補足情報

# PCI DSS v4.x:補完的コントロールおよびカスタマイズされたアプローチに関するガイダンス

バージョン:1.0

日付：2026 年 6 月

著者：PCI Security Standards Council

# ドキュメントの変更

| 日付 | バージョン | 説明 |
|---|---|---|
| 2026 年 6 月 | 1.0 | 初回リリース |

*免責事項：本文書の英語版は、PCI SSC ウェブサイト上で利用可能になっており、全ての目的において、これらの文書の正規版と見做される。本記述と英語版記述との間に曖昧もしくは不一致がある限りにおいては該当部分に相当する英語版が優先される。*

# コンテンツ

# 概要

Payment Card Industry Data Security Standard（PCI DSS）は、セキュリティ目標を達成する手法において柔軟性を認めています。PCI DSS v4.x には、PCI DSS のコントロールを実装と検証のための 2 つのアプローチ、すなわち「定義されたアプローチ」と「カスタマイズされたアプローチ」が含まれています。これら 2 つのアプローチは、意図、要素、文書化、および検証の点で異なります。

このドキュメントでは、それぞれのアプローチを重点的に説明し、以下の点についても触れています：

- 評価対象となる主体の役割について取り上げる
- 関連評価者の役割について説明し、
- これらの手法に関する文書、よくある質問への回答を提供します。

評価対象となる組織向けに、本文書には以下の記入済み事例が掲載されています：

- 補償制御ワークシート、
- カスタマイズされたアプローチのための制御マトリックス、そして
- カスタマイズされたアプローチのための、対象を絞ったリスク分析

評価者向けに、この文書にはコンプライアンスに関するレポートの完成例「付録 E カスタマイズされたアプローチ」のテンプレートが含まれています。

# 対象読者と目的

本書は、補償制御またはカスタマイズされたアプローチを開発、運用、管理、または評価するすべての組織による使用を意図しています。これには、PCI DSS の評価を実施する評価者や、評価を受ける事業体が含まれます。

本書の目的は、補償制御およびカスタマイズされたアプローチの一貫した運用を支援するための実用的なガイダンスを提供することです。

PCI Security Standards Council (PCI SSC) は、コンプライアンスの強制や、特定の導入事例がコンプライアンスに適合しているかどうかの判断を行う責任を負いません。組織は、アクワイアラー（マーチャントバンク）、決済ブランド、またはその他の組織など、コンプライアンスプログラムを管理する組織と連携して、組織のコンプライアンス検証および報告責任を理解する必要があります。

本書のガイダンスは、PCI DSS またはその他の PCI SSC 基準における要件を追加、拡張、置換、あるいは上書きするものではありません。発行時点では、PCI DSS の現在のバージョンは v4.0.1 ですが、ここで提供される一般的な原則と実践は将来のバージョンにも適用される可能性があります。

# PCI DSS v4.x の制御を実装および検証するための選択肢

PCI DSS v4.x では、組織が PCI DSS 要件を実装および検証のための 2 つのアプローチ、すなわち「定義されたアプローチ」と「カスタマイズされたアプローチ」が含まれています。

**定義されたアプローチ**は、PCI DSS の制御策を実装および検証するための従来からの手法であり、PCI DSS の最初のバージョンから採用されています。**補償制御**は、規定された要件をそのままの形で満たすことを妨げる、正当かつ文書化された技術的または業務上の制約がある組織にとって、定義**されたアプローチの枠組み内で選択可能な手段の一つです**。要件を満たすように更新できないレガシーシステムやプロセスが存在する場合、代替コントロール（補償制御）がしばしば用いられます。

**カスタマイズされたアプローチ**は、各 PCI DSS 要件 (該当する場合) のセキュリティ目標に焦点を当てており、企業は、定義された要件に厳密に従わない方法で、要件に記載されているカスタマイズされたアプローチの目標を満たすためのコントロールを実装できます。個々のカスタマイズされた実装はそれぞれ異なるため、規定されたテスト手順は存在しません。その代わり、実装された統制が所定の目的を満たしていることを検証できるよう、評価者はその特定の実装に適したテスト手順を導き出す必要があります。

***カスタマイズされたアプローチは、すべての PCI DSS 要件において選択可能なオプションですか？***

PCI DSS 要件の大部分は、「定義されたアプローチ」または「カスタマイズされたアプローチ」のいずれかを用いて満たすことができます。ただし、いくつかの要件にはカスタマイズされたアプローチの目標が明記されていないため、カスタマイズされたアプローチのオプションはありません。

***カスタマイズされたアプローチは、どのような種類の組織を対象としていますか？***

このカスタマイズされたアプローチは、セキュリティ慣行におけるイノベーションを支援することを意図しており、組織が自社のセキュリティ統制策によって PCI DSS の目標をどのように達成しているかを示す際の柔軟性を高めるものです。このアプローチは、専任のリスク管理部門の設置や組織全体でのリスク管理体制の構築など、セキュリティに関して強固なリスク管理体制を実践している、リスク管理の成熟度が高い組織に推奨されます。

カスタマイズされたアプローチを用いて実装・検証された管理策は、「定義されたアプローチ」の要件が提供するセキュリティと同等か、それを上回るセキュリティを実現するものと見込まれます。したがって、カスタマイズされた実装を検証するために必要となる文書化や労力のレベルも、規定のアプローチの場合より大きくなることになります。

***SAQ（自己問診票）に回答する組織は、カスタマイズされたアプローチを採用できますか？***

自己評価質問票（SAQ）では、カスタマイズされたアプローチの利用はサポートされていません。カスタマイズされたアプローチを用いて検証を行うことを希望する組織は、PCI DSS の「準拠報告書（ROC）」テンプレートを使用して、評価結果を文書化できる場合があります。カスタマイズされたアプローチの適用に関する質問（SAQ の対象となる事業者が、カスタマイズされたアプローチを利用するために代わりに ROC を作成・提出できるかといった点を含む）については、常に、決済ブランドやアクワイアラなど、コンプライアンスプログラムを管理する組織に問い合わせる必要があります。

***補償制御とカスタマイズされたアプローチの違いは何ですか？***

補償制御は、カスタマイズされたアプローチとは異なる目的を果たすものであるという点に留意することが重要です。組織に制約があり、規定された要件を満たすことが**できない**場合に使用される補償制御とは異なり、カスタマイズされたアプローチは、記載されているものとは異なる方法で要件を**満たすことを選択した**企業向けです。この場合、当該組織は、規定された要件の代わりに、規定された「カカスタマイズされたアプローチの目標」を満たさなければなりません。カスタマイズされたアプローチが最も大きな成果を上げるのは、当該組織が強固なセキュリティ・プロセスと優れたリスク管理体制を備え、かつ、その目標を達成するセキュリティコントロールの文書化、テスト、および維持を効果的に設計する能力を有している場合です。

組織がその要件に対してカスタマイズされたアプローチを実装していない場合でも、要件の意図を理解するために要件のカスタマイズされたアプローチの目標が検討される場合があることに注意してください。

***同一の要件に対して、補償制御とカスタマイズされたアプローチを併用することは可能ですか？***

はい。ある組織は、特定のシステムコンポーネントに対しては補償制御を使用し、他のシステムコンポーネントに対しては同一の要件を満たすためにカスタマイズされたアプローチを使用することができます。要件 5.3.1 を例に挙げると、特定の種類のサーバーについて、正当かつ文書化されたビジネス上の制約により当該要件を満たすことができない場合、組織はその要件を充足するために補償制御を利用することができます。当該組織は、最新のマルウェアの脅威を検知・対処するための独自のアプローチを導入している他のシステムコンポーネントについても、同一の要件を満たすために、そのカスタマイズされたアプローチを採用することを選択できます。当該組織は、別のシステムコンポーネント群に対しても、その同じ要件を満たすために、規定されたアプローチを使用することができます。

***ある組織が「カスタマイズされたアプローチ」の目的を満たさない独自のアプローチを設計した場合、その目的を達成するために、代わりに補償制御を使用することは可能ですか？***

いいえ。カスタマイズされたアプローチでは、補償制御はオプションではありません。カスタマイズされたアプローチは、要件における「カスタマイズされたアプローチの目標」を満たす独自の管理策を策定することを選択した組織を対象としています。組織がカスタマイズされたアプローチを策定したものの、技術的またはビジネス上の制約によってその「カスタマイズされたアプローチの目的」を達成できない場合、それは当該組織が、自ら達成不可能なカスタマイズされたアプローチを設計したことを意味します。これが、カスタマイズされたアプローチでは補償制御がオプションではない理由です。

