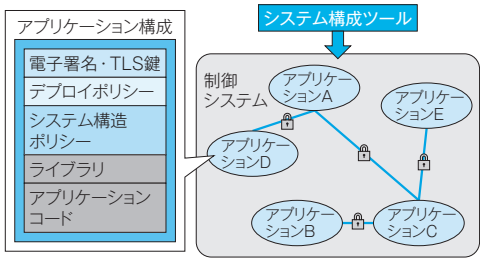
産業制御システムのセキュリティ技術

平田敏樹 Toshiki Hirata

キーワード アプリケーションセキュリティ，静的解析，電子署名，通信制限，通信秘匿

概　要



開発したセキュリティ技術の概要

社会的な重要性から，産業制御システムはインターネットに接続されずにローカルネットワークで運用されることが多かった。近年のクラウドコンピューティング技術の発展で，産業制御システムをインターネットに接続し，外部システムと連携することによって，様々な付加価値を得ることができるようになった。外部ネットワークと産業制御システムを接続することで，新たなセキュリティリスクが生み出されることになり，産業制御システムへのセキュリティ対策の重要性は高まっている。

本技術は，制御システムソフトウェアやシステム構成の改ざんに対応するために開発したセキュリティ技術である。制御システムを構成するアプリケーションの完全性と通信の機密性を保証し，不正使用や意図しない誤使用からシステムを防御する。

1　まえがき

産業制御システムのセキュリティインシデントは，年々増加している。2010年に海外で発生したスタックスネットは，産業制御システムに対する標的型攻撃として注目を集めた。

クラウドコンピューティング技術の発展で，近年の産業制御システムはインターネットに接続し，外部システムと連携して稼働する事例が増えつつある。また産業制御システムは，汎用のOS・ソフトウェア・プロトコルを使用して構築されるようになった。これらの点から，産業制御システムへのセキュリティ対策の重要性は高まっている。

当社はNIST Special Publication 800-83[1]を参考に，起こりうるセキュリティインシデントを分析し，対策となるセキュリティ技術の研究開発を進めている。

本稿では，主に制御システムソフトウェアやシステム構成の改ざんに対応するために開発したセキュリティ技術を紹介する。

2　セキュリティ技術の概要

開発したセキュリティ技術は，以下の5つの要素から構成される。

2.1　コード検証ツール

アプリケーションコード，ライブラリに対して静的解析を行うツールである。静的解析では，アプリケーションごとに定義された使用可能な関数リストを用いる。ソフトウェアのぜい弱性につながるOSの関数呼び出しや，ライブラリの関数呼び出しを制限する役割がある。コード検証ツールは，アプリケーションに限られた関数のみを使用させることで，アプリ

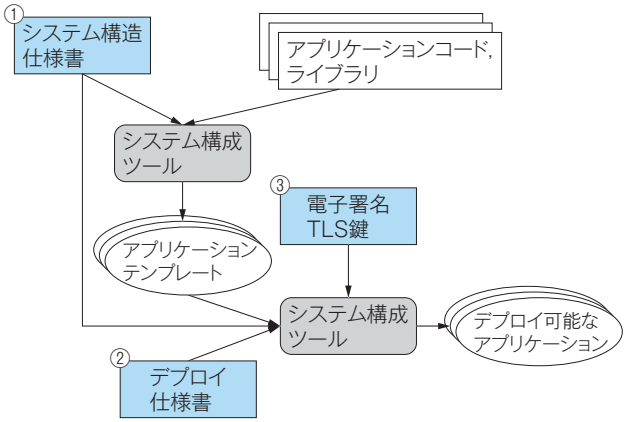
ケーションのぜい弱性を作り込まないようにする。

2.2 デプロイ可能なアプリケーション

デプロイ可能なアプリケーションとは，アプリケーションに様々なポリシー・認証情報・設定情報を付加し，一つにまとめたものである。本技術を用いる制御システム内で，唯一起動できるアプリケーションの型となる。

