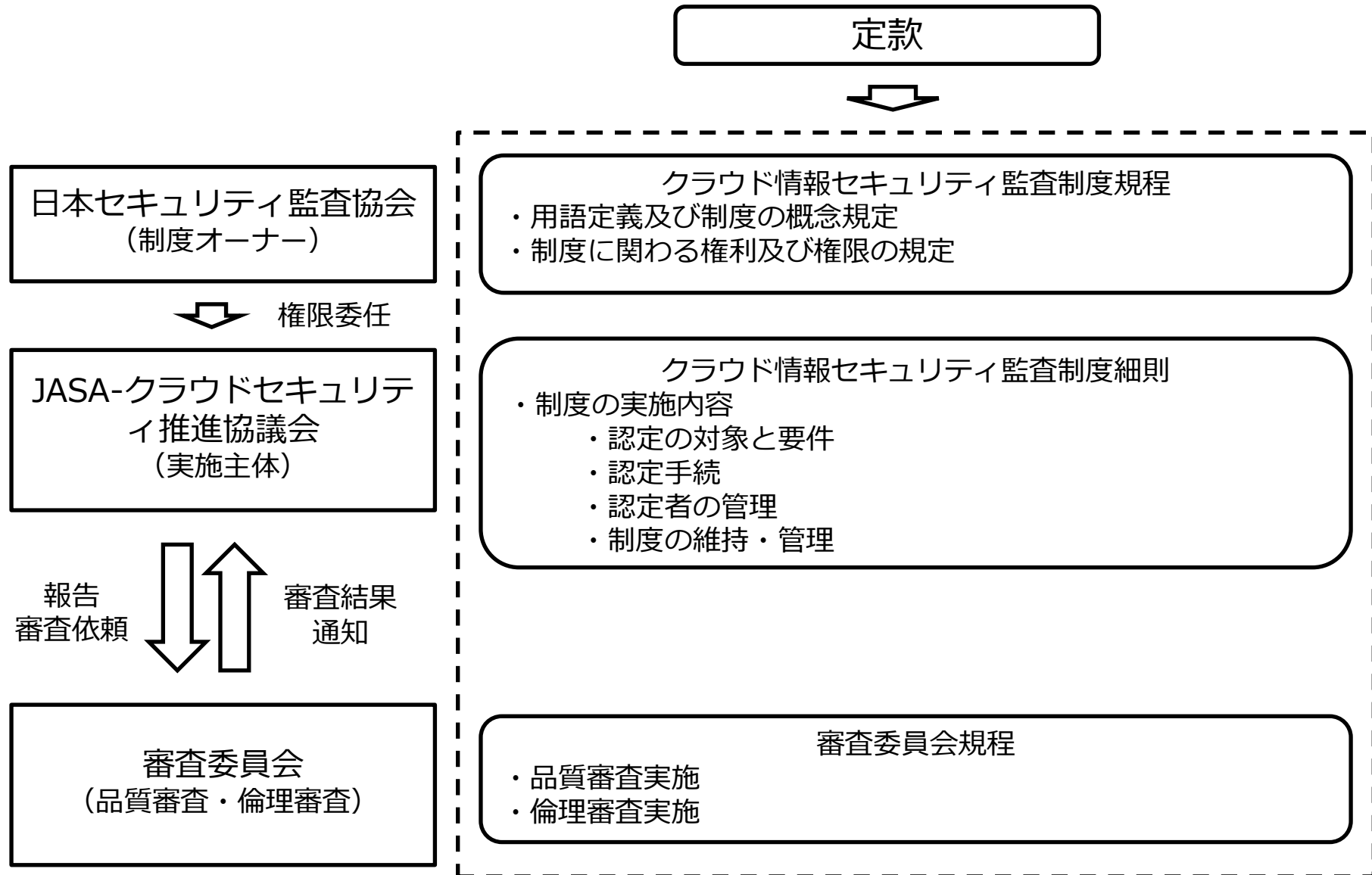




クラウド情報セキュリティ監査制度 細則解説書

2015年1月30日

1.組織間の関係（細則の位置づけ） 第1条関係



2.公開する資料

■ 一般の公開

【細則に明記されているもの】

- ① 基本リスク一覧(第2条)
- ② クラウド情報セキュリティ外部監査人の登録名簿（第4条）
- ③ 使用許諾の消滅したCSマーク（第21条）
 - ・ 公表の有無は、コア会議の決定に従う
- ④ クラウド情報セキュリティ管理基準（第29条）
（基本言明要件を含む：公表主体は経済産業省なので、許可が必要）
- ⑤ 経過期間（第29条）
 - ・ 基本リスク、クラウド情報セキュリティ管理基準及び監査標準手続の改訂時

