FUSION Forensics
– ゲートウェイ型操作ログ監査証跡サービス –

July/2013

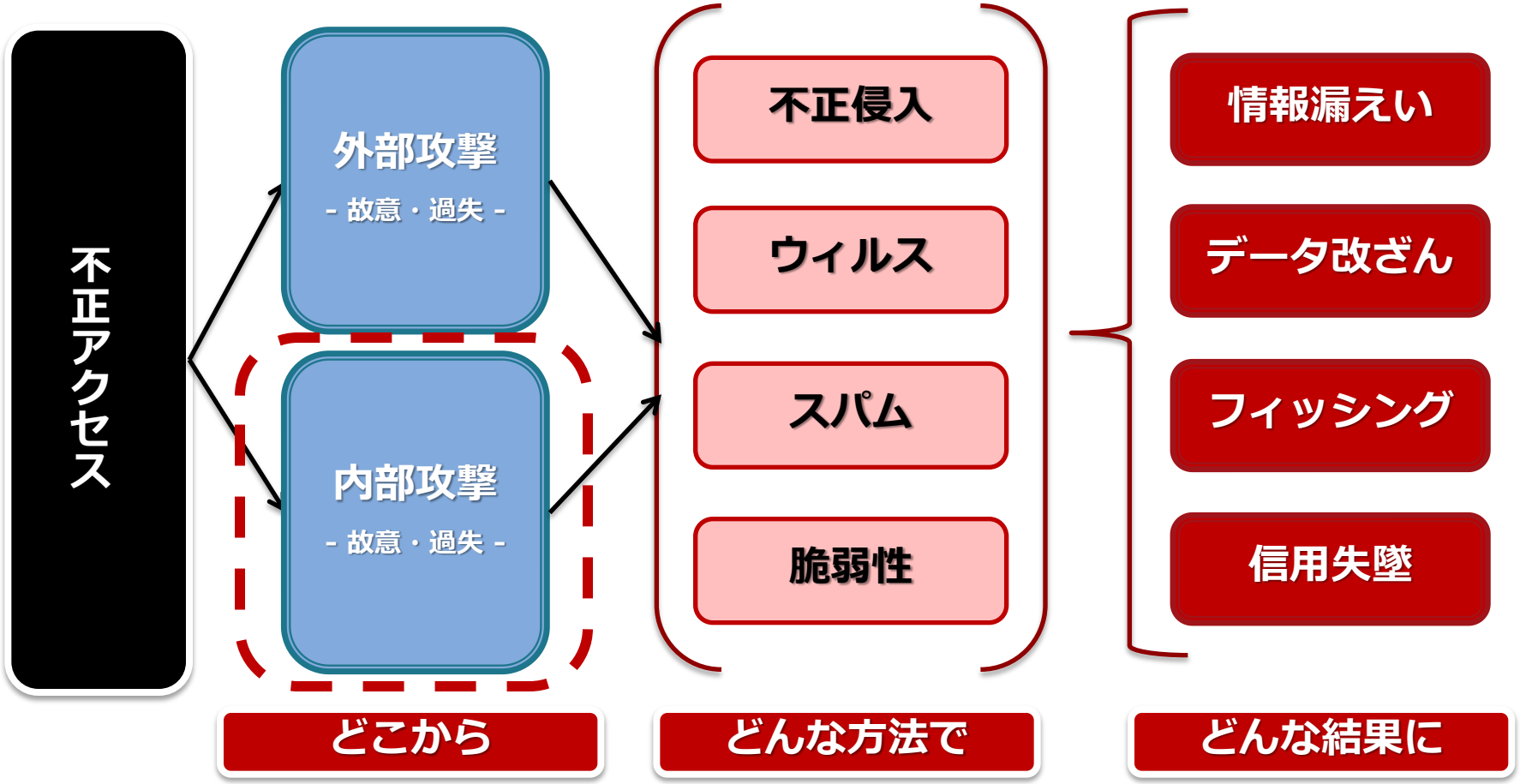
Business Promotion Dept., Fusion Communications Corp.
http://www.fusioncom.co.jp/

