vol.10

PCI DSS徹底解説 第10回

仮想環境に対するPCI DSSの視点…Part.1

NTTデータ先端技術株式会社

川島祐樹

仮想環境ガイドラインの公開

2011年6月14日、PCI SSCより、仮想環境に関するガイドライン、「Information Supplement: PCI DSS Virtualization Guidelines」が公開されました。このガイドラインは、PCI SSC内の“SIG(Special Interest Group)"と呼ばれる、特定の分野に関する議論が行われるワーキンググループの中の、”Virtualization SIG“が長い議論の末まとめたものです。

以下のPCI SSCのプレスリリースによれば、Virtualization SIGはCitrix SystemsのChief Security StrategistであるKurt Roemer氏を筆頭に、30を超える組織から構成されているとのことです。

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

このガイドラインは、PCI SSCのウェブサイトから自由にダウンロードすることができますので、詳細についてはこちらをご覧ください。

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

ここでは、このガイドラインに書かれている内容を、簡単に紹介したいと思います。なお、読み解くにあたり、誤訳や誤解がある可能性もあります。実際に何らかの判断をされる場合の正確な情報としては、上記の公式ドキュメントを参照していただきますよう、お願いいたします。

また、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。

【免責事項】

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㈱までお願い致します）。

1. Introduction（はじめに）

この補足資料は、PCI DSSに沿って仮想技術の使用に関するガイドラインを提供するものである旨と、カード会員データ環境における仮想技術の使用に関する4つの原則が示されています。4つの原則とは以下の通りです。

a. カード会員データ環境で仮想技術を使用する場合、PCI DSSはそれらの仮想技術にも適用される

b. 仮想技術には、他の技術には関連しない新たなリスクを伴う。よって、カード会員データ環境における仮想技術の使用時は、それらの新たなリスクを確実に評価しなければならない

c. 仮想技術の実装方法は多様であるため、特定の仮想化された実装環境について、決済トランザクションプロセスや決済カード情報を含むあてはまる特性を識別し、文書化して徹底的に洗い出さなければならない

d. PCI DSS要件を満たす仮想環境を作り上げるのに万能な手段や解決方法は存在しない。管理方法や手順は、仮想化がどのように使用され、実装されるかによって異なるだろう

少し回りくどいので、簡単な言葉で言い換えてみましょう。

a. 仮想化していようとしていまいと、カード会員データを扱う環境であればPCI DSSの対象となる

b. 仮想技術を使う場合、仮想技術を使わない場合と比べて特別に気をつけなければいけないことがある

c. とはいえ仮想技術や実際の環境も幅広いので、個々の実際の環境でリスクを洗い出し、文書化し、対策を練らなければならない

d. 万能な方法などない

※カード会員データ環境 ・・・カード会員データを取り扱う環境、およびそこに直接接続する環境。詳細は〝PCI DSS v2.0、適用範囲〟の項を参照して下さい。

a、c、dは特に仮想技術についてだけいえることではありません。PCI DSSのスコープの考え方は原則通りですし、要件を満たすためには様々な方法がある事も、仮想環境でなくとも同様です。つまり、PCI DSSの原則が、仮想環境でも同様に適用されますよ、という念押しに過ぎないというのが筆者の印象です。ですので、特にbの部分、仮想環境特有のリスクをどうとらえるかが重要になる事でしょう。

2. Virtualization Overview (仮想化の概要)

Virtualization Overviewでは、「仮想化とは何か」といった事について記載されています。仮想化、仮想技術については様々な定義があるかと思いますが、本書において、あらためて仮想化を定義しています。

2.1 Virtualization Concepts and Classes

ここでは、仮想化について「物理的な制約からコンピューティングリソースを抽象化すること」であり、近年は“workload”という用語が使われていること、仮想化はいわゆるVirtual Machine (以下VM)だけでなく、様々な“workload”があると述べられています。“workload”を辞書で引いてみると、“仕事量”、“業務上の負担”といったような訳が出てきます。仮想化を行うレイヤー、もしくは対象、くらいの意味で間違いはないでしょう。

