税理士が知っておくべき情報セキュリティのリスクと対策

LRM株式会社

目次

はじめに

会社概要

私たち**LRM株式会社**は、クライアント企業様の**「情報セキュリティ水準向上」**と
「業務効率・業務品質高度化」の両立を目指し、各種事業を展開してまいります。

会社名　LRM株式会社

住所　**東京オフィス**

〒141-0031 東京都品川区西五反田7-1-9

博多オフィス

〒812-0013 福岡県福岡市博多区博多駅東2-5-19

神戸オフィス

〒650-0023 兵庫県神戸市中央区栄町通1-2-10

連絡先　0120-979-873

info@lrm.jp

設立　2006年12月

代表　幸松 哲也

認証等　ISO/IEC27001:2013

IS605509/ISO27001:2013

ISMS認証は東京オフィス、
神戸オフィスで取得しています。

事業　**コンサルティング事業**

- プライバシーマーク取得支援
- ISMS/ISO27001認証取得支援
- クラウドセキュリティ認証取得支援
- ISMS＆プライバシーマーク運用支援
- セキュリティBPO

ソリューション事業

- 情報セキュリティ総合支援サービス「Seculio」
- メール自動暗号化サービス「メールZipper」
- PCログ管理サービス「セキュログ」
- 容量無制限クラウドストレージサービス「box」
- セキュリティ対策サービス「ZENMU」

本セミナーで得られること

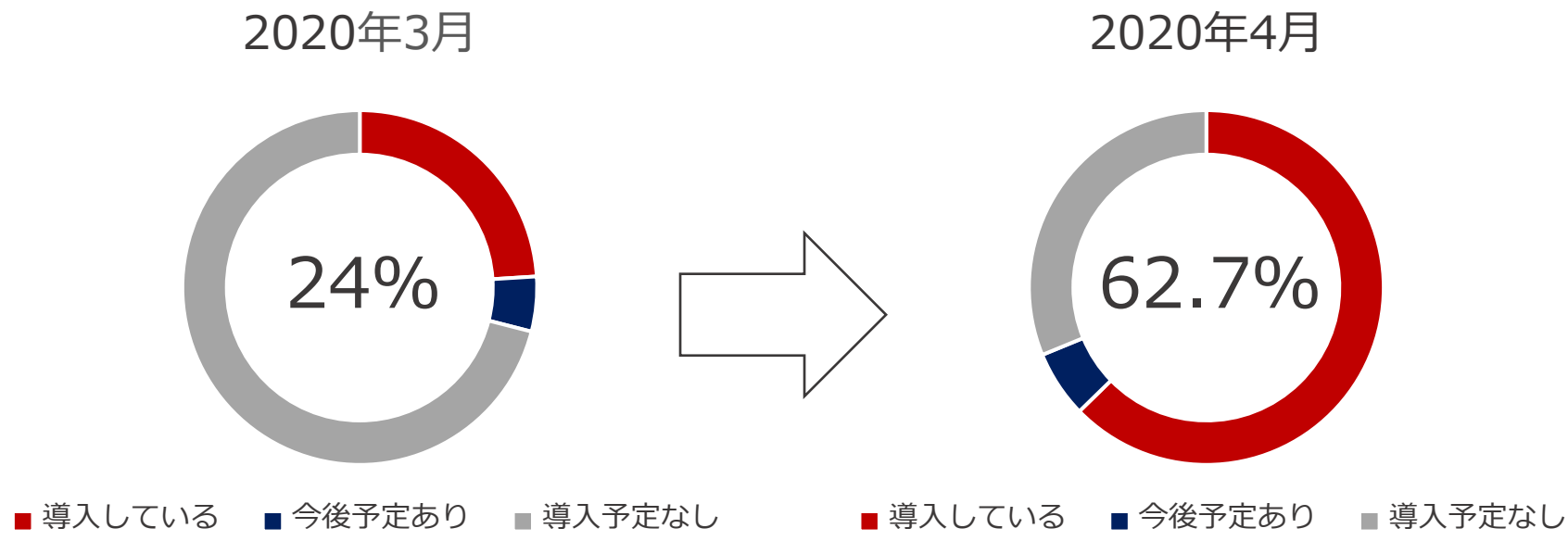
- ✓ 新しい働き方における基本となるセキュリティ対策がわかる！
- ✓ 業界特有のセキュリティリスクを把握し対策につなげることができる！
- ✓ セキュリティにおける第三者認証(ISMS・Pマーク)がクライアントからなぜ求められるのかがわかる！
- ✓ 自社でISMS・Pマークを取得する場合の取り組みイメージがわかる！

コロナ禍における企業/士業の働き方の変化

企業/士業が直面する新たな情報セキュリティリスク

新型コロナウイルス感染症の影響で多くの企業がテレワークへ移行

都内企業に務める従業員への調査結果



2020年5月11日に東京都が発表した、「東京都 テレワーク導入緊急調査」より

コロナ禍における企業/士業の働き方の変化

1 働く場所

コロナ流行以前は、一部の企業以外はオフィスに出社し業務に携わることが当たり前でした。しかし、コロナの流行をきっかけに、政府主導でテレワークの推進が図られ、今や働く場所に制限がなくなりました。働く環境が変われば、想定されるセキュリティリスクも変わってきます。企業としてもテレワークにおけるセキュリティ対策が必須となります。

2 アウトソーシング

働き方の変化により、それは本当に自社内で対応しなければならない業務かを見直し、今まで自社で行っていた業務をアウトソーシングもしくはツール導入する企業も増えています。例えば、自社の売り上げに直結する業務にリソースを割けるように経理業務を全て他の企業に委託するということが挙げられます。

3 紙から電子

多くの企業はテレワークへの移行に合わせて、クラウドストレージサービスを導入し、情報の電子化を進めています。特にクラウドサービスを利用すると、インターネットに接続するだけでどこにいても業務を行うことができ、大手企業から中小企業まで導入が進められています。

