

広域災害対応型クラウド基盤構築に向けた研究開発 省電力アクセスネットワーク制御技術の 研究開発

平成25年10月1日

日本電気株式会社
田中 淳裕

日本電気株式会社
沖電気工業株式会社
奈良先端科学技術大学院大学



目次

クラウド利用におけるユーザの問題意識と解決施策

社会インフラとしてのクラウド

アクセスネットワークの課題

研究開発スケジュール

東北地区での実証実験および技術成果について

福島県の高등학교での実証実験

研究開発の内容

課題(1) 省電力アクセスネットワークの高信頼化技術

省電力センサ遠隔管理技術

課題(2) 省電力アクセスネットワーク向け暗号通信路確立技術

省電力鍵更新技術

まとめ

成果

実用化

社会実装に向けて

今後の課題

クラウド利用におけるユーザの問題意識



そもそもクラウドなんか導入しなくてもやっていける。PCと台帳で済んでいる。コスト増はNo

「通常」



BCPに向け、クラウドの有効性は分かるが投資コストの増加と特定プロバイダへロックイン心配

「備え」



災害時におけるサービスの継続性が見えない。複数事業者契約など負担増も免れないのでは

「緊急」



クラウドはネットワークが崩壊しても必要な時に必要な情報を住民や事業者提供できるのか

「復旧(興)」

高信頼・省電力クラウドサービス基盤

環境適応型ネットワーク基盤

省電力アクセスネットワーク基盤

事業者間を含む異なるクラウド間を相互接続し、資源の相互融通を可能とすることで低コストで高信頼なクラウドを自由に選択

IPネットワークの電力を自律的に大幅削減することでネットワークコストを抑え電力不足時でもネットワークサービスを継続する

ネットワークインフラが崩壊してもクラウド&センサーを連携して地域の情報をタイムリに提供できるネットワークを提供する

クラウド利用におけるユーザの問題意識と解決施策



そもそもクラウドなんか導入しなくてもやっていける。PCと台帳で済んでいる。コスト増はNo

「通常」



BCPに向け、クラウドの有効性は分かるが投資コストの増加と特定プロバイダへロックイン心配

「備え」



災害時におけるサービスの継続性が見えない。複数事業者契約など負担増も免れないのでは

「緊急」



クラウドはネットワークが崩壊しても必要な時に必要な情報を住民や事業者に提供できるのか

「復旧(興)」

省電力アクセスネットワーク基盤

ネットワークインフラが崩壊してもクラウド&センサーを連携して地域の情報をタイムリに提供できるネットワークを提供する

社会インフラとしてのクラウド

クラウドサービスは、広域災害に強く復興に有効な社会インフラとして有効。クラウドサービスが社会インフラとして活用されるためには、遠隔・周辺的环境・人・物の情報を収集し利活用できるよう、「高信頼性」、「高安全性」が求められると共に、電源供給が不安定な状況下でも長期運用可能な「対災害性」を備えることが重要。

「省電力型アクセスネットワーク制御技術」は、広域災害での情報収集に必要となる、高い信頼性や安全性を確保しつつ、省電力化された低コスト＋長期運用可能なクラウドサービスを実現する省電力アクセスネットワーク基盤。

安心・便利なサービスを社会・生活・ビジネスで活用

クラウドサービス

省電力型アクセスネットワーク制御技術により実現される社会インフラにより遠隔・周辺的环境・人・物の情報を収集

節電/データセキュリティ

防災・減災
事業継続

ホーム

オフィス

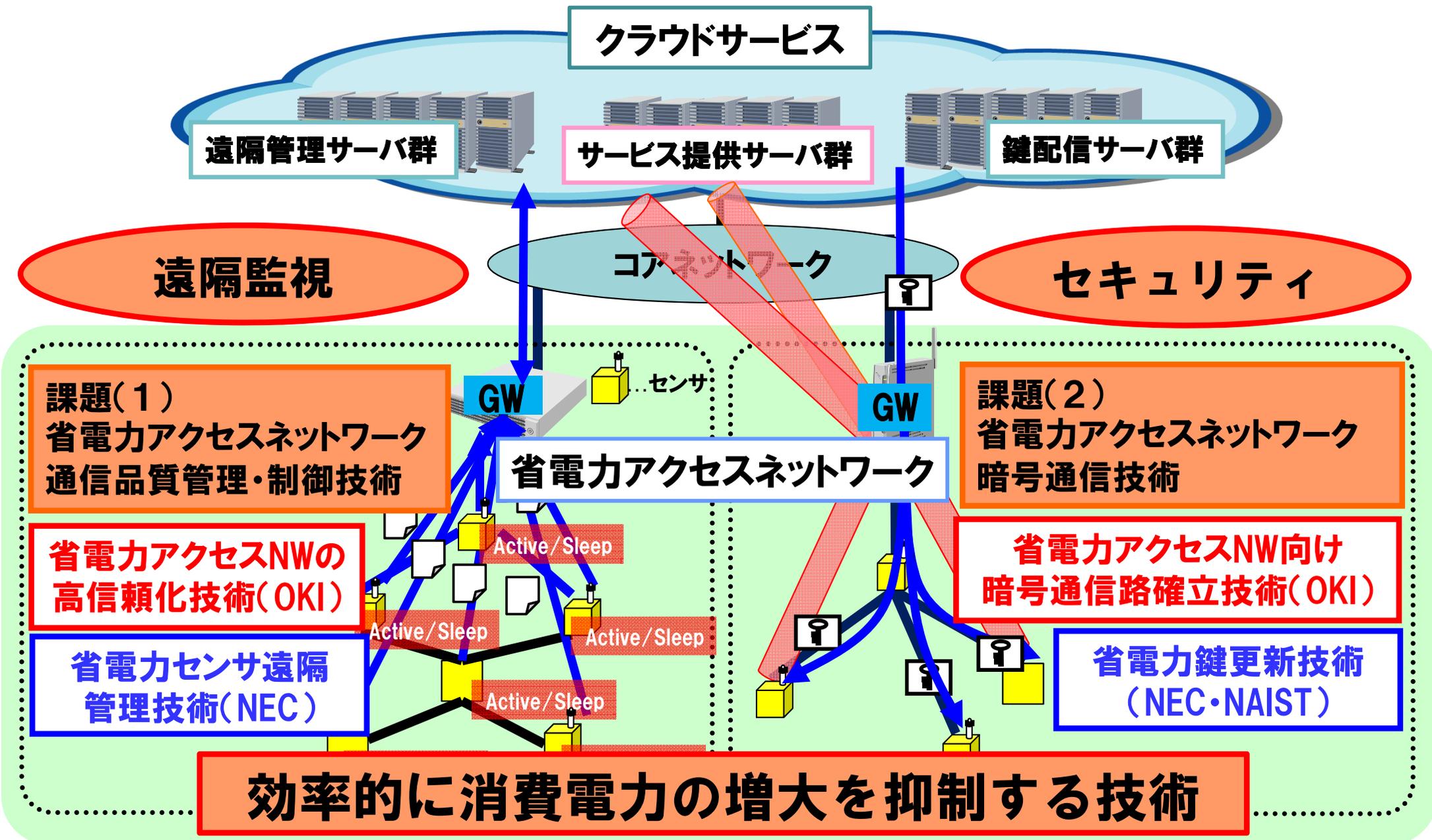
気象/災害

エネルギー

都市/インフラ

農水産業/環境

アクセスネットワークの課題



課題(1)(2)の成果連携により、従来技術に対して消費電力を50%削減する。

研究開発スケジュール

			H23年度	H24年度
課題1	省電力アクセスネットワークの高信頼化技術	沖電気工業株式会社	高信頼化技術の検討・設計、 シミュレーション評価	実機評価・検証
	省電力センサ遠隔管理技術	日本電気株式会社	省電力センサ遠隔管理方式の 設計とシミュレーション評価	省電力センサ遠隔管理 方式の開発と実証
課題2	省電力アクセスネットワーク向け暗号通信路確立技術	沖電気工業株式会社	暗号通信路確立処理代行方式の検討・設計	実機評価・検証
	省電力鍵更新技術	日本電気株式会社 奈良先端科学技術 大学院大学	アクセスNW通信量削減方式と セキュリティパラメタ決定方式の設計・実装	アクセスNW通信量削減方式と セキュリティパラメタ決定方式の評価
プロジェクト間連携			連携に向けた検討・連携	

連携評価

東北地区での実証実験 および技術成果



福島県の高等学校での実証実験(1)

