



Identify
Record
Report

ObserveIT – 概要紹介

February 2011



www.observeit-sys.com



OBSERVEIT 概要



市場チャレンジ



- 会計責任者不足
- 不十分な監査ログ

何が発生したのを十分に把握することが必要!



ObserveIT: ユーザーサーバー上の セキュリティカメラ!



WHAT:

身分識別

記録

報告

HOW:

共有されたユーザセッション
毎に、特定命名されたユーザ
が結び付けられる。

全てのセッションの映像が
キャプチャーされる。

全てのユーザセッションを監
査、レビュー、検索と再現

WHY:

会計責任:
PCI, HIPPA, SOX , ISO又は、ほ
かの監査要求に対して、管理
者にデータの変更を通知する
だけでなく、操作した人を特
定することが重要。

盲点の解決:
ログは全ての操作を記録でき
ない。映像はユーザの操作を
全て記録する。この価値は、
ログと比べることはできない。

高速と便利なアクセス:
レポートを自動的に作成。
ユーザ記録を高速に解析し、
疑問に対し迅速に解答。大量
の人力資源を軽減し、質、量
ともに保証。



何でビデオで記録しますか？

- 人々は自分の行為が記録されていることが分かっている場合、その行為は普段とちょっと違う
 - 子供部屋のカメラの前では、怒られないような行動をする
 - 道路で監視カメラが設置される場合、スピード出し過ぎで走ろうとしますか？
 - コールセンターの電話録音が生産率を改善する

ObserveITが無ければ、何を逃がしてしまうの？

■ ファイル内の改変を正確的に示す

- ファイルシステムの監査ではウェブコンフィグファイルが改変されたことのみを表示する
- 実行問題を発見する時、ObserveITの映像再生は、DBAに編集された“connection string”キーを表示する

■ システムがUI操作にドライブされて変わっている

- プロパティ画面の単一チェックボックスが複数のコンフィグファイルに改変をおこす。
- ObserveITで表示しているのはファイル改変のリバースエンジニアリングではなく、実際にその改変を引き起こす動作。

■ コピー/出力/画面キャプチャー

- コピーとペースなどの動作を含めて、ObserveITは画面上全ての操作をキャプチャーする。

ビジネス・ケース

■ リモートで操作者を監視

- 全ての操作者がサーバーで何をしているかということが詳しく把握できる
- セキュリティ、会計責任とポリシーの方針を改善する
- 透明な品質保証制度 (SLA) と請求書検証
- ユーザに責任が指摘されることがなくなる

■ 管理されるサービスを監視

- 使用対象: VAR、MSPとリモートIT支持チーム
- 取引先のサーバで従業員のパフォーマンスを監視する
- 信用を改善し、SLAの測定を定量化する
- 問題を発見する処理のスピードをアップする

■ 質量保証レポートを自動に作成

- PCI, HIPAA, SOXとISO標準に満足する
- 正確なユーザ身分承認
- 全てのサーバーアクセスとDBアクセスを追跡する
- アプリケーションだけではなく、操作人もレポート
- 変更できない証拠

■ 根本原因分析

- 誰が何をしているかを把握する⇒問題を根本的に解決できる
- 即時に根本原因を確定する
- ネットワーク監視ツール内部から警報する
- ヒューマンエラーを防ぐ

400以上の導入先

Manufacturing/Pharma



Financial



Telecommunications



IT Services



Gov't/Utilities/Healthcare/Education





重要な特色: なぜ、OBSERVEITを必要とされるの か

全てのものを記録する：完璧なプロトコルカバレッジ

- ネットワークプロトコルとクライアントアプリケーションに対する不明確性
- 全てリモートセッションまたコンソールセッションをキャプチャする



Terminal



Windows セッションの映像記録とメタデータ

監査セッション一覧表

Server	MASTER-DC2		...	Go		
Up to	January	2010	Print this information			
			Filter by user	-All-		
Results: 1 - 12 of 12			1			
Session Duration	Login	User	Server	Client	Slides	Video
2/1/2009						
5:34 PM - 8:38 PM	Administrator	noam	MASTER-DC2	(local)	1366	
5:13 PM - 5:13 PM	Administrator	noam	MASTER-DC2	(local)	2	
1/28/2009						
8:49 PM - 8:50 PM	Administrator	noam	MASTER-DC2	(local)	19	
8:01 PM - 8:35 PM	Administrator	noam	MASTER-DC2	(local)	118	
					Print this information	Print detailed information
ObserveIT - Login (4.0.3.0)						
Program Manager (2)						
Group Policy Management (3)						
New GPO						
Group Policy Object Editor (2)						

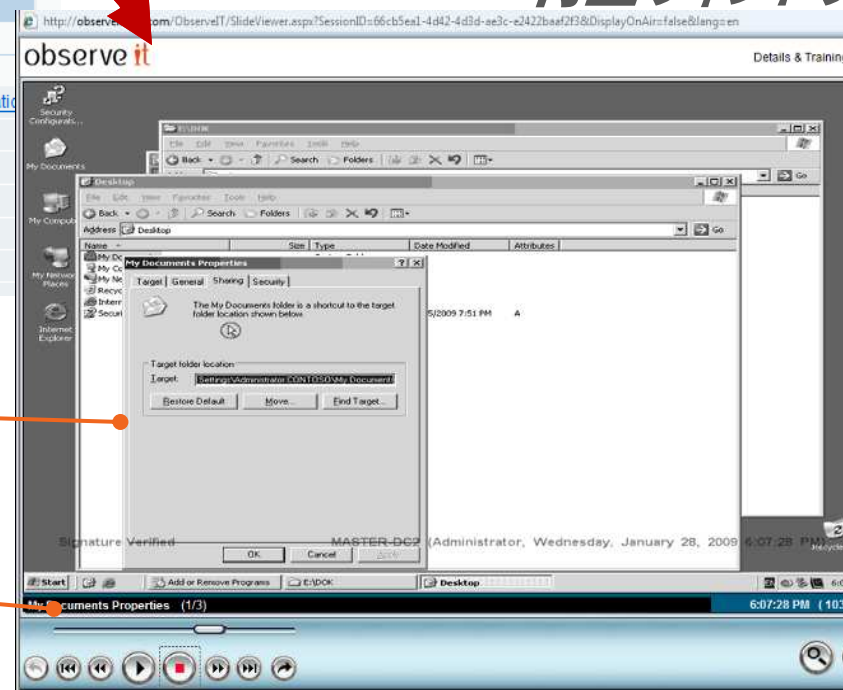
ObserveITにすべてのユーザセッションを載せる

セッション毎に全ての動作詳細を載せる

実際のビデオの再生

ビデオ映像中にどこでもすぐに移動できる

再生ウィンドウ



UNIX セッションの映像記録とメタデータ

監査セッション一覧表

Session Duration	Login	User	Server	Client	Slides	Video
3/21/2010						
11:57 AM - 11:57 AM	Administrator	n/a	solarisvm1	Client	120	
				Print this information	Print detailed information	
chmod						
11:23 /bin/chmod a+x /tmp/session						
Time	Process ID	Function	Params			
11:23 PM	6995	EXEC	chmod a+x /tmp/session			
11:23 PM	6995	OI MOD	/tmp/session			
rm						
11:35 /bin/rm -f /tmp/session						
Time	Process ID	Function	Params			
11:35 PM	6996	EXEC	rm -f /tmp/session			
11:35 PM	6996	UNLINK	/tmp/session			

