JSSA システム監査学会

# Society5.0の実現に向けたクラウドによるITサービスとその監査保証

Cloud-based IT services for realizing Society 5.0 - a study of implementing its audit and assurance

2020年11月6日

システム監査学会
IT監査保証の判断基準研究プロジェクト

日本電気株式会社
鈴木　夏彦
システム監査技術者, CIA, CISA

JSSA システム監査学会

この資料の内容は、発表者を含む研究プロジェクトメンバーの見解であり、メンバーの所属組織等とは関係ありません。

本資料の無断転載はお断りします。

JSSA システム監査学会

# 目次

JSSA システム監査学会

# IT監査保証の判断基準研究プロジェクト

## 2020年度研究テーマ

**ドラッカーの『テクノロジストの条件』を基本書として用い、
以下を主要テーマにテクノロジーモニタリングの研究と実践を行い、
その成果を発表**

a. クラウド、サイバーセキュリティ等にかかる基準・標準の動向調査
b. 各研究プロジェクトメンバーによるビジネスとテクノロジーの最新動向の研究
c. 監査、評価手法、ツールにかかるグローバルな標準、基準の動向調査
d. コンピュータサイエンス、経営学、心理学、社会学とその背景となる哲学の研究
e. 上記研究成果の定例研究会等での発表および学会誌等への投稿

JSSA システム監査学会

# IT監査保証の判断基準研究プロジェクト メンバー

## 主査；松尾 明（公認会計士, CISA, TOGAF9認定アーキテクト）

※　五十音順

| メンバー名 | 所属など |
|---|---|
| 石島 隆 | 法政大学経営大学院教授 |
| 遠藤 正之 | 静岡大学情報学部教授 |
| 杉山 哲男 | コイネージ株式会社　CIA, CISA |
| 鈴木 夏彦 | 日本電気（株） システム監査技術者, CIA, CISA |
| 成田 和弘 | 三菱UFJトラストシステム（株） システム監査技術者, CIA, CISA |
| 牧野 博文 | （株）東芝　システム監査技術者, ITストラテジスト, 情報処理安全確保支援士, ITコーディネータ, CISA |
| 水野 英治 | システム監査人事務所イレブンス　システム監査技術者, 公認システム監査人(CSA), MBA |
| 米川 弘幸 | SMBC日興証券（株） システム監査技術者, CIA, CISA |

JSSA システム監査学会

# 発表者紹介 (鈴木 夏彦)

**15年**

**ITサービス事業の内部統制、サービスマネジメント、セキュリティマネジメントに係る整備・運用・監査業務に従事**

主な業務と実績

- ✓クラウドサービス、データセンター、マネージドサービスの内部監査
- ✓海外現地法人を含む全社ITサービスマネジメント標準策定・展開
- ✓システム運用業務の作業品質総点検 (約200プロジェクト)
- ✓システムセキュリティ計画策定 (NIST SP800-53)
- ✓お客さま向け内部監査サービス (国内・海外拠点/約15年)

**国内/海外・社外/社内の多数のITサービス提供組織と協働**

JSSA システム監査学会

# 研究目的

## Society5.0の実現に向けたクラウドによるITサービスとその監査保証

*Cloud-based IT services for realizing Society 5.0 - a study of implementing its audit and assurance*

**クラウド・バイ・デフォルト原則**など、新たな価値を創出するITサービスの需要が急速に高まり、クラウド環境が提供する先進技術と強力なコンピューティングパワーは、**Society5.0**を実現するための新しいサービスを生みだすための必須の**インフラストラクチャー**となった。一方で、重要インフラへのサイバー攻撃などのリスクも高まっており、**安全なクラウドサービスを調達するための制度**や**プライバシー保護**に係わる**法や規制、基準等の整備**も進んでいる。Society5.0の実現に向け、クラウドを活用した**安心・安全なITサービスを継続的に提供するITサービスとその監査保証の判断基準**について考察する。

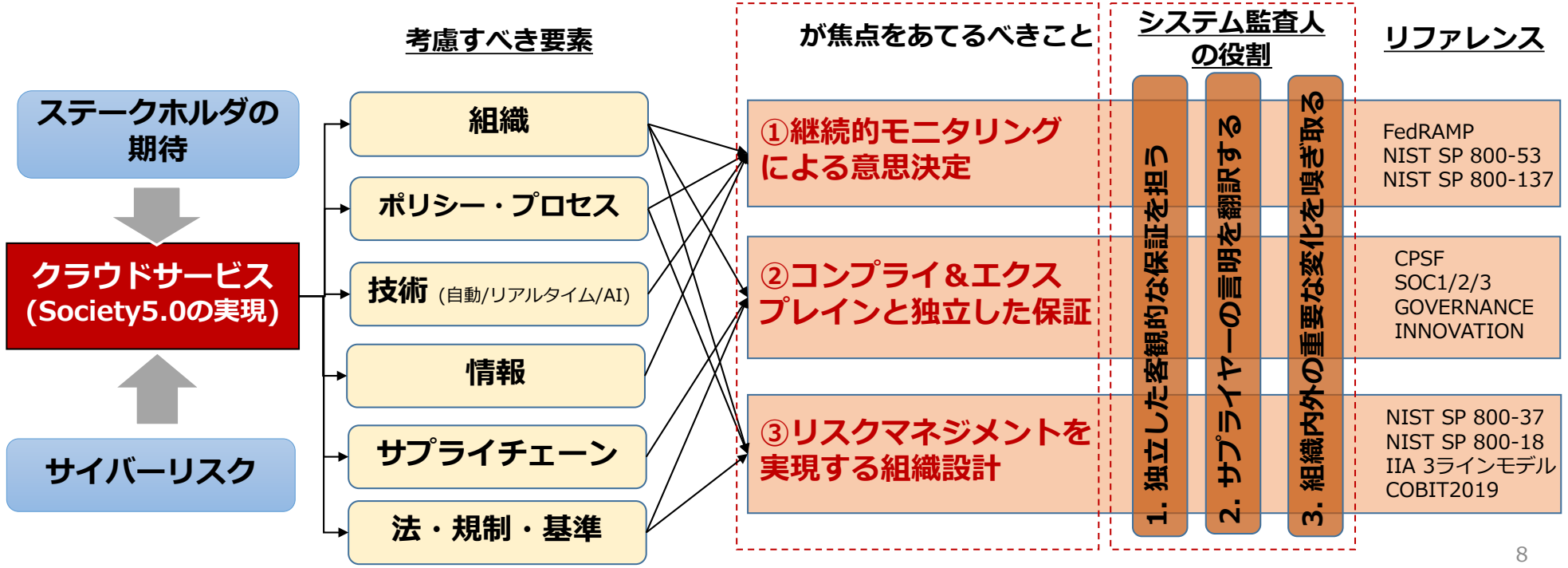
JSSA システム監査学会

# 研究報告サマリ

リサーチクエスチョン:

1 クラウドサービスを活用したITサービスを提供する組織を含む

**Society5.0の実現に向けて、クラウドサービス提供組織(CSP)[1]が焦点を当てて取り組むべきことは何か。その中で、システム監査人はどのような役割を果たすべきか。**



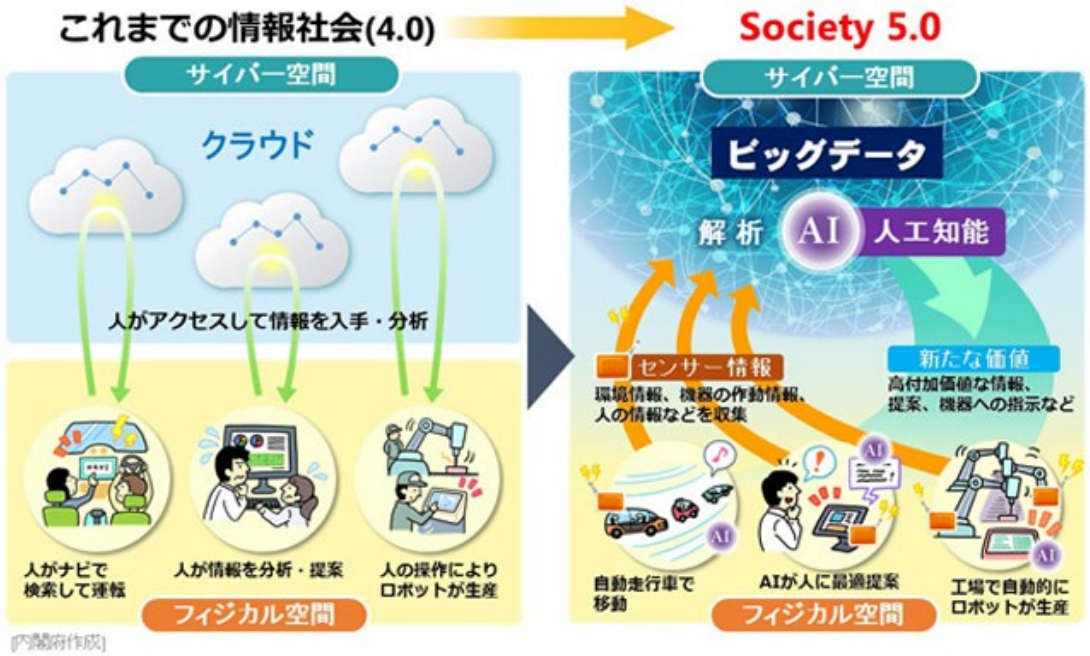
JSSA システム監査学会

# Society 5.0とクラウドサービス

JSSA システム監査学会

# Society5.0の目指す社会

サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムで経済発展と社会的課題の解決を両立する、人間中心の新たな価値




**/断片情報/人**

**/リアルタイム/AI**

(出所) 内閣府, Society5.0 経済発展と社会的課題の解決を両立するSociety 5.0へ, 内閣府. (オンライン) (引用日: 2020年5月31日.)
https://www8.cao.go.jp/cstp/society5_0/

JSSA システム監査学会

# Society 5.0を支えるインフラストラクチャの要件

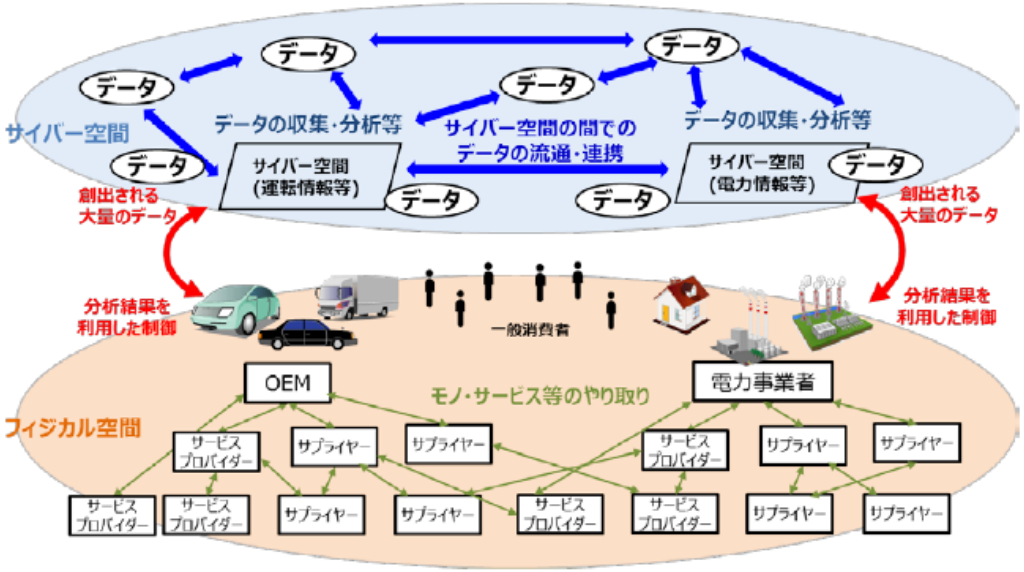



図 i-2 「Society5.0」社会におけるモノ・データ等のつながりのイメージ

- ✓ 部分的ではなく**全体的な対応を通じた信頼性**（trustworthiness）を確保することが必要
- ✓ 情報のデジタル化**機能の信頼性の確保**や大量のデータの正確性・流通・連携を支える**セキュリティ対策**も重要な課題

(出所) 経済産業省サイバーセキュリティ課,サイバー・フィジカル・セキュリティ対策フレームワーク, 経済産業省. (オンライン) (引用日: 2020年5月31日.), 11 https://www.meti.go.jp/press/2019/04/20190418002/20190418002-2.pdf, 図i-2, pp.2-3.

