Deloitte.
デロイト トーマツ

国立大学法人　長岡技術科学大学
御中

情報セキュリティ研修

情報漏えいが法人に与えるリスク

有限責任監査法人トーマツ
2016年12月8日

トーマツ.

講師紹介

冨永　素司
有限責任監査法人トーマツ
リスクアドバイザリー
ディレクター

経歴

- 2000年に監査法人トーマツ（現 有限責任監査法人トーマツ）に入社。品質・環境・情報セキュリティ・個人情報保護等のISO・Pマーク取得支援コンサルティングの経験を経て、金融機関等のシステムリスク管理態勢の監査、システム更改プロジェクトのリスク管理態勢の第三者評価及び内部監査支援、J-SOX対応支援、情報セキュリティ監査、BCMS、ISMS、Pマーク取得コンサルティング、会計監査におけるIT統制監査等に従事等に従事している。
  現在は、一般事業会社及び地方自治体のマイナンバー対応支援等に従事している。
- マイナンバー対応、BCMS、ISMS、Pマークに関するセミナー講師多数。
- 公認情報システム監査人（CISA）

主要なプロジェクト実績

- 一般事業会社及び地方自治体のマイナンバー対応支援業務
- プライバシーマーク個人情報保護マネジメントシステムコンサルティング
- ISO27001情報セキュリティマネジメントシステムコンサルティング
- 金融機関及び一般事業会社のJ-SOX支援業務
- 地方銀行・信用金庫・証券会社の財務諸表監査の一環でシステムレビュー
- 地方銀行・信用金庫・証券会社のシステムリスク管理態勢の監査
- 信用金庫、証券会社のシステム更改プロジェクトのリスク管理態勢の第三者機関評価

