今すぐアクション！ 信頼を支える、現地責任者の確かな備え

在タイ日系企業が直面している内外からの脅威

脅威の代表例として不正やサイバー攻撃が挙げられますが、社内にて十分な備えを行うことは難しい分野です。また、限られた資源の中で有効かつ実効性のある備えを行うためには、在タイ現地責任者が外部の知見を取り入れつつ、本社と連携し、現地の文化や環境を踏まえた対策を主導することが求められています。

日本人経営者だけでは不正を発見し、対応することが難しい	海外子会社は本社より不正やサイバー攻撃のリスクが高い	サイバー攻撃の対象は本社や大企業よりも海外拠点や中小企業が中心

内部脅威：経営陣や従業員による不正

Key Points

- タイでは経営陣や従業員による不正が多い
- 日本人経営者や自社内だけでの対応は難しい
- 予期せぬ事態に備えた事前の対応が重要

年次の会計監査や内部監査で不正は検知されていないので、当社は問題なく対策できているのでは？

会計監査や内部監査を受けていても、多くの企業で不正が潜在しています。

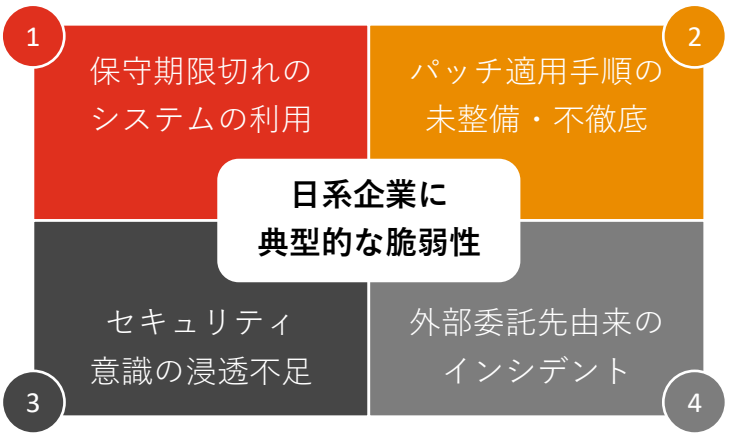
Alert
- ✓ 不正検知に特化した調査が不十分
- ✓ 特定の従業員への権限集中
- ✓ 詳細不明なタイ語のみの書類に対する口頭補足と承認

タイにおける不正対応を穏便に進めるには第三者の利用が有効です。

外部脅威：サイバー攻撃

Key Points

- サイバー攻撃は年々増加しており、現地の大企業よりも対策の不十分な日系企業のタイ拠点を含む中小規模の組織への攻撃が増加している
- 製造ラインの停止やシステム総入れ替えなど甚大な被害が発生している
- 対策の実効性を保つためには、本社主導の全社的対策だけではなく、現地法人としてのセキュリティの管理が必要



ファイアウォールやアンチウィルスソフトを導入しているので、最低限の対策はできているのでは？

現地拠点に求められる「必要最低限」の水準は高くなっています。

Alert
- ✓ セキュリティ担当者の不在
- ✓ IT環境・リスクへの理解が不十分
- ✓ 日本人に対策状況が共有されていない
- ✓ 定期的な見直しが行われていない
- ✓ 本社との役割分担が不透明

「今」攻撃を受けたとしても本社や取引先への説明責任を果たせる備えが求められます。

在タイ
日系企業向け

不正対策・サイバー対策のご案内

不正リスクへの対応

現状理解、調査・是正、継続的改善を含めた、一気通貫した不正対策をご提供します。

現状理解	ヘルスチェック	不正対策手続や通常業務に係る全社観点でのポリシー・プロセスのレビューや関係者へのインタビューを通じて、不正リスクを評価します。
	不正リスクアセスメント	不正対策手続や通常業務に係る業務観点でのポリシー・プロセスのレビューや関係者へのインタビューを通じて、不正リスクを評価します。また、貴社のご要望に合わせて、評価に加えてポリシー・プロセスの構築も実施します。
調査・是正	不正調査・フォレンジック	発覚した不正・不祥事の詳細な調査や、疑わしい人物・取引に係る裏付けの取得を支援します。デジタルフォレンジックを通じた証拠保全から、不正実施者への措置、再発防止策の策定まで一貫したご支援をご提供します。
継続的改善	内部監査（不正対応）	不正対策の観点からの内部統制評価やデータ分析による不正の兆候の検証を、内部監査の一環としてご支援します。監査手続の策定から実行支援まで、貴社のご要望に合わせたサービスをご提供します。
	内部通報制度	タイ語・英語による内部通報窓口の提供によりローカルスタッフからの声を集約し、貴社のマネジメント層にご報告します。通報された事象への対応から実効性を高めるための体制構築支援まで幅広くご支援します。

サイバーセキュリティリスクへの対応

簡易評価から実践的対策まで、貴社のご状況に合わせたセキュリティサービスをご提供いたします。

	Starter Plan	Standard Plan
サイバーヘルスチェック	在タイ日系企業に課題の多い領域を対象にセキュリティ対策状況を簡易評価	ISO,NIST CSFなどのガイドラインに基づく包括的なセキュリティ対策状況の評価
サイバー対策構築支援	規定類のレビュー・作成・更新やインシデント対応体制の構築支援	平時のモニタリングやシステム管理態勢を含む包括的なリスク管理態勢の構築支援
研修・訓練	基本的なセキュリティの考え方や管理策、個人レベルの注意事項などの研修	フィッシングメール訓練やUSB Drop訓練など実際の攻撃を想定した実践的訓練
内部監査（サイバー）	サイバーセキュリティや法令対応の観点を踏まえた内部監査計画・手続の策定	内部監査の実行支援および内部監査人へのOJTによる知見の移転
復旧対応支援	インシデント対応体制・プロセスのレビューおよび構築支援	実際にランサムウェア・マルウェアの攻撃を受けた際の対応・復旧支援
サイバーフォレンジック	サイバーインシデント発生時に、証拠の収集や影響範囲の特定、関係各所への報告などインシデント対応の包括的なサポート	

お問い合わせ先

不正対策

Phansak Sethsathira
Risk Assurance Partner
phansak.s.sethsathira@pwc.com

魚住 篤志 ／ Atsushi Uozumi
Partner
atsushi.uozumi@pwc.com

サイバー対策

Prasert Jarusripat
Risk Assurance Partner
prasert.jarusripat@pwc.com

中雄 俊和 ／ Toshikazu Nakao
Senior Manager
toshikazu.n.nakao@pwc.com