

## 第三章

# 畜産物情報追跡管理システム及び 農産物情報追跡管理システムの 実証実験

## 1 モバイル IPv6 による個体識別・状態監視（プレゼンス）管理技術

### 1.1 実験要求事項

#### (1) CoA アドレスとホームアドレスの適切な対応付け

移動先にて付与された CoA アドレス(以下、CoA)とホームアドレス(以下、HoA)の対応付けについて、IPv6 温度センサーが移動先で接続した際、CoA がホームエージェント(HA)及びコレスポンデントノード(CN)に通知され、ホームエージェントのバインディングキャッシュ(BC)が更新されることを検証する。

#### (2) 状態変化の保持

牛個体の状態(プレゼンス)を変化させ、変化後の値がプレゼンスサーバに通知されて、最新の値が保持できることを検証する。

#### (3) 状態変化の取得

牛個体の状態を変化させ、任意にプレゼンスサーバから最新の値が取得できることを検証する。

#### (4) 位置情報の取得

牛個体を移動させ、同一の IPv6 アドレスに関連付けられた CoA から、位置情報を取得できることを検証する。

## 1.2 実験仕様、手順

### (1) CoA と HoA の適切な対応付け

IPv6 温度センサーを「場所 1」に配置し、電源を on にする。

追跡管理 MIPv6 装置(HA)のコンソールで以下のコマンドにより BC の状態を確認する。

```
% mip6control c
```

ここで、IPv6 温度センサーの HoA (実際には名前解決によりホスト名が表示) と「場所 1」の Prefix を持った CoA が出力されることを確認する。

IPv6 温度センサーを「場所 2」へ移動させる。

一定時間(IPv6 温度センサーの処理間隔)経過後、と同じ手順で BC の状態を確認する。

```
% mip6control c
```

ここで、IPv6 温度センサーの HoA (実際には名前解決によりホスト名が表示) と「場所 2」の Prefix を持った CoA が出力されることを確認する。

### (2) 状態変化の保持

IPv6 温度センサーの電源を on にする。

追跡管理基本装置のコンソールで以下のコマンドによりデータベース内の最新の温度を確認する。

```
% sudo u tomcat4 s
```

```
tomcat4% psql epro
```

```
epro=> select * from cattleheathistory;
```

ここで、最新の温度を記録しておく。

IPv6 温度センサーを手で包み、センサ部の周囲の温度を上昇させる。

一定時間 (IPv6 温度センサーの処理間隔) 経過後、と同じ手順でデータベース内の最新の温度を確認する。

```
% sudo u tomcat4 s
```

```
tomcat4% psql epro
```

```
epro=> select * from cattleheathistory;
```

ここで、最新の温度を確認し、状態変化が記録されていることを確認する。

### (3) 状態変化の取得

IPv6 温度センサーの電源を on にし、スリープ間隔を最短 (1 分) にする。

追跡情報表示装置から追跡管理基本装置にブラウザでアクセスし、最新の温度が取得できることを確認する。

```
http://ushituisseki-sv.agri-epro.jp/cattle/UC-012/inputip.jsp
```

にアクセスし、「牛肉 ID」に IPv6 温度センサーのモバイル IPv6 ホームアドレス (以下、MIPv6 HoA) を入力し、「検索」ボタンを押す。次に「と畜前体温履歴」、「日時履歴」、「実測値」の順にボタンを押す。

ここで、最新の温度を記録しておく。

IPv6 温度センサーを手で包み、センサ部の周囲の温度を上昇させる。  
一定時間（IPv6 温度センサーの処理間隔）経過後、と同じ手順により、追跡情報表示装置で最新の値が取得できることを確認する。

<http://ushituisseki-sv.agri-epro.jp/cattle/UC-012/inputip.jsp>  
にアクセスし、「牛肉 ID」に IPv6 温度センサーの MIPv6 HoA を入力し、「検索」ボタンを押す。次に「と畜前体温履歴」、「日時履歴」、「実測値」の順にボタンを押す。

ここで、最新の温度を確認し、状態変化を取得できることを確認する。

#### (4) 位置情報の取得

IPv6 温度センサーを「場所 1」に配置し、電源を on にする。

追跡情報表示装置から追跡管理基本装置にブラウザでアクセスし、現在の位置情報が「場所 1」であることを確認する。

<http://ushituisseki-sv.agri-epro.jp/cattle/UC-012/inputip.jsp>  
にアクセスし、「牛肉 ID」に IPv6 温度センサーの MIPv6 HoA を入力し、「検索」ボタンを押す。次に、「位置履歴」ボタンを押す。

ここで、現在の位置を記録しておく。

IPv6 温度センサーを「場所 2」へ移動させる。

一定時間（IPv6 温度センサーの処理間隔）経過後、と同じ手順により、追跡情報表示装置で、現在の位置情報が「場所 2」であることを確認する。

<http://ushituisseki-sv.agri-epro.jp/cattle/UC-012/inputip.jsp>  
にアクセスし、「牛肉 ID」に IPv6 温度センサーの MIPv6 HoA を入力し、「検索」ボタンを押す。次に、「位置履歴」ボタンを押す。

ここで、位置情報の取得が行われていることを確認する。

### 1.3 実験実施環境

#### (1) 実験実施場所

NEC エンジニアリング社内（NEC 横浜技術センター）

#### (2) 実験実施環境構成図

1.2 項(1)～(4)の実験を実施した実験環境の構成図を図 3-1-1 に示す。

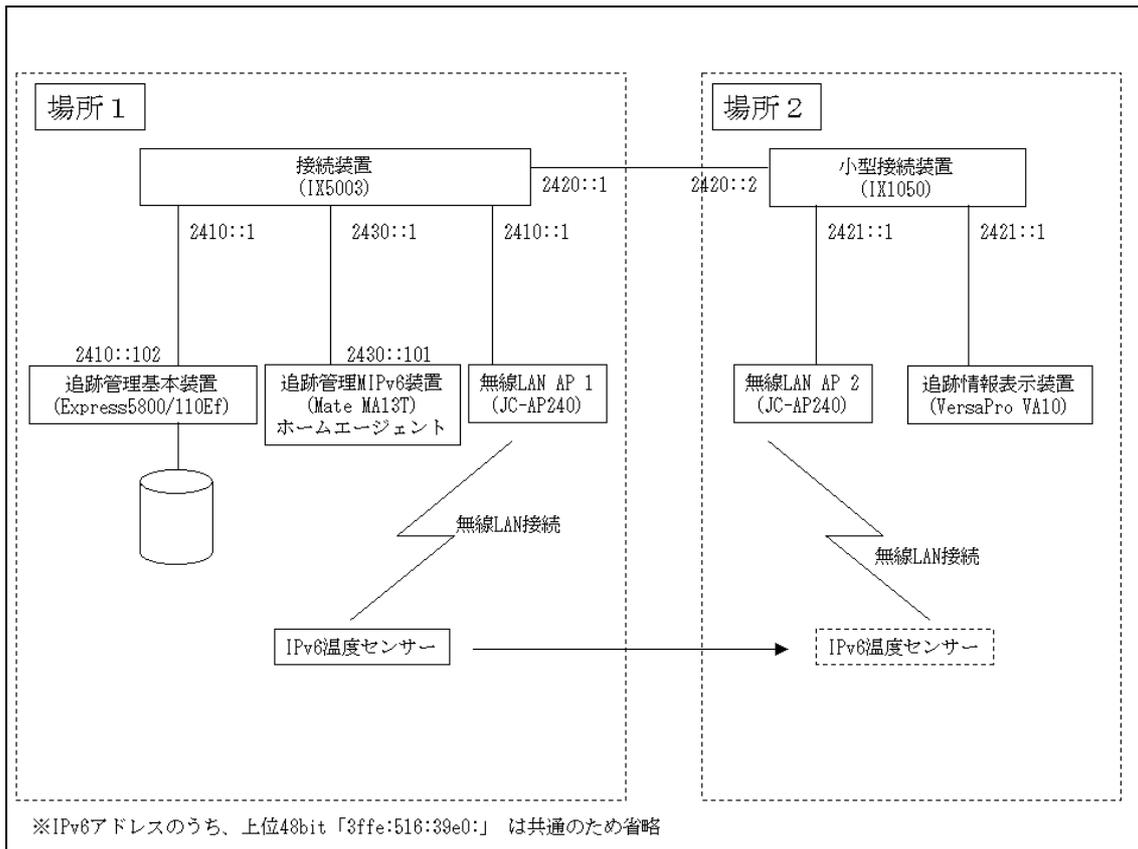


図 3-1-1 実験実施環境構成図

図 3-1-1 を説明する。「場所 1」と「場所 2」はそれぞれ「岐阜県モデル牧場（岐阜県畜産研究所）」と「食肉流通センター（食肉センター）」を想定しており、各機材及び IPv6 アドレス体系は現地と同じ構成としている。

「場所 1」のネットワーク Prefix は「3ffe:516:39e0:2410」となり、「場所 2」のネットワーク Prefix は「3ffe:516:39e0:2421」となる。

また、「場所 1」と「場所 2」は、無線 LAN の範囲が物理的に重複するため、常にどちらかのアクセスポイントの電源を off にすることで、IPv6 温度センサーの移動実験を可能としている。

(1)～(4)の実験で使用した IPv6 温度センサーは以下の表 3-1-1 の通りである。

表 3-1-1 実験に使用した IPv6 温度センサー

実験仕様	IPv6 温度センサーのホスト名	IPv6 温度センサーの MIPv6 HoA
(1)	sensor11	3ffe:516:39e0:2430:260:b3ff:fe6a:ec94
(2)	sensor22	3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f
(3)	sensor22	3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f
(4)	sensor22	3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f

## 1.4 実験実施結果

### (1) CoA アドレスと HoA アドレスの適切な関連付け

IPv6 温度センサーを「場所 1」に配置し、電源を on にする。

追跡管理 MIPv6 装置(HA)のコンソールで以下のコマンドにより BC の状態を確認する。

```
% mip6control c
```

< コマンド実行結果 >						
phaddr			pcoa	flags	seqno	lifetim
	addr	ltxp	state			
sensor11						
	3ffe:516:39e0:2410:260:b3ff:fe6a:ec94					
	3ffe:516:39e0:2430:203:47ff:fee2:1e68	AHSD--		3431	416	351
	---					

コマンド実行結果を解説する。実行結果の 1 行目から 3 行目まではタイトルであり、4 行目から 6 行目までがタイトルに対するデータとなる。1 行目タイトルの phaddr に対する 4 行目の「sensor11」が本実験で使用した IPv6 温度センサーのホスト名で、タイトルの pcoa に対する 5 行目の「3ffe:516:39e0:2410:260:b3ff:fe6a:ec94」が CoA である。CoA のネットワーク Prefix が「場所 1」のネットワーク Prefix である「3ffe:516:39e0:2410」と一致していることが分かる。IPv6 温度センサーを場所 2 へ移動させる。

一定時間(IPv6 温度センサーの処理間隔)経過後、と同じ手順で BC の状態を確認する。

```
% mip6control c
```

< コマンド実行結果 >							
phaddr			pcoa	flags	seqno	lifetim	ltxp
	addr	state					
sensor11							
	3ffe:516:39e0:2421:260:b3ff:fe6a:ec94						
	3ffe:516:39e0:2430:203:47ff:fee2:1e68	AHSD--		6768	416	389	
	---						

コマンド実行結果を解説する。IPv6 温度センサーのホスト名「sensor11」に対する CoA が「3ffe:516:39e0:2421:260:b3ff:fe6a:ec94」に変わっており、これは「場所 2」のネットワーク Prefix「3ffe:516:39e0:2421」と一致していることが分かる。

この結果より、IPv6 温度センサーの移動に応じて HA の BC が更新されることが確認できた。

(2) 状態変化の保持

IPv6 温度センサーの電源を on にする。

追跡管理基本装置のコンソールで以下のコマンドによりデータベース内の最新の温度を確認する。

```
% sudo u tomcat4 s
tomcat4% psql epro
epro=> select * from cattleheathistory;
```

< コマンド実行結果 >

mipv6hoa	tod
animalheat   comment	
-----+-----	
+-----+-----	
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC95	2003-02-04 16:10:49+09
-273	
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC95	2003-02-04 16:53:43+09
24.56	
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC95	2003-02-04 17:01:07+09
24.56	
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC94	2003-02-04 17:02:58+09
-273	
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC94	2003-02-04 17:03:03+09
-273	
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC94	2003-02-04 17:07:23+09
23.44	
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC94	2003-02-04 17:07:24+09
23.44	
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC95	2003-02-04 17:07:41+09
24.37	
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC95	2003-02-04 18:03:36+09
24.66	
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC94	2003-02-04 18:03:38+09
33.7	
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC95	2003-02-04 18:14:33+09
24.56	
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC94	2003-02-04 18:14:36+09
24.52	
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC95	2003-02-04 18:31:02+09
24.47	
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC95	2003-02-04 18:31:03+09
24.47	
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC95	2003-02-04 18:31:37+09
24.47	
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC94	2003-02-04 18:31:40+09
25.1	
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC9F	2003-02-04 18:32:49+09
25.05	

(17 rows)

コマンド実行結果を解説する。このコマンドにより、追跡管理基本装置内のデータベースの情報を表示している。実行結果の1行目~2行目はタイトルであり、4行目以下がデータとなる。タイトル mipv6hoa は IPv6 温度センサーの MIPv6 HoA であり、tod は温度を取得した時刻、animalheat は計測温度である。データの最終行の mipv6hoa 「3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f」はこの実験で使用した IPv6 温度センサーであり、2003年2月4日18時32分49秒に25.05 を計測していることが分かる。

IPv6 温度センサーを手で包み、センサ部の周囲の温度を上昇させる。

一定時間 (IPv6 温度センサーの処理間隔) 経過後、と同じ手順でデータベース内の最新の温度を確認する。

```
% sudo u tomcat4 s
tomcat4% psql epro
epro=> select * from cattleheathistory;
```

< コマンド実行結果 >			
mipv6hoa		tod	
animalheat	comment		
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC95		2003-02-04 16:10:49+09	
-273			
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC95		2003-02-04 16:53:43+09	
24.56			
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC95		2003-02-04 17:01:07+09	
24.56			
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC94		2003-02-04 17:02:58+09	
-273			
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC94		2003-02-04 17:03:03+09	
-273			
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC94		2003-02-04 17:07:23+09	
23.44			
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC94		2003-02-04 17:07:24+09	
23.44			
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC95		2003-02-04 17:07:41+09	
24.37			
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC95		2003-02-04 18:03:36+09	
24.66			
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC94		2003-02-04 18:03:38+09	
33.7			
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC95		2003-02-04 18:14:33+09	
24.56			
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC94		2003-02-04 18:14:36+09	
24.52			
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC95		2003-02-04 18:31:02+09	
24.47			
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC95		2003-02-04 18:31:03+09	
24.47			

3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC95		2003-02-04	18:31:37+09	
24.47				
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC94		2003-02-04	18:31:40+09	
25.1				
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC9F		2003-02-04	18:32:49+09	
25.05				
3FFE:0516:39E0:2430:0260:B3FF:FE6A:EC9F		2003-02-04	18:41:43+09	
29.5				
(18 rows)				

コマンド実行結果を解説する。 項のデータと比較すると、最終行に同じ IPv6 温度センサーの最新のデータが追加されていることが分かる。同日の 18 時 41 分 43 秒に 29.5 を記録しており、温度変化を正常に記録していることが分かる。

