鍵管理とは

Rootゾーン鍵管理を例に
7/15/2011@JANOG 28

大久保　智史

Tomofumi Okubo

Cryptographic Key Manager, IANA / DNS Operations

Internet Corporation for Assigned Names and Number

鍵管理はなぜ必要か

その鍵に頼る全ての人の信用を得るため。
適切な鍵管理無くしては安全なインターネットは実現できない。

- 鍵を守る（鍵の危殆化の防止）
- 鍵の異常を把握する（鍵の危殆化の検知）
- 鍵の生成、使用、破壊に関する歴史的事実を証明する（監査証跡で証拠の連鎖を構成）

鍵管理とは

鍵管理とは、継続的に監査可能な状態を
維持しつつ、論理的、そして物理的に秘密鍵を危殆化から保護し、鍵のライフサイクルを管理する手法。

鍵管理とは

鍵管理とは、継続的に監査可能な状態を
維持しつつ、論理的、そして物理的に秘密鍵を危殆化から保護し、鍵のライフサイクルを管理する手法。

もう少しかみくだくと…

鍵管理とは

- 鍵の生成、使用、破壊に関する全ての記録をとること（＝キーセレモニーの実施）
- 記録が途切れないように管理をすること
- 鍵を物理的に保護すること
- 鍵を取り巻く環境を整備すること
- 方針や手順書などの文書の整備をすること
- 鍵管理に携わる人員を管理すること

鍵管理は多角的なアプローチが必要！

組織に最適な鍵管理

- リスクに基づいて決定する
- 資産の特定＞脅威の特定＞脆弱性の特定＞可能性の決定＞インパクト分析＞リスクの特定
- リスク分析に基づいてコントロールを決定する

つまりは…

組織に最適な鍵管理

- なにを守りたいのか
- それはどのような脅威にさらされているのか
- どのような弱点が考えられるのか
- どのような確率で起こりうるのか
- 起こったらどのような影響があるのか

を明確にして最後に、

- 弱点が攻撃を受けて脅威にさらされる確率とその影響を鑑みて、どうやって守るのかを決める！

組織に最適な鍵管理

リスクに基づいた鍵管理策の策定が有効なワケ

- 組織の規模、保護する資産の価値、予算にあわせて柔軟に設計できる
- リスク分析を行っているので、鍵管理プロセス構築のための予算が取りやすい（そう、計画と一緒に上役に提出するだけ！）
- 根拠が明確なので、意思決定が比較的容易

鍵管理の手法

- 職務の分轄（職務分掌）
- 複数人操作
  - M of N, Dual Occupancy, Dual Control, Two Person Integrityなど
- 最小権限の付与
- 連続障壁制限
- Need to Know
- 監査証跡を管理して、証拠の連鎖を維持する
- 監査（せめて内部でも…）

次にルートゾーンのKSK運用を例に説明します

Root KSKの鍵管理の場合

鍵管理における職務の分轄

- セレモニー管理者＝Ceremony Administrator
- 立会人　＝Internal Witness
- 金庫番　＝Safe Security Controller
- システム管理者　＝System Administrator
- 暗号員　＝Crypto Officer
- 鍵復鍵持ってる人　＝Recovery Key Share Holder
- 物理アクセス管理者
  ＝Physical Security Control Manager
- KSK運用セキュリティ
  ＝ICANN KSK Operations Security

