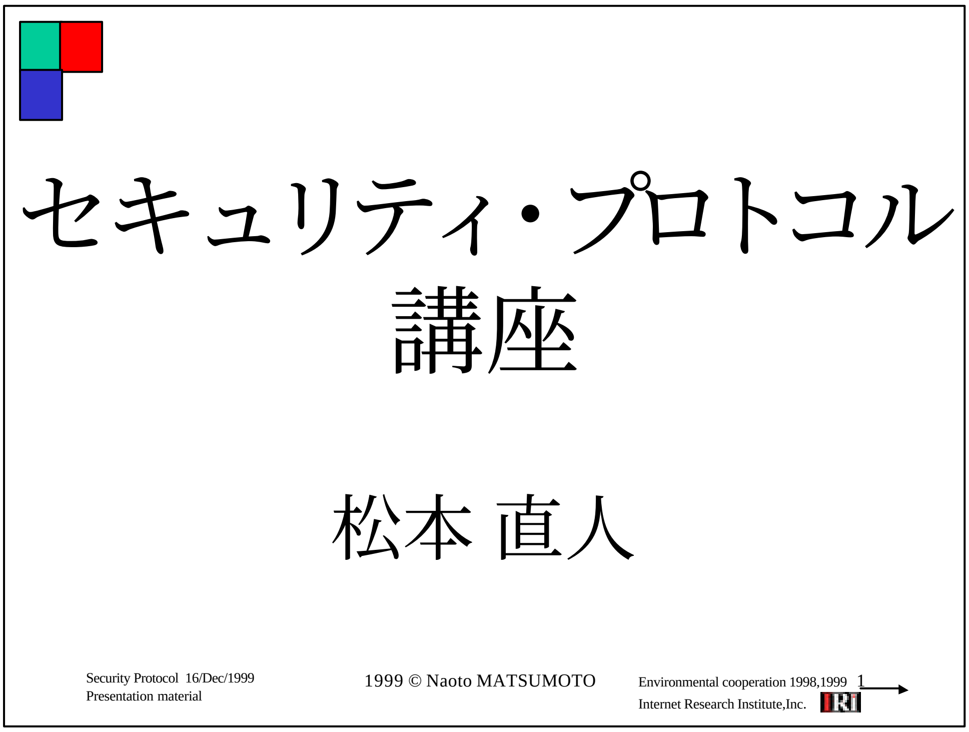
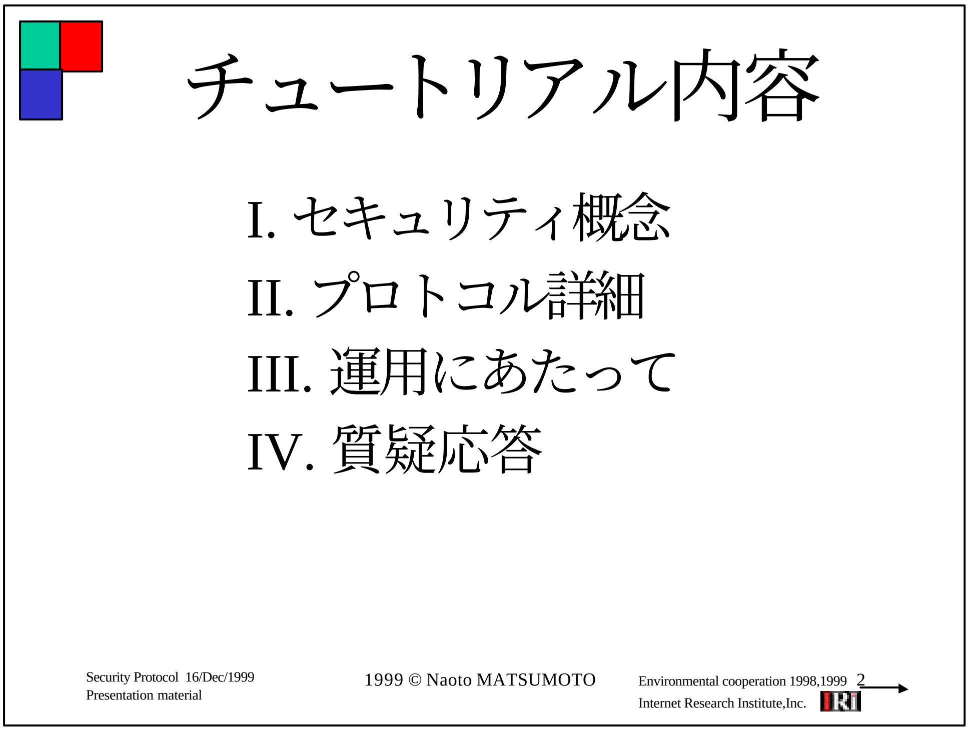


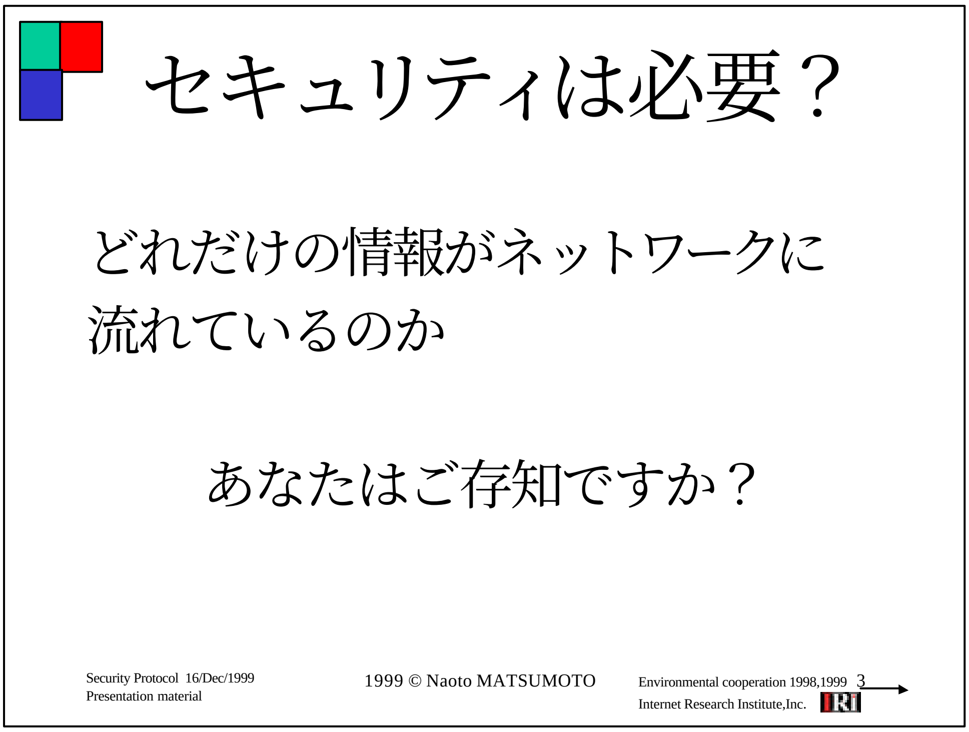
セキュリティ・プロトコル講座

松本 直人



チュートリアル内容

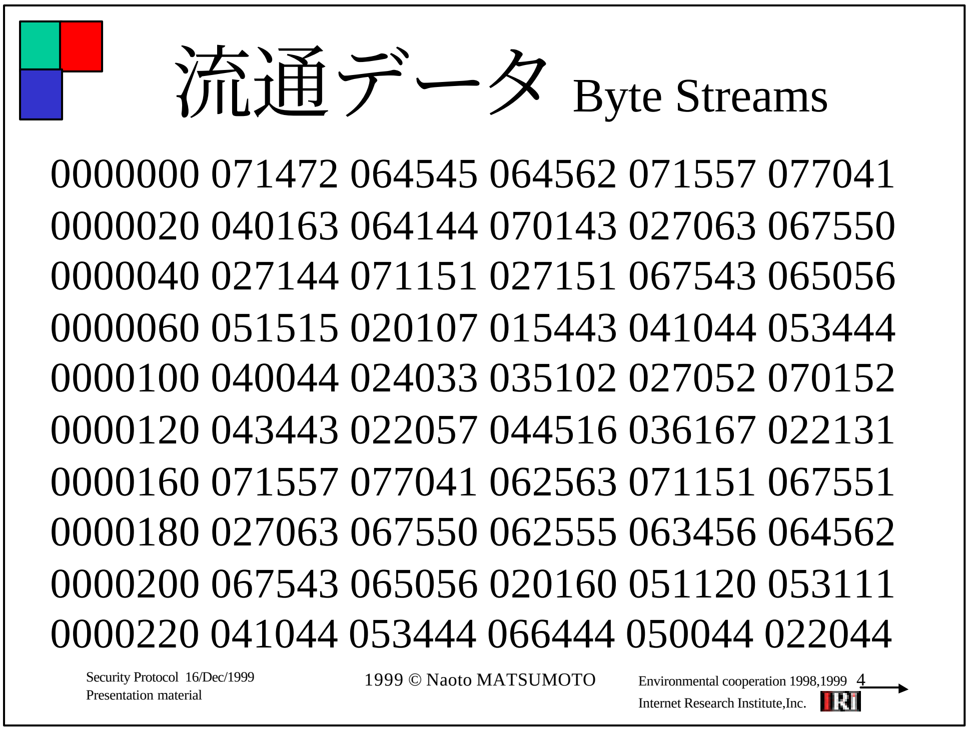
I. セキュリティ概念
II. プロトコル詳細
III. 運用にあたって
IV. 質疑応答



セキュリティは必要？

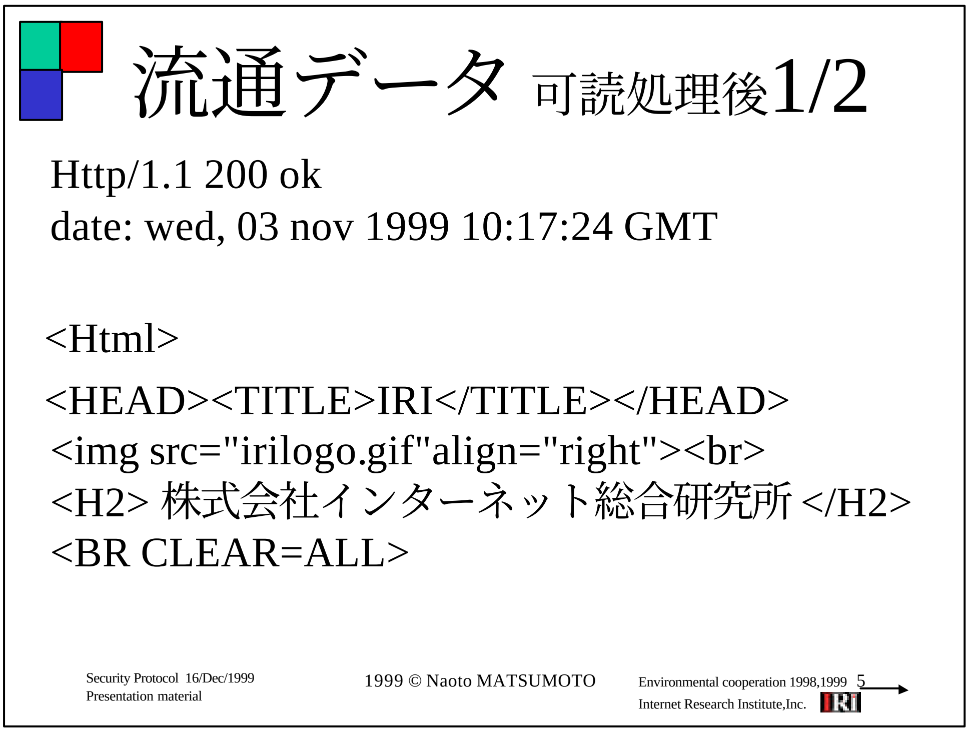
どれだけの情報がネットワークに
流れているのか

あなたはご存知ですか？



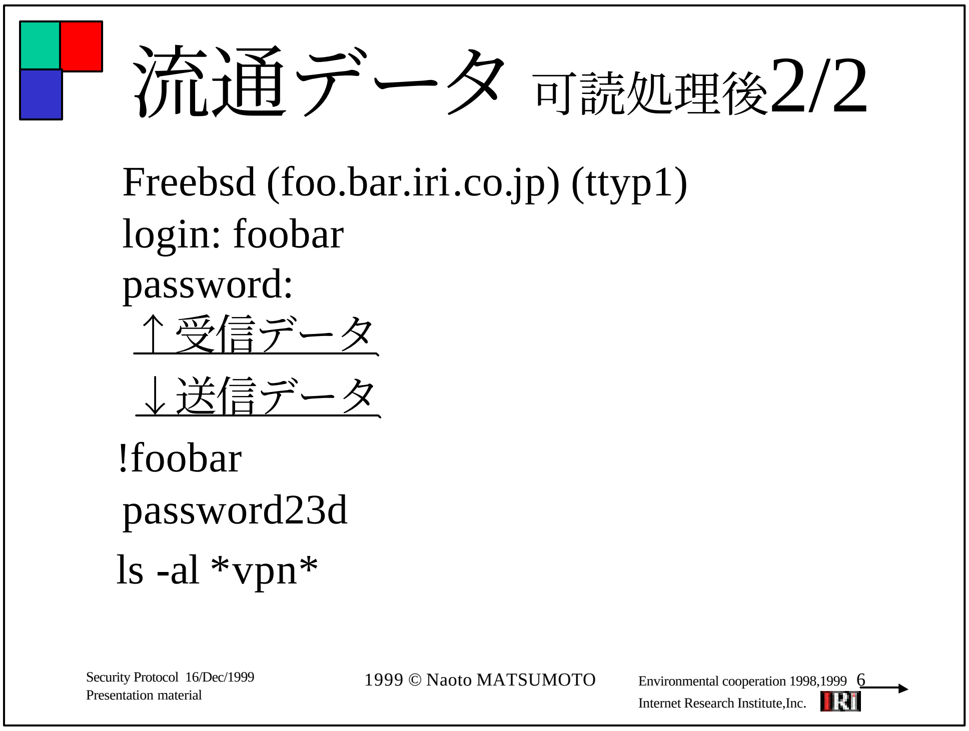
流通データ Byte Streams

```
0000000 071472 064545 064562 071557 077041
0000020 040163 064144 070143 027063 067550
0000040 027144 071151 027151 067543 065056
0000060 051515 020107 015443 041044 053444
0000100 040044 024033 035102 027052 070152
0000120 043443 022057 044516 036167 022131
0000160 071557 077041 062563 071151 067551
0000180 027063 067550 062555 063456 064562
0000200 067543 065056 020160 051120 053111
0000220 041044 053444 066444 050044 022044
```



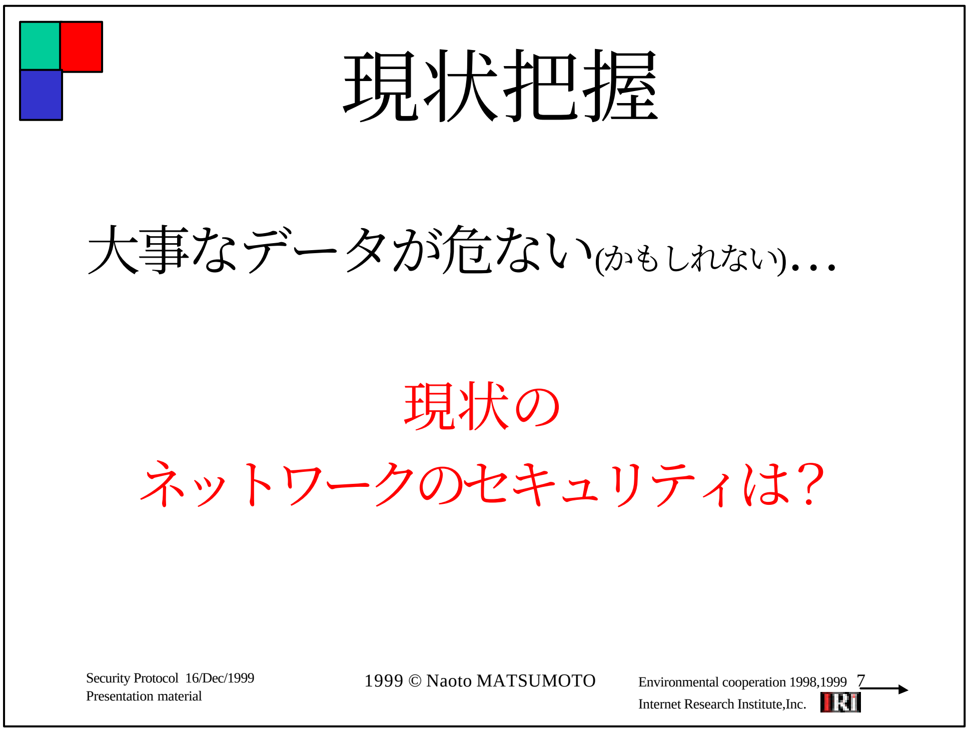
流通データ 可読処理後1/2

```
Http/1.1 200 ok
date: wed, 03 nov 1999 10:17:24 GMT

<Html>
<HEAD><TITLE>IRI</TITLE></HEAD>
<img src="irilogo.gif"align="right"><br>
<H2> 株式会社インターネット総合研究所 </H2>
<BR CLEAR=ALL>
```



流通データ 可読処理後2/2

```
Freebsd (foo.bar.iri.co.jp) (ttyp1)
login: foobar
password:
 ↑受信データ
 ↓送信データ
!foobar
password23d
ls -al *vpn*
```



現状把握

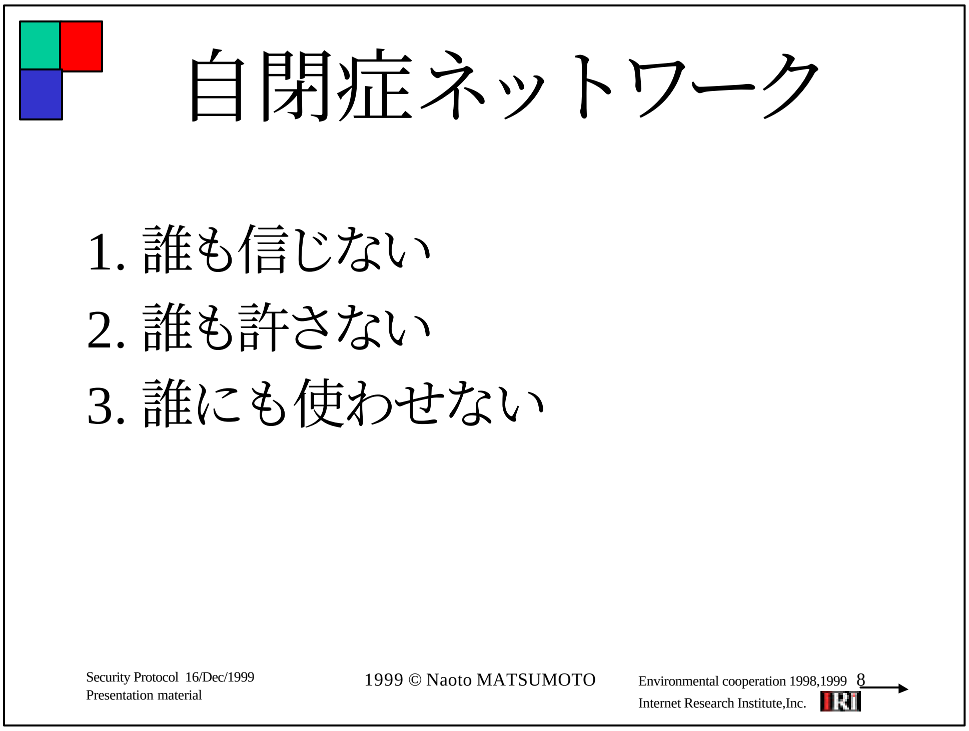
大事なデータが危ない(かもしれない)…

現状の
ネットワークのセキュリティは？

Security Protocol 16/Dec/1999
Presentation material

1999 © Naoto MATSUMOTO

Environmental cooperation 1998,1999 7
Internet Research Institute,Inc.



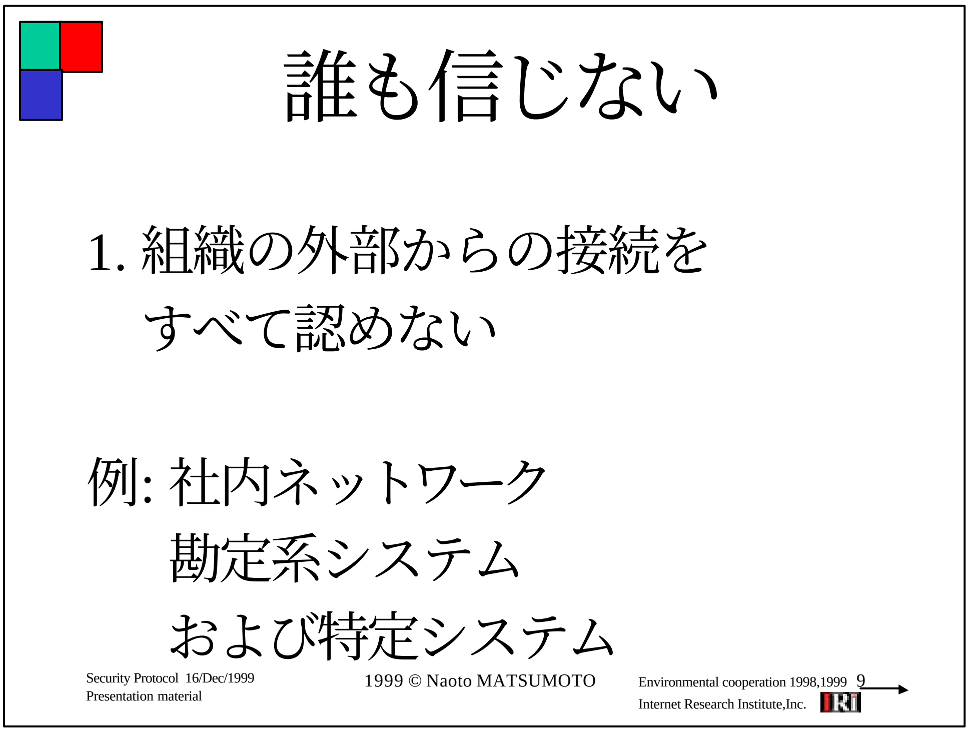
自閉症ネットワーク

1. 誰も信じない
2. 誰も許さない
3. 誰にも使わせない

Security Protocol 16/Dec/1999
Presentation material

1999 © Naoto MATSUMOTO

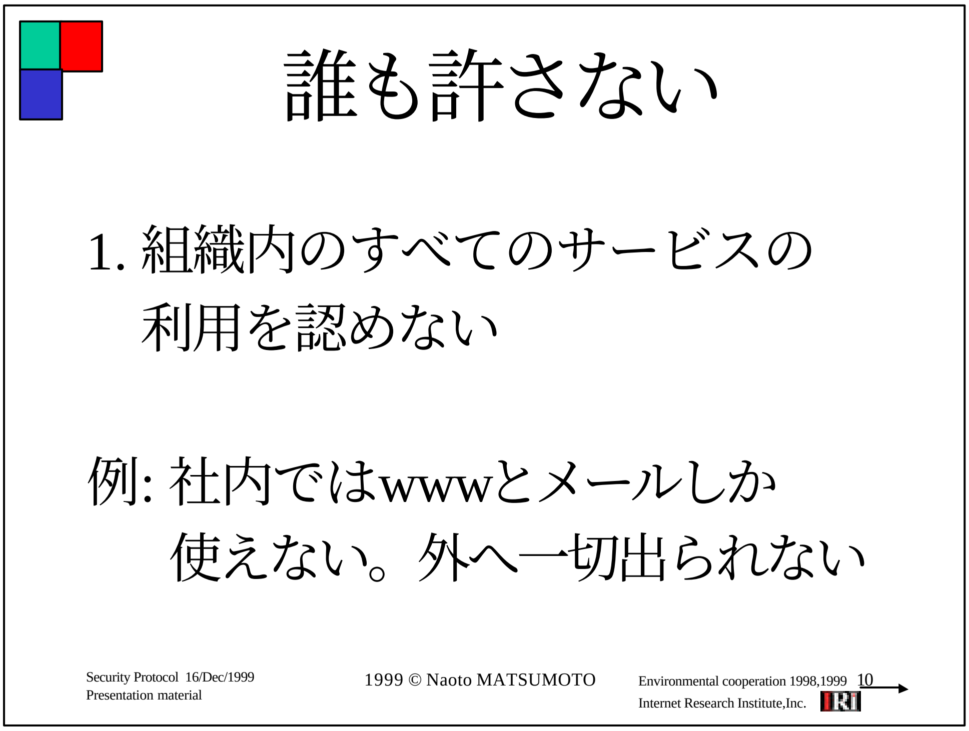
Environmental cooperation 1998,1999 8
Internet Research Institute,Inc.



誰も信じない

1. 組織の外部からの接続を
   すべて認めない

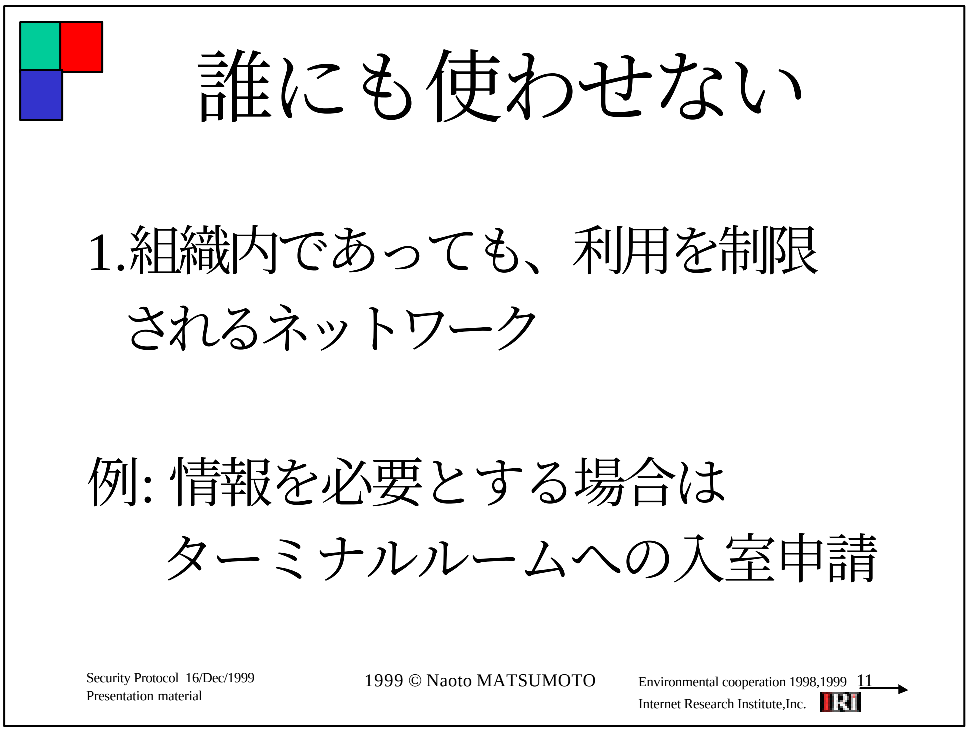
例: 社内ネットワーク
　勘定系システム
　および特定システム



誰も許さない

1. 組織内のすべてのサービスの
   利用を認めない

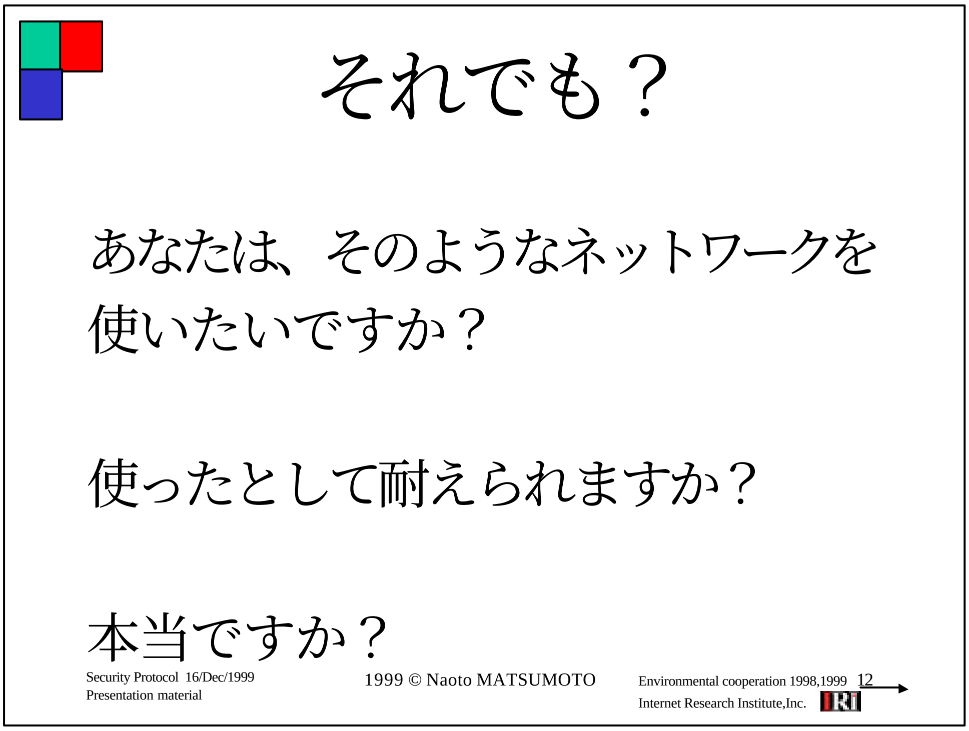
例: 社内ではwwwとメールしか
　使えない。外へ一切出られない



誰にも使わせない

1.組織内であっても、利用を制限
　されるネットワーク

例: 情報を必要とする場合は
　　ターミナルルームへの入室申請

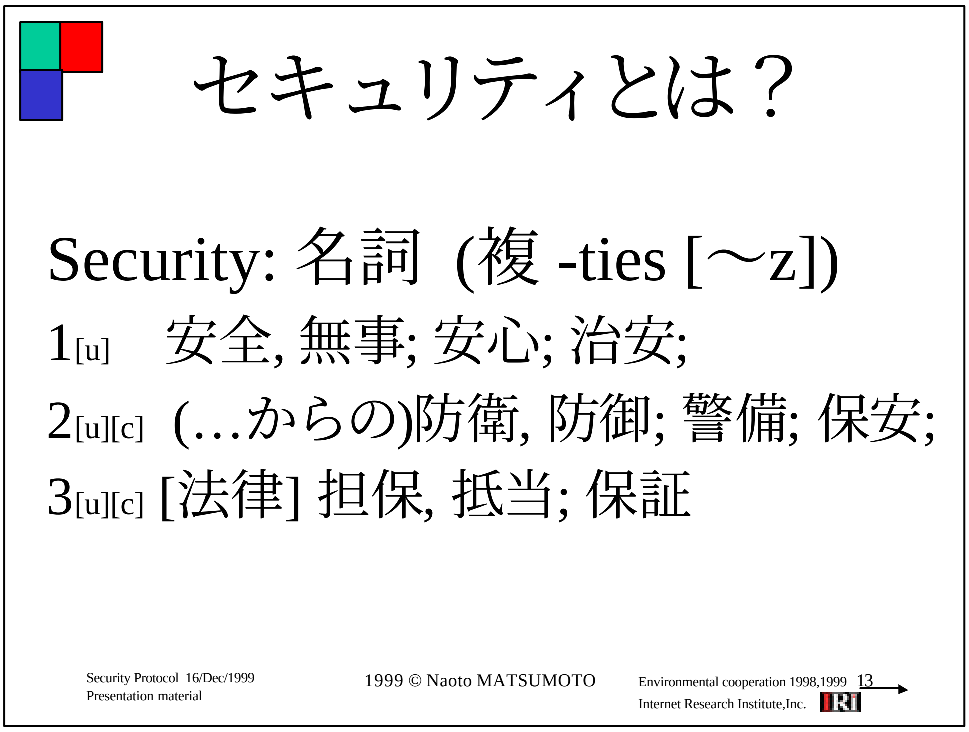


それでも？

あなたは、そのようなネットワークを
使いたいですか？

使ったとして耐えられますか？

本当ですか？



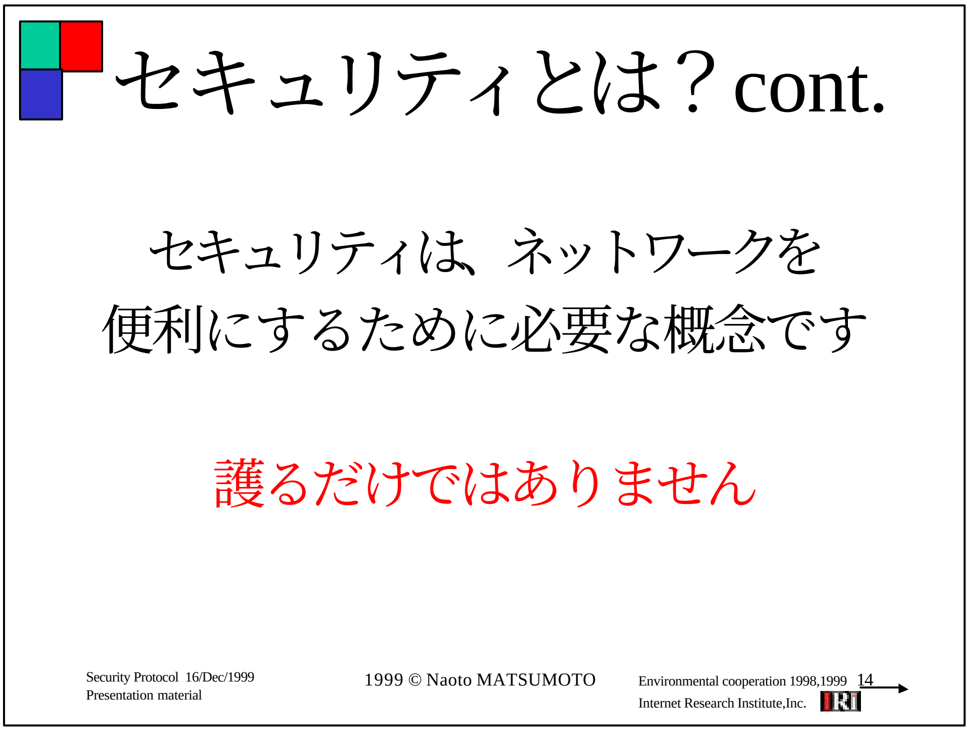
セキュリティとは？

Security: 名詞 (複 -ties [～z])

1[u]　安全, 無事; 安心; 治安;

2[u][c] (…からの)防衛, 防御; 警備; 保安;

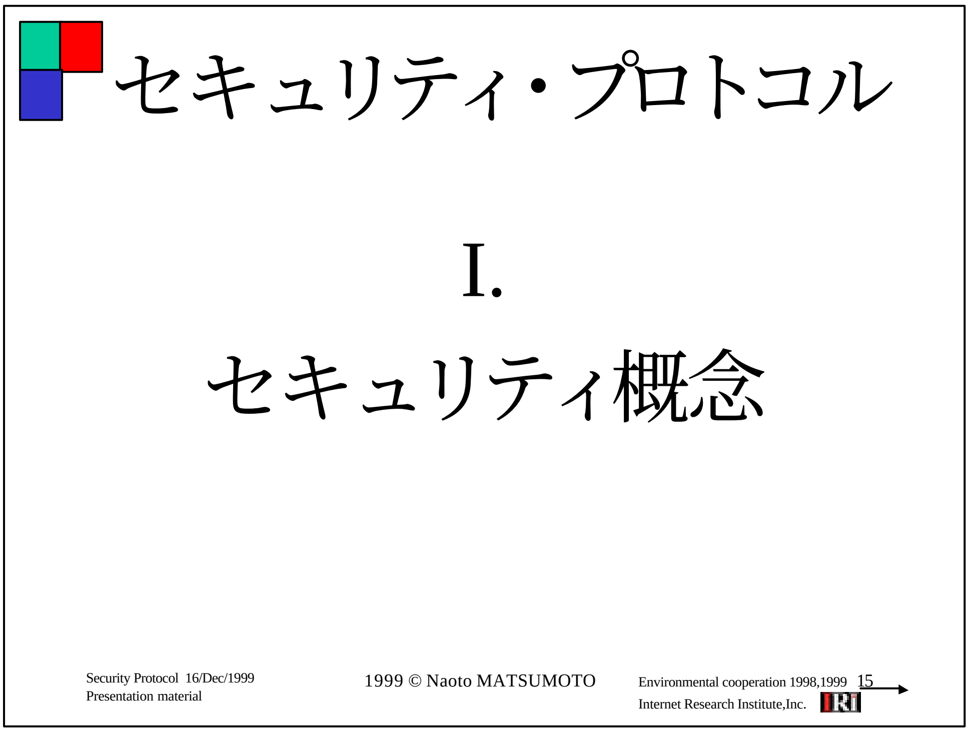
3[u][c] [法律] 担保, 抵当; 保証



セキュリティとは？cont.