ある組織が、カスタマイズされたアプローチを用いて PCI DSS 要件を満たすことができないと判断し、かつ、技術的または業務上の制約により「定義されたアプローチ」の要件を記載通りに満たすことができない場合、当該組織は、その定義されたアプローチの要件に基づく補償制御を導入することを選択できます。

# ユースケースの比較：補償制御およびカスタマイズされたアプローチの例

*これらの例は、補償制御やカスタマイズされたアプローチの検討が必要となり得るユースケースを区別するためにのみ提示されています。これらのユースケースは、特定の環境に適した、あるいはその環境での使用が推奨される実際の実装や制御を示すことを意図したものではありません。当該組織は、補償制御やカスとマイズされた制御の許容性および使用について、常に評価者およびコンプライアンス関連文書の提出先となる組織に確認を行う必要があります。*

| 補償制御によって対応 | カスタマイズされたアプローチで対応 |
|---|---|
| **要件 3.3.1.2**<br>承認後、SAD は保存されます。これは、当該組織が保存を禁止する技術を有していないためです。 | *この要件は、カスタマイズされたアプローチの対象ではありません。* |
| **要件 3.5.1**<br>技術的な制約により、PAN を暗号化したり、その他の方法で読み取り不能にしたりすることはできません。 | |
| **要件 5.2.1**<br>技術的な制約により、特定のシステムにはマルウェア対策ソリューションを導入できません。 | **要件 5.2.1**<br>すべてのマルウェアを検出し、そのインストールや実行を阻止する仕組みが導入されています。 |
| **要件 8.3.6**<br>クラウドプロバイダーのツールではパスワード設定を変更できず、提供されている設定は PCI DSS の要件を満たしていません。<br>*実装される制御に応じて、補償制御またはカスタマイズされたアプローチのいずれかによって対応可能です。* | |
| | **要件 11.3.1**<br>内部の脆弱性は、内部脆弱性スキャン以外の方法で特定されます。 |
| **要件 11.3.2**<br>ASV ツールの変更が予定されているため、次回の外部脆弱性スキャンを予定通りに実施することができません。 | *この要件は、カスタマイズされたアプローチの対象ではありません。* |
| | **要件 11.5.1**<br>IDS/IPS 以外の仕組みが、異常なネットワークトラフィックの検知に使用されます。 |

# 補償制御とカスタマイズ・アプローチの役割

## 組織の役割：補償制御

事業体は、使用時に補償制御を定義し、1 つ以上の補償制御ワークシート (CCW) に記入することでそれらの補償制御を文書化することが期待されます。当該組織の CCW には、以下を含める必要があります:

- 当該組織が PCI DSS の要件を規定通りに満たすことを妨げる、明確に 定義された技術的および／またはビジネス上の制約。
- 補償制御の定義、および当該制御が元の要件の目的や増大したリスクにどのように対処するかの説明（例：そのコントロールを構成する人、プロセス、ポリシー、技術の観点からの説明）。
- 当初の管理の目的：
  - 当該組織は、本目的のために、当該要件の「カスタマイズされたアプローチの目標」を使用することができるが、使用する義務はありません。
- 補償制御ルによって達成される目的：
  - これは、必須ではありませんが、PCI DSS 要件における「カスタマイズされたアプローチの目標」として明記されるものであっても構いません。
- 当初の管理策が欠如していることによって生じる、あらゆる追加的なリスクに関する説明。文書には、このリスクおよびその対処方法についての理解が反映されている必要があります。
- 当該組織が補償制御を検証およびテストする方法についての説明。
- 当該組織が補償制御を検証およびテストする方法についての説明。

PCI DSS v4.x の付録 C には、CCW のサンプルが記載されています。*補償制御ワークシート追加の補償制御ワークシート*のテンプレートは、PCI SSC ウェブサイトの「PCI DSS」配下にある「Document Library（ドキュメントライブラリ）」で入手可能です。

## 評価者の役割：補償制御

評価者は、毎年の PCI DSS 評価において、対象組織の補償制御ワークシート（CCW）を徹底的に評価し、当該 CCW が「付録 C」の項目を明確かつ効果的に文書化し、それらに対処していることを確認する必要があります。補償制御ワークシート（上記の「組織の役割」の下に記載）。

当該組織が文書化した正当な技術的または業務上の制約について、評価者は、その制約の妥当性までを確認する必要はありません。評価者に求められるのは、当該組織によってその制約が詳細に文書化されていることを確認することだけです。ただし、評価者は、補償制御が整備され、かつ有効に機能していることを確認するために、当該組織が導入した制御要素をテストすることが求められます。

評価者には、以下のことが求められます：

- 該当する場合、コンプライアンス報告書（ROC）または自己評価質問票（SAQ）に、当該組織の CCW（補完的統制策）を記載してください。
- 関連する要件および検討中の制御に該当する場合は、構成設定の調査、文書のレビュー、プロセスの観察などを含む、補償制御のテストを実行します。
  - その要件に関するテスト手順は、当該要件に対して想定されるテストの種類を示す指針とみなすことができます。
- ROC を作成する際、補償制御によって PCI DSS 要件を満たしている各項目については、以下の通りとします：
  - 「補償制御」のチェックボックスにチェックを入れてください。
  - 評価者によるテストおよび証拠が、当該要件が満たされていることをどのように実証しているかについての説明を記載してください。
  - 評価者の作業用文書にテスト内容を記録し、その証拠を他の評価証拠と共に保管してください。

***過去に見落とされていた要件に対処するために、補償制御を使用することは可能ですか？***

いいえ。PCI DSS v4.x の付録 B については：補償制御の記述が更新され、*過去に見落とされた要件に対して、遡及的に補償制御を適用することはできない旨が明確化されました。*補償制御をこのような方法で使用することは、当初から意図されていませんでした。例えば、本来実施されるべきであった業務が実施されず、その際、それに対処するための措置も講じられなかった場合など。ただし、組織は業務の将来の遂行に影響を及ぼし得る要因（例えば、予定されているシステムの停止や担当者の休暇など）に対処するために、補償制御を導入することも可能です。

***複数の PCI DSS 要件を満たすために、補償制御を使用することはできますか？***

はい。複数の要件を満たせないというリスクを低減するために、補償制御が設計される場合があります。ただし、当該補償制御によって各要件がどのように満たされるかについては、個別の補償制御ワークシートにそれぞれ文書化する必要があります。

各要件に関連するすべての目的およびリスクに対処する必要があり、また、各要件について補償制御を個別に検証しなければなりません。

***補償制御の使用は、限定された期間に限る必要がありますか？***

いいえ。補償制御の適用期間を限定しなければならないという要件はありません。ただし、評価対象となる組織は、補償制御が依然として有効かつ必要であることを確認するために、組織はそれらの制御を毎年見直す必要があります。例えば、新しい技術やシステムの導入に伴い、要件の目的を達成するために補償制御の修正が必要となる場合や、あるいは補償制御が不要となり、当初の PCI DSS 要件をそのままの形で満たせるようになる場合があります。

同様に、評価者は、当該リスクへの対処および要件への適合のために、対象組織の補償制御が依然として適切かつ必要であることを確認するよう、年次でそれらを見直すことが求められます。

# 組織の役割：カスタマイズされたアプローチ

評価対象組織は、以下の手順を含む、カスタマイズされた統制の設計、開発、分析、導入、および保守を行います：

- 本書の「参考文献および関連資料」のセクションに記載されている、 カスタマイズされたアプローチに関する情報を確認してください。
- 各カスタマイズ・コントロールを定義・文書化し、そのコントロールが要件の目的をどのように満たすかについての説明を含めてください。カスタマイズされたコントロールに関する情報を記録する際に使用できるテンプレートについては、[1] *「制御マトリックスのテンプレート（サンプル）」*を参照してください。
- 「規定された要件」と同等以上の保護を提供するのに十分な堅牢性をそのカスタマイズされた制御策が備えていることを示す、対象を絞ったリスク分析を実施し、その結果を文書化すること。[1] カスタマイズされた管理策に関する情報を記録する際に使用できるテンプレートについては、 *「サンプル：特定リスク分析テンプレート 1」*を参照してください。
- 各カスタマイズされた制御が、要件の目的を有効に達成していることを確認するテストを実施し、その結果を文書化してください。実施したテストおよびその結果を記録する際は、*「制御マトリックスのサンプル・テンプレート」*を参照してください。
- 各統制の有効性が、時間の経過とともにどのように監視・維持されるかについて説明してください。
- カスタマイズされたアプローチを導入する計画については、評価者と早期に協議してください。
- カスタマイズされた各コントロールに関するすべての文書を評価者に提供します。

