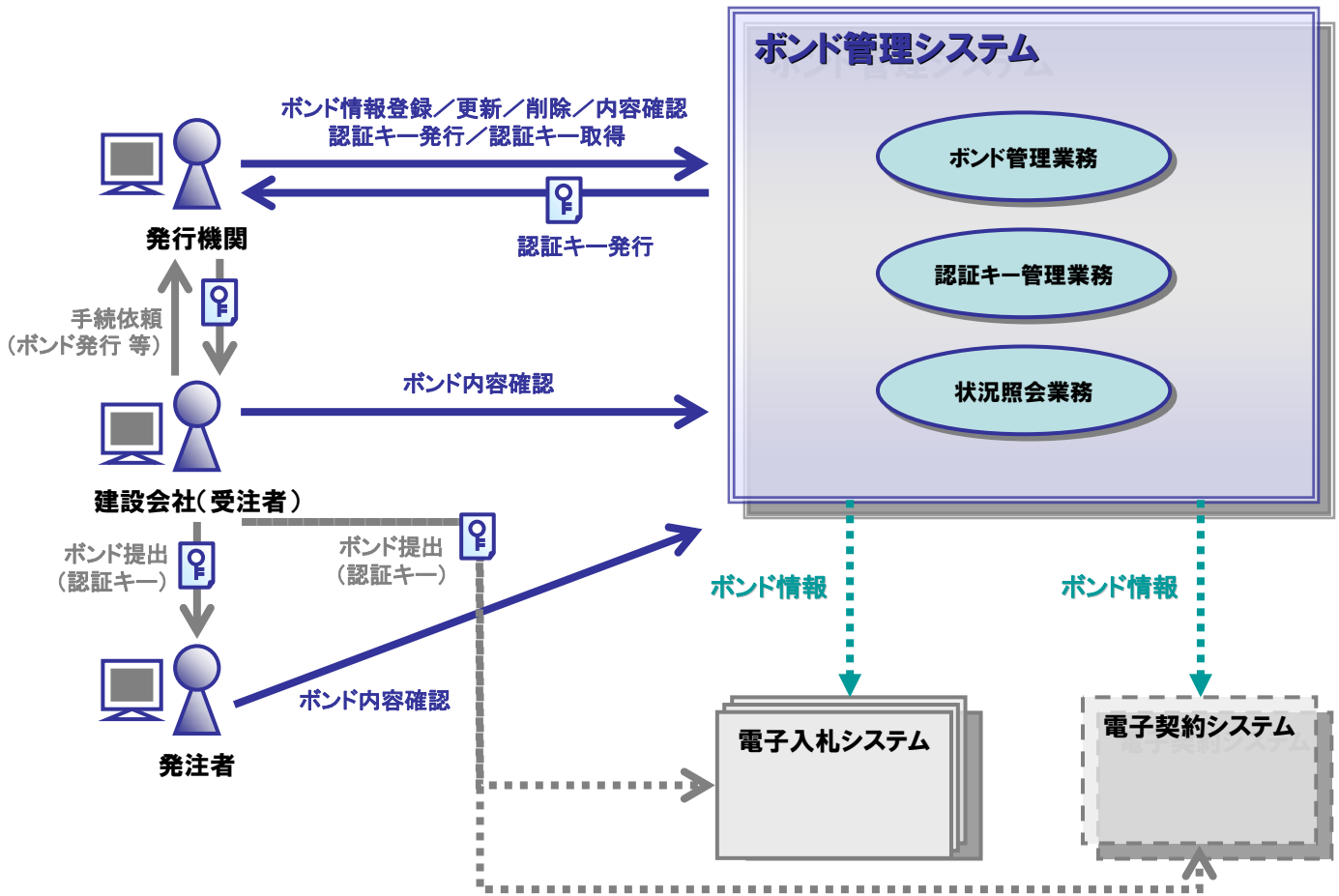
資料１

ボンド電子化の仕様（案）について

第二回　入札ボンド・履行ボンドの
電子化に関する勉強会

平成２０年９月１８日

■システム全体像とシステム化範囲



【凡例】 ：システム ：業務 ：業務の流れ ：データの流れ ：システム外業務の流れ

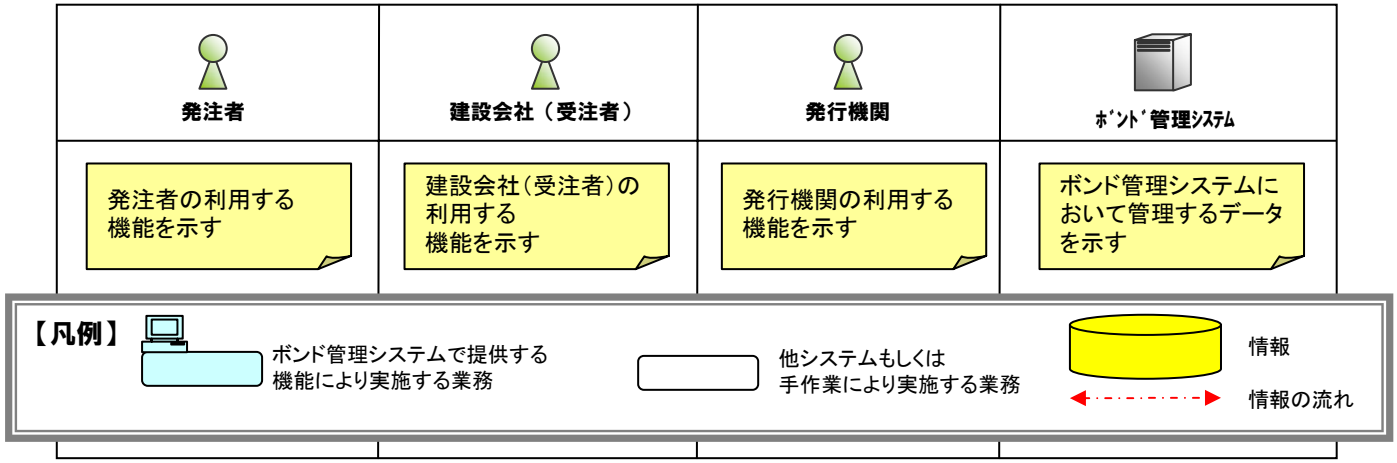
※ 点線は、将来的な検討対象となるシステム／業務／流れを表している。

■ビジネスフロー

