VOL. 3

PCI DSS 徹底解説 第３回 ネットワークセグメンテーションによるアプローチ

川島 祐樹
NTT データ・セキュリティ株式会社

2008 年 10 月、PCI DSS バージョン 1.2 が公開されました。
まだ英語版しかありませんが、Summary of Changes（変更点の概要）も公開されていますので、ご一読下さい。
https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

PCI DSS バージョン 1.2 では、様々な項目について明確化、説明の付与などが行われ、より分かりやすく、必要に応じて柔軟になっています。基本的な考え方は変わっていませんが、注目すべき事項として、ネットワークセグメンテーションについての説明が詳しくなり、重要性が強調されたことがあげられます。

通常、ネットワークセグメンテーションというとルータを使用してし、ブロードキャストドメインを分割することを指しますが、PCI DSS で言及しているネットワークセグメンテーションはさらに厳格なセグメンテーションが定義されており、カード会員データを守るために非常に効果的なアプローチになります。PCI DSS のバージョン 1.1 でもネットワークセグメンテーションについては言及されていなかったわけではありませんが、バージョン 1.2 になってさらに詳しく定義されたといえます。

ネットワークセグメンテーションのもつ本当の意味

まずは、ネットワークセグメンテーションのもつ本当の意味と重要性について、なぜこの部分の重要性が強調されたのか、バージョン 1.2 の更新部分を通して考えてみましょう。PCI DSS バージョン 1.2 の、12 要件に入る前、序文の部分の冒頭に記載されていますが、PCI DSS においてはネットワークセグメンテーションについて、「カード会員データの存在する環境を、カード会員データの存在しない部分から隔離することによって、以下の 4 点を減少させることができる」とされています。

1.PCI DSS 審査の対象範囲
2.PCI DSS 審査のコスト
3.PCI DSS の要求事項の実装と管理のコストと難易性
4. 組織のもつリスク

ネットワークセグメンテーションによって、対象範囲の縮小、そして対応コストや管理コスト、様々なコストを抑えられるというのは、企業にとって極めて重要な事です。しかし、最も重要なのは、4 番目の「組織の持つリスク」を減少させることができる点だと考えています。セキュリティの仕事をしていると「セキュリティにはお金をいくらかけて良いかわからない」という声をよく聞きますが、いくらかけて良いのかがわからないのは、リスク分析が不足していることが原因です。定量的なリスク分析では、企業の持つリスクを、年間で損失が発生する確率 (Annualized Rate of Occurance)× 単 一 の 損 失 額 (Single Loss Expectancy) で、年間損失予測額 (Annualized Loss Expectancy) として算出することができますが、カード会員データの存在する箇所を集約し、隔離することで、発生確率も、単一の損失額も、ぐっと減らすことができるわけです。

少し話はそれますが、PCI DSS では、リスク管理について言及されているのは要件 12.1.2「脅威と脆弱性を特定し、正式なリスク評価につながる年間プロセスを含んでいる」と、その他の要件で数か所言及されているだけであり、その手法や PDCA サイクルの枠組みが詳細に記述されているわけではありません。そのため、PCI DSS への準拠と ISMS の導入などは重複するものではないということがわかります。

＊参考文書・・・「新たなリスク管理の展開」
http://www.nttdata-sec.co.jp/article/security/071031.html

もしも年間損失予測額以上のコストをかけなければ十分な対策を実施できないのであれば、そのビジネス自体は常に継続困難の危機にさらされることになるため、根本的に考え直さなくてはなりませんが、基本的にこの年間損失予測額が、行うべきセキュリティ対策の上限額になるはずです。
どの程度下回ることができるかは、その対策の費用対効果に依存することになります。そのため、ネットワークセグメンテーションを行うことは、PCI DSSの調査、および対策や維持管理を行うコストを減らすことだけではなく、自組織の持つリスク自体を減少させることができます。
つまり、稼働しているシステムに大幅な変更を施すのは容易なことではありませんが、初期投資の金額に左右されずに、長期的なコスト (TCO) を考えれば、比較的大きな変更となるネットワークセグメンテーションであっても、対応方法のひとつとして十分考慮する価値があるはずです。

