

**Deloitte.**

リスクインテリジェントな企業に  
なるための9つの原則

**トーマツ**



# はじめに

せっかくのビジネスチャンス、思うように成果が出ない、と感じることはありませんか？

- ・ 海外進出先の売上が伸びない
- ・ 買収先との統合シナジーが生まれにくい
- ・ 新規事業が一向に黒字化しない・・・

一方、経営を揺るがしかねない出来事に、ヒヤッとすることはありませんか？

- ・ 重大なコンプライアンス違反
- ・ 不正による巨額損失
- ・ 個人情報の流出・・・

もし心当たりがあるようなら、ご自身に問いかけてみてください。

重要な戦略を決めるとき、

- ・ 必要な情報は揃っていますか
- ・ 適切なメンバーで議論を十分に尽くしていますか
- ・ 意思決定が“無謀な賭け”になっていませんか・・・

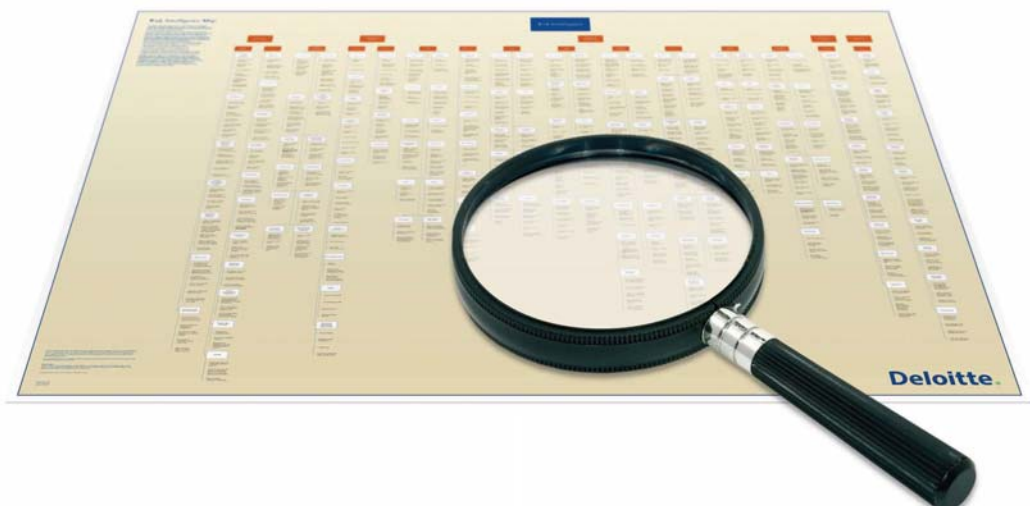
あるいは、社内のルールや日々の業務において、

- ・ ミスを防止／発見する仕組みはできていますか
- ・ 経営層は不正をさせない組織風土作りに入れていますか
- ・ モニタリング活動は徹底されていますか・・・

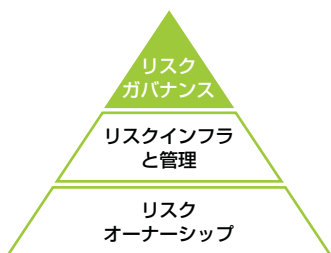
一見ばらばらのようにも思えますが、これらはすべて“ガバナンスが効いているか”という問いかけに他なりません。つまり、ビジネスのチャンスを活かすのも、ダメージを未然に防ぐのも、“ガバナンス”が大きく影響を与えているということ、ぜひ再認識してください。

デロイト トーシュートーマツは、ガバナンスを効かせて企業価値を向上させる有効な手立てのひとつとして、“リスクインテリジェンス”を提唱しています。もちろんここで言うリスクとは、マイナスのものばかりではなく、ガバナンスに関わるあらゆる要素を包含したものです。

