組織間の安全な情報共有を実現する「MAGIC」の情報ガバナンスソリューション

Paul Wang　Kang Wei Woo　Jens-Matthias Bohli　Joao Girao　Ghassan Karame　Wenting Li

要 旨

都市計画担当者が直面する課題を解消するには、多くのケースで各種の行政機関の協力が必要です。問題解決には多様な組織の関与が必要なものの、それらの組織の慣例や作業手順は互いに矛盾することがあります。各機関が協調して対応するには、セキュリティ権限の異なる各機関がこうした矛盾に影響されることなく、シームレスに課題に貢献できなくてはなりません。NECの省庁間連携ソリューション「Multi-AGencies, 1 Concert（MAGIC）」（マジック）は、個々の行政機関が保有するリソースや情報の共有化を、セキュリティモデルを損なわずに実現できるプラットフォームを提供します。これを可能にするには、適切な情報ガバナンスを行える仕組みが必要です。本稿では、「MAGIC」の情報ガバナンスソリューションにおける技術について紹介します。

KeyWords　端末正当性検証／情報ガバナンス／ユーザーアクセス制御／省庁間連携／電子証拠

1. はじめに

治安や安全に関わる行政機関や世界中の都市計画担当者が、都市をより安全にするための取り組みを続けているなかで、異なる行政機関の間でのデバイスや情報の共用が重要になっています。警察や救急サービス、陸上輸送、環境、水道などに関わる行政機関は、都市全体の監視計画に従い、連携して都市の観察や火災や洪水の監視を行うことにより、さまざまな脅威の兆候を把握しようとしています。目的に合ったリソースを共用することで、行政機関は重大な状況にいち早く気付き、最適な対応を取れるようになったり、予想される事態に陥ることを回避したりすることさえ可能になります。

しかし、リソースの共用には情報ガバナンスの問題が伴います。NECの省庁間連携ソリューション「Multi-AGencies, 1 Concert（MAGIC）」（マジック）は、端末正当性検証機能とアクセス制御機能を提供します。

端末正当性検証機能は、さまざまな行政機関の設置する機器がセキュリティ侵害されておらず、そこからアクセスできる情報に信頼性があることを保証します。

これに加え、アクセス制御機能は、多元的なアクセス権限によって情報を保護しつつ、さまざまな省庁から必要な情報へ的確にアクセスすることを可能にします。これは、ある状況に協働して対処している各行政機関に対して、個々のセキュリティポリシーに従いながら、正当なユーザーが、正当な場所から、正当な状態で、need-to-know原則（情報は知る必要のある人にのみ開示するという原則）に基づいてデータセットにアクセスできることが保証されている、ということを意味します。

2. 端末正当性検証機能

2.1 モバイルデバイスのための端末正当性検証

最近では、信頼性が検証されていないデバイスに対するリモート認証がますます必要とされており、さまざまなコンピューティング環境において、静的あるいは動的にルート・オブ・トラスト（信頼基点）を生成するため多くの提案がなされています。既存のソリューションのほとんどは、モバイルデバイスにセキュリティチップ（Trusted Platform Module：TPM）を組み込むことで、デバイス自体を信頼基点とすることを目指しています[1) 2)]。しかし、標準的なPCプラットフォームで信頼基点の生成を実現するアーキテクチャは数多く存在しますが、モバイルデバイスや組み込みデバイスへ適用しようとすると容易ではありません。

