高信頼性・高安全性を有する ネットワーク共生環境の構築技術の創出

菊野 亨
大阪大学大学院情報科学研究科
〒 565–0871 吹田市山田丘 1–5
kikuno@ist.osaka-u.ac.jp

井上 克郎
大阪大学大学院情報科学研究科
〒 565–8531 豊中市待兼山町 1–3
inoue@ist.osaka-u.ac.jp

藤原 融
大阪大学大学院情報科学研究科
〒 565–0871 吹田市山田丘 1–5
fujiwara@ist.osaka-u.ac.jp

増澤 利光
大阪大学大学院情報科学研究科
〒 565–8531 豊中市待兼山町 1–3
masuzawa@ist.osaka-u.ac.jp

1 はじめに

本テーマでは，ネットワーク共生環境を，安心・信頼のおける真に豊かな情報社会の基盤として実現することを目的とし，その高信頼性・高安全性を達成する技術について研究を行った．従来の研究分野による分類に基づけば，ソフトウェア工学，分散システム工学，ディペンダビリティ工学，セキュリティ工学を主軸とする研究である．これらの研究分野は，情報システムの高信頼化・高安全化に不可欠であり，本テーマは COE プログラムにおける他テーマに対し，基盤となるべき要素技術の提供を目的とする領域横断的なテーマとして位置づけることができる．

本テーマでは，主として，以下のサブテーマに取り組んできた．また，それぞれのサブテーマに留まらず，それらの総合分野において多様な研究を推進してきた．

1. 高信頼・高安全な情報システムを実現するためには，その基盤たるソフトウェアの安定性・信頼性が不可欠である．そこで，ソフトウェアの効果的な設計・運用・管理を可能とするソフトウェア工学の確立を目指す．
2. 情報システムは，通信技術を基盤とした分散システムの形態を取ることになる．そこで，分散環境におけるプロセス協調の実現，あるいは，障害や分散環境の動的な変化への自律的適応性を実現するために，分散システム工学，ディペンダビリティ工学を基盤とする効果的な解法の提案を目指す．
3. 情報システムにおけるデータの漏洩や攻撃などに対処し，高度なセキュリティを確保することは，もはや普遍的といってよい課題である．そこで，これらを実現する系統的な方法論としてのセキュリティ工学の確立を目指す．

さらに本テーマでは，生物共生ネットワークの生成過程の研究で得られた生物学上の知見の，高信頼・高安全な情報システムの基盤技術への適用を模索した．

以下では，本研究プロジェクトの全期間を通じて，各サブテーマごとに得られた主な研究成果について説明する．

2 高信頼・高安全ソフトウェアの設計・運用・管理

2.1 ソフトウェア分析に基づく高信頼・高安全化手法

ソフトウェアの分析や信頼性の向上のための種々の技術を検討，評価を行なってきた．主として以下のテーマに取り組んだ．

- プログラム解析による信頼性，安全性の向上
- ソフトウェアシステム類似度メトリクス
- ソフトウェアシステムの自動分類
- ソフトウェア部品グラフのべき乗則の調査と部品検索への応用

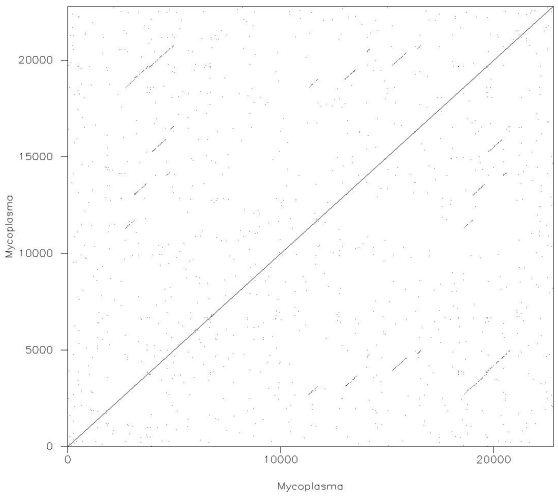


図 1: マイコプラズマの遺伝子配列中の同型部分（阪大松田研究室提供）

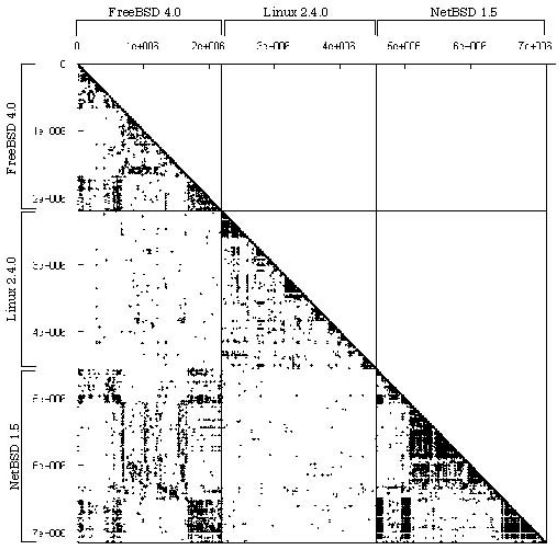


図 2: 3 種類の Unix 系 OS の中のコードクローン

以下に，各テーマに関して得られた成果について説明する．

「プログラム解析による信頼性，安全性の向上の研究」では，主にコードクローン解析の研究を行なった．コードクローンとは，プログラム中に現れる同形の部分テキストの対で，プログラムの一部をコピー・ペーストを行なってプログラムの作成を行なう場合に生じるものである [7]．一対の片方のコードクローンにバグがあると，他方も修正が必要になる，など，プログラムの保守性を低下させる大きな要因となっている．

