

# セキュリティガイドライン策定 に向けた自主的取り組み ～ガイドライン策定の基本方針～

2016年11月8日

一般社団法人FinTech協会

理事 マーク マクダッド (マネーツリー株式会社)

(発表者) 事務局長 落合 孝文 (渥美坂井法律事務所)

事務局 原島 茂幸 (新日本有限責任監査法人)

# 目次

## 1. ガイドラインの論点

## 2. 前提事項の確認

- 1) リスクベースアプローチとは?
- 2) リスクの種類

## 3. ガイドラインの構成

- 1) 「概念編」と「基準項目編」への分割
- 2) チェックポイント項目の特性と対応方針
- 3) ガイドライン項目の章立て
- 4) FinTech固有のリスクの取込み
- 5) 想定リスクや対策事例の明示
- 6) 新技術の活用によるリスク管理

## 4. いただいたコメントと課題認識

## 5. 作業スケジュール

## 別紙. セキュリティガイドライン (第1案の抜粋)

# 1. ガイドラインの論点

第1回分科会での提示案、意見、アンケート、関係者ヒアリング等を基にした論点は次の通り。

## ガイドラインの構成


- a. 多忙なベンチャー経営者、担当者向けに適度な分量とする。
- b. 起業時のクイックリファレンスとして有益なものとしたい。

## リスクベースアプローチ

- c. リスクベースアプローチにより作成すべき。
- d. 情報管理に加え、可用性と完全性の観点も必要。
- e. FinTechはスマートデバイスが肝。

## 金融機関との協業

- f. 金融機関担当者とのリスクに関するコミュニケーションが上手いかわからないことがある（新技術利用・リスク評価チェックリストなど）。
- g. 金融サービスである以上、一定水準のセキュリティ確保は必須。

- 
- 1) 概念編（クイックリファレンス）と基準項目編（ガイドライン）に分けて編集する。 [a/b]
  - 2) クラウド利用を前提とすること、少人数組織で運営すること等FinTechベンチャーのリスクに応じて記載内容を定める。 [a/c/d/e]
  - 3) FISC安対基準（現行）の内容を取捨選択のうえ取込み、FinTechベンチャーとしてリスクや優先度が低い項目以外はものの無いよう、事後検証可能とする。 [d/g]
  - 4) スマートデバイスのセキュリティ管理をはじめ、FinTechとしてリスクの高い領域はFISC安対基準（現行）以上に踏み込む。  
(FISCに定めが無くても採り上げる) [e]
  - 5) 想定する（軽減を狙う）リスクおよび具体的対策事例を明示する。 [f]
  - 6) リスク管理上有効な新技術については、FICS安対で定める対策との関連を解説する。 [c]

## 2.前提事項の確認

### 1)リスクベースアプローチとは？

FISC「金融機関における外部委託に関する有識者検討会報告書」(平成28年6月)  
“Ⅲ リスクベースアプローチ” サマリー (24頁)

- (1)安全対策は個々の情報システムの**リスク特性に応じて必要十分なものとする。**
- (2)リスク顕在化後の事後対策と**比較衡量**(ひかくこうりょう)**したうえ、企業価値の最大化**をめざし経営資源配分を決定する。
- (3)上記原則に則り妥当な意思決定が行われるなら安全対策の**独自決定が可能。**
- (4)サービスの外部性や保有情報の機微性が高い場合、安全対策決定には**社会的・公共的な観点**も重要。

## 2.前提事項の確認

### 2)リスクの種類

情報システムの安全性とは、災害・障害・犯罪・不正行為、その他の脅威から保護されていること。これには、次の3点等が含まれる。（FISC「金融機関等のシステム監査指針」）

- 機密性(confidentiality)  
重要な情報が非権限者に知られることがないように保護されていること  
⇒暗号化や権限管理などによりデータや情報を漏らさないようにすること
- 可用性(availability)  
必要とされる情報が必要なときに利用可能であり、また必要な資源の継続的使用が確保されていること  
⇒機器/ネットワークの二重化や稼働状況監視等により、継続して稼働できるように(サービスが止まらないように) すること
- 完全性(integrity)  
不正や障害等により情報の一貫性が失われることがないように保護されていること  
⇒DBのロールバック機能やファイル間のデータ整合性確認により、情報が一貫するように保つこと

