H3C SecPath L2TP IPsec VPN

簡易マニュアル(LDAP 認証 CLI 編)

(iNode L2TP IPsec VPN client)

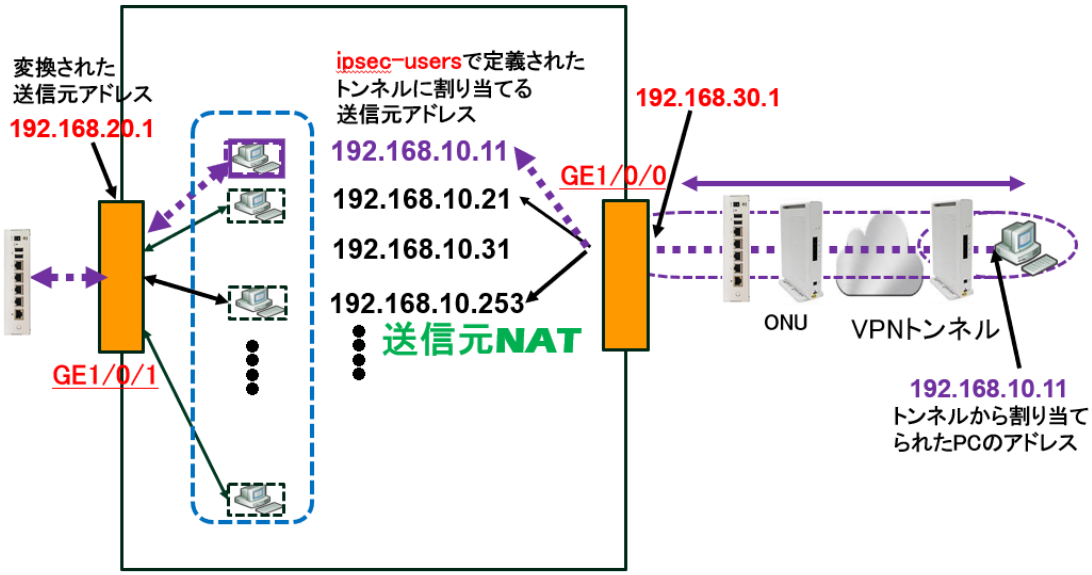
V1.4

2021/7/7

内容

1. テストトポロジ

テスト環境では、LDAP と Active Directory 連携によるユーザー認証を実施。
Active Directory のドメインは ad.rem-system.com としています。



この例は version 7.1.064, Release 9345P14 で実施しました。

クライアントソフトウェア適応システム：Windows7、8、Vista、10、XP、Windows Server 2003

2. L2TP IPsec VPN 設定パラメーター

2.1 基本設定

パラメーター	設定値
LNS サーバー	192.168.30.1
代替 LNS サーバー	192.168.30.1
IPsec	Enable
認証モード	Pre-shared-key
認証キー	test
IPsec サーバー	LNS サーバーを使用

2.2 L2TP トンネル

パラメーター	設定値
認証モード	PAP
Hello パケット送信間隔	60 秒
L2TP ポート	1701

2.3 IPsec パラメーター

パラメーター	設定値
モード	トンネル
SA ライフタイム	3600 秒
ESP トランスフォーム	3DES(16 bit) / ESP-MD5
AH	MD5
PFS	なし
アドレス変換	NAT トラバーサル

2.4 IKE パラメーター

パラメーター	設定値
ネゴシエーションモード	Aggressive
認証アルゴリズム	SHA
暗号化アルゴリズム	DES-CBC
DH グループ	2
IKE ポート	500
SA ライフタイム	86400 秒
ローカルセキュリティゲートウェイ名	Inode
リモートセキュリティゲートウェイ名	lns
keepalive パケット受信間隔	なし
keepalive パケット送信間隔	なし

3. SecPathF1020 側の設定手順

手順1：SecPath の内部、外部インターフェースに IP アドレスを割り当てる

```
#インターフェースの IP 設定
interface GigabitEthernet1/0/0
 ip address 192.168.30.1/32
#
interface GigabitEthernet1/0/1
 ip address 192.168.20.1 24
#
```

手順2. IPsec VPN の設定をする

VPN クライアントに割り当てられる IP アドレスプールの設定をする

```
#VPN クライアントへ割り当てる IP アドレスプールの設定
 ip pool pool 192.168.10.11 192.168.10.253
 ip pool pool gateway 192.168.10.1
#
interface Virtual-Template1
 ppp authentication-mode pap
 remote address pool pool
 ip address 192.168.10.1 255.255.255.0
#
```

VPN クライアントのログインユーザー、パスワードの設定をする

```
#ログインユーザー設定
local-user client class network
 password simple client
 service-type ppp
 authorization-attribute user-role network-operator
```

#

IPsec ポリシーの設定をする

```
ipsec transform-set 1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec transform-set 2
 encapsulation-mode transport
 esp encryption-algorithm aes-cbc-128
 esp authentication-algorithm sha1
#
ipsec transform-set 3
 encapsulation-mode transport
 esp encryption-algorithm aes-cbc-256
 esp authentication-algorithm sha1
#
ipsec transform-set 4
 encapsulation-mode transport
 esp encryption-algorithm des-cbc
 esp authentication-algorithm sha1
#
ipsec transform-set 5
 encapsulation-mode transport
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm sha1
#
ipsec transform-set 6
 encapsulation-mode transport
 esp encryption-algorithm aes-cbc-192
 esp authentication-algorithm sha1
#
#ipsec policy-template 1 1
 transform-set 1 2 3 4 5 6
 ike-profile 1
#
ipsec policy 1 1 isakmp template 1
#
```

L2TP の設定をする

```
#L2TP 設定
l2tp-group 1 mode lns
 allow l2tp virtual-template 1
 undo tunnel authentication
#
 l2tp enable
```

IKE ポリシーの設定をする

```
#IKE プロファイル
ike profile 1
 keychain 1
 exchange-mode aggressive
 local-identity fqdn lns
 match remote identity address 0.0.0.0 0.0.0.0
 match remote identity fqdn inode
 proposal 1 2 3 4 5 6
#IKE プロポーザル
ike proposal 1
 dh group2
 authentication-algorithm md5
#
ike proposal 2
 encryption-algorithm 3des-cbc
 dh group2
 authentication-algorithm md5
#
ike proposal 3
 encryption-algorithm 3des-cbc
 dh group2
#
ike proposal 4
 encryption-algorithm aes-cbc-256
 dh group2
#
ike proposal 5
 dh group2
#
ike proposal 6
```

```
 encryption-algorithm aes-cbc-192
 dh group2
```

IPsec トンネルキーの設定をする

```
#基本設定(認証モード、認証キー)
ike keychain 1
 pre-shared-key address 0.0.0.0 0.0.0.0 key simple test
#
```

手順 3. セキュリティゾーンとセキュリティポリシーを設定する

```
#セキュリティゾーンのデフォルト設定
 security-zone intra-zone default permit
#セキュリティゾーンのインターフェース設定
security-zone name Trust
 import interface GigabitEthernet1/0/1
#
security-zone name Untrust
import interface Virtual-Template1
#
security-zone name Management
import interface GigabitEthernet1/0/0
#IP セキュリティポリシーの設定
security-policy ip
 rule 0 name 1
  action pass
rule 1 name 0
  action pass
  counting enable
  source-zone Local
  source-zone Trust
  source-zone Untrust
  destination-zone Local
  destination-zone Trust
  destination-zone Untrust
#
```