・実証実験日程/場所

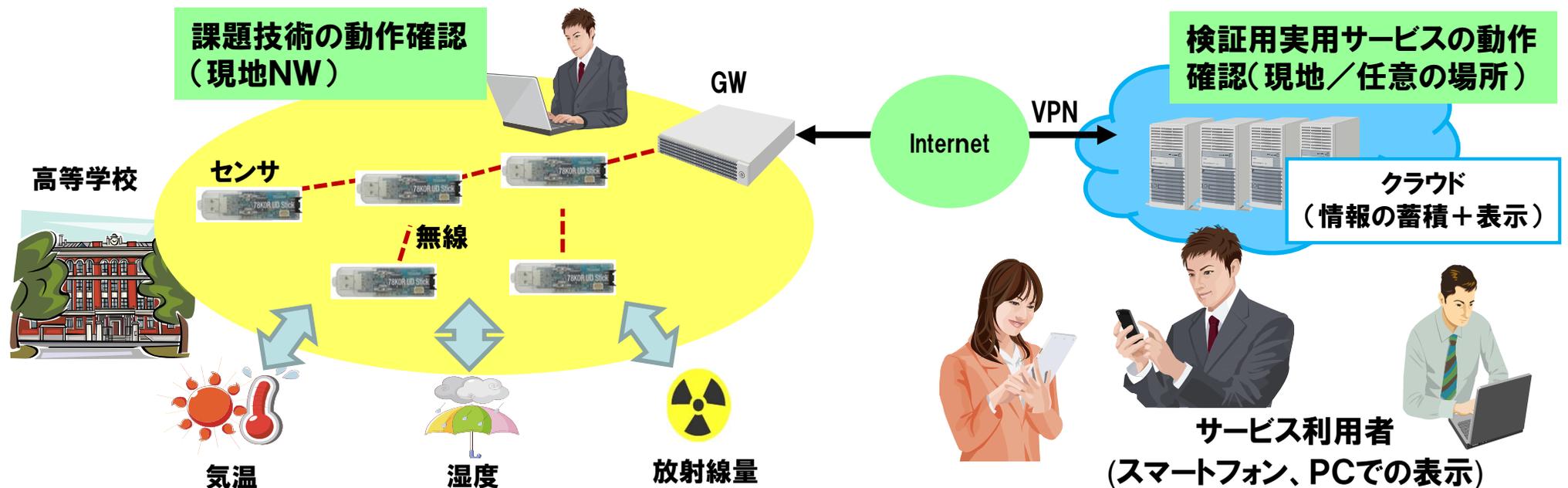
- 2012/11/12(月) ~ 2012/11/16(金)
- 福島県高等学校

・検証実験の目的

- 東北地区の復興/産業振興に貢献する社会インフラサービスを想定。検証用実用サービスの動作するネットワーク環境において、各課題技術の実用性検証を実施。

・実証実験内容

- 地方公共団体などで使用する、広域災害の発生前/中/後に役立つ環境情報(気温、湿度、放射線量)をクラウドから参照できるサービスを提供。
- 地域コミュニティとして高等学校敷地内において、スマートフォン等から環境情報を参照。



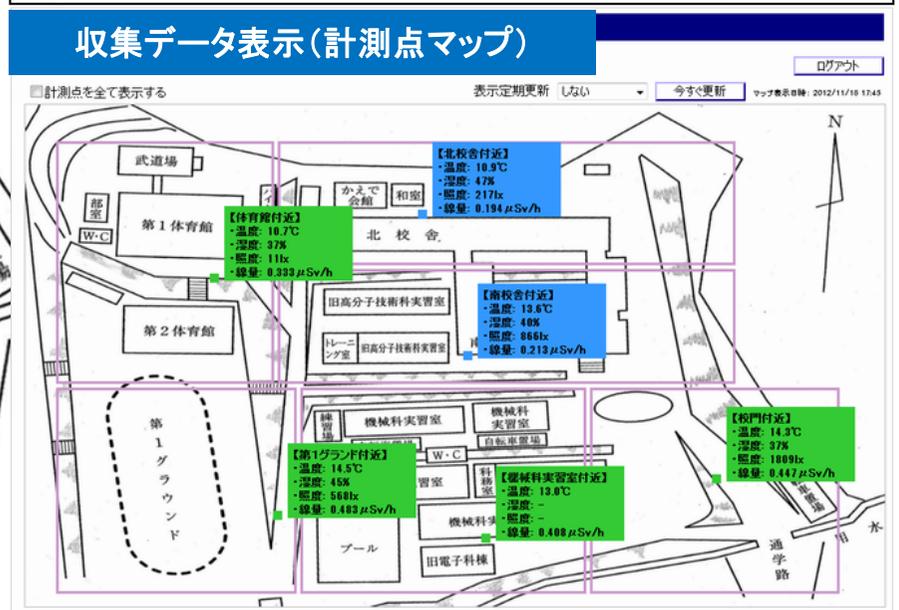
福島県の高等学校での実証実験(2)

・実証実験内容(続き)

- 敷地内に約60個の気温/照度、湿度、放射線センサを設置。
- 収集したデータはクラウド上に収集され、学校関係者にリアルタイムで提供。

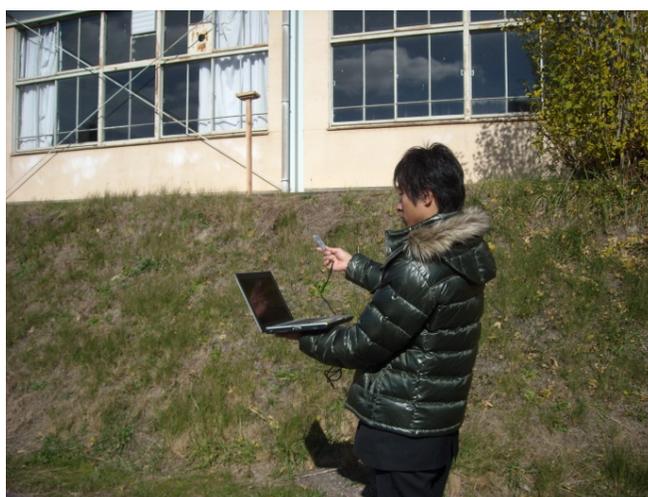
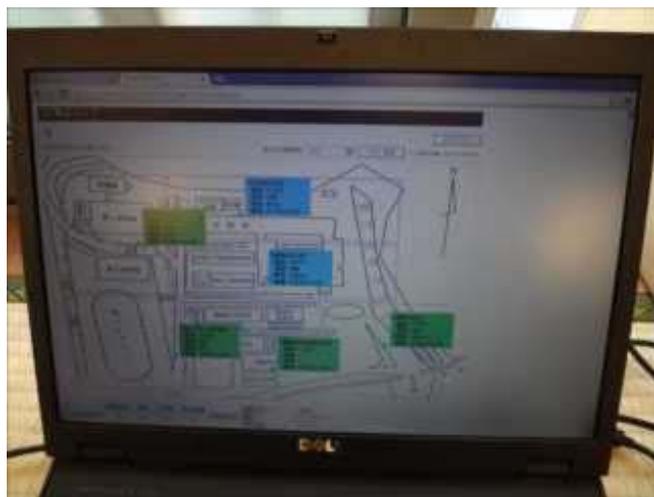


■ ■ ■ センサー設置場所



福島県の高등학교での実証実験 (3)

実証実験の様子 設置/実験



福島県の高等学校での実証実験(4)

実証実験の様子
体験学習/講演



課題(1) 省電力アクセスネットワークの高信頼化技術(1)

アクセスネットワーク内の省電力マルチホップ技術のスリープ制御を最適化し、通信の高い信頼性を保ちつつ、省電力化を実現

■ アクセスNWの省電力マルチホップ技術 無線ノードの受信待機時間の削減や、パケット送信時の制御パケット送信を削減する技術

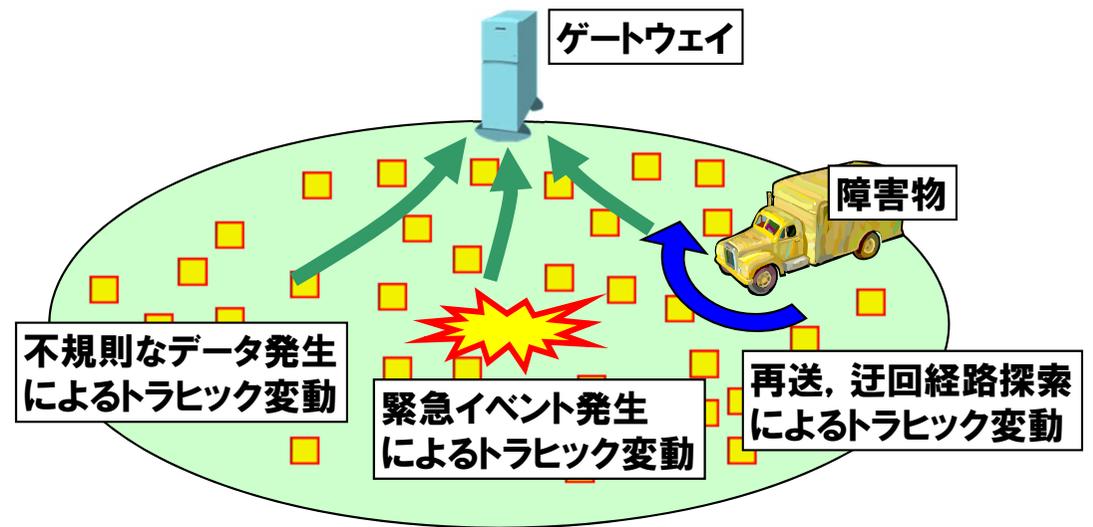
【成果】

・トラヒックの変動に応じたスリープ制御方式
アクセスネットワーク内のトラヒック変動に応じて、最適なスリープ制御パラメタを動的に決定する方式を開発し、無駄な受信待機を削減し省電力効果の高いネットワークを実現。

