適用範囲とセグメンテーション ガイダンス

Original:

PCI SSC『Guidance PCI DSS Scoping and Segmentation』

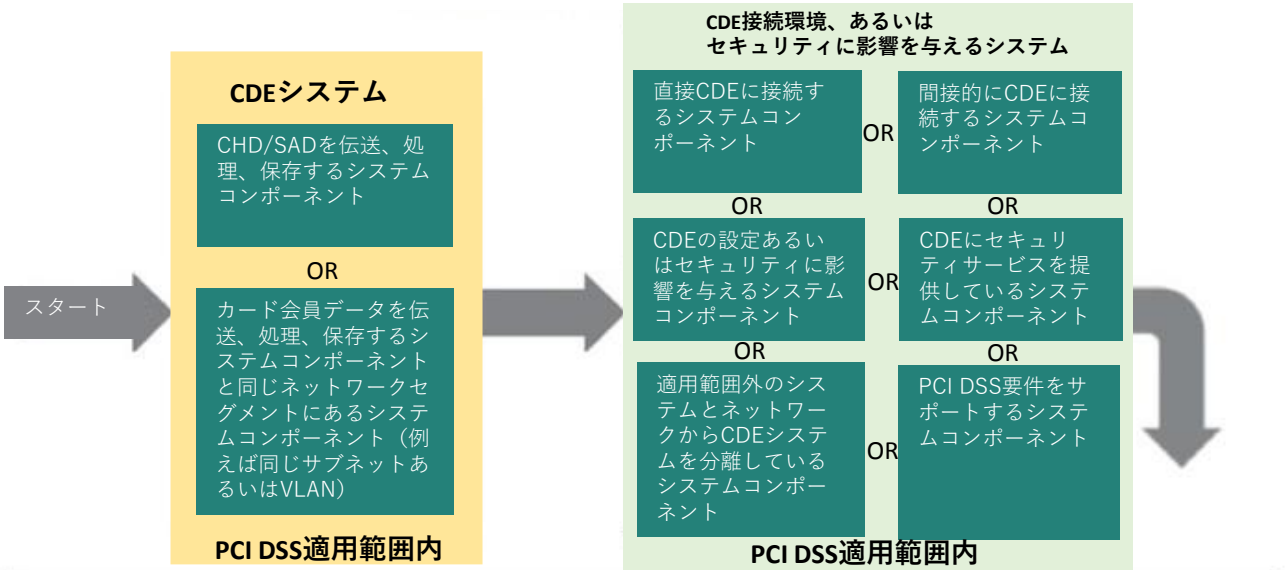
v1.1

※この抄訳はあくまでも参考として案内させて頂いたものであり、
原文と抄訳との間に齟齬がある場合には、英語の原文が優先となります。

国際マネジメントシステム認証機構
International Certificate Authority of Management System

3　適用範囲の定義と分類

図1-PCI DSS 適用範囲の分類



適用範囲外

システムコンポーネントはCHD/SADの伝送、処理、保存を**行わない。**

＋

システムコンポーネントは、CHD/SADの伝送、処理、保存するシステムとして同じネットワーク上に存在**しない。**（例えば同じサブネットやVLANではない。）

＋

システムコンポーネントは、CHDのいかなるシステムとも接続できない。

＋

システムコンポーネントは、上記に記述されたいずれの「CDE接続環境あるいはセキュリティに影響を与えるシステム」では**ない。**

＝

このカテゴリー全てに適合すれば、システムはPCI DSSの適用範囲外といえるだろう。

「CDE接続環境」あるいは「CDEのセキュリティに影響を与える」に接続するシステムは、適用範囲外のシステムが、適用範囲内のシステムコンポーネント経由でアクセスすることを防ぐコントロールが、適切に実装されている場合に限り、本分類に含むことができるであろう。

このアプローチでは、システムコンポーネントはこれらのカテゴリの1つにのみ、分類できる。これらのカテゴリは階層的であり、CDEシステムが最も高いカテゴリーとして最初に考慮されるべきである。 システムがCDEシステムの基準を満たしている場合、下位カテゴリの記述も満たしているかどうかにかかわらず、CDEシステムになる。

- 次のカテゴリには、接続先システムとセキュリティに影響を与えるシステムが含まれる。 適用範囲外システムの分類の前に優先して評価されるカテゴリである。 範囲外であるとみなされるには、システムは範囲外カテゴリの**すべて**の基準を満たし、上位カテゴリの基準のいずれも該当しては**ならない。**

- 各カテゴリの詳細は次の通りである。

システムタイプ	説明	範囲と適用性
CDE システム	• CHD/SADの伝送、処理、保存を行うシステムコンポーネント あるいは ・システムコンポーネントは、CHD/SADの伝送、処理、保存するシステムコンポーネントと同じネットワークセグメントにある（例えば同じサブネットあるいはVLAN）	システムは • PCI DSS適用範囲以内である • 全てのPCI DSS要求事項に対し、評価し、各要件の適用性を判断しなければならない。
CDE接続環境および/またはセキュリティに影響を与えるシステム	• システムコンポーネントは異なるネットワーク（あるいはサブネットかVLAN）であるがCDEにアクセスまたは接続できる（例えば内部ネットワーク接続を経由して） あるいは • システムコンポーネントは別のシステム経由ー例えばCDEにアクセスする踏み台サーバの接続経由でーCDEにアクセスまたは接続できる。 あるいは • システムコンポーネントは設定あるいはCDEのセキュリティ、またはCHD/SADの処理の方法に影響を与える可能性がある。例えばリダイレクトサーバや名前解決サーバなど。 あるいは • システムコンポーネントはCDEにセキュリティサービスを提供する。例えばネットワークトラフィックフィルタリング、パッチ展開サーバ、認証管理。 あるいは • システムコンポーネントは時刻サーバと監査ログの保存サーバのように、PCI DSS要求事項をサポートする。 あるいは	システムは • PCI DSSの適用範囲である。接続が特定のシステム上で特定のポートあるいはサービスに限定されてる場合でも、それらのシステムが適用可能なセキュリティ管理が確実であることを検証するために適用範囲内となる。 • 全てのPCI DSS要求事項に対し、評価し、各要件の適用性を判断しなければならない。 • CDEシステムと適用外のシステムの間にアクセスするパスを提供してはならない。