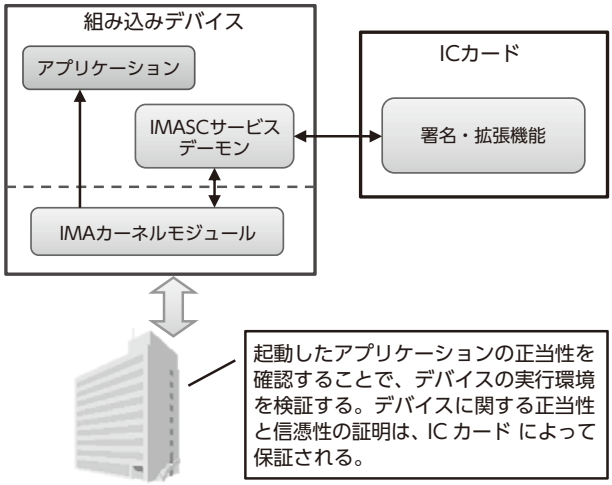

図１　IMASCのアーキテクチャ概要

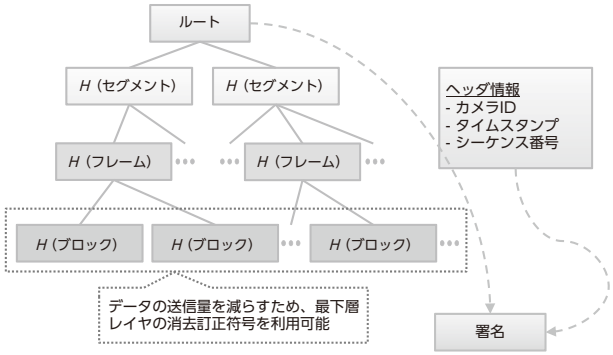

図２　セマンティック映像データへの適応ハッシュ木

NEC 欧州研究所のIMASC技術は、TPMに依存しなくても、モバイルデバイス内部でセキュアな認証されたブートを可能にし、既存のソリューションの欠点に対処しています。IMASCはソフトウェアベースの正当性検証ソフトウェア（例えばIBMのIMA[2)]）を利用して、デバイス内の全ての実行可能コードを読み込み前に計測します。IMASCはまた、カーネルとデバイス内のICカードとのインタフェースだけを行う新しいサービスを開始します。実行中のバイナリを計測するためのシステムコールを傍受すると、カーネルはすぐに計測結果をICカードへ送信し、認証が行われます。

IMASCは更に、ICカード上の特別に設計されたJavaアプレットにより、簡単な暗号処理とカウンタのみを使用して、TPMが本来提供していた拡張専用機能をエミュレートします。こうした仕組みにより、デバイスに保存された計測ログを破損・削除・変更する可能性のある攻撃者が存在しても、セキュリティを保証します。これらがIMASCの主な特長です（図1）。

2.2 映像否認防止（映像データの信頼性検証）

映像監視カメラは、物理的脅威の検知や犯罪の捜査支援を目的に、公的私的を問わず広範な場所に展開されています。この結果、映像監視で得られたデータを証拠として裁判で使用するためには、否認防止証拠と呼ばれる信憑性と正当性の証明が必要となります。

しかし、既存ソリューションのほとんどは、映像ソースの信頼性を認証するため、映像ストリームのデジタル署名をネットワークレイヤで確認することに専念しています。このため、この認証工程は複雑で、大きなストレージと多量の演算を必要とします。

NEC 欧州研究所の映像否認防止技術は、実際の映像符号化手順に基づいており、メタデータを最小限追加することでデータソースからの再計算が行えます。また、適応ハッシュ木を利用することにより、否認防止証拠を映像のブロック単位からフレーム単位、またはセグメント単位にまで、伝送回線の品質に応じて、減らすことができます（図2）。更にこの技術は映像データの部分的喪失を許容しているため、データの一部が喪失した場合でも映像の残りの部分の信憑性を確認することができます。

こうした特長に加え、カメラモジュール内に搭載したIMASCソリューションを利用して、映像作成時にソフトウェアがセキュリティ侵害を受けていないことを確認しています。これにより、映像が検知不能な形で改ざんされていないこと、デジタル署名がその後に生成されたこと、といった否認防止証拠に関する付加的保証を提供できます。

3. アクセス制御機能

センサやカメラが広範なInternet of Things（モノのインターネット）に接続された状態では、さまざまな行政機関が監視用インフラを効果的に活用できることが重要になります。例えば、カメラは保安機関と環境機関の両方から同時に利用可能なのか、誰が撮影映像にアクセス可能なのか、誰が駅などの特定の場所にいる疑わしい人物の分析結果を見ることができるのか、などに応えられなくてはなりません。

その解決となるのは、未来の安全な都市に向けたソ

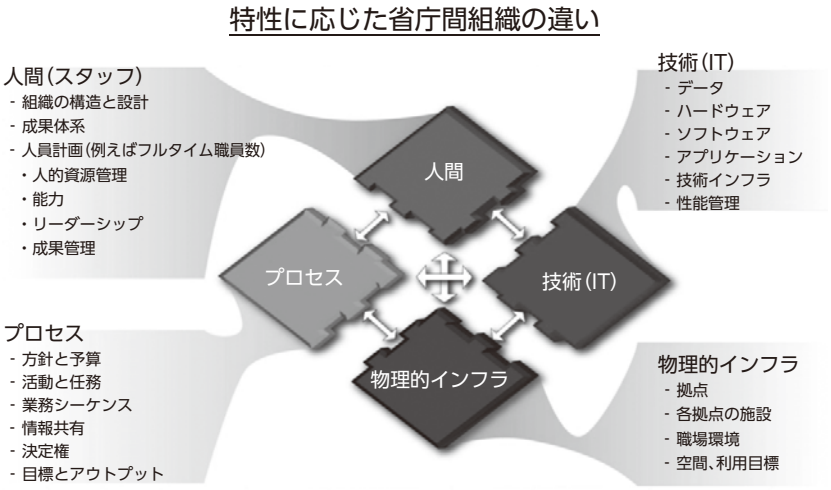

図3　オーソリゼーションと制御

リューションで鍵となる、情報ガバナンスです。MAGICのアクセス制御機能は単なる認証サーバではなく、安全な都市に関わるシステム全体のアクセスポリシーを定め、市民のプライバシーを守りながら、権限を持つ行政機関のユーザーに権利を与えるものです。

