PCIDSSセキュリティフォーラム 2014
セッション02

2014年7月29日(火) 11:10～11:55

東京国際フォーラムガラス棟6F会議室「G602」

「PCIDSSv3.0新規要件
委託先管理強化への対応」
～RSA Archer eGRC Platformのご紹介～

テクマトリックス株式会社

セキュリティソリューション技術部　榎本有子

TechMatrix
テクマトリックス株式会社

セッション内容

- カード決済環境の複雑化に伴い、カード会員データに関わる業務を委託する場合の情報管理方法が深堀りされました。
  委託先契約書、業務内容、手順の保持の他、定期的な確認を行うことができるサポートツール「 RSA Archer eGRC Platform 」をご紹介いたします。

アジェンダ

Ⅰ．PCI DSS バージョン2.0 から3.0への変更点

Ⅱ．委託先管理で要求されている事項

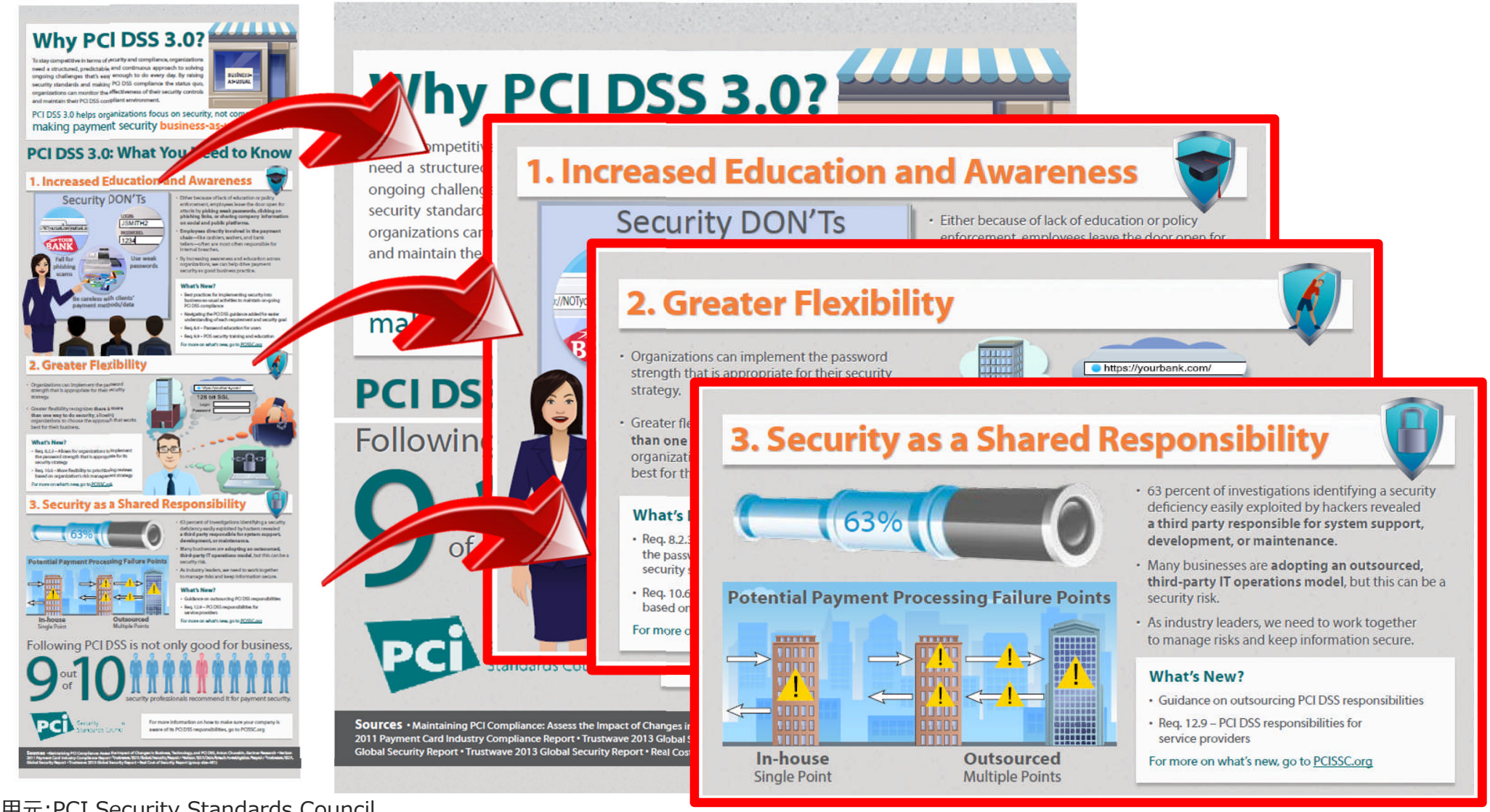
Ⅲ．要求事項への対応方法（現状）

Ⅳ．理想的な委託先管理を実現するためのRSA Archer eGRC Platform

Ⅴ．RSA Archer eGRC Platformについて

Ⅰ．PCI DSS バージョン2.0 から3.0への変更点

Ⅰ．PCI DSS バージョン2.0 から3.0への変更点
1）改定概要：概念



引用元:PCI Security Standards Council
PCI COUNCIL PUBLISHES PCI DSS AND PA-DSS VERSION 3.0
Why PCI DSS 3.0?
