

## ～制御センターによる情報連携システム～



## ID連携トラストフレームワークとは (経済産業省が主催で研究・検討されている)

### 目的

インターネット上で、利用者のデータやサービスの受け渡しを行う企業群が、「利用者が、その相手を信用して情報利用を任せられる」状態であることを保証する枠組みのことである。

(参考)経済産業省「ID連携トラストフレームワーク」:[http://www.meti.go.jp/policy/it\\_policy/id\\_renkei/](http://www.meti.go.jp/policy/it_policy/id_renkei/)

### 目的達成の為の要件

- 1 ユーザの本人確認が、正しく行われること
  - 2 ID パスワードの管理の煩わしさから解放すること
  - 3 公共 民間企業等の間で、情報連携が、安全に適切に行われること
- 上記要件をクリアすることにより、オンライン完結型社会を目指している

### 具体的な利用例

- 1 就職活動に於いて、大学の卒業証書やその他の資格証明書を企業に提供する際
  - 2 公的証明書(納税証明書 所得証明書 不動産登記簿等)を企業側に提出する際
  - 3 医療関係のカルテ等を病院間でやりとりする際等
- ※ 経済産業省主催の「ID連携トラストフレーム・ビジネスコンテスト」において、弊社の「共通1-dayパスワード発行センタ構想」が、アイデア部門で奨励賞を受賞しました(2015年3月)

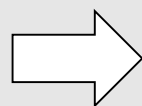
## 背景

### 社会的背景

- オンラインでサービス提供を受ける場合でも、本人確認の為に証明書類を紙に頼っているケースが多い。
- 事業者は、提出される本人確認書類の真偽を確認する手段が少ない。オンラインで即時確認ができない。  
このため、サービス提供までに時間がかかり、利用者、事業者双方が機会損失をしている。
- オンライン完結社会の実現が望まれる。

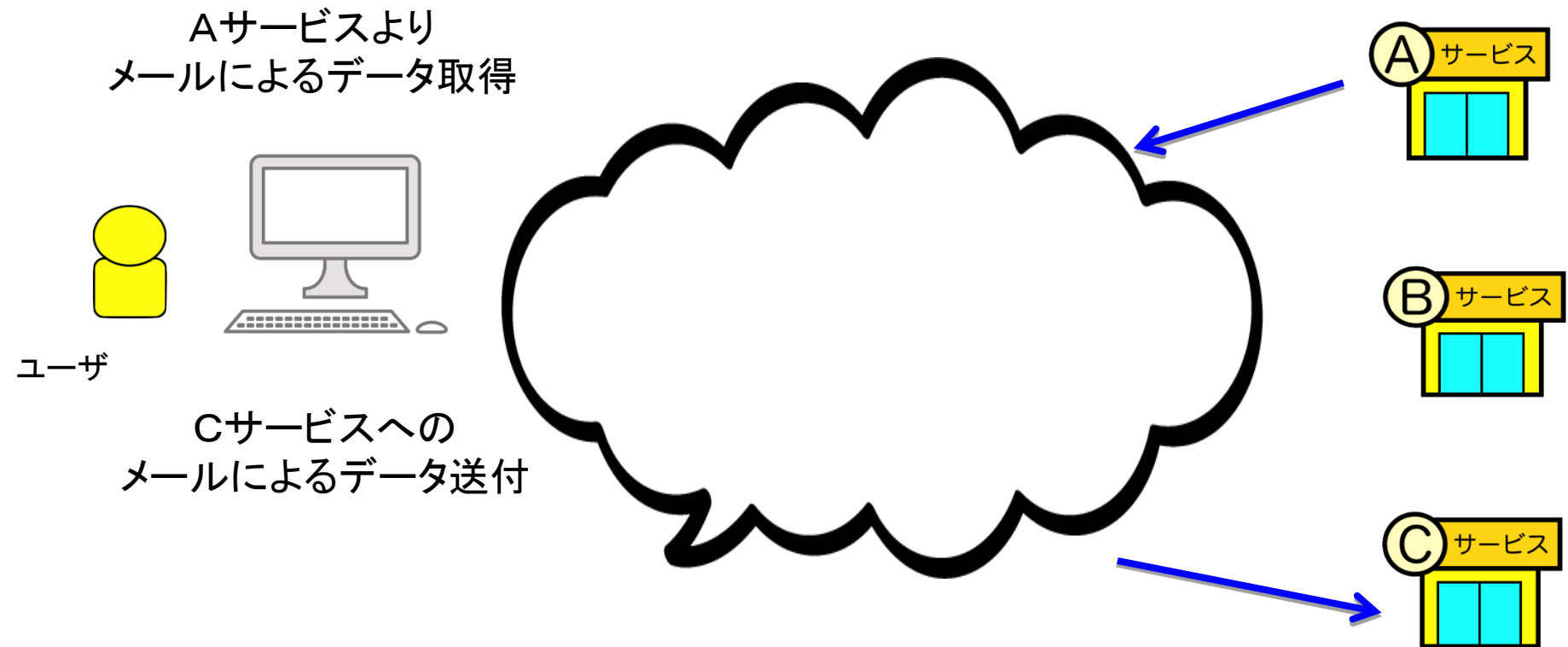
(参考)2015年9月17日JIPDEC資料:「公的個人認証サービスの民間開放に期待されること」

