

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

平成 21 年6月

経済産業省

序文

企業の情報セキュリティに対する取組が、顧客（格付対象者）、取引先、株主、格付結果の利用者、政府関係当局などの利害関係者から適切に評価されるためには、各企業の取組が比較可能な形式で提示される必要がある。

企業の情報セキュリティに対する取組が、顧客（格付対象者）、取引先、株主、格付結果の利用者、政府関係当局などの利害関係者から適切に評価されるためには、各企業の取組が比較可能な形式で提示される必要がある。

情報セキュリティ格付は、各企業の取組状況を明らかにし、企業の情報管理の強化、効率化や有効性確保に寄与する公益性の高い仕組みである。

本文書は、情報セキュリティ格付機関が使用することを意図し、情報セキュリティ格付機関が満たすべき要求事項を明確化している。

本要求事項を順守することで、格付機関が必要な能力をもち、一貫して公平な方法で運用され、国内及び国際的に認知され、格付機関による格付結果の受入れが促進されることを意図している。

本要求事項は、格付機関が、自らの責任において、以下に示す全ての要求事項に準拠した自社の規範を定め、それらを順守していることを、自ら宣言するために利用することができる。

なお、時限的な例外措置として、一部の要求事項を変更して適用したり、あるいは一部の要求事項を除外したりすることも可能だが、その場合には、変更して適用した要求事項及び除外した要求事項について、その内容及び理由を完全かつ明確に宣言しなければならない。

