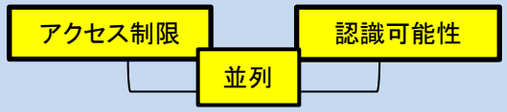
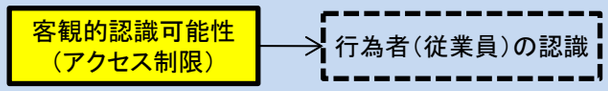
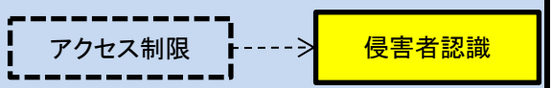
秘密管理性について（考え方の整理案）

（別紙1）

	A アクセス制限＝保護要件の一つ	B アクセス制限＝認識可能性確保の限度で必要（ただし、保護要件）		C アクセス制限＝立証手段
考え方	相当程度の秘匿措置がされた情報を保護 行為者の認識可能性が認められるだけでは足りず、相当程度の有形の（「客観的」な）秘匿措置がされた情報が法的保護に値する。（「穴」があってはならない） 	保有者の秘密管理意思が示された情報を保護 経済活動の安定性及びそのための情報接触者の情報識別性の観点から、通常情報に接する可能性のある者の認識可能性が生ずる程度に、企業の秘密管理意思が外形的に示された情報について、法的に保護する。 		侵害者が秘密と認識する情報を保護 侵害者への帰責性の観点から、具体的な行為者が秘密であると認識していた情報を法的に保護する。 （アクセス制限は、保護要件ではないが、行為者の認識を立証するために通常必要となるにすぎない。） 
当てはめ・必要なアクセス制限の程度	【原則】 ・どの程度のアクセス制限が必要となるかの基準がなく、必要となる具体的なアクセス制限の程度を内在的に決定できない。 【秘匿措置】 個別文書等に対する理想的な秘匿措置（※）に親和的。 ※パスワードの定期的変更、施錠管理の徹底等 （想定事例） ID・パスワードは限定した者に付与されていたが、紙媒体は施錠可能ではないところに保管されていたため秘密管理性を否定	【原則】 ・特定の情報について、企業の「秘密として管理」しようとする意思を従業員等（※）が容易に認識できるものを法的に保護。 ※ 職場環境において、通常、当該情報に接する可能性がある従業員又は業務委託先（この認識可能性の主体の範囲については下記２つを含め広狭考え方がありえるため、要検討）。なお、侵入者については、経済活動の安定性を考慮する必要がなく、ごく低いレベルの認識可能性が生ずる程度の秘匿措置で足りる、又は、そもそも侵入者の認識可能性は考慮せず、従業員等の内部者の認識可能性を考慮すれば足りる。 ・具体的な措置は、情報の性質、企業規模、情報に接する可能性がある者の種類等によって異なるが、標示、物的措置（保管、パスワード）、人的措置（就業規則、文書管理規則等）の組み合わせにより「対象の特定」とそれにふさわしい「取扱いの制限」がポイント。 **情報に接する可能性がある者の範囲（認識可能性の主体の範囲）の考え方の例** **①事実上、情報に接する可能性がある者（侵入者等の外部者は除く）** → 営業秘密保有者たる企業の従業員全員にとっての認識可能性 **②属する部署の職務上、情報に接する可能性がある者** → 当該情報を取り扱っている部署ごとに、当該部署内の全員にとっての認識可能性		【原則】 ・Bとほぼ同様 （実務においては、全ての従業員が秘密として認識する程度の秘匿措置を行うことが予想される）。 ・ただし、アクセス制限が全くなくとも、侵害者（個別の従業員）がたまたま秘密として認識する場合は、差止め等の対象としうる。 【秘匿措置の例】 ・Bとほぼ同様。
判断単位	【複数部署で共有ケース】 ・法人単位で判断。（一部部署でも不適切な管理だと、秘密管理性が否定） 【委託先と共有ケース】 ・委託先との関係では秘密保持契約の締結に加え、当該契約の実効性（監査等）を求める考えと親和的（委託先従業員の認識可能性も必要）。（委託元から漏えいした場合でも、委託先から漏えいした場合でも同様）	【複数部署で共有ケース】 ・法人単位で判断（一部部署でも認識可能性が不十分だと秘密管理性否定） 【委託先と共有ケース】 ・委託先など取引先との関係では、秘密範囲を特定した秘密保持契約の締結（秘密管理意思の表示）で足りる。（委託元から漏えいした場合） ※ 保有者に求められるのは合理的なアクセス制限であり、委託先の監査のように実行困難な措置を講じることは不要。 ※ 一部取引先との関係で秘密保持契約がされていない場合の取り扱いは、管理不徹底ケースに準じる。 ※ 委託先から漏えいした場合には、委託先の秘匿措置が問題となる。	【複数部署で共有ケース】 ・部署単位で判断（漏えいした部署における認識可能性が十分であれば秘密管理性肯定） 【委託先と共有ケース】 ・漏えいした部署における認識可能性に影響を及ぼさない限り、委託先との関係では特段の秘匿措置は不要。（秘密保持契約も不要） ※ 委託先から漏えいした場合には、委託先の秘匿措置が問題となる。	【複数部署で共有ケース】 【委託先と共有ケース】 ・いずれも、侵害者単位で判断。
管理不徹底	・全社的に共有された秘密について、一部部署の不適切な管理を理由として、全社的に秘密管理性が否定されうる（「穴がある」「相当程度の秘匿措置」が実行されていない）。	・一部部署において一時的又は偶発的に低レベルな秘匿措置が行われている場合であっても、必ずしも秘密管理性は失われない（あくまで、企業全体として認識可能性が十分か否かの問題となる）。	・部署単位で判断（漏えいした部署における認識可能性が十分であれば秘密管理性肯定）	・侵害者（個別従業員）の認識の問題。（少なくとも全社的に秘密管理性は喪失しない。）
留意点	・TRIPS協定の条文※より厳しい要件となる可能性があり、整合性については精査の必要。 ※注 39条１（ｃ）当該情報を合法的に管理する者により、当該情報を秘密として保持するための、状況に応じた合理的な措置がとられていること。	・TRIPS、不競法条文と整合的。		・「秘密として管理されている」という条文の文言と整合的ではない。 ・個別の従業員等の具体の「秘密」としての認識を問題とするため、秘密の外縁が確定困難（従業員等の予測可能性ないし取引の安定を阻害する可能性）。

（注）本稿にいう「アクセス制限」は、秘密マークの記載や秘密保持契約等も含む情報の秘密保持のために必要な管理（秘匿措置）をしていることを指す。