

VISA / JCB

PCI セキュリティ・スキャン手順

バージョン 1.0

この資料は、『PCI セキュリティ・スキャン手順』を理解するために、Visa International 東京事務所および JCB が試訳した参考資料です。この資料は正式な Visa および JCB の業務文書ではありません。正は英語版の「Payment Card Industry Data Security Scan Procedures Version 1.0 December 2004」とします。万一、本文書と英語版（原本）に翻訳、解釈の相違があった場合は英語版が優先されます。

2004 年 12 月

免責

『PCIセキュリティ・スキャン手順』は、Visa およびJCBのカード情報を格納、処理、または伝送するすべての事業者が PCI データ・セキュリティスタンダード(以下 PCI 基準)を満たすためのネットワーク・セキュリティ・スキャンを実施する際の「ガイドライン」として使用される。ただし、Visa Asia Pacific およびJCBは、セキュリティ侵害または損害が発生した場合であっても、スキャンの結果が要件に準拠しているかどうかに関わらず、何ら責任または義務を負うものではない。

注意事項

『PCI セキュリティ・スキャン手順』は、一連の Visa Asia Pacific および JCB のカード情報セキュリティ (AIS) 文書の一部である。Visa Asia Pacific および JCB のメンバー金融機関およびそのエージェント (加盟店とサービス・プロバイダ) は、必ず PCI 基準に従って、カード会員情報を処理、格納、伝送しなければならない。

Visa Asia Pacific の AIS プログラムの詳細に関しては、<http://www.visa-asia.com/secured> を参照のこと。

JCB の AIS プログラムの詳細に関しては <http://www.jcb-global.com/> を参照のこと。

日本語翻訳

バージョン	更新日付
1.0	2005年6月1日

目的と対象読者

本書は、PCI の要件に準拠するネットワーク・セキュリティ・スキャンを実施するための手順とガイドラインを示す。

本書は、準拠を実証するために自身のインフラストラクチャをスキャンする加盟店、外部委託のサービス・プロバイダを対象読者としている。

はじめに

PCI 基準は、カード会員情報を格納、処理、または伝送するメンバー金融機関、加盟店、サービス・プロバイダに対するセキュリティ要件の詳細を示している。加盟店やサービス・プロバイダが PCI 基準への準拠を実証するには、各カード会社の規定に従い、ネットワークのセキュリティ・スキャンを定期的実施する必要がある。

ネットワーク・セキュリティ・スキャンは、脆弱性管理プログラムと組み合わせて使用される必要不可欠なツールである。スキャンは、Web サイトまたは外部に露出している IP アドレスを含んだ IT インフラストラクチャの脆弱性や設定ミスを判別するのに役立つ。

スキャン結果は、インターネット・ハッキングに対する保護を向上するような効率的なパッチ管理やその他のセキュリティ手段をサポートする貴重な情報を提供する。

ネットワーク・セキュリティ・スキャンは、外部に接続している IP アドレスを持つすべての加盟店とサービス・プロバイダに対して適用される。たとえ事業者が Web ベースのトランザクションを提供していない場合も、システムをインターネットからアクセス可能にするようなサービスがほかにある場合がある。電子メールや従業員のインターネット・アクセスなどの基本機能により、会社のネットワークからのインターネット・アクセスが発生する。これらの重要ではないように思われるインターネットとの接続が、適切に管理されていない加盟店やサービス・プロバイダのシステムへの侵入経路になっている場合がある。

スキャン手順

ネットワーク・スキャン要件に準拠するために、加盟店やサービス・プロバイダは、次のガイドラインに従って、Web サイトまたは外部に接続している IP アドレスを持つ IT インフラストラクチャをスキャンしなければならない。