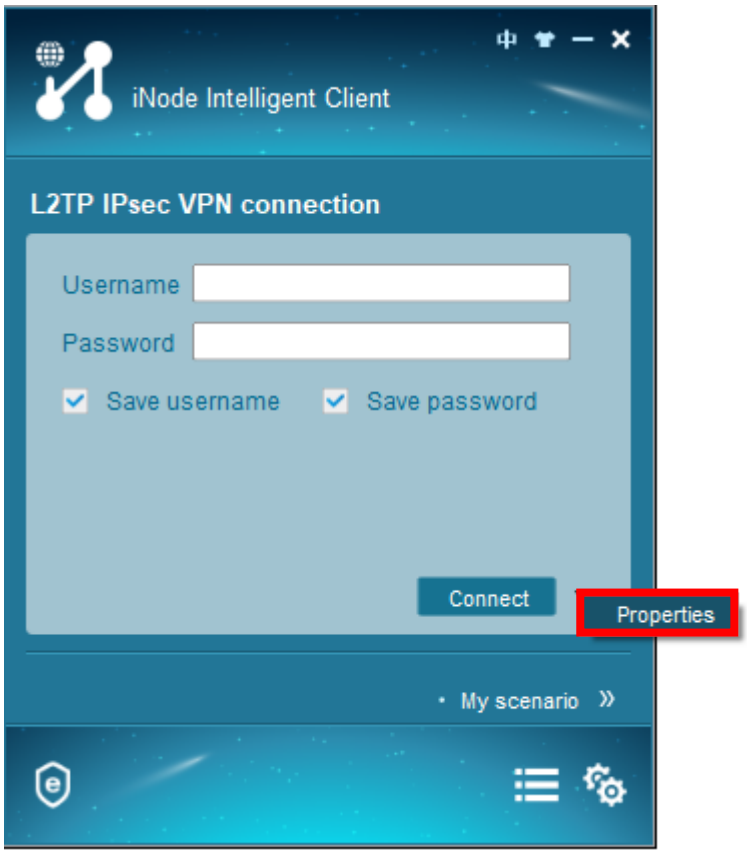
手順 4. LDAP サーバーの設定をする

```
#LDAP 認証の設定
ldap server rem-system
 login-dn CN=Administrator,CN=Users,DC=ad,DC=rem-system,DC=com,DC=local
 search-base-dn DC=ad,DC=rem-system,DC=com,DC=local
 ip 192.168.20.10
 login-password simple test
 protocol-version v2
#
ldap scheme user_db
 authentication-server rem-system
#
```

4. クライアント側の設定

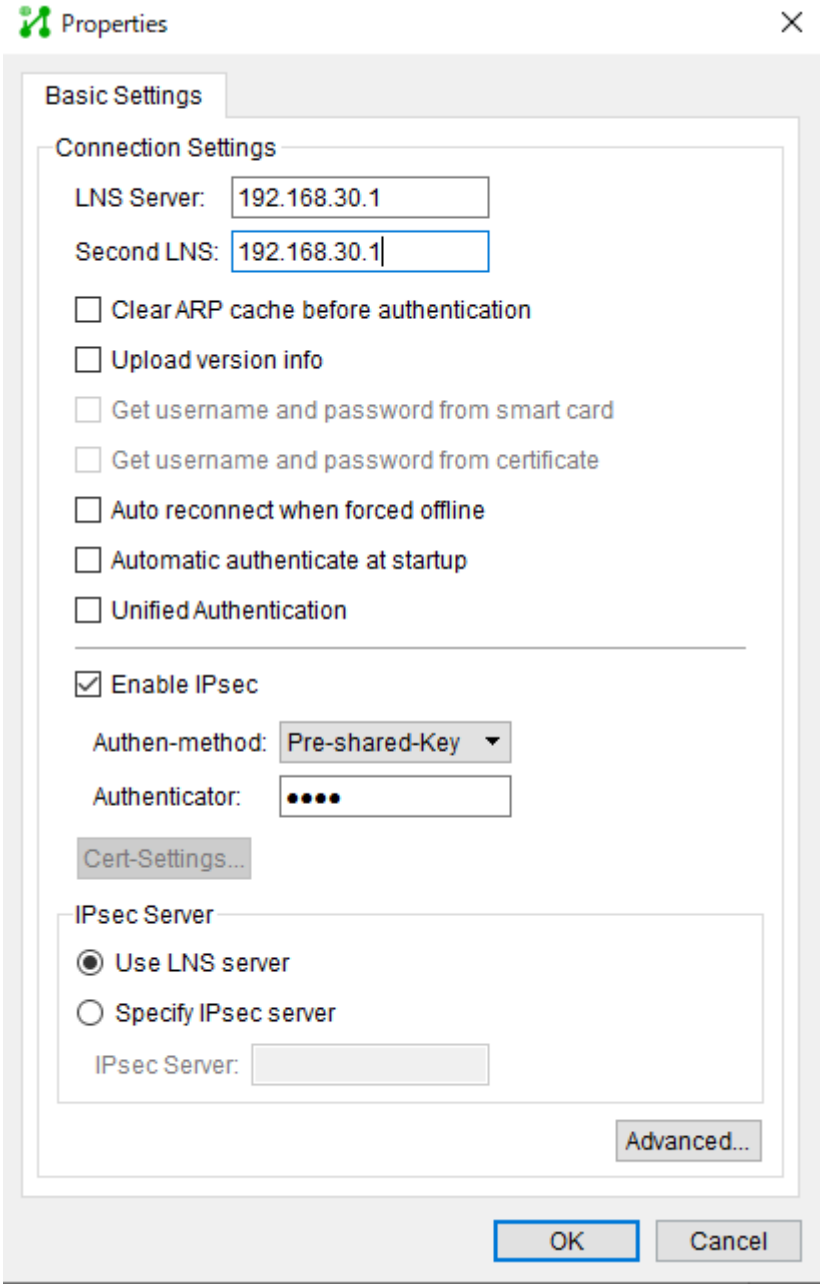
① デスクトップの iNode Client のアイコンをダブルクリックします。

② Connect ボタンを右クリックして Properties が現れたら、Properties ボタンをクリックします。

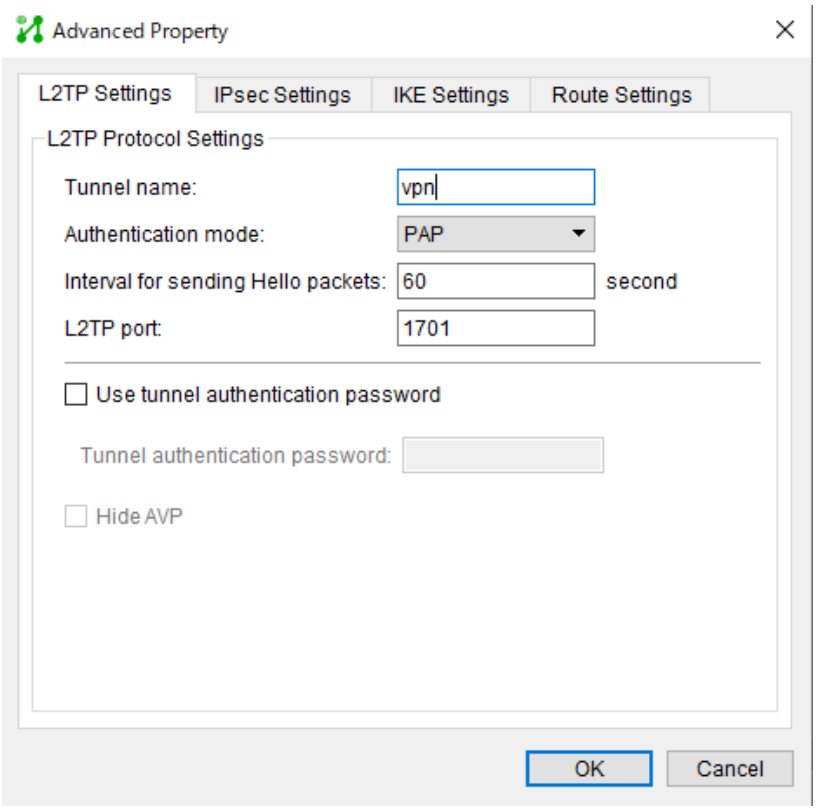


③ 基本設定

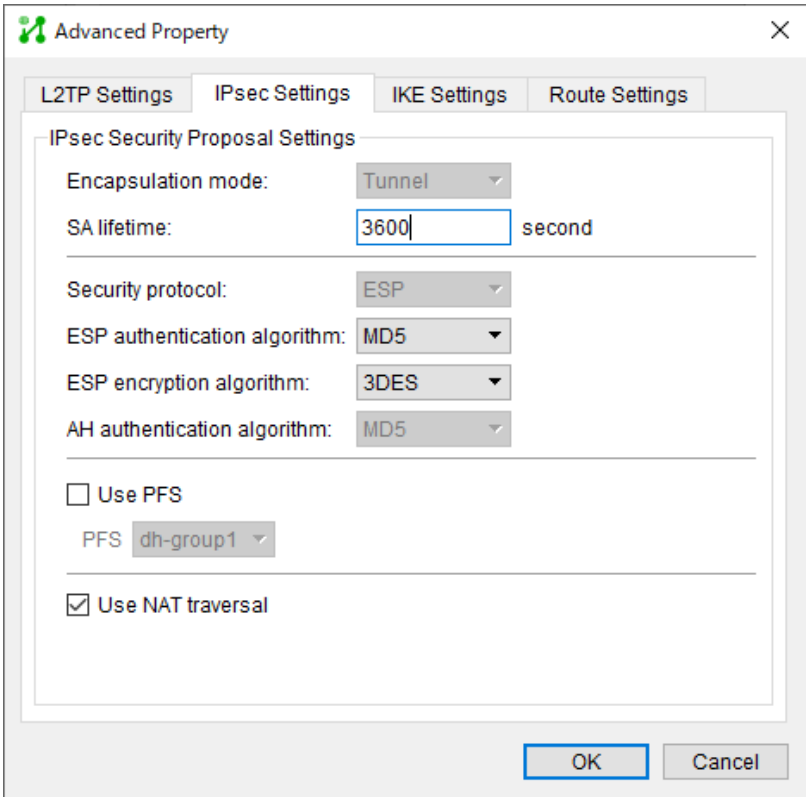
SecPath の外部 IP アドレスを入力し、IPsec、IPsec サーバーの設定を行います。