【一般周知のためのもの】

- ⑥ CSマーク発行状況一覧（詳細は後述）

■ 会員への公開

- ⑦ 監査標準手続（第2条）
- ⑧ 外部評価手続（第2条）



3. 自主監査と適合監査（規程第4条）

- クラウド情報セキュリティ監査は自主監査と適合監査の2つがある
- 自主監査と適合監査の要件は下図の通りである
- 適合監査は自主監査のうち、外部評価等により標準としての監査であると認められたものをいう

自主監査

情報セキュリティ監査基準に準拠

クラウド情報セキュリティ管理基準に
準拠した管理策の実装・運用

クラウド情報セキュリティ監査人

監査人の独立性確保

監査標準手続に準拠した手続

所定様式での監査プロセスの記録

要件充足のアカウントビリティ
(3年間の根拠資料保存)

適合監査

クラウド情報セキュリティ外部監査人
による自主監査の評価

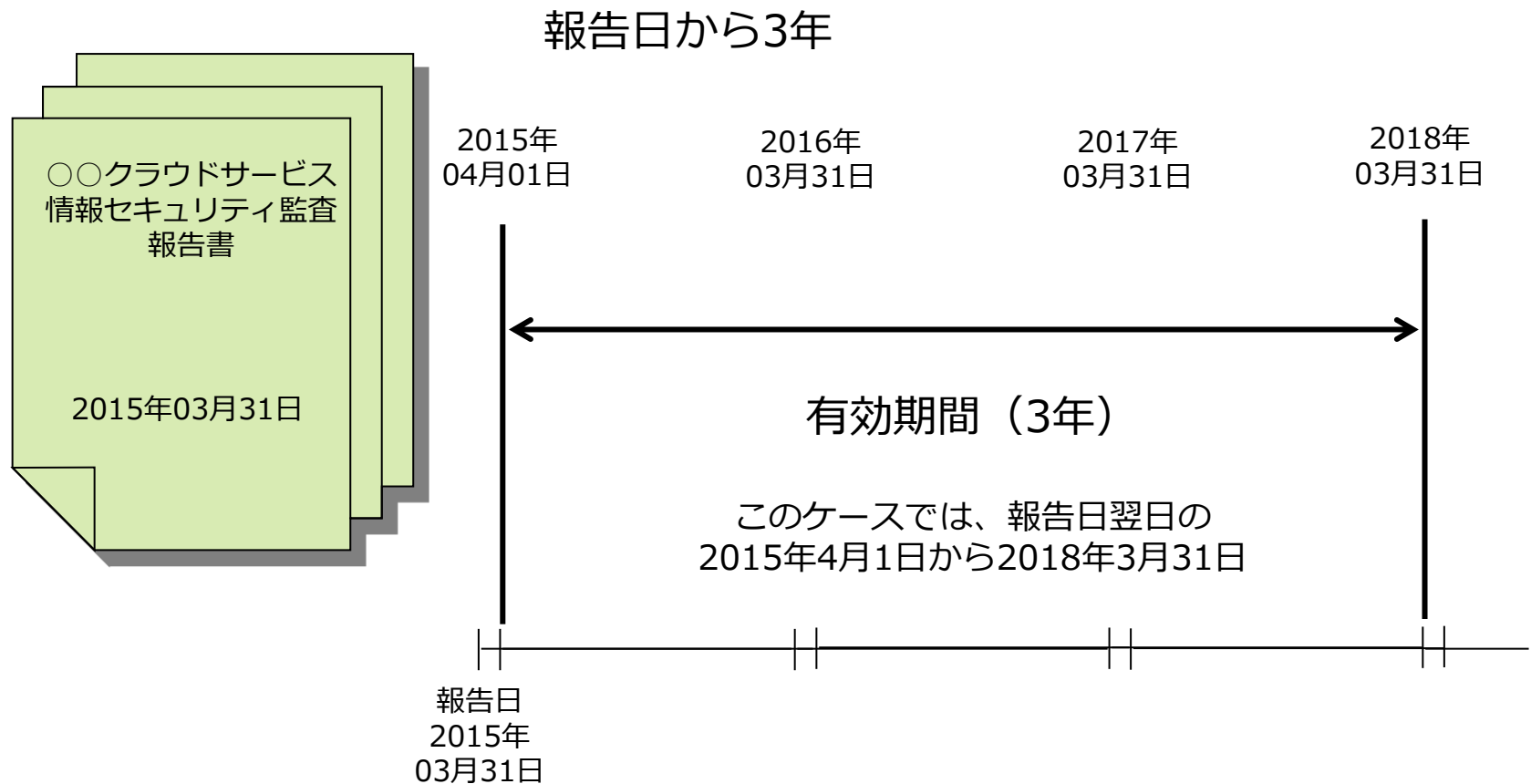
