ホワイトペーパー

PSR

2023 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

先進のPCIセキュリティプログラム管理の設計

Verizon Cyber Security Consulting

verizon

表紙について

表紙の5列×5列のキューブの図は、セキュリティプログラム管理の複雑さを表しています。セキュリティプログラムの設計は、機械的な3次元（3D）の組み合わせパズルを解くようなものです。列を回転させるたびに、システム全体に影響を及ぼします。50億通りあるパズルを解くのに苦労する人もいれば、数秒で解いてしまう人もいます。この違いは、その方法論に関係しています。

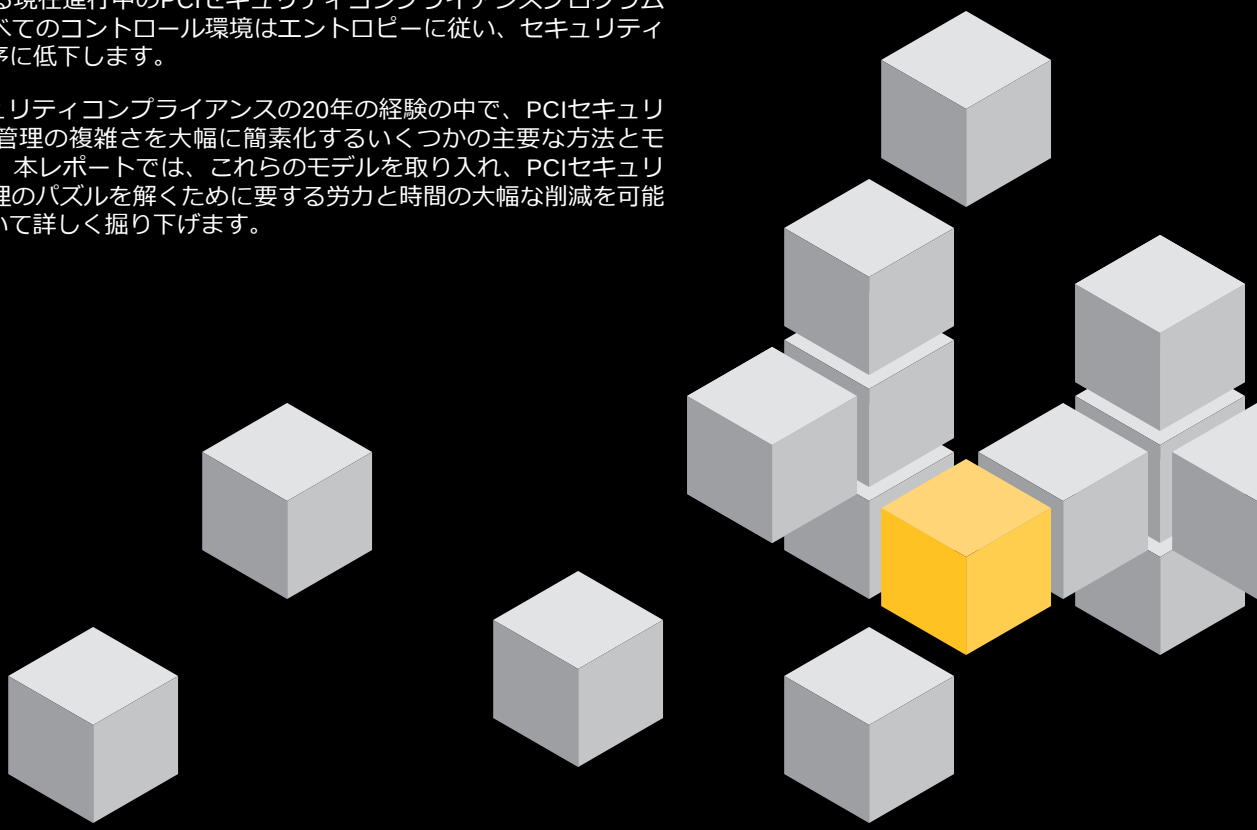
試行錯誤で解を求めるのではなく、ある方法を使えば簡単に解くことができます。列を回転させながら、自分の希望に合った形にするまで、多くの時間を費やすこともできます。あるいは、信頼の置ける論理的なやり方で、時間、労力、コストをかけずに、可能な限り最良の結果で素早く解くこともできます。

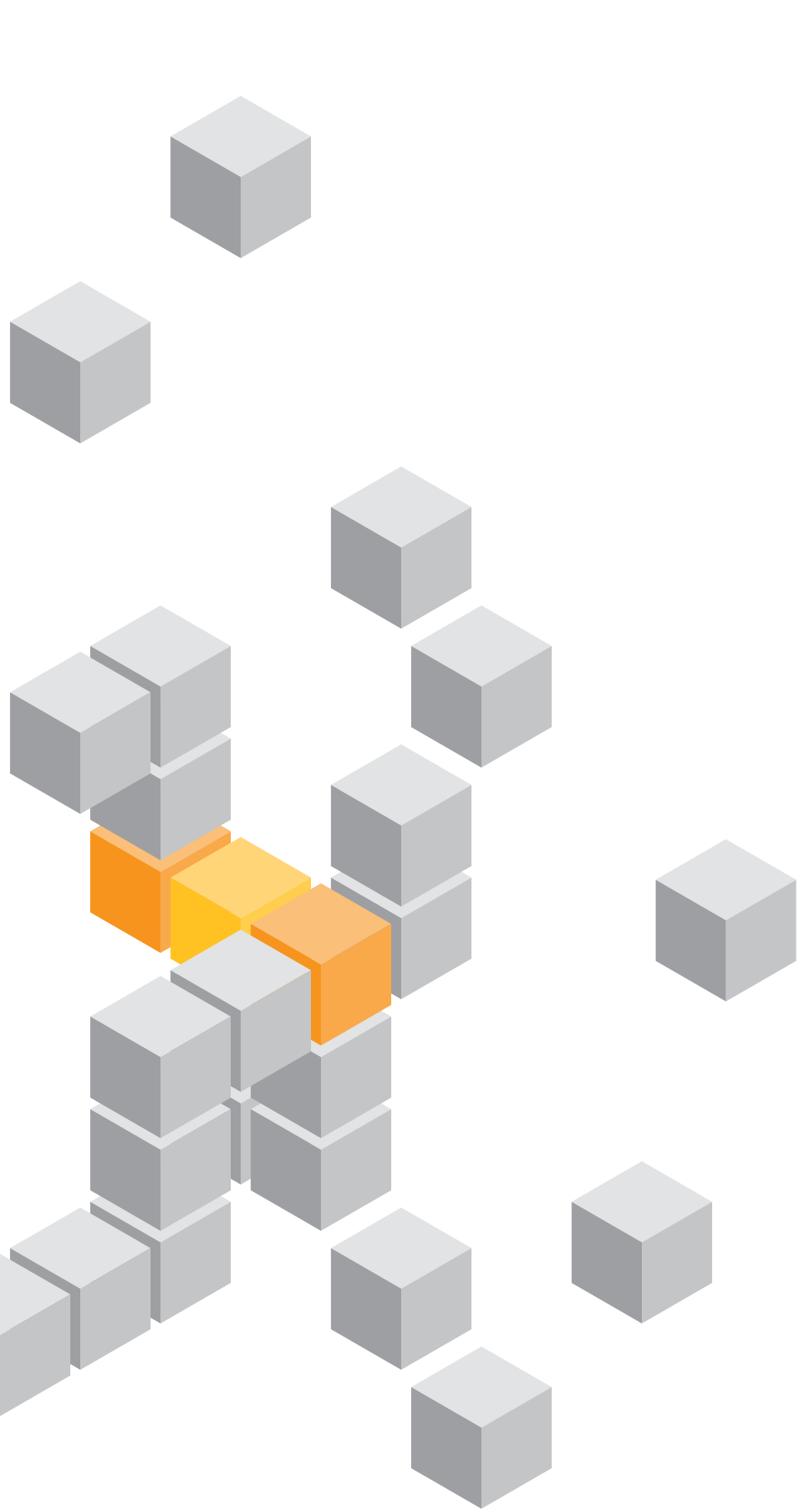
同様に、ペイメントカード業界（PCI）のセキュリティプログラムでも、多くの要素を調整する必要があります。このような複雑さは、健全なプログラム設計（正しい手順を適用するための手法の適用）、および様々な調整間の因果関係を理解することによって、大幅に軽減することができます。

表紙のキューブは、特定の列（黄色）を強調し、より大きなシステムの観点の中で特定のコンポーネントを解決するという、重点化の必要性を表しています。規則性を考えずにいじくり回して全体を一気に解こうとするのではなく、各レイヤーを1つずつ整列させる方法論的で体系的なアプローチを用いることで、システム全体を少しずつ整列させていくことができます。

パズルが完成すると、シャッフルして再度パズルを解くことになります。これは、適切なコントロールができなくなり、各コンポーネント（人、プロセス、テクノロジー）に継続的な注意が必要となる現在進行中のPCIセキュリティコンプライアンスプログラムを思い起こさせます。すべてのコントロール環境はエントロピーに従い、セキュリティコントロール環境は無秩序に低下します。

ベライゾンは、PCIセキュリティコンプライアンスの20年の経験の中で、PCIセキュリティプログラムの設計と管理の複雑さを大幅に簡素化するいくつかの主要な方法とモデルを紹介してきました。本レポートでは、これらのモデルを取り入れ、PCIセキュリティコンプライアンス管理のパズルを解くために要する労力と時間の大幅な削減を可能にする統合的な手法について詳しく掘り下げます。





目次

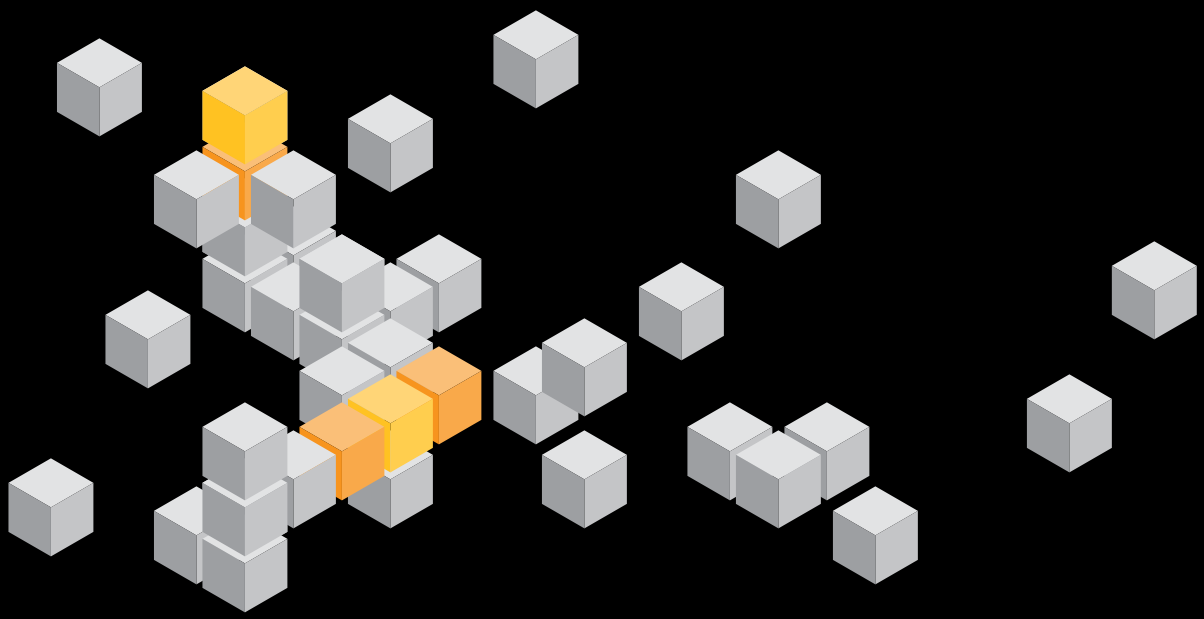
先進のPCIセキュリティプログラム管理の設計

はじめに

このレポートでは、ペイメントカード業界（PCI）のセキュリティプログラムの重要な成功要因と設計アプローチに 関する20年にわたる『決済システムのセキュリティに関するレポート』（PSR）の調査から学んだことの概要を説明します。本レポートでは、PSRで浮き彫りにされ、組織に実質的な価値を与え続けている、長期にわたって実証されたモデル、テクニック、およびコンセプトの統合セットを紹介します。

