

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



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