群知能を基礎とする暗号システムの提案

木下研究室　　茂木　崇将（200802936）

Ⅰ．まえがき

web サイトの閲覧や web を介してデータベースにアクセスするクラウドシステム. そのクラウドが形成するコミュニティ内の情報が常に変化する, という前提において、クラウドの情報漏洩を防止することは、新しい情報を作る行為とともに重要な課題である. しかし, 従来の情報セキュリティ技術は“変動する環境”に適応するというよりもむしろ, 変動を否定し, 変動に抗するシステムである.

変動に適応しつつも情報漏洩を防止するアクセス制御を使った群知能システムを基にし, 群知能のアクセス制御システムにおける暗号システムの位置付けを考察する.

Ⅱ．基礎知識

1.　群知能

群知能は単純なエージェントの個体群から構成される.Boid は鳥の群れをシミュレーションできる群知能アルゴリズムであり,以下の三つの力をもつ.

-Alignment（すぐ隣の動きに合わせる力）
-Cohesion（群れの中心に向かおうとする力）
-Separation（距離を一定に保とうとする力）

2.　暗号システム

情報をやり取りする際に,第三者に改ざんされないよう,規則に従ってデータを変換し暗号化するシステム.

3.　Tanimoto 係数　$$T(A,B)=\frac{A\cdot B}{|A|^2+|B|^2-A\cdot B}$$

Ⅲ．群知能の中の暗号システムの提案

集合論的同一性と家族的類似性の違いは何か

家族的類似の定義：

{FA}i と{FA}j の類似性を Tanimoto 係数で計算する。

Tanimoto 係数が，設定された閾値以上の場合，家族的類似とする。家族的類似で定義される２つの異なる言語ゲーム（群知能システム）において，それらが家族的類似の中に含まれるのかを以下のように判定する。

群知能システム[i]が群知能システム[j] に含まれる場合：

{FA}i の各 particle は規則 R に従う.

{FA}j の各 particle は規則 R に従う.

{FA}i の各 particle 間の Tanimoto 係数が，設定された閾値以上である.

{FA}j の各 particle 間の Tanimoto 係数が，設定された閾値以上である.

{FA}i と{FA}j 間の各 particle の Tanimoto 係数が，設定された閾値以上である.

ある状態において，　{FA}i の particle は，{FA}j の particle に集合論的に含まれる.

{FA}i の各 particle は規則 S に従う.

{FA}j- {FA}i の各 particle は規則 S に従わない.

家族的類似で集まった群れの振る舞いを図 1 に示す。

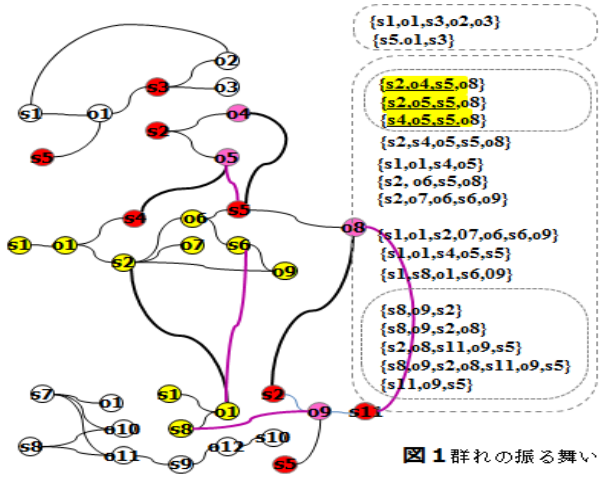

図 1 群れの振る舞い

Ⅳ．まとめ

群知能のアクセス制御システムにおける暗号システムの位置付けを考察し，「群知能の中の暗号システムは群知能のアクセス制御という視点の群れの中, 及び群れを横断する新しい群れを形成するものである」ことを示した。

文献

[1] 久保直也，森住哲也，鈴木一弘，木下宏揚：“変動する秩序の中でパーソナリティを区別するマルチエージェントシステム”，電子情報通信学会，2011 年暗号と情報セキュリティシンポジウム SCIS2011，(2011.1).

[2] 久保直也，森住哲也，鈴木一弘，能登正人，木下宏揚：“群知能を適用したアクセス制御システム”，暗号と情報セキュリティシンポジウム scsi2012, (2012-01).