第５回情報セキュリティ格付けセミナー

第三者証明書発行サービスに関する最新動向

株式会社アイ・エス・レーティング

2017年7月7日

鈴木　茂幸

当資料に記載の内容は予告なく変更することが御座いますので、予めご了承願います。

第三者証明書発行サービスとは

〇企業が様々な製品やサービスを提供するにあたり、消費者や取引先から提供上のプロセスの正当性や適切性等について説明を求められることがあります。その場合、内部調査、内部監査等により応えることもできますが、外部から見たときには利害関係上同一であると見なされてしまうことがあり、必ずしもベストの方法とは言えません。

〇アイ・エス・レーティングでは、利害関係のない中立な第三者の評価機関として、専門的かつ客観的な立場 から、プロセスの内容や質、事業者の経営や企業統治の状況を確認し、その正当性・適切性について証明書を発行する「第三者証明書発行サービス」を提供しています。

〇貴社と貴社の製品やサービスの信頼性の向上を「第三者証明書発行サービス」によりご支援致します。

なぜアイ・エス・レーティングなのか

〇アイ・エス・レーティングでは、「情報セキュリティ格付けサービス」・「第三者証明書発行サービス」を提供しています。
利害関係のない中立な第三者の評価機関として、専門的かつ客観的な立場 から、プロセスの内容や質、事業者の経営や企業統治の状況を確認し、その正当性・適切性について証明書を発行することが可能です。

アイ・エス・レーティングは、第三者による客観的な評価を行う機関として、次のようなメリットを保持しています。

■公正、中立の格付機関
格付機関として設立されているため、株主が格付審査に影響力を行使できないように1社・1企業グループの出資比率を20%以下に抑えるなど、公正性、中立性が高い機関。

■格付機関としてのノウハウ
格付機関として、様々な格付を実施してきた中で、製品やサービスの提供プロセスの正当性・適切性を判断するノウハウが確立。

■お客様の目的にあわせて証明項目をカスタマイズ
お客様の業種、取引先等の事情により、第三者証明したい内容が異なることに対応し、事前に打ち合わせにより、証明項目をカスタマイズ。

安全管理措置の点検、委託先の監督責任

番号法、改正個人情報保護法により個人情報管理の安全管理措置が義務づけられています。
また、業務委託に対して、事前の安全管理措置の確認や安全管理措置の状況確認の必要性（番号法では必須作業）が課せられています。さらに、「サイバーセキュリティ経営ガイドライン」（経済産業省）では、経営の3原則として

（1）経営者は、IT活用を推進する中で、サイバーセキュリティリスクを認識し、リーダシップによって対策を進めることが必要
（2）自社は勿論のこと、系列企業やサプライチェーンのビジネスパートナー、ITシステム管理の委託先を含めたセキュリティ対策が必要
（3）平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策、対応に係わる情報の開示など、関係者との適切なコミュニケーションが必要

経営者は、3原則を認識し、対策を進めることが重要であると規定されています。

■自社の安全管理措置の確認はどうしてますか？
■委託先の安全管理措置の確認はどうしてますか？
■委託先を含めたセキュリティ対策の状況確認はどうしてますか？

実効性のある委託先の監査、コスト削減を
第三者証明書発行サービスで実現します。

特定個人情報（マイナンバー）の安全管理措置

■基本方針の策定

事業者の名称
関係法令・ガイドライン等の遵守
安全管理措置に関する事項
質問及び苦情処理の窓口など

■取扱い規定の策定

取得の段階の安全管理措置
利用する段階の安全管理措置
保存する段階の安全管理措置
提供行う段階の安全管理措置
削除・廃棄を行う段階の安全管理措置

■組織的安全管理措置

組織体制の整備
取扱規定等に基づく運用
取扱状況を確認する手段の整備
情報漏えい等事案に対する体制の整備
取扱い状況の把握及び安全管理措置の見直し

■人的安全管理措置

取扱担当者の監督
事務取扱担当者の教育

■物理的安全管理措置

特定個人情報を取扱う区域の管理
機器及び電子媒体等の盗難防止
電子媒体等を持ち出す場合の漏えい等の防止
個人番号の削除、機器及び電子媒体等の廃棄

■技術的安全管理措置

アクセス制御
アクセス者の識別と認証
外部からの不正アクセス等の防止
情報漏えい等の防止

特定個人情報の安全管理措置（委託先の監督）

委託先の監督

委託先の適切な選定

委託先に安全管理措置を遵守させるために必要な契約

委託先における特定個人情報の取扱い状況の把握

■必要かつ適切な監督

委託先において、番号法に基づき委託者自らが果たすべき安全管理措置と同等の措置が講じられるよう必要かつ適切な監督を行わなければならない。

■契約内容

秘密保持契約
事業者内からの特定個人情報持出し禁止
特定個人情報の目的が利用の禁止
再委託における条件
漏えい事案等が発生した場合の再委託先の責任
委託契約終了後の特定個人情報の返却または廃棄
従業者に対する監督・教育
契約内容の遵守状況についての報告を求める規定など
特定個人情報を取扱う従業者の明確化
委託者が委託先に対して実地の調査を行うことができる規定

個人情報保護法改正のポイント

1. 個人情報保護委員会の新設

個人情報取扱事業者に対する監督権限を各分野の主務大臣から委員会に一元化。

2. 個人情報の定義の明確化

①利活用に資するグレーゾーン解消のため個人情報の定義を身体的特徴等が対象になる事を明確化。

②要配慮個人情報（本人の人種、信条、病歴など本人に対する不当な差別又は偏見が生じる可能性のある個人情報）の取得については、原則として本人同意を得ることを義務化。

3. 個人情報の有用性を確保（利活用）するための整備

匿名加工情報（特定の個人を識別することができないように個人情報を加工した情報）の利活用の規定を新設。

4. いわゆる名簿屋対策

①個人データの第三者提供に係わる確認記録作成等を義務化。（第三者から個人データの提供を受ける際、提供者の氏名、個人データの取得経緯を確認した上、その内容の記録を作成し、一定期間保存することを義務付け、第三者に個人データを提供した際も、提供年月日や提供先の氏名等の記録を作成・保存することを義務付ける。）

②個人情報データベース等を不正な利益を図る目的で第三者に提供し、又は盗用する行為を「個人情報データベース等不正提供罪」として処罰の対象とする。

5.その他

①取扱う個人情報の数が5000以下である事業者の対象外とする制度を廃止。

②オプトアウト（＊）規定を利用する個人情報取扱事業者は所要事項を委員会に届け出ることを義務化し、委員会はその内容を公表。（＊本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止する場合、本人の同意を得ることなく第三者に個人データを提供することができる。）

③外国にある第三者への個人データの提供の制限、個人情報保護法の国外適用、個人情報保護委員会による外国執行当局への情報提供に係わる規定を新設。

個人情報とは（改正法の内容）

〇個人情報の定義の明確化を図るために、その情報単体でも個人情報に該当することとした「個人識別符号」の定義を設けた。

「個人識別符号」とは以下の①②のいずれかに該当するものであり、政令・規則で個別に指定される。

①身体の一部の特徴を電子計算機のために変換した符号

⇒DNA、顔、虹彩、声紋、歩行の態様、手指の静脈、指紋・掌紋

②サービス利用や書類において対象者ごとに割り振られる符号

⇒公的な番号

旅券番号、基礎年金番号、免許証番号、住民票コード、マイナンバー、各種保険証等

※他の情報と容易に照合することで特定の個人を識別することができる情報は、個人情報に該当する。

個人情報の安全管理措置

■基本方針の策定

個人情報取扱事業者は、個人データの適切な取扱について組織として取り組むため、基本方針を策定することが重要である。

■取扱い規定の策定

個人情報取扱事業者は、その取扱う個人データの漏えい等の防止、その他個人データの安全管理のために、個人データの具体的な取扱いに係わる規律を整備しなければならない。

■組織的安全管理措置

組織体制の整備
個人データの取扱いに係わる規律に従った運用
個人データの取扱状況を確認する手段の整備
情報漏えい等事案に対する体制の整備
取扱い状況の把握及び安全管理措置の見直し

■人的安全管理措置

従業者の教育

■物理的安全管理措置

個人データを取扱う区域の管理
機器及び電子媒体等の盗難防止
電子媒体等を持ち出す場合の漏えい等の防止
個人データの削除、機器及び電子媒体等の廃棄

■技術的安全管理措置

アクセス制御
アクセス者の識別と認証
外部からの不正アクセス等の防止
情報システムの使用に伴う漏えい等の防止

個人情報の安全管理措置（委託先の監督）

委託先の監督

委託先の適切な選定

講ずべき安全管理措置に定める各項目が、委託する業務内容に沿って確実に実施されることについて、予め確認しなければならない。

委託契約の締結

委託契約には、当該個人データの取扱いに関する、必要かつ適切な安全管理措置として、委託元、委託先双方が同意した内容とともに、委託先における委託された個人データの取扱い状況を委託元が合理的に把握することを盛り込むことがのぞましい。

委託先における特定個人情報の取扱い状況の把握

委託先における委託された個人データの取扱い状況を把握するためには、定期的に監督を行う等により、委託契約で盛り込んだ内容の実施の程度を調査した上で、委託の内容等を見直しを検討することがのぞましい。
また、委託先が再委託を行おうとする場合は、委託を行う場合と同様、委託元は、委託先が再委託する相手方、再委託する業務内容、再委託先の個人データの取扱い方法等について、委託先から事前報告を受け又は承認を行うこと、及び委託先を通じて又は必要に応じて自らが、定期的に監査を実施すること等により、委託先が再委託先に対して委託先の監督を適切にはたすこと、及び再委託先が安全管理措置を講ずることを十分に確認することが望ましい。

監査の実効性向上とコスト削減

〇現実的な話として、一部の委託先は委託元が直接立入って検査することを、他のお客様情報に触れる可能性があるとの理由で、完全な形では受け入れ難い可能性がある。

⇒直接ビジネスとの利害関係がない格付会社が立入検査を実施することで、金融庁が求めている「外部委託先における業務の実施状況を定期的又は必要に応じてモニタリングする等、外部委託先において顧客等に関する情報管理が適切に行われていることを確認」を達成可能となる。

〇委託先からの意見として、「毎年、数十社（多いところでは百社以上）より、様式及び確認の観点が異なるチェックリストへの回答、及び現地審査への対応を行っており、毎日のように監査対応を行っている。各委託元からのチェックリストを標準化（共通化）して欲しい、との意見について解決策になる。

⇒各委託元（金融機関、事業者）は共通のガイドライン等を踏まえてチェックリストを作成しているはずである。共通化することで負担を軽減することについて検討の余地はある。

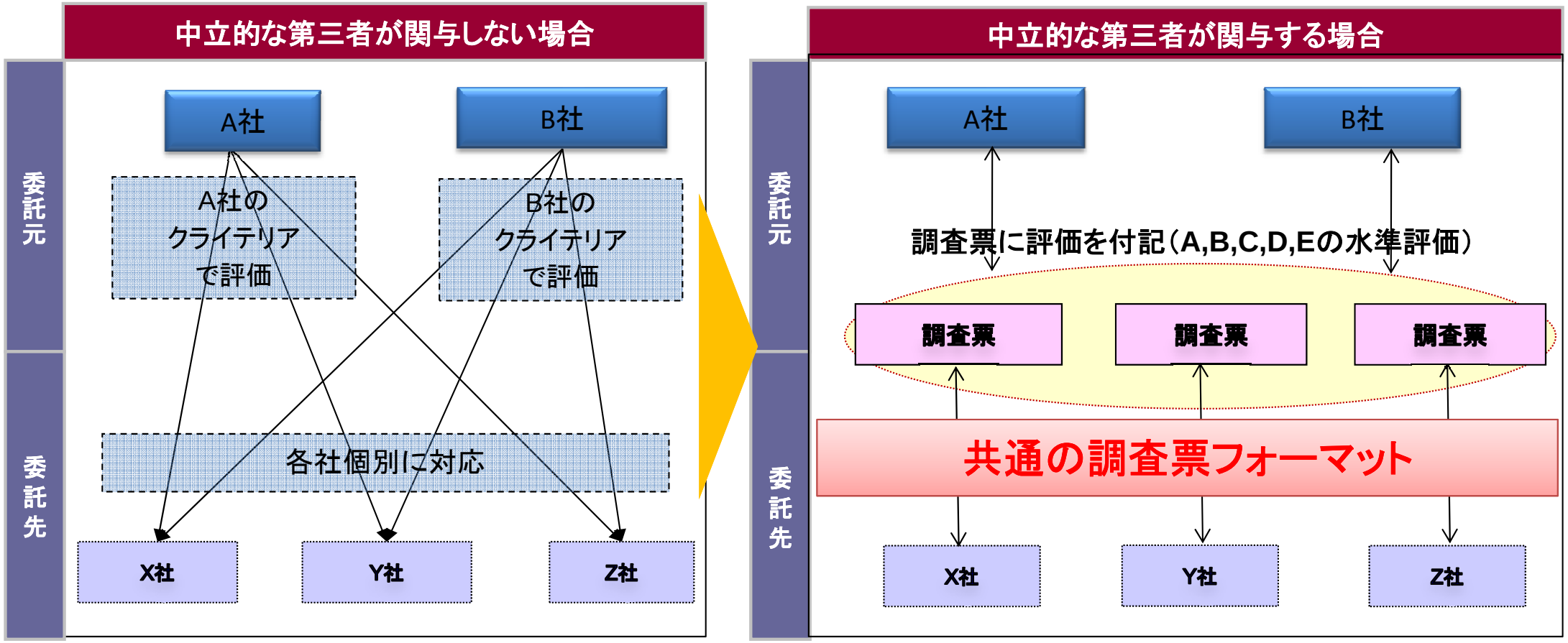
弊社が展開する情報セキュリティのレベルに関する共通の評価プラットフォーム（n対nの解消）が広がると委託元及び委託先（監督当局を含め）の業務効率化が図れる。

〇委託先監査スキル、委託先管理コスト削減

⇒システムのスキルがないので、監査出来ない。コスト効果を目的に、外部に委託したのに監査にコストがかかってしまっては意味がない。

共通の評価プラットフォーム（n対nの解消）

■多くの企業が客観的な評価指標（項目）を共同利用するなど、社会全体のコストを低減する方策が求められている。この制度では、政府のガイドラインに示されている「委託先の選定」と「委託時の必要かつ適切な監督」に共通の調査票を活用できる、安全管理措置に関する評価項目の共通の枠組みが確立し、委託先調査の社会インフラ形成され、取引先・委託先の重複調査が解消される、ことを目指している。



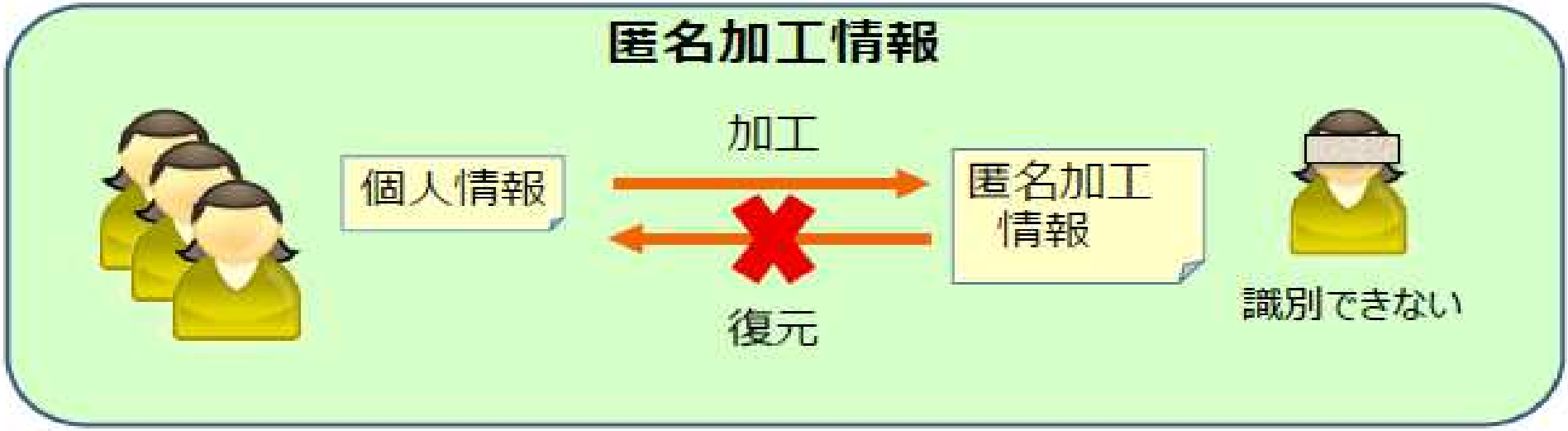
ビックデータ対応

○匿名加工情報の制度

・匿名加工情報とは、特定の個人を識別することができないように個人情報を加工し当該個人情報を復元できないようにした情報。

・個人情報の取扱いよりも緩やかな規律（作成時、第三者提供時の公表等）の下、自由な流通・利活用を促進することを目的に個人情報保護法の改正によりあらたに導入。

・匿名加工情報の**作成方法の基準を個人情報保護委員会規則**で定める。



匿名加工情報に関する規則

○ 匿名加工情報の作成方法に関して、最低限の規律として、次の措置を講ずることを求める。
なお、詳細は自主ルールに委ねる。

■特定の個人を識別することができる記述等（例：氏名）の全部または一部を削除（置換を含む。以下同じ。）すること。
■個人識別符号の全部を削除すること。
■個人情報と他の情報とを連結する符号（例：委託先に渡すために分割したデータとひも付けるID）を削除すること。
■特異な記述等（例：年齢１１６歳）を削除すること。
■上記のほか、個人情報とデータベース内の他の個人情報との差異等の性質を勘案し適切な措置を講ずること。

匿名加工情報を作成する事業者が行うべきこと

- 適正な加工を行うこと
- 加工方法自体を安全に管理すること
- 作成した際、情報項目等を公表すること
- 他の企業に第三者提供する際、情報項目と提供方法を公表すること
- また、提供先へ匿名加工情報であることを明示すること
- （自ら活用する場合）本人の再識別は禁止すること
- 安管理の措置、苦情の処理などの措置を講じ、内容を公表すること

消費者とのリスクコミュニーションが必要

匿名加工情報を提供する目的及び消費者のメリットについても、
その確認状況を第三者として証明書に記載して消費者の納得感を高める

☆☆第三者証明書の活用により匿名加工情報の利活用の推進☆☆

客観的な第三者による確認（法制度対応など）

■ 委託先の安全管理措置（特定個人情報、個人情報）

・特定個人情報の取扱いに関する安全管理措置の確認

・特定個人情報の取扱い状況の確認

・個人情報の取扱いに関する安全管理措置の確認

・個人情報の取扱い状況の確認

■ 委託先の安全管理措置（営業機密等の情報セキュリティ）

・委託先の情報セキュリティに対する対策の確認

・委託先の情報セキュリティ運用状況の確認

■ 匿名加工情報の利活用における消費者リスクコミュニケーション

・匿名加工情報に関する安全管理措置の確認

・消費者（個人情報の提供主体）に対して安心・安全を提示

☆☆「安心」・「安全」・「信用」・「信頼」の見える化☆☆

客観的な第三者による確認（ビジネスに活用）

第三者の客観的な評価を積極的にビジネスに活用

■ 自社の企業ポリシーの裏付けとして活用

信用・信頼の見える化

・「20年セキュリティのお約束」　（クマヒラ様）

■ ASPサービスの差別化に活用

完全性（改ざん防止）・可用性（通信障害の耐性）の事実を証明

・「ギフトカードASPサービス」　（凸版印刷様）

■ データセンターファシリティ

日本データセンター協会のファシリティスタンダードの全項目の事実を証明

・「アウトソーシングセンター」　（三谷産業様）

■ ITサービス継続

経済産業省「ITサービス継続ガイドライン改訂版」の全項目の事実を証明

・「ギフトカードASPサービス」　（凸版印刷様）

・「アウトソーシングセンター」　（三谷産業様）

■ 情報セキュリティ対策

自社のセキュリティ基準、経産省・文科省の個人情報保護のガイドラインを
リファレンスとして、対策実施内容を証明

・「やるKeyサービス」　（凸版印刷様）

☆☆「安心」・「安全」・「信用」・「信頼」の見える化☆☆

客観的な第三者による確認（ビジネスに活用）

第三者の客観的な評価にビジネスに活用

■ **製品の安全性を確認（無実の証明）**

サービスの向上目的でのリモート保守業務、障害対応の迅速化目的での監視業務において重要情報を搾取していない・守秘義務を順守していることを第三者が証明する。

- サービスの為に自社のセンターと通信する機能を備えているが、その機能がお客様の個人情報等の機密情報を漏えいするような動作を行っていないこと第三者が証明する。
- 監視業務を受託しているが、監視場所・監視装置に対するセキュリティ対策実施状況とお客様の管理手順が遵守されていることを第三者が証明する。

■ **セキュリティ事故（信頼回復支援） ⇒ 損害保険ジャパン日本興亜株式社様と提携**

情報セキュリティ事故発生後の対応が完了したことを第三者が証明する。
再発防止策が完了し、対策が有効であることを外部の専門家である第三者が確認し、対策が実施されている ことを証明する。（情報漏えい保険付帯サービス）

☆☆「安心」・「安全」・「信用」・「信頼」の見える化☆☆

ビジネスを支援

第三者として客観的な評価を実施するとともに、第三者としてビジネスを支援します。

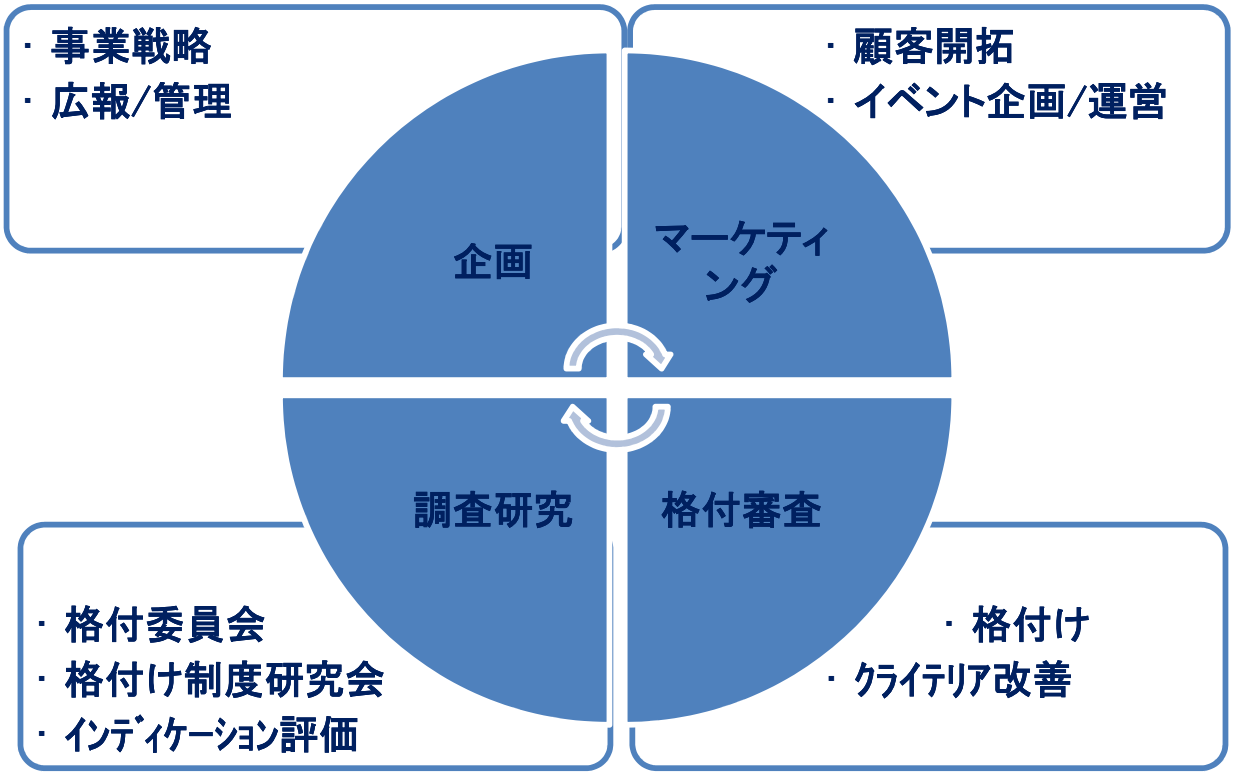
■ 弊社ホームページに記載します。（公表可の場合）
第三者証明書のダウンロードができます。

■ 格付け通信によるメールマガジンを発信します。（日経BP社のサービス活用）
情報セキュリティ格付け結果の公表、第三者証明取得結果の公表による企業のアピールと弊社のプロモーションを目的とし、◆IT格付通信◆として発信しています。

--☆PR☆----------
◆IT格付通信049◆詳細 http://www.israting.com (I.S.Rating)
☆株式会社クマヒラ様・株式会社熊平製作所様、第三者による客観的な評価実施！☆
セキュリティシステムGGシリーズ『20年セキュリティのお約束』の評価を実施。
「互換性のある製品提供」・「新機能の追求」・「運用サポート体制の充実」により
20年セキュリティを実現。2014年から毎年継続調査を実施、4年連続で取得！
----------☆PR☆--

--☆PR☆----------
◆IT格付通信050◆詳細⇒ http://www.israting.com (I.S.Rating)
「ギフトカードASPサービス」凸版印刷様、富士通エフ・アイ・ピー様の共同事業
☆ 情報セキュリティ最高格付け【AAAis】を5年連続で取得しました！ ☆
☆ 第三者による客観的な評価も5年連続で実施し第三者証明書を取得しました！ ☆
☆ 新規顧客の獲得や来店促進、アップセルにつながるカードソリューションです ☆
----------☆PR☆--

「格付・第三者証明」で確かめ合う、情報の安心・安全」



お問合せ先

株式会社アイ・エス・レーティング
TEL： 03-3273-8830
E-mail： ISR@israting.com http://www.israting.com/

なお、当資料に記載の内容は予告なく変更することが御座いますので、予めご了承願います。