの不備が原因でコントロールシステムの効力が失われているために、そのような事態になっています。個々のPCI DSSのコントロールは常にコントロールシステムの一部として機能し、例外はありません。不具合の多くは、コントロールの耐性や順応性をコントロールの依存関係や相互依存関係の観点から適切に評価していないことが原因で発生しています。さらには、持続性のある環境から運用上のサポートが得られず、それが原因でコントロールの実効性が大幅に低下しているケースが多々あります。

目標とは何か？

目標では、望ましい結果、成果、組織のミッションの方向性、野心的な計画を、計測可能な結果として具体的な数値に落とし込みます。セキュリティ上、コンプライアンス上の主な目標の内容は事前に数値化できます。そして、実装と運用のタスクおよびプロセスを通じて、あるいは、目標の達成に向けた取り組みにおいて達成できた目標（または達成できなかった目標）を具体的に評価する必要があります。

組織内で目標を明確に周知すれば、日々の業務で目的や目指す方向性が意識されるようになり、アカウンタビリティが促進され、チームメンバーはチームにおいて自らの果たす役割を意識しながら責任を持って職務にあたるようになります。円滑なコミュニケーションは、宣言されている目標の達成に向けたコラボレーションを支える基盤になります。

PCIのセキュリティの遵守に向けて明確な目標を設定すれば、以下の4つのメカニズムを通じて、個人のパフォーマンスにプラスの影響がもたらされます。

- 目標が明確になることで、目標と関係のある活動に取り組むようになり、目標と関係のない活動からは離れるようになる
- 目標が周知されることで、士気が高まり、活動が活発になる
- すでに身に着けている知識を目標の達成に活かそうと努めたり、目標の達成に必要な知識を習得しようとしたりする
- 目標が繰り返し意識されるようになるので、粘り強く業務に取り組むようになり、より高い目標の達成に向けて努力するようになる

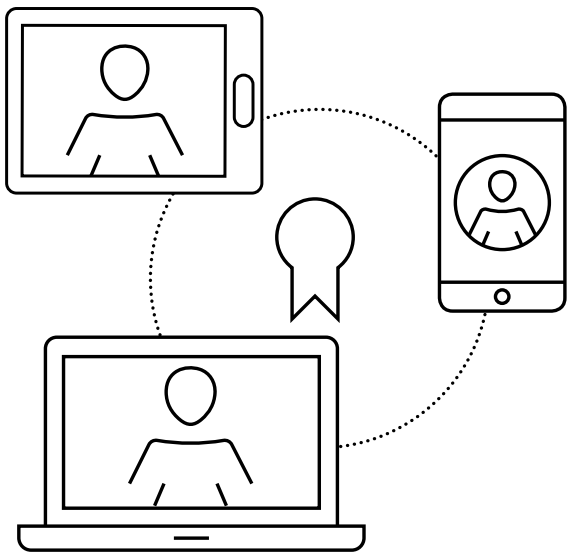
答えを得る価値のある質問を以下に示します。

- データのセキュリティやコンプライアンスに関してどのような目標を定めて内部に周知すべきか？
- 4つあるセキュリティ確保のためのライン（2019年版のPSRの12ページを参照）の各々のメンバーが表現しているのは同じ目標か？セキュリティやコンプライアンスの観点から考えるとどの目標を優先すべきか？
- PCI DSSのコントロールは、コントロール環境全体の何パーセントを占めていれば実効性と持続性が確保されていると言えるのか？
- 意図したかたちで、または偶然達成された成果がどの程度あるか？

実効性と持続性のあるコンプライアンスの実現を目標に掲げるべきであるのは明らかですが、多くの組織では、そうはなっていないのが実情です。関係性を明らかにするのに高度な診断のスキルは必要ありません。そして、目標にしていない目標が達成されることはありません。実効性と持続性のあるセキュリティコントロールの実現をコントロール環境において達成すべき明示的な目標に定めている組織に出会うことは滅多にありません。さまざまなレポートで繰り返し述べているように、予測性、一貫性、再現性のある質の高い成果を偶然ではなく意図的に達成できなければなりません。

