

ITベンダにおける 個人情報保護の取組例

2011年1月11日
株式会社日本総合研究所
法務部長 大谷和子

1. 会社概要

事業内容	システムインテグレーション、ネットワークインテグレーション、先端情報技術開発、経済調査・研究・政策提言、事業・経営戦略研究等
創立年月日	昭和44年2月20日
資本金	100億円
主要株主	(株)三井住友フィナンシャルグループ(100%)
従業員数	2,000名(平成22年3月)

【参考】 事業に関する各種登録(情報セキュリティ関係抜粋)

情報セキュリティマネジメントシステム登録 (ISO/IEC 27001:2005/JIS Q27001:2006)	登録番号:JQA-IM0037 適用範囲: 鰻谷センター及び西九条センターにおける クレジットの特定先の処理・通信業務の受託運用
システムサービス企業(システムインテグレーター)登録	登録番号:経済産業省(関)20110155号
特定システムオペレーション企業等認定	認定番号:経済産業省(関)18310019号
プライバシーマーク使用許諾事業者認定	許諾番号:11820002(07)号

その他、システム監査企業台帳登録、情報セキュリティ監査企業台帳登録等

2. 個人情報の取扱いに関する業務の概要

	個人情報を取扱う業務	個人情報の種類(氏名,住所,電話番号など)
1	調査研究 コンサルティング	アンケート (氏名・住所・電話番号・会社名・部署名・e-mailアドレス等)
2	出版物の発行	申込書 (氏名・住所・電話番号・会社名・部署名・e-mailアドレス等)
3	セミナー シンポジウム 講演会	申込者の個人情報・講師の個人情報 (氏名・住所・電話番号・会社名・部署名・e-mailアドレス等)
4	人事・委託先管理	従業員の個人情報、委託先の個人情報 (氏名・住所・生年月日・電話番号・家族の氏名・業務経歴・会社名・ 部署名・e-mailアドレス等)
5	採用情報	応募者の個人情報 (氏名・住所・電話番号・生年月日・業務経歴・e-mailアドレス等)
6	SI関連サービス 情報処理業務の受託	受託に伴う情報 (氏名・住所・生年月日・口座番号・カード番号・電話番号・e-mailアド レス等)

その他インハウス情報の取扱いがある。

3. 受託業務に伴う個人データ等の取扱い

日本総研
The Japan Research Institute, Limited

サービス紹介 | 経営コラム・レポート | 経済・政策レポート | セミナー・イベント | 研究員紹介 | 採用情報 | **会社情報** | お問い合わせ

ホーム > 会社情報 > 事業内容 > システム開発部門 > Gomezクレジットカードランキングで1位を獲得する三井住友VISAカード様のカード会員専用サイトを構築

会社情報

事例紹介

Gomezクレジットカードランキングで1位を獲得する三井住友VISAカード様のカード会員専用サイトを構築

カードシステム事業本部

クレジットカードの会員向けサービスをインターネット上で24時間、365日提供できるように、三井住友VISAカード、三井住友マスターカードの会員向けサービスサイト、「Vpass」の構築を行っている。「Vpass」の立ち上げ当初から開発に携わっている開発第二グループのマネジャー、田川氏は、次のように話す。

「従来のカード会員向けのサービス受付は支店、サービスセンターや電話対応が主で、カード紛失などの緊急対応を除くと平日の9時から17時までと限られた時間でしかサービス提供できていませんでした。そこで、24時間・365日サービス提供ができる「インターネット支店」を作れないか、というのが当初の発想でした。元々当社は、V-Mailという三井住友カードのインターネット・ショッピングモールの実証実験に携わっていたのですが、そのときのノウハウを元に、この「Vpass」の開発に取り組んだのです。」

最初のサービスがスタートしたのは1999年8月。まだインターネット上での商用サービスがスタートして間不长、一般ユーザーのインターネット環境もダイヤルアップが中心で、ブロードバンド化も進んでいないころのため、セキュリティ面や接続の安定性なども考慮しつつ、まずは機能などを限定したスモールスタートを切った。

