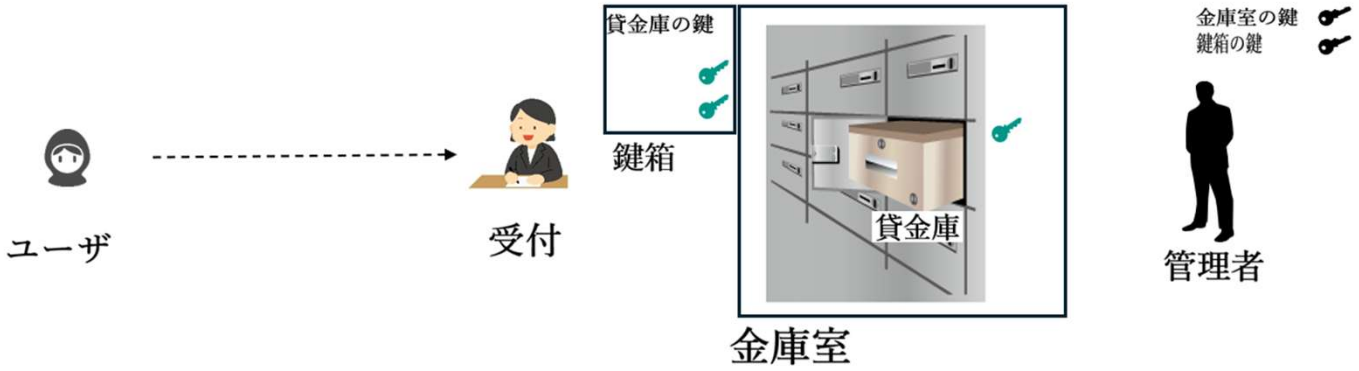
資料－４　電子契約サービスのセキュリティ比較（方式別イメージ）

＜貸金庫サービスに例えた比較＞



① **本RSSによる当事者署名（DTBS真正性保証：特許技術）**
DTBS真正性が**保証**される**リモート署名。**署名鍵は事業者のHSMに保管され、HSMで署名要求を検証する点は、④**SCAL2と同じ**。DTBSの真正性を検証し署名する**改良モデル**。**ランサムウェア**等の中間攻撃による**DTBS入替**が成立しない設計。（従来困難だったDTBS真正性を、実装・運用・監査のレベルで担保する）

受動型フリーアカウントのオプションで、署名要求に対し、相手も当事者型署名が可能となる。相手は、有料会員にならなくても署名応答が可能であり、従量課金（送信料、電子証明書発行料）の負担で済む。

貸金庫に例えると：マイナンバーカード認証を貸金庫に実装し、貸金庫の鍵とマイナンバーカード認証の両方が揃って開錠するモデル。銀行内部者だけでは**開錠**できない**貸金庫サービス**に匹敵。技術革新により低コストで運用負担も少ない。

② **立会人型の署名**（事業者鍵による署名：多数派）
メール等で本人の同意を確認し、契約書に事業者の鍵で署名する方式。幹事当事者に月額料と送信料が発生するが、相手当事者に費用発生がなく利便性が高い。しかし、**当事者の署名がない**。当事者の一方が否認した場合など、法的根拠が希薄であり、**重要な契約には不向き**。

貸金庫に例えると：金庫室内の棚（貸金庫はない）に番号札で保管し、ホテルのクローク方式に対応するモデル。
個別の金庫がないので、**高価な貴重品**の保管には不向きなサービス。

③ **当事者による署名**（リモート署名の原型：少数派）
当事者達の電子証明書によりリモート署名を付与する方式。契約の厳格性と本人性は格段に高いが、相手も有料会員になる必要がある（月額料と送信料が発生）。会員でない場合、月額料等を強いることが難点。
一方、署名鍵が事業者の管理下に置かれることから、内部不正の可能性が残る。 **（GMOサインが代表例）**

貸金庫に例えると：会員毎の貸金庫内に保管。会員証で鍵を受領し、本人が貸金庫を開錠するモデル。
個別の金庫に保管なので②に比べてはるかに安全。（貸金庫の費用が事業者の負担になる）
一方、貸金庫の鍵の管理不備や**内部不正**による開錠の取得する可能があるサービス。

④ **当事者による署名（SCAL2）**
当事者のリモート署名を付与する方式は③と同じ。署名鍵は、事業者のHSMに保管され、2要素による強固な認証と署名者の操作で鍵を活性化するモデル。当事者署名の厳格性と**本人性は非常に高い**。
一方、DTBS真正性検証がなく、内部の権限者又は**ランサムウェア**によるDTBSの**入替えリスクが残る**。

貸金庫に例えると：鍵箱からの鍵の取り出しに本人しか知らないPIN入力を必須とし、本人がのみが貸金庫を開錠できるモデル。社員や受付による鍵の取得はできないため、一般的な**内部不正からも強固に守られる**。
一方、**銀行内部の権限者**は、合鍵や鍵箱の鍵を使用して、貸金庫の開錠が可能であるサービス。