

Deloitte.



Risk Advisoryサービス紹介

Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.

東南アジア/タイ拠点がとるべきセキュリティ対策

今後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ると考えられる

今後起こり得るシナリオ



法規制への対応が必要となる



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



サイバーインシデントが発生する

シナリオに至る材料

- ✓ 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
-
- ✓ 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
-
- ✓ 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



法規制への対応が必要となる



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



サイバーインシデントが発生する

対応方針

- 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
-
- 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
-
- 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

サイバーに係る取り組み（例）

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)

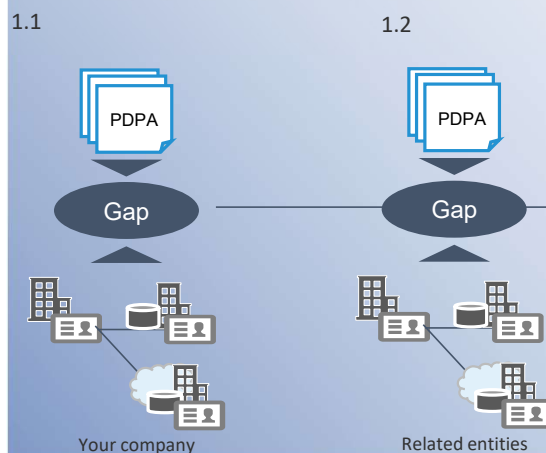
1. PDPA (個人情報保護対応)

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	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)

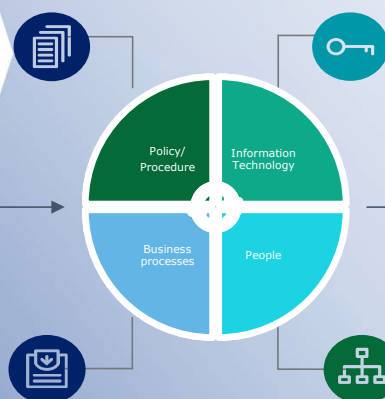
1. Gap分析フェーズ

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)



