

SPARC M12/M10 リモートデスクトップを 使ってみよう

～リモートデスクトップ
構築ガイド～



2019年9月

第1.2版

富士通株式会社

■ 使用条件

- 著作権・商標権・その他の知的財産権について

コンテンツ（文書・画像・音声等）は、著作権・商標権・その他の知的財産権で保護されています。

本コンテンツは、個人的に使用する範囲でプリントアウトまたはダウンロードできます。ただし、これ以外の利用（ご自分のページへの再利用や他のサーバへのアップロード等）については、当社または権利者の許諾が必要となります。

- 保証の制限

本コンテンツについて、当社は、その正確性、商品性、ご利用目的への適合性等に関して保証するものではなく、そのご利用により生じた損害について、当社は法律上のいかなる責任も負いかねます。本コンテンツは、予告なく変更・廃止されることがあります。

- 輸出または提供

本製品を輸出または提供する場合は、外国為替および外国貿易法および米国輸出管理関連法規等の規制をご確認のうえ、必要な手続きをおとりください。

- 本書で使用するフリーウェアのサポートについて

- サーバで使用する Solaris に同梱されたフリーウェア(VNC サーバ)のサポートは、富士通サポートデスク契約が前提のベストエフォート対応となり、公開情報および富士通が保持する情報で解決しない場合、それ以上の原因究明および回避策は提供しません。
- クライアントの Windows PC で使用するフリーウェア(VNC クライアント・ターミナルエミュレータ)は、サポート対象外となります。

■ 商標について

- UNIX は、米国およびその他の国におけるオープン・グループの登録商標です。
- SPARC M12/M10、SPARC64 およびすべての SPARC 商標は、米国 SPARC International, Inc.のライセンスを受けて使用している、同社の米国およびその他の国における商標または登録商標です。
- Oracle と Java は、Oracle Corporation およびその子会社、関連会社の米国およびその他の国における登録商標です。
- Microsoft、Windows、Windows Server は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- その他各種製品名は、各社の製品名称、商標または登録商標です。

はじめに

本書の内容

- 本書は、SPARC M12/M10 におけるリモートデスクトップの環境構築・接続手順、およびリモートデスクトップで使用するリモートコンソールの接続手順について記載しています。
- Oracle Solaris 11.3 のリモートデスクトップに関するドキュメントは、以下を参照してください。
Oracle Solaris 11.3 デスクトップ管理者ガイド
https://docs.oracle.com/cd/E62101_01/html/E62852/
「第 12 章 X Window System の操作」
→ X11 ディスプレイへのアクセス
→ ゲストのグラフィカルログインを提供するように VNC を設定する方法
- SPARC M12/M10 のリモートコンソールに関するドキュメントは、以下を参照してください。
XSCF リファレンスマニュアル(XCP 版数別一覧)
<https://www.fujitsu.com/jp/products/computing/servers/unix/sparc/downloads/manual/xscf-ref/>
「システム管理コマンド」
→ console

留意事項

- Solaris 11.4、Solaris 11.3 および Solaris 10 の機能に基づいて作成しています。
- 本書に記載の設定値(ホスト名、IP アドレスなど)は参考例です。手順実行時には、システム環境に応じて読み替えてください。

本書での表記

- 以下の用語は略称を用いて表記する場合があります。

略称	正式名称
Solaris	Oracle Solaris
OVM	Oracle VM Server for SPARC
SRU	Support Repository Update
VNC	Virtual Network Computing
GUI またはデスクトップ	グラフィカルユーザーインターフェース
CUI またはコンソール	キャラクタユーザーインターフェース
GPU	グラフィックスコントローラー
XSCF	eXtended System Control Facility
SSH	Secure Shell
GNOME	GNU Network Object Model Environment
GDM	GNOME Display Manager
CDE	Common Desktop Environment
JDS	Java Desktop System

本書内のプロンプト表記について

- オペレーションの説明に記載しているプロンプトは、以下の表記により操作する環境や権限を区別しています。

プロンプト	操作環境・権限
XSCF>	XSCF のシェル
\$	Solaris の一般ユーザーシェル
#	Solaris のスーパーユーザーシェル
C:¥>	Windows のコマンドプロンプト
PS C:¥>	Windows の PowerShell

- 実際のコマンド入力は、太字で記述しています。

```
# svcadm enable gdm
```

目 次

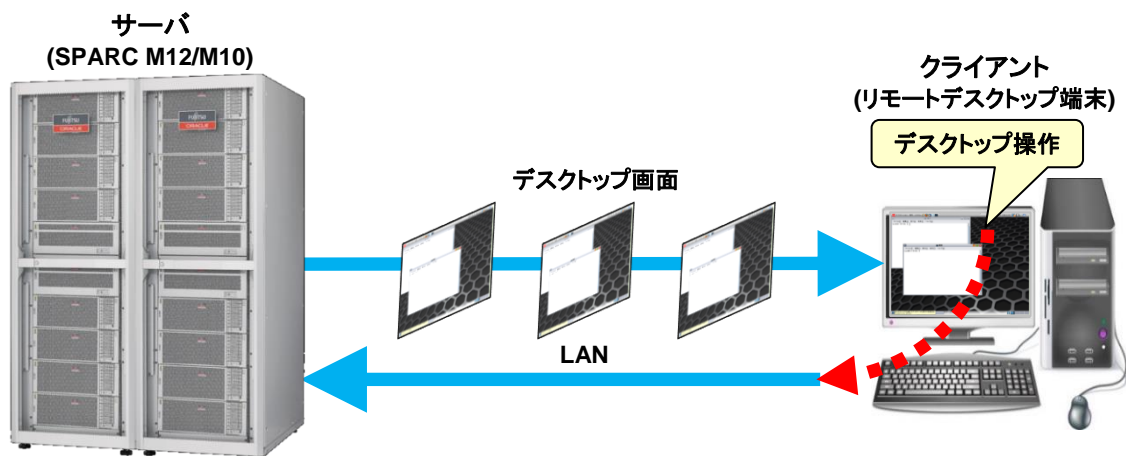
1. 概要	1
1.1. ローカル環境とリモート環境の比較	2
1.1.1. デスクトップ構成と操作	2
1.1.2. 仮想化環境におけるデスクトップの動作可否	5
1.1.3. デスクトップ仕様	6
1.1.4. セキュリティ対策の検討	7
1.1.5. リモートデスクトップの体感性能(参考)	8
1.2. リモート環境のセキュリティ対策	9
1.2.1. リモートデスクトップ	9
1.2.2. リモートコンソール	11
2. リモートデスクトップのシステム要件	12
2.1. サーバ動作環境	12
2.2. クライアント検証環境	13
2.3. 使用リソース(参考値)	14
3. リモートデスクトップの環境構築・接続手順	15
3.1. 手順の流れ	15
3.1.1. リモートデスクトップのサーバ環境構築手順	15
3.1.2. リモートデスクトップのクライアント環境構築・接続手順	18
3.2. リモートデスクトップのサーバ環境構築手順	20
3.2.1. Solaris 11 gdm サービスの場合	20
3.2.2. Solaris 10 cde-login サービスの場合	24
3.2.3. Solaris 10 gdm2-login サービスの場合	28
3.3. リモートデスクトップのクライアント環境構築・接続手順	31
3.3.1. Tera Term の SSH ポートフォワーディングを使用する場合	31
3.3.2. PuTTY の SSH ポートフォワーディングを使用する場合	37
3.3.3. リモートデスクトップ接続	42
4. リモートコンソールの接続手順	49
4.1. Tera Term の場合	49

4.2. PuTTY の場合	53
付録 A リモートデスクトップのデータ暗号化確認手順	56
A.1 TigerVNC によるデータ暗号化の場合	56
A.2 SSH ポートフォワーディングによるデータ暗号化の場合	58
付録 B リモート接続手順の自動化サンプルスクリプト	59
B.1 リモートデスクトップ接続	59
B.1.1 SSH ポートフォワーディング接続用 Tera Term マクロスクリプト	59
B.1.2 TigerVNC 用 Windows バッチファイルスクリプト	63
B.1.3 TigerVNC 用 Windows PowerShell スクリプト	68
B.2 リモートコンソール接続	74
B.2.1 リモートコンソール接続用 Tera Term マクロスクリプト	74
B.2.2 GNOME 内でのリモートコンソール接続用シェルスクリプト	77
付録 C トラブルシューティング	83
C.1 サーバで検出したトラブル	83
C.1.1 xvnc-inetd サービス起動時に、サービスの状態が"maintenance"に遷移する	83
C.1.2 サービス起動時に、サービスの状態が"online"に遷移しない	84
C.1.3 サービス停止時に、サービスの状態が"disabled"に遷移しない	84
C.1.4 サービスの状態が"degraded"、"maintenance"、または"offline"となっている	84
C.2 クライアントで検出したトラブル	86
C.2.1 Tera Term による SSH 接続時に、セキュリティ警告が表示される(1)	86
C.2.2 Tera Term による SSH 接続時に、セキュリティ警告が表示される(2)	88
C.2.3 PuTTY による SSH 接続時に、"Security Alert"が表示される(1)	90
C.2.4 PuTTY による SSH 接続時に、"Security Alert"が表示される(2)	91
C.2.5 TigerVNC 使用時に、"Connection timed out"が表示される	93
C.2.6 TigerVNC 使用時に、"writeTLS:(unknown error code)(10054)"が表示される	93
C.2.7 TigerVNC 使用時に、"(retry_send_packet:10054)"が表示される	93
C.2.8 TigerVNC 使用時に、"Connection refused"が表示される	95
C.2.9 TigerVNC 接続時に、"No matching security types"が表示される	97
C.2.10 TigerVNC 接続時に、"No supported security types"が表示される	97
C.2.11 TigerVNC 接続時に、ログイン画面が表示されない	99
C.2.12 gdm2-login サービス使用時に、TigerVNC が接続途中で終了する	101

C.2.13 TigerVNC 使用時に、"Connection reset by peer (10054)"が表示される	102
C.2.14 TigerVNC で接続した GNOME 内の入力動作が遅れる	103
C.2.15 cde-login サービスで JDS を使用時に、リモートデスクトップ画面が正しく表示されない ..	104
改版履歴	105

1. 概要

リモートデスクトップとは、Windows PC 等のクライアント(リモートデスクトップ端末)から、LAN で接続したサーバ(SPARC M12/M10)のデスクトップを操作する機能のことをいいます。



本書では、Solaris のリモートデスクトップを制御するソフトウェアとして VNC を使用した場合の環境構築・接続手順、およびリモートデスクトップで使用するリモートコンソールの接続手順について記載します。

1.1. ローカル環境とリモート環境の比較

デスクトップを使用する環境には、ローカル環境とリモート環境があります。

リモートデスクトップを使用する環境(リモート環境)と、サーバに直接ディスプレイ・キーボード・マウスを接続する環境(ローカル環境)には、使用するハードウェアやソフトウェア、仮想環境での動作、ディスプレイの最大解像度などの違いがあります。

リモートデスクトップを構築するうえで、ローカル環境からリモート環境への移行も考慮し、本項では両環境の比較をデスクトップ観点で行います。

1.1.1. デスクトップ構成と操作

ローカル環境とリモート環境のデスクトップ構成と操作を比較します。

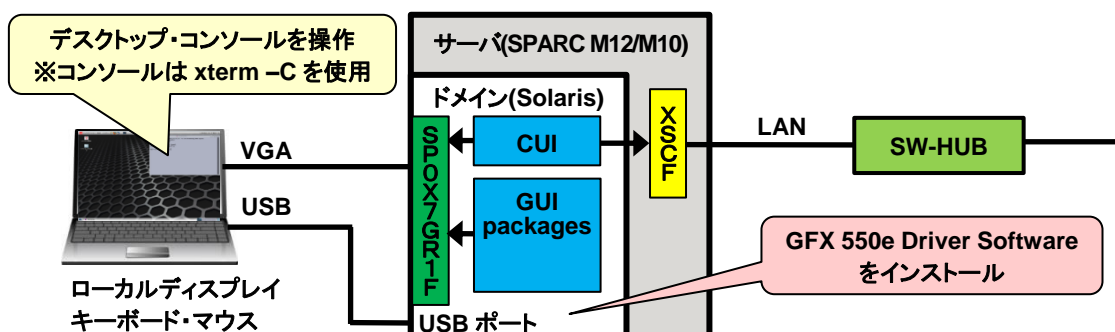
両環境のデスクトップを使用するうえでのコンソールについても比較します。

● ローカル環境

ローカル環境では、グラフィックスカード(SP0X7GR1F)を SPARC M12/M10 に実装後、ローカルディスプレイとキーボード・マウスを、それぞれグラフィックスカードと USB ポートに接続します。

さらに、グラフィックスカード添付のソフトウェア(GFX 550e Driver Software)を SPARC M12/M10 にインストールし、この環境で Solaris のデスクトップとコンソールを操作します。

デスクトップ内のコンソールには、xterm -C を使用します。



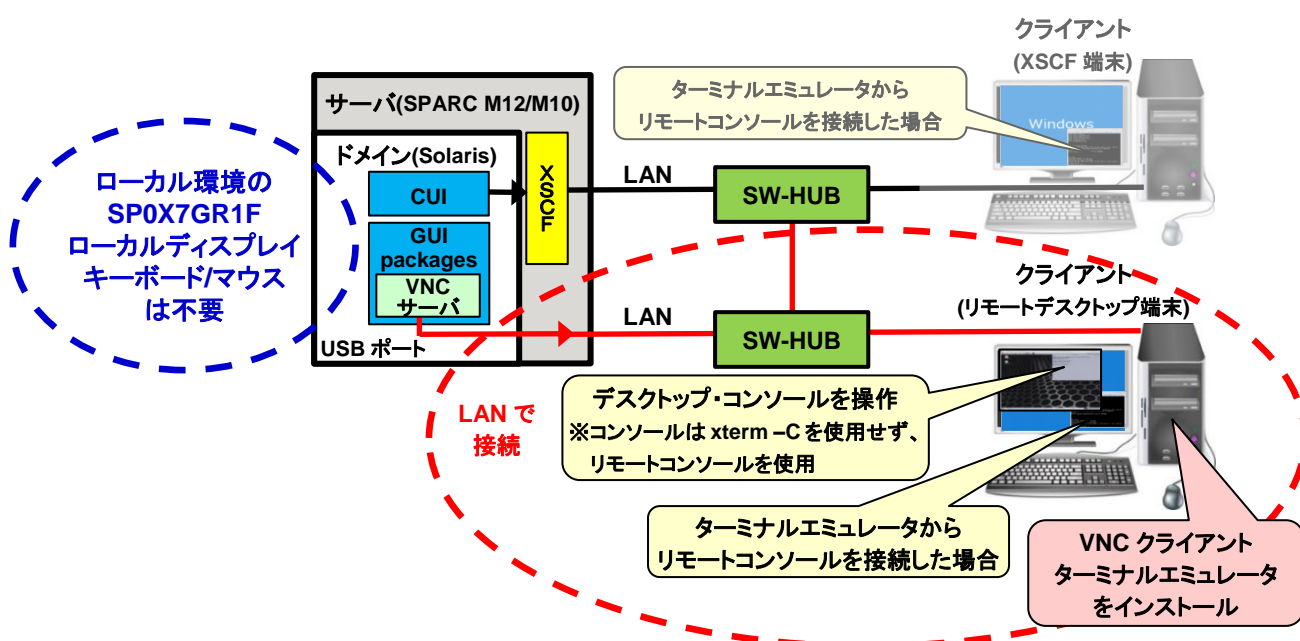
● リモート環境

リモート環境では、ローカル環境で使用していたハードウェアの代わりに、LAN を介してリモートデスクトップ端末と SPARC M12/M10 を接続します。

さらに、VNC クライアントとターミナルエミュレータのソフトウェアをリモートデスクトップ端末にインストールし、この環境で Solaris のデスクトップとコンソールを操作します。

デスクトップ内のコンソールには、`xterm -C` を使用せず、XSCF に接続したリモートコンソールを使用します。

リモートコンソールは、同一の SPARC M12/M10 に接続したリモートデスクトップ端末または XSCF 端末のターミナルエミュレータから接続できます。



● デスクトップ構成の比較

以下は、デスクトップで使用するハードウェアとソフトウェアの構成をローカル環境とリモート環境で比較した表です。

デスクトップ構成		ローカル環境	リモート環境
ハードウェア		グラフィックスカード (SP0X7GR1F)	Windows PC
		ディスプレイ	
		グラフィックスケーブル	LAN
		キーボード・マウス	
ソフトウェア	デスクトップ(GUI)	GFX 550e Driver Software	VNC (TigerVNC, RealVNC など)
	コンソール(CUI)		ターミナルエミュレータ (Tera Term, PuTTY など)

1.1.2. 仮想化環境におけるデスクトップの動作可否

仮想化環境におけるデスクトップの動作可否についてローカル環境とリモート環境で比較した表を以下に示します。

仮想化環境		デスクトップの動作可否	
		ローカル環境	リモート環境
OVM	制御ドメイン	○	○
	I/O ルートドメイン・I/O ドメイン	×	○
	ゲストドメイン	×	○
ゾーン(*1)	ノングローバルゾーン	×	○
	カーネルゾーン	×	○

○:動作可、×:動作不可

*1:Solaris 11.1 を使用する場合、SRU14021(SRU11.1.16.5.0)以降の適用が必要です。

1.1.3. デスクトップ仕様

ローカル環境とリモート環境のデスクトップ仕様を下表で比較します。

リモート環境のデスクトップ仕様は、使用するデスクトップ端末に依存しますが、下表は FMV ESPRIMO DH シリーズの GPU(Intel UHD Graphics 630)を例にしています。

デスクトップ仕様		ローカル環境 (SP0X7GR1F)	リモート環境 (Intel UHD Graphics 630)
シングルディスプレイの 最大解像度	アナログ	1920x1200	1920x1200
	デジタル	1280x1024	3840x2160
マルチディスプレイの 最大台数(上段) および 最大解像度(下段)	アナログ	2 台	未サポート(*1)
		1600x1200 x 2 台	
	デジタル	2 台	3 台
		1280x1024 x 2 台	3840x2160 x 2 台 1920x1200 x 1 台
マルチデスクトップの 最大デスクトップ数	ディスプレイ 1 台内に デスクトップを重複して 表示する場合	不可	10 デスクトップ(*2) (*3)
	ディスプレイ 1 台ごとに デスクトップを独立して 表示する場合	未サポート	3 デスクトップ(*2)

*1: 使用するモデルによっては、アナログのマルチディスプレイをサポートするモデルもあります。

*2: 各デスクトップに異なるユーザーでログインできます。

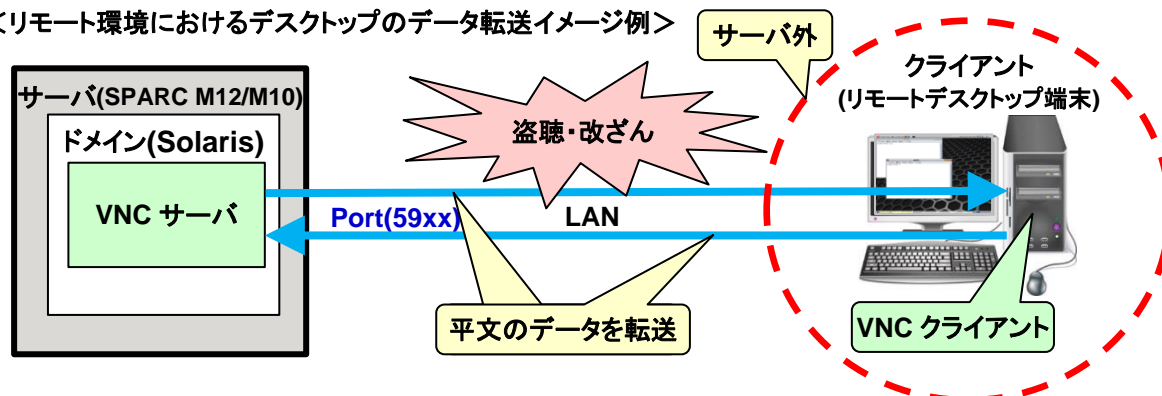
*3: 以下の環境条件で測定した接続実績値です。

環境条件		内容
サーバ	本体装置	SPARC M10-4
	OS 版数	Solaris 11.3 SRU18081(SRU11.3.35.6.0)
クライアント	本体装置	Windows PC
	OS 版数	Windows 7 Pro SP1 32bit
	使用 VNC ソフトウェア版数	TigerVNC Viewer Version 1.8.0
データ暗号化手段		TigerVNC の TLS 暗号化

1.1.4. セキュリティ対策の検討

ローカル環境では、サーバとディスプレイ間だけに閉じて平文のデータを転送するため、セキュリティ問題は発生しませんが、リモート環境では、LAN を介してサーバ外のクライアントと平文のデータを転送するため、盗聴や改ざんなどのセキュリティ問題が発生する恐れがあります。

＜リモート環境におけるデスクトップのデータ転送イメージ例＞



このため、リモート環境ではセキュリティ対策を検討する必要があります。

リモート環境でイントラネットを使用する場合は、企業内などの閉じた環境になるため、一般的にはセキュリティ対策は不要ですが、インターネットを使用する場合は、グローバルな環境になるため、セキュリティ対策が必要となります。

リモート環境におけるセキュリティ対策の手段については、「[1.2 リモート環境のセキュリティ対策](#)」を参照してください。

1.1.5. リモートデスクトップの体感性能(参考)

本項では、下表の環境条件でリモートデスクトップを操作したときの体感性能について記載します。

測定条件		内容
サーバ	本体装置	SPARC M10-4
	OS 版数	Solaris 11.3 SRU18081(SRU11.3.35.6.0)
	CPU	SPARC64 X 2.8GHz 1 プロセッサ 2 コア(計 4 スレッド)
	メモリ	32GB
	LAN	1000Mbps(*1)
クライアント	本体装置	Windows PC
	OS 版数	Windows 7 Pro SP1 32bit
	CPU	Intel Core i3 M350 2.27GHz 1 プロセッサ 2 コア(計 4 スレッド)
	メモリ	4GB
	LAN	100Mbps(*1)
デスクトップの解像度		1280x1024
データ暗号化手段		TigerVNC の TLS 暗号化

*1:スイッチングハブと実際に接続したときのリンク速度です。

ローカル環境のデスクトップ操作を基準にしたときのリモートデスクトップの体感性能を下表に示します。

デスクトップ操作	リモートデスクトップの体感性能
ログイン～デスクトップ表示	○
xterm 上の vi スクロール(*2)	○
ウィンドウ移動	○
ウィンドウ拡縮	○

○:劣化なし、×:劣化あり

*2:vi でのスクロールに使用したファイルの行数(サイズ)は、1000 行(81000 バイト)です。

1.2. リモート環境のセキュリティ対策

リモート環境で通信するデータは、「[1.1.4 セキュリティ対策の検討](#)」で述べたとおり、セキュリティ対策の検討が必要です。

1.2.1. リモートデスクトップ

本項では、リモートデスクトップのセキュリティ対策として、下表のデータ暗号化手段について説明します。

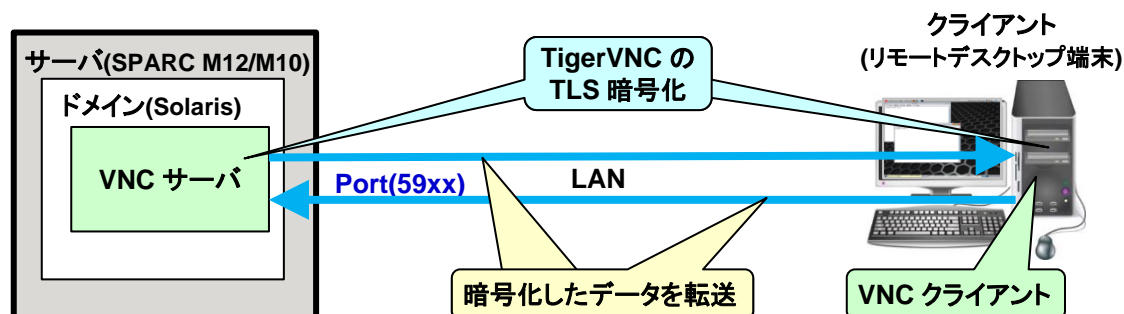
以下は、推奨するデータ暗号化手段を OS 版数ごとに整理した表です。

データ暗号化手段	Solaris 11.4 以降	Solaris 11.3		Solaris 11.1 ～ Solaris 11.2 SRU15102	Solaris 10 1/13
		SRU18041 以降	SRU18032 以前		
TigerVNC の TLS 暗号化	◎	◎	—	—	—
SSH ポートフォワーディング	○	○	◎	◎	◎

◎: 推奨、○: 動作可、—: 未サポート

1) TigerVNC の TLS 暗号化

VNC ソフトウェアの一つである TigerVNC は、TLS(Transport Layer Security)による暗号化通信に対応しており、この機能を使用することで、リモート環境でもデスクトップを安全に使用することができます。



