SCIS 2002 The 2002 Symposium on Cryptography and Information Security
Shirahama,Japan, Jan.29-Feb.1,2002
The Institute of Electronics,
Information and Communication Engineers

電子セキュリティトークンのモデル化と応用
Modeling Digital Security Token and Its Application

松浦幹太*
Kanta Matsuura

あらまし 情報セキュリティ技術のおかげで，様々な電子トークンが取引可能となる．それらのトークンには，例えば購入時に検証に合格した電子証明書が使用時にも合格するとは限らないなどの理由により，価格変動以外にも予測不能な価値変動リスクが伴う．このようなリスクに対処する方策として，派生物の導入によるリスクヘッジが考えられる．残念ながら，完全に電子化されたネットワークの世界では，古典的な理論のモデルや仮定がすべて利用できるとは限らない．本論文は，ネットワーク社会に即したリスク管理理論の基礎を提示し，その工学的応用の可能性を示すことを目的とする．

キーワード 電子取引, 電子証明書, 電子トークン, 派生物, 価値変動リスク, リスク管理.

1 はじめに

情報セキュリティ技術のおかげで，ネットワークを介して様々な電子トークン (以下では単に「トークン」と表記) が取引可能となる．ただし信頼できるディレクトリに実時間アクセスできるとは限らないため，価格変動以外にも不確定性リスクが伴う．例えば公開鍵基盤に基づく一連の電子証明書 (以下では単に「証明書」と表記) によって機能が保証されるトークンを考えよう．購入者は購入時にすべての証明書を検証し，無効化済み証明書リスト (CRL: Certificate Revocation List) もチェックして，問題がなかったとする．しかしそれでも，実際にそのトークンを利用する時に検証者が行う同様の作業にすべて合格するとは限らない．理由は，いくつか考えられる．まず，購入から利用までの間に一連の証明書のいくつかが有効期限以外の予期せぬ理由で無効になっている可能性がある．また，無効化チェックの精度を上げるため検証にオンラインサーバが必要な実装ならば，サーバが混雑やサービス妨害攻撃で閉塞している可能性もある．あるいはまた，一連の証明書から何らかの信頼度 (trust metric)[1]–[6] が算出できるように定義されているシステムならば，トークンを利用しようとした時にその信頼度がかなり低下しており，もはや利用不可と判定されるかもしれない．この種の変化は予測不能であり，リスクが生じる．しかも，利用実績に応じたポイント制度や各種の事前登録会員割引などの複雑なサービスをそれぞれディジタル署名で実現すれば，その都度付随する証明書に起因するリスクが生じ得る．

このような不確定性に起因するリスクに対処する方策として，派生物の導入によるリスクヘッジがある．従来の金融の世界では，Black-Scholes のオプション価格評価方程式 [7] などに触発され，派生物理論と応用が発展した．しかし残念ながら，完全に電子化されたネットワークの世界では，古典的な理論のモデルや仮定がすべて利用できるとは限らない．本論文は，ネットワーク社会に即したリスク管理理論の基礎を提示し，その工学的応用の可能性を示すことを目的とする．この目的を達成するため，まず 2章でトークンをモデル化する．続いて，その基本的な派生物を 3章で定義し，価格評価方程式を導く．4章では，さらに単純化された場合の数値評価と，リスク計測への工学的応用について考察する．

2 モデル化

2.1 概略

トークンに付随する価格以外の重要な数値を一般に価値 (value) と呼ぶことにし，背景価値 (implicit value) と呼ばれる確率過程に支配されているとする．トークンには，発行時の背景価値の実現値 (occurrence) に依存した額面価値 (explicit value) が書き込まれる．1 つのトークンが複数種類の価値をもつこともあり得る．不特定多数の購買者を扱い，しかも匿名性のある電子支払い手段を容認するので，現存の金融機関と顧客の関係のように口座制 (accountability) を仮定することはできない．よって任意に細かい額をやり取りすることは原則として無理

* 東京大学生産技術研究所・大学院情報学環．〒 153-8505 目黒区駒場 4-6-1. Institute of Industrial Science, Interfaculty Initiative for Information Studies, University of Tokyo, Komaba 4-6-1, Meguro-ku, Tokyo 153-8505, JAPAN

