

2009年度第4回ITリスク学研究会

一般消費者向けWebサービスにおける
認証情報の盗難を前提としたなりすまし対策に関する考察

A study on measures for the spoofing attack
in the Web Service for general consumers

2010年1月16日

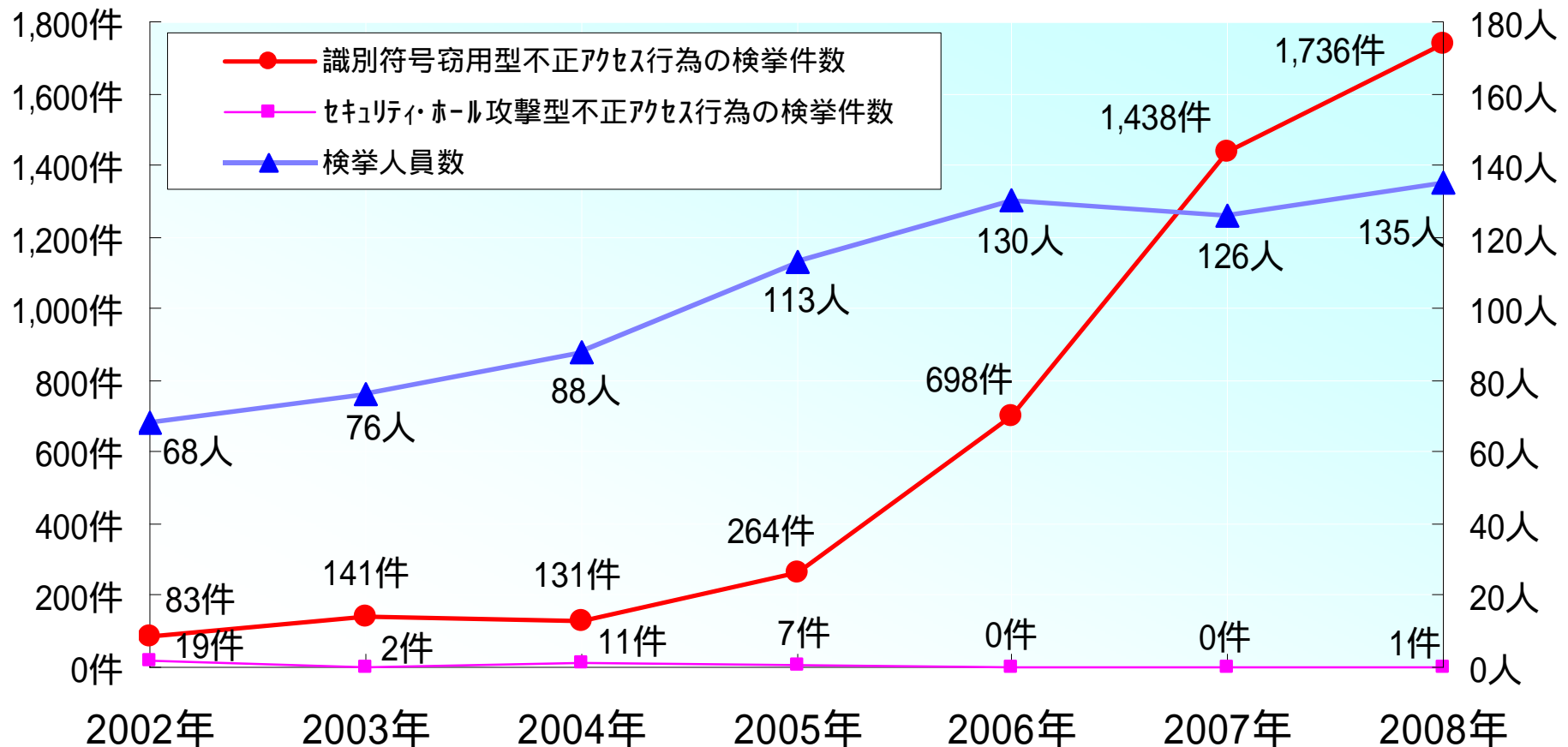
情報セキュリティ大学院大学
小柳研究室 修士課程2年 磯貝 雄治

1. なりすまし被害の発生状況とその原因
2. 認証情報の盗難を前提としたなりすまし対策の必要性
3. インターネット・バンキングにおけるなりすまし対策の実施状況
4. 認証情報の盗難を前提としたなりすまし対処の分類
5. 認証情報の盗難を前提としたなりすまし対策の強化案
6. まとめ

1. なりすまし被害の発生状況とその原因
2. 認証情報の盗難を前提としたなりすまし対策の必要性
3. インターネット・バンキングにおけるなりすまし対策の実施状況
4. 認証情報の盗難を前提としたなりすまし対処の分類
5. 認証情報の盗難を前提としたなりすまし対策の強化案
6. まとめ

認証情報の盗用による犯罪件数の増加

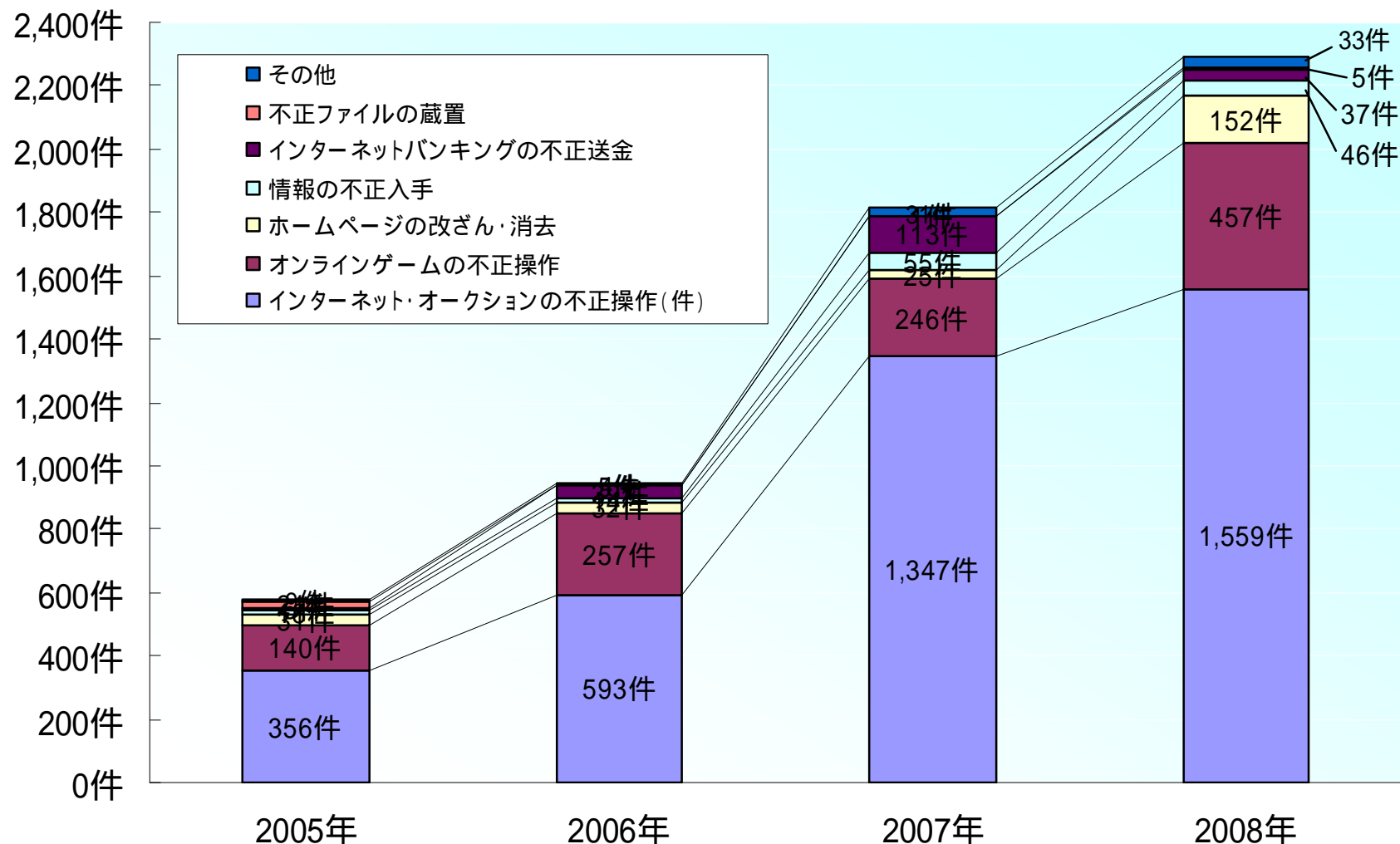
不正アクセス禁止法違反の検挙件数と検挙人員数の推移（警察庁）



検挙件数は急増しているのに検挙人員数に変化が少ない 認証情報の流出が増えている

不正アクセス行為の目的

不正アクセス行為後の行為の内訳の推移（警察庁）



不正アクセス行為の動機

不正アクセス行為の動機の内訳（警察庁）

不正アクセス行為の動機	2005年	2006年	2007年	2008年
不正に金を得るため	167件	419件	1,186件	1,498件
オンラインゲームで不正操作を行うため	25件	211件	133件	120件
嫌がらせや仕返しのため	31件	31件	62件	52件
好奇心を満たすため	20件	26件	55件	17件
顧客データの収集等情報を不正に入手するため	23件	10件	0件	12件
料金の請求を免れるため	0件	1件	2件	3件
自分の技量を図るため	2件	0件	0件	0件
その他	3件	0件	0件	35件
計	271件	698件	1,438件	1,737件

インターネット・バンキングにおける被害状況

インターネット・バンキングによる預金等不正払戻し(被害発生状況・補償状況) (金融庁)

