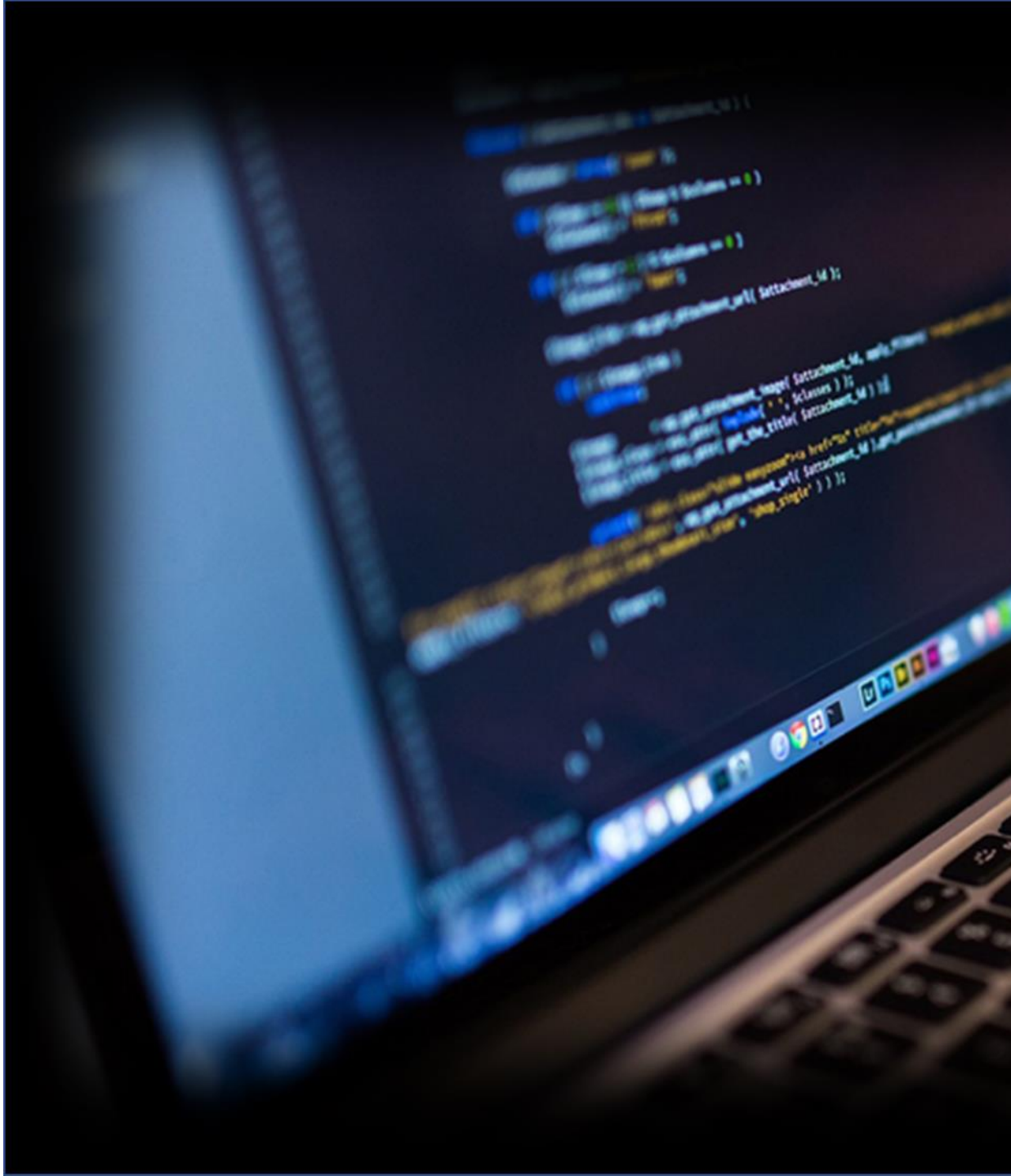
TrustSoT

Solution Intoduction

2022

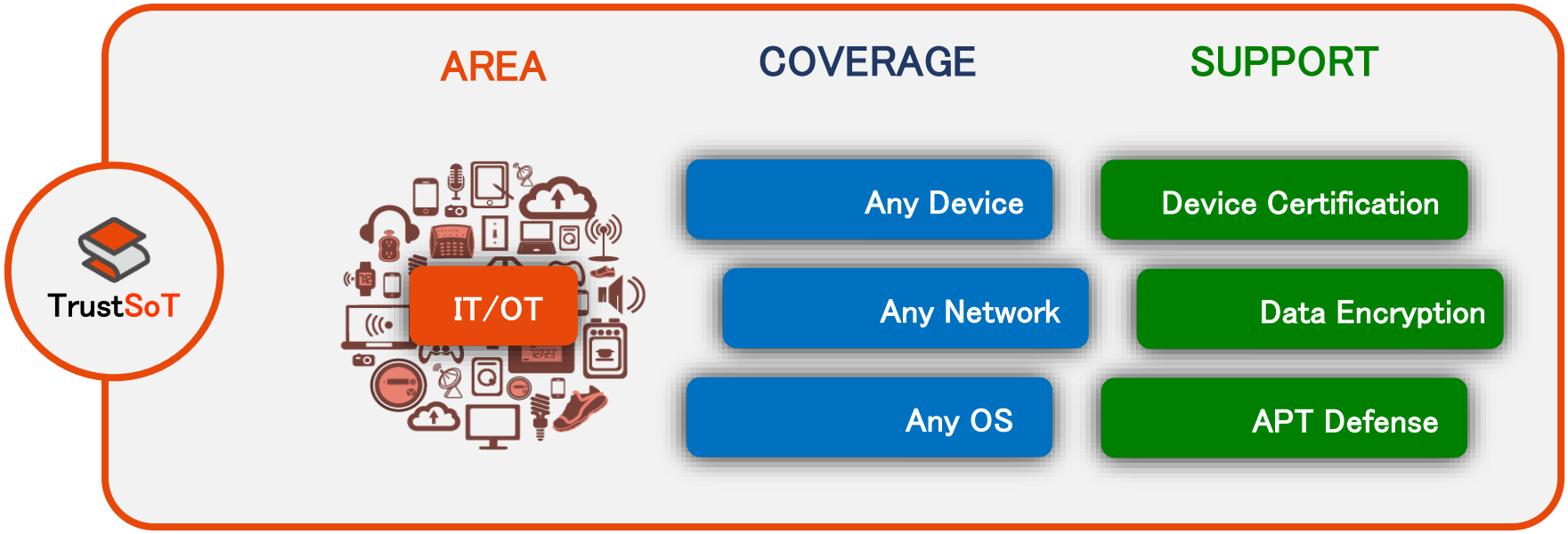


TrustSoT Concept

TrustSoTは自社特許を基盤に

- 「超軽量 S/W Library」,「Device 認証」と「データ生成時の暗号化」技術を利用し
- 「Decive」,「Network」,「OS」の種類に縛られず
- 「個人情報」、「企業および公共機関の機密情報」、「クラウドなどの委託管理情報」「大容量ストリーミング映像」は勿論、

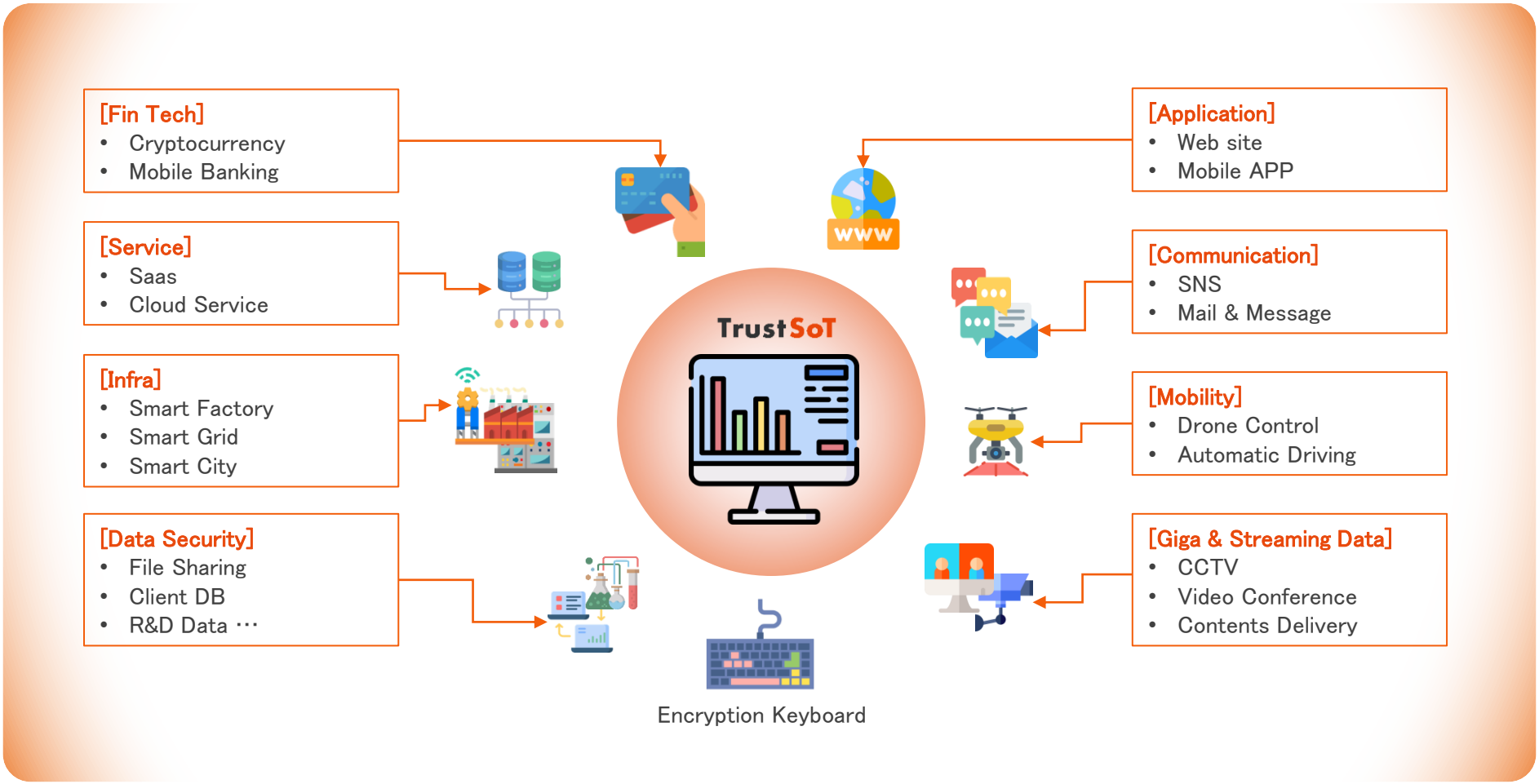
  「遠隔および自動制御分野(OT/ICS注1))」「通信インフラ構成」で顧客の目的に対し最高の保安体制を提供します。



