Deloitte.

Deloitte Thailand JSG Webinar

アジア進出日系企業のリスクマネジメントとサイバーリスク動向

DELOITTE TOUCHE TOHMATSU JAIYOS ADVISORY CO., LTD.

MAKING AN IMPACT THAT MATTERS since 1845

アジア進出日系企業のリスクマネジメントとサイバーリスク動向

デロイト タイ
シニアマネジャー　畠山 多聞
コンサルタント　藤原 一成

本日の登壇者

畠山　多聞

デロイトタイ

Risk Advisory

シニアマネジャー / 日系企業責任者

経歴

- 2006年 監査法人トーマツ（現 有限責任監査法人トーマツ）に入社。日系・外資系企業の会計監査に従事。J-SOX導入準備及びIFRS導入支援業務も多く手がける。
- 2012年　経済産業省企業会計室に着任。3年間にわたり、国際基準対応や企業と投資家の対話促進に関するコーポレートガバナンス政策立案に従事。
- 2015年 アドバイザリー事業部グローバルグループに帰任し、日系アジア拠点のガバナンス強化に関するアドバイザリー業務に従事。2017年 リスクアドバイザリーインド日系責任者としてデリー事務所駐在。
- 2021年2月より現職。リスクアドバイザリータイ日系責任者としてバンコク事務所駐在。日系企業向けにガバナンス、リスク管理、決算業務、内部統制等の経営管理体制強化に関する支援を行う。

資格

- 公認会計士（日本）

藤原　一成

デロイトタイ

Risk Advisory

コンサルタント / サイバーセキュリティ担当

経歴

- 2018年 デロイトトーマツコンサルティング合同会社に入社。日系企業のサイバーセキュリティアセスメントや官公庁の調達基準策定、サプライチェーン強靭化支援等に従事。
- 2019年 デロイトトーマツサイバー合同会社に出向。日系企業に対するサイバーセキュリティアドバイザリー等に従事。
- 2019年 タイのバンコク事務所に駐在。在タイ日系企業への需要予測精度向上支援や官公庁の日ASEAN協力情報の発信推進支援等を行う。
- 2020年 有限責任監査法人トーマツ リスクアドバイザリー事業部に出向（バンコク事務所への駐在は継続）。日系企業および外資系企業に対するサイバーセキュリティ関連の支援を担当。現在は、外資系自動車メーカーにおけるサイバーセキュリティレビューの支援を行う。

アジア進出日系企業におけるリスクマネジメント

調査目的と調査対象企業等

■調査目的

✓ アジア地域 (インドネシア、シンガポール、タイ、フィリピン、マレーシア、ベトナム、ミャンマー、中国、台湾およびインド) に進出している日系企業におけるリスクマネジメントの対応状況、不正への取組み状況及びCOVID-19に対する対応状況を把握し、現状の基礎的データを得ること

✓ 調査の実施および結果の開示を通じアジア進出日系企業における「リスクマネジメント」の認識を高め日系企業の経営に貢献すること

■調査対象企業

✓ インドネシア、シンガポール、タイ、フィリピン、マレーシア、ベトナム、ミャンマー、中国、台湾およびインドに進出している日系企業の関係会社 (地域統括会社含む)[回答件数(2018年、2019年は過去調査における回答件数)]

	Indonesia	Singapore	Thailand	Philippines	Malaysia	Vietnam	Myanmar	China	Taiwan	India	Total
2018	57	23	87	7	45	-	-	177	-	17	413
2019	69	74	103	15	69	49	53	99	39	32	602
2020	79	88	130	35	73	45	63	61	42	38	654

■調査方法

✓ Webおよび紙ベースによる調査を実施 (2020年9月21日～10月22日)

■調査項目

【第1部】アジアにおけるリスクマネジメント体制

【第2部】アジアにおける不正の発生状況

【第3部】COVID-19に対する対応状況

【第1部】アジアにおけるリスクマネジメント体制

「優先して着手が必要と思われるリスク」について、アジア拠点側ではCOVID-19の影響でサプライチェーンへのリスクがランクインし、これまで以上に対応が求められる

日本本社が考える海外拠点のリスク			アジア拠点が考える海外拠点のリスク	
疫病の蔓延(パンデミック)等の発生	39.6%	第1位	疫病の蔓延(パンデミック)等の発生	39.8%
グループガバナンスの不全	18.5%	第2位	市場における価格競争	29.1%
異常気象(洪水・暴風など)、大規模な自然災害(地震・津波・火山爆発・地磁気嵐)	13.5%	第3位	人材流失、人材獲得の困難による人材不足	17.9%
製品/サービスの品質チェック体制の不備	13.5%	第3位/第4位	従業員の不正・贈収賄等	16.4%
サイバー攻撃・ウイルス感染等による情報漏えい	11.7%	第5位	人件費高騰	15.4%
人材流失、人材獲得の困難による人材不足	11.7%	第6位	為替変動	12.4%
為替変動	10.4%	第7位	米中貿易摩擦の激化	11.5%
市場における価格競争	9.5%	第8位	サプライチェーン寸断	10.7%
事業に影響するテクノロジーの変革	9.0%	第9位	会計・税務関連法規制違反	10.4%
従業員の不正・贈収賄等	8.6%	第10位	原材料ならびに原油価格の高騰	10.2%

■日本本社側では異常気象・災害の発生やサイバー攻撃など事業の継続性に直接影響を及ぼすリスクが認識されている一方、アジア拠点では新興勢力の影響によると考えられる価格競争やアジア拠点ならではの不正・贈収賄など通常のビジネスに関するリスクが認識されており、日本本社側とアジア拠点側とのリスクの認識に明確な違いがでている。
■日本本社側で認識されているがアジア拠点では認識されていないテクノロジーに関連するリスク(サイバー攻撃やテクノロジーの変革)は、アジア側で今後顕在化することが予想される。
■アジア拠点側では米中貿易摩擦の激化が7位にランクインし、米中関係がアジア諸国へ大きく影響を及ぼすことを示唆している。
■アジア拠点側ではCOVID-19の影響でサプライチェーンへのリスクがランクインし、これまで以上に対応が求められる。