FUSION COMMUNICATIONS 楽天

システム運用で顕在化しているセキュリティリスク

■ セキュリティリスク例：不正アクセスの場合

システムを利用している様々な状況で、不正アクセスのきっかけが存在している。
提供している側は、常にそのリスクを背負って、運営していかなければならない。



FUSION COMMUNICATIONS 楽天

Strictly Confidential

年々増加する不正アクセス、セキュリティ事故

■ 内部犯行における不正アクセス、セキュリティ事故

【主な事例2ケース】

企業名	事故名	時期	不正ｱｸｾｽ者	内容
某通信ﾓﾊﾞｲﾙ会社	関西地域（大阪府、兵庫県、京都府、滋賀県、奈良県）における通信障害を引き起こした内部犯行	2011年5月	業務委託先元社員	元社員は、業務に使用していた制御用端末に、3月8日～9日にかけて不正プログラムを入力、ATM伝送装置の回線設定データを改ざんし、基地局を停波させた。
某クラウド系事業者	大量データの消失 データ復旧の不備による情報漏洩	2012年6月	社員	大量データの消失は、ベテラン担当者が社内マニュアルに従わず独自の更新プログラムでメンテナンスを実施したことによりに発生。直接の原因は、脆弱性対策のために独自の更新プログラムを改訂したが不備がありバックアップ環境も含め、ほぼ全てのサーバのデータが消失した。

【本人を特定するのにコスト（人・時間・費用）が最もかかっているケース】

企業名	事故名	時期	不正ｱｸｾｽ者	内容
派遣先企業	PC遠隔操作による爆破予告、無差別殺人を予告する愉快的犯行	2012年9月	4人誤逮捕 2013/3/25現在、元派遣会社社員を起訴	派遣先のPCを経由して、他人のPCに遠隔操作用のウィルスを仕込み、仕込んだPCを経由して複数のHPへ不正に書き込み、業務を妨害したとして、ハイジャック防止法違反などで起訴されている。操作履歴が不明な状況から本人に至る確定的な証拠があがっていない。

システムの多様化、利用者の増加により、不正アクセスやセキュリティ事故が増加する一方、あらゆるコストも増加している。

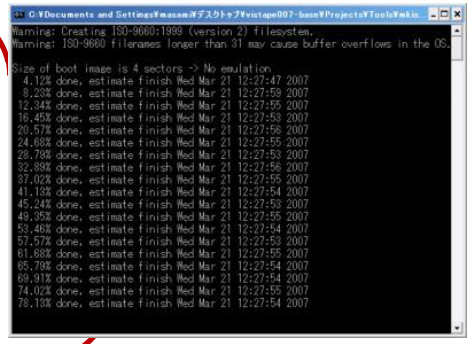
FUSION COMMUNICATIONS　楽天

もし、セキュリティ事故（インシデント）が発生したら？？

■ 原因を特定するためにまず実施すべきことは、ログの確認！

でも・・・、

- ログが正しくとれていただろうか。
- どのログを見ればよいのだろうか。
- ログがありすぎて、時間がかかりすぎる。
- 正しい分析はどうやってやるのだろうか。
- ログが欠落していた。戻せるのか。
- このログは、正しいのかわからない。



そもそもログを取得していなかったり、
ログ分析の方法が不明瞭だったりと、
正しい対処を迅速に行うことができない・・・

自社環境でこのような状況。
クラウド環境を利用していたら、どんなことになるのか・・・

FUSION COMMUNICATIONS　楽天

Strictly Confidential

クラウド環境におけるログ監査（ログ管理）

現状: 利用者の操作ログを取得・提供しているクラウド事業者はいない

- クラウド事業者（IaaS）における一般的なアクセス管理は、**ユーザ権限管理及び認証機能のみ**の提供としている。
- クラウドサービス利用者（開発者・運用者）の操作ログ（アクセスログ）を取得・管理・開示しているサービス事例は、見受けない。
- オンプレ型としてアクセス管理を有するソリューション・パッケージは多いが、**マルチテナント化しているソリューション・パッケージは無い**。