セキュリティは、ネットワークを
便利にするために必要な概念です

護るだけではありません



セキュリティ・プロトコル

I.

セキュリティ概念

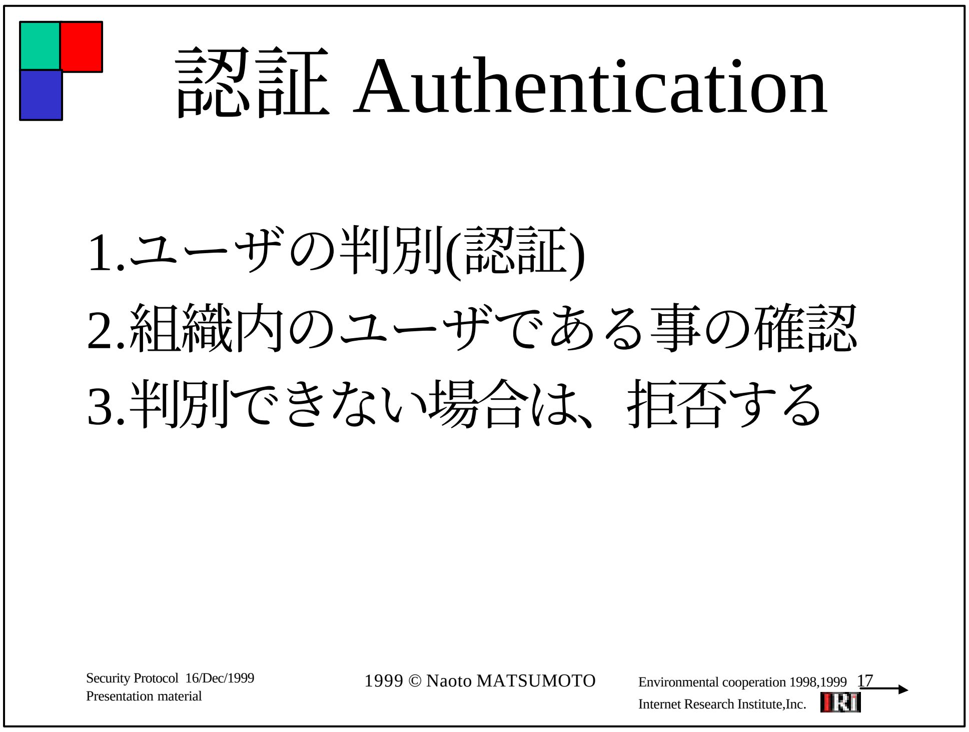
セキュリティ・プロトコル

基本的な分類は

認証 Authentication

制御 Authorization (Control)

防御 Defense

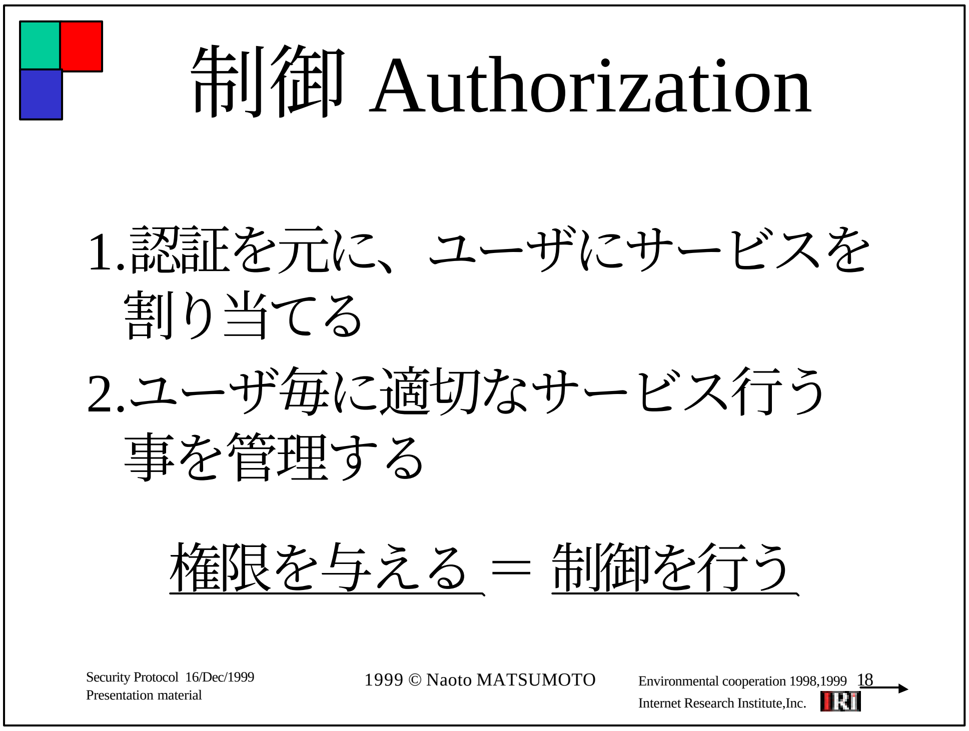


認証 Authentication

1.ユーザの判別(認証)

2.組織内のユーザである事の確認

3.判別できない場合は、拒否する



制御 Authorization

1.認証を元に、ユーザにサービスを割り当てる

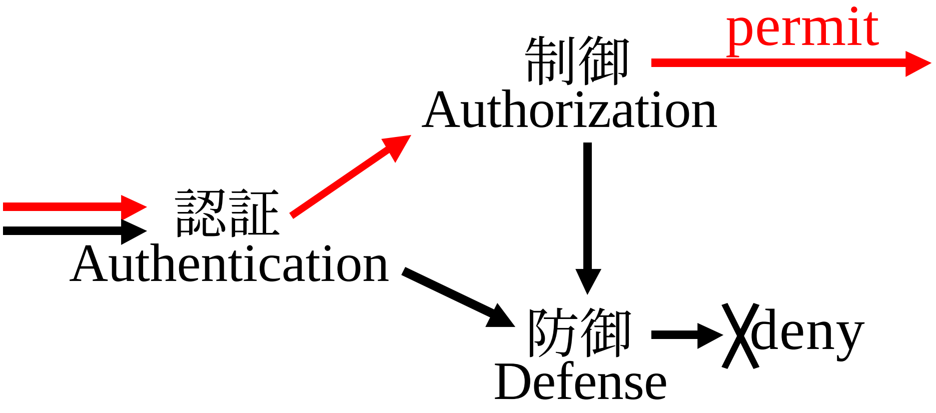
2.ユーザ毎に適切なサービス行う事を管理する

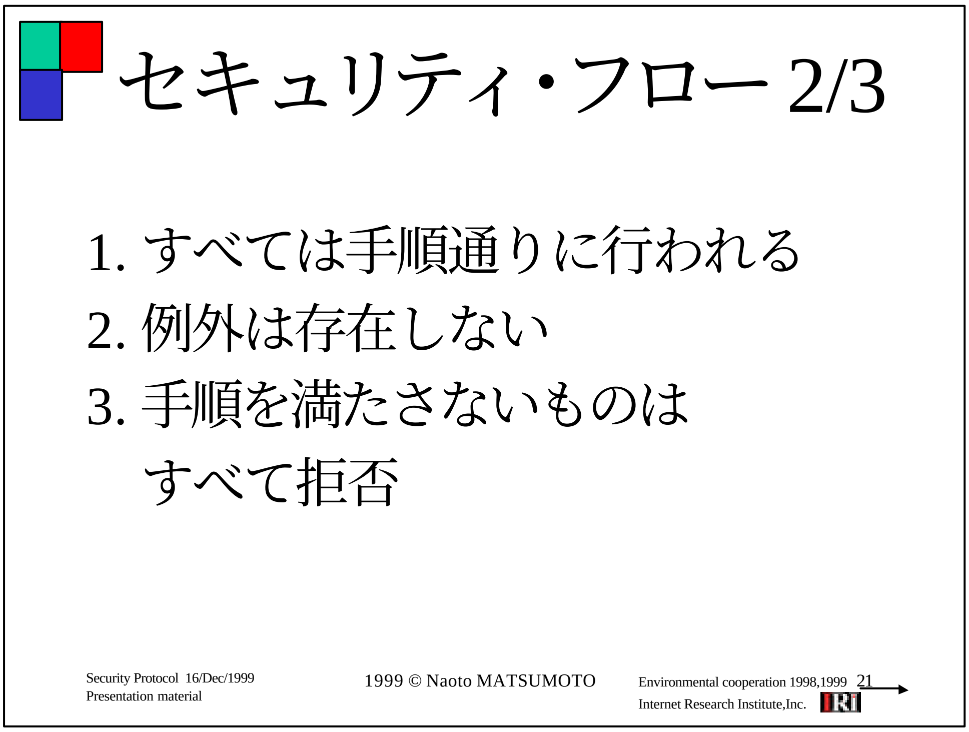
権限を与える ＝ 制御を行う

防御 Defense

1.すべてにおいて判断できない
　外敵(想定)から自らを防御する

セキュリティ・フロー 1/3





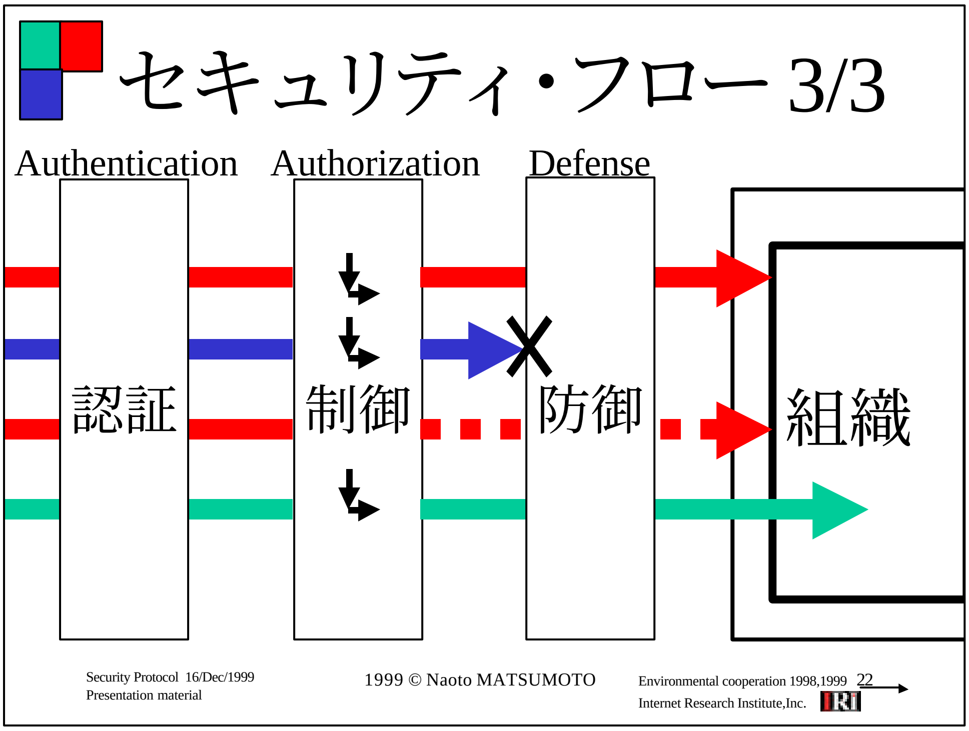
セキュリティ・フロー 2/3

1. すべては手順通りに行われる
2. 例外は存在しない
3. 手順を満たさないものは
   すべて拒否

Security Protocol 16/Dec/1999
Presentation material

1999 © Naoto MATSUMOTO

Environmental cooperation 1998,1999 21
Internet Research Institute,Inc.



セキュリティ・フロー 3/3

Authentication Authorization Defense

認証

制御

防御

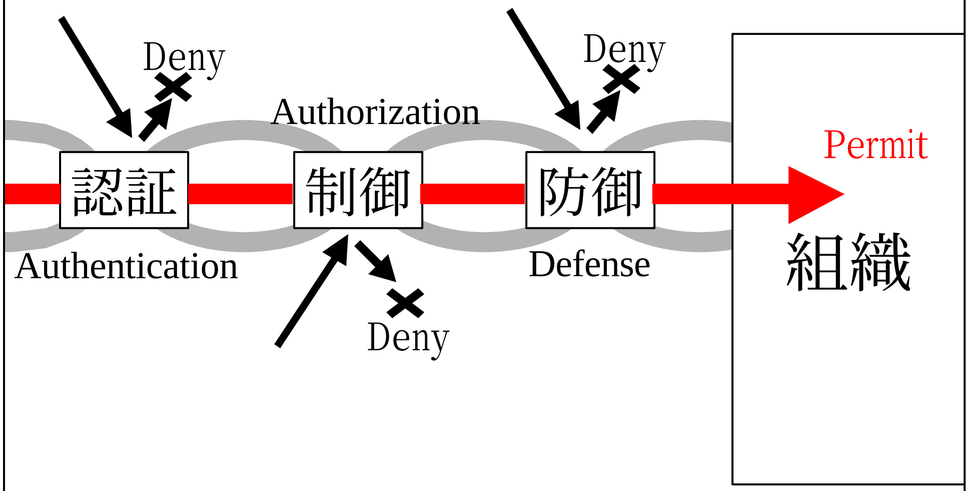
組織

Security Protocol 16/Dec/1999
Presentation material

1999 © Naoto MATSUMOTO

Environmental cooperation 1998,1999 22
Internet Research Institute,Inc.

セキュア・チェーン

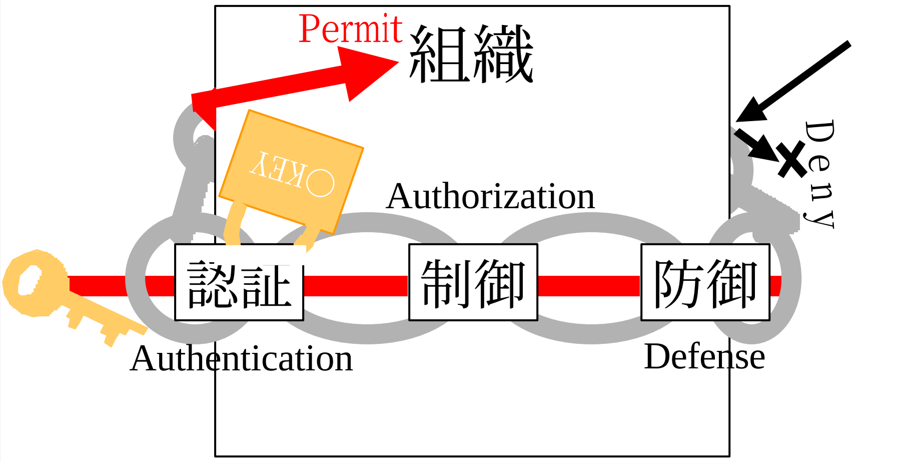


Security Protocol 16/Dec/1999
Presentation material

1999 © Naoto MATSUMOTO

Environmental cooperation 1998,1999 23
Internet Research Institute,Inc.

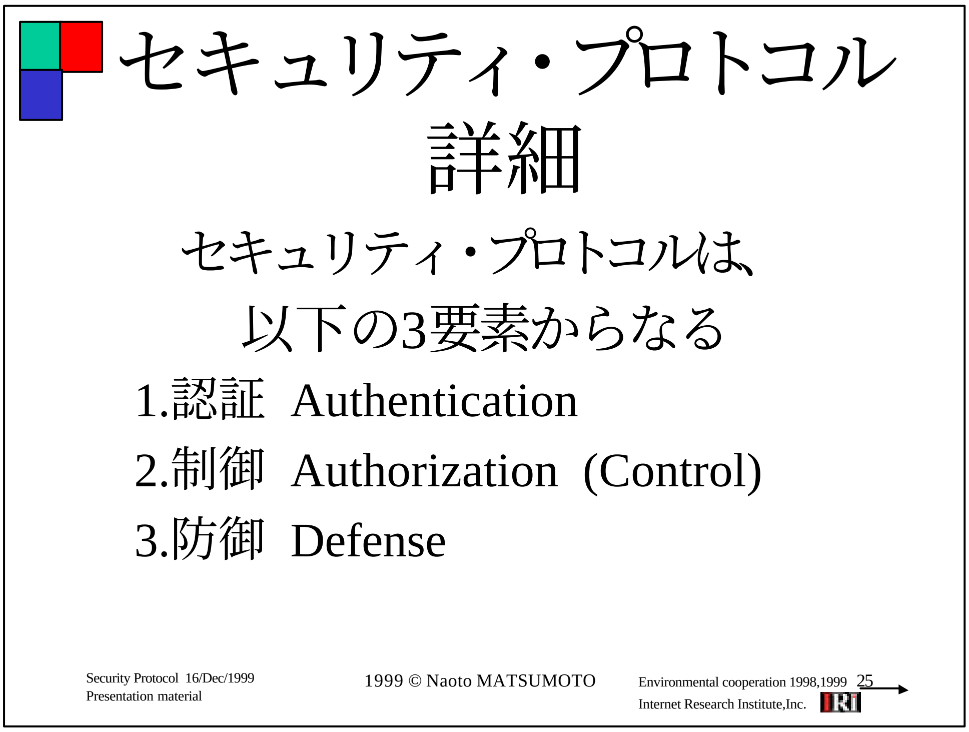
セキュア・チェーン ...cont



Security Protocol 16/Dec/1999
Presentation material

1999 © Naoto MATSUMOTO

Environmental cooperation 1998,1999 24
Internet Research Institute,Inc.



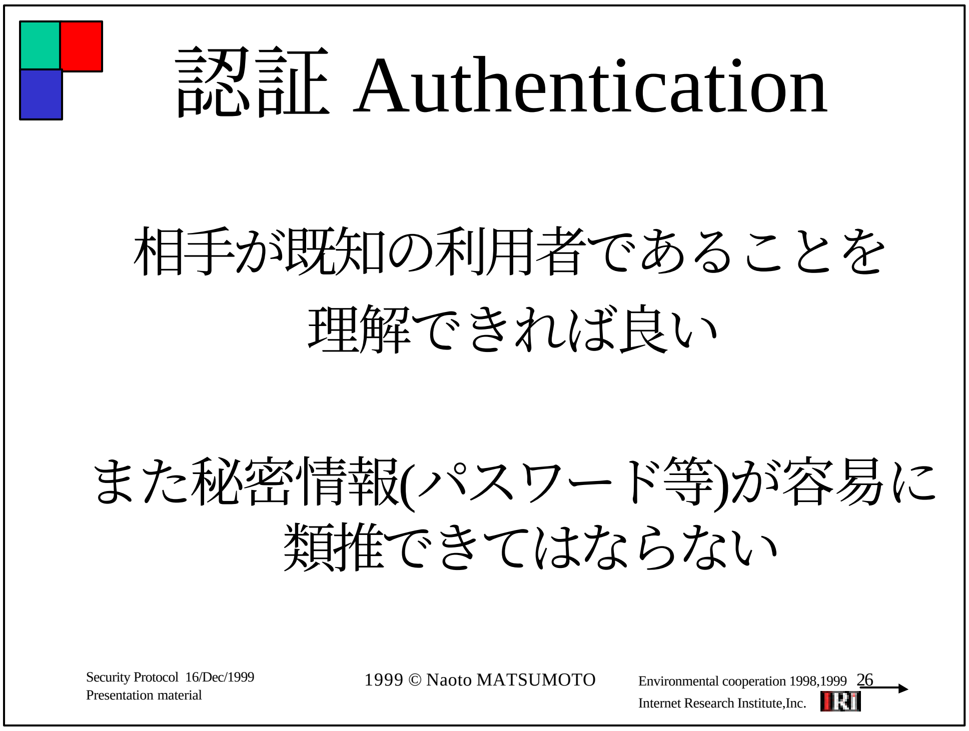
セキュリティ・プロトコル詳細

セキュリティ・プロトコルは、
以下の3要素からなる

1.認証　Authentication

2.制御　Authorization (Control)

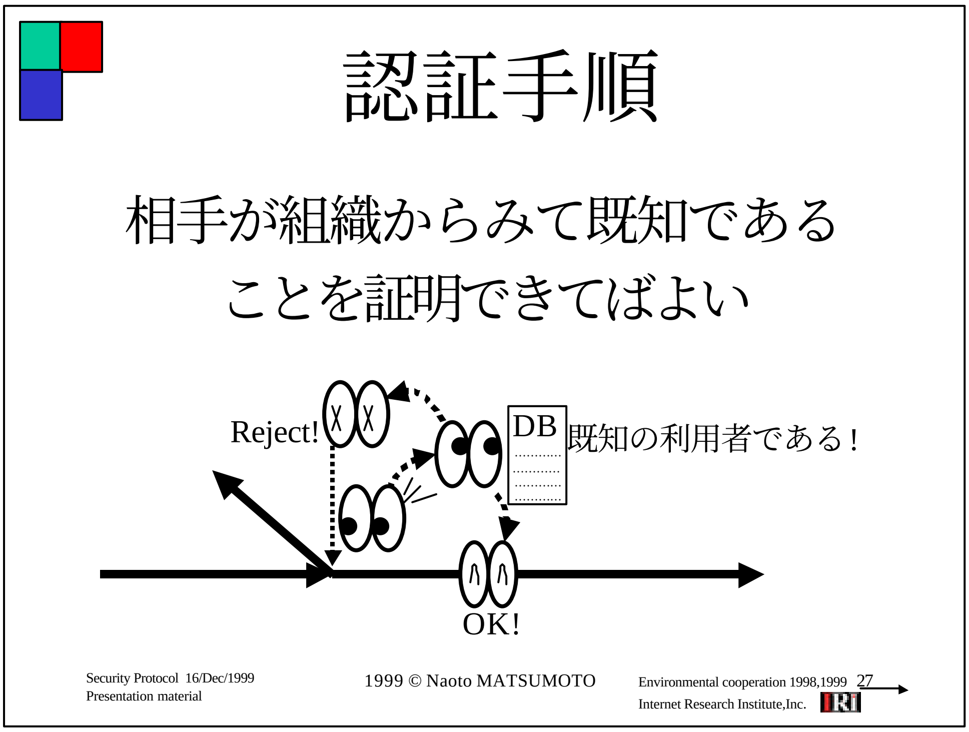
3.防御　Defense



認証 Authentication

相手が既知の利用者であることを
理解できれば良い

また秘密情報(パスワード等)が容易に
類推できてはならない



認証手順

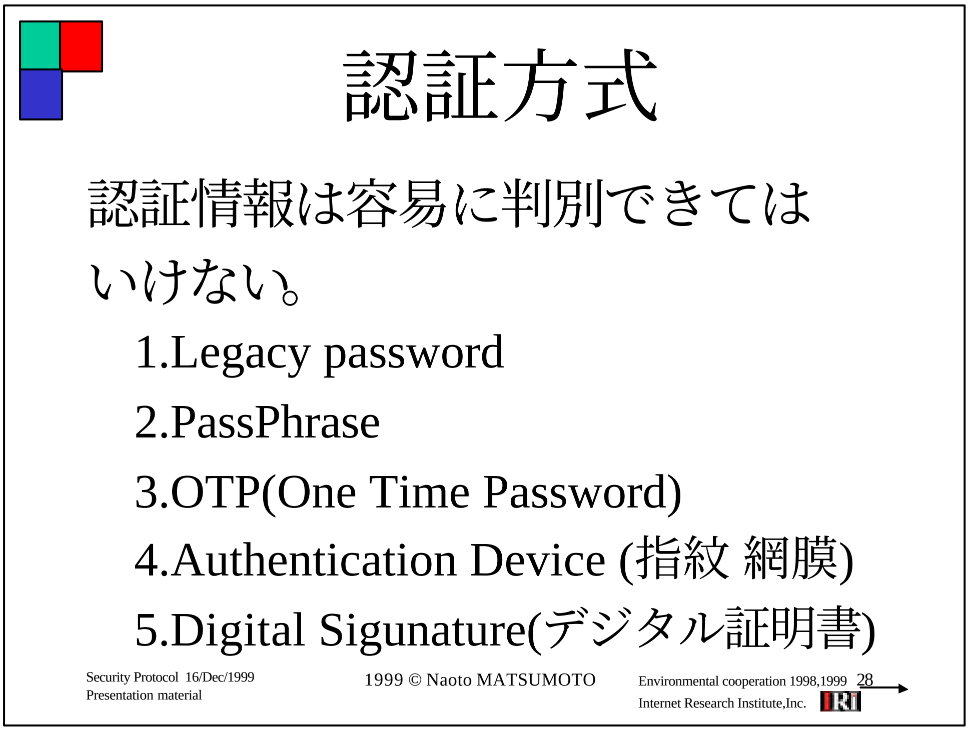
相手が組織からみて既知である
ことを証明できてばよい

Reject!

DB

既知の利用者である！

OK!



認証方式

認証情報は容易に判別できては
いけない。

1.Legacy password

2.PassPhrase

3.OTP(One Time Password)

4.Authentication Device (指紋 網膜)

5.Digital Sigunature(デジタル証明書)

認証実装 ...cont

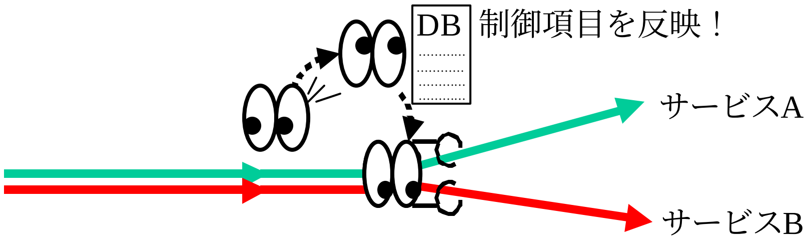
以下の実装と前述の方式が密接に
関わって認証が機能する場合が多い

RADIUS,TACACS,SecureID,
defender,LDAP...etc

(特にリモートアクセス環境において)

制御 Authorization

認証(Authentication)を終えた
利用者に
適切なサービスを提供する



制御実装

RADIUS

TACACS

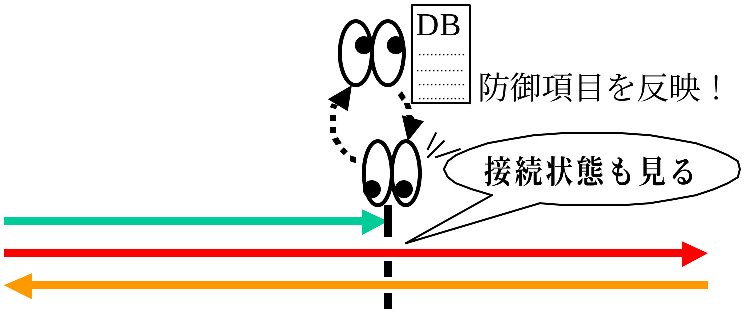
TACACS+

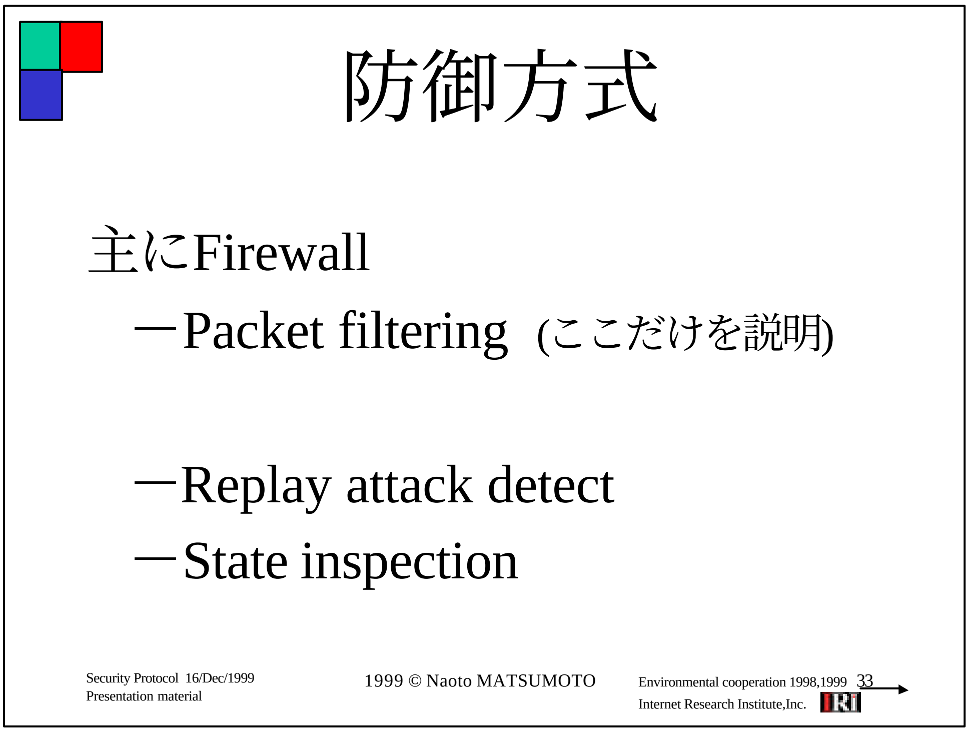
DAIMETER (将来的には)

※認証と制御の実装は一体である場合が多い

防御 Defense

認めるべきではないサービスに
対して防御を行う





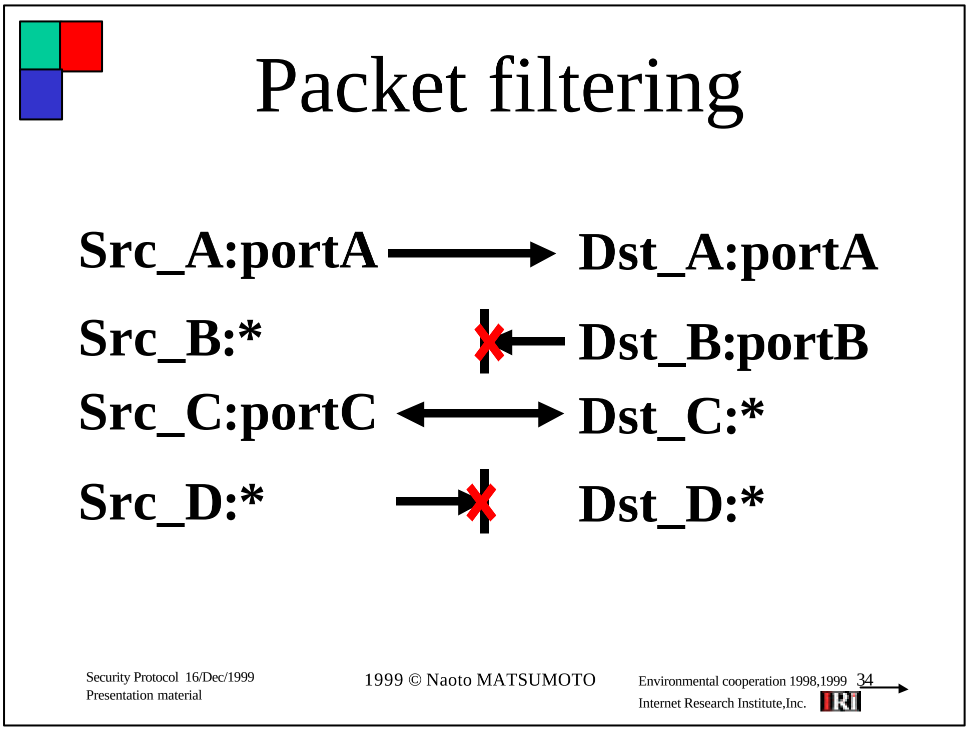
防御方式

主にFirewall

ー Packet filtering (ここだけを説明)