本研究では，大規模なプログラム群に対して高速に含まれるコードクローンを検出するツール CCFinder を作成し，多くの対象に適用した [9]．

このコードクローン検出技術は，生物の遺伝子配列より，同型部分を検出するアルゴリズム（サフィックス木アルゴリズム）を用いており，その結果の表現法も非常に似ている．図 1 はマイコプラズマ菌の遺伝子配列の中の同型部分をスキャッタプロットで表現した物で，点の列が長いほど長い同型部分列を持っている事を示している（大阪大学大学院情報科学研究科松田研究室提供）．

図 2 には，3 つの Unix 系 OS(FreeBSD, NetBSD, Linux) のカーネル部分の同型部分（コードクローン）を点で示している．この結果は対角線を中心に対象なので，下部のみを表示している．

我々は，コードクローン分析技術を普及させるためにソフトウェア工学工房においてセミナー活動などを行なった（詳細は，教育プログラム「ソフトウェア工学工房」を参照）．この活動を通じ，多くの利用者を獲得する事ができた．

「ソフトウェアシステム類似度メトリクスの研究」では，すでに開発されたソフトウェアシステム同士の相異点を定量的に比較するためのメトリクスとそれを計測するためのツール SMMT に関する研究を行った．作成したツールを複数の類似した大規模ソフトウェアに適用することによって，ソフトウェアがどのように開発されてきたかを視覚的にわかりやすく表示させることが可能となった．

「ソフトウェアシステムの自動分類の研究」では，生物の種の分類作業と同様に，多種多様なソフトウェアに対して，それぞれの持つ特徴を解析し，自動分類する手法について研究を行った．

近年，インターネット上には膨大なソフトウェア開発プロジェクトが登録されているため，実際に希望するソフトウェアや類似ソフトウェアを検索するためには，ソフトウェアがうまく分類，整理されていなければならない．現存するリポジトリサービスでは，プロジェクトを登録する人がそのプロジェクトの分類を行う．しかし，このような手動分類では分類先となるカテゴリ集合を定義するのに労力がかかる．また，個々のソフトウェアがどのカテゴリに分類されるのか，分類を行うソフトウェア登録者に依存するため分類の一貫性に問題がある．

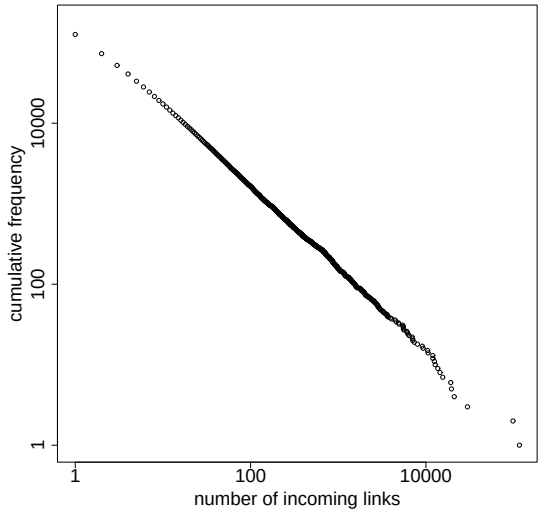


図 3: ソフトウェア部品集合の部品グラフの入力次数の分布

このような問題を解消するために，自動的にソフトウェアの分類を行う MUDABlue システムの提案を行った．MUDABlue は潜在的意味解析手法 (Latent Semantic Analysis: LSA) を用いて，カテゴリ集合の作成とソフトウェアの分類を自動的に行う．MUDABlue はソースコードのみに依存するため，管理者の入力は一切必要としない．LSA は単語間の意味的繋がりを統計的手法を用いることで抽出する．

「ソフトウェア部品グラフのべき乗則の調査と部品検索への応用の研究」においては，ソフトウェア部品群が持つ利用関係が，生物界に良く見られるべき乗則に従うかどうかを調査した．ここでは，大規模なソフトウェア集合のソフトウェア部品グラフ（Java の基礎的なライブラリである，JDK や，JDK を用いて構築した複数のシステムの集合）に対して調査を行なった．さらに，ソフトウェア部品検索への応用を考慮し，キーワード検索などにより取得した部品群からなる部分グラフの性質についても調査した．

その結果，図 3 のように，多数のソフトウェアを含む集合の入力次数の分布は，べき乗則に従うことがわかった [5]．また，キーワード検索によって得られた部分グラフに対しても，比較的少数の部品数で構成されるにもかかわらずべき乗則に従うことがわかった．また，その際の係数 a は，ほぼ 2 であり，多くの生物界のシステムで現れるべき乗則の係数とほぼ同じである．

このようにソフトウェアの分析や信頼性の研究に関し，生物界の種々の知見と通じる部分があることは興味深い．今後は，このような生物界の知見に基づき，ソフトウェアの特性やシステム開発の人間活動の性質を分析し，効率の良い開発作業に結び付く手法を探索する事が必要になろう．

