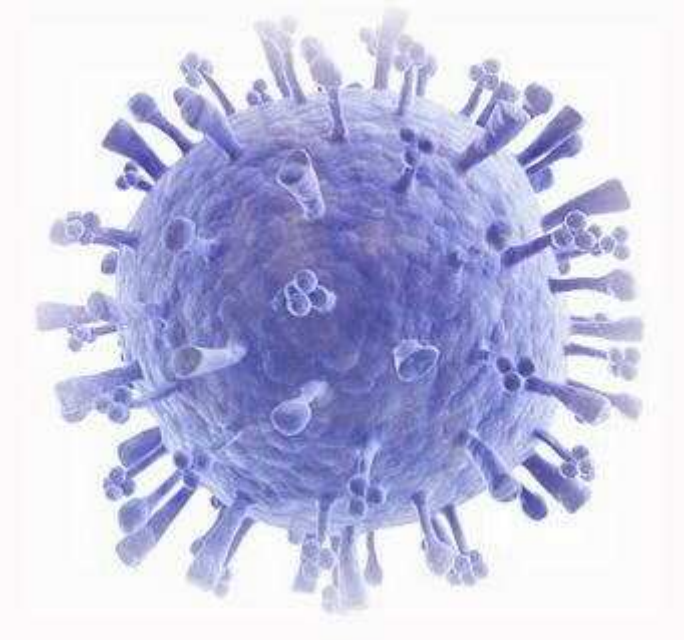
JCDSC

2012年1月26日(木)

ASVの要件

(PCISSCのプログラムガイドVer1.2より)



日本カード情報セキュリティ協議会

ベンダー部会事務局/森　大吾

ASV認定の国内ベンダー

JCDSC

・NRIセキュアテクノロジーズ株式会社
・NTTデータ先端技術株式会社
・京セラコミュニケーションシステム株式会社
・三和コムテック株式会社 （米国McAfee Inc.社／McAfee Secure）
・TI S（ソラン株式会社を統合）
・日本アイビーエム株式会社
・日本オフィス・システム株式会社 （米国Control Case社/ControlCaseGRC）
・プロティビティ ジャパン
・ベライゾン ビジネス

未掲載の会員企業様は、
ご連絡ください。

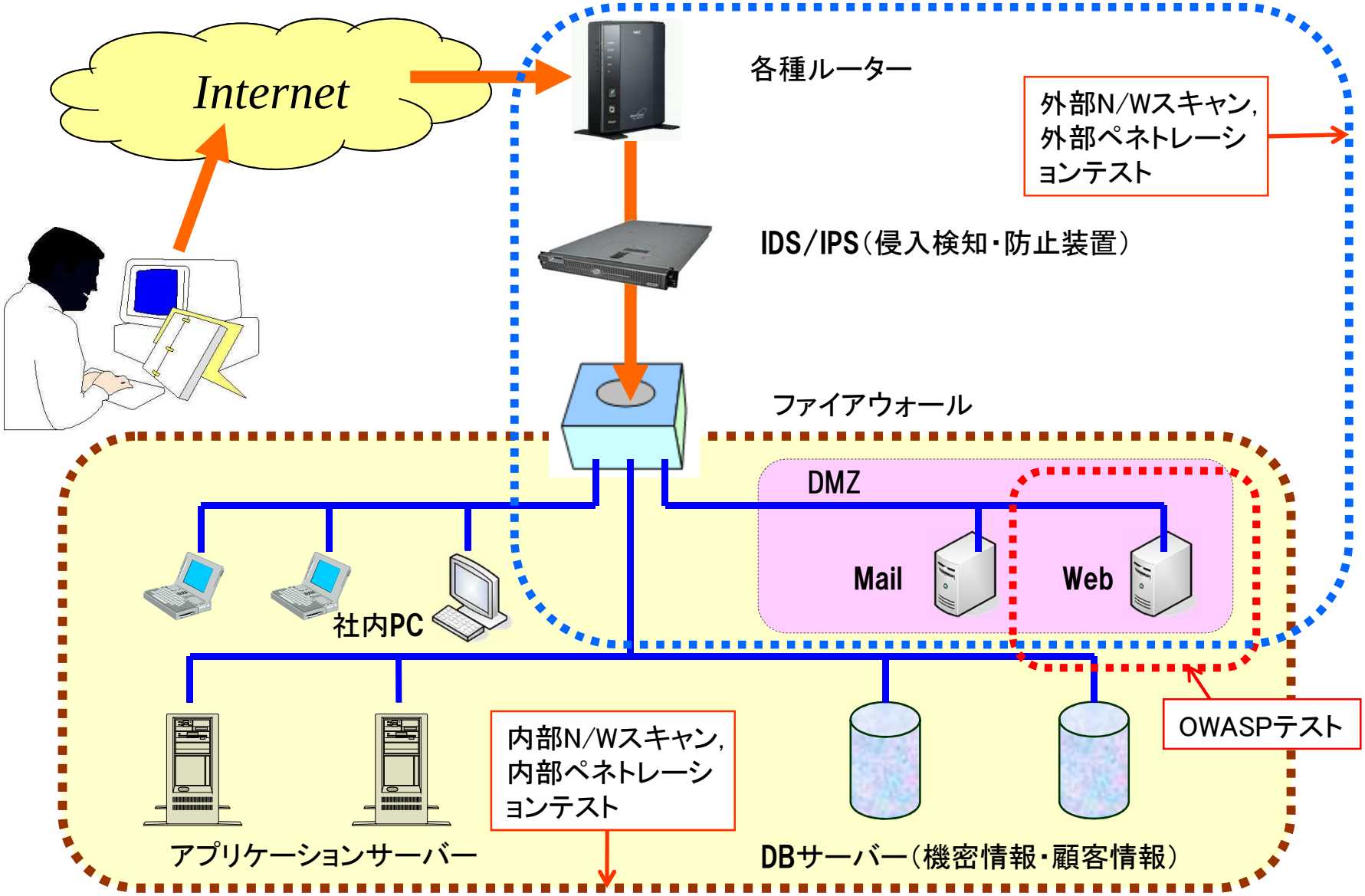
出典：JCDSC（日本カード情報セキュリティ協議会）サイト 2012.1

【PCIDSS要件】
11.2 内部および外部ネットワークの脆弱性スキャンを少なくとも四半期に一度、およびネットワークでの大幅な変更（新しいシステムコンポーネントのインストール、ネットワークトポロジーの変更、ファイアウォール規則の変更、製品アップグレードなど）後に実行する。