ボンド管理システムで実現するビジネスフローは、下記の入札業務、契約業務の大きく2つに体系付けられる。それぞれのビジネスフローを次ページ以降に示す。

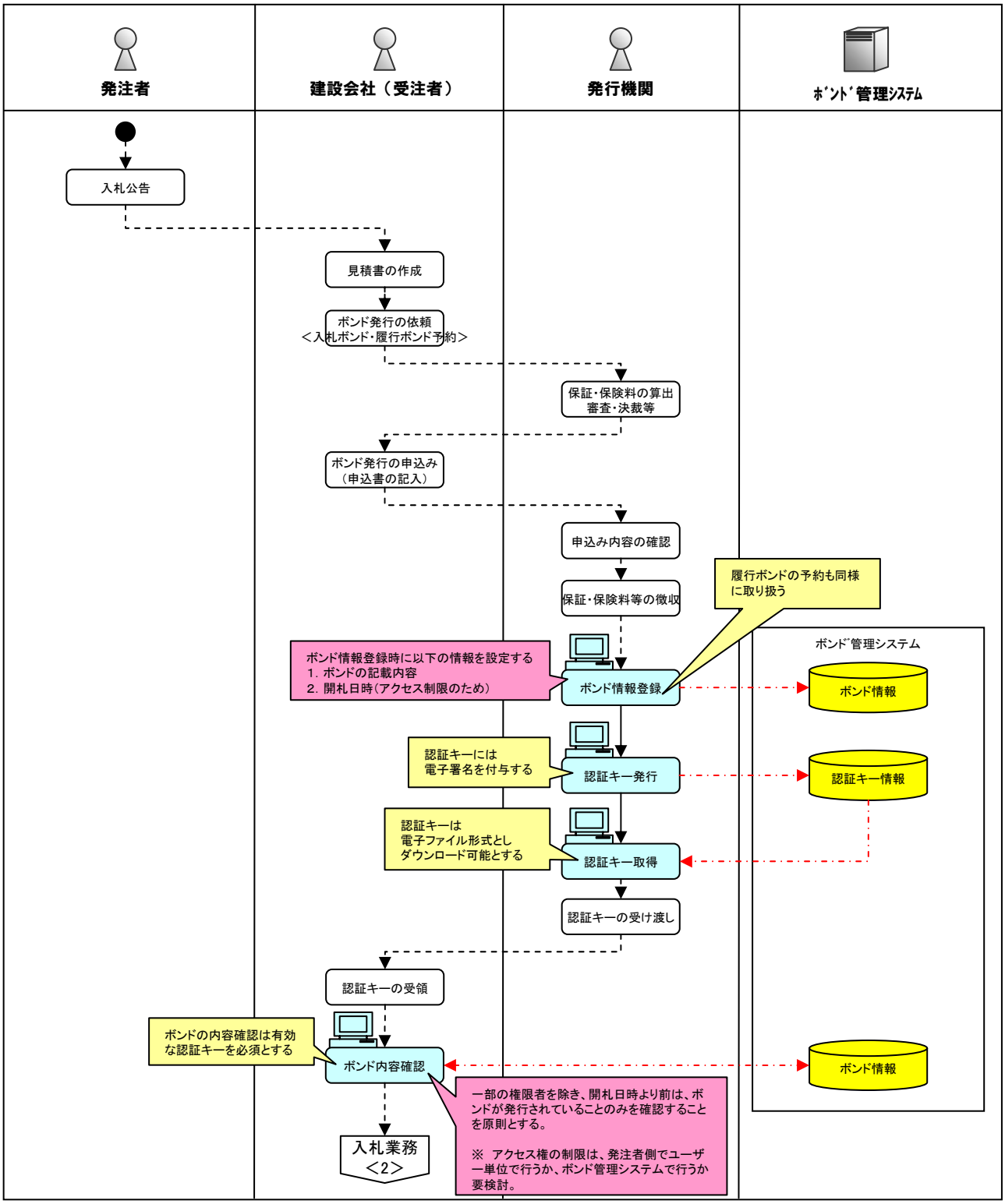
No	ビジネスフロー名称		概要
1	F01	入札業務	発行機関より入札ボンドの発行を受けた建設会社が入札に参加し落札する業務フロー
2	F02	契約業務	発行機関より履行ボンドの発行を受けた建設会社（受注者）が発注者との間で契約締結を行い検査・請求/支払を行い契約を完了する業務フロー

