IoTのための情報セキュリティ・ネットワーク最適化

高知工科大学　情報学群　教授　清水明宏
教授　福本昌弘

研究概要

IoTデータを有効に利活用するためには、リアルタイムで安全に全一元化するとともに、安心してデータを提供してもらえる情報セキュリティと、利用者に負担をかけない情報・サービス共有ネットワークの実現が不可欠である。そのため、IoT機器に搭載可能な処理負荷が小さく安全が保障された認証アルゴリズムとして、センサーノード側では排他的論理和と加算のみで実現できる認証方式SAS (Simple And Secure password authentication protocol)-Lを開発している。また、情報共有する際には、部分復元を可能とする秘密分散法を用いることで、情報理論的に安全に分散情報共有できるとともに正規の利用者のみが安全に利用できる地域情報共有管理の実現を目指している。さらに、耐災害性に優れた低コストでの運用が可能な地域情報共有ネットワークに適した通信方式の検討を行っている。

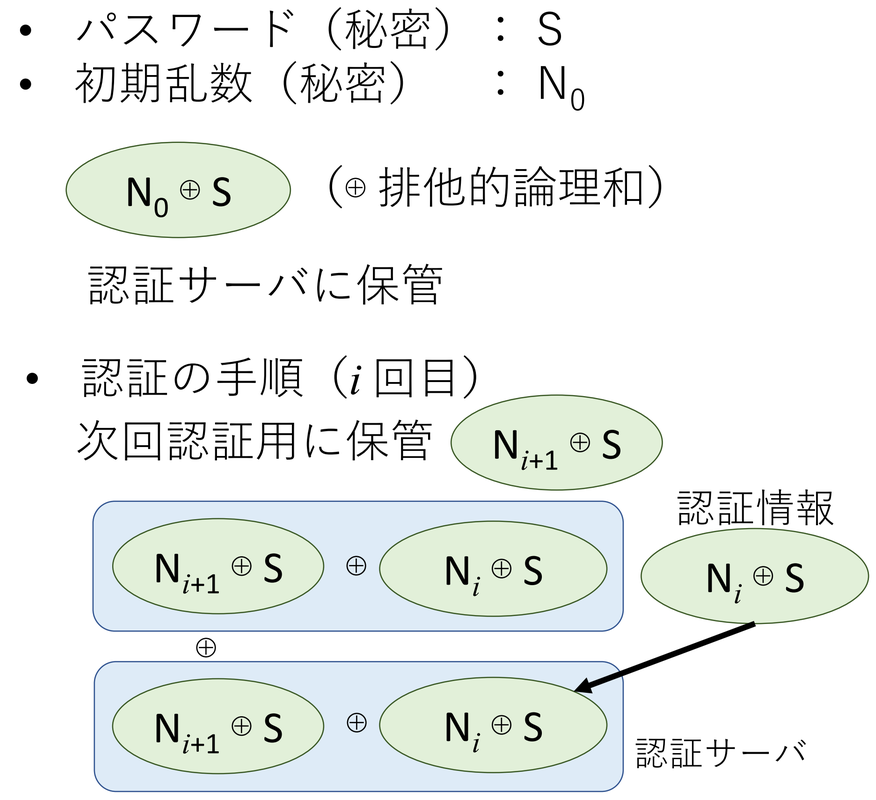

