

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。これがゼロデイ攻撃です。
- 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

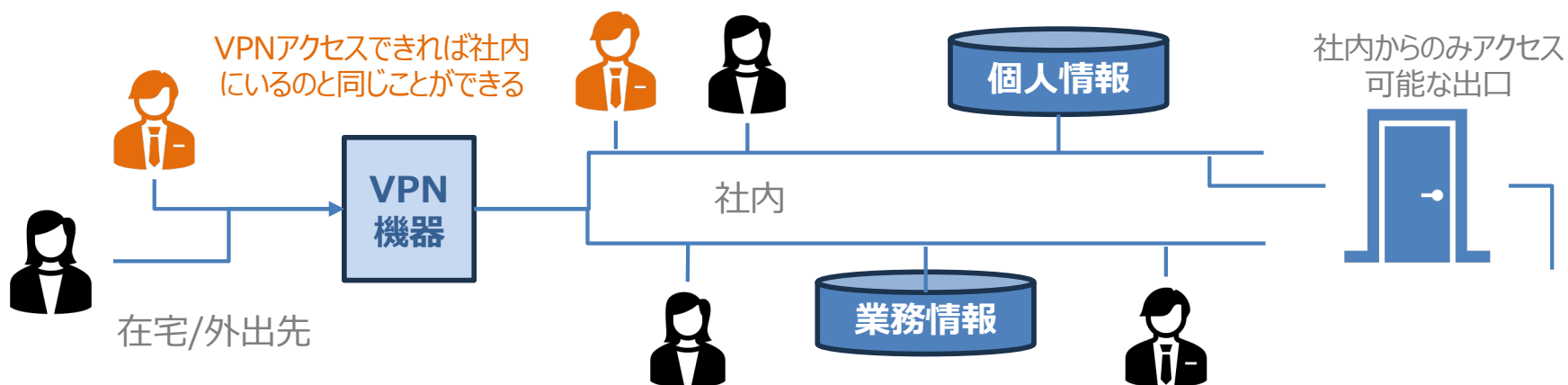
テレワーク環境で利用されるVPNが狙われている

- 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。

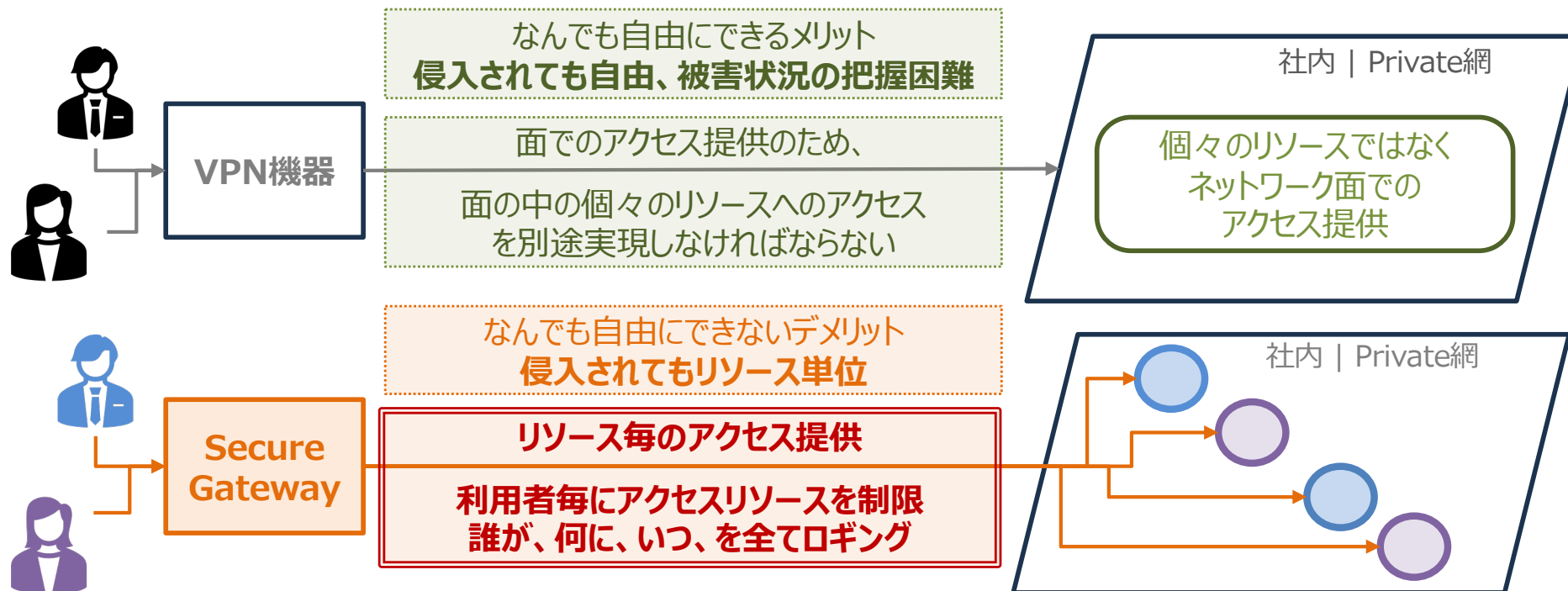
なぜVPNが狙われるのか？

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。
- クラサーバ・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があります

定常的なセキュリティ運用・教育が必要



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

Secure ICT Gateway Cloud Service

uchida@secure-ict.com

Gateway登録

Gateway一覧

▼ Sender | Receiver デプロイ

SecureGatewayは以下の接続構成です。

- Sender : L4(tcp), L6(ssl) の client-server 通信をする場合に必須になります。
- Receiver : Local 環境への接続の場合に必要なになります。

Sender Docker DL Receiver Docker DL Windows SndRecv共通APL DL

インターネット環境 プライベートネット

接続種別: Receiver経由 (Local環境接続は Receiver経由)

接続種別: 直接接続

デプロイ対象: Sender (Local) Winアプリ or Docker

デプロイ対象: Receiver (Local) Winアプリ or Docker

L4通信 (L4|L6 client) L7通信 (Web client)

Local Client (L4|L6 client) Browser (Web client)

Web Server (Internet) L4 | L6 Server (Internet)

Local Server (L4|L6 server) Local Server (Web)

https://{servicedomain} oxyz/

(*) s...接続などのストリーム通信は原則として L4(tcp)を使ってください。L6(ssl)は区間毎にsshコネクションが構築される構成です。

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

アクセスログ

SecureGateway Access Log