注1) OT/ICS : “Operational Technology/Industrial Control System”, 運営 技術/産業制御システム

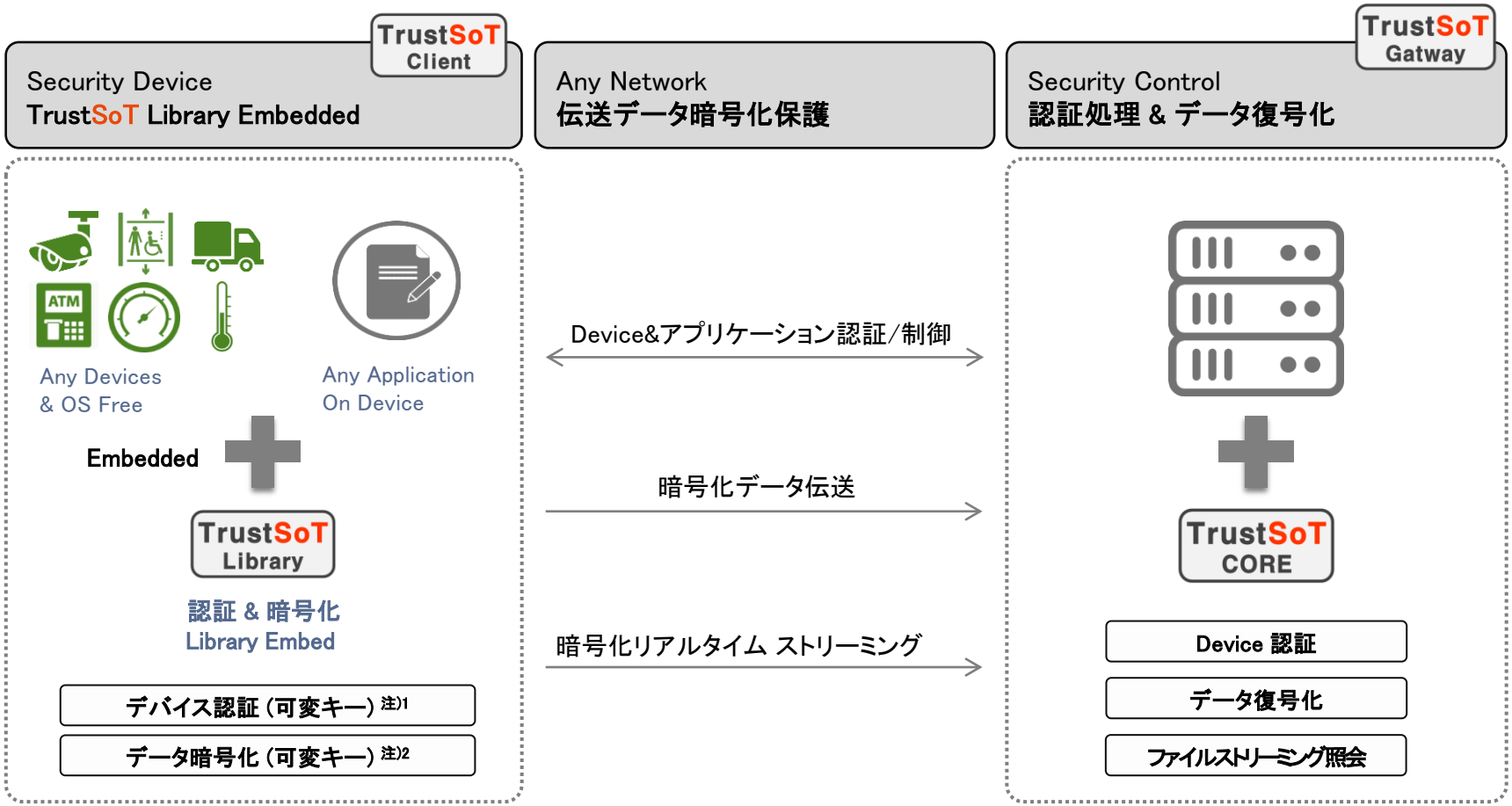
■ TrustSoTは、すべての分野に適用可能

多様な形態のネットワーク、そして**主要データと制御命令を暗号化**して保護します。



TrustSoT Core Technology

■ 認証/暗号化

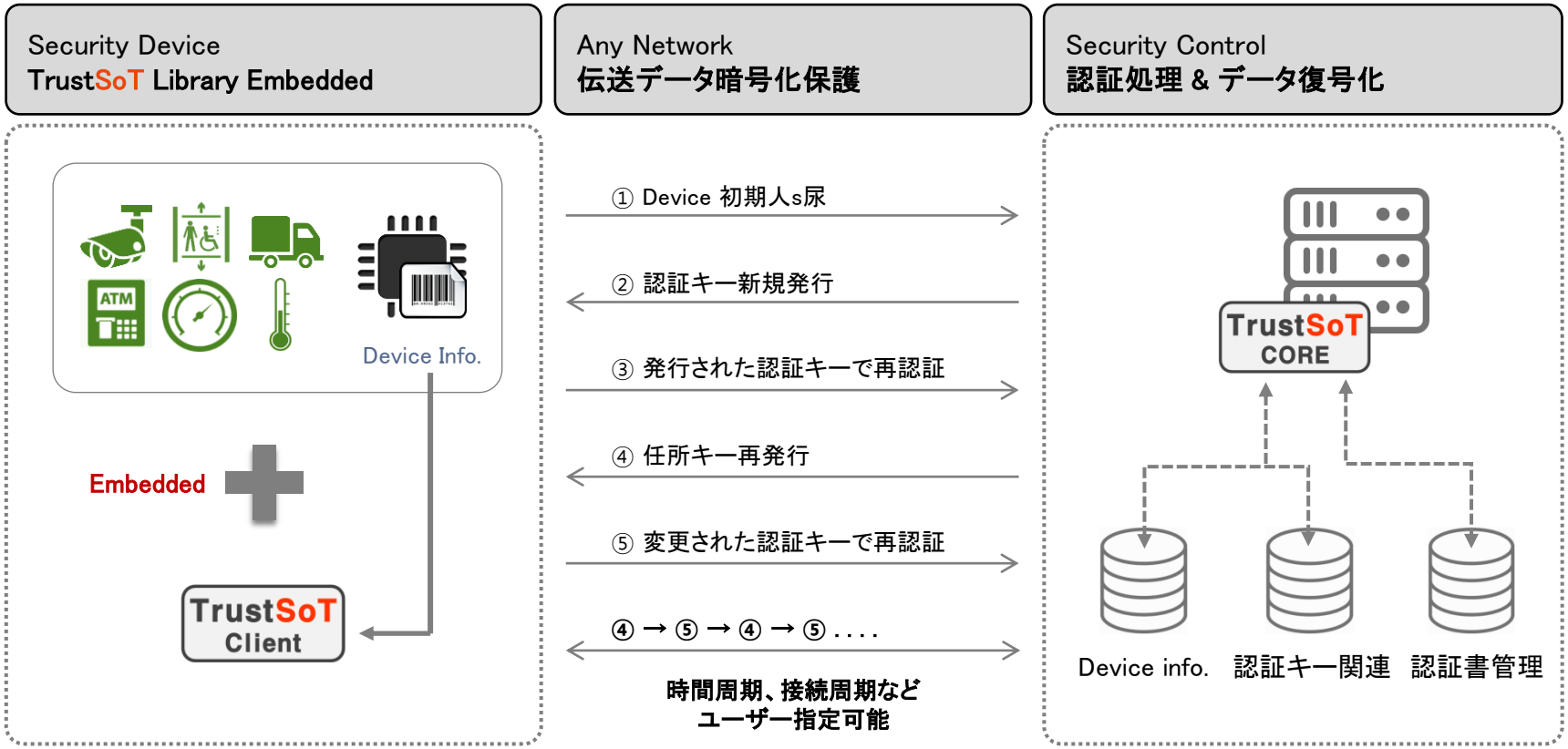


注)1 Page7~8 核心技術「**デバイス認証**」参照
注)2 Page9~10 核心技術「**データ暗号化**」参照

「デバイス認証」

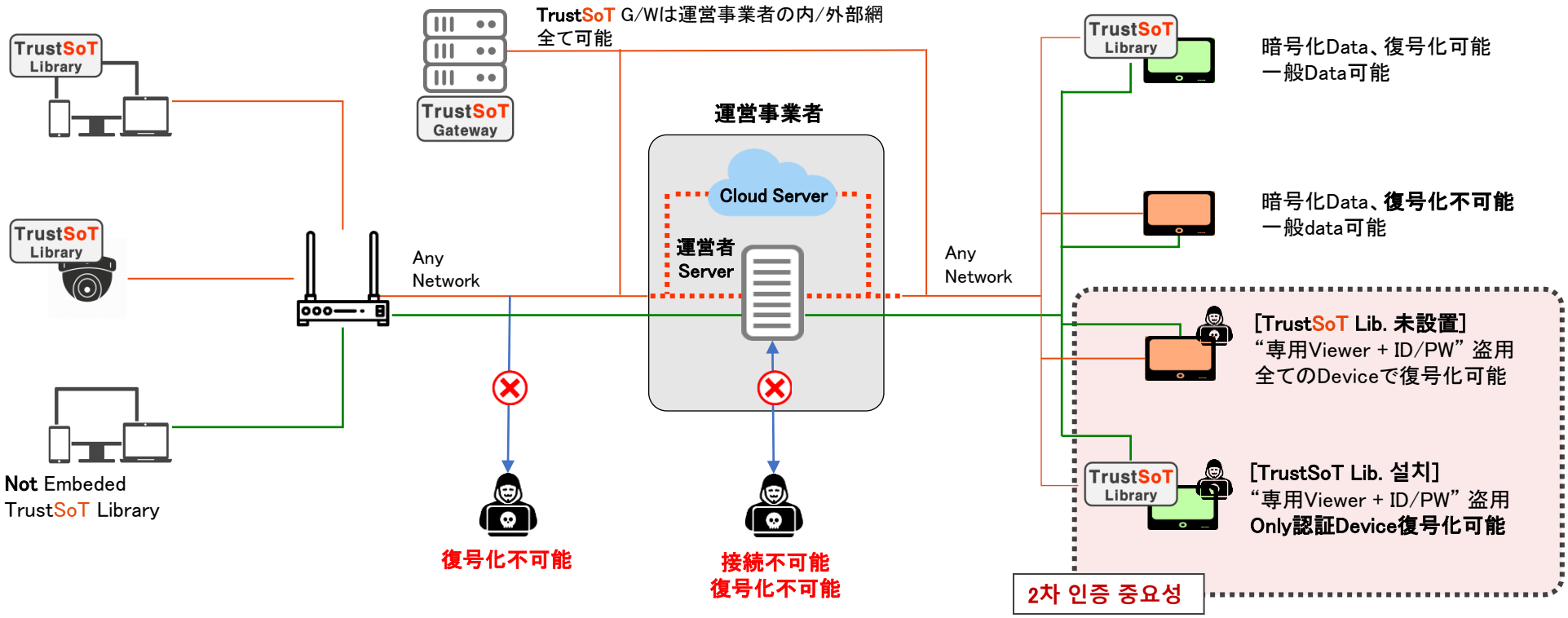
■ TrustSoTが適用されたDeviceは

該当機器のUnique(個別) 情報基盤で認証され、初期認証以降からはシステム連結時毎回新規認証キーの更新を受け
認証信頼性を極大化します。



■ TrustSoTの可変型認証キー基盤Device 2次認証の重要性

- ID、PWを通じ物理的な1次認証後、別途のユーザーの行動がなく定められた政策(時間基準、接続基準など)により
  ユーザーの別途行動がなくても持続的に2次認証開始
- ID、PWのヘルプ時にも認証を受けたDevice以外の接続はできず
  ID、PWの認証を受けたDEVICE全てが奪われてもDeviceを制御することで映像接続および情報流出はできません。

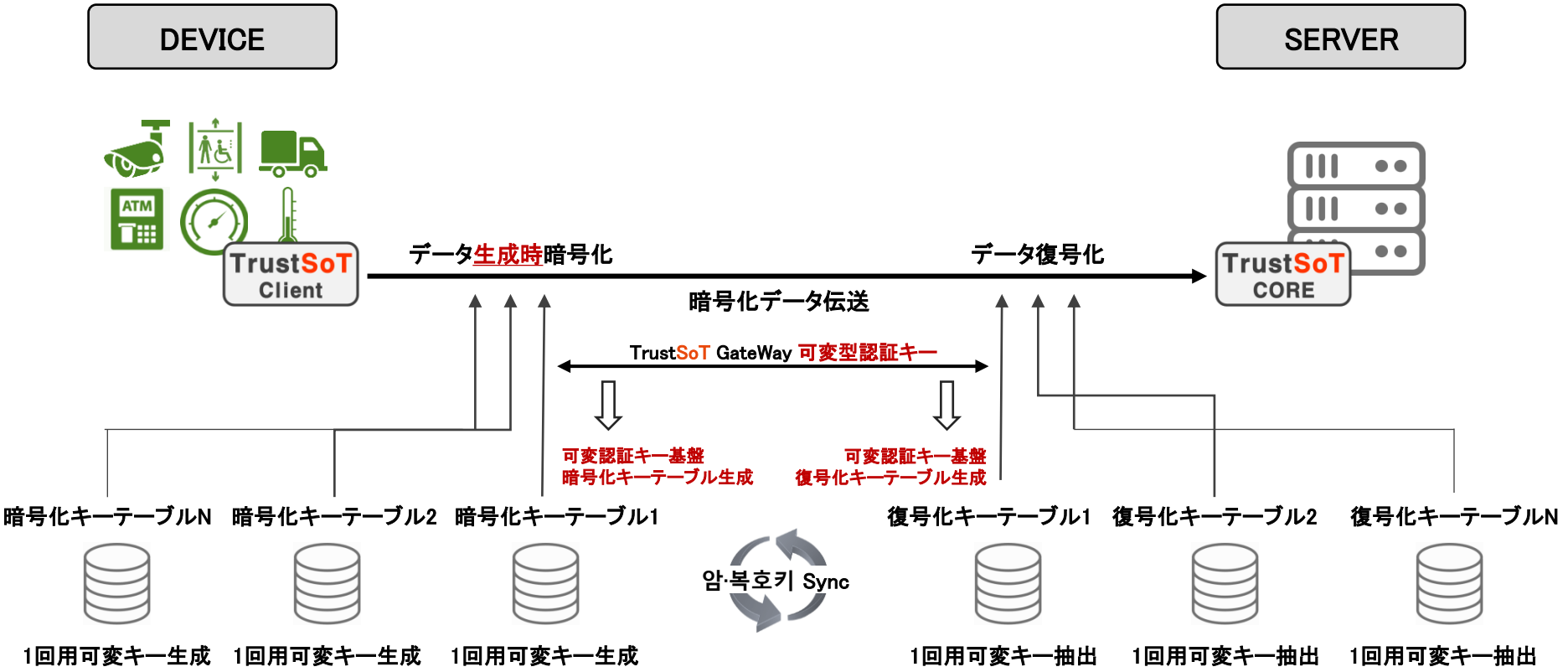


「データ暗号化」

■ TrustSoTが適用されたDeviceは

データ生成時から非定期的(Random) 1回用可変型暗号化キーを基盤にしたデータ暗号化を行い

伝送または保管中の全てのデータを完璧に保護 (標準認証暗号モジュールおよびアルゴリズム支援)