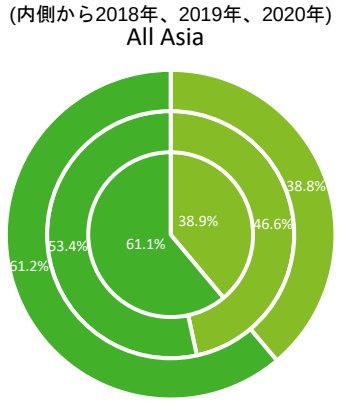
【第2部】アジアにおける不正の発生状況

前年から減少しているものの、依然として回答社数の3分の1以上の会社で不正が発覚している

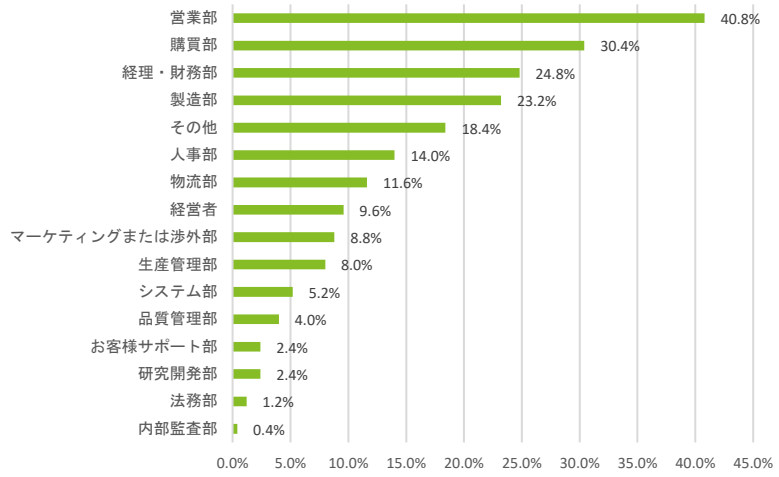
[不正調査：不正の発覚割合の減少はCOVID-19の影響か]

- ✓ 顕在化したまたは懸念がある不正が2年前の水準のほぼ同程度となっているが、COVID-19対応に追われてプロセスのモニタリングや内部監査が十分に行えず、不正発覚が遅れた可能性がある(表1)
- ✓ 引き続き、営業・購買・経理・財務・製造における不正が多い傾向となっている(表2)
- ✓ 不正の種類について、**経費や購買などの不正支出や在庫の横領等に加え、「情報の不正利用、不正な報告」**も多い傾向となり、不正支出や情報に関する統制の整備の必要性を示した結果となった(表3)