本要求事項の記載内容は、社会環境や市場ニーズの変化に適時適切に対応するため、定期的な見直しを実施するものとする。

1. 適用範囲

本文書は、情報セキュリティ格付を行う機関の能力、並びにそれら機関に対する要求事項について規定する。

2. 用語及び定義

2.1 情報セキュリティ格付（以下、“格付”という。）

格付の対象となる企業、組織及び業務等の情報セキュリティ水準を表すための指標

2.2 情報セキュリティ格付機関（以下、“格付機関”という。）

情報セキュリティ格付を意見として表明する機関

2.3 アナリスト

格付意見を形成するために、格付機関が定めた格付方法に従って、格付業務を実施する者

3. 一般要求事項

3.1 法的及び契約上の事項

3.1.1 法的責任

格付機関は、すべての格付業務に法的責任を負うことができる法人または法人内の一部の組織として明確に位置づけられなければならない。

3.1.2 格付の合意

格付機関は、格付に関して、格付対象者との間で、法的に拘束力のある合意書を締結しなければならない。

3.1.3 格付の決定に関する責任

格付機関は、格付の決定の根拠となる、十分な客観的証拠を評価する責任を負わなければならない。

格付機関は、格付の付与、更新、範囲の拡大ないし縮小、中止を含む決定に責任を負わなければならない。

3.2 品質

格付機関は、格付方法を定め、その手順を文書化しなければならない。

格付機関は、厳格で体系的な格付方法及び手順を用いなければならない。

アナリストは、格付機関が定めた格付方法及び手順を用いて格付業務を実施しなければならない。

格付機関は、個々の格付業務に関する記録を、社会通念に照らして合理的な期間に亘り保存しなければならない。

格付機関は、誤りのある格付結果又は誤解を生じる可能性のある格付結果等の公表又は開示を避けるため、それらを回避するための手順を文書化しなければならない。

格付機関は、個々のアナリストによる格付結果の偏りを防止するため、複数のアナリストからなる格付チームを編成して格付業務を実施しなければならない。

格付機関は、格付の最終更新期日を格付ごとに表示しなければならない。

格付機関は、公表（または対象者を限定して開示）している格付を中止する場合には、その事実を公表（または限定された対象者に開示）しなければならない。

3.3 公正性と誠実性

格付機関及び従業員は、格付に関係するすべての利害関係者に対して、公正かつ誠実に対応しなければならない。

格付機関は、格付業務の開始前に格付結果を保証するような行為や言動を従業員が行うことを禁止しなければならない。

格付機関は、従業員が取引先に対して利益供与を求め、及び提供を受けることを禁止しなければならない。

格付機関は、関連する基準、手順及び関係法令等の順守に責任を有する者（コンプライアンス責任者）を特定しなければならない。

格付機関の従業員は、コンプライアンス違反を発見した場合、直ちにコンプライアンス責任者に通報しなければならない。

コンプライアンス責任者から報告を受けた経営層は、直ちに必要な措置を講じなければならない。

コンプライアンス責任者への指揮命令系統は、格付業務とは独立させなければならない。

3.4 独立性と客観性

格付機関及びアナリストは、格付業務及び格付結果の独立性及び客観性を維持しなければならない。

格付機関は、情報セキュリティレベルに関連する事項のみによって格付結果を決定しなければならない。

格付機関は、その格付結果が利害関係者に対して与える影響を鑑みて、自らの格付業務を抑制したりしてはならない。

格付機関は、自身が属する法人及びその関係会社と、格付対象者及びその関係会社との間に事業上の関係が存在すること又はしないことによって格付結果に影響を与えてはならない。

格付機関は、格付業務に従事する従業員を、格付業務の費用を協議するための格付対象者との協議に関与させてはならない。

3.5 透明性

格付機関は、格付方法、手順、格付の前提条件等を公表しなければならない。

格付機関は、格付結果等の公表又は開示に関する方針を公表しなければならない。

格付機関は、格付方法、手順及び方針等を変更する際は、あらかじめ変更点を公表しなければならない（軽微な変更は除く）。

格付機関は、格付を付与又は更新する際に、格付意見の形成に至った経緯について表明しなければならない。

3.6 機密保持

格付機関及び従業員は、格付対象者に関するすべての占有情報を機密として保たなければならない。

格付機関及び従業員は、格付対象者との機密保持契約に反して、占有情報を開示してはならない。

格付機関及び従業員は、格付対象者との機密保持契約の範囲において、格付業務を実施する目的にのみ、占有情報を利用してはならない。

格付機関の従業員は、格付業務に必要な場合を除き、他のいかなる目的のためにも、占有情報を利用又は共有してはならない。

3.7 公平性のマネジメント

3.7.1 一般

格付機関は、公平性の重要性を理解し、利害抵触を管理し、格付業務及びアナリストの認証プロセスの客観性を確実にすることを宣言する、公にアクセス可能な書面を有しなければならない。

格付機関は、公平性に関する容認できない脅威がある場合は、格付を提供してはならない。

格付機関は、他の格付機関の格付を実施してはならない。

経営層、格付機関の従業員又は委員会委員であって、格付業務に影響を及ぼし得る者は、公平に活動しなければならず、公平性を損なう商業的、財務的圧力等を許してはならない。

トップマネジメントは、格付機関の公平性について、コミットメントしなければならない。

3.7.2 格付のコンサルティングとの関係

格付機関は、格付機関のいかなる部門においても、格付のコンサルティングを実施してはならない。

格付機関は、格付のコンサルティング機関と格付機関の関係が、公平性に関する容認できない脅威となる場合、そのコンサルティング機関から格付のコンサルティングを受けた者に対して格付を実施してはならない。

格付機関は、格付のコンサルティング機関に格付を外部委託してはならない。

格付機関は、格付のコンサルティング機関の活動と結び付けた営業活動をしてはならない。

格付機関は、格付対象者に格付のコンサルティングを提供した者を、当該コンサルティングの提供終了後2年間は、当該格付対象者に対する格付業務に従事させてはならない。

ない。

3.7.3 利害抵触の排除

格付機関は、格付の提供から生じる利害抵触の可能性を特定し、分析し、文書化しなければならない。また、その情報を公平性委員会に提供しなければならない。

格付機関が属する法人及び格付機関は、経営層の構成、株主の構成、収益の構成、人事・報酬体系その他の要因により利害抵触が生じる可能性がある場合、これを防止するための適切な措置を講じなければならない。