この結果より、牛の状態変化をプレゼンスサーバに通知し、状態変化を正常に保持できることが確認できた。

### (3) 状態変化の取得

IPv6 温度センサーの電源を on にし、スリープ間隔を最短（1分）にする。  
追跡情報表示装置から追跡管理基本装置にブラウザでアクセスし、最新の温度が取得できることを確認する。

<http://ushituisseki-sv.agri-epro.jp/cattle/UC-012/inputip.jsp>

にアクセスし、「牛肉 ID」に IPv6 温度センサーの MIPv6 HoA を入力し、「検索」ボタンを押す。次に「と畜前体温履歴」、「日時履歴」、「実測値」の順にボタンを押す。

<コマンド実行結果> 図 3-1-2 参照

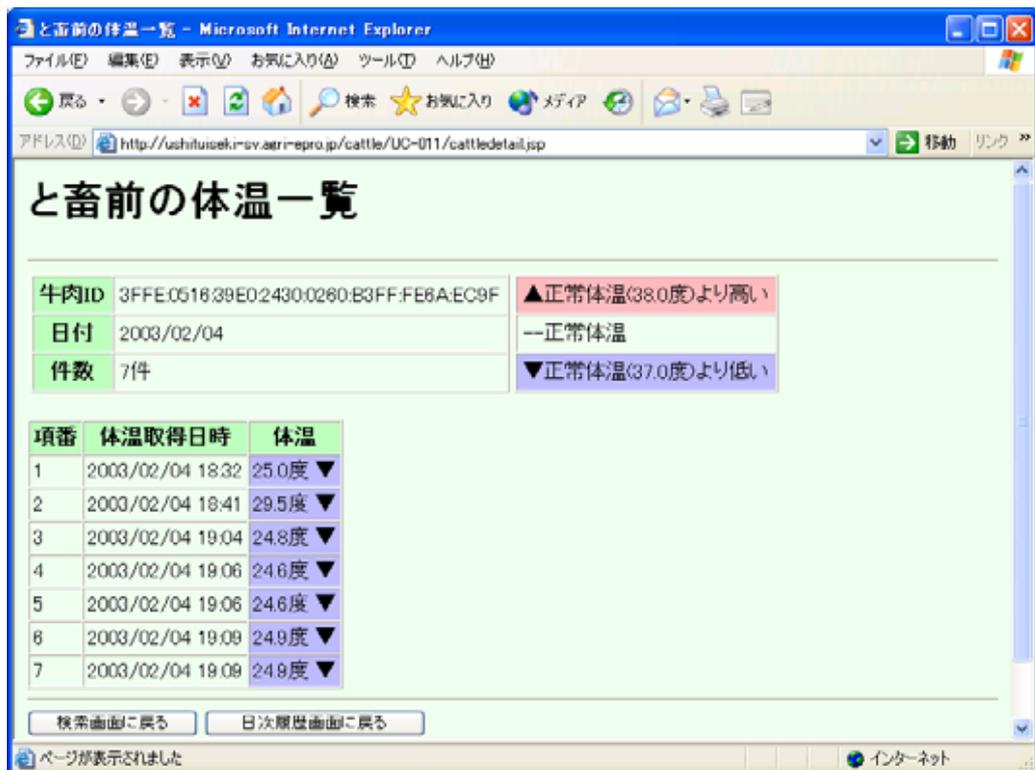


図 3-1-2 状態変化前の温度履歴

コマンド実行結果を説明する。HoA が「3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f」の IPv6 温度センサーのデータを取得している。2003 年 2 月 4 日 19:09 に 24.9 を記録していることが分かる。

IPv6 温度センサーを手で包み、センサー部の周囲の温度を上昇させる。

一定時間（IPv6 温度センサーの処理間隔）経過後、と同じ手順により、追跡情報表示装置で最新の値が取得できることを確認する。

<http://ushituisseki-sv.agri-epro.jp/cattle/UC-012/inputip.jsp>

にアクセスし、「牛肉 ID」に IPv6 温度センサーの MIPv6 HoA を入力し、「検索」ボタンを押す。次に「と畜前体温履歴」、「日時履歴」、「実測値」の順にボタンを押す。

<コマンド実行結果> 図 3-1-3 参照

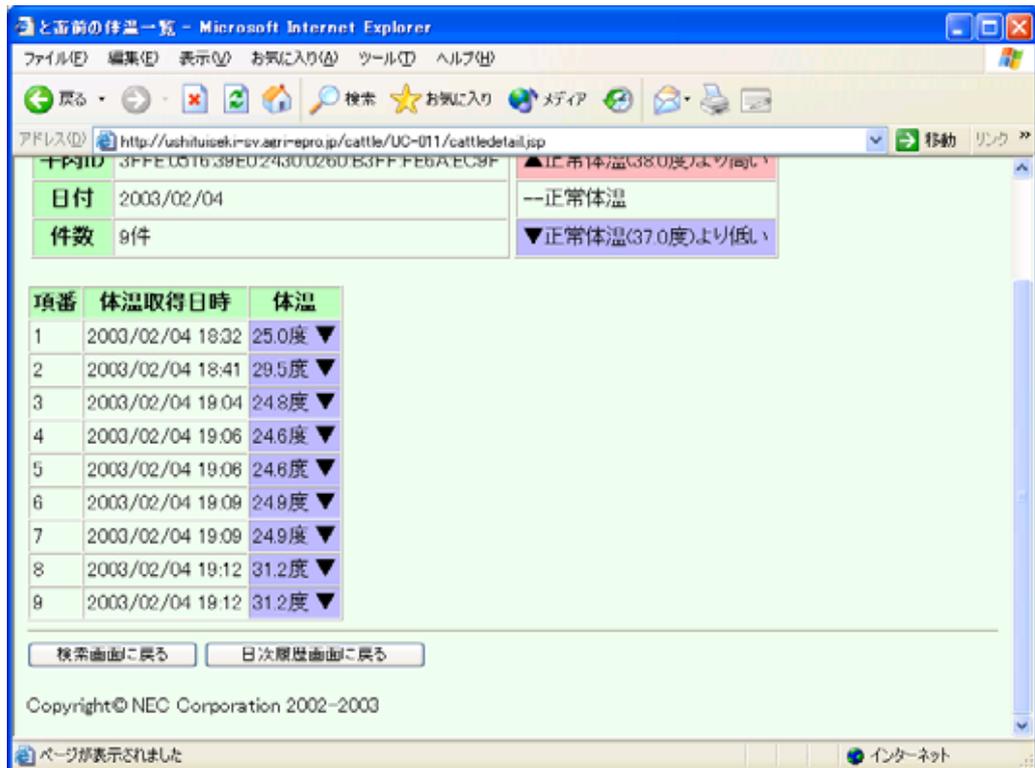


図 3-1-3 状態変化後の温度履歴

コマンド実行結果を説明する。HoA が「3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f」の IPv6 温度センサーのデータを取得しているが、項のデータと比較すると、19 時 12 分に最新の温度データを取得していることが分かる。項の最新データは 19 時 9 分であり、スリープ間隔と各種動作時間を合わせて約 3 分で最新のデータを取得している。この 3 分間隔というのは、牛の体温変化で見た場合、充分連続的な値と考えられることから、擬似的にはあるが任意のタイミングで最新の値を取得していると言える。

この結果より、牛個体の状態変化に対して、任意にプレゼンスサーバから最新の値を取得できることが確認できた。

#### (4)位置情報の取得

IPv6 温度センサーを「場所 1」に配置し、電源を on にする。

追跡情報表示装置から追跡管理基本装置にブラウザでアクセスし、現在の位置情報が「場所 1」であることを確認する。

<http://ushituisseki-sv.agri-epro.jp/cattle/UC-012/inputip.jsp>

にアクセスし、「牛肉 ID」に IPv6 温度センサーの MIPv6 HoA を入力し、「検索」ボタンを押す。次に、「位置履歴」ボタンを押す。

< コマンド実行結果 > 図 3-1-4 参照

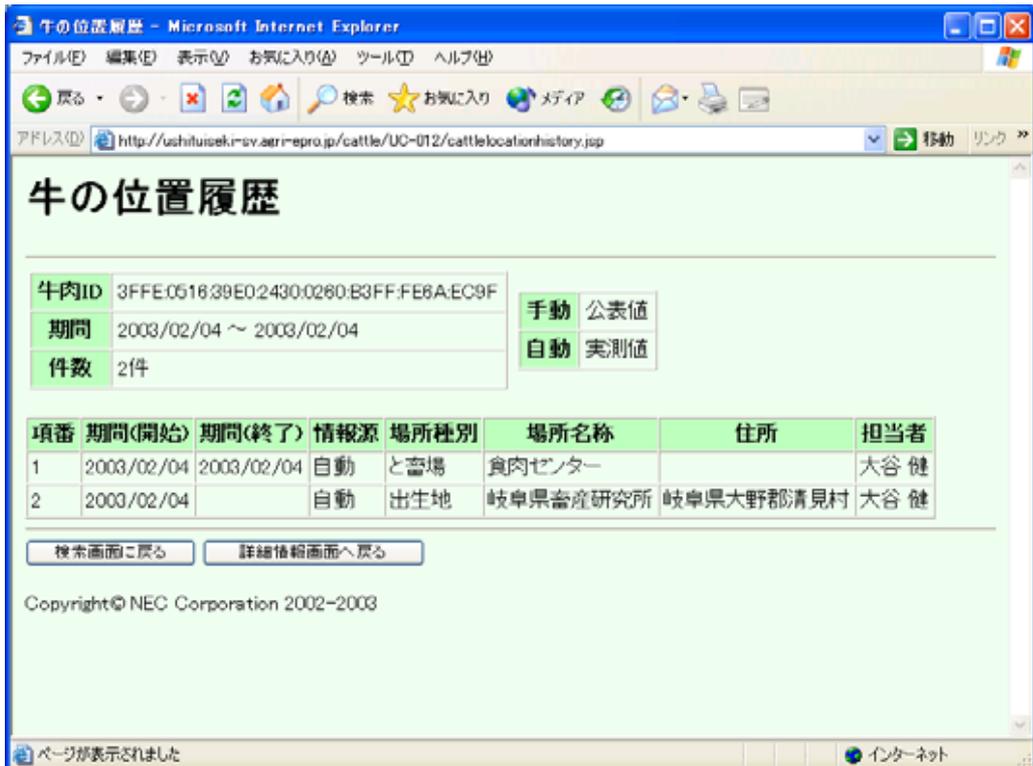


図 3-1-4 移動前の位置履歴

コマンド実行結果を説明する。HoA が「3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f」

のセンサのデータを取得している。位置履歴の最新の値が、「岐阜県畜産研究所」になっており、「場所 1」に IPv6 温度センサーが存在することを表わしている。

IPv6 温度センサーを「場所 2」へ移動させる。

一定時間 (IPv6 温度センサーの処理間隔) 経過後、と同じ手順により、追跡情報表示装置で、現在の位置情報が「場所 2」であることを確認する。

<http://ushituisseki-sv.agri-epro.jp/cattle/UC-012/inputip.jsp>

にアクセスし、「牛肉 ID」に IPv6 温度センサーの MIPv6 HoA を入力し、「検索」ボタンを押す。次に、「位置履歴」ボタンを押す。

< コマンド実行結果 > 図 3-1-5 参照



図 3-1-5 移動後の位置履歴

コマンド実行結果を説明する。HoA が「3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f」の IPv6 温度センサーのデータを取得しているが、と比較して、位置履歴の最新の値が「食肉センター」に変わっており、IPv6 温度センサーの移動により位置情報を取得していることが分かる。

この結果と、本章 (1)項「CoA と HoA の適切な対応付け」の実験結果より、生個体を移動させ、同一の IPv6 アドレスに関連付けられた CoA から、位置情報を取得できることが確認できた。

## 1.5 結果と考察

本章では、「モバイル IPv6 による個体識別・状態監視（プレゼンス）管理技術」として、4つの実験を行った。それぞれの結果をまとめ、考察する。

### (1) CoA と HoA の適切な対応付け

この実験は、モバイル IPv6 の基本動作を確認するものであり、1.4 実験実施結果(1)項に記述した通り、CoA と HoA の適切な対応付けが行われていることを確認できた。これによりモバイル IPv6 の「MN が異なるネットワークセグメント上へ移動しても、MN と CN 間の通信が切断されない」という動作が可能となることが分かる。

### (2) 状態変化の保持

この実験は、IPv6 温度センサーで取得したデータがモバイル IPv6 ネットワークを經由して、正常にサーバに反映されるかを確認するものであり、1.4 実験実施結果(2)項に記述した通り、IPv6 温度センサー取得データの変化をサーバ側で正常に記録できていることが確認できた。これにより、モバイル IPv6 を使用した MN からデータを蓄積する CN へ正常にデータ通信が行われていると言える。

### (3) 状態変化の取得

この実験は、プレゼンスサーバを經由して IPv6 温度センサーから任意にデータを取得することを確認するものであり、1.4 実験実施結果(3)項に示した通り、完全にリアルタイムではないが、体温というコンテンツとしてはリアルタイムに近いタイミングでのデータ取得を行うことができていると言える。完全に任意と言えるタイミングでのデータ取得には、物理的にセンサのバッテリー動作上の制約があり、現時点では実現できていないが、今後の課題として取り組む必要がある。

### (4) 位置情報の取得

この実験は、モバイル IPv6 の CoA を利用してセンサの位置情報を取得することを確認するためのものであり、1.4 実験実施結果(4)項に示した通り、IPv6 温度センサーの移動によって、位置情報を更新・取得することができていることが分かる。また、これにより、(1)項の「MN が異なるネットワークセグメント上へ移動しても、MN と CN 間の通信が切断されない」を、より具体的に証明したとも言える。

モバイル IPv6 による「MN が移動しても通信が切断されない」「CoA のネットワーク Prefix より位置情報を取得する」という基本的な機能の確認であったが、モバイル IPv6 を使うことで、これらの機能要求を満たすことが可能であると言える。

## 2 IPv6 温度センサーへの IPsec の実装技術

### 2.1 実験要求事項

#### (1) IPsec の暗号化動作

IPsec オプションを外した場合と、IPsec (固定鍵方式) で通信した場合の、一連の IP パケットをそれぞれモニターして比較し、IPsec を用いない場合のパケットの内容の解読が可能であることに対して、IPsec 通信時のモニターした内容の解読が不可能であることを確認する。

#### (2) 疑似不正アクセス

疑似不正アクセス端末から、IPv6 温度センサーに IPsec 通信を使って接続を試みる。その際、任意の鍵で多数回接続を試みると共に、事前に定義された固定鍵を用いて接続を試みることにより、疑似不正アクセス端末からの接続は、固定鍵で定義された鍵を用いた場合のみ可能であることを確認する。

#### (3) モバイル IPv6 と IPsec の同時動作

IPv6 温度センサーがモバイル IPv6 により、CoA を変化させた時に、牛用追跡管理装置との通信記録を確認することにより、アドレスの変化が起きても、通信エラーが発生していないことを確認する。

## 2.2 実験仕様、手順

### (1) IPsec の暗号化動作

IPv6 温度センサーの電源を on にする。

HA と IPv6 温度センサーでそれぞれ以下のような設定を行い、HA と IPv6 温度センサー間の IPsec を無効にする。

<HA 側>

```
% sh /root/mn_ipsec.sh stop
```

```
% sh /root/filter_kai.conf
```

< IPv6 温度センサー側 >

/usr2/go.sh の内容のうち、以下の 2 行をコメントアウトする。

```
setkey f /usr2/local/v6/etc/ipsec/mn.cf
```

```
mip6control S 1
```