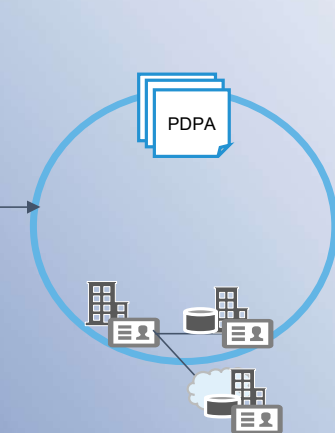
2. 導入フェーズ

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



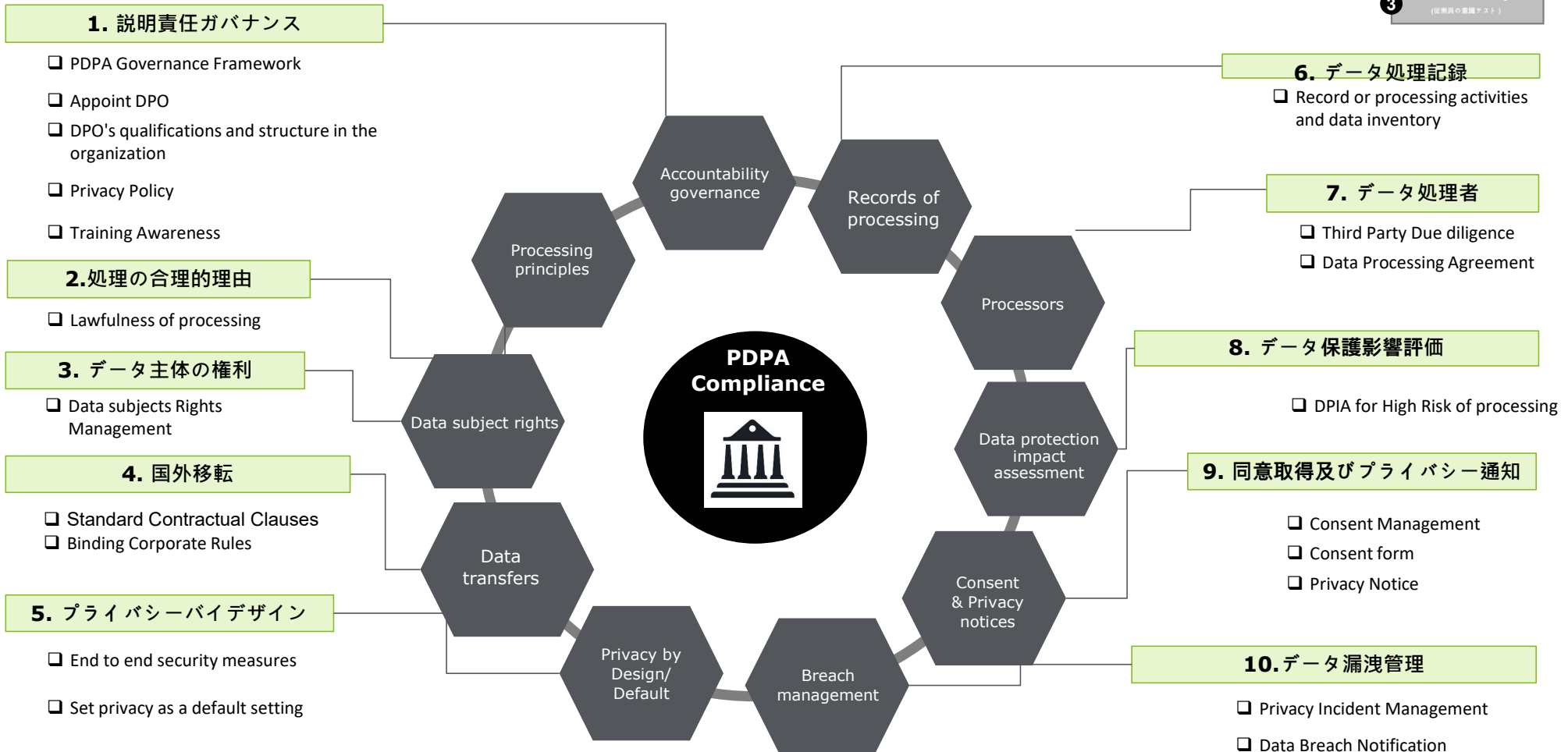
3. 確認フェーズ

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



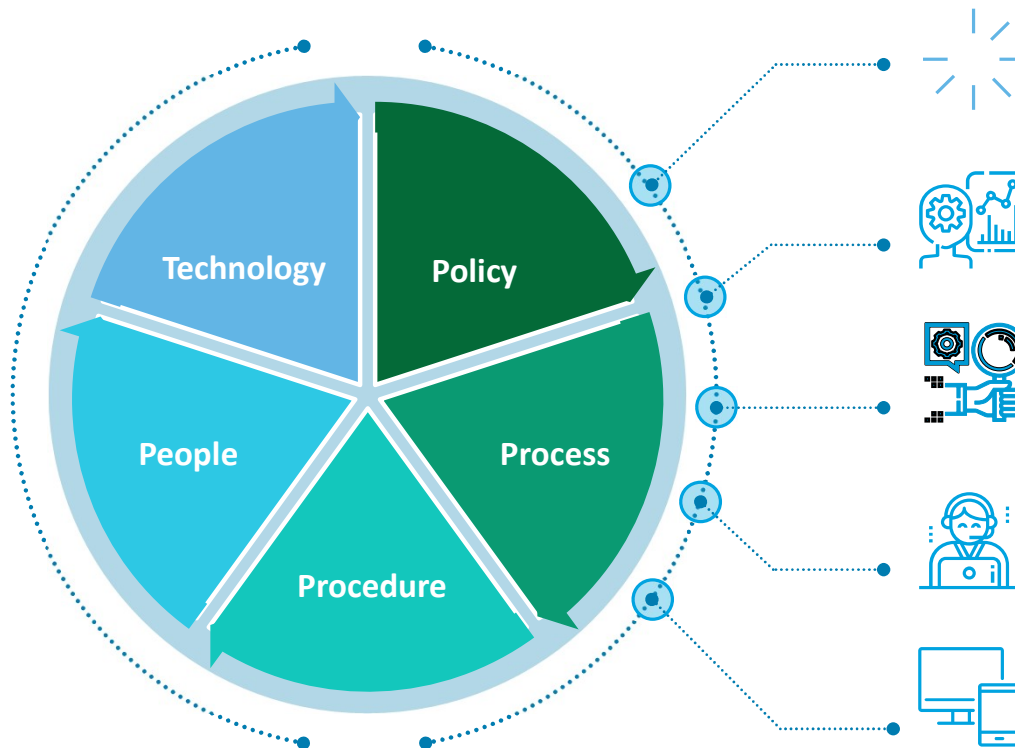
1. PDPA (個人情報保護対応) - Key requirements

- 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 (従業員意識テスト)