# 3. ガイドラインの構成

## 1) 「概念編」と「基準項目編」への分割

他のガイドライン等を参考に、チェックポイントとクイックリファレンス部分を分ける。

例：FISC「金融機関等のシステム監査指針」

「第1部 フレームワーク」 ⇒ 「概念編」

「第2部 チェックポイント集」 ⇒ 「基準項目編」



リスク評価の  
考え方など


リスクに応じて  
実際に遵守する  
基準項目

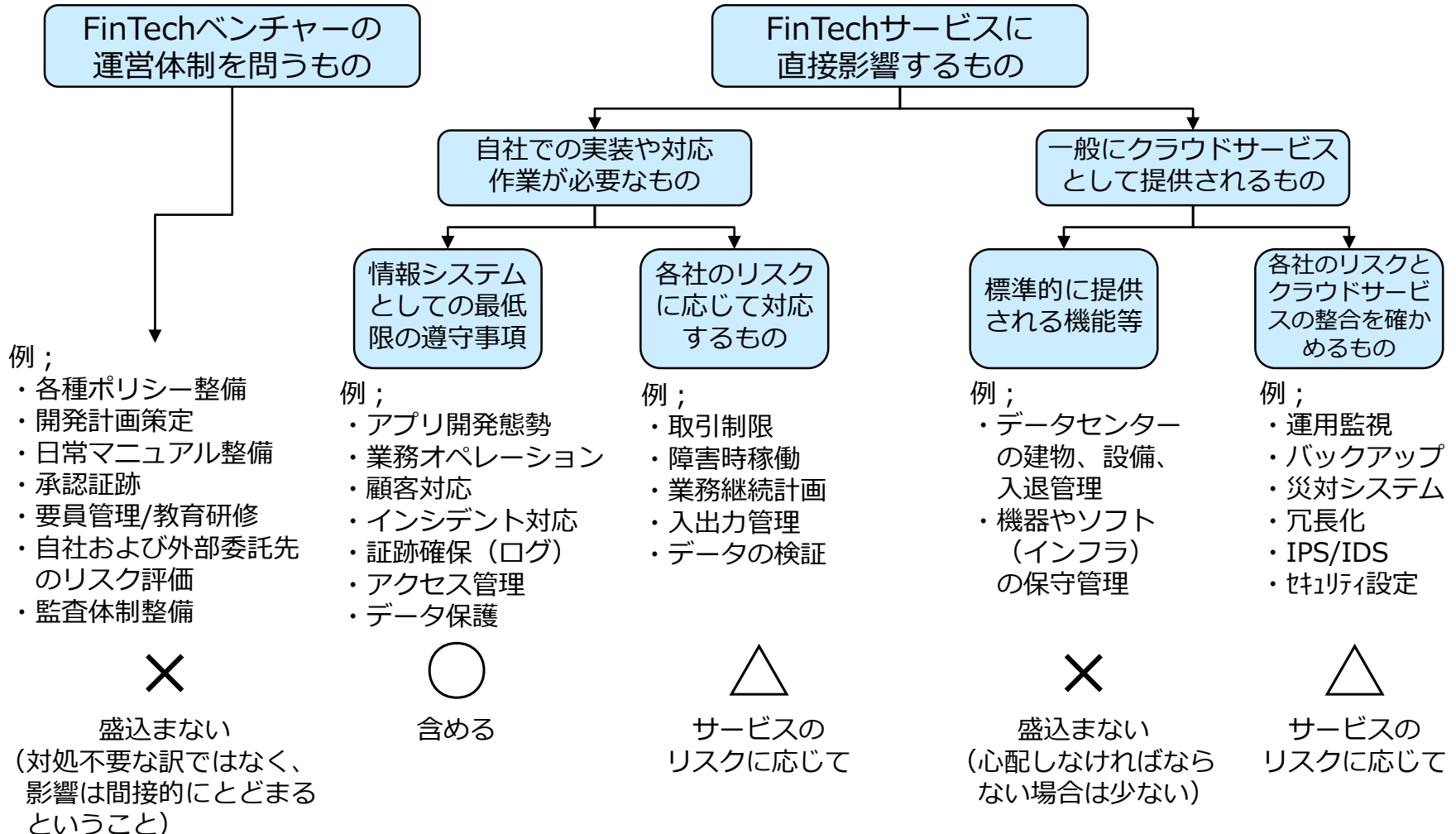
概念編

チェックポイント編

# 3.ガイドラインの構成

## 2)チェックポイント項目の特性と対応方針

FISC安対基準等公的なガイドライン等で対象とされる項目の特性に応じて、FinTechとしての優先順位など対応方針を定める。



# 3.ガイドラインの構成

## 3)ガイドライン項目の章立て

2)の方針に従うとともに、FISC安全対策基準の内容を取捨選択\*して取込み、次のような章立てとする。

(「別紙. FISC安全対策基準各項目の取扱方針案」により選択根拠を明確化する)

### データ管理 (機密保護)

- ・ 保管場所に応じたデータ管理 (クラウド/自社機器/顧客デバイス)
- ・ 通信データ保護 ・ 暗号鍵と電子証明書

### アクセス管理 ログ取得

- ・ OS/基盤/アプリ権限管理 ・ ログ取得と監査 ・ 顧客認証

### 運用管理・ 監視

- ・ 稼働監視 ・ 業務管理 (入出力管理) ・ 顧客対応 (問合せ)
- ・ インシデント管理 ・ 障害対応 ・ BCP

### 構成管理

- ・ 冗長化/障害対策 ・ 災害対策
- ・ マルウェア対策/パッチ ・ サイバー防衛(DNSキャッシュポイズニング他)

