災害時における802.1X認証をベースとしたネットワークリソース割り当て制御システム

○渡辺俊貴*，木下峻一*，山崎康広**，後藤英昭*，曽根秀昭*
*東北大学サイバーサイエンスセンター
**NEC クラウドシステム研究所

2013年3月4日(月)
第6回ネットワーク仮想化時限研究専門委員会

発表の流れ

- 研究背景
- 災害時避難所等で要求されるアクセス制御
- ネットワークリソース割り当て制御システム
- プロトタイプシステムを用いた動作検証
- まとめ

研究背景

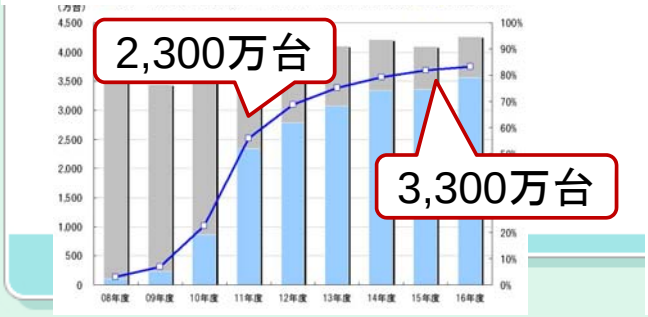
- 災害時に避難所や駅等で多数のネットワーク利用者が発生
  - 避難所：平均300人程度，最大3,000人程度が集中(3/14@仙台市)
  - 帰宅困難者：主要駅では1,000人以上(3/11,21:00@首都圏)

出典：宮城県ホームページ・警察庁広報資料

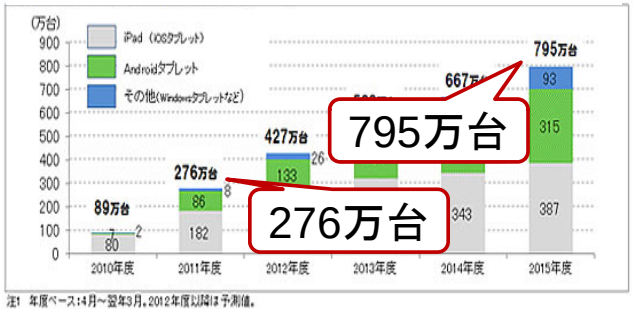
- 無線LAN通信機能を備える端末の普及
  - スマートフォン，タブレット端末等

⇒災害時避難所等における情報収集の手段として
無線LAN通信機能を備える端末が有効

MM総研：スマートフォン市場規模の推移・予測(12年3月)



ICT総研：タブレット端末市場に関する需要動向調査



災害時避難所等での無線通信の課題

- 災害時避難所等でアクセスポイントを無料開放することが期待される.
  - 導入，管理コストの観点から災害時専用のアクセスポイントの用意は困難

⇨ 平常時に利用しているアクセスポイントを災害時に無料開放
⇨ 災害時に迅速かつ安全にアクセスポイントを開放する仕組みが必要

- 1か所のアクセスポイント付近に大勢のユーザが集まる.
  - アクセスの集中により通信効率が低下

⇨ 災害時に重要なユーザ・通信の判断して優先的に処理

研究目的

- 災害時におけるネットワークリソース割り当て制御の実現
  各種サーバへのアクセス権限，通信の優先度
  - ユーザやフローに応じて，柔軟にアクセス権限・優先度の設定
    - フロー：意味のあるデータのまとまり
  - 迅速かつ容易にアクセス権・優先度を反映

[アプローチ]

- ユーザ認証時に得られるユーザの属性情報とネットワーク提供機関側のアクセスポリシー等を考慮してアクセス権限・優先度を決定
- OpenFlowを用いてアクセス制御を実行

災害時におけるアクセス制御への要求

- 事前設定の少なさ
  - 災害時用の情報としてあらかじめ避難所側に設定しておく情報を最小限に抑える.

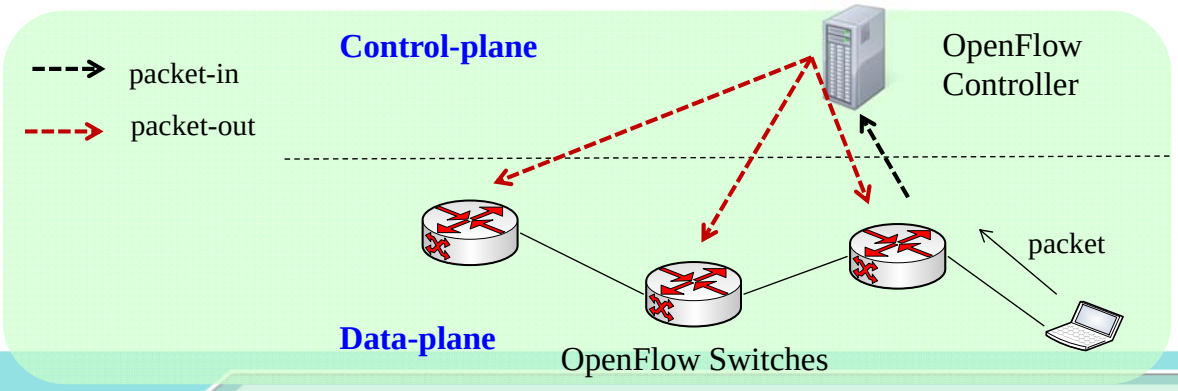
  ⇒災害時に必要なユーザ情報を属性情報として，認証時に取得
- 災害時を想定した柔軟なアクセス制御
  - 一般ユーザや公共機関ユーザに対して個別にアクセス権限を設定
  - 公共機関ユーザの通信，災害関係のサイトへのアクセス等を優先処理

