ユーザー，デバイス，データを認証するセキュリティソリューション

Security Solutions Offering Safe and Secure Authentication of Users, Devices and Systems, and Programs

薩川　満明 SATSUKAWA Mitsuaki　　福岡　寛規 FUKUOKA Hiroki　　畠中　一成 HATANAKA Issei

ビッグデータを利活用するCPS（サイバーフィジカルシステム）の実現には，様々なケースでユーザー，デバイス，及びプログラム（データ）の認証やセキュリティ対策の強化が必要になる。

東芝インフラシステムズ（株）は，ICカード及び周辺システムの開発で長年にわたって培った認証・暗号化・鍵管理技術をベースにしたセキュリティソリューションとして，⑴一つのデバイスで多要素認証が可能なBISCADE，⑵セキュリティ対策が難しい機器をネットワーク化するCYTHEMIS，及び⑶オンラインで更新したプログラムの正当性を担保するAKTEGRISを開発し製品化することにより，顧客のシステムやデバイスのセキュリティ強化に貢献している。

The progress of cyber-physical system (CPS) technologies in processing large volumes of data generated in the physical space has given rise to the need for enhanced security measures for the authentication of users, devices and systems, and programs in various situations.

Toshiba Infrastructure Systems & Solutions Corporation has developed and released the following security solutions based on authentication, encryption, and key management technologies cultivated through the development of integrated circuit (IC) cards and peripheral systems: (1) the BISCADE card and BISCADE dongle, comprising security devices that achieve multi-factor authentication through the combination of a possession factor with biometrics in a single package; (2) the CYTHEMIS Internet of Things (IoT) security solution, which makes it possible to network devices that lack adequate security measures; and (3) the AKTEGRIS security solution, which ensures the validity of firmware at the time of online updates. These security solutions are contributing to enhanced security of customers' devices and systems.

1. まえがき

近年のインターネットの普及により，様々なデバイスがネットワークで接続され，そこから得られるビッグデータを利活用するCPSが実現されつつある。CPSにおいては，様々なケースで，デバイスやシステムを利用するユーザー，デバイス，及びデバイス内で動作するプログラム（データ）の正当性や安全性を確保する仕組みが必要となる。

東芝インフラシステムズ（株）は，ICカード及び周辺システムの開発で半世紀にわたって培ってきた認証・暗号化・鍵管理技術をベースに，下記の3種類のソリューションを開発し，展開を進めている。

⑴　BISCADE　　指紋照合でユーザーを認証するセキュリティデバイス（2020年に提供開始）

⑵　CYTHEMIS　　デバイスを認証するセキュリティソリューション（2019年に提供開始）

⑶　AKTEGRIS　　保護対象デバイスのファームウェア更新セキュリティサービス（2016年に提供開始）

AKTEGRIS，BISCADE，CYTHEMISの頭文字から，“セキュリティABCサービス”と呼んでいるこれらのソリューションは，単独，あるいは組み合わせて利用することで，**図1**に示すような様々なユースケースでのセキュリティ対策が可能となる。

