第37回システム監査学会研究大会

サイバーリスク時代の内部統制とシステム監査

2023年6月16日

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 (NEC)

鈴木　夏彦

システム監査技術者, CIA, CISA

©2023 Japan Society for Systems Audits. All Rights Reserved.

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。

©2023 Japan Society for Systems Audits. All Rights Reserved.

目次

- IT監査保証の判断基準研究プロジェクト メンバー
- 発表者紹介
- 研究目的
- サイバーリスクの現状
- 基準・規格・ガイドラインの動向
- サイバーリスク時代のシステム監査
- 内部監査への言明の監査の活用
- おわりに

©2023 Japan Society for Systems Audits. All Rights Reserved.

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
鈴木　夏彦	日本電気株式会社 (NEC)　システム監査技術者, CIA, CISA
成田　和弘	有限責任監査法人トーマツ　システム監査技術者, CIA, CISA
牧野　博文	株式会社東芝　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

©2023 Japan Society for Systems Audits. All Rights Reserved.

発表者紹介 (鈴木 夏彦)

現在の業務

クラウドサービス・データセンター・システム運用サービスに係る
IT全般統制評価・システム監査・情報セキュリティ監査

業務を取り巻く背景

- 官公庁・企業のデジタルシフト
- サイバーリスクの高まり
- 制度・規格・基準ガイドラインの強化
- システム監査への高まる期待

本研究の目的

**サイバーリスク時代において、内部監査人が向かうべき
システム監査の方向性を考察する。**

©2023 Japan Society for Systems Audits. All Rights Reserved.

研究目的

発表タイトル ：サイバーリスク時代の内部統制とシステム監査

2023年4月に公開された「財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の改訂について (意見書) 」では、内部統制の基本的要素における「ITへの対応」において、**ITの委託業務に関わる統制**の重要性や、**クラウドやリモートアクセスの普及に伴うサイバーリスク**の高まり等を踏まえた**情報システムのセキュリティ確保**の重要性が追加された。また、内部統制の独立的評価を担う**内部監査人**についても、**熟達した専門的能力**と**専門職としての正当な注意**をもって職責を全うすること等の重要性が追加された。

これらの変更点を踏まえ、**サイバーリスク時代において、内部監査人が向かうべきシステム監査の方向性**を考察する。

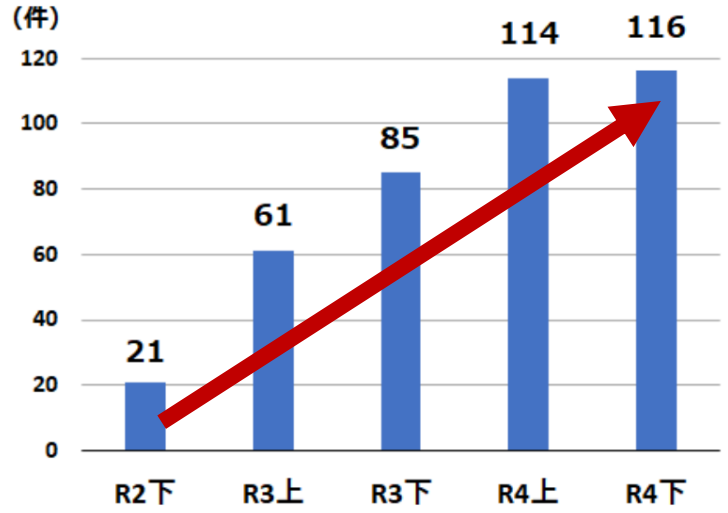
©2023 Japan Society for Systems Audits. All Rights Reserved.

サイバーリスクの現状

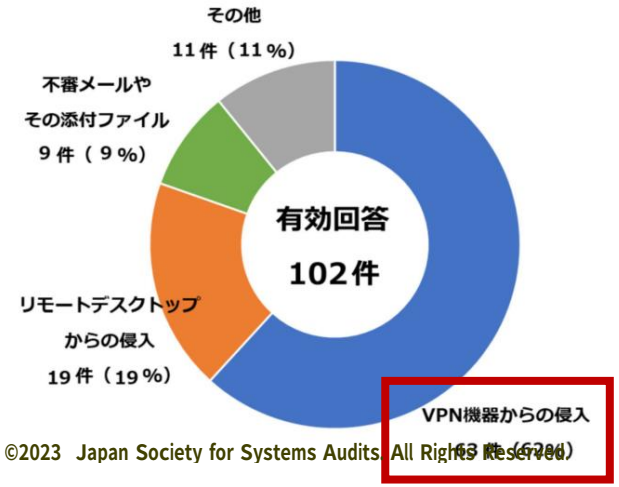
©2023 Japan Society for Systems Audits. All Rights Reserved.

サイバー空間の脅威

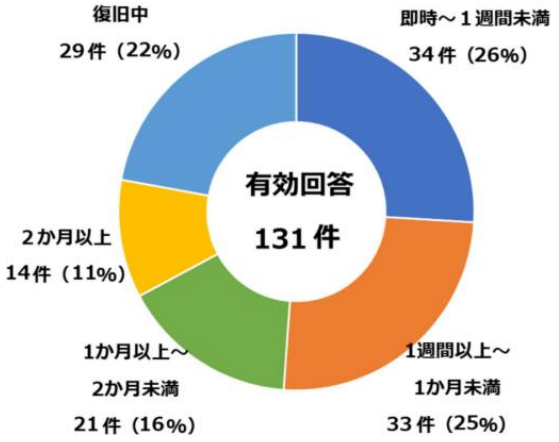
ランサムウェア被害報告件数



感染経路



復旧に要した期間



- **2022年 ランサムウェア*1 被害230件（前年比 57.5%増）**
  - VPN機器等からの侵入が63%
  - 復旧まで2か月以上を要した事例も有り
- **組織の事業存続を脅かす被害事例多数**
  - 電子カルテシステムを復旧できず医療業務が数か月停止
  - 情報システムを復旧できず、財務諸表の提出期限を延長
  - 国内工場の製造ラインが停止 等

