金融リスクマネジメント&サイバーセキュリティーフォーラム2019
講演資料

企業のリスクをクラウドで一元管理
～国内開発のGRCサービスのご紹介

2019/10/16
株式会社GRCS
CSO 徳永　拓

株式会社GRCS 会社概要

会社名	株式会社GRCS（旧NANAROQ／2018年3月1日商号変更）
設立	2005年3月
決算期	11月
資本金	132百万円
役員構成	代表取締役社長　佐々木慈和（ササキヨシカズ） 取締役 兼 CTO　塚本拓也 取締役 兼 CCO　田中郁恵 社外取締役　久保惠一
所在地	東京都千代田区五番町1-9　MG市ヶ谷ビルディング9F
従業員数	約80名
許可番号	労働者派遣事業（派13-311240） 有料職業紹介事業（13−ユ−301890）
所属団体	一般社団法人日本CISO協会（理事） 日本カード情報セキュリティー協議会（運営委員）
資格	PCI DSS認証審査機関

GRCS

www.grcs.co.jp

株式会社GRCSのサービス紹介

企業経営における リスク管理ソリューション GRC	ENTERPRISE RISK MT	ISO31000に準拠したERMを支援するクラウドサービス
	SUPPLIER RISK MT	外部委託先リスクマネジメントクラウドサービス
	RSA Archer GRC Platform	GRCの統合管理を実現するプラットフォーム
	OneTrust	クラウド型GDPR・プライバシー管理ツール
	Snow	ライセンス管理を最適化するソフトウェア
サイバーセキュリティ リスク管理ソリューション CSIRT・教育	CSIRT MT	CSIRTに必要な機能を実装したクラウドサービス
	CSIRT MT.mSS	MSS事業者、社内SOC向けのマルチテナント型CSIRT MT
	脆弱性TODAY	脆弱性情報日次配信サービス
	ゲーム学習型教育クラウドサービス	ゲーム学習型教育クラウドサービス
インシデント検知・可視化 ソリューション 検知・フォレンジック	SIEM.AI MT	オープンソースとAIを活用したSIEM
	RSA NetWitness	ネットワークフォレンジック・インシデント検知
	DARKTRACE	AIを利用した機械学習によるインシデント検知
	IMPERVA INCAPSULA	WAF・DDoS対策・CDNを提供するクラウドサービス
次世代型エンドポイント 保護ソリューション EDR・DLP・CASB	Carbon Black.	エンドポイントを防御する次世代型AV＋EDR
	DIGITAL GUARDIAN	次世代データ・プロテクション・プラットフォーム
	Bromium	次世代仮想隔離型エンドポイントプロテクション
	netskope	全デバイスのクラウド利用を把握、保護、対処を実現

GRCSのご紹介

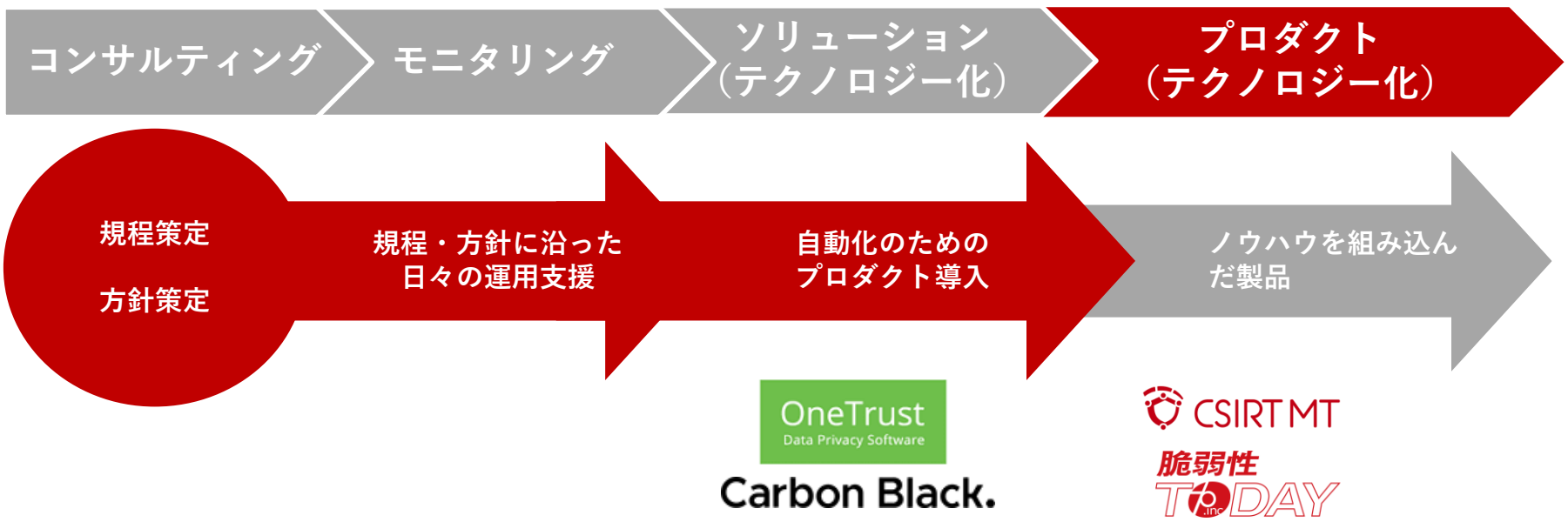
株式会社GRCSのビジョン

GRCS

テクノロジーデシンプルニ

企業が社会の変化に伴い対応しなければいけない、複雑なガバナンス、リスク、コンプライアンス、セキュリティをテクノロジーの力を活用してシンプルにする。

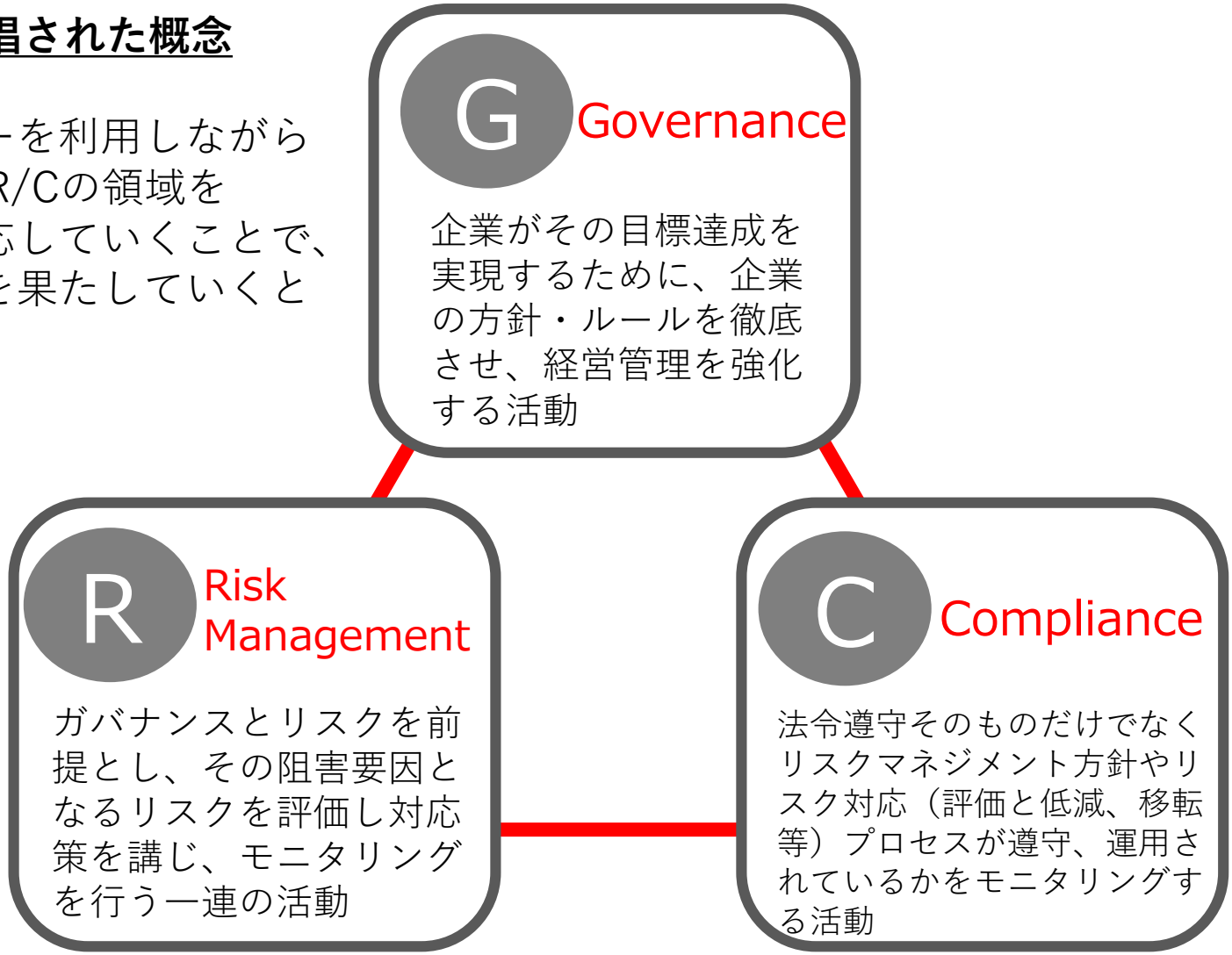
ソリューション事業 ⟷ プロダクト事業



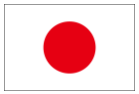
GRCとは

21世紀に入って提唱された概念

新しいテクノロジーを利用しながら
相互に関連するG/R/Cの領域を
統合・効率的に対応していくことで、
企業・組織の責任を果たしていくという考え方



日本におけるGRC

日本 		米国 
GRCの知名度は高まっているが、十分に浸透はしておらず、業種や会社規模によっても差が大きい	対応状況	GRCの概念は広く理解されており、多くの企業で経営の中の重要な要素として注目されている
GRCへの対応に関しては、該当業務を担当する部署に権限が与えられ、業務単位でボトムアップで実施されている例が多い	組織文化	CRO（リスク管理責任者）がアサインされ、トップダウンで垂直統合型でGRCの推進が行われている例が多い
業務の固有性が強いため、個々のGRC要件に適合した、小規模なソリューションが適合する例が多い	適合製品	大規模かつ網羅的なGRCソリューションを全社的に導入する方式が適合する例が多い