図1　極簡易な計算のみで実現されるSAS認証方式により世界最高峰の安全性を保障

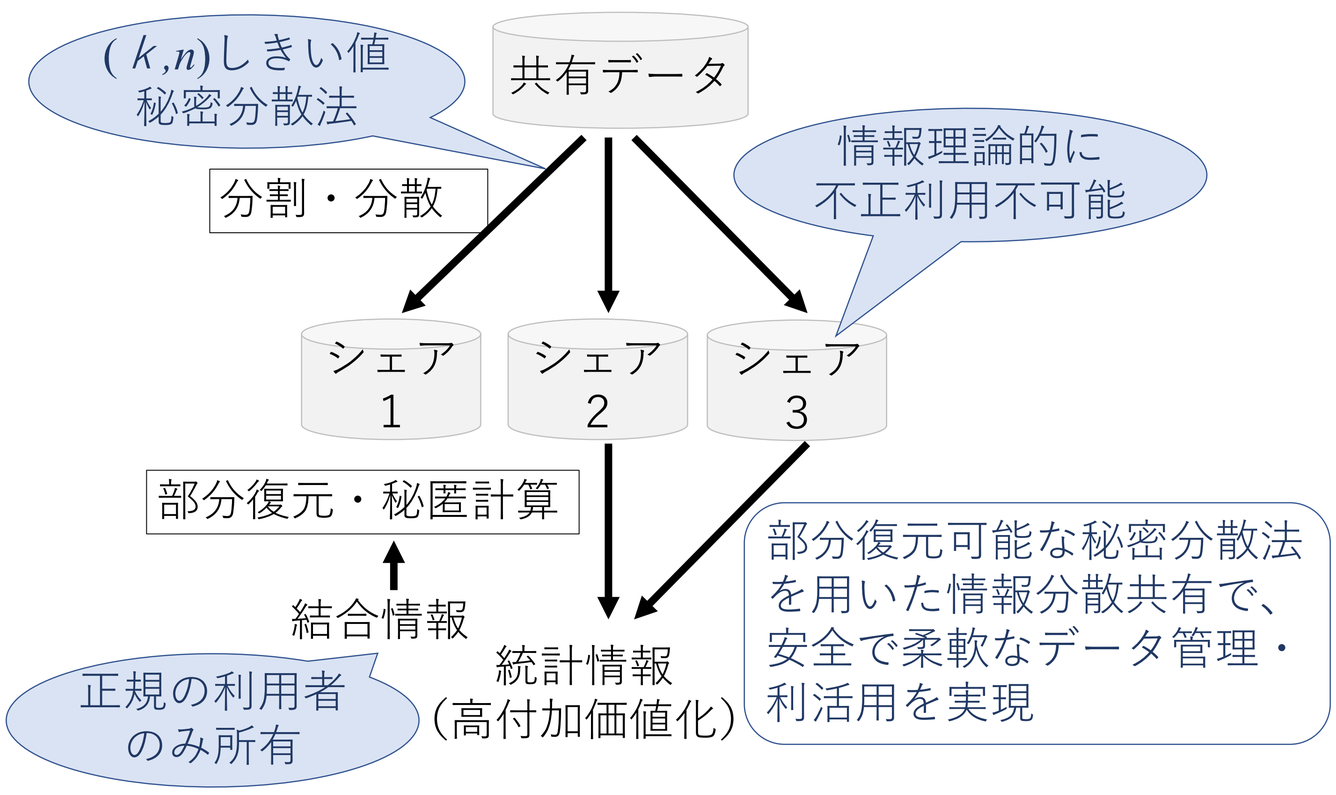

図2　量子コンピューティング時代にも情報理論的に安全性を保障できる部分復元可能な秘密分散法

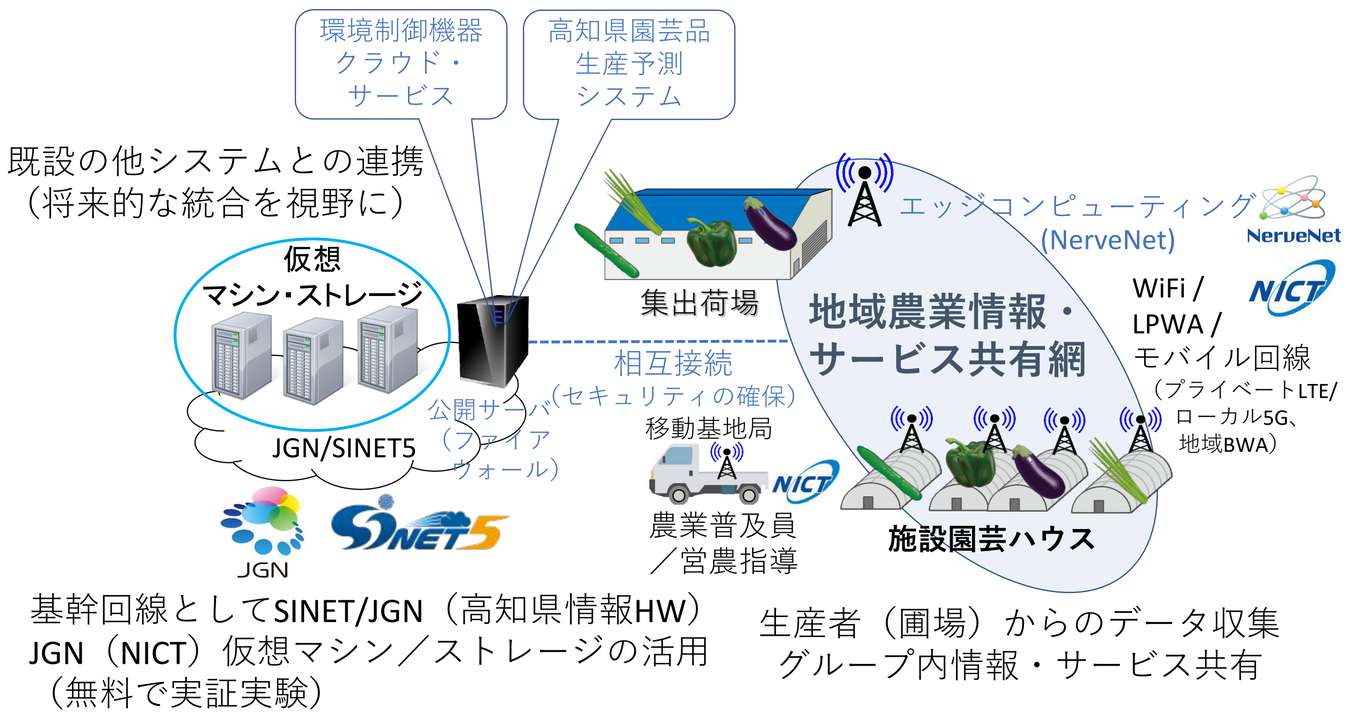

図3　Next次世代型施設園芸農業IoP (Internet of Plants)のための地域情報共有ネットワークの実現例

応用範囲

安全・安心な地域でのデータ共有の仕組みを構築することで、多くの分野で情報を集積・一元化できるようになる。

今後の展開

実証実験による有効性の確認や実装を進めることで関連産業への貢献をはかる。

高知工科大学
KOCHI UNIVERSITY OF TECHNOLOGY

〒782－8502　高知県香美市土佐山田町宮ノ口185
高知県公立大学法人 高知工科大学 研究連携部 IoP推進事務室
TEL:0887-53-9065　E-mail: iop@ml.kochi-tech.ac.jp