Deloitte.

Heads Up

2014 年 4 月 8 日
第 21 巻　第 9 号

注：本資料は Deloitte & Touche LLP が作成し、有限責任監査法人トーマツが翻訳したものです。
この日本語版については有限責任監査法人トーマツにお問合せください。
この日本語版は、読者のご理解の参考までに作成したものであり、英語版ニュースレターの補助的なものです。あくまで英語版が（正）となります旨、ご了承下さい。

目次：

- サイバーセキュリティ大統領令及びフレームワーク
- サイバーセキュリティの展望
- 公開会社の開示
- 取締役会及び上席リーダーシップの役割
- ベスト・プラクティス
- 次のステップ

SEC 委員長であるメアリー・ジョー・ホワイトは、サイバーセキュリティに関する脅威は世界的なものであり、我々の経済、例えば、「我々の重要インフラストラクチャー、我々の金融市場、銀行、知的財産、及び・・・・アメリカの消費者の私的データ」に憂慮すべきリスクを引き起こしていると強調した。

サイバーに関するお話
SEC のサイバーセキュリティ円卓会議のハイライト

ジョー・ディレオ（Joe Dileo）及びリンゼー・マカリスター（Lyndsey MacAlister）（デロイト＆トウシュ LLP）

2014 年 3 月 26 日、SEC はサイバーセキュリティ及び関連する市場参加者（例えば、公開会社、ブローカー・ディーラー、投資アドバイザー及び名義書換代理人）の課題に関する円卓会議を主催した。冒頭の挨拶において、SEC 委員長であるメアリー・ジョー・ホワイト（Mary Jo White）は、サイバーセキュリティに関する脅威は世界的なものであり、我々の経済、例えば、「我々の重要インフラストラクチャー、我々の金融市場、銀行、知的財産、及び・・・・アメリカの消費者の私的データ」に憂慮すべきリスクを引き起こしていると強調した。彼女はこれらのリスクは、「情報課（Division of Intelligence）による世界的脅威リストの筆頭であり、テロリズムさえ凌いでいる」と特に言及した。政府官僚、専門的サービス提供者、学者、投資家、作成者及び取引市場代表者等の広範な経歴をもったパネリストは、これらのサイバーセキュリティの課題を評価し対応する経験を共有した。

当 *Heads Up* は、SEC 円卓会議で議論された三つの主要トピックを強調するものである。すなわち、(1)現在のサイバーセキュリティの展望、(2)公開会社の開示問題、及び(3)サイバーセキュリティに関する脅威の評価及び対応における取締役会及び上席リーダーシップの役割、である。この出版物はまた、会社がサイバー攻撃に対する準備及び対応にあたり考慮しうる、ベスト・プラクティスについてサイバーセキュリティ関連ガイダンス及びパネリストの見解を要約するものである。

サイバーセキュリティ大統領令及びフレームワーク

彼らの見解に対する前触れとして、多くのパネリストが、2013 年 2 月のオバマ大統領のサイバーセキュリティに関する大統領令*「重要インフラストラクチャーのサイバーセキュリティ強化」*、及び国立標準技術研究所（NIST）のサイバーセキュリティ・フレームワーク*「重要インフラストラクチャーのサイバーセキュリティ強化フレームワーク」*に言及した。

当大統領令は、国の重要インフラストラクチャー[1]の「安全性及び回復力を強化する米国の方針」を伝達し、それをサイバー脅威から保護するために発行された。当大統領令の規定は、(1)米国政府機関と私的セクター会社間のサイバー脅威関連情報のより適時の共有、(2)サイバーセキュリティ・リスクを低減する「基準となる」フレームワークの開発、(3)サイバーセキュリティ・フレームワークの導入を支援する自主的で重要なインフラストラクチャー・サイバーセキュリティ・プログラムの確立、及び(4)最も大きなリスクにさらされている重要インフラストラクチャーの識別、を含む。

