

---

オペレーション証跡ソリューション  
**Illegal View**  
ご説明資料

株式会社 日立ソリューションズ・クリエイト

# Contents

---

- 1 .セキュリティの情勢
- 2 .Illegal Viewとは
- 3 .メニュー体系
- 4 .最後に
- 5 .ご参考資料

---

# 1. セキュリティの情勢

# 1. セキュリティの情勢

## 1 内部関係者による相次ぐ情報漏洩事件

発生日	概要
2016年2月	AA社の元執行役員が、子会社に出向中、営業秘密である主力製品の情報を私物のUSBメモリに保存して持ち出し、その後の転職先の競合企業BB社に開示したとして不正競争防止法違反の疑いで逮捕された。
2015年10月	市職員が市民の個人情報を含む行政情報等のファイル約220万件を、職場に貸与されたUSBメモリを使い不正に持ち出し、自宅に保管していた。停職6ヶ月の処分。
2015年9月	市職員が、約68万件の有権者情報を無断で自宅に持ち帰り、外部に流出させた。懲戒免職処分。
2015年4月	A社の元社員ら（4名）が、営業秘密である包装機械の設計図を不正に取得したとして不正競争防止法違反で逮捕された。2013年に退職後、競合他社へ転職している。また転職先の企業に、差止め及び損害賠償等提起。両罰規定により罰金の支払いが命じられた。

### 内部不正事件の傾向

- 内部関係者による情報窃取の場合、漏洩規模が大きくなりやすい
- 狙われるのは企業の競争力に関わる重要情報であることが多い

### 動き

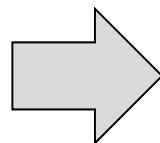
- 経済産業省から経済団体へ個人情報保護法等の遵守に関する周知徹底を要請（2014年8月）
- IPA（情報処理推進機構）：「組織における内部不正防止ガイドライン」を改訂（2015年3月）

# 1. セキュリティの情勢

## 2. セキュリティ インシデントにおける要因の変化

今まで

- 外部からの攻撃を想定
- 「社員は大丈夫」という考え方



これから

- 外部から攻撃に加え、社内情報にアクセスできる「内部」の人も監視が必要

## 3. 内部不正のトライアングル



3つの要因全てが揃ったとき  
内部不正が発生する

※米国 犯罪学者クレッシーの不正  
トライアングル理論

**内部不正を阻止する製品が求められています**

---

## 2 .Illegal Viewとは

- 2. 1 Illegal Viewとは
- 2. 2 Illegal View機能
- 2. 3 Illegal View構成
- 2. 4 システム環境

## 2 - 1 . Illegal Viewとは

 Windows画面を常時記録する製品です。

### 1 PC・サーバに監視カメラを設置するイメージ

Windows画面に対する操作を隅々まで録画（※）  
※画像の断片を記録し繋ぎ合わせたもの

### 2 他社製品と比較して少ないデータ容量で記録 \*当社調べ

独自の画像圧縮技術により、解像度を落とさず  
少ないデータ容量による記録を実現します。

### 3 様々なログと動画を連動して記録

様々なログと動画が同期しており、見たい箇所をピンポイントで再生できます。

### 4 様々なアラームと制御が設定できます。

アプリケーションの起動、ファイルへのアクセス、リムーバブルドライブの接続などを検知した際の、メール通知や強制ロックなどの設定ができます。

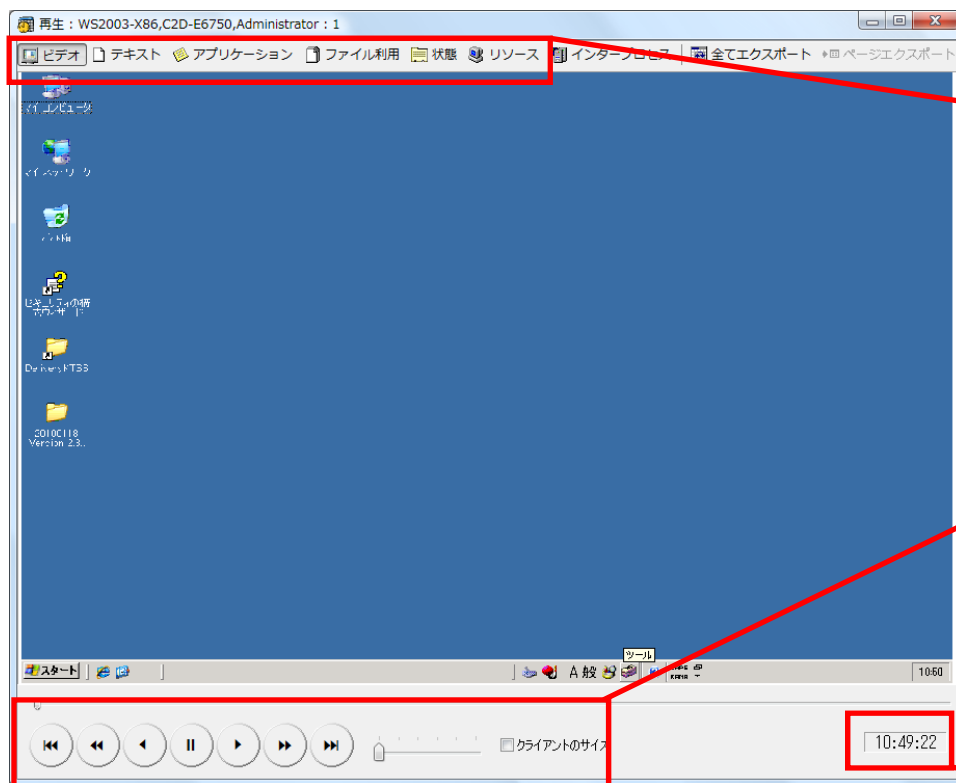


録画されているという意識から不正行為への「抑止力」に繋がります

## 2 - 2 . Illegal View機能

### PC・サーバに監視カメラを設置するイメージ

管理コンソールから、記録データをビデオデッキを使用する様に簡単な操作で閲覧できます。



タブを切り替える事で、  
動画や、様々なログを表示します。

記録データの再生、早送り、  
巻き戻しなどできます。

標準で以下の再生機能を有します。

2倍速再生、4倍速再生  
2倍速逆再生、4倍速逆再生

時間を入力することで、  
ピンポイントで再生できます。



### Illegal Viewの録画性能

独自の画像高圧縮技術により、

- 記録画像サイズ30MB/8時間を実現
- 解像度を落とさない
- 文字つぶれが無い

それにより

- 大規模・大容量の記憶装置は必要ありません。
- ネットワーク/PCに負荷をほとんど与えません。

### 他社製品との比較

【比較条件】

PC 1 台、解像度XGA(1024x768)、5秒間隔、16色へ減色、  
1日(8時間連続記録)、マルチモニタ無しの場合

他社製品との比較	Illegal View	A社製品	B社製品
記録画像サイズ	30MB	780MB	100MB
減色	あり	なし	なし
解像度	変化せず 文字つぶれ無し	減 文字がつぶれる	減 文字がつぶれる
画像記録方式	独自方式	MPEG	MPEG

