vol. 9

PCI DSS徹底解説 第9回

ASVの役割と定期的なテスト

NTTデータ先端技術株式会社

川島祐樹

当社ASV新資格更新のお知らせ

2011年3月10日、PCI SSCより脆弱性スキャンを行う認定スキャンベンダであるASVに対する新たな要件が追加されました。これはASVに対する要件であり、PCI DSS準拠を進める、もしくは維持する加盟店やサービスプロバイダに対する要件ではありません。告知の詳細は下記のリンクをご覧下さい。

“PCI SECURITY STANDARDS COUNCIL STRENGTHENS APPROVED SCANNING VENDOR (ASV) PROGRAM WITH PCI DSS TRAINING”

https://www.pcisecuritystandards.org/pdfs/pr_110308_asv_training.pdf

このASVに対する追加要件の内容は、最低2名、”PCI ASV Training”を受講し、テストに合格しなければならないというもので、これまでは企業として資格を持っていればサービスを提供できたのですが、今後は企業としての資格に加え、専門家として従業員も資格を取得、維持しなければならなくなります。この従業員に対する資格は”Qualified ASV Employee”と呼ばれます。非公式ではありますが、”QAE”という頭文字後で呼ぶことがあります。当社では2011年6月に2名合格し、企業および専門家としての資格を維持することができました。当社では、サービス品質向上のため、QAEを増やす予定でいます。

良い機会ですので、ここで脆弱性スキャンや、ペネトレーションテストの要件と、ASVの役割、これらへの準拠を進めるにあたってのアドバイスをご紹介させていただきます。

PCI DSSとQSA、ASVの関係

PCI DSSでは、6カテゴリ、12要件に分類されていますが、ASVはその中のカテゴリ「ネットワークの定期的な監視およびテスト」、要件11「セキュリティシステムおよびプロセスを定期的にテストする」が関連します。

カテゴリ	要件
安全なネットワークの構築と維持	要件1. カード会員データを保護するために、ファイアウォールをインストールして構成を維持する
	要件2. システムパスワードおよび他のセキュリティパラメータにベンダ提供のデフォルト値を使用しない
カード会員データの保護	要件3. 保存されるカード会員データを保護する
	要件4. オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する
脆弱性監理プログラムの整備	要件5. アンチウィルスソフトウェアまたはプログラムをしようし、定期的に更新する
	要件6. 安全性の高いシステムとアプリケーションを開発し、保守する
強固なアクセス制御手法の導入	要件7. カード会員データへのアクセスを、業務上必要な範囲内に制限する
	要件8. コンピュータにアクセスできる各ユーザに一意のIDを割り当てる
	要件9. カード会員データへの物理アクセスを制限する
ネットワークの定期的な監視およびテスト	要件10. ネットワークリソースおよびカード会員データへの全てのアクセスを追跡および監視する
	要件11. セキュリティシステムおよびプロセスを定期的にテストする
情報セキュリティポリシーの整備	要件12. すべての担当者の情報セキュリティポリシーを整備する

表1. ASVが関連する要件11

PCI DSS要件11では、5つのサブ要件から構成されています。要件のタイトルで示されているとおり、ネットワークやシステムを定期的にテストおよび監視し、侵害を予防したり、侵害の発生を早期に検出したりして被害を最小限に抑えることを目的としている要件となっています。ASVが登場するのは要件11.2となります。

要件	説明
要件11.1 ワイヤレスアクセスポイントのスキャン	四半期毎に無線アナライザや無線IDS/IPS等を使用して、不正なワイヤレスアクセスポイントを検出する。
要件11.2 脆弱性スキャン	四半期毎、およびシステムの大幅な変更時に、脆弱性スキャンを実施して既知の脆弱性を検出する。
要件11.3 ペネトレーションテスト	年に1回、およびシステムの大幅な変更時に、ペネトレーションテストを実施して既知の脆弱性を検出する。
要件11.4 IDS/IPSによるトラフィックの監視	侵害の発生を直ぐに検出できるよう、IDSもしくはIPSを導入してトラフィックを監視する。
要件11.5 ファイル整合性の監視	侵害の発生を直ぐに検出できるよう、ファイル整合性監視ツールを導入して重要なファイルの整合性を監視する。