  ⇒認証時の属性情報を利用して柔軟にアクセス権限・優先度を設定
- 容易かつ迅速なアクセスポイントの開放，ポリシーの設定
  - 専門的な知識がない避難所責任者でも容易に設定変更可

  ⇒OpenFlowを利用してネットワーク機器を集中管理・制御

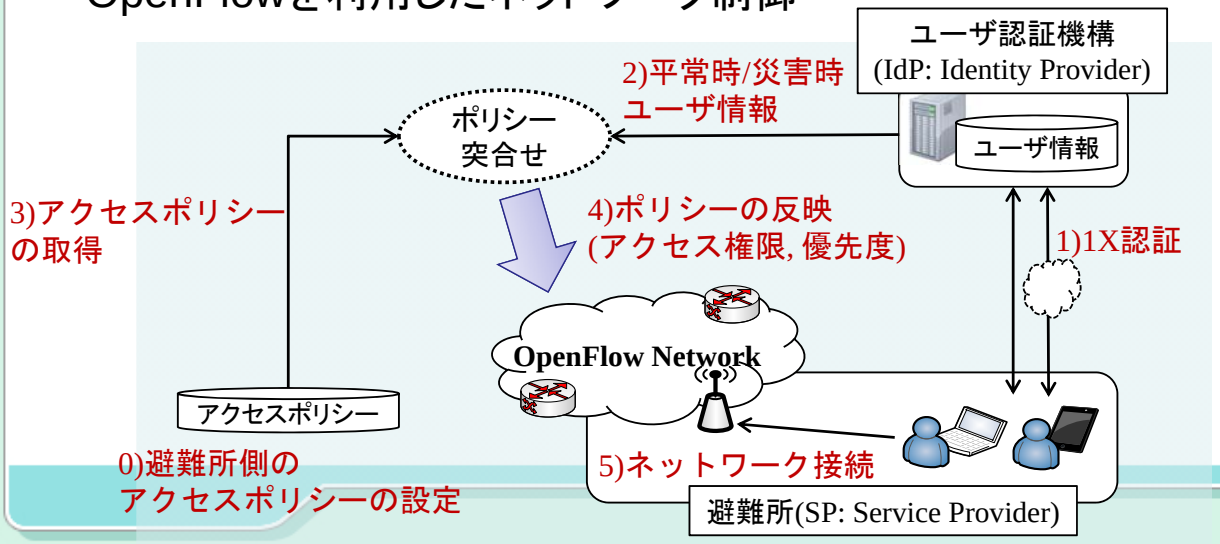
OpenFlow

- データプレーンとコントロールプレーンが独立したネットワーク制御技術
  - OpenFlow Controller(OFC)が集中的に経路制御等を行う.
    - OFSはパケットを受信時，転送先情報を保持していなければOFCにパケットを転送(packet-in)
    - OFCはパケットの転送先を計算して，パケットの転送情報を各OFSに通知(packet-out)