そこで、仮想化を行う対象、つまり“workload”毎に説明がされています。

・OS仮想化

単一の物理サーバ上で動作するオペレーティングシステムのリソースを複数の仮想環境、仮想サーバ、ゲスト、ゾーン等に分割するもの。この場合、全てのパーティション（部分）は下位にある同一のOSカーネル（ベースシステム）を使用する。

・ハードウェア／プラットフォーム仮想化

ハードウェア仮想化は、ハイパーバイザー技術を通じて実現される。それには2種類あり、タイプ1 ハイパーバイザーは、“native(ネイティブ)”もしくは“bare metal(ベアメタル)”といいハードウェア上で直接稼働し、ハードウェアリソースへのアクセスを整理する。タイプ2ハイパーバイザーは、既存のOS上で1アプリケーションとして稼働し、各VMに必要とされる物理リソースをエミュレートする。

・ネットワーク仮想化

ネットワークの仮想化は、物理ネットワーキングから論理ネットワーキングを分離する。ルータやファイアウォール、IPS、ロードバランサなど、ほぼ全ての種類のネットワーク機器が仮想アプライアンスとして利用可能。通常のスタンドアロンのホストと異なり、“Data plane”、“Control plane”、“Management plane”の3つの“plane”を持つ。Data planeはホスト間のデータの伝送、Control paneはネットワーク機器間のトラフィックやネットワーク、ルーティング情報、Management planeは機器の管理を請け負う。

・データストレージ仮想化

データストレージの仮想化では、ネットワーク上の複数の物理ストレージ機器が1つのストレージ機器として使用する例等(SAN等)がある。データストアの文書化、管理をしようとする際に、データが複数の場所に分散される点がひとつの重要な課題となる。

・メモリ仮想化

メモリの仮想化では、利用可能な物理メモリを複数のシステムから集約し、仮想化されたメモリの“pool(プール)”を作成し、システムコンポーネント間で共有する。

データストレージの仮想化と同様、複数の物理メモリリソースを1つの仮想リソースとすることにより、データの保管場所の文書化をする際には課題となる。

目新しい事が書いてあるわけではありませんが、「データの保管」に関するものとして、ストレージやメモリの仮想化の際には単一のデータが複数の物理的な拠点(機器)に分散してしまうという点がひとつの重要なポイントとなりそうな事がわかります。

2.2 Virtual System Components and Scoping Guidance(仮想システムコンポーネントとスコープガイダンス)

Virtual System Components and Scoping Guidanceでは、仮想環境でよく見られるコンポーネントの説明をしています。PCI DSSの基本原則である「カード会員データを扱う全てのシステムコンポーネント、およびそこに直接接続するシステムコンポーネントが対象となる」という観点について、これら仮想環境におけるコンポーネントも追加で検討すべき、とされています。

また、重要な考え方として、「特定の仮想システムコンポーネントがスコープ範囲内であるかどうかは、その技術および当該環境においてどのように実装されているかに依存する」とされています。仮想システムコンポーネント毎に、その定義とスコーピングに関するガイダンスが記載されていますので、確認してみましょう。

2. Virtualization Overview (仮想化の概要)

・Hypervisor(**ハイパーバイザー**)

仮想マシンをホストする、もしくは管理する責任をもつソフトウェアもしくはファームウェア。Virtual Machine Monitor(VMM)と呼ばれるコンポーネントを含むことがあり、これは仮想マシンのハードウェア抽象化を実装、管理するもので、ハイパーバイザープラットフォームの管理機能とも考えられる。

スコープガイダンス：

ハイパーバイザー上にPCI DSSの対象となるホストが1つでも存在すれば、ハイパーバイザーも対象となる

・Virtual Machine(**仮想マシン**)

ハイパーバイザー上で動作する、いわゆる「ゲスト」。

スコープガイダンス：

カード会員データを保管、処理、伝送する、もしくはカード会員データ環境に接続したり、入り口となる場合はその仮想マシン全体が対象となる。

・Virtual Appliance(**仮想アプライアンス**)