管

立

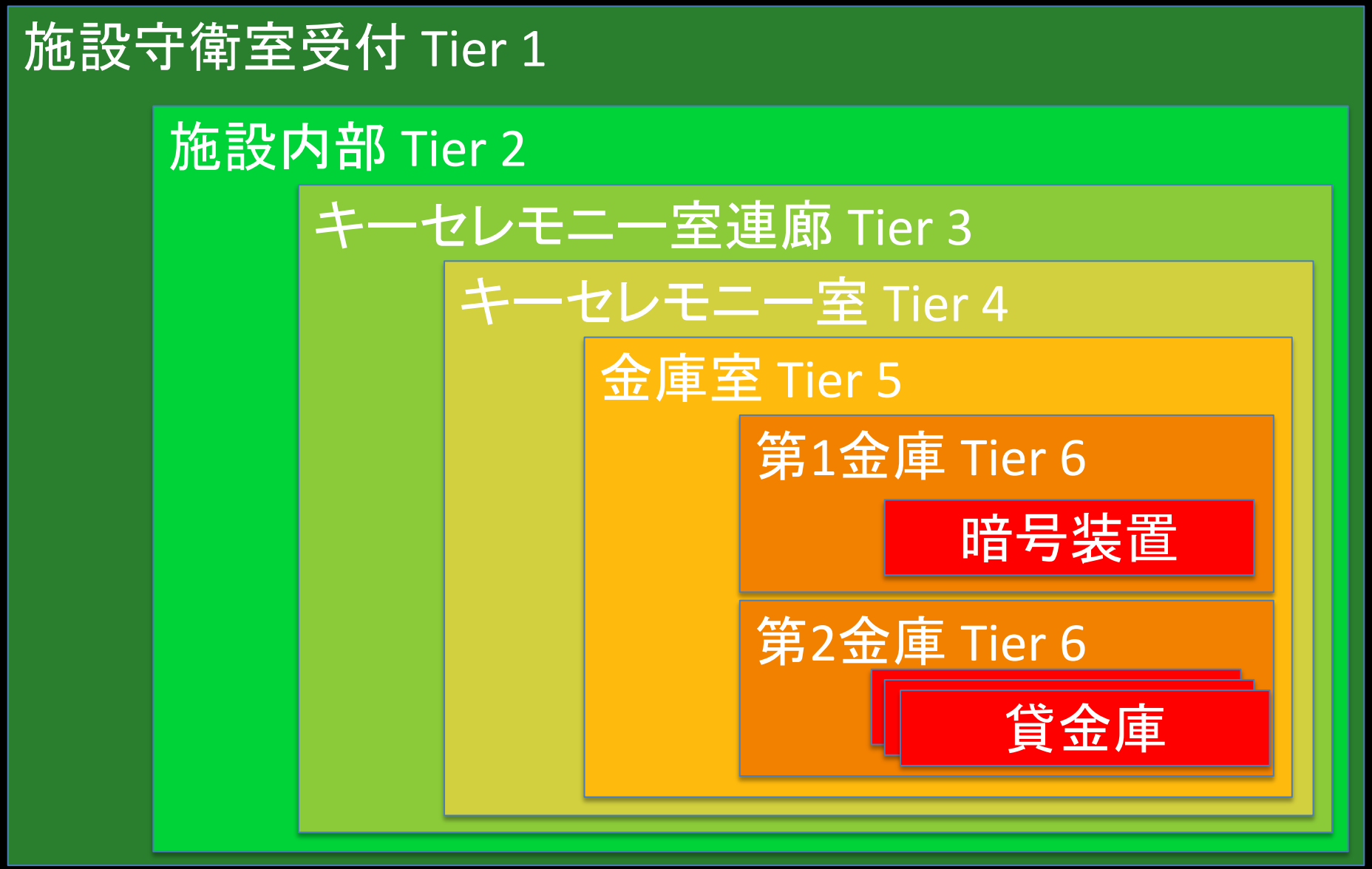
金

シ

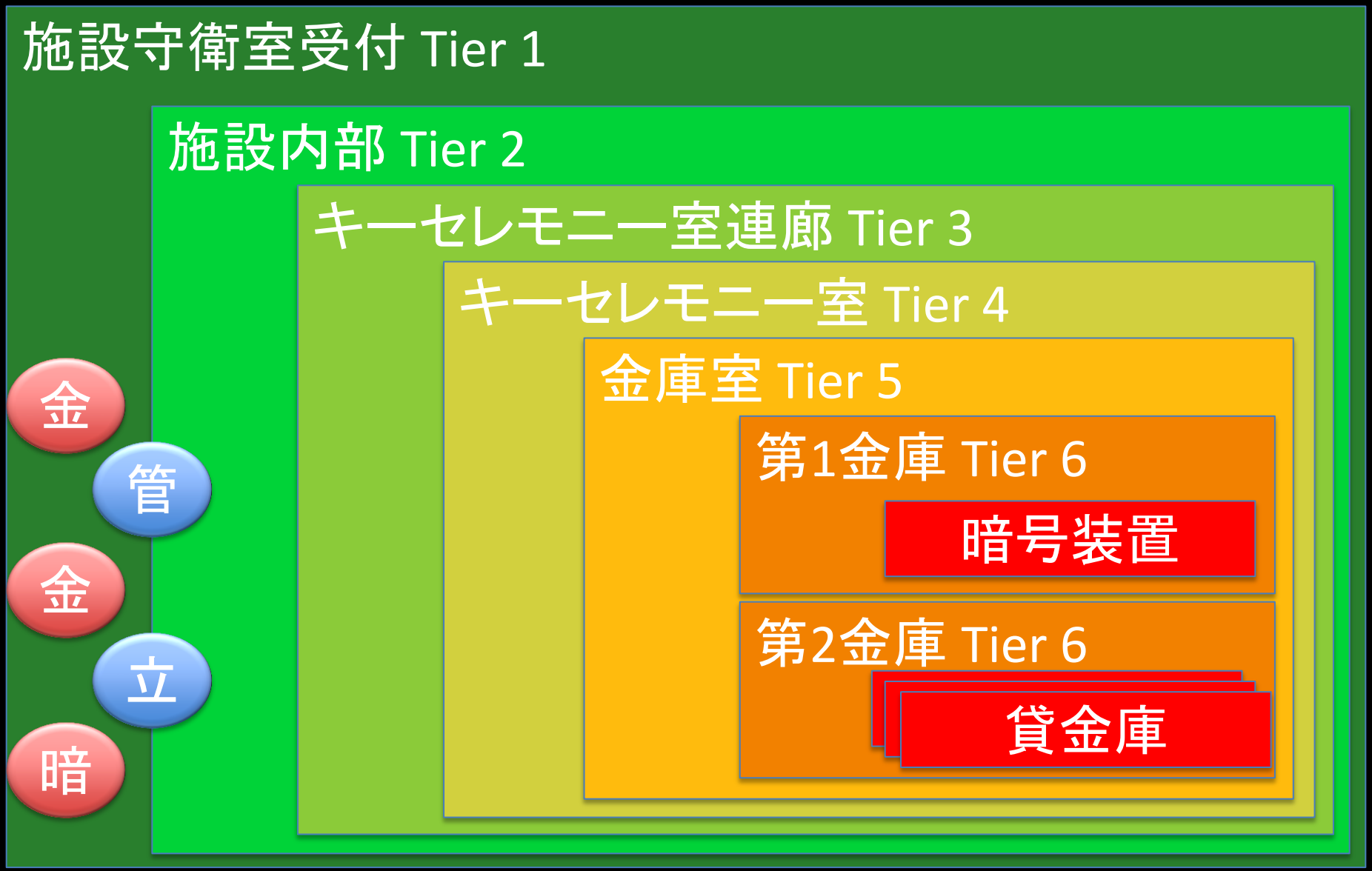
暗

私

Root KSKの鍵管理の場合

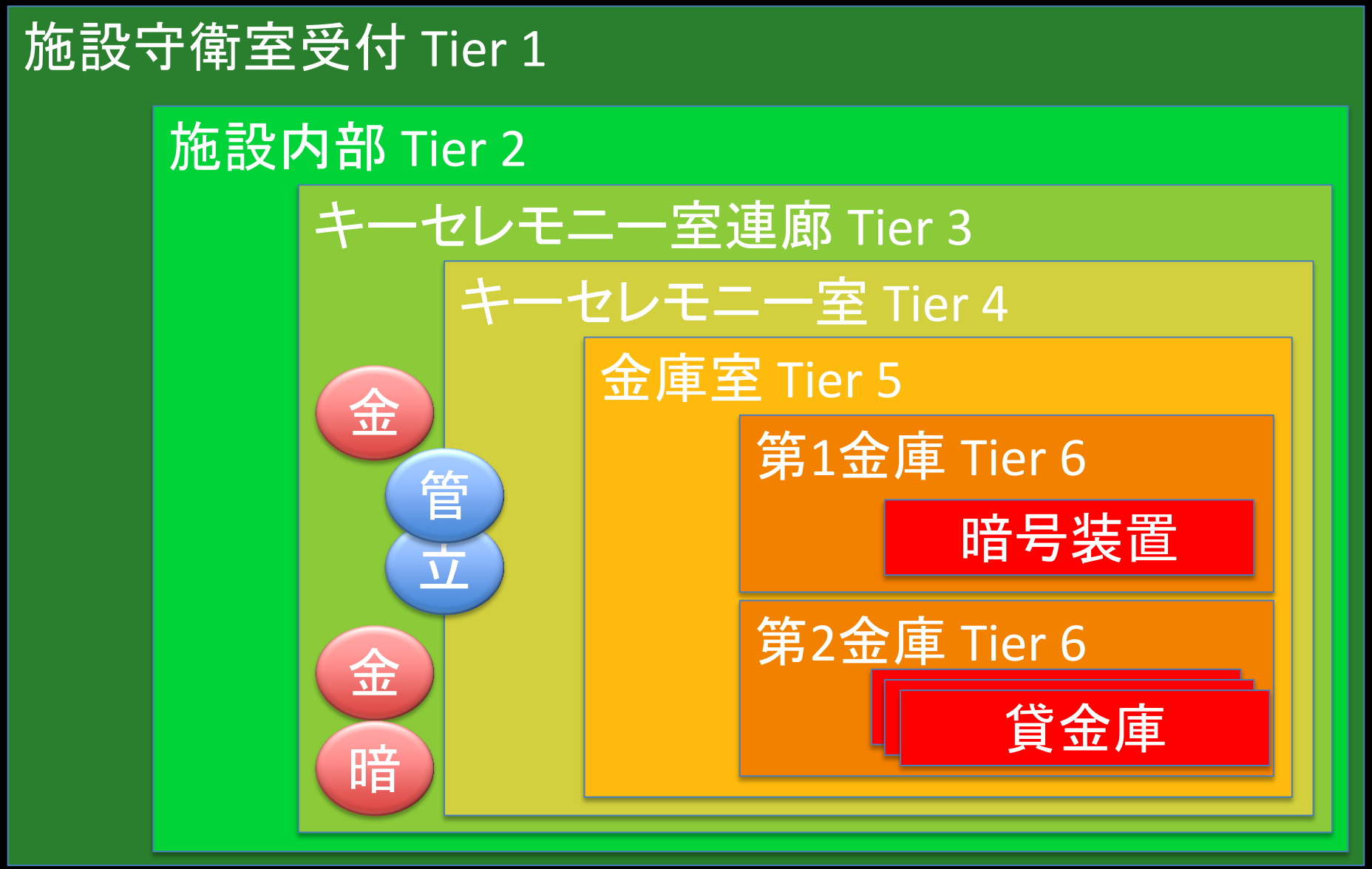


Root KSKの鍵管理の場合



Root KSKの鍵管理の場合

Root KSKの鍵管理の場合

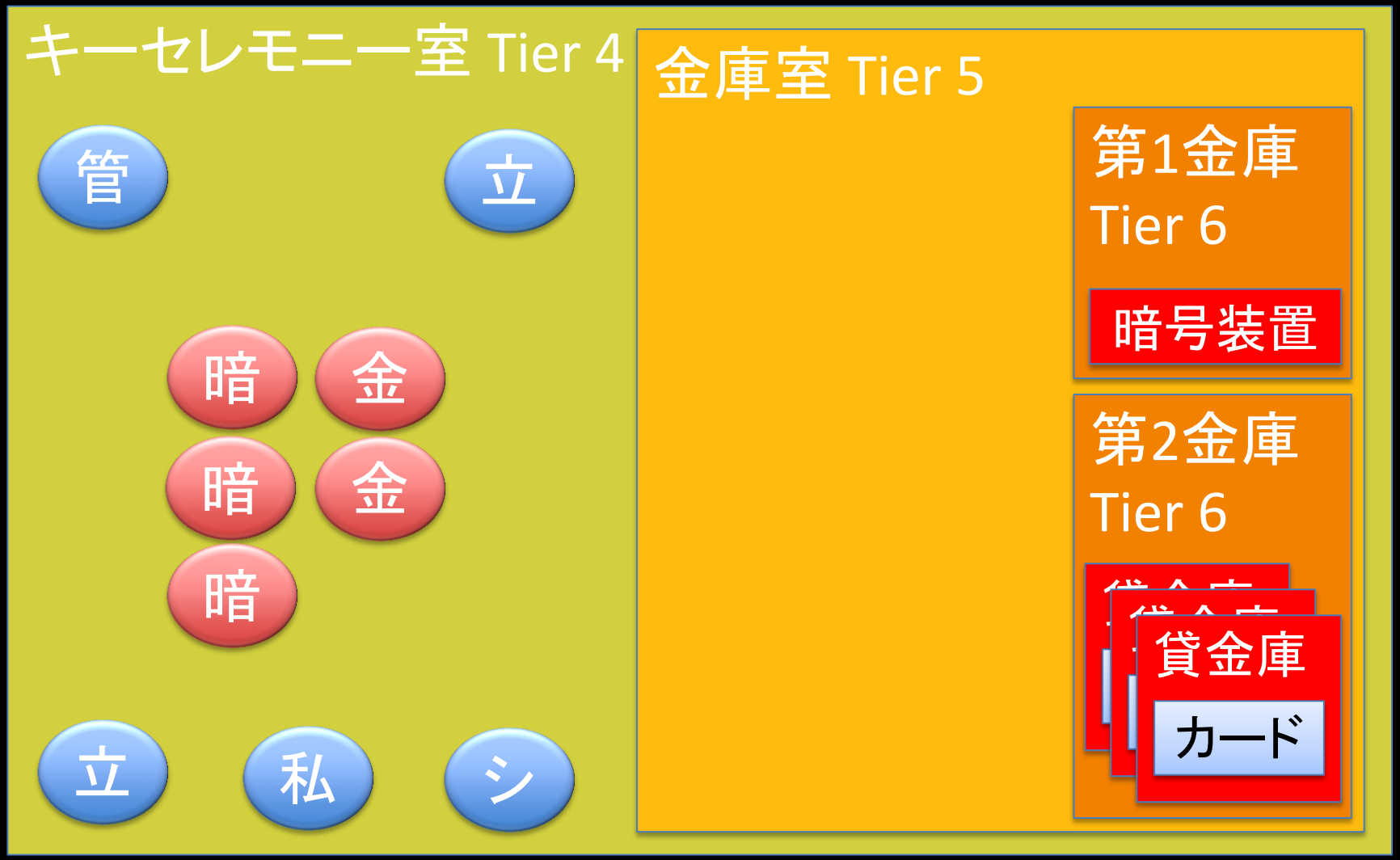


Root KSKの鍵管理の場合

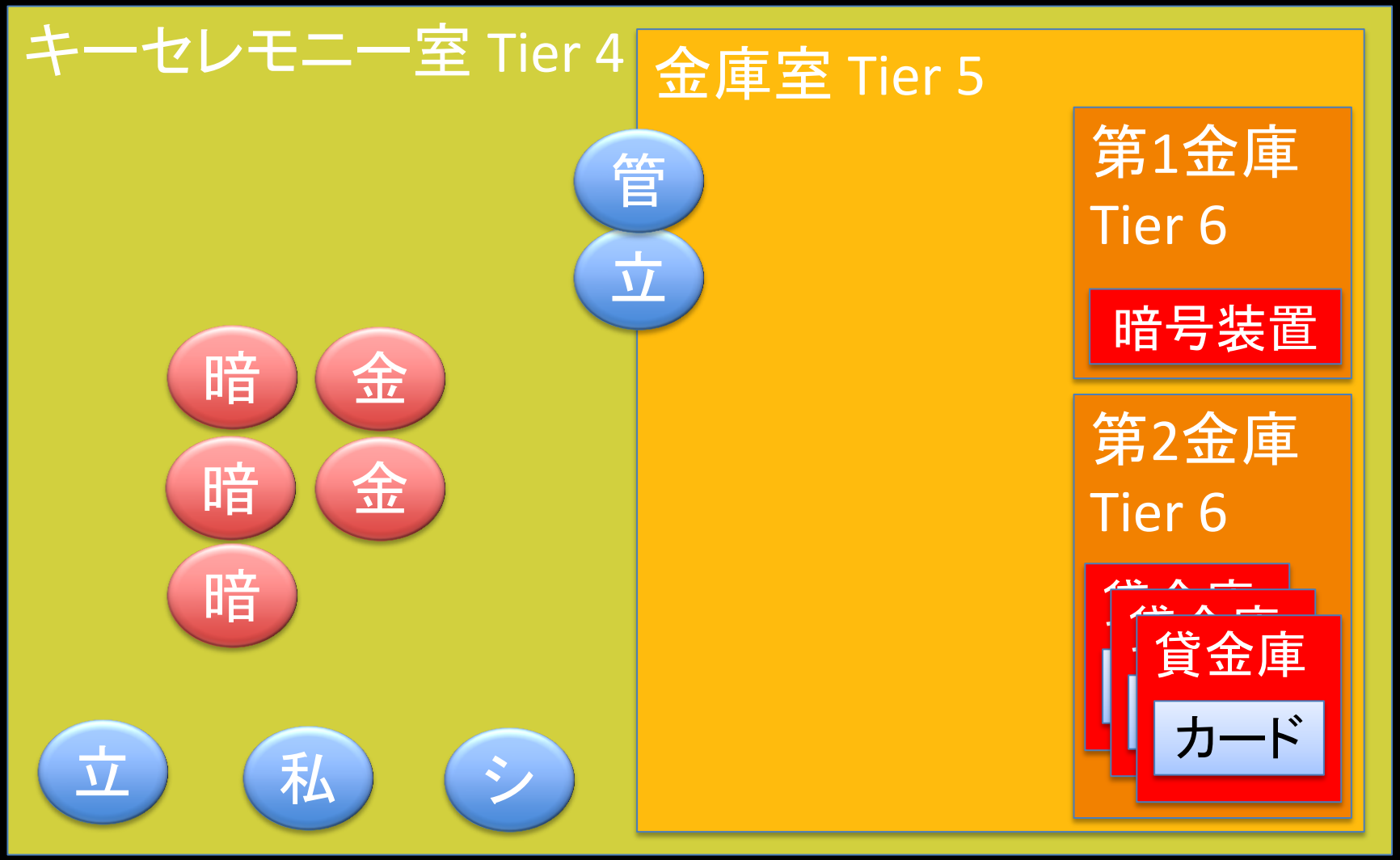
Root KSKの鍵管理の場合

