分類基準表

別表2

機密性の分類基準

区分	基準値	分類基準	対象となる情報資産	適用ガイド
厳秘情報【ラベリング対象】	3	情報漏洩時に社会的問題となる又は賠償問題に発展する可能性があるもの。 (組合員、一般利用者に影響が出るもの)	個人情報にあたる顧客情報 上記を格納するサーバ、アクセス可能なPC等端末、及びそのソフト	■ハードウェア等そのもの自体が情報でないものについては、そのもの自体のほかそれらが扱う情報にも着目して評価すること。
社外秘情報【ラベリング無し】	2	JA(農協)等取引先に影響を及ぼす。 (組合員、一般利用者に直接は影響が出ないもの)	社員情報、顧客団体の経営情報 上記を格納するサーバ、アクセス可能なPC等端末、及びそのソフト	
	1	情報が漏洩しても大きな問題とならない。	上記以外の情報	

完全性の分類基準

区分	基準値	分類基準	対象となる情報資産	適用ガイド
非常に高い	3	情報が変更及び改ざんされた場合、ビジネスへの影響が甚大かつ重大であるもの	個人情報にあたる顧客情報　等 上記を格納するサーバ、アクセス可能なPC等端末、及びそのソフト	■ハードウェア等そのもの自体が情報でないものについては、そのもの自体のほかそれらが扱う情報にも着目して評価すること。
高い	2	情報が変更及び改ざんされた場合、ビジネスへの影響が大きいもの	上記のうち利用範囲が限定的なもの・複写等原本でないもの、社員情報、JA情報、ソースプログラム、仕様書、契約書等 上記を格納するサーバ、アクセス可能なPC等端末、及びそのソフト	
低い	1	情報が変更及び改ざんされた場合、ビジネスへの影響がほとんどないもの	上記のうち利用範囲が極めて限定的なもの・複写等原本でないもの、上記以外の情報資産	

可用性の分類基準

区分	基準値	分類基準	対象となる情報資産	適用ガイド
非常に高い	3	60分以内に利用可能にしなければならない情報資産	オンライン処理、ネットワーク(WAN,LAN)、統合ネットワーク等 上記を格納するサーバ、アクセス可能なPC等端末、及びそのソフト	■ハードウェア等そのもの自体が情報でないものについては、そのもの自体のほかそれらが扱う情報にも着目して評価すること。
高い	2	当日には利用可能にしなければならない情報資産	口振システム、日計等更新処理、期限付き登録処理　等 上記を格納するサーバ、アクセス可能なPC等端末、及びそのソフト	
低い	1	翌日以降に利用可能にしなければならない情報資産	上記以外(帳票システム等)	

分類基準表

別表2

重要度の分類基準

区分	評価値	分類基準	対象となる情報資産	適用ガイド
非常に重要	2	厳秘情報にあたるもの	個人情報にあたる顧客情報及び顧客団体の経営情報、自社の経営機密情報　等　（情報資産識別「A:情報」「G:プロセス」において使用）	
重要	1	社外秘情報にあたるもの	上記以外の情報　（情報資産識別「A:情報」「G:プロセス」において使用）	

脅威の評価基準

大きさ	評価値	評価基準	偶発的脅威の評価基準	適用ガイド
高	3	発生する可能性は高い 発生頻度は1ヶ月に1回以上である	通常の状態で発生する可能性が高い脅威	■偶発的脅威についても考慮すること。 ■現在講じられている対策内容を考慮して評価すること。 （地震という脅威は、耐震工事がされている場合とされていない場合では評価値は異なる。盗難という脅威は施錠管理ができている場合とできてない場合では評価値は異なる。）
中	2	発生する可能性は中程度である 発生頻度は1年以内に1回あるかないかである	特定の状況下もしくは特定の担当者の不注意で発生する可能性が高い脅威	
低	1	発生する可能性は低い 1年以内に発生する可能性は低い	通常の状態では発生する可能性は低い脅威	

脆弱性の評価基準

大きさ	評価値	評価基準	対象となる脆弱性の説明	適用ガイド
高	3	対策がほとんど施されておらず、いつでも脅威を顕在化させる事象を誘引する可能性がある脆弱性	技術的対策/物理的対策、管理的対策（手順の確立、文書化など）のいずれもほとんど施されていない状況 一般者が普通に実施可能な状況	■評価値＝2の例（脆弱性の例：具体的状況の例） ユーザID／パスワード管理の不備：ユーザIDを共用している（個人別管理ができていない）。 ユーザID／パスワード管理の不備：ユーザIDの見直しがなされていない。 ユーザID／パスワード管理の不備：ビルトインアカウントを使用している（有効になっている）。 バックアップ管理の不備：バックアップは採っているが、実際に使用できるか確認されていない。 予防点検の不備（保守契約の不備）：定期点検（保守）はしているが、その内容が明確でない。 予防点検の不備（保守契約の不備）：定期点検（保守）はしているが、その内容が十分か評価見直しされていない。 各種運用の不備：管理策は講じられているが、実運用において遵守状況が不十分。 ■上記事例の状況にあっても、別の対策により脆弱性が低減されている場合もある。（セキュリティUSBｷｰで個人別使用管理がされている等）
中	2	一部対策が施されているが、脅威が顕在化する可能性がある脆弱性	技術的対策/物理的対策、管理的対策（手順の確立、文書化など）において一部対策が施されているが、対策の追加、未対策の情報資産への対策の適用等が必要である状況 専門知識を持つ者、あるいは一般者でも調査を実施すれば可能な状況	
低	1	適切な管理策が施されていて、脅威がほとんど顕在化しない脆弱性	技術的対策/物理的対策、管理的対策（手順の確立、文書化など）が適切に施されている状況	