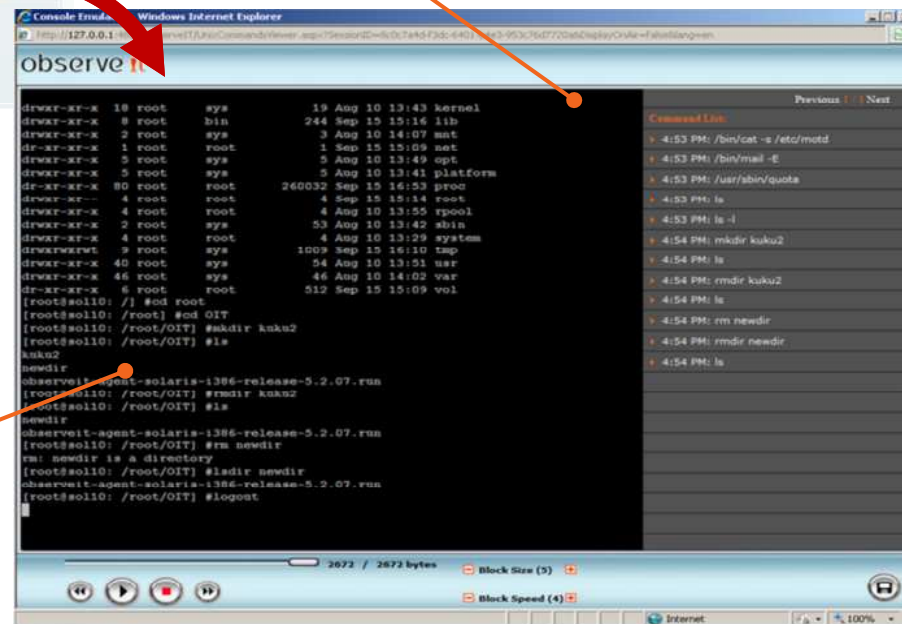
ビデオを再生する

ユーザコマンド
のリスト

再生ウィンドウ

一つコマンドにつき一つ
システムコールの明細リ
ストを載せる

実際に操作した画
面のビデオ再生

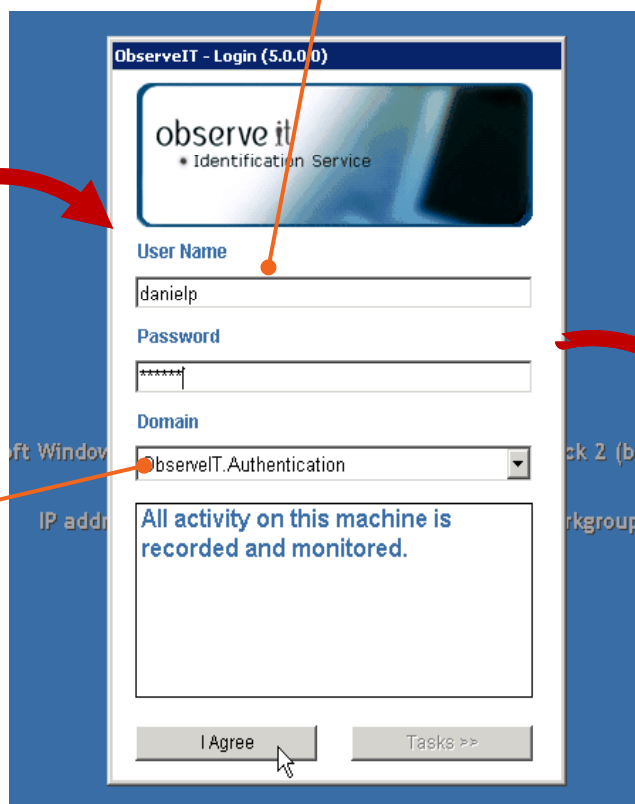


特権ユーザの身分認証

一般的な“administrator”で
ユーザ登録する



システムへのアクセス権限を認める
前に、ObserveITが命名したユーザア
カントの証明を要求する



認証のためのアクティブ
ディレクトリ

認証を取ってから、全てのセッ
ション監査記録にアクチュアル
ネームで標識する

Session Duration	Login	User	Server	Client	Slides	Video
			2/1/2009			
4:32 PM - 8:11 PM	Administrator	Daniel	MASTER-DC1	(local)	26	
			1/25/2009			
7:28 PM - 8:46 PM	Administrator	Daniel	MASTER-DC1	(local)	510	

検索とナビのためのインテリジェントなメタデータ

全ての動きの
文字概要

ユーザ、サーバー、日付、時刻、アプリ
ケーション名などで検索とフィルタ

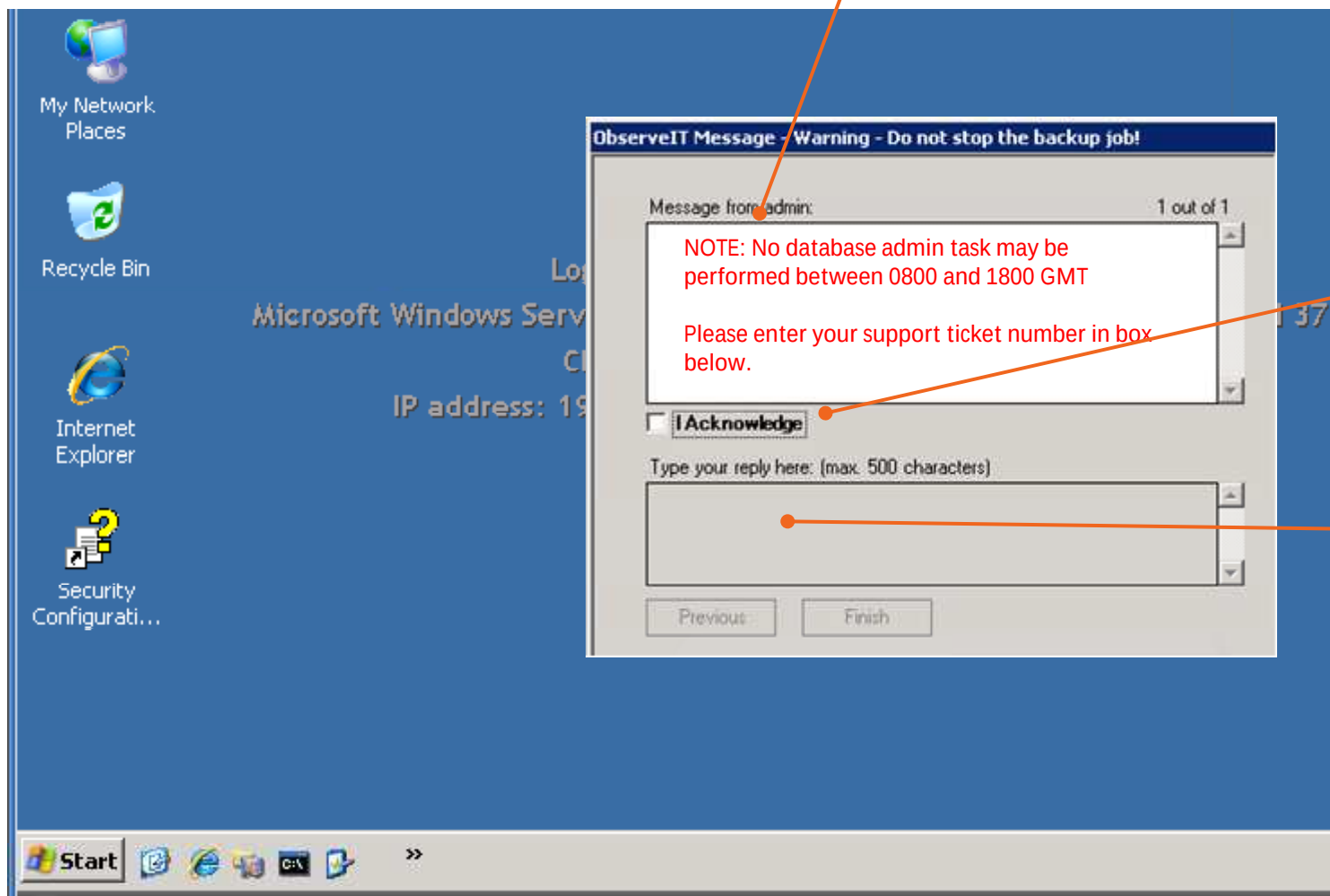
The screenshot displays the 'User Diary' section of the ObserveIT application. The left sidebar contains navigation links: 'Activities', 'Resources', 'Search', 'Latest Sessions', 'Quick Help', 'Installation', and 'Getting Started'. The main content area, titled 'Activity View', includes search filters for 'Login' (Daniel), 'Up to' (December 2009), and 'Server used' (MASTER-DC1 (1/28/2009)). Below these filters, a table shows search results for user 'Daniel'.

Session Duration	Login	User	Server	Client	Slides	Video
2/1/2009						
4:32 PM - 8:11 PM	Administrator	Daniel	MASTER-DC1	(local)	26	
1/25/2009						
7:28 PM - 8:46 PM	Administrator	Daniel	MASTER-DC1	(local)	510	
6:15 PM - 7:17 PM	Administrator	Daniel	MASTER-DC1	(local)	376	
Print this information Print detailed information						
\\192.168.2.254\ObserveITAgent (3)						
Program Manager (13)						
System Properties (3)						
Computer Name Changes (3)						
Local Area Connection Status (6)						
Active Directory Users and Computers (8)						
dnsmgmt - [DNS]						
dnsmgmt - [DNSMASTER-DC1] (2)						

見たい所でビデオ
を再生する

ユーザメッセージング

ユーザがサーバーに登録している時に、
各ユーザにポリシーと最新のステータス
を送る



会社標準が理解されること
と認められることを保証
する

問題追跡のために、
adminサポートチケット番
号を取り込む

リアルタイム再生

Server Diary | User Diary | Configuration | Search | Reports | Training | About

Activities

Activity View

Server: MASTER-DC2 [Go]

Up to: January 2010 [Print this information]