格付機関は、過度な資本、取引又は人的関係のある組織を対象にした格付を行ってはならない（「過度な」とは、一つの企業集団が、格付機関が属する法人の発行した株式のうち、10%を超える株式を保有している状態などをいう）。

格付機関は、従業員に対して、利害抵触の可能性のある状況を提示させなければならない（提示すべき状況には下記を含む）。

- ・ 格付対象者及び格付対象者と関係を有し利害抵触の可能性のある企業の有価証券等の保有（集団投資スキーム持分を除く）
- ・ 格付対象者との間における、雇用又は他の重要な事業上の関係の存在
- ・ 格付対象者に現在勤務している直系親族の存在
- ・ その他、利害抵触の可能性のある現在または過去の関係

格付業務に携わる従業員及び経営層は、格付対象者及び格付対象者と関係を有し利害抵触の可能性のある企業の有価証券等を取引してはならない（集団投資スキーム持分を除く）。

3.8 債務及び財務

格付機関は、格付業務の実施に伴うリスクを評価し、それらに起因して債務が発生することが合理的に見込まれる場合には、当該債務の種類・規模・数等に応じて、当該債務を担保できる適切な対応の処置（例えば、保険加入又は、資本金、準備金の積立て、一定金額の資本金・準備金の維持、格付契約上の手当て）を講じなければならない。

格付機関は、自身の財務及び収入源を評価し、商業的、財務的又はその他の圧力によって公平性が損なわれていないことを公平性委員会に対して継続的に実証しなければならない。

3.9 情報セキュリティ

格付機関は、情報セキュリティ基本方針をすべての関連する従業員に周知し、必要な場合には、その他の関係者にも周知しなければならない。

格付機関は、情報セキュリティ基本方針の要求事項を実施するため、及び格付に関連

するリスクマネジメントのために、適切なセキュリティ管理策を運用しなければならない。

格付機関は、管理策に関係するリスク、及び管理策の運用・維持方法を含め、セキュリティ管理策を文書化しなければならない。

経営層は、格付機関の情報セキュリティ基本方針を承認しなければならない。

3.10 苦情への適切な対応

格付機関は、格付対象者又は格付対象者の利害関係者等の他の当事者から受けた苦情を取り扱う手順を文書化しなければならない。

格付機関は、苦情に伴う処置を記録し保管しなければならない。

格付機関は、その際に、透明性と機密保持の間での適切な均衡を図らなければならない。

3.11 異議申し立て

格付機関は、異議申し立てを受理し、評価し、及び対応を決定するための手順を定めて文書化しなければならない。

格付機関は、異議申し立ての処理手順の概要を公表しなければならない。

格付機関は、異議申し立ての提出、調査及び決定によって、申し立てをした者に対する差別的行動を行ってはならない。

格付機関は、格付を実施した者と異なる者を異議申し立ての処理に従事させなければならない。

格付機関は、異議申し立てに対する決定を、異議申し立て対象に関与しなかった者によって行うか、又は見直し及び承認しなければならない。

4. 組織運営機構に対する要求事項

4.1 組織構造及びトップマネジメント

格付機関が属する法人及び格付機関は、経営層、アナリスト及び委員会の責務、責任及び権限を示す組織構造を文書化しなければならない。

格付機関が属する法人及び格付機関は、次の各事項に関する包括的な権限及び責任を有するトップマネジメントを特定しなければならない。

- ・ 格付機関の運営に関する方針の策定
- ・ 方針及び手順の実施の監督
- ・ 格付業務及びスキームの開発
- ・ 格付のパフォーマンス並びに苦情への適切な対応
- ・ 格付に関する決定
- ・ 必要に応じて特定の活動を委任するための、委員会又は個人への権限の委譲

- ・ 契約上の取決め
- ・ 格付業務に対する適切な資源の提供

格付機関は、格付業務にかかわる委員会への委任事項、運営及び委員の任命に関する正式な規則を有しなければならない。

4.2 公平性委員会

格付機関は、次の事項を行う委員会を設置しなければならない。

- ・ 公平性にかかわる方針の策定を支援する
- ・ 利害関係による偏った又は他の考慮を許すような傾向を抑制する
- ・ 透明性及び一般社会の認識も含む、格付の信頼性に影響する問題について助言する
- ・ 格付及び意思決定プロセスの公平性についてレビューする