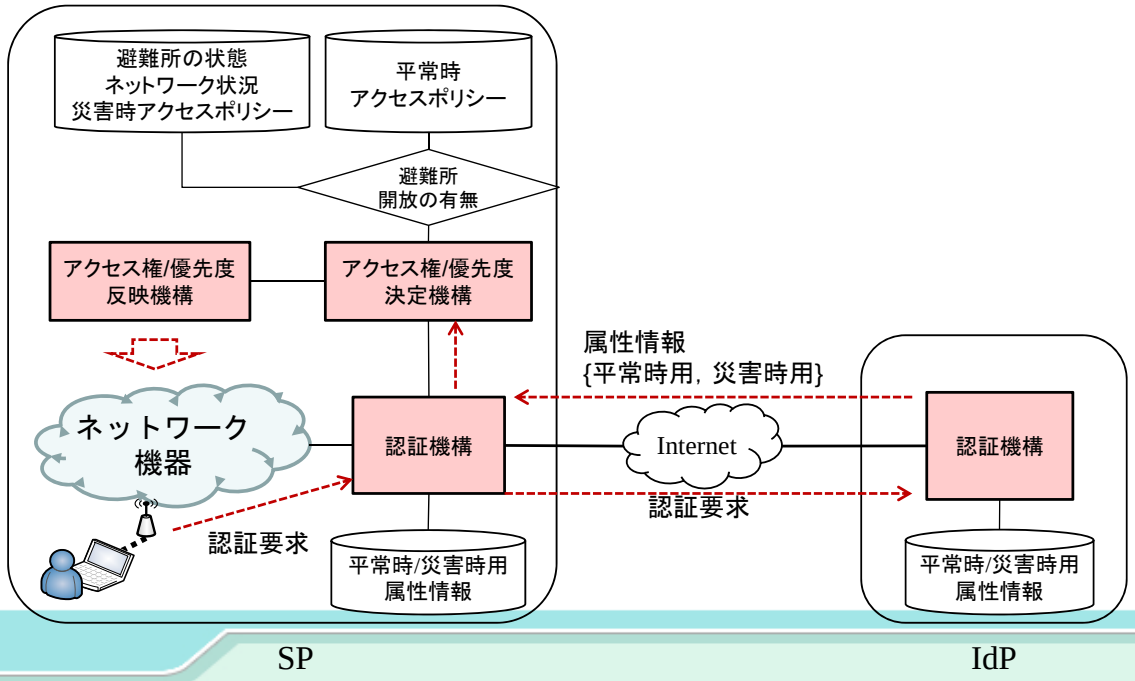
本システムで想定する認証環境

- ユーザは避難所からアクセス時，802.1Xに基づく認証を行う
  - 平常時からの利用者，公共機関ユーザはユーザ登録済み
  - 一般の避難者には共有アカウントの配布や認証失敗者に対する制御
- 認証後，ユーザ情報と避難所側のアクセスポリシーの突合せ
- OpenFlowを利用したネットワーク制御



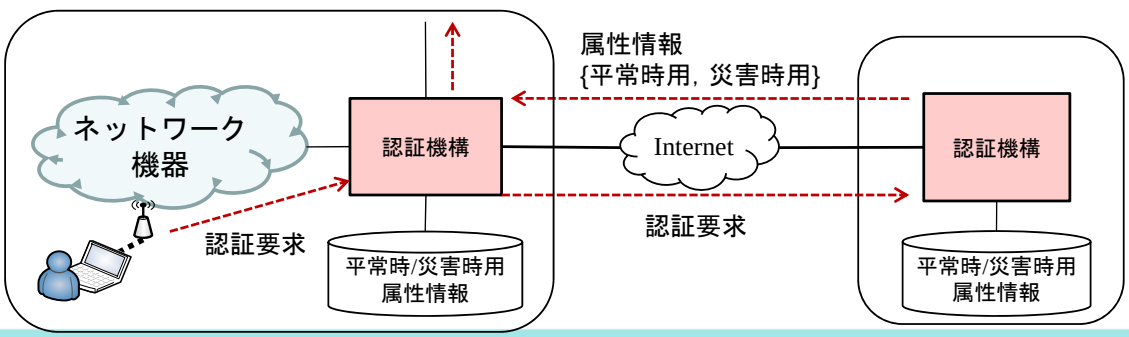
ネットワークリソース割り当て制御システム

- 提案システムの構成
  - 認証機構，アクセス権/優先度決定機構，アクセス権/優先度反映機構



認証機構(1/3)

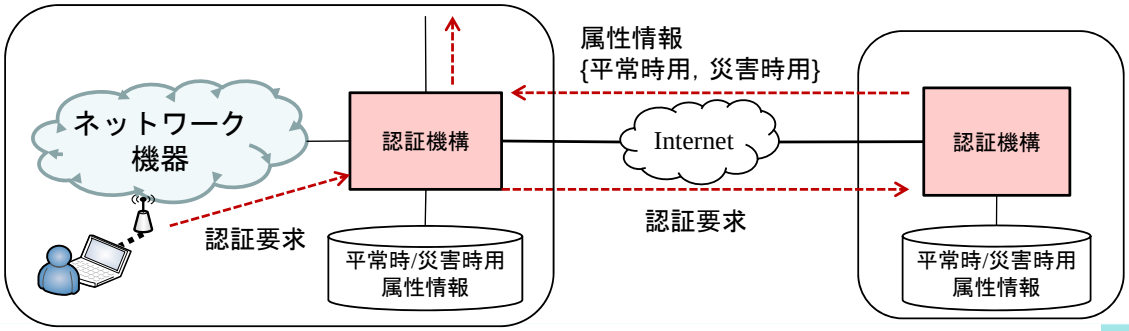
- 1)IEEE802.1Xに基づくユーザ認証を行う.
- 2)平常時/災害時用のユーザの属性情報をDBから抽出
  - ローミング認証の場合は認証結果メッセージに付加して返信



認証機構(2/3)