11.2.2 四半期に一度の外部の脆弱性スキャンは、PCISSCによって資格を与えられた、認定スキャニングベンダー（ASV）によって実行される必要がある。

各種検査の範囲 （イメージ）

JCDSC



ASVプログラムガイド

Payment Card Industry (PCI)
Approved Scanning Vendors

Program Guide
Reference 1.0
PCI DSS Version 1.2
March 2010

PCISSC（国際協議会）が規定している、ASVによる外部N/Wスキャンの実施基準。
ASVの認定を得るための、検査内容の品質について定めている。（英語版のみ）

1.確認する範囲（P12掲載の抜粋）

JCDSC

・顧客からASVに以前提供されたIPアドレスやドメインで、顧客の要望で除外されたものでも、対象に含めます。

・顧客から提供されたそれぞれのドメインが、顧客からすでに提供されたものであるかを確認するために、ドメインのIPアドレスを調べます。

・提供されたそれぞれのドメインに、普通のホスト名のDNS検索を実行します。顧客が提供しなかった「www」「メール」その他など。

・DNS検索によるMX記録で、見つかるすべてのIPアドレスを確認します。
・ウェブで到達できる範囲外のIPアドレスでも、すべてウェブサーバーを確認します。（JavaScript、 Meta redirect 、HTTP codes 30xを再調査に含めます）。

・文書化されていない領域で、顧客が所有しているドメインがないか、確認します。

・顧客がインターネット・サービス・プロバイダ（ISP）やホスティング・プロバイダーを利用している場合、ASVがスキャンできるよう、調整をする必要があります。
・特定のIPアドレスをスキャン対象から除外する場合は、適切な検査範囲とネットワークの分割を、顧客は証明する必要があります。

2.ASVスキャンの検査項目（P13掲載の抜粋）

・ASVスキャンは、すべての伝送制御プロトコル（TCP）ポートのスキャンを実行する。
・また、以下のサービスに関連したUDPポートを含む、一般のユーザー・データグラム・プロトコル（UDP）ポートのスキャンも実行する。
・認証サービス（例えばラディウスとKerberos）、バックドアとリモートアクセス・アプリケーション、バックアップ・アプリケーション、データベース・サーバー、DNS（ドメインネーム・システム）
・NetBIOSとCIFS、NFS（ネットワーク・ファイル・システム）、
・NTP（ネットワーク・タイム・プロトコル）、P2P（ピア・ツー・ピア）とチャット・アプリケーション
・RIP（ルーティング・インフォメーション・プロトコル）を含むルーティング・プロトコル
・RPC（リモート・プロシージャ呼出し）とRPCエンドポイント・マッピング
・SNMP（Simple Network Management Protocol）とSNMPトラップ、syslog
・TFTP（Trivial File Transfer Protocol）
・ISAKMP、L2TPとナッタを含むVPN（仮想プライベートネットワーク）
・スキャン顧客を、悪意のある活動と関連したポートを含む脆弱さにさらすかもしれない、他の一般のUDPポート

3.ASVスキャンの必須構成要素（P15掲載の抜粋）

JCDSC

●テストする必要のあるサービス、デバイス、オペレーティング・システム

・Firewalls & Routers すべてのフィルタリングデバイス、
・Operating Systems オペレーティングシステムが、ベンダーがサポートしているバージョンであるかを、調べられなければならない。
・DBサーバー、Webサーバー、アプリケーションサーバー、
・Common Web Scripts CGIスクリプトや電子商取引関連のスクリプト、ASP、PHPなどのような一般に見つかるスクリプトを見つけて、脆弱さを探索する。
・Built-in Accounts ルーターのビルトインか、デフォルトアカウントであるか、ファイアウォール、オペレーティングシステム、ウェブサーバー、データベース・サーバー、アプリケーション、POSシステムまたは他の構成要素を調べる。
・DNSサーバー、メールサーバー、Webアプリケーション、
その他のアプリケーション、ワイヤレス・アクセスポイント、
バックドア、SSL/TLS、リモートアクセス、
Point-of-sale (POS) ソフトウェア

4.ASV側の責任・禁止事項 （P13掲載の抜粋）

JCDSC

・Be Non-disruptive　破壊的でないこと

●次のようなテストは認められません:
・Denial of service (DoS)　DOS攻撃
・Buffer overflow exploit　バッファ・オーバーフロー
・Brute-force attack resulting in a password lockout
　　パスワード・ロックアウト中の暴力的な攻撃
・Excessive usage of available communication bandwidth
　　利用できるコミュニケーション帯域幅の過度の使用

●Perform host discovery ホストの探索
ASVスキャンは、ICMP反響(—ping)に応じない、運転中のシステムを確認する、理にかなった試みをしなければなりません。

●スキャンが、顧客のシステム環境に影響を与えないようにする。

●顧客のシステム環境を故意に変更したり、侵入したりしない。

END