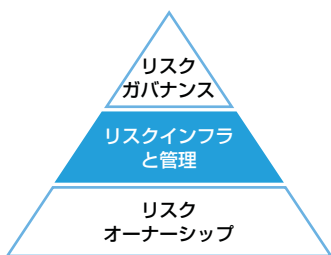
それでは、リスクインテリジェントな企業になるための9つの原則をご紹介します。



# リスクインテリジェントな 企業になるための9つの原則



リスクガバナンス		
<b>リスクの考え方の共有</b> 企業価値の保護と創造の両面からリスクが理解され、それらが組織全体で共有されている。	<b>フレームワークの共通化</b> 共通のフレームワークが、組織全体のリスクマネジメントに利用されている。	<b>役割と責任の明確化</b> リスクマネジメントに関連する役割、責任、権限が明確に定められている。
会社機関による監督		
取締役会、監査役会等のガバナンスに関わる会社機関が、その責任を果たすために組織のリスクマネジメント活動をしっかりと見通している。		

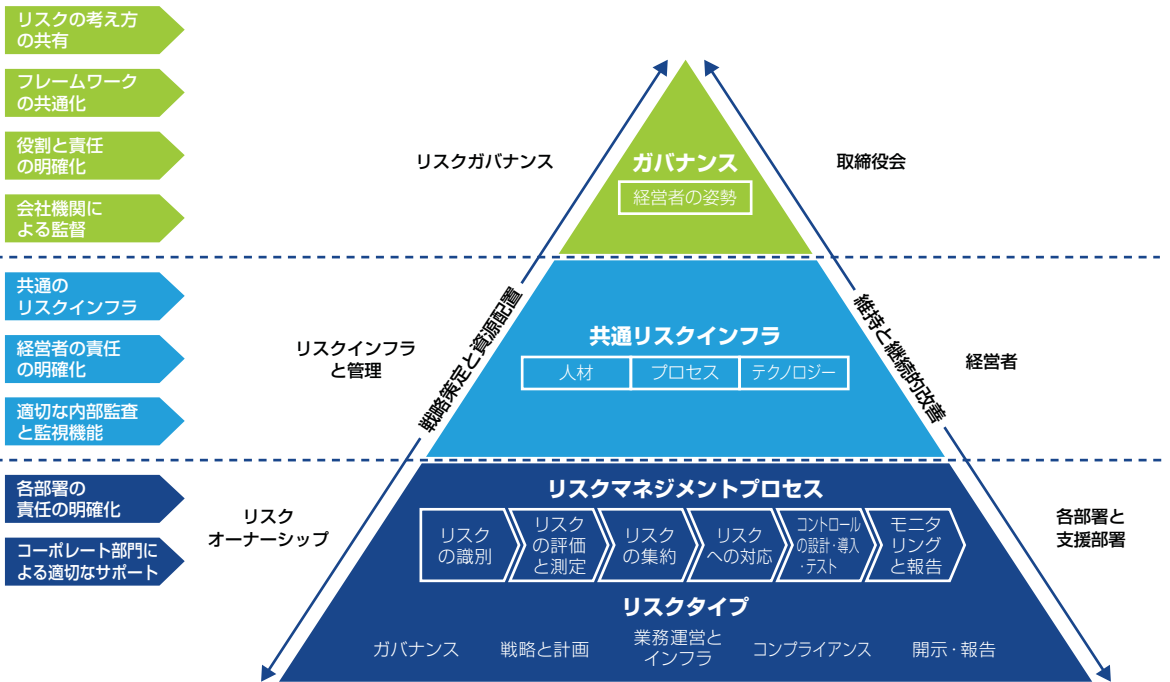


リスクインフラと管理		
<b>共通のリスクインフラ</b> 各部署がリスクに関する責任を果たすために、共通のインフラが利用されている。	<b>経営者の責任の明確化</b> 有効なリスクマネジメントプログラム（設計、導入、維持に関して）の設計、導入、維持に関して、経営者が最大の責任を負っている。	<b>適切な内部監査と監視機能</b> 特定の部署（内部監査、リスクマネジメント、コンプライアンスなど）は、取締役会と経営者に対し、リスクマネジメントプログラムの有効性を監視し、報告している。