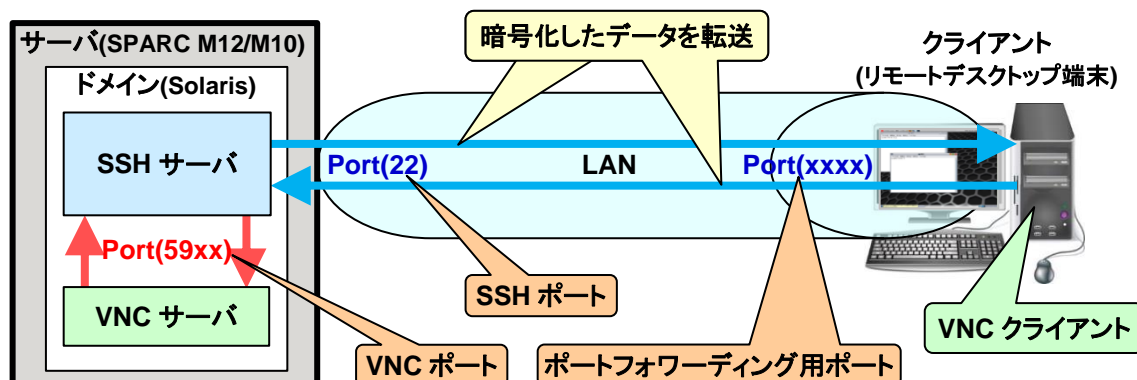
TLS 暗号化の設定手順は、「[3.2.1 Solaris 11 gdm サービスの場合 5\)](#)」および「[3.3.3 リモートデスクトップ接続 2\)](#)」を参照してください。

サーバ側の TLS 暗号化は、Solaris 11.3 SRU18041 以降でのサポートとなるため、この OS 版数を使用する場合は TigerVNC によるセキュリティ対策を推奨します。

2) SSH ポートフォワーディング

SSH ポートフォワーディングは、クライアントのポートフォワーディング用ポートと、サーバの VNC ポート間で、SSH ポートを介して暗号化したデータを転送する機能です。

この機能で通信を行えば、リモート環境でもデスクトップを安全に使用することができます。

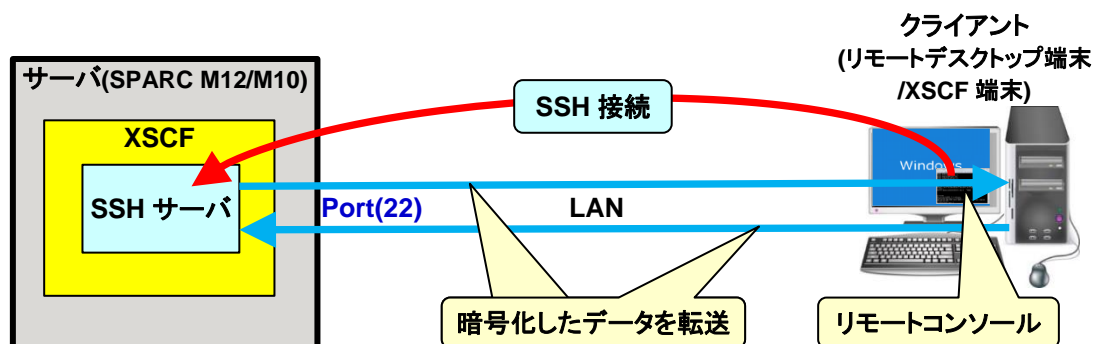


SSH ポートフォワーディングの設定手順は、「[3.3.1 Tera Term の SSH ポートフォワーディングを使用する場合](#)」または「[3.3.2 PuTTY の SSH ポートフォワーディングを使用する場合](#)」を参照してください。

SSH ポートフォワーディングによるセキュリティ対策は、Solaris 11.1～Solaris 11.3 SRU18032 または Solaris 10 1/13 の場合に使用します。

1.2.2. リモートコンソール

リモートコンソールのセキュリティ対策は、クライアントから XSCF への SSH 接続にて対応します。SSH で通信を行えばデータが暗号化され、リモート環境でもコンソールを安全に使用することができます。



XSCF への SSH 接続手順は、「[4.1 Tera Term の場合](#)」または「[4.2 PuTTY の場合](#)」を参照してください。

2. リモートデスクトップのシステム要件

2.1. サーバ動作環境

リモートデスクトップのサーバ動作環境を下表に示します。

動作環境		Solaris 11	Solaris 10
本体装置		SPARC M12/M10	
	CPU	SPARC64 X 2.8GHz 1 プロセッサ 2 コア(計 4 スレッド)以上	
	メモリ	32GB(8G x 4)以上	
	LAN(*1)	100Mbps 以上	
OS		Solaris 11.1 以降	Solaris 10 1/13
X Window システム (*2)	ディスプレイ マネージャー	GDM(gdm サービス)	以下のいずれかを選択 • dtlogin(cde-login サービス) • GDM(gdm2-login サービス)
	デスクトップ環境	GNOME(*3)	以下のいずれかを選択 • CDE • JDS
	VNC サーバ	TigerVNC Server(*4) (*5) (*6)	RealVNC Server(*7)

*1: LAN のトラフィックが集中する環境では、動作が遅くなることがあります。

*2: X Window システムを使用するためには、以下のパッケージグループのインストールが必要です。

OS	パッケージグループ
Solaris 11	solaris-desktop
Solaris 10	エンドユーザーシステムサポート

*3: Solaris 11.3 以前は GNOME2、Solaris 11.4 以降は GNOME3 となります。

*4: TigerVNC の TLS 暗号化は、Solaris 11.3 SRU18041(SRU11.3.31.6.0)以降でサポートします。

*5: TigerVNC の暗号化と認証については、「A.1 TigerVNC によるデータ暗号化の場合 2) [参考](#)」を参照してください。

*6: TigerVNC は、Solaris に同梱されたフリーウェアです。

*7: RealVNC は、Solaris に同梱されたフリーウェアです。

2.2. クライアント検証環境

本書に記載した手順は、下表のクライアントを使用した環境で検証しています。

検証環境		クライアント-1	クライアント-2	クライアント-3
本体装置		Windows PC		
	CPU	Intel Core i3 M350 2.27GHz 1 プロセッサ 2 コア (計 4 スレッド)	Intel Core i5 5300U 2.3GHz 1 プロセッサ 2 コア (計 4 スレッド)	Intel Celeron 2950M 2.00GHz 1 プロセッサ 2 コア (計 2 スレッド)
	メモリ	4GB	6GB	6GB
	LAN	100Mbps	100Mbps	100Mbps
OS		Windows 7 Pro SP1 32bit	Windows 8.1 Enterprise 64bit	Windows 10 Pro 64bit
	ソフトウェア	VNC クライアント	TigerVNC Viewer Version 1.8.0 (*1) (*3) (*4)	
		ターミナル エミュレータ	Tera Term Version 4.97 (*2) (*3) PuTTY Version 0.70 (*2) (*3)	

*1: TigerVNC は、商用利用可能なフリーウェアです。

*2: Tera Term および PuTTY は、商用利用可能なフリーウェアです。

*3: 各フリーウェアの公式ダウンロードサイトからダウンロードします。

インストール方法は、各フリーウェアのインストール手順に従ってください。

*4: TigerVNC の暗号化と認証については、「A.1 TigerVNC によるデータ暗号化の場合 2) [参考](#)」を参照してください。

2.3. 使用リソース(参考値)

本項では、下表の測定条件でリモートデスクトップを操作したときの使用リソースについて記載します。

測定条件		内容
サーバ	本体装置	SPARC M10-4
	OS 版数	Solaris 11.3 SRU18081(SRU11.3.35.6.0)
	CPU	SPARC64 X 2.8GHz 1 プロセッサ 2 コア(計 4 スレッド)
	メモリ	32GB
	LAN	1000Mbps(*1)
クライアント	本体装置	Windows PC
	OS 版数	Windows 7 Pro SP1 32bit
	CPU	Intel Core i3 M350 2.27GHz 1 プロセッサ 2 コア(計 4 スレッド)
	メモリ	4GB
	LAN	100Mbps(*1)
デスクトップの解像度		1280x1024
データ暗号化手段		TigerVNC の TLS 暗号化

*1: スイッチングハブと実際に接続したときのリンク速度です。

デスクトップ上で以下のコマンドを実行中に測定した使用リソース(参考値)を下表に示します。

実行コマンド	使用リソース	サーバ	クライアント
xterm 上での cat コマンド(*2)	CPU(使用率)	8%	5%
	メモリ(使用量)	300MB	17MB
	ネットワーク(使用量)	2Mbps	
/usr/bin/glxgears コマンド (デモ表示)	CPU(使用率)	3%	25%
	メモリ(使用量)	600MB	18MB
	ネットワーク(使用量)	12Mbps	

*2: cat コマンドに使用したファイルの行数(サイズ)は、100000 行(8100000 バイト)です。

上記リソースは、デスクトップの解像度やマルチデスクトップのデスクトップ数にほぼ比例して増加します。

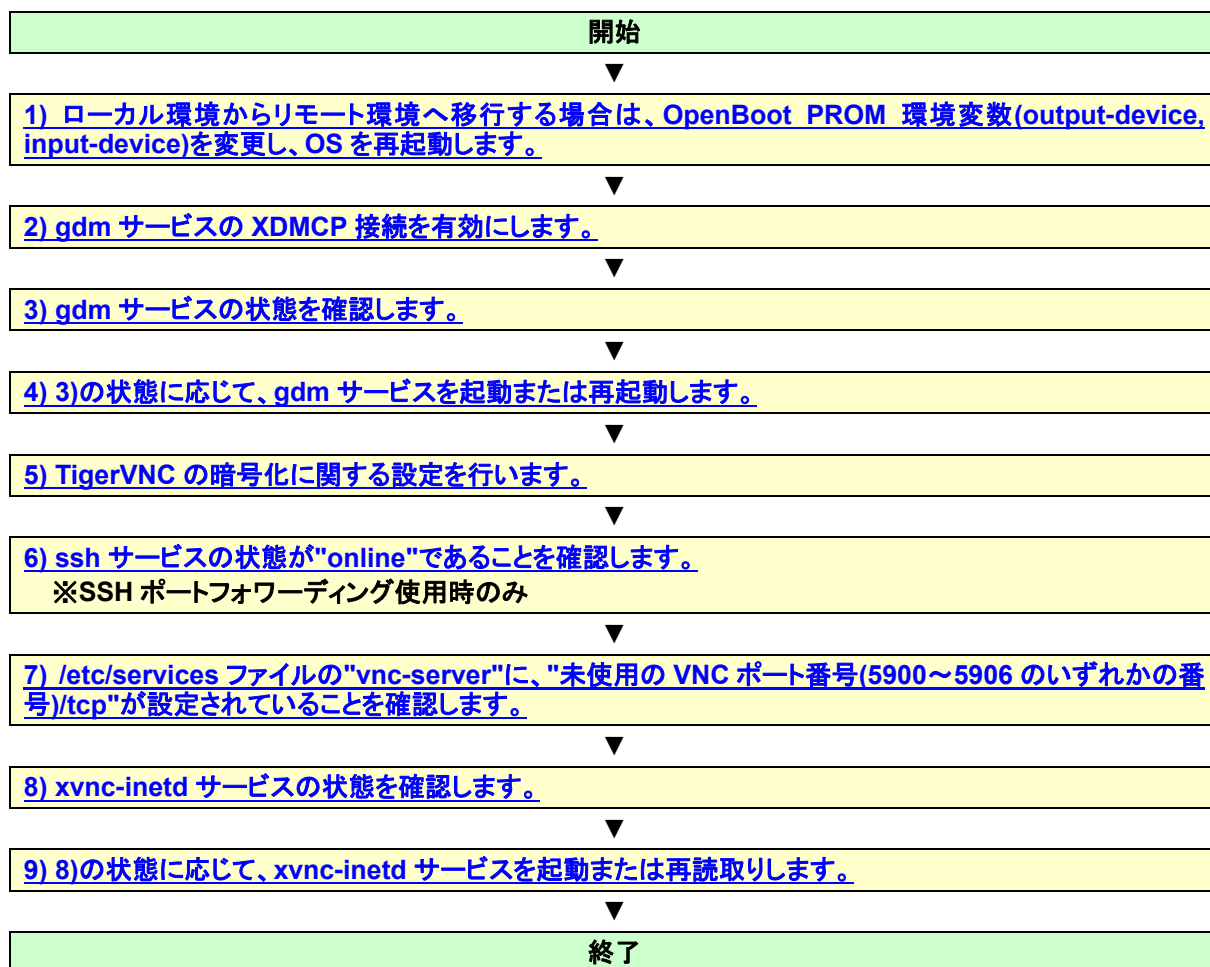
3. リモートデスクトップの環境構築・接続手順

3.1. 手順の流れ

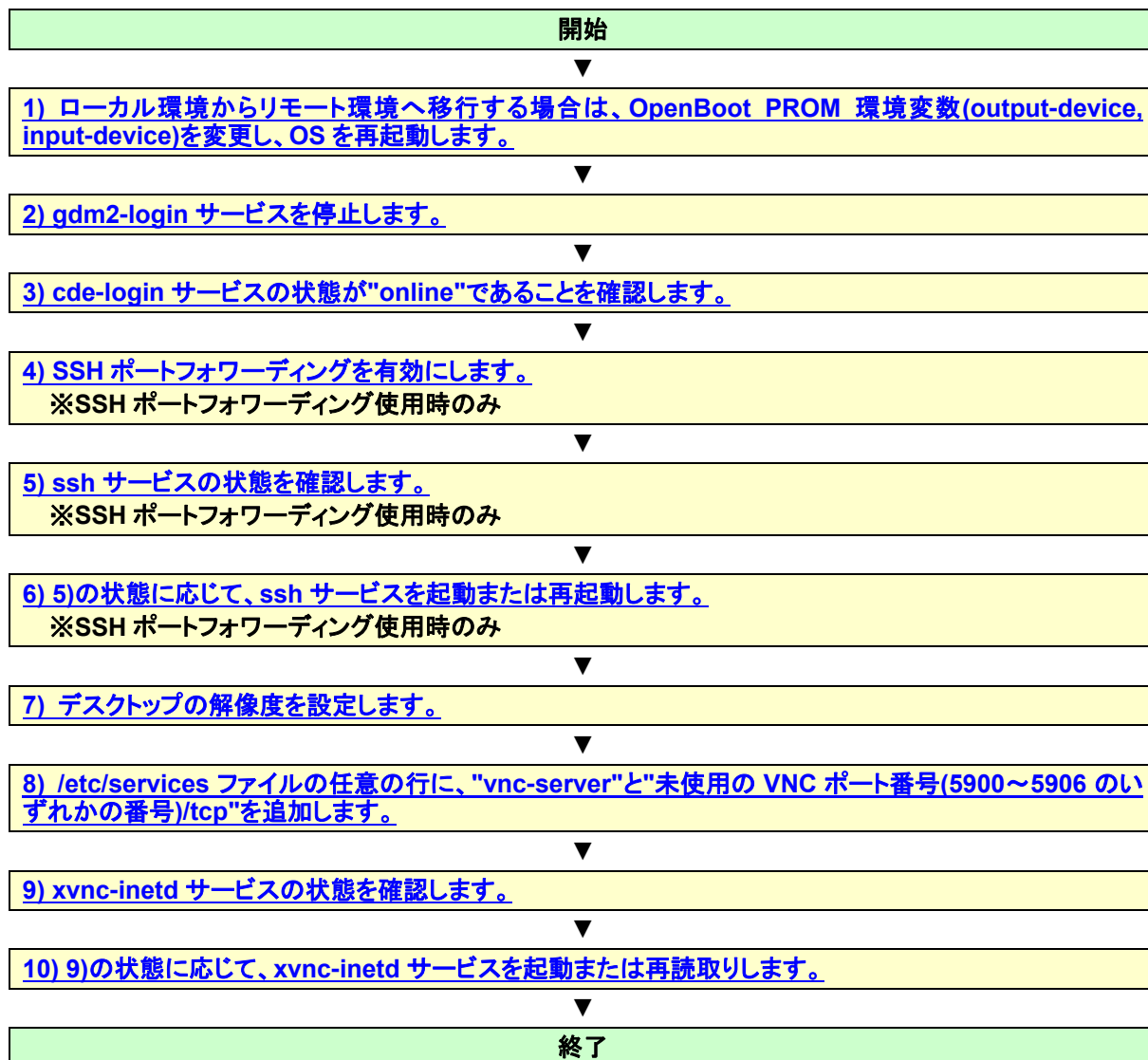
リモートデスクトップの環境構築・接続手順の流れを以下に示します。

3.1.1. リモートデスクトップのサーバ環境構築手順

● Solaris 11 gdm サービスの場合



● Solaris 10 cde-login サービスの場合



● Solaris 10 gdm2-login サービスの場合



3.1.2. リモートデスクトップのクライアント環境構築・接続手順

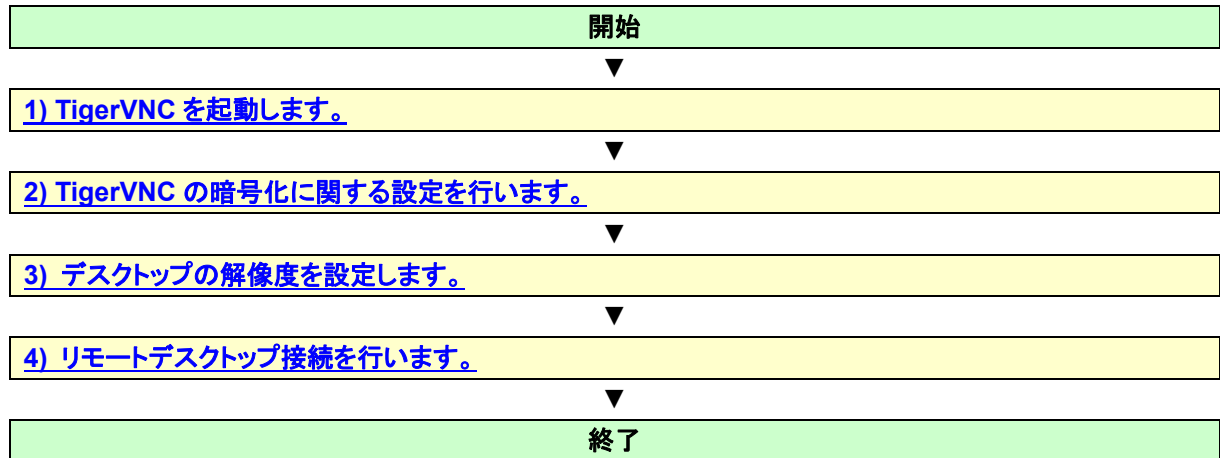
● Tera Term の SSH ポートフォワーディングを使用する場合



● PuTTY の SSH ポートフォワーディングを使用する場合



● リモートデスクトップ接続



3.2. リモートデスクトップのサーバ環境構築手順

本項では、サーバ(SPARC M12/M10)におけるリモートデスクトップの環境構築手順を、使用する OS 版数とサービスの組合せごとに説明します。

Point

サーバ環境構築手順は、サーバの電源切断や OS 起動後に再実行する必要はありません。

3.2.1. Solaris 11 gdm サービスの場合

- 1) ローカル環境からリモート環境へ移行する場合は、OpenBoot PROM 環境変数(output-device, input-device)を変更し、OS を再起動します。

OpenBoot PROM 環境変数(output-device, input-device)を"virtual-console"に設定します。

```
# eeprom output-device=virtual-console
# eeprom input-device=virtual-console
```

上記コマンドを実行後、OpenBoot PROM 環境変数(output-device, input-device) が"virtual-console"に設定されたことを確認します。

```
# eeprom | grep put-device
output-device=virtual-console
input-device=virtual-console
```

上記設定を反映するために、OS を再起動します。

```
# shutdown -i6 -g0 -y
```

- 2) gdm サービスの XDMCP 接続を有効にします。

/etc/gdm/custom.conf ファイルを開き、[xdmcp]の下に"Enable=true"を追加します。

```
# vi /etc/gdm/custom.conf
:
[xdmcp]
Enable=true
:
```

- 3) gdm サービスの状態を確認します。

[実施例]

```
# svcs gdm
STATE      STIME      FMRI
online     15:22:14  svc:/application/graphical-login/gdm:default
```

4) 3)の状態に応じて、gdm サービスを起動または再起動します。

gdm サービスの状態が"disabled"の場合はサービスを起動(enable)し、"online"の場合はサービスを再起動(restart)します。

```
# svcadm enable gdm
```

または

```
# svcadm restart gdm
```

- ▶ サービスの状態が"degraded"、"maintenance"、または"offline"の場合は、「[C.1.4 サービスの状態が"degraded"、"maintenance"、または"offline"となっている](#)」を参照してください。

上記コマンドを実行後、サービスの状態が"online"に遷移したことを確認します。

```
# svcs gdm
STATE          STIME      FMRI
online         15:34:21  svc:/application/graphical-login/gdm:default
```

確認した状態が"online*"の場合は、状態遷移中のため、しばらくしてから状態を再確認します。

- ▶ サービスの状態が"online"に遷移しない場合は、「[C.1.2 サービス起動時に、サービスの状態が"online"に遷移しない](#)」を参照してください。

5) TigerVNC の暗号化に関する設定を行います。

"SecurityTypes"の設定状態を確認します。

[実施例:"SecurityTypes"が"None"に設定されている場合]

```
# inetadm -l xvnc-inetd | grep exec
exec="/usr/bin/Xvnc -inetd -query localhost -once -SecurityTypes None"
```

i) "TLSNone"(暗号化あり)を設定する場合

- ▶ TigerVNC の TLS 暗号化は、Solaris 11.1~Solaris 11.3 SRU18032 は未サポートのため、[ii\)](#)の手順に進みます。

確認した"SecurityTypes"がすでに"TLSNone"である場合は、[6\)](#)の手順に進みます。

"SecurityTypes"が"TLSNone"以外の場合は、"TLSNone"を設定します。

```
# inetadm -m xvnc-inetd exec="/usr/bin/Xvnc -inetd -query localhost -once
-SecurityTypes TLSNone"
```

上記コマンドを実行後、"SecurityTypes"が"TLSNone"に設定されたことを確認します。

```
# inetadm -l xvnc-inetd | grep exec
exec="/usr/bin/Xvnc -inetd -query localhost -once -SecurityTypes TLSNone"
```

ii) "None"(暗号化なし)を設定する場合

確認した"SecurityTypes"がすでに"None"である場合は、[6\)](#)の手順に進みます。

"SecurityTypes"が"None"以外の場合は、"None"を設定します。

```
# inetadm -m xvnc-inetd exec="/usr/bin/Xvnc -inetd -query localhost -once  
-Securitytypes None"
```

上記コマンドを実行後、"SecurityTypes"が"None"に設定されたことを確認します。

```
# inetadm -l xvnc-inetd | grep exec  
exec="/usr/bin/Xvnc -inetd -query localhost -once -SecurityTypes None"
```

6) ssh サービスの状態が"online"であることを確認します。(SSH ポートフォワーディング使用時のみ)

```
# svcs ssh  
STATE          STIME      FMRI  
online         15:22:49  svc:/network/ssh:default
```

確認したサービスの状態がすでに"online"の場合は、[7\)](#)の手順に進みます。

サービスの状態が"disabled"の場合は、サービスを起動します。

```
# svcadm enable ssh
```

- ▶ サービスの状態が"degraded"、"maintenance"、または"offline"の場合は、「[C.1.4 サービスの状態が"degraded"、"maintenance"、または"offline"となっている](#)」を参照してください。

上記コマンドを実行後、サービスの状態が"online"に遷移したことを確認します。

```
# svcs ssh  
STATE          STIME      FMRI  
online         15:37:28  svc:/network/ssh:default
```

確認した状態が"online*"の場合は、状態遷移中のため、しばらくしてから状態を再確認します。

- ▶ サービスの状態が"online"に遷移しない場合は、「[C.1.2 サービス起動時に、サービスの状態が"online"に遷移しない](#)」を参照してください。

- 7) `/etc/services` ファイルの"vnc-server"に、"未使用の VNC ポート番号(5900～5906 のいずれかの番号)/tcp"が設定されていることを確認します。

```
# vi /etc/services
:
vnc-server      5900/tcp
:
```

"vnc-server"の定義がない場合は、`/etc/services` ファイルの任意の行に、"vnc-server"と"未使用の VNC ポート番号/tcp"を追加します。

[実施例: VNC ポート番号(5901)を追加する場合]

```
# vi /etc/services
:
xxxxxxx        5900/tcp
vnc-server      5901/tcp
:
```

- 8) `xvnc-inetd` サービスの状態を確認します。

```
# svcs xvnc-inetd
STATE      STIME    FMRI
disabled   15:22:48 svc:/application/x11/xvnc-inetd:default
```

- 9) 8)の状態に応じて、`xvnc-inetd` サービスを起動または再読み込みします。

`xvnc-inetd` サービスの状態が"disabled"の場合はサービスを起動(enable)し、"online"の場合はサービスを再読み込み(refresh)します。

```
# svcadm enable xvnc-inetd
```

または

```
# svcadm refresh xvnc-inetd
```

- ▶ サービスの状態が"degraded"、"maintenance"、または"offline"の場合は、「[C.1.4 サービスの状態が"degraded"、"maintenance"、または"offline"となっている](#)」を参照してください。

上記コマンドを実行後、サービスの状態が"online"に遷移したことを確認します。

```
# svcs xvnc-inetd
STATE      STIME    FMRI
online     15:40:12 svc:/application/x11/xvnc-inetd:default
```

確認した状態が"online*"の場合は、状態遷移中のため、しばらくしてから状態を再確認します。

- ▶ サービスの状態が"online"に遷移しない場合は、「[C.1.2 サービス起動時に、サービスの状態が"online"に遷移しない](#)」を参照してください。

3.2.2. Solaris 10 cde-login サービスの場合

- 1) ローカル環境からリモート環境へ移行する場合は、OpenBoot PROM 環境変数(output-device, input-device)を変更し、OS を再起動します。

OpenBoot PROM 環境変数(output-device, input-device)を"virtual-console"に設定します。

```
# eeprom output-device=virtual-console
# eeprom input-device=virtual-console
```