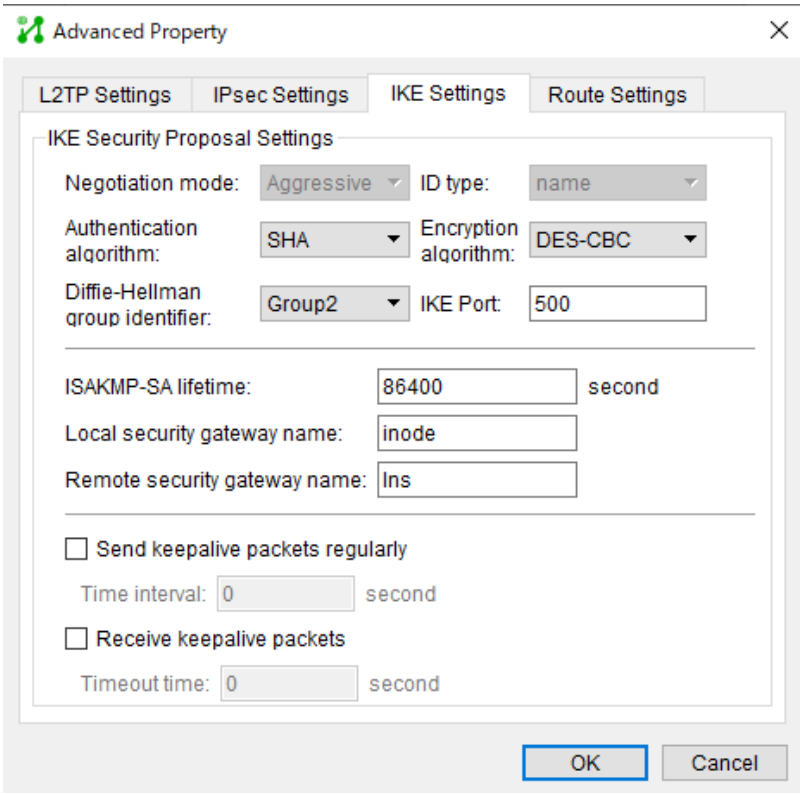
④L2TP の設定を行います。



⑤IPsec の設定を行います。



⑥IKE の設定を行います。

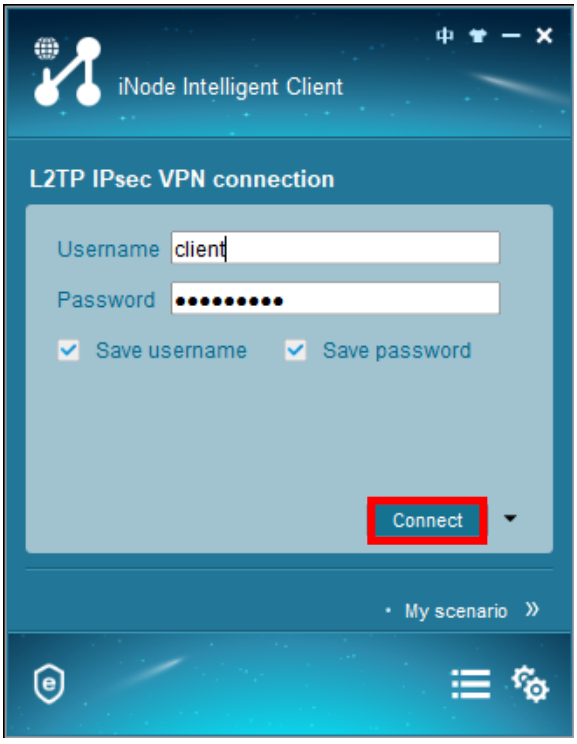


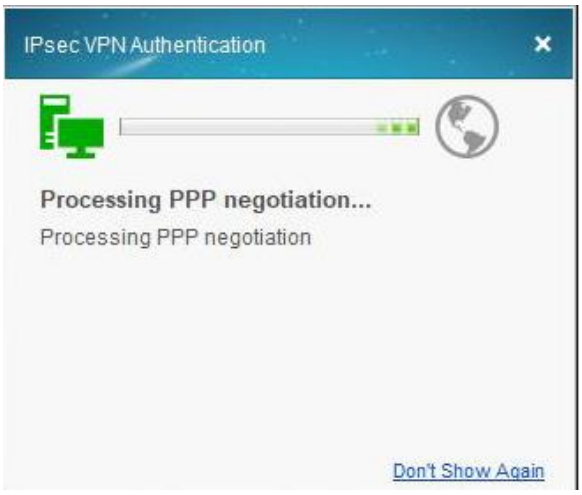
以上でクライアントの設定は完了しました。

5. 接続と切断

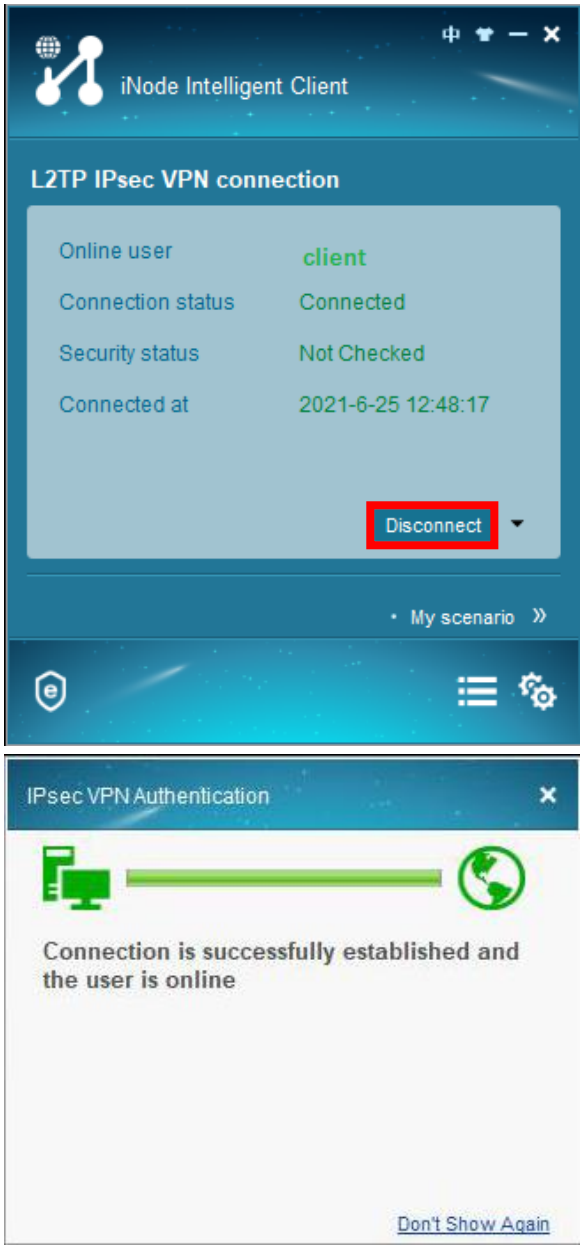
① デスクトップの iNode Client のアイコンをダブルクリックします。

② iNode Client のログイン画面が表示され、ユーザー名(client)とパスワード(client)を入力します。
そして、 Connect ボタンをクリックします。





