Secure ICT Gatewayシステム

脱VPNを実現するシステムです

「プライベートネットにもアクセスできる新時代のL4,L7セキュアゲートウェイ」

「情報セキュリティ規定から実現されるインシデント管理とセキュリティ検査」

それらを「高度な認証、高度なACL、アクセスログ」を有したクラウド基盤

なぜSecure ICT Gatewayが必要なのか？

それはセキュリティに有益な製品であるだけでなく、

社員全員をもセキュリティに強みを持った人材にするからです。

現在のセキュリティ情勢

コロナウィルス対策でテレワーク導入が増え、それを狙う攻撃が多発

- 情報セキュリティ事故のうち「テレワーク等のニューノーマルな働き方を狙った攻撃」が組織部門の3位にランクイン　（2020年IPA調べ）

個人情報保護による情報漏洩などへの制裁の世界的強化

- 2021年のGDPRによる制裁件数は400件超（セキュリティの取組み不備でもペナルティ）
  - NTTデータ（2022/11）顧客情報漏洩で 940万円の制裁金　：　日本企業初適用
  - Google 個人情報の利用目的のユーザへの提示不備などで 62億円の制裁金
  - 米アマゾン・ドット・コムは、消費者に対する広告表示がGDPR違反で 970億円の制裁金

  その他多数
- 情報漏洩だけでなく、セキュリティへの取り組み不備で制裁金が課されます
- 日本版GDPR/CCPA 個人情報保護法も欧米に倣って厳格化方向

セキュリティへの取り組み強化は社会的義務。企業存続の必須条件に。

情報漏洩による損出が、「社会的制裁」に加え「巨額制裁金」まで

企業が取り組むべきセキュリティ施策

情報セキュリティは、３つの要素と3つの脅威があります

- 3要素：機密性(Confidentiality)、完全性(Integrity)、可用性(Availability)
- 3脅威：物理的脅威、技術的脅威、人的脅威

3要素の実現には様々な施策や製品がありますが、それらは完全なものではありません

- それらを使うのが人だからです。 人的脅威
- セキュリティ製品も進化するマルウェアに対して完全な防御にはなり得ません。 技術的脅威

「人的脅威」と「技術的脅威」、「物理的脅威」はセットでの取り組みが必須

技術的脅威　：製品が完全ではない事例の一部を紹介

- ウィルスチェック製品は、どこかで発生した情報を元にして同じウィルスの発生を検知するもの。
  → 初めてのウィルスや、発生情報を元にするまでの期間には、全く意味がありません。これがゼロディ攻撃です。
- WEBサイトの改ざんによる不正サイトアクセス
  → 信頼のおける安全なサイトでも、そのサイトが改ざんされ、不正サイトへ転送されることがあります。
- 標的型攻撃
  → 存在する人を装って特定の人を狙い撃ちしてメールなど送り付け、不正サイトアクセスさせる手法です。
  見抜ける？と思うかもしれませんが、「ラテラルフィッシング」などは専門家でも見抜くことは困難です

Secure ICT Gateway(SIG)が開発された背景

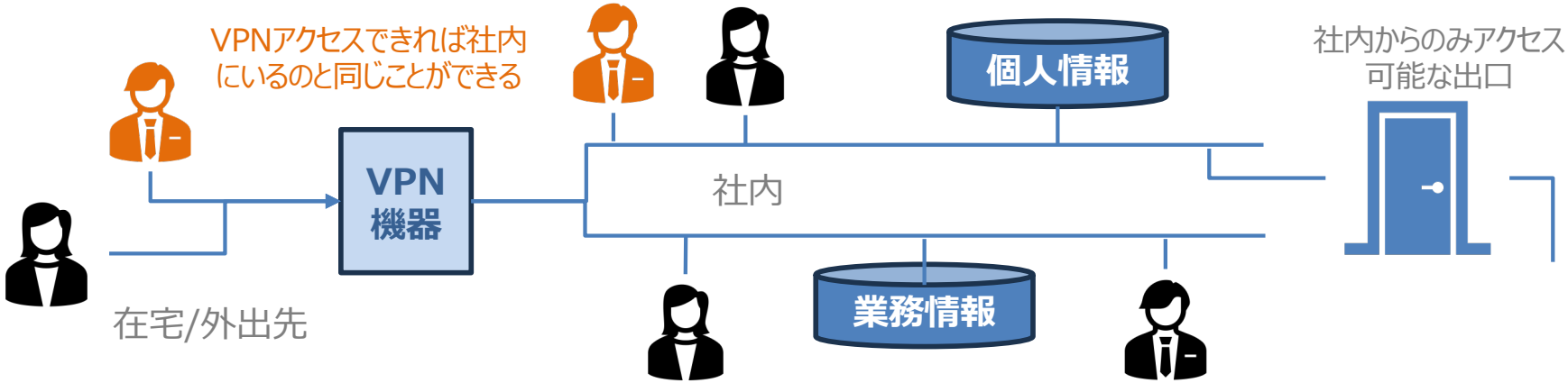
テレワーク環境で利用されるVPNが狙われている

- 2020年8月、米パルスセキュア社製VPN装置の脆弱性を利用した不正アクセスが発生し、国内外900社、国内大手企業38社が被害を受けました。
- 2021年10月、米Fortinet社製VPN装置の脆弱性を利用した不正アクセスが発生し、徳島県のつるぎ町立半田病院で電子カルテ一切が利用できなくなりました。

