Deloitte.
デロイト トーマツ

増大するリスクに備える
IoTサイバーセキュリティプログラム

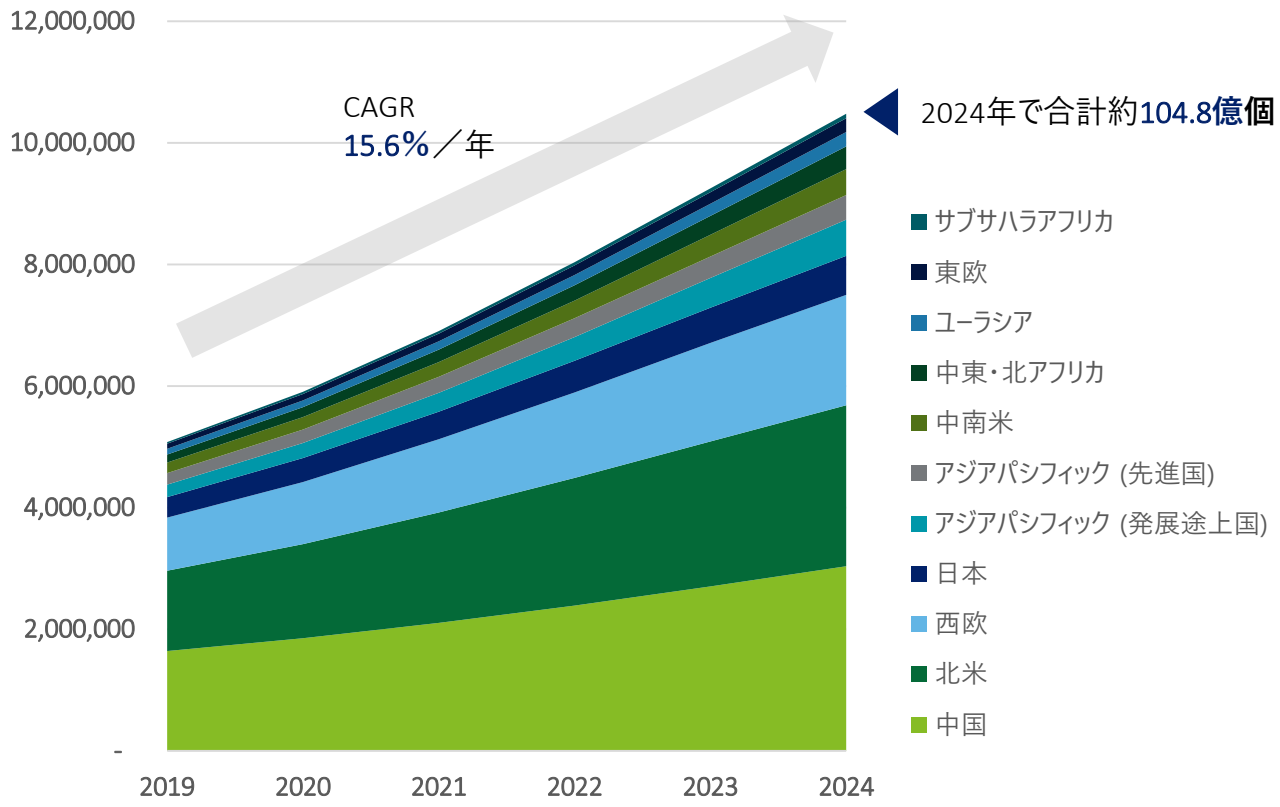
デロイト トーマツ コンサルティング合同会社

目次

IoT機器数は今後もユースケースの拡充により堅調に増加することが予想される

IoT機器数の推移

世界のIoT機器実装数予測 (単位：1,000ユニット)



出所：Gartner “Forecast: Internet of Things, Endpoints and Communications, Worldwide, 2019-2029”に基づきデロイト トーマツ作成

概況

- IoT機器の小型化、低廉化、性能向上によるユースケースの拡充が後押しし、世界のIoT機器実装数は**今後5年間も年率約15%で堅調に増加する**ことが予想されている

↓

- より膨大な数のIoT機器がインターネットに接続し、通信を行うようになる為、**セキュリティリスクに晒されるケースが増加する**

© 2021. For information, contact Deloitte Tohmatsu Consulting LLC.