企業/士業が直面する新たな情報セキュリティリスク

1 紙やPCを始めとする情報資産の持ち出し

テレワークを行うために、今までオフィスから持ち出すことがなかった資料やPCを持ち出すということが考えられます。
PCや紙媒体の重要資料の持ち出しは、紛失・盗難・廃棄ミスといったリスクがあり企業として対策を実施することが求められます。

2 委託先企業選定の重要性

業務のアウトソーシングやツールの導入を行った場合、委託先に自社の機密情報を預けることになります。委託先企業で個人情報の漏えい等があった場合、委託元としての監督責任や社会的責任、場合によっては法的責任を負うことになります。
企業はセキュリティを含めた選定基準を設け、委託先を選定することが求められています。

3 クラウドツールのアクセス権限の設定

クラウドサービスを利用する企業では、担当者の閲覧権の設定ミスにより、個人情報が世界中の誰でも閲覧できる状態になってしまうというリスクがあります。
インターネットに接続できる場所であればどこからでも利用できることから、閲覧権限の設定ミス、不正アクセスの脅威、情報の持ち出し、と利便性の反面、多数のリスクがあることを把握した上での対策実施が求められています。

最新の事故事例から学ぶ

注目すべき情報漏えい事故事例

クラウドサービスの閲覧権限の設定不備による顧客情報の漏えい

概要

2021年、クラウド会計ソフト大手のfreee株式会社は、クレジットカード番号を含む約2800件の顧客情報が漏洩した恐れがあると公表しました。
同社が利用する社外のクラウド型お問い合わせ管理システムにおいて、お問い合わせ受付内容の一部が、約10日間、第三者からアクセスしうる状態となっていました。

原因

同社は、社外のクラウド型お問い合わせ管理システムの利用における権限設定の不備により、第三者によるアクセス可能な状態にあったことが原因であると公表しています。

再発防止のためには

同社は、発見後すぐに設定を変更し第三者からアクセスを不可能としました。
再発を防ぐためには、最小限の担当者しかアクセス権を変更することができないようにした上で、定期的なアクセス権の見直しを実施することが必要です。

参照:https://corp.freee.co.jp/news/system-research.html

機密情報の持ち出しによる情報漏えい

概要

ソフトバンクは、2019年末に同社を退職して楽天モバイルに転職した元社員が、秘密保持契約を結んでいたにもかかわらずソフトバンクの営業機密情報を不正に持ち出していたことが判明し21年1月に逮捕されたと発表しました。不正に持ち出された営業秘密は、4Gと5Gネットワーク用の基地局設備や、基地局同士や基地局と交換機を結ぶ固定通信網に関する技術情報でした。同社は、今後、当該社員への損害賠償請求を含めた措置を検討しています。

原因

元社員が、転職先への手土産とするために悪意を持って機密情報の持ち出しを行ったことが原因となります。

再発防止のためには

本件では、元社員と秘密保持契約を結んでいたにもかかわらず起きた事件となります。すべてを防ぐことはできませんが、企業として、セキュリティ教育を実施する、ログの分析を行う等の対策を実施して、不正な持ち出しを防ぐため最大限の対策を行うことが重要です。

委託先の企業が、誤ったFAX番号を申請者に連絡

概要

2020年8月、埼玉県は、同県の事務作業を委託した企業によるミスが原因で、個人情報を記載した書類を全くの第三者に誤送付する事故が発生したことを発表しました。同県は、中小企業・個人事業主追加支援金審査事務を、民間の企業に委託していました。この委託先企業は、審査に必要となる書類を送付する宛先のFAX番号が変更になることを受け、申請者85名にFAX番号の変更を通知しました。
しかしその際、誤ったFAX番号を伝えてしまっていたため、9名の申請者が、その誤ったFAX番号宛に審査書類を誤送付してしまいました。