CDE接続環境および/またはセキュリティに影響を与えるシステム	• システムコンポーネントは適用範囲外のシステムとネットワークからCDEを分離するセグメンテーションを提供する。例えば信頼できないネットワークからのトラフィックを防ぐ設定をしたファイアウォール。	

システムタイプ	説明	範囲と適用性
適用範囲外	• システムコンポーネントはCHD/SADの伝送、処理、保存を行わない。 そして • システムコンポーネントはCHDの伝送、処理、保存を行うシステムとして同じネットワークやサブネットあるいはVLANに存在しない。 そして • システムコンポーネントはCDEのシステムに接続、あるいはアクセスすることができない そして • システムコンポーネントは適用範囲内のシステム経由でCDEにアクセスすることやCDEのセキュリティ管理に影響を与える事はできない。 そして • システムコンポーネントは上記のCDE接続システムまたはセキュリティに影響を与えるシステムについて記載された内容を一切含まない。 注記：これらシステムはPCI DSSの範囲外だが、セキュアでなければCDEへのリスクは存在する事になる。適用範囲外のシステムやネットワークについてもセキュリティのベストプラクティスの実装を強く推奨する。	適用範囲外のシステムは • PCI DSSの範囲外である。したがってPCI DSSの要求事項は求められない。 • CDEのどのシステムにもアクセスはできない。アクセスができるシステムは適用範囲内となる。 • 適切に安全を保障されていない、信頼できない（あるいは公共）と考えられる。 • CDE接続システムやセキュリティに影響を与えるシステムと同じネットワーク（あるいはサブネットかVLAN）上に存在するか、あるいは他の方法で接続できるとして、適用範囲外のシステムから適用範囲内のシステム経由でCDEにアクセスできないことを確実にするコントロールが必要である。このコントロールは少なくとも年に一度の検証を行わなければならない。

4.1 例1：CDE接続環境シェアードサービス

注記：図解は一例である。それぞれのネットワークは異なるため、あるネットワークではうまく機能するセグメンテーションが、別のネットワークでは機能しない可能性がある。したがって使用されるセグメンテーションの手法は、PCI DSSの要件ごとに徹底的にテストを行い、想定通りの動作を確認し、効果的なセグメンテーションが継続し提供されていることを確認する。 同様にここに記載されているコントロールはPCI DSSに追加されてあり、全ての環境で必要なものもあれば必要でないものもある。

「シェアードサービス」は、CDE内のシステムと適用外のシステムを含めた企業全体に提供する、認証や管理サポートといったサービスの一般的なシステムコンポーネントを指す。

一般的なシェアードサービスには以下が含まれるがこれらに限定しない。
- ディレクトリと認証 (例えばActive DirectoryやLDAP/ AAA)
- NTP- ネットワークタイムプロトコル
- DNS-ドメインネームサービス
- SMTP-Simple Mail Transfer Protocol
- 監視とスキャンツール
- バックアップツール
- アンチウイルスとパッチ展開サーバ