Root KSKの鍵管理の場合

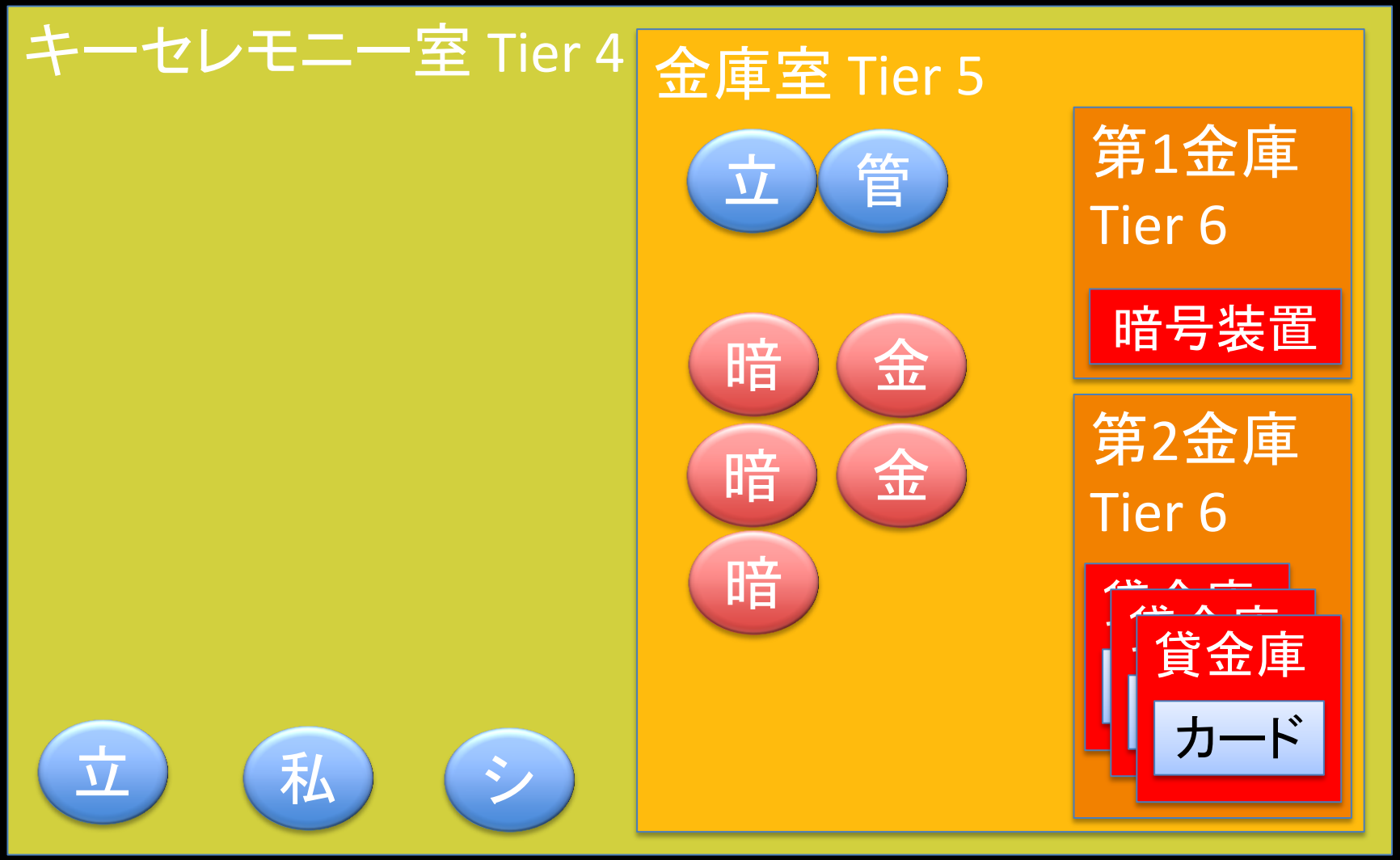
Root KSKの鍵管理の場合



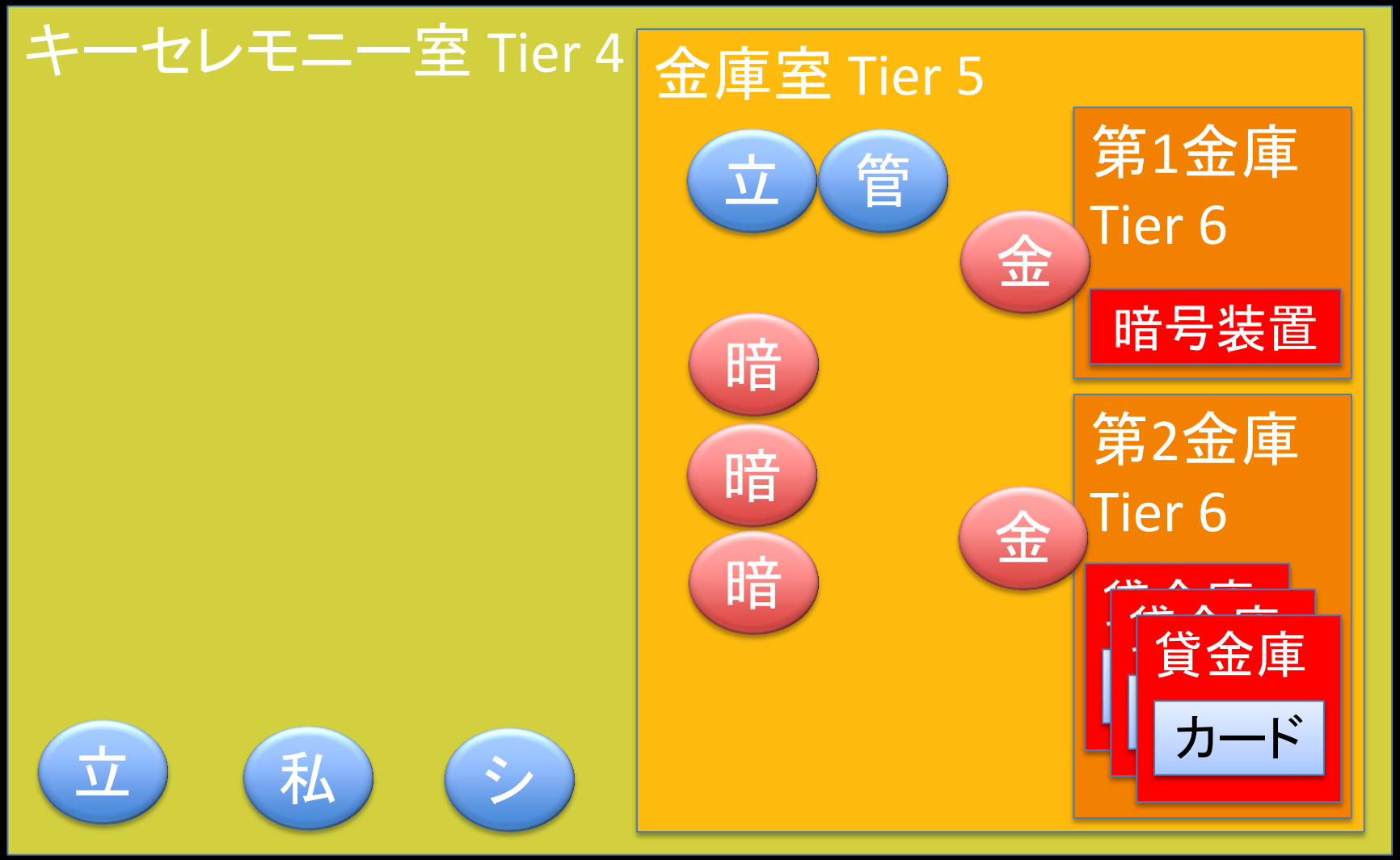
Root KSKの鍵管理の場合



Root KSKの鍵管理の場合

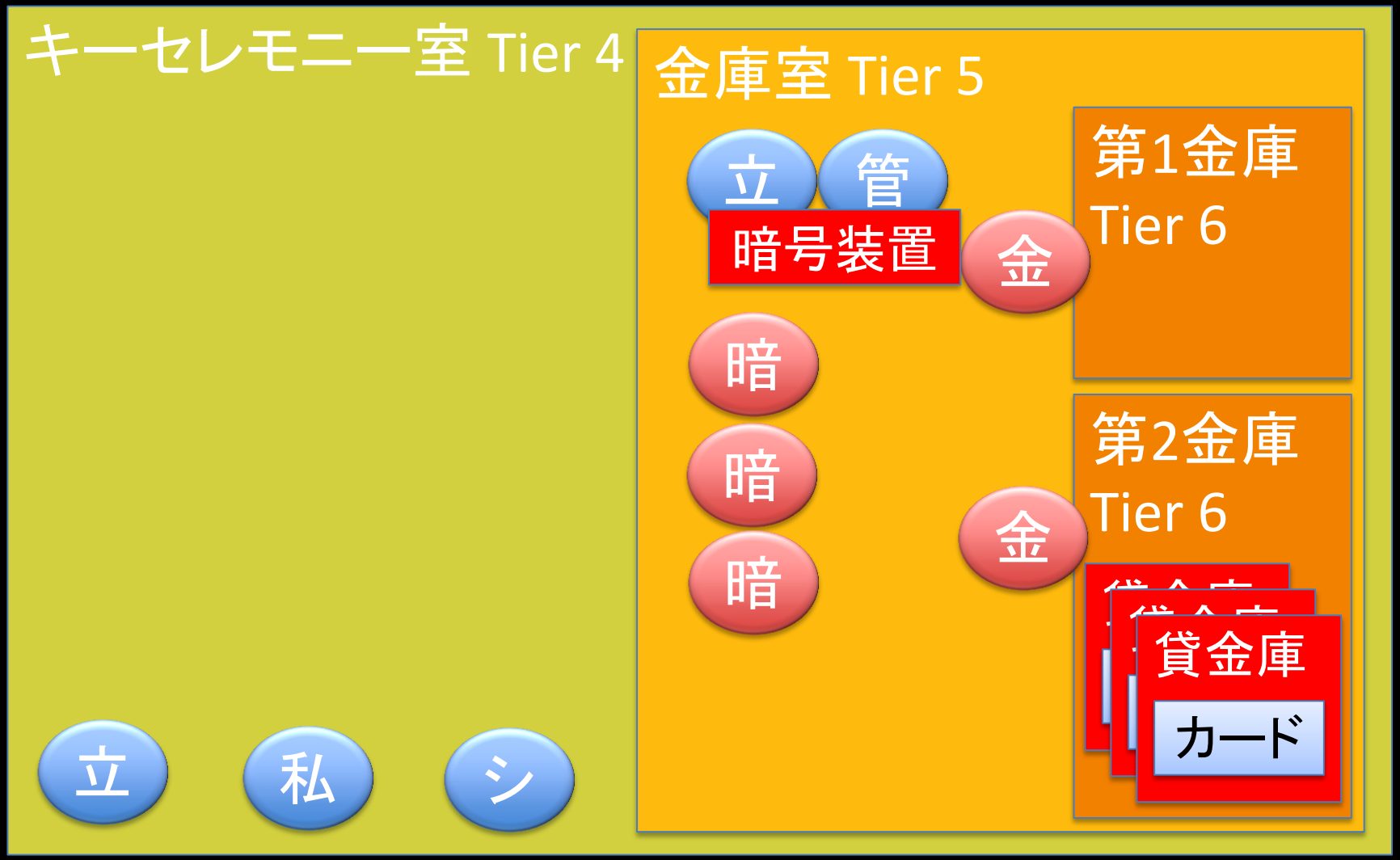


Root KSKの鍵管理の場合

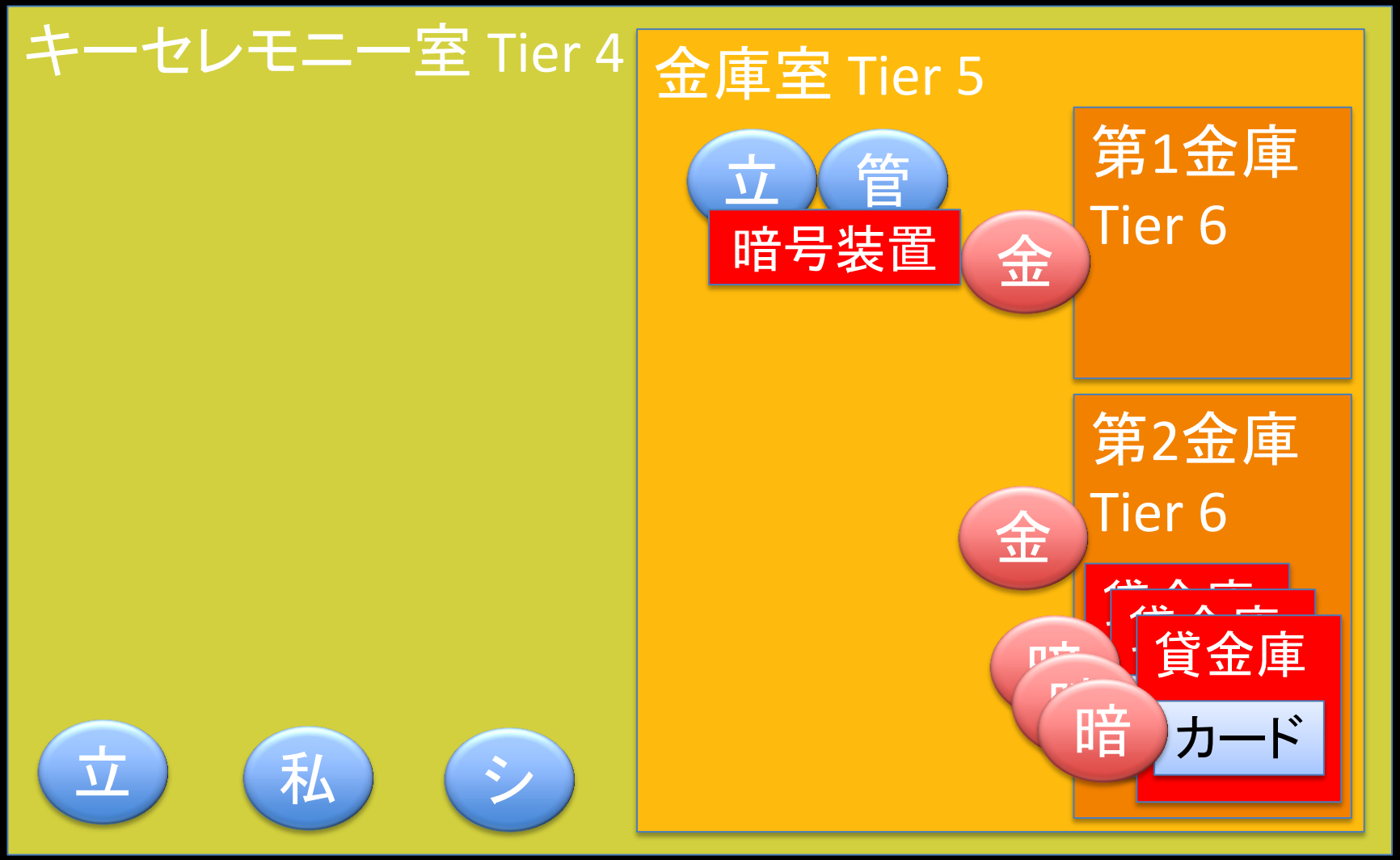


Root KSKの鍵管理の場合

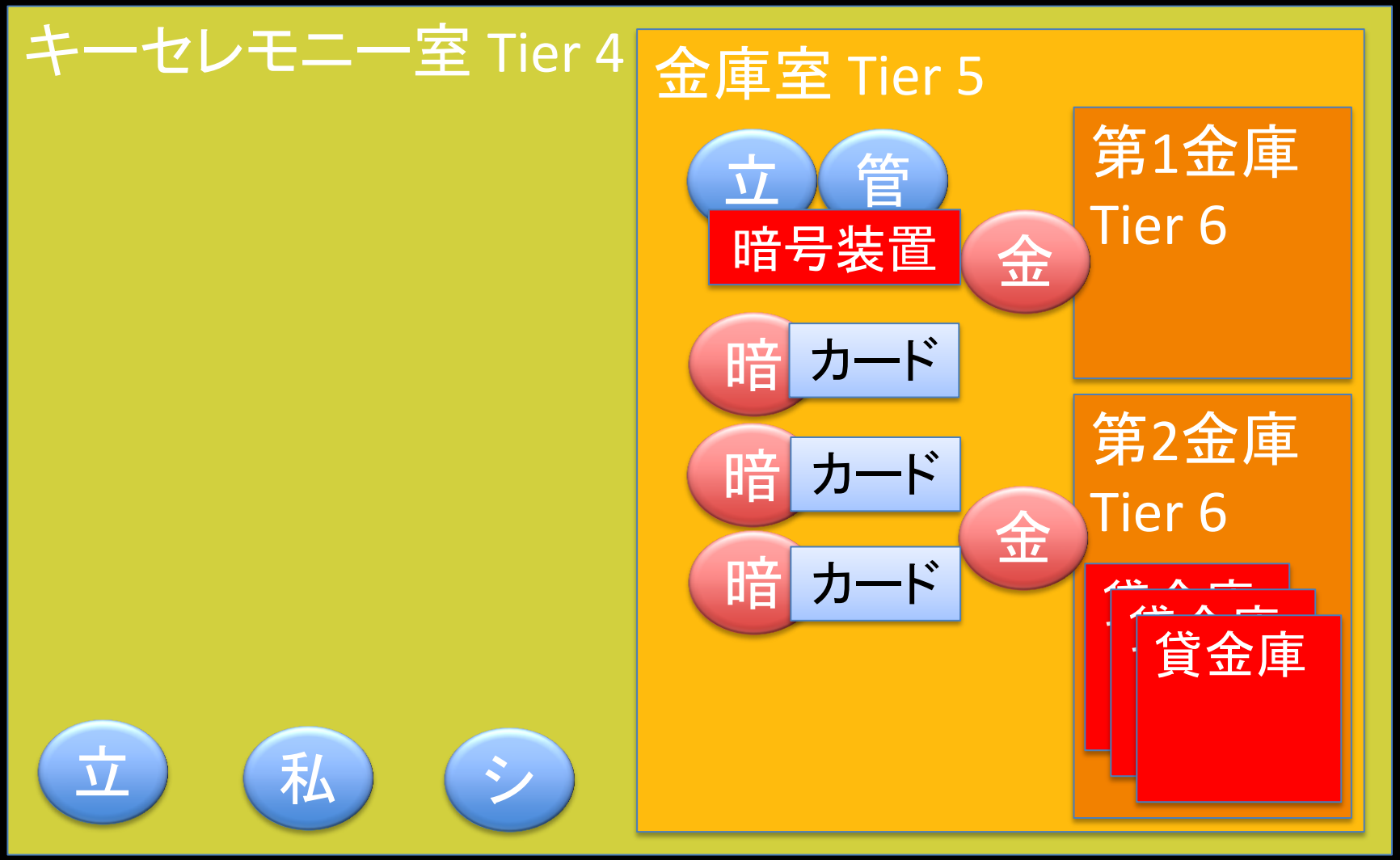
Root KSKの鍵管理の場合