JSSA システム監査学会

# クラウドにおけるセキュリティ脅威

Cloud Security Alliance 11の悪質な脅威 (2019年)

1. データ侵害
2. 設定ミスと不適切な変更管理
3. クラウドセキュリティアーキテクチャと戦略の欠如
4. ID、資格情報、アクセス、鍵の不十分な管理
5. アカウントハイジャック
6. 内部者の脅威
7. 安全でないインターフェースとAPI
8. 弱い管理プレーン
9. メタストラクチャとアプリストラクチャの障害
10. クラウド利用の可視性の限界
11. クラウドサービスの悪用・乱用・不正利用

**事業継続性が侵されるリスク**

**利用者とCSP双方の経営課題**



出所) Cloud Security Alliance, クラウドの重大セキュリティ脅威　11の悪質な脅威 2019 日本語版. 日本クラウドセキュリティアライアンス. (オンライン) (引用日: 2020年5月31日) https://www.cloudsecurityalliance.jp/site/wp-content/uploads/2019/10/top-threats-to-cloud-computing-egregious-eleven_J_20191031.pdf

JSSA システム監査学会

# セキュリティ・プライバシーに係る主な法・規制・制度

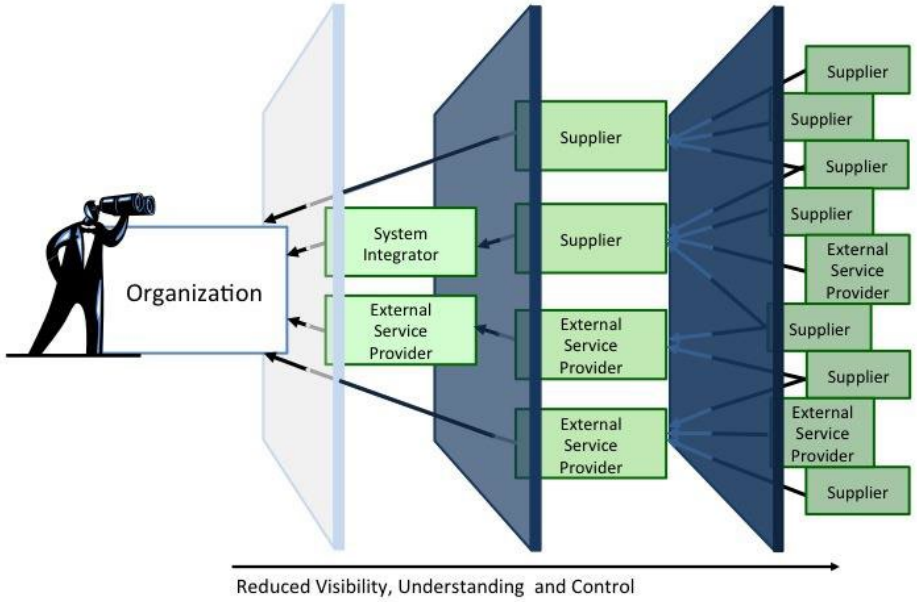
**主なクラウドサービスに係る法・規制・制度・ガイドラインの動向**

| 区分 | 国 | 名称 | 概要 |
|---|---|---|---|
| セキュリティ |  | **ISMAP** | 政府クラウドサービス調達制度。**情報セキュリティガバナンス、セキュリティマネジメント、1000を超えるセキュリティ管理策の基準の対応と監査を要件**。2020年度開始。 |
| |  | **CPSF** | 経済産業省のサイバー・フィジカル・セキュリティ対策フレームワーク。Society5.0の実現に向けた求められるセキュリティ対策の全体像とセキュリティ対策例を明示 |
| |  | **NIST CSF** | サイバーセキュリティフレームワーク。グローバルでの**サイバーセキュリティの推奨ベースライン**として広く普及 |
| |  | **NIST SP 800-53** | 連邦政府情報システムのセキュリティ管理策。米国**FedRAMP**をはじめ、各国が参照する具体的な**808のセキュリティ管理策**で構成 |
| プライバシー |  | **改正個人情報保護法** | 個人情報を取り扱う全ての事業者に、データの取得から消去に至る**データ保護原則**を義務付け |
| |  | **GDPR** | EU一般データ保護規則。**個人データを収集・処理する事業者に対する義務**を定義。違反時は全世界売上高4%又は2000万ユーロの制裁金 |
| 業界・業種 |  | **(金融) FISC 安全対策基準** | FISC安全対策基準第9版令和2年3月版。**金融情報システム**の**外部委託先の統制**と**ITガバナンス**に基づくリスクベースアプローチを強化 |
| |  | **(医療) 3省2ガイドライン** | 厚労省・総務省・経産省によるCSPを含む**医療情報取り扱い事業者**向けガイドライン。患者情報等の個人情報に求められる品質等を定義 |

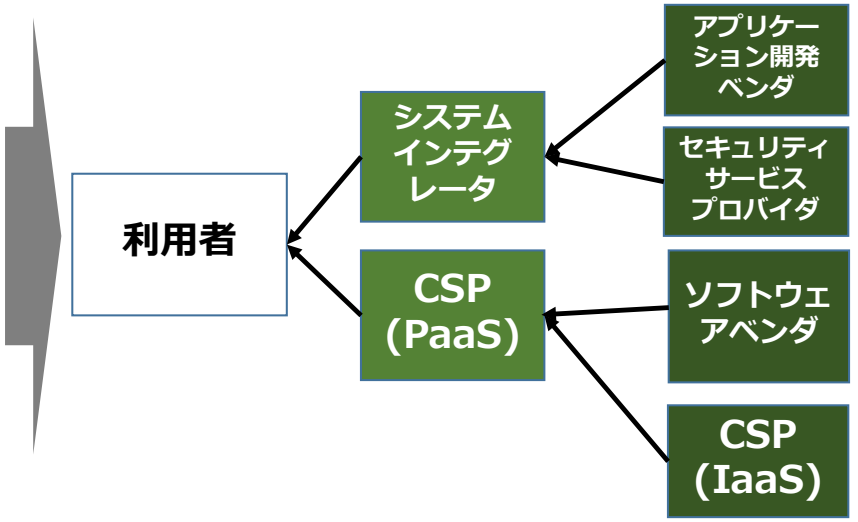
JSSA システム監査学会

# サプライチェーンリスク

サービスをインテグレーションする利用形態が普及、経済産業省やIPAの調査においても、サプライチェーンの弱点(海外拠点・取引先等)を悪用した攻撃が増加




クラウドサービスのサプライチェーン (例)




(出所) 経済産業省, 昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性について, 2020年6月12日 (オンライン)
National Institute of Standards and Technology, NIST Special Publication 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations, NIST. (オンライン) (引用日: 2020年 5月31日.), https://csrc.nist.gov/publications/detail/sp/800-161/final

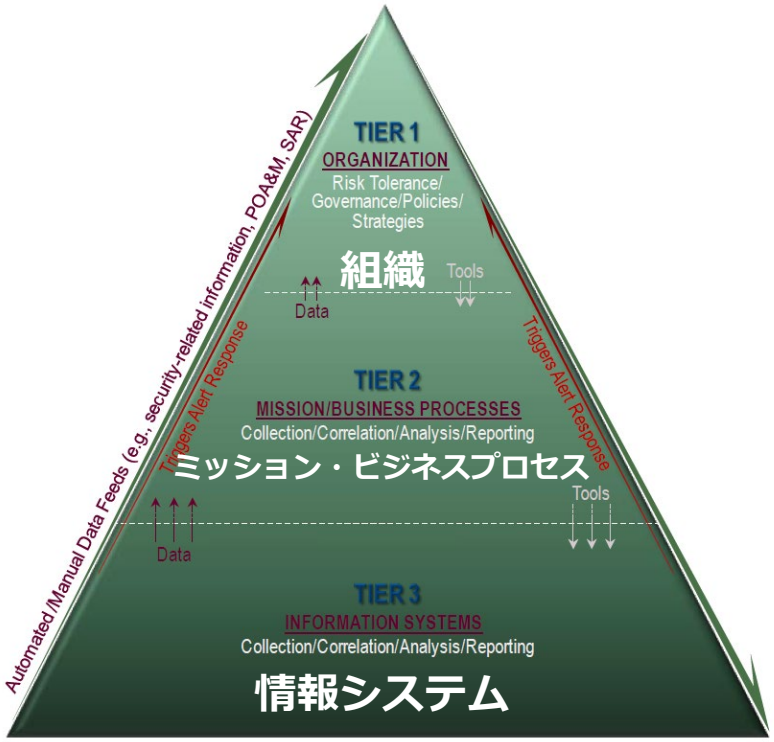
JSSA システム監査学会

# CSPが焦点をあてて取り組むべきこと

## ①継続的モニタリングによる意思決定

JSSA システム監査学会

# 継続的モニタリングとは




- Information Security Continuous Monitoring (NIST SP800-137)

  ***Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.***

  セキュリティ管理策、脆弱性および脅威の意識を持ち続ける ことによって**リスク管理上の意思決定をサポート**すること

- 事業体の価値 (COSO 全社的リスクマネジメント)
  事業体の価値は、全体的な戦略の決定から日々の意思決定まで、**経営者が行う意思決定を通じてそのほとんどが決定**される。それらの意思決定により、価値が創造されるか、維持されるか、実現されるか、あるいは損なわれるかが確定することになる

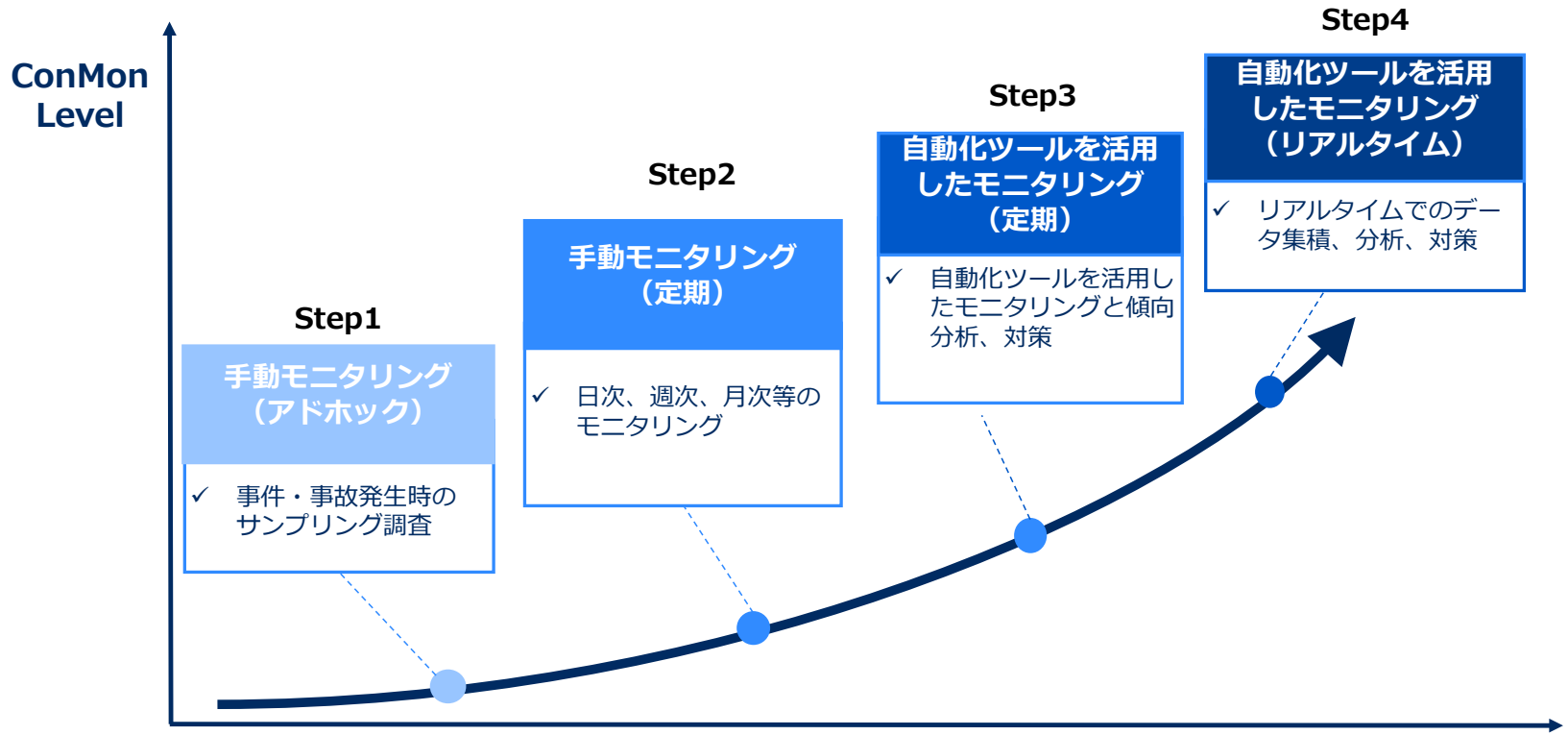
出所)

オンライン) (引用日: 2020年5月31日.), https://csrc.nist.gov/publications/detail/sp/800-137/final p.8
, 2018, COSO 全社的リスクマネジメント-戦略およびパフォーマンスとの統合-, 同文舘出版, p.36

