

変化し続ける途上の ID (Identity on the way to its body changes)

【Key words】

変化し続ける途上の ID、ID のオリジナルとコピーの互換性、ID 情報の使用权、シンクロナイズド・クロック、METEORA

【初めに】

スキミング・キャンセラーの「キャンセル」の意味は、少なくとも取引時の ID を破棄することです。●[キャンセルとは何か？](#) そのキャンセルの信頼性を担保している技術があります、それが「シンクロナイズド・クロック」です（以降、単に、クロックと言う）。

【シンクロナイズド・クロック】

クロックは、二個のサイコロと、サイコロを振る二人と、サイコロを観測している第三者と、この三つの実体が行うゲームの一部始終です。この文書は、第三者を省いて、サイコロが起こすイベントに限定して解説します。



クロックは三つの実体が創るゲームのことです。



サイコロを振ったら、目が一致したとします。これを「シンクロナイズ(Sync)」と言います；イベント①と参照する。この時に限り、少なくとも取引時の ID を捨てる。



サイコロを振ったら、目が一致しなかった時、これを「ア・シンクロナイズ(Async)」と言います；イベント②と参照する。

一度でもイベント②が起きると、サイコロを振ってもイベント①に復帰しない；これをイベント③と参照する。

サイコロを振る、この行為が何を意味するか別の機会に譲ります。ここではサイコロが

変化し続ける途上の ID (Identity on the way to its body changes)

起こすイベントについてののみ紹介しています。実際のサイコロは、その面が 2^{256} もあります。この数は宇宙に存在する素粒子の数に相当するかも知れないほどの数です。二度と「ア・シンクロナイズ」から「シンクロナイズ」には復帰しないという根拠は、サイコロの面が 2^{256} 面もあり、その二つのサイコロの面が一致する事象には出会えないこと、正確に言うと、一致する事象は無視できる確率 $1/2^{256}$ になる、ということ。クロックは①②③の確率事象の信頼性をギャランティする仕組みです。●【監視スクリーン】

【キャンセルとクロック】

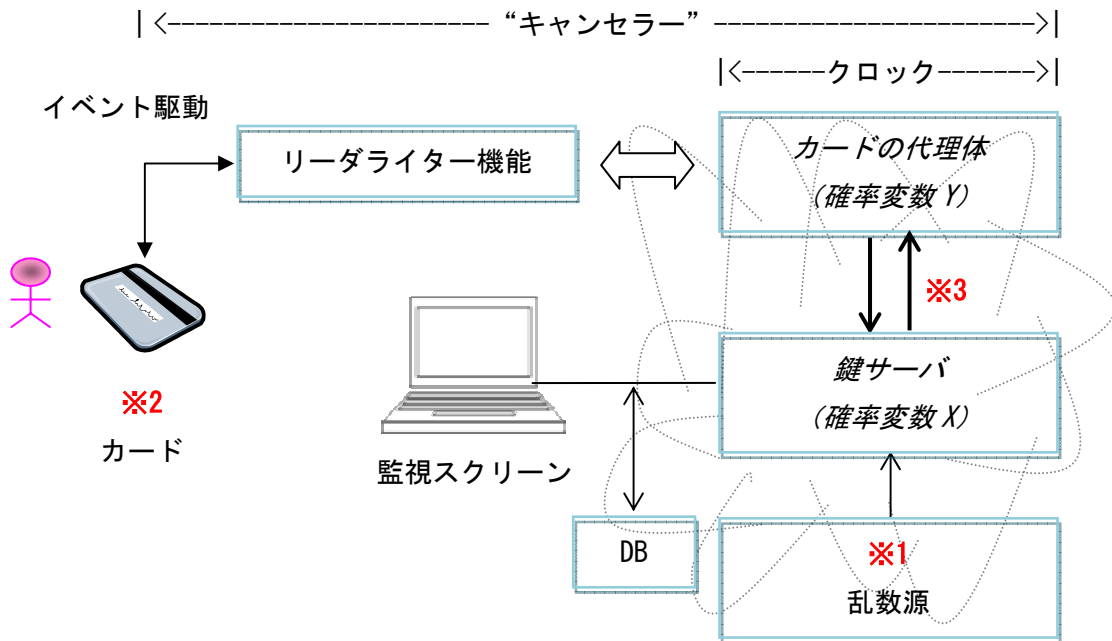


図1；クロックの構成要素

図1において、

※1は乱数源です；確率事象です。

※2はモバイル記憶（カード）です；これも確率事象です。

※3は独自プロトコルのクロックとHTTPのクロックと在る。

クロックは、偽造カードなど IDの二重使用を検出し、その時刻・経路を特定し、犯人像を訴求すること、をギャランティするシステムです。ですから、カードも確率事象として扱う仕組みです。図1の事象を体験できます。●[有料セミナー](#)

