オンプレじゃなくても大丈夫！
パブリッククラウド利用でのPCI DSS準拠の勘所

2015.7.28

株式会社エクシード

サービス開発グループ　杉森　貴博

はじめに

～会社紹介、自己紹介～

会社概要・沿革

株式会社エクシード （Xseed Co., Ltd.）

設立	2006年9月21日
資本金	7420万円
所在地	東京都品川区東五反田3-20-14 高輪パークタワー7F
電話	03-6422-0021
FAX	03-6422-0022
代表者	代表取締役社長　立川　健児
従業員数	65名　（2015年1月末現在） *パートナーを含む：約150名在籍
事業内容	マネージドサービスプロバイダー事業 ITプラットフォームインテグレーション事業
認証資格	**ISMS 認証基準：JIS Q 27001:2014（ISO/IEC27001:2013）** **認証番号：ICMS-SR0078** **PCI DSS 適合基準：PCI DSS Version3.0** **監査対象範囲：「PCI DSS 準拠マネージド・サーバサービス」のためのインフラ**

沿革

■ 2006	株式会社エクシード　設立 OSSサーバホスティング事業開始
■ 2008	㈱ワイズノット・ソリューション・テクノロジーズ よりネットワークソリューション事業譲受 OSSサーバホスティング、レンタルサーバ事業強化 ネットワンシステムズ（株）との資本提携 クラウド･サーバサービス「myDC」リリース（国内初）
■ 2009	運用管理システムSaaSリリース（NRIと協業） パブリック・クラウド「Libra」リリース
■ 2010	**ISMS認証、PCI DSS認証同時取得（国内初）**
■ 2013	APN　スタンダードコンサルティングパートナー認定 運用自動化フレームワーク「Cloudrop」リリース
■ 2014	ネットワンシステムズ（株）へ全株式譲渡 IBM Softlayerパートナー登録 ID統合管理システム運用サービス「XIDM」をリリース

自己紹介

杉森　貴博
株式会社　エクシード
サービス企画部門　サービス開発グループ　グループマネージャ
t-sugimori@xseed.co.jp

外資系ハードウェアベンダ、コンサルティング会社を経て2009年1月にエクシードに参画。
その後、システム仮想化、VDI構築、仮想環境の運用設計等のインフラ系案件のPMを担当。
2015年2月から現職。

PCI DSSに関しては、2010年の認定取得活動から関与。社内情報セキュリティ管理者も兼任。

パブリッククラウドの話をする前に・・

PCI DSSにおける第三者サービスの利用に関して

- **Third-Party Security Assurance**
  https://www.pcisecuritystandards.org/documents/PCI_DSS_V3.0_Third_Party_Security_Assurance.pdf

  PCI DSS準拠における3rdParty製品、サービスを利用する際に注意する点、順守すべき点をPCI SSCがまとめたドキュメント。

以下4つの内容が記載されている

- **Third-Party Service Provider Due Diligence**
- **Engaging the Third-Party Service Provider**
- **Written Agreements, Policies, and Procedures**
- **Maintaining Relationships with and Monitoring Third-Party Service Providers**

PCI DSSにおける第三者サービス、製品の利用に関して

- **Payment Card Industry（PCI）データセキュリティ基準 要件とセキュリティ評価手順　バージョン3.1**

「第三者サービスプロバイダ/アウトソーシングの使用」から抜粋

第三者サービスプロバイダの準拠確認には2 つのオプションがあります。

1)　自ら **PCI DSS 評価を行い**、その証拠を顧客に提出して準拠していることを示すことができます。

PCI DSSに準拠したサービスを利用する

2) 自ら **PCI DSS 評価を行わない**場合は、顧客の各PCI DSS 評価期間中にサービスのレビューを受ける必要があります。

PCI DSS審査の際に準拠しているかを確認する

PCI DSSにおける第三者サービス、製品の利用に関して

PCI DSS準拠・運用を容易にするためには、
PCI DSS準拠済みのサービスを使うことが理想。

パブリッククラウドにおいても、同様に考える必要がある。

パブリッククラウドのPCI DSS準拠

～ホントに大丈夫なんです！～

パブリッククラウドのPCI DSS準拠状況(2015/7/28時点)