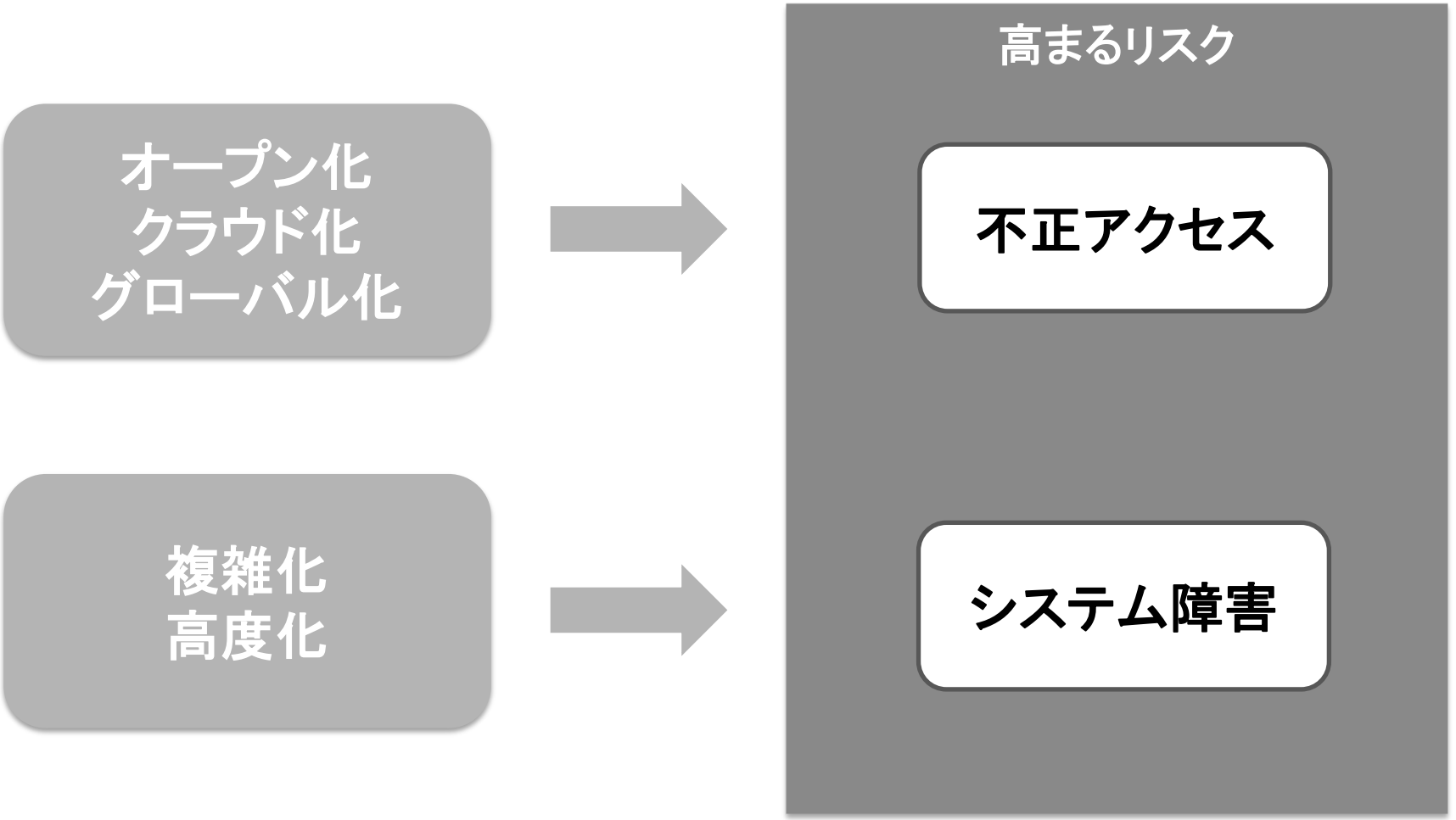
目次

本資料の意見に関する部分は筆者の私見であり、有限責任監査法人トーマツの公式見解ではありません。

１．情報管理が求められる背景

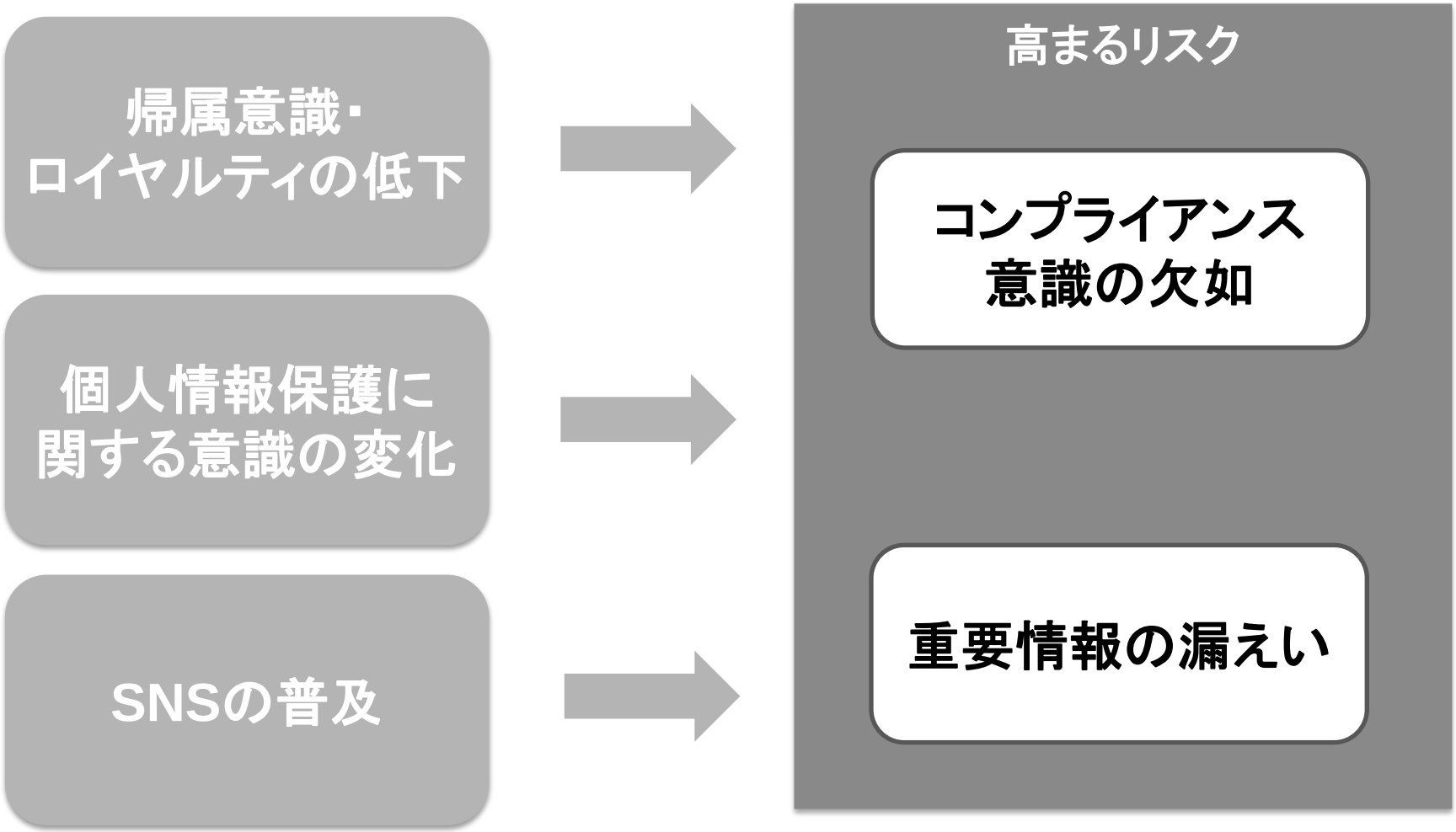
情報漏えいリスクを高めるITの技術革新

ITの目覚ましい技術革新



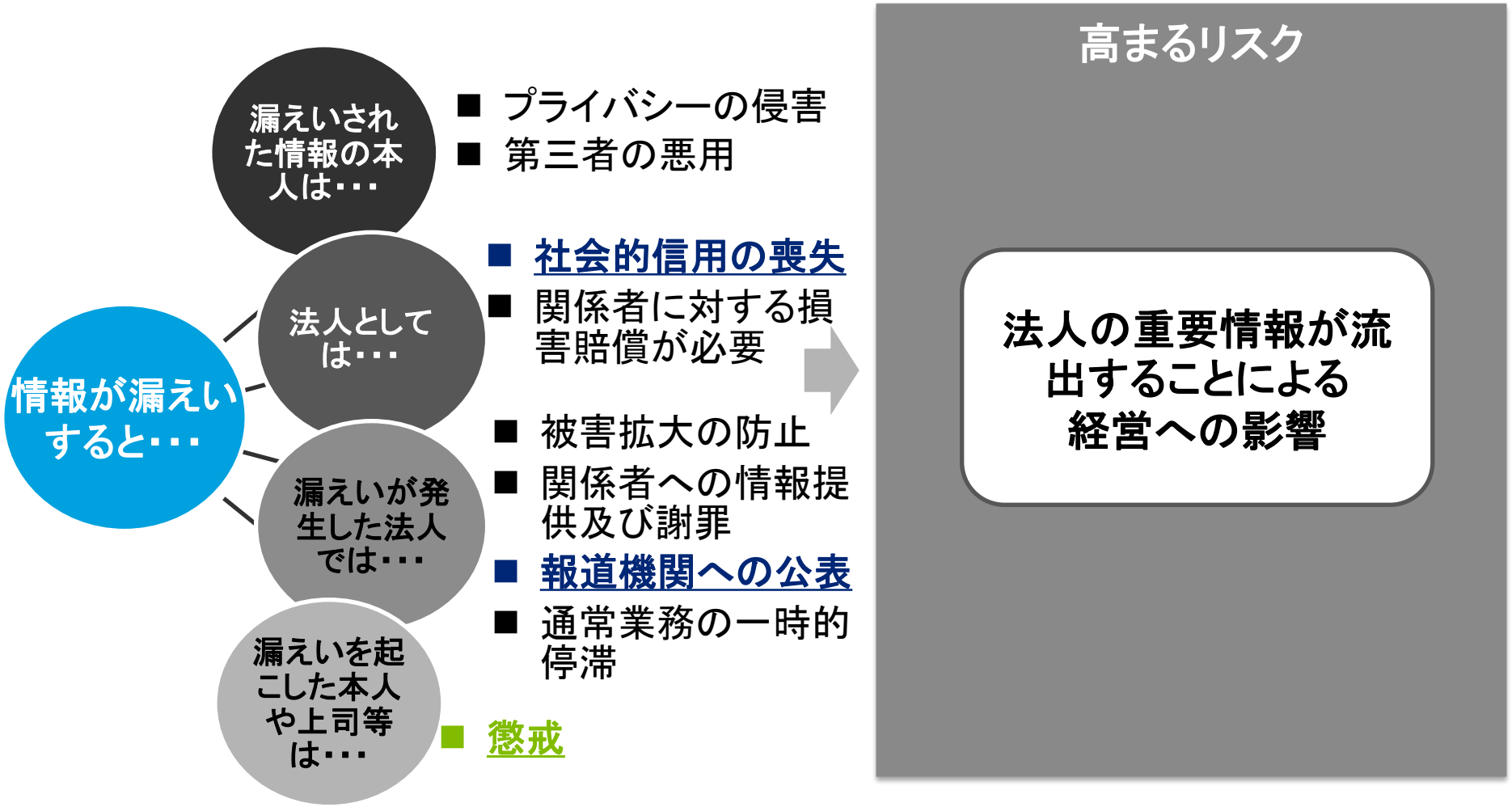
従業員の意識の変化に着目

雇用環境や従業員の意識の変化



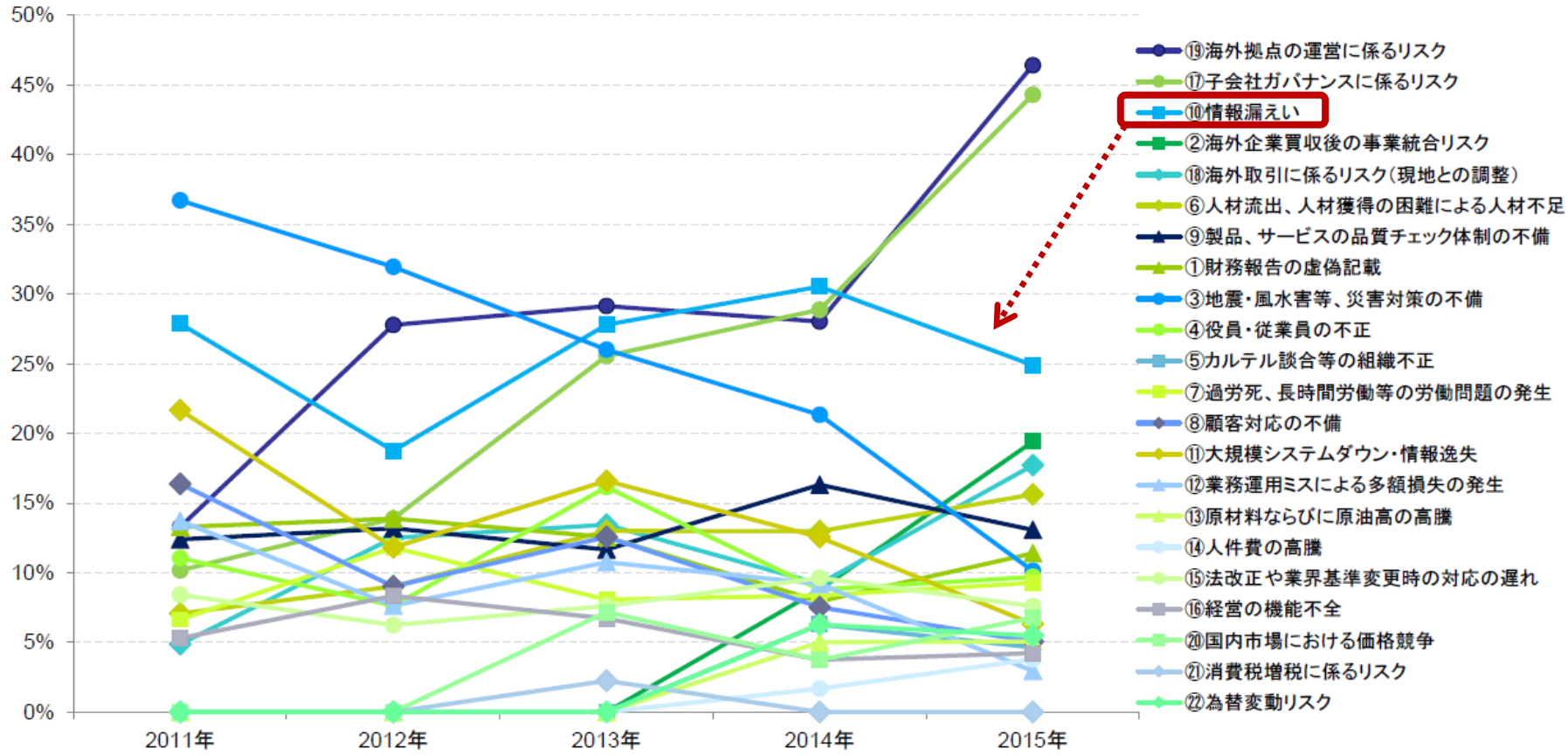
情報の重要性が経営へ直結

情報漏えいのインパクトの増加



情報漏えいは組織全体の重要リスク

優先して着手が必要と思われるリスクの過去5年間推移

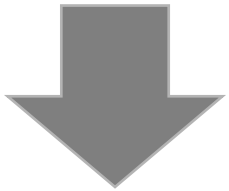


出所：デロイトトーマツ企業リスク研究所：企業リスクマネジメント調査（2015年版）集計結果

情報漏えいへの対策は重要な経営課題

情報管理は経営課題と社内的責任

ITの目覚ましい技術革新	雇用環境や従業員の意識の変化	情報の重要性の高まり



情報管理は、法人にとって重要な経営課題であり、社会的責任であるとの認識が必要

２．情報漏えいの現状

情報漏えいの現状

個人情報漏洩事件･事故一覧

個人情報漏洩事件・事故一覧（1ページ目 / 全304ページ）

2016/11/08 シルバー人材センターが市報の配布名簿を紛失 - 和歌山市
2016/11/07 不正アクセスでクレカ情報流出の可能性 - 日本精神科看護協会
2016/11/07 マルウェア感染で債務者情報が流出か - 新生銀行関連会社
2016/11/07 メルマガ誤送信でメアドが流出 - わかさ出版
2016/11/04 個人情報が保存されたノートPCが所在不明 - NICT
2016/11/04 「古物取引承諾書」を保管期限前に誤廃棄 - ブックオフ
2016/11/04 組織間の配送過程で介護保険関連資料が所在不明に - 大阪市
2016/11/04 中学校で個人情報含む連絡票を紛失 - 堺市
2016/11/02 教員が中学校生徒の個人情報含む私物USBメモリを紛失 - 大阪市
2016/11/02 個人情報の廃棄ミスを公表 - JR西日本ホテル開発