リスクオーナーシップ	
<b>各部署の責任の明確化</b> 各部署は、自部署の業績に責任を負うとともに、経営者の定めたフレームワークに従って自部署のリスクマネジメントを遂行する責任を負っている。	<b>コーポレート部門による適切なサポート</b> 特定の部署（財務、法務、IT、人事など）は、全社のリスクマネジメントに広範な影響を持つとともに、他の各部署のリスクマネジメント遂行をサポートする役割を担っている。

# リスクインテリジェンス の枠組み



# リスクは 脅威か、チャンスか？

原則 #1: 企業価値の保護と創造の両面からリスクが理解され、それらが組織全体で共有されている。

## リスクの考え方の共有

リスクは一般的に、ビジネスでは避けるべきものとして話題にのぼります。これは、多くの人々が、リスクをビジネスに対する脅威、すなわちビジネスに悪影響を及ぼすものとして捉えているからだと思われます。

しかし、リスクを異なった切り口で捉えると、もっと豊富に話題にのぼるようになります。例えば、価値の創出に必要な見返りあるものとしてリスクを捉え直すのです。

新商品開発、海外マーケットへの進出、ライバル会社の吸収合併等の多大な労力を伴うチャレンジングな試みにおいて、関連するリスクを適切に管理できない場合、期待する成果が得られないかもしれません。

したがって、リスクを単なる脅威としてではなく、同時に成長と収益拡大をもたらすものとして、従来よりも広い視野で捉え直すことが肝要です。



# フレームワークを 持っているか？

## フレームワークの共通化

多くの企業において、リスクマネジメントは細切れで、統一感がないものとなっています。細切れのアプローチでは、リスクマネジメントやそのためのソフトウェア等のツールの導入において重複作業を招き、リスク情報が混乱する結果となります。

効果的な企業のリスクマネジメントの構築には、フレームワークが欠かせません。COSO ERMやISO 31000のようなリスクフレームワークは、リスクを考慮した意思決定を効率良く行うことを可能にします。また、貴社のビジネスチャンス进行评估の際の、合理的プロセスを提供します。さらに、どのチャンスを選択し、どのリスクを回避すべきかを判断する際の助けとなる、体系的な手引きとなるものです。

よって、リスクフレームワークは、貴社のリスクマネジメントの目標達成をサポートする確固としたものである必要があります。また、貴社独自の戦略、新構想、組織構造等を取り込むことができることも必要です。さらに、貴社の業界や規制に対応できるものでなければなりません。

しかし、どのリスクフレームワークを使用するかについて、考えすぎる必要はありません。重要なのは、貴社のニーズを満たすように、リスクフレームワークを利用することができるかどうかです。

---

原則 #2: 共通のフレームワークが、組織全体のリスクマネジメントに利用されている。



# リスクマネジメントは 全員参加型か？

原則 #3: リスクマネジメントに関連する役割、責任、権限が明確に定められている。

## 役割と責任の明確化

リスクマネジメントを正しく行うためには、管理活動が連動していかなくてはなりません。すなわち、様々な役割の人々が同時に協調しながら、管理活動を行う必要があるのです。

もしかしたら、貴社の中には、自分がリスクマネジメントの役割の一端を担っていることを自覚していない人がいるかもしれません。貴社の営業部長、商品開発部長、システム管理部長などの方々は、リスク管理は他人事だと思っているかもしれません。

そのような考え方を変えることが、貴社のリスクインテリジェンス増進のために必要不可欠です。従業員一人一人に、リスクインテリジェンスの意味が何なのか、なぜ組織全体と各従業員にとって重要なのか、さらに、日々の業務で実際に何を実行すべきかを明確に伝える必要性があります。

そのためには、明確な情報伝達、リスクに焦点を置いた強固な社風、リスク関連の取組みに対する報酬制度、インテリジェントなリスクマネジメント促進の教育制度等が必要となります。