内容は講演にてご紹介します

日本リージョンを使う場合

日本リージョンを使う場合、以下２つのサービスが対象となります。

日本リージョンは
PCI DSSVer3.0**準拠済み**

審査時にAoCを提示する

日本リージョンは
PCI DSS Ver3.1**取得準備中**

事前に日本MSに確認・相談

PCI DSS準拠に関して提供される情報

AWS, Azure共にPCI DSS適用範囲を記載したレポートを提供しています。まずこのレポートを入手し、内容を確認することになります。

・・・が、**それぞれ入手方法が違う**ため、注意が必要です。

PCI DSSに関する情報提供サイト

AWS

AWS PCI DSS レベル 1 よくある質問
http://aws.amazon.com/jp/compliance/pci-dss-level-1-faqs/

Azure

Payment Card Industry (PCI) Data Security Standard (DSS) Level 1
http://azure.microsoft.com/ja-jp/support/trust-center/compliance/pci-dss/

関係資料の入手

内容は講演にてご紹介します

関係資料の入手

内容は講演にてご紹介します

説明資料の違い

AWS

ドキュメントは120ページ程度。

詳細に要件項目で**ユーザが何をやるべきかを「詳細」**に記載している。

Azure

ドキュメントは13ページ。

AoCなので、**要件項目毎の対応状況が「概要」**で記載されている。

どこに対応しているか？

内容は講演にてご紹介します

お話できる範囲で・・

- 要件で必要とされている**「機能」**については提供されている。
  Firewallのステートフルインスペクション機能やウィルスチェック機能等
  ただし、**一部未対応なものもある**ため、詳細はドキュメントを確認。

- システムを設置しているデータセンターの物理セキュリティ部分は担保される。→審査時のデータセンタ確認がなくなる！

設計・設定要件や運用要件対応は、
利用者側の責任となる。

導入効果

PCI DSS特有の環境ではなく、他のユーザも使っている環境ですので、
パブリッククラウドのメリットは十分に享受できます。

メリット①：初期投資コストの削減

メリット②：柔軟なリソースの増減

メリット③：高い可用性を安価に実現

実際に利用する際のポイントは？

次項では、AWSを例にとって、利用する際のポイントを紹介します。

AWSでの利用ポイント

AWSの責任共有モデル

AWSは責任共有モデル(shared responsibility model)を採用しています。この方式はAWS,利用ユーザそれぞれの責任範囲を明確にしており、PCI DSSとの相性が良いです。

AWS利用のポイント

方法その1：AWSサービスを使う

方法その2：その他サービス・製品を使う

AWSでサービスを使う

AWSで提供しているPCI DSS準拠サービスは以下となります。(*1)

- AWS Auto Scaling
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- Amazon DynamoDB (DDB)
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)
- Amazon Glacier
- AWS Identity and Access Management (IAM)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon SimpleDB (SDB)
- Amazon Simple Storage Service (S3)
- Amazon SQS
- Amazon SWF
- Amazon Virtual Private Cloud (VPC)

上記以外のサービスの利用はお勧めしません。

(*1)https://s3.amazonaws.com/awsmedia/jp/wp/AWS_Risk_and_Compliance_Whitepaper.pdfの情報を基に記載

