PCI DSS徹底解説 第11回

仮想環境に対するPCI DSSの視点…part.2

NTTデータ先端技術株式会社

川島祐樹

はじめに

前回、「仮想環境に対するPCI DSSの視点…part.1 」では、PCI SSCによって公開されたガイドライン“Information Supplement: PCI DSS Virtualization Guidelines”の前半を読み解きました。

前半では、まず使用される言葉や概念の定義を行っており、PCI DSSにあまり依存しない形で、仮想環境特有のリスクを考察していると考えられます。Part.2の本書では、前回挙げられたリスクに対して、どのような対策を行うべきであるのかを、比較的細かく説明しています。

付録文書、Appendix—Virtualization Considerations for PCI DSSでは、要件毎に何をすべきかが記載されています。PCI DSSへの準拠が求められる環境や、同等のセキュリティレベルが求められる環境において仮想技術の導入を検討する場合は、この付録文書を参考にしてリスク洗い出しと適切な対策の検討を行っていただくことをお勧めします。

※本書ではAppendixの翻訳は記載していません。PCI SSCでは順次、文書の各国語への翻訳を行っていますので、いずれ正式な翻訳版が公開されるはずですが、明確な予定は立っていないようです。

注意事項／免責事項

本書は、PCI Security Standards Council(PCI SSC)によって公開された文書をNTTデータ先端技術株式会社によって解釈、抄訳したものをベースとした、弊社独自の文書であり、PCI SSCによる見解や解釈を正式に示すものではありませんのでご注意下さい。

PCI SSCプレスリリース 公式文書

https://www.pcisecuritystandards.org/pdfs/pci_pr_20110614.pdf

Information Supplement: Virtualization 公式文書

https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf

【免責事項】

翻訳は大部分が意訳となっているため、システムの設計や構築、運用に関する判断をされる際は、元文書を参考にしていただけますようお願いいたします。

また、以下の免責事項をよくご確認、ご承諾のうえご利用下さい。

- 本文書の転載・加工・再配布はご遠慮ください。
- 本文書を使用することによっていかなる損害が生じようとも、当社は一切責任を負いません。
- 各規格名、会社名、団体名は、各社の商標または登録商標です。
- 本文書の内容についてPCI SSCへのお問い合わせはご遠慮ください（お問い合わせは、NTTデータ先端技術株式会社までお願い致します）。

4. Recommendations (推奨事項)

前章では、仮想環境に特有のリスクを洗い出し、対応していく際の観点が挙げられましたが、本章では、それを踏まえてどのような対策を行うべきかを説明しています。なお、ここではまだ解説は概念的で、具体的に何をすべきかが記載されているわけではありません。対策を行う際のひとつの観点であると考えるのが良いでしょう。

4.1 一般的な推奨事項

4.1.1 仮想技術に関連するリスクの評価

あらゆるリスク領域を識別し、適切に対策を行うため、注意深くかつ徹底的に、仮想システムに関連するリスクを評価する。仮想環境および仮想システムコンポーネントは、年次のリスク評価プロセスに含め、文書化し、詳細なビジネス上および技術上の評価を伴うべきである。

4.1.2 カード会員データ環境のスコープに対する仮想化の影響度合いの理解

仮想化により環境を少数の物理ハードウェアプラットフォームに集約する場合、仮想システムの設定は複雑になり、カード会員データ環境の境界およびスコープの識別が難しくなる。仮想環境は、PCI DSSの”Scope of Assessment for Compliance with PCI DSS Requirements”ガイダンスをもとに評価する。

ハイパーバイザー上にひとつでもスコープ内のホストがある場合、同ハイパーバイザー上における、たとえば仮想マシン、仮想アプライアンス、ハイパーバイザープラグイン等を含むすべてのシステムコンポーネントを対象とすることを推奨する。

