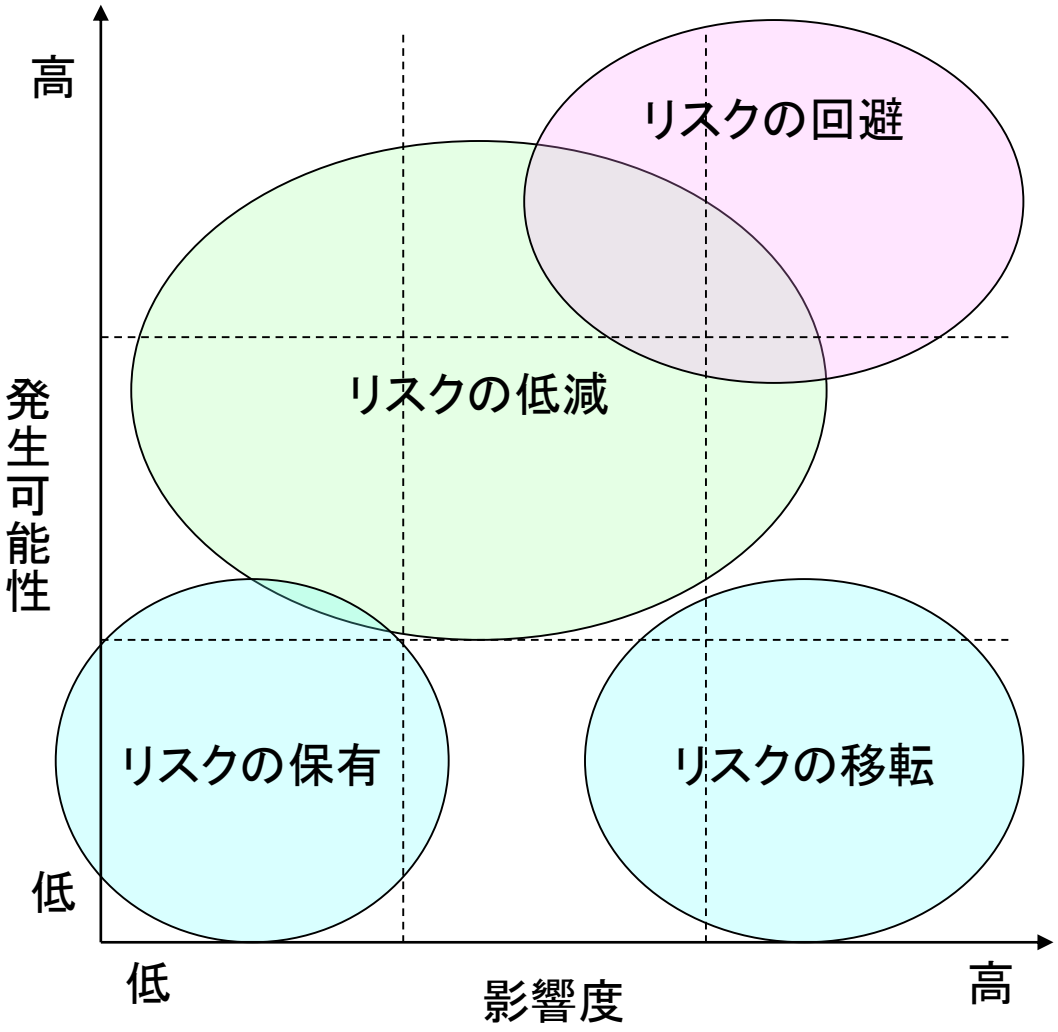
参考資料２

■リスク対応の考え方



リスクの影響度と発生可能性を評価し，
対応策を決める。
・考えられるリスクごとに，その影響度と
　発生可能性を評価する。

例（セキュリティ措置をしない場合の評価）
・なりすましによる準備書面提出
　　リスク影響度：中
　　リスク発生可能性：低
・準備書面の事後的改ざん
　　リスク影響度：高
　　リスク発生可能性：中
※ これらのリスク評価は例として記載した
　　もので，正確なものではない。

左図の引用元：
IPA「情報セキュリティ教本 改訂版」2009年.

■認証と署名

・文書作成者（提出者）が，自己の作成・提出を否認することがありうる。
・このような事態を防止する技術を，否認防止（non repudiation)という。
・公開鍵暗号に基づく電子署名（デジタル署名）は，否認防止の技術のひとつ。
・対象文書の重要性（否認のリスク)との関係で，メリハリのある方式選択が重要。

	特徴	方式例	紙の場合のイメージ
電子署名 Signature	本人による作成・申請を，第三者が確認できる。 事後にも確認が可能。	電子証明書を利用するデジタル署名（公開鍵暗号方式に基づく署名）	実印を押印した書面と印鑑証明書を受領
認証 Authentication	本人による作成・申請を，受領者が確認(*)	ID パスワードによる方式	個人番号カード等で本人を確認して（押印のない）書類を受領

(*) 第三者による確認（否認防止）のためには，そのための措置が必要

登録時(証明書発行時・ID付与時)の本人確認の保証レベル（Level of Assurance)も重要
・マイナンバーカードの署名機能を用いれば安全性は高い。
・ID-PWの付与時の本人確認方法は，そのIDの重要性により異なる。

※ 参考資料：各府省CIO連絡会議「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」，2010年8月.
https://www.kantei.go.jp/jp/singi/it2/guide/guide_line/guideline100831.pdf