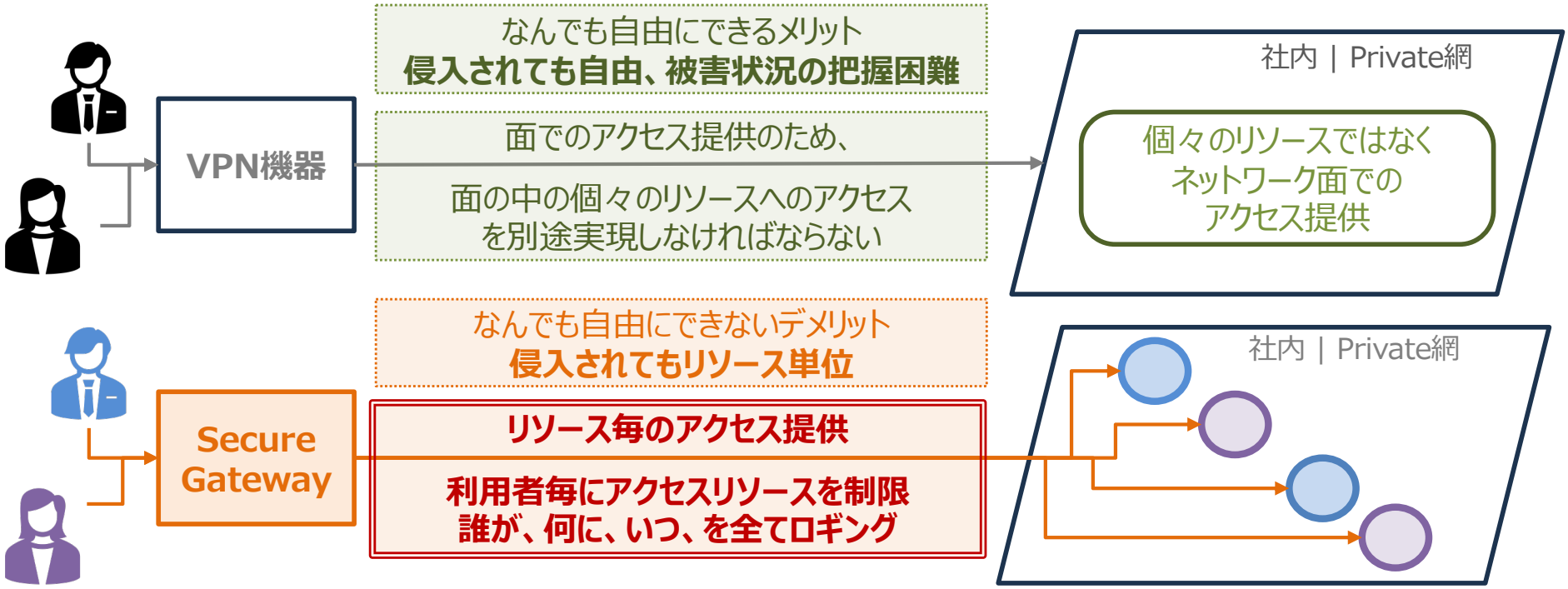
なぜVPNが狙われるのか？

VPNを日本語にすれば仮想私設網。つまりこの網に侵入できてしまえば、あとは**社内で作業しているのと同じことが全て、無制限にできてしまう**からです。

侵入による犯罪リスクに対して、リターンが極めて大きいからなのです



Secure ICT Gateway(SIG)が実現する脱VPN



なんでもできる利便性　<<　利用者・リソース毎のアクセス制限

SIGの導入により、社員がアクセスできる情報やシステムの整理も併せて実現

□ VPNでないと操作が困難な作業は？

- SIGは、sshでのterminal操作が可能な通信路を提供できるので問題なし。
- クラサバ・システムも TCP(L4)レベルでの通信路を提供できるので問題なし。