日本のGRCにおける課題

◎GRC推進への導入障壁

- ガバナンス形態（独立性）
- 業務固有のリスクとそれ以外
- 組織と階層の複雑さ
- 限られた予算

◎GRCソリューション導入のポイント

- 経営層の理解を得られるか
- カスタマイズ（費用、保守への波及）
- 現場への負荷

株式会社GRCSのビジョン（再）

品質偽装
風評被害
GDPR
異常気象
改ざん
詐欺
監督省庁

GRCS

テクノロジーデシンプルニ

企業が社会の変化に伴い対応しなければいけない、複雑なガバナンス、リスク、コンプライアンス、セキュリティをテクノロジーの力を活用してシンプルにする。

ハラスメント
隠ぺい
個人情報保護法
横領
情報漏洩
不正アクセス
気候変動
トランプ

GRCSが活用するテクノロジー

◎AI（機械学習）

◎自動化（RPA）

◎クラウド（SaaS）

新しいテクノロジーを活用します

GRCSが実現する「シンプル」

◎すぐに（即時性）

◎誰にでも（属人化しない）

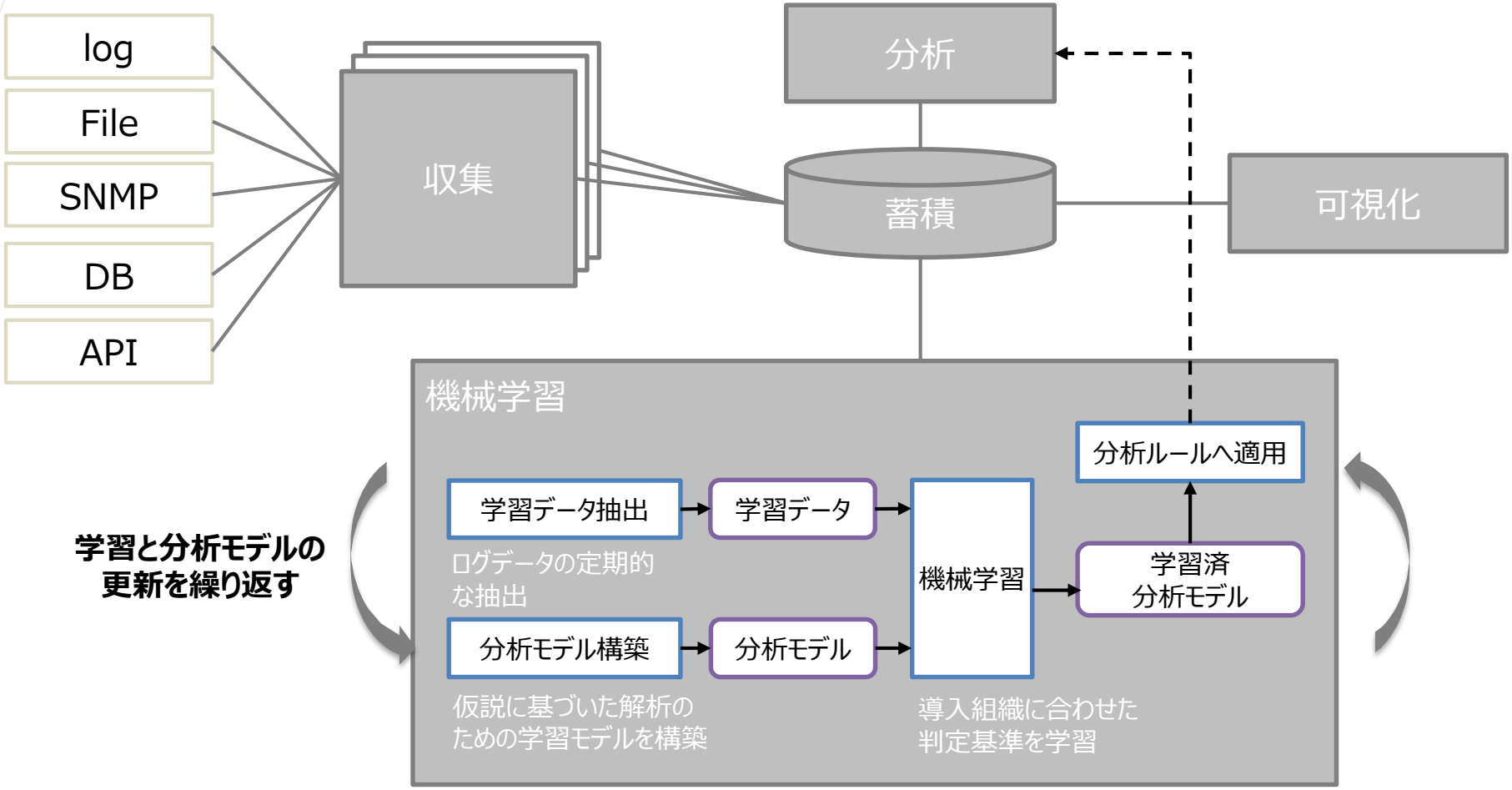
◎わかりやすい（一元化・ダッシュボード）

形骸化しない実効性のあるGRCを実現します

GRCSの取り組み例

GRCSの取り組み事例①

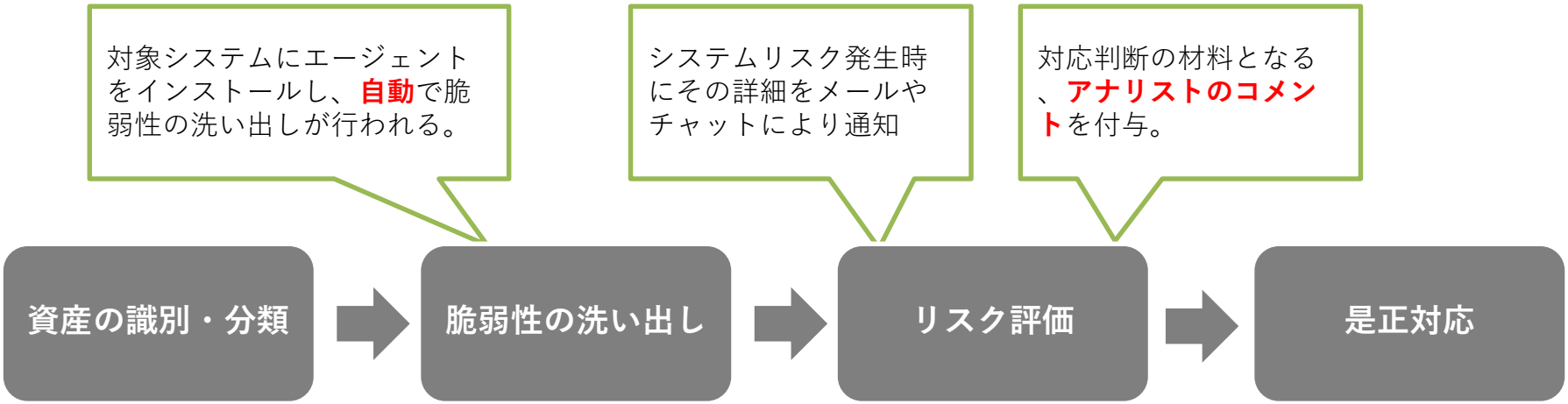
オープンソースを組み合わせたデータ分析ツールの開発



GRCSの取り組み事例②

近日発表予定

システムリスク（脆弱性）の検出とリスク評価の自動化



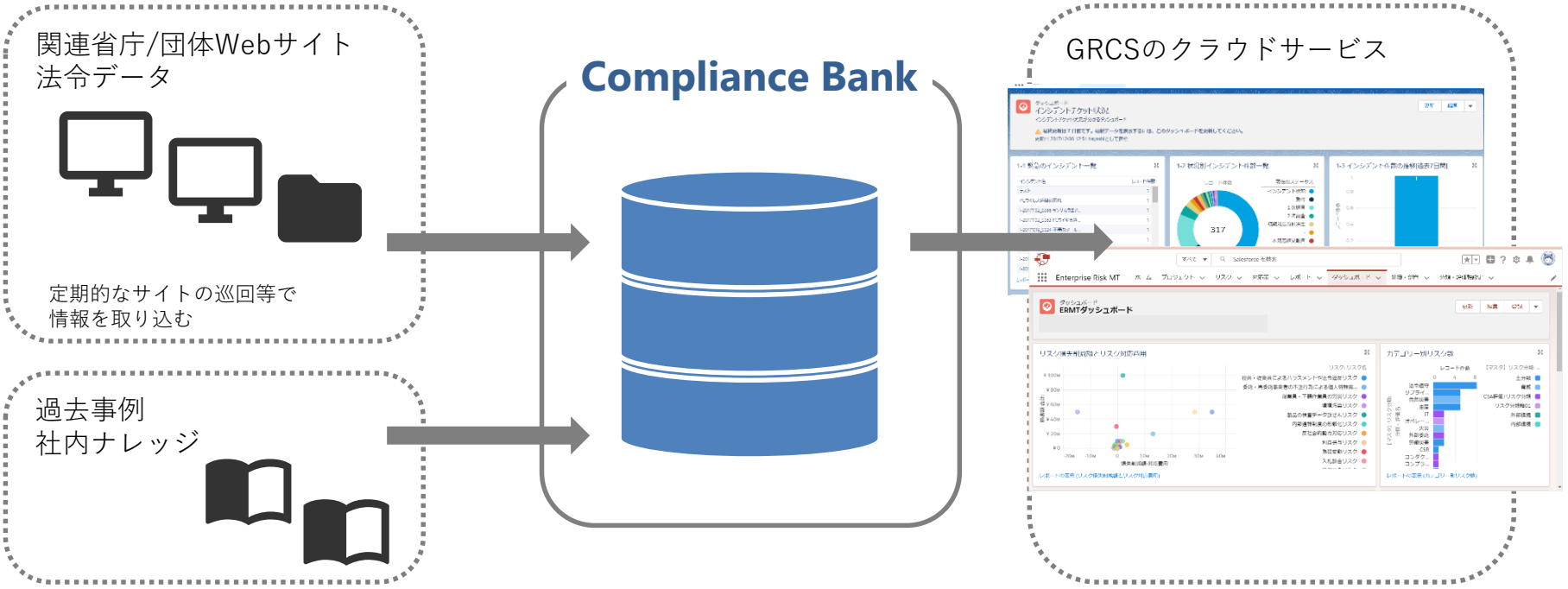
Point

CISO、事業部門など、役割に応じたダッシュボートを提供し、全体の把握や個別の残課題のリストアップが可能。

GRCSの取り組み事例③

開発中

リスク・コンプライアンス関連情報のデータベース化



関連省庁や団体のWebサイトに掲載された情報や、社内の過去事例やナレッジなどをまとめてデータベース化し可視化

自動的に取り込んだ情報を、適時適切に関係者へ配信

機械学習やサジェスト機能を用いてリスク管理・コンプライアンス対応を効率化

GRCSのクラウドサービス

GRCSのリスク管理サービス特徴

1 クラウドベースのアーキテクチャ

- 海外子会社や社外（委託先など）からのアクセスが可能
- 契約後すぐにデータを投入して利用開始が可能
- 機密データを保管する上で不安のないサービスレベル（セキュリティ）

2 スモールスタート可能なライセンスモデル

- 機能単位に分割しており、部署の予算でも購入しやすい金額感
- 会社規模にかかわらず利用ユーザー数ベースの課金モデル
- 現場への展開前に主管部署のみでのお試しができる

3 日本企業の利用に最適化した構成・テンプレート

- 日本固有のビジネス形態への対応（承認フロー、再委託など）
- 日本企業の利用実績に基づいた、実用的なテンプレート
- 画面表示や項目等を日英で切り替えが可能（グローバル対応）

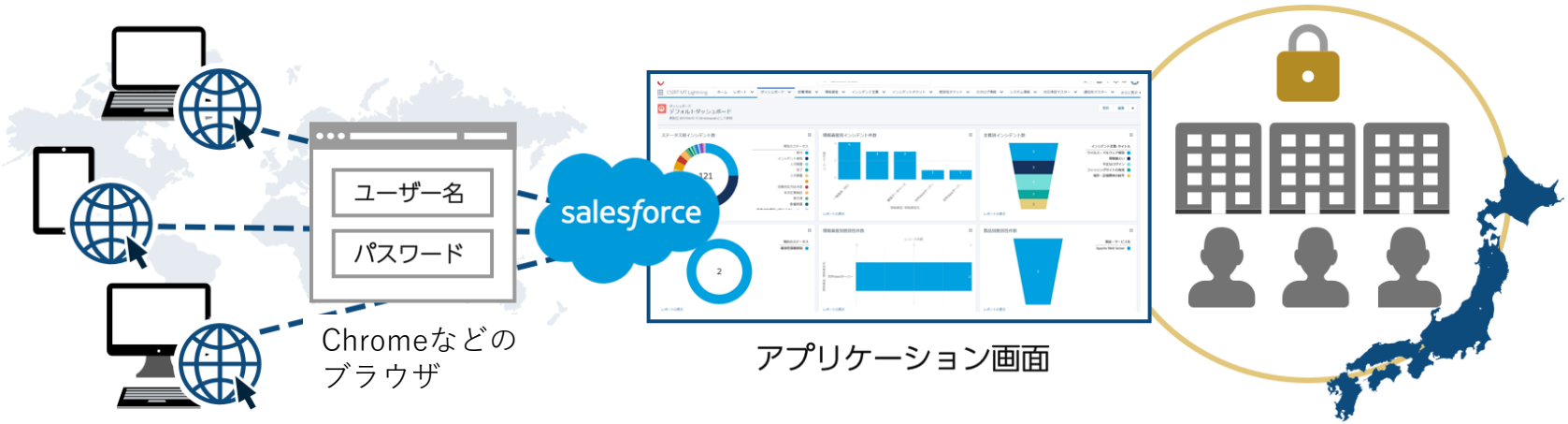
クラウドベースのアーキテクチャ

エリア

普段お使いのWebブラウザから海外など離れた拠点からも利用可能です。

セキュリティ

お客様環境（組織）ごとにデータやユーザは区分され、セキュリティ面も心配はありません。データも日本国内のデータセンターに保管されます。



プラットフォーム

株式会社セールスフォース・ドットコムが提供するプラットフォームである、「Salesforce App Cloud」上で動作します。

スモールスタート可能なライセンスモデル

ユーザーライセンス（利用するユーザー数 x 単価）
5ユーザーから利用開始が可能
使う機能・見える範囲を絞ったユーザーの単価を低く設定

※利用ユーザーの権限イメージ

リスク管理部ユーザー	**・各部門から上がってくるリスク情報の取りまとめ責任者** ・各種初期設定を行なう ・MTを日常業務に利用 ・MTのデータを利用し、上層部に報告を行う ・全ての情報を閲覧できる
リスクオーナー	**・部門でのリスク情報の取りまとめ責任者** ・部分的に初期設定を行なう ・担当のリスクや対応策の進捗状況について、リスク管理部に定期的にレビューを依頼する ・閲覧可能な情報の幅は設定可能
現場部門 **（担当者）**	**・実際に現場で実務を担当し、リスクを報告・対応する担当者** ・リスク対応においては、MT上で、自身が担当のリスクや対策の進捗状況について定期的に報告を行う ・自身が関わる情報のみ閲覧可能
モニタリングユーザー	・取締役や監査役など、リスク管理・内部監査に対して責任がある立場のユーザー

