VOL. 6

# PCI DSS 徹底解説 第 6 回
# 無線環境におけるセキュリティ対策


## 川島 祐樹

NTT データ・セキュリティ株式会社


### PCI DSS Wireless Guideline の公開

PCI DSS は、現在 (2010/03/10) バージョン 1.2.1 が最新です。PCI DSS の更改ライフサイクルは、以下の URL で示されている通り 24 ヶ月、すなわち 2 年に 1 回バージョンアップが行われることになります。ちなみに、派生するセキュリティ基準 "PA-DSS(Payment Application DSS)"、"PTS(PIN Transaction Security)" についても同様のライフサイクルプロセスになります。

PCI DSS のライフサイクルプロセス
https://www.pcisecuritystandards.org/pdfs/OS_PCI_Lifecycle.pdf

しかし、実装段階になると、加盟店や QSA、PO(Participating Organization) などから様々な疑問が PCI SSC に寄せられ、これをうけて補足情報 (Information Supplement) が公開されることがあります。この補足情報の中には、PCI SSC に関連する様々な企業が参加する "SIG(Special Interest Group)" というグループで内容が検討されるものがあります。以下が、現在公開されている補足情報文書です。

https://www.pcisecuritystandards.org/security_standards/pci_dss_supporting_docs.shtml

- Penetration Testing( 要件 11.3) - 2008 年 3 月
- Application Reviews and Web Application Firewalls Clarified ( 要件 6.6) -2008 年 10 月
- PCI DSS Wireless Guideline - 2009 年 7 月

今回は、これらの補足情報のうち、PCI DSS Wireless Guideline の内容の紹介をしたいと思います。無線が導入されている、もしくは検討されているような場合、PCI DSS 準拠の必要有無に限らず役立つ情報がまとまっていますので、是非ご一読ください。

### 文書の構成

PCI DSS Wireless Guideline（以下、" 無線ガイドライン ") には、おもに以下の内容が記載されています。

- 目的と対象
- PCI DSS 準拠のための無線運用ガイド
- 無線を使用していない場合も対応が必要となる要件
- 無線を使用している場合に対応が必要となる要件

PCI DSS には " 無線ネットワーク (Wireless Network)" に関連する要件が盛り込まれていますが、この目次からわかる通り、無線ネットワークが存在しない環境であったとしても、対策を行わなくてはならない要件もあるのです。なお、無線ガイドラインで言及しているのは 802.11 WLAN のみであり、Bluetooth や GPRS はカバーしていません。

### カード会員データ環境 (CDE、Cardholder Data Environment) の定義

カード会員データ環境 ( 以下、CDE) の定義は、無線ネットワークに限られることではなく、PCI DSS の準拠を目指す、もしくは維持するにあたって必ず理解が必要な考え方です。無線ガイドラインでも、冒頭でこの定義が行われています。これはよく目にするところかと思いますが、CDE とみなす大原則は以下の 2 点です。

(1) カード会員データを伝送、処理、保管するコンピュータ環境
(2) その環境に直接接続されるネットワークや装置

おそらく、(1) はわかりやすいかと思いますが、(2) の考え方が難しいところです。

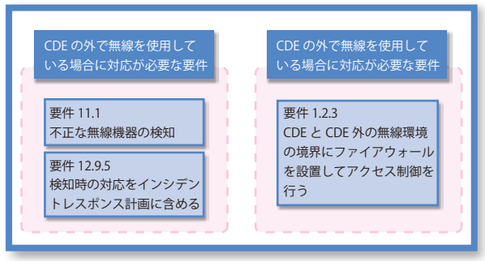
基本的に、CDE の境界で必要最小限のアクセスのみ許可し、適切に難読化 ( 暗号化など ) を行っていれば、その境界までが CDE であると考えて良いでしょう。無線ガイドラインでは、CDE において、以下 2 つの観点で無線に関連する要件を分類し、紹介しています。

(1) CDE に無線が一切存在しなくとも、対応しなくてはならない要件
(2) CDE に無線が存在する場合に、対応しなくてはならない要件

つまり、CDE に無線が存在しなければ、対応しなくてはならない要件は (1) のみ、CDE に無線が存在する場合は、(1) と (2) 両方の対策を行わなくてはならないことになります。