であり，トークン単位（１個，２個，･･･）の制約を受けるのが自然である．そのような制約を表現するためのモデル化が必要であろう．適切な管理（例えば著作権管理や鍵管理，証明書管理）がなされているため，トークンは一般には複製自由ではない．いったん供給されたら，その後の流通は，無秩序な複製ではなく何らかの取引として実現される．その取引は，額面価格だけでなく額面価値や背景価値にも依存し得る．

2.2 セキュリティトークン

不確定性リスクのあるトークンを以下のようにセキュリティ・トークン（セトック）としてモデル化する．

定義 2.1 (セトック)
セトック *(setok: security token)* とは，*4* つの属性

内容 (contents): 必要ならばメッセージ認証子や電子署名なども含む．

額面価格 (explicit price): 購入時に支払われた非負の価格．$\bar{S}$で表す．

額面価値 (explicit values): 購入時における内容の質を表現する非負の数値の組．$\bar{V}_1, \bar{V}_2, \cdots, \bar{V}_m$ で表す．m を額面価値の**次元**と呼ぶ．各要素$\bar{V}_i$が大きければ大きいほど，高い質を表す．

時刻印 (timestamp): 購入時刻 t_0を信頼できる方式で示す．

を額面に持ち，２つの確率過程

背景価格 (implicit price): 非負の確率過程．Sで表す．

背景価値 (implicit values): 非負の確率過程の組．$V_1, V_2, \cdots, V_n$ で表す．n を背景価値の**次元**と呼ぶ．

と次のように関連づけられているディジタルオブジェクトである．

- 額面価格は**価格解釈過程** *(price-interpretation process)* $Y(t)=y(t, S(t))$ の購入時における実現値である．価格解釈過程は非負過程である．$y=(t,s)$ は**価格解釈関数** *(price-interpretation function)* と呼ばれ，s に関して単調増加である．額面価格を書き換えることはできない．
- 額面価値は**価値解釈過程** *(value-interpretation processes)* $H_1(t)=h_1(t,V_1(t),V_2(t),\cdots,V_n(t))$, $H_2(t)=h_2(t, V_1(t), V_2(t), \cdots, V_n(t)), \cdots, H_m(t)=h_m(t, V_1(t), V_2(t), \cdots, V_n(t))$ の購入時における実現値である．すべての価値解釈過程は非負過程である．$h_1(t, v_1, v_2, \cdots, v_n)$, $h_2(t, v_1, v_2, \cdots, v_n)$, $\cdots$, $h_m(t, v_1, v_2, \cdots, v_n)$ は**価値解釈関数** *(value-interpretation functions)* と呼ばれる．どの額面価値も，書き換えることはできない．

システムとしてのセトックは，表記法 *(notation)* を明示したい時には $(S, Y; V, H, n, m)$ などと書く．発行済みの個々のデータオブジェクトとしてのセトックは**シェア** *(share)* と呼ばれ，$(\bar{S}; \bar{V}_1, \bar{V}_2, \cdots, \bar{V}_m; t_0)$ などと表記される．

定義 2.2 (一次元価値セトック) セトックは，その額面価値が１次元である場合かつその場合に限り，**一次元価値である** *(single-valued)* といわれる．この時，添字を省略して$\bar{V} = H(t_0) = h(t_0, V_1(t_0), V_2(t_0), \cdots, V_n(t_0))$ などと書くことができる．

2.3 諸性質定義用の語彙

本節では，個々の具体的なセトックやシェアを特徴づける際に用いる用語を定義する．

定義 2.3 (払戻可能性) セトックのシェア $(\bar{S};\ \bar{V}_1,\ \bar{V}_2,\ \cdots,\ \bar{V}_m;\ t_0)$ は，条件「時域 $\boldsymbol{T}$内ならばいつでも，そのシェアを額面価格$\bar{S}$で売却できる」が満たされる場合かつその場合に限り，$\boldsymbol{T}$-**払戻可能である** *($\boldsymbol{T}$-refundable)* といわれる．$\boldsymbol{T}$は**払戻可能期間** *(refundable period)* と呼ばれる．払戻可能期間は確定的であるとは限らず，連続的でなくともよい．特に，$[t_0, \infty)$-払戻可能である場合には，**永久払戻可能である** *(∞-refundable)* といわれる．同じく $[t_0, t_0 + T_R)$-払戻可能である場合には，払戻可能期間の長さ T_Rを（太字にせず）用いて T_R-払戻可能 *(T_R-refundable)* と書いてよい．払戻可能期間を特に明示しない場合は，単に「払戻可能」という．