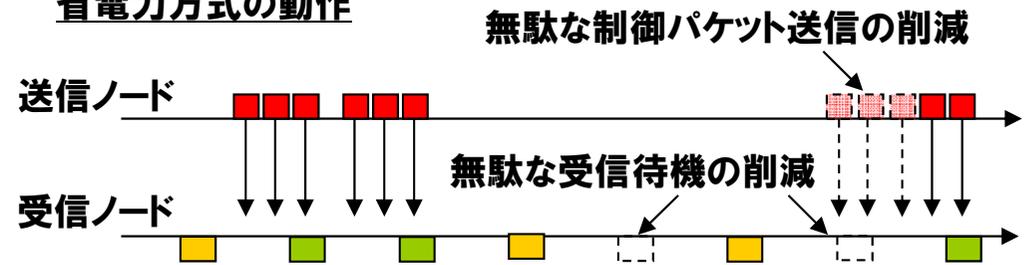
・ブロードキャスト通信時の消費電力削減方式
802.15.4e CSLを使った省電力方式において、ブロードキャスト時のコストが大きいという課題に対してスリープタイミングの同期を考慮することで、無駄な制御パケットの送信を削減し省電力化を実現。

・従来技術に対して消費電力を50%以上(最大約70%)削減(計算機シミュレーションにより確認)。

省電力アクセスネットワークのトラヒック変動

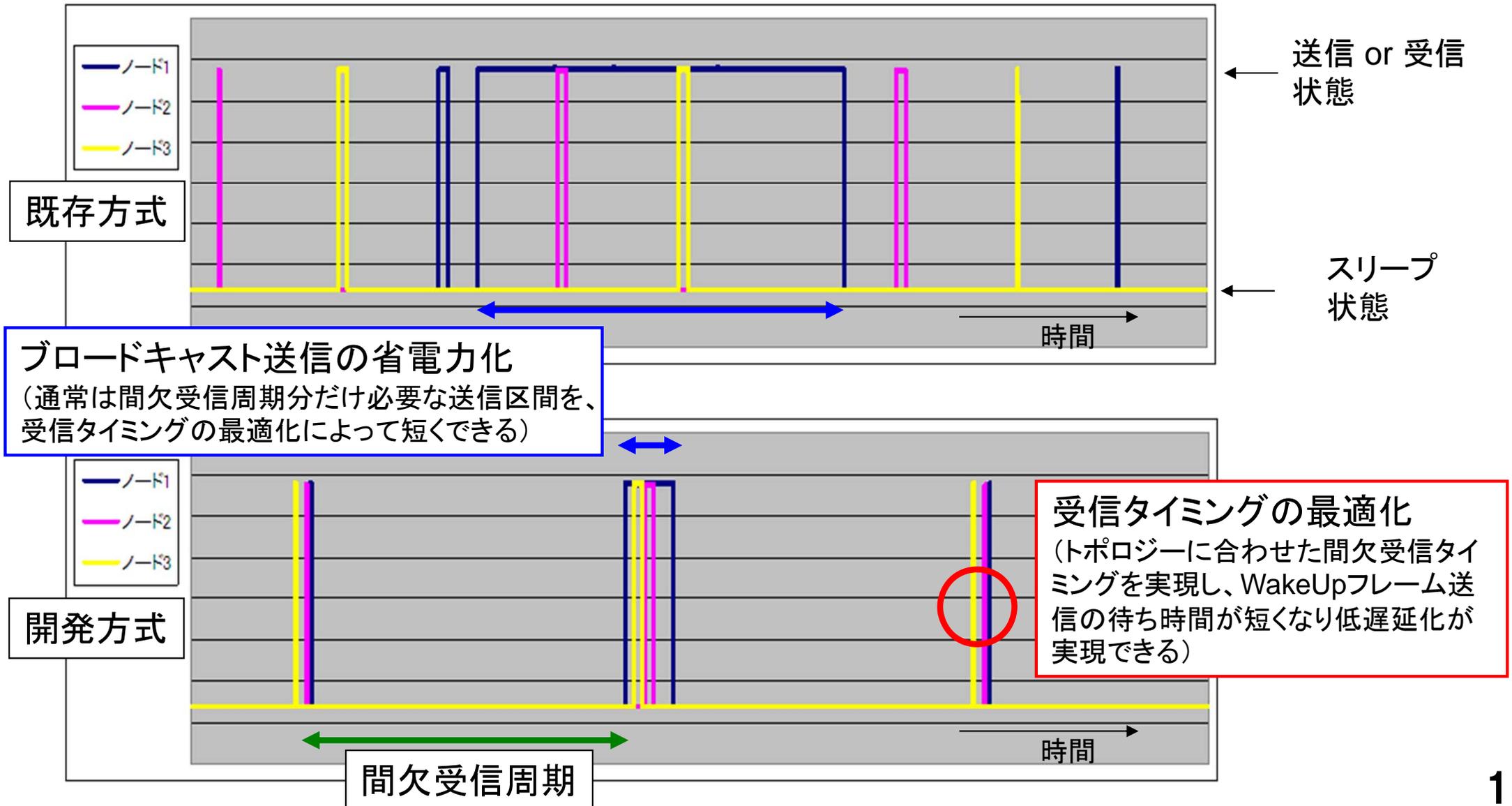


省電力方式の動作



課題(1) 省電力アクセスネットワークの高信頼化技術(2)

測定器により各無線ノードの送受信区間、スリープ区間を確認
(ノード1によるブロードキャスト送信時の動作ログ、Lowがスリープ状態)

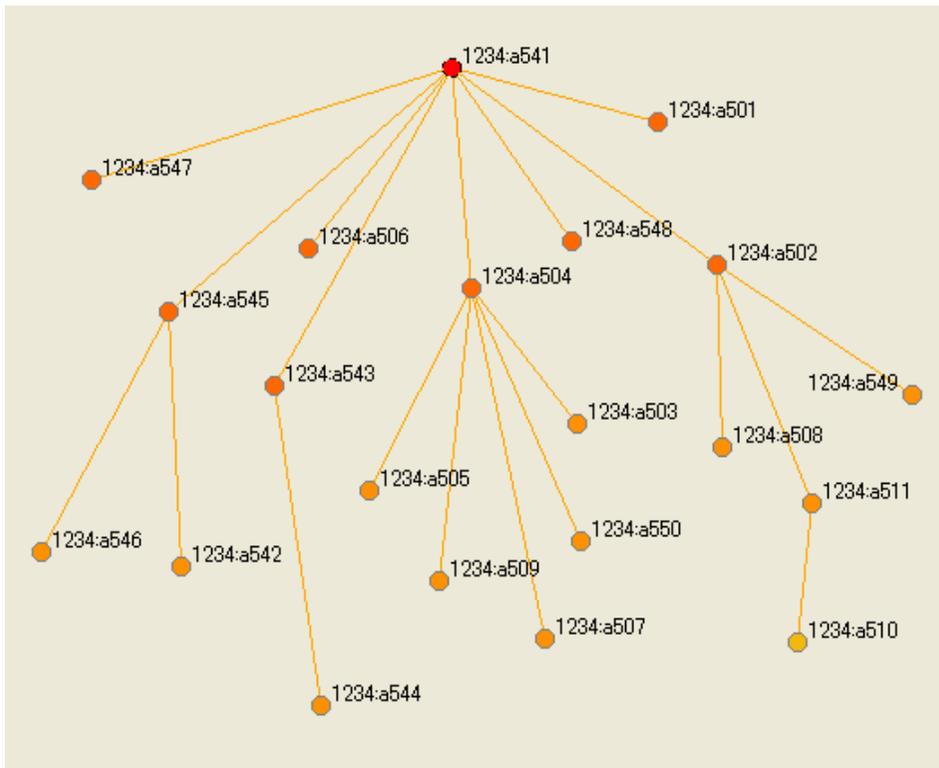


課題(1) 省電力アクセスネットワークの高信頼化技術(3)

本プロジェクトで開発した920MHz帯省電力無線機を用いて、省電力マルチホップネットワークを構成し、各ノードでスリープ時間を測定し、消費電力を確認

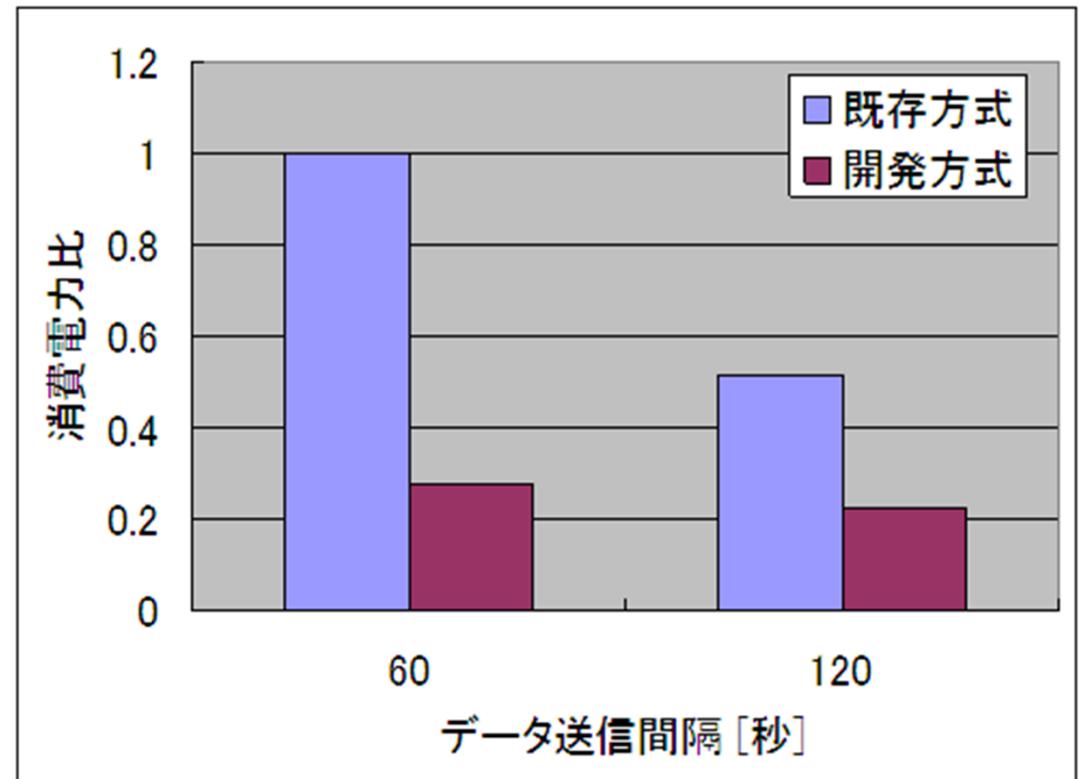
■ 実験時のネットワークポロジ

省電力マルチホップ方式を用いて、中継ノードの省電力動作と各ノードからのセンサデータの収集を確認。



■ 消費電力比較

実験結果より、本方式を用いることで、従来技術に対して消費電力を60~70%削減。



※従来技術:IEEE802.15.4e規定のCSL (Coordinated Sampled Listening)

