接続性・安全性を確保するネットワーク検証

Verification Technologies which Ensure Connectivity and Security for Networked Products

石 川 博 一* 楠 堂 忠 夫*
Hirokazu Ishikawa Tadao Kusudo

エネルギーマネジメントシステムおよびそれを構成する機器において，多様なユーザー環境での接続性の確保と，日々高度化するクラッカーなどからの攻撃に耐えるセキュリティ耐性を確保する取り組みとして，接続検証技術とセキュリティ検証技術を説明する．

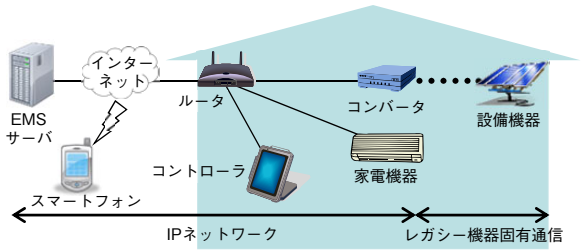
It is important to have network verification technologies to ensure connectivity in a variety of customer network situations and ensure security against the attacking methods of crackers that are advancing every day for development of the energy management system and its components.

1. ネットワーク製品の接続性，安全性確保

エネルギーマネジメントシステム（Energy Management System．以下，EMSと記す）および構成機器をはじめとしたネットワークに接続する機器を開発するにあたり，その接続性とセキュリティ耐性を確保することは重要である．

当社では，接続性の確保のために，ユーザーが保有する多様なネットワーク環境を再現，動作評価を行う「互換性試験」と，ネットワーク機能の規格適合性および，異常系に対する挙動を評価する「機能性試験」を合わせた「接続検証」を実施している．

また，日々進化するクラッカー（悪意のある攻撃者）などからの攻撃に備えたセキュリティ耐性を確保する取り組みとして，システムを構成する各機器に対するぜい弱性を診断する「機器単体診断」，システムを構成する各機器と通信するサーバアプリケーションについてぜい弱性を診断する「サーバ診断」，システムを構成する各機器およびサービスサーバと連動して動作させた際のぜい弱性を診断する「システムを対象とした診断」を合わせた「セキュリティ検証」を実施している．



第1図 エネルギーマネジメントシステムの構成例
Fig. 1 Example of energy management system

本稿では，特にEMSで必要となるネットワーク検証の方針を述べる．

2. 接続検証技術

ユーザーが使用するさまざまな宅内のネットワーク環境との接続性を確保するため，EMSおよび構成機器の開発スケジュールに沿って実施すべき対応として，機能性試験と互換性試験を策定した．

2.1 機能性試験

機能性試験は，過去のネットワーク機器・システムの検証において蓄積した実環境での特異事例，開発者の間違い事例といったノウハウを基に構成するブラックボックステストである．

EMSおよび構成機器に対する検証の際は，特に以下の観点を考慮することが重要である．

① 信頼性：通信切断時などの異常処理評価，復旧処理の評価および，異常処理が他の処理と整合性があることを評価

② エラー表示：システムの利用形態から，ユーザーが常時動作を確認していない点に着目，エラー表示の内容やタイミングを評価

③ テスト範囲の分割化：EMSには，IP（Internet Protocol）ネットワークやレガシーの機器固有の通信機能など，多様な通信形態が存在する（**第1図**参照）．試験の抜け漏れ，効率化を実現するため，試験範囲を試験のステップごとに定義し評価を実施

2.2 互換性試験

互換性試験は，多様なユーザー環境を想定したうえで，試験環境を構築し，動作の正常性を評価する．

* 解析センター
ネットワーク・セキュリティ技術サポートグループ
Network And Security Engineering Support Group,
Analysis Center

近年，インターネットサービスプロバイダやルータに不審と判断された通信を遮断する機能など，独自の機能を盛り込む傾向がある．これに対し，EMSおよび構成機器で採用している通信方式が遮断されないか事前に評価し，問題が判明した場合はその原因と対策を明確にすることが重要である．