2.2 ホームネットワークシステムにおける機器間でのサービス競合の検出

電力線通信等の技術の実用化に伴い，今後急速な普及が予想されるホームネットワークシステムを対象に，システム中の機器が提供する複数のサービスが互いに干渉することで誤動作を招く可能性を検出し，異種サービスの共生を信頼高く実現する方法について研究を行った [13]．

具体的には，まず，ホームネットワーク上の機器の動作を正確に記述できるよう，簡易なモデル化言語を定義した．この言語を利用することで，各機器の動作を表現したモデルを記述することが可能となる．一旦，形式的な各機器の動作記述が得られれば，計算機を用いてそれらを統合し，システム全体の動作を表現するモデルを生成することができる．このモデルを解析することで，意図しない機器間の干渉や不具合の検出が可能となる．モデルの解析には，モデル検査と呼ばれる，状態探索に基づく自動検証手法を応用している．実験の結果，最新のモデル検査技術を用いることで，極めて短時間（数秒程度）で検証が可能なことが分かった．

この研究は，当初，ホームネットワークを設計する際に行う，静的な検証を念頭に進めてきたものであるが，上記の通り，検証時間が非常に短いため，機器がホームネットワークに追加されるのを検知したネットワーク自体が，自律的に検証手続きを起動し検証を行うといった動的な用途への応用も可能である．

2.3 全ペアテストと生物学的状態探索の応用

ソフトウェアに潜在する不具合を，テスト工程において確実に検出する技術は，信頼性の高いソフトウェアの実現において，欠かすことができな

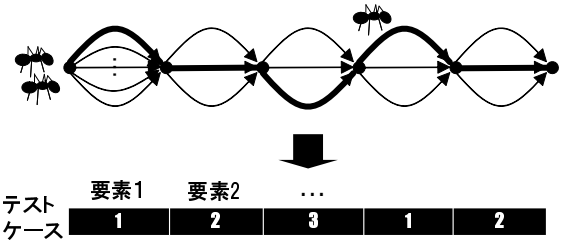


図 4: アントコロニーアルゴリズムによるテストケースの生成

い．全ペアテストは，そのような技術として，近年特に注目を集めているテスト手法である [1]．これは，ソフトウェアへの入力空間をすべてテストするのではなく，二つの次元（パラメータ）の値のペアすべてを，少なくとも一度テストするという手法であり，全数テストと比べ大幅にテストケース数が減らせ，かつ，高い不具合検出能力を有すものと認識されている．しかしながら，そのようなテストを少ないテストケース数で完了するためには，テストケースを適切に選択することが必要であり，これには計算機による支援が不可欠である．

そこで，Java プログラムに対する標準的なテストフレームワークである JUnit を用いて，全ペアテストを容易に実施することが可能なツールを開発した．このツールでは，テストケースを生成する際，遺伝アルゴリズム，あるいは，アントコロニーアルゴリズムという生物学的状態探索手法を用いることで，全ペアテストに必要なテストケース数の削減を行っている [20]（図 4）．今後は，広く用いられている統合開発環境である Eclipse に，開発したツールをプラグインとして組み入れることを予定している．

3　高信頼・高安全分散システム

3.1　エピデミック通信による高信頼マルチキャスト

疫病の伝染過程を模倣することで，高信頼なマルチキャストを実現するエピデミック通信について，更なる信頼性向上のための手法の開発を行った．マルチキャストは，ネットワーク上の特定のノード集合に対し，同一メッセージを配信する通信サービスである．複数のノードにデータの複製を保持させるレプリケーション技術は，分散システムの高信頼化の主要な技術であるが，マルチキャストはレプリケーションの実現に不可欠な通信サービスであり，その高性能化・高信頼化の重要性は言を待たない．

エピデミック通信では，各ノードが隣接ノードをランダムに選びメッセージを転送することで，マルチキャストを行う [3]．したがって，単一故障点となるノードが存在せず，また，同じメッセージが冗長に転送されるため，ノードや通信の障害に対し高い耐性が実現できる．これは，一旦流行が広まった疫病の伝染や噂の拡散の阻止が極めて難しいという現象に対応している．

本研究では，エピデミック通信の信頼性を更に高めるため，幾つかの最適化手法を開発した．まず，メッセージ伝搬状況が思わしくない場合，各ノードが自律的にメッセージの再送を行うという適応的手法を導入した [25]．この判断の基準についても，隣接ノードの状況を観測することで，適切に行う手法を考案した．様々なトポロジーのネットワークを対象にシミュレーション実験を行った結果，殆どの場合で，これらの提案手法によって，メッセージ受信に失敗するノード数を大幅に減少できることが分かった [17].

3.2　生態系の単一個体群モデルに基づく資源数制御

大規模なネットワーク環境で，メモリや通信帯域などのネットワーク資源を有効に利用してタスクを効率的に実行するには，モバイルエージェントやファイル・レプリカの数を，ネットワークの規模に応じて適切に設定することが重要である．例えば，モバイルエージェントを利用した分散システムでは，ネットワーク中のエージェント数が多いほど処理に要する時間が減少するが，システム資源（計算資源，通信帯域など）の消費は増加する．一方，ネットワーク環境は本質的にダイナミクスを有するものであり，このエージェントやファイル・レプリカ数制御には，ネットワーク規模の変化に対する適応性を有することが要求されている．

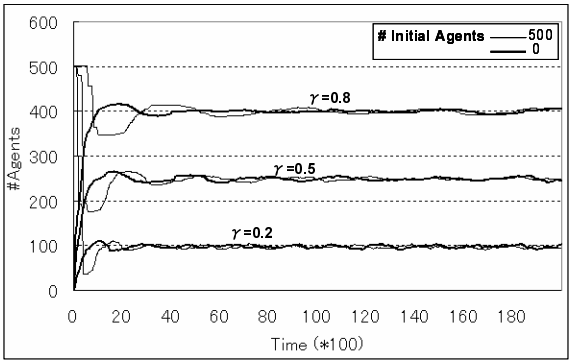
生態系では，環境における単一種個体群の個体数が，環境から供給される食物量に応じて安定するという単一種個体群モデルが知られている [4].