<想定容量>

PC 20 台、期間5年間(1,825日)にした場合でも  
想定容量 (理論値) は**約1.1TB**

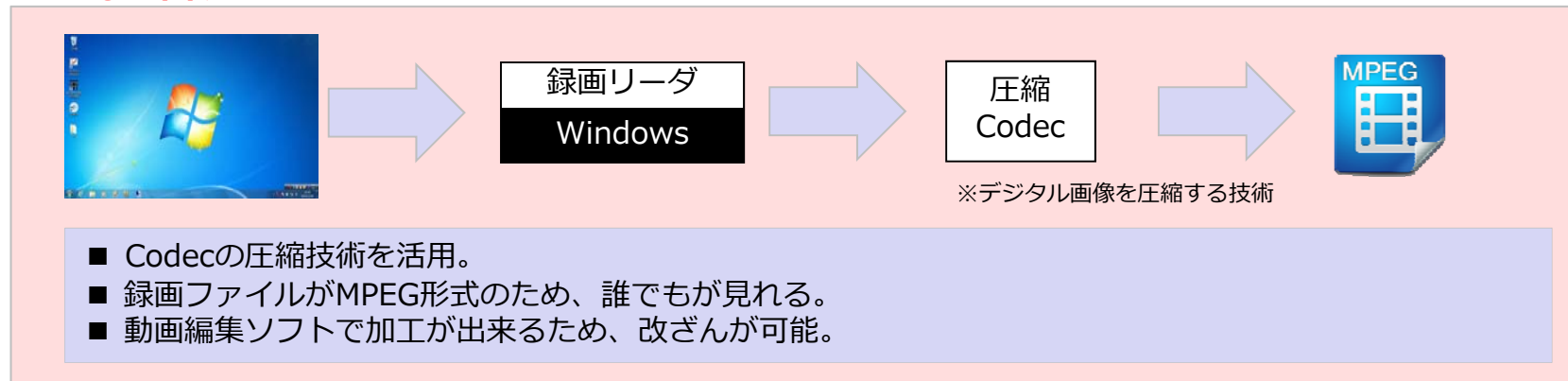
※：想定容量は理論値であり、実際のHDD容量を保証するものではありません。

※：他社製品の情報については、調査した時点での内容であり、最新の製品と異なる場合があります。

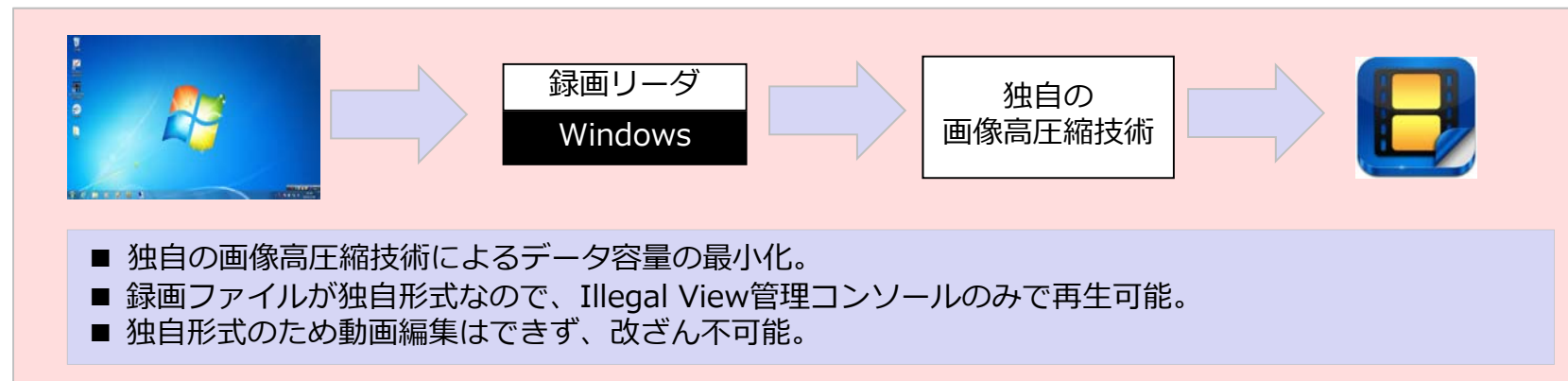
## 2 - 2 . Illegal View機能

### Illegal Viewの録画機能

#### 一般的な録画機能



#### Illegal View録画機能



## 2 - 2 . Illegal View機能

### ■ テキストで出力されるログと動画の連動

多くの製品は「テキスト型」、「動画型」に分別

テキスト型	保存される情報	テキストログ
	メリット	証拠を保管するストレージサイズを抑えることができる。
	デメリット	<ul style="list-style-type: none"> <li>・ログから証拠の解析が必要で再現性が低い。</li> <li>・ログを加工することで証拠の改ざんが可能。</li> <li>・パッケージ化されており、要望に合わせた加工が困難。</li> </ul>
動画型	保存される情報	動画もしくは画像
	メリット	<ul style="list-style-type: none"> <li>・証拠を完全に再現でき、解析の負担が低い。</li> <li>・証拠の改ざんが限りなく不可能に近い。</li> </ul>
	デメリット	<ul style="list-style-type: none"> <li>・証拠を保管するためのストレージサイズが肥大化する。</li> <li>・確認したい情報を効率的に収集しにくい。</li> <li>・動画取得をメイン機能としている製品が少なく、オプション扱いの場合が多い。</li> </ul>

Illegal Viewは「テキスト型」「動画型」それぞれのメリットを有しております。

Illegal View	保存される情報	動画（画像）+テキストログ
	メリット	<ul style="list-style-type: none"> <li>・動画取得をメイン機能としている。</li> <li>・操作を完全に再現可能。</li> <li>・動画（画像）とテキストログが連動しており、見たい情報を簡単に検索できる。</li> <li>・独自の圧縮方式を採用しておりストレージサイズを抑えることができる。</li> <li>・ご要望に合わせたカスタマイズ開発が可能。</li> </ul>
	デメリット	特になし

## 2 - 2 . Illegal View機能

### 見たい箇所をピンポイントで再生

様々なログと動画の連動により、録画された画像をピンポイントで効率的に再生できます。

テキストログ

キーボードログ

アプリケーションログ

ファイル利用ログ

状態ログ

リソースログ

選択した場面から映像を再生

## 2 - 2 . Illegal View機能

### アラーム設定と通知

以下のアラームと通知を設定できます。

- ・ **誰が** (どのPCで/どのユーザで/どのグループで)
- ・ **何をしたら** (例：アプリケーションを起動したら)
- ・ **どうするか** (メール配信/強制ロックなど)

アラーム機能	アプリケーション	アプリケーションの起動通知・起動制限をおこないます
	リソース	PCへのハードウェア・ソフトウェアの変更を通知します
	ファイルアクセス	ファイルの利用通知・利用制限をおこないます
	キーワード	デスクトップ上の文字列を検知し通知します
	リムーバブルドライブ	リムーバブルドライブの接続を検知し通知します
	ログイン	ログインとログインユーザを検知し通知します
	システム	製品の状況を通知します
通知方法	メール配信	登録された管理者へメールを送信します
	コンソールへ警告表示	管理コンソール上にポップアップを出力します
	ログ記録	アラーム内容のログを記録します
	メッセージ送信	対象PCへメッセージを送信します
	強制ロック	コンピュータ画面をロックします



## 2-2. Illegal View機能

### ■ アラーム設定例①（ログインアラーム）

Windowsへログイン時、「記録している」旨を通知する設定例  
(抑止力強化に効果的)

ログインアラームの設定

名称: ログイン時、監視対象であること通

説明: ログイン時に記録している旨を通知する。

イベント:

クライアントセット: デモ用

ユーザセット: <すべてのユーザ>

アクション:

コンソール上に警告を表示     Eメールを送信

ログを記録     デスクトップをロック

記録条件を変更    <default>

通常の記録条件に戻すのは 0 秒後

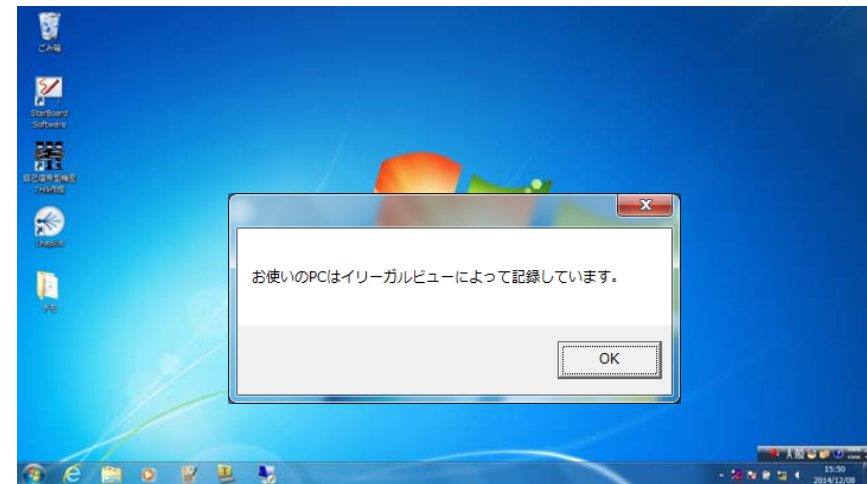
通常の記録条件に戻すのはユーザのログオフ

特殊アクション:

デスクトップにメッセージを表示する  
お使いのPCはイリーガルビューによって記録しています。

実行

OK    キャンセル



## 2-2. Illegal View機能

### ■ アラーム設定例② (キーワードアラーム)

特定のキーワード ("マル秘")を検知し、対象PCを強制ロックする設定例

キーワードアラームの設定

名称: PCロック対象キーワード

説明: PCロック対象キーワードを検知→クライアントをロックする

イベント:

キーワードセット: PCロック対象キーワード

クライアントセット: デモ用

ユーザセット: デモ用

アクション:

コンソール上に警告を表示  Eメールを送信

ログを記録  デスクトップをロック

記録条件を変更 <default>

通常の記録条件に戻すの 0 秒後

特殊アクション:

アラーム発生 0 秒以内は次のアラームを発生させ

デスクトップにメッセージを表示する

PCロック対象キーワードを検知した為、お使いの

実行

OK キャンセル

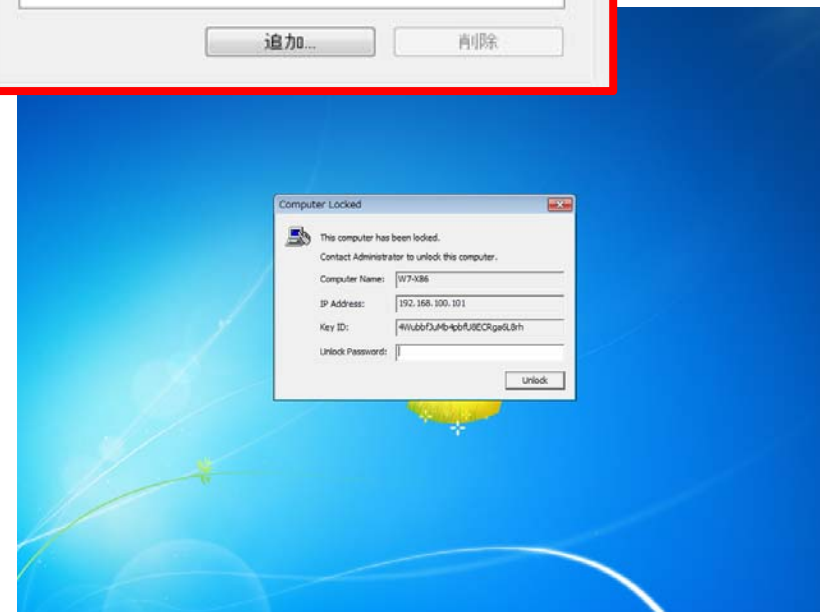
キーワード:

キーワードテキスト

極秘

マル秘

追加... 削除



## 2-2. Illegal View機能

### 制御設定例① (リムーバブルドライブアラーム)

USBメモリなどの“リムーバブルドライブ”の利用の制御設定例

リムーバブルドライブアラームの設定

名称: USBメモリの利用を制限

説明:

イベント:

クライアントセット: IviewClient

ユーザセット: <すべてのユーザ>

アクション:

コンソール上に警告を表示     Eメールを送信

ログを記録     デスクトップをロック

イベントログに記録

記録条件を変更    <default>

通常の記録条件に戻すのは 0 秒後

特殊アクション:

読み取りと書き込みを禁止

書き込みを禁止

デスクトップにメッセージを表示する

実行

OK    キャンセル

リムーバブルディスクの接続を検知し、動作を制御できます。

- 読み取りと書き込みを禁止
- 書き込みを禁止
- デスクトップにメッセージを表示



## 2 - 2 . Illegal View機能

### 制御設定例② (ホワイトリスト)

アプリケーションの起動を検知し通知、ホワイトリストに登録されているアプリケーション以外は起動させない設定

アプリケーションアラームの設定

名称: White List  
説明: ホワイトリスト以外のアプリケーションの起動を禁止

イベント:  
フィルタタイプ: 許可  
アプリケーションセット: White List  
クライアントセット: IviewClient  
ユーザセット: <すべてのユーザ>  
 リストに存在しないアプリケーションが実行されたらアラーム

アクション:  
 コンソール上に警告を表示  
 ログを記録  
 記録条件を変更  
 Eメールを送信  
 デスクトップをロック  
記録条件を変更: <default>  
 通常の記録条件に戻すのは 0 秒後  
 通常の記録条件に戻すのはアプリケーションの終了後

特殊アクション:  
 アプリケーションを起動させない  
 デスクトップにメッセージを表示する  
許可以外のアプリが起動されました

実行

OK キャンセル

アプリケーションセットの作成

名称: White List  
説明: 利用可能なアプリケーションを登録しておくリスト

アプリケーション:

アプリケーション名	IV コード
wuauclt.exe	F7BB94F1
wsqmcons.exe	D14306D8
wmiprvse.exe	9C32260A
WMIADAP.EXE	FD329FB6
wlms.exe	C76C38B0
winlogon.exe	B89012C4
wininit.exe	2FC8F3C5
wermgr.exe	62651AE8
userinit.exe	6271D6A2

追加... 削除 インポート...

OK キャンセル

## 2 - 3 . Illegal View構成

### 『サーバ・クライアント・コンソール』の構成

#### Illegal Viewサーバ

Illegal Viewのマネージャー  
各Illegal Viewクライアントの制御、画像データを保管します。

#### 管理コンソール

Illegal View製品を管理・設定するためのコンソールです。  
(コンソールは**ライセンスフリー**です)

#### Illegal Viewクライアント

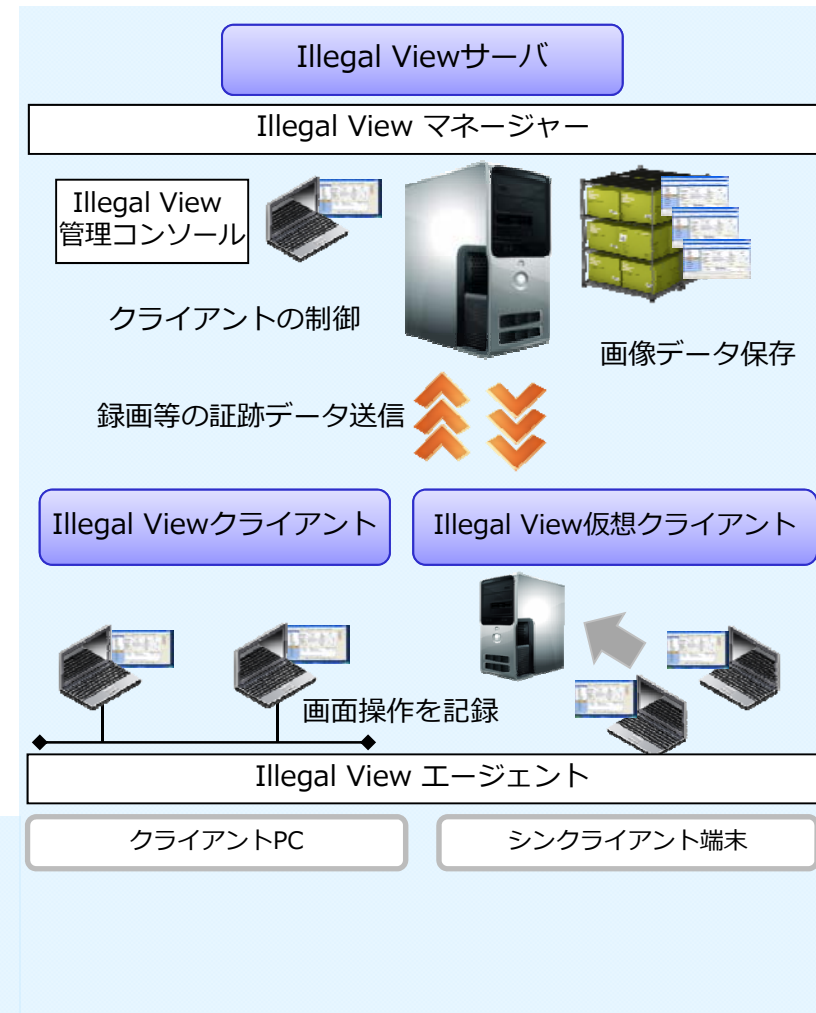
Illegal Viewのエージェント  
Illegal Viewサーバからの命令を受け付けて実行します。  
Illegal Viewサーバへのデータ送信やコンソールへの通知も  
本クライアントが実行します。

#### Illegal View仮想クライアント

Illegal Viewのリモート接続用エージェント  
RDSやVMware 上の操作を取得する際に導入が必要です。  
デスクトップ転送 (VNC等) の場合は不要です。