⇒ 単にオンプレ型のソリューション・パッケージをクラウドサービスに適用するとなるとコストや契約条件面の折り合いがつかない。

FUSION COMMUNICATIONS 楽天

FUSION Forensics ～ FUSION Cloud内で運用する操作ログ監査証跡サービス～

FUSION Forensics：操作ログ監査証跡サービス

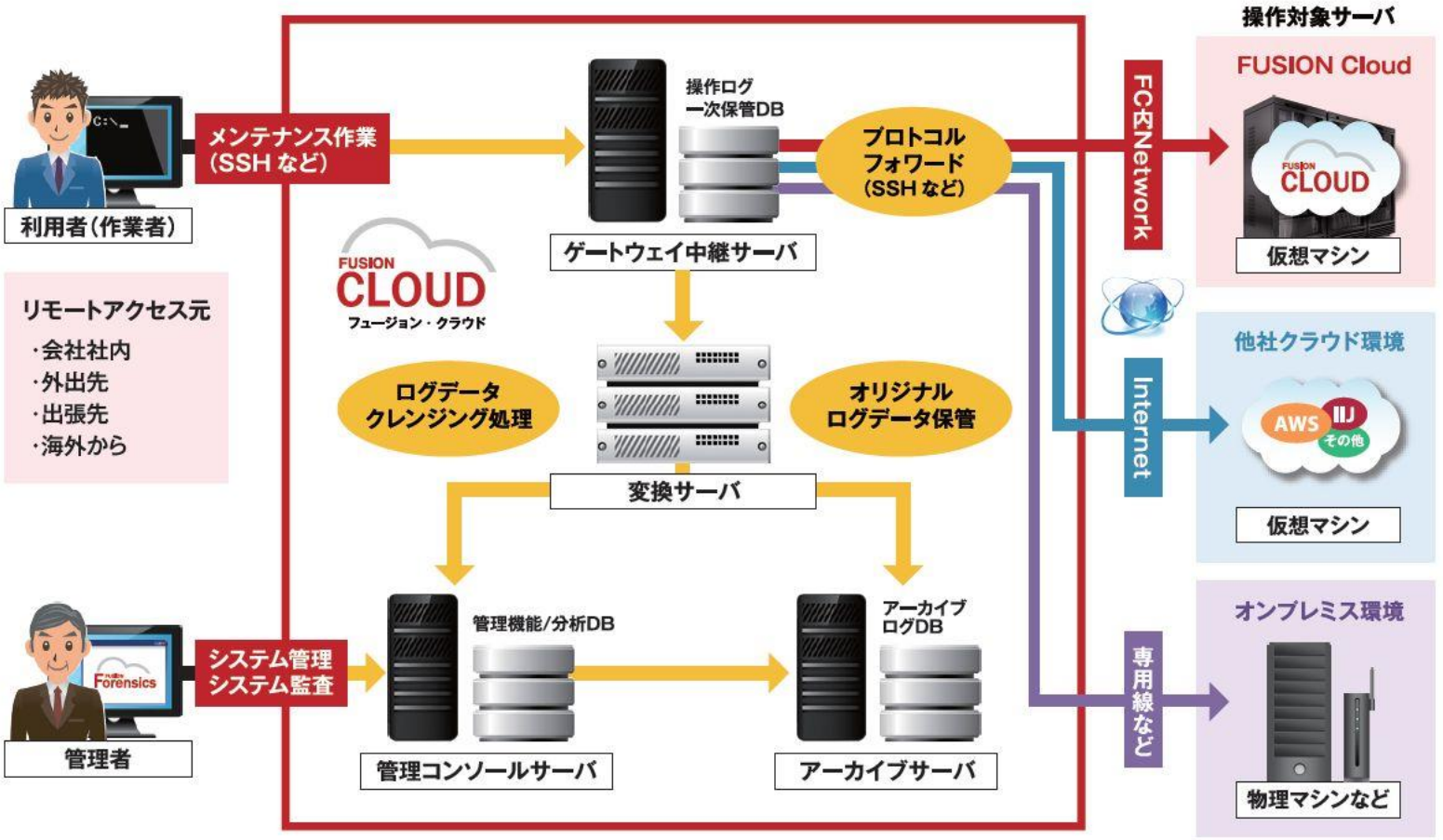
IaaS利用者に対する操作ログを取得・管理する機能を提供！！

- 利用者ごとに、**操作対象環境に対する操作ログ（アクセスログ）を取得**し、一元管理（**検索・一覧表示・操作ログダウンロード**）機能を提供。
- 取得可能な操作ログのプロトコルの第一弾は、 **SSH / TELNET / FTP / SFTP / SCP** であり、実行コマンド一覧のログも個別に提供が可能。
- 当サービス利用は、**他のクラウド事業者、或いは、オンプレミスの自社環境からの利用が可能**。
- **ログの保存期間は、1年以上**の保管が可能。**保管しているログの容量によって、課金**する形態（保管コストが高くなった場合は、個別対応にて、ログのローテーションの対応が可能）