上記コマンドを実行後、OpenBoot PROM 環境変数(output-device, input-device) が"virtual-console"に設定されたことを確認します。

```
# eeprom | grep put-device
output-device=virtual-console
input-device=virtual-console
```

上記設定を反映するために、OS を再起動します。

```
# shutdown -i6 -g0 -y
```

- 2) gdm2-login サービスを停止します。

```
# svcadm disable gdm2-login
```

上記コマンドを実行後、サービスの状態が"disabled"に遷移したことを確認します。

```
# svcs gdm2-login
STATE          STIME      FMRI
disabled       15:37:22  svc:/application/gdm2-login:default
```

確認した状態が"online*"の場合は、状態遷移中のため、しばらくしてから状態を再確認します。

- ▶ サービスの状態が"disabled"に遷移しない場合は、「[C.1.3 サービス停止時に、サービスの状態が"disabled"に遷移しない](#)」を参照してください。

3) cde-login サービスの状態が"online"であることを確認します。

```
# svcs cde-login
STATE      STIME    FMRI
online     15:38:29 svc:/application/graphical-login/cde-login:default
```

確認したサービスの状態がすでに"online"の場合は、[4\)](#)の手順に進みます。

サービスの状態が"disabled"の場合は、サービスを起動します。

```
# svcadm enable cde-login
```

- ▶ サービスの状態が"degraded"、"maintenance"、または"offline"の場合は、「[C.1.4 サービスの状態が"degraded"、"maintenance"、または"offline"となっている](#)」を参照してください。

上記コマンドを実行後、サービスの状態が"online"に遷移したことを確認します。

```
# svcs cde-login
STATE      STIME    FMRI
online     15:50:29 svc:/application/graphical-login/cde-login:default
```

確認した状態が"online*"の場合は、状態遷移中のため、しばらくしてから状態を再確認します。

- ▶ サービスの状態が"online"に遷移しない場合は、「[C.1.2 サービス起動時に、サービスの状態が"online"に遷移しない](#)」を参照してください。

4) SSH ポートフォワーディングを有効にします。(SSH ポートフォワーディング使用時のみ)

/etc/ssh/sshd_config ファイルを開き、AllowTcpForwarding を yes に設定します。

```
# vi /etc/ssh/sshd_config
:
AllowTcpForwarding yes
:
```

5) ssh サービスの状態を確認します。(SSH ポートフォワーディング使用時のみ)

```
# svcs ssh
STATE      STIME    FMRI
online     15:37:50 svc:/network/ssh:default
```


6) 5)の状態に応じて、ssh サービスを起動または再起動します。(SSH ポートフォワーディング使用時のみ)

ssh サービスの状態が"disabled"の場合はサービスを起動(enable)し、"online"の場合はサービスを再起動(restart)します。

```
# svcadm enable ssh
```

または

```
# svcadm restart ssh
```

- ▶ サービスの状態が"degraded"、"maintenance"、または"offline"の場合は、「[C.1.4 サービスの状態が"degraded"、"maintenance"、または"offline"となっている](#)」を参照してください。

上記コマンドを実行後、状態が"online"に遷移したことを確認します。

```
# svcs ssh
STATE          STIME      FMRI
online         15:58:44  svc:/network/ssh:default
```

確認した状態が"online"の場合は、状態遷移中のため、しばらくしてから状態を再確認します。

- ▶ サービスの状態が"online"に遷移しない場合は、「[C.1.2 サービス起動時に、サービスの状態が"online"に遷移しない](#)」を参照してください。

7) デスクトップの解像度を設定します。

Point

- Solaris 10 の場合は、クライアントでの解像度設定を無視するため、以下の手順でデスクトップの解像度を設定します。
- Solaris 10 の場合は、TLS 暗号化は未サポートのため、inetadm コマンドのパラメーターに必ず "-SecurityTypes None"を指定します。

[実施例: 解像度をデフォルトのまま使用する場合]

```
# inetadm -m xvnc-inetd exec="/usr/X11/bin/Xvnc -inetd -query localhost -once -SecurityTypes None"
```

[実施例: 解像度を 1280x1024 に設定する場合]

```
# inetadm -m xvnc-inetd exec="/usr/X11/bin/Xvnc -inetd -query localhost -once -SecurityTypes None -geometry 1280x1024"
```

設定した内容を確認します。

[実施例: 解像度を 1280x1024 に設定した場合]

```
# inetadm -l xvnc-inetd | grep exec
exec="/usr/X11/bin/Xvnc -inetd -query localhost -once -SecurityTypes None -geometry 1280x1024"
```

- 8) `/etc/services` ファイルの任意の行に、`"vnc-server"`と未使用の VNC ポート番号(5900～5906 のいずれかの番号)/`tcp`"を追加します。

[実施例: VNC ポート番号(5900)を追加する場合]

```
# vi /etc/services
:
vnc-server      5900/tcp
:
```

- 9) `xvnc-inetd` サービスの状態を確認します。

```
# svcs xvnc-inetd
STATE      STIME      FMRI
disabled   15:37:49   svc:/application/x11/xvnc-inetd:default
```

- 10) 9)の状態に応じて、`xvnc-inetd` サービスを起動または再読み込みします。

`xvnc-inetd` サービスの状態が`"disabled"`の場合はサービスを起動(`enable`)し、`"online"`の場合はサービスを再読み込み(`refresh`)します。

```
# svcadm enable xvnc-inetd
```

または

```
# svcadm refresh xvnc-inetd
```

- ▶ サービスの状態が`"degraded"`、`"maintenance"`、または`"offline"`の場合は、[「C.1.4 サービスの状態が"degraded"、"maintenance"、または"offline"となっている」](#)を参照してください。

上記コマンドを実行後、サービスの状態が`"online"`に遷移したことを確認します。

```
# svcs xvnc-inetd
STATE      STIME      FMRI
online     15:55:08   svc:/application/x11/xvnc-inetd:default
```

確認した状態が`"online"`の場合は、状態遷移中のため、しばらくしてから状態を再確認します。

- ▶ サービスの状態が`"online"`に遷移しない場合は、[「C.1.2 サービス起動時に、サービスの状態が"online"に遷移しない」](#)を参照してください。

3.2.3. Solaris 10 gdm2-login サービスの場合

- 1) ローカル環境からリモート環境へ移行する場合は、OpenBoot PROM 環境変数(output-device, input-device)を変更し、OS を再起動します。

OpenBoot PROM 環境変数(output-device, input-device)を"virtual-console"に設定します。

```
# eeprom output-device=virtual-console
# eeprom input-device=virtual-console
```

上記コマンドを実行後、OpenBoot PROM 環境変数(output-device, input-device) が"virtual-console"に設定されたことを確認します。

```
# eeprom | grep put-device
output-device=virtual-console
input-device=virtual-console
```

上記設定を反映するために、OS を再起動します。

```
# shutdown -i6 -g0 -y
```

- 2) グラフィックスカードの実装状態に応じて、/etc/X11/gdm/gdm.conf ファイルの[xdmcp]と[servers]を編集します。

[実施例: グラフィックスカード未実装時]

```
# prtdiag | grep mko
# ←グラフィックスカードの情報が表示されないことを確認します。
```

[実施例: グラフィックスカード実装時]

```
# prtdiag | grep mko
/BB0/PCI2          PCIE   TSI, mko          GFX550      --
                  /pci@8500/pci@4/pci@0/pci@9/pci@0/TSI, mko@0
```

/etc/X11/gdm/gdm.conf ファイルを開き、グラフィックスカードの実装状態に応じて、下表のように [xdmcp] と [servers] を編集します。

グラフィックスカードの 実装状態	/etc/X11/gdm/gdm.conf の編集項目	
	[xdmcp]	[servers]
未実装	[xdmcp] の下の "Enable" を "true" に 設定します。	[servers] の下の "0=Standard" の行頭に "#" を追加し、無効な状態にします。
実装		[servers] の下の "0=Standard" はデフォルト のまま有効な状態にします。

[実施例: グラフィックスカード未実装時]

```
# vi /etc/X11/gdm/gdm.conf
:
[xdmcp]
:
Enable=true
:
[servers]
:
#0=Standard
:
```

[実施例: グラフィックスカード実装時]

```
# vi /etc/X11/gdm/gdm.conf
:
[xdmcp]
:
Enable=true
:
[servers]
:
0=Standard
:
```

3) cde-login サービスを停止します。

```
# svcadm disable cde-login
```

上記コマンドを実行後、サービスの状態が"disabled"に遷移したことを確認します。

```
# svcs cde-login
STATE      STIME      FMRI
disabled   16:33:23  svc:/application/graphical-login/cde-login:default
```

確認した状態が"online*"の場合は、状態遷移中のため、しばらくしてから状態を再確認します。

- ▶ サービスの状態が"disabled"に遷移しない場合は、[「C.1.3 サービス停止時に、サービスの状態が"disabled"に遷移しない」](#)を参照してください。

4) gdm2-login サービスの状態を確認します。

```
# svcs gdm2-login
STATE      STIME      FMRI
disabled   16:16:01  svc:/application/gdm2-login:default
```

5) 4)の状態に応じて、gdm2-login サービスを起動または再起動します。

gdm2-login サービスの状態が"disabled"の場合はサービスを起動(enable)し、"online"の場合はサービスを再起動(restart)します。

```
# svcadm enable gdm2-login
```

または

```
# svcadm restart gdm2-login
```

- ▶ サービスの状態が"degraded"、"maintenance"、または"offline"の場合は、[「C.1.4 サービスの状態が"degraded"、"maintenance"、または"offline"となっている」](#)を参照してください。

上記コマンドを実行後、サービスの状態が"online"に遷移したことを確認します。

```
# svcs gdm2-login
STATE      STIME      FMRI
online     16:36:01  svc:/application/gdm2-login:default
```

確認した状態が"online*"の場合は、状態遷移中のため、しばらくしてから状態を再確認します。

- ▶ サービスの状態が"online"に遷移しない場合は、[「C.1.2 サービス起動時に、サービスの状態が"online"に遷移しない」](#)を参照してください。

6) 「[3.2.2 Solaris 10 cde-login サービスの場合 4\)](#)」以降の手順を実行します。

3.3. リモートデスクトップのクライアント環境構築・接続手順

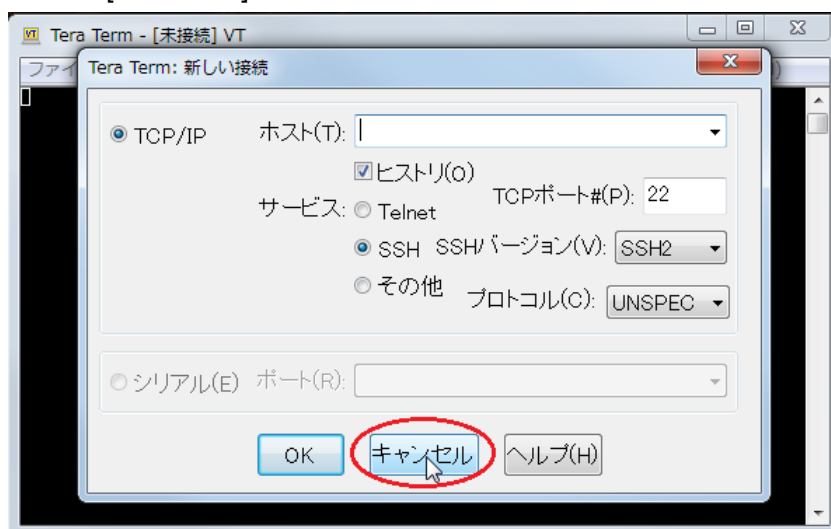
本項では、クライアント(Windows PC)におけるリモートデスクトップの環境構築・接続手順について説明します。

3.3.1. Tera Term の SSH ポートフォワーディングを使用する場合

SSH ポートフォワーディングのターミナルエミュレータとして、Tera Term を使用する場合は手順を説明します。

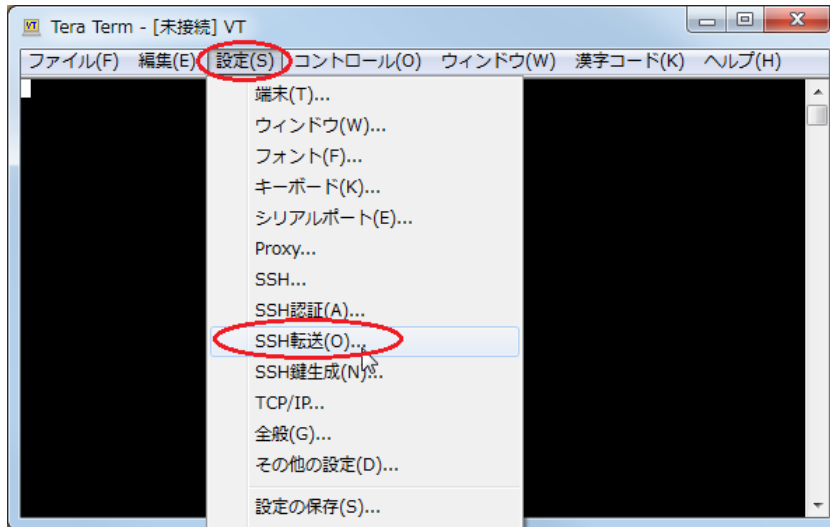
1) Tera Term を起動します。

Tera Term ウィンドウと、[Tera Term: 新しい接続]ダイアログが表示されますが、このダイアログは不要なため、[キャンセル]をクリックします。

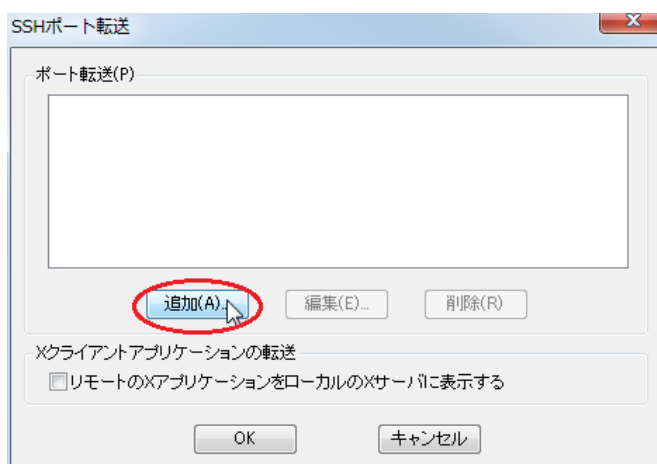


2) SSH ポートフォワーディングを設定します。(初期設定時のみ)

1)で表示された Tera Term ウィンドウの[設定]メニューから[SSH 転送]を選択します。



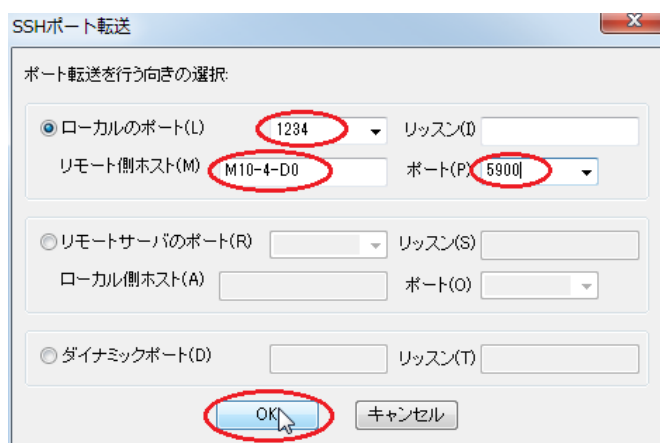
上記を選択後に表示された[SSH ポート転送]ダイアログの[追加]をクリックします。



次に表示された[SSH ポート転送]ダイアログで以下の項目を設定し、[OK]をクリックします。

設定項目	設定内容	設定例
ローカル側のポート(L)	未使用のクライアントポート番号(1~65535) ※ 使用中のポート番号は、「 A.2 SSH ポートフォワーディングによるデータ暗号化の場合 」を参考に、netstat コマンドなどで確認できます。 ※ 複数のドメインに接続する場合は、ドメイン単位に異なるクライアントポート番号を設定する必要があります。	1234
リモート側ホスト(M)	サーバのホスト名または IP アドレス(xxx.xxx.xxx.xxx)	M10-4-D0
ポート(P)	「 3.2.1 Solaris 11 gdm サービスの場合 7) 」または「 3.2.2 Solaris 10 cde-login サービスの場合 8) 」で設定した VNC ポート番号	5900

[実施例]



SSHポート転送

ポート転送を行う向きの選択:

☒ ローカル側のポート(L) 1234 リッスン(I)

リモート側ホスト(M) M10-4-D0 ポート(P) 5900

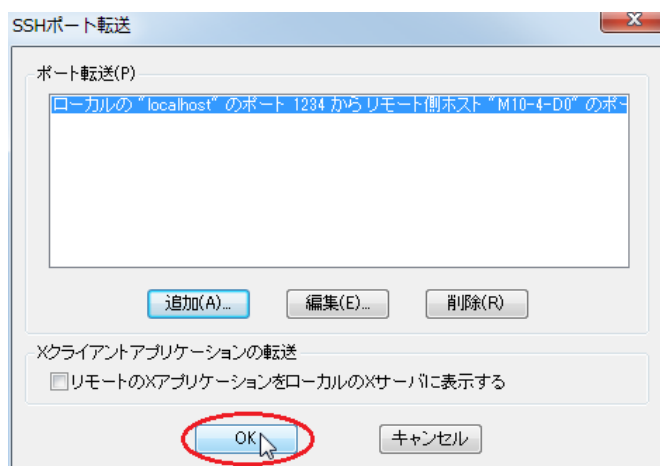
☐ リモートサーバのポート(R) リッスン(S)

ローカル側ホスト(A) ポート(O)

☐ ダイナミックポート(D) リッスン(T)

OK キャンセル

戻ったダイアログで[OK]をクリックします。



SSHポート転送

ポート転送(P)

ローカルの "localhost" のポート 1234 からリモート側ホスト "M10-4-D0" のポ

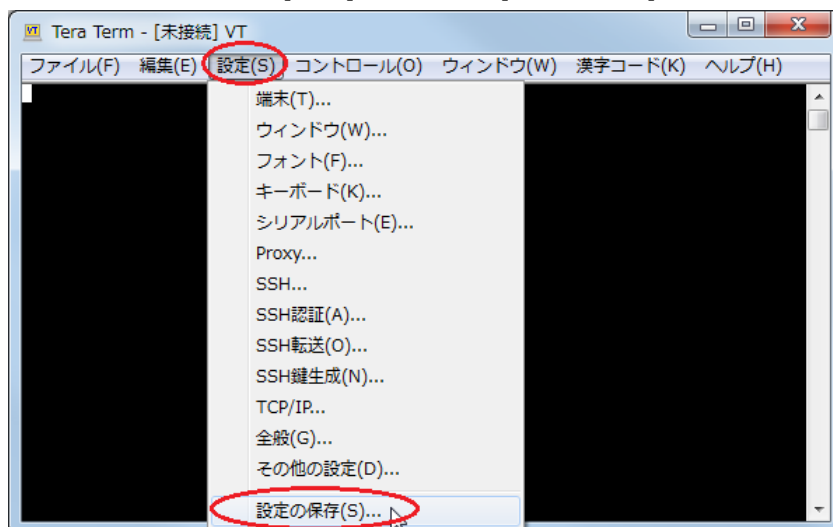
追加(A)... 編集(E)... 削除(R)

Xクライアントアプリケーションの転送

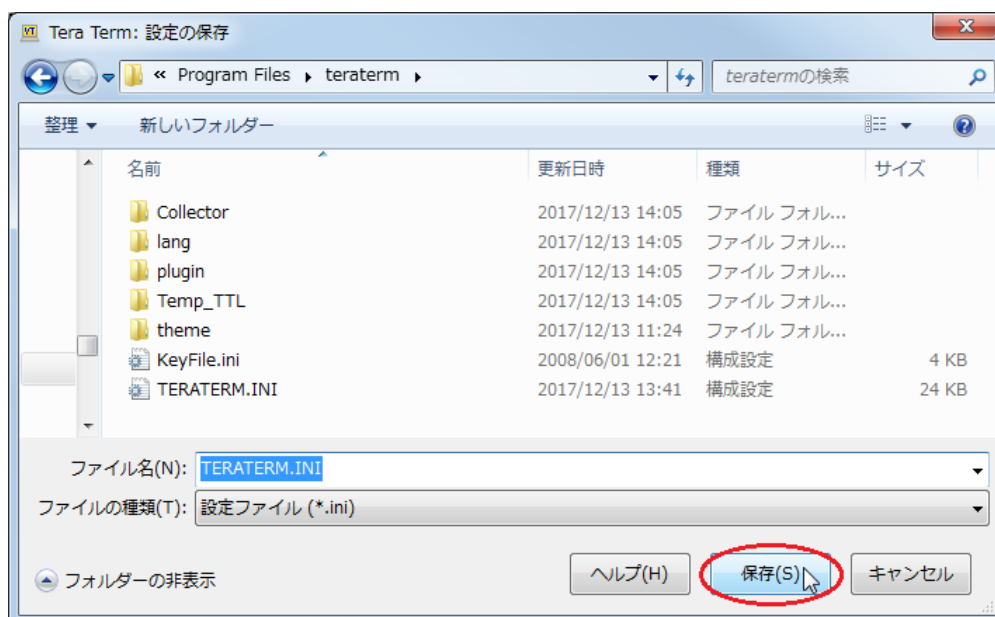
☐ リモートのXアプリケーションをローカルのXサーバに

OK キャンセル

Tera Term ウィンドウの[設定]メニューから[設定の保存]を選択します。



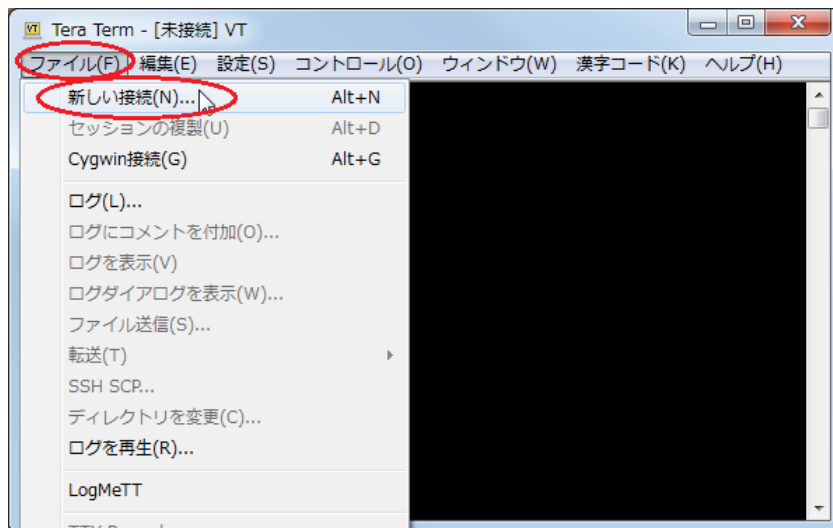
上記を選択後に表示された[Tera Term: 設定の保存]ダイアログから、ファイル名"TERATERM.INI"で[保存]をクリックします。



上記設定を保存することで、次回以降は SSH ポートフォワーディングの設定手順が不要となります。

3) サーバに SSH 接続します。

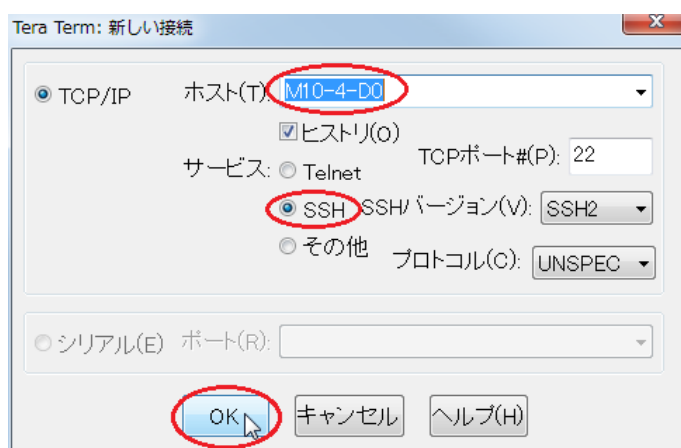
Tera Term ウィンドウの[ファイル]メニューから[新しい接続]を選択します。



上記を選択後に表示された[Tera Term: 新しい接続]ダイアログで以下の項目を指定し、[OK]をクリックします。

指定項目	指定内容	指定例
ホスト(T)	サーバのホスト名または IP アドレス(xxx.xxx.xxx.xxx)	M10-4-D0
サービス	SSH を選択	SSH

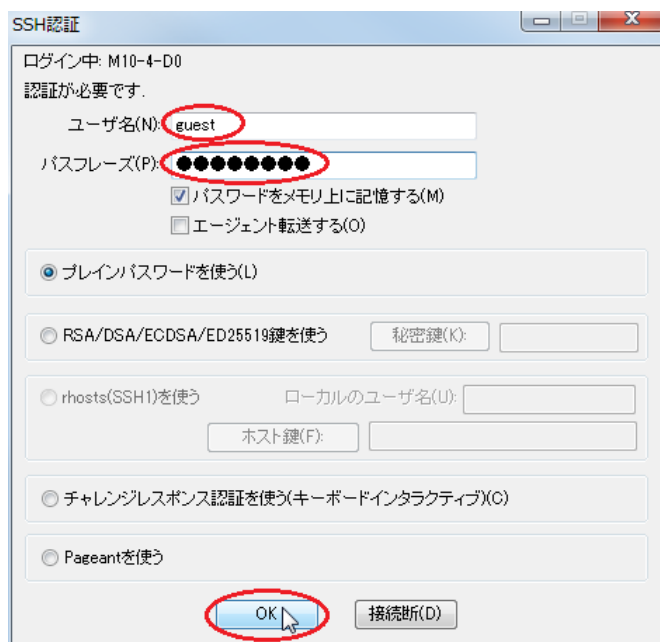
[実施例]