- 平常時用/災害時用の属性情報の定義

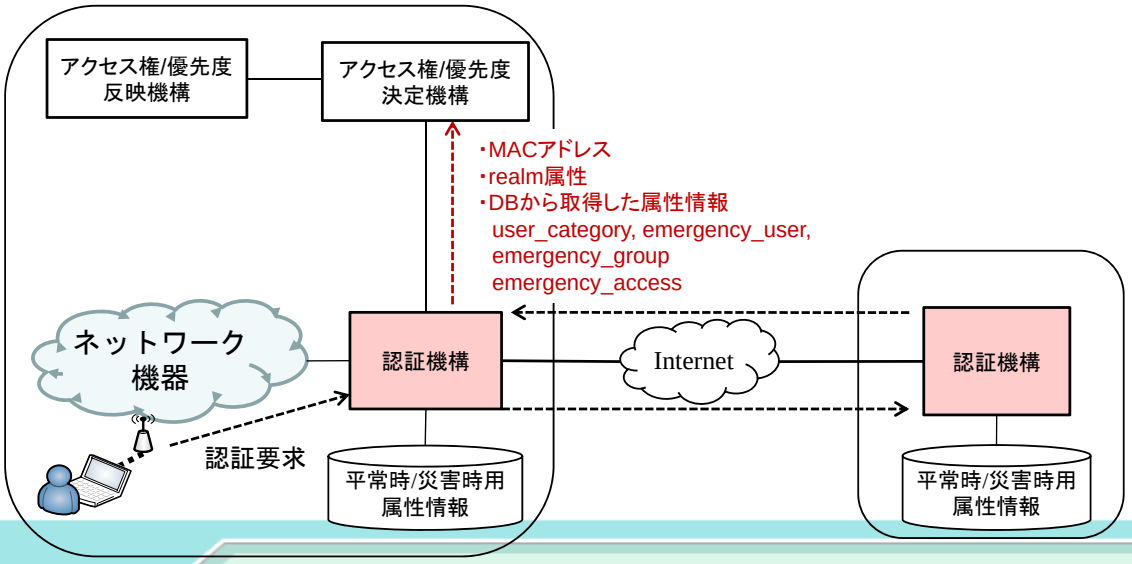
利用モード	属性名	属性内情報	情報の意味	具体例
平常時用([1])	user-category	role	ユーザの役職・権限	privileged
	realm		ユーザの所属	tohoku.ac.jp
災害時用	emergency	emergency_user	要緊急性ユーザを表す	TRUE / FALSE
		emergency_group	緊急性を有する根拠	Medical service
		emergency_access	優先アクセスしたい宛先	X.X.X.X



[1] T. Watanabe, et al. ``Flexible Access Control Framework Considering IdP-side's Authorization Policy in Roaming Environment," Int'l Workshop on MidArch'12, pp. 76-81 (July 2012).

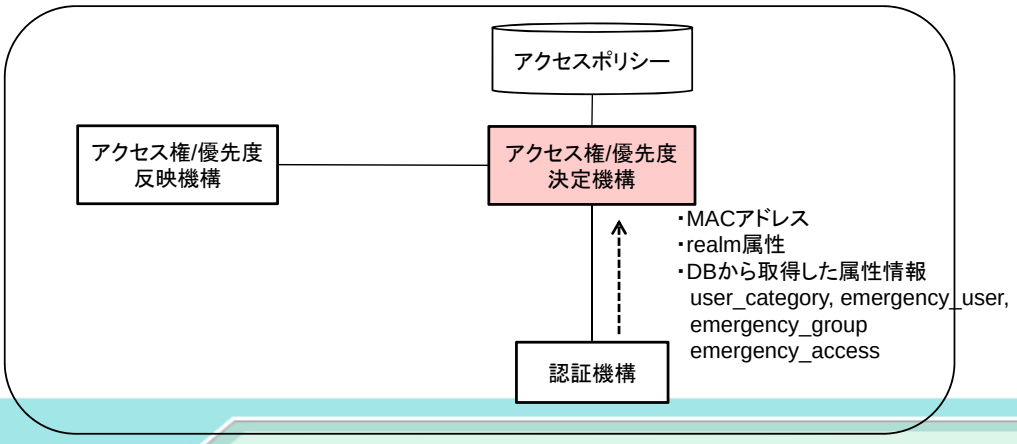
認証機構(3/3)

- 3)認証時に得られた情報をアクセス権/優先度決定機構に通知
  - 認証を行ったユーザ端末のMACアドレス
  - realm属性
  - IdPから取得した属性情報



アクセス権/優先度決定機構(1/3)

- ユーザのアクセス権および優先度を決定する.
  - 1)避難所側のアクセスポリシーを設定
  - 2)受信した属性情報をもとにそのユーザに割り当てるグループID(GID)を決定
    - グループID:同じ権限をもつユーザや，同じアクセスポリシーで管理されているサーバ群に割り当てるID