課題(1) 省電力センサ遠隔管理技術(1)

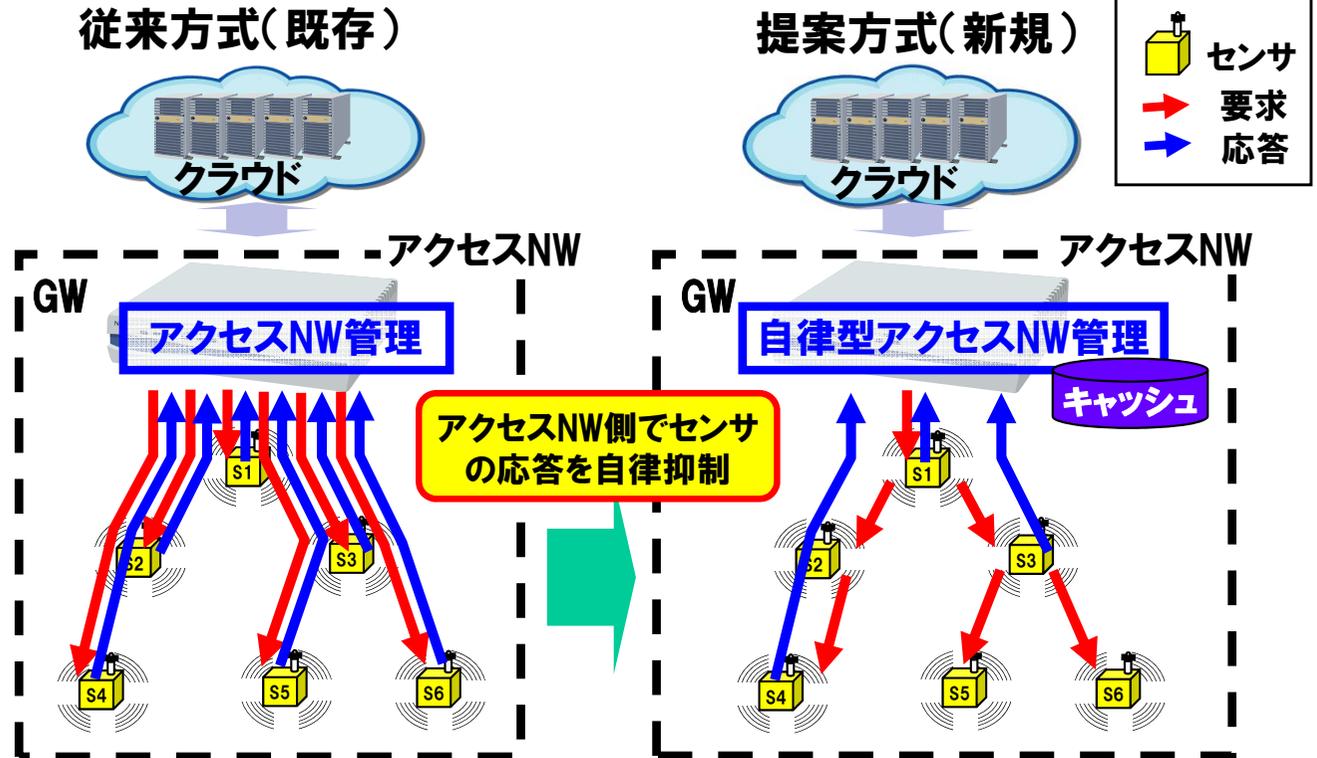
自律的にアクセスネットワークにおける管理通信効率の向上と省電力化を実現する
ゲートウェイの自律型省電力センサ遠隔管理技術を開発

■ 自律型省電力センサ遠隔管理方式

ゲートウェイのキャッシュを用いた情報補完により、センサからの応答を自律的に抑制。

【技術・成果】

- 自律的にセンサの応答を抑制し、管理通信トラフィックを低減。抑制した情報をキャッシュ情報から補完してクラウドに通知。
- 実証実験により、**実アクセスNW(センサNW)上で、提案技術の実用性と有効性を確認。**
- 従来技術に対して**消費電力を50%以上(最大約90%)削減**(計算機シミュレーションにより確認)。



