セキュリティ監査の自動化への取り組み

2025年 1月

佐藤 要太郎

自己紹介

PwC Japan有限責任監査法人

リスクアシュアランス部門

セキュリティやシステム監査、ITガバナンス高度化支援、内部監査支援等に従事。DXが進んだ企業（デジタルエンタープライズ）やモダンエンジニアリング（Agile/DevOps）を行う企業に対するリスクコントロールアドバイザリーを得意とする。

レポート
- トラストをともに駆ける（DevOps態勢下のITコンプラ対応） 2022
- 公的機関におけるパブリッククラウド調達の新たな方向性 2016

書籍
- クラウド・リスク・マネジメント 2021
- ソフトウェア開発の会計・税務・リスクマネジメント 2023

ISACA東京支部基準委員会 元メンバー

システム監査
技術者（IPA）

本日のお話し

最新の技術要素に触れながら、セキュリティ監査の自動化を解説します。

今どこまで自動化が実現できるのかとともに、ラストワンマイル対応に向けた論点にも触れます。

アジェンダ

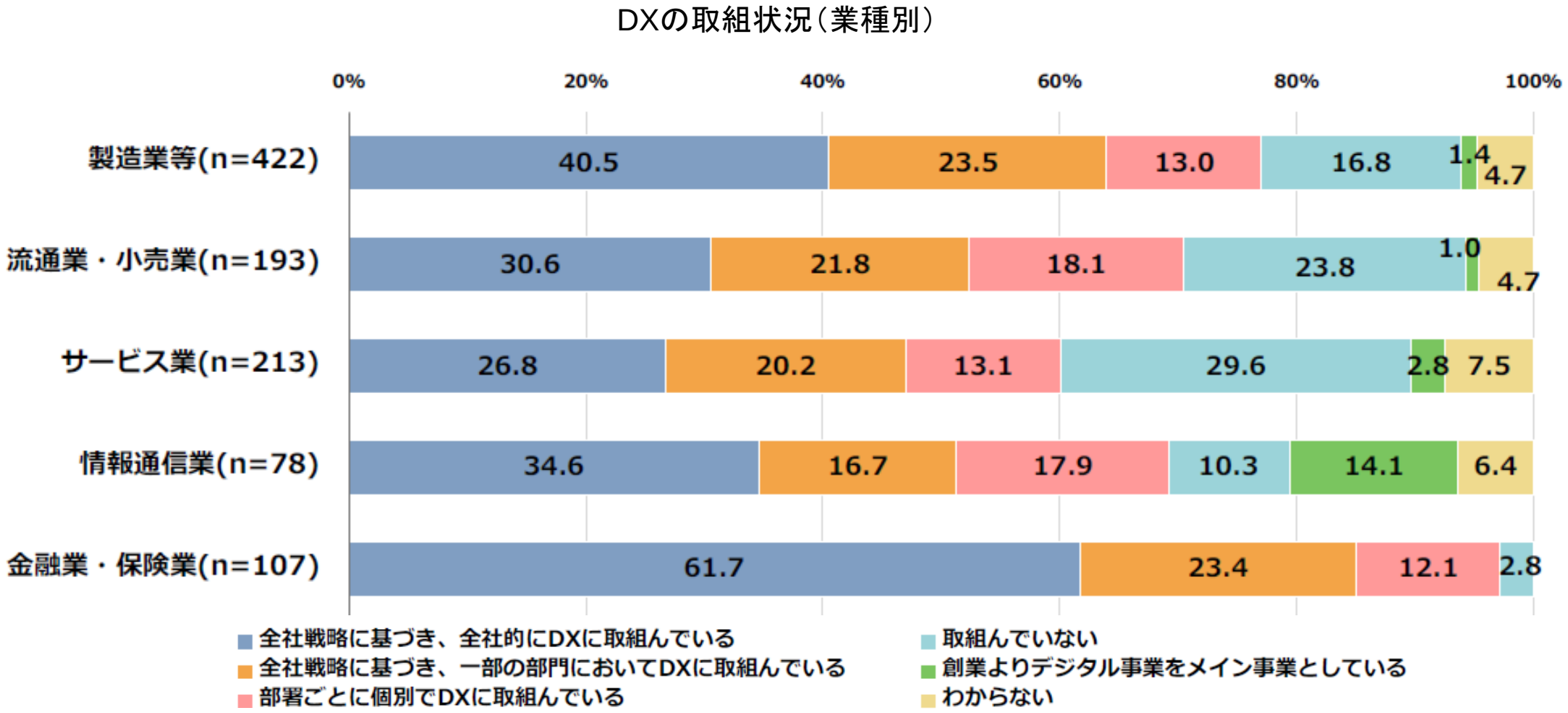
1. 今何が起きているのか
2. セキュリティ監査現場の課題
3. ソリューションとなりうる技術要素
4. セキュリティ監査の自動化
5. 将来に向けて

1

今何が起きているのか

デジタル活用は日常かつ戦略アジェンダ

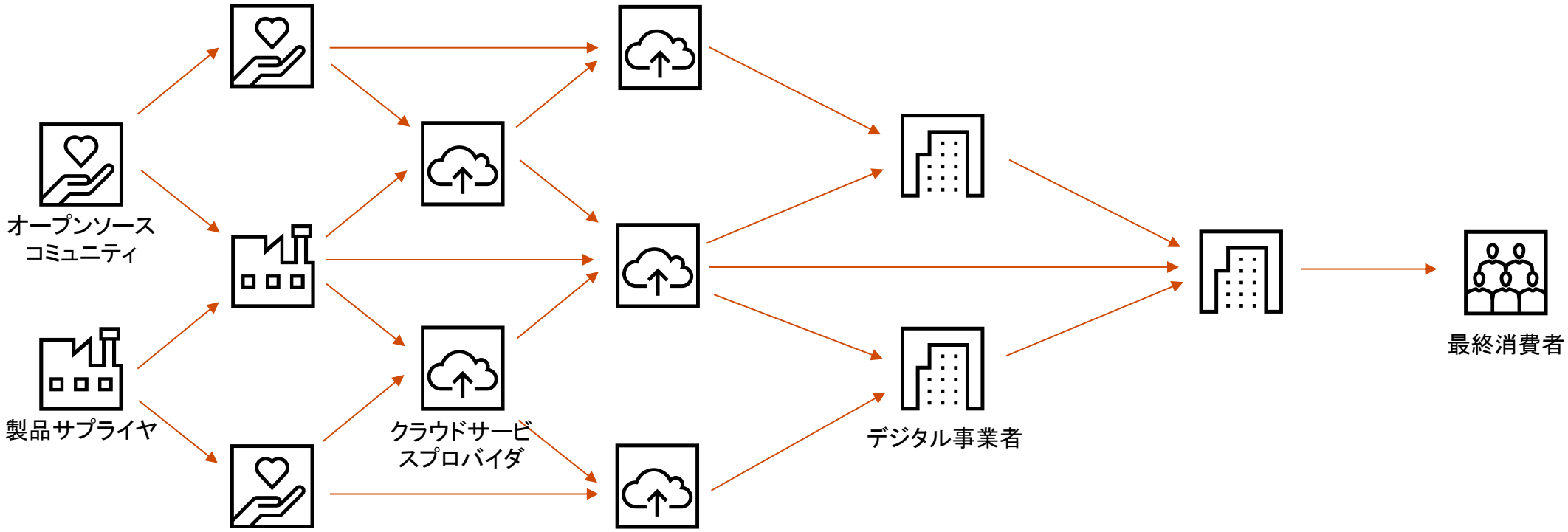
多くの組織がデジタルトランスフォーメンションを推進しています。



Source : 情報処理推進機構 DX動向2024

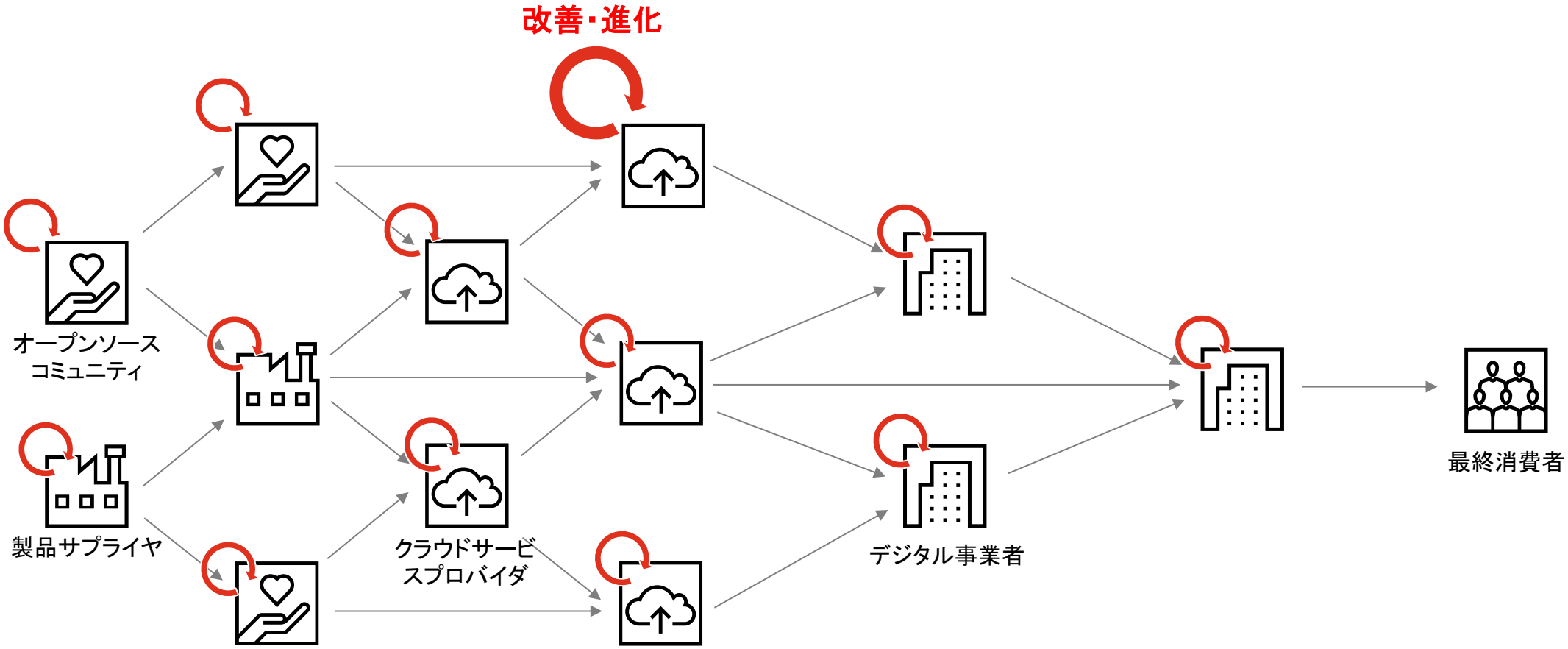
デジタルサービスのサプライチェーン

最終消費者に向けてデジタルサービスがつらなっています。



デジタルサービスの素早い進化は連なっている

ソフトウェアサプライチェーンの特徴として、それぞれがスピード感を持って改善・進化した結果が素早く連鎖します。



デジタルサービスの改善・進化は早い

毎週、毎日の改善が行われています。

小売（EC）
50 万/年

消費財
3 回/日

SaaS
16 回/月

航空
20 回/日

Source : 公開情報を基に作成

デジタル活用に伴うセキュリティリスク

インシデントが発生し続けています。

ネットワーク製品

ファイアウォール管理インターフェイスにおける重大な脆弱性が悪用され、認証回避やルート権限でのコマンド実行、機密情報を狙う攻撃が確認された。

セキュリティ製品

重大な欠陥を見過ごしたままソフトを更新し配付。ユーザー端末が影響を受けた。この障害により、世界中の航空会社のフライトの欠航、一部の銀行システムへのアクセス遮断、大規模医療ネットワークの障害、といった影響が発生した。

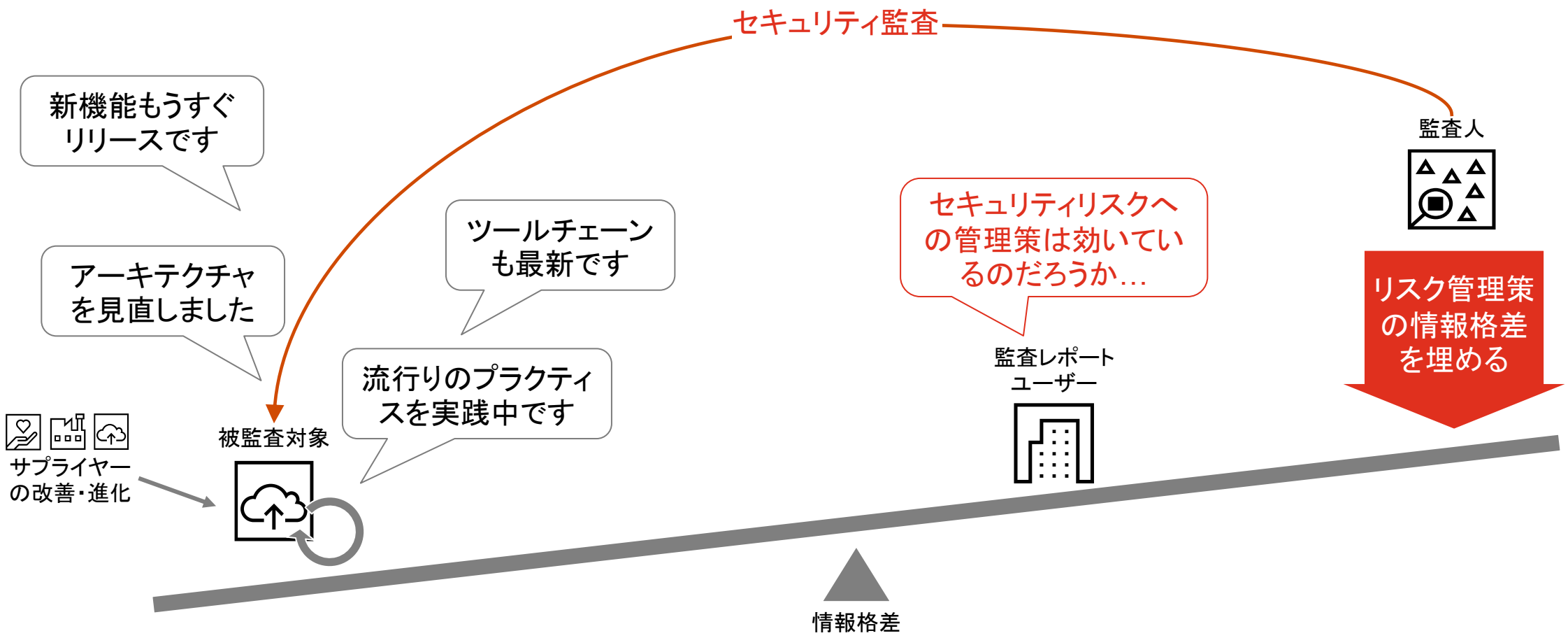
ネットサービス

特定のサーバーに異常な高負荷が確認されサービス停止。当該サーバを切り離してサービスを再開したところ、、別のサーバーに同様の高負荷が発生し、再びサービス停止。原因はマルウェア感染であった。

Source : 公開情報を基に作成

セキュリティ監査の役割は拡大

改善・進化し続けるデジタルサービスへの安心に向けて、セキュリティ監査の役割は拡大しています



セキュリティ監査等の市場規模は拡大中

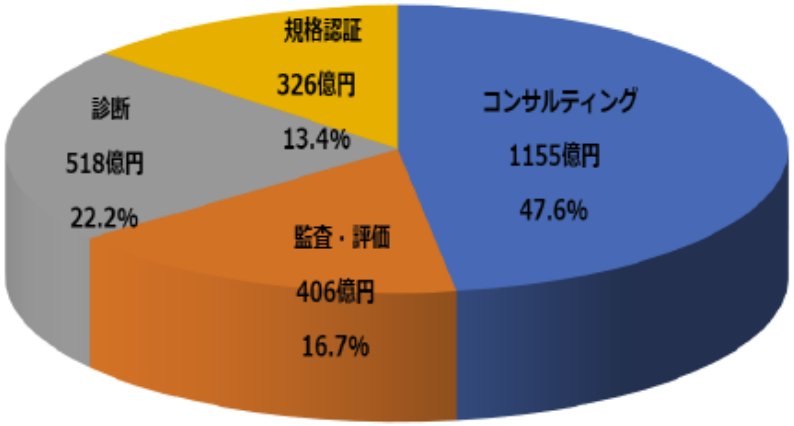
2022年度

２４２６億円

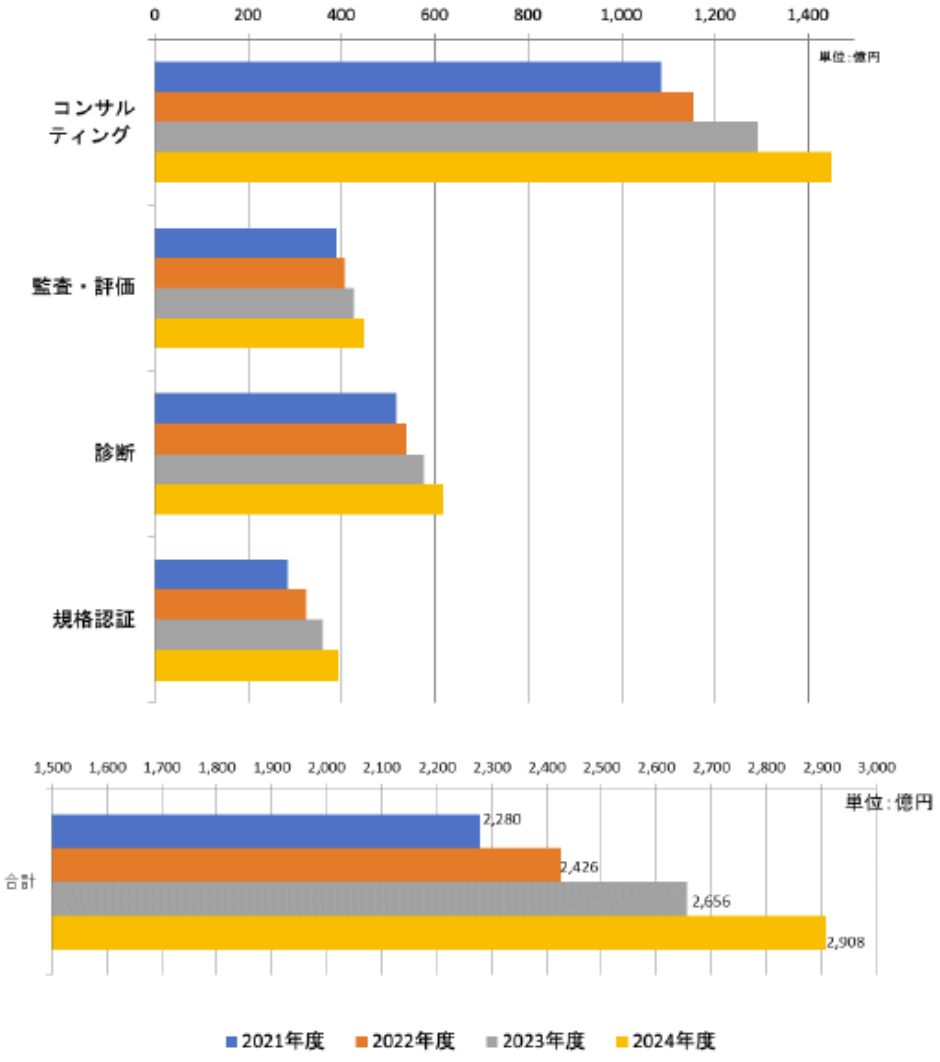
↑6.4%増

2021年度

２２８０億円



- ここ数年はコロナ禍を起因とするリモートワークへの切り替え需要によるコンサルティングサービス市場が拡大傾向にあり、2022年度はリモートワークだけの企業数は減少傾向にあったもののハイブリット型の勤務体制となる企業多かったことから、概ね昨年度までの流れからは変わらずに堅調な推移となった。
- 今後も本カテゴリは拡大傾向にあると思われるが、景気動向の影響が大きいカテゴリであり、情報セキュリティの重要性の認識は従来より高まっていることから、引き続き堅調な成長が見込まれる。