仮想コンポーネントの設計時に、スコープ外と考えられるようなシステムも含めてPCI DSS要件を適用することは、仮想環境のセキュリティベースラインができるだけでなく、複数のセキュリティプロファイルを管理する際の複雑性、リスクを軽減し、スコープ内のコンポーネントの準拠確認におけるオーバーヘッドや労力の低減にもなる。

4.1.3 物理アクセスの制限

単一の物理システムで複数のコンポーネントを稼働させることは、攻撃者が物理アクセスを得た際の影響範囲を広げる結果となる。物理的な対策を評価する際は、単一の物理ホストが提供する全てのVM、ネットワーク、セキュリティデバイスアプリケーション、ハイパーバイザーに同時にアクセスできる、未承認もしくは悪意のある個人による潜在的な侵害を考慮すべきである。また、未使用の物理インタフェースは使用できないようにし、物理的、もしくはコンソールレベルのアクセスは確実に制限と監視を行う。

4.1.4 多層防御の実装

多層防御は様々な観点で必要とされることであり、物理環境における予防・検知・復旧、論理的なセキュリティ対策においてはネットワーク、ホスト、アプリケーション、データレイヤーの保護、認証されていない物理アクセスからの媒体、システム、設備の保護、迅速かつ効率的な潜在的侵害の監視および対応、重要資産の取り扱いや脅威の識別、侵害発生時の対応などに対するトレーニングと教育などを含む。

また、ポリシー、プロセス、手順書が文書化され、あらゆる関係者がそれを理解し、実行していることも重要である。

仮想環境を保護するための多層防御も全く同様で、例えば物理デバイス、ハイパーバイザー、ホストプラットフォーム、ゲストOS、VM、境界、ホスト内部のネットワーク、アプリケーション、データなどのそれぞれのレイヤーの保護や、物理対策、ポリシーと手順書の文書化、関係者の教育、などを含める必要がある。

4. Recommendations (推奨事項)

4.1.5 セキュリティ機能の分離

物理環境でもいえることだが、仮想環境についてはさらに重要な点となる。

VMが提供するセキュリティ機能は、物理環境で要求されるのと同様、プロセス分離のもと実装すべきである。例えば、ファイアウォールのような予防的制御の機能を果たすものは、カード会員データをもつホストと結びつけてはならない。同様に、ネットワーク分離の制御機能自体と、ネットワークセグメンテーションの制御の改変を検知するためのログ集約機能は混在すべきではない。

同一のハイパーバイザー上でこのようなセキュリティ機能を実装するのであれば、別のマシンにインストールされていると考えられ得るレベルの分離を施すべきである。

4.1.6 最小権限と責務の分離の徹底

ハイパーバイザーへの管理アクセスに使用するアカウントと認証情報は注意深く管理し、リスクレベルによってはより制限の強いハイパーバイザーアクセスを使用する。二要素認証や管理パスワードの二重／分割管理などの実装も検討し、ハイパーバイザーへのローカルおよびリモートアクセスを含める。個々の仮想コンポーネントについては適切な役割ベースのアクセス制御を実装し、リソースへの不必要なアクセス防止と責務の分離を徹底する必要がある。

一管理者がファイアウォールと監視サーバ両方へのアクセスが可能というような状況にならないよう、管理権限は適切に分離する。ベストプラクティスとしては、特定のVM機能、仮想ネットワーク、ハイパーバイザー、ハードウェア、アプリケーション、データストアに応じて管理アクセスを制限する。

4.1.7 ハイパーバイザー技術の評価

すべてのハイパーバイザーが適切なセキュリティ機能を持っているわけではないので、適切なパッチ管理、および脅威や脆弱性の利用に対応できる機能について、導入前にハイパーバイザーのセキュリティをテストする。