IoT機器に関連する深刻なセキュリティインシデントも発生しており、開発者コミュニティでもセキュリティに対する懸念が強くなっている

IoTにおけるセキュリティ課題

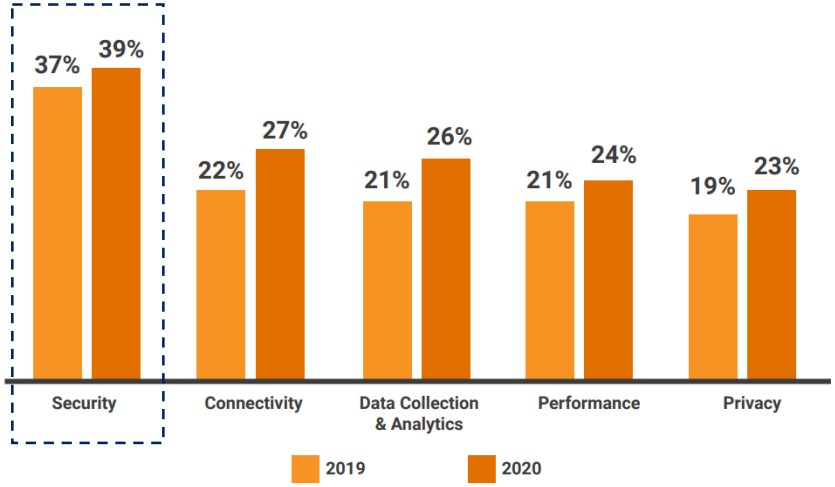
主なIoTセキュリティインシデント

- 直近5年内でIoT機器に感染し**ボットネット化するマルウェアが流行**し、今後もIoT機器の増加に応じてセキュリティの脅威が増していくことが想定される

Mirai	• 2016年、IoT機器を対象とするマルウェア「Mirai」によって世界で**約50万台のIoT機器が感染**し、特定のサイトに大規模DDoS攻撃が行われた
IoTroop / IoT_reaper	• 2017年に発見されたマルウェアで、**数百万台規模のIoT機器に感染し**大型ボットネットを構成した