組織は、ペイメントカードのセキュリティプログラムおよび成果物のコントロールを確立し、維持するために、明確な可視性と見通しを提供してくれる方法を求めています。こうした組織には、障害への対応からセキュリティプログラムのパフォーマンス低下の原因への対処に重点を移し、プログラムのインプット、パフォーマンス、アウトプットを高度に予測可能にする手法によるアプローチが必要です。過去10年間に、いくつかのコンプライアンス管理プログラムの設計が試行されました。ベライゾンは、複雑なPCIセキュリティコンプライアンス管理の課題に組織がうまく対処できるよう、一連のモデル、手法、およびテクニックを評価、設計、発表してきました。

本レポートでは、あらゆる企業規模および業種向けに、利用可能な最良の方法とモデルのいくつかを活用し、 PCIセキュリティプログラムのほぼすべての側面の設計と運用を簡素化し、改善するための統合的なアプローチを紹介します。



組織が予測可能なパフォーマンスとプログラム全体の成功を設計によって達成できるよう、ベライゾンは20年以上にわたって、セキュリティモデルの探求と改良を行い、セキュリティプログラムの設計を進めてきました。このレポートに挙げる方法と概念は、以下の方策をとることで、組織がプログラムとプロジェクトをより簡単に設計し、重要な問題に集中し、セキュリティコンプライアンスの運用環境を簡素化し、最も重要な制約を克服するのに役立ちます。

- プログラム全体と各主要要件に関する明確な目標を策定し、周知する
- 少ないリソースを合理的に配分して経済的なアプローチを考案する
- PCIセキュリティプログラムに組み込むことができる重要なプログラム設計と管理の要件を作成する
- 明確なプログラム目標を策定し、セキュリティ戦略の設計に必要なフレームを確立する
- PCIセキュリティコンプライアンス環境の範囲を縮小し、積極的に制御する
- 適用されるPCIセキュリティ基準（Data Security Standard［DSS］、PIN Transaction Security、Point-to-Point Encryption［P2PE］、3-D Secure［3DS］、Secure Software）やその他の規制（Society for Worldwide Interbank Financial Telecommunications［SWIFT］のCustomer Security Control Framework［CSCF］）など、さまざまなセキュリティ基準の要件を1つに統合する
- プログラムが不調となる根本原因を明らかにする論理的なプロセスを考え、プログラム管理を行う
- チームが適切な仕事をこなし、何に重点を置き、何を無視すべきかを確信できるようにするためのプロセスを推進する
- 最も重大な制約を特定し、克服するための方法を開発する
- 正式なプログラムマネジメントの実践、クリティカルチェーン、成熟度モデルの必要性を理解し、そのような実施の指針と評価を行う

これらの重要なツールとモデルは、PCIセキュリティコンプライアンス管理を成功させた多くの組織から学んだ教訓に基づいて、既存のプログラムを改良したり、新しいプログラムを設計したりする際に役立ちます。

PCIセキュリティの複雑さを軽減するベライゾン独自のアプローチを紹介いたします。

本レポートでは、決済システムのセキュリティの複雑さを軽減するために設計された方法、テクニック、およびモデルについて概説します。

メンタルモデルの価値

メンタルモデルとは、概念やプロセスなど、何がどのように機能するかを表現したものです。モデルを活用すると、重要な側面に重点を置くためにできるだけ多くの部分を削ることで、そのプロセスをよりよく理解することができます。

PCIセキュリティプログラムの改善におけるモデルのメリット

システムや環境の詳細な情報をすべて頭に入れておくことは困難です。そのため、モデルを使って複雑なものを理解しやすく整理しやすい塊に単純化します。運用プロセス、管理、およびコントロールを適切に構造化することは、PCIセキュリティプログラムを円滑かつ効率的に実行する上で大きなメリットをもたらします。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では、メンタルモデルが、セキュリティプログラムの参加者に情報を提示する際のコンテキストを決定するのに非常に有効です。

モデルを使うと、関連性の強い要素と弱い要素が存在する理由を検討することができます。また、推論し、プロセスを見通し、構造化し、要約し、重要なことに集中するのにも役立ちます。モデルによって、セキュリティのコントロール環境、コントロール環境についての個々人の理解、コントロール環境のコンポーネント間の機能と関係性などに対する見方が形成されます。モデルはまた、個人やチームが自身の能力、実行するタスク、学習曲線について持つ見解も形成します。これらはすべて、概念化によって大きく左右されます。

詳しくはhttps://fs.blog/mental-modelsの『Mental Models: The Best Way to Make Intelligent Decisions (~100 Models Explained)』をご覧ください。

メンタルモデルは、ヒューリスティックである限り、ある程度不正確である可能性が高く、システムのすべての側面をカプセル化することはできません。

「本質的には、すべてのモデルは間違っているが、中には有用なものもある[1]。」

—George E. P. Box氏

「情報セキュリティの実務家はさらなる認知の危機に注目し、新しいモデル化を切望している。実際、私たちはしばしば優れたモデルを使いすぎたり、実用的な目的を超えて拡張したりしている。... 問題なのは、私たちがモデルに飢えていて、理に適ったモデルが見つかるとすぐに飛びつき、乱用してしまうことだ。結局のところ、私たちが優れたモデルを求めるのは、堅牢なツールボックスが欲しいからなのだ。しかし、すべての仕事にハンマーが使えるわけではないし、14インチの丸ノコも必要としない[2]。」

—Chris Sanders氏

複雑さを単純化するメンタルモデル

モデルは、従業員を組織化して指揮し、タスクを割り振り、セキュリティコンプライアンスプログラムに関する意思決定を行うための方法を提供するため、あらゆる規模の企業にとって重要となる設計、運用、管理の構造を表現します。また、目標や目的を達成するために個人とチームを調整し、管理するために、組織がどのように活動を構成するのが最善であるかを理解させてくれます。モデルにより、正式なコミュニケーション手段を明確にし、個々人の独立した行動をどのように連携させるかを明らかにすることができます。

「私たちの思考の質は、頭の中にあるモデルと、目の前の状況におけるその有用性に比例します。モデルが多ければ多いほど、つまりツールボックスが大きければ大きいほど、現実を見るための正しいモデルを手にする可能性が高くなります[3]。」

1 George E. P. Box、『Science and statistics』、Journal of the American Statistical Association、Taylor & Francis, Ltd. on behalf of the American Statistical Association, 1976年

2 Chris Sanders、『Information Security Mental Models』、2019年5月、https://chrissanders.org/2019/05/infosec-mental-models

3 『Mental Models:The Best Way to Make Intelligent Decisions (~100 Models Explained)』、Farnam Street、2023年7月28日アクセス、 https://fs.blog/mental-models

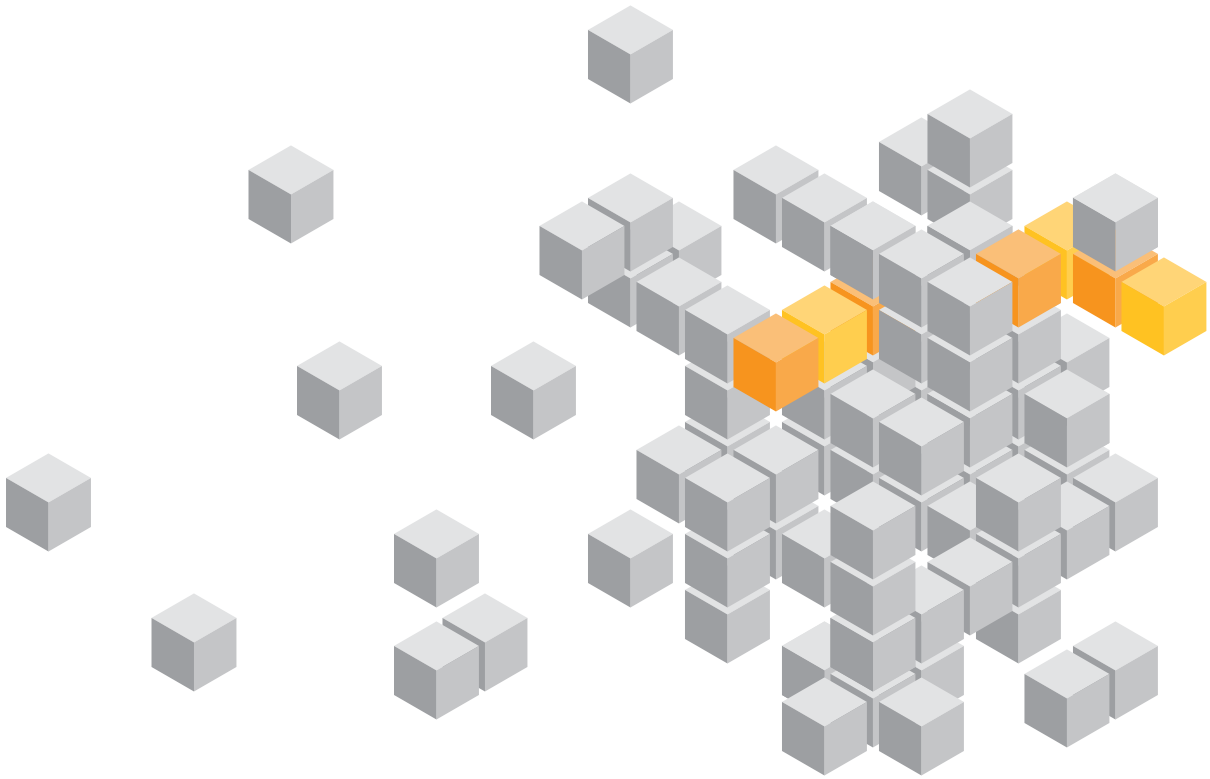
PCIセキュリティプログラムの目標

PCIセキュリティプログラムの目標を明確に定めることは、プログラム設計の最も重要な最初の一歩です。プログラムの存在理由と達成目標を伝えることは、すべてのPCIセキュリティの取り組みにとって重要な成功要因です。目標の明確化は、プログラムが成功しているかどうかを判断するために現実を評価する基準となります。しかし、その重要性にもかかわらず、プログラムの仕様書に明確な目標の記述を含めている組織は驚くほど少ないのです。PCIセキュリティコンプライアンスの目的を定義せずに、適切なリーダーシップと戦略を実現することはできません。

