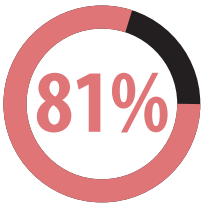
ペイメントデータセキュリティの必須事項

強力なパスワード

リスクは何か？



盗まれたパスワードや弱いパスワードのいずれかを利用したハッキング関連の侵害

(Verizon Data Breach Investigations Report 2017)

弱いパスワードやデフォルトパスワードを使用することが、企業にとってデータ漏洩の主な原因のひとつとなっています。

パスワードは、コンピュータやペメントデータのセキュリティに不可欠です。効果的なパスワードにするには、強度を高め、定期的に更新する必要があります。

コンピュータ機器およびソフトウェア（ペイメント端末）には、「password」や「admin」といったベンダのデフォルトパスワードや事前設定パスワードが設定されている場合がほとんどですが、これらは犯罪者によって広く知られてしまったり、簡単に悪用されてしまったりすることがあります。

変更が必要な、典型的なデフォルトパスワード

[なし]	root
[製品/ベンダ名]	匿名の
1234 または 4321	タベース
パス	ゲストマネージャ
アクセス	シークレット
パスワード	SysAdmin
admin	ユーザ

パスワードのベストプラクティス

侵害のリスクを最小限に抑えるため、企業はベンダのデフォルトパスワードを強力なものに変更し、共有しないようにする必要があります。従業員ごとに個別のログイン ID とパスワードを使用するようにしてください。

定期的にパスワードを変更する

パスワードは歯ブラシのように扱います。他人に使わせないようにして、3 カ月ごとに新しいものに交換します。

パスワードを共有しない

各従業員は個別のログイン ID とパスワードを使用し、決して共有しないようにします。

推測しにくいパスワードにする

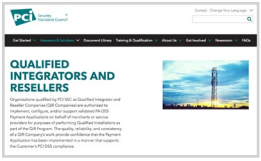
最も一般的なパスワードは、「password」、「password1」、「123456」です。このようなパスワードは、ユーザーの半分にあたる人が使用しているため、ハッカーが簡単に推測できてしまいます。強力なパスワードにするには、大文字と小文字、数字、記号の組み合わせ（!@#$&* など）を含む、7 文字以上の文字列にします。数字と記号を含むフレーズにすると強力なパスワードになる可能性があります。たとえば、好きな趣味（ILove2Fish4Trout! など）のように、ユーザーにとって特定の意味を持って覚えやすいフレーズを選択することが重要です。

リソース

リソースについては、pcissc.org/Merchants

ベンダおよびサービスプロバイダは、企業がデフォルトのパスワードを特定して変更できるよう支援します

安全な決済のためのガイドは、ペイメントデータを盗難から守るためのセキュリティの基本を企業に提供します。システムのインストーラを見つけることができます。



PCI 認定インテグレータ/リセラ（QIR）リストのリソースを使用して、企業は強力なパスワード、およびその他のペイメントデータセキュリティの必須事項について、PCI セキュリティ・スタンダードカウンシル（PCISSC）によるトレーニングを受けたシステムのインストーラを見つけることができます。

このビデオでは、ベンダのデフォルトパスワードを強力なパスワードに変更し、パスワードを共有しないようにすることで、ビジネスが侵害される可能性を最小限に抑える方法をご紹介します。

PCI Security Standards Council