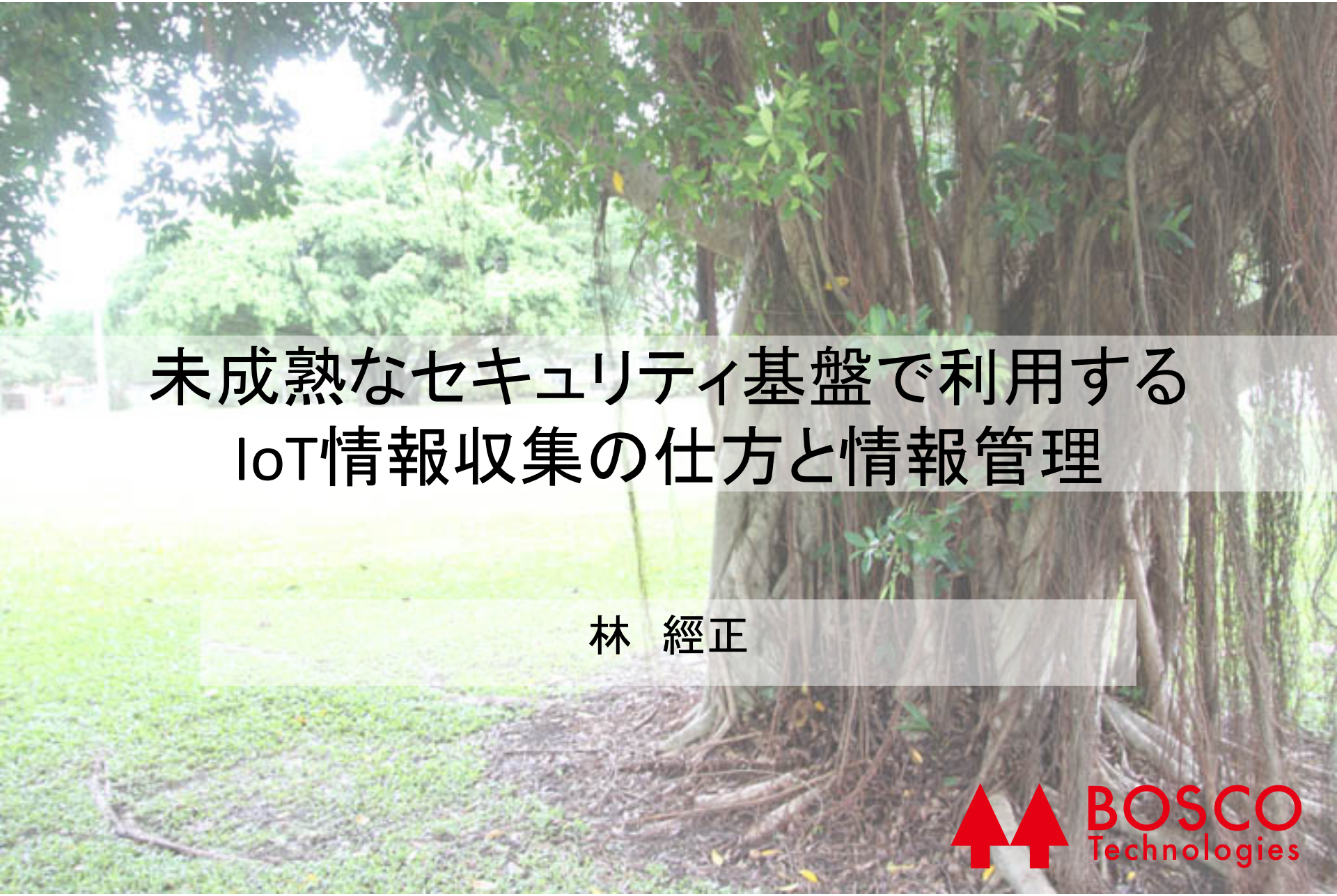


未成熟なセキュリティ基盤で利用するIoT情報収集の仕方と情報管理

林　經正

BOSCO Technologies

アジェンダ

- IoTの未成熟なセキュリティ基盤
- IoT情報の収集制御の課題
- IoT情報へのアクセス制御の課題
- 上記2つの課題を解決する技術
  - ビジネスコード
  - ユニバーサル・アクセス制御