本研究では，この単一種個体群モデルを適用することによって，ネットワーク中のモバイルエージェントやファイル・レプリカの数を，ネットワークのノード数に対して一定の割合に保つ手法を提案した [21, 22]．また，提案手法が，ノード数に対してレプリカ数を所定の比に保つことを，ランダムネットワークやスケールフリーネットワークなどのさまざまな種類のネットワークに対するシミュレーション実験によって確認した（図 5(a)）．さらに，ネットワークの規模が動的に変化する環境において，ネットワーク規模の変化に応じて，レプリカの数を適応的に制御できることをシミュレーション実験によって示した（図 5(b)）．

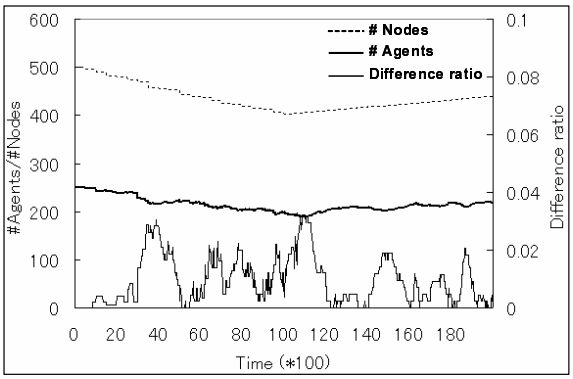
3.3 ノードの自律動作によるオーバーレイネットワークのトポロジーマッチング

Peer-To-Peer (P2P) システムによって用いられるオーバーレイネットワークでは，下部の物理ネットワークの構造と独立して自由なトポロジーを設定することができる．このことは，P2P システムに高い柔軟性をもたらすと同時に，物理ネットワークとオーバレイネットワークとのトポロジー間に大きな不一致が生じた場合に，過度の通信負荷や，信頼性の低下といった問題を引き起こす原因となる [18].

そこで本研究では，この不一致を解消し，効率的なオーバーレイネットワークを動的に構築するための手法を開発した [6]．提案手法では，各ノードは物理ネットワーク上の距離を反映した隣接ノード間の通信コストを基準に，局所的なリンクの繋ぎ換えを繰り返し行う．このような各ノードの局所的な動作の結果，オーバーレイネットワークのトポロジーを，物理ネットワークのそれに近づけ，ネットワーク全体の負荷を軽減することが可能となる．同時に提案手法は，各ノードが保持するリンク数も配慮し，ネットワーク全体のリンクの総数は一定に保ちながら，各ノードが最終的にできるだけ同程度のリンクを有すように動作する．このため，得られるオーバーレイネットワークは，ノード故障の際にネットワーク分割を起こす確率が極めて低くなる．負荷の軽減と高信頼化という提案法のこれらの利点は，シミュレーション実験によっても確認することができた.



(a) 静的ネットワーク



(b) 動的ネットワーク

図 5: スケールフリーネットワークにおけるモバイルエージェント数制御

3.4 高度な適応性を有する P2P 情報検索方式

Peer-To-Peer (P2P) システムでは，ネットワーク中に分散しているファイル等の資源から，必要とする資源をいかにして探索するかは重要な問題の一つである．これまでフラッディングに基づく手法や分散ハッシュ表に基づく手法など，さまざまな手法が研究されているが，それら手法にはスケーラビリティの欠如や，計算機の参加離脱といった P2P ネットワークの動的変化に弱いなどいった問題が存在する．これらの問題を解決する手法としてランダム性に基づいた手法がいくつか提案されており，たとえば文献 [14] などが知られている．

膨大な端末群で構成される P2P ネットワークでの情報検索において，端末の参加離脱が激しい場合においても正常に動作し，しかも時々刻々変化

する情報の検索頻度などに対し，パフォーマンスの最適化を自動的に行う自己適応型の手法の確立が本研究の目的である．

文献 [14] で提案されている方式は激しく端末の参加離脱に頑強ではあるが，自己適応性を有していない事が知られている．そこで本研究では，参加離脱への頑強さを保ったまま，情報の検索頻度に応じた通信メッセージ量を自動的に最適化する手法を提案し，シミュレーション実験によりその有効性を示した [26].