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

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)



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

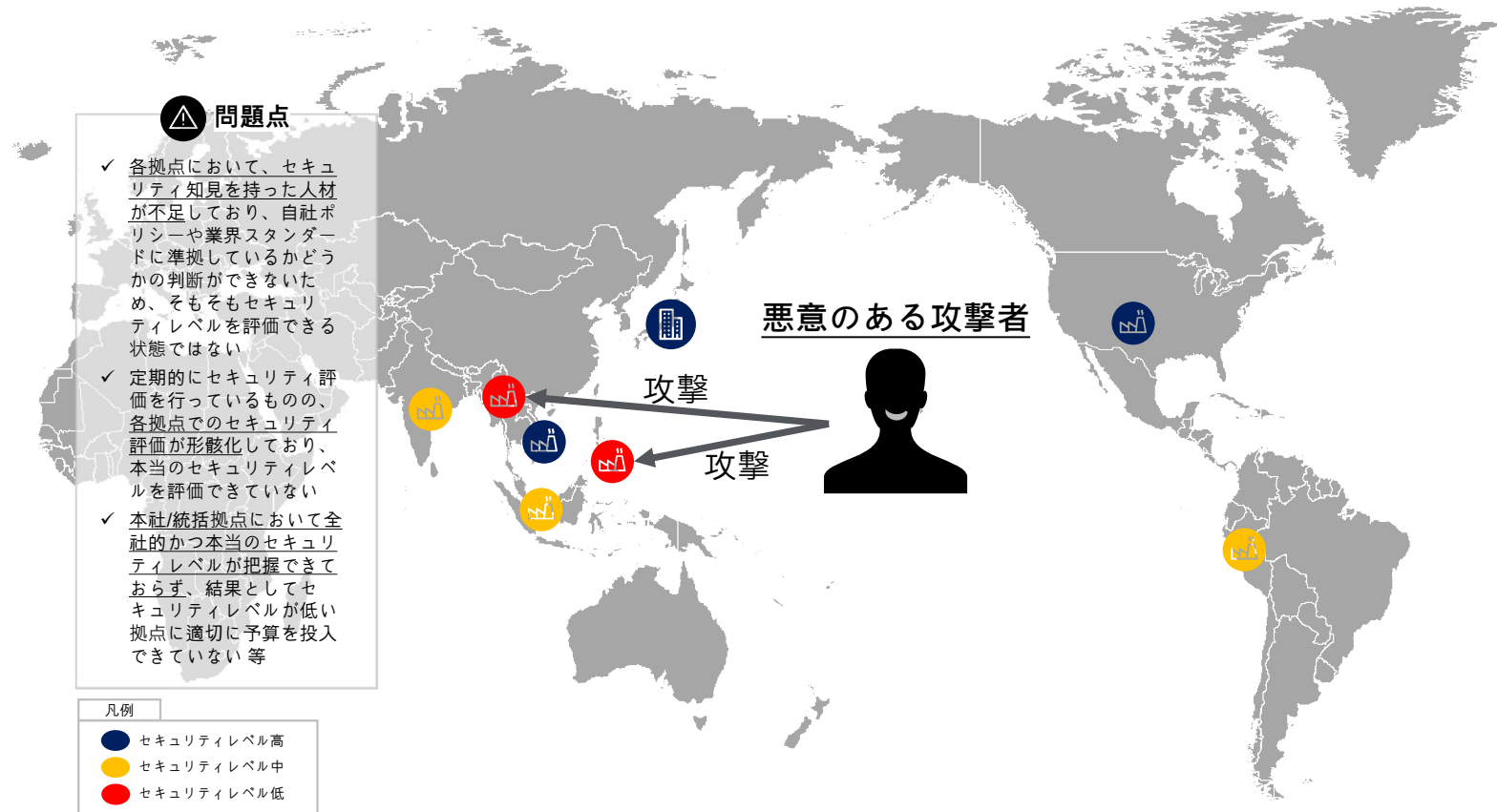
All Employees need to have an awareness and sufficient understanding on the PDPA and data privacy. 従業員等に対するプライバシー意識向上