原因

委託先の企業が誤った送付先を申請者に送付してしまったことが原因です。

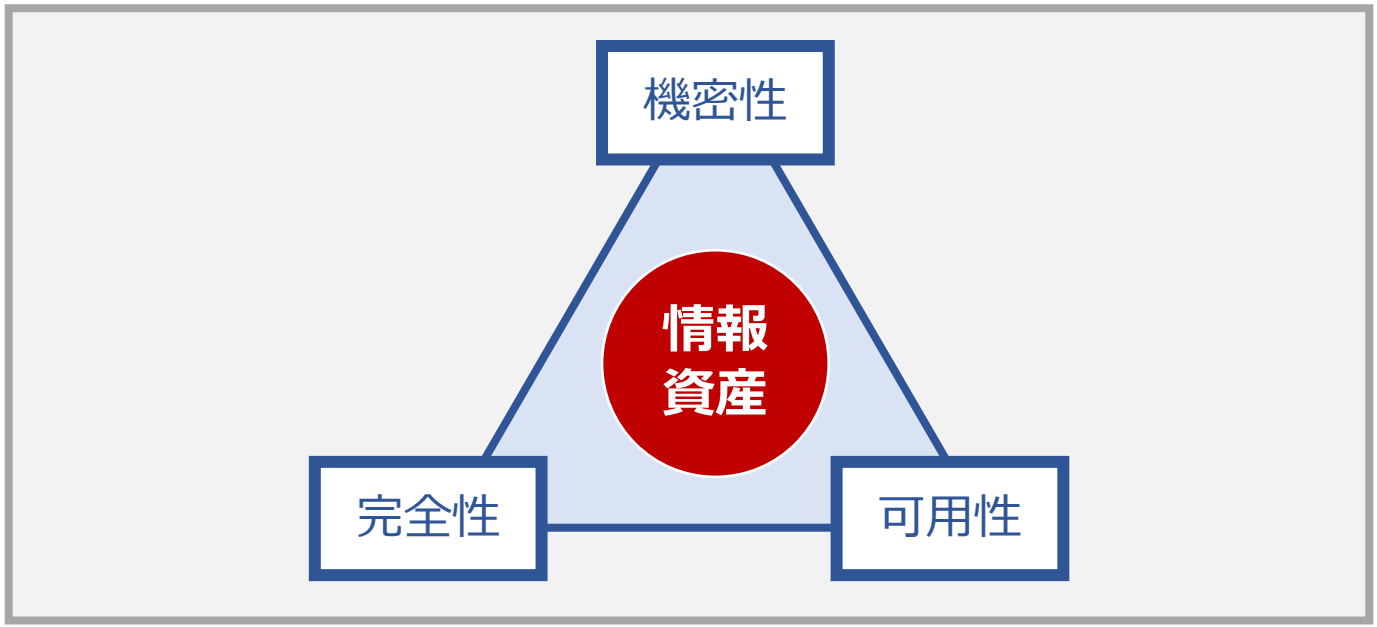
再発防止のためには

埼玉県の立場として、委託先のミスを防ぐことは率直に言って困難ですが、「重要情報の取扱い時にはダブルチェックするようにルール化やルールの周知をしているか」など運用状況の確認を行っていれば、事故自体を防げたかもしれませんし、少なくとも、委託元として「できる限りの対策を講じていた」と言えたでしょう。

あらゆるリスクに備えた対策の実施

企業が講じるべき情報セキュリティ対策

情報セキュリティの重要性　三要素



機密性 Confidentiality	完全性 Integrity	可用性 Availability
情報資産が、勝手に盗み見られないように守ること	勝手に改ざんされないように、また、その内容が正確であるように守ること	適切な人が、必要なときに使えるように守ること

情報セキュリティの重要性

情報セキュリティ事件・事故の発生

直接的な被害

- 業務活動の停滞・中断
- 契約解除・違約金
- 関係先への説明・お詫び
- 原因調査・原状回復コスト
- 追加対策の実施コスト

間接的な被害

- 被害者への損害賠償の発生
- 業務停止処分の恐れ
- 市場からの信頼の失墜
- 売り上げ減少・営業の難航
- 企業モラル低下・退職誘発

顧客を守り、取引先を守り、会社を守り、ひいては従業員を守るために
企業として**情報セキュリティ**の取り組みが必要不可欠

紙文書の取扱いにおけるセキュリティ

1 保管場所の施錠

個人情報が記載された紙文書は施錠保管を実施し、担当者以外が閲覧をすることがないようにする必要があります。鍵付きの保管庫に保管し、必要な時のみ取り出して利用します。そして利用後は速やかに元の場所に戻すようにしましょう。

各個人の机は、社外に出かける時、帰宅する際には、各机は施錠するようにしましょう。

2 クリアデスクの継続実施

重要文書の紛失・盗難を予防するため、机の上下は整理整頓し、放置を防ぎましょう。

もし重要文書などをデスクの上に放置しているのを見かけた場合は、従業者同士で声を掛け合い、クリアデスクを習慣化することが継続的な実施の鍵となります。

3 シュレッダーにかけてから廃棄

個人情報が書かれた紙文書は、必ず「シュレッダーにかける」など第三者が情報を確認できない状態にして廃棄しましょう。裏紙として使用することは禁止です。

ごみを漁って個人情報を持ち去る事案もありますので、注意が必要です。

1 パスワードの設定

PCのOSの起動時にパスワードを設定し、業務利用するOSアカウントに第三者がログオンできないようにしましょう。

パスワード設定時は、複雑なパスワードを設定するよう意識してください。

2 スクリーンセーバーの設定

担当者の離席時に第三者がPCを操作してしまう、内容を閲覧してしまうというといったことがないよう、一定時間PCを操作しない状態で放置しておくと自動で画面にロックがかかるように設定しておきましょう。

離席時には都度手動でロックをかけるのも良いでしょう。

3 ウイルス対策ソフトの自動更新

ウイルス感染による外部漏えいを防ぐため、ウイルス対策ソフトを自動でアップデートがかかるように設定しましょう。

メール利用時におけるセキュリティ

1 送信先の二重確認

個人情報の取扱いにおける事件の原因として、最も多いのがメールの誤送信です。

メールを送信する前に、宛先が正しいか必ず確認を行いましょう。

2 複数の宛先へ送る場合はBccで送付

取引先（担当者）やセミナー参加者など複数の人に同時にメールを送信する必要がある場合は、送信先が他の受信者に見えるのを避けるため、送信先のアドレスをToやCCでなく、BCCに入れましょう。

3 添付ファイルの暗号化

メール本文には個人情報を記入せず、添付ファイルに記入し送信しましょう。

添付ファイルはパスワードをかけた状態で送りましょう。パスワードは別のメールで送るなどし、ファイルが添付されたメールには記載してはいけません。

直接メールにファイルを添付するのではなく、クラウドストレージサービスのURLを閲覧権限の設定の上共有することも有効です。

クラウドサービス利用時におけるセキュリティ

1 アクセス権の設定

どの情報が、どの範囲の対象者からアクセス可能であるかを意識し、外部へ公開するときは特にアクセス権の設定の確認を行いましょう。

管理者は、定期的にアクセス権の確認を行い、必要に応じて権限付与の範囲を再検討、アクセス権の整理を行いましょう。

2 サービスごとのパスワード設定

クラウドサービスのIDやパスワードを他のサービスでも使いまわしていた場合、一つの流出から他のサービスの情報までもが漏えいする可能性が高まります。

IDやパスワードは、複雑なパスワードを設定するとともに、個別のサービスごとに異なるものを設定しましょう。

3 退職者のアカウント管理

退職者のアカウント削除、アクセス権の制限が行えておらず、退職後もインターネット上のクラウドシステムなどにログインできてしまう状況であれば退職者からの個人情報漏えいにつながりかねません。