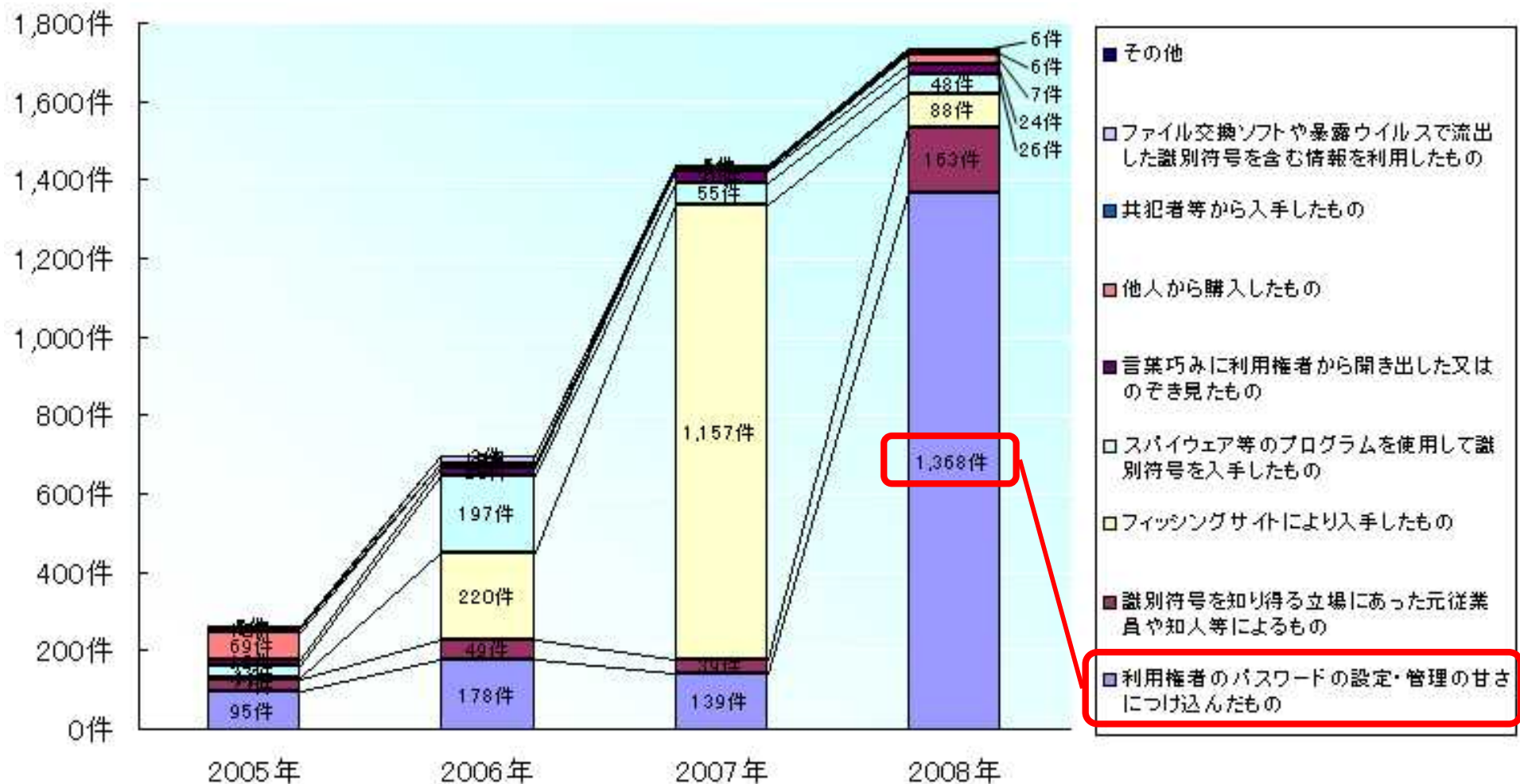
時期	計			補償の状況(件)			
	件数 (件)	金額 (百万円)	平均被害額 (万円)	処理方針決定済			調査・検討中 等
				計	補償	補償しない	
2005年2月～3月	1	0	0	1	-	1	-
2005年度	49	105	214	47	38	9	2
2006年度	102	129	127	96	69	27	6
2007年度	233	191	81	207	186	21	26
2008年度	136	142	105	60	32	28	76
4月～6月	48	84	175	37	23	14	11
7月～9月	7	19	273	4	-	4	3
10月～12月	38	16	42	9	4	5	29
1月～3月	43	23	54	10	5	5	33
2009年度	24	13	56	5	1	4	19
4月～6月	17	7	43	4	-	4	13
7月～9月	7	6	88	1	1	-	6
計	545	582	106	416	326	90	129

(注1)平成21年10月15日までに金融庁及び財務局に報告のあった被害を集計している。

(注2)「時期」とは被害の発生した年度(又は四半期)を示す。

認証情報の盗取手口


識別符号窃用型不正アクセス行為に係わる犯行の手口の内訳（警察庁） (認証情報の盗用による不正アクセス)



1. なりすまし被害の発生状況とその原因
2. **認証情報の盗難を前提としたなりすまし対策の必要性**
3. インターネット・バンキングにおけるなりすまし対策の実施状況
4. 認証情報の盗難を前提としたなりすまし対処の分類
5. 認証情報の盗難を前提としたなりすまし対策の強化案
6. まとめ

一般消費者向けWebサービスの認証情報管理における問題点

1. 認証情報はサービス利用者が管理することになっている
 - サービス提供者側だけでサービス利用者の認証情報を盗難から保護することはできない
2. Webサービスは基本的に誰でも利用することができる
 - サービス利用者のセキュリティに関する認識や知識は一様ではない
 - 年齢も様々であるので、システムに対する理解力や学習能力は一様ではない
3. 操作端末はサービス利用者の私有物であるか、第三者の所有物である
 - サービス利用者の操作端末のセキュリティに対して直接的な関与ができない
4. サービスを利用するかどうかの選択権は一般消費者側にある
 - サービス提供者にとってはサービスを利用してもらわなければ意味が無い
 - サービス利用者に対して強制的な指導や教育、監査等を行う、管理が悪ければ強制的に排除する、といった行為を実施することが現実的に不可能である。
 - セキュリティのために利便性を犠牲にすることが必ずしも受け入れられるかどうか分からない
5. 守るべき資産はサービス利用者自身のものである
 - 守るべき資産が他人のものではないので、資産保護に対する使命感や責任感、あるいはプレッシャーというものをサービス利用者は持つ必要性がない

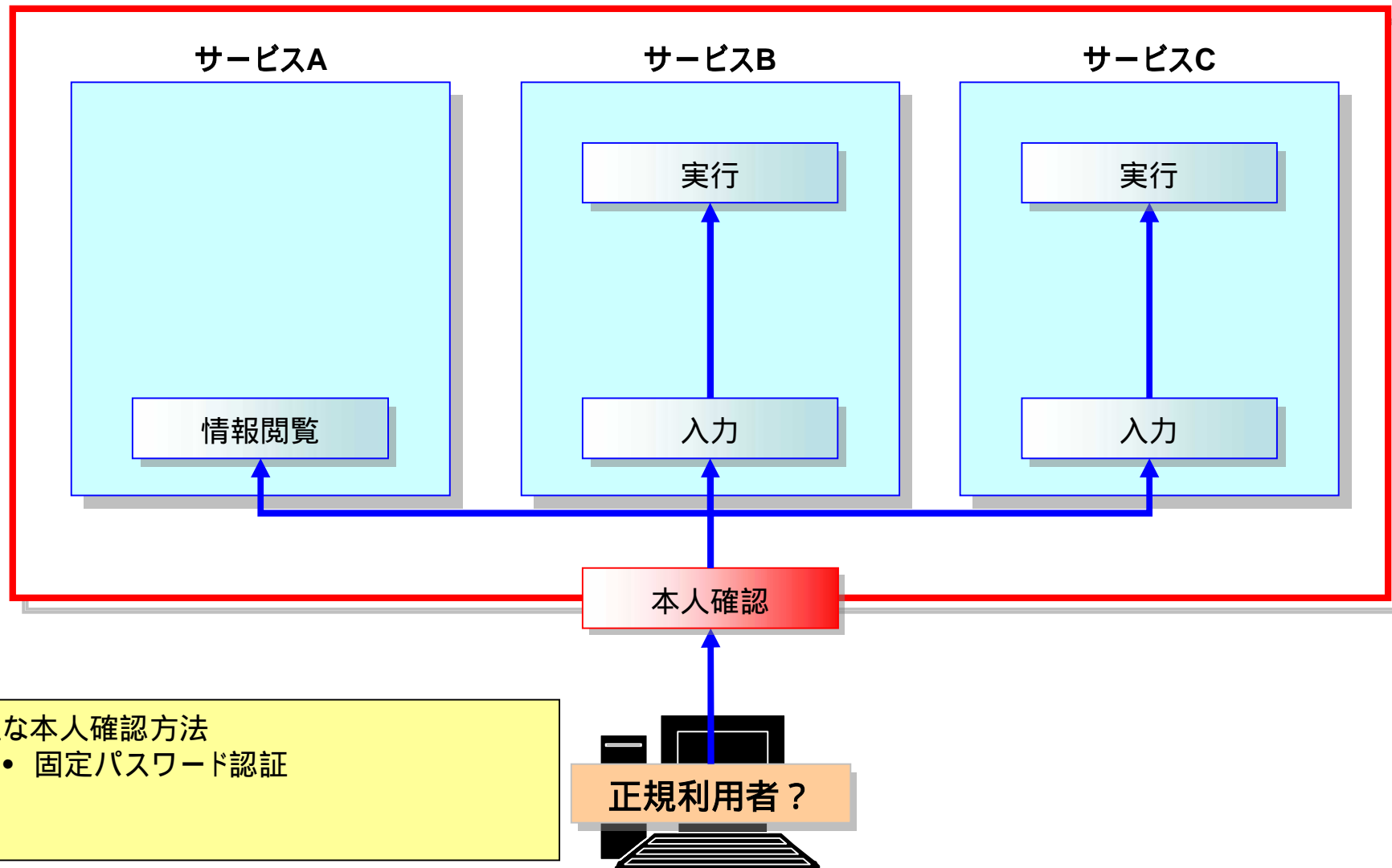
- 
- サービス利用者から認証情報の盗難が無くなることは期待できない
 - サービス提供者側からの認証情報の流出も実際に発生している

認証情報の盗難を前提としたなりすまし対策が必要である

1. なりすまし被害の発生状況とその原因
2. 認証情報の盗難を前提としたなりすまし対策の必要性
3. インターネット・バンキングにおけるなりすまし対策の実施状況
4. 認証情報の盗難を前提としたなりすまし対処の分類
5. 認証情報の盗難を前提としたなりすまし対策の強化案
6. まとめ

