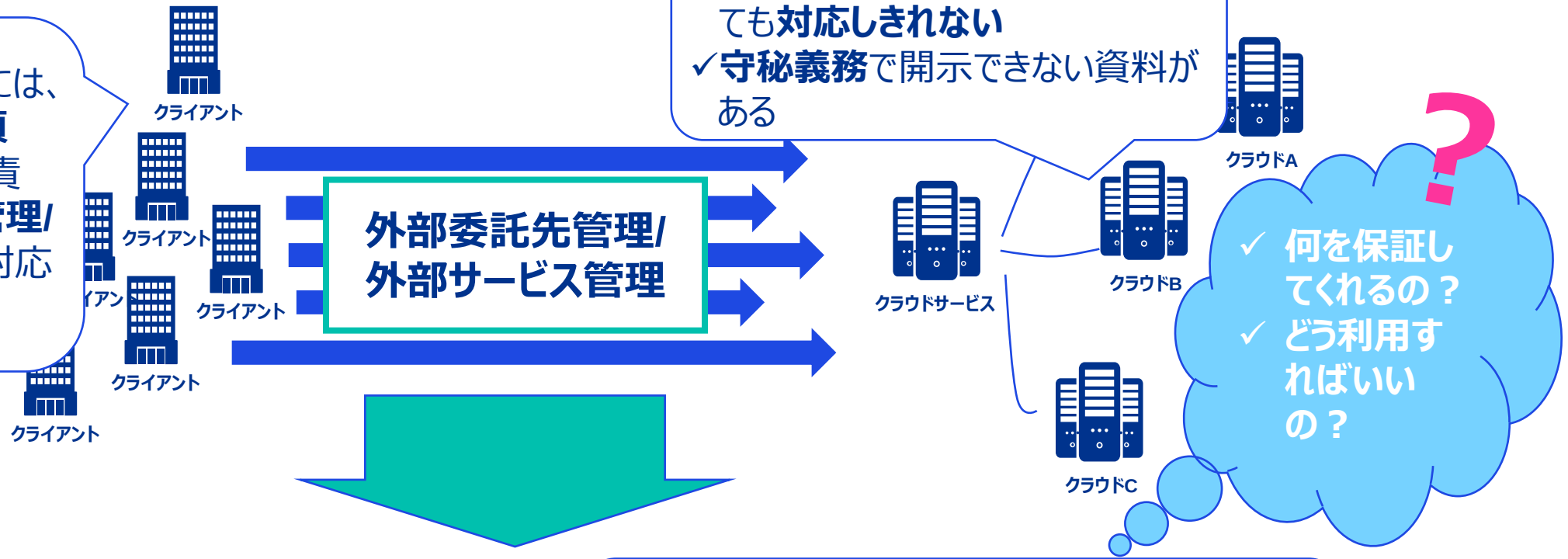
略歴紹介

山口 達也
Tatsuya Yamaguchi

現職	有限責任あずさ監査法人 Digital Innovation & Assurance統轄事業部 Digital Advisory事業部長／パートナー　山口 達也
経歴	● 都銀システム開発部門に約9年勤務し、国内外勘定システム、情報系システム、市場系システムを担当 ● 朝日監査法人（現あずさ監査法人）に転職後、約20余年間にわたり、財務諸表監査におけるIT統制監査、システムリスク管理態勢、セキュリティ管理態勢、大型システムプロジェクトマネジメント管理態勢等、さまざまなシステム・セキュリティに関する管理態勢の外部監査、内部監査支援等の評価系業務に従事 ● 上記評価系業務と並行し、日本年金機構第三者検証委員会、ISMAP検討委員会監査WG等の委員会等に、委員・参与として参画 ● 日本システム監査人協会 理事 日本セキュリティ監査協会 理事 内閣サイバーセキュリティセンター（NISC）情報セキュリティ指導専門官 ● 公認システム監査人（CSA）、公認情報セキュリティ主任監査人（CAIS）、 公認情報システム監査人（CISA)
専門領域	以下に関する第三者評価（外部監査）及び内部監査支援 ● ITガバナンスフレームワーク管理 ● IT/システムリスク管理 ● 大規模システムプロジェクトマネジメントリスク管理 ● 情報セキュリティ・サイバーセキュリティ管理 ● 内部監査品質管理（IIA）

情報セキュリティ監査の需要は確実に拡大

✓DXを推進するためには、**クラウド利用は必須**
✓顧客に対する説明責任：**外部委託先管理/外部サービス管理**対応が必要



✓個別にモニタリング・監査に来られても**対応しきれない**
✓**守秘義務**で開示できない資料がある

事実上、独立した第三者が**代表して評価**を実施し、その結果を**関係者に公開し、活用する仕組み**が必須

✓ 各種認証制度（ISMS、ISO、ISMAP・・・）
✓ 保証報告書（SOC１、**２**、３）
✓ **保証型システム監査・セキュリティ監査**

監査・保証の種類（私見・一例）

日本語では「監査」「保証」と呼ばれる評価の仕組みも、実際は何種類かに分類される。以下は**明確な定義が存在するものではないし、厳密に区分できるものでもない**が、監査業界？でのイメージは以下の通り。

日本語	英語	概要（イメージ）
監査	Inspection	◆ルールへの準拠状況のみを確認（運用状況評価だけ）
	Assessment	◆ルールの妥当性を含めて確認 ◆実際に確認した部分のみを対象に評価※1
	Audit	◆実際に確認した部分を含め、全体を評価※1
保証	Assurance	◆提示された命題（言明等）に対して、その命題が事実に即して正しいか否かを確認※2 ◆結果的に損害等が発生した場合、直接的な賠償等の補償はない
	Guarantee	◆結果的に損害等が発生した場合、それを補償する ◆これに該当する保証業務はない。実質は保険。

※１：AuditとAssessmentの違い

「 A,B,Cシステムを所管するX部署の情報セキュリティ監査を実施の際、A,Bシステムを確認した結果として、、、」

【Audit】

X部署のセキュリティ対策は評価基準に従って対応されている。

【Assessment】

X部署のAシステム、Bシステムのセキュリティ対策は評価基準に従って対応されている

※２：保証型監査/各種評価制度の仕組み

言明書に記載されていることを確認

言明書に書いていないことは、<u>見ていない</u>

次世代の情報セキュリティ監査

監査/評価結果を正しく活用するためには・・・・

監査を実施する側

結果を利用する側

双方での進化が必要