退職者のアカウントの管理は抜け漏れのないように行いましょう。

顧問先企業に進言すべきセキュリティチェックポイント

情報漏えいを防ぐためには、働き方に合わせたセキュリティ対策を実施することが重要です。
士業の皆様は、顧問先企業へ下記の点を進言することをお勧めします。

- ✓ **テレワークを実施する際のセキュリティルールはあるか**
  - ✓ 情報の持ち出しルールは決まっているか
  - ✓ 社外におけるWi-Fiの利用ルールは決まっているか
  - ✓ インシデント発生時のルール(連絡経路等)は決まっているか
- ✓ **委託先企業の選定の基準があるか**
  - ✓ 委託先に求めるセキュリティ水準を定めているか
  - ✓ 秘密保持に関する契約を委託先と締結しているか
  - ✓ どこにどのような情報を委託しているか明確にし管理しているか
- ✓ **社内におけるクラウドサービスの利用状況を把握しているのか**
  - ✓ 社外へ共有する場合は、閲覧権限が必要最低限になっているか
  - ✓ 社員が私物利用していないか
  - ✓ ログインパスワードが類推されやすい文字列で設定されていないか

組織としてセキュリティ対策を行う

働き方の多様化により、セキュリティに関して考慮すべき要素が増えていることがわかりました。

GDPRの存在や個人情報保護法の改正に伴い、各企業においては、取引先等からこれまで以上に実際的なセキュリティルールの運用が求められることとなります。

そこで、自社のセキュリティレベルを証明する手段として、昔ながらのISMSやPマーク、近年注目を集めるISO27017やISO27701等の第三者認証が脚光を浴びています。

セキュリティに関する第三者認証を取得しているかどうかは、顧問先の企業様のみならず、税理士様をはじめとする企業を選定する際の基準になってきています。

情報セキュリティとISMS/Pマークの関係

Information Security Management System

の略語で、組織の情報セキュリティを管理する仕組みのことです。

企業をはじめとする様々な組織が、情報を適切に管理し、
機密を守るために考案された枠組みのことをいいます。

システム上のセキュリティ対策だけでなく、情報の取扱いポリシーや、
具体的な計画、さらに運用、見直しまでを含めたマネジメント体系を
指します。

人間が業務を行う以上、情報漏えいを「完全に無くす」ことは難しい。

「情報を漏らさせない」「情報が漏れても被害を最小限に抑えられる」
ような**「仕組み作り」**が必要。

＝マネジメントシステムの構築が重要！

プライバシーマーク(Pマーク)とは？

Pマークは、「**個人情報保護**」に特化した第三者認証です。

Pマーク制度は、日本工業規格「JIS Q 15001個人情報保護マネジメントシステム―要求事項」に適合して、個人情報について適切な保護措置を講ずる体制を整備している事業者等を認定して、その旨を示すPマークを付与し、事業活動に関してPマークの使用を認める制度です。

上記の適切な保護措置を講ずる体制を

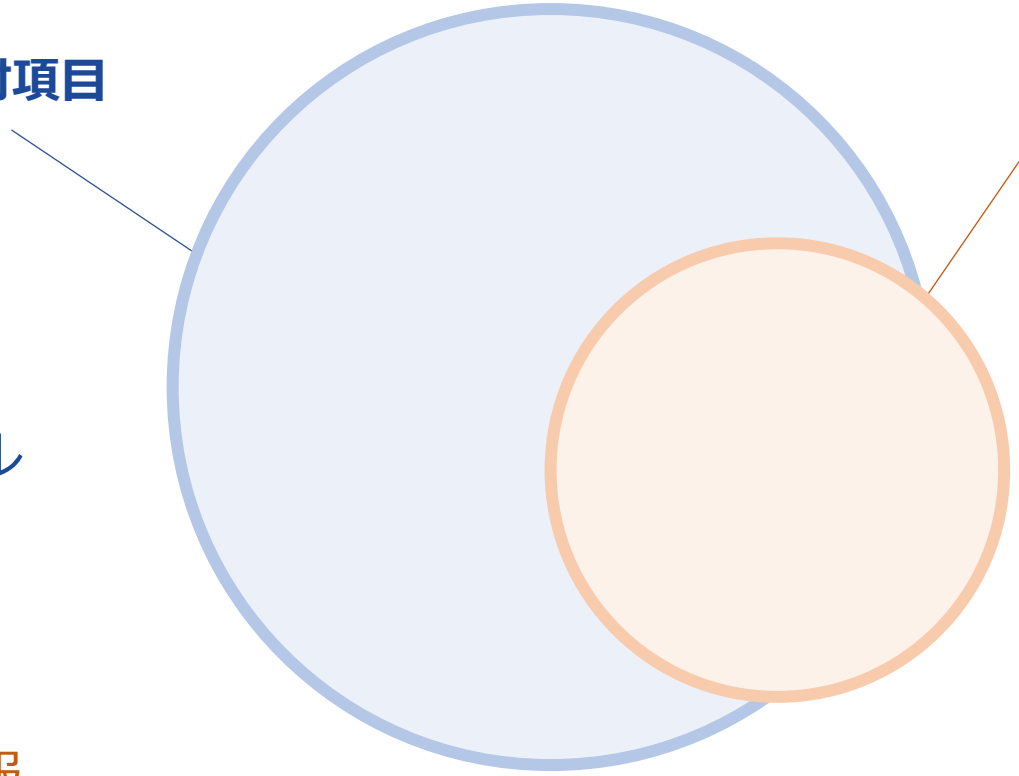
Personal information protectionManagement Systems(PMS)

と呼び、プライバシーマークの取り組みにおいては、PMSの構築が主眼となります。

企業の情報資産と個人情報の関係

ISMSにおける検討項目

- ✓ 営業情報
- ✓ 新サービス
- ✓ 設計情報
- ✓ 経営機密
- ✓ 作業マニュアル
- ✓ 企業ノウハウ
- ✓ 顧客情報
- ✓ 社員情報
- ✓ 人事情報
- ✓ 預かり個人情報