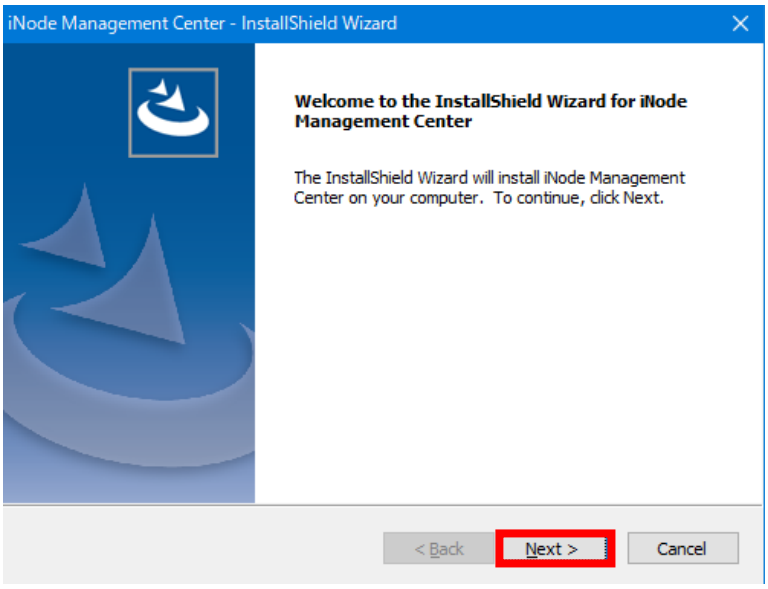
③ サーバーとの接続が完了しました。



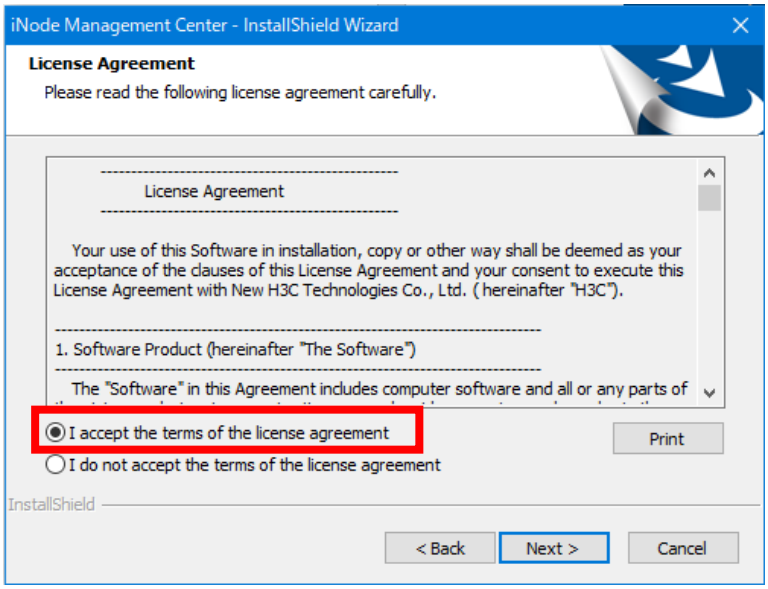
④ サーバーとの接続を切るには Disconnect ボタンをクリックします。

付録 1. iNode クライアントのインストール

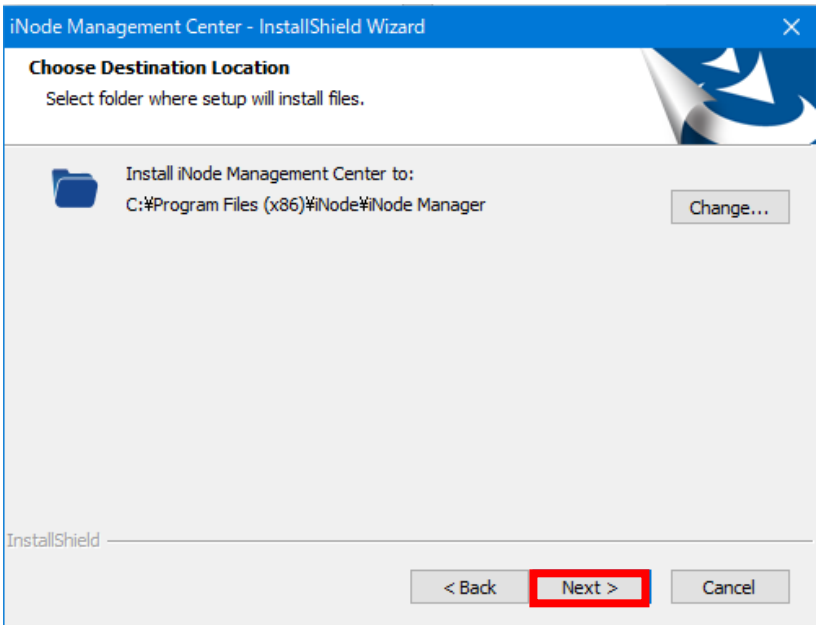
iNode Management center のインストール。



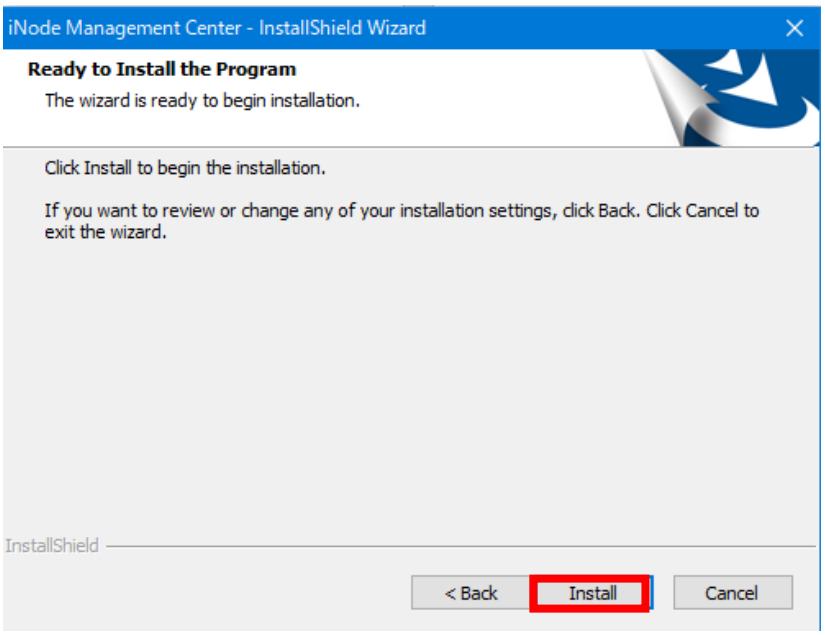
① ライセンス規約に承諾



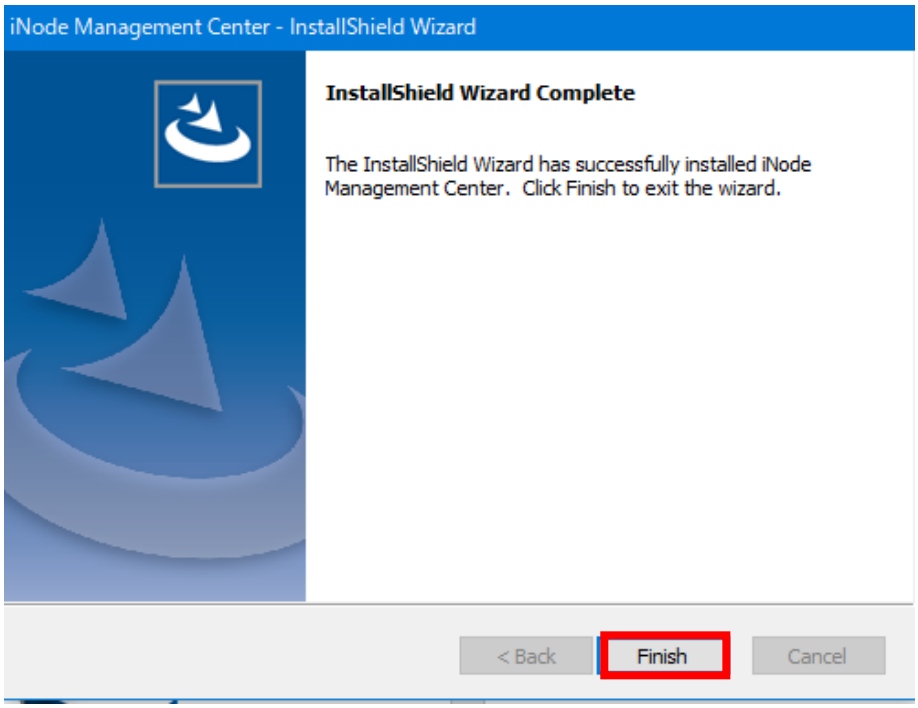
② インストール場所の設定



③ インストールの開始



④ iNode Management Center インストールの完了