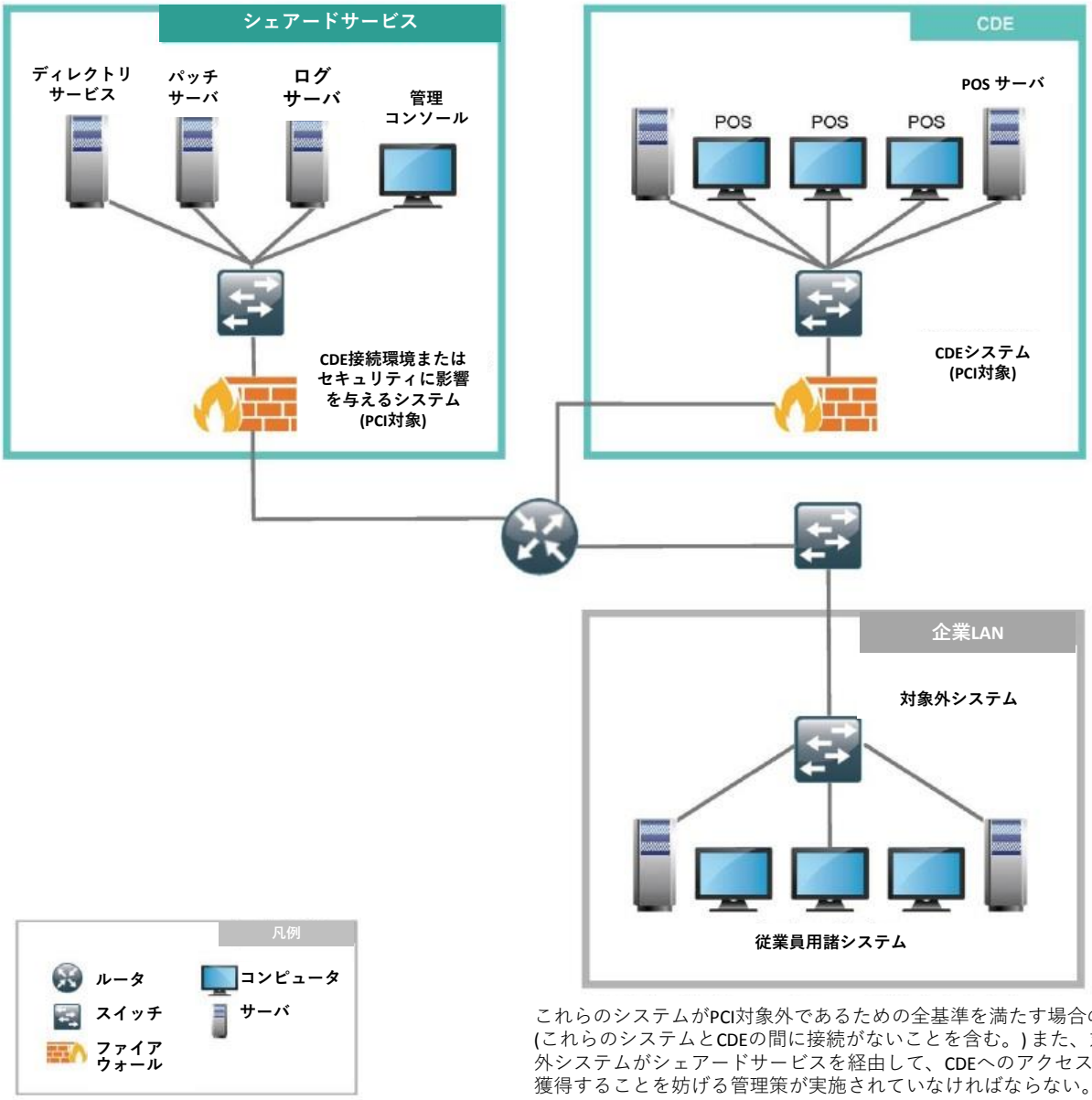
この例ではシェアードサービスはセグメンテーションされているCDEの外側に位置づけされているが、CDEにサービスを提供している。またシェアードサービスは適用範囲外とみなされている他の提携しているシステムに、認証およびまたは運用サポートの機能を提供する。これらのシェアードサービスはCDEに接続してサービスが提供されるので、PCI DSSの適用範囲内となる。

このシナリオでの課題は、企業LANのシステムがシェアードサービスに接続できるがCDEにアクセスできないように、CDEから効果的なセグメンテーションを実行する方法である。言い換えればPCI DSSの適用範囲外でシステムを保ちながら、CDEと企業LAN両方をサポートするシェアードサービスの確立方法である。

上記のこれら定義に加え以下の原則が適用される。図2と3を参照。
- シェアードサービスシステムへの管理アクセスはシェアードサービス内のネットワークからのみ許可され、それらアクセスは全てログに記録と監視をされる。
- CDEシステムへの管理アクセスはCDEあるいはシェアードサービスの指定されたシステムからのみ許可される。
- シェアードサービスシステムからCDEの全ての管理アクセスは、マルチファクター認証を使用する。全てのCDEの管理アクセスは、全てログに記録と監視をされる。
- 企業LANからのシェアードサービスへのアクセスで使用されるアカウントは、CDEのアクセス権を持たない。
- 全てのアクセスコントロールは、シェアードサービスとCDEゾーンのファイアウォールで確立し管理される。

