# 2-205 自律分散概念に基づく不正侵入検知システム

## Autonomous Intruder Detection System based on Autonomous Decentralized Systems

○柳川小次郎（明治大学） 稲吉基悦（明治大学） 向殿政男（明治大学）

Kojiro YANAGAWA, Dept of Computer Science, School of Science and Technology, Meiji University.
1-1-1 Higashi-mita, Tama-ku, Kawasaki-shi, Kanagawa-ken 214-8571 Japan
Motoyoshi INAYOSHI, Meiji University
Masao MUKAIDONO, Meiji University

Recently, many companies and universities are defending the network systems by the Firewall and IDS. The management costs of the above security technologies are very expensive because the skillful administrators are required to keep the system in good working order. This paper proposes the Autonomous Intruder Detection Systems based on Autonomous Decentralized Systems (A-IDS). All of hosts that are composed a network system are watched from other hosts in A-IDS. Therefore, when a network system is attacked, the system is possible to take counter measure at once because even if any host is attacked, another terminal is not attacked. Thus, the security ability of the network system to be strengthened and an administrator's burden is reduced by A-IDS. Accordingly, it is possible to cut down the management cost of the network security systems.

***Key Words***: Intruder Detection System, Autonomous Decentralized Systems, Network Security

### 1. はじめに

近年，インターネットの普及が様々な分野に深い影響を与えているなか，ネットワークセキュリティー技術がますます注目を集めている．なかでも，コンピュータやネットワークに対する不正行為を検出し，通知する不正侵入検知システム(IDS: Intruder Detection System)に関する研究は盛んに行われている[(1) (2) (3) (4)]．IDSとファイアウォールを組み合わせることによって，より安全なシステムを構築することが可能である．しかしながら，従来のIDSには次のような問題点がある．

(問題 1) IDS が攻撃対象となり機能障害が発生した場合，システムが無防備になる．

(問題 2) IDSのルールに登録されていない不正侵入は検知できない．

(問題 3) 新種の侵入手法が判明した場合，管理者がIDSのルールを手動で変更しなければならない為，対応へのタイムラグが生じる．

我々は，これらの問題を解決する為に，IDSに自律分散概念[(5) (6)]を適用した，自律分散概念に基づく不正侵入検知システム(A-IDS: Autonomous Intruder Detection Systems)を提案する．

### 2. 不正侵入検知システム IDS

IDSは設置場所によってネットワーク型とホスト型に分類される．ネットワーク型IDSは防御したいネットワークにステルスモードで接続され，ネットワークセグメントを流れるすべてのトラフィックを監視する．ホスト型IDSは防御したいホストにインストールされ，ホストの監査機能と連携してログファイルやファイルの改ざんの監視を行う．IDSの侵入検知アルゴリズムには不正検出と異常検出の2種類が存在する．不正検出ではあらかじめ登録されたルールベースとのマッチングによって不正侵入を検出し，異常検出では事前に作成しておいた通常の運用形態のテンプレートとは異なる振る舞いを検出する．ネットワーク型IDSは不正検出アルゴリズムが，ホスト型IDSには異常検出アルゴリズムが用いられることが多い．IDSをファイアウォールやウイルス対策ソフトと連携させるでより安全なシステムを構築可能である．

しかしながら，IDSにはいくつかの問題点があり，我々は特に以下の問題点に注目した．

(1) ネットワーク型IDSの問題
- (1.1) 高速ネットワークに接続された場合，すべてのトラフィックを検査することは困難である．
- (1.2) IDS のルールに登録されていない不正侵入は検知できない．
- (1.3) 新種の侵入手法が判明した場合，管理者がIDSのルールを手動で変更しなければならない為，対応へのタイムラグが生じる．

(2) ホスト型IDSの問題
- (2.1) 個々のホストに導入するため，管理コストが高い．
- (2.2) 任意のホスト型IDSが攻撃を受けた場合，他のホスト型IDSでは検知・対応できない．

(3) 共通の問題
- (3.1) IDS自体が攻撃対象となり機能障害が発生した場合，監視対象が無防備になる．
- (3.2) 1度の不正アクセスで成立する部類の攻撃には，不正侵入検出後に対応しても間に合わない．