評価対象の組織が、独自に構築した統制を効果的に実施・維持していくためには、それらの統制に対する責任を組織内部に取り込み、主体的にその統制を自らのものとして管理・運用していくことが重要です。

# 評価者の役割：カスタマイズされたアプローチ

カスタマイズされたアプローチが採用される場合、評価者は、以下の手順を実施する上で役立つ当該組織のカスタマイズされたアプローチに関する文書を、事前に受け取るものとします：

- 対象となる PCI DSS 要件が、カスタマイズされたアプローチの適用対象であることを 確認してください。
- カスタマイズされた統制を十分に理解するために、当該組織の文書を見直ししてください。
  - 制御マトリックスおよび特定リスク分析の双方が完了し、提供されていることを確認してください。

[1] 「サンプルテンプレート」には、2 つのテンプレートが含まれています：カスタマイズされたアプローチ – 1) カスタマイズされたアプローチ – 統制マトリックスのサンプル・テンプレート、および 2) カスタマイズされたアプローチ – 特定リスク分析のサンプル・テンプレート。本ドキュメントは、PCI SSC のウェブサイトにある「ドキュメントライブラリ内の「PCI DSS」のセクションでご覧いただけます。各組織がこれらのテンプレートの特定の形式に従うことは必須ではありませんが、PCI DSS 要件 12.3.2 で規定されている通り、当該組織のカスタマイズされたアプローチの制御マトリックス」および「対象を絞ったリスク分析」には、これらのテンプレートに含まれるすべての情報が盛り込まれている必要があります。

- 各カスタマイズされたコントロールについて、以下を含む十分な文書化がなされていることを確認してください：
  - 当該文書には、「カスタマイズされたアプローチの制御マトリックス」および「対象を絞ったリスク分析」の各テンプレートで規定された、必要な情報がすべて含まれています。
  - 当該文書は、カスタマイズされた管理策が、どのようにして「定義された要件」と同等以上の保護を提供するのかを説明しています。
- 当該組織がカスタマイズされた統制に対して実施したテストおよびその結果を検討し、当該主体のテストが当該統制を十分に評価するものであったかどうかを判断してください。
- 各カスタマイズ・コントロールの徹底したテストにつながる、堅牢なテスト手順を策定してください。
  - 当該組織が提供する文書は、評価者が統制の運用方法を理解し、適切なテスト手順を導き出せる程度に詳細なものでなければなりません。
  - 評価者が、当該組織によるテストが統制の徹底した評価を行っていると判断した場合、評価者は、統制の有効性に関する自らのテストを実施するにあたり、当該組織のテストを任意に活用することができます。この場合、評価者は、当該組織が使用したものとは異なるサンプルセットを使用すべきです
- カスタマイズされた各コントロールの実装について、独立したテストを実施してください。当該組織のテスト結果のみに依拠しないでください。評価者のテストの目的は、コントロールが以下の条件を満たしているかどうかを判断することです：
  - 要件の「カスタマイズされたアプローチの目標」を満たしています、
  - 継続的な有効性を確保するために維持され、
  - 「導入済み」との判断に至るのに十分である。
- -各カスタマイズされたコントロールについて、要件の箇所および ROC の *付録 E* の両方で文書化してください：*カスタマイズされたアプローチのテンプレート*
  - 評価の際、PCI DSS 要件を満たすためにカスタマイズされたコントロールが使用される各ケースについて、評価者は本付録に記入します。
  - 評価者は、対象組織の文書に記載されたカスタマイズされた統制に関する情報に加え、自ら策定したテスト手順、当該統制が整備され有効に運用されていることを確認するために自ら検討した証拠、および自ら実施したテストの結果についての詳細を記載することが求められます。

***カスタマイズされたアプローチの場合、当該組織によって実施されるテストは、評価者によるテストの代わりとなり得ますか？***

いいえ。統制の有効性を実証するために、当該組織が独自の（カスタマイズされた）アプローチを導入・維持する一環として実施するテストは必要ですが、それは評価者によるテストに取って代わるものではありません。評価者は独立したテストを実施し、そのテスト結果に基づいて評価者としての検証の結論を導き出さなければならない。評価者が、当該組織によるテストが統制の徹底した評価を提供するものであると判断した場合、評価者は、当該組織が使用したものとは異なるサンプルセットを用いて、同一のテストを実施することができます。

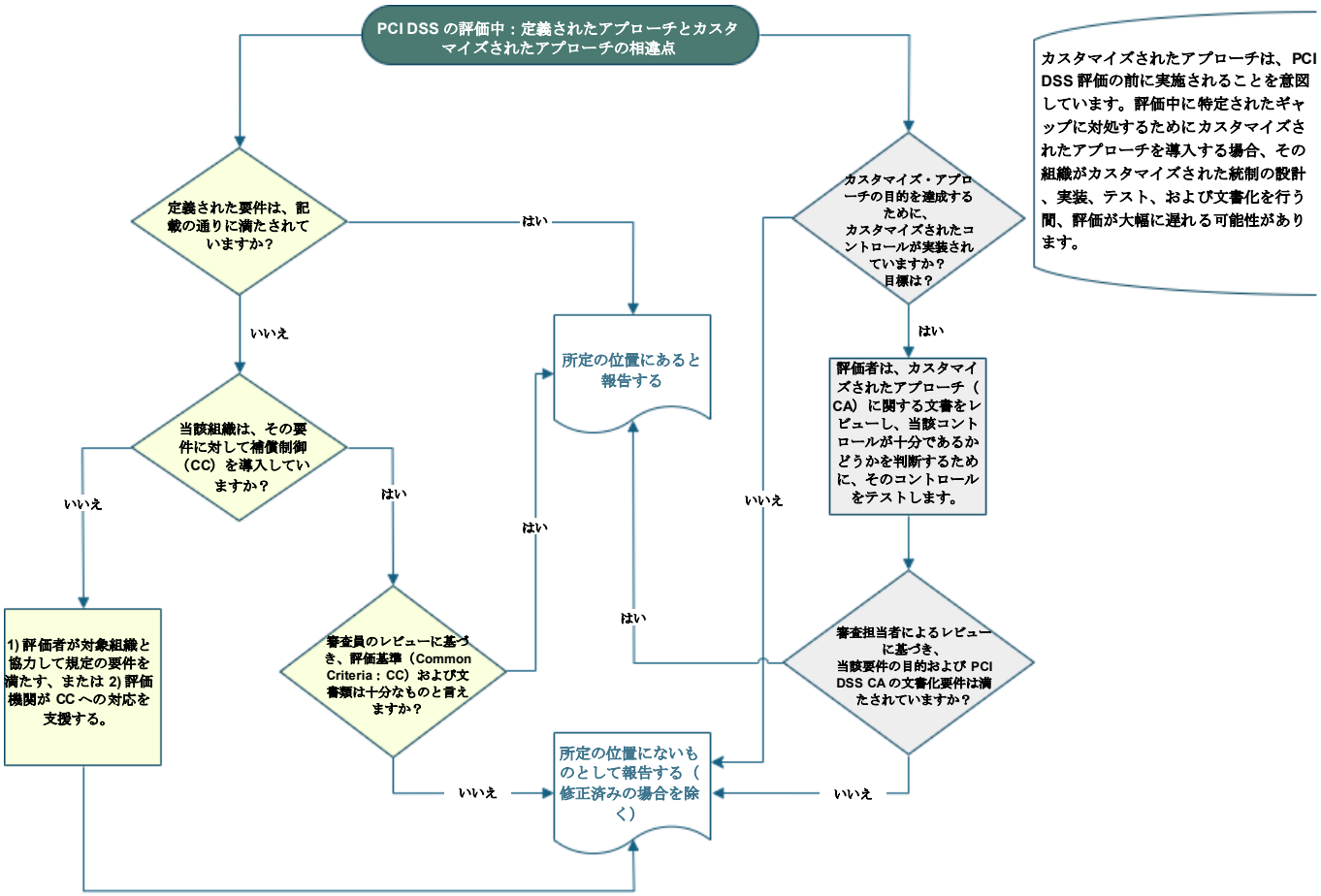
***カスタマイズされたアプローチには、補償制御よりも多くの文書が必要なのはなぜですか?***