ー Replay attack detect

ー State inspection



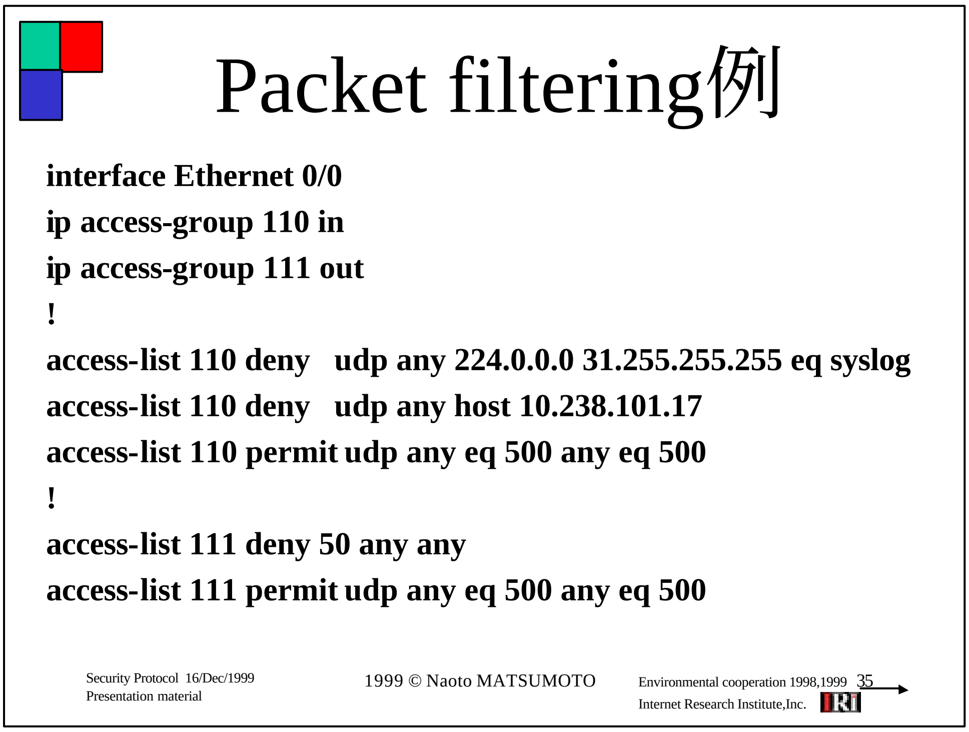
Packet filtering

Src_A:portA → Dst_A:portA

Src_B:* ✗← Dst_B:portB

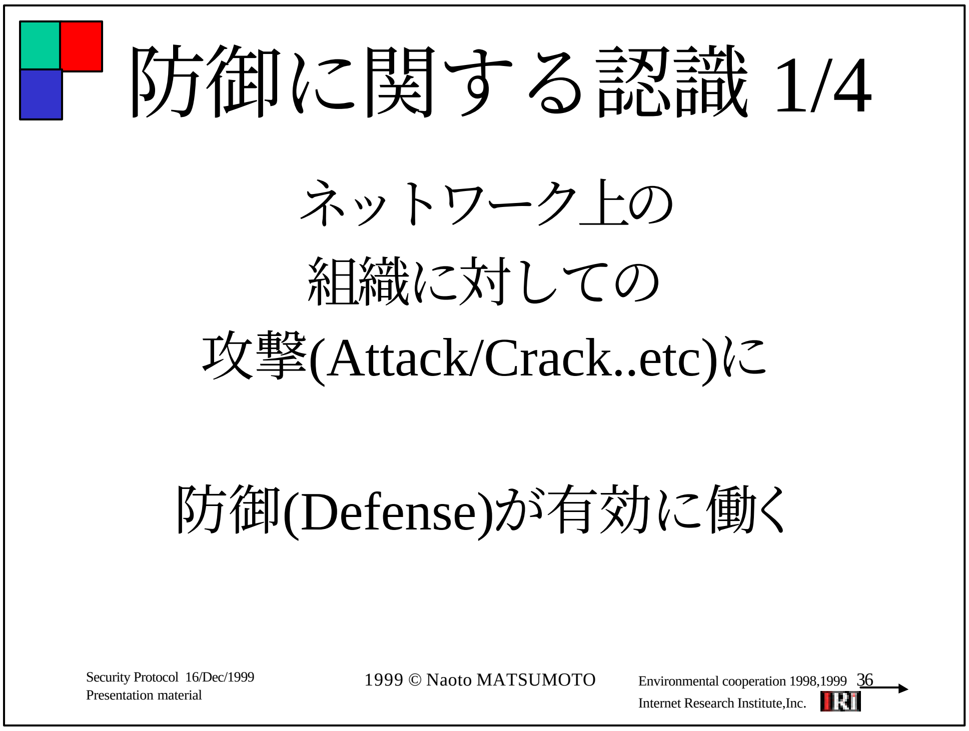
Src_C:portC ↔ Dst_C:*

Src_D:* →✗ Dst_D:*



Packet filtering例

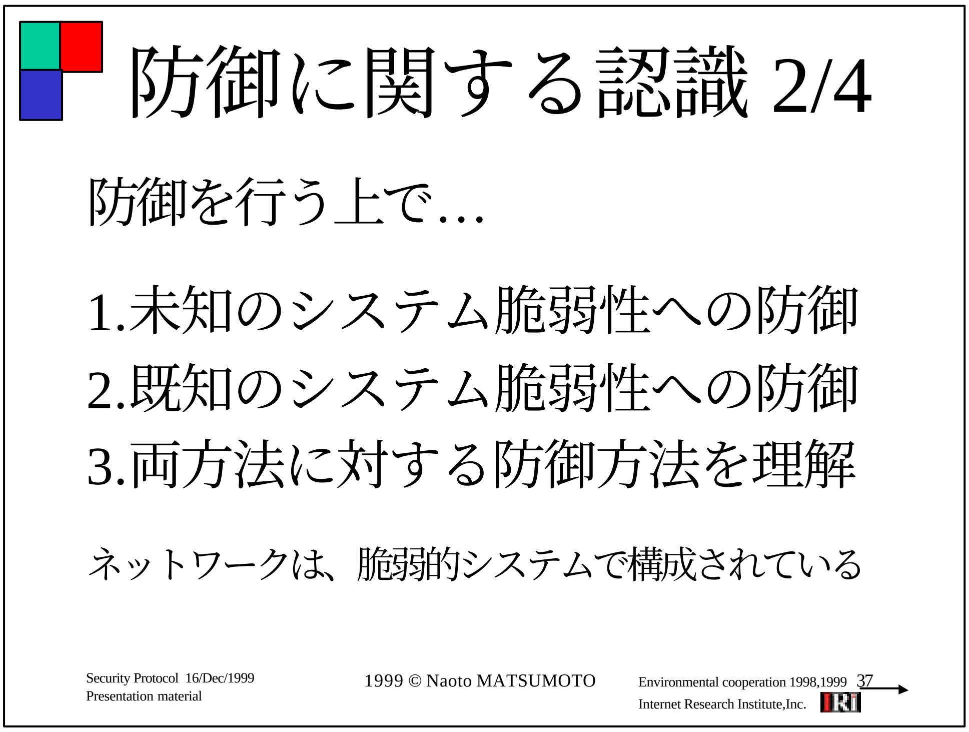
```
interface Ethernet 0/0
ip access-group 110 in
ip access-group 111 out
!
access-list 110 deny   udp any 224.0.0.0 31.255.255.255 eq syslog
access-list 110 deny   udp any host 10.238.101.17
access-list 110 permit udp any eq 500 any eq 500
!
access-list 111 deny 50 any any
access-list 111 permit udp any eq 500 any eq 500
```



防御に関する認識 1/4

ネットワーク上の
組織に対しての
攻撃(Attack/Crack..etc)に

防御(Defense)が有効に働く



防御に関する認識 2/4

防御を行う上で…

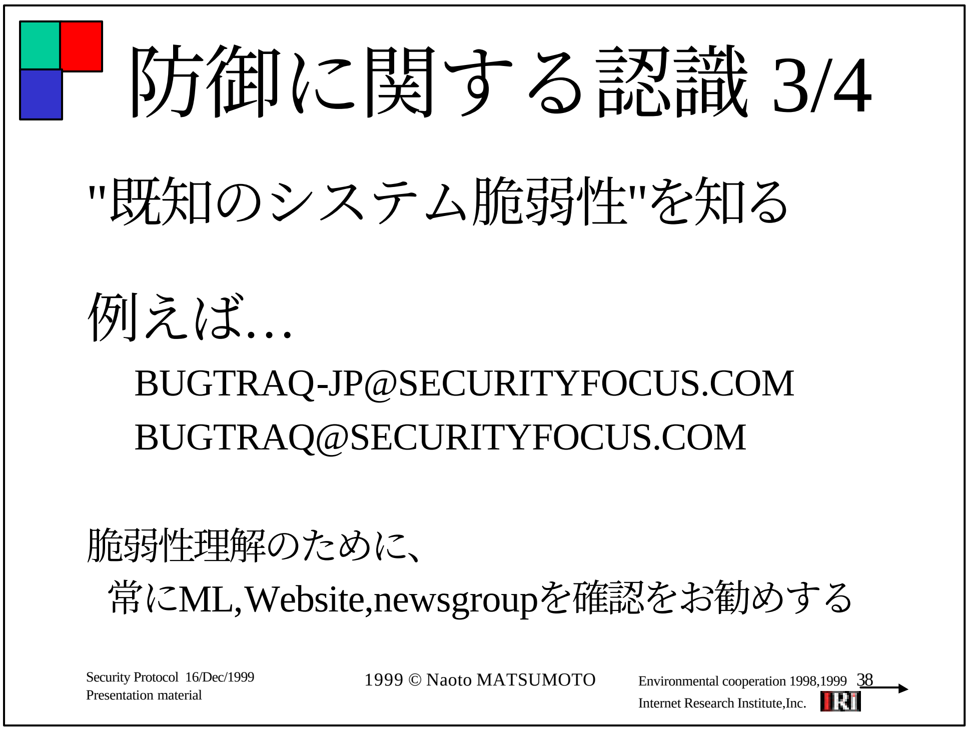
1.未知のシステム脆弱性への防御
2.既知のシステム脆弱性への防御
3.両方法に対する防御方法を理解

ネットワークは、脆弱的システムで構成されている

Security Protocol 16/Dec/1999
Presentation material

1999 © Naoto MATSUMOTO

Environmental cooperation 1998,1999 37
Internet Research Institute,Inc.



防御に関する認識 3/4

"既知のシステム脆弱性"を知る

例えば…

BUGTRAQ-JP@SECURITYFOCUS.COM
BUGTRAQ@SECURITYFOCUS.COM

脆弱性理解のために、
常にML,Website,newsgroupを確認をお勧めする

Security Protocol 16/Dec/1999
Presentation material

1999 © Naoto MATSUMOTO

Environmental cooperation 1998,1999 38
Internet Research Institute,Inc.

防御に関する認識 3/4

"防御方法を理解"について

例えば…

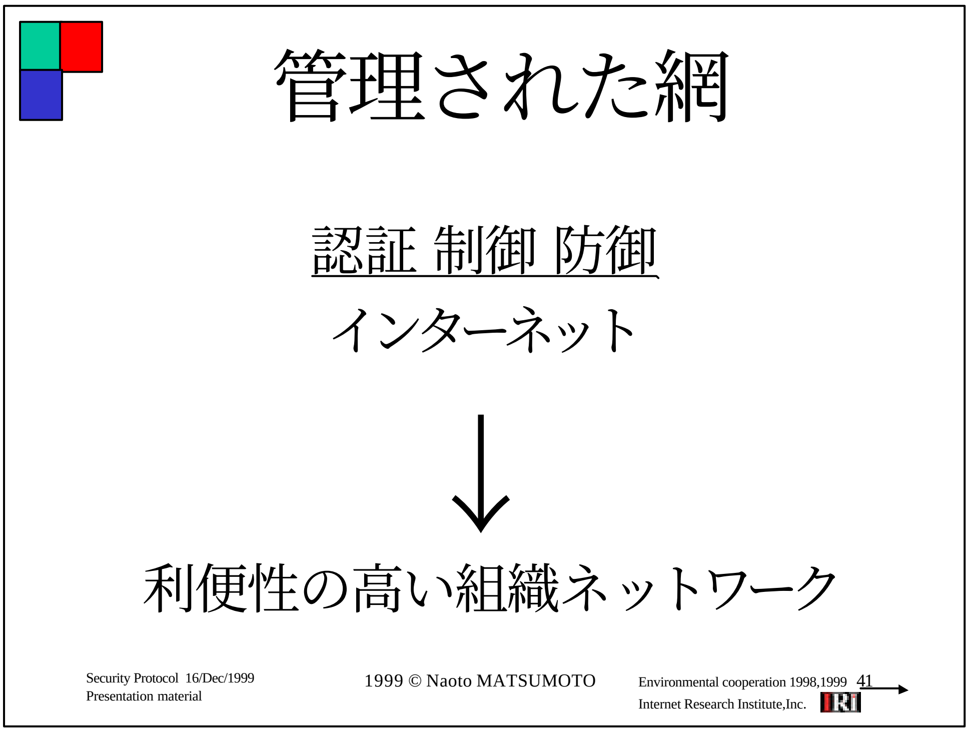
Firewall Defenders

http://www.firewall.gr.jp/

Firewallが全てでは無いが、理解を深める事が必要

セキュリティ・プロトコル

認証、制御、防御を的確に
適用した場合には、
どのような
ネットワークが構成されるのか？



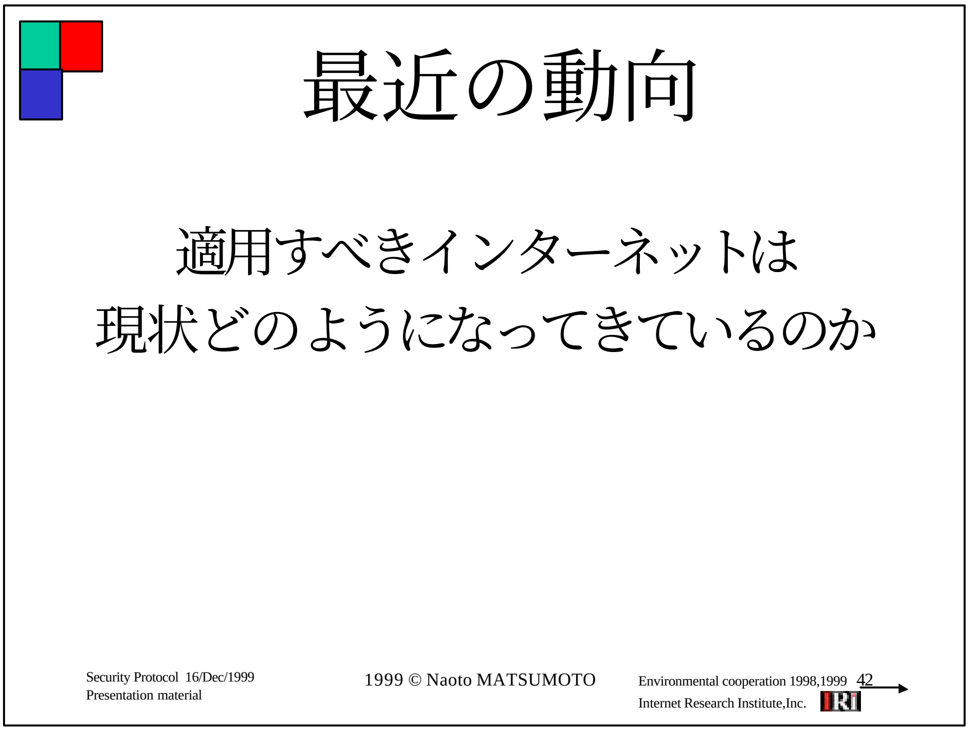
管理された網

認証 制御 防御

インターネット

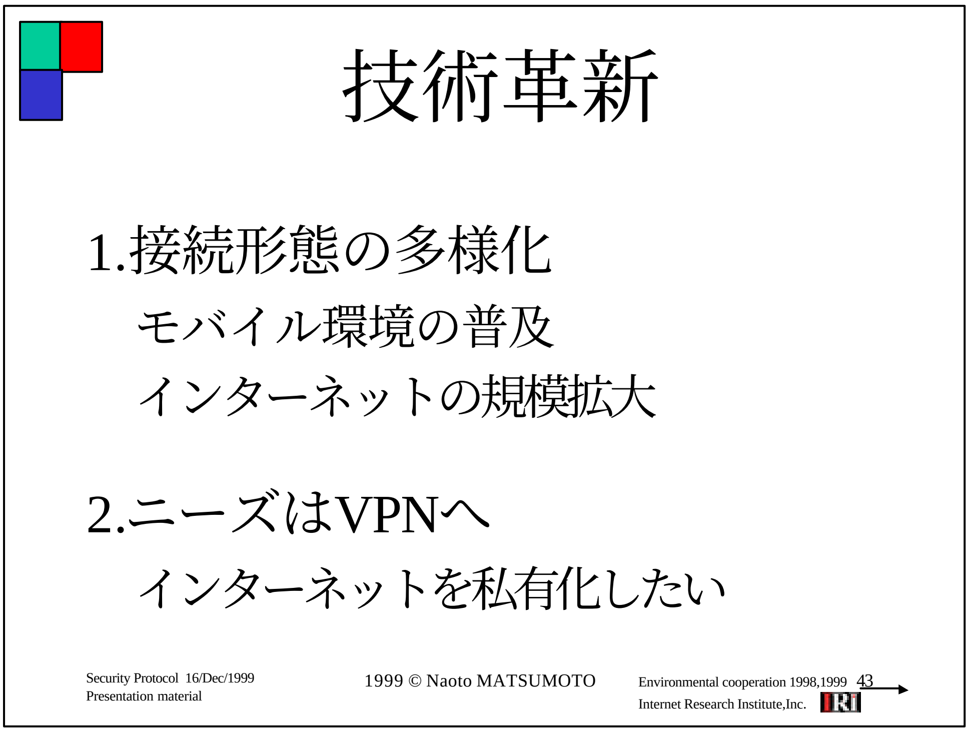
↓

利便性の高い組織ネットワーク



最近の動向

適用すべきインターネットは
現状どのようになってきているのか



技術革新

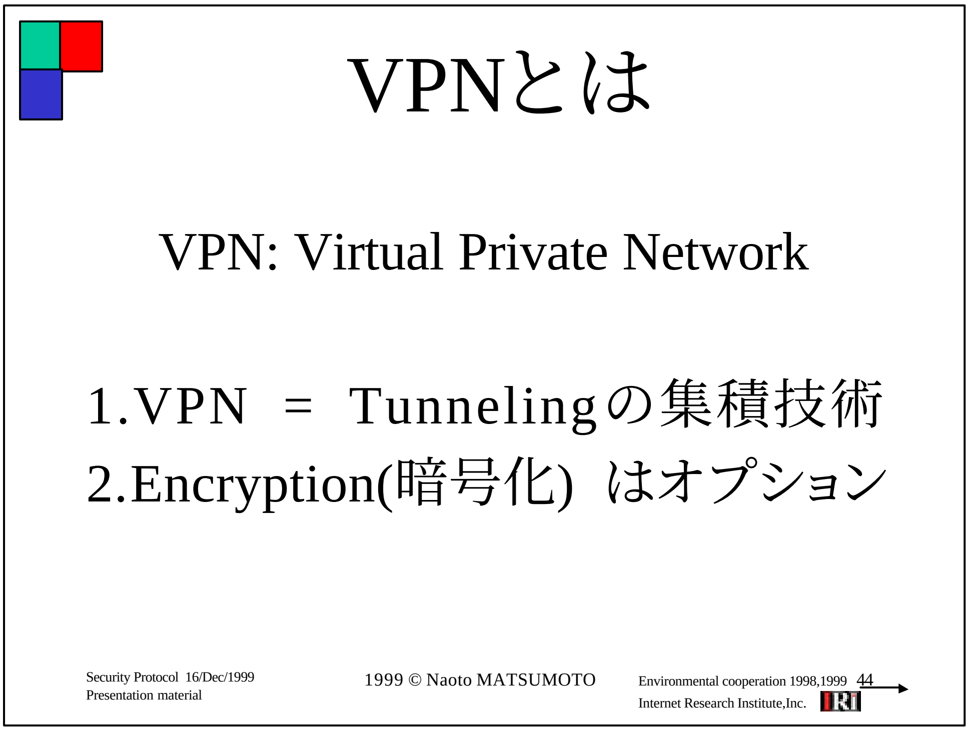
1.接続形態の多様化

モバイル環境の普及

インターネットの規模拡大

2.ニーズはVPNへ

インターネットを私有化したい

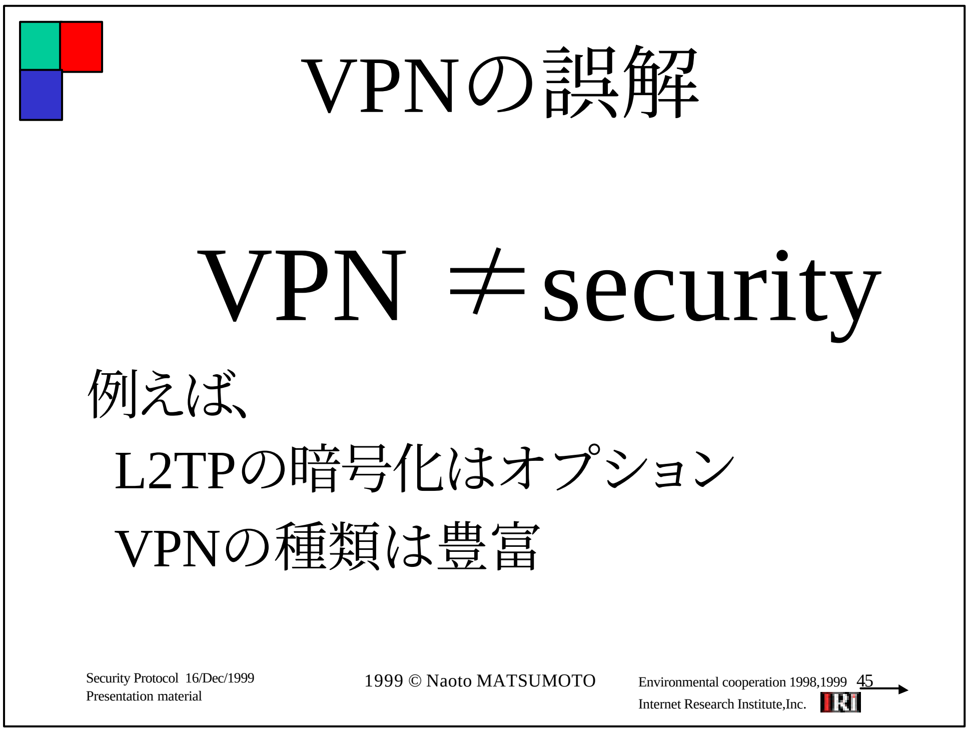


VPNとは

VPN: Virtual Private Network

1.VPN = Tunnelingの集積技術

2.Encryption(暗号化) はオプション



VPNの誤解

VPN ≠security

例えば、

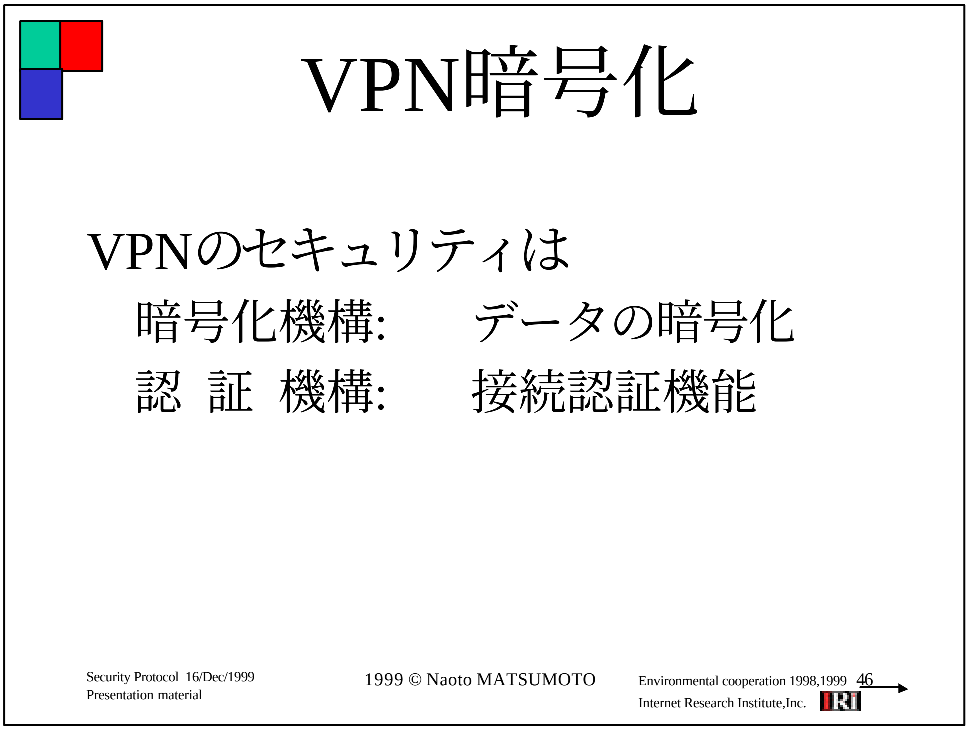
L2TPの暗号化はオプション

VPNの種類は豊富

Security Protocol 16/Dec/1999
Presentation material

1999 © Naoto MATSUMOTO

Environmental cooperation 1998,1999 45
Internet Research Institute,Inc.



VPN暗号化

VPNのセキュリティは

暗号化機構:　　データの暗号化

認　証　機構:　　接続認証機能

Security Protocol 16/Dec/1999
Presentation material

1999 © Naoto MATSUMOTO

Environmental cooperation 1998,1999 46
Internet Research Institute,Inc.

よくある誤解

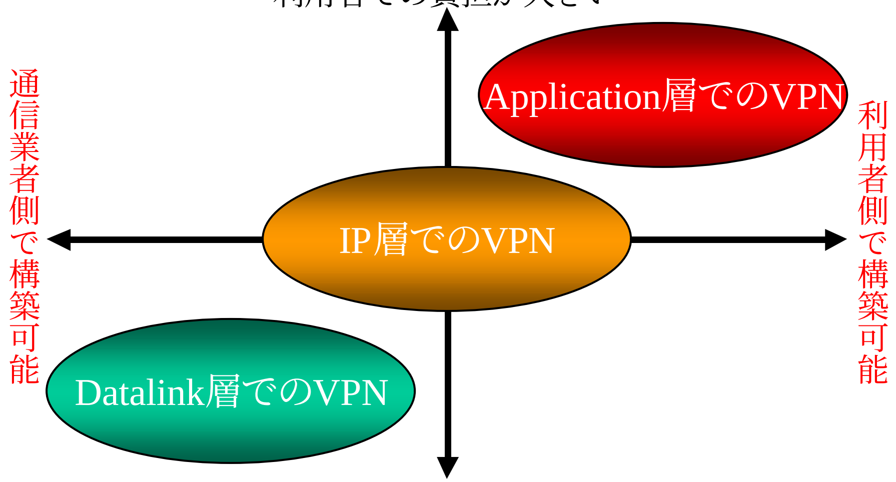
暗号技術≠ハッシュ技術

DES≠MD5

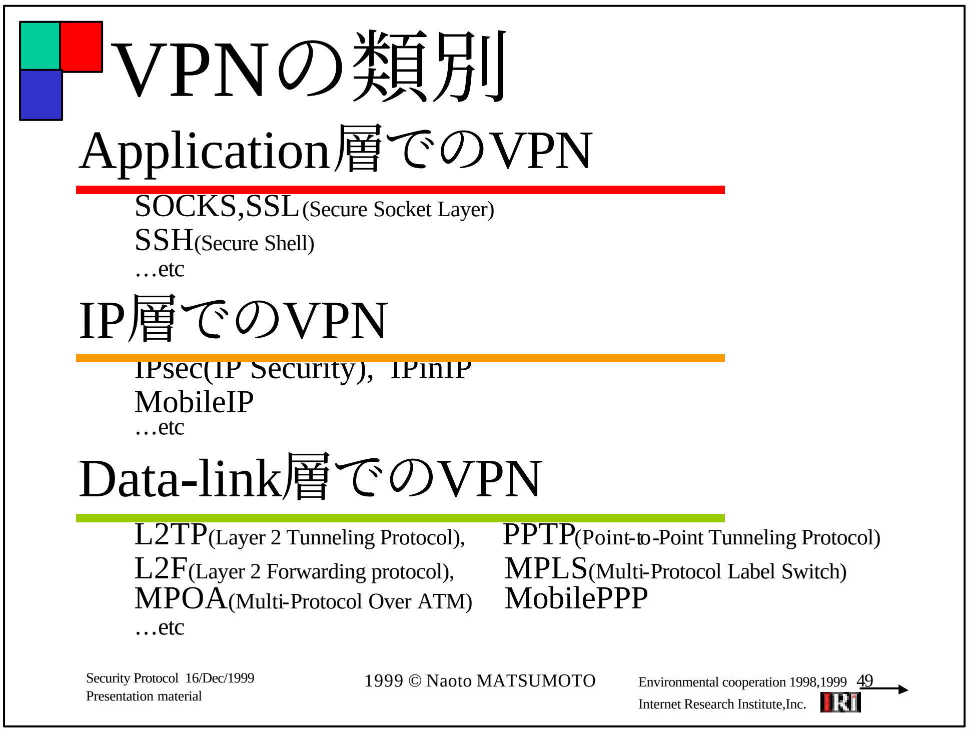
暗号処理用技術　署名処理用技術

VPNの種別

利用者での負担が大きい



通信事業者での負担が大きい



VPNの類別

Application層でのVPN

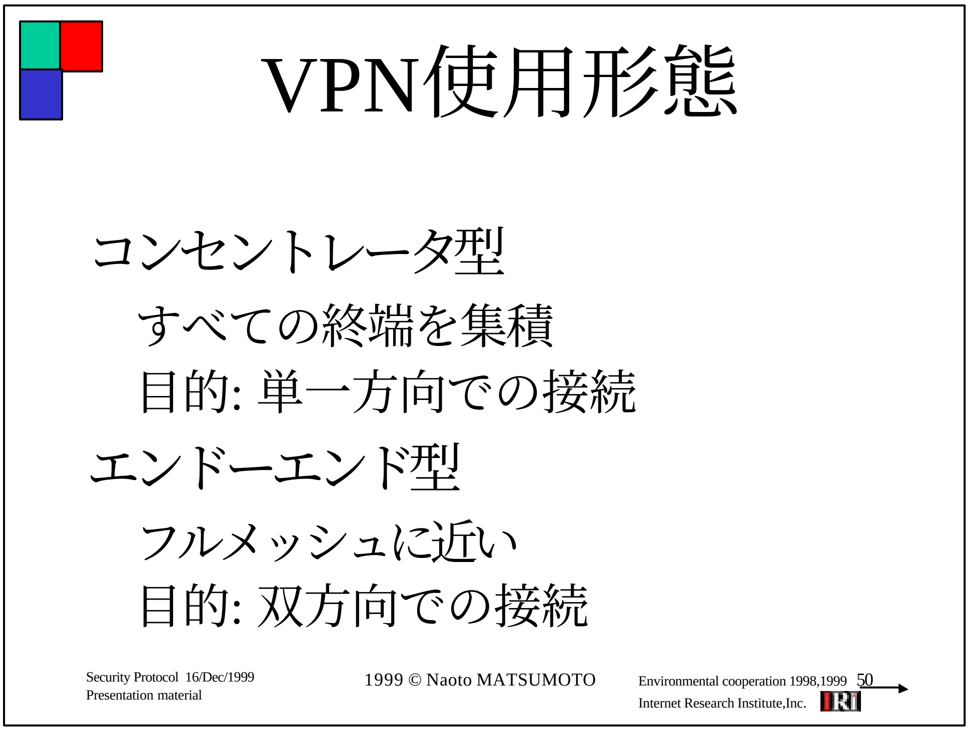
SOCKS,SSL(Secure Socket Layer)
SSH(Secure Shell)
…etc

IP層でのVPN

IPsec(IP Security), IPinIP
MobileIP
…etc

Data-link層でのVPN

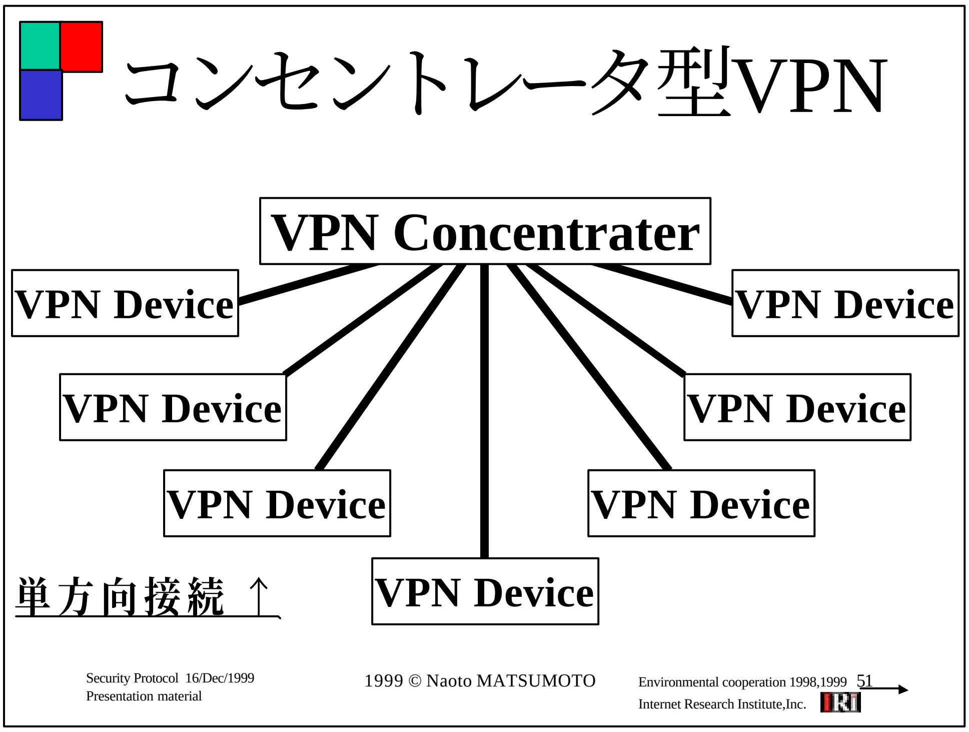
L2TP(Layer 2 Tunneling Protocol), PPTP(Point-to-Point Tunneling Protocol)
L2F(Layer 2 Forwarding protocol), MPLS(Multi-Protocol Label Switch)
MPOA(Multi-Protocol Over ATM) MobilePPP
…etc



VPN使用形態

コンセントレータ型
- すべての終端を集積
- 目的: 単一方向での接続

エンドーエンド型
- フルメッシュに近い
- 目的: 双方向での接続



コンセントレータ型VPN

VPN Concentrater

VPN Device

VPN Device

VPN Device

VPN Device

VPN Device

VPN Device

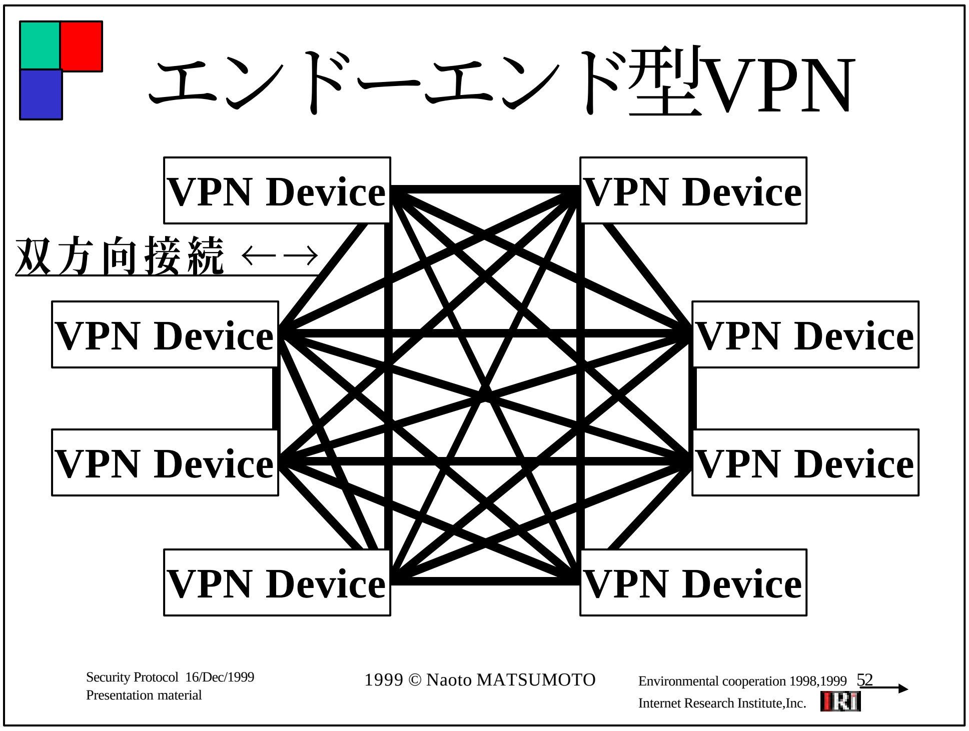
VPN Device

単方向接続 ↑

Security Protocol 16/Dec/1999
Presentation material

1999 © Naoto MATSUMOTO

Environmental cooperation 1998,1999 51
Internet Research Institute,Inc.



エンドーエンド型VPN

VPN Device

VPN Device

双方向接続 ←→

VPN Device

VPN Device

VPN Device

VPN Device

VPN Device

VPN Device

Security Protocol 16/Dec/1999
Presentation material

1999 © Naoto MATSUMOTO

Environmental cooperation 1998,1999 52
Internet Research Institute,Inc.

VPN利用

ではVPNに、認証,制御,防御を
的確に適用した場合には、
どのようなネットワークが
構成されるのか？

VPNの利用

認証+制御+防御

. VPN .