図2-セグメンテーション図解例：接続環境シェアードサービス

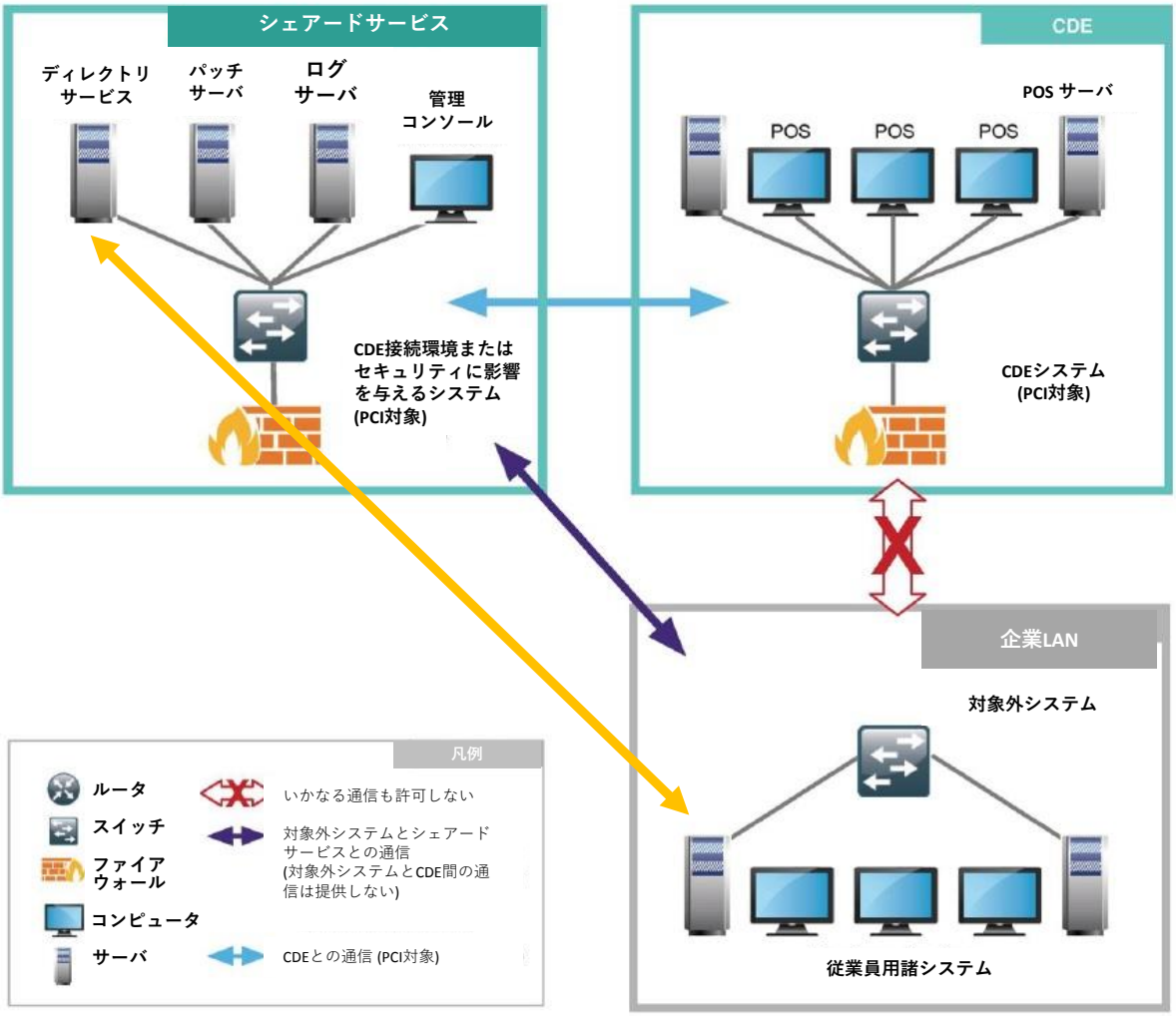
シナリオ1



これらのシステムがPCI対象外であるための全基準を満たす場合のみ。(これらのシステムとCDEの間に接続がないことを含む。) また、対象外システムがシェアードサービスを経由して、CDEへのアクセスを獲得することを妨げる管理策が実施されていなければならない。

図3-論理データフロー接続環境シェアードサービス

シナリオ1: 論理データフロー



これらのシステムがPCI対象外であるための全基準を満たす場合のみ。(これらのシステムとCDEの間に接続がないことを含む。) また、対象外システムがシェアードサービスを経由して、CDEへのアクセスを獲得することを妨げる管理策が実施されていなければならない。

下の表は上記の図2と図3に示すネットワークゾーンとPCI DSSスコープへの潜在的な影響をまとめたものである。

ネットワークゾーン	カテゴリー	PCI DSS適用範囲の影響
CDE	CDEシステム	すべて適用可能なPCI DSS要件の範囲内
シェアードサービス	CDE接続環境または セキュリティに影響を与えるシステム	すべて適用可能なPCI DSS要件の範囲内
企業LAN	システム範囲外	範囲外 企業LANにあるシステムが適用範囲外と判断される前に、セグメンテーションコントロールのあらゆるテストを行い検証しなければならない。シェアードサービスにアクセスする企業LANのシステムと人員は、シェアードサービス経由でCDEにアクセスできないようにする必要がある。セグメンテーションコントロールは少なくとも毎年一度検証されなければならない。

4.2 例2：CDE外のCDE管理端末

上記管理策に加え、次のセグメンテーション原則が例2には適用されること。

・踏み台サーバ(Bastion host)はシェアードサービスネットワークに設置されていること

・ファイアウォールおよびルータのルールは以下を保証すること。
- 企業LANから踏み台サーバへのアクセスは、管理端末からの特定のメンバーからのみに制限され、他の全ての接続の試みはブロックされること。
- 管理端末はCDEに直接アクセスできず、CDEへのアクセスに際しては必ず踏み台サーバを経由すること。

・Active MonitoringおよびDLP (Data Loss Prevention)が適切であり、カード会員データがCDEから踏み台サーバに転送できないことを確実にすること。

・踏み台サーバそのものの管理はローカルコンソールのみにより行い、リモートからの管理を行わないこと。

・管理端末自体はカード会員データを保管、処理、または送信しないこと。

・管理端末は完全にPCI DSSのスコープ内であり、すべての適用可能な要件が適用されていること。

・管理端末 (Untrustedネットワークに設置されねばならないもの)は、PCI DSS要件1.4に則り、パーソナルファイアウォール機能で防護されること。

・管理端末の使用は特定の管理担当者に制限すること。

・管理端末からの踏み台サーバへのアクセスは、CDE管理用アカウントとは異なるユーザアカウントによること。踏み台サーバへのアクセス用アカウントは踏み台サーバに対して、特権上昇を有しないこと。

