組み込みデバイスを対象としたセキュリティ機能の実現方式に関する検討*

北澤繁樹，河内清人，米田健，藤井誠司，中川路哲男†
三菱電機株式会社 情報技術総合研究所‡

1 はじめに

近年，ユビキタスネットワークを見据えた情報家電，携帯電話，PDA（Personal Digital Assistance）などの組み込みデバイスは高度な通信機能に加え，情報管理機能やコンテンツ再生機能など多くの機能を有している．こうした組み込みデバイスでは使用できるリソースが限られているため，十分なセキュリティ機能を確保できないといった問題がある．したがって，近い将来，組み込みデバイスが通常のコンピュータと同様にネットワークに接続されるようになると，ウイルスなどの攻撃対象とされてしまう恐れがある [1].

そこで，本論文では，使用可能なリソースに制限がある組み込みデバイスをネットワーク経由の攻撃から防御するための機能について検討する．

2 組み込みデバイスへの攻撃と対策

組み込みデバイス上で動作するプログラムの多くは，セキュリティを考慮した Java 言語で実装され，仮想マシン上で実行されるため，悪意のあるプログラムを直接実行することによる組み込みデバイスへの被害は小さい．しかしながら，組み込みデバイスの基本機能は，処理速度や処理内容の理由からマシン語で実装されている．こうした，マシン語で実装されている個所への攻撃は，通常のコンピュータと同様に可能である．例えば，コンテンツデータ内にマシン語で記述された不正なコードが含まれていた場合は，ライブラリのバグによりそのコードが実行されてしまうことがある [2]．したがって，組み込みデバイスに対する攻撃で脅威となるのは，言語的にセキュリティで保護されていないマシン語で記述されたコードへの攻撃である．

また，攻撃を検知した後に対策をとることも重要である．組み込みデバイスでは，安定して処理が継続することが求められるため，攻撃の影響によって動作が不安定にならないようにする対策が必要である．

3 攻撃検知技術

コンテンツデータなどの入力データに不正なコードを埋め込み，そのコードを実行させるような攻撃に有効な検知方式としては，パターンマッチング方式および Behavior Blocking 方式 [3] がある．

3.1 パターンマッチング方式

パターンマッチング方式では，既存の攻撃からその攻撃の特徴を抽出し，その特徴に類似したデータがコンピュータ上に存在した場合，それを検知する．パターンマッチング方式の長所と短所を以下に示す．

長所
- 高速処理が可能
- 特徴情報の随時更新による柔軟な対策が可能

短所
- 未知の攻撃を検知できない
- デコード処理が必要

デコード処理は，入力データの詳細な検査を行う場合，各データのフォーマットごとに必要となるため，監視プログラムの肥大化や負荷増加の原因となる．

3.2 Behavior Blocking 方式

Behavior Blocking 方式では，プログラムのコンピュータリソースへのアクセスを監視し，そのプログラムが許可されていないアクセスを行おうとした場合，それを検知し，制御する方式である．監視する対象はシステムコール（ディスクアクセス，メモリアクセスなど）となる．Behavior Blocking 方式の長所と短所を以下に示す．

長所
- 未知の攻撃を検知可能
- デコード処理が不要
- メンテナンスフリー

短所
- システムコールを呼ぶ攻撃のみ監視可能
- システムコール実行時のオーバヘッドが増加

4 議論

ここでは，どのような方式が組み込みデバイスに適しているのかを保護対象，保守性，制限の観点から議論する．

保護対象 保護の対象としては，組み込みデバイスに保管されているデータが挙げられる．例えば，携帯電話や PDA 内部には利用者の個人情報が保管されており，情報家電では機器の制御情報などが保管されているため，これら内部のデータの漏洩や改竄は被害が大きい．

保守性 組み込みデバイスは，ハードウェアに特化して実装され，また，その種類や数が膨大になるため，それら一つ一つに対して十分なメンテナンスを行うことは困難である．したがって，メンテナンスフリーであることは重要な要素となる．

制限 組み込みデバイスでは使用できるリソースに制限があることから，実装において，実行負荷が軽いこと，および実装サイズが小さいことといった制約が存在する．

これらの観点から，Behavior Blocking 方式は，パターンマッチング方式と比較して，メンテナンスフリーな点，およびコンテンツデータの監視にデコード処理を伴わない点などから組み込みデバイス上での実装に適している．さらに，Behavior Blocking 方式ではデータなどにアクセスする

*A Security Equipment for Embedded Devices
†Shigeki KITAZAWA, Kiyoto KAWAUCHI, Takeshi YONEDA, Seiji FUJII, Tetsuo NAKAKAWAJI
‡ Mitsubishi Electric Corporation, Information Technology R&D Center, 5-1-1, Ofuna, Kamakura, Kanagawa, 247-8501, Japan

際のシステムコールも監視可能であるため，内部データの保護も可能である．ただし，システムコール発行時の負荷が上がってしまう点については，改良の余地がある．

また，対策としては，組み込みデバイスが攻撃を受ける前の安定した状態を保存しておき，攻撃を検知した場合には保存してある状態まで復旧することを考える．復旧後，攻撃を受ける原因となった処理をスキップすることにより，たとえ攻撃を受けた場合であっても安定動作可能となる．