4.1.8 ハイパーバイザーの強化

ハイパーバイザーは単一障害点となるため、以下の追加の対策を推奨する。

- 管理機能の利用は、あらかじめ決められたネットワークおよびデバイスからのみに制限する。
- 全ての管理機能に対しての多要素認証を要求する。
- 全ての変更に対する適切な変更管理。通常の変更管理プロセスで要求される内容に追加で管理対策を検討する。
- ハイパーバイザー管理者がハイパーバイザーの監査ログの変更、消去、無効化ができないよう管理機能を分離する。
- ハイパーバイザーのログは、物理的に分離された安全なストレージに、可能な限りリアルタイムで送信する。
- ワークロード間のセグメンテーション、セキュリティコントロール、コミュニケーションチャネルの整合性を脅かすことを示す動作や行動を識別するため、監査ログを監視する。
- ハイパーバイザーの認証情報でアプリケーション、データ、個々の仮想コンポーネントへのアクセスができないよう、管理機能において責務を分離する。
- 仮想化ソリューションを実装する前に、当該ソリューションがどのようなセキュリティ管理をサポートし、ハイパーバイザーの侵害のリスクを低減できるか確認する。

4. Recommendations (推奨事項)

4.1.9 仮想マシンおよびその他のコンポーネントの強化

上記のハイパーバイザー向け対策は、VMなど仮想コンポーネントにも適用可能であり、推奨する。全ての項目が仮想マシンや仮想コンポーネントに適用できるとは限らない。実装方法は個別に確認すべきである。

- 全ての不必要なインタフェース、ポート、デバイス、サービスを無効化もしくは削除する。
- 全ての仮想ネットワークインタフェースおよびストレージ領域を安全に設定する。
- 仮想マシン内で稼働するすべてのOSおよびアプリケーションも同様に強化する(要塞化する)。
- ログは、分離された安全なストレージに、できるだけリアルタイムに送信する。
- 暗号鍵管理の取り扱いの整合性を確認する。
- 個々のVMの仮想ハードウェアおよびコンテナを強化する(要塞化する)。
- その他適用可能なセキュリティ対策があれば適用する。

4.1.10 管理ツールの適切な使用の定義

管理ツールでは、仮想システムにおけるシステムバックアップやリストア、リモート接続、マイグレーション、設定変更等を行うことができる。スコープ内のコンポーネントを管理するための管理ツールは、スコープ内のコンポーネントのセキュリティや機能に直接的なインパクトを与えるため、管理ツールもスコープに入ると考えられる。管理ツールへのアクセスは業務上必要とされる関係者のみに限定されるべきであり、管理ツール機能の使用についての役割と責任を分離し、管理ツールの使用は監視し、ログを取得する。

4.1.11 VMの動的な性質の理解

VMは稼働中のもの以外に、休止状態の場合があるが、特に非アクティブもしくは休止状態のVMは、事実上、機密情報や仮想デバイスの詳細設定を含むデータセットである。休止状態のVMにアクセスできてしまえば、コピーして別の場所で稼働させたり、休止状態のVMイメージファイルの中をスキャンしてカード情報やその他機密情報を発見したりすることもできる。このためバックアップや休止状態のVMイメージへのアクセスは確実に制御、監視、管理しなければならない。

また、カード情報を含む非アクティブのVMは、その他のカード会員データの保管先と同等の機密レベルで取り扱う必要がある。つまり、データが不要となった際のVMの安全な削除、また、VMに関連する変更管理、監視、通知プロセスや、すべてのアクセスおよび行動の記録が必要となる。

4.1.12 仮想ネットワークセキュリティ機能の評価

仮想ネットワークインフラストラクチャでは、理想的には、(先述の)データ面、制御面、管理面すべてにおいてセキュリティ対策を実装することが望ましいが、必ずしもこれら3レベルで手段が存在するわけではない。そのような時には特に、下位にある物理コンポーネントが十分に分離されていること、および保護されていることで、仮想ネットワークデバイス間に経路を提供しない事が重要である。つまり、仮想ネットワークデバイスは、仮想システムを分離されたハードウェアであるかのようにする役割がある。

4.1.13 稼働する全ての仮想サービスの明確な定義

共有ホスティングサービスでは、仮想技術が使われていることがあるが、そのようなサービスの利用を検討する際は、ホストされる環境をその他の環境から、管理上、プロセス上、および技術上、適切に分離されていることを確認すべきである。例えば認証、ネットワークおよびアクセス制御、暗号化、ロギングなどの分離がある。