https://www.pcisecuritystandards.org/pdfs/PCIDSS.pdf

Ⅰ．PCI DSS バージョン2.0 から3.0への変更点
1）改定概要：概念

1. 教育と意識の向上
   - Increased Education and Awareness
2. 更なる柔軟性
   - Greater Flexibility
3. セキュリティ責任の共有
   - Security as a Shared Responsibility

カード会員データを取り扱う環境の
新しい脅威や技術にも対応していく

引用元:PCI Security Standards Council
PCI COUNCIL PUBLISHES PCI DSS AND PA-DSS VERSION 3.0
Why PCI DSS 3.0?
https://www.pcisecuritystandards.org/pdfs/PCIDSS.pdf

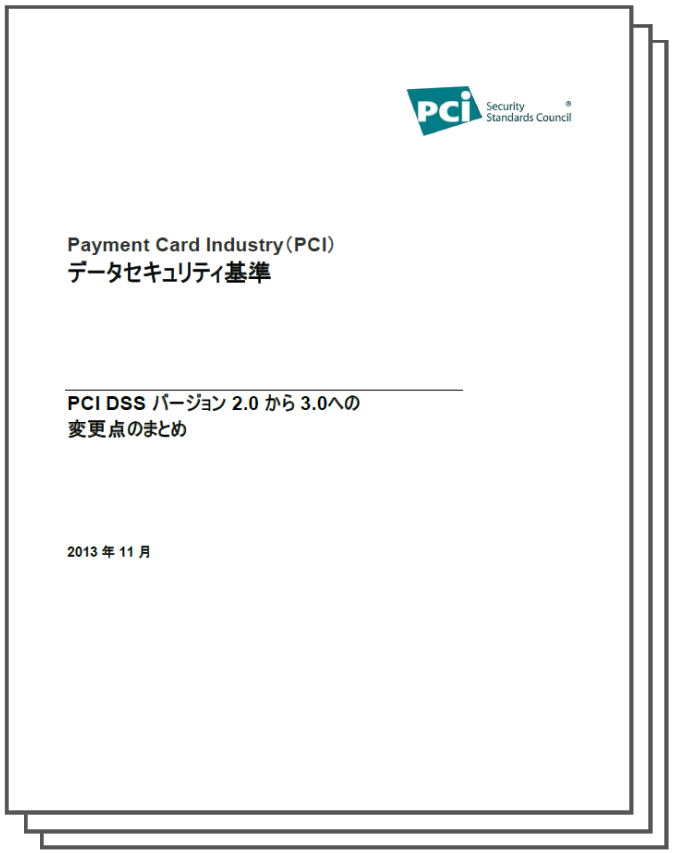
Ⅰ．PCI DSS バージョン2.0 から3.0への変更点
1）改定概要：基準ドキュメントの変更内容

- ドキュメント構成の変更
  要件へのガイドラインの追記
  - 要件
  - テスト手順
  - ガイドライン
- 要件項目数の精査
  - v2.0：280項目　⇒　v3.0：399項目

ガイドライン追記による
テスト手順の具体化、充実化

引用元:PCI Security Standards Council
PCI DSS v3.0
PCI DSS v2.0
https://ja.pcisecuritystandards.org/minisite/en/