SecureGateway(SIG)による人的脅威の解消

SIGといえど、利用者が標的型攻撃などでマルウェア感染してしまえば、当該利用者に付与された権限の範囲で情報漏洩する可能性はあります

定常的なセキュリティ運用・教育が必要

SIG

適切なインシデント管理で被害を最小限に

情報セキュリティ規定、情報セキュリティ対策基準　の提供
（そのまま利用可能ですが、会社の運用に合わせた微調整なども可能）

セキュリティ検査機能の提供

・社員へのセキュリティ小テストを随時実施
※問題をセキュリティ管理者が作成可能
・社員へのセキュリティ調査の実施

インシデント時の対処フロー提供

・システム利用によって発生から解決までの一連の処理フローが実現可能
※システムに従えばすべき対処行動に間違い、抜けなし
・全てのインシデント情報を紛失なく保存

付録：Secure ICT Gateayシステムの現機能一覧

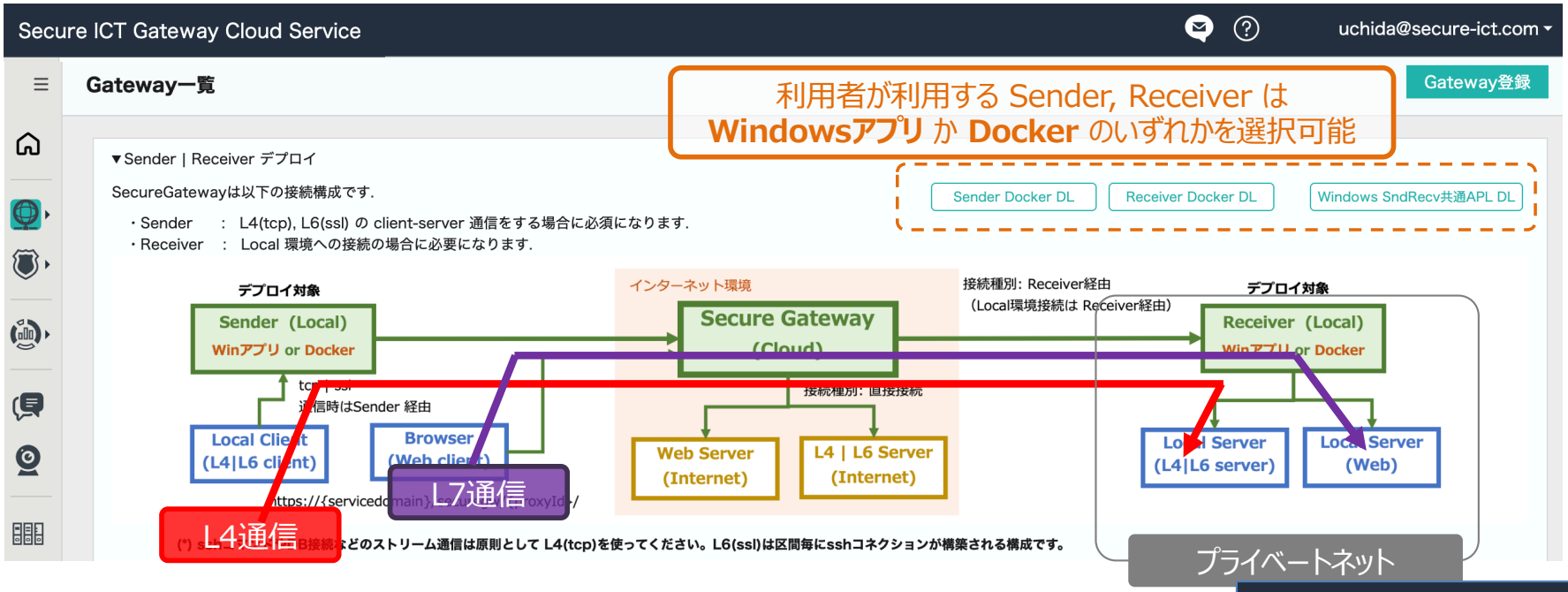
- **Secure Gateway機能**
  - L4のセキュリティ・ゲートウェイ機能（提供する sender, receiver docker の配備要: DL可能）
  - L7のセキュリティ・ゲートウェイ機能（privateネットへの接続では receiver docker の配備要: DL可能）
  - ACLグループによる接続制限
- **CSIRT機能**
  - インシデント管理（インシデント発生から完了までのフロー制御）
  - セキュリティ検査（全社員への選択テスト型の検査と解析）
  - 規定書類の提供（情報セキュリティ規定書、情報セキュリティ対策基準）
- **データ収集・分析機能**
  - 原因分析 (現在は Ridge, Lassoの回帰分析のみ)
  - 名寄せ解析(RecordLinkage(phonetic含む) + Kakashi + 独自データ加工)
  - データセット管理 (csv, parquet, rdb(mysql, postgres)　利用可能DB拡張は容易だが今すべきことでは。。。)
  - 秘匿分散(MPC)によるデータ収集と秘匿分析 (sum,mean,var,stdev,correl)
- **チャット機能、ビデオ会議機能**
  - チャットが可能
  - 数十人が参加可能(SFU方式)なビデオチャット機能 (録画機能については現在実装中)
- **タスク管理機能**
  - Kanban機能　(Gantの実装は検討中：メイン機能ではなくこの機能の充実の価値に疑問)
- **動画・画像管理機能**
  - 動画・画像のアップロードや、システム画面からの撮影動画・画像を保存できる機能　（何かあったらすぐ撮影・保存）
- **基本機能**
  - OTPによる2段階認証 (アクセストークンによるOTP認証回避も可能)
  - アカウント管理機能
  - アクセスログ機能
  - ACL機能（機能別アクセス制限、SecureGateway接続先制限）
  - シングルサインオン (SP機能)

セキュリティ・メイン機能

セキュリティ運用支援機能

セキュリティ・利用機能

Secure ICT Gateway機能



ブラウザからのHTTP/HTTPS通信は**Secure ICT Gatewayの認証下でのみ利用可能**
※Secure ICT Gateway専用のアクセスログに通信が記録されます

Raw TCP/IP 通信では、Senderを配置し、Senderに**Secure ICT Gatewayアカウントのアクセストークン**を設定することで、認証とACL適用を実現します。

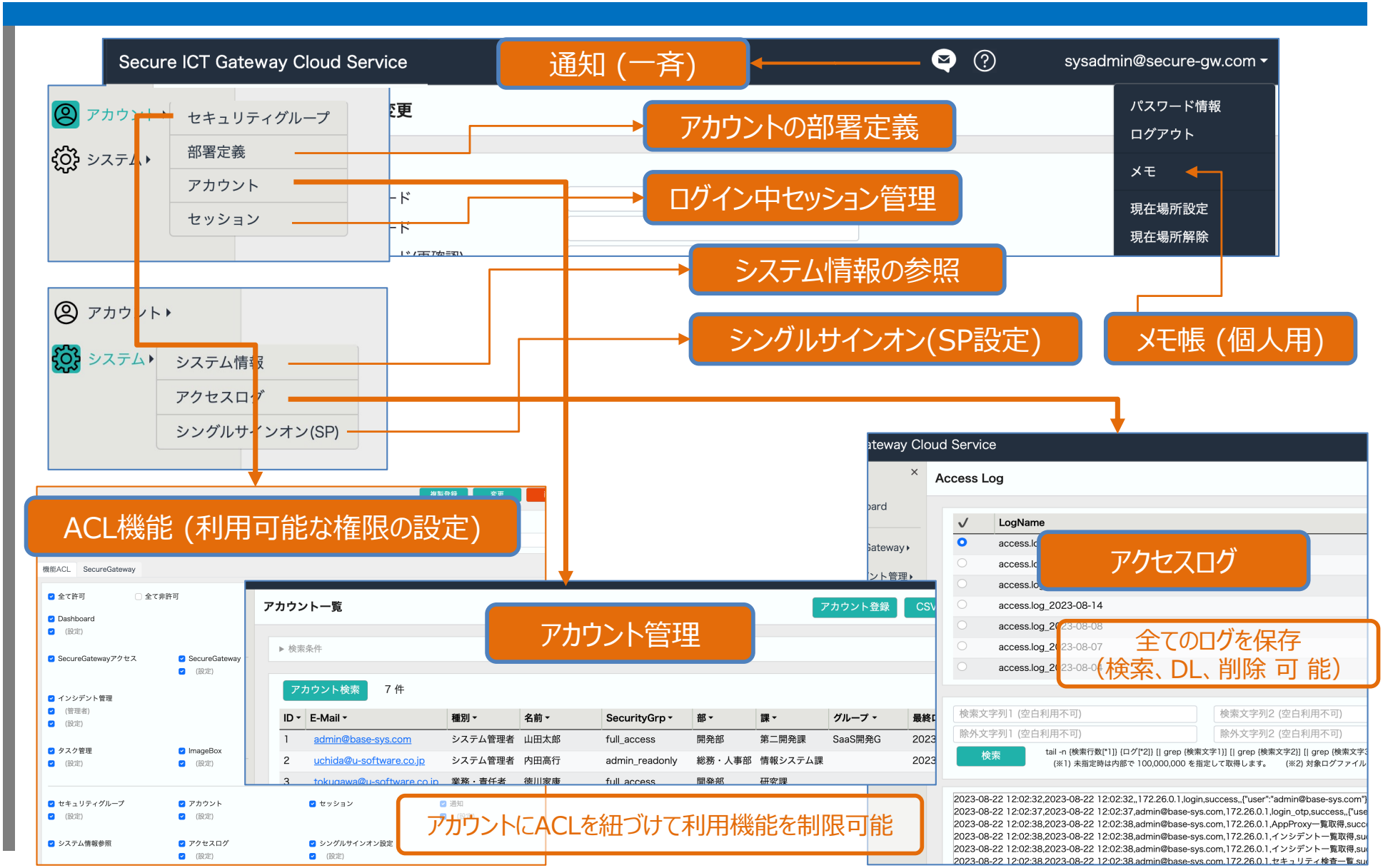
SSL通信は透過転送ではないため、Senderにて一旦終端します。そのため、クライアントアプリからの宛先はSenderとなります。これに付随してSenderではSSLプライベート証明書を使います。