コンプライアンスの検証評価に合格することを目標にするだけでは、PCIセキュリティプログラムの最終目標の仕様としては不十分です。最終目標までの中間目標として、データを効果的かつ持続的に保護することを含める必要があります。コントロール可能なプロセス、予測可能な結果、およびコントロール環境全体にわたる測定可能なパフォーマンスを備えた、より高いレベルのプロセスと能力の成熟度に向けて継続的に改善する必要があります[4]。

PCIセキュリティコンプライアンスプログラムにおける組織の全体的な目標は、ペイメントカードのデータを効果的かつ継続的に保護するための合理的な保証を、一貫した予測可能かつ持続可能な方法で提供する成熟したコントロール環境を開発、維持、および継続的に改善することです。

この目標を達成するために、PCIセキュリティコンプライアンスプログラムは、追加のセキュリティ、リスク管理、およびガバナンスのフレームワーク、（セキュリティ運用モデル、戦略、およびセキュリティビジネスモデル）と統合されサポートされます。



4 「コントロール環境」の説明については、17 ページをご覧ください。

PCI DSSの全体的な目標

この目標には、5つの重要な要素が含まれています。

1. **開発、維持、および継続的な改善**
2. **成熟したコントロール環境**
3. **合理的な保証**
4. **ペイメントカードデータの効果的かつ継続的な保護**
5. **一貫性のある予測可能で持続可能な方法**

プログラムの全体的な目標は、チームが目指すべきものであり、コンプライアンスの戦略およびプログラム内のすべての意思決定、タスク、活動に影響を与えるものです。したがって、PCI DSS準拠の全体的な目的と、意図する全体的な望ましい結果を慎重に定義する必要があります。

PCIセキュリティプログラムの設計は、システムの全体的な目標を特定することから始めます。次に、目標の重要な成功要因となる要件を達成するために、中間目標に優先順位を設定して目標の達成に向けた戦略を策定します。戦術についてはこの後で説明します。戦術を最初に開発し、それを局所的に実施（部分的に最適化）する組織は、それを数回繰り返すと失速する傾向があります。通常、セキュリティおよびコンプライアンスチームの方向性は組織の他のメンバーからは十分に理解されません。戦略と戦術に対して体系的でグローバルな最適化アプローチが必要になります。

詳細については、ベライゾンの2022年版PSR[5]の8、18、および25～31ページ、86ページの「CI DSS Key Requirements goal ƅ atements（PCI DSS主要要件の目標設定）」、および146ページの「付録 A：Primer for c afting ɐ ɑ rity and o mpliane goals（セキュリティとコンプライアンスの目標作成の手引き）」をご覧ください。

PCIセキュリティプログラムの成功の定義

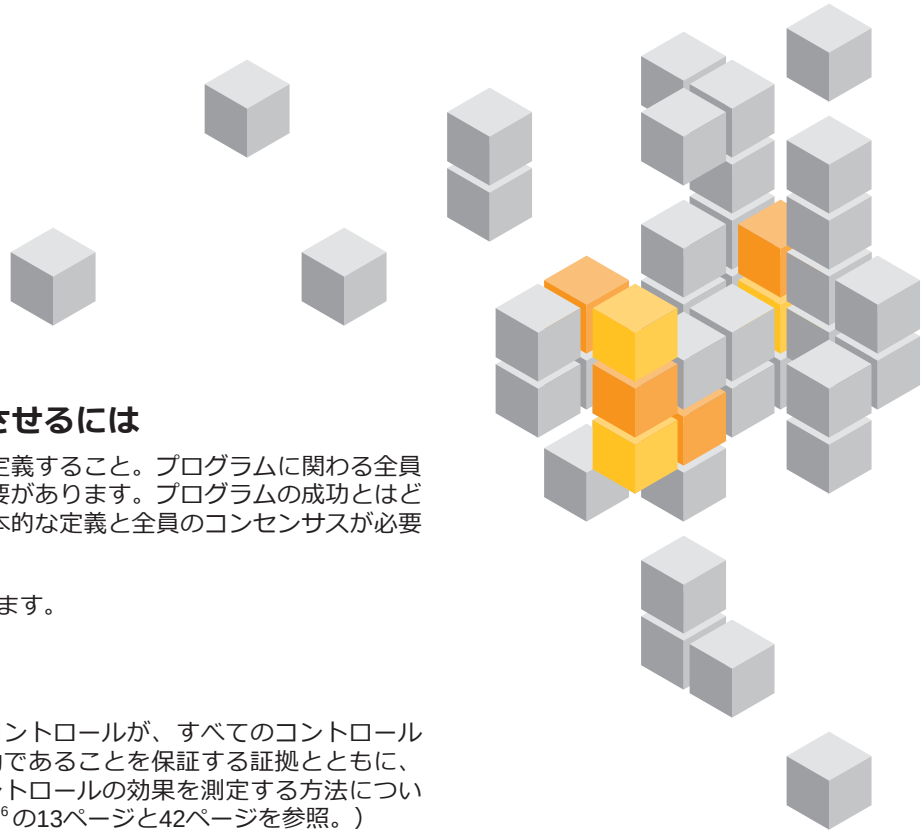
多くの組織は、依然とコンプライアンス検証評価の結果をもって、PCI DSSプログラムの成功を測定しています。これは通常、コンプライアンス検証の面のみを測定するものですが、コンプライアンスプログラムの成功は、さまざまな観点から測定できます。たとえば、プロジェクトおよびプログラム管理の観点からは、時間ベースの主要業績評価指標（KPI）（サイクルタイム、1回限りの完了、変更回数、プランニング時間と費やした時間の比較）、予算ベースのKPI（予算と実際の支出の比較）、マイルストーンと現在までの達成度といった従来のプロジェクト管理メトリックでプログラムのパフォーマンスを測定することができます。リソースの効率性、実効性、有効性という観点に立ったプロジェクトのパフォーマンス測定は、リスクの程度やペイメントカードのアカウントデータが 組織によってどの程度保護されているかについてはあまり多く語ることはありません。これは、PCIセキュリティコンプライアンス規制の違反に関係するリスクと負債の軽減の進捗状況に関わっています。

PCIセキュリティプログラムの取り組みのレベルは、最終的に主に次の3つの要因によって決まります。

- **複雑さ：**コントロール環境の複雑さのレベル
- **熟練度：**セキュリティコントロール環境を設計、実装、維持、および評価するための熟練度（スキルと経験/適正と能力）
- **集中化：**投資のビジネスモデル、リソースを的確に方向付ける戦略、運用、サポートフレームワークの適用、プログラムの集中的な設計と実行など、重要な目標への集中力の最適化

チームの熟練度が非常に高くても、注意散漫で集中力を欠いていると、パフォーマンスは向上しません。

5 2022 PSR https://www.verizon.com/business/resources/reports/2022-payment-security-report.pdf



PCIセキュリティプログラムを成功させるには

目的の達成を思い描いて開始すること。目標を定義すること。プログラムに関わる全員が、プログラムの達成目標を明確に理解する必要があります。プログラムの成功とはどのようなものであるかについて、少なくとも基本的な定義と全員のコンセンサスが必要です。

成功が認められるのは、以下の5つの成果によります。

1. 実効性のあるプログラム

そのコントロール環境と主要なコントロールが、すべてのコントロールの目的の意図を満たすうえで有効であることを保証する証拠とともに、正しい仕事を実施します。（コントロールの効果を測定する方法については、ベライゾンの2018年版PSR[6]の13ページと42ページを参照。）

2. 効率的な実施

リソースの無駄を最小限に抑え、最適な方法で実施し、経済的なプログラムの成果を出します。

3. 戦略的な整合性

プログラムの設計と実行は戦術的でも事後的でもなく、全体的な事業戦略を支援するために戦略的な整合性を持ちます。（戦略の測定方法については、ベライゾンの2022年版PSRの29ページと30ページを参照。）

4. 持続可能なパフォーマンス

コンプライアンス管理は短距離走ではなくマラソンです。コントロールと環境の持続可能なライフサイクル管理が必要とされます。

5. 継続的な成熟度の向上

プログラムのプロセスは、プロセス能力よりも高い成熟度に向けて継続的に進歩しなければなりません。（測定と成熟度モデルについては、ベライゾンの2019年版PSR[7]の25～29ページを参照。）

これらの成果は、それぞれ設計によって達成することが可能です。これら5つの重要な成功基準を達成するためには、それぞれの基本的な範囲と設計、実施、測定の方法を知る必要があります。

6 2018 PSR https://www.verizon.com/business/resources/reports/payment-security/2018/

7 201 PSR https://www.verizon.com/business/resources/reports/payment-security/

管理モデル

セキュリティマネジメントキャンバス

成功する戦略的なPCIセキュリティプログラムの設計と管理には、統合的な視点が必要です。これは、プログラムの主要なコンポーネントおよび重要なインプットとアウトプットをエンドツーエンドで可視化することを意味します。これは、またプログラムが効果的かつ持続可能であるための重要な成功要因でもあります。PCIセキュリティコントロールプログラムは一時的な取り組みではありません。PCIセキュリティを規制する法令の遵守は長期的なビジネス上の関心課題であり、継続的なコンプライアンス運用を長年にわたって維持する能力を開発するには戦略的プランニングが必要です。セキュリティビジネスモデル、セキュリティ戦略、セキュリティ運用モデル、およびセキュリティフレームワークと基準を意図的かつ構造的に統合することなく、セキュリティコンプライアンスプログラムを設計および運用しようとする組織は、その結果に対して困難な戦いを強いられることになります。その結果、回避すべきプログラム設計と管理の落とし穴に直接足を踏み込むことになります。設計が不十分なプログラムは、組織の他の部門のビジネスミッション、ビジョン、業務と十分に整合性をとった強固な基盤の上に作成されていないため、常に問題の対応に追われることになります。セキュリティマネジメントキャンバス（TSMC：The Seαrity Management Canναs）は、プログラムのパフォーマンスを低下させるいくつかの根本原因に対処します。

正しい仕事を正しい順序で行う可能性を引き出す、極めて強力なフレームワーク

この管理モデルは、PCIセキュリティプログラムのパフォーマンス管理に関する20年の経験に基づいており、ベライゾンが開発し、2020年のPSR [8]で発表したものです。（2020年版PSRの15～17ページの「Elements of a high-performance data security enν ronment（高性能データセキュリティ環境の要素）」を参照。）TSMCは、あらゆるPCIセキュリティプログラムを正しい視点と順序で配置する非常に強力なフレームワークです。TSMCの5つの柱は、すべての組織が開発、維持、および適用すべき一連の統合ドキュメントに示されています。