Pマークにおける検討項目

- ✓ 顧客情報
- ✓ 社員情報
- ✓ 人事情報
- ✓ 預かり個人情報

ISMSの検討項目は、システム関連部分等への言及がある分、
Pマークに比べて広範に渡っています。

マネジメントシステムの構築　PDCAサイクル

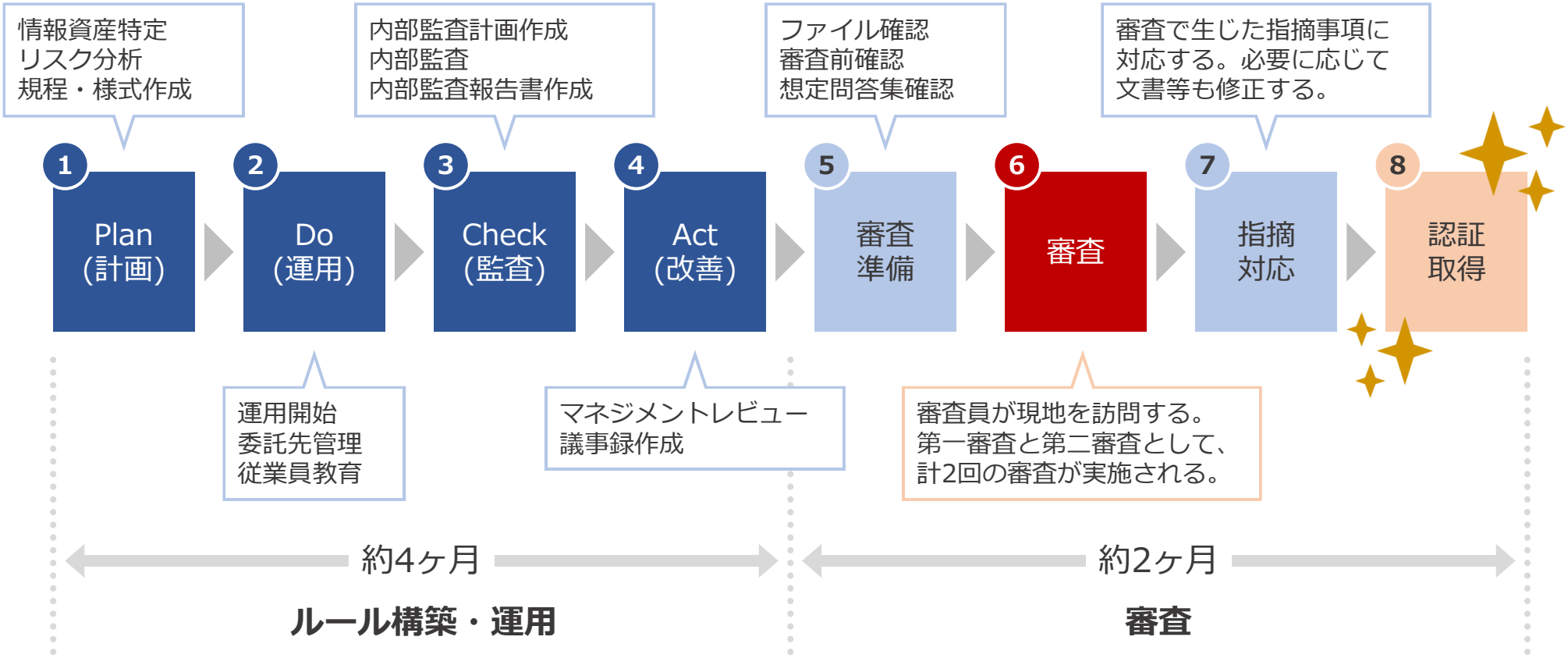
世界的に、マネジメントシステムの体系は、**PDCAサイクル**の
考え方がベースとなっています。

組織の特性を踏まえた**計画(Plan)**を立案し、
計画に基づくルール・対策を**実行(Do)**し、
上記の有用性や結果を**点検(Check)**し、
情報セキュリティ体制の**改善(Act)**を図り、
それを翌年の**計画(Plan)**立案に繋げる…