インターネット

↓

より柔軟な広域組織ネットワーク

ネットワークの多様化

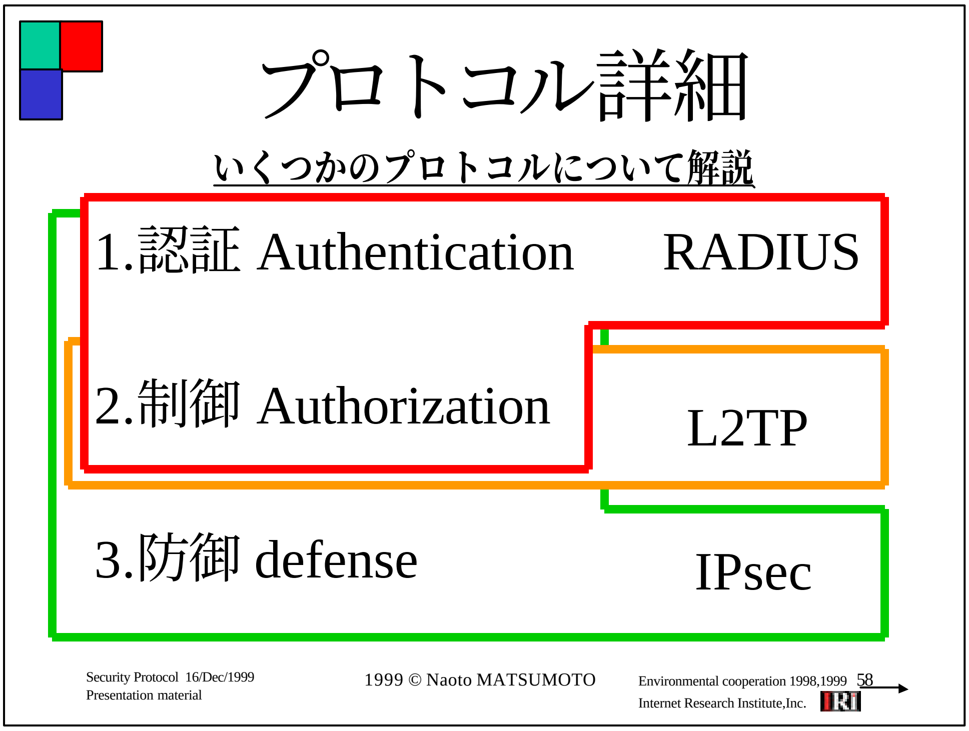
多様化するネットワークを
いかにに利便性を削らずに
運用していくか？

<u>セキュリティ・プロトコルを理解し</u>
<u>適切な場所で用いる</u>

休憩

セキュリティ・プロトコル

II
プロトコル詳細



プロトコル詳細

いくつかのプロトコルについて解説

1.認証 Authentication RADIUS

2.制御 Authorization L2TP

3.防御 defense IPsec

RADIUS

Remote **A**ccess **D**ail-**I**n **U**ser **S**ervic

リモートアクセスユーザ向けサービス用途

RFC2138 Standards Track

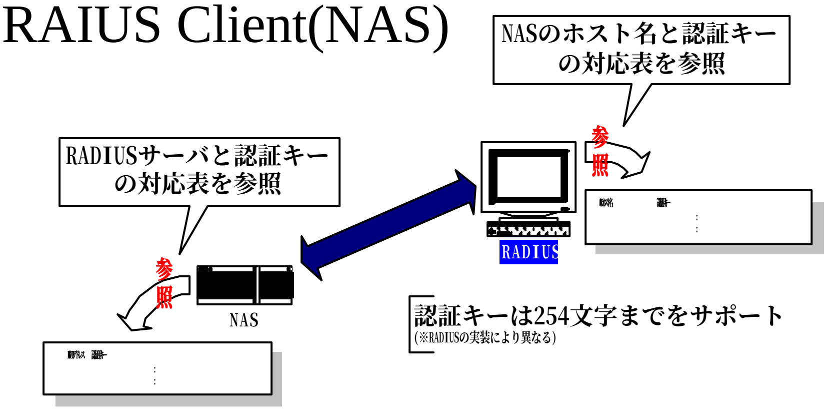
RADIUS全般に関する記述

※RFC2139 RADIUS Accounting

RADIUS基本動作

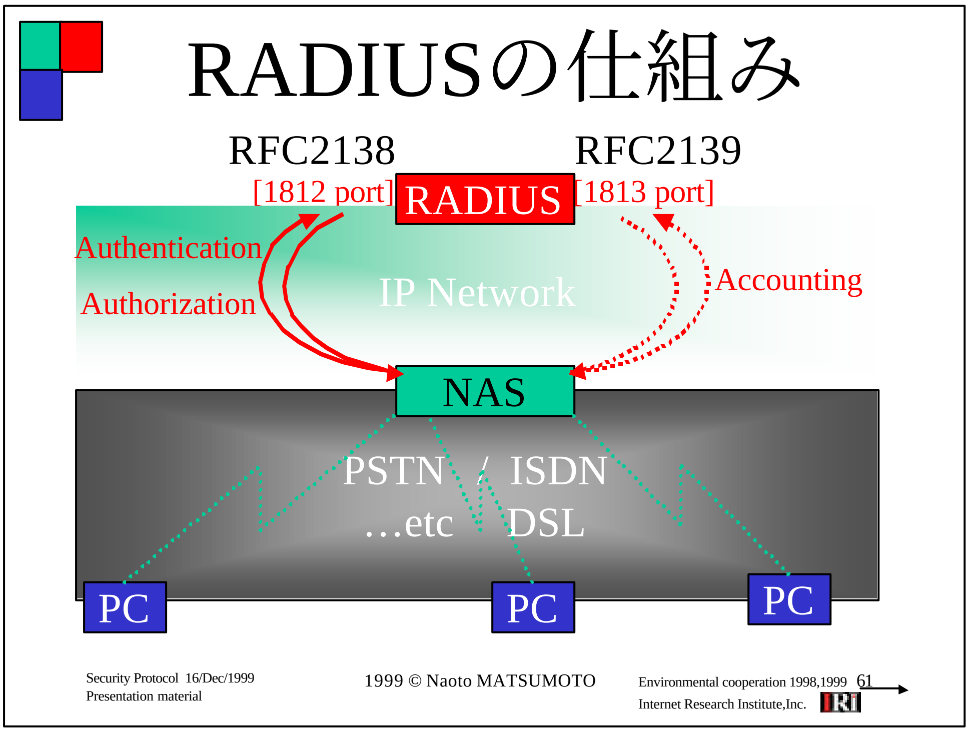
RADIUS Serverと

RAIUS Client(NAS)



NASのホスト名と認証キーの対応表を参照
参照
RADIUS
RADIUSサーバと認証キーの対応表を参照
参照
NAS

認証キーは254文字までをサポート
(※RADIUSの実装により異なる)



RADIUSの仕組み

RFC2138 RFC2139

[1812 port] RADIUS [1813 port]

Authentication

Authorization

IP Network

Accounting

NAS

PSTN / ISDN

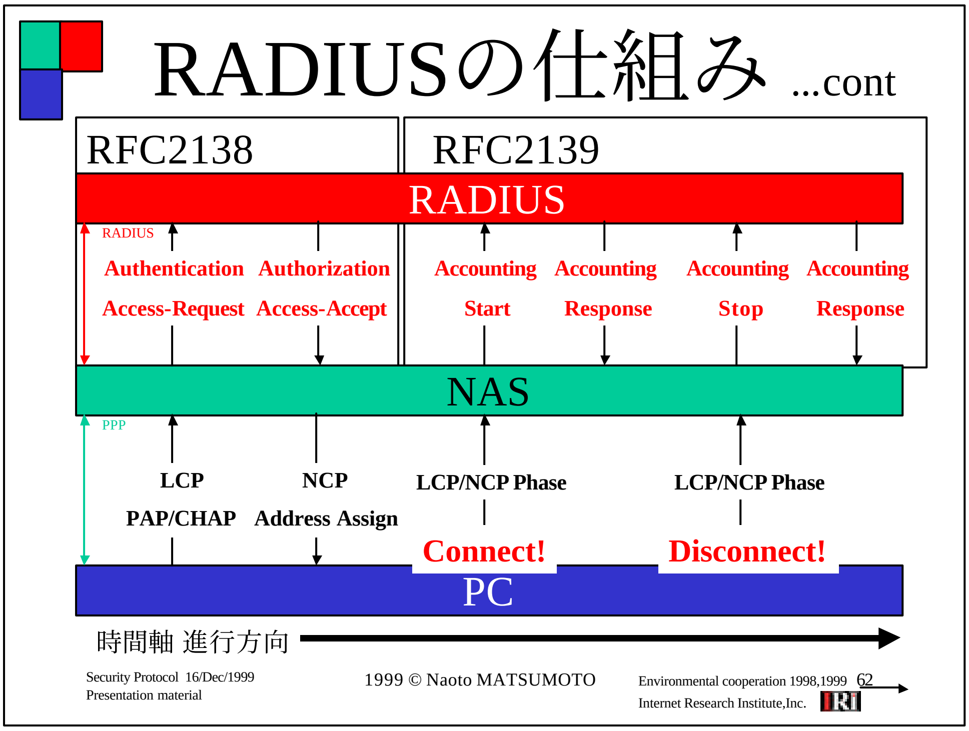
…etc DSL

PC PC PC

Security Protocol 16/Dec/1999
Presentation material

1999 © Naoto MATSUMOTO

Environmental cooperation 1998,1999 61
Internet Research Institute,Inc.



RADIUSの仕組み ...cont

RFC2138 RFC2139

RADIUS

RADIUS

Authentication Authorization

Access-Request Access-Accept

Accounting Start

Accounting Response

Accounting Stop

Accounting Response

NAS

PPP

LCP PAP/CHAP

NCP Address Assign

LCP/NCP Phase

Connect!

LCP/NCP Phase

Disconnect!

PC

時間軸 進行方向

Security Protocol 16/Dec/1999
Presentation material

1999 © Naoto MATSUMOTO

Environmental cooperation 1998,1999 62
Internet Research Institute,Inc.

RADIUS Authentication

```
Code:      Access-Request
Identifier: 85
Authentic:  1234567890123456
Attributes:
      User-Name = “not@iri.co.jp”        :RADIUS認証を求めるユーザ名
      Service-Type = Framed-User
      NAS-IP-Address = 203.63.154.1
      NAS-Port = 1234
      NAS-Port-Type = Async
      User-Password = "<205><234><3><18><185><131><163><202>vH"
sending Access-Request...
```

RADIUS Authorization

```
Code:      Access-Accept
Identifier: 85
Authentic:  6<0>o<191><201><25><233>y<17><242>Fr<221><144>^7
Attributes:
      Service-Type = Framed-User                    :ユーザサービス
      Framed-Protocol = PPP                         :の設定情報を
      Framed-IP-Address = 255.255.255.254           :RADIUS Server
      Framed-IP-Netmask = 255.255.255.255           :から取得する。
      Idle-Timeout = 3600                           :タイムアウトは3600秒
```

RADIUS構成要素

1.RADIUS daemon

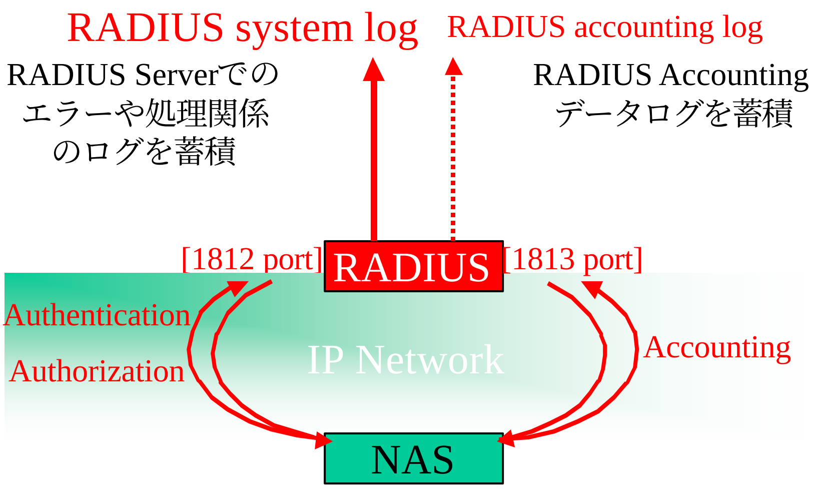
各種OSのプロセスとして動作

2.Authentication Database

RADIUSユーザ認証情報を管理

最近のRADIUSではLDAP,SQL経由でユーザ管理

RADIUS入出力データ



RADIUS system log

RADIUS Serverでの
エラーや処理関係
のログを蓄積

RADIUS accounting log

RADIUS Accounting
データログを蓄積

[1812 port]

RADIUS

[1813 port]

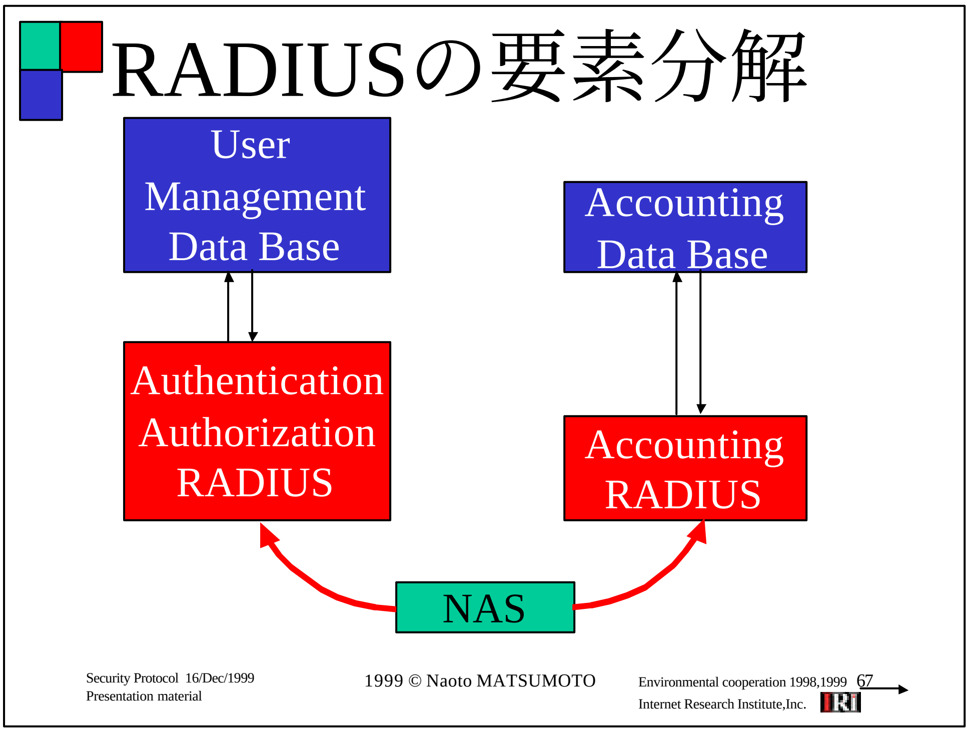
Authentication

Authorization

IP Network

Accounting

NAS



RADIUSの要素分解

User Management Data Base

Accounting Data Base

Authentication Authorization RADIUS

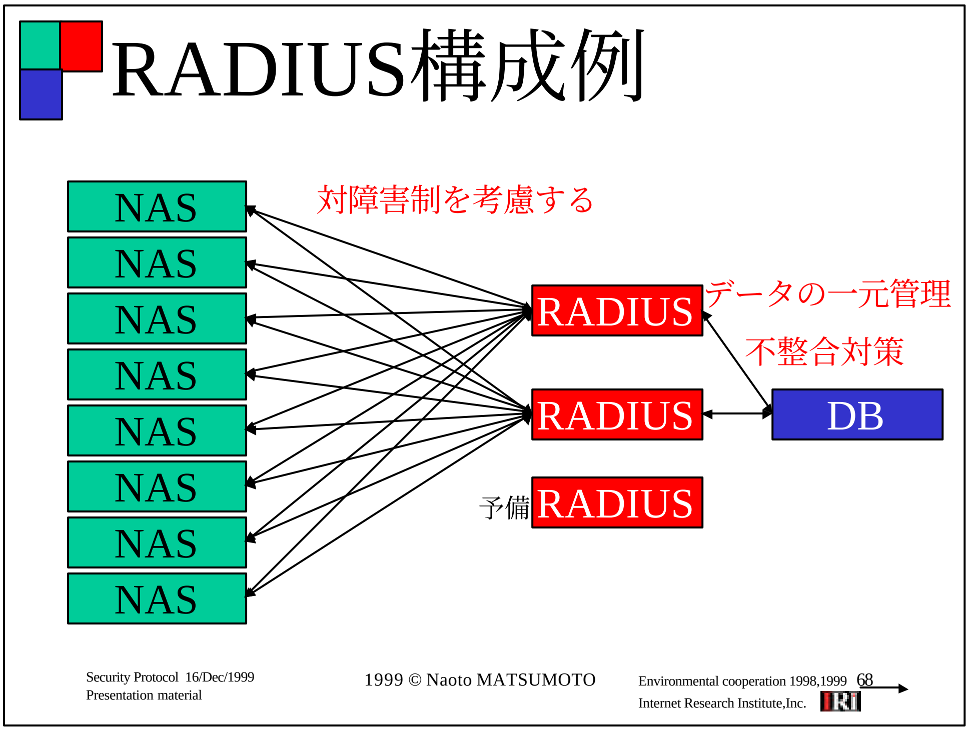
Accounting RADIUS

NAS

Security Protocol 16/Dec/1999
Presentation material

1999 © Naoto MATSUMOTO

Environmental cooperation 1998,1999 67
Internet Research Institute,Inc.



RADIUS構成例

NAS

NAS

NAS

NAS

NAS

NAS

NAS

NAS

対障害制を考慮する

RADIUS

データの一元管理

不整合対策

RADIUS

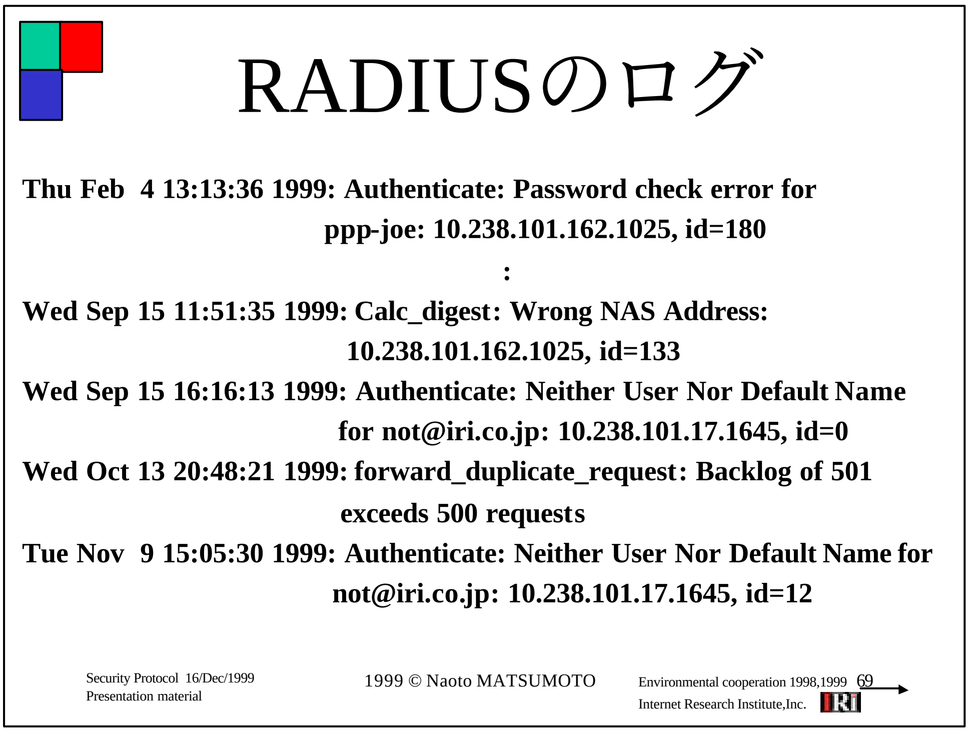
DB

予備RADIUS

Security Protocol 16/Dec/1999
Presentation material

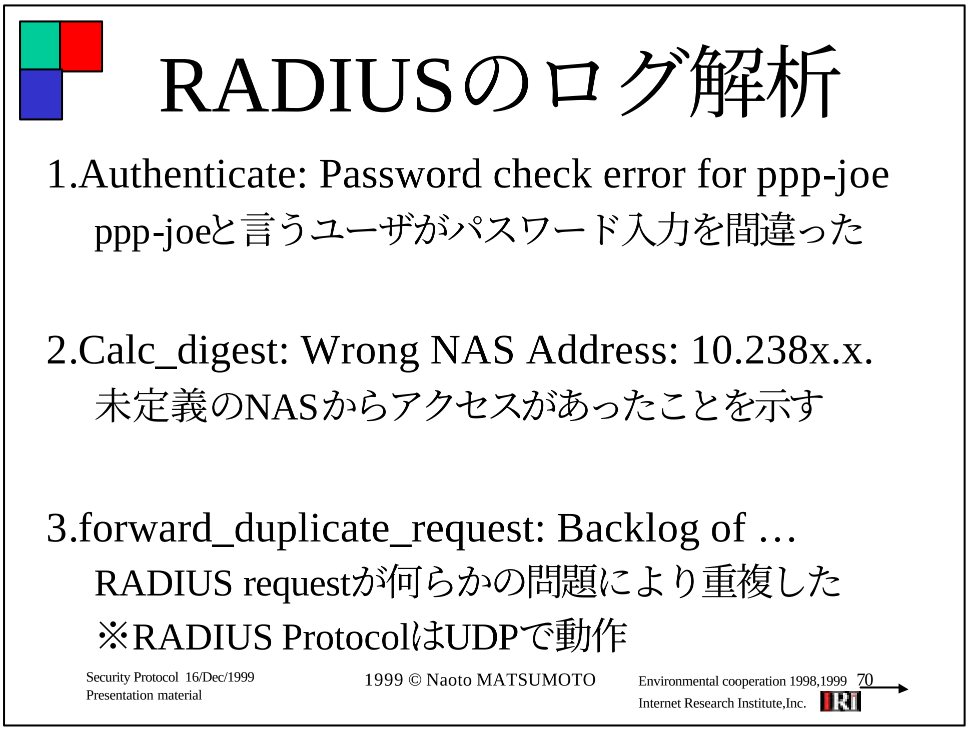
1999 © Naoto MATSUMOTO

Environmental cooperation 1998,1999 68
Internet Research Institute,Inc.



RADIUSのログ

```
Thu Feb  4 13:13:36 1999: Authenticate: Password check error for
                              ppp-joe: 10.238.101.162.1025, id=180
                                            :
Wed Sep 15 11:51:35 1999: Calc_digest: Wrong NAS Address:
                                10.238.101.162.1025, id=133
Wed Sep 15 16:16:13 1999: Authenticate: Neither User Nor Default Name
                               for not@iri.co.jp: 10.238.101.17.1645, id=0
Wed Oct 13 20:48:21 1999: forward_duplicate_request: Backlog of 501
                               exceeds 500 requests
Tue Nov  9 15:05:30 1999: Authenticate: Neither User Nor Default Name for
                              not@iri.co.jp: 10.238.101.17.1645, id=12
```



RADIUSのログ解析

1.Authenticate: Password check error for ppp-joe

ppp-joeと言うユーザがパスワード入力を間違った

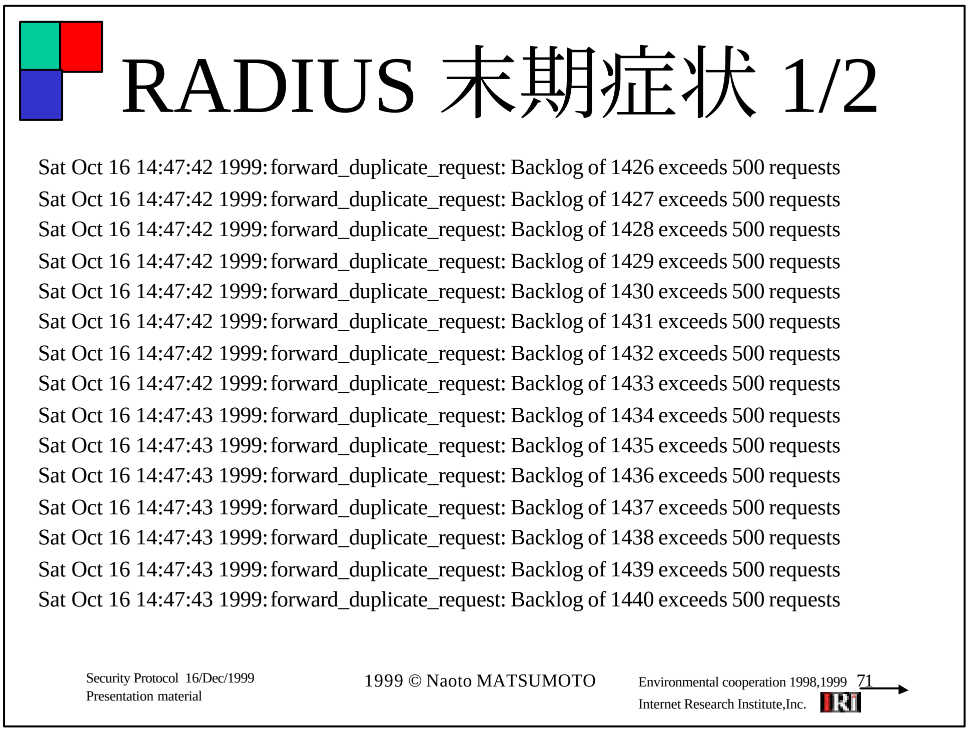
2.Calc_digest: Wrong NAS Address: 10.238x.x.

未定義のNASからアクセスがあったことを示す

3.forward_duplicate_request: Backlog of …

RADIUS requestが何らかの問題により重複した

※RADIUS ProtocolはUDPで動作



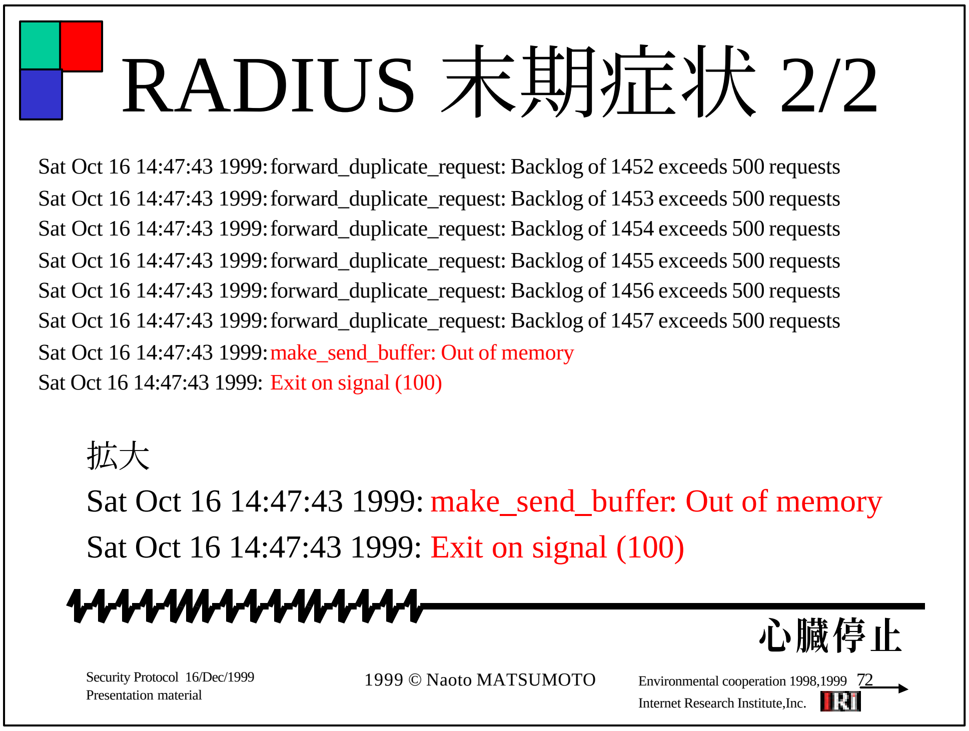
RADIUS 末期症状 1/2

```
Sat Oct 16 14:47:42 1999: forward_duplicate_request: Backlog of 1426 exceeds 500 requests
Sat Oct 16 14:47:42 1999: forward_duplicate_request: Backlog of 1427 exceeds 500 requests
Sat Oct 16 14:47:42 1999: forward_duplicate_request: Backlog of 1428 exceeds 500 requests
Sat Oct 16 14:47:42 1999: forward_duplicate_request: Backlog of 1429 exceeds 500 requests
Sat Oct 16 14:47:42 1999: forward_duplicate_request: Backlog of 1430 exceeds 500 requests
Sat Oct 16 14:47:42 1999: forward_duplicate_request: Backlog of 1431 exceeds 500 requests
Sat Oct 16 14:47:42 1999: forward_duplicate_request: Backlog of 1432 exceeds 500 requests
Sat Oct 16 14:47:42 1999: forward_duplicate_request: Backlog of 1433 exceeds 500 requests
Sat Oct 16 14:47:43 1999: forward_duplicate_request: Backlog of 1434 exceeds 500 requests
Sat Oct 16 14:47:43 1999: forward_duplicate_request: Backlog of 1435 exceeds 500 requests
Sat Oct 16 14:47:43 1999: forward_duplicate_request: Backlog of 1436 exceeds 500 requests
Sat Oct 16 14:47:43 1999: forward_duplicate_request: Backlog of 1437 exceeds 500 requests
Sat Oct 16 14:47:43 1999: forward_duplicate_request: Backlog of 1438 exceeds 500 requests
Sat Oct 16 14:47:43 1999: forward_duplicate_request: Backlog of 1439 exceeds 500 requests
Sat Oct 16 14:47:43 1999: forward_duplicate_request: Backlog of 1440 exceeds 500 requests
```

Security Protocol 16/Dec/1999
Presentation material

1999 © Naoto MATSUMOTO

Environmental cooperation 1998,1999 71
Internet Research Institute,Inc.



RADIUS 末期症状 2/2

```
Sat Oct 16 14:47:43 1999: forward_duplicate_request: Backlog of 1452 exceeds 500 requests
Sat Oct 16 14:47:43 1999: forward_duplicate_request: Backlog of 1453 exceeds 500 requests
Sat Oct 16 14:47:43 1999: forward_duplicate_request: Backlog of 1454 exceeds 500 requests
Sat Oct 16 14:47:43 1999: forward_duplicate_request: Backlog of 1455 exceeds 500 requests
Sat Oct 16 14:47:43 1999: forward_duplicate_request: Backlog of 1456 exceeds 500 requests
Sat Oct 16 14:47:43 1999: forward_duplicate_request: Backlog of 1457 exceeds 500 requests
Sat Oct 16 14:47:43 1999: make_send_buffer: Out of memory
Sat Oct 16 14:47:43 1999: Exit on signal (100)
```

拡大

```
Sat Oct 16 14:47:43 1999: make_send_buffer: Out of memory
Sat Oct 16 14:47:43 1999: Exit on signal (100)
```

Security Protocol 16/Dec/1999
Presentation material

1999 © Naoto MATSUMOTO

Environmental cooperation 1998,1999 72
Internet Research Institute,Inc.

L2TP

L2TP

Layer Two Tunneling Protocol

RFC2661 Standards Track

暗号化はオプションである

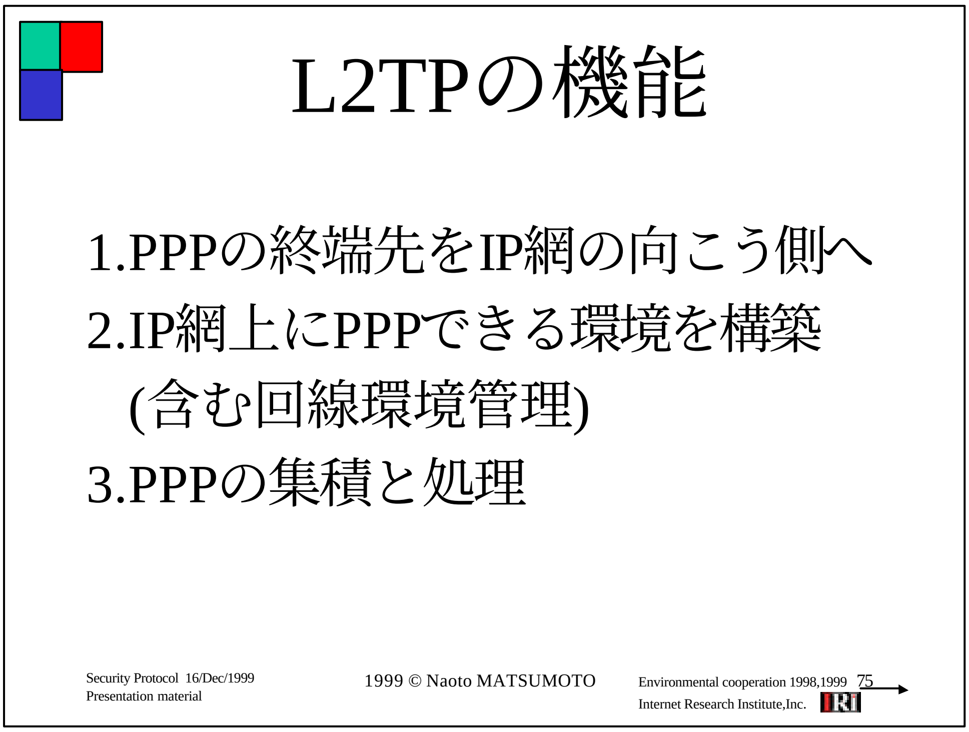
現在のL2TPには実装されていない

L2TPの誤解

L2TP ＝ PPP over IP

L2TP ≠暗号化

L2TP ＝Tunneling

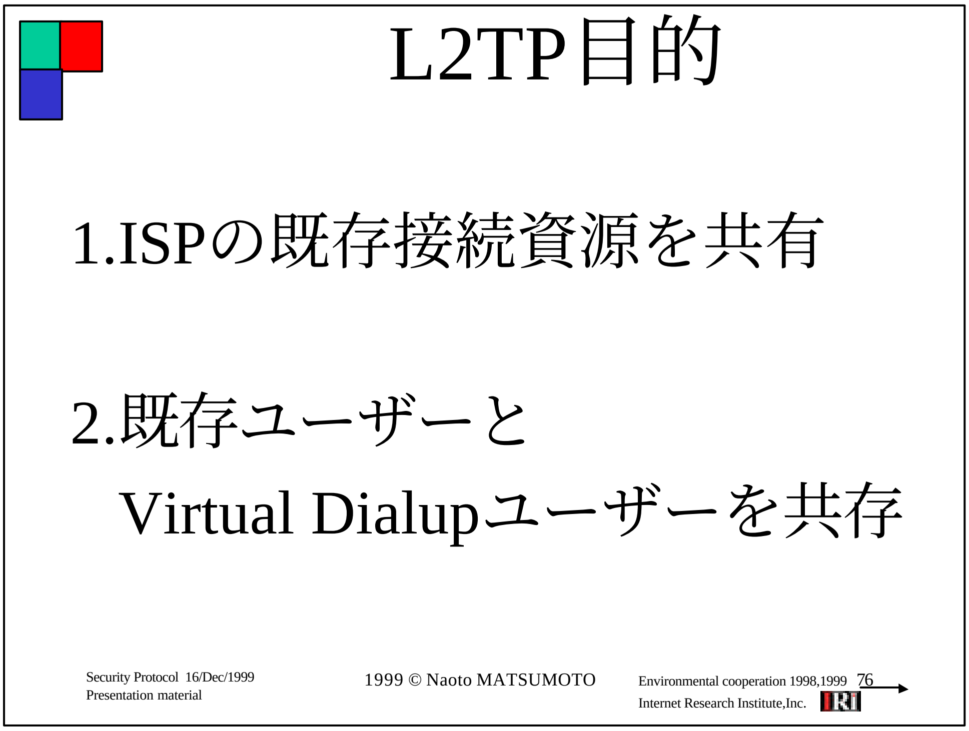


L2TPの機能

1.PPPの終端先をIP網の向こう側へ

2.IP網上にPPPできる環境を構築
(含む回線環境管理)

3.PPPの集積と処理



L2TP目的

1.ISPの既存接続資源を共有

2.既存ユーザーと
Virtual Dialupユーザーを共存

L2TPプロトコル概要

LACで動作

1.PPP Datagramをカプセル化

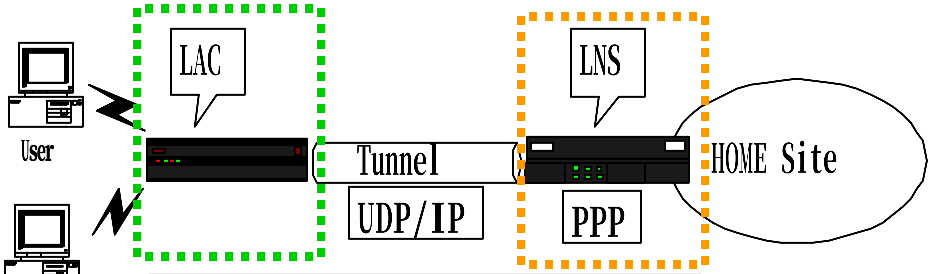
2.カプセル化データを搬送(UDP)