カスタマイズされた実装は、設計や環境によって異なり、評価対象組織によって全面的に設計されます。そのコントロールは各組織が独自に設計するものであり、PCI DSS 上では定義されていないため、あらかじめ定められたテスト手順も存在しません。そのため、当該組織による文書化を徹底することが不可欠です。具体的には、統制の内容、その実施方法、リスクの特定、リスクへの対応策、組織による統制のテスト方法、統制がいかにして所定の目的を達成しているか、そして統制が継続的に有効であることを組織がいかにして保証しているか、といった事項を明確にする必要があります。

この文書により、評価者は統制とその運用方法を十分に理解し、それに基づいて適切なテスト手順を導き出し、当該統制を独自に検証することが可能になります。

以下の図は、PCI DSS の評価において、補償制御へのアプローチとカスタマイズ・アプローチがどのように異なるかを示しています。

## 図 1：PCI DSS 審査における「定義されたアプローチ」と「カスタマイズされたアプローチ」の相違点



# 補償制御およびカスタマイズされたアプローチの文書化

各組織は、代替的または個別に構築された補償制御またはカスタマイズされた制御について、明確かつ完全で、適切に構成された文書を作成することが推奨されます。詳細な文書は、統制（コントロール）や環境、そしてその統制がいかにして PCI DSS の要件や目的の意図を満たしているかを理解・評価するための、強固な基盤を評価者に提供します。

当該組織の文書の質は、評価者が統制を検証し、説得力のある結論を導き出す能力に直接的な影響を及ぼします

補償制御およびカスタマイズされた実装のいずれについても、当該組織の文書には以下の内容を記載する必要があります：

- 第三者が読んでも理解できるよう、完全かつ明確に記述してください。
- 文書化されていない文脈に依存することなく、それ単独で成立するようにしてください。
- 目標がどのように達成され、リスクにどのように対処されているかを明確に示してください。
- 当該統制が有効に機能していることを組織がどのように確認したかを示す証拠を提示してください。これには、検証、テスト、および継続的な保証に関する組織のプロセスや結果の詳細を含める必要があります。

***組織の文書や証拠が不完全な場合でも、補償制御やカスタマイズされたアプローチを検証することは可能でしょうか？***

いいえ。文書が不十分な場合、評価者は、その統制が有効に設計され、運用されていることを検証できない可能性があります。対象組織が評価者に対して十分な証拠を提示しない場合、あるいは当該組織の文書や統制が十分であるという確証を評価者が得られない場合、評価者は「未整備」という判定が適切であると判断することができます。

# 評価者の独立性

評価者の独立性は PCI DSS 評価の基本原則であり、補償制御とカスタマイズされた実装を検証する場合にも同様に適用されます。評価対象組織は、補償制御の策定、導入、および維持に責任を負います。

***QSA は、組織に代わって統制を設計または実装することができますか？***

QSA の従業員は、対象組織による統制の設計や導入を支援できる場合がありますが、QSA 企業は、*「QSA 資格要件」*および*「QSA プログラムガイド」*に定められた独立性要件を遵守しなければなりません。これには、PCI DSS の評価を実施または支援する QSA（認定セキュリティ評価機関）の担当者が独立性を保ち、利益相反が生じないようにするための「職務の分離」に関する統制を整備・運用することが含まれます。

ある統制の設計や実装に関与した QSA（認定セキュリティ評価機関）の担当者が、補償制御や個別設計された制御について、そのテスト、評価、または評価の支援を行うことは、利益相反に当たります。詳細については、PCI SSC の FAQ ページにある *FAQ 1562*、「顧客向けの特定のコントロールを設計、開発、または実装する QSA の担当者は、それらのコントロールを評価することも許可されていますか？」を参照してください。

**特に、カスタマイズされたアプローチについて**

QSA（認定セキュリティ評価機関）の担当者は「カスタマイズされたアプローチ」に関連するコンサルティングサービスを提供できますが、独自の管理策を設計・導入するために QSA を必要とする組織は、このアプローチには適していない可能性があります。なぜなら、そうした組織では、当該管理策を維持し、その有効な運用を継続していくことが困難になる恐れがあるからです。リスク管理の成熟度や取り組みへの意欲に加え、独自のカスタマイズされた統制を策定・導入・維持するために必要なリソースを備えた組織は、そうした制御を通じて長期的なセキュリティの実効性を実現できる可能性が高まります。

補償制御またはカストマイズされた制御の策定に、評価者または QSA 企業が関与した場合は、その旨を準拠報告書（ROC）のセクション 1.4 に記載しなければなりません。

# 参考文献および関連資料

以下の PCI DSS v4.x のセクションおよび付録、ならびに以下のガイダンス文書、テンプレート、および様式を参照してください：

**カスタマイズされたアプローチのために**

- PCI DSS v4.x の導入部（セクション 8）では、補償制御とカスタマイズ・アプローチを比較し、双方のアプローチの概要を説明しています。
- PCI DSS v4.x の付録 D では、カスタマイズされたアプローチについて、必須とされる「対象を絞ったリスク分析」の要素や、対象組織および評価者の双方の責任など、詳細が規定されています。
- PCI DSS v4.x の*図 5：要件の構成要素の理解*では、各要件内における「定義されたアプローチ要件および（該当する場合）カスタマイズされたアプローチの目標の記載箇所が示されています。
- 要件 12.3.2 は、カスタマイズされたアプローチによって満たされる PCI DSS 要件を対象とする「特定のリスク分析（TRA）」について、その要素を規定しています。
- PCI DSS 4.x 準拠報告書（ROC）テンプレート、付録 E カスタマイズ・アプローチ・テンプレート
- *サンプルテンプレート：カスタマイズされたアプローチ*については、PCI SSC のウェブサイトにあるドキュメントライブラリ内の「PCI DSS」のセクションでご覧いただけます。この文書には、以下が含まれています：
  - カスタマイズされたアプローチ — 制御マトリックスのサンプル・テンプレート
  - カスタマイズされたアプローチ — ターゲットを絞ったリスク分析テンプレート（サンプル）
- *PCI DSS v4.x:「ターゲット型リスク分析（TRA）に関するガイダンス」* — PCI DSS v4.x に含まれる 2 種類のターゲット型リスク分析（TRA）について説明しています。

**補償制御について**

- PCI DSS v4.x において：
  - 導入部第 8 項。ここでは、補償制御とカスタマイズされたアプローチを比較し、双方のアプローチの概要を説明しています。
  - *付録 B：*定義および基本基準を提示する*補償制御*。
  - *付録 C：*補償制御ワークシート：PCI DSS の要件を満たすために補償制御を定義する際、事業体が使用するワークシートのサンプル。
- 補償制御を文書化する際に使用できる*追加の補償制御ワークシート*は、PCI DSS におけるドキュメントライブラリ内の PCI DSS で入手可能です。

# 付録：補償制御およびカスタマイズされたアプローチに関する、記入済みテンプレートの例

## 組織の記入済み例：補償制御ワークシート

*これは補償制御ワークシートに記入する際の一例として提示されているものであり、特定の環境に適した、あるいは推奨される実際の統制の例として意図されたものではないことにご留意ください。*