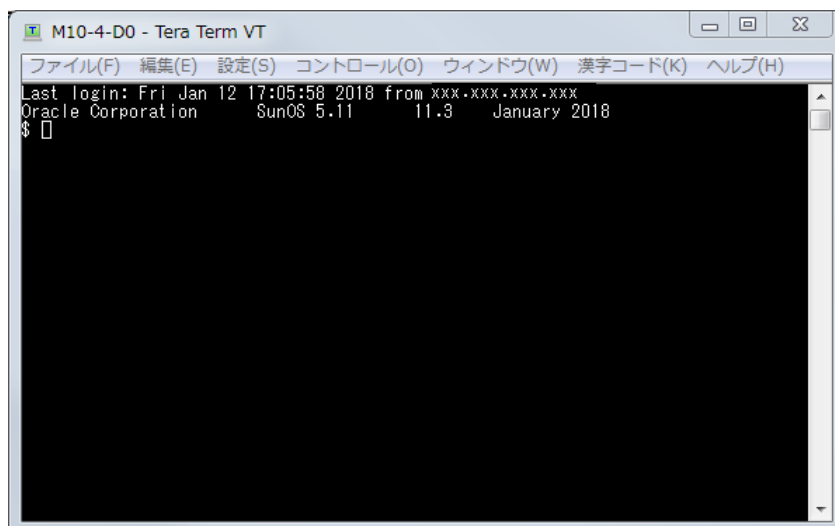
[OK]をクリック後に表示された[SSH 認証]ダイアログで、"ユーザ名(N)"と"パスワード(P)"を入力し、[OK]をクリックします。

"ユーザ名(N)"には、サーバに登録済みのユーザーを指定することが可能です。

[実施例:"ユーザ名(N)"に guest を入力する場合]



サーバに正常に接続すると、Tera Term ウィンドウにターミナルエミュレータ画面が表示され、SSHポートフォワーディングが使用可能となります。



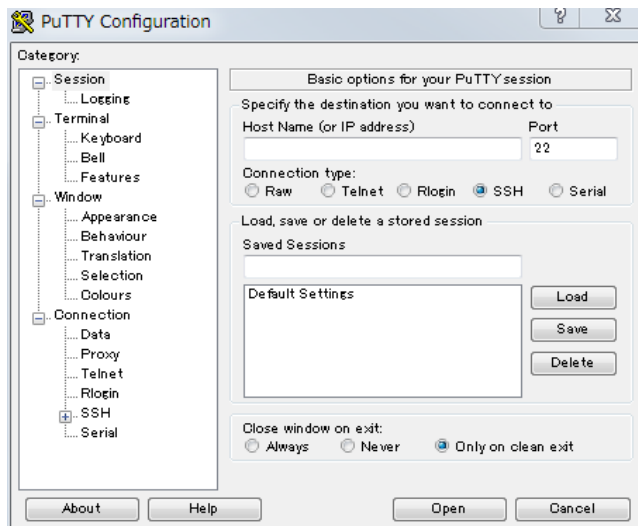
- 4) 「[3.3.3 リモートデスクトップ接続](#)」の順に進み、リモートデスクトップ接続を行います。

3.3.2. PuTTY の SSH ポートフォワーディングを使用する場合

SSH ポートフォワーディングのターミナルエミュレータとして、PuTTY を使用する場合は手順を説明します。

1) PuTTY を起動します。

[PuTTY Configuration]ダイアログが表示されます。



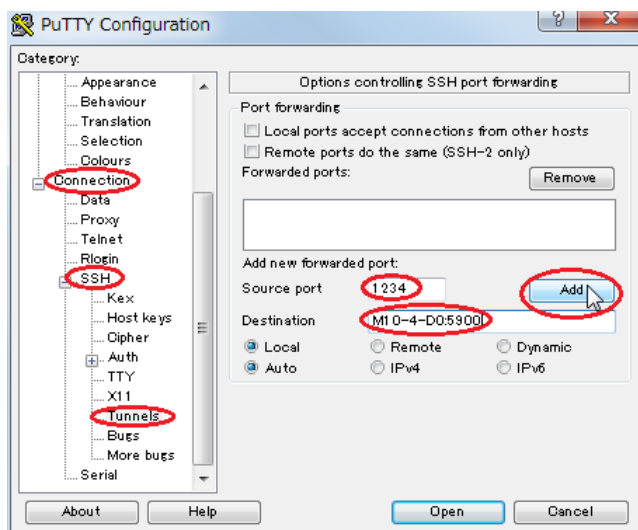
2) SSH ポートフォワーディングを設定します。

i) 新規セッションを作成する場合(初期設定時のみ)

1)で表示された[PuTTY Configuration]ダイアログの[Category]から[Connection]-[SSH]-[Tunnels]を選択した画面で以下の項目を設定し、[Add]をクリックします。

設定項目	設定内容	設定例
Source port	未使用のクライアントポート番号(1~65535) ※ 使用中のポート番号は、「 A.2 SSH ポートフォワーディングによるデータ暗号化の場合 」を参考に、netstat コマンドなどで確認できます。 ※ 複数のドメインに接続する場合は、ドメイン単位に異なるクライアントポート番号を設定する必要があります。	1234
Destination	以下を"."で区切った情報 <ul style="list-style-type: none"> サーバのホスト名または IP アドレス(xxx.xxx.xxx.xxx) 「3.2.1 Solaris 11 gdm サービスの場合 7)」または「3.2.2 Solaris 10 cde-login サービスの場合 8)」で設定した VNC ポート番号 	M10-4-D0:5900

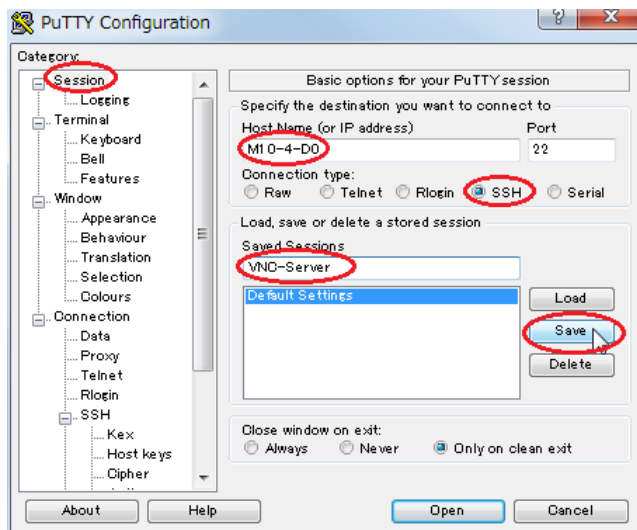
[実施例]



次に[PuTTY Configuration]ダイアログの[Category]から[Session]を選択した画面で以下の項目を設定し、[Save]をクリックします。

設定項目	設定内容	設定例
Host Name (or IP address)	サーバのホスト名または IP アドレス(xxx.xxx.xxx.xxx)	M10-4-D0
Connection type	SSH を選択	SSH
Saved Sessions	任意の保存セッション名	VNC-Server

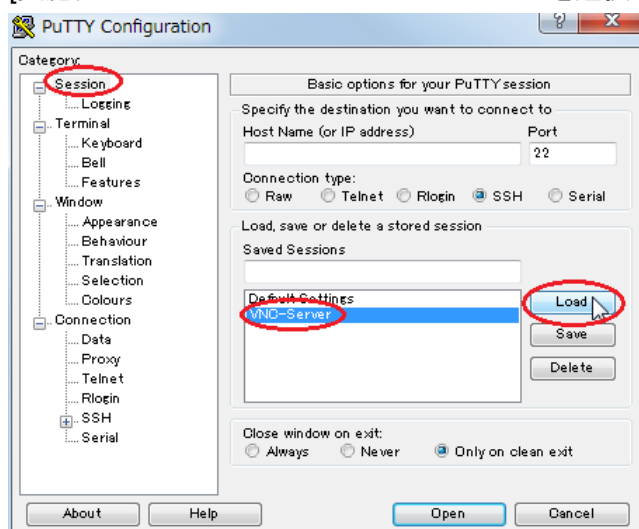
[実施例]



ii) 保存されたセッションを使用する場合

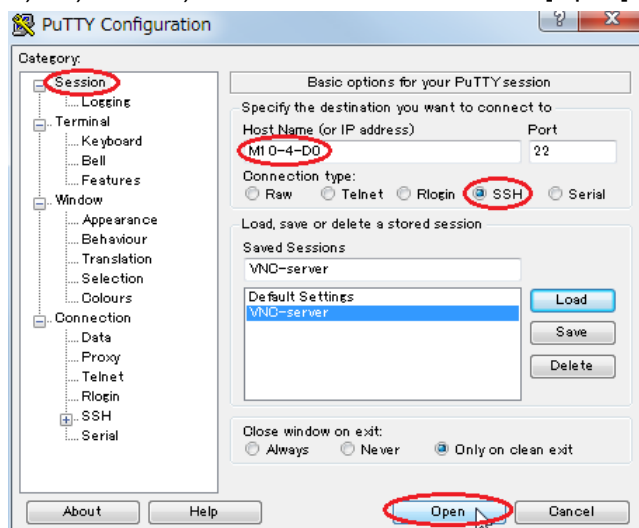
1)で表示された[PuTTY Configuration]ダイアログの[Category]から[Session]を選択します。
この選択画面の"Saved Sessions"から i)で保存したセッションを選択し、[Load]をクリックして設定を反映します。

[実施例: "Saved Sessions"から VNC-Server を選択する場合]



3) サーバに SSH 接続します。

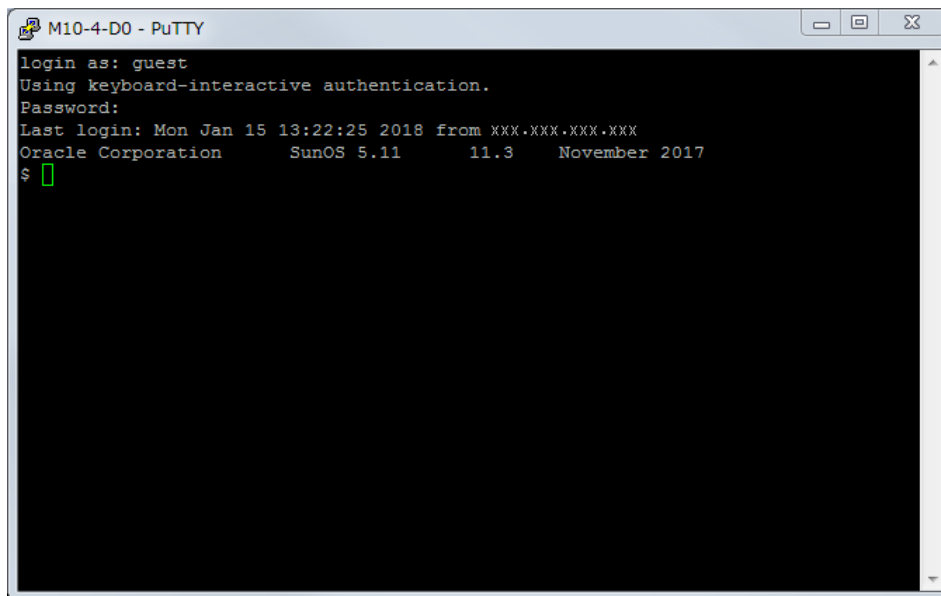
2)の i)または ii)を実施したあとのダイアログで[Open]をクリックします。



サーバに正常に接続すると、PuTTY ウィンドウにターミナルエミュレータ画面が表示され、SSH ポートフォワーディングが使用可能となります。

この画面で"login as"(ユーザー)と>Password"(パスワード)を入力します。
"login as"には、サーバに登録済みのユーザーを指定することが可能です。

[実施例:"login as"に guest を入力する場合]



- 4) 「[3.3.3 リモートデスクトップ接続](#)」の手順に進み、リモートデスクトップ接続を行います。

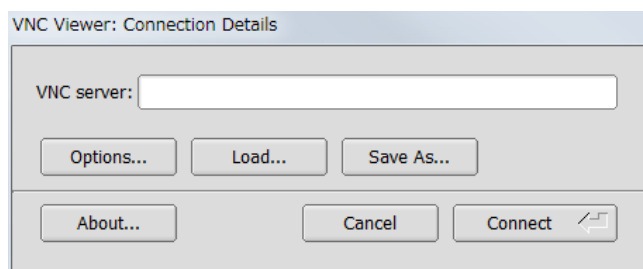
3.3.3. リモートデスクトップ接続

TigerVNC を使用してリモートデスクトップ接続を行う手順について説明します。

SSH ポートフォワーディングを使用する場合は、「[3.3.1 Tera Term の SSH ポートフォワーディングを使用する場合](#)」または「[3.3.2 PuTTY の SSH ポートフォワーディングを使用する場合](#)」の手順を実行したあとにリモートデスクトップ接続を行います。

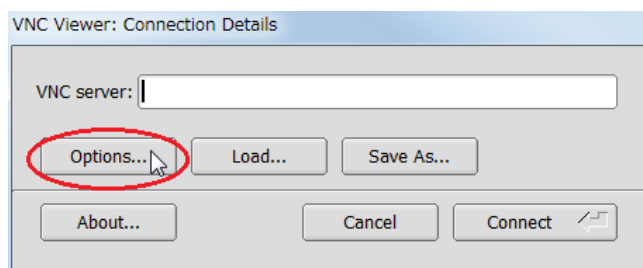
1) TigerVNC を起動します。

[VNC Viewer: Connection Details]ダイアログが表示されます。

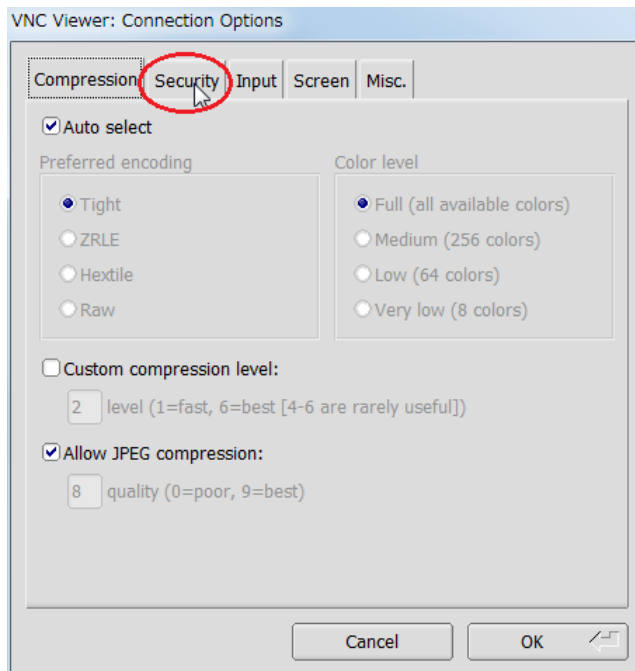


2) TigerVNC の暗号化に関する設定を行います。(初期設定時のみ)

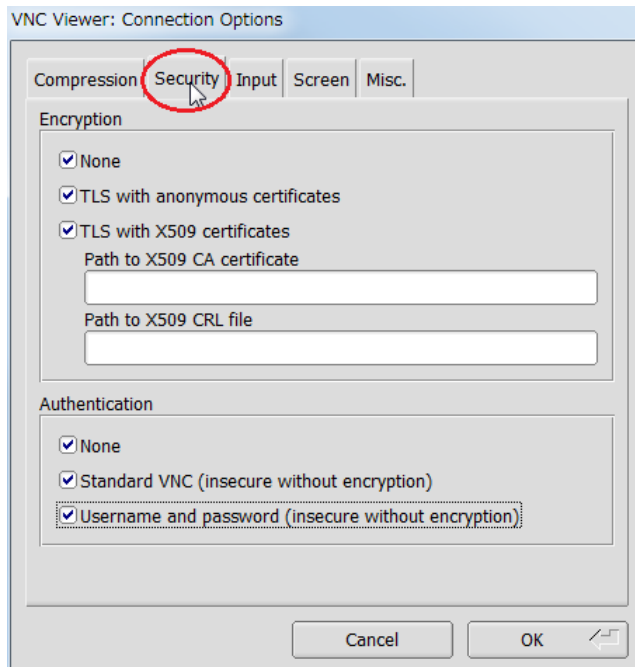
1)で表示された[VNC Viewer: Connection Details]ダイアログの"Options..."をクリックします。



"Options..."をクリック後に表示された[VNC Viewer: Connection Options]ダイアログの[Security]タブを選択します。



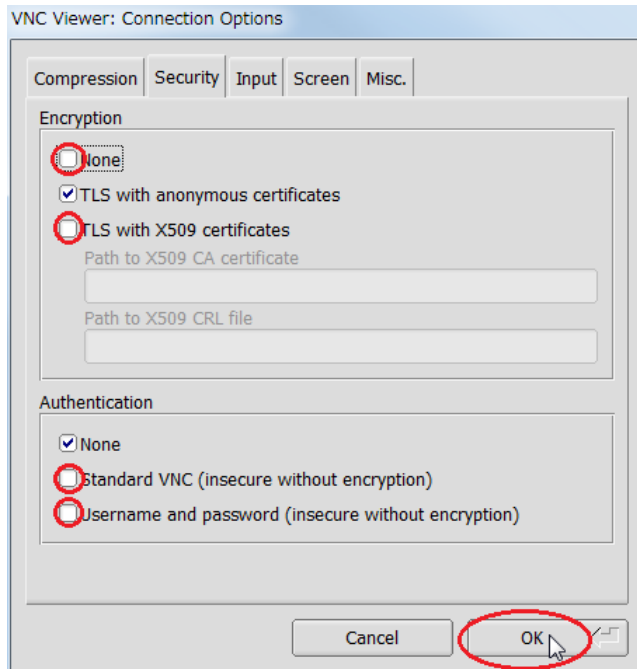
選択した[Security]タブが表示されます。



i) "TLSNone"(暗号化あり)を設定する場合

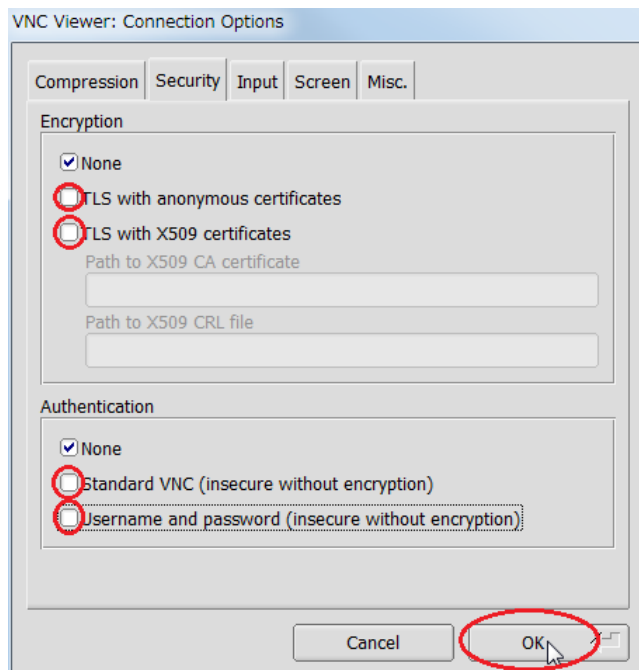
- ▶ サーバ側の OS 版数が Solaris 11.1～Solaris 11.3 SRU18032 または Solaris 10 1/13 の場合は、[ii\)](#)の手順に進みます。

[Security]タブで"Encryption"の"TLS with anonymous certificates"以外および"Authentication"の"None"以外のチェックを無効にし、[OK]をクリックします。



ii) "None"(暗号化なし)を設定する場合

[Security]タブで"Encryption"と"Authentication"の"None"以外のチェックを無効にし、[OK]をクリックします。

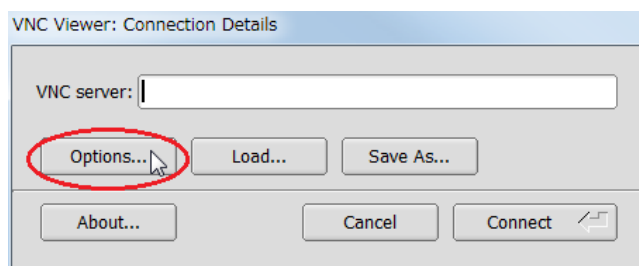


3) デスクトップの解像度を設定します。(Solaris 11 の解像度変更時のみ)

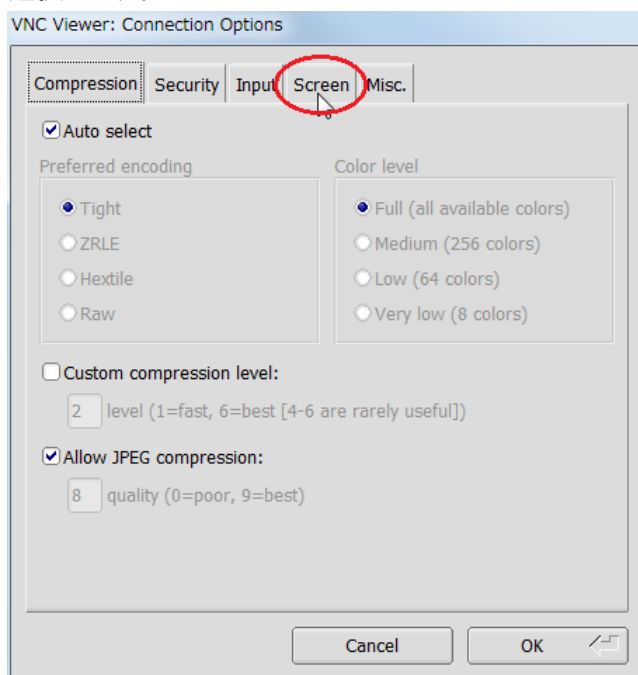
Point

Solaris 10 の場合は、クライアントでの解像度設定を無視するため、「[3.2.2 Solaris 10 cde-login サービスの場合 7\)](#)」の手順を参照し、サーバからデスクトップの解像度を設定してください。

1)で表示された[VNC Viewer: Connection Details]ダイアログの"Options..."をクリックします。

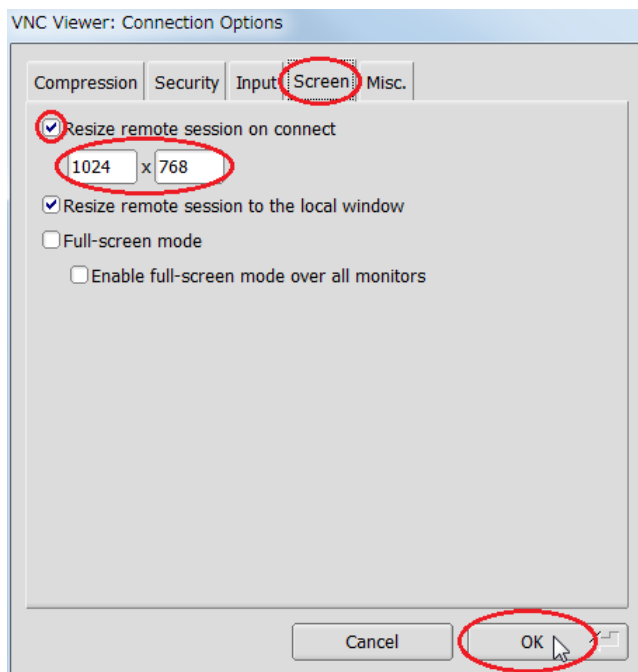


"Options..."をクリック後に表示された[VNC Viewer: Connection Options]ダイアログの[Screen]タブを選択します。



上記を選択後に表示された[Screen]タブで"Resize remote session on connect"をチェックし、デスクトップの解像度を入力後、[OK]をクリックします。

[実施例: 解像度に 1024x768 を入力する場合]



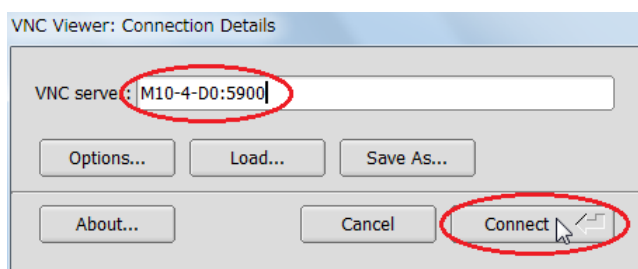
4) リモートデスクトップ接続を行います。

1)で表示された[VNC Viewer: Connection Details]ダイアログの"VNC Server"に、i)または ii)の表の項目を"ホスト:ポート番号"の書式で指定し、[Connect]をクリックします。

i) SSH ポートフォワーディングを使用しない場合

指定項目	指定内容	指定例
ホスト	サーバのホスト名または IP アドレス(xxx.xxx.xxx.xxx)	M10-4-D0:5900
ポート番号 (VNC)	「 3.2.1 Solaris 11 gdm サービスの場合 7) 」または「 3.2.2 Solaris 10 cde-login サービスの場合 8) 」で設定した VNC ポート番号	