具体的な目標を持たなければ、業務は停滞し、必要な投資は容易に得られず、意味のある成果を達成することはできません。

当然のことながら、CISOもセキュリティチームも時間に余裕があるわけではありません。日々の業務は常に切迫しており、現状を省みたり、将来に目を向けたりするよりも目の前の業務が優先されてしまうのです（これらの点については、2020年版のPSRで詳しく触れています）。データのセキュリティとコンプライアンスの目標を適切に設定すれば、コントロール環境の業務に携わるチームも個人も明確なビジョンが得られます。もしもそれができないとなると、セキュリティに影響が生じ、セキュリティ確保のための４つのラインのいずれかのチームが特に影響を受けることになります。



制約のセオリーならびに、決済システムのセキュリティとの関連性

制約の理論（TOC：Theory of Constraints）は実績のあるプロセス管理の方法論であり、TOCを活用すれば、実効性と持続性に優れたコントロール環境の実現を阻む根本原因を明らかにして、問題に対処することが可能です。TOCでは、目標の達成を阻む最も重要性の高い制約要因を体系化された手順を通じて把握できます。そしてそれらの要因を排除したり、状況を変えたりして目標の達成を阻害する要因が解消されるように、集中した取り組みを行います。

TOCの考え方に従えば、管理が容易なシステムであっても、少しでも制約事項が存在すれば、それが原因で達成できる目標は限られてしまいます。そのため、TOCでは科学的なアプローチを通じてシステムの改善を追及しています。TOCの創始者であり、TOCについての著作もあるEliyahu M. Goldratt氏の説明によれば、TOCとは、「継続的な改善のプロセス」であり、複雑な問題を解決するためのシンプルなソリューションを生み出せる思考プロセスの1つであるといいます[8]。

PCIのセキュリティの遵守やデータのセキュリティなどを扱う複雑なシステムは概してそのどれもが、相互に関連した複数のアクティビティから構成されています。少なくとも、そのようなアクティビティの1つはシステム全体に影響を与える制約事項となり、そのような制約事項が少なくとも1つは常に存在します。そしてそれどころか、プロセス全体が制約事項になることすらあります。そして、他の部署や経営陣ですら制約事項と見なされることもあるのです。一連のアクティビティに対して最も関連性の薄い制約を特定することにより、その制約をシステムに制約を与える要因とは見なさないようにできます。システムの他の要素や、システムにつながる外部の要素も、制限をもたらす要因になります。また、この手法をPCI DSSのコンプライアンス環境に適用すれば、コントロール環境に必要なレベルの実効性や持続性を持たせるうえで障害となる制約事項を解消することができます。

大局的な視点を持つ

TOCは、優先順位付けの手法です。複雑なシステムにおいて検証されていない仮説を特定し、仮説を確認して、仮説の問題を修正します。TOCを活用すれば、ライン、プロセス、組織全体の背景情報を考慮しながら個々の手順やプロセスをきめ細かく評価できます。このような包括的な視点は、TOCにおいて重要な役割を果たします。組織を部署、部門の集合として捉えるためです。

組織には数多くの変動要素が存在します。TOCを利用すれば、最大の成果を上げられる方法やポイントをコストをかけずに特定できます。TOC専用のツールも複数存在します。これらのツールでは、問題の認識や問題の解決に一貫性のある体系的手法を利用でき、目標を見失うことがありません。

TOCの体系を活用すれば、最も大きな影響を受ける可能性のある領域で継続的な改善を実施することが可能です。包括的な視点を持ち、継続して制約事項を探すことで、プロセスのコントロールが強化され、新たな能力を開拓できます。そして多くの場合、新規の投資は不要です。言い換えれば、TOCでは、新たな機器やリソースなどにすぐに投資はせず、既存資産の活用を図るのです。これはまさに、PCIのセキュリティコンプライアンス機能を強化するうえで多くの組織が必要としているソリューションです。（2022年版のPSRでは、セキュリティプログラムにTOCを効果的に適用する方法を詳しく説明しています）。

8 Eliyahu M. Goldratt、『What is this thing called Theory of Constraints and how should it be implemented?』、The North River Press、1999年。