**要件番号および定義：** PCI DSS 要件 8.4.2 – カード会員データ環境（CDE）へのすべてのアクセスに対して、多要素認証（MFA）が実装されていること。

| | 必要な情報 | 説明 |
|---|---|---|
| **1. 制約** | 元の要件への準拠を妨げる正当な技術的またはビジネス上の制約を文書化します。 | ABC Org は、従来の支払い承認プラットフォーム (システム ID：独自仕様の UNIX バージョン 5.2 上で動作する PCIPAY-AUTH-01 本プラットフォームは、RADIUS、SAML、または PAM ベースの MFA モジュールを含む、最新の MFA メカニズムとの統合をサポートしていません。このプラットフォームはベンダーによるサポートが提供されていますが、変更を加えると、ベンダーサポートやシステムの整合性が無効となります。<br><br>本システムの更改は「Project PCIPAY-MODERN-02」の一環として計画されており、2027 年第 4 四半期の完了が予定されています。 |
| **2. 補償制御の定義** | 補償制御を定義してください：すなわち、それらが本来の統制の目的および（もしあれば）増大したリスクにどのように対処するのかを説明してください。 | ABC 組織は、以下の補償制御を導入しました。<br><br>**ジャンプホストでの MFA 強制**<br><br>PAY-AUTH-01 へのすべてのアクセスは、ネットワークセグメント VLAN-SEC-ADM 内に配置された、管理専用のジャンプホストに制限されています。<br><br>ジャンプホストへのアクセスには、以下が必要です：<br>▪ 一意のユーザーID<br>▪ パスワード認証<br>▪ ハードウェアベースの認証トークン（FIPS 認定デバイス）<br>▪ Active Directory（AD）認証の統合<br><br>**ネットワークアクセス制御**<br><br>ファイアウォールルールにより、PAY-AUTH-01 へのアクセスはジャンプホストからのみに制限されています。ユーザーのワークステーション、VPN 接続、またはその他のネットワークセグメントからの直接アクセスは、技術的に阻止されています。ファイアウォールルールセットのリファレンス：FW-RULE-SET-CDE-ADM-V3。<br><br>**セッションの監視とログ記録** |

| | 必要な情報 | 説明 |
|---|---|---|
| | | すべての管理セッションは、以下の通りです：<br>▪ 一元的に記録されています<br>▪ エンタープライズ SIEM プラットフォーム（SecurityLog-SIEM-01）に転送されました。<br>▪ 最低 12 ヶ月間保持されています<br><br>**セッションの録画**<br><br>PAY-AUTH-01 への管理セッションは、特権アクセス管理（PAM）ソリューションである PAM-SEC-01 を使用して記録されます。セッションの録画は、フォレンジックおよび監視の目的で保存されます。<br><br>**セキュリティの監視とアラート通知**<br><br>SIEM は、以下の対象についてアラートを生成します：<br>▪ 不正アクセスの試み<br>▪ 定義された管理可能時間外のアクセス<br>▪ 権限昇格の試み<br><br>アラートは SOC 担当者によって確認されます。 |
| **3. 目標** | 当初の制御の目的を定義してください。 | 複数の認証要素を使用することにより、CDE へのアクセスに対する強力な認証を確保します。 |
| | 補償制御によって達成される目的を特定してください。<br><br>*__注記：__これは、PCI DSS において当該要件について記載されている「カスタマイズされたアプローチの目標」とすることも可能ですが、必ずしもそうである必要はありません。* | 当該補償制御は、PCIPAY-AUTH-01 へのアクセスを許可する前に MFA（多要素認証）を強制し、かつシステムへの直接アクセスを防止することで、その要件の目的を達成します。 |
| **4. 特定されたリスク** | 本来の制御策が欠如していることによって生じる、追加のリスクを特定してください。 | PCIPAY-AUTH-01 上で直接 MFA を実装できないことに伴うリスクには、以下が含まれます：<br>▪ 認証情報の侵害の可能性<br>▪ カード会員データシステムへの不正アクセス<br><br>導入された補償制御は、以下を確保することで、このリスクを低減します：<br>▪ アクセス前に MFA 認証が強制されます。<br>▪ 直接アクセスは禁止されています<br>▪ すべてのアクセスは監視、記録、および確認が行われます<br><br>残留リスクは「低」と評価されています。 |

| | 必要な情報 | 説明 |
|---|---|---|
| **5. 補償制御の検証** | 補償制御がどのように検証およびテストされたかを定義してください。 | 当該組織は、以下の方法により、補償制御の有効性を検証します：<br>▪ 四半期ごとのファイアウォールルールレビュー（証拠：四半期ごとのファイアウォール・ルールの見直し（証拠：FW-Review-Reports）<br>▪ 四半期ごとの特権アクセスレビュー（証拠：アクセスレビュー記録）<br>▪ ジャンプホストにおける MFA 強制適用の四半期ごとの検証<br>▪ SIEM アラートの月次レビューおよび検証<br>▪ 特権アクセス制御に関する年次内部監査<br><br>当該組織は、制御が有効であることを確認するために、この検証の証拠をレビューしました：<br>▪ ファイアウォールの設定<br>▪ アクセス制御設定<br>▪ SIEM アラートレポート<br>▪ セッションの録画ログ |
| **6. メンテナンス** | 補償制御を維持するためのプロセスおよび制御を定義します。 | 当該組織は、以下の方法により、補償制御の有効性を維持しています：<br>▪ ファイアウォールおよびジャンプホストの設定変更を管理する変更管理手順<br>▪ 継続的な SIEM 監視<br>▪ 四半期ごとのアクセスレビュー<br>▪ 補償制御の適用可能性に関する年次レビュー<br><br>補償制御のレビュー担当者：最高情報セキュリティ責任者<br><br>レビュー頻度：年間 |

# 組織の記入済み例：カスタマイズされたアプローチのための制御マトリックス

*注記 なお、これはカスタマイズされたアプローチに基づく制御マトリックスを作成する際の一例として提示されているものであり、特定の環境に適した、あるいは推奨される実際の制御の例として意図されたものではありません*

| 制御マトリックスカスタマイズされたアプローチのための制御マトリックス・テンプレート ― 記入済みサンプル<br>被評価機関が記入すること | | |
|---|---|---|
| カスタマイズされた 制御名／識別子 | 音声識別および認証 | |
| この制御策によって満たされる PCI DSS 要件番号および目的 | 要件 ＃：8.2.8 | 目標：ユーザーセッションは、権限のあるユーザー以外は使用できません。 |
| **制御の詳細** | | |
| 実装されている制御策は**何ですか**？ | 当該組織は、運用上の衛生管理を目的として、「ゼロタッチ」環境を運用しています。特定の環境では、ユーザーはキーボードを使ってログインするのではなく、コンピュータに対して音声で命令を出すだけです。<br>システムに初めてログインする際、ユーザーは「ユーザー名を認識」という音声コマンド（例：「アリスを認識」）を発行します。<br>このシステムはまず、ユーザー固有の音声紋（ボイスプリント）を用いてユーザーを識別・認証するとともに、物理的な入退室制御システムへの照会を通じて、そのユーザーが当該環境内に実際に存在することを確認します。続いて、録音された音声の再生による不正利用を防ぐため、また音声紋（ボイスプリント）の再確認を行うために、画面に表示された 3 つのランダムな単語をユーザー（例：アリス）に復唱するよう求めます。その段階では、ユーザーはログインしています。<br>そのシステムは、音声コマンドを絶えず待ち受けています。ログイン中のユーザーのセッションは、そのユーザーが当該エリア内にいる間は有効ですが、アクセスカードを使用してエリアから退出すると終了します。<br>ユーザーがコマンドを発行するたびに、その音声紋が検証されます。ログイン中のユーザーのものと一致しない場合、拒否され、ログに記録されます。ログは SIEM に取り込まれます。 | |

| 制御マトリックスカスタマイズされたアプローチのための制御マトリックス・テンプレート ― 記入済みサンプル<br>被評価機関が記入すること | |
|---|---|
| | 別のユーザーが、そのユーザーがログイン中の端末を使用しようとした場合、音声紋が一致しないため、システムはそのコマンドを拒否します。<br>例えば、システムの正規ユーザーではあるものの Alice の端末にはログインしていない Dave か、あるいは悪意ある攻撃者である Mary が Alice のシステムに近づき、「ポッド・ベイのドアを開けろ」と命じたとします。するとコンピュータは、その命令が Alice によるものではないと認識して「それはできません」と応答し、同時に不正アクセスの試みとして記録を残します。<br>さらに、システム上の USB インターフェースやブルートゥースは無効化されているため、音声認識システムを手動でバイパスすることはできません。 |
| 制御は**どこに**実装されていますか？ | 製造施設 17。ネバダ。 |
| 制御は**いつ**実施されますか？ | 音声によるリクエストが解析されるたびに。 |
| その制御策について、全体的な責任と説明責任を負うのは**誰**ですか？ | 情報セキュリティ責任者 |
| その制御の管理、維持、および監視には、**誰**が関与していますか？ | セキュアオペレーションエンロールメント部門は、新規システム利用者の登録（オンボーディング）を担当しています。これには、利用者へのトレーニングや、信頼性の高いボイスプリントを生成するために十分な音声サンプルを採取することが含まれます。<br>本システムの管理・保守は Acme Voiceprint Security Technologies 社に委託されています。同社は要件 12.8 に基づき運用を行っており、不正検知や本人確認、さらにはコンタクトセンターにおける顧客情報へのアクセス制御といった用途で、多くの主要金融機関に同技術を提供しています。 |
| **当該制御策が*適用される* PCI DSS の*各要件について*、対象組織は以下の詳細を提示します：** | |
| 当該組織は、実装された制御が PCI DSS 要件の***目的***をどのように満たしているかを記述します。 | コマンドが発行されるたびに（声紋による生体認証で）実質的な再認証が行われるため、セッションを利用できるのはログイン中のユーザーのみです。他の許可されたユーザーや許可されていないユーザーは、そのログインセッションを使用できません。 |