追跡管理 MIPv6 装置(HA)のコンソールで以下のコマンドによりネットワークを流れるパケットを取得する。

```
% tcpdump X -s 1600 -w [file_name] ip6 e
```

ここで、HA と IPv6 温度センサー間のパケットの内容を確認し、温度データ等が目視で識別可能なことを確認する。

HA と IPv6 温度センサーでそれぞれ以下のような設定を行い、HA と IPv6 温度センサー間の IPsec を有効にする。

<HA 側>

```
% sh /root/mn_ipsec.sh start
```

```
% sh /root/filter.conf
```

< IPv6 温度センサー側 >

でコメントアウトした/usr2/go.sh 内の以下の 2 行を有効にする。

```
#setkey f /usr2/local/v6/etc/ipsec/mn.cf
```

```
#mip6control S 1
```

追跡管理 MIPv6 装置(HA)のコンソールで以下のコマンドによりネットワークを流れるパケットを取得する。

```
% tcpdump X -s 1600 -w [file_name] ip6 e
```

ここで、HA と IPv6 温度センサー間のパケットの内容を確認し、HA と IPv6 温度センサー間を流れるデータが、暗号化により解読不能状態であることを確認する。

資料 3-1 として、mn.cf、mn\_ipsec.sh、mn\_ipsec0.sh、filter.conf、filter\_kai.conf を添付する。

### (2) 疑似不正アクセス

IPv6 温度センサーの電源を on にする。

(1) 項と同様の設定を行い、HA と IPv6 温度センサー間の IPsec を有効にする。

疑似不正アクセス端末 1 から IPv6 温度センサーに以下のコマンドを実行し、アクセスを試みる。

```
%ping6 3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f
```

ここで、IPsec のポリシー設定により、未登録の IP アドレスを持った端末ではアクセスが拒否されることを確認する。

疑似不正アクセス端末 2(不正アクセス者が登録済み HA の IP アドレスを入手し、IP アドレスの偽装に成功したと仮定)に、事前登録されていない鍵を設定し(mn\_ipsec.sh に不正な鍵を書き込む)、以下のコマンドにより、IPv6 温度センサーと不正アクセス端末 2 の SA を比較し、鍵情報が異なることを確認する。

```
%setkey D
```

不正アクセス端末 2 で以下のコマンドを実行し、IPv6 温度センサーにアクセスを試みる。

```
%ping6 3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f
```

ここで、IP アドレスは HA のアドレスを偽装しているが、鍵が一致しないためにアクセスが拒否されることを確認する。

疑似不正アクセス端末 2 に、事前登録された鍵を設定し(mn\_ipsec.sh に事前登録した鍵を書き込む)、以下のコマンドにより、IPv6 温度センサーと不正アクセス端末 2 の SA を比較し、鍵情報が一致していることを確認する。

```
%setkey D
```

不正アクセス端末 2 で以下のコマンドを実行し、IPv6 温度センサーにアクセスを試みる。

```
%ping6 3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f
```

ここで、IP アドレスによるアクセス制限と鍵の一致により、アクセスが可能であることを確認する。

### (3) MIPv6 と IPsec との同時動作

IPv6 温度センサーを「場所 1」に配置し、電源を on にする。

(1) 項と同様の設定を行い、HA と IPv6 温度センサー間の IPsec を有効にする。HA で以下のコマンドにより、BC の状態を確認する。

```
%mip6control c
```

ここで、「場所 1」の Prefix を持った CoA が出力されることと同時に、HA から IPv6 温度センサーへの通信が可能な状態であることを確認する。

IPv6 温度センサーを「場所 2」に移動させる。

HA で以下のコマンドにより BC の状態を確認する。

```
%mip6control c
```

ここで、「場所 2」の Prefix を持った CoA が出力されることと同時に、HA から IPv6 温度センサーへの通信が可能な状態であることを確認する。

## 2.3 実験実施環境

### (1) 実験実施場所

NEC エンジニアリング社内（NEC 横浜技術センター）

### (2) 実験実施環境構成図

2.2 項(1)～(3)の実験を実施した実験環境の構成図を図 3-2-1 に示す。

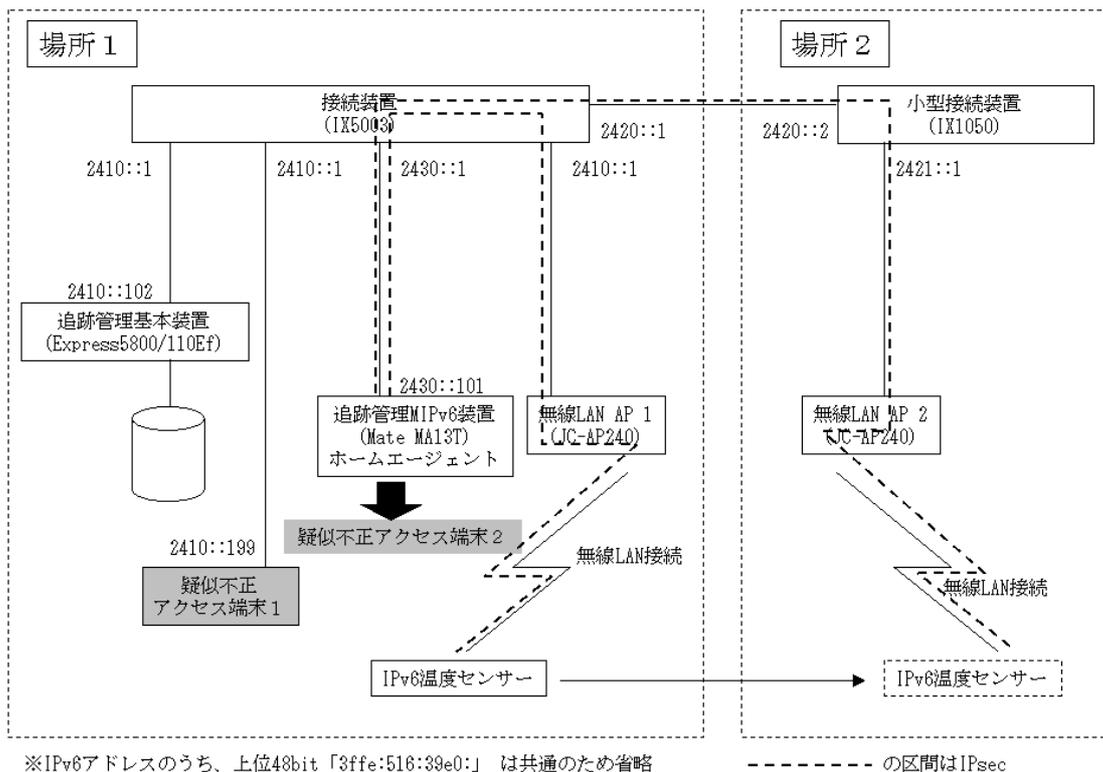


図 3-2-1 実験実施環境構成図

図 3-2-1 を説明する。「場所 1」と「場所 2」はそれぞれ「岐阜県モデル牧場（岐阜県畜産研究所）」と「食肉流通センター（食肉センター）」を想定しており、各機材及び IPv6 アドレス体系は現地と同じ構成としている。

HA と IPv6 温度センサー間で IPsec をトランスポートモードで使用可能な状態にしており、追跡管理基本装置と IPv6 温度センサーの通信は、IPv6 温度センサーと HA 間のトンネルモードによる IPsec が使用可能となっている。さらに、事前に登録された IP アドレス以外からの通信は IPsec のポリシー設定により排除される。

「場所 1」のネットワーク Prefix は「3ffe:516:39e0:2410」となり、「場所 2」のネットワーク Prefix は「3ffe:516:39e0:2421」となる。

また、「場所 1」と「場所 2」は、無線 LAN の範囲が物理的に重複するため、

常にどちらかのアクセスポイントの電源を off にすることで、IPv6 温度センサーの移動実験を可能としている。

さらに、疑似不正アクセス実験のために、疑似不正アクセス端末 1 として PC を 1 台と、疑似不正アクセス端末 2 として HA を使用している。疑似不正アクセス端末の IPv6 アドレスは「3ffe:516:39e0:2410::199」とした。

(1) ~ (3)の実験で使用した IPv6 温度センサーは以下の表 3-2-1 の通りである。

表 3-2-1 実験に使用した IPv6 温度センサー

実験仕様	IPv6 温度センサーのホスト名	IPv6 温度センサーの MIPv6 HoA
(1)	sensor1	3ffe:516:39e0:2430:22:fa:9ae:e801
(2)	sensor22	3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f
(3)	sensor22	3ffe:516:39e0:2430: 260:b3ff:fe6a:ec9f

## 2.4 実験実施結果

### (1) IPSec の暗号化動作

IPv6 温度センサーの電源を on にする。

HA と IPv6 温度センサーでそれぞれ以下のような設定を行い、HA と IPv6 温度センサー間の IPsec を無効にする。

< HA 側 >

```
% sh /root/mn_ipsec.sh stop
```

```
% sh /root/filter_kai.conf
```

< IPv6 温度センサー側 >

/usr2/go.sh の内容のうち、以下の 2 行をコメントアウトする。

```
setkey f /usr2/local/v6/etc/ipsec/mn.cf
```

```
mip6control S 1
```

追跡管理 MIPv6 装置(HA)のコンソールで以下のコマンドによりネットワークを流れるパケットを取得する。

```
% tcpdump X -s 1600 -w [file_name] ip6 e
```

< コマンド実行結果 >

< IPv6 温度センサー HA >

```
19:06:52.649331 0:0:4c:64:71:6f 0:3:47:e2:1e:68 ip6 1111:
3ffe:516:39e0:2410:260:b3ff:fe6a:287a > 3ffe:516:39e0:2430::101:
3ffe:516:39e0:2430:22:fa:9ae:e801.49153 > 3ffe:516:39e0:2410::102.5060: P
1:986(985) ack 1 win 17280 <nop,nop,timestamp 0 407261> [flowlabel 0xfa851]
0x0000 6000 0000 0421 293f 3ffe 0516 39e0 2410 `....!)??...9.$
0x0010 0260 b3ff fe6a 287a 3ffe 0516 39e0 2430 `....j(z?...9.$0
0x0020 0000 0000 0000 0101 600f a851 03f9 0640 .....`..Q...@
0x0030 3ffe 0516 39e0 2430 0022 00fa 09ae e801 ?...9.$0.".....
0x0040 3ffe 0516 39e0 2410 0000 0000 0000 0102 ?...9.$.....
0x0050 c001 13c4 2c65 0b3b ac84 449c 8018 4380 ....,e.;..D...C.
0x0060 913a 0000 0101 080a 0000 0000 0006 36dd . :.....6.
0x0070 4e4f 5449 4659 2073 6970 3a5b 3366 6665 NOTIFY.sip:[3ffe
0x0080 3a35 3136 3a33 3965 303a 3234 3130 3a3a :516:39e0:2410::
0x0090 3130 325d 3a35 3036 3020 5349 502f 322e 102]:5060.SIP/2.
0x00a0 300d 0a46 726f 6d3a 203c 7369 703a 5b33 0..From:.<:sip:[3
0x00b0 6666 653a 3531 363a 3339 6530 3a32 3433 ffe:516:39e0:243
0x00c0 303a 3232 3a66 613a 3961 653a 6538 3031 0:22:fa:9ae:e801
0x00d0 5d3e 3b74 6167 3d37 3735 6434 3335 312d ]>;tag=775d4351-
0x00e0 3533 6334 3864 3936 2d32 6232 3665 3062 53c48d96-2b26e0b
0x00f0 2d34 3138 6665 6463 662d 3139 6462 6331 -418fedcf-19dbc1
0x0100 3965 0d0a 5669 613a 2053 4950 2f32 2e30 9e..Via:..SIP/2.0
0x0110 2f54 4350 205b 3366 6665 3a35 3136 3a33 /TCP.[3ffe:516:3
0x0120 3965 303a 3234 3330 3a32 323a 6661 3a39 9e0:2430:22:fa:9
0x0130 6165 3a65 3830 315d 3a34 3931 3533 0d0a ae:e801]:49153..
0x0140 546f 3a20 3c73 6970 3a5b 3366 6665 3a35 To:.<:sip:[3ffe:5
0x0150 3136 3a33 3965 303a 3234 3130 3a3a 3130 16:39e0:2410::10
0x0160 325d 3a35 3036 303e 0d0a 4361 6c6c 2d49 2]:5060>..Call-I
```