クラウド情報セキュリティ外部監査人
の独立性

協議会による適合性の評価



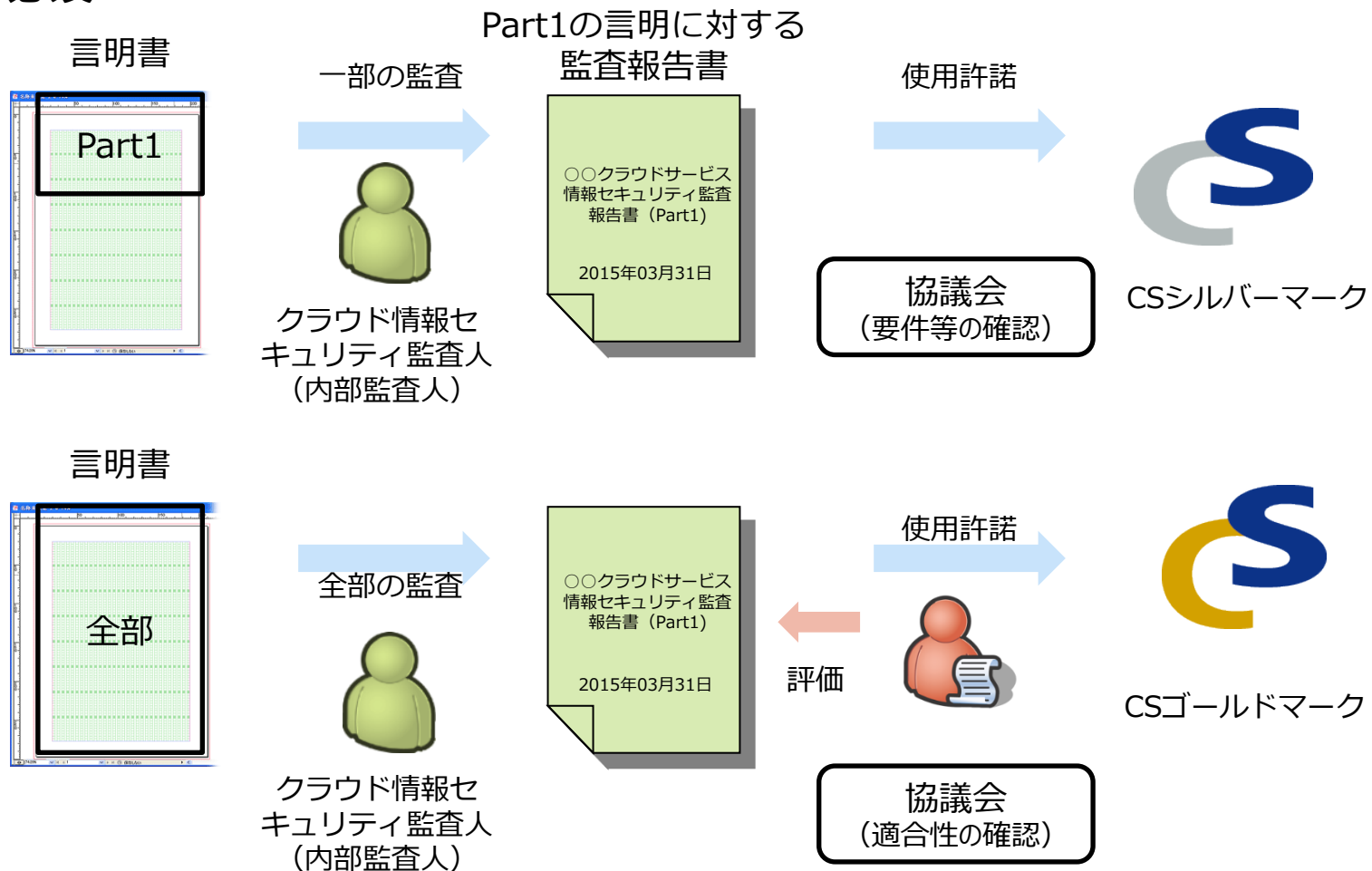
4. 期日の定義

- 期日は、民法の定めるところに従う。
- 「初日不算入の原則」が適用され、報告日の3年後の同日が期間の終了日となる。



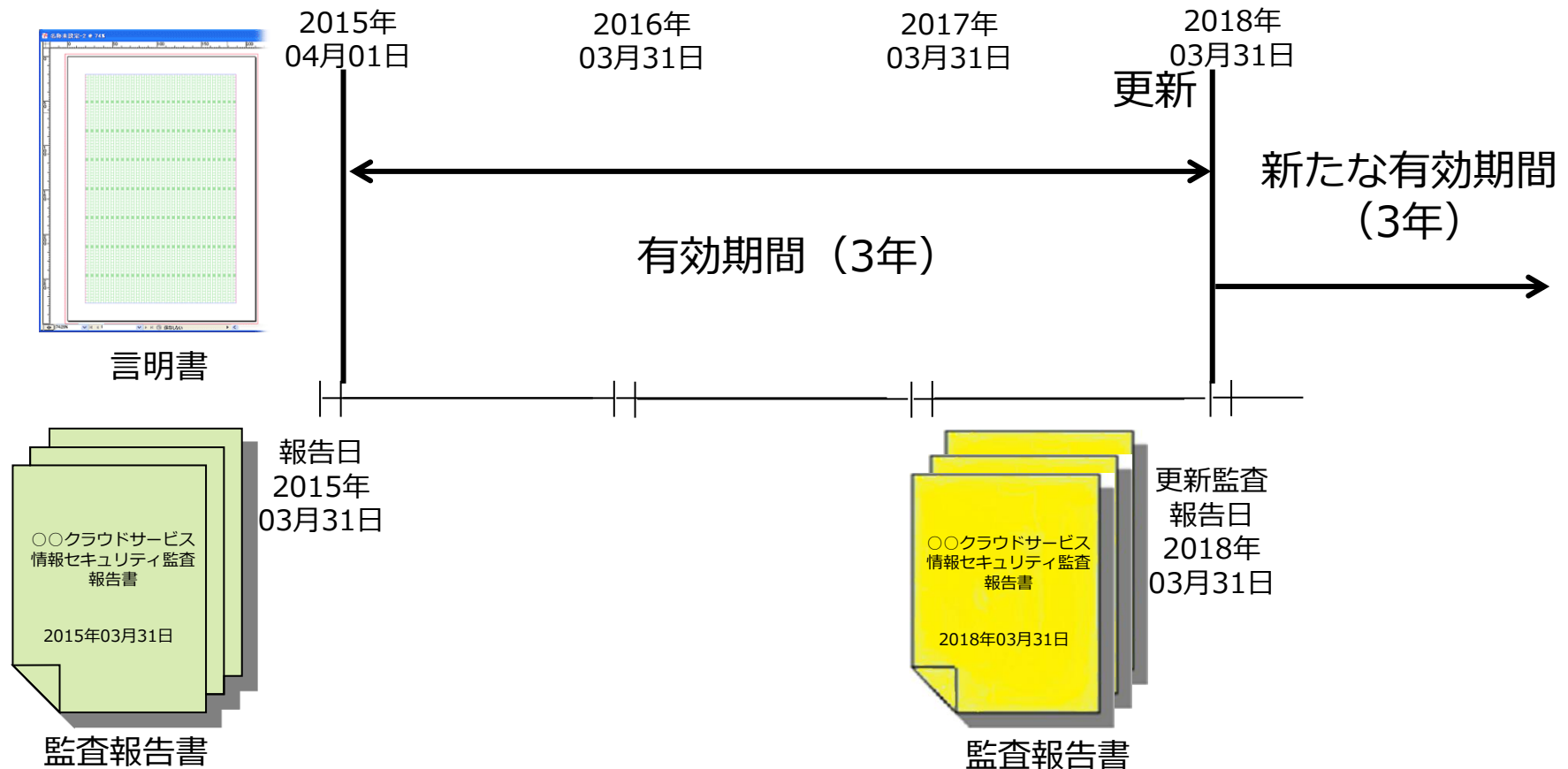