※SecureGateway専用のアクセスログに通信が記録されます

CSIRT機能

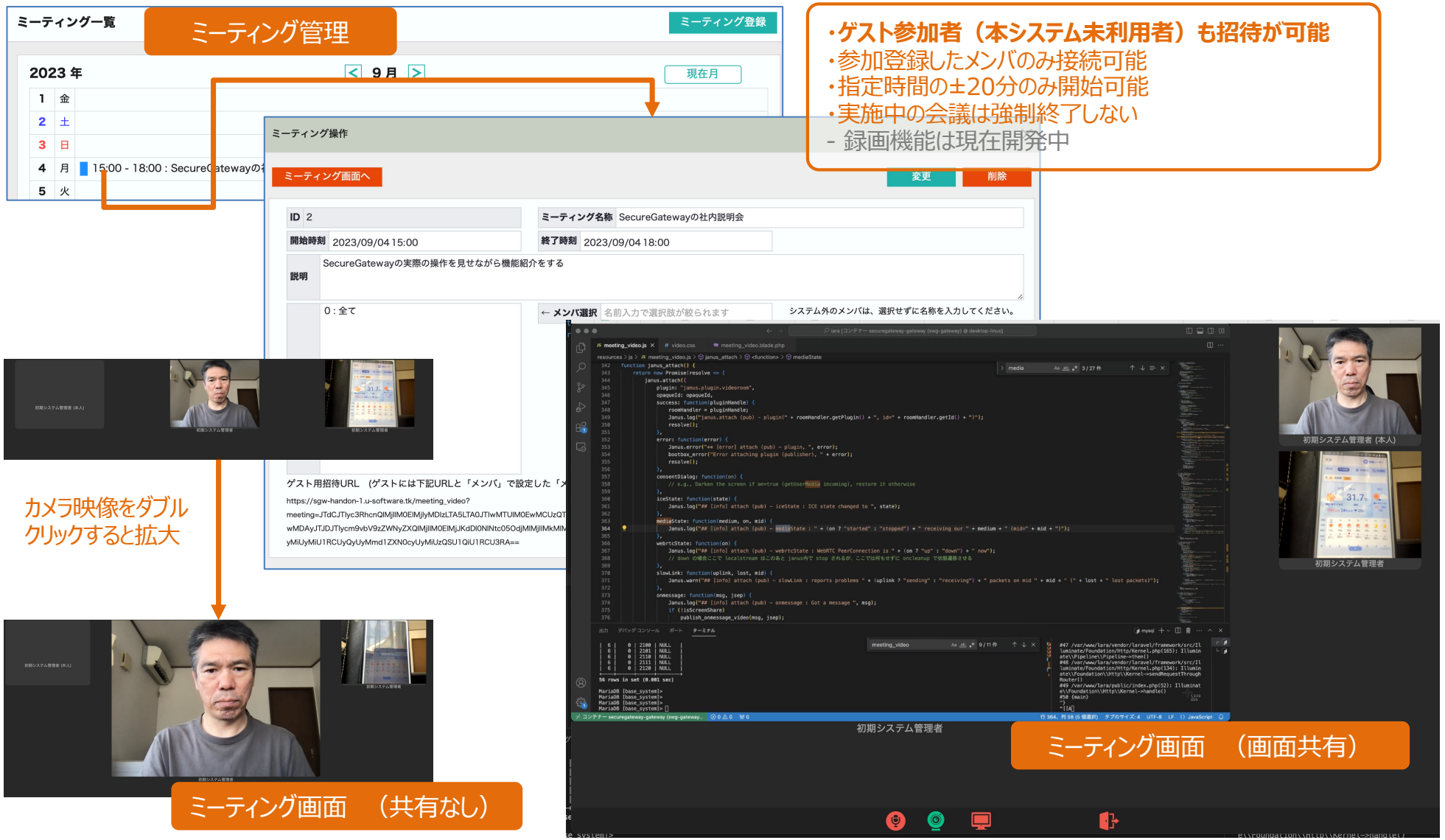

Secure ICT Gateway Cloud Service
インシデント報告
Dashboard
インシデント管理
分析
Task管理
ImageBox
マップ
アカウント
システム
インシデント発生報告
報告後の経緯・対応
再発防止策
再発防止策(承認)
社内・社外への対応など
報告書を参照しながらすべき対応がわかります
インシデント種別
ウィルス感染（WEB閲覧）
保護状態
パスワード保護
件数
Secure ICT Gateway Cloud Service
sysadmin@secure-gw.
セキュリティ検査
複製登録
編集キャンセル
編集保存
削除
SecureGateway
ID
検査名称
サンプル）情報セキュリティ定期検査
検査内容
情報セキュリティの定期検査のサンプル。全問正解するまで完了になりません。
検査完了日
2023/10/31
種別
テスト(合格必須)
合格点数
100
状態
作成中
検査中
完了
設問数
10
設問1
回答選択
複数選択可
回答個数
5
設問文言
PCや利用システムのパスワードに関して間違っているものを選びなさい
選択1
自分しか知らないで単語の組み合わせなら使って良い
選択3
一定の長さがあればアルファベットのみでよい
選択5
パスワード入力はブラインドタッチ等で迅速に入力すべきである
参照
DL(PDF)
置き換え
セキュリティ検査問題の作成
作成問題で試験
未完了者検索等
SecureGateway Cloud Service
セキュリティ規定
・情報セキュリティ規定書
・情報セキュリティ対策基準
情報セキュリティ規定
インシデント管理や検査は「規定書」に規定されています。

