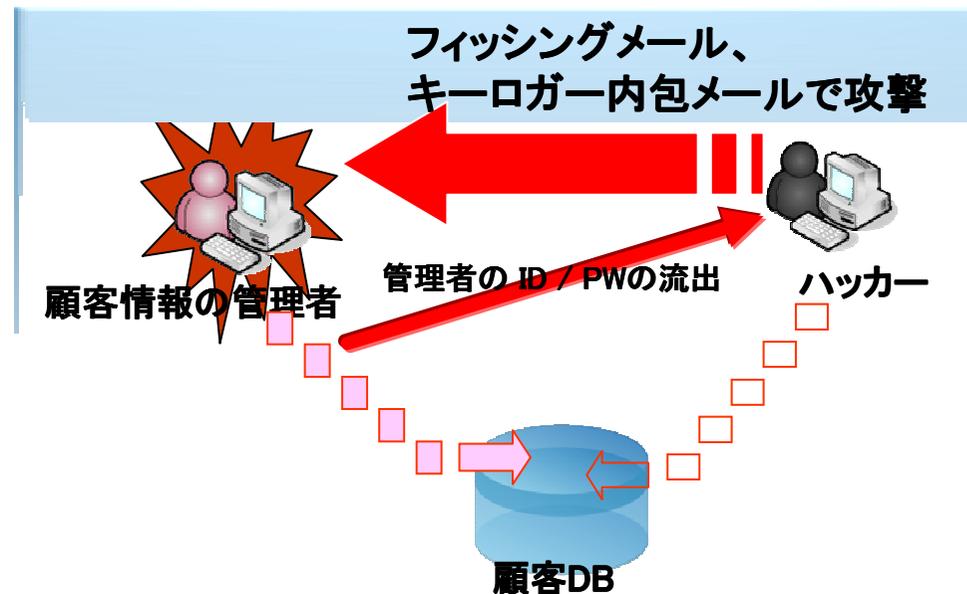


※サイバー脅威の増加と固定パスワードの危険性

インターネットバンキングの攻撃



顧客情報の管理者の攻撃



現在のオンラインの大部分
ログイン方式のID/PWを使用

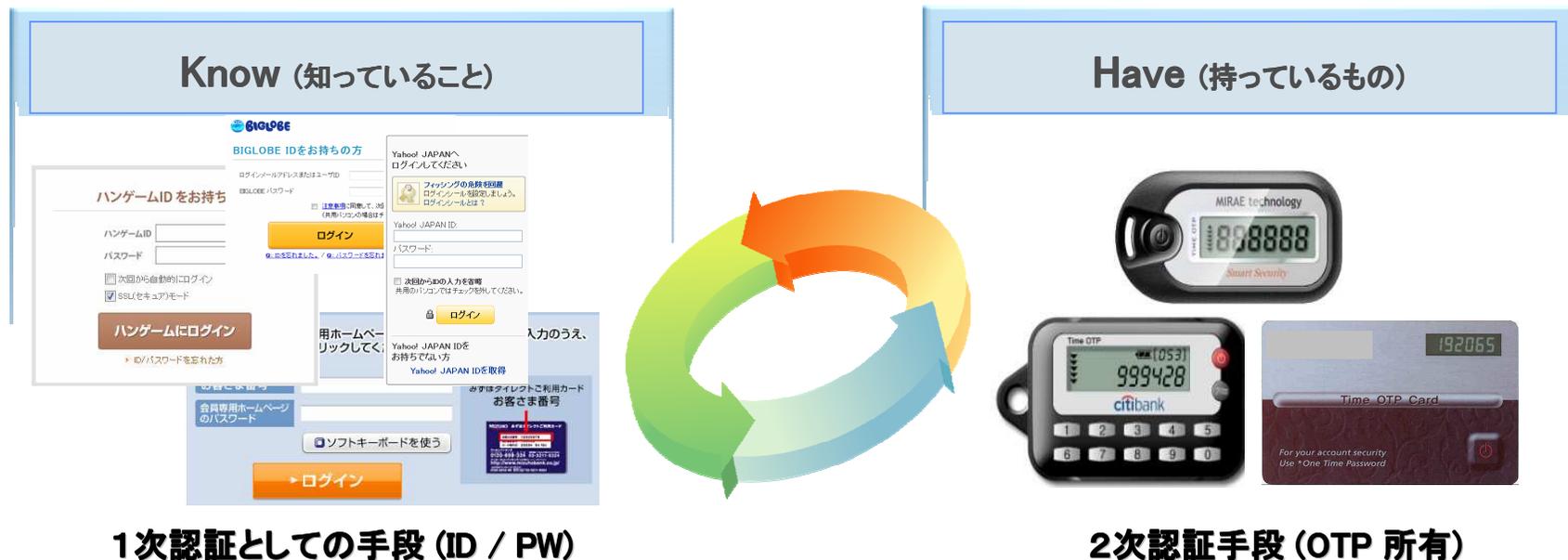


個人情報流出、
犯罪型ハッキングが増加



固定パスワードに代わる
強固なセキュリティを持った本人
認証手段が必要

❖ 2つの認証を利用したセキュリティの強化方案



自分だけが所有しているOTP (One Time Password : 使い捨て暗証番号)を2次認証手段として使うことで、アカウント情報が流出しても完璧なセキュリティを実現。

❖ OTP(One Time Password : 使い捨て暗証番号)

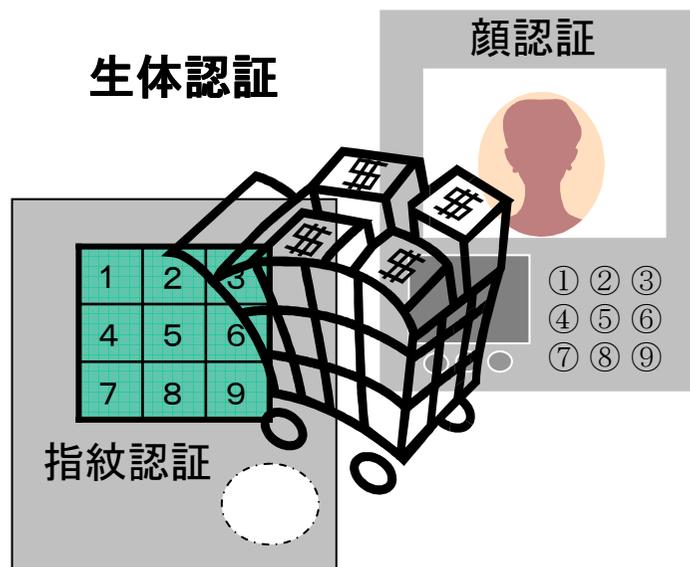
OTPはオンライン上でユーザが本人確認のために使う一度限り有効な暗証番号として、ユーザが本人認証を受ける度に新しい暗証番号を使い、セキュリティ性を高めるものである。また、一度使われたOTP番号は二度と使うことができない。