IoT開発者の主な懸念事項

- IoT開発者の間では、アウトプットに直結するデータ収集・分析やパフォーマンス等よりも**セキュリティにより多くの懸念が寄せられている**



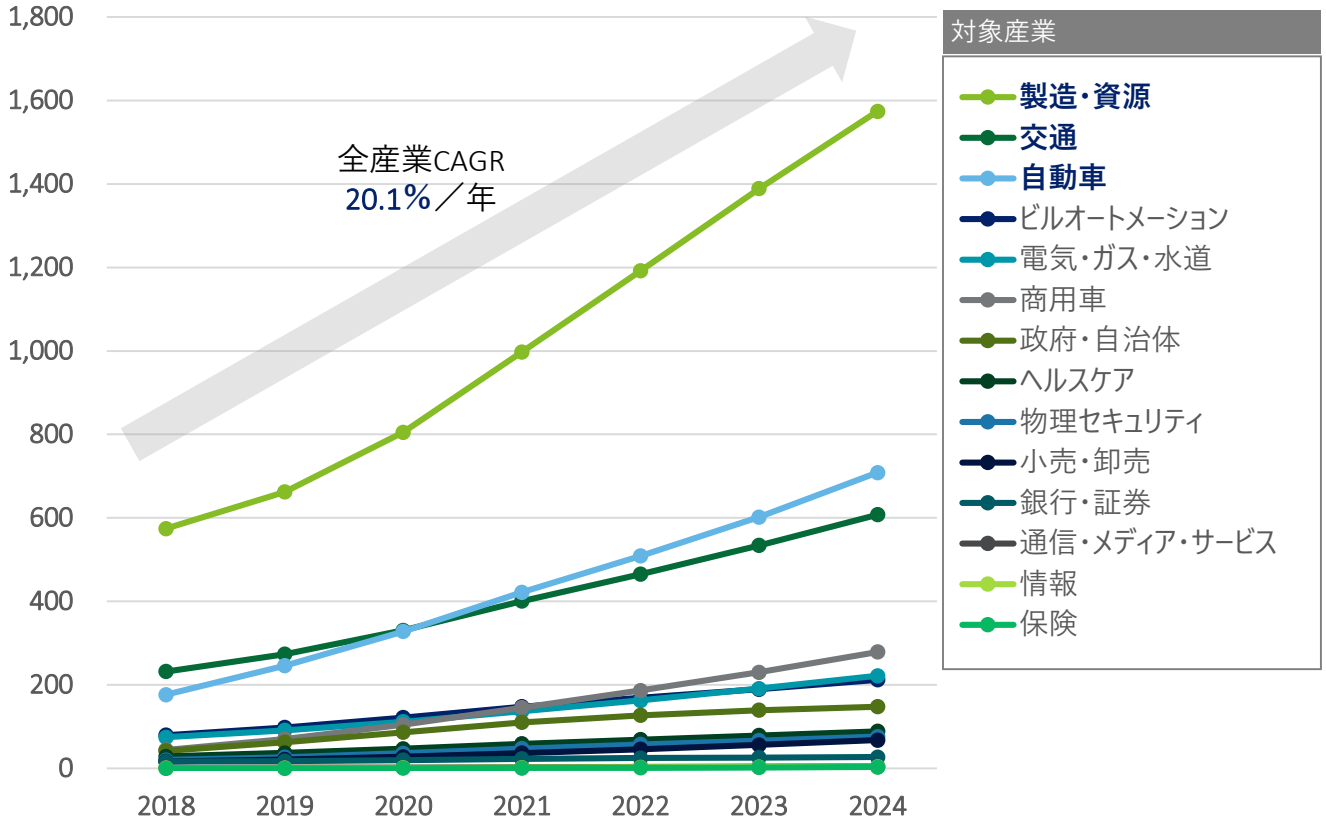
出所：Eclipse IoT

© 2021. For information, contact Deloitte Tohmatsu Consulting LLC.

IoT機器数の増加やセキュリティ脅威の強まりに対し、各産業でIoTセキュリティ投資の増加が予想される

IoTセキュリティ投資のトレンド

産業別 IoT セキュリティ投資コスト総額予測 (単位：Million USD)



出所：Gartner “Market Trends: IoT Edge Device Security, 2020”に基づきデロイト トーマツ作成

概況

- 全産業のIoTセキュリティ投資のトレンドとして、**平均で年率20%程度のコストの増加**が想定されている
- 特に金額規模が大きく今後も継続的な伸びが見込まれる産業としては以下3つとなっている
  - **製造・資源**
  - **交通**
  - **自動車**

© 2021. For information, contact Deloitte Tohmatsu Consulting LLC.

IoTセキュリティではセキュリティ管理体制の不備・人材不足が主要課題であり、各企業はツール導入や管理体制・ガイドライン構築等の対策を行っている

IoTセキュリティ対策事例

各企業が抱えるIoTセキュリティの課題

IoT機器の増加に対する不十分なガバナンス

- 社内外に管理対象のIoT機器が多数存在し、**エンドポイントセキュリティ環境が把握できない**ままNWに接続されている
- 全てのIoT機器で常にセキュアな環境を保つ**管理体制が確保できていない**

IoTセキュリティに関する社内の知見不足

- IoT機器における**セキュリティ対策の必要性に対する認識が薄い**
- サイバーセキュリティの知見を持つ**人材が社内に十分おらず**、現状の問題点や解決方法の把握に時間とコストが掛かる

IoTセキュリティに対する海外市場のニーズの高まり

- 欧米では**IoT機器のセキュリティに関する規制が続々と生まれており**、特に海外進出を進める製造業関連の企業は対応を迫られている

各企業におけるIoTセキュリティ対策事例

事例① 脆弱性自動解析ツール導入

■ **電子機器メーカー**

対策

- 製品である電子機器の脆弱性を自動で解析し、対応策や新たなBOMを出力する**ツールを導入**

効果

- 設計段階からセキュリティに配慮した設計を実施できるようになり、効率的な開発が実現
- BOM（材料表）の精度向上

事例② 一元管理体制・ガイドライン構築

■ **製造業**

対策

- グループ横断の**セキュリティ専門部門を設置**し、管理範囲等見直しの上、一元管理体制構築
- **IoTセキュリティガイドラインを制定**

効果

- 部署横断の管理体制構築により検知対象が拡大し、攻撃検知が早期化
- セキュリティ担当者不在時の問題対処速度向上

© 2021. For information, contact Deloitte Tohmatsu Consulting LLC.

