平成17年度 情報工学コース卒業研究報告要旨

宮尾・河口 研究室	氏　　名	飯 塚 裕 一
卒業研究題目	ソフトウェアの安全・安心な ネットワークインストール手法	

近年，家電製品・携帯電話・自家用車など様々な機器に組み込みシステムが用いられている．現状ではこれらの組み込みシステムで利用されるソフトウェアの多くは，機器の動作中に変更されることはない．しかし，柔軟性の向上等の点からネットワーク内の端末間を自由に移動し，システムに自動的にインストールされる移動ソフトウェアの利用が今後増えると考えられる．しかし，移動ソフトウェアには利用者が意図しない移動ソフトウェアがインストールされてしまうという問題がある．故に，利用者が安心してシステムを利用するためには，移動ソフトウェアのインストール時に認証が必要である．

既存の動的インストール可能なシステムで認証手法を持つものとして Java アプレットや i アプリがある．これらのシステムにおいてはソフトウェアを信頼できる・信頼できないという単純な区別でしか動作制限ルールを決められない．例えば，信頼できないソフトが個人情報・ネットワークにアクセスするのは許可しないが，自分で作成したバックアップソフトが個人情報にのみアクセスするのは許可し，ベンダーによって公認されたソフトウェアは個人情報・ネットワークにアクセスするのは許可する，といった複雑な制限ルールを決めることは不可能である．

本研究では，組み込みシステムおよび移動ソフトウェアが相互に情報提供することにより，利用者の要求に応じた細粒度のインストール制限を実現するセキュリティモデルを提案する．そのために，組み込みシステムにどのような移動ソフトウェアのインストールを許可するかを表すポリシ，及び移動ソフトウェアの動作内容を表すマニフェストを定義する．そして，移動ソフトウェアをインストールする際に，マニフェストの動作内容とポリシの許容動作を照合する方法を提案する．照合は，マニフェストに記述された動作内容がポリシに記述された許容動作を超えていないかどうかを全項目について判断する．その際，システムに組み込まれた証明書とマニフェストの電子署名の照合も行われる．また，一度照合を行ったソフトウェアには次回の認証を簡略化可能となるトークンと呼ばれるデータを発行する．

提案セキュリティモデルにより，利用者にとって安全に移動ソフトウェアをインストールするための柔軟なルールを組み込みシステムに適用できる．例えばテレビの場合，製造会社が認定した公式ベンダーのソフトウェアのみ EPG（電子番組表）データを書き換え可能にする．また，署名付の出所が明確であるソフトウェアには現在閲覧中の番組情報に限って他のシステムに持ち出すことを許可する一方，署名のないソフトウェアは EPG データの読み取りのみ可能とし現在閲覧中の番組情報を持ち出すことは許可しないように利用者がルールを設定可能である．このように，利用者の要求に応じた柔軟なセキュリティを構築可能であり，製造会社やベンダ等の保障による安心感と同時に，ユーザによる複雑な応用設定を可能にしている．

今後の課題としては，マニフェストやポリシの記述の汎用性を高めることが挙げられる．異なる機器間で汎用的な項目として定義できない動作も多数存在するため，複雑な動作制限を与える際にマニフェストやポリシの記述が煩雑になる．そのため，さらに定義方法を工夫してより容易に記述する方法を検討する必要がある．