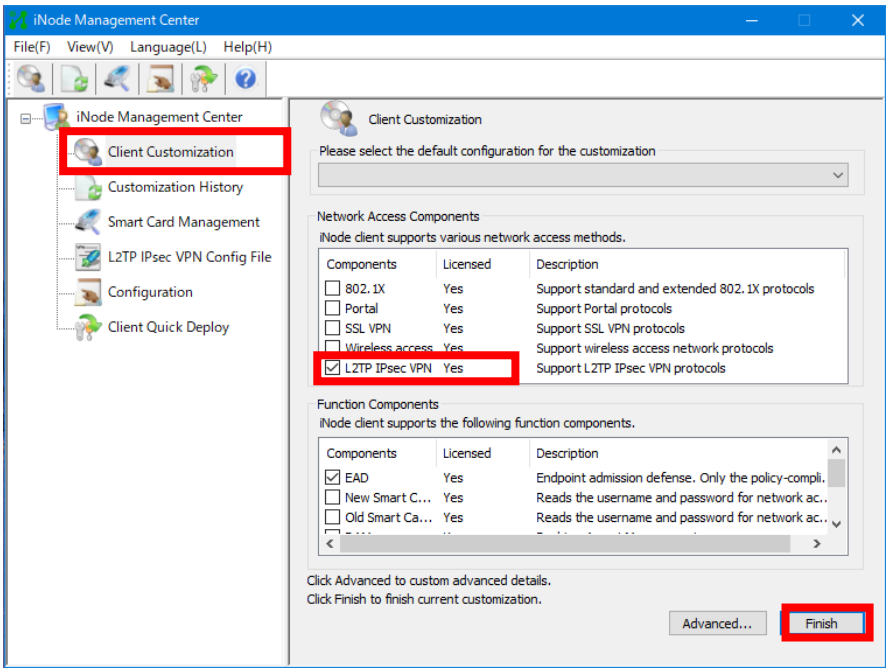


iNode Client インストールパッケージの作成

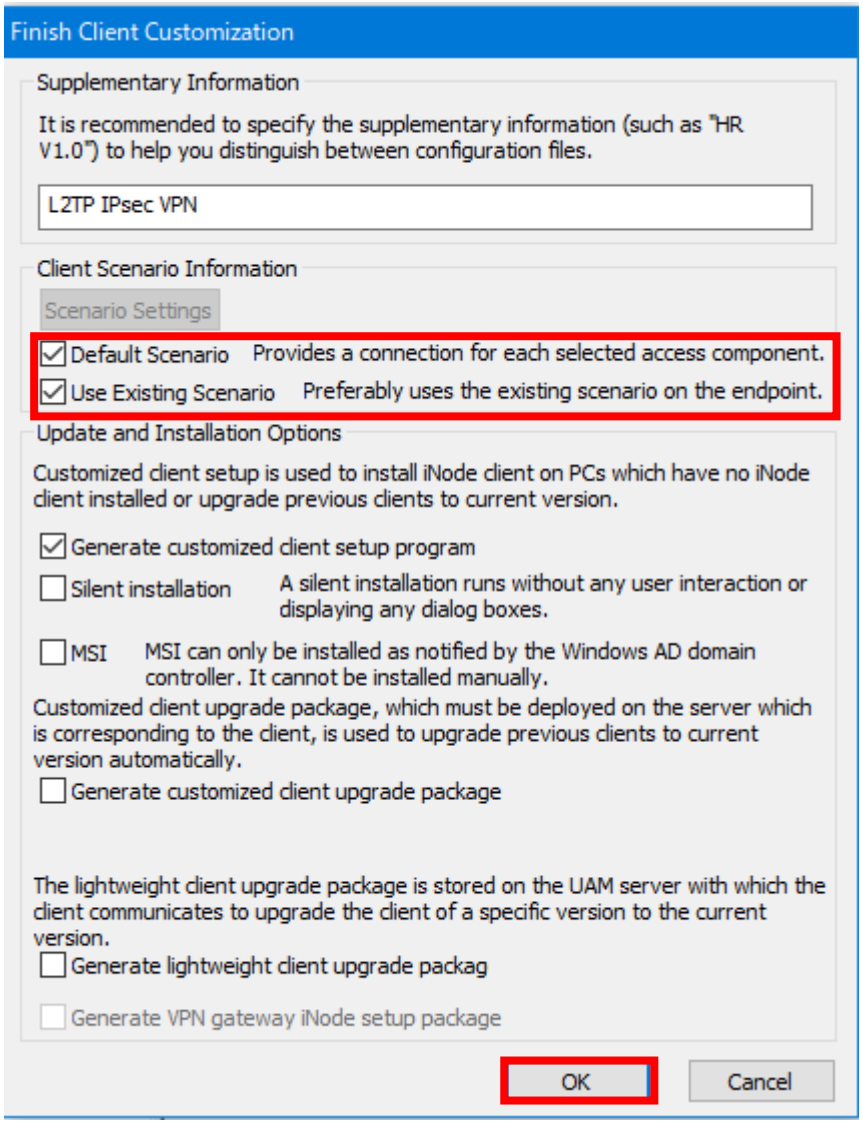
① iNode Management Center の起動

② L2TP の iNode Client をインストールします。

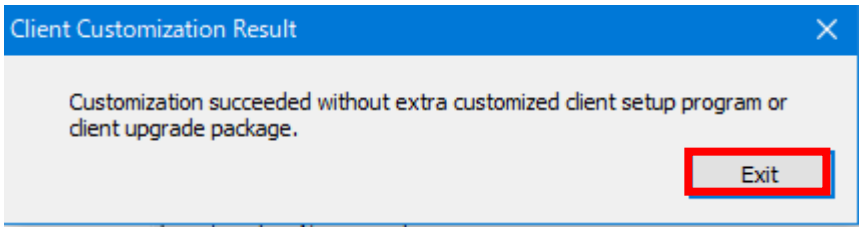
Network Access Component で、L2TP IPsec VPN のみにチェックをいれて、
Finish をクリックします。



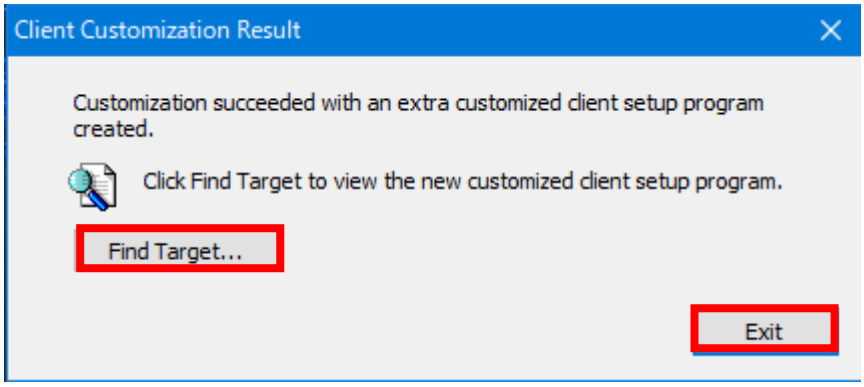
③ インストールされるパッケージに名前を付け、Client Scenario Information を Default Scenario, Use existing Scenario にチェックして OK をクリックします。