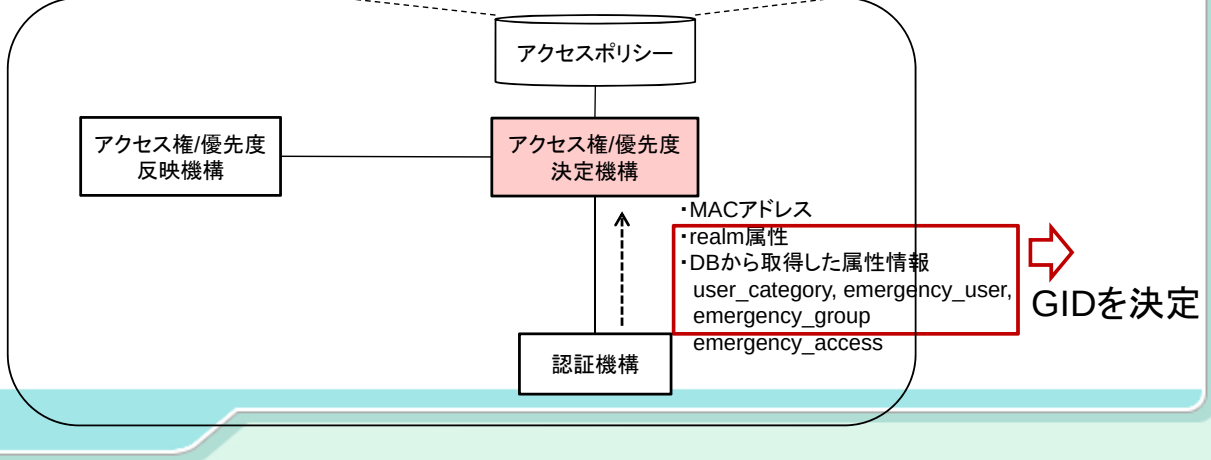


アクセス権/優先度決定機構(2/3)

- ユーザのアクセス権および優先度を決定する.

避難所側のアクセスポリシー例:

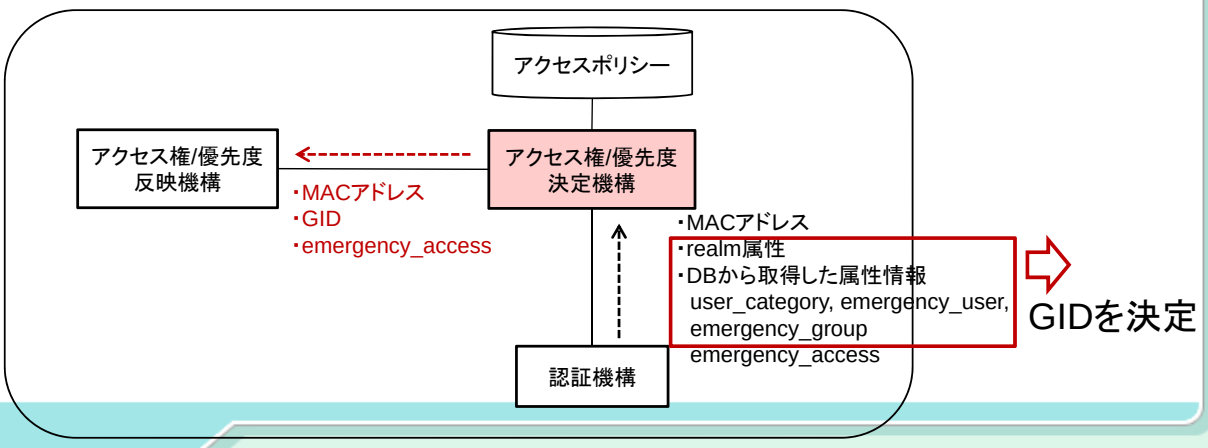
role	realm	emergency_user	emergency_group		GID
*	*	TRUE	*	⇒	101
privileged	tohoku.ac.jp	FALSE	NULL	⇒	102



アクセス権/優先度決定機構(3/3)

- 決定した情報をアクセス権/優先度反映機構に通知
  - 3)アクセス権情報として以下の情報をアクセス権/優先度反映機構に通知
    - 割り当てられたGID，ユーザ端末のMACアドレス，emergency_access情報

（IdPから送られてきた場合のみ）



アクセス権/優先度反映機構(1/2)

- 通知されたアクセス権をもとにパケットの処理方法を決定する.
  - 1)基本的な情報をあらかじめ登録
    - 各種ネットワークリソースに割り当てるGID
    - 通信可能なGIDの組

GID情報

id	MAC	IP	GID
1	-	Y.Y.Y.Y/24	201

通信可能グループ情報

id	GID	GID	priority
1	101	201	1
2	102	201	0

アクセス権/優先度決定機構で定義されている，ユーザに割り当てるGID等

アクセス権/優先度反映機構(2/2)

- 通知されたアクセス権をもとにパケットの処理方法を決定する.
  - 2)アクセス権/優先度決定機構から受信した情報を登録
    - 受信したMACアドレスとGIDを対応付け
    - emergency_access属性がある場合は，そのリソースへの優先処理設定を行う.

例：GID=102, MAC=12:34:56:78:9A:BC,emergency_access=X.X.X.X が通知された場合

GID情報

id	MAC	IP	GID
1	-	Y.Y.Y.Y/24	201
2	12:34:56:78:9A:BC	-	102
3	12:34:56:78:9A:BC	-	1001
4	-	X.X.X.X	1002

通信可能グループ情報

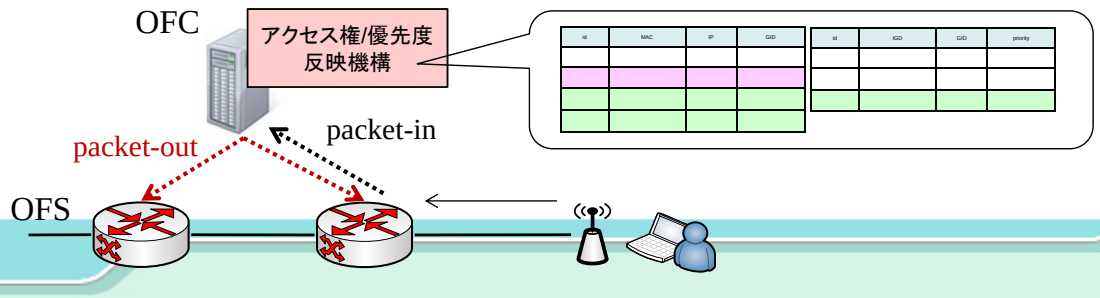
id	GID	GID	priority
1	101	201	1
2	102	201	0
3	1001	1002	1