### 無線を使用していない場合も対応が必要となる要件

無線を使っていないのに対策が必要な要件とは、どのような要件なのでしょうか。ずばり、以下 3 つの要件が当てはまります。




**要件 11.1 無線アナライザを少なくとも四半期に一度使用して、または使用中のすべての無線デバイスを識別するための無線 IDS/IPS を導入して、無線アクセスポイントの存在をテストする。**

この要件の目的は、" 不正な " 無線アクセスポイントを発見することが目的です。無線アナライザを使う方法と、無線 IDS/IPS を使う方法が選択肢として挙げられています。ここでは、解決策として、結局有線側に接続する必要があるのだから有線側のデバイススキャン ( 例えば、nmap などを使う ) で良いのでは？と考えがちですが、無線ガイドラインによると、その方法では誤検知、非検知の確立が高い事、意図的に隠ぺいされたものを発見できないことから、有線スキャンでは不十分であると明確に述べられています。

無線アナライザと、無線 IDS/IPS のどちらを使うのが良いのか、という点については、基本的に CDE となる拠点が単一の場合は無線アナライザ、CDE となる拠点が複数存在する大型組織の場合は無線 IDS/IPS を使うことが推奨されています。

また、発見された不正な無線デバイスを排除するためのプロセスが必要です。すなわち、不正な無線デバイスの検知はトリガであり、そこからインシデントレスポンスプロセスにつながっていく必要があります。インシデントレスポンスプロセスに関する要件は、以下、12.9.5 になります。

**要件 12.9.5 ( インシデント対応計画に ) 侵入検知、侵入防止、およびファイル整合性監視システムからの警告を含める。**

最後に、CDE の外に存在する無線経由のトラフィックについて言及されています。ここで述べられているのは、カードトランザクションとは無関係の無線ネットワークからのユーザが CDE に入り込んでくることを防ぐことです。以下の要件が該当します。

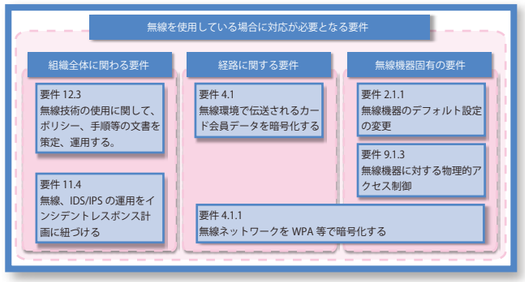
**要件 1.2.3 すべてのワイヤレスネットワークとカード会員データ環境の間に境界ファイアウォールをインストールし、ワイヤレス環境からカード会員データ環境へのすべてのトラフィックを拒否または制御 ( そのようなトラフィックが業務上必要な場合 ) するようにファイアウォールを構成する。**

これは、基本的に必要となるトラフィックのみファイアウォールを通過するようにしていれば問題ないはずですが、分離のための一例として VLAN による CDE と無線ネットワークの分離は不十分であると書かれています。VLAN はアクセス制御の手段ではなく、大規模な LAN を効率的に管理するための技術であるため、単に VLAN を分けるだけでなく、アクセス制御も行わないと、この要件に対応しているとはいえないでしょう。

細かい部分ではファイアウォールのログの確認やファイアウォールルールの 6 カ月毎のレビューも関連するところですが、CDE に無線が存在しない場合も対応しなければならない要件として、主に上記 3 つが挙げられています。

### CDE で無線を使用している場合に対応が必要となる要件

次に書かれているのが、CDE で無線を使用している場合に適用される要件です。下記の通りの要件が該当します。




CDE で無線を使用していない場合には N/A( 該当しない ) となる要件もあります。ここでは、簡単に説明を記述しますが、無線ガイドラインには詳細な説明と、店舗などのサンプルネットワーク構成によるケーススタディ等が記載されていますので、是非そちらもご参照ください。

無線アクセスポイントだけではありませんが、物理的にアクセスが可能な場所に設置されているデバイスは、リセットボタンを押しながら再起動することにより設定がリセットされるデバイスがあります。また、物理的にアクセス可能である場合のリスクとしては、シリアルコンソールによる操作なども挙げられます。よって、以下の要件が対象になり、物理的アクセス制御 ( 許可なしに入れない場所に設置する、など ) となります。これは、適切にアクセス制御を施すことが可能なアクセスポイントの選定、といった事にもなりうる要件です。