0x0170	443a	2037	6265	3963	3162	642d	3838	6161	D:.7be9c1bd-88aa
0x0180	3130	322d	3364	3338	3530	3962	2d37	3436	102-3d38509b-746
0x0190	6239	6662	652d	3264	3034	3431	3766	405b	b9fbe-2d04417f@[
0x01a0	3366	6665	3a35	3136	3a33	3965	303a	3234	3ffe:516:39e0:24
0x01b0	3330	3a32	323a	6661	3a39	6165	3a65	3830	30:22:fa:9ae:e80
0x01c0	315d	0d0a	4353	6571	3a20	3120	4e4f	5449	1]..CSeq:.1.NOTI
0x01d0	4659	0d0a	436f	6e74	6163	743a	203c	7369	FY..Contact:.<si
0x01e0	703a	3762	6539	6331	6264	2d38	3861	6131	p:7be9c1bd-88aa1
0x01f0	3032	2d33	6433	3835	3039	622d	3734	3662	02-3d38509b-746b
0x0200	3966	6265	2d32	6430	3434	3137	6640	5b33	9fbe-2d04417f@[3
0x0210	6666	653a	3531	363a	3339	6530	3a32	3433	ffe:516:39e0:243
0x0220	303a	3232	3a66	613a	3961	653a	6538	3031	0:22:fa:9ae:e801
0x0230	5d3a	303b	7472	616e	7370	6f72	743d	7463	]0;transport=tc
0x0240	703e	0d0a	4d61	782d	466f	7277	6172	6473	p>..Max-Forwards
0x0250	3a20	3730	0d0a	5573	6572	2d41	6765	6e74	:.70..User-Agent
0x0260	3a20	4775	7070	792f	312e	300d	0a43	6f6e	..Guppy/1.0..Con
0x0270	7465	6e74	2d4c	656e	6774	683a	2034	3533	tent-Length:.453
0x0280	0d0a	0d0a	3c70	7265	7365	6e63	6520	656e	....<presence.en
0x0290	7469	7479	3d22	7369	703a	5b33	6666	653a	tity="sip:[3ffe:
0x02a0	3531	363a	3339	6530	3a32	3433	303a	3232	516:39e0:2430:22
0x02b0	3a66	613a	3961	653a	6538	3031	5d22	3e0a	:fa:9ae:e801]">.
0x02c0	2020	3c74	7570	6c65	2069	643d	2263	6174	..<tuple.id="cat
0x02d0	746c	6522	3e0a	2020	2020	3c73	7461	7475	tle">.....<statu
0x02e0	733e	0a20	2020	2020	203c	6370	733a	6361	s>.....<cps:ca
0x02f0	7474	6c65	4578	7465	6e73	696f	6e0a	2020	ttleExtension...
0x0300	2020	2020	2020	786d	6c6e	733a	6370	733d	.....xmlns:cps=
0x0310	2275	726e	3a6e	6574	6c61	623a	7061	7261	"urn:netlab:para
0x0320	6d73	3a78	6d6c	3a6e	733a	6361	7474	6c65	ms:xml:ns:cattle
0x0330	2d70	7265	7365	6e63	652d	7365	7276	6963	-presence-servic
0x0340	6522	3e0a	2020	2020	2020	2020	3c63	7073	e">.....<cps
0x0350	3a74	656d	7065	7261	7475	7265	3e32	322e	:temperature>22.
0x0360	3337	3030	3031	3c2f	6370	733a	7465	6d70	370001</cps:temp
0x0370	6572	6174	7572	653e	0a20	2020	2020	2020	erature>.....
0x0380	203c	6370	733a	4d49	5076	3643	6f41	3e5b	..<cps:MIPv6CoA>[
0x0390	3366	6665	3a35	3136	3a33	3965	303a	3234	3ffe:516:39e0:24
0x03a0	3130	3a32	3630	3a62	3366	663a	6665	3661	10:260:b3ff:fe6a
0x03b0	3a32	3837	615d	3c2f	6370	733a	4d49	5076	:287a]</cps:MIPv
0x03c0	3643	6f41	3e0a	2020	2020	2020	2020	3c63	6CoA>.....<c
0x03d0	7073	3a54	4f44	3e31	3034	3530	3434	3436	ps:TOD>104504446
0x03e0	3930	3030	3c2f	6370	733a	544f	443e	0a20	9000</cps:TOD>..
0x03f0	2020	2020	203c	2f63	7073	3a63	6174	746c	.....</cps:cattl
0x0400	6545	7874	656e	7369	6f6e	3e0a	2020	2020	eExtension>.....
0x0410	3c2f	7374	6174	7573	3e0a	2020	2020	3c63	</status>.....<c
0x0420	6f6e	7461	6374	3e3c	2f63	6f6e	7461	6374	ontact></contact
0x0430	3e0a	2020	3c2f	7475	706c	653e	0a3c	2f70	>...</tuple>.</p
0x0440	7265	7365	6e63	653e	0a				resence>.
 < HA 追跡管理基本装置 >									
19:06:52.649362 0:3:47:e2:1e:68 0:0:4c:64:71:6f ip6 1071:									

```

3ffe:516:39e0:2430:22:fa:9ae:e801.49153 > 3ffe:516:39e0:2410::102.5060: P
1:986(985) ack 1 win 17280 <nop,nop,timestamp 0 407261> [flowlabel 0xfa851]
0x0000 600f a851 03f9 063f 3ffe 0516 39e0 2430 `..Q...??...9.$0
0x0010 0022 00fa 09ae e801 3ffe 0516 39e0 2410 .".....?...9.$
0x0020 0000 0000 0000 0102 c001 13c4 2c65 0b3b .....e.;
0x0030 ac84 449c 8018 4380 913a 0000 0101 080a ..D...C...:.....
0x0040 0000 0000 0006 36dd 4e4f 5449 4659 2073 .....6.NOTIFY.s
0x0050 6970 3a5b 3366 6665 3a35 3136 3a33 3965 ip:[3ffe:516:39e
0x0060 303a 3234 3130 3a3a 3130 325d 3a35 3036 0:2410::102]:506
0x0070 3020 5349 502f 322e 300d 0a46 726f 6d3a 0.SIP/2.0..From:
0x0080 203c 7369 703a 5b33 6666 653a 3531 363a .<sip:[3ffe:516:
0x0090 3339 6530 3a32 3433 303a 3232 3a66 613a 39e0:2430:22:fa:
0x00a0 3961 653a 6538 3031 5d3e 3b74 6167 3d37 9ae:e801]>;tag=7
0x00b0 3735 6434 3335 312d 3533 6334 3864 3936 75d4351-53c48d96
0x00c0 2d32 6232 3665 3062 2d34 3138 6665 6463 -2b26e0b-418fedc
0x00d0 662d 3139 6462 6331 3965 0d0a 5669 613a f-19dbc19e..Via:
0x00e0 2053 4950 2f32 2e30 2f54 4350 205b 3366 .SIP/2.0/TCP.[3f
0x00f0 6665 3a35 3136 3a33 3965 303a 3234 3330 fe:516:39e0:2430
0x0100 3a32 323a 6661 3a39 6165 3a65 3830 315d :22:fa:9ae:e801]
0x0110 3a34 3931 3533 0d0a 546f 3a20 3c73 6970 :49153..To:<sip
0x0120 3a5b 3366 6665 3a35 3136 3a33 3965 303a :[3ffe:516:39e0:
0x0130 3234 3130 3a3a 3130 325d 3a35 3036 303e 2410::102]:5060>
0x0140 0d0a 4361 6c6c 2d49 443a 2037 6265 3963 ..Call-ID:.7be9c
0x0150 3162 642d 3838 6161 3130 322d 3364 3338 1bd-88aa102-3d38
0x0160 3530 3962 2d37 3436 6239 6662 652d 3264 509b-746b9fbe-2d
0x0170 3034 3431 3766 405b 3366 6665 3a35 3136 04417f@[3ffe:516
0x0180 3a33 3965 303a 3234 3330 3a32 323a 6661 :39e0:2430:22:fa
0x0190 3a39 6165 3a65 3830 315d 0d0a 4353 6571 :9ae:e801]..Cseq
0x01a0 3a20 3120 4e4f 5449 4659 0d0a 436f 6e74 :.1.NOTIFY..Cont
0x01b0 6163 743a 203c 7369 703a 3762 6539 6331 act:<sip:7be9c1
0x01c0 6264 2d38 3861 6131 3032 2d33 6433 3835 bd-88aa102-3d385
0x01d0 3039 622d 3734 3662 3966 6265 2d32 6430 09b-746b9fbe-2d0
0x01e0 3434 3137 6640 5b33 6666 653a 3531 363a 4417f@[3ffe:516:
0x01f0 3339 6530 3a32 3433 303a 3232 3a66 613a 39e0:2430:22:fa:
0x0200 3961 653a 6538 3031 5d3a 303b 7472 616e 9ae:e801]:0;tran
0x0210 7370 6f72 743d 7463 703e 0d0a 4d61 782d sport=tcp>..Max-
0x0220 466f 7277 6172 6473 3a20 3730 0d0a 5573 Forwards:.70..Us
0x0230 6572 2d41 6765 6e74 3a20 4775 7070 792f er-Agent:.Guppy/
0x0240 312e 300d 0a43 6f6e 7465 6e74 2d4c 656e 1.0..Content-Len
0x0250 6774 683a 2034 3533 0d0a 0d0a 3c70 7265 gth:.453....<pre
0x0260 7365 6e63 6520 656e 7469 7479 3d22 7369 sence.entity="si
0x0270 703a 5b33 6666 653a 3531 363a 3339 6530 p:[3ffe:516:39e0
0x0280 3a32 3433 303a 3232 3a66 613a 3961 653a :2430:22:fa:9ae:
0x0290 6538 3031 5d22 3e0a 2020 3c74 7570 6c65 e801]">...<tuple
0x02a0 2069 643d 2263 6174 746c 6522 3e0a 2020 .id="cattle">...
0x02b0 2020 3c73 7461 7475 733e 0a20 2020 2020 ..<status>.....
0x02c0 203c 6370 733a 6361 7474 6c65 4578 7465 .<cps:cattleExte
0x02d0 6e73 696f 6e0a 2020 2020 2020 2020 786d nsion.....xm
0x02e0 6c6e 733a 6370 733d 2275 726e 3a6e 6574 lns:cps="urn:net

```

0x02f0	6c61 623a 7061 7261 6d73 3a78 6d6c 3a6e	lab:params:xml:n
0x0300	733a 6361 7474 6c65 2d70 7265 7365 6e63	s:cattle-presenc
0x0310	652d 7365 7276 6963 6522 3e0a 2020 2020	e-service">.....
0x0320	2020 2020 3c63 7073 3a74 656d 7065 7261	....<cps:tempera
0x0330	7475 7265 3e32 322e 3337 3030 3031 3c2f	ture>22.370001</
0x0340	6370 733a 7465 6d70 6572 6174 7572 653e	cps:temperature>
0x0350	0a20 2020 2020 2020 203c 6370 733a 4d49	.....<cps:MI
0x0360	5076 3643 6f41 3e5b 3366 6665 3a35 3136	Pv6CoA>[3ffe:516
0x0370	3a33 3965 303a 3234 3130 3a32 3630 3a62	:39e0:2410:260:b
0x0380	3366 663a 6665 3661 3a32 3837 615d 3c2f	3ff:fe6a:287a]</
0x0390	6370 733a 4d49 5076 3643 6f41 3e0a 2020	cps:MIpV6CoA>...
0x03a0	2020 2020 2020 3c63 7073 3a54 4f44 3e31	.....<cps:TOD>1
0x03b0	3034 3530 3434 3436 3930 3030 3c2f 6370	045044469000</cp
0x03c0	733a 544f 443e 0a20 2020 2020 203c 2f63	s:TOD>.....</c
0x03d0	7073 3a63 6174 746c 6545 7874 656e 7369	ps:cattleExtensi
0x03e0	6f6e 3e0a 2020 2020 3c2f 7374 6174 7573	on>.....</status
0x03f0	3e0a 2020 2020 3c63 6f6e 7461 6374 3e3c	>.....<contact><
0x0400	2f63 6f6e 7461 6374 3e0a 2020 3c2f 7475	/contact>...</tu
0x0410	706c 653e 0a3c 2f70 7265 7365 6e63 653e	ple>.</presence>
0x0420	0a	.

コマンド実行結果を解説する。結果の前半は IPv6 温度センサーから HA への通信パケットであり、後半は同じデータを HA が追跡管理基本装置へ転送した通信パケットである。

各パケットの 1 行目から 4 行目は、パケットの送信元および宛先等を表わすヘッダ部分である。5 行目以降は縦に 3 分割されているが、左側がデータ行、中央が実データ、右側が ASCII データに変換したものである。

前半パケットのヘッダ部は、パケットが IPv6 温度センサーの CoA 「3ffe:516:39e0:2410:260:b3ff:fe6a:287a」から HA 「3ffe:516:39e0:2430::101」宛の通信であることを表しているが、実際には内部の IPv6 ヘッダから IPv6 温度センサーの HoA 「3ffe:516:39e0:2430:22:fa:9ae:e801」から追跡管理基本装置 「3ffe:516:39e0:2410::102」への通信パケットがカプセル化されていることをわかる。

後半パケットのヘッダ部では、HA がヘッダ部を書き換え、IPv6 温度センサーの HoA 「3ffe:516:39e0:2430:22:fa:9ae:e801」から追跡管理基本装置 「3ffe:516:39e0:2410::102」へのパケットとしていることが分かる。

データの内容としては、共に同じ内容であるが前半パケットの「0x0340」から「0x0370」と後半パケットの「0x0320」から「0x0340」にかけて温度データ(ASCII データのハンチング部分)を送信しており、22.370001 を計測していることが分かる。

HA と IPv6 温度センサーでそれぞれ以下のような設定を行い、HA と IPv6 温度センサー間の IPsec を有効にする。

<HA 側>

```
% sh /root/mn_ipsec.sh start
```

```
% sh /root/filter.conf
```

```
< IPv6 温度センサー側 >
```

でコメントアウトした/usr2/go.sh 内の以下の 2 行を有効にする。

```
#setkey f /usr2/local/v6/etc/ipsec/mn.cf
```

```
#mip6control S 1
```

追跡管理 MIPv6 装置(HA)のコンソールで以下のコマンドによりネットワークを流れるパケットを取得する。

```
% tcpdump X -s 1600 -w [file_name] ip6 e
```

```
< コマンド実行結果 >
```

```
< IPv6 温度センサー HA >
```

```
18:50:53.340632 0:0:4c:64:71:6f 0:3:47:e2:1e:68 ip6 1174:
3ffe:516:39e0:2410:260:b3ff:fe6a:287a > 3ffe:516:39e0:2430::101: DSTOPT
ESP(spi=0x10aee801,seq=0x7) [flowlabel 0x36f7d]
0x0000 6003 6f7d 0460 3c3f 3ffe 0516 39e0 2410 \.o}.`<??...9.$
0x0010 0260 b3ff fe6a 287a 3ffe 0516 39e0 2430 .`...j(z?...9.$0
0x0020 0000 0000 0000 0101 3202 0102 0000 c910 .....2.....
0x0030 3ffe 0516 39e0 2430 0022 00fa 09ae e801 ?...9.$0.".....
0x0040 10ae e801 0000 0007 a4e5 a773 353f 7788 .....s5?w.
0x0050 59c0 9d07 7485 6499 3a1d 70e8 ef31 360a Y...t.d.:.p..16.
0x0060 abf7 b7db 019d bf69 2994 7861 e91e 9412 .....i).xa...
0x0070 d93e d555 1d87 a3ba f2dc 5ddc 80f2 7d72 .>.U.....]...}r
0x0080 5d76 1ef2 f97e ef3c d9bd 4218 23ca d572 ]v...~.<..B.#..r
0x0090 e289 ab4e eb41 4b82 87c3 6119 58d5 b924 ...N.AK...a.X..$
0x00a0 99cb 29ed ffc1 1de9 5e42 3c4b 26a7 a0e3 ..).....^B<K&...
0x00b0 a815 59ed 50c6 bb94 5b2a 304b 3039 fb48 ..Y.P...[*0K09.H
0x00c0 f83c 7b2a 80cc 409b 7a7f 9e7e 430e 9aa5 .<{*..@.z..~C...
0x00d0 75f6 fa3b 3341 c3a9 4bc7 294e 93e5 5a86 u.;3A..K.)N..Z.
0x00e0 5a65 de61 6d5c fe04 ee8a 7bba 15ce ef07 Ze.am¥....{.....
0x00f0 9fcf c009 915b 07bd 3e90 a7f6 fb65 0e26 ....[.>.....e.&
0x0100 5c7e 23e8 4f5b 2cdb 0750 7823 5afe c70e ¥~#.O[...Px#Z...
0x0110 ddb4 156b 8f77 3f73 9729 18e6 1725 52a1 ...k.w?s)...%R.
0x0120 a0f3 6d63 774f bfd4 75de f66b 9ef0 3dc5 ..mcwO..u.k..=.
0x0130 176e a268 8205 b9d1 59a1 5da3 233a ed82 .n.h....Y.]#...
0x0140 cee5 acfc ca9f c3ac 9cf1 2750 ff53 91e5 .....P.S..
0x0150 921e b390 9fb1 0db6 42e1 2c65 c1d3 54f4 .....B.,e..T.
0x0160 8714 8e3c a380 fce1 601e 357d 77d7 3c27 ...<.....`5}w.<'
0x0170 14e4 a661 baf7 d10e c23d 2111 0db4 8df6 ...a.....=!.....
0x0180 0c22 f77e b25d 8481 77df d9df a8af 0ac3 .".~.]..w.....
0x0190 8c90 d8ee 4526 9092 ee51 ffe0 1d5e c894 ....E&...Q...^..
0x01a0 9d32 6438 0f37 56b4 aea9 251e 5b57 952d ..2d8.7V...%.[W.-
0x01b0 8986 4936 6378 8e16 5b19 92fc c2bc 9378 ..I6cx..[.....x
0x01c0 9c17 4739 296d b88b cad5 7f85 5be8 9065 ..G9)m.....[.e
0x01d0 81d2 47e7 159a 5b70 379c 6b77 c89e bc5a ..G...[p7.kw...Z
0x01e0 4d8d 42d6 dfb8 0001 733b 4186 fa91 faf3 M.B.....s;A.....
0x01f0 6b5f 72b6 aff2 777e 9056 8d3b 1b7a 9ecf k_r...w~.V.;z..
0x0200 813e fcb0 07bb 813e 6a1a 0166 4b13 9e99 .>.....>j..fK...
0x0210 3bd8 3e47 6ae1 8b9a 07a3 e379 03be 368d ;:>Gj.....y..6.
0x0220 4beb f12e c1fe 73bd e4b5 316b 5ee4 cf9b K.....s...1k^...
0x0230 a6a6 9ba2 1c1a 8b3e 1b60 d25a 10b3 0b5f .....>.`Z..._
```