仮想マシン内で動作するよう設計され、パッケージ化されたソフトウェアイメージ。一般的に、基本的なOSコンポーネントと単一アプリケーションから成り、特定の機能を提供する。Virtual Security Appliance(VSA)もしくはSecurity Virtual Appliance(SVA)と呼ばれるものは、強化されたOSと単一のセキュリティアプリケーションで構成される。これらの例としては、ファイアウォール、IPS/IDS、アンチウィルス等がある。

スコープガイダンス：

スコープ内のシステムコンポーネントやネットワークに接続したり、これらに対してサービスを提供したりするような仮想アプライアンス、およびカード会員データ環境のセキュリティにインパクトを与え得るVSA/SVAは対象となると考えられる。

・Virtual Switch or Router(**仮想スイッチ、仮想ルータ**)

仮想スイッチ、仮想ルータは、ネットワークレベルのルーティングやスイッチング機能を持つソフトウェアコンポーネントで、例えばハイパーバイザーのドライバ、モジュール、もしくはプラグイン等として、仮想サーバプラットフォームにおける重要な部分となり得る。単一の物理アプライアンス上のコンポーネントとして、複数のネットワーク機器の仮想アプライアンスとして実装されるものもある。

スコープガイダンス：

先述の仮想アプライアンスと同様、カード会員データ環境内に存在する、もしくはカード会員データ環境にサービスを提供していたり、接続していたりする場合は対象となる。

仮想スイッチや仮想ルータを搭載した物理デバイスも、その仮想コンポーネントがスコープ内のネットワークに接続するような場合、対象となる。

・Virtual Applications and Desktops(**仮想アプリケーション、仮想デスクトップ**)

アプリケーションやデスクトップ環境も、仮想化されてエンドユーザに機能を提供することができる。これらは一般的に中心的な拠点に設置され、リモートデスクトップインタフェースによりアクセスされる。仮想デスクトップではシンクライアントやモバイル機器を含む多数の種類の機器からアクセスを受け付けることができる。POS、カスタマーサービス、その他決済機構の中で様々な役割を持つことがある。

スコープガイダンス：

カード会員データの処理、保管、伝送に関わるのであれば仮想アプリケーションや仮想デスクトップも対象となる

仮想アプリケーションや仮想デスクトップが同じ物理ホストもしくはハイパーバイザー上にあり、十分なセグメンテーションが行われていない場合、スコープ内となるだろう。

※4.2の“Recommendations for Mixed Mode Environments”にさらに詳しい解説がある

2. Virtualization Overview (仮想化の概要)

・Cloud Computing(**クラウドコンピューティング**)

パブリック、セミ・パブリック、プライベートなインフラ上で提供される、サービスもしくはユーティリティとしてのコンピューティングリソースの使用。クラウドベースのサービスでは通常、接続されたシステムの“pool”、“cluster”として提供されており、複数のユーザ、事業体、テナントに対してコンピューティングリソースがサービスベースのアクセスとして提供される。

スコープガイダンス：

クラウドコンピューティングを使用する場合、数多くのスコープに関する課題、懸念事項がある。

- サービスについて徹底的に調べ、詳細を理解すること
- そのサービス特有のリスクを詳しく評価すること
- その他マネージドサービスと同様、PCI DSS要件を維持するために、それぞれの当事者が持つ責任が明確に定義され、文書化されている必要がある

クラウドプロバイダー側としては、どのPCI DSS要件、システムコンポーネント、サービスがクラウドプロバイダー自身のPCI DSS準拠範囲となるのか、また、どの要件、コンポーネント、サービスがプロバイダー自身の準拠範囲ならないため、それらの準拠はサービスを利用する事業体側の責任となる旨を、サービス契約書(Service Agreement)で明確に文書化する必要がある。またサービスプロバイダとして、当該環境がPCI DSSに準拠していることを示すための十分な証跡と保証を提供すべきである。