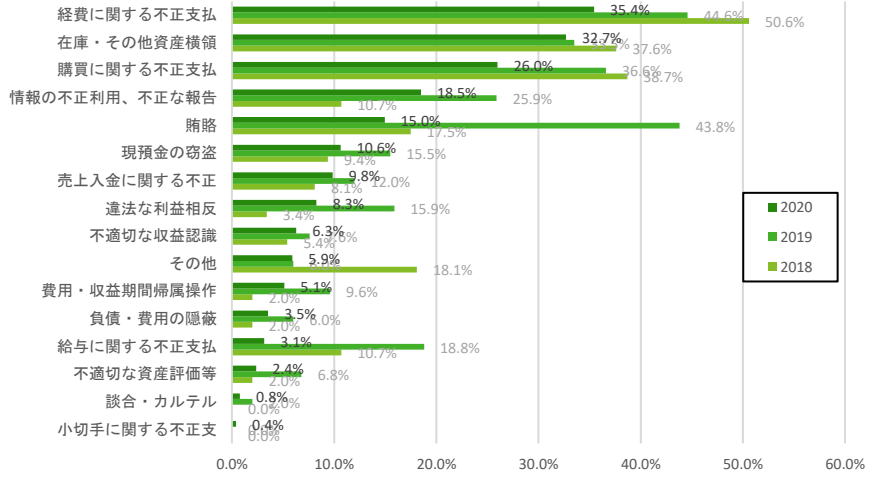
(表1)過去三年間の不正発覚の有無



(表2)不正が発覚した部署

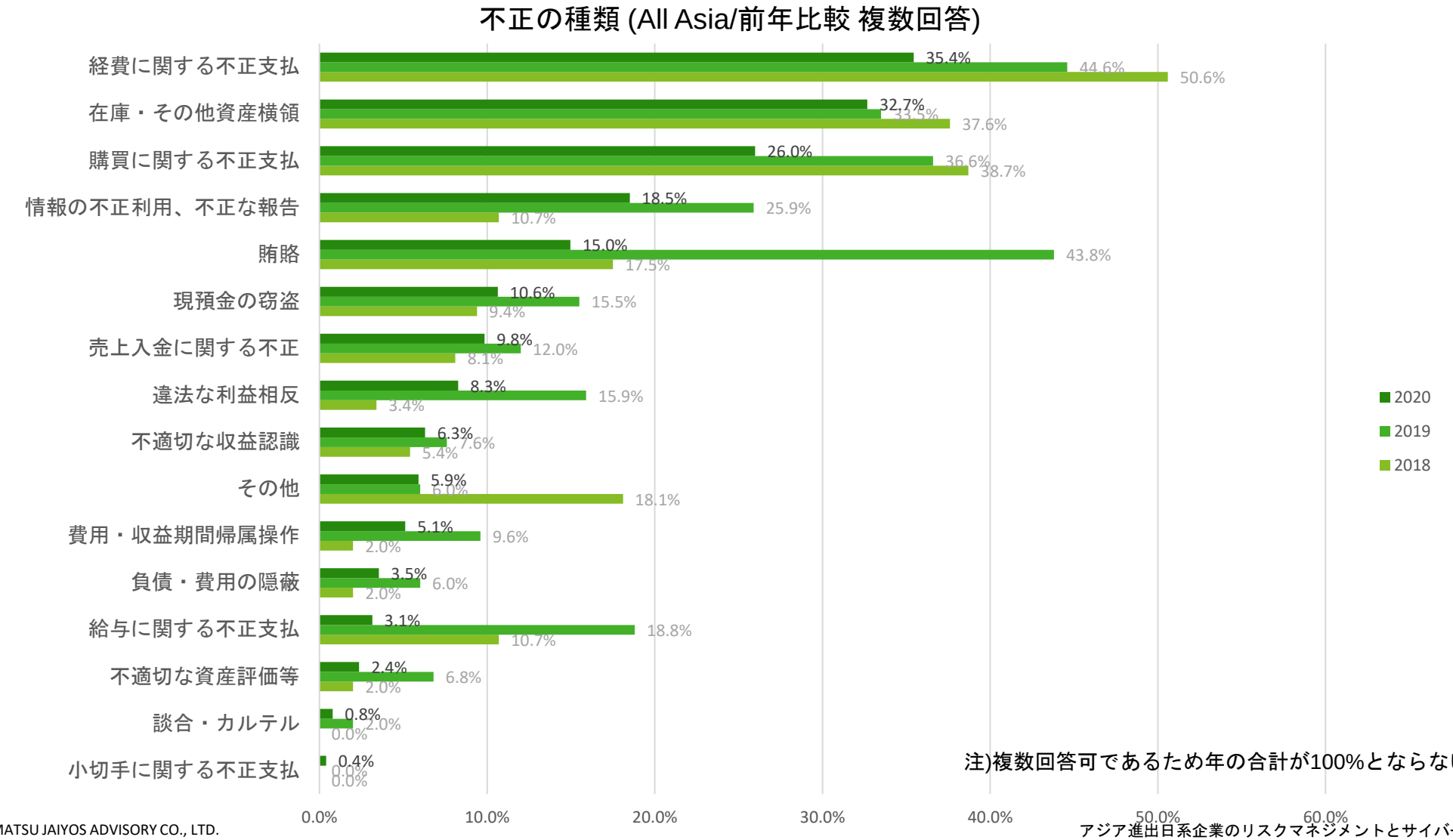


(表3)不正の種類



【第2部】アジアにおける不正の発生状況

不正の種類について、経費や購買などの不正支出や在庫の横領等に加え、「情報の不正利用、不正な報告」も多い傾向となり、不正支出や情報に関する統制の整備の必要性を示した結果となった



注)複数回答可であるため年の合計が100%とならない

【第3部】COVID-19に対する対応状況

日本本社とアジア拠点で業務プロセスの標準化・自動化、リモートワークを見越したペーパーレスの推進等業務プロセス全体の対策が上位に挙げられた

日本本社が考えるCOVID-19対策			アジア拠点が考える海外拠点のCOVID-19対策	
危機管理体制強化	32.9%	第1位	コスト削減	38.8%
企業戦略の見直し	31.8%	第2位	企業戦略の見直し	33.5%
リモートワークの推進	28.0%	第3位	業務プロセスの標準化	20.2%
コスト削減	22.7%	第4位	危機管理体制強化	19.1%
ペーパーレスの推進	18.4%	第5位	リモートワークの推進	16.4%
新商品・サービス開発	17.2%	第6位	新商品・サービス開発	13.6%
業務プロセスの標準化	17.2%	第7位	業務プロセスの自動化	11.9%
セキュリティ強化：予防(例：アセスメント、IT資産管理、脆弱性管理)	16.6%	第8位	資金最適化	11.9%
業務プロセスの自動化	8.7%	第9位	内部統制強化	10.7%
システムの見直し・導入	8.2%	第10位	ペーパーレスの推進	10.6%

- 日本本社とアジア拠点で概ね同様の対策がランクイン。日本側では危機管理体制強化が首位でありガバナンス体制の構築にかかる対策が最も多く挙げられたが、アジア拠点ではコスト削減を挙げる企業が多く、日々のオペレーションでの対応が重視されていることが伺える。
- 日本本社とアジア拠点で業務プロセスの標準化・自動化、リモートワークの推進、ペーパーレスの推進がいずれもランクインしており、業務の変革が求められていることが読み取れる。
- 特にアジア拠点側で業務プロセスの標準化・自動化、内部統制強化が高位にランクインしていることは業務プロセス改善の余地が十分にあり、COVID-19を契機にこれらの課題が顕在化したものと考えられる。

Post /with Covid-19
東南アジア拠点が抱える経営上の課題

Risk Topic in SEA

Post /with Covid-19 東南アジア拠点が抱える経営上の課題

Post /with Covid-19におけるリモートワークや駐在員減員を前提とした**ガバナンス見直し**に際しては、**デジタル活用によるリスク管理の効率化・高度化**が有用。また、デジタル活用に際しては**セキュリティリスク**への留意も必要。

東南アジア拠点が抱える経営上の課題	対策例
戦略的サードパーティリスク管理 サプライヤー、ディラー代理店等のサードパーティーに関する多面的なリスク分析と迅速な意思決定を支援するため、財務データ、取引データ、外部公表データ等を活用した、データベース構築が重要となる	• MIS(マネジメントインフォメーションシステム)の構築
新オペレーションの最適化 リモートワーク導入や人員削減後のリソースの下、持続的な利益体質を実現するため、オペレーション全体(業務量、性質、付加価値等)を見直し、最適なオペレーションを再構築する必要がある	• プロセス/タスクマイニング • アウトソース及びRPA導入
不正リスクのモニタリング 人員削減、給与カット等の人事施策の結果として生じるモチベーション低下に起因する不正リスク(横領、親族企業を絡めた不公正取引、機密情報持ち出しなど)を抑止する必要がある	• データアナリティクス(購買経費等) • リモート監査
サイバーセキュリティ対策 ITシステムや情報機器を可視化のうえ、SEA拠点におけるセキュリティリスク・脆弱性を網羅的に導出することで、セキュリティ対策の抜け漏れやバラつきつきへの対策が不可欠である	• 法規制対応 • アセスメント/侵入テスト • セキュリティトレーニング

サイバーセキュリティの動向

今後の考えられるシナリオ

サイバー脅威の増加により、サイバーインシデントがいつ発生しても不思議ではない状況に加え、サイバー意識の高まりに伴う客観的なサイバー能力の説明や担保、および各国の法規制にも対応が必要となってくると考えられる

今後起こり得るシナリオ	シナリオに至る材料
法規制への対応が必要となる	✓ 東南アジア各国でサイバーセキュリティ関連の法規制が整備されてきている動きがある ✓ タイでは2019年に個人情報保護法が策定、現在は本施行まで延長期間中
客観的なサイバーセキュリティ能力の証明が必要となる	✓ 各業界のサイバーセキュリティに対する意識が高まっており、取引先を選定する際にもサイバーセキュリティ能力がどの程度有するかが重要視されている ✓ タイでは中央銀行BOTがタイの銀行に年に一回の侵入テストを求めている
サイバーインシデントが発生する	✓ 東南アジアではサイバーインシデントが多く発生している ✓ HQのセキュリティ予算に比べて、東南アジアの拠点に投入されるセキュリティ予算は低い傾向にあり、サイバーセキュリティ対応は後回しになりがち ✓ 従業員のサイバーセキュリティへの意識が低い傾向、および専門性を持った人材が不足している