ある対策を実施して終わりではなく、**継続的に運用できる仕組み**を
構築することが、情報セキュリティの本質的な強化に繋がります。

ISMS/Pマーク認証取得までのプロセス

ISMS取得スケジュール　※プロジェクトの流れ

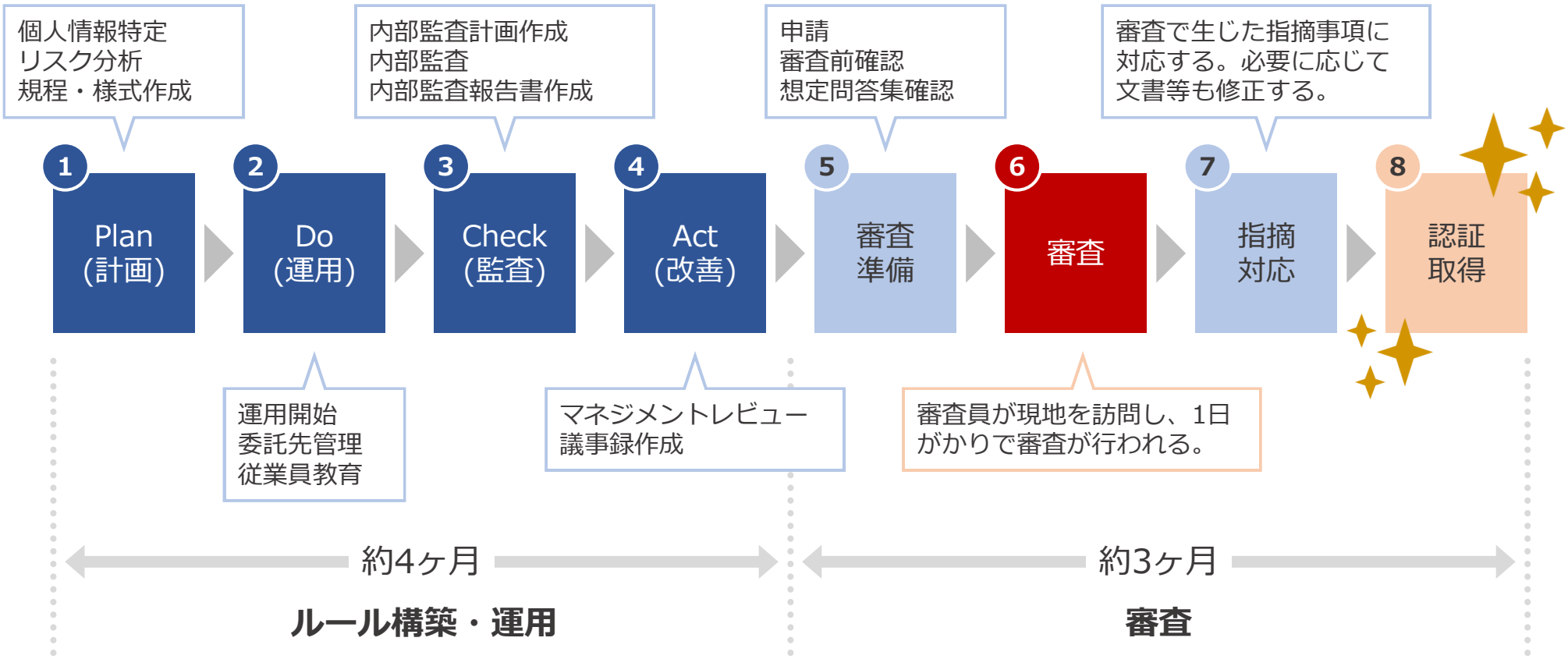


※上記スケジュールはあくまで一例です。組織の規模感や難易度により変動します。

ISMS取得スケジュール　※タイムライン

分類	1ヶ月目			2ヶ月目			3ヶ月目			4ヶ月目			5ヶ月目			6ヶ月目		
	上旬	中旬	下旬	上旬	中旬	下旬	上旬	中旬	下旬	上旬	中旬	下旬	上旬	中旬	下旬	上旬	中旬	下旬
キックオフ																		
情報資産洗い出し																		
リスク分析																		
委託先管理																		
文書・様式類作成																		
従業員教育																		
内部監査																		
マネジメントレビュー																		
第一段階審査																		
第二段階審査																		
指摘事項対応																		
ISMS認証取得																		

Pマーク取得スケジュール　※プロジェクトの流れ



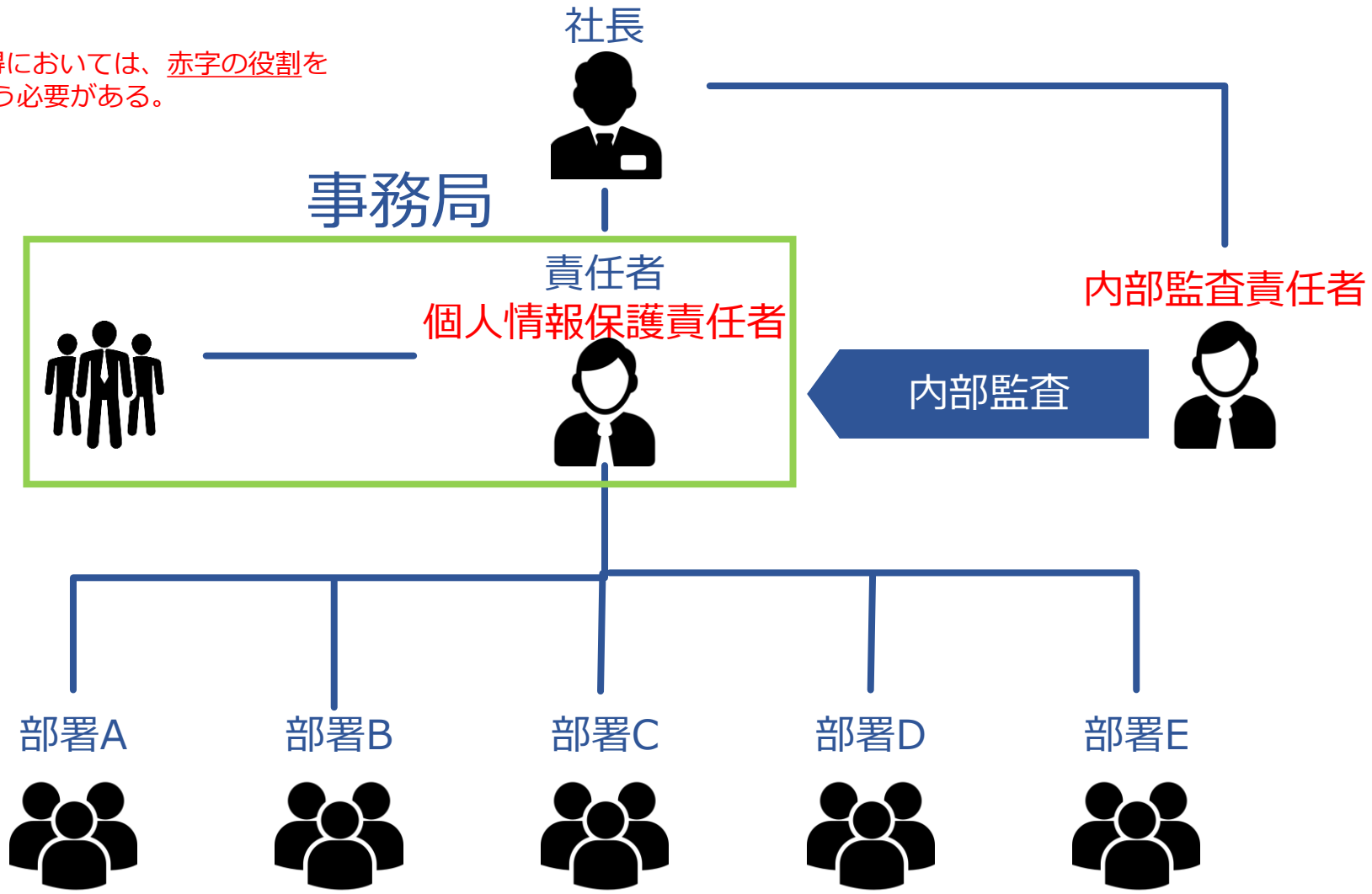
※上記スケジュールはあくまで一例です。組織の規模感や難易度により変動します。

Pマーク取得スケジュール　※タイムライン

分類	1ヶ月目			2ヶ月目			3ヶ月目			4ヶ月目			5ヶ月目			6ヶ月目			7ヶ月目		
	上旬	中旬	下旬	上旬	中旬	下旬	上旬	中旬	下旬	上旬	中旬	下旬	上旬	中旬	下旬	上旬	中旬	下旬	上旬	中旬	下旬
キックオフ																					
個人情報洗い出し																					
リスク分析																					
委託先管理																					
文書・様式類作成																					
従業員教育																					
運用確認																					
内部監査																					
マネジメントレビュー																					
申請																					
文書審査																					
現地審査																					
指摘事項対応																					
Pマーク認証取得																					