定義 2.4 (厳格な払戻可能性) セトックは，以下の *3* つの条件が満たされる場合かつその場合に限り，**厳格に** $\boldsymbol{T}$-**払戻可能である** *(strictly $\boldsymbol{T}$-refundable)* といわれる．

- 任意のシェアが払戻可能である．
- どのシェアについても，払戻可能期間は確定的である．
- 所有者は，払戻可能期間外にはいかなる価格でもシェアを売却できない．

特に，厳格に$\emptyset$-払戻可能なセトックは，**払戻不可能である** *(unrefundable)* といわれる．

定義 2.5 (取引可能性) 一次元価値セトックのシェア $(\bar{S};\ \bar{V};\ t_0)$ は，以下の *2* つの条件が満たされる場合かつその場合に限り，$\boldsymbol{T}$-**取引可能である** *($\boldsymbol{T}$-tradable)* といわれる．

- $\bar{V} > 0$ である．
- 時域$\boldsymbol{T}$内ならばいつでも，価値解釈過程が正であって所有者は**価値比例価格** *(value-proportional price)*

$$S_p = \frac{\bar{V}}{h(t, V_1(t), V_2(t), \cdots, V_n(t))} y\left(t, S\left(t\right)\right)$$

でそのシェアを売却できる．

$\boldsymbol{T}$は**取引可能期間** *(tradable period)* と呼ばれる．取引可能期間は確定的であるとは限らず，連続的でなくともよい．特に，$[t_0, \infty)$-取引可能である場合には，**永久取引可能である** *(∞-tradable)* といわれる．同じく $[t_0, t_0 + T)$-取引可能である場合には，T-取引可能 *(T-tradable)* と書いてよい．取引可能期間を特に明示しない場合は，単に「取引可能」という．

定義 2.6 (厳格な取引可能性) セトックは，以下の *3* つの条件が満たされる場合かつその場合に限り，**厳格に$\boldsymbol{T}$-取引可能である** *(strictly $\boldsymbol{T}$-tradable)* といわれる．

- 任意のシェアが取引可能である．
- どのシェアについても，取引可能期間は確定的である．
- 所有者は，取引可能期間外にはいかなる価格でもシェアを売却できない．

特に，厳格に$\emptyset$-取引可能なセトックは，**取引不可能である** *(untradable)* といわれる．

定義 2.7 (オンライン分割可能性) セトック $(S,\ Y;\ V,\ H,\ n,\ m)$ は，条件

- 価格解釈課程の実現値が正である時点 $t = t_0$においては必ず，誰もが任意の正の**注文価格** *(order price)*S_cを指定して，それに対する**比例額面価値** *(proportional explicit values)*

$$\frac{S_c}{Y(t_0)} h_i(t_0, V_1(t_0), V_2(t_0), \cdots, V_n(t_0))$$

$(1 \leq i \leq m)$ を記載されたシェアを購入できる．

を満たす場合かつその場合に限り，**オンライン分割可能である** *(online-divisible)* といわれる．オンライン分割可能でないセトックは，**オンライン分割不可能である** *(online-indivisible)* といわれる．

定義 2.8 (オフライン分割可能性) 正の額面価格$\bar{S}$を有するシェア $(\bar{S};\ \bar{V}_1,\ \bar{V}_2,\ \cdots,\ \bar{V}_m;\ t_0)$ は，所有者がそのシェアを**価格比例的に** *(price-proportional manner)* 任意の割合で二分割できる場合かつその場合に限り，**オフライン分割可能である** *(offline-divisible)* といわれる．ここに，価格比例的であるとは，$(\bar{S}^1; \bar{V}_1^1, \bar{V}_2^1, \cdots, \bar{V}_m^1; t_0)$ と $(\bar{S}^2; \bar{V}_1^2, \bar{V}_2^2, \cdots, \bar{V}_m^2; t_0)$ に分割した際に次式が成立することである*:*

$$\bar{S}^1 + \bar{S}^2 = \bar{S},\ \bar{S}^1 > 0,\ \bar{S}^2 > 0,$$

$$\bar{V}_j^i = \frac{\bar{S}^i}{\bar{S}} \bar{V}_j \quad (i = 1, 2; j = 1, 2, \cdots, m)$$

