VOL. 5

PCI DSS 徹底解説 第５回
カード会員データを探せ！！

川島 祐樹
NTT データ・セキュリティ株式会社

まずは PCI DSS のスコープを再確認

前回以前にもお伝えしている通り、PCI DSS の対象範囲は、カード会員データの処理、つまり以下が行われているところです。

- 伝送・・・ルータ、ファイアウォールなど
- 処理・・・FEP(Front End Processor)、アプリケーションサーバなど
- 保管・・・メインフレーム、データベースサーバ、ログサーバ、紙、電子媒体など

通過するだけであったとしても、PCI DSS 対応を行わなければならない対象となります。もちろん、通過するだけのサーバと、保存も行っているサーバでは対策にかかるコストに違いは出るでしょう。しかし、伝送、処理、保管のうちいずれかを行っているサーバやネットワーク機器が 1 つでも存在する場合、そのセグメント自体が対象となってしまうことから、スコープを見極める際には気をつける必要があります。
例えば図 1 のように、ファイアウォールなどでアクセス制御がほどこされていたとしても、各セグメントにカード会員データを伝送もしくは保存しているサーバが 1 台ずつ存在するだけで、同一セグメント（両方のセグメント）にあるサーバは、カード会員データを取り扱っていないにもかかわらず、対象となってしまいます。

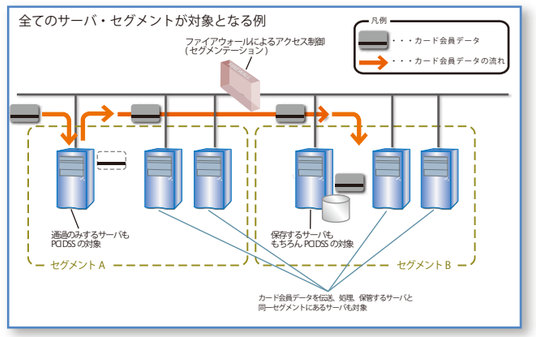

図 1. 全サーバが対象となってしまう例

無駄に PCI DSS 対象範囲が広がってしまうのは不本意ですから、以下のように、カード会員データを取り扱うサーバや機器は、単一もしくは少数のセグメントに閉じ込めて、孤立化させるのが理想的です。

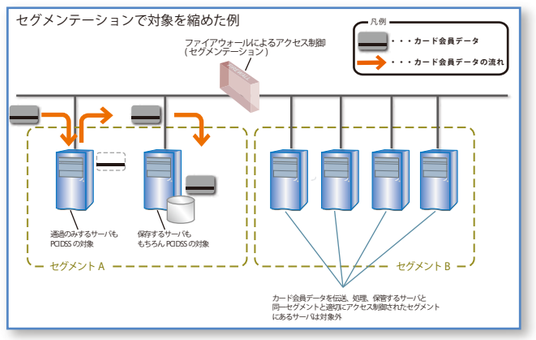

図 2. セグメンテーションで対象を縮めた例

ただし、このように構成を変更できることはむしろまれであり、簡単に対象範囲を縮めることはなかなかできないでしょう。システム更改など大規模な見直しの機会には必ず、設計段階から上記の PCI DSS 対象範囲の考え方を考慮すべきです。

カード会員データを探せ！！

では、上記、セグメンテーションのようなボトムアップアプローチではなく、現状のシステムを目の前にして、コスト対効果は多少悪くても現在の構成を維持したままひとまず短期的な準拠を目指すという、トップダウンアプローチも選択肢としてはあるはずです。そのような時はまずどうしたら良いのでしょうか。ずばり、これしかありません。

とにかくカード会員データを探す！

今、動いている業務全体を通して、とにかくカード会員データを探します。データベースサーバやホストコンピュータなど、カード会員データが存在していることが明確な部分は当然ですが、特に以下のような場所を探してみるのが良いでしょう。

●店舗
- POS レジ、CAT 端末
- 店舗サーバ
- 無線 LAN のログ

●センタ
- アプリケーションサーバのログ
- データベース
- メインフレーム
- バックアップ媒体
- バッチサーバ

●オフィス
- マニュアルオペレーションで使用するデータ（EXCEL 等）
- インプリンタ伝票
- FAX の記録、もしくは受信したもの
- 端末内のメール
- メールサーバのアーカイブ、ログ

もちろん、各環境において、「もっとこういうところにもあるはず」と、カード会員データを取り扱っている皆様はお気づきになられることかと思います。是非、関連業務をされている様々な方で集まり、「ありそうな場所」の洗い出しを行ってみて下さい。