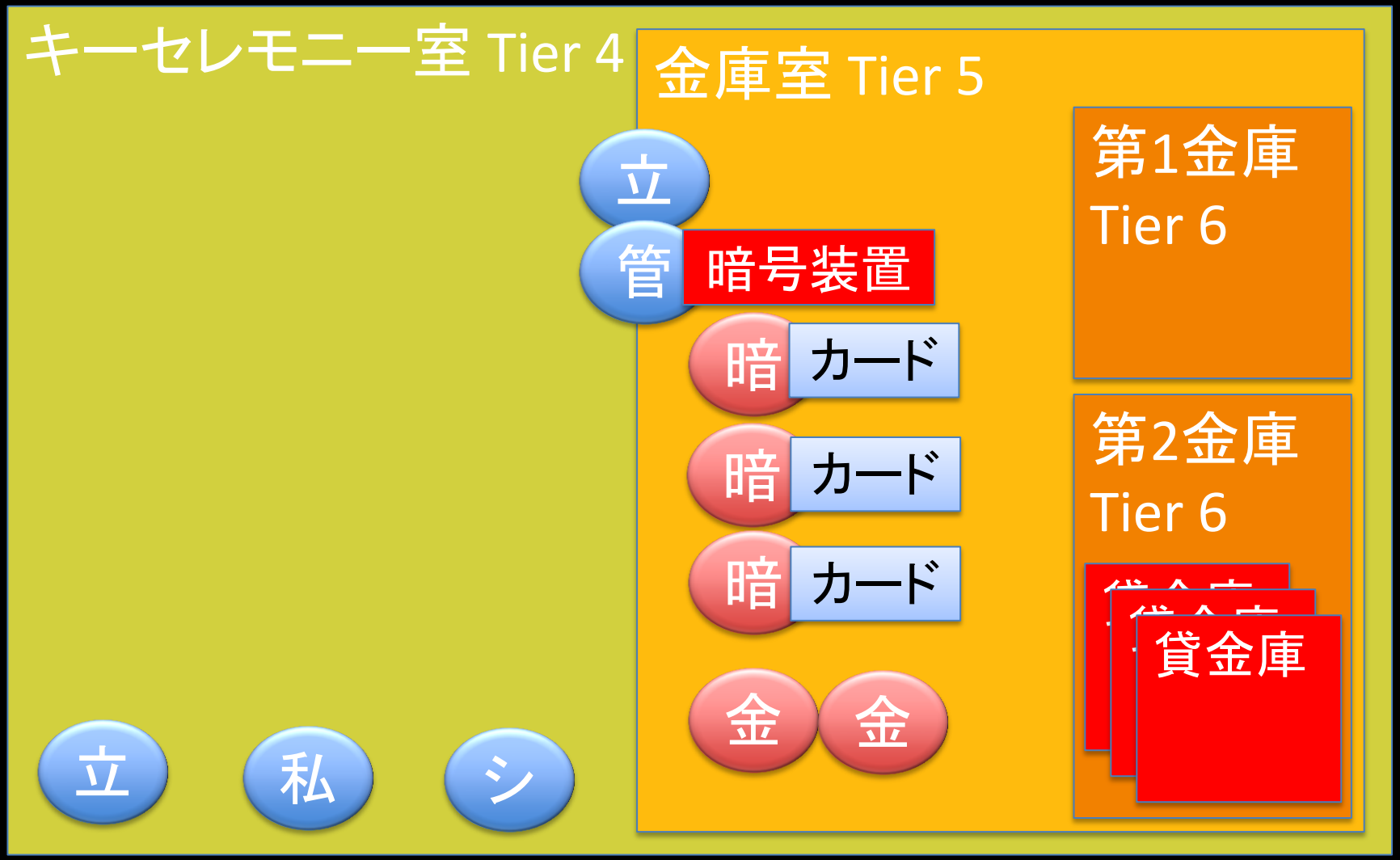
Root KSKの鍵管理の場合



Root KSKの鍵管理の場合

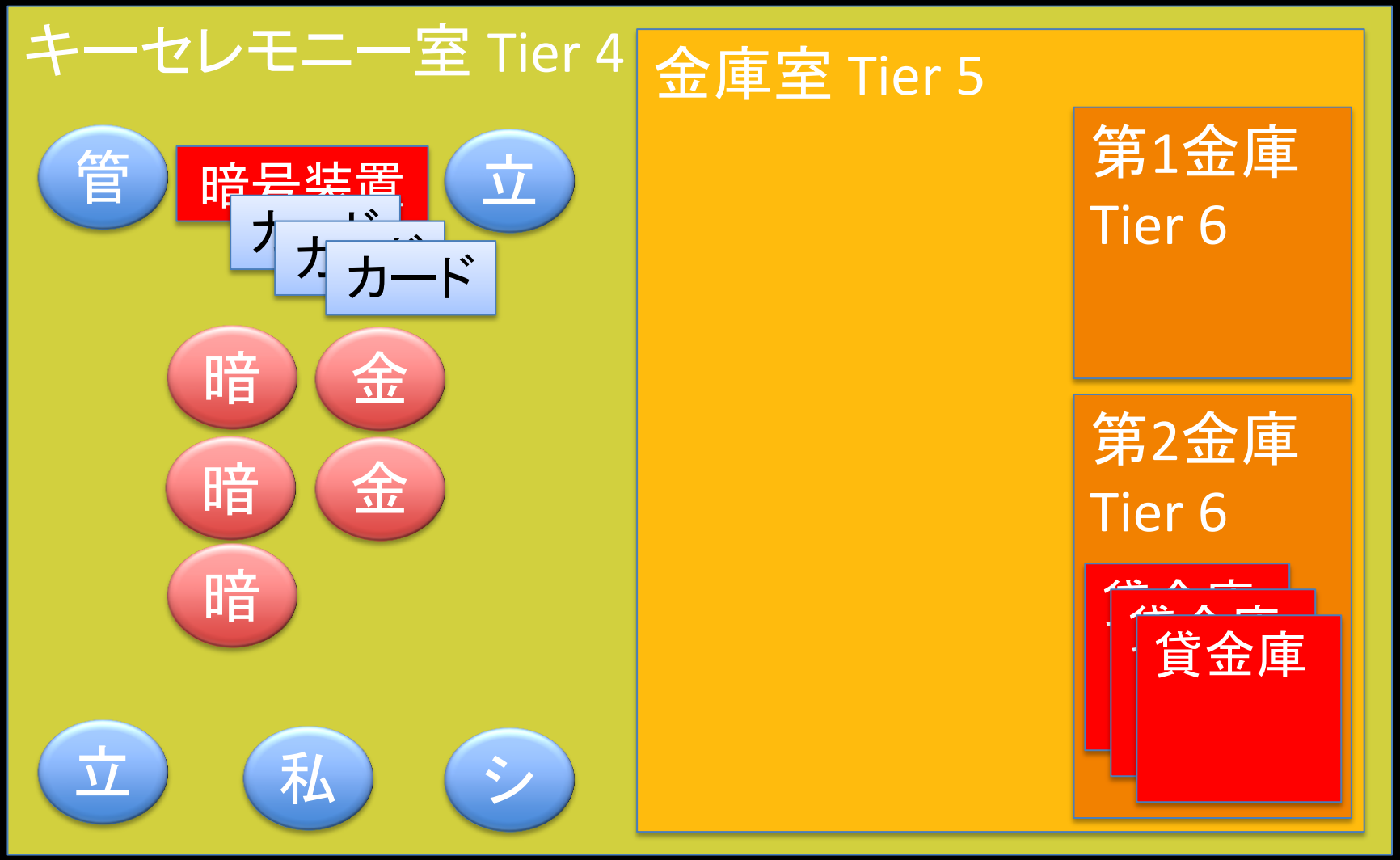


Root KSKの鍵管理の場合



Root KSKの鍵管理の場合

Root KSKの鍵管理の場合



百聞は一見に如かず！

ルートKSKのキーセレモニーを見てみる？

http://dns.icann.org/ksk/stream/

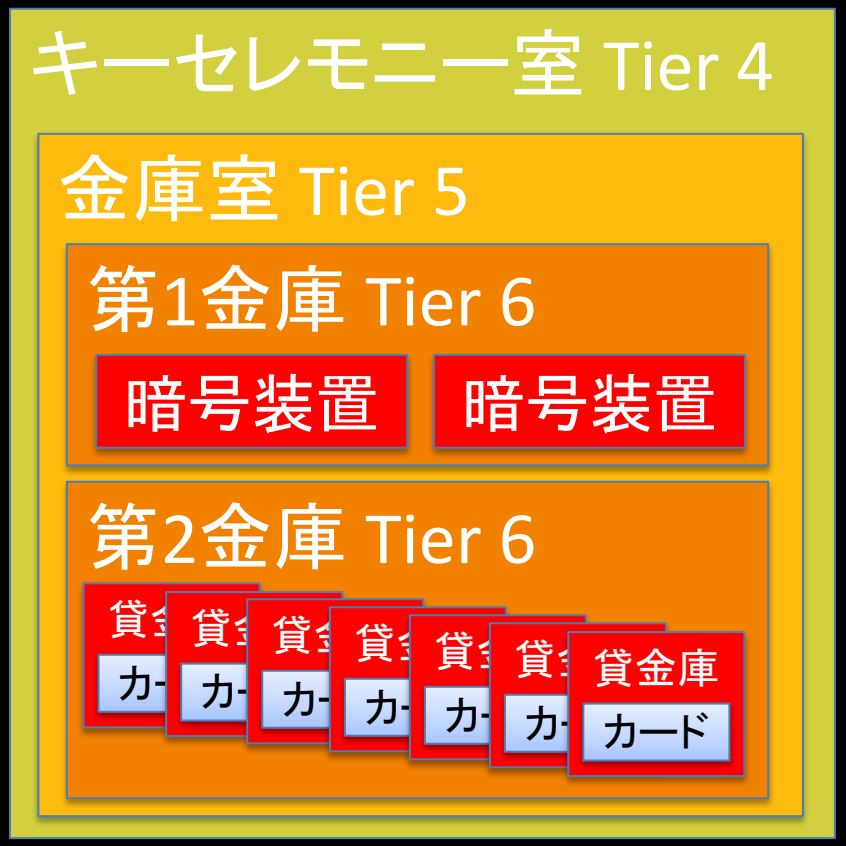
７月２１日午前５時（JST）上映開始予定

なんと民田さんもご出演の予定！

乞うご期待！

Root KSKの鍵管理の場合