（参考）ビジネスフロー凡例



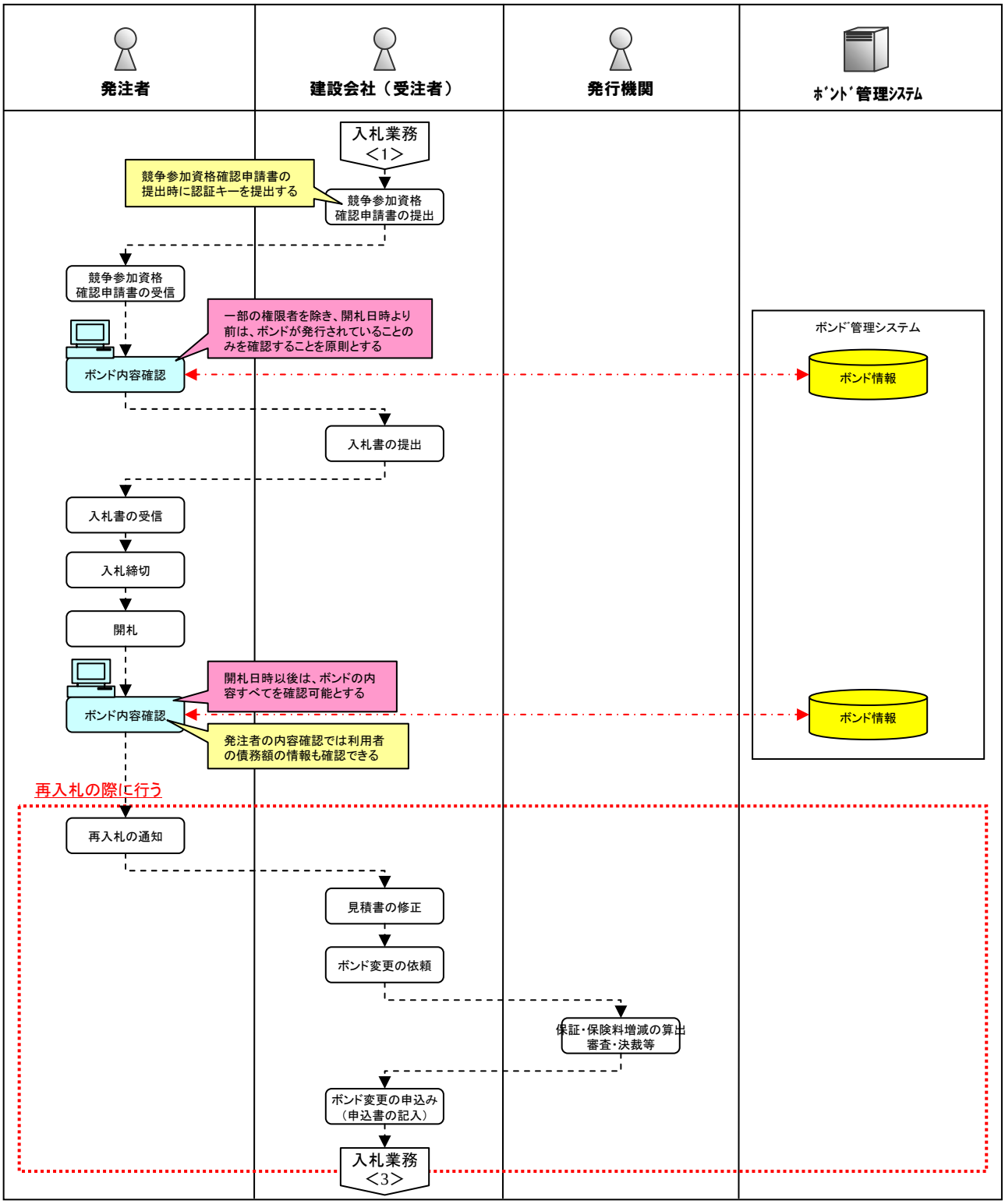
ビジネスフロー

システム名	ボンド管理システム	
ビジネスフローID／名	F01	入札業務＜1＞



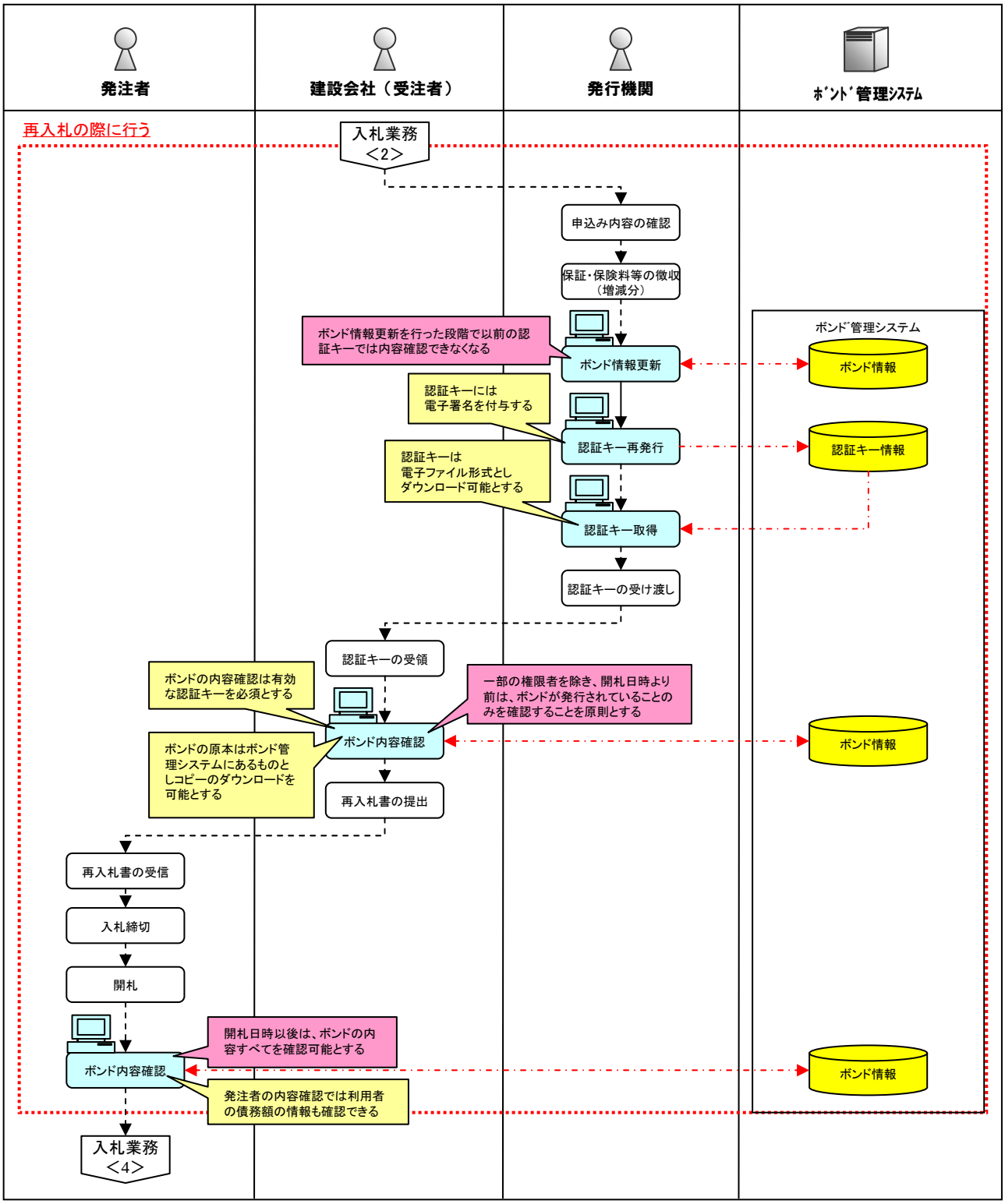
ビジネスフロー

システム名	ボンド管理システム	
ビジネスフローID／名	F01	入札業務＜2＞



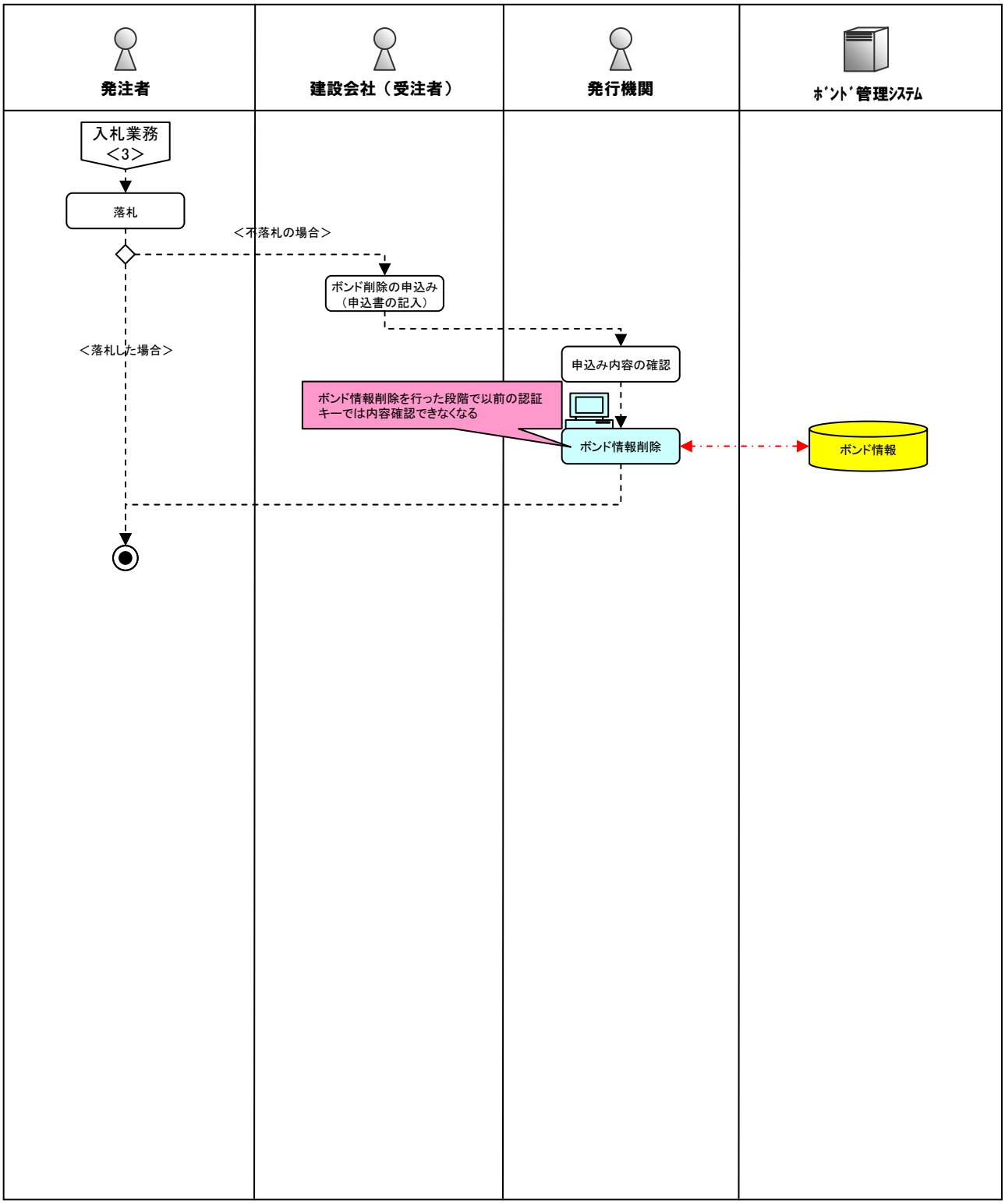