編集者注：国土安全保障省（DHS）は、16 の重要インフラストラクチャー・セクターを識別した。各セクターについて、DHS は、要約、セクター特有計画及びその他のリソースを提供した。現在のサイバーセキュリティの展望に関連して、セクターの議論においては、あるパネリストは、金融サービス及びエネルギー・セクターが、最も攻撃にさらされていると特に言及した。

[1] 当大統領令は、重要インフラストラクチャーを、「物理的又は仮想的かを問わず、米国にとって極めて重大であるため、当該システム及び資産の無能力又は破壊が、保安、国の経済的安全保障、国民保険若しくは安全、又はそれら事項の組合せを衰弱させることになる、システム及び資産」と定義付けている。

大統領令に対応して、NIST は、2014 年 2 月にサイバーセキュリティ・フレームワークの第一版を発行した。当フレームワークは、NIST の信ずるところは、サイバーセキュリティ関連リスク管理に対する、戦略的、費用効率的アプローチであると概説している。NIST によれば、当フレームワークは、「サイバーセキュリティ活動を導くためにビジネス・ドライバーを使用し、サイバーセキュリティ・リスクを組織の管理プロセスの一環として考慮することに焦点を当てている。」当フレームワークは、規模又は複雑性にかかわらず、全ての会社により使用されることを意図されており、また、「重要インフラストラクチャーの安全性及び回復力」を会社が改善できるようになるリスク管理原則（及びベスト・プラクティス）を包含している、とのことである。しかしながら、NIST は、当フレームワークは、サイバーセキュリティ・リスクに対処する「全てに適用する一つの（one-size-fits-all）」アプローチではないと会社に警告している。

編集者注：2014 年 3 月 21 日、CAQ は、独立外部監査人のサイバーセキュリティに関する責任を強調するアラートを発行した。当アラートは、パネリストの議論の準備を助けるために、円卓会議前に発行されたものであり、財務諸表及び ICFR 双方の監査において実施されるサイバーセキュリティ関連監査手続を要約するものである。これは、財務報告システムに対する「未承認のアクセスにより生じる会社の財務諸表に対する重要な虚偽表示のリスクの評価を含む。」

サイバーセキュリティの展望

パネリストは、サイバー攻撃加害者の様々なタイプ、並びに彼らの攻撃を行なう手口及び動機について説明した。

パネリストは、サイバー攻撃加害者の様々なタイプ、並びに彼らの攻撃を行なう手口及び動機について説明した。新たなサイバー脅威はしばしば、その他の脅威が打ち倒されるや否や発生するため、あるパネリストは、脅威の急速な進展を、「もぐらたたき」ゲームに例えた。

円卓会議における主要テーマは、サイバー脅威が、テクノロジーのみならず事業体の広範な業務にまで影響を与える可能性があることであった。デロイト&トウシュ LLP のサイバー・リスク・サービスのディレクターであるメアリー・ギャリガン（Mary Galligan）は、三つ又の「脅威マトリックス」を概説した。すなわち、(1)脅威ベクトル、(2)脅威インテリジェンス、及び(3)脅威回復力、である。脅威ベクトルはサイバー攻撃の加害者と彼らの攻撃の理由を含む。脅威インテリジェンスは、データの保全は十分ではなく、政府及びその他の私的セクター当事者間の情報共有もまた必要である、との認識を含む。脅威回復力—或いは出来事を速やかに識別、修復及び回復する事業体の能力—は重要である。なぜならば、サイバー攻撃はしばしば、その他の脅威のリスクを高めるためである。当該追加的脅威は、事業体の日々のビジネス業務の混乱、評判に対するダメージ（攻撃そのものからのみならず、事業体の攻撃に関する開示の公衆の反応も含む）、及びサイバー攻撃対応及び修復コストを含む。