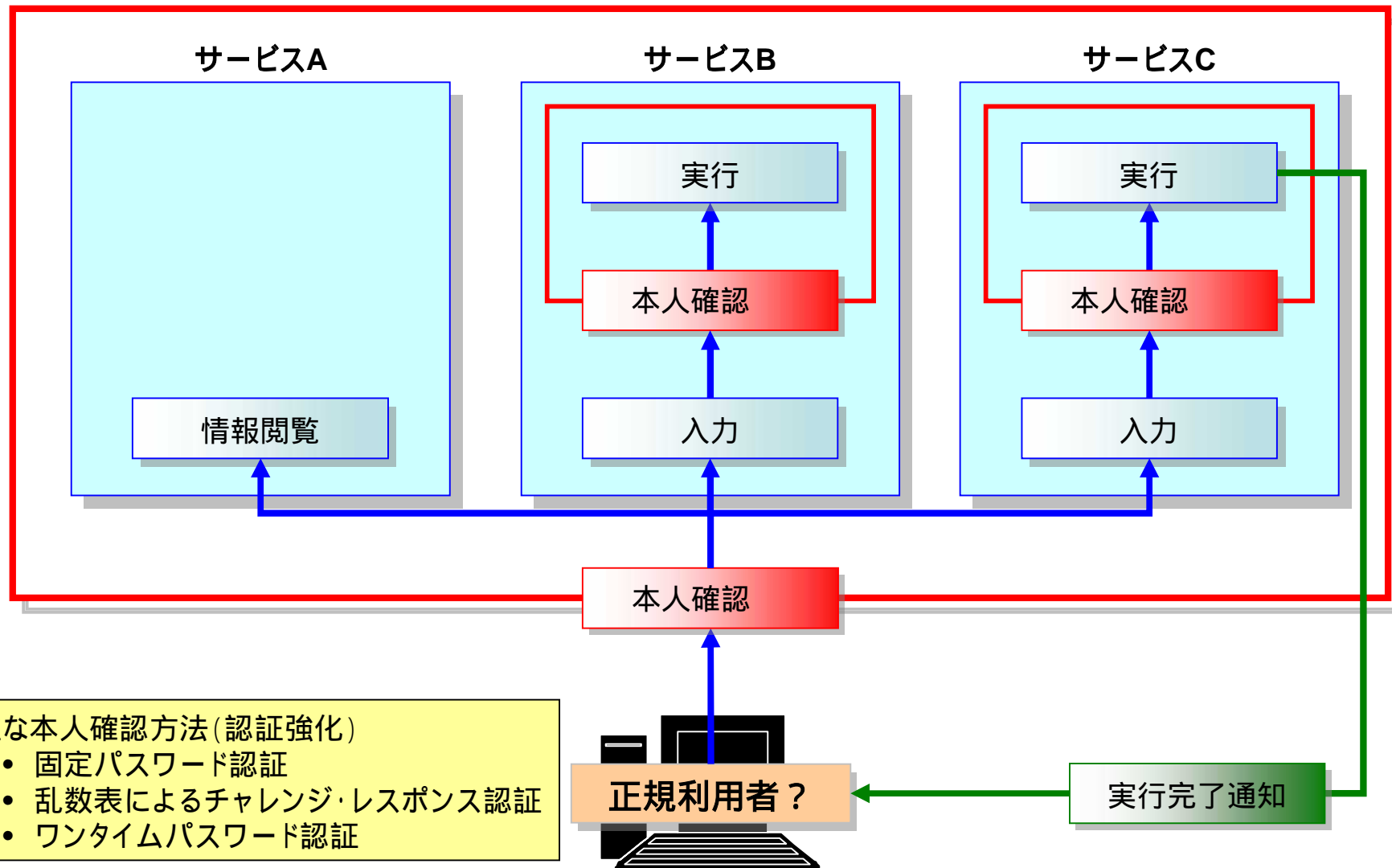
これまでのなりすまし対策

サービス提供サイト

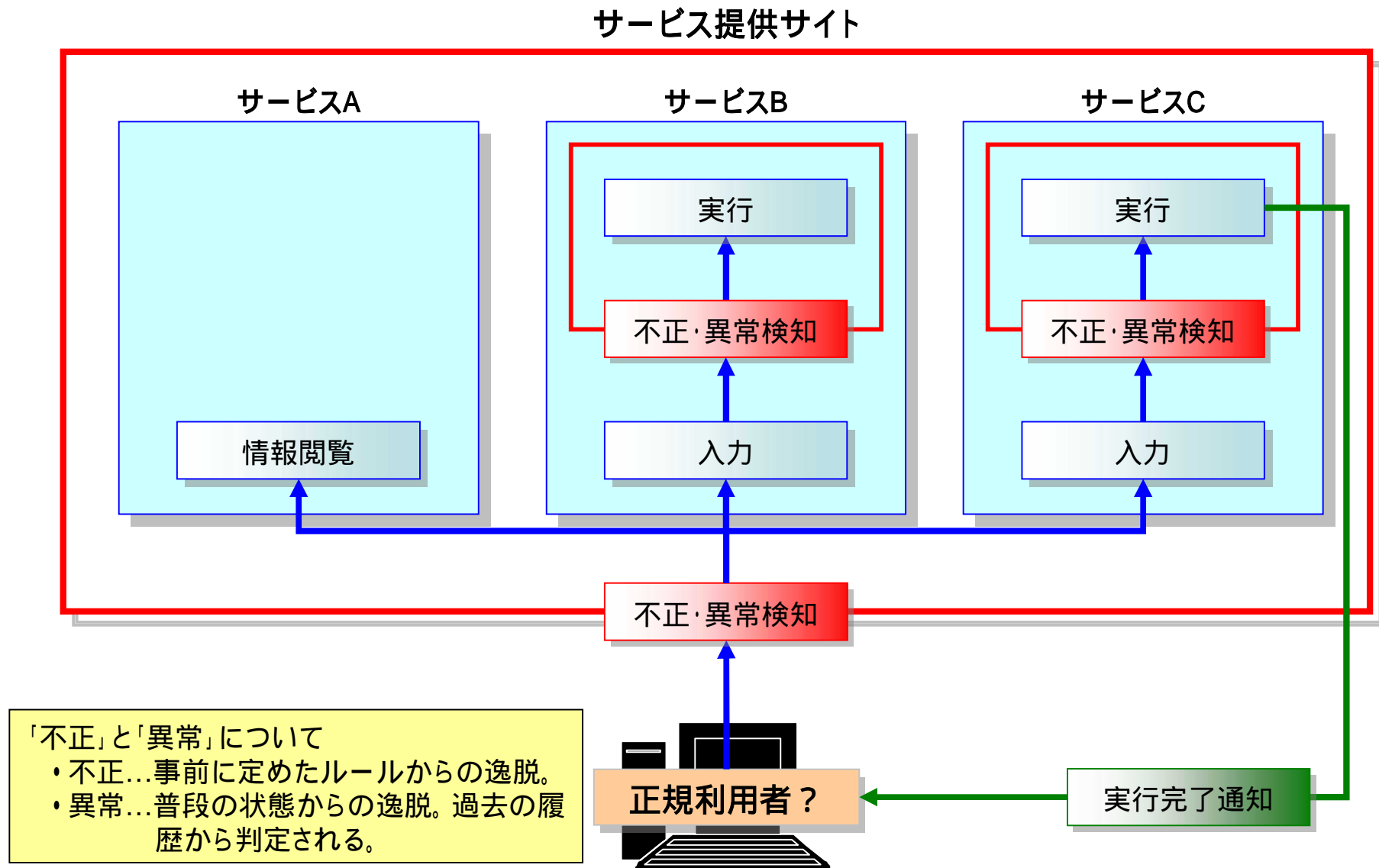


認証の強化・本人確認の二重化(追加認証)・サービス実行の通知

サービス提供サイト

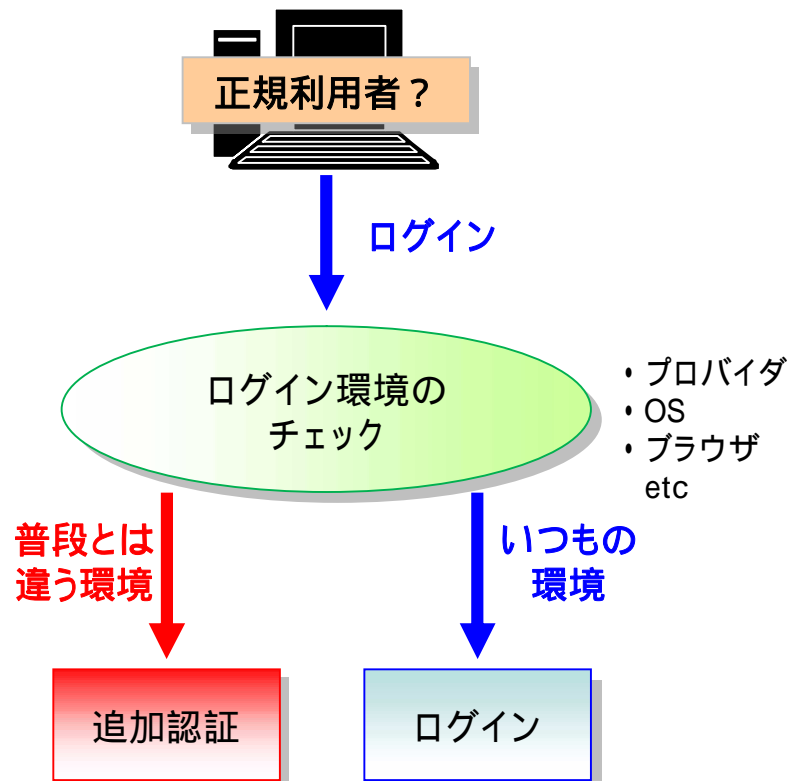


100

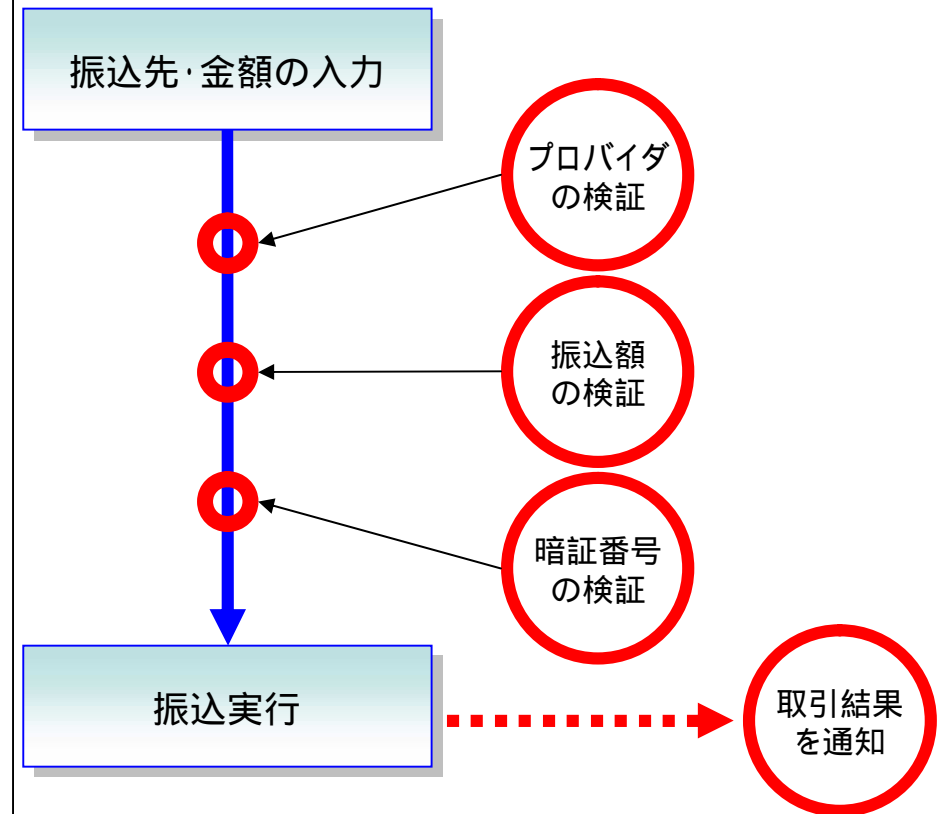


不正・異常の検知の例

リスクベース認証



振り込み時の不正・異常検知 (利用プロバイダの限定・振込限度額の設定 ・追加認証・取引完了通知)



ログイン時のなりすまし対策

インターネット・バンキング・サイトのなりすまし対策実施状況(ログイン時)

順位	銀行名	ログイン					
		PC利用の 一時停止	利用PC の限定	利用プロバイダ の限定	リスクベース 認証	ログイン通知 サービス	ログイン 履歴
1	A銀行	×	×	×	×	×	
2	B銀行	×		×	×	×	
3	C銀行	×	×			×	
4	D銀行	×	×	×		×	
5	E銀行	×	×	×	×	×	
6	F銀行	×	×	×	×	×	
7	G銀行	×	×	×	×	×	
8	H銀行	×	×	×		×	
9	I銀行		×	×	×		
10	J銀行	×	×	×	×	×	