セキュリティプログラムが5番目の柱になっているのは、それなりの理由があることに注意してください。これは、先行する柱の結果との依存関係に焦点を当てるためです。これは、効率的で効果的なPCIセキュリティコンプライアンス管理プログラムを成功裏に管理するために必要なインプットとアウトプットということだけでなく、チームが知っておく必要のある業務範囲について、文脈に沿った豊富な視点を提供するものです。この構造により、適切な作業を適切な順序で適切に行う可能性が開けます。セキュリティコンプライアンスプログラムのための決定と行動は、すべてこのキャンバス内で行ないます。すべての組織は、強固な基盤を構築するために、活動におけるこれらの柱に投資する必要があります。

なお、セキュリティマネジメントキャンバスについては、2022年版PSRの32～41ページで詳しく触れています。

一元管理ビュー

セキュリティマネジメントキャンバスでは、セキュリティとコンプライアンスの管理プロセス全体を一望することができます。このキャンバスに、効果的な管理システムの基盤となるブロックが提示されています。TSMCの構造に基づいてプログラムを設計し実施することで、非常に価値のある重要なドキュメントが作成され、プログラムのライフサイクル全体を通じて重要な意思決定を行うために必要である正確なインプットが得られます。

TSMCを使用して、このキャンバス上の各コンポーネントとその関係に照らしてプログラムの進捗を評価し、見逃していたものを見つけ、ステップの見落としや無視がもたらす結果を見て、修正を行えば、時間と労力を大きく節約することができます。

8　2020 PSR、 https://www.verizon.com/business/resources/reports/2020-payment-security-report.pdf

セキュリティマネジメントキャンバス

5つの柱	セキュリティ ビジネスモデル	セキュリティ戦略	セキュリティ 運用モデル	フレームワークと基準	セキュリティ プログラム
ドキュメント	**ビジネスモデル** 価値提案 ステークホルダー 目標と目的 コアプロセスの アーキテクチャ リソース 文化 法規制 リスク管理 ガバナンス	**戦略** ステークホルダー 優先事項 – 目標 – 目的 **業務範囲** – 集中 – 範囲内 – 業務外 **リソース** – 社内 – サードパーティ 戦略的管理における7つ のトラップ	**運用** （バリューチェーン、 視覚的表現） ステークホルダーとの 関係 組織図 地図 – 施設と運営 組織プロセス –コアプロセス – サポートプロセス セキュリティ プロセス ネットワーク アーキテクチャ 機能責任 能力マップ 制約マップ	**セキュリティフレーム ワークと基準の統合** PCI DSS PCI PIN PCI P2PE PCI 3DS CIS CSC NIST CSF SWIFT CSP **基準とフレームワーク要 素のカバー状況** 部分的実装 完全実装 **環境全体の実装範囲** 部分的実装 完全実装	**プログラム管理** プログラムオフィス プログラム憲章 **プログラム設計** ライフサイクル管理 **プログラムの範囲** リソース（4L） 制約（7C） 持続可能性（9F） **プロジェクト マネジメント** 成熟度 – プロセス – 能力 パフォーマンス – メトリック – レポート
説明	すべての要素を結びつける包括的なモデルです。これにより、セキュリティとコンプライアンスへの投資に対する支援を得やすくなります。ビジネスモデルには、ステークホルダーに最大限の価値を提供するための目標とコアプロセスの構造が定義されます。戦略運用、セキュリティフレームワーク、セキュリ ティプログラム間の整合性をサポートします。	アプローチを定義し、セキュリティコンプライアンス目標の慎重な選択と優先順位付けを決定します。戦略では「何を」と「なぜ」を定義しますが、「どのように」は定義しません。セキュリティ戦略を成功させるには、セキュリティビジネスモデルと整合させる必要があります。	セキュリティおよびコンプライアンスの運用おいて機能的なコンポーネントを表すドキュメントの集成です。リソースと中核的なプロセスとを整合させ、セキュリティとコンプライアンスの運用から組織に価値がどのように創出されるかを視覚的に示します。コントロール環境がどのように機能し、どこを改善する必要があるかを理解するなど、パフォーマンスの問題を診断するのに最適です。現在の運用モデルがあるなら、運用をどのように改善すべきかを定義するための目標運用モデルも必要です。	セキュリティとコンプライアンスの管理システムのサポートガイドとして機能します。これらがプログラムやプロジェクトの構造を動かします。その成否は、実装の巧拙によって決まります。	長期的な目標を達成するためにプロジェクトの集合体を設計および管理することで成果を実現します。プログラムの成否は、先行する4つの柱（ビジネスモデル、戦略、運用モデル、フレームワーク）との相互作用とそのサポートにかかっています。

図1

GRC²モデル

目標
必要事項
制約事項

X

ガバナンス
リスク管理
コンプライアンス

多くの組織では、PCIセキュリティコンプライアンスプログラムをより広範なガバナンスプログラムから分離しており、さまざまなプログラム間におけるタスクの重複や繰り返しを回避する同期化アプローチの効果と効率性を認識していません。単一のコーポレートガバナンスの傘下でさまざまな規制要件を満たすための統一されたコンプライアンスアプローチには、コンプライアンスとリスク管理に大きなメリットがあります。組織は、少なくとも年1回、ガバナンスプログラムの目標、要件、制約を再検討すべきです。

GRC（ガバナンス、リスク管理、コンプライアンスの頭文字）は、管理規律と運用フレームワークを包摂する用語です。組織の目標と目的を確実に実現するために、GRCは、明確に定義された測定可能なパフォーマンス基準を確立できるよう、組織全体をカバーする統合的なアプローチを必要とします。言い換えれば、ビジネス慣行としてのGRCの主な目的は、組織のあらゆるレベルにおいて予測可能で信頼できるパフォーマンスをサポートするために、十分に調整され統合された能力の集合体を開発し維持することです。これは、リスクを効果的に管理し、コンプライアンス要件を満たしながら、ITとビジネス目標とを整合させるための構造化されたアプローチです。組織は、目標と戦略目的を達成し、ステークホルダーのニーズを満たすために、この必要不可欠な能力を開発する必要があります。

GRCの範囲は、ガバナンス、リスク管理、コンプライアンスだけにとどまりません。保証やパフォーマンス管理も含まれます。GRCのアプローチが適切に実施されれば、意思決定の俊敏性と信頼性が向上し、コスト、重複部分、および影響を受ける運用が削減され、信頼性の高いパフォーマンスが持続し、価値が実現されます。

PCIセキュリティプログラムをGRCと統合する価値

ベライゾンは、2022年版のPSR（21ページ）で GRC²モデルを開発し、公表しました。すべてのGRC活動が同期して統合されることで、効率性が向上し、企業にとって最終損益の財務上のメリットにつながります。

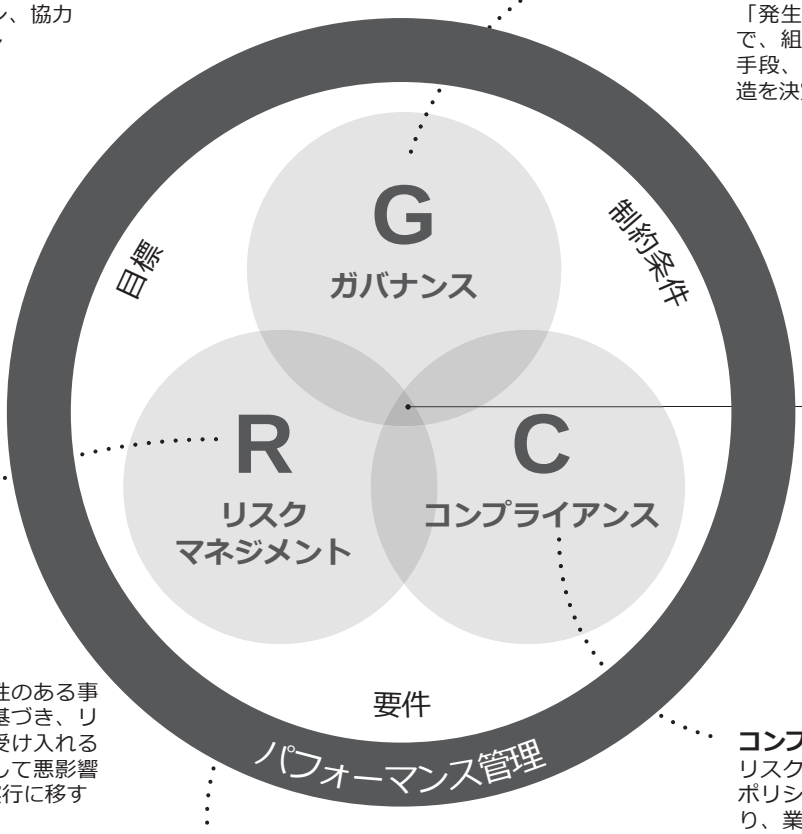
PCIセキュリティプログラムは、その大枠となる企業のガバナンス、リスク管理、およびコンプライアンスの取り組みと完全に統合されていますか？

GRC² モデルの相互作用

GRCを構成する3つのプラクティスでは、共通の相互に関連するタスクを共有し、責任とプロセスの領域が重複しています。これらは統合され、複合的なプラクティスとして扱われることで、効果が高まります。

GRC
組織の管理とコントロールにおいて、さまざまなステークホルダー間における基準の統一化、コミュニケーション、協力を促進するマネージメントモデル

ガバナンス
選択した戦略（パフォーマンスと成果）への「リスク対策」とその運用からの「発生リスク」を統合的に管理することで、組織の目標と目的、それを達成する手段、結果を監視する手段を定義する構造を決定する



リスクマネジメント
企業資産に悪影響を及ぼす可能性のある事象や状況の特定、評価、予測に基づき、リスク（脅威、脆弱性、影響）を受け入れるか、リスク対策の選択肢を適用して悪影響を軽減するかの意思決定を行い実行に移す

コンプライアンス
リスクを軽減するための戦術的な行動。ポリシー、基準、手順の伝達と実施により、業界規制と政府の法規制の両方を遵守する

パフォーマンス管理
評価、報告、是正、改善を通じて戦略目的の達成を支援する継続的なコミュニケーションプロセスであり、目標、目的、要件、制約の緩和（GRCの各ドメインにおける重要なタスク）を明確に規定する必要がある

図2

GRC²モデルの詳細については、2022年版PSRの20～24ページをご覧ください。

統合プログラム設計

ツール、モデル、手法の価値

プログラムの設計においてツール、モデル、手法が重要である理由

多くの組織にとって、PCIセキュリティとコンプライアンスに取り組む過程の大部分は、一連のバラバラな活動から正式なプログラムの作成に移行することです。組織のセキュリティの一連の取り組みやポリシーの方向性が固まっていないと、必然的にコンプライアンスが低下し、コントロールの効果が減少し、情報漏洩のリスクが高まります。これを回避するためには、最高情報セキュリティ責任者（CISO）は、明確なコミュニケーションと強力な指導力に支えられた機動的なリーダーシップと体系化されたガバナンスを提供する必要があります。前進するための再編成のプロセスにおいては、モデルや手法の活用が重要な役割を果たします。