また，ランダムウォークに基づいた検索手法に対しブルームフィルタ (bloom filter) を適応的に使用する手法を提案し，検索効率の大幅な向上を行った [23]．提案手法では各端末が所有する情報オブジェクト（のハッシュ値）の集合をブルームフィルタにより圧縮表現し，それを周囲の端末に配布することで所有情報オブジェクトを通知する．ブルームフィルタはその性質上，オブジェクトの有無の検索を誤る場合がある．ブルームフィルタの作成方法を，ブルームフィルタを配布する距離と情報検索頻度に関連づけて選択することにより，誤り確率を大幅に下げるとともに，通信量も大きく削減可能であることをシミュレーション実験により示した．

3.5 自己安定分散システム

自己安定分散システム [2] は，計算機の一時的な故障や動的変化のためにネットワークがどのような状況に陥っても，十分に長い間新たな故障や動的変化が発生しなければ，自動的に正常動作に復帰することを保証する．つまり，自己安定分散システムは，一時的な故障や動的変化に対する高度な適応性を有する．

しかし，自己安定分散システムが正常な状況に復帰するためには，十分に長い間新たな故障や動的変化が発生せず，すべての計算機が正しく動作することが必要である．しかし，大規模分散システムにおいては，故障や動的変化が頻繁に発生する状況は避け難く，十分に長い間，すべての計算機が正しく動作するという仮定は受け容れ難い．そこで，間欠的に生じる故障や動的変化，あるいは，永久的な故障にかかわらず，正常な状況に復帰できる自己安定システムを実現することが重要である．

そこで本研究では，自己安定分散システムの故障や動的変化に対する高度な頑健性として，安全収束という新たな概念を提案した [8]．これは，故障や動的変化が生じたときに，迅速に安全な状況に復帰し，その後は安全性を保ちながら自己最適化を行うというものである．また文献 [8] では，アドホックネットワークのクラスタリングに重要な役割を果たす支配集合の選出に，この概念を適用することに成功した．

また，間欠的な故障や動的変化が頻繁に発生する分散システムにおいて，故障や動的変化がシステムに与える影響を定量化することにより，自己安定システムが正常な状況に復帰するのに要する時間と故障や動的変化の頻度の関係を解明する手法を提案した [10, 15]．さらに，永久故障として，ビザンチン故障が存在する分散システムにおける自己安定システムの実現法について考察し，永久ビザンチン故障に対する故障耐性を有する自己安定分散システムを設計した [11, 12, 19].

4 高信頼性・高安全性を実現する通信技術

ディジタルコンテンツ流通のための高信頼・高安全な通信システムの実現やそれに関連する基礎研究として，様々なコンテンツ配信サービスのためのプロトコルやその要素技術，インデックス付きで管理されているデータのアクセス方式，推論による情報漏えいへの対策，誤り訂正符号に関する研究を行ってきた．

以下では，これらのうちで代表的な成果について報告する．

4.1 ポリシーの自己更新が可能なアクセス制御システム

本研究において，アクセス制御の対象となるコンテンツは，XML コンテンツ（コンテンツ本体とその作者等の属性情報を含む XML 文書）である．コンテンツの配信環境としては，XML コンテンツに対するアクセス制御ポリシーを保有するブラウザが存在し，各ユーザが自由に XML コンテンツを作成・配信できる P2P 型ネットワークを想定す

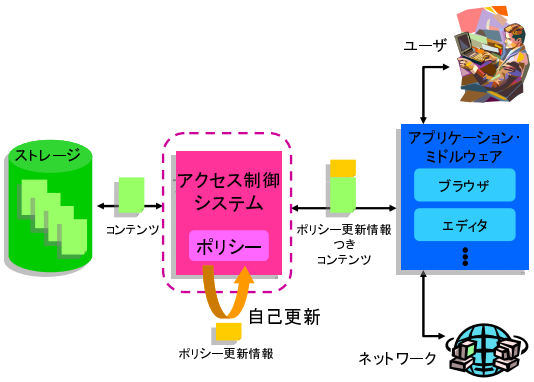


図 6: ポリシーの自己更新が可能なアクセス制御システム

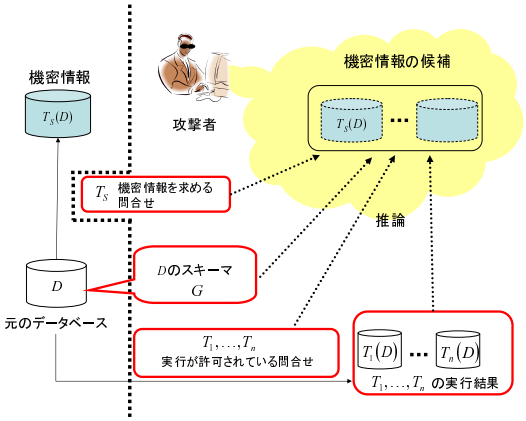


図 7: 対象とする推論攻撃の概要

る．ただし，違法コンテンツの氾濫などの無秩序状態を避けるため，ネットワークの監視機関が存在し，各ユーザに対してアクセス制御ポリシーを配布するものとする．このような配信環境において，将来起こり得るあらゆる状況を想定し，アクセス制御ポリシーをあらかじめ記述しておくことは現実的ではない．

そこで本研究では，監視機関によりポリシーの更新情報が XML コンテンツに埋め込まれ，その XML コンテンツをブラウザに読み込むときにポリシーが更新されるシステムを提案した．ただし，更新情報と既存のポリシーの安全性は確保されているものとする．これにより，各ユーザが保有するアクセス制御ポリシーの管理を自動化することができ，ポリシー管理の煩雑さを解消することができる．次に，提案システムの実現を行った．XML 文書に対するポリシー記述言語として OASIS で標準化された XACML を採用し，標準的な XACML プロセッサのひとつを搭載した PC 上に提案システムを実現した．また，アクセスを読み出しだけに制限した提案システムを，XSLT プロセッサのみを搭載した PC 上に実現した．自己更新処理にあたっては，更新情報に含まれる更新ポリシーと，既存の XACML ポリシーをどのように結合すべきかを検討した．

