ＳＡＡＪ近畿支部第１７８回定例研究会

テーマ　：　働き方改革におけるシステム監査の有用性

平成31年3月15日

株式会社ディレクタイズ
島﨑　智久
（米国公認会計士、社会保険労務士、システム監査技術者）

本日のアジェンダ

- はじめに
- １．働き方改革関連法案の主なTopicと背景
- ２．働き方改革による職場環境の変化（テレワークをベース）における
  システム監査の有用性
- ３．デジタルレイバーと呼ばれるRPAにおけるシステム監査の有用性
- ４．システム監査の将来的方向性について

はじめに（講師略歴と会社概要）

（講師略歴）

氏名　：　島﨑　智久（しまざき　ともひさ）　　株式会社ディレクタイズ／エグゼクティブコンサルタント　米国公認会計士・社会保険労務士・システム監査技術者

大手監査法人系コンサルティングファームにてＩＴ及びビジネスコンサルティングに従事した後、株式会社ディレクタイズの設立メンバーとして参画する。
人事労務や経営管理系の業務領域を主軸として、企業規模を問わず多業種に渡り多くの企業に対して、コンサルティングを手掛けてきた。ＩＴコンサルティング領域においては、主に、ＢＰＲ、フィージビリティスタディ、ＩＴ基本構想策定、ＲＦＰ作成、ＥＲＰ上流工程作業（要件定義、基本設計）、ＥＲＰプリセールス活動に従事した。また、内部統制コンサルティング、大規模プロジェクトのマネジメント業務も複数経験している。
最近では、働き方改革関連法対策コンサルティング、SIベンダー経営企画策定支援、基幹系システム導入プロジェクト支援、予算管理業務コンサルティングなどを手掛けている。

ディレクタイズ（Direcitze）とは？

企業のあるべき「方向性（Direct）」を的確に示し、その「方向性に向かう（ize）」ための　最適なソリューションをご提供することを　企業コンセプトとして設立された経営コンサルティング会社です。

会社の特徴

創業者メンバーは、大手監査法人系のコンサルティング会社出身者で、数多くの企業に対して、様々な経営課題等を、クライアントと一緒に解決してきた専門家の集団です。クライアントと共に成長していきたいという思いから、「わかりやすい」、「高品質」、「低コスト」、　「スピーディー」なサービスの提供をモットーにしております。また、公認会計士、税理士、社会保険労務士、米国公認会計士、システム監査技術者、　中小企業診断士等の有資格者によるコンサルティングが可能なため、ワンストップで、企業課題に取り組めます。

会社概要

- 商号　　：　株式会社ディレクタイズ
- 代表者　：　代表取締役　篠原　恵
- 所在地 〒550-0014　　大阪市西区北堀江1-5-9 北堀江サンシステムBLDG.6F　　TEL：（06）4390-8810　/　FAX：（06）4390-8820
- 資本金：2,100万円
- 設立：2001年7月
- 従業員数：15名
- E-Mail info@directize.co.jp　　URL：http://www.directize.co.jp/
- 有料職業紹介事業　：　紹介事業許可 許可番号（27-ユ-301883）　一般労働者派遣　：　派遣事業許可 許可番号（般27-300987）
- 主な事業目的　経営コンサルタント業、ソフトウェア業、人材派遣業、企業及び団体の役員・社員に対する研修、講演会、セミナーの企画及び実施、各種マーケティング業務

はじめに（本日の定例会の目的）

■本日の定例会の目的は、以下の通りです。

「働き方改革」というテーマにおける、システム監査の有用性を認識共有して頂き、今後のシステム監査業務領域の拡大と新しいシステム監査のスキーム構築に向けて議論できる場を提供することを目的とします。

１．働き方改革関連法案の主なTopicと背景

■働き方改革関連法案の主なTopic

（１）労働時間の上限規制（※中小企業は2020年4月1日から）

・月45H・年360H（休日労働含まない）の原則は変わりなしだが、
特別条項で年720H （休日労働含まない）・単月100H未満・
6カ月間以内の複数月でも平均80Hまで（休日労働含む）
月100時間超残業は産業医等の面接指導（管理監督者等を含む労働時間把握義務）
自動車運行業務、建設事業、医師などは5年猶予

