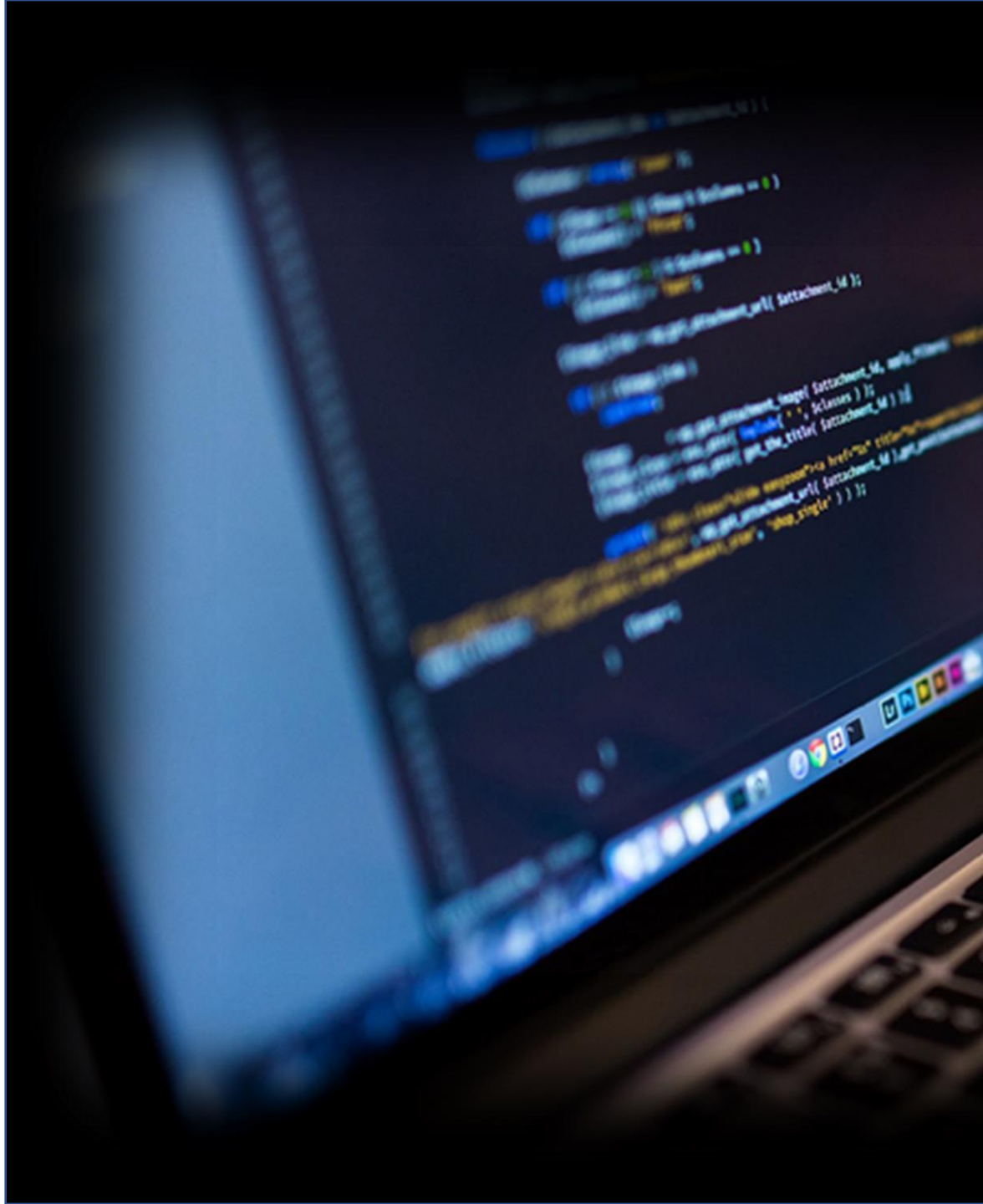
TrustSoT 概要

APT 保安（OT.ICS部分）

2022



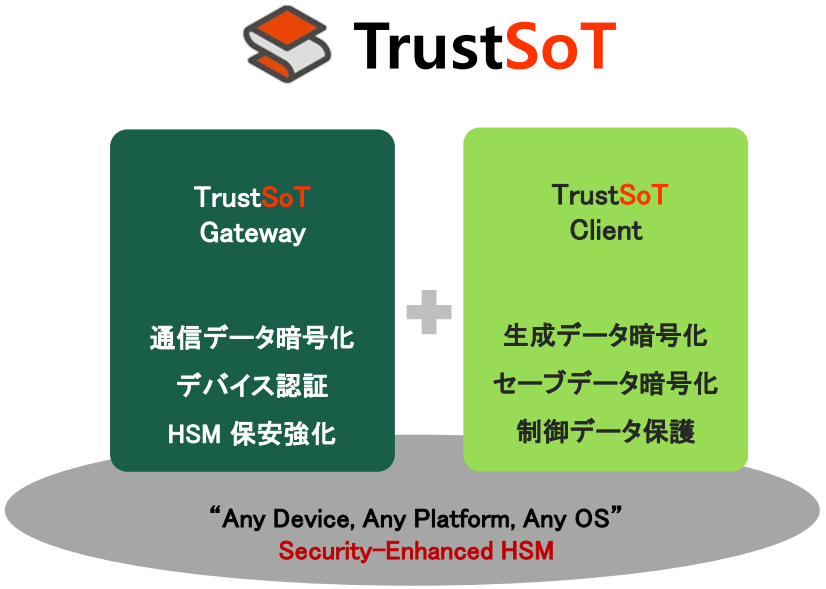
目次

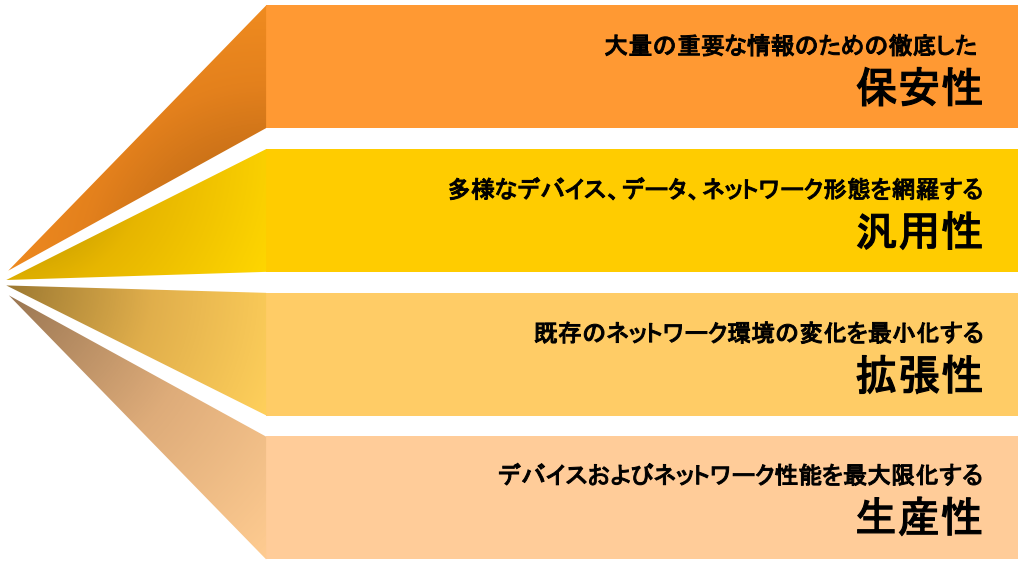
TrustSoT紹介

最小限の投資で次世代ネットワーク環境で保安性とインテグリティを実現

超軽量Cilent LibraryでIoT Devicesおよびセンサーまで認証と管理
データと制御指示の双方向暗号化

APT注)1 攻撃対応に最も効果的なソリューション

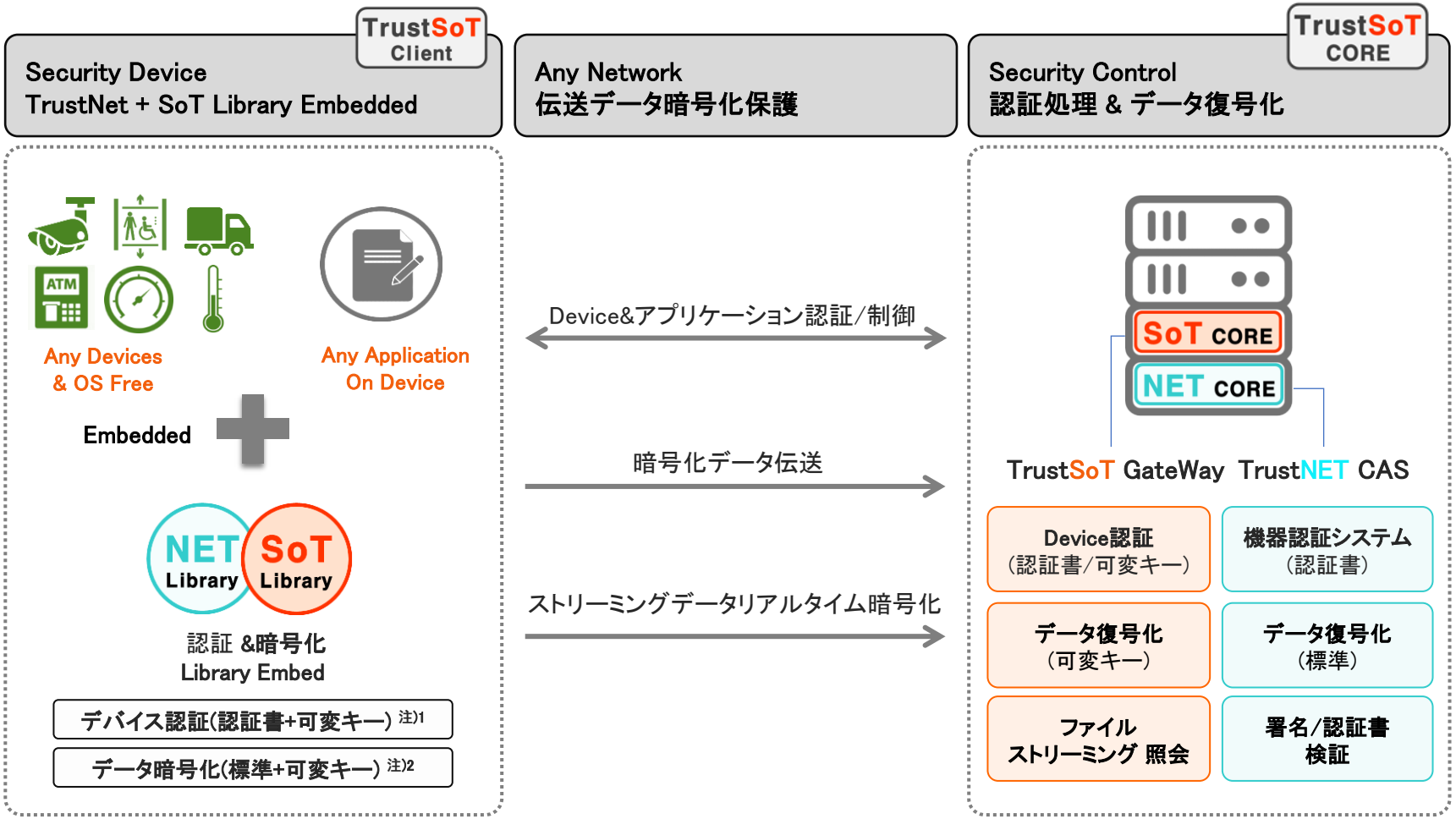




多様なデバイスおよびネットワーク形態で重要なデータに対する完璧な保護方法を提供

※ 注)1 APT : “Advanced Persistent Threats” 即ち, “知能的で持続脅威” (Chaper 2 参照)