オフライン分割可能でないシェアは，**オフライン分割不可能である** *(offline-indivisible)* といわれる．

定義 2.7や定義 2.8における価格比例性は単純過ぎると考える読者もいるかもしれないが，本論文では「複雑な状況は価値解釈関数や価格解釈関数でモデル化する」という立場をとっている．

定義 2.9 (価値の失効可応性) セトック $(S,\ Y;\ V,\ H,\ n,\ m)$ が *1* つ以上の背景価値に関して単調増加である価値解釈関数を１つ以上持っているとする．それらの背景価値すべてを $\{V_{j_1},\ V_{j_2},\ \cdots,\ V_{j_s}\}$ とする．このセトックは，$V_{j_1}(t) = V_{j_2}(t) = \cdots = V_{j_s}(t) = 0$ である時かつそのような時に限って，**失効した** *(compromised)* といわれる．そして，以下の条件が満足される場合かつその場合に限り，**価値に関して失効可応である** *(compromise-responsive in value)* といわれる：

- $V_{j_1},\ V_{j_2},\ \cdots,\ V_{j_s}$のうち１つ以上の背景価値に関して単調増加であるような任意の価値解釈関数 h_iについて，「$V_{j_1}(t) = V_{j_2}(t) = \cdots = V_{j_s}(t) = 0$ ならば必ず $H_i(t) = 0$ となる」が成り立つ．

$H_i(t)$ が実現値として *0* を取る時，そのセトックは i 番目の額面価値に関して**無効化された** *(revoked)* という．

定義 2.10 (価格の失効可応性) セトック $(S,\ Y;\ V,\ H,\ n,\ m)$ が１つ以上の背景価値に関して単調増加である価値解釈関数を１つ以上持っているとする．それらの背景価値を $\{V_{j_1},\ V_{j_2},\ \cdots,\ V_{j_s}\}$ とする．このセトックは，以下の条件が満足される場合かつその場合に限り，**価格に関して失効可応である** *(compromise-responsive in price)* といわれる：

- $V_{j_1}(t) = V_{j_2}(t) = \cdots = V_{j_s}(t) = 0$ ならば必ず $Y(t) = 0$ である．

3　トークン派生物

3.1　コールオプション

ネットワーク生活では，支払いも電子的に済ませたいであろう．一般に電子マネーなどの支払い方式では，使用可能な通貨単位のきめ細かさと効率がトレード・オフの関係にある [8]．したがって，購入単位の価格が固定されていれば，利用可能な支払い方式の選択肢が広がる．そこで，ここでは基礎理論の手始めとして，価格解釈過程が単位プロセスである一次元価値セトックを扱う．その他の種々の性質も含め，次の仮定を置く．

仮定 3.1 (無効化リスクのあるセトック) 本章以降では，以下の性質を満たす一次元価値セトック $(S,\ Y;\ V,\ H,\ n,\ 1)$ を考察する．

1. 価格解釈過程は単位プロセス $Y(t) = 1$ である．
2. オンライン分割不可能である．
3. どのシェアもオフライン分割不可能である．
4. セトックに対するショート・ポジションは認められない．
5. T-取引可能であって，$T = \tau_T(t, H(t))$ は次の確率過程で表される．

$$\tau_T(t,h) = \begin{cases} T_0 & (\text{if } h > 0) \\ 0 & (\text{if } h = 0) \end{cases}$$

ここに，$T_0 > 0$ は確定的な正定数である．

6. T_R-払戻可能であって，$T_R = \tau_R(t, H(t))$ は次の確率過程で表される．

$$\tau_R(t,h) = \begin{cases} 0 & (\text{if } h > 0) \\ T_1 & (\text{if } h = 0) \end{cases}$$

ここに，$T_1 > 0$ は確定的な正定数である．

7. 失効が起こらない限り，$H(t)$ の実現値は正の有限値である．
8. 失効の生起は，強度λのポアソン過程にしたがう．
9. 価値に関して失効可応である．

価格は一定と仮定したので，価格に関する派生物を定義することはできない．そこで，価値に関して権利を約束するタイプの派生物を考える．

定義 3.1 (ヨーロッパ型コールオプション) 時刻 $t = t_0$ に発行される**ヨーロッパ型コールオプション** *(European call option)* とは，「将来の指定された時刻 $T_m (< t_0 + \min\{T_0, T_1\})$ において当該セトックのシェアを *1* つ，約束した額面価値 Kを記載して固定単位価格で購入することができる」という権利を所有者に与える派生物である．T_mは**満期** *(maturity)*，Kは**行使価値** *(strike value* または *exercise value)* と呼ばれる．