5. CSシルバーマークとCSゴールドマークの使用許諾

- CSシルバーマークは基本リスクの一部でも要件を満たせば使用許諾
- CSゴールドマークは全ての基本リスクに対する対策が行われていることが必須



6.CSマーク使用許諾の基本形

- 基本言明要件を全て満たした言明書 1 つに対して、1 つのCSマークが基本
- これを3年ごとに更新（細則第15条、16条）*



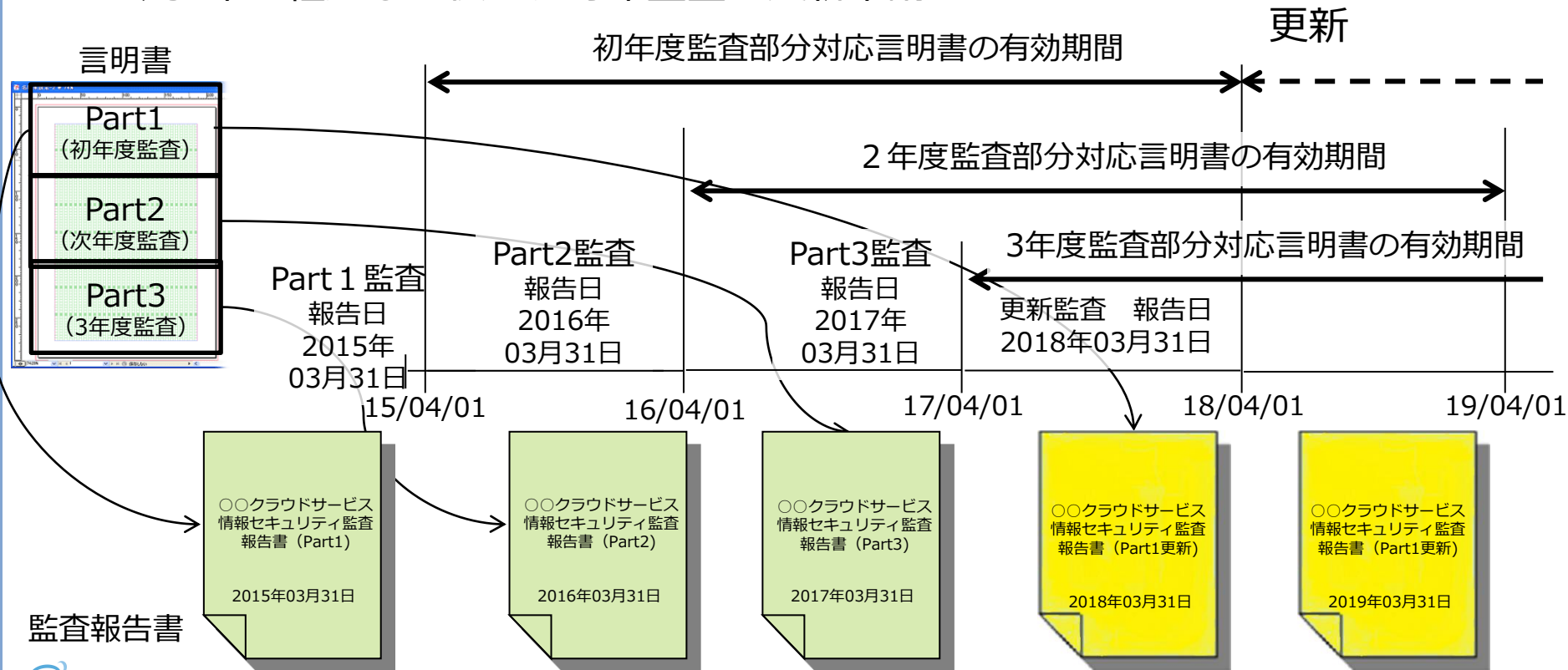