3.PPP Datagramをカプセルから摘出

4.PPP上でLCP/NCPの処理を実行

LNSで動作

L2TPの処理イメージ



LAC: L2TP Access Concentrator
LNS: L2TP Network Server

L2TPの動作

1.認証(Authentication)　[外部に依存]

RADIUS等に依存

2.制御(Authorization)　[外部と連携]

PPPと連携

3.防御(defense)　[外部に依存]

上位層(IP層)での制御に依存

暗号化に関して

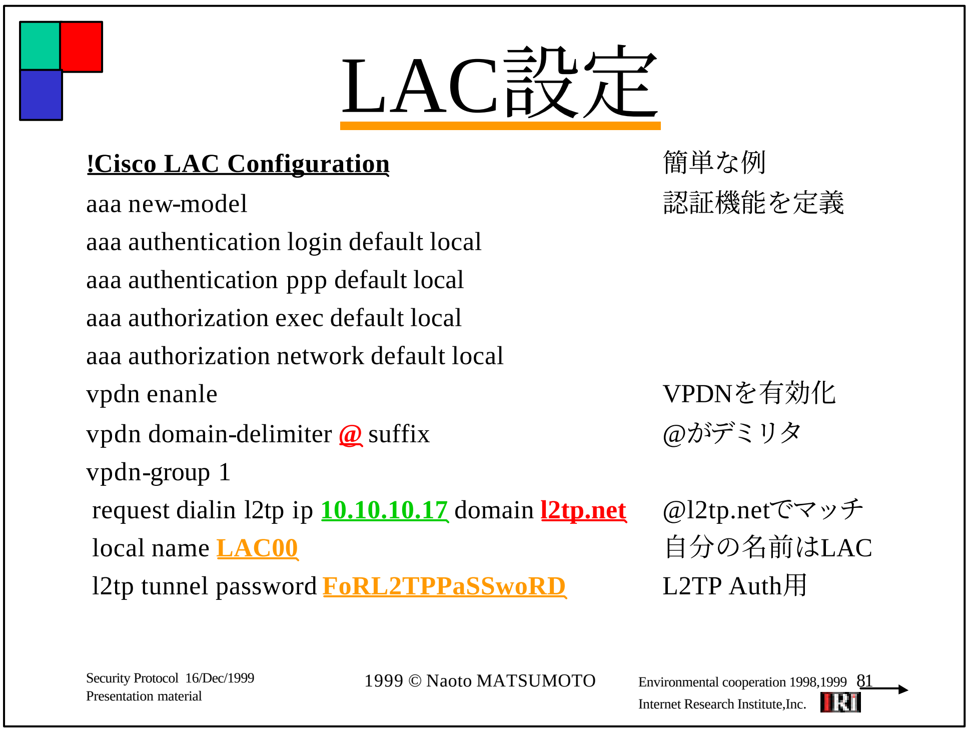
L2TPには、暗号化アルゴリズムは
含まれていない

では…

1.PPP Encryption (Layer 2 Encryption)

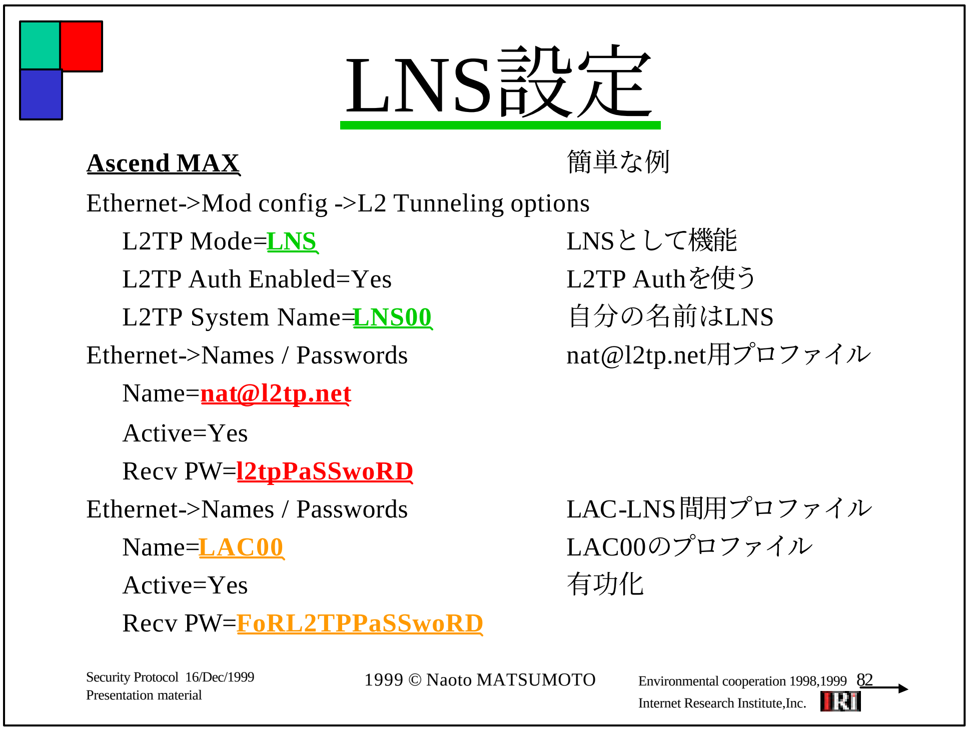
2.IPsec (Layer 3 Encryption)

3.Application Layer Encryption



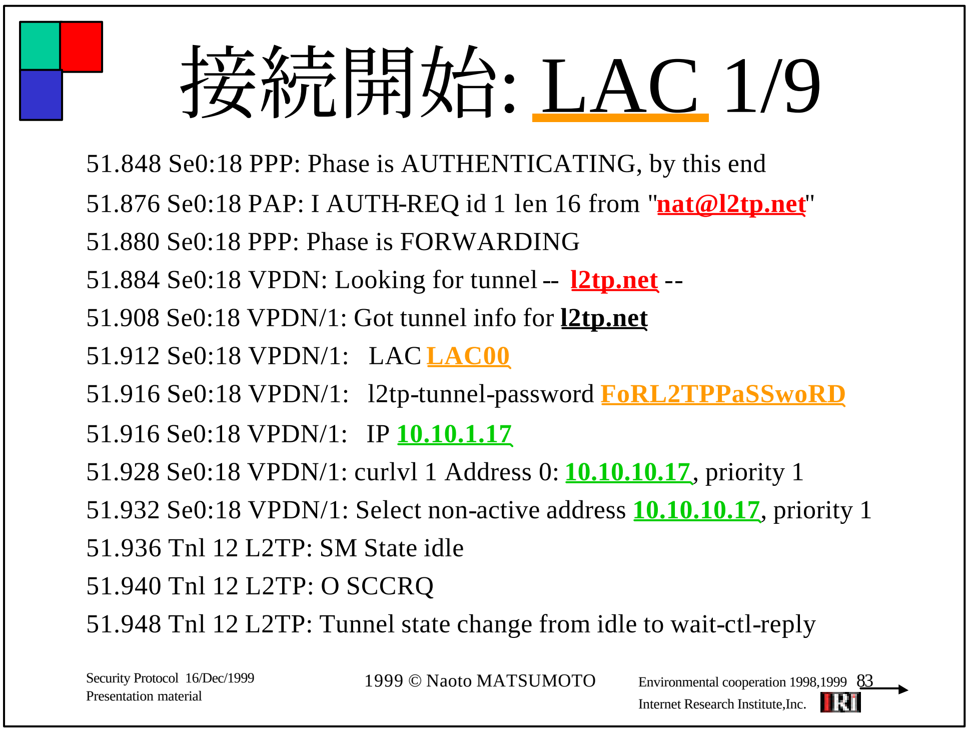
LAC設定

```
!Cisco LAC Configuration                                 簡単な例
aaa new-model                                            認証機能を定義
aaa authentication login default local
aaa authentication ppp default local
aaa authorization exec default local
aaa authorization network default local
vpdn enanle                                              VPDNを有効化
vpdn domain-delimiter @ suffix                           @がデミリタ
vpdn-group 1
 request dialin l2tp ip 10.10.10.17 domain l2tp.net      @l2tp.netでマッチ
 local name LAC00                                        自分の名前はLAC
 l2tp tunnel password FoRL2TPPaSSwoRD                    L2TP Auth用
```



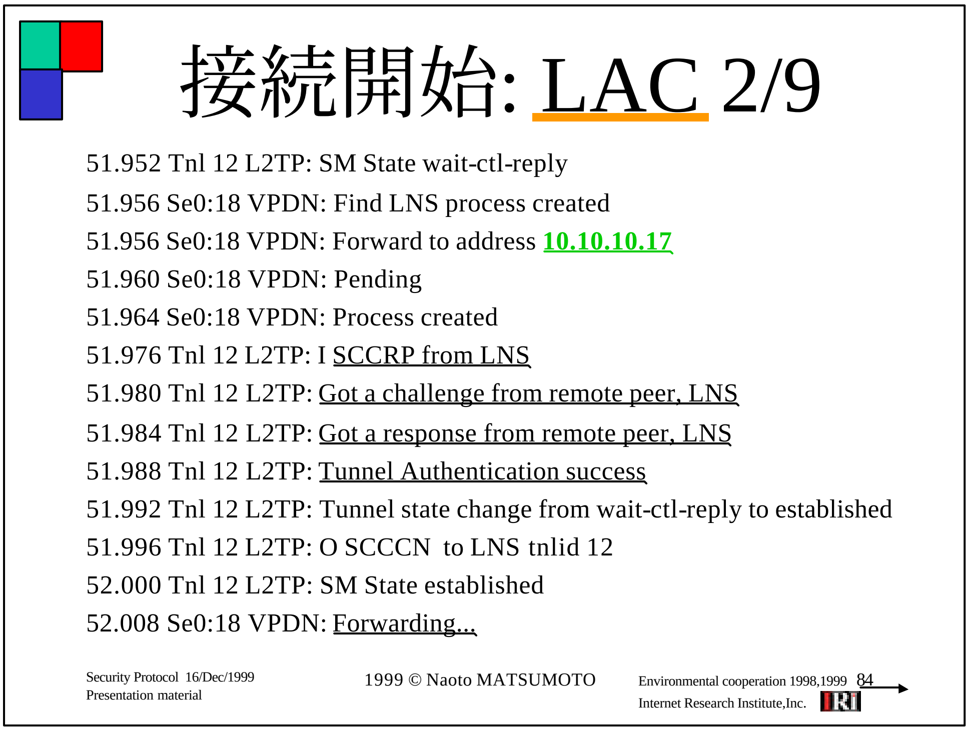
LNS設定

```
Ascend MAX                                        簡単な例
Ethernet->Mod config ->L2 Tunneling options
   L2TP Mode=LNS                                  LNSとして機能
   L2TP Auth Enabled=Yes                          L2TP Authを使う
   L2TP System Name=LNS00                         自分の名前はLNS
Ethernet->Names / Passwords                       nat@l2tp.net用プロファイル
   Name=nat@l2tp.net
   Active=Yes
   Recv PW=l2tpPaSSwoRD
Ethernet->Names / Passwords                       LAC-LNS間用プロファイル
   Name=LAC00                                     LAC00のプロファイル
   Active=Yes                                     有功化
   Recv PW=FoRL2TPPaSSwoRD
```



接続開始: LAC 1/9

```
51.848 Se0:18 PPP: Phase is AUTHENTICATING, by this end
51.876 Se0:18 PAP: I AUTH-REQ id 1 len 16 from "nat@l2tp.net"
51.880 Se0:18 PPP: Phase is FORWARDING
51.884 Se0:18 VPDN: Looking for tunnel -- l2tp.net --
51.908 Se0:18 VPDN/1: Got tunnel info for l2tp.net
51.912 Se0:18 VPDN/1:   LAC LAC00
51.916 Se0:18 VPDN/1:   l2tp-tunnel-password FoRL2TPPaSSwoRD
51.916 Se0:18 VPDN/1:   IP 10.10.1.17
51.928 Se0:18 VPDN/1: curlvl 1 Address 0: 10.10.10.17, priority 1
51.932 Se0:18 VPDN/1: Select non-active address 10.10.10.17, priority 1
51.936 Tnl 12 L2TP: SM State idle
51.940 Tnl 12 L2TP: O SCCRQ
51.948 Tnl 12 L2TP: Tunnel state change from idle to wait-ctl-reply
```



接続開始: LAC 2/9

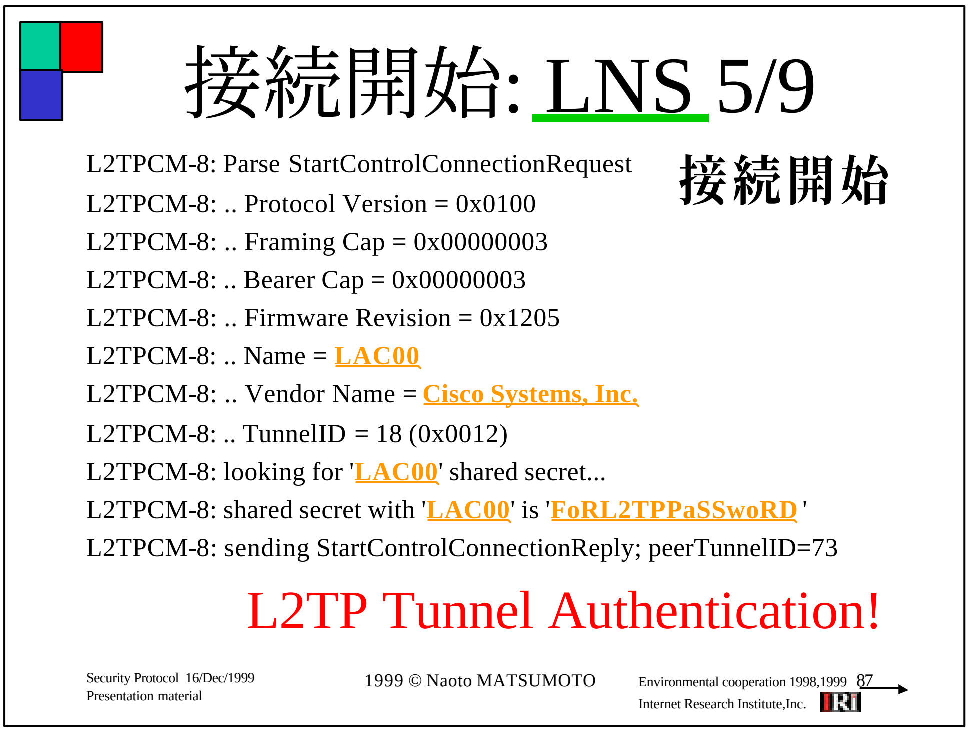
```
51.952 Tnl 12 L2TP: SM State wait-ctl-reply
51.956 Se0:18 VPDN: Find LNS process created
51.956 Se0:18 VPDN: Forward to address 10.10.10.17
51.960 Se0:18 VPDN: Pending
51.964 Se0:18 VPDN: Process created
51.976 Tnl 12 L2TP: I SCCRP from LNS
51.980 Tnl 12 L2TP: Got a challenge from remote peer, LNS
51.984 Tnl 12 L2TP: Got a response from remote peer, LNS
51.988 Tnl 12 L2TP: Tunnel Authentication success
51.992 Tnl 12 L2TP: Tunnel state change from wait-ctl-reply to established
51.996 Tnl 12 L2TP: O SCCCN  to LNS tnlid 12
52.000 Tnl 12 L2TP: SM State established
52.008 Se0:18 VPDN: Forwarding...
```

接続開始: LAC 3/9

```
52.012 Se0:18 VPDN: Bind interface direction=1
52.016 Tnl/Cl 12/12 L2TP: Session sequencing disabled
52.020 Tnl/Cl 12/12 L2TP: Session FS enabled
52.024 Tnl/Cl 12/12 L2TP: Session state change from idle to wait-for-tunnel
52.028 Se0:18 Tnl/Cl 12/12 L2TP: Create session
52.032 Tnl 12 L2TP: SM State established
52.036 Se0:18 Tnl/Cl 12/12 L2TP: O ICRQ to LNS 12/0
52.044 Se0:18 Tnl/Cl 12/12 L2TP: Session state change from wait-for-tunnel
                                        to wait-reply
52.048 Se0:18 VPDN: nat@l2tp.net is forwarded
52.088 Se0:18 Tnl/Cl 12/12 L2TP: O ICCN to LNS 12/1
```

接続開始: LAC 4/9

```
52.096 Se0:18 Tnl/Cl 12/12 L2TP: Session state change from wait-reply
                                        to established
53.048 %LINEPROTO-5-UPDOWN: Line protocol on Interface
                                        Serial0:18, changed state to up
57.324 %ISDN-6-CONNECT: Interface Serial0:18 is now connected to
                                        03540#98## not@l2tp.net
```

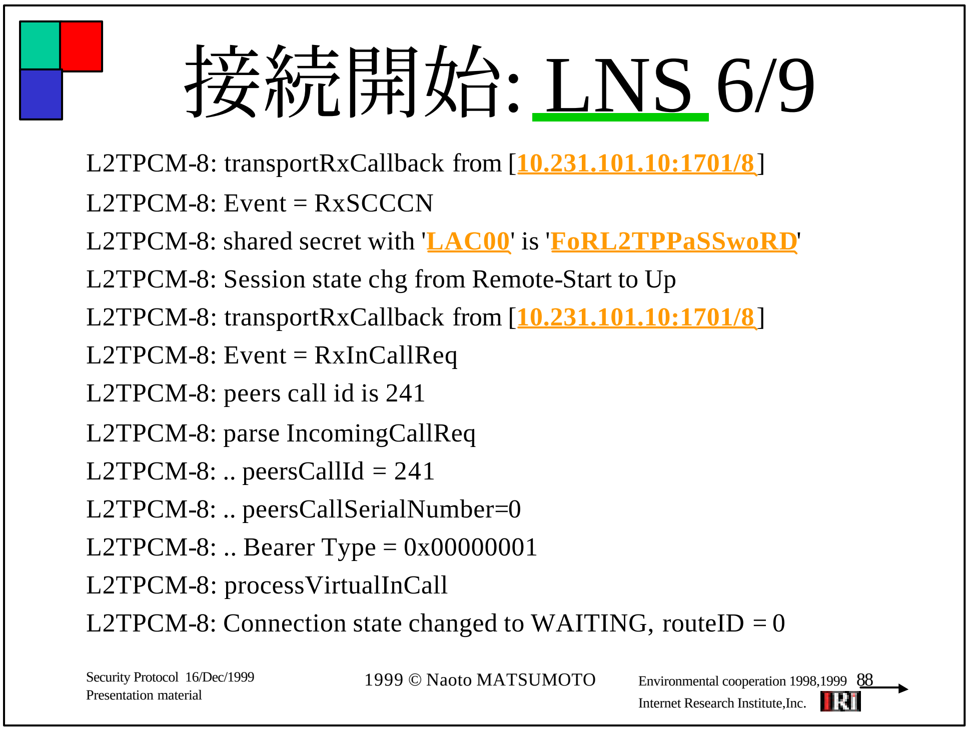


接続開始: LNS 5/9

接続開始

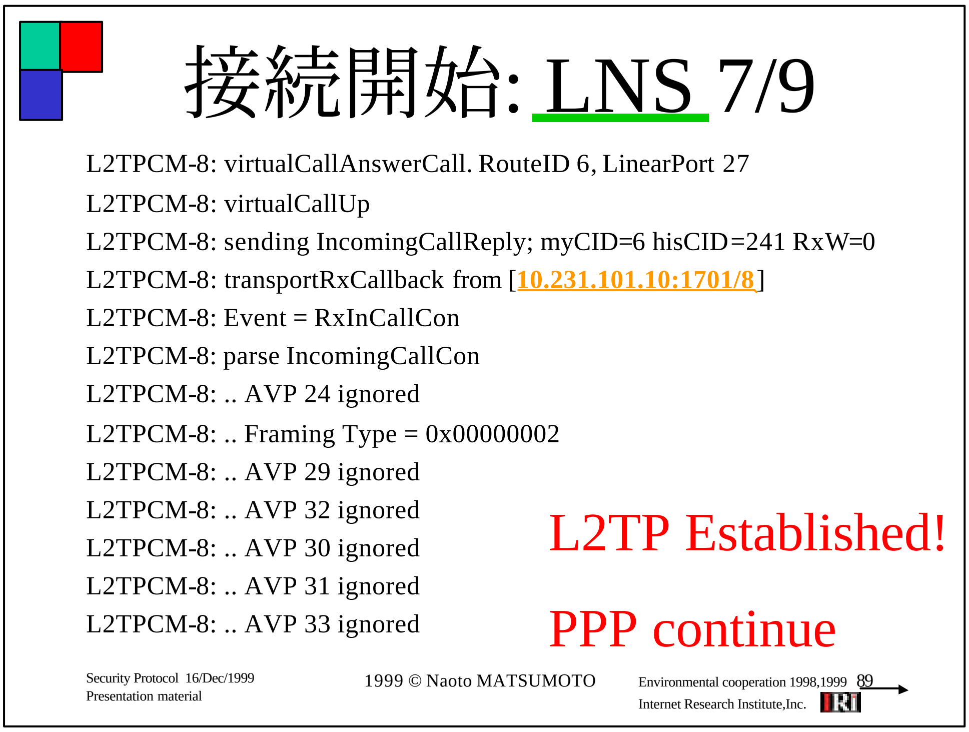
```
L2TPCM-8: Parse StartControlConnectionRequest
L2TPCM-8: .. Protocol Version = 0x0100
L2TPCM-8: .. Framing Cap = 0x00000003
L2TPCM-8: .. Bearer Cap = 0x00000003
L2TPCM-8: .. Firmware Revision = 0x1205
L2TPCM-8: .. Name = LAC00
L2TPCM-8: .. Vendor Name = Cisco Systems, Inc.
L2TPCM-8: .. TunnelID = 18 (0x0012)
L2TPCM-8: looking for 'LAC00' shared secret...
L2TPCM-8: shared secret with 'LAC00' is 'FoRL2TPPaSSwoRD '
L2TPCM-8: sending StartControlConnectionReply; peerTunnelID=73
```

L2TP Tunnel Authentication!



接続開始: LNS 6/9

```
L2TPCM-8: transportRxCallback from [10.231.101.10:1701/8]
L2TPCM-8: Event = RxSCCCN
L2TPCM-8: shared secret with 'LAC00' is 'FoRL2TPPaSSwoRD'
L2TPCM-8: Session state chg from Remote-Start to Up
L2TPCM-8: transportRxCallback from [10.231.101.10:1701/8]
L2TPCM-8: Event = RxInCallReq
L2TPCM-8: peers call id is 241
L2TPCM-8: parse IncomingCallReq
L2TPCM-8: .. peersCallId = 241
L2TPCM-8: .. peersCallSerialNumber=0
L2TPCM-8: .. Bearer Type = 0x00000001
L2TPCM-8: processVirtualInCall
L2TPCM-8: Connection state changed to WAITING, routeID = 0
```

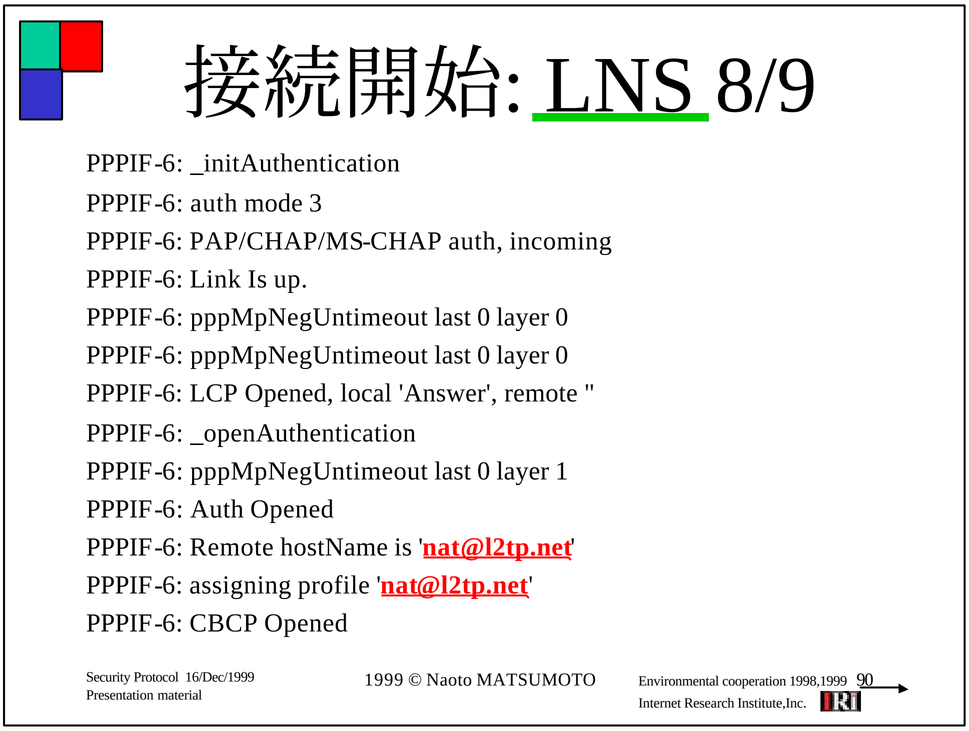


接続開始: LNS 7/9

```
L2TPCM-8: virtualCallAnswerCall. RouteID 6, LinearPort 27
L2TPCM-8: virtualCallUp
L2TPCM-8: sending IncomingCallReply; myCID=6 hisCID=241 RxW=0
L2TPCM-8: transportRxCallback from [10.231.101.10:1701/8]
L2TPCM-8: Event = RxInCallCon
L2TPCM-8: parse IncomingCallCon
L2TPCM-8: .. AVP 24 ignored
L2TPCM-8: .. Framing Type = 0x00000002
L2TPCM-8: .. AVP 29 ignored
L2TPCM-8: .. AVP 32 ignored
L2TPCM-8: .. AVP 30 ignored
L2TPCM-8: .. AVP 31 ignored
L2TPCM-8: .. AVP 33 ignored
```

L2TP Established!

PPP continue



接続開始: LNS 8/9

```
PPPIF-6: _initAuthentication
PPPIF-6: auth mode 3
PPPIF-6: PAP/CHAP/MS-CHAP auth, incoming
PPPIF-6: Link Is up.
PPPIF-6: pppMpNegUntimeout last 0 layer 0
PPPIF-6: pppMpNegUntimeout last 0 layer 0
PPPIF-6: LCP Opened, local 'Answer', remote ''
PPPIF-6: _openAuthentication
PPPIF-6: pppMpNegUntimeout last 0 layer 1
PPPIF-6: Auth Opened
PPPIF-6: Remote hostName is 'nat@l2tp.net'
PPPIF-6: assigning profile 'nat@l2tp.net'
PPPIF-6: CBCP Opened
```

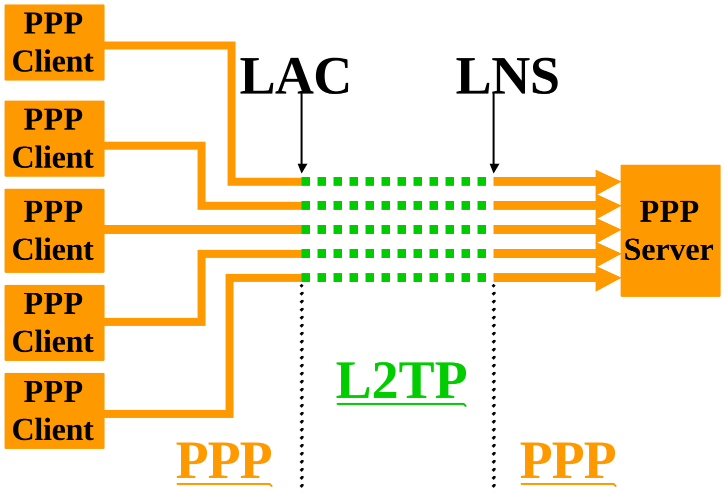
接続開始: LNS 9/9

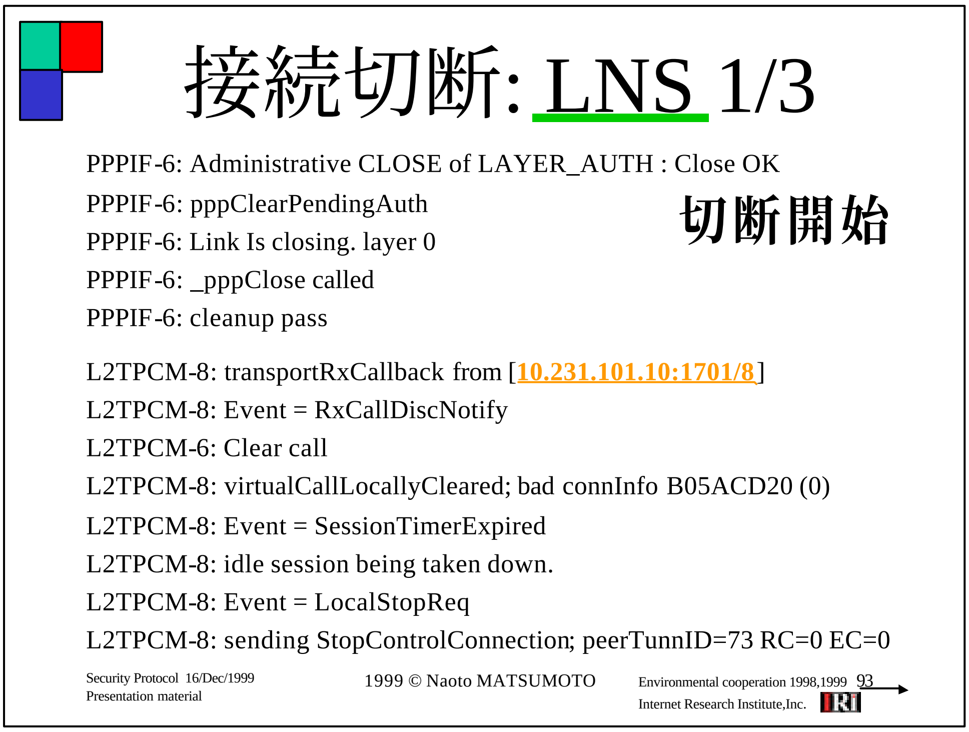
接続完了

```
PPPIF-6: pppMpSendNeg Pkt
PPPIF-6: pppMpNegTimeout layer 4
PPPIF-6: vj comp on
PPPIF-6: using address from pool 0
PPPIF-6: Allocated address [10.10.10.162]
PPPIF-6: opening IPNCP: 10.10.10.17 -> 10.10.10.162
PPPIF-6: pppMpSendNeg Pkt
PPPIF-6: pppMpNegUntimeout last 0 layer 4
PPPIF-6: pppMpSendNeg Pkt
PPPIF-6: pppMpSendNeg Pkt
PPPIF-6: pppMpNegUntimeout last 0 layer 4
PPPIF-6: IPNCP Opened to 10.10.10.162
```

PPP CONNECT!