西海岸
エルセグンド、カリフォルニア



東海岸
カルペパー、ヴァージニア

Root KSKの鍵管理の場合

西海岸
エルセグンド、カリフォルニア

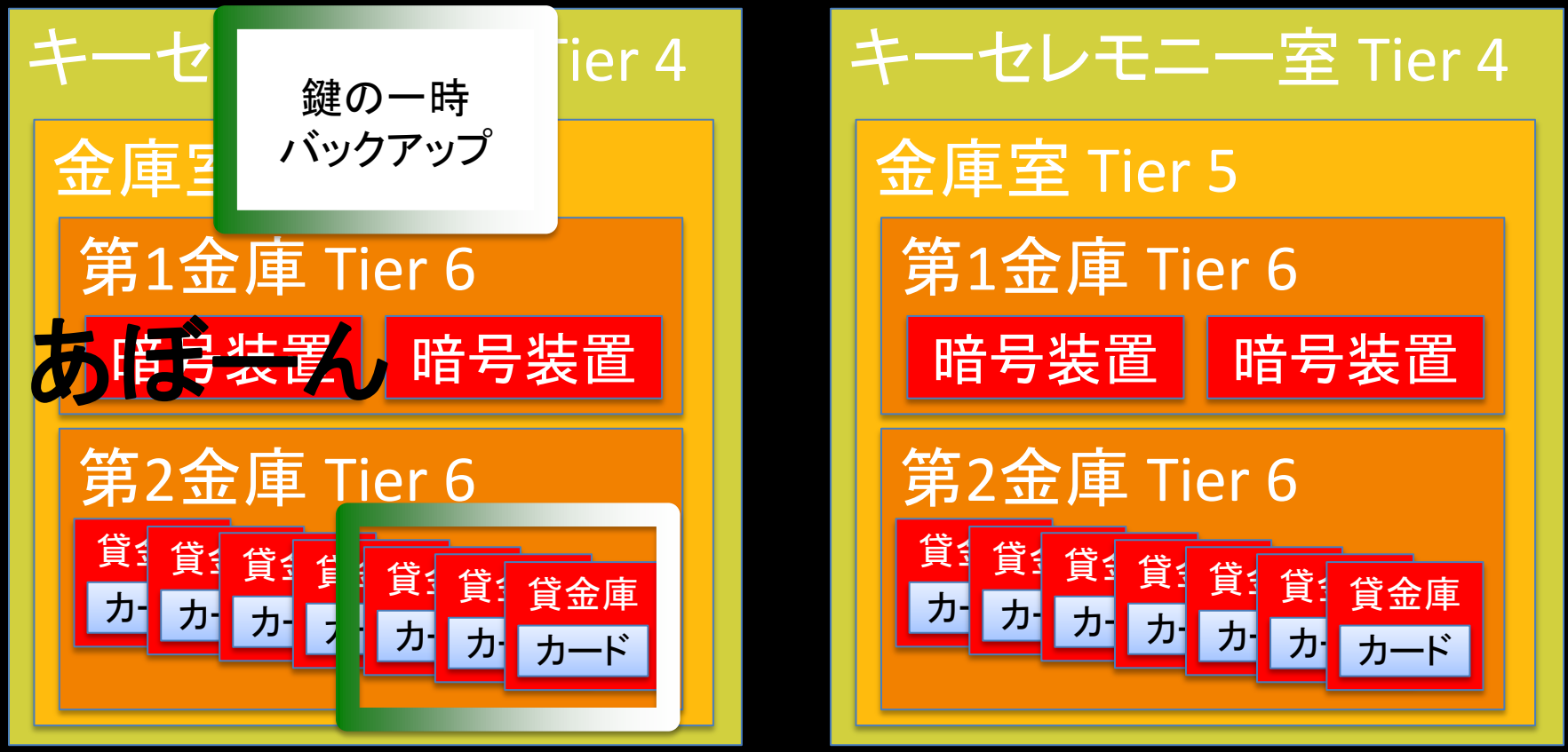
あぼーん

東海岸
カルペパー、ヴァージニア

Root KSKの鍵管理の場合

西海岸
エルセグンド、カリフォルニア

東海岸
カルペパー、ヴァージニア



Root KSKの鍵管理の場合

西海岸
エルセグンド、カリフォルニア

キーセレモニー室 Tier 4

金庫室 Tier 5

第1金庫 Tier 6

暗号装置 暗号装置

あぼーん

第2金庫 Tier 6

貸金庫
カード

東海岸
カルペパー、ヴァージニア