東南アジア進出日系企業のサイバーに係る取り組み

在東南アジアの日系企業は、サイバーセキュリティアセスメントやトレーニング等、サイバーセキュリティを重要経営アジェンダと位置づけて取り組んでいる

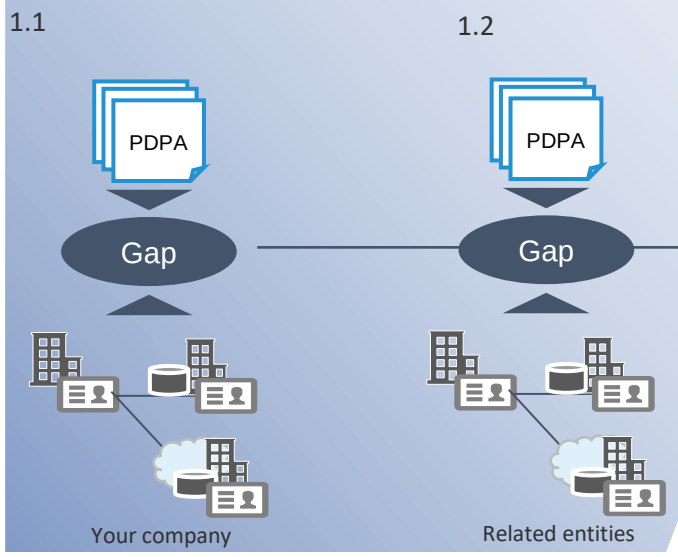
今後起こり得るシナリオ	対応方針	サイバーに係る取り組み（例）
法規制への対応が必要となる	▪ 準拠すべき法規制の整理 ▪ 対応するための人員確保・体制整理 ▪ 法規制対応のタイムライン検討	1 PDPA (個人情報保護対応)
客観的なサイバーセキュリティ能力の証明が必要となる	▪ 全般的なサイバーセキュリティアセスメントを実施し、自社のサイバーセキュリティ能力を把握および整理 ▪ 特定システムの侵入テストを実施して脆弱性や改善ポイントが無いかを確認	2 Cybersecurity Assessment (サイバーセキュリティアセスメント)
サイバーインシデントが発生する	▪ 従業員のサイバーセキュリティへの意識向上 ▪ サイバーインシデント発生時の対応を確認	3 User Awareness Testing (従業員の意識テスト)

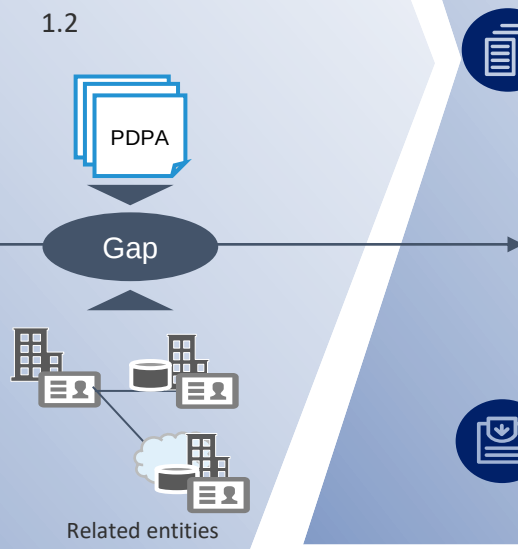
1. PDPA (個人情報保護対応)

現状を把握、法令の要請事項との比較を行い、Gap事項を改善することでPDPAに準拠した個人情報保護態勢を構築する

1. Gap分析フェーズ

1. 貴社において保有している個人情報及び管理状況の確認、法令との比較、Gap事項に対する改善案の策定を行う
2. 貴社関連会社に関しても上記と同様に、個人情報及び管理状況の確認、法令との比較、Gap事項に対する改善案の策定を行う（例：日本本社、販売会社など）



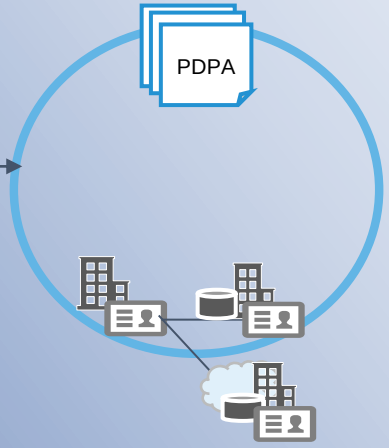


2. 導入フェーズ

改善案に従い、規程整備、システム対応等を行い、個人情報管理態勢を構築する

3. 確認フェーズ

構築した個人情報管理態勢について追加ガイドライン等との整合等、法令遵守状況を最終確認する



1. PDPA (個人情報保護対応) - Key requirements

1 PDPA (個人情報保護対応)
2 Cybersecurity Assessment (サイバーセキュリティアセスメント)
3 User Awareness Testing (従業員の意識テスト)

1. 説明責任ガバナンス

- ❑ PDPA Governance Framework
- ❑ Appoint DPO
- ❑ DPO's qualifications and structure in the organization
- ❑ Privacy Policy
- ❑ Training Awareness