ビジネスフロー

システム名	ボンド管理システム	
ビジネスフローID／名	F01	入札業務＜3＞



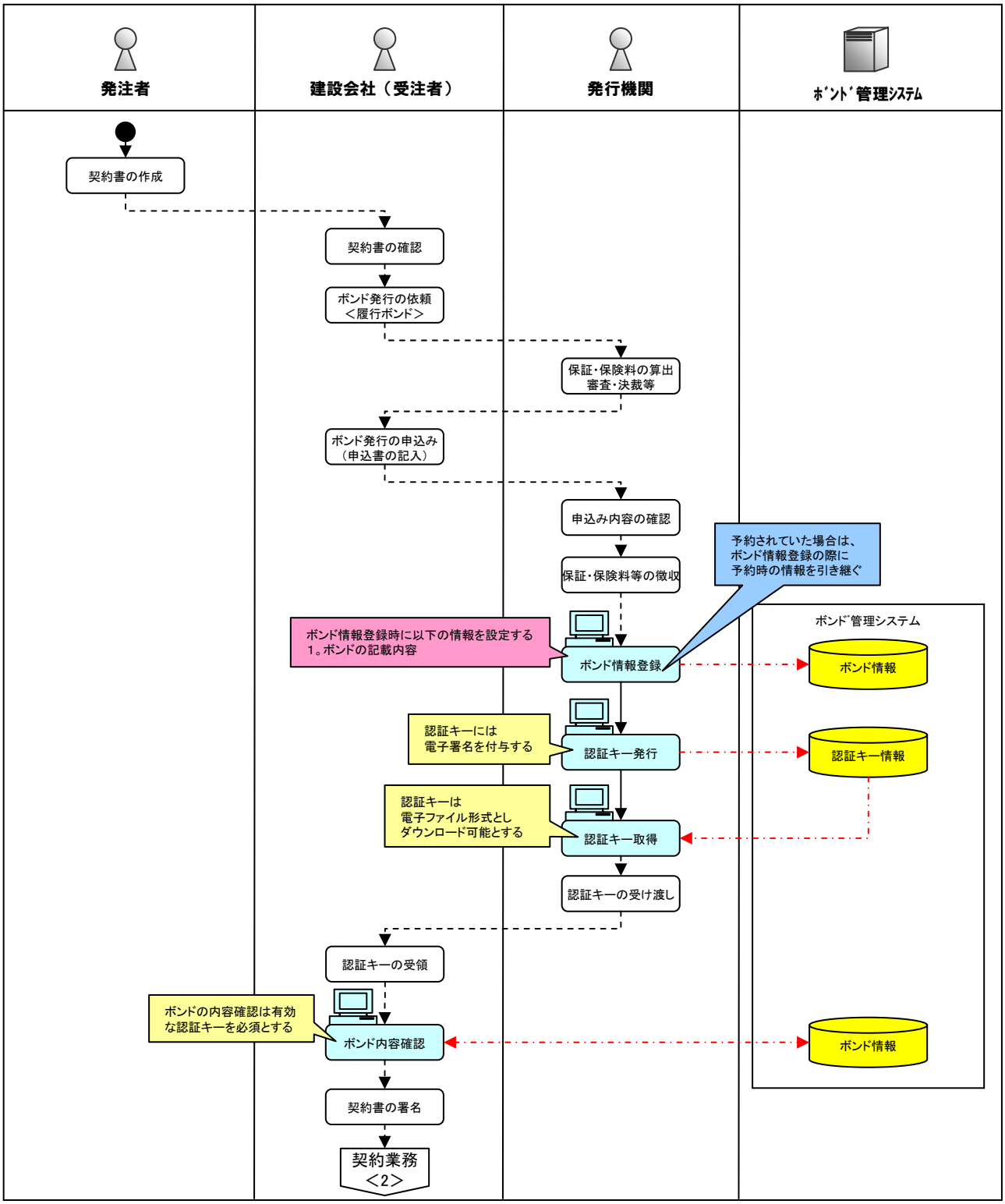
ビジネスフロー

システム名	ボンド管理システム	
ビジネスフローID／名	F01	入札業務＜4＞



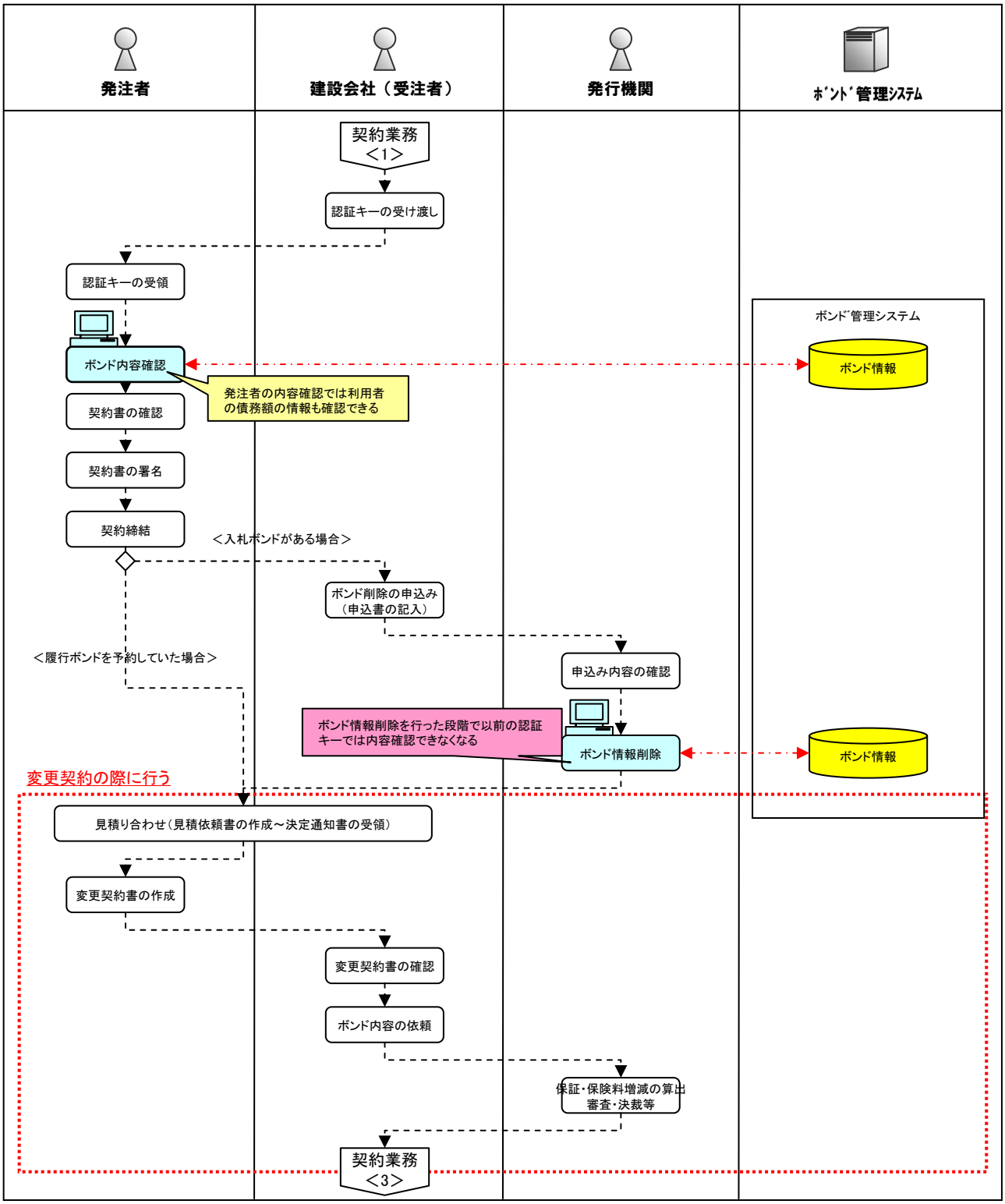
ビジネスフロー

システム名	ボンド管理システム	