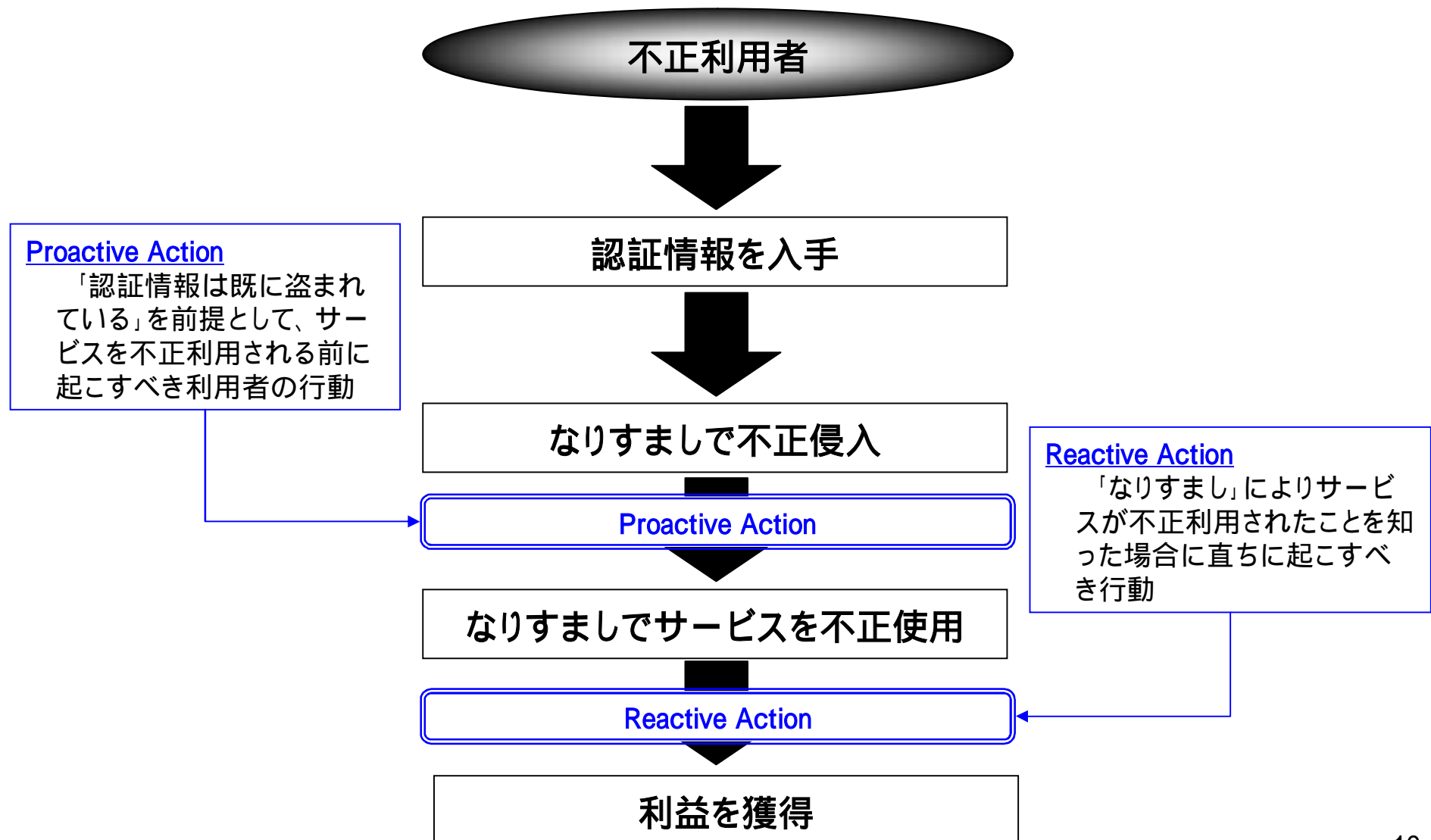
サービス提供時のなりすまし対策

インターネット・バンキング・サイトのなりすまし対策実施状況(振込み時)

順位	銀行名	振込み(出金)				
		振込限度額 の設定	振込先 の制限	追加認証		取引完了 通知
				初期	強化オプション	
1	A銀行		×	第一暗証(数字4桁)	暗証カード	
2	B銀行		×	取り引き暗証番号 (5ケタの半角数字)		
3	C銀行		×	暗証番号	暗証番号+ワンタイム認証	
4	D銀行		×	ご利用カード(乱数表)	ワンタイムパスワード	
5	E銀行		×	WEB取引パスワード +認証番号表	WEB取引パスワード +モバイルキー	
6	F銀行			ワンタイムパスワード		
7	G銀行		×	確認ナンバー (キャッシュカード裏面記載)		
8	H銀行		×	第2暗証番号の ランダム入力	ワンタイムパスワード	
9	I銀行		×	暗証番号		
10	J銀行		×	ご契約カードの確認番号		

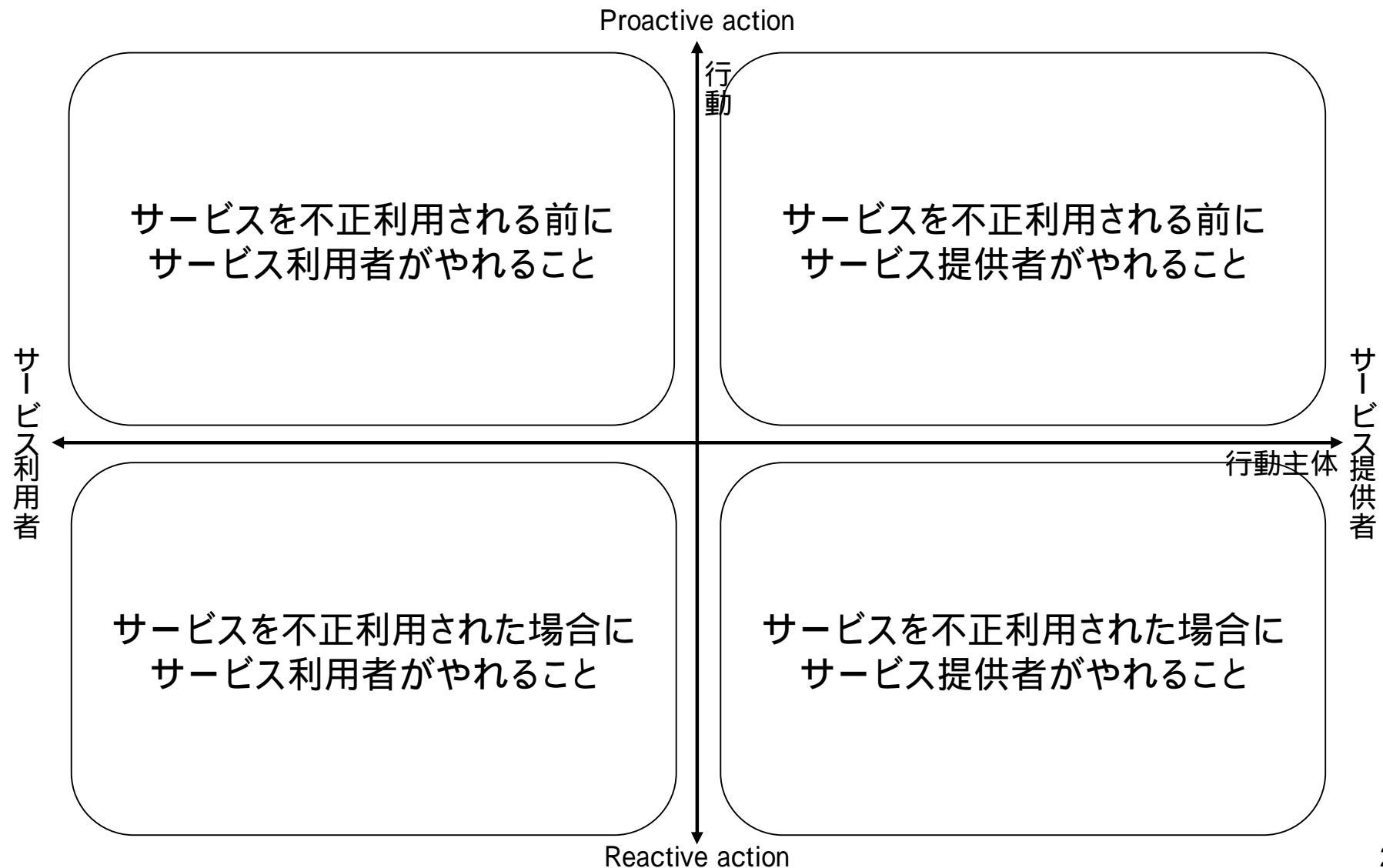
1. なりすまし被害の発生状況とその原因
2. 認証情報の盗難を前提としたなりすまし対策の必要性
3. インターネット・バンキングにおけるなりすまし対策の実施状況
4. **認証情報の盗難を前提としたなりすまし対処の分類**
5. 認証情報の盗難を前提としたなりすまし対策の強化案
6. まとめ

