ISA100.11a 無線システムの強固なセキュリティ対策

Strong Security Measures Implemented in ISA100.11a Wireless System

北野 欽一 *1　　山本 周二 *1
Kinichi Kitano　　Shuji Yamamoto

横河電機は，インダストリアルオートメーション用無線通信規格 ISA100.11a の標準化活動に設立当初から参画し，同規格に適合した製品展開を進めている。ISA100.11a を含めたフィールド無線のプラント現場への普及拡大がすすんでいるが，導入にあたってセキュリティが重要視されることが多い。本稿では ISA100.11a 規格に組み込まれたセキュリティ対策と当社のセキュリティに対する取り組みを紹介する。

From the beginning, Yokogawa has been participating in standardization and dissemination of ISA100.11a, a wireless communication standard for industrial automation advocated by the International Society of Automation (ISA), and has been expanding its product portfolio with conformance to this standard. Although field wireless standards including ISA100.11a are being introduced into plants widely, security is still one of the major concerns. This paper introduces the security measures of ISA100.11a and Yokogawa's efforts to enhance plant security.

1. はじめに

プラント現場への無線の本格導入が進んでいる。フィールドのデバイスを無線化することで，信号配線および電源配線の配線コストの削減，設置工期の短縮，高所や飛び地など物理的 / コスト的に配線困難な場所の計測，回転 / 移動する観測点の計測，定修時などの一時的な計測など，有線にはないさまざまなメリットを享受できる。そのため，現場の無線への期待は高い。

しかしながら，フィールド無線導入において通信の信頼性に並ぶ重要な要件としてセキュリティが挙げられることが多い。無線の特徴である，目に見えない，どこまで到達しているかわからないという特性に対する懸念だけでなく，無線 LAN と混同され同様の脆弱性を持つのではないかという，技術の違いの理解不足による懸念も挙げられている。

横河電機が普及を推進している無線規格 ISA100.11a[(1)] はユーザの要求に基づいて作成された規格であり，当初より信頼性やセキュリティを念頭に置いて仕様を作成している。無線や計装の専門家だけでなくセキュリティの専門家も仕様作成に参加しているため，堅強なセキュリティ技術が組み込まれたフィールド無線のプロトコルとなっている。

*1 IA プラットフォーム事業本部新分野開発センター
無線ソリューション部

本報告では，無線一般のセキュリティの脅威について紹介し，次に ISA100.11a が提供するセキュリティ対策および横河電機のセキュリティに対する取り組みを紹介する。

2. 制御システム構成例

図 1 に ISA100.11a に基づくシステム構成の例を示す。

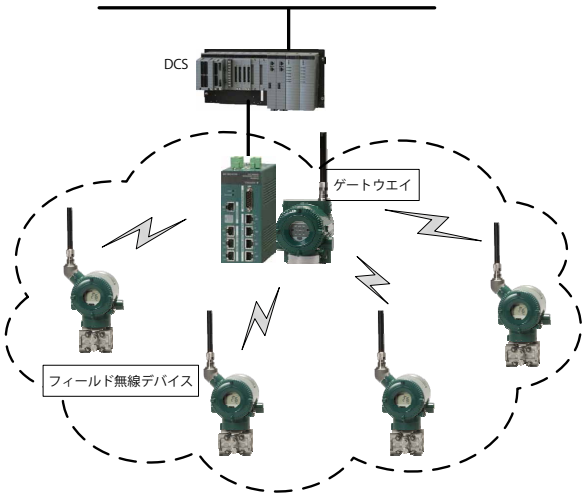

図 1 制御システム構成例

ゲートウエイは分散型制御システム (DCS) などの上位システムと ISA100.11a フィールド無線デバイスの間の通信を司る装置である。さらにゲートウエイは，通信の

スケジュールや通信の経路の決定など ISA100.11a 通信そのものを司るシステムマネージャに加え，フィールド無線デバイスの認証や暗号鍵の管理といったセキュリティを管理するセキュリティマネージャを含んでいる。

3. 無線に対するセキュリティの脅威

無線で送受信されるデータとして，プロセス値や操作出力値といった運転用のデータ，生産量や商取引量のような製造向けデータ，無線の状態や設定情報などの無線システムの管理に使用されるデータが挙げられる。

そのような重要な情報を扱うフィールド無線システムに対して一般的に以下のような脅威が知られている。

- 盗聴
- 改ざん
- なりすまし
- 再送攻撃

3.1 盗聴

悪意のある第三者が無線を故意に傍受し，通信内容を盗み取ろうとすることを盗聴と呼ぶ。

もし，悪意を持つ人に何らかの方法により無線で送受信される通信からデータを盗み見されたら，製造のノウハウ，生産量のような経営数字が漏えいする懸念がある。また、無線システムの管理用データが，無線システムへの違法アクセスのヒントを与えてしまう可能性もある。