### 企画/開発/ 変更管理

- ・ 品質管理 ・ 変更管理 ・ セキュアプログラミング

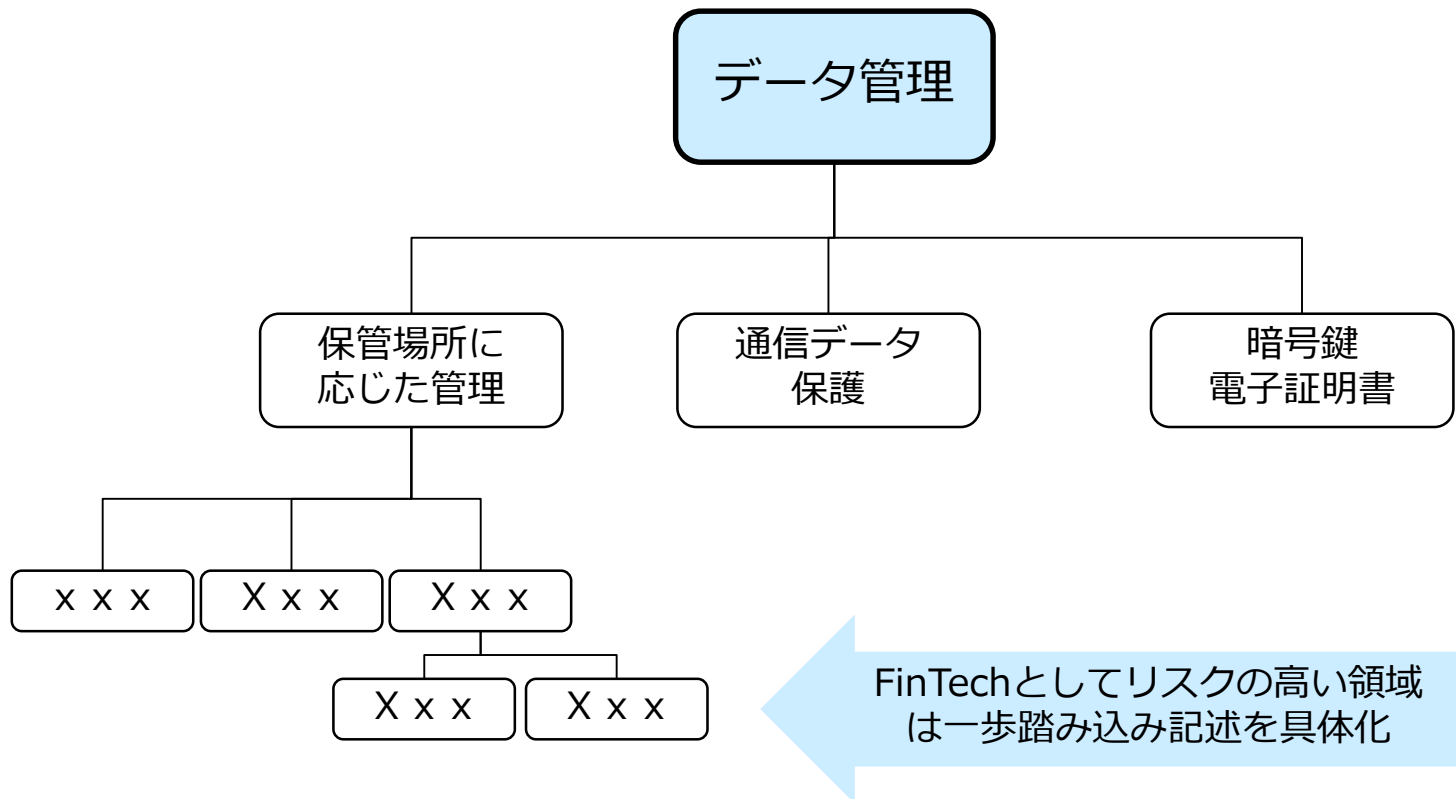
凡例 黒字：第1回分科会提示案 赤字：今回追加案



# 3. ガイドラインの構成

## 4) FinTechの性質に応じたリスクの取込み

スマートデバイス関連やアプリケーション層のセキュリティをはじめとしたFinTechとしてリスクが高い領域については、一歩踏み込み記述の具体化を目指す。



基準項目の構成案に沿い順次  
細分化・深掘りしていく

FinTechとしてリスクの高い領域は一歩踏み込み記述を具体化

# 3. ガイドラインの構成

## 5) 想定リスクや対策事例の明示

【サービス内容によらず、必須とする項目】

基準項目	想定リスク	適用例	対策事例（該当ある場合は悪例も）
ルートアカウントの目的外使用や悪用を牽制する。	特定の者が単独で使用でき、使用状況もチェックされない場合は目的外使用や悪用の誘因となる。	全ての場合	<ul style="list-style-type: none"> <li>・2要素認証を導入し、各要素を別の者が保有することにより、単独使用を不可とする。</li> <li>・単独使用を可能としておく場合は、使用状況（ログオン/オフ日時、アカウント名、使用コマンド等）を使用者以外の管理者へ都度通知（警告）し、検証可能とする。</li> <li>・通知（警告）はメール送付の他、使用状況リストを出力する方法がある。この場合、当該リストはルート権限者による変更不可なものとし、改ざんを防止する。</li> </ul>

【サービス内容により適用を選択する項目】

基準項目	想定リスク	適用例	対策事例（該当ある場合は悪例も）
入力したデータの正確性を件数と合計金額の一致により確認する。	誤入力により値が不正確となる。	紙面の読取り等人手が介在し正確性の担保を慎重に行う必要性が高い場合	<ul style="list-style-type: none"> <li>・入力前の帳票の件数と合計金額を算出し、入力後のものと比較して一致していることを確認する。</li> <li>・予め、件数と合計金額を算出、表示する機能を実装しておく。</li> </ul>