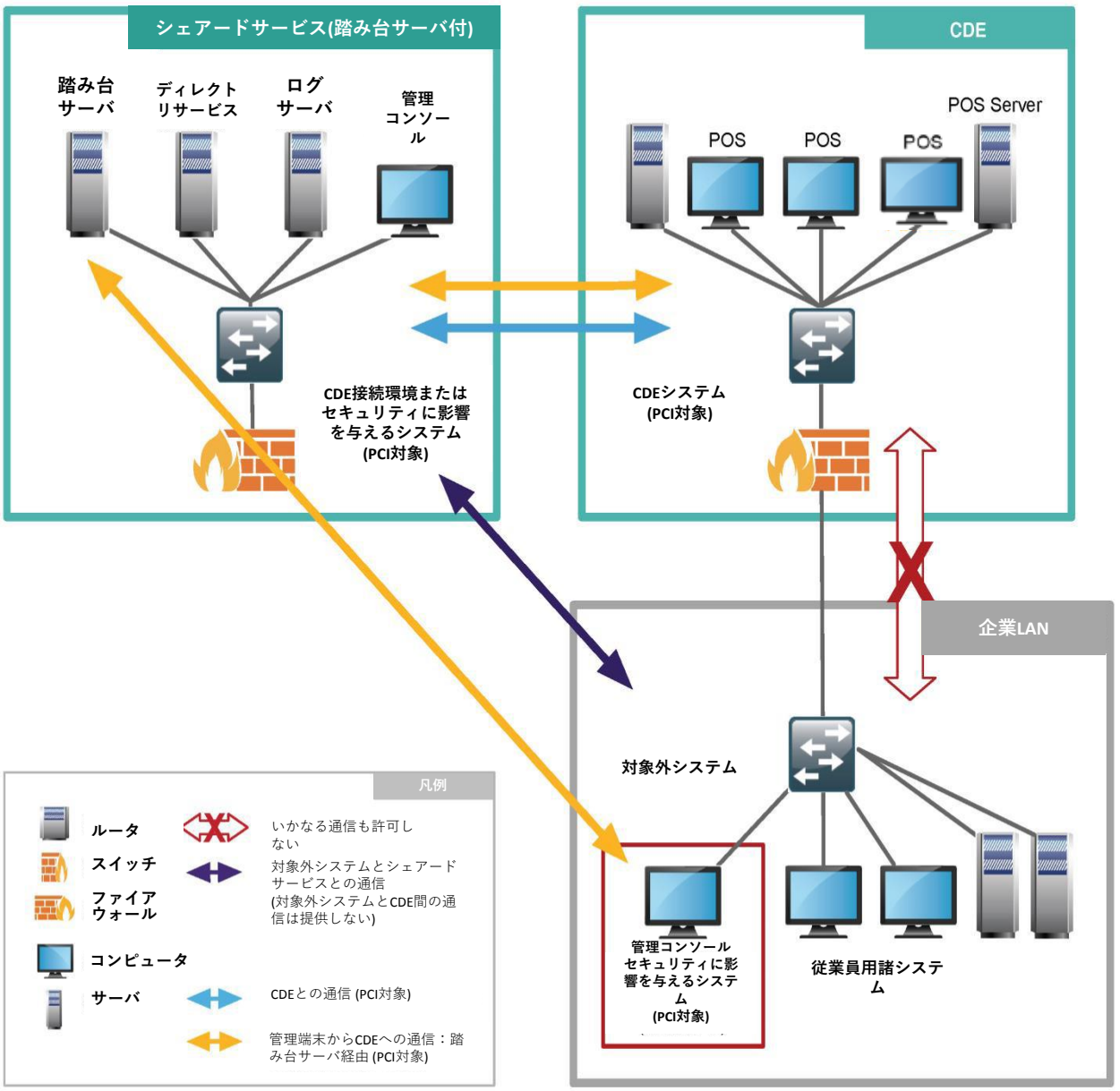
・管理端末から踏み台サーバへのアクセスは多要素認証を要求すること。少なくとも多要素認証手段の1つは、管理端末からは独立しており、管理担当者の手中にあること。
(例えば、「持っているもの」として認証される物理スマートカードまたはトークン)

・すべての適用可能なPCI DSS要件は適切であり、管理端末から踏み台サーバへの接続が、ファイアウォール、IDS/IPS、マルウェア対策、そしてその他の脅威からの防御ツールや技術を含み、セキュアであること。

・すべての適用可能なPCI DSS要件は適切であり、踏み台サーバからCDEへの接続が、ファイアウォール、IDS/IPS、マルウェア対策、そしてその他の脅威からの防御ツールや技術を含み、セキュアであること。

図5 – 論理データフロー：企業LAN内のセキュリティに影響を与えるシステムからのCDEシステム管理

シナリオ2: 論理データフロー



これらのシステムがPCI対象外であるための全基準を満たす場合のみ。(これらのシステムとCDEの間に接続がないことを含む。) また、対象外システムがシェアードサービスを経由して、CDEへのアクセスを獲得することを妨げる管理策が実施されていなければならない。

多要素認証ガイダンス

Original:

PCI SSC『Multi Factor Authentication Guidance』v1

※この抄訳はあくまでも参考として案内させて頂いたものであり、
原文と抄訳との間に齟齬がある場合には、英語の原文が優先となります。

国際マネジメントシステム認証機構
International Certificate Authority of Management System

【概要】

多要素認証の目的は、物理ロケーション、コンピューティングデバイス、ネットワークやデータベースといった資産へのアクセスに対し、高度な保障を与えることである。

多要素認証は権限のないユーザによるアクセスを防ぐための重層的なメカニズムを作成する。本資料には業界が許可した指針や多要素認証に関連したベストプラクティスが記載されている。

多要素認証とPCI DSS

PCI DSSは要件8.3とそのサブ要件の中で定義されているような多要素認証が実装されることを要求している。これらの要件の意図にあるガイダンスは、"多要素認証は、アクセスが許可される前にユーザに対し少なくとも2つの独立した認証形式(要件8.2で定義されている)を提示することを要求している"を含む規格のガイダンス欄に記載されている。

PCI DSS要件8.3では現状このガイダンス資料に記載されている全ての指針を、組織が多要素認証を導入する際に要求していないものの、これらの指針は規格の今後のバージョンで組み合わされるかもしれない。