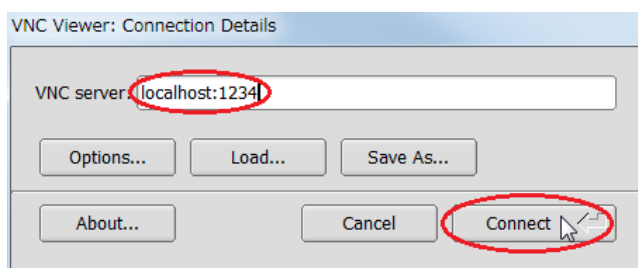
[実施例]



ii) SSH ポートフォワーディングを使用する場合

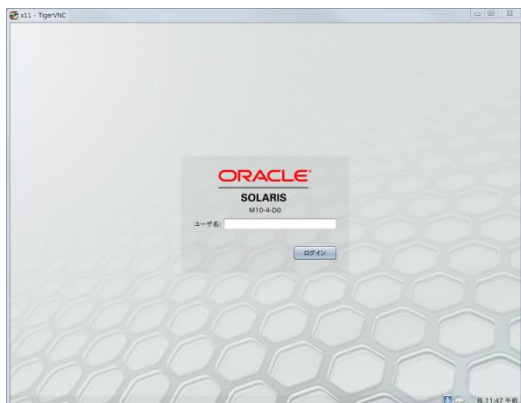
指定項目	指定内容		指定例
ホスト	クライアントのローカルホスト名 (localhost) または IP アドレス (127.0.0.1)		localhost:1234
ポート番号 (クライアント)	Tera Term	「 3.3.1 Tera Term の SSH ポートフォワーディングを使用する場合 2) 」で指定した ローカルのポート 」	
	PuTTY	「 3.3.2 PuTTY の SSH ポートフォワーディングを使用する場合 2) i) 」で指定した Source port 」	

[実施例]

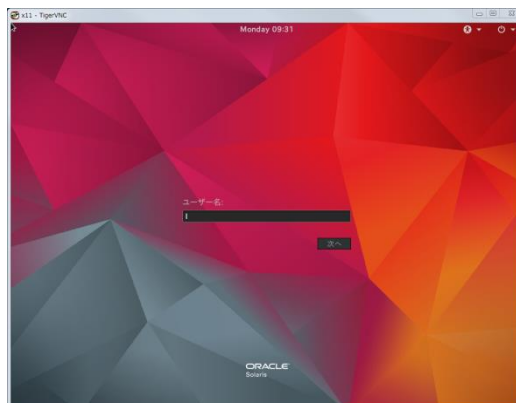


i)または ii)の指定で[Connect]をクリック後に、ディスプレイマネージャーのログイン画面が表示されます。

[例: Solaris 11.3 の場合(gdm サービス)]



[例: Solaris 11.4 の場合(gdm サービス)]



[例: Solaris 10 1/13 の場合(cde-login サービス)]



[例: Solaris 10 1/13 の場合(gdm2-login サービス)]



《注意》

- ii)の指定でリモートデスクトップを使用中の間は、「[3.3.1 Tera Term の SSH ポートフォワーディングを使用する場合](#)」または「[3.3.2 PuTTY の SSH ポートフォワーディングを使用する場合](#)」で SSH ポートフォワーディング用に接続したターミナルエミュレータを切断しないでください。
- ログイン画面が正しく表示されない場合は、「[C.2.11 TigerVNC 接続時に、ログイン画面が表示されない](#)」を参照してください。

4. リモートコンソールの接続手順

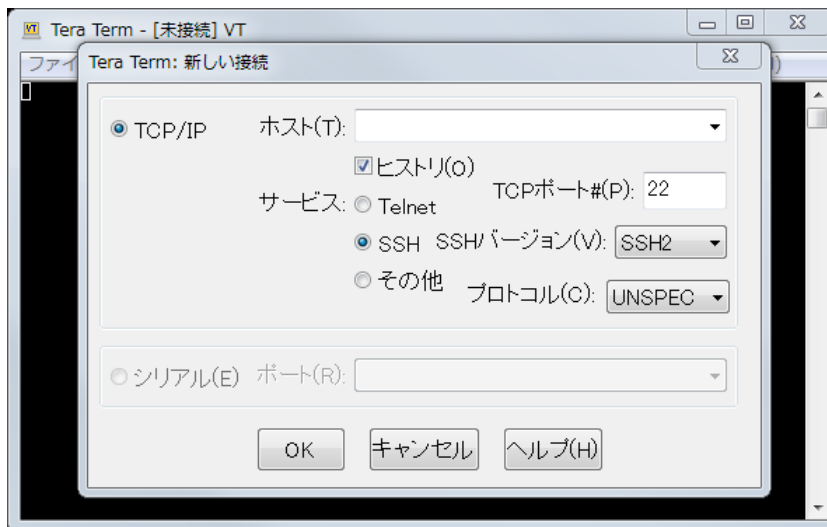
本章では、クライアント(Windows PC)におけるリモートコンソールの接続手順について説明します。

4.1. Tera Term の場合

リモートコンソールのターミナルエミュレータとして、Tera Term を使用する場合は手順を説明します。

1) Tera Term を起動します。

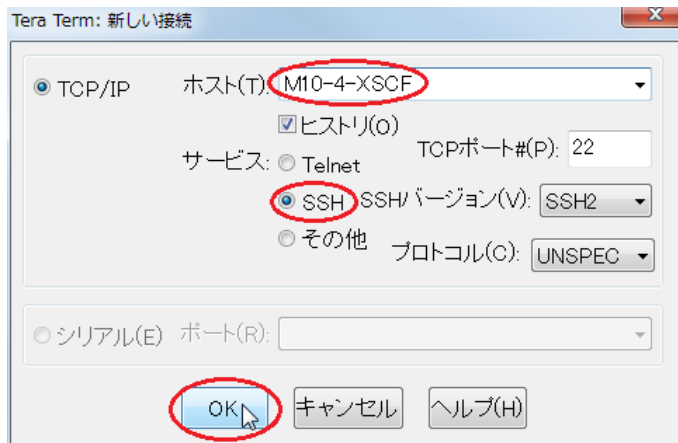
Tera Term ウィンドウと、[Tera Term: 新しい接続]ダイアログが表示されます。



2) XSCF に SSH 接続します。

1)で表示された[Tera Term: 新しい接続]ダイアログで以下の項目を指定し、[OK]をクリックします。

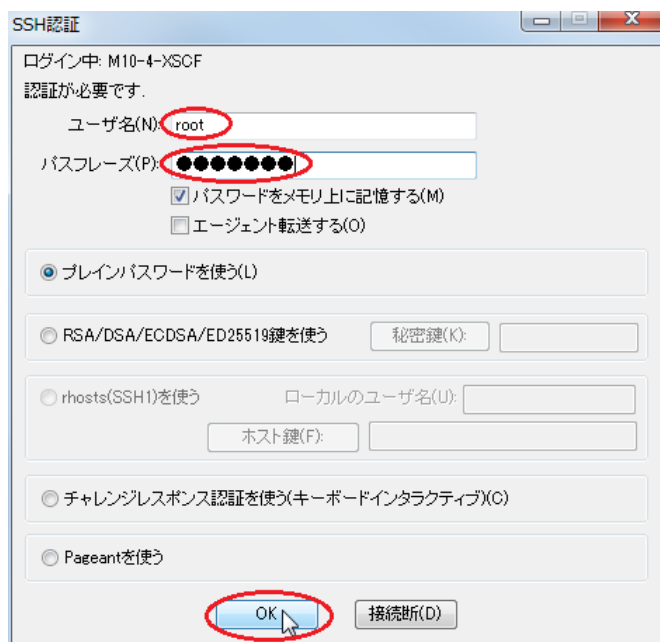
指定項目	指定内容	指定例
ホスト(T)	XSCF のホスト名または IP アドレス(xxx.xxx.xxx.xxx)	M10-4-XSCF
サービス	SSH を選択	SSH

[実施例]

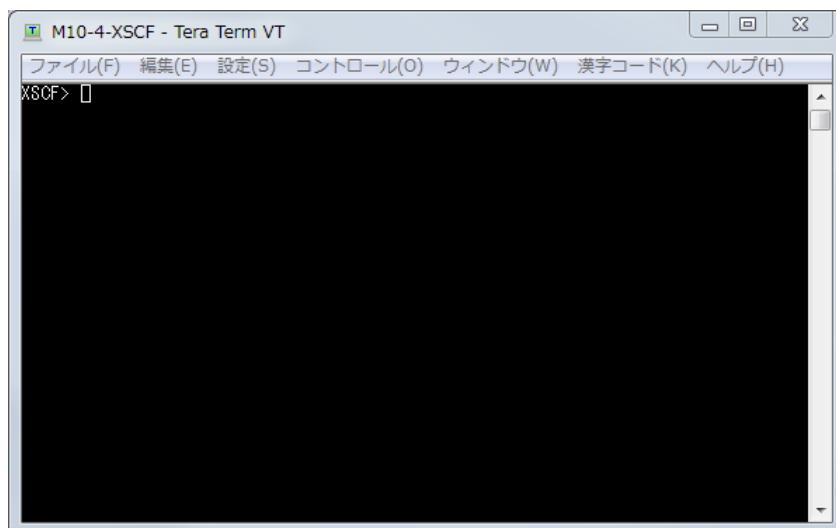
[OK]をクリック後に表示された[SSH 認証]ダイアログで、"ユーザ名(N)"と"パスワード(P)"を入力し、[OK]をクリックします。

"ユーザ名(N)"には、XSCF シェルの console コマンドが実行可能なユーザーを指定します。

[実施例:"ユーザ名(N)"に root を入力する場合]



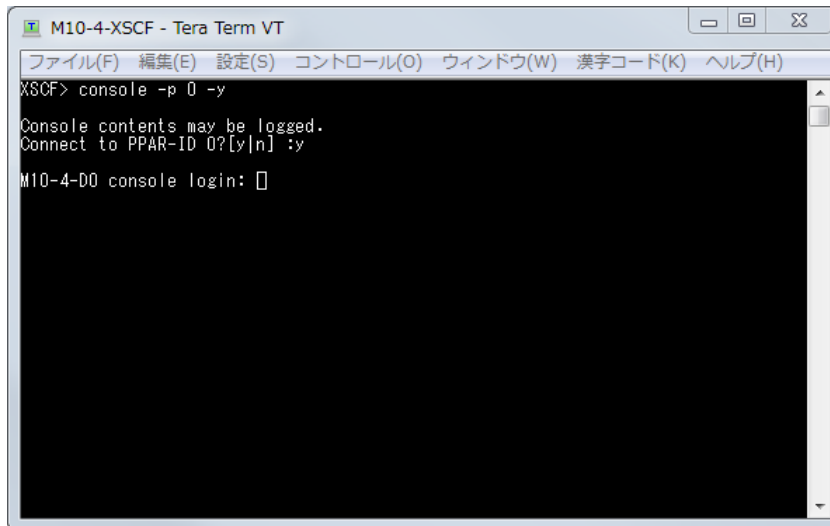
XSCF に正常に接続すると、Tera Term ウィンドウにターミナルエミュレータ画面が表示されます。



3) XSCF シェルから制御ドメインコンソールに接続します。

2)で接続したターミナルエミュレータ画面で、XSCF シェルの console コマンドを実行します。

[実施例:ドメイン 0 のコンソールに接続する場合]

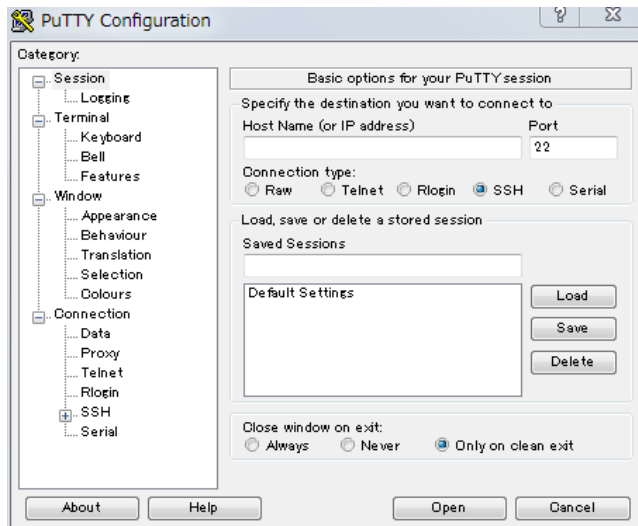


4.2. PuTTY の場合

リモートコンソールのターミナルエミュレータとして、PuTTY を使用する場合は手順を説明します。

1) PuTTY を起動します。

[PuTTY Configuration]ダイアログが表示されます。

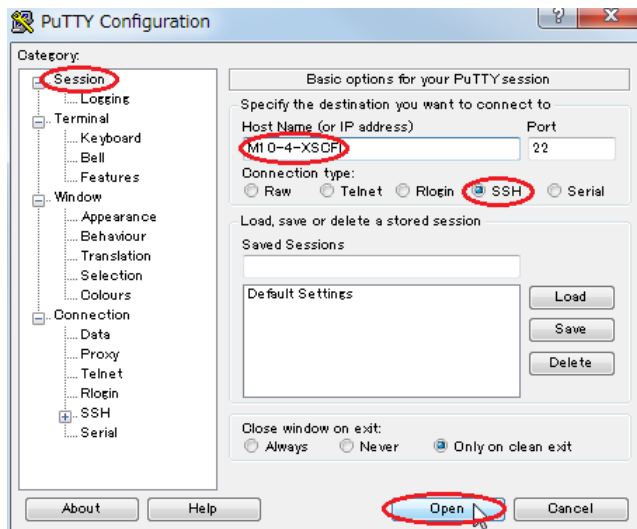


2) XSCF に SSH 接続します。

1)で表示された[PuTTY Configuration]ダイアログの[Category]から[Session]を選択した画面で以下の項目を指定し、[Open]をクリックします。

指定項目	指定内容	指定例
Host Name (or IP address)	XSCF のホスト名または IP アドレス(xxx.xxx.xxx.xxx)	M10-4-XSCF
Connection type	SSH を選択	SSH

[実施例]

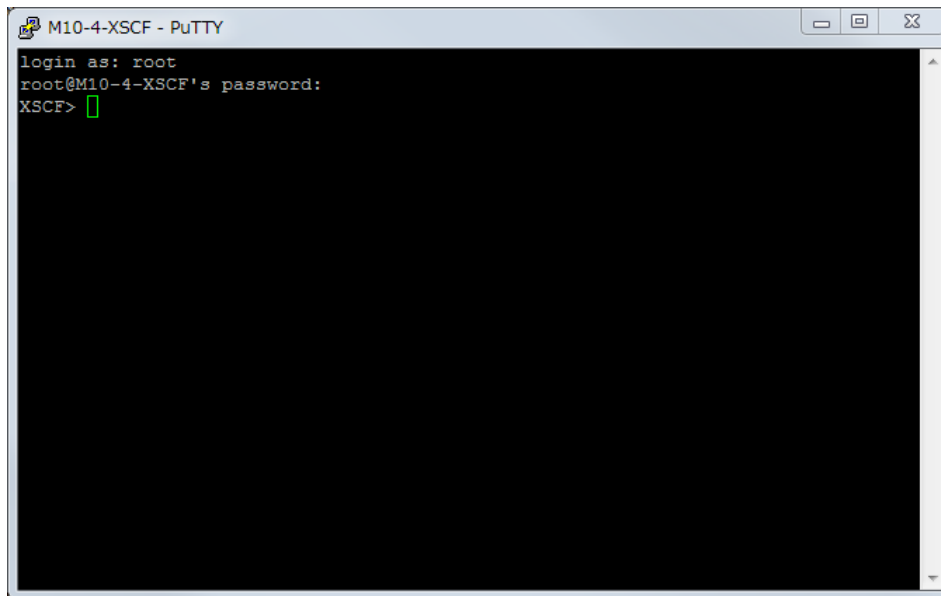


XSCF に正常に接続すると、PuTTY ウィンドウにターミナルエミュレータ画面が表示されます。

この画面で"login as"(ユーザー)と"password"(パスワード)を入力します。

"login as"には、XSCF シェルの console コマンドが実行可能なユーザーを指定します。

[実施例:"login as"に root を入力する場合]

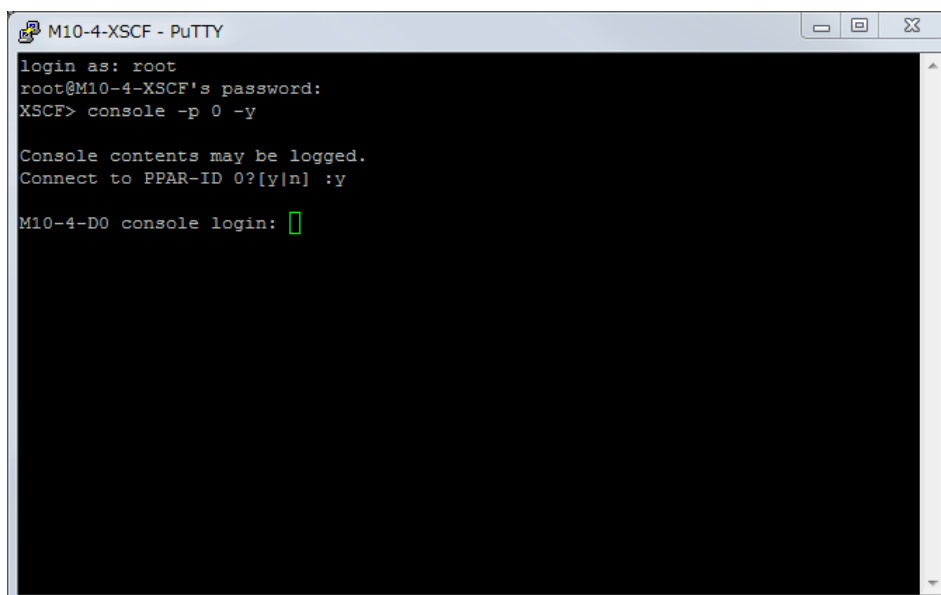


```
M10-4-XSCF - PuTTY
login as: root
root@M10-4-XSCF's password:
XSCF> 
```

3) XSCF シェルから制御ドメインコンソールに接続します。

2)で接続したターミナルエミュレータ画面で、XSCF シェルの console コマンドを実行します。

[実施例:ドメイン 0 のコンソールに接続する場合]



```
M10-4-XSCF - PuTTY
login as: root
root@M10-4-XSCF's password:
XSCF> console -p 0 -y

Console contents may be logged.
Connect to PPAR-ID 0?[y/n] :y

M10-4-D0 console login: 
```

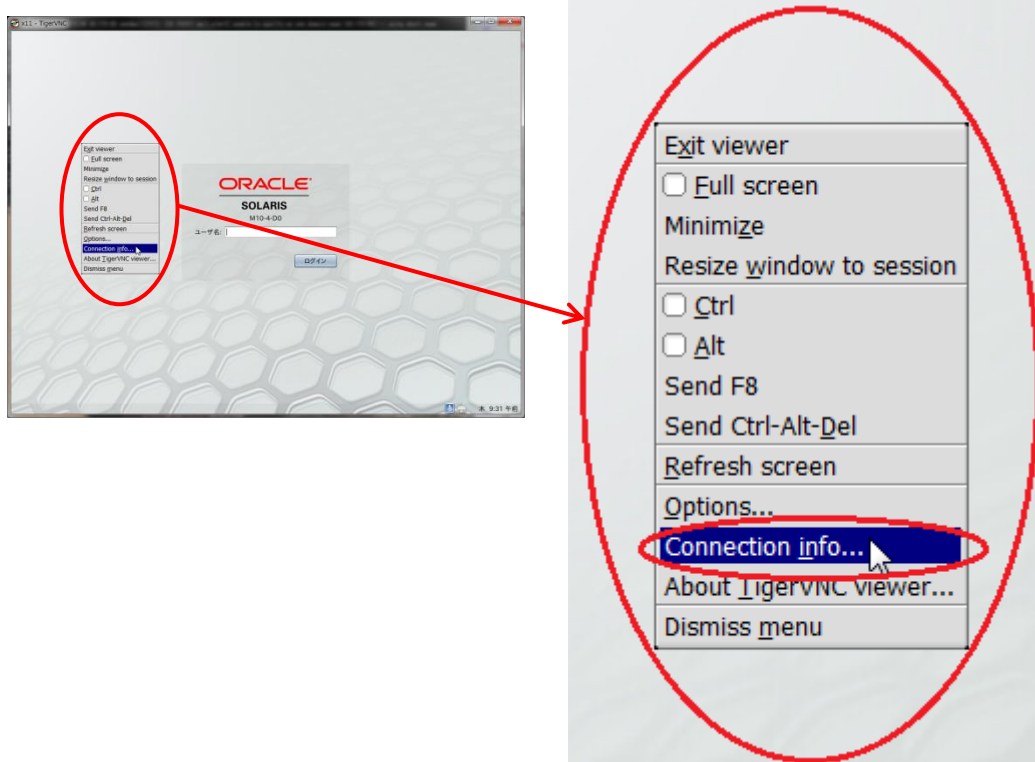
付録 A リモートデスクトップのデータ暗号化確認手順

本付録では、リモートデスクトップのデータが暗号化されているかをクライアントで確認する手順について説明します。

A.1 TigerVNC によるデータ暗号化の場合

1) TigerVNC の接続情報を表示します。

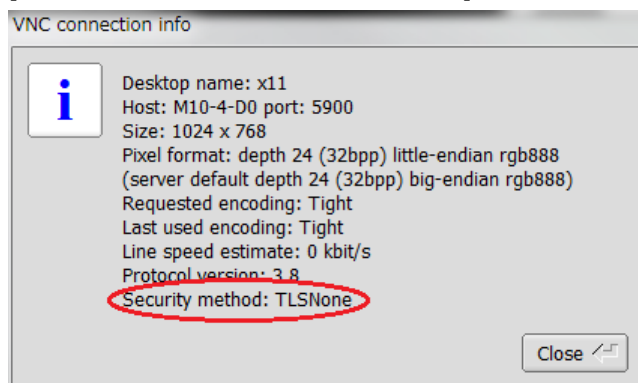
TigerVNC のログイン画面またはデスクトップ画面で[F8]キーを押下してコンテキストメニューを表示し、[Connection info...]を選択します。



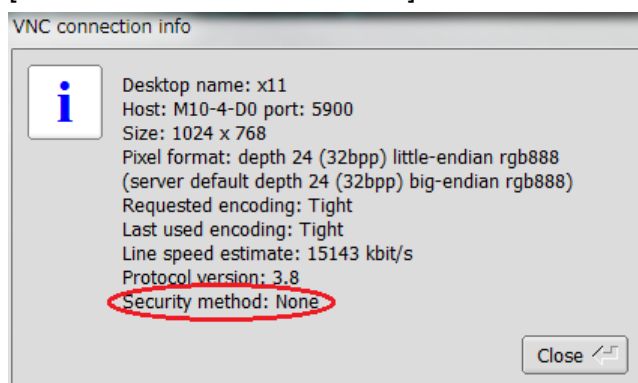
2) TigerVNC の"Security method"を確認します。

表示された[VNC connection info]により、TigerVNC の"Security method"を確認します。

[実施例: TLS で暗号化されている場合]



[実施例: 暗号化されていない場合]



<参考: TigerVNC の暗号化と認証の組合せ>

TigerVNC がサポートする暗号化と認証の組合せ(Security method)を下表に記載します。

暗号化と認証の組合せは、以下の 9 パターンとなります。

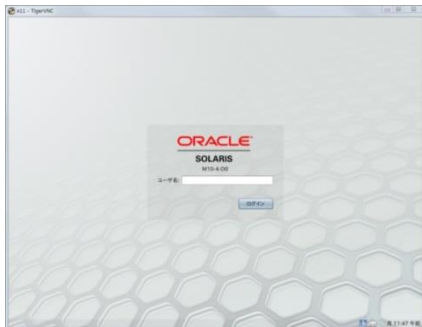
Security method		認証		
		なし	パスワード	ユーザー + パスワード
暗号化	なし	None	VncAuth	Plain
	TLS	TLSNone	TLSVnc	TLSPlain
	TLS+証明書	X509None	X509Vnc	X509Plain

本書では、"[TLSNone](#)"(暗号化: TLS、認証: なし)および"[None](#)"(暗号化: なし、認証: なし)の手順を記載しています。

A.2 SSH ポートフォワーディングによるデータ暗号化の場合

1) リモートデスクトップ接続を行います。

TigerVNC のログイン画面またはデスクトップ画面が表示された状態で、以降の手順を実施します。



2) クライアントで netstat コマンドを実行します。

Windows での確認方法は、コマンドプロンプト、PowerShell とともに共通で、以下のように指定します。

[コマンド指定方法]

```
netstat -an | findstr "クライアントの IP アドレス" | findstr "サーバの IP アドレス  
¥:590[0-6]"
```

3) 2)の実行結果により、SSH ポートフォワーディングで暗号化されているかを確認します。

SSH ポートフォワーディングで暗号化されている場合は、2)の実行結果に"ESTABLISHED"状態の VNC ポート番号(5900~5906 のいずれかの番号)が表示されません。

[実施例: SSH ポートフォワーディングで暗号化されている場合]

```
C:¥> netstat -an | findstr "192.168.1.22" | findstr "192.168.0.111¥:590[0-6]"  
←"ESTABLISHED"状態の VNC ポート番号が表示されないことを確認します。  
C:¥>
```

SSH ポートフォワーディングで暗号化されていない場合は、2)の実行結果に"ESTABLISHED"状態の VNC ポート番号が表示されます。

[実施例: SSH ポートフォワーディングで暗号化されていない場合]

```
C:¥> netstat -an | findstr "192.168.1.22" | findstr "192.168.0.111¥:590[0-6]"  
TCP      192.168.1.22:51839      192.168.0.111:5900      ESTABLISHED
```