[http://www.meti.go.jp/policy/it\\_policy/id\\_renkei/150917\\_3\\_JIPDEC.pdf](http://www.meti.go.jp/policy/it_policy/id_renkei/150917_3_JIPDEC.pdf)



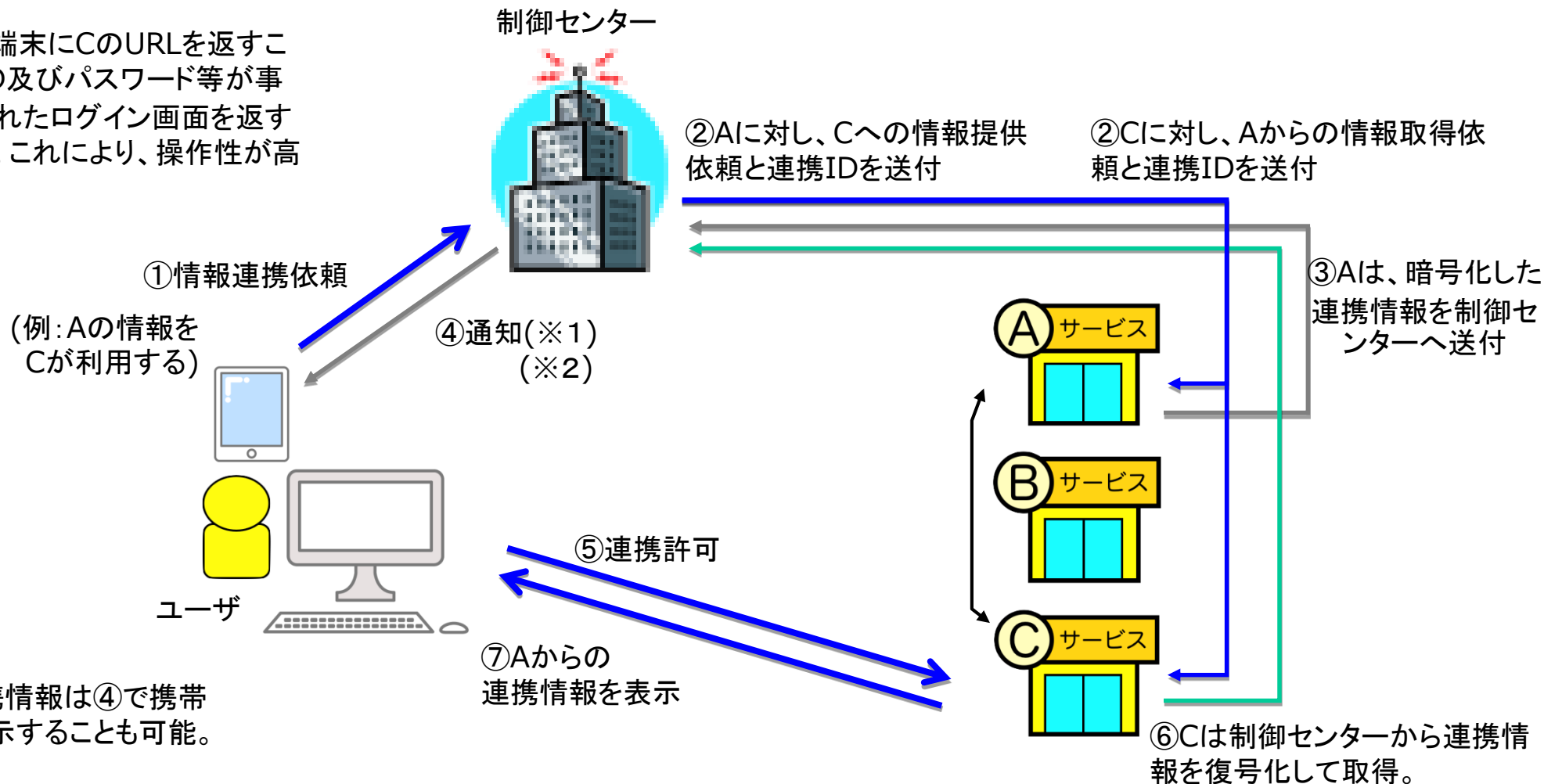
上記課題を解決して、安全性を確保しつつ、且つ、ユーザが関係するサービスシステム間の  
情報連携できる仕組みを着想致しました。