Source : 日本ネットワークセキュリティ協会 国内情報セキュリティ市場2023年度調査報告から引用

2

セキュリティ監査現場の課題

監査ターゲットは進化し続けている

技術進展に合わせてプロダクトそのものや実践手法、そしてセキュリティ管理策が進化・変化し続けています。

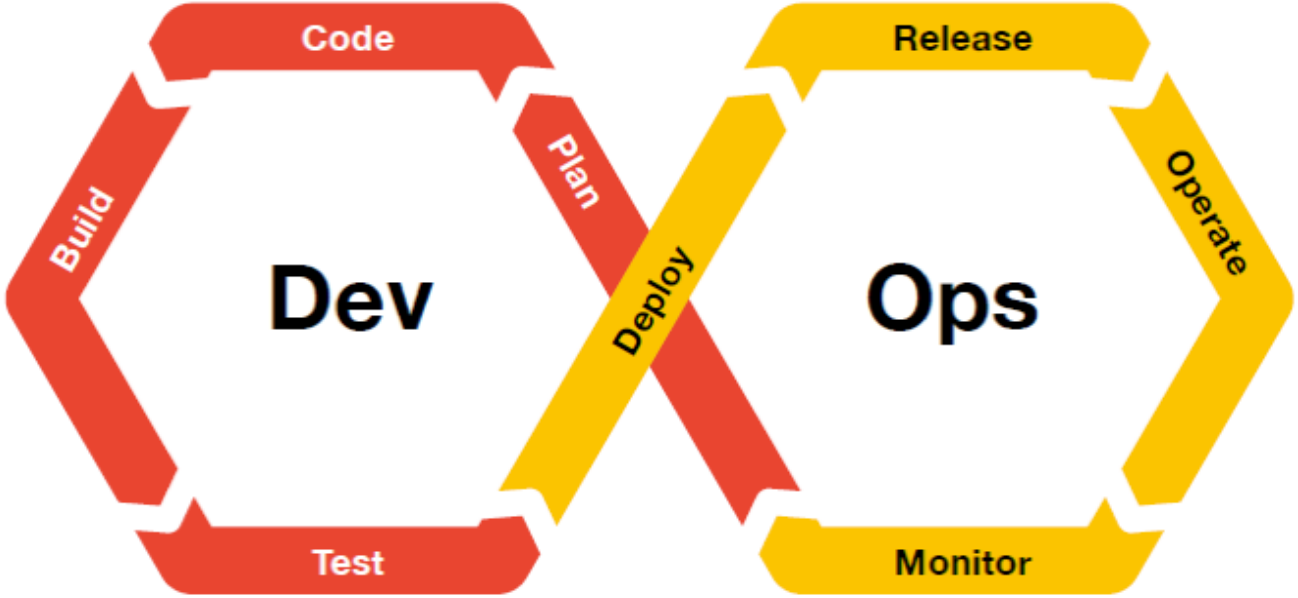
クラウドネイティブ	マイクロサービス	コンテナオーケストレーション
Infrastructure as Code（IaC）	イミュータブルインフラ	SRE
DevOps | DevSecOps	CI/CD	オブザーバビリティ
ゼロトラストアーキテクチャ	シフトレフト	Policy as Code
・・・		

監査ターゲットの進化 | DevOpsとは

実践手法やツールに留まらない、体制や組織文化も含む概念です。本講演では、関連の深い自動化周りに注目します。

- 定義
  ビジネスの価値をより確実かつ迅速にエンドユーザーへと届け続けるために、開発チームと運用チームが協調してソフトウェアサービス／システムを開発する環境やプロセス、組織文化
- 特徴
  - 自動化されたパイプライン
  - 継続的インテグレーション／デプロイメント
  - 高速で信頼性の高い自動テスト
  - ローリスクリリースを支えるアーキテクチャ

  ・・・



Source :Gene Kim, Jez Humble, Patrick Debois, John Willis, 2016. The DevOps HANDBOOKを参考に作成

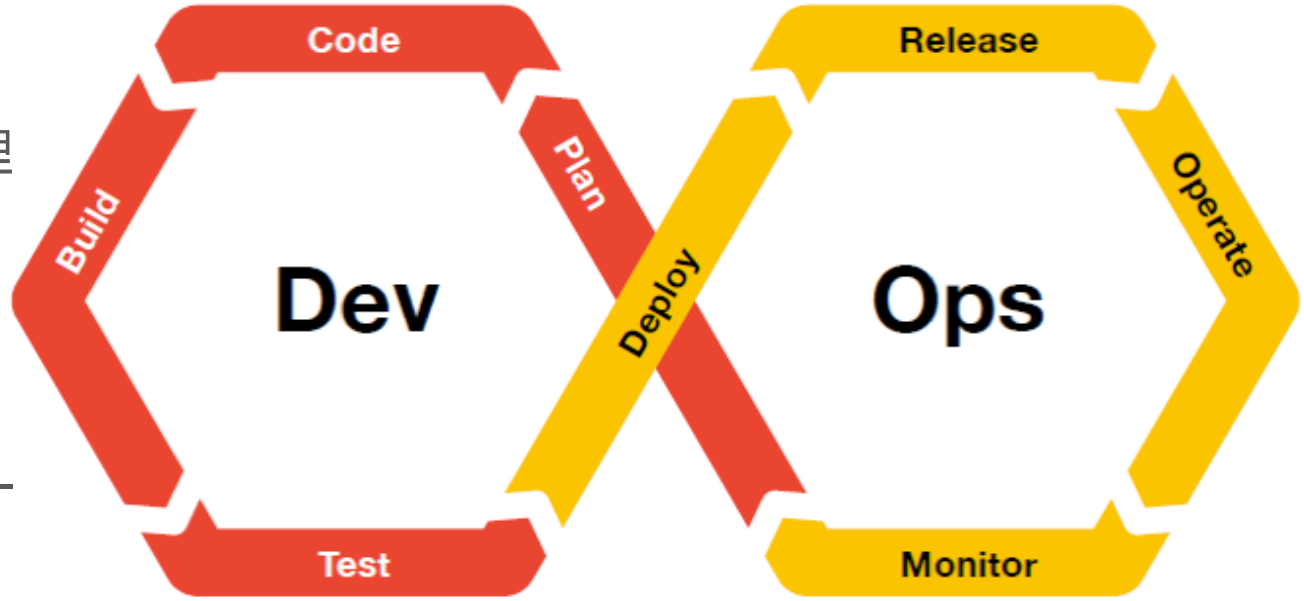
DevOps | ツールチェーンによる自動化

監査ターゲットはツールチェーン導入によって自動化されています。

パイプライン・CI/CD

構成・バージョン管理

チケットワークフロー



Infrastructure as Code

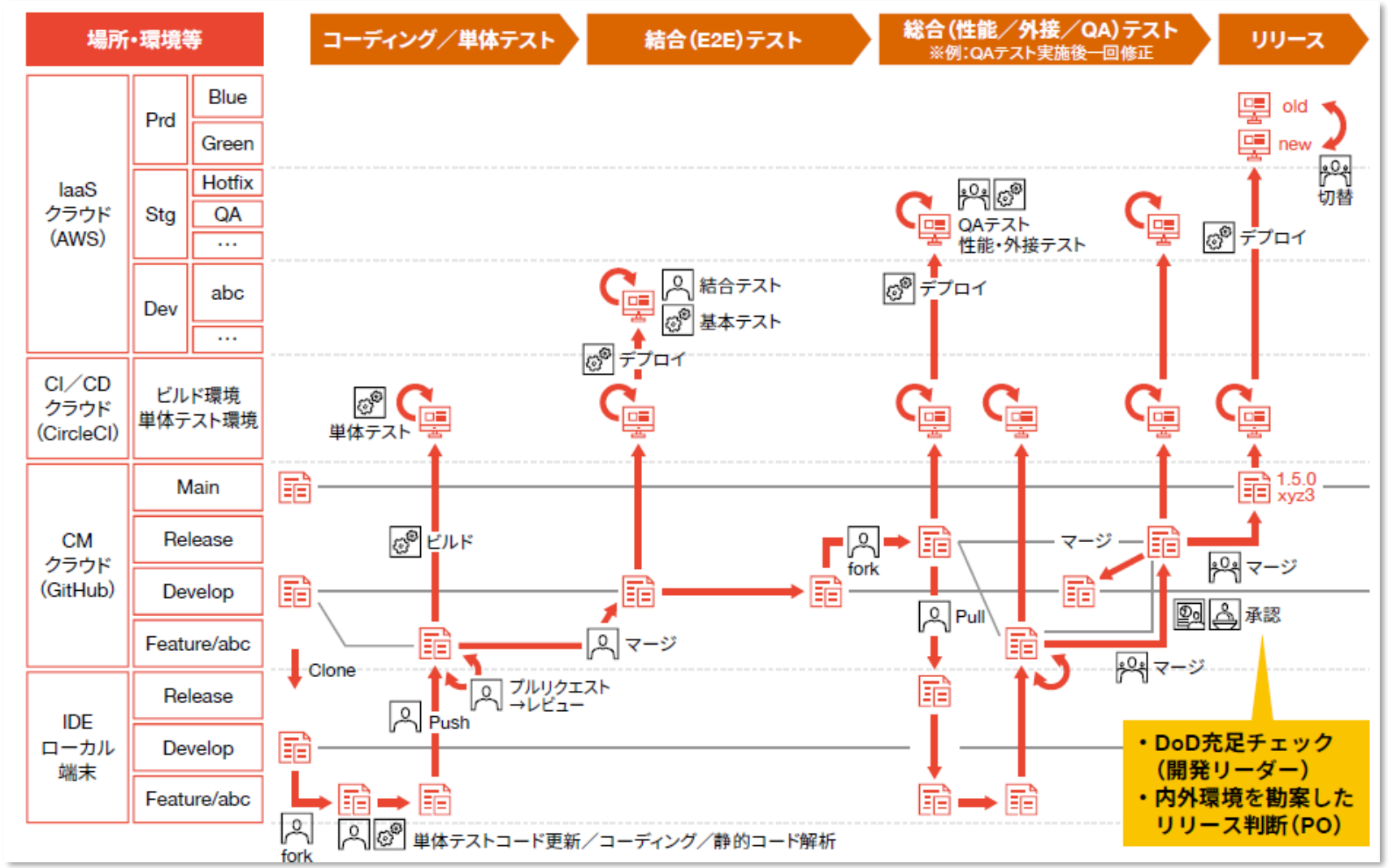
アクセス制御基盤

自動テストスイート

モニタリングツール

DevOps | ツールチェーンによる自動化（開発）

リリースまでの作業*の大部分がツールを介して行われます。



***一連の流れを「パイプライン」と呼称します**

Source: PwC https://www.pwc.com/jp/ja/knowledge/thoughtleadership/dev-ops220228.html

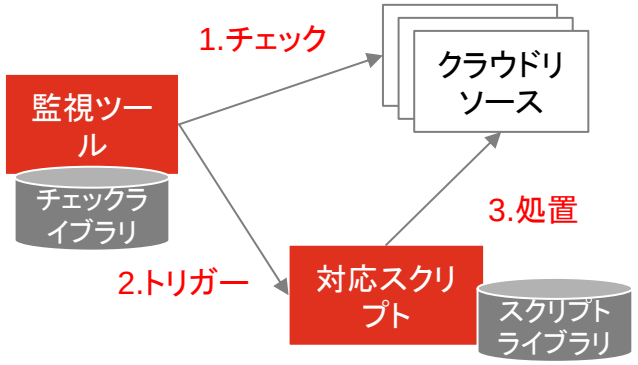
DevOps | ツールチェーンによる自動化（運用）

運用作業の大部分もツールによる自動化が行われます。

発見的統制（監視～臨時本番作業）

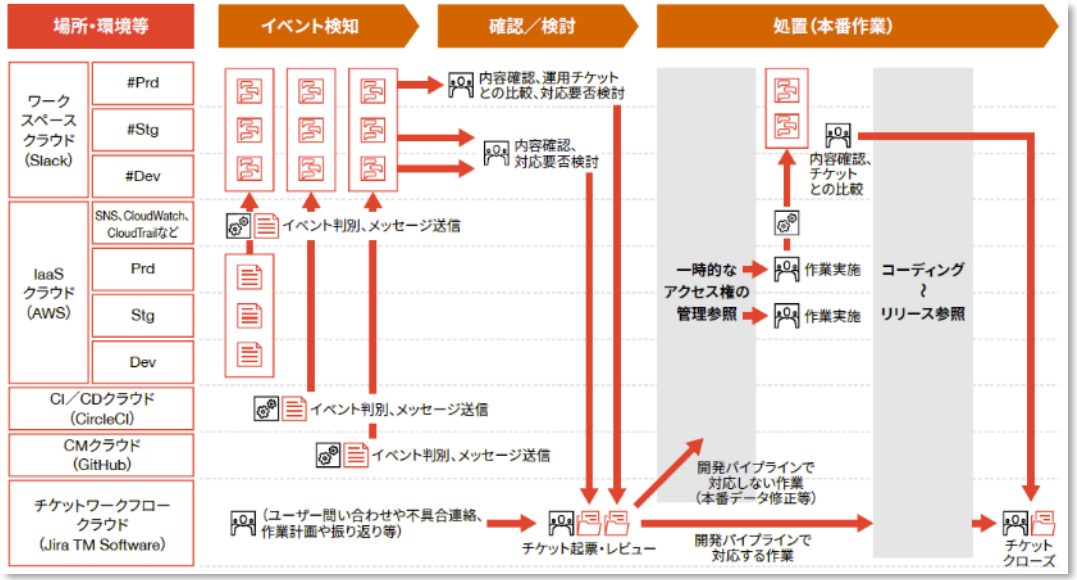
対応手順を想定できる事象

- 封じ込め、修正等の手順を予めスクリプト化し、イベント検知をトリガーに自動処置



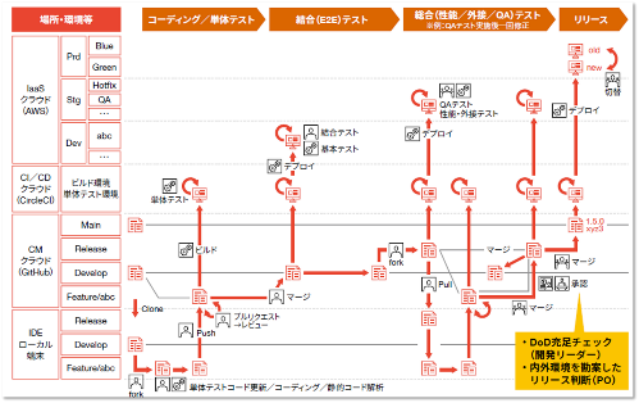
対応手順を想定できない事象

- 監視、修正等のコミュニケーションをCHATツール、チケットワークフロー上で行い、また対応スクリプトをパイプライン経由で実行する



計画作業

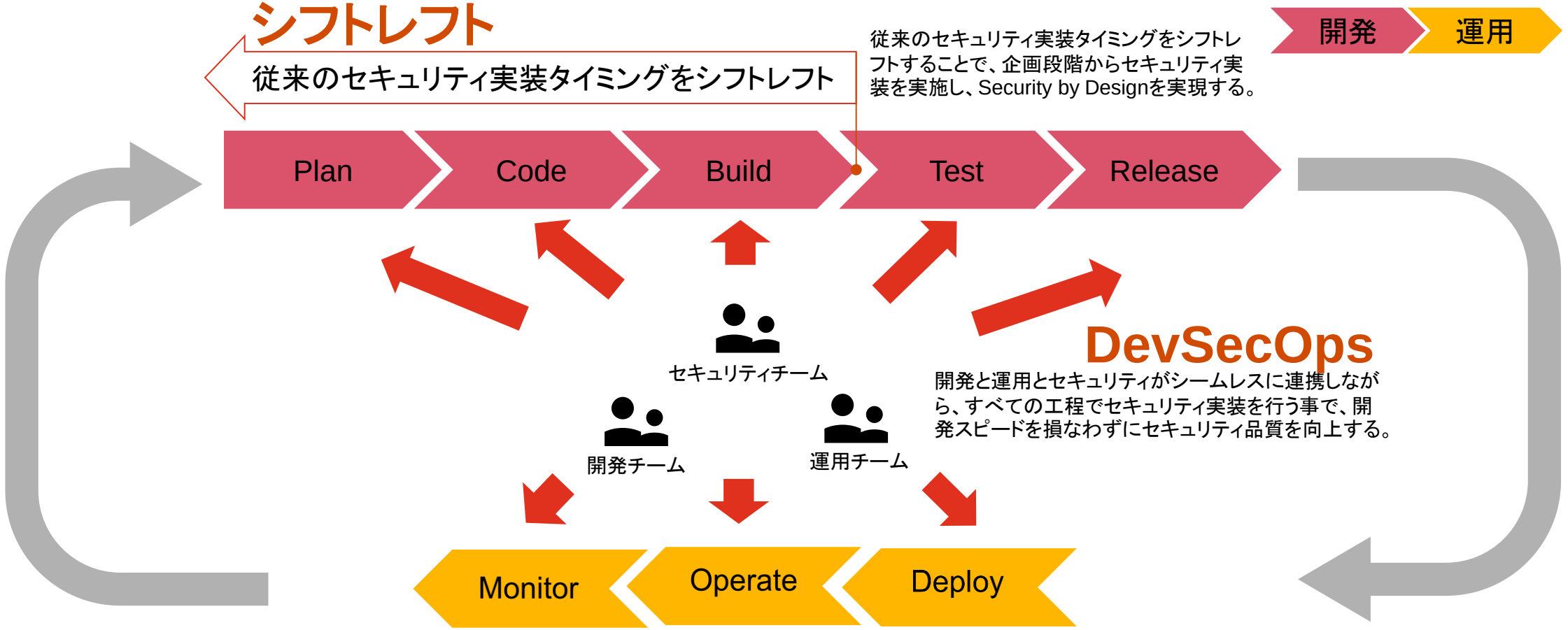
- IaC、つまりコードとして管理されているため、アプリケーション開発と同様のツールチェーンによる作業
- 本番環境に直接アクセスして更新することは原則しない。全てパイプライン経由で実行（レビューや承認）。



Source: PwC https://www.pwc.com/jp/ja/knowledge/thoughtleadership/dev-ops220228.html

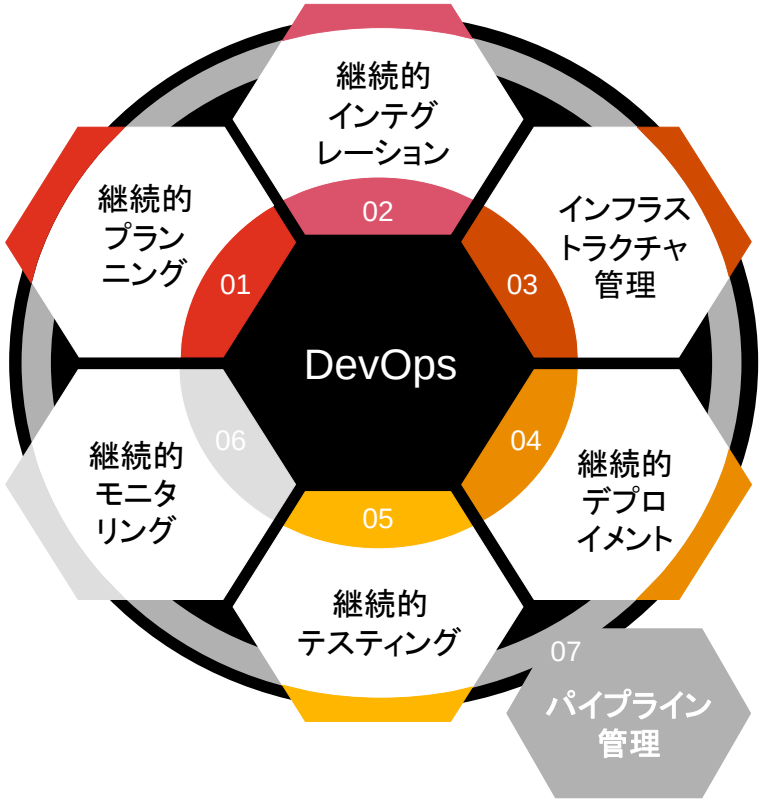
DevSecOps | セキュリティ管理策の埋め込み

自動化されたDevOps環境にセキュリティ管理策を埋め込むことで、スピードとセキュリティ品質を両立させます。



DevOps | セキュリティ管理策とのその他の関連個所

DevOpsのプラクティスとツールは、セキュリティ管理策の実装の新たな形となる可能性があります。



DevOps ドメイン		セキュリティドメイン	関連プラクティス / ツール	
01	継続的 プランニング	システム要件の一貫性	• 完了の定義（DoD） • ユーザストーリー受入基準	チケットワーク フロー
02	継続的インテグ レーション	コーディング品質の確保	• プルリクエスト • ソースコード解析	構成管理 SCA/SAST
03	インフラストラク チャ管理	インフラ構成の管理	• IaC • イミュータブルインフラ	IaC
04	継続的 デプロイメント	本番移行態勢の整備	• チケットとのリンケージ • Blue/Green デプロイメント	CD
05	継続的 テスティング	テストによる品質の確保	• 自動化されたテスト • テストスクリプト管理	Test Suite
06	継続的 モニタリング	障害復旧態勢の整備	• パフォーマンス監視 • カナリアリリース	APM CD
07	パイプライン 管理	開発と運用の分離 変更の受入・承認	• ソースコードアクセス管理 • パイプライン保護	CI/CD