表2. ASVが登場する要件11.2

この中でも特に関連性の高い要件11.2と11.3について説明します。

要件11.2で求められる対策とASVスキャン

要件11.2では、いくつかの重要なポイントがあります。まずは脆弱性スキャンを行うタイミングについて、以下のタイミングで実施することが求められています。

・四半期毎

・システムの大幅な変更後

・基準値を超えた脆弱性検出時

四半期毎のスキャンをベースに定期的に実施、加えてシステムの大幅な変更時は臨時として実施、そしてそれぞれのスキャン時に基準値を超えた(「高」レベルの)脆弱性が発見された場合に再度実施する、という全体像になります。図1の、『③「高」レベルの脆弱性発見時』のスキャンは、①、②で「高」レベルの脆弱性が発見されなければ実施する必要はありませんし、再スキャンで再度脆弱性が検出されてしまった場合、さらにスキャンを行わなければならないため、複数回になる可能性がありますが、ここではその詳細は省略します。

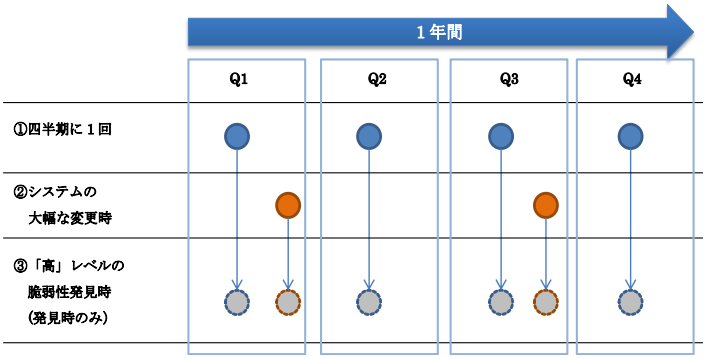

図1.　要件11.2 脆弱性スキャン年間実施契機(例)

また、これらのタイミングで、2種類の脆弱性スキャンを行う必要があります。2種類とは、外部ネットワークに対する脆弱性スキャンと、内部ネットワークに対する脆弱性スキャンの2種類です。

1.　外部ネットワークに対する脆弱性スキャン

2.　内部ネットワークに対する脆弱性スキャン

この条件を整理すると、先ほどの図1は、図2のように細分化することができます。

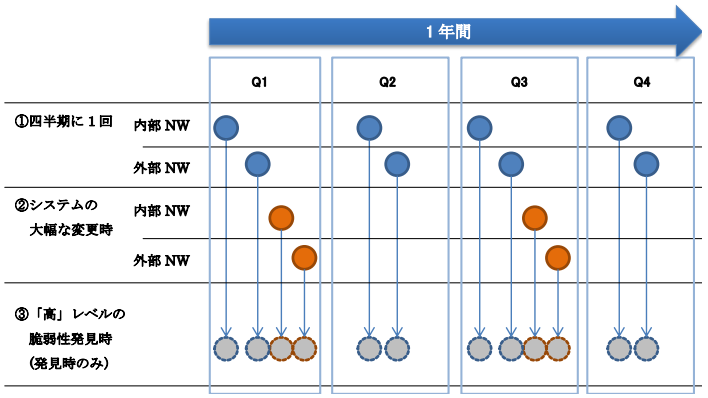

図2.　要件11.2 脆弱性スキャン年間実施契機(例)

図2を眺めてみると、実に数多くの脆弱性スキャンを実施しなければならないように見えてしまいますが、この負担を軽減する方法はいくつもあります。この方法については、本書の最後に記載しますので、そちらをご覧下さい。

さまざまな種類の脆弱性スキャンがありますが、この中に「ASVによって実施されなければならないスキャン」があります。それは、①四半期に1回のスキャンのうち、「外部ネットワーク」に対するスキャンです。つまり図3の赤枠で囲んだ部分です。

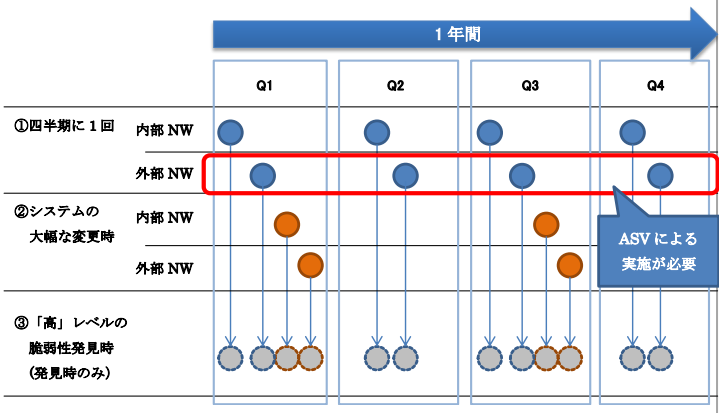

図3.　要件11.2 脆弱性スキャン年間実施契機(例)
ASVによる実施が必要なスキャン

PCI DSS徹底解説 第9回　ASVの役割と定期的なテスト

このように、ASVによる実施が必要な、四半期に一回の外部ネットワークへの脆弱性スキャンを「ASVスキャン」と呼ぶこともあります。逆に、四半期毎のスキャンでも内部ネットワークに対するスキャンや、システムの大幅な変更時のスキャン、「高」レベルの脆弱性発見時のスキャンはASVによって実施されなくても構いません。この点についての詳細も、本書の最後に記載しますのでご参照下さい。