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

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

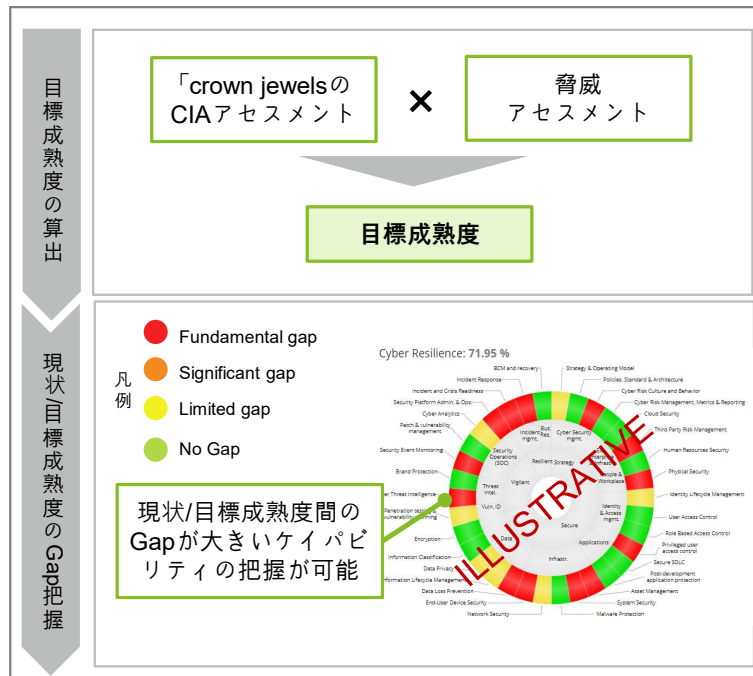


2. Cybersecurity Assessment (サイバーセキュリティアセスメント)

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

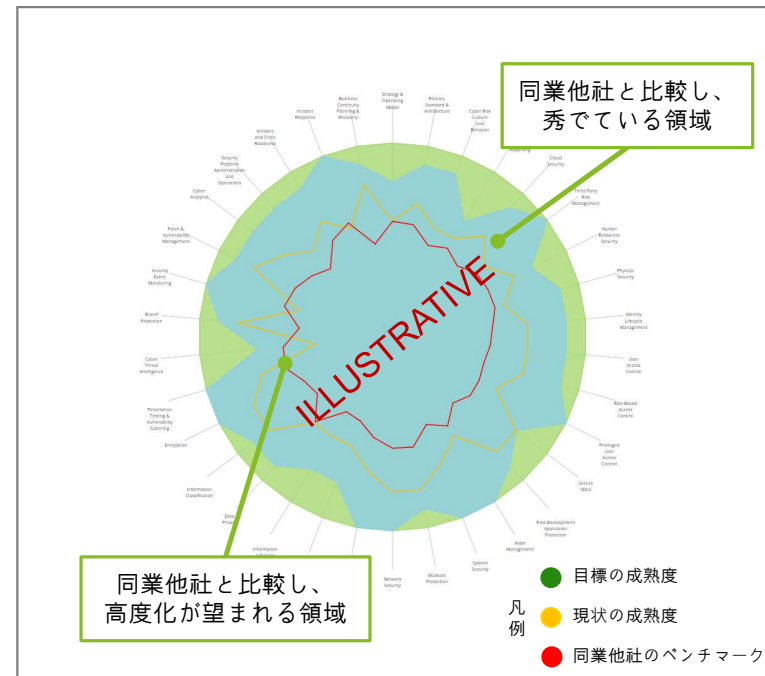
目標の成熟度の設定によるGap把握

- 「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



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



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 rogue 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)