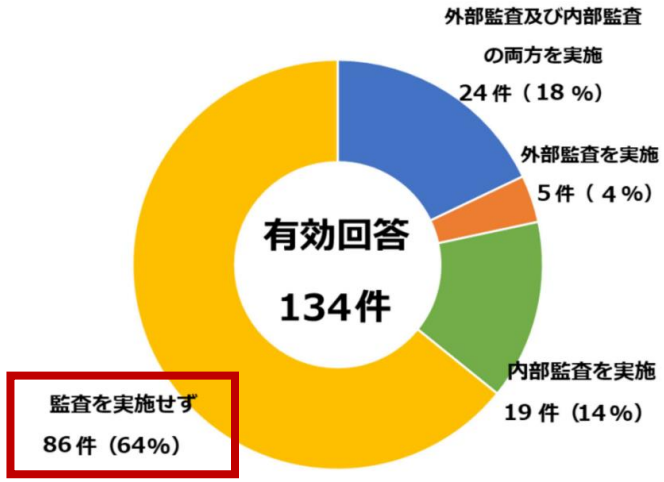
*1 感染すると端末等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価（金銭又は暗号資産）を要求する不正プログラム

(出所) 警察庁「広報資料 令和４年におけるサイバー空間をめぐる脅威の情勢等について　令和５年３月16日」(2023)
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

©2023 Japan Society for Systems Audits. All Rights Reserved.

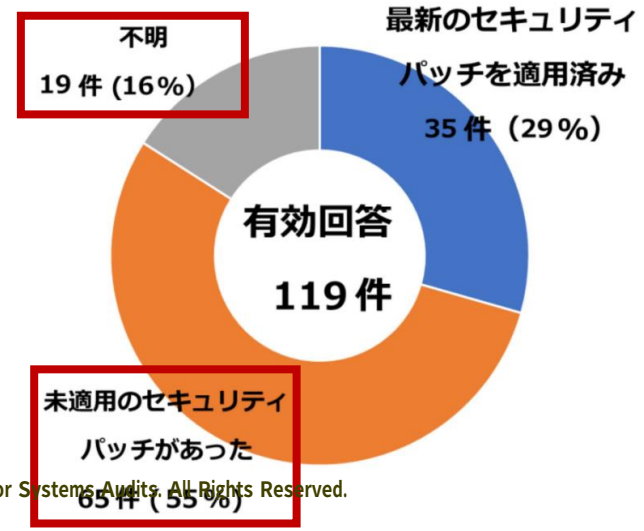
被害組織の監査実施状況及びパッチ適用状況

被害企業・団体等の情報セキュリティ監査の実施状況



- **監査未実施 64%**
  - サイバーリスクを考慮した情報セキュリティに係る監査が実施されていない
  - 被害組織の36%は監査を実施しているものの実効性は不明

侵入経路とされる機器のセキュリティパッチの適用状況



- **パッチ未適用 55% 不明 16%**
  - セキュリティ上のぜい弱性を抱えた情報システムが過半数

(出所) 警察庁「広報資料 令和４年におけるサイバー空間をめぐる脅威の情勢等について 令和５年３月16日」(2023) https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

©2023 Japan Society for Systems Audits. All Rights Reserved.

基準・規格・ガイドラインの動向

©2023 Japan Society for Systems Audits. All Rights Reserved.

財務報告に係る内部統制の評価及び監査の基準及び実施基準の改訂

システム監査に携わる内部監査人が重要な役割を担うことが期待されている。

システム監査や内部監査に関連する主な改訂内容（抜粋）

- 内部統制の基本的要素
  - 「ＩＴへの対応」では、**ＩＴの委託業務に係る統制の重要性**が増していること、**サイバーリスクの高まり**等を踏まえた**情報システムに係るセキュリティの確保が重要**であることを記載

- 内部統制に関係を有する者の役割と責任
  - **内部監査人**については、**熟達した専門的能力と専門職としての正当な注意**をもって職責を全うすること、取締役会及び監査役等への報告経路も確保すること等の重要性を記載

（出所）企業会計審議会 「財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の改訂について（意見書）令和５年４月７日」 (2023) https://www.fsa.go.jp/news/r4/sonota/20230407/20230407.html

©2023 Japan Society for Systems Audits. All Rights Reserved.

財務報告に係る内部統制の評価及び監査の基準及び実施基準の改訂(詳細)

