イノベーションの意志

経営者の意思決定のプロセスを助けるために（時間を短くするために)、この文書をご用意しました。

【様々なビジネスモデルに応じる】

スキミング・キャンセラーを利用者に判り易く表現するとしたら…ATM やクレジット端末に併設されたリーダライター（下の写真）です；カードで決済した後など、これを愛用してください、そうしたら「なりすまし」を根絶してくれます…という説明になります。これが基本の姿です。ソフトウエアですから、現実解は様々な姿に変身することが出来ます。国々の事情に合わせることもできます☞ English version

日本では複数の金融機関が ATM に相乗りしているサービスも有るから、表面上は一つの金融機関だけで実施する現実解は無いように見えます；しかし、そんなことはありません。私達は特定金融機関（特定のカード会社）だけでも実施可能な現実解を用意しています。

まず、基本の姿を再確認しましょう；基本形にも複数ありますが、いずれも、カード ID は固定部データと可変部データとで構成されています。

ATM 併設のリーダライター；これでカード ID の可変部を捨てています。この型のキャンセラーは富裕層など特定顧客向けのサービスに使えます。どのレイヤーの銀行にも囲い込み戦略として役立つもの。

携帯電話に非接触型 IC チップを持たせ､携帯電話をリーダライターにしたキャンセラー；これでカード ID の可変部を捨てています；クレジットカード/ATM カードのどちらにもサービスを行えます。

ショッピングセンターや金融街に設置されたリーダライター；特定顧客の ATM カード、ゴールドカード、ブラックカード、などにサービスを行う。金融機関やカード会社の信頼性を訴える宣伝に役立つキャンセラーです。

ネットショッピングで流出した ID データ…このデータの使用停止イベントを起こすのは「生きているパスワード」です；これは既存のパスワードシステムに互換です。☛【基本形の変身】

以上が基本形です。

【基本形の変身】

では、基本形の変身に入ります；これは、ATM 網に複数の金融機関が相乗りしている場合でも、カード端末に複数のカード会社が相乗りしている場合でも、特定の会社だけにサービスを許す現実解です。基本形では、カード ID は固定部と可変部とで構成されていましたが、変身形では、ID の可変部を携帯電話のメモリに置き、カード ID の方は従来の固定部だけになる。このメモリ上の可変部を何らかのイベント駆動で捨てることになります。（下記写真は、イベント駆動の様子をデモしています、製品ではありません）

(a) 可変部のコピーは存在しない様子

(b) ID の二重使用を検出した様子

上の携帯電話(a)が持つメモリ上の可変部を「生きているパスワード」と呼びます。生きているパスワードと既存のパスワード（暗証番号）とが「互換なシステム」ならば、それは、相乗りしている ATM でも、金融機関が単独で導入できる現実解です。

【パスワードのシステム互換】

まず、既存の決済端末は；カード ID と暗証番号（生体情報）を運用する端末です。ここの ID はカード ID と暗証番号（生体情報）で構成されています。

カード ID と暗証番号（生体情報）で ID が構成されている。

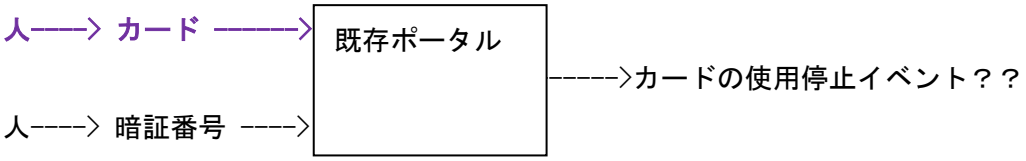

図 1；既存の決済端末

既存の決済端末にはセキュリテイが欠如しています；すなわち、スキミングされた ID、流出した ID に対して、カードの使用停止イベントは起きない、なりすましを許す、訳有り端末です。