すなわち、リスクマネジメントでは、以下のように、一連の協調的な活動が求められます。

- ・取締役会が方向性を決める。
- ・取締役がリスクプログラムを策定し推進する。
- ・各部署がリスクマネジメントの成功のためにチームとして働く。
- ・特定の部署（人事、経理、IT、法務、税務）がリスクプログラムを支援する。
- ・内部監査、リスクコンプライアンス部門がリスク管理の結果を監視する。



# リスクを語る共通の言葉があるか？

## 共通のリスクインフラ

リスクの専門家達は、仲間内で行動しがちです。同じ価値観や行動パターンを持ち、自分だけの決まり事を作りがちです。

しかし、リスクの専門家達は仲間の壁を越えて活動する必要があります。なぜならば、リスクは隔離されたところには存在しないからです。よって、仲間の壁の内側だけでリスクマネジメントを行うことは不可能なのです。

効果的かつ効率的にリスクを管理して利益を得るには、専門分野の枠を超えるための架け橋が必要です。特に、リスクマネジメントのための共通基盤を構築する必要があります。貴社のすべての部署の業務において、共通のリスクマネジメントの技術や処理方法を活用する必要があります。

ここでいう架け橋とは、組織内部の枠をこえて調和し、すべてのリスク管理者が共通の用語と定義を使い、リスク管理活動の重複を排除することを意味しています。

さらに、架け橋の作業を行うに当たっては、リスクインテリジェンスマップのようなツールのお勧めします。ツールを活用することで、今までに考えもしなかったリスクに気づくかもしれません。さらに、リスクの全体像を描くことは、リスク対応のアプローチを標準化することに役立ちます。

リスク管理技術、測定方法、処理プロセス、専門用語等を共通化することにより、組織内のすべての部署や機能を、架け橋でつなげるような効果を得ることができるのです。

原則 #4: 各部署がリスクに関する責任を果たすために、共通のインフラが利用されている。



# 取締役は自社の リスクを知っているか？

原則 #5: 取締役会、監査役会等のガバナンスに関わる会社機関が、その責任を果たすために組織のリスクマネジメント活動をしっかりと見通している。

## 会社機関による監督

取締役の中には、自社の中でリスクをどのように管理しているか知らない人もいられるかもしれません。このような状態は、もちろん避けるべきです。取締役会は経営者がリスクに適切に対応するよう監督するといった責任を負っています。この責任は、正しい情報が伝達されていないと果たすことはできません。

責任を果たし、価値を創造するためには、取締役会は以下を実行すべきです。

- ・ リスクを議題に載せること。リスク対応に追われる前に、事前にリスクのために時間を割いておきましょう。リスクについて、毎回の取締役会で議論したとしてもやり過ぎではないでしょう。
- ・ 現在のリスクの構造を検証しましょう。リスクはどのように管理されていますか。専門分野をまたぐ架け橋はありますか。
- ・ 定期的に管理チームがリスクを再検証しましょう。組織の重要な戦略の実行を妨げるリスクを識別しましょう。
- ・ リスクの対処方法について協議しましょう。どこに最大のチャンスがありますか。何が戦略上の目標達成を妨げているのでしょうか。
- ・ 組織のリスクの許容範囲を確認しましょう。どの程度までのリスクなら負えますか。どれくらいのリスクなら積極的に負いますか。また、実際にはどれ位負っているのでしょうか。それらは想定内のものですか。
- ・ 納得いくまで確認しましょう。それぞれの担当役員に聞いてみてください。「どれくらい自信がありますか。それはなぜですか。」
- ・ 内部監査部門や外部のコンサルタントにリスクマネジメントプログラムの有効性を評価してもらいましょう。