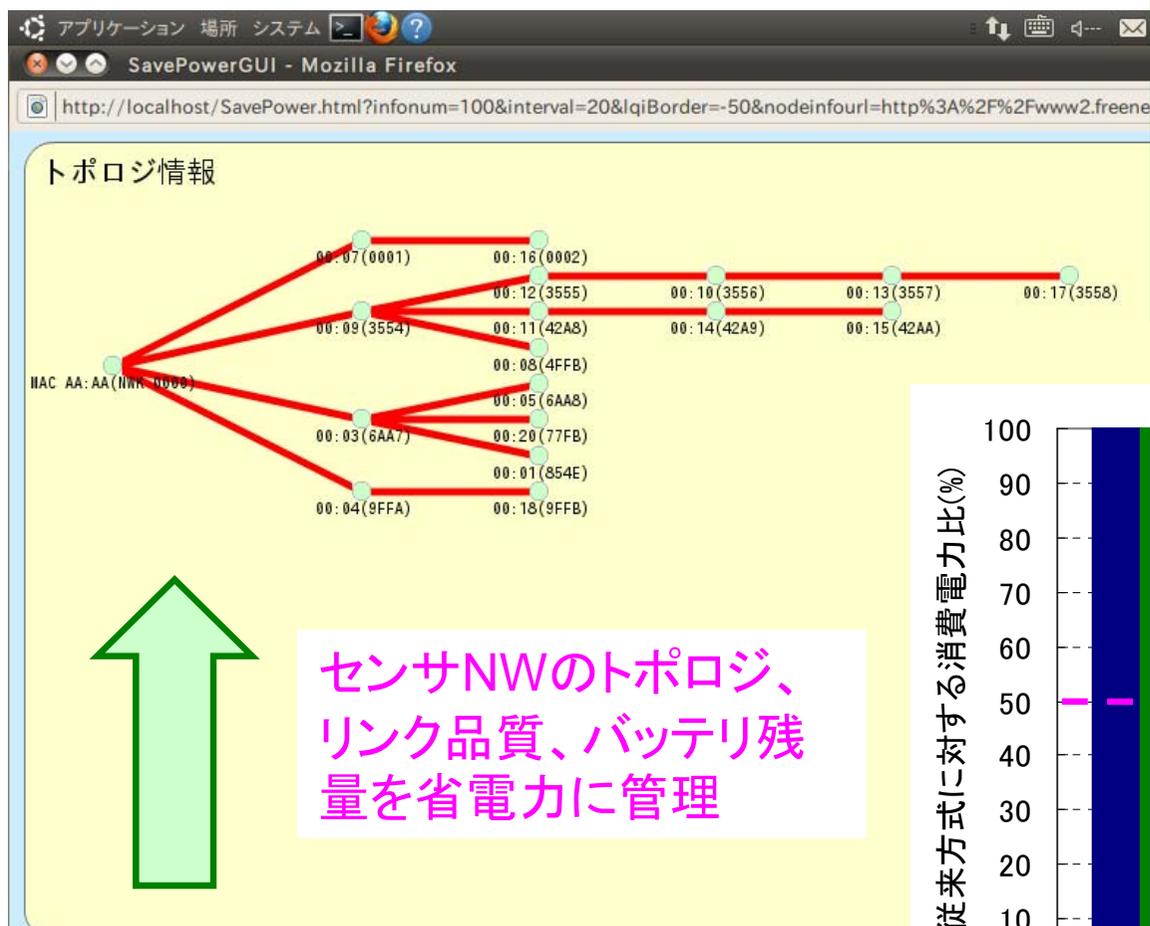
既存方式の問題点

- ・クラウドから管理要求を逐一中継するため**管理メッセージが膨大**

提案方式の特徴

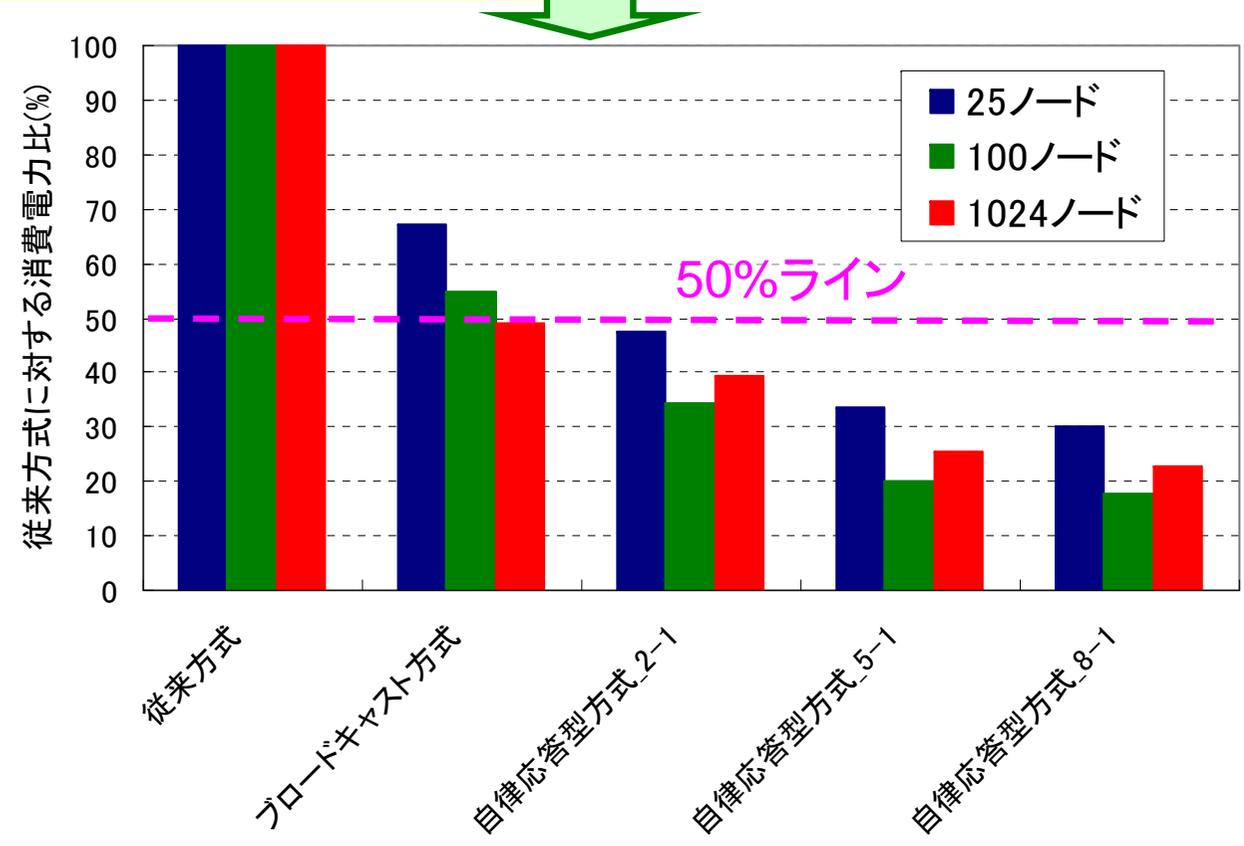
- ・ブロードキャストによる管理要求効率化
 - ・情報補完による自律的なセンサの応答抑制
- ⇒**管理メッセージ削減により省電力化**

課題(1) 省電力センサ遠隔管理技術(2)



センサNWのトポロジ、
リンク品質、バッテリー残
量を省電力に管理

● 自律機能により、省電力化と管理通信トラフィック量のトレードオフを考慮した遠隔管理で従来技術に対して消費電力を50%以上削減。(計算機シミュレーションによる評価、最大1000台規模。)

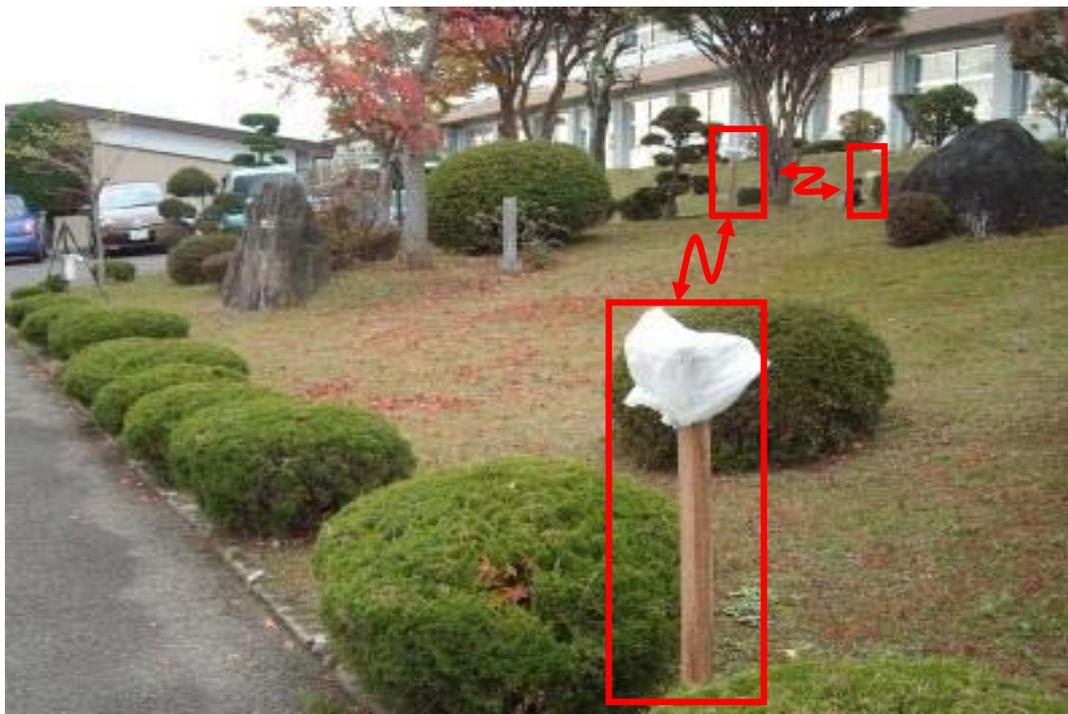


● センサNW管理が、実際の運用・構築において重要であることを再確認。
● 管理通信を抑制し、省電力管理を実現しつつも、実センサNWを的確に管理できることを確認。

※従来技術:
IP機器向けのSNMP、およびZigBee準拠の管理技術

課題(1) 省電力センサ遠隔管理技術(3)

マルチホップ通信イメージ

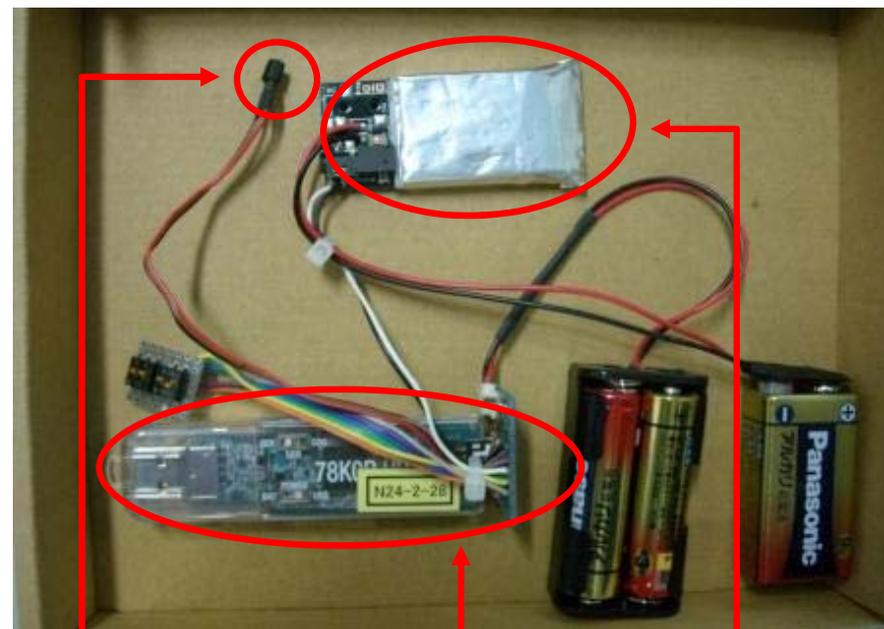


システム利用イメージ



省電力管理の確認

実証実験使用デバイス構成



温度センサ

放射線センサ

ZigBeeデバイス
(自律管理機能搭載)

センサデータ収集・閲覧サービス
(web閲覧)

課題(2) 省電力アクセスネットワーク向け暗号通信路確立技術(1)