監査ターゲットは進化し続けている（再掲）

進化・変化し続ける現場に、監査側もキャッチアップする必要があります。

クラウドネイティブ	マイクロサービス	コンテナオーケストレーション
Infrastructure as Code（IaC）	イミュータブルインフラ	SRE
DevOps | DevSecOps	CI/CD	オブザーバビリティ
ゼロトラストアーキテクチャ	シフトレフト	Policy as Code
・・・		

セキュリティ監査手続きのキャッチアップが必要なのは三割程度か

感覚的ですが、、、例えば、クラウドネイティブやDevOps、ゼロトラストを採用しデジタル化が進んだ組織の場合、ISO27001監査の3割程度に、監査手続き上の何らかのキャッチアップが必要と考えられます。

組織的管理策

5.1 情報セキュリティ方針群
5.2 役割及び責任
5.3 職務の分離
…
5.9 情報及びその他の資産の目録
…
5.12 情報の分類
5.13 情報のラベル付け
5.14 情報の転送
5.15 アクセス制御
5.16 識別情報の管理
5.17 認証情報
5.18 アクセス権
5.19供給者関係における情報セキュリティ
…

人的管理策

6.1 選考
6.2 雇用条件
6.3 意識向上，教育及び訓練
・・・
6.7 リモートワーク
・・・

物理的管理策

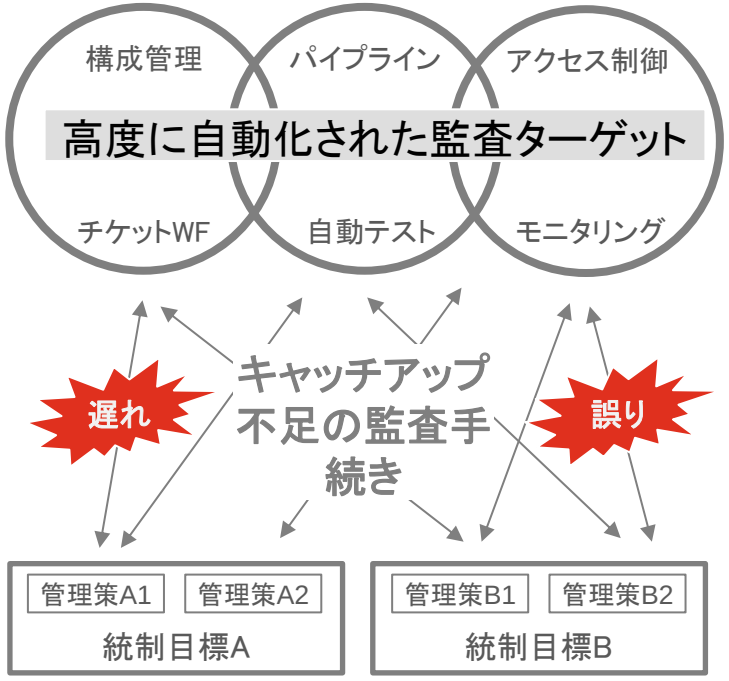
7.1 物理的セキュリティ境界
7.2 物理的入退
7.3 オフィス・部屋及び施設
・・・

技術的管理策

8.1 利用者エンドポイント機器
8.2 特権的アクセス権
8.3 情報へのアクセス制限
8.4 ソースコードへのアクセス
8.5 セキュリティを保った認証
8.6 容量・能力の管理
8.7 マルウェアに対する保護
8.8 技術的ぜい弱性の管理
8.9 構成管理
8.10 情報の削除
8.11 データマスキング
8.12 データ漏えい防止
8.13 情報のバックアップ
8.14 情報処理施設・設備の冗長性
・・・

セキュリティ監査手続きのキャッチアップ不足が招く不幸

コストは高止まり、スピードも確保できない結果はユーザーに跳ね返ります。



被監査対象

- 監査対応コスト増
- 改善・進化スピードの阻害

監査人

- 監査コスト増
- 監査期間増

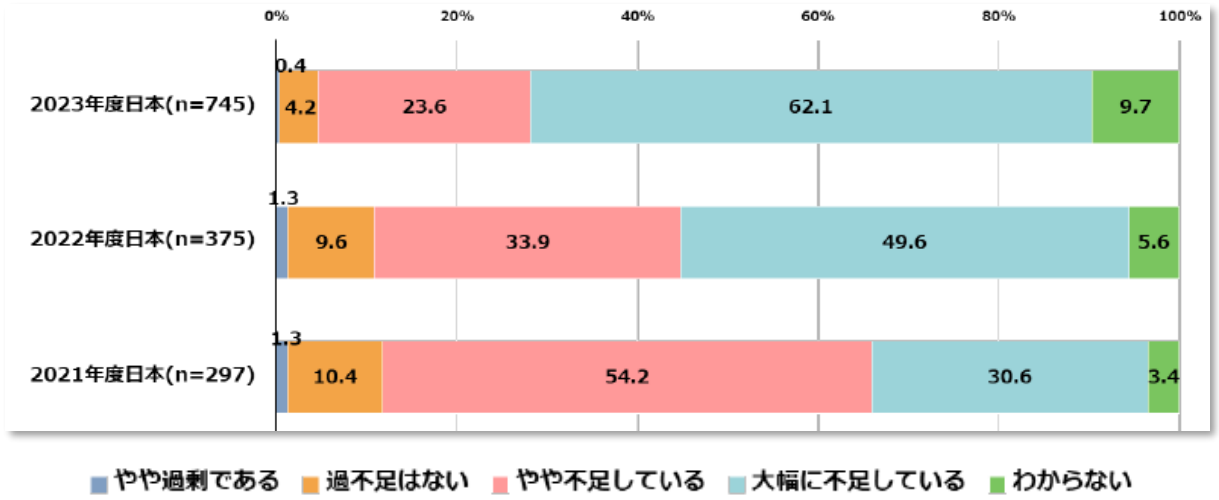
監査レポート
ユーザー

- サービス（監査ターゲット）利用料の増加
- サービス改善・進化の便益享受の遅れ（利用承認が下りない、リスクを感じるので利用しない）

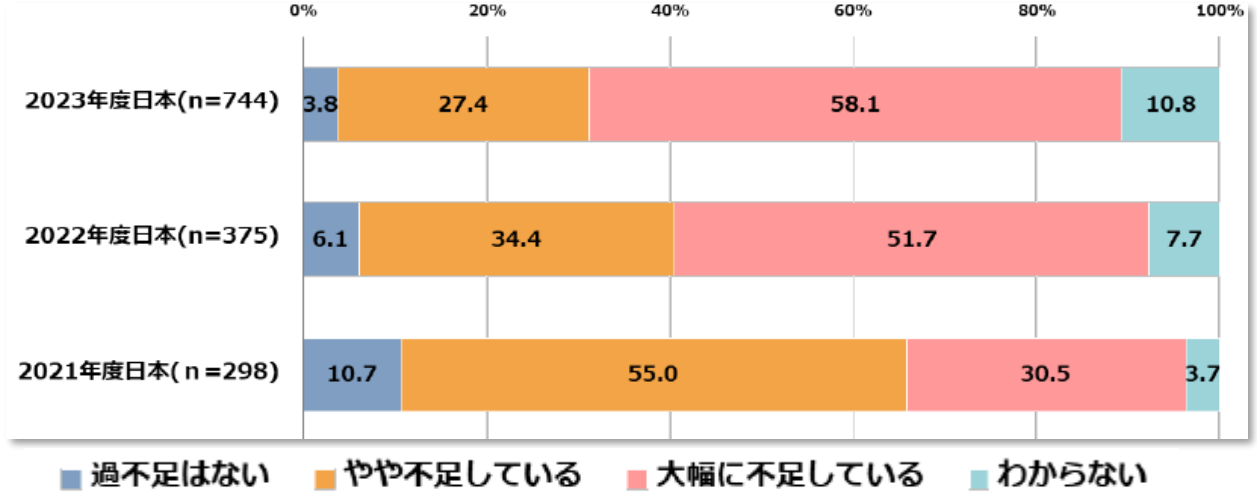
人材の外部調達は難しい...

ケイパビリティのある人間の投入を模索するも、そもそも日本全体で不足している状態です

DX推進人材の「量」の確保



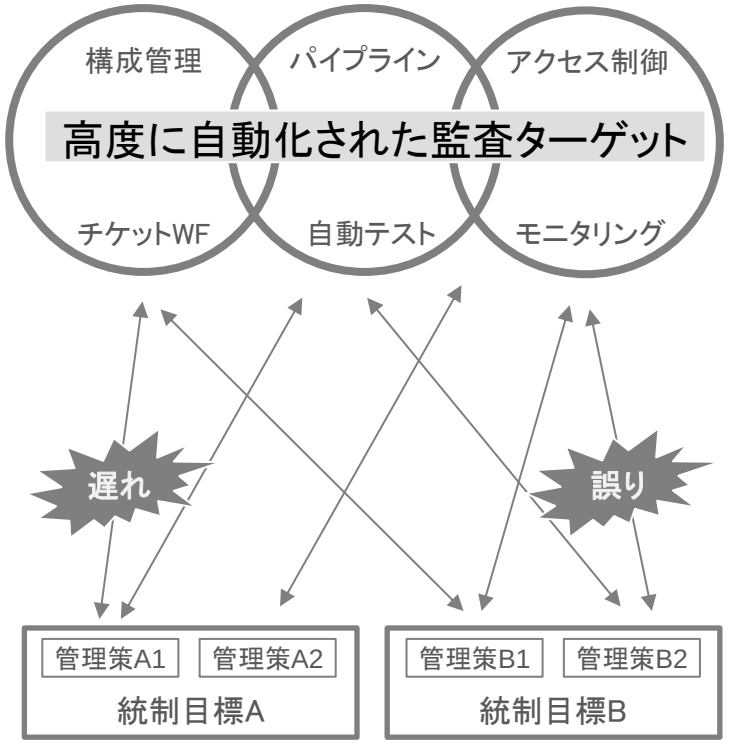
DX推進人材の「質」の確保

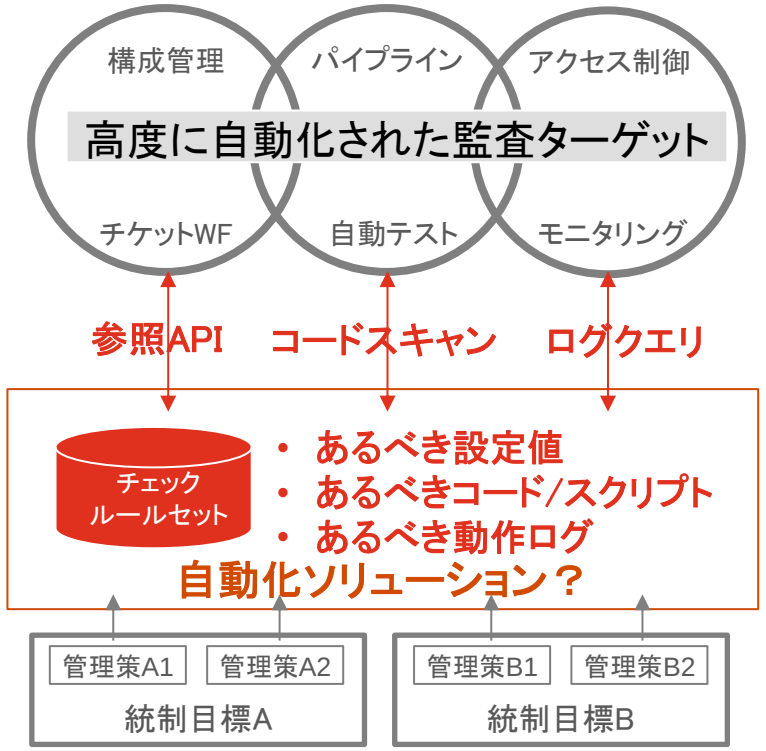


Source : 情報処理推進機能DX動向2024

監査ターゲットが自動化されているなら、監査自体も自動化

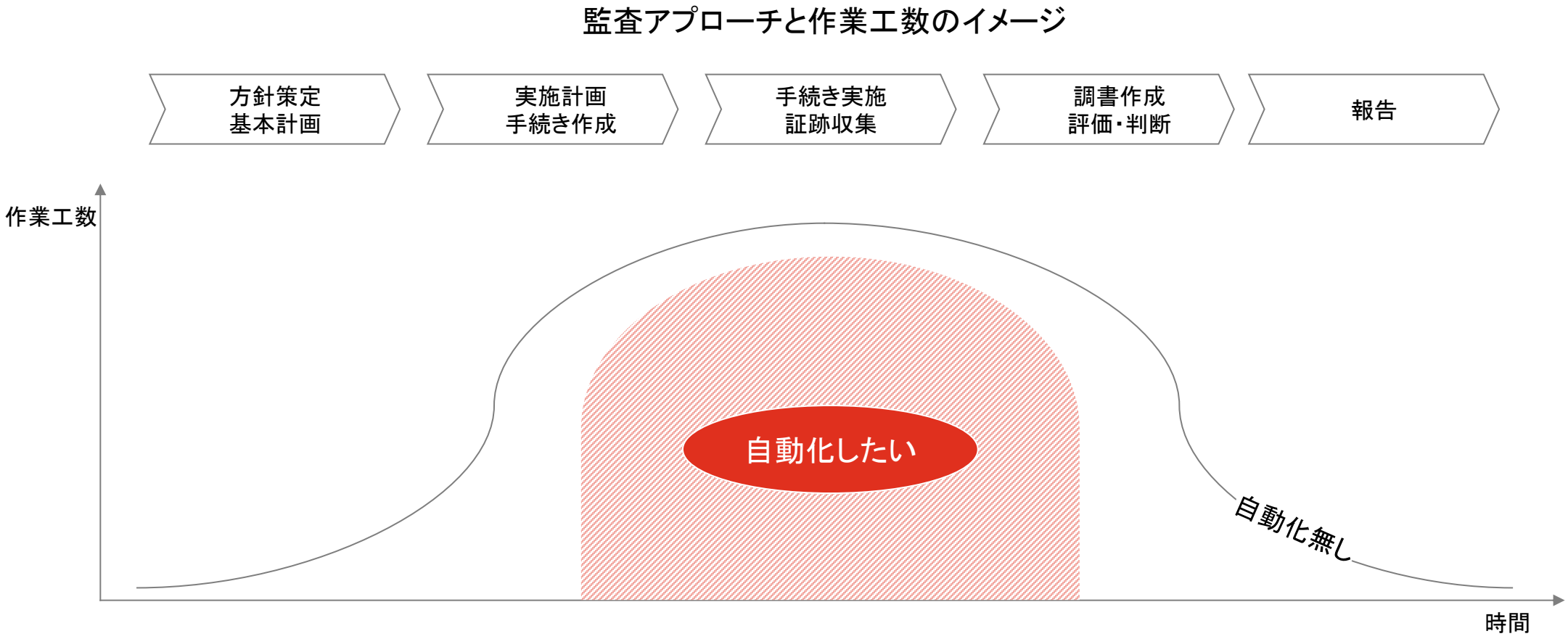
ツールチェーンの設定値や動作ログを機械が検証することで自動化できると考えられます





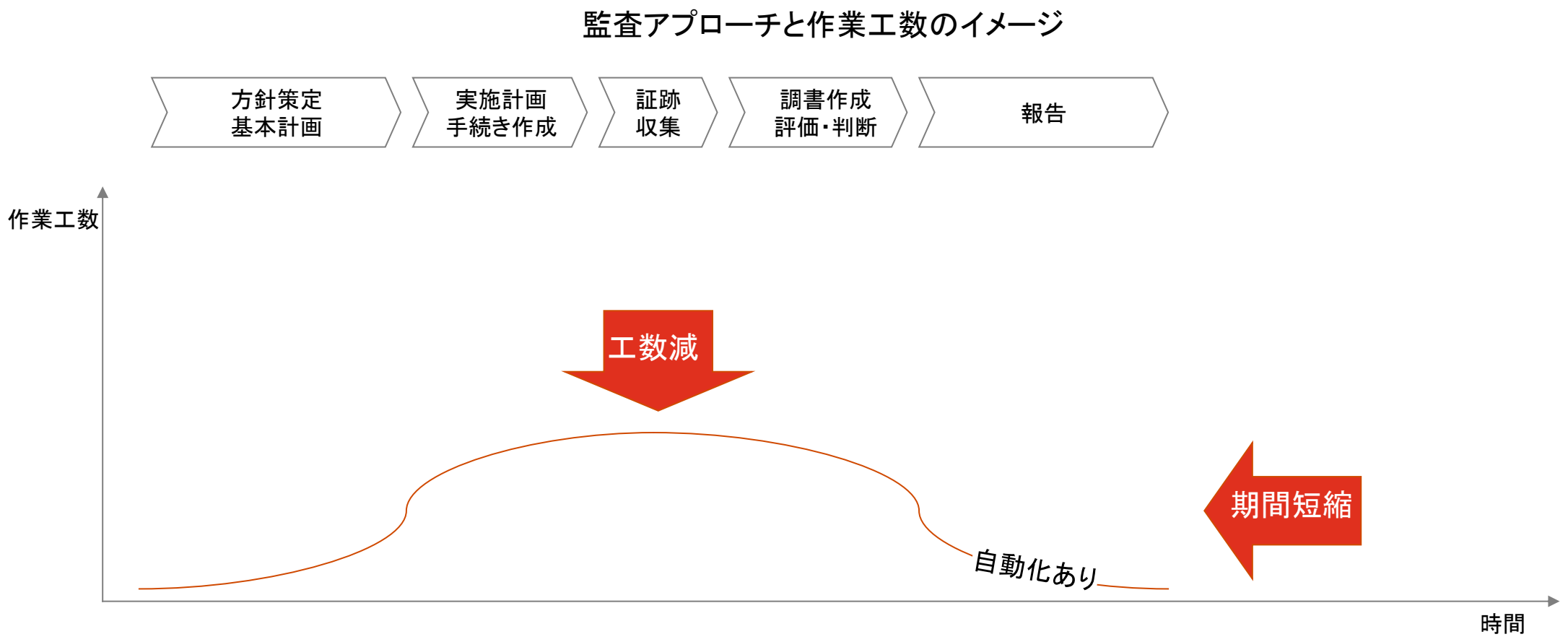
作業レベルの活動を自動化したい

機械が作業を行い、人間は判断のみを行う形が理想ではないでしょうか



作業工数が削減、監査期間も短縮

作業レベルの活動が自動化できれば、総工数も削減され、監査期間も短縮されるはずです。



自動化検討のコンテキスト整理

監査対応側
（サービスの提供者等）

- 新機能を素早くリリースしユーザーに届けたい
- 最新のプラクティス、ツールを積極採用し自動化している

監査実施側

- 従前の監査手続きの一部は再利用できず工数がかかる
- 手続きキャッチアップや判断に人間の工数を使い、作業レベルは機械に任せたい

結果報告のユーザー
（サービスの利用者等）

- 新機能をすぐに利用したい。利用料も安い方がよい
- 監査報告等がないと利用承認が下りない、リスクを感じるので利用しない

3

ソリューション候補

ソリューション候補

運用状況の評価に向けては、各ツールが提供する監査ログやセキュリティデータレイク/SIEM製品がキーとなりますが、ログに対するクエリ実行が主体であり自動化文脈からそれる（より広く、モダン化の文脈になる）要素もあるため本講演では割愛します。

セキュリティ監査の自動化に向けて活用できる技術要素が揃ってきています。

CSPM / CNAPP

クラウド上のインフラストラクチャやアプリケーション、およびアプリケーションライフサイクルをスキャンし、定義されたルールへの違反を検出します。公知のセキュリティガイドラインに対応したルールセットを持つ製品が多く存在します。

セキュリティ監査自動化文脈では手続きの実施、証跡収集を中心に活用します。

GRCツール

機能部門別に行っていた、ガバナンス、リスク、コンプライアンス関連活動の業務負担や複雑化傾向への対応に向けて、組織全体で一気通貫な統合管理を行うための支援ツールです。