# 経営者が率先しているか？

## 経営者の責任の明確化

リスクに対する責任は、皆が負っています。しかし、もしあなたが経営者であれば、その責任はもっと重いものとなります。

経営者はリーダーシップと権限を与えられています。それらを駆使して、見返りあるリスクをとることについて従業員に考えさせること、リスクマネジメントを全ての組織階層で推進すること、目標値を設定すること、外部への説明責任を履行すること、取締役会への責任を果たすこと、変化を促進すること、さらに、リスクインテリジェントな組織文化を確立することが必要です。

あまりにも多くを求めているとは思いますが、どうしても実行できるでしょうか。まず手始めに、役員レベルで構成するリスク委員会を設置して、管理職のリスクに対する洞察力を高め、リスクインテリジェントプログラムの作成を支援するのです。

ある企業では、チーフリスクオフィサー（CRO）が、役員で構成されるリスク管理委員会の主要メンバーとなっています。CROは他の役員と協議して、各事業部門のリスク管理方針と手法の開発を進め、組織がリスクをどの程度まで許容できるのかを議論し、評価したうえでリスク情報を経営者や取締役会等の監督機関に報告します。

CROの役割は組織によって千差万別ですが、組織が必要とする要件やリスクの理念に合致していなければなりません。組織によっては、ビジネスパートナーであったり、促進者であったり、交通整理の警察官のような役割であったりさえします。どのような役割にせよ、CROが上記のリスクプログラムについて主要な責任を負っているのです。

---

**原則 #6：有効なリスクマネジメントプログラムの設計、導入、維持に関して、経営者が最大の責任を負っている。**



# リスクのオーナーは 決まっているか？

原則 #7: 各部署は、自部署の業績に責任を負うとともに、経営者の定めたフレームワークに従って自部署のリスクマネジメントを遂行する責任を負っている。

## 各部署の責任の明確化

皆さん全員が、リスクに対して責任を負っています。それでは、それぞれのリスクの責任者“オーナー”は誰でしょうか。

リスクのオーナーについては、組織中で混乱を防ぐためシンプルに考えるのが良いでしょう。すなわち、もし皆さんが部署のトップならば、その部署のリスクを負っていると考えるのです。

言い換えると、仮にある部署の業績について責任を負っているならば、その部署の日々のリスク管理の責任も負っていることとなります。しかし、これにより、その部署の他のメンバーが、リスクへの責任を負わなくてもよいという訳ではありません。

リスクへの責任を負うとは何を意味するのでしょうか。他の仕事と同様に、リスクへの責任を負う者は、リスクを識別、測定、監視、管理して経営者へ報告する必要があります。さらに、リスク意識の向上、有効なリスク分析に基づいたリスク対策の優先順位の見直し等の責任を負っています。

しかしながら、一方では言うまでもなく、リスクのオーナーは、組織のルールに従って対応する必要があります。例えば、部門独自のリスク管理のフレームワークを選ぶことはせず、与えられたフレームワークの中で活動するのです。また、組織のリスク許容レベルを決定することはせず、組織が決定したリスクレベルの範囲内で活動を行うのです。