2.処理の合理的理由

- ❑ Lawfulness of processing

3. データ主体の権利

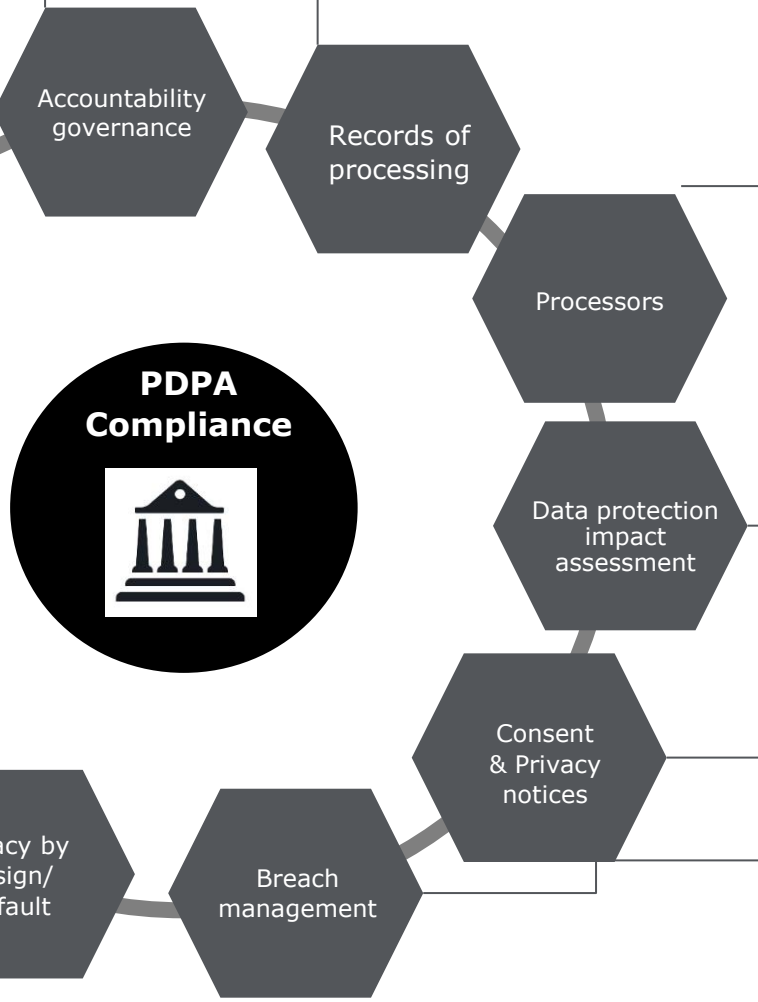
- ❑ Data subjects Rights Management

4. 国外移転

- ❑ Standard Contractual Clauses
- ❑ Binding Corporate Rules

5. プライバシーバイデザイン

- ❑ End to end security measures
- ❑ Set privacy as a default setting



6. データ処理記録

- ❑ Record or processing activities and data inventory

7. データ処理者

- ❑ Third Party Due diligence
- ❑ Data Processing Agreement

8. データ保護影響評価

- ❑ DPIA for High Risk of processing

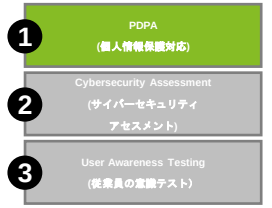
9. 同意取得及びプライバシー通知

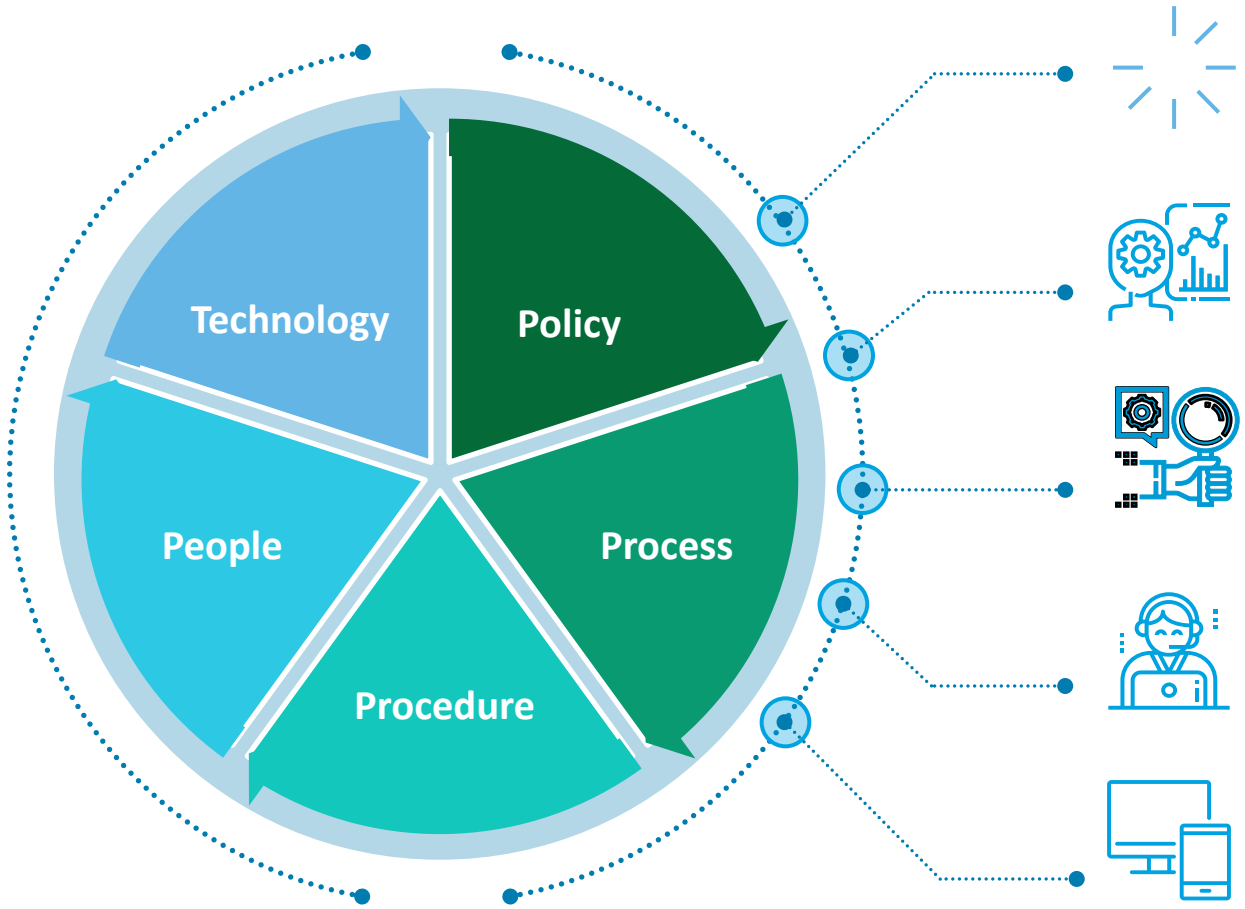
- ❑ Consent Management
- ❑ Consent form
- ❑ Privacy Notice

10.データ漏洩管理

- ❑ Privacy Incident Management
- ❑ Data Breach Notification

1. PDPA (個人情報保護対応) - 改善対応　PDPA Impacts – Overall





Policy and Governance

- Policies developed or embedded in the policy of the organization for example Personal Data Protection Policy, Security Policy, PDPA Incident Management Framework　関連規程・ポリシーの見直し

Process

Working process being revised and communicated throughout the organization on the awareness of personal data protection.　業務プロセスの見直し及び周知

Procedure

Procedure being develop under the privacy principle and ensure control throughout the organization　標準手続及びコントロールの見直し

People

All Employees need to have an awareness and sufficient understanding on the PDPA and data privacy.　従業員等に対するプライバシー意識向上

Technology

Technology need to be developed and implemented to align with the requirements of PDPA and enhance security & privacy and control processes.
ITシステムの見直し及び機能追加