本論文ではこれらの問題を解決する為に，自律分散概念に基づく不正侵入検知システムを提案する．

### 3. 自律分散概念に基づく不正侵入検知システム A-IDS

A-IDS では防御したいネットワーク内のすべての端末が，別の端末によって監視される相互監視の形態をとる．そのため如何なる端末が攻撃を受けても，攻撃を受けていない別の端末で，侵入の検知と対応を管理者の介入なしで自律的に行うことが可能である．

相互監視によって形成されるリング状の論理的なネットワークを**A-IDS 監視ネットワーク**と呼ぶ（図1）．

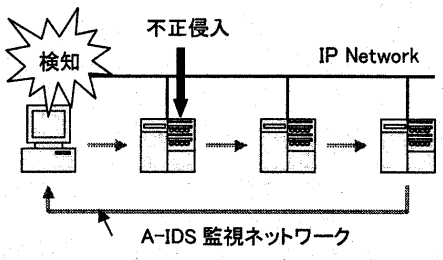


Fig. 1 A-IDS Monitor Network

端末は A-IDS 監視ネットワークのトポロジに従って監視対象の端末とデータ交換を行い，監視対象の端末が正常に動作しているか，すなわち不正侵入を受けていないかを監視する．A-IDS 監視ネットワークは監視対象の IP ネットワーク上に構築されるのではなく，インターネットに接続されていない専用ネットワーク上に構築される．これは A-IDS 監視ネットワーク上で行うメッセージ交換を盗聴，改竄されない為と，比較的通信コストが高い自律分散システムのトラフィックを監視対象の IP ネットワークに反映させない為である．

このような物理的な専用ネットワークを **A-IDS データフィールド**と呼ぶ．A-IDS データフィールドのアーキテクチャは，自律分散概念におけるデータフィールドと同じである．従って，A-IDS データフィールド上の通信はすべてブロードキャストによって行われる．

A-IDS データフィールドを用いてデータ交換を行える端末を **A-IDS クライアント**と呼ぶ．A-IDS クライアントは **A-IDS アトム**と IDS から構成される．A-IDS アトムは自律分散概念におけるアトムと同じく，自らを管理し必要に応じて他のサブシステム（A-IDS アトム）と協調する機能を持っている．A-IDS は IDS に特化したアトムであり，アプリケーションとして，IDS とのインタフェースしか持たない．A-IDS アトムは連携する IDS の入出力である“A-IDS クライアントへのイベント情報（パケットの送受信やコマンド入力等）”と“IDS が検知した不正進入に関する情報”を A-IDS データフィールドへ送出し，他の A-IDS アトムにこれらの情報を提供する．同様に，A-IDS アトムは他の A-IDS クライアントの IDS への入出力情報を A-IDS データフィールドから獲得する．

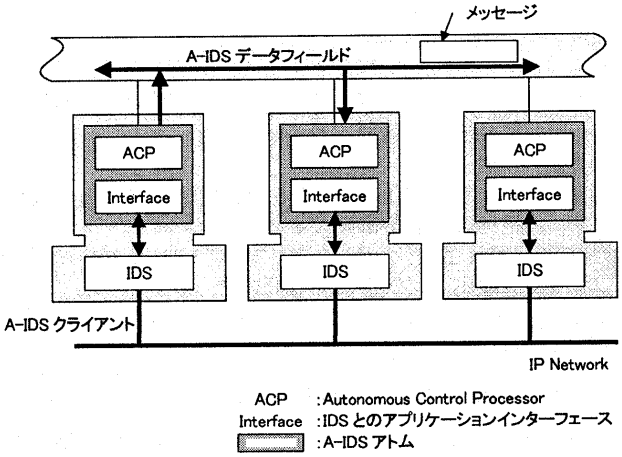


Fig. 2 Architecture of A-IDS Atom

A-IDS クライアントは図 2 に示すように A-IDS クライアントへの不正侵入を監視している IDS が，A-IDS データフィールドを介して他の A-IDS クライアントと協調動作可能な A-IDS アトムと連携する構成をとっている．従って，従来の IDS では，IDS の監視対象が攻撃の標的にならなければ得ることのできなかった不正侵入に関する情報を，A-IDS は攻撃の標的にならずとも得ることが可能である．すなわち，A-IDS クライアントは，他の A-IDS クライアントが何時，どのようにして侵入されたのかを知ることが可能である．

A-IDS クライアントは内包する IDS の種類によって**ホスト型 A-IDS** と**ネットワーク型 A-IDS** に分類される．A-IDS の基本的なシステム構成を図 3 に示す．