セキュリティ監査自動化文脈では、規程や言明の記述管理や監査プロジェクトの管理に活用します。

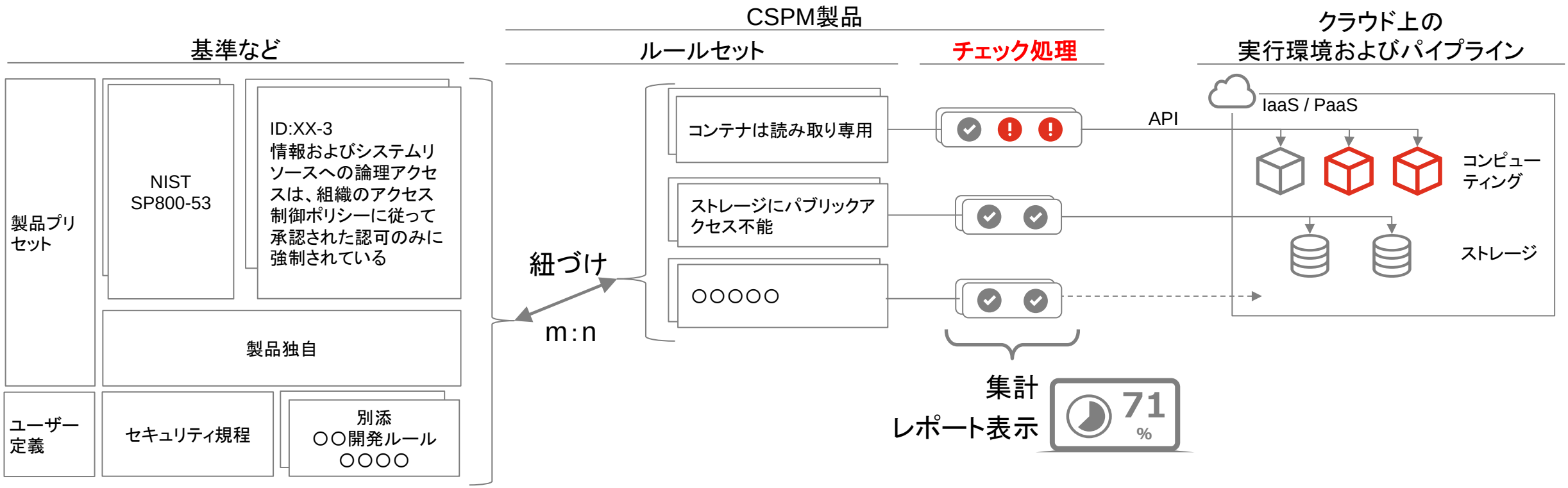
OSCAL

特定のシステムに対するセキュリティ管理策の実装状況の言明、評価計画、評価結果や、セキュリティ管理策のカタログを記述する様式を、機械可読可能な形式で定めた記述言語です。

セキュリティ監査自動化に向けて、機械と人間の橋渡しが期待できます。

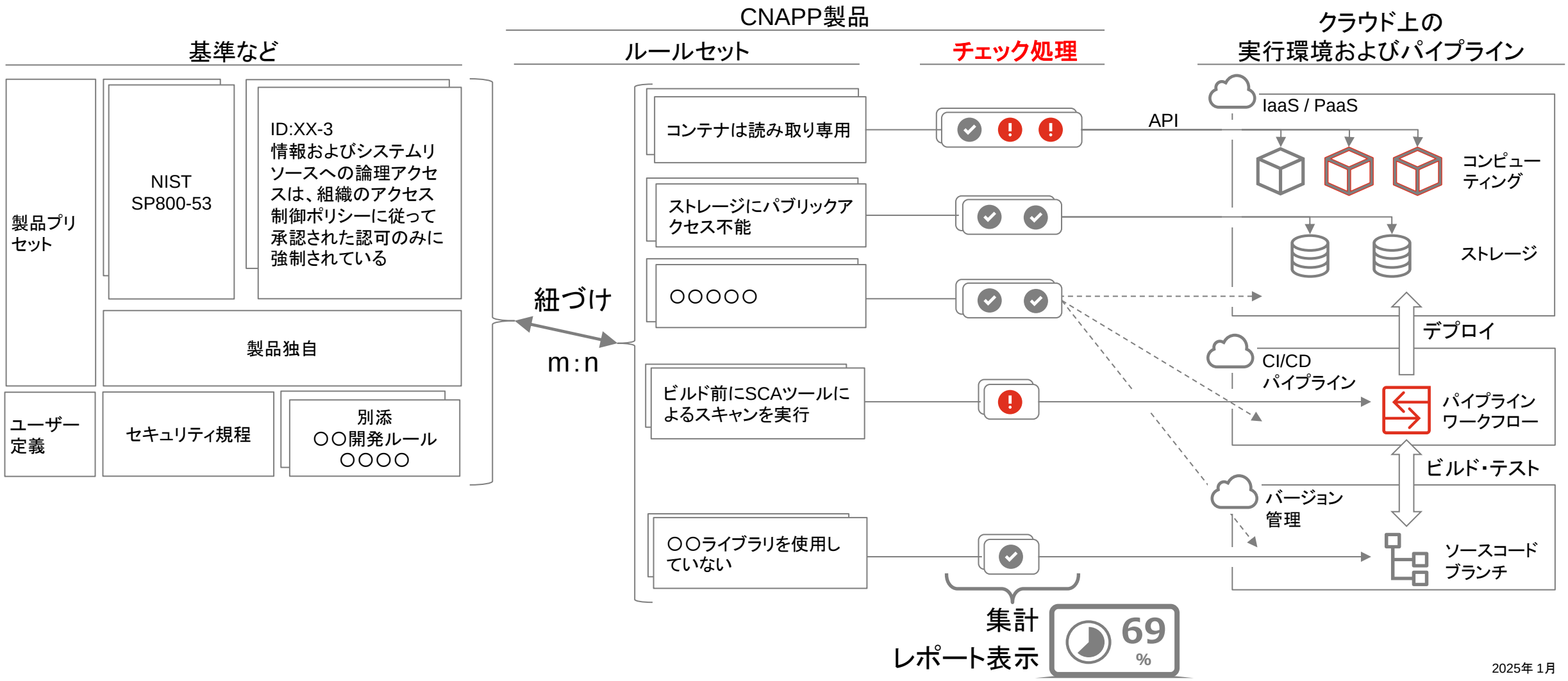
Cloud Security Posture Management（CSPM）

クラウド上のインフラストラクチャを中心にスキャンし、ルール違反をチェックします。



Cloud Native Application Protection Platform（CNAPP）

CSPMのカバー範囲にアプリケーションのビルドやデプロイも加えて、ライフサイクル全体をチェックします。

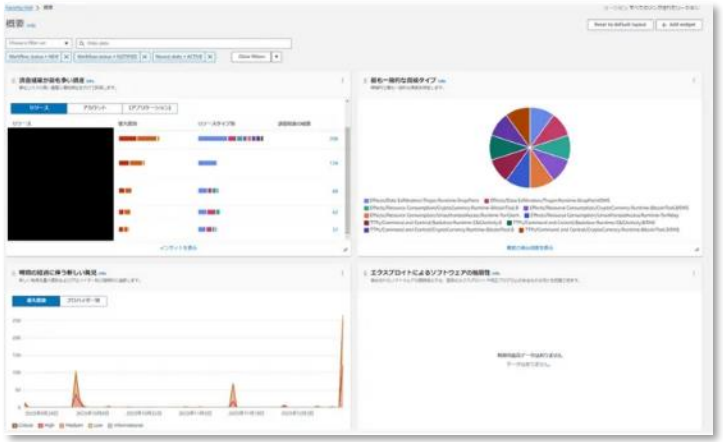


IaaS/PaaSプロバイダーの提供サービス

セキュリティ監査の自動化に活用可能なチェック処理やルールセットを提供しています。

AWS
Security Hub / Conformance Packs for Config

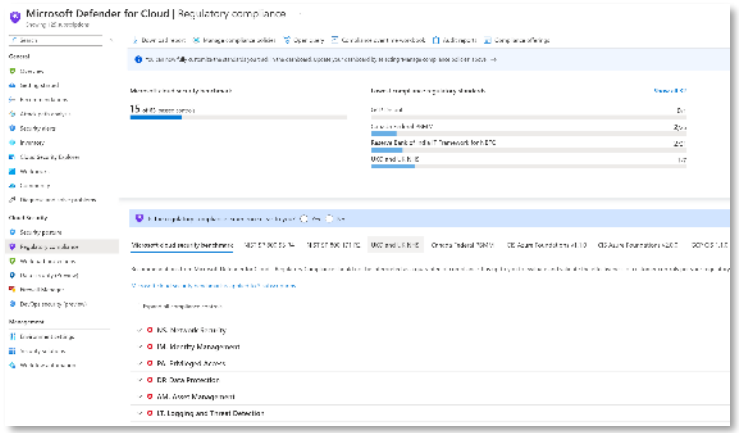
AWS Security Hub を使用すると、セキュリティのベストプラクティスのチェックを自動化し、セキュリティアラートを単一の場所と形式に集約し、すべての AWS アカウントで全体的なセキュリティの体制を把握することができます。
コンフォーマンスパックは、カスタム Config ルール等を使用したセキュリティチェック等の向けの汎用コンプライアンスフレームワークを提供します。



ルールセット例
- CIS Benchmark
- HIPAA
- NIST CSF
- NIST SP800-53
- PCI DSS
- FedRAMP

Azure
MS Defender for Cloud / Policy

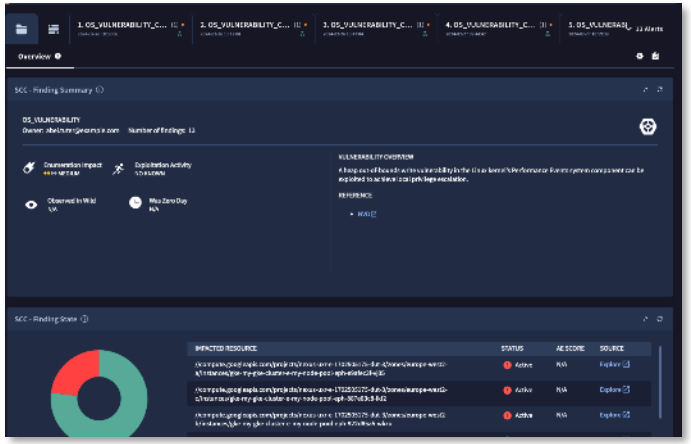
Microsoft Defender for Cloud はCNAPPであり、さまざまなサイバー脅威や脆弱性からクラウドベースのアプリケーションを保護するように設計されたセキュリティ対策とプラクティスから構成されています。
Azure Policy は、組織の標準を適用し、コンプライアンスを大規模に評価するのに役立ちます。コンプライアンス ダッシュボードを通じて、環境の全体的な状態を評価するための集計ビューを提供します



ルールセット例
- CIS Benchmark
- HIPAA
- ISO27001
- NIST SP800-53
- PCI DSS
- FedRAMP

Google Cloud
Security Command Center / Assured Workloads

Security Command Center は、さまざまなセキュリティ標準のコントロールにマッピングされた検出機能でコンプライアンスをモニタリングします。
Assured Workloads によって、Google Cloud ユーザーは規制、リージョン、主権の要件をサポートするためにコントロールを適用できます。



ルールセット例
- CIS Controls
- HIPAA
- ISO27001
- NIST SP800-53
- NIST CSF
- FedRAMP

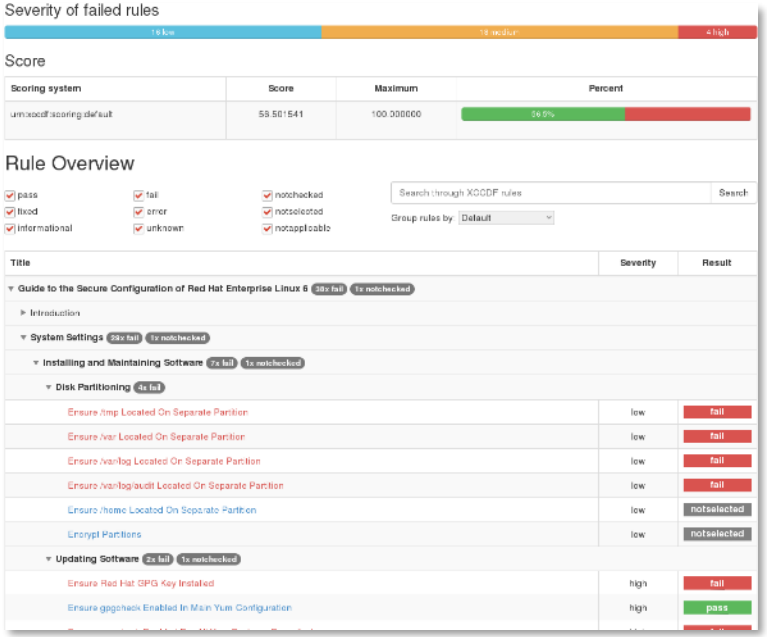
Source : https://aws.amazon.com/jp/security-hub/ 、https://docs.aws.amazon.com/config/ 、https://learn.microsoft.com/ja-jp/azure/defender-for-cloud/ 、https://learn.microsoft.com/en-us/azure/governance/policy/、および https://cloud.google.com/security-command-center/、https://cloud.google.com/security/products/assured-workloads を基に作成。また、PwCは、アマゾンウェブサービス（AWS）、マイクロソフト、Google Cloudとアライアンスを組んでいます。https://www.pwc.com/jp/ja/services/alliances.html

オープンソースソフトウェアも存在

セキュリティ監査の自動化に活用可能なチェック処理やルールセットを持ちます。

OpenSCAP
Audit, Fix and be Merry

NISTのSecurity Content Automation Protocol（セキュリティコンテンツ自動化規約。通称SCAP）で記述されたチェックリスト使用して、**対象リソースへスキャン**を行う。PCI-DSSやUSGCB（米国連邦政府機関が広く導入するIT製品向けのハードニング基準）に対応する**OS設定等がSCAPで公開**されている。



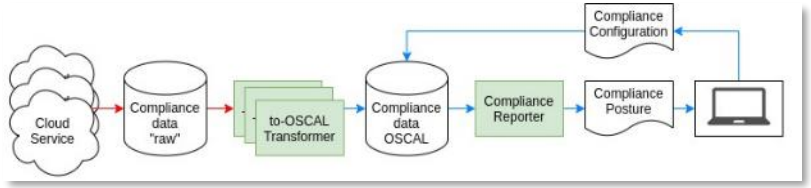
Gatekeeper

Kubernetes等で広く使用されているポリシーエンジンのOpen Policy Agentを使用して、Kubernetesクラスター向けの**ポリシーを定義し適用**できる。クラスター上のリソース以外に、IaCに対してもコミット時に**チェックを行える**。ユーザーがポリシーを作成する必要があるが、**ベストプラクティスがコミュニティ上で別途公開**・更新されている。


```
{
  "level": "info",
  "ts": 1632889070.3075402,
  "logger": "controller",
  "msg": "container <kube-scheduler> has no resource limits",
  "process": "audit",
  "audit_id": "2021-09-29T04:17:47Z",
  "event_type": "violation_audited",
  "constraint_group": "constraints.gatekeeper.sh",
  "constraint_api_version": "v1beta1",
  "constraint_kind": "K8sContainerLimits",
  "constraint_name": "container-must-have-limits",
  "constraint_namespace": "",
  "constraint_action": "deny",
  "constraint_enforcement_actions": [],
  "constraint_annotations": {
    "test-annotation-1": "annotation_1"
  },
…
```


Compliance-trestle

NISTのOSCAL（セキュリティ統制記述言語。後述）を活用した、**コンプライアンス成果物の作成、検証、管理**用ツール。統制記述と設定値の橋渡しをGitワークフローで行える。開発者に使いやすく、またコンプライアンスに関する利害関係者らに透明性が確保される。また例えば、CIS Benchmarkを具体製品設定のOSCAL記述への**変換ロジックが別コミュニティ上で公開**されている。




```
{
  "uuid": "18c61fb2-8603-440d-9d9a-8d6d1e232cd3",
  "control-id": "CIS-1.1.2",
  "description": "Ensure that the API server pod specification file
  "props": [
    {
      "name": "XCCDF_rule",
      "ns": "https://oscal-compass.github.io/compliance-trestle/sch
      "value": "xccdf_org.ssgproject.content_rule_file_groupowner_k
      "class": "scc_goal_name_id",
      "remarks": "Verify Group Who Owns The Kubernetes API Server P
```


Source : https://www.open-scap.org/ 、https://open-policy-agent.github.io/gatekeeper/ および https://oscal-compass.github.io/compliance-trestle/ を基に作成

Open SCAPは米国立標準技術研究所（NIST）の認定を受けたオープンソースプロジェクトです。Gatekeeperを含むOpen Policy AgentおよびCompliance-trestleは非営利団体であるCloud Native Computing Foundationのオープンソースプロジェクトです。

Governance Risk Compliance（GRC）ツール

複数のモジュールから構成される統合型プラットフォーム製品では、セキュリティに関する規程の記述管理や、監査プロジェクトの管理も行えます。

統合型プラットフォーム製品の機能モジュール例

セキュリティ監査自動化文脈で活用が見込まれるモジュール

ポリシー管理
- 企業内のポリシーを集中管理
- 法令、ガイドライン、社内規定、各種業務手順を体系化。
- 法令と社内ルール、ポリシー改訂等の自動化。

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。
- 検出事項の識別、改善計画の管理。

リスク管理
- 企業が認識するリスクに対して、リスクアセスメントの実施、リスク対応計画の策定、リスク対応の進捗状況や有効性評価などの一連の流れを管理。

インシデント管理
- 日常的に発生した障害や、サイバー攻撃の記録を取得し、発生したインシデントの分析や改善事項を管理。（インシデントの特定、インシデントの評価、調査状況の管理、インシデントの解決、インシデント傾向のレポートなど）。

ビジネス継続管理
- 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、迅速な対応をサポート。
- 事業継続計画・災害復旧計画の文書化、計画の有効性の測定等、BCP活動を支援。（事業影響度分析、事業継続計画の文書化、災害復旧計画の文書化、計画の有効性を検証、危機となるイベントを追跡、計画のメンテナンスを自動化）

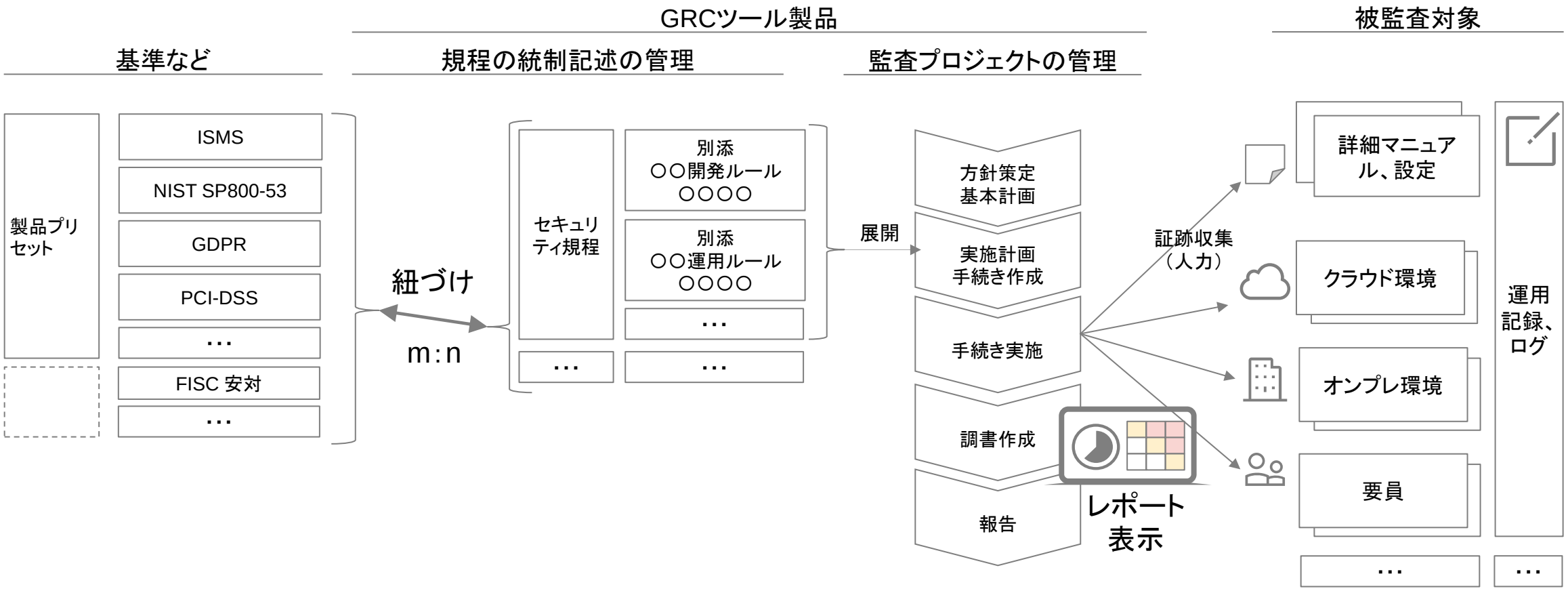
委託先管理
- 委託先企業のデータを集中的に管理し、委託先企業のリスク評価や規程類、法令、ガイドラインへの準拠状況と関連性を明確化。