JSSA システム監査学会

# 継続的モニタリングの強化ステップ

Society5.0時代には、人海戦術による主導モニタリングから、**自動化メカニズムによるリアルタイム・モニタリング**が求められていく




(出所) 経済産業省,GOVERNANCE INNOVATION, 経済産業省. (オンライン) (引用日: 2020年5月31日.), https://www.meti.go.jp/press/2019/12/20191226001/20191226001-3.pdf p.37等を参考に発表者作成

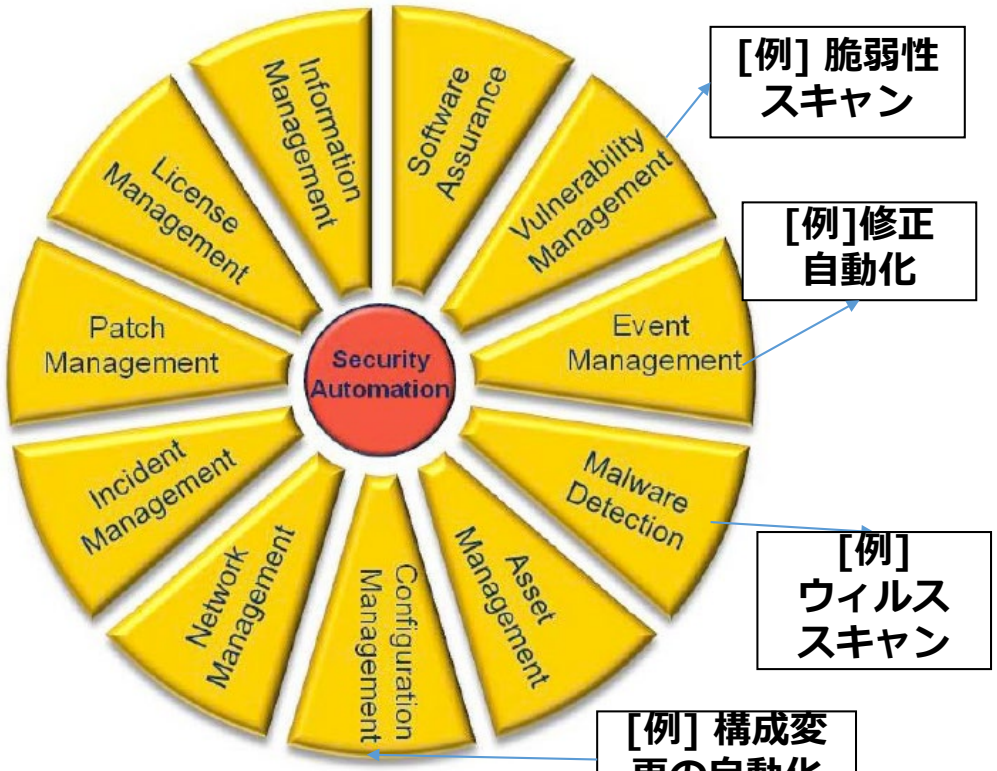
JSSA システム監査学会

# 継続的モニタリングを支える自動化

## 自動化の背景

- ✓頻繁なAP開発・変更要請
- ✓セキュリティ脅威とスピード
- ✓複雑なアーキテクチャー
- ✓膨大なデータギャザリング
- ✓意思決定のための可視化
- ✓サービスの品質強化・維持

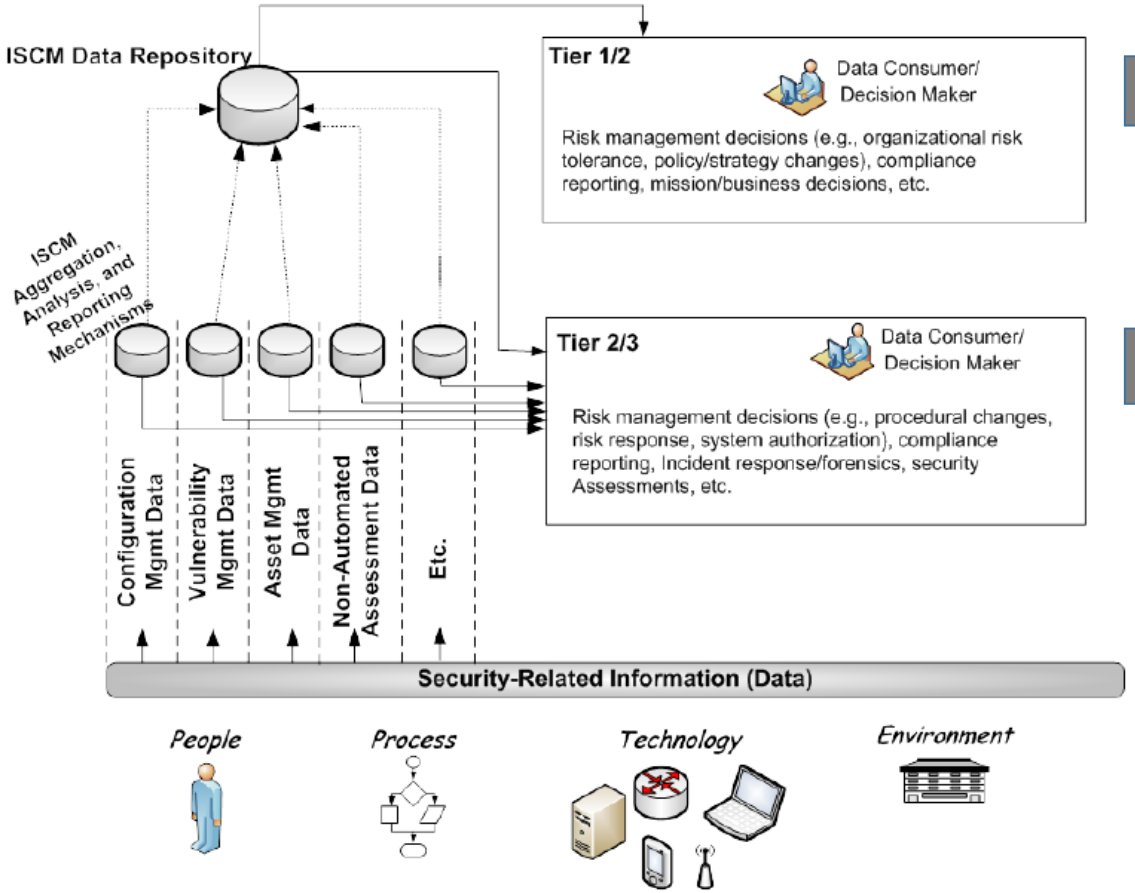
## 継続的モニタリングを支える11の自動化対象領域




(出所) National Institute of Standards and Technology, NIST Special Publication 800-137 Information Security Continuous Monitoring for Federal Information Systems and Organizations, NIST. (オンライン) (引用日: 2020年5月31日.), https://csrc.nist.gov/publications/detail/sp/800-137/final p.D-4.

JSSA システム監査学会

# 継続的モニタリングによる意思決定




**組織レベルの意思決定**
- ✓リスク選好の変更
- ✓ポリシー・戦略の変更 等

**プロセスレベルの意思決定**
- ✓ リスク対応
- ✓ 手順の変更
- ✓ システムの変更承認 等

出所) National Institute of Standards and Technology, NIST Special Publication 800-137 Information Security Continuous Monitoring for Federal Information Systems and Organizations, NIST. (オンライン) (引用日: 2020年5月31日.), https://csrc.nist.gov/publications/detail/sp/800-137/final p. D-8

JSSA システム監査学会

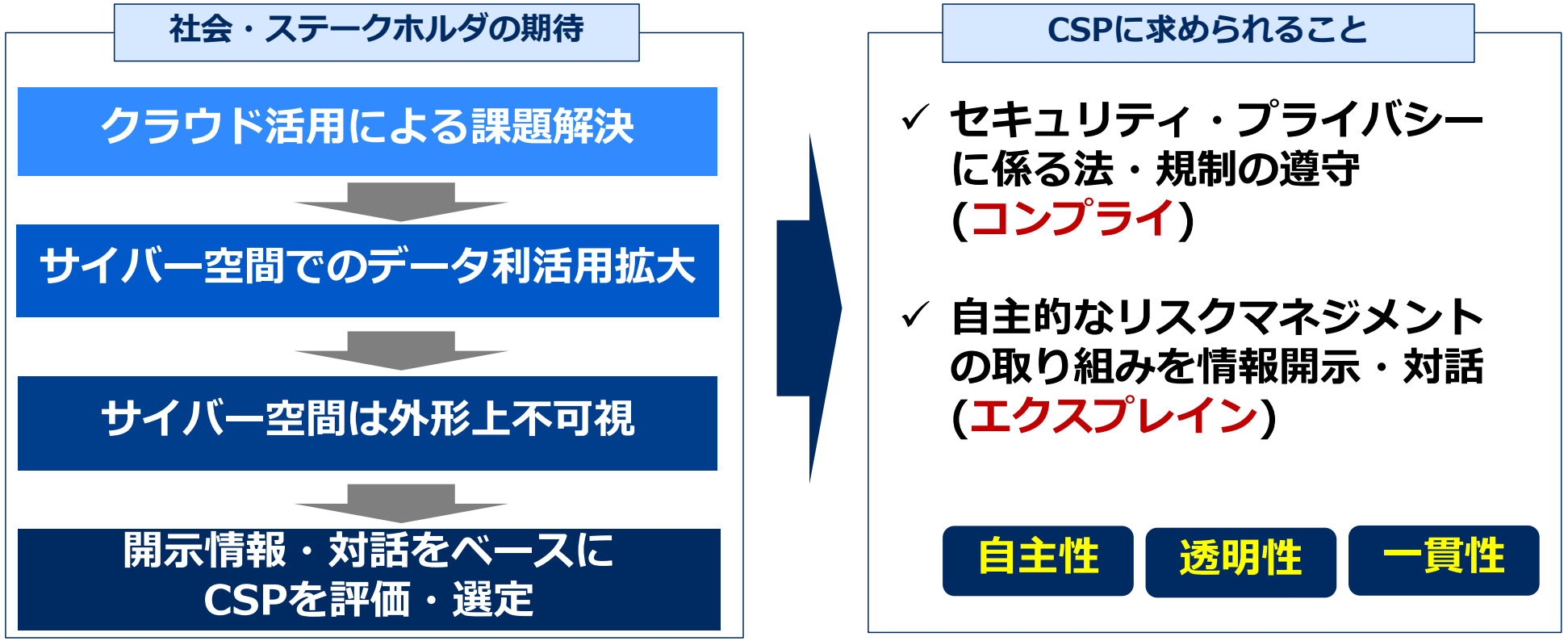
# CSPが焦点をあてて取り組むべきこと

# ②コンプライ＆エクスプレインと独立した保証

JSSA システム監査学会

# コンプライ＆エクスプレインとは

CSPには、法令遵守を前提としながら、自主的な組織のリスクマネジメントへの取り組みの情報開示・対話が一層求められていくことが想定される

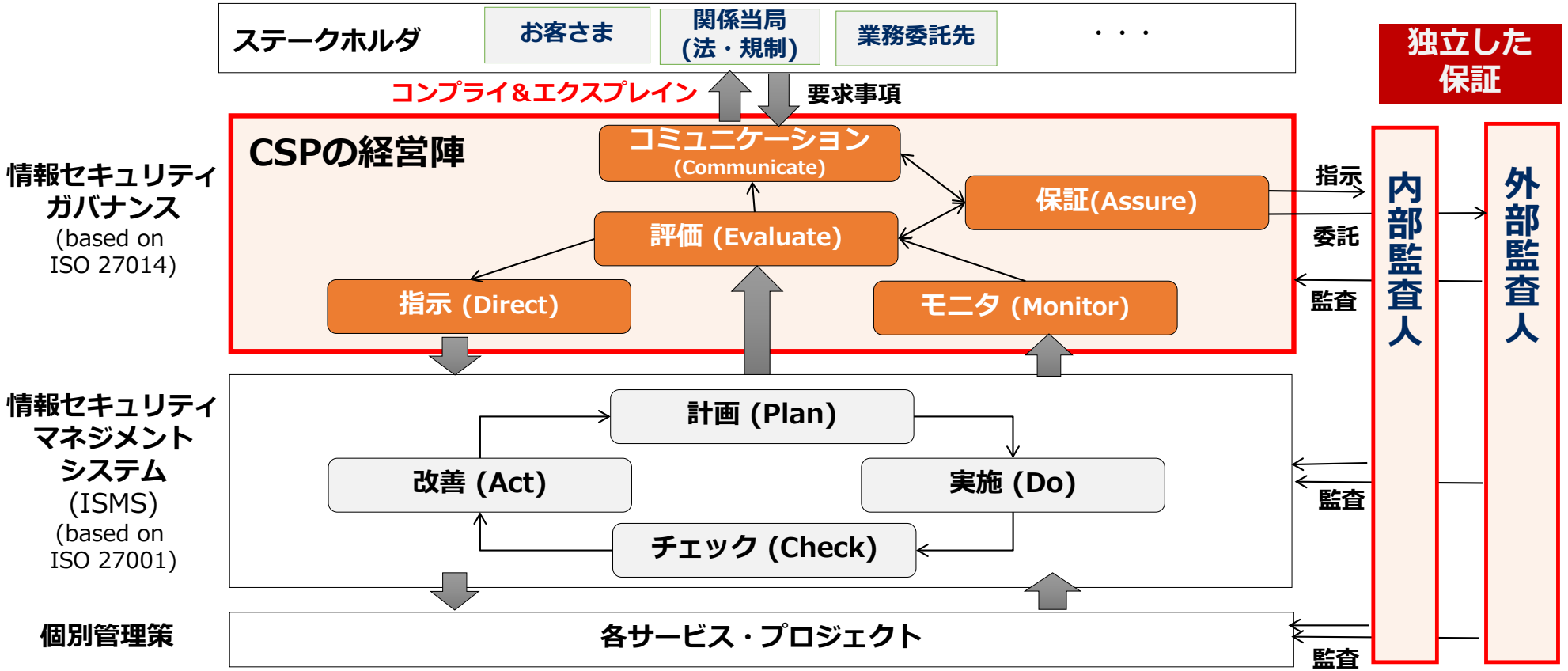



参考) 経済産業省,GOVERNANCE INNOVATION, 経済産業省. (オンライン) (引用日: 2020年10月11日.), https://www.meti.go.jp/press/2020/07/20200713001/20200713001-1.pdf