0x0240	7160 e56f 7484 a4ec 5319 2cb4 178c 1eff	q`.ot...S,.....
0x0250	50e8 6fea ad70 7ffd 9dcc c397 3255 6f54	P.o.p.....2UoT
0x0260	839a 7d3e ff00 bd04 1439 5ed9 69de 76af	..}>.....9^.i.v
0x0270	4935 f693 5634 6875 d329 38e6 f6fe 6c2e	I5..V4hu.)8...l
0x0280	fcfe 35d2 4e06 0e4b 114f 6c22 964b 5688	..5.N.K.Ol".KV.
0x0290	0511 98a1 119f b512 0f79 07ea a5af 6d7a	.....y....mz
0x02a0	4e11 8e0d 1759 0e84 857e 8bb4 cfc4 f1d6	N....Y...~.....
0x02b0	ad50 ce4f 9659 044f 391e 9a60 b3da c268	.P.O.Y.O9..`...h
0x02c0	ef35 5ccc bf35 073b 2396 225d ab67 3d12	.5¥..5.;#."].g=.
0x02d0	bf3b d55e 8a95 5312 26de 4f31 727a 5559	.;.^..S.&.O1rzUY
0x02e0	d6da 368e 3a7d 11d7 a2c2 486a 7ed6 861a	..6.}....Hj~...
0x02f0	0b09 6d26 e4a8 2a56 f2ec 9f4a 05bd 67c2	..m&..*V...J.g.
0x0300	feab 5d94 7019 fbe4 7e44 ddf5 3d6e 4f58	..].p...~D.=nOX
0x0310	0624 8266 3413 4d94 974b f7b3 a3b4 069f	.S.f4.M.K.....
0x0320	13b8 96f4 4610 efcd 7e8b 0646 2e09 53cb	....F...~.F.S.
0x0330	e351 0505 f362 5fe6 62a4 4fcd c2b9 7cb3	.Q...b_.b.O... .
0x0340	201c f37a 1905 2035 7324 4dff eac4 0b50	...z...5s\$M....P
0x0350	0731 0631 5c17 0382 3833 bdfc bda6 48b2	.1.1¥...83....H.
0x0360	3f25 ddc2 20a0 04fe 4f07 86c9 da27 b31d	?%.....O....'..
0x0370	cf0d 4a82 414a 49a6 e50b d634 ce1c 4f71	..J.AJl....4..Oq
0x0380	35aa 0e0d 190e a3b2 1f54 bbe4 b79e 9b30	5.....T.....0
0x0390	2e67 fe4f 3d0e d979 1552 040a 828b 82ca	.g.O=.y.R.....
0x03a0	adc5 1919 2409 7b8f 158e fcc1 efed 7a7b	....\$.{.....z{
0x03b0	eb40 9dfc c0b9 262c 8006 5a15 df0c eb46	@....&...Z....F
0x03c0	8285 da8b 642d 802e c82d c5cd 5ee8 5e28	....d-...-..^..^(
0x03d0	4f22 6267 b392 c3de a3b7 5ea7 8650 722e	O"bg.....^..Pr.
0x03e0	70c3 1f7d afcd b824 6aca 9cb6 edb1 5a5b	p.}...\$j.....Z[
0x03f0	b4b0 b710 657d d46e 0f58 f65d deb4 b48f	....e}.n.X.]....
0x0400	7ab7 759b 9ba9 dedb 0766 15a8 69f5 6219	z.u.....f.i.b.
0x0410	5c35 4657 0937 6f80 c35f 9509 d242 2782	¥5FW.7o..._...B'.
0x0420	de4c 3bd3 912a 0872 d5a9 116c 3ce7 4f06	.L;..*..r...l<.O.
0x0430	5775 66a2 b225 2e68 7a7e a29e dcbc 8805	Wuf..%.hz~.....
0x0440	18ec b69a 9d95 17cc 5fd9 86e4 7ffa 88fc	....._.....
0x0450	caa3 d833 329a 6b6b 4949 88fe 574d f0fa	...32.kkII..WM..
0x0460	f258 af63 e9c2 5d06 b222 1747 3b58 5616	.X.c.].".G;XV.
0x0470	c96e ef8a 9304 a56b 4aa9 1d8e a678 1244	.n.....kJ....x.D
0x0480	19ae c827 acd9 b304	...!....
 < HA 追跡管理基本装置 >		
18:50:53.340711 0:3:47:e2:1e:68 0:0:4c:64:71:6f ip6 1071:		
3ffe:516:39e0:2430:22:fa:9ae:e801.49153 > 3ffe:516:39e0:2410::102.5060: P		
1:986(985) ack 1 win 17280 <nop,nop,timestamp 0 311343> [flowlabel 0x36f7d]		
0x0000	6003 6f7d 03f9 063f 3ffe 0516 39e0 2430	`o}....??...9.S0
0x0010	0022 00fa 09ae e801 3ffe 0516 39e0 2410	.".....?...9.S.
0x0020	0000 0000 0000 0102 c001 13c4 2cfb 71d9	.....,q.
0x0030	70a7 1b94 8018 4380 fc95 0000 0101 080a	p....C.....
0x0040	0000 0000 0004 c02f 4e4f 5449 4659 2073	...../NOTIFY.s
0x0050	6970 3a5b 3366 6665 3a35 3136 3a33 3965	ip:[3ffe:516:39e
0x0060	303a 3234 3130 3a3a 3130 325d 3a35 3036	0:2410::102]:506
0x0070	3020 5349 502f 322e 300d 0a46 726f 6d3a	0.SIP/2.0..From:
0x0080	203c 7369 703a 5b33 6666 653a 3531 363a	.<sip:[3ffe:516:
0x0090	3339 6530 3a32 3433 303a 3232 3a66 613a	39e0:2430:22:fa:
0x00a0	3961 653a 6538 3031 5d3e 3b74 6167 3d37	9ae:e801]>;tag=7

0x00b0	3735 6434 3335 312d 3533 6334 3864 3936	75d4351-53c48d96
0x00c0	2d32 6232 3665 3062 2d34 3138 6665 6463	
	-2b26e0b-418fedc	
0x00d0	662d 3139 6462 6331 3965 0d0a 5669 613a	f-19dbc19e..Via:
0x00e0	2053 4950 2f32 2e30 2f54 4350 205b 3366	.SIP/2.0/TCP.[3f
0x00f0	6665 3a35 3136 3a33 3965 303a 3234 3330	fe:516:39e0:2430
0x0100	3a32 323a 6661 3a39 6165 3a65 3830 315d	:22:fa:9ae:e801]
0x0110	3a34 3931 3533 0d0a 546f 3a20 3c73 6970	:49153..To:<sip
0x0120	3a5b 3366 6665 3a35 3136 3a33 3965 303a	: [3ffe:516:39e0:
0x0130	3234 3130 3a3a 3130 325d 3a35 3036 303e	2410::102]:5060>
0x0140	0d0a 4361 6c6c 2d49 443a 2037 6265 3963	..Call-ID:.7be9c
0x0150	3162 642d 3838 6161 3130 322d 3364 3338	
	1bd-88aa102-3d38	
0x0160	3530 3962 2d37 3436 6239 6662 652d 3264	
	509b-746b9fbe-2d	
0x0170	3034 3431 3766 405b 3366 6665 3a35 3136	04417f@[3ffe:516
0x0180	3a33 3965 303a 3234 3330 3a32 323a 6661	:39e0:2430:22:fa
0x0190	3a39 6165 3a65 3830 315d	0d0a 4353 6571
	:9ae:e801]..CSeq	
0x01a0	3a20 3120 4e4f 5449 4659 0d0a 436f 6e74	:.1.NOTIFY..Cont
0x01b0	6163 743a 203c 7369 703a 3762 6539 6331	act:<sip:7be9c1
0x01c0	6264 2d38 3861 6131 3032 2d33 6433 3835	
	bd-88aa102-3d385	
0x01d0	3039 622d 3734 3662 3966 6265 2d32 6430	
	09b-746b9fbe-2d0	
0x01e0	3434 3137 6640 5b33 6666 653a 3531 363a	4417f@[3ffe:516:
0x01f0	3339 6530 3a32 3433 303a 3232 3a66 613a	39e0:2430:22:fa:
0x0200	3961 653a 6538 3031 5d3a 303b 7472 616e	9ae:e801]:0;tran
0x0210	7370 6f72 743d 7463 703e 0d0a 4d61 782d	sport=tcp>..Max-
0x0220	466f 7277 6172 6473 3a20 3730 0d0a 5573	Forwards:.70..Us
0x0230	6572 2d41 6765 6e74 3a20 4775 7070 792f	er-Agent:.Guppy/
0x0240	312e 300d 0a43 6f6e 7465 6e74 2d4c 656e	1.0..Content-Len
0x0250	6774 683a 2034 3533 0d0a 0d0a 3c70 7265	gth:.453....<pre
0x0260	7365 6e63 6520 656e 7469 7479 3d22 7369	sence.entity="si
0x0270	703a 5b33 6666 653a 3531 363a 3339 6530	p:[3ffe:516:39e0
0x0280	3a32 3433 303a 3232 3a66 613a 3961 653a	:2430:22:fa:9ae:
0x0290	6538 3031 5d22 3e0a 2020 3c74 7570 6c65	e801]">...<tuple
0x02a0	2069 643d 2263 6174 746c 6522 3e0a 2020	.id="cattle">...
0x02b0	2020 3c73 7461 7475 733e 0a20 2020 2020	..<status>.....
0x02c0	203c 6370 733a 6361 7474 6c65 4578 7465	..<cps:cattleExte
0x02d0	6e73 696f 6e0a 2020 2020 2020 2020 786d	nsion.....xm
0x02e0	6c6e 733a 6370 733d 2275 726e 3a6e 6574	lns:cps="urn:net
0x02f0	6c61 623a 7061 7261 6d73 3a78 6d6c 3a6e	lab:params:xml:n
0x0300	733a 6361 7474 6c65 2d70 7265 7365 6e63	s:cattle-presenc
0x0310	652d 7365 7276 6963 6522 3e0a 2020 2020	e-service">.....
0x0320	2020 2020 3c63 7073 3a74 656d 7065 7261	....<cps:tempera
0x0330	7475 7265 3e32 322e 3231 3939 3939 3c2f	ture>22.219999</
0x0340	6370 733a 7465 6d70 6572 6174 7572 653e	cps:temperature>
0x0350	0a20 2020 2020 2020 203c 6370 733a 4d49	.....<cps:MI
0x0360	5076 3643 6f41 3e5b 3366 6665 3a35 3136	Pv6CoA>[3ffe:516
0x0370	3a33 3965 303a 3234 3130 3a32 3630 3a62	:39e0:2410:260:b
0x0380	3366 663a 6665 3661 3a32 3837 615d 3c2f	3ff:fe6a:287a]</
0x0390	6370 733a 4d49 5076 3643 6f41 3e0a 2020	cps:MIPv6CoA>...

0x03a0	2020 2020 2020 3c63 7073 3a54 4f44 3e31	.....<cps:TOD>1
0x03b0	3034 3530 3433 3531 3030 3030 3c2f 6370	045043510000</cp
0x03c0	733a 544f 443e 0a20 2020 2020 203c 2f63	s:TOD>.....</c
0x03d0	7073 3a63 6174 746c 6545 7874 656e 7369	ps:cattleExtensi
0x03e0	6f6e 3e0a 2020 2020 3c2f 7374 6174 7573	on>.....</status
0x03f0	3e0a 2020 2020 3c63 6f6e 7461 6374 3e3c	>.....<contact><
0x0400	2f63 6f6e 7461 6374 3e0a 2020 3c2f 7475	/contact>...</tu
0x0410	706c 653e 0a3c 2f70 7265 7365 6e63 653e	ple>.</presence>
0x0420	0a	.

コマンド実行結果を解説する。 と同じく、結果の前半は IPv6 温度センサーから HA への通信パケットであり、後半は同じデータを HA が追跡管理基本装置へ転送した通信パケットである。

前半パケットのヘッダ部では「ESP...」という箇所より ESP による暗号化が行われていることが分かる。また、センサの CoA 「3ffe:516:39e0:2410:260:b3ff:fe6a :287a」から HA 「3ffe:516:39e0:2430::101」への通信パケットであることは分かるが、暗号化されているためパケットがカプセル化されている事は隠蔽され、さらに前半パケットの ASCII データからも、暗号化により可読データではないことがわかる。

対して後半パケットでは、トンネルモード IPsec の適用範囲は IPv6 温度センサーと HA 間だけであるため、HA が暗号化を解いて追跡管理基本装置に転送したパケットは内容が可読であり、ヘッダ部からはセンサの HoA 「3ffe:516:39e0:2430:22:fa:9ae:e801」から追跡管理基本装置の「3ffe:516:39e0:2410::102」への通信パケットであることが分かり、ASCII データの「0x0320」から「0x0340」にかけて温度データ（ASCII データのハンチング部分）を送信しており、22.219999 を計測していることが分かる。

この結果より、IPsec を用いない場合の IPv6 温度センサーと HA 間の通信パケットは解読可能(可読)であることに対して、IPsec を用いた場合の IPv6 温度センサーと HA 間の通信パケットは解読が不可能(困難)であることが確認できた。

## (2)疑似不正アクセス

IPv6 温度センサーの電源を on にする。

(1) 項と同様の設定を行い、HA と IPv6 温度センサー間の IPsec を有効にする。  
疑似不正アクセス端末 1 から IPv6 温度センサーに以下のコマンドを実行し、アクセスを試みる。

```
%ping6 3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f
```

### < コマンド実行結果 >

```
PING
3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f(3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f) from 3ffe:516:39e0:2410::199 : 56 data bytes

--- 3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f ping statistics ---
35 packets transmitted, 0 packets received, 100% packet loss
```

コマンド実行結果を解説する。不正アクセス端末 1「3ffe:516:39e0:2410::199」から IPv6 温度センサー「3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f」への通信に失敗しており、これは IPsec のポリシーに設定した、事前登録したアドレス以外からのアクセスを拒否する機能が働いたためであることが推測できる。

疑似不正アクセス端末 2(不正アクセス者が登録済み HA の IP アドレスを入手し、IP アドレスの偽装に成功したと仮定)に、事前登録されていない鍵を設定し(mn\_ipsec.sh に不正な鍵を書き込む)、以下のコマンドにより、IPv6 温度センサーと不正アクセス端末 2 の SA を比較し、鍵情報が異なることを確認する。

```
%setkey D
```