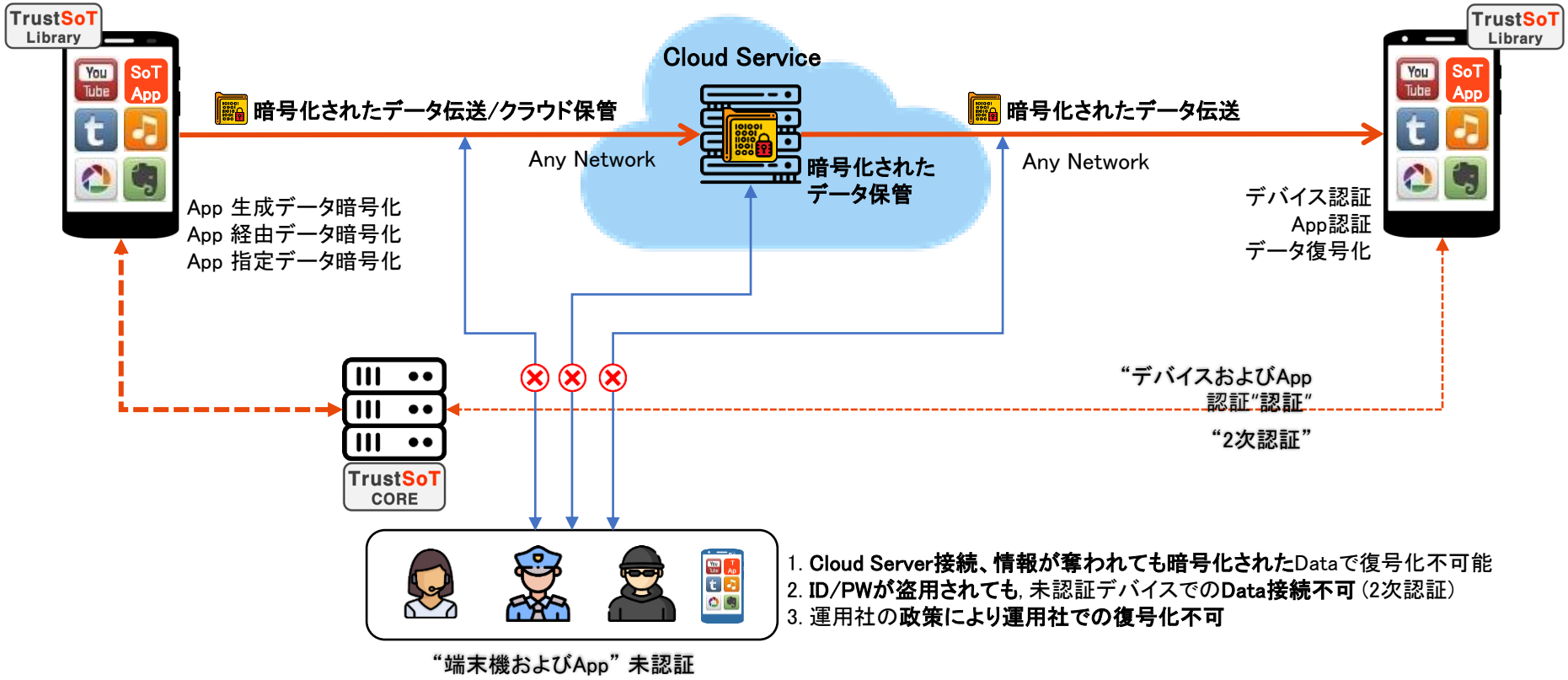


■ TrustSoT vs. 既存データ暗号化技術

TrustSoT	TPM 方式	Chip 方式
■ SW基盤認証および暗号化ライブラリー適用だけで保安可能 ※ 既構築された装備にアップデートなどを通じインベッティング	□ TPM認証のためHW製作段階から設計必要	△ Chip認証およびデータ暗号化のためにH/W製作段階から設計が必要
■ 可変型認証キー基盤機器認証	□ 固定キー基盤の認証方式	△ 多くの固定キー基盤の認証方式 ※ 固定キー流出時データ復号化可能
■ 生成データ暗号化および受信データ復号化 ※ 可変型暗号化キーシンク技術	□ 生成データ暗号化不可能	
■ 通信区間暗号化不必要 ※ 伝送データ暗号化で流出しても解読不可能	□ 低仕様、低電力環境で適用困難	△ 通信区間暗号化が必要などからIoTのような低仕様、低電力環境では適用困難
■ TrustSoT ファイルビューワを利用、文書保安中央管理可能		
■ 認証およびデータ受信状況モニタリングおよび制御		
■ IoTのような低仕様、低電力環境でも駆動		

TrustSoT Case Study

■ TrustSoTが適用されたAppの全てのデータは生成時に即時暗号化されクラウドサーバにアップロードされます。
よって、認証を受けていない端末機は勿論、Cloudサービス運営者も顧客データを閲覧することはできません。
社内機密情報が第三者の機関に保管され不安感を解消できるCloudサービスの提供が可能です。



Cloud 保管中の暗号化データはハッカーは勿論、運営者および公式的な確認手続きでも復号化不可能

TrustSoT Cloud Security vs. 一般Cloud Service

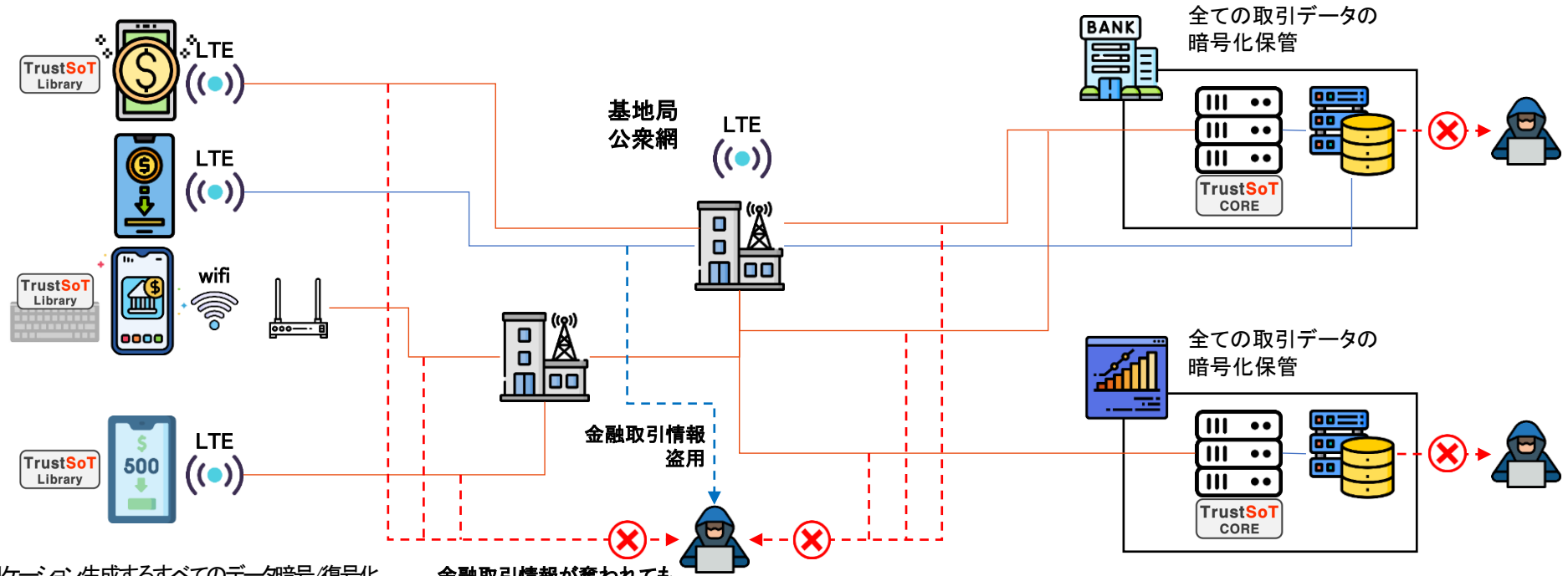
区分	TrustSoT Cloud Security	一般 Cloud Service
アプリケーション認証方式	TrustSoT可変型キーを通じ端末機+アプリケーション 2次認証方式	ID、MACアドレス基盤一般認証方式
データ保護	TrustSoT認証アプリケーションでデータ生成時暗号化	別途のデータ保護(暗号化など)支援なし
ネットワーク保安	暗号化データ状態をクラウドアプリケーション/ ダウンロード(ネットワーク上でハッキングされても データ復号化不可能)	アップロード時ネットワークハッキングデータ流出可能
クラウド ハッキング対策	暗号化されたデータがクラウドにアップロードされ 認証された端末機(アプリケーション)以外はデータ 仕様不可能	クラウドハッキング時(ID/PW流出など) 全てのデータ 流出事故発生脆弱性
端末機紛失時 処理方式	紛失した端末機のアプリケーションを使用不可に選定し クラウドにアップロードされたデータを完璧に保護	クラウド接続 ID/PW変更以外に対策なし

■ Solution1

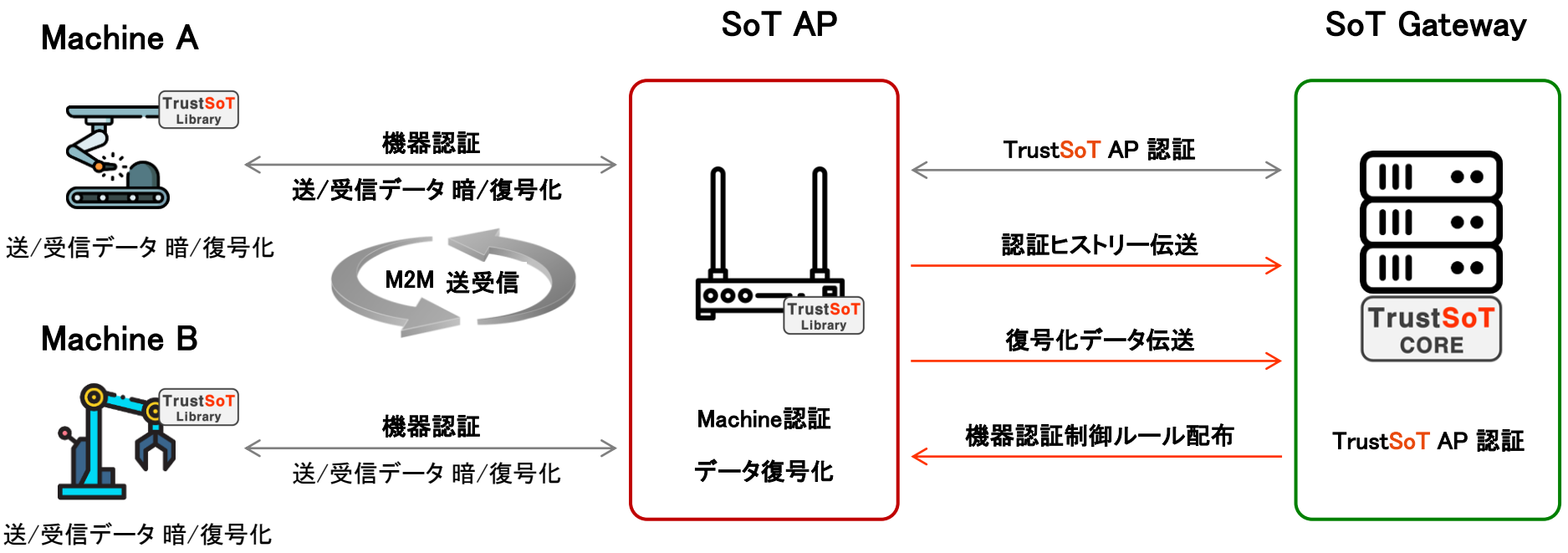
銀行 AppにTrustSoTを適用しAppで発生する全てのデータは生成時に即時暗号化され全ての取引を完璧に保護します。

■ Solution2

銀行 App内部にTrustSoT “保安キーボード” (page21)の適用を通じ入力、セーブ、伝送される全てのデータの暗号化を通じ
全ての取引を完璧に保護します、