Filter by user: -All-

Results: 1 - 12 of 12

Session Duration	Login	User	Server	Client	Slides	Video
2/1/2009						
5:34 PM - 8:38 PM	Administrator	noam	MASTER-DC2	(local)	1366	[Video Icon]
5:13 PM - 5:13 PM	Administrator	noam	MASTER-DC2	(local)	2	[Video Icon]
1/28/2009						
8:49 PM - 8:50 PM	Administrator	noam	MASTER-DC2	(local)	19	[Video Icon]
8:01 PM - 8:35 PM	Administrator	noam	MASTER-DC2	(local)	118	[Video Icon]

[Print this information] [Print detailed information]

ObserveIT - Login (4.0.3.0)

Program Manager (2)

Group Policy Management (3)

New GPO

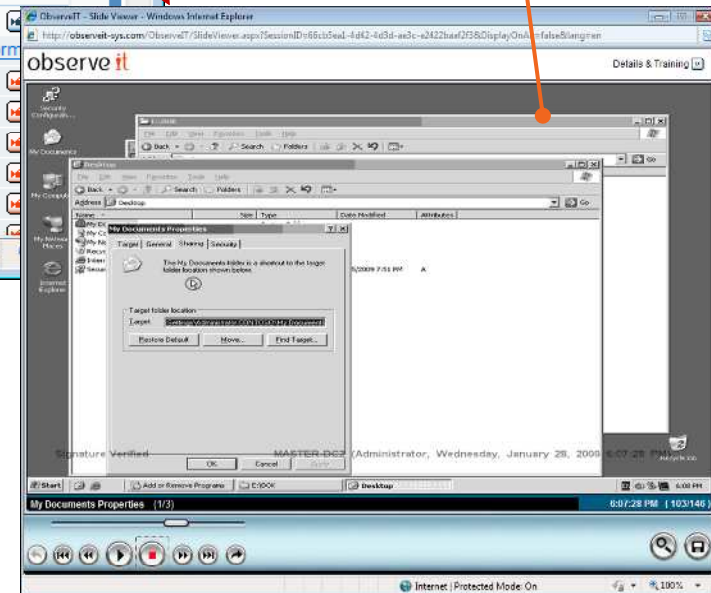
Group Policy Object Editor (2)

Hide these specified drives in My Computer Properties

Internet | Protected Mode: On

リアルタイム
再生を始める

ユーザが操作
中の時、リ
モートでセッ
ションの動作
が見える



レポートの自動作成: 標準レポートとカスタマーレポート

標準監査レポートと自分で作った調査レポート

Report List

Scheduled Reports For Console User: ... Go

Create New Custom Report

Name	Description	Modified	User	
Custom Reports				
SAMPLE: Admin-related tasks - Past Week	Administrative-related tasks performed on monitored servers.	15/11/09	admin	Run Cached Schedule Copy Edit Delete
SAMPLE: App usage grouped by Server Name - Past Week	All apps used on monitored servers. Grouped by Server Name.	25/10/09	admin	Run Cached Schedule Copy Edit Delete
SAMPLE: Apps usage per Server grouped by App Name - Past Week	Report all apps used on the monitored servers. Grouped by App Name.	25/10/09	admin	Run Cached Schedule Copy Edit Delete

メールでのレポートの自動送信をスケジュールする

HTML,XMLまたはExcelの形で、レポートを送信する

明確な要求によりレポートを設計する:
内容の含め、データのフィルタ、ソートとグループ

Server

☒ Server Name ☐ Group Policy Name ☐ Installation Date

☒ Recording Status ☐ Server Version

☒ Sessions Count ☐ Server Last Activity Date

Sessions

☐ Is Session Alive ☐ Machine Name

☐ Session Start DateTime ☐ Session Start Date

☐ Session Video ☐ Session Start Time

☐ Session End DateTime ☐ Client Name

☐ Session End Date

Select columns by which to group your report.

Group By: Server Name Sort Order: Ascending Group Dates By: Date

and then by: Session Start Date Sort Order: Ascending Group Dates By: Date

and then by: User Name Sort Order: Ascending Group Dates By: Date

Select criteria to determine which records to display.

Standard Filter

Start Date: Dec 5 2009 End Date: Jan 5 2010 The Past Period: 1 Past Months

Advanced Filter

Application Name contains regedit Past Weeks

None equals Past Weeks

None equals Past Weeks

None equals Past Weeks

None equals Past Weeks

Selected Columns

Server Name
Server Version
Recording Status
Sessions Count
Server Last Activity Date

Top
Up
Down
Bottom

システムモニターのインテグレーション

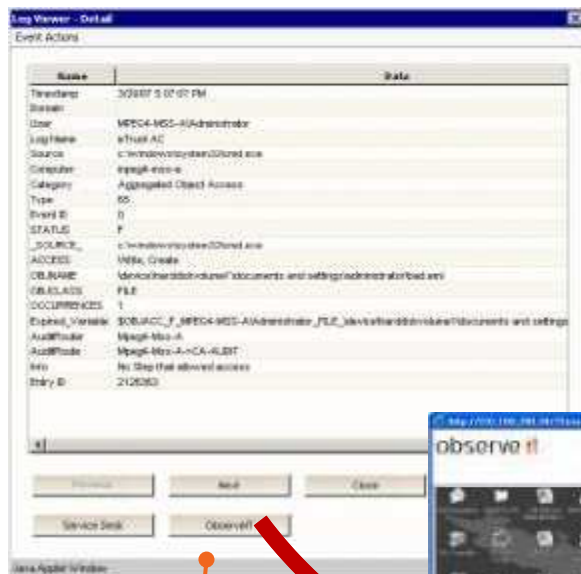
■ ネットワーク管理環境内部から即時再生

- システム: Microsoft SCOM, CA-Unicenter, IBM Tivoli, HP OpenView

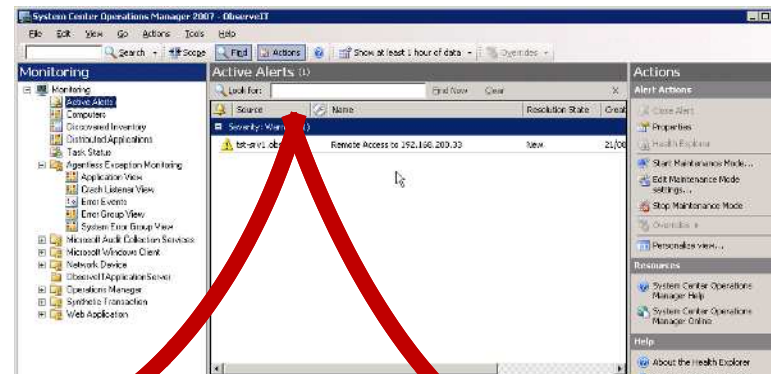
■ リアルタイム警報

- 発生時点: ファイルアクセス・削除、ネットワーク共有、レジストリエディタ、リモートデスクトップ接続、URLアクセスなど

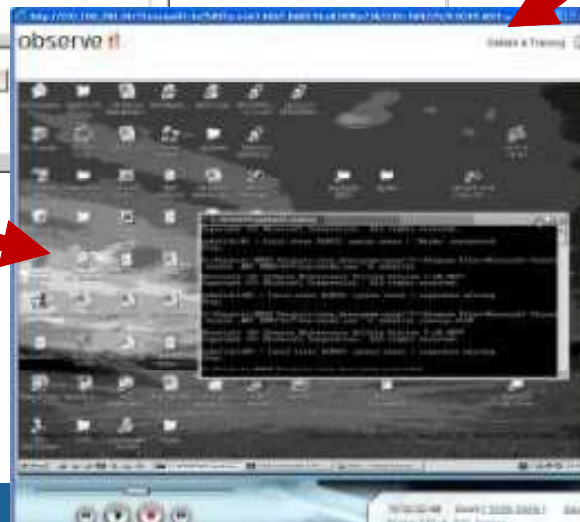
CA-Unicenter に ObserveIT の警報



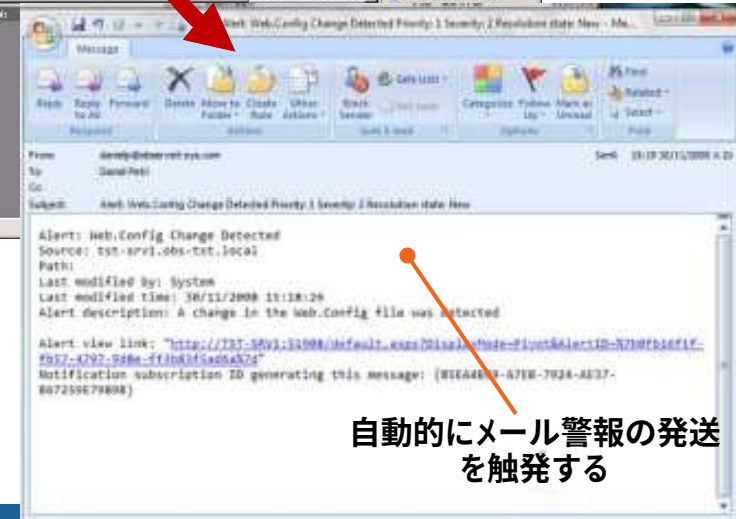
MS SCOM に ObserveIT の警報



警報をクリックしてObserveIT
の映像再生を見る



自動的にメール警報の発送
を触発する



APIインターフェース

企業アプリ中にスクリプトとカスタマ
DLLSでObserveIT代理をコントロール
する

プロセスID、
プロセスネーム又は
ウェブURLに基づいて、
カスタマーイベントに
よって記録されたセッ
ションを開始、停止、
中止、再開

```
api_recording.js

try
{
    var agentApi = new ActiveXObject("ObserveIT.AgentAPI.Proxy");

    var sessionId = agentApi.StartByComputerName( computerName.value, newSession);

    sessionId = agentApi.StartByProcessId( processIdText.value, newSession);

    sessionId = agentApi.StartByDomainName( domainText.value, newSession);

    var res = agentApi.StopByComputerName( computerName.value, newSession);
}

catch (err)
{
    error = err;
}
```