JSSA システム監査学会

# コンプライ＆エクスプレインを支える独立した保証

情報セキュリティガバナンスにおける保証のイメージ




(出所) ISO, ISMAP等を参考に発表者作成

JSSA システム監査学会

# 業務受託会社の保証報告

## System and Organization Controls(SOC)報告書

| | | 財務報告に係る内部統制 | 財務報告に関連しない領域を含む内部統制 | |
|---|---|---|---|---|
| | | SOC 1 | SOC 2 | SOC 3 |
| 報告書の主題 | | 委託会社の財務報告に係る受託会社の内部統制 | 受託業務における受託会社の以下の項目（トラストサービス基準）に係る内部統制<br>セキュリティ、機密保持、可用性、プライバシー、処理のインテグリティ | |
| 検証の基準 | 国際 | ISAE3402 | ISAE3000 | ISAE3000 |
| | 米国 | SSAE18（AT-C sec.105・205・320） | SSAE18（AT-C sec.105・205） | SSAE18（AT-C sec.105・205） |
| | 日本 | 監査基準委員会実務指針第86号 | IT委員会実務指針第7号 | IT委員会実務指針第2号 |
| 報告書の構成 | | タイプ1：受託業務に係るシステムの記述、並びに内部統制のデザインの適切性に関する報告書　または<br>タイプ2：受託業務に係るシステムの記述、並びに内部統制のデザインの適切性および運用状況の有効性に関する報告書（内部統制のテスト手続きおよびテスト結果を含む） | | 概要報告書のみ |
| 再委託会社の扱い | | 業務受託会社の記述書は、下記いずれの方式も採用可能<br>(a)除外方式　(b)一体方式　（但し除外方式の場合でも、再受託会社のサービスの性質の情報を提供する） | | 無限定適正意見を受けるためには、重要なすべての再受託会社の内部統制を含む必要があるが、委託会社の重要な内部統制は含まれてはならない。 |
| 意図されている報告書の利用者 | | • 受託会社の経営者<br>• 委託会社とその会計監査人 | • 受託会社の経営者<br>• 受託会社<br>• その他受託業務の内容や適用される規準等を理解したい企業、団体等 | ・不特定多数の利用者 |

(出所) デロイトトーマツグループ, SOC報告書の種類,デロイトトーマツ, (オンライン) (引用日: 2020年5月31日.), https://www2.deloitte.com/jp/ja/pages/risk/articles/or/soc-type.html

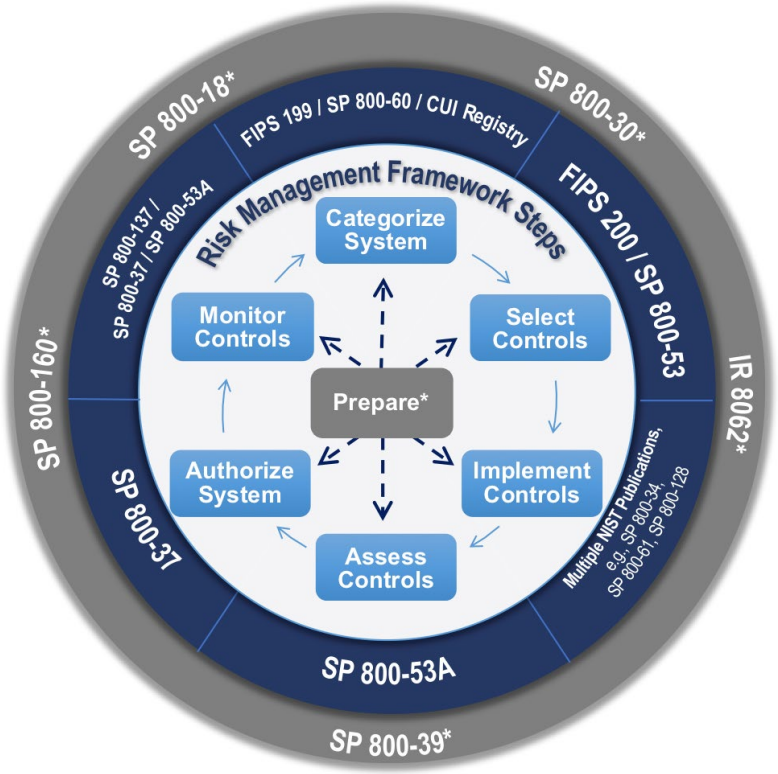
JSSA システム監査学会

# CSPが焦点をあてて取り組むべきこと

# ③リスクマネジメントを実現する組織設計

JSSA システム監査学会

# NIST リスクマネジメントフレームワーク (RMF)




セキュリティ及びプライバシーのためのシステムライフサイクルアプローチ (NIST SP 800-37 Rev2)

| ステップ | 主要ドキュメント |
|---|---|
| 1. 情報システムの**分類** | |
| 2. セキュリティ管理策の**選択** | |
| 3. セキュリティ管理策の**実施** | **システムセキュリティ計画 (SSP)** |
| 4. セキュリティ管理策の**評価** | セキュリティ評価レポート (SAR) |
| 5. 情報システムの**運用認可** | |
| 6. セキュリティ管理策の**監視** | **行動計画とマイルストーン (POA&M)[1]** |

行動計画とマイルストーン: CSPが作成・維持する、評価やモニタリングで発見された不備、脆弱性、欠陥とその改善計画の詳細を記述した文書



(出所) National Institute of Standards and Technology, NIST Special Publication 800-37 Rev. 2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, 2016, NIST. (オンライン) (引用日: 2020年 5月31日.), https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/finalをベースに発表者作成

JSSA システム監査学会

| フレームワーク | IIA Three Lines Model | NIST SP 800-37 rev.2 | COBIT®2019 |
|---|---|---|---|
| 着眼点 | アシュアランス | セキュリティ&プライバシー | I&Tガバナンス |
| 統治機関 | | | 取締役会 |
| 最高経営者 | | HEAD OF AGENCY | 最高経営責任者(CEO) |
| N/A | | AUTHORIZING OFFICIAL<br>CHIEF INFORMATION OFFICER | 最高情報責任者(CIO)<br>最高財務責任者(CFO)<br>最高デジタル責任者(CDO) |
| 第1ライン | 業務とリスク管理 | SYSTEM OWNER<br>INFORMATION OWNER<br>MISSION OR BUSINESS OWNER<br>SYSTEM ADMINISTRATOR | ビジネスプロセスオーナー<br>開発責任者<br>IT運用責任者<br>IT管理責任者<br>サービスマネージャ<br>データ管理部門<br>プロジェクトマネージャ |
| 第2ライン | コンプライアンス | | 法務顧問 |
| | セキュリティ | SENIOR AGENCY INFORMATION SECURITY OFFICER<br>SYSTEM SECURITY OR PRIVACY OFFICER | 情報セキュリティマネージャ<br>プライバシー責任者 |
| | リスクマネジメント | SENIOR ACCOUNTABLE OFFICIAL FOR RISK MANAGEMENT | プロジェクトマネジメントオフィス |
| | 品質保証 | | |
| | 内部統制 | | |
| | 持続可能性 | | 事業継続マネージャ |
| | N/A | | |
| 第3ライン | 内部監査 | CONTROL ASSESSOR | 監査 |
| 外部のアシュアランス提供者 | | CONTROL ASSESSOR | |

**＋ビジネスモデル**
**＋他標準・フレームワーク**

**ITIL®4**
**SIAM®**
**VeriSM™**

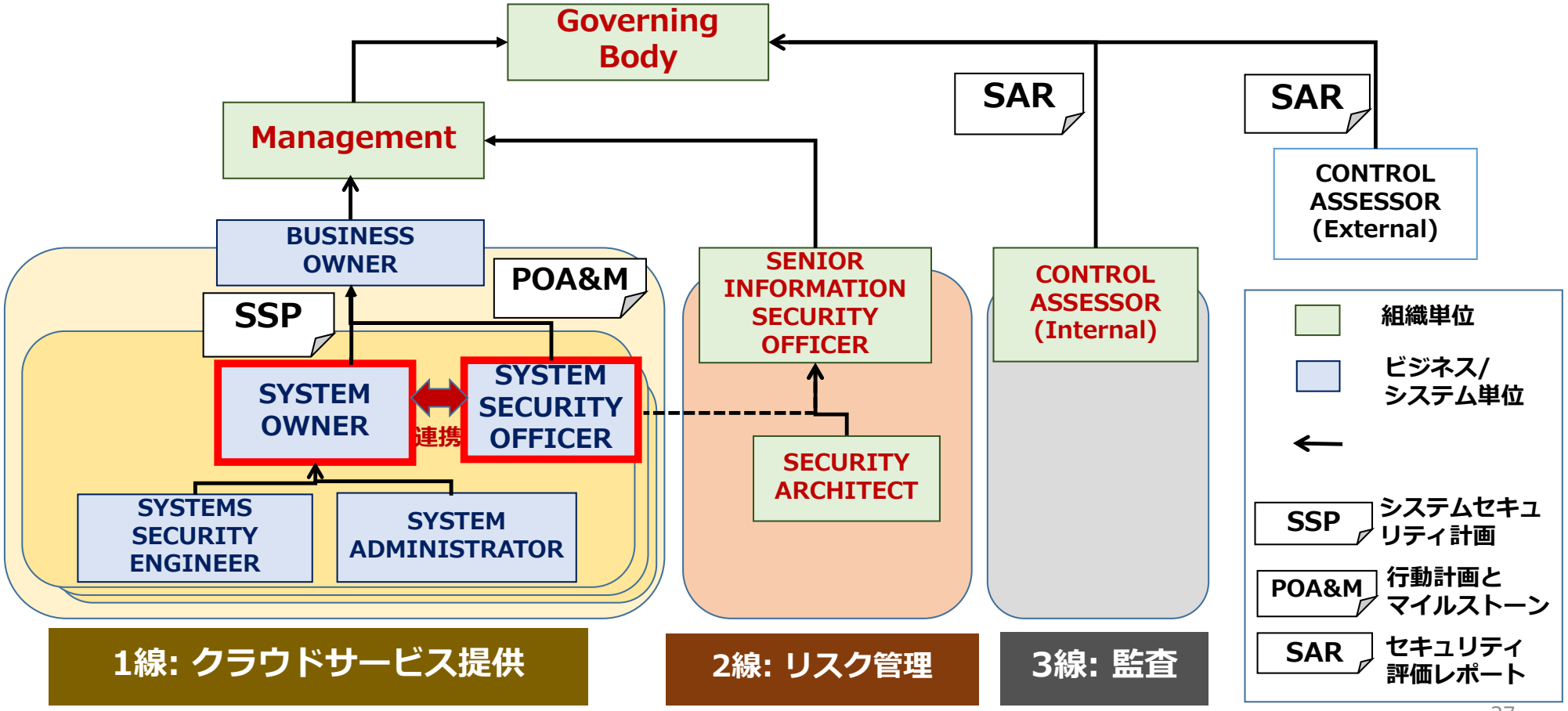
**自組織の役割定義のインプット**

(出所) IIA, The IIA's New Three Lines Model An update of the Three Lines of Defense, IIA. (オンライン) (引用日: 2020年8月17日)
https://na.theiia.org/about-us/about-ia/Pages/Three-Lines-Model.aspx 等をベースに発表者作成