Ⅰ．PCI DSS バージョン2.0 から3.0への変更点
2）要件12：情報セキュリティポリシーの維持



要件 12		変更点	種類
PCI DSS v2.0	PCI DSS v3.0		
12.1.1 12.2	1.5、2.5、3.7、 4.3、5.4、6.7、 7.3、8.8、9.10 、10.8、11.6	12.1.1（すべての PCI DSS 要件を解決するための情報セキュリティポリシー向け）および 12.2（運用セキュリティ手順向け）における以前の要件を統合し、それぞれを ひとつの要件として、これらを要件 1 から 11 に移動。	明確化
12.1.3	12.1.1	以前の要件 12.1.3 を 12.1.1 に移動。	明確化
12.1.2	12.2	1 個の年間リスク評価プロセス向けに以前の要件 12.1.2 を 12.2 に移動し、対象のリスク評価は少なくとも毎年*および対象の環境に対して顕著な変更点の後*で実施されなければならないことを明確化。	発展型要件
12.3.4	12.3.4	「ラベル付け」が使用されるべき 例であることを明確化。	明確化
12.3.8	12.3.8	ポリシーが特定のアイドル状態後にリモートアクセスセッションを切断するために実装されていることを検証するための新しいテスト手順。	明確化
12.3.10	12.3.10	リモートアクセス技術を経由してカード会員データにアクセスする担当者向けに承認済み事業が存在する状況において、対象のデータがすべての適用可能な PCI DSS 要件に準拠して保護される必要があることを明確化するために要件およびテスト手順間の文を整合。	明確化
12.8	12.8	カード会員データを共有している、またはカード会員データのセキュリティに影響を与える可能性がある、サービスプロバイダを管理するためのポリシーおよび手順を実装し維持する目的を明確化。	明確化
12.8.2	12.8.2	対象のサービスプロバイダの書面による契約/承諾に関する適用可能な責任を明確化。	明確化
	12.8.5	どの PCI DSS 要件がそれぞれのサービスプロバイダにより管理され、どの要件が対象の事業体により管理されるかについての情報を維持するための新しい要件。	発展型要件
	12.9	要件 12.8 において指定される、それぞれの顧客に対して書面による契約/承諾を提供するためのサービスプロバイダ向けの新しい要件。*2015 年 7 月 1 日まで有効*	発展型要件
12.9.x	12.10.x	セキュリティ監視システムからの警告がインシデント応答プラン内に含まれるべきであることを明確化するために。要件 12.10.5 の番号を変更し、内容を更新。	明確化

引用元:PCI Security Standards Council
Payment Card Industry（PCI）データセキュリティ基準
PCI DSS バージョン 2.0 からバージョン 3.0 への変更点のまとめ 2013年11月
https://ja.pcisecuritystandards.org/_onelink_/pcisecurity/en2ja/minisite/en/docs/PCI_DSS_v3_Summary_of_Changes.pdf

Ⅰ．PCI DSS バージョン2.0 から3.0への変更点
2）要件12：情報セキュリティポリシーの維持

要件番号	v2.0		v3.0	
	要件	テスト手順	要件	テスト手順
12.8	カード会員データをサービスプロバイダと共有する場合は、サービスプロバイダを管理するためのポリシーと手順を維持および実施して、以下を含める。	事業体がカード会員データをサービスプロバイダ（バックアップテープ保管施設、Web ホスティング企業やセキュリティサービスプロバイダなどの管理対象サービスプロバイダ、または不正モデリング目的でデータを受信するサービスプロバイダなど）と共有する場合は、観察、ポリシーと手順のレビュー、および関連文書のレビューを通じて、以下を実行する。	カード会員データがサービスプロバイダと共有される場合は、次の項目を含め、サービスプロバイダを管理するポリシーと手順を維持および実装する。	ポリシーと手順の観察とレビュー、関連文書のレビューを通して、カード会員データを共有するか、カード会員データのセキュリティに影響を及ぼす可能性のあるサービスプロバイダ（たとえば、バックアップテープ保管施設、Web ホスティング企業やセキュリティサービスプロバイダなどの管理対象サービスプロバイダ、または不正モデリング目的でデータを受信するサービスプロバイダなど）を次のように管理するプロセスが実装されていることを確認する。

引用元:PCI Security Standards Council
PCI DSS v3.0
PCI DSS v2.0
https://ja.pcisecuritystandards.org/minisite/en/