1. すべてのスキャンは、認可されたベンダーで、外部委託業者のネットワーク・セキュリティ・スキャン・ベンダーにより実施されなければならない。すべての準拠スキャン・ベンダーは、規定された一連の手順に従ってスキャンを実施する必要がある。これらの手順では、カスタマ環境の正常な運用が影響を受けることがなく、またベンダーがカスタマ環境に侵入したり、環境を改変したりすることが一切ないことを記述する。
2. 平均月間トランザクション量が 10,000 を超えるすべての加盟店とサービス・プロバイダには、四半期毎のスキャンが必要である。
3. 本番環境のネットワークまたはアプリケーションが変更された場合、新しい脆弱性がインフラストラクチャに入り込んでいないことを保証するために、追加スキャンが必要である。
4. 加盟店とサービス・プロバイダは、Web サイトや IT インフラストラクチャをスキャンする前に次のことを実行しなければならない。
 - 外部に接続する全てのアクティブな IP アドレスのリストをスキャン・ベンダーに提供する。
 - どの IP アドレスおよびサービスがアクティブかを判断するために、ネットワーク調査を通じて外部に接続している全 IP 範囲を確かめるようにスキャン・ベンダーに要求する。
5. すべてのアクティブな IP アドレスおよび装置の定期的スキャンを実行するために、ベンダーと連絡を取る。
6. ファイアウォールや外部ルーター（トラフィックのフィルタリングに使用されている場合）など、すべてのフィルタリング装置をスキャンする。DMZ を構築するためにファイアウォールまたはルーターを使用している場合、それらの装置の脆弱性をスキャンしなければならない。
7. すべての Web サーバーをスキャンする。

Web サーバーにより、インターネット・ユーザーは Web ページを見たり、Web 加盟店と対話したりすることができる。これらのサービスは、インターネットから完全にアクセス可能なので、脆弱性のスキャンが不可欠である。
8. アプリケーション・サーバーがある場合、これをスキャンする。

アプリケーション・サーバーは、Web サーバーと、バックエンド・データベースやレガシー・システムとの間のインターフェースまたは「仲介者」として動作する。たとえば、カード会員が加盟店またはサービス・プロバイダとカード番号を共有する場合、アプリケーション・サーバーは、セキュリティが保たれたネットワークとの間でデータを伝送する機能を提供する。ハッカーは、これらのサーバーやそのスクリプトにある脆弱性を悪用して、カード情報を格納している可能性のある内部データベースにアクセスする。

Web サイト構成によっては、アプリケーション・サーバーがないことがある。この場合、Web サーバー自身がアプリケーション・サーバーとして動作するように構成されている。

9. すべての個別開発の Web アプリケーションをスキャンする。

最も捕らえにくい脆弱性としては、加盟店やサービス・プロバイダの個別開発による電子商取引(e コマース)アプリケーションを通じて入り込む危険性がある。

10. ドメイン・ネーム・サービス(DNS)をスキャンする。

DNS サーバーは、ドメイン名をインターネット・プロトコル(IP)アドレスに変換することにより、インターネット・アドレスを管理する。加盟店やサービス・プロバイダは、独自の DNS サーバーを使用しているか、インターネット・サービス・プロバイダ(ISP)が提供する DNS サービスを利用している。DNS サーバーが脆弱な場合、ハッカーは加盟店やサービス・プロバイダの Web ページを騙し、カード情報を収集できる可能性がある。

11. メール・サーバーをスキャンする。

通常、メール・サーバーは、DMZ 内にあり、ハッカーの攻撃に対して脆弱な場合がある。このサーバーは、Web サイト全体のセキュリティを維持する上で重要な要素である。

12. すべてのロード・バランサをスキャンする。

環境の性能と可用性を向上するために、ロード・バランサにより、トラフィック負荷を複数の物理サーバーに分散することができる。加盟店やサービス・プロバイダの環境がロード・バランサを使用している場合、ロード・バランサの背後にあるすべてのサーバーをスキャンする必要がある。ロード・バランサの背後にある物理サーバーをすべてスキャンしないと、脆弱性が検出されないまま残っている可能性がある。

13. 仮想ホストをスキャンする。

Web サイトのホスティングを利用しているすべての加盟店は、ホスティング・プロバイダに対して、外部に接続しているインフラストラクチャ全体をスキャンし、要件への準拠を実証するように要求しなければならない。

ホスティング環境を使用している場合、1つのサーバーに複数の Web サイトが入っているのが普通である。この場合、加盟店はホスティング会社の他のカスタマとサーバーを共有していることになる。これは、他者の Web サイトを通じたサーバーの悪用をまねく可能性がある。

14. 無線 LAN(WLAN)の無線アクセス・ポイントをスキャンする。

WLAN を使用すると、確認と対応を要するデータ・セキュリティ・リスクが新たに生ずる。加盟店、プロセッサ、ゲートウェイ、サービス・プロバイダ、その他の事業者は、潜在的な脆弱性と設定ミスを見つけるために、自身の無線コンポーネントをスキャンしなければならない。