例えば1年間の残業上限は、45H×6カ月（270H）＋75H×6カ月（450H）＝720H

（２）高度プロフェッショナル制度

・労働時間規制適用外となる（年収1,075万円以上の人が対象）
・コンサルタント職（事業・業務の企画運営に関する高度な考案または助言の業務）も対象
※いわゆるシステムコンサルタントは対象外です。
・事業主は、年間１０４日以上、４週間で４日以上の休日を確保することなどの義務がある

（３）有休休暇5日取得の義務化

・管理監督者や有期雇用者も含む
・10日以上付与される労働者のみ対象

（４）同一労働同一賃金（大企業は2020年4月1日から、中小企業は2021年4月1日から）

・非正規社員との手当の差などを説明・解消する必要がある（通勤手当など）
・派遣労働者にも適用

■その他労働関連における主なTopic

（１）外国人労働者の受入増加

・言語や文化の違いによる対応（マニュアルの多言語対応、ハラル対応など）
・赴任時の赴任期間見込みが5年以内の場合は、日本の社会保険の適用外
・社会保険料の支払で社会保障協定はあるが、イギリスと韓国は年金期間の通算が無い

（２）副業許可

・割増賃金の支払義務が発生する会社は、「法定時間外に使用した事業主は、労働基準法第37条に基づき、割増賃金を支払わなければならない（昭23.10.14基収2117号）」と示されており、通算して１日８時間を超える勤務をさせた会社となります。

（３）70歳まで就労

・2025年4月から65歳雇用（経過措置完了）

■総括（個人的見解）

✓ 少子高齢化で労働力不足が懸念され、経済成長率の低下が予想される。そこで、高齢者や育児介護期間中の労働力活用、企業の生産性向上を核に経済成長率を維持させたい。また、支給開始年齢の引き上げとマクロ経済スライド下で年金支給額を減らす。

2．働き方改革による職場環境の変化（テレワークをベース）におけるシステム監査の有用性

■テレワークの概要

※「tele = 離れた所」と「work = 働く」をあわせた造語
「在宅勤務」「モバイルワーク」「サテライトオフィス勤務（施設利用型勤務）」の3つのテレワークの総称

（1）在宅勤務（終日在宅勤務）
終日、所属するオフィスに出勤しないで自宅を就業場所とする勤務形態のこと
・メリット・・通勤負担の軽減、時間有効活用
・主な対象者　・・育児・介護期の従業員、障がい者の方
※部分在宅勤務もある

（2）モバイルワーク
移動中、顧客先、カフェなどを就業場所とするもの
・メリット・・移動時間の削減
・主な対象者　・・営業職、所属オフィス外の勤務が中心の社員など

（3）サテライトオフィス勤務（施設利用型勤務）
勤務先以外のオフィススペースでパソコンなどを利用した働き方。
専用型、共用型のオフィススペースを利用、顧客近接、従業員自宅近接、遊休施設や空き家利用
・メリット・・移動時間の削減
・主な対象者・・営業職、所属オフィス外の勤務が中心の社員など

※上記3つのパターンでは、在宅勤務のニーズが高い

テレワークの主な効果

- ✓ 企業側・・通勤費削減、離職率低下＆定着率向上（優秀な人材確保）など
- ✓ 従業員側・・プライベート（育児・家事など）の時間確保など
- ✓ 業務プロセスの改革につながる

※参考：厚生労働省「テレワークではじめる働き方改革」テレワークの導入・運用ガイドブック

■テレワークのためのICT環境構築に向けての留意点

①マネジメント　②セキュリティの確保　③コミュニケーションの３つの視点が重要

（1）マネジメント

①テレワークのルール策定
　対象者、対象業務、頻度

②労務管理
　法的規制（労基法、労災）
　勤怠管理、プレゼンス管理（在席管理）、業務管理（スケジュールなど）

（勤怠管理）
　事業場外労働のみなし労働時間制の対象となるのは、
　事業場外で業務に従事し、使用者の具体的な指揮監督が及ばず労働時間の算定が困難な業務です。

　１）情報通信機器が、使用者の指示により常時通信可能な状態におくこととされていないこと
　　情報通信機器を通じた使用者の指示に即応する義務がない状態であることを指す。なお、この使用者の指示には黙示の指示を含む。
　２）　随時、使用者の具体的な指示に基づいて業務を行っていないこと
　　「具体的な指示」には、例えば、当該業務の目的、目標、期限等の基本的事項を指示することや、これら基本的事項について所要の変更の指示をすることは含まれない。