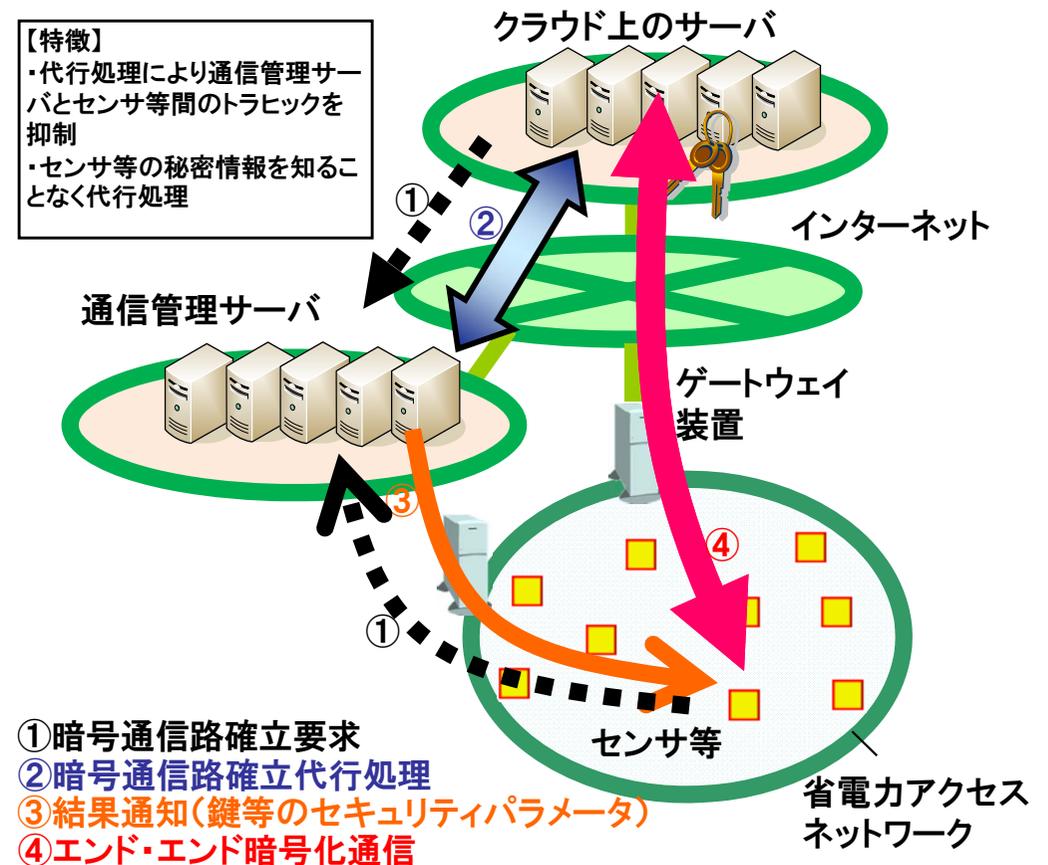
アクセスNWの通信トラヒックを抑制しつつ、クラウド上のサーバとセンサ等との間に安全性の高いエンド・エンドパスを確立する暗号通信路確立代行技術を開発

■ 暗号通信路確立代行技術

アクセスNWで汎用プロトコル (TLS, IPsec) を動作させる場合に、省電力動作の阻害要因となっていた、暗号通信路確立にかかる通信トラヒックを削減する技術。

【成果】

- ・アクセスNW外部の通信管理サーバに暗号通信路確立を代行させることにより、アクセスNWのトラヒック量を30~40%に削減。
- ・遠隔サーバにセンサ等を認証させるために必要な秘密情報を代行装置に預けることなく代行処理させることにより、クラウド等の外部の計算資源を利用する場合でも安心な代行システムを確立。
- ・従来技術に対して消費電力を50%削減(計算機シミュレーションにより確認)。

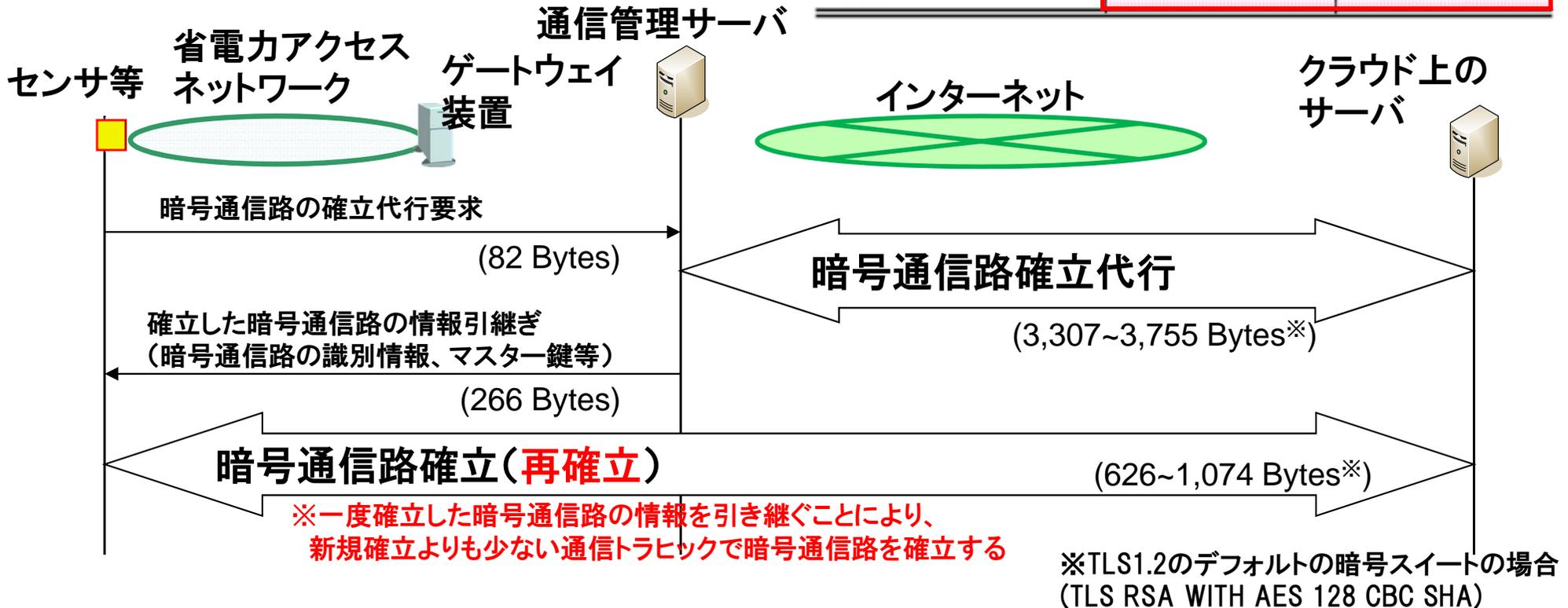


課題(2) 省電力アクセスネットワーク向け暗号通信路確立技術(2)

PC上実装プログラムによる動作確認より、無線NW部のトラフィック量削減を確認。
⇒消費電力を**50%**削減

表2: 省電力アクセスネットワークの通信量の比較

処理	通常 TLS (バイト)	代行 TLS (バイト)
暗号通信路確立要求	-	82
暗号通信路確立	3,307 ~ 3,755	-
暗号通信路確立結果	-	266
暗号通信路再確立	-	626 ~ 1,074
合計	3,307 ~ 3,755	974 ~ 1,422
比率	1	0.26 ~ 0.43



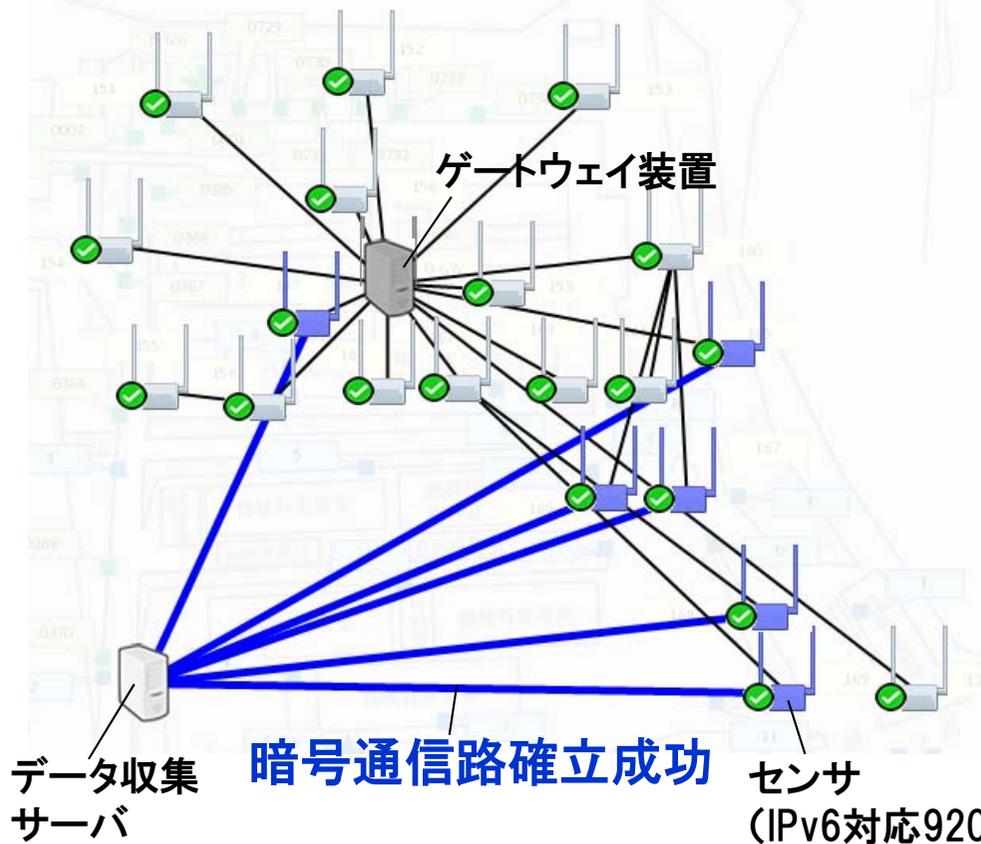
課題(2) 省電力アクセスネットワーク向け暗号通信路確立技術(3)