キーセレモニー室 Tier 4

金庫室 Tier 5

第1金庫 Tier 6

暗号装置 暗号装置

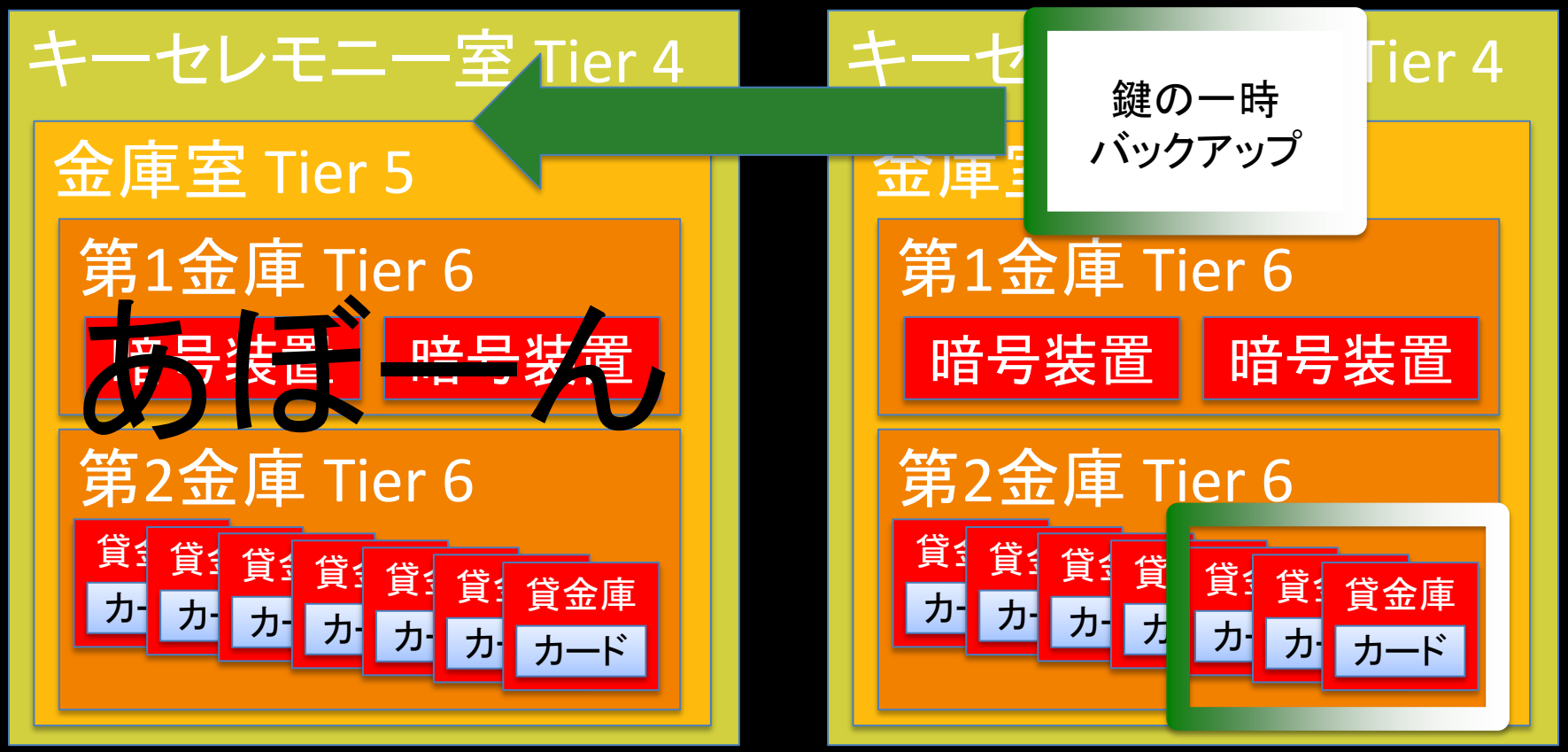
第2金庫 Tier 6

貸金庫
カード

Root KSKの鍵管理の場合

西海岸
エルセグンド、カリフォルニア

東海岸
カルペパー、ヴァージニア



Root KSKの鍵管理の場合

西海岸
エルセグンド、カリフォルニア

キーセレモニー室 Tier 4

金庫室 Tier 5

第1金庫 Tier 6

暗号装置 暗号装置

あぼーん

第2金庫 Tier 6

貸金庫 カード

東海岸
カルペパー、ヴァージニア

キーセレモニー室 Tier 4

金庫室 Tier 5