上述の配信環境において，監視機関が違法 XML コンテンツを発見し，そのコンテンツへのアクセス否認ポリシーを埋め込んだ XML コンテンツをネットワーク上へと流している状況を考える．このような状況において，ポリシー更新情報がネットワーク上に広まる速度をシミュレーションにより評価した．また，実現したそれぞれのシステムが，この XML コンテンツを読み込むことにより，ポリシーの自己更新を行い，更新後のアクセス制御ポリシーが意図した通りのアクセス判定を行うことを確認した．これらの成果の一部は，Bio-ADIT 2006 のポスターセッションで発表した．

4.2 XML データベースへの推論攻撃に対する安全性の定式化と検証

機密情報が格納されているデータベースシステムにおいて，セキュリティ面での管理が必ずしも正確に行われていないことが問題となっている．特に，機密情報への直接のアクセスを禁止していても，アクセスを許可されている情報や実行を許可された問合せの結果，ドメイン知識などを基に，本来権限の無いユーザがその機密情報を推論できてしまう場合がある．そのような推論を行うことを推論攻撃と呼ぶ．推論攻撃によりどのような情報が得られるかは，一般に自明ではない．したがって，高安全性をもつデータベースシステムを構築・運用するために，データベース管理者は，機密情報に対して推論攻撃が成功する可能性をあらかじめ把握できることが重要である．

本研究では，推論攻撃に対する安全性の 1 つの定式化として，「推論攻撃により機密情報の値の候補が 1 つに絞り込まれる可能性 (特定可能性) がないこと」を採用した．そして，ある前提条件のもとで，特定可能性を検証する決定性多項式時間アルゴリズムを提案した．このアルゴリズムは，まず，問い合わせとその結果から，逆型推論を用い

てもとのデータベースの候補集合を求める．さらに，型推論を用いて機密情報の値の候補集合を求める．最後に，その候補集合が 1 要素からなるかどうかを判定する．この成果を論文 [24] としてまとめた．

本研究ではさらに，特定可能性による定式化では区別できない以下のような実用上両極端な状況を区別できるよう，新たな定式化を行った．

- 機密情報の値の候補が数個にしかならず，特定されないまでも推論攻撃の効果が非常に高い．
- 機密情報の値の候補の個数が非常に多く，攻撃の効果がない，あるいは非常に低い．

また，より実用的な検証アルゴリズム開発を目指して，対象とする問合せクラスの拡張を行っている．今年度内にこれらの成果についての学会発表を行う予定である．

4.3 秘匿性と一貫性を保証する通信効率の良いデータアクセス方式

インデックス付きでデータが管理されているデータベースを考える．データベースサーバに対して，得たいデータのインデックスを送り，それに対する返答から所望のデータを計算する状況を考える．安全性に関する要求として，検索インデックスの秘匿，データベースの秘匿，結果の一貫性検証の三つがある．検索インデックスの秘匿とは，アクセスしようとするデータのインデックスをサーバから秘匿できることである．データベースの秘匿とは，サーバがもつデータベースに関して返答から分かることが所望のデータだけであることである．結果の一貫性検証とは，得られた結果がインデックスに対応したものであることを検索者が検証できることである．すなわち，データベースが更新されない限り，同じ問い合わせ（インデックス）について同じデータが得られ，そのことを検証できることを意味する．

これまでに，これらの安全性に関する要求を全て満たすデータアクセス方式が提案されている．しかし，従来方式ではデータ検索時の通信効率は非常に良いが，データベース更新時の通信量がデータベースのサイズに比例してしまい，通信効率が悪い．

そこで，これらの安全性に関する要求を全て満たし，データ検索時及びデータベース更新時の通信量が共にデータベースのサイズに比例しないデータ検索方式を提案した [16]．提案方式では，暗号技術として Merkle 木と呼ばれるハッシュ木，コミットメント方式，紛失通信を利用している．Merkle 木を利用することで，データベース更新時の通信量を $O(1)$ とすることができた．また，データ検索時の通信量である問い合わせと返答の大きさは，データベースのサイズ N に対して $O((\log N)^2)$ である．このように，提案方式はデータベースの更新が頻繁に起こる場合に特に効率が良い．利用する暗号技術が安全であるという仮定のもとで，提案方式が安全性に関する要求を全て満たすことを証明した．この成果を論文 [16] としてまとめた．

4.4 誤り訂正符号の厳密な性能評価

誤り訂正符号の正確な性能評価を行うことは，高信頼なシステムを構成する技術として重要な課題である．そのため，記号位置置換やトレリス構造を活用して，局所重み分布の計算法の計算量削減を行った．局所重み分布とは，零語に隣接する符号語に関する重み分布である．記号位置置換不変性を用いて，局所重み分布を計算する方法や局所重み分布の計算に有用な性質等を導出した．これらの成果は，論文としてまとめ，IEEE の論文誌に掲載された [27]．

さらに，トレリス構造，及びバイナリーシフトと呼ばれるアフィン変換の部分クラスを用いることにより局所重み分布の計算法の改良を図った．これにより，符号長 256，3 次のリード・マラー符号について計算時間を，従来法（我々が提案している方法）の 1/256 に削減することに成功し，その局所重み分布を求めた．この成果を論文 [28] としてまとめた．