Ⅰ．PCI DSS バージョン2.0 から3.0への変更点
2）要件12：情報セキュリティポリシーの維持

要件番号	v2.0		v3.0	
	要件	テスト手順	要件	テスト手順
12.8.2	サービスプロバイダが自社の所有するカード会員データのセキュリティに対して責任を負うことに同意した、書面での契約を維持する。	書面による契約に、カード会員データのセキュリティに対して責任を負うことへのサービスプロバイダの同意が含まれていることを確認する。	サービスプロバイダは、プロバイダが、顧客に代わって所有、保存、処理、送信するカード会員データのセキュリティについて、または顧客のカード会員データのセキュリティに影響を与える範囲について責任を持つことを認める内容の書面による契約書を維持する。	書面による契約を調べて、サービスプロバイダが、顧客に代わって所有、保存、処理、送信するカード会員データのセキュリティについて、または顧客のカード会員データのセキュリティに影響を与える範囲について責任を持つことを認める内容の書面による契約書を維持していることを確認する。

引用元:PCI Security Standards Council
PCI DSS v3.0
PCI DSS v2.0
https://ja.pcisecuritystandards.org/minisite/en/

Ⅰ．PCI DSS バージョン2.0 から3.0への変更点
2）要件12：情報セキュリティポリシーの維持

要件番号	v2.0		v3.0	
	要件	テスト手順	要件	テスト手順
12.8.5	—	—	各サービスプロバイダに対し、どのPCI DSS 要件がサービスプロバイダによって管理され、どのPCI DSS が事業体によって管理されるかについての情報を維持する。	各サービスプロバイダに対し、どのPCI DSS 要件がサービスプロバイダによって管理され、どのPCI DSS が事業体によって管理されるかについての情報を事業体が維持していることを確認する。
12.9	インシデント対応計画の実施	—	12.10に移動	—

引用元:PCI Security Standards Council
PCI DSS v3.0
PCI DSS v2.0
https://ja.pcisecuritystandards.org/minisite/en/

Ⅰ．PCI DSS バージョン2.0 から3.0への変更点
2）要件12：情報セキュリティポリシーの維持

要件番号	v2.0		v3.0	
	要件	テスト手順	要件	テスト手順
12.9	—	—	サービスプロバイダ用の追加要件:顧客に代わって所有、保存、処理、送信するカード会員データのセキュリティについて、または顧客のカード会員データのセキュリティに影響を与える範囲について責任を持つことを認める内容の書面による契約書を維持する。	サービスプロバイダのポリシーと手順をレビューし、書面による契約のテンプレートを読んで、サービスプロバイダが、顧客のカード会員データや機密の認証データを取り扱う、アクセスする、または他の方法で保存、処理、送信するか、顧客のカード会員データ環境を顧客に委託されて管理するという業務範囲において該当するすべてのPCI DSS 要件を順守するという同意を書面にて顧客に提示したことを確認する。

引用元:PCI Security Standards Council
PCI DSS v3.0
PCI DSS v2.0
https://ja.pcisecuritystandards.org/minisite/en/

Ⅱ．委託先管理で要求されている事項

Ⅱ．委託先管理で要求されている事項

「カード会員データを共有している、またはカード会員データの
セキュリティに影響を与える可能性があるサービスプロバイダー」

「委託先」

- カード会員データを取り扱う業務やシステムを外部に委託している場合の委託先を全て洗出しリスト化する。
- カード会員データの取り扱いや、PCI DSS準拠に関する責任分岐点を明確にし、書面上で契約を締結する。
  （取り扱う情報の種類や、委託する業務の内容によって異なる。）
- 委託先のPCI DSS準拠ステータスを最低年１回確認する。

カード会員データ委託元としての委託先管理責任

Ⅲ．要求事項への対応方法（現状）

Ⅲ．要求事項への対応方法（現状）

■　委託先管理に必要な情報

- 委託先情報
  - 企業情報
  - 階層　委託先⇒再委託先⇒再々委託先…（責任分岐の明確化）
  - カード会員データ取扱い範囲、業務内容、影響先
- 契約書情報
  - 締結有無
  - 法規制変更に伴う見直し実施有無
- PCI DSS準拠ステータス、確認結果
  - 確認表
  - 現場確認、証跡