　※利用ツール例・・Cyzen（サイゼン）GPS情報と共に活動記録、日報管理

（プレゼンス管理）在席管理
　※利用ツール例・・Sococo（ソココ）仮想オフィスで音声会議などが出来る

（業務管理）
　※利用ツール例・・サイボウズ：スケジュール、ワークフロー

※参考：厚生労働省「テレワークではじめる働き方改革」テレワークの導入・運用ガイドブック

■テレワークのためのICT環境構築に向けての留意点

①マネジメント　②セキュリティの確保　③コミュニケーションの３つの視点が重要

（２）セキュリティの確保

①ルールによるセキュリティ

セキュリティガイドライン・ルールの策定と浸透（セキュリティポリシー）

・自宅における作業環境、PCの保管及び管理方法
・自宅における休憩中のPCの取り扱い
・モバイルワークにおけるPCの管理方法（モバイル機器ストラップ、のぞき見防止など）
・オフィスから持ち出すPCの管理（暗号化、BIOSパスワード）
・オフィス以外での情報管理（紙情報の管理、共有スペースでの情報管理）

→ルール浸透のための継続的な教育研修が必須

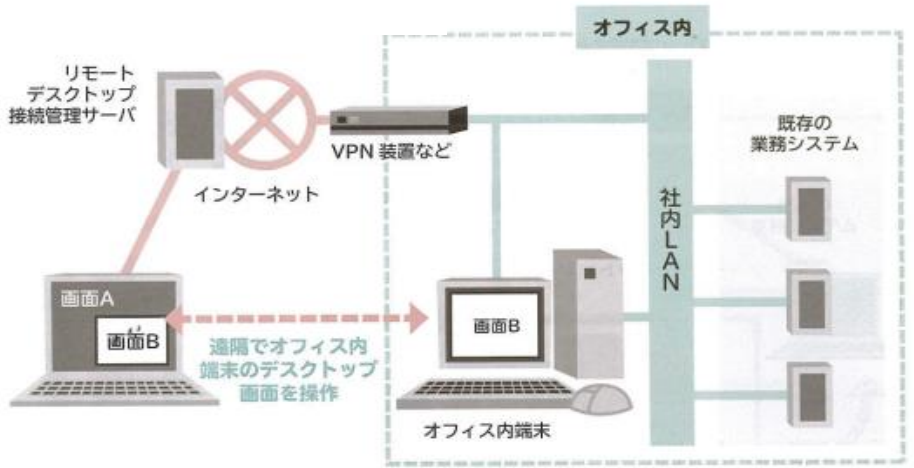
■６つのテレワーク環境におけるシステム方式

１）リモートデスクトップ方式

（magicConnect）

オフィス内PC環境を、オフィス外から
遠隔操作する（例：USBキーによる接続）

メリット・・・手元にデータが残らない、
比較的安価な導入
デメリット・・電気代（PC常時立ち上げ）、
ウィルス対策
（電源オン・オフの管理）



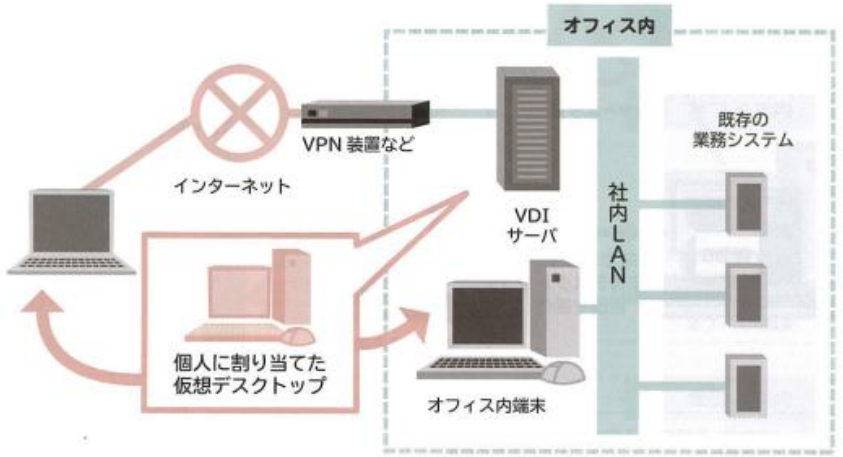
※参考：厚生労働省「テレワークではじめる働き方改革」テレワークの導入・運用ガイドブック