パネリストは、サイバー攻撃の加害者（及び彼らの攻撃の背後にある動機）を、以下の広範なカテゴリーに分類した。

- *民族国家及びスパイ*—国の保安機密又は知的財産を盗むことを目指す者。
- *組織犯罪者*—金銭及び私的又は事業体の消費者機密情報（例えば、個人情報）を盗むために、洗練されたツールを用いる加害者。
- *テロリスト*—米国における主要な経済的インフラストラクチャーに対する攻撃を目論む者。
- *「ハクティビスト（Hacktivist）」*—組織の機密情報を盗む又は公表することにより社会的又は政治的声明を表明することを欲する個人又はグループ。

数人のパネリストは、組織の内部者がリスクを引き起こしていると強調した。なぜならば、主要システム及び業務に関する彼らの詳細な知識及びアクセス権のゆえである。特に、パネリストは、「問題のある退職者（bad leavers）」（すなわち、事業体との雇用が終了した個人）について事業体に警告した。パネリストはまた、(1)事業体のシステムに対する物理的アクセスを有する第三者（例えば、顧客、ベンダー又は下請け業者）、又は彼らのシステムが、事業体のシステムにアクセスする可能性があるが、サイバー攻撃にさらされやすい者との関係、(2)海外業務、及び(3)モバイル・デバイスを通じて事業体のシステムにアクセス可能な従業員、により生じるサイバーセキュリティ・リスクについて議論した。

サイバー攻撃を実行するために使用される手口としては、インフラストラクチャーの混乱、サービスの拒否、「ランサムウェア（ransomware）」（すなわち、身代金が支払われるまでファイルを暗号化する）、及び窃盗が含まれる。パネリストは、これらのサイバーセキュリティ侵害の様々な例、例えば、ブローカーのシステムが侵害され、不正な取引が実行された状況でのブローカー・ディーラー関係を例示した。その他の例としては、投資アドバイザーの財産管理クライアントの個々の口座を乗っ取ろうとする試みが挙げられた。加えて、様々なフィッシング・スキームが議論された。例えば、攻撃者がベンダー又は顧客のふりをして、(1)口座情報の確認の要求をする、又は(2)資金が不適切な口座に送金されるよう、虚偽の電子メールを事業体の従業員に送付する、等である。

事業体は、脅威、手口、加害者及びその動機を見通すことを力説され、彼らのシステムにおけるサイバー攻撃にたいする脆弱性を評価することをアドバイスされた。あるパネリストは、サイバー事件は無作為かつ偶発的発生から、徹底的かつ系統的な攻撃に進化したとの見解を示した。当該攻撃者は、事業体の脆弱性が明らかになることを根気よく待ち、事業体のシステムに対するアクセスをひとたび得れば、執拗である。

公開会社の開示

重要性に関しての詳細説明にあたり、パネリストは、重要性概念のサイバーセキュリティ開示への適用の挑戦課題について述べた。それはしばしば、重要な定性的要素を有する事件を記述し、又は定量的影響が未知であるためである。

2011 年 10 月、SEC の企業財務局は、CFDG トピック 2*「サイバーセキュリティ」*[2]を発行した。これは、サイバーセキュリティ事件の増加に対応するものであり、これら事件の一部は、(1)直接的ダメージ（実際及び評判の双方）、(2)彼らの顧客に対する影響、及び(3)将来のサイバーセキュリティ攻撃からの保護水準の上昇に関する重要な回復及びその他のコストを特定の会社に発生させた。

当委員会は、パネリストに、現在のサイバーセキュリティに関連した開示ガイダンスの有効性に関して質問した。あるパネリストは、現在のサイバーセキュリティに関連した開示ガイダンスの多くは、「文例集（boilerplate）」であり、登録者向けに作るのではなくCFDG トピック 2 の文言を反復していると特に言及した。しかしながら、他のパネリストは、適応された開示の提供の潜在的リスクについて述べた。ある者は、より具体的な開示は、攻撃者が会社に侵入することを助ける細部を含む可能性があるため、会社の脆弱性を高めかねない、との懸念を表明した。