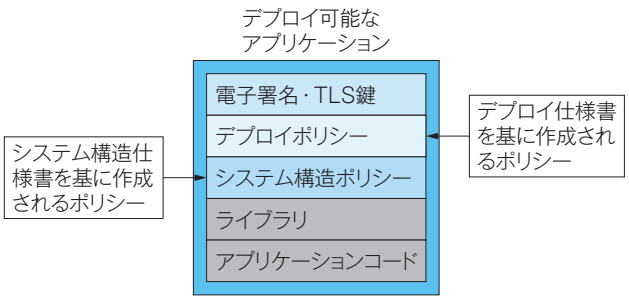
デプロイ可能なアプリケーションは，アプリケーションコード・ライブラリを，システム設定に関する仕様書とともにシステム構成ツールに入力することで作成される。

第 1 図にデプロイ可能なアプリケーションの作成順序を示す。作成にはシステム構成ツールを用いる。システム構成ツールは3段階の作業を行う。1段階目（**第 1 図** ①）ではシステム構造仕様書，2段階目（**第 1 図** ②）ではデプロイ仕様書，3段階目（**第 1 図** ③）では電子署名とTLS（Transport Layer Security）通信に使用する鍵をアプリケーションに組み込む。システム構造仕様書には，アプリケーションの通信先の定義情報・通信種別などの情報が含まれている。またデプロイ仕様書には，アプリケーションを本番環境に展開する時に必要になる具体的なホスト設定情報が含まれている。



第 1 図　デプロイ可能なアプリケーションの作成順序

システム構成ツールを用いてデプロイ可能なアプリケーションを作成する順序を示す。



第 2 図　デプロイ可能なアプリケーションの構成

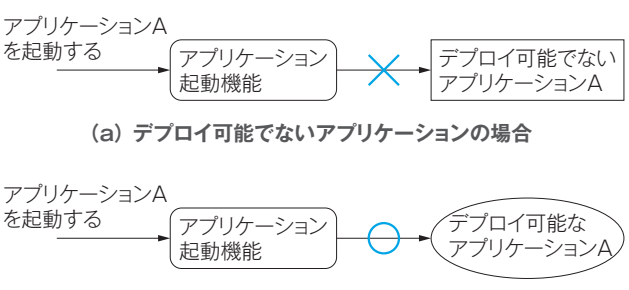
システム構成ツールで作成したデプロイ可能なアプリケーションの構成を示す。

第 2 図にデプロイ可能なアプリケーションの構成を示す。システム構成ツールに入力する仕様書を使用して，セキュリティポリシーが作成され，アプリケーションに組み込まれている。また電子署名はデプロイ可能なアプリケーションが不正に改ざんされていないことを確認するために組み込まれている。

2.3 アプリケーション起動機能

第 3 図にアプリケーション起動機能の概要を示す。アプリケーション起動機能は，デプロイ可能なアプリケーションを起動させるために使用する。すべてのアプリケーションの起動は，アプリケーション起動機能を通して行われる。システム構成ツールを使用せず，デプロイ可能でないアプリケーションの起動は行われない。

第 4 図にアプリケーション起動機能の順序を示す。アプリケーション起動機能は，デプロイ可能なアプリケーションに含まれている電子署名を検証し，アプリケーションの内容が変更されていないことを確認する。電子署名の検証後，アプリケーション起動機能はデプロイ可能なアプリケーションを新規に展開し，アプリケーションが起動できる状態にする。



第 3 図　アプリケーション起動機能の概要

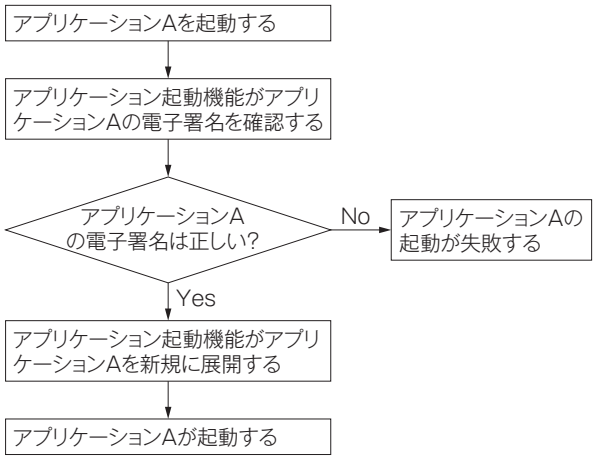
アプリケーション起動機能の役割を示す。

2.4　アプリケーションの通信制限

第 5 図にアプリケーションの通信制限の概要を示す。アプリケーションが指定された通信先と通信するように制限する機能である。デプロイ可能なアプリケーションは，アプリケーションの通信先の定義情報を含んでいる。アプリケーションの通信が開始される時には，定義情報にある通信相手・通信種別であるかのどうかの確認が行われる。アプリケーションの通信先の定義情報には他のアプリケーションだけでなく，データベースやファイルなどのリソースへのアクセス制限情報も含まれている。