セキュリティプログラムは、事前プランニングをほとんど行わず、後手の対応でその場しのぎに開発されることが多々あります。定義が十分になされたプログラムは、包括的なプログラム目標を達成するためにどのように意思決定を行い、資源を配分するかについての指針となります。

プログラムおよびプロジェクトの設計と管理は、PCIセキュリティを成功させるための基本的なスキルとプロセスです。プログラムを設計することが重要なのは、プログラムを全体として効率的に実行するすべての部分に影響を与えるためです。プログラムおよびプロジェクトの設計は、通常、PCIセキュリティコンプライアンスの運営委員会、プロジェクトマネージャー、および主要なステークホルダーによって実施される初期のプランニング段階を指します。このプランニング段階では、成功を確実にするための重要なプロジェクト要素を策定します。

戦略は、プログラムを前進させる中心的な役割をはたします。セキュリティは、目先の小さな目標を掲げた短期的なプロジェクトではなく、組織のセキュリティ態勢を向上させる使命、目的、および戦略を備えた長期的なプログラムへと進化させる必要があります。CISOの主な目的には、多くの場合、連携と組織全体のリソースを活用した情報セキュリティプログラムの策定、情報セキュリティガバナンスの促進、セキュリティの方向性とリソース投資に関するシニアリーダーシップへの助言、情報セキュリティリスクを管理するための適切なポリシーの策定などが含まれます。

PCIセキュリティプログラムは、プログラムのライフサイクルを通じて予測可能なパフォーマンスを実現するように設計する必要があります。そのためには、明確に定義された目標に向けてリソースを投入し、マイルストーンと重要な成功要因を含む経済的なロードマップを確立する必要があります。設計が優れたプログラムは、作業効率を高め、目標を達成し、社内外のステークホルダーが毎回望むものに応えます。これは、資源の無駄をなくし、生産性の低さに対処し、過剰なコストを抑制し、ステークホルダーの不満を回避するためのソリューションです。

設計の優れたPCIセキュリティプログラム

- プロセスとシステムの開発および管理を実質的にサポートする
- 活動を設計および実行する各段階を指示し、コントロールするために、さまざまな手法を活用する
- プログラム管理者と参加者の基礎となる合理的な立場をどのように確立するかだけでなく、人々がいつどのようにコミュニケーションし、意思決定を行うかを決定する

統合セキュリティプログラムの設計モデルと手法

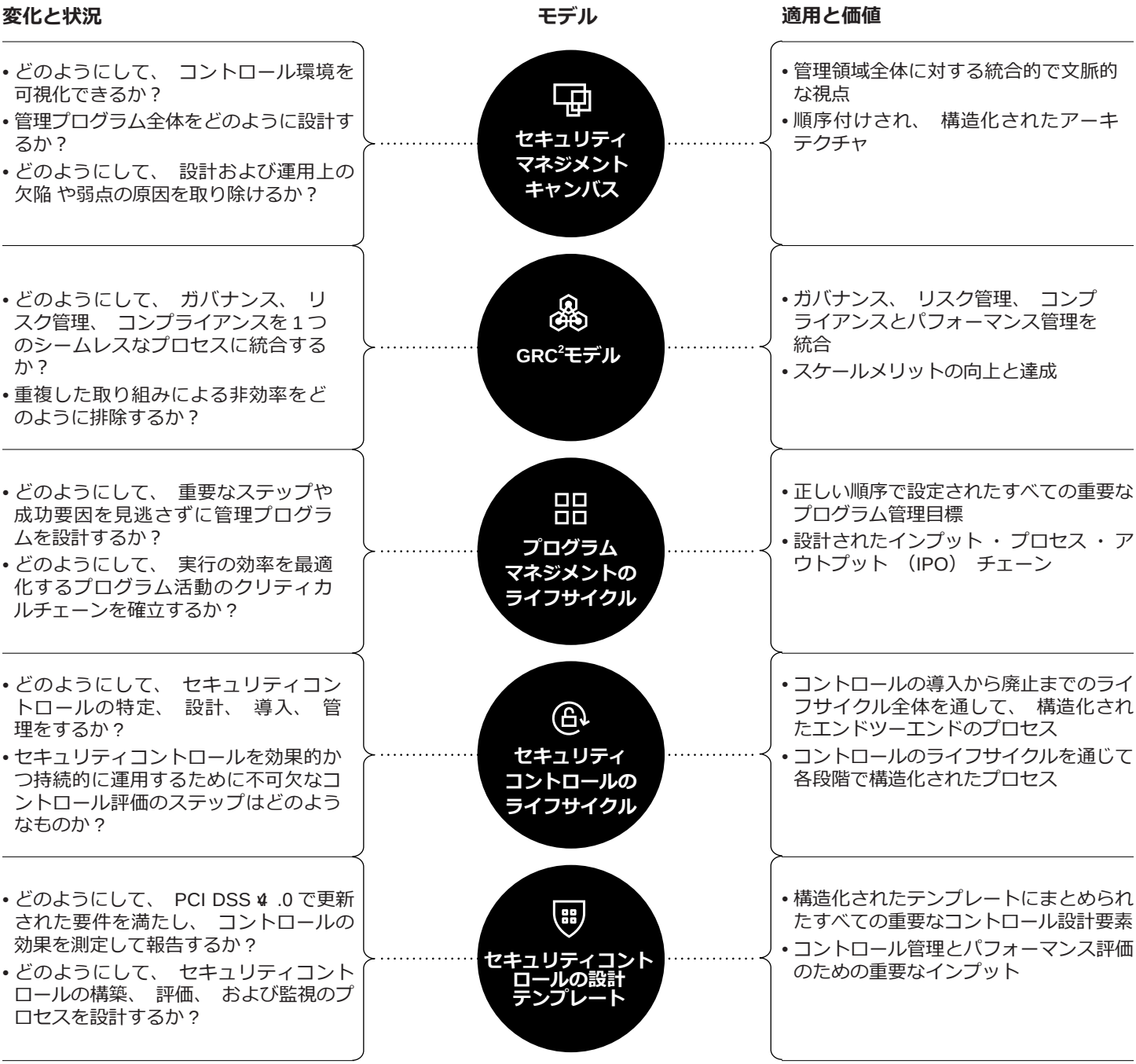


図 3

プログラム管理設計における誤り

セキュリティコントロールプログラムを設計する際に、組織は次のような誤りを犯しがちです。

- コンプライアンスプログラムを策定する際に、ステークホルダーに早期の賛同を得ることを怠る
- 目標および望ましい成果（コントロール環境の持続可能性及び実効性の組み込みを含む）を明確にしない
- プログラムではなくプロジェクトを設定し、プログラムの成果ではなくプロジェクトの成果を重視する
- セキュリティプログラムの包括的な性質と複雑さを過小評価し、継続的なプログラム支援に必要な能力を確保しない
- 明確なプログラム目標の設定を怠り、コンプライアンスに重点を置き、効果的なデータ保護に重点を置かない
- 持続可能なプロセスの構築を怠る
- 組織の縦割りを維持することで、コミュニケーション、パフォーマンス、持続可能性を阻害する
- テクノロジーに重点を置き、プロセスや手順を軽視する
- 忘れる、投資しない、急いだ結果、組織の能力開発が不十分
- トレーニングや教育への取り組みが不十分

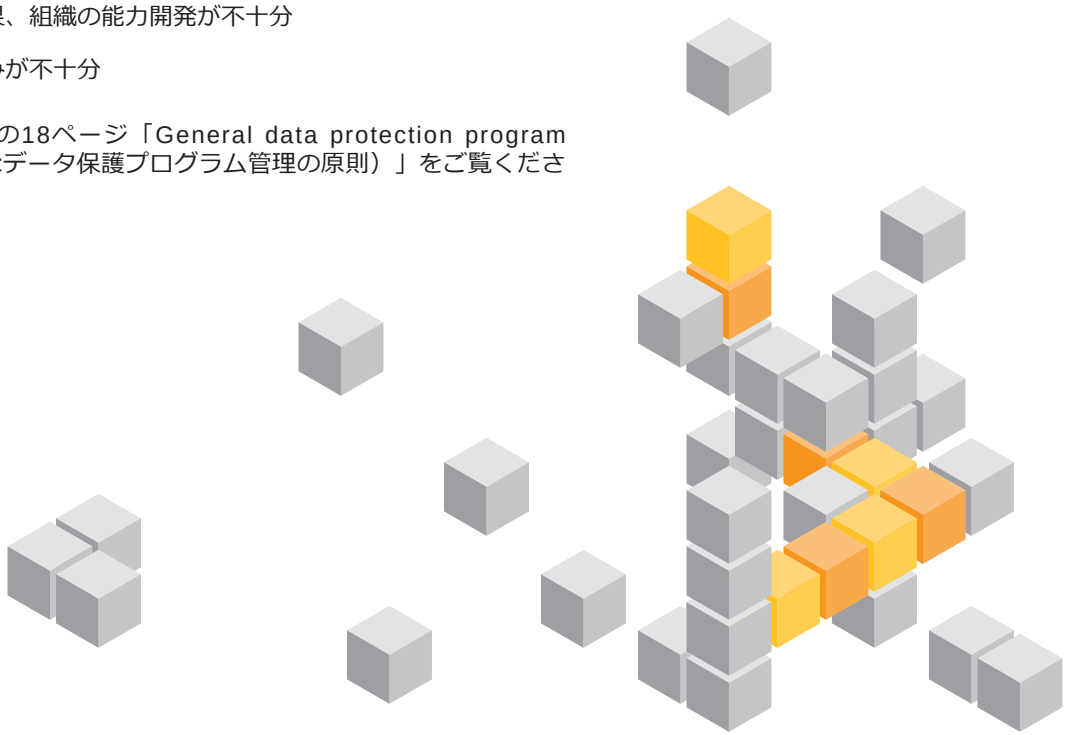
詳細については、2019年版PSRの18ページ「General data protection program management principles（一般的なデータ保護プログラム管理の原則）」をご覧ください。

プログラム改善の取り組み

PCIセキュリティプログラムのパフォーマンスと結果を改善する方法は次の2つだけです。

- プロセスの手順またはステップを改善する。
- 人的要素も含め、その手順で使用されるコンポーネントを改善する[9]。

これ以外の方法はありません。コンポーネントと手順の改善を論理的に統合する方法を適用すれば最良の結果が得られます。



9 Ron Carroll, “Box Theory™ for small business—create high-performance systems,” accessed August 7, 2023, https://www.boxtheorygold.com/blog/box-theory-for-small-business-create-high-performance-systems