### < コマンド実行結果 >

#### < IPv6 温度センサー >

```
3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f 3ffe:516:39e0:2430::101
esp mode=any spi=268632068(0x10030004) reqid=0(0x00000000)
E: rijndael-cbc 4e45434d 4950362d 4550524f 4a454354
seq=0x00000002 replay=0 flags=0x00000040 state=mature
created: Feb  4 21:31:32 2003   current: Feb  4 21:33:18 2003
diff: 106(s)   hard: 0(s)     soft: 0(s)
last: Feb  4 21:31:36 2003   hard: 0(s)     soft: 0(s)
current: 240(bytes)   hard: 0(bytes) soft: 0(bytes)
allocated: 2   hard: 0 soft: 0
sadb_seq=1 pid=92 refcnt=2
3ffe:516:39e0:2430::101 3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f
esp mode=any spi=537067524(0x20030004) reqid=0(0x00000000)
E: rijndael-cbc 4e45434d 4950362d 4550524f 4a454354
seq=0x00000000 replay=0 flags=0x00000040 state=mature
created: Feb  4 21:31:32 2003   current: Feb  4 21:33:18 2003
diff: 106(s)   hard: 0(s)     soft: 0(s)
last: Feb  4 21:31:36 2003   hard: 0(s)     soft: 0(s)
current: 160(bytes)   hard: 0(bytes) soft: 0(bytes)
allocated: 2   hard: 0 soft: 0
sadb_seq=0 pid=92 refcnt=1
```

```
< コマンド実行結果 ( 続き ) >
< 不正アクセス端末 2 >
3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f 3ffe:516:39e0:2430::101
  esp mode=any spi=268632068(0x10030004) reqid=0(0x00000000)
  E: rijndael-cbc 4e45434d 4950372d 4550524f 4a454354
  Seq=0x00000000 replay=0 flags=0x00000040 state=mature
  Created: Feb  4 20:37:04 2003  current: Feb  4 20:38:21 2003
  diff: 77(s)  hard: 0(s)  soft: 0(s)
  last:  hard: 0(s)  soft: 0(s)
  current: 0(bytes)  hard: 0(bytes)  soft: 0(bytes)
  allocated: 0  hard: 0  soft: 0
  sadb_seq=2 pid=8464 refcnt=1
3ffe:516:39e0:2430::101 3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f
  esp mode=any spi=537067524(0x20030004) reqid=0(0x00000000)
  E: rijndael-cbc 4e45434d 4950372d 4550524f 4a454354
  seq=0x00000000 replay=0 flags=0x00000040 state=mature
  created: Feb  4 20:37:04 2003  current: Feb  4 20:38:21 2003
  diff: 77(s)  hard: 0(s)  soft: 0(s)
  last:  hard: 0(s)  soft: 0(s)
  current: 0(bytes)  hard: 0(bytes)  soft: 0(bytes)
  allocated: 0  hard: 0  soft: 0
  sadb_seq=1 pid=8464 refcnt=1
```

コマンド実行結果を解説する。前半部は IPv6 温度センサーの SA であり、後半部は HA の SA である。各ノードで双方向の設定を持っているが、ここではその内容はほぼ同じである。

実行結果のハンチング部分は鍵に関する情報を表わしており、IPv6 温度センサーと HA それぞれの情報を比べると微妙に異なることから、鍵が一致していないことが分かる。

不正アクセス端末 2 で以下のコマンドを実行し、IPv6 温度センサーにアクセスを試みる。

```
%ping6 3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f
```

```
< コマンド実行結果 >
PING6(56=40+8+8 bytes) 3ffe:516:39e0:2430::101 -->
3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f

--- 3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f ping6 statistics ---
14 packets transmitted, 0 packets received, 100% packet loss
```

コマンド実行結果を解説する。不正アクセス端末 2「3ffe:516:39e0:2430::101」から IPv6 温度センサー「3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f」への通信に失

敗

しているが、不正アクセス端末 2 の IPv6 アドレスは HA の IPv6 アドレスであるため、このアドレスによってアクセスを拒否されることは無く、不正な鍵を使ったためにアクセスが拒否されたと推測できる。

疑似不正アクセス端末 2 に、事前登録された鍵を設定し(mn\_ipsec.sh に事前登録した鍵を書き込む)、以下のコマンドにより、IPv6 温度センサーと不正アクセス端末 2 の SA を比較し、鍵情報が一致していることを確認する。

```
%setkey D
```

```
< コマンド実行結果 >
```

```
< IPv6 温度センサー >
```

```
3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f 3ffe:516:39e0:2430::101
 esp mode=any spi=268632068(0x10030004) reqid=0(0x00000000)
 E: rijndael-cbc 4e45434d 4950362d 4550524f 4a454354
 seq=0x00000002 replay=0 flags=0x00000040 state=mature
 created: Feb  4 21:31:32 2003 current: Feb  4 21:33:18 2003
 diff: 106(s) hard: 0(s) soft: 0(s)
 last: Feb  4 21:31:36 2003 hard: 0(s) soft: 0(s)
 current: 240(bytes) hard: 0(bytes) soft: 0(bytes)
 allocated: 2 hard: 0 soft: 0
 sadb_seq=1 pid=92 refcnt=2
3ffe:516:39e0:2430::101 3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f
 esp mode=any spi=537067524(0x20030004) reqid=0(0x00000000)
 E: rijndael-cbc 4e45434d 4950362d 4550524f 4a454354
 seq=0x00000000 replay=0 flags=0x00000040 state=mature
 created: Feb  4 21:31:32 2003 current: Feb  4 21:33:18 2003
 diff: 106(s) hard: 0(s) soft: 0(s)
 last: Feb  4 21:31:36 2003 hard: 0(s) soft: 0(s)
 current: 160(bytes) hard: 0(bytes) soft: 0(bytes)
 allocated: 2 hard: 0 soft: 0
 sadb_seq=0 pid=92 refcnt=1
```

```
< 不正アクセス端末 2 >
```

```
3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f 3ffe:516:39e0:2430::101
 esp mode=any spi=268632068(0x10030004) reqid=0(0x00000000)
 E: rijndael-cbc 4e45434d 4950362d 4550524f 4a454354
 seq=0x00000000 replay=0 flags=0x00000040 state=mature
 created: Feb  4 20:47:35 2003 current: Feb  4 20:47:51 2003
 diff: 16(s) hard: 0(s) soft: 0(s)
 last: hard: 0(s) soft: 0(s)
 current: 0(bytes) hard: 0(bytes) soft: 0(bytes)
 allocated: 0 hard: 0 soft: 0
 sadb_seq=3 pid=8495 refcnt=1
3ffe:516:39e0:2430::101 3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f
 esp mode=any spi=537067524(0x20030004) reqid=0(0x00000000)
 E: rijndael-cbc 4e45434d 4950362d 4550524f 4a454354
 seq=0x00000000 replay=0 flags=0x00000040 state=mature
 created: Feb  4 20:47:35 2003 current: Feb  4 20:47:51 2003
 diff: 16(s) hard: 0(s) soft: 0(s)
 last: hard: 0(s) soft: 0(s)
 current: 0(bytes) hard: 0(bytes) soft: 0(bytes)
 allocated: 0 hard: 0 soft: 0
```

```
sadb_seq=2 pid=8495 refcnt=1
```

コマンド実行結果を解説する。IPv6 温度センサーと不正アクセス端末の鍵情報（ハンチング部分）を比較すると、内容が同じであることが確認できる。これにより、鍵が一致していることが分かる。

不正アクセス端末 2 で以下のコマンドを実行し、IPV6 温度センサーにアクセスを試みる。

```
%ping6 3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f
```

```
< コマンド実行結果 >
PING6(56=40+8+8 bytes) 3ffe:516:39e0:2430::101 -->
3ffe:516:39e0:2421:260:b3ff:fe6a:ec9f
16 bytes from 3ffe:516:39e0:2421:260:b3ff:fe6a:ec9f, icmp_seq=0 hlim=62
time=16.267 ms
16 bytes from 3ffe:516:39e0:2421:260:b3ff:fe6a:ec9f, icmp_seq=1 hlim=62
time=4.563 ms
16 bytes from 3ffe:516:39e0:2421:260:b3ff:fe6a:ec9f, icmp_seq=2 hlim=62
time=4.128 ms
16 bytes from 3ffe:516:39e0:2421:260:b3ff:fe6a:ec9f, icmp_seq=3 hlim=62
time=4.354 ms

--- 3ffe:516:39e0:2421:260:b3ff:fe6a:ec9f ping6 statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/std-dev = 4.128/7.328/16.267/5.163 ms
```

コマンド実行結果を解説する。不正アクセス端末 2「3ffe:516:39e0:2430::101」から IPv6 温度センサー「3ffe:516:39e0:2430:260:b3ff:fe6a:ec9f」への通信に成功しているが、これは、鍵を一致させたことによるものだと言える。

この結果より、疑似不正アクセス端末からの接続は、事前に定義された鍵を用いた場合のみ可能であることが確認できた。

### (3)MIPv6 と IPsec の同時動作

IPv6 温度センサーを「場所 1」に配置し、電源を on にする。

(1) 項と同様の設定を行い、HA と IPv6 温度センサー間の IPsec を有効にする。

HA で以下のコマンドにより、BC の状態を確認する。

```
%mip6control c
```

< コマンド実行結果 >						
phaddr	addr		pcoa	flags	seqno	lifetim
	ltxp	state				
sensor22						
3ffe:516:39e0:2410:260:b3ff:fe6a:ec9f					3ffe:516:39e0:2430::101	
AHSD--	39178	416	355	---		

コマンド実行結果を解説する。IPv6 温度センサーは「場所 1」の Prefix を持った CoA「3ffe:516:39e0:2410:260:b3ff:fe6a:ec9f」を取得できており、センサと HA の通信が可能なが分かる。

IPv6 温度センサーを「場所 2」に移動させる。

HA で以下のコマンドにより BC の状態を確認する。

```
%mip6control c
```

< コマンド実行結果 >						
phaddr	addr		pcoa	flags	seqno	lifetim
	ltxp	state				
sensor22						
3ffe:516:39e0:2421:260:b3ff:fe6a:ec9f					3ffe:516:39e0:2430::101	
AHSD--	65393	416	339	---		

コマンド実行結果を解説する。IPv6 温度センサーは「場所 2」の Prefix を持った CoA「3ffe:516:39e0:2421:260:b3ff:fe6a:ec9f」を取得できており、センサと HA の通信が可能なが分かる。

この結果より、IPsec が有効な状態で CoA の変化が起きても、通信に問題がないことが確認できた。

## 2.5 結果と考察

本章では「IPv6 温度センサーへの IPsec の実装実験」として、3 つの実験を行った。それぞれの結果をまとめ、考察する。

### (1) IPsec の暗号化動作

この実験は、IPsec によるデータの暗号化の有効性を確認するものであり、1.4 実験実施結果(1)項に示した通り、IPsec を無効とした場合はデータが可読であったのに対して、IPsec により暗号化されたデータは解読できないことが確認できた。

### (2) 疑似不正アクセス

この実験は、IPsec による通信を行っているノードに対して、不正アクセス端末より、IPsec 通信を試み、事前に定義された鍵を使うことの有効性を確認するものであり、1.4 実験実施結果(2)項に示した通り、事前に定義された鍵を使用しなかった場合は、通信に失敗し、事前に定義した鍵を使うことで通信に成功することが確認できた。また、IPsec のポリシー設定により、事前に通信可能なアドレスを登録することで、未登録のアドレスからの通信も失敗することを確認できた。

### (3) モバイル IPv6 と IPsec の同時動作

この実験は、モバイル IPv6 の動作により、MN の CoA が変化した場合でも IPsec 通信を正常に行うことができるかを確認するものであり、1.4 実験実施結果(3)項に示した通り、IPsec を有効とした環境下において、MN を移動させた場合においても、CoA の更新が正常に行われ、モバイル IPv6 と IPsec が同時に動作していることが確認できた。

IPv6 温度センサーへの IPsec 実装実験として、IPsec によるデータの秘匿性、認証といった機能と、MN が移動することによって、動的にアドレスを変化させるモバイル IPv6 と認証機能を持つ IPsec の同時動作についての検証であったが、いずれも想定通りの動作を行い、IPv6 温度センサーに IPsec を実装することが充分可能であると言える。

### 3 その他（技術的）

#### 3.1 結果と改善点

技術面の結果としては、IPv6 温度センサーとモバイル IPv6 による温度データ取得と位置データの取得、およびモバイル IPv6 と IPsec を同時動作させ、データの暗号化および不正アクセス防止に一定の効果があることが検証できた。基本的なインフラの整備および動作検証という観点からすれば、良好な結果が得られたと言える。

しかし、本実験を実用に向けてより高度化するにあたって、追跡管理システムの技術的な改善点として、以下を挙げる。

##### (1) データ取得の完全リアルタイム化

遠隔監視システムに共通して言えることであるが、現在、IPv6 温度センサーとサーバ間のデータ通信は、IPv6 温度センサーが自立で起動したタイミングでのみ可能であり、サーバから任意のタイミングでデータ要求を行うことができない。これは IPv6 温度センサーがバッテリー動作しており、動作時間を確保するために間欠動作を行っているためである。IPv6 温度センサー本体の改良により、電源に不安が無くなった際に、任意のタイミングでのデータ取得が可能になる。

##### (2) IPv6 温度センサーの温度計測方法の検討および小型化・省電力化

今回開発した IPv6 温度センサーは、生きた牛への取付を重視して開発されたため、と畜後の枝肉およびさらに細かく切断された食肉への取付には向いていない。

枝肉への取付にあたっては、保存時の肉内部の温度計測が重要であるため、肉内部の温度計測が今後の課題になると思われるが、食品としての安全性および商品価値に影響を与えない計測が可能な IPv6 温度センサーを開発する必要がある。

枝肉をさらに切断した食肉へのセンサの取付に関しては、IPv6 温度センサーの小型化もさることながら、出荷後の駆動時間を充分確保する必要があり、バッテリーの高性能化および IPv6 温度センサーの省電力化も重要な課題となる。

##### (3) 食肉への IPv6 アドレス割り当て

今回の実験では、牛一頭に対して、固有な IPv6 アドレスを割り当てることを考えたが、枝肉が切断されて食肉として流通することを考えると、それだけでは不十分になる。単に食肉に IPv6 アドレスを割り当てることは簡単であるが、牛の IPv6 アドレスから一定のルールにより生成可能な IPv6 アドレスを食肉に割り当て、最終的には、食肉の偽装防止に利用することが課題となる。

##### (4) モバイル IPv6 と IPsec（プリシェアド鍵方式）の同時動作

今回、実証実験でモバイル IPv6 と同時に動作した IPsec は固定鍵方式を採用したが、より高度なセキュリティ確保可能なプリシェアド鍵方式の採用は今後の課題となる。プリシェアド鍵方式では、事前認証および鍵生成（固定鍵方式では事前設定）が行われるため、アドレスが動的に変化するモバイル IPv6 への対応や、省電力化を目標とする MN への負担増などが課題となる。

これらの改善点をクリアすることにより、実用に向けたシステム構築が可能になるものと考えられる。

#### 4 消費者の安心感の向上

##### 4.1 実験要求事項

IPv6 による追跡管理が可能になることにより、消費者の安心感が向上したかどうか、ヒアリング・アンケートにより検証する。

##### 4.2 実験仕様、手順

今回の実験フィールドである山梨県において、2/24～26の期間中に一般モニターを対象とした以下のようなアンケートを実施した。アンケート実施前に畜産物情報追跡管理システム及び農産物情報追跡管理システムの概要について説明し、モニター装置を使って、画面操作を行って頂いた。それぞれのシステムの画面例を資料3-2として添付する。

###### <アンケート内容>

- (1) 牛個体に重複しない番号を付けて管理する事で、牛肉の生産者や流通経路に関する情報が検索可能となれば、牛肉に対する安心感はどの程度向上しますか？  
非常に向上する 　少しは向上する 　全く向上しない 　その他(具体的に)
- (2) 洋蘭に重複しない番号を付けて管理する事で、洋蘭の生産者や流通経路に関する情報が検索可能となれば、商品に対する安心感はどの程度向上しますか？  
非常に向上する 　少しは向上する 　全く向上しない 　その他(具体的に)