AWSサービスを使う

PCI DSS環境上で利用を推奨するサービスは以下となります。

- **AWS Auto Scaling**
- AWS CloudHSM
- AWS CloudTrail
- **AWS Direct Connect**
- Amazon DynamoDB (DDB)
- **Amazon Elastic Block Store (EBS)**
- **Amazon Elastic Compute Cloud (EC2)**
- **Elastic Load Balancing (ELB)**
- Amazon Elastic MapReduce (EMR)
- Amazon Glacier
- AWS Identity and Access Management (IAM)
- Amazon Redshift
- **Amazon Relational Database Service (RDS)**
- Amazon Route 53
- Amazon SimpleDB (SDB)
- **Amazon Simple Storage Service (S3)**
- Amazon SQS
- Amazon SWF
- **Amazon Virtual Private Cloud (VPC)**

各サービス毎に**要件項目への対応状況が違う**場合があり、
前出のコンプライアンスパックでの詳細確認が必要です。

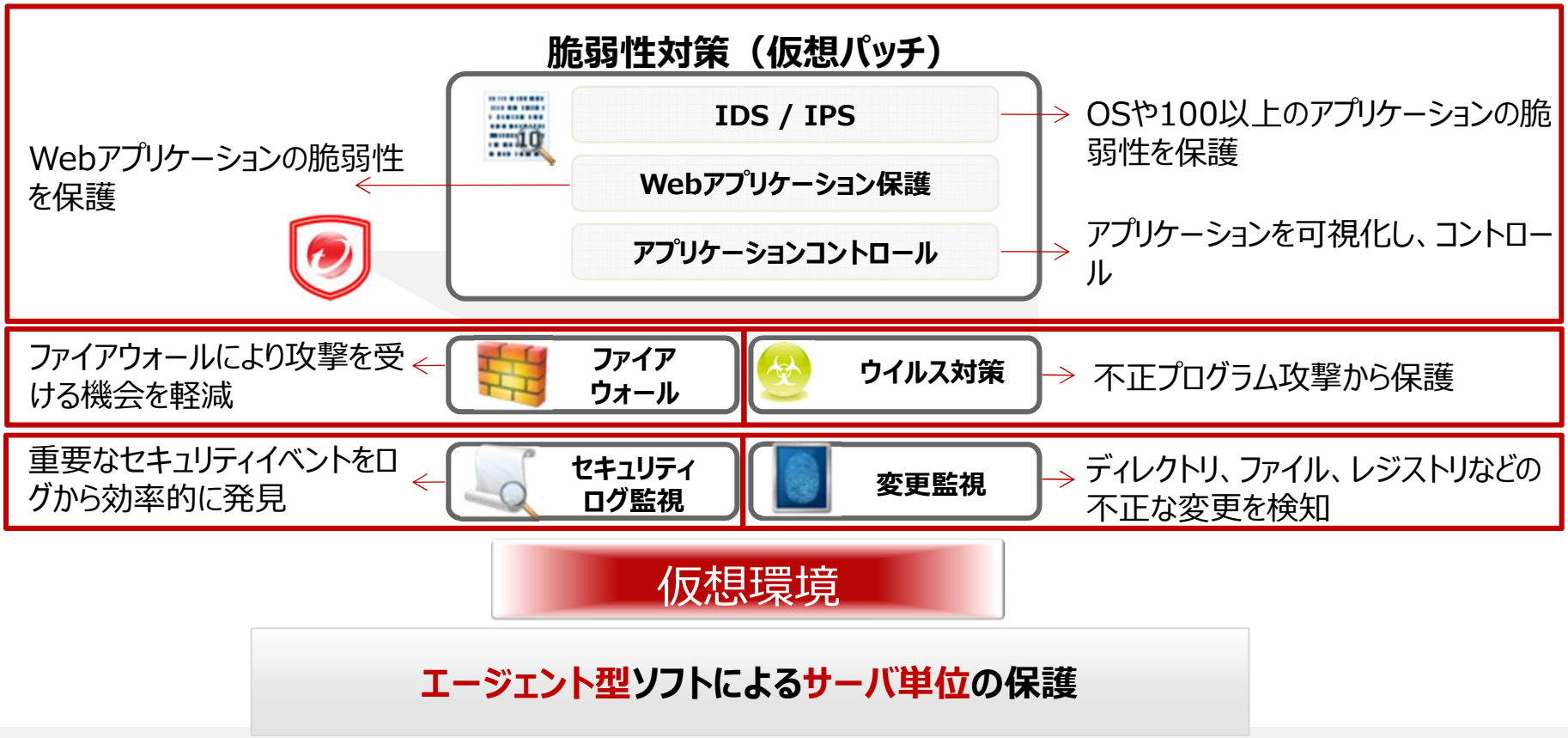
他サービス・製品を使う

AWSで対応していない部分に関しては、オンプレと同様にサービス、製品の導入を検討します。

製品：　各要件で求められている「機能」を提供している製品