1 PDPA
(個人情報保護対応)

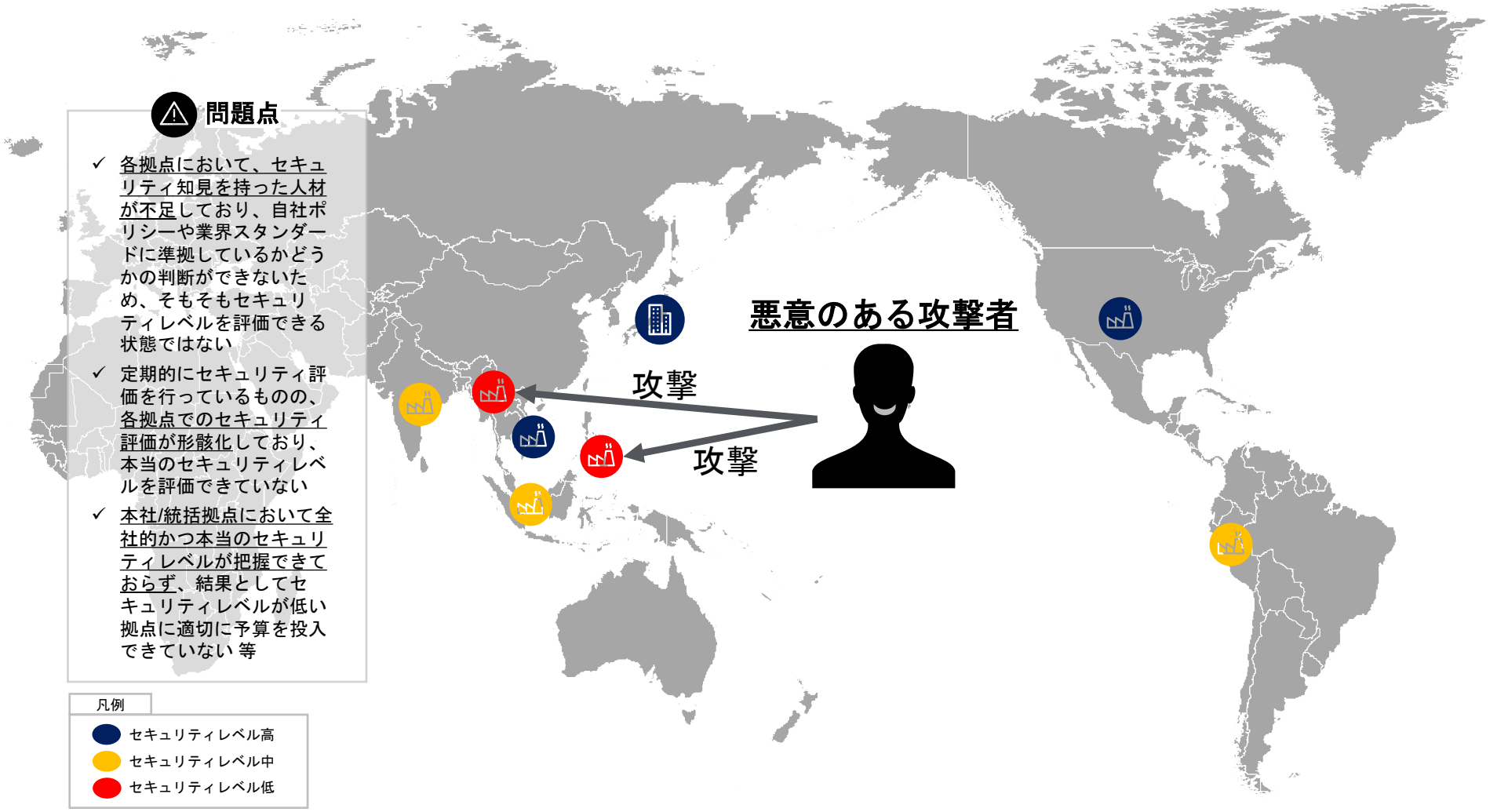
2 Cybersecurity Assessment
(サイバーセキュリティ
アセスメント)

3 User Awareness Testing
(従業員の意識テスト)

2.各拠点のセキュリティレベルのばらつきと問題点

セキュリティレベルの低い拠点は悪意のある攻撃者からの攻撃の穴になり得るため、

客観的な現状把握と高セキュア化に向けた適切なロードマップを策定することが必要です



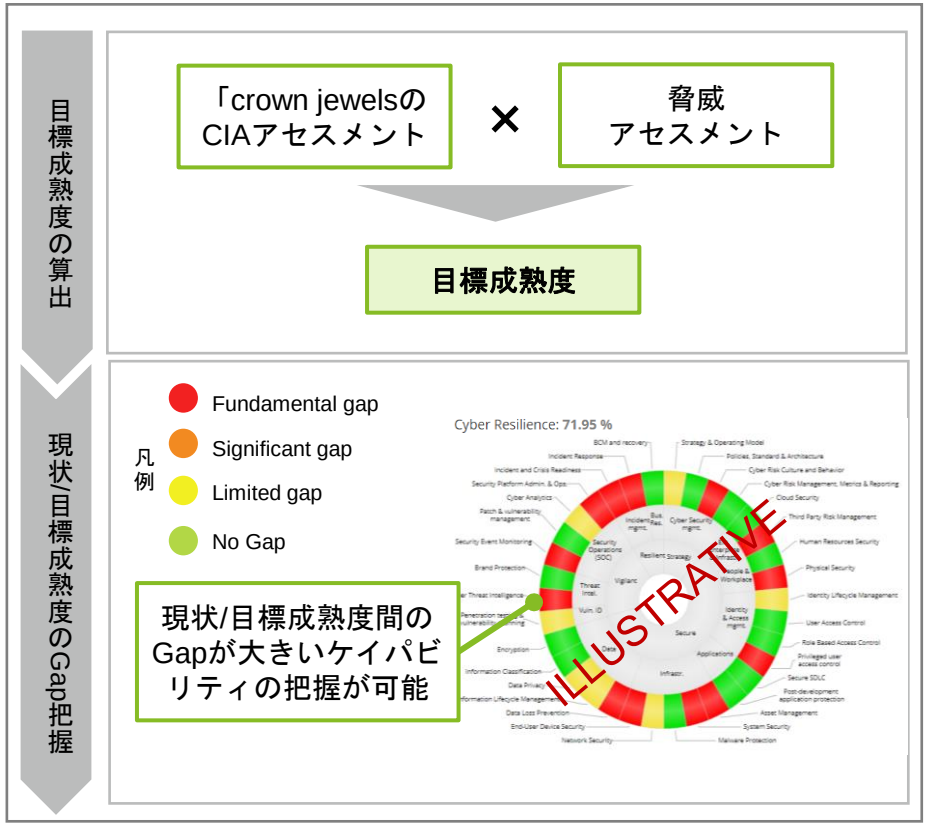
2. Cybersecurity Assessment (サイバーセキュリティアセスメント)