FUSION COMMUNICATIONS　楽天

Strictly Confidential

FUSION Forensics：全体構成図



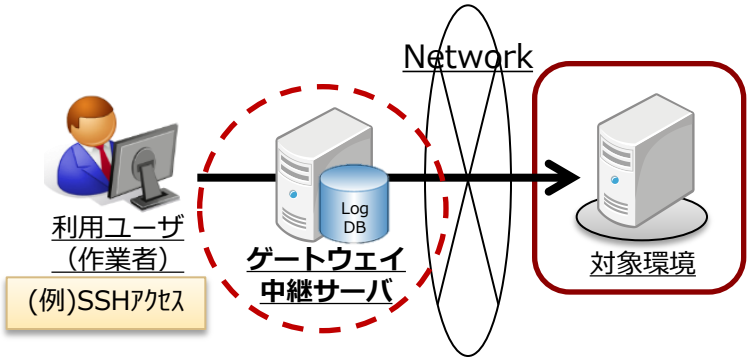
FUSION Forensics：操作ログ取得機能

■ 操作ログ取得機能

- 接続方式
  - ・2段階認証接続方式、メニュー型接続方式
- 対象プロトコル
  - ・**SSH / Telnet**
  - ・**FTP / SFTP**
  - ・**SCP**
- 対象ソフト
  - ・Tera Term / PuTTY / WinSCP

※各対象プロトコルを用いて接続する場合は、上記ソフトの組み合わせ等でご利用頂きます。

※接続端末の利用制限は、上記ソフトウェアの仕様に依存します。



- 対象接続先仕様
  - ・FUSION CloudからInternet経由で接続可能な接続先まで提供可能
  - ・仮想サーバに限らず、物理サーバ、ネットワーク機器などにも利用可能
  - ・自社環境へ接続する場合は、個別環境（中継サーバ、VPN接続環境）をご用意