ASVの役割

ASVは、四半期に1回の外部ネットワークに対する脆弱性スキャンを実施する必要があります。とはいっても、ASVはただスキャンを実施して報告書を送れば良いだけではなく、いくつかの役割があります。これは必ずしもスキャンを依頼する加盟店やサービスプロバイダ側で把握しておく必要はありませんが、QSA、ASV含め、ステークホルダーの役割を把握しておくと全体としてスムーズに進めることができるでしょう。

ASVは、ASV Validation Requirementという、ASVが守らなければならない要件を満たしていることを証明することでASVとなり、ASVスキャンのサービスを実提供することができます。この要件を満たし、ASVスキャンを提供できるベンダの一覧は、以下のPCI SSCサイトで閲覧することができます。

PCI SSC - Approved Scanning Vendors

https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php

ASVや、ASVスキャンに係るステークホルダーの役割については、PCI SSCが公開する”ASV Program Guide”の、”Roles and Responsibilities”で確認できます。ここでは重要なポイントのみ羅列したいと思います。

ASVの役割

- PCI DSSおよびPCI SSCにより提供される文書に従い、要件11.2の外部脆弱性スキャンを行う
- 顧客環境の通常運用に影響を与えないこと、かつ侵入、環境の意図的な変更などは行わないこと
- 個々のコンポーネント（サーバやネットワーク機器）に対するスキャンのPASS/FAILの判断を行う
- 顧客に提供された全てのIPアドレスレンジおよびドメインをスキャンする
- もし不明な（顧客に提示されていない）IPアドレスでのホストやサービスの稼動が検出された場合、顧客に問い合わせる

QSAの役割

- QSAは、PCI DSS審査を行う立場で全ての要件を確認する
- その中で、要件11.2の対応結果のレビューも行う（スキャン自体を行うわけではない）

顧客の役割

- PCI DSSに準拠する。その中で要件11.2の対応の一部として、ASVスキャンをASVより受ける
- 外部脆弱性スキャンのスコープを定義し、ASVにIPアドレスやドメイン名を提示する
- ASVスキャンの実施中、IDSやIPS、ロードバランサーなど、スキャンの正確性に影響を与えうるものについてはASVと相談して対応する（特定の期間のみ無効化する、もしくはログを無視する、など）

PCI DSSの審査では、対象範囲の特定にQSAの責任が重くのしかかってきますが、ASVによる外部脆弱性スキャンでは、対象範囲の特定に顧客から提示される内容がベースとなり、あくまで顧客側の責任という形になっています。とはいえ難しいことはそれほどなく、当該環境に係るグローバルIPアドレスおよび使用されているドメイン名を提示すれば特に問題はないはずです。

ASVスキャンの特徴

さて、ASVスキャンというものは、具体的にどのような内容なのか、「ASVは、スキャン時に顧客の環境に影響を与えないようにすること」とあるものの、脆弱性スキャンという通信を行うわけですから、何らかの影響は与えざるを得ません。ASVスキャンの内容についての要件は、上記と同様、ASV Program Guideの13ページ”ASV Scan Solution – Required Components”に詳細が記載されています。また、これはASVに対する実際の脆弱性スキャンの内容についての要件ですので、ここで求められる特徴は、PCI SSCで公開されているリストに掲載されたASVによる脆弱性スキャンであれば、すべて満たしているということになります。では、ASVスキャンの特徴をご紹介します。

- 非破壊的、つまりDoSやバッファオーバーフロー、ブルートフォースなどの攻撃や、通信帯域の過剰な占有を行ってはならない
- ホストを識別する。なお、ICMP echoだけで判断してはならない
- ポートスキャンを行う。全てのTCPとよく使用されるUDPをスキャンすること
- OS/サービスのフィンガープリントを行う。なお、可能な限りサービスをポート番号だけで判断しない
- 一般的なプラットフォームをすべて対象とすること（Linuxしか対応していない、等はNG）
- 検出レベルを正確に表現する（脆弱性の存在が確実ではない場合はそのように報告する）