他方、生きてるパスワードでは、ユーザが携帯上のスキミング・キャンセラーを運用していて、それゆえ、流出 ID にはカードの使用停止イベントが起きます。ここで ID はカード ID と生きているパスワードで構成されています。

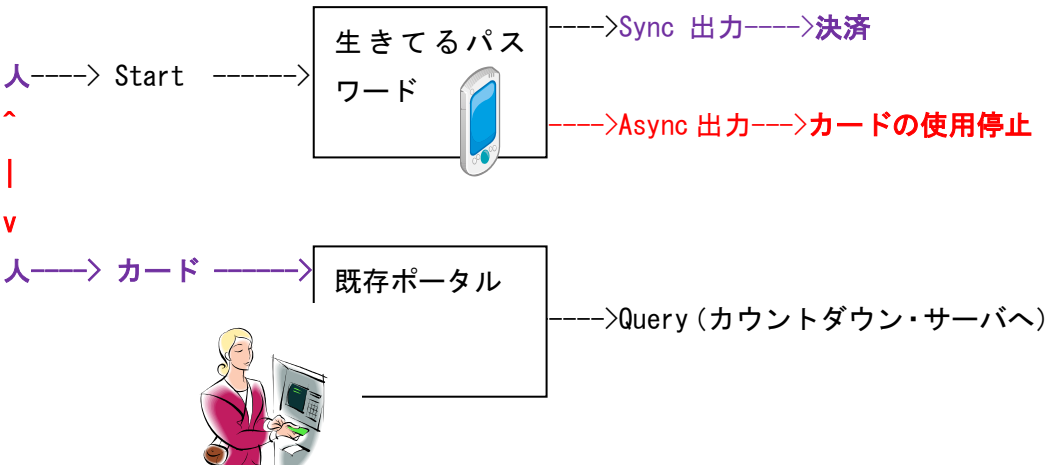

図２；パスワードのシステム互換

図 1 と図２は同じくカードイベントを共有にしていますが、図 1 では、スキミング ID にも決済を許可してしまいます。図２では、スキミング ID にはカードの使用停止イベントが起きます。

【セキュリティ・プロトコル】

図２のプロトコルは一つではない；たとえば、生きているパスワードの「Start」が

先か、あるいは、カードイベントが先か、それによって、各々通信プロトコルに違いが出る。が、基本は一つ；①生きているパスワードを「Start」させる人と、カードイベントを起こす人、が同一人の時に限り、そして、②クロックが Sync する時に限り、③サービスサイト又は端末は ID の認証イベントを受け取る。②の Sync 状態は 10 秒以内だけ維持される。クロック ☛変化し続ける途上の ID。☛ATM 疑似デモ有り。

【カードの使用停止イベント】

図２、カードの使用停止イベントは、次の事件に対応して、１００%起きます；

１．生きているパスワードが流出した時；

２．カードイベントが起きてから、10 秒以内に、生きているパスワードが走らない時；
これは、恐らく、偽造カードか紛失カードが使われた時でしょう。☛トップページの犯罪者の追跡

なお、操作のやり直しが許される場合、

３．生きているパスワードが走ってから、10 秒以内にカードイベントが起きない時；

【セキュリテイの圧倒的な優位性】

生きているパスワードは、少なくもカード入力の度に Sync か Async かの二者択一を出力します；通常は Sync 状態ですが（☛トップページの予防）、Sync から Async に移行する場合があります；☛トップページの責任分解点。この時は、犯罪者の「追跡」を行える経路情報が即刻に提供されます。☛有料セミナー。☛トップページの犯罪者の追跡

他方、Async から Sync には移行できません。但し、Async から Sync に移行する確率は存在します、それがトップページに記載した $1/2^{256}$ です；☛変化し続ける途上の ID。