Eni Cli

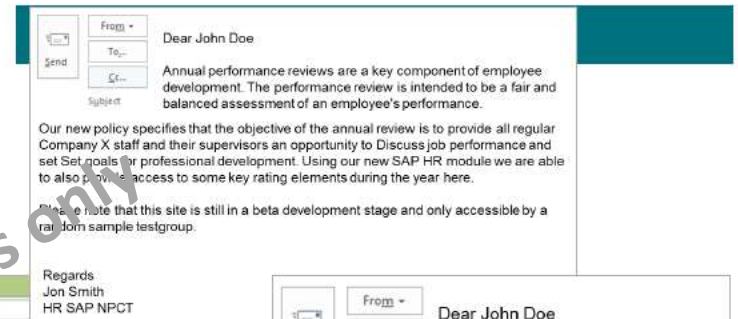


Access restricted area

Following someone into a secured or restricted area

【参考】Phishing (フィッシング)

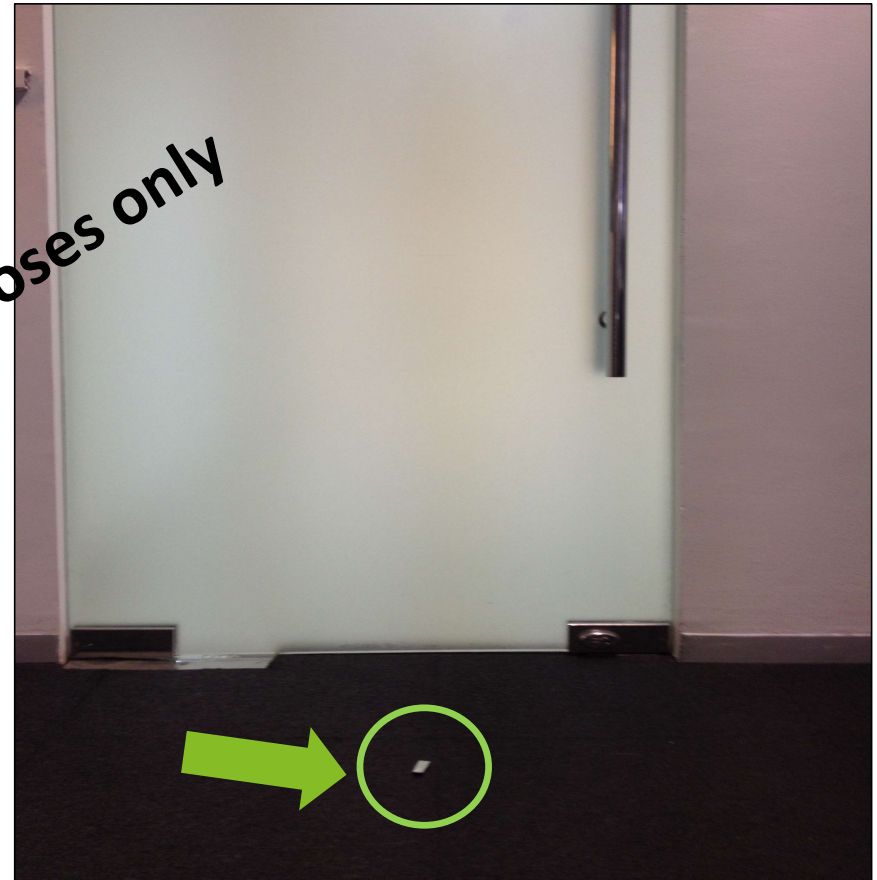
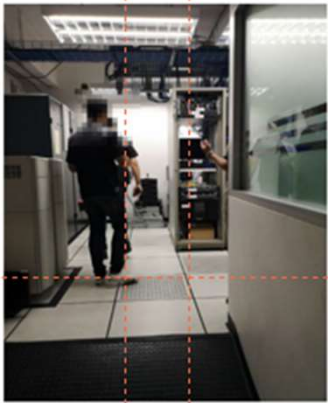
- 1 PDPA (個人情報保護対応)
- 2 Cybersecurity Assessment (サイバーセキュリティアセスメント)
- 3 User Awareness Testing (従業員の意識テスト)



For illustrative purposes only

【参考】USB Drop Test (USBドロップテスト)

- ① PIPA
(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)