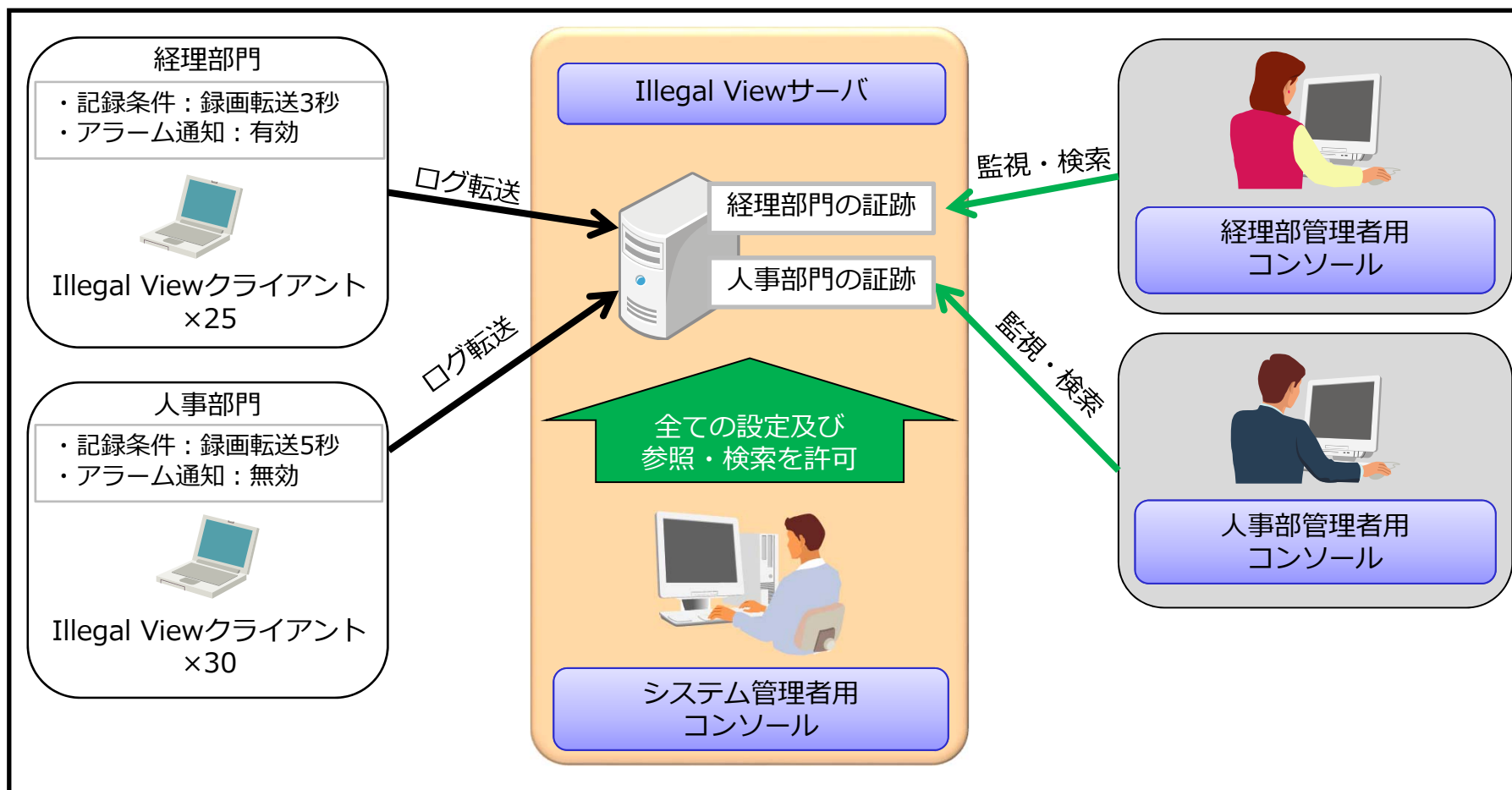
Illegal ViewサーバとIllegal Viewクライアントがネットワーク上で疎通可能な環境であれば、画面を記録できます。

インターネット経由でもデータの受け渡しも可能です。



## 2-3. Illegal View構成例

### 構成例（部門別）



Illegal Viewの**管理コンソールはライセンスフリー**です。（複数の管理者端末にインストール可能）  
また、**部門管理者毎のアクセス権限が設定でき、見える範囲を厳密に設定できます。**

## 2-4. システム環境①

### Illegal Viewサーバ

OS (*1) (*2) (*7)	<ul style="list-style-type: none"><li>• Windows Server 2016</li><li>• Windows Server 2012 R2 Windows Server 2012</li><li>• Windows Server 2008 R2 Windows Server 2008</li><li>• Windows 8.1(*3)</li><li>• Windows 7(*3)</li></ul>
CPU	Pentium4以上を推奨
Memory	2GByte以上を推奨
HDD	サーバプログラム格納に20MByte, 保存するデータ量(*4)(*5)(*6)
CDドライブ	サーバプログラムインストールに利用
ディスプレイ	640x480 以上の解像度 256 色以上表示可能

### Illegal Viewクライアント

OS (*1) (*2)	<ul style="list-style-type: none"><li>• Windows Server 2016</li><li>• Windows Server 2012 R2 Windows Server 2012</li><li>• Windows Server 2008 R2 Windows Server 2008</li><li>• Windows 10</li><li>• Windows 8.1</li><li>• Windows 7</li></ul>
CPU	Pentium4以上(推奨)
Memory	1GByte以上を推奨
HDD	クライアントプログラム格納に20MByte, オフラインモードの設定値(*8)
CDドライブ	クライアントプログラムインストールに利用
ディスプレイ	640x480 以上の解像度 256 色以上表示可能

## 2-4. システム環境②

### Illegal Viewコンソール

OS (*1) (*2)	<ul style="list-style-type: none"><li>• Windows Server 2012 R2 Windows Server 2012</li><li>• Windows Server 2008 R2 Windows Server 2008</li><li>• Windows 8.1(*3)</li><li>• Windows 7(*3)</li></ul>
CPU	Pentium4以上(推奨)
Memory	512MByte以上(推奨)
HDD	コンソールプログラム格納に20MByte
CDドライブ	コンソールプログラムインストールに利用
ディスプレイ	1,024x768 以上の解像度 256 色以上表示可能

(\*1)各OSの日本語版/英語版、32bit/64bitに対応しています。

(\*2)物理/仮想環境については、弊社製品が対応するOSが正常に動作することと物理/仮想環境によりOSの情報等書き換えられていないことが前提となります。そのため物理/仮想環境固有に発生した事象については免責といたします。

物理/仮想環境固有に発生した事象についての対応は試みますが、問題の特定・解決・回避、製品の改修などを実現することが不可能な場合もありますことをご了承ください。

(\*3)サーバ用途OS ではないため、本製品導入後のネットワーク障害は免責といたします。

(\*4)サーバPCのディスク容量がなくなった場合、クライアントからの転送データは記録しません。

(\*5)1クライアントあたり1日の最大記録サイズは4GByteを上限とし、以降のクライアントからの転送データは記録しません。

(\*6)ひとつのサーバには最大5,000クライアントを登録することができます。

(\*7)64bit系OSへの64bit版の導入には事前にMicrosoft Accessデータベースエンジン2010再頒布可能コンポーネントの導入が必要です。

(\*8)オフライン記録中にクライアントPCのディスク容量がなくなった場合、クライアントプログラムは記録を停止します。

---

## 3.メニュー体系

### 3. 1 製品体系

## 3-1. 製品体系（1/3）

### ① 基本ライセンス

#### 販売単位価格

ライセンス	標準価格 1ライセンスあたり
Illegal Viewサーバ	¥1,000,000
Illegal Viewクライアント	¥50,000
Illegal View仮想クライアント	¥70,000

※最少構成は、Illegal Viewサーバ1、Illegal Viewクライアント1。

※1サーバで1,000台程度のクライアントを管理できます。

※ Illegal View仮想クライアント数はリモートデスクトップ接続の同時アクセス数。

※ Illegal Viewクライアントが導入した端末に対してリモート接続すれば記録可能。

## 3-1. 製品体系 (2/3)

### ② オプション (参考)

ライセンス	説明
ビデオExport	記録画像をAVI形式に変換・出力する機能です。 一般のメディアプレーヤーで再生可能となります。
連続アラーム	アラーム条件の組み合わせが連続的に発生したことを検知・制御できるオプションです。
レポート	履歴やアラームのテキスト系ログをCSV形式やPDF形式でのエクスポートおよび出力日時を指定できます。



## 3-1. 製品体系 (3/3)

### ③ 初期インストール作業支援・保守

項目	価格
初期インストール作業支援	個別見積
年間保守	ご購入ライセンス (基本・オプション) 標準価格の20%

- ※ 保守は初年度から必要です。  
保守内容にはメールによるお問い合わせ、および、製品のバージョンアップを含みます。  
(保守契約の締結が無い場合、バージョンアップには別途新規にライセンス費用が発生します。)  
バージョンアップに関わるSE作業は個別見積りとなります。

---

## 4 .最後に

### 録画ソフト導入検討にあたり

録画ソフト導入検討にあたり、他社製品と以下のポイントに注目して比較頂けると幸いです。

#### 1 様々なログと動画が連動したピンポイント再生

多くの類似製品と違い、テキスト型、動画型のそれぞれメリットを有しており、ログと動画の連動によるピンポイント再生が可能ですので、見たい情報を簡単に検索でき、対象の操作を完全に再現することができます。

#### 2 「データ容量」

録画ソフトとして、最も重視されるのは「データ容量」です。  
(データ容量が大きい場合、ハードディスクの増設に加え、PC負荷、ネットワークトラフィックにも影響を及ぼします。)

セキュリティ対策は「**永続的に実施するもの**」という観点でご検討をお願いします。

---

## 5. ご参考資料

- 5. 1 事例紹介
- 5. 2 補足

### 導入目的

外部委託するサーバメンテナンスの安全確保のため、現地における作業および監視員による作業監視を義務付けられていたが、オンラインメンテナンスを導入することにより、監視員の撤廃および迅速な改修作業によるコスト削減を実現する。