改訂版	現行
2. 内部統制の基本的要素 (6) ＩＴ（情報技術）への対応 （略） ＩＴ環境の飛躍的な進展によってＩＴが組織に深く浸透した現状に照らして、本基準における「Ⅰ．内部統制の基本的枠組み」では、「ＩＴへの対応」を基本的要素の１つに加えている。組織の業務内容がＩＴに大きく依存していたり、組織の情報システムがＩＴを高度に取り入れている等、現状では多くの組織がＩＴ抜きでは業務を遂行することができなくなっている。また、**情報システムの開発・運用・保守などＩＴに関する業務の全て又は一部を、外部組織に委託するケースもあり、かかるＩＴの委託業務に係る統制の重要性が増している。**さらに、**クラウドやリモートアクセス等の様々な技術を活用するに当たっては、サイバーリスクの高まり等を踏まえ、情報システムに係るセキュリティの確保が重要である。**ＩＴへの対応を基本的要素に加えたことは、組織に深くＩＴが浸透している現状では、業務を実施する過程において組織内外のＩＴに対し適切に対応することが、内部統制の目的を達成するために不可欠となっていることを示したものであって、組織に新たなＩＴシステムの導入を要求したり、既存のＩＴシステムの更新を強いるものではない。	2. 内部統制の基本的要素 (6) ＩＴ（情報技術）への対応 （略） ＩＴ環境の飛躍的な進展によってＩＴが組織に深く浸透した現状に照らして、本基準における「Ⅰ．内部統制の基本的枠組み」では、「ＩＴへの対応」を基本的要素の１つに加えている。組織の業務内容がＩＴに大きく依存していたり、組織の情報システムがＩＴを高度に取り入れている等、現状では多くの組織がＩＴ抜きでは業務を遂行することができなくなっている。ＩＴへの対応を基本的要素に加えたことは、組織に深くＩＴが浸透している現状では、業務を実施する過程において組織内外のＩＴに対し適切に対応することが、内部統制の目的を達成するために不可欠となっていることを示したものであって、組織に新たなＩＴシステムの導入を要求したり、既存のＩＴシステムの更新を強いるものではない。

（出所）企業会計審議会 「財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の改訂について（意見書）令和５年４月７日」 (2023) https://www.fsa.go.jp/news/r4/sonota/20230407/20230407.html

©2023 Japan Society for Systems Audits. All Rights Reserved.

財務報告に係る内部統制の評価及び監査の基準及び実施基準の改訂(詳細)

改訂版	現行
４．内部統制に関係を有する者の役割と責任 （４）内部監査人 （略） 内部監査人は、内部統制の整備及び運用状況を調査、検討、評価し、その結果を組織内の適切な者に報告する。内部監査人は、経営者の直属として設置されることが多く、内部統制の独立的評価において重要な役割を担っている。 内部監査人がその業務を遂行するには、内部監査の対象となる組織内の他の部署等からの制約を受けることなく、客観性を維持できる状況になければならない。このため、経営者は、内部監査人の身分等に関して、内部監査の対象となる業務及び部署から独立し、当該業務及び部署に対し直接の権限や責任を負わない状況を確保することが重要である。 また、**内部監査人は、熟達した専門的能力と専門職としての正当な注意をもって職責を全うすることが求められる。** さらに、内部監査の有効性を高めるため、経営者は、内部監査人から適時かつ適切に報告を受けることができる体制を確保することが重要である。**同時に、内部監査人は、取締役会及び監査役等への報告経路を確保するとともに、必要に応じて、取締役会及び監査役等から指示を受けることが適切である。**	４．内部統制に関係を有する者の役割と責任 （４）内部監査人 （略） 内部監査人は、内部統制の整備及び運用状況を調査、検討、評価し、その結果を組織内の適切な者に報告する。内部監査人は、経営者の直属として設置されることが多く、内部統制の独立的評価において重要な役割を担っている。 内部監査人がその業務を遂行するには、内部監査の対象となる組織内の他の部署等からの制約を受けることなく、客観性を維持できる状況になければならない。このため、経営者は、内部監査人の身分等に関して、内部監査の対象となる業務及び部署から独立し、当該業務及び部署に対し直接の権限や責任を負わない状況を確保することが重要である。 また、内部監査の有効性を高めるため、経営者は、内部監査人から適時・適切に報告を受けることができる体制を確保することが重要である。

（出所）企業会計審議会 「財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の改訂について（意見書）令和５年４月７日」（2023）https://www.fsa.go.jp/news/r4/sonota/20230407/20230407.html

©2023 Japan Society for Systems Audits. All Rights Reserved.