強固なセキュリティ

■ エージェントとサーバーの間の通信

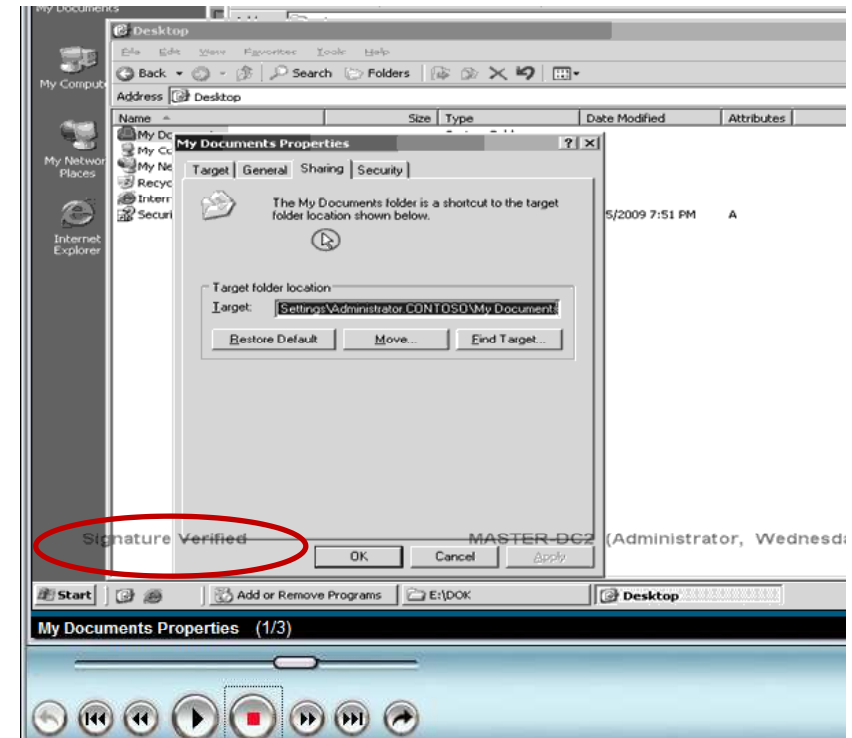
- AES暗号化方式—「Rijndael」方式
- トークン交換
- SSLプロトコール (選択可)
- IPSecトンネル (選択可)

■ データベース記憶装置

- キャプチャーされたセッションにデジタル署名をつける
- 標準SQLデータベースが企業データ安全保障の方法を相続する

■ 監視器機構

- プロセスが終了される場合、エージェントを再起動する
- 監視プロセス自体が停止される場合、エージェントは監視器再起動を触発する
- メール警報は許可されなくても任意の監視器・エージェントに送信できる



録画ポリシールール

サーバー毎にポリシールールの項目を含める。または、含めないことによって、ユーザ・ユーザグループ、又はアプリケーションが録画ポリシーを決める

ユーザ毎に、どのアプリケーションで記録するか、メタデータを記録するかどうか、ステルスモードを指定するかどうかを決める

Server Policies

Server Policies Template

[Back to Server Policies Templates](#) | [Linked Servers](#)

Name: Default Server Policy Template

System Policy

☒ Enable recording

☒ Show tray icon

☐ Enable hotkeys

☐ Enable recording notification

Set image format: Gray Scale Server Compression

Set session timeout (minutes): 15

Offline Policy

☐ Enable

Restrict to max number of items: 1000

Identification Policy

☒ Enforce Login

Please enter Domain Name \ User Name (i.e *administrator or OBSERVEIT\danielp) to enforce identification for that user. You can add multiple users to this list

User	Domain (* for all)	User Name
☐	*administrator	

Domain\User Created Date

1/25/2009

User Recording Policy

☒ Record all Users

Please enter Domain Name \ User Name (i.e *administrator or OBSERVEIT\danielp) to record all users excluding this user. You can add multiple users to this list.

Exclude: User

Domain (* for all) \ User Name

Add

Domain\User	Created Date
-------------	--------------

Remove

☐ Record only the following Users

Please enter Domain Name \ User Name (i.e *administrator or OBSERVEIT\danielp) to only record this user's activities and accessed applications. You can add multiple users to this list.

Enable: User

Domain (* for all) \ User Name

Add

Domain\User	Created Date
-------------	--------------

Remove

Application Recording Policy

☒ Record all applications

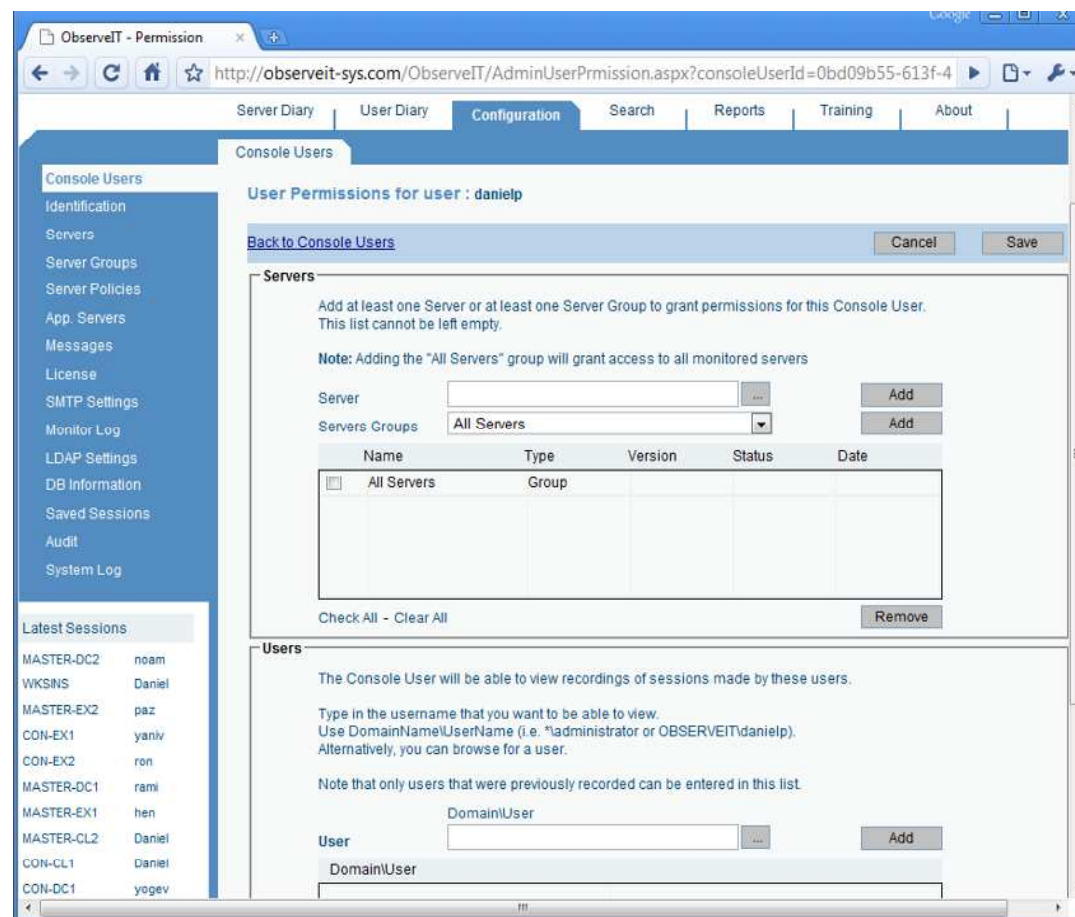
Exclude: Active Directory Installation Wizard - dcpromo.exe