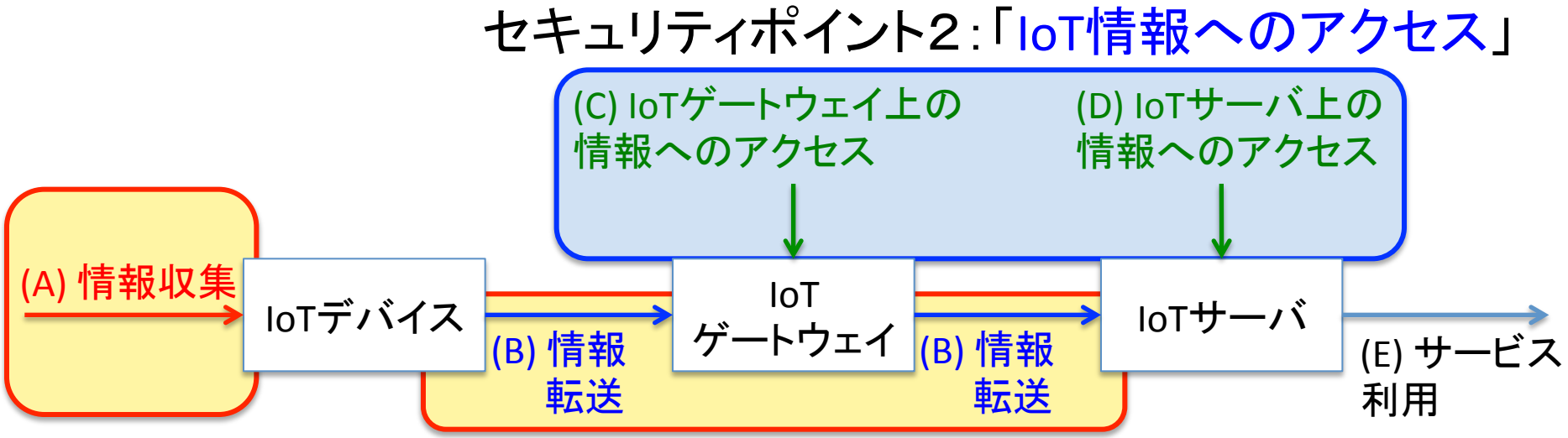
自己紹介と、会社紹介

- 株式会社ボスコ・テクノロジーズ・代表取締役
  - 東工大修士修了→NTT→ベンチャー数社
- 会社概要
  - 自動化・仮想化・セキュリティ技術に強み
  - 直接お客様の声を聞ける環境でシステム開発・運用
  - 最先端技術を利用した製品開発
  - 全世界数万台のサーバ・ネットワーク機器を運用
- IoTゲートウェイの開発などに従事
  - 情報・機能制御（データ収集、データへのアクセス）
  - ICT上のリソースの最適化制御技術に関する技術開発
    - 産学連携で基礎研究を実施
    - 他社には無いサービスを提供する自社製品開発