コントロール環境

効果的な持続可能なコントロールの達成は、全体的なコントロール環境に依存することを知ることが重要です。全体的な環境の影響を方程式に含めずに、コンプライアンス環境を改善できると考えてはなりません。PCIセキュリティコンプライアンスのサブシステムが、そのサブシステムが運用される大枠となるシステムとどのように関連しているかを把握する必要があります。これには、システム思考の適用が必要です（2022年版PSRの 9ページと71ページを参照）。

組織のコントロール環境は、管理システム全体に広範な影響を及ぼします。プログラムパフォーマンスのほとんどの側面は、大きなコントロール環境内の他のコンポーネントから直接的または間接的に影響を受けています。コントロール環境レベルでのテストの設計と実行は複雑で困難な作業になることがあるため、多くの組織では下位レベルのサブ環境のみに重点を置いています。

PCIセキュリティのコントロール環境の定義

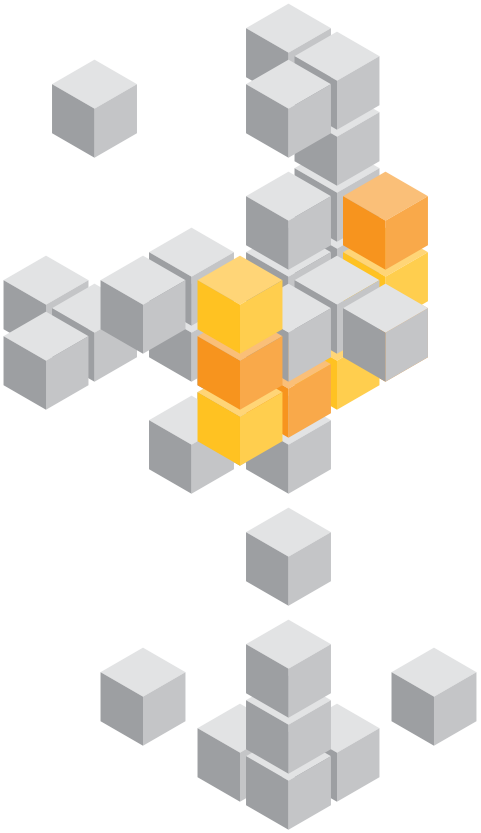
PCIセキュリティコンプライアンス環境が運用される全体的な大規模システムを説明するために、コントロール環境が言及されることがよくあります。コントロール環境とは、組織全体で内部コントロールを実施するための基盤となる構造と基準を備えた継続的な管理プロセスです。コントロール環境は明確に定義され、ドキュメント化され、コミュニケーションされ、評価され、維持されなければなりません。包括的であるということは、環境を管理するために経営陣がとるすべての行動、戦略的ガバナンスと業務上の日々の活動管理、すべての参加者、方針、基準、手順、ツール、プロセス、ドキュメントが含まれるということです。

コントロール環境：環境全体ーコンプライアンス環境とデータのセキュリティに影響を及ぼすすべての環境とコンポーネントを組み合わせたもの

コンプライアンス環境： PCIセキュリティコンプライアンス環境全体ーコンプライアンスと検証の範囲に含まれるすべてのコンポーネント（複数のセキュリティ規格の要件を含む）

カード会員のデータ環境（CDE：Cardholder Data Environment）： 中核となるペイメントアカウントデータの保存、送信、および処理環境

図4. 対象範囲となる環境全体のマッピング



これら3つの環境は、統合コントロールシステム全体を構成します。それぞれの環境について、以下に簡単に説明します。

1. コントロール環境

コントロール環境は、広範で全体的な環境であり、外部コントロール環境と内部コントロール環境の両方を含みます。全体的なコントロール環境のパフォーマンスと成熟度は、そのサブ環境のパフォーマンスに直接影響し、多くの場合、決め手となります。

外部コントロール環境
この環境には、組織内の状況に対して影響力を行使できるすべての外部主体が含まれます。例えば、各ビジネスには、そのビジネスやコンポーネント（人、プロセス、文書化、ITシステム）の側面に影響を与えたり、影響を与えうる様々な外部主体が存在し、組織の内部コントロール環境にも影響を与えます。

内部コントロール環境
内部コントロール環境は、組織全体で内部コントロールを実施するための基盤となる一連の構造、方針、プロセス、基準によって内部で管理されます。内部コントロール環境には、組織内部の方針、基準、手続を遵守するために適用するすべてのコントロール活動、情報伝達、リスク評価、監視活動が含まれます。この環境には、通常、より広範なガバナンス、リスク管理、コンプライアンスの範囲、すなわちPCIセキュリティ、および組織が遵守しなければならないその他の規制が含まれます。

実効性のあるコントロール環境

有能な従業員は、実効性のあるコントロール環境における自身の責任と権限の限界を理解しています。彼らは、知識が豊富で、心がけがよく、正しいことを正しい方法で行うことを守ります。効果的なコントロールシステムは、どこで失敗が起きているのか、その失敗の責任は誰にあるのかを迅速に特定し、情報を公開します。それにより、是正措置が確実に取られ、パフォーマンスを測定、報告され、継続的に改善が行なわれます。

2. コンプライアンス環境

この環境には、すべてのコンプライアンスコンポーネント（システムコンポーネントおよびコンプライアンスと検証の範囲内にあるその他のコンポーネント）が含まれます。CDEに含まれるものもあれば、接続されたセキュリティに影響を与えるシステムコンポーネントなど、CDEに含まれないものもあります。

コンプライアンスの範囲：この範囲には、PCI DSS 管理要件の対象となるすべての該当するシステムコンポーネント、人、およびプロセスが含まれます。CDEに加え、その他の対象コンポーネントとして以下のものが含まれます。

- アカウントデータまたは「保存（Store）、処理（Process）、送信（Transmit）」（SPT）コンポーネントのセキュリティに影響を与える可能性のあるすべてのコンポーネント
- SPTコンポーネントのコンプライアンスに必要なコンポーネント
- SPTコンポーネントに直接接続できるシステムコンポーネント
- SPTコンポーネントに間接的に接続できるシステムコンポーネント
- 任意のSPTコンポーネントに無制限に接続可能なシステムコンポーネント
- CDEシステムを対象外システムからセグメント化するシステムコンポーネント

検証の範囲：この範囲には、コンプライアンスの範囲に含まれるか含まれないかに関係なく、システムコンポーネント、人、およびプロセスへの適用が必要とされるすべてのコンプライアンス検証の評価タスクが含まれます。例えば、外部評価の段階では、認定セキュリティ評価機関（QSA：Qualified Security Assessor）は、定義済みのコンプライアンス範囲から除外されている場合でも、さまざまなコンポーネントをサンプリングすることが求められます。これは、要求される範囲とコンプライアンスの基準がすべて満たされていることを確認し、定義済みの範囲が正確であることを検証し、 すべてのコンポーネントのコンプライアンスを確認するためです。検証範囲は常に、コンプライアンス範囲よりも大きく、多くのシステムコンポーネントを含みます。コンプライアンス範囲に含まれるシステムはすべて、自動的に検証範囲にも含まれますが、その逆はありません。

3. カード会員のデータ環境（CDE）

CDEは、PCI DSSコンプライアンスと検証の範囲において中核となるペイメントアカウントデータの保存、送信、および処理環境です。CDEには、ペイメントアカウントデータ（カード会員のデータまたは機密認証データ）を保存、処理、または送信するすべてのシステムコンポーネントが含まれます。

コンプライアンス環境

コンプライアンス環境には、ペイメントカードデータのセキュリティコンプライアンス環境の広範な組織全体の範囲を構成する他のPCIセキュリティ基準（DSSを除く）の要件の対象となるコンポーネントも含まれる場合があります。これは、ペイメントカードのアカウントデータのセキュリティとPCI DSS要件への準拠のための準備に必要な範囲内のコンポーネントの本体を示すものです。

コンプライアンスの範囲を縮小するために、組織はCDEに不必要なシステムコンポーネント、人、およびプロセスを含めないようにする必要があります。このようなコンポーネントでも、コンプライアンス範囲から除外することの妥当性を実証および確認するために、検証範囲に含める必要があることがよくあります。

コントロール環境の持続可能性

持続可能なセキュリティおよびコンプライアンスとは、将来の目標と目的を達成する能力を損なうことなく、現在のニーズを満たすコントロール環境を開発することと理解されます。

2022年版PSRの主な調査結果（82ページ）によると、持続可能なコントロール環境を維持している組織は半数以下（約43%）となっています。多くの組織が、PCIセキュリティプログラムの強度を効果的に測定する方法を理解していません。コントロール環境とセキュリティコントロールは、整備せずに放置しておくと劣化する傾向があります。パフォーマンスの監視と測定を行なわない組織は、パフォーマンスの基準から逸脱していることに気付かないことがよくあります。また、プログラムのパフォーマンスを測定できる基準や、プログラム評価を実行するための効果的な方法がない場合もあります。この欠陥は通常、次のような一連の望ましくない結果をもたらします。

- コントロール環境の持続可能性が規定されていない、ドキュメント化されていない、または不明である。
- 目標が、持続可能なコントロールの実効性に向けてプログラムを推進しない。
- 能力の成熟度が不明、または理解が足りない、改善への道筋が不明確である。
- 個々のコントロールおよびコントロールシステムの効果が不明、規定されていない、またはドキュメント化されていない。
- コントロールシステムではなく、個々のコントロールの管理が行われており、コントロールシステム（特定のコントロール目的を サポートする関連するコントロールのグループ）が特定されていない。
- コントロールのパフォーマンス能力が不確実であり、測定されておらず、報告されていない（重要な監視の欠如）。
- 予測不可能なセキュリティコントロールの機能不全が発生する。
- コントロールの障害に対する対応と復旧が構造化されておらず、 結果が不確実である。

このニーズに対応するため、ベライゾンは2018年版PSR（4～23ページ）で「9 Factors of Control Effectiveness and Sustainability（コントロールの実効性と持続可能性の9つの要因）」を公表しました。この重要なモデルは、組織が PCIセキュリティプログラムの持続可能性と効果を判断するための統合評価フレームワークを適用するのに役立ちます。このフレームワークにより、高度に構造化され、反復可能で一貫性のある方法でPCIセキュリティプログラム全体の盲点を特定することができます。また、内部および外部のコントロール環境と、リスクを軽減するために必要なコントロールを定義および監視するための重要なインプットを得るプロセスを容易にします。同時に組織は、コントロールのパフォーマンス、データ保護の実効性、および持続可能性に影響する制約を特定および定義し、コントロール環境の設計および運用に関するパフォーマンス要件および基準を定義およびコミュニケーションする必要もあります。

管理の持続可能性

すべての重要なコントロールは、効果的であることに加え、コントロールの目標を確実に達成するために持続可能である必要があります。すべての重要なセキュリティコントロールシステムが、適用されるコントロールのすべての目標を長期にわたり一貫して満たせているか監視し、頻繁に測定し、報告することが重要です。このように要求されるセキュリティコントロール性能のレベルは、重要な管理システムが構成や機能仕様の基準から著しく逸脱することなく維持される必要があります。