サービス：　PCI DSSに関するコンサル、設計構築、運用サービス等

Trend Micro社　DeepSecurity　概要



AWS構成例

内容は講演にてご紹介します

構成のポイント

内容は講演にてご紹介します

まとめ

準拠済みのクラウドサービス利用

- 現時点では、日本での利用としてはAmazon AWSを推奨。
- PCI DSS取得範囲に入っているサービスを活用する。

準拠範囲の確認

- クラウドサービス側で用意しているドキュメントの確認が必要。
- わからない部分はクラウドベンダに確認。（思い込みは禁物）

明確なセキュリティ責任分担

- ベンダ側と自社側の責任分担範囲を明確にしておく。
- 審査での説明だけではなく、有事の際の対応でも有用。

もっと効率化を図るには？

PCI DSSの要件を紐解くと・・

機能

採用する製品等について
○○な機能を持っている事など。

設計・設定

●●な設定をすること、
▽▽な制限を行う事など。

運用

XXな運用をする事、
△△を維持する事など。

運用がタイヘン・・

PCI DSSでは運用に関する準拠事項が多い

- セキュリティソフトウェアを使った運用・設定の維持
  IPS・IDS/改ざん検知/Firewall/WAF/ログ監視/ウイルス対策
- アカウント管理
- アクセス記録、ログ集約管理
- 脆弱性検査、対策、管理
- ドキュメント作成・維持
- 担当者の教育とその記録

等々・・・

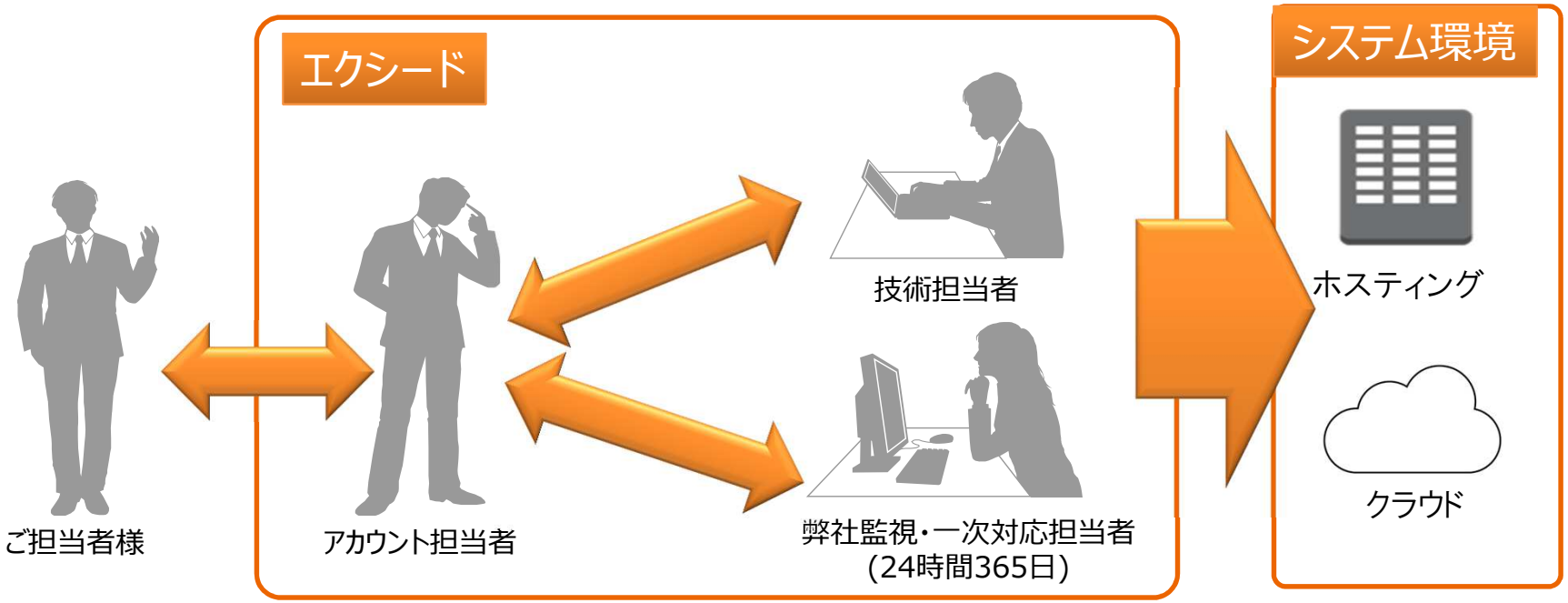
パブリッククラウドを活用するだけでは、
効率化できない運用作業は多数発生します。