日本企業の利用に最適化した構成・テンプレート

◎テンプレート例

- インシデント対応のプレイブック
- 委託先リスク評価項目
- 委託先リスクチェックシート
- リスク一覧

◎多言語対応

- 日本語
- 英語
- その他（中国語繁体字等に今後対応予定）

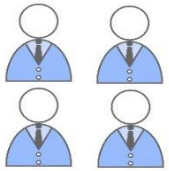
その他の導入効果（例）

1. ファイルの送受信・催促などの自動化による工数削減

Before　メール等を作成する手間が膨大。過不足チェックや催促が手作業
After　ツールで期日周知・予告・催促を自動的に行うためラクラクに

2. ステークホルダーとの調整・コミュニケーションの効率化

Before　会議を開催するにも担当役員の予定が合わず先延ばしになってしまう
After　ツール上で常に最新の状況を共有可能、疑問点はツール上で解消



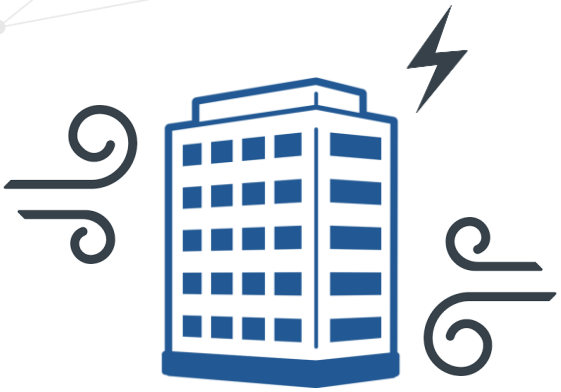
3. 離れた拠点、海外とのリスクマネジメント情報の共有の実現

Before　子会社や海外法人のリスクについては年1度のヒアリングのみ
After　入力しやすい画面や言語を用意する事で、リスク報告の習慣化

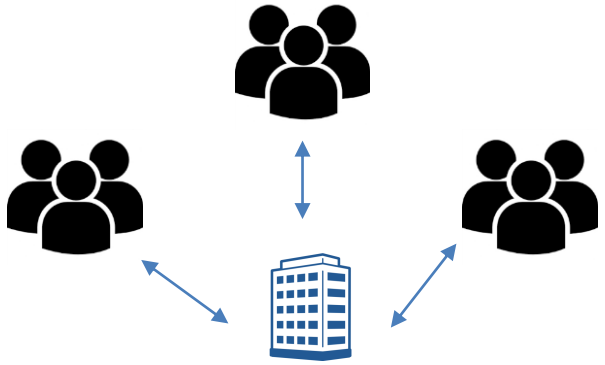
全社的リスク管理

Enterprise Risk MT

全社的リスク管理 の必要性



グローバル化や社会情勢の変化や災害発生、最近では内部不正や品質問題など、企業は多種多様なリスクを抱えるようになってきています。



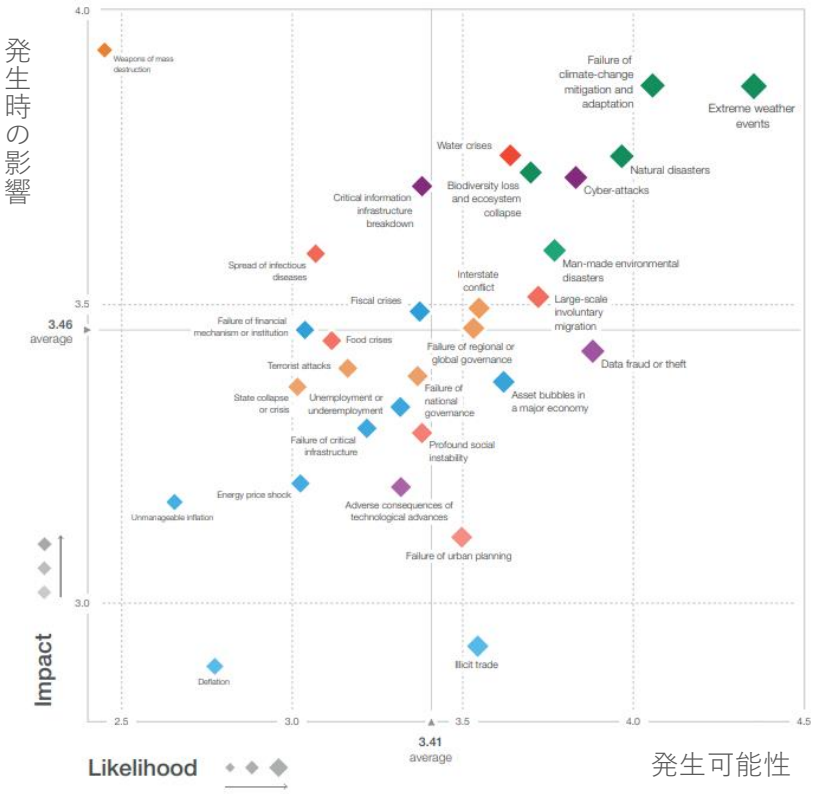
企業成長を持続させつつ、取引先・顧客、株主などのステークホルダーに対する責任を果たすために、様々な粒度でいろいろな分野に潜むリスクを管理する必要があります。
（会社法、有価証券報告書 etc）

全社的リスク管理（ERM：Enterprise Risk Management）とは、
・組織全体を対象にリスクを認識・評価し
・残余リスクの最小化を図るために、
・重要リスクの対応に優先的にリソースを配分し、
・継続的にリスク管理体制を強化していく一連のプロセス です。

グローバルにおけるリスクの変化

グローバルリスクの状況

- 世界経済フォーラムグローバルリスクレポート：グローバルリスクごとの発生確率と影響の分布



発生可能性の高い上位リスク

順位	2019年	2018年	2017年
1	異常気象	異常気象	異常気象
2	気候変動の緩和や適応への失敗	自然災害	自然災害
3	自然災害	気候変動の緩和や適応への失敗	大規模な非自発的移住
4	サイバー攻撃	サイバー攻撃	テロ
5	水危機	水危機	サイバー攻撃

出所）World Economic Forum Global「The Global Risks Report 2019」
https://www.weforum.org/reports/the-global-risks-report-2019
日本語版 http://www3.weforum.org/docs/WEF_GRR2019_日本語版.pdf

ESGのリスク管理が重要に

ESGとリスクマネジメント

2019年の上位リスク

順位	発生可能性	発生時の影響
1	**異常気象**	大量破壊兵器
2	**気候変動の緩和や適応への失敗**	**異常気象**
3	**自然災害**	**気候変動の緩和や適応への失敗**
4	サイバー攻撃	**水危機**
5	**水危機**	**自然災害**

出所）World Economic Forum Global 「The Global Risks Report 2019」
https://www.weforum.org/reports/the-global-risks-report-2019
日本語版　http://www3.weforum.org/docs/WEF_GRR2019_日本語版.pdf

ESGに関連するリスク（太字）が多数挙がっている

Environment（環境）
Social（社会）
Governance（企業統治）

企業活動において、
ESGをいかに重視し対応しているかが、
企業を評価する上での重要な指標に。

今後は、ESGのリスクを
しっかりと把握し マネジメントしていくか
が大きなテーマとなると考えられる。

※「ESGリスクに関わるガイダンス」を、2018年にCOSOおよびWBCSDが発行しています

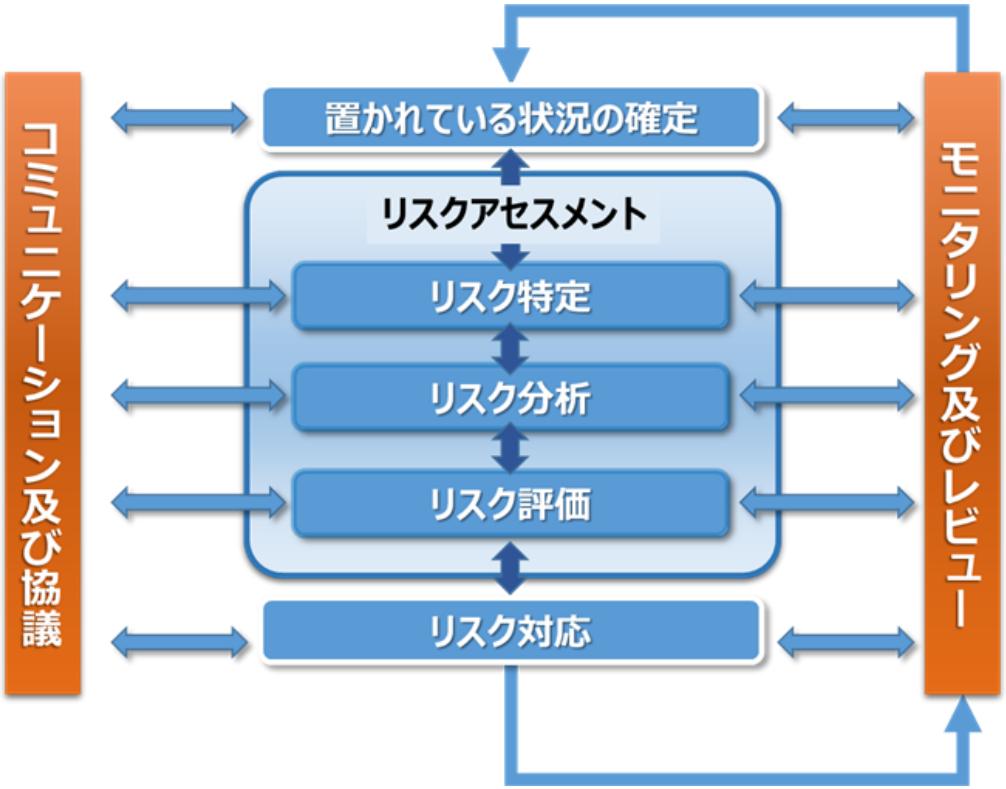
ERMの標準的なプロセス（ISO31000）

ERMのガイドラインの１つであるISO31000では、リスクマネジメントを3つの要素から構成されるもの、として捉えています。3つの要素とは「原則」「枠組み」「プロセス」です。