### 採用理由

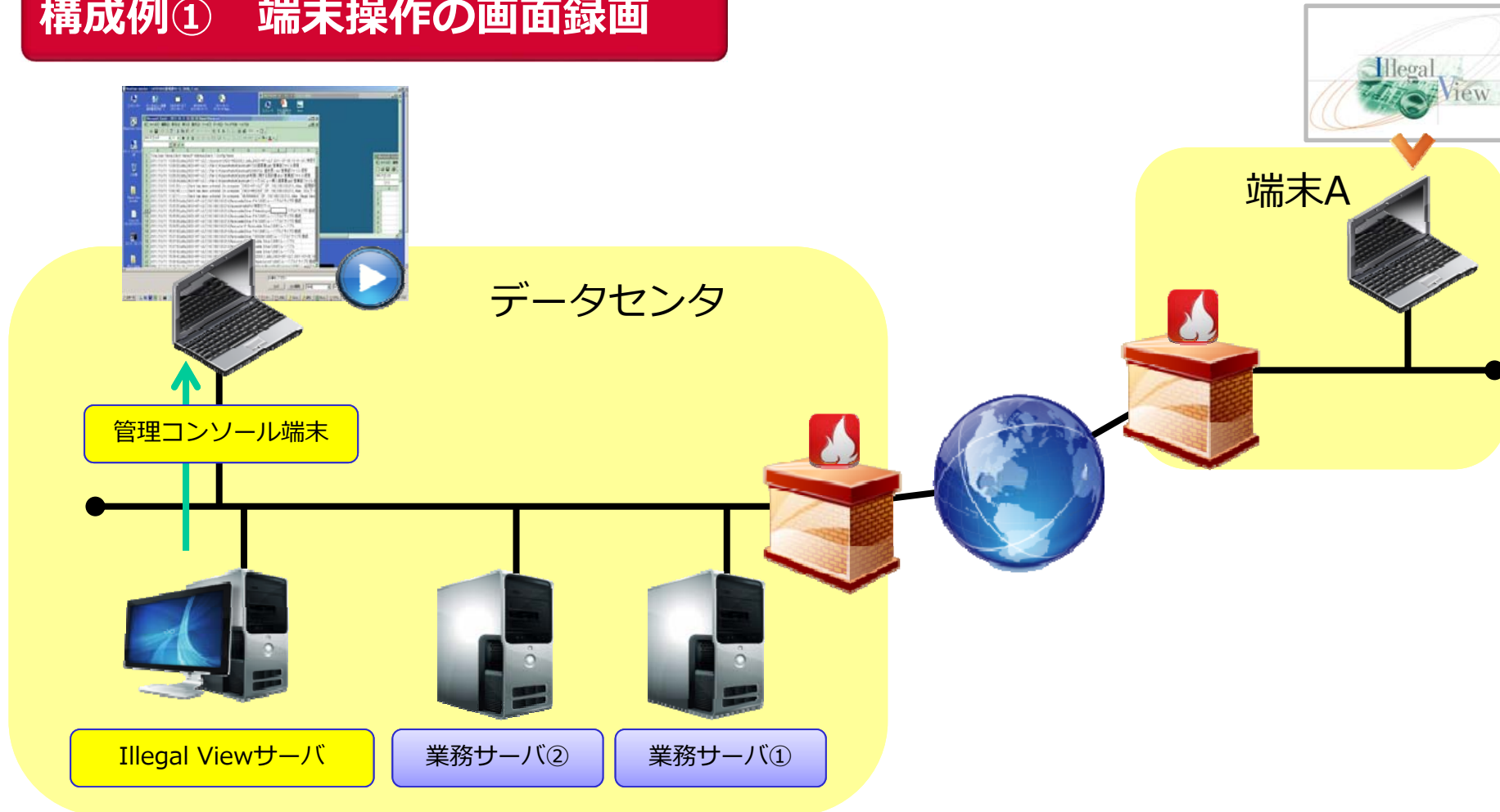
作業内容が画像によって記録できるので安全。  
リアルタイムで監視しながら、必要に応じて、作業を強制的に中断、中止も可能。  
将来的にクライアントのメンテナンスへの拡大も視野に入れているが、接続台数が1,000台程度となっても問題ない。

### 導入効果

監視員は通常業務の傍ら、作業をリアルタイムに監視することができるようになった。  
作業内容が記録されているので、意味不明な操作に対するクレームを証拠（操作内容画像）と共に提示できるようになった。  
メンテナンス時間が短くなったことで、メンテナンス価格の引き下げに成功した。

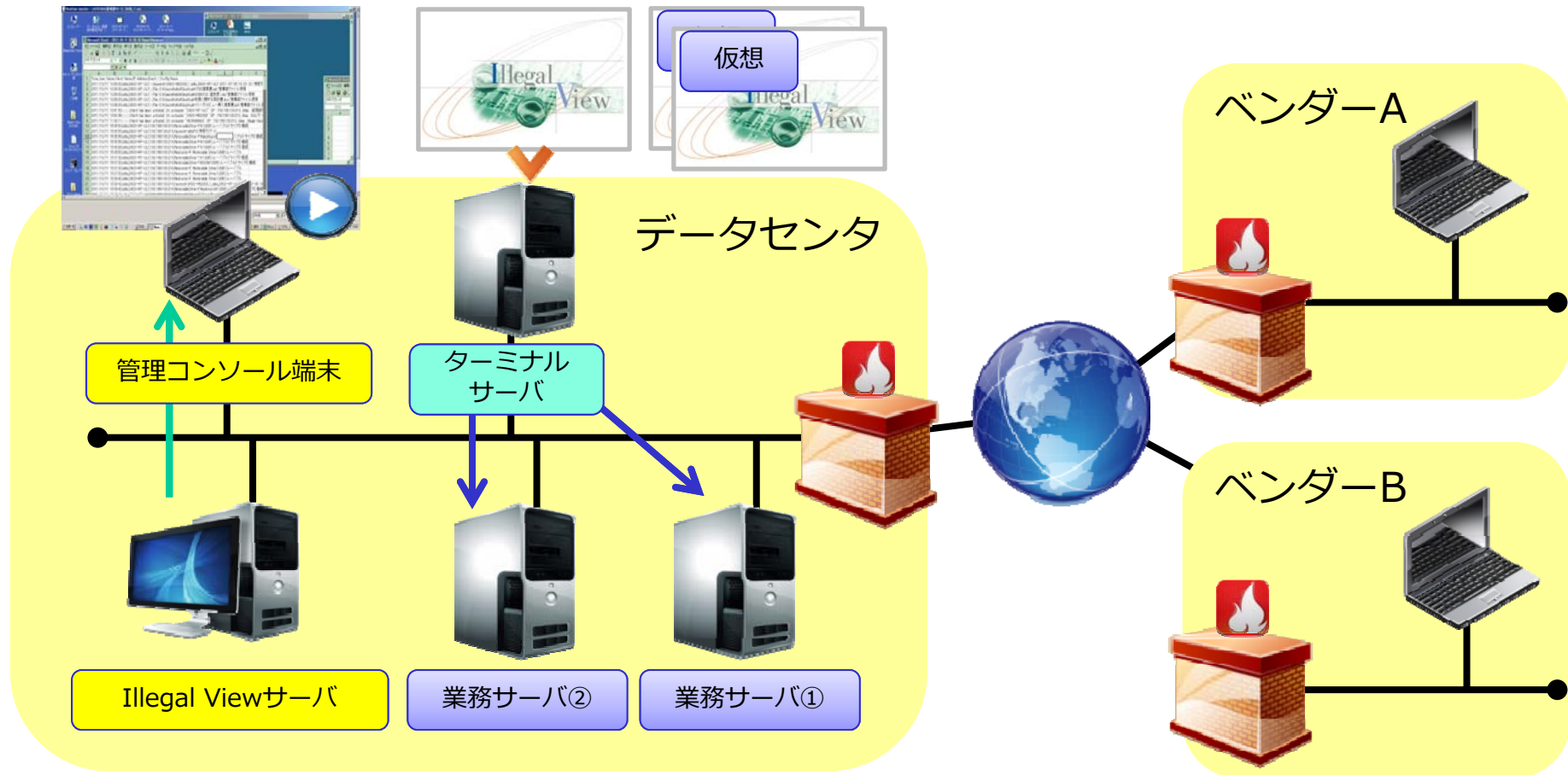
# 5-1. 事例紹介① (サーバ保守作業証跡管理)