■テレワークのためのICT環境構築に向けての留意点

2）仮想デスクトップ方式

Vmware、AWS、Citrix（シトリックス）
サーバーが提供する仮想デスクトップに遠隔で操作

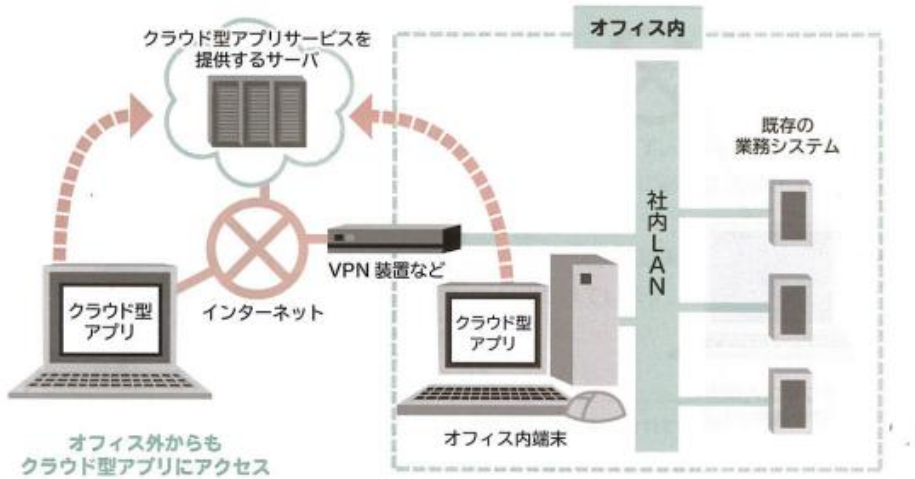
メリット・・・手元にデータが残らない
デメリット・・VDI(Virtual Desktop Infrastructure)
サーバーが必要
高性能なPC操作（設計・デザイン職）
には向かない



3）クラウド型アプリ方式・・会議システムなど

Web上のクラウドアプリにアクセスして操作

メリット・・・設備コストはほぼかからない
デメリット・・端末にデータ保存も可能、
アプリ利用コストは契約内容に依存



※参考：厚生労働省「テレワークではじめる働き方改革」テレワークの導入・運用ガイドブック

■テレワークのためのICT環境構築に向けての留意点

4）セキュアブラウザ方式（※システム構成は、基本的にクラウド型アプリ方式と同じ）
CACHATTO
専用のブラウザからアクセスすることで、閲覧した情報を端末に残さず、端末から持ち出せない。
クラウド型アプリ方式の安全性を高めたもの。

メリット・・手元にデータが残らない
デメリット・・利用コストは契約内容に依存（基本年単位）

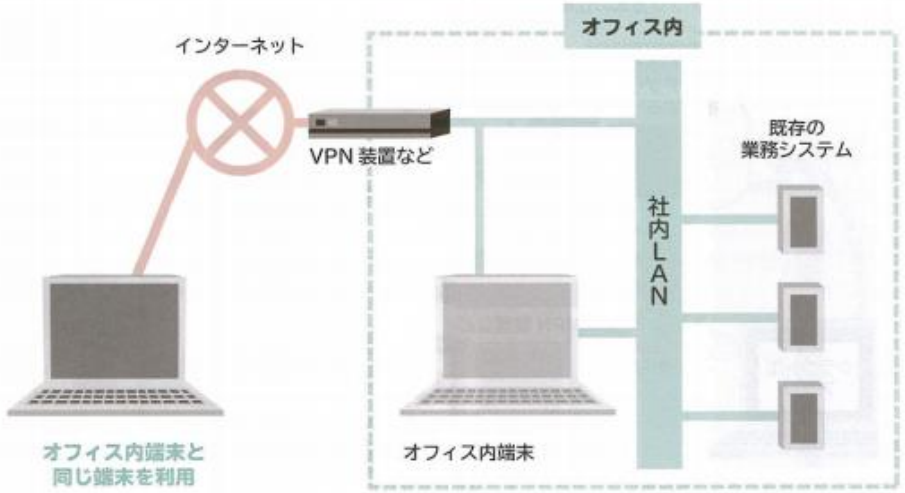
5）アプリケーションラッピング（コンテナ）方式（※システム構成は、基本的にクラウド型アプリ方式と同じ）
moconavi（モコナビ）
コンテナと呼ばれる暗号化した安全な領域を作成し、その中でアプリを動作させる。
BYOD(Bring Your Own Device)の実現
業務で利用するシステムやデータは専用アプリからしか操作できないため、他のアプリから業務データを閲覧したり端末内にデータを保存したりすることはできない