15. スキャン・ベンダーの IP アドレスが受け入れられるように、IDS/IPS を構成する。これが不可能な場合、IDS/IPS がその作業を妨げないような場所からスキャンを行う必要がある。

準拠レポート

アクワイアラ、加盟店、サービス・プロバイダは、カード会社が事業者の準拠状況を認識できるように、カード会社所定の準拠レポート要件に従う必要がある。スキャン・レポートは共通フォーマットでなければならないが、結果は、各カード会社の要件に従って提出しなければならない。結果を誰に提出するかについては、加盟店の契約金融機関に問い合わせるか、各カード会社の Web サイトをチェックする。

レポートの読み取りと解釈

承認されたネットワーク・スキャン・ベンダーは、ネットワーク・スキャンの結果に基づいて情報レポートを作成することができる。

スキャン・レポートでは、脆弱性またはリスクの種類、関連する問題の診断、分離された脆弱性の修正またはパッチ方法に関するガイダンスについて記述する。レポートでは、スキャン・プロセスで識別された脆弱性に関する格付けを行う。

ネットワーク・スキャン・ベンダーが、独自の脆弱性レポート方法を持っていることがある。しかし、公正で一貫した準拠格付けを保証するために、ハイレベルのリスクが常にレポートされる必要がある。スキャン・レポートの解釈については、ベンダーに相談すること。

次の表は、ネットワーク・スキャン・ソリューションが脆弱性を格付けする方法を示している。この表を提示するのは、ハイレベルとみなされる脆弱性とリスクの種類を紹介するためである。

準拠しているとみなされるには、スキャン結果がハイレベルの脆弱性を含んでいてはならない。次の例では、レベル 3、4、または 5 に指定された脆弱性が、ハイレベルの脆弱性に相当する。

レベル	重大度	説明
5	緊急	トロイの木馬、ファイル読み書きの悪用、リモート・コマンド実行
4	重大	トロイの木馬、ファイル読み取り悪用の可能性
3	高	限られた読み取り、ディレクトリ・ブラウズの悪用、サービス拒否 (DoS)
2	中	ハッカーが設定上の機密情報を取得する可能性
1	低	ハッカーが設定上の情報を取得する可能性

レベル 5

レベル 5 の脆弱性の場合、リモート侵入者が、リモート・ルートまたはリモート・アドミニストレータ能力を保有してしまう。ハッカーは、このレベルの脆弱性を利用して、ホスト全体のセキュリティを脅かすことができる。レベル 5 は、ファイルシステムのフル読み書き権限、ルートまたはアドミニストレータ・ユーザーとしてのコマンドのリモート実行権限をリモート・ハッカーに与えるような脆弱性を含んでいる。バックドアやトロイの木馬の存在も、レベル 5 の脆弱性として分類される。

レベル 4

レベル 4 の脆弱性の場合、リモート・ユーザーとしては侵入できるが、リモート・アドミニストレータまたはルート・ユーザーの権限は保有しない。レベル 4 の脆弱性では、ファイルシステムへの部分的アクセス(例: 書き込みアクセス権限はないが読み取りアクセス権限をもつ)をハッカーに与える。機密情報を露呈するような脆弱性も、レベル 4 の脆弱性として分類される。

レベル 3

レベル 3 の脆弱性の場合、セキュリティ設定を含む、ホストに格納された特定の情報へのアクセスをハッカーが保有してしまう。このレベルの脆弱性では、侵入者がホストを悪用する可能性がある。レベル 3 の脆弱性の例として、ファイル内容の露呈、ホスト上の特定のファイルへのアクセス、ディレクトリの閲覧、フィルタリング・ルールやセキュリティ・メカニズムの露呈、サービス拒否 (DoS) 攻撃に対する脆弱さ、メール・リレーなどのサービスの不正使用などがある。

レベル 2

レベル 2 の脆弱性の場合、サービスの詳しいバージョンなど、一部の機密情報をホストから露呈させてしまう。ハッカーは、この情報を利用して、ホストに対する攻撃方法を研究することができる。

レベル 1

レベル 1 の脆弱性の場合、開いたポートなどの情報を露呈させてしまう。