格付機関は、委員会の構成、委任事項及びメンバーの責務、権限、力量並びに委員会の責任を正式に文書化しなければならない。

- ・ 単一の利害関係者だけが支配的にならないための均衡のとれた利害関係者の代表による構成
- ・ 委員会の機能を果たすために必要なすべての情報に、格付対象者との機密保持契約、及び機密保持等の格付機関が定める規程に反しない範囲でアクセスできる権限
- ・ 助言が尊重されない場合で、かつ、社会通念上、妥当な助言と認められる場合に、独自の行動をとる権利、など

4.3 格付委員会

格付機関は、独立かつ公正な格付を期するため、格付を決定する唯一の機関として格付委員会を設けなければならない。

格付委員会は、格付に当たっては、外部からのあらゆる圧力、干渉を排除し、独立を堅持しなければならない。

5. 資源に対する要求事項

5.1 経営層及びアナリストの力量

格付機関が属する法人及び格付機関は、経営層及びアナリストによって実施される機能を定めなければならない。

格付機関は、格付の専門分野及び格付業務における必要な力量を定めなければならない。

格付機関は、力量を実証する方法を定めなければならない。

格付機関は、アナリストが、格付プロセス、基準等に精通していることを確実にしなければならない。

格付機関は、アナリストが、格付の種類及びそれが運用される地域に関する適切な知

識を有することを確実にしなければならない。

アナリストは、専門分野及び地域に関する助言が得られる専門知識にアクセスできなければならない。

格付の付与、更新、範囲の拡大・縮小、中止を決定するグループ又は個人は、該当する基準等を理解し、格付プロセス及び格付チームの勧告を評価する、実証された力量を有しなければならない。

5.2 格付に関するアナリスト

5.2.1 一般

格付機関は、格付方法や手順等を管理し、信頼を与える格付を提供するために、十分な力量を持つアナリストを自身の組織の一部として持たなければならない。

格付機関は、格付チームのリーダーを含む十分な人数のアナリスト及び技術専門家を雇用するか又はいつでも利用できるようにしなければならない。

格付機関は、各関係者にその責務、責任及び権限を明確に示さなければならない。

格付機関は、アナリスト及び技術専門家が力量を持つことを実証した範囲に限定して、それらのアナリスト及び技術専門家を起用しなければならない。

格付機関は、格付業務に関するすべてのアナリストによる的確な業務の実施を確実にしなければならない。

5.2.2 教育・訓練

格付機関は、アナリストの選定、教育・訓練、正式な承認及び技術専門家の選定に関するプロセスを明確にしなければならない。

格付機関は、教育・訓練の必要性を特定し、特定の教育・訓練を提供するか又はそのような教育・訓練へのアクセスを提供しなければならない。

格付機関は、アナリストが、必要な教育実績、業務経験、訓練実績を有することを確認しなければならない。

格付機関は、筆記、口述、実技、観察又は他の手段で、アナリストの力量を試験しなければならない。

5.2.3 監視

格付機関は、関与するすべてのアナリストのパフォーマンスを監視し測定するための文書化された手順を備えなければならない。

格付機関は、アナリストのパフォーマンスを定期的に観察しなければならない。

格付機関は、アナリストの力量をその実績に照らしてレビューしなければならない。

アナリストに対する監視の手順は、現地での観察、報告書のレビュー及び格付対象者又は市場からの情報を組み合わせなければならない。

格付機関は、アナリストの継続的な力量を確認する公平な評価が行われていることを保証するための適切な手順及び条件を備えなければならない。

5.3 個々の外部アナリスト及び外部技術専門家の起用

格付機関は、外部アナリスト及び外部技術専門家に、格付機関が定める方針及び手順に従うことを誓約する同意書を要求しなければならない。

上記の同意書では、機密保持、営業上及び他の利害関係からの独立性を取扱い、格付を担当する可能性のある組織との現在又は過去の関わりを通知するように要求しなければならない。