3.1 **ホスト型 A-IDS**　重要な端末に搭載されたホスト型 IDS が端末への不正侵入を監視するように，ホスト型 A-IDS も搭載された端末への不正侵入を監視する．また，ホスト型 A-IDS は他の A-IDS クライアントへの不正侵入を監視する．不正侵入を検知したホスト型 A-IDS は不正侵入に関する情報をネットワーク型 A-IDS に報告する．

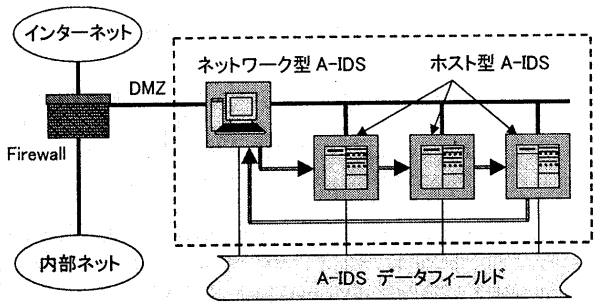


Fig. 3 Basic System Constitution of A-IDS

3.2 **ネットワーク型 A-IDS**　ネットワーク型 A-IDS はネットワーク型 IDS と同様に防御対象のネットワークを監視する．ネットワーク型 A-IDS はステルスモードでネットワークに接続するのではなく，ファイアウォールのように 2 つのセグメントを繋ぐように接続する．ネットワーク型 A-IDS は両セグメントから入力されるパケットをルールベースに基づいて監視し，問題があるパケットは破棄する．このルールベースは他の A-IDS クライアント（ホスト型 A-IDS）からの報告に基づいて変更可能である．すなわち任意の A-IDS クライアントが侵入を検知し，攻撃がネットワーク経由で行われた場合，侵入者からのパケットをネットワークから一時的に排除可能である．また，同じ手口の不正侵入に対する耐性をネットワーク全体に与えることが可能である．ただしこの場合は，何れかの A-IDS クライアントが不正侵入を検知することが前提条件となる．

ネットワーク型 A-IDS はフェイルセーフな構造になっている．ネットワーク型 A-IDS が DoS 攻撃等によって停止状態に追いやられたとしても，以降の不正侵入用のパケットはネットワーク型 A-IDS を通過することができず，外部からの不正パケットは防御対象のネットワークに到達することができない．また，内部から不正パケットが送信された場合は外部への被害の拡大を防ぐと共に，ネットワーク型 A-IDS を監視していたホスト型 A-IDS によって容易に犯人の特定が可能である．

## 4. A-IDS における致命的攻撃の検知方法

従来の IDS と異なり，A-IDS は端末が停止状態に追いやられても検知が可能である．本章では，A-IDS での致命的攻撃の検知方法について述べる．

A-IDS アトムは監視している A-IDS アトムに対し，A-IDS 監視ネットワーク経由で定期的に生存確認信号(SYN)を送信する．生存確認信号を受信した A-IDS アトムは即座に生存応答信号(ACK)を返信する．もし，一定時間内に生存応答信号が戻ってこなければ，監視先の端末が致命的攻撃によって停止状態に追い込まれたということである．A-IDS では，この生存信号のやり取りと，以下のプロセスを組み合わせて用いることで致命的攻撃を検知することができる．

(Step-1) 端末 A に対してパケット受信や，オフラインからのコマンド入力等のイベントが入力される．

(Step-2) 端末 A の A-IDS アトムは連携する IDS を用いて，イベントが不正侵入でないか検査する．

(Step-3) イベントが危険ではないと判断したら端末 A の A-IDS アトムはイベントを A-IDS 監視ネットワーク経由で，端末 A を監視している端末 B の A-IDS ア

トムに転送する．端末 B の A-IDS アトムは受け取ったイベントを保存する．

(Step-4) 端末 A はイベントの処理を実行する．

上記のプロセスによって，イベントを入力された端末で未知の不正侵入を検出できなくとも，生存応答信号が戻ってこなかった時点で，監視元の A-IDS アトムは不正侵入と不正侵入に用いられたイベントを検知可能である．

生存応答信号が戻ってこなかった場合，A-IDS アトムは最後の生存応答信号の前に受け取ったイベントを A-IDS 監視ネットワークに所属する全ての A-IDS アトムへ**警報**と共にブロードキャストする．