IoTの未成熟なセキュリティ基盤：①～④

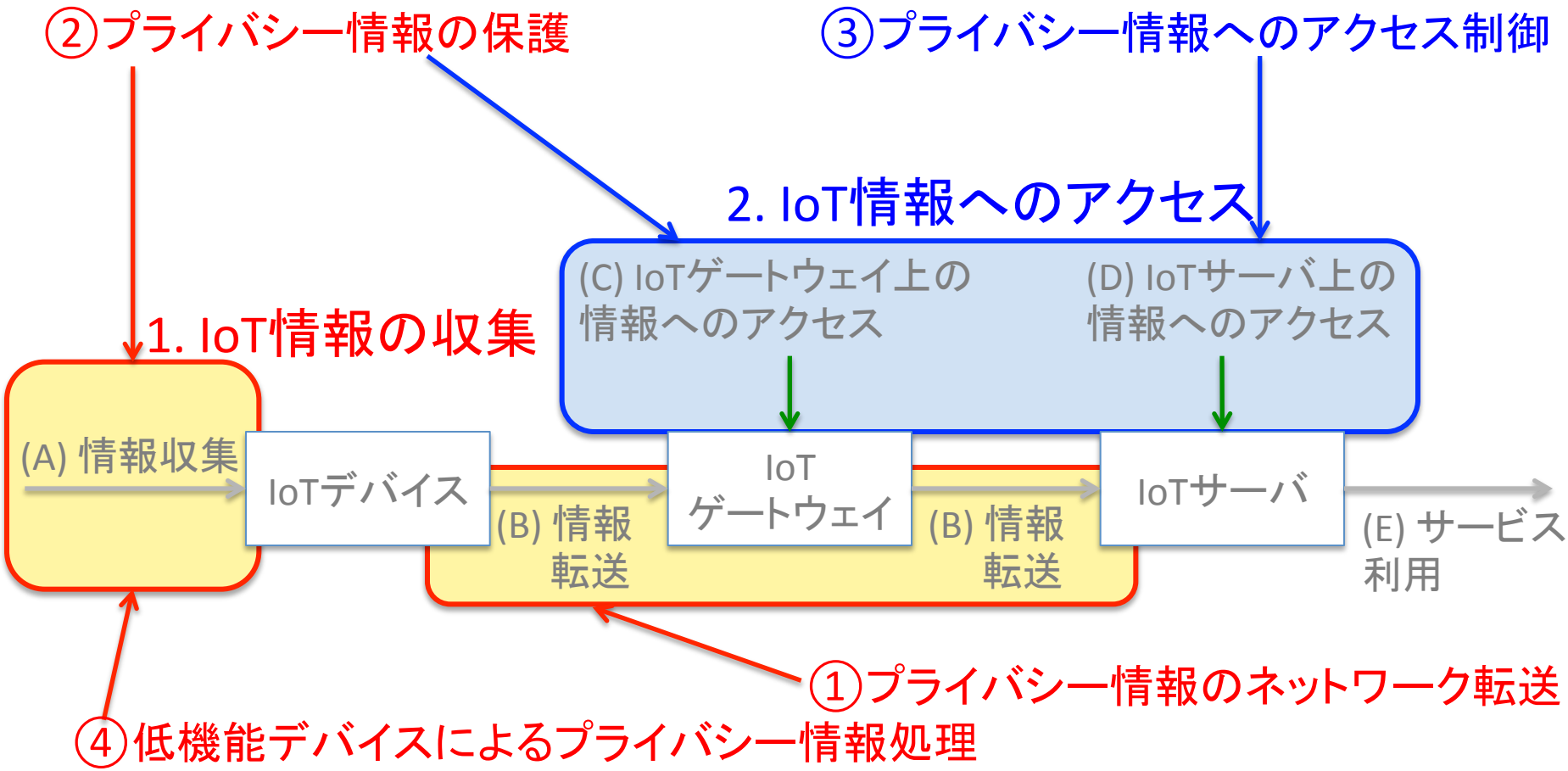
- 重要なプライバシー情報、機密情報等を本講演では、「プライバシー情報」として表現
- プライバシー情報の制御技術が確立されていない
  - ① プライバシー情報のネットワーク転送
  - ② プライバシー情報の保護
  - ③ プライバシー情報へのアクセス制御
- 低機能IoTデバイスのセキュリティ脆弱性
  - 車等に搭載する高機能デバイス
    - 複雑な暗号化処理などを実現しやすい
  - カメラや小型センサーなどの低機能デバイス
    - ④ ほとんど生の情報を処理（情報送信）