日本総研
The Japan Research Institute, Limited

サービス紹介 | 経営コラム・レポート | 経済・政策レポート | セミナー・イベント | 研究員紹介 | 採用情報 | 会社情報 | お問い合わせ

ホーム > サービス紹介 > 事業内容 > 人事・経理・人材開発 > 人事評価制度

人事評価制度

人材マネジメント・ツールとしての人事評価制度

人事評価制度は、社員各人の能力・貢献度と、処遇の適正バランスを維持するための指標を特定する、非常に重要な機能です。しかも、その機能のみを重視した制度では不十分です。人事評価制度には、社員各人の職務遂行状況を点検し、さらなる人材力アップに資する情報を企業と個人に提供する機能、そして企業が社員に対して期待する行動メッセージを伝達する、人材マネジメント・ツールとしての機能が求められるからです。

人事評価制度の[設計・改定]にあたって、以上の共通認識を持ちつつ、各企業の事業形態や人員構成、そして、組織風土等により調整された、運用しやすい仕組みを提案します。

主要サービス

職務調査システム

人事評価の基準として通常、(1)年度計画に基づく重点課題(目標管理シートに記載)、(2)日常コア業務、(3)上司指示事項の3つが挙げられます。このうち(1)と(3)は明確ですが、(2)に関しては等級別の職務要件書を作成しないと明確になりません。このプロセスを省くと等級別コア業務が特定できず、管理職および上位等級の者が下位等級の仕事ばかりやっているという事態が多くの会社で発生しています。当該職務調査システムは、等級別のコア業務および通常業務を洗い出し等級別に分類するとともに、業務遂行に必要な能力も明確にするシステムです。このシステムでは、業務を洗い出した後、分類法という方法で行った職務区分が簡単に可視化できるとともに、能力の記述方法も標準化しているため容易に入力するという利点を備えています。

→ 職務調査の詳細説明(PDF155.4KB)

チーム業績評価と360度評価

研究開発部門、病院、学校など、一般的な評価制度・手法がなじみにくい専門職チームの評価には「チーム業績評価+360°評価」の仕組みが最適です。個人主義的風土を「組織業績志向」に変革する上でも効果があります。

4. 個人情報保護及び情報セキュリティへの取組

(1) 対外ホームページにおける「個人情報保護方針」等の公表

個人情報保護法に基づく公表事項

株式会社日本総合研究所
個人情報保護管理者
常務執行役員 下福葉耕治

弊社は、個人情報の保護に関する法律(平成15年法律第57号、「個人情報保護法」といいます。)に基づき、以下のとおり公表します。

1. 利用目的

弊社は、次の利用目的で社外の方の個人情報を取り扱います。これらの利用目的を変更する場合は、ご本人に通知又は弊社ホームページに公表します。

類型	利用目的
(1) システム・インテグレーション業務、ソフトウェア開発業務、関連サービスの実施に際して、個人情報等の委託を受ける場合の個人情報	金融等の分野におけるシステム・インテグレーション業務、ソフトウェア開発業務、情報システムのアウトソーシングサービス、情報システムのアプリケーション・サービス・プロバイダ業務、データ・センター業務、情報処理サービス及びこれらに付随するデータの出入力、プリント業務、データ伝送等のサービスを業として行うために委託された情報について、委託者である企業、国、地方自治体、独立行政法人その他各種法人、各種官利非官利の団体等との委託契約に定める義務を履行するため 例えば、委託者がクレジットカード会社の場合、弊社の提供するカードシステムに伝送されたクレジットカード会員のカード利用に関するデータを弊社のコンピュータで処理し、カード会員に送られる計算書も出力する業務の一部で個人情報を取り扱うことがあります。 また、アウトソーシングサービスの一部でヘルプデスクサービスを実施する場合、問い合わせを防止し、委託者からのお問い合わせを正確に認識するための、ヘルプデスクへのお問い合わせ等の通話を録音することがあります。
(2) 調査研究、コンサルティングの業務に際して、個人情報等の委託を受ける場合の個人情報	政策提言、経営戦略、人材育成、事業開発・再構築、マーケティング、制度改定等の調査研究、コンサルティングを業として行うために委託された情報について、委託者である企業、国、地方自治体、独立行政法人その他各種法人、各種官利非官利の団体等との委託契約に定める義務を履行するため 例えば、委託者が電子商取引のビジネスを新規に行おうとする企業の場合、当該企業が実施した電子商取引に関する消費者アンケート結果を分析し、消費者のニーズを検討したうえで委託者の計画に提言を行う業務の一部でアンケート回答者の個人情報を取り扱うことがあります。
(3) 当社の提供するソフトウェア、書籍、サービス等の申込者・利用者に関する個人情報	当社が開発又は販売するソフトウェア、書籍又はサービスに申込み、又はこれを購入しあるいは契約されたお客様について、商品の発送、関連するアフターサービス、商品のアップデート、新バージョン、サービスの内容変更又は廃止等のお知らせを行い、あわせてお客様からのお問い合わせ等に対応するため 例えば、弊社のパッケージソフトウェアを購入されたお客様にバージョンアップの