警報を受け取った A-IDS アトムは，自身が連携する IDS のルールに危険なイベントを追加することで，危険なイベントへの耐性を身に付ける．イベントがネットワーク経由の場合，ネットワーク型 A-IDS は危険なパケットを送信してきた端末からのアクセスを一時拒否する等の対策を平行して行う．

## 5. A-IDS 監視ネットワークの構築と再構築

本章では，A-IDS 監視ネットワークの構築と再構築のプロセスについて述べる．A-IDS 監視ネットワークは以下のような時にネットワークトポロジが変化する．

A) A-IDS 監視ネットワークに端末が追加された時
B) A-IDS 監視ネットワークに参加している何れかの端末が，不正侵入によって機能を停止した時
C) A-IDS 監視ネットワークに参加している何れかの端末が，管理者によって電源を OFF された時

### 5.1 A-IDS 監視ネットワークへの端末の追加

A-IDS 監視ネットワークに端末が追加された時，A-IDS アトムは以下のプロセスで，A-IDS 監視ネットワークのネットワークトポロジを変化させる．（図 4）

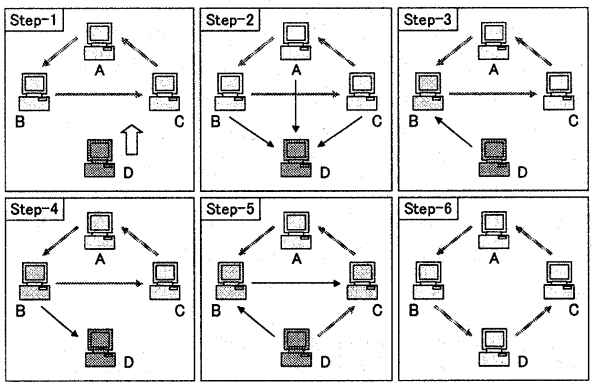


Fig. 4 Addition of A Terminal to An A-IDS Monitor Network

(Step-1) 追加された端末 D の A-IDS アトム *Atom-D* は，契約ネットプロトコル[7]のタスク告示メッセージを用いて“*Atom-D* の監視”という契約の締結要求を A-IDS データフィールドにブロードキャストする．

(Step-2) *Atom-D* からのタスク告示メッセージを受け取った各 A-IDS アトムは，*Atom-D* 宛ての入札メッセージを送信する．

(Step-3) *Atom-D* は自らの嗜好にあった入札メッセージを送ってきたアトム（図 4 では *Atom-B*）に対して落札メッセージを送信し，契約“*Atom-D* の監視”を締結する．この段階では *Atom-D* と契約を締結した *Atom-B* は *Atom-D* の監視をまだ開始しない．

(Step-4) *Atom-B* が何れかの A-IDS アトムを監視していれば，*Atom-B* は *Atom-D* に対し，*Atom-B* が締結していた契約（図 4 では契約“*Atom-C* の監視”）の譲渡を伝える．

(Step-5) *Atom-D* は *Atom-C* の監視を開始すると，*Atom-B* に契約引継ぎが終了した旨を知らせる．*Atom-B* は *Atom-D* からの報告を受け取ると，*Atom-C* に対して契約“*Atom-C* の監視”を *Atom-D* が引継いだことを伝え *Atom-D* の監視を停止する．

(Step-6) *Atom-B* は，*Atom-D* の監視を開始する．

### 5.2 不正侵入による端末の停止 その 1

A-IDS アトムは，監視先の端末が致命的攻撃を受けて停止したと判断した場合，A-IDS 監視ネットワークに報告すると同時に，A-IDS 監視ネットワークの再構築を行う．何故ならば，不正侵入を受けた端末によって監視されていた端末が，誰にも監視されない危険な状態で放置されているからである．

監視先の端末が不正侵入によって停止に追いやられた場合，A-IDS アトムは以下のプロセスで，A-IDS 監視ネットワークを再構成する．（図 5）

(Step-1) 端末 A のアトム *Atom-A* は，監視先の端末 B が不正侵入を受けたと判断．

(Step-2) *Atom-A* は警報と共に危険なイベントを A-IDS データフィールドへブロードキャストする．警報を受信した各 A-IDS アトムはイベントに基づいてルールを変更し，イベント受信を一旦停止する．その後，*Atom-A* は端末 B のアトム *Atom-B* に監視されていた端末に対する応答要求を A-IDS データフィールドにブロードキャストする．