現状の成熟度と目標の成熟度間のGapを示すとともに、同業他社との
ベンチマーク比較により、高度化が望まれる領域が明示的に特定可能です

1. PDPA (個人情報保護対応)
2. Cybersecurity Assessment (サイバーセキュリティアセスメント)
3. User Awareness Testing (従業員の意識テスト)

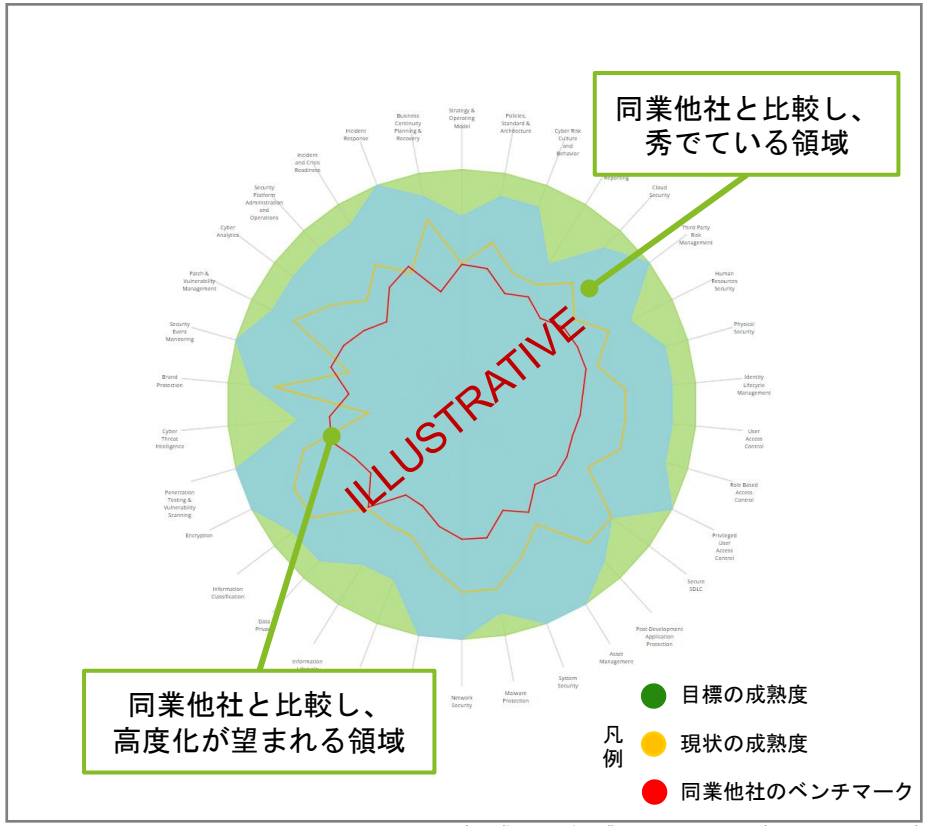
目標の成熟度の設定によるGap把握

- 「crown jewels」のCIAアセスメントと脅威アセスメントにより、サイバーケイパビリティ毎の目標の成熟度を自動的に算出する



ベンチマーク比較

- サイバーケイパビリティ毎に詳細なレベルで同業他社との現状の態勢状況を比較することで対策が望まれる領域や他社に比べて秀でている領域を把握する



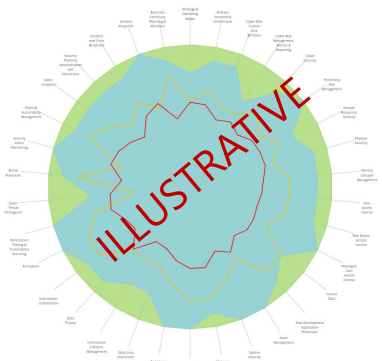
【参考】サイバーセキュリティアセスメントの報告イメージ

1. PDPA（個人情報保護対応）
2. Cybersecurity Assessment（サイバーセキュリティアセスメント）
3. User Awareness Testing（従業員の意識テスト）

ケイパビリティビュー

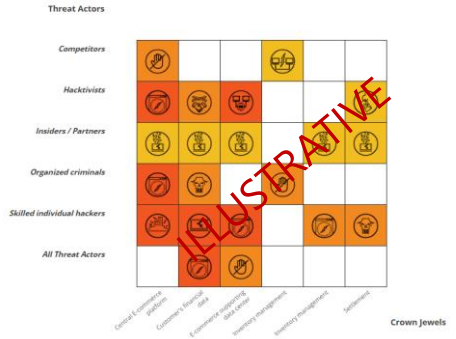
- サイバーケイパビリティの現状の成熟度をアセスメントした結果から算出された成熟度と目標の成熟度とのGapの大きさを、ケイパビリティ毎に可視化

成熟度ビュー



- 現状の成熟度をアセスメントした結果と目標の成熟度とのGapをケイパビリティ毎に可視化
- 同業他社とのベンチマーク比較の結果を可視化

脅威ビュー



- 脅威アセスメントの結果を可視化

トレンドビュー

- サイバーケイパビリティの成熟度の増減の経過を可視化

ハウスビュー

- ビジネス特性とサイバーケイパビリティの現状および目標成熟度とのGapを可視化

リスク許容度ビュー

- 組織のビジネス特性の把握や「crown jewels」のCIAアセスメントから、組織のリスク許容度を可視化

3. User Awareness Testing (従業員の意識テスト）

フィッシングやテスト用のUSBを実際に執務室に設置する等のプログラムを企画し、

サイバーセキュリティへの意識度を定量的に測り、レポートします

1. PDPA（個人情報保護対応）
2. Cybersecurity Assessment（サイバーセキュリティアセスメント）
3. User Awareness Testing（従業員の意識テスト）

Phishing (フィッシング)

Entice to Click

Email may contain malicious links with a sense of urgency to lure users into clicking it

Please give me your credentials!

Phishing attempts may try and extract your sensitive account information

To open that Attachment or not?

Emails may contain malicious attachments which can infect your device with a harmful virus

USB Drop test (USBドロップテスト)

Logo / label

USB drive may have customized logo/labeled to increase chance of a curious staff plug the USB drive in their computer

To open file or not?