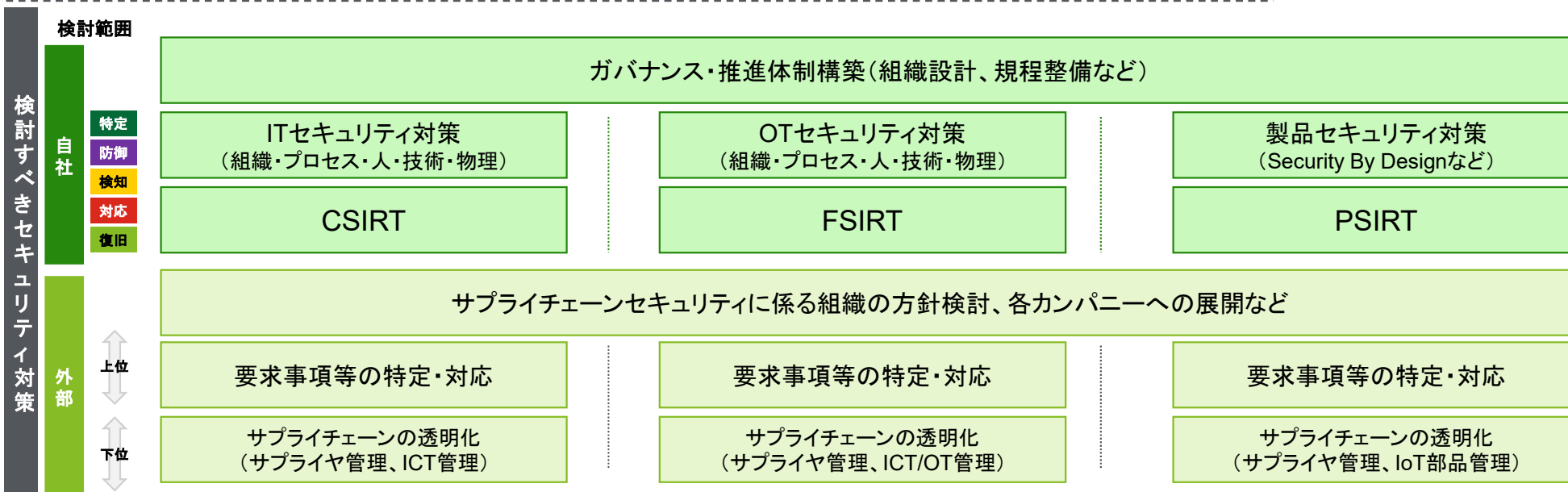
Member firms and DTTL: Insert appropriate copyright
[To edit, click View > Slide Master > Slide Master]

Presentation title
[To edit, click View > Slide Master > Slide Master]

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	<ul style="list-style-type: none"> ✓ データビジネスの信頼性 ✓ システムの安定稼働 	<ul style="list-style-type: none"> ✓ OTシステムのセキュリティ ✓ 工場のセーフティ 	<ul style="list-style-type: none"> ✓ 提供する商材自体のセキュリティ





Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

About Deloitte Thailand

In Thailand, services are provided by Deloitte Touche Tohmatsu Jaiyos Co., Ltd. and its subsidiaries and affiliates.

This document has been prepared by Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd. for the sole purpose of providing a proposal to the parties to whom it is addressed in order that they may evaluate the capabilities of Deloitte Touche Tohmatsu Jaiyos Co., Ltd. to supply the proposed services.

The information contained in this document has been compiled by Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd. and includes material which may have been obtained from information provided by various sources and discussions with management but has not been verified or audited. This document also contains confidential material proprietary to Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd. Except in the general context of evaluating our capabilities, no reliance may be placed for any purposes whatsoever on the contents of this document or on its completeness. No representation or warranty, express or implied, is given and no responsibility or liability is or will be accepted by or on behalf of Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd. or by any of its partners, members, employees, agents or any other person as to the accuracy, completeness or correctness of the information contained in this document or any other oral information made available, and any such liability is expressly disclaimed.

This document and its contents are confidential and may not be reproduced, redistributed or passed on, directly or indirectly, to any other person in whole or in part without our prior written consent.

This document is not an offer and is not intended to be contractually binding. Should this proposal be acceptable to you, and following the conclusion of our internal acceptance procedures, we would be pleased to discuss terms and conditions with you prior to our appointment.

© 2021 Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.