OpenFlowを利用したアクセス制御の流れ

- OFSがユーザからのパケットを受信時(packet-in発生時)
  - 1)パケットヘッダ内の情報を基に該当するGIDを取得
  - 2-1)取得したGIDの組が登録されている場合
    - priority設定有り：ヘッダを変更してパケット転送フローエントリーを打つ

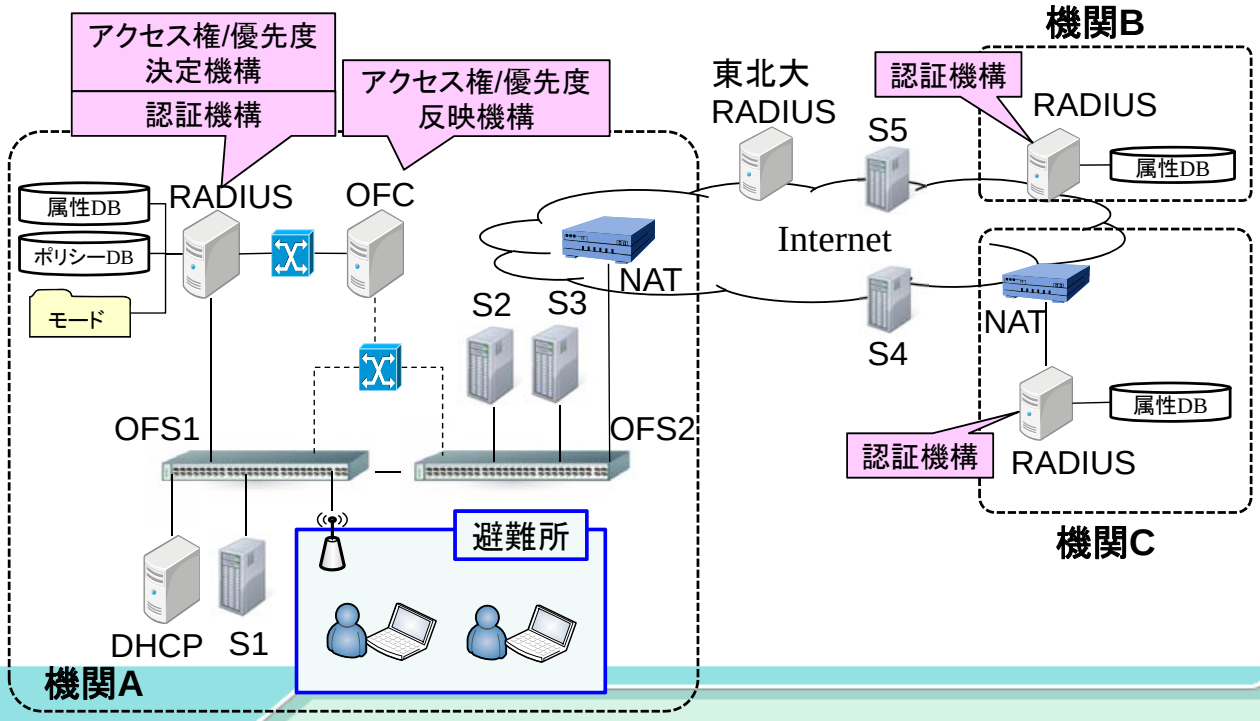
ToS(Type of Service)フィールド	IP Precedence値	5
VLAN tagフィールド	PCP(Priority Code Point値)	7

    - priority設定無し：パケット転送のフローエントリーを打つ
  - 2-2) 取得したGID同士の組が登録されていない場合
    - パケット廃棄のフローエントリーを打つ



実験ネットワーク構成

- ユーザは機関Aの避難所からネットワークにアクセス



評価環境(1/2)

- 4ユーザ，5種類のサーバを想定

user1	公共機関ユーザ
user2	平常時ユーザ(特権有り)
user3	平常時ユーザ(特権無し)
user4	避難者等一般ユーザ

S1	機関Aの業務用等ローカルサーバ
S2	機関Aのその他のサーバ
S3	災害時に不適切なサーバ
S4	優先的にアクセスできる災害関係サーバ
S5	その他一般的なインターネット上のサーバ

- 各機関の認証機構で付与する属性情報

機関A	user4	
機関B	user1	emergency_user={true}
機関C	user2	role={privileged}, emergency_access={S2}
	user3	role={unprivileged}, emergency_acdess={S2}

評価環境(2/2)

- 評価項目
  - アクセス可否
    - Pingに対する応答の有無で確認
  - 優先度制御
    - パケットヘッダのToSフィールドのIP Precedence値およびVLAN tagフィールド内PCP値がOFSで書き換えられていることで確認