JSSA システム監査学会

# 役割と責任の割り当て

リスクマネジメントを実現するサービス提供組織 (イメージ)




(出所) IIA 3ラインモデル、NIST SP800-37に基づき発表者作成

JSSA システム監査学会

# システム監査人の役割とトラストチェーン

JSSA システム監査学会

# Society5.0時代のシステム監査人の役割

内部監査人を想定

## 1. 独立した客観的な保証を担う
✓第３のラインとして統制を評価
✓自動/リアルタイム/AIを活用した技術的統制の評価

## 2. サプライヤーの言明を翻訳する
✓サプライヤーの統制を理解し、自社ポリシーと照合・評価・伝達
✓CSPとクラウド利用者のセキュリティ責任共有モデルの理解

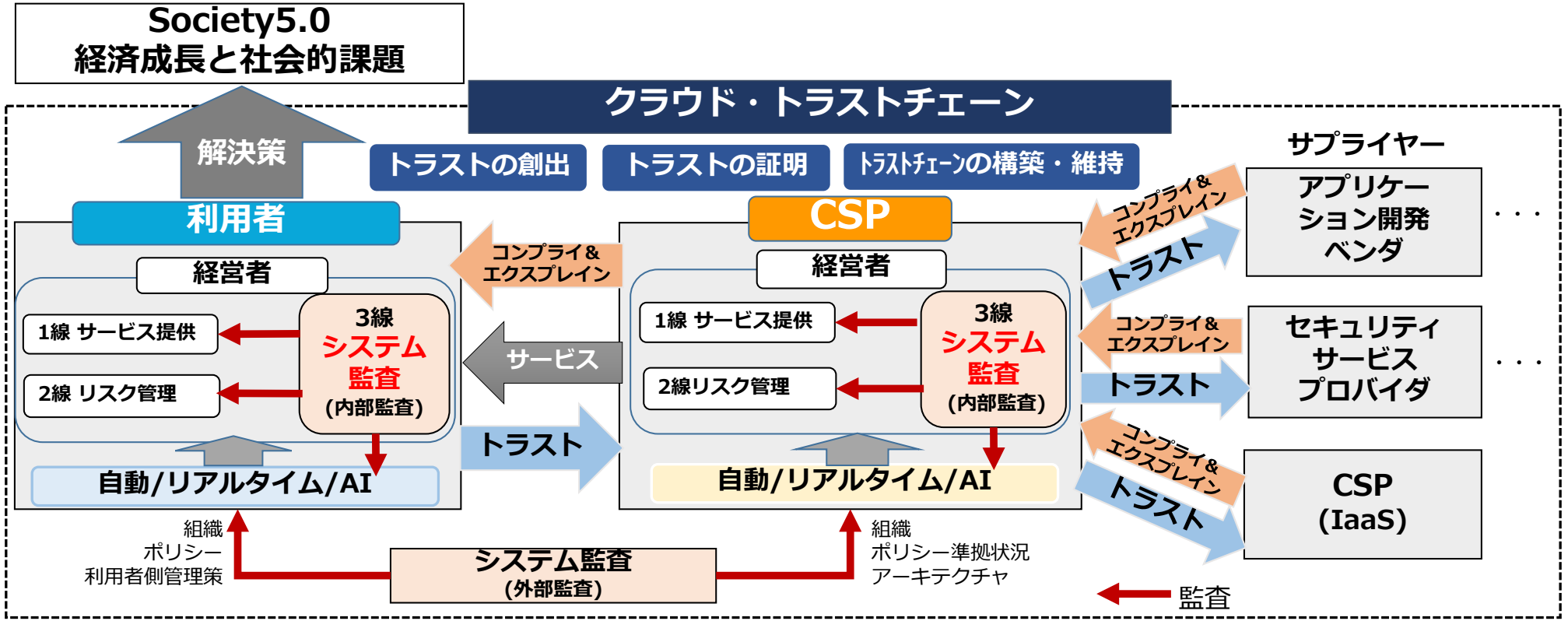
## 3. 組織内外の重要な変化を嗅ぎ取る
✓リスク、法・規制・標準、技術、ステークホルダのニーズに係る重要な変化をいち早く察知

**継続的モニタリング、コンプライ＆エクスプレインに貢献**

JSSA システム監査学会

# 目指す姿: クラウド・トラストチェーン

コンプライ&エクスプレインとその保証をサプライチェーン全体で実現していくことにより、トラストの創出・証明・構築・維持につなげていく




(参考) 経済産業省　商務情報政策局　サイバーセキュリティ課, サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の概要, 平成31年4月18日, 経済産業省 (オンライン) (引用日: 2020年5月31日) https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

JSSA システム監査学会

natsuhiko@nec.com

JSSA システム監査学会

# Appendix

JSSA システム監査学会

# クラウドコンピューティングの定義

クラウドコンピューティングの定義 (NIST SP 800-145)


- ✓ **共用**の構成可能なコンピューティングリソース[1]の集積に
- ✓ **どこからでも、簡便に、必要に応じて、ネットワーク経由でアクセス**することを可能とするモデルであり
- ✓ 最小限の利用手続きまたはサービスプロバイダとのやりとりで**速やかに**割り当てられ提供される

コンピューティングリソース: ネットワーク、サーバ、ストレージ、アプリケーション、サービス

(出所) Cloud Security Alliance 「クラウドコンピューティングのためのセキュリティガイダンス（第4版）」日本語版. 日本クラウドセキュリティアライアンス. (オンライン) (引用日: 2020年5月31日.) https://cloudsecurityalliance.jp/j-docs/CSA_Guidance_V4.0_J_V1.1_20180724.pdf, p.12.

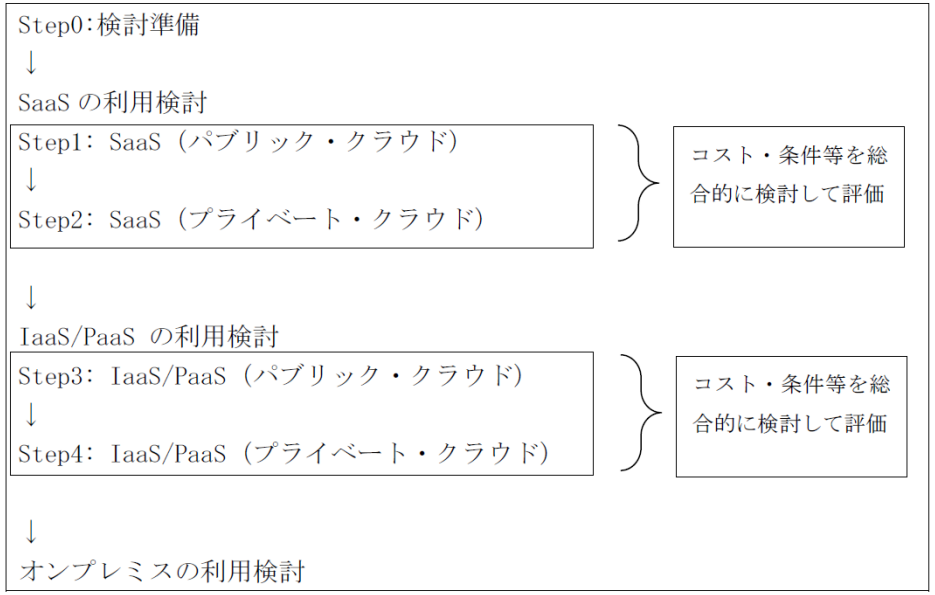
JSSA システム監査学会

# インフラストラクチャはクラウド中心に

政府情報システムは、**クラウドサービスの利用を第一候補**として検討
(「政府情報システムにおけるクラウドサービスの利用に係る基本方針」より)

**クラウドのメリット**

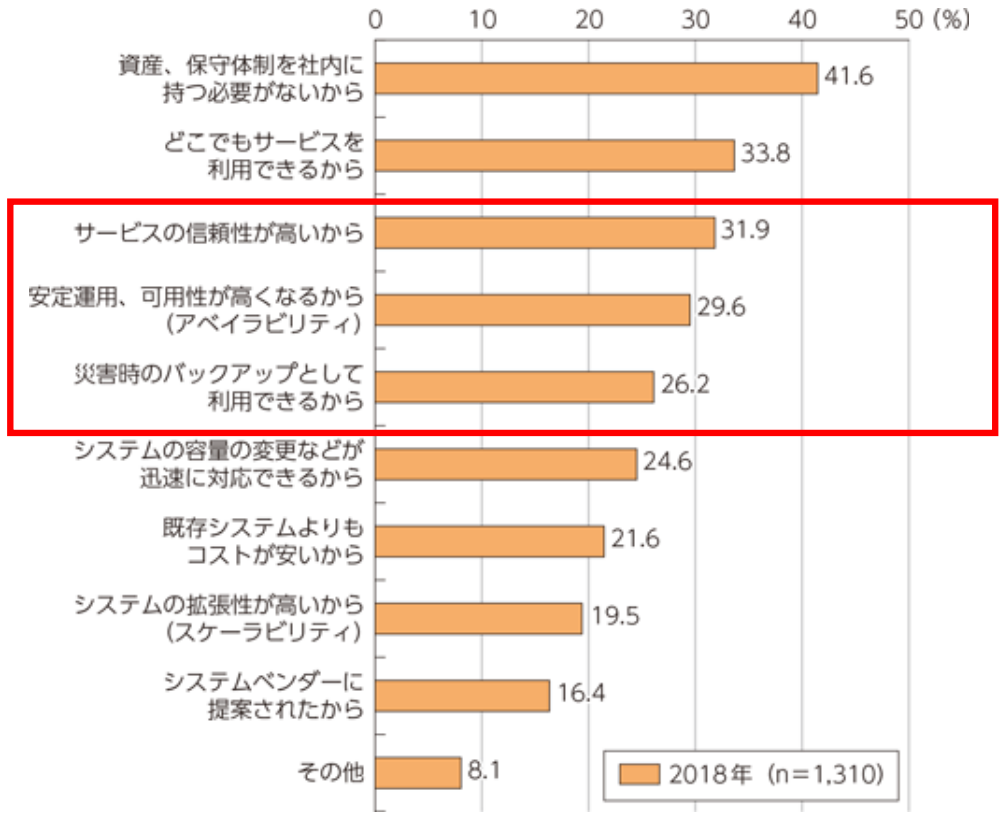
1. **効率性**の向上
2. **セキュリティ水準**の向上
3. **技術革新対応力**の向上
4. **柔軟性**の向上
5. **可用性**の向上




(出所)各府省情報化統括責任者(ＣＩＯ)連絡会議決定, 政府情報システムにおけるクラウドサービスの利用に係る基本方針, 2018年(平成30年)6月7日, 政府CIOポータル. (オンライン) (引用日: 2020年5月31日) https://cio.go.jp/sites/default/files/uploads/documents/cloud_%20policy.pdf pp.3-7.

JSSA システム監査学会

クラウドサービスを利用している理由 (2018年)




(出所) 総務省, 令和元年度版 情報通信白書, 総務省. (オンライン) (引用日: 2020年5月31日)
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r01/html/nd232140.html

**クラウドサービス利用**
**58.7%** (n=2,107)

**導入効果あり**
**83.2%** (n=1,302)

**安心・安全のため利用**

JSSA システム監査学会

# サイバー攻撃の高度化

大企業から中小企業まで、**サプライチェーンの弱点**を狙ったサイバー攻撃が顕在化・高度化
2020年1月以降、国内の複数の**防衛**関連の大企業に対する高度なサイバー攻撃が発生

- **サイバー攻撃による昨今の被害の特徴**
  - **標的型攻撃の更なる高度化**
    - マルウェア添付に加え、ユーザ動作を介さない侵入手法
  - **サプライチェーンの弱点への攻撃**
    - 海外拠点や取引先等セキュリティが弱い組織が攻撃起点
  - **不正ログイン被害の継続的な発生**
    - リスト型攻撃による不正ログインが継続的に発生

**IPA 情報セキュリティ10大脅威2020 (組織向け)**

| 順位 | 脅威 |
|---|---|
| 1 位 | 標的型攻撃による機密情報の窃取 |
| 2 位 | 内部不正による情報漏えい |
| 3 位 | ビジネスメール詐欺による金銭被害 |
| 4 位 | サプライチェーンの弱点を悪用した攻撃 |
| 5 位 | ランサムウェアによる被害 |
| 6 位 | 予期せぬ IT 基盤の障害に伴う業務停止 |
| 7 位 | 不注意による情報漏えい（規則は遵守） |
| 8 位 | インターネット上のサービスからの個人情報の窃取 |
| 9 位 | IoT 機器の不正利用 |
| 10 位 | サービス妨害攻撃によるサービスの停止 |