本プロジェクトで開発したIPv6対応920MHz帯省電力無線機20台、ゲートウェイ装置1台の構成でマルチホップネットワークを構築し技術検証

※IPv6対応によりクラウド上のサーバとインターネットを介してエンドエンドのパスを確立

■ 実験時のネットワークポロジ

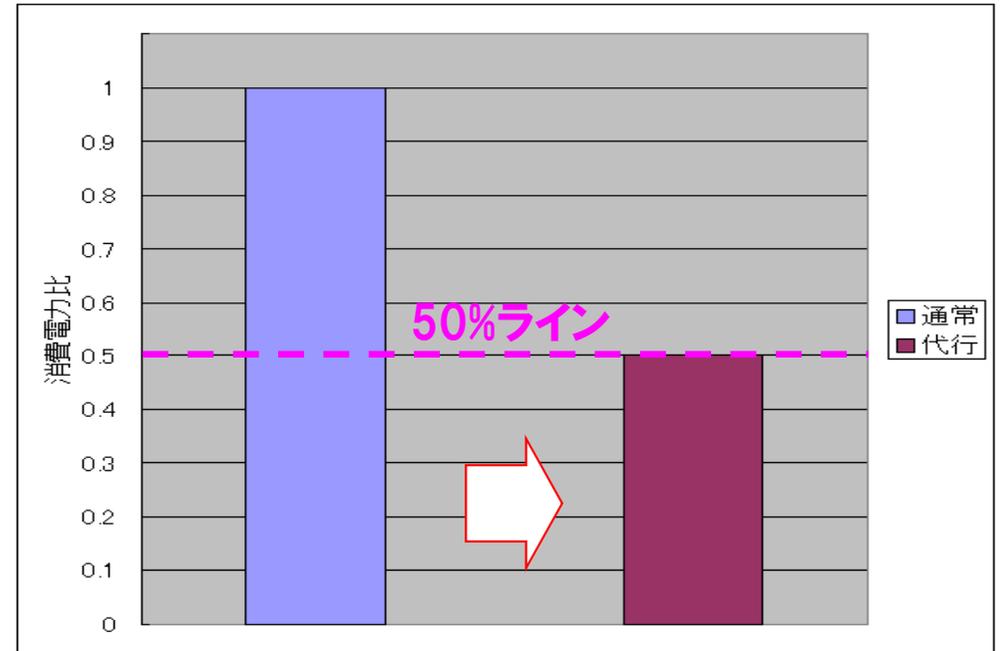
暗号通信路確立処理の代行方式を用いて、**エンド・エンドの暗号通信路**上でセンシングデータをセキュアに配送できることを確認。



■ 消費電力比較

実験結果より、本代行方式を用いることで、従来技術に対して消費電力を**50%削減**。

※従来技術:TLS (TransportLayerSecurity) を利用した暗号通信路確立技術



課題(2) 省電力暗号鍵更新技術(1)

送信元を偽る「なりすまし」やデータを偽造する「改ざん」等をされない高い信頼性を担保する**鍵更新技術**を開発(NEC). 実験的評価の正しさを数理的に確認(NAIST)

省電力暗号鍵更新技術

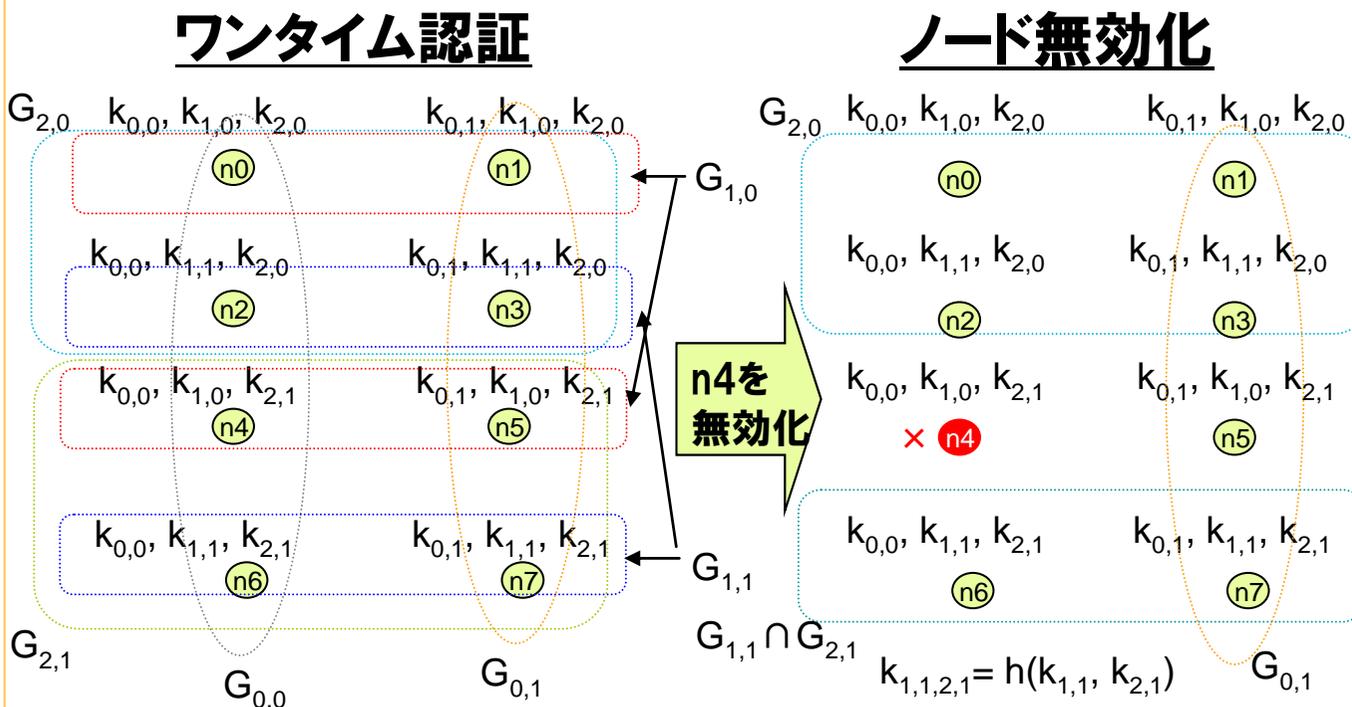
【提案技術】

●鍵更新情報の配付にかかる消費電力増加問題を、**センサ集合の包含関係を多次元的に利用**する配付方式によって解決。

【効果】

- センシング毎に鍵を更新するワンタイム認証を**従来技術に対して12%以下の通信量**で実現。
- 署名鍵の選択配付によるノード無効化の動作も確認。
- 従来技術に対して**消費電力を50%以上削減**(計算機シミュレーションにより確認)。

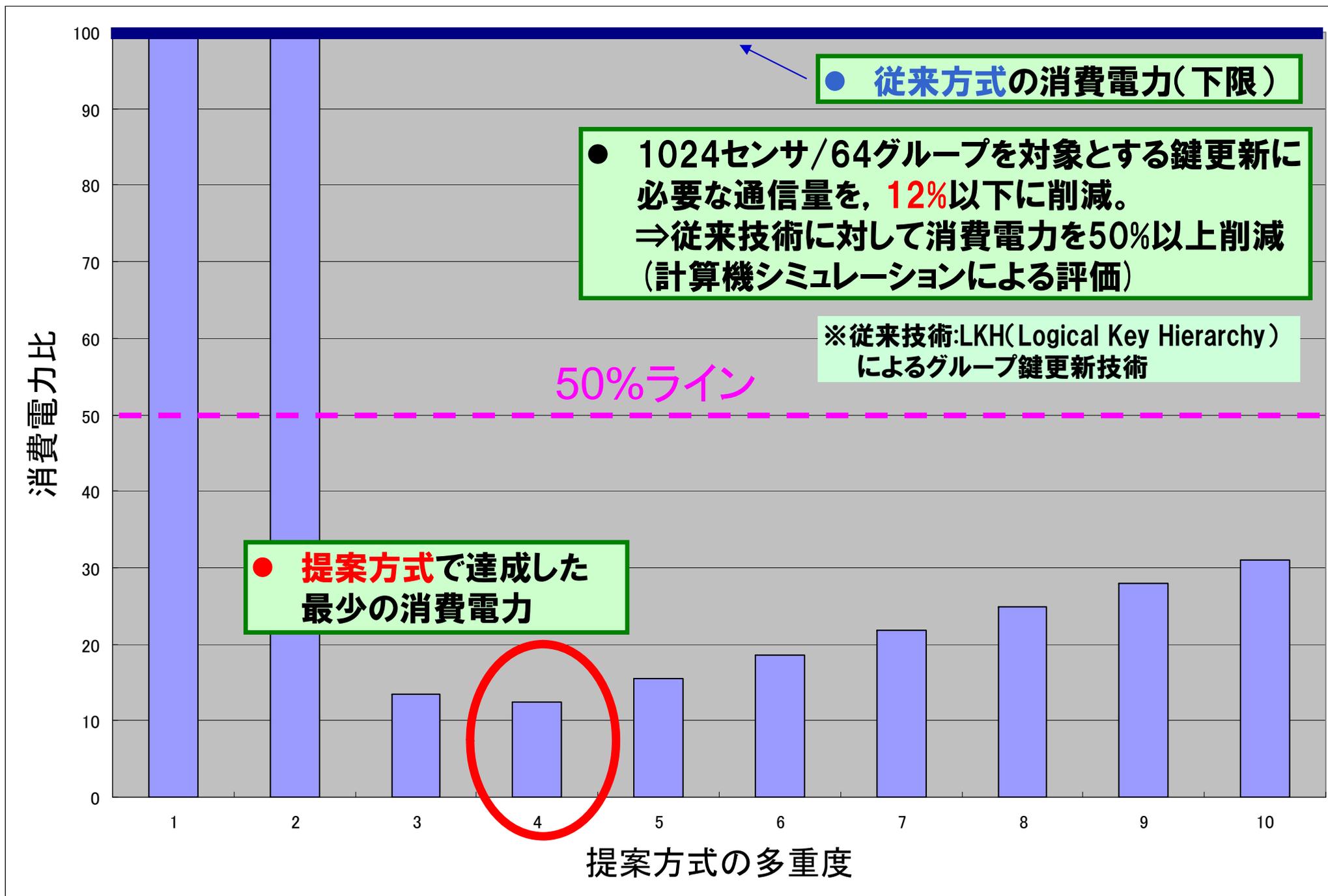
- 属性集合 $G_{i,j}$ に対応する属性鍵 $k_{i,j}$ をGW-センサ間で共有
- 鍵更新の必要なセンサを全て被覆する属性集合を n 通り決定し、 n 通りの属性鍵で署名鍵を配付 (n :**多重度**)