## 従来の連絡方法



## 本システムでの情報連携の流れ

(※1)携帯端末にCのURLを返すことにより、ID及びパスワード等が事前に入力されたログイン画面を返すことが可能。これにより、操作性が高くなる。



(※2)連携情報は④で携帯端末に表示することも可能。

## 特徴

### ユーザが主体

情報連携の対象先は、ユーザが指示して、且つ連携情報の確認後にサービス提供される。ユーザが知らないうちに情報が使われることはない。

### 連携情報の暗号化 並びに証明書の発行

連携情報は、通常は暗号化されて、制御センターに送られる為、その中身を制御センターは、知ることができない。内容は、暗号化されているが、その情報元については、制御センターが、証明書を添付することができる。

### 複数の企業を対象

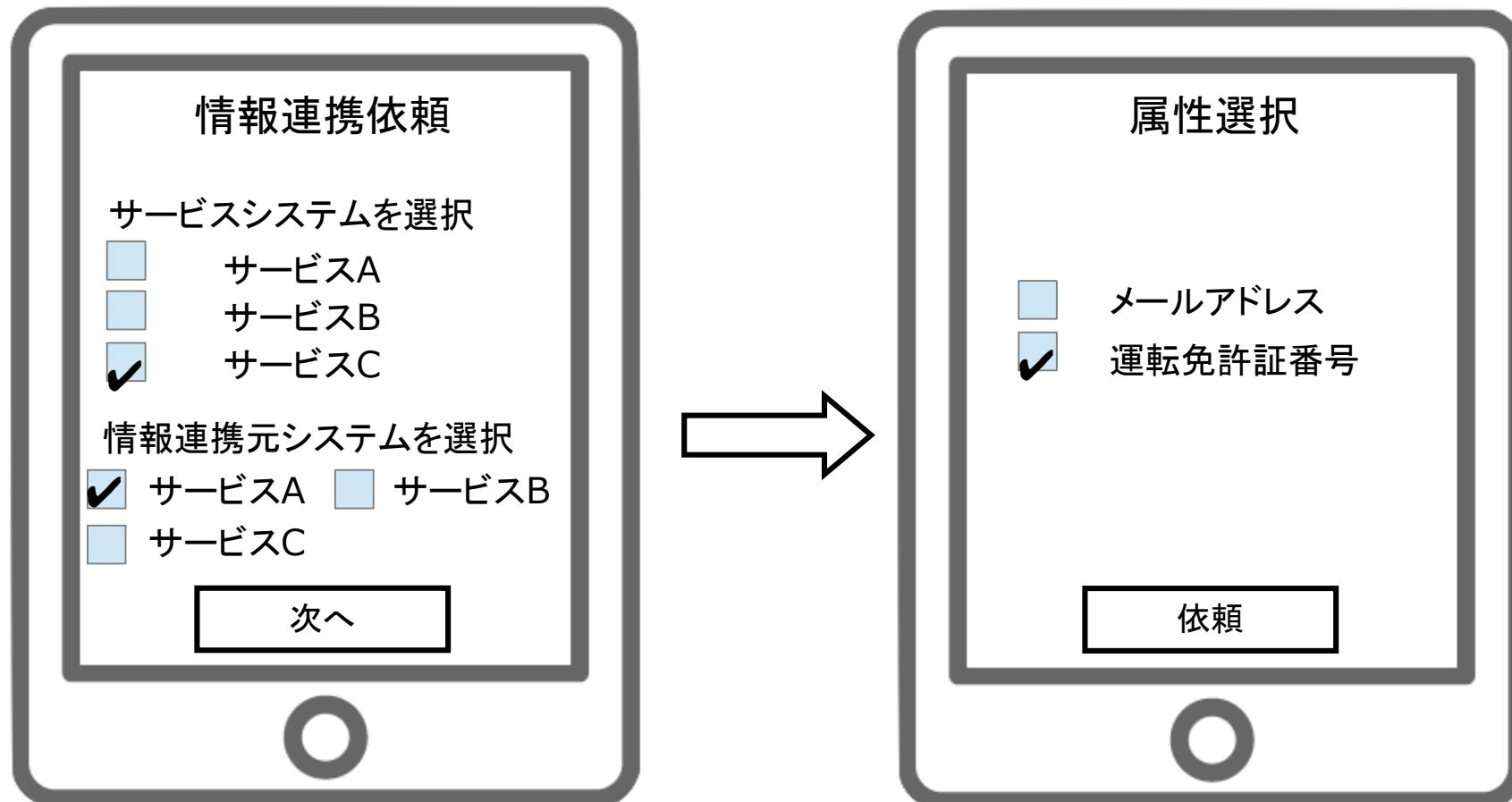