また，局所重み分布を用いることにより，復号誤り率の下界，上界の改善を行った．復号誤り率について，単純な和集合下界，和集合上界においては，重み分布を局所重み分布に置き換えることによって，より精度の高い結果が得られることが知られている．しかし，単純な和集合下界，和集合上界は，もともとあまりよい下界・上界ではない．そこで，同じ考え方に基づくが，より精度の高い

下界，上界が最近提案されている．例えば，加法的白色ガウス雑音 (AWGN) 通信路における復号誤り率の Seguin 下界，Poltyrev 上界等である． これらの下界，上界に対しても局所重み分布を用いることが可能であることを示し，実際に局所重み分布を用いた下界や上界の評価をいくつかの線形ブロック符号を対象に行った．その結果，BCH 符号，リード・マラー符号，ゴーレイ符号等で復号誤り率の下界，上界が改善されることを確認した．例えば，AWGN 通信路の SN 比が 0dB のとき，$(31, 26)$ ハミング符号の復号誤り率の上界は 3.4×10^{-1} であり，下界は 9.4×10^{-4} から 1.1×10^{-2} へ改善された．

5 おわりに

本研究テーマでは，ネットワーク共生環境を，安心・信頼のおける真に豊かな情報社会の基盤として実現することを目的とし，その高信頼化・高安全化のための技術について研究を行った．本研究プロジェクトの全期間を通じて，各サブテーマに関してさまざまな基幹技術の開発を進めることができ，高信頼性・高安全性を有するネットワーク共生環境の構築技術の創出に貢献できたものと考えている．

本研究テーマの今後の展望として，ポストユビキタス時代のアンビエント情報社会の実現に向けて，高信頼性・高安全性を有する情報システム構築のための研究に取り組むことが重要である．本研究の各サブテーマでは，具体的には，以下の展望が考えられる．

1. ソフトウェアの分析や信頼性の研究を推進する事は，アンビエント情報社会を実現するためには必須のものである．アンビエント情報社会では，多数の端末やネットワーク機器が有機的に連携し，その機能を発揮するが，個々の機器のソフトウェアの信頼性を確保する事は重要なテーマである．個々のソフトウェアシステムが，予定通りであるかどうか，静的，動的に検証する必要がある．また，アンビエント情報社会を実現するためには，非常に多種の機器のソフトウェア開発が必須であるが，個別にソフトウェア開発を行なう事は，手間の増大を招き，経済的に困難である．ソフトウェアプロダクトラインの考えを導入し，より効率なソフトウェア群の開発を行なう技術開発が必須となる．
2. 稠密な分散環境におけるプロセス協調の実現，あるいは，障害や分散環境の動的な変化への自律的適応性を実現することは，アンビエント情報社会を実現するためには必須のものである．アンビエント情報社会では，多数の端末やネットワーク機器が有機的に連携して動作するが，高信頼・高安全な情報システムを構築するための連携動作について，その基盤技術を構築することが重要な課題である．
3. 情報システムにおけるデータの漏洩や攻撃などに対処し，高度なセキュリティを確保することアンビエント情報社会を実現するためには必須のものである．これまでの安全性（セキュリティ）に関する研究では，匿名性など，個人情報をなるべく出さずにサービスを実現することが重要な目標の一つであったが，アンビエントネットワーク社会では必然的に個人に関する情報を出さざるを得ず，それをいかに守るかが重要な課題となる．

参考文献

[1] Copeland, L., “A Practitioner’s Guide to Software Test Design,” Artech House (Dec. 2003).

[2] Dolev, S., “Self-Stabilization,” The MIT Press (2000).

[3] Eugster, P. T., Guerraoui, R., Kermarrec, A.-M., Massoulié, L., “Epidemic Information Dissemination in Distributed Systems,” IEEE Computer, Vol. 37, No. 5, pp. 60–67 (May 2004).

[4] Haberman, R., “Mathematical Model: Population Dynamics,” Prentice Hall (1977).

[5] 市井 誠, 松下 誠, 井上克郎, “ソフトウェア部品グラフの次数分布におけるべき乗則の調査,” ソフトウェア信頼性研究会第 3 回ワークショップ論文集, pp. 87–96 (2006 年 7 月).

[6] Ikeda, S., Tsuchiya, T., and Kikuno, T., “A Decentralized Scheme for Network-Aware Reliable Overlay Construction,” Proc. of Int’l Conf. on Information Networking 2006 (ICOIN 2006), pp. 955–964 (Jan. 2006).

[7] 井上克郎, 神谷年洋, 楠本真二, “コードクローン検出法,” コンピュータソフトウェア, Vol. 18, No. 5, pp. 529–536 (2001 年 9 月).

[8] Kakugawa, H., and Masuzawa, T., "A Self-stabilizing Minimal Dominating Set Algorithm with Safe Convergence," Proc. of Int'l Workshop on Advances in Parallel and Distributed Computational Models (APDCM 2006), 103, 8 pages (Apr. 2006).

[9] Kamiya, T., Kusumoto, S., and Inoue, K., "CCFinder: A Multilinguistic Token-Based Code Clone Detection System for Large Scale Source Code," IEEE Transaction on Software Engineering, Vol. 28, No. 7, pp. 654–670 (July 2002).