評価結果

- 平常時および災害時のアクセス制御の結果

ユーザ	認証機関		平常時 S1	平常時 S2	平常時 S3	平常時 S4	平常時 S5	災害時 S1	災害時 S2	災害時 S3	災害時 S4	災害時 S5
公共機関ユーザ	機関B	アクセス	×	×	×	×	×	×	○	○	○	○
		優先	–	–	–	–	–	–	○	○	○	○
平常時ユーザ1 (privileged)	機関C	アクセス	○	○	○	○	○	○	○	×	○	○
		優先	×	×	×	×	×	×	○	–	○	×
平常時ユーザ2 (unprivileged)	機関C	アクセス	○	○	○	○	○	○	○	×	○	○
		優先	×	×	×	×	×	×	×	–	○	×
一般ユーザ	機関A	アクセス	×	×	×	×	×	×	○	×	○	○
		優先	–	–	–	–	–	×	×	–	○	×

[平常時のポリシー]
・公共機関ユーザ，一般ユーザはアクセス不可
・優先処理はしない

[災害時のポリシー]
・公共機関ユーザ，一般ユーザもアクセス可
・公共機関ユーザの全通信，全ユーザの災害関係サイトへのアクセスは優先処理
・不適切サイトは公共機関ユーザ以外アクセス不可

アクセス権/優先度反映機構での出力(1/2)

- アクセス禁止(GID未登録)

```
[REFLECT_ACCS]modify_flow_entry: dpid(0x000100255c6b68b9)
[REFLECT_ACCS]Packet-In received ( datapath_id = 0x100, transaction_id = 0xdc8f0, buffer_id =
0xffffffff, total_len = 74, in_port = 15, reason = 0, data_len = 74 ).
[REFLECT_ACCS]match=[wildcards = 0(none), in_port = 15, dl_src = 18:3d:a2:82:a1:70, dl_dst = 6
8:b5:99:cc:1f:6a, dl_vlan = 0xffff, dl_vlan_pcp = 0, dl_type = 0x800, nw_tos = 0, nw_proto = 1
, nw_src = 172.24.1.198/32, nw_dst = 172.24.1.40/32, tp_src = 8, tp_dst = 0]
[REFLECT_ACCS]get_sgid: GID(424)
[REFLECT_ACCS]get_sgid: GID(428)
[REFLECT_ACCS]get_sgid: GID(10000)
[REFLECT_ACCS]get_dgid: GID(207)
[REFLECT_ACCS]get_dgid: GID(10001)
[REFLECT_ACCS]handle_packet_in: judge access NG
[REFLECT_ACCS]Discarding packets for a certain period ( datapath_id = 0x100, match = [wildcard
s = 0(none), in_port = 15, dl_src = 18:3d:a2:82:a1:70, dl_dst = 68:b5:99:cc:1f:6a, dl_vlan = 0
xffff, dl_vlan_pcp = 0, dl_type = 0x800, nw_tos = 0, nw_proto = 1, nw_src = 172.24.1.198/32, n
w_dst = 172.24.1.40/32, tp_src = 8, tp_dst = 0], duration = 5 [sec] ).
[REFLECT_ACCS]Packet-In received ( datapath_id = 0x100, transaction_id = 0xdc8f3, buffer_id =
0xffffffff, total_len = 74, in_port = 15, reason = 0, data_len = 74 ).
[REFLECT_ACCS]match=[wildcards = 0(none), in_port = 15, dl_src = 18:3d:a2:82:a1:70, dl_dst = 6
8:b5:99:cc:0f:ac, dl_vlan = 0xffff, dl_vlan_pcp = 0, dl_type = 0x800, nw_tos = 0, nw_proto = 1
, nw_src = 172.24.1.198/32, nw_dst = 172.24.1.40/32, tp_src = 8, tp_dst = 0]
```


アクセス権/優先度反映機構での出力(2/2)