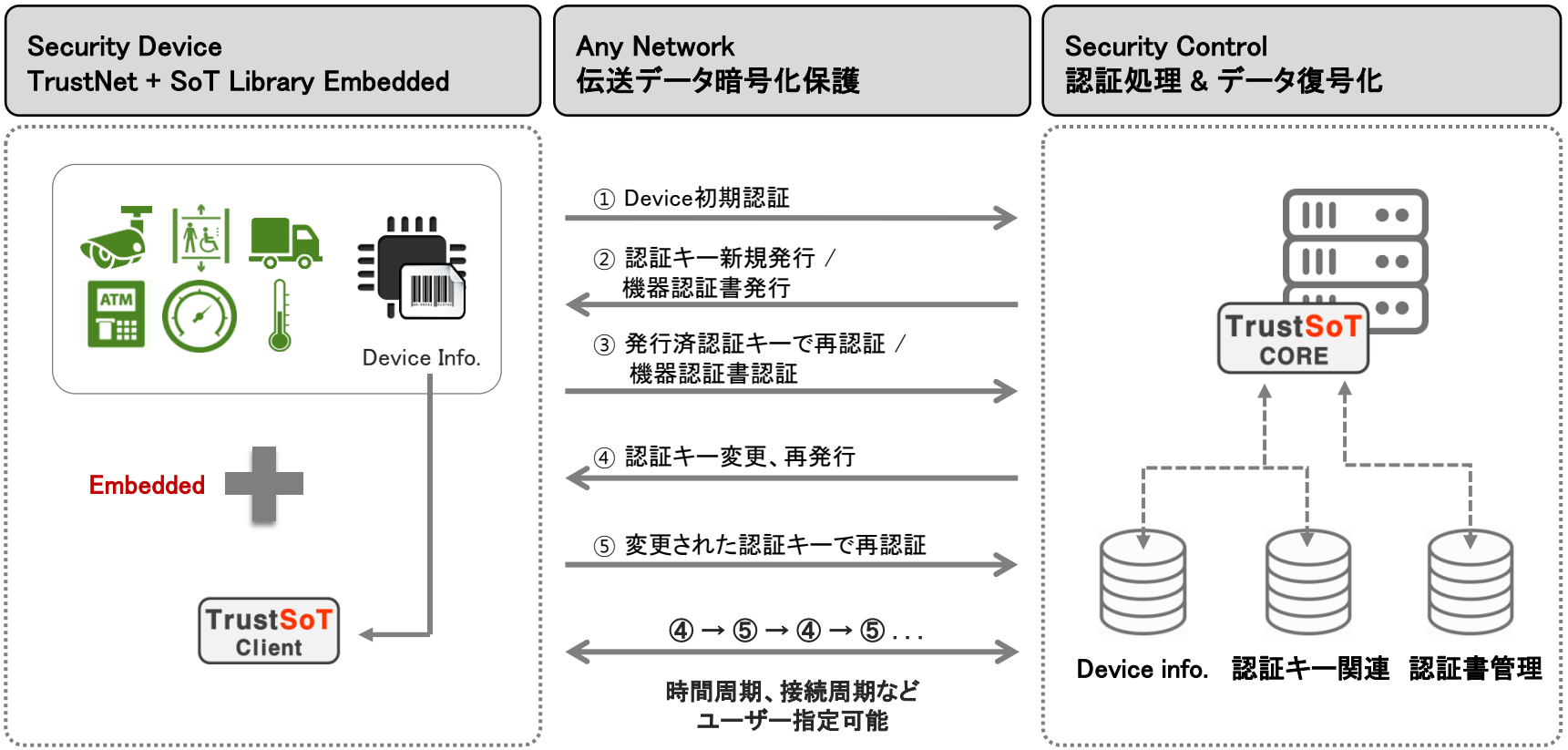
認証および暗号化



注)1 Page6 核心技術 “デバイス認証“ 参照
注)2 Page7 核心技術 “データ暗号化“ 参照

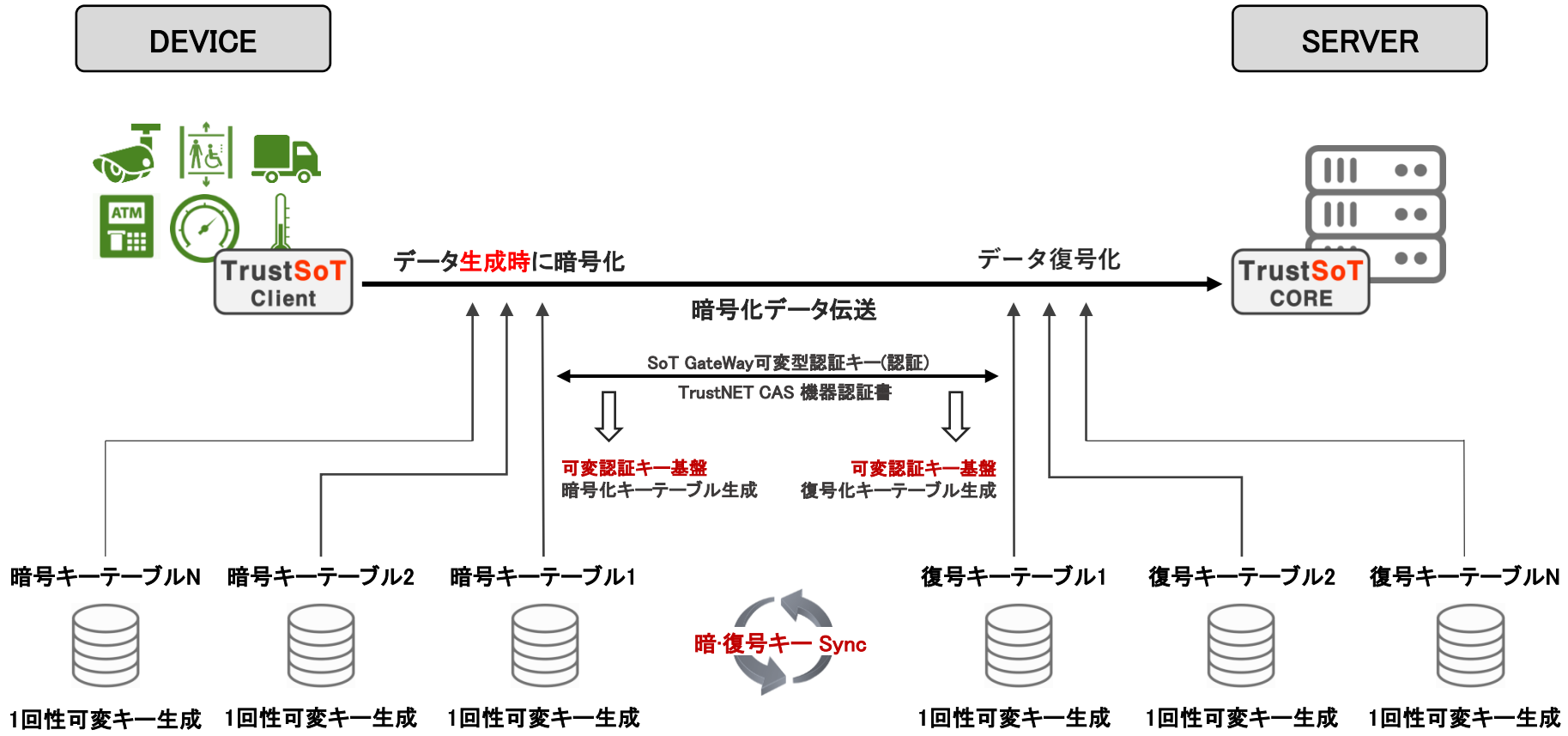
核心技術“デバイス認証”

- Trust NET & SoTが適用されDeviceはUnique(個別)に設定され、初期の認証後からは
  システムに接続時毎回新規認証キーの更新を受け認証信頼性を極大化(機器認証書サポート可能)



核心技術“データ暗号化”

- Trust NET & SoTは、
  データ生成時から1回性可変型暗号化キーを基盤としたデータ暗号化を遂行し伝送または
  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サポート）

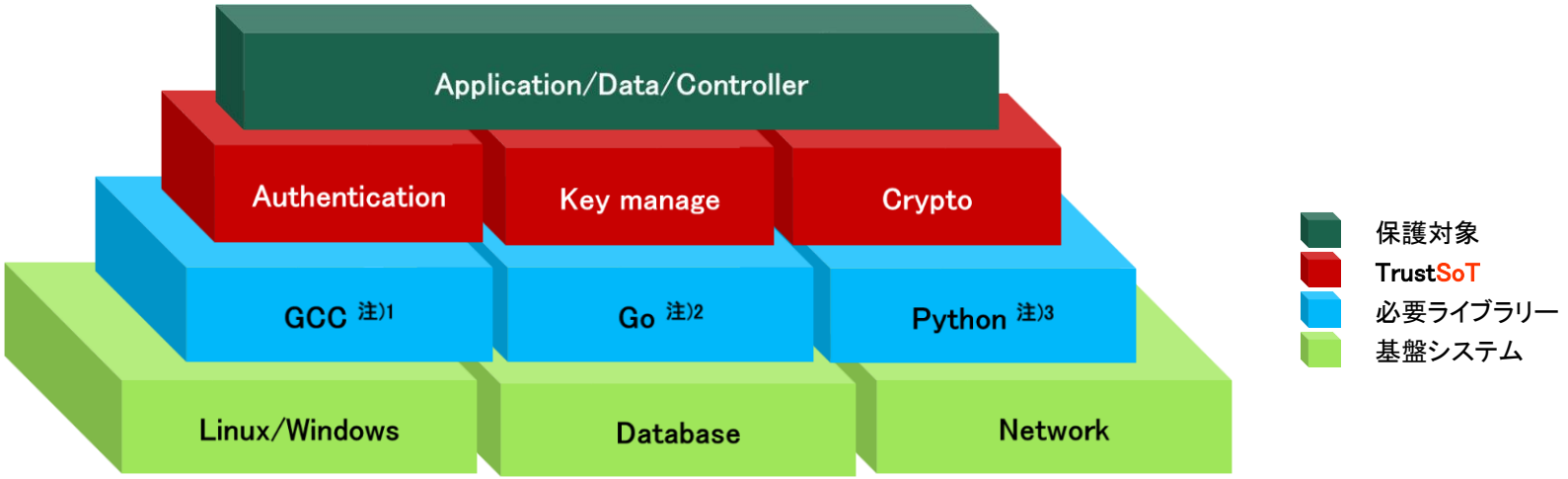


TrustSoT S/W

100%自社特許を基盤に100% 自社開発されたエンジンとライブラリーで構成されています。

韓国特許： 装置認証キーを利用したデータ暗号化方法およびシステム(第10-2028151号)

- 日本特許 第2017-563588号、アメリカ特許：16/603,339



[TrustSoT software Architecture]

注)1 GCC
C/C++ 言語ライブラリーで主に速度を要する各種データ処理などのために開発に使用

注)2 Go
ウェブ基盤ユーザー画面の開発言語 / 内部に Webのジャバスクリプターやhtmlが使用されるが核心運営言語はGo言語

注)3 Python
ログ分析収集と人工知能モジュールの適用などを担当 / 大部分のログ分析収集、人工知能モジュールがこのPythonで提供

S/W構成

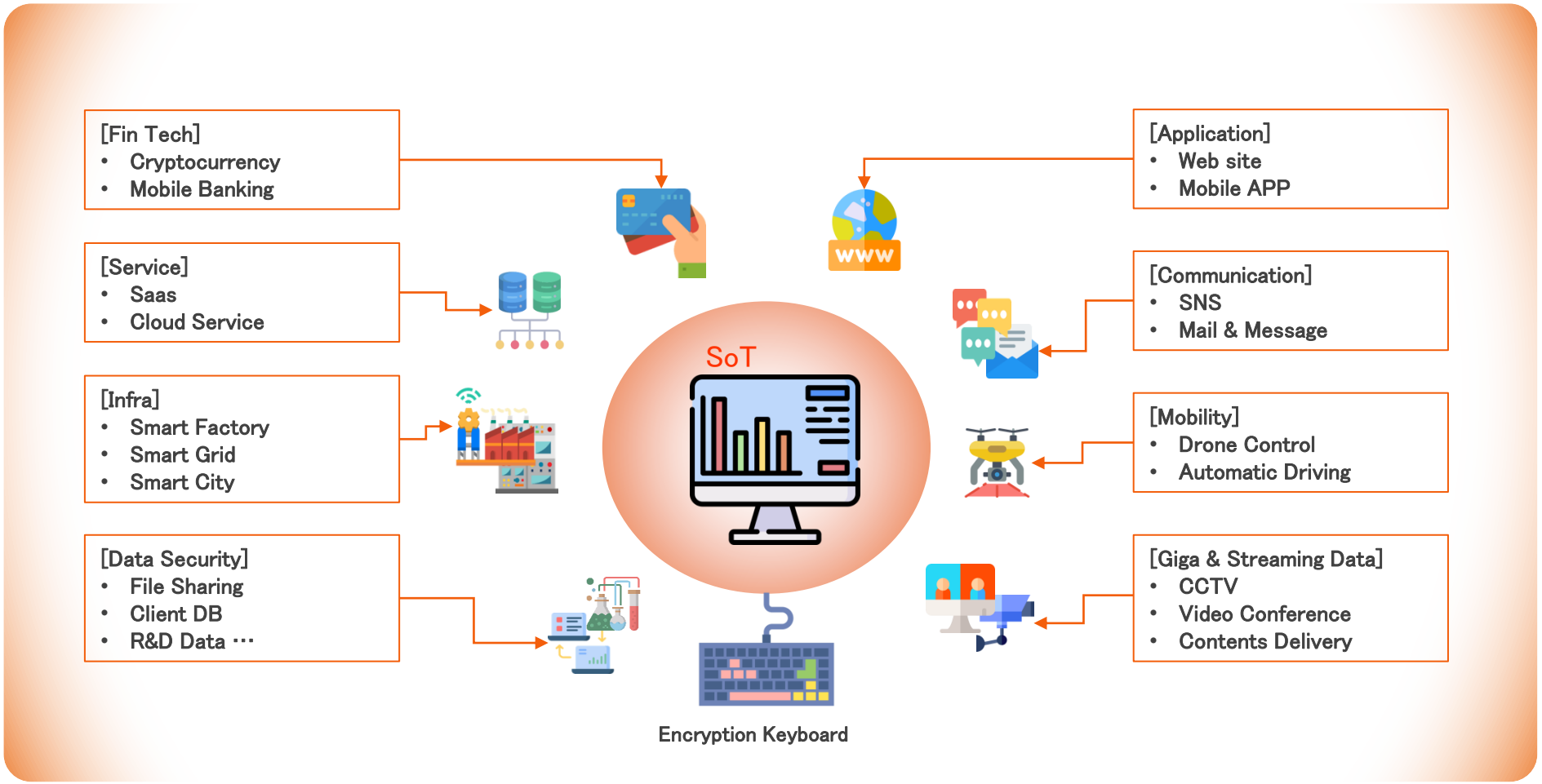
区分	Linux	Windows
バージョン	Kernel 3.X以上	7以上
標準配布版	Ubuntu 18.04, CentOS 7.6	Windows 7, Windows 10
具現環境	C/C++, Python 3.X, Shell script	C/C++, Python 3.X, C#
ライブラリー	GCC 7.1以上	.NET 4.0以上
開発ツール	大部分の開発ツールサポート	Visual studio 2017以上
データベース	Postgressql 11以上	Postgresql 11以上
パッケージング方式	独自実行およびDocker	独自実行およびDocker