1対NとN対1のいずれの対応も可能である。例えば、ある企業のサービス提供に関して、複数の資格証明書を同時に取得することができる。

### マイナンバー制度への活用

マイナンバー制度で検討されているマイナーポータルへの認証を安全に行い、且つ情報連携を可能にする。

※使用期限・使用回数は柔軟に設定できます。

## 情報連携依頼時の携帯端末の画面遷移



## 選択可能な属性の決め方

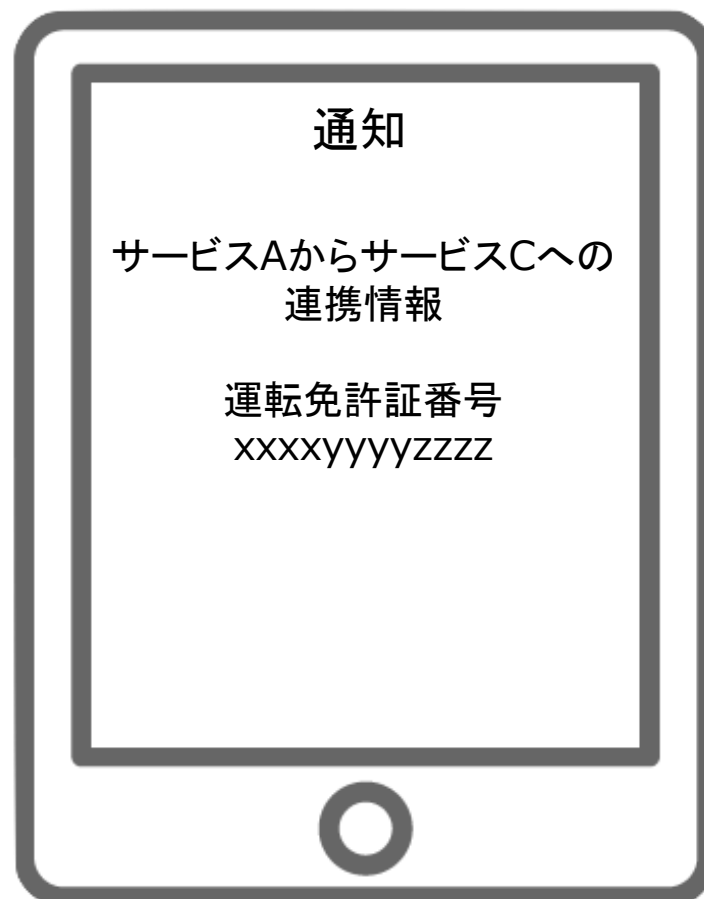
属性	サービスA			サービスB			サービスC		
	保有	提供可否	受入可否	保有	提供可否	受入可否	保有	提供可否	受入可否
ログインID	Y	N	N	Y	N	N	Y	N	N
名前	Y	Y	N	Y	N	N	Y	N	N
メールアドレス	Y	Y	N	Y	N	N	Y	Y	Y
運転免許証番号	Y	Y	N	Y	N	N	N	-	Y
...	...	...	...	...	...	...	...	...	...