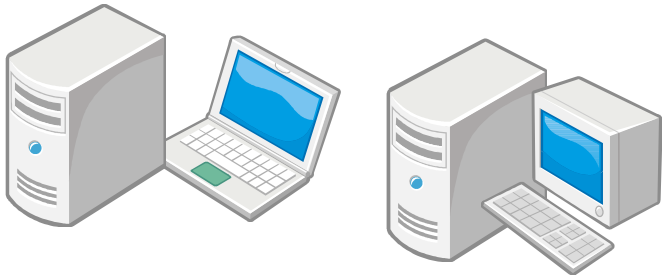
■　委託先にPCI DSS準拠状況**を確認する**ための手段

- チェックシートの配付
- 現場確認

Ⅲ．要求事項への対応方法（現状）

■　手間となっている事項

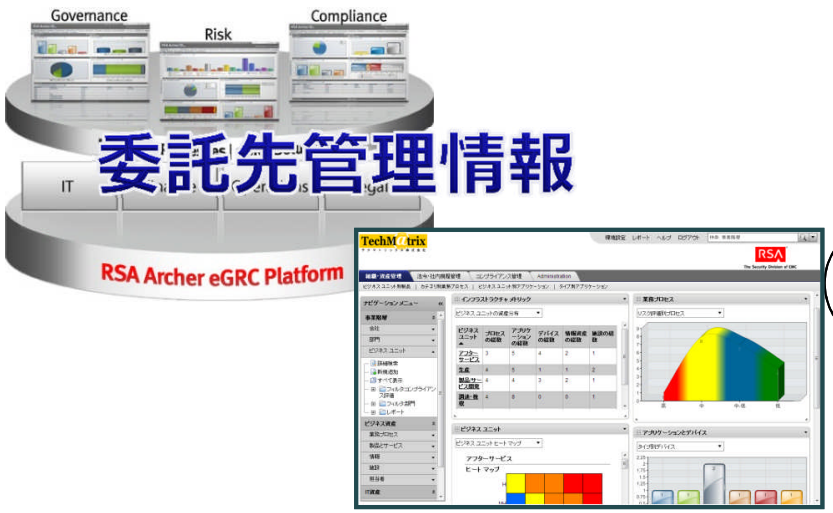
- 委託先内容取り纏め、情報更新
  - 重複した情報を管理している
  - 最新情報が連携されていない
- 委託先へのPCI DSS準拠状況 質問
  - 一斉配信
  - 質問受付
  - 期日管理
- 準拠状況確認結果の集計、報告書作成作業
  - 条件に応じたデータ集計
    - 要件番号毎
    - 委託先グループ毎
    - 取り扱っているカード会員データ毎
    - 業種毎　など



Ⅳ. 理想的な委託先管理を実現するための RSA Archer eGRC Platform

Ⅳ. 理想的な委託先管理を実現するための RSA Archer eGRC Platform

- 「RSA Archer eGRC Platform（Archer）」は、
  『マネジメントシステム』を効率的に運用**するためのソフトウエアツール**です。
- 委託先に関する様々な情報を一元的に管理し、様々な情報に活用することができます。



- 企業情報
  - 階層　委託先⇒再委託先⇒再々委託先
  - カード会員データ取扱い範囲、業務内容、影響先
- 契約書情報
  - 締結有無
  - 法規制変更に伴う見直し実施有無
- PCI DSS準拠ステータス、確認結果
  - 確認表
  - 現場確認、証跡
- PCI DSS準拠事項

Ⅳ. 理想的な委託先管理を実現するための RSA Archer eGRC Platform

管理名	数	データベース名	登録内容
ベンダー管理	1	ベンダー プロファイル	各ベンダーに関する情報を管理します。ベンダー名、役割、担当者、契約内容、アセスメント結果、事業影響度分析など様々な情報がリンクされます。
	2	担当者	連絡先および担当者情報のセントラル リポジトリとして機能し、デバイス管理者や業務プロセス管理責任者などの組織内の主要なタスクに関与する担当者の情報を文書化するものです。
	3	契約	ベンダーと顧客に関連づけられた契約リストを管理します。
	4	契約事項	ベンダーと、社内の個々のビジネス ユニットの間の契約事項のリストを管理します。
	5	施設	組織のすべての施設のリストを管理します。
	6	ベンダー財務 アセスメント	「ベンダープロファイル」に登録されたベンダーに対して財務状況のアセスメント、アセスメント結果の取り纏めを行います。
	7	第1階層 アセスメント	「ベンダープロファイル」に登録されたベンダーに対して「委託先」向けのアセスメント、アセスメント結果の取り纏めを行います。
	8	第2階層 アセスメント	「ベンダープロファイル」に登録されたベンダーに対して「再委託先」向けのアセスメント、アセスメント結果の取り纏めを行います。
	9	質問ライブラリ	アセスメント作成時の参考となる質問集