2016/11/01 学生の個人情報含む書類やPCを紛失 - ニトリ
2016/10/31 消防団で要援護者名簿が所在不明 - 熊本市
2016/10/27 融資関連など顧客情報3.7万件が流出、金銭要求する脅迫メールも - 優良住宅ローン
2016/10/27 顧客情報が記載された振込依頼書を紛失 - 三島信金
2016/10/27 児童の個人情報含む記録ノートを紛失 - 大阪市の小学校
2016/10/25 PCに不正アクセス、顧客情報流出の可能性 - 自動車ディーラー

- 情報セキュリティに関する事件・事故は「個人情報漏えい」が従前に引き続きトップ項目となっています。
- 1週間に10件ぐらいが報告されている状況が継続しています。

出所：security-nextHP（2016年11月9日調べ）

情報漏えいインシデントの損害賠償額は増加傾向にあります。

2015年個人情報漏えいインシデント概要データ

項目	2015年	2014年	2013年	2012年
漏えい人数	469万0063人	4999万9892人	925万2305人	972万65人
インシデント件数	799件	1591件	1388件	2357件
想定損害賠償総額	2541億3663万円	1兆6642億3910万円	1438億7184万円	2132億6405万円
1件当たりの平均漏えい人数	6578人	3万2616人	7031人	4245人
1件当たりの平均損害賠償額	3億3705万円	10億8561万円	1億926万円	9313万円
1人当たりの平均損害賠償額	2万8020円	5万2625円	2万7701円	4万4628円

インシデント分析結果

漏えい人数、インシデント件数は減少傾向にあるが、1件あたりの**平均損害賠償額は増加傾向にある。**

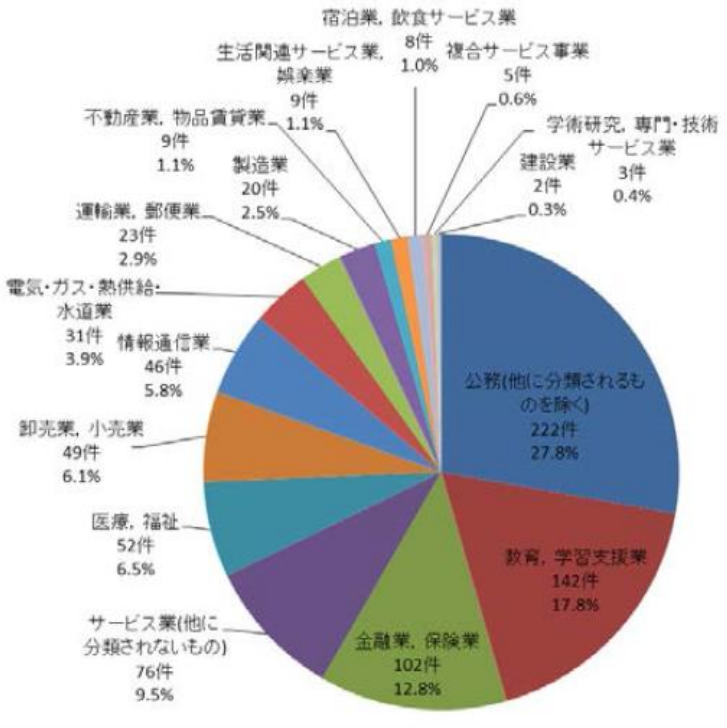
なお、2014年は大規模な個人情報漏えい事件が1件発生したため、漏えい人数、想定損害賠償総額が多くなっている。

■ 損害賠償額＝（基礎情報価値×機微情報度×本人特定容易度）×情報漏洩元組織の社会的責任度×事後対応評価
- 機微情報：政令で定める記述等が含まれる個人情報（改正個人情報保護法：要配慮個人情報
- 社会的責任度：個人情報の適正な取り扱いを確保すべき個別分野の業種（医療、金融・信用、情報通信など）、及び公的機関、知名度の高い大企業