- securegw_access.log_20230721
- securegw_access.log_20230720
- securegw_access.log_20230719
- securegw_access.log_20230718
- securegw_access.log_20230717
- securegw_access.log_20230716
- securegw_access.log_20230715
- securegw_access.log_20230714

検索文字列1 (空白利用不可) 検索文字列2

除外文字列1 (空白利用不可) 除外文字列2

検索

tail -n {検索行数[*]} {ログ[*]} | grep {検索文字列1} | grep {検索文字列2}

(※1) 未指定時は内部で 100,000,000 を指定して取得します。

23/07/19 10:04:03 23/07/19 10:04:04 ok 376 172.26.0.1 www.lac.co.jp www.lac.co.jp

23/07/19 10:04:03 23/07/19 10:04:04 ok 379 172.26.0.1 www.lac.co.jp www.lac.co.jp

23/07/19 10:04:04 - start 384 -----

23/07/19 10:04:04 - start 385 -----

23/07/19 10:04:03 23/07/19 10:04:04 ok 382 172.26.0.1 www.lac.co.jp www.lac.co.jp

CSIRT機能

Secure ICT Gateway Cloud Service

インシデント報告

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

報告後の経緯・対応

再発防止策

再発防止策(承認)

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

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

The screenshot shows the main dashboard of the Secure ICT Gateway Cloud Service. The top navigation bar includes a notification bell with the text "通知 (一斉)" and the user email "sysadmin@secure-gw.com". The left sidebar contains menu items for "アカウント" (Accounts) and "システム" (System). The main content area is divided into several sections, each with a callout box:

- アカウントの部署定義** (Account Department Definition): Points to the "部署定義" (Department Definition) menu item.
- ログイン中セッション管理** (Login Session Management): Points to the "セッション" (Session) menu item.
- システム情報の参照** (Reference of System Information): Points to the "システム情報" (System Information) menu item.
- シングルサインオン(SP設定)** (Single Sign-On (SP Setting)): Points to the "シングルサインオン(SP)" menu item.
- メモ帳 (個人用)** (Memo Pad (Personal)): Points to the "メモ" (Memo) menu item.
- アクセスログ** (Access Log): Points to the "アクセスログ" (Access Log) menu item.
- アカウント管理** (Account Management): Points to the "アカウント一覧" (Account List) table.
- ACL機能 (利用可能な権限の設定)** (ACL Function (Setting of Available Permissions)): Points to the "機能ACL" (Feature ACL) section.
- 全てのログを保存 (検索、DL、削除可能)** (Save All Logs (Search, Download, Deletion Possible)): Points to the "Access Log" table.
- アカウントにACLを紐づけて利用機能を制限可能** (Possible to Restrict Usage Functions by Linking ACL to Accounts): Points to the "アカウント管理" (Account Management) section.

The "アカウント一覧" (Account List) table contains the following data:

ID	E-Mail	種別	名前	SecurityGrp	部	課	グループ	最終ログイン日時
1	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	2023-08-22 12:02:32
2	uchida@u-software.co.jp	システム管理者	内田高行	admin_readonly	総務・人事部	情報システム課		2023-08-22 12:02:37
3	tokugawa@u-software.co.jp	業務・責任者	徳川家康	full_access	開発部	研究課		2023-08-22 12:02:38

The "Access Log" table shows the following data:

LogName	LogContent
access.log_2023-08-07	
access.log_2023-08-08	
access.log_2023-08-14	
access.log_2023-08-22	

タスク管理機能

The screenshot displays a task management interface with several key components:

- タスク管理グループ一覧 (Task Management Group Overview):** Located at the top left, it includes a search bar and a list of groups. A callout labeled **複数タスク管理** (Multiple Task Management) points to the search and group selection area.
- タスク管理グループ (Task Management Group):** A central panel showing details for a specific group, including its ID and name.
- Kanban定義 (Kanban Definition):** A table defining the boards used in the Kanban view. A callout labeled **ボード定義** (Board Definition) points to this table.

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
7	議事録	ALL	bg-white
- タスク操作 (Task Operation):** A detailed view of a task, including its title, board, progress, and completion date. A callout labeled **タスク** (Task) points to this section.

Task details: TaskId 30, Title 情報セキュリティ検査機能, Board 処理済み, Progress 100%, Completion 2023/08/31 18:00.
- タスクボード (Task Board):** A visual representation of tasks across different boards (未処理, 処理中, 処理済み, ペンディング). Tasks are shown as cards with status tags (design, make, test) and progress indicators.

データ収集・分析機能1

原因分析、名寄せ、MFA統計のバックグラウンドジョブ管理（結果取得含む）

分析メニュー: 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

分析ジョブ一覧

状態	ID	種別	分析セットID	タイトル
完了	112	回帰分析	1	Kaggle House
完了	111	回帰分析	1	Kaggle House
完了	110	回帰分析	1	Kaggle House

分析ジョブ詳細 (ID: 112)

種別: 回帰分析 | タイトル: Kaggle House Price 予測解析

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

データセット詳細 (ID: 14)

名称: Kaggle House Price 解析のTestデータ | 種別: CSV upload

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

定義情報 (データセット・直アクセス)

Schema	Table	Column	データ参照 (3件のみ)
-	14.csv	▼ Rows [1,459], Cols [80]	▼ データ参照
		Id	(1461), (1462), (1463)
		MSSubClass	(20), (20), (60)
		MSZoning	(RH), (RL), (RL)
		LotFrontage	(80), (81), (74)

名寄せ

名寄せ実行

名寄せセット操作

対象データセット・テーブル [1]

Table	名	ファイル
カラムグループ-1	name	11.csv
カラムグループ-2	prefectureName	cityName
カラムグループ-3	カラム選択	カラム選択

対象データセット・テーブル [2]

Table	名	ファイル
カラムグループ-1	name	12.csv
カラムグループ-2	prefectureName	cityName
カラムグループ-3	カラム選択	カラム選択