* 言明書の内容に変更があれば新規の使用許諾



7.リソースの制約がある自主監査場合（3カ年以内で分割可能）

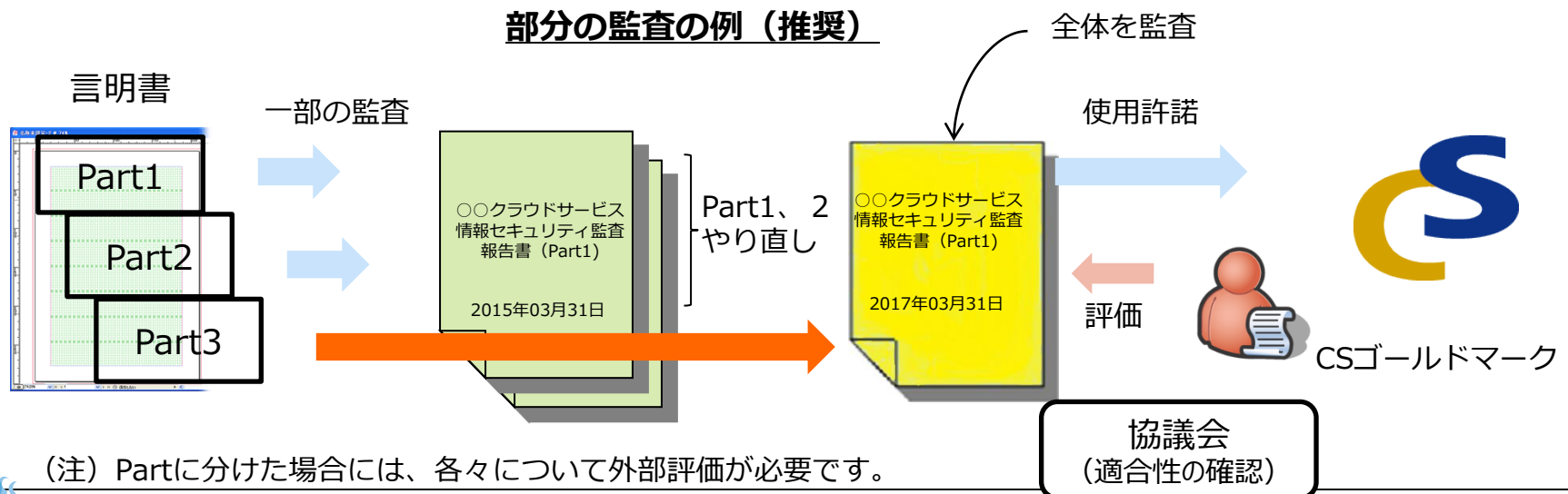
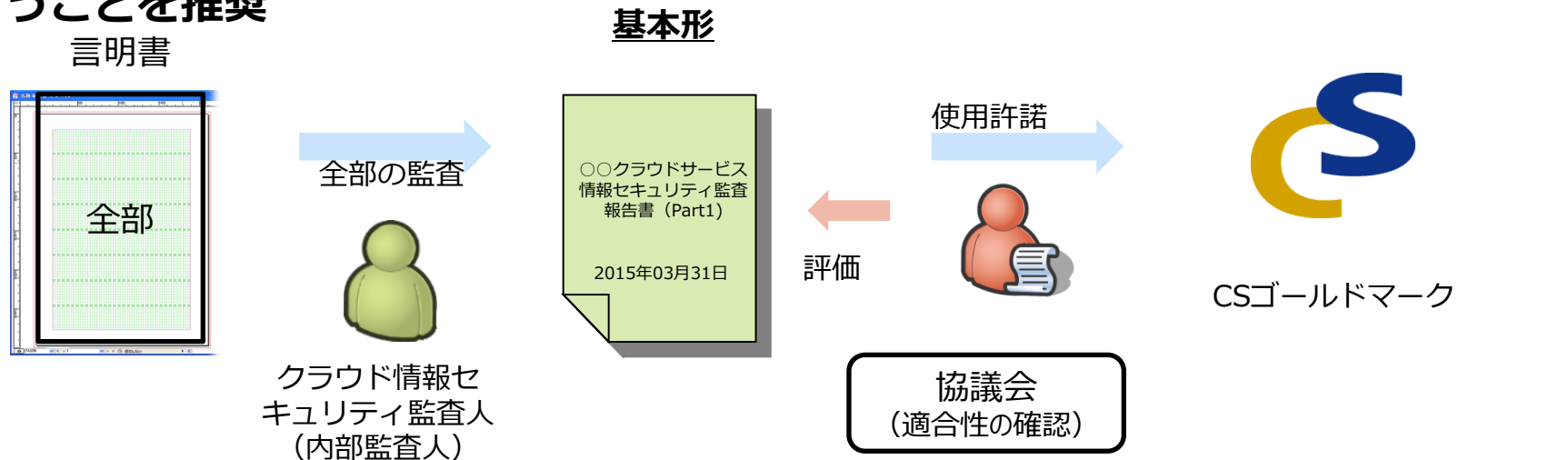
■ リソースの関係で基本言明要件を全て満たした状態に対して、3カ年で監査を分割して行う必要がある場合