メリット・・手元にデータが残らない
デメリット・・利用コストは契約内容に依存
全てのコンテナは同じOSしか使えない

■テレワークのためのICT環境構築に向けての留意点

6）会社PC持ち帰り方式
主にVPN経由で操作する

メリット・・・使い慣れた端末で操作できる
デメリット・・盗難・紛失による情報漏洩



②技術的セキュリティ対策

1）アクセス管理・制限
端末管理
認証管理（本人認証、端末認証）
アクセスログ・監視

2）暗号化
HDD暗号化
情報漏洩防止機能付きUSB
セキュアコンテナ

3）運用面
電子データの原本保存（電子署名・タイムスタンプ、ブロックチェーン）
ウィルス対策
物理的なセキュリティ・・自宅内のPC施錠棚の有無（執務環境の明記と誓約書）

4）ネットワーク上のセキュリティ
VPN専用ルータなど

※参考：厚生労働省「テレワークではじめる働き方改革」テレワークの導入・運用ガイドブック

■総務省：テレワークセキュリティガイドライン（※システム監査視点をピックアップ）

1．情報セキュリティ保全対策
- セキュリティガイドライン・ルールの策定と浸透（セキュリティポリシー）
- 定期的な実施状況監査
- 情報資産の分類（機密情報、業務情報、公開情報）　→テレワークの持ち出し可能範囲・・業務と公開のみなど
- フォルダのアクセス制御
- ペーパーレス化
- 情報セキュリティ教育・啓蒙活動の継続（テレワーク作業）
- セキュリティ事故発生時の体制・ルール
- 就業規則への罰則規定（抑止効果）

2．マルウェアに対する対策
- フィルタリング
- 追加のアプリインストール原則禁止（許可制）
- ウィルス定義ファイル更新、アップデート

3．端末の紛失・盗難に対する対策
- 貸出端末のセキュリティ対策と端末台帳管理

4．重要情報の盗聴に対する対策
- 無線LANの脆弱性対策（VPN経由など）

5．不正アクセスに対する対策
- 多要素認証（生体認証など）
- アクセスログ

6．外部サービスの利用に対する対策
- 業務目的のSNS利用の禁止

■テレワークのためのICT環境構築に向けての留意点

①マネジメント　②セキュリティの確保　③コミュニケーションの３つの視点が重要

（3）コミュニケーション

会議（音声、Web）、ビジネスチャット（Chatworks）、eメールは消える！？
ビジネスチャットはAPI連携して同時翻訳できるので、相手の母国語を気にせずチャットできる

（その他補足）
※VDT作業における労働安全衛生管理のためのガイドラインについて
ディスプレイ画面上における照度500ルクス以下
書類上及びキーボード上における照度300ルクス以上

テレワーク留意点まとめ

✓ テレワークにはシステムの利用が欠かせないため、自社の業種業態・社員構成などに考慮してシステム方式を決定する必要がある。また、その際におけるセキュリティ対策やルール整備には、システム監査的な視点に十分留意する必要がある。

3．デジタルレイバーと呼ばれるRPAにおけるシステム監査の有用性

■現在、数多くのRPAツールが提供されており、作業品質やサービス品質の向上、生産性向上、間接コストの削減など様々なメリットが教授でき、導入企業も多く存在している。