【クロックのトポロジー】

クロックは従来に無い効果を論理的に導きます；第三者信頼機関を必要としないことと、IDの二重使用を検出する信頼性です。クロックは既存のシステムと並列（独立）に

変化し続ける途上の ID (Identity on the way to its body changes)

稼働します (図 2)。ID は固定部と可変部で構成されています。

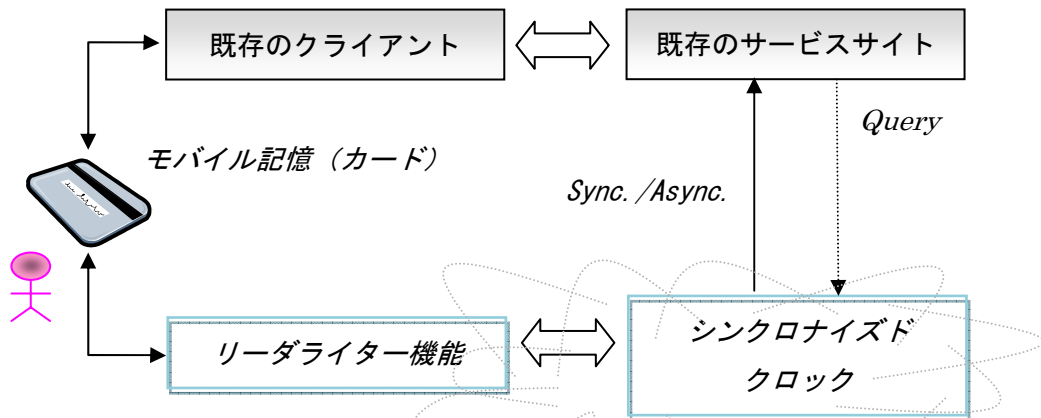


図 2 ; クロックの使い方、一例

図 2 の配置とは異なり、カードの代理体 (図 1) を既存ネットへ実装した事例もあります。例えば、既存の PC にリーダーライターを付加して構成したクロックが、アマダの事例です ; 社員にシングル・サインオンを提供し、その際、パスワード入力を要求しません。☛[アマダ導入事例](#) ですから、人に負担をかけず、企業にも負担を掛けないことは明らかです。導入作業は 1 カ月も有れば十分。なお、モバイル記憶+リーダーライター+通信部は携帯電話 1 個で実現する、そのような実装例もあります。

【監視スクリーン】

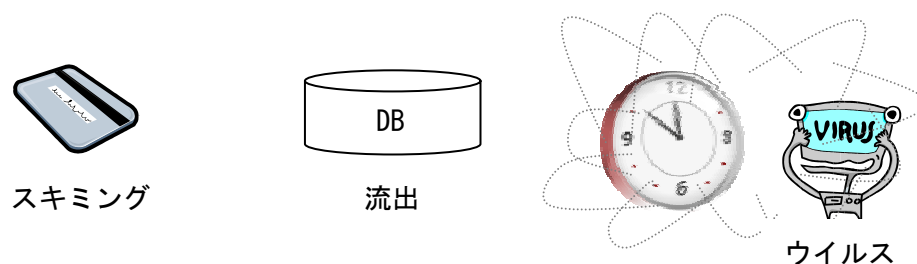
Event Event time	Alternative		address	Logging time
	Sync log	Async log		
14		b8efdc7	192.168.201.60	2009/11/27 14:13:24
13		b8efdc7	192.168.201.60	2009/11/27 14:10:58
12		b8efdc7	192.168.201.60	2009/11/27 14:10:23
11		464812a	192.168.201.70	2009/11/27 14:09:49
10		464812a	192.168.201.70	2009/11/27 14:09:34
9	66eccc9		192.168.201.60	2009/11/27 14:08:00
8	464812a		192.168.201.60	2009/11/27 14:07:48
7	b1c1c74		192.168.201.60	2009/11/27 13:54:46
6	30f2e75		192.168.201.60	2009/11/27 13:53:58
5	9889b47		192.168.201.60	2009/11/27 13:51:07
4	423fcb4		192.168.201.60	2009/11/27 13:50:50
3	71d2037		192.168.201.60	2009/11/27 13:50:17
2	5fc605a		192.168.201.60	2009/11/27 13:48:59
1	3997552		192.168.201.60	2009/11/27 12:03:52

クロックの監視スクリーンを示します。「シンクロナイズ」と「ア・シンクロナイズ」

は二者択一です。「シンクロナイズ」の証拠を [Sync ログ](#) と言う ; 「ア・シンクロナイズ」の証拠を [Async ログ](#) とする。監視スクリーンに見る通り、Sync ログと Async ログは二者択一です。同じ行に IP アドレス、ログ時刻が表示されています。これが ID の二重使用の検出事例です。 [有料セミナー](#)

【クロックの必要性】

モバイル記憶には スキミングの脅威 が有り、DB には 情報流出の脅威 が有り、代理体と鍵サーバには ウイルスによる情報流出の脅威 が有ります。従来の暗号系は鍵が流出した時には為す術がないことをご存知の通りです。