なお、サイバー防衛やセキュアプログラミング関連の項目は、公的ガイド\*等を参照する方式も検討する。

\* IPA<独>情報処理推進機構>各種ガイド、OWASP TOP10、SANS CWE TOP25など

# 3.ガイドラインの構成

## 6)新技術の活用によるリスク管理

- ✓ 次のような新技術を活用することにより、負荷軽減と同時にFISC安対基準の趣旨と同等のリスク管理が可能である。しかしながら、FISC安対基準はその字義通りにのみ解釈され、管理手法や技術が趣旨に則っているのか検討されないまま不適とされてしまう恐れがある。
- ✓ ガイドラインにおいてこのような新技術を解説し、リスクコミュニケーションの向上を図ることによって、FinTechを含めた金融システム全体の有効化と効率化に寄与していくことを目指す。
- ✓ 現時点で具体的に想定するものは次の2例であるが、会員より広く事例を募集する。
- ✓ 原則として対策の一事例としての記載を想定するが、イミュータブルインフラの例など影響範囲が大きい場合は、個別テーマとして代替可能な基準項目を明示する方法も検討する。

### エンベロープ暗号化 [envelop]

- データ鍵自体を暗号化して保存
- 意図されたデータ受信者に対してのみ、平文化されたデータ鍵が与えられるとともに、当該平文鍵を速やかに削除する
- 煩雑な鍵管理プロセスを省略できる

### イミュータブルインフラ [immutable]

- 一度セットアップされたインフラ（サーバ）は変更しない
- 変更したい場合は、クラウド上に新規インスタンスとして作成する
- 作業を新規インスタンスへの切替に集約することにより、変更権限の管理を簡素化できる

## 4.いただいたコメントと課題認識



### 金融庁

- ✓ 新技術の活用により、既存の基準と同等のセキュリティ水準を実現しながらも管理負荷を軽減出来る、といった事例を示してくれることを期待する。  
⇒「3.6)新技術の活用によるリスク管理」の通り。

### FISC

- ✓ 安対基準は、金融機関等が適切な安全対策を実施するにあたり参考とするものとして、作成されており、FISCの会員でもあるFinTech協会が、安対基準を参考としながら、自らのガイドラインを策定されることには、なんら問題はない。(参考「安対基準第8版 I 安全対策基準の考え方」)
- ✓ 安対基準は、もともと基幹オンラインコンピュータ・システムを対象として作られており、ベンチャー企業のような少人数の企業を必ずしも前提としているとはいえ、そうした視点を取り込むことも、「安全性を確保しつつも、イノベーションの成果を享受する」という観点で必要とも考える。  
⇒「3.2)チェックポイント項目の特性と対応方針」の通り。
- ✓ 安対基準は基幹オンラインシステムを前提としており、FinTechベンチャーのような少人数組織の実態にそぐわない場合があるならばFinTechに関する有識者検討会で発信してほしい。  
⇒協会のガイドライン検討過程で出された意見等を発信していくとともに、有識者検討会の最終成果（新しい基準等）と協会のガイドラインの関係整理は今後の課題とする。

### 全銀協

- ✓ 協会のガイドラインには会員を守る役割とともに、金融機関との協業を推進する役割もあるはずであり、ガイドラインのガバナンスの透明性確保が重要であるが、FISCのガイドラインと合流する可能性もあるのか。  
⇒課題として認識する。

# 5.作業スケジュール

分類	項目	FY2016							
		9	10	11	12	1	2	3	
対関係機関	金融庁、全銀協への情報共有と議論		随時実施						
	FISC新安全対策基準 (FinTech) 有識者検討会議		2016.10~2017.6 月次程度で開催 協会内の協議内容を随時発信 *1						
協会内活動	理事会							★ 制定決議*2	
	分科会での報告と協議	★ 基本方針説明と合意	★	★	★	★	★	★ 最終案説明と合意*2	
	準備会による協議 関係者と事務局の相対相談等		有識者、協力者等関係者を招集、 または相対で協議・相談						
	既存FISC安対項目の 取込方針策定 (取捨選択)		有識者、協力者と事務局で協議し検討						
	ガイドライン記述作業		事務局主体で継続作業						