- 委託先の階層は、初期値は2階層ですが、レベルに応じた階層にカスタマイズを行います。
- 「PCI DSSアセスメント」データベースや、「個人情報保護ガイドラインアセスメント」データベースなどを作成し管理します。

Ⅳ. 理想的な委託先管理を実現するための RSA Archer eGRC Platform

V．RSA Archer eGRC Platformについて

Ⅴ. RSA Archer eGRC Platformについて

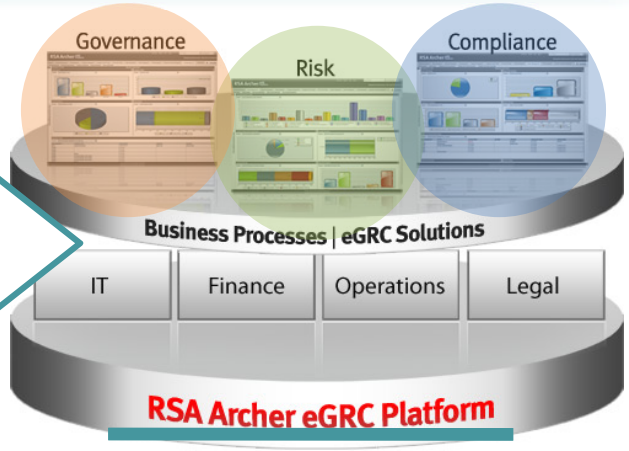
- 「RSA Archer eGRC Platform（Archer）」は、
『マネジメントシステム』を効率的に運用するためのソフトウエアツールです。
- 企業では、「法令、規程、契約、手順などの要求事項の管理」を初めとし、
「コンプライアンス管理」や「リスク管理」「内部監査管理」「教育管理」
「(個人)情報管理」「委託先管理」など様々な『マネジメントシステム』が
運用されています。
社内活動の他にも、
「ISO9001：品質/14001：環境/27001：ISMS/JISQ15001：Pマーク」など
のISO規格や「PCIDSS、FISC」などの業界標準の『マネジメントシステム』を
運用している場合があります。
これら『マネジメントシステム』の運用では、同一の情報が複数の部門で管理
されていたり、同じ対象や事象について、マネジメントシステム毎に、リスクアセ
スメント、手順の見直し、内部監査やマネジメントレビューを行うなど、重複運
用されていることが多いです。
- 「Archer」 は、「情報の一元化・共有管理」を行うことで
『様々な情報を、役割・責任に応じて見たい形に整理し、業務の効率化を実現』して
いきます。

V. RSA Archer eGRC Platformについて

マネジメントシステムに関係する様々な情報

要求事項
　法令、規程、契約、手順
リスクアセスメント情報
　アセスメント対象資産/事象
リスク情報
　リスク結果、リスク対応計画、残留リスク
　事業への影響度、発生の可能性
監査情報
　監査結果、是正・予防要求
インシデント情報
　事件・事故内容、是正・予防要求、教育活動
有効性評価情報
　目標値、測定結果
財務情報
　予算、実績、格付
関係先情報
　社内（責任者、関係者）、外部委託先
ISO規格/業界標準
　ISO9001　：品質
　ISO14001　：環境
　ISO27001　：情報セキュリティ
　JISQ15001：個人情報保護
　ISO22301　：事業継続
　ISO20000　：ITサービス
　PCIDSS
　FISCガイドライン　・・・