データ収集・分析機能2

分析

- 分析ジョブ
- データセット
- Task → 名寄せセット
- Image → 原因分析セット
- マップ → MPC統計セット

カラム毎の Encoding(OneHot|Ordinal|Log) | 数値制限

Column	Condition	数値か	非数値
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]		

原因分析

対象範囲 先頭 対象行数 10000

データ参照 〇 データ表示

▼ 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

対象範囲 先頭 対象行数 10000

Kaggle-HousePrice-Test 14.csv 14.csv

データ参照 〇 データ表示

分析結果 Excel (DL)

Column name	score	p-value
OverallQual	2930.799393	0
GrLivArea	1408.121694	3.0582E-216
GarageCars	1258.349493	3.0934E-199
ExterQual	1246.126735	8.306E-198
KitchenQual	1174.156206	2.9305E-189
GarageArea	1071.7338	1.106E-176
BasmtQual	1053.79512	1.9904E-174
TotalBsmntSF	873.7117938	7.5318E-151
GarageFinish	841.2385405	2.1003E-146

Grid Search

Score: 0.908001518

GridSearch Param: {"alpha": [0.001, 0.1, 1, 10, 20, 50, 100, 1000], "tol": [0.01, 0.05, 0.1, 0.5, 1]}

Best {"alpha": 10, "tol": 0.01}

Coef, Intercept

Intercept: 15.21908913

Coef: -0.000557102 LotFrontage, 1.68786E-06 LotArea, 0.025521554 Street, 0.012721652 Alley, -0.000637652 LotShape, -0.024283836 Utilities

今を未来にする。 Bring the future in NOW.

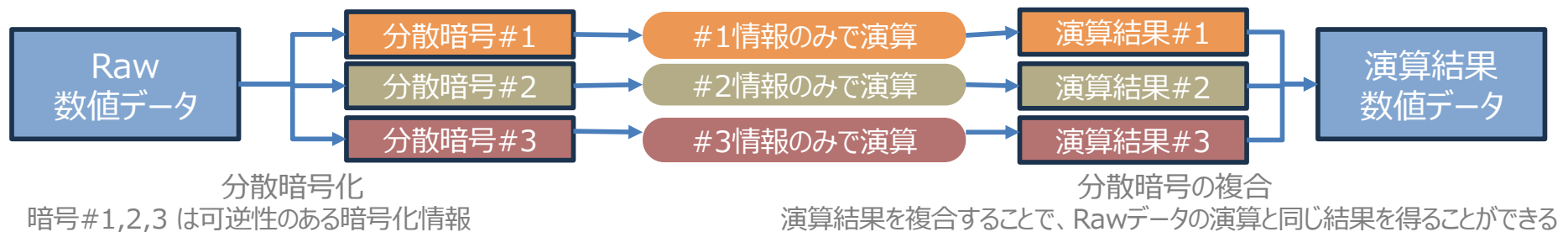
株式会社ユーソフトウェア

14

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。



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

The screenshot displays the 'Image Box' management interface. At the top, there are tabs for '写真撮影' (Photo Shooting) and '動画撮影' (Video Shooting). The main area shows a list of files with columns for ID, thumbnail, and edit options. Three callout boxes highlight specific features: '動画・画像の一覧画面' (List view of videos and images) points to the file list; '撮影動画の保存' (Save shooting video) points to the '動画撮影' tab; and '管理画像の参照・DL・コメント編集' (Reference, download, and comment editing for management images) points to the '編集' (Edit) button on a file. Two inset windows show the '撮影 & アップロード' (Shooting & Upload) process, with callouts for '撮影画像の保存' (Save shooting image) pointing to the '写真撮影 & アップロード' (Photo Shooting & Upload) button and a comment input field.

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

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 >>

管理画像の参照・DL・コメント編集

撮影画像の保存

写真撮影 & アップロード

コメント << [撮影 & アップロード] 前に入力してください >>

ID	Thumbnail	登録日	登録者	説明
ID.6	[Thumbnail]	2023-07-13 11:57:28	山田太郎	SecureGateway最新の管理画面
ID.4	[Thumbnail]	2023-06-06 20:37:19	山田太郎	ちょっとしたテスト
ID.3	[Thumbnail]	2023-06-06 20:37:19	山田太郎	