データそのものに価値がなくても，情報が漏えいしたことが報道などを通じて知らされることで無線システムを提供する企業と使用する企業共に社会的信用を失う可能性もある。

3.2 改ざん

悪意のある第三者が通信を故意に傍受し，通信内容に変更をすることを改ざんと呼ぶ。

プロセス値や操作出力が，悪意を持って改ざんされたことに気付かないまま使用された場合，生産物の質の低下だけでなく，異常な出力による装置の損傷，さらには人命に被害を及ぶことも考えられる。

3.3 なりすまし

通信を送受信する権限がない機器が，権限を持つ機器であるかのようにネットワーク上で振る舞うことを，なりすましと呼ぶ。

なりすましとして，正規のデバイスへのなりすましと，正規のゲートウエイへのなりすましが考えられる。もし悪意を持ったデバイスが無線ネットワークに参加して正規のデバイスになりすますと，偽のプロセス値を上位システムに送ることが可能となる。悪意を持った機器が正規のゲートウエイになりすますと，不正な操作出力値をバルブやアクチュエーターのようなデバイスに送ることが可能となる。

3.4 再送攻撃

なりすましの特別なものとして再送攻撃と呼ばれる攻撃がある。これは通信を記録して，後で記録した通信を再送するものである。再送攻撃には暗号を解読することなく攻撃可能という特徴がある。

フィールド無線の規格によっては，再送攻撃に対する防御の仕組みが用意されていない。防御が用意されていない場合，下記のような攻撃とその影響が一例として想定できる。

ゲートウエイがバルブに開くよう通信する。バルブは正規のゲートウエイからの通信なので指示されたとおりバルブを開く。悪意を持ったデバイスがこの通信を記録する。悪意を持ったデバイスは後でこの通信を再送する。記録された通信は正規のゲートウエイからの通信と区別がつかないので，再送された通信を受け取ったバルブはバルブを開く。このようにして悪意を持ったデバイスは，本来想定されていないタイミングで不正にバルブを操作することが可能になる。

4. ISA100.11a のセキュリティ機能

前述のような脅威に備え ISA100.11a に組み込まれたセキュリティ機能は以下の要求を満たすよう設計されている。

- 送信元が正規のデバイスであり，かつ通信内容が第三者に改ざんされていないことを保証する
- 最先端の暗号を使用して機密性を保証する
- 再送攻撃に対する防御を提供する

これらの要求を満たすために，ISA100.11a には以下のセキュリティ技術が導入されている。

- デバイスの認証
- 通信の暗号化
- メッセージ認証の導入
- 通信鮮度の概念の導入

いくつかの論文が，ISA100.11a が他のフィールド無線プロトコルよりも強固なセキュリティを提供すると報告している。[(2) (3)]

4.1 デバイス認証

デバイスのネットワーク参加時のなりすましの防止が，強固なセキュリティの要である。ISA100.11a では，ゲートウエイはネットワークに参加する権限のあるデバイスに限って暗号鍵を共有し，正しい相手しか暗号鍵を知らないことを前提に暗号化と改ざん防止を実現している。

したがって，万一なりすました偽のデバイスが暗号鍵を持ってしまえば，ゲートウエイは正規のデバイスからのデータなのか，偽のデバイスからのデータなのか区別がつかなくなる。

そのため，偽のデバイスや偽のゲートウエイへの対策として，ISA100.11a は，プロビジョニングと呼ばれる認証用の鍵の共有方法を定義し，ネットワークに参加時に，デバイスとゲートウエイ間でその認証用の鍵を基に相互に認証することを必須としている。認証に成功したゲートウエイとデバイスで暗号鍵を共有する。

この認証用の鍵をジョインキーと呼んでいる。デバイスのプロビジョニングには赤外線通信を利用する。赤外線の遠くまで飛ばないという特徴を活かした秘匿性の高いデータ転送となっている。プロビジョニングは**図 2** に示すように PC に接続した赤外線アダプタをデバイスの赤外線ポートに 30cm 以内に近づけて実施する。

デバイスに組み込まれたジョインキーを読み返すことはできないようになっている。プロビジョニングの度に新しいジョインキーが生成される。したがってデバイスごとに異なるジョインキーが用意される。一方各デバイスのジョインキーはファイルに保存され，ゲートウエイにダウンロードされる。