(Step-3) *Atom-B* に監視されていた *Atom-C* が *Atom-A* に対して応答する．

(Step-4) *Atom-A* は応答要求を返してきた *Atom-C* に対して，*Atom-C* と *Atom-B* が締結していた“*Atom-C* の監視”という契約を *Atom-A* が引継いだことを伝える．

(Step-5) *Atom-A* は，*Atom-C* の監視を開始する．

(Step-6) *Atom-A* は警報解除を A-IDS データフィールドへブロードキャストし，各 A-IDS アトムは停止していたイベント受信を再開する．

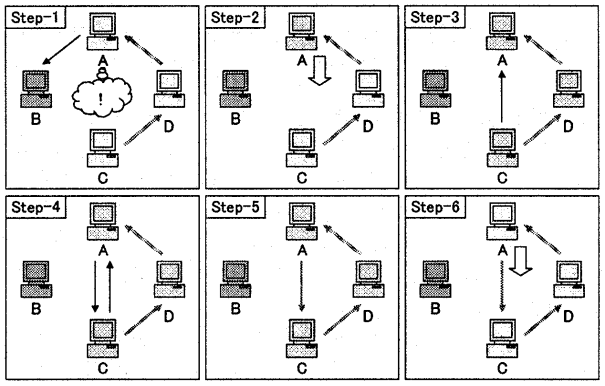


Fig. 5 Rebuilding an A-IDS Monitor Network

### 5.3 不正侵入による端末の停止 その 2

A-IDS 監視ネットワーク内の複数の端末が同時に不正侵入を受けた場合，5.2 節で述べたプロセスの Step-3 で応答が返ってこない可能性がある．このような場合，5.2 節のプロセスでは A-IDS 監視ネットワークを再構築できない．このように A-IDS 監視ネットワークが崩れた場合 A-IDS アトムは以下のプロセスで A-IDS 監視ネットワークを再構成する．（図 6）

(Step-1) 端末 A のアトム *Atom-A* は，監視先の端末 B が不正侵入を受けたと判断．

(Step-2) *Atom-A* は警報と共に危険なイベントを A-IDS データフィールドへブロードキャストする．警報を受信した各 A-IDS アトムはイベントに基づいてルールを変更し，イベント受信を一旦停止する．その後，*Atom-A* は端末 B のアトム *Atom-B* に監視されていた端末に対する応答要求を A-IDS データフィールドにブロードキャストする．

(Step-3) *Atom-B* に監視されていた *Atom-C* も致命的不正侵入によって停止状態にあるので *Atom-A* に対して応答できない．

(Step-4) 警報発信から一定時間経過しても *Atom-A* に監視を要求するタスク告示が届かない場合，*Atom-A* は A-IDS 監視ネットワークの一斉再構築を要求するタスク告示メッセージを A-IDS データフィールドにブロードキャストする．

(Step-5) 一斉再構築要求を受信した全ての A-IDS アトムは現在締結している契約を破棄し，構築状態に推移する．その後，それぞれの端末は独自に A-IDS 監視ネットワークへの参加を行っていく．

(Step-6) A-IDS 監視ネットワークの再構築が終了し，各 A-IDS アトムは停止していたイベント受信を再開する．

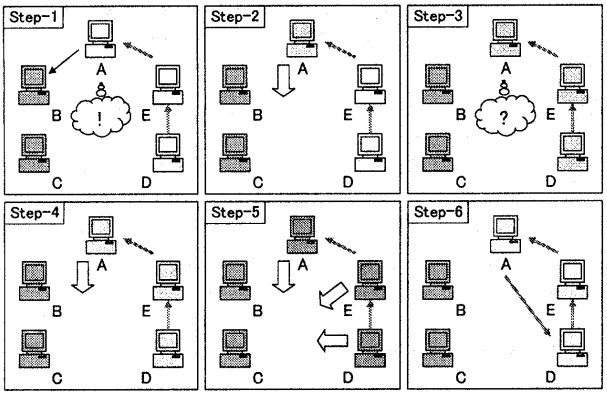


Fig. 6 Rebuilding an A-IDS Monitor Network when Topology Collapsed by the Intrusion at the same time