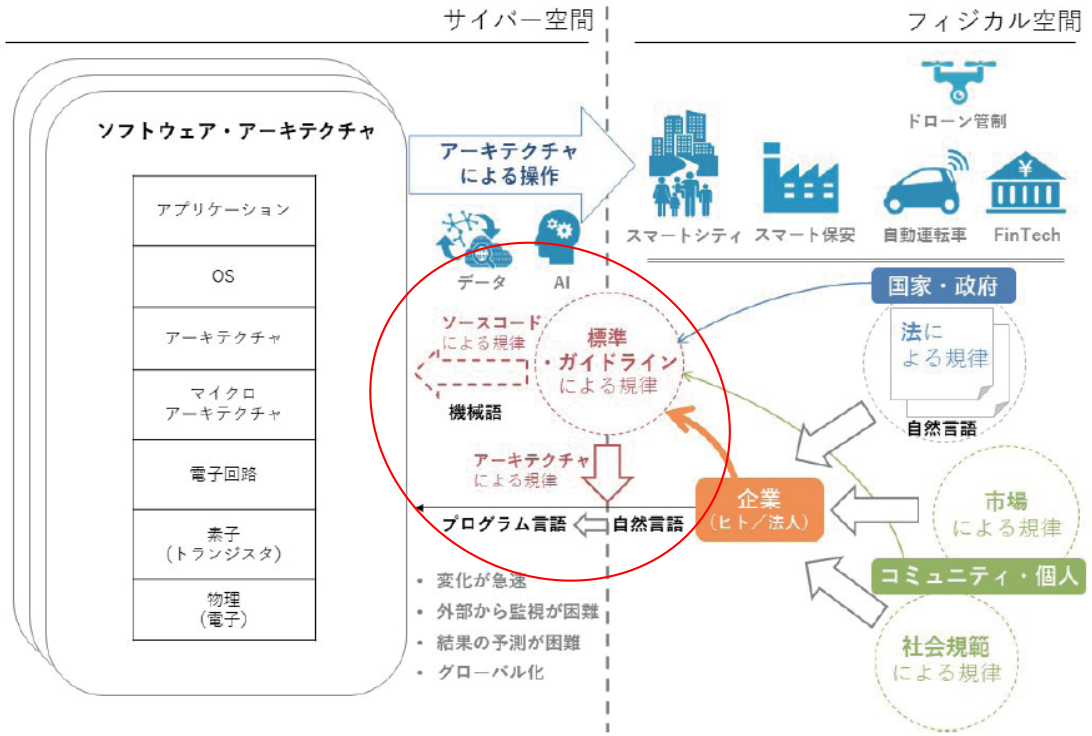
**局所的な技術的対策に加えて、組織的なサイバーセキュリティ対策がMUSTに**

(出所) 経済産業省, 昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性について, 2020年6月12日 (オンライン)

JSSA システム監査学会

# ガバナンス構造の変化

## ソフトウェアへの依存＝アーキテクチャ（ソースコード）がフィジカル空間をコントロール




**/断片情報/人**

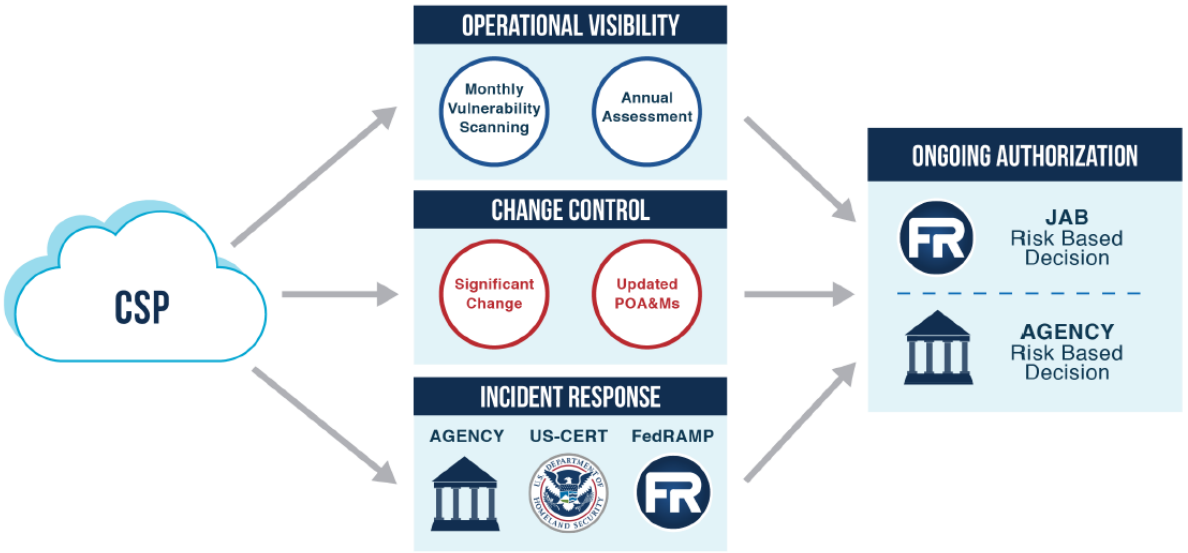
**/リアルタイム/AI**

(参考) 経済産業省,GOVERNANCE INNOVATION, 経済産業省. (オンライン) (引用日: 2020年10月11日.), https://www.meti.go.jp/press/2020/07/20200713001/20200713001-1.pdf

JSSA システム監査学会

# FedRAMPの継続的モニタリング

米国政府のクラウド調達プログラム (FedRAMP)の継続的モニタリングは、**運用の可視化**、**変更の統制**、**インシデント対応**の3要素から構成




- **Operational Visibility**
  **運用の可視化**
  - 月次の脆弱性スキャン
  - 年次のアセスメント
- **Change Control**
  **変更の統制**
  - 重要な変更の伝達
  - POA&Msの更新
- **Incident Response**
  **インシデント対応**

(出所) FedRAMP, SECURITY ASSESSMENT FRAMEWORK Version 2.4 Nov. 15, 2017, FedRAMP. (オンライン) (引用日: 2020年5月31日)
https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Assessment_Framework.pdf Figure 3

JSSA システム監査学会

# 自動化に関する要求事項の例（NIST SP 800-53 rev.4）

**CM-3 構成変更管理 - (3) 変更を自動で実施する**

- ✓ 組織は、現在の情報システムベースラインに対する変更を実施するための**自動化されたメカニズム**を使用し、更新されたベースライン管理策を設置基盤に展開する。

**CM-5 構成変更管理 - (5) 自動化されたセキュリティレスポンス**

- ✓ ベースライン構成が不正に変更された場合に、情報システムが［組織が定めたセキュリティレスポンス］を自動的に実施する。

**RA-5 脆弱性スキャン**

- ✓ 組織は、脆弱性スキャンツールと技法を用いる。それらはツール間の相互運用を容易にし、以下を満たす標準を使用することによって、**脆弱性管理プロセスの一部を自動化**できることが求められる：
  - プラットフォーム、ソフトウェアの欠陥、および誤った設定を列挙する
  - チェックリストとテスト手順をフォーマットする
  - 脆弱性による影響を評価する

**SI-2 欠陥の修正 - (5) 自動化されたソフトウェア/ ファームウェアアップデート**

- ✓ 組織は、［指定：組織が定めた情報システムコンポーネント］に［指定：組織が定めた、セキュリティ関連のソフトウェアアップデートやファームウェアアップデート］を自動でインストールする。

**SI-4 情報システムのモニタリング - (2)リアルタイム分析のための自動化されたツール**

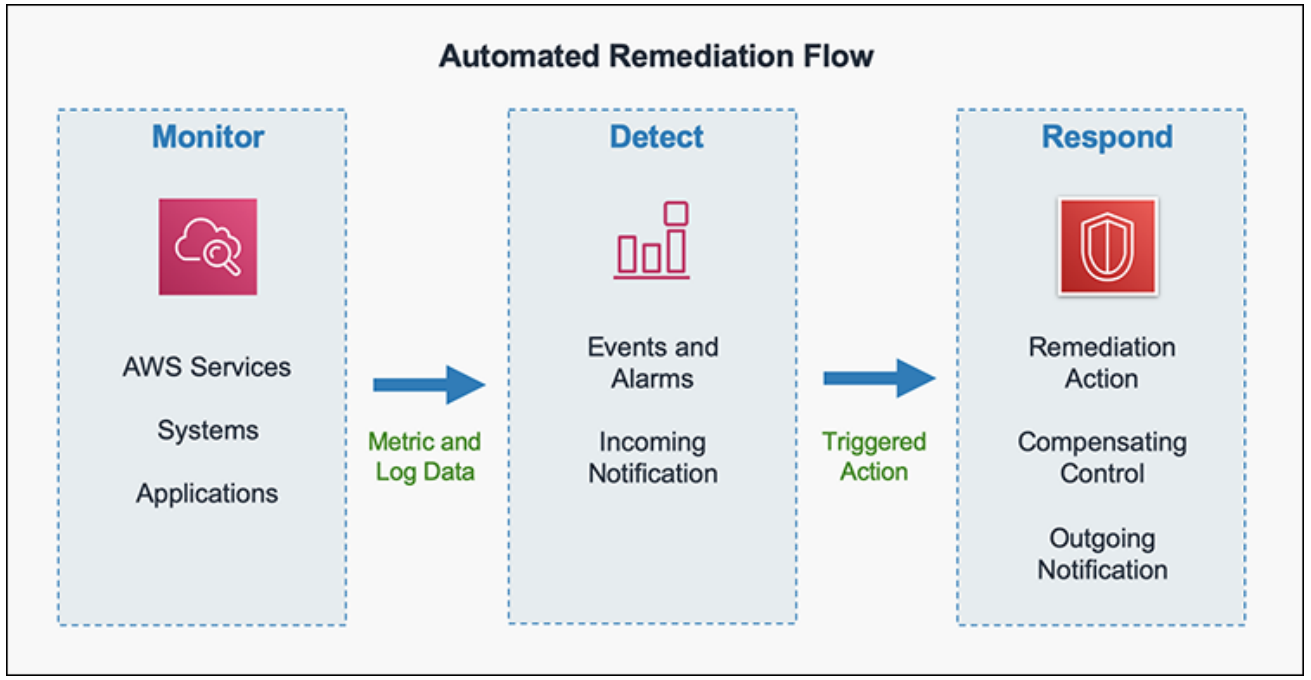
- ✓ 組織は、イベントのリアルタイムに近い分析を支援する自動化されたツールを使用する

出所) National Institute of Standards and Technology, NIST Special Publication 800-53 rev.4, 連邦政府情報システム および連邦組織のためのセキュリティ管理策とプライバシー管理策 , IPA. (オンライン) (引用日: 2020年5月31日.), https://www.ipa.go.jp/files/000056415.pdf

JSSA システム監査学会

# [自動化例] イベント・ドリブンでの修正自動化 (AWS)

モニタリングにより検知された**イベントをトリガー**に、修正のためのアプリケーションコードを自動で実行

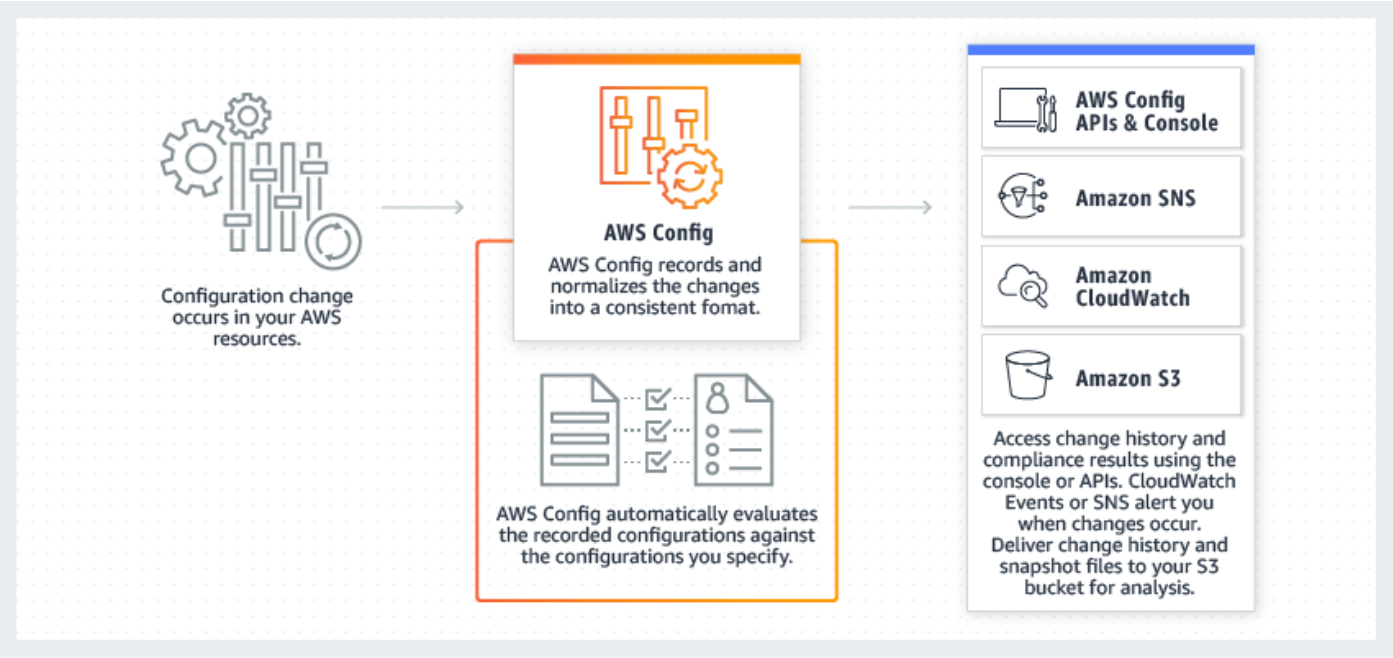



（出所）Amazon Web Servicesブログ, AWS 環境でセキュリティレスポンスの自動化を始める方法, AWS. (オンライン) (引用日: 2020年5月31日.), https://aws.amazon.com/jp/blogs/news/how-get-started-security-response-automation-aws/