パネリストは、事業体は、サイバーセキュリティ侵害について、FBI 又は DHS 等の組織から学ぶ場合がある、と説明した。侵害された当該情報は、機密事項であり、事業体は、サイバー事件を開示することができないかもしれないからである。オバマ大統領の大統領令が要求する情報共有促進の精神に照らして、あるパネリストは、委員会及びその他の連邦機関は、登録者が侵害された場合には、お互いに伝達することを確かにするよう要求した。パネリストは、有効な代理人間コミュニケーションは、ある代理人が登録者により多くの開示を要求する一方で、他の代理人が、事件を開示しないよう登録者に命じる可能性がある状況を緩和することになる、と特に言及した。

編集者注：最近の「2014 年 SEC 声明」会議で強調されたように、SEC スタッフは、サイバーセキュリティ侵害に関連する情報の開示と、詳細開示の提供による潜在的サイバー攻撃のための計画表を作成し、特に登録者が調査において当局と共同している場合には、しばしば事業体が均衡を図る必要があることを認めた。SEC スタッフはまた、登録者が、文例集のサイバーセキュリティ開示を避け、代わりに、もし実施可能で重要であるならば、(1)リスクにさらされているビジネスの側面、2)新たな情報の更新、及び(3)コスト見積もり、を含めるべく彼らの開示を作ることで、「開示効率性」を実践することを推奨した。「2014 年 SEC 声明」会議に関するこれ以上の情報については、デロイトの 2014 年 3 月 20 日付 *Heads Up* を参照されたい。

パネリストはまた、重要でない事象に関する開示は、投資者にとって有意ではなく、会社の訴訟エクスポージャーを高める可能性があるとの見解を示した。重要性に関しての詳細説明にあたり、パネリストは、重要性概念のサイバーセキュリティ開示への適用の挑戦課題について述べた。それはしばしば、重要な定性的要素を有する事件を記述し、又は定量的影響が未知であるためである。

[2] CFDG トピック 2 は、重要なサイバーセキュリティ事項に関連する潜在的開示に関する解釈ガイダンスを提供するものである。SEC スタッフのガイダンスによれば、事業体は、登録者による(1)財務諸表、(2)リスク・ファクター、(3)訴訟、並びに(4)開示統制及び手続、における開示に関連して考慮事項に対処しなければならないものとされる。

あるパネリストは、しばしば州の法律は、顧客情報に影響を与えるセキュリティー侵害に焦点を当てており、事業体が、事業体のシステムにおける侵害がある場合に提供を要求される開示に関して、低い閾値をもたらす結果となる。その結果として、事業体はしばしば、重要でない侵害に関して細かい開示を提供する結果となる。—あるパネリストが信じた事実は、以下に示すデータでサポートされている。すなわち、サイバー事件が開示された後に登録者の株価が少し下落する、又は株価がより顕著に下落する場合には株価は短期間に回復する。

編集者注:SEC は、サイバーセキュリティ開示規定に関する追加ガイダンスを提供する予定であるか否かについて決定していないが、パネリストは、リスクの性質の進展により陳腐化する可能性がある規範的規則設定よりも、原則主義規則設定を選好する、と言及した。パネル・ディスカッションの要約に当たり、SEC 委員のカーラ・ステイン(Kara Stein)は、委員会は、登録者に対して十分なサイバーセキュリティ開示ガイダンスを提供しているか否か質問した。彼女は、パネリストに、サイバーセキュリティ開示に関する「最低限の基準」が必要か否か、又は様々な種類の登録者を前提として可能であるか、を質問することにより詳しく述べた。ステイン女史は、パネリストが継続的に、サイバーセキュリティ脅威に対処するための多次元的アプローチの利用について議論していたことを強調した。彼女は、委員会が、「[開示]規定においてダイナミック」である必要があるかもしれず、そのようなアプローチは、登録者に過度の負担を与えることなく、投資者に有意義な開示を促進する可能性がある、と提言した。