「RSA Archer eGRC 」による情報の一元化・共有管理



ニーズに沿った可視化業務効率化の実現

役割、責任に応じたダッシュボードの利用

V. RSA Archer eGRC Platformについて

- 「管理ソリューション」と「基本機能」の組み合わせと設定により、マネジメントシステムのご要望に応じた内容に作り上げていきます。

10個の管理ソリューション		
1	Policy Management	ポリシー管理
2	Enterprise Management	エンタープライズ管理
3	Risk Management	リスク管理
4	Compliance Management	コンプライアンス管理
5	Incident Management	インシデント管理
6	Vendor Management	委託先管理
7	Threat Management	脅威管理
8	Business Continuity Management	事業継続管理
9	Audit Management	監査管理
10	Security Operation Management (SecOps)	SOC運用管理
※	Issue Management	問題管理
	Task Management	タスク管理

8個の基本機能 (プラットフォーム)		
①	Application Builder	アプリケーションビルダー
②	Reports & Dashboard	レポート&ダッシュボード
③	Access Control	アクセスコントロール
④	Workflow	ワークフロー
⑤	Notifications	通知、レポート管理
⑥	Integration	情報統合
⑦	User Experience	教育・訓練、意識向上
⑧	Globalization	複数言語対応

※Issue, Task Managementは、共通Solutionです。

V. RSA Archer eGRC Platformについて

■ 10個の管理ソリューション

- 管理ソリューションには、ソリューション運用に見合った標準アプリケーション（データベース群）が設定されています。

1. ポリシー管理
   - 規程類を集中的に管理します。法令やガイドラインと、社内規程、契約、手順について、該当項目番号へのマッピングを行い、企業内におけるポリシー管理をサポートします。
2. エンタープライズ管理
   - 企業情報（部門、事業部、関係会社）と資産・インフラ情報を一元管理します。業務プロセスが適切に運用されていることを管理します。
3. リスク管理
   - 風評、財務、業務、セキュリティなど全てのリスクについて、アセスメント、リスク対応計画の作成、進捗や有効性評価などの一連の流れについて管理することが出来ます。
4. コンプライアンス管理
   - コントロールフレームワーク、管理手順やテスト計画を管理します。また、欠陥の識別、改善計画の管理を行います。
5. インシデント管理
   - サイバー攻撃や物理的な事故の記録を取得し、エスカレーション方法の確立、インシデントの分析や改善事項を管理します。

V. RSA Archer eGRC Platformについて

■ 10個の管理ソリューション

6. 委託先管理
   - 委託先企業のデータを集中的に管理し、委託先企業のリスク評価や規程類、法令、ガイドラインへの準拠性と、関係性を明確にします。
7. 脅威管理
   - 既存の脅威情報の分析、管理を行い、企業に対する攻撃や不安要素を早期に検知します。
8. 事業継続管理
   - 非常事態発生時に、必要な事業継続や災害復旧計画を指示し、迅速な対応のサポートを行います。
9. 監査管理
   - 監査計画、優先度判断、人員、手順、および、報告書作成の管理を一元的に行い、監査工程の効率性を高めます。
10. SOC運用管理
   - セキュリティ監視機器からSOCに送られるアラートの集中管理とインシデント対応のワークフローの自動化により、インシデント処理に必要な情報の共有、担当者間のプロセス フローの管理、インシデント対応状況のモニタリングや稼働管理などを行い、SOC運用を可視化します。