(2) 個人情報取得のWeb画面例

日本総研
The Japan Research Institute, Limited

お申し込みの流れ

- 【1】個人情報保護方針の同意
- 【2】お申し込み内容の入力
- 【3】入力内容の確認
- 【4】お申し込み完了

WEBからのお申し込み
セミナー・イベント参加お申し込み

お申し込み内容

セミナー情報

セミナー名	【会員登録】クレジットカード公金収納フォーラム
日時	2011年03月31日(木)00:00~00:00 <small>※ご希望の日程を選択してください。</small>
場所	-
講師	-
参加費	-
定員	-

お申し込み者の情報

お名前	ORIS山田太郎
-----	----------

日本総研 CAREER GATE
JRI RECRUITING INFORMATION 2011

「知」磨く。
— 共に響きあう強い個人の集団へ —

（株）日本総合研究所（日本総研）における個人情報の取扱いについて

- 個人情報の取扱方針
日本総研はプライバシーマークの付与・認定を受けております。会員の個人情報は日本総研が定める「個人情報保護方針」に準じ、適切な保護措置を講じ、厳重に管理いたします。
- 個人情報の利用目的
ご登録いただきました個人情報は以下の目的のために利用させていただきます。下記以外の目的で個人情報を利用する場合は、改めて目的をお知らせし、同意を得るものといたします。
 - 採用関連情報の提供
 - 採用選考活動
 - 社員としてお迎えするための必要書類
 - インターンシップ等のイベントの実施
- 個人情報取り扱いの委託の予定
CAREER GATEの運営の一部を社外に委託するために、株式会社ワークス・ジャパン、日本データビジョン株式会社にご登録頂きました個人情報の取扱いを委託します。尚、株式会社ワークス・ジャパン、日本データビジョン株式会社とは、秘密保持契約を締結し、個人情報については厳重に管理いたします。
- 個人情報をご提供することの任意性及び当該情報を入手なかった場合に会員に生じる結果について
エントリーに際し、必須となっている項目については正確にご記入ください。虚に誤り・漏れ等があった場合には、採用選考において不利益を被る可能性がございます。
- 開示・訂正・利用停止等の申し立て先及び個人情報の取扱いに関する苦情、ご相談の受付窓口
(ご本人様よりお申し立てがあったときは遅滞なく開示・訂正・利用停止等の措置をとります。詳しくは日本総研の「個人情報保護法に基づく公表事項」4をご覧ください。)

1. 本登録における個人情報取扱責任者:
社長室(人事) 森 正樹

2. 苦情・相談窓口:
社長室(人事) 朝倉採用担当
電話: 03-3288-4731 FAX: 03-3288-4717
E-mail: recruit@jri.co.jp

3. 「個人情報保護法に基づく公表事項」:
<http://www.jri.co.jp/privacy/3nhp.html>をご覧ください。

同意する 同意しない

Copyright © 2007-2011 The Japan Research Institute, Ltd.

(3) 安全管理措置(組織的・物理的・技術的)

各種規定の整備

- ◆ 情報管理規則、情報・文書管理要領 他(セキュリティ・オフィサーの設置)
- ◆ 個人情報保護コンプライアンス・プログラム・個人情報取扱要領、個人情報取扱手続
- ◆ 外部委託先情報管理要領
- ◆ 受託システム開発・運用規則 他

ビル入退館管理の実施・防犯カメラ・一部建物の場所の秘匿

ICカードによる執務室への入退室管理の実施

OA環境へのアクセス認証をICカード認証に限定

自宅パソコンにおける電子文書取扱状況の点検(年1回以上)

- ◆ 対象者 全役員・従業員・派遣スタッフ
- ◆ 点検項目
 - ◆ 自宅パソコンへの「ファイル交換ソフト」のインストール有無
 - ◆ 自宅パソコン内への持帰った業務に係る情報の保存の有無

個人情報の外部持ち出しに対する対策(システムの対応)

- ◆ メール査閲、Webメールへの接続防止、パスワードのない添付ファイルの送信防止
- ◆ ツールを用いた可搬性記憶媒体への書込みの制限

ウィルス対策ツールの自動更新、パッチ等自動配信

ソフト検疫(脆弱性対応未対応PC・ウィルス定義ファイルの更新未対応)

各種アクセスログの記録・保存・点検

ファイアウォールその他の具体的セキュリティは社外秘

(4) 従業者の監督

社内規定・ルールの再徹底に注意喚起(年1回)

- ◆ 機密情報の持ち出し・持ち帰りに関するルールの徹底
- ◆ 情報漏洩防止のためのチェック体制の徹底
- ◆ 緊急時(情報漏洩の発生等)の報告体制の徹底

誓約書の提出(年1回)

- ◆ 対象者 全役員・従業員・派遣スタッフ・委託先要員

(5) 委託先の監督

「パートナー登録カード」新規先の場合は委託先選定の基礎資料・既存先の場合は定期的更新(年1回)による個人情報保護水準の確認
委託先に対するモニタリングの実施(年1回)・一定の基準で抽出した委託先への実査有

情報管理に関する覚書等、個人情報保護水準を担保するために必要な契約を締結

業務単位での情報管理状況報告書(年2回)の確認



(6) 教育

新人研修(毎年4月)・キャリア採用者研修(随時)の実施

個人情報保護理解度確認調査の実施(毎年1回)

- ◆ eラーニング形式で全役員・従業員・派遣スタッフに漏れなく実施
- ◆ 基準点(90点)未達の場合、再解答が必要。
- ◆ 解答結果を人材育成担当者にフィードバックし、部室単位でのフォローアップ研修の実施

「情報管理の手引き」の配布

セキュリティ・オフィサー向け研修の実施

(7) 自主点検と監査

自主点検(年2回以上)・定期的(年1回)の全部門を対象とする監査

(8) 個人情報保護マネジメントシステム(PMS)の運営による定期的見直し

リスク分析結果、監査結果、内外の苦情等によるスパイラスアップ
マネジメントレビュー



5. ISMSの認定

内容

- ◆ 情報セキュリティマネジメントシステムの維持・向上・強化
- ◆ 「センターセキュリティに関する基本方針書」等のISMS文書の制改定

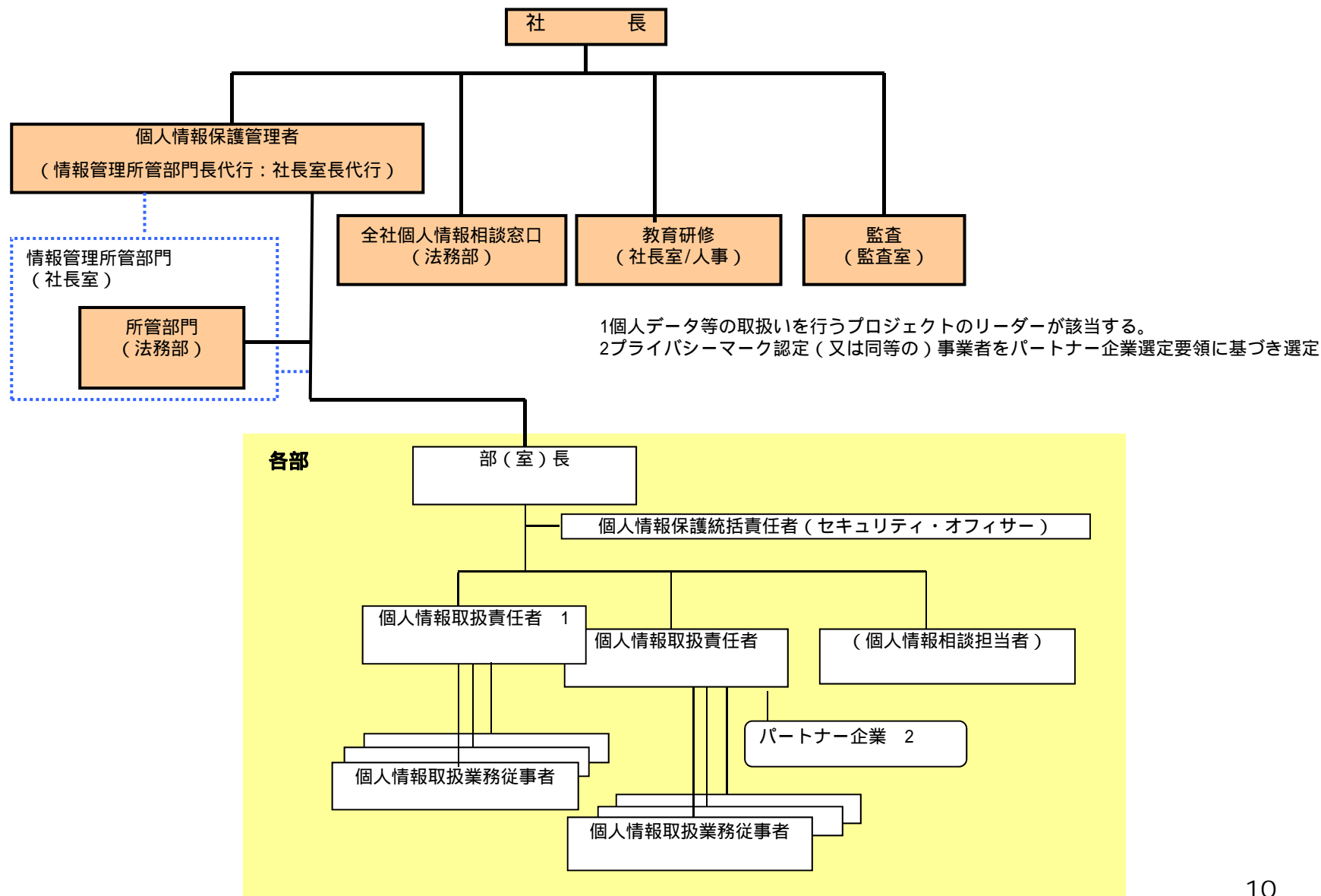
適用範囲

- ◆ 鰻谷センター(鰻谷)(4階の南側事務室、6階の電算室)
- ◆ 西九条センター(西九条)(5階の事務室、デリバリ室及び配送センター、7階の電算室)
- ◆ 大阪本社(土佐堀)(16階 南西区画の事務室)

対象情報資産

上記適用範囲におけるセンター運営及びアウトソーシングサービス遂行上で保護すべきすべての情報資産(情報・データ、設備・機器、ソフトウェア、人員)を対象とする。

6. 個人情報保護マネジメントシステム(PMS)運営体制



7. PMSを担う部室の責任者

■ セキュリティ・オフィサー

- 各部門内での運用ルールの制定、部員への意識付け
 - 体制整備、規定の運用、方針の周知徹底
- 各種「個人情報取扱伺」等の記載事項のチェック
 - 通知必要事項の内容確認
- 「個人情報管理台帳」、「個人情報取扱伺」等の取扱状況監視
 - 個人情報保存・廃棄の定期的なトレース
- 収集情報、顧客からの提供データ取扱への意識改革
- セキュリティ管理の徹底
 - 情報の盗用、消失、改ざんの防止、アクセス権の付与、施錠可能なキャビネへの保管等の指導

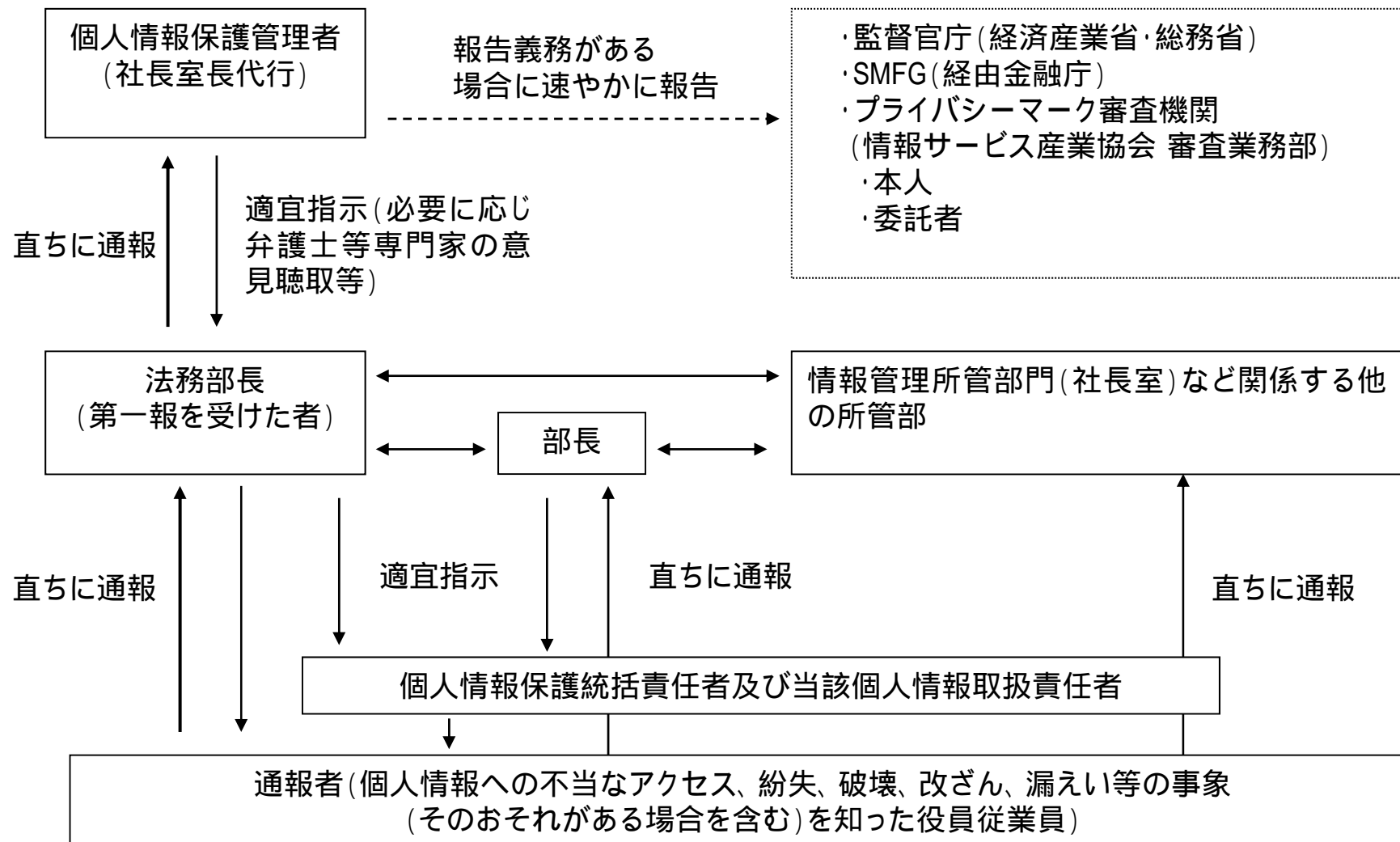
■ 個人情報取扱責任者(各プロジェクトにおける個人情報の取扱責任者)

- 個人情報の取得・入力、移送・送信、利用・加工、保管、消去・廃棄の各段階においてルールを遵守して業務を遂行
- 個人情報取扱業務従事者に対するアクセス権限の付与及び監督

■ 個人情報取扱業務従事者(個人情報を取り扱う従業者)

- 個人情報取扱責任者の指示のもと個人情報の取得・入力、移送・送信、利用・加工、保管、消去・廃棄の各段階において与えられた権限の範囲内で業務を遂行する

8. 緊急時対応



9. 定期的見直し

見直しのトリガー	対応要否
監査報告	要
リスク調査及び対策実施状況	要
個人情報取扱いに関する法令諸規則の改廃状況	要
社会情勢、国民の認識、技術の進歩など諸環境の変化	要
定期点検の結果	要
事故後の事後対応の結果	不要
前回までの見直しの結果に対するフォローアップ	不要
教育研修の実施結果	不要
苦情その他外部からの意見	該当なし
当社及び子会社の事業領域の変化	該当なし
当社のリスク所管部室その他事業者の内外から寄せられた改善のための提案	該当なし
規定外事項	該当なし

【法令諸規則の改廃動向】

事業承継の場合に個人情報の保護のために必要な契約を締結する旨PCP4.2.8に反映

施行日	法令諸規則等	対応要否	その理由
2008/5/1	個人情報の保護に関する法律施行令の改正	不要	個人情報取扱事業者の範囲の限定に関する事項が追加されたが当社の位置づけに変更はない
2008/4/25	個人情報の保護に関する基本方針の改定	不要	個人情報取扱事業者等が講ずべき個人情報の保護のための措置に関する基本的な事項への追加。各種ガイドライン(下記経産省、金融庁ガイドライン)に相次いで反映済み
2009/9/1	個人情報の保護に関する基本方針の改定	不要	消費者庁新設に伴う軽微改定
2009/10/9	個人情報の保護に関する法律についての経済産業分野を対象とするガイドラインの改定	要	・第三者提供に該当しない事業承継の場合の注意事項の追加(4.2.8へ) ・「個人情報の取得元又はその取得方法(取得源の種類等)の具体的明記」については今後の検討課題へ
2009/11/20	金融分野における個人情報保護に関するガイドラインの改定	今後	「個人情報の取得元又はその取得方法(取得源の種類等)の具体的明記」については今後の検討課題へ
2009/12/1	割賦販売法改正法(2008/6/1公布)	不要	クレジットカード番号等の適切な管理に関する章(第3章の4)が新規追加。当該規定は、直接には、当社から見て委託元であるクレジット事業者に課せられているため、当社としては社会情勢の変化として認識するにとどめる。

【社会情勢の変化】

更に巧妙化をとげるウィルス、不正アクセス等への対応について、引き続き、技術動向等の注視

社会情勢、技術の進歩等の変化	当社の対応
1. 二次被害を伴う個人情報流出事件の多発 ・証券会社の元管理職員によるユーザIDの窃用事案(約149万件の漏えい) ・クレジットカード会社の流出事件(委託先の原因)では5000件を超える不正利用との報道	・書出し制御システムにより特権ユーザからの申請でも書出しは防止可能 ・開発と運用の分離により委託先における個人情報の取扱いは基本的にない
2. USBメモリなど外部メディアやPDFファイルを通じた感染等 コンピュータウィルスの感染ルートの拡大 (IPA情報セキュリティ白書2009)	・ウィルス対策ソフトの強化 ・ソフト検疫システムの導入により対応可
3. Gumblerによるホームページ改ざん等による個人情報の取得	・CMSの導入によりFTP経由での改ざんは防止可
4. 割賦販売法の改正等 クレジットカード番号の管理がクレジット事業者等の義務へ。 万一の事故によるレピュテーションリスクは極めて大きい。	・クレジットカード会社からの要請が高まる可能性

10. 第三者による検証等

- ◆ 金融庁「金融コングロマリット監督指針」(平成21年)等に基づくリスク管理・顧客保護の観点からの株主のグループ会社統一基準に基づく社内諸制度のモニタリング(年2回)
- ◆ プライバシーマーク使用許諾事業者認定の更新に伴うJISQ15001:2006に基づく審査
- ◆ 日本総研グループ各社の個人情報保護体制強化の支援
- ◆ 弊社自らの情報発信・コンサルティング

以上

本資料は発表者の見解の私的な整理であり、所属機関を代表する意見・表明等ではありません。