3.2 価格評価

仮定 3.2 (市場環境) 本論文では，簡単のため，以下のように単純化した市場環境を考える*:*

1. 通信には時間的にも経費的にもコストがかからない．
2. セトックに関する仮定 *3.1*以外には，どの参加者も，取引量の規制を受けない．したがって，銀行と無リスク利率 r_fで任意の金額の資金を出し入れできる．
3. 無リスク資産の価格過程 Bは，方程式 $dB(t) = r_f B(t)dt$ で記述される．
4. どの時点でも，購買価格と売却価格は同一である．
5. 裁定取引は存在しない．

さて，満期T_mのヨーロッパ型コールオプションの価格過程を $C(t)$ とし，価格評価のための連続時間確率過程モデルとして次のようなものを考える．

仮定 3.3 (連続時間モデル) 以下の性質が成り立つ状況で関数 $c(t,h)$ を用いて価格過程が $C(t) = c(t, H(t))$ と書けるとする：

- 関数 $c(t,h)$ は $C^{1,2}$-級であって，定義域は$\boldsymbol{R}_+ \times \boldsymbol{R}_{++}$（ただし$\boldsymbol{R}_{++}$は正の実数の集合，$\boldsymbol{R}_+$は非負の実数の集合）である．
- 任意の $t \in \boldsymbol{R}_+$に対して $c(t,0) = 0$ である．
- 価値解釈過程のダイナミクスは次式で与えられる．

$$dH = (1 - \lambda(t,H(t))dt)\{\mu(t,H(t))Hdt + \sigma(t,H(t))HdW\} + \lambda(t,H(t))dt \cdot (-H)$$

ただし$\mu(t,H(t))$ と$\sigma(t,H(t))$ はそれぞれドリフト *(drift)* 係数とボラティリティ*(volatility)* を表す適合過程であって，Wは今とっている確率測度 *(objective measure)* の下での *Wiener* 過程である．適合過程$\lambda(t,H(t))$ で表されるポアソンジャンプのリスクは系統的（*systematic*）である．

- 適合過程 $G(t) = \{H(t)\}^{-1}$を定義し，対応する実現を $g = 1/h$ と書く．c を t と gの関数と見なす場合に混乱を避けるため，$\hat{c}(t,g) = c(t,1/g)$ という表記法を用いる．関数$\hat{c}$も $C^{1,2}$-級であるとする．

紙面の都合で導出仮定は省略するが，オプション価格に関して次の定理が得られる．

定理 3.1 (価格評価の境界値問題) 無裁定条件を満たす $C(t) = c(t, H(t))$ という形の価格過程は，

$$c(t,h) = \begin{cases} \hat{c}(t,1/h) & \text{for } h > 0 \\ 0 & \text{for } h = 0 \end{cases}$$

に限られる．ただし$\hat{c}(t,g)$ は境界値問題

$$\frac{\sigma^2}{2} g^2 \hat{c}_{gg} + (r_f - \lambda)\, g\hat{c}_g - (r_f + \lambda)\hat{c} + \hat{c}_t = 0$$

$$\hat{c}(T_m, g) = \max\{0, Kg - 1\}$$

の定義域 $[0, T_m] \times \boldsymbol{R}_{++}$ における解である．

4　考察

4.1　失効リスクのない場合の解析解

価値に関して書かれたオプションの基本的な性質を考察するため，本節では，解析解導出の容易な単純化した状況を考える．すなわち，失効リスクがなく（$\lambda = 0$）係数μとσが確定的定数という状況で，境界値問題を解く．解いた結果，次の定理が得られる．

定理 4.1 (単純化された状況のオプション価格) μとσが確定的定数であって，かつ，$\lambda = 0$ ならば，オプション価格は次式で与えられる：

$$c(t,h) = \frac{K}{h} N\left[d_1(t,h)\right] - \exp\left\{-r_f(T_m - t)\right\} N\left[d_2(t,h)\right]$$

ただし Nは正規分布の累積分布関数

$$N[d] = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{d} \exp\left(-\frac{x^2}{2}\right) dx$$