以下のような基本的な問いに答えを得る際にTOCが役立つ

- なぜ変える必要があるのか？（目標は何なのか？）
- 何を変える必要があるのか？（どこに問題があって何が根本原因なのか？）
- 何に変更するべきなのか？（解決策は何か？）
- どのように変更を実現できるのか？（どのように実装できるのか？）

以下の作業においてTOCは威力を発揮します。

- 目標、要件、目的を明らかにする
- 目標の背後に隠れている重要な成功要因を目標ごとに3つから5つ特定する
- システムで目標を達成するのに必要な変動要素と条件を明らかにする
- 個々の重要な成功要因で求められる条件を特定する[9]

必要十分条件の概念を活用すれば、PCI DSSの個々のセキュリティコントロールの間に存在するさまざまな関係性や個々のコントロールの状態とそれらの関係性を把握することができます。また、PCI DSSのコントロールとPCI DSS以外のコントロールの間の関係性の把握でも、必要十分条件の概念が役立ちますが、求められるコントロールの有効性と持続性を実現するうえでこのような関係性の把握は欠かせません。カスタムのコントロール設計と検証のアプローチを選択する組織にとって、これらの情報の把握は今後ますます重要になることが予想されます。

9 H.William Dettmer、『The Logical Thinking Process:A Systems Approach to Complex Problem Solving』、American Society for Quality Press、2007年。

PCI DSS v4.0において指針となるポイント

1. すぐに準備を始める

まだ運用が始まっていないからと、PCI DSS v4.0の要件に対応するための準備を遅らせてはいけません。PCI DSS v3.2.1の要件を完全に遵守できているとしても、まだ準備を始める必要がないと考えるのは間違いです。

2. 万全の体制で準備を始めるために、PCI DSS v3.2.1の要件は完全に遵守する

万全の体制で準備を始めましょう。カード会員のデータ環境（CDE：Cardholder Data Environment）に適用される要件ごとにあらかじめ定義されたアプローチに従い、遵守の状況を確認します。また、コントロールシステムの耐性と順応性も評価しておきます。コントロールの不備をすばやく特定して修正できるよう能力を高めておく必要もあります。個々の要件が、明示されている要件の目的に合致しているかどうかも確認します。

3. PCI DSS v4.0 の要件を理解する

PCI DSS v4.0の要件のすべてに注意深く目を通し、変更されたコントロール、削除されたコントロール、新しく追加されたコントロール、項番に変更があったコントロール、将来適用される予定のコントロールに注意します。PCI DSS全体の内容に照らして、個々の要件におけるコントロールの目的と意図を把握します。主要要件の12、11、10、8に加えられた変更の影響が特に大きくなっています（影響度が高い項番順に列挙）。

4. コントロールの設計とコンプライアンスの検証のためのオプションは賢く選択する

カスタマイズされたアプローチを選択した場合は、カスタムのセキュリティコントロールのコンプライアンス検証の準備で、早い段階に作業量が増える可能性があります。カスタマイズされたアプローチでは、コントロールリスクが増大する可能性がありますが、代替コントロールで定義されたアプローチよりも強力かつ永続的なセキュリティコントロールソリューションが実現します。代替コントロールを使用する場合は、ビジネス上または技術上の制約が存在することを文書で証明する必要があります。（2018年版PSRの23ページおよび41ページに、コントロールの有効性の評価方法の例が記載されていますので、参考にしてください）。これまでの事前定義済みコントロールと同様に、カスタムコントロールでは、コントロールの目的と意図を中断なく満たすことができる運用上の継続的な有効性があることを、長期間にわたって示す必要があります。

5. カスタマイズされたアプローチは慎重に選択する

環境のいずれかにカスタマイズされたアプローチを適用する場合は、必要な作業の範囲を管理するための準備が必要になります。運用する環境内で実効性と持続性を維持できる設計がコントロールには求められます。また、関連する目的の意図をコントロールが満たしていることを証明できるように、エビデンスをドキュメント化しておくことも必要です。カスタマイズされたアプローチでは、体系化された詳細なドキュメントによるアプローチを用意しなければなりません。外部による検証に先立ち、コントロールの実効性を内部的に評価する役割担う担当者には十分な経験が求められます。この役割では、コンピテンシー、成熟度、テストという3つの主要な要素に注意を払います。この作業では、検証と承認の作業を実際に行わねばなりません。