### 4.3 実験実施環境

4.2 項の実験を実施した環境の概略図を図 3-4-1 に示す。

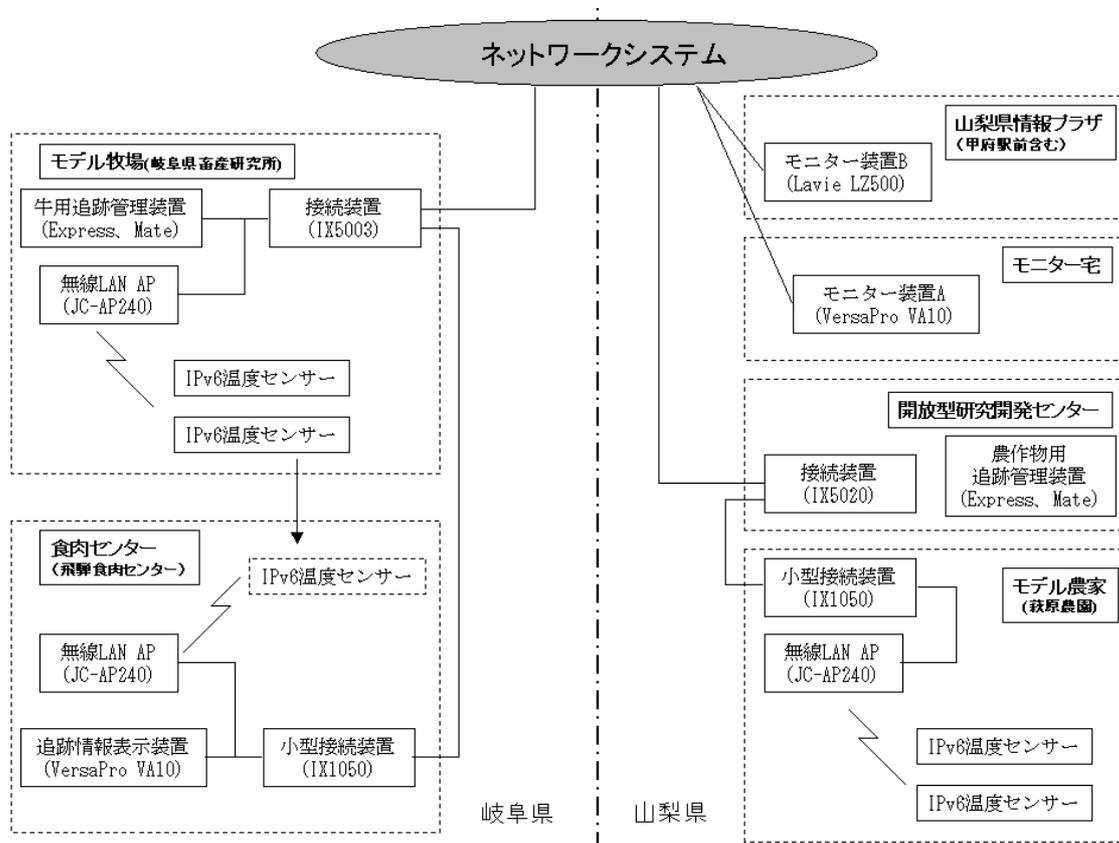


図 3-4-1 実験実施環境概略図

図 3-4-1 を説明する。「モデル牧場」と「食肉センター」は岐阜県に存在し、この間を IPv6 温度センサーが牛の出荷に合わせて移動を行う。「山梨県情報プラザ」「モニター宅」「開放型研究開発センター」「モデル農家」は山梨県に存在し、一般モニターは「山梨県情報プラザ」と「モニター宅」にて、畜産物情報追跡管理システム及び農産物情報追跡管理システムにアクセスし、画面操作を行って頂いた。山梨県情報プラザでのアンケート時の様子を写真 3-4-1 に示す。



写真 3-4-1 山梨県情報プラザでのアンケート実施風景

#### 4.4 実験実施結果

(1) 畜産物情報追跡管理システムによる消費者の安心感の向上  
アンケートの(1)に対する回答は図 3-4-2 のようになった。

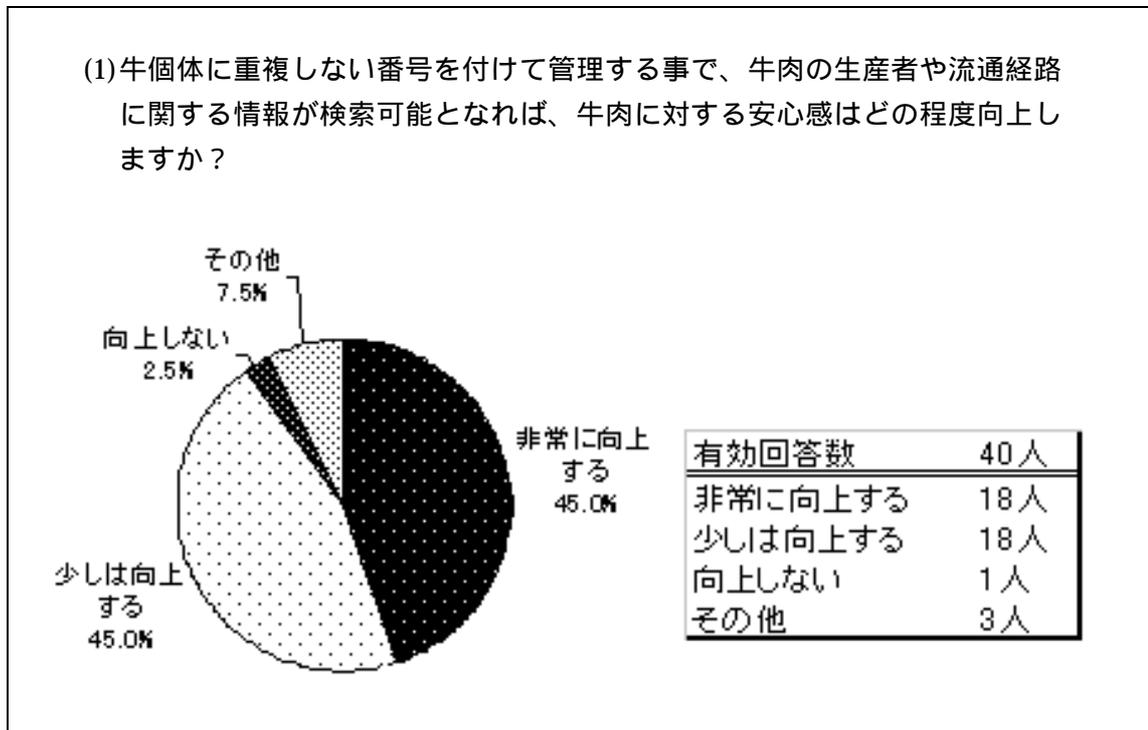


図 3-4-2 追跡管理による牛肉の安心感向上について

「非常に向上する」「少しは向上する」と答えた人が全体の 90%を占め、追跡管理の有効性を期待する意見が多い。

「その他」と答えた人からは以下のような具体的意見が得られた。

- ・エサの流過程をより具体的にさせる必要がある
- ・牛1頭を購入するわけではない
- ・表示される情報の信頼性向上が重要

(2) 農産物情報追跡管理システムによる消費者の安心感の向上  
アンケートの(2)に対する回答は図 3-4-3 のようになった。

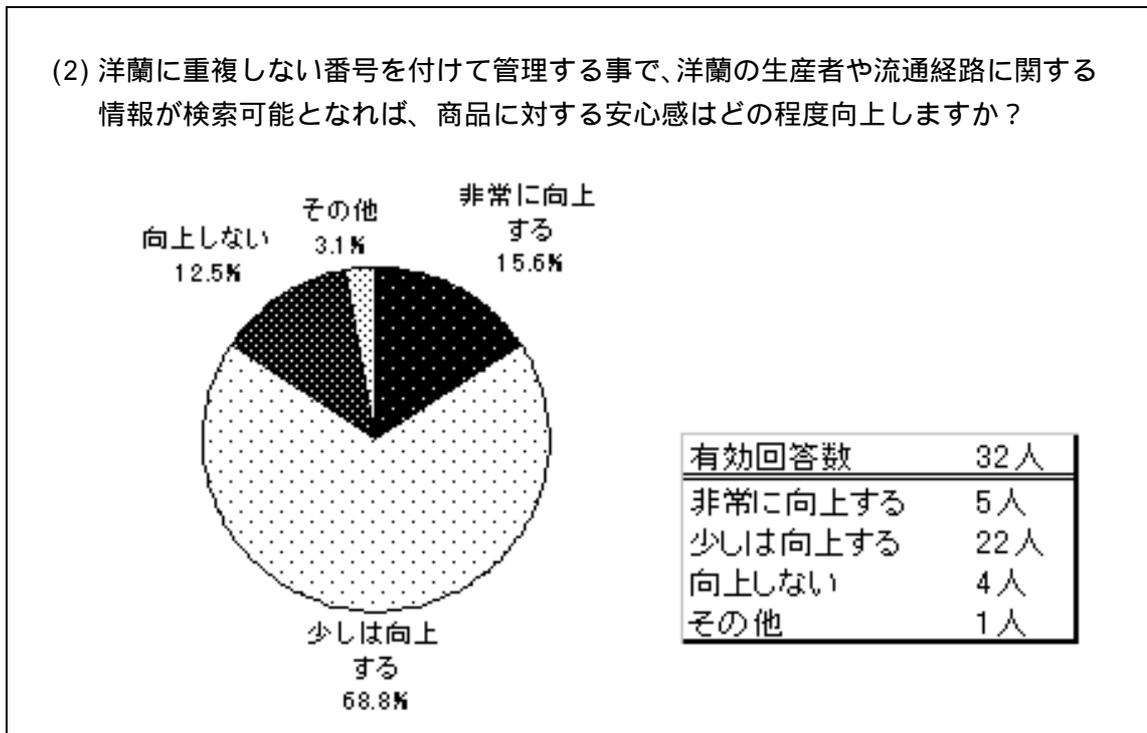


図 3-4-3 追跡管理による洋蘭の安心感向上について

「非常に向上する」「少しは向上する」と答えた人が全体の約 85%を占めているが、牛肉の安心感向上に比べると、「非常に向上する」の割合がかなり少なくなっている。

「その他」と答えた人からは以下のような具体的意見が得られた。

- ・安心感は向上しないが、ブランド化に期待ができる

#### 4.5 結果と考察

本実験では牛肉と洋蘭を対象とした、追跡管理に対する安心感の向上についてのアンケートを実施したが、牛肉においても洋蘭においても共に「安心感が向上する」という結果を得ることができた。しかしながら、食品である牛肉と非食品である洋蘭を比較すると、牛肉の追跡管理に対する期待が大きい。

安心感向上のために、技術的課題でも述べたが、枝肉後の追跡を可能とする仕組み作りが必須である。加えて詳細な情報の公開と、公開した情報の正確性を保証する仕組み作りが今後の課題となる。

## 5 生産物の価値の向上

### 5.1 実験要求事項

消費者が IPv6 により追跡管理された農畜産物を追跡管理されていない農畜産物に比べて高額であっても購入する意志を有するかどうか、ヒアリング・アンケートにより検証する。

### 5.2 実験仕様、手順

4.2 項のアンケート実施時に合わせて以下のアンケートを実施した。

<アンケート内容>

(1) 生産者や流通経路を検索可能な牛肉が、検索不可能な牛肉に比べて、どの程度まで高額であっても購入したいと思いますか。

2倍以上 1.5倍 1.3倍 1.2倍 1.1倍 1.05倍 同額でないを買わない  
同額であっても買わない その他(具体的に)

(2) 生産者や流通経路を検索可能な洋蘭が、検索不可能な洋蘭に比べて、どの程度まで高額であっても購入したいと思いますか。

2倍以上 1.5倍 1.3倍 1.2倍 1.1倍 1.05倍 同額でないを買わない  
同額であっても買わない その他(具体的に)

### 5.3 実験実施環境

5.2 項の実験を実施した環境の概略図を図 3-5-1 に示す。

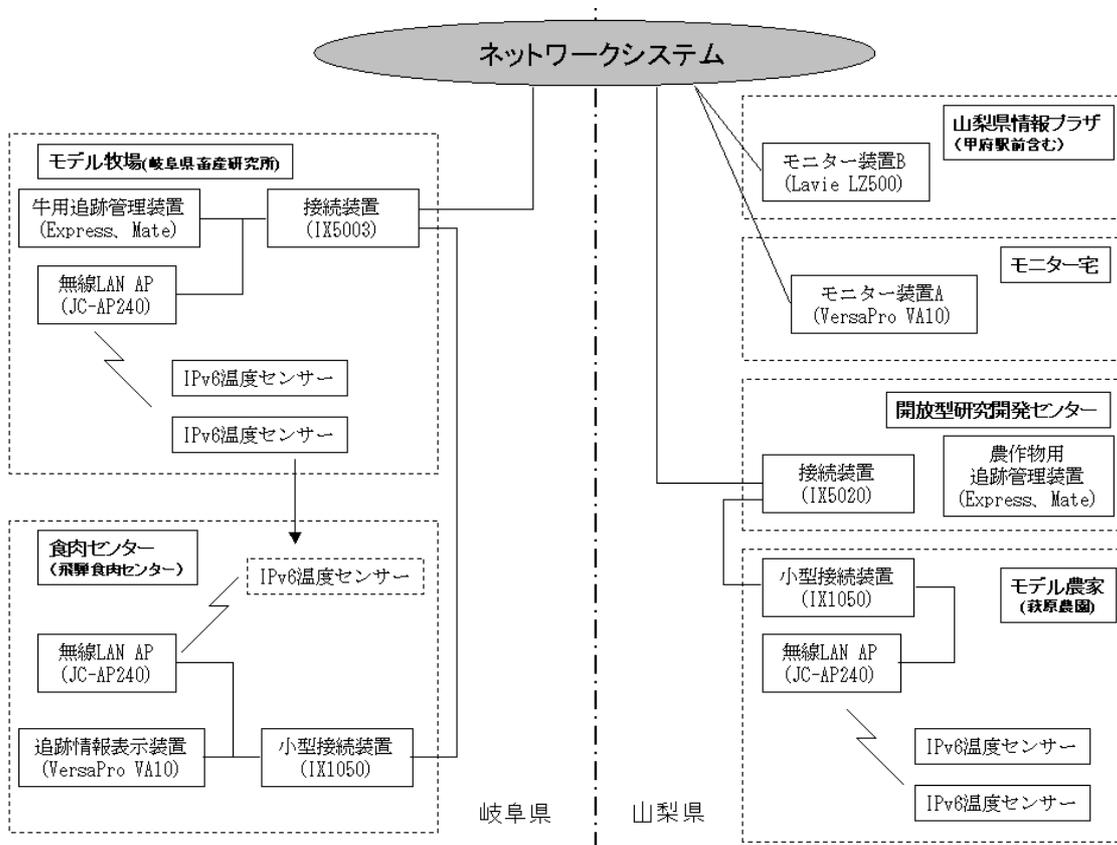


図 3-5-1 実験実施環境概略図

図 3-5-1 を説明する。「モデル牧場」と「食肉センター」は岐阜県に存在し、この間を IPv6 温度センサーが牛の出荷に合わせて移動を行う。「山梨県情報プラザ」「モニター宅」「開放型研究開発センター」「モデル農家」は山梨県に存在し、一般モニターは「山梨県情報プラザ」と「モニター宅」にて、畜産物情報追跡管理システム及び農産物情報追跡管理システムにアクセスし、画面操作を行って頂いた。