取締役会及び上席リーダーシップの役割

パネリストは、取締役会及び上席リーダーシップが、サイバーセキュリティ脅威に対する会社の事前準備及び回復力の有効性にとって、重要であると提言した。

あるパネリストは、取締役会の約 1 パーセントが、サイバーセキュリティ又はテクノロジーの専門的知識を有していると特に言及した。この統計は、ホワイト委員長が、事業体の統治機構内で、誰がサイバーセキュリティ事項に責任を負うのかに関するパネリストのフィードバックを求める質問を促した。パネリストは、これは多くの会社で相違があるが、監査又はリスク委員会が当該責任を有していると言及した。いくつかの組織が、サイバーセキュリティ委員会を組成している。あるパネリストは、複雑なサプライ・チェーン又は多角的販売-配達モデルを有する事業体は、彼らの IT インフラストラクチャーの異なる側面に関して別個のサイバーセキュリティ委員会を有しうる、と言及した。

サイバーセキュリティ・リスクの評価を支援する外部専門家と契約する取締役会数が増加する一方、パネリストは、事業体が、(1)別個のサイバーセキュリティ委員会又は(2)取締役会に従事する専門家一名若しくは委員会のうちの一つ(例えば、法務、報酬又は会計事項に関する委員会)を有することを要求すべきであるとは信じていない。代わりに、パネリストは、取締役会及び上席リーダーシップが、サイバーセキュリティ脅威に対する会社の事前準備及び回復力の有効性にとって、重要であると提言した。サイバーセキュリティ・リスクに関する統治責任を履行すると期待される方法に関して、事業体の統治機構(及びその他のリーダーシップ役割)における個人は、正しい質問を提起する、脅威の戦略的含意を理解する、及び事業体のプロトコル及び対応プログラムの長期的卓越性に焦点を当てることができることが必要である。

ベスト・プラクティス

当イベント中の様々なポイントにおいて、パネリストは、組織におけるサイバーセキュリティ・リスク対応について彼らが信じるベスト・プラクティスを共有した。ベスト・プラクティスの議論は、文化、モニタリング及び情報共有、並びにサイバーセキュリティ計画を含むものであった。

文化

多くのパネリストは、IT ソリューション又は特定の内部統制の単なる導入は、継続的に変化するサイバーセキュリティ脅威への対処に十分ではないことに合意した。数人のパネリストは、サイバー攻撃の回避は、適切なバックグラウンド・チェック等の、雇用プロセスにおける継続的努力に始まると提言した。加えて、パネリストは、組織内の全従業員が、お互いにサイバーセキュリティ・リスクを有し、組織は、当該事項に関する警戒に関して強い「経営者の姿勢(tone at the top)」を有さなければならない。

あるパネリストは、上級マネジメントは、「キーボードから始まる」サイバーセキュリティ文化の形成に重要な役割を果たすことができ、そこにおいて、サイバーセキュリティは、解決すべき IT 部門に係るテクノロジー課題と見られるのではなく、全従業員がアクションを取り、彼らの会社の情報保護における彼らの役割を理解するという、ビジネス課題であるとの意見を表明した。

継続的モニタリング及び情報共有

パネリストは、会社が、広範囲脅威モデリング、定期的システム検証、ギャップ分析、リスク・マネジメント、及び回復計画等、継続的モニタリング活動に従事することを推奨した。パネリストが提言した、その他の共通のベスト・プラクティスは、従業員が、会社のデータ及び業務の誠実さを保護する彼らの責任を理解していることを確かめる侵入テストであった。侵入テストは、偽のフィッシング電子メールを従業員に送り、従業員に彼らのパスワードの変更を要求するボイスメールを残す、及び従業員の誰かが彼らのコンピューターに偽の有害ソフトをダウンロードするか否かをテストするために、共有エリアに有害ソフトが入ったフラッシュ・ドライブを置いておく、等の脆弱性テストを含む。