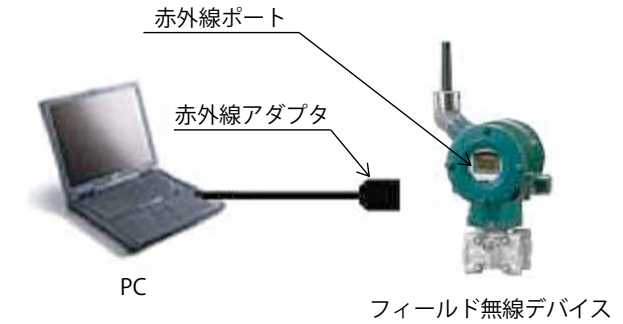

図 2 デバイスのプロビジョニング例

ネットワーク参加時の認証はチャレンジレスポンスと呼ばれる認証方法を使用している。チャレンジレスポンスは認証用の鍵をネットワーク上に直接送らない秘匿性の高い認証方法である。これは “ なぞなぞ ”（チャレンジ）を相手に送り，相手はチャレンジに対して認証用の鍵を基に回答（レスポンス）する認証である。送信側は自分でもチャレンジから認証用の鍵を用いてレスポンスを計算する。相手からのレスポンスと自分で計算したレスポンスが一致すれば相手も認証用の鍵を知っていると判断し，それをもって相手が正しい相手であることの根拠とする。ISA100.11a 通信の場合，この認証用の鍵がジョインキーとなる。

ISA100.11a のチャレンジレスポンスによる相互認証を**図 3** に示す。デバイスは疑似乱数とジョインキーからチャレンジ C_A を生成してゲートウエイに送信する。ゲートウエイはチャレンジに対するレスポンス R_A を生成してデバイスに返信する。デバイスは自分で計算したレスポンスと R_A を比較し一致すればゲートウエイを正規のゲートウエイであると認証する。デバイスは R_A をゲートウエイからのチャレンジとしてレスポンス R_B を生成してゲートウエイに返信する。ゲートウエイは自分で計算したレスポンスと R_B を比較して一致すればデバイスが正規であると認証する。このように，デバイスとゲートウエイは相互に認証するようになっている。

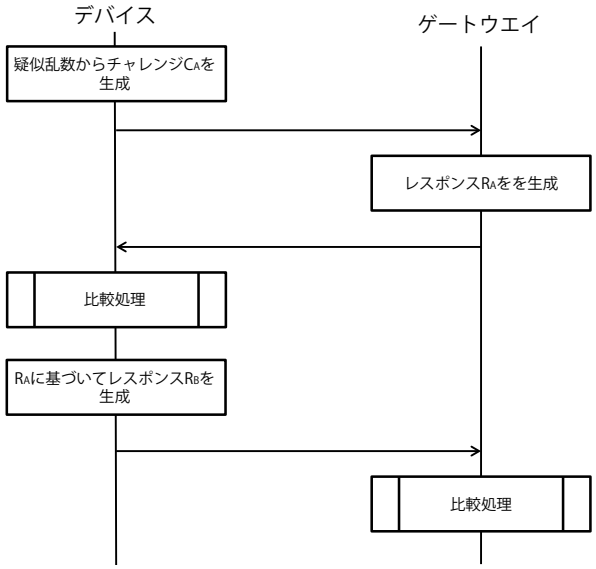

図 3 チャレンジレスポンスによる相互認証

4.2 通信の暗号化

盗聴に対する有効な対策は暗号化である。暗号化することで無線が傍受されても有効なデータを取り出すことが不可能になる。

ISA100.11a は暗号化アルゴリズムとして AES (Advanced Encryption Standard) を採用している。AES はアメリカ合衆国の暗号化標準で，欧州連合でも暗号規格として採用されている。金融機関や電子商取引で実績もある堅牢な暗号化アルゴリズムである。

AES には総当たり攻撃以外の有効な攻撃方法が見つかっていない。総当たり攻撃への有効な対策は長い鍵を使用することである。ISA100.11a では 128 ビットの鍵を使用している，128 ビットの鍵の組み合わせは $3.4 * 10^{38}$ となり，現在最速のスーパーコンピューターを 10 億台用意しても暗号解読に 10 億年が必要となる [4]。

2011 年に AES が破られたという記事が流れたが，これは AES を解読するアルゴリズムが発見されたわけでなく，これまでより約 4 倍効率の良い総当たり攻撃の方法が見つかっただけである [5]。さきほどの計算例では，最速のスーパーコンピューターを 10 億台用意しても 2.5 億年必要である。

さらに，暗号鍵はセキュリティマネージャにより定期的に更新される。したがって，もしも暗号鍵が総当たり攻撃で解読されたとしても，解読が完了した時点ではもうその暗号鍵は使用されていない。しかも，暗号鍵はデ