ビジネスフローID／名	F02	契約業務＜1＞



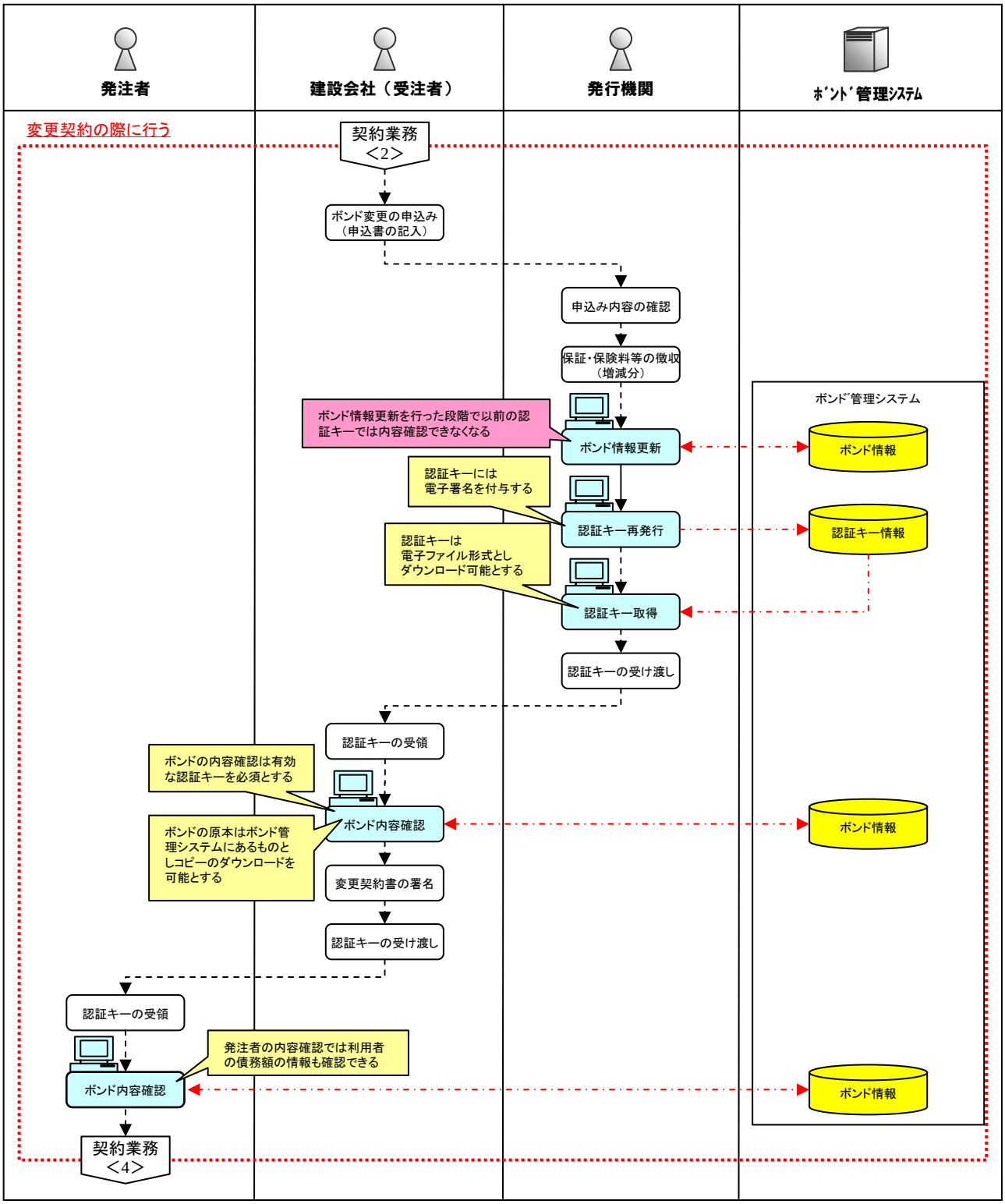
ビジネスフロー

システム名	ボンド管理システム	
ビジネスフローID／名	F02	契約業務＜2＞



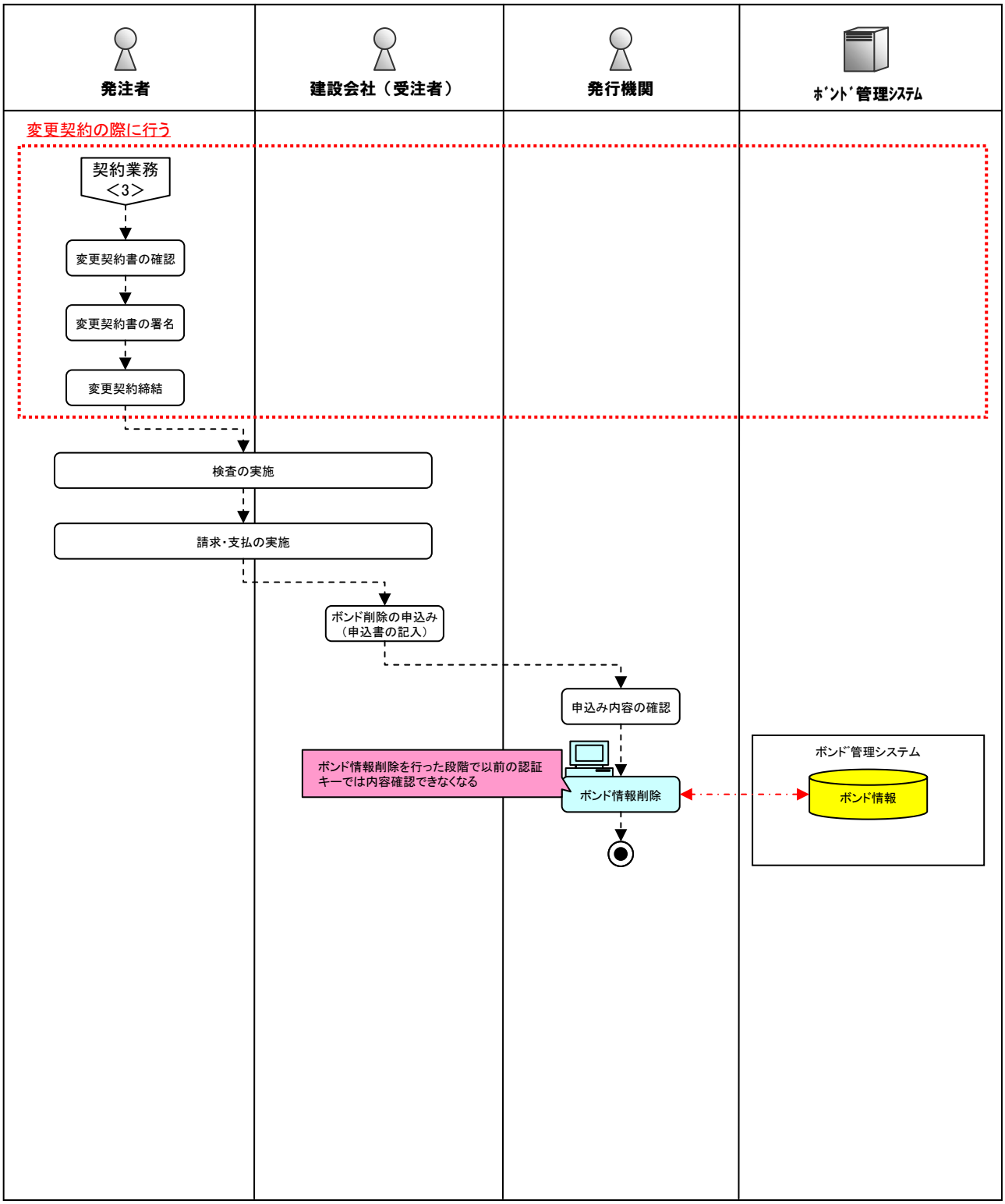
ビジネスフロー

システム名	ボンド管理システム	
ビジネスフローID／名	F02	契約業務＜3＞



ビジネスフロー

システム名	ボンド管理システム	