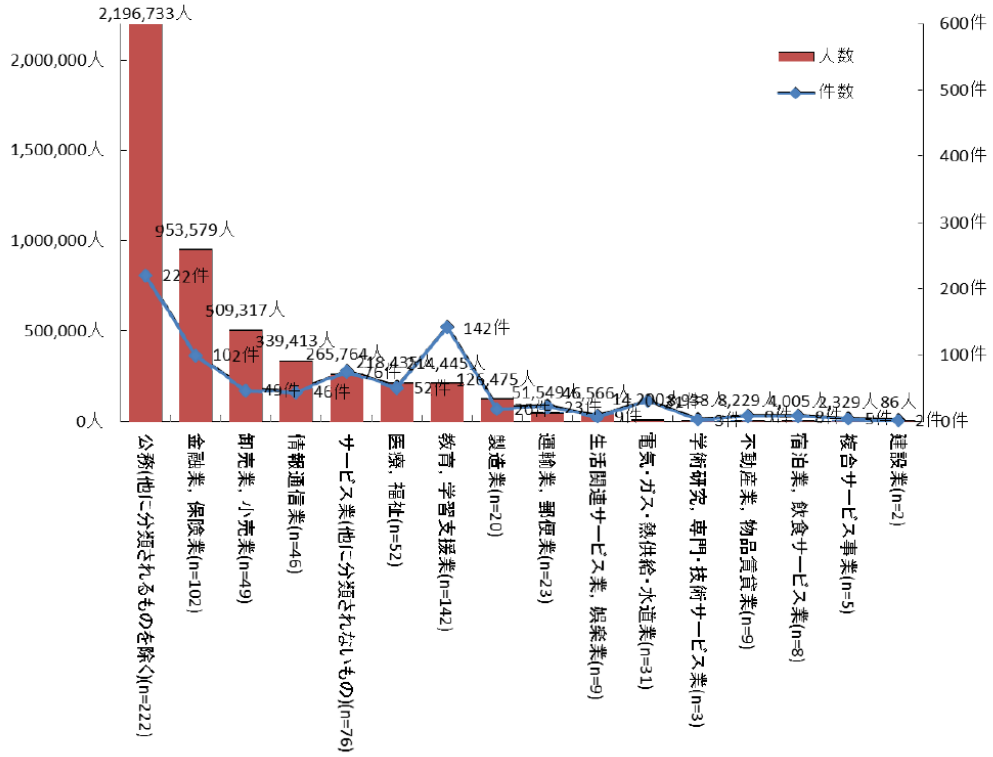
下記の資料表形式を加工して引用
- 2015年情報セキュリティインシデントに関する調査報告書【速報版】Ver.1.0（NPO　日本ネットワークセキュリティ協会）
- 2014年情報セキュリティインシデントに関する調査報告書　～個人情報漏えい編～　第.1.0版（NPO　日本ネットワークセキュリティ協会）
- 2013年情報セキュリティインシデントに関する調査報告書　～個人情報漏えい編～　第.1.0版（NPO　日本ネットワークセキュリティ協会）
- 2012年情報セキュリティインシデントに関する調査報告書　～個人情報漏えい編～　第.1.0版（NPO　日本ネットワークセキュリティ協会）

発生件数に見る行政の指導の強弱

業種別発生件数



業種別インシデント件数と漏えい人数

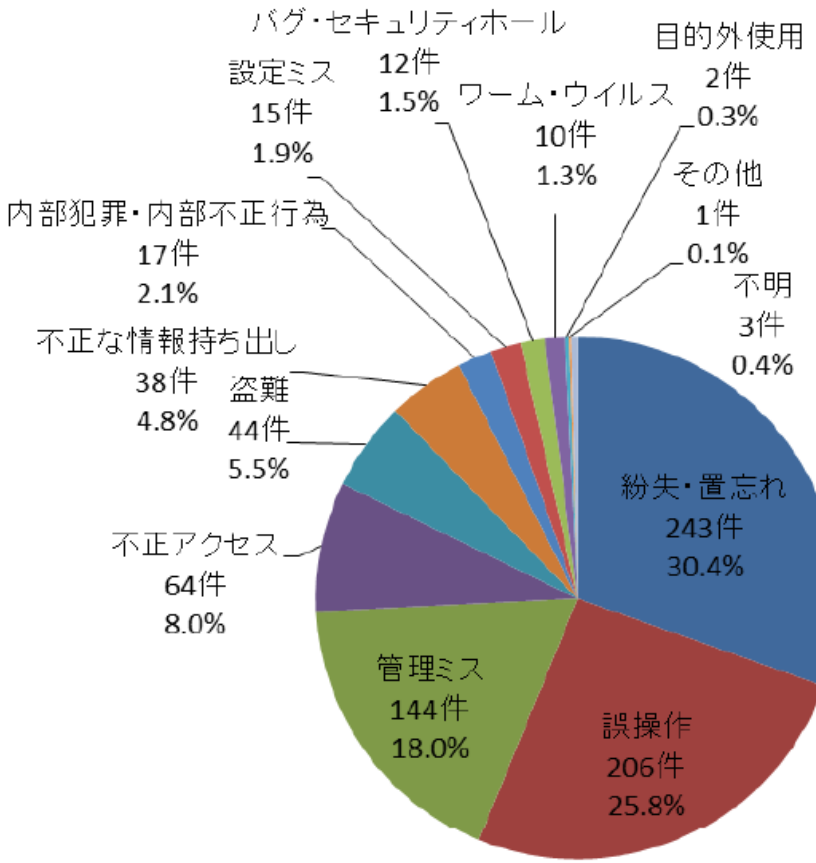


■ 「公務」及び「金融業、保険業」「教育、学習支援業」「医療、福祉」が、常に上位を占めている。これは、個人情報を取り扱うことが多いことに加え、個人情報保護に関する行政の指導が強く働いている業種であり、インシデントを積極的に公表することが多いからである。

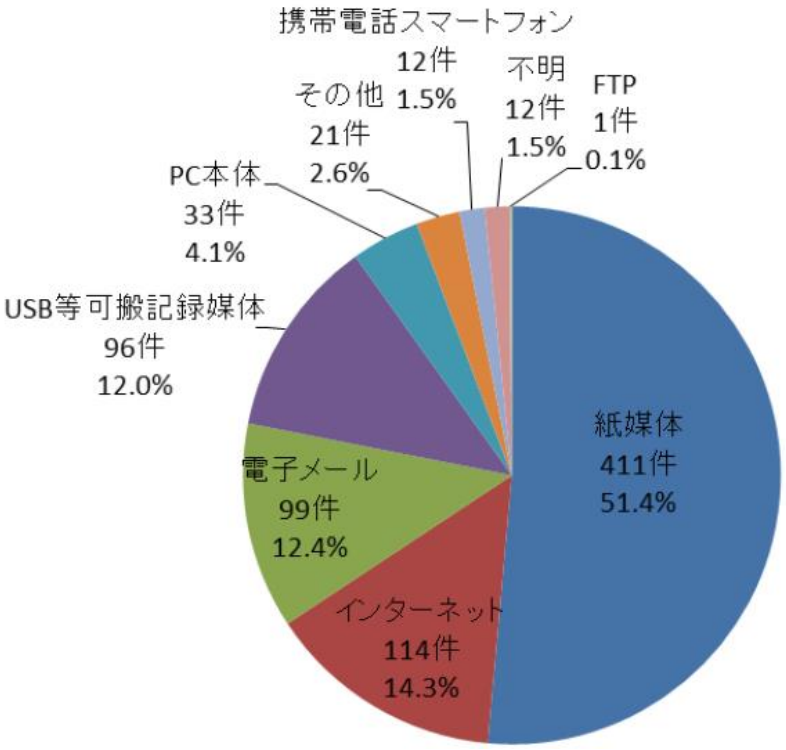
出所：NPO日本ネットワークセキュリティ協会：2015年情報セキュリティインシデントに関する調査報告書【速報版】