※個別環境を必要とする場合は、ご要件に応じて、当サービス料金以外の追加料金が発生いたします。

FUSION Forensics：操作ログ管理・監査機能

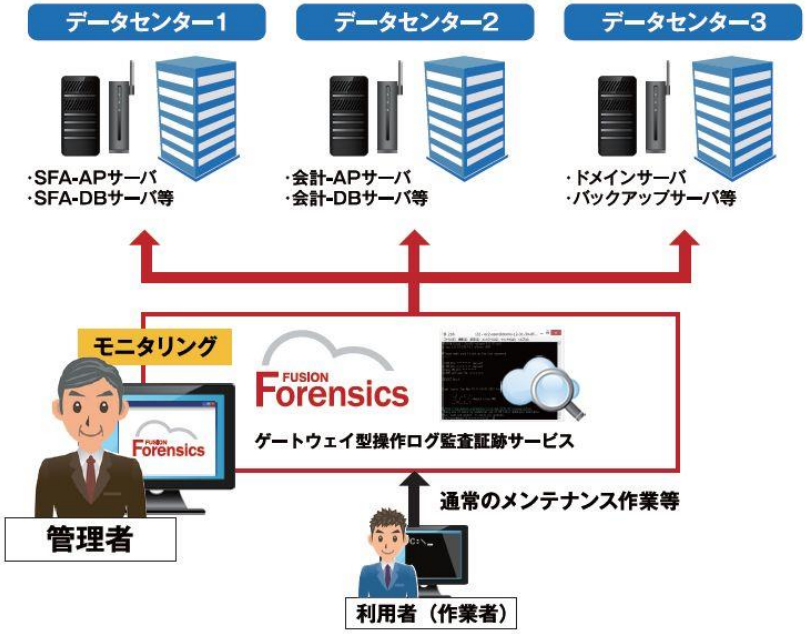
■ 操作ログ管理・監査機能

- 管理コンソール機能
  - ・Web管理画面にて、提供 ※対象ブラウザ：Internet Explorer / Firefox / Chrome
- 検索機能
  - ・指定検索（対象サーバ、接続元IP、操作期間、操作ユーザ、コマンドなど）
  - ・検索結果からのユーザ、プロトコル、接続先による絞り込み検索
- ログダウンロード
  - ・暗号キー付ログのダウンロード
- ユーザ管理機能
  - ・利用ユーザ / 管理ユーザの検索、一覧表示
  - ・ユーザ登録、パスワード変更
  - ・操作対象環境登録、更新、削除　※8月中旬提供予定機能
- その他
  - ・操作ログアーカイブ総容量表示機能　※8月中旬提供予定機能
  - ・マルチテナント対応
  - ・管理者操作ログ機能

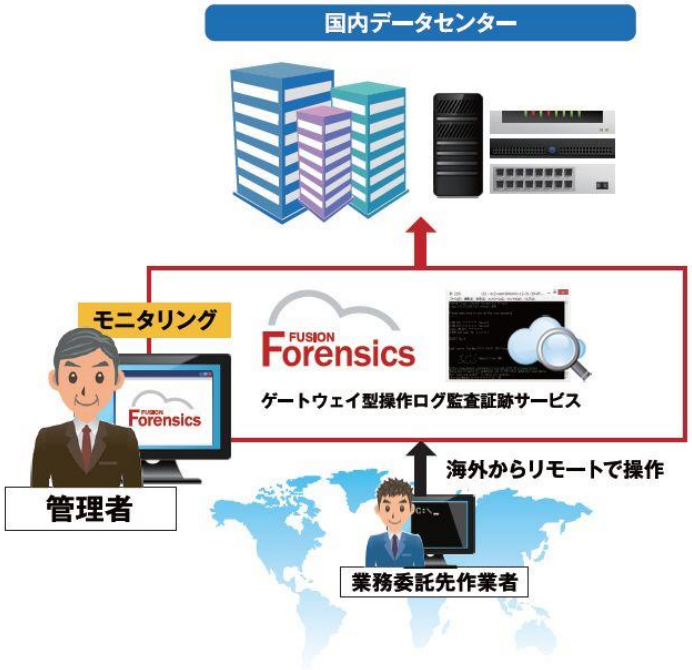
FUSION COMMUNICATIONS　楽天

FUSION Forensics：ご利用例

◆ 複数のロケーションにある機器(NW機器・サーバ)の全ての操作ログを取得・保管する



◆ 遠方にある業務委託先のリモート作業をモニタリングする



FUSION COMMUNICATIONS　楽天

Strictly Confidential

サービスロードマップ

■ ロードマップ

2013年5月リリース

IaaS利用者向けサービス提供開始！！

- 操作対象環境に対する作業の操作ログを取得
- 中継サーバを介して、仮想マシンにアクセス
- 取得ログは、以下を対象とする。
  - SSH、Telnet、FTP、SCP、SFTP
- 中継サーバへの基本アクセスは、証明書を利用
  - 2段階認証接続方式
  - メニュー型接続方式
- 管理コンソールのご提供
  - 操作ログ検索・ログ一覧表示機能
  - 利用者個別に操作ログのDLが可能
  - マルチテナント化対応
- サポートサービスのご提供
  - 問い合わせ（平日9:00～17:00）
  - 環境構築支援、SI支援サービス