監査管理
- 監査計画の策定から監査手続の実施、監査結果の報告プロセスについて、リソース管理、監査手続書の作成サポート、報告書のテンプレート等を管理。

ITオペレーショナルリスク管理
- セキュリティ監視機器から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等を実施。
- 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。

Governance Risk Compliance（GRC）ツール

セキュリティに関する規程の記述管理や、監査プロジェクトの管理が行えます。



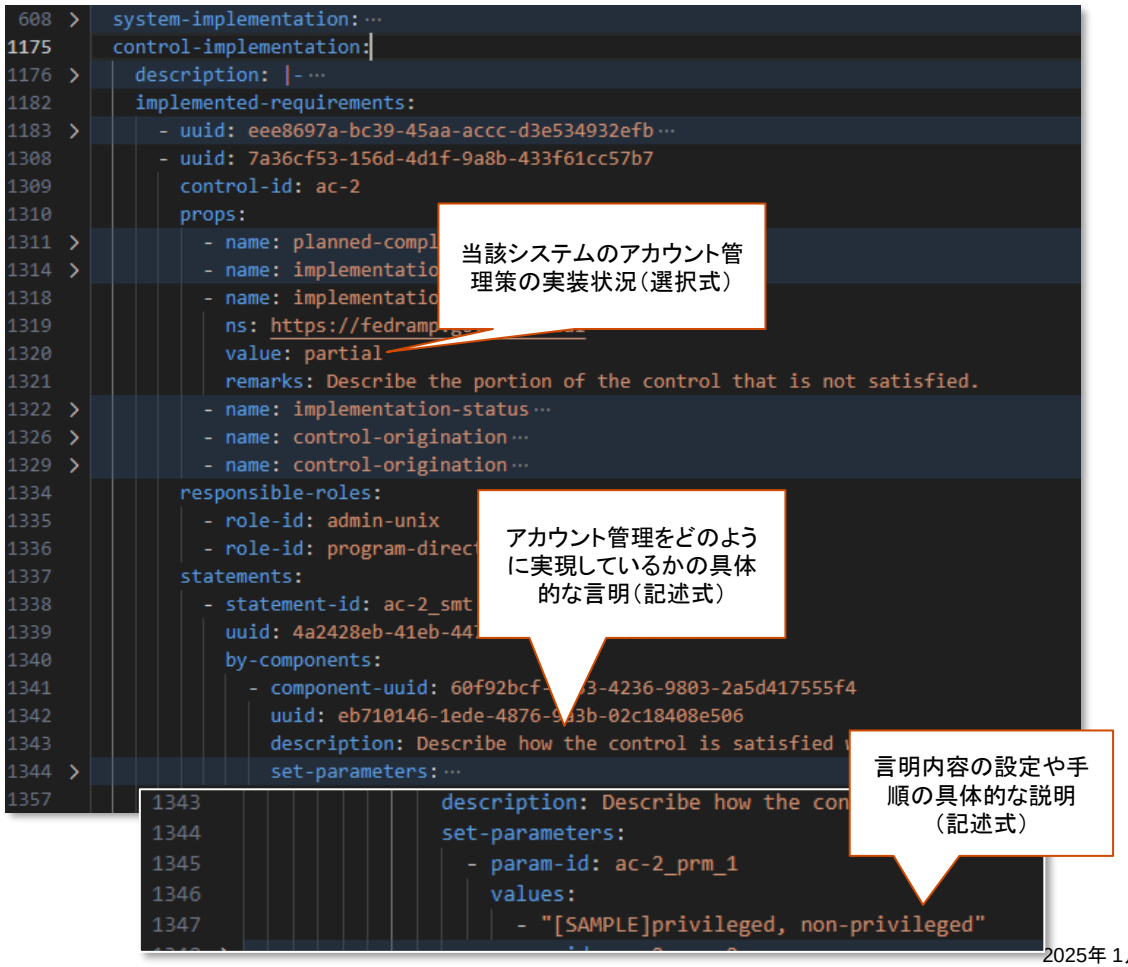
Open Security Controls Assessment Language（OSCAL）

セキュリティ統制の記述言語であり、評価、監査、および継続的な監視の高度化に向けて機械可読性を確保しています。

- 概要
  特定のシステムに対するセキュリティ管理策の実装状況の言明、評価計画、評価結果や、セキュリティ管理策のカタログを記述する様式を、**機械可読可能な形式で**定めたもの。
  言語はXML,JSON,YAMLから選択できる。

  活用によって以下が実現できると考えられている。
  - 正確な情報共有と処理による、コミュニケーションコストの削減（ペーパーワーク対比）
  - セキュリティ自己評価や監査の効率、適時性、正確性、一貫性の改善
  - セキュリティモニタリングの高頻度化（continuous assurance）化
- 作成機関
  米国立標準技術研究所（NIST）

FedRAMP SSP*のOSCAL記述例（*ISMAP言明書相当）



Source： 米国立標準技術研究所(NIST) https://pages.nist.gov/OSCAL/ および https://github.com/GSA/fedramp-automation を基に作成
PwC

OSCALサンプル

自然言語の記述を機械可読可能な形式とするための言語です。

Data at Rest (DAR)

Ref #	Areas of DAR[5]	CMVP # [6]	CM Vendor Name	Module Name	Usage	Encryption Type	Notes[7]
1	PostgreSQL database *<Use Case Example - Please Delete>*	#3980 ☐ Embedded CM ☐ Third-party CM ☒ Uses OS CM ☒ In FIPS Mode ☐ Other _____	Canonical Ltd.	Ubuntu 18.04 OpenSSL Cryptographic Module	Volume encryption	☒ Full disk ☐ File ☐ Record ☐ None ☐ Other _____	
2	App server local storage *<Use Case Example - Please Delete>*	#2931 ☐ Embedded CM ☐ Third-party CM ☒ Uses OS CM ☒ In FIPS Mode ☐ Other _____	Microsoft	Windows Server 2016	OS and application binaries	☐ Full disk ☒ File ☐ Record ☐ None ☐ Other _____	CM is Historical, per NIST CMVP. Plans to move to Windows 2019 upon Active FIPS-140-validation achieved. See POA&M ID 123.
3	S3 buckets *<Use Case Example - Please Delete>*	#4177 ☒ Embedded CM ☐ Third-party CM ☐ Uses OS CM ☒ In FIPS Mode ☐ Other _____	AWS	Key Management Service (KMS) HSM	Server-side encryption with KMS keys (SSE-KMS) used to encrypt bucket	☒ Full disk ☐ File ☐ Record ☐ None ☐ Other _____	

[5] Each entry should be the component or asset where the FIPS-140 validated cryptographic module is located.
[6] If using cryptography that lacks FIPS validation, state "No FIPS". If unencrypted, state "Unencrypted".
[7] For example, specify if the historical CM is used or the store lacks encryption entirely. Include the related POA&M ID, remediation plans, etc.

The `link` with `rel="used-by"` is used to identify the component that is using the cryptographic module (e.g., Areas of DAR).

4.11 Cryptographic Modules Implemented for Data-at-Rest (DAR)

The approach is the same as in section 4.14 (cryptographic module data-in-transit).

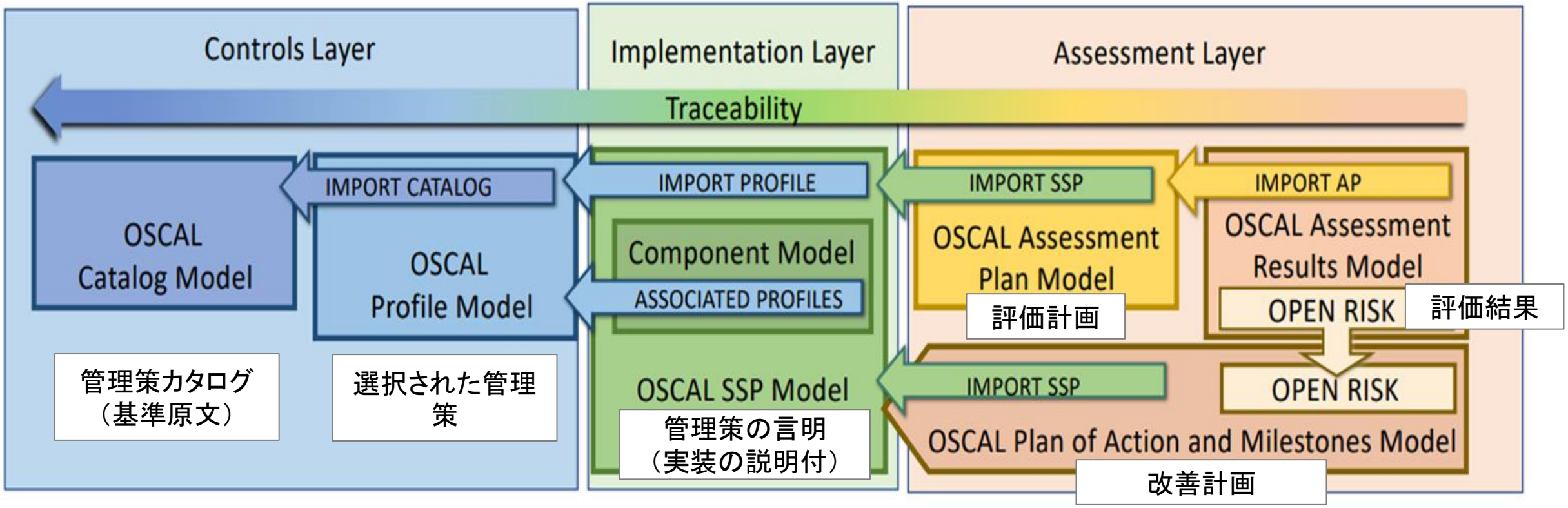
Component Representation: Example Product with FIPS 140-2 Validation

```
<!-- system-characteristics -->
<system-implementation>
    <!-- user -->
    <!-- Minimum Required Components -->

    <!-- FIPS 140-2 Validation Certificate Information -->
    <!-- Include a separate component for each relevant certificate -->
    <component uuid="uuid-value" type="validation">
        <title>Module Name</title>
        <description><p>FIPS 140-3 Validated Module</p></description>
        <prop ns="https://fedramp.gov/ns/oscal" name="asset-type"
              value="cryptographic-module" />
        <prop ns="https://fedramp.gov/ns/oscal" name="vendor-name"
              value="CM Vendor"/>
        <prop ns="https://fedramp.gov/ns/oscal" name="cryptographic-module-usage"
              value="data-in-transit"/>
        <prop name="validation-type" value="fips-140-3"/>
        <prop name="validation-reference" value="0000"/>
        <link href="https://csrc.nist.gov/projects/cryptographic-module-
validation-program/Certificate/0000" rel="validation-details" />
        <status state="operational" />
    </component>

    <!-- FIPS 140-2 Validated Product -->
    <component uuid="uuid-value" type="software" >
        <title>Product Name</title>
        <description><p>A product with a cryptographic module.</p></description>
        <link href="#uuid-of-validation-component" rel="validation" />
        <status state="operational" />
    </component>

    <!-- service -->
</system-implementation>
<!-- control-implementation -->
```

Source :米国立標準技術研究所(NIST)　https://pages.nist.gov/OSCAL/　および https://github.com/GSA/fedramp-automation を基に作成

OSCALで記述できる範囲

管理策カタログ、言明書、評価計画、評価結果と改善計画まで包括的に記述できます。



被評価者は引き続き、管理策に対応する実設定や手順を言明します。

評価者（監査人）は引き続き、別途の仕組みで証跡を収集し準拠状況を評価します。

Source :米国立標準技術研究所(NIST) https://pages.nist.gov/OSCAL/ を基に作成

ソリューション候補（再掲）

運用状況の評価に向けては、各ツールが提供する監査ログやセキュリティデータレイク/SIEM製品がキーとなりますが、ログに対するクエリ実行が主体であり自動化文脈からそれる（より広く、モダン化の文脈になる）要素もあるため本講演では割愛します。

セキュリティ監査の自動化に向けて活用できる技術要素が揃ってきています。

CSPM / CNAPP

クラウド上のインフラストラクチャやアプリケーション、およびアプリケーションライフサイクルをスキャンし、定義されたルールへの違反を検出します。公知のセキュリティガイドラインに対応したルールセットを持つ製品が多く存在します。

セキュリティ監査自動化文脈では手続きの実施、証跡収集を中心に活用します。

GRCツール

機能部門別に行っていた、ガバナンス、リスク、コンプライアンス関連活動の業務負担や複雑化傾向への対応に向けて、組織全体で一気通貫な統合管理を行うための支援ツールです。

セキュリティ監査自動化文脈では、規程や言明の記述管理や監査プロジェクトの管理に活用します。

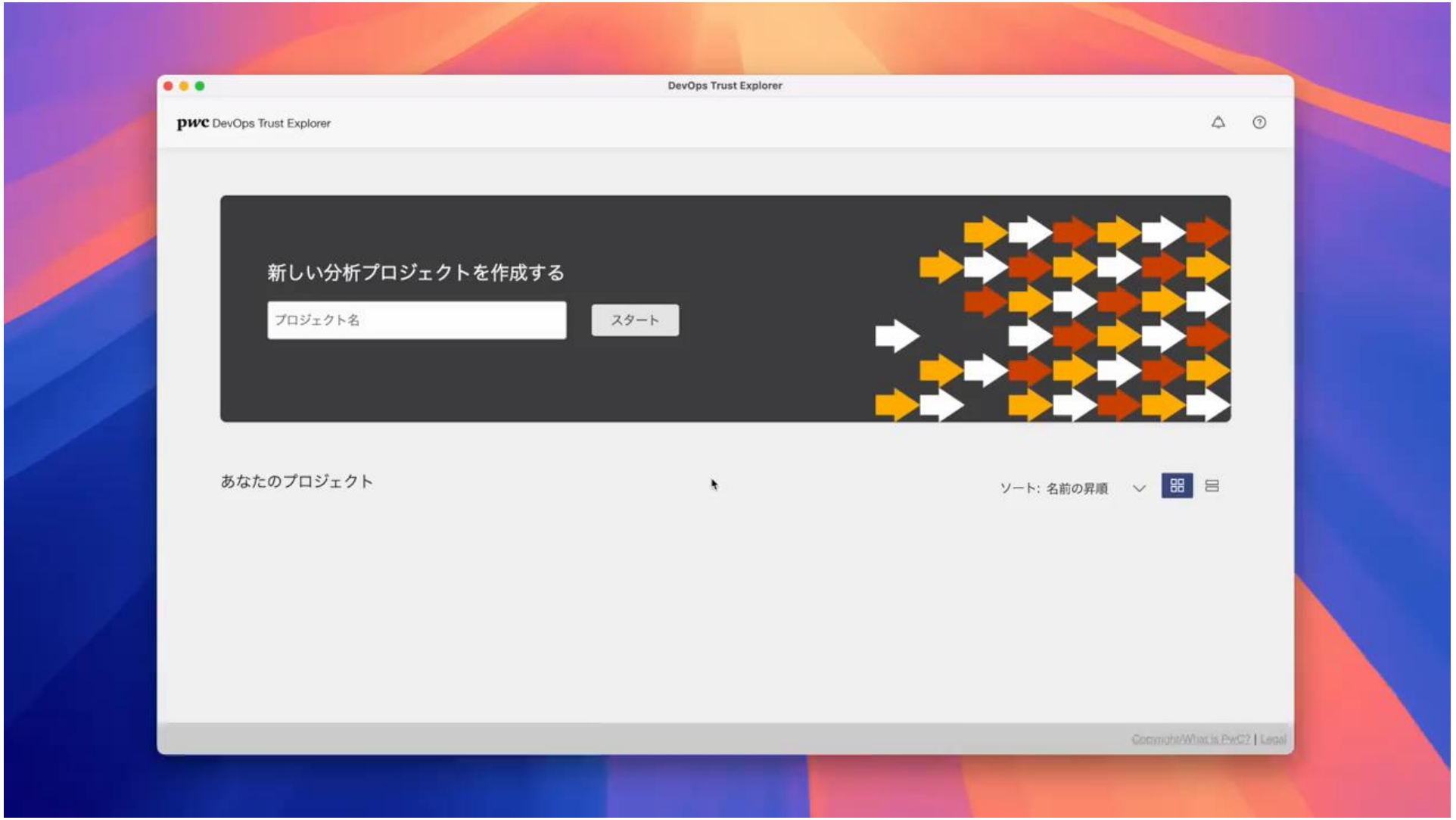
OSCAL

特定のシステムに対するセキュリティ管理策の実装状況の言明、評価計画、評価結果や、セキュリティ管理策のカタログを記述する様式を、機械可読可能な形式で定めた記述言語です。

セキュリティ監査自動化に向けて、機械と人間の橋渡しが期待できます。

おまけ

弊法人で開発中のプロダクト、DevOps Trust Explorerを紹介させてください

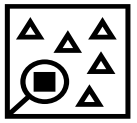


4

セキュリティ監査の自動化

自動化の狙い

監査実施側と監査対応側双方のコストが下がり、またそれによって脅威動向の変化や技術進展による監査対象の進化に追随できる高速化が狙えます。



監査実施側

- 監査作業の一部を機械処理に置き換えることで高速かつ正確になる。これによって、作業工数や人的単純ミスのフォロー工数が削減できる。
- 監査アプローチ上のクリティカルパスであった人的作業の必要工数が削減されることで、計画から報告までに要していた期間も短縮される。

監査対応側

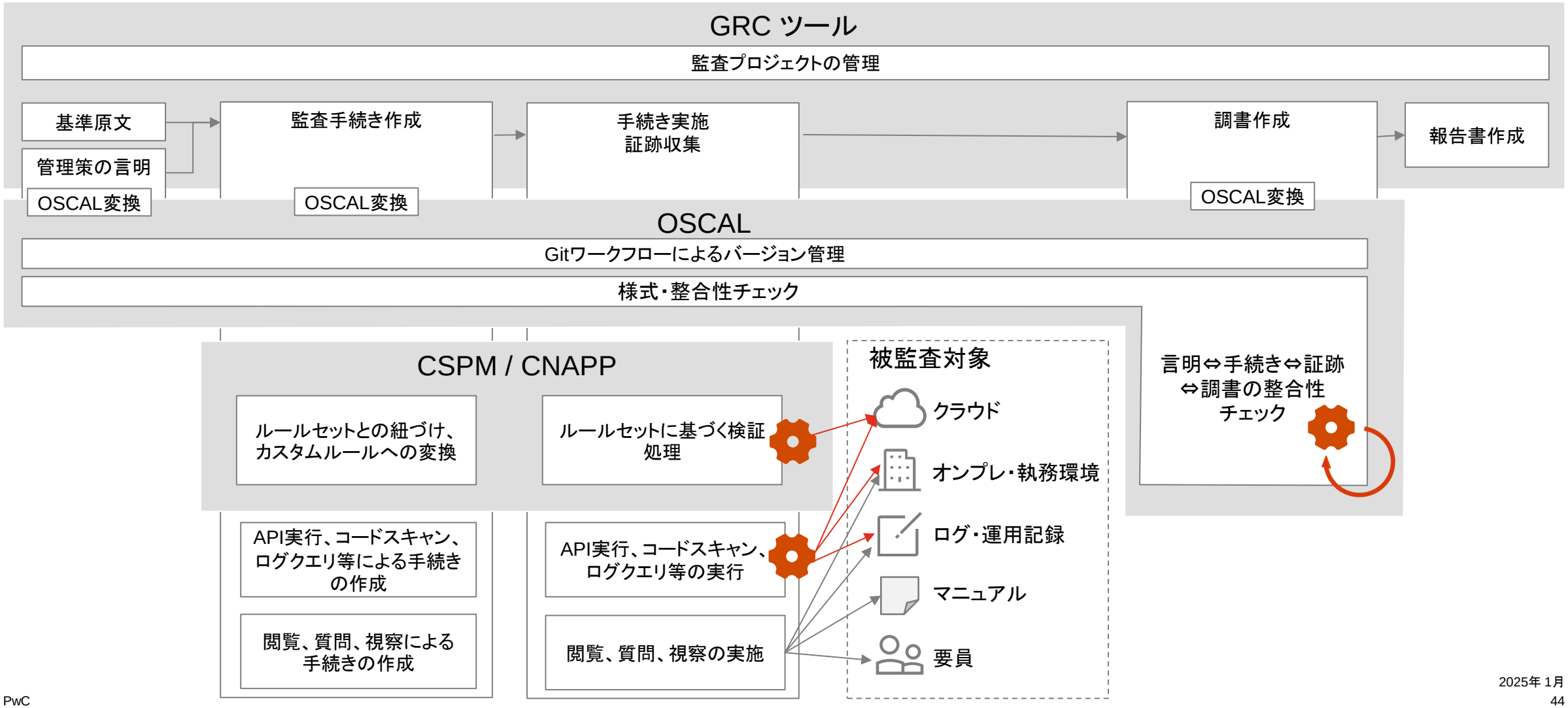
- 監査対応作業の一部が機械処理に置き換えられたことで、対応工数が削減できる。ユーザー向けの事業や業務により多くの工数を割り当てることができる
- 監査実施側に直接的あるいは間接的に支払っていたコストが下がる
- 脅威動向による基準の変化や、技術進展による監査対象（システムやプロダクト、サービスやその管理の仕組み）の進化に対して、素早く監査を終え、ユーザーに直接あるいは間接的に報告できる