なりすまし対処における行動の分類



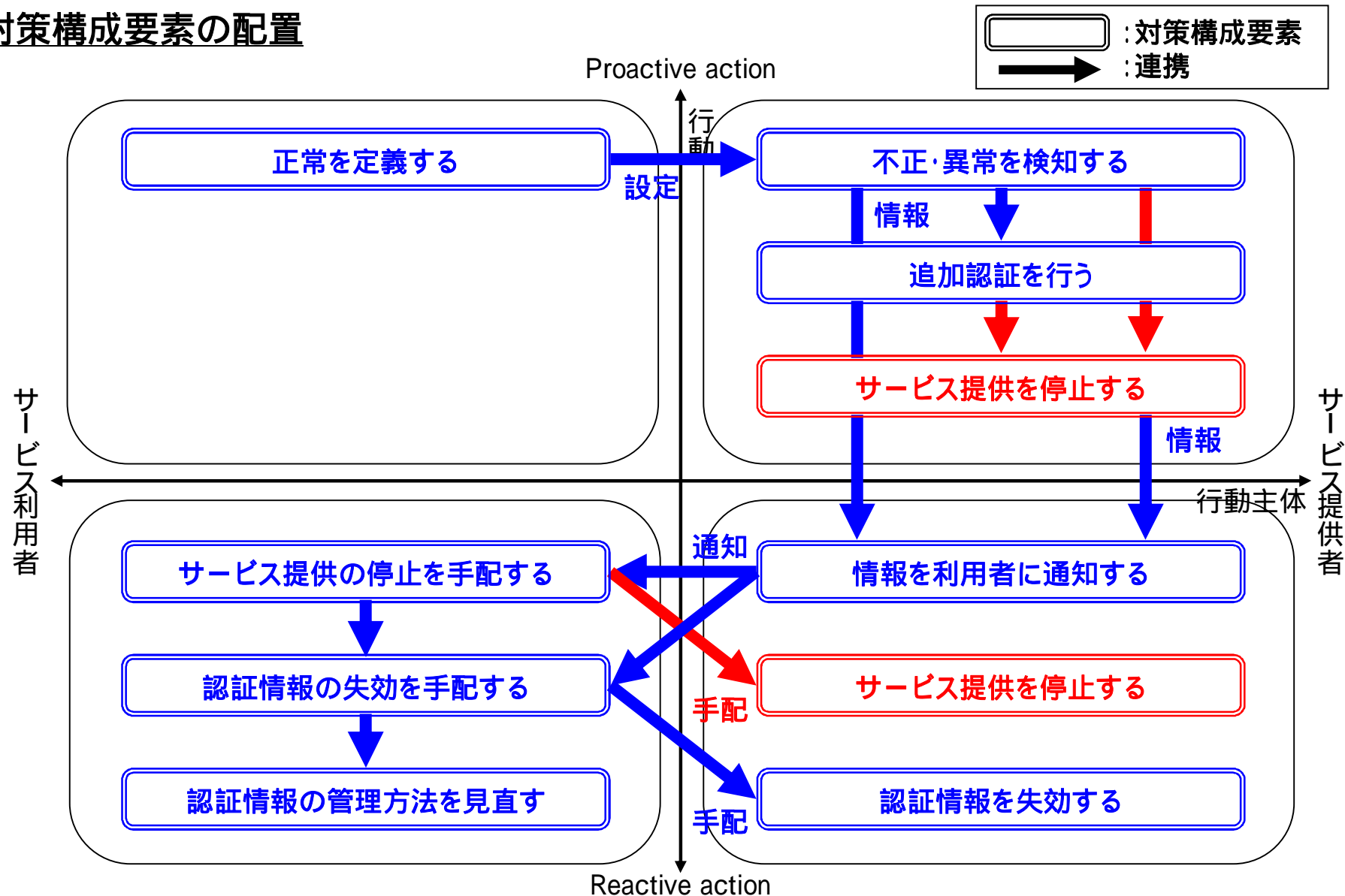
なりすまし対策構成要素配置図

なりすまし対策構成要素配置図



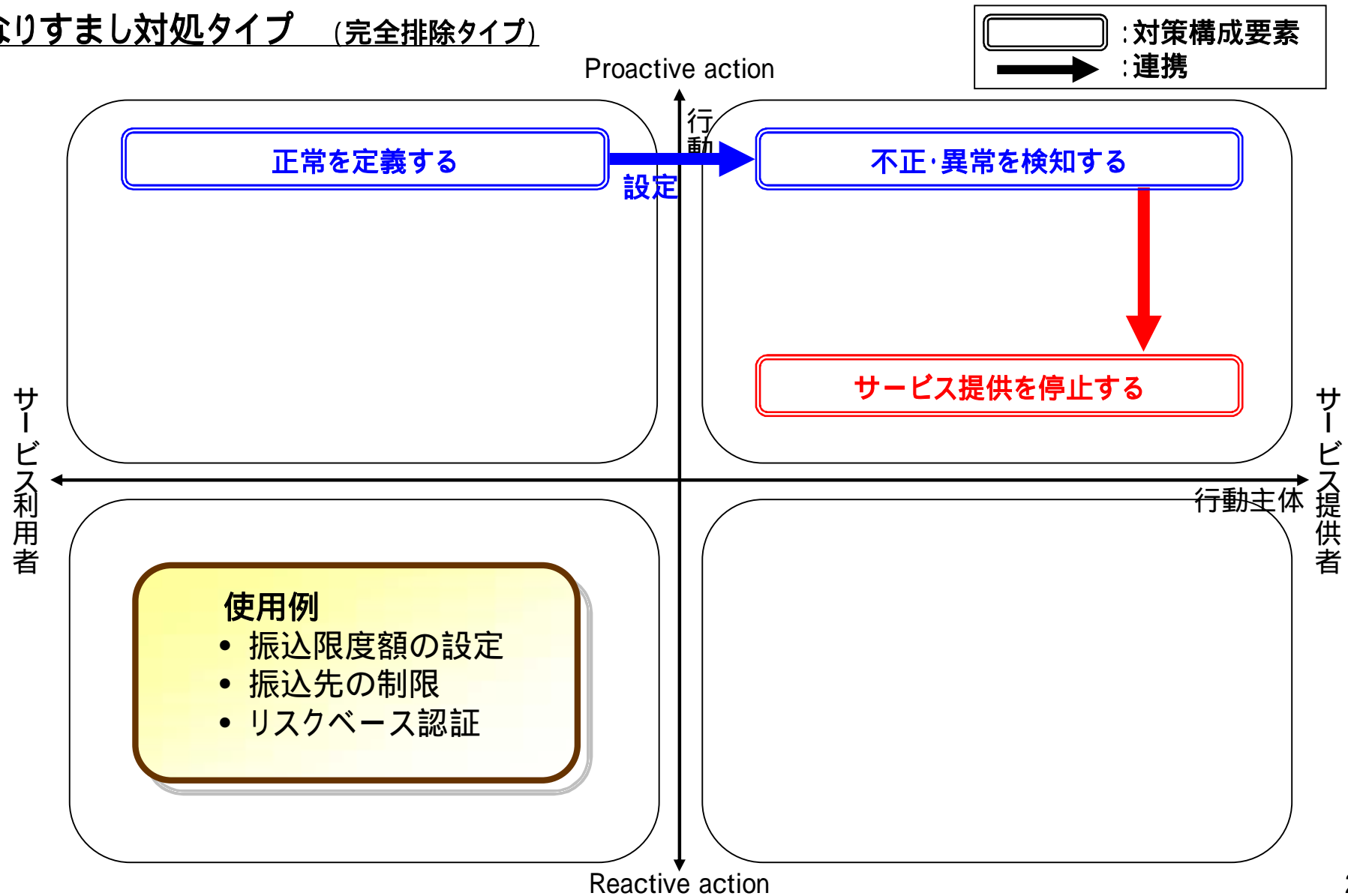
なりすまし対策構成要素配置図

対策構成要素の配置



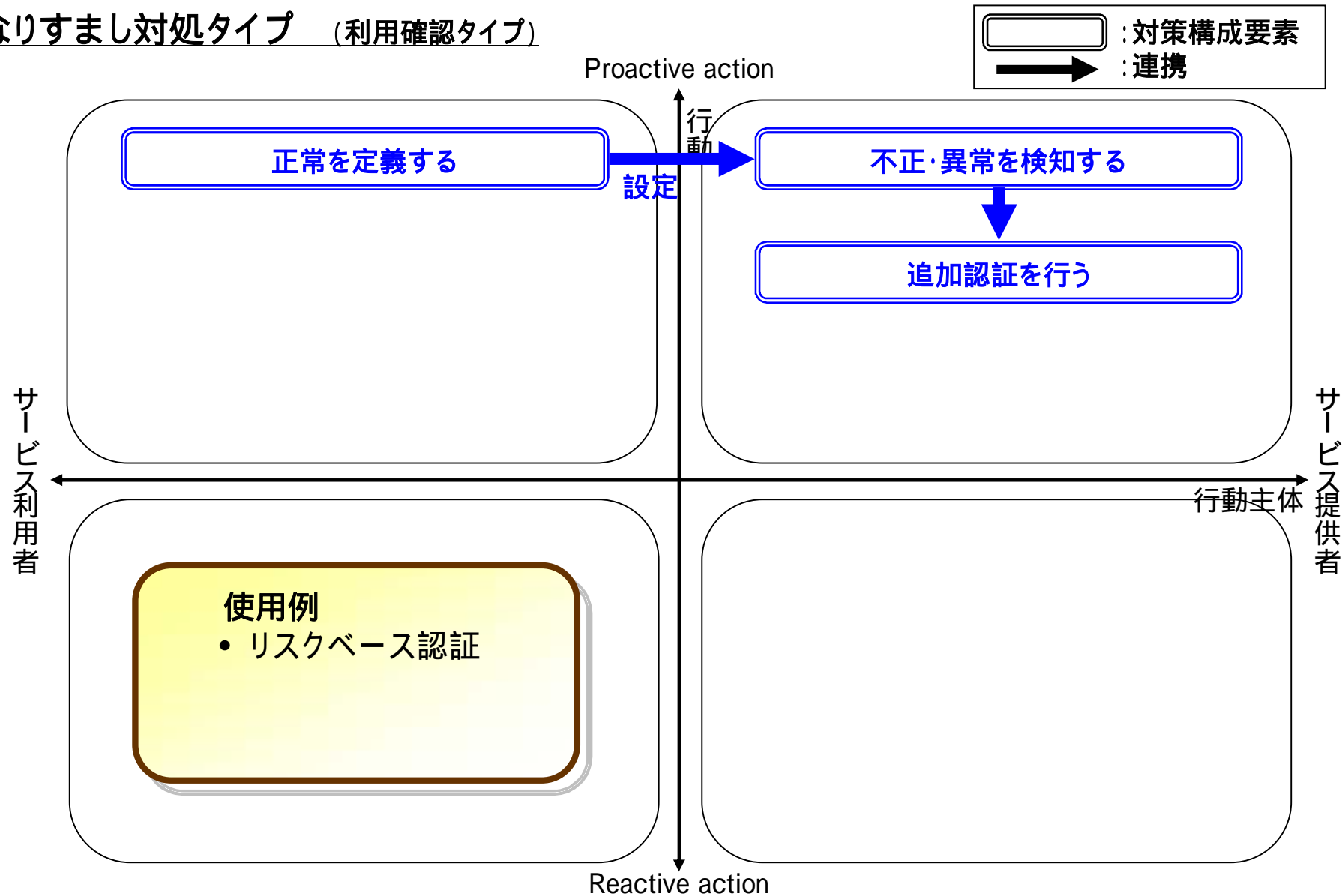