当社では，市場普及率および，先述の独自機能や簡単設定機能の有無など，技術的な特徴を考慮し，過去10年間にわたり収集した500機種以上のルータなどの中継器および，65構成以上のインターネット接続回線を保有している．このなかから，さらにルータの宅内側通信の問題事例といった種々のノウハウも考慮して環境を選定し，ユーザー環境での接続性確保を図った．

3. セキュリティ検証技術

悪意をもつ第三者からの攻撃・脅威から安全性を確保するため，クラッカーおよびウィルス・ワームの感染によって侵入される可能性・影響が比較的高い範囲を優先度が高い検証範囲とする．今回は，TCP（Transmission Control Protocol ）/IPネットワークとの接続点を有するところを対象とした．EMSおよび構成機器においては，次の4点を考慮することが重要である．

- 機器単体の診断
- サーバの診断
- システムを対象とした診断
- 上記診断の定期的な実施

3.1 機器単体の診断

組込み機器（家電）では，CPUやメモリーなどのリソース量には制約が伴う．そのため，PCのようにウィルス対策ソフトウェアを導入することもなく，高度なセキュリティ対策機能や異常な操作指示・入力値の適切な処理が省略される傾向がある．

EMSでは電力消費量の見える化，節電につながる電力消費量のピークシフトなどの機能を搭載している．このように電気使用料などの個人情報および機器の制御情報が機器において処理・蓄積される．

近年，クラッカーが組込み機器やスマートメータをターゲットとした攻撃やぜい弱性の情報公開も増加傾向にあり，それに備えたセキュリティ対策が必要になっている．セキュリティ対策の有効性を確認するための診断として，既知のぜい弱性への対応，組込み機器に搭載された設定用Web機能，サーバとの通信内容，USB/SDカードなどの外部インターフェース，機器のファームウェアなどを通して情報漏えい・改ざん・機能停止がなされないかの確認が必要である．

3.2 サーバの診断

機器とEMSサーバ間の通信は，利用者の目に触れにくいため，開発者によるセキュリティ対策の水準が低くなりがちである．EMSでは設置機器や電力消費量の情報が機器とEMSサーバ間で伝達されている．さらには，機器に対する制御情報（例えば，エアコンに対する電源ON/OFFなど）についても伝達されている．消費電力量など，個人情報に関わる情報の取り扱いや不正操作にもつながりかねない内容を取り扱うため，セキュリティ対策は必須と言える．

EMSサーバでは，機器制御および機器からの情報を取り込むための機器用インターフェース，利用者からの設定を受け付けるための簡易登録サイト，リモートメンテナンス用のバックオフィスのインターフェース，CEMS（Community Energy Management System）サーバとのインターフェースなどをもつ．それぞれのインターフェースにおいて，機器のなりすまし，および，サーバのなりすましを想定し，個人情報，パスワードなどの漏えい，制御情報の改ざん，および，システムダウンの対策ができているかの観点で，ぜい弱性診断を実施する必要がある．

3.3 システムを対象とした診断

機器およびサーバの個別のぜい弱性診断に加え，システム全体の観点で診断を行う必要がある．主にシステムの外部から侵入が可能かの観点と，システムの内部に侵入されてしまった場合どのようなことが行われてしまうのかの2つの着眼点から診断を行う必要がある．

また，メンテナンス用の設備（アップデート用サーバまたは管理用PCなど）やスマートメータの自動検針機能など，一般の利用者からアクセスが比較的難しいとされるところも診断が必要と考えられる．さらには，最近のスマートフォンとの連携サービスの普及を考慮すれば，スマートフォンにインストールされるアプリケーションに関してもセキュリティ対策および診断を行う必要がある．

4. 今後の展望

本稿では，EMSおよび構成機器の接続性・セキュリティ耐性を確保し，ネットワーク品質を高める取り組みを記載した．今後は，他社製品も含め，多様化する接続形態やアプリケーションなどについて検証技術を確立し，当社製品のさらなるネットワーク品質の向上に取り組みたい．