情報漏えいインシデント原因の多くは人為的ミスに起因するものです。

漏えいの原因（件数）



漏えい媒体・経路別の漏えい件数



出所：NPO日本ネットワークセキュリティ協会：2015年情報セキュリティインシデントに関する調査報告書【速報版】

組織としてルールを整備し、従業者に遵守してもらうことが重要です。

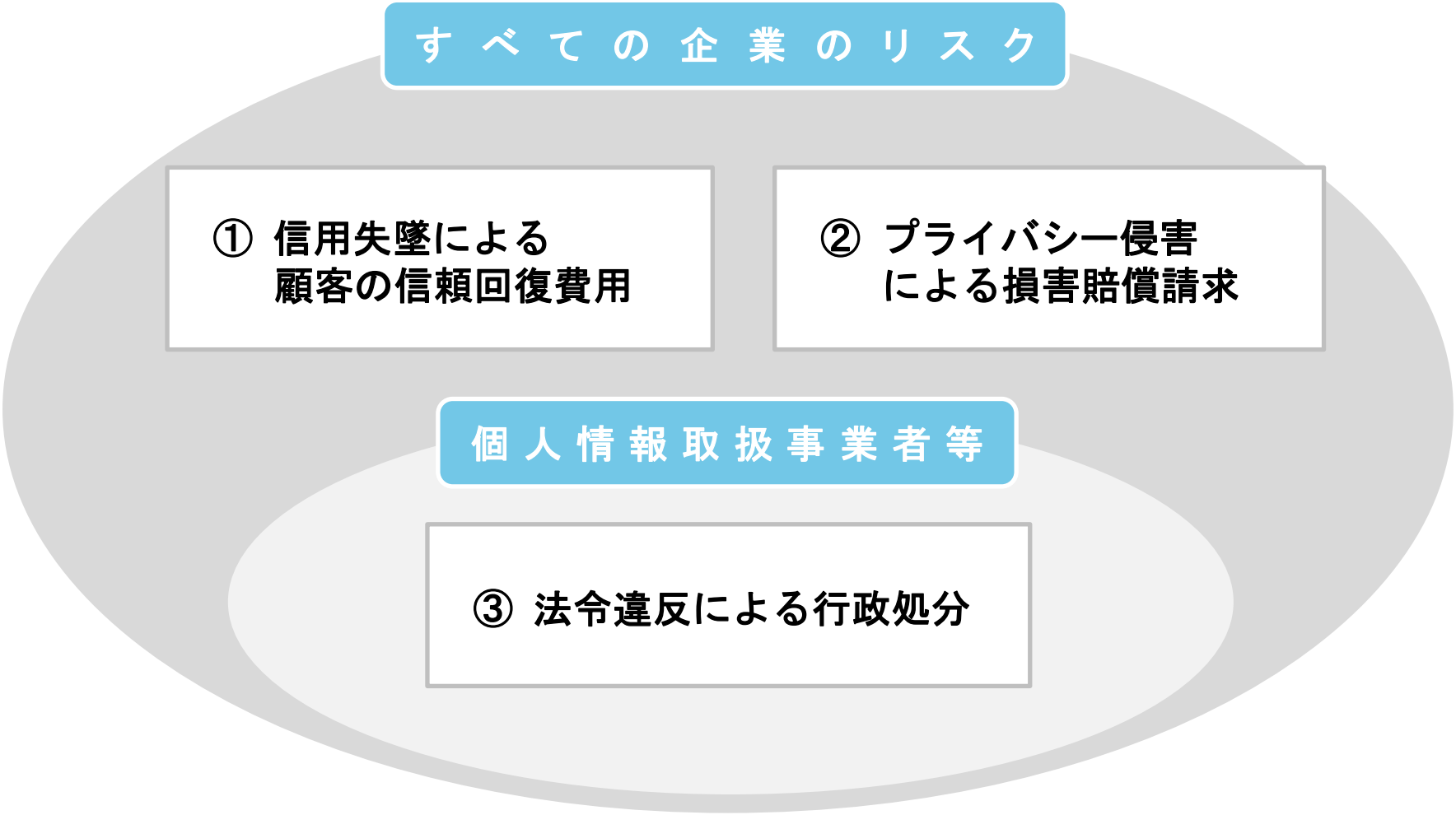
事故原因から求められる会社の対応

事故原因		会社のとるべき対応
紛失・置き忘れ	● 持ち出し許可を得た情報を、持ち出し先や移動中に置忘れたり、紛失したりした場合。 ● **個人の管理ミス**によって発生した場合。	会社は「誤操作」「紛失・置忘れ」「管理ミス」を発生させないために、**組織としてルールを整備し従業者に遵守してもらう**ことが求められます。
誤操作	● あて先を書き間違えたり、操作ボタンを間違えて押したりするなどの**人間のオペレーション**によって情報が漏えいした場合。	
管理ミス	● 社内や主要な流通経由において紛失・行方不明となった場合。 ● 作業手順の誤りや、情報の公開、**管理ルールが明確化されていなかった**ために業務上において漏えいした場合。 ● 紛失の責任が組織にある場合。	

３．情報漏えいが法人に与えるインパクト

情報漏えい3つのリスク

すべての企業が対象です。



①信頼回復費用(1/4):免責にならない委託先の行為

通信教育・出版事業A社の事例

流出内容	■ 顧客個人情報 3,504万件(4,800万人分)
概要	■ 顧客情報データベースシステムの保守・運用委託先(グループ会社の委託先)の社員が、個人のスマートフォンをシステムに接続し、顧客情報(子どもや保護者の氏名、住所、電話番号、性別、生年月日)を不正に窃取。名簿業者への販売を繰り返していた ■ 委託先社員の不正行為は2013年末～2014年6月にわたり繰り返し実行され、情報流出した被害者宛に、不審なDMが届く等の被害が発生していた ■ システムはUSBストレージの接続禁止設定がされていたものの、異なる接続方式であるスマートフォンの接続は可能な状態となっていた ■ A社は被害者からの問い合わせにより、調査を進め事件が発覚した

①信頼回復費用(2/4):2年連続の赤字

社内外への影響

社外への影響	■会員への謝罪文の送付 ■情報漏えいが確認された顧客に対して、**500円の金券を配布**その他、お詫び対応や受講費の減額等で約200億円を準備 ■弁護士を中心とした調査委員会の発足、調査の実施、報告 ■2015年3月期連結決算において、「情報セキュリティ対策費」として、**260億円(補償200億・対策60億)**を計上 ■2016年3月期、会員数が**約10%減少(2期連続赤字決算)**
社内への影響	■外部委託先の社員は、不正競争防止法違反の疑いで逮捕 ■責任部署にいた2名の**取締役が引責辞任** ■情報管理を強化することを目的として、情報セキュリティ企業と共同出資で会社を設立 ■最高法務責任者(CLO)、情報セキュリティ監視委員会の設置 ■ISMSの取得(2015年5月完了)

①信頼回復費用(3/4):大きな企業価値の毀損

株価へ与えた影響

①信頼回復費用(4/4):その他の事例

各社の信頼回復方法

	漏洩事例	信頼回復の方法	発表された信頼回復の費用
大手コンビニ	✓ カード会員約56万人分の個人情報漏洩	✓ リストに記載された115万人にお詫び状と500円の商品券	✓ 対策費用は商品券と合わせて総額約6億円
大手プロバイダー	✓ ADSL(非対称デジタル加入者線)サービスの顧客情報約590万人の個人情報漏洩	✓ 漏洩した590万人に500円の金券を送付	✓ 総額約40億円 ✓ その他管理やシステムの強化費用に数億円
大手石油小売	✓ カード会員約92万人の個人情報漏洩	✓ カードの会員92万人にガソリン代500円分を割引くカードポイントの付与	✓ 総額約5億円
大手通販	✓ 通信販売の顧客情報約66万人分の個人情報漏洩	✓ 個人情報漏洩を受けて、約2ケ月の販売の自粛	✓ 同社によれば、今回の販売自粛により100億円の損失が発生しているという

②損害賠償請求

プライバシーの侵害のよる判例

	漏洩事例	損害賠償
宇治市	✓ 住民基本台帳データが21万人分が漏洩	✓ 京都地裁判決では1人当たり賠償額：**1万円（弁護士費用5千円）**
エステ会社	✓ 5万人分の詳細情報が閲覧可能状態に	✓ 対象者のうち、男女10人が**計1，150万円の損害賠償**を求める訴訟を起こした。 ✓ 判決では**1人当たり賠償額：3万円（ただし、迷惑メールなどの2次被害のない者は1万7千円）** ✓ 顧客激減、人件費増大