一方、クロックの代理体と鍵サーバは、ID が流出し、それが使われた時にはア・シンクロナイズします。で、ID の流出がどこで起きようと (カード、DB、クロックに仕掛けられたウイルスで有ろうと)、クロックは ID の二重使用の検出を ギャランティ します。

【参考】

サイコロゲームを観測している第三者

二人のサイコロを観察している第三者、この三つの実体が創るゲームについて、一言触れず。私達の記憶は薄れて行くのが正常です。しかし、記憶が消えないという悩みを抱えている方も居ます。 [超記憶症候群](#)。どちらにしろ、記憶を通して私は私という「ID 意識」が立ち現われて来ます。実は、サイコロゲームを観測している第三者を入れるとこの「ID 意識」を議論する情報理論に成ります。 *生命感と情報理論の世界初の出会い*。

記憶が消えないという悩みは巨大なログを意識下に抱えている悩みですが、「ID 意識」にはそのようなログが要りません。スキミング・キャンセラーを導入するに当たって、繰り返し繰り返し ID の可変部を捨てる、捨てる、と説明して来ました。しかし、サイコロを観測している 第三者はゲームが情報エントロピーを不変に維持していることを証明します ; 時間に対して不変になっていますから、このゲームはクロックになるしか無いのです。

私たちの体の細胞は毎日毎日、絶え間なく捨てられています。 [生物と無生物のあいだ](#)。まるで、雪だるまが太陽に照らされて溶けて行くかのように見えます、にも関わらず、私は私という ID 意識が立ち現われて来ます。 *ID 意識にとってはログは不要*なのです。私たちの体細胞も「情報エントロピーを不変に維持している」という考えに対応します。

スキミング・キャンセラーを通して、人は ID の可変部を捨てて「なりすまし」の侵入を拒否できるように成りました。同じく、私たちの体細胞も、毎日毎日、絶えず捨てられて行き、実は、二重人格（ジキルハイド状態）を拒否していると考えられます。

ID 意識の正体はクロック！今のところ、これは仮説です。チョコレートという言葉聞いて、何か思い出します；事件、味わい、感情、クオリアの違い、など。思い出す、これは「情報エントロピーを不変に維持している何か」に、チョコレートという記号が投入された結果です。コンピュータがやってるような、データの照合・一致の結果では無い！！

私達は時間を意識する能力、あるいは見る能力がありません、空間感覚を通して時を見ることは出来ています；もう一つは、記憶を通して時間が立ち現われる；このように時を意識しています。それを邪魔しているのが超記憶症候群、超記憶と ID 意識を両立させることは苦痛でしょう。正常な頭脳は「時間の中で情報エントロピーを不変に維持できる」から、記憶が甦る、そのような記憶の情報理論が成り立ちます。ID 意識が立ち上がるメカニズムと時間はどちらかがどちらかの原因になっている可能性があります。

クロックの構成要素、(確率変数 Y) と (確率変数 X) のペア、これが筆者には DNA の二重らせんに見えます。遺伝子は、決して固定データではなく確率事象とした扱われるものです、仮説ですが。

クローンを大量に生産している物理学があります、並行宇宙論です。量子論の素直な帰結には違いないのですが、何か欠落しているのです。その何か？とは「時間の中で情報エントロピーを不変に維持できる生命体」の欠落です。サイコロゲームを観測している第三者が欠落しているのです。物理学がサイコロだけを見ているから、並行宇宙論になるのです、第三者を入れないから、クローンを大量生産する物理学になるのです；仮説として提供していますが、やはりアインシュタインの方が正しい。

いずれにしろ、いつか、どこかに、情報エントロピーを不変に維持している生命体と DNA の働き、あるいは、ID 意識とクロック、または、暗号に騙された並行宇宙論などの議論を置きます。

●超記憶症候群●「忘れられない脳」ランダムハウス講談社刊

●生物と無生物のあいだ●講談社刊

【参考】

疑似 ATM デモ

経営者の意思決定のプロセスを助けるために疑似 ATM デモを用意しました。ID 情報の流出に警報を発したり、ID の流出（リスク）を無効にしたりするデモと、パスワードのシステム互換のデモを用意しています。経営者、起業家の方からお申し込みを頂いた時に限り実施しています。お申し込みは直接、筆者（渡辺）宛てに行えます。実施場所は神奈川県伊勢原市石田 200 番地アマダ敷地内が原則です。●【パスワードのシステム互換】

変化し続ける途上の ID (Identity on the way to its body changes)

宛て先 ; eiiji@meteora.co.jp cc:oi-eiiji@tempo.ocn.ne.jp (渡辺)

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、自社の強みをアピールしたい方、などセミナー（メニュー、キャンセラーとは何か？を参照のこと）をお薦めします；

記述、渡辺栄治 (METEORA)

2009 年 11 月 29 日