2013年夏頃より順次リリース予定

追加機能サービス提供開始（予定）！！

- 追加取得ログは、以下を対象とする。
  - SSH証明書無し
  - HTTP、HTTPS
  - Windows ・・・ RDP
- 操作ログ管理機能強化（レポート）
- 管理コンソール機能強化（ダッシュボード、検索）
- 管理コンソール認証機能強化対応
- 個別環境提供、カスタマイズ対応

（2013年度中：提供予定サービス）

- オンプレ環境向けサービス提供
- VPC連携機能提供
- ファイル送受信機能提供
- アカウントAD連携機能提供
- アラート機能提供
- 管理ポータル機能提供

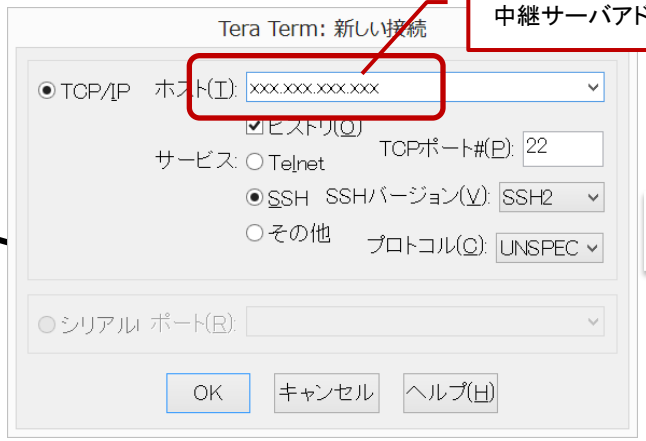
※案件対応の都合等により、提供内容が事前の予告なく変わる可能性がございます。予めご了承ください。