【認証要素】

多要素認証の全体の認証プロセスはPCI DSS要件8.2で定義されている3つの認証方法のうち少なくとも2つを要求している。

a) ユーザが知っていること、

例えばパスワードやパスフレーズのようなもの。この方法はパスワードやパスフレーズ、PINや秘密の質問の回答(チャレンジレスポンス)などのユーザが提供した情報の照合を含める。

b) ユーザが所有しているもの、

例えばトークンデバイスやスマートカードのようなもの。この方法はユーザが所有する特定のアイテム(物理的、論理的なセキュリティトークンやワンタイムパスワード、キーフォブ(認証措置)、従業員カード、電話のSIMカードなど)の照合を含む。モバイル認証のためにはスマートフォンの場合、デバイス上に存在しているワンタイムパスワードアプリや暗号化の材料(すなわち証明書やキー)と結合し、所有因子を提供する。

c) ユーザ自身を示すもの、

例えば生体認証のようなものがある。この方法は個々に対し固有の特徴を照合する。例えば網膜スキャン、指紋スキャン、指静脈スキャン、顔認識、音声認識、掌形認識、耳朶形状認証

地理位置情報や時間といった別種類の情報は認証プロセスの中に追加で含まれるかもしれないが、3つの因子のうち少なくとも2つは前述で識別された因子を常に使用しなければならない。

例えば、地理位置情報や時間はユーザのワークスケジュールに従って既存ネットワークへのリモートアクセスを制限する。これらの追加基準の使用はアカウントの乗っ取りや悪意のある行動といったリスクをさらに軽減するかもしれないものの、リモートアクセス方法では”知っていること、所持しているもの、自身を示すもの”の因子のうち少なくとも2つを通じて認証を要求するべきである。

【認証メカニズムの独立性】

多要素認証のために使われている認証メカニズムは、1因子へのアクセスが他の因子へのアクセスを認めないように独立されているべきであり、1因子へのセキュリティ侵害は、他の因子による完全性または機密性に影響させない。

例えば、もし認証情報の1セット(例えばユーザネーム/パスワード)が認証要素として使用され、そして2つ目の因子(例えばワンタイムパスワード)が送られるemailアカウントへのアクセス権としても使用される場合、これらの因子は独立していない。

似たようなもので、Laptop上のソフトウェア証明書(所持しているもの)が、そのLaptopへログインするために使用した同じ認証情報(知っていること)によって保護されている場合も独立とはならない。

デバイスに組み込まれている認証情報の問題点は、因子間の独立性を失う可能性があることである。これは、デバイスの物理的な所有により、そのデバイス自体またはデバイス上に保管、生成されている証明書やソフトウェアトークンのようなトークン(所持しているもの)を通じて機密(知っていること)へのアクセスを許可されるようなケースが考えられる。

そのため、認証要素の独立性は因子の物理的な分離により成し遂げられるが、堅牢で孤立した実行環境(Trusted Execution Environment (TEE)、Secure Element (SE)、Trusted Platform Module(TPM) ※専門用語)も独立性の要件を満たすことができるであろう。

異なるチャネルを利用した認証（OOB認証）

Out-of-bandは認証方法として異なるネットワークやチャネルを通じて伝達される認証プロセスのことを言う。

認証要素がシングルデバイスやチャネルを通じて伝達されると(例えば、デバイスを通じて認証情報を入力し、そのデバイスがソフトウェアトークンを受信したり、保管したり、生成する)、デバイス管理を行うことができる悪意のあるユーザが両方の認証要素を入手することができる。

スマートフォンへのワンタイムパスワードの伝送は、効果的なOut-of-band方法を従来考慮されている。しかしながら、同じ電話を使用してワンタイムパスワードを入力する場合(例えばWebブラウザを用いるなど)、 2番目の因子としてワンタイムパスワードの有効性は事実上無効となる。

認証メカニズムのOut-of-band伝達は多要素認証のための保障レベルを向上させる追加コントロールとなる。Out-of-band伝達を使わない認証プロセスの場合、正規ユーザが認証要素を保持していることを確実にするためのコントロールを確立するべきである。

暗号トークン

暗号トークンはデバイスの中に組み込まれているものや、外付けリムーバブルメディアに格納されているものがある。

以下に述べられる暗号トークンは、"※1: NIST SP800-164"や"※2: NIST SP800-157"に基づき、モバイルコンピューティングデバイスでよく使われる因子からの一般的なものを考慮している。

参考

※1 URL: http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf

※2 URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf

■リムーバブル(組み込まれていない)ハードウェア暗号トークン

このデバイスの種類では、プライベートキーはハードウェア暗号モジュール(もしくは物理的セキュリティトークン)の中に登録されており、モバイルコンピューティングデバイスから物理的に分離されている。

モバイルコンピューティングデバイスやトークンに保管されている暗号へのアクセスは、他へのアクセスを許可しない。それゆえ、認証要素の独立性を維持している。

以下に記載する形状因子は、Secure Element (SE)となるようなモバイルデバイスに安全性と機密性を与える改竄防止の暗号化コンポーネントをサポートしている。

・暗号モジュール搭載のSDカード

モバイル電話やタブレットコンピュータのようなポータブルデバイスの中で使用する不揮発性メモリカードフォーマット

・暗号モジュール搭載のリムーバブルUICC (SIMカード)

UICC(SIMカード)は Global Platform Card Specification v2.2.1 [GP-SPEC]基づいて設定されており、IO (Input/Output)の機能と同様に記憶装置や処理として使用される。

・暗号モジュール搭載のUSBトークン

USBトークンはモバイルデバイスやパソコンを含めた様々なITコンピューティングプラットフォーム上のUSBポートに挿入するデバイスである。

USBトークンは記憶装置を搭載し、暗号法のプロセス機能も含んでいるものもある。(例えば、ユーザ特定を照合するための暗号化メカニズム)