- ・本テーブルは制御サーバが保持  
(携帯端末のアプリが保持しても可)
- ・保有“Y”として実際の値が入っていても可

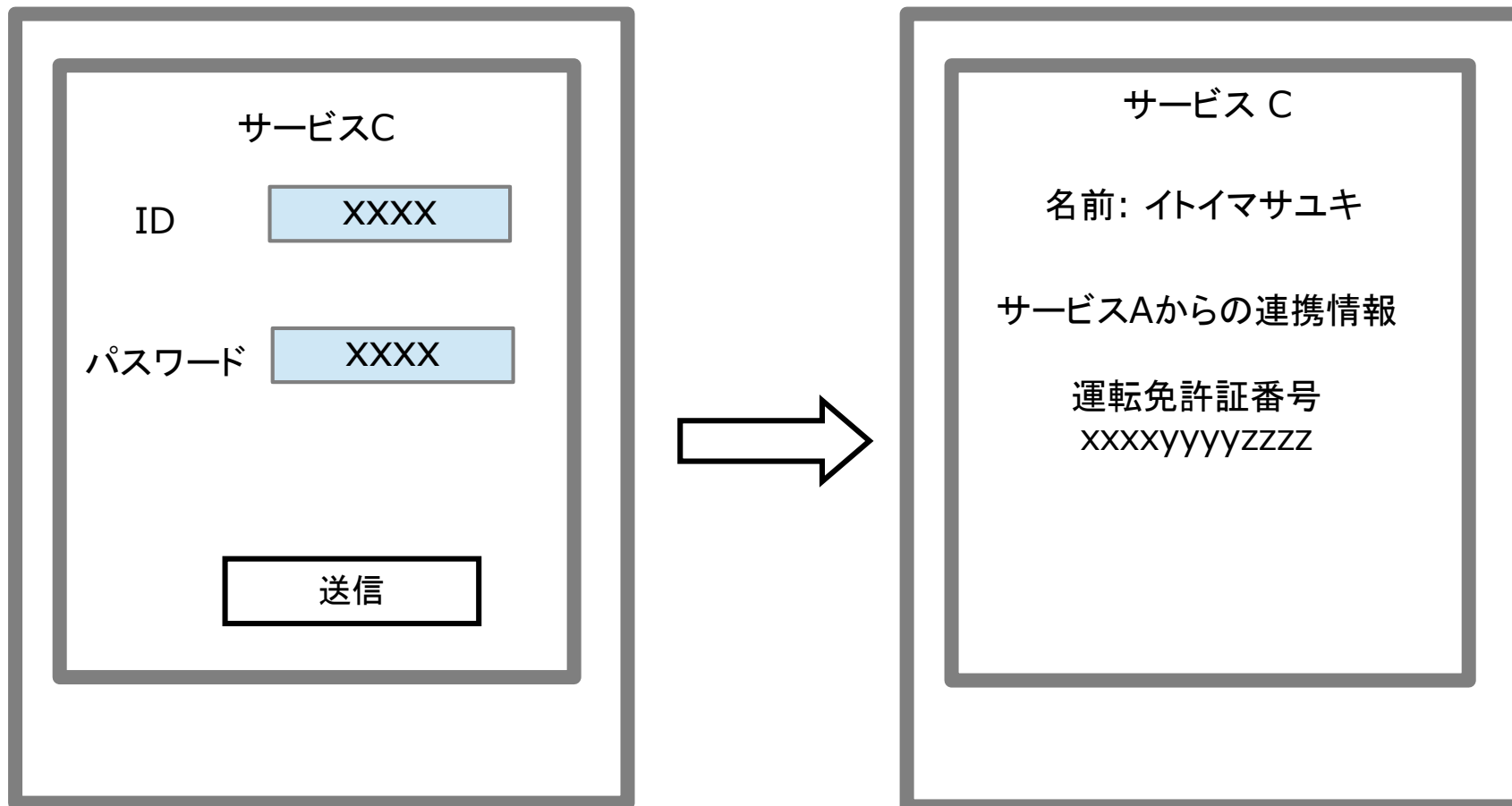
サービスA(連携元)が提供可(Y)、且つ、  
サービスC(連携先)が受入可(Y)  
= **選択可能な属性**