FUSION COMMUNICATIONS　楽天

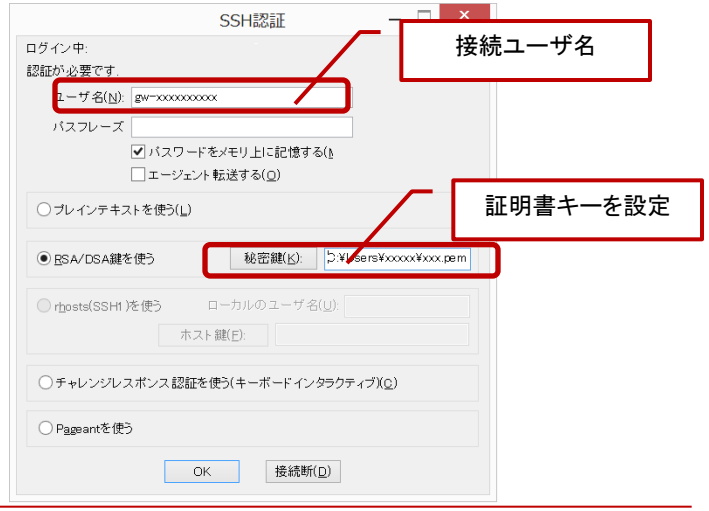
ご利用手順

■ ご利用手順（Tera Termを利用して、操作対象環境にSSH接続する場合）

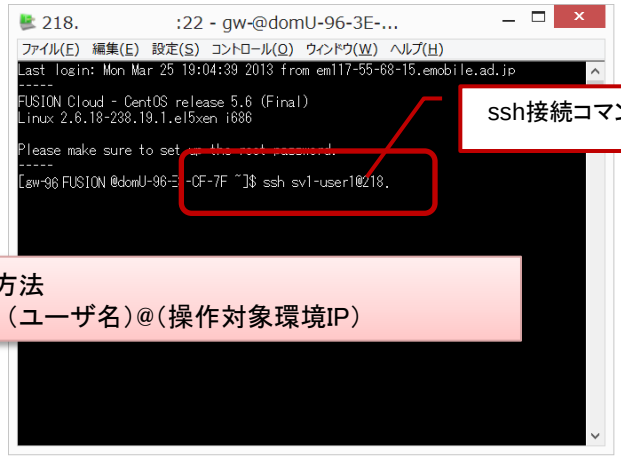
STEP.1 中継サーバに接続



STEP.2 ユーザ名と配布された認証キーを入力

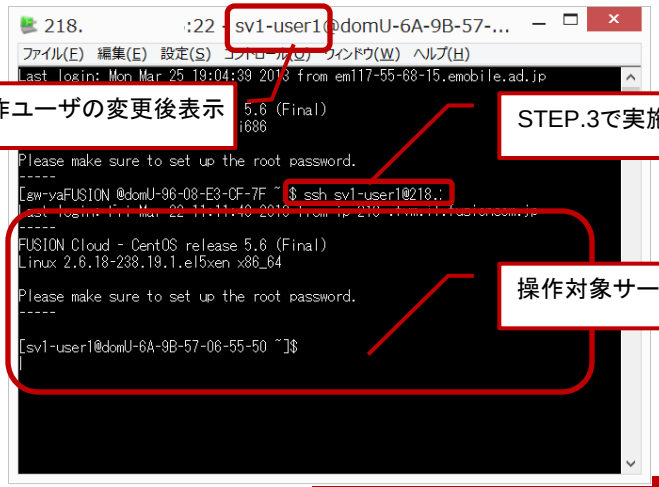


STEP.3 操作対象環境へ接続



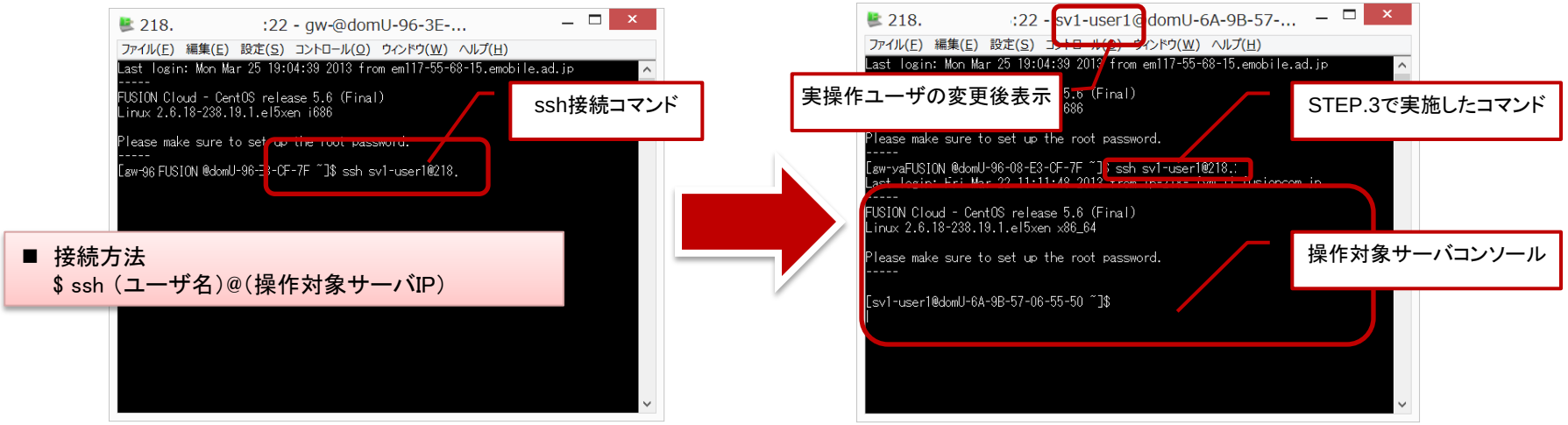
■ 接続方法
$ ssh（ユーザ名）@（操作対象環境IP）