## 構成例① 端末操作の画面録画



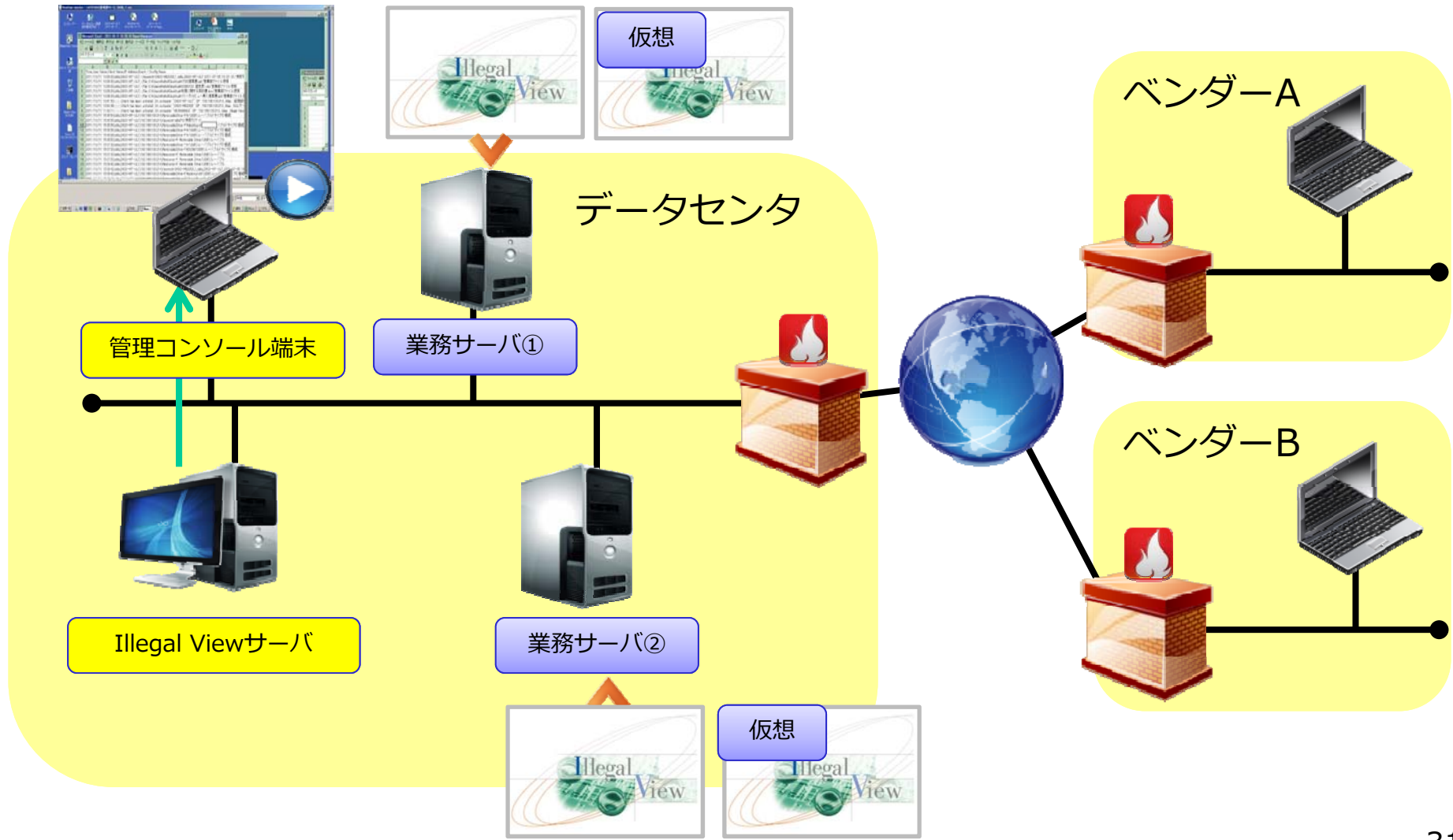
# 5-1. 事例紹介① (サーバ保守作業証跡管理)

## 構成例② ターミナルサーバ経由の画面録画



# 5-1. 事例紹介① (サーバ保守作業証跡管理)

## 構成例③ 業務サーバ操作の画面録画





## 5-1. 事例紹介② (顧客情報漏えい対策)

### 導入目的

転職・部署移動する社員が極めて多くかつ頻繁であるため、  
故意・無意識に関わらず顧客情報を持ち出す可能性を抑止する。

### 採用理由

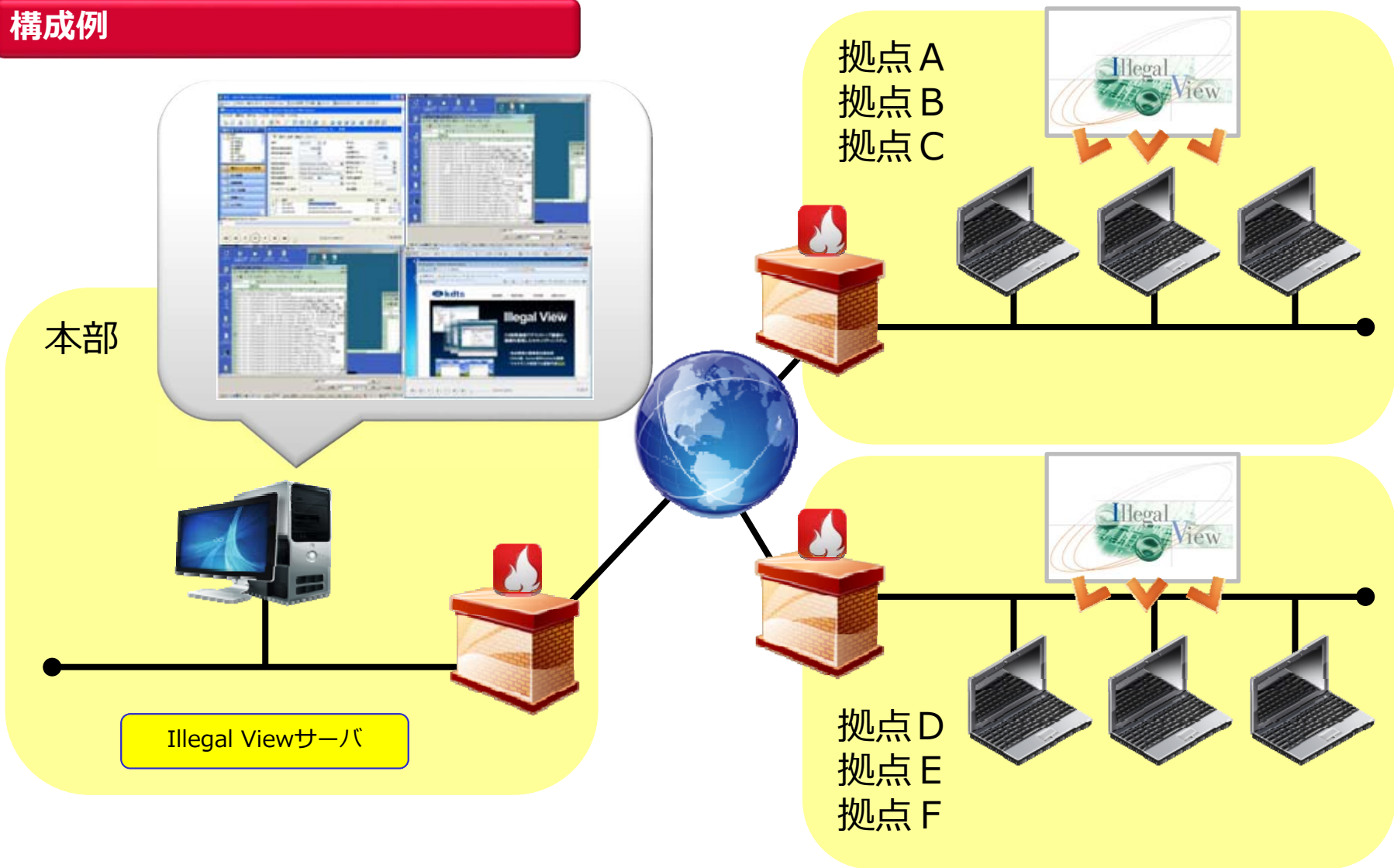
6500台の端末から監視対象端末をリアルタイムに指定(現在500台)し、操作画面を記録可能。  
監視対象端末に、「操作画面を記録中」という表示する事で、抑止効果が図れる。

### 導入効果

- 社員に端末操作を全て常時録画していることを周知する事により抑止効果が向上している。
- 内部不正など重大な問題が生じた場合に、詳細な操作証跡を警察などの機関に提供する事も可能になった。
- 頻繁な異動を想定して、あらかじめ全端末に対策を施して準備しておく方式により、適正な投資と円滑な端末切り替え作業が可能になる。

# 5-1. 事例紹介② (顧客情報漏えい対策)

## 構成例



### 導入目的

スーパーバイザー 1 人あたりが管理するオペレータ人数を引き上げる。  
オペレーションミスの申告があった場合にその原因を簡単に確認できるようにする。  
ベテランオペレータの操作録画を新人オペレータ教育に利用する。  
属人的な評価を廃止して、平等なオペレータ評価基準を策定する。