その他規格・基準等の動向

サイバーセキュリティやプライバシーリスク、クラウドサービス等外部サービスの活用等の対策を盛り込んだ改訂が実施されている。

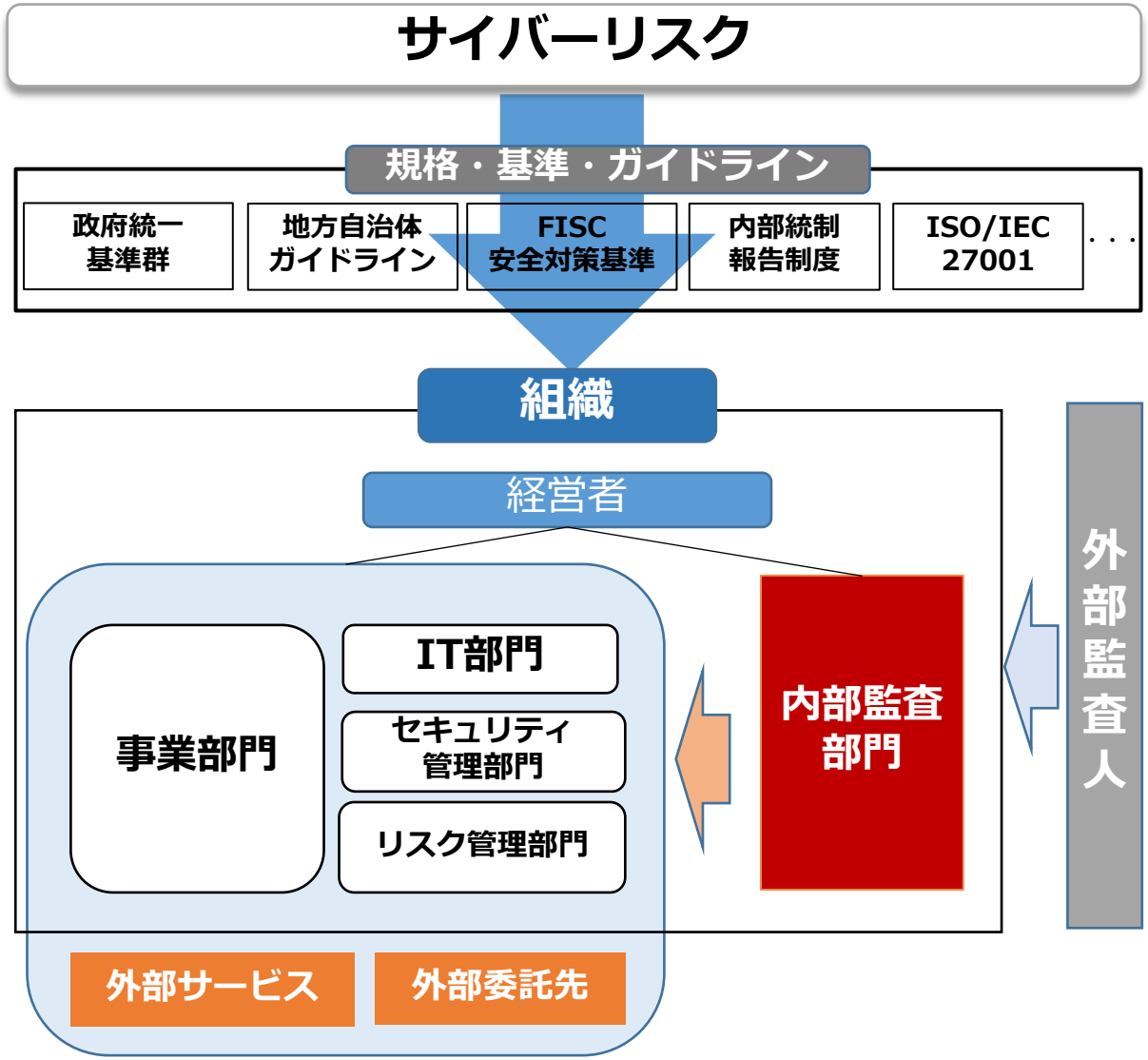
- **ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements (2022年10月)**
  - 情報セキュリティマネジメントシステム（ISMS）の規格であるISO/IEC 27001が改訂され、サイバーセキュリティやプライバシーに係る11の管理策が追加　https://www.iso.org/standard/27001
- **金融機関等コンピュータシステムの安全対策基準・解説書（第10版 改訂) (2022年12月)**
  - サイバーセキュリティに関する新たなリスクへの対策等が追加
    https://www.fisc.or.jp/publication/book/005614.php
- **経済産業省「情報セキュリティサービス基準」 第3版 (2023年3月)**
  - IoTシステムの機器検証、Webアプリケーションぜい弱性診断、プラットフォームぜい弱性診断のサービス「機器検証サービス」の追加　https://www.meti.go.jp/press/2022/03/20230330002/20230330002.html
- **経済産業省「システム管理基準」(2023年4月)**
  - データの利活用の取り組み、クラウドサービス等の外部サービスの利用増大等を考慮した改訂(出所)
    https://www.meti.go.jp/policy/netsecurity/sys-kansa/

©2023 Japan Society for Systems Audits. All Rights Reserved.

サイバーリスク時代のシステム監査

©2023 Japan Society for Systems Audits. All Rights Reserved.

サイバーリスク時代の内部統制と内部監査



©2023 Japan Society for Systems Audits. All Rights Reserved.

(出所)　発表者作成

◆ サイバーリスク時代の内部統制

- サイバーリスクに対応するための内部統制・情報セキュリティマネジメントシステムの設計と実装・運用
- **独立した組織（内部監査部門）による、サイバーリスクとそのコントロールの定期的・継続的な検証**
- 外部監査人による内部統制の検証と保証
- 監査結果に基づく継続的な改善

◆ サイバーリスク時代の内部監査

- サイバーリスク及び外部サービス活用のリスク、それらのコントロールに係る熟達した専門知識・能力（専門家活用を含む）
- サイバーリスク及び外部サービス活用のリスク、それらのコントロールに係る専門職としての正当な注意