基本機能


Secure ICT Gateway Cloud Service
通知 (一斉)
sysadmin@secure-gw.com
パスワード情報
ログアウト
メモ
現在場所設定
現在場所解除
アカウント
システム
セキュリティグループ
部署定義
アカウント
セッション
アカウントの部署定義
ログイン中セッション管理
システム情報の参照
シングルサインオン(SP設定)
メモ帳 (個人用)
システム情報
アクセスログ
シングルサインオン(SP)
ACL機能 (利用可能な権限の設定)
Access Log
LogName
access.log_2023-08-14
アクセスログ
全てのログを保存
(検索、DL、削除 可 能)
アカウント一覧
アカウント登録
アカウント検索
7 件
ID
E-Mail
種別
名前
SecurityGrp
部
課
グループ
admin@base-sys.com
システム管理者
山田太郎
full_access
開発部
第二開発課
SaaS開発G
uchida@u-software.co.jp
内田高行
admin_readonly
総務・人事部
情報システム課
アカウント管理
アカウントにACLを紐づけて利用機能を制限可能

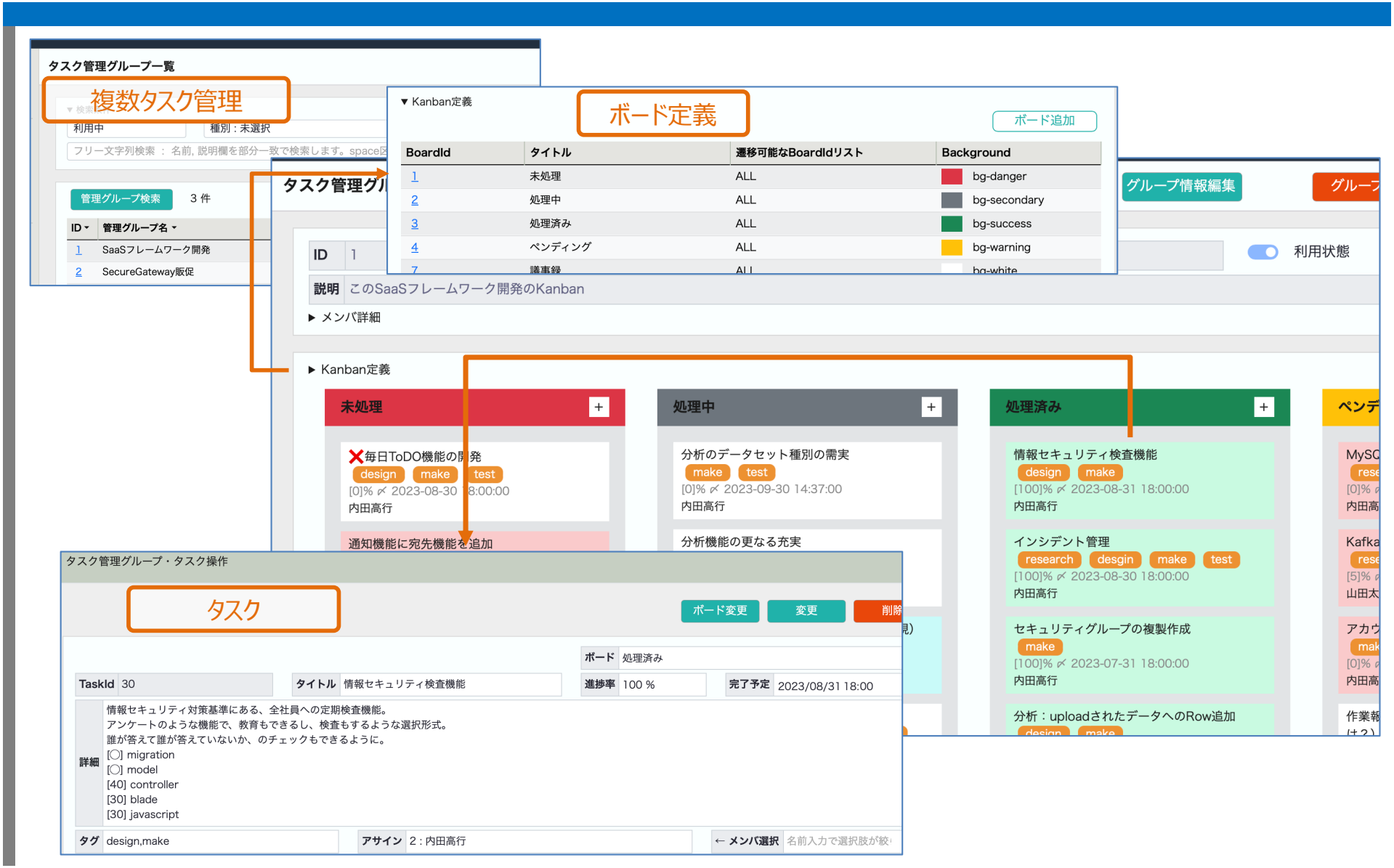
ビデオ会議機能

janus-gateway のクライアント開発したビデオチャット
(slackも利用しているビデオチャットのOSS)