### 採用理由

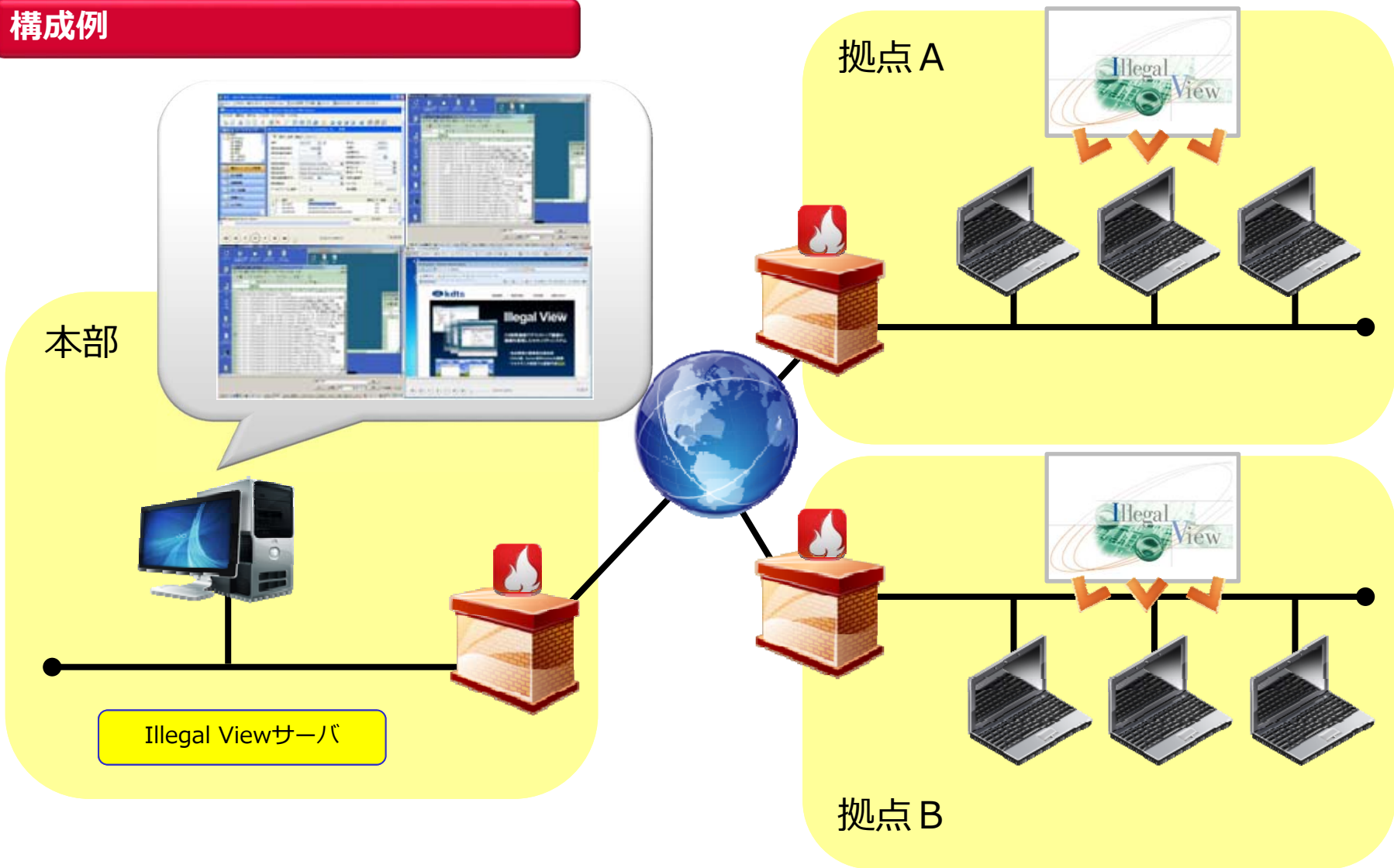
リーダーがリアルタイムにオペレータの操作を手元で確認可能。  
管理サーバ1台あたりで1,000台単位のPCを管理可能。  
データサイズが小さいため、長期間のデータ保存でも記録システムへの負荷が低い。

### 導入効果

- リアルタイムモニター機能によりオペレータの作業モニター化で、スーパーバイザー1人あたりのオペレータ管理人数を従来の**10名から20名に拡大**成功。
- 記録画像による新人オペレータ教育の効率化が図れた。
- 評価基準策定によるオペレータの本当の実力判断をおこなえるようになった。
- リーダーがオペレータの対応を簡単に確認できるようになったことでクレーム対策がタイムリーかつ容易になった。

# 5-1. 事例紹介③ (コールセンターオペレータ品質向上)

## 構成例



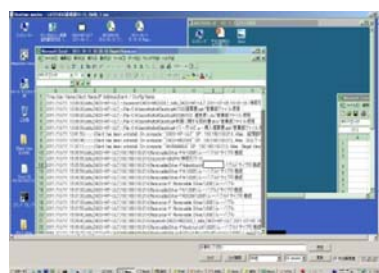
## 5-2. 補足（リアルタイムモニタ）

### “今”おこなわれている操作を把握

現在のデスクトップの様子をリアルタイムに表示します。  
表示色はPCの設定色、フルカラー～モノクロよりお選びいただけます。  
表示間隔は0.5秒、1秒、2秒、3秒、4秒、5秒よりお選びいただけます。  
表示条件を変更すると、録画の記録条件も合わせて変更されます。  
画面をロック、逆にロックを解除することができます。  
リモートデスクトップの画像も表示することができます。

今現在おこなわれている操作をモニタリングできるため、重要な作業  
に対してのリモートクロス確認や、危険な操作実施者の操作をロックする  
といった制御も可能です。