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

適用分野

TrustSoTは全ての分野に適用可能で、
多様な形態のネットワークそして主要データと制御指示を暗号化し保護します。

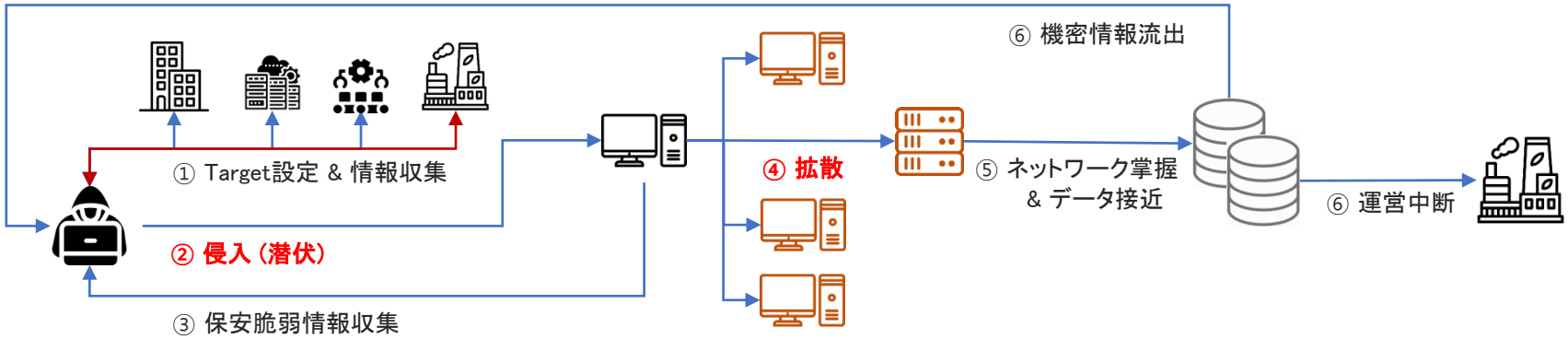


新しい保安環境

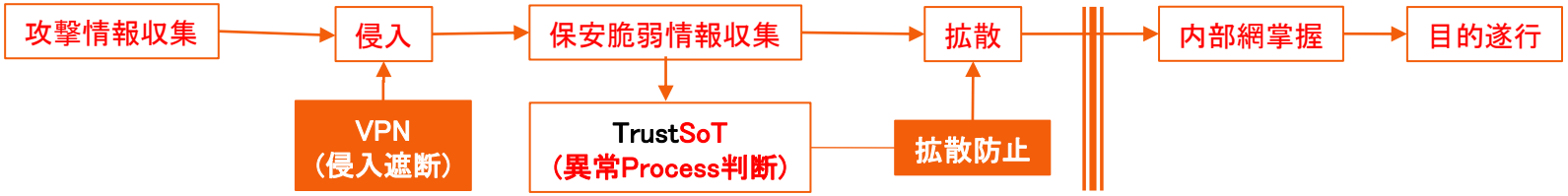
（APT：Advanced Persistent Threats）

PKI(SSL/TLS)、VPNなど大部分の保安ソリューションを無力化するAPT攻撃

- “Advanced Persistent Threats” 即ち, “知能的持続脅威”
- APT攻撃は過去の不特定多数を攻撃とは違い**特定対象を目標**に定め、目標の内部に侵入を成功させるまで多様な IT技術と攻撃方式を基盤とした多様な保安脅威を生み出す**攻撃を持続**
- 内部に**侵入**後、拠点を作り収集された**保安脆弱点を利用**し内部の正常システム(PC、サーバなど)まで**拡散**
- 内部システム掌握後機密情報収集、運営中断、システム障害など **侵入目的を遂行**
- 近年大部分のハッキングの手段として、特に PKI、VPNの脆弱点を攻略



“TrustSoT”と“VPN”は、相互補完体制を構成時APT攻撃に対する完璧な保安ソリューション実現可能



（page23 “TrustSoT & VPN 相互保安としての役割” 参照）

APT 攻撃と既存の悪性コード攻撃の相違点

既存の悪性コード攻撃と違うAPT攻撃の代表的特徴

① Advanced（知能的）

② Persistent（持続的）

③ Motivated（動機）

④ Targeted（目標）

区分	悪性コード攻撃	APT 攻撃
攻撃分布	無差別大量発信	緻密に組織化された計画
攻撃対象	無差別不特定	政府機関、団体、企業
攻撃頻度	一回性	持続性
攻撃技術	悪性コードデザイン	高度の知能的保安脅威を 同時に利用
探　知　率	1ヶ月以内発見時99%探知	1ヶ月以内に発見されても10%以下
攻撃結果	悪性コード感染、個人情報流出	機密資料流出、システム作動不能、 社会基盤施設麻痺

ITとICSの環境比較

- **IT**(Information Technology)　：インターネットなどオープンネットワーク等を活用した情報通信技術
  OT(Operational Technology)　：産業用機械や工程運営のための技術、過去閉鎖網内で運営されていたが徐々にオープンネットワーク領域に拡大
  ICS(Industrial Control System)：各種機械類と工程を制御するシステム、閉鎖網内で運営、専用ハードウェア/運営体制/ソフトウェアなど
  大部分が専用規格を使用して**保安に対して低い認識**

区分		IT	ICS
H/W	装備構成	標準装備(PC、サーバ)	**標準装備、工程特化装備**
	構成変化周期	短い	**変化はほとんどない**
	パッチおよび保守	性能向上のため頻繁に発生	**可用性を理由にほとんどない**
S/W	運営ソフトウェア(OS)	汎用OS	**制御機器(Windows) 制御対象(カスタマイジングEmbedded OS)**
	主な使用ソフトウェア	業務用商用および独自開発	**カスタマイジングされた商用および独自開発**
	アップデート周期	機能エラーと保安パッチ頻繁に実行	**機能エラー以外保安パッチなし**
保安	保安目的	重要データ流出とサービス中断遮断	**生産および工程中断可能性遮断**
	保安事故影響	流出データの重要度による被害	**生産および工程中断の直接的被害**
		法的問題および会社信頼度に影響	**製品に対する信頼性被害**

OT/ICSに対する主要APT脅威経路

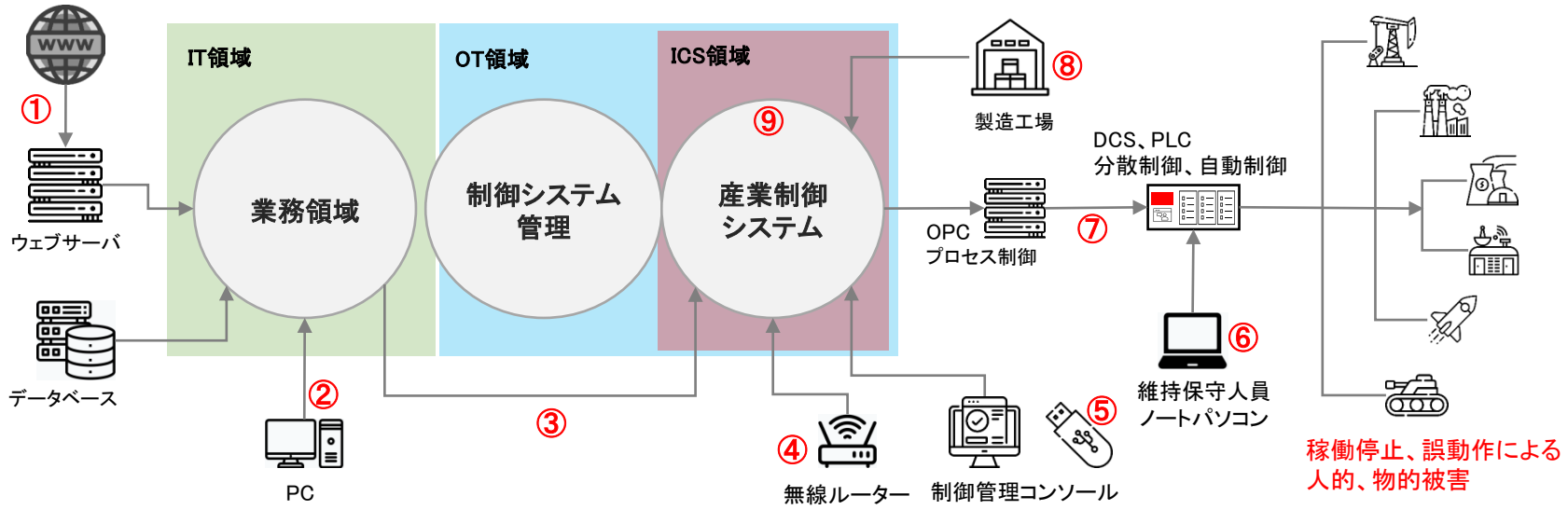
ネットワーク網領域区分

- 従業員が業務を行うIT(業務)領域
- 製品生産を行うOT(制御システム管理)領域
- 製造工程を制御し製品を生産するICS(産業制御システム)領域

多様な保安脅威

- IT保安脅威(ハッキング、悪性コード感染、APT攻撃)
- 業務領域に優先侵入し内部情報を収集後ICS領域を攻撃
- 不法的なICS領域侵入による攻撃

	APT脅威経路	TrustSoT
①	ハッキング、APT攻撃などIT保安攻撃	
②	悪性コード感染後網内拡散	○
③	業務網から ICS網に非認可連結悪用	
④	ICS網内無線認証迂回および脆弱点攻撃	
⑤	USB 利用、悪性コード拡散、重要情報流出	○
⑥	外注/維持保守人員の感染されたノートパソコン	○
⑦	制御指示の偽変造およびプロトコル情報流出	○
⑧	製造会社沿革維持保守チャネル悪用	○
⑨	端末ネットワーク障害(二重化未適用)	



※ 対応策 : Chapter3 “TrustSoTのOT/ICS APT攻撃対応” 参照

OT/ICS分野のAPT攻撃に対する脆弱点

OSアップデート(保安パッチ) カバー不足

大部分の産業分野で**OSアップグレード(保安パッチ)を行うわず運営中**

- 原因1) 閉鎖網(独立網)状態での長期運営という特性上**保安パッチでカバーできず**
- 原因2) 産業制御特性上リアルタイム成果、中断無しの運営という原則でパッチ過程の問題発生時**運営中断の事態懸念**
  特に、**SCADAプログラムはWindowバージョンで、Window OSの場合アップグレードを通じ保安パッチが必須**

※ 韓国Daily Secu紙 (2021.02.14)

- アメリカ フロリダ 水質処理施設に対するサイバー攻撃の細部情報公開
- 水質処理場のSCADAシステムに遠隔でアクセスし上水道の**水酸化ナトリウム投与量を危険な水準まで引き上げる攻撃**
  (現状を発見した担当者の処置で解決)
- 侵入方法 : 制御システムに連結し工場のPCの1台に設置されたTeamViewer ソフトバンクを通じSCADA(Supervisory Control and Data Acquisition) システムにアクセス
- 脆 弱 点 : アップグレードされないWindows7 運営体制の32ビットバージョン使用(**2020年1月14日 以降アップデート中断**)
  遠隔アクセスのため**同じパスワードを内部で共有**
  ファイアウォール保護機能未設置
- 解 決 策 : ソフトウェアを含めたPC、装置および応用プログラムをパッチおよび最新状態に維持
  強力なパスワードで2段階認証使用