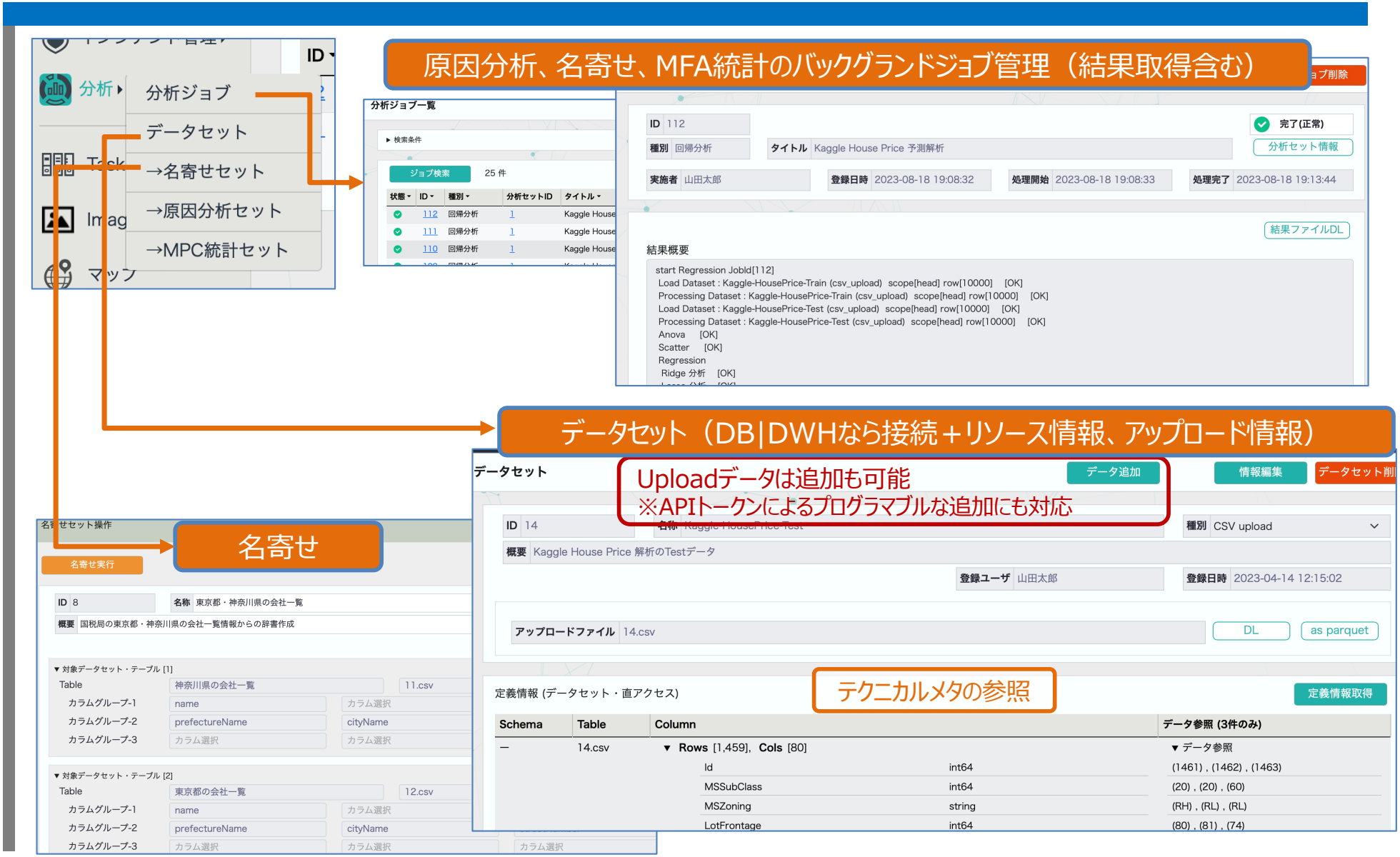


- **ゲスト参加者（本システム未利用者）も招待が可能**
- 参加登録したメンバのみ接続可能
- 指定時間の±20分のみ開始可能
- 実施中の会議は強制終了しない
- 録画機能は現在開発中