セキュリティコントロールシステムが達成できる持続可能性のレベルは、コントロール環境とどの程度整合性がとられ、統合されているかに大きく依存します。したがって、コントロール環境の持続可能性は、環境内のコントロールの持続可能性に直接影響します。

必要なパフォーマンスと効果を維持するために必要とされる労力と資源（コスト、人、注意、時間）の量を追跡することは、コントロールの持続可能性の重要な指標となります。 また、環境全体にわたるすべての重要なプロセス領域においてキャパシティ、能力、資質、コミットメント、コミュニケーションなどの要件がどれだけ満たされているか監視することも欠かせません（26ページ「コントロール設計テンプレートの必要性と価値」を参照）。

持続可能なプログラム設計のためのガイダンス

一般に、持続可能性の問題は、プログラムの様々な段階でもたらされることがあります。 詳細については、22ページの「PCIセキュリティプログラム管理のライフサイクル」をご覧ください。

持続可能なコンプライアンスとデータ保護を実現するには、ワークロードの量とタスクの複雑さという二つの課題を管理し、積極的に対処する必要があります。ワークロードの量が処理能力を上回ったり、コンポーネント間の因果関係が複雑過ぎて理解し管理する能力を越えたりすると、持続可能性に直接影響します。

管理可能なコンプライアンスとデータ保護を実現するためのルール：

- コンポーネント（情報、システム、タスク）の量が、それをタイムリーに処理するための人材やシステムのリソース能力を超えないようにする。
- タスクの複雑さが人やシステムの能力や適性を超えないようにする。

量的な問題を管理するためのステップとして、よくあるのは以下のような手法です。

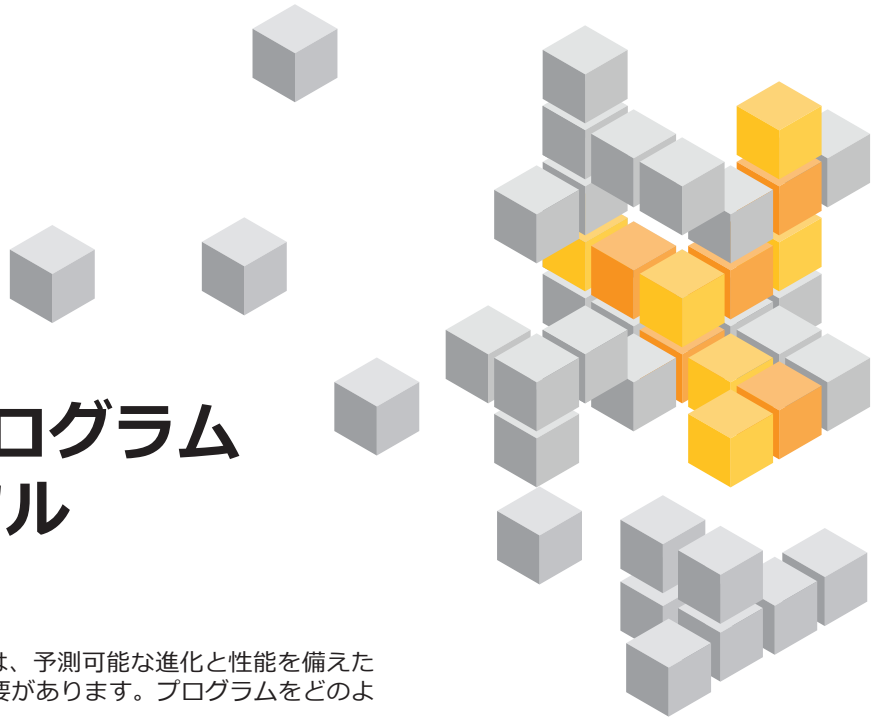
1. **業務範囲の縮小**
可能な限り業務範囲を調整および縮小し、コントロール環境に関連する作業量を削減する。

2. **自動化**
テンプレートを活用し、作業ルーチンとワークフローを確立する。可能な限り多くの作業を自動化し、手作業による入力を減らす。

3. **集中化**
プログラムの目標達成に貢献する仕事のみに取り組む。

4. **投資**
利用可能なリソースを増やす（より多くの人を雇うか、第三者に委託する）。

一般的に、複雑さをめぐる問題のほとんどは、分析とコミュニケーション、そして構造化された方法による作業を通じて解決することができます。そのため、コンプライアンスプログラムを構造化された変更管理プロセスに統合することは、持続可能性を達成する上で非常に有益です。



PCIセキュリティプログラム管理のライフサイクル

プログラムアーキテクチャ

高性能なPCIセキュリティプログラムを実現するには、予測可能な進化と性能を備えたプログラムを設計し、設計によって成功を収める必要があります。プログラムをどのように構築するかが重要です。

すべてのプログラムには、重要な要素と基本的なコンポーネントがあります。プログラムのパフォーマンスが低下する根本的な原因に対処するには、プログラムにこれらの重要なコンポーネントがすべて含まれている必要があります。各コンポーネントの間には、一方向または双方向の依存関係があり、プログラムのライフサイクルの様々な段階で焦点となります。すべてのプログラムには、構想段階から最終段階の完了に至るまでのライフサイクルがあります。ライフサイクルは、プログラムのパフォーマンスを提供し、持続可能性を向上させるための重要な要素です。

図5に示す視覚モデルを使って、プログラム活動がどのように構成されるべきか、また、構想から完了までのワークフローがどのように進行するかという視点を確保することができます。

プログラムのライフサイクル管理

セキュリティコンプライアンスプログラムは、次のような段階を定義したプログラムのライフサイクル管理を行ないます。

1. **構想化と開始**
2. **定義とプランニング**
3. **立ち上げと実行**
4. **パフォーマンスと管理**
5. **継続的改善**

プログラムはそれ自体で存在し、実行するものではありません。プログラムは作られるものであり、そのパフォーマンスは、プログラムがどのように設計され、組織の他の部分とどのように相互作用するかの結果です。したがって、プログラムのアーキテクチャ（コンポーネントの構成と関係、実行順序）を作成するために適用されたプログラム構造とアプローチは、非常に重要です。明確で周知の依存関係と因果関係が、プログラムの効果、実行効率、成果を決定します。

プログラムのライフサイクルは、プロジェクトのライフサイクル管理とよく似ていますが、本質的な違いがあります。プログラムとプロジェクトの違いは、プロジェクトの期間がプログラムよりも比較的短いことです。

ライフサイクルの主要な3段階

1. **第1段階：プログラムのプランニングと設計段階**
これはプログラムの構想と開始であり、これに続いて作業の範囲を決めるプランニング活動が行われます。

2. **第2段階：プログラムの実行と管理段階**
プログラムが開始されると、作業のパフォーマンスを管理およびコントロールするための構造化された事前定義済みの手法が必要となります。これには、関連するすべてのプロジェクトにおける業務範囲、リソース容量、その他の主要な測定基準のコントロールが含まれます。

3. **第3段階統合プログラムのパフォーマンス評価と改善段階**
プログラムの立ち上げ後に開始され、プログラム管理と並行して実行します。プログラムの効果と効率性を測定する必要があります。プログラムの成果物の品質をレビューし、能力とプロセスの成熟度を評価します。

プログラムおよびプロジェクトのライフサイクル管理は、PCIセキュリティプログラム管理の統合された部分であり、そうあるべきです。これは、パフォーマンスの優れたプログラムを実現するためのソリューションの一部です。プログラムのパフォーマンス、プログラムによって一括管理されるプロジェクトの集合体、および全体的な成果と目標に向けた目的（スループット）の達成率は、各ライフサイクル段階における設計と実行の品質に直接依存します。

プログラムの成功を目指すのであれば、ライフサイクル管理を無視すべきではありません。これらの段階のいずれかをスキップすると、最終的に悪影響を及ぼすことになります。

1 プログラムのプランニングと設計		2 プログラムの実行と管理		3 評価と改善	
構想化と開始	**定義とプランニング**	**プログラムの立ち上げ**	**プログラムのパフォーマンスと管理**	**プログラムの効果**	**プログラムの効率**
プログラムオフィス プログラム憲章 – 目的 – ステークホルダー – 前提条件 – リスク プログラムの承認	プログラムプラン – プログラム目標 – 要求事項 – 目的 – 制約事項 業務範囲 – 作業切り分けスケジュール 予算 リスク管理	コミュニケーション プログラムとプロジェクトのキックオフ ステータスとトラッキング 品質 予測	マイルストーンと目標 実行と成果パフォーマンス – スループット 監視と報告 管理 – 範囲 – リソース – 制約 – インプット：時間と労力 – 予算	プログラムの成果評価 – 成果物の品質 プログラムプロセス評価 – 能力の成熟度 – プロセスの成熟度 プロジェクトのパフォーマンス評価 – プロジェクトの事後評価 プログラム設計の評価 継続的改善	

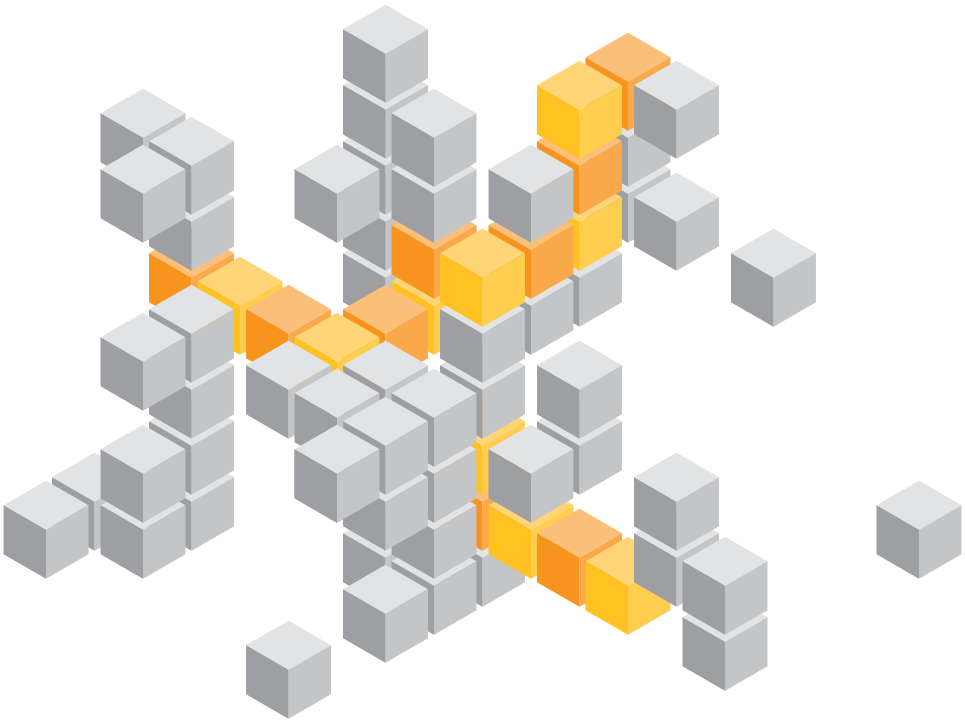
図 5.PCIセキュリティプログラム管理のライフサイクル

セキュリティコントロールのライフサイクル

プログラム管理のライフサイクルに加え、プログラムの設計にもセキュリティコントロールのライフサイクルを組み込むべきです。

ベライゾンは、2016年版PSR[10]（7ページ）でセキュリティコントロールのライフサイクルフレームワークを公表し、2017年版[11]（10ページ）で更新版を再公表し、2018年版PSR（17ページ）でフレームワークを拡張しています。