(参考) 内部監査人協会「内部監査の専門職的実施の国際基準」（2013）

サイバーリスク時代の情報システムを取り巻く環境

絶え間ないサイバー攻撃

シャドークラウド

サプライチェーンリスク

自動化/AIの導入・利用

アジャイル等の高速開発

プライバシーリスク

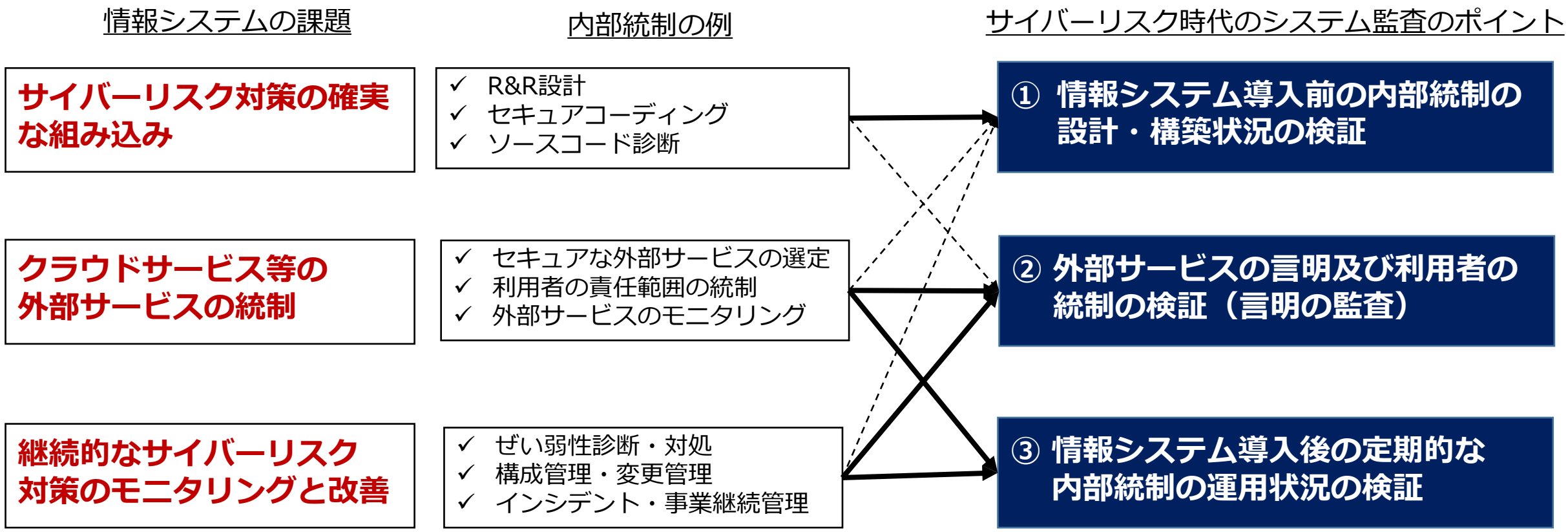
サイバーリスク時代の情報システムの課題

- サイバーリスク対策の確実な組み込み
- クラウドサービス等の外部サービスの統制
- 継続的なサイバーリスク対策のモニタリングと改善

©2023 Japan Society for Systems Audits. All Rights Reserved.

(出所)　発表者作成

サイバーリスク時代のシステム監査のポイント

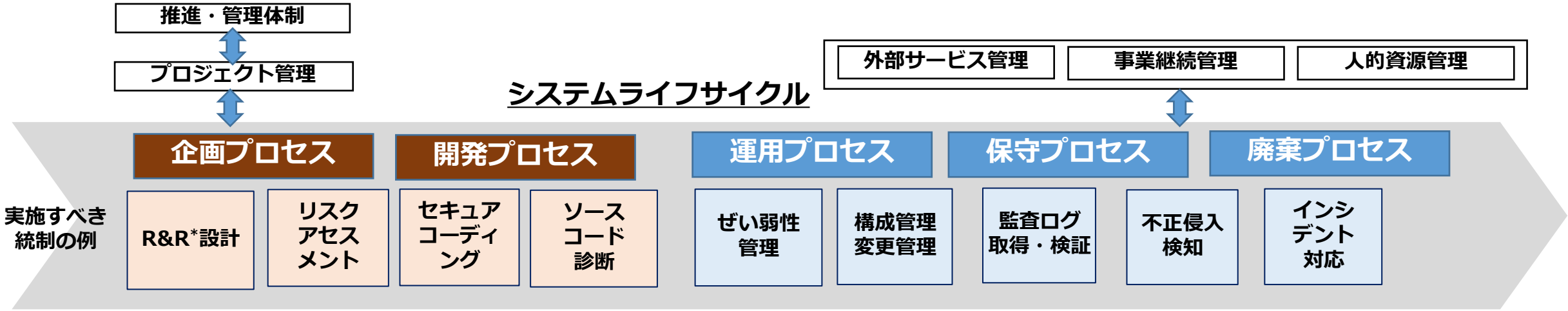


（出所） 発表者作成

©2023 Japan Society for Systems Audits. All Rights Reserved.

① 情報システム導入前の内部統制の設計・構築状況の検証

情報システムの企画・開発段階でシステム監査を実施することにより、導入後には実装が困難なサイバーリスク統制を確実に実装を促していくことが必要



導入前のシステム監査のチェックポイント例

- ✓ 情報セキュリティ方針や法規制・基準等への遵守状況
- ✓ R&R(役割と責任）の設計状況
- ✓ サイバーリスクアセスメントの実施状況
- ✓ 外部サービス利用計画に基づく外部サービス選定状況
- ✓ セキュアコーディングの実施状況
- ✓ ソースコード診断の実施状況

等

*) R&R: Roles and Responsibilities 役割と責任

(参考) 経済産業省「システム管理基準」(2023) https://www.meti.go.jp/policy/netsecurity/sys-kansa/

©2023 Japan Society for Systems Auditors All Rights Reserved

② 外部サービスの言明及び利用者の統制の検証

外部サービス言明又は監査報告書が存在するクラウドサービスプロバイダ（CSP）を選定し、その内容を定期的に検証し、且つ外部サービスが担わない利用者側統制を検証することが必要

図 3-1 CSP とクラウド利用者間のセキュリティ責任

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

内部監査人の役割

- 自社が利用するクラウドサービスの種類(IaaS/PaaS/SaaS)に応じ、CSPが担うセキュリティ責任に関する言明及び（又は）監査報告書を検証し、自社のサイバーリスク対策の要求事項に合致しているかを検証
- Cloud customer (クラウド利用者)が担うセキュリティ責任について、その統制が整備・運用されているかを検証

（出所） 日本クラウドセキュリティアライアンス「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）」(2018) 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, p.9 図3-1
（参考）日本クラウドセキュリティアライアンス「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）」(2018) https://cloudsecurityalliance.jp/j-docs/CSA_Guidance_V4.0_J_V1.1_20180724.pdf, p22