Add

Domain\User	Created Date
-------------	--------------

広がるユーザ権限

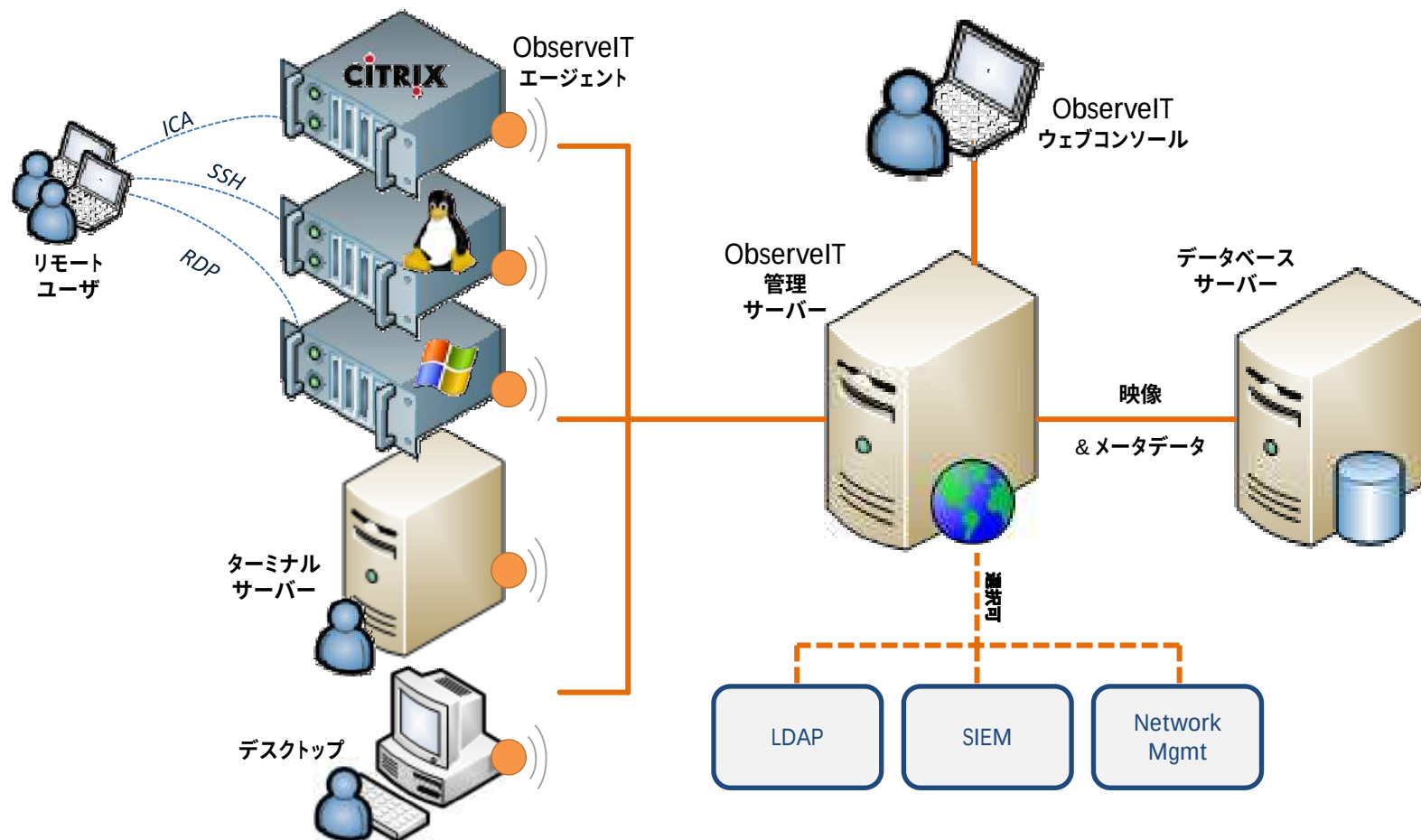
- きめ細かなアクセス権限 / アクセスコントロール
 - ・ ユーザ毎にルールを制定
 - ・ ユーザがどのセッションを再生できるかを指定
- 権限に基づくフィルタ操作が全ての内容アクセスに影響を与える
 - ・ レポート
 - ・ 検索
 - ・ 映像再生
 - ・ メタデータ照会
- 緊密にアクティブディレクトリを統合する
 - ・ 自分のAD庫に管理権限を複数のグループにさせる
- ObservaITウェブコンソールにアクセスすることも監視される
 - ・ ObservaIT監査ツール自体
- 質量保証標準を満足