- ▶ 上記 VNC ポート番号は、「[3.2.1 Solaris 11 gdm サービスの場合 7\)](#)」または「[3.2.2 Solaris 10 cde-login サービスの場合 8\)](#)」で指定した値です。

付録 B リモート接続手順の自動化サンプルスクリプト

本付録では、リモートデスクトップおよびリモートコンソールの接続手順を自動化するサンプルスクリプトについて説明します。

作成したサンプルスクリプトは、Windows のタスクスケジューラなどに登録することで、ログイン時に自動実行することも可能です。

B.1 リモートデスクトップ接続

B.1.1 SSH ポートフォワーディング接続用 Tera Term マクロスクリプト

本スクリプトは、「[3.3.1 Tera Term の SSH ポートフォワーディングを使用する場合](#)」で説明した手順を自動化したものです。

リモートデスクトップ接続まで行うには、「[B.1.2 TigerVNC 用 Windows バッチファイルスクリプト](#)」または「[B.1.3 TigerVNC 用 Windows PowerShell スクリプト](#)」のスクリプトを続けて実行する必要があるため、本スクリプトはこれらのスクリプトからも使用されます。

SSH ポートフォワーディングを使用せずにリモートデスクトップ接続を行う場合は、本スクリプトの実行は不要です。

1) SSH ポートフォワーディング接続用の Tera Term マクロスクリプトを作成します。(初期設定時のみ)

クライアントで作成するスクリプト名を、auto_login_ssh_tunnel.ttl として説明します。

[使用パラメーター]

パラメーター	設定内容	編集の必要性
HOST_NAME	サーバのホスト名または IP アドレス(XXX.XXX.XXX.XXX)	必須
USER_NAME	サーバにログインするためのユーザー名	必須
PASSWORD_FILE	上記 HOST_NAME と USER_NAME に対するパスワードの保存ファイル名(*1) (*2)	任意

*1: PASSWORD_FILE をファイル名のみで指定する場合は、スクリプトと同一のフォルダーに保存されます。格納パスを含めたファイル名を指定することも可能です。

*2: PASSWORD_FILE の保存フォルダーには、スクリプトの実行ユーザーに対する読み込みと書き込みのアクセス権限が必要です。

アクセス権限がないフォルダーを指定した場合は、PASSWORD_FILE で指定したファイルが以下のフォルダーに保存されます。

C:\¥Users¥[ユーザー名]\¥AppData¥Local¥VirtualStore¥Program Files¥teraterm¥

auto_login_ssh_tunnel.ttl スクリプトを以下の内容で作成し、環境に合わせて編集します。

[auto_login_ssh_tunnel.ttl の内容]

```

;-----
; サーバのホスト名または IP アドレス (xxx. xxx. xxx. xxx)
;-----
; 設定例)
;   HOST_NAME = 'M10-4-D0'
;   HOST_NAME = '192.168.0.111'
;
; "HOST_NAME = "のあとを編集します。
;   HOST_NAME = ''
;-----
; サーバにログインするためのユーザー名
;-----
; 設定例)
;   USER_NAME = 'guest'
;
; "USER_NAME = "のあとを編集します。
;   USER_NAME = ''
;-----
; 上記 HOST_NAME と USER_NAME に対するパスワードの保存ファイル名
;-----
;   必要に応じて、"PASSWORD_FILE = "のあとを編集します。
;   PASSWORD_FILE = 'password.dat'
;-----
;=====
; サーバパスワードの設定または取得
;=====
MSG_PASSWD = HOST_NAME
strconcat MSG_PASSWD '['
strconcat MSG_PASSWD USER_NAME
strconcat MSG_PASSWD ']'
getpassword PASSWORD_FILE MSG_PASSWD PASSWORD
;=====
; サーバ接続
;=====
MSG_CONNECT = HOST_NAME
strconcat MSG_CONNECT ':22 /ssh /auth=password /user='
strconcat MSG_CONNECT USER_NAME
strconcat MSG_CONNECT '/passwd='
strconcat MSG_CONNECT PASSWORD
connect MSG_CONNECT

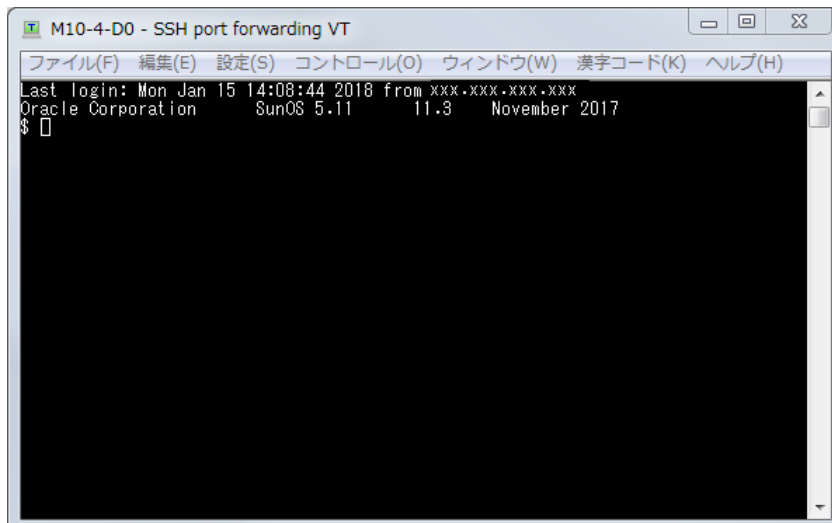
```

```
=====
: ウィンドウタイトル設定
: =====
WINDOW_TITLE = param2
strcompare WINDOW_TITLE ''
if result != 0 then
    setttitle WINDOW_TITLE
endif

end
```

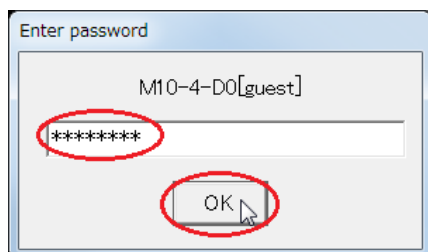
2) 1)で作成したスクリプトを実行します。

サーバに自動接続した SSH ポートフォワーディング用のターミナルエミュレータ画面が Tera Term ウィンドウに表示されます。

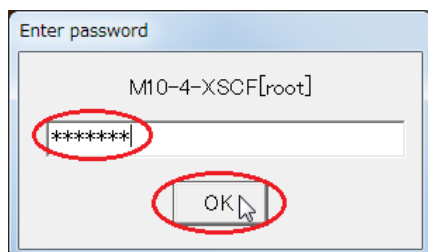


なお、初回実行時など、暗号化パスワードが未保存の状態では、[Enter password]ダイアログが表示されるため、指定したサーバのユーザーに対するパスワードを入力し、[OK]をクリックします。

[実施例: サーバのホスト名が"M10-4-D0"、ユーザーが"guest"の場合]



[実施例: XSCF のホスト名が"M10-4-XSCF"、ユーザーが"root"の場合]



一度パスワードを入力すると、PASSWORD_FILE で指定したファイルに暗号化パスワードが保存されるため、次回以降は[Enter password]ダイアログは表示されません。

PASSWORD_FILE で指定したファイルには、ホスト名、ユーザー名、およびそれらの組合せに対する暗号化パスワードが以下のように行単位で保存されます。

```
[Password]
HOST_NAME1 [USER_NAME1]=暗号化パスワード 1
HOST_NAME1 [USER_NAME2]=暗号化パスワード 2
HOST_NAME2 [USER_NAME1]=暗号化パスワード 3
:
:
```

パスワードを変更した場合は、エディタなどにより上記ファイルの該当行を削除したうえでスクリプトを実行すると、初回実行時と同様に[Enter password]ダイアログが表示されるため、変更後のパスワードを入力します。

該当行を削除せずにスクリプトを実行した場合は、古いパスワードが使用されるため、サーバ接続が失敗します。

該当行を削除する代わりに、ファイル削除によってすべての暗号化パスワードを削除することも可能です。

B.1.2 TigerVNC 用 Windows バッチファイルスクリプト

1) TigerVNC 用の Windows バッチファイルスクリプトを作成します。(初期設定時のみ)

クライアントで作成するスクリプト名を、auto_start_vnc.bat として説明します。

[使用パラメーター]

パラメーター	設定内容	編集の必要性
HOST_NAME	サーバのホスト名または IP アドレス(XXX.XXX.XXX.XXX)	必須
SSH_TUNNEL	SSH ポートフォワーディング要否フラグ 0:なし(デフォルト) 1:あり(「B.1.1 SSH ポートフォワーディング接続用 Tera Term マクロスクリプト」 のスクリプトを実行)	任意
TTP_EXE	SSH ポートフォワーディング用 Tera Term マクロの実行プログラムパス ※ SSH_TUNNEL=1 の場合に使用 ※ インストール環境に合わせて変更が必要 例:"C:¥Program Files¥teraterm¥tftpmacro.exe"	任意
TTP_MACRO	SSH ポートフォワーディング用 Tera Term マクロスクリプトパス ※ SSH_TUNNEL=1 の場合に使用 ※ 「B.1.1 SSH ポートフォワーディング接続用 Tera Term マクロスクリプト」 で作成したスクリプトパスを指定	任意
PORT_NO	SSH_TUNNEL の値により、以下のいずれかのポート番号を指定 • SSH_TUNNEL=0 の場合 「3.2.1 Solaris 11 gdm サービスの場合 7)」 または 「3.2.2 Solaris 10 cde-login サービスの場合 8)」 で設定した VNC ポート番号 • SSH_TUNNEL=1 の場合 「3.3.1 Tera Term の SSH ポートフォワーディングを使用する場合 2)」 で設定した ローカルポート	任意
PROCESS_CHECK	TigerVNC 二重起動抑止フラグ 0:なし 1:あり(デフォルト)	任意
VNC_COMMAND	TigerVNC の実行プログラムパス ※ インストール環境に合わせて変更が必要 例:"C:¥Program Files¥TigerVNC¥vncviewer.exe"	任意
VNC_OPTIONS	TigerVNC のコマンドオプション • セキュリティタイプ 【設定例】 -SecurityTypes TLSTLSNone • デスクトップの解像度(Solaris 11 のみ有効) 【設定例】 -DesktopSize 1024x768 • フルスクリーン 【設定例】 -FullScreen ※ Solaris 10 のデスクトップの解像度設定は、 「3.2.2 Solaris 10 cde-login サービスの場合 7)」 の手順を参照 ※ 詳細は TigerVNC のマニュアルを参照	任意

auto_start_vnc.bat スクリプトを以下の内容で作成し、環境に合わせて編集します。

[auto_start_vnc.bat の内容]

```
@echo off

rem -----
rem サーバのホスト名または IP アドレス (xxx. xxx. xxx. xxx)
rem -----
rem 設定例)
rem   set HOST_NAME="M10-4-D0"
rem   set HOST_NAME="192.168.0.111"

rem "set HOST_NAME="のあとを編集します。
rem   set HOST_NAME=""

rem -----
rem SSH ポートフォワーディング要否フラグ
rem -----
rem SSH_TUNNEL=0 : SSH ポートフォワーディングなし
rem SSH_TUNNEL=1 : SSH ポートフォワーディングあり

rem 必要に応じて、"set SSH_TUNNEL="のあとを編集します。
rem   set SSH_TUNNEL=0

rem -----
rem SSH ポートフォワーディング用 Tera Term マクロの実行プログラムパス
rem -----
rem 必要に応じて、"set TTP_EXE="のあとを編集します。
rem   set TTP_EXE="C:\Program Files (x86)\teraterm\ttpmacro.exe"
rem   set TTP_EXE="C:\Program Files\teraterm\ttpmacro.exe"

rem -----
rem SSH ポートフォワーディング用 Tera Term マクロスクリプトパス
rem -----
rem 必要に応じて、"set TTP_MACRO="のあとを編集します。
rem   set TTP_MACRO="C:\sample script\auto_login_ssh_tunnel.ttl"

rem -----
rem ポート番号
rem -----
rem SSH_TUNNEL=0 の場合は、VNC ポート番号 ("5900" ~ "5906" のいずれか) を指定します。
rem SSH_TUNNEL=1 の場合は、クライアント側ポート番号 (例: "1234") を指定します。

rem 必要に応じて、"set PORT_NO="のあとを編集します。
rem   set PORT_NO="5900"

rem -----
rem TigerVNC の二重起動抑止フラグ
```

```

rem -----
rem PROCESS_CHECK=0 : TigerVNC の二重起動抑止なし
rem PROCESS_CHECK=1 : TigerVNC の二重起動抑止あり

rem 必要に応じて、“set PROCESS_CHECK=”あとを編集します。
set PROCESS_CHECK=1

rem -----
rem TigerVNC の実行プログラムパス
rem -----
rem 必要に応じて、“set VNC_COMMAND=”あとを編集します。
rem set VNC_COMMAND="C:¥Program Files (x86)¥TigerVNC¥vncviewer.exe"
set VNC_COMMAND="C:¥Program Files¥TigerVNC¥vncviewer.exe"

rem -----
rem TigerVNC のコマンドオプション
rem -----
rem セキュリティタイプ :
rem Solaris 11 の場合は、“-SecurityTypes TLSNone”または“-SecurityTypes None”
rem を指定します。
rem Solaris 10 の場合は、“-SecurityTypes None”を指定します。
rem デスクトップの解像度 :
rem Solaris 11 の場合のみ、“-DesktopSize ”のあとに指定します。
rem Solaris 10 の場合は、サーバ側で指定します。
rem フルスクリーン :
rem フルスクリーン表示する場合は、“-FullScreen”を指定します。

rem 必要に応じて、“set VNC_OPTIONS=”あとを編集します。
rem set VNC_OPTIONS=-SecurityTypes None
rem set VNC_OPTIONS=-SecurityTypes None -DesktopSize 1920x1080 -FullScreen
set VNC_OPTIONS=-SecurityTypes TLSNone -DesktopSize 1024x768

rem -----

rem =====
rem 初期設定
rem =====
rem Tera Term ウィンドウタイトル
set TTP_TITLE="SSH port forwarding"

rem ネットワーク接続監視間隔(秒) ※0 を指定した場合は監視なし
set WATCH_INTERVAL=120

rem TigerVNC 接続先 ホスト:ポート
if %SSH_TUNNEL% == 1 (
set HOST_PORT="localhost:%PORT_NO%"
) else (

```



```
        set HOST_PORT="%HOST_NAME%:%PORT_NO%"
    )

rem =====
rem TigerVNC の二重起動抑止
rem =====
if %PROCESS_CHECK% == 1 (
    tasklist | findstr "vncviewer" > NUL
    if ERRORLEVEL 1 goto :LOOP
    rem =====
    rem すでにプロセスあり(二重起動) --> 終了
    rem =====
    echo "すでに vncviewer のプロセスが存在します。"
    timeout 5
    exit /B 1
)

:LOOP
rem =====
rem ホストのネットワーク疎通確認
rem =====
ping -n 1 %HOST_NAME% > NUL
if %ERRORLEVEL% == 0 (
    rem =====
    rem ネットワーク接続が可能な場合
    rem =====
    if %SSH_TUNNEL% == 1 (
        tasklist /v /fi "imagename eq ttermpro.exe" | findstr %TTP_TITLE% > NUL
        if not ERRORLEVEL 1 goto :VNC_START
        rem =====
        rem SSH ポートフォワーディング用 Tera Term マクロスクリプト実行
        rem =====
        start "" /WAIT %TTP_EXE% %TTP_MACRO% %TTP_TITLE%
    )
) else (
    rem =====
    rem ネットワーク接続が不可能な場合
    rem =====
    if %WATCH_INTERVAL% == 0 (
        rem =====
        rem ネットワーク接続監視なし --> 終了
        rem =====
        echo "ネットワークに接続できません。"
        timeout 5
        exit /B 1
    )
    echo "ネットワーク接続を監視します。"
    timeout %WATCH_INTERVAL%
```

```
        goto :LOOP
    )

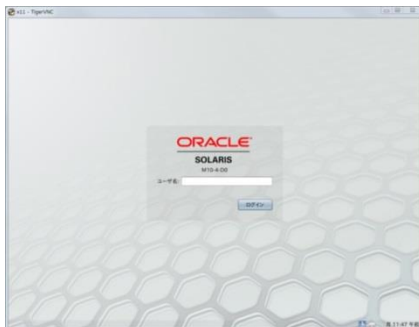
:VNC_START
rem =====
rem TigerVNC 起動
rem =====
start "" %VNC_COMMAND% %HOST_PORT% %VNC_OPTIONS%

exit /B 0
```

2) 1)で作成したスクリプトを実行します。

編集したスクリプトのパラメーター内容でリモートデスクトップ接続を行います。

[実施例: Solaris 11.3 の場合]



B.1.3 TigerVNC 用 Windows PowerShell スクリプト

1) TigerVNC 用の Windows PowerShell スクリプトを作成します。(初期設定時のみ)

クライアントで作成するスクリプト名を、auto_start_vnc.ps1 として説明します。

[使用パラメーター]

パラメーター	設定内容	編集の必要性
host_name	サーバのホスト名または IP アドレス(XXX.XXX.XXX.XXX)	必須
ssh_tunnel	SSH ポートフォワーディング要否フラグ 0:なし(デフォルト) 1:あり(「B.1.1 SSH ポートフォワーディング接続用 Tera Term マクロスクリプト」 のスクリプトを実行)	任意
ttp_exe	SSH ポートフォワーディング用 Tera Term マクロの実行プログラムパス ※ ssh_tunnel=1 の場合に使用 ※ インストール環境に合わせて変更が必要 例:"C:¥Program Files¥teraterm¥ttpmacro.exe"	任意
ttp_macro	SSH ポートフォワーディング用 Tera Term マクロスクリプトパス ※ ssh_tunnel=1 の場合に使用 ※ 「B.1.1 SSH ポートフォワーディング接続用 Tera Term マクロスクリプト」 で作成したスクリプトパスを指定	任意
port_no	ssh_tunnel の値により、以下のいずれかのポート番号を指定 • ssh_tunnel=0 の場合 「3.2.1 Solaris 11 gdm サービスの場合 7)」 または 「3.2.2 Solaris 10 cde-login サービスの場合 8)」 で設定した VNC ポート番号 • ssh_tunnel=1 の場合 「3.3.1 Tera Term の SSH ポートフォワーディングを使用する場合 2)」 で設定した ローカルポート	任意
process_check	TigerVNC 二重起動チェック要否フラグ 0:なし 1:あり(デフォルト)	任意
vnc_command	TigerVNC の実行プログラムパス ※ インストール環境に合わせて変更が必要 例:" C:¥Program Files¥TigerVNC¥vncviewer.exe"	任意
vnc_options	TigerVNC のコマンドオプション • セキュリティタイプ 【設定例】 -SecurityTypes TLSNone • デスクトップの解像度(Solaris 11 のみ有効) 【設定例】 -DesktopSize 1024x768 • フルスクリーン 【設定例】 -FullScreen ※ Solaris 10 のデスクトップの解像度設定は、 「3.2.2 Solaris 10 cde-login サービスの場合 7)」 の手順を参照 ※ 詳細は TigerVNC のマニュアルを参照	任意

auto_start_vnc.ps1 スクリプトを以下の内容で作成し、環境に合わせて編集します。

[auto_start_vnc.ps1 の内容]

```
# -----
# サーバのホスト名または IP アドレス (xxx. xxx. xxx. xxx)
# -----
# 設定例)
#   $host_name = "M10-4-D0"
#   $host_name = "192.168.0.111"
#
# "$host_name = "のあとを編集します。
# $host_name = ""
#
# -----
# SSH ポートフォワーディング要否フラグ
# -----
# $ssh_tunnel = 0 : SSH ポートフォワーディングなし
# $ssh_tunnel = 1 : SSH ポートフォワーディングあり
#
# 必要に応じて、"$ssh_tunnel = "のあとを編集します。
# $ssh_tunnel = 0
#
# -----
# SSH ポートフォワーディング用 Tera Term マクロの実行プログラムパス
# -----
# 必要に応じて、"$ttp_exe = "のあとを編集します。
# $ttp_exe = "C:\Program Files (x86)\teraterm\ttpmacro.exe"
# $ttp_exe = "C:\Program Files\teraterm\ttpmacro.exe"
#
# -----
# SSH ポートフォワーディング用 Tera Term マクロスクリプトパス
# -----
# 必要に応じて、"$ttp_macro = "のあとを編集します。
# $ttp_macro = "C:\sample script\auto_login_ssh_tunnel.ttl"
#
# -----
# ポート番号
# -----
# $ssh_tunnel = 0 の場合は、VNC ポート番号 ("5900" ~ "5906" のいずれか) を指定します。
# $ssh_tunnel = 1 の場合は、クライアント側ポート番号 (例: "1234") を指定します。
#
# 必要に応じて、"$port_no = "のあとを編集します。
# $port_no = "5900"
#
# -----
# TigerVNC の二重起動抑止フラグ
# -----
# $process_check = 0 : TigerVNC の二重起動抑止なし
```

```
# $process_check = 1 : TigerVNC の二重起動抑止あり

# 必要に応じて、“$process_check = ”のあとを編集します。
$process_check = 1

# -----
# TigerVNC の実行プログラムパス
# -----
# 必要に応じて、“$vnc_command = ”のあとを編集します。
# $vnc_command = "C:¥Program Files (x86)¥TigerVNC¥vncviewer.exe"
# $vnc_command = "C:¥Program Files¥TigerVNC¥vncviewer.exe"

# -----
# TigerVNC のコマンドオプション
# -----
# セキュリティタイプ :
#     Solaris 11 の場合は、“-SecurityTypes TLSNone”または“-SecurityTypes None”
#     を指定します。
#     Solaris 10 の場合は、“-SecurityTypes None”を指定します。
# デスクトップの解像度 :
#     Solaris 11 の場合のみ、“-DesktopSize ”のあとに指定します。
#     Solaris 10 の場合は、サーバ側で指定します。
# フルスクリーン :
#     フルスクリーン表示する場合は、“-FullScreen”を指定します。

# 必要に応じて、“$vnc_options = ”のあとを編集します。
# $vnc_options = "-SecurityTypes None"
# $vnc_options = "-SecurityTypes None -DesktopSize 1920x1080 -FullScreen"
# $vnc_options = "-SecurityTypes TLSNone -DesktopSize 1024x768"

# -----

# =====
# 初期設定
# =====
# Tera Term ウィンドウタイトル
# $ttp_title="SSH port forwarding"

# ネットワーク接続監視間隔(秒) ※0 を指定した場合は監視なし
# $watch_interval = 120

# TigerVNC 接続先 ホスト:ポート
# if ($ssh_tunnel -eq 1) {
#     $port = "localhost" + ":" + $port_no
# } else {
#     $port = $host_name + ":" + $port_no
# }
```

```
# =====
# TigerVNC の二重起動抑止
# =====
if ($process_check -eq 1) {
    Get-Process "vncviewer" -ErrorAction SilentlyContinue > $null
    if ($? -eq $true) {
        # =====
        #  すでにプロセスあり(二重起動) --> 終了
        # =====
        Write-Host "すでに vncviewer のプロセスが存在します。"
        timeout 5
        exit 1
    }
}

While ($true) {
    # =====
    #  ホストのネットワーク疎通確認
    # =====
    ping -n 1 $host_name > $null
    if ($? -eq $true) {
        # =====
        #  ネットワーク接続が可能な場合
        # =====
        if ($ssh_tunnel -eq 1) {
            Get-Process | Where-Object {$_.Name -eq 'ttermpro'} | Select-Object
MainWindowTitle | findstr $ttp_title > $null
            if ($? -eq $false) {
                # =====
                #  SSH ポートフォワーディング用 Tera Term マクロスクリプト実行
                # =====
                &"$ttp_exe" "$ttp_macro" "$ttp_title"
                # =====
                #  Tera Term マクロスクリプト実行待ち時間を設定(3 秒)
                # =====
                Start-Sleep -s 3
            }
        }
        break
    } else {
        # =====
        #  ネットワーク接続が不可能な場合
        # =====
        if ($watch_interval -eq 0) {
            # =====
            #  ネットワーク接続監視なし --> 終了
            # =====
        }
    }
}
```

```

        Write-Host "ネットワークに接続できません。"
        timeout 5
        exit 1
    }
    Write-Host "ネットワーク接続を監視します。"
    timeout $watch_interval
}
}

# =====
#   TigerVNC 起動
#   =====
Start-Process $vnc_command -ArgumentList "$port $vnc_options"

exit 0

```

2) PowerShell スクリプトの実行セキュリティポリシーを確認します。(初期設定時のみ)

[実施例]

```
PS C:\> Get-ExecutionPolicy
Restricted
```

実行ポリシーが"RemoteSigned"の場合は、[4\)](#)の手順に進みます。

3) PowerShell スクリプトの実行セキュリティポリシーを"RemoteSigned"に変更します。(初期設定時のみ)

実行ポリシーが"RemoteSigned"以外の場合は、PowerShell の管理者権限で"RemoteSigned"への変更と変更確認を行います。

[実施例]

```
PS C:\> Set-ExecutionPolicy RemoteSigned
```

実行ポリシーの変更

実行ポリシーは、信頼されていないスクリプトからの保護に役立ちます。実行ポリシーを変更すると、`about_Execution_Policies` のヘルプトピックで説明されているセキュリティ上の危険にさらされる可能性があります。実行ポリシーを変更しますか？