※ TrustSoTの対応 (page18～22 参照)

対応1) OSアップグレードとは関係なく Client PC, Server(Scada)で発生する全てのポートおよびパケット監視後異常徴候時アラームまたはネットワーク遮断

対応2) ID/PW共有または奪われたとしても認証を受けた端末機以外からの接近遮断(制御指示不可)

APT主要攻撃事例

☐ **3.20 電算網障害** – 韓国

- ウィルス会社のアップデートサーバ迂回侵入、1年以上潜伏後攻撃開始(北朝鮮)
- ブーティング領域破壊で電算網障害(PC、ATMなど約48,000台システム障害)
- TV局(KBS, MBC, YTN) / 銀行(Shinhan Bankなど)

☐ **平昌オリンピック開幕式攻撃** – 韓国

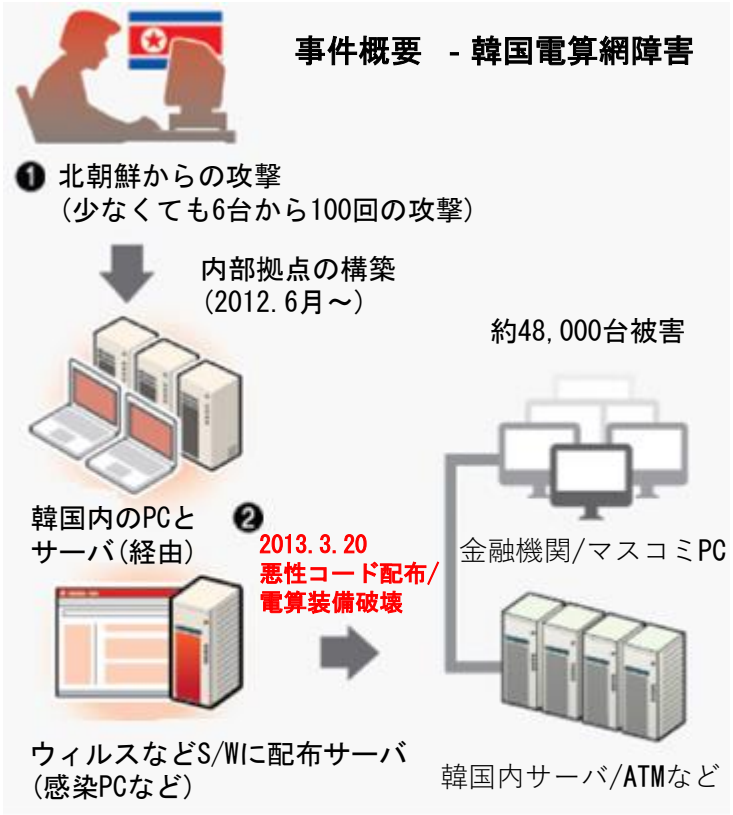
- 2018年2月 9日 午後 8時の開幕式をターゲット、核心サーバ50台破壊
  . 開幕式1ヶ月前オリンピック運営本部電算室ルーターハッキング後PC 300台感染
  44個のアカウント情報奪いサーバ接近権限確保
- オリンピック関連ウェブサイト障害、オリンピック現場WiFi中断、メディアセンター IPTV中断、8時以後チケット販売中断(開幕式空席発生)
- ロシア海外偵察局(北朝鮮に偽る)

☐ **Colonial Pipeline 稼働中断** – アメリカ

- ランサムウェア攻撃、ロシアのダークサイド(DarkSide)推定
- 300万バレル/日 送油管障害、供給問題発生、油価格 5~6% 上昇

☐ **Stuxnet** – イラン

- **シーメンスSCADAシステムを目標に製作**された精巧で**軍事的水準の悪性コード**
- 原子力、電気、鉄鋼、半導体、化学など主要産業基盤施設の制御システムの誤作動発生
- 2010年7月 イラン原子力発電所作動妨害 (シーメンス SCADA システム)



TrustSoTのOT/ICS APT攻撃対応

APT 攻撃に対する“監視および探知”および “ネットワーク遮断(技術的防御)と危険警告(管理的防御)”

TrustSoTは、全てのルートのAPT拡散経路を監視および探知し異常徴候発見時遮断および警告

[監視および探知]

☐ Client

- 行為機関分析 : TrustSoT Agentは外部から受信される全てのファイルに対し
  該当ファイルが実行される時、異常 Process、Patternなどのイベントを監視

☐ Network

- Port Scanning : IPとPortで発生する異常 Service 監視
- Traffic Analysis : Trafficの増減に対する異常パターン監視

☐ Server

- 保安情報/イベント管理(SIEM) : 収集された異常徴候Dataに対する分析で事前処置実行
- Log分析 : システムログおよび Timelineなどを構成し攻撃監視
- 未認証 Clientの接近監視(ID, Passwordなどユーザー情報と関係なく未認証Clientに対し遮断)

[遮断および警告]

☐ 上記攻撃対象に対する異常徴候をリアルタイム監視および探知し、異常徴候発見時該当Clientから感染データが拡散されないよう
ネットワーク遮断および感染内容警告

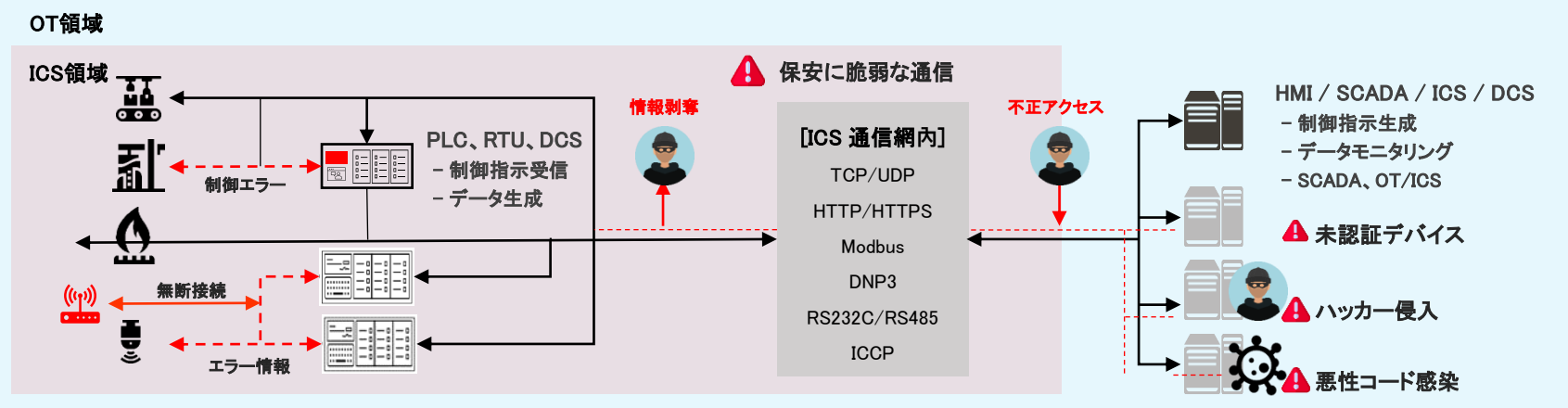
※ APT攻撃に対する現在の対応状況

- 2019年からAPT攻撃に対する警告を継続発動されてはいるが現在防御ソリューションはメールに添付されたファイルを実行時警告メッセージ、
感染事例分析を通じたウィルス開発だけであることが確認された (KISA : 韓国インターネット振興院意見)

OT/ICS保安に対するTrustSoT

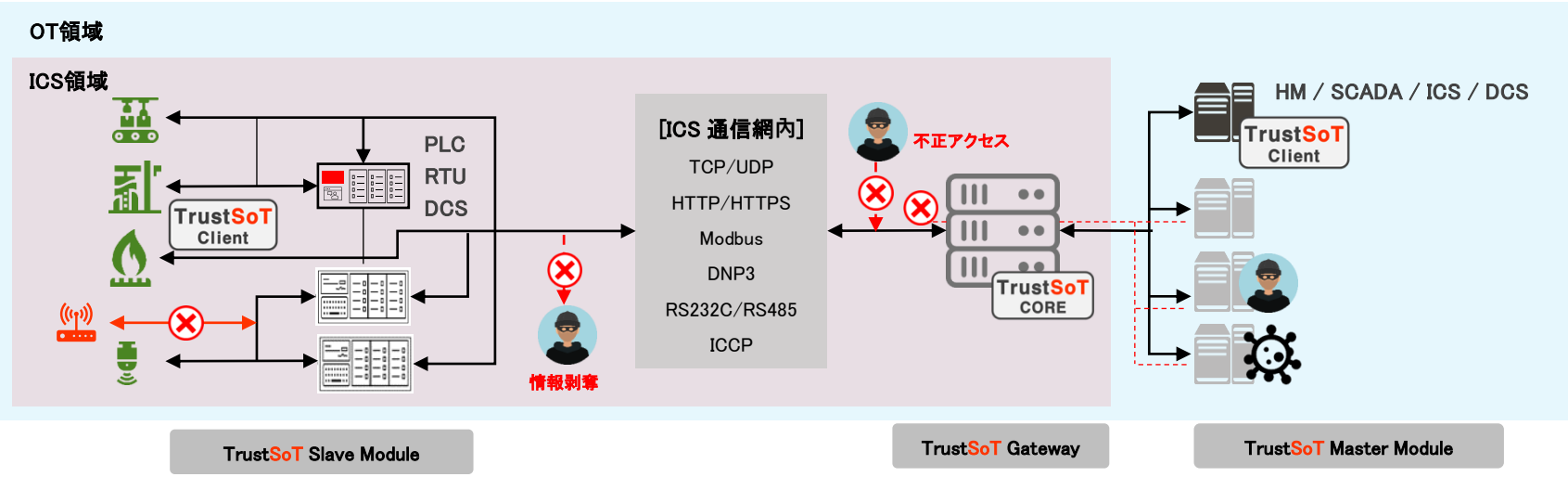
AS-IS

既存OT/ICS(産業制御)分野の構成は
内部で行われている機器制御とモニタリングに対し保護策がなく各部分別に多様な保護体系が必要



TO-BE

OT/ICS(産業制御)分野で発生する可能性のある各種保安問題を解決するため
TrustSoTは、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



GatewayおよびModule主要機能

TrustSoT Slave Module

復号化キー要請
制御指示復号化および確認
認証書発行/削除要請
データ生成、認証情報伝送
送信データ生成 / 受信データ分析

TrustSoT Gateway

データ中継(Proxy)
Master , Slave間認証および接近制御
(認証、暗号化)可変キー管理
伝送データ分析モニタリングログ収集

TrustSoT Master Module

暗号化キー要請
制御指示暗号化
認証書発行/削除要請
データ認証情報確認
送信データ生成 / 受信データ分析

SMART FACTORY DEMO SYSTEM (with SIEMENS)

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

“SIEMENS Korea” 検証実施 : SIEMENS PLCを活用した “制御データの暗号化” および “受信側の復号化”を通じ制御データの安全な保護および正常制御動作確認(SIEMENS Korea 技術チームおよび営業チーム確認)

TrustSoT vs. 他社ソリューション

既存APT保安ソリューションが悪性コードの**設置(侵入)に対する防御に集中**する一方
TrustSoTは感染された機器から**拡散防止と重要データの保護(暗号化)に集中**し他社製品に比べ差別化/優位性を確保

区分	Paloalto	Symantec ATP (Advanced Threat Protection)	TrustSoT
URL基盤悪性コード侵入防止	○	○	×
Email 悪性コード感知	○	○	×
Network 攻撃防御	○	○	△ 装備ポート監視
悪性コード感染後自防配布	× Application 基盤監視 政策樹立(許可、遮断など) 公開/非公開悪性コード遮断	△ 発見された悪性コードに 対する防御	○ プロセッサ監視 公開、非公開悪性コード 実行警報および遮断
生成ファイル保護	×	×	○ Agent基盤ファイル実行イベント監視
ICS(産業制御) プロトコルサポート	×	×	○
機器ユーザー監視	×	×	○
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**

TrustSoT & VPN相互保安としての役割

保安Solution別機能

Solution	機能
PKI	通信区間の接続と通信区間暗号化のためのソリューション
VPN	仮想のPrivate Networkを具現し、保護されているネットワーク網に**外部からの接続を不可能**にするソリューション
TrustSoT	通信区間の接続に対する制御だけ可能な PKI、VPNとは違い **Application Levelで認証と暗号化**を通じ ネットワークに連結する機器やソフトウェア**内部からの保安**を提供