【振り込め詐欺、マネーローダリング防止のセキュリティ】

以上の他に、生きているパスワードの特筆すべき効果は送金業務にも現れます。送金業務は振り込み人と受取人が起こすイベントのはずです。しかし、*現在の ATM の作業は受取人の確証を得ないまま実施しています*。ここが詐欺の付け入る隙になっています。受取人の携帯にも生きてるパスワードを提供しましょう（登録には銀行がコミットする）、そしたら*振り込め詐欺を困難にします*。☛日刊工業新聞，2009 年 7 月 23 日、7 月 30 日、「人と携帯電話とパスワード」

【銀行経由の清算業務】

上のセキュリテイを企業間や個人間の清算業務に拡張することも出来ます。携帯電話の利便性を活かしながら、銀行と、振り込み人と、受取人と、の三者が送金イベントの確証を共有します、いつでも、どこでも、即刻。☛日刊工業新聞，2009 年 7 月 23 日、7 月 30 日、「人と携帯電話とパスワード」

【表面上の利便性】

パスワードのシステム互換に付随するセキュリテイは上述のごとくです。目に見える利便性は「パスワード入力から解放されるユーザ」の姿です。「Start」ボタンを押す、カードを挿入する、これだけの動作です。

【紛失事故】

自分のことは自分で守れる、そういうセキュリテイを人に提供する、それが生きてるパスワードの特徴です；カードの紛失を防止するセキュリテイでは無く、また携帯電話の紛失を防止するセキュリテイでも無い。☛【セキュリテイの圧倒的な優位性】。が、カードや携帯電話の紛失事故に、届出をしてもらうことが結局、ユーザを守ることになります。☛トップページの責任分解点。☛有料セミナー。ただ、紛失に気付かない場合の気付くまでのセキュリテイも欲しい、ということであるならば、指紋認証付きの携帯電話を利用するのも一つの方法です。

【適用範囲】

パスワードのシステム互換は、金融に限らず適用範囲が広く浸透力が強い。たとえば、既存の EC サイト、既存の企業内情報基盤、等への適用も即可能です。（メーカか SIer の出番）

【顧客囲い込み】

数社相乗りの ATM や決済端末ではなく、自社の ATM だけでサービスを提供するモデル、高額資産家などに向けた顧客囲い込みにも役立ちそうです。特定 ATM にキャンセラーを実装するも良し、ATM 併設型のキャンセラーも良し。こうしたサービスは信金・地銀様の戦略にも貢献するかと思われます。

【SOX 法、JSOX 法への対応】

JSOX 法は、パスワードのリスクをパスワードのせいにすることを許さない、しっかり管理せよ、と命じています。管理を厳密に行うガイドラインには、たとえば、ISO27000 が有ります。これには人件費がかさむ！株式会社アマダは、スキミング・キャンセラーをイントラの PC に導入してパスワード入力を社員にさせない仕組みを工夫しました。この利便性ゆえに拡張が容易。現在、IT サービスカーにも展開中。☛アマダ導入事例

【交渉テーブル】

上述のように、新技術はセキュリテイと利便性を両立しつつ、社会経済基盤の様々な場所に適応する力を持っています、あるいは潜在ニーズを顕在化する力を持っています。

どの分野の、どのセキュリテイと利便性に関するライセンスが欲しいか、意思を表明なさるアーリーアダプターには、その部分の先行利益（先着順？）を含む契約に入ることになります。交渉テーブルと ATM 疑似デモ（パスワードのシステム互換）を用意しています。お申し込みは直接、筆者宛て（渡辺栄治）に行えます；

☛ eiji@meteora.co.jp　cc;oi-eiji@tempo.ocn.ne.jp

【有料セミナー】

新技術（認証 I/F）を一早く知りたい方、アマダ事例の導入を検討したい方、認証 I/F のアプリケーションを自ら考えたい方、認証 I/F のアプリケーションを市場へ提案したい方、自社の強みをアッピールしたい方、などセミナー（メニュ、キャンセラーとは何か？を参照のこと）をお薦めします；

☛Start small. But, start now!

記述、渡辺栄治　(METEORA)、
2009 年 12 月 8 日