JSSA システム監査学会

# [自動化例] 構成変更の評価自動化 (AWS)

ベースライン構成の変更を検知し、事前に設定済の**ルール**で評価、アラートの発行や変更履歴をストレージへ保存
ルール設定のためのAWS Config Rule Development Kit (RDK) も公開

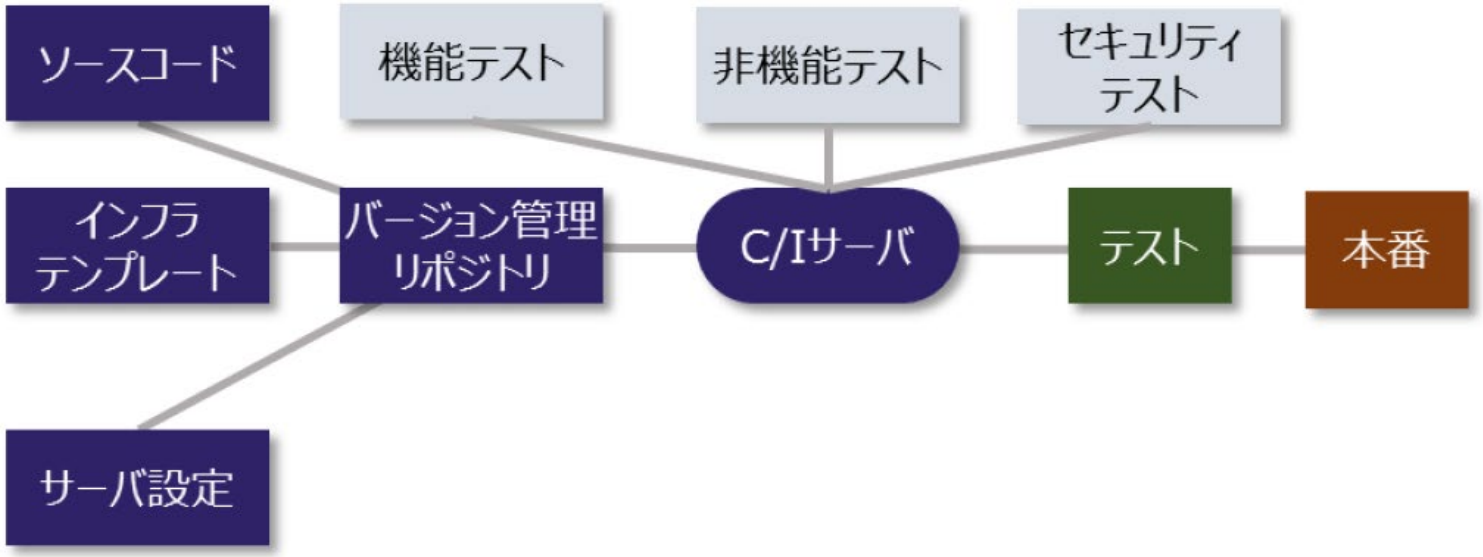



) Amazon Config, AWS リソースの設定を記録して評価, AWS. (オンライン) (引用日: 2020年5月31日.),

JSSA システム監査学会

# [自動化例] 開発・変更プロセスの自動化 (CI/CD)

Continuous Deployment パイプライン




(出所) Cloud Security Alliance 「クラウドコンピューティングのためのセキュリティガイダンス（第4版）」日本語版. 日本クラウドセキュリティアライアンス. (オンライン) (引用日: 2020年5月31日.) https://cloudsecurityalliance.jp/j-docs/CSA_Guidance_V4.0_J_V1.1_20180724.pdf, p.111.

JSSA システム監査学会

# システムセキュリティ計画 (SSP)

情報システムに対するセキュリティ要求事項を満たすために既に導入・または導入が計画されている
セキュリティ管理策について記述する文書 (NIST SP 800-18)

Information System Security Plan Template

1. Information System Name/Title:
2. Information System Categorization:
3. **Information System Owner:**
4. **Authorizing Official:**
5. **Other Designated Contacts:**
6. **Assignment of Security Responsibility**:
7. Information System Operational Status:
8. Information System Type:
9. **General System Description/Purpose**
10. **System Environment**
11. **System Interconnections/Information Sharing**
12. Related Laws/Regulations/Policies
13. **Minimum Security Controls**

(出所) National Institute of Standards and Technology, NIST Special Publication 800-18 Rev.1 Guide for Developing Security Plans for Federal Information Systems, NIST. (オンライン) (引用日: 2020年 5月31日.), https://csrc.nist.gov/publications/detail/sp/800-18/rev-1/final

JSSA システム監査学会

# 行動計画とマイルストーン)

CSPが作成・維持する、評価やモニタリングで発見されたセキュリティ上の不備、脆弱性、欠陥とその改善計画の詳細を記述した文書 (CSPのトラッキング)

POA&Mに記述する項目

| | | |
|---|---|---|
| POA&M ID | 改善計画の概要 | 最初のリスク評価値 |
| コントロール | 最初の発見日 | 調整後のリスク評価値 |
| Weakness 名 | 完了予定日 | リスク調整 |
| Weakness 内容 | マイルストン | 誤検知 |
| Weakness 発見したソース | マイルストンの変更 | 運用上の要求事項 |
| Weakness ソース識別子 | ステータス日 (最新の対応日) | 対象外の根拠 |
| 資産の識別子 | ベンダー依存状態 | 補助資料 |
| 連絡先 | 最新のベンダチェックイン日 | 承認欄 (自動) |
| 必要なリソース | 開発ベンダの製品名 | |

(出所) FedRAMP, Plan of Actions and Milestones (POA&M) Template Completion Guide version 2.1 February 21, 2018, FedRAMP. (オンライン) (引用日: 2020年5月31日), https://www.fedramp.gov/assets/resources/documents/CSP_POAM_Template_Completion_Guide.pdf を参考に発表者訳

JSSA システム監査学会

# 役割と責任の定義と割り当て

では、組織のリスクマネジメントプロセスに関与する主な役割と責任が示されており、それぞれの役割がRMFのタスクレベルでマッピングされている

- AUTHORIZING OFFICIAL
- AUTHORIZING OFFICIAL DESIGNATED REPRESENTATIVE
- CHIEF ACQUISITION OFFICER
- CHIEF INFORMATION OFFICER
- COMMON CONTROL PROVIDER
- CONTROL ASSESSOR
- ENTERPRISE ARCHITECT
- HEAD OF AGENCY
- INFORMATION OWNER OR STEWARD
- MISSION OR BUSINESS OWNER
- RISK EXECUTIVE (FUNCTION)
- SECURITY OR PRIVACY ARCHITECT
- SENIOR ACCOUNTABLE OFFICIAL FOR RISK MANAGEMENT
- SENIOR AGENCY INFORMATION SECURITY OFFICER
- SENIOR AGENCY OFFICIAL FOR PRIVACY
- SYSTEM ADMINISTRATOR
- SYSTEM OWNER
- SYSTEM SECURITY OR PRIVACY OFFICER
- SYSTEM USER
- SYSTEMS SECURITY OR PRIVACY ENGINEER

**セキュリティ・プライバシーに必要な20の役割と責任を定義**



(出所) National Institute of Standards and Technology, NIST Special Publication 800-37 R2 Risk Management Framework for Information Systems and Organizations, NIST. (オンライン) (引用日: 2020年5月24日.), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf, pp.114-125

JSSA システム監査学会

# 役割と責任のRMFステップへの割り当て

NIST SP800-37 rev.2（APPENDIX E SUMMARY OF RMF TASKS）では、RMFの各ステップのタスクレベルで**Primary Responsibility** (以下**P**) とSupporting Roles (以下省略)を明確化

| 役割 | 準備 [組織ﾚﾍﾞﾙ] | 準備 [ｼｽﾃﾑﾚﾍﾞﾙ] | 分類 | 選択 | 実施 | 評価 | 認可 | 監視 |
|---|---|---|---|---|---|---|---|---|
| AUTHORIZING OFFICIAL | P | P | P | P | | P | P | P |
| AUTHORIZING OFFICIAL DESIGNATED REPRESENTATIVE | | | P | P | | P | P | |
| CHIEF ACQUISITION OFFICER | | | | | | | | |
| CHIEF INFORMATION OFFICER | P | | | | | | | |
| COMMON CONTROL PROVIDER | | | | P | P | P | P | P |
| CONTROL ASSESSOR | | | | | | P | | P |
| ENTERPRISE ARCHITECT | | P | | | | | | |
| HEAD OF AGENCY | P | | | | | | | |
| INFORMATION OWNER OR STEWARD | | P | P | | | | | |
| MISSION OR BUSINESS OWNER | P | P | | | | | | |
| RISK EXECUTIVE (FUNCTION) | P | | | | | | | |

出所) National Institute of Standards and Technology, NIST Special Publication 800-37 R2 Risk Management Framework for Information Systems and Organizations, NIST. (オンライン) (引用日: 2020年5月24日.), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf, pp.114-125

JSSA システム監査学会

# 役割と責任のRMFステップへの割り当て (cont.)

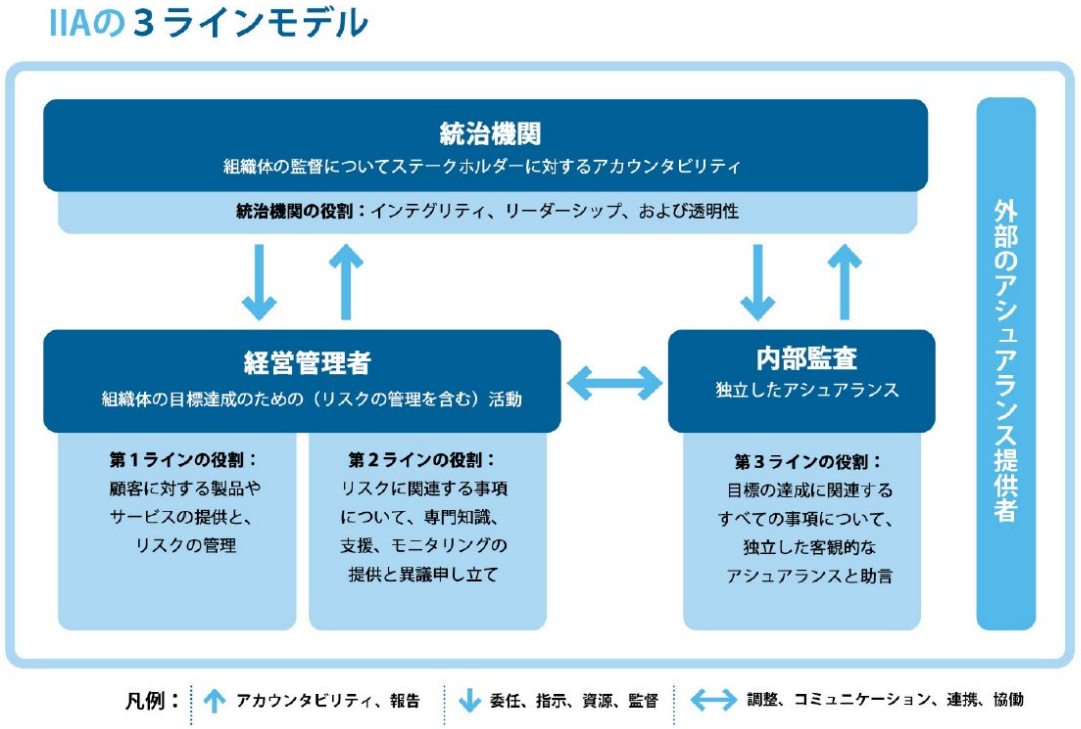
| Roles | 準備 [組織レベル] | 準備 [システムレベル] | 分類 | 選択 | 実施 | 評価 | 認可 | 監視 |
|---|---|---|---|---|---|---|---|---|
| SECURITY OR PRIVACY ARCHITECT | | P | | P | | | | |
| SENIOR ACCOUNTABLE OFFICIAL FOR RISK MANAGEMENT | P | | | | | | | |
| SENIOR AGENCY INFORMATION SECURITY OFFICER | P | | | | | | | P |
| SENIOR AGENCY OFFICIAL FOR PRIVACY | P | P | P | | | | | P |
| SYSTEM ADMINISTRATOR | | | | | | | | |
| SYSTEM OWNER | | P | P | P | P | P | P | P |
| SYSTEM SECURITY OR PRIVACY OFFICER | | P | | P | | | | |
| SYSTEM USER | | | | | | | | |
| SYSTEMS SECURITY OR PRIVACY ENGINEER | | | | | | | | |