保安ソリューション別保安脅威に対する対応可能可否

攻撃累計	比率	PKI	VPN (Network基盤)	TrustSoT (Device基盤)	TrustSoTの対応方法
文書基盤 **悪性コード配布**	90%	×	○	○	認証を受けた機器とユーザーが認証を受けたアプリケーションにより 生成された文書なのか確認 (**監査時の拡散遮断**)
悪性コードによる **DDos 攻撃**	3%	○	○	△	**認証を受けた類型のパケット**以外の遮断 (サービス中断防止)
バックドア基盤 **不法侵入**	2%	×	○	△	**認証を受けたデバイス**と特許暗号化技術を通じ 暗号化されたデバイスだけ接近可能
ファイル/データ剥奪	2%	×	○	○	ファイル、データ別に可変キー基盤認証暗号化で 各暗号化別に 他の情報に暗号化され **認証機器とユーザーだけ復号化可能**
産業用制御など **各種プロトコル偽/変造**	1%	×	×	○	プロトコル生成時データに対する暗号化および 受信先の復号化時**認証とプロトコル分析遮断**

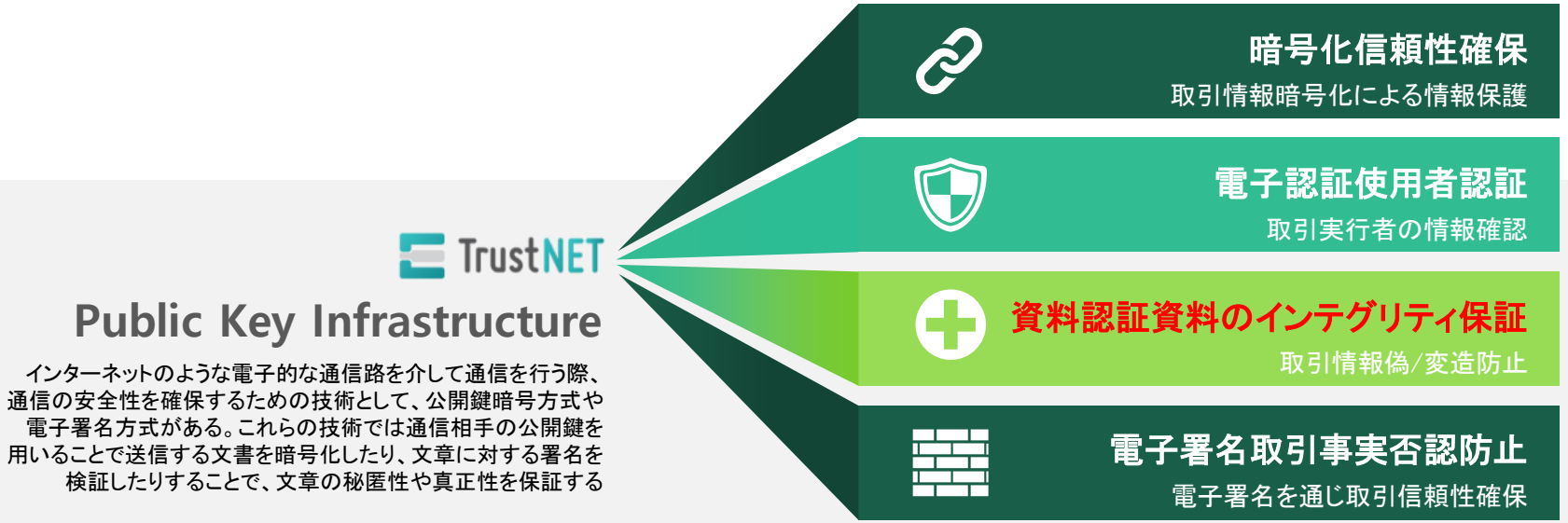
保安ソリューション別機能

区分		機能	説明
TrustSoT	Gateway （管理機能）	認証	ユーザー、デバイス、アプリケーションおよびデータとファイルに対する認証および接近制御
		暗号化	ユーザー、デバイス、アプリケーションから生成されるデータ暗号化のために 暗号化モジュールおよび暗号化キー運営
		Client制御	TrustSoT Agent, TrustSoT SCADAなど専用クライアントの実行、接近制御
		ログ	各種ログ収集およびモニタリング
	Workstation （一般業務）	暗号化	指定ファイルとデータ暗号化
		プロセス監視	デバイスの実行プロセス監視、通報および遮断
		イベント監視	デバイス OSの発生イベントの監視、通報および遮断
		通信監視	指定ポート以外のポート監視通報および遮断
	ICS （制御ネットワーク）	制御指示保護	制御部からのPLCに伝達される制御指示認証/暗号化
		プロトコル監視	指定されたプロトコル以外のプロトコルの送受信遮断
		接近制御	認証されたユーザー、デバイスおよびアプリケーション以外の制御ネットワーク遮断
		状態管理	連結された制御ネットワークの各種装備とOSに対する状態モニタリングおよび管理情報提供
TrustNet		PKI	公開鍵基盤認証ソリューション
		KMS (HMS)	S/W(H/W) 方式のキー管理ソリューション
		公式認証暗号化モジュール	韓国政府から認証を受けた暗号化モジュール(KCMVP)

TrustNET紹介

PKI

公開鍵基盤(Public Key Infrastructure)、インターネット上の取引の秘密を維持しながら取引当事者達情報を確認できるセキュリティ技術、
クライアント用プログラムの設置を行わず公開鍵暗号方式の認証発行が可能



提案背景

Needs

分散システム環境でのデータ交流を通じビジネス活性化による情報保護の必要性が高まり、多様な通信環境および端末機を通じた情報交流は常に情報流出の危険性を秘めています。

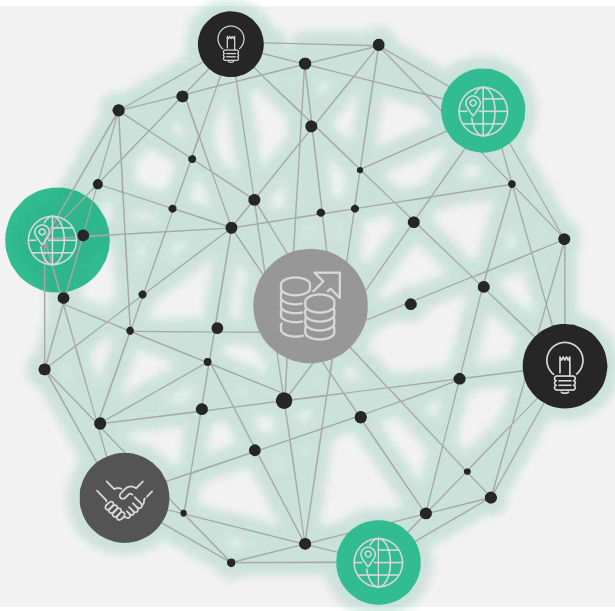
安全な情報交流を通じビジネスの活性化をためにはデータのインテグリティおよび機密性が保障されなければならず拡張性を容易にすることができるセキュリティインフラが必要である。

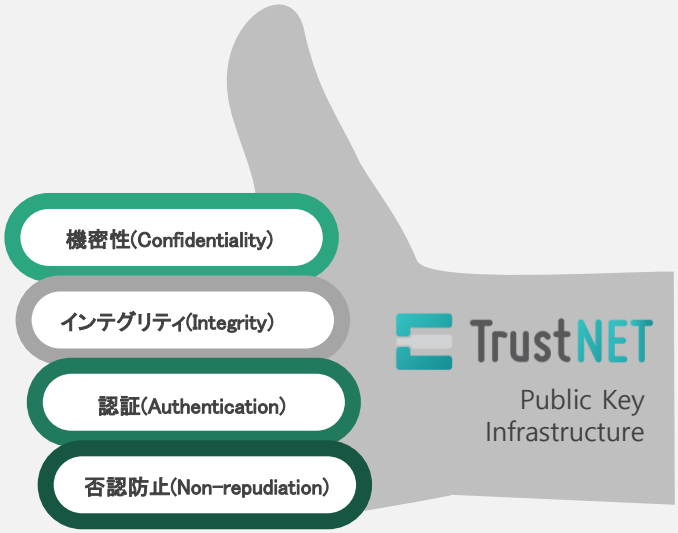
背景

インターネットの発展、
インターネットを通じた個人情報、
企業情報資産の流通情報増加

問題点

通信内容盗聴、
不法ユーザーデータ変造、
送受信事実否認

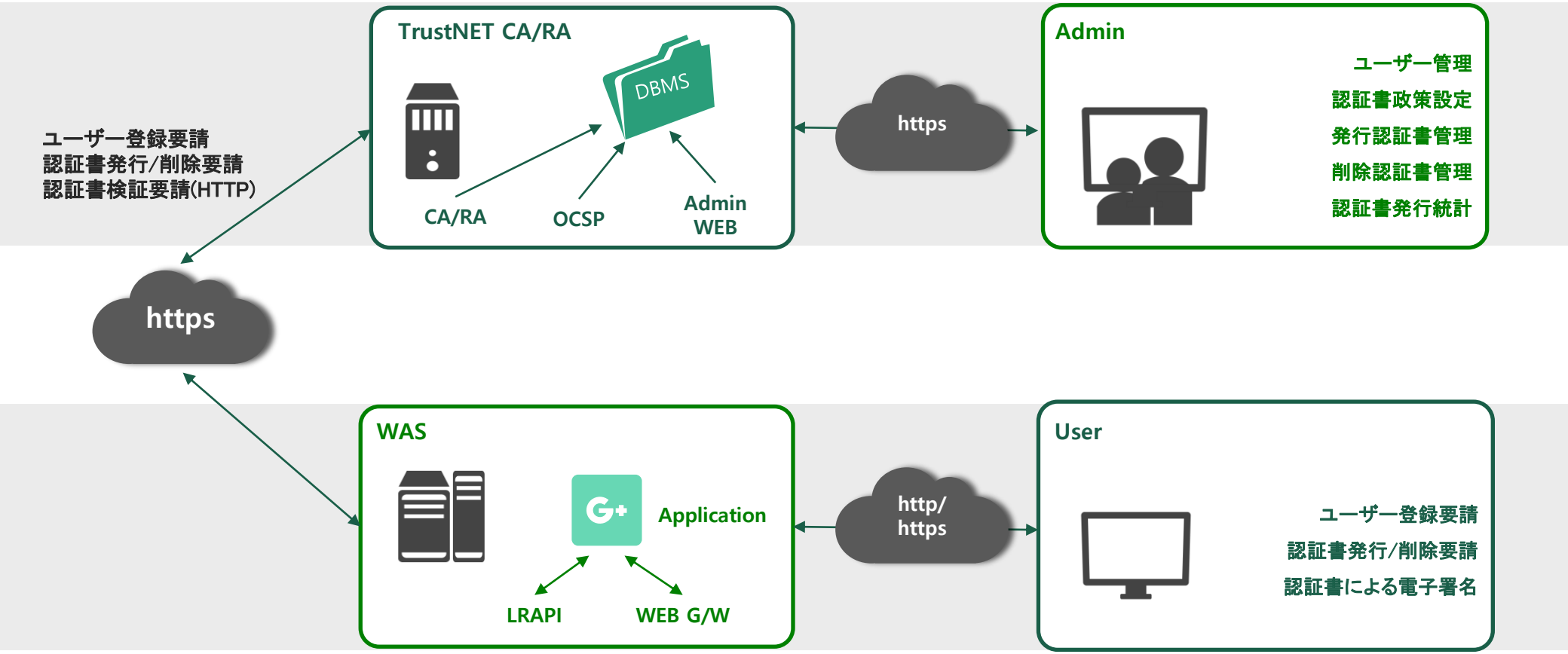




PanStarEnterprise

SoTIST

製品構成図



製品構成および主要機能

区分			機能	備考
サーバ	TrustNET CA/RA		ユーザー情報の登録および認証書の生成、削除、権限停止機能を行う PKI 核心システム	TrustNETでは認証書の有効性検証をOCSPを基本にする
	TrustNET OCSP		リアルタイムで認証書の有効性を検証するシステム	CA、OCSPサーバがハンドリングするRDB別途必要
	管理者Web Console		認証書政策設定、発行、削除および統計情報確認	CRL使用時LDAP別途必要
応用	TrustNET LRAPI, Web Gateway	ActiveX client	TrustNET CA/RA サーバに認証書発行のためのユーザー登録、ユーザー削除、認証書削除 機能を実行するためのライブラリー	TrustNET CA client設置が必要
クライアント	TrustNET CA-Client For PC	ActiveX client	ユーザーPCに設置されるコントロールでWindows IE 環境下で認証書の発行および管理を遂行	
		Multi client	ユーザーPCに設置されるコントロールでWindows, Linux, Mac環境下で認証書の発行および管理を遂行	Non Plug-in Client使用 IEはActive Xを使用するが場合もある
	TrustNET CA-Client For Mobile	Internal Storage	内部サーバなどに認証書、個人キーをセーブしApplication形態で提供されVPN Appまたは該当認証書が必要な他のAppで認証書の使用が可能	Android, iOS環境サポート
		External Storage	外部サーバなどに認証書、個人キーをセーブしLibrary形態で提供され認証書の発行および管理を遂行	Android, iOS環境サポート
	TrustNET Non-Native CA-Client		別途のクライアントモジュールの設置なくWebでクライアント機能遂行	HTML5をサポートする全てのウェブブラウザ