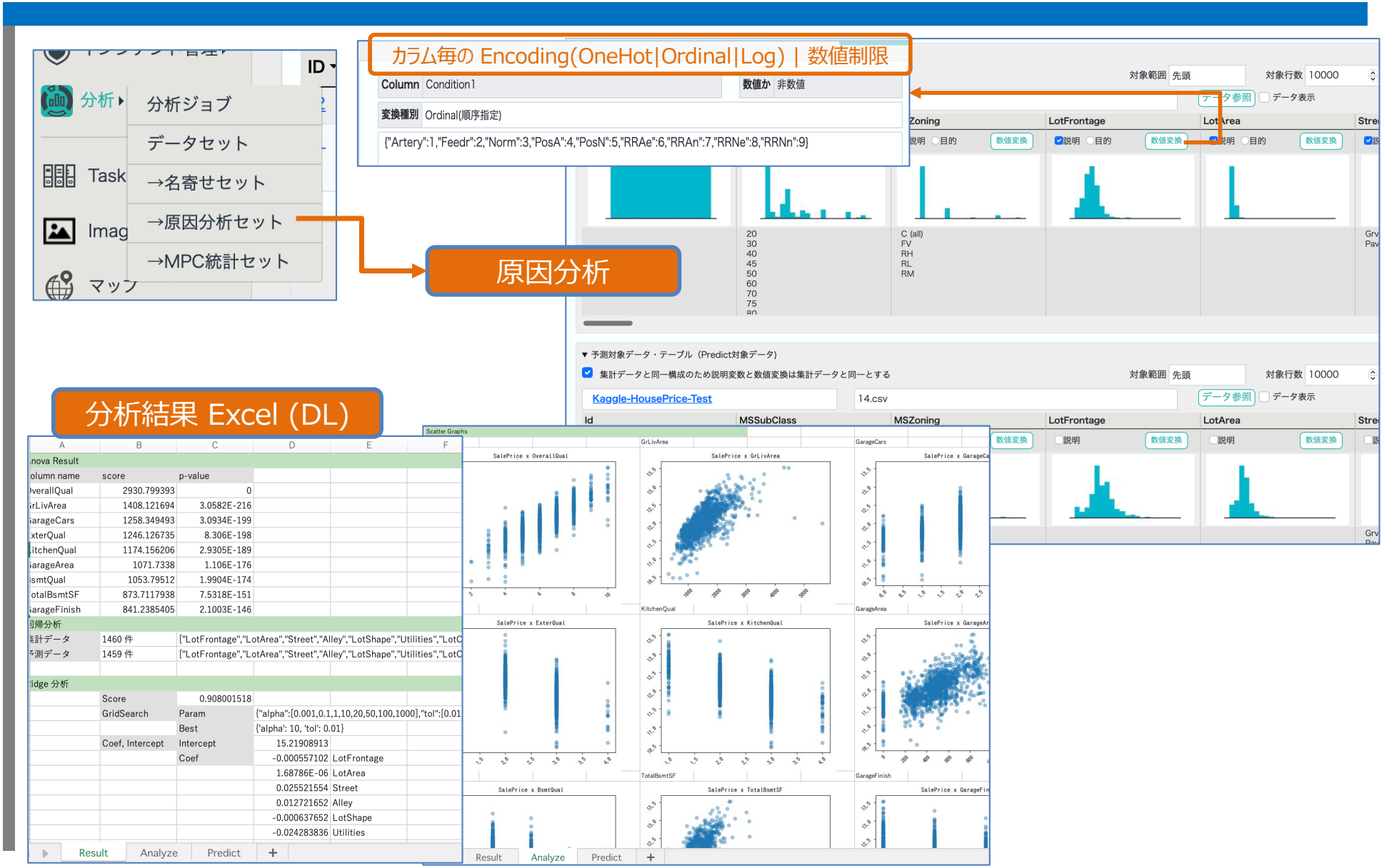
タスク管理機能


タスク管理グループ一覧
複数タスク管理
管理グループ検索
3 件
ID
管理グループ名
1 SaaSフレームワーク開発
2 SecureGateway販促
▼ Kanban定義
ボード定義
ボード追加
BoardId
タイトル
遷移可能なBoardIdリスト
Background
1 未処理 ALL bg-danger
2 処理中 ALL bg-secondary
3 処理済み ALL bg-success
4 ペンディング ALL bg-warning
グループ情報編集
利用状態
説明 このSaaSフレームワーク開発のKanban
▶ メンバ詳細
▶ Kanban定義
未処理
処理中
処理済み
毎日ToDO機能の開発
design make test
内田高行
通知機能に宛先機能を追加
分析のデータセット種別の需実
make test
2023-09-30 14:37:00
内田高行
分析機能の更なる充実
情報セキュリティ検査機能
design make
2023-08-31 18:00:00
内田高行
インシデント管理
research desgin make test
2023-08-30 18:00:00
内田高行
セキュリティグループの複製作成
make
2023-07-31 18:00:00
内田高行
分析：uploadされたデータへのRow追加
タスク管理グループ・タスク操作
タスク
ボード変更
変更
削除
ボード 処理済み
TaskId 30
タイトル 情報セキュリティ検査機能
進捗率 100 %
完了予定 2023/08/31 18:00
詳細
情報セキュリティ対策基準にある、全社員への定期検査機能。
アンケートのような機能で、教育もできるし、検査もするような選択形式。
誰が答えて誰が答えていないか、のチェックもできるように。
[〇] migration
[〇] model
[40] controller
[30] blade
[30] javascript
タグ design,make
アサイン 2 : 内田高行
← メンバ選択

データ収集・分析機能1


分析
分析ジョブ
データセット
→名寄せセット
→原因分析セット
→MPC統計セット
原因分析、名寄せ、MFA統計のバックグランドジョブ管理（結果取得含む）
分析ジョブ一覧
ジョブ検索
25 件
ID 112
種別 回帰分析
タイトル Kaggle House Price 予測解析
完了(正常)
分析セット情報
実施者 山田太郎
登録日時 2023-08-18 19:08:32
処理開始 2023-08-18 19:08:33
処理完了 2023-08-18 19:13:44
結果ファイルDL
結果概要
start Regression JobId[112]
Load Dataset : Kaggle-HousePrice-Train (csv_upload) scope[head] row[10000] [OK]
Processing Dataset : Kaggle-HousePrice-Train (csv_upload) scope[head] row[10000] [OK]
Load Dataset : Kaggle-HousePrice-Test (csv_upload) scope[head] row[10000] [OK]
Processing Dataset : Kaggle-HousePrice-Test (csv_upload) scope[head] row[10000] [OK]
Anova [OK]
Scatter [OK]
Regression
Ridge 分析 [OK]
データセット（DB|DWHなら接続＋リソース情報、アップロード情報）
Uploadデータは追加も可能
※APIトークンによるプログラマブルな追加にも対応
名寄せ
名寄せ実行
ID 8
名称 東京都・神奈川県の会社一覧
概要 国税局の東京都・神奈川県の会社一覧情報からの辞書作成
データセット
データ追加
情報編集
データセット削
ID 14
種別 CSV upload
概要 Kaggle House Price 解析のTestデータ
登録ユーザ 山田太郎
登録日時 2023-04-14 12:15:02
アップロードファイル 14.csv
DL
as parquet
テクニカルメタの参照
定義情報 (データセット・直アクセス)
定義情報取得
Schema
Table
Column
データ参照 (3件のみ)
14.csv
Rows [1,459], Cols [80]
Id int64 (1461) , (1462) , (1463)
MSSubClass int64 (20) , (20) , (60)
MSZoning string (RH) , (RL) , (RL)
LotFrontage int64 (80) , (81) , (74)

データ収集・分析機能2


分析
分析ジョブ
データセット
→名寄せセット
→原因分析セット
→MPC統計セット
原因分析
カラム毎の Encoding(OneHot|Ordinal|Log) | 数値制限
Column
Condition1
変換種別
Ordinal(順序指定)
{"Artery":1,"Feedr":2,"Norm":3,"PosA":4,"PosN":5,"RRAe":6,"RRAn":7,"RRNe":8,"RRNn":9}
対象範囲
先頭
対象行数
10000
データ参照
データ表示
Zoning
LotFrontage
LotArea
予測対象データ・テーブル（Predict対象データ）
集計データと同一構成のため説明変数と数値変換は集計データと同一とする
Kaggle-HousePrice-Test
14.csv
分析結果 Excel (DL)
Result
Analyze
Predict

データ収集・分析機能3 (MPC)