[Y] はい(Y) [N] いいえ(N) [S] 中断(S) [?] ヘルプ (既定値は "Y"): Y

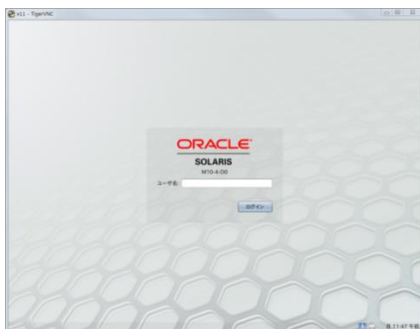
```
PS C:\>
```

```
PS C:\> Get-ExecutionPolicy
RemoteSigned
```

4) 1)で作成したスクリプトを実行します。

編集したスクリプトのパラメーター内容でリモートデスクトップ接続を行います。

[実施例: Solaris 11.3 の場合]



Point

スクリプト実行時に以下のメッセージが表示された場合は、"Y"を入力して続行してください。

実行ポリシーの変更

実行ポリシーは、信頼されていないスクリプトからの保護に役立ちます。実行ポリシーを変更すると、`about_Execution_Policies` のヘルプトピックで説明されているセキュリティ上の危険にさらされる可能性があります。実行ポリシーを変更しますか？

[Y] はい(Y) [N] いいえ(N) [S] 中断(S) [?] ヘルプ (既定値は "Y"): Y

B.2 リモートコンソール接続

B.2.1 リモートコンソール接続用 Tera Term マクロスクリプト

本スクリプトは、「[4.1 Tera Term の場合](#)」で説明した手順を自動化したものです。

1) リモートコンソール接続用の Tera Term マクロスクリプトを作成します。(初期設定時のみ)

クライアントで作成するスクリプト名を、auto_login_console.ttl として説明します。

[使用パラメーター]

パラメーター	設定内容	編集の 必要性
HOST_NAME	XSCF のホスト名または IP アドレス(XXX.XXX.XXX.XXX)	必須
USER_NAME	XSCF にログインするためのユーザー名	必須
PASSWORD_FILE	上記 HOST_NAME と USER_NAME に対するパスワードの 保存ファイル名(*1) (*2)	任意
CONSOLE_COMMAND	制御ドメインコンソール接続コマンド	任意

*1: PASSWORD_FILE をファイル名のみで指定する場合は、スクリプトと同一のフォルダーに保存されます。格納パスを含めたファイル名を指定することも可能です。

*2: PASSWORD_FILE の保存フォルダーには、スクリプトの実行ユーザーに対する読み込みと書き込みのアクセス権限が必要です。

アクセス権限がないフォルダーを指定した場合は、PASSWORD_FILE で指定したファイルが以下のフォルダーに保存されます。

C:\¥Users¥[ユーザー名]\¥AppData¥Local¥VirtualStore¥Program Files¥teraterm¥

auto_login_console.ttl スクリプトを以下の内容で作成し、環境に合わせて編集します。

[auto_login_console.ttl の内容]

```

;-----
; XSCF のホスト名または IP アドレス (xxx. xxx. xxx. xxx)
;-----
; 設定例)
;   HOST_NAME = 'M10-4-XSCF'
;   HOST_NAME = '192.168.2.100'
;
; "HOST_NAME = "のあとを編集します。
; HOST_NAME = ''
;-----
; XSCF にログインするためのユーザー名
;-----
; 設定例)
;   USER_NAME = 'root'
;
; "USER_NAME = "のあとを編集します。
; USER_NAME = ''
;-----
; 上記 HOST_NAME と USER_NAME に対するパスワードの保存ファイル名
;-----
; 必要に応じて、"PASSWORD_FILE = "のあとを編集します。
; PASSWORD_FILE = 'password.dat'
;-----
; 制御ドメインコンソール接続コマンド
;-----
; 必要に応じて、"CONSOLE_COMMAND = "のあとを編集します。
; CONSOLE_COMMAND = 'console -p 0 -y -f'
;-----
;-----
; XSCF パスワードの設定または取得
;=====
MSG_PASSWD = HOST_NAME
strconcat MSG_PASSWD '['
strconcat MSG_PASSWD USER_NAME
strconcat MSG_PASSWD ']'
getpassword PASSWORD_FILE MSG_PASSWD PASSWORD
;=====
; XSCF 接続

```

```
=====
MSG_CONNECT = HOST_NAME
strconcat MSG_CONNECT ':22 /ssh /auth=password /user='
strconcat MSG_CONNECT USER_NAME
strconcat MSG_CONNECT '/passwd='
strconcat MSG_CONNECT PASSWORD
connect MSG_CONNECT

=====
; 制御ドメインコンソール接続
=====

wait 'XSCF'
sendln CONSOLE_COMMAND
sendln

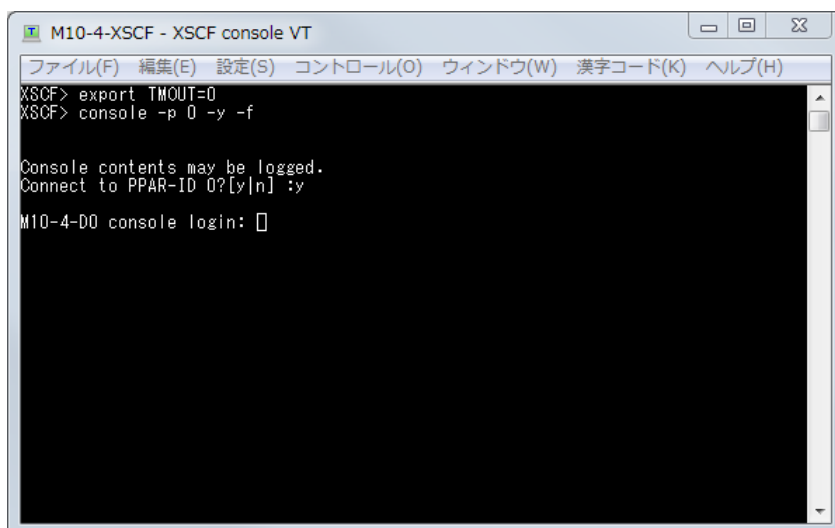
=====
; ウィンドウタイトル設定
=====

WINDOW_TITLE = 'XSCF console'
settitle WINDOW_TITLE

end
```

2) 1)で作成したスクリプトを実行します。

XSCF に SSH で接続した Tera Term ウィンドウのターミナルエミュレータ画面から、リモートコンソールに自動接続します。



[Enter password]ダイアログが表示された場合は、[「B.1.1 SSH ポートフォワーディング接続用 Tera Term マクロスクリプト 2\)」](#)の手順を参照してください。

B.2.2 GNOME 内でのリモートコンソール接続用シェルスクリプト

本スクリプトは、リモートデスクトップ(GNOME)内でのリモートコンソール接続を自動化したものです。
このスクリプトを GNOME の自動起動アプリに登録することで、GNOME へのログイン時に自動実行することが可能です。

本項のオペレーションは、GNOME に guest でログインすることを前提に説明します。

1) xterm の自動実行シェルスクリプトを作成します。(初期設定時のみ)

GNOME に guest でログインした環境で作成するスクリプト名(絶対パス)を、
/export/home/guest/auto_login_console.sh として説明します。

[使用パラメーター]

パラメーター	設定内容	編集の 必要性
HOST_NAME	XSCF のホスト名または IP アドレス(XXX.XXX.XXX.XXX)	必須
USER_NAME	XSCF にログインするためのユーザー名	必須
PASSWORD	上記ユーザー名に対するパスワード	必須
PPAR_ID	接続サーバの制御ドメインコンソールに対する PPAR-ID	任意

auto_login_console.sh スクリプトを以下の内容で作成し、環境に合わせて編集します。

作成したスクリプトには、実行権の付与が必要です。

[auto_login_console.sh の内容]

```
#!/bin/bash

#-----
# XSCF のホスト名または IP アドレス (xxx. xxx. xxx. xxx)
#-----
# 設定例)
#   HOST_NAME=' M10-4-XSCF'
#   HOST_NAME=' 192. 168. 2. 100'

# "HOST_NAME="のあとを編集します。
HOST_NAME=' '

#-----
# XSCF にログインするためのユーザー名
#-----
# 設定例)
#   USER_NAME=' root'

# "USER_NAME="のあとを編集します。
USER_NAME=' '

#-----
# 上記ユーザー名に対するパスワード
#-----
# "PASSWORD="のあとを編集します。
PASSWORD=' '

#-----
# 接続サーバの制御ドメインコンソールの PPAR-ID
#-----
# 必要に応じて、“PPAR_ID=”のあとを編集します。
PPAR_ID=' 0'

#-----

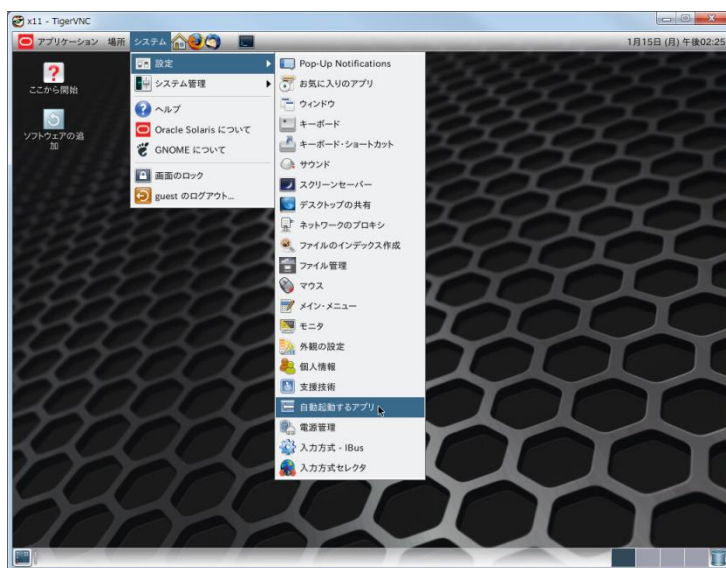
#=====
# 制御ドメインコンソール接続
#=====
expect -c "
set timeout -1
spawn /usr/bin/ssh ${USER_NAME}@${HOST_NAME} -o "StrictHostKeyChecking=no"
expect ¥"password:¥"
send ¥"${PASSWORD}¥n¥"
```

```
expect ¥"XSCF¥"
send ¥"console -y -p $ {PPAR_ID} -f¥n¥"
send ¥"¥n¥"
interact
"
```

2) 1)で作成したスクリプトを GNOME の自動起動アプリに登録します。(初期設定時のみ)

i) GNOME2(Solaris 11.3 以前)の場合

guest でログインした GNOME2 のメニューバーから、[システム]-[設定]-[自動起動するアプリ]を選択します。



上記を選択後に表示された[自動起動するアプリの設定]ダイアログの[自動起動するプログラム]タブで、[追加]をクリックします。

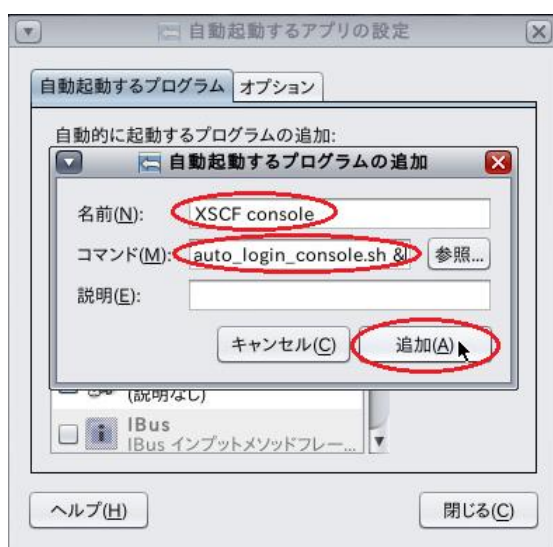


[追加]をクリック後に表示された[自動起動するプログラムの追加]ダイアログで以下の項目を設定し、[追加]をクリックします。

設定項目	設定内容	設定例
名前(N)	[自動起動するプログラム]の登録名	XSCF console
コマンド(M)	[自動起動するプログラム]に登録するコマンドライン(*1)	/usr/bin/xterm -title "Console" -sb -rightbar -e /export/home/guest/auto_login_console.sh &

*1: xterm コマンドの-e オプションのパラメーターには、[1](#))で作成したスクリプト名を絶対パスで指定します。

[実施例]



戻ったダイアログで[閉じる]をクリックします。



ii) GNOME3(Solaris 11.4 以降)の場合

guest で GNOME3 ヘログインしたあと、端末を起動します。



起動した端末で、自動起動アプリを格納するためのディレクトリ(`${HOME}/.config/autostart`)を作成し、このディレクトリに移動します。

```
# mkdir ${HOME}/.config/autostart
# cd ${HOME}/.config/autostart
```

autostart ディレクトリに移動したあと、以下の例を参考に、自動起動アプリを `xterm.desktop` として作成します。

[xterm.desktop の作成例]

```
# ここから編集不可
[Desktop Entry]
Type=Application
# ここまで編集不可

Exec=/usr/bin/xterm -title "Console" -sb -rightbar -e
/export/home/guest/auto_login_console.sh &
```


xterm.desktop の変更可能なパラメーターは、以下のように設定します。

パラメーター	設定内容	設定例
Exec	自動起動アプリに登録する コマンドライン(*1)	/usr/bin/xterm -title "Console" -sb -rightbar -e /export/home/guest/auto_login_console.sh &

*1: xterm コマンドの -e オプションのパラメーターには、[1\)](#)で作成したスクリプト名を絶対パスで指定します。

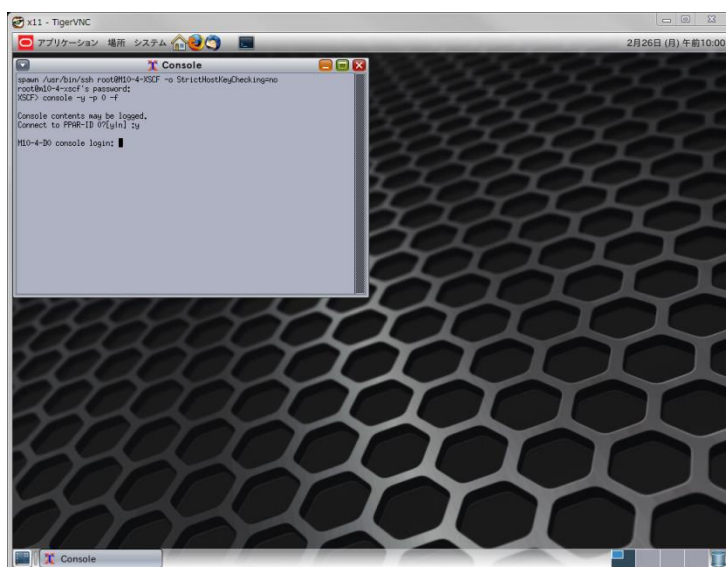
Point

自動起動アプリの拡張子は必ず".desktop"とする必要がありますが、アプリ名(本項では xterm)は任意に変更が可能です。

3) GNOME にログインし、1)で作成したスクリプトを自動実行します。

2)まで完了した状態で GNOME に guest でログインし、1)で作成したスクリプトの自動実行により、リモートコンソールに接続します。

[実施例:GNOME2 の場合]



付録 C トラブルシューティング

C.1 サーバで検出したトラブル

C.1.1 xvnc-inetd サービス起動時に、サービスの状態が"maintenance"に遷移する

■現象

xvnc-inetd サービスの起動(enable)、再起動(restart)、または再読み取り(refresh)を行うと、xvnc-inetd サービスの状態が"maintenance"に遷移します。

[例: xvnc-inetd サービス起動時に、状態が"maintenance"に遷移した場合]

```
# svcadm enable xvnc-inetd
# svcs xvnc-inetd
STATE          STIME      FMRI
maintenance    16:20:19  svc:/application/x11/xvnc-inetd:default
```

■原因

/etc/services ファイルに"vnc-server"が正しく登録されていない可能性があります。

■対処方法

最初に xvnc-inetd サービスを停止し、サービスの状態が"disabled"に遷移したことを確認してください。

```
# svcadm disable xvnc-inetd
# svcs xvnc-inetd
STATE          STIME      FMRI
disabled       16:23:29  svc:/application/x11/xvnc-inetd:default
```

確認した状態が"online*"の場合は、状態遷移中のため、しばらくしてから状態を再確認します。

- ▶ サービスの状態が"disabled"に遷移しない場合は、[「C.1.3 サービス停止時に、サービスの状態が"disabled"に遷移しない」](#)を参照してください。

次に下表の手順を参照し、/etc/services ファイルに"vnc-server"を正しく登録したうえで、xvnc-inetd サービスを起動してください。

OS	手順参照先
Solaris 11	3.2.1 Solaris 11 gdm サービスの場合 7) ～ 9)
Solaris 10	3.2.2 Solaris 10 cde-login サービスの場合 8) ～ 10)

C.1.2 サービス起動時に、サービスの状態が"online"に遷移しない

■現象

svcadm コマンドによりサービスの起動(enable)、再起動(restart)、または再読み取り(refresh)を行っても、サービスの状態が"online"に遷移しません。

[例:gdm サービス再起動時に、状態が"disabled"に遷移した場合]

```
# svcadm restart gdm
# svcs gdm
STATE          STIME      FMRI
disabled       14:45:08  svc:/application/graphical-login/gdm:default
```

C.1.3 サービス停止時に、サービスの状態が"disabled"に遷移しない

■現象

svcadm コマンドによりサービスを停止しても、サービスの状態が"disabled"に遷移しません。

[例:xvnc-inetd サービス停止時に、状態が"degraded"に遷移した場合]

```
# svcadm disable xvnc-inetd
# svcs xvnc-inetd
STATE          STIME      FMRI
degraded       16:23:29  svc:/application/x11/xvnc-inetd:default
```

C.1.4 サービスの状態が"degraded"、"maintenance"、または"offline"となっている

■現象

確認したサービスの状態が"degraded"、"maintenance"、または"offline"となっています。

[例:確認した ssh サービスの状態が"offline"となっている場合]

```
# svcs ssh
STATE          STIME      FMRI
offline        10:05:22  svc:/network/ssh:default
```

<C.1.2・C.1.3・C.1.4 共通>

■原因

該当サービスに何らかの異常がある可能性があります。

■対処方法

該当サービスに関連する設定などに問題がないかを確認します。

問題が見つかった場合は、被疑箇所を正しく修正してください。

問題が見つからなかった場合は、OS 再起動後にサービスが意図する状態に遷移したかを確認し、意図どおりの状態でなければ、意図する状態に遷移させてください。

[例:OS 再起動後に gdm サービスが意図する"online"状態に遷移した場合]

```
# shutdown -i6 -g0 -y
:
<OS 再起動中>
:
# svcs gdm
STATE          STIME      FMRI
online         15:09:08  svc:/application/graphical-login/gdm:default
```

[例:OS 再起動後に gdm サービスが意図する"online"状態に遷移しなかった場合]

```
# shutdown -i6 -g0 -y
:
<OS 再起動中>
:
# svcs gdm
STATE          STIME      FMRI
disabled       14:58:41  svc:/application/graphical-login/gdm:default
# svcadm enable gdm
# svcs gdm
STATE          STIME      FMRI
online         15:11:38  svc:/application/graphical-login/gdm:default
```

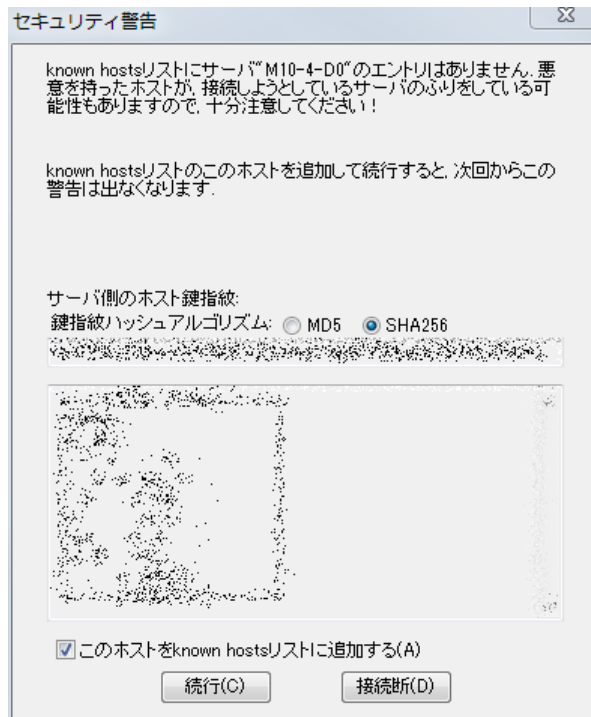
OS 再起動後のオペレーションでも意図する状態に遷移しない場合は、当社技術員に連絡してください。

C.2 クライアントで検出したトラブル

C.2.1 Tera Term による SSH 接続時に、セキュリティ警告が表示される(1)

■現象

Tera Term による SSH 接続で、以下のセキュリティ警告が表示されます。



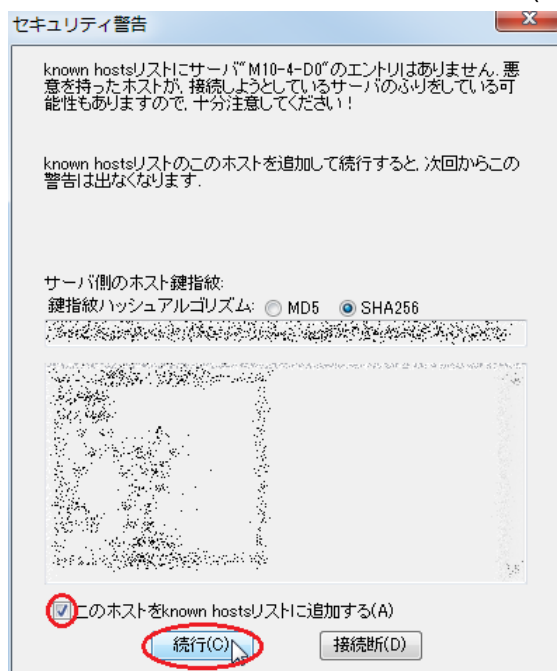
■原因

サーバへの初回接続時など、サーバの公開鍵が未登録であることが原因です。

■対処方法

[セキュリティ警告]ダイアログで"このホストを known hosts リストに追加する(A)"をチェック後に[続行]をクリックし、SSH 接続を行ってください。

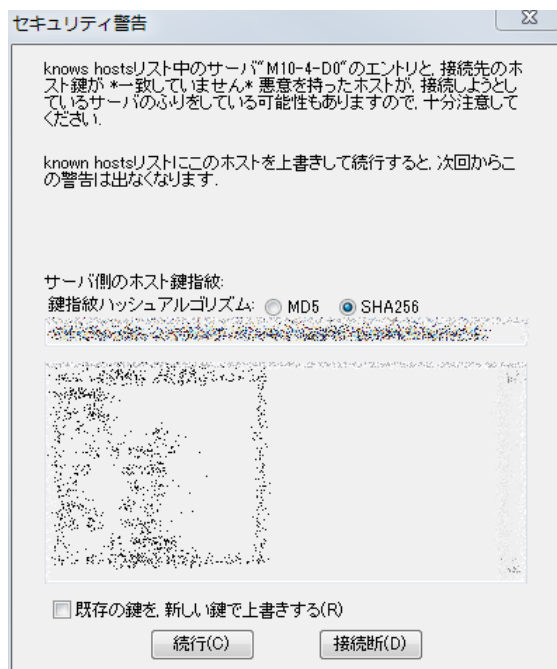
"このホストを known hosts リストに追加する(A)"をチェックすることで、公開鍵が登録されます。



C.2.2 Tera Term による SSH 接続時に、セキュリティ警告が表示される(2)

■現象

Tera Term による SSH 接続で、以下のセキュリティ警告が表示されます。



■原因

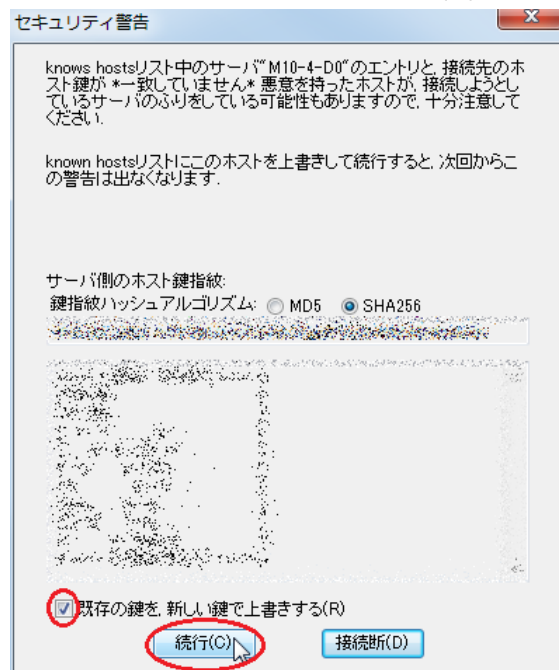
サーバの公開鍵が変更された可能性があります。

■対処方法

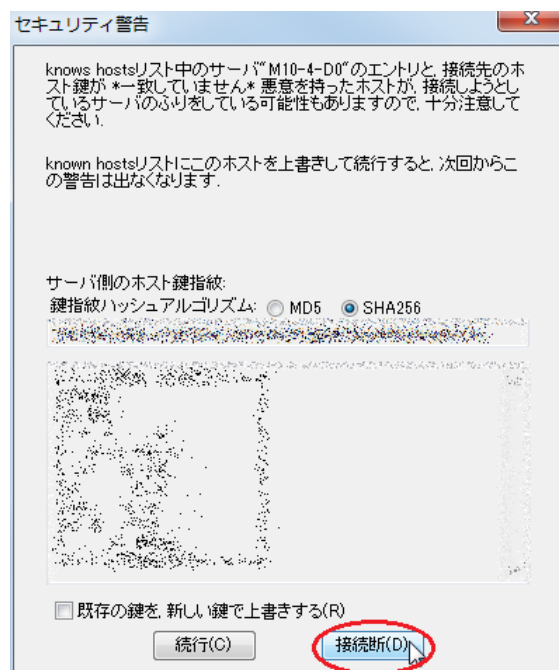
なりすましの可能性があるため、サーバ管理者に公開鍵の変更履歴を確認します。

確認の結果、公開鍵が変更されていた場合は、[セキュリティ警告]ダイアログの"既存の鍵を、新しい鍵で上書きする(R)"をチェック後に[続行]をクリックし、SSH 接続を行ってください。