エクシードが提供するPCI DSS準拠サービスの紹介

～PCI DSSシステムをより効率的に構築・運用するために～

PCI DSS準拠セキュアマネージドサービスのご紹介

弊社の運用チームにてお客様のPCI DSSシステム環境における運用をご提供するサービスとなります。
PCI DSS順守に必要な基本サービスに加え、監視、運用管理系のオプションサービスを提供しています。



得意分野へ集中

PCI DSS準拠セキュアマネージドサービスを利用することにより、インフラ運用部分の要件を当社にお任せいただき、**該当分野におけるお客様の対応を減らすことが可能**です。

PCI DSSの取得要件

アプリケーション要件

インフラ・システム運用要件

お客様はアプリケーション要件に注力いただけます。

インフラ・システム運用部分をワンストップでサポートします。

ログ監査、脆弱性検査等のセキュリティ運用

TREND MICRO

Logstorage

ログ収集、アクセス制御、ウィルスチェック等のセキュリティ機能の提供

amazon web services

Microsoft Azure

or

ファシリティ・基盤部分の提供

Amazon Web Services、AWSおよびAmazon Web Servicesロゴは、Amazon.com, Inc.またはその関連会社の商標です。

対応すべき要件を減らす

○：全て弊社にて対応　△：一部お客様にて対応が必要　×：全てお客様にて対応

	PCI DSS要件	対応
1	カード会員データを保護するために、ファイアウォールをインストールして維持する	
2	システムパスワードおよびその他のセキュリティパラメータにベンダ提供のデフォルト値を使用しないカード会員データの保護	
3	保存されるカード会員データを保護する	
4	オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する脆弱性管理プログラムの維持	
5	すべてのシステムをマルウェアから保護し、ウィルス対策ソフトウェアまたはプログラムを定期的に更新する	
6	安全性の高いシステムとアプリケーションを開発し、保守する強力なアクセス制御手法の導入	