## 通知時の携帯端末の画面



## PC画面の遷移



## 情報連携の流れ (認証システムとの組合せ)

(※1)携帯端末にCのURLを返すことにより、ID及びパスワード等が事前に入力されたログイン画面を返すことが可能。これにより、操作性が高くなる。

制御センター



②パスワード発行

③Aに対し、Cへの情報提供依頼と連携IDを送付

③Cに対し、Aからの情報取得依頼と連携IDとパスワードを送付

①パスワード発行&情報連携依頼

(例:Aの情報を利用する)

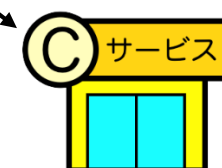
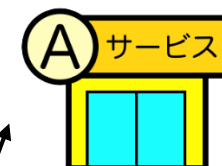


ユーザ

⑤パスワード通知(※1)  
(※2)

⑥通知されたパスワードでログインし、連携許可

⑧Aからの連携情報を表示

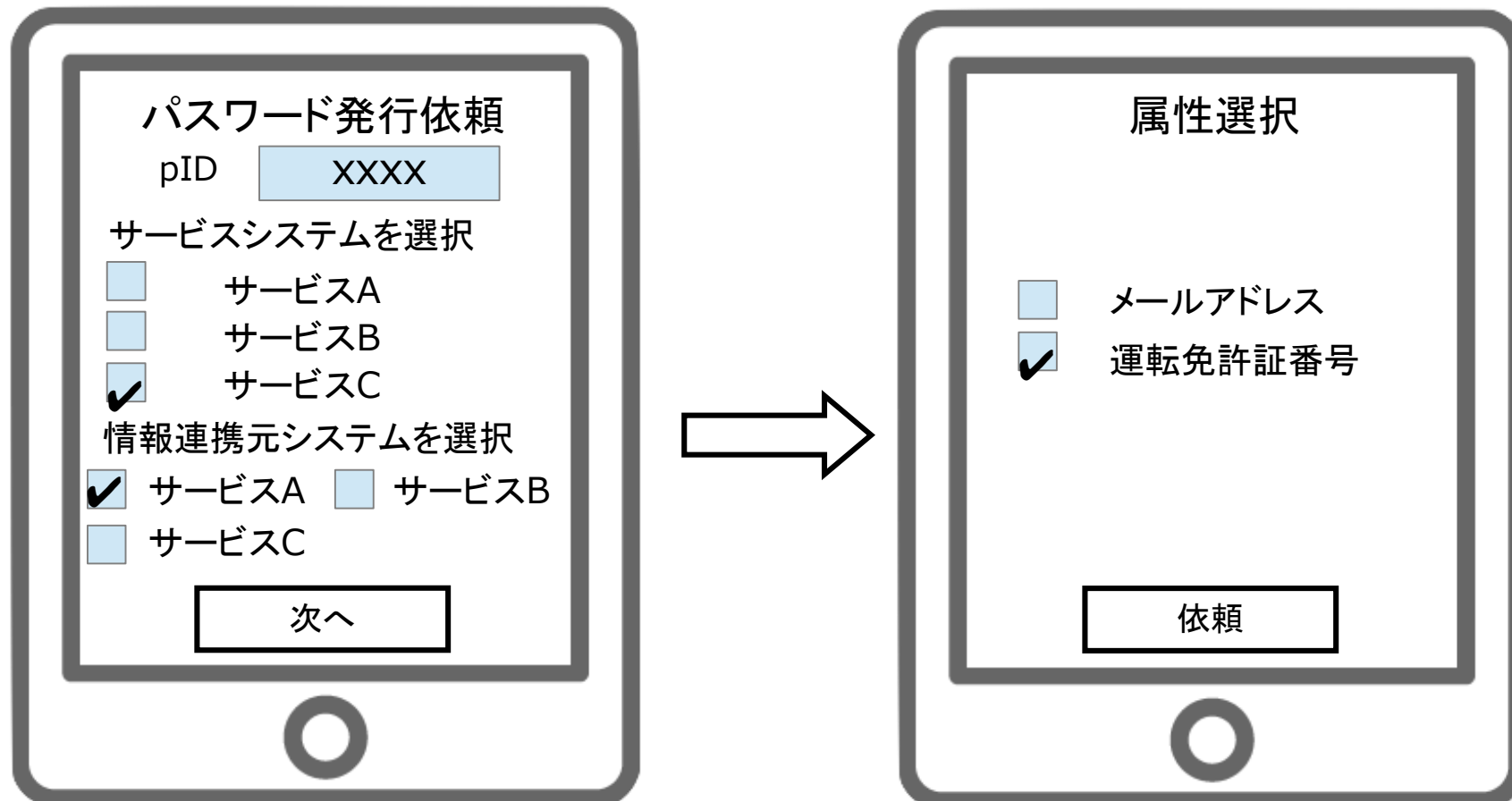


④Aは、暗号化した連携情報を制御センターへ送付

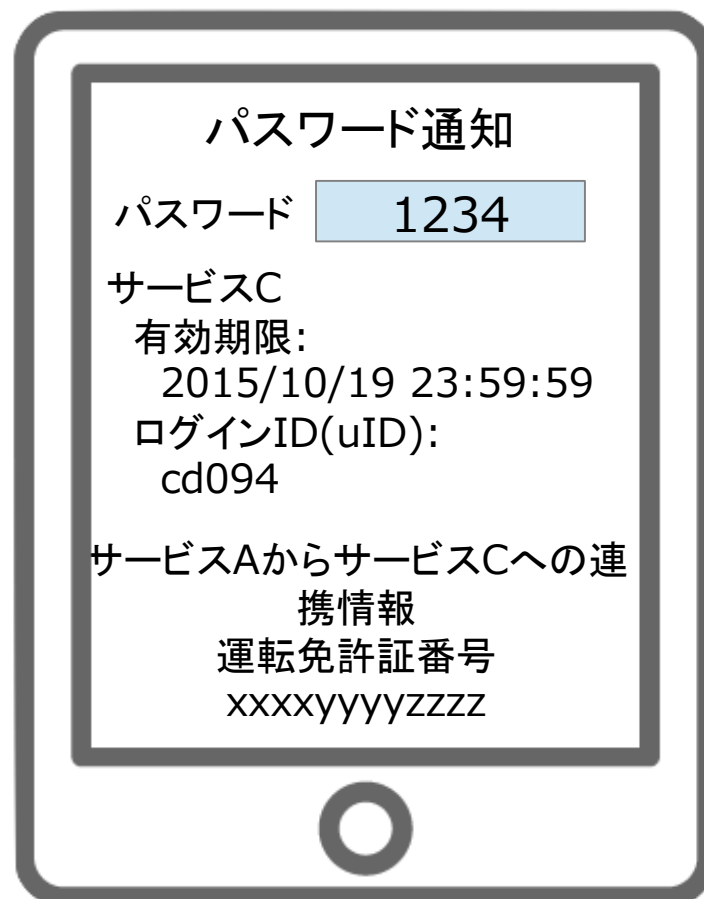