#### 5.4 実験実施結果

##### (1) 畜産物追跡管理システムによる生産物の価値の向上

アンケートの(1)に対する回答は図 3-5-2 のようになった。

(1) 生産者や流通経路を検索可能な牛肉が、検索不可能な牛肉に比べて、どの程度まで高額であっても購入したいと思いますか。

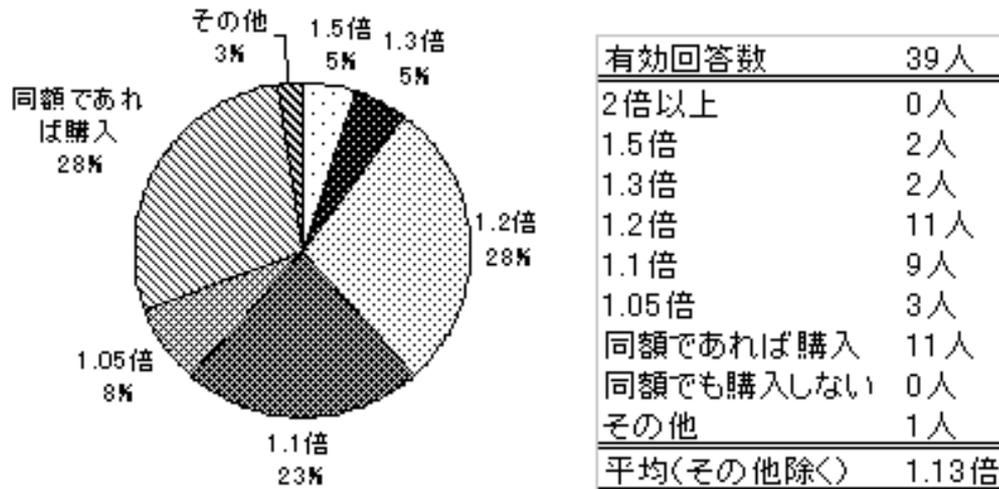


図 3-5-2 追跡管理による牛肉の価値向上について

「1.2倍」「同額であれば購入」の回答が最も多く、次に「1.1倍」の回答が多かった。

「その他」と答えた人の意見は「分からない」であった。

(2) 農産物追跡管理システムによる生産物の価値の向上

アンケート(2)に対する回答は図 3-5-3 のようになった。

(2) 生産者や流通経路を検索可能な洋蘭が、検索不可能な洋蘭に比べて、どの程度まで高額であっても購入したいと思いますか。

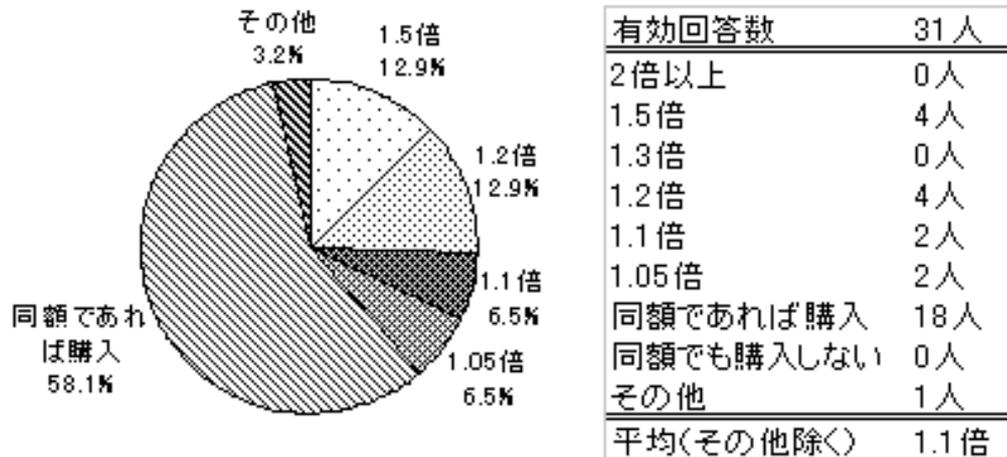


図 3-5-3 追跡管理による洋蘭の価値向上について

「同額であれば購入」の回答が他を圧倒している。しかしながら、「1.5倍」と答えた人も4人居る。

「その他」と答えた人からは以下のような具体的意見が得られた。

- ・アフターケア(サービス)が含まれるなら少々高くても良い

## 5.5 結果と考察

本実験では牛肉と洋蘭を対象とした、追跡管理に対する価値の向上についてのアンケートを実施した。牛肉に関しては、70%程度の人が金銭的負担があっても追跡管理された牛肉の購入を行うと回答しており、追跡管理による価値の向上が認められる。一方、洋蘭に関しては、金銭的負担を許容するのは40%に減り、やはり食品に比べると、追跡管理による価値向上が難しいとも言える。しかし、アンケートの回答にもあったように、生産者と直結した「アフターサービス」を可能とすることで、食品とは異なった付加価値の向上が可能となり、食品以外の様々な商品に対する応用も期待できる。

また、アンケート実施時には、牛肉と洋蘭に関わらず「追跡管理によるコストを価格に転嫁するのはどうか」といった声を聞く事も多く、「同額でないと買わない」を選んだ人の多数が、こういった意見であるのではないかと考えられる。

## 6 生産者の意識変化

### 6.1 実験要求事項

IPv6により追跡管理されることにより、生産者の意識がどのように変化したかどうか、生産者の顔が見えることによるメリットとセキュリティ・プライバシーに係る懸念のデメリットの両面についてヒアリング・アンケートにより検証する。

### 6.2 実験仕様、手順

今回の実験フィールドである山梨県および岐阜県において、2/24～3/7の間に山梨県モデル農家および岐阜県モデル牧場の方々を対象とした以下のようなアンケートを実施した。アンケート実施前に畜産物情報追跡管理システム及び農産物情報追跡管理システムの概要について説明し、システムのモニターを使って画面操作を行って頂いた。それぞれのシステムの画面例は資料3-2として添付する。

<アンケート内容>

- (1) 消費者に生産者の顔が見えるようになることで、意識が変わりますか？(複数選択可)  
より品質の高い商品を提供しなければと思う。  
生産者をアピールできるような商品を提供したいと思う。  
特に変わらない。  
その他(具体的に)
- (2) 消費者に生産者の情報を公開することによって、考えられるメリットについて挙げて下さい。(複数選択可)  
商品を安心して購入してもらうことができる。  
生産者個人がブランド化され、商品の付加価値を高めることができる。  
その他(具体的に)
- (3) 消費者に生産者の情報を公開することによって、考えられるデメリットについて挙げて下さい。(複数選択可)  
生産者の個人情報が漏れる。  
今まで以上に品質に気を遣い、コスト高になる。  
その他(具体的に)

### 6.3 実験実施環境

6.2 項の実験を実施した環境の概略図を図 3-6-1 に示す。

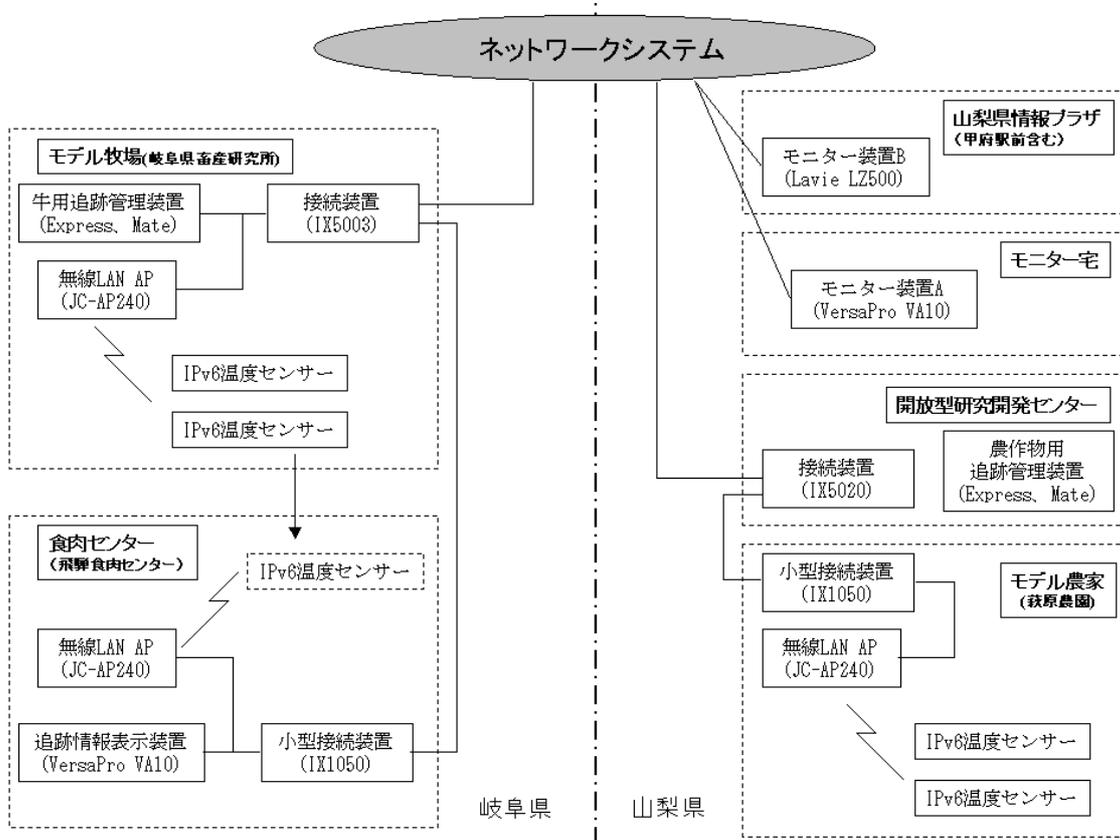


図 3-6-1 実験実施環境概略図

図 3-6-1 を説明する。「モデル牧場」と「食肉センター」は岐阜県に存在し、この間を IPv6 温度センサーが牛の出荷に合わせて移動を行う。「山梨県情報プラザ」「モニター宅」「開放型研究開発センター」「モデル農家」は山梨県に存在する。「モデル牧場」および「モデル農家」の方々に畜産物情報追跡管理システム及び農産物情報追跡管理システムのモニターを利用して、画面操作を行って頂いた。

## 6.4 実験実施結果

### (1) 追跡管理による生産者の意識変化

アンケート(1)に対する回答は表 3-6-1 のようになった。

表 3-6-1 追跡管理による生産者の意識変化について

(1)消費者に生産者の顔が見えるようになることで、意識が変わりますか？(複数選択可)	回答者数 12人
より品質の高い商品を提供しなければと思う。	11人
生産者をアピールできるような商品を提供したいと思う。	8人
特に変わらない。	0人
その他	1人

「より品質の高い商品を提供」と「生産者をアピール」の両方をほとんどの回答者が選択しており、追跡管理によって生産者の意識は向上するという結果が得られた。

「その他」を選んだ人においても、「安全な商品を提供したい」という意見であり、生産者の意識の高さが伺える。

### (2) 追跡管理による生産者の考えるメリット

アンケート(2)に対する回答は表 3-6-2 のようになった。

表 3-6-2 追跡管理による生産者の考えるメリットについて

(2)消費者に生産者の情報を公開することによって、考えられるメリットについて挙げて下さい。(複数選択可)	回答者数 12人
商品を安心して購入してもらうことができる。	6人
生産者個人がブランド化され、商品の付加価値を高めることができる。	10人
その他	2人

「商品を安心して購入」の6人に対して、「生産者個人がブランド化」と答えた人が10人という結果が選られた。これは、安全性だけではなく、その他の付加価値を加えた総合的な価値向上に繋がるという期待の現われだと言える。

「その他」を選んだ人においては、「情報公開により生産者個人の考え方を消費者に伝える事が容易になる」「生産現場に対して消費者が目を向けるきっかけになれば」という意見もあった。

### (3) 追跡管理による生産者の考えるデメリット

アンケート(3)に対する回答は表 3-6-3 のようになった。

表 3-6-3 追跡管理による生産者の考えるデメリットについて

(3)消費者に生産者の情報を公開することによって、考えられるデメリットについて挙げて下さい。(複数選択可)	回答者数 12人
生産者の個人情報漏れる。	7人
今まで以上に品質に気を遣い、コスト高になる。	4人
その他	1人

「生産者の個人情報漏れる」を選択した人が一番多く、生産者の情報をどこまで公開するのが、今後の検討課題だと言える。また、「コスト高になる」が4人居

たが、これは消費者向けのアンケート結果にもあったように、追跡管理によるコスト高の価格への転嫁を懸念するものだと言える。

「その他」を選んだ人においては、「追跡管理の情報を偽造することに対する注意が必要」という意見があり、情報の信頼性対策が充分でなければ、消費者に対してはマイナスイメージになることへの懸念であると考えられる。

## 6.5 結果と考察

本実験では、畜産業(牛肉)および農産業(洋蘭)を営む生産者に対して、追跡管理システムによる生産者の意識変化についてのアンケートを実施した。牛肉か洋蘭かに関わらず、追跡管理によって、消費者に対して商品の生産者が公開されることに対する前向きな意識変化を期待できることが分かった。

しかし、生産者の懸念材料として「個人情報の漏洩」「コスト高」「情報の信頼性確保」が挙げられている。「個人情報の漏洩」については、IPsecの利用等による技術上対策に加えて「消費者が必要とする情報」と「生産者が公開可能な情報」の両側面から対応の検討が必要となる。「コスト高」「情報の信頼性」についても今後の課題として取り組む必要がある。

## 7 その他（社会的）

### 7.1 結果と改善点

ヒアリング・アンケートによる社会的検証の結果としては、消費者および生産者共に、追跡管理による品質保証に一定の効果があるという意識が高いことが検証できた。

また、消費者からは、規定のアンケート以外に以下のような意見が挙がった。

- ・情報が公開されても情報が改竄されてしまうことが懸念され、信頼できる人間（第三者機関）による保証が必要ではないか。
- ・洋蘭は食品ではないので、詳しく知ろうとは思わない。
- ・公開した情報に対して、一般の人が理解可能な指標を設けるべき。
- ・生産者の情報に加えて、商品の品質（ランク、人気度など）も合わせて表示されると良い。
- ・狂牛病問題の対策に非常に役立つと思われる。
- ・国際的にスタンダードなシステムへの展開が必要。
- ・物流の過程で温度のセンシングなどの高度な管理が必要なものはない。
- ・情報公開できない生産者は淘汰されるのではないか。

これらの意見は、追跡管理システムへの期待と共に、現状で不足している点を明確に指摘しているものが多い。

この結果も踏まえて、追跡管理システムの今後の改善点として、以下を挙げる。

#### (1) 公開データの信頼性確保

データ通信上は IPsec などの技術を使用する事により、データの信頼性を高める事が可能であるが、元となるデータの入力および商品を取り扱うのは人間であり、「公開データの信頼性に疑問」といった意見が複数挙がった。技術的に対応可能な部分もあるが、人間が行う作業部分については、「作業方式を明文化し第三者機関での認証を行う」などの信頼性確保を課題とする。

#### (2) 生産者および流通業者へのフィードバック

追跡管理システムにより、消費者と生産者が直接繋がり、消費者から生産者へのフィードバックが容易になると考えられる。生産者は消費者のニーズを知る事ができ、より質の高い生産活動を行う事が可能になると考えられ、追跡管理システムにフィードバック機能の追加が望まれる。

#### (3) 商品の在庫管理

追跡管理システムの位置追跡を応用し、商品の在庫管理を行うことを目指す。IPv6 通信可能なタグを商品に取り付け、位置追跡による商品の有無と、データ通信による賞味期限等の情報を組み合わせることで、人手を介さない在庫管理が可能になる。

これらの改善点をクリアすることで、生産者および消費者によりメリットの多いシステムになると考えられる。