◎主管部署が事務局となる
・カタログの作成
・評価や管理策のレビュー
・ヒアリング
・進捗確認等

◎進め方
・アンケート方式
・ヒアリング方式
・折衷型

などで進めていく



ISO31000におけるプロセスの概念

Enterprise Risk MT 製品コンセプト

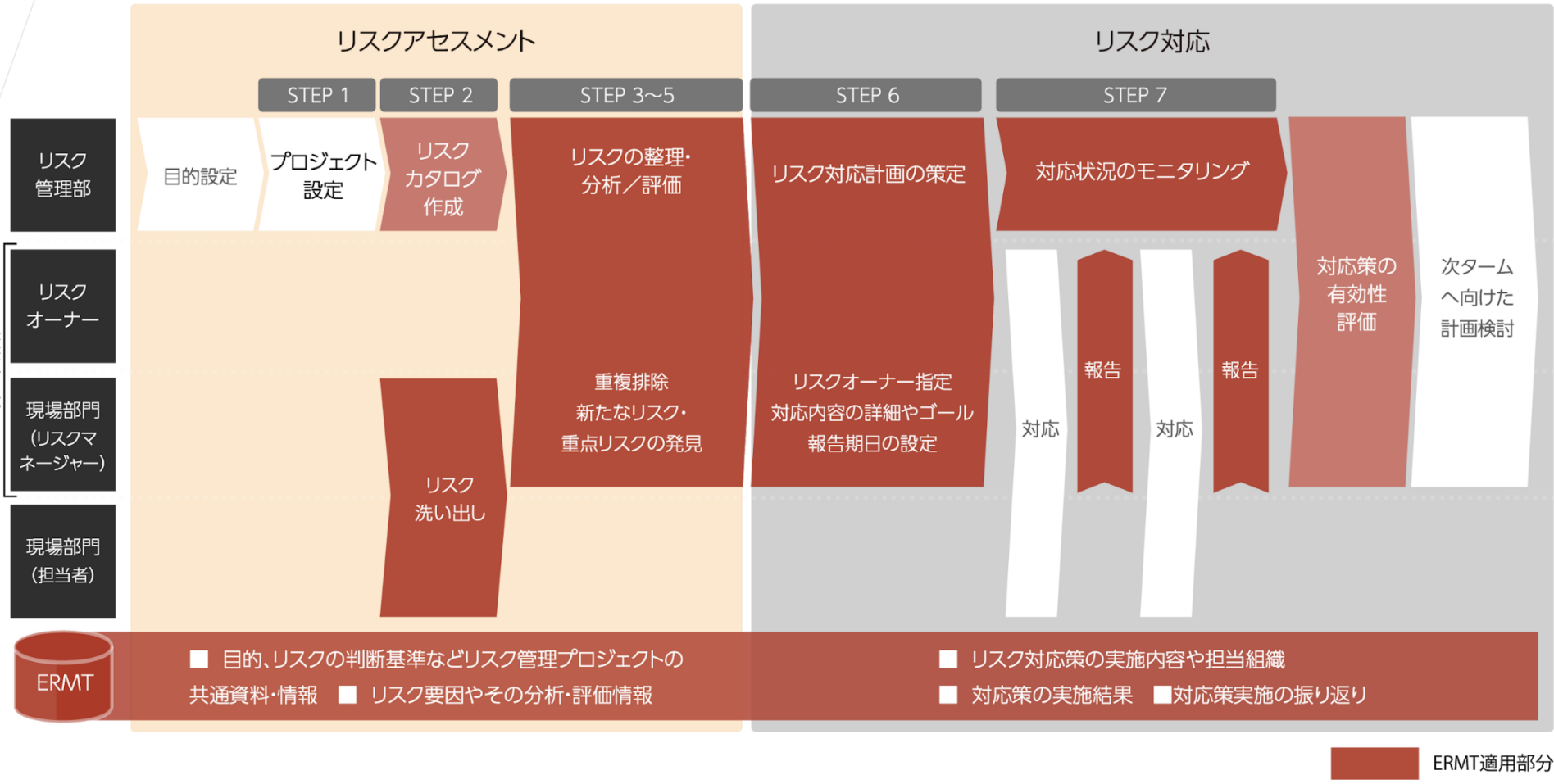
全社的リスク管理のハードル ERMTが解決します！

- リスクマネジメントの国際ガイドラインISO31000:2018ベース
- 可視化・分析がデータ量に関わらず自由自在
- 収集・集計・催促等を自動化して工数削減
- クラウドサービスで導入が容易
- スモールスタート可能なライセンスモデル

ISO準拠のねらいは、多角的な利用を踏まえた全社的リスク管理基盤の提供を目指している点にあります

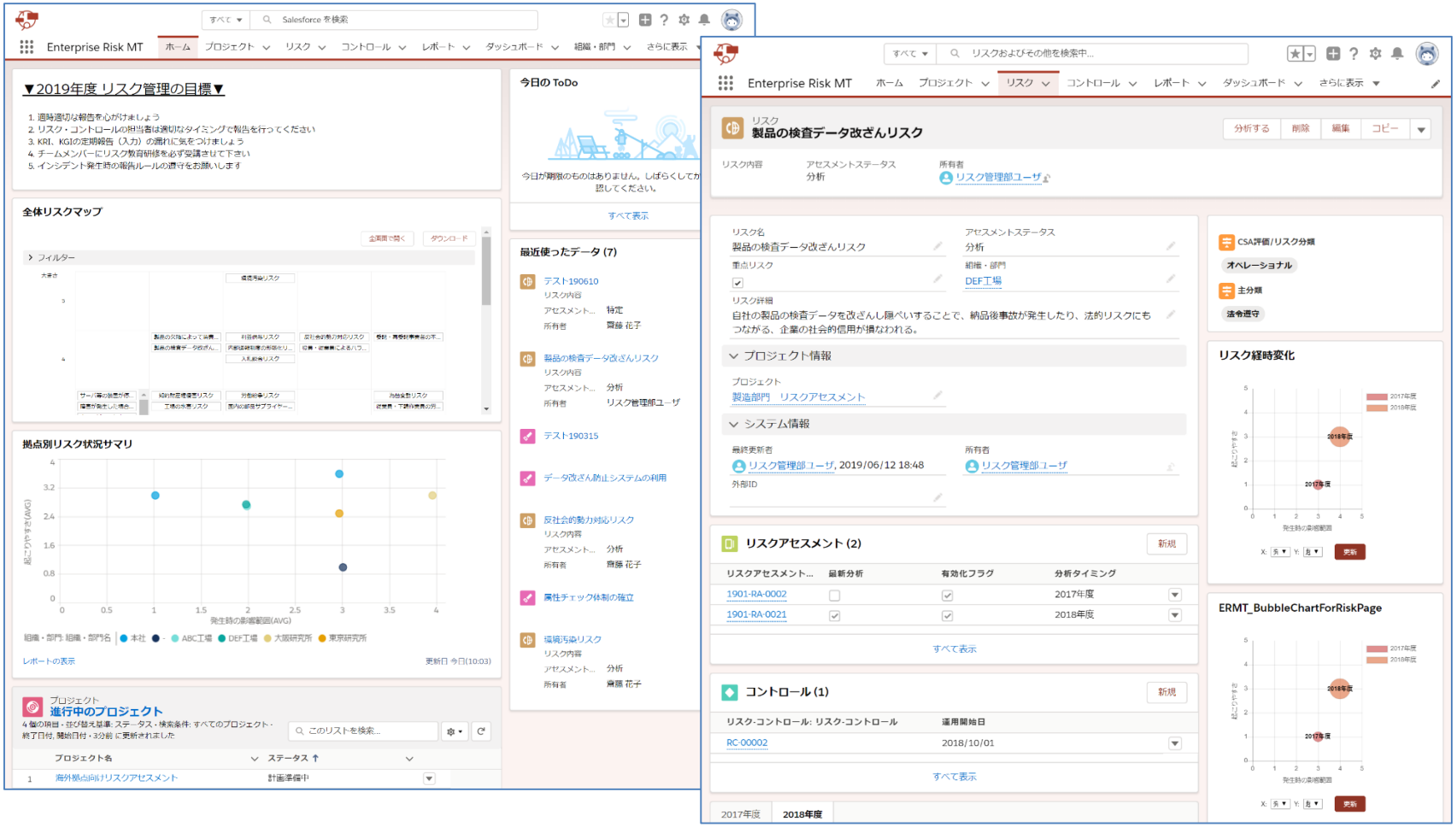
Enterprise Risk MTを用いたERM運用例

ERMTは 全社的リスク管理のプロセスを広範囲にカバーし、支援します。



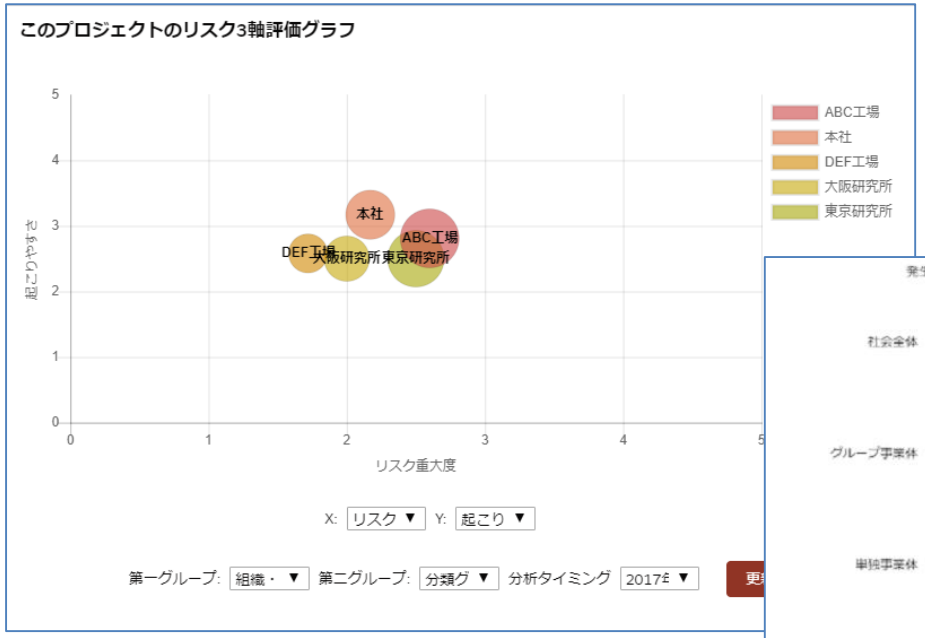
Enterprise Risk MT 入力画面

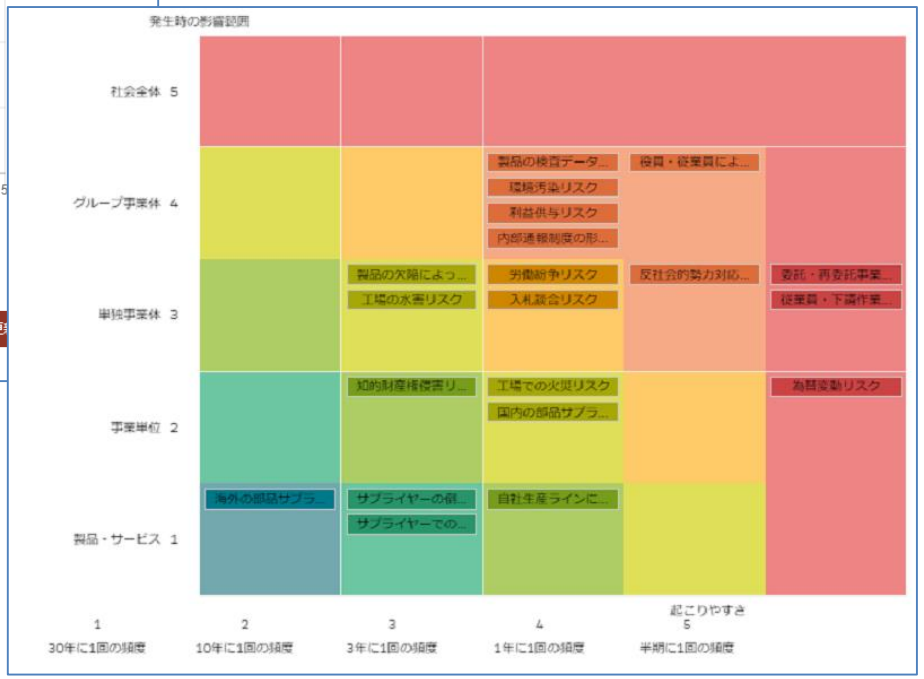
Salesforceのわかりやすい入力画面から、フェーズ毎に情報を簡単に入力可能です。Excel等で作成したCSVファイルのインポート・エクスポートも専用ツール・ウィザードを利用でき、難しい操作は必要ありません。



Enterprise Risk MT 分析画面

リスクマップやクロス集計など多角的な分析が可能です。
部署別・拠点別のリスク一覧や平均との比較なども表示でき、リスクマトリックス（2軸）とバブルチャート（3軸+1）が標準装備されています。





Enterprise Risk MT 導入事例

【解決した課題】

- 50人の幹部社員にヒアリングを行い、グループ内のリスクは約300項目にも上るが、CSR推進グループが1つのExcelファイルで管理を行っていた。
- データ分析はExcelのデータを並べ替えたり組み替えたりして、マンパワーでどうにか対処していた。