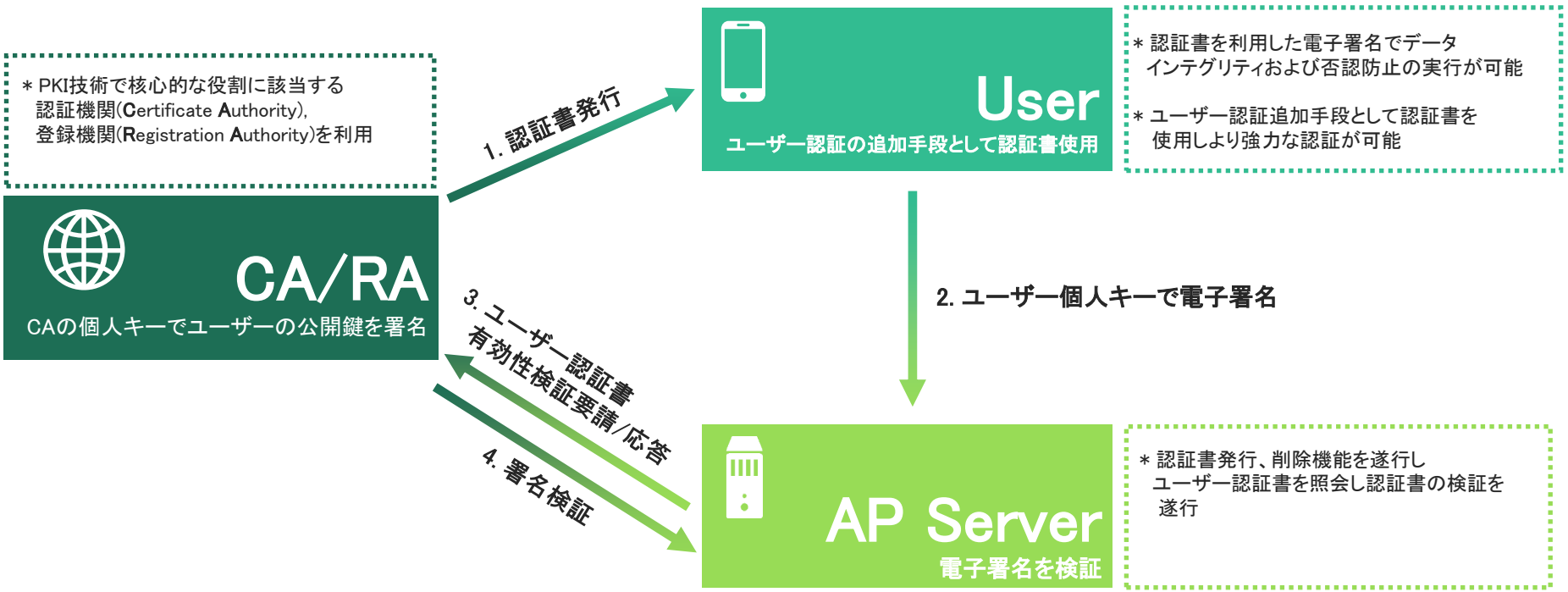
TrustNET Client Toolkit

	区分	機能
Toolkit	TrustNET Toolkit for JAVA	C/S Application運営環境に適用するセキュリティライブラリー
	TrustNET Toolkit for C/S	ジャバ統合環境に適用するセキュリティジャバクラス
	TrustNET Toolkit for ASP	NT用ASPウェブサーバ環境下で適用するセキュリティライブラリー
	TrustNET Toolkit for .NET	NET Application環境下で適用するセキュリティライブラリー
	TrustNET Toolkit for PHP	PHP基盤のウェブ環境に適用するセキュリティライブラリー

TrustNET構成要素別用途および機能

用途

- ユーザーの情報登録を通じユーザーDNを付与し認証書の発行のための参照番号、認可コードを発行
- 国際標準技術および最新技術の積極的反映



主要機能

認証書管理機能

全ての認証書の発行、再発行、削除機能
RFC 2510 CMPを利用した認証書管理機能
DBMS種類に関係なく認証書セーブ管理機能
(別途DBMSを使用しない場合MariaDB使用)
LDAPサーバ連動を通じた認証書掲示機能

認証書政策設定機能

認証書有効期間、キー期限、キー使用に対する設定機能
1人1認証書または1人複数認証書政策設定機能
認証書保存期間に対する設定機能
CRL更新周期設定機能

CRL生成および管理サポート

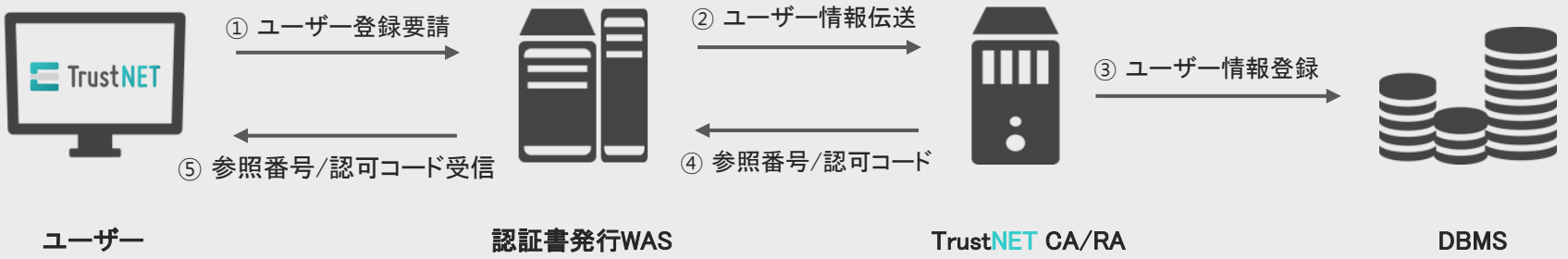
認証書の有効性検証のためのOCSPを基本提供、
別途要請によるCRL生成およびLDAP掲示機能提供
CRL更新周期設定による周期的更新が行われ、
CRL掲示位置を認証書に添付

ユーザー管理および統計

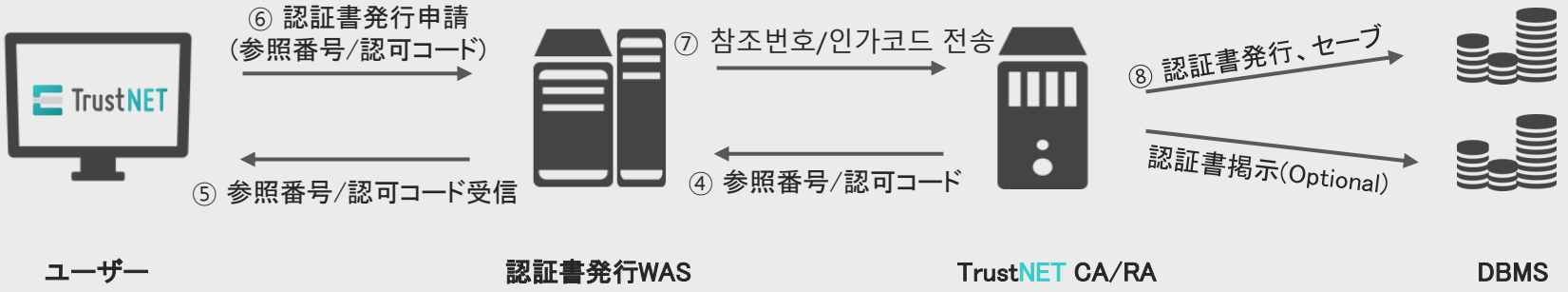
ユーザーを区分登録、削除機能
認証書情報(状態、SN、DNなど)照会および
退職などによる認証書削除機能提供
月別ユーザー登録統計機能
月別認証書発行および削除統計機能

認証書発行手順

ユーザー登録

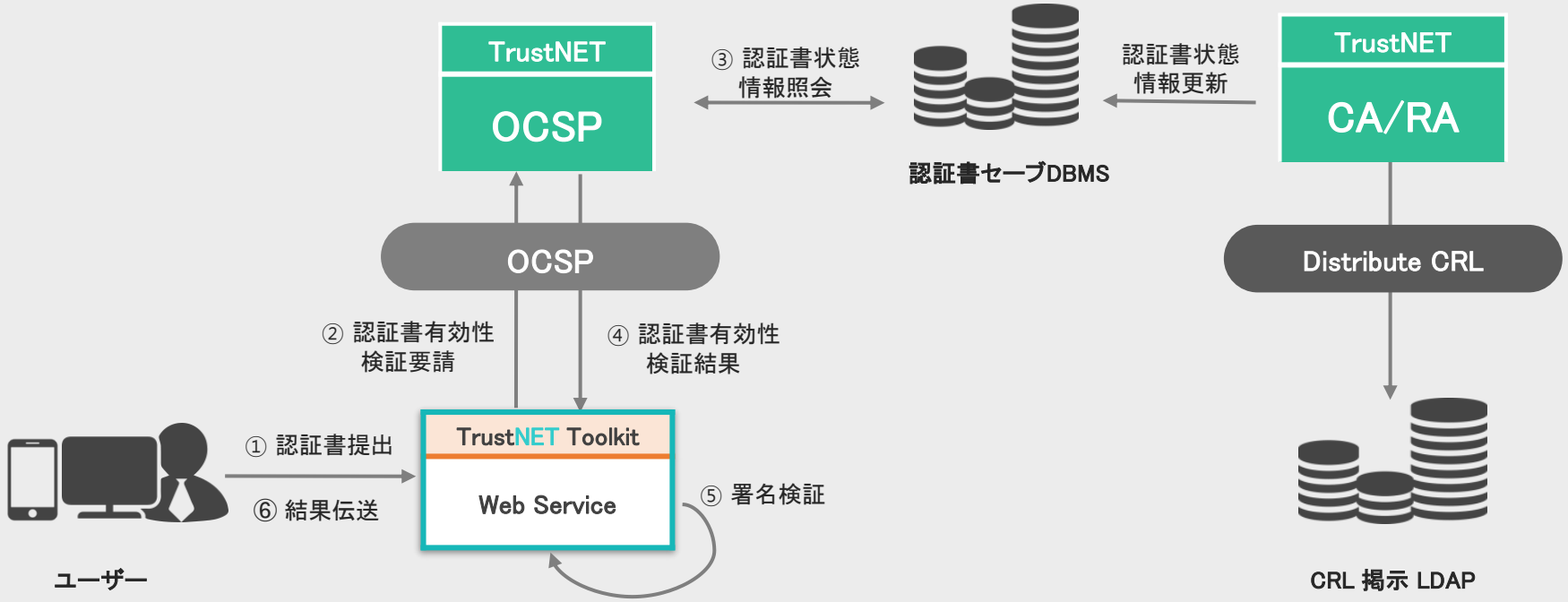


認証書発行



用途

- OCSPはCRL（認証書削除リスト)要請なく認証書の有効性をリアルタイムで検証できるシステム
- 顧客の要請にLDAP構成されCRL検証を行う機能も提供



主要機能

- 認証書の有効性を**リアルタイムで検証可能**なシステム

リアルタイム認証書状態の確認

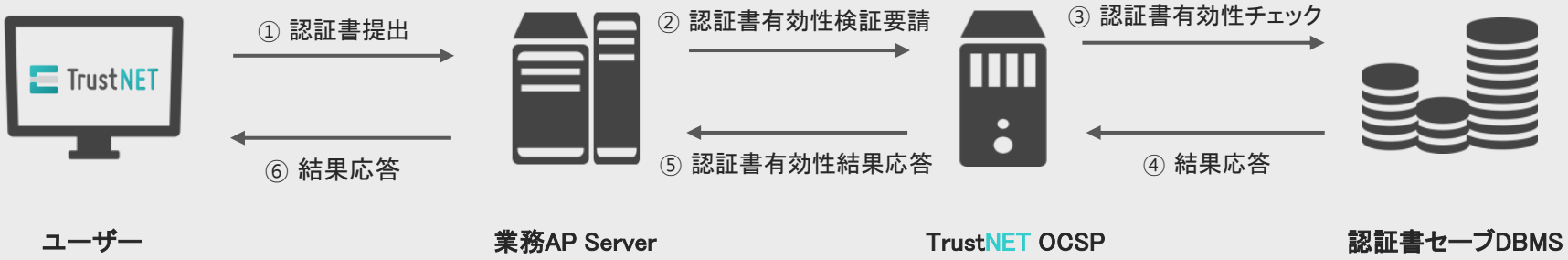
- ✓ OCSP検証要請に対し検証要請認証書をリアルタイムで状態を確認する機能
- ✓ 削除された認証書に対する削除日時および削除理由などの情報提供
- ✓ 認証書有効性検証に失敗された認証書の失敗原因をログに記録する機能