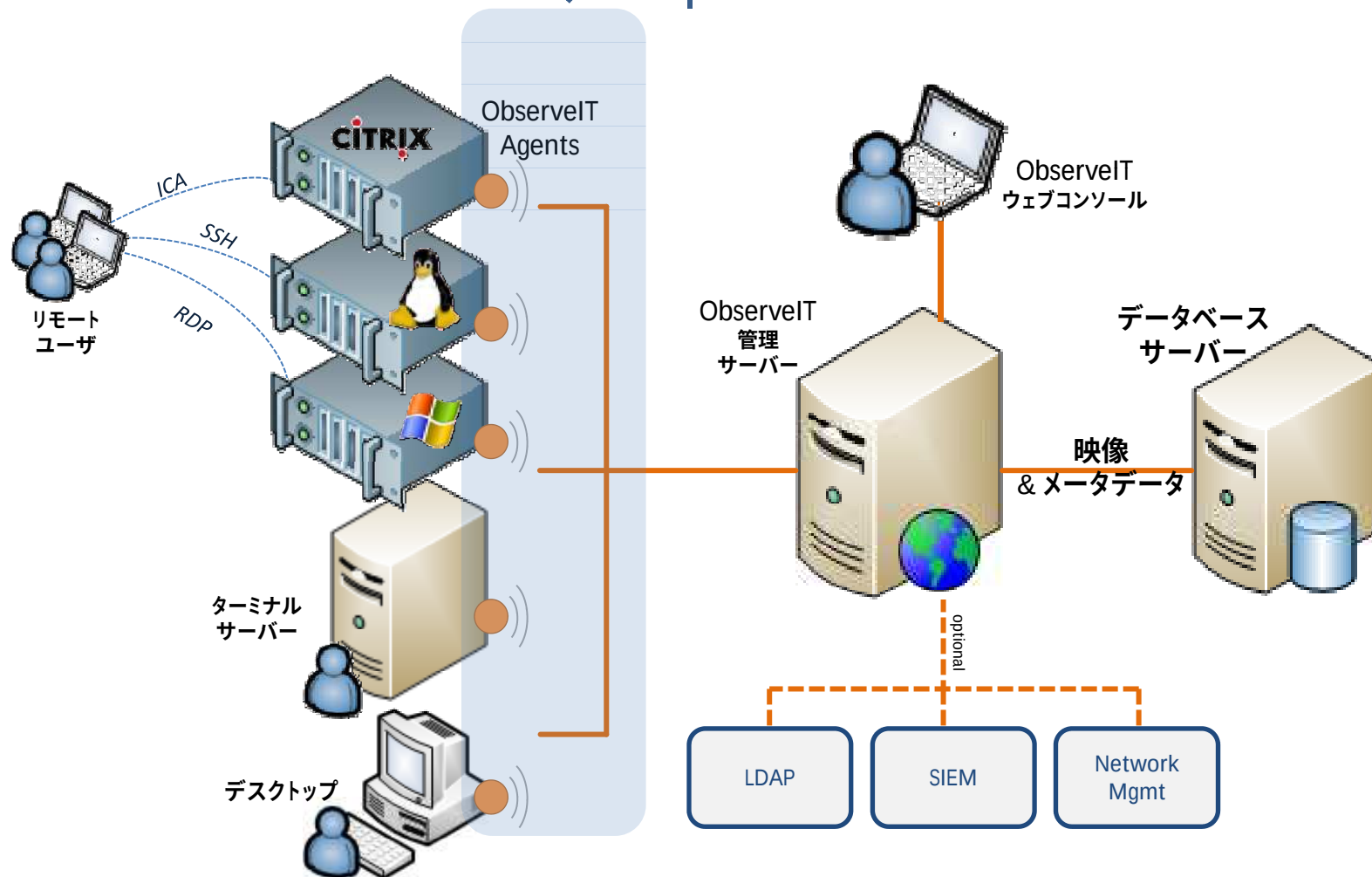
システム構成

ObserveIT 構成

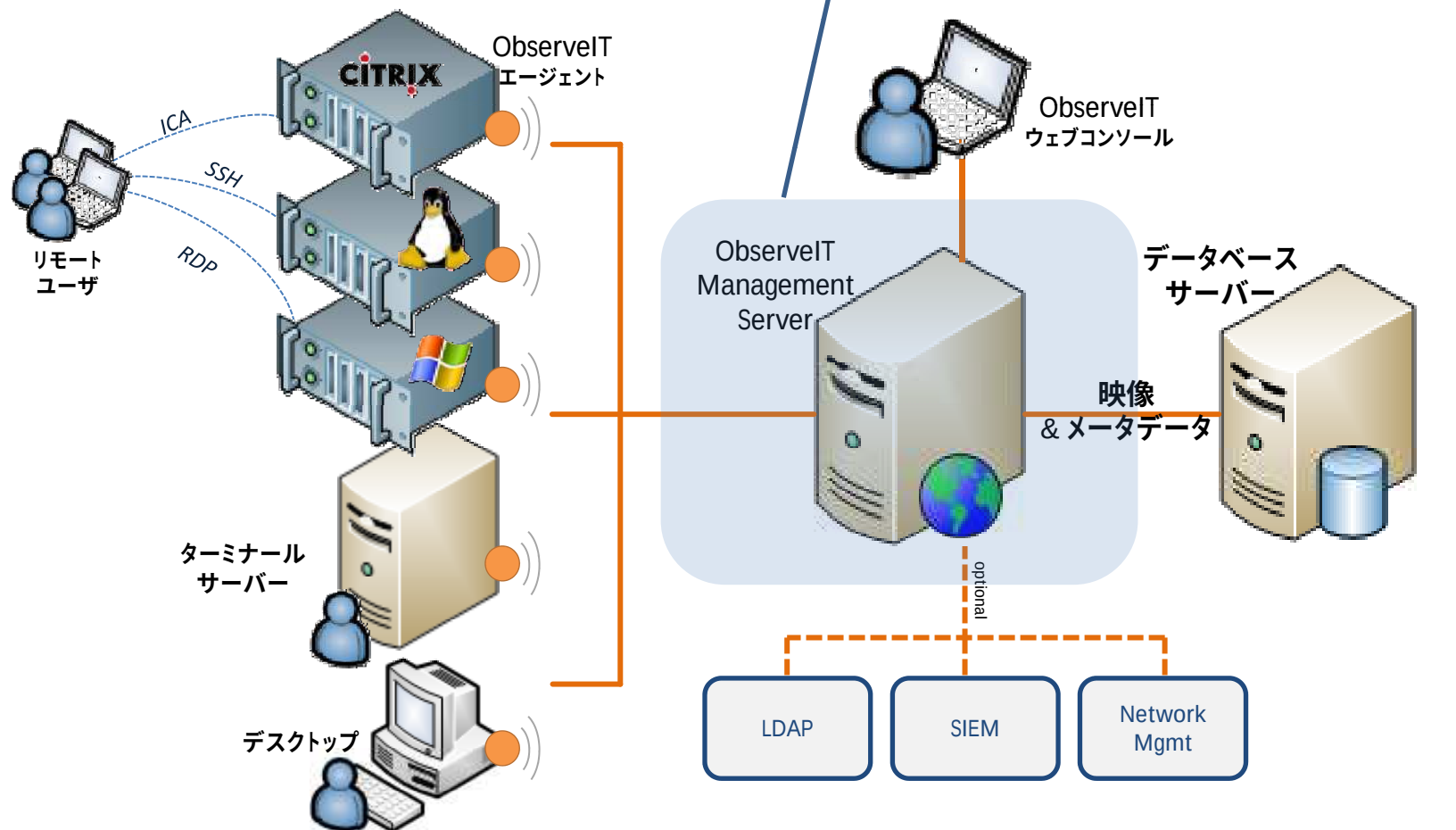


ObserveIT 構成: エージェント

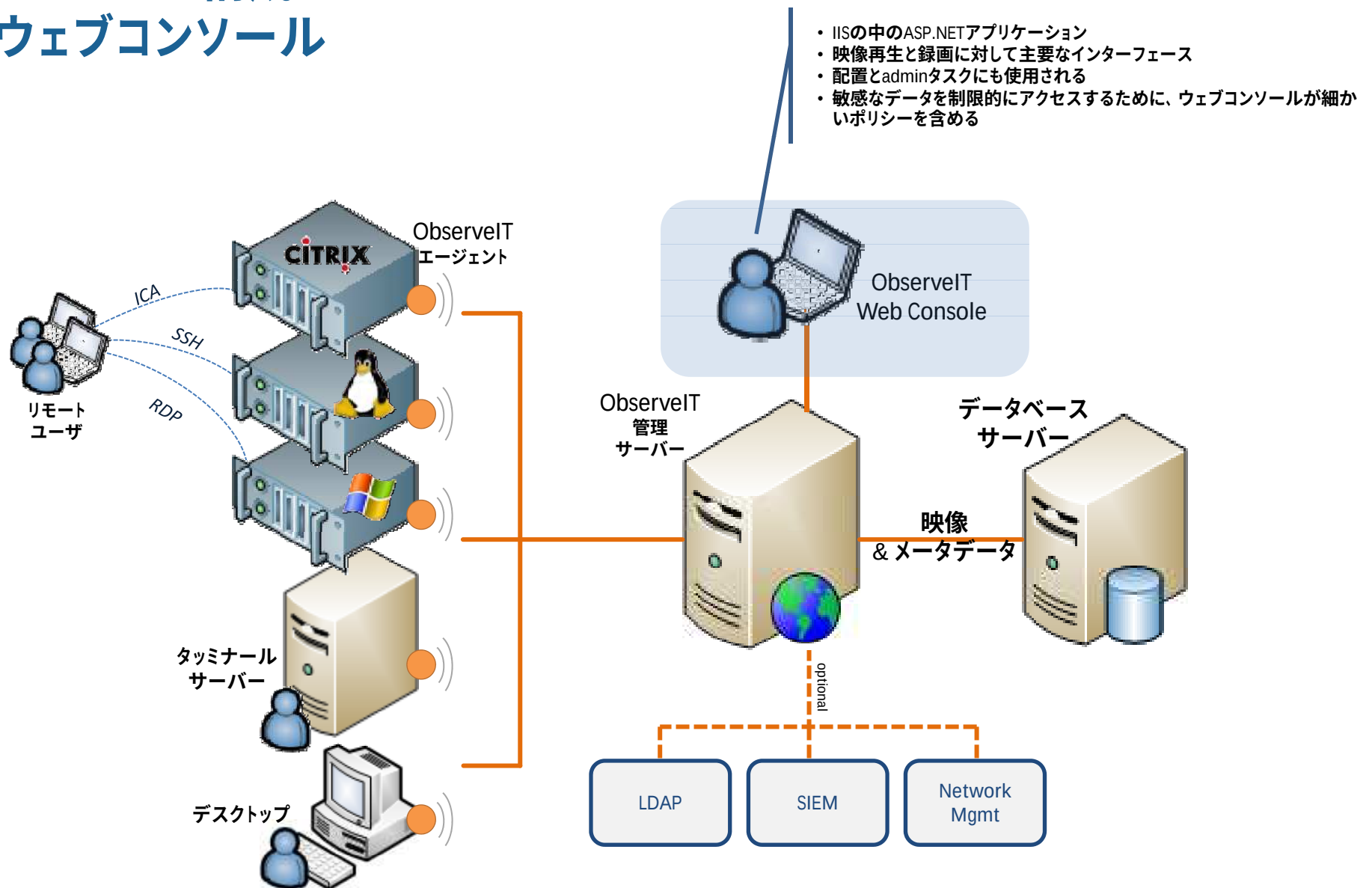
- モニターサーバー毎にセットされる
- 全てのユーザ動作に対して画面コピーとメタデータをキャプチャする
- HTTP POSTを経由して、管理サーバーに通信する
- 全ての内容が暗号される
- 監視器が勝手に変更することを防ぐ