結果報告のユーザー
（サービスの利用者等）

- 監査対応側（サービス提供側）に間接的に支払っていた監査対応コストが下がる
- 脅威動向の変化に対してもセキュリティリスクを抑えてサービスを利用できる
- 監査対象（システムやプロダクト、サービスやその管理の仕組み）の進化に対して、監査が素早く終わり、最新の仕様をすぐに利用開始できる

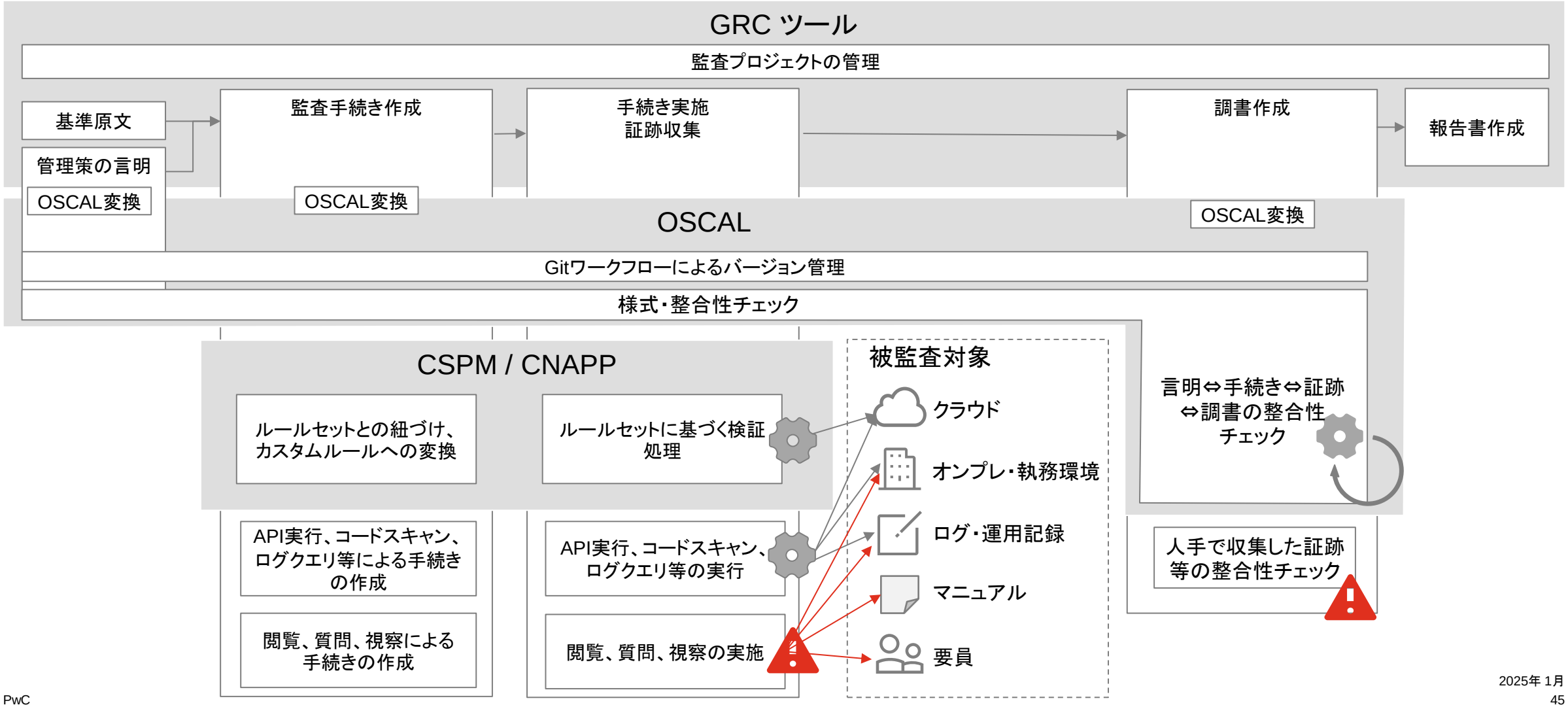
ソリューションの組み合わせで自動化を実現？

証跡収集や調書の様式・整合性チェックを中心として自動化が期待できますが、、、、



フィジカル空間は対象外

フィジカル空間に残る被監査対象に対しては、人手の作業が以前発生します。



証跡収集の自動化が期待できるのは3割程度か

キャッチアップが必要な個所と、証跡収集の自動化が期待できる箇所はほぼイコールと考えられます。

組織的管理策

5.1 情報セキュリティ方針群
5.2 役割及び責任
5.3 職務の分離
…
5.9 情報及びその他の資産の目録
…
5.12 情報の分類
5.13 情報のラベル付け
5.14 情報の転送
5.15 アクセス制御
5.16 識別情報の管理
5.17 認証情報
5.18 アクセス権
5.19供給者関係における情報セキュリティ
…

人的管理策

6.1 選考
6.2 雇用条件
6.3 意識向上，教育及び訓練
・・・
6.7 リモートワーク
・・・

物理的管理策

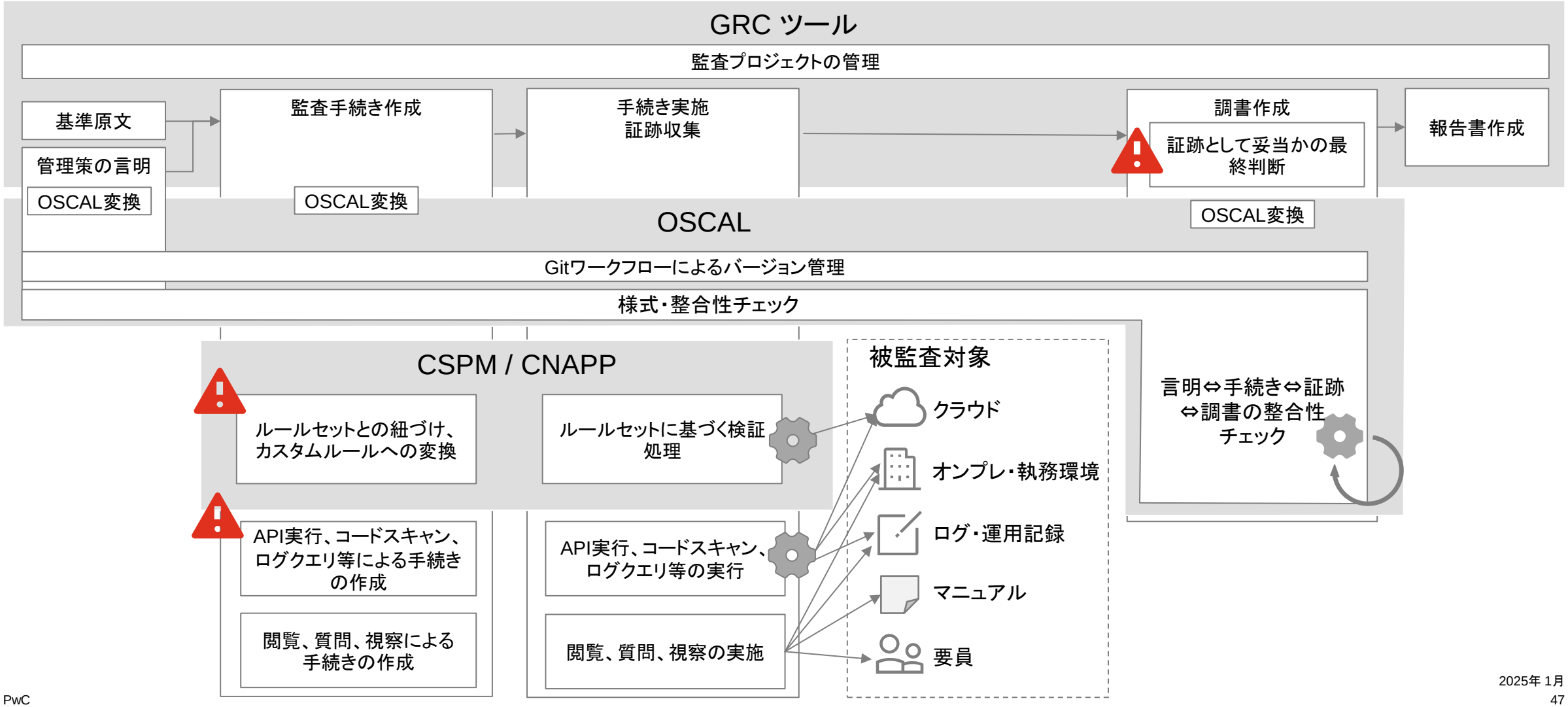
7.1 物理的セキュリティ境界
7.2 物理的入退
7.3 オフィス・部屋及び施設
・・・

技術的管理策

8.1 利用者エンドポイント機器
8.2 特権的アクセス権
8.3 情報へのアクセス制限
8.4 ソースコードへのアクセス
8.5 セキュリティを保った認証
8.6 容量・能力の管理
8.7 マルウェアに対する保護
8.8 技術的ぜい弱性の管理
8.9 構成管理
8.10 情報の削除
8.11 データマスキング
8.12 データ漏えい防止
8.13 情報のバックアップ
8.14 情報処理施設・設備の冗長性
・・・

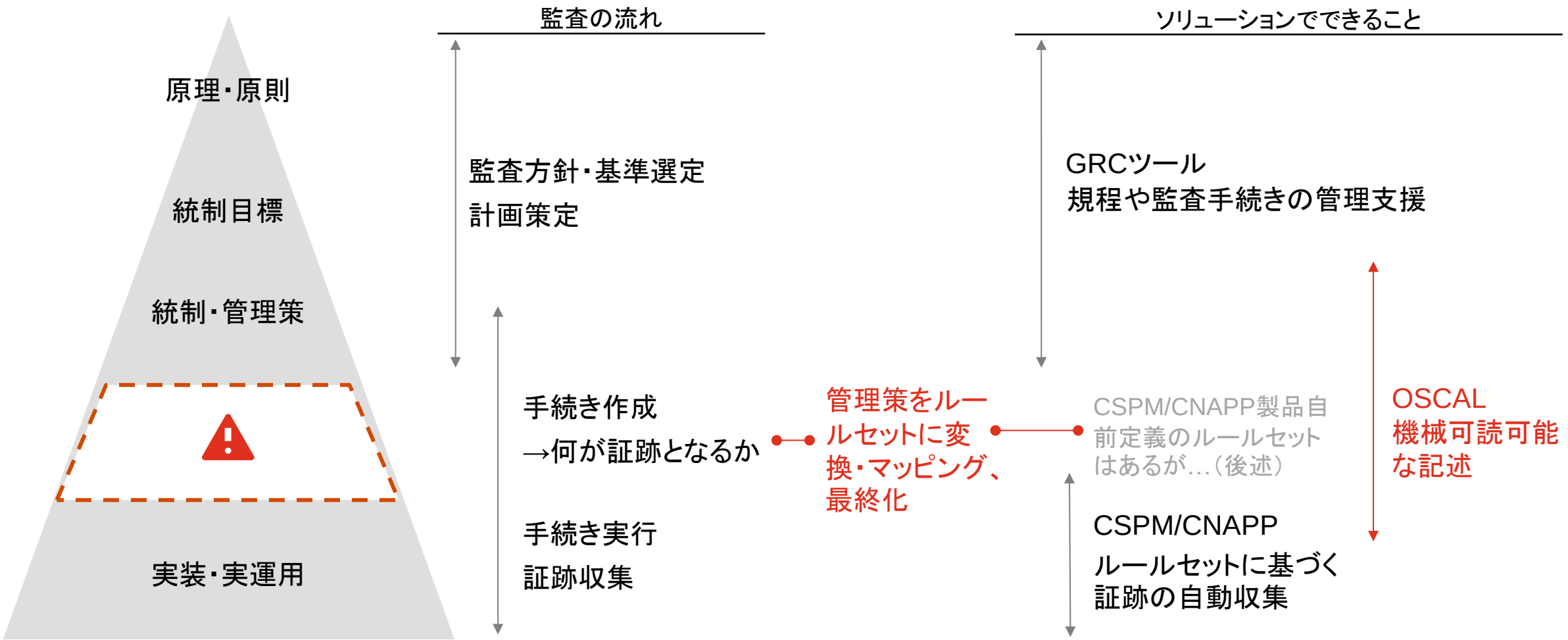
苦しいラストワンマイル

“機械に何を収集させるか”“証跡として妥当か”の判断は、基準とコンテキストを理解した人間でなければ行えません。



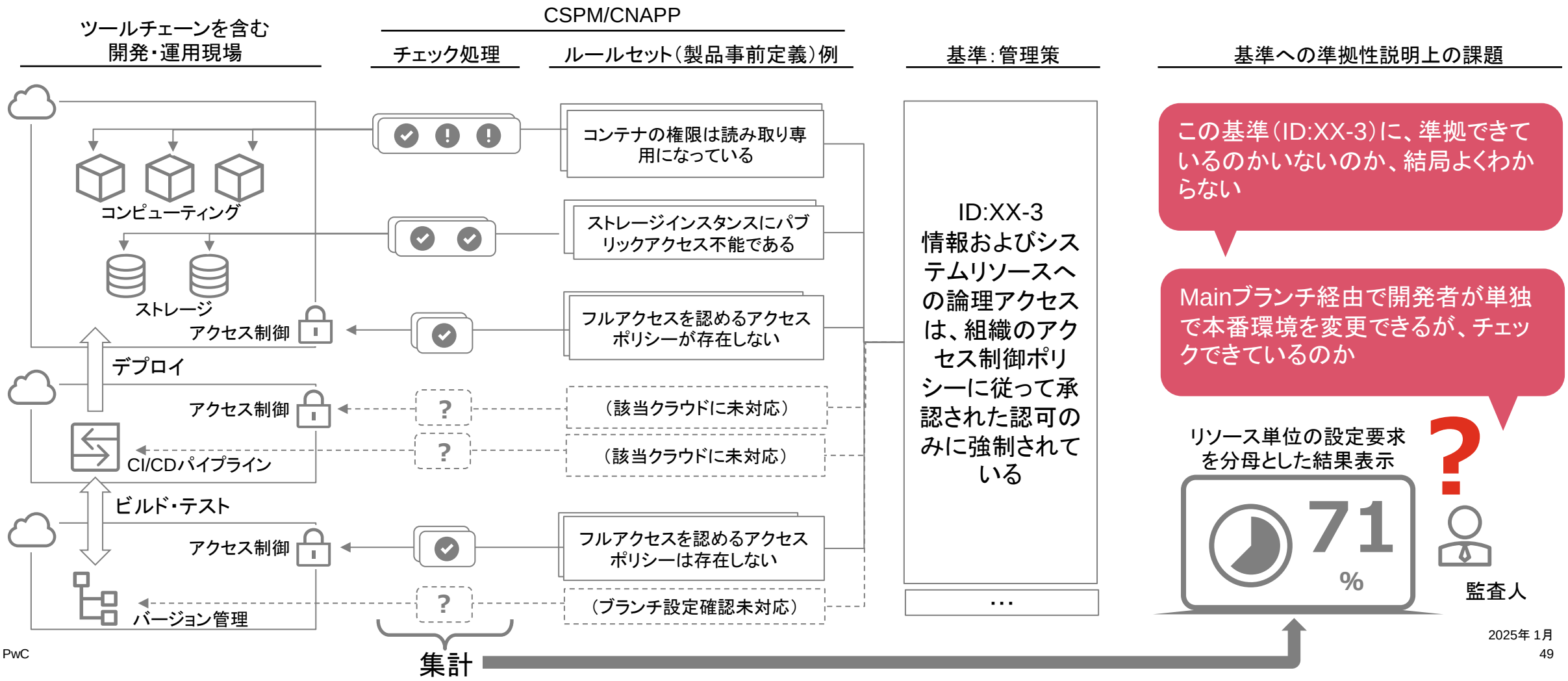
ラストワンマイルの中心はOCSALか

機械と人間の橋渡しであるOSCALを用いれば、何が証跡となるかを記述できます。



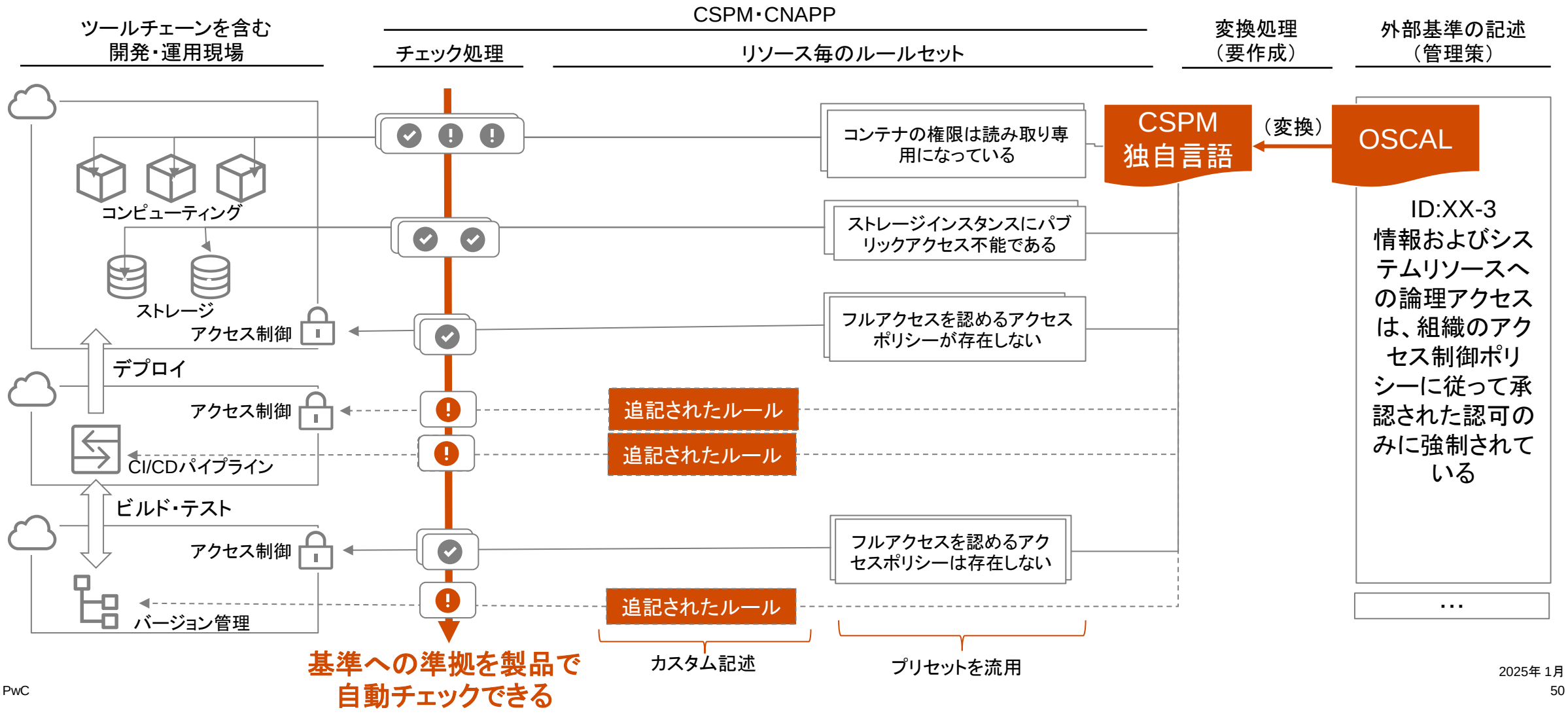
ラストワンマイル例 | リソース横串の証跡収集

製品事前定義ルールセットがリソース単位の場合、そのチェック証跡では管理策への準拠が直接的にわかりません。



ラストワンマイル対応例 | OSCAL活用でリソース横串のルール定義

OSCALで横串証跡を定義・記述したうえで、製品ルールセットのカスタム記述に変換し、チェックを行います。



FedRAMPとは、米国連邦政府におけるクラウドセキュリティ認証制度です。日本のISMAP制度に相当します。

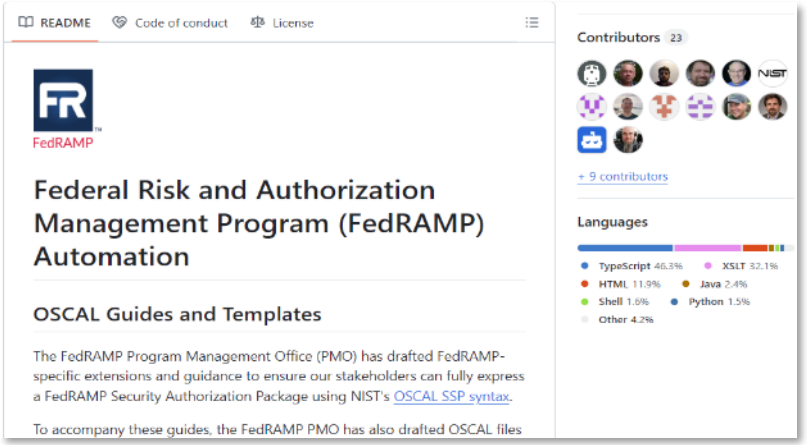
OSCAL活用ユースケース

米国ではOSCALを活用したFedRAMP Automationプロジェクトが推進されています。

プロジェクト概要

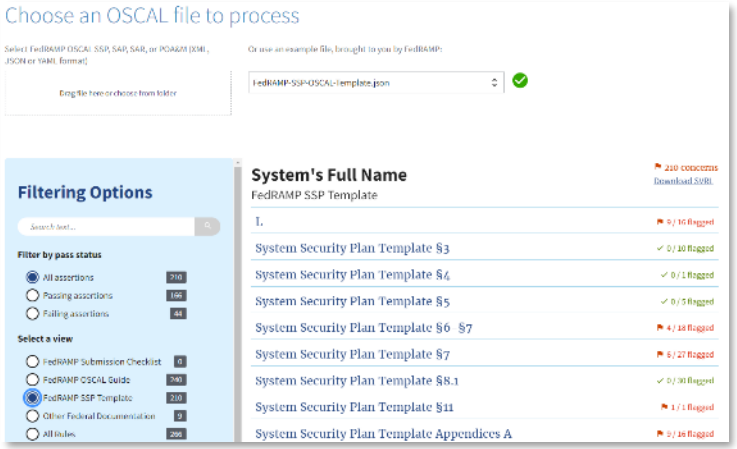
米国連邦政府のクラウドサービス認証制度であるFedRAMPでは、既にOSCAL様式での文書提出が可能である。FedRAMP Automationプロジェクトでは、OSCAL様式での文書作成を支援するツールやガイドに加えて、OSCALで記述された内容のValidationチェックプログラムを提供している。