なりすまし対処の分類

なりすまし対処タイプ (完全排除タイプ)



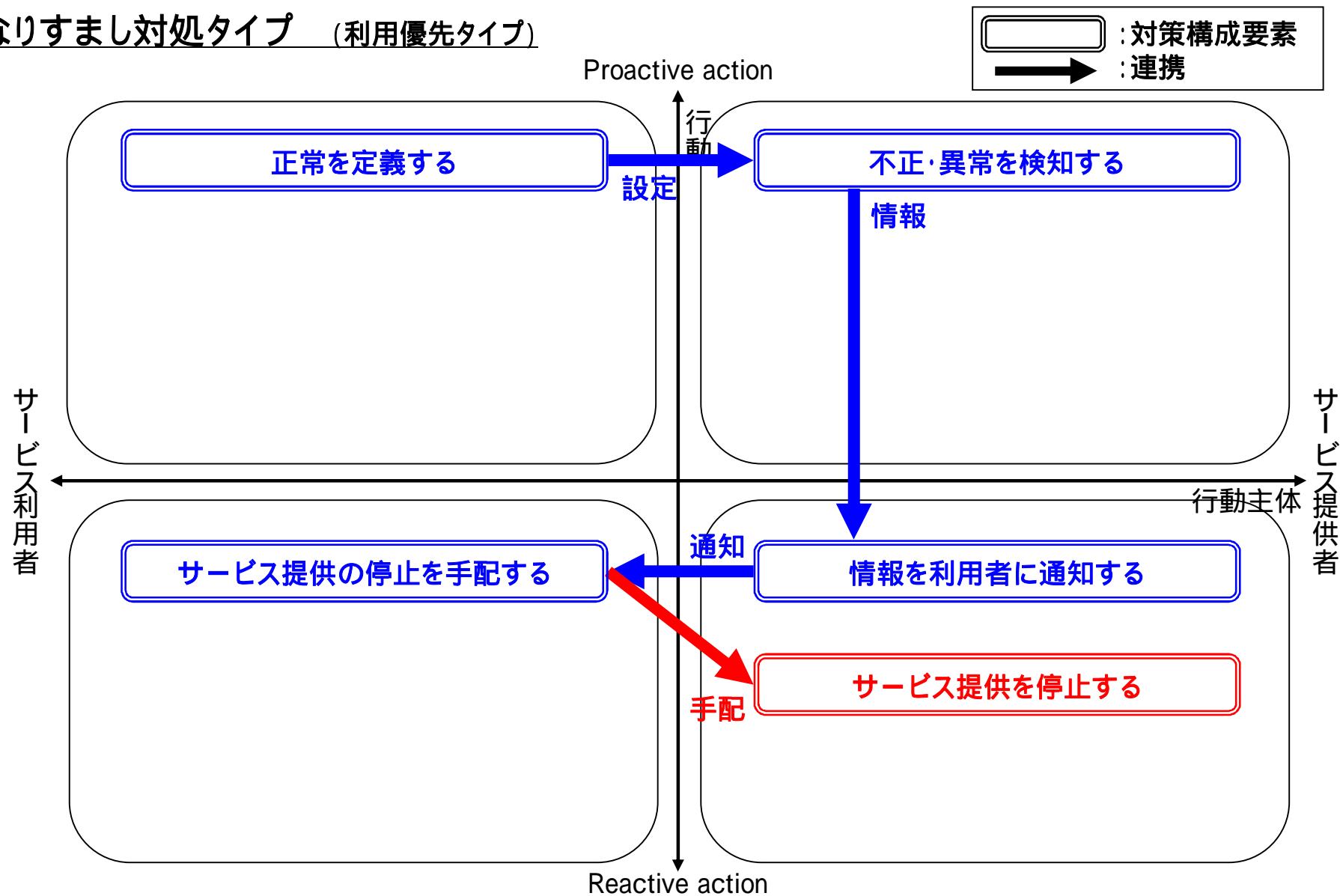
なりすまし対処の分類

なりすまし対処タイプ (利用確認タイプ)



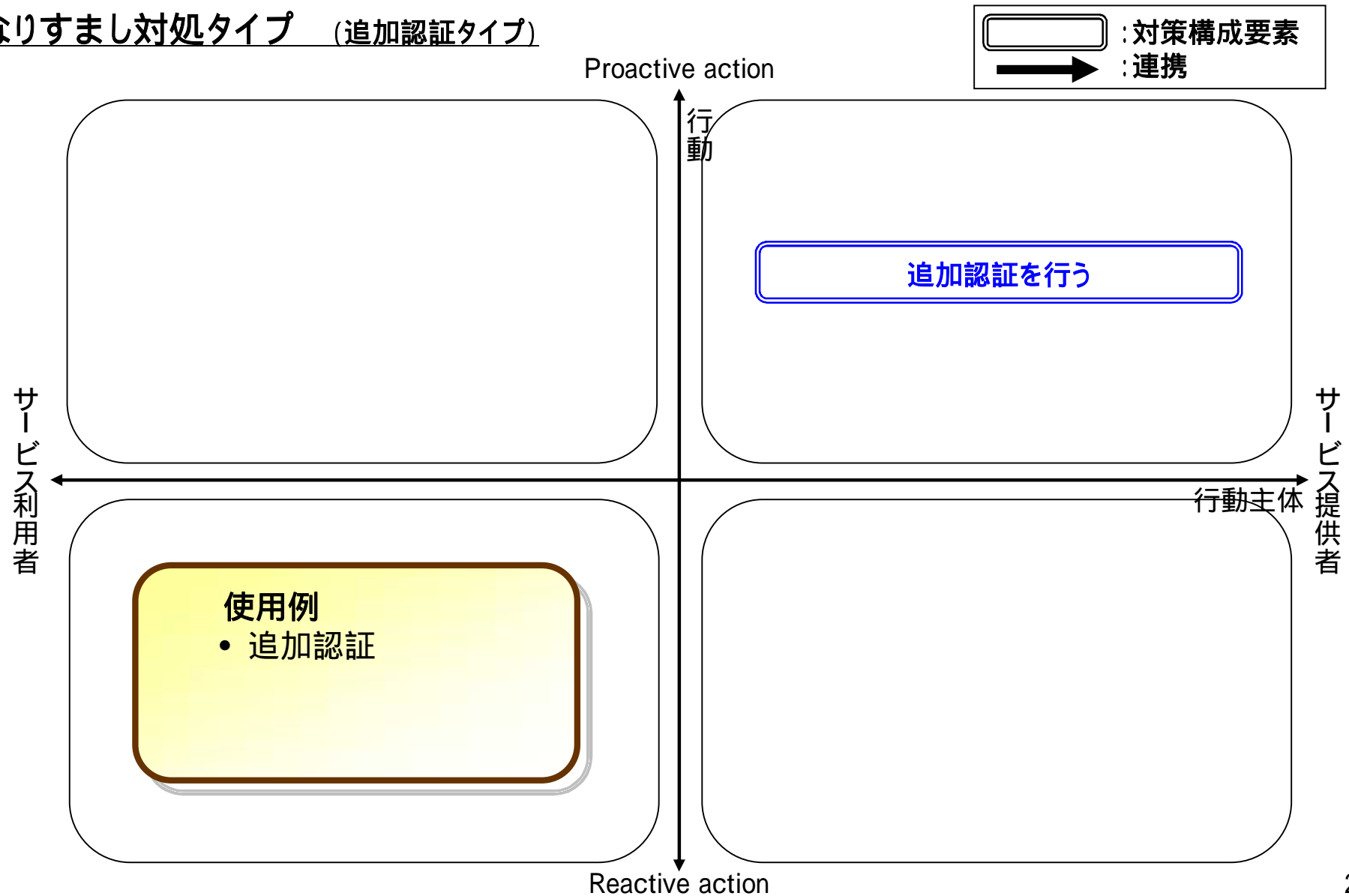
なりすまし対処の分類

なりすまし対処タイプ (利用優先タイプ)



