B-5

汎用機器を用いた信号システムの安全性・セキュリティ確保

信号保安システムで汎用機器やデータセンタを用いる際の安全性・セキュリティ確保について、適用対象の特性に応じて複数の対策手法を提案しました。

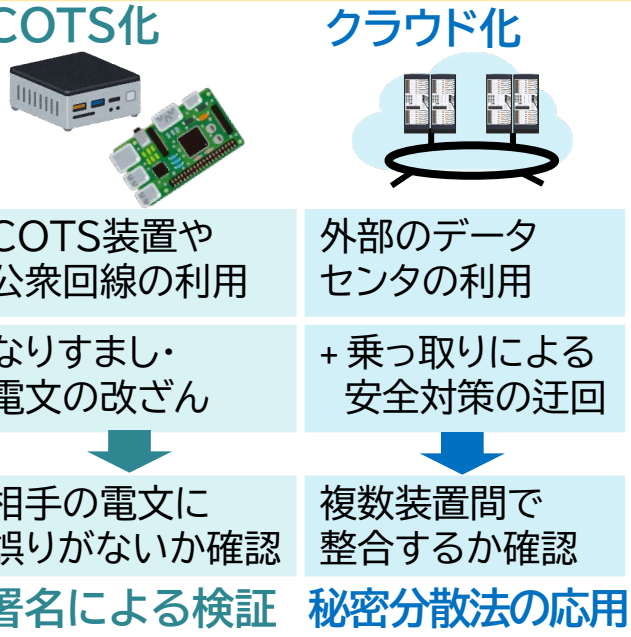
研究の背景と目的

- システムの低コスト化や保守作業の効率化のために、信号保安システムで汎用機器・汎用ソフトウェア(COTS)やデータセンタを利用するニーズが高まっています。
- COTS化にはサイバー攻撃のリスクが伴うため、安全性とサイバーセキュリティを確保する技術が必要です。
- 特に外部のデータセンタを利用する場合、OS等の脆弱性をついた安全対策技術の迂回の防止や、サービスを妨害する攻撃への耐性向上が求められます。

研究成果

- 適用対象に合わせ、課題(想定される脅威)と対策の基本原理について整理しました。
- 実績のある暗号化技術(署名)による安全性確保手法を提案しました。通信装置自体の防護に依存しないため、公衆回線の利用が可能です。
- プライバシー保護の用途で使われる秘密分散法を制御に応用することで、サイバー攻撃への耐性を高める手法を提案しました。

適用対象と対策の基本原理



今後の展開

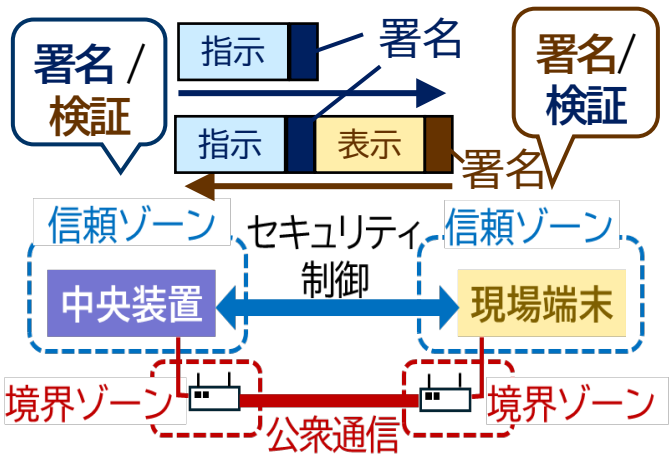
- 署名技術を用いた汎用装置主体の信号保安システムを試作し、実用化を目指します。
- 秘密分散法の応用によるセキュリティ確保手法については、連動装置等の具体的アプリケーションを想定して、改良と検証を進めます。

信号技術研究部(信号システム)

汎用機器の適用イメージと効果

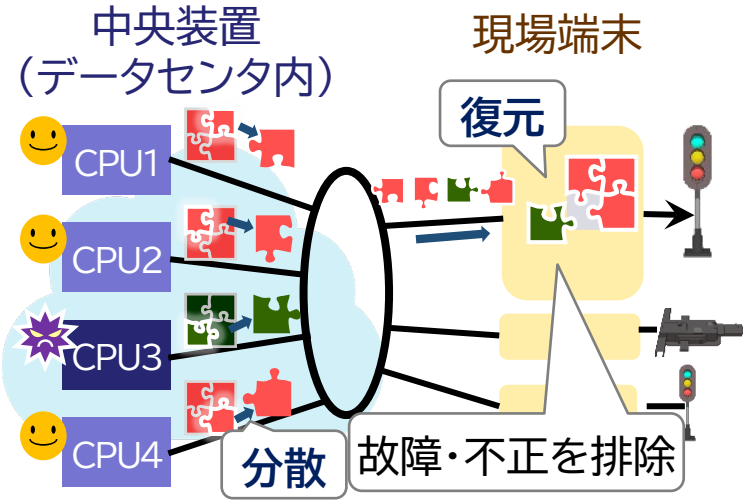
専用ハードウェアとソフトウェアの構成を、汎用ハードウェアとソフトウェア、専用アプリケーションに置き換えることで、低コスト・高性能化が期待されます。さらに、システムの主機能をクラウド上（データセンタ）で実行することで、一層の低コスト化と災害への耐性向上が期待されます。

署名によるセキュリティ確保



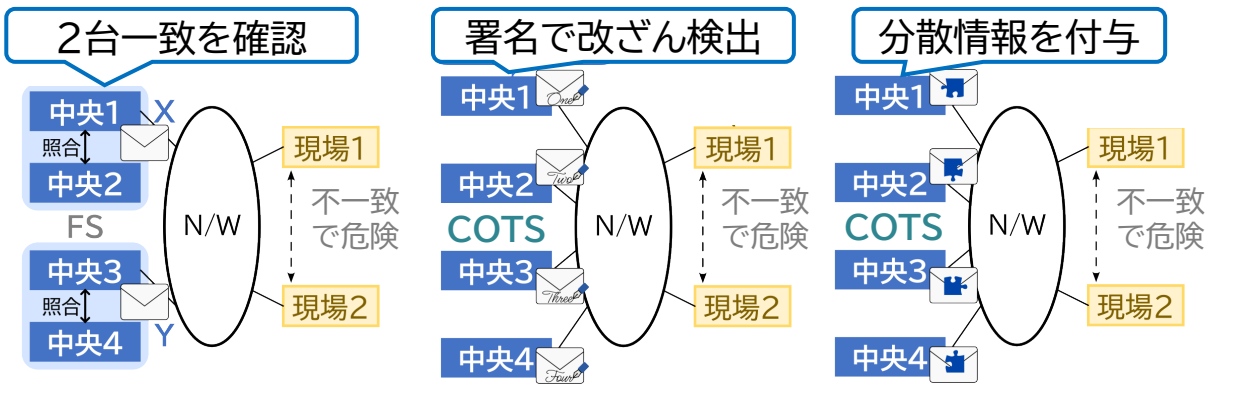
✓危険側制御の防止

秘密分散法を応用したセキュリティ確保



✓攻撃下での機能維持

故障やサービスを妨害する攻撃への耐性向上



	FS比較照合（従来）	署名による検証	秘密分散による検証
中央1 故障 / 中央4 故障	安全側停止	機能維持	機能維持
中央1 乗っ取り / 中央2 故障	危険	安全側停止	機能維持

➡安全性の向上　➡安定性の向上