④ L2TP IPsec VPN Client のインストールパッケージが作成できましたので、Exit をクリックします。

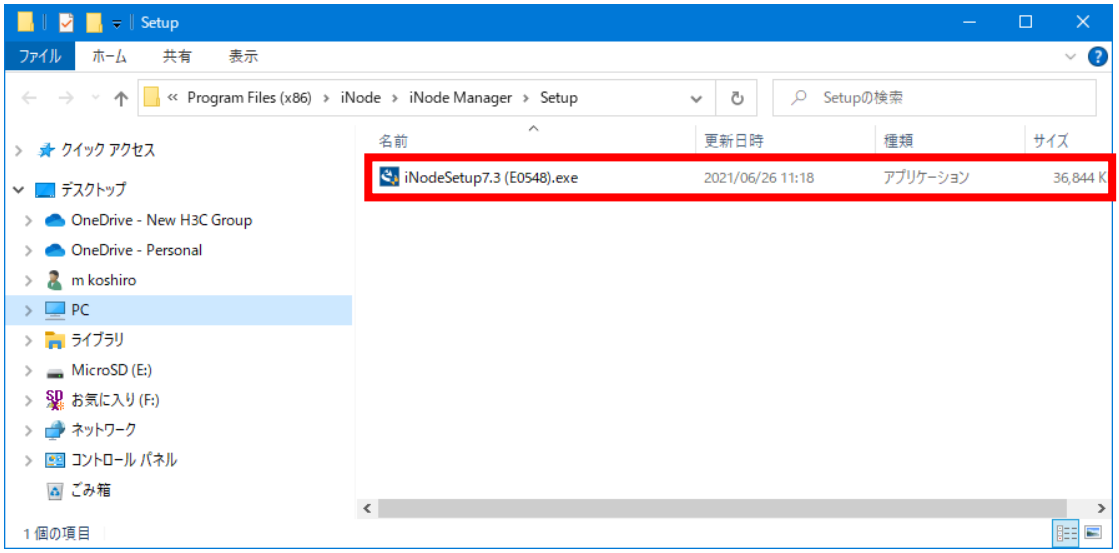


⑤ Client Customization Result ウインドウが表示されますので、Find Target をクリックして、iNode Clilent のインストールプログラムの場所を確認します。



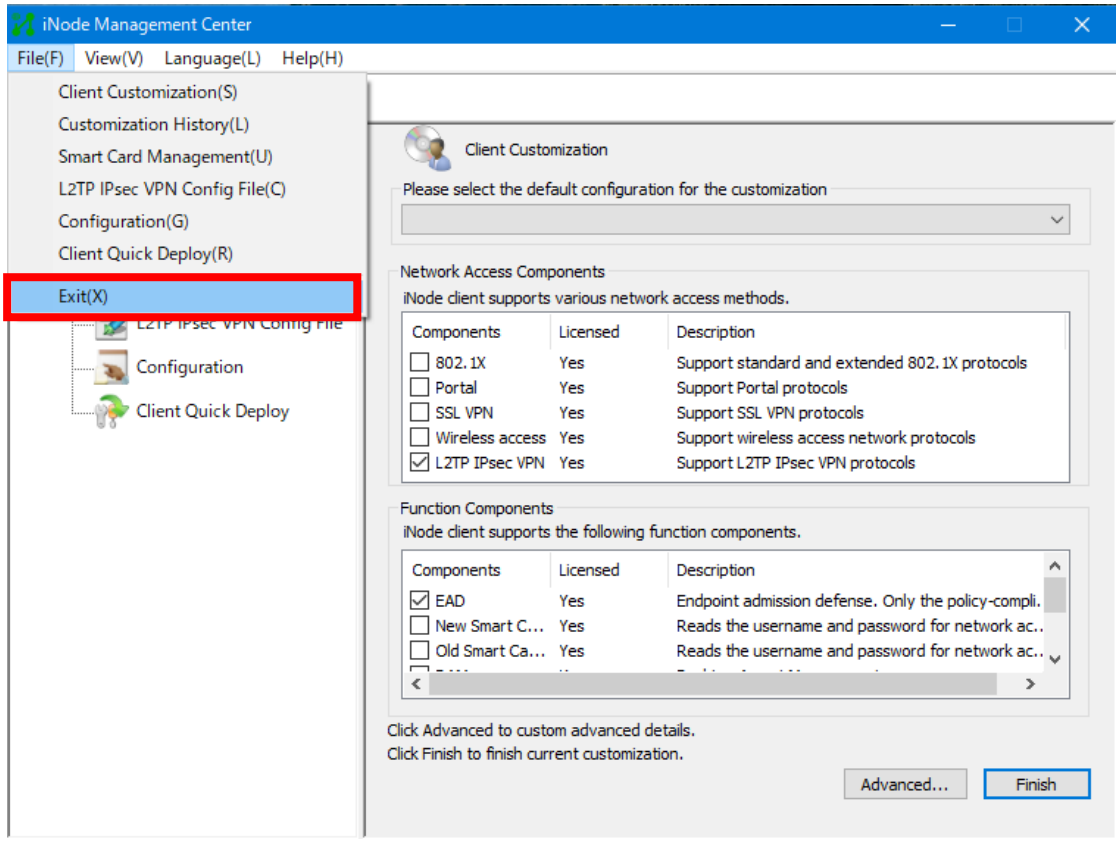
⑥ iNode Clilent のインストールプログラムの場所です。

C:\Program Files(x86)\iNode\iNode Manager\Setup



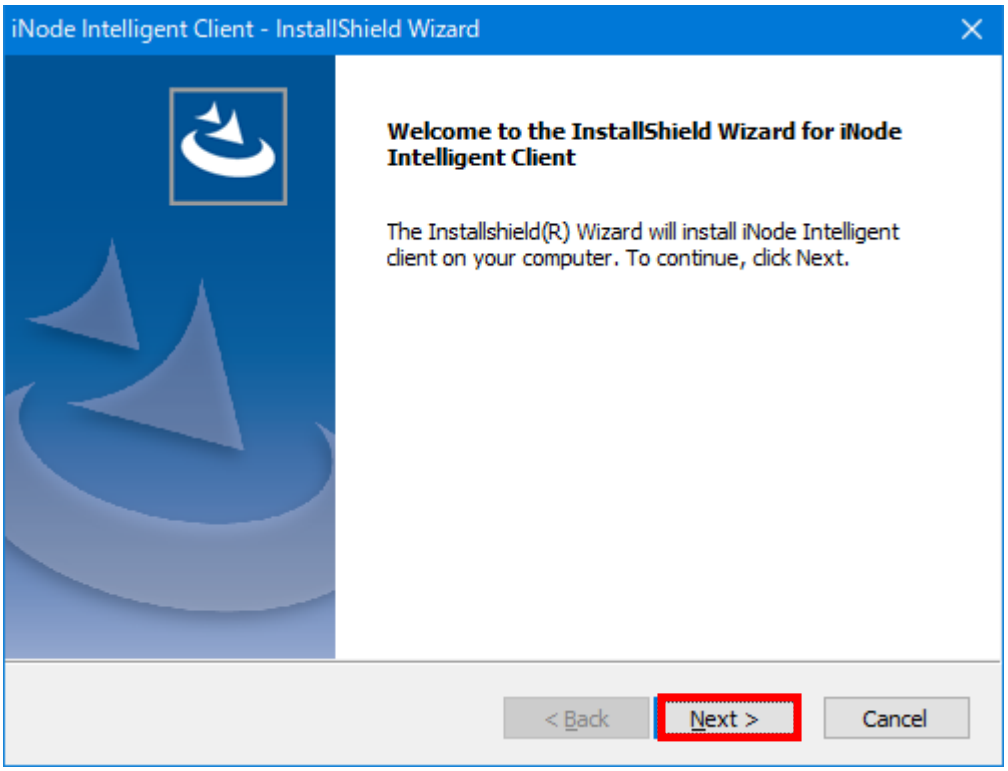
⑦ 上記 Client Customization Result ウインドウで、Exit をクリックします。