※問題管理　：それぞれのマネジメントソリューションで発生している問題事項、例外事項改善計画を管理します。
タスク管理：Todo 事項を管理します。

V. RSA Archer eGRC Platformについて

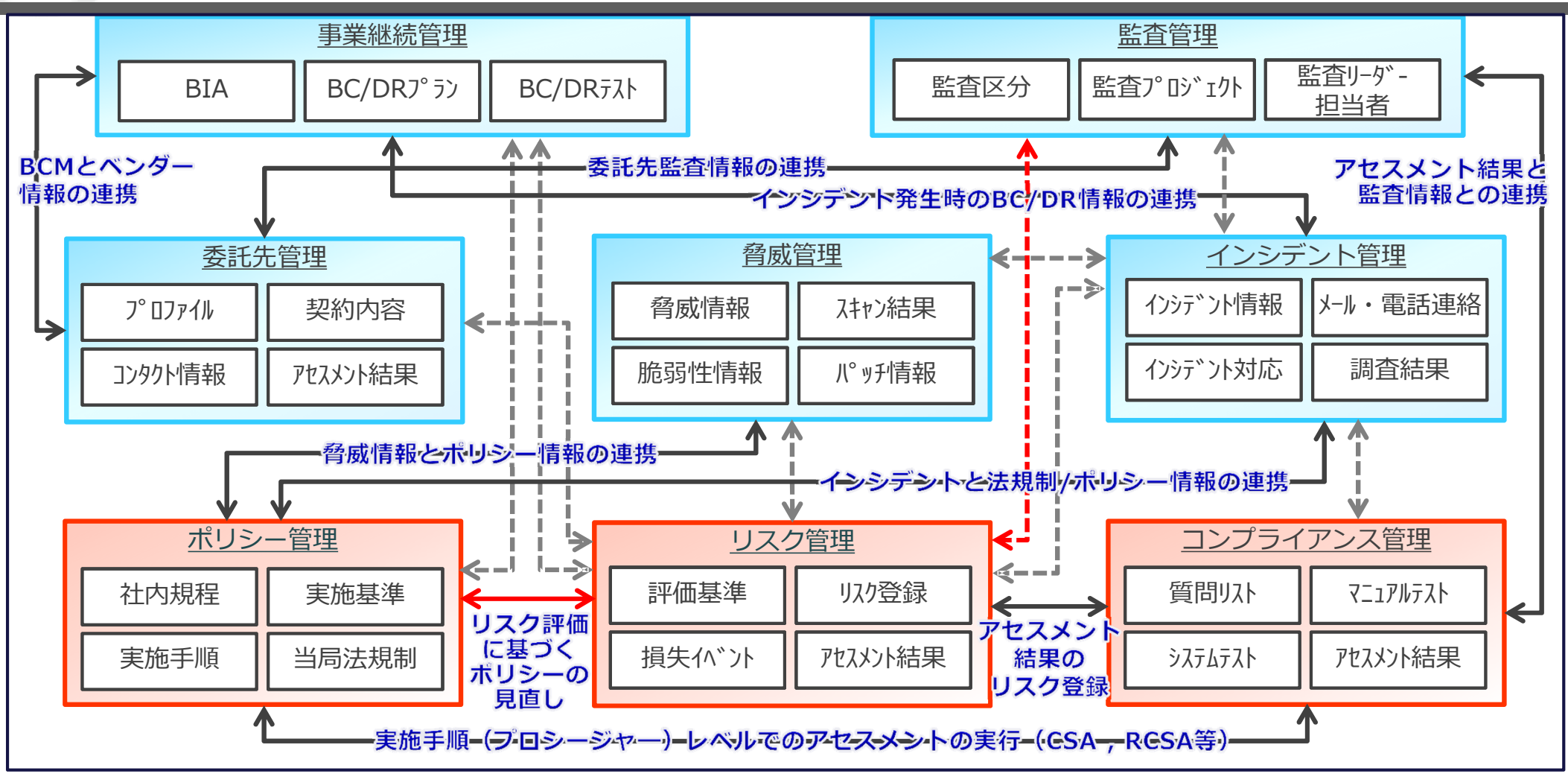
■ 基本機能

- RSA Archer各モジュールには、それぞれ自由に基本設定を行うことが可能です。自社の組織体系や管理フローに見合ったArcherを構築することが出来ます。
- 主な機能
  - アクセス制御（設定単位例：グループ / モジュール / レコード / レコード内にある入力フィールドなど）
  - 画面設定（ワークシート / ダッシュボード / レポート、コーポレートカラーの利用　など）
  - フィールド作成（テキスト / 数値（計算式含む） / 値リスト / 相互参照 / ユーザリスト　など）
  - アセスメント（質問ライブラリ / 自己質問の登録）
  - 連携（csvファイルからのデーター括登録 / Active Directory連携 / Web Services API　など）
  - 教育訓練（掲示板 / クイズ　など）

■ システム要件

- サーバ　：　Windows Server（2008 R2、2012）
  - Web Tier　　：Microsoft Internet Information Server (IIS)
  - Services Tier　：.NET Framework.
  - Database Tier：Microsoft SQL Server（2008 R2、2012）
- クライアント　：　Internet Explorer , Firefox , Chrome
  - プラグイン　　：Microsoft Silverlight

V. RSA Archer eGRC Platformについて



ご清聴ありがとうございました。

RSA Archerを利用して、
情報の効果的な活用、運用の効率化を実感してください。

<デモご要望、問い合わせ先>
テクマトリックス株式会社
セキュリティソリューション技術部　RSA Archer担当　榎本
archer-info@techmatrix.co.jp