| 制御マトリックスカスタマイズされたアプローチのための制御マトリックス・テンプレート ― 記入済みサンプル<br>被評価機関が記入すること | |
|---|---|
| 当該組織は、**実施した**テストおよびその結果について記述し、それによって、当該制御が適用される要件の目的を満たしていることを実証します。 | システムの動作を検証し、ユーザーセッションへの不正アクセスを試みるため、「アクメ・セキュア・テスティング・サービス（Acme Secure Testing Services）」にセキュリティ評価が委託されました。彼らはこれを行うことができませんでした。<br>また、同社は別途レッドチーム演習を実施しましたが、正規の音声ユーザーになりすましてシステムを侵害し、不正アクセスを行うことにも失敗しました。 |
| 当該組織は、**実施した**個別のリスク分析の結果を簡潔に説明します。その説明には、導入された制御の内容と、当該制御が対象となる PCI DSS 要件の定義されたアプローチと同等以上の保護レベルを提供することを、その分析結果がどのように裏付けているかについての記述が含まれます。このリスク分析を文書化する方法の詳細については、別途「特定リスク分析テンプレート」を参照してください。 | 当該の要件制御が適用されている場合、ログイン中のユーザーがワークステーションを離れると、セッションがタイムアウトするまでの 15 分間、権限を持たない脅威アクターがそのワークステーションにアクセスできる状態が生じます。この制御機能により、ユーザーが物理的にその環境内にいる間はセッションが常にアクティブな状態に保たれ、各コマンドの音声パターンが、実際にログインしているユーザーによるものであると検証された上で実行されます。<br>したがって、このシステムは、定義された検証制御よりも高いレベルのリスクに対処します。 |
| 当該組織は、制御が維持され、かつその有効性が継続的に確保されるよう実施した措置について説明します。*例えば、当該組織が制御の有効性をどのように監視しているか、制御の不備がどのように検知され対応されているか、そしてどのような措置が講じられているか、といった点です。* | GRC チームのメンバーは毎月、施設内で音声コマンドを発したり、事前に録音・取得した音声を使用したりして、ユーザーセッションの乗っ取りを試みます。この演習は文書化された手順に従って実施され、その結果はシステムによって音声録音されます。各テスト終了後、音声記録および手順ログは、ガバナンス・リスク・コンプライアンス責任者によって確認されます。<br>不審な事案の報告手順が整備されています。システムがログインしていない状態の音声に反応したとユーザーが疑う場合、従うべき手順が定められています。すべてのユーザーは、本手順の運用に関する訓練を受け、模擬インシデント報告書の作成を完了しています。この手順の使用は、ユーザーの年次セキュリティトレーニングに含まれています。現在までに、事故は報告されていません。 |

# 組織の記入済み例：カスタマイズされたアプローチに向けた、対象を絞ったリスク分析

*注記 これは、カスタマイズされたアプローチの対象リスク分析を完了するための 1 つの方法の例としてのみ提供されており、特定の環境に適した、またはその環境での使用が推奨される実際の制御の例として意図されたものではないことに注意してください。*

| カスタマイズされたアプローチの対象を絞ったリスク分析 – 完成例<br>被評価機関が記入すること | |
|---|---|
| **項目** | **詳細** |
| **1. 要件を特定する** | |
| **1.1** 記載されている PCI DSS 要件を特定します。 | 8.2.8 ユーザーセッションが 15 分を超えてアイドル状態となった場合、端末またはセッションを再有効化するには、ユーザーによる再認証が必要となります。 |
| **1.2** 記載されている PCI DSS 要件の目的を特定します。 | ユーザーセッションは、権限のあるユーザー以外は使用できません。 |
| **1.3** 当該要件が防止することを意図している弊害について説明してください。 | 内部または外部の脅威アクターが、正規ユーザーの放置されたセッションを乗っ取る可能性があります。脅威アクターは、活動の実行、データへのアクセス、およびコマンドの発行を行うことが可能となり、それらの行為はログイン中のユーザーによるものとして誤って記録されることになります。<br>システムやデータへの不正アクセスが発生する可能性があります。<br>ログファイルは不正確なものとなり、実際には実行していない操作であっても、ログイン中のユーザーの識別情報が記録されてしまうことになります。 |
| **2. 提案されている解決策について説明してください** | |
| **2.1** カスタマイズされた制御名／識別子音声識別および認証 | 音声識別および認証 |
| **2.2** 現状の要件のうち、提案するソリューションにおいて変更されるのはどの部分ですか？ | 現在使用されているシステムは、アクティブ状態とアイドル状態を特に区別していないため、セッションが 15 分間「アイドル」状態であったことを検知する機能を備えていません。その代わりに、ログイン済みのユーザーは、初回認証およびログイン完了後であればいつでもシステムに対して音声コマンドを発行できます。ただし、発行された各コマンドについては、それがログイン中のユーザーによって発行されたものであるかどうかが検証されます。<br>ログイン中のユーザーによって発行されたコマンドのみが受け付けられます。 |
| **項目** | **詳細** |

| カスタマイズされたアプローチの対象を絞ったリスク分析 – 完成例<br>被評価機関が記入すること | | | | | | |
|---|---|---|---|---|---|---|
| **2.3** 提案された解決策は、どのようにしてその悪用を防ぐのでしょうか？ | 各音声コマンドは実行前に検証されるため、ログイン中のユーザー以外の人物から発せられたコマンドは検証に失敗し、システムによって実行されることはありません。したがって、これにより、内部または外部の攻撃者が正規ユーザーの無人セッションを乗っ取ることができなくなります。 | | | | | |
| **3.　カード会員データの機密性侵害につながるような、不正行為の発生可能性の変化を分析します** | | | | | | |
| **3.1** 制御マトリックスに詳述されている、不正行為が発生する可能性に影響を及ぼす要因について説明してください。 | システムが受信する各コマンドは、ログイン中のユーザーによって発行されたものであるかどうかが検証されます。これにより、ログイン セッションが脅威アクターによって乗っ取られる可能性が低くなります。定義された要件に基づくと、脅威アクターは、認証済みセッションが放置されている間に物理的にアクセスし、そのセッションを乗っ取るための 15 分間の猶予（ウィンドウ）を有することになります。<br>導入された制御策の下では、脅威アクターがログイン中のユーザーのセッションを使用してコマンドを発行する余地はありません。 | | | | | |
| **3.2** カスタマイズされた制御策を適用した後でも、不正行為が発生し得る理由を説明してください。 | 本システムは徹底的なテストを経ており、音声合成や録音再生といった技術的な手法によって突破されることはありません。また、そうした試みが行われたとしても、ログイン状態を維持するためにその場に物理的に居合わせる必要があるログイン中のユーザーによって、即座に気づかれるものと想定されます。<br>脅威アクターが、ログイン中のユーザーを物理的に威嚇することでこの制御を回避する可能性がありますが、本システムには「緊急事態監視機能」が備わっています。この機能は、ユーザーには作動の兆候を一切示さずに、警備担当者へ通報を行います。<br>セキュリティのテストおよび評価演習において、当該システムは、攻撃者を想定した者によって回避されることはありませんでした。 | | | | | |
| **3.3** カスタマイズ・アプローチで詳述されている制御策は、規定のアプローチの要件と比較して、不正行為が発生する可能性をどの程度変化させるものですか？ | いたずらが起こる可能性は高いです | ☐ | 変更なし | ☐ | いたずらが起こる可能性は低いです | ☒ |