第1金庫 Tier 6

暗号装置 暗号装置

あぼーん

第2金庫 Tier 6

貸金庫 カード

Root KSKの鍵管理の場合

西海岸
エルセグンド、カリフォルニア

東海岸
カルペパー、ヴァージニア

鍵復元鍵（RKSH）　カード　カード　カード　カード　カード　カード　カード

Root KSKの鍵管理の場合

Root KSKの暗号鍵管理まとめ

- キーセレモニーは鍵管理のほんの一面
- 実際は事前処理と事後処理がたっくさん！
  - 暗号機器の在庫調査や棚卸し
  - アクセス権の棚卸し
  - 監査対応
  - 文書管理（DPSや他のポリシー、手順書）
  - 監査証跡の管理
  - 設備のメンテナンス
  - その他…

ご参考

鍵管理方針の策定のご参考に…

- ルートKSKの運用で使われているスクリプト等
  - https://www.iana.org/dnssec/
- DNSSEC Policy & Practice Statement Framework（宣伝です！）
  - http://tools.ietf.org/html/draft-ietf-dnsop-dnssec-dps-framework-04
- ISO21188:2006やANSI X9.79-2001
  - ただしこれらは認証局向けに書かれているのでご注意を！でも大変参考になります。

ご清聴ありがとうございました。

Thanks（゜д゜）

ご質問、ご要望はこちらへ↓

tomofumi.okubo@icann.org