であって，

$$d_1(t,h) = \frac{1}{\sigma\sqrt{T_m - t}} \left\{ \ln\left(\frac{K}{h}\right) + \left(r_f + \frac{\sigma^2}{2}\right)(T_m - t) \right\},$$

$$d_2(t,h) = d_1(t,h) - \sigma\sqrt{T_m - t}.$$

である．

ここで，$H(0) \in [80, 120]$ の範囲で様々なパラメータ値に対して $C(0)$ を計算し，定理 4.1で与えられる解析解の性質を数値的に調べる．以降では，$C(0)$, $H(0)$ をそれぞれ単に C, Hと書く．１年を時間の単位とし，無リスク利率 r_fは

$$r = \exp(r_f) - 1 \tag{1}$$

によって年率 rに換算する．基本的なパラメータ設定は $\sigma = 0.2$，$K = 100$，$r = 0.5$ [%] とする．満期 T_mを $T_m = 0.5, 1, 2$ としたそれぞれの場合につき，横軸 H の値に対して縦軸に Cをプロットする．

結果を図 1に示す．いずれも単調減少のグラフが得られている．これは，行使価値を固定すれば，現在価値が低ければ低いほどオプションが有利になるためである．3 つの曲線を比較すると，次のように直感的な解釈に合致する．満期が遠ければ遠いほど，直感的には，不確かさが増す．この影響が，オプション価格の（現在価値に対する）変化を緩和している．すなわち，現在価値が行使価値より小さい領域 $H < K = 100$ では大きな T_m の方が低いオプション価格をもたらしており，現時点でのオプションの有利さが（小さな T_mと比べて）相対的に小さい．逆に，現在価値が行使価値より大きい領域 $H > K = 100$ では大きな T_mの方が高いオプション価格をもたらしており，現時点でのオプションの不利さが（小さな T_mと比べて）相対的に小さい．

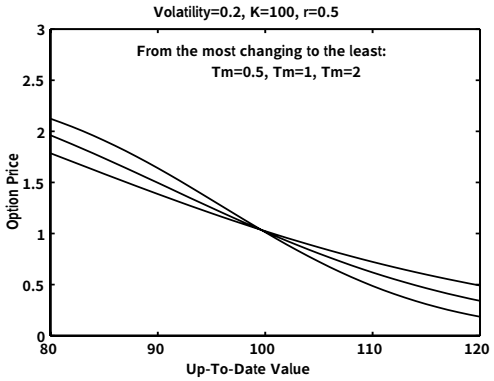

図 1: 現在価値に対するオプション価格の変化．右下がりグラフの変化が激しいものから順に，満期を $T_m = 0.5, 1, 2$ とした場合の様子を示している．

4.2　リスク計測への応用

まだ起きていない無効化のリスクを表すパラメータλの値をネットワーク社会がどう捉えているか，合理的に知る方法はあるだろうか．リスク調査としてもっとも簡便なものは意見を求めるアンケート調査だが，残念ながら主観の入り込む余地が極めて大きい．そのような主観的要素を避けるため，直接計測はできなくとも推定いわば間接計測の方法を構築したい．本節では，本論文で導入した価格評価のアプリケーションとして，この間接計測法について簡単に考察する．すなわち，λ以外のパラメータが市場観測から得られている場合にλを推定する問題である．

λが既知でオプション価格 Cが未知ならば，定理 3.1の境界値問題を数値的に解いて Cを求めればよい．これを順方向の計算とすれば，今考えている Cが既知でλが未知の問題は，逆問題である．もっとも単純な逆問題解法は，次のように Cの観測値と計算値の誤差を繰り返し計算で十分小さくする方法である．

(方法 1)
1. 最近の観測データから r_f, σを定める．
2. リスクλの初期推定値を定める．
3. 現在の市場観測値 Hとλの推定値を入力し，定理 3.1からオプション価格を計算する．
4. オプション価格の計算値と現在の観測値の誤差が十分小さいかどうかを調べる．着目しているセトックについて，満期や行使価値の異なるオプション銘柄が複数あれば，それらのデータをすべて用いて各銘柄に関する誤差の二乗和を考える．
5. 誤差が十分小さければ終了し，現在の推定値を解とする．

6. 誤差がまだ十分小さくなければ，リスク推定値を修正して同様のプロセスを繰り返す．直感的には，オプション価格の計算値が観測値と比べて高過ぎる傾向にあればリスク推定値を上方修正して計算値を下げるようにする．これは，無効化が起きればオプションが無意味（オプションを行使してセトックを購入しても，同じ価格の払戻が可能なだけであって，ペイオフは0）となってしまうからである．