このプロジェクトはオープンソースとしてGitHub上に公開・推進されている。



代表的な成果物

- 提出文書のOSCALテンプレート
  - System Security Plan（言名書）
  - Assessment Plan（第三者評価計画）
  - Assessment Results（評価結果報告書）
  - Plan Of Action & Milestones（改善計画）
- OSCAL化ベースラインカタログ（管理基準）
- Validationプログラム
  - Documents Provided Check（書類存在チェック）
  - Overall SSP Checks（SSP内容確認）



創出効果* *実測データ未確認

クラウド サービス プロバイダー は、
言明書をより迅速かつ正確に作成し、政府の審査に提出する前に、その内容の多くを検証できるようになる

第三者評価組織は、
セキュリティ評価活動の計画、実行、レポートを自動化し、効率化/高度化できる

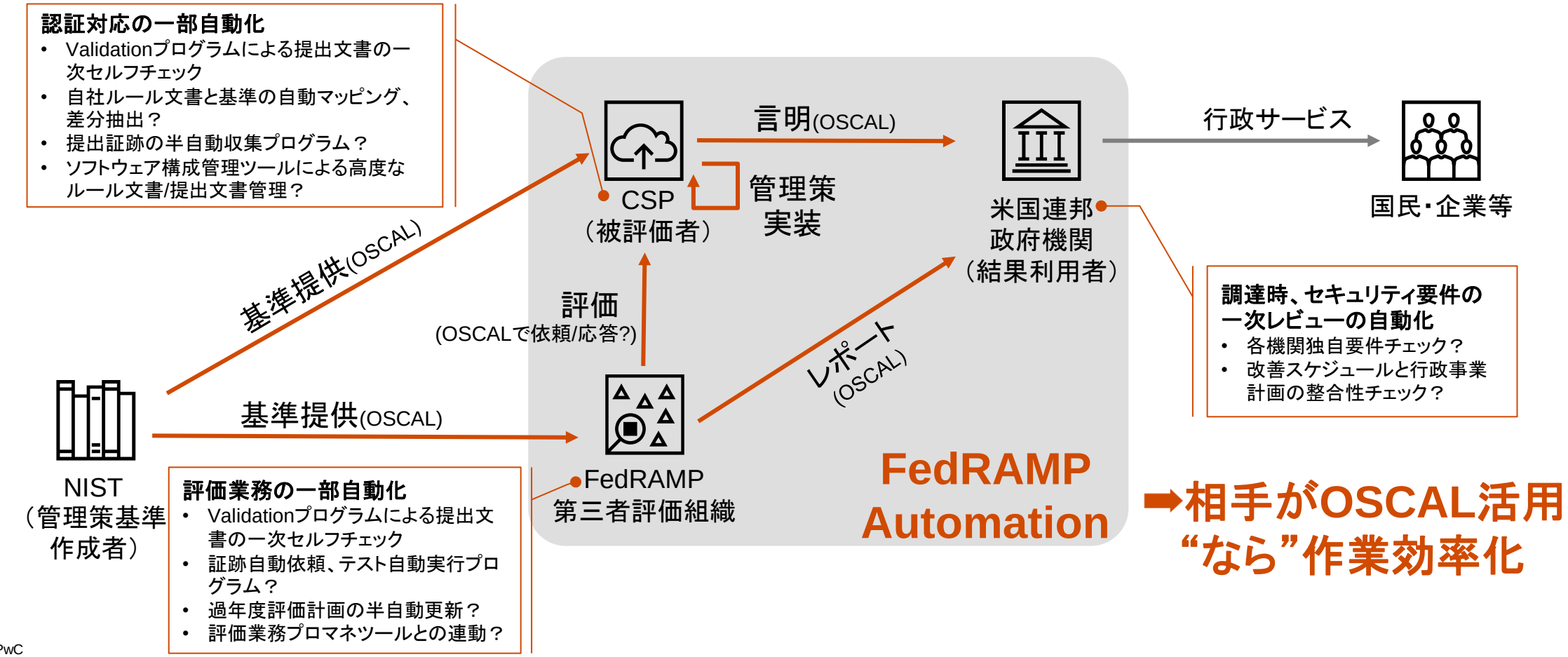
米国連邦政府機関は、
FedRAMP セキュリティ認可パッケージのユーザーとしての確認・レビューを迅速化できる

Source :米国立標準技術研究所(NIST) https://github.com/GSA/fedramp-automation および https://www.fedramp.gov/FedRAMP-moves-to-automate-the-authorization-process/を基に作成

FedRAMP Automation プロジェクトの現状

OSCAL活用の現状は、被評価者、評価者、結果利用者の作業効率化と考えられます。

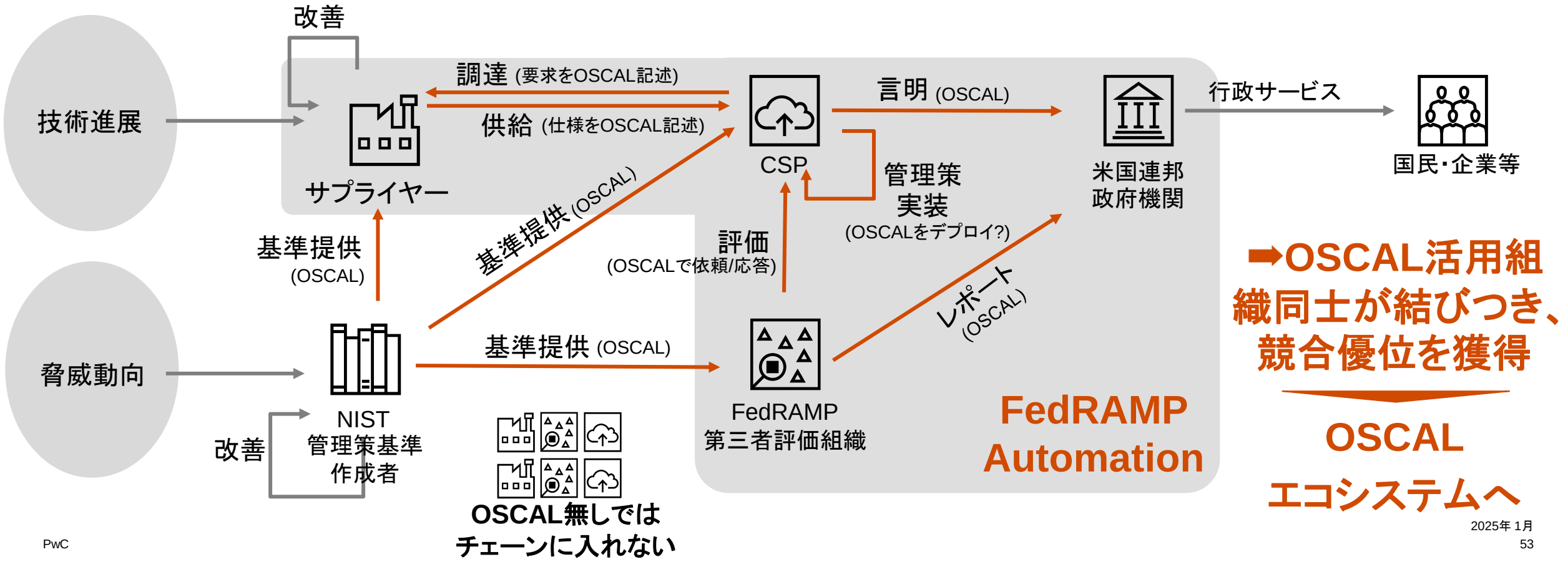
FedRAMP サプライチェーンとOSCAL活用（現在）



FedRAMP Automation プロジェクトから想定できる将来

OSCAL活用組織同士が強く結びつきサプライチェーン全体でエコシステムが形成される可能性があります。

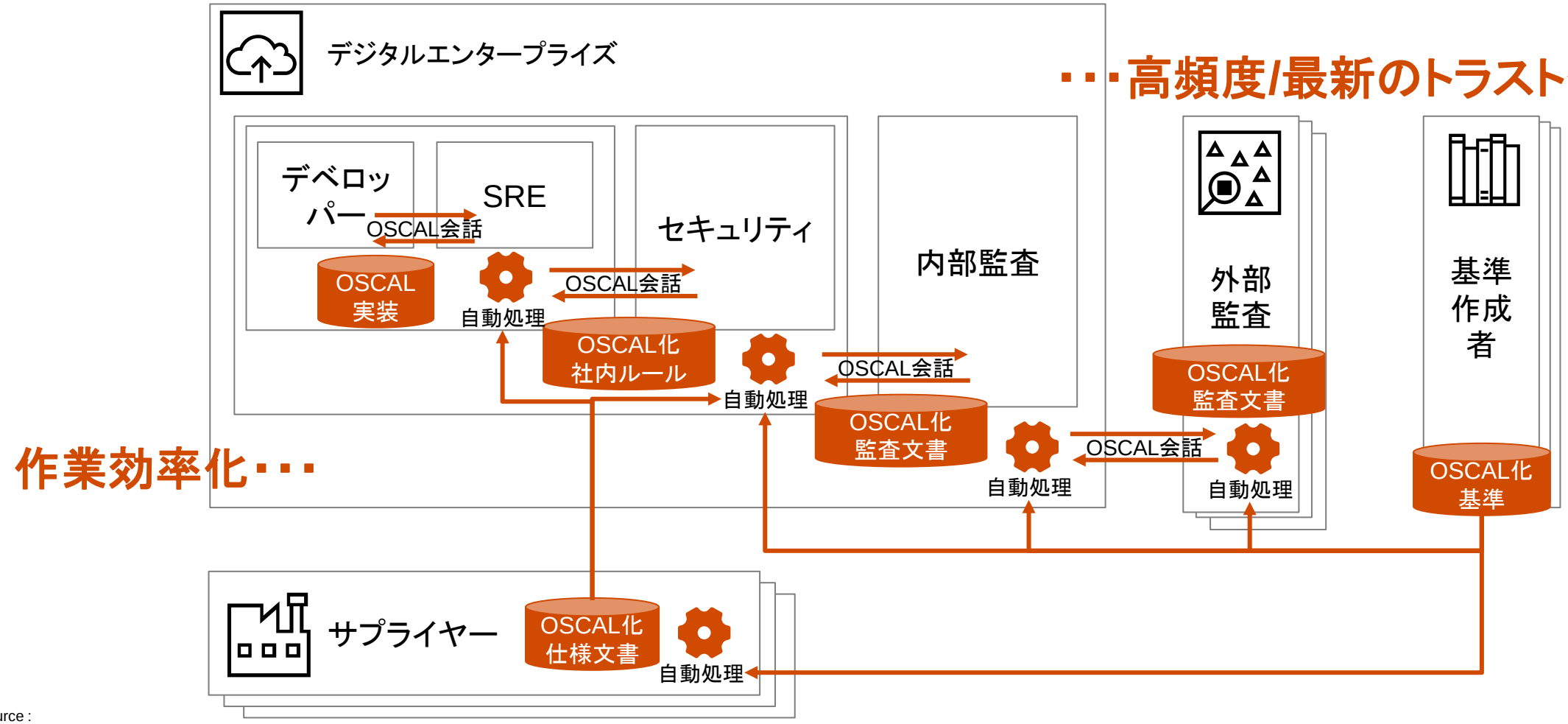
FedRAMP サプライチェーンとOSCAL活用（将来）



想定できる将来

政府認証文脈を外しても、OSCALエコシステムに乗った組織群では、作業効率化や高頻度化メリットが期待できます。

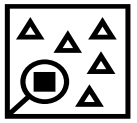
赤：メリットが期待できる箇所



Source :
PwC

自動化の狙い（再掲）

監査実施側と監査対応側双方のコストが下がり、またそれによって脅威動向の変化や技術進展による監査対象の進化に追随できる高速化が狙えます。



監査実施側

- 監査作業の一部を機械処理に置き換えることで高速かつ正確になる。これによって、作業工数や人的単純ミスのフォロー工数が削減できる。
- 監査アプローチ上のクリティカルパスであった人的作業の必要工数が削減されることで、計画から報告までに要していた期間も短縮される。

監査対応側

- 監査対応作業の一部が機械処理に置き換えられたことで、対応工数が削減できる。ユーザー向けの事業や業務により多くの工数を割り当てることができる
- 監査実施側に直接的あるいは間接的に支払っていたコストが下がる
- **脅威動向による基準の変化や、技術進展による監査対象（システムやプロダクト、サービスやその管理の仕組み）の進化に対して、素早く監査を終え**、ユーザーに直接あるいは間接的に報告できる

結果報告のユーザー
（サービスの利用者等）

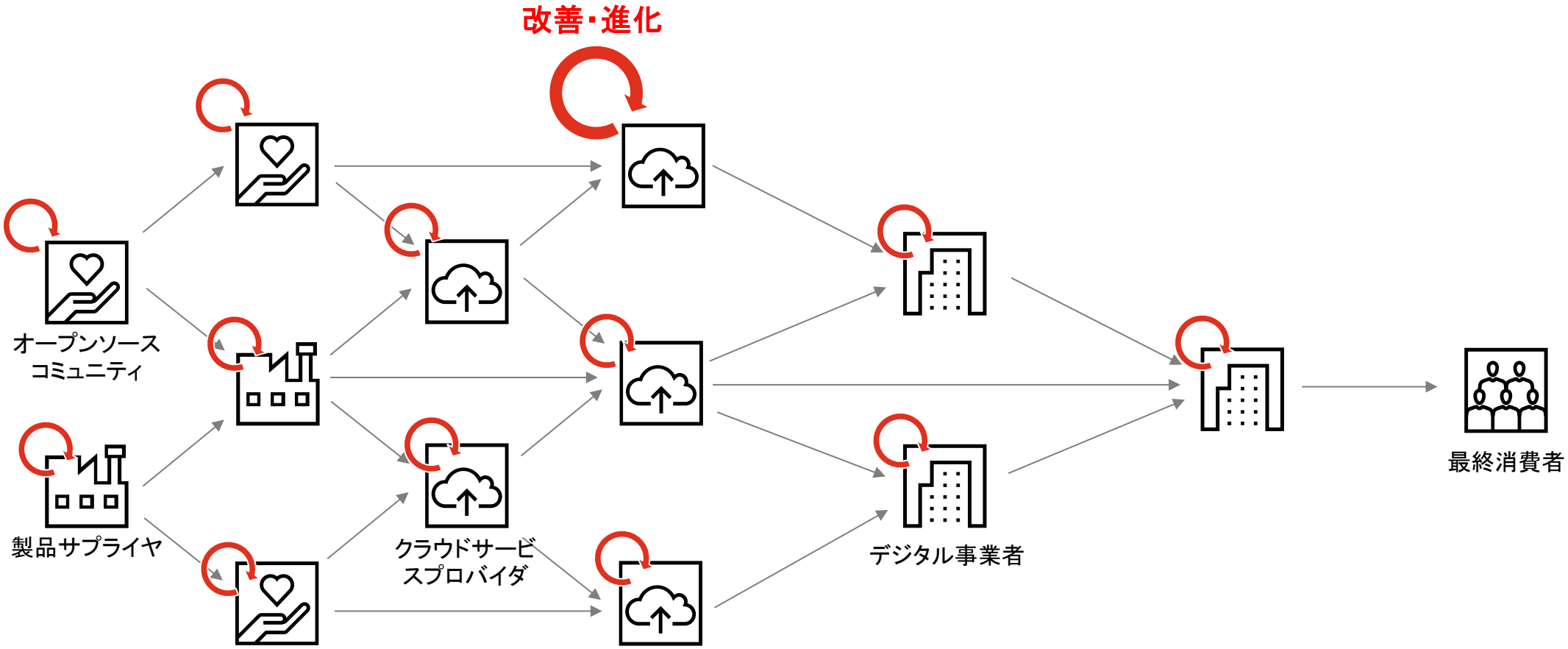
- 監査対応側（サービス提供側）に間接的に支払っていた監査対応コストが下がる
- **脅威動向の変化に対してもセキュリティリスクを抑えてサービスを利用できる**
- **監査対象（システムやプロダクト、サービスやその管理の仕組み）の進化に対して、監査が素早く終わり、最新の仕様をすぐに利用開始できる**