4. Recommendations (推奨事項)

4.1.14 技術的な理解

仮想化環境は、トラディショナルな物理環境と大幅に異なるため、仮想技術を理解しなければ安全な環境を構築することはできない。業界ガイドライン等も参考にすべきである。業界ガイドラインとは以下のようなものがある。

- The Center for Internet Security (CIS)
- International Organization for Standardization (ISO)
- ISACA (formerly the Information Systems Audit and Control Association)
- National Institute of Standards Technology (NIST)
- SysAdmin Audit Network Security (SANS) Institute

4.2 混在環境における推奨事項

4.2.1 混在環境におけるセグメンテーション

大原則として、異なるセキュリティレベルのVMは同一ハイパーバイザーや同一物理マシン上に配置すべきではない。なぜならセキュリティレベルが低い方に落ちてしまうからである。

基本ルールとして、スコープ内のホストがあれば、同一ハイパーバイザー上にある、本来関連しないサーバでもスコープ内となる。なぜなら、ハイパーバイザーもしくはホストOSが、仮想コンポーネント間の物理的、論理的、もしくは両方のコネクションを提供することになり、確実な分離／セグメンテーションが成し遂げられないからである。

もし、仮想コンポーネント間で十分にセグメンテーションが行えたとしても、セキュリティレベルの異なるコンポーネントをそれぞれ別に維持する事は、全体としてPCI DSSに準拠してしまう事よりも難しくなってしまう可能性もあるだろう。

4. Recommendations (推奨事項)

4.3 クラウドコンピューティング環境における推奨事項

プライベートクラウド

システムコンポーネントは所有者によって完全に制御され、信頼できるシステムコンポーネントのみから成る。

パブリッククラウド

利用する側の企業が所有していない、もしくは全ての制御は行えないシステムコンポーネントから成る。どの程度クラウド提供事業者側に制御が残るかはサービスの種類、例えばInfrastructure as a Service(IaaS)、Platform as a Service(PaaS)、Software as a Service(SaaS)などによって異なる。パブリッククラウドの場合、リソースが全体で共有されるものであるため、物理的な分離は現実的ではない。

ハイブリッドクラウド

プライベートクラウドとパブリッククラウドの組み合わせ。プライベートクラウド同士や、プライベートクラウドとパブリッククラウドを接続して構築する。所有権やデータ、システムコンポーネントの制御は複数の事業体に分割され、スコープの境界と責任範囲は複雑になる。

また、IaaS、PaaS、SaaSによって、クラウド提供事業者側とクラウド利用者側の責任範囲が異なる。ただしサービスによって異なるため、利用するクラウドサービスを個々に評価し、クラウド提供事業者とクラウド利用者の責任範囲を明確にすることが重要である。

クラウドではインフラストラクチャが共有される事により、PCI DSS準拠を成し遂げるにあたって障壁が発生する。その障壁には、以下のようなものがある。

- クラウド環境における分散アーキテクチャにより、環境に対する新たな技術レイヤの追加や、複雑性の増加が発生する。
- パブリッククラウド環境は公に面し、インターネット上のどこからでも当該環境にアクセスが許可されるよう設計されている。
- インフラストラクチャはもともと動的な性質であるため、テナント環境間の境界が流動的。
- 利用者から、インフラストラクチャ内部や関連したセキュリティ対策を一部もしくは全く確認できない。
- 利用者によるカード会員データストレージの制御が限定されている、確認できない、もしくは制御できない。
- マルチテナント環境では、利用者から「誰が」リソースを共有しているのか、隣人（同環境でリソースを共有している利用者）がシステム、データストア、その他リソースを利用開始したときにどのような潜在的なリスクがあるのかを知る術がない。

