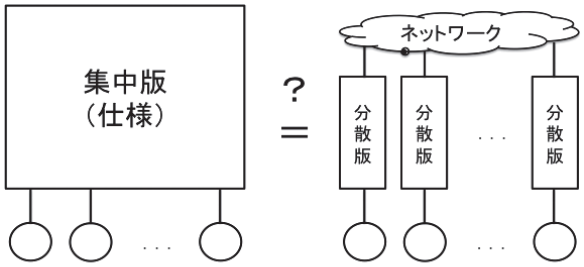
K05 形式手法に基づくシステム検証技術

情報科学部・情報科学科・教授・河辺　義信
kawabe@aitech.ac.jp

キーワード　形式手法、システム検証、ソフトウェア、セキュリティ検証

概要

コンピュータシステムの設計の正しさを保証する技術として、ソフトウェア工学などで「形式手法」が盛んに研究されている。これは、オートマトンなどを用いてシステムを仕様記述し、正しさをフォーマルに検証する手法である。たとえば、実装と仕様の同等性を保証するために、形式手法のテクニックが用いられる。



「仕様＝実装」となっているか？

我々の研究室では、形式手法によるシステム検証を行っている。具体的には、形式的仕様記述言語を用いて仕様を記述し、定理証明器で正しさを検証する。情報セキュリティへの形式手法の適用に力を入れており、これまでにプライバシやトラストに関する形式検証法を開発している。

セールスポイント

1．通信システム・分散システムの正しさを論理的に保証することができる。
2．大規模システムの正しさを、計算機で半自動的に検証できる。
3．不具合発生が致命的となるミッションクリティカルシステムの検証に有効である。

企業等での活用例、今後の展望等

1．航空・医療・鉄道向け等のミッションクリティカルシステムの正しさを設計時に検証できます。
2．セキュリティ安全基準（ISO/IEC 29128 や 15408）を満たすシステムの開発に役立ちます。

SDGs、ゼロカーボンへの寄与

経済発展や福祉を支えるインフラとなるコンピュータシステム（電子商取引・電子投票・医療システムなど）を、強靭で高信頼なものにする点で寄与します。
（SDGs目標　9．1 番）

参考資料

・ Probabilistic anomymity via coalgebraic simulations, Theoretical Computer Science, volume 411, No. 22-24, pp. 2239-2259, 2010.
・ On Trust Confusional, Trust Ignorant, and Trust Transitions, Trust Management XIII, pp. 178-195, 2019.