③法令による行政処分（1/5）

情報漏えい等に関する法令

名称	狙い	特徴
個人情報保護法 （個人情報の保護に関する法律）	個人情報の有用性に配慮しつつ、 個人の権利利益を保護すること。 （対象例：個人情報を名簿屋へ転売）	個人情報を取り扱う事業者に対して、 遵守すべき義務等を定める。 刑事罰が盛り込まれている。 2017年改正個人情報保護法施行予定
マイナンバー法 （行政手続きにおける特定の個人を識別する番号の利用等に関する法律）	個人情報の保護に十分に配慮しつつ、社会保障制度、税制、災害対策に関する分野における利用の促進を図るとともに、他の行政分野及び行政分野以外の国民の利便性の向上。	①付番 ②情報連携 ③本人確認 その他 ・個人情報保護委員会の設置 ・罰則の強化　等
不正アクセス禁止法 （不正アクセス行為の禁止等に関する法律）	刑法上処罰されない（窃盗罪が適用しにくいなど）情報に対する不正アクセスについて、直接取り締まること。 （対象例：クレジットカードの番号を盗む）	不正にアクセスしただけで犯罪。 （見ただけです、は通らない。） ID・パスワードの漏洩も処罰の対象。
不正競争防止法	不正競争の防止と不正競争に係る 損害賠償について定め、営業秘密を保護すること。 （対象例：自社ノウハウを持ち出して他社へ転職）	ノウハウなどの営業秘密を保護するために制定されたもので、不正取得と不正使用の両方について縛りをかけるもの。

③法令による行政処分(2/5):改正個人情報保護法の概要

改正のポイント

① 個人情報の定義の明確化	・個人情報の定義の明確化(個人識別符合及び要配慮個人情報の明示) ・取り扱う個人情報が5,000人以下の小規模取扱事業者への対応
② 適切な規律の下で個人情報等の有用性を確保	・匿名加工情報に関する加工方法や取り扱い、取り扱い事業者等に関する規定の整備
③ 個人情報の保護を強化	・トレーサビリティの確保(第三者提供に係る確認及び記録の作成義務) ・不正な利益を図る目的による個人情報データベース等提供罪の新設 ・本人同意を得ない第三者提供(オプトアウト規定)の届出、公表等厳格化
④ 個人情報保護委員会の新設及びその権限	・個人情報保護委員会を新設し、現行の主務大臣の権限を一元化
⑤ 個人情報の取り扱いのグローバル化	・国境を越えた適用と外国執行当局への情報提供に関する規定の整備 ・外国にある第三者への個人データの提供に関する規定の整備
⑥ その他事項	・個人情報取扱事業者における更なる安全管理措置の徹底

出所:首相官邸「個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律案」概要

③法令による行政処分(3/5):改正不正競争防止法の概要(1/2)

営業秘密侵害の「範囲」が拡大

変更点	内容
① 営業秘密侵害罪の目的要件の変更	従来は同業他社などがビジネスを有利に進める目的で営業秘密を不正に取得した場合だけが対象とされていたが、改正法ではカネ目当てや不満や恨みをはらすためなど**「保有者に損害を加える目的」(図利加害目的)**が対象となった。
②第三者による営業秘密の不正な取引に対する刑事罰の対象範囲の拡大	
③従業員などによる営業秘密の領得自体への刑事罰の対象	従来は従業者や取引先等、営業秘密を保有者から示された者については、使用・開示に至った段階で初めて刑事罰の対象。 改正法では①記録媒体などの横領、②記録媒体などの記録の複製作成、③記録媒体などの記録の消去義務に違反した上で消去したように仮装する行為、という方法で、営業秘密を領得した場合にのみ限定した上で処罰対象とした。 **※コピー禁止の資料を無断でコピーしたり、持出禁止の資料を無断で外部に持ち出す行為等)**

出所:「営業秘密管理指針　平成15年1月30日　(最終改訂平成25年8月16日)」(経済産業省)
「改正不正競争防止法の概要」「不正競争防止法の一部を改正する法律について」(経済産業省 知的財産政策室)

③法令による行政処分(4/5):改正不正競争防止法の概要(2/2)

不正競争防止法のポイント

不正競争防止法上の営業秘密の保護については、同法上の「営業秘密」の定義を満たす必要があります。

営業秘密とは

秘密として管理されていること(秘密管理性)
有用な営業上または技術上の情報であること(有用性)
公然と知られていないこと(非公知性)

営業秘密として保護を受けるための一般的管理方法

・紙媒体の隅に、「厳秘」や「秘」2などのスタンプを押したり、シールを貼り付ける。
・施錠可能な金庫、などに施錠して保管する。
・コンピュータの閲覧に関するパスワードやIDを設定する。
・定期的行われる朝礼などの際に、随時、営業秘密の取り扱いなどの注意喚起を行う。

出所:「不正競争防止法　2012　」(経済産業省 知的財産政策室)

③法令による行政処分(5/5):【参考】会社法

会社法における会社役員の責任

情報セキュリティに関する体制が不備であるため、情報の漏えい、改ざん又は滅失(消失)若しくは毀損(破壊)によって会社又は第三者に損害が生じた場合、会社の役員(取締役・監査役等)は、どのような責任を問われ得るか

内部統制の概念と情報セキュリティ

各裁判例によれば、内部統制とは「会社が営む事業の規模、特性等に応じたリスク管理体制」と定義される。取締役には、会社に対する善管注意義務(会社法第330 条、民法第644 条)に基づいて、このような内部統制に関する基本方針を取締役会で決定し、決定した基本方針に従った内部統制を構築する義務がある。この「リスク」の中には、情報セキュリティに関するリスクが含まれ得るため、リスク管理体制の構築には、情報セキュリティを確保する体制の構築が含まれ得る。情報セキュリティを確保する体制は、内部統制に含まれ得るといえる。

考え方

取締役会が決定した情報セキュリティ体制が、当該会社の規模や業務内容にかんがみて適切でなかったため、情報の漏えい等により会社に損害が生じた場合、体制の決定に関与した取締役は、会社に対して、任務懈怠(けたい)に基づく損害賠償責任(会社法第423条第1項)を問われ得る。

また、決定された情報セキュリティ体制自体は適切なものであったとしても、その体制が実際には定められたとおりに運用されておらず、取締役(・監査役)がそれを知り、又は注意すれば知ることができたにも関わらず、長期間放置しているような場合も同様である。

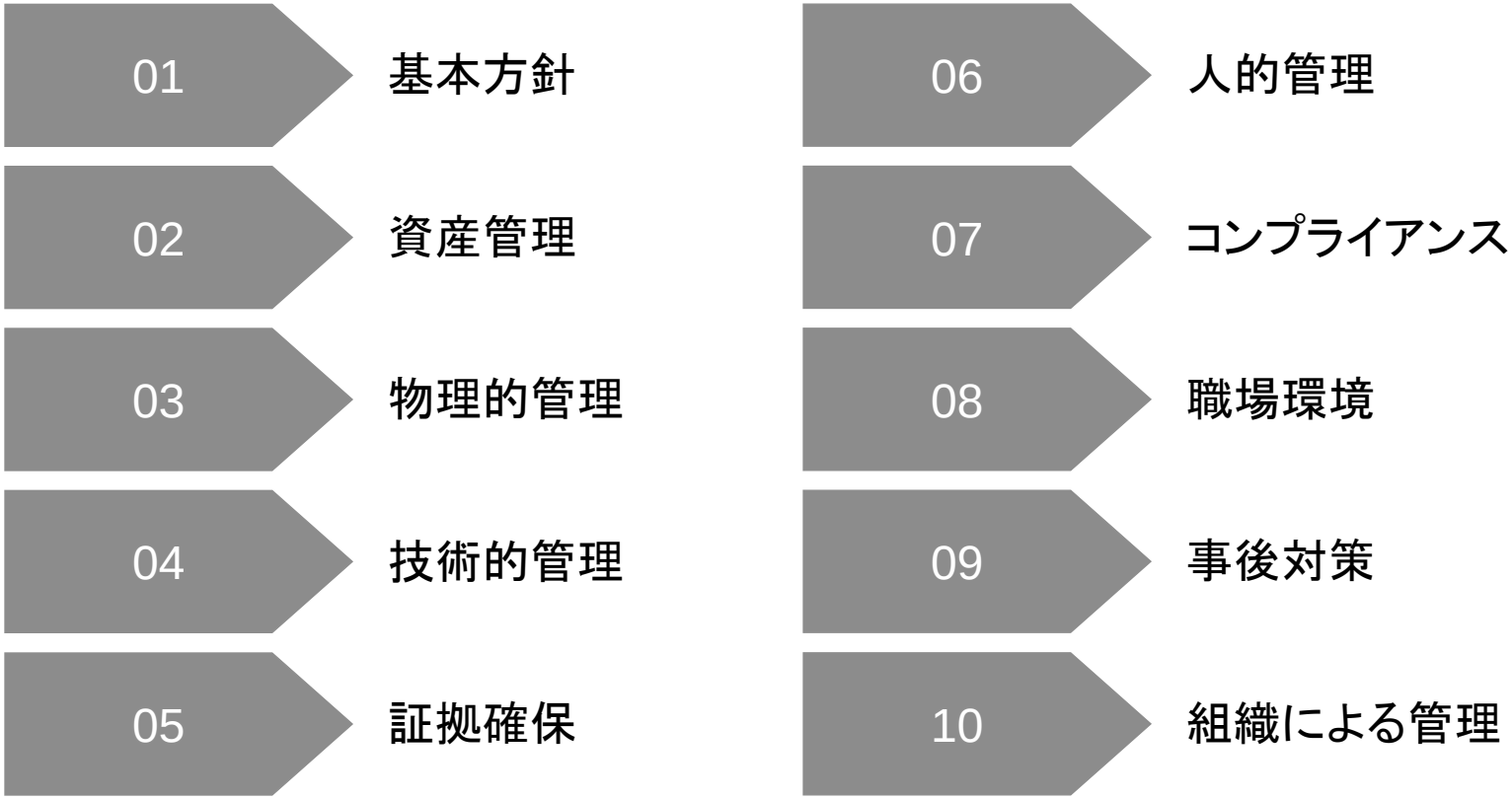
個人情報の漏えい等によって第三者が損害を被ったような場合、取締役・監査役に任務懈怠につき悪意・重過失があるときは、第三者に対しても損害賠償責任を負う