※4.3 Recommendations for Cloud Computing Environmentsにさらに詳しい解説がある。

3. Risks for Virtualized Environments (仮想環境のリスク)

Risks for Virtualized Environmentsでは、仮想環境特有のリスクについて解説されています。仮想環境におけるPCI DSS対応は、大原則は非仮想環境と同様という旨は先述の通りですが、その大原則の上で、仮想環境特有のリスクを追加で検討する必要があるという意味で、本文書の最も重要なパートであるといえるでしょう。

3.1 仮想環境内の物理環境における脆弱性

物理インフラストラクチャに対する攻撃や存在する脆弱性は、仮想化されたシステムやネットワークにおいても同様にあてはまる。また、仮想環境をどれほど安全に構築しようとも、十分な物理的対策も必要である。

3.2 新たな攻撃の側面を作り出すハイパーバイザー

仮想環境特有のリスクのうち最も重要な箇所は、ハイパーバイザーである。なぜなら、ハイパーバイザーが侵害を受ける、もしくは適切に設定されていない場合、その上で稼働する全ての仮想マシンはリスクにさらされているということになるからである。このように、当該環境が侵害されることで全体がリスクにさらされてしまうような箇所は"単一障害点(Single Point of Failure, SPOF)"と呼ばれる。どんなに仮想マシンを安全に設定、運用していても、ハイパーバイザーが適切に設定、運用されなければリスクは上書きされてしまうことになる。

このように侵害を受ける入り口となってしまうリスクもあるが、ハイパーバイザー自身も、(仮想環境ではない)通常の物理サーバでは存在しない攻撃の対象となり得る。ハイパーバイザーの持つ分離技術、アクセス制御、要塞化、パッチ等がそれにあたる。また、ハイパーバイザーのデフォルト設定はしばしば安全でない事もある。

これらのことから、ハイパーバイザーに対する最小権限の原則や、監視等の適用も非常に重要となる。

3.3 仮想化されたシステムやネットワークの複雑性の増加

仮想環境では、仮想マシンと仮想マシンの間でのデータの伝送など、システムとネットワークにまたがった実装となることがあり、仮想ネットワーク、仮想ファイアウォール等を経由することもあり得る。このような実装は運用上のメリットもある反面、システムは複雑になり、各レイヤーに対する追加のセキュリティ対策や複雑なポリシー管理が必要となることが考えられる。

複雑性の増加は、設定ミス等が増える可能性もあり、さらには仮想コンポーネントはしばしば複製されて利用されるため、脆弱性がひとつ見つかると非常に影響範囲が広くなってしまうことも考えられる。

3.4 物理システム上の複数機能の実装

仮想環境における懸念事項のひとつとして、ひとつの仮想システム機能が侵害を受ける事により、同一物理環境上のその他の機能にもその影響が及ぶ可能性がある点が挙げられる。仮想技術の中には、機能(仮想マシン)毎のプロセス分離を強制することでこのリスクを排除しようとするものもあるが、それでも1物理システム上で複数機能を持つ事は攻撃者がホストシステムへの物理アクセスを得る可能性を高めるため、安心してはならない。

※次節参照

3.5 異なる信頼性を持つVMの混在

カード会員データを持つような、高い信頼性の求められるシステムと、それ以外の高い信頼性が求められないシステムが同一の物理環境上にホストされるような場合、注意深くリスク評価を行う必要がある。つまり、高い信頼性が求められないシステムは、侵害を受ける可能性が高くなり、そこからさらに高リスクな侵害に広がってしまう可能性があるからだ。

ここでは、信頼性レベルの著しく異なる仮想マシンは、同一の物理環境に置く事は推奨できない、ととらえることができると筆者は考えています。

3. Risks for Virtualized Environments (仮想環境のリスク)

3.6 責務の分離の欠落

ネットワーク管理者とシステム管理者の分離など、ユーザの役割をきめ細かく定義することは非常に難しく、特に仮想環境においてはハイパーバイザーへのアクセスはスイッチ、ファイアウォール、決済アプリケーション、ログ収集サーバ、データベースなど広範囲のアクセス権をあたえ得る。単一の拠点もしくは一人のユーザからのアクセスを可能とすることから、適切な責務の分離の監視と強制が非常に重要である。