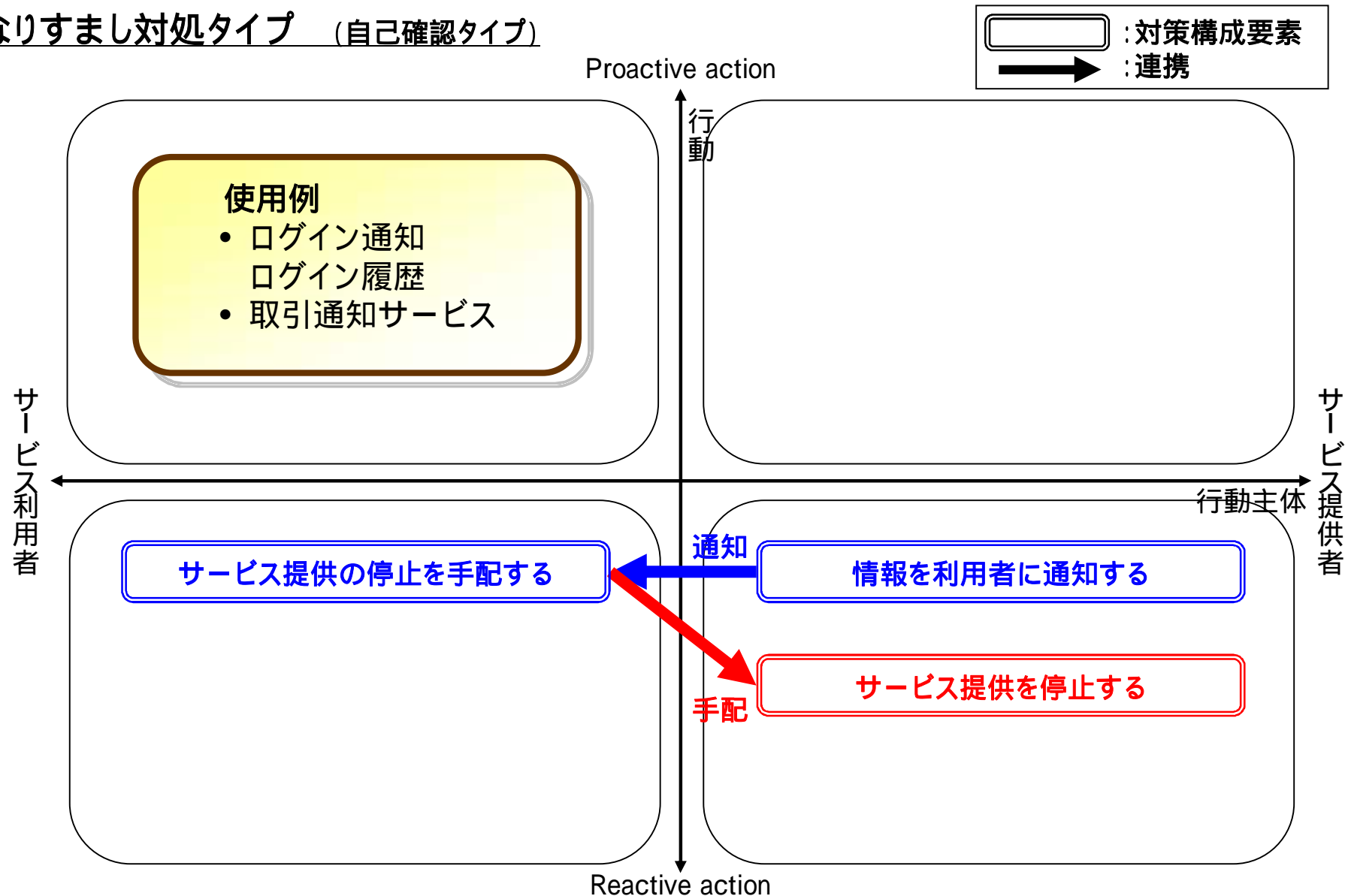
なりすまし対処の分類

なりすまし対処タイプ (追加認証タイプ)



なりすまし対処の分類

なりすまし対処タイプ (自己確認タイプ)



なりすまし対応タイプ一覧

タイプ (完全排除)	<p>正規利用者？ → 利用要求 → 検知有り → サービス → 停止</p>	振込限度額の設定 振込先の制限 リスクベース認証
タイプ (利用確認)	<p>正規利用者？ → 利用要求 → 検知有り → サービス → 追加認証 → 検知有り → 正規利用者 → 停止</p>	リスクベース認証
タイプ (利用優先)	<p>正規利用者？ → 利用要求 → 検知有り → サービス → 検知通知 → 検知有り → 正規利用者 → 停止指示 → サービス提供</p>	
タイプ (追加認証)	<p>正規利用者？ → 利用要求 → 検知無し → サービス → 追加認証 → 検知有り → 正規利用者 → 停止</p>	本人確認の二重化
タイプ (自己検知)	<p>正規利用者？ → 利用要求 → 検知無し → サービス → サービス利用通知 → 検知有り → 正規利用者 → 停止指示 → サービス提供</p>	ログイン通知 ログイン履歴 取引通知サービス

「認証情報の盗難を前提とする」なりすまし対応タイプ

タイプ (完全排除)		振込限度額の設定 振込先の制限 リスクベース認証
タイプ (利用確認)		リスクベース認証
タイプ (利用優先)		
タイプ (追加認証)		本人確認の二重化
タイプ (自己検知)		ログイン通知 ログイン履歴 取引通知サービス

1. なりすまし被害の発生状況とその原因
2. 認証情報の盗難を前提としたなりすまし対策の必要性
3. インターネット・バンキングにおけるなりすまし対策の実施状況
4. 認証情報の盗難を前提としたなりすまし対処の分類
5. **認証情報の盗難を前提としたなりすまし対策の強化案**
6. まとめ

なりすまし対策におけるサービス利用者への選択肢の提供

利用条件を厳しくして
未然になりすましを排除する

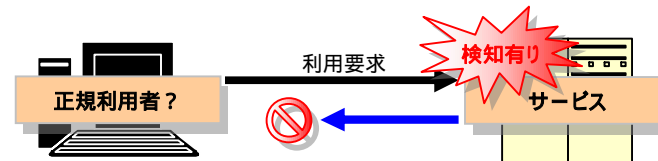
- ・ 使用パソコンの限定
- ・ 振込限度額の設定
- ・ 使用ブラウザの限定
- ・ 振込先の制限
- ・ 使用プロバイダの限定
- ・ Etc.

サービス利用者の
選択肢

システムを当てにせず
なりすましは自分で確認する

(1) なりすまし対処タイプ (完全排除タイプ)

- 利用条件(正常とする条件)を厳しくして未然になりすましを排除する
- 被害を未然に防ぐことができる
- 普段と異なる環境から急に利用したくなくても利用できない場合がある



(2) なりすまし対処タイプ (利用優先タイプ)

- 普段と異なる環境から急に利用したくなくなった場合でも利用できるようにする
- タイプと違って不正や異常があった場合にのみ通知が出されるので、普段は普通に利用することができる。
- なりすましがあって、通知を受けてから停止するまでの間に被害が大きくなる可能性はある

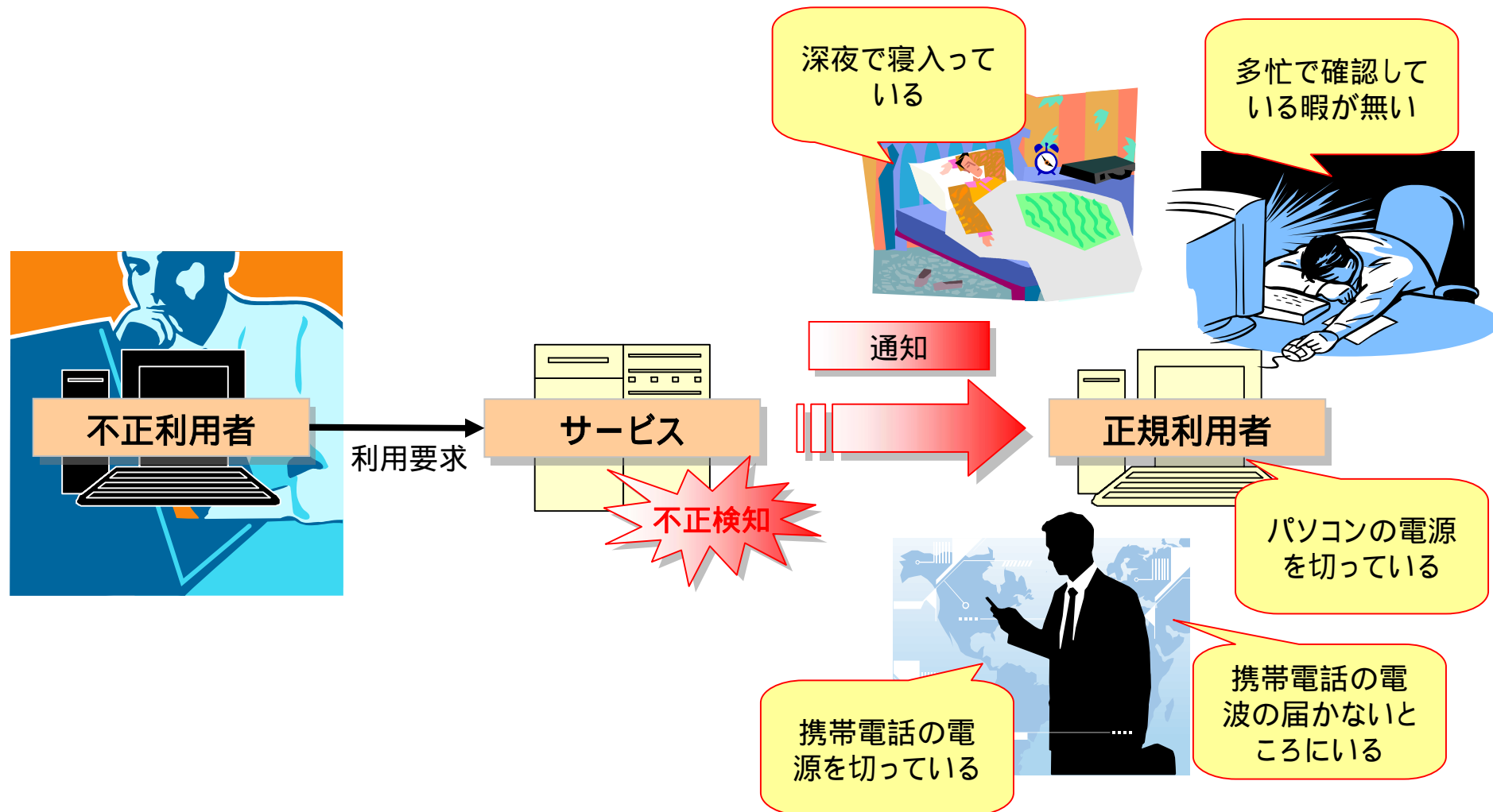


(3) なりすまし対処タイプ (自己確認タイプ)