ここでは各内容について詳説しませんが、注意深く、かつ正確に実施することが求められています。また、ASVによる実施が求められてはいませんが、内部脆弱性スキャンや、脆弱性検出・システム改修後の再スキャン等についても、実施手順や実施内容はこのProgram Guideを参考にしていただくのが良いでしょう。

要件11.2 脆弱性スキャンと要件11.3ペネトレーションテストの違い

要件11.2とは別に、要件11.3では年に一回、およびシステムの大きな変更後や、脆弱性検出時のペネトレーションテスト実施が求められています。

脆弱性スキャンとペネトレーションテスト、ともにシステムのセキュリティテストであることはわかりますが、どのような違いがあるのでしょうか。これはどこかで明確に定義されているわけではありませんが、PCI DSSの世界ではひとつのガイダンスが公開されています。

Information Supplement: Penetration Testing

https://www.pcisecuritystandards.org/documents/information_supplement_11.3.pdf

この文書には、具体的な細かい手順等は記載されていませんが、いくつかの重要な考え方が示されています。まず、脆弱性スキャンとペネトレーションテストの違いを表していると考えられる、重要な一節がありましたので、原文から抜粋したいと思います。

> *[excerpt] The goal of penetration testing is to determine whether unauthorized access to key systems and files can be achieved.*
>
> *（ペネトレーションテストの目的は、主要システムやファイルへの承認されていないアクセスが達成可能かを判断することです。）*

つまり、脆弱性スキャンでは、脆弱性を発見することはできても、システムやファイルへのアクセスが可能かどうかまでは確認できません。これがひとつの大きな違いと言えるでしょう。この文書には、他にもいくつかの考え方が記載されていますので、簡単にご紹介します。

・要件11.2と要件11.3は全くの別物である。11.2では脆弱性を識別（発見）し、報告するだけだが、ペネトレーションテストでは、検出された脆弱性を利用し、実際に承認されていないアクセス、もしくは悪意のある行動が可能かどうかを検証する。

・要件11.3のペネトレーションテストは、QSAやASV等が実施する必要はない。ただし、内部の担当者が実施する場合は、テスト対象の環境からは独立した組織の、経験豊富なペネトレーションテスターが実施しなければならない。

・ペネトレーションテストは、何も対象の情報を得ずに実施するブラックボックステストでも、対象に関する情報をあらかじめ取得したうえで実施するホワイトボックステストでも構わない。

おわりに：年間計画のススメ

ASVスキャンの概要と、ペネトレーションテストについて少し触れましたが、如何でしたでしょうか。PCI DSSは、大分類が12要件あり、小項目でいうと280項目に及ぶ要件に対応しなければなりません。その中のたった2要件に過ぎないのに、こんなに大変なのか、と感じられた方もいらっしゃるかもしれません。

これは、文面通りに無計画に実施してしまうと確かに対応が難しくなるかもしれませんが、少し工夫することで対応コストが時間的/費用的ともに削減できる可能性があります。そのためには、もっとも重要な点として、年間計画、可能であればさらに中長期的に計画を立てることです。いくつかのポイントを以下に記載します。なお、これは要求事項ではありませんし、ひとつの仮説にすぎません。ご検討の際の一参考情報としてのみご活用下さい。

- ペネトレーションテストと脆弱性スキャン、どちらを先に実施する方が、効率が良いかを判断する

  ⇒　通常、脆弱性スキャンで問題点が無くなった後でも、ペネトレーションテストにより追加の脆弱性が検出されることが少なくありません。

- システム更改のタイミングは計画／調整可能か

  ⇒　「四半期毎のスキャン」と、「システムの大きな変更後のスキャン」のタイミングを合わせればスキャン回数は減らせるかもしれません。

- 検出された脆弱性の基準や、対応フローを統一する

  ⇒　脆弱性スキャンやペネトレーションテスト、判断基準や実施フローが統一できれば、各スキャン／テストにおけるオーバーヘッドが減らせる可能性があります。

- 外部ベンダか、内部組織か

  ⇒　11.2.2の外部脆弱性スキャン以外のスキャンやテストを、内部組織で行うか、外部ベンダに依頼するか。また、外部ベンダでも複数ベンダに依頼するか、統一するか。これはシステムの形態や規模にかなり依存しますが、各スキャン／テストで独自に実施するよりも、全体を通して考えることで、効率的な選択方法が見つかる可能性があります。

他にも賢く対応するコツがあるかもしれません。本書や、本書でご紹介した文書等も参考にしていただければ幸いです。

PCI DSS徹底解説 第9回
ASVの役割と定期的なテスト

発行：2011年9月7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>