- アクセス許可(GID登録)，優先度設定あり

```
[REFLECT_ACCS]modify_flow_entry: dpid(0x000100255c6b68b9)
[REFLECT_ACCS]Packet-In received ( datapath_id = 0x100, transaction_id = 0xd99f9, buffer_id = 0xffffffff, total_len = 74, in_port = 1
5, reason = 0, data_len = 74 ).
[REFLECT_ACCS]match=[wildcards = 0(none), in_port = 15, dl_src = 18:3d:a2:82:a1:70, dl_dst = 54:52:00:7f:95:ca, dl_vlan = 0xffff, dl_
vlan_pcp = 0, dl_type = 0x800, nw_tos = 0, nw_proto = 1, nw_src = 172.24.1.198/32, nw_dst = 172.24.1.43/32, tp_src = 8, tp_dst = 0]
[REFLECT_ACCS]get_sgid: GID(424)
[REFLECT_ACCS]get_sgid: GID(428)
[REFLECT_ACCS]get_sgid: GID(10000)
[REFLECT_ACCS]get_dgid: GID(202)
[REFLECT_ACCS]get_dgid: GID(302)
[REFLECT_ACCS]get_dgid: GID(10002)
[REFLECT_ACCS]handle_packet_in: judge access OK(priority=1)
[REFLECT_ACCS]make_path: Access OK and priority flow
[REFLECT_ACCS]modify_flow_entry_priority: pathtype(MOST_LOWER), dpid(0x000100255c6b68b9)
[REFLECT_ACCS]modify_flow_entry_priority: pathtype(MOST_UPPER), dpid(0x0000000000000100)
[REFLECT_ACCS]Packet-In received ( datapath_id = 0x100255c6b68b9, transaction_id = 0x8651b, buffer_id = 0xffffffff, total_len = 74, i
n_port = 14, reason = 0, data_len = 74 ).
[REFLECT_ACCS]match=[wildcards = 0(none), in_port = 14, dl_src = 54:52:00:7f:95:ca, dl_dst = 18:3d:a2:82:a1:70, dl_vlan = 0xffff, dl_
vlan_pcp = 0, dl_type = 0x800, nw_tos = 0, nw_proto = 1, nw_src = 172.24.1.43/32, nw_dst = 172.24.1.198/32, tp_src = 0, tp_dst = 0]
[REFLECT_ACCS]get_sgid: GID(202)
[REFLECT_ACCS]get_sgid: GID(302)
[REFLECT_ACCS]get_sgid: GID(10002)
[REFLECT_ACCS]get_dgid: GID(424)
[REFLECT_ACCS]get_dgid: GID(428)
[REFLECT_ACCS]get_dgid: GID(10000)
[REFLECT_ACCS]handle_packet_in: judge access OK(priority=1)
[REFLECT_ACCS]make_path: Access OK and priority flow
[REFLECT_ACCS]modify_flow_entry_priority: pathtype(MOST_LOWER), dpid(0x0000000000000100)
[REFLECT_ACCS]modify_flow_entry_priority: pathtype(MOST_UPPER), dpid(0x000100255c6b68b9)
[REFLECT_ACCS]Packet-In received ( datapath_id = 0x100255c6b68b9, transaction_id = 0x8651d, buffer_id = 0xffffffff, total_len = 74, i
n_port = 14, reason = 0, data_len = 74 ).
[REFLECT_ACCS]match=[wildcards = 0(none), in_port = 14, dl_src = 54:52:00:7f:95:ca, dl_dst = 18:3d:a2:82:a1:70, dl_vlan = 0xffff, dl_
vlan_pcp = 0, dl_type = 0x800, nw_tos = 160, nw_proto = 1, nw_src = 172.24.1.43/32, nw_dst = 172.24.1.198/32, tp_src = 0, tp_dst = 0]
```

OFS上での統計情報

- パケットヘッダの書き換え

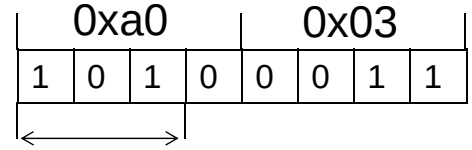
```
<entry 5901>
 table type                 : normal1
 forwarding state           : software-based
 matched octets             :                 574 octets
 matched packets            :                   7 packets
 green and yellow octets    :                 602 octets
 green and yellow packets   :                   7 packets
 red octets                 :                   0 octet
 red packets                :                   0 packet
 idle timer(max/current)    :      602 sec /   513 sec
 hard timer(max/current)    :        0 sec /     0 sec
 priority                   : exact (65535)
 added command              : flowmod
 added time                 : 2013/02/15 01:50:09 JST
 last modified time         : -
 flow cookie                : 0x4

 match
  match type          : STANDARD#
  input port          : 0/22[0x00000016]
  src mac address     : 183d.a282.a170
  dst mac address     : 5452.007f.95ca
  input vlan          : 4094
  input vlan pcp      : 7
  ethernet type       : 0x0800[IPv4]
  tos (dscp, ecn)     : 0xa0/0x03 (0x28, any)
  ip protocol         : 1[ICMP]
  src ip address      : 172.24.1.198
  dst ip address      : 172.24.1.43
  ipv6 flow label     : any
  icmp type           : 8(0x08)
  icmp code           : 0(0x00)
  metadata            : 0x0000000000000000

 action 1
  type                : STRIP_VLAN

 action 2
  type                : OUTPUT
  out port            : 0/14[0x0000000e]
```

優先フローは
　ToSフィールド内IP Precedense値が5
　VLAN tagフィールド内PCP値が7
に書き換えられている.



IP Precedence
3bit

まとめ

- 災害時における802.1X認証をベースとしたネットワークリソース割り当て制御システム
  - 認証時の属性情報を利用し，ユーザやフローに応じた柔軟なアクセス制御の実現
  - OpenFlowを利用し，迅速かつ容易にアクセスポリシーを切り替え・反映

[今後の課題]

- 実現する優先度制御の検討
  - 現状はパケットヘッダの書き換えによる優先度制御

⇩

  - 災害時において，ユーザ間の公平性や帯域保証などのより詳細なQoS制御の必要性および実現方法の検討

謝辞

- 本研究の一部は，総務省の委託研究「大規模災害時に被災地の通信能力を緊急増強する技術の研究開発（災害時避難所等における局所的同報配信技術の研究開発）」プロジェクトで実施された.