常に変化し続けるサイバー脅威の性質を前提に、パネリストは、情報共有の最重要性を再度述べた。しかしながら、パネリストは、サイバー攻撃に関する情報は機密情報（分類されていない場合）であり、事業体は、当該情報共有おける障壁に直面する可能性がある。これらの障壁は、(1)情報共有における不透明なチャンネル又はフォーラム、又は(2)政府からの分類された情報を入手する適切なセキュリティー・クリアランスを有していない個人、を含む可能性がある。しかしながら、パネリストは、情報共有の継続的改善を推奨した。これは、事件が早く発見され、早くその他の組織に説明されればされるほど、より早く(1)組織が同様の攻撃に対処及び攻撃から回復することができ、(2)市場及び経済的混乱が軽減されるためである。

多くのパネリストは、会社は、彼らの業務の最も脆弱な側面に集中すべきであることに合意した。

サイバーセキュリティ計画、プロトコル及び統制

パネリストは、サイバーセキュリティ・リスクは、一回の IT ソリューションにより対処されえず、継続的に評価されなければならず、事業体は、ある意味でその他のビジネス・リスクと同様に、サイバーセキュリティ・リスクの軽減する試みが必要がある、と説明した。結果として、会社は継続的に、ビジネス・プロセス及び主要システムに関連する彼らの脆弱性を継続的に評価しなければならない。会社の限定的資源及びサイバーセキュリティ資源の欠如を前提として、多くのパネリストは、会社は、全社的リスクについて広範囲に焦点を当てるのではなく、彼らの業務の最も脆弱な側面に集中すべきであることに合意した。リソースがあまりに薄く引伸ばされると、脆弱性は十分にカバーされず、より大きなリスクを会社に残す。会社の脆弱性の評価に当たり、ギャリガン女史は、会社は以下の質問を考慮すべきであると要約した。

- 保護はどのようなに優先順位付けされるべきか？どのような情報が本当に保護される必要があるか（すなわち、リスク評価がされるべきであるか）？
- システムに対するアクセス、特に第三者のアクセスはどのように管理されるべきか？
- モニタリング努力に関連する発見事項はどのように評価されるか（すなわち、会社は、モニタリング活動の結果及び発見事項を有効にレビューする適切な専門知識を有する十分なリソースを有するか）？

多くのパネリストは、従業員が攻撃が行われる前に、対応する方法を知ることができるように、対応及び回復計画の設定並びに計画の実践の重要性を強調した。有効なサイバーセキュリティ回復計画はまた、主要な利害関係者によりまた彼らと共に継続的に更新されなければならない。

会社はまた、上席リーダーシップ、取締役会の委員会、及び取締役会に対する、サイバーセキュリティ事件の報告に関する明確に定義された閾値を含む、適切なエスカレーション・フレームワークを創設するよう助言されている。これらの脅威の定量的影響は当初は明確でない可能性があるため、パネリストは、当該閾値は、サイバー事件の異なる性質を考慮するに十分にフレキシブルであるべきと推奨した。

次のステップ

パネリストからのフィードバック入手に加え、SEC は、構成員に、彼らのインプットを共有すべく、オンラインで意見を求めている。SEC は、当パネル及びその他の利害関係者から入手した情報を分析し、追加措置をとることを検討することを予定している。—これには、既に発行されたガイダンスの有効性評価が含まれる。加えて、彼の準備された見解において、SEC 委員のルイス・アギュラー（Luis Agular）は、識別された課題を議論するため、及び委員会への勧告を行うため、近日中に、サイバーセキュリティ・タスクフォースを組成するよう、委員会へ勧告した。

登録

デロイトの Accounting Standards and Communications Group が発行する *Heads up* およびその他の会計に関する出版物を希望される方は、以下のウェブサイトにご登録ください（www.deloitte.com/us/subscriptions）。