【導入効果】

- **作業時間が大幅に削減**された。
  →分析作業はRisk Organizer上で数クリックするだけ
  →リスクの分析と対策の策定に時間を割けるようになった
- 様々な角度から分析することが可能になった為、「**潜在リスク**」**を発見**する一助となった。
- **ESGのリスクに関する洗い出しの機能等、**国内開発のクラウドサービスのため**要望が迅速に実現**された。

外部委託先リスク管理

Supplier Risk MT

外部委託先リスク管理が必要な背景

企業において、外部委託は業務を遂行する上で必要不可欠です。一方、外部委託先における不祥事は数多く発生しており、昨今、適切な外部委託先管理は、重要テーマとして対応が義務付けられており、経営の重要な関心事項となっています。

■ 委託先における不祥事の例

- **印刷会社個人情報漏洩**
  個人情報の一部が業務委託先の社員により不正に持ち出された
- **教育サービス個人情報漏洩**
  グループ企業の委託先社員から大量の個人情報が漏洩し、業績が悪化し赤字転落
- **地銀データ不正取得**
  保守を請け負っていた二次受け社員が解析用ログを悪用して預金が不正に引き出された
- **プロバイダー顧客情報漏洩**
  代理店の社員が不正に取得し、経営陣を恐喝した

■法規制・ガイドライン

- **個人情報保護法**
  -第22条　委託先の監督
- **金融庁監督指針**
  -III -3-3-4　外部委託（主要行等）
  -II -3-2-4　外部委託（中小・地域金融機関）
  -II -5-1　保険会社の事務の外部委託
- **割販法**
  -第35条3ノ43　八
- **サイバーセキュリティ経営ガイドライン**
  - 3.3.（7）IT システム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保

外部委託先のセキュリティ管理を適切に行わず、事故が起こった場合の経営リスクは非常に高い

Supplier Risk MT 製品コンセプト

Supplier Risk MT（サプライヤーリスクMT）は、業務委託に関わるセキュリティリスクの一元的な管理、可視化、コミュニケーションを支援するためのアプリケーションです。

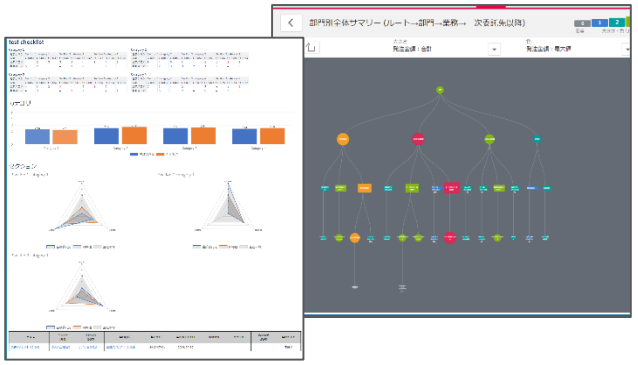
製品の特徴

- ✓ **Web・クラウド**での集約管理による**一元化**と**工数削減**
- ✓ 注視すべき**委託先**とその**セキュリティリスクレベル**が一目瞭然
- ✓ **自己点検結果**や**再委託**関係など多角的な視点での委託先評価を支援
- ✓ 委託先管理と委託契約の**マスターデータベース**としても活用可能

Supplier Risk MT ユーザー利用イメージ

ユーザーの権限および組織（部門）に応じた階層的な管理が行えます。
全社の情報が閲覧できる「パワーユーザー」、自部門に関する情報にのみアクセスできる「マネージャーユーザー」、業務や委託先に関する情報を入力する「一般ユーザー」を用意することで、組織内部の独立性を保った管理を実現します。
「委託先ユーザー」は、点検フォームへの入力、送信のみ実施します。

※社内ユーザーのアクセス権限は柔軟に設定できます。



全体のリスク情報を分析

パワーユーザー
（委託先管理統括部署）

点検フォームに入力し送信

委託業務情報を入力

マネージャーユーザー
（委託元部署）

一般ユーザー
（委託元部署）

委託先ユーザー
（委託先企業）

Supplier Risk MT 導入効果

主な導入効果を以下に記します。

経営層

自社の委託先管理状況を俯瞰したい

委託先管理統括部署

各部門の委託先の管理状況を一元的に把握したい

委託元部署

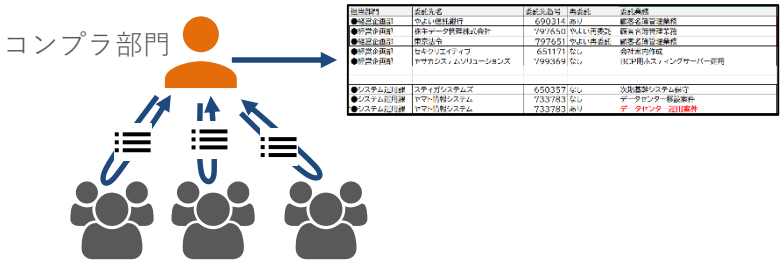
自部門の委託状況の管理工数を削減して効率的に行いたい

- これまでも実施している**委託先管理全体を一元化**する。
- 委託先の自己点検結果を**委託先がWebフォームで直接回答**することも可能であるため、委託元としての**収集・集計負荷が低減**される。
- 自社組織や委託先企業・業務情報と併せて、委託先自己点検回答もデータベース化することにより、様々な角度から**効率的で適切な評価**が可能となる。
- 二段階以上の委託（再委託）を含め、**一目で委託状況を把握**する。
- 社内それぞれの立場に合わせた**見るべき、見たい情報が得られる。**

Supplier Risk MT 導入事例

Before

現場部門から収集した委託先・委託業務情報を1Excelファイルに集約

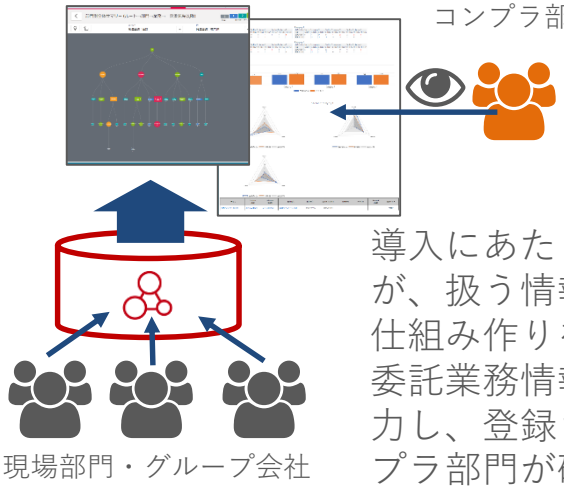


課題

◆取りまとめ担当者の属人的な作業になりがち、また情報収集に追われ適切な分析を行う時間がない

◆再委託関係などのデータを構造的に管理できず、1ファイルにまとまっていても、全体感がつかみにくい

After



導入にあたり、コンプラ部門が、扱う情報の取捨や社内の仕組み作りを実施
委託業務情報は現場部門が入力し、登録された情報をコンプラ部門が確認、分析

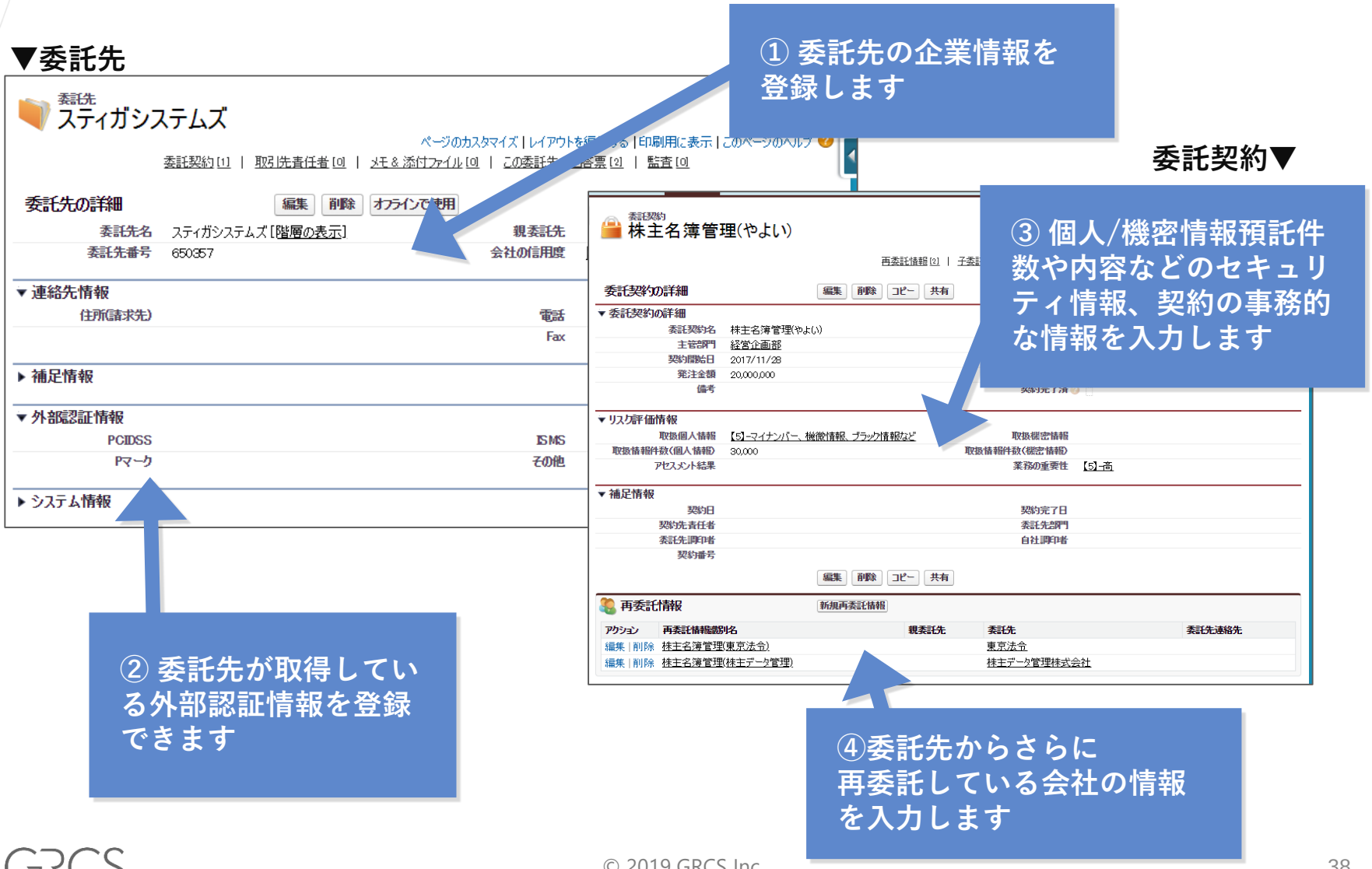
解決した課題以外のベネフィット

◆契約(基本/個別)やその稟議の情報、実際の業務内容、また委託先監査結果など、1つの委託業務に関連した情報を一元化し蓄積しているので、委託先管理状況をワンストップで確認できる