⑧ **iNode Management Center は File(F)メニューから Exit して終了します。**

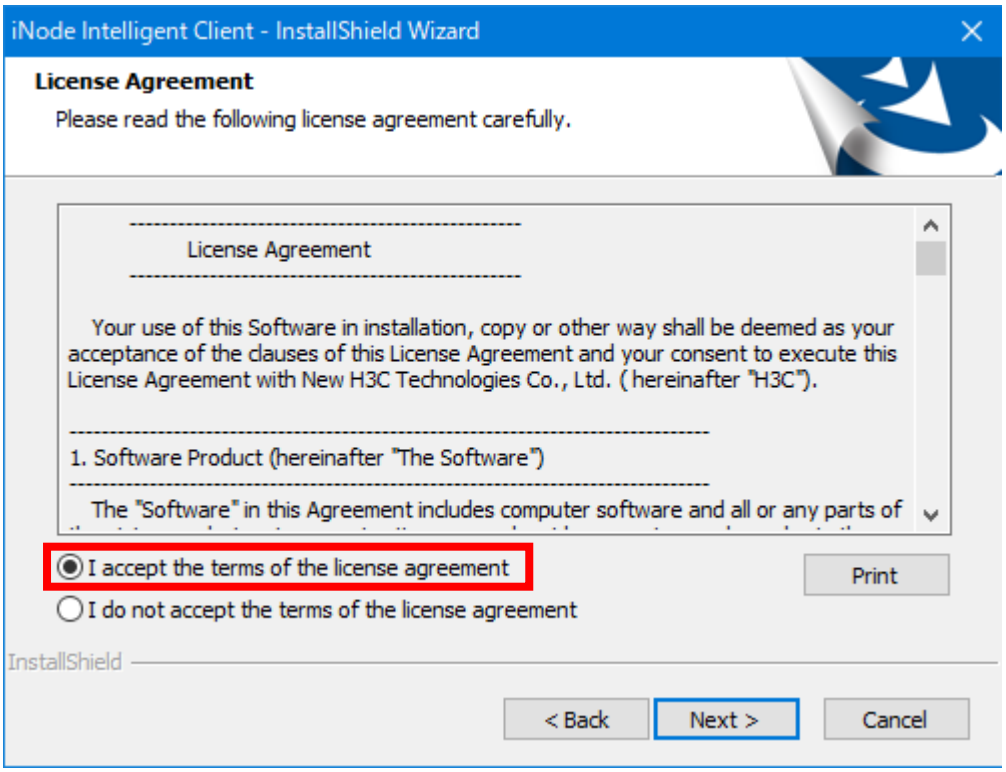


iNode クライアントのインストール

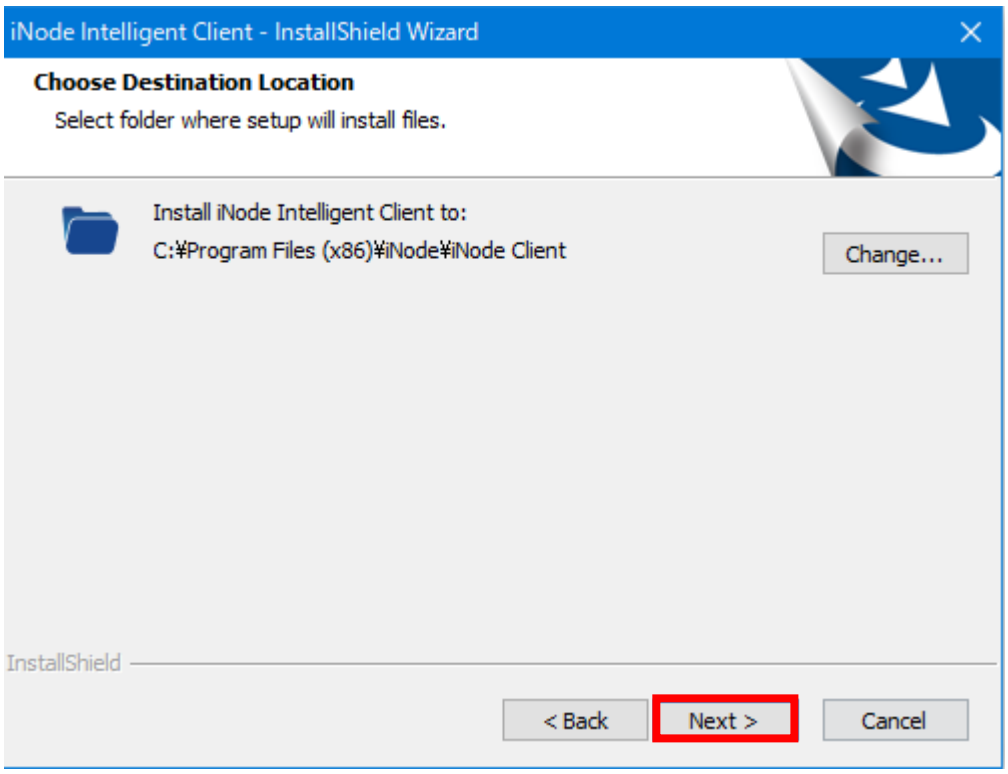
① **iNodeSetup7.3(E05048).exe をダブルクリックして起動します。**



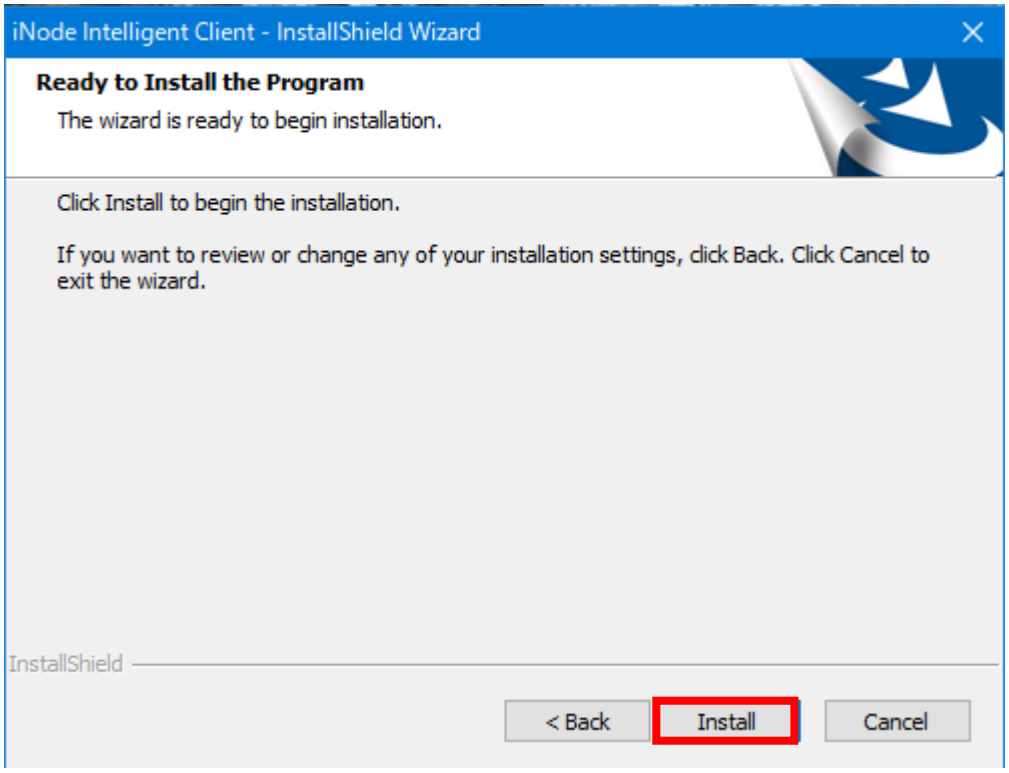
② **ライセンス規約を承認します。**



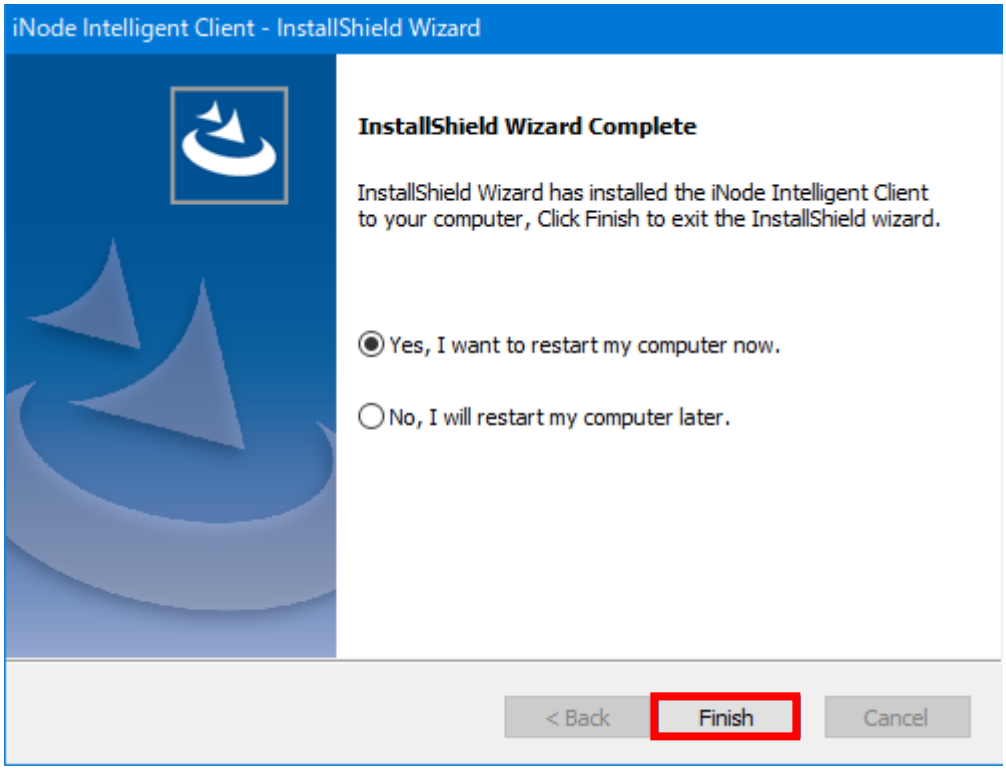
③ iNode Client のインストールされる場所を確認して、Next をクリックします。
C:\Program Files(x86)\iNode\iNode Client