ビジネスフローID／名	F02	契約業務＜4＞



■ID、パスワードの利用

発行機関、発注者、建設会社ともに、ID、パスワードにてユーザ管理を行うことにより、個人単位での電子化された入札ボンドの閲覧、登録権限の付与など、要望に応じた細かい設定が可能となるが、以下のデメリットも想定される。

① システムへの初期登録が必要
② アクセス権限の付与作業が必要
③ 個人単位での付与の場合は異動等に伴うメンテナンスが煩雑
④ 個人情報の管理が必要

③、④については、発注者、建設会社の多数が保有している電子入札の電子証明書を活用することで対応が可能（発行機関は状況に応じて電子証明書発行用のICカードリーダーの導入が必要）だが、初期登録やアクセス権付与（①、②）についてはID、パスワードの場合と同様な作業が発生する。

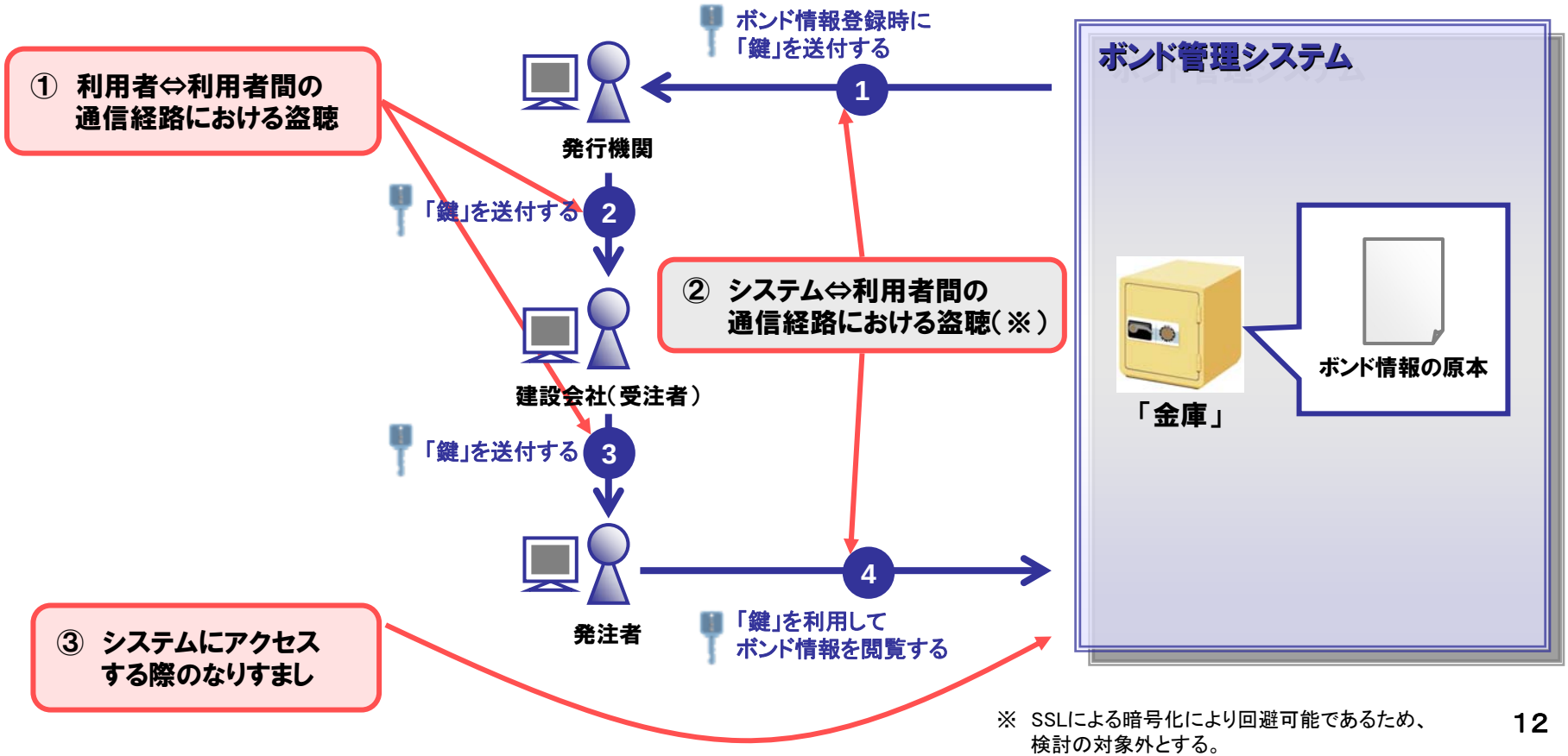
次頁以降ではID、パスワードを利用しない場合の認証方式について、基本的な考え方や認証方式について記載する。