OCSP情報検証機能

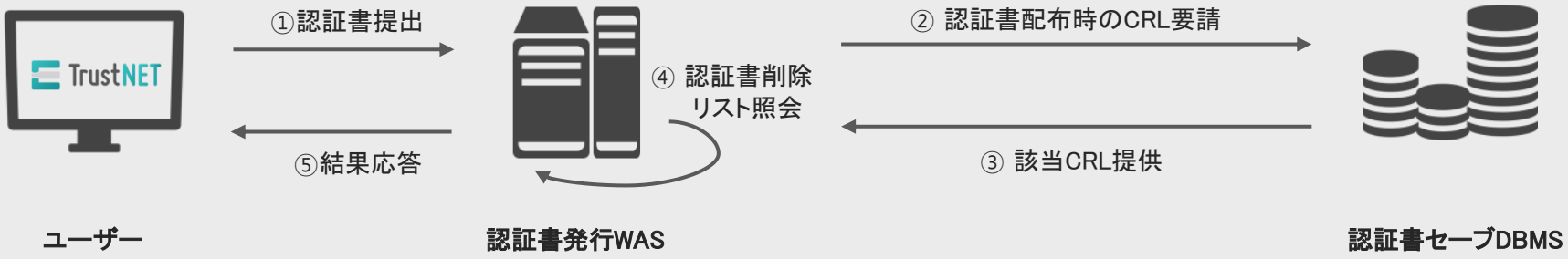
- ✓ OCSP要請情報に対する署名確認機能
- ✓ OCSP要請者の認証書を発行機関の公開鍵で検証し発行機関で署名された認証であるかを検証
- ✓ OCSP 要請者の認証書の有効性なのかを発行機関DB情報と比較し発行者の認証書が従属された認証機関の認証書なのかを確認
- ✓ 検証された認証書の発行者情報を発行機関の発行認証書と比較し発行機関で発行された認証書なのかを検証する機能

認証書検証手順

OCSP検証

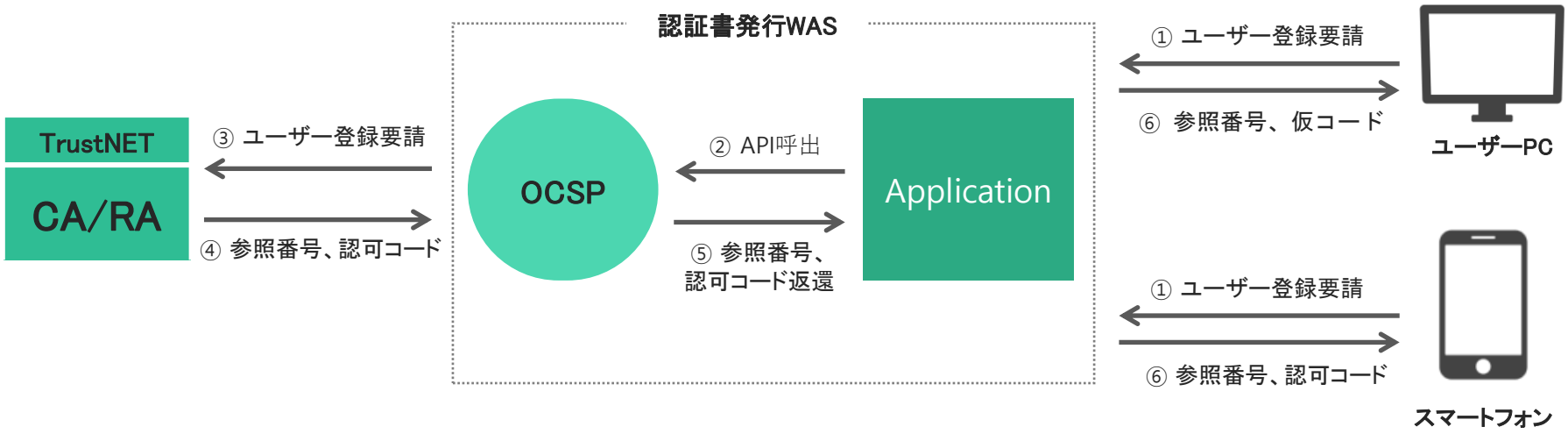


CRL検証



LRAPI用途

- TrustNET CA/RA サーバに認証書発行のユーザー登録、ユーザー削除、認証書削除の機能遂行に必要なAPIライブラリー形態の提供、顧客要請に対しLDAP構成を行いCRL検証を行える機能も提供
- 認証書発行のウェブ画面製作時運用プログラムで各機能に該当するAPIを呼出し使用



主要機能

- TrustNET CA/RA サーバで認証書発行時に必要な作業を行えるように**API機能提供**

リアルタイム認証書状態確認

- ✓ TrustNET CA/RAサーバとの暗号化(https)通信
- ✓ TrustNET CA/RAサーバでユーザー登録/再登録、削除要請
- ✓ TrustNET CA/RAサーバで認証書削除要請
- ✓ JAVA 1.3以上の全ての環境下で使用可能

OCSP情報検証機能

- ✓ TrustNET CA/RAサーバとの暗号化(https)通信
- ✓ TrustNET CA/RAサーバ応答に対しTrustNET CA Clientにインテグリティ検証要請
- ✓ ユーザー登録結果の参照番号、認可コードを利用し認証書の発行および再発行
- ✓ クライアントにはCA Clientが設置され動作されなくてはならない
- ✓ JAVA 1.3以上の全ての環境下で使用可能

PC Client

ActiveX Client

- ✓ ActiveXで製作および配布
- ✓ Windows Internet Exploreのみ使用可能
- ✓ 私設認証書の発行を受け

  PC内のFile形態でセーブ
- ✓ 発行された私設認証書の

  管理機能サポート

TrustNET
CA
PC Client

発行された認証書のローカルディレクトリーにFile 形態で
保管され、Web BrowserまたはOS種類によって
ActiveX / Non Plug-in方式の2種類に区分されます。

Windows - Internet Explore環境下では
ActiveXモジュールが設置され、その他のブラウザ
(chrome, safari, opera, firefox, Edge)または
OSではNon Plug-inモジュールが設置され
作動します。
各モジュールがサポートする機能は同じです。

ActiveX
Non Plug-in
2 Ways

- ✓ Non Plug-in方式のモジュール製作および配布
- ✓ Internet Explore環境を含むブラウザと

  Windows、その他OS(Linux, MacOS)

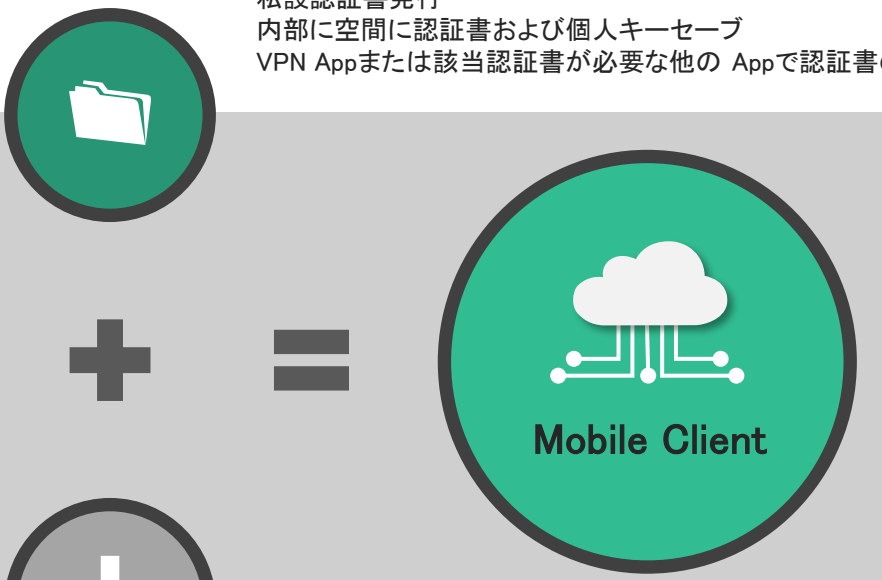
  環境で使用
- ✓ 私設認証書の発行後PC内File形態でセーブ
- ✓ 私設認証書の発行、管理機能サポート

Non Plug-in Client

Mobile Client

Internal Storage Ver.

私設認証書発行
内部に空間に認証書および個人キーセーブ
VPN Appまたは該当認証書が必要な他の Appで認証書の使用可能



TrustNET CA Mobile Clientはスマートフォンアプリケーションで
私設認証書の発行および管理が可能な機能を提供

発行された認証書のセーブ状態によってInternal Storage / External Storageの
2つのバージョンに区分され、

Internal Storageはクライアントで認証書の発行後OSが認識できる内部空間に
セーブ後他のAppまたはOSで認証書を使用可能で、

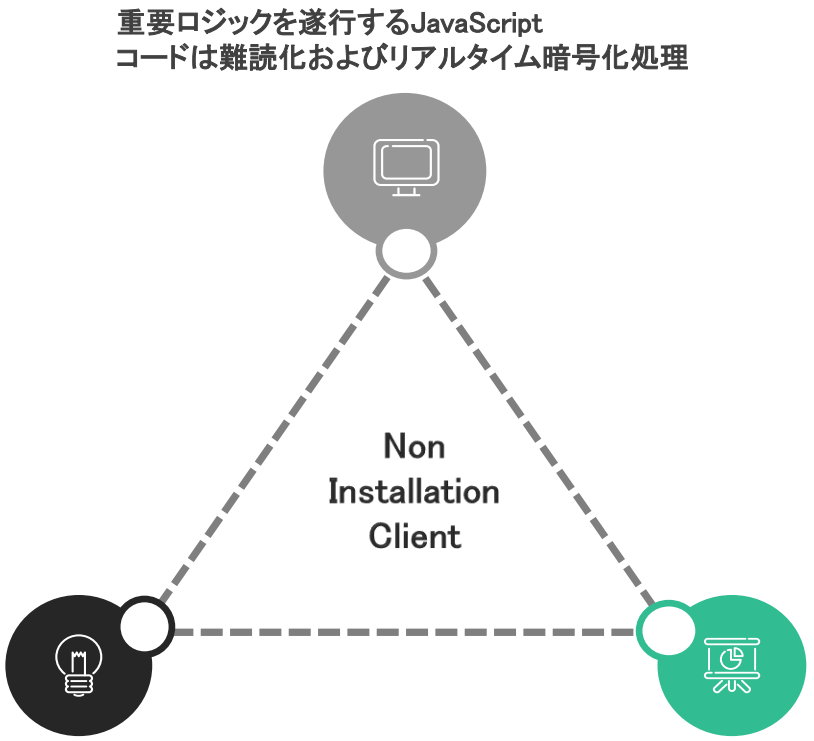
External StorageはSD CardまたはApp内部フォルダを生成しセーブされ、認証書を
使用する機能を提供する。

External Storage Ver.