# サポートチームはあるか？

## コーポレート部門による適切なサポート

財務、法務、人事、税務、及びITのような部署は、それぞれの部署のリスクを管理するだけでなく、他部署のリスク管理も支援するという点から他の部署と異なります。

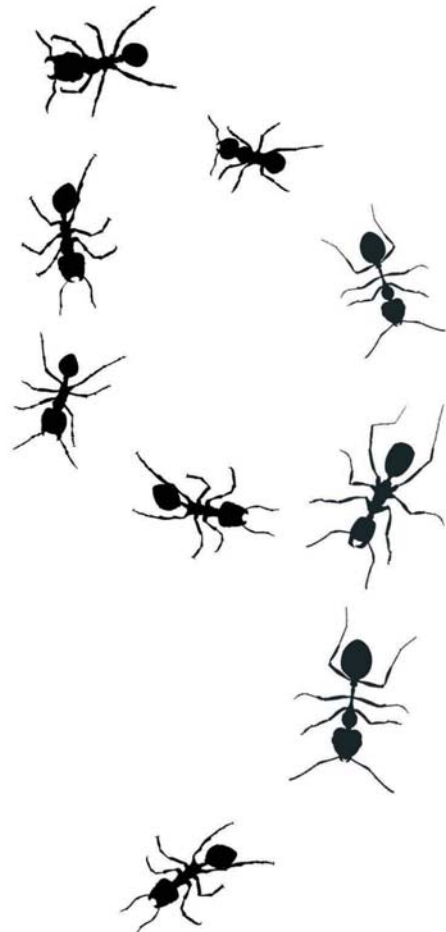
これら支援部署は、通常の部署と同様に、各業務固有のリスクに対して主要な責任を負います。また同時に、各部署の職務範囲を超えたリスクへの責任も負っています。

例えば、財務部門は、リスクを踏まえた内部統制の評価を実施する際に主要な役割を果たしますが、これにより、リスクアセスメントの幅広い能力が備わっているはずで、この能力はうまく工夫すれば、他の部門でも利用することができるでしょう。IT部門は、テクノロジーに関連するリスクばかりでなく、他の部署のリスクの監視や軽減に寄与することができます。人事部門は、主に人材育成に関連する責任を負っていますが、従業員のアンケート調査や退職面談の結果の情報を利用することで、懸念されるリスク要因を特定することができるのです。

これらの支援部署は組織全体を広くカバーしているため、リスク軽減を図るための全社的な方針を決め、内部統制を開発し、それを強化する役割を担うことになります。そして、各部署を支援し、各部署が収益を求めて賢くリスクテイクしていくことを支援するのです。さらに、経営者のために重要な情報を収集し、リスク軽減のための分析も行います。

リスクフレームワークの中での主要な役割を明確化した上で、支援部署がリスク委員会及びその他の重要な会議に出席することが重要です。

**原則 #8: 特定の部署（財務、法務、IT、人事など）は、全社のリスクマネジメントに広範な影響を持つとともに、各部署のリスクマネジメント遂行をサポートする役割を担っている。**



# リスクの監視に 手抜きはないか？

原則 #9: 特定の部署 (内部監査、リスクマネジメント、コンプライアンスなど) が、取締役会と経営者に対し、リスクマネジメントプログラムの有効性を監視し、報告している。

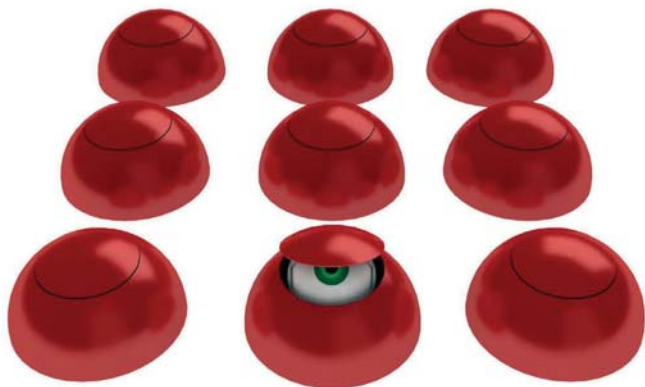
## 適切な内部監査と監視機能

リスク管理において、組織内の特定のグループは、ユニークな役割を担っています。例えば、内部監査部やコンプライアンス部、リスク管理部の役割です。これらのグループの主な責任は、内部統制やリスクの管理が有効に機能しているかを監視することです。

この役割によって、上記の特定のグループは他の部署から区別されます。これらのグループは、組織の本来の業務の企画や運営を行う責任を負っているわけではありません。このグループの役割は、組織のリスク管理活動を監視し有効性を高めることです。

具体的な役割や責任は、組織によって様々です。ある組織では、監視以上のことを行う場合もありますし、また他の組織では、監視の実行が制限されている場合もあります。具体的な役割は、以下の通りです。