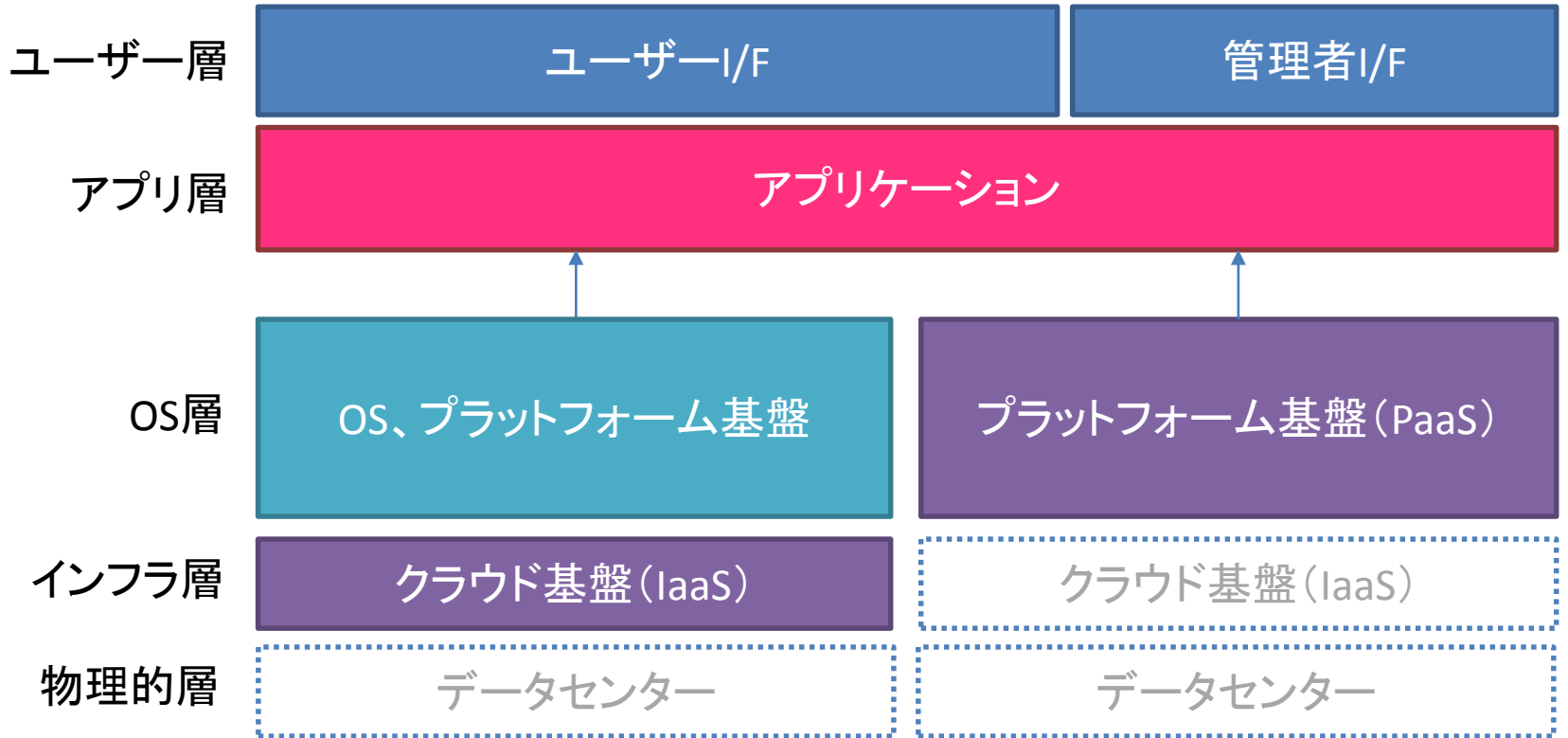
\*1 FISC有識者会議の最終成果と協会ガイドラインの位置付け整理は今後の課題とする。