パブリッククラウドにおいては、クラウドアーキテクチャが不可視である点について追加の対策が必要である。つまりパブリッククラウドや同等の環境においては、カード会員データ環境に対する追加のリスクを補完するため、強力な予防的、検知的、復旧的制御が必要となる。クラウドサービスプロバイダは、カード会員データを取り扱う顧客をホスティングする場合、クラウド環境が顧客のPCI DSS対象範囲となった場合に備える必要がある。つまりどの要件に対する対策はクラウドサービスプロバイダの範囲外で、顧客側の責任で準拠しなければならないのかを明示する。

4. Recommendations (推奨事項)

4.4 仮想環境のリスク評価におけるガイダンス

仮想技術は実装の多様性から基準と呼べるものが存在しないため、企業は個々の環境を評価して、関連するリスクを洗い出し、適切な対策を実施する必要がある。

リスクアセスメントは様々な手法があるが、どの手法を使った場合でも脅威と脆弱性の識別、当該環境に対するリスクの理解を含むべきである。ここではいくつかの仮想環境上で含めるべきリスクアセスメントのポイントを挙げる。

4.4.1 環境の定義

脅威や脆弱性を識別する前に、まずは当該環境に関連する、人、プロセス、技術を含む環境の理解が重要である。まずはPCI DSSの対象内、対象外に関わらず潜在リスクが影響を与え得るあらゆる側面について検討すべきである。

仮想環境の定義には最低限、以下を含む。

- ハイパーバイザー、ワークロード、ホスト、ネットワーク、管理コンソール、その他のコンポーネントを含む、全てのコンポーネントの識別
- 各コンポーネントについて、物理拠点の詳細
- 各コンポーネントについて、主要機能と責任者の詳細
- コンポーネントへの、もしくはコンポーネント間の可視性についての詳細
- 異なるコンポーネント間、コンポーネントとハイパーバイザー間、コンポーネントと下位のホストシステムもしくはハードウェアリソース間のトラフィックフローの識別
- 内部ホスト、仮想コンポーネント、その他のシステムコンポーネントとの間の通信チャネルとデータフローの識別
- コンポーネント間の通信を可能とする、全ての外向き通信チャネルの識別
- 役割の定義と承認を含む、管理インタフェース、ハイパーバイザーアクセスメカニズムの詳細
- リムーバブルディスクドライブやUSB、パラレルポートやシリアルポートを含む、全ての仮想および物理ハードウェアコンポーネント
- 各ホストにおける、仮想コンポーネントの数と種類、コンポーネントとホストの分離、仮想コンポーネントの機能およびセキュリティレベル

4.4.2 脅威の識別

このプロセスでは、機密性、完全性、可用性の損失に伴う可能性のある顕在的な、および潜在的な脅威を識別する。これにはあらゆるシナリオ、アクション、イベントを含める必要がある。

仮想環境は、非仮想環境と同様の脅威が存在するが、仮想化の追加レイヤーにリスクが潜在する可能性がある。例えば、ハイパーバイザーを標的とするような仮想技術特有の新種の悪意のあるコードや論理攻撃、共有ハードウェアコンポーネント間の安全でない外部への通信チャネルなどがある。攻撃や脅威を識別するには、各コンポーネントの主要機能と責任者を詳しく把握することが重要である。

4.4.3 脆弱性の識別

仮想環境に依存しない技術的な脆弱性と同様、特定の仮想化技術やその環境で実装される設定についての脆弱性を識別する必要がある。仮想化レイヤーが追加されることによる複雑性の増加や、動的な性質、共有を行う性質、下位アーキテクチャの可視性の低さに起因する脆弱性が存在するだろう。

脆弱性は技術的な視点のものだけでなく、運用プロセス、不十分な担当者の教育、対策の監視の欠如、物理セキュリティの隙間等にも存在する可能性がある。

4.4.4 リスクの評価と対応

リスクアセスメントでは、仮想環境におけるカード会員データや、その他機密情報を保護するための、あらゆる追加の対策を識別する必要がある。とくに、仮想技術に関連した潜在するセキュリティ事故を駆逐するには、PCI DSS要件だけでなく、それに加えて仮想環境特有の対策を行う必要があるだろう。