◆監査結果も記録できるので、経年変化を把握できる

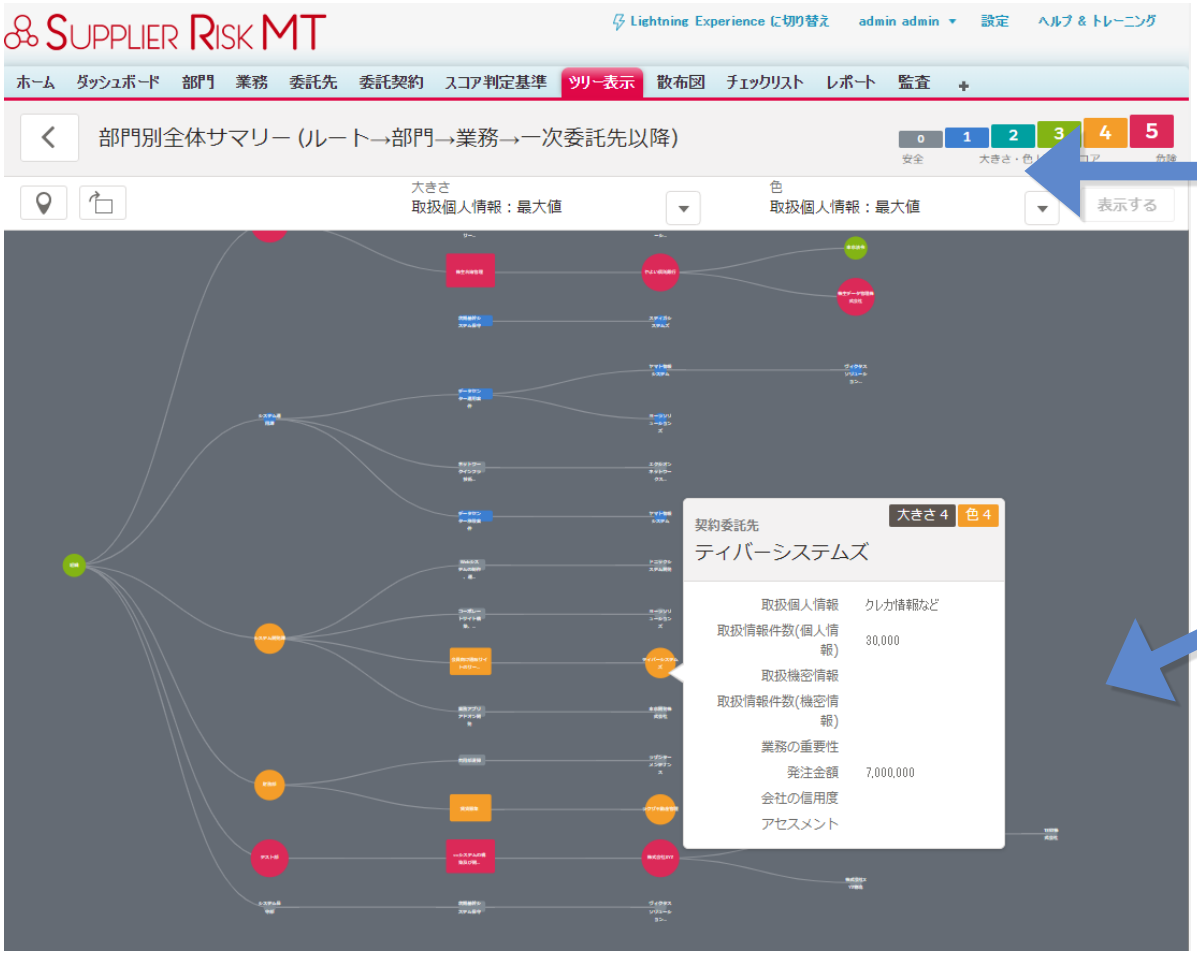
Supplier Risk MT 入力画面

委託先企業や委託業務について登録します。



Supplier Risk MT 分析画面

業務委託の階層構造を視覚的に把握することができます。個人情報の預託件数や業務の重要度、会社の信用度など8要素から2つ選択して可視化し、注視すべき委託先を明確にします。

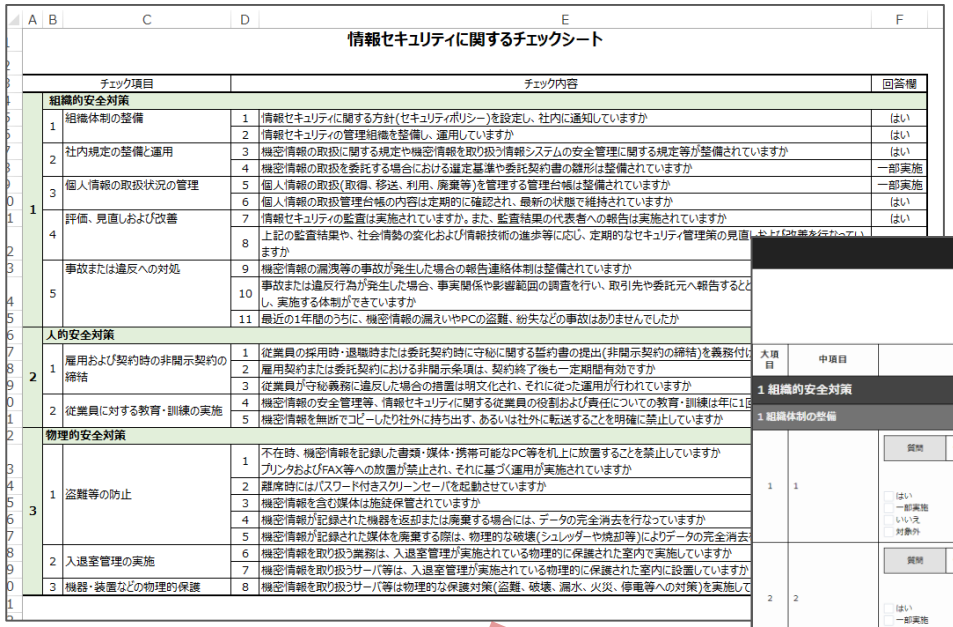


① 評価する要素を2つ(それぞれ”大きさ”と”色”)選択します

② リスクの高い委託先や再委託先のノードが色や大きさで表示されます

Supplier Risk MT 点検フォーム画面

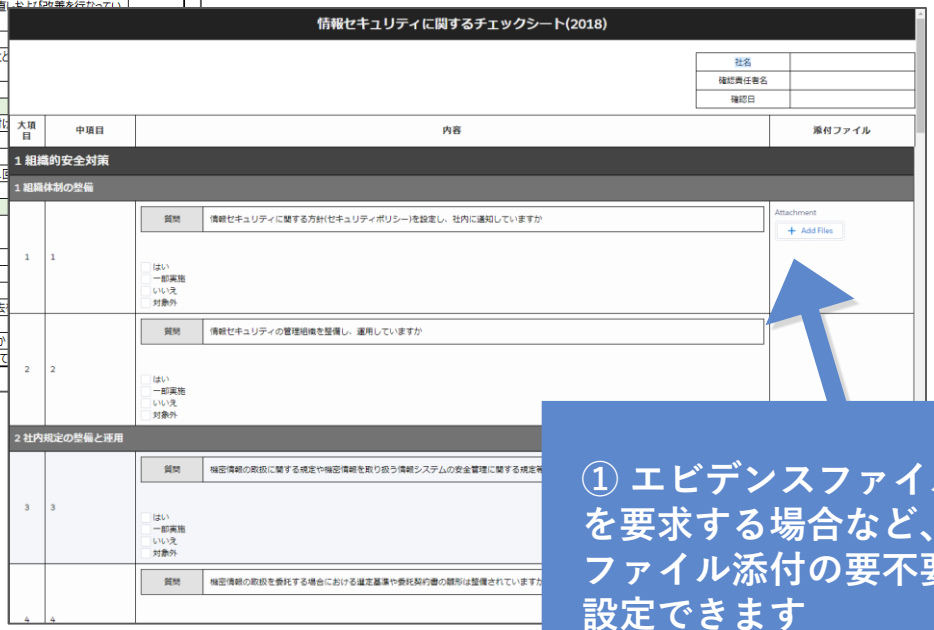
質問と回答選択肢(最大6つ)を設定し、複数の質問をセクション(中項目)、カテゴリ(大項目)、チェックシートという枠組みでまとめ、点検フォームを作成します。
委託先ユーザーはログイン後このフォームにアクセスし、点検内容を入力・送信します。



情報セキュリティに関するチェックシート

		チェック項目		チェック内容	回答欄
1	組織的安全対策				
	1	組織体制の整備	1	情報セキュリティに関する方針(セキュリティポリシー)を設定し、社内に通知していますか	はい
			2	情報セキュリティの管理組織を整備し、運用していますか	はい
	2	社内規定の整備と運用	3	機密情報の取扱に関する規定や機密情報を取り扱う情報システムの安全管理に関する規定等が整備されていますか	はい
			4	機密情報の取扱を委託する場合における選定基準や委託契約書の雛形は整備されていますか	一部実施
	3	個人情報の取扱状況の管理	5	個人情報の取扱(取得、移送、利用、廃棄等)を管理する管理台帳は整備されていますか	一部実施
			6	個人情報の取扱管理台帳の内容は定期的に確認され、最新の状態で維持されていますか	はい
	4	評価、見直しおよび改善	7	情報セキュリティの監査は実施されていますか。また、監査結果の代表者への報告は実施されていますか	はい
			8	上記の監査結果や、社会情勢の変化および情報技術の進歩等に応じ、定期的なセキュリティ管理策の見直しおよび改善を行っていますか	
	5	事故または違反への対処	9	機密情報の漏洩等の事故が発生した場合の報告連絡体制は整備されていますか	
			10	事故または違反行為が発生した場合、事実関係や影響範囲の調査を行い、取引先や委託元へ報告するとともに、実施する体制ができていますか	
			11	最近の1年間のうちに、機密情報の漏えいやPCの盗難、紛失などの事故はありませんでしたか	
2	人的安全対策				
	1	雇用および契約時の非開示契約の締結	1	従業員の採用時・退職時または委託契約時に守秘に関する誓約書の提出(非開示契約の締結)を義務付けていますか	
			2	雇用契約または委託契約における非開示条項は、契約終了後も一定期間有効ですか	
			3	従業員が守秘義務に違反した場合の措置は明文化され、それに従った運用が行われていますか	
	2	従業員に対する教育・訓練の実施	4	機密情報の安全管理等、情報セキュリティに関する従業員の役割および責任についての教育・訓練は年に1回以上実施していますか	
			5	機密情報を無断でコピーしたり社外に持ち出す、あるいは社外に転送することを明確に禁止していますか	
3	物理的安全対策				
	1	盗難等の防止	1	不在時、機密情報を記録した書類・媒体・携帯可能なPC等を机上に放置することを禁止していますか プリンタおよびFAX等への放置が禁止され、それに基づく運用が実施されていますか	
			2	離席時にはパスワード付きスクリーンセーバを起動させていますか	
			3	機密情報を含む媒体は施錠保管されていますか	
			4	機密情報が記録された機器を返却または廃棄する場合には、データの完全消去を行なっていますか	
			5	機密情報が記録された媒体を廃棄する際は、物理的な破壊(シュレッダーや焼却等)によりデータの完全消去を行なっていますか	
	2	入退室管理の実施	6	機密情報を取り扱う業務は、入退室管理が実施されている物理的に保護された室内で実施していますか	
			7	機密情報を取り扱うサーバ等は、入退室管理が実施されている物理的に保護された室内に設置していますか	
	3	機器・装置などの物理的保護	8	機密情報を取り扱うサーバ等は物理的な保護対策(盗難、破壊、漏水、火災、停電等への対策)を実施していますか	

▲Excelのチェックシート



情報セキュリティに関するチェックシート(2018)