■ID、パスワードを利用しない場合の運用手順とセキュリティリスク

本システムでは、電子化されたボンド情報の管理を下記の通り実施することを検討している。
- 原本はシステム内に保存されている1ファイルのみとする
- その1ファイルを利用者（発注者、発行機関、建設会社）が適宜参照する

上記を前提とした場合、ボンド情報は言わばシステム内の「金庫」に保管される状態となる。

ボンド情報をシステム内の「金庫」に保管する際の、「金庫の鍵」の基本的な運用手順を下図に示す。
また、各手順において、情報セキュリティ上の脅威が考えられる。



※ SSLによる暗号化により回避可能であるため、検討の対象外とする。

■認証方式の比較

本システムにおける認証方式は、「金庫の鍵」を軸として以下の4案が考えられる。各案のメリット（セキュリティ対策効果）とデメリット（コスト）は下表の通りである。

番号	「金庫の鍵」	セキュリティ対策効果		コスト	
		①利⇔利間の盗聴（※）	③なりすまし	費用	運用
1	**パスワード** 数字や文字列から構成されるパスワード	×　→　○ （※）	×	○ 費用はかからない。	○ パスワードを知っているユーザは誰でもアクセスできる。
2	**ワンタイムパスワード** 一定時間ごとに変更されるパスワード	○	×	× 利用者全員によるパスワード生成用ハードウェア/ソフトウェア（「トークン」）の所持が必要。	× トークンを所持しているユーザ以外、アクセスできない。
3	**電子署名されたパスワード** 電子署名されたパスワード	×　→　○ （※）	○	△ 発行機関のクライアント端末に、暗号化のための装置（ICカードリーダ）が必要。	○ 暗号化されたパスワードを所持しているユーザ以外、アクセスできない。
4	**バイオメトリクス** 指紋や静脈などの生体情報	○	○	× 利用者全てのクライアント端末に、生体認証装置が必要。	× 参照権を持ち、かつシステムに生体情報が登録されたユーザ以外、アクセスできない。

（※）「①利用者⇔利用者間の盗聴」リスクについては、下記の方策との併用により回避できる。

番号	方　策	コスト	
		費用	運用
1	**暗号化された電子メールを利用して「鍵」を送付する**	○ フリーの暗号化ツール（PGP等）を利用すれば費用はかからない。	△ 運用開始時のみ、ツールのインストール等の作業が必要。
2	**CD-R等の媒体を利用して送付するなど、回線を介さず「鍵」を送付する**	△ 媒体の費用が必要。	× 物理的な送付に伴う手間が生じる。

■クライアントアプリケーションの要件（案）

ボンド管理システムの利用にあたって、必要となる利用者環境について以下に示す。

項目		条件
端末	OS	Microsoft社製の「Windows」への対応を必須とし、その他のOSへの対応については実証実験時において決定する
	ブラウザ	ブラウザを利用する場合、Microsoft社製の「Internet Explorer」への対応を必須とし、その他のブラウザの対応については実証実験時において決定する
	Java環境	Javaアプレットなどを利用する場合、複数のJavaバージョンに対応可能となるよう検討すること （なお、同一の端末上で操作することになる他システム（特に電子入札コアシステム）への影響を考慮しバージョン等は決定すること）
	その他	ICカードリーダ等が付属されていること（※発行機関の端末のみ）
回線		インターネットへの接続が可能な回線を有すること
証明書 （※発行機関のみ）		以下のすべての条件を満たした証明書を利用可能とする ・ボンド管理システムが要求するプロファイル情報が格納されていること ・以下のいずれかが発行した証明書であること ①商業登記認証局 ②公的個人認証局 ③ブリッジ認証局と相互認証している政府共用認証局もしくは民間認証局 ・ICカードに格納されていること ・標準的なインタフェース仕様に準拠した認証局の発行した証明書であること

■保証債務残高管理の高度化（案）

ボンドの電子化により、各発行機関が発行するボンドのデータをボンド管理システムに登録することで、保証債務残高管理をシステムで行うことができる。
保証債務残高管理の案としては以下の案が挙げられる。

1） 残高について共有する

a）全保証機関における保証債務残高合計
b）各保証機関における保証債務残高
c）ボンド毎の保証残高
d）その他

2） 保証期間と残高について共有する

a）全保証機関における保証債務残高の推移
b）各保証機関における保証債務残高の推移
c）ボンド毎の保証債務残高及び保証期間
d）その他

上記各案の採用にあたって、紙のボンドの保証額を合わせて管理する場合は、発行機関において紙で発行したボンドの保証額の投入が必要となる。