社内の体制　※あくまで一例

※Pマーク取得においては、赤字の役割を
別々の方が担う必要がある。



必須の費用

- ✓ 審査料金のみ(認証マーク利用料含む)！
  それ以外は、必須ではありません

とは言え、例えば1拠点30名ほどの場合・・・

- ✓ 審査費用：70万円～110万円
- ✓ コンサルティング料金： 85万円～90万円
- ✓ 設備投資：
  - ✓ リスク分析の結果によって変動する可能性あり
  - ✓ とは言え、大規模な投資が必要になることは少ない

ISMS認証取得、維持に必要な費用　※審査イメージ

ケース 1

事業：クラウドサービス
拠点：1拠点(東京都港区)
人数：5名

審査	金額
初回審査	790,000円
継続審査 (1年目)	290,000円
継続審査 (2年目)	290,000円
再認証審査 (3年目)	525,000円

ケース 2

事業：システム開発
拠点：1拠点(東京都千代田区)
人数：30名

審査	金額
初回審査	945,000円
継続審査 (1年目)	365,000円
継続審査 (2年目)	365,000円
再認証審査 (3年目)	675,000円

ケース 3

事業：携帯電話販売
拠点：8拠点(東京都渋谷区)
人数：270名

審査	金額
初回審査	2,060,000円
継続審査 (1年目)	955,000円
継続審査 (2年目)	955,000円
再認証審査 (3年目)	1,490,000円

必須の費用

- ✓ 申請～付与登録料のみ！
  それ以外は、必須ではありません

とは言え、例えば30名ほどの場合・・・

- ✓ 新規取得時の審査に関わる費用
  - ✓ 申請料：約5万円
  - ✓ 審査料：約47万円
  - ✓ 付与登録料：約10万円
- ✓ コンサルティング料金： 60万円～70万円
- ✓ 設備投資：
  - ✓ リスク分析の結果によって変動する可能性あり
  - ✓ とは言え、大規模な投資が必要になることは少ない

Pマーク認証取得、維持に必要な費用　※審査イメージ

必須の費用

※消費税10%込

種別	新規			更新		
事業者規模	小	中	大	小	中	大
申請料	52,382	52,382	52,382	52,382	52,382	52,382
審査料	209,524	471,429	995,238	125,714	314,286	680,952
マーク使用料	52,382	104,762	209,524	52,382	104,762	209,524
計	**314,288**	**628,573**	**1,257,144**	**230,478**	**471,430**	**942,858**

事業者規模

業種分類	資本金の額　又は出資の総額 従業員数	小規模	中規模	大規模
製造業・その他	資本金の額 又は 出資の総額 従業者数	2～20人	3億円以下 又は 21～300人	3億円超　かつ 301人～
卸売業	資本金の額 又は 出資の総額 従業者数	2～5人	1億円以下 又は 6～100人	1億円超　かつ 101人～
小売業	資本金の額 又は 出資の総額 従業者数	2～5人	5千万円以下 又は 6～50人	5千万円超　かつ 51人～
サービス業	資本金の額 又は 出資の総額 従業者数	2～5人	5千万円以下 又は 6～100人	5千万円超　かつ 101人～

ISMSとPマークの比較

ISMS・Pマークの取得は、次のような項目や、自社で力を入れたいポイント、外部からの要請を踏まえ検討を行いましょう。

自社にあったセキュリティ体制の構築

セキュリティに関する検討項目において、「実施しなければならない」ことが明確なPマークに比べ、 ISMSの場合は「どのような対策を実施するか」を自社の実態に合わせ判断することができることからより自社にあったセキュリティ体制を構築することが可能です。

費用面

ISMS審査は毎年、Pマーク審査は隔年の実施になります。また、ISMSは企業規模により審査費用が従量的に変動しますので、審査においてのランニングコストはPマークの方がコンパクトになります。

知名度

ISMSに比べてPマークの方が取得企業が多く、一般的な知名度はPマークの方が上です。従って、たとえばBtoCの企業や、町の中小企業を相手取る士業事務所などは、Pマークを選ばれるケースが多いです。

システム面におけるセキュリティ強化

ISMSを構築するにあたり検討が必要な項目では、システムの取得、開発や保守に関する項目があり、システム・IT面における実質的なセキュリティレベルの向上が期待できます。自社システムの開発を行っている企業はISMSを優先し選ばれるケースが多いです。

税理士法人ネイチャー国際資産税様

- **取得した認証**
  ISMS認証

- **お取り組みの期間**
  約1年間（月1回の打ち合わせ）

- **ISMS認証取得の目的**
  情報セキュリティ事故などのリスクに対する備えとして、社内の仕組みを改善するため

- **ISMSを取得したことによる成果**
  ①情報セキュリティマネジメントシステム構築
  マニュアルの他、ネットワーク図や資産管理台帳などを作成したことで、セキュリティ体制やネットワーク環境などを管理する仕組が構築できました。
  ②従業員教育の基盤構成
  セキュリティマニュアルは、情報セキュリティについて体系的に教育する材料にもなっています。周知徹底の抜け漏れを低減することが可能となりました。