総務省と経済産業省の公表したガイドラインでは、IoT機器の以下6点の特徴に触れ、企業にこれらを踏まえたセキュリティ対策を呼び掛けている

IoT特有の性質

① 脅威の影響範囲・規模の大きさ

NWに接続される**IoT機器数が急増しており**、攻撃を受けた際に波及する範囲やその影響規模が拡大している

② 機器のライフサイクルの長さ

IoT機器の**ライフサイクルは長いものが多く**、構築時の対策の危殆化が進み年々セキュリティリスクが増加する

③ 可視性の低さ

IoT機器には画面が無い為**人目による監視が行き届きにくく**、セキュリティリスクの迅速な検知かつ対策が困難である

④ IoT機器とNW間の相互理解の不足

環境や特性の相違により**IoT機器とNW間の相互理解が不十分**な為、IoT 機器がNWに接続される際に所要の安全や性能を満たせないリスクがある

⑤ 限定的な機能・性能

IoT機器の**限られた処理能力、ハードウェアの機能的な限界**により、強固なセキュリティを搭載することができない

⑥ 想定外の接続リスク

様々なモノがNWに接続されることで、当初開発者やサービス提供者が想定していなかった接続が行われるリスクがある

出所：総務省HP「IoTセキュリティガイドライン ver1.0（案）」

© 2021. For information, contact Deloitte Tohmatsu Consulting LLC.

IoTサイバーセキュリティプログラムを通じて、IoT機器の現状を理解し、セキュリティ脅威に対処する為の指針、アプローチの設定を行う

IoTサイバーセキュリティプログラム

概況

課題

- IoT機器数の増加やセキュリティ脅威の表出に対し、各社とも**効果的なIoTセキュリティアプローチを定義し、賢明なセキュリティ投資を行う必要がある**

解決の方向性

- 複数のステップで設計されたIoTサイバーセキュリティプログラムを通じて、IoTネットワークに接続するICS(産業制御システム)下のアセットの抽出と、それらに対するセキュリティ指針やアプローチの設定を行う