6. コントロールの設計テンプレートとマネージメントテンプレートを活用する

定期的な評価でコントロールの実効性を評価することが重要であるのは明らかです。コントロールの設計ドキュメントを体系的に作成すれば、作業に時間がかかっても非常に役立ちます。必要とするセキュリティコントロールやセキュリティコントロールシステムごとにコントロール設計プロファイルを生成する標準のテンプレートを作成して継続的に適用する方法は、どの組織にも勧められるベストプラクティスです。カスタムコントロールのアプローチを導入する場合には特にそうであると言えます（詳細は、16ページの「コントロールの設計テンプレートの必要性と価値」の項を参照）。

7. コントロールの設計の検証を早期に実施する

コントロールの設計の内容は、設計の初期段階でなるべく早めに、ISAやQSAなどの監査人、監査機関と共有し、その内容が受け入れられるものであるかどうか、関連する要件や目的に沿っているかどうかを判断します。コントロールの設計、機能、運用、メンテナンス、評価に関して内容やスケジュール、手法を詳細にドキュメント化していないと、カスタムコントロールの設計の承認が遅れるおそれがあります。

8. 継続的に評価ができるよう準備する

継続的な評価のための設計、実装、メンテナンスをセキュリティチームが実施する際に要件や制約となる事柄を明確化します。これを行うためには、能力のプランニングが必要です。また、年間を通じて、プロセスをサポートし、定期的な評価を行い、環境のコントロールの状態をドキュメントやレポートにまとめる作業で、複数のチームの関与が必要です。PCI DSSのコンプライアンスエビデンスを内部的に記録していくことを、通常の業務活動の一環として継続する必要があります。

コントロールの設計テンプレートの必要性と価値

テンプレートは、コントロールシステムを強化するうえで大いに役立ちます。コントロールの展開、運用、メンテナンスが容易になり、これらの作業での透明性と一貫性が高まります。また、コントロールの設計とコントロールの運用に関する問題を早期に把握するうえでも役立ちます。さらには、コントロールの環境において、実効性や能力を強化する際にも威力を発揮し、コントロールの目的や機能、運用上の制限事項を把握するうえで強く求められる視点も提供されます。

通常、PCI DSSのコントロールプロファイルドキュメントは、PCI DSSの12の項目に従い、コントロールシステムごとに準備する必要があります。

1. **コントロールの目的：**
   適用されるコントロールやコントロールシステムの目的を定義します。

2. **コントロールの責任者：**
   担当や責任を割り当てます。

3. **コントロール機能：**
   管理、手続き、テクニカルなどのような、コントロール機能の内容を記述します。

4. **コントロールのタイプ：**
   予防型、検知型、事後対応型、指示型などのような、適用されるコントロールのタイプを記述します。

5. **アーキテクチャ：**
   システム専用、共通、ハイブリッドなどのような、コントロールアーキテクチャの種類を定義します。

6. **コントロールするリスク：**
   コントロールとリスクのマトリックスやマッピングを使用するなど、コントロールで抑制する主なリスクを記述します。

7. **コントロールのテスト：**
   コントロールのテストの手順を記述します。

8. **実装：**
   実装の範囲、コントロール、手順の実装、依存関係について既定します。PCI DSSの主なコントロールと依存関係があるすべてのPCI DSSのコントロールをリスト化します。

9. **運用：**
   コントロールの運用仕様をドキュメント化し、プロセスの範囲、運用の依存関係、サポートプロセス、コントロールのサポート要件、ユーザ、システム、プロセス、サードパーティにコンポーネントが与える影響を定義します。

10. **メンテナンス：**
    コントロールにおけるメンテナンスの仕様、範囲、メンテナンスのプロセスを定義します。

11. **パフォーマンスメトリック：**
    主要パフォーマンス指標（KPI）などの、PCI DSSの指標の一覧を提供します。これらは、コントロールのパフォーマンスの評価に使用できます。