米国内のとあるホワイトペーパー (下記参照) においては、PCI DSS に準拠し、維持するコストは、複雑なシステムや古いシステムでは数百万ドル (＝数億円) かかるとも言われています。ちなみに、PCI DSS に準拠せず、情報漏えいが発生してしまった場合は、準拠、維持するコストに比べ、20 倍を簡単に超えてしまう、という分析結果もあります。

＊参考文書・・・"PCI Compliance Cost Analysis: A Justifled Expense."
A joint analysis conducted by Solidcore Systems, Emagined Security ando Fortrex. Jan. 2008

どうやってセグメンテーションを行えば良いのか？

では、ネットワークセグメンテーションは、実際にどのように行えば、対象範囲を縮めることができるのでしょうか。PCI DSS で挙げられているネットワークセグメンテーションの方法は 3 種類あります。

(1) ファイアウォールで分割
カード会員データを取り扱っている環境 (以下、カード会員データ環境) と取り扱っていない環境の境界にファイアウォールを導入し、アクセスコントロールを施すことでセグメンテーションを行います。この方法は、PCI DSS で求められているセグメンテーションの最も標準的な手法です。当然ながら、カード会員データ環境とそれ以外の環境の間で行われる通信は、業務上必要最低限のプロトコルに制限する必要があります。ファイアウォールがあれば良いというわけではありません。もちろん、ファイアウォールのアクセス制御リストや設定について文書化を行う必要がありますので、このファイアウォールについては PCI DSS の要件 1 をはじめとする各種要求に応じて文書化、設定、変更管理等を実施する必要があります。

(2) ルータによるアクセス制御で分割
ルータは、ネットワーク、つまりブロードキャストドメインを分割し、ACL を設定することでアクセス制御を施すことができる製品があります。これを利用して、ファイアウォールと同等の IP アドレスやポートでの制御を行えば適切なセグメンテーションを行っているといえます。ただし、本来アクセス制御機器ではないルータやスイッチは、アクセス制御リストの設定方法が煩雑であったり、ものによってはステートフルに通信を制御できないものがあるため、変更が発生した際の運用コストや設定ミスの危険性を考えると、必ずしも最良の選択肢ではないと考えられます。

ネットワークセグメンテーションのコツ

(3) その他の技術
その他の技術と記載されていますが、基本的には上記のように必要最低限の通信のみ通過できるようアクセス制御を施さない限り、PCI DSS の対象範囲を縮小できるネットワークセグメンテーションと呼ぶことはできません。

まず、現状においてどのようなカード会員データを扱っており、それらのデータがどのような流れで動くのかを確認することが第一です。カード会員データを扱っている環境は、クレジットカードの機能やサービスの進歩や事業規模の変化などから、同一の規模や形態で存続することはあまり考えられず、数年もすると自組織でどのようなカード会員データを扱っているのか、どこの何のデータが存在するのかが把握できなくなってしまうことも珍しくありません。ネットワークセグメンテーションだけのためではありませんが、今一度自組織で扱っているカード会員データの種類と量、場所を洗い出し、ネットワーク図上にカード会員データの流れを表してみることが重要です。もちろん、各種デバイス、サーバに保管されているログなども含めて洗い出すのは容易なことではありませんが、ここまで出来てしまえば、今後、システム変更などが発生した際にも参考にできますし、何より PCI DSS 対象範囲が縮小できるだけのネットワークセグメンテーションの第一歩とすることができます。

カード会員データのフローを描くことができたら、カード会員データをどこに集約し、どの部分にアクセス制御機構を実装するかを考える必要があります。アクセス制御は、必要最低限のユーザが必要に応じて限られた場所からのみ、限られた操作のみできるよう実施する必要があります。同時に考えなくてはならないことは、同セグメントからの盗聴ができないようにすることや、アクセス記録の取得、管理方法です。少なくともカード会員データの存在する環境側ではどのようなアクセスがきて、誰がいつ、何をしたのかを記録することが必要です。

現状を知ることが、PCI DSS の対象範囲を縮小する第一歩です。頭ではわかっているつもりでも、その知識は複数の担当者の頭の中に分散していたり、思い違いもあるかもしれません。文書化し、情報共有することで、効率良くネットワークセグメンテーションを行うことができるでしょう。