バイスごとに異なるので，総当たり攻撃で何億年もかかって暗号鍵を解読しても，特定のデバイスの特定の数日の通信の内容しか得られない。

4.3 メッセージ認証

メッセージ認証は，通信が正しい相手から来たこと，途中で改ざんされていないことを確認する仕組みである。これは暗号鍵を知っているデバイスだけが生成でき，通信に埋め込まれるメッセージ認証コードで実現される。すなわち，メッセージ認証コードが異なった場合，暗号鍵を知らない偽の相手からの送信か，途中で改ざんされたと判断し通信を破棄する。

初期の無線 LAN は通信の誤り検出にチェックサムを使用していた。チェックサムは通信の内容のみから計算されるので，チェックサムごと通信を改ざんされると改ざんを検知することは不可能であった。ISA100.11a に導入されたメッセージ認証コードは改ざん防止に有効である。

4.4 通信鮮度

再送攻撃の対策として有効な手段は通信に鮮度の概念を導入することである。データの発信から一定時間以内に受信した通信のみ受け入れる。

ISA100.11a 無線ネットワークに属する各デバイスはミリ秒単位で時刻を同期して，通信に時刻の情報を付加することで送信時刻の適性を判定している。

5. セキュリティ機能の効果

以下の表にフィールド無線一般の脅威に対して，ISA100.11a が提供するどの機能が対策となるかを示す。

表 1 ISA100.11a 提供のセキュリティ機能の効果

	デバイス認証	通信の暗号化	メッセージ認証	通信鮮度
盗聴	○	○	○	—
改ざん	○	—	○	—
なりすまし	○	—	○	—
再送攻撃	—	—	○	○

デバイス認証，通信の暗号化，メッセージ認証，通信鮮度は 4 つを組み合わせて初めて堅牢なセキュリティを実現する。どれが欠けてもセキュリティ的に脆弱な通信となってしまう。たとえば，メッセージ認証なしに通信を暗号化しても，受信側で正しい値を受け取った保証がない。デバイス認証なしでは，通信を暗号化しても暗号鍵を共有している相手が正しい相手かどうかの保証がない。通信鮮度なしでは正しい相手の過去の通信が，悪意を持った相手に使い回しされても検知できない。

6. 横河電機の取り組み

堅牢なセキュリティを持つ通信プロトコルを採用しただけで堅牢な無線システムが実現できるわけではない。セキュリティを意識した製品開発と，製品が正しく実装されていることの確認が必要となる。

横河電機では製品実装にあたって以下の取り組みを実施している。

- 製品にもたらされるセキュリティのリスクについて設計時に検討
- 脆弱性を作りこまないコーディングについてプログラマに教育
- ソースコードに対して解析ツールでセキュリティ的に問題のある個所を検知

これだけでは，製品実装上の間違いや思い込みによる脆弱性を検知できないので，さらに実際の無線システムに対して社内外の有識者に製品のセキュリティ評価をいただくことで脆弱性検出の活動をおこなっている。

将来的には，IEC62443 のセキュリティ要件を満たしていることを示すために ISASecure EDSA 取得を目指す。

7. おわりに

横河電機が提供するフィールド無線システムについて，セキュリティ上の脅威と対策について紹介してきた。初期の無線 LAN を反面教師として，これまでに知られている無線セキュリティ上の脅威に対しては ISA100.11a に対策がプロトコル内に組み込まれているので，ISA100.11a に準拠したデバイスであれば自動的に対策がされていることになる。

開発する側のセキュリティ対策技術やツールが日進月歩で進歩しているのと同じように，攻撃側の技術やツールも同様に進歩している。費用や処理時間の面から不可能と考えられていた攻撃が，技術の進歩によりある日突然現実味のある攻撃となる。当社も立ち止まることなくシステムのセキュリティを強化して対抗していく。

参考文献

(1) ISA-100.11a-2011, Wireless system for industrial automation: Process control and related applications
(2) Gengyun Wang, “Comparison and Evaluation of Industrial Wireless Sensor Network Standards ISA100.11a and WirelessHART,” Master of Science Thesis, Communication Engineering, 2011
(3) Cristina Alcaraz, Javier Lopez, “A Security Analysis for Wireless Sensor Mesh Networks in Highly Critical Systems,” IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews,” Vol. 40, Issue 4, 2010, pp. 419-428
(4) Mohit Arora, “How secure is AES against brute force attacks?,” EE Times, 2012, http://www.eetimes.com/document.asp?doc_id=1279619
(5) Andrey Bogdanov, Dmitry Khovratovich, Christian Rechberger, “Biclique Cryptanalysis of the Full AES,” Advances in Cryptology – ASIACRYPT 2011, Vol. 7073, 2011, pp. 344-371