IoTシステムのセキュリティは何処に注目するの？



BOSCO Technologies

未成熟なセキュリティの影響先



BOSCO Technologies

未成熟なセキュリティの影響先の整理

1. IoT情報の収集
   - ① プライバシー情報のネットワーク転送
   - ② プライバシー情報の保護
   - ④ 低機能デバイスによるプライバシー情報処理
2. IoT情報へのアクセス
   - ② プライバシー情報の保護
   - ③ プライバシー情報へのアクセス制御

未成熟なセキュリティの具体的な課題

1. IoT情報の収集制御の課題
   - 同意されずにプライバシー情報収集
   - プライバシー情報を低セキュリティでネットワークに送信
   - 第三者のプライバシー情報を容易に取得
2. IoT情報へのアクセス制御の課題
   - 誰がどのプライバシー情報にアクセスできるのか制御困難
     - 正確な制御が難しい
   - プライバシー情報へのアクセスログの正確な保存
   - 個人特定を防ぐ制御の仕組み

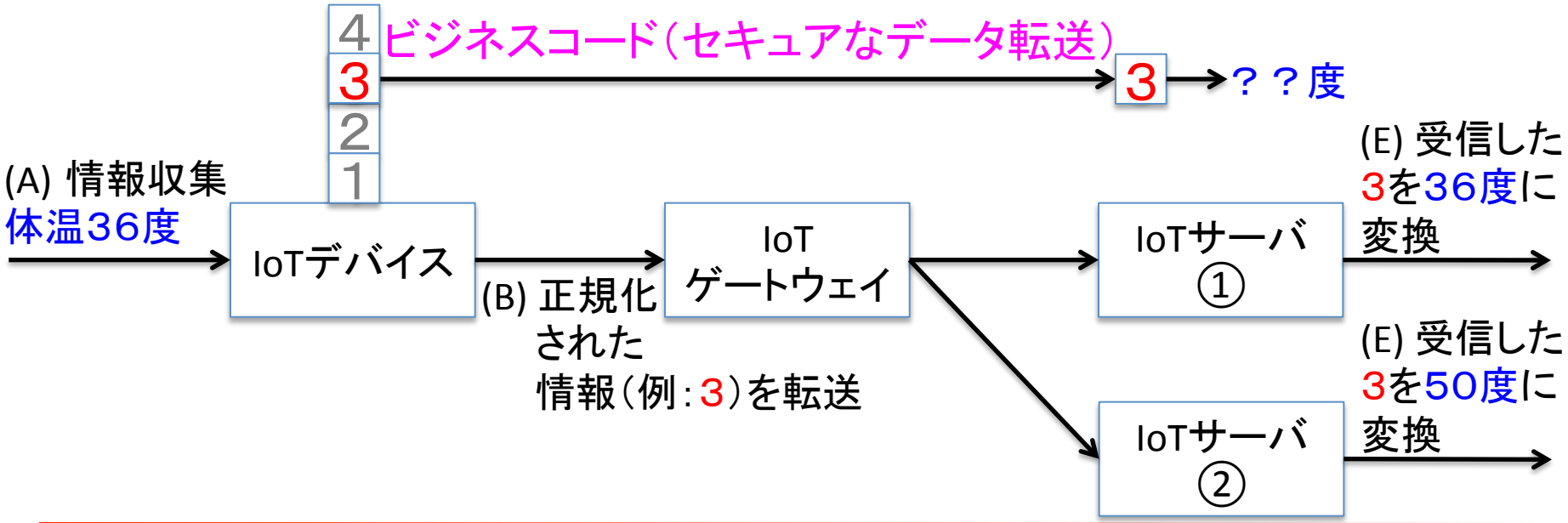
1．IoT情報の収集制御の解決技術

ビジネスコードをIoTデバイスから送信

- IoTデバイスで取得した「生」の情報をネットワークに送信しない
- 正規化された情報をネットワークに送信
- 受信した（正規化された）情報は、IoTサーバや、IoTゲートウェイで本来の情報に変換