アクセス制御を行うセンターサーバは、慎重な扱いを要する情報へのアクセス権限を持つユーザーにはその情報を即座に取得できるようにし、権限のないユーザーには許可されていない情報に触れさせない、といったことを可能にします。重要なことは、アクセスを必要とする人、その人にだけアクセスを許容することです（図3）。権限に基づいたデータや情報へのアクセスを実現するため、データはロールベースアクセス制御で効果的に管理されています。

例えば実際の都市マップでは、対象となる人物や車両の追跡はアクセス権限のある人のみが行え、アクセス権限のない人は権限外のコンテンツを見ることさえできません。ここでも重要なことは、アクセスを必要とする人、その人にだけ、アクセスを許容することです。

4. むすび

アクセス制御とガバナンス方針の実施とを通じて情報や生データをセキュアに共用することで、情報は電子証拠として法廷に提出することも可能となります。デバイスとノードの完全性が強化されているので、デジタル署名入りセンサのコンテンツを否認防止に確実に利用できます。都市中に張り巡らされたサーバ、ノード、各種センサに関する完全性の状況は、固定されているかモバイルであるか、あるいはアドホックであるかに関わらず、監視可能です。

情報ガバナンスは、さまざまなリソースや情報の安全な利用を可能にします。MAGICは、異なる行政機関間に存在するインフラや技術的な障害を乗り越えることを支援し、人材活用の最適化に貢献します。また、状況の把握や安全に対する脅威への予知を向上します。

*Javaは、Oracle Corporation及びその子会社、関連会社の米国及びその他の国における登録商標です。

参考文献

1) B. Parno, et al.：Bootstrapping Trust in Commodity Computers, In Proceedings of the IEEE Symposium on Security and Privacy,2010
2) IBM：IBM 4758 Basic Services Manual Release 2.54 http://www-03.ibm.com/security/cryptocards/pdfs/IBM_4758_Basic_Services_Manual_Release_2_54.pdf

執筆者プロフィール

Paul Wang
Global Safety Division
CTO、Head of Strategy & Management

Kang Wei Woo
Global Safety Division
Technical Director

Jens-Matthias Bohli
NEC Europe Ltd.
NEC Laboratories Europe
Chief Researcher

Joao Girao
NEC Europe Ltd.
NEC Laboratories Europe
Manager

Ghassan Karame
NEC Europe Ltd.
NEC Laboratories Europe
Senior Researcher

Wenting Li
NEC Europe Ltd.
NEC Laboratories Europe
Research Scientist

関連URL

NEC Public Safety Portal
http://www.nec.com/safety

NEC技報のご案内

NEC技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報(日本語)

NEC Technical Journal(英語)

Vol.67 No.1　社会の安全・安心を支えるパブリックソリューション特集

社会の安全・安心を支えるパブリックソリューション特集によせて
NECが目指すパブリックソリューションの全体像
NECのパブリックセーフティへの取り組み

◇ 特集論文

効率・公平な暮らし

マイナンバー制度で実現される新しいサービス
ワールドカップを支えた「NECのスタジアム・ソリューション」
魅力あふれるフライトインフォメーションシステムの実現
駅の新サービス実現を加速するSDNソリューション
マルチデバイス対応テレビ電話通訳の通訳クラウドサービス
カラーユニバーサルデザインを採用した使いやすいスマートフォン向けネットバンキングサービス
安全・安心を実現する世界一の顔認証技術
顔認証製品と社会ソリューションでの活用

安全・安心な暮らし

ICTを活用したヘルスケアへの取り組み
組織間の安全な情報共有を実現する「MAG1C」の情報ガバナンスソリューション
「MAG1C」における大規模メディア解析及び共有デジタルサイネージ機能
シンガポールにおけるより安全な都市「セーファー・シティ」の構築
アルゼンチン ティグレ市の未来を守るビデオ解析ソリューション
群衆行動解析技術を用いた混雑推定システム
音声・音響分析技術とパブリックソリューションへの応用
昼夜を問わず24時間監視を実現する高感度カメラ
人命救助を支援するイメージソリューション
Emergency Mobile Radio Network based on Software-Defined Radio

重要インフラの安全・安心

新幹線の安全・安定輸送を支える情報制御監視システム
水資源の有効利用をICTで実現するスマートウォーターマネジメント技術の研究開発
センサとICTを融合させた漏水監視サービス
沿海域の重要施設へ接近する不審対象を監視する港湾監視システム
インバリアント解析技術(SIAT)を用いたプラント故障予兆監視システム
赤外線カメラの画像処理技術と応用例
高度化するサイバー攻撃への取り組み「サイバーセキュリティ・ファクトリー」

社会の安全・安心を支える先端技術

国家基盤を支える指紋認証の高速高精度化技術
次世代放送を支える超高精細映像圧縮技術とリアルタイム4K映像圧縮装置

◇ NEC Information

NEWS

NEC「衛星インテグレーションセンター」の稼働を開始
陸上自衛隊の活動を支える「浄水セット・逆浸透2型」の開発

Vol.67 No.1
(2014年11月)

特集TOP