L2TP網の状態

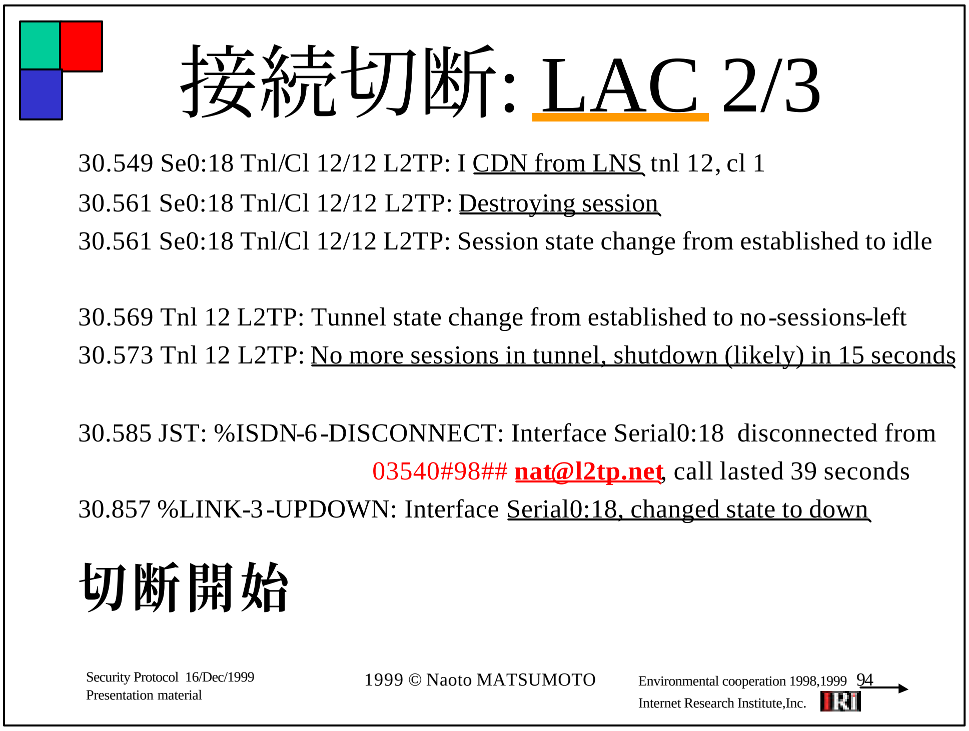




接続切断: LNS 1/3

```
PPPIF-6: Administrative CLOSE of LAYER_AUTH : Close OK
PPPIF-6: pppClearPendingAuth
PPPIF-6: Link Is closing. layer 0
PPPIF-6: _pppClose called
PPPIF-6: cleanup pass

L2TPCM-8: transportRxCallback from [10.231.101.10:1701/8]
L2TPCM-8: Event = RxCallDiscNotify
L2TPCM-6: Clear call
L2TPCM-8: virtualCallLocallyCleared; bad connInfo B05ACD20 (0)
L2TPCM-8: Event = SessionTimerExpired
L2TPCM-8: idle session being taken down.
L2TPCM-8: Event = LocalStopReq
L2TPCM-8: sending StopControlConnection; peerTunnID=73 RC=0 EC=0
```

切断開始



接続切断: LAC 2/3

```
30.549 Se0:18 Tnl/Cl 12/12 L2TP: I CDN from LNS tnl 12, cl 1
30.561 Se0:18 Tnl/Cl 12/12 L2TP: Destroying session
30.561 Se0:18 Tnl/Cl 12/12 L2TP: Session state change from established to idle

30.569 Tnl 12 L2TP: Tunnel state change from established to no-sessions-left
30.573 Tnl 12 L2TP: No more sessions in tunnel, shutdown (likely) in 15 seconds

30.585 JST: %ISDN-6-DISCONNECT: Interface Serial0:18  disconnected from
                          03540#98## nat@l2tp.net, call lasted 39 seconds
30.857 %LINK-3-UPDOWN: Interface Serial0:18, changed state to down
```

切断開始

接続切断: LAC 3/3

切断完了

```
30.889 Se0:18 PPP: Phase is TERMINATING
30.893 Se0:18 LCP: State is Closed
30.893 Se0:18 PPP: Phase is DOWN
30.897 Se0:18 VPDN: Cleanup
30.897 Se0:18 VPDN: Reset
30.901 Se0:18 VPDN: Unbind interface
31.857 %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0 :18,
    changed state to down

45.580 Tnl 12 L2TP: O StopCCN  to LNS tnlid 12
45.588 Tnl 12 L2TP: Tunnel state change from no-sessions-left to shutting-down
45.596 Tnl 12 L2TP: Shutdown tunnel
45.596 Tnl 12 L2TP: Tunnel state change from shutting-down to idle
```

L2TP Debug Ascend

```
> l2tpcm
L2TPCM debug is now ON
> pppif
PPPIF debug is ON

> pppif
PPPIF debug is OFF
> l2tpcm
L2TPCM debug is now OFF
```

L2TP Debug Cisco

```
L2tp-router#debug vpdn ?
  error          VPDN Protocol errors
  event          VPDN event
  l2tp-sequencing  L2TP sequencing
  l2x-data       L2F/L2TP data packets
  l2x-errors     L2F/L2TP protocol errors
  l2x-events     L2F/L2TP protocol events
  l2x-packets    L2F/L2TP control packets
  packet         VPDN packet
```

L2TP相互接続

LAC \ LNS	3Com	Ascend	Cisco	Nortel
3Com	○	○	○	○
Ascend	○	○	○	○
Cisco	未確認	○	○	○

○ 接続確認

VPN Operators Workshop [01]
L2TP(Layer 2 Tunneling Protocol) Interoperability Test 1999/Apr/19-21 (3days)

RADIUSとL2TP

LACにおけるRADIUSとの連携(例 Cisco)

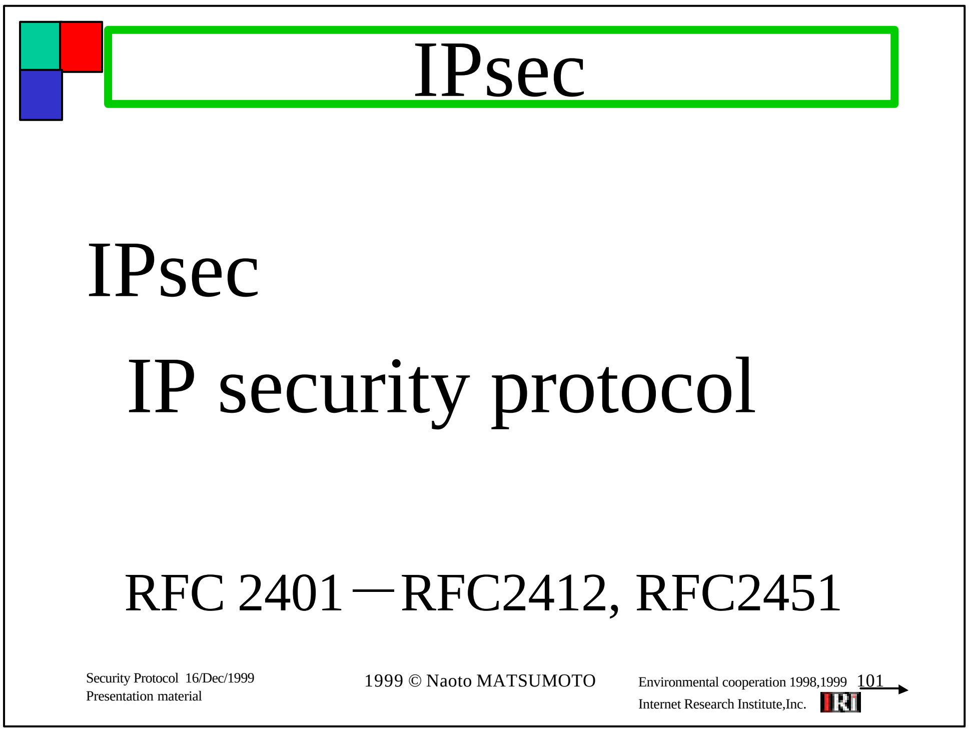
```
l2tp.net
        Service-Type = Outbound,
        Cisco:Cisco-Avpair="service=ppp",
        Cisco:Cisco-Avpair="protocol=vpdn",
        Cisco:Cisco-Avpair="vpdn:tunnel-id=l2tp-net-tunnel",
        Cisco:Cisco-Avpair="vpdn:tunnel-type=l2tp",
        Cisco:Cisco-Avpair="vpdn:l2tp-tunnel-password=secret",
        Cisco:Cisco-Avpair="vpdn:ip-addresses=10.10.10.17"
```

L2TPまとめ [確認]

L2TP ＝ PPP over IP

L2TP ≠暗号化

L2TP ＝Tunneling



IPsec

IPsec

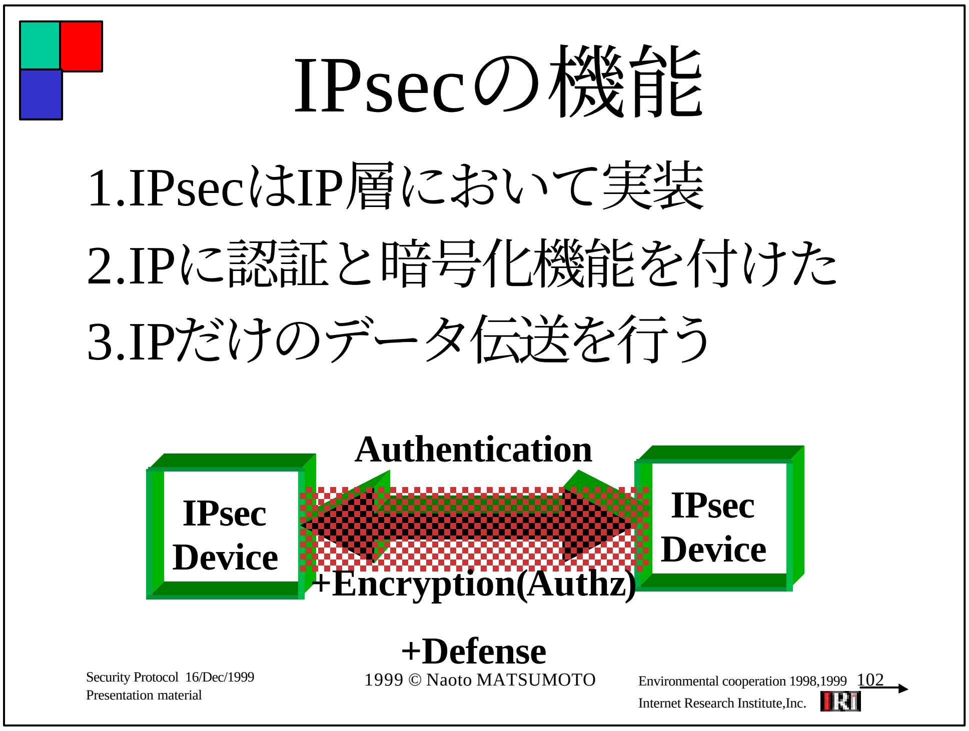
IP security protocol

RFC 2401－RFC2412, RFC2451

Security Protocol 16/Dec/1999
Presentation material

1999 © Naoto MATSUMOTO

Environmental cooperation 1998,1999 101
Internet Research Institute,Inc.



IPsecの機能

1.IPsecはIP層において実装

2.IPに認証と暗号化機能を付けた

3.IPだけのデータ伝送を行う

Authentication

IPsec Device

IPsec Device

+Encryption(Authz)

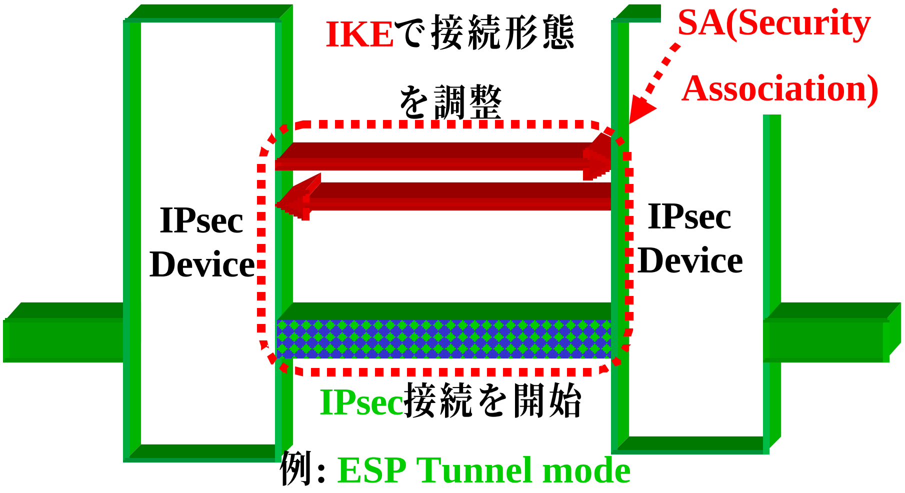
+Defense

Security Protocol 16/Dec/1999
Presentation material

1999 © Naoto MATSUMOTO

Environmental cooperation 1998,1999 102
Internet Research Institute,Inc.

IPsec接続



この状態が

SA(Security Association)

IKEで接続形態を調整

IPsec Device

IPsec Device

IPsec接続を開始

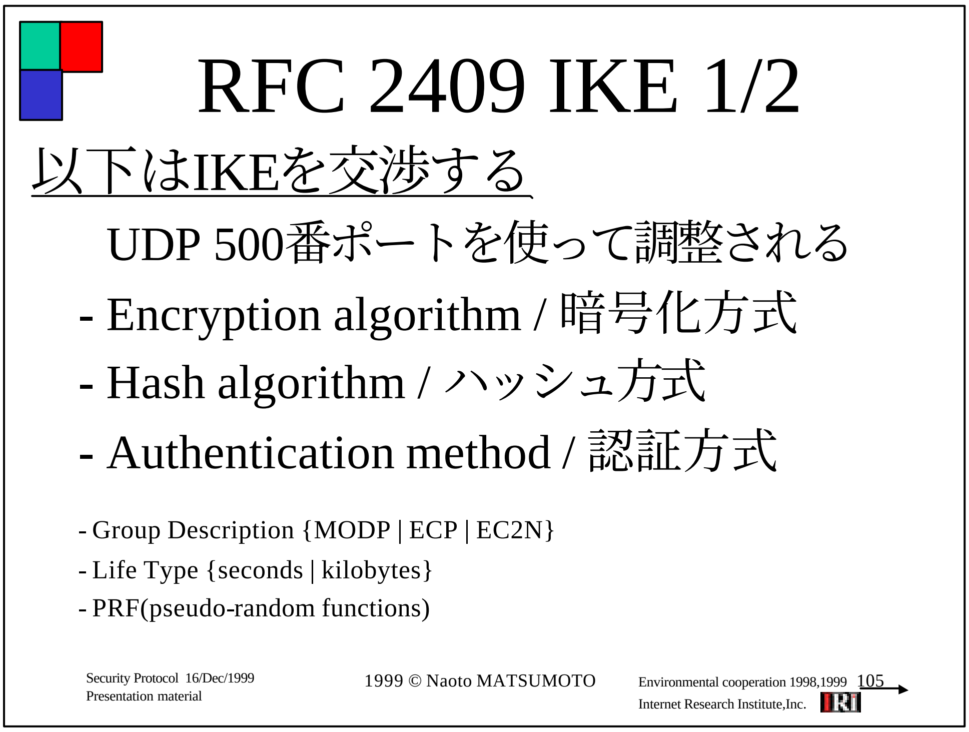
例: ESP Tunnel mode

IPsecのしくみ

1.IKE

2.AH {Transport | Tunnel mode}

3.ESP {Transport | Tunnel mode}



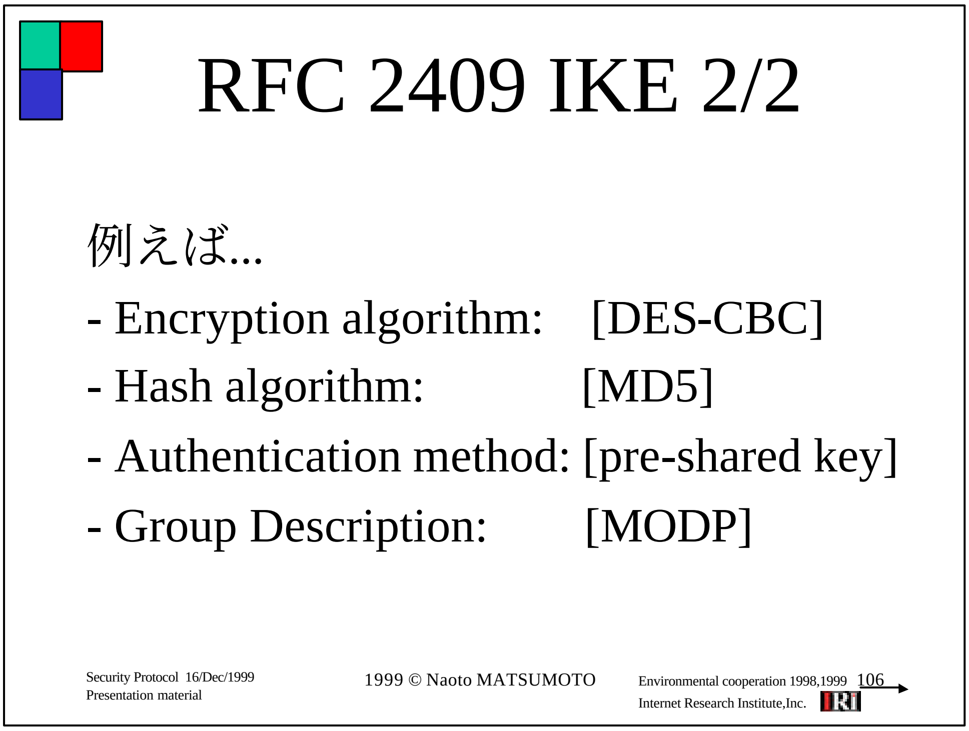
RFC 2409 IKE 1/2

以下はIKEを交渉する

UDP 500番ポートを使って調整される

- Encryption algorithm / 暗号化方式
- Hash algorithm / ハッシュ方式
- Authentication method / 認証方式

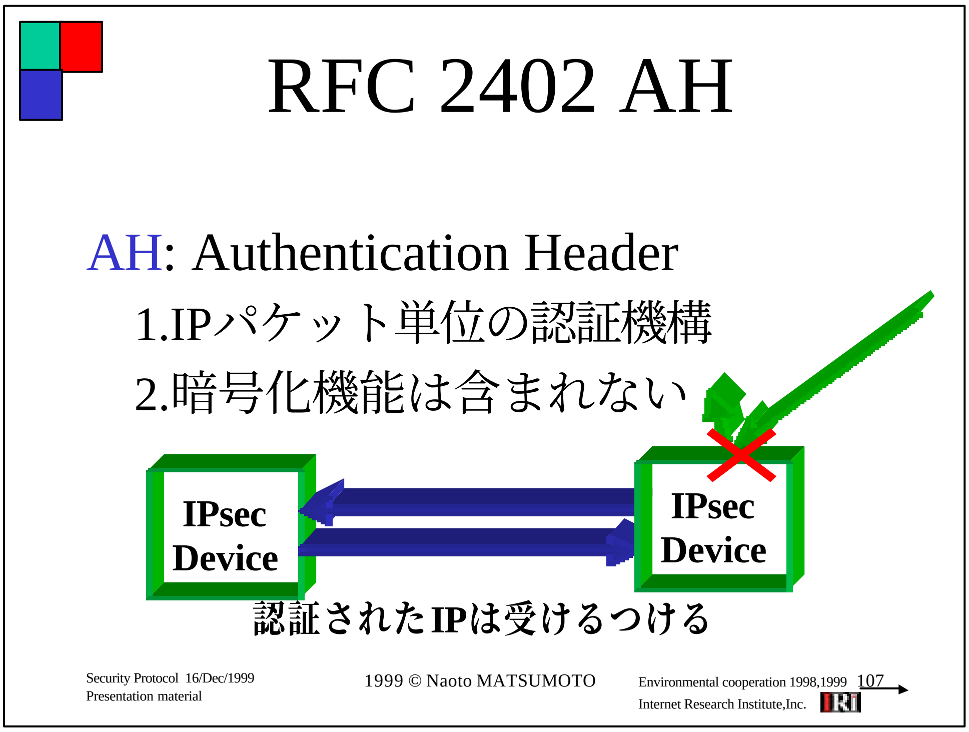
- Group Description {MODP | ECP | EC2N}
- Life Type {seconds | kilobytes}
- PRF(pseudo-random functions)



RFC 2409 IKE 2/2

例えば...

- Encryption algorithm: [DES-CBC]
- Hash algorithm: [MD5]
- Authentication method: [pre-shared key]
- Group Description: [MODP]



RFC 2402 AH

AH: Authentication Header

1.IPパケット単位の認証機構

2.暗号化機能は含まれない

IPsec Device

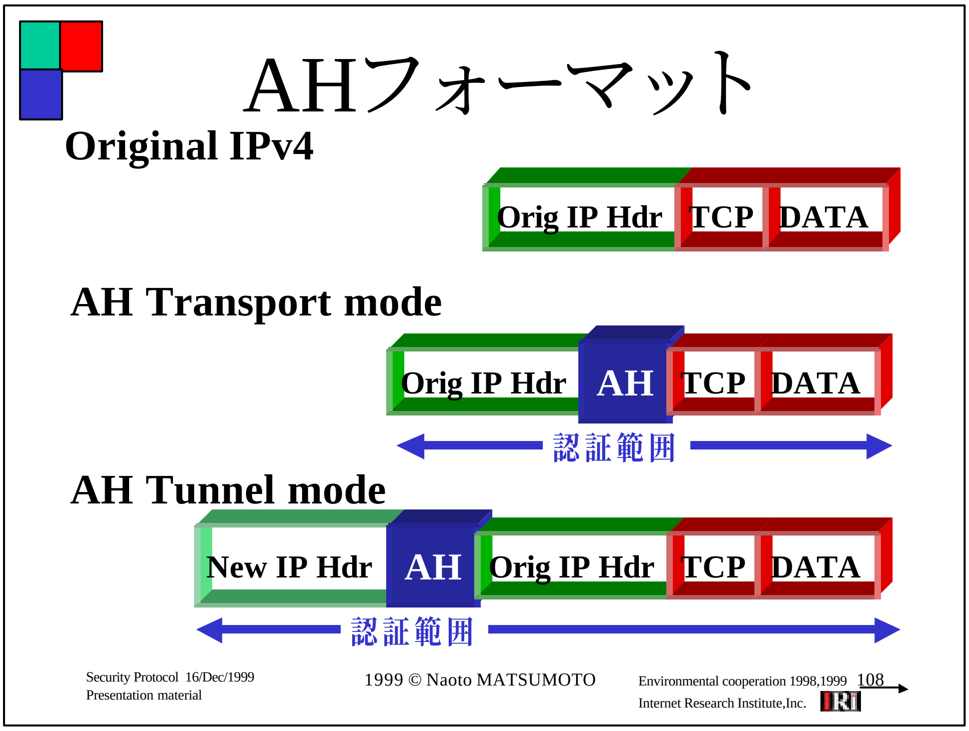
IPsec Device

認証されたIPは受けるつける

Security Protocol 16/Dec/1999
Presentation material

1999 © Naoto MATSUMOTO

Environmental cooperation 1998,1999 107
Internet Research Institute,Inc.



AHフォーマット

Original IPv4

Orig IP Hdr | TCP | DATA

AH Transport mode

Orig IP Hdr | AH | TCP | DATA

認証範囲

AH Tunnel mode

New IP Hdr | AH | Orig IP Hdr | TCP | DATA

認証範囲

Security Protocol 16/Dec/1999
Presentation material

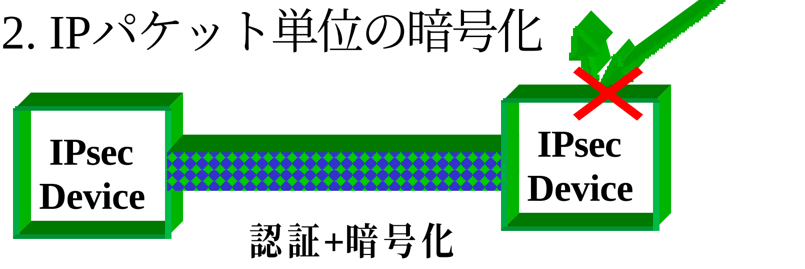
1999 © Naoto MATSUMOTO

Environmental cooperation 1998,1999 108
Internet Research Institute,Inc.

RFC 2406 ESP

ESP: Encapsulating Security Payload

1. IPパケット単位の認証機構
2. IPパケット単位の暗号化



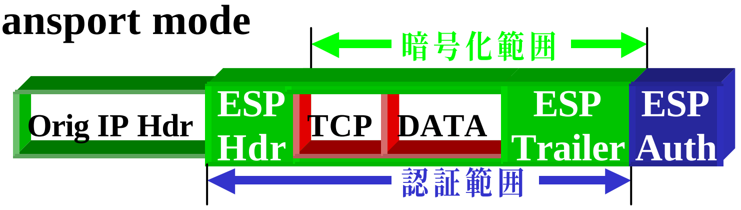
Security Protocol 16/Dec/1999
Presentation material

1999 © Naoto MATSUMOTO

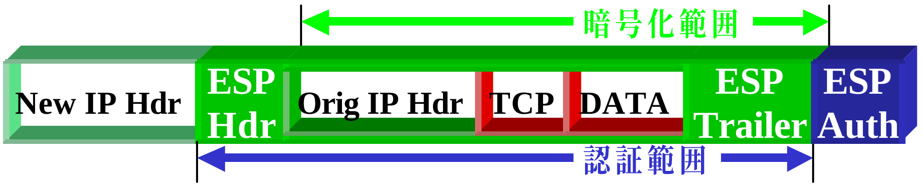
Environmental cooperation 1998,1999 109
Internet Research Institute,Inc.

ESPフォーマット

ESP Transport mode



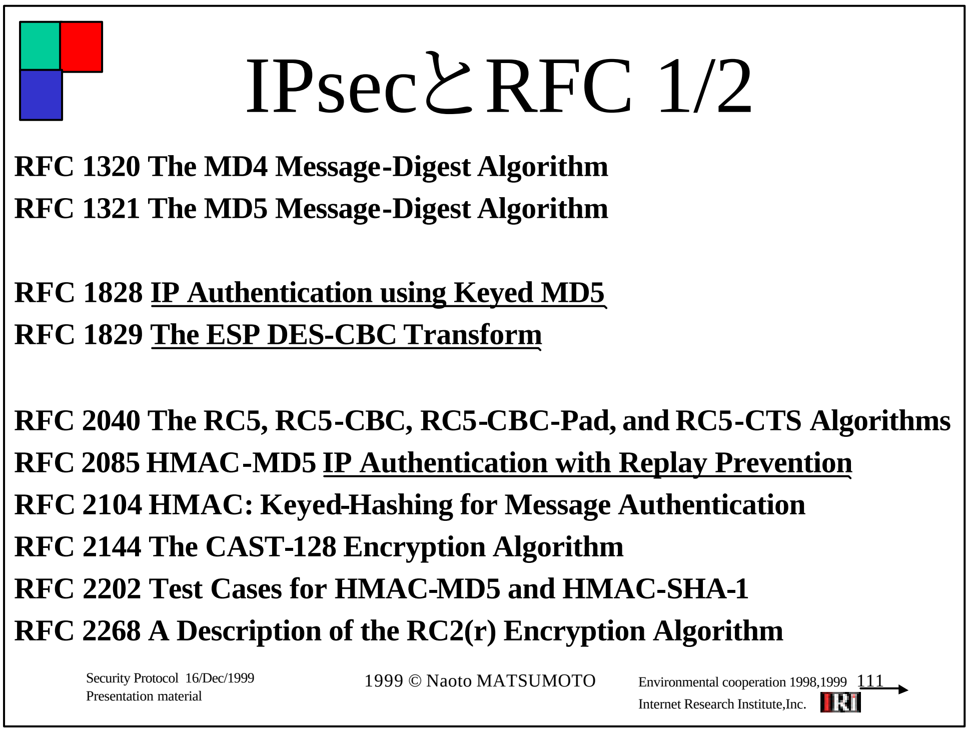
ESP Tunnel mode



Security Protocol 16/Dec/1999
Presentation material

1999 © Naoto MATSUMOTO

Environmental cooperation 1998,1999 110
Internet Research Institute,Inc.

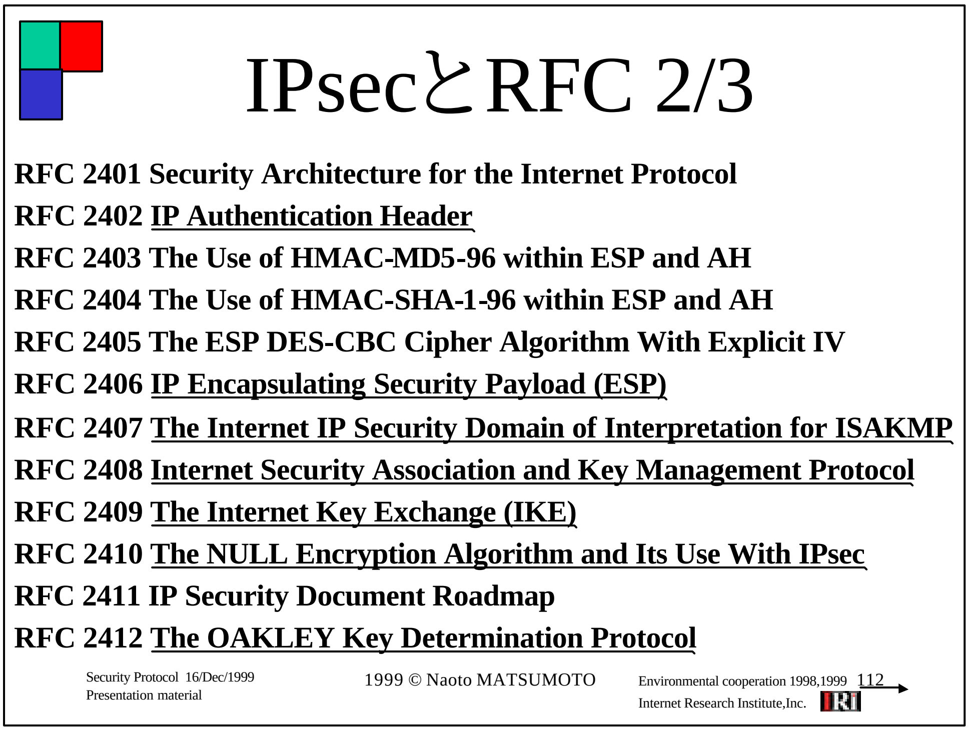


IPsecとRFC 1/2

RFC 1320 The MD4 Message-Digest Algorithm
RFC 1321 The MD5 Message-Digest Algorithm

RFC 1828 IP Authentication using Keyed MD5
RFC 1829 The ESP DES-CBC Transform

RFC 2040 The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms
RFC 2085 HMAC-MD5 IP Authentication with Replay Prevention
RFC 2104 HMAC: Keyed-Hashing for Message Authentication
RFC 2144 The CAST-128 Encryption Algorithm
RFC 2202 Test Cases for HMAC-MD5 and HMAC-SHA-1
RFC 2268 A Description of the RC2(r) Encryption Algorithm



IPsecとRFC 2/3

RFC 2401 Security Architecture for the Internet Protocol
RFC 2402 IP Authentication Header
RFC 2403 The Use of HMAC-MD5-96 within ESP and AH
RFC 2404 The Use of HMAC-SHA-1-96 within ESP and AH
RFC 2405 The ESP DES-CBC Cipher Algorithm With Explicit IV
RFC 2406 IP Encapsulating Security Payload (ESP)
RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP
RFC 2408 Internet Security Association and Key Management Protocol
RFC 2409 The Internet Key Exchange (IKE)
RFC 2410 The NULL Encryption Algorithm and Its Use With IPsec
RFC 2411 IP Security Document Roadmap
RFC 2412 The OAKLEY Key Determination Protocol

IPsecとRFC 3/3

RFC 2451 The ESP CBC-Mode Cipher Algorithms
RFC 2631 Diffie-Hellman Key Agreement Method
RFC 2521 <u>ICMP Security Failures Messages</u>
RFC 2522 (E) Photuris: Session-Key Management Protocol
RFC 2523 (E) Photuris: Extended Schemes and Attributes
RFC 2709 <u>Security Model with Tunnel-mode IPsec for NAT Domains</u>

※**<u>Policy Handling RFC = 0</u>**

だいたいがStandards Track

※これ以外に**Interner-Drafts**も多数出ている

IPsecの実装

使われ方は2つ

1.コンセントレータ型

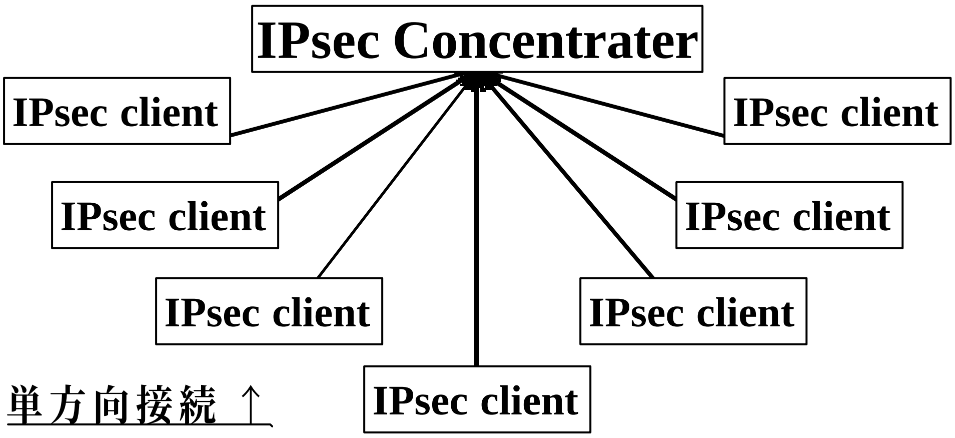
<u>IPsec client ー IPsec concentrator</u>

2.エンドーエンド型

<u>IPsec SGW*1 ー IPsec SGW</u>

(SGW*1 = Security Gateway)

コンセントレータ型IPsec



IPsec Concentrater

IPsec client

IPsec client

IPsec client

IPsec client

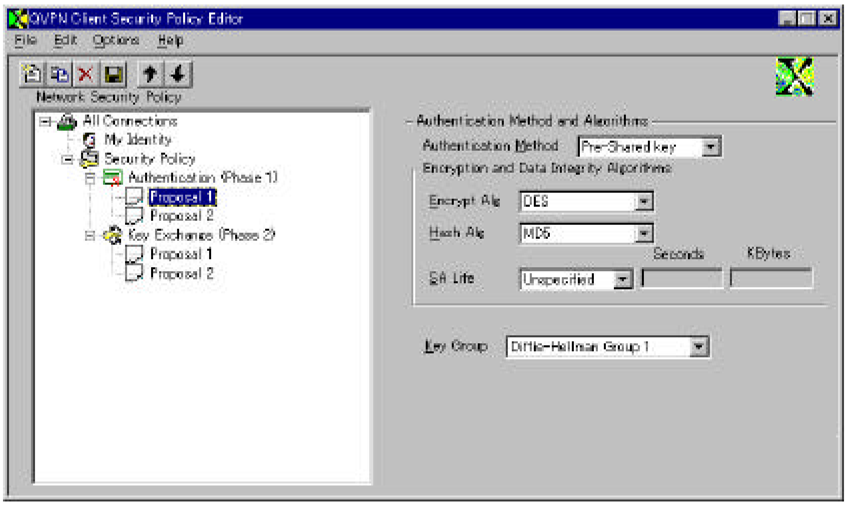
IPsec client

IPsec client

IPsec client

単方向接続 ↑

IPsec client X 1/8



Authentication Method: Pre-Shared key

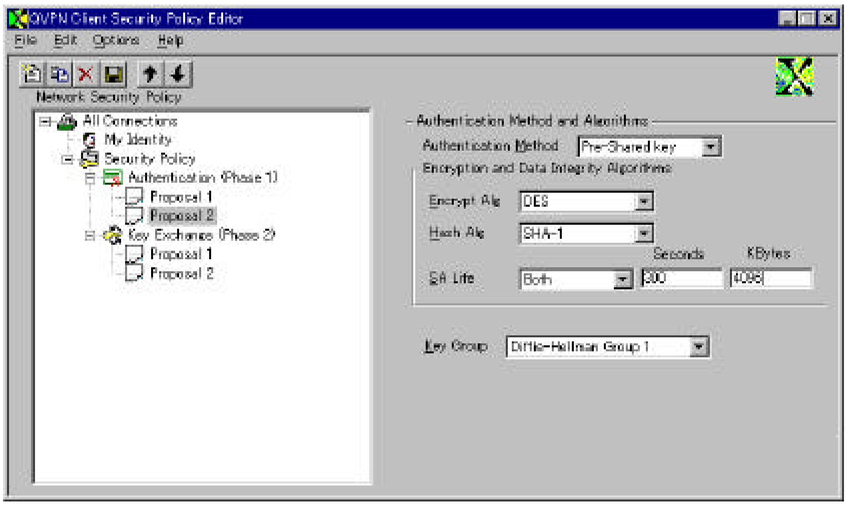
Encrypt Alg: DES

Hash Alg: MD5

SA Life: Unspecified   Seconds   KBytes

Key Group: Diffie-Hellman Group 1

IPsec client X 2/8



Authentication Method and Algorithms

Authentication Method: Pre-Shared key

Encryption and Data Integrity Algorithms

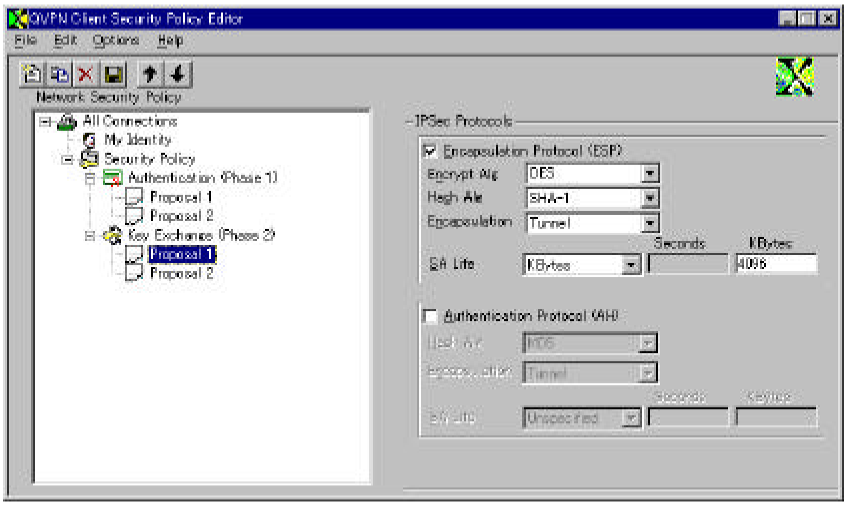
Encrypt Alg: DES

Hash Alg: SHA-1

		Seconds	KBytes
SA Life	Both	300	4096

Key Group: Diffie-Hellman Group 1

IPsec client X 3/8



IPSec Protocols

☑ Encapsulation Protocol (ESP)

Encrypt Alg: DES

Hash Alg: SHA-1

Encapsulation: Tunnel

		Seconds	KBytes
SA Life	KBytes		4096

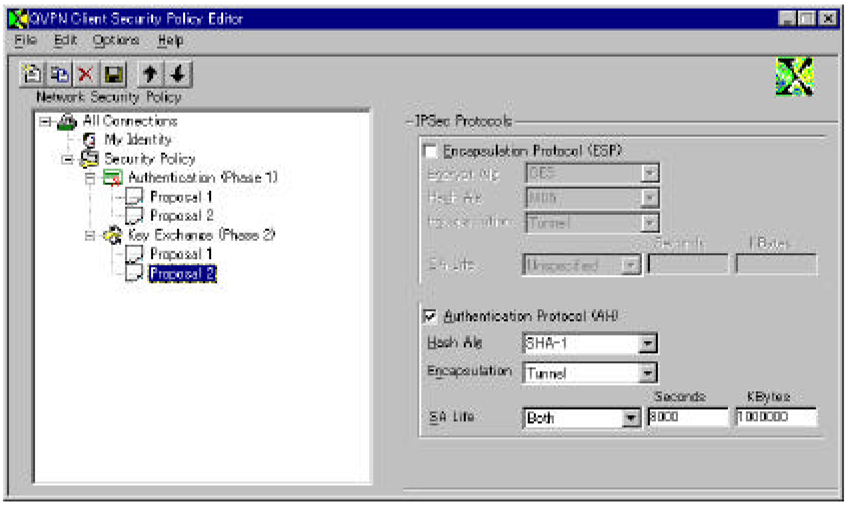
□ Authentication Protocol (AH)

Hash Alg: MD5

Encapsulation: Tunnel

		Seconds	KBytes
SA Life	Unspecified		

IPsec client X 4/8



IPSec Protocols

□ Encapsulation Protocol (ESP)

Encrypt Alg: DES

Hash Alg: MD5

Encapsulation: Tunnel

SA Life: Unspecified — Seconds: — KBytes:

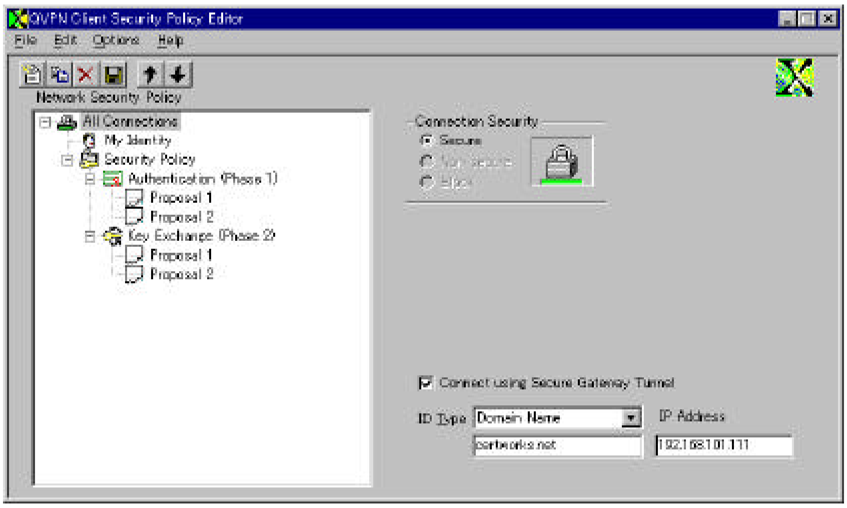
☑ Authentication Protocol (AH)

Hash Alg: SHA-1

Encapsulation: Tunnel

SA Life: Both — Seconds: 8000 — KBytes: 1000000

IPsec client X 5/8



Connection Security

● Secure

○ Non-secure

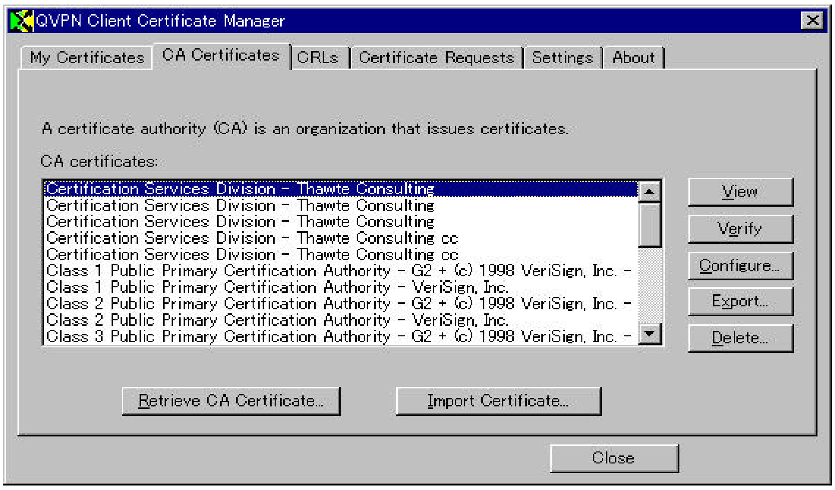
○ Block

☑ Connect using Secure Gateway Tunnel

ID Type: Domain Name — certworks.net

IP Address: 192.168.101.111

IPsec client X 6/8

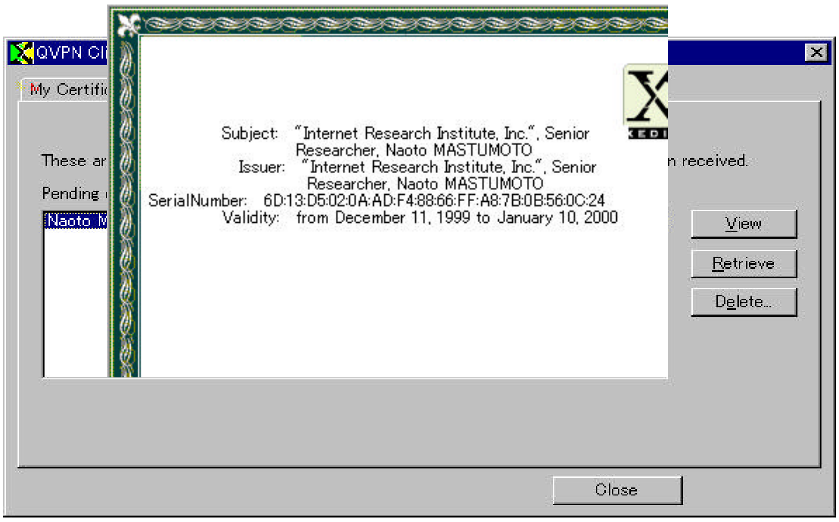


A certificate authority (CA) is an organization that issues certificates.