社名	
確認責任者名	
確認日	

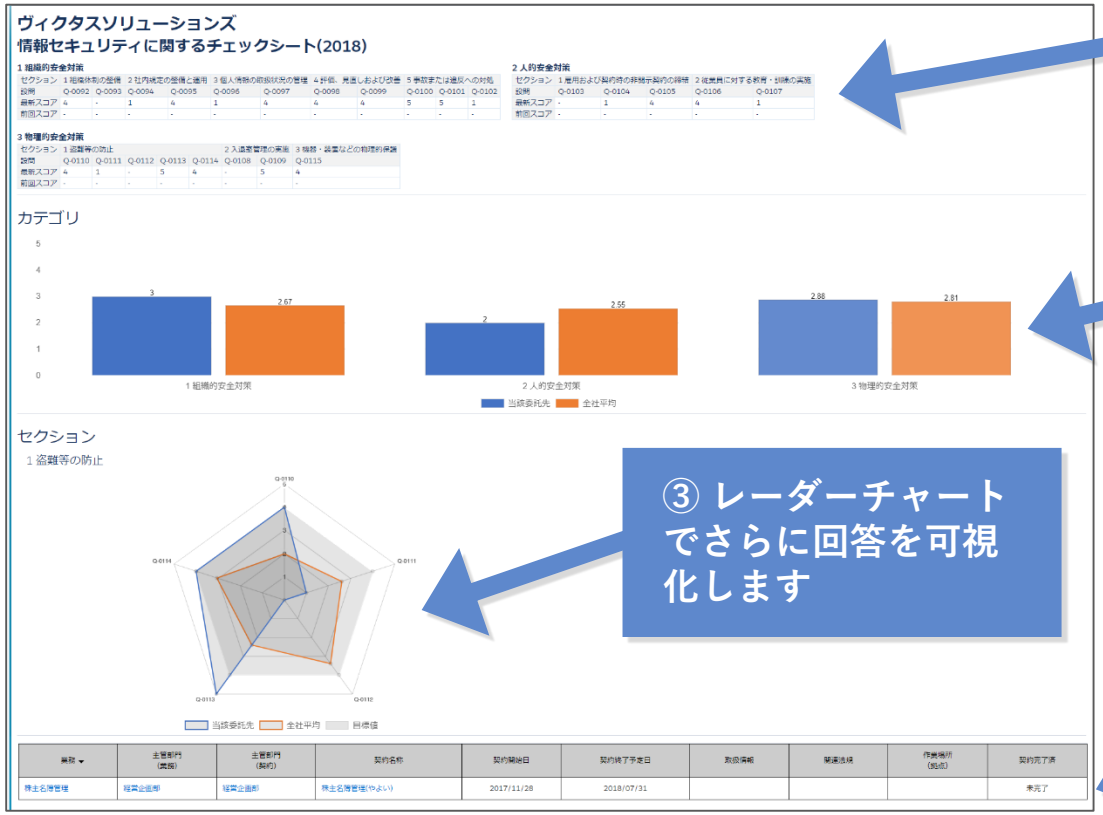
大項目	中項目	内容	添付ファイル
1 組織的安全対策			
1 組織体制の整備			
1	1	質問: 情報セキュリティに関する方針(セキュリティポリシー)を設定し、社内に通知していますか はい / 一部実施 / いいえ / 対象外	Attachment: + Add Files
2	2	質問: 情報セキュリティの管理組織を整備し、運用していますか はい / 一部実施 / いいえ / 対象外	
2 社内規定の整備と運用			
3	3	質問: 機密情報の取扱に関する規定や機密情報を取り扱う情報システムの安全管理に関する規定等が整備されていますか はい / 一部実施 / いいえ / 対象外	
4	4	質問: 機密情報の取扱を委託する場合における選定基準や委託契約書の雛形は整備されていますか	

▲作成した点検フォーム

① エビデンスファイルを要求する場合など、ファイル添付の要不要が設定できます

Supplier Risk MT 回答画面

委託先の点検回答内容に関して、個社毎に前年対比や傾向などをレーダーチャートで表示します。当該委託先に委託している業務の詳細情報もこのサマリー画面で見ることができます。



①回答スコアを表形式で表示します

② 設問カテゴリ毎の平均値を表示します

③ レーダーチャートでさらに回答を可視化します

④ 当該企業に委託している業務情報を表形式で表示します

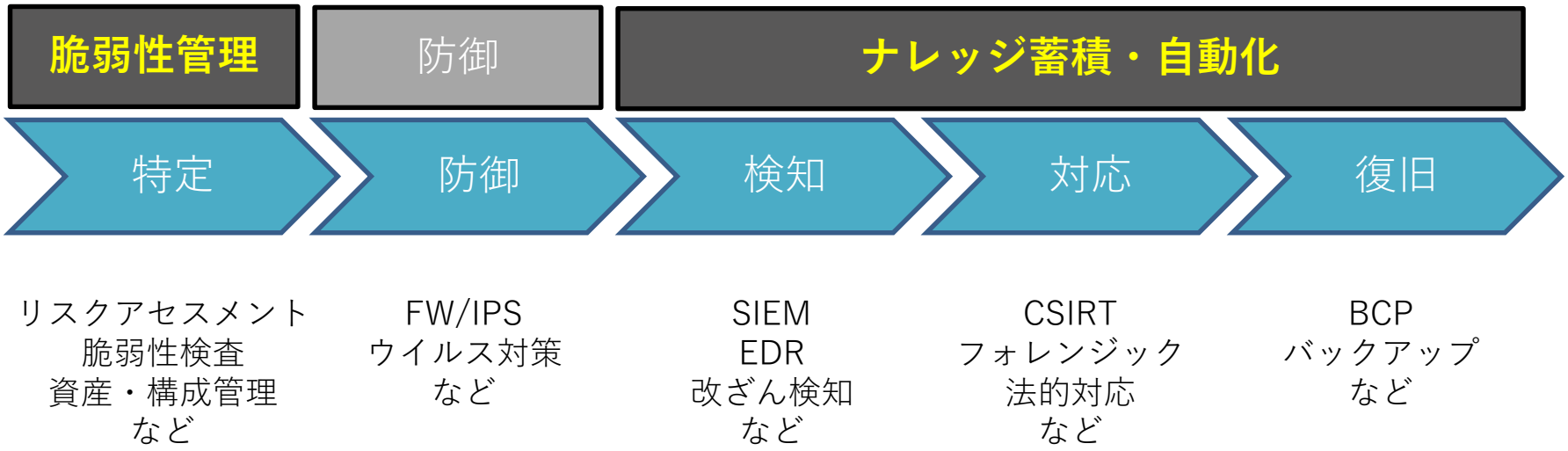
サイバーインシデントリスク管理

CSIRT MT

サイバーインシデント管理の必要性

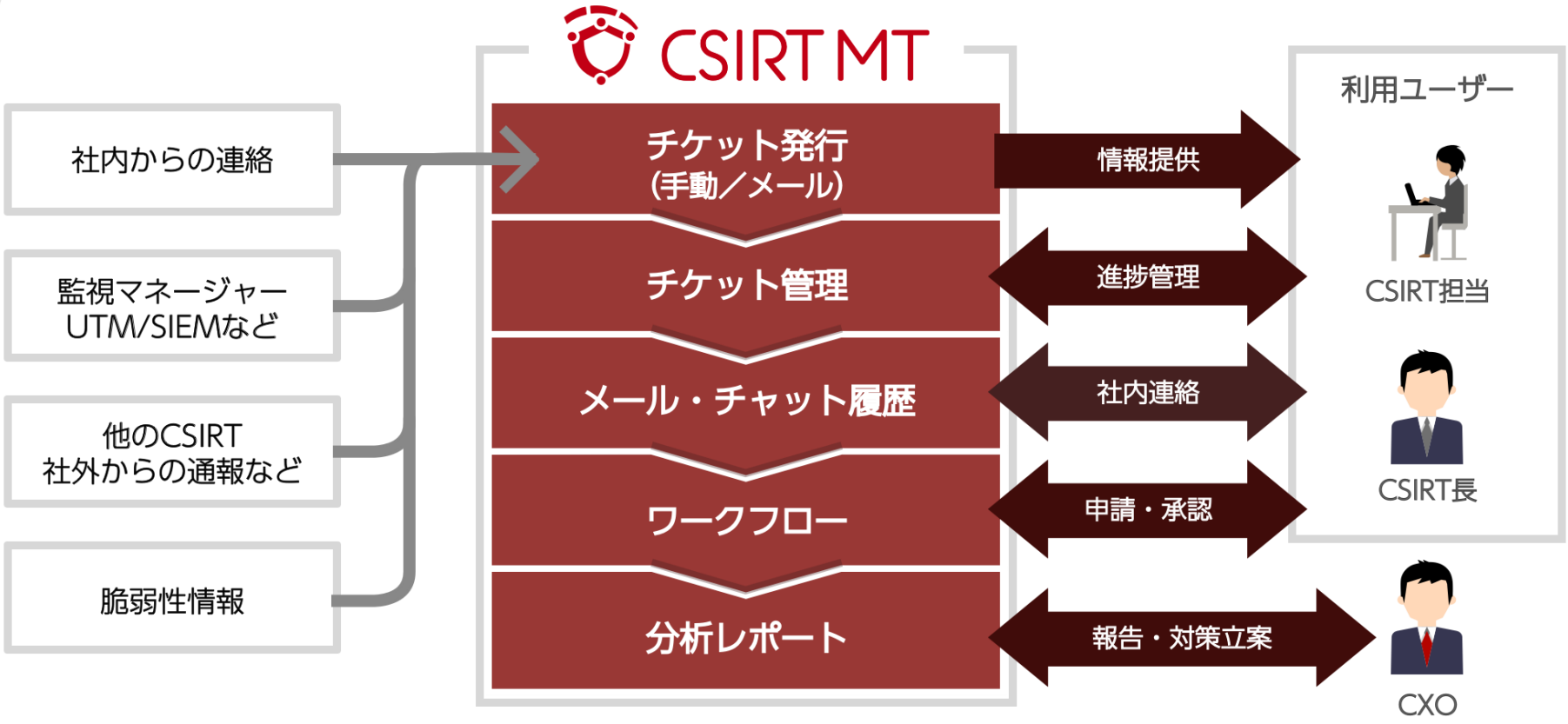
- サイバー攻撃の多様化・高度化
- 攻撃による被害の大規模化
- CSIRTによる対処の必要性

インシデント対応における対策例



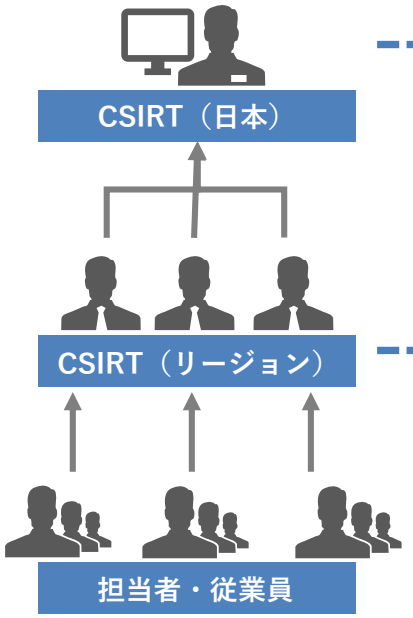
CSIRT MT製品コンセプト

CSIRTやSOCの運用に最適化した、チケット・タスク管理と
情報共有のためのクラウドアプリケーションです。



CSIRT MT 導入事例

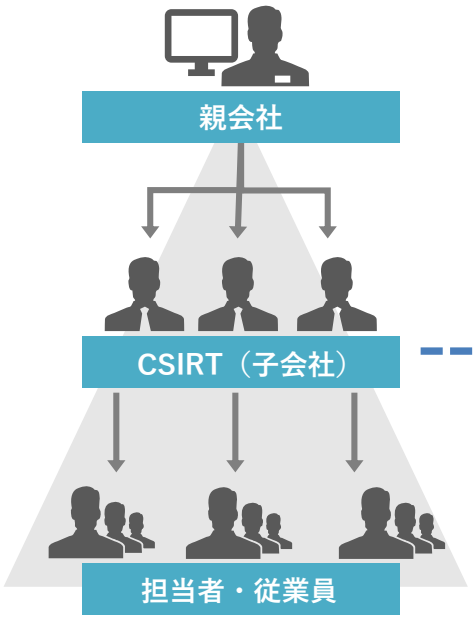
A. グローバル企業（インシデント対応）



②日本のCSIRTチームが、インシデントの状況把握・指示および案件Closeの承認を行う。

①リージョンのCSIRTメンバーが、担当エリア内でのインシデントを報告（英語）

B. グループ企業（脆弱性対応）



①親会社から定期的に脅威情報・脆弱性情報を提供

②子会社で各情報に対して、自社での該当有無と、対応の進捗確認を実施し、親会社に報告。

CSIRT MTインシデント管理画面

インシデント対応における調査項目を網羅したチケット管理をメインに、関係者への通知、行うべき項目のチェックリスト、進捗状況やファイルを随時追記していくメモ＆添付ファイル等の必要機能をすべて一元化しています。

CSIRT MT プレイブック画面

インシデントチケット内に、調査・対応すべき項目をあらかじめチェックリストとして設定し、実施履歴と結果を管理することができます。公的ガイドラインにて推奨されている確認項目に加えて弊社オリジナルのサンプルが設定されています。もちろん追加や編集は自由に可能です。

「ウイルス・マルウェア感染」・・・GRCSが提供するサンプル項目と、ガイドラインの推奨項目をセット
「不正アクセス」「情報漏えい」「DoS攻撃」・・・ガイドラインの推奨項目をセット