- ▶ 3つの（部分）言明書に同じCSシルバーマーク（番号）を使用
- ▶ 2年度以降の部分ごとに、追加申請（第12条）
 - － 追加部分が、他の言明書の言明範囲と重ならないこと（第10条）
- ▶ 丸3年が経過した後は、毎年監査の更新申請



8. CSゴールドマークの使用許諾

- CSゴールドマークの場合は、全ての基本リスクに対する言明を一括して行うことを推奨



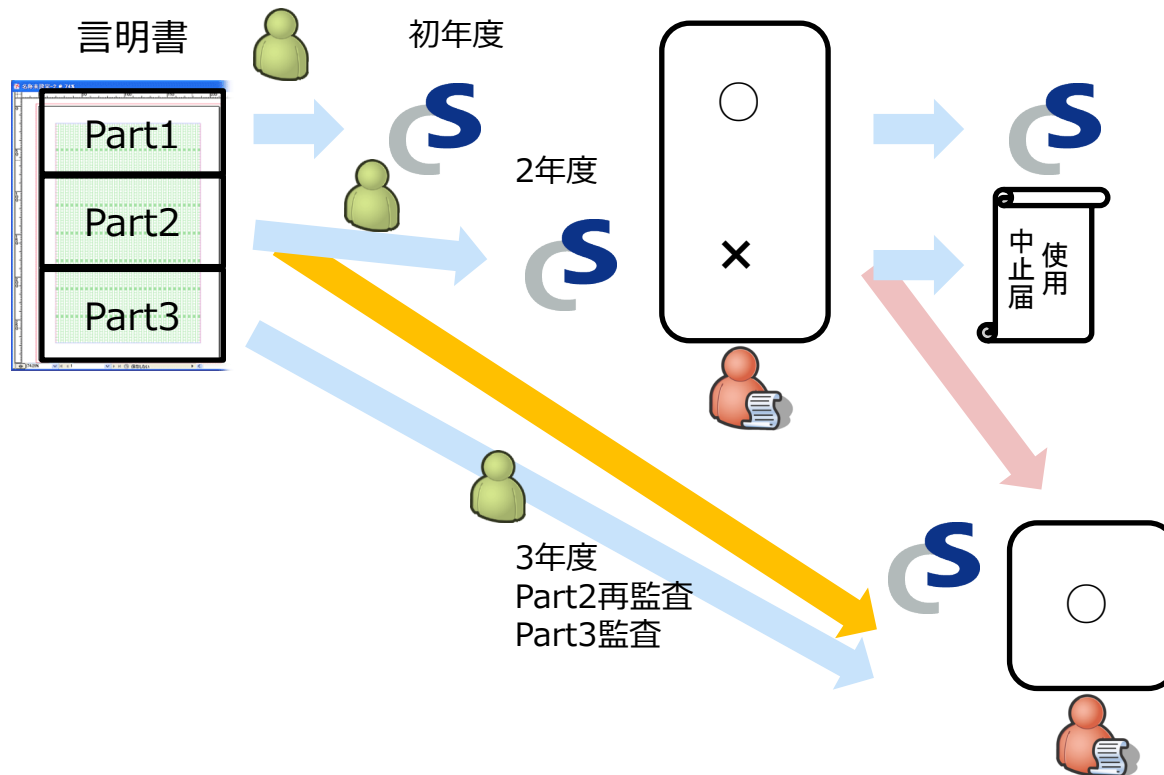
9. 使用許諾の独立と従属（複数年に分けた監査で使用許諾を申請）

- **CS ゴールドマークについては、一括した監査を推奨しています。**
 - ▶ただし、リソース等の制約により部分の監査を複数年に分けて行った場合にも、各々について外部評価手続を行い、すべての基本要件を満たしていることが確認できれば、CSゴールドマークの取得ができます。
- **CSゴールドマーク取得のためには、複数回に分かれようとも、基本言明要件のすべてに対する監査として、全部が一体のものとみなします。**
 - ▶仮に、3つの部分のうちの一つの部分が適合監査として認められない場合は、他の部分が適合性があると認められても、適合監査とは認められません。また、CSゴールドマークの使用も認められません。
 - ▶これが使用許諾の従属という意味です。
- **一方、CSシルバーマークでは、同一の使用許諾番号であっても、各々の部分は独立であり、差し替えが可能です。**
- **次ページで具体例を紹介します。**