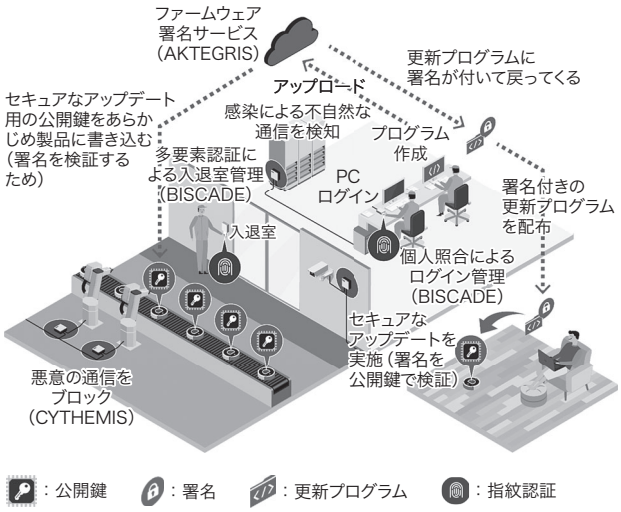


図1．セキュリティソリューションの適用例

AKTEGRIS，BISCADE，及びCYTHEMISを組み合わせて製造工場に適用することにより，トータルなセキュリティ強化及び利便性の向上が可能となる。

Example of application of security solutions to manufacturing facility

ここでは，それぞれのソリューションについて，背景や，特長，導入事例などについて述べる。

2. BISCADE

2.1 背景

PC（パソコン）や様々なサービスなどへのログオンや，入退ゲートにおいてユーザーの認証を行う場合，カードやドングルなどの所持要素や，ID（識別情報）やパスワードのような知識要素を用いた認証が，今でも多く利用されている。しかし，カードの貸し借りやID・パスワードの流出など，本人成り済ましによる犯罪や不正は年々増加傾向にあり，より厳格な認証手段として，指紋・顔・静脈といった，盗まれることがなく，貸し借りができない生体要素を使用した生体認証が使われるケースが増えている。また，前述した三つの要素のうち，二つ以上を組み合わせて認証を行う多要素認証の必要性も高まっている。

2.2 BISCADEカード及びBISCADEドングルの特長

当社は，“カード・ドングルの所持による所持認証”と“指紋照合による生体認証”の多要素認証を一つのカード・ドングルで実現可能な“BISCADEカード”及び“BISCADEドングル”（以下，これらの総称としてBISCADEと略記）を開発した。

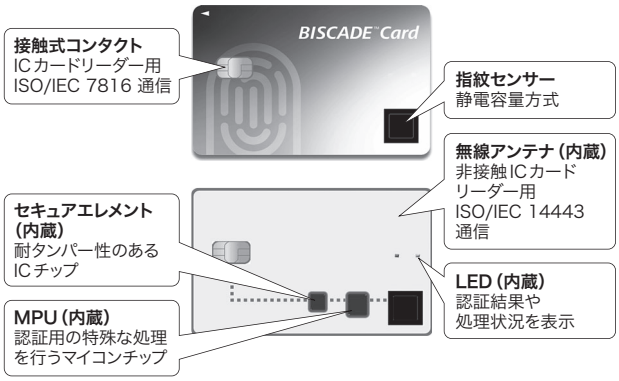
利用者の指紋情報は，クレジットカードなどにも利用されるセキュリティチップに事前に登録しておく（複数登録可能）。認証時には，BISCADE上の指紋センサーから取得した指紋情報と，事前に登録した指紋情報の照合をBISCADE内のICチップで行う。登録，認証とも指紋情報はBISCADE内に限り利用されるため，漏洩（ろうえい）リスクは低い。また，指紋情報は個人所有のBISCADEのセキュリティチップだけに保存されているため，紛失時の漏洩リスクも低く，大量流出の危険性もない。

図2に示すBISCADEカードは，ISO/IEC（国際標準化機構／国際電気標準会議）規格の現行クレジットカードの大きさ，厚さ，及び強度に準拠しており，既存の金融決済端末やICカードリーダーをそのまま使用できる。現時点では接触式カードだけだが，2022年度中に非接触式カードの製品化を予定している。

BISCADEドングルは，USB（Universal Serial Bus）typeCインターフェースを備えており，**図3**に示すとおり，直接PCやタブレットなどに挿して使用できる。

2.3 効果，導入事例

“ICカード＋指紋認証”で生体認証，多要素認証を実現するBISCADEの利用により，従来の“ICカード＋パスワード”による認証に比べて，セキュリティの向上だけではなく，IDや複雑なパスワードを管理・記憶する必要がなくなるため，利便性も向上する。



LED：発光ダイオード　　MPU：マイクロプロセッサー

図2. BISCADEカードの構成

BISCADEカードは，ISO/IEC規格の現行クレジットカードの大きさ，厚さ，及び強度に準拠しており，既存の金融決済端末やICカードリーダーをそのまま使用できる。

Configuration of BISCADE card

図3. BISCADEドングルの利用シーン

BISCADEドングルを，PCやタブレットなどのUSB typeCインターフェースに差し込むことにより，同時に指紋認証が行われる。

Scene of usage of BISCADE dongle

BISCADEカードは，（株）ローレルインテリジェントシステムズが発売しているセキュリティシステム“FSS®SmartLogon® TFPA”に採用され，セキュリティと利便性を向上させた新たなPCログオンカードとして，自治体などで使用されている。