Multi-Party Computation(MPC)とは

- MPCとは①暗号化して分散されたデータを、②分散されたシステムで暗号化されたまま独立して計算できる秘匿計算(秘密)の技術手法の一つです。

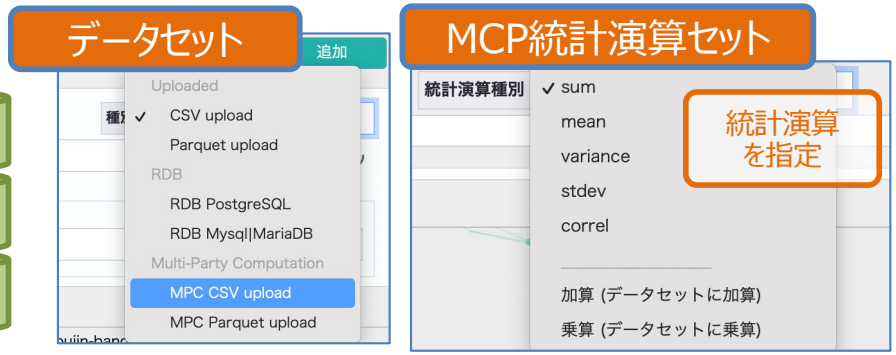
分散暗号化
暗号#1,2,3 は可逆性のある暗号化情報

分散暗号の複合
演算結果を複合することで、Rawデータの演算と同じ結果を得ることができる

技術の特徴

- 分散したそれぞれで暗号化したまま演算することができる
- 暗号化のまま演算できるのに元データ複合するのは、技術利点を損なってしまう。
- 可逆暗号のため、一部の分散情報の漏洩では復元は不能ですが、全て漏洩すると復元できてしまいます。
- 分散ストレージとの差別化
  - 分散ストレージは分散したままでは要をなさず、利用時には元情報を複合する必要があります。元情報を複合時に情報漏洩するリスクがあるのです。

実装イメージ



動画・画像管理機能

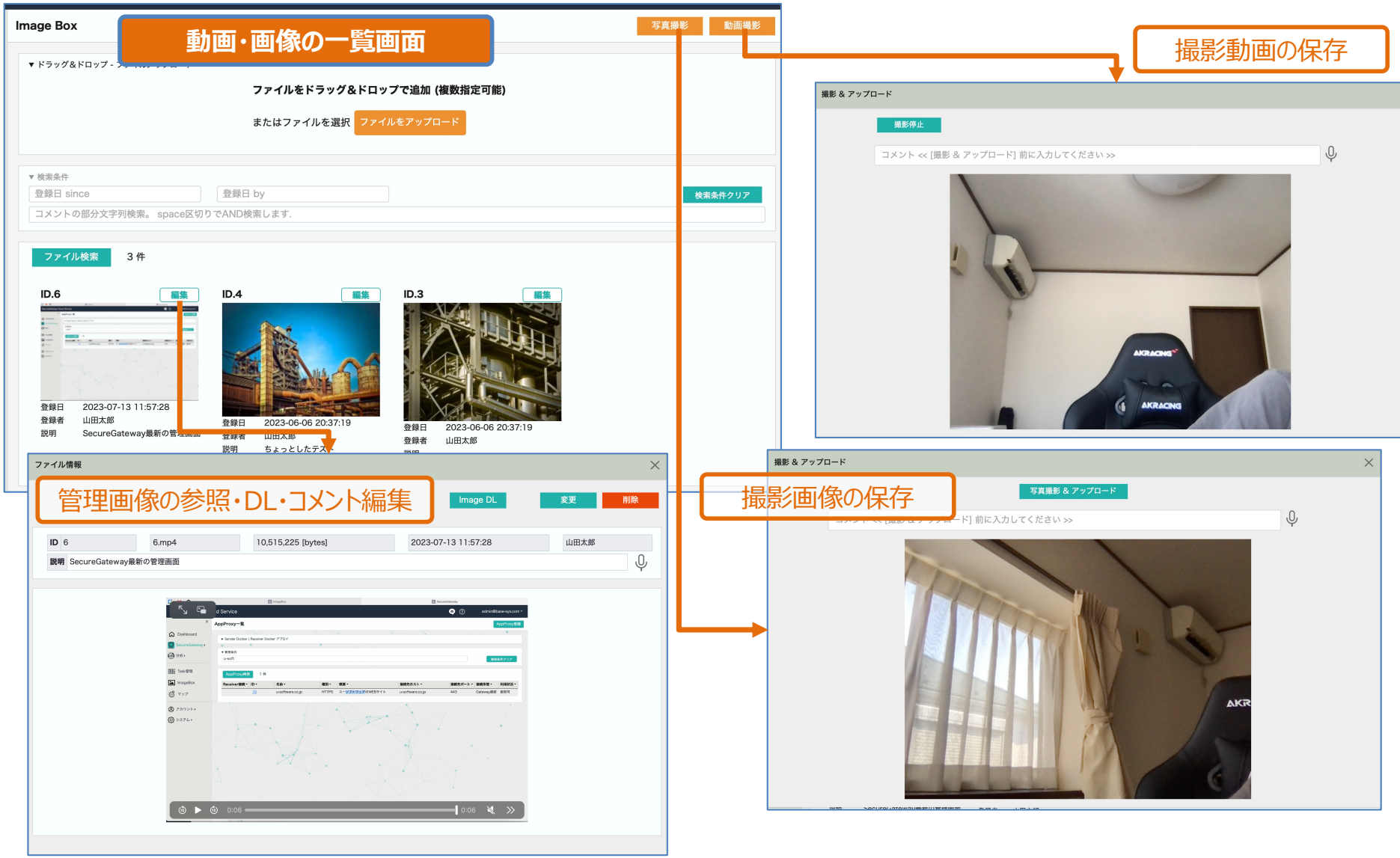


Image Box
動画・画像の一覧画面
写真撮影
動画撮影
撮影動画の保存
ファイルをドラッグ&ドロップで追加 (複数指定可能)
またはファイルを選択
ファイルをアップロード
検索条件
登録日 since
登録日 by
検索条件クリア
コメントの部分文字列検索。 space区切りでAND検索します.
ファイル検索
3 件
ID.6
編集
登録日 2023-07-13 11:57:28
登録者 山田太郎
説明 SecureGateway最新の管理画面
ID.4
編集
登録日 2023-06-06 20:37:19
登録者 山田太郎
説明 ちょっとしたテスト
ID.3
編集
登録日 2023-06-06 20:37:19
登録者 山田太郎
撮影 & アップロード
撮影停止
コメント << [撮影 & アップロード] 前に入力してください >>
ファイル情報
管理画像の参照・DL・コメント編集
Image DL
変更
削除
ID 6
6.mp4
10,515,225 [bytes]
2023-07-13 11:57:28
山田太郎
説明 SecureGateway最新の管理画面
撮影画像の保存
撮影 & アップロード
写真撮影 & アップロード