3.7 休止状態の仮想マシン

多くの仮想化プラットフォームでは、VMはアクティブ状態でも休止状態でも存在できる。休止状態のVMは活発に使用されない事からセキュリティ対策を見落としがちであり、例えば最新のパッチが適用されていないVMが再稼働することによって仮想環境へのバックドアにもなり得る。また、稼働中にカード会員データを受信したVMが休止状態になった場合に、認識していない、かつ安全でない状態での保管となり得る。このため休止状態のVMの管理にも注意を払う必要がある。

3.8 VMイメージとスナップショット

VMイメージやスナップショットを取得する際に、カード会員データを保持してしまっていると、気づかないうちにカード会員データを保管してしまうことになり、最悪の場合ネットワーク上で広くカード会員データを持ってしまうことにもなり得る。また、取得したスナップショットやイメージ自体も安全に保管しないと、攻撃者がアクセスし、脆弱性もしくは悪意のあるコードをイメージに注入することができるかもしれない。侵害を受けたイメージが環境全体に配置されてしまったら、複数ホストに被害が広がってしまう。

3.9 未成熟な監視ソリューション

仮想化が広まるのとともに、ロギングや監視の必要性は強まっているものの、現在のところ物理的な環境と比べて仮想環境の監視を行うツールは成熟しているとはいえない。ホスト内の通信や、仮想ネットワーク上のVM間のトラフィックは非仮想環境と同レベルの監視が求められるのと同時に、ハイパーバイザーや管理インタフェース等を含む仮想環境特有の詳細なログも必要とされる。

3.10 仮想ネットワークセグメント間の情報の漏出

ネットワークの仮想化を検討する際には、論理ネットワークセグメント間の情報の漏出のリスクに注意を払う必要がある。データ保護機構が回避されてしまえば、データが管理外の場所に漏出してしまう可能性があり、管理機構が侵害を受けてしまうとデータレベルでの情報の漏洩やネットワークベースのセキュリティ制御機構がバイパスされるようなネットワーク経路等への影響が発生する可能性もある。仮想環境でネットワークを分離する際は、物理ネットワークの時と同レベルのセキュリティ機能を提供するのがきわめて望ましい。

3.11 仮想コンポーネント間の情報の漏出

仮想環境では、同一ホスト上で稼働する仮想コンポーネント間での情報の漏出が起こり得る。たとえば攻撃者はひとつのコンポーネントを使って同一のホスト上で稼働するその他のコンポーネントの情報を収集し、さらなる侵害のための情報を得ることができるかもしれない。もしくは、ホスト側へのアクセス権を得ることで、そのホスト上で稼働する複数のVMが取り扱う機密情報を入手することができるかもしれない。VM間での情報の漏出を防ぐためには、すべての物理リソース（メモリ、CPU、ネットワーク等）の隔離を行う必要がある。

おわりに：PCI DSS×仮想環境 Part 1

本書では、PCI SSCより公開されたInformation Supplement: Virtualization Guidelineに沿って、内容の解釈をすすめてきました。今回はかなり幅広く、用語や概念の定義からはじまり、リスクの洗い出しの部分まで読み解きました。

次回は、ここで洗い出されたリスクについて、どのような対策を行うべきなのか、”Recommendations(推奨事項)”の章に入っていきます。

単に仮想技術とはいっても、その概念や対象とする範囲など、かなり幅広くなってしまい、なかなか具体的な対策方法まで落とし込めない分野ではありますが、考え方のベクトルを示すひとつの参考になるはずですので、次回もあわせてお読みいただければ幸いです。

PCI DSS徹底解説 第10回

仮想環境に対するPCI DSSの視点…Part.1

発行：2011年11月24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>