CA certificates:

```
Certification Services Division - Thawte Consulting
Certification Services Division - Thawte Consulting
Certification Services Division - Thawte Consulting
Certification Services Division - Thawte Consulting cc
Certification Services Division - Thawte Consulting cc
Class 1 Public Primary Certification Authority - G2 + (c) 1998 VeriSign, Inc. -
Class 1 Public Primary Certification Authority - VeriSign, Inc.
Class 2 Public Primary Certification Authority - G2 + (c) 1998 VeriSign, Inc. -
Class 2 Public Primary Certification Authority - VeriSign, Inc.
Class 3 Public Primary Certification Authority - G2 + (c) 1998 VeriSign, Inc. -
```

IPsec client X 7/8



These ar

n received.

Pending

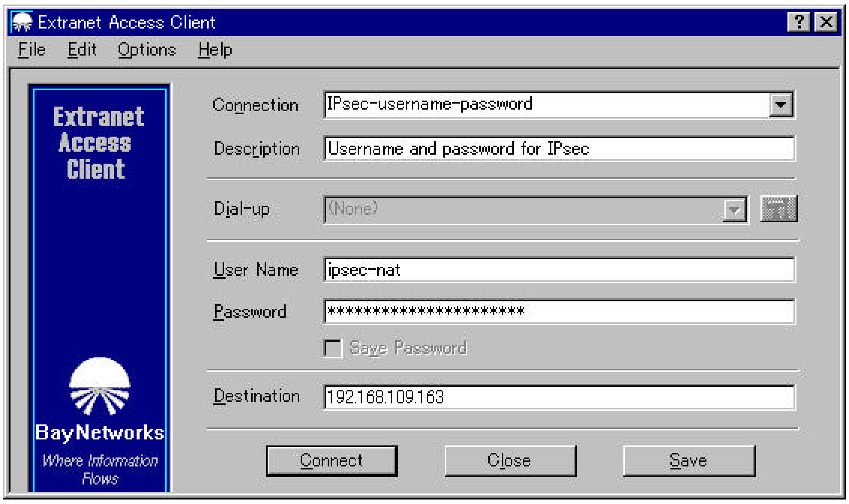
Naoto M

Subject: "Internet Research Institute, Inc.", Senior Researcher, Naoto MASTUMOTO
Issuer: "Internet Research Institute, Inc.", Senior Researcher, Naoto MASTUMOTO
SerialNumber: 6D:13:D5:02:0A:AD:F4:88:66:FF:A8:7B:0B:56:0C:24
Validity: from December 11, 1999 to January 10, 2000

IPsec client X 8/8

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIB3TCCAUYCAQAwYjEqMCgGA1UEChMhSW50ZXJuZXQgUmVzZWFyY2ggSW5zdGl0
dXRlLCBJbmMuMRowGAYDVQQLExFTZW5pb3IgUmVzZWFyY2hlcjEYMBYGA1UEAxMP
TmFvdG8gTUFTVFVNT1RPMIGeMA0GCSqGSIb3DQEBAQUAA4GMADCBiAKBgHwhUsnR
q2P6PGA0UiviV4obYswtuv03r1dhkkYg5Nnbqiyhgviil0LleLUiRJg0KeULKyTc
82x+9Wn0czLq0vvQ0YTrB9YJXxGx0X+rdI63J3CvIBV0CYDU80WKvMoXCdLPd6ti
mU+GRdGJN/o6j12e4VbQMJNZ8PMxm5BL4SKJAgMBAAGgPDA6BgkqhkiG9w0BCQ4x
LTArMCkGA1UdEQQiMCCHBMrubByBDW5vdEBpcmkuY28uanCCCWlyaS5jby5qcDAN
BgkqhkiG9w0BAQQFAA0BgQBYaU1AcQThh5gQ6gySsDjQ4n9/UGibmdad8hSpSC0p
hYsv6FqDmN07zvVRv9PViu87Zdn9Iir24R90tQKY+IGKZixv0XYw8/vAUMB0sNw6
2Ed3ABnJFGHBagZRwyLwuI3vjzmJMbWFKQnSwnTz8E6Eg3bHGrrTqyEKBigu3/db
Pg==
-----END NEW CERTIFICATE REQUEST-----
```

IPsec client N 1/3



Connection: IPsec-username-password

Description: Username and password for IPsec

Dial-up: (None)

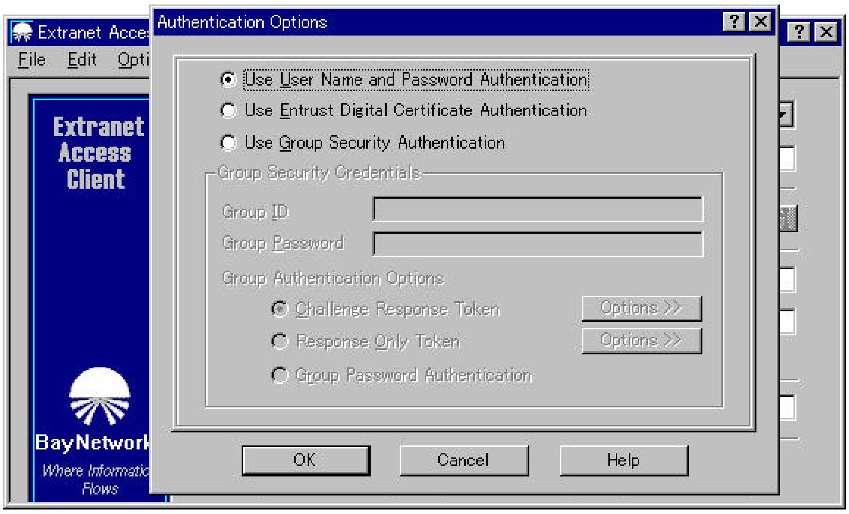
User Name: ipsec-nat

Password: **********************

□ Save Password

Destination: 192.168.109.163

IPsec client N 2/3



Authentication Options

● Use User Name and Password Authentication

○ Use Entrust Digital Certificate Authentication

○ Use Group Security Authentication

Group Security Credentials

Group ID

Group Password

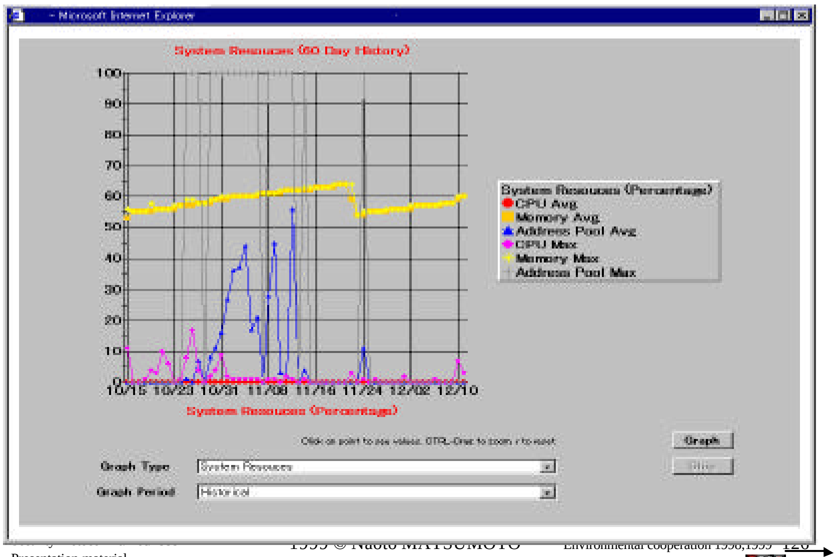
Group Authentication Options

● Challenge Response Token [Options >>]

○ Response Only Token [Options >>]

○ Group Password Authentication

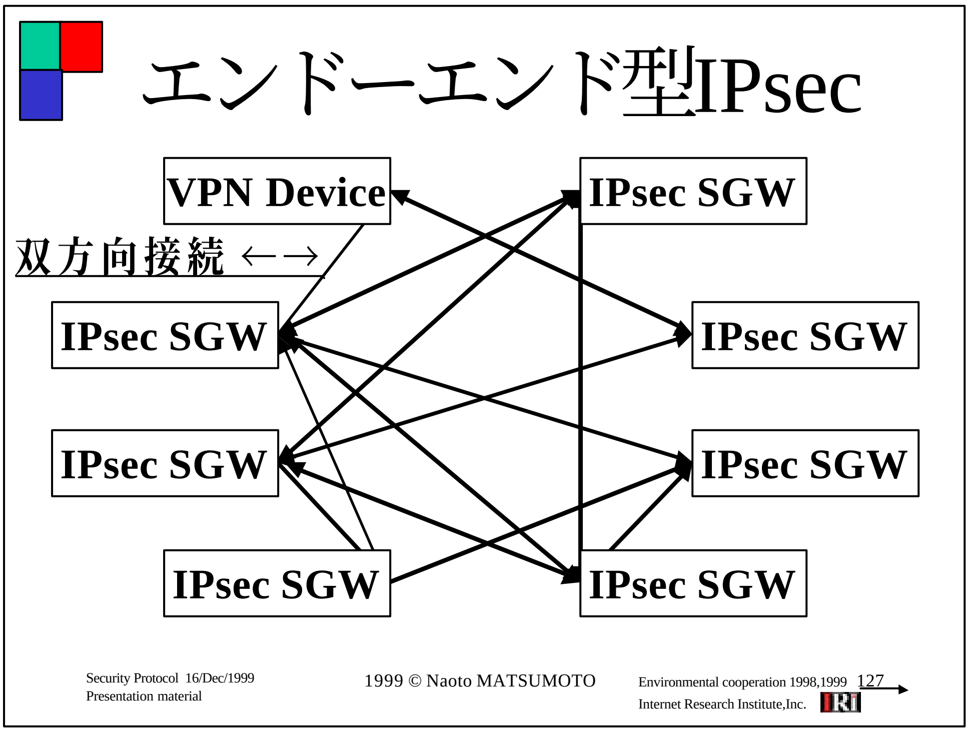
IPsec client N 3/3



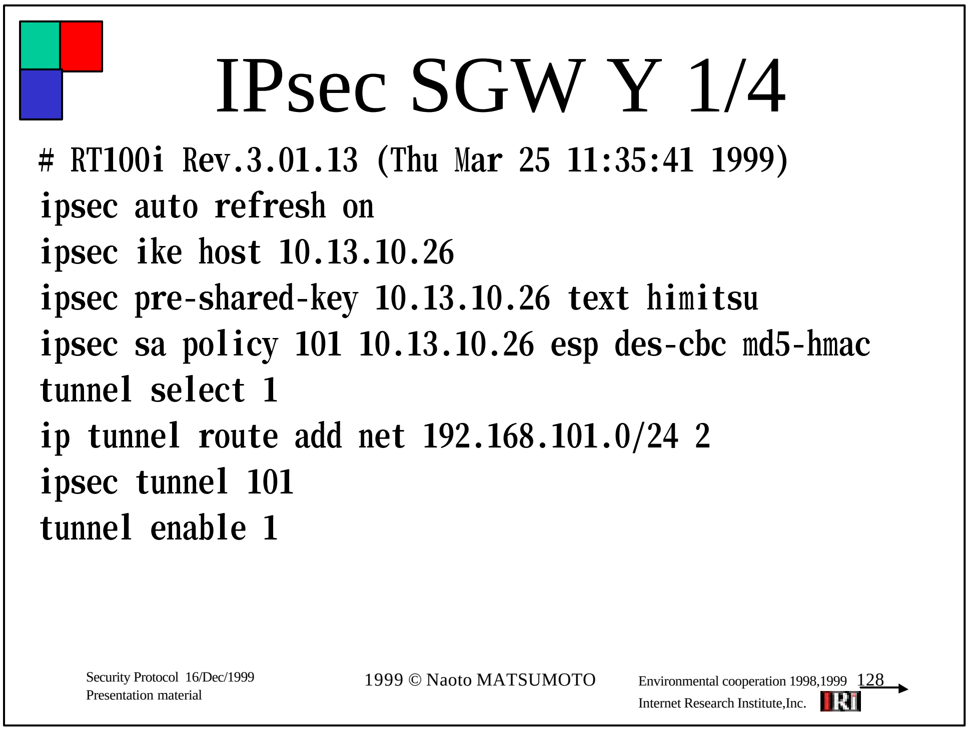
Click on point to see values. CTRL-Drag to zoom, r to reset.

Graph Type: System Resources

Graph Period: Historical

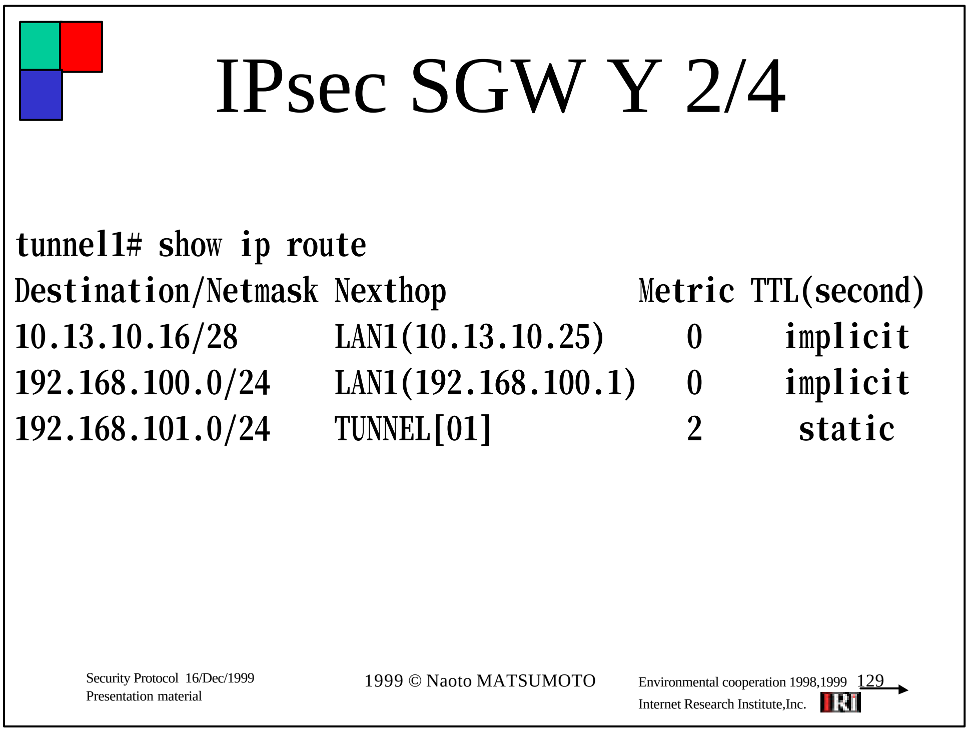


エンドーエンド型IPsec



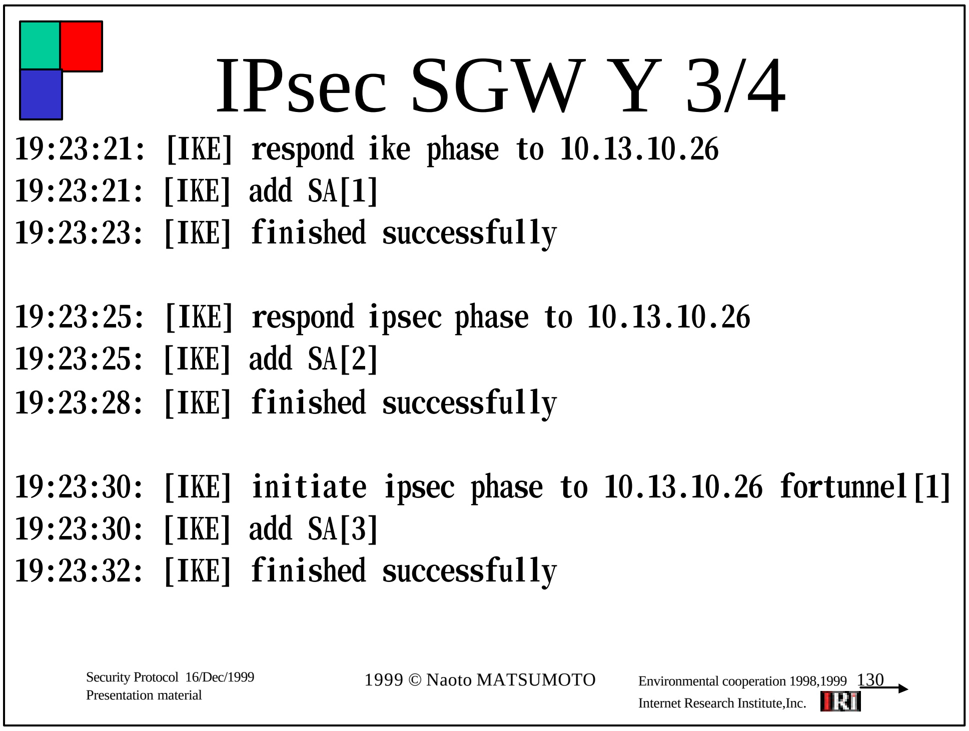
IPsec SGW Y 1/4

```
# RT100i Rev.3.01.13 (Thu Mar 25 11:35:41 1999)
ipsec auto refresh on
ipsec ike host 10.13.10.26
ipsec pre-shared-key 10.13.10.26 text himitsu
ipsec sa policy 101 10.13.10.26 esp des-cbc md5-hmac
tunnel select 1
ip tunnel route add net 192.168.101.0/24 2
ipsec tunnel 101
tunnel enable 1
```



IPsec SGW Y 2/4

```
tunnel1# show ip route
Destination/Netmask Nexthop             Metric TTL(second)
10.13.10.16/28      LAN1(10.13.10.25)     0      implicit
192.168.100.0/24    LAN1(192.168.100.1)   0      implicit
192.168.101.0/24    TUNNEL[01]            2       static
```



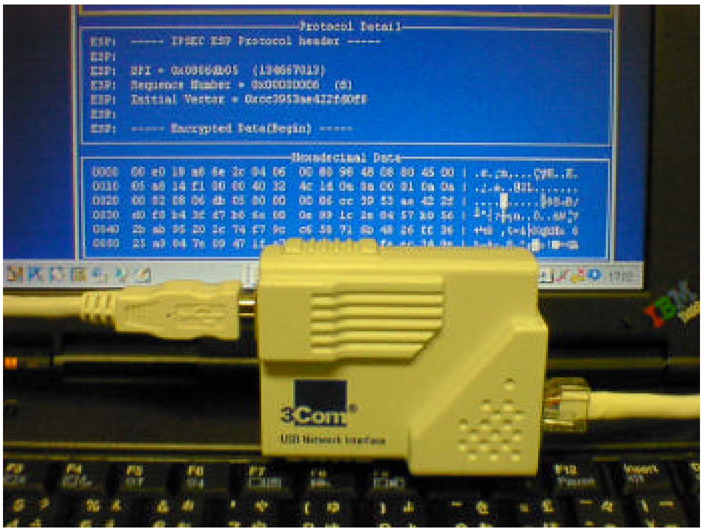
IPsec SGW Y 3/4

```
19:23:21: [IKE] respond ike phase to 10.13.10.26
19:23:21: [IKE] add SA[1]
19:23:23: [IKE] finished successfully

19:23:25: [IKE] respond ipsec phase to 10.13.10.26
19:23:25: [IKE] add SA[2]
19:23:28: [IKE] finished successfully

19:23:30: [IKE] initiate ipsec phase to 10.13.10.26 fortunnel[1]
19:23:30: [IKE] add SA[3]
19:23:32: [IKE] finished successfully
```

IPsec SGW Y 4/4

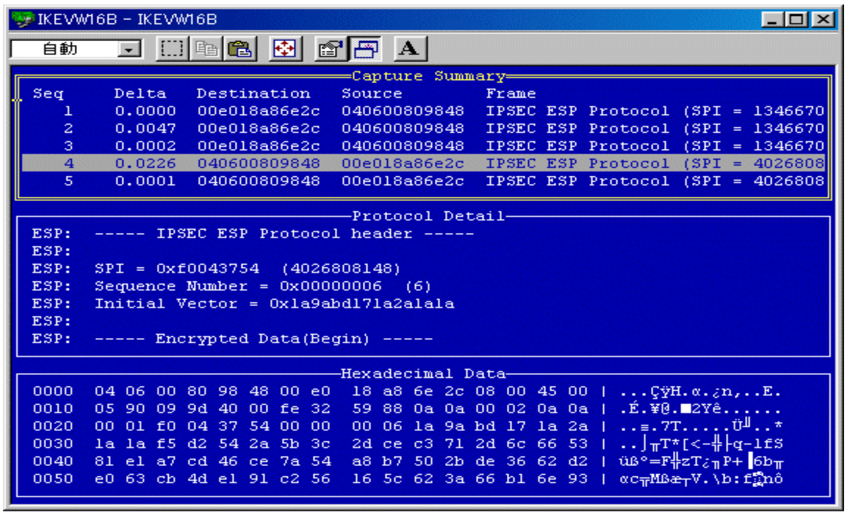
```
tunnel1# show ipsec sa
SA[1] / Duration: 28365(s), Direction: bidirection
Remote Host: 102.138.108.26
Protocol: IKE
Status: established idle
SPI: F6 1D 7D E9 87 1B 35 64 FA C2 FB 09 F7 AE E3 90
Key: 0D ** ** ** **   (confidential)   ** ** ** ** F6
SA[2] / Duration: 28369(s), Direction: receive
Remote Host: 10.138.108.26
Protocol: ESP (Mode: tunnel), IKE SA: SA[1]
Algorithm: DES-CBC (for Auth.: HMAC-MD5)
Status: established idle
SPI: F2 4A 7F E3
Key: E0 ** ** ** **   (confidential)   ** ** ** ** 67
```

IPsecツール 1/5



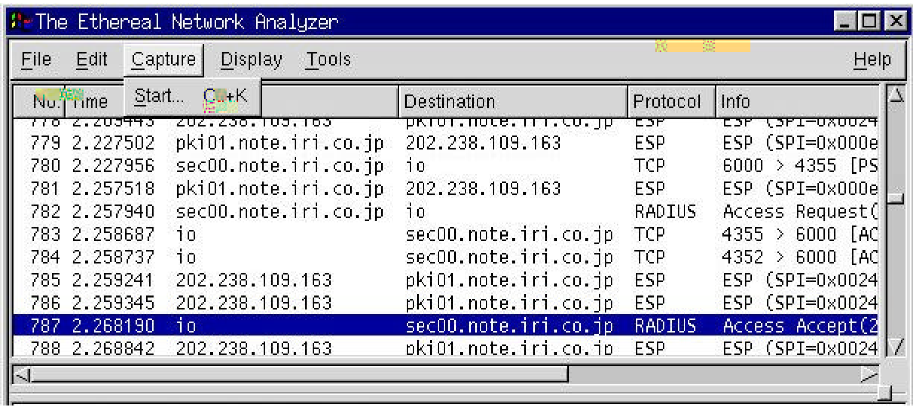
```
Protocol Detail
ESP:  ----- IPSEC ESP Protocol header -----
ESP:
ESP:  SPI = 0x0806db05  (134667013)
ESP:  Sequence Number = 0x00000006  (6)
ESP:  Initial Vector = 0xcc3953ae422fd0f0
ESP:
ESP:  ----- Encrypted Data(Begin) -----

Hexadecimal Data
0000  00 e0 18 a6 6e 2c 04 06  00 80 98 48 08 00 45 00
0010  05 a8 14 f1 00 00 40 32  4c 14 0a 8a c0 01 0a 0a
0020  00 02 08 06 db 05 00 00  00 06 cc 39 53 ae 42 2f
0030  d0 f0 b4 3f 47 b6 6e 00  0a 89 1c 2a 04 57 b0 56
0040  2b ab 95 20 3c 74 f7 9c  c6 58 71 8b 48 26 ff 36
0050  25 a9 04 7e 09 47 1f
```

IPsecツール 2/5

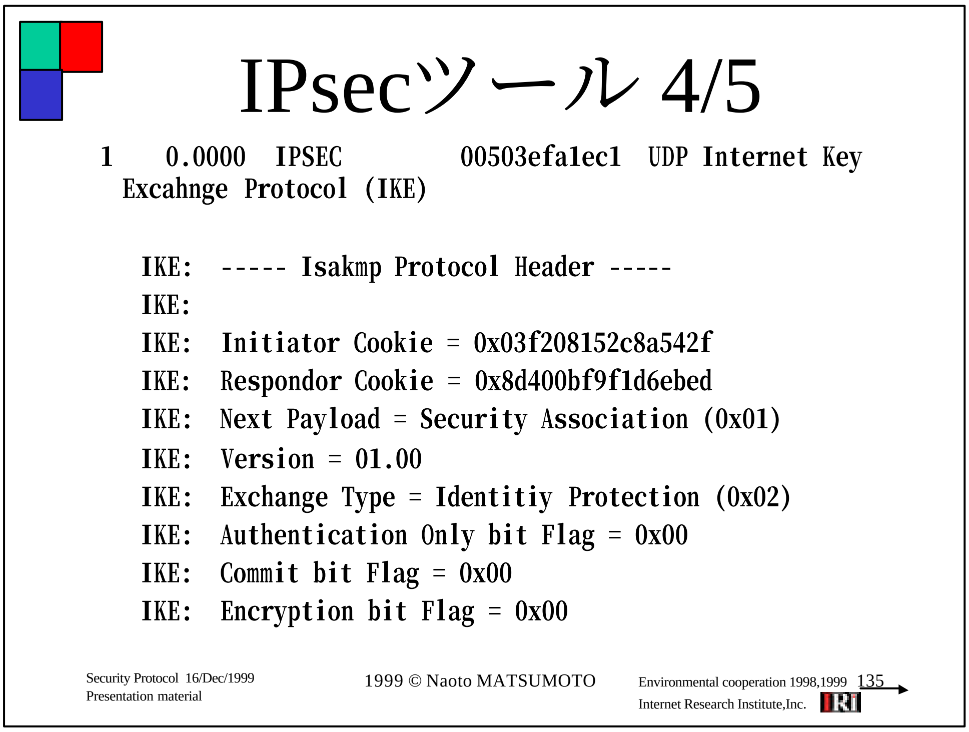


```
                           Capture Summary
Seq      Delta   Destination   Source        Frame
    1    0.0000  00e018a86e2c  040600809848  IPSEC ESP Protocol (SPI = 1346670
    2    0.0047  00e018a86e2c  040600809848  IPSEC ESP Protocol (SPI = 1346670
    3    0.0002  00e018a86e2c  040600809848  IPSEC ESP Protocol (SPI = 1346670
    4    0.0226  040600809848  00e018a86e2c  IPSEC ESP Protocol (SPI = 4026808
    5    0.0001  040600809848  00e018a86e2c  IPSEC ESP Protocol (SPI = 4026808

                           Protocol Detail
ESP:   ----- IPSEC ESP Protocol header -----
ESP:
ESP:   SPI = 0xf0043754  (4026808148)
ESP:   Sequence Number = 0x00000006  (6)
ESP:   Initial Vector = 0x1a9abd171a2a1a1a
ESP:
ESP:   ----- Encrypted Data(Begin) -----

                          Hexadecimal Data
0000   04 06 00 80 98 48 00 e0  18 a8 6e 2c 08 00 45 00 | ...ÇÿH.α.¿n,..E.
0010   05 90 09 9d 40 00 fe 32  59 88 0a 0a 00 02 0a 0a | .É.¥@.■2Yê......
0020   00 01 f0 04 37 54 00 00  00 06 1a 9a bd 17 1a 2a | ..≡.7T.....Ü╜..*
0030   1a 1a f5 d2 54 2a 5b 3c  2d ce c3 71 2d 6c 66 53 | ..⌡╥T*[<-╬├q-lfS
0040   81 e1 a7 cd 46 ce 7a 54  a8 b7 50 2b de 36 62 d2 | üßº═F╬zT¿╖P+▐6b╥
0050   e0 63 cb 4d e1 91 c2 56  16 5c 62 3a 66 b1 6e 93 | αc╦Mßæ┬V.\b:f▒nô
```

IPsecツール 3/5

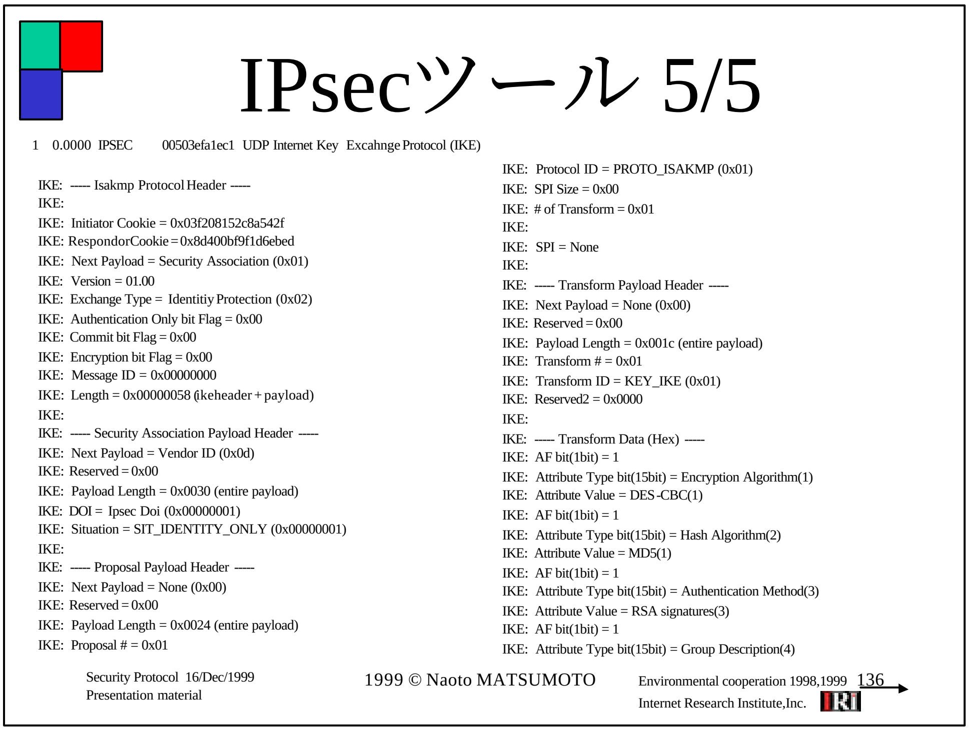