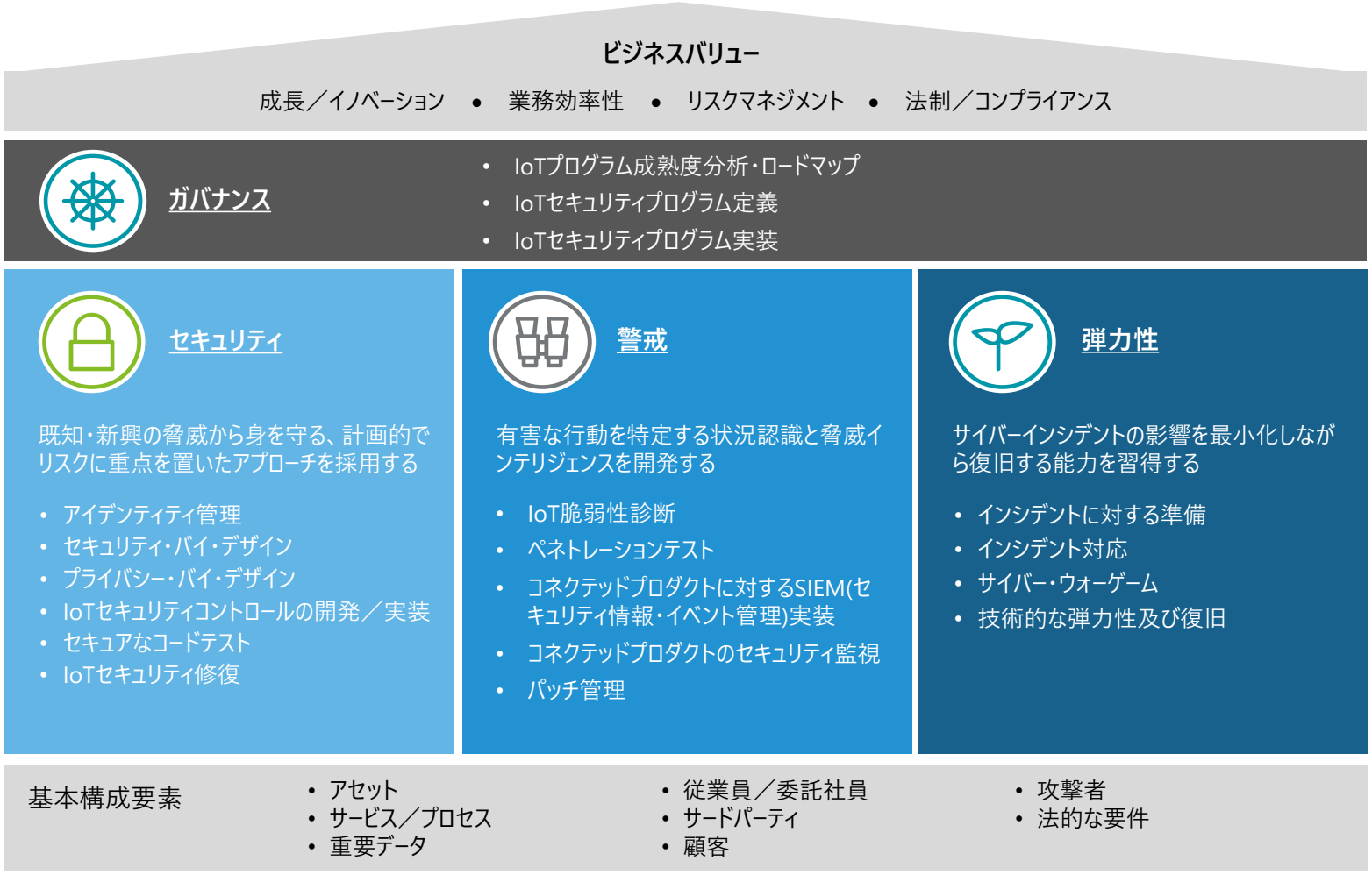
プログラム内容

	ステップ	想定成果物
目的／タイムライン共有 (Why/When)	1 プロジェクト開始	• プロジェクトのキックオフプレゼンテーション • プロジェクト作業計画
対象判別／評価 (For What)	2 アセットの検出と管理	• ICSアセット／インベントリのステータスレポート • ICSアセット管理ソリューションの統合に係る推奨事項 • ICSアセット管理のTo-Beアーキテクチャの文書化 • ICSアセット管理ツールの推奨事項
	3 ネットワーク評価	• ネットワーク評価／ステータスレポート • To-Beリファレンスアーキテクチャ／ブループリント
指針／アプローチ設定 (How)	4 ポリシー、手順及び標準	• ICSセキュリティポリシードキュメント (更新版) • ICSセキュリティドメインのポリシー／標準 (更新版) • コントロールカタログ
	5 セキュリティ監視	• OT固有の監視ユースケース • IT・OT監視ソリューションの統合に関する推奨事項
	6 トレーニング／ワークショップ	• ICS固有のトレーニング内容 • 高度なコミュニケーション戦略 • トレーニング実施計画／スケジュール

© 2021. For information, contact Deloitte Tohmatsu Consulting LLC.

Deloitteの定義するIoTセキュリティフレームワークを活用し、既存のセキュリティポリシーや手順、標準の妥当性、網羅性を評価する

Deloitte IoTセキュリティフレームワーク



© 2021. For information, contact Deloitte Tohmatsu Consulting LLC.

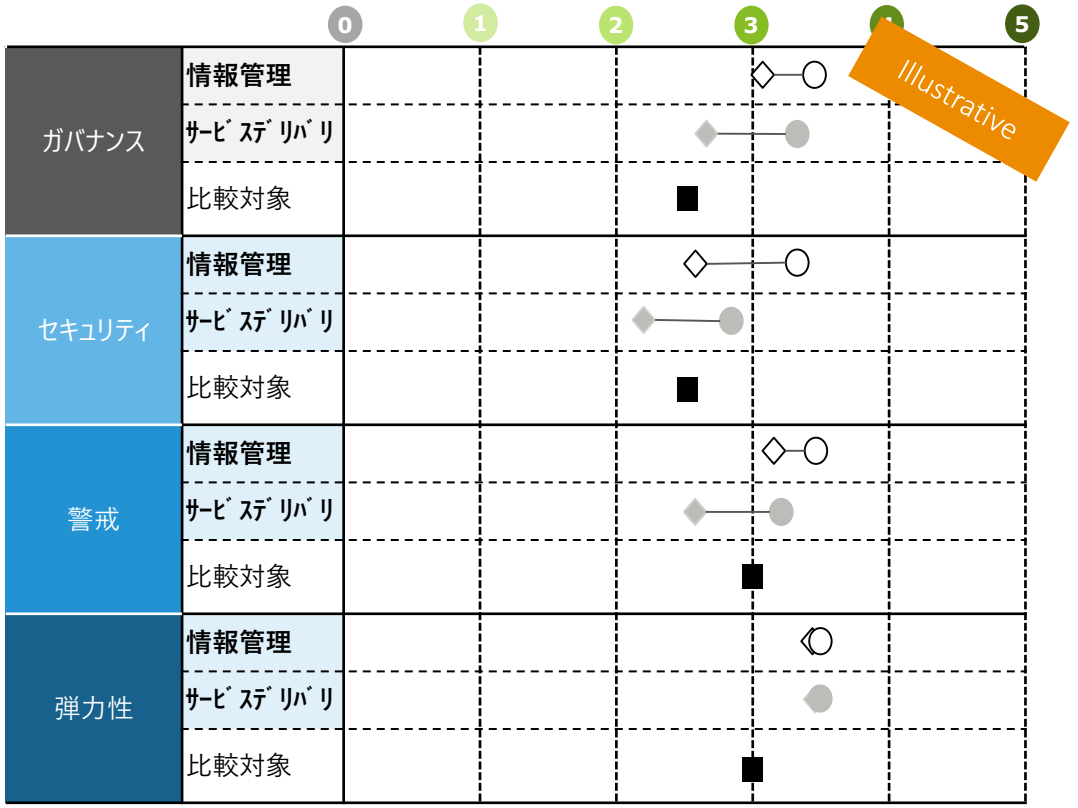
前述の各ドメインに紐づくケイパビリティに基づきクライアントの現状のIoTセキュリティ成熟度を評価し、要件策定のインプットとする