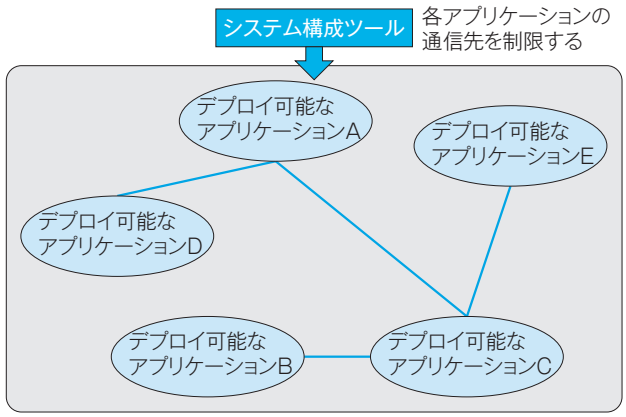
2.5　アプリケーションの通信秘匿

アプリケーションの行う全ての通信は，TLSによって暗号化される。



第 4 図　アプリケーション起動機能の順序

アプリケーション起動機能の状態遷移図を示す。



第 5 図　アプリケーションの通信制限の概要

システム構成ツールによるアプリケーションの通信制限の概要を示す。

3　セキュリティ技術の特長

第 1 表に本技術の対策するセキュリティ脅威を示す。

本技術は先に紹介した5つの要素を以下のように組み合わせることで，セキュリティ対策となる。

(1) コード検証ツールを用いて，ぜい弱性を作り込まないようにアプリケーションを開発する。

(2) システム構成ツールを用いて，信頼性の高いアプリケーションをデプロイ可能なアプリケーションにする。

(3) アプリケーション起動機能を用いて，デプロイ可能なアプリケーションを起動させる。起動するアプリケーションは，アプリケーション起動機能による電子署名の検証によって，システム構成ツールを使用した状態からアプリケーションの内容が変更されていないことが保証される。

(4) アプリケーションが通信を開始する時，通信先の検証が行われる。アプリケーションは，仕様書に含まれる定義情報の制限内の通信のみ許可される。

(5) アプリケーションは，許可された通信先とTLSによって暗号化されたデータをやり取りする。

第 1 表　セキュリティ技術の対応範囲

セキュリティ技術で対策できるセキュリティ脅威と対策となる要素を示す。

セキュリティ脅威	対策
通信の乗っ取り：不正な第三者による通信の横取り	エンドポイント認証のTLS 1.2を使用
中間者攻撃（MITM）：盗聴又は不正操作を目的とした通信の中継及び妨害	TLS 1.2を使用した通信で通信の完全性を確保
メッセージ攻撃：不正もしくは無効な要求又は応答の送信	TLS 1.2を使用した通信で攻撃を軽減
データの引き出し：制限のないネットワークの使用では，アプリケーションがデータを不正に送信する恐れがある。	アプリケーションコード・ライブラリに静的解析を行い，ぜい弱性を作り込まない対策を講じる。
アプリケーションコードの置き換え：不正なアプリケーションコードを実行	アプリケーション起動機能による電子署名の認証で，不正に改ざんされたアプリケーションは実行されない。
コードインジェクション攻撃：アプリケーションに悪意のあるコードを挿入	ぜい弱性の作り込みを防ぐために静的解析を行い，インジェクションによるリスクを軽減

4　むすび

本稿では，制御システムソフトウェアやシステム構成の改ざんに対応するために開発したセキュリティ技術を紹介した。今後も制御システムを安心して使用できるように，アプリケーションレベルでの必要なセキュリティ技術の開発を続けていく。

・本論文に記載されている会社名・製品名などは，それぞれの会社の商標又は登録商標である。

《参考文献》

(1) NIST Special Publication 800-82, “Guide to Industrial Control Systems (ICS) Security,” 2011, (http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf) (2014年12月2日閲覧)

《執筆者紹介》

平田敏樹
Toshiki Hirata
ICT製品・サービス統括本部開発部
産業制御システムのセキュリティ技術開発に従事