\*2 なお、FISC他関係各機関の議論の状況によっては協会ガイドライン完成が後倒しとなる可能性もある。

# 別紙 セキュリティガイドライン (第1稿の抜粋)

次頁以降は参考資料であり、この第1案の検討のための分科会等を経て、ここまでにご説明した方針に基づく改版を進めております。

# アクセス権限



# クラウドアクセス権限

クラウドの場合、何でもルートアカウントがつく

## 行うべきこと

- 全てのアカウントのログインに2経路認証(2FA)を有効にする
- ルートアカウントにログインするには、2FAまたはパスワードを分けることで2人以上を必要とする
- ルートログインがあった場合、経営者に通知されるように設定する
- ルートアカウントと別に普段使う特権IDとエンジニアIDを作成する
- 業務などによってアクセス権限のレベルを書面化し、社員に遂行するための最低限のアクセスをさせる

## 行うべきでないこと

- アカウント(ルートでなくても)を共有する(「誰が」が不明になるため)



# アプリアクセス権限

## 行うべきこと

- 管理画面のアカウントのログインに2経路認証(2FA)を有効に
- ユーザーアカウントのログインに2経路認証(2FA)を利用させる
- 業務などによって管理画面のアクセス権限のレベルを書面化し、社員に遂行するための最低限のアクセスをさせる

## 行うべきでないこと

- ユーザーのパスワードを生の状態で格納する(Hashをせず)
- 独自のユーザー認証フレームワークを作る(Best Practiceツール)