**5.4 管理者による端末の停止** A-IDS 監視ネットワークに属している端末が，管理者によって停止された場合，A-IDS アトムは，自身を監視している A-IDS アトムに対して停止信号を送信してから停止状態に移行する．停止信号を受け取った A-IDS アトムは直ちに A-IDS 監視ネットワークへの追加プロセス（5.2 節）へ移行し，A-IDS 監視ネットワークの再構築を開始する．

このプロセスが無いと，電源を落とされた端末を監視している A-IDS アトムによって不正侵入によって端末が停止したと誤解され，各端末のルールベースが誤った修正をされる危険性がある．

## 6. プロトタイプによる実験

本章ではプロトタイプシステムによる A-IDS の実証実験の結果を報告する．実験システムは図 7 に示すように 3 台のホスト型 A-IDS を搭載した端末と，1 台のネットワーク型 A-IDS を搭載した端末，そして侵入用の端末から構成される．

A-IDS が端末を停止させる未知の致命的攻撃に対して有効かを検証する実験として，侵入用の端末から実験システム内の端末 C に対して telnet 接続を試み，その後，端末 C の LAN ケーブルを抜くことで，端末 C を停止状態にした．

実験の結果，端末 C を監視していた端末によって，端末 C が停止した原因と思われる telnet 接続要求のパケットがネットワーク型 A-IDS に報告され，以後，侵入用の端末からの接続は，ネットワーク型 A-IDS によって遮断された．また，ネットワーク型 A-IDS のルールを攻撃前に戻して再度，端末 B に telnet を試みても，ホスト型 A-IDS によって接続が拒否された．以上の実験から，A-IDS が未知の致命的攻撃に対して有効であることを確認した．

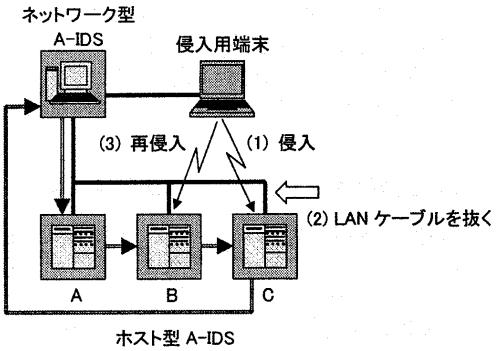


Fig. 7 Constitution of An Experiment System

## 7. おわりに

本論文では，システムへの不正侵入を自律的に検知・対応する A-IDS の提案を行っている．A-IDS では，システムを構成する端末が相互に監視している為，いかなる端末が攻撃を受けても，攻撃を受けていない別の端末で即座に対処を行うことが可能であり，従来の IDS の問題点のいくつかを解決可能である．特に，従来の IDS では管理者が手動で行っていた，判明した新たな侵入手口への対応を A-IDS では自動的に対応する為，IDS のルール更新の際に発生するタイムラグを大幅に短縮することが可能である．同時に，従来の IDS のもうひとつの問題点であった管理者への巨大な負担を削減することが可能である．

これにより，A-IDS を用いることによって，安価で強固なセキュリティシステムを構築することが可能である．

## 参考文献

(1) P. Parras, D. Schnackenberg, S. Staniford-Chen, M. Stillman, and F. Wu, "The Common Intrusion Detection Framework Architecture," J. Computer Security, 1998.

(2) N. Kato, H. Nitou, K. Ohta, G. Masfield, and Y. Nemoto, "A Real-Time Intrusion Detection System(IDS) for Large Scale Networks and Its Evaluations," IEICE Trans. On Communication, Vol.E82-B, No.11, pp.1817-1825, Nov 1999

(3) 浅香，女部田，井上，岡澤士，後藤，"不正侵入の痕跡と判別分析によるリモートアタックの検出法"，電子情報通信学会論文誌 B, Vol. J85-B No.1 pp.60-74 2002.

(4) 武井，太田，加藤，根元，"トラヒックパターンを用いた不正アクセス検出及び追跡方式"，電子情報通信学会論文誌 B, Vol.J84-B No.8 pp.1464-1473 2001.

(5) Mori, K. et al., "Autonomous Decentralized Software Structure and its Application," IEEE Proc. Fall Joint Computer Conference, pp. 1056-1062(1986).

(6) 河野，"自律分散システム，" 情報処理学会論文誌，情報処理，Vol.36, No.11, pp. 1054-1061(1995).

(7) Smith, R. G., "The contract net protocol: high-level communication and control in a distributed problem solver," IEEE Tran. Comput, C-29, No.12, pp. 1104-1113 1980.