(この同意書の下でアナリストを起用することが外部委託には該当しない)

5.4 アナリスト及び技術専門家の記録

格付機関は、アナリスト及び技術専門家の力量の記録を維持しなければならない。

格付機関は、関連する資格、教育・訓練、経験、所属、専門的地位、力量及び過去に提供した関連するコンサルティングを含む、最新の記録を維持しなければならない。

5.5 外部委託

格付機関は、外部委託をしてもよい条件を明確にするプロセスを有しなければならない。

格付機関は、機密保持及び利害抵触を含む各種取り決めを内容とする、法的に拘束力のある合意を締結しなければならない。

格付機関は、格付の付与、更新、範囲の拡大・縮小、中止の決定は、決して外部委託してはならない。

格付機関は、次の事項を実施しなければならない。

外部委託したすべての活動に対して責任を負うこと

委託先及びその担当者が、力量、公平性及び機密保持を含む、この規格の該当する規定にも適合することを確実にすること

委託先及びその担当者が、格付対象者と関わりを持たないことを確実にすること

格付機関は、委託先を適格と判断し、監視するための文書化された手順を有しなければならない。

6. マネジメントシステムに対する一般要求事項

6.1 一般

格付機関は、本文書の要求事項の順守を支援及び実証するため、マネジメントシステムを確立、文書化、実施及び維持しなければならない。

トップマネジメントは、格付機関の活動のための方針及び目標を確立及び文書化しな

なければならない。

トップマネジメントは、本文書の要求事項に従ったマネジメントシステムを開発し実施する事に対するコミットメントの証拠を提供しなければならない。

トップマネジメントは、この方針が格付機関のすべての階層において理解、実施及び維持されることを確実にしなければならない。

トップマネジメントは、経営層の中から、他の責任とかわりなく、次の事項を含む責任及び権限をもつ者を任命しなければならない。

- ・ マネジメントシステムに必要なプロセス及び手順の確立、並びに実施及び維持を確実にする
- ・ マネジメントシステムのパフォーマンス及び改善の必要性に関して、トップマネジメントに報告する

6.2 マネジメントシステムマニュアル

格付機関は、本文書の該当するすべての要求事項を、マニュアル又は関連文書で取り扱わなければならない。

格付機関は、すべての関係する要員が、マニュアル及び関係文書を利用できることを確実にしなければならない。

6.3 文書管理

格付機関は、本文書の履行に関係する文書（内部及び外部文書）を管理するための手順を確立しなければならない。

格付機関は、次の事項を手順の中で定めなければならない。

- ・ 発行前に、適切かどうかの観点から文書を承認する。
- ・ 文書をレビューする。また、必要に応じて更新し、再承認する。
- ・ 文書の変更の識別及び現在の改訂版の識別を確実にする。
- ・ 該当する文書の適切な版が、必要なときに、必要なところで使用可能な状態にあることを確実にする。
- ・ 文書が読みやすく、容易に識別可能な状態であることを確実にする。
- ・ どれが外部で作成された文書であるかを明確にし、その配布が管理されていることを確実にする。
- ・ 廃止文書が誤って使用されないようにする。また、これらを何らかの目的で保持する場合には、適切な識別をする。

6.4 記録の管理

格付機関は、本文書の履行に関係する記録の識別、保管、保護、検索、保管期間及び廃棄に関して、必要な管理方法を規定するための手順を確立しなければならない。

格付機関は、その契約上及び法的義務と整合する期間、記録を保持するための手順を確立しなければならない。

格付機関は、記録へのアクセスを機密保持の取り決めに整合させなければならない。

6.5 マネジメントレビュー

6.5.1 一般

トップマネジメントは、本文書の履行に関係する明示された方針及び目標を含めて、マネジメントシステムが、引き続き適切で、妥当で、かつ、有効であることを確実にするために、あらかじめ定められた間隔でレビューする手順を確立しなければならない。