BISCADEドングルは，（株）ソリトンシステムズの児童・生徒向けPCログオンシステムに採用された。その有用性や利便性は，東京学芸大学附属小金井小学校の協力の下，レノボ・ジャパン（同）とも連携して実施した「簡単で安全なPCログオンシステム実証研究」のキーデバイスとして利用することで検証できた。

3. CYTHEMIS

3.1 背景

研究・開発拠点では，研究装置や開発装置を動かすためにカスタマイズされたPCを使用している例が多い。これらのPCは，セキュリティ対策（OS（基本ソフトウェア）のアップデート，ウイルス対策ソフトウェアの導入など）を行うことで稼働しなくなる懸念があるため，安易にセキュリティ対策を取ることができない。また，このようなセキュリティ対策の取れないPCに対して，組織内イントラネットの多くは，基幹ネットワークに直接接続させないセキュリティポリシーを設定しており，ネットワークに接続されずに運用されている。そのため，これらのPCのデータ移動についてはネットワーク経由ではなく，外部メモリーを使用し，手動で行われている。この外部メモリーを使用したデータ転送では，紛失によるデータ漏洩のリスクや，データ移動に時間が掛かるという問題がある。

3.2 CYTHEMISの特長

CYTHEMISはセキュリティ対策を行いたいデバイス（以下，保護対象デバイスと略記）に外付けする小型のCYTHEMISデバイスとそれらを一括管理するCYTHEMIS管理システムを組み合わせたセキュリティソリューションである（**図4**）。CYTHEMISデバイスは8.4（縦）×8.4（横）×3.8（高さ）cmの小さいボックス形状の製品であり，二つのNetwork Interface Cardを搭載し，保護対象デバイスとネットワークの間に挟み込む形で接続される。電源供給はAC（交流）電源で行う。

CYTHEMISには，三つの大きな特長がある。一つ目は，CYTHEMISデバイス間での相互認証と通信の暗号化である。CYTHEMISデバイスは，4章で詳細に述べるPrivate CA（Certificate Authority）の技術を使用して公開鍵証明書を取得し，これを相互に提示することで通信相手の正当性を確認した上で通信を行う。また，通信を暗号化することにより，通信内容の改ざんや盗聴を防ぐことができる。二つ目は，許可する通信のリスト（以下，パスリストと略記）による通信の監視である。CYTHEMISデバイスはあらかじめ管理システムで設定したパスリストをダウンロードし，CYTHEMISデバイスを通過する通信をパスリストと照合する。合致しない場合は，不正な通信として検知・警告・遮断を行うことができる。三つ目は，CYTHEMIS管理システムの一元管理機能である。この機能により，CYTHEMIS管理システム上で保護対象機器やCYTHEMISデバイスの情報，及びCYTHEMISデバイスが検知した不正と思われる通信の情報を確認できる。これにより，ネットワークのどこで不正と思われる通信が発生しているのかをいち早く発見でき，セキュリティ対応を迅速に実行できる。

3.3 導入事例

国立研究開発法人 物質・材料研究機構は，我が国における物質・材料研究分野の中心的な役割を果たしている機構であり，人工知能を含む情報科学を材料研究に応用するマテリアルズ・インフォマティクスを推進している。研究装置を制御し，研究データを記録するPC（以下，制御・記録PCと略記）の中には，セキュリティ対策を取れないものがあり，そこからデータを移動する際に，研究者は外部メモリーを用いて手動で行わざるを得ず，研究効率が阻害されていた。このような制御・記録PCを，CYTHEMISの導入でCYTHEMISデバイスが保護したことで，高速なデータ

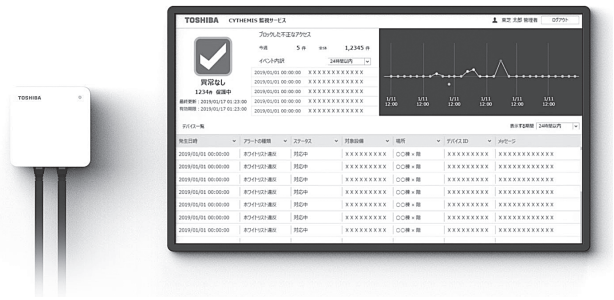


図4. CYTHEMISデバイスと管理システム

CYTHEMISは，保護対象デバイスに外付けする小型のCYTHEMISデバイスとそれらを一括管理するCYTHEMIS管理システムを組み合わせた，セキュリティソリューションである。