以降の節では，Behavior Blocking 方式をベースとし，実行負荷を抑えることを考慮した攻撃検知および対策機能の実装方式を提案する．

5 提案方式

5.1 概要

システムの概要を図 1 に示す．

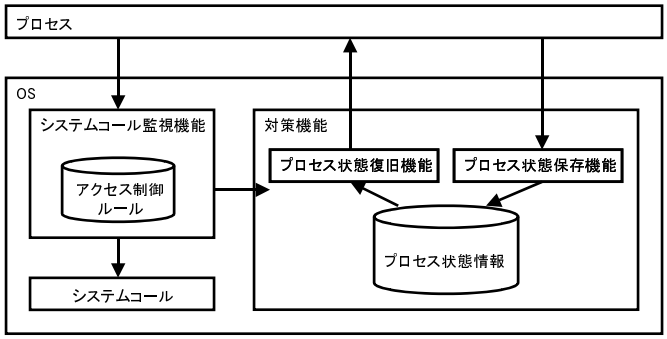

図 1: 提案方式概要図

提案方式では，システムコール監視機能によってプロセスが発行するシステムコールを監視し，そのシステムコールが正当なものであるかどうかを判定する．正当なシステムコールであると判定された場合は，そのままシステムコールを実行するが，不当なシステムコールであると判定された場合は，対策機能を呼び出す．各機能の詳細について，次節以降で説明する．

5.2 システムコール監視機能

システムコール監視機能では，プロセスから発行されるシステムコールをフックし，アクセス制御ルールに基づいてシステムコールの正当性を判定する．アクセス制御ルールでは，各プロセスに対して発行が許可されているシステムコールが記述されており，アクセス制御ルールに一致しないシステムコールをプロセスが発行した場合にはそれを検知する．この制御ルールに記述する制御内容（監視対象とするシステムコールの種類や，正当性の判定方法）によって，システムコール時にかかるオーバヘッドを調整できる．例えば，許可されたアドレス以外からのシステムコール発行を検知するといった制御内容であればシステムコール監視機能のオーバヘッドは小さくなる．

5.3 対策機能

対策としてプロセスの状態を復旧するための 2 つの機能について説明する．ただし，ここでいうプロセスの状態とは，ある時点でのレジスタ値とスタックを指すものとする．

プロセス状態保存機能 プロセス状態保存機能は，プロセスから呼び出され，その時点のプロセスのレジスタ値およびスタック領域をプロセス状態として保存する．

プロセス状態復旧機能 プロセス状態復旧機能は，システムコール監視機能によって不正なシステムコールが検知された場合に呼び出され，保存してあるプロセスの状態情報（レジスタ値，スタック）を用いて，攻撃を受けたプロセスの状態を復旧する．

5.4 検知時の処理

図 2 に，読み込んだコンテンツデータに埋め込まれていた不正なコードが実行されてしまった場合の処理を示す．各処理について以下に述べる．

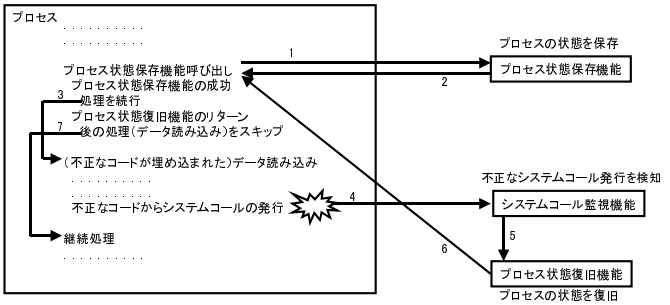

図 2: 検知時の処理

1. プロセスがプロセス状態保存機能を呼び出してプロセスの状態を保存する．
2. プロセス状態保存機能からプロセスへ処理が戻る．
3. プロセス状態の保存に成功した場合，入力データの読み込みを行う．
4. 入力データ中に埋め込まれた不正コードからシステムコールが発行される．
5. システムコール監視機能が不正なシステムコールを検知し，プロセス状態復旧機能を呼び出す．
6. プロセス状態復旧機能によりプロセスの状態を復旧され，プロセス状態保存機能を呼び出した直後までプロセスの処理が戻る．
7. プロセス状態復旧機能によりプロセス状態の復旧が行われていた場合は，データの読み込みをスキップする．

6 まとめ

本論文では，使用可能なリソースに制限がある組み込みデバイス上で実現可能な攻撃検知および対策機能について検討し，組み込みデバイス上で実装する方式としては，Behavior Blocking 方式が最も実現性が高いことが分かった．

次に，Behavior Blocking 方式をベースとした攻撃検知方式と，検知後の対策としてプロセスの状態する方式を提案した．本方式では，組み込みデバイス上でコンテンツに不正なコードを埋め込むような攻撃に対しての対策が可能である．また，アクセス制御ルールの記述内容によってシステムコールのオーバヘッドを調整できる．さらに，プロセスの状態を復旧するため，安全な処理の継続が可能となる．

参考文献

[1] ウイルスの脅威，携帯電話と PDA は「今のところ安全」 http://www.zdnet.co.jp/news/0010/02/mobilevirus.html
[2] CAN-2002-1327, http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1327
[3] Behavior blocking repels new viruses, http://www.nwfusion.com/news/2002/0128antivirus.html