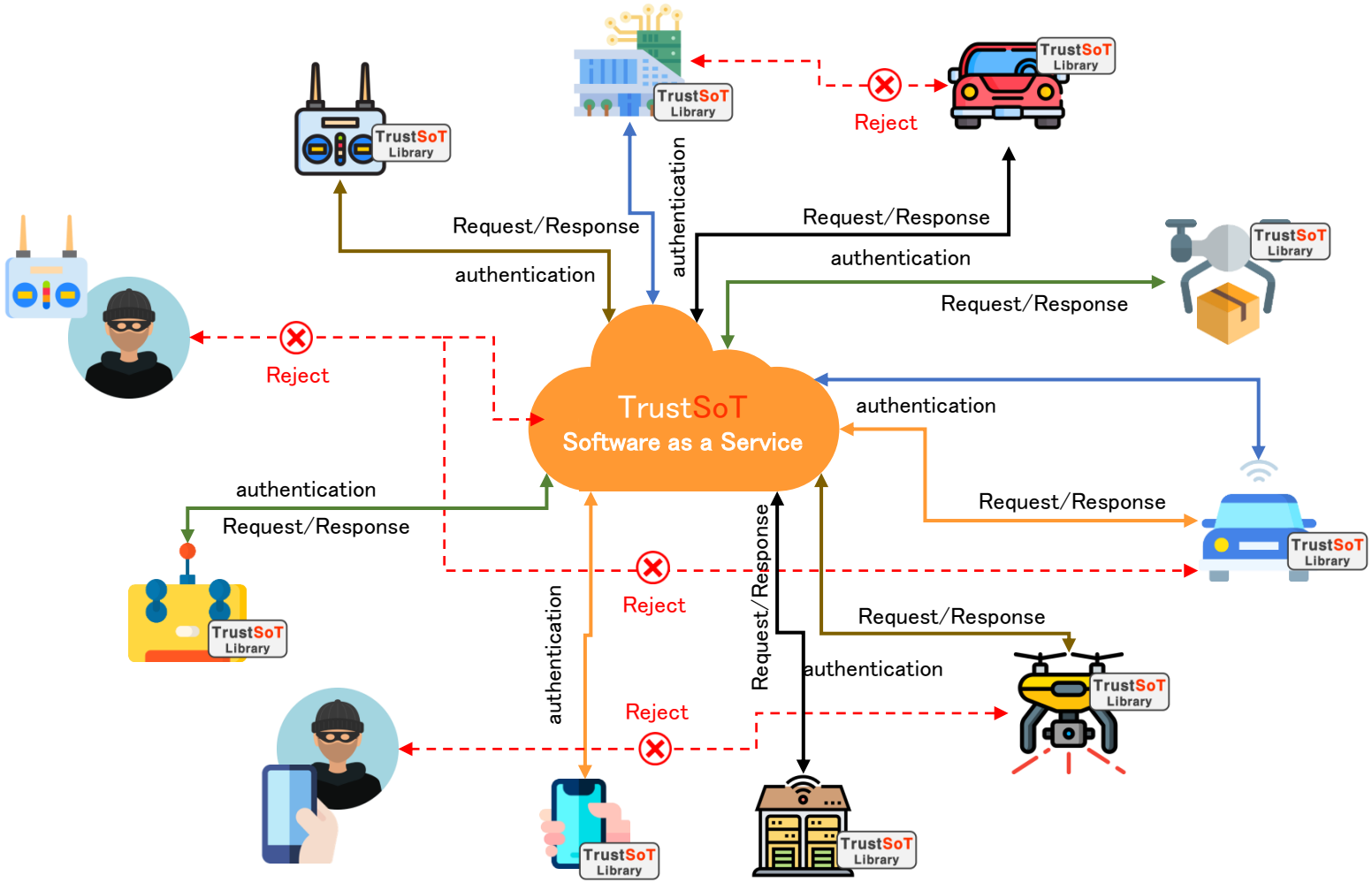


■ TrustSoTは多様なIoTコンバージェンス分野で最適されたDeviceの認証およびデータ保護を支援します。



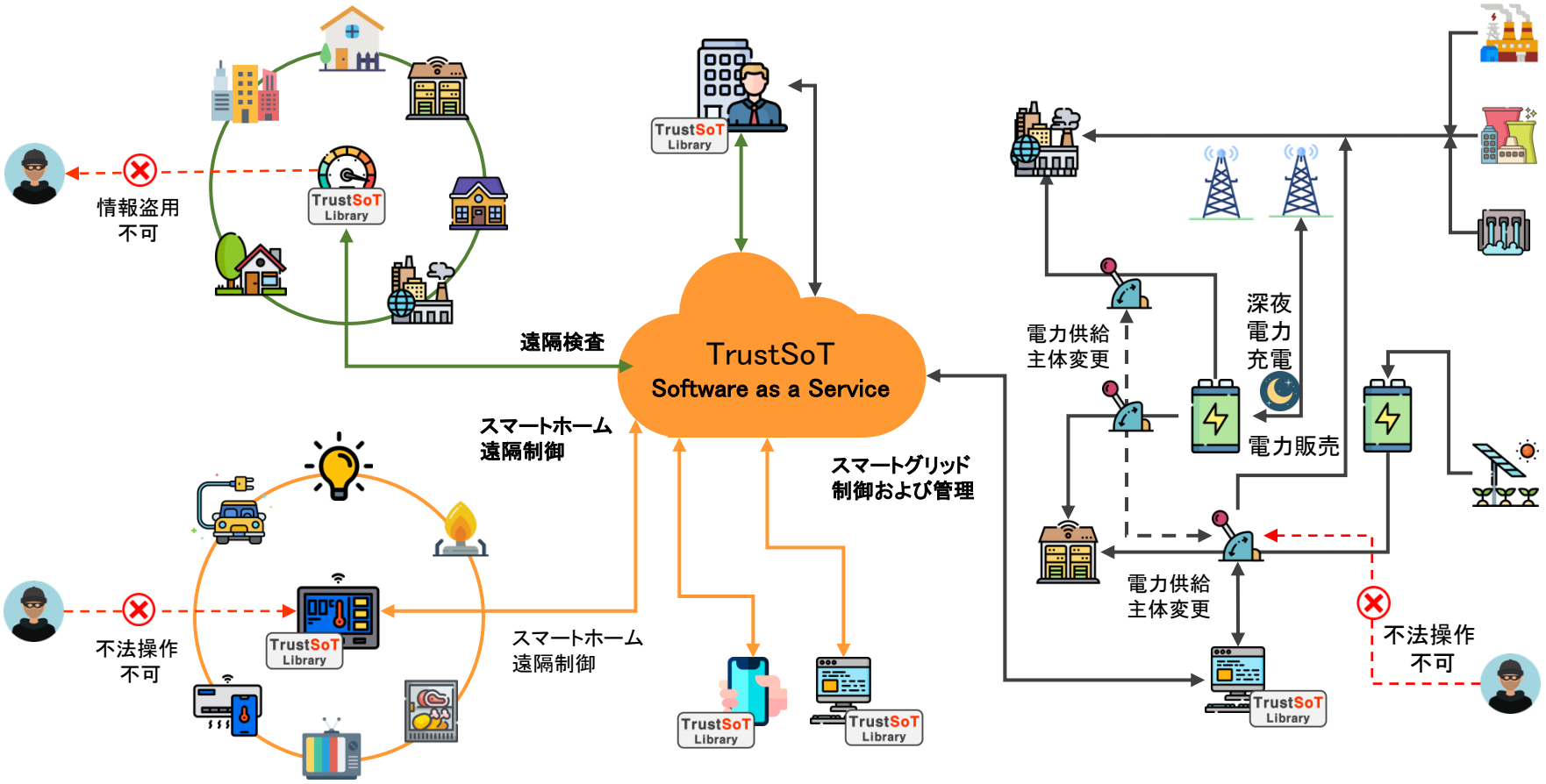
企業および公共インフラのM2M構成で、TrustSoT ソリューション(AP、GateWayなど)の適用を通じ 機器間認証および送受信データに対し源泉からの保安可能

■ TrustSoTは、多様な移動体の制御信号保護と制御Deviceに対する認証を支援します。



移動体と制御Devices間の認証および制御信号の完璧な保護を通じ誤作動を事前に防止

■ TrustSoTは、産業は勿論軽量IoTデバイスに対する多様なデバイスに対する認証および相互送受信データの保護を支援します。



Devices間の認証および制御信号およびDevice発生データの完璧な保護を通じ誤作動および情報流出防止

TrustSoT Product

製品および適用分野

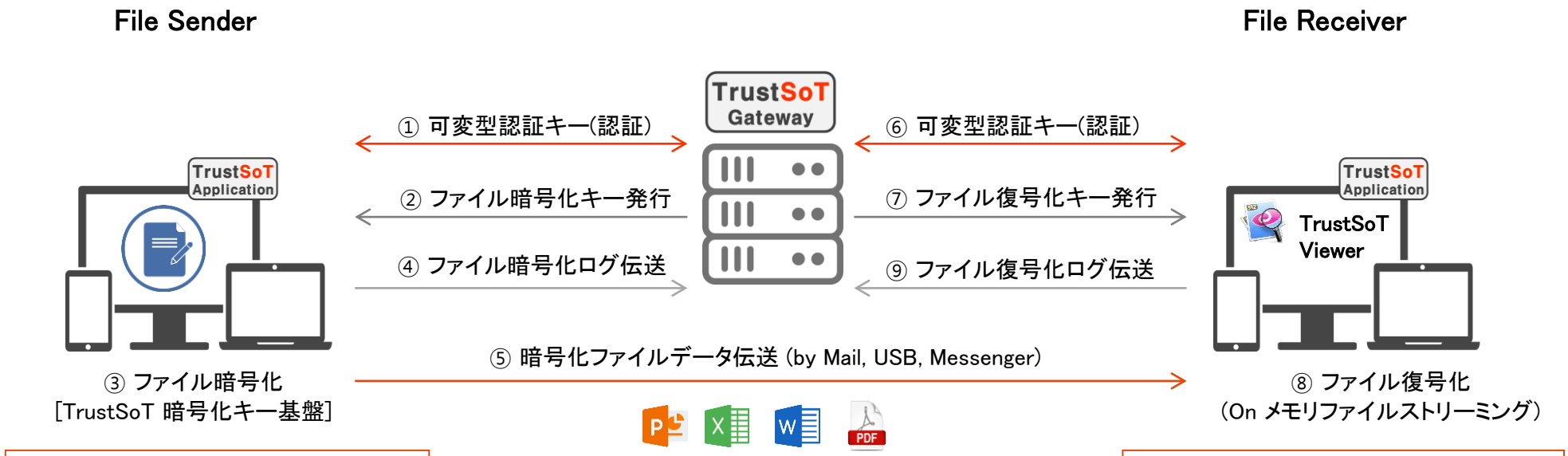
■ **TrustSoT 基盤技術を** IT 領域の多様な分野のソリューションに適用は勿論、OT/ICT 分野に対する産業用制御分野にも適用することで、顧客環境に即時適用可能な Apllication および製品開発を継続して推進しています。

Soft ware	**TrustSoT CORE** **Gateway　　Devices 認証 / Data 暗号化** ネットワーク内全てのDeviceに対する超軽量ライブラリー 基盤保安認証支援および相互認証 Deviceのデータ送受信時 完璧な暗号化 & 復号化支援	**TrustSoT Keyboard** (キーボード入力データ暗号化) **Plug in + Gateway** TrustSoT 技術基盤の仮想キーボードプラグインを通じ、 既存のキーボードの変更なしに作成された全てのテキストも 暗号化され保管/伝送することで、キーボードを通じて生成された 全てのデータを源泉保護
	TrustSoT File (ファイル暗号化) **Application+Gateway** Deviceに設置されたアプリケーションを通じファイルを暗号化し伝送し、ファイル受信者が TrustSoT ファイル専用ビューワを通じ該当ファイルを Streamingだけ可能にしたファイル保安ソリューション	**TrustSoT IMG** (映像データ暗号化) **Application+Gateway** Cameraに設置されたアプリケーション (エージェント)を通じ映像データを暗号化および復号化、キャプチャ防止、遠隔ハッキング防止などの映像コンテンツ不法コピーおよび流通防止機能を提供
	TrustSoT Mail (メール暗号化) **Plug in + Gateway** TrustSoT 技術基盤のウェブブラウザプログインを活用、 全てのウェブメールサービスの電送テキストおよび添付ファイルを源泉保護、メール伝送以降にも送信メール保安 制御支援	**TrustSoT OT/ICS** (SCADA/PLC 制御データ暗号化) **Application+Gateway** SCADA 制御 Deviceに設置されたエージェントを通じ Deviceの認証および制御 Dataの暗号化、不正 Access、情報流出防止とAgent 基盤 Process監視を通じ悪性コード探知、警告および内部網拡散遮断
Hard ware	**TrustSoT Security Camera** (Security CCTV Camera) with **TrustSoT IMG**	**TrustSoT LTE Router** (Security LTE Router) with **TrustSoT CORE** (認証/暗号化)