$k_{0,0}, k_{0,1}$ で署名鍵を暗号化して同報
 多重度に応じて他の鍵でも同報
 (例: $k_{2,0}, k_{2,1}$ 又は $k_{1,0}, k_{1,1}$ で同報)

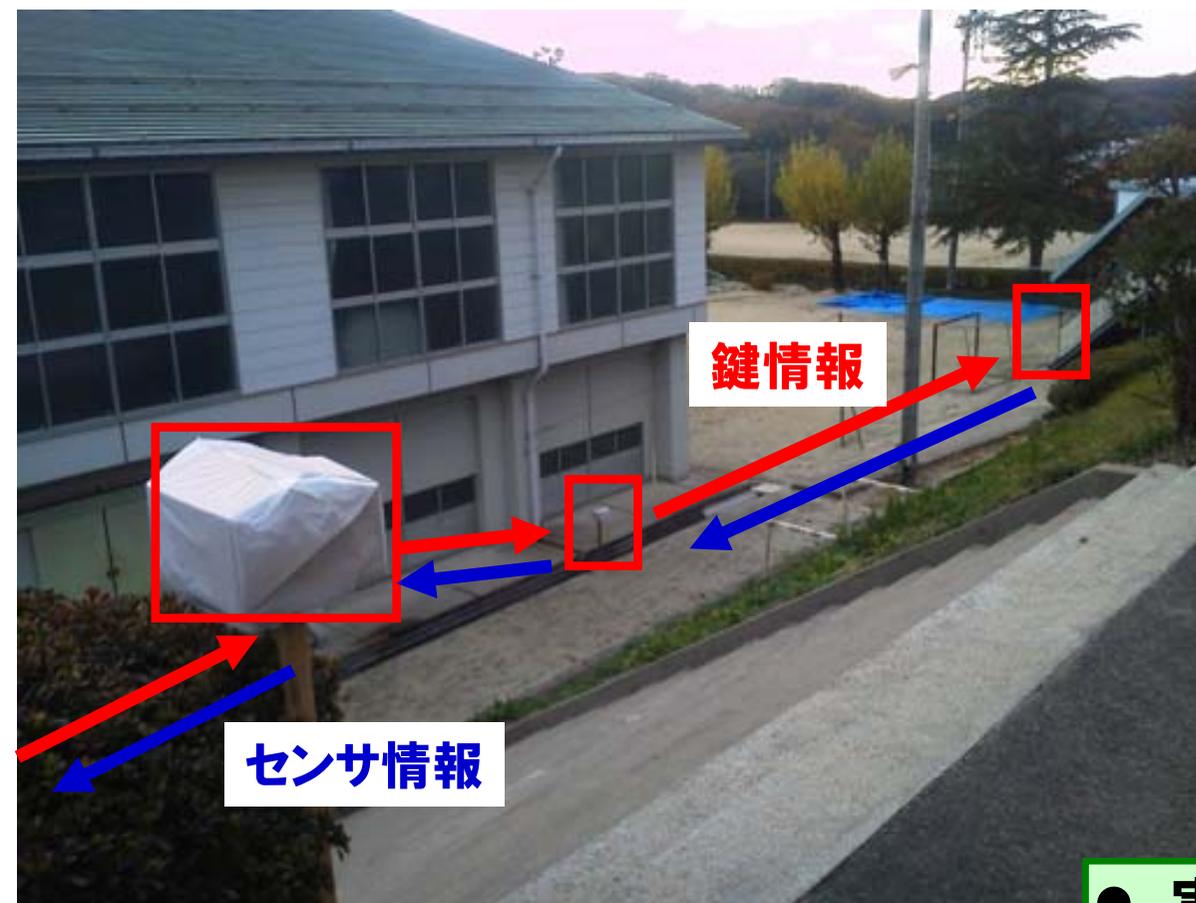
$k_{0,1}, k_{2,0}, k_{1,1,2,1}$ を
 用いて同報

課題(2) 省電力暗号鍵更新技術(2)



課題(2) 省電力暗号鍵更新技術(3)

マルチホップ通信イメージ



実証実験使用デバイス構成



- 実証実験にて、センシング毎に署名鍵を更新するワンタイム認証の運用を実現。
- 署名鍵の選択配付によるノード無効化の動作も確認。

まとめ



成果

電源供給が不安定な環境下でも、無線センサネットワークの省電力化を実現し、長期運用が可能。

遠隔管理で省電力

セキュアで省電力

課題(1)
センサ遠隔
管理機能

課題(1)
高信頼化

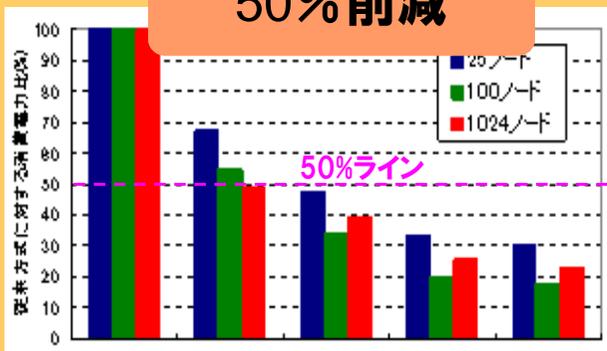
課題(2)
暗号通信
路確立

課題(1)
高信頼化

課題(2)
鍵配信
処理機能

課題(1)
高信頼化

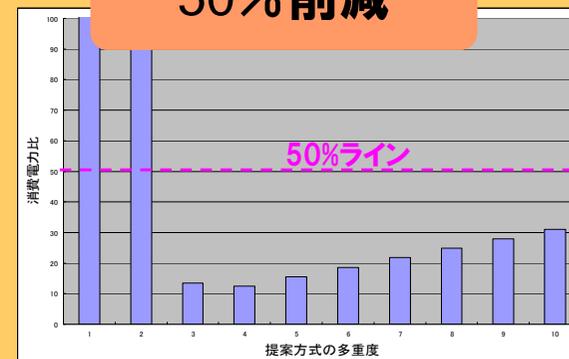
50%削減



50%削減



50%削減



実用化

		H25	H26	H27	H28
製品化 (短期)	東北被災地への環境モニタリングソリューション提案	 提案/導入			
	N大学へのセンサネットワークシステム →受注決定	 提案/導入			
製品化 (中長期)	無線センサーノード機器への 成果適用	 検討/実証実験		 製品化	
	センサネットワークサービスへの成果適用	 検討/実証実験		 製品化	

社会実装に向けて

省電力アクセスネットワーク制御技術は、災害に強いクラウドサービスを実現するアクセスネットワーク基盤として、社会インフラ分野での省電力・低コスト＋長期運用可能な無線センサネットワークを実現

被災地に有効な無線ネットワークシステム

省電力アクセスネットワーク 制御技術の適用領域

環境監視

放射線などの広域監視



施設監視

橋・道路などの公共インフラ監視



防災監視

地震・津波・火山などの観測/監視



各種クラウドサービスを提供する

高信頼クラウドサービス制御基板技術

環境対応型ネットワーク構成シグナリング技術

センサ向けクラウド/NWの省電力化と故障即時切替との連携

GW

地方公共
ネットワーク

電子行政サービス

IP電話端末・高速インターネットサービス

独居世帯支援

遠隔医療

緊急広報・防災活動

移動通信システム

今後の課題

課題	
クラウドへの接続性	クラウドへの接続が不可能になったとしても、継続的に情報収集・提供が可能な仕組みが必要。
ゲートウェイの自律分散化	ゲートウェイをSPOF (※)とせず、適切な機能分散や代行を行いながら、完全なダウンを防ぐ仕組みが必要。
センサネットワークサービスの継続性	複数無線方式 (ZigBee・無線LAN・Bluetooth) への対応。 周辺環境 (天候 / 植物の成長 / 車の通過) の影響への対応。
システム寿命とデバイスの世代交代のギャップ解消	20～30年のシステム寿命に対して、数年単位で登場する新しいデバイスをいかにシステムに取り込み、利活用するか。

※SPOF (Single Point of Failure)