⑦Cは制御センターから連携情報を復号化して取得。

(※2)連携情報は④で携帯端末に表示することも可能。

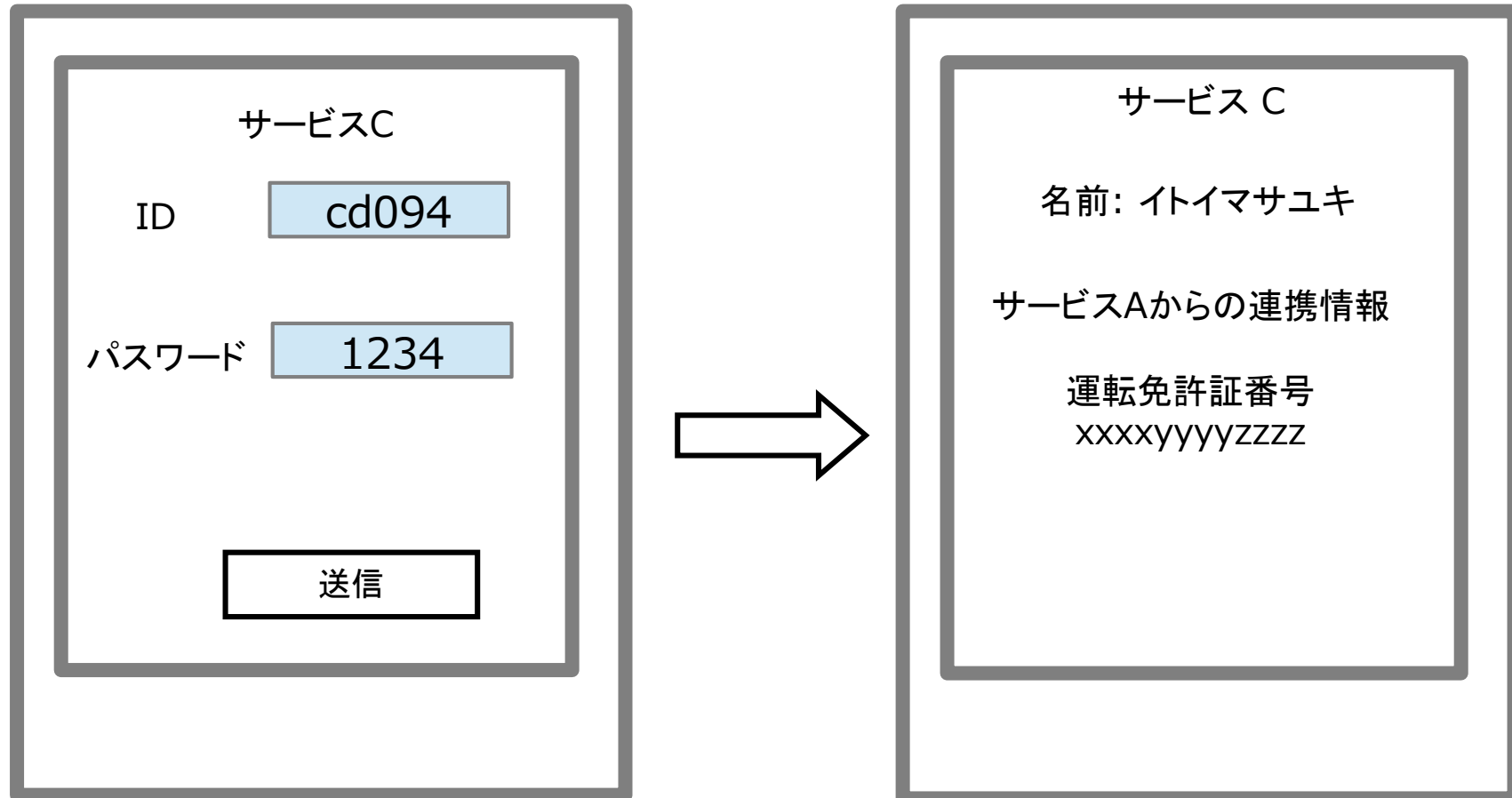
## パスワード発行&情報連携依頼時の携帯端末の画面遷移 (認証システムとの組合せ)



## パスワード通知時の携帯端末の画面 (認証システムとの組合せ)



## PC画面の遷移 (認証システムとの組合せ)



ご精読  
ありがとうございました