セキュアエレメントを組み込んだもの(ICカード)を含むUSBトークンの実装は認証プロセス内で使用するのに適している。

■組み込み暗号化トークン

認証情報と、その関連付けられたプライベートキーはモバイルデバイス(※3: NIST IR7981参照)に搭載されている暗号モジュールで使用される。

これらのモジュールはモバイルデバイスのコンポーネントであるハードウェア暗号モジュールの形式か、それともデバイス上で起動しているソフトウェア暗号モジュールの形式である。

参考

※3 URL: http://csrc.nist.gov/publications/drafts/nistir-7981/nistir7981_draft.pdf

ハードウェア暗号モジュールは不変性、小攻撃面、信頼性のある動作をもつのでソフトウェアよりも望ましい。また、機能を実行するための信頼性を保障する。

ソフトウェア内で認証情報や付随するプライベートキーを保護または使用することは、キーが盗まれたり不正侵入されるようなリスクが潜在的に増加する。

【認証要素の保護】

誤使用を防ぐために、認証メカニズムの完全性や認証データの機密性を守る必要がある。

PCI DSS要件8で定義されたコントロールは権限のないアクセスや使用から認証データを保護することを保障する。

例えば：

・パスワードや他の"知っていること"のデータは、推測あるいは総当り攻撃されないように難しくするべきであり、権限のない人へ公開されないように保護するべきである。

・生体認証や他の”自身を示すもの”のデータは、誰かによってデータが存在しているデバイスへアクセスされ、許可なく複製または使用されないように保護されるべきである。

・スマートカード、ソフトウェア証明書、または他の"所持しているもの"のデータは、共有されるべきではなく、権限のない人によって複製や持ち出されないように保護されるべきである。

多目的で使用される個人用デバイス (例えば、モバイル電話やタブレットなど)を前提とする認証要素を使用する場合、デバイスが不正アクセスされるリスクを軽減するために適切に管理されるべきである。

【多段階 vs 多要素】

PCI DSSは、多要素認証の中の全ての因子は認証メカニズムがリクエストされたアクセスを許可する前に照合されることを要求している。さらに、個々の因子での成功や失敗といった情報は、全ての因子が提示されるまで、ユーザに与えられるべきでない。

もし権限のないユーザが個々の認証要素の妥当性を推測できるなら、たとえ異なる因子がそれぞれのステップで使用されていても、全体の認証プロセスとしてはシングル因子認証のステップが連なる集合体となる。

例えば、もしユーザが認証情報(例えば、ユーザネーム/パスワード)を提示し、一度認証に成功すると、認証のための2つ目の因子(例えば、生体認証)の提示を導く、これは”多段階”認証と考えられる。

多段階および多要素の両方の認証は同じ環境内で存在することもある。

例えば、ユーザがカードデータ環境へアクセスをするために独立した多要素認証プロセスを開始する前にコンピュータへログインするための認証ステップを実行するかもしれない。

このシナリオの例として、リモートユーザが企業のLaptopへログインするために認証情報を入力する。その後でユーザは多要素認証として認証情報と物理的なスマートカードまたはHWトークンといった組み合わせを使用して組織ネットワークへVPN接続を開始する。

【認証へのSMS利用】

PCI DSSはペイメント業界だけではなく、全ての業界をカバーするNISTやISO, ANSIのような業界の規格を信頼している。

NISTは現在SMSの使用を許可しているとはいえ、SMSや音声を使用したOOB認証は推奨されていないとアドバイスしており、”※4: DRAFT NIST Special Publication 800-63B Digital Authentication Guideline”の次リリースから削除されるかもしれない。

参考

※4 URL: https://pages.nist.gov/800-63-3/sp800-63b.html

【法律と規制】

組織は多要素認証の使用のための要件を定義するようなローカルおよび地域の法律を知ることを必要とする。

例えば、消費者が支払いを開始することやリスクの高い取引を実行することに認証を使用する時に追加の要求があるかもしれない。加えて、法律や規則はPCI DSSによる要求よりももっと厳しい多要素認証要件をもっている可能性もある。

PCI SSCは全ての組織に対し地域の法律や規則が多要素認証の実装上で存在する潜在的な影響を気付かせるように促す。

多要素認証のためのPCI DSSの要件はローカルや地域の法律、政府規則や他の法律上の要件に取って代わらない。

【一般的な認証シナリオ】

ここでは多要素認証のいくつかの一般的な認証シナリオとそれに対する考察を検証する

<認証ステップ>

Step1: Laptopへのログイン

Step2: CDE/企業ネットワークへのログイン

シナリオ1

ユーザは一つの認証情報セット(ユーザネーム/パスワードA)をデバイスにログインするために使用し、またそのデバイス上で保管されているソフトウェアトークンのアクセスにも同じ認証情報セットが使用されている。

そこからCDEや企業ネットワークへの接続を確立するために、異なる認証情報セット(ユーザネーム/パスワードB)およびソフトウェアトークンによって生成されるワンタイムパスワードを認証に使用する。

もし両方の因子(パスワードBとソフトウェアトークン)が有効であれば、認証システムは要求されたアクセスを許可する。

<使用している認証方法>

Step1:

・ユーザが知っていること- パスワードA

Step2:

・ユーザが知っていること- パスワードB

・ユーザが所持しているもの- パスワードAを使用した(Laptop上の)ソフトウェアトークン

認証要素の独立性を保障するために、このシナリオでは認証情報のコピーができず、他のデバイス上では使用されないような方法で物理デバイスに組み込まれているソフトウェアトークン(所持しているもの)を要求する。