Software

TrustSoT File（ファイル暗号化）

■「TrustSoT File」アプリケーションが設置された Deviceはファイルを暗号化し伝送し、
該当ファイルを受信し「TrustSoT File」アプリケーションが設置されたユーザーは「TrustSoT Gateway」を通じ認証後、
「TrustSoT File ビューワ」を通じてのみ復号化および照会が可能（Deviceへの保管不可）になることで、
内部網だけでなく全領域で文書ファイルの完璧な保安および中央管理が可能です。

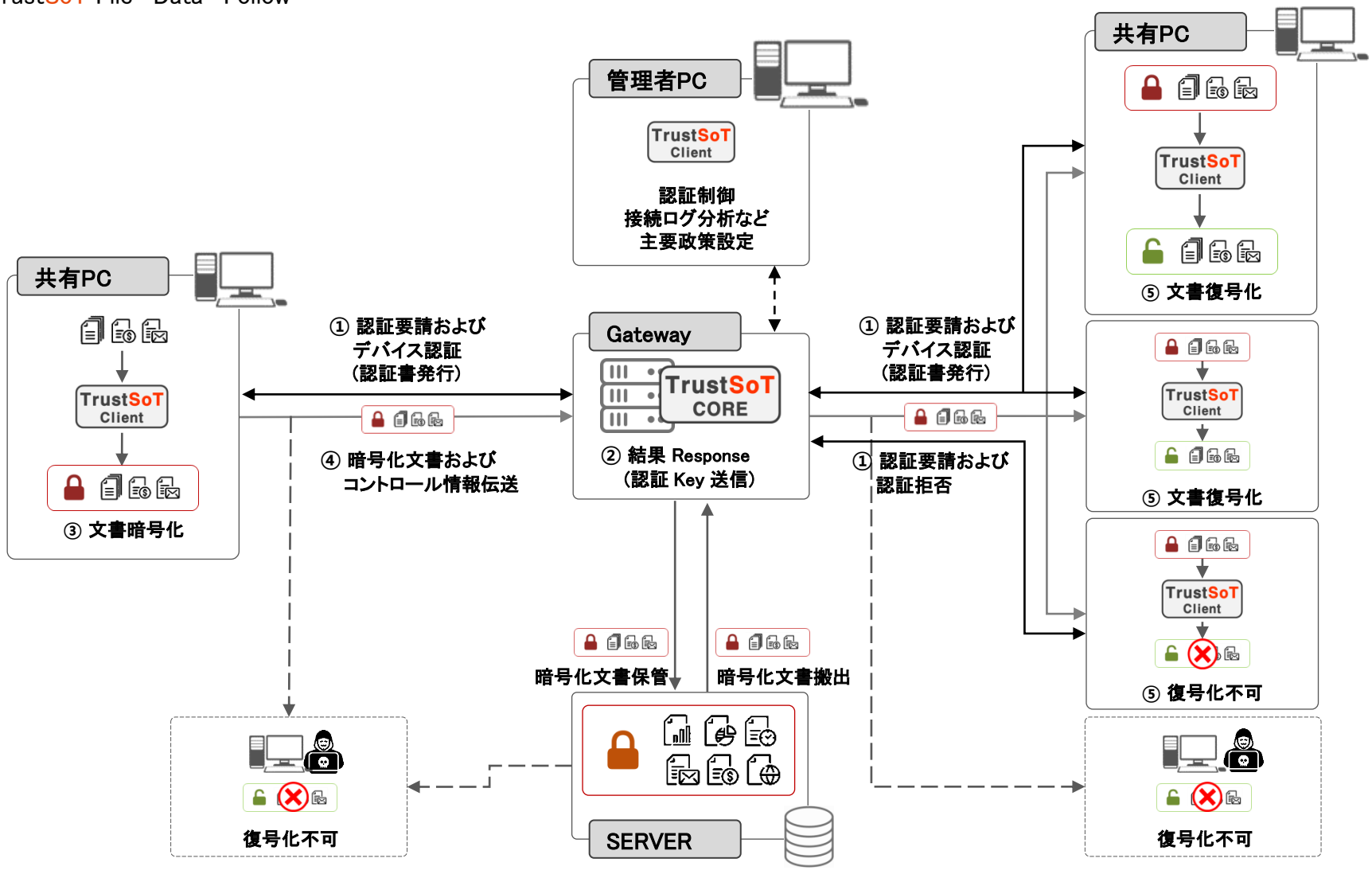


- ファイル暗号化時、受信者指定機能提供
- 指定された受信者以外ファイル照会不可

- 復号化ファイルはTrustSoT ファイルビューワのみ照会可能
- 復号化されたファイルはDeviceに保管不可

「TrustSoT File」User間 送受信暗号化メールは TrustSoT Gatewayでも復号化不可

■ TrustSoT File “Data” Follow



■ TrustSoT File vs. 一般文書中央化技術

区分	TrustSoT File	일반 문서중앙화 방식
伝送期間制約	■ データ伝送期間暗号化適用不必要	□ 内部封鎖網具現必要
ファイル暗号化	■ 外部ファイル伝送時、文書を暗号化し伝送 ■ 可変型暗号化キーを通じ暗号化されたデータを伝送し、ハッキング時にもファイル流出を防止	□ ファイル暗号化はオプションで、一般暗号化方式 □ 外部ファイル搬出時、許可または権限必要
ファイル保護	■ ファイルを暗号化するユーザーが受信者の指定が可能でm認証を受けた受信者に限りファイル照会が可能 ■ 受信者は復号化されたファイルを照会のみ可能で個人 Deviceに保管できない	□ ファイルを受信した外部ユーザーのPC環境を制御することはできない(搬出記録のみ存在)

TrustSoT Mail/SNS/App. 暗号化

■「TrustSoT Mail」ウェブブラウザ用 Plug-inを通じて ウェブメール、SNS、Mobile Appのテキストおよび添付ファイルに対する暗号化を行います。

また、メール伝送後にも多様な保安制御および事後管理を支援します。

別途のネットワーク保安ソリューションなくTrustSoT Library or Plug-in だけでも保安メールおよびこれに対する事後管理が可能

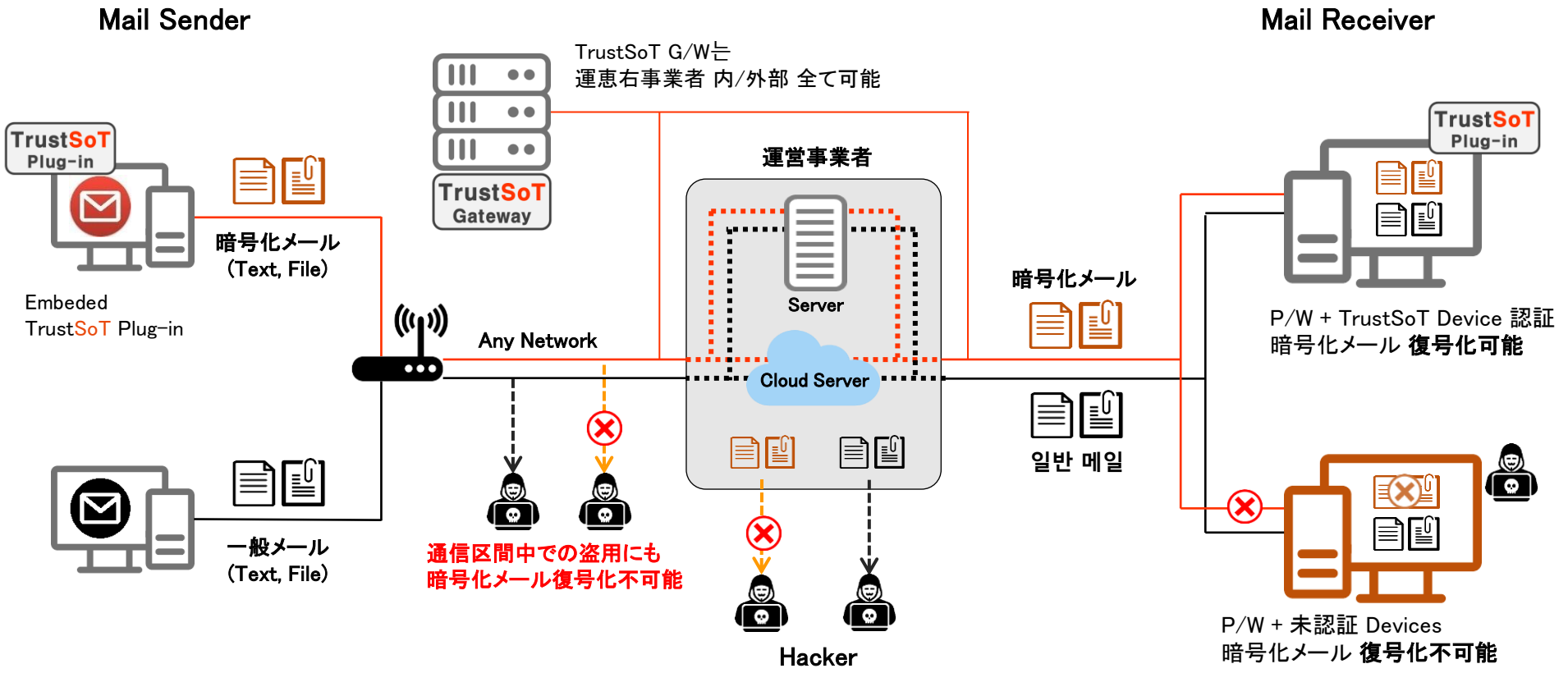
- 作成されたメールDATA暗号化
- 添付ファイル暗号化
- 伝送用/サーバ内 暗号化保管
- 再伝送権限管理
- 閲覧回数制御可能
- エラー発送時開封不可設定

送信者が設定した権限内で
受信/閲覧/再伝送/保管可能

「TrustSoT Mail」User間 送受信暗号化メールはTrustSoT Gatewayでも復号化不可

TrustSoT Mail (メール暗号化)

■ TrustSoT Mail “Text & File” Follow



運営者 Server、Cloud 保管中の暗号化メールを盗用時にも復号化不可能

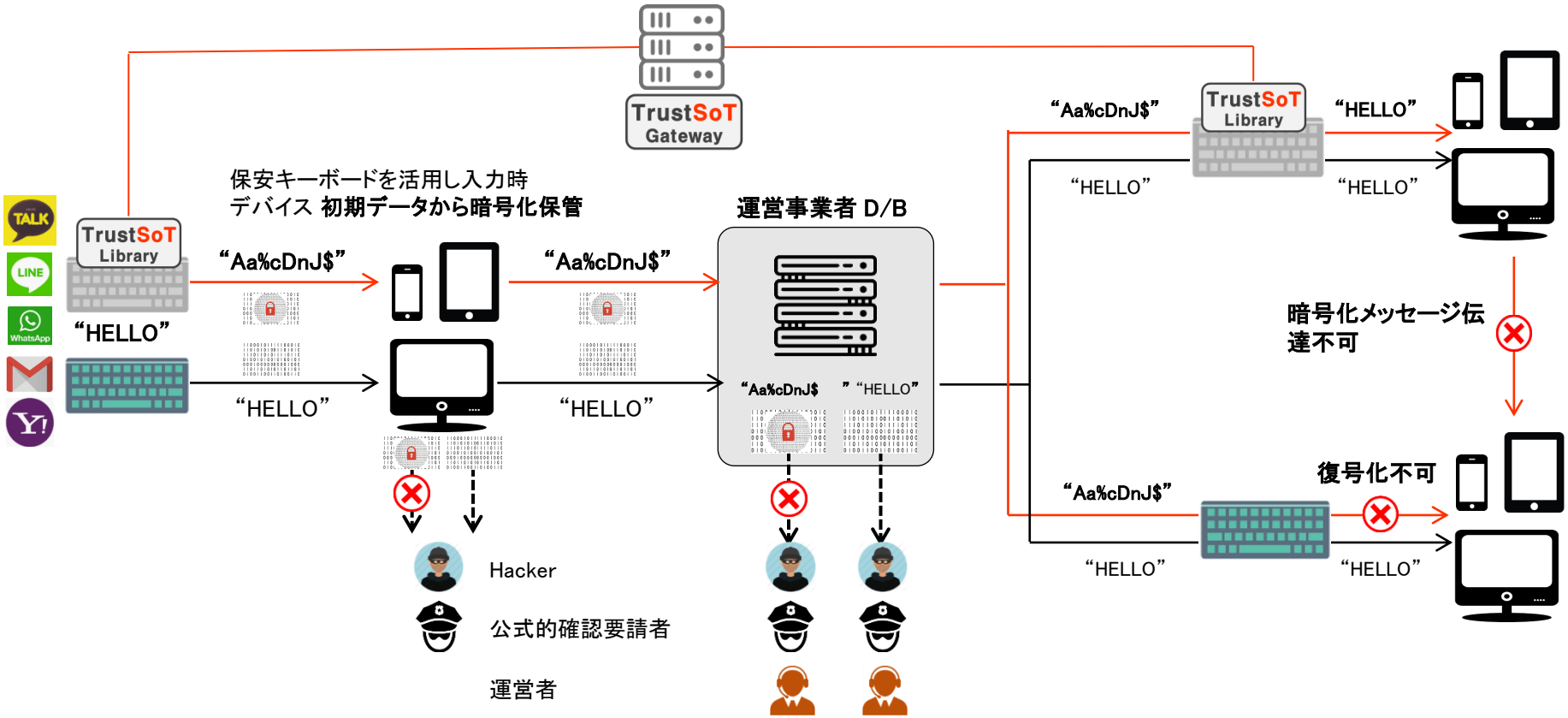
(保管中の一般メール盗用時内容確認可能)