繰り返し計算の回数や，方法1のステップ3で解く境界値問題の数値解法に求める精度次第では，十分迅速にリスク推定値が得られないかもしれない．しかし，リスクがある値λ^*を越えているかどうかを知りたいだけならば，繰り返しをせずに済ますことができる可能性がある．すなわち，方法1のステップ6で用いた着眼点を利用して，次のような方法を考えることができる．

(方法2) 1. 方法1のステップ3に同じ．

2. $\lambda = \lambda^*$とする．
3. 現在の市場観測値Hと$\lambda = \lambda^*$を入力して，定理3.1からオプション価格の計算値を得る．
4. オプション価格の計算値が現在の観測値よりも高いかどうかを調べる．着目しているセトックについて，満期や行使価値の異なるオプション銘柄が複数あれば，それらのデータをすべて用いて統計的検定で判別する．
5. 計算値が高いと判別されれば，リスクがλ^*よりも高いと判断する．

5 おわりに

本論文では，情報セキュリティ技術を応用したネットワーク取引で避けられないであろうリスクについて基礎理論を展開し，応用の可能性の一つを示した．理論で用いるモデル化では，取引される電子トークンを，価格以外にも予測不能な時間的変化をする価値を属性として持つオブジェクトとして定義した．このオブジェクトをセトックと名付け，その諸性質を定義した．既存の金融取引の世界との違いに留意しつつ本質を逃さない範囲でできる限り単純化したセトックの価値に関して，リスクをヘッジする派生物としてヨーロッパ型コールオプションを定義した．そして，セトックの無効化リスクを系統的なリスクであると仮定して，オプション価格を決める方程式を導出した．

無効化リスクなどがないと単純化した状況では，方程式の解析解を導出し，オプション価格の基本性質を調べた．結果は,「将来の不確かさが増せば現在の有利さや不利さが緩和される」という直感的理解のできるものであった．

無効化リスクのある場合には，オプション価格評価理論の応用として，そのリスクの間接計測法を簡単に考察した．主観の入り込む余地が大きいアンケート調査と比べて，間接計測法はその客観性だけでなく，自動化できる可能性という利点がある．詳細は今後様々な研究が必要となろうが,「情報セキュリティシステムで知りたいけれども今までは知る術のなかったパラメータ」を間接的にでも計測できる可能性を示したという点が重要だと考える．

参考文献

[1] Maurer, U.: "Modelling a Public-Key Infrastructure", *Computer Security — ESORICS'96* (Bertino, E., Knuth, H., Martella, G. and Montolivo, E.(eds.)), Lecture Notes in Computer Science 1146, Springer-Verlag, pp. 325–350 (1996).

[2] Essin, D. J.: "Patterns of Trust and Policy", *Proc. of New Security Paradigms Workshop '97*, pp. 38–47 (1997).

[3] Reiter, M. K. and Stubblebine, S. G.: "Toward Acceptable Metrics of Authentication", *Proc. of the 1997 IEEE Symposium on Security and Privacy*, pp. 10–20 (1997).

[4] Reiter, M. K. and Stubblebine, S. G.: "Resilient Authentication using Path Independence", *IEEE Trans. Comput.*, Vol. 47, No. 12, pp. 1351–1362 (1998).

[5] Reiter, M. K. and Stubblebine, S. G.: "Authentication Metric Analysis and Design", *ACM Transactions on Information and System Security*, Vol. 2, No. 2, pp. 138–158 (1999).

[6] Kohlas, R. and Maurer, U.: "Confidence Valuation in a Public-Key Infrastructure Based on Uncertain Evidence", *Proc. of Third International Workshop on Practice and Theory in Public Key Cryptosystems (PKC 2000)* (Imai, H. and Zheng, Y.(eds.)), Lecture Notes in Computer Science 1751, Springer-Verlag, pp. 93–112 (2000).

[7] Black, F. and Scholes, M.: "The Pricing of Options and Corporate Liabilities", *Journal of Political Economy*, Vol. 81, pp. 637–654 (1973).

[8] Eng, T. and Okamoto, T.: "Single-Term Divisible Electronic Coins", *Advances in Cryptology — EUROCRYPT'94* (Santis, A. D.(ed.)), Lecture Notes in Computer Science 950, Springer-Verlag, pp. 306–319 (1995).