その上で、デバイスに対する物理セキュリティは、デバイス所有を証明するための要求されるセキュリティコントロールとなる。そうでなければ、もしソフトウェアトークンへのアクセスが単にデバイス(ローカルまたはリモートで)にログインすることにすぎない場合、全体の認証プロセスは”ユーザが知っていること”を2度使用することとなる。

シナリオ2

ユーザは一つの認証情報セット(ユーザネーム/パスワードA、または生体認証など)をデバイスにログインするために使用し、また、そのデバイス上で保管されているソフトウェアトークンのアクセスにも同じ認証情報セットが使用されている。

そこからCDEや企業ネットワークへの接続を確立するために、ユーザはソフトウェアトークンと併用して、異なる認証情報セット(ユーザネーム/パスワードB)を自動入力させるブラウザウィンドウを起動する。(例えばデバイス上のキャッシュやパスワードマネージャの使用)

<使用している認証方法>

Step1:

・ユーザが知っていること-パスワードA

Step2:

・ユーザが知っていること- なし (パスワードBは自動入力されるため)

・ユーザが所持しているもの- パスワードAを使用した(Laptop上の)ソフトウェアトークン

このシナリオでは、認証情報のシングルセット(パスワードA)は両方の因子(パスワードBとソフトトークン)へのアクセスを与えるので、認証要素間の独立性は保障されない。

シナリオ3
ユーザは一つの認証情報セット(パスワードA)をデバイスにログインするために使用し、CDEや企業ネットワークへの接続は最初の認証情報セット(パスワードA)と、モバイルデバイス上のソフトウェアトークンによって生成されるワンタイムパスワードの両方を使用する。

<使用している認証方法>
Step1:
・ユーザが知っていること- パスワードA
Step2:
・ユーザが知っていること- パスワードA
・ユーザが所持しているもの- (モバイルデバイス上の)ソフトウェアトークン

このシナリオでは、同じパスワード(ユーザが知っていること)をLaptopとCDE/企業ネットワークの両方の認証に使用していても、モバイルデバイス上のソフトウェアトークンは認証メカニズムの間で独立性を保障し2つ目の因子(ユーザが所持するもの)として使用される。

もしモバイルデバイスからCDE/企業ネットワークへの接続を確立する場合、認証メカニズムの独立性を証明するために追加のセキュリティコントロールが必要となる。

シナリオ4

ユーザは多要素認証(パスワードと生体認証)をデバイスにログインするために使用し、そこからCDEや企業ネットワークへの接続を確立するために、シングル認証要素(署名されたチャレンジレスポンス（秘密の質問に対する回答など）、あるいは異なるパスワードやデジタル証明書)を使用する。

<使用している認証方法>

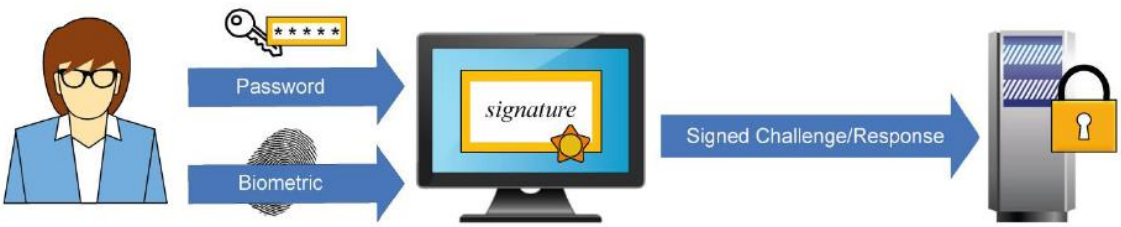
Step1:

・ユーザが知っていること- パスワード

・ユーザ自身を示すもの- 生体認証

Step2:

・ユーザが所持しているもの- 多要素認証を使用した(Laptop上の)署名されたチャレンジレスポンス



このシナリオでは、デバイスは多要素認証が厳格に実装され、必ず実行されることを保障するために強化し、制御されるべきであり、CDE/企業ネットワークへ接続する前に、常に実行されるべきである。これはユーザがセキュリティ設定を変更したり無効化できなくしたりすること(例えば多要素認証の無効化や認証回避)、そして認証要素の独立性を維持されることの保障することを含む。

さらに、権限のないユーザがデバイスとCDE/企業ネットワーク間で確立された”信頼”に対し構造的な利用をすることを防ぐために追加管理を必要とするかもしれない。
構造的な利用の例としては、悪意のあるユーザが正規ユーザによって使用されたパスワードや生体認証の情報なしで、彼らがCDE/企業ネットワークと接触することを許可するようなデバイス上のプロセスを実行するといったものがある。

ユーザが自身のデバイスを管理する場合 (例えばBYOD (Bring Your Own Device): 自分のデバイスを持ち込む環境) ではユーザ自身に管理されるデバイスは堅牢で孤立した実行環境(TEE, SE, TPMのような　※専門用語)を維持すべきであり、そのユーザにより悪影響を与えられたり、あるいは認証を回避したりすることができないようにするべきである。
そうでなければ、組織は多要素認証がデバイス上で厳密に実装され、使用を強制しているという保障はない。

※用語

SE: Secure Elementの頭文字

改竄防止ハードウェアプラットフォーム。安全にアプリケーションを実行させ、機密データおよび暗号化データを安全に保管する機能を備える。

TEE: Trusted Execution Environmentの頭文字

例えば隔離された実行を可能にする安全な機能を提供するソフトウェア

TPM: Trusted Platform Moduleの頭文字

通常のマイクロコントローラからは物理的に独立した専用のモジュールであり、暗号化キーをそのモジュールに組み込むことにより安全なハードウェアとしてデザインされている。安全な暗号化キーの生成やキー使用制限のための機能を備える。