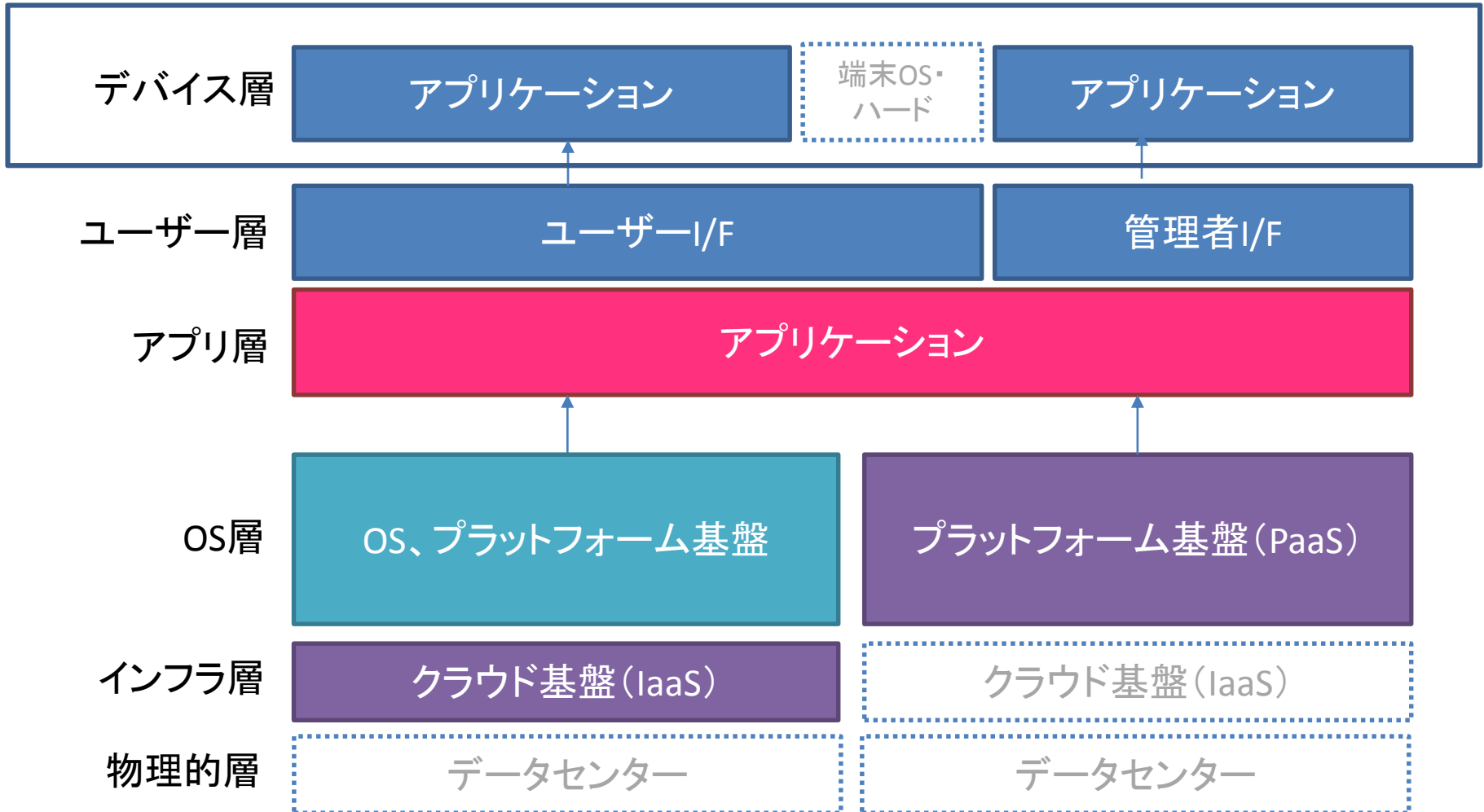
## 行うべきこと

- 通信する時(動的)も格納する時(静的)もデータを暗号化する
- クラウドで暗号化は設定になっているケースが多い
- 暗号キーの管理体制をしっかりと、定期的にキーを交換する
- 必要がある時以外、ローカルのDBよりDBaaSを活用する
- データのセンシティブ性によって格納可能な場所の規定を定めて、その規定を社内で周知させる
- 規定外の漏洩があるための対策を設ける、そして事件を記録する

## 行うべきでないこと

- 必要以上にセンシティブデータを格納する

# データ管理：デバイス



# データ管理：デバイス

## 行うべきこと

- センシティブデータが端末にある場合、ハードウェアキーストアによる暗号化を採用する
- セキュリティ強化に対応しているOSのみに利用させる
- センシティブデータが端末にある場合、アプリケーションレベルの認証を導入する(生体認証、パスワード、OOB認証)
- スマフォとサーバー間の通信の場合、ピンニングを活用する(TLS)

# チェンジ管理

## 行うべきこと

- Orchestration層 (Chef, Ansible, CloudFormation等) を活用することによって変更不可能なインフラ・アプリを設ける
- Orchestration層のコードもバージョン管理にチェックインする
- 採用するクラウド・技術・ライブラリーの脆弱性関連のメーリングリストなどに購読し、アナウンスを常に確認する
- パッチ適用するプロセスを導入する