出典:「情報セキュリティ関連法令の要求事項週　2009/06」(経済産業省)

４．情報漏えいリスクを低減させる内部統制と内部監査

多岐にわたる内部統制

情報漏えいリスク低減のための10の施策



出所：独立行政方針情報処理推進機構「組織における内部不正利用ガイドライン」

形骸化していない経営者のリーダーシップ

01. 基本方針

■考えられるリスク

- 経営者による情報漏えい対策への基本方針の策定及び実行のリーダーシップが明確でない場合、実効性のある管理体制が構築できない恐れがある
- 組織内の多岐にわたる部門に存在する重要情報に対し、組織横断的な対策や管理がなされていないと、情報漏えいが発生する危険が高まる

■リスクを低減させる内部統制／内部監査時の確認ポイント

- 経営者による基本方針の策定と方向付け
- 基本方針実行のためのリソース確保の指示
- 定期的なモニタリングと見直し
- 情報漏えい対策の総括責任者の任命
- 総括責任者による各部門担当者の任命
- 情報漏えいの管理体制・部門連携体制の構築
- 業務委託先まで含んだ連携体制の構築

出所：独立行政方針情報処理推進機構「組織における内部不正利用ガイドライン」

必須である定期的な見直し

02. 資産管理

■考えられるリスク

- 情報の重要性の分類、及び重要性に応じて管理しない場合、対策が不十分となり不正発生時に責任を追及できない
- 情報システムにおいて利用者ID やアクセス権が適切に設定されないと、本来アクセス権のない者に重要情報のアクセスを許してしまい、重要情報が不正に利用される恐れがある
- システム管理者は多くの権限を持つため、不正行為を働こうとする「機会」を常に保有している

■リスクを低減させる内部統制／内部監査時の確認ポイント

重要情報の把握と、取扱ルール・管理者の決定	取扱ルールに基づく重要情報へのアクセス権限の設定
必要最小限の権限付与（人員、権限レベル、利用期間）	委託先従業員等への権限付与時の契約上の措置
定期的なアクセス権の見直し	システム管理者（複数名）の任命と相互監視

出所：独立行政方針情報処理推進機構「組織における内部不正利用ガイドライン」

現場での観察及び実機の確認

03. 物理的管理

■考えられるリスク

- 組織が保有する重要情報を格納する装置や情報機器（モバイル端末や記憶媒体含む）に不正に触れることが可能な状態であったり、管理がなされていないと、破壊による業務妨害や、重要情報の盗難・漏えい等の恐れがある
- 個人の情報機器や記憶媒体を持ち込まれると、重要情報を格納して持ち出される恐れがある
- 個人の情報機器や記憶媒体の組織による管理は困難であり、ウイルス感染や操作ミスにより重要情報が漏えいする恐れがある

■リスクを低減させる内部統制／内部監査時の確認ポイント

- セキュリティ強化すべき物理的領域の決定
- 役職員・外部業者毎の入退室管理
- 物理的保護策の実施（認証、監視カメラ、ログ取得等）
- 情報機器や記憶媒体の台帳管理
- 情報機器や記憶媒体の持ち出し時の管理
- 個人の情報機器等の業務利用及び持込ルールの決定
- 個人の情報機器等の組織ネットワークへの接続の制限

出所：独立行政方針情報処理推進機構「組織における内部不正利用ガイドライン」

技術上見過ごされている持ち出し方法の確認

04. 技術的管理

■考えられるリスク

- 組織のネットワーク管理が十分でない場合、パソコン内の重要情報が外部に意図せずに漏えいしてしまう恐れや、外部のファイルを実行することでマルウェア感染を起こしてしまう恐れがある
- SNSや外部掲示板への書き込みが制限されていないと、重要情報がアップロードされてしまい、情報が漏えいする恐れがある
- 情報機器や記録媒体を暗号化等の技術的対策を施さずに持ち出すと、盗難や紛失にあった際に情報が漏えいする恐れがある
- 外部に委託する業務内容と適切なセキュリティ対策を確認せずに契約すると、委託先のセキュリティ不備により情報が漏えいする恐れがある

■リスクを低減させる内部統制／内部監査時の確認ポイント

組織内で使用するソフトウェアインストールの制限	Webアクセスの制限（SNS、掲示板等）
パソコン機器等のパスワード管理	VPN等を用いた通信の暗号化
重要情報の受渡ルールの制定（承認・暗号化・記録等）	受渡しルールの委託先・再委託先等への周知徹底
重要情報の取り扱いに関する契約、定期的確認	

出所：独立行政方針情報処理推進機構「組織における内部不正利用ガイドライン」

ログの分析方法の確認

05. 証拠確保

■考えられるリスク

- ログ・証跡を記録していないと、ログ・証跡から不正行為を検知することができないため、発見の遅れ、発見時に被害が拡大する恐れや不正者の追跡が困難になる恐れがある
- ログ・証跡を記録していないと、システム管理者による不正の機会が増大することになり、システム管理者不正に繋がる恐れがある

■リスクを低減させる内部統制／内部監査時の確認ポイント

重要情報へのアクセス履歴、利用者の操作履歴の取得	ログの定期的確認
ログ・記録の保存の周知	ログの一定期間の保存
システム管理者以外によるログの確認	

出所：独立行政方針情報処理推進機構「組織における内部不正利用ガイドライン」

継続的な教育の重要性

06. 人的管理

■考えられるリスク

- 従業員への教育を実施しないと、情報資源管理に対するモラルの低下につながり、情報漏えい等に繋がる恐れがある
- 雇用終了時の機密保持契約を締結しないと、機密情報に対する認知、取り扱いが不明確になり、機密情報を公開してしまう恐れがある
- 退職予定従業員に対し、セキュリティカード等の返却、情報資産の削除、IDの削除等がタイムリーに行われない場合、社内ネットワークへの不正侵入の踏み台として利用され、情報資産が持ち出される恐れがある