カード会員データがここにあった！次にどうするか

カード会員データのある場所を調べられる限り、また、考え付く限り挙げられたら、実際に探してみます。探し方は様々な方法があると思いますが、以下のような観点で探してください。

▼カード会員データに関する、直接的な情報

まずは、カード会員データ自体の情報を確認します。これらの情報がなければ、PCI DSS 対策をしようとしても過不足が必ず生じてしまうでしょう。ただ、あまりに長期間かけて調べていると終わりがない作業のようになってきてしまいますので、２～３週間、遅くとも 1 か月くらいで調べ終え、次のステップに進むのが良いと思います。もちろん、規模にもよりますので、皆様の環境に合わせてうまく「短すぎず、長すぎない」期間を目標に立て、実施してみてください。

どこに保存されているのか？

物理的、および論理的な「場所」を確認します。店舗なのか、もしくはセンタなのか、センタであればどのサーバの、どのファイル、もしくはデータベース上であればどのテーブルにあるのかを確認します。

カード会員データの種類は？

磁気ストライプデータなのか、PAN なのか、PAN の一部なのか、有効期限もあるのか、など、カード会員データといっても具体的にどのような情報が存在するのかを確認します。

どうやって保存されているのか？

保存されているカード会員データは、そのまま平文で保存されているのか、もしくは暗号化されているのか。切り捨てられて一部だけ保存されているのか、マスキングされているのか、など、どのように保存されているのかを、主に「そのデータを見てカード会員データを判読できるか」という観点で確認します。

その他の情報

保存されている件数、どれだけの期間保管している必要があるのか、もしくは、特に決まっていないのか、など、件数と保存期間について確認します。このあたりは次第に確認が難しくなってくるかもしれません。件数はあまり細かく確認する必要はありませんし、期間についても「１年」なのか「５年」なのか「１０年」なのか、「リソースのもつ限り」なのかが確認できれば良いでしょう。

▼カード会員データに関する、間接的な情報

上記のようにカード会員データの場所、種類、方法、件数と保存期間、が確認できたら、次はこれらの情報に関連する情報を深く調べていきます。具体的には、以下のような情報です。

アプリケーション

決済アプリケーションであれば、その決済アプリケーションの名前やバージョン、機能の概要を調べます。POS 上のオーソリゼーションやセトルメント、また、センタ側でそれらの通信に対応するもの、ネット決済であれば Web アプリケーションの一部など、決済アプリケー ションには様々な種類がありますが、それぞれのアプリケーションについて、「PABP」もしくは「PA-DSS」に準拠しているかどうかを確認します。サードパーティのベンダが開発、販売しているものであれば、ベンダに確認する必要があるかもしれません。

保存先／データベース

上記アプリケーションで使用しているデータベースがあればデータベースの名前やバージョンを調べます。それぞれに保管されたカード会員データは、暗号化等が行われているかどうかも確認します。

ハードウェア、OS、およびその他の情報

決済アプリケーションやデータベースが稼働している、OS の種類とバージョン、アンチウィルスソフトウェアの導入状況、ファイル完全性監視を行っているのであればそのソフトウェア名もしくは方法を確認します。

ログ記録状況

上記、アプリケーション、データベース、OS 上において、どのようにログが記録されているのか、記録されたログはどれくらい保管されているのかを確認します。

確認しなければいけない情報は、想像よりも多かったかと思います。しかし、後々の対応のスピードや、手戻りの少なさは、ここでどれだけ正確に確認できるかにかかっているでしょう。複数部署はまたがることはもちろん、サードパーティの企業や、SIer など、企業間もまたがって対応しなければわからない情報もあるかもしれません。しかし、PCI DSS 対応を行うこと自体、組織や会社の敷居をまたがった協力体制が必要なはずですから、ある意味 PCI DSS 準拠のための体制作りも兼ねている、と考えてみても良いのかもしれません。

すべて確認できたら？

これらの情報を調べ終わってしまえば、既に「どの部分が危なそうだ」と、だいたいわかってしまうかもしれません。リスクの高そうな部分から対応されることをお勧めします。もちろん、前回ご紹介した「Prioritized Approach」も活用されると良いのではないでしょうか。
実は、これらの情報は、PCI DSS の最終的な報告書、「Report on Compliance」に記載しなければならない情報なのです。つまり、PCI DSS に準拠するためには避けて通れないプロセスになります。QSA が審査をするにあたり、これらの情報を提出する、もしくは審査中に同様の内容を尋ねることは確実です。（コンサルティング等も提供している QSA であれば、これらの作業を手伝ってくれるかもしれません。）これから準拠を目指すのであれば、できるだけ早い段階でこれらの情報の確認に着手することをお勧めします。