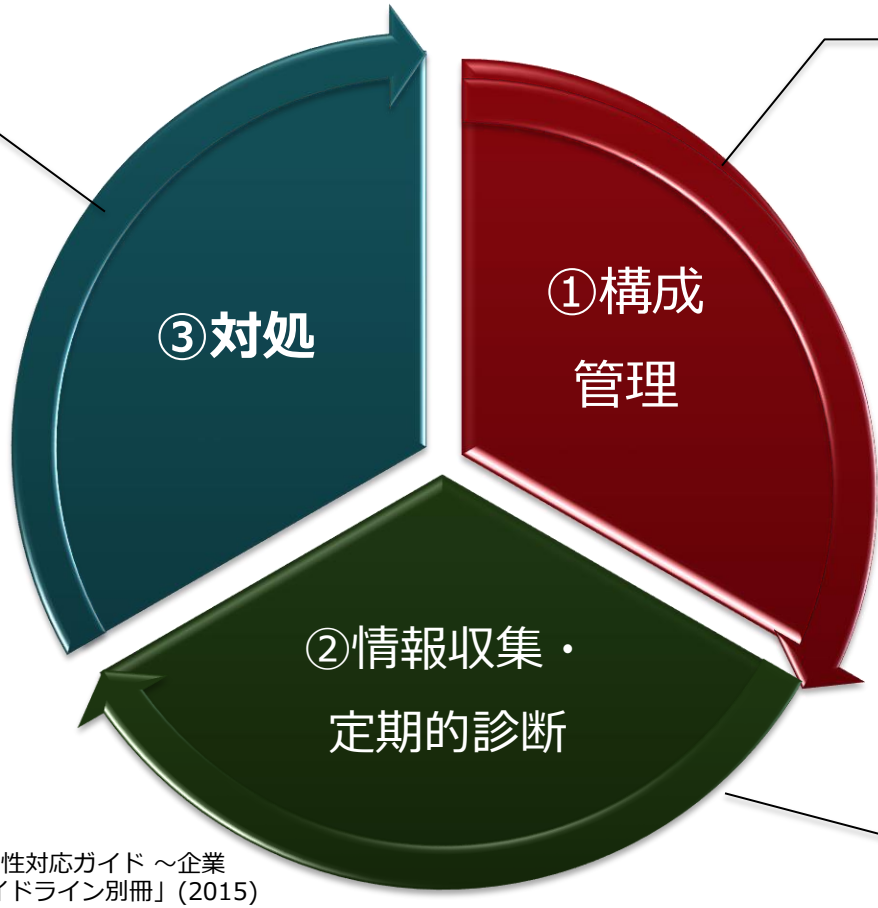
©2023 Japan Society for Systems Audits. All Rights Reserved.

③ 情報システム導入後の定期的な内部統制の運用状況の検証

導入後のサイバーリスク対策で必須となるぜい弱性管理では、①構成管理 ②ぜい弱性情報の収集と診断 ③対処 の３要素が確実に実施されているかを継続的に検証することが必要

ぜい弱性管理の３要素と監査のポイント

検出したぜい弱性への タイムリー&適切な対処（パッチ適用・設定変更等）が実施されているか



情報システムを構成するソフトウェア及びハードウェア情報の管理と維持が適切に実施されているか

ぜい弱性情報のタイムリーな収集と定期診断が実施されているか

※定期診断の例
- ✓ ソースコード診断
- ✓ Webアプリケーション診断
- ✓ プラットフォーム診断
- ✓ ペネトレーションテスト等

（参考）独立行政法人情報処理推進機構他「セキュリティ担当者のための脆弱性対応ガイド ～企業情報システムの脆弱性対策～ 情報セキュリティ早期警戒パートナーシップガイドライン別冊」(2015)
https://www.ipa.go.jp/security/vuln/websecurity/ug65p900000197fc-att/000044737.pdf

©2023 Japan Society for Systems Audits. All Rights Reserved.

内部監査への言明の監査の活用

©2023 Japan Society for Systems Audits. All Rights Reserved.

クラウドサービス調達・認証制度

国内外のクラウド調達・認証制度では、CSP(クラウドサービスプロバイダ)に対して経営者の**言明***を要求。
クラウドサービスの言明では、セキュリティ管理策について、**誰が**（統制実施者）、**何のために**（統制の目的）、**いつ**（統制頻度）、**何をするか**（統制の内容）等を記述

✓：調達・認証制度が採用している規格・基準

調達・認証制度		ISMSクラウド セキュリティ 認証制度	ISMAP 日本政府クラウド サービス調達制度	FedRAMP 米国政府クラウド サービス調達制度	SOC2 セキュリティ 保証報告制度
国		グローバル	日本	米国	グローバル
監査の主題		非言明	**言明**	**言明**	**言明**
規格・基準	ISO/IEC 27001	✓	✓	✓	
	ISO/IEC 27002	✓	✓		
	ISO/IEC 27014		✓		
	ISO/IEC 27017	✓	✓		
	政府統一基準		✓		
	NIST SP 800-53		✓	✓	
	TSP Section 100				✓

*) **言明**: 自己申告 (statement) 。真偽（またはその確からしさの程度）を決定することのできる文。財務諸表、内部統制報告書も言明の例 (鳥羽・秋月, 2001)

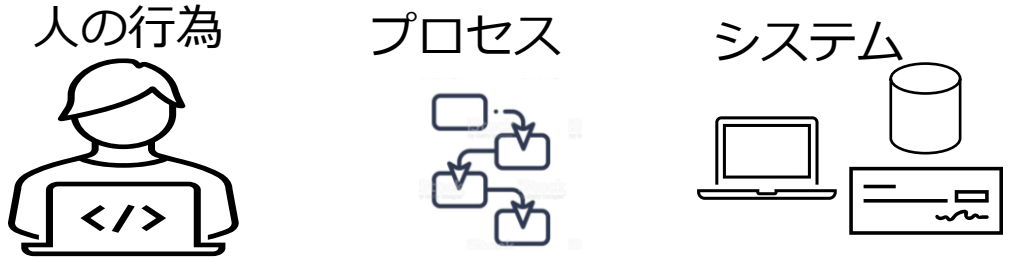
©2023 Japan Society for Systems Audits. All Rights Reserved.