| カスタマイズされたアプローチの対象を絞ったリスク分析 – 完成例<br>被評価機関が記入すること | | | | |
|---|---|---|---|---|
| **項目** | **詳細** | | | |
| **3.4** カスタマイズされた制御策が導入された場合における、不正行為が発生する可能性の変化に関する評価の根拠を提示してください。 | 攻撃者がログイン中のユーザーのセッションを乗っ取るために利用できていた 15 分間の猶予時間はゼロになります。すべてのコマンドについて、ログイン中のユーザーから送信されたものであるかどうかが検証されるためです。 | | | |
| **4. アカウントデータへの不正アクセスが及ぼす影響の変化を分析します** | | | | |
| **4.1** 本ソリューションが対象とするシステムコンポーネントの範囲において、本ソリューションに障害が発生した場合、どの程度の量のアカウントデータが不正アクセスのリスクにさらされることになりますか？ | **4.1.1** 保存されている PAN の数 | なし。当該組織は PAN を保存しません。 | **4.1.2** 12 ヶ月間に処理または送信された PAN の数 | 3,200 万 |
| **4.2** カスタマイズされた制御が直接的にどのように……するかの説明：<br>攻撃者が成功した場合、侵害された個々の PAN の数を減らす、および/または<br>漏洩した PAN（カード番号）をカードブランドへより迅速に通知できるようにします。 | 導入された制御策は、アカウントデータへの不正アクセスによる影響を低減するものではありません。 | | | |
| **5. リスクの承認およびレビュー** | | | | |
| **5.1** 私は上記のリスク分析を検討し、詳述された提案のカスタマイズされたアプローチを使用することが、該当する PCI DSS 要件について、規定のアプローチと同等以上の保護レベルを提供するものであることに同意します。 | [署名] | | | |
| **5.2** 本リスク分析は、遅くとも以下の期日までにレビューおよび更新されなければなりません。 | [日付] | | | |

# 評価者用記入済みサンプル：コンプライアンス報告書 ― 付録 E カスタマイズされたアプローチ・テンプレート

*なお、これは「コンプライアンス報告書」を作成する際の一例として提示されているに過ぎず、特定の環境に適した、あるいは推奨される実際の制御の例として意図されたものではありません。*

**要件番号および定義：**PCI DSS 要件 8.2.8：ユーザー セッションが 15 分を超えてアイドル状態になった場合、ユーザーは端末またはセッションを再アクティブ化するために再認証する必要があります。

| カスタマイズされたアプローチに関するコンプライアンス報告書テンプレート ― 記入済みサンプル<br>評価者が記入すること | |
|---|---|
| 「カスタマイズされたアプローチの目標」を達成するために使用される各制御について、その**カスタマイズされた制御名または識別子を特定してください。**<br>*（**注記**：評価対象組織の制御マトリックスに記載されているカスタマイズされた制御名を使用してください。）* | 音声識別および認証 |
| 「カスタマイズされたアプローチの目標」を達成するために使用される**各制御について説明してください。**<br>*（**注記**：「カスタマイズされたアプローチの目標」については、「PCI DSS（PCI データセキュリティ基準）要件および「カストマイズされたテスト手順」）を参照してください。* | 目標：ユーザーセッションは、権限のあるユーザー以外は使用できません。<br>1. ユーザーは音声コマンドのみを使用してシステムにログインします。このシステムはまず、ユーザー固有の音声紋（ボイスプリント）を用いてユーザーを識別・認証するとともに、物理的な入退室制御システムへの照会を通じて、そのユーザーが当該環境内に実際に存在することを確認します。その後、システムは録音再生による不正利用を防ぐため、画面に表示されたランダムな 3 つの単語を復唱するようユーザーに求め、音声紋（ボイスプリント）の 2 次確認を行います。<br>2. そのシステムは、音声コマンドを絶えず待ち受けています。ログイン中のユーザーのセッションは、そのユーザーが当該エリア内にいる間は有効ですが、アクセスカードを使用してエリアから退出すると終了します。<br>3. ユーザーがコマンドを発行するたびに、その音声紋が検証されます。ログイン中のユーザーのものと一致しない場合、拒否され、ログに記録されます。ログは SIEM に取り込まれます。<br>4. 別のユーザーがそのユーザーがログインしている端末を使用しようとすると、声紋が一致せず、システムはコマンドを拒否します。<br>5. システム上の USB インターフェースおよびブートウースは無効化されているため、音声認識システムを手動でバイパスすることはできません。 |

| カスタマイズされたアプローチに関するコンプライアンス報告書テンプレート ― 記入済みサンプル<br>評価者が記入すること | |
|---|---|
| 当該制御が「カスタマイズされたアプローチ」の目的を**どのように満たしているか、説明してください。** | カスタマイズされたアプローチの目標：ユーザーセッションは、権限のあるユーザー以外は使用できません。<br>コマンドが発行されるたびに（声紋による生体認証で）実質的な再認証が行われるため、セッションを利用できるのはログイン中のユーザーのみです。他の許可されたユーザーや許可されていないユーザーは、そのログインセッションを使用できません。 |
| この要件に対するカスタマイズされたアプローチを裏付けるものとして、レビュー対象となった**制御マトリックスの文書を特定してください。** | Doc-10 – アプローチ制御マトリックスのカスタマイズ |
| 本要件に対するカスタマイズされたアプローチを裏付けるものとして、レビュー対象となった**「特定リスク分析」の文書を特定してください。** | Doc-11 – カスタマイズされたアプローチ（TRA） |
| **以下の事項を証明する評価者の氏名を特定してください：**<br>当該組織は、PCI DSS v4.x の制御マトリックス・テンプレートで指定されているすべての情報を含む制御マトリックスを完成させました。PCI SSC のウェブサイトに掲載されている、カスタマイズされたアプローチを支援するテンプレート、および制御マトリックスの結果は、本要件に対するカスタマイズされたアプローチを裏付けるものです。<br>当該組織は、PCI DSS v4.x の「ターゲットを絞ったリスク分析」テンプレートに規定されたすべての情報を含む、ターゲットを絞ったリスク分析を完了しました。PCI SSC のウェブサイトに掲載されている「カスタマイズされたアプローチ」を支援するテンプレート例、およびリスク分析の結果が、当該要件に対するカスタマイズされたアプローチの適用を裏付けていること。 | ジョセフィン・アセッサー |

## カスタマイズされたアプローチに関するコンプライアンス報告書テンプレート ― 記入済みサンプル

評価者が記入すること

**実装された制御がカスタマイズされたアプローチの目的を満たしていることを検証するために、**評価者が策定・**実施したテスト手順について説明してください。**例えば、当該カスタマイズされた制御が、定義されたアプローチによって提供されるものと同等以上の保護レベルを確保するのに十分な堅牢性を備えているか、といった点が含まれます。

***注記 1：****技術的なレビュー（例えば、構成設定や運用の有効性などの確認）は、可能かつ適切である場合には実施すべきです。*

***注記 2：****必要に応じて、評価者によって導き出された各試験手順について、行を追加してください。追加する「評価者策定の試験手順」ごとに、その右側にあるすべての行が確実にコピーされるようにしてください。*

| | | |
|---|---|---|
| 評価者が策定した試験手順をここに入力してください：<br><br>1.a) 環境にアクセスした後、利用可能な場合は、提供されたキーボードを使用してシステムへのログインを試みてください。<br><br>1.b) 環境へのアクセスを確保した後、所定の音声コマンドを使用してシステムへのログインを試みてください。<br><br>1.c) 権限を持つユーザーがシステムにログインした後、画面に表示された 3 つのランダムな単語を繰り返してください。<br><br>1.d) ユーザーがシステムにログインした後、別の権限を持つユーザーに、画面に表示された 3 つのランダムな単語を復唱させてください。<br><br>2.a) 権限のあるユーザーが室内にいる状態で、評価者の声で音声コマンドを発行してください。 | **テストの対象を特定してください**（例：インタビュー対象者、レビューしたシステム構成要素、観察したプロセスなど）。<br><br>***注記****：試験対象のすべての品目は、個別に識別可能でなければなりません。* | カスタマイズされた進入制御が稼働している「本番施設 17（ネバダ）」環境下のコンソール A およびコンソール B において、Int-1、Int-2、および Int-3 の支援を受けて試験を実施しました。<br><br>Int-10 と協議し、テスト 1 および 2 の実施中に発生した異常が記録・確認されたことを検証しました。 |
| | この試験手順において検討された**すべての証拠を特定してください。** | Doc-22（テスト 1 および 2 の期間における SIEM ログ）をレビューしました。<br><br>評価者は、ConsoleA および ConsoleB を含む環境へ、権限を持つユーザーに続いて入りました。<br><br>テスト 5.a) まず、評価者はコンソールを確認し、システムの USB インターフェースおよびブルートゥース機能が利用できないことを検証しました。<br><br>テスト 1.a) その際、評価者は、いずれのコンソールにもログインするためのキーボードが用意されていないことを確認しました。<br><br>テスト 1.b) 次に、評価者は所定の音声コマンドを使用してシステムへのログインを試みました。システムは、評価者が権限のあるユーザーではないためログインできない旨のエラーメッセージを表示しました。 |