9-2. 使用中止届の活用-使用許諾の独立と従属（利用例）

- (例) 3ヶ年計画で初年度、2年度のシルバーマーク使用許諾をとり、翌年ゴールドマークの取得を狙ったケースで、2年度目の監査が外部評価により、適合監査としては不十分であると評価された場合



シルバーマークは独立使用許諾なので、初年度分を3年度目も継続使用。2年度目は使用中止届を提出。

CSゴールドマーク

初年度目（Part 1）と3年度目（Part 2、3）を合わせて、ゴールドマークの使用許諾申請が可能。



9-2. 使用中止届の活用-使用許諾の独立と従属（利用例）

- Part2の部分は監査に瑕疵があることが分かったのでCSマーク使用規定の7.1 および細則第17条の2に基づき、使用中止届を出す必要があります。
- Part2が、外部評価などにより、適合性がないとみなされる場合でも、Part1 部分についてはシルバーマークの使用が継続できます。
 - ▶シルバーマークのでは、各言明が独立なので、Part 1 の言明に対するCSシルバーマークの使用には問題がありません。
- CSゴールドマーク取得のためには、3年度目に、Part2部分の再監査とPart3 を監査し、外部評価人の評価を受ける必要があります。そのうえでPart1と合わせてCSゴールドマークの使用許諾の申請をすることができます。
 - ▶Part2部分の使用をしていない場合、Part1とPart2及び3の言明範囲に、既存のPart2が重複してしまい、基本言明を分割したとはみなされません。このため、Part2 及び 3の部分は追加申請ではなく新規申請となります。その結果、Part1とPart2及び3 は二つの異なった言明とみなされ、ゴールドマークの申請の要件を満たさないことになります。
 - －（第10条 追加申請の対象）CSシルバーマークの使用対象となっているCS言明書に記載されたクラウドコンピューティングサービスに対して、当該CS言明書の範囲に含まれない基本言明要件を含む新たなCS言明書を作成した会員



【参考】 CSマークの使用と登録番号

■ CSマークの使用には以下の8つの内容が含まれる（CSマーク使用規定）

- ① 言明書にCSマークを付する行為。
- ② クラウドコンピューティングサービスの提供に当たりその提供を受ける者の利用に供する物（譲渡し、又は貸し渡す物を含む。以下同じ。）にCSマークを付する行為。
- ③ クラウドコンピューティングサービスの提供に当たりその提供を受ける者の利用に供する物にCSマークを付したものをを用いてクラウドコンピューティングサービスを提供する行為。
- ④ クラウドコンピューティングサービスの提供の用に供する物（クラウドコンピューティングサービスの提供に当たりその提供を受ける者の利用に供する物を含む。以下同じ。）にCSマークを付したものをクラウドコンピューティングサービスの提供のために展示する行為。
- ⑤ クラウドコンピューティングサービスの提供に当たりその提供を受ける者の当該クラウドコンピューティングサービスの提供に係る物にCSマークを付する行為。
- ⑥ 電磁的方法（電子的方法、磁気的方法その他の人の知覚によって認識することができない方法をいう。次号において同じ。）により行う映像面を介したクラウドコンピューティングサービスの提供に当たりその映像面にCSマークを表示してクラウドコンピューティングサービスを提供する行為。
- ⑦ クラウドコンピューティングサービスに関する広告、価格表若しくは取引書類にCSマークを付して展示し、若しくは頒布し、又はこれらを内容とする情報にCSマークを付して電磁的方法により提供する行為。
- ⑧ 上記②から⑤において、物にCSマークを付することには、クラウドコンピューティングサービスの提供の用に供する物又はクラウドコンピューティングサービスに関する広告をCSマークの形状とすることが含まれるものとする。

■ CSマークの記載される登録番号は、協会がCSマークの使用を許諾した言明書に対して、協議会が付与する登録番号



10. CSシルバーマークの公開例

サービス名 (企業名)	基 本 リ ス ク															監査年月		
																◎	○	●
	H 01	H 02	H 03	H 04	H 05	H 06	M 07	M 08	M 09	M 10	M 11	L 12	L 14	L 18	L 19	初 年 度	次 年 度	3 年 度
〇〇〇〇クラウド (△△△△株式会社)	◎	◎	○	◎	◎	○	○	○	○				○			27 04	28 04	
クラウド×××× (株式会社KKKK)	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	27 08		