(参考) 鳥羽・秋月「監査の理論的考え方」(2001, 6頁)

非言明の監査と言明の監査の違い

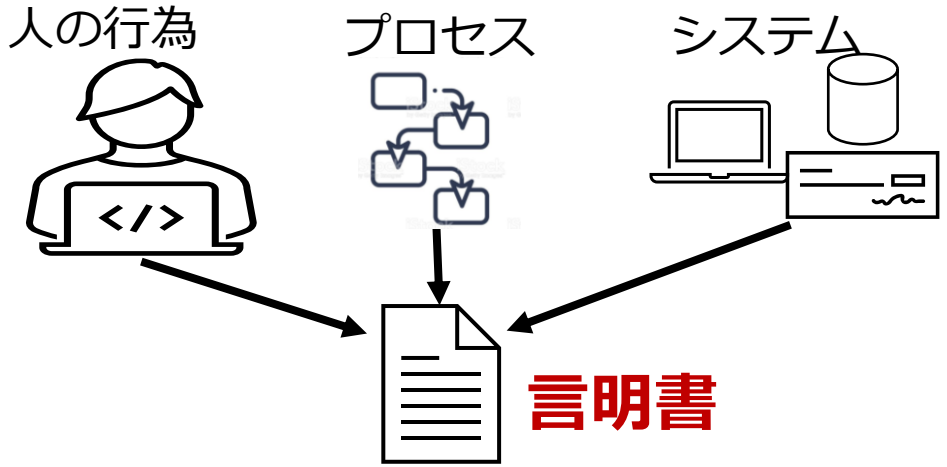
監査人の結論が求められる**監査の主題**による区分

非言明の監査



人の行為・プロセス・システム
そのものを監査

言明の監査



人の行為・プロセス・システムの
状況や結果を記述した言明を監査

(参考) 鳥羽・秋月「監査の理論的考え方」(2001, 6頁)

©2023 Japan Society for Systems Audits. All Rights Reserved.

非言明の監査と言明の監査の比較

監査の主題	非言明の監査	言明の監査
監査の対象	行為・プロセス・システムそのものを対象	行為・プロセス・システムの状況や結果を記述した言明を対象
メリット	• 当事者の申告とは無関係に内部監査人の裁量で監査が可能（情報流出事故に係る**内部不正の原因究明**等に適する）	• **統制の責任者の所在が明確化** • クラウドサービス提供部門の従業員の**当事者意識の醸成** • 内部監査人の力量によるばらつきが少ない
デメリット	• 内部監査人自ら責任の所在を確認要（**帰責を探求⇒現場の抵抗**） • 内部監査人の力量でばらつきが多い	• 内部監査人が言明の内容に反する証拠を求めない**確証傾向***のリスク

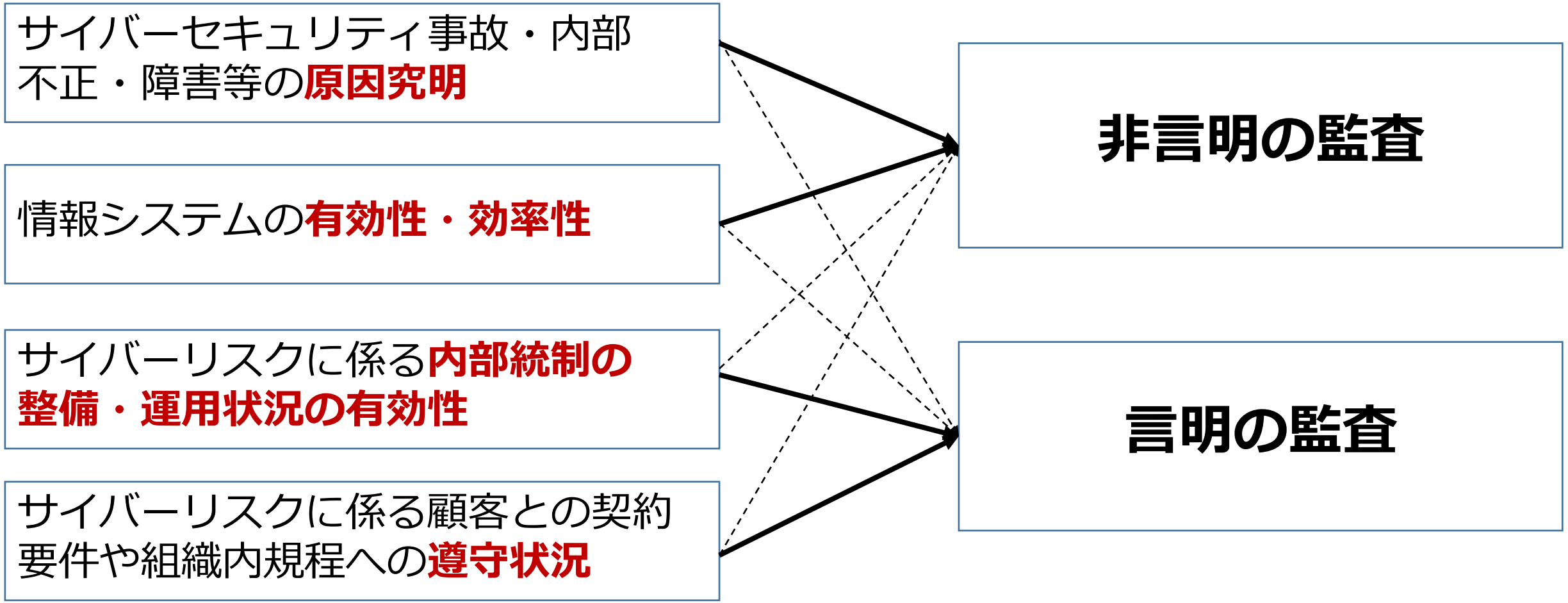
*) **確証傾向** (confirmation proneness): 自分の主張に役立つ情報を入手するように努め、都合の悪い情報の源泉への接触は避けようとする人の特性・傾向（鳥羽, 2016）