LRM株式会社紹介

LRM株式会社の強み (1) 使いやすい文書体系

LRM株式会社では、効率性、合理性を重視するベンチャー企業やIT企業の支援実績をもとに、シンプルな文書フォーマットを構築しました。

いたずらにドキュメント量を増やし、結果として運用工数を肥大化させるのではなく、まずは必要十分な文書体系を構築し、その後に適宜見直すことを推奨します。

他コンサルティング会社の場合(例)

LRM株式会社のフォーマットの場合(例)

LRM株式会社の強み (2) 多数の専属コンサルタント

コンサルタントの大部分は、弊社専属のコンサルタントです。正規雇用のメンバーで、常に社内での情報交換や相互連携、切磋琢磨に励んでいます。

また、数名のパートナーコンサルタントは、専属コンサルタントと同質のサービスを提供しつつ、より高度な専門的見地からご支援を行います。


幸松 哲也


高橋 昌志


三崎 悠之亮


小池 寿宜


金子 裕人


山岸 七海


川島 達也


松原 敬之


宮崎 俊一


松岡 哲郎


二宮 良介


石濱 雄基


柴田 大輔

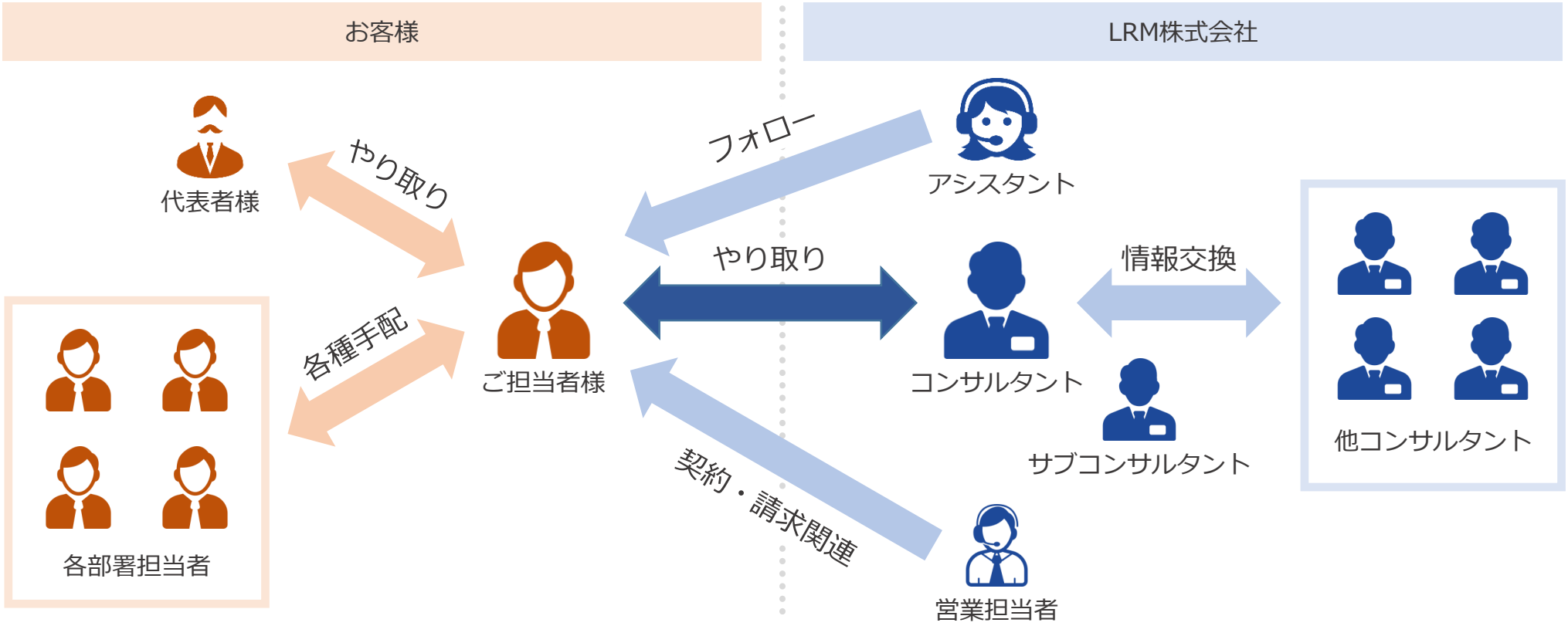

小池 竜平


村田 一彦


吉村 健

LRM株式会社の強み (3) 安心のチームコンサルティング

弊社は、コンサルティング提供の際、複数ポジションの人間がご支援に関わります。
チームでのコンサルティングを実現することで、お客様対応のスピード＆品質を向上させつつ、かつ、担当者を体調不良等をはじめとする属人的な理由でプロジェクトが停滞することを防ぎます。



取引実績

WANTEDLY ウォンテッドリー株式会社	明日のグレートカンパニーを創る Funai Soken 株式会社船井総合研究所	ほけんの窓口 ほけんの窓口グループ株式会社
chatwork ChatWork株式会社	accenture アクセンチュア株式会社	弁護士ドットコム 弁護士ドットコム株式会社
KAGOYA カゴヤ・ジャパン株式会社	OBC 株式会社OBC	光通信 株式会社光通信
ぴあ ぴあ株式会社	Gunosy 株式会社Gunosy	三菱商事 三菱商事株式会社
SoftBank Technology ソフトバンクテクノロジー株式会社	WORKS APPLICATIONS 株式会社ワークスアプリケーションズ	JTE ジェイティ エンジニアリング株式会社
AOI Pro. 株式会社AOI Pro.	nulab 株式会社ヌーラボ	QUALITIA 株式会社クオリティア
Atrae 株式会社アトラエ	studist 株式会社スタディスト	
エン・ジャパン エン・ジャパン株式会社	日テレITプロデュース NIPPON TV IT PRODUCE 株式会社日テレITプロデュース	株式会社リアルワールド REALWORLD 株式会社リアルワールド

一部・順不同・敬称略

Security Diet

LRM株式会社