**OTP番号の有効時間が
決められていて安全性が強い。**

時間同期方式のOTPはOTP番号が決められている時間(15秒、30秒、1分)ごとに変わるので、他の人にOTP番号が流出しても使える時間が短いので安全である。

❖ OTP機器導入のメリット



- ・認証機器が高価
- ・慣れるまで何度か認証失敗することがある。
- ・利用者本人しか認証システムに認証情報を登録できない。



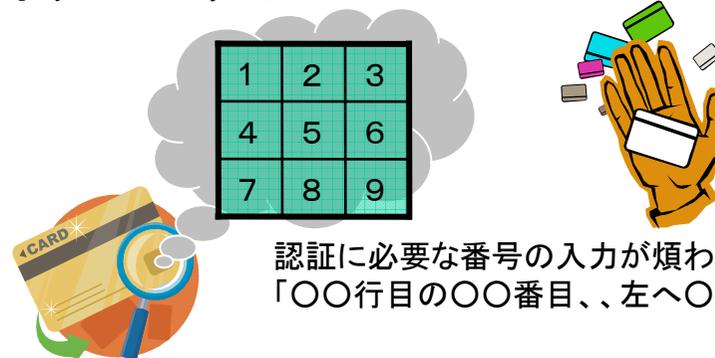
OTP 認証システム



バリエーションが豊富で導入も簡単
機器も安価でセキュリティーも強固



ネットバンクカード



認証に必要な番号の入力が煩わしい。
「〇〇行目の〇〇番目、左へ〇〇桁入力・・・」

❖ OTP認証システム

○キーホルダー型
暗証番号認証式で
セキュリティを高めた
モデル



○キーホルダー型
最小モデル



○カード型
携帯性が抜群



○横長のキーホルダー型
セキュリティを高めたモデル



○スマートカードリーダー機器取り付け型
別途液晶モニターとバッテリーを
取り付けOTPを出力するモデル



○携帯OTP型
携帯をOTP機器として使う



ユーザ

インターネット