CYTHEMIS device and management system

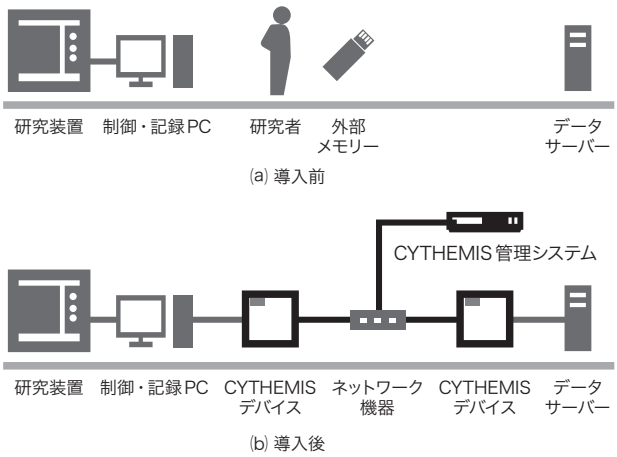


図5. CYTHEMIS導入によるネットワークへの接続

制御・記録PCを，CYTHEMISデバイスが保護したことで，高速なデータ移動が可能な構内ネットワークへのセキュアな接続を実現できた。

Connection of equipment to network applying CYTHEMIS

移動が可能な構内ネットワークへのセキュアな接続を実現し（**図5**），研究効率の大幅な改善に貢献できた。

4. AKTEGRIS

4.1 背景

ネットワーク環境の普及により，出荷済みの製品に対し，内部のプログラムをオンラインで更新するニーズが高まっている。これにより，機能拡張や不具合の改修に要するリードタイムやコストを低減できる反面，制御プログラムを不正に改ざんされ，情報漏洩や人命が危険にさらされるリスクも高まっている。こうしたことを防ぐには，①更新されるプログラムが正しいものであることと，②通信相手が正しく，通信内容が秘匿されていることを，担保する必要がある。実現方法としては，①は電子署名を，②は暗号化機能を備えた通信プロトコルを，使用することが一般的である。AKTEGRISは，これらをデバイスの製造元などのユーザーが実現できるようにするためのデータ（電子署名，公開鍵証明書）を提供するクラウドサービスである。