5. Conclusion (おわりに)

全体のまとめが記載されている。このような新しい技術には新しい攻撃ベクトルが発生するため、個々にリスクアセスメントを行うことや、PCI DSSの対象範囲だけでなく、関連する、もしくは隣接する環境もふまえて最適化されるよう対策を検討、実施していく事が推奨されているように読み取れる。

仮想システムを安全にするための万能な方法は存在しない。多くのアプリケーションが存在し、ある仮想環境で適切な対策が他の仮想環境で適切であるとも限らない。目に見える機能もあるが、仮想化アーキテクチャ内で働く下位の機能や通信は、適切に理解かつ管理されない限り、未知の攻撃ベクトルとなり得る。

多くの技術で見られるのと同様、仮想化の業界スタンダードがないため、ベンダ特有のベストプラクティスや推奨事項が存在している。企業ではこれをよく理解し、それぞれの環境を評価して仮想化がもたらす当該環境固有のリスクを識別し、カード会員データ環境のセキュリティを包含しなくてはならない。

仮想環境では、ひとつのVMもしくはコンポーネントの侵害が他コンポーネントの侵害につながるため、コンポーネントすべてを安全に実装しなければならない。仮想コンポーネントを設計する場合は、スコープ外だと考えられるような場合でも、PCI DSSセキュリティ要件に一貫して対応することで、ベースラインがセキュアになるだけでなく、全体として仮想環境の複数のセキュリティプロファイル管理に関連する複雑性やリスクを低めることができる。この理由から、PCI DSSスコープ内のハイパーバイザーやホスト上で稼働するコンポーネントはすべてPCI DSSのスコープ内とすることを推奨する。

6. Acknowledgments (謝辞)

ここでは省略する。

7. Appendix - Virtualization Considerations for PCI DSS (付録 - PCI DSSにおける仮想化に関する考察)

各要件において、仮想化環境で考慮すべき事項が記載されている。ただし、説明にあるとおり、これは要件ではないので、PCI DSSを上書きしたり、入れ替わったりする性質のものではなく、また、仮想化環境でカード会員データを取り扱う際は、このガイダンスの内容だけでなく、環境毎にリスクアセスメントを行い、ここに記載されていないリスクと対策も検討する必要がある。

実際には、この付録文書にあるように、各要件と実際の環境を照らし合わせ、本書に記載された内容を参考に対策を検討していくことが重要となるだろう。

おわりに：PCI DSS×仮想環境 part.2

本文書では、色々と詳しく説明がされているものの、根本となる部分は一貫していたことにお気づきなのではないでしょうか。筆者が本書から読み取ったポイントを、3つに絞り込んでみます。

大原則は変わらない。カード会員データを扱うシステム、および当該システムに直接接続するシステムは対象となる。

仮想コンポーネントがカード会員データを取り扱う場合、同一ハードウェア上／ハイパーバイザー上で稼動する仮想コンポーネントは、対象とすることが強く推奨される。

仮想技術の実装は多様であるため、現在のところ統一的なセキュリティ対策は示すことができない。このため個々の実環境でリスクアセスメントを行った上、脆弱性、脅威を洗い出し、対策を検討する必要がある。

本書は、PCI DSSの視点で検討が進められたものである一方、広く適用できる内容となっています。また、今後PCI DSS準拠が求められる環境の中で仮想技術やクラウドサービス等の導入を検討される際には、ひとつのよりどころになるのではないでしょうか。

PCI DSS徹底解説 第11回

仮想環境に対するPCI DSSの視点…Part.2

発行：2011年12月28日 NTTデータ先端技術株式会社

■この記事に関するお問い合わせ

NTTデータ先端技術株式会社　セキュリティ事業部

セキュリティコンサルティングBU

PCI推進グループ<pci@intellilink.co.jp>