- 不正・異常検知がどれだけ厳しくなったとしても、正規利用者と不正利用者を100%見分けることはできない。システムを当てにせず、すべて自分で確認する
- なりすましがあって、通知を受けてから停止するまでの間に被害が大きくなる可能性はある
- 不正や異常がなくても通知が出されるので、煩わしくなり確認しなくなる可能性もある。



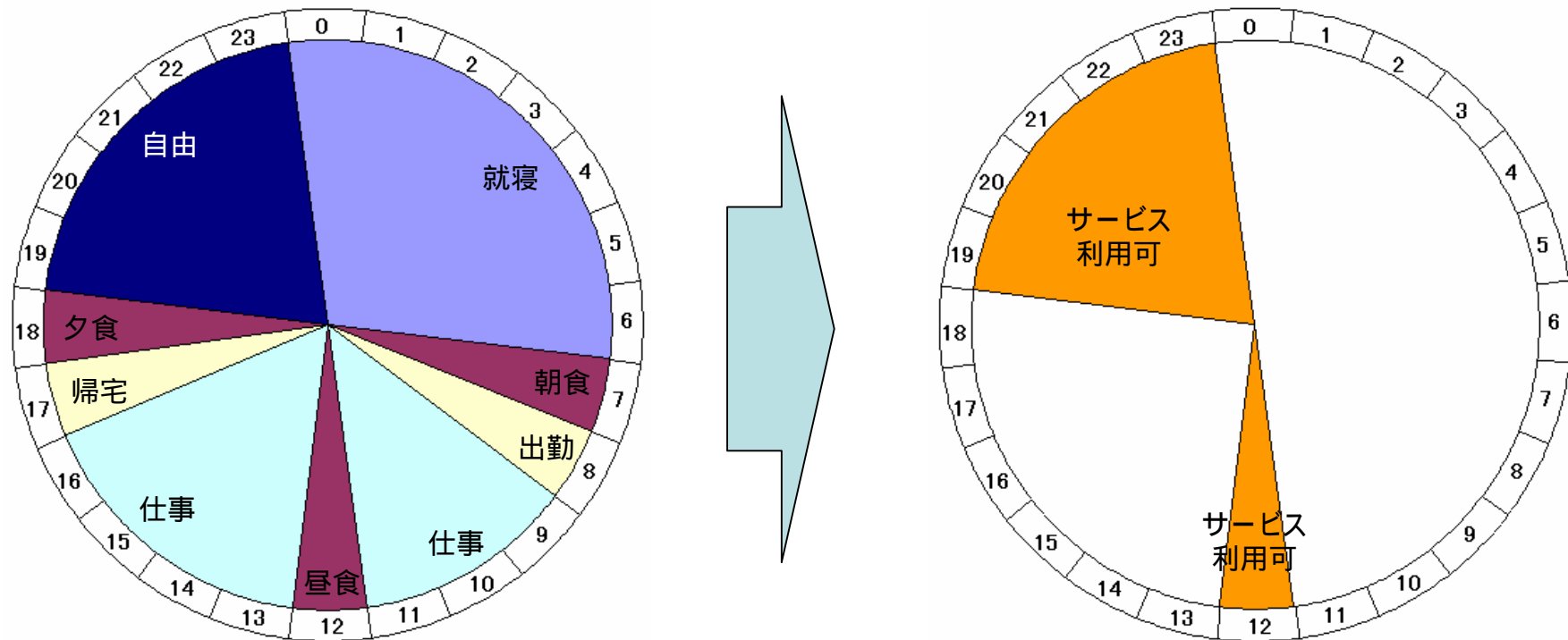
「通知」の欠点



サービス利用者がいつでも通知を受け取れる状態かどうかは分からない

サービス利用時間帯の自主制限

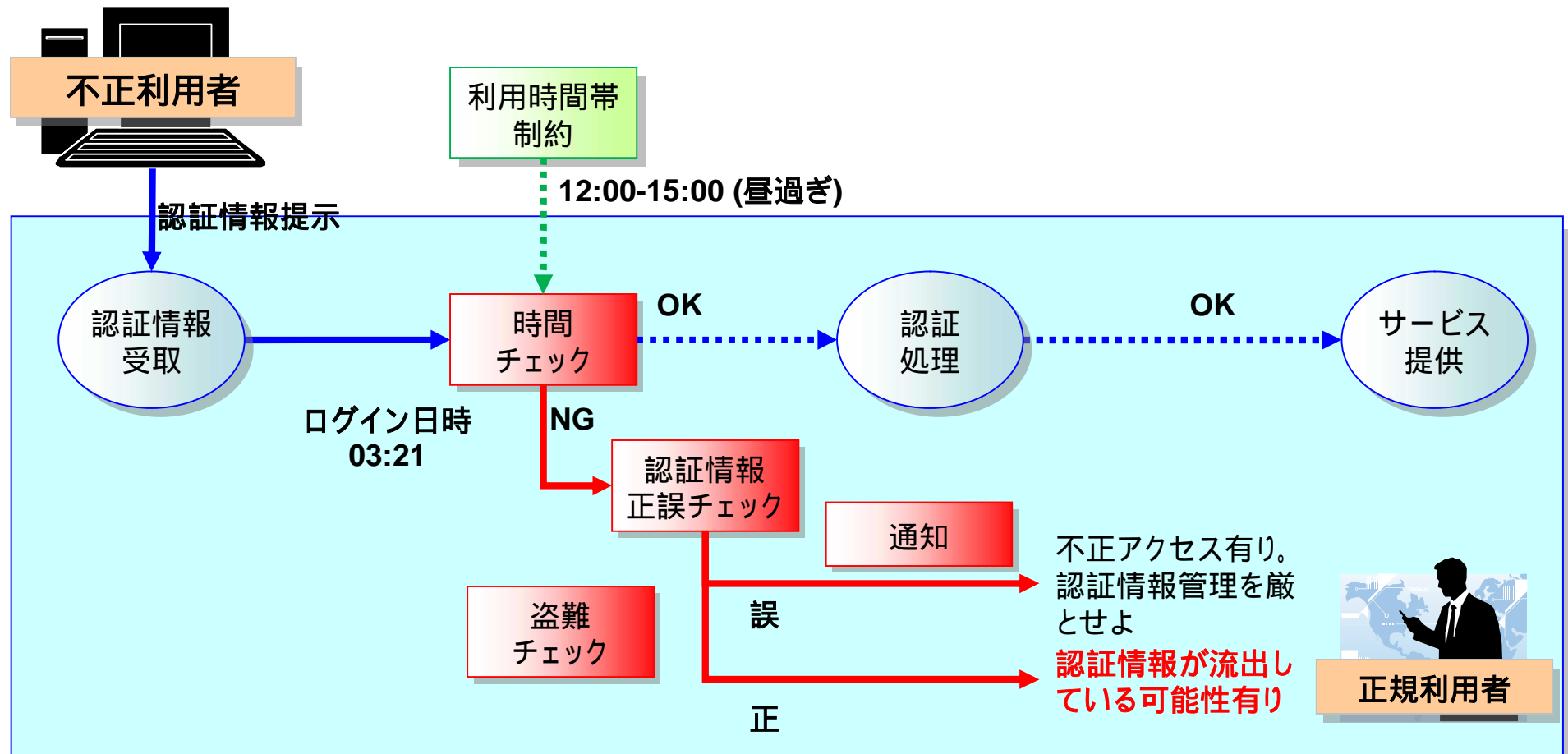
サービスを利用しない / 利用できない時間帯はサービス提供をOFFにする



自主制限項目		選択肢(例)
時間	時刻	06:00-09:00 (朝) / 09:00-12:00 (昼前) / 12:00-15:00 (昼過ぎ) / 15:00-18:00 (夕方) / 18:00-21:00 (夜のはじめ頃) / 21:00-24:00 (夜遅く) / 00:00-03:00 (未明) / 03:00-06:00 (明け方)
	曜日	月曜日、火曜日、水曜日、木曜日、金曜日、土曜日、日曜日
	出勤日/休日	(例) 出勤日: 月曜日-金曜日、休日: 土曜日・日曜日・祝日

認証情報の盗難チェック

サービスの利用条件を利用者自ら狭めることでなりすましを排除する可能性を高めると同時に、提示してきた認証情報がもし正しいものであるならば認証情報が他人に盗取されていると判断することもできる。つまり、認証情報の流出の早期発見が可能となる。



盗難の早期発見による社会全体のなりすまし被害の低減

「盗難チェック」や「なりすまし対処」の結果で、情報流出の早期発見が可能となる。

うちから
情報流出？

通報！



サービス提供者

盗難チェック

サービス

なりすまし対処

通知

正規利用者

不正利用者

利用要求

逮捕！

通報！



警察

1. なりすまし被害の発生状況とその原因
2. 認証情報の盗難を前提としたなりすまし対策の必要性
3. インターネット・バンキングにおけるなりすまし対策の実施状況
4. 認証情報の盗難を前提としたなりすまし対処の分類
5. 認証情報の盗難を前提としたなりすまし対策の強化案
6. まとめ

- (1) 一般消費者向けWebサービスにおいては、認証情報の盗難を前提としたなりすまし対策が必要である。
- (2) なりすましへの対策は、サービス利用者自らが自身のサービス利用スタイルに合わせて選択できるようにしたほうがよい。
- (3) サービス利用時間帯を制限することで、サービス利用者にとって以下の利点が考えられる。
 - 高い確率でなりすまし対処に必要な通知をすぐ受け取ることができるようになる。
 - 利用が制限されている時間帯は確実な安心感を得ることができる。
- (4) 認証情報の流出が早期に発見できるようになれば、個人の被害を低減させるばかりではなく、犯罪の早期発見やサービス提供者からの情報流出の早期発見につながる可能性があり、社会全体のなりすまし被害の低減が期待できるようになる。

ご清聴ありがとうございました。