USB may contain malicious files which can infect your device with a harmful virus

Rogue access point (偽アクセスポイント)

Similar looking network

Setting up rough AP to lure users to connect and login

Credential for connecting network

You may be prompt to enter your credential to access network

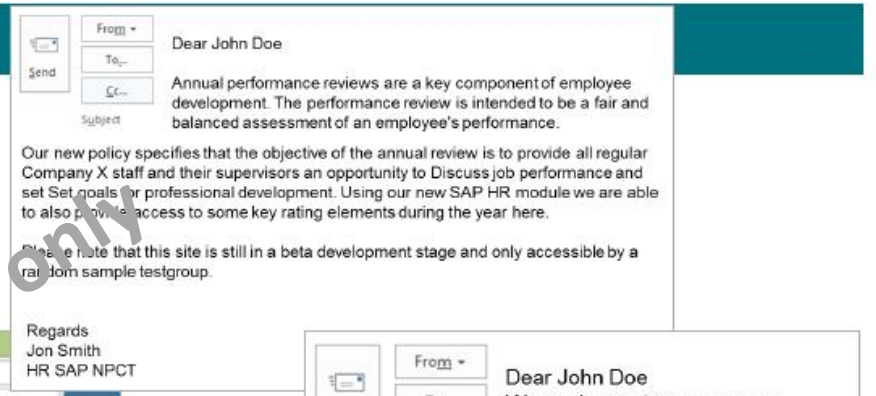
Tailgating (共連れ入室)

Access restricted area

Following someone into a secured or restricted area

【参考】Phishing (フィッシング)

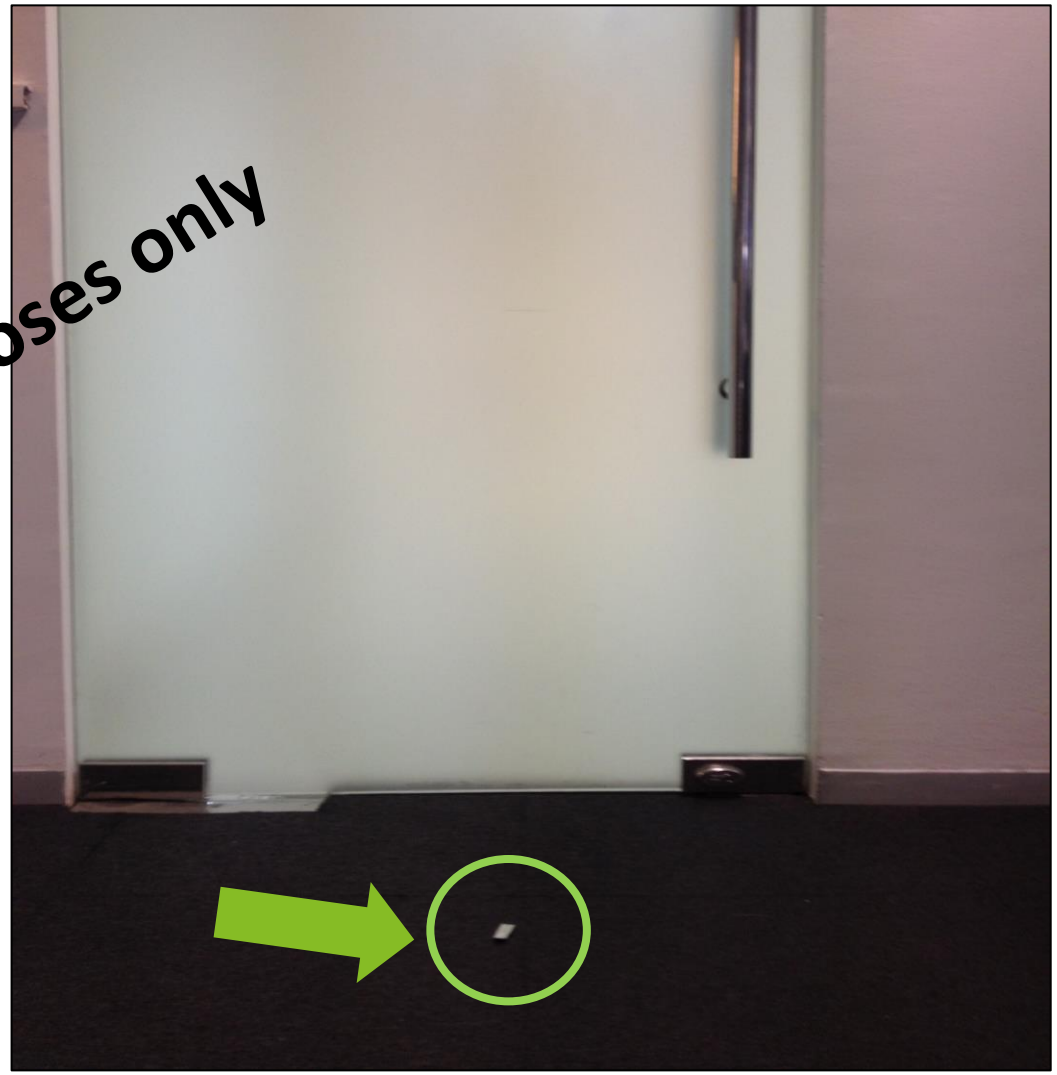
1. PDPA (個人情報保護対応)
2. Cybersecurity Assessment (サイバーセキュリティアセスメント)
3. User Awareness Testing (従業員の意識テスト)



【参考】USB Drop Test (USBドロップテスト)

1. PDPA (個人情報保護対応)
2. Cybersecurity Assessment (サイバーセキュリティアセスメント)
3. User Awareness Testing (従業員の意識テスト)

For illustrative purposes only



まとめ：サイバーリスク対策の全体像

セキュリティの取組みとしては、全社横断的な検討及び対応と、各製品及び製品プラットフォームのセキュリティ対策の実行が両軸で必要

	エンタープライズ	工場	商材（製品・サービス）
主なリスク	情報のCIAの侵害	生産ラインの停止	商材の品質に係る問題
守るべきもの	✓ データビジネスの信頼性 ✓ システムの安定稼働	✓ OTシステムのセキュリティ ✓ 工場のセーフティ	✓ 提供する商材自体のセキュリティ

検討すべきセキュリティ対策

検討範囲

自社（特定／防御／検知／対応／復旧）

- ガバナンス・推進体制構築（組織設計、規程整備など）
- ITセキュリティ対策（組織・プロセス・人・技術・物理）／CSIRT
- OTセキュリティ対策（組織・プロセス・人・技術・物理）／FSIRT
- 製品セキュリティ対策（Security By Designなど）／PSIRT

外部（上位／下位）

- サプライチェーンセキュリティに係る組織の方針検討、各カンパニーへの展開など
- 要求事項等の特定・対応
- サプライチェーンの透明化（サプライヤ管理、ICT管理）
- 要求事項等の特定・対応
- サプライチェーンの透明化（サプライヤ管理、ICT/OT管理）
- 要求事項等の特定・対応
- サプライチェーンの透明化（サプライヤ管理、IoT部品管理）

Deloitte.