データは常に何重ものセキュリティによって保護される必要があります。セキュリティコントロールがライフサイクルの各段階でどのように管理されているかによって、データの暴露や潜在的なデータ侵害を引き起こすコントロールリスクの可能性が決まります。コントロールのライフサイクルに関する理解不足は、コントロール環境の萎縮につながる要因となります。これは、最終的にセキュリティ侵害やデータの漏洩につながりかねません。データの漏洩/侵害は、複数のセキュリティコントロールが存在しないか、または失敗したために発生します。コントロールが失敗するのは、設計、運用、またはメンテナンスに弱点が存在する結果です。多くの場合、これは効果のないコントロール環境の結果です。したがって、組織は、コントロールのライフサイクルの各段階が、基盤となるプロセス、運用効率、セキュリティコントロールの効果にどのような影響を与えるかを理解することが不可欠です。



10 "2016 Payment Security Report," Verizon, 2016, https://www.verizon.com/business/resources/reports/2016-verizon-psr-mainreport.pdf
11 "2017 Payment Security Report," Verizon, 2017, https://www.verizon.com/business/resources/reports/2017-payment-security-report-en.pdf

セキュリティコントロールのライフサイクル

構想化：セキュリティコントロールのライフサイクルの第1段階でリスクを軽減したり、または要件を満たすために、新しいコントロールの必要性、または既存のコントロールの適用可能性が認識されます。コントロールの意図と関連するコントロールの目的が明確にされ、共有されます。

設計と構築：第2段階では、コントロールまたはコントロールシステムの正確な目的と機能のパラメータが定義されます。これには、コントロールの依存関係とコントロールシステムの定式化が含まれます。 コントロール設計プロファイルテンプレートについては26ページをご覧ください。

コントロールのテスト：ドキュメント化されたコントロールのテスト基準と手順を適用して、コントロールがその対象となるコントロール環境内での実際の運用において、事前定義済みの機能仕様および運用仕様をどの程度満たしているかを評価、テスト結果をドキュメント化します。

実装と展開： コントロールまたはコントロールシステムを段階的に実装し、導入を広げていきます。導入したコントロールが最初から完璧に機能することはほとんどないため、展開中および展開後に不備な点を是正するための調整が必要になる可能性が高くなります。

運用と監視：この体系的な監視では、コントロールとパフォーマンスのそれぞれの目標が達成されているかどうかを判断するために、状況とパフォーマンスのデータを長期にわたって収集し、保存と報告を行ない、コントロール活動を監視します。

コントロールのメンテナンス：このコントロールシステムの運用では、計画的、予測的、予防的、是正的、または適応的なコントロールメンテナンスによって、基準に沿ったコントロールの運用を維持します。コントロール環境の変化による影響を低減し、変化に適応させます。

改善と進展：コントロールシステムの設計、統合、運用を強化するために、コントロールに修正や改良を加えます。これにより、コントロールの運用における効率性と効果、および環境コンポーネント間の連携動作を改善します。

コントロールの成熟度： 成熟段階では、コントロールシステムが確立され、機能要件と運用要件を満たし、妥当なレベルの堅牢性と回復力を備えた実績を確立します。継続的な改善が可能な設計と運用をコントロールします。

機能低下と改廃：コントロールの有用性が低下して役目が終わった場合、またはより効果的または効率的なコントロールに置き換えられる場合に、運用環境にあるコントロールを交換または終了します。

図6. セキュリティコントロールのライフサイクル（2018年版PSR、17ページ）

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上で大いに役立ちます。コントロールの導入、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。

基本的なレベルでは、通常、PCI DSSのコントロールプロファイルドキュメントには、以下の項目が記載されています。

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記述します。
コントロールの責任者
担当や責任を割り当てます。
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。
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。
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。
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。
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または参照します。
実装
実装の範囲、コントロール、手順の実装、依存関係について規定します。
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。
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。
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。
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。

図 7

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、2018年版PSRの12ページおよび 2022年版PSRの60ページをご覧ください。

効率性と実効性

多くの組織では、PCIセキュリティプログラム管理のアプローチにおいて効率性が過度に重視されています。こうしたアプローチでは、PCIセキュリティ要件の実装状態を最短時間で測定し、奨励する傾向があります。このため、「チェックボックス」的なアプローチになりがちで、真に実効性のあるコントロール環境を構築できない場合があります。

PCIセキュリティのアプローチでは、効率性と実効性を区別することが重要です。

- **効率性**
  時間、労力、リソースの無駄が最も少ない最適化された方法で特定のタスクを実行すること
- **実効性**
  時間の長さにかかわらず、必要な結果を得るために適切なタスクを実行し、多くの価値を提供または優れた成果をあげる、より良い結果を生み出す能力

つまり、実効性とは正しい仕事をすることであり、効率性とは仕事を正しく遂行することです。いずれの場合も、正しい成果とは何か、どのような仕事をすべきかを定義できるという前提が必要になります。

そして、どちらか一方だけというわけでもありません。まず実効性があることを心がけるべきですが、時間やリソースをどれだけ効率良く使っているかについても心に留める必要があります。間違った仕事を効率的にこなすのは時間の無駄であり、正しい仕事を効率的にこなすことが成功の秘訣です。

効率的なチームを作るには？

- 最小限の時間と労力で最大のアウトプットを引き出すことに集中する。
- 秩序の整った作業プロセスを用いる。
- ルールを定義し、それに従う。
- 標準化と自動化を受け入れる。

効率性は高くとも実効性のないチームは、期限の厳守とチェックボックスのチェックに時間をかけすぎているのかもしれません。適切なプロジェクトに優先順位をつけずに、このようなことをしている可能性があります。チームは、何をすべきかを特定する（正しい目標と目的を確立する）必要があります。その上で、仕事をより効率的に進めるために、プロセスを最適化するための投資を行うべきです。効率性の向上は、アウトプットのスピードと量を増加させます。しかし、それでも良い結果にならないことがあります。効率重視は、達成すべき目標から目をそらすことにもなりかねません。組織のセキュリティおよびコンプライアンスの目標を達成するためのものでない作業は、実際には重要なものでないことに注意してください。

データセキュリティの7原則

データセキュリティの原則を理解することの価値は計り知れません。成功するPCIセキュリティプログラムを設計および管理するための基本原則として以下のものが挙げられます。

- 成功は運ではなく、設計によって達成される。
- どのコントロールも、ただ存在するだけでなく、有効でなければならない。
- コントロールには依存関係があり、単独ではなくコントロールシステムとともに機能する。
- コントロールが持続可能であるためには、そのコントロール環境も持続可能でなければならない。
- 運用のパフォーマンス指標を測定し、報告すること。
- すべてのコアプロセスのインプット、アクティビティ、アウトプットは、パフォーマンスの低下をタイムリーに検出、防止、修正できるよう、一貫性があり、予測可能なものでなければならない。
- 適切なプロセスと能力の成熟に向けて、継続的な改善がなされる必要がある。

これらの基本原則をおろそかにしてはなりません。

出典：2020年版PSR、14ページ

実効性のあるチームを作るには

- 正しいことを正しい方法で行うことに集中する。
- 成果主義を貫く。
- 全体像に集中する。
- 必要に応じて優先順位を変える。

実効性があるとは、最良の成果が動的な目標であることを理解することです。そのためには、先を見越して、最良の結果を得るためにどこにリソースを投入すべきかを判断する必要があります。実効性のあるチームは、その影響力が最大となる場所に時間とエネルギーを投資します[12]。実効性を向上させることで、目標とする結果の達成も加速します。しかし、生産プロセスの効率が低いと、達成速度が遅くなる可能性があります。間違った方向に速く進みたいのか、それとも正しい目的地に向かってゆっくり進みたいのか、検討が必要です。

戦略的データセキュリティ管理における7つのトラップ

データセキュリティに持続可能性と実効性が欠けるのは、ビジネス、戦略、運用アーキテクチャの設計と実行が不十分であることが主な原因です。（これらのトラップの詳細については、2020年版PSRの12ページと22～61ページを参照。）これらの障害に対処することは、強力なコンプライアンスブリッジを構築するだけでなく、必要に応じて適応できるプログラムを構築することになります。

トラップ1	**リーダーシップに欠ける**
トラップ2	**戦略的支援を確保できない**
トラップ3	**リソーシング能力の欠如**
トラップ4	**健全な戦略設計ができない**
トラップ5	**戦略の実行力に欠ける**
トラップ6	**能力とプロセスの成熟度が低く、継続的な改善ができない**
トラップ7	**コミュニケーションと企業文化に制約がある**

バランスをとる―効率良く実効性を高める

やるべきことが多い組織は、生産性を高めることの価値を理解しています。セキュリティチームとコンプライアンスチームは、より効率的であることに努め、日々のToDoリストの項目をできるだけ多くチェックし、短時間により多くのことを処理したいと考えていますが、目標の達成に貢献する作業を優先する（すなわち、効率性よりも実効性を優先する）必要があります。

すべてのPCIセキュリティプログラムは、効率性よりも実効性を優先するように設計する必要があります。

最終的に、チームは効率良く効果を高めるように努力する必要があります。これは、正しいことを適切に実行し、効率性と実効性のバランスを正しく保つことを意味します。

12 Maggie Wooll、『Still chasing efficiency?Find out why effectiveness is a better goal』、BetterUp、2022年 https://www.betterup.com/blog/efficiency-vs-effectiveness

以上で、先進のペイメントセキュリティプログラムの設計に関して簡潔にまとめたレポートを終わります。先進のセキュリティプログラムの評価について詳しくは、Verizon Payment Security Practice（paymentsecurity@verizon.com）までお問い合わせください。

Verizon 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サービスは、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。

決済システムのセキュリティに関するレポート（PRS）

すべてのPSRをhttps //www.verizon.com/paymentsecurityreportからご覧いただけます。

ベライゾン2023 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

先進のペイメントセキュリティプログラムの設計に関するホワイトペーパー

発行日：2023年8月

編集チーム

筆頭著者
Christian Oostenen

筆頭編集者
Cynthia B. Hansen

Verizon Cyber Security Consulting

セキュリティ担当マネージングディレクター
Kristof Philipsen

アソシエイトディレクター、グローバルGRCリーダー
Samuel Rinkin

Payment security consulting practice

グローバルリード
Sebastien Marais

米国
Matt Arntsen

APAC
Ferdinand Delos Santos

EMEA
Loic Breat

グローバルビジネスインテリジェンス
Christian Oostenen

法務レビュー
Richard Cooper
Sudha Kantor

チームのメールアドレス
paymentsecurity@verizon.com

verizon

verizon.com/paymentsecurityreport