■リスクを低減させる内部統制／内部監査時の確認ポイント

従業員への継続的な教育	教育内容の見直し
職位に応じた教育内容の展開	機密保持契約には、機密保持の対象を明記
雇用終了前の一定期間からパソコン等の監視	

出所：独立行政方針情報処理推進機構「組織における内部不正利用ガイドライン」

内部漏えいに関する誓約状況の確認

07. コンプライアンス

■考えられるリスク

- 情報漏えいに対する処分等が明確になっていないと、不当解雇の訴えにより処分が無効になる恐れがある
- 従業員が機密保持契約書等を提出していないと、重要情報を保護する義務があることを認識できない恐れや懲戒処分等が法的に認められない恐れがある

■リスクを低減させる内部統制／内部監査時の確認ポイント

- 重要情報の対象の明確化
- 査問委員会等による事実関係の明確化
- 刑事告発等の法的な手続きの内部規程の整備
- 契約書提出の徹底
- 入社時以外にも契約書・誓約書の更新手続き

出所：独立行政方針情報処理推進機構「組織における内部不正利用ガイドライン」

職場環境の影響の理解

08. 職場環境

■考えられるリスク

- 人事評価が公平になされないと、不平や不満を要因とした環境低下を招き、情報漏えいを誘発する恐れがある
- 人事異動が定期的になされないと、特定の重要情報を特定の従業員が取り扱うことになり、不正を誘発する恐れがある
- 人事異動が定期的になされないと、特定の重要情報の取り扱いに対する緊張感が薄くなり、情報管理機器等の誤操作を誘発する恐れがある

■リスクを低減させる内部統制／内部監査時の確認ポイント

評価基準の明確化

部長等へ評価基準の遵守の徹底

定期的な人事異動の実施

出所：独立行政方針情報処理推進機構「組織における内部不正利用ガイドライン」

具体的な漏えい発生を想定した事後対策

09. 事後対策

■考えられるリスク

- 事故の影響範囲を特定できない場合、迅速な事後対策が施せない恐れがある
- 事故の影響範囲を特定できない場合、法的処置等の対応を検討できない恐れがある
- 事故を引き起こした当事者の処罰を検討しない場合、同様の事故を再発させてしまう恐れがある
- 再発防止策を実施しない場合あるいは再発防止策を組織の内部に周知しない場合、同様の事故を再発させてしまう恐れがある

■リスクを低減させる内部統制／内部監査時の確認ポイント

事故発生時の対応手順や報告手順の整備	事故の具体的状況が検証可能な証拠（記録）の保全
外部の関係者（監督官庁、委託先業者）との連絡体制	内部の関係部署との連携（連絡体制）
労働法制を順守した懲戒処分に関する内部規程の整備	再発防止策の検討、実施

出所：独立行政方針情報処理推進機構「組織における内部不正利用ガイドライン」

通報制度の整備及びモニタリングの実効性の確認

10. 組織による管理

■考えられるリスク

- 通報制度が整備されていない、もしくは従業員に具体的利用方法が周知されていない場合、事故の予兆は通報されず、事故への対応が遅れるだけでなく、事故の予兆を見逃してしまう恐れがある
- 定期的及び不定期にモニタリングによる確認を実施しない場合、事故対応の状況や組織の問題が確認できず、効果的な対策の実施や見直しができない恐れがある

■リスクを低減させる内部統制／内部監査時の確認ポイント

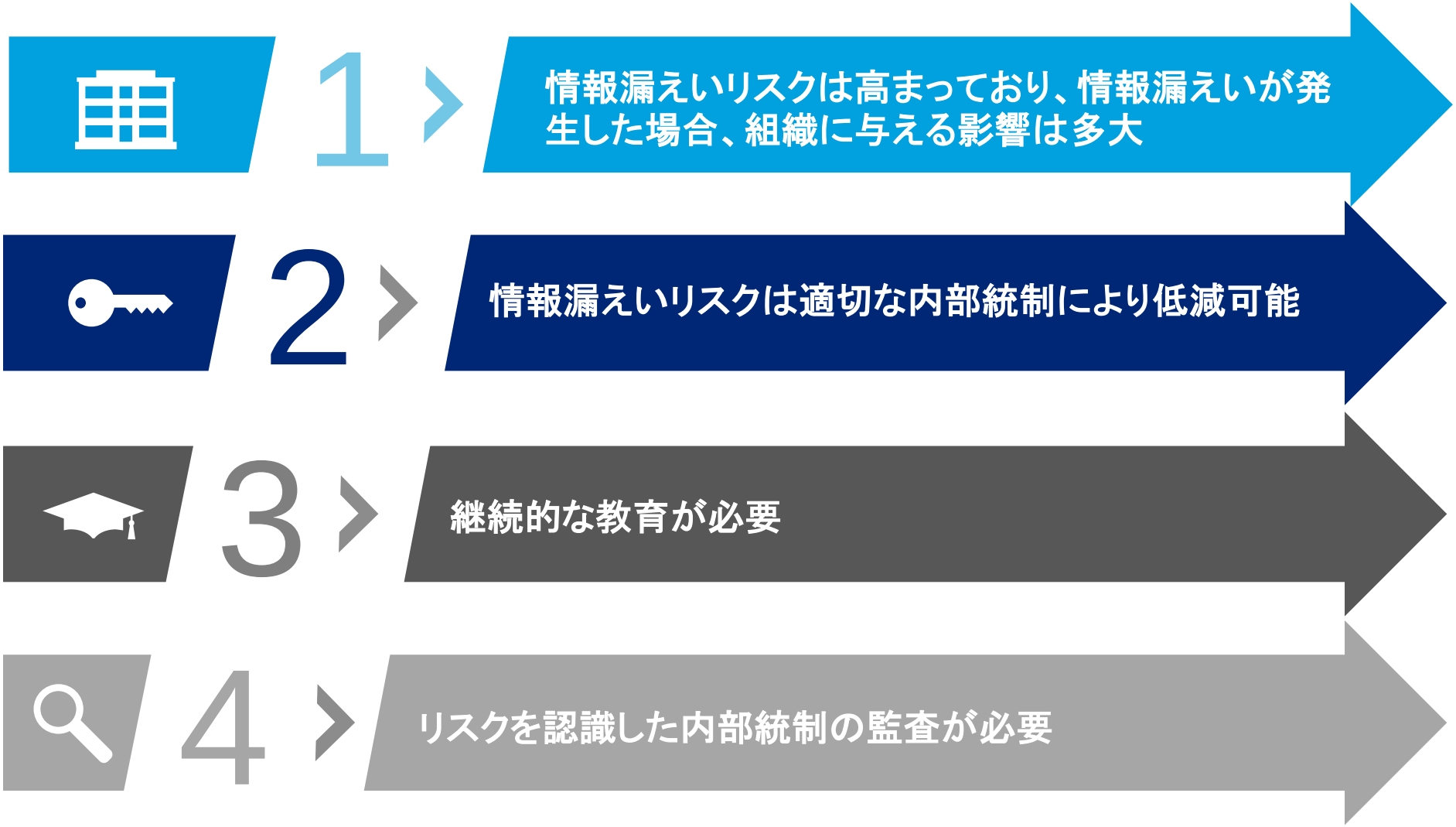
受付窓口や通報時の提供情報等の明示	従業員への通報制度の周知・教育
モニタリング及び監査結果の経営者への報告	モニタリング結果を検討し、必要に応じた対策の見直し

出所：独立行政方針情報処理推進機構「組織における内部不正利用ガイドライン」

5. まとめ

まとめ

情報管理のPDCAサイクル



Deloitte. トーマツ.
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 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およびDT弁護士法人を含む）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、税務、法務、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8,700名の専門家（公認会計士、税理士、弁護士、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）は、監査、コンサルティング、ファイナンシャルアドバイザリーサービス、リスクマネジメント、税務およびこれらに関連するサービスを、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Fortune Global 500®　の8割の企業に提供しています。“Making an impact that matters”を自らの使命とするデロイトの約225,000名の専門家については、Facebook、LinkedIn、Twitterもご覧ください。

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（“DTTL”）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。Deloitteのメンバーファームによるグローバルネットワークの詳細は www.deloitte.com/jp/about 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。