私設認証書発行
外部空間に認証書および個人キーセーブ
個人キーパスワードの変更
キー/認証書削除

Non Installation Client

- JavaScriptとHTML5技術を基盤にNativeコードのないクライアント機能を遂行



- TrustNET Non-Native CA-Clientは JavaScriptとHTML5技術を利用し別途のモジュール設置の費用なしにPC、モバイル環境で同じように使用できるクライアント
- 発行された認証書はウェブブラウザ内にセーブされ使用
- 安全に暗号化されセーブされることで流出や不正利用されるリスクを低減

主要機能

- TrustNET CA/RAサーバに認証書発行に必要な作業を行えるようAPI機能提供

PC Client

- ✓ TrustNET CA/RAサーバとのデータインテグリティ検証機能
- ✓ 認証書発行に必要な認証書生成要請情報生成および認証書/個人キーセーブ機能
- ✓ 認証書/個人キー削除機能、個人キーパスワード変更機能

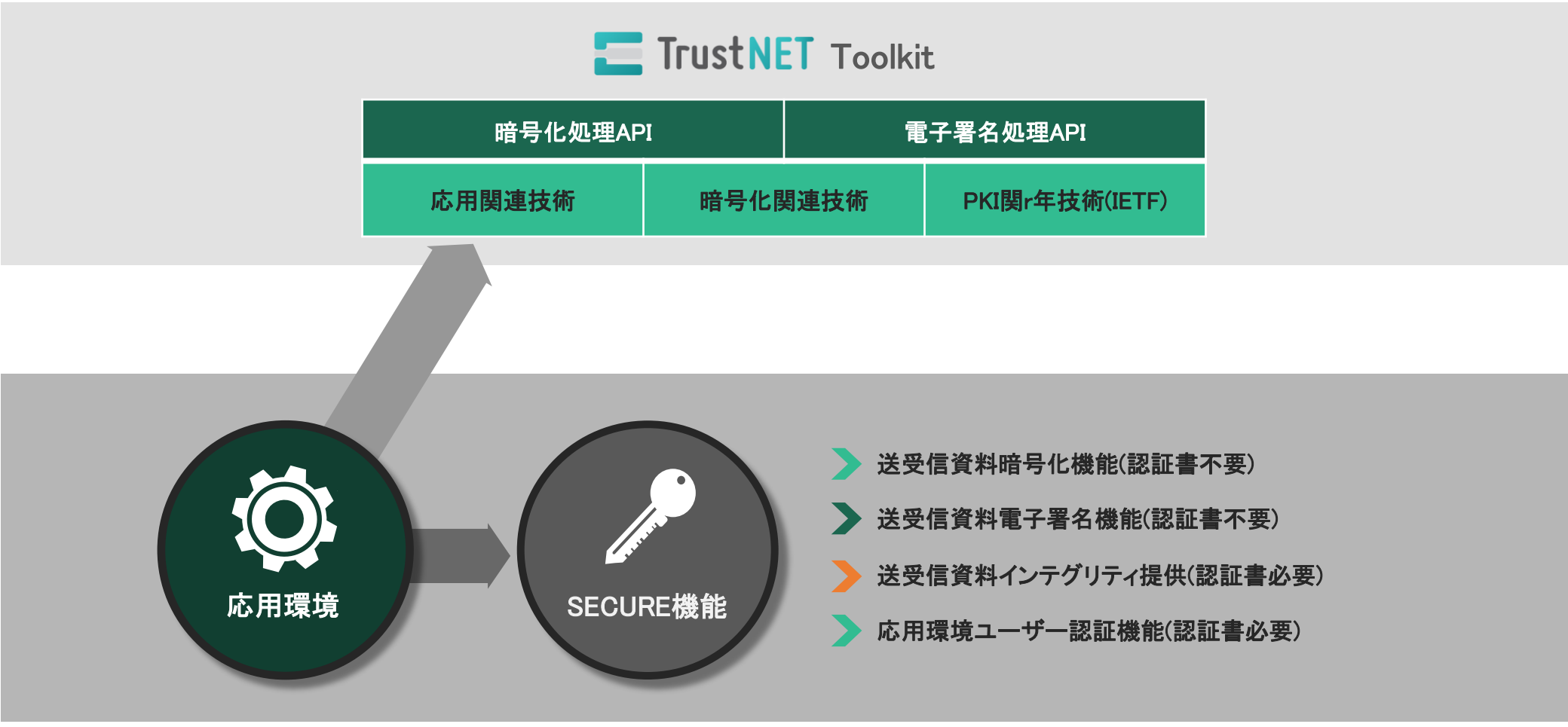
Mobile Client

- ✓ TrustNET CA/RAサーバとのデータインテグリティ検証機能
- ✓ 認証書発行に必要な認証書生成要請情報生成および認証書/個人キーセーブ機能
- ✓ VPN Appまたは他のAppで認証書を使用できるよう内部空間に認証書セットをセーブする機能
- ✓ 外部セーブ空間に認証書セーブ時、認証書/個人キーの削除機能、個人キーパスワード変更機能

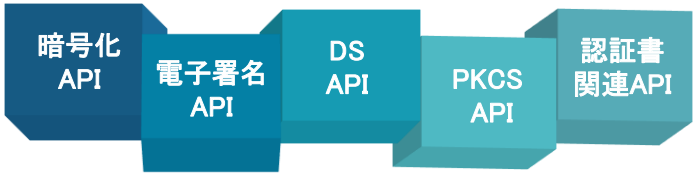
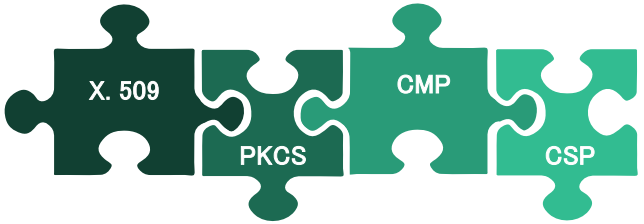
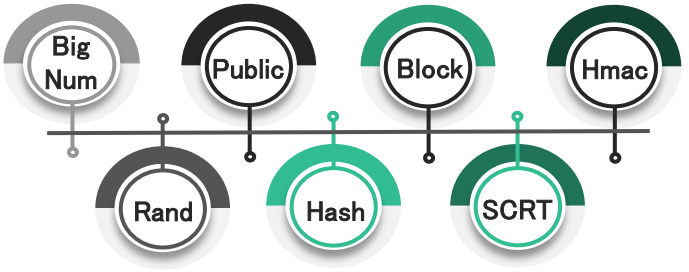
Non-Native Client

- ✓ TrustNET CA/RAサーバとのデータインテグリティ検証機能
- ✓ 認証書発行に必要な認証書生成要請情報生成および認証書/個人キーセーブ機能
- ✓ 認証書/個人キー削除機能、個人キーパスワード変更機能
- ✓ 認証書のインポート/エクスポート機能提供

用途



製品構成

区分	Linux	Windows
Toolkit(API)		■ 各種暗号化アルゴリズム提供 (暗号、電子署名、Hash、 ランダムナンバー生成など..)
Cert Library		■ 認証書(X509)検証、経路検索機能 ■ 暗号文章処理機能 ■ 認証書要請/削除などCAインターペイ機能 ■ 暗号化資料インコーディング/デコーディング
Crypto Library		■ サーバ応用プログラムで暗号化 ■ 電子署名/検証などに対する機能提供 ■ レジストリおよびスマートカード インターフェースサポート

主要機能

区分	機能	特徴
暗/復号化機能	対称キーアルゴリズムおよび公開鍵アルゴリズムを使用し特定資料を暗号化/復号化可能機能	▪ 特定資料および任意資料に対する暗/復号化可能 ▪ 添付ファイルに対する暗/復号化機能
電子署名機能	特定資料に対し電子署名値を生成し 署名値を検証する機能	▪ 添付ファイルに対する電子署名機能
暗号化キー生成および キー交換機能	暗号化に使用されるセッションキー(暗号化キー)を 安全に生成し交換(共有)可能な機能提供	▪ SSL V3とTLS V1.1でのキー共有機能と同一方式
認証書I/O機能	認証書および個人キーをレジストリ、ハードディスク、 スマートカード、USBなどにバックアップおよび復旧可能な機能	▪ 多様な形式のセーブ形式提供 (PKCS#12、PEM、DERインコーディング、 デコーディング機能) ▪ PKCS#8形態の秘密キー管理
PKCS#7メッセージ (電子封筒)機能	RSAの標準形式の暗号化および電子署名メッセージの 生成/復旧機能サポート	▪ 保安メール、XMLなどに対する拡張性提供
認証書件所機能	各種認証機関から発行された認証書に対する 有効性検証(経路検証) 機能提供	
電子署名認証センター 認証書連動機能	社内私設認証書および電子署名認証センターの認証書を 統合しインターフェース可能機能提供	▪ 大手電子署名認証センター発行認証書および 電子署名認証センター相互連動認証書処理

主要機能

区分	機能	特徴
認証書管理機能	認証書発行要請プロトコルであるCMP注)1 方式による認証書発行申請および認証書削除、更新、認証書パスワード変更、インコーディング、デコーディングなどに対する機能提供	▪ CMP標準認証機関(電子署名認証センター含む)のインターフェース可能 ▪ スマートカードおよびUSBなどへのインターフェース提供
認証書GUI (ユーザーインターフェース)機能	保存媒体別認証書選択および個人キー取得などの便利な画面インターフェース機能提供	▪ 電子署名認証センター認証書処理 ▪ 認証書自動選択機能提供
多様な形態のクライアント提供	ActiveX、モバイル、Non-Native環境など多様な環境で使用可能なクライアント製品の提供可能	▪ PC、モバイル環境で使用される全ての環境をサポート可能 ▪ Non-Nativeサポートクライアントは HTML5機能をサポートするウェブブラウザでなければならない

注)1 CMP : Certificate Management Protocol

特徴および長所

注文型ツールキット提供

ツールキット構造が3階層で構造されているため
顧客が望む機能だけを容易に再構成することが可能

関連標準完璧なサポート

韓国内標準アルゴリズムサポート、その他公開鍵アルゴリズム
および暗号学的標準の完璧な順守

共用認証書処理

現在5社の電子署名認証センター用認証書処理
(暗/復号化、電子署名、インターフェース、スマートカードサポート)

処理速度および安定性確保

マルチスレッド環境を考慮した設計により安定性および
処理速度保障(K電子署名/検証時 約0.03秒)

多様な環境サポート

ウェブToブラウザ、クライアントToサーバ、サーバToサーバ
など多様な構造と応用環境をサポート

多様な構築経験

多様なPKI構築経験
(共用および大規模認証センター構築、多様な電子署名認証センター連動)

TrustNET主要仕様

関連標準

区分	技術要素	標準根拠案	技術説明
認証	認証書規格	X.509 v3, RFC3280	適用技術はインターネット標準案RFC 2459の認証書規格を採択し 他のPKI領域との連動のため最小限の機能を確保
	認証書削除リスト規格	X.509 v2, RFC3280	認証書と同一のインターネット標準案RFC 2459が適用され高い連動性確保
	認証書管理手順	RFC 2510, RFC 2511 draft-ietf-pkix-cmp-transport-protocols-01	認証書発行/削除/更新のため相互メッセージ部分でインターネット標準案 RFC 2510と実際のメッセージの伝送部分の板—ネット標準案であるdraft-ietf-pkix-cmp-transport-protocols-01を適用し終端間連動性を確保
	認証書検証	RFC 3280	認証書の有効性検証のため経路認証部分はインターネット標準案RFC 2459を準用し 相互認証時に認証書の憲章に対する連動性を確保
	認証書分配	RFC 2559, RFC 2585, RFC2587	発行された認証書を配分するため標準化されたディレクトリー構造を通じLDAP サポートおよびHTTP やFTPその他のネットワークプロトコルを通じ接近者のために RFC 2585を適用し分配の容易性を確保
通信プロトコル	CRMF	RFC 2511	Certificate Request
	CMP	RFC 2510	Internal messaging cross certification
	SSL	RFC 6101	Secure Socket Layer
	X.509 PKI-OCSP	RFC 2560	Online Certificate Status Protocol
	CMS	RFC 2630	Cryptographic Message Syntax
	LDAP	LDAP	Communication LDAP
	SQL	SQL	Internal Communication
	HTML5	World Wide Web Consortium	HTML5

関連標準

区分	技術要素	標準根拠案	技術説明
技術	RSA暗号化	PKCS #1	RSAアルゴリズムを利用したデータ暗号化および電子署名生成と関連した業界標準をサポート
	パスワード基盤データ暗号化	PKCS #5 v2.0	パスワード基盤の暗号化のためにキー誘導関数PBKDF2および8バイト以上のブロック暗号キーを利用したPBES2をサポート
	認証書拡張構造	PKCS #6	拡張された認証書構造をサポートするため業界標準で署名メッセージなどで添付機能をサポート
	電子署名および暗号データ化	PKCS #7, RFC 2630, RFC 2634	公開鍵暗号化方式を利用し電子署名メッセージおよび暗号メッセージ、ダイジェストメッセージなどの電子文書標準をサポオート
	個人キー構造	PKCS #8	個人キーの保管および移動のためのメッセージ形式および暗号化された個人キー標準をサポート
	認証書要求様式	PKCS #10, RFC 2511	認証書発行要求時メッセージの標準構造でPKCS #10対比POPおよび構造が改善されたRFC 2511を追加サポート
	ユーザー情報交換	PKCS #12	ユーザー個人キーおよび認証書その他保安資料などの移動保管および伝達様式の標準であるPCでの認証書移動手段をサポート

サポート環境

区分			備考
サーバ	TrustNET CA/RA		JAVA 1.7以上の全てのOS環境サポート DBMS : Oracle, MS-SQL, MySQL, MariaDB, TiberoDBサポート （その他DBMSはポーティングされサポート可能）
	TrustNET OCSP		
	管理者Web Console		
応用	TrustNET LRAPI, Web Gateway	ActiveX client	JAVA 1.3以上の全てのOS環境サポート
クライアント	TrustNET CA-Client For PC	ActiveX client	Browser : Internet Explorer OS : Windows (Windows 8.1 tile UI 除く)
		Multi client	Browser : Chrome, Safari, Opera, Firefox, Edge OS : Windows, Mac, Linux
	TrustNET CA-Client For Mobile	iOS	iOS 6.0以上
		Android	Android 4.0 (Ice Cream Sandwich)以上 (Internal Storage Version基準)
	TrustNET JavaScript CA-Client		HTML5をサポートする全てのOSおよびウェブブラウザ修正

主要供給実績

主要供給実績

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	