出所) National Institute of Standards and Technology, NIST Special Publication 800-37 R2 Risk Management Framework for Information Systems and Organizations, NIST. (オンライン) (引用日: 2020年5月24日.), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf, pp.114-125

JSSA システム監査学会

# IIAの3ラインモデル

組織体が、目標達成を支援し、かつ、強力なガバナンスとリスク・マネジメントを最も促進する構造とプロセスを特定するためのモデル (2020年7月改訂)
⇒ **内部監査の統治機関に対するレポーティングラインを明確化**




## 統治機関

- 組織体の監督についてステークホルダーに対するアカウンタビリティ

## 経営管理者

- **第1ライン**の役割
  - 組織体の目標達成とリスク管理
- **第2ライン**の役割
  - リスク関連の専門知識・支援・モニタリング

## 内部監査（第3ライン)

- 独立した客観的なアシュアランス

## 外部のアシュアランス提供者

- ステークホルダーの利益保全
- 内部アシュアランスの補完

出所) IIA, The IIA's New Three Lines Model An update of the Three Lines of Defense, IIA. (オンライン) (引用日: 2020年8月17日)

JSSA システム監査学会

# 技術のマネジメントに必要なこと

## P・F・ドラッカー『テクノロジストの条件』より

- 最大の危険は、新技術の影響を予測できると誤解し、本当に重要な仕事を軽んじることである。技術というものの全貌を知るには予測は無効である。
- 発展途上の技術についてはモニタリングが必要である。つまり、観察し、評価し、判定していかなければならない。**技術について、観察し、評価し、判定してくことこそがマネジメントの責任**である。
- これからの複雑で変化の激しい時代においては、みずからが世の中に与える影響についてはすべて自分に責任があるという倫理観が不可欠。

（出所）P・F・ドラッカー (2005) ,テクノロジストの条件 はじめて読むドラッカー (技術編)【Kindle版】, ダイヤモンド社, 位置No.4149

JSSA システム監査学会

# セキュリティ責任共有に基づく監査

図 3-1 CSP とクラウド利用者間のセキュリティ責任　Cloud customer　CSP

| Category | Major Security Technology Requirement | IaaS | PaaS | SaaS |
|---|---|---|---|---|
| Infrastructure security | Physical and network security | CSP | CSP | CSP |
| Virtualization security | Virtualization platform, virtual storage, and API security | CSP | CSP | CSP |
| | Virtual network | Cloud customer | CSP | CSP |
| Host security | Antivirus, intrusion prevention, host security hardening, and patch management of OS, firmware updates | Cloud customer | CSP | CSP |
| Middleware security | Container, API, database, and resource management platform security | Cloud customer | CSP | CSP |
| Application system security | Web vulnerability scanning, web tamper protection (WTP), anti-DDoS, application firewall, Identity and access management (IAM), and API security, DLP solutions | Cloud customer | Cloud customer | CSP |
| Data security | Data transmission and storage security, integrity protection, backup, and recovery | Cloud customer | Cloud customer | Cloud customer |
| Security management | Network audit, network behavior management, traffic control management, key and certificate management, IAM, database audit, cloud log audit, host security management | Cloud customer / CSP | Cloud customer / CSP | Cloud customer / CSP |
| Security O&M | Security operations center (SOC), security situation awareness (SSA), web vulnerability scanning, system vulnerability scanning, security event monitoring, baseline configuration check, and security audit | Cloud customer / CSP | Cloud customer / CSP | CSP |

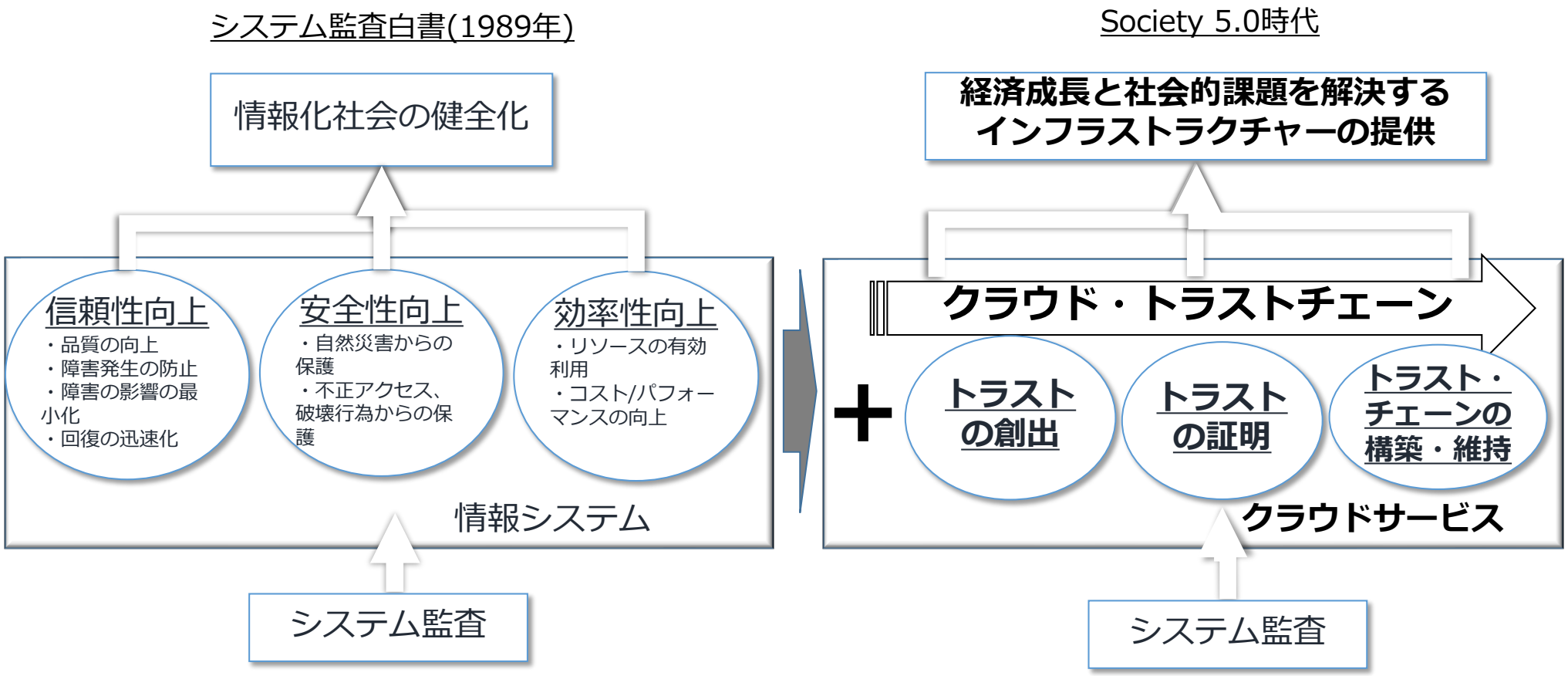
**の監査人**は、「内部のセキュリティ対策と利用者向けのセキュリティ機能をはっきりと文書で示し、クラウド利用者が情報に基づく意思決定をできるようにしているか、それらセキュリティ対策を適切に設計し実装しているか」を監査する。

**クラウド利用者の監査人**は、「クラウドプロジェクトに際し、責任分担表を作成して誰がどの対策をどのように実装する必要があるのかを文書で示しているか、必要な準拠すべき基準に対応しているか」を、CSPの監査報告書等も参照し、監査する。

（出所） CSA, クラウドにおける セキュリティサービスの効果的な管理のガイドライン（日本語版）, 日本クラウドセキュリティアライアンス, 2018, (オンライン) (引用日: 2020年5月31日.), https://www.cloudsecurityalliance.jp/site/wp-content/uploads/2019/09/Guideline-on-Effectively-Managing-Security-Service-in-the-Cloud-06_02_19_J_FINAL.pdf, p9.図　3-1
（参考）CSA, クラウドコンピューティングのためのセキュリティガイダンス バージョン4.0（日本語版）, 日本クラウドセキュリティアライアンス, 2018, (オンライン) (引用日: 2020年5月31日.), https://cloudsecurityalliance.jp/j-docs/CSA_Guidance_V4.0_J_V1.1_20180724.pdf, p22

JSSA システム監査学会

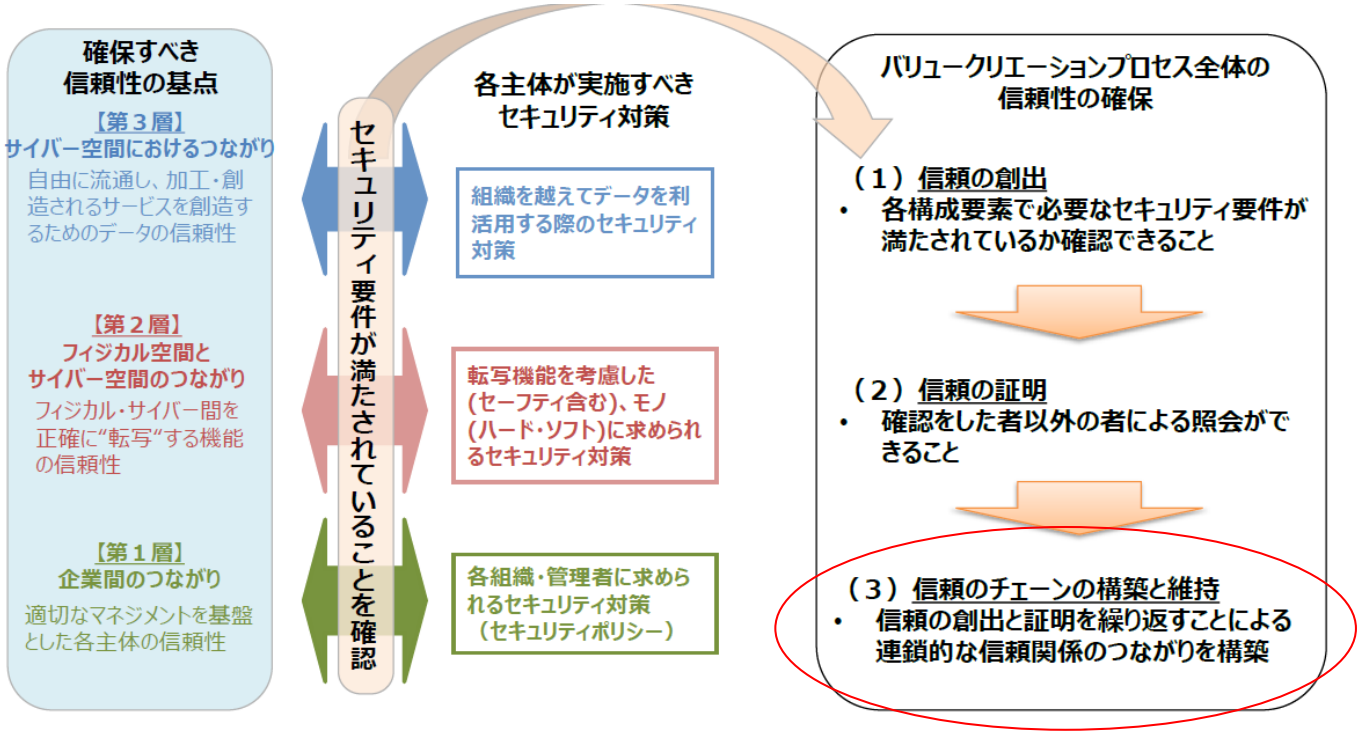
# システム監査の目的




/（財）日本情報処理開発協会編 (1989), システム監査白書1989, コンピュータ・エージ社, p28, 図1-3 システム監査の目的

JSSA システム監査学会

# CPSFにおける信頼のチェーンの考え方




**信頼の創出と証明の繰り返しによる連鎖的な信頼関係のつながり**

**バリュークリエイションプロセス全体のセキュリティを実現**

出所) 経済産業省　商務情報政策局　サイバーセキュリティ課, サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の概要, 平成31年4月18日, 経済産業省 (オンライン) (引用日: 2020年5月31日) https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf