主催：情報セキュリティ格付け制度研究会

IT-BCP第三者証明書発行サービスについて

情報セキュリティ格付け制度研究会

2012年10月26日

三好　眞

（株式会社アイ･エス･レーティング）

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。

目次

格付制度

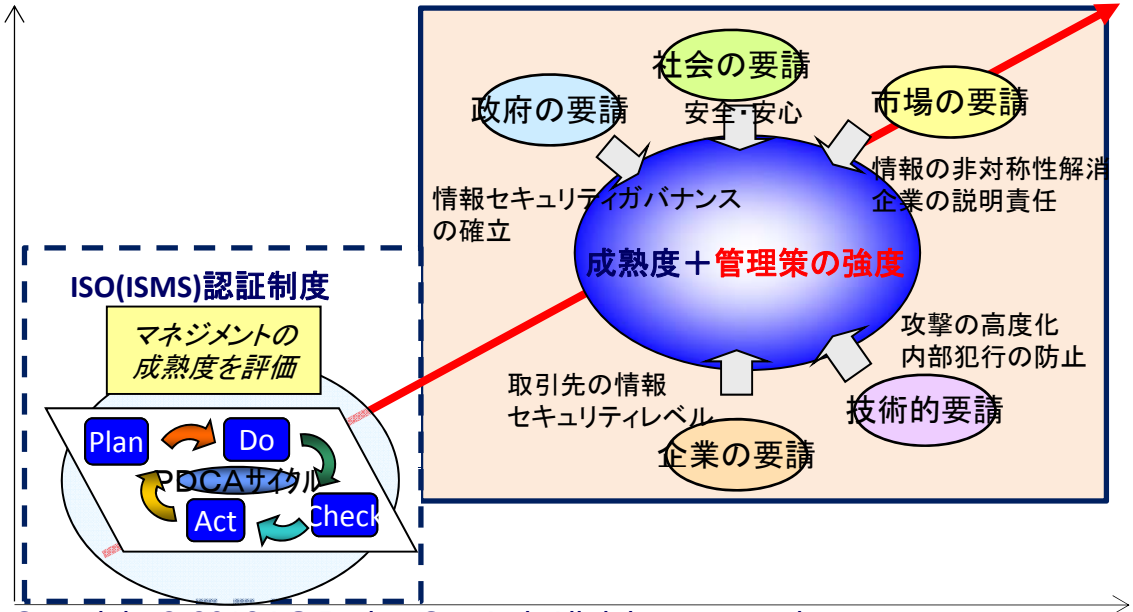
格付制度の目的

●産業構造審議会が「情報セキュリティ基本問題委員会報告書」（07年5月）にて、新たな三つの戦略のうち、**企業が取り組むべき優先的・重点的課題に「民間格付けの必要性や促進」**を盛り込む。民間格付けについては3年以内に着手し早期実現を目指す

●産業構造審議会が「情報セキュリティ格付を実施する各種機関の運営に関する一般要求事項」（09年5月）を公表。各企業が積極的に情報セキュリティ対策に取り組むためには**「企業における情報セキュリティ対策の実施が当該企業の価値の向上につながるような市場メカニズムを働かせる」**ことが必要

●信頼性向上を目指した情報セキュリティの取組状況開示が有効だが、実施状況を詳細に公表することは、情報セキュリティ対策の問題点を明らかにしてしまう危険性がある

●情報セキュリティ**対策の詳細を明らかにせず、対策の実施状況のみを開示する方法として「情報セキュリティ格付け」が有効**であり、その社会的位置付けを明確にし、格付け結果の**公平性を担保するため「情報セキュリティ格付」に対する規律**が必要



■マネジメント成熟度に加え、これまで見えにくかった**情報漏えい対策の強度を“見える化”**することで、取引先間相互の信頼構築。

■後を絶たない情報セキュリティ事故、社会・市場は**認証制度に加え、実態に即してレベルを評価**する制度を要請。

■ステークホルダー全体を意識し、説明責任を果たすとともに、**対策水準をアピール**する。

政府動向

産業構造審議会「情報セキュリティ格付機関の規律に関する基準」

■基準の目的

（09年5月）

・民間組織による情報セキュリティ格付の信頼性を高めるために、**情報セキュリティ格付機関において満たすべき行動規範的要件**を多面的観点から整理・検証
・海外の情報セキュリティ格付に関連する機関との連携等の可能性を踏まえ、必要に応じ**国際標準の枠組みも視野**に入れる

■基準の構成

1. 一般要求事項
法的及び契約上の事項、公正性と誠実性、独立性と客観性、透明性、機密保持、品質、**公平性のマネジメント**、債務及び財務、情報セキュリティ、苦情への適切な対応、異議申し立て

2. 組織運営機構に対する要求事項
組織構造及びトップマネジメント、公平性委員会、**格付委員会**

3. 資源に対する要求事項
経営層及び**アナリストの力量**、格付に関するアナリスト、個々の外部アナリスト及び外部技術専門家の起用、アナリスト及び技術専門家の記録、外部委託

4. マネジメントシステムに対する一般要求事項
一般、マネジメントシステムマニュアル、文書管理、記録の管理、マネジメントレビュー、内部監査、是正処置、予防処置

出典：経済産業省　産業構造審議会資料を参考に加筆

株式会社アイ・エス・レーティングが第一号として適合宣言

株式会社アイ・エス・レーティングの公正性・中立性についての考え方

- **一部の企業、特定の企業が作った制度でなく、多くの企業が参画して作った制度とするため、業種や企業グループを越えた幅広い企業の理解を求め、多数の会社が株主として参画**
- **株主が格付審査に影響力を行使できないようにするため、1社・1企業グループの出資比率を20%以下に抑えるというルールを設定**
- **債券などの信用格付機関に求められる「公正性・中立性の基準」に相応する運営管理を実施**

格付制度

株主構成と事業内容

株式会社
アイ・エス・レーティング

所在地：東京都中央区日本橋
資本金：3億9,000万円(2012年9月現在)
設　立：2008年5月2日

■事業内容：

1. 情報セキュリティの評価業務
2. 情報セキュリティアナリストの認定業務
3. 情報セキュリティ格付けに関する
   調査・教育・出版等の業務

（注）利益相反を回避するためにソリューション提供等は行っていません。

出資（25社）　情報セキュリティ格付制度に賛同

ICT・ハイテク製造
パナソニック
富士通
ソニー

ドキュメント
富士ゼロックス
キヤノンマーケティングジャパン

印刷
凸版印刷
大日本印刷

シンクタンク
野村総合研究所
三菱総合研究所

セキュリティ関連
綜合警備保障　コクヨ
クマヒラ　GSX
シマンテック

銀行
みずほコーポレート銀行
北洋銀行

保険
三井住友海上火災保険
損害保険ジャパン

金融関係
ダイヤモンドレンタルシステム
ゴールドマンサックス

新聞・電力
日本経済新聞社
東京電力

格付・認証機関
格付投資情報センター
TUVラインランドジャパン

他業界
ワコールホールディングス

経済産業省の取組み

ITサービス継続ガイドライン（改訂版）の策定

- ITへの依存関係が変わり、ITサービスが停止することにより業務が停止するケースも増えてきている。その潜在リスクや業務のIT依存に起因する脆弱性を認識することが重要である。
- 東日本大震災において、我が国は過去に例を見ない広域かつ複合的な災害に直面した。緊急時においても守るべき根本原則を明確にしておくことにより、「想定外」の事態が発生したとしても、適切な対応を取ることは可能である。
- 本ガイドラインは、組織 におけるITサービスの企画、開発、調達、導入、運用、保守などに携わる部門等が、事業継続マネジメント（BCM）に必要なITサービス継続を確実にするための枠組みと具体的な実施策を示し、取り組みの実効性の向上を支援することを目的とする。

ITサービス継続検討ワーキンググループ

構成員（所属組織）

（主査）
- 名古屋工業大学

（委員）
- 社団法人 日本情報システム・ユーザー協会
- 株式会社富士通総研
- NKSJリスクマネジメント株式会社
- 株式会社日立製作所
- 日本ヒューレット・パッカード株式会社
- 株式会社NTTデータ
- 情報セキュリティ大学院大学
- 富士ゼロックス株式会社
- 日本電気株式会社
- 株式会社アイ・エス・レーティング
- 公益財団法人 金融情報システムセンター
- 特定非営利活動法人 日本セキュリティ監査協会

（オブザーバー）
- 経済産業省
- 独立行政法人 情報処理推進機構
- 一般財団法人 日本情報経済社会推進協会

（順不同/敬称略）

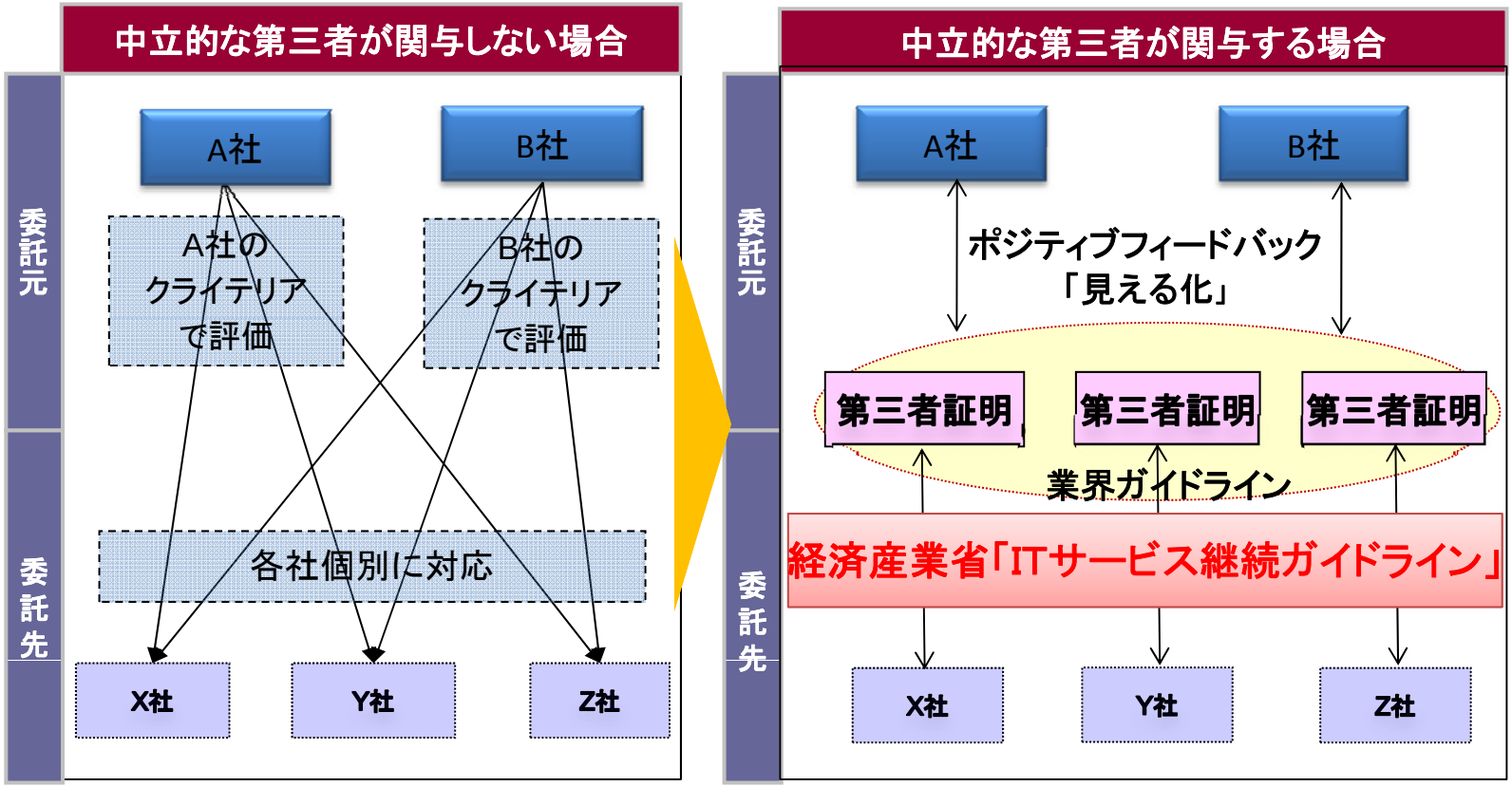
IT-BCP

第三者証明書発行サービスの目的

■ 経済産業省ITサービス継続ガイドラインの管理項目を活用して、組織（企業・団体）のIT-BCPに関するマネジメント・プロセスを客観的に確認。ひいては、事業者間で輻輳しかねない相互の取引確認を第三者証明書を用いて解消し、調査コスト・工数の効率化を図るなど社会的なコスト削減。

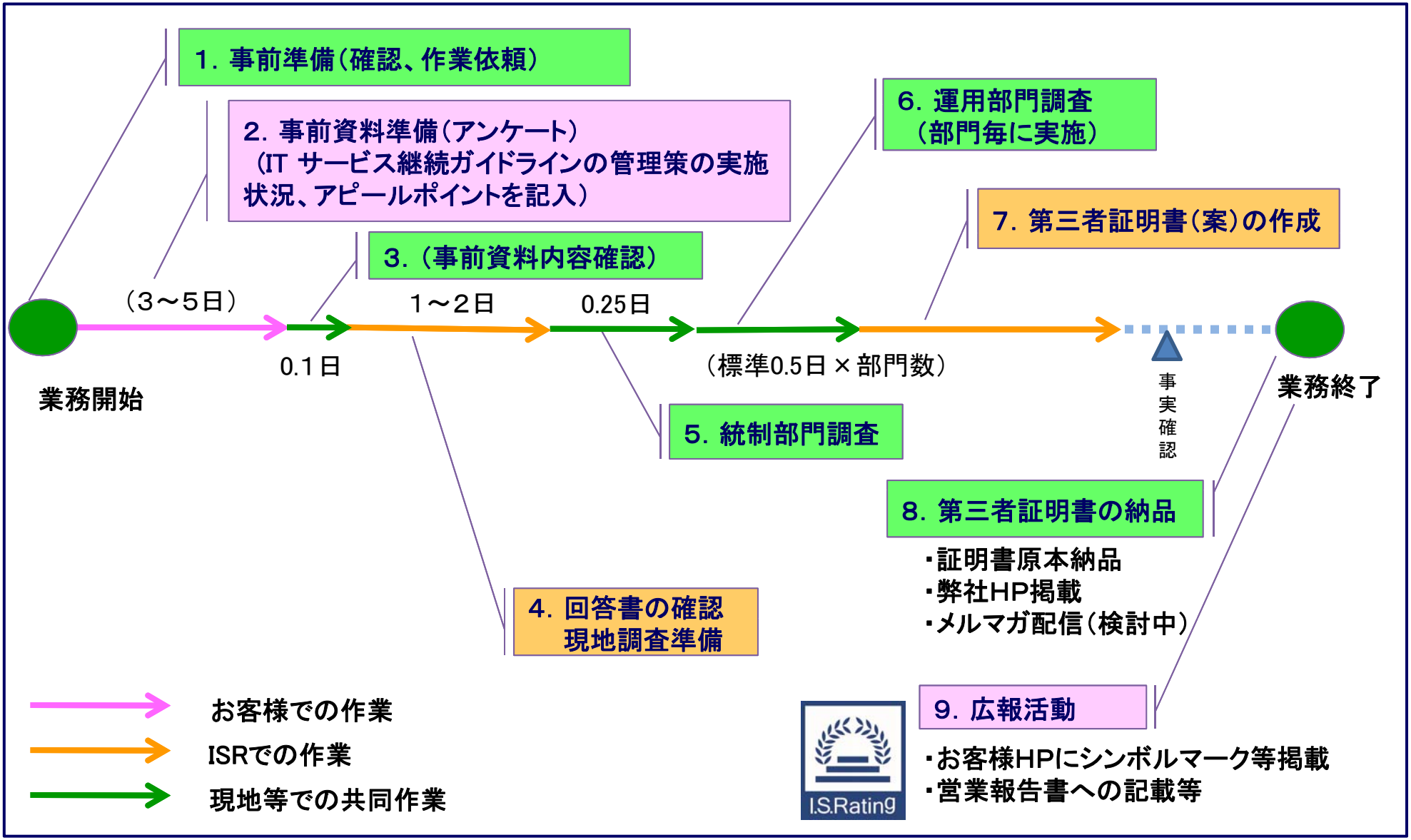
■ 第三者証明書により信頼確保に向けた取組の“見える化”により説明責任を果たすとともに、ステークホルダーにアピールすることで販路拡大等につなげる機会を創出。

■ 専門知識を有する第三者が客観的な立場で対策状況を診断することで自社の強み・弱みが浮き彫りになり、経営資源配分等の基礎資料として活用可能。



IT-BCP

第三者証明書発行の標準工程



IT-BCP

ホームページへの掲載事例

弊社HP掲載イメージ「第三者評価一覧」

企業・団体名	三谷産業株式会社	証明書IDコード	10000230115B1201
調査スコープ	アウトソーシングデータセンター		
調査対象	データセンターにおけるITサービス継続対策		
調査事項	ITサービス継続対策 実施状況	交付日 （有効期限）	2012年10月15日 （2013年10月14日）
リファレンス	経済産業省 「ITサービス継続ガイドライン改訂版（平成24年）」	第三者証明書	PDF
アピールポイント	【二重化、冗長化された電源】 同社グループ会社にて自家発電装置の燃料（軽油）を取扱っており、自前で燃料の調達を行い安定した運用を継続することが可能。 【データ保管体制の強化】 免震構造のデータ保管庫棟をサーバ棟と別の建物として保有しており、サーバとの同時被災を防ぎデータ媒体を安全に保管可能。		

■調査スコープと調査対象を設定して、アプリ開発等の対象部門や対象業務等を特定可能です。
■調査の方法は、責任者等へのヒアリング、規程および台帳類の閲覧、関連設備の視察等によります。
■第三者証明書は、調査実施日における事象について事実であることを証明するものです。
■利用期限は、証明書交付日から1年を目安としています。
■第三者証明書は、被調査組織等から入手した情報に依拠して形成した当社の意見であり、被開示者、閲覧者等に対し、参考情報としてご提供されるものです。

■ステークホルダーへのアピールポイントについての取組み内容のうち、特筆すべきポイントを記載（150字以内）します。取引先からよく聞かれる項目を説明することで、販路拡大等につなげる機会を創出しています。

IT-BCP

第三者証明書の構成（1）全体構成

調査概要

確認事項1「サマリー」

■2ページ程度。最初のページは、調査スコープ、調査対象、有効期限等の**調査概要**（HP掲載内容とほぼ同じ）を記載。
■2ページ目は、**確認事項のサーマリー**を記載。3ページ以降の詳細な確認事項の纏めに加え、会社パンフ等からの引用を素材に、**組織・技術・人の視点で表した対策の概要**。

確認事項2「IT サービス継続ガイドラインの管理策」

■2ページ程度。
■経済産業省IT サービス継続ガイドラインの管理策で構成。
（詳細説明は次ページ参照）

■1、2ページ程度。**注力している取組み**や今年度の**重点的な取組み**など、特筆すべき事項を公表すると、取引先等にアピールできます。

確認事項3「アピールポイント」

項目	優れている点
①立地の安全性、免震構造、二重化・冗長化された電源	・・・
②雷対策の充実、火災対策の充実、データ保管体制の強化	・・・
③ネットワーク接続の継続性、運用要員確保、緊急宿泊設備	・・・
④今年の特別確認テーマ「電源と通信手段の確保、訓練の充実」の取組み	・・・

IT-BCP

第三者証明書の構成（2）IT サービス継続ガイドライン

確認事項2「IT サービス継続ガイドラインの管理策」

管理項目	項目詳細	必須
5.1 計画	5.1.1 IT サービス継続計画	○
5.2 実装	5.2.1 情報システムアーキテクチャの決定	△
	5.2.2 費用対効果の検討	－
	5.2.3 関連基準等との整合性	－
	5.2.4 データの保全	○
	5.2.5 システムの保全	△
	5.2.6 通信回線	－
	5.2.7 電源の確保	○
	5.2.8 クライアント環境	△
5.3 運用	5.3.1 従業員	△
	5.3.2 ワークスペース	－
	5.3.3 外部サービス	△
	5.3.4 サービスレベル管理	△
5.4 テストと監査	5.4.1 テスト・訓練・演習	○
	5.4.2 監査	－
5.5 改善	5.5.1 IT サービス継続計画のレビュー	○
	5.5.2 情報の記録	○
	5.5.3 平時からの情報収集と検証	△

■IT サービス継続計画は、経営陣によって承認されなければならない。また必要な範囲で従業員及び関連する外部関係者に開示し、通知しなければならない。

■IT サービス継続に必要となるデータを保全するための技術的措置を講じなければならない。

■IT サービス継続に必要な情報システムを稼働させるための電源を確保しなければならない。

■IT サービス継続計画の有効性を確認するため、定期的にテストを行い、対処能力の向上、計画の改善を行わなければならない。

■IT サービス継続計画は、定期的もしくは重大な変化が発生した場合に、その適切性・有効性を確実なものとするためにレビューを行わなければならない。

■組織はIT サービス継続に関して発生した情報システム障害等について記録しなければならない。

左記の○印は必須項目で、未実施の場合は証明書に未実施と記入する事になります。△印は実施すべき項目、－印は実施が望ましい項目です。

ビジネスモデル

評価結果の利用～ソリューション提案

ビジネス
パートナー
募集中

- 電源確保
- 緊急時の連絡手段
- 訓練/実効性
- 委託先管理

■ Before-Afterモデル

提供するソリューションの成果測定に利用する

第三者証明書 → コンサルティング ソリューション提供 → 第三者証明書

■ 予算獲得モデル

インディケーション評価で対策ポイントを絞り込む

第三者証明書 → IT-BCP対策 予算稟議作成 → コンサルティング ソリューション提供

■ クロージングモデル

提供したソリューションの評価基準に利用し検収をスムーズに

コンサルティング ソリューション提供 → 第三者証明書

●ガバナンス
●説明責任
●情報開示
↓
信頼性・投資対効果
↓
企業価値

「第三者証明」で確かめ合う、情報の安全安心！

IT-BCP対策に加え、取引先にアピールしたい情報セキュリティや環境への取組みを、1つの証明書に記載して証明することもできます。

＜参考＞政府動向

情報セキュリティ格付け制度の背景

■ この度の情報セキュリティ格付けの取組みは、国の動き(グローバル情報セキュリティ戦略)と連動しての民間主導の仕組み作り

〈背景〉
- 社会の神経系となった情報技術
- 事故の影響の増大
- コンプライアンス(個人情報保護法 等)
- 情報セキュリティ強化と、企業競争力や企業価値の向上との関係が見えにくい

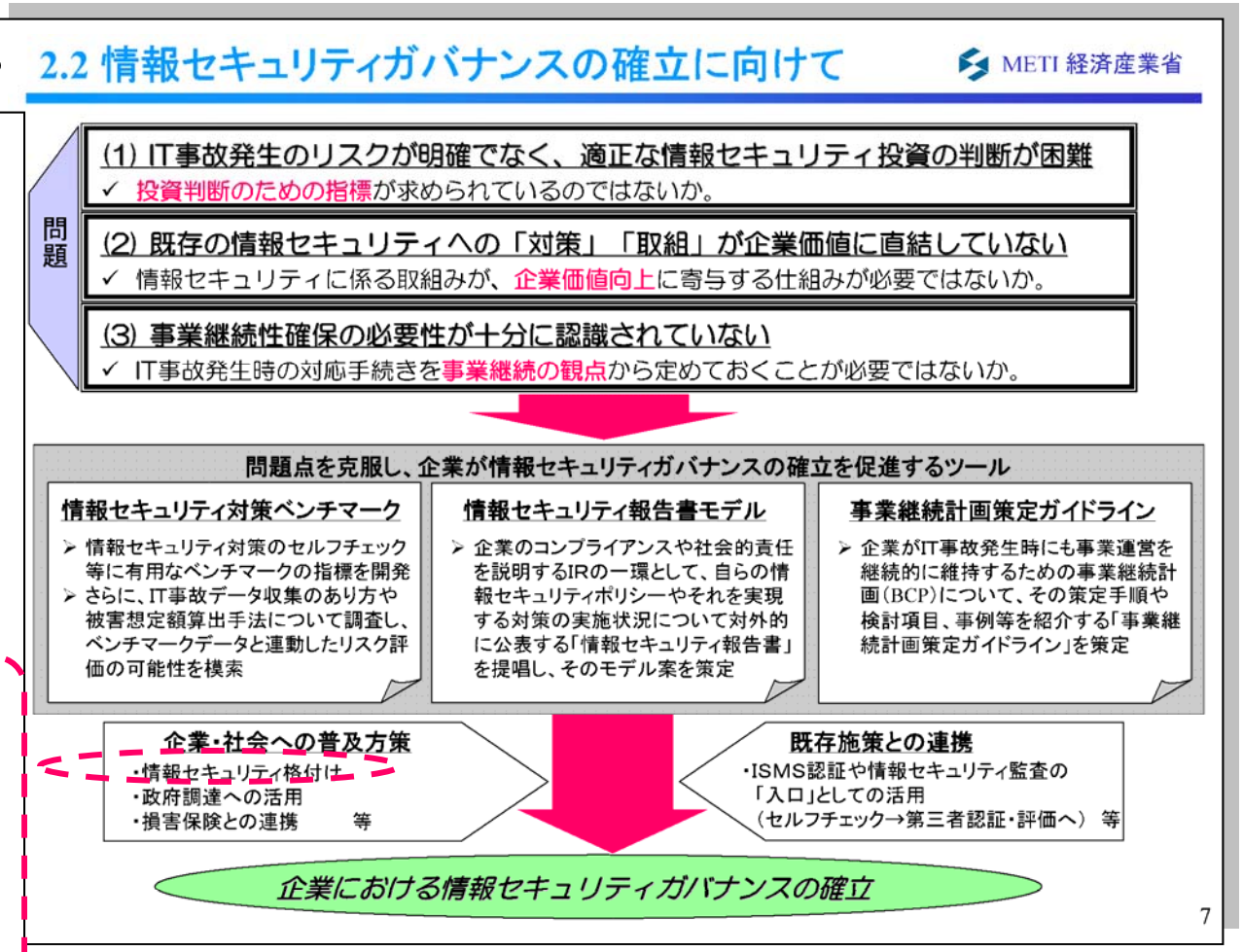
「情報セキュリティガバナンスの確立」

〈グローバル情報セキュリティ戦略〉
経済産業省 2007年5月

(企業の領域)

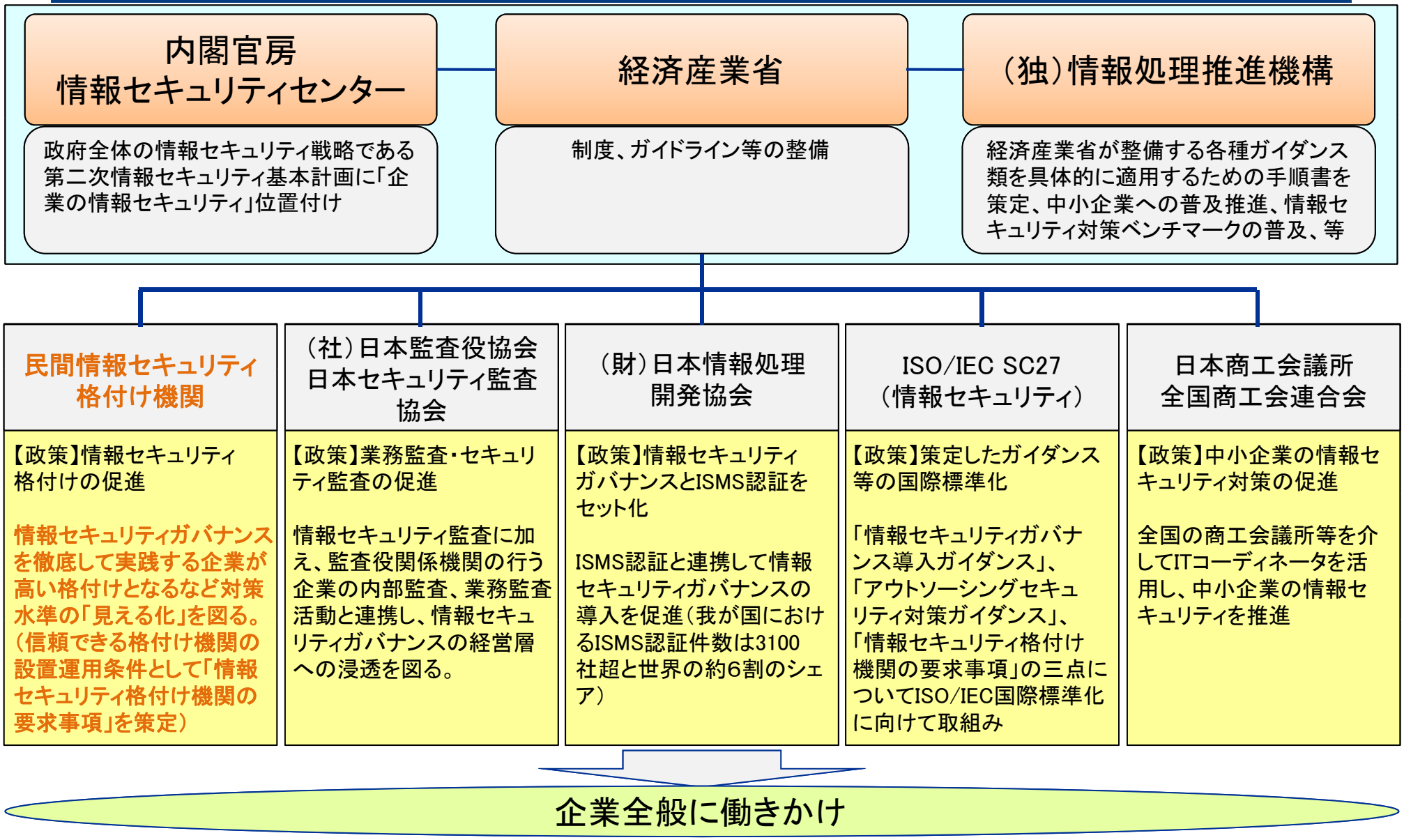
情報セキュリティ対策の成熟度向上等に向けた市場メカニズムの強化

情報セキュリティ対策状況に係る情報開示を通じた民間格付けの促進等



＜参考＞政府動向

情報セキュリティガバナンス確立促進政策

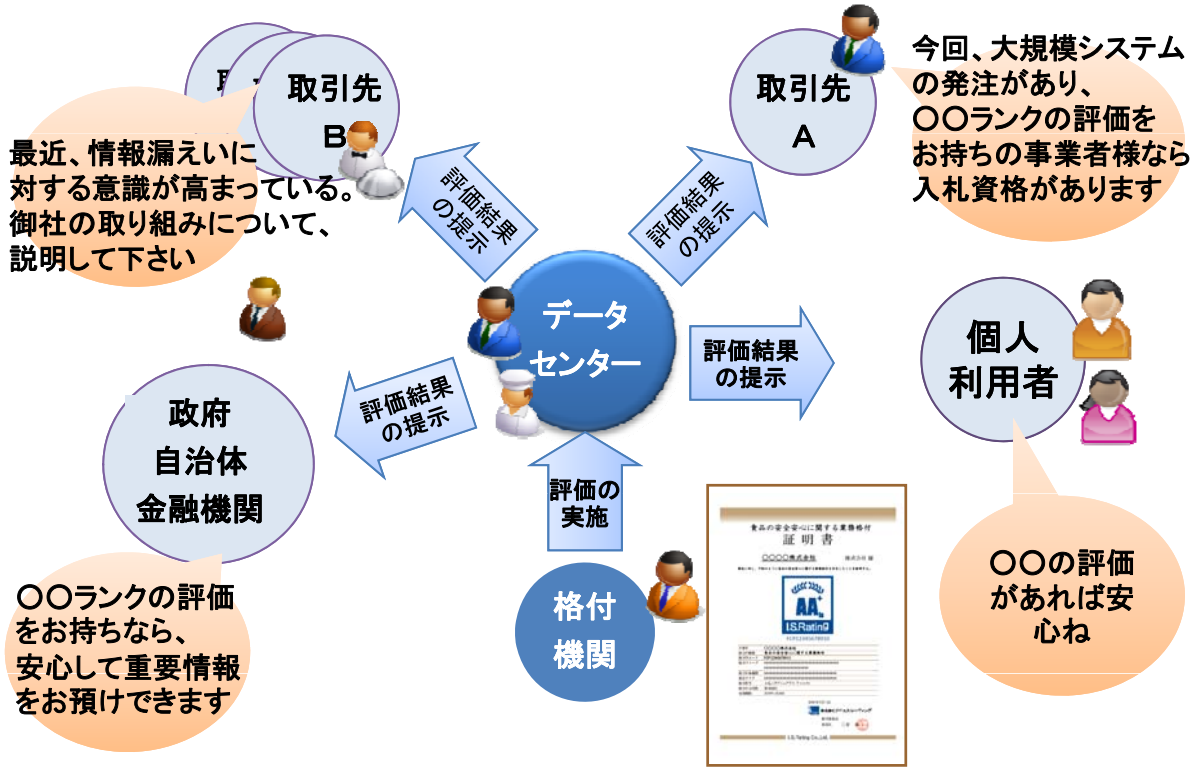


出典：経済産業省　産業構造審議会資料を参考に加筆

＜参考＞格付制度

格付けの活用イメージ

■ 第三者による客観評価（17段階）を用いて、経営者や現場責任者が自社の情報漏えい対策を客観的な視点で再点検する。
　　□ 自社・自組織のレベルがわかる　他社・他組織とレベル比較ができる
■ 格付けを取引先間の対策水準の確認基準として利用すると、相互に品質の見える化が実現できる。
　　□ 採用基準の共通尺度として利用
■ 格付けを公表して、ステークホルダーに情報漏えいに対する積極的な取り組みをアピールすると、販路拡大等の機会が増える。
　　□取引先にアピールできる（BtoB）　個人利用者にアピールできる(BtoC)



●社会が変化して、自社・取引先間で業務システムを相互接続することが一般的になり、さらに業務自体をアウトソーシングするなど、**データセンター等を利用する形態が増加**の一途を辿っている

●グローバルな分業体制が進展した結果、国内外の企業への委託業務が増え、**ガバナンスの対象範囲が大きく拡大**している

●**ASP/SaaSは、内部犯罪を含め、情報漏えいの危険にさらされており、**そのような環境下、マネジメントシステムの存在を認証するだけでは不十分であり、**格付は情報セキュリティの強度を確認する社会システムとして**有用だろう。（10年2月実施「制度研究会データセンター格付ニーズ調査」より）

＜参考＞格付制度

情報セキュリティ格付け制度研究会「設立趣旨」

（背景）

■ わが国は戦後、経済を中心として目覚しく発展、世界経済をリードする存在となった。90年代に入り、ITなどの科学技術の高度化や世界的な分業体制の進展を背景に、情報システムは経済活動のライフラインと言われるまでに成長した。しかし社会のIT化などが進む中で、情報漏えいやシステムダウンが頻発するようになり、情報セキュリティが新たに深刻な社会・経営問題になりつつある。政府・民間を問わずリスクが様々な形で顕在化しており、政府、企業、個人のあらゆる分野において、既存の社会システムをセキュリティの視点で見直す必要がある。

■ 情報セキュリティに関わるリスクは新たな脅威である。この脅威は、産業界に致命的なダメージを与えるばかりか、国家の存立を危うくする惧れもある。この共通認識に立脚し、多くの企業が協力して新たな脅威に立ち向かうことが急務となっている。

（課題）

■ 社会が変化して、自社・取引先間で業務システムを相互接続することが一般的になり、さらに業務自体をアウトソーシングしてデータセンターでシステムを共同利用する形態も増加の一途を辿っている。また、グローバルな分業体制が進展した結果、国内外の企業への委託業務が増え、ガバナンスの対象範囲が大きく拡大している。

■ 情報管理強化の一環として、多くの企業が業務委託先の管理を充実するなか、委託会社・受託会社におけるセキュリティ水準の相互確認作業は膨大なものとなっている。セキュリティ品質の向上は、1つの企業や団体などの閉じた環境の中で完結するものではない。業務の効率化と有効性を確保するには、多くの企業が客観的な評価指標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。この問題に対処するために新たな仕組みを構築し、財やサービスに付随する個人情報、技術情報や営業機密などの情報管理を徹底することが課題となっている。

■ また、情報セキュリティに対する投資を自社の製品やサービスの競争力強化に結びつけ、企業価値を向上させること、格付けを用いた市場メカニズムの創設によるガバナンスの確立も課題となっている。

（目的）

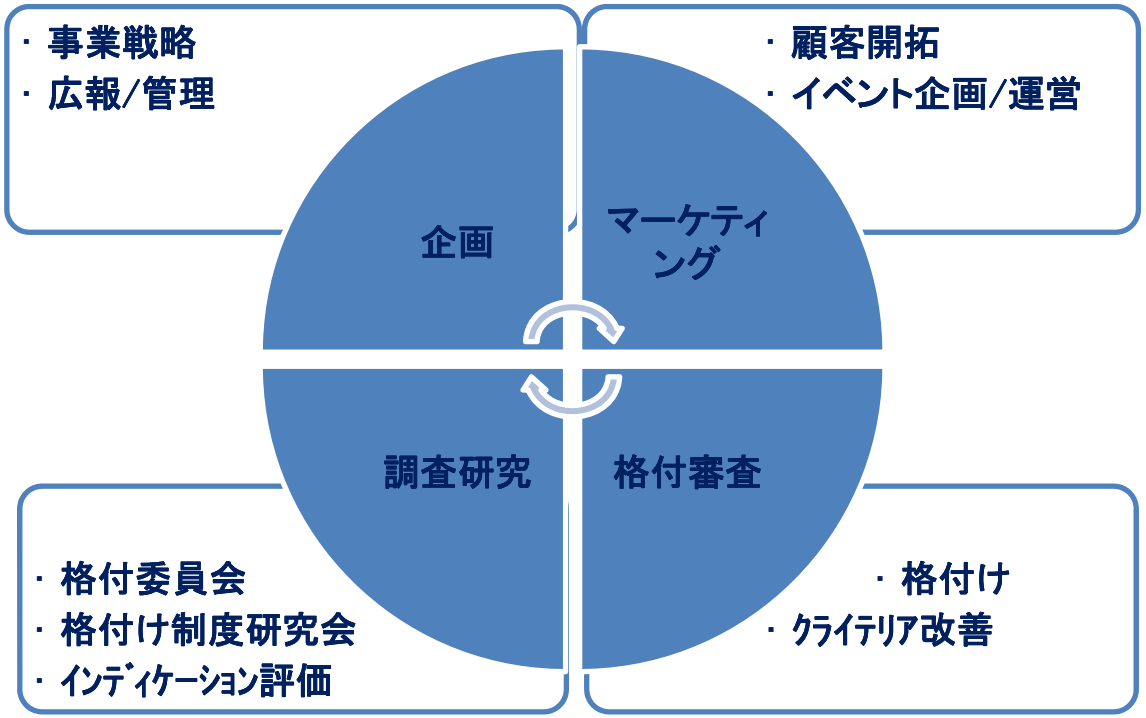
■ 格付け制度研究会は以上の課題などの解決に向け、社会や企業の情報セキュリティ・ガバナンスの向上に資する諸活動を企画・立案し、実行する。

■ 社会的インフラとして「情報セキュリティ格付け制度」の確立を目指し、世界経済システムのなかでも信頼されるわが国の経済基盤の確立に貢献していく。

■ 業界横断的な情報セキュリティ格付けの取り組みにより、高度なセキュリティレベルを実現した組織が、市場において高い評価を獲得し、企業価値の向上を実現していく仕組み作りを目指す。

■ 多くの企業や団体が会員として参画できる仕組みを準備し、業種・業態の枠組みを超えた活動を行う。

「第三者証明」で確かめ合う、情報の安全安心！



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。