- ・ 現在のリスク管理の状況を評価し、さらに、経営者が将来のリスクや機会を理解する手助けをします。
- ・ 組織が受容するリスクが、身の丈に合っているか判断します。
- ・ どのようにリスクが相互作用して何をもたらすのか、組織がそのリスク低減を適切に考慮しているかについて確認します。
- ・ リスク管理における非効率性を排除する手段を調査します。
- ・ 収益と株主価値増大をもたらすリスクを明らかにし、そのリスクに対する経営資源の活用を促します。
- ・ 対応が不十分なリスク分野に対する注意を促し、経営資源の投入を支援します。
- ・ 不正のような重要なリスクに関する、深い専門知識を提供します。
- ・ コントロールのデザイン及び改善に関与し、リスクアセスメントの実施と評価を行います。



## お問い合わせ

### 有限責任監査法人トーマツ エンタープライズ リスク サービス

東 京 〒100-0005 東京都千代田区丸の内3-3-1 新東京ビル

Tel: 03-6213-1112

大 阪 〒541-0042 大阪府大阪市中央区今橋4-1-1 淀屋橋三井ビルディング

Tel: 06-4560-6021

名古屋 〒450-8530 愛知県名古屋市中村区名駅3-13-5 名古屋ダイヤビルディング3号館

Tel: 052-565-5517

福 岡 〒810-0001 福岡県福岡市中央区天神1-4-2 エルガーラ

Tel: 092-751-1517

[www.tohmatsu.com/ers](http://www.tohmatsu.com/ers)

### デロイト トーマツ リスクサービス株式会社

本 社 〒100-0005 東京都千代田区丸の内3-3-1 新東京ビル

Tel: 03-6741-5410

[www.tohmatsu.com/dtrs](http://www.tohmatsu.com/dtrs)

### デロイト トーマツ コンサルティング株式会社

〒100-0005 東京都千代田区丸の内3-3-1 新東京ビル

Tel: 03-5220-8600

[www.tohmatsu.com/dtc](http://www.tohmatsu.com/dtc)

トーマツグループはデロイト トウシュ トーマツ(スイスの法令に基づく連合組織体)における日本のメンバーファーム各社(有限責任監査法人トーマツと税理士法人トーマツ、およびそれぞれの関係会社)の総称です。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、各社がそれぞれの適用法令に従い、監査、税務、コンサルティング、ファイナンシャルアドバイザーサービス等を提供しております。また、国内約40都市に約6,700名の専門家(公認会計士、税理士、コンサルタントなど)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。詳細はトーマツグループWebサイト([www.tohmatsu.com](http://www.tohmatsu.com))をご覧ください。

Deloitte(デロイト)は監査、税務、コンサルティングおよびファイナンシャルアドバイザーサービスをさまざまな業種の上場・非上場クライアントに提供しています。全世界140か国にわたるメンバーファームのネットワークで、ワールドクラスの品質と地域に対する深い専門知識により、いかなる場所でもクライアントの発展を支援しています。デロイトの165,000人におよぶ人材は"standard of excellence"となることを目指し、"誠実性"、"卓越した価値の提供"、"相互信頼"、"文化的多様性"といった価値観を共通するカルチャーで結ばれています。継続的な知識習得、チャレンジングな経験、豊富なキャリア形成の機会といった環境を生かしながら、Deloitteのプロフェッショナルは企業責任(CSR)を強化し、社会からの信頼を築き、各々の地域社会に貢献していきます。

Deloitte(デロイト)とは、スイスの法令に基づく連合組織体のデロイト トウシュ トーマツおよび相互に独立した個別の法的存在であるネットワーク組織のうちのメンバーファームのひとつあるいは複数を指します。デロイト トウシュ トーマツとメンバーファームの法的な構成についての詳細は[www.tohmatsu.com/deloitte](http://www.tohmatsu.com/deloitte)をご覧ください。

© 2009 Deloitte Touche Tohmatsu LLC. All rights reserved.

Member of  
Deloitte Touche Tohmatsu