(参考) 鳥羽・秋月「監査の理論的考え方」(2001, 9頁, 25頁)

©2023, Japan Society for Systems Audits, All Rights Reserved.

非言明の監査と言明の監査の併用(案)

非言明の監査及び言明の監査のメリット・デメリットを踏まえ、内部監査の目的に応じた併用を提案



(出所) 発表者作成

©2023 Japan Society of Information Systems Audits. All Rights Reserved.

言明の監査の内部監査への導入ステップ(案)

1. **規準の確立**
   - 情報システムが遵守すべきサイバーリスク統制のベースラインを確立

2. **統制部門の明確化**
   - 組織において統制を担う部門を明確化

3. **統制記述の作成**
   - 統制の実施者、統制の目的、統制の頻度、統制の内容を記述

4. **内部監査の実施**
   - 統制記述に基づいた内部監査を実施
   - 非言明の監査を併用

5. **統制記述の最新化と維持**
   - 外部環境・内部環境の変化に基づき、統制記述を維持・最新化

(出所) 発表者作成

©2023 Japan Society for Systems Audits. All Rights Reserved.

おわりに

©2023 Japan Society for Systems Audits. All Rights Reserved.

サイバーリスク時代のシステム監査の方向性

	従来の内部監査	サイバーリスク時代のシステム監査
監査の段階	サービスイン後中心	**システムライフサイクル全体（システム導入前及び導入後）**
監査の対象	自社のシステム中心	**外部サービス及び外部委託先を含むサプライチェーン全体**
監査の主題	非言明の監査中心	**言明の監査と非言明の監査のハイブリッド**

（出所）　発表者作成

©2023 Japan Society for Systems Audits. All Rights Reserved.

まとめ

- **サイバーリスク時代のシステム監査のポイント**
  - ① 情報システム導入前のサイバーリスク対策の検証
  - ② クラウドサービスの統制(言明)と、利用者としての統制の検証
  - ③ ぜい弱性対策など、内部統制の運用状況を継続的な検証

- **内部監査における言明の監査の活用**
  - 統制実施者の明確化、当事者意識の醸成等のメリット
  - 内部監査の目的に合わせ、非言明の監査と言明の監査を併用

©2023 Japan Society for Systems Audits. All Rights Reserved.

主な参考文献・資料

- アメリカ会計学会（青木茂男監訳・鳥羽至英訳）(1982)『基礎的監査概念』国元書房
- 蟹江章編著(2010)『ガバナンス構造の変化と内部監査』同文舘出版
- 亀岡恵理子・福川裕徳・永見尊・鳥羽至英(2021)『財務諸表監査　改訂版』国元書房
- 喜入博・島田裕次・角田善弘共著、日本内部監査協会編 (2003) 『情報システム監査の基礎と実践』同文舘出版
- 清原健・武井洋一・三宅英貴・鈴木正人編著 (2019) 『会計不正の予防・発見と内部監査―リスク・マネジメントトガバナンス強化に向けた活用―』同文舘出版
- 鳥羽至英 (2016) 「財務諸表監査の質と監査上の懐疑に関する論点整理」早稲田大学商学第446号
- 鳥羽至英・秋月信二共著(2001)『監査の理論的考え方 -新しい学問「監査学」を志向して-』森山書店
- 鳥羽至英・秋月信二共著(2018)『監査を今、再び、考える。監査を考える原点は何か？』国元書房
- 鳥羽至英・八田進二・高田敏文共訳(1996)『内部統制の統合的枠組み　理論篇』白桃書房

- 企業会計審議会 「財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の改訂について（意見書）令和５年４月７日」 (2023) https://www.fsa.go.jp/news/r4/sonota/20230407/20230407.html
- 経済産業省「システム管理基準」（2023）https://www.meti.go.jp/policy/netsecurity/sys-kansa/
- 警察庁「広報資料 令和４年におけるサイバー空間をめぐる脅威の情勢等について 令和５年３月16日」(2023) https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf
- 独立行政法人情報処理推進機構他「セキュリティ担当者のための脆弱性対応ガイド～企業情報システムの脆弱性対策～情報セキュリティ早期警戒パートナーシップガイドライン別冊」(2015) https://www.ipa.go.jp/security/vuln/websecurity/ug65p900000197fc-att/000044737.pdf
- 日本クラウドセキュリティアライアンス「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）」(2018) 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
- 日本クラウドセキュリティアライアンス「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）」(2018) https://cloudsecurityalliance.jp/j-docs/CSA_Guidance_V4.0_J_V1.1_20180724.pdf
- FedRAMP https://www.fedramp.gov/
- ISMAP - 政府情報システムのためのセキュリティ評価制度　https://www.ismap.go.jp/csm

©2023 Japan Society for Systems Audits. All Rights Reserved.

鈴木 夏彦
natsuhiko@nec.com

©2023 Japan Society for Systems Audits. All Rights Reserved.