STEP.4 操作対象環境ログイン ⇒ SSH通常利用

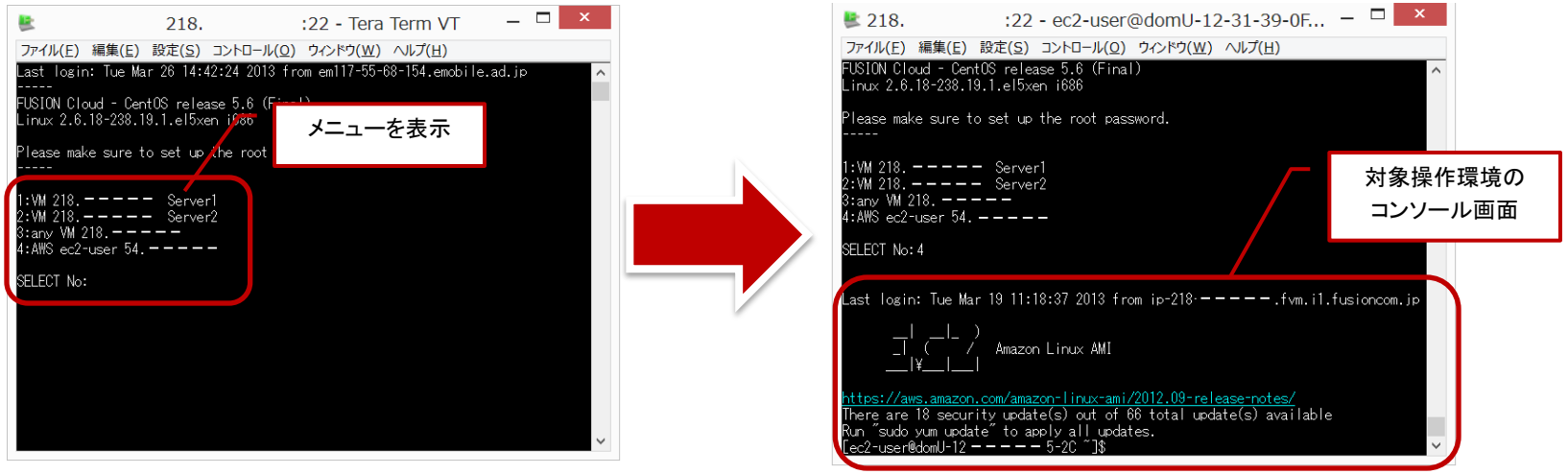


接続方式（2パターン）

■ 2段階認証接続方式

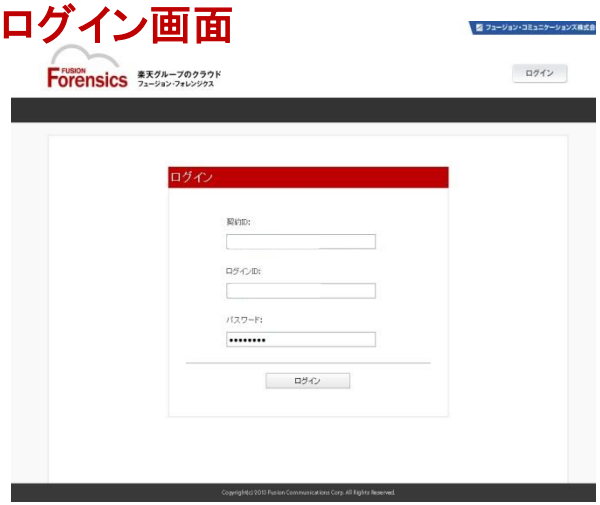


■ メニュー型接続方式



管理コンソール

ログイン画面



ユーザ管理画面

管理コンソールトップ画面

FUSION COMMUNICATIONS

楽天

Strictly Confidential

ご査収の程、何卒宜しくお願い申し上げます。

フュージョン・コミュニケーションズ
事業推進部
Tel：050-5528-8471
E-Mail：cloud_plan@fusioncom.co.jp