[10] Masuzawa, T., and Kakugawa, H., "Self-stabilization in spite of Frequent Changes of Networks: Case Study of Mutual Exclusion on Dynamic Rings," Proc. of Int'l Symposium on Self Stabilizing Systems (SSS 2005), pp. 183–197 (Oct. 2005).

[11] Masuzawa, T., and Tixeuil. S., "A Self-Stabilizing Link-Coloring Protocol Resilient to Unbounded Byzantine Faults in Arbitrary Networks," Proc. of Int'l Conf. on Principles of Distributed Systems (OPODIS 2005), pp. 283–298 (Dec. 2005).

[12] Masuzawa, T., and Tixeuil, S., "Bounding the Impact of Unbounded Attacks in Stabilization," Proc. of Int'l Symposium on Stabilization, Safety and Security of Distributed Systems (SSS 2006), pp. 440–453 (Nov. 2006).

[13] 松尾尚文, 土屋達弘, 菊野 亨, "Detecting Injected Safety Errors in the Chandra-Toueg Algorithm with Model Checking," 第 3 回システム検証の科学技術シンポジウム (Oct. 2006).

[14] Miura, K., Tagawa, T., and Kakugawa, H., "A Quorum-Based Protocol for Searching Objects in Peer-to-peer Networks," IEEE Transactions on Parallel and Distributed Systems, Vol. 17, No. 1, pp. 25–37, (Jan. 2006).

[15] Nakaminami, Y., Kakugawa, H., and Masuzawa T., "An Advanced Performance Analysis of Self-stabilizing Protocols: Stabilization Time with Transient Faults during Convergence," Proc. of Int'l Workshop on Advances in Parallel and Distributed Computational Models (APDCM 2006), 106, 8 pages (Apr. 2006).

[16] Nakayama, S., Yoshida, M., Okamura, S., and Fujiwara, T., "A Private and Consistent Data Retrieval Scheme with Log-Squared Communication," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E90-A, No. 1 (Jan. 2007, to appear).

[17] 奥山拓矢, 土屋達弘, 菊野 亨, "ゴシップ型ブロードキャストの高信頼化のための適応的再送手法の提案," 電子情報通信学会技術研究報告, Vol. 106, No. 198 (2006 年 8 月).

[18] Ren, S., Guo, L., Jiang, S., and Zhang, X., "SAT-Match: A Self-Adaptive Topology Matching Method to Achieve Low Lookup Latency in Structured P2P Overlay Networks," Proc. of 18th Int'l Parallel and Distributed Processing Symposium (IPDPS 2004), pp. 83–91, 2004.

[19] Sakurai, Y., Ooshita, F., and Masuzawa, T., "A Self-stabilizing Link-coloring Protocol in Tree Networks with Permanent Byzantine Faults," Journal of Aerospace Computing, Information, and Communication, Vol. 3, No. 8, pp.420–436 (Aug. 2006).

[20] Shiba, T., Tsuchiya, T., and Kikuno, T., "Using Artificial Life Techniques to Generate Test Cases for Combinatorial Testing," Proc. of Annual Int'l Computer Software and Applications Conf. (COMPSAC 2004), pp. 72–77 (Sept. 2004).

[21] Suzuki, T., Izumi, T., Ooshita, F., Kakugawa, H., and Masuzawa, T., "Bio-inspired Replica Density Control in Dynamic Networks," Proc. of Int'l Workshop on Biologically Inspired Approaches to Advanced Information Technology (Bio-ADIT 2006), pp. 281–293 (Jan. 2006).

[22] Suzuki, T., Izumi, T., Ooshita, F., and Masuzawa, T., "Self-adaptive Mobile Agent Population Control in Dynamic Networks Based on the Single Species Population Model," IEICE Transactions on Information and Systems, Vol. E90-D, No. 1 (Jan. 2007, to appear).

[23] 高橋佑典, 泉 泰介, 増澤利光, "P2P ネットワークにおける決定性減衰型ブルームフィルタの提案と検索効率の評価," 電子情報通信学会技術研究報告 (NS2006-133), 奨励講演, Vol. 106, No. 355, pp. 55–60 (2006 年 11 月).

[24] 高須賀史和, 橋本健二, 石原靖哲, 藤原 融, "XML データベースへの推論攻撃による機密情報特定可能性の形式化とある前提条件のもとでの特定可能性検証法の提案," 日本データベース学会 Letters, Vol. 5, No. 2, pp. 21–24 (2006 年 9 月).

[25] Tsuchiya, T., Ikeda, S., and Kikuno, T., "Counter-Based Reliability Optimization for Gossip-Based Broadcasting," Computer Communications, Vol. 29, No. 9, pp. 1516–1521 (May 2006).

[26] Wu, Y., Izumi, T., Ooshita, F., Kakugawa, H., and Masuzawa, T., "An Adaptive Randomized Searching Protocol in Peer-to-peer Systems," Proc. of ACM Symposium on Applied Computing (SAC 2007), (Mar. 2007, to appear).

[27] Yasunaga, K., and Fujiwara, T., "Determination of the Local Weight Distribution of Binary Linear Block Codes," IEEE Transactions on Information Theory, Vol. 52, No. 10, pp. 4444–4454 (Oct. 2006).

[28] Yasunaga, K., Fujiwara, T., and Kasami, T., "Local Weight Distribution of the (256, 93) Third- Order Binary Reed-Muller Code," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E90-A, (2007, to appear).