## カスタマイズされたアプローチに関するコンプライアンス報告書テンプレート ― 記入済みサンプル

| 評価者が記入すること | | |
|---|---|---|
| 2.b) 許可されたユーザーがアクセスカードを使用してそのエリアから退出した後、そのユーザーがコマンドを発する際の音声録音を使用して、システムに音声コマンドを入力してください。<br><br>3.a) テスト 1 および 2 の結果について、SIEM ログを確認してください。<br><br>3.b) SIEM ログの確認を担当する担当者に話を聞き、テスト 1 および 2 の間に何らかの異常が捕捉されたかどうかを確認してください。<br><br>4.a) 2.b.にて試験済み。<br><br>5.a) USB インターフェースおよびブルートゥース機能について、システムを調査してください。 | 本試験手順に基づき評価者が実施した試験の**結果**と、それらの結果がいかにして、実装された制御策が「カスタマイズされたアプローチの目標」を満たしていることを検証しているかについて**説明してください**。 | テスト 1.c) 次に、Int-1 が各コンソールにログインする様子を評価者が観察し、各コンソールに受け入れられた音声コマンドの使用状況を記録しました。続いて評価者は、各コンソールの画面に表示された 3 つの単語を復唱し、システムがユーザーをログインさせず、音声応答が認識されなかった旨のエラーを表示したことを記録しました。<br><br>テスト 1.d）Int-2 が画面に表示された 3 つの無作為な単語を繰り返す様子を、評価者が観察しました。システムは Int-2 によるシステムへのアクセスを拒否し、音声紋が一致しない旨の通知を発行しました。<br><br>テスト 2.a) Int-1 がシステムに正常にログインし、ファイル xyz を開くという Int-1 のコマンドに対してシステムが応答しているように見えた時点で、評価者はシステムに対し、ファイル xyz を開くようコマンドを発行しました。システムはファイルのオープンを拒否し、音声紋が登録済みのユーザーと一致しないという警告メッセージを表示しました。<br><br>テスト 2.b およびテスト 4.a）評価者は、ログイン中のユーザーがアクセスカードを使用して当該環境から退出する様子を観察しました。ログインしていたユーザーが環境から退出した後、評価者は、以前のユーザーがシステムに対してコマンドを実行した際の記録を使用し、システムへのコマンド実行を試みました。システムはそのコマンドの実行を拒否し、ユーザーがシステムからログオフされたという応答を返しました。<br><br>テスト 3.a.)評価者は、テスト実施期間中に生成された SIEM ログを入手し、システムがアクセスやコマンド実行の失敗を適切に記録していることを確認しました。<br><br>テスト 3.b）評価者は、システムへのアクセス試行に関するアラートを受信したことを確認するため、Int-10 に聞き取りを行いました。<br><br>評価者は、当該制御が設計通りに意図した通りに機能しており、かつ、その設計がユーザーセッションを権限あるアクセスを取得したユーザーのみに限定する上で有効であると判断しました。 |

**継続的な有効性を確保するために制御が維持されていることを検証する**目的で、評価者が策定・実施した**テスト手順を文書化してください**。例えば、当該組織がどのように統制の有効性を監視しているか、また、制御の不備がどのように検知・対応され、どのような措置が講じられるかといった点が含まれます。

***注記 1 :****技術的なレビュー（例えば、構成設定や運用の有効性などの確認）は、可能かつ適切である場合には実施すべきです。*

***注記 2:****必要に応じて、評価者によって導き出された各試験手順について、行を追加してください。追加する「評価者策定の試験手順」ごとに、その右側にあるすべての行が確実にコピーされるようにしてください。*

| カスタマイズされたアプローチに関するコンプライアンス報告書テンプレート ― 記入済みサンプル<br>評価者が記入すること | | |
|---|---|---|
| 評価者が策定した試験手順をここに入力してください：<br><br>1) GRC の制御テストに関する文書化された手順を毎月確認します。<br><br>2) 過去 12 ヶ月間の結果の日時を確認し、検査が毎月実施されていることを検証してください。<br><br>3) 制御が期待通りに機能したこと、および GRC 責任者が結果をレビューしたことを検証するために、記録されたテスト結果を 2 件選択する。<br><br>4) 文書化された不審なインシデントの報告手順を検討し、システムがログインしていない音声に応答した場合に担当者がとるべき行動がその手順に十分に記載されていることを確認する。<br><br>5) 年次セキュリティ・トレーニング資料をレビューし、すべてのユーザーが当該手順の運用に関するトレーニングを受けていることを確認する。<br><br>6) ダミーのインシデント報告書を 5 件無作為に選定し、記載の網羅性を確認する。<br><br>7) 確認されたインシデントが発生した場合は、インシデント報告書を確認してください。確認済みのすべてのインシデント報告書をレビューしてください。 | **テストの対象を特定してください**（例：インタビュー対象者、レビューしたシステム構成要素、観察したプロセスなど）。<br><br>***注記**：試験対象のすべての品目は、個別に識別可能でなければなりません。* | GRC 手順 (Doc-3) および過去 12 か月の検査結果 (Doc-4)、<br><br>Int-1 への聞き取りを行い、2025 年 3 月および 2025 年 8 月の試験結果（Doc-16、Doc-17）を確認しました。<br><br>Int-1 と、文書化された不審な事案の報告手順を確認しました。<br><br>Int-1、Int-2、および Int-3 と共に、年次セキュリティ・トレーニング資料を確認しました。Int-10 から Int-14 が作成したダミーのインシデント報告書をレビューしました。<br><br>過去 12 ヶ月間にインシデントが発生していないことを確認しました。 |
| | この試験手順において検討された**すべての証拠を特定してください。** | テスト 1 ：Doc-3<br><br>テスト 2：Doc-4<br><br>テスト 3：Doc-16、Doc-17、Int-01<br><br>テスト 4：Doc-20<br><br>テスト 5：Doc-23<br><br>テスト 6：Doc-50、51、52、53、54 |

| カスタマイズされたアプローチに関するコンプライアンス報告書テンプレート ― 記入済みサンプル<br>評価者が記入すること | | |
|---|---|---|
| | このテスト手順に対して評価者が実施したテストの**結果**と、これらの結果によって、実装された制御が継続的な有効性を確保するために維持されていることをどのように検証するかを**説明します。** | 制御を毎月テストするための GRC 手順は、音声コマンドによる制御が意図した通りに機能しているかを確認する上で、明確かつ有効であると見受けられます。GRC は試験を毎月実施し、その結果は手順に記載された通りに記録されました。実施日時、実施者、および検査結果を含め、結果は適切に記録されているようでした。<br><br>不審な事案の報告手順は、明確かつ適切であると見受けられます。報告要件には、生産施設 17 の IT 担当者が使用しなければならない様式（インシデント報告書）が含まれています。ネバダ。製造施設 17 の全 IT スタッフが確認済み。ネバダは、人事部から入手したトレーニングログを確認することでトレーニングを受けてきました。また、人事記録から無作為に 5 件のダミーのインシデント報告書を抽出し、それらが手順に従って作成されていることを確認しました。<br><br>過去 12 か月間、Int-1 から取得したインシデント ログを Int-1 で確認しました。ログにはいくつかの事象が記録されていましたが、音声コマンド制御に関連するものはいずれも見当たりませんでした。当該制御策に関連するインシデントは発生していないことを、Int-1 に確認しました。<br><br>したがって、当該制御を維持することは、ユーザーセッションをシステムにログインした権限のあるユーザーに限定するという効果を継続的に確保するものと考えられます。 |