4.2 AKTEGRISの機能

4.2.1 ファームウェア署名サービス

更新プログラムの正当性を担保するために用いる暗号鍵の生成・保管や，電子署名を生成するサービスを，以下のように提供する。

⑴ ユーザーは，AKTEGRISの鍵生成アルゴリズムを用いて，署名の生成と検証のための公開鍵と秘密鍵のペアを**図6**のように生成

⑵ そのうちの公開鍵を，ユーザーがデバイスに書き込み，デバイスを市場に出荷

⑶ デバイス内部プログラムに更新が生じた際には，ユーザーは，再びAKTEGRISを使用し，先の公開鍵とペアを成す秘密鍵で，更新プログラムの電子署名を生成

⑷ デバイス側では，公開鍵により電子署名を検証した上でプログラムの更新を行うことで，不正なプログラムの混入を防止

4.2.2 Private CA

デバイス間通信の安全性を確保するための，公開鍵証明書を発行するサービスを提供する。公開鍵証明書のフローを，**図7**に示す。

⑴ AKTEGRIS側ではまず，Private CAの公開鍵と秘密鍵のペアを生成

⑵ デバイス証明書が必要になった際，デバイス側で，デバイスの公開鍵と秘密鍵のペアを生成

⑶ デバイスがデバイス公開鍵をAKTEGRISに送付して，デバイス証明書を要求

⑷ AKTEGRIS側では，Private CAの秘密鍵を用いてデバイス証明書を発行

⑸ AKTEGRISがデバイスにデバイス証明書を送付

⑹ デバイス証明書の検証に必要なPrivate CA証明書も，併せて送付

機器間通信を行うデバイスは，公開鍵証明書を相互に提示することで，通信相手の正当性と，通信内容の機密性・完全性を確保できる。

4.3 AKTEGRISの特長

ファームウェア署名サービス，Private CAサービスのいずれも，FIPS 140-2（注1）レベル3を取得したHSM（Hard-

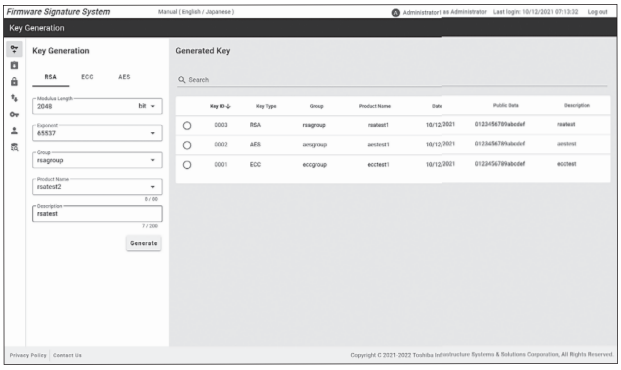


図6. AKTEGRIS（ファームウェア署名）の鍵生成画面例

AKTEGRISが生成する公開鍵と秘密鍵のペアを利用することで，ファームウェアの更新プログラムが正しいものであることを検証できる。

Example of key generation display of AKTEGRIS firmware signature system

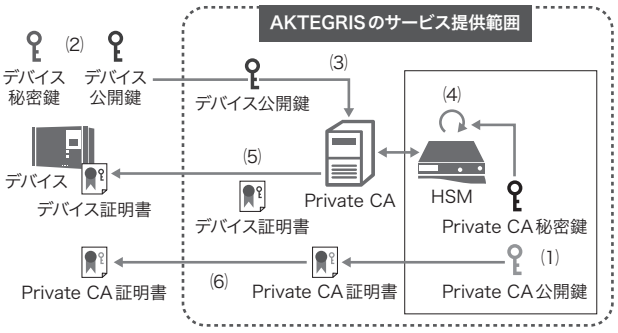


図7. AKTEGRIS（Private CA）の公開鍵証明書の発行フロー

機器間通信を行うデバイスは，公開鍵証明書を相互に提示することで，通信相手の正当性と，通信内容の機密性・完全性を確保できる。

Flow of processes for public key certificate issuance using AKTEGRIS private certificate authority (CA) service

（注1） FIPS（Federal Information Processing Standards）は，米国の情報処理標準規格。このうち140-2は，暗号モジュールに関するセキュリティ要件を規定。

ware Security Module）内の安全な環境で，暗号鍵や電子署名の生成を実行する。HSMは鍵の保管も担っており，ファームウェア署名サービスでは電子署名に用いる秘密鍵を，Private CAサービスではCAの秘密鍵を，それぞれ15年以上，長期保管可能である。また，データのバックアップや，バックアップ媒体の金庫保管などの，標準的な保守サービスを提供している。

4.4　導入事例

AKTEGRISは，社内外や国内外の顧客に向けて，2016年からサービスを提供している。顧客の一つである半導体ベンダーは，OSを再インストールしても除去できないマルウェアの脅威に対する，より高度なセキュリティ対策として採用している。また，別の顧客である自動車部品サプライヤーは，コネクテッドカーの潮流における，より強固なセキュリティ対策のニーズを満たすために，導入している。

5. あとがき

CPSの要素であるユーザー，デバイス，データを認証し，セキュリティを強化するBISCADE，CYTHEMIS，AKTEGRISについて，背景や，特長，導入事例などについて述べた。

現在は各ソリューション単独での導入となっているが，二つ，又は三つを組み合わせて導入することにより，様々なユースケースにおけるトータルなセキュリティの強化及び利便性の向上が期待できる。当社は，今後もセキュリティABCサービスとして展開し，CPSの実現に貢献する。

・FSSは，（株）ローレルインテリジェントシステムズの登録商標。

薩川　満明　SATSUKAWA Mitsuaki
東芝インフラシステムズ（株）セキュリティ・自動化システム事業部 カード・セキュリティシステム営業部
Toshiba Infrastructure Systems & Solutions Corp.

福岡　寛規　FUKUOKA Hiroki, Ph.D.
東芝インフラシステムズ（株）セキュリティ・自動化システム事業部 カード・セキュリティシステム営業部
博士（理学）
Toshiba Infrastructure Systems & Solutions Corp.

畠中　一成　HATANAKA Issei
東芝インフラシステムズ（株）セキュリティ・自動化システム事業部 カード・セキュリティシステム営業部
Toshiba Infrastructure Systems & Solutions Corp.