"既存の鍵を、新しい鍵で上書きする(R)"をチェックすることで、公開鍵が上書きされます。



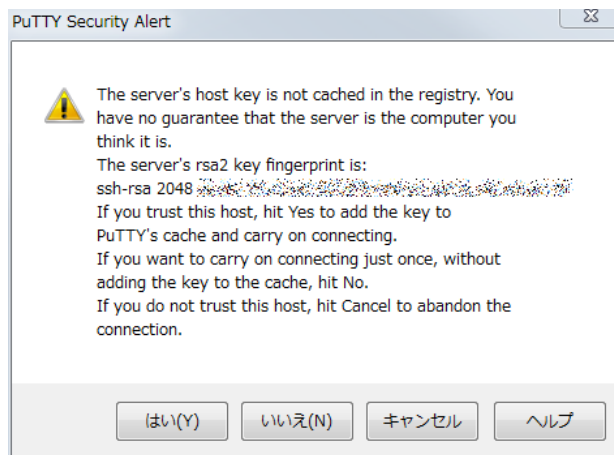
公開鍵が変更されていない場合は、[セキュリティ警告]ダイアログで[接続断]をクリックし、SSH 接続を中断してください。



C.2.3 PuTTY による SSH 接続時に、"Security Alert"が表示される(1)

■現象

PuTTY による SSH 接続で、以下の"Security Alert"が表示されます。



■原因

サーバへの初回接続時など、サーバの公開鍵が未登録であることが原因です。

■対処方法

[PuTTY Security Alert]ダイアログで[はい]をクリックし、SSH 接続を行ってください。

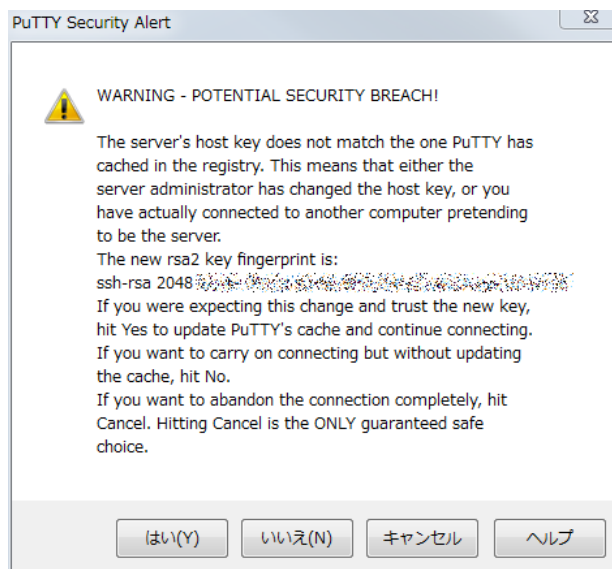
[はい]をクリックすることで、公開鍵が登録されます。



C.2.4 PuTTY による SSH 接続時に、"Security Alert"が表示される(2)

■現象

PuTTY による SSH 接続で、以下の"Security Alert"が表示されます。



■原因

サーバの公開鍵が変更された可能性があります。

■対処方法

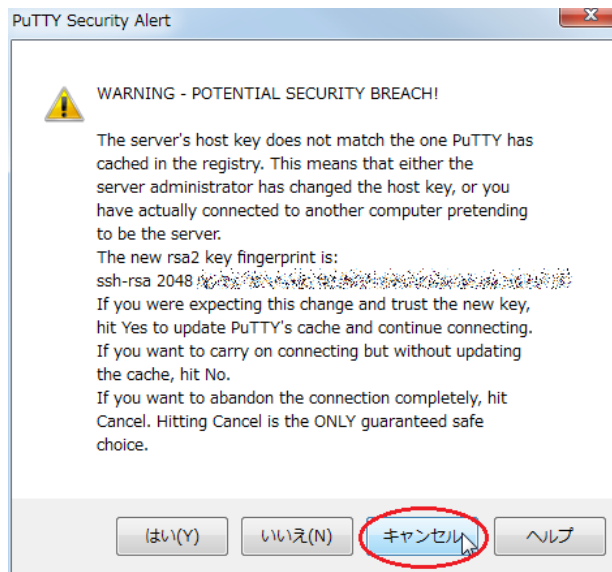
なりすましの可能性があるため、サーバ管理者に公開鍵の変更履歴を確認します。

確認の結果、公開鍵が変更されていた場合は、[PuTTY Security Alert]ダイアログで[はい]をクリックし、SSH 接続を行ってください。

[はい]をクリックすることで、公開鍵が上書きされます。



公開鍵が変更されていなかった場合は、[PuTTY Security Alert]ダイアログで[キャンセル]をクリックし、SSH 接続を中断してください。



《注意》

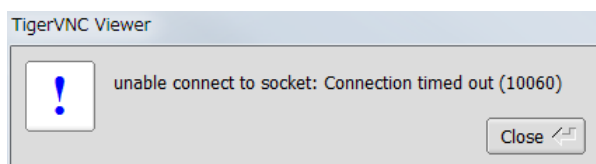
[いいえ(N)]をクリックすると、公開鍵を無視して SSH 接続するため、注意してください。

C.2.5 TigerVNC 使用時に、"Connection timed out"が表示される

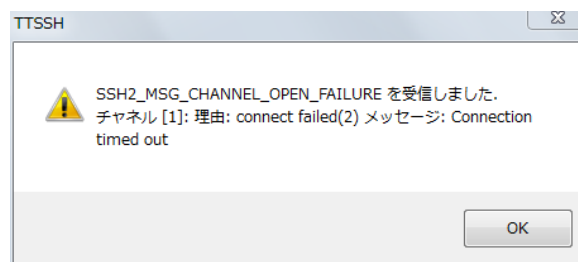
■現象

TigerVNC でリモートデスクトップ使用時に、以下のいずれかの"Connection timed out"メッセージが表示されます。

[メッセージ 1]



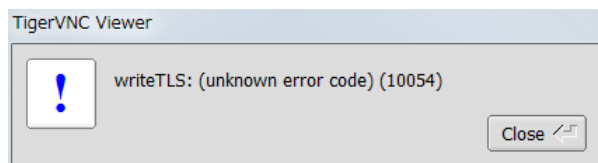
[メッセージ 2]



C.2.6 TigerVNC 使用時に、"writeTLS:(unknown error code)(10054)"が表示される

■現象

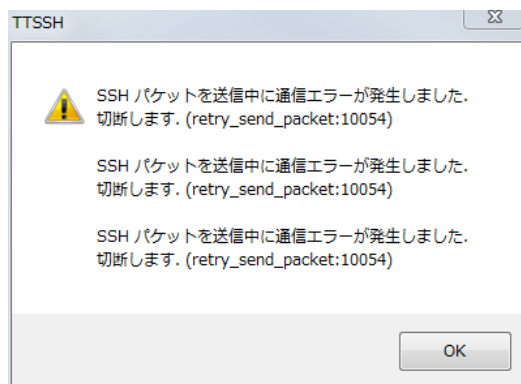
TigerVNC でリモートデスクトップ使用時に、"writeTLS:(unknown error code)(10054)"のメッセージが表示されます。



C.2.7 TigerVNC 使用時に、"(retry_send_packet:10054)"が表示される

■現象

TigerVNC でリモートデスクトップ使用時に、"(retry_send_packet:10054)"のメッセージが表示されます。



<C.2.5・C.2.6・C.2.7 共通>

■原因

以下のいずれかの可能性があります。

- a) 接続先サーバが停止状態である。
- b) サーバとクライアント間のネットワーク接続に問題がある。

■a)の復旧方法

接続先サーバを起動後に、TigerVNC でリモートデスクトップに再接続してください。

■b)の復旧方法

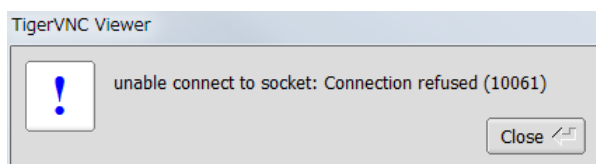
ネットワーク機器の接続を確認し、ネットワークを正常な接続状態にしたうえで、TigerVNC でリモートデスクトップに再接続してください。

C.2.8 TigerVNC 使用時に、"Connection refused"が表示される

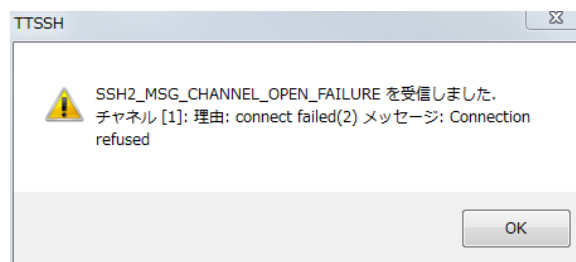
■現象

TigerVNC でリモートデスクトップ使用時に、以下のいずれかの"Connection refused"メッセージが表示されます。

[メッセージ 1]



[メッセージ 2]



■原因

以下のいずれかの可能性があります。

- サーバまたはクライアントで指定したポート番号に誤りがある。
- SSH ポートフォワーディング使用時に必要な SSH 接続が行われていない。
- /etc/services ファイルに"vnc-server"が正しく登録されていない。

■a)の対処方法

下表の手順に従ってポート番号を確認し、正しいポート番号を設定したうえで、TigerVNC でリモートデスクトップに再接続してください。

確認先		手順参照先	
		Solaris 11	Solaris 10
サーバ	/etc/services	3.2.1 Solaris 11 gdm サービスの場合 7)	3.2.2 Solaris 10 cde-login サービスの場合 8)
クライアント	SSH ポートフォワーディングを使用していない場合		
	TigerVNC	3.3.3 リモートデスクトップ接続 4) i) VNC ポート番号	
	SSH ポートフォワーディングを使用している場合		
	TigerVNC	3.3.3 リモートデスクトップ接続 4) ii) クライアントポート番号	
	Tera Term	3.3.1 Tera Term の SSH ポートフォワーディングを使用する場合 2) VNC ポート番号 、 クライアントポート番号	
	PuTTY	3.3.2 PuTTY の SSH ポートフォワーディングを使用する場合 2) i) VNC ポート番号 、 クライアントポート番号	

上記手順でも接続できない場合は、クライアントの OS を再起動してから、再度 TigerVNC でリモートデスクトップに接続してください。

■b)の対処方法

「[3.3.1 Tera Term の SSH ポートフォワーディングを使用する場合](#)」または「[3.3.2 PuTTY の SSH ポートフォワーディングを使用する場合](#)」の手順を参照し、SSH ポートフォワーディング接続後に TigerVNC でリモートデスクトップに再接続してください。

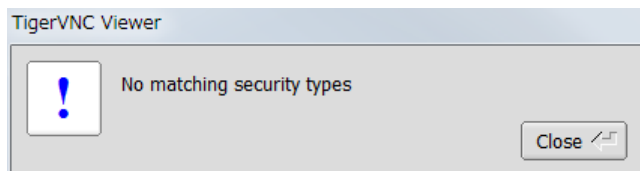
■c)の対処方法

「C.1.1 xvnc-inetd サービス起動時に、サービスの状態が"maintenance"に遷移する」の[対処方法](#)を実施したうえで、TigerVNC でリモートデスクトップに再接続してください。

C.2.9 TigerVNC 接続時に、"No matching security types"が表示される

■現象

TigerVNC でリモートデスクトップ接続時に、"No matching security types"のメッセージが表示されます。



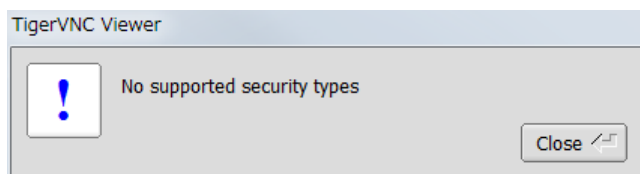
■原因

TigerVNC の暗号化に関する設定がサーバとクライアントで異なります。

C.2.10 TigerVNC 接続時に、"No supported security types"が表示される

■現象

TigerVNC でリモートデスクトップ接続時に、"No supported security types"のメッセージが表示されます。



■原因

TigerVNC の暗号化に関する設定で、未サポートの"SecurityTypes"を指定しています。

<C.2.9・C.2.10 共通>

■対処方法

- Solaris 11.3 SRU18041 以降の場合

サーバは「[3.2.1 Solaris 11 gdm サービスの場合 5\)](#)」の手順を、クライアントは「[3.3.3 リモートデスクトップ接続 2\)](#)」の手順を参照し、双方の暗号化に関する設定を同一にしたうえで、TigerVNC でリモートデスクトップに再接続してください。

- Solaris 11.1～Solaris 11.3 SRU18032 または Solaris 10 1/13 の場合

サーバは「[3.2.1 Solaris 11 gdm サービスの場合 5\) ii\)](#)」または「[3.2.2 Solaris 10 cde-login サービスの場合 7\)](#)」の手順を、クライアントは「[3.3.3 リモートデスクトップ接続 2\) ii\)](#)」の手順を参照し、サーバの"SecurityTypes"とクライアントの"Encryption"を"None"に設定後、TigerVNC でリモートデスクトップに再接続してください。

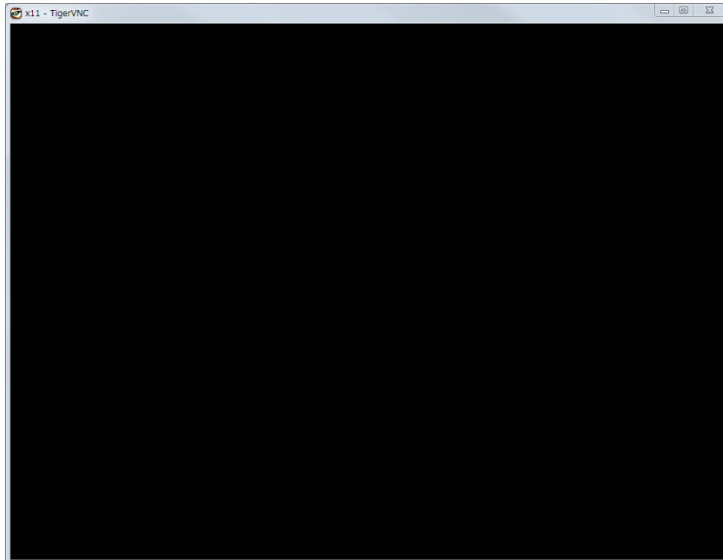
《注意》

両 OS 版数とも、サーバとクライアントを"None"に設定すると TigerVNC の TLS 暗号化が無効になるため、セキュリティ対策が必要な場合は、「[3.3.1 Tera Term の SSH ポートフォワーディングを使用する場合](#)」または「[3.3.2 PuTTY の SSH ポートフォワーディングを使用する場合](#)」の手順を参照し、SSH ポートフォワーディングによる暗号化を行ってください。

C.2.11 TigerVNC 接続時に、ログイン画面が表示されない

■現象

TigerVNC でリモートデスクトップ接続時に、以下のようにログイン画面が表示されません。



■原因

以下のいずれかの可能性があります。

- a) 以下のいずれかのサービス状態が"online"でない。
 - xvnc-inetd サービス
 - gdm サービス
 - cde-login/gdm2-login サービス
- b) ディスプレイマネージャーの XDMCP 接続が有効でない。

■a)の対処方法

下表の手順を参照し、サーバの該当サービスを起動したうえで、TigerVNC でリモートデスクトップに再接続してください。

サービス名	手順参照先	
	Solaris 11	Solaris 10
xvnc-inetd	3.2.1 Solaris 11 gdm サービスの場合 8)~9)	3.2.2 Solaris 10 cde-login サービスの場合 9)~10)
gdm	3.2.1 Solaris 11 gdm サービスの場合 3)~4)	—
cde-login	—	3.2.2 Solaris 10 cde-login サービスの場合 3)
gdm2-login	—	3.2.3 Solaris 10 gdm2-login サービスの場合 4)~5)

■b)の対処方法

下表の手順を参照し、サーバのディスプレイマネージャーの XDMCP 接続を有効にしたうえで、TigerVNC でリモートデスクトップに再接続してください。

OS	手順参照先
Solaris 11	3.2.1 Solaris 11 gdm サービスの場合 2)~4)
Solaris 10 ※ gdm2-login サービス使用時のみ	3.2.3 Solaris 10 gdm2-login サービスの場合 2)~5)

C.2.12 gdm2-login サービス使用時に、TigerVNC が接続途中で終了する

■現象

Solaris 10 の gdm2-login サービス使用時に、TigerVNC がリモートデスクトップへの接続途中で終了します。

■原因

以下のいずれかの可能性があります。

- a) 同時接続クライアント数の上限値を超えて TigerVNC でリモートデスクトップに接続している。
- b) /etc/services ファイルに"vnc-server"が正しく登録されていない。

■a)の対処方法

現在接続中の TigerVNC をすべて終了させ、サーバの同時接続クライアント数の上限値を、実際に接続するクライアント数以上に変更したうえで、TigerVNC でリモートデスクトップに再接続してください。

この上限値の変更は、下記実施例のように、/etc/X11/gdm/gdm.conf ファイルの[xdmcp]の下を編集したあと、gdm2-login サービスの再起動とサービス状態の"online"への遷移確認により行います。

[実施例: 同時接続クライアント数の上限値(デフォルト:2)を 5 に変更する場合]

```
# vi /etc/X11/gdm/gdm.conf
:
[xdmcp]
:
#DisplaysPerHost=2
DisplaysPerHost=5
:
#
# svcadm restart gdm2-login
# svcs gdm2-login
STATE      STIME      FMRI
online     16:40:01  svc:/application/gdm2-login:default
```

確認した状態が"online*"の場合は、状態遷移中のため、しばらくしてから状態を再確認します。

- ▶ サービスの状態が"online"に遷移しない場合は、[「C.1.2 サービス起動時に、サービスの状態が"online"に遷移しない」](#)を参照してください。

■b)の対処方法

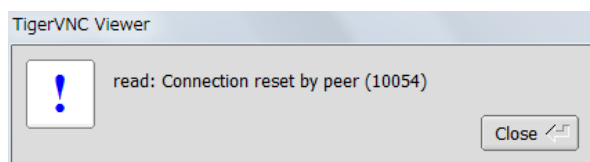
「C.1.1 xvnc-inetd サービス起動時に、サービスの状態が"maintenance"に遷移する」の[対処方法](#)を実施したうえで、TigerVNC でリモートデスクトップに再接続してください。

C.2.13 TigerVNC 使用時に、"Connection reset by peer (10054)"が表示される

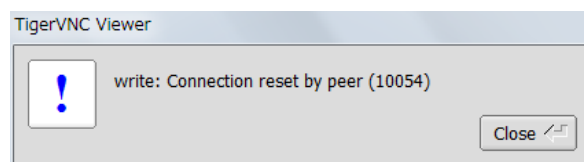
■現象

TigerVNC 使用時に、以下のいずれかの"Connection reset by peer (10054)"のメッセージが表示されます。

[メッセージ 1]



[メッセージ 2]



■原因

以下のいずれかの可能性があります。

- a) サーバとクライアント間のネットワーク接続に問題がある。
- b) TigerVNC を終了する前に、SSH ポートフォワーディングのターミナルエミュレータを閉じた(Xボタンのクリックなど)。

■a)の復旧方法

ネットワーク機器の接続を確認し、ネットワークを正常な接続状態にしたうえで、TigerVNC でリモートデスクトップに再接続してください。

■b)の回避方法

TigerVNC 終了後に、SSH ポートフォワーディングのターミナルエミュレータを終了してください。

■b)の復旧方法

現象発生後に TigerVNC を使用する場合は、「[3.3.1 Tera Term の SSH ポートフォワーディングを使用する場合](#)」または「[3.3.2 PuTTY の SSH ポートフォワーディングを使用する場合](#)」の手順を参照し、SSH ポートフォワーディング接続後に TigerVNC でリモートデスクトップに再接続してください。

C.2.14 TigerVNC で接続した GNOME 内の入力動作が遅れる

■現象

TigerVNC でリモートデスクトップに接続した GNOME 内のキーボードやマウスの入力動作が遅れます。

■原因

TigerVNC の TLS 暗号化をサポートしていないサーバの OS 版数で、TLS 暗号化を使用している可能性があります。

■対処方法

TigerVNC の TLS 暗号化を使用する場合は、サーバの OS 版数を Solaris 11.3 SRU18041 以降にアップデートしてください。

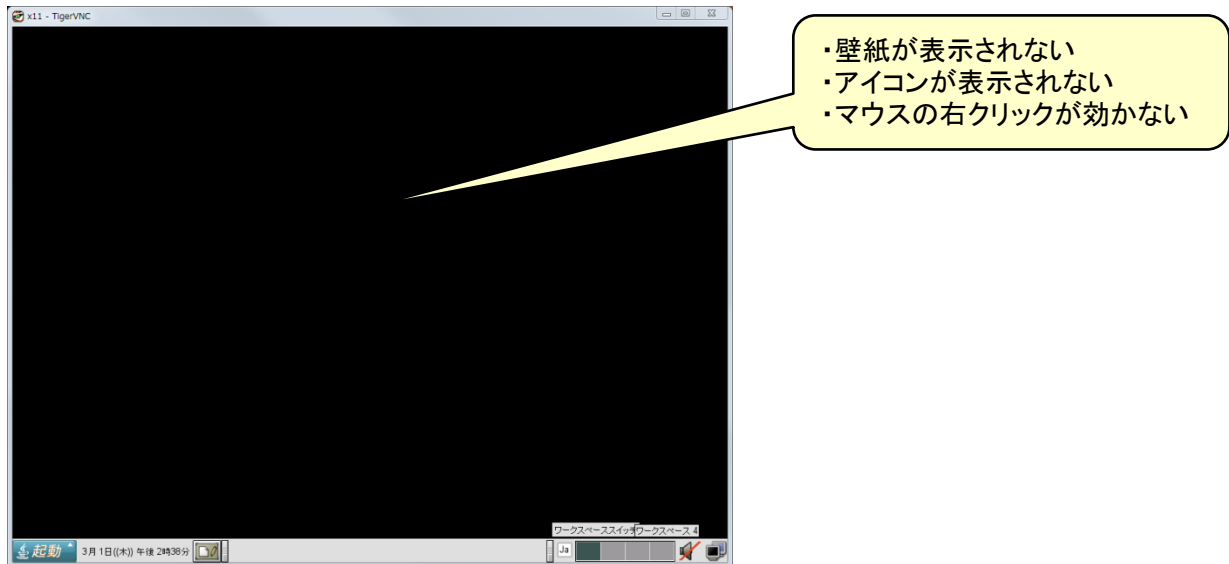
Solaris 11.3 SRU18041 以降にアップデートできない場合は、「[3.2.1 Solaris 11 gdm サービスの場合 5\) ii\)](#)」と「[3.3.3 リモートデスクトップ接続 2\) ii\)](#)」の手順を参照し、サーバの"SecurityTypes"とクライアントの"Encryption"を"None"に設定後、TigerVNC でリモートデスクトップに再接続してください。

双方を"None"に設定すると TigerVNC の TLS 暗号化が無効になるため、「[3.3.1 Tera Term の SSH ポートフォワーディングを使用する場合](#)」または「[3.3.2 PuTTY の SSH ポートフォワーディングを使用する場合](#)」の手順を参照し、SSH ポートフォワーディングによる暗号化を行ってください。

C.2.15 cde-login サービスで JDS を使用時に、リモートデスクトップ画面が正しく表示されない

■現象

Solaris 10 の cde-login サービスで JDS にログインしたとき、TigerVNC のリモートデスクトップ画面が以下のように正しく表示されません。



■原因

cde-login サービスで JDS を使用する複数の利用者が、ほぼ同時刻にログインした可能性があります。

■回避方法

JDS を複数の利用者で使用する場合は、「[3.2.3 Solaris 10 gdm2-login サービスの場合](#)」の手順を参照し、cde-login サービスの代わりに gdm2-login サービスを使用してください。

■対処方法

リモートデスクトップに接続中の TigerVNC をすべて終了させたあと、cde-login サービスを再起動し、サービスの状態が"online"に遷移したことを確認してから、TigerVNC でリモートデスクトップに再接続してください。

```
<クライアント>
TigerVNC をすべて終了

<サーバ>
# svcadm restart cde-login
# svcs cde-login
STATE      STIME      FMRI
online     15:40:29   svc:/application/graphical-login/cde-login:default
```

確認した状態が"online*"の場合は、状態遷移中のため、しばらくしてから状態を再確認します。

- ▶ サービスの状態が"online"に遷移しない場合は、「[C.1.2 サービス起動時に、サービスの状態が"online"に遷移しない](#)」を参照してください。

改版履歴

改版日時	版数	改版内容
2019.02.21	1.0	新規作成
2019.07.04	1.1	3.1.1 (c)および 3.2.3 (2)の手順を修正
2019.08.01	1.2	全体的に体裁修正