④ Install ボタンをクリックしてインストールを始めます。



⑤ インストールが完了しました。



補足：デスクトップには iNode Client を起動するためのアイコンが作成されます。

Finish をクリックして、Windows を再起動後、クライアントを開始します。
クライアントの設定は、前記「4. クライアント側の設定 」をご覧ください。

付録 2. SecPathF1020 側の設定例

```
#
version 7.1.064, Release 9345P14
#
 sysname H3C
#
context Admin id 1
#
 irf mac-address persistent timer
 irf auto-update enable
 undo irf link-delay
 irf member 1 priority 1
#
 ip pool l2tp1 192.168.10.11 192.168.10.253
#
 password-recovery enable
#
vlan 1
#
controller Cellular1/0/0
#
interface Virtual-Template1
 ppp authentication-mode pap
 remote address pool l2tp1
 ip address 192.168.10.1 255.255.255.0
#
interface NULL0
#
interface GigabitEthernet1/0/0
 port link-mode route
 ip address 192.168.30.1 255.255.255.0
 nat outbound 3000
 ipsec apply policy 1
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.20.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
#
```

```
interface GigabitEthernet1/0/3
 port link-mode route
#
interface GigabitEthernet1/0/4
 port link-mode route
#
interface GigabitEthernet1/0/5
 port link-mode route
#
interface GigabitEthernet1/0/6
 port link-mode route
#
interface GigabitEthernet1/0/7
 port link-mode route
#
interface GigabitEthernet1/0/8
 port link-mode route
#
interface GigabitEthernet1/0/9
 port link-mode route
#
interface GigabitEthernet1/0/10
 port link-mode route
#
interface GigabitEthernet1/0/11
 port link-mode route
#
interface GigabitEthernet1/0/12
 port link-mode route
#
interface GigabitEthernet1/0/13
 port link-mode route
#
interface GigabitEthernet1/0/14
 port link-mode route
#
interface GigabitEthernet1/0/15
 port link-mode route
#
interface GigabitEthernet1/0/16
 port link-mode route
#
interface GigabitEthernet1/0/17
```

```
 port link-mode route
#
interface GigabitEthernet1/0/18
 port link-mode route
#
interface GigabitEthernet1/0/19
 port link-mode route
#
interface GigabitEthernet1/0/20
 port link-mode route
#
interface GigabitEthernet1/0/21
 port link-mode route
#
interface GigabitEthernet1/0/22
 port link-mode route
#
interface GigabitEthernet1/0/23
 port link-mode route
#
security-zone intra-zone default permit
#
security-zone name Local
#
security-zone name Trust
 import interface GigabitEthernet1/0/1
#
security-zone name DMZ
#
security-zone name Untrust
 import interface Virtual-Template1
#
security-zone name Management
 import interface GigabitEthernet1/0/0
#
 scheduler logfile size 16
#
line class aux
 user-role network-operator
#
line class console
 authentication-mode scheme
 user-role network-admin
```

```
#
line class usb
 user-role network-admin
#
line class vty
 user-role network-operator
#
line aux 0
 user-role network-admin
#
line con 0
 user-role network-admin
#
line vty 0 63
 authentication-mode scheme
 user-role network-admin
#
 ssh server enable
#
 arp ip-conflict log prompt
#
ldap server rem-system
 login-dn CN=Administrator,CN=Users,DC=ad,DC=rem-system,DC=com,DC=local
 search-base-dn DC=ad,DC=rem-system,DC=com,DC=local
 ip 192.168.20.10
 login-password simple test
 protocol-version v2
#
ldap scheme user_db
 authentication-server rem-system
#
domain system
#
 domain default enable system
#
role name level-0
 description Predefined level-0 role
#
role name level-1
 description Predefined level-1 role
#
role name level-2
 description Predefined level-2 role
```

```
#
role name level-3
 description Predefined level-3 role
#
role name level-4
 description Predefined level-4 role
#
role name level-5
 description Predefined level-5 role
#
role name level-6
 description Predefined level-6 role
#
role name level-7
 description Predefined level-7 role
#
role name level-8
 description Predefined level-8 role
#
role name level-9
 description Predefined level-9 role
#
role name level-10
 description Predefined level-10 role
#
role name level-11
 description Predefined level-11 role
#
role name level-12
 description Predefined level-12 role
#
role name level-13
 description Predefined level-13 role
#
role name level-14
 description Predefined level-14 role
#
user-group system
#
local-user admin class manage
 password hash
$h$6$UbIhNnPevyKUwfpm$LqR3+yg1IjNct39MkOR0H0iQXLkYB3jMqM4vbAeoXOhbabI
IFnjJPEGR00YiYA1Sz4LiY3FmEdru2fOLMb1shQ==
```

```
 service-type ssh terminal https
 authorization-attribute user-role level-3
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
local-user client class network
 password cipher $c$3$bUwUitzIeC0lGT/e2EZdVgyMcNcWD3QwxQ==
 service-type ppp
 authorization-attribute user-role network-operator
#
session statistics enable
#
 ipsec logging negotiation enable
#
ipsec transform-set 1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec transform-set 2
 encapsulation-mode transport
 esp encryption-algorithm aes-cbc-128
 esp authentication-algorithm sha1
#
ipsec transform-set 3
 encapsulation-mode transport
 esp encryption-algorithm aes-cbc-256
 esp authentication-algorithm sha1
#
ipsec transform-set 4
 encapsulation-mode transport
 esp encryption-algorithm des-cbc
 esp authentication-algorithm sha1
#
ipsec transform-set 5
 encapsulation-mode transport
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm sha1
#
ipsec transform-set 6
 encapsulation-mode transport
 esp encryption-algorithm aes-cbc-192
 esp authentication-algorithm sha1
#
```

```
ipsec policy-template 1 1
 transform-set 1 2 3 4 5 6
 local-address 192.168.30.1
 ike-profile 1
#
ipsec policy 1 1 isakmp template 1
#
l2tp-group 1 mode lns
 allow l2tp virtual-template 1
 undo tunnel authentication
#
 l2tp enable
#
 ike logging negotiation enable
#
ike profile 1
 keychain 1
 exchange-mode aggressive
 local-identity fqdn lns
 match remote identity address 0.0.0.0 0.0.0.0
 match remote identity fqdn inode
 match local address GigabitEthernet1/0/0
 proposal 1 2 3 4 5 6
#
ike proposal 1
 dh group2
 authentication-algorithm md5
#
ike proposal 2
 encryption-algorithm 3des-cbc
 dh group2
 authentication-algorithm md5
#
ike proposal 3
 encryption-algorithm 3des-cbc
 dh group2
#
ike proposal 4
 encryption-algorithm aes-cbc-256
 dh group2
#
ike proposal 5
 dh group2
```

```
#
ike proposal 6
 encryption-algorithm aes-cbc-192
 dh group2
#
ike keychain 1
 match local address GigabitEthernet1/0/0
 pre-shared-key address 0.0.0.0 0.0.0.0 key cipher
$c$3$ZS5ysc5WxbGXqQ4HAqHMVJPEYd83fKs=
#
 ip https enable
 webui log enable
#
 loadbalance isp file flash:/lbispinfo_v1.5.tp
#
security-policy ip
 rule 0 name 1
  action pass
 rule 1 name 0
  action pass
  counting enable
  source-zone Local
  source-zone Trust
  source-zone Untrust
  destination-zone Local
  destination-zone Trust
  destination-zone Untrust
#
```