- アプリごとに配置のプロセスを導入し、できる限り自動化する

# ログ・監査

## 行うべきこと

- アプリのログデータを各システムから自動送信でルートアカウントしか改ざんが出来ないストレージに格納する(読込アクセスはOK)
- 事件が発生する前提で、状況が把握できる程度の情報のログを記録する
- クラウドの設定変更をログし、変更されたら自動的に通知させる
- エンジニアによるセンシティブな作業が必要な場合、自動的に通知させる

## 行うべきでないこと

- センシティブなデータのログを記録する

# 査定・保証

## 行うべきこと

- サービスインする前に必ず、及び年間1回以上、第3者による侵入テストを行い、報告書の指摘の重要度に応じて対応する
- 第3者にコードのレビューをしてもらう
- Bug Bountyプログラムを定期的に行う(ベンチャーにとってコストパフォーマンスが良いもの)
- 将来的にPCI-DSS等、基準に準拠する必要がある場合、必要とされる前から企画段階からシステムを構築していく

## 行うべきでないこと

- ある基準に準拠しているから安全安心と勘違いする

# Best Practice

## 行うべきこと

- 多重対策・多重暗号化を図る
- 暗号化のみならず、システム間の認可も重要視する
- 自前主義ではなく、信頼される実績のあるクラウドベンダーに技術 Stack の下の層を投げる
- WEBサービスを営む場合、HSTS技術を採用する
- 該当する場合、DNSSecを利用する

## 行うべきでないこと

- セキュリティにおいてSPOFを許す