```
No. Time                                     Destination           Protocol  Info
778 2.203443  202.238.109.163       pki01.note.iri.co.jp  ESP       ESP (SPI=0x0024
779 2.227502  pki01.note.iri.co.jp  202.238.109.163       ESP       ESP (SPI=0x000e
780 2.227956  sec00.note.iri.co.jp  io                    TCP       6000 > 4355 [PS
781 2.257518  pki01.note.iri.co.jp  202.238.109.163       ESP       ESP (SPI=0x000e
782 2.257940  sec00.note.iri.co.jp  io                    RADIUS    Access Request(
783 2.258687  io                    sec00.note.iri.co.jp  TCP       4355 > 6000 [AC
784 2.258737  io                    sec00.note.iri.co.jp  TCP       4352 > 6000 [AC
785 2.259241  202.238.109.163       pki01.note.iri.co.jp  ESP       ESP (SPI=0x0024
786 2.259345  202.238.109.163       pki01.note.iri.co.jp  ESP       ESP (SPI=0x0024
787 2.268190  io                    sec00.note.iri.co.jp  RADIUS    Access Accept(2
788 2.268842  202.238.109.163       pki01.note.iri.co.jp  ESP       ESP (SPI=0x0024
```



IPsecツール 4/5

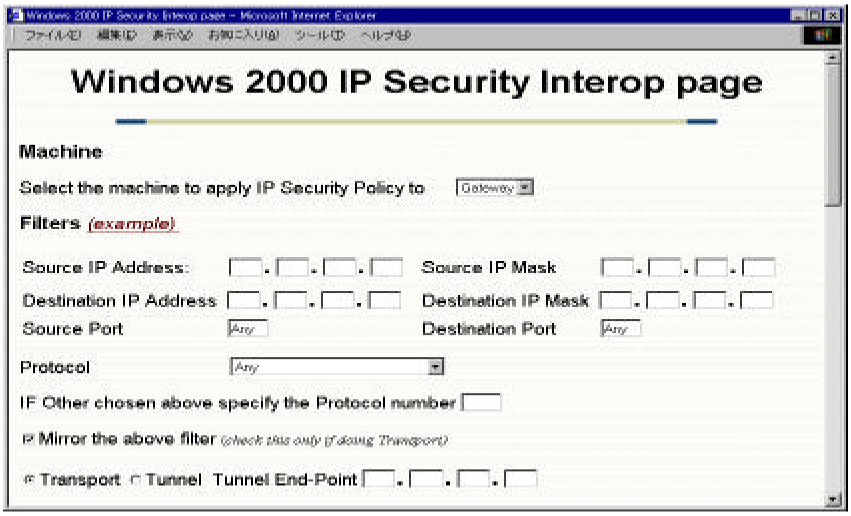
```
1    0.0000  IPSEC        00503efa1ec1  UDP Internet Key
  Excahnge Protocol (IKE)

    IKE:  ----- Isakmp Protocol Header -----
    IKE:
    IKE:  Initiator Cookie = 0x03f208152c8a542f
    IKE:  Respondor Cookie = 0x8d400bf9f1d6ebed
    IKE:  Next Payload = Security Association (0x01)
    IKE:  Version = 01.00
    IKE:  Exchange Type = Identitiy Protection (0x02)
    IKE:  Authentication Only bit Flag = 0x00
    IKE:  Commit bit Flag = 0x00
    IKE:  Encryption bit Flag = 0x00
```



IPsecツール 5/5

```
1   0.0000  IPSEC      00503efa1ec1  UDP Internet Key  Excahnge Protocol (IKE)

IKE:  ----- Isakmp Protocol Header -----
IKE:
IKE:  Initiator Cookie = 0x03f208152c8a542f
IKE: RespondorCookie = 0x8d400bf9f1d6ebed
IKE:  Next Payload = Security Association (0x01)
IKE:  Version = 01.00
IKE:  Exchange Type =  Identitiy Protection (0x02)
IKE:  Authentication Only bit Flag = 0x00
IKE:  Commit bit Flag = 0x00
IKE:  Encryption bit Flag = 0x00
IKE:  Message ID = 0x00000000
IKE:  Length = 0x00000058 (ikeheader + payload)
IKE:
IKE:  ----- Security Association Payload Header -----
IKE:  Next Payload = Vendor ID (0x0d)
IKE: Reserved = 0x00
IKE:  Payload Length = 0x0030 (entire payload)
IKE:  DOI =  Ipsec Doi (0x00000001)
IKE:  Situation = SIT_IDENTITY_ONLY (0x00000001)
IKE:
IKE:  ----- Proposal Payload Header -----
IKE:  Next Payload = None (0x00)
IKE: Reserved = 0x00
IKE:  Payload Length = 0x0024 (entire payload)
IKE:  Proposal # = 0x01
IKE:  Protocol ID = PROTO_ISAKMP (0x01)
IKE:  SPI Size = 0x00
IKE:  # of Transform = 0x01
IKE:
IKE:  SPI = None
IKE:
IKE:  ----- Transform Payload Header -----
IKE:  Next Payload = None (0x00)
IKE: Reserved = 0x00
IKE:  Payload Length = 0x001c (entire payload)
IKE:  Transform # = 0x01
IKE:  Transform ID = KEY_IKE (0x01)
IKE:  Reserved2 = 0x0000
IKE:
IKE:  ----- Transform Data (Hex) -----
IKE:  AF bit(1bit) = 1
IKE:  Attribute Type bit(15bit) = Encryption Algorithm(1)
IKE:  Attribute Value = DES-CBC(1)
IKE:  AF bit(1bit) = 1
IKE:  Attribute Type bit(15bit) = Hash Algorithm(2)
IKE:  Attribute Value = MD5(1)
IKE:  AF bit(1bit) = 1
IKE:  Attribute Type bit(15bit) = Authentication Method(3)
IKE:  Attribute Value = RSA signatures(3)
IKE:  AF bit(1bit) = 1
IKE:  Attribute Type bit(15bit) = Group Description(4)
```

IPsecの動向1/2



Windows 2000 IP Security Interop page - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

Windows 2000 IP Security Interop page

Machine

Select the machine to apply IP Security Policy to: Gateway

Filters *(example)*

Source IP Address: __.__.__.__ Source IP Mask __.__.__.__

Destination IP Address __.__.__.__ Destination IP Mask __.__.__.__

Source Port: Any Destination Port: Any

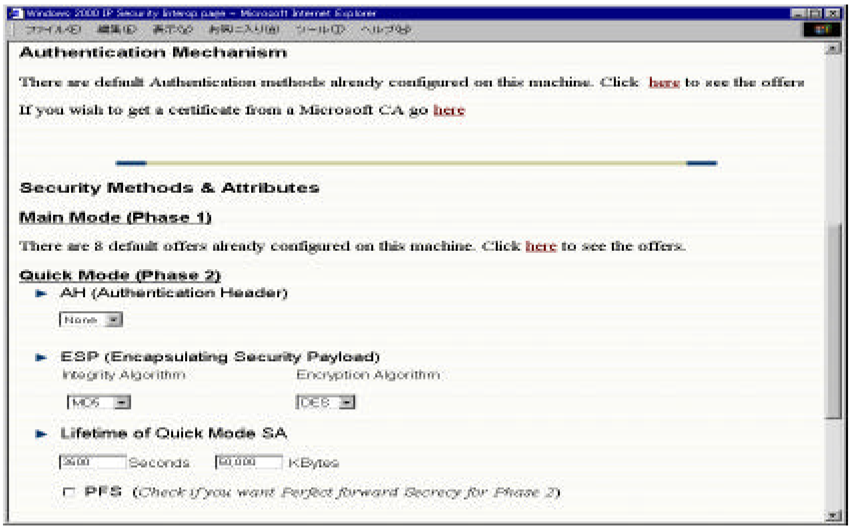
Protocol: Any

IF Other chosen above specify the Protocol number

☑ Mirror the above filter *(check this only if doing Transport)*

● Transport ○ Tunnel Tunnel End-Point __.__.__.__

IPsecの動向2/2



Windows 2000 IP Security Interop page - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

Authentication Mechanism

There are default Authentication methods already configured on this machine. Click here to see the offers

If you wish to get a certificate from a Microsoft CA go here

Security Methods & Attributes

Main Mode (Phase 1)

There are 8 default offers already configured on this machine. Click here to see the offers.

Quick Mode (Phase 2)

- AH (Authentication Header): None
- ESP (Encapsulating Security Payload)
  Integrity Algorithm: MD5 Encryption Algorithm: DES
- Lifetime of Quick Mode SA
  3600 Seconds 50,000 KBytes

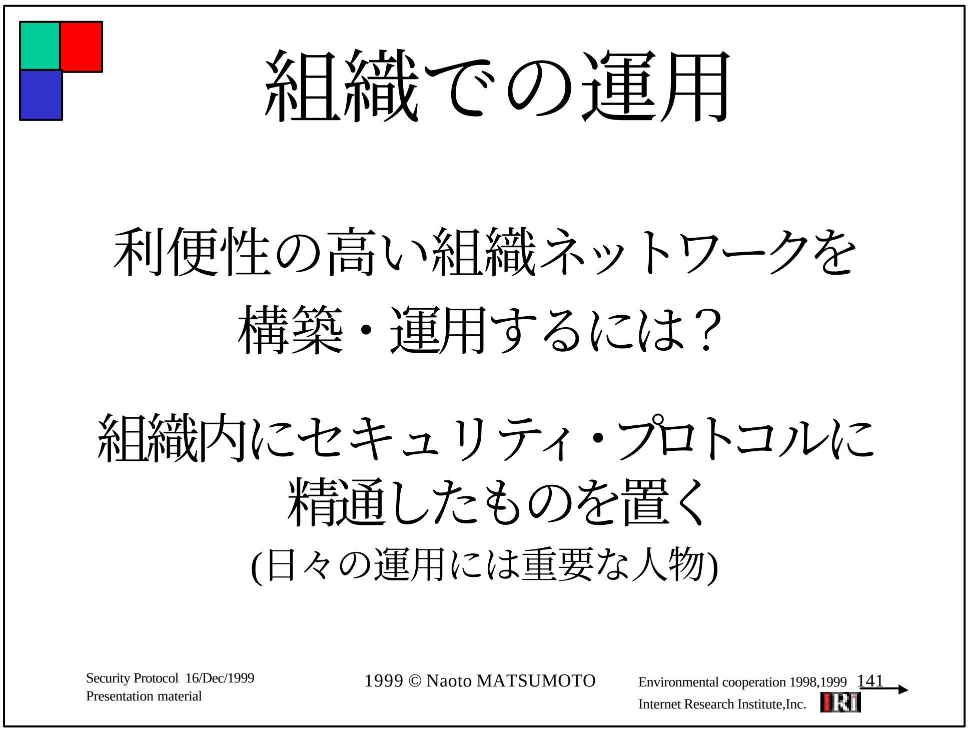
□ PFS *(Check if you want Perfect forward Secrecy for Phase 2)*

休憩

セキュリティ・プロトコル

III

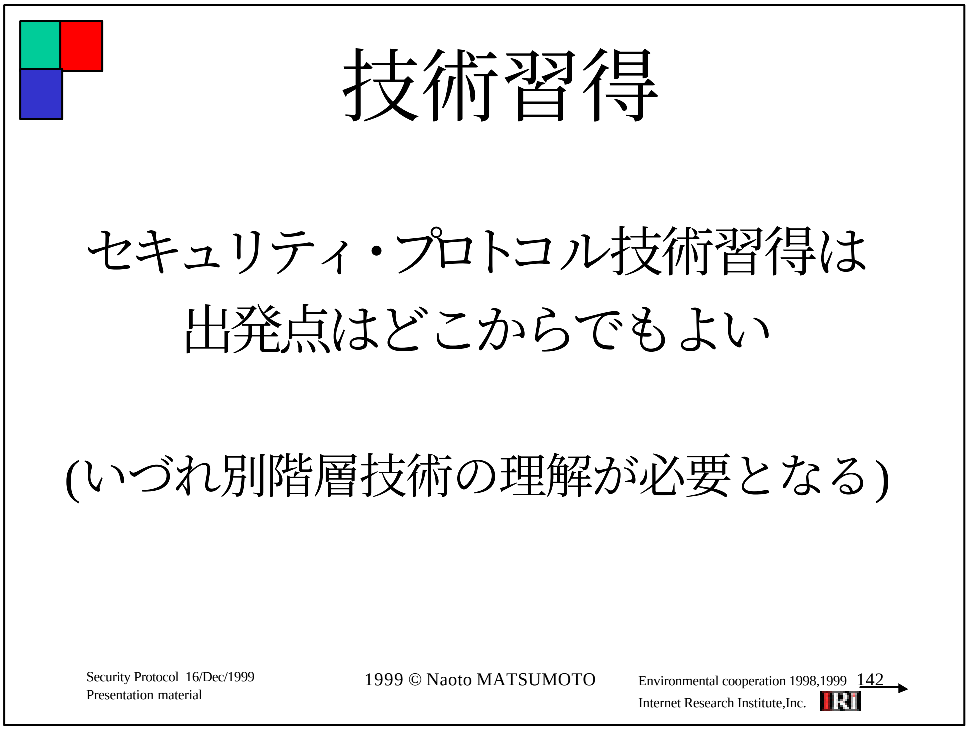
運用にあたって



組織での運用

利便性の高い組織ネットワークを
構築・運用するには？

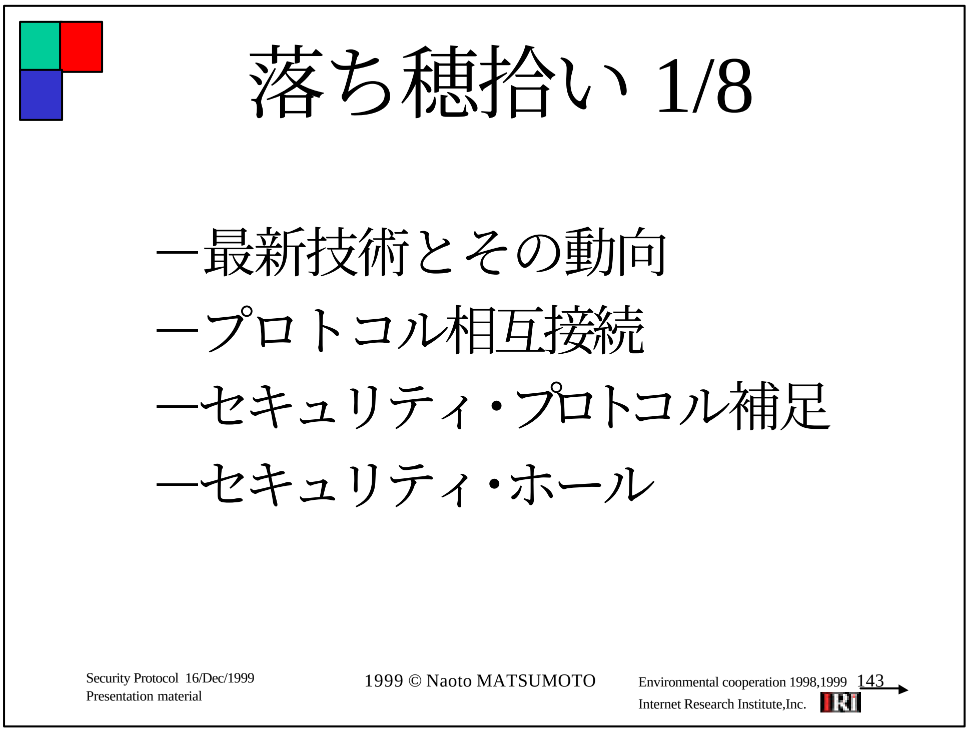
組織内にセキュリティ・プロトコルに
精通したものを置く
(日々の運用には重要な人物)



技術習得

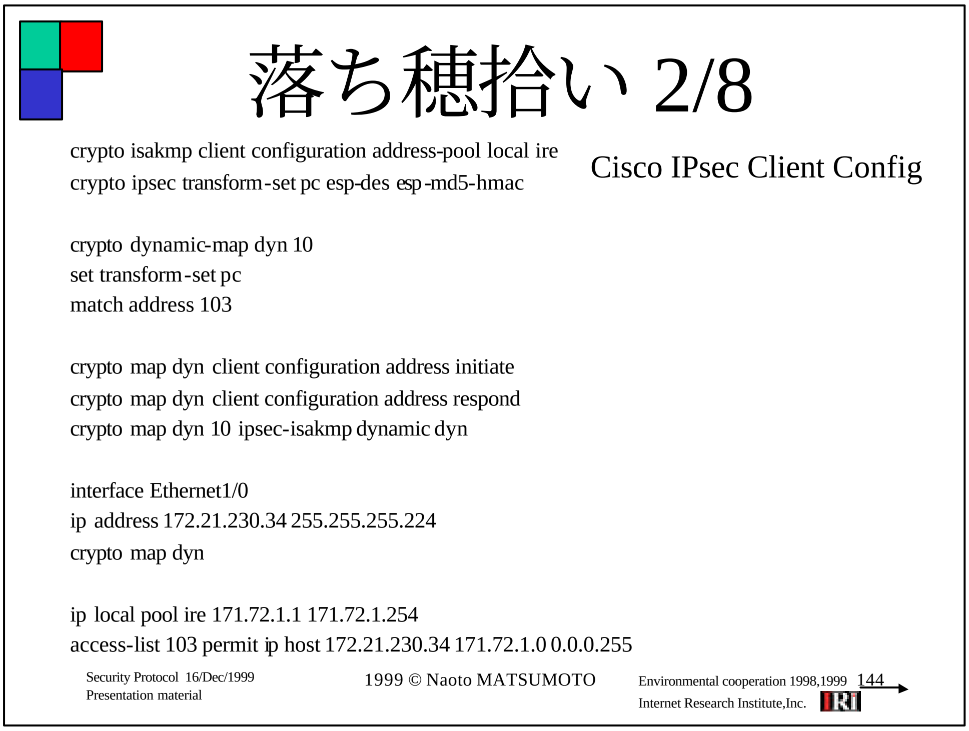
セキュリティ・プロトコル技術習得は
出発点はどこからでもよい

(いづれ別階層技術の理解が必要となる)



落ち穂拾い 1/8

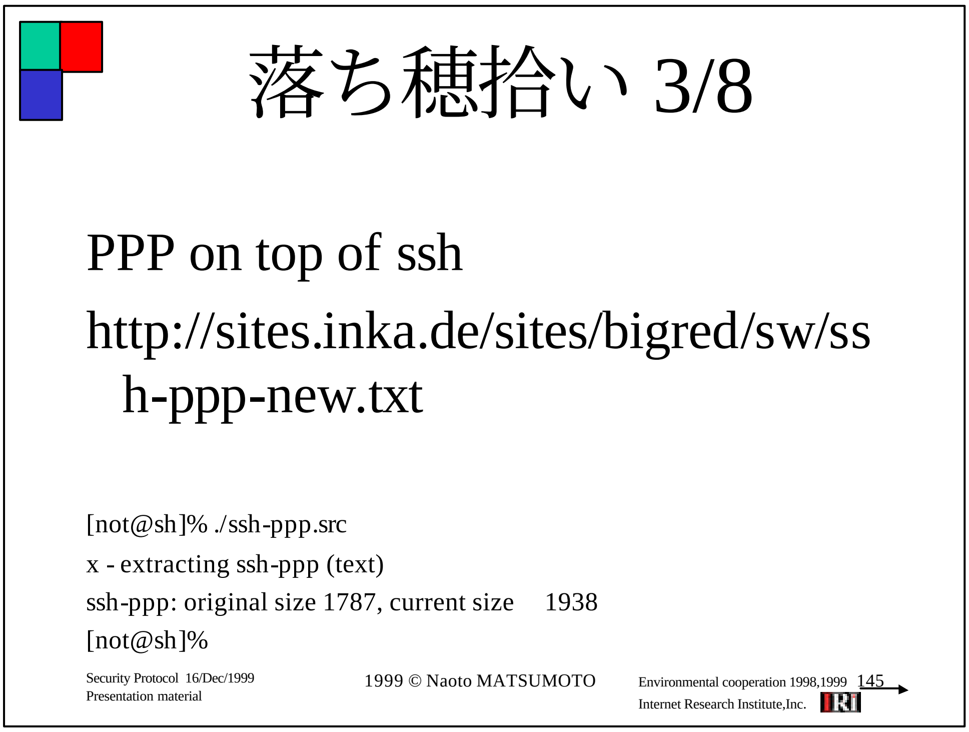
―最新技術とその動向
―プロトコル相互接続
―セキュリティ・プロトコル補足
―セキュリティ・ホール



落ち穂拾い 2/8

Cisco IPsec Client Config

```
crypto isakmp client configuration address-pool local ire
crypto ipsec transform-set pc esp-des esp-md5-hmac

crypto dynamic-map dyn 10
set transform-set pc
match address 103

crypto map dyn client configuration address initiate
crypto map dyn client configuration address respond
crypto map dyn 10 ipsec-isakmp dynamic dyn

interface Ethernet1/0
ip address 172.21.230.34 255.255.255.224
crypto map dyn

ip local pool ire 171.72.1.1 171.72.1.254
access-list 103 permit ip host 172.21.230.34 171.72.1.0 0.0.0.255
```

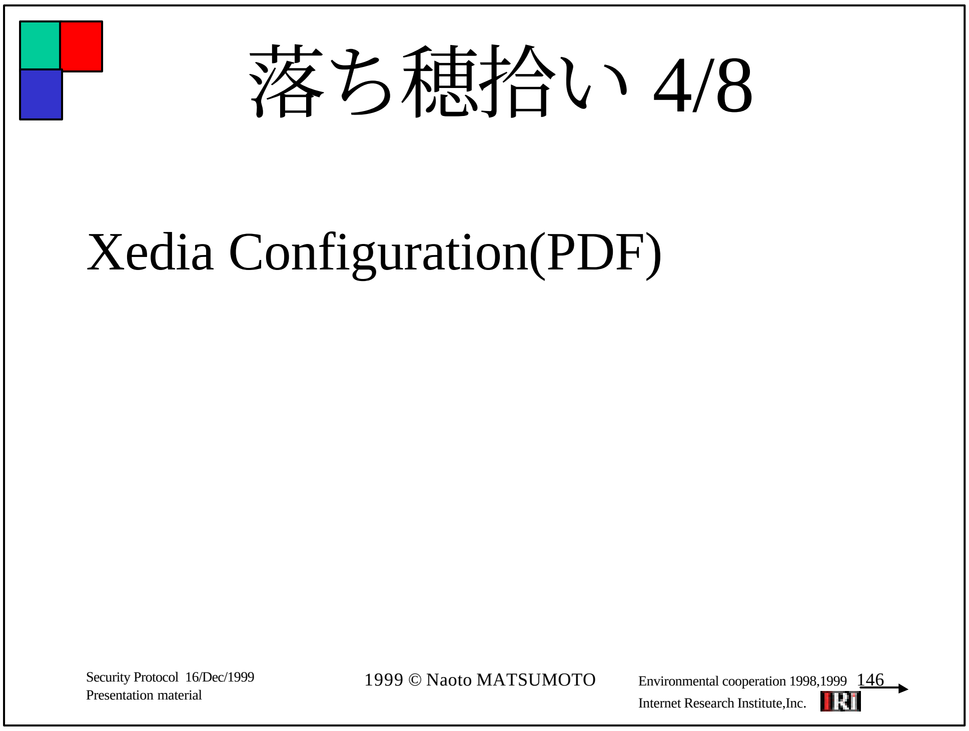


落ち穂拾い 3/8

PPP on top of ssh

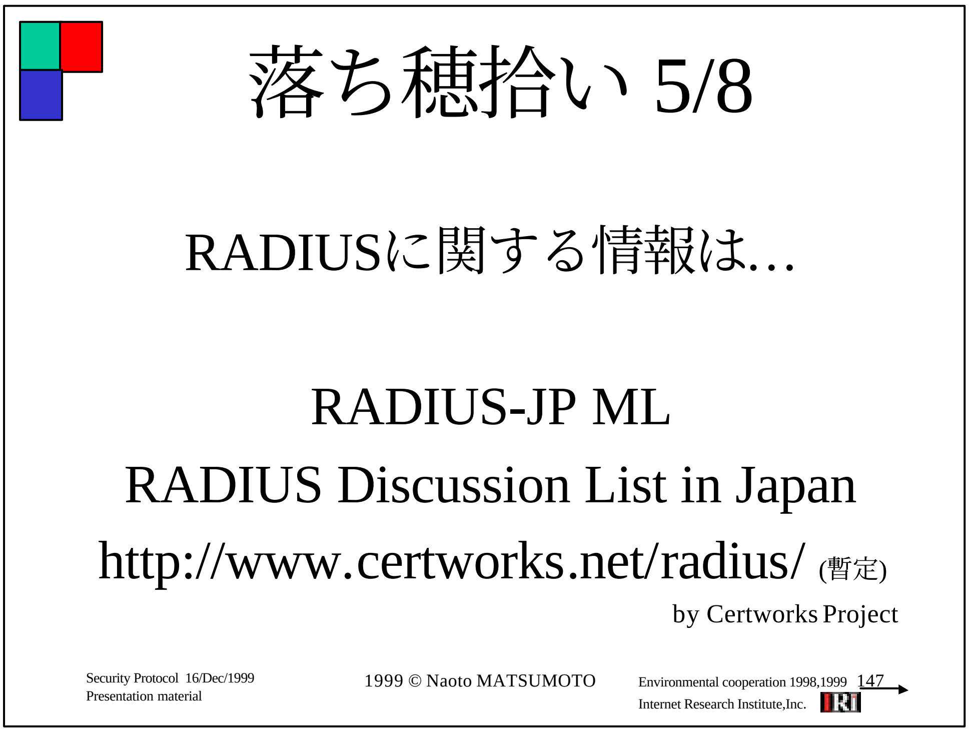
http://sites.inka.de/sites/bigred/sw/ssh-ppp-new.txt

```
[not@sh]% ./ssh-ppp.src
x - extracting ssh-ppp (text)
ssh-ppp: original size 1787, current size    1938
[not@sh]%
```



落ち穂拾い 4/8

Xedia Configuration(PDF)



落ち穂拾い 5/8

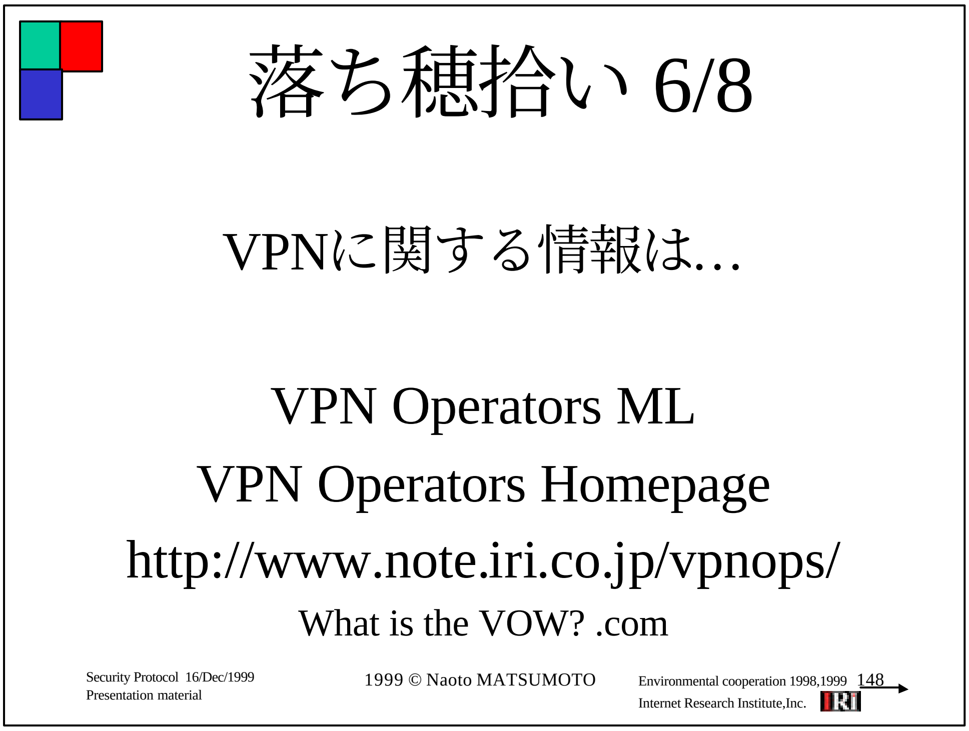
RADIUSに関する情報は…

RADIUS-JP ML

RADIUS Discussion List in Japan

http://www.certworks.net/radius/ (暫定)

by Certworks Project



落ち穂拾い 6/8

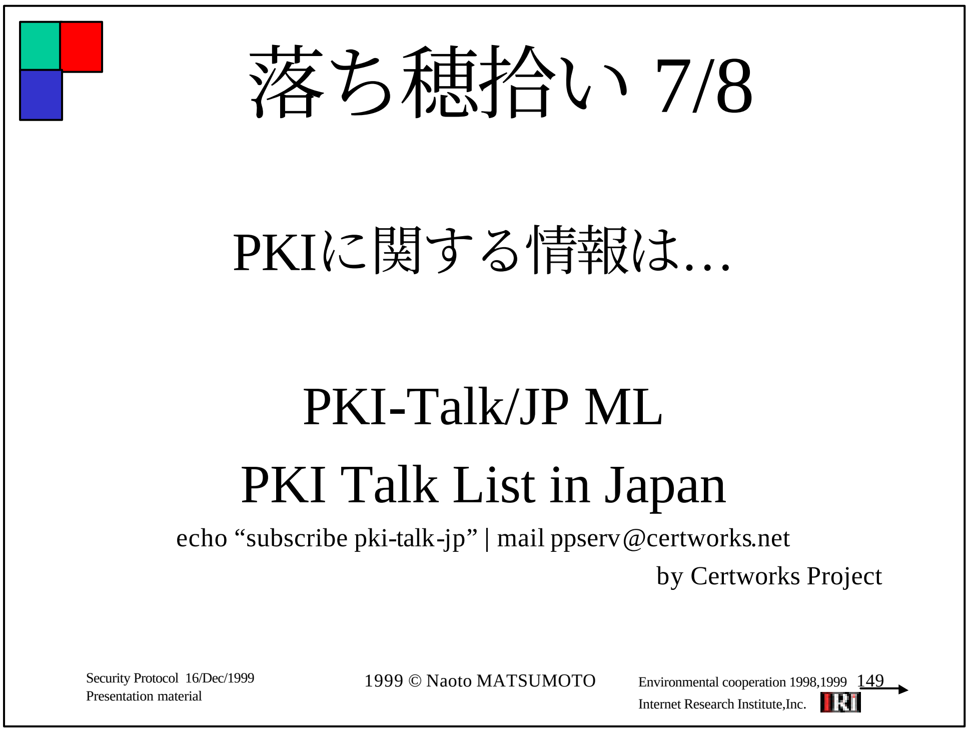
VPNに関する情報は…

VPN Operators ML

VPN Operators Homepage

http://www.note.iri.co.jp/vpnops/

What is the VOW? .com



落ち穂拾い 7/8

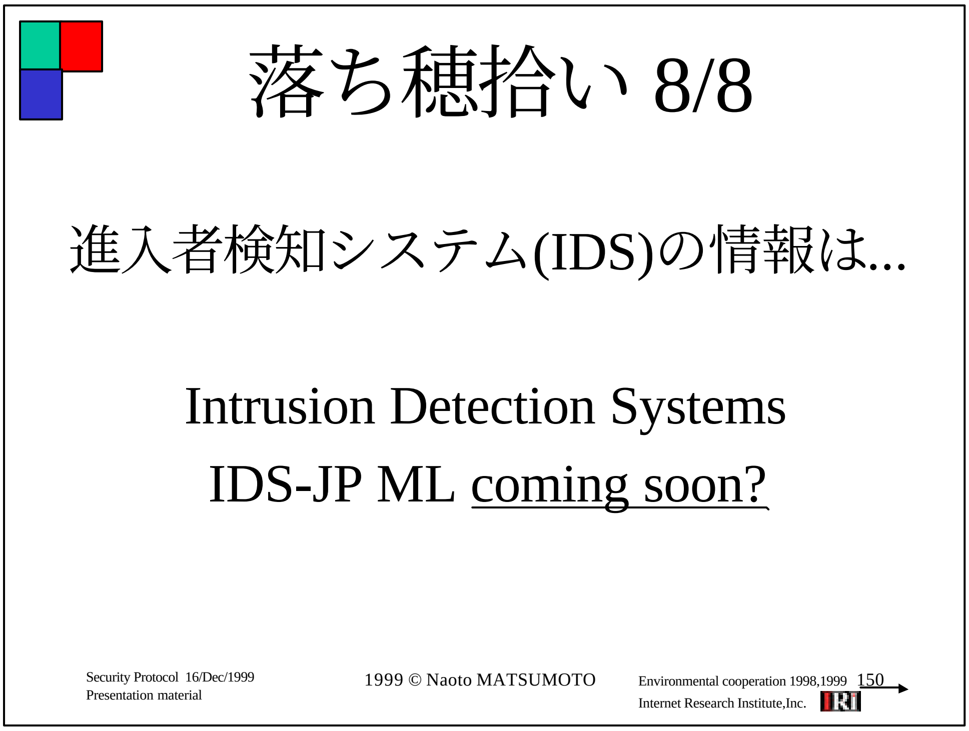
PKIに関する情報は…

PKI-Talk/JP ML

PKI Talk List in Japan

echo “subscribe pki-talk-jp” | mail ppserv@certworks.net

by Certworks Project



落ち穂拾い 8/8

進入者検知システム(IDS)の情報は...

Intrusion Detection Systems

IDS-JP ML coming soon?

セキュリティ・プロトコル

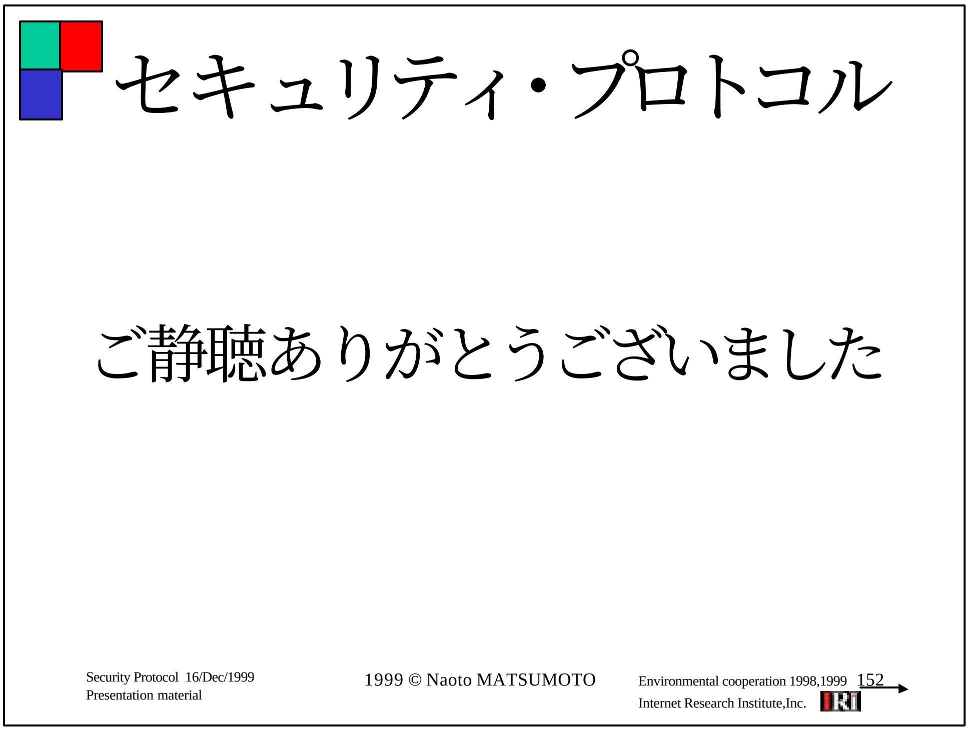
IV

質疑応答

Security Protocol 16/Dec/1999
Presentation material

1999 © Naoto MATSUMOTO

Environmental cooperation 1998,1999 151
Internet Research Institute,Inc. IRI



セキュリティ・プロトコル

ご静聴ありがとうございました

Security Protocol 16/Dec/1999
Presentation material

1999 © Naoto MATSUMOTO

Environmental cooperation 1998,1999 152
Internet Research Institute,Inc. IRI