5

将来に向けて

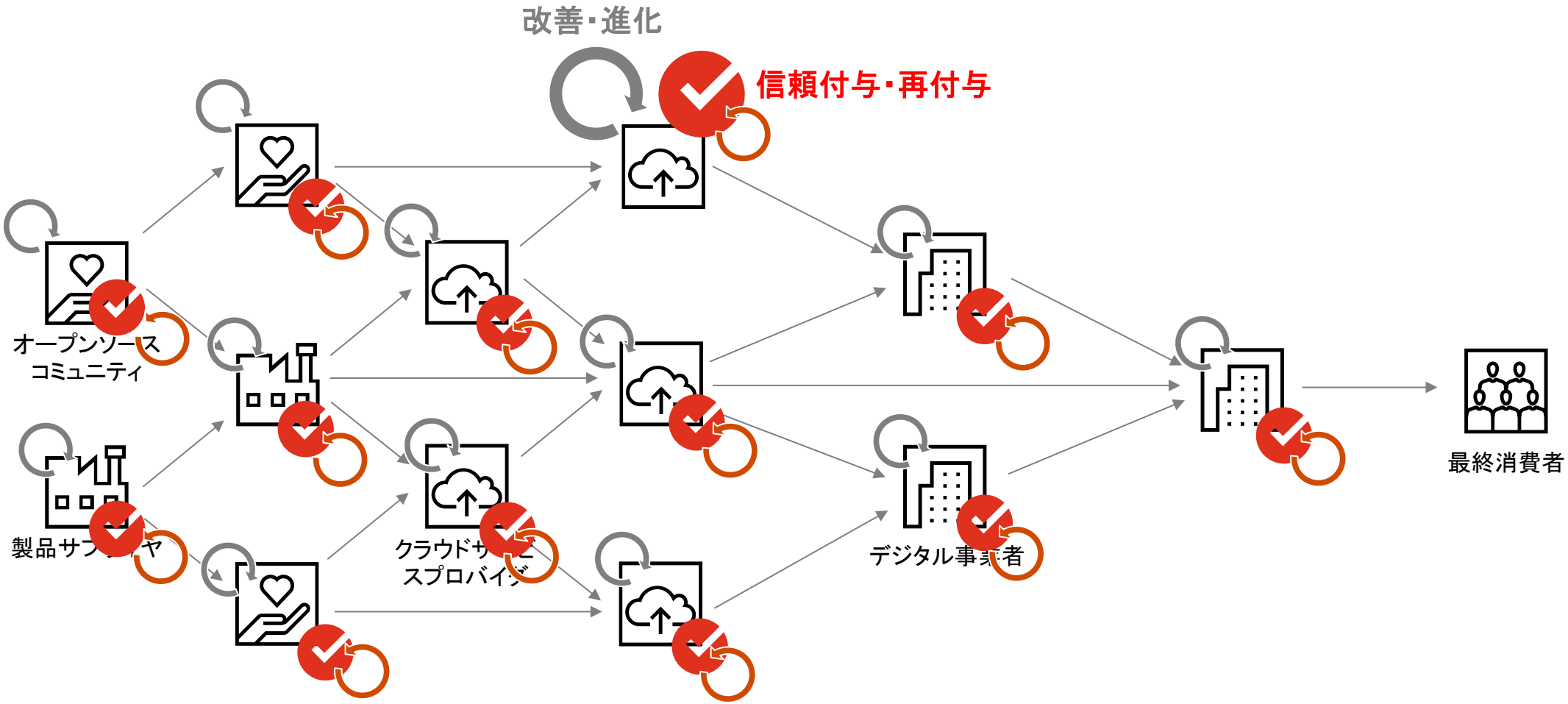
デジタルサービスの素早い進化は連なっている（再掲）

ソフトウェアサプライチェーンの特徴として、それぞれがスピード感を持って改善・進化した結果が素早く連鎖します。



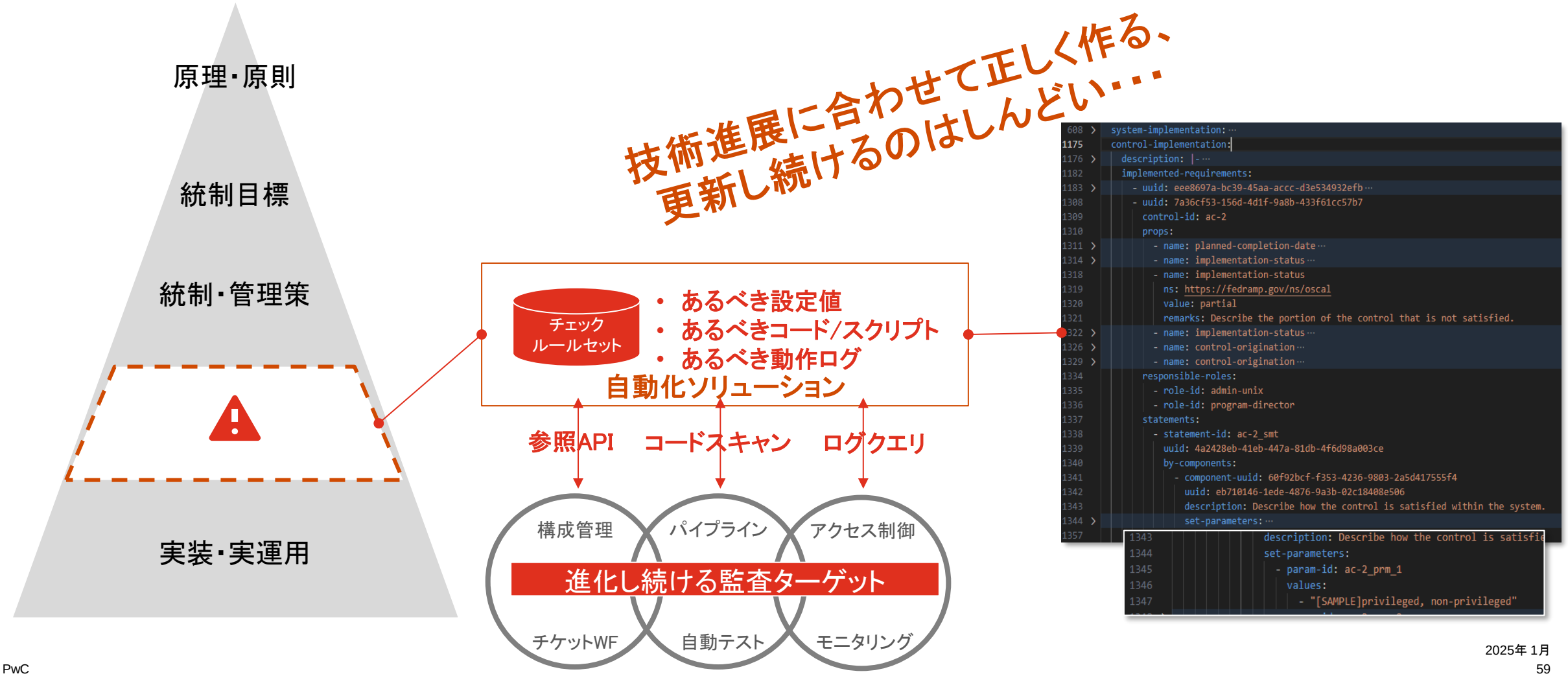
信頼の付与・再付与も自動化で追随

スピード感を持ってセキュリティ監査が追随できれば、社会全体に大きく寄与できます。



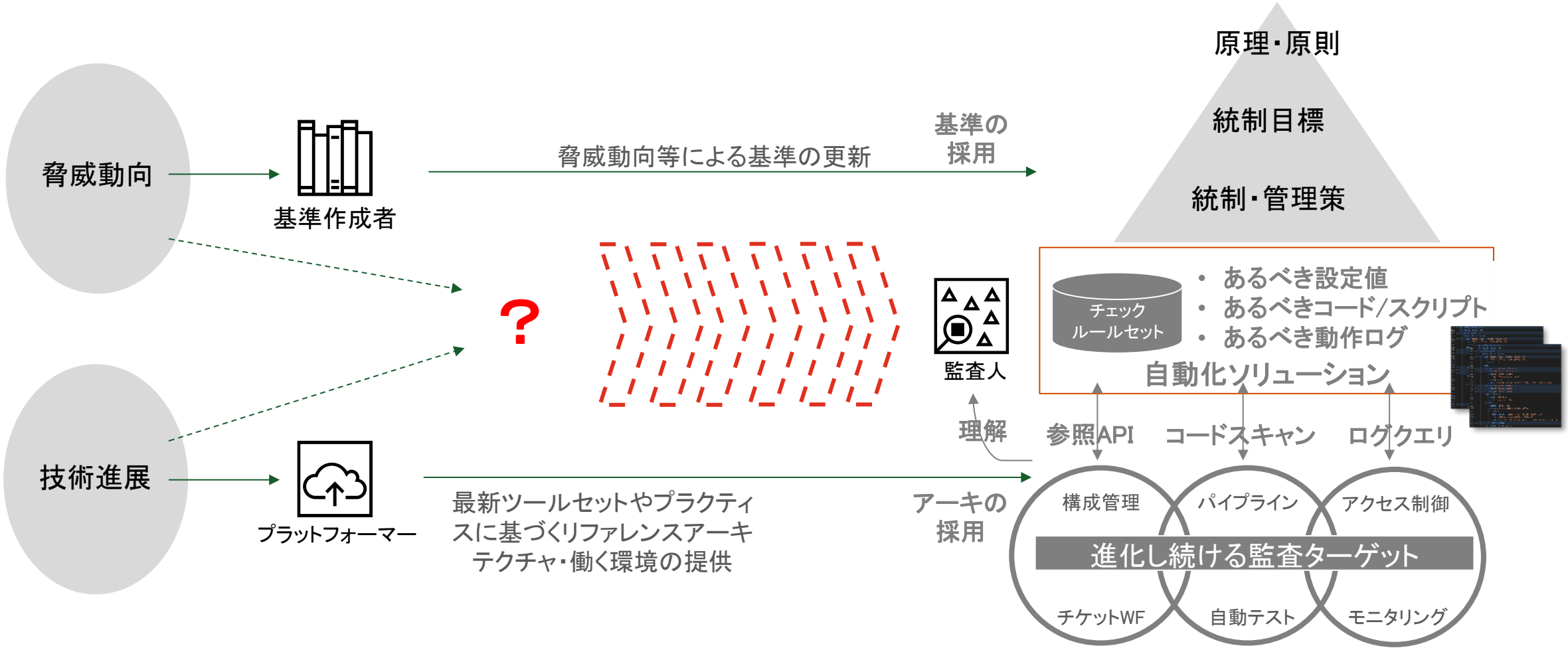
ラストワンマイル対応の労力を抑えられないか

チェックルールセットの初期作成、および監査ターゲットの進化に合わせた継続更新は労力がかかります。



ラストワンマイル対応の追い風が欲しい

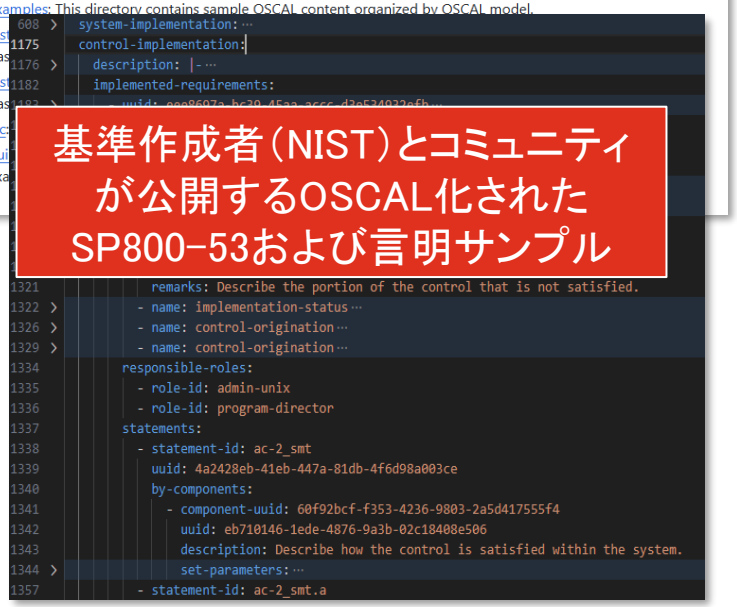
チェックルールセット更新の大元トリガーである技術進展や脅威動向を、ダイレクトに監査人が受け止めづらい状態です。

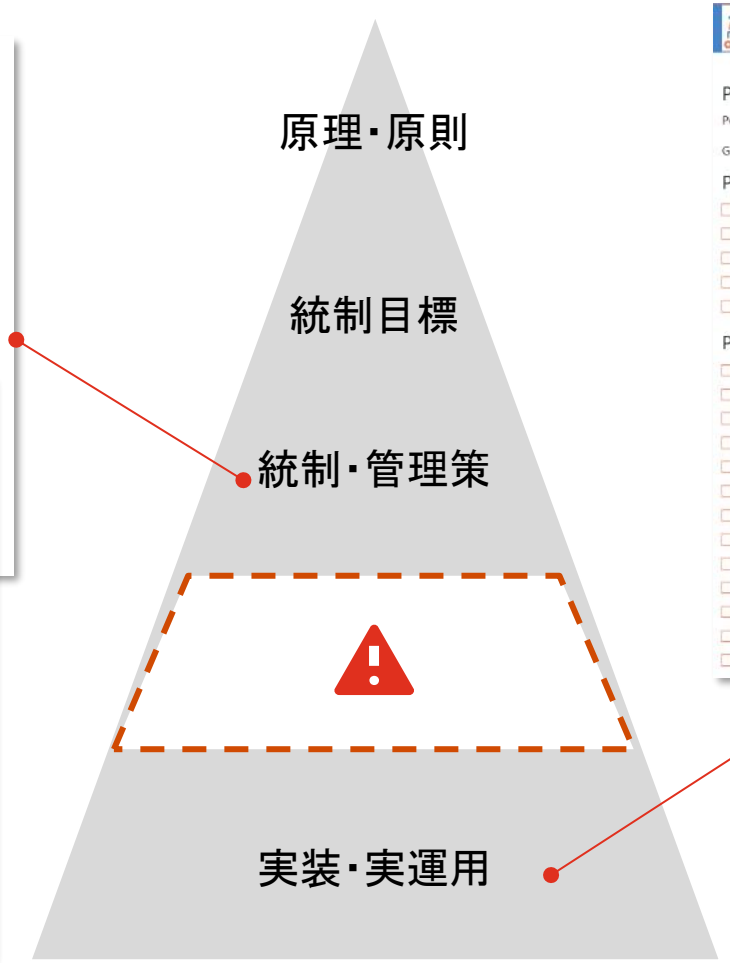


追い風周辺部品 | OSCAL化基準 & Policy as Code

一部の基準は既にOSCAL化されています。また、特定の基準とは紐づいていないものの特定のプロダクトに対してはセキュリティベストプラクティスが設定・ソースコードレベルの解像度（Policy as Code）で公開されています。

基準作成者（NIST）とコミュニティが公開するOSCAL化されたSP800-53および言明サンプル



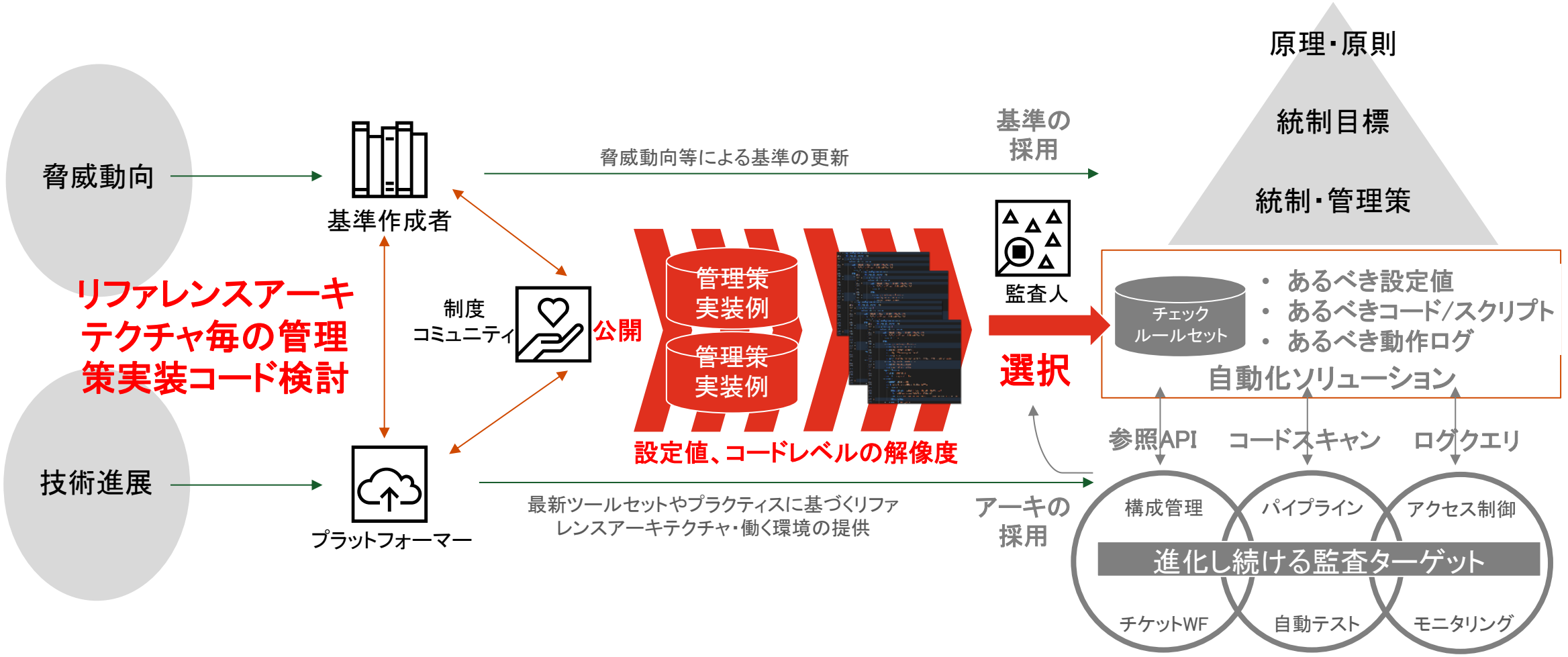


特定プロダクト向けのハードニング・要塞化設定（Policy as Code）

Source :米国立標準技術研究所(NIST) https://github.com/usnistgov/oscal-content および https://kyverno.io/policies/ を基に作成。また、Kyveroは非営利団体であるCloud Native Computing Foundationのオープンソースプロジェクトです。

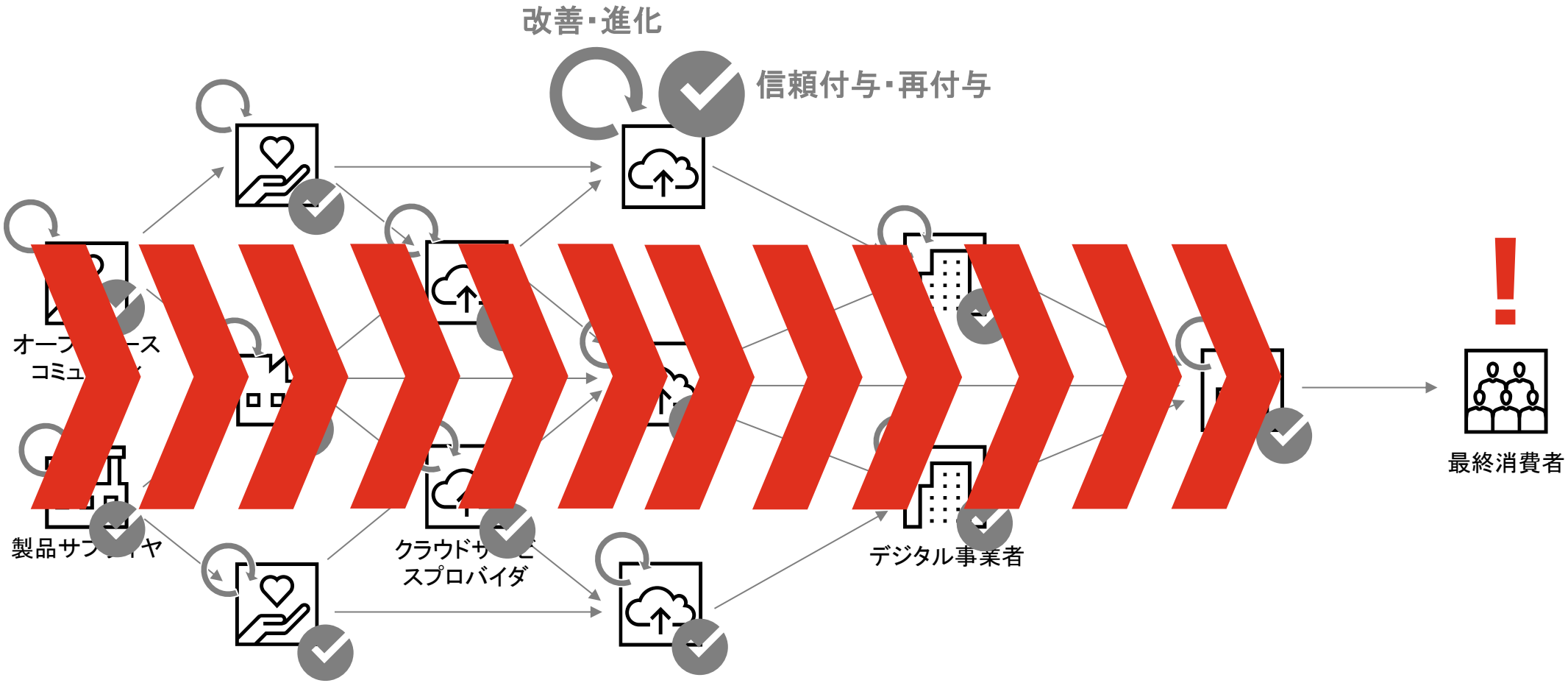
制度コミュニティからの追い風“管理策実装コード例の公開”イメージ

技術進展や脅威動向を踏まえた、設定値、コードレベルの実装コードを検討・公開する制度コミュニティがあれば、各組織の自動化が加速します。



セキュリティ監査の自動化で社会全体を加速させよう

スピード感を持ってセキュリティ監査が追随できれば、社会全体に大きく寄与できます。



“

技術の変化に対応し、より良いサービス提供を約束し、経済的繁栄のニーズのバランスを取るためには、アジリティは贅沢品ではなく必需品である。

世界経済フォーラム
年次総会

Thank you

www.pwc.com/jp