対応すべき要件を減らす

○：全て弊社にて対応　△：一部お客様にて対応が必要　×：全てお客様にて対応

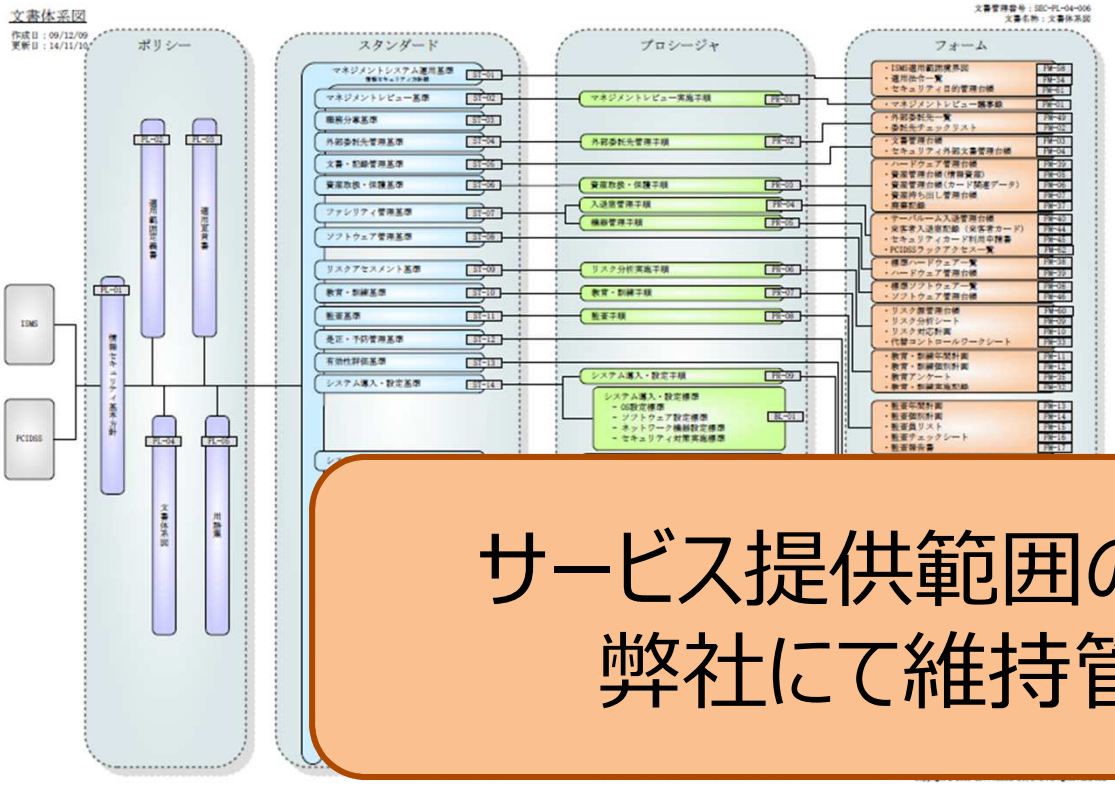
	PCI DSS要件	対応
7	カード会員データへのアクセスを、業務上必要な範囲内に制限する	
8	システムコンポーネントへのアクセスを識別・認証する	
9	カード会員データへの物理アクセスを制限するネットワークの定期的な監視およびテスト	
10	ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する	
11	セキュリティシステムおよびプロセスを定期的にテストする情報セキュリティポリシーの維持	
12	すべての担当者の情報セキュリティに対応するポリシーを維持する	