■ TrustSoT Mail vs. 一般保安メールソリューション

区分	TrustSoT Mail	Gmail 保安サービス (USA, C社)	情報流出防止ソリューション (KOR, U社)
ユーザー認証	■ ブラウザプログインを通じ複合認証 ■ 別途アプリケーション設置不必要 ■ 可変認証で完璧認証保安	□ メール受信者PWを通じユーザー認証 □ 送信PW認知時全てのメール閲覧可能	△ Agent(Software) 設置を通じた認証
データ保安	■ 全ての暗号化アルゴリズム適用可能 ■ TrustSoT データ保安技術適用 ■ メールテキストブラウザ上で暗号化 ■ プログインを通じ暗号化された ファイル添付 ■ 添付ファイル容量制限なし	□ メール送受信設定 PW 基盤保安 □ メールテキスト AES25 インコーディング支援 □ メールファイル添付時 AES25 インコーディング後、C社 クラウドアップロード/ リンク方式 □ 添付ファイル容量最大 100M	△ テキストおよびファイルはサーバに アップロードされ暗号化後データ伝送 △ 該当データビューワ(Agent)が設置 された全ての端末機で復号化可能 △ サーバで添付ファイル容量制限
互換性	■ 全てのOS、全てのウェブブラウザ互換 ■ 全てのモバイルアプリケーション ライブラリー支援	□ 一部ウェブブラウザ、Gmailサービス 専用 □ 専用モバイルウェブダウンロード必要	△ Agentが提供する OS 環境のみ支援 △ データ照会のため専用ビューワ 設置必要
ソリューション 導入 ROI	■ TrustSoT Gateway および プログイン費用のみ発生 ■ 全てのメールサービス適用可能	□ ユーザー当 一括 5ドル/月サービス料金 □ Gmail サービスに限り利用可能	△ ソリューション構築発生 (サーバ、Agent) △ 必要時ネットワーク、端末保安費用発生

TrustSoT Keyboard (暗号化仮想キーボード)

■ 「TrustSoT KeyBoard」 Libraryが適用した全てのデバイスの初期入力装置のDataの生成時から
暗号化を適用することで通信区間保安ソリューションと連動なしでも完璧なデータの保護が可能です。
また、データの共有以降にも安吾かが維持され "中央の命令"によって各デバイスの復号化 可能/不可能です。(差別化)



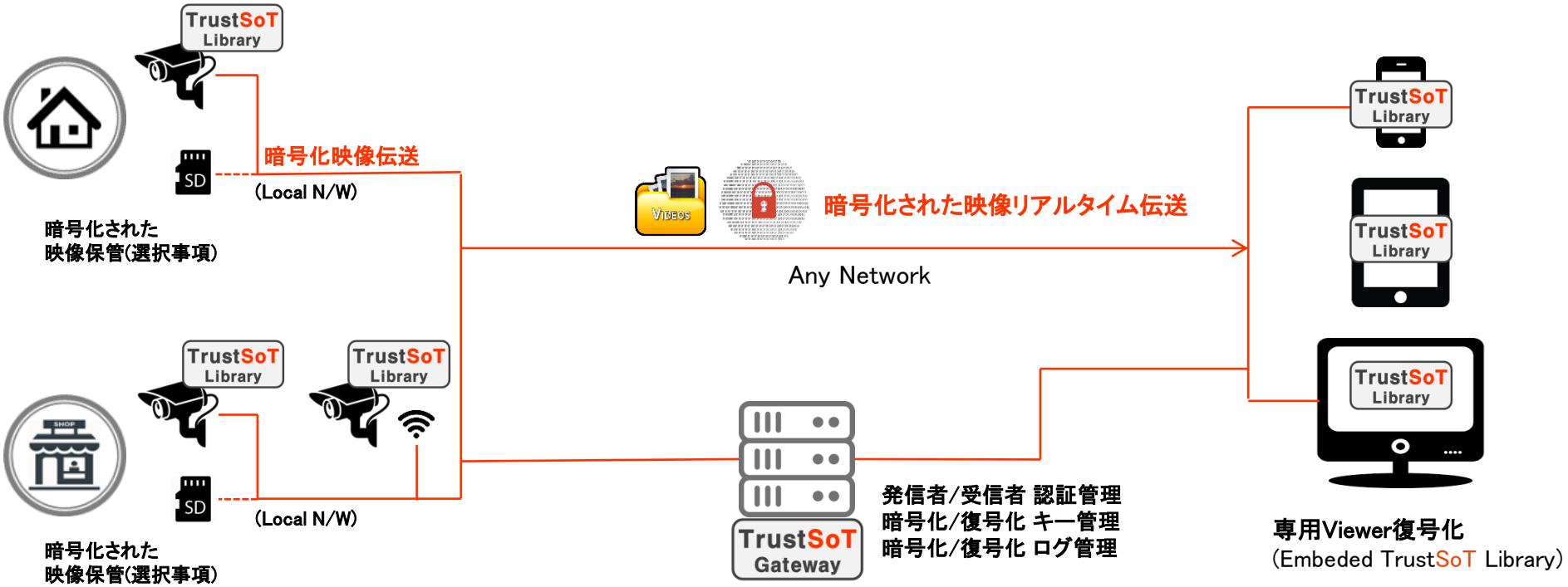
運営者 Server、Cloud 保管中の暗号化データはハッカーは勿論、運営者および公式的な確認手続きにも復号化不可

■ 主要機能

区分	機能
商用暗号化キーボード	□ メッセンジャー、メールをはじめ全ての文書とウェブ、そして生成データを暗号化 □ 暗号化データ共有時復号化ができるよう指定した対象(人、デバイス)のみ復号化可能 □ 復号化された回数、期間などを制限可能 □ 復号化権限キャンセル可能 (復号化権限が与えられたとしても復号化権限がキャンセルされたユーザーは権限キャンセル前、後の文章を復号化することはできない)
企業暗号化キーボード	□ 一般暗号化キーボード機能をすべて適用 □ キーボード入力/暗号化/認証ログ収集 □ キーボードが設置されたデバイスに対する一部監視 (スクリーンキャプチャ、悪性アプリケーション駆動監視など)
付加特殊機能	□ 暗号化文字列のイメージ化、RGB化 (保管、共有) □ 運営者提供 Open APIを活用、画面に出力されているメッセンジャー(LINE、SNSなどの会員自動認識)(復号化権限制御) **- 暗号化データクラウドサービス(バックアップ)でデータの安全な保管および復旧可能**

TrustSoT IMG (映像データ暗号化)

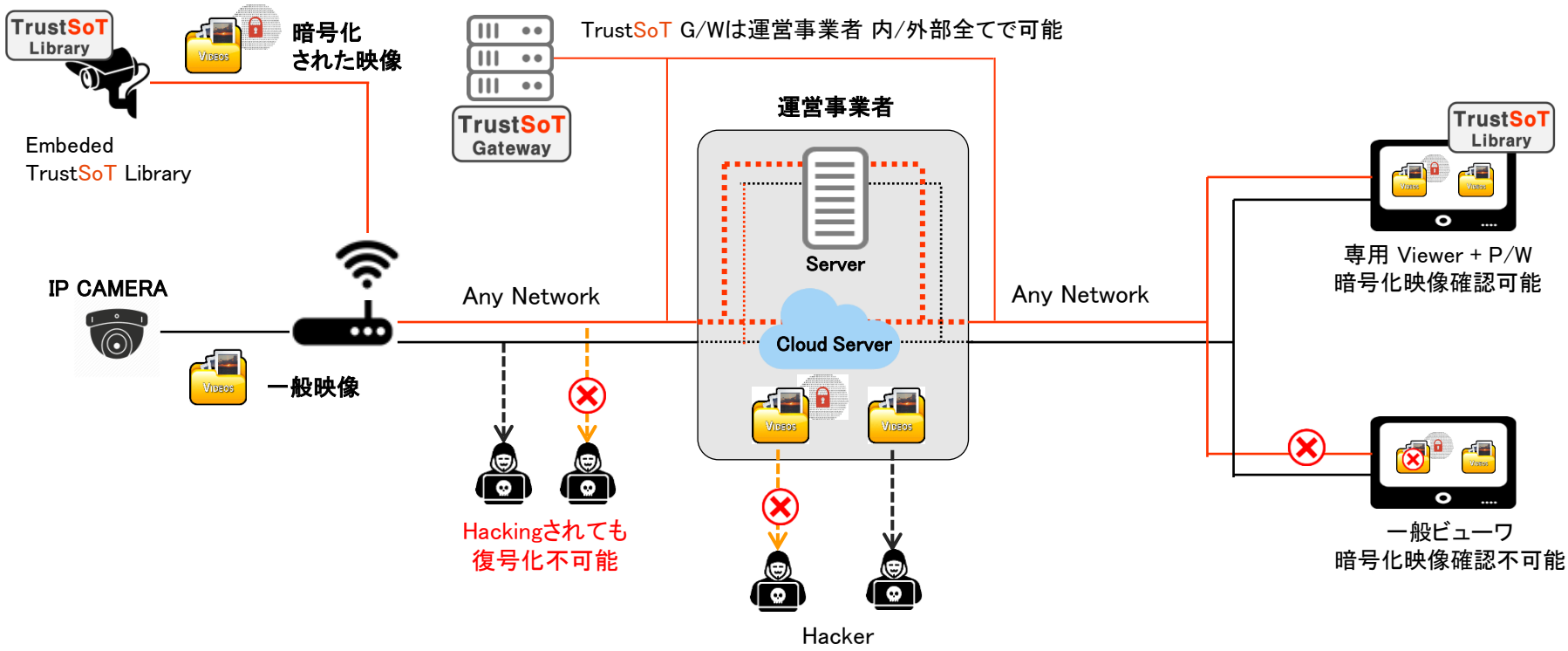
■ 「TrustSoT IMG」 Libraryが適用された CCTVカメラなど映像データ発生機器の映像データの発生時から暗号化が適用され
映像データが流出しても解読ができないよう、映像の不法盗用、コピー、流通が根本的に防止できます。



「TrustSoT IMGl」 User間 送受信暗号化映像はTrustSoT Gatewayでも復号化不可

TrustSoT IMG (映像データ暗号化)

TrustSoT IMG “Video & Image” Follow



運営者 Server、Cloud保管中の暗号化映像を盗用時にも復号化不可能
(保管中の一般メール盗用時内容確認可能)