インシデント対応チェックリスト(21)
2 件のレコードがチェックされました。

チェックされたレコードを全て保存する　New

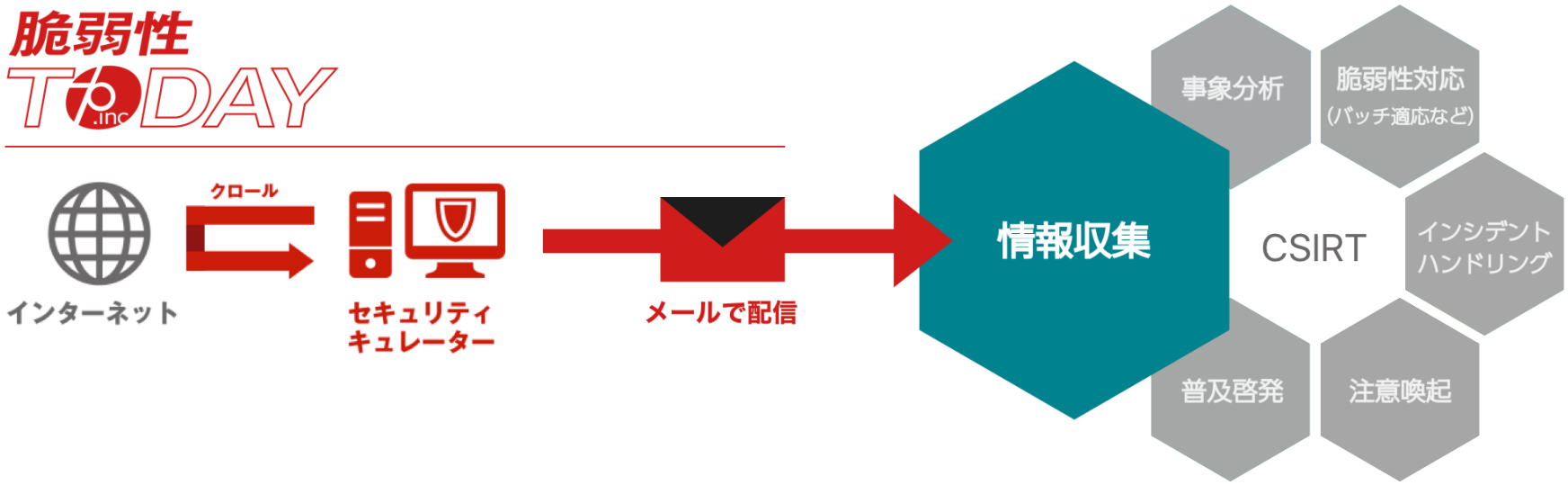
	インシデント定義	チェック内容	調査項目	担当	実施日時
☑	ウイルス・マルウェア感染/Virus・...	・どのPCか？ ・ウイルスを受信したのは何時か？ ・ウイルスは駆除できたか？	ウイルスの感染状況は確認できたか？	徳永	2018/02/27 12:00:00
☑	ウイルス・マルウェア感染/Virus・...	・リアルタイムでの検知か？定期ス...	検知のタイミングは？	徳永	2018/02/28 12:00:00
☐	ウイルス・マルウェア感染/Virus・...	・すべてのPCの最近のスキャン実施...	他のPCは感染していないか？		
☐	ウイルス・マルウェア感染/Virus・...	・情報漏えい、データ改ざん・破壊...	ウイルスの種別やウイルスが感染し...		
☐	ウイルス・マルウェア感染/Virus・...	・スキャンの履歴・結果を確認 ・ウイルスの種類が分かればウイル...	既存のウイルスチェックソフトウェ...		
☐	ウイルス・マルウェア感染/Virus・...	・すべてのPCでパターンファイルの...	すべてのPCでパターンファイルの最...		
☐	ウイルス・マルウェア感染/Virus・...	・すべてのPCのスキャン結果を確認。	すべてのPCで再スキャンを実施した...		
☐	ウイルス・マルウェア感染/Virus・...	・送信元が不明、サイトのドメイン...	メールサービスでウイルス送信元か...		
☐	ウイルス・マルウェア感染/Virus・...	・トロイの木馬、バックドア、リモ...	検知したウィルスの種類は？どのよ...		
☐	ウイルス・マルウェア感染/Virus・...	・最近のスキャン実施日時 ・ファイル、レジストリ等の更新日付	いつから感染していたか？		
☐	ウイルス・マルウェア感染/Virus・...	・感染日時の確認、感染日時前のバ...	ウイルスに感染した場合、デバイス...		

CSIRT MT 脆弱性情報画面

日々発表される脆弱性情報や脅威情報をチケットとして登録し、システム構成情報とマッチしたチケットに対して、パッチ適用などの対策の進捗を管理。該当IT資産や承認者への承認依頼、関係者への通知等の機能をすべて一元化します。

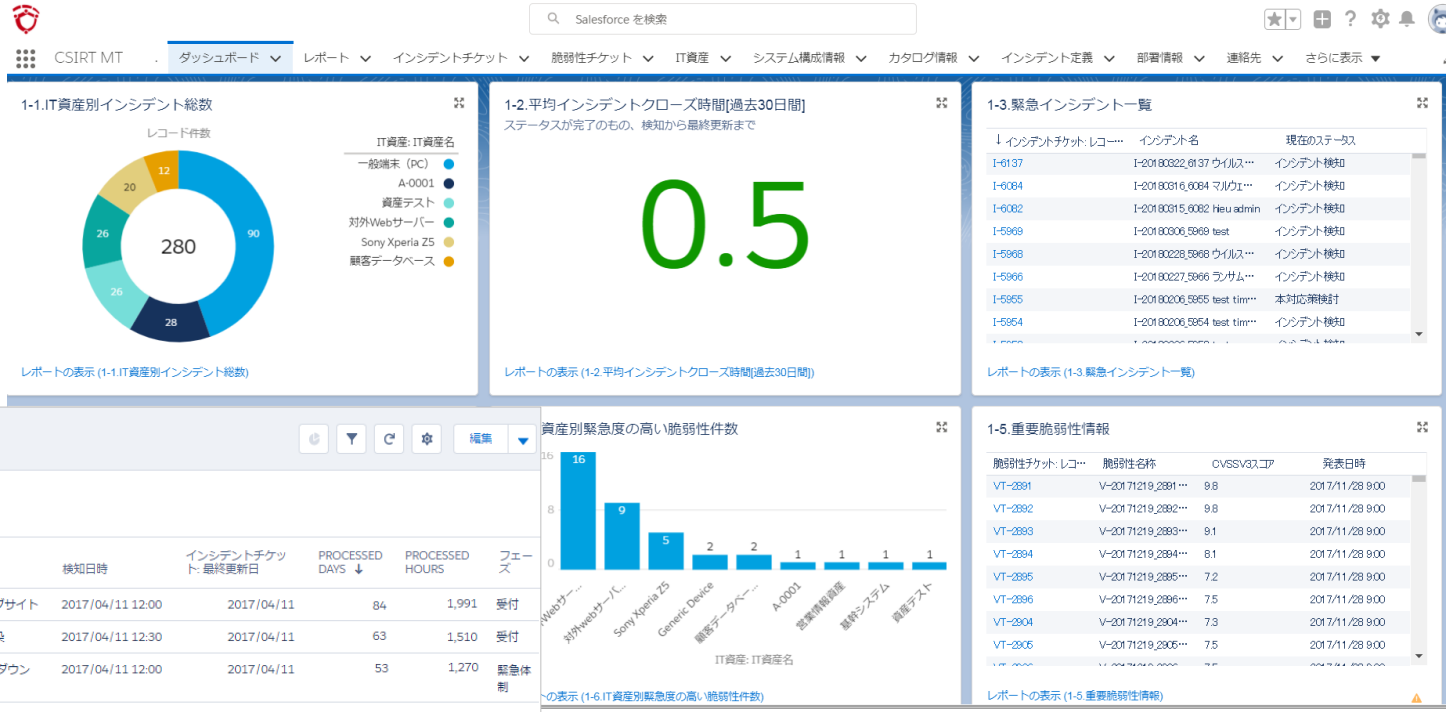
脆弱性TODAYとの連携

脆弱性情報日次配信サービス「脆弱性TODAY」は、日々作業が煩雑な脆弱性情報収集を弊社コンサルタントが行い、更に整理し当日午後に配信するサービスです。
国内外のセキュリティ最新情報を毎日、いち早く収集する事によりCSIRTの運用を大きくサポート。また、予めCSIRT　MTに登録された情報資産にマッチする脆性を自動で検知し、初動もスムーズに進めることが可能です。



CSIRT MT レポート＆ダッシュボード

標準でCISO向けとCSIRTの現場向けダッシュボードを実装。いつでも瞬時に状況把握が可能。また、運用状況に関するレポートも「お客様ごとの切り口」で簡単に作成でき経営層への報告業務を支援します。



ご参考

MT製品評価プログラム

お客様環境下で製品を実際に1か月間無償でご評価頂けるPOC（ Proof of Concept ）プログラムをご用意しております。製品画面、操作性、フィールドに仮データを入力頂き運用イメージを創造頂く事が可能です。
＊ロケーションによりオンサイト、電話会議等、**第一週目のライセンスご提供後、コンサルタントとの操作レビュー、　操作上、お客様運用上の疑問等のレビュー打合せ**を実施しております。

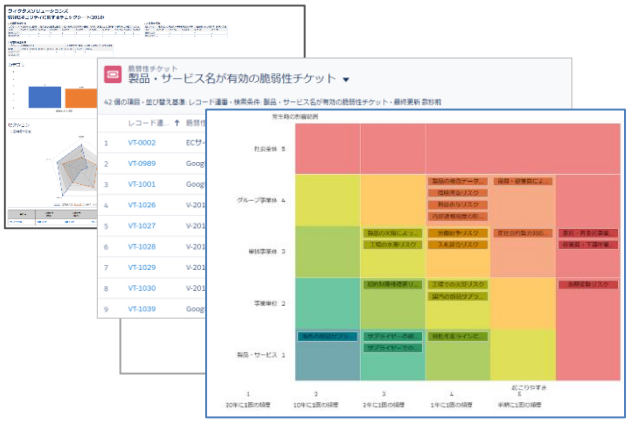
実施期間：約4週間（想定スケジュール例）

1週目 初期操作 → 2週目 レビュー操作 → 3週目 → 4週目 運用想定

期間中はお客様運用イメージ、操作性、将来の運用イメージを想定

弊社コンサルとのレビュー打合せの項目サンプル

フィールド毎にお客様との打合せを実施し、具体的な運用イメージを協議。



保険代理店管理（保険GRC MT）

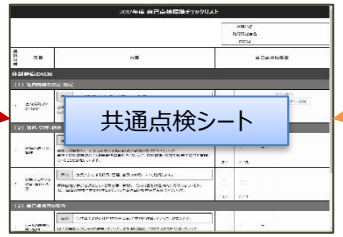
保険GRC MTは、生命保険会社様と募集代理店様、両社の点検負荷を大幅に削減することができるサービスです。
募集代理店のご担当者様が、クラウド上に構築された保険GRC MTにアクセスし、共通自主点検シートに対して入力・送信することで、各生命保険会社様が入力結果を取得できる仕組みです。
この取得の際には、ファイルのアップロード機能を利用すれば、点検の証跡（エビデンス）を取得する事も出来ます。

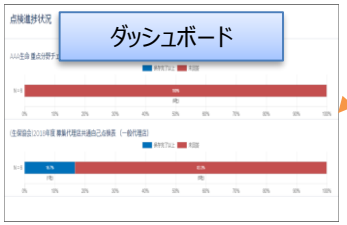
【概要】

募集代理店

- ✓ 募集代理店が自主点検シートに一度回答するだけで、委託元の保険会社全てに対して回答が完了します※1
- ✓ また、エビデンスをファイルにて、アップロードすれば、保険会社への提出も可能
- ✓ 共通点検シート以外の項目がある場合は、その追加シートへの回答も可能
- ✓ 未対応事項については、回答期限をセットする事で、保険GRC MTがトラッキングを実施

自主点検ソリューション





保険会社

- ✓ 募集代理店の点検結果とエビデンスを閲覧可能。
- ✓ 共通点検シート以外(独自の質問)がある場合は、そのシートもアップすることが可能
- ✓ ダッシュボードにて、対応状況や未対事項への改善進捗状況を把握することが可能

※1　委託元の生命保険会社が、本システムを利用している事が前提となります。

GRCS

www.grcs.co.jp

ご清聴ありがとうございました。