12. **ガバナンス：**
    関連性のあるポリシー、基準、フレームワーク、規制について記述します[10]。

10 コントロールプロファイルのドキュメント化の詳細については、弊社発行の『2018 Payment Security Report』（https://enterprise.verizon.com/resources/reports/2018/2018_payment_security_report_en_xg.pdf）の12ページをご参照ください。

2021 PSR Verizon Cyber Security Consulting
PCI DSS v4.0インサイト

発行日：2021年11月4日

編集チーム：

筆頭著者
Cis e van Oos en

共著者
Cy thia B. Hans n

筆頭編集者
Cy thia B. Hans n

寄稿者
Abdelk im Aoued Ahmed Bab a、Claire Lavelle、
d hn Galt、Mib elle Wire、Mik ail Banguerk 、
Sean Sweeney

決済システムのセキュリティに関するコンサルティングプラクティス

Veri n Cyber Security Consulting
セキュリティ担当マネージングディレクタ
Kris of Philipe n

グローバルリード
Sam u nk n

米国
Matthew Arns en

APAC
Ferdinand Delos Santos

EMEA
Loic Breat

グローバルインテリジェンス
Cis e van Oos en

チームのメールアドレス
pay n ente u rity@ veri n.o m

コントロールの設計プロファイルを適切に管理することで、コントロールの品質やコントロール環境にプラスの効果がもたらされます。コントロールの設計とコントロールの運用の仕様を明確化すれば、コントロールのパフォーマンスに求められる内容を把握するうえでの視点や背景情報が得られます。また設計上の制約事項を特定、周知したり、主要なコントロールシステムの運用要件やメンテナンス要件をリスト化したりできます。このようなプロファイルがないと、セキュリティチームとコンプライアンスチームは、問題を早期に発見して修正するための方向性が十分につかめず、その結果、コントロールが機能しなくなってしまいます。通常、設計プロファイルの仕様を細かく規定すればその分、コントロールを強化でき、パフォーマンスの予測性を高められます。

コントロールの設計プロセスを適切に管理することで、一貫性、完全性、信頼性のあるタイムリーな運用を実現するという観点から、コントロールの実効性を向上させることができます。

繰り返すことに価値がある

コントロールの設計では、体系的な手法が必要になります。また、PCCI DSSで定義している、依存関係や相互依存関係を持つコントロールの集合では、十分な実効性と持続性を確保するために、個々のコントロール環境ごとのカスタマイズが必要です。十分に考えられた体系的なコントロール設計の手法がないと、実装する個々のコントロールの効力が実装に携わるチームや個人の意欲だけに大きく左右されるようになります。そうなるとコントロールの有効性や持続性の要件に基づいた、コントロールの実際の効力を評価することが不可能になってしまいます。