ビジネスコードとは？

- ビジネスコードの2つの機能
  - IoTデバイスから生データの代わりにビジネスコードを送り、情報を受取る正規のサーバでのみビジネスコードを本来の情報に変換
  - IoTデバイスでは、収集した生データを正規化されたビジネスコードに変換して、ネットワークに転送
- 例1：IoTデバイスで体温36度取得し、予め決められた正規化された情報（1から4のうち3）として転送する



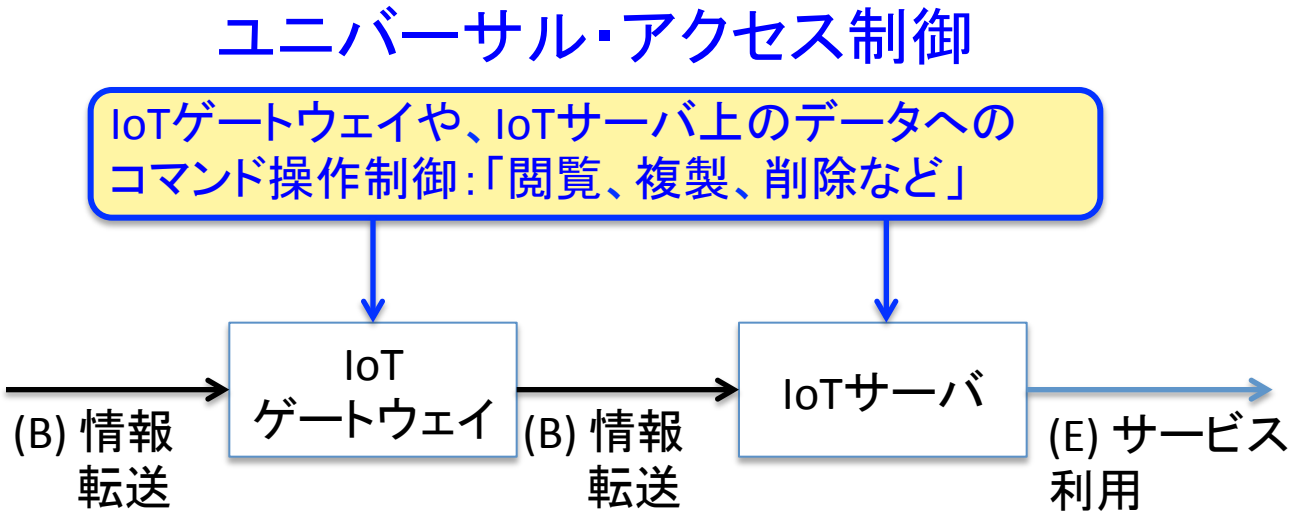
ビジネスコードの特徴と効用

- 特徴
  - 業務に合わせて、デバイス上の正規化ルールと、IoTサーバ（IoTゲートウェイ）の組合せを管理する
- 効用
  - 低機能デバイス上で容易に、低コストで実現可能
  - プライバシー情報を直接ネットワーク転送する必要が無く、セキュアな通信を実現
  - 本来受取るべきでないIoTサーバがビジネスコードを受信した場合、元の情報に復元することが難しい

2. IoT情報へのアクセス制御の解決技術

IoT情報へのアクセスは、ユニバーサル制御

- IoTサーバ（やIoTゲートウェイ）のどの様な環境でも、蓄積された情報へのアクセスを制御
- IoTサーバ上のOS等に依存せず、情報へのアクセス制御
- アクセスするユーザ毎、IoTサーバ毎にコマンド操作制御



BOSCO Technologies

ユニバーサル・アクセス制御とは？