財務責任者のための *Dbriefs*

Dbriefs へぜひご参加ください。*Dbriefs* はデロイトのウェブキャスト・シリーズで、重要な問題を常に把握しておくために必要な実践戦略を提供するものです。「財務責任者」シリーズのウェブキャストを通じ、以下のテーマに関する貴重なアイデアや重要な情報にアクセスしてください。

- 事業戦略および税務
- 税務に関する財務報告
- 取引およびビジネス・イベント
- 企業価値の強化
- ガバナンスおよびリスク
- 財務報告
- テクノロジー

Dbriefs は CPE クレジット取得のための、身近にご利用いただける便利で柔軟な方法も提供します。今後のウェブキャストに関するお知らせをお受け取りいただくには、以下のウェブサイトにて、*Dbriefs* にご登録ください（http://www.deloitte.com/us/dbriefs）。

今後予定されている以下の *Dbriefs* ウェブキャストへの登録が可能です。下記のリンクより今すぐご登録ください：

- Quarterly Accounting Roundup: An Update on Important Developments（6 月 25 日午後 2 時（東部夏時間））

Technical Library と US GAAP Plus

デロイトはご登録いただいた方々を対象に、会計や財務開示に関する資料のオンライン・ライブラリーへのアクセスを提供しています。Technical Library: The Deloitte Accounting Research Tool と呼ばれるこのライブラリーには、弊社の会計および SEC マニュアルならびにその他の会計および SEC の解釈指針のみならず、FASB、EITF、AICPA、PCAOB、IASB、SEC の資料などが含まれています。

営業日ごとに更新される Technical Library は使いやすくデザインされており、ナビゲーションシステムは強力な検索機能を備えているため、いつでも、どのコンピューターからでも瞬時に情報を入手することを可能にします。Technical Library 登録者には、ライブラリーへの最新の情報をハイライトした週報「*Technically Speaking*」もお送りします。登録やオンライン上のデモンストレーションなどの詳細については、デロイトのウェブサイト www.deloitte.com/us/techlibrary をご覧ください。

さらに、US GAAP Plus にも忘れずにアクセスしてください。これは、米国 GAAP に重点を置いた、会計に関するニュース、情報や出版物を取り上げるデロイトの新しい無料ウェブサイトです。このウェブサイトには、FASB の活動や *FASB Accounting Standards Codification*™のアップデート、そして、PCAOB、AICPA、SEC、IASB、IFRS 解釈指針委員会などのその他の米国と国際会計基準の設定主体や規制当局の進展に関する記事が掲載されています。今すぐチェックしてください！

トーマツグループは日本におけるデロイト トウシュ トーマツ リミテッド（英国の法令に基づく保証有限責任会社）のメンバーファームおよびそれらの関係会社（有限責任監査法人トーマツ、デロイト トーマツ コンサルティング株式会社、デロイト トーマツ ファイナンシャルアドバイザリー株式会社および税理士法人トーマツを含む）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リー等を提供しています。また、国内約 40 都市に約 7,300 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）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 アドバイザリーサービスを、さまざまな業種にわたる上場・非上場のクライアントに提供しています。全世界 150 を超える国・地域のメンバーファームのネットワークを通じ、デロイトは、高度に複合化されたビジネスに取り組むクライアントに向けて、深い洞察に基づき、世界最高水準の陣容をもって高品質なサービスを提供しています。デロイトの約 200,000 名を超える人材は、“standard of excellence”となることを目指しています。

Deloitte（デロイト）とは、英国の法令に基づく保証有限責任会社であるデロイト トウシュ トーマツ リミテッドならびにその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の関係会社のひとつまたは複数を指します。DTTL および各メンバーファームはそれぞれ法的に独立した別個の組織体です。DTTL（または”Deloitte Global”）はクライアントへのサービス提供を行いません。DTTL およびそのメンバーファームについての詳細は www.tohmatsu.com/deloitte/ 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。

© 2014. For information, contact Deloitte Touche Tohmatsu LLC

Member of
Deloitte Touche Tohmatsu Limited