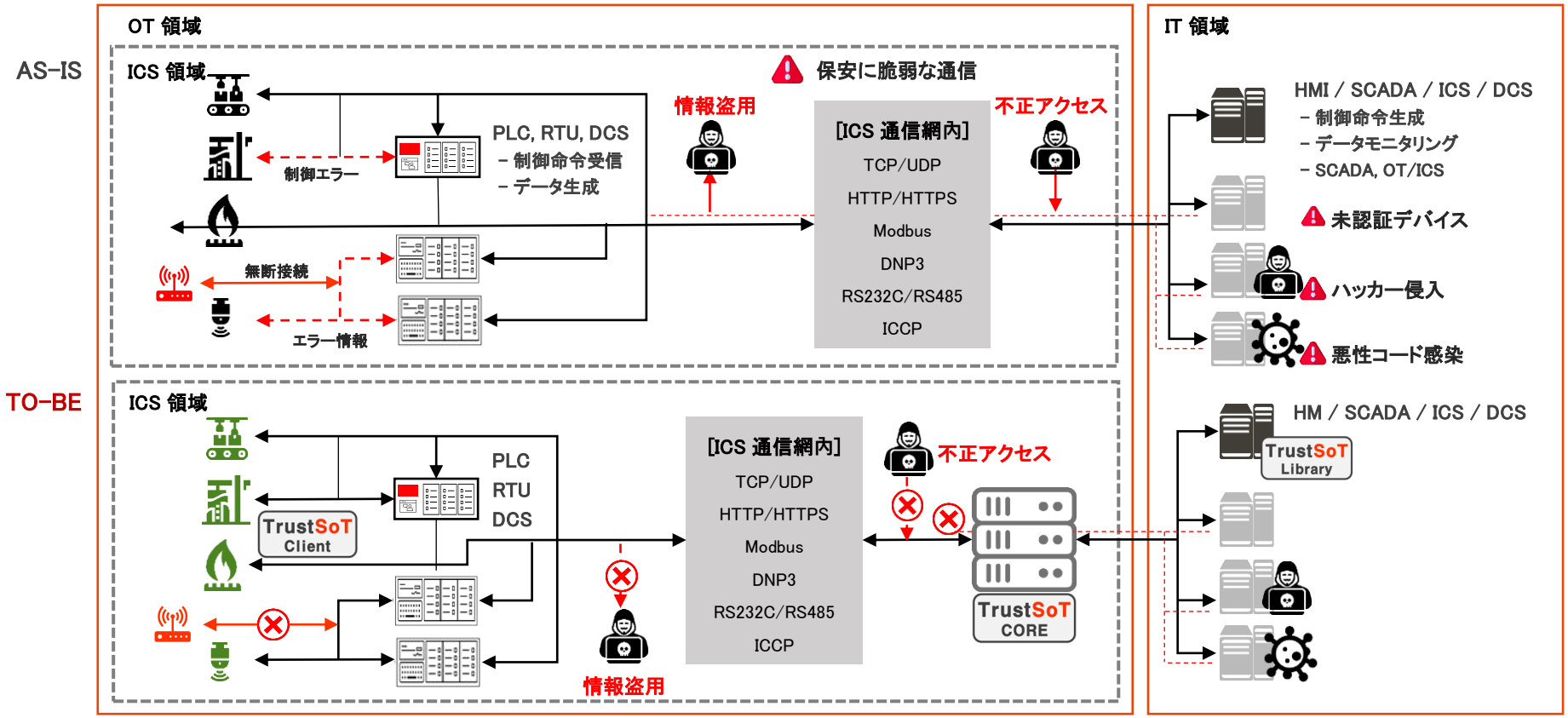
■ TrustSoT IMG vs 一般 CCTV 暗号化技術比較

区分	TrustSoT IMG	一般 CCTV 暗号化
伝送区間制約	■ 映像生成時即時 Header 暗号化 ■ データ伝送区間暗号化適用不必要	□ 映像生成時暗号化不可 □ データ伝送区間内 Header 暗号化
データ保存	■ 映像生成時即時 Header 暗号化および独自保管 ■ 通信断絶時にも限度容量内データ保存	□ 映像データ伝送時暗号化方式 □ 通信断絶時送出できなかった映像データ流失
データ保護	■ 可変型認証キー基盤端末機保安認証支援 ■ 可変型暗号化キーを通じリアルタイムで暗号化されデータが伝送されるためハッキング時にもデータ流出防止	□ IPまたはMACアドレス方式の基礎的端末機認証 □ 伝送区間内固定キー基盤 Header 暗号化方式で該当キー流出時データ保安不可
データ暗号化時点	■ CCTV 映像データ生成時から暗号化する唯一の軽量ソリューション(AES256 以上)	□ 映像生成時ではなく、伝送時に暗号化される方式

TrustSoT OT/ICS（産業制御信号/データ暗号化）

■「TrustSoT OT/ICS 」は、網構成(内部網/閉鎖網) 特性上機器制御とモニタリングに対する特別な保護対策がなく
各部分別に多様な保護体系が必要、既存のOT/ICS(産業制御) 分野に対し、発生する各種保安問題を解決するために
デバイス認証、データ暗号化およびイベント監視などを通じ制御分野を保護します。

■ TrustSoT OT/ICS “Control Signal/Data” Follow



Gateway および Module 主要機能

TrustSoT Slave Agent	TrustSoT Gateway	TrustSoT Master Agent
復号化キー要請	データ仲介(Proxy)	暗号化キー要請
制御命令復号化および確認	Master、Slave間 認証および接続制御	制御命令暗号化
認証書発行/破棄要請	(認証、暗号化)可変キー管理	認証書発行/破棄要請
データ生成、認証情報伝送	伝送データ分析モニタリングログ収集	データ認証情報確認
送信データ生成 / 受信データ分析		送信データ生成 / 受信データ分析

OT/ICS 部門での追加機能 : 悪性コード内部拡散防止機能

区分	Paloalto	Symantec ATP (Advanced Threat Protection)	TrustSoT
悪性コード感染後 内部拡散防止機能	× 公開/非公開悪性コード遮断	× 公開悪性コード遮断	○ 公開/非公開悪性コード 実行警報および内部拡散防止(**遮断**)
生成ファイル保護	×	×	○
ICS(産業制御) プロトコル支援	×	×	○
機器使用者監視	×	×	○
ファイル流出保護	○	×	○
主要機能	侵入遮断	侵入遮断	**拡散遮断 データ暗号化**

Hardtware

Security Camera (TrustSoT IMG 適用)

項目		仕様	項目		仕様
無線		IEEE802.11b/g/n	動作感知		動作が感知されると自動でON (感知距離5m)
映像出力		HD960P	レンズ		3.6mm/90° 視野角レンズ (Option : 2.8mm/120°)
圧縮方式		H.264	音声支援		遠隔双方向音声送受信機能
OS	スマートフォン	Android, iOS	消費電力		< 5W
	PC	Windows	電球数量	LED	25pcs
保管メモリ		2 ~ 64GB micro SD		赤外線	4pcs (Night vision 8~10m)
Back Up		Mobile, PC	ソケット		E27/E26/B22
レンズ解像度		1.3mega pixel	重量		280g
アラーム		動作感知、音、メッセージ、照明	仕様環境		-20° C ~ 50° C
保管時間		最大24日/ 64G micro SD	仕様電源		AC 100~250V

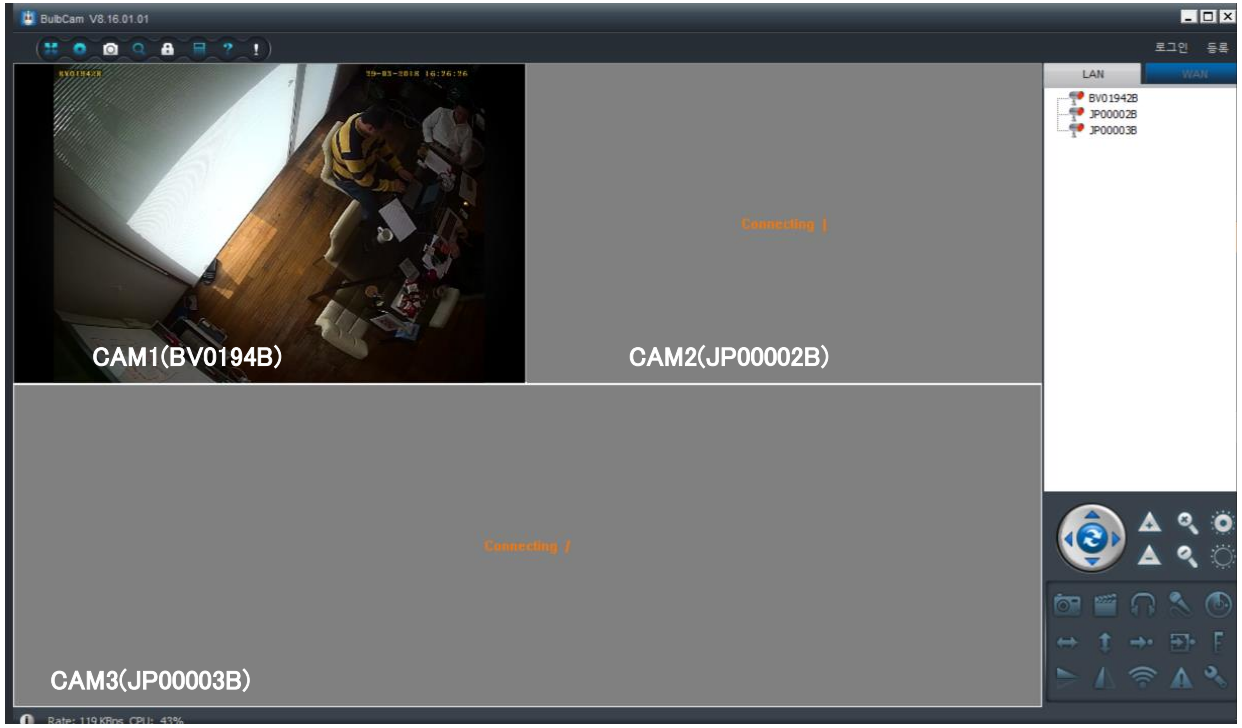
※ 本規格は製品導入検討過程で変更されることがあります。

IB-175W
[White Light]

IB-175Y
[Warm Light]

■ 一般ビューワ : TrustSoT Library 未適用 Camera “CAM1(BV0194B)”の映像確認可能
TrustSoT Security Camera “CAM2(JP00002B)”と “CAM3(JP00003B)”の暗号化映像確認不可能

■ 専用ビューワ : TrustSoT Security Cameraの暗号化映像確認可能 (復号化)



一般 Viewer (PC)

TrustSoT 専用 Viewer
(Android)

■ TrustSoT IMG 映像暗号化処理性能検査結果과

SoT 処理性能検証結果

測定①～暗号化(SoT G/W経由)・ローカル接続

PC時計	動画	差分	差分（平均）
15:50:53.277	15:50:52.119	00:00:01.158	
15:51:54.529	15:51:53.355	00:00:01.174	
15:52:55.836	15:52:54.685	00:00:01.151	00:00:01.172
15:53:58.118	15:53:56.944	00:00:01.174	
15:54:59.808	15:54:58.604	00:00:01.204	

測定②～暗号化なし(カメラ直接)・ローカル接続

PC時計	動画	差分	差分（平均）
15:58:01.560	15:58:00.387	00:00:01.173	
15:59:01.930	15:59:00.764	00:00:01.166	
16:00:03.291	16:00:02.132	00:00:01.159	00:00:01.166
16:01:09.404	16:01:08.238	00:00:01.166	
16:02:05.961	16:02:04.795	00:00:01.166	

結果 • 監視カメラ映像の暗号化／復号処理による遅延： 6ミリ秒

【参考】測定③～暗号化(SoT G/W経由)・インターネット経由

PC時計	動画	差分	差分（平均）
15:45:21.934	15:45:20.733	00:00:01.201	
15:46:23.730	15:46:22.523	00:00:01.207	
15:47:22.212	15:47:20.993	00:00:01.219	00:00:01.222
15:48:22.852	15:48:21.586	00:00:01.266	
15:49:24.069	15:49:22.852	00:00:01.217	

【参考】測定④～暗号化なし(カメラ直接)・インターネット経由

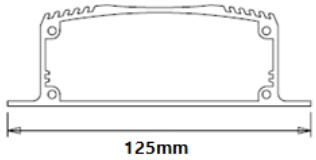
PC時計	動画	差分	差分（平均）
16:03:52.539	16:03:51.258	00:00:01.281	
16:04:55.657	16:04:53.992	00:00:01.665	
16:06:02.528	16:06:00.090	00:00:02.438	00:00:01.640
16:07:00.273	16:06:58.852	00:00:01.421	
16:08:04.168	16:08:02.773	00:00:01.395	

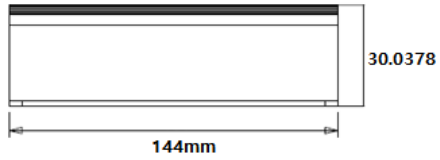
<結果考察及び備考>
- SoT経由（暗号化／復号処理）とカメラ直接間に堅調な遅延影響は認識できず。
- 取得結果にブレが生じている点は、ネットワークの品質もしくはカメラの映像配信処理にも依存している可能性がある。
- インターネット経由での測定は時間帯によるネットワーク遅延の要素が加味されるため、実使用時の参考までとする。

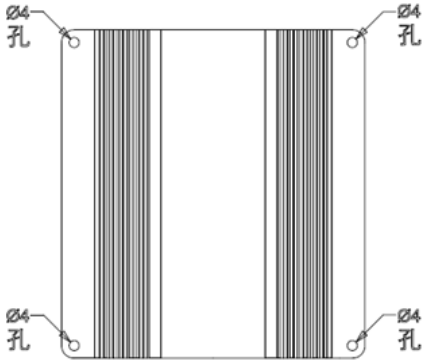
Security LTE Louter (TrustSoT CORE 適用)