12要件に対する準拠率

71%

弊社AoC,RoC記載内容に準じて算出

ドキュメント整備・管理の省略化



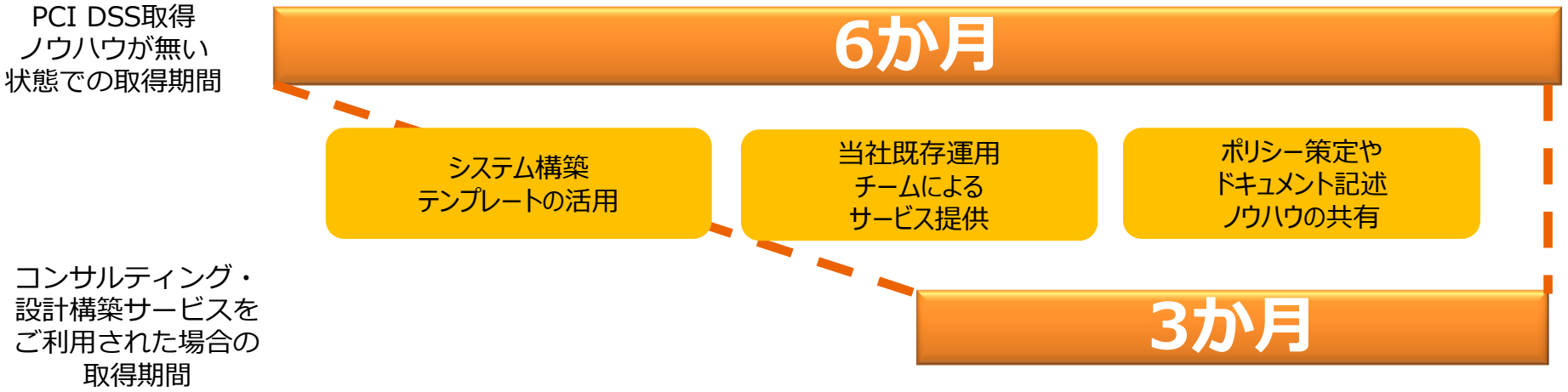
サービス提供範囲のドキュメントは
弊社にて維持管理を実施

エクシードが提供するPCI DSS準拠サービスの全容

インフラとシステム運用においてワンストップでサービス提供を行います。

導入効果　導入期間の短縮

弊社コンサルティング、設計・構築サービスにより、PCI DSSの導入期間短縮が可能。



導入期間を50%に短縮可能

※上記期間は弊社の実績から算出したものであり、お客様のシステムによって実際の期間は異なります。

設計品質の担保：審査資格保持者のサポート

弊社のPCI DSSシステム基盤構築では、PCI DSS審査資格保持者により適宜レビューを実施します。その結果、PCI DSS準拠のシステム設計構築品質を保ちつつ、迅速に設計・構築を進めることが可能となっております。

システム基盤設計構築時の審査資格保持者の作業内容

基本設計時点での仕様検討フォロー

設計が固まった段階での
PCI DSS適用のレビュー

運用品質の担保

2010年よりISMS、PCI DSSのデュアル運用を実施。5年間の運用実績があります。

対応規格	バージョン	適用時期
ISMS	JIS Q 27001:2006 （ISO/IEC27001:2006）	2010～2014
	JIS Q 27001:2014 （ISO/IEC27001:2013）	2014～
PCI DSS	Ver 1.2	2010～2011
	Ver 2.0	2011～2012
	Ver 2.1	2012～2014
	Ver 3.0	2015～
	Ver 3.1	2015/9対応予定

まとめ

準拠済みのクラウドサービス利用	• PCI DSSに準拠しているパブリッククラウドを利用可能です。 • 弊社にはクラウドシステム構築のノウハウがあります。
信頼できる運用サービス	• 弊社の運用サービスはPCI DSS　Ver3.0準拠済みです。 • PCI DSSシステムのインフラ部分の運用は全てお任せください。
明確なセキュリティ責任分担	• システム設計、運用設計を経て、お客様とのセキュリティ責任分担を漏れなく明確にします。その結果を基に運用サービスを提供します。
的確な準拠対応コンサルティング	• 弊社のコンサルティングサービスにて認定取得のためのご支援をします。 • PCI DSS審査の経験者がお客様の対応について助言します。

私達がサービスをお届けします！

内容は講演にてご紹介します

LET ENGINEERS FREE!

www.xseed.co.jp

Xseed Co., Ltd. | Takanawa Park Tower 7F, 3-20-14, Higashi Gotanda, Shinagawa-ku, Tokyo 141-0022
Tel. +81(0)3-6422-0021 | Fax. +81(0)3-6422-0022 | E-mail info@xseed.co.jp | www.xseed.co.jp