IoTセキュリティ成熟度評価

ドメイン	ケイパビリティ
ガバナンス	戦略及びオペレーティングモデル
	サイバーリスク管理及びコンプライアンス
	ポリシー及び標準
	⋮
セキュリティ	情報・アセット分類
	データプライバシー
	データ消失防止
	情報ライフサイクル管理
	アプリケーションセキュリティ
	ネットワークセキュリティ
	⋮
警戒	サイバー脅威インテリジェンス
	セキュリティイベント管理
	ネットワーク／システムアナリティクス
	⋮
弾力性	サイバーセキュリティインシデント対応
	ビジネス継続性及び災害復旧(DR)
	⋮

成熟度評価

クライアントの現状のIoTセキュリティに関するケイパビリティを情報管理、サービスデリバリ双方の観点からCMMI(能力成熟度モデル統合)に基づき5段階評価し、改善すべき点を明らかにする



© 2021. For information, contact Deloitte Tohmatsu Consulting LLC.

Deloitte.
デロイト トーマツ

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーであるデロイト トーマツ合同会社ならびにそのグループ法人（有限責任監査法人トーマツ、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイト トーマツ税理士法人、DT弁護士法人およびデロイト トーマツ コーポレート ソリューション合同会社を含む）の総称です。デロイト トーマツ グループは、日本で最大級のビジネスプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザリー、コンサルティング、ファイナンシャルアドバイザリー、税務、法務等を提供しています。また、国内約30都市以上に1万名を超える専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト（www.deloitte.com/jp）をご覧ください。

Deloitte（デロイト）とは、デロイト トウシュ トーマツ リミテッド（“DTTL”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人のひとつまたは複数を指します。DTTL（または“Deloitte Global”）ならびに各メンバーファームおよびそれらの関係法人はそれぞれ法的に独立した別個の組織体です。DTTLはクライアントへのサービス提供を行いません。詳細はwww.deloitte.com/jp/aboutをご覧ください。
デロイト アジア パシフィック リミテッドはDTTLのメンバーファームであり、保証有限責任会社です。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける100を超える都市（オークランド、バンコク、北京、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザリー、リスクアドバイザリー、税務およびこれらに関連するプロフェッショナルサービスの分野で世界最大級の規模を有し、150を超える国・地域にわたるメンバーファームや関係法人のグローバルネットワーク（総称して“デロイトネットワーク”）を通じFortune Global 500®の8割の企業に対してサービスを提供しています。“Making an impact that matters”を自らの使命とするデロイトの約312,000名の専門家については、（www.deloitte.com）をご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、その性質上、特定の個人や事業体に具体的に適用される個別の事情に対応するものではありません。また、本資料の作成または発行後に、関連する制度その他の適用の前提となる状況について、変動を生じる可能性もあります。個別の事案に適用するためには、当該時点で有効とされる内容により結論等を異にする可能性があることをご留意いただき、本資料の記載のみに依拠して意思決定・行動をされることなく、適用に関する具体的事案をもとに適切な専門家にご相談ください。

© 2021. For information, contact Deloitte Tohmatsu Consulting LLC.

IS 669126 / ISO 27001

Member of
Deloitte Touche Tohmatsu Limited