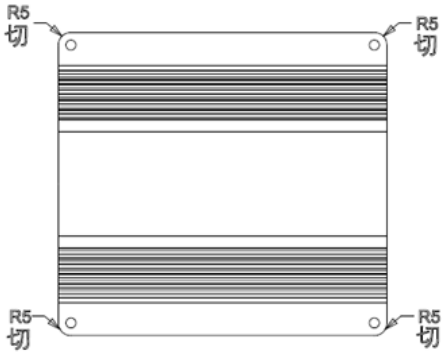
■ H/W	Indoor Type with PSE	Remark
CPU	ARM Cortext-A8 AM3352 (600MHz)	
Memory	512Mbyte	
Flash Memory	eMMC 4Gbyte	
LAN	1 x 10/100 Base-T With 35W PSE	
WAN	1 x 10/100 Base-T	
Wi-Fi	IEEE802.11 a/b/g/n 2.4G/5G Dual Band	
3G/LTE Dual Mode	M.2 Con. Support	
LTE Antenna	2dBi, 1T1R Dipole Antenna	
Status LED	1-LTE, 1-LAN, 1-WAN, 1-PWR, 1-WIFI	
USB 2.0	Host port 1	
Console	RS-232 Lite	RX,TX,GND
Surge Protection	10/700μs / 400W	
ESD Protection	Contact : ±8KV, Air : ±15KV	
Operating Temperature	-40 ~ 85℃	
Operating Humidity	10 ~ 90%	Non-condensing
Input Voltage/Current	DC 24V / 2.5A max Adaptor	
Power Consumption	<10W (35W / PSE 1port)	
Dimension	144mmx125mmx32mm	
Weight	< 380g (< 430g in case PSE)	

■ S/W	characteristics
VPN	Multi and Bonding Tunnel
	Split Tunneling
	IPsec, IKE Version 1,2
	Transport / Tunnel Mode
	Crypto Algorithms(3DES, AES123/192/256)
	Authentication Algorithms(MD5,SHA1,SHA2)
	Dead Peer Detection
	NAT Traversal
Firewall	Stateful packet Inspection
	Tuples direction/Type
	Static, Dynamic NAT
	Exclude, Double NAT
Network	Route Mode/ Multipath route
	Policy based routing
	QoS / DHCP Server, Relay
	DDNS/ LLDP
IPv6	IPv6 Routing/Firewall/Ipsec
	6 to 4, ISATAP
Management	SNMP v1/2/3
	CLI, Web UI
	Syslog
	System Firmware update function



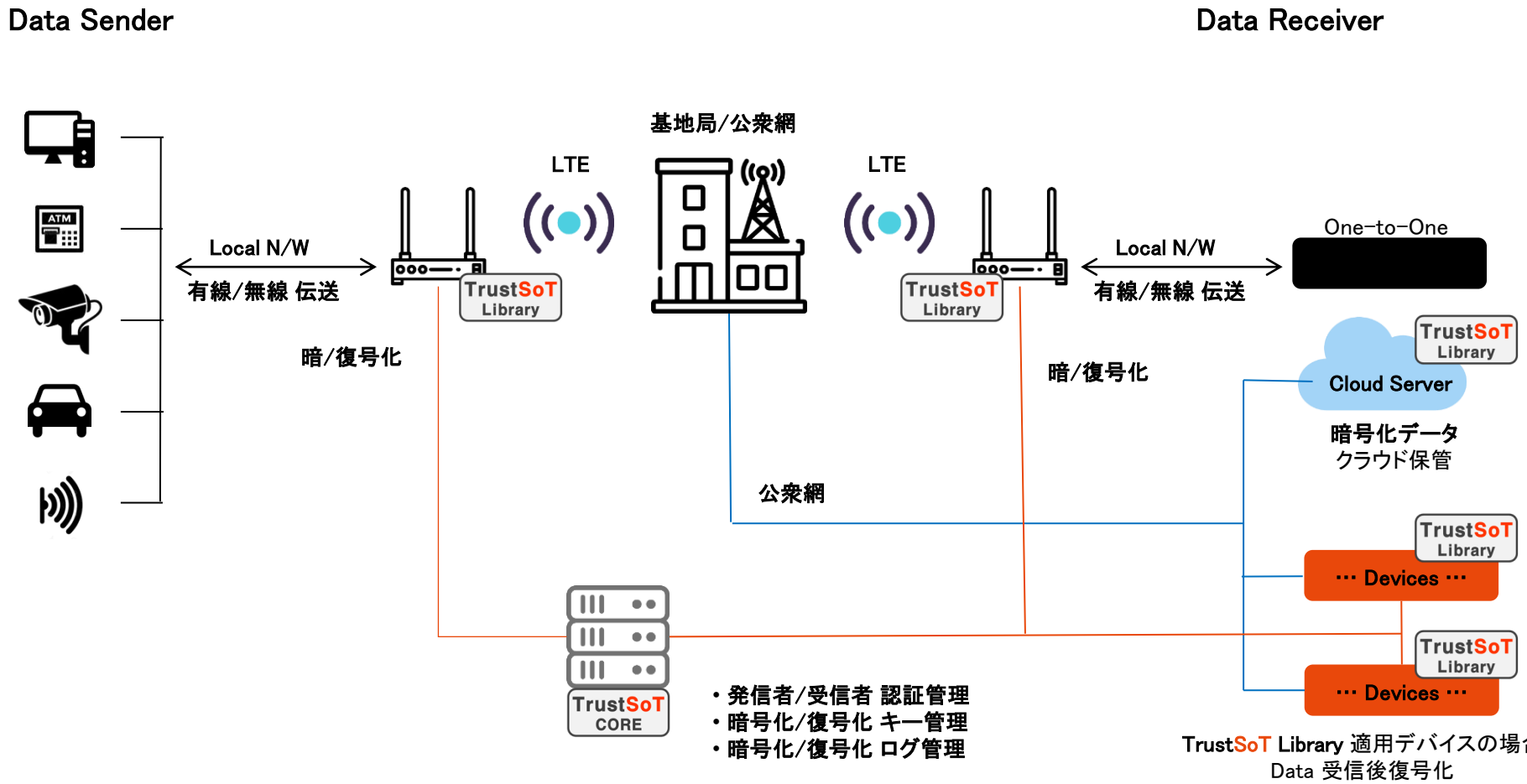






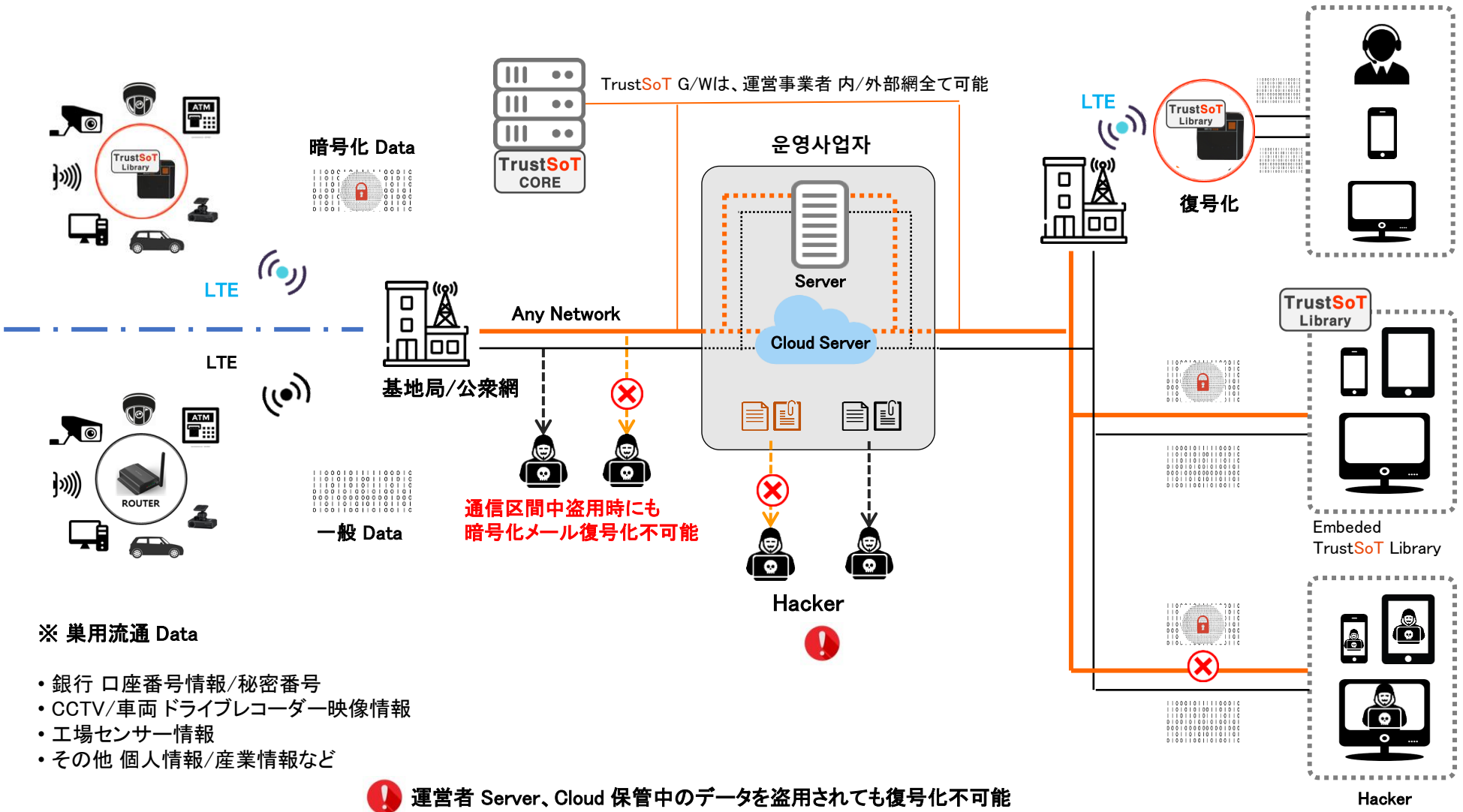
Security LTE Louter (TrustSoT CORE 適用)

■ 全てのDeviceで発生するDataを “TrustSoT LTE Router”を通じ LTE 伝送時、
公衆網やCloud サービスを適用しても Dataの暗号化伝送および保管が可能です。



Security LTE Louter (TrustSoT CORE 適用)

TrustSoT Security 4G Louter "Data" Follow



※ 巣用流通 Data

- 銀行 口座番号情報/秘密番号
- CCTV/車両 ドライブレコーダー映像情報
- 工場センサー情報
- その他 個人情報/産業情報など

運営者 Server、Cloud 保管中のデータを盗用されても復号化不可能
(保管中の一般メール盗用時内容確認可能)

TrustSoT SCADA/PLC Demo System S/W構成

区分	Linux	Windows
バージョン	Kernel 3.X 以上	7 以上
標準配布	Ubuntu 18.04, CentOS 7.6	Windows 7, Windows 10
具現環境	C/C++, Python 3.X, Shell script	C/C++, Python 3.X, C#
ライブラリー	GCC 7.1 以上	.NET 4.0 以上
開発ツール	一般的な開発ツール支援	Visual studio 2017 以上
データベース	Postgressql 11 以上	Postgresql 11 以上
パッケージング方式	単独実行およびDocker	単独実行およびDocker

TrustSoT SCADA/PLC Demo System H/W構成

区分	最低仕様	平均仕様	最高仕様
CPU	4Core	8Core	8Core
CPU architecture	Intel x86_64	Intel x86_64	Intel Xeon
Memory	8GB	16GB	32GB
SSD	256GB	1TB	1TB x 4EA(RAID)
N/W card	Ethernet 1Gbps 2個以上	Ethernet 1Gbps 2個以上	Ethernet 1Gbps 2個以上
Power Supply	2EA	2EA	2EA
Interface Port	USB 3.0	USB 3.0	USB 3.0
User	less than 1,000	less than 5,000	less than 10,000

TrustSoT SCADA/PLC Demo System

区分	構成
CPU	Siemens PLC 315-2 PN/DP
DI	Siemens PLC 321 (32Points)
DO	Siemens PLC 322 (32Points)
DIN Rail	Siemens DIN Rail for CPU 3xx
Power	Weidmuller 100~240V AC
Button	24V DC Input Push Button
Lamp	24V DC Output Lamp

※ Sofrware
Siemens Operation, Engineering and
TrustSoT encrypt communication library

Supply Performance

サムスン電子	サムスン重工業	サムスンSDS	サムスンコーニング精密素材
サムスン火災	サムスン生命	サムスン人力開発院	サムスン電子サービス
サムスン証券	サムスン物産	サムスンディスプレイ	サムスンコーニング アドバンスドグラス

Hana Bank	Hana Capital	Hana金融投資
Hana Card	Hana貯蓄銀行	Hana金融持株
Hana生命	Hana資産信託	Hana Members

中央報勲病院	大田報勲病院	韓国報勲福祉医療財団
仁川報勲病院	光州報勲病院	
釜山報勲病院	大岳報勲病院	