**要件 9.1.3 無線アクセスポイント、ゲートウェイ、およびハンドヘルドデバイスへの物理アクセスを制限する。**

次に、アクセスポイントのデフォルト設定の変更です。ワイヤレスデバイスだけではありませんが、出荷時の状態の各種設定は脆弱であるケースが多いことから、適切にセキュリティチューニングを行う必要があります。管理コンソールや SNMP、WEP のみによるアクセス制限、などのほかにも、正しく管理するための時刻同期やログ等について、適切に設定を行う必要があるでしょう。

**要件 2.1.1 カード会員データ環境に接続されている、またはカード会員データを伝送するワイヤレス環境の場合、ワイヤレスベンダのデフォルト値を変更する。これには、デフォルトのワイヤレス暗号化キー、パスワード、SNMP コミュニティ文字列が含まれる ( ただし、これらに限定されない )。認証および伝送のために、強力な暗号化技術のワイヤレスデバイスセキュリティ設定が有効になっていることを確認する。**

PCI DSS では、IDS もしくは IPS を導入してネットワーク全体を監視し、不正もしくはその可能性が発生した時のためのインシデントレスポンス体制を維持することが求められます。無線 IDS/IPS を使用している場合は、通常の IDS/IPS と同様に管理することが求められています。ただし、無線 IDS/IPS 自体が必須要件というわけではありませんので、あくまで、「無線 IDS/IPS を使用している場合、単に設置しておくだけではなく、適切に運用しなさいと」いう意味であると私はとらえています。

**要件 11.4 侵入検知システムや侵入防止システムを使用して、カード会員データ環境内のすべてのトラフィックを監視し、侵害の疑いがある場合は担当者に警告する。すべての侵入検知および防止エンジンを最新状態に保つ。**

次は、WEP を使ってはいけない、という要件です。では、どのような設定 / 方式なら良いのかというところにも触れられており、802.1x と AES を併用した WPA/WPA2 を使用することが推奨されています。また、WPA PSK(Pre Shared Key) の場合、パスワードは 13 文字以上のランダム文字列の使用、および定期的な鍵変更が推奨されています。

**要件 4.1.1 カード会員データを伝送する、またはカード会員データ環境に接続しているワイヤレスネットワークには、業界のベストプラクティス (IEEE 802.11i など ) を使用して、認証および伝送用に強力な暗号化を実装する。**

これも無線ネットワークに限られる要件ではありませんが、無線ネットワーク自体は先述のように WPA 等で暗号化されていますが、これはあくまで経路の暗号化ですので、カード会員データを伝送する場合はエンドツーエンドの暗号化手法として、SSL/TLS、IPSEC などを使う必要がある、ということになります。

**要件 4.1 オープンな公共ネットワーク経由で機密性の高いカード会員データを伝送する場合、強力な暗号化と SSL/TLS または IPSEC などのセキュリティプロトコルを使用する。(～略)**

最後に、無線ネットワークの使用にあたり、様々なポリシーを策定、運用する必要があることが述べられています。重要なテクノロジは、企業が承認した製品のリストの中から選び、許可された方法での使用のみに限ること、カード会員データを無線経由で伝送する際は必ず暗号化すること、などをポリシーに盛り込む必要があります。もちろん、ポリシーだけというわけではなく、関連する手順書なども必要になってくることでしょう。

**要件 12.3 従業員に公開されている重要なテクノロジ ( リモートアクセステクノロジ、無線テクノロジ、リムーバブル電子メディア、ラップトップ、携帯情報端末 (PDA)、電子メイルの使用、インターネットの使用など ) に関する使用ポリシーを作成して、すべての従業員および派遣社員向けにこれらのテクノロジの適切な使用を定義する。これらの使用ポリシーでは以下を要求する。**

### 今後の展開予測

無線ガイドラインは、現在のところ Wireless SIG によってまとめられた独立したガイドラインという位置付けではありますが、PCI DSS 次期バージョンの内容検討時には、このガイドラインに記載された内容が加味される可能性もあります。カード会員データを扱っている場合はもちろん、扱っていない場合でも、本ガイドラインをご一読されることをお勧めします。

※日本語版 Wireless Guideline につきましては、E-mail にてお問い合わせください。
E-mail：pci@nttdata-sec.co.jp