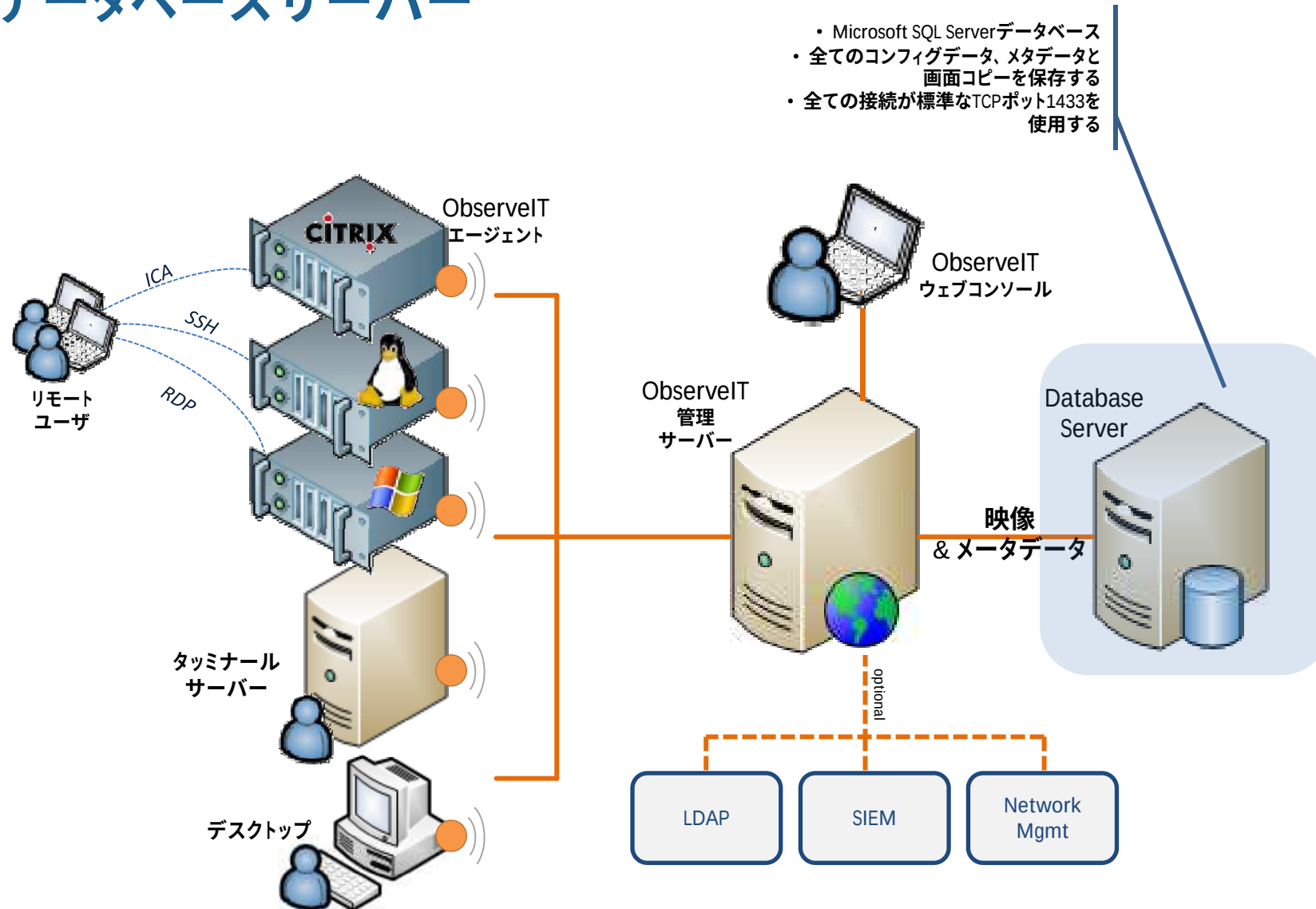
ObserveIT 構成: 管理サーバー



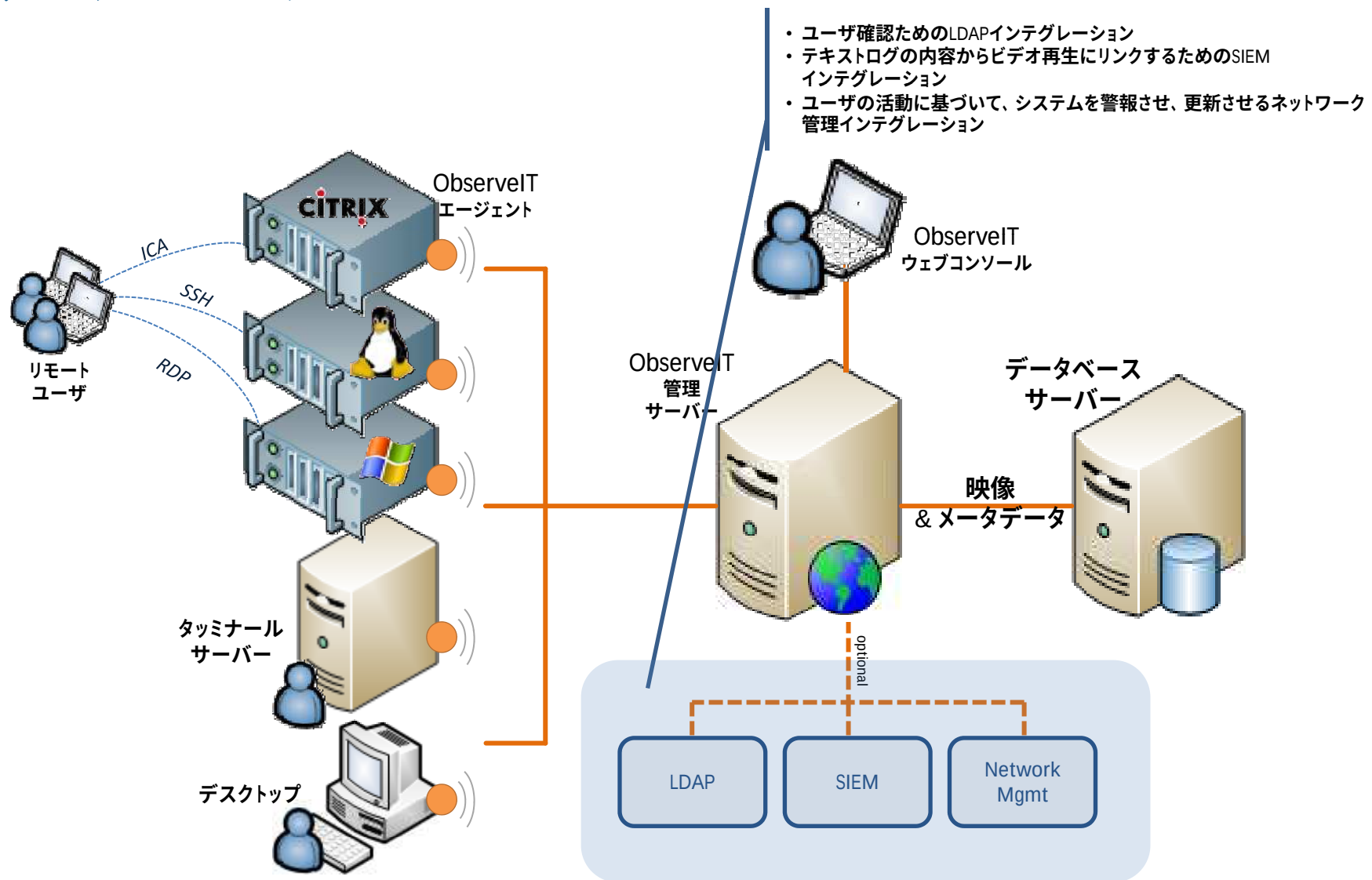
ObserveIT 構成: ウェブコンソール



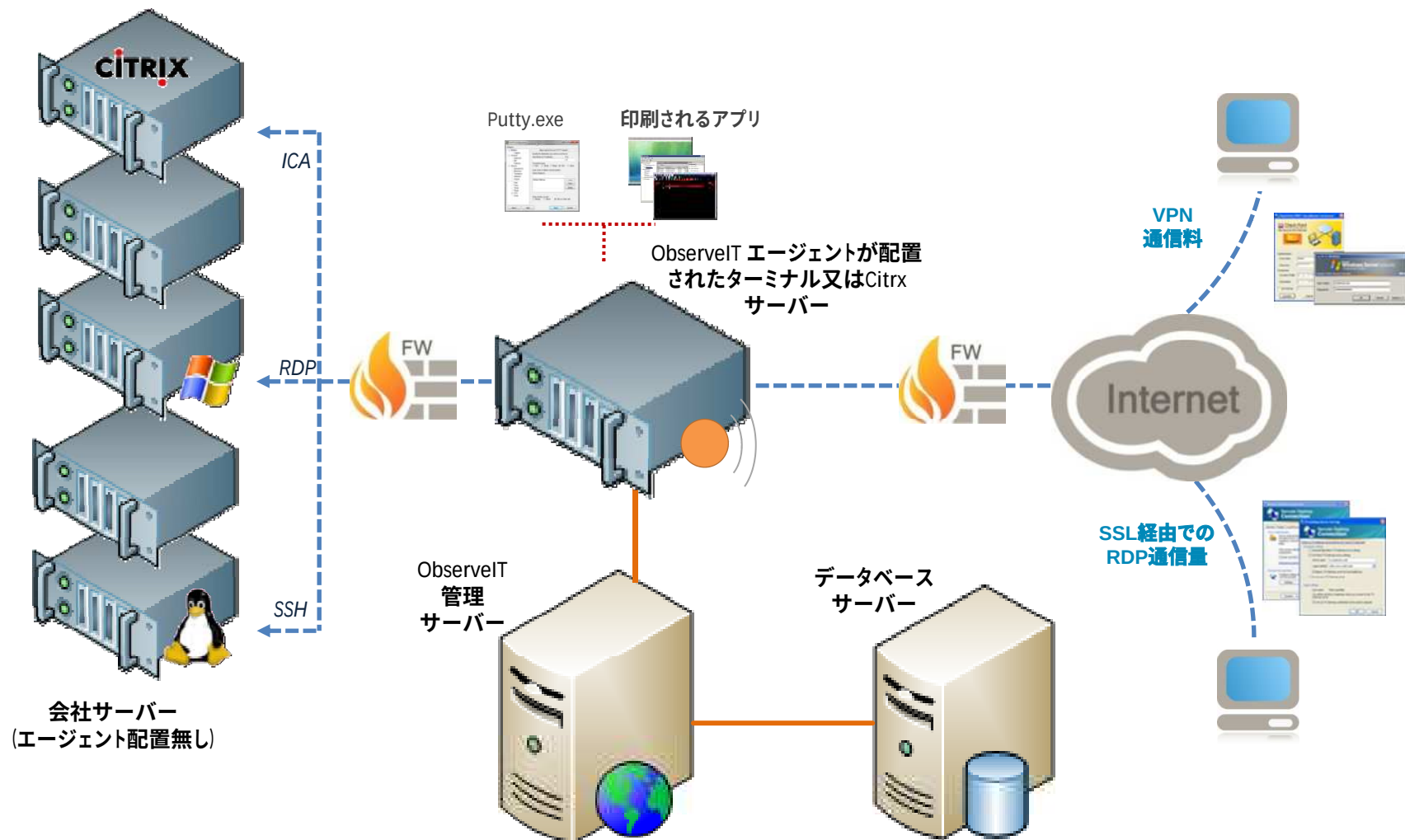
ObserveIT 構成: データベースサーバー



ObserveIT 構成: データベースサーバー



ゲートウェイ配置 (エージェント無し)





顧客事例の研究



HIPAA質量保証監査

TOSHIBA

産業： 医療設備メーカー
解決案： 質量保証レポートの自動化 (HIPAA))
会社： 東芝医療システム

ビジネス環境

- 世界規模の病院、医療センターで医療映像製品 (MRI,CT,US,X-Ray) が配置される
- 顧客支持処理がリモートセッションを請求して、配置されたシステムにアクセスする

チャレンジ

- 厳格なHIPAA質量保証規制が必ず強制され、かつ論証できる
- さらに、SLA委員会がサービス回数とサービス期間の可視を要求する

解決案

- ObserveITがゲートウェイ構造にセットアップ
- 全てのアクセスはエージェントに監視されるCitrixゲートウェイを経由してルートする
- 実際のアクセスされているシステムはエージェント無し
- 細かい事故概要を含めて、Toshibaは24x7 SLAレポートに達する
- 自動的にHIPAA規制証拠書類を作成し、品質保証費用を減少させるし、顧客(病院)の満足度を改善する



市場売買手形交換所のPCI質量保証

産業: 金融サービス
解決案: 質量保証レポートの自動化 (PCI)

ビジネス環境

- 主要な手形交換所が具体的なPCI証拠書類を提供しなければならない

チャレンジ

- 一つ一つの監査レポートサイクルがログ収集の主な努力成果である
- システム変更の実際原因が認識されていない時、監査結果が不完備

解決案

- ObserveITの導入後、監査報告の完全自動化
- 監査拒否がなくなる

リモートユーザ監査機能向けのISO27001質量保証



産業: 公共事業・建築業
解決案: 質量保証レポートの自動化 (ISO 27001)
会社: Elektrotim

ビジネス環境

- 多くの政府と会社の顧客がISO質量保証を要求する
- 基幹業務のERPプラットフォームが外部のサービス提供者に管理される
- 会社の経営哲学が安全、確実と高標準を掲げている

“我々のITシステムにアクセス
していた第三者との問題を
防ぐために、リモートユーザ
監査機能の実装を要求した”

Przemysław Jasiński
IT部門マネージャ
Elektrotim

チャレンジ

- 質量保証の必要条件は、ネットワークにアクセスするすべての外部ユーザの動作を監視、記録すること

解決案

- ObserveITが会社サーバーとTS機械に配置される
- 画面コピーと、簡単に検索できるテキストインデックスを組み合わせる
- リモート接続でシステムにアクセスすることがすべて安全に記録される
- 事件毎に調査するとき、ログに迅速的にアクセスできる



リモート管理者ユーザ監視



産業: 金融サービス
解決案: リモート監査
会社: VocaLink

ビジネス環境

- 売買プラットフォームが全ヨーロッパに配布される
- 60,000台ATM機械をサポートする
- 毎日90,000,000件の売買を決済する

チャレンジ

- 合併期間、二つの会社間に、共有した特権を含め、システム資源のアクセスをコントロールする
- 一般的なシステム管理機能と可視化を実現

解決案

- 2008: 会社併合中にObserveITが配置されて、サーバーの動作をモニター、監査する
- 2009: 併合後、良好な可視化の実現により、システム全体的に配置される



医療システムリモート監査

SIEMENS

産業： 医療設備
解決案： リモート監査
会社： Siemens Medical Instruments

“ObserveITはサーバーですべての単一ユーザセッションを記録することができるだけでなく、記録をインデックスすることができ、我々を興味エリアに集中させる。”

Robert Ng,
Siemens

ビジネス環境