トップマネジメントは、少なくとも年 1 回は、マネジメントレビューを実施しなければならない。

6.5.2 マネジメントレビューへのインプット

格付機関は、マネジメントレビューへのインプットに、次の情報を含めなければならない。

- ・ (情報セキュリティ基本方針を含む) 方針及び手順の適切さ
- ・ 内部監査等の監査の結果
- ・ 本文書の履行に関係する格付対象者及び利害関係者からのフィードバック
- ・ 公平性委員会からのフィードバック
- ・ 予防処置及び是正処置の状況
- ・ 前回までのマネジメントレビューの結果に対するフォローアップ
- ・ 目的の達成状況
- ・ マネジメントシステムに影響を及ぼす可能性のある変更
- ・ 異議申し立て及び苦情

6.5.3 マネジメントレビューからのアウトプット

格付機関は、マネジメントレビューからのアウトプットに、次の事項に関する決定及び処置を含めなければならない。

- ・ マネジメントシステム及びそのプロセスの有効性の改善
- ・ 本文書の履行に関係する格付業務の改善
- ・ 資源の必要性

6.6 内部監査

格付機関は、本文書の要求事項が履行され、また、マネジメントシステムが有効に実施及び維持されていることを検証する内部監査に関する手順を確立しなければならない。

い。

格付機関は、前回までの監査の結果だけでなく、監査対象のプロセス及び領域の重要性を考慮して、内部監査のプログラムを計画しなければならない。

格付機関は、少なくとも 12 ヶ月に 1 回は内部監査を実施しなければならない。

格付機関は、マネジメントシステムが本文書に従って継続して有効に実施されており、かつ、実績に基づく安定性を実証できる場合は、内部監査の頻度を減らすことができる。

格付機関は、次の事項を確実にしなければならない。

- ・ 内部監査は、格付、監査及び本文書の要求事項に関する十分な知識をもち、資格を与えられた要員によって実施する。
- ・ 監査員は、自らの仕事は監査しない。
- ・ 監査対象の領域に責任を負う要員に、監査の結果について知らせる。
- ・ 内部監査の結果生じる処置を、適時、かつ、適切な方法で行う。
- ・ 改善の機会があれば明確にする。

6.7 是正処置

格付機関は、その運営における不適合の特定及び管理のための手順を確立しなければならない。

格付機関は、不適合の再発を予防するため、必要な場合、不適合の原因を除去する処置をとらなければならない。

格付機関は、直面した問題の影響に対して適切な是正処置を実施しなければならない。

格付機関は、是正処置の手順において、次の事項に対する要求事項を定めなければならない。

- ・ 不適合の特定（例えば、苦情及び内部監査における）
- ・ 不適合の原因の決定
- ・ 不適合の修正
- ・ 不適合が再発しないことを確実にする処置の必要性についての評価
- ・ 必要とされた処置の決定及び適時の実施
- ・ 実施された処置の結果の記録
- ・ 是正処置の有効性のレビュー

6.8 予防処置

格付機関は、潜在的な不適合の原因を除去する予防処置をとるための手順を確立しなければならない。

格付機関は、潜在的問題から予測される影響に対して適切な予防処置を実施しなければならない。

格付機関は、予防処置の手順において、次の事項に対する要求事項を定めなければならない。

- ・ 潜在的不適合及びその原因の特定
- ・ 不適合の発生を予防する処置の必要性についての評価
- ・ 必要とされた処置の決定及び実施
- ・ 実施した処置の結果の記録
- ・ 実施した予防処置の有効性のレビュー

参考文献

[1] JIS Q 17021:2007 適合性評価—マネジメントシステムの審査及び認証を行う機関に対する要求事項

注記 対応国際規格：ISO/IEC 17021:2006, Conformity assessment-Requirements for bodies providing audit and certification of management systems (DT)

[2] JIS Q 20000-1:2007 情報技術—サービスマネジメント—第1部：仕様

注記 対応国際規格：ISO/IEC 20000-1:2005, Information technology-service management-Part1: Specification (IDT)

(了)