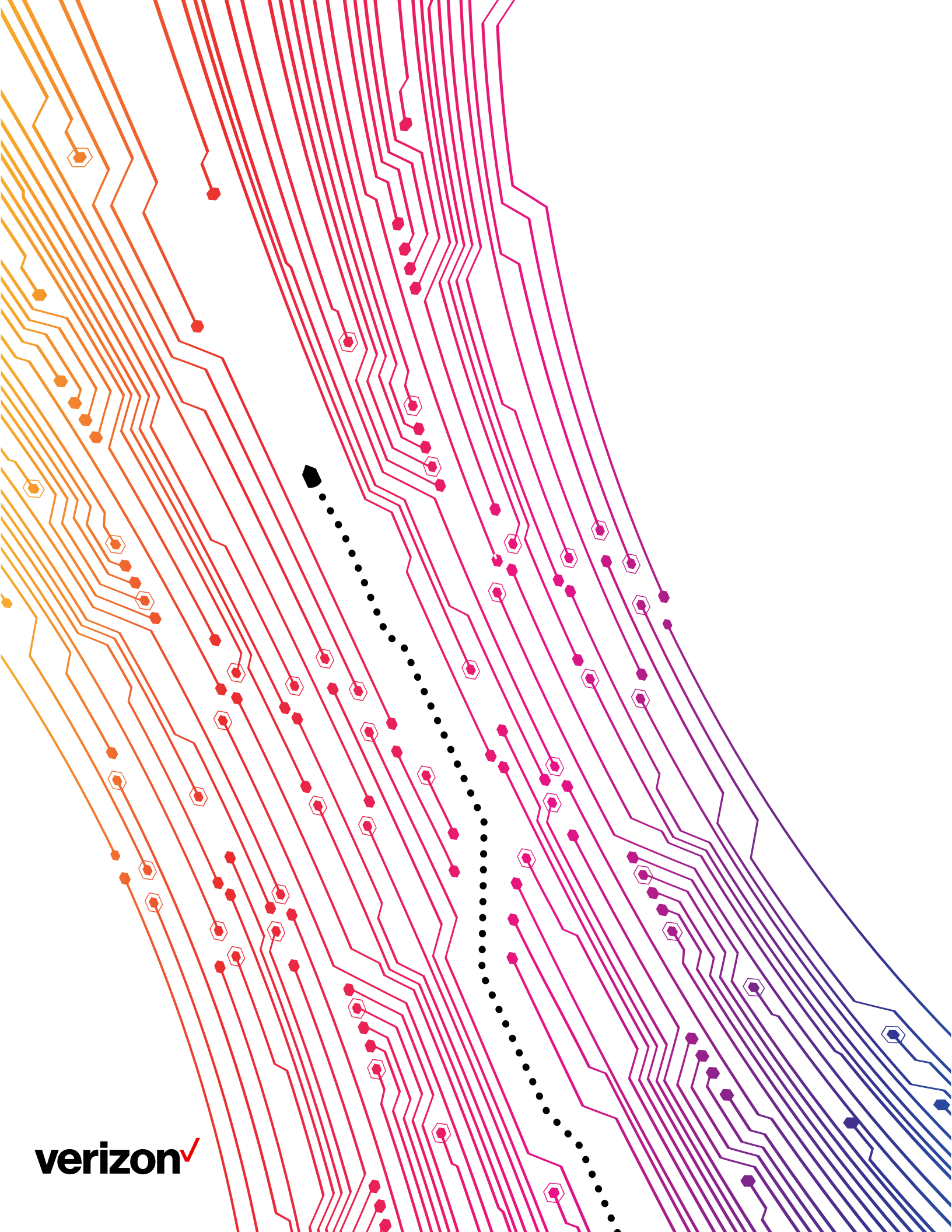
コントロールの依存関係には、さまざまなギャップが存在するのが普通です。この点は、何度でも繰り返す価値がある重要なことです。標準のPCI DSSコントロールを実装している組織で問題が発生していることはよく知られています。そこには、コントロールは実装するだけで機能し、調整は不要との想定があるからです。しかし、何もしなければ、ほとんどの場合、コントロールは機能しません。コントロールの設計を実際に評価し、コントロールの設計を支えるプロセスを導入しないと、持続性のあるかたちで意図したとおりにコントロールを機能させることは不可能です。

コンプライアンスの検証評価を実施したQASがしばしば驚く事実があるといいます。セキュリティコントロールの運用や設計で日常的にエラーが発生している状態を組織が進んで受け入れているというのです。一方、経営陣も、小さいながらもずっと続くコントロールやコンプライアンスのエラーを、回避するのが容易なケースにもかかわらず仕方のない許容できるものとして我慢しているのです。

すべてのPSRをveri n.o m/pay n ente u rity eportからご覧いただけます。

Veri n Cyber Security Consultingについて

本書は、世界30カ国に600人以上のコンサルタントを擁し、PCI（Payment Card Industry）の分野でグローバルリーダーであるVerizon Cyber Security Consultingが作成したものです。ベライゾンは、PCI Qualified Security Assessorで構成される最大規模のチームを有しています。2002年からサービスの提供を開始し、世界で最も長い歴史を持つPCIサービスプロバイダーです。ベライゾンの決済セキュリティ業務は、PCIおよびSWIFTのコンサルティング、評価、プログラム成熟度改善サービスを提供しています。ベライゾンは、サイバーセキュリティコンサルティングのポートフォリオ全体で、適用される規制や基準に確実に準拠しながら、お客様がサイバー脅威を特定、保護、検知、対応、回復できるようサービスを提供しています。


verizon