- 内部と顧客の解決方法に向ける企業サーバーホストのビジネスアプリ
- サーバーがさまざまな権限を持っているスタッフメンバーに管理され、アクセスされる
- アクセスも多くの外部の販売契約者に向ける

チャレンジ

- ObserveITが現れる前に、サーバーでユーザの活動を記録する実行可能の方法がない

解決案

- ObserveITがすべての内部と外部委託販売管理者の監査責任を提供する
- 報告と検索が重大問題に適用される
- 速やかな配置が速く、簡単にできるuptimeを保証する。(uptime: 連続稼働時間を表示するプログラムである):
“我々がする必要があることの全ては小さなエージェントをサーバーにインストールしてモニターされ、記録装置が直ちに始まり、何の配置と設定が要求されない”



特権を持つユーザ監査



産業: 健康管理IT
解決案: 特権を持つユーザ監査
会社: 健康管理アクセス促進中心

“サーバーが立ちあがると動作を保つこと。品質保証を示すため、管理者のニーズも周知することはキーポイントである”

“われわれは、IT管理者と内部スタッフで、すべてのサーバーアクセスを記録することが必要である。”

Vinay Singh
IT実施マネージャ

ビジネス環境

- Webに基づくシステムが家庭の健康範囲、社会サービスとほかの連邦と州のサポートプログラムを結ぶ
- 三つの離れたデータセンターを通じて、サーバー93台とワークステーション91台に配置され、管理される

チャレンジ

- センターはデータの安全性、有用性、アクセスと応答の利便性に専念する。
- 個人健康記録データの正確性とデータアクセスの質量保証に関する政府規則が提供され、センターは安全性とすべてのデータとサーバーアクセスを詳細な監査方法をに改良しようと努める

解決案

- 確実に開発者と管理者が何をしているかを知ること、不安がない
- 規則順守の用法レポートの即時実現
- システム故障の速やかな応答時間



第三販売者によりエラーの削減



産業: 通信
解決案: 根本原因解析 + モニター
会社: Pelephone

“ObserveITが配置されたため、
ユーザがさらにサーバー操作
に慎重となる。
アクションが再生されることが素晴らしい
効果をあげる。”

Isaac Milshtein
取締役、IT 営業、
Pelephone

ビジネス環境

- 三つホストセンター中に、1200個サーバーのIT環境
- 複数のビジネスアプリケーション(課金, CRM, etc.)と複数の顧客向けのアプリケーション (移動サービスの収入)

チャレンジ

- 他社製のアプリで サービスの品質を維持する
- 特権を持っている活動を追跡する

解決案

- 2006: まず五つ内部のビジネスアプリサーバー上に、ObserveITが配置。ミッションクリティカルが要求されるアプリでのトラブルを解決し、外部委託管理で不適当な行動を確認する
- 2007: 全社のシステムでObserveITが配置された
- 2008: ObserveITがCA-Unicenter環境に統合された
- 2008: 現在:
 - 複数顧客向けのサービス停止が解決された
 - サービス停止による収入損失を取り除くことを通じて、投資収益率が向上



IT会社で管理されたサービス監視

産業: ITサービス
解決案: 管理されたサービス監視

ビジネス環境

- ITサポート提供会社が世界規模で40分野以上の1000クライアントにシステム管理サービスを提供する

チャレンジ

- 各顧客が異なる接続プロトコル要求がある (VNC経由やRDP経由やCitrix経由など)

解決案

- 外向きのゲートウェーを配置してから、顧客サーバー上のすべてのセッションが記録された
- 導入後は、システム問題に関して顧客からのクレームが少なくなる
- 発生した問題について、すべての行動が適正であることが証明された記録は、速やかに提供されるようになった



Thank You!

www.observeit-sys.com

ObserveIT会社紹介

- 2006年設立
- 監査ソフトウェア製品に専念する
 - 最初のGA製品のリリース:2007年
 - 現在の製品バージョン:V5.2
- グローバルプレゼンス
 - 世界範囲で企業顧客400社
 - チャンネルパートナーが5つの大陸をカバー
 - コンピューターアソシエーツでOEMと配布契約