リモート作業確認  
画面のロック・解除  
メッセージ送信



管理コンソール

操作画面転送

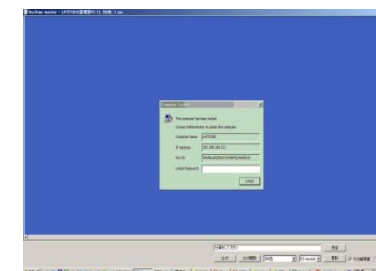


メッセージ送信、ロック指示

Illegal Viewサーバ



操作画面



ロック画面

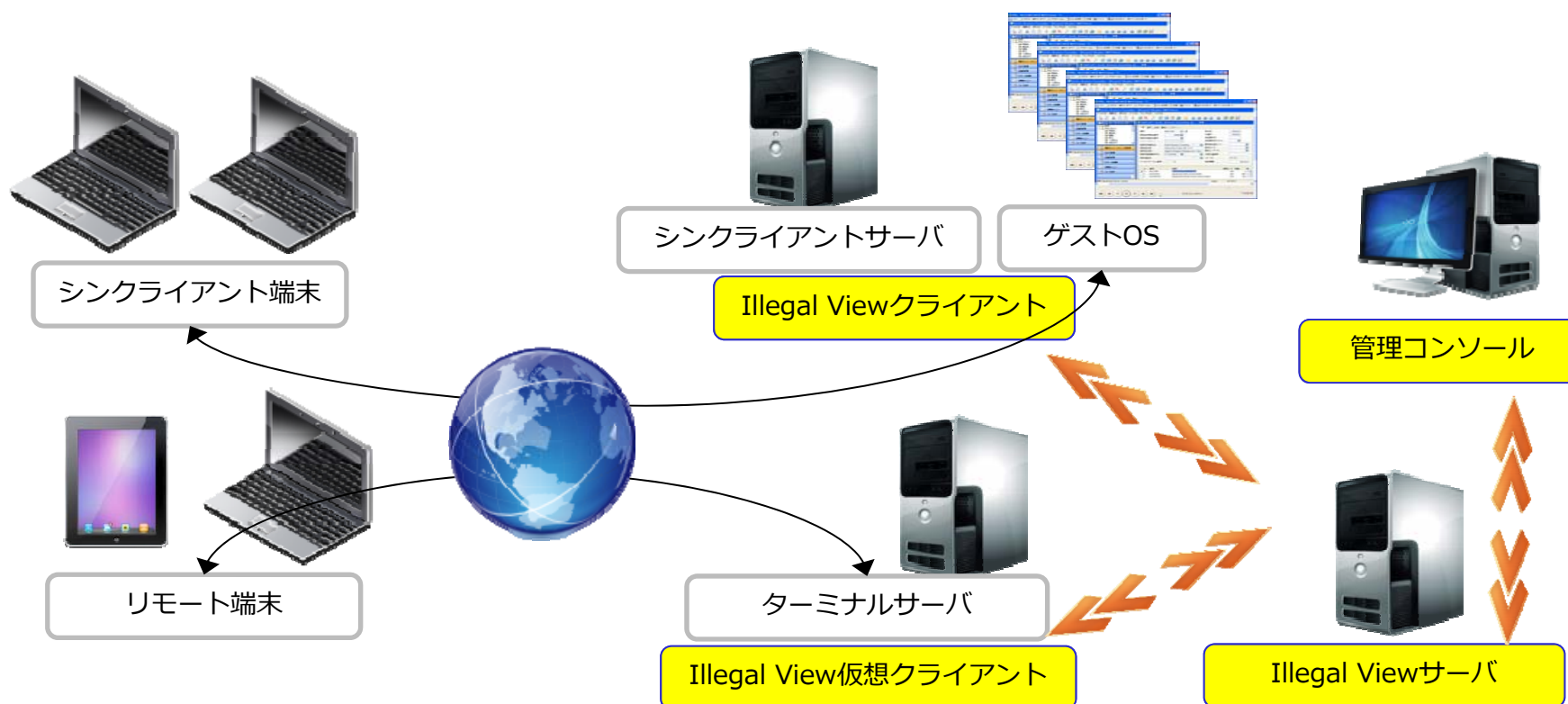
Illegal Viewクライアント

## 5-2. 補足（仮想環境録画）

### 仮想環境やリモート接続の証跡も

仮想環境にも対応しています。  
RDSやシンクライアント環境の仮想接続操作も録画できます。

ターミナルサービス  
RDP(マイクロソフト)  
VMware  
XenApp



## 5-2. 補足 (セキュリティ)

### 暗号化されたデータ通信

Illegal ViewサーバとIllegal Viewクライアント間の通信は暗号化されており、パケットスニファリング等によるパケット盗聴を防ぐことができます。

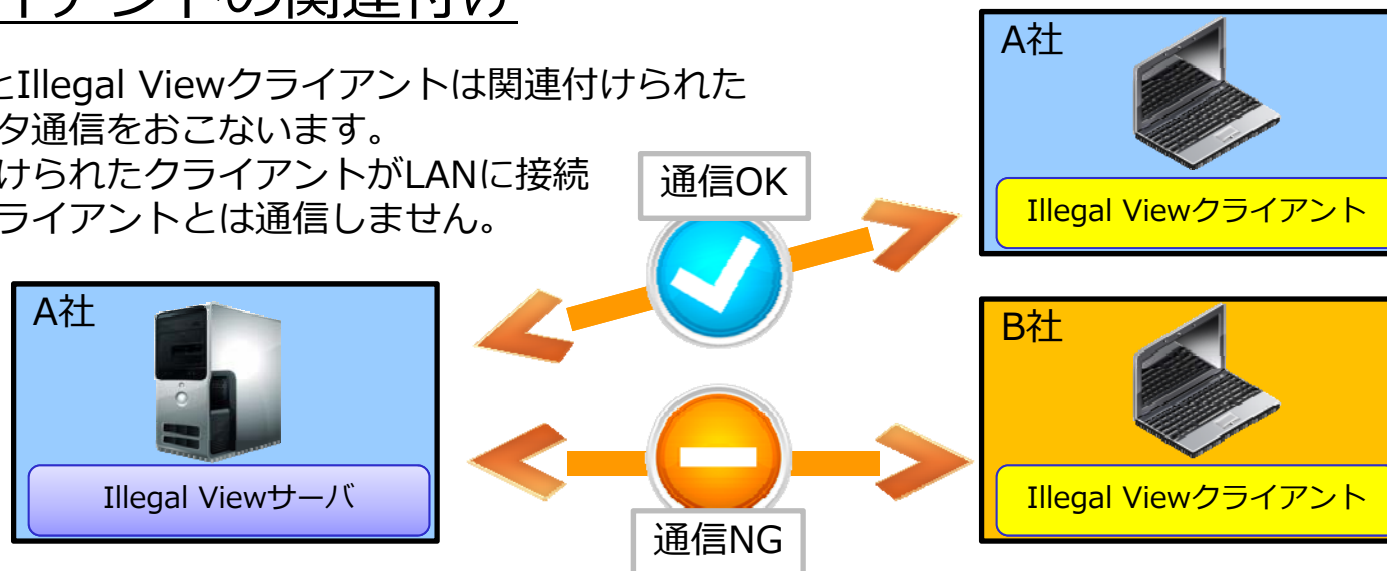
通信暗号化  
S/C関連付け



※インターネット間での通信をおこなう場合はVPN等の利用を推奨いたします。

### サーバとクライアントの関連付け

Illegal ViewサーバとIllegal Viewクライアントは関連付けられた関係下のみで、データ通信をおこないます。別のサーバと関連付けられたクライアントがLANに接続された場合、そのクライアントとは通信しません。



## 5-2. 補足（システム無効化対策）

### 情報漏洩の防止

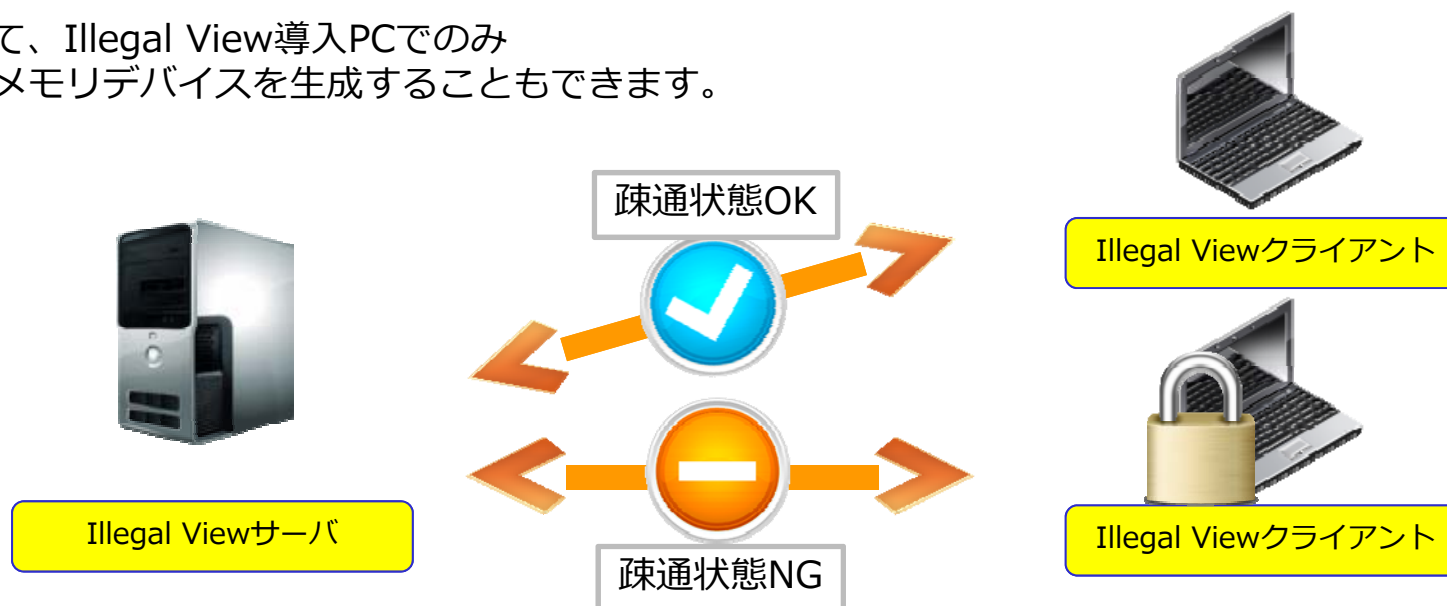
Illegal ViewクライアントがIllegal Viewサーバと疎通できない場合にWindowsの起動/PCの利用を停止することができます。

オブザーバ機能  
ステルス機能  
ファイアウォール対策

クライアント側PCのタスクマネージャーにIllegal Viewプログラムは表示されず、ユーザはプログラムを停止させることはできません。また、プログラムファイルも非表示となっており、管理者権限を駆使してもサービスを停止することができません。

OA用のPCにこの設定を加えることで、盗難や紛失といったトラブルの発生時に情報漏洩を防ぐことができます。

オプションとして、Illegal View導入PCでのみ利用可能なUSBメモリデバイスを生成することもできます。





# 他社商品名、商標等の引用に関する表示

- イリーガルビュー、Illegal Viewは、株式会社ケイディティエスの登録商標です。
- HITACHI、およびJP1は、株式会社日立製作所の商標または登録商標です。
- Microsoftは、米国およびその他の国における米国Microsoft Corp.の登録商標です。
- Windowsは、米国およびその他の国における米国Microsoft Corp.の登録商標です。
- Windows Serverは、米国およびその他の国における米国Microsoft Corp.の商標です。
  
- その他記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。