			対応アプリケーション認識強度 弱→強			
			画面イメージによる認識	一部アプリにてオブジェクト認識	多くのアプリにてオブジェクト認識	多くのアプリにてオブジェクト認識＋VDI(リモートデスクトップ)対応
ロボット配置柔軟性 強→弱	管理機能あり	サーバー集中配置（無人/全自動型）とオペレータPC配置（有人/半自動型）の両方をサポート	Verint(RRA) NEC Software Robot Solution	WinActor/WinDirector	BizRobo/BasicRobo (Kofax Kapow10)	UiPath(Orchestrator含む) Automation Anywhere Pega(RPA+RDA)※1
		サーバー集中配置（無人/全自動型）のみサポート		RPA Express(WorkFusion)	BluePrism NICE(Robotic Automation)	
	管理機能なし	オペレータPC配置（有人/半自動型）をサポート	ipaS CELF RPAオプション (sikulix)	Autoブラウザ名人 (Selenium)	NICE(Desktop Automation)	UiPath(Orchestratorなし)

※1管理機能としては、BPMS管理機能のみを提供。

※資料提供元：株式会社サン・プラニング・システムズ

■RPA導入のリスクについて

（１）アクセス管理、データセキュリティ

社員ではないIDで各種データにアクセスすることから、そのIDが悪用され、データ改ざん、データ漏えいなどにつながるリスクがある。

（２）業務知識のブラックボックス化

自動化により業務知識を有する担当社員が少なくなり、緊急時への対応が困難になるリスクがある。

（３）誤処理のリスク

業務が変更になったにもかかわらず、RPAのロジックが変更されない場合など、RPAによって誤った業務が継続的に実施されるリスクある。

■RPAにおけるシステム監査視点における留意点

（１）全社統制

・RPA導入後における職務権限・責任の明確化
・担当業務の役割・範囲の理解（社員教育）

（２）ＩＴ全般統制

・RPAのロボに対するアクセスコントロール（ユーザーID、パスワード管理）
・ロボットの運用管理（24時間稼働可能、監視）

（３）ＩＴ業務処理統制、業務処理統制

・J-SOX文書（業務フローチャート、RCM、業務記述書）修正
・基本的には、RPA利用によりリスクは軽減されるはず

■ ＩＴ委員会研究報告第42号（スプレッドシート統制の箇所抜粋）
RPA導入時においても参考にすべきと思われる。

区分	統制手続きの例
ロジックの検証	組み込まれたロジックの正確性は検算等により適切に確認されているか。
アクセス・コントロール	スプレッドシートへのアクセスは適切に制限されているか。
変更管理	仕様の確定、テスト、責任者による承認等の手続が正式に定められているか。
バックアップ	バックアップの頻度、対象、保管場所、保存期間は適切か。
バージョン管理	命名規則等の新バージョンのみが使用されるための仕組みはあるか。
データの完全性とセキュリティ	数式やマスター・データ等のデータ処理にとって重要な項目が、不正又は不注意 な変更から保護されているか。
文書化	スプレッドシートの仕様等は文書化され、適切に更新されているか。
他システムとの連携の程度	他システムとのデータのダウンロード・アップロードは自動で行われているか、またアップロードの場合、連携先システムのデータアクセスや変更管理手続が適用されているか。

今後の方向性

✓ 今後AIやRPA利用に関する監査的な方針が示されると思われるが、労働力不足の中、企業生産性向上の中心になると思われる。

４．システム監査の将来的方向性について

■システム監査の目的とは？

「システム監査基準」（平成30年4月改訂）では、システム監査の目的を「情報システムにまつわるリスクに適切に対処しているかどうかを、独立かつ専門的な立場のシステム監査人が点検・評価・検証することを通じて、組織体の経営活動と業務活動の効果的かつ効率的な遂行、さらにはそれらの変革を支援し、組織体の目標達成に寄与すること、又は利害関係者に対する説明責任を果たすこと」としている。

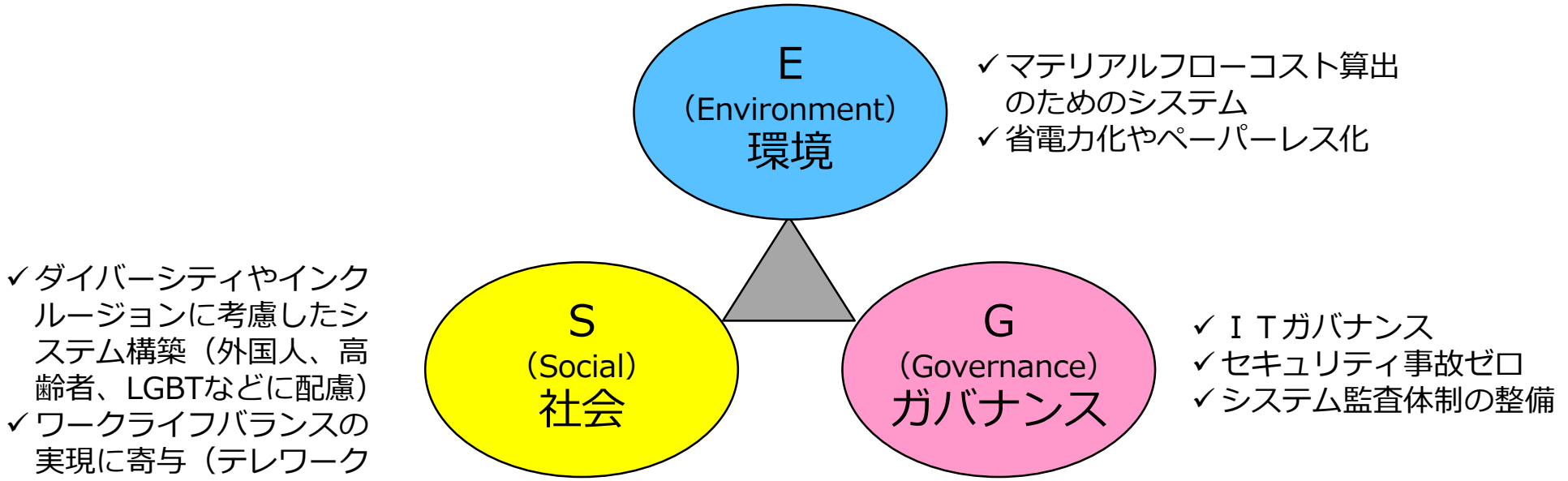
「システム管理基準」（平成30年4月改訂）において「ITガバナンスとは経営陣がステークホルダのニーズに基づき、組織の価値を高めるために実践する行動であり、情報システムのあるべき姿を示す情報システム戦略の策定及び実現に必要となる組織能力である」としている。また、経営陣はITガバナンスを実践する上で、情報システムにまつわるリスク（以下「情報システムリスク」という。）だけでなく、予算や人材といった資源の配分や、情報システムから得られる効果の実現にも十分に留意する必要がある。

つまり

システム監査　→　ＩＴガバナンスの実現　→　組織（企業）価値の向上　→　組織目標の達成に寄与

■今後のシステム監査には、ＥＳＧの視点も必要なのでは？

ESG投資とは、投資家が、環境(Environment)、社会(Social)、統治(Governance)に対する企業の対応を考慮して行う投資。企業の財政や経営状態を示した財務諸表では分からない、二酸化炭素排出量削減や従業員の適切な労務管理、社外取締役の独立性といった各分野への対応が、結果的に企業の長期的な成長や、持続可能な社会の実現につながるという考え方の下、企業の投資価値を測る新たな評価基準のこと。
（「SDGs：2015年9月の国連サミットで採択された国連加盟国が2016年～2030年の15年間で達成するために掲げた目標」とも連動）



システム監査の将来的方向性（個人的見解）

✓ システム監査の実施にあたり、システム監査基準、システム管理基準、情報セキュリティ管理基準をベースにしつつ、ESGのような加点方式（減点方式では無い）の項目を加えることで、企業価値の増大に、より一層寄与することができるのではないかと考えます。

ご清聴ありがとうございました。

Thanks a lot for your time.

Directize
Directize Consulting Group

- 株式会社ディレクタイズ　島﨑　智久
- 〒550-0014
  大阪市西区北堀江1-5-9 北堀江サンシステムBLDB.6F
  TEL：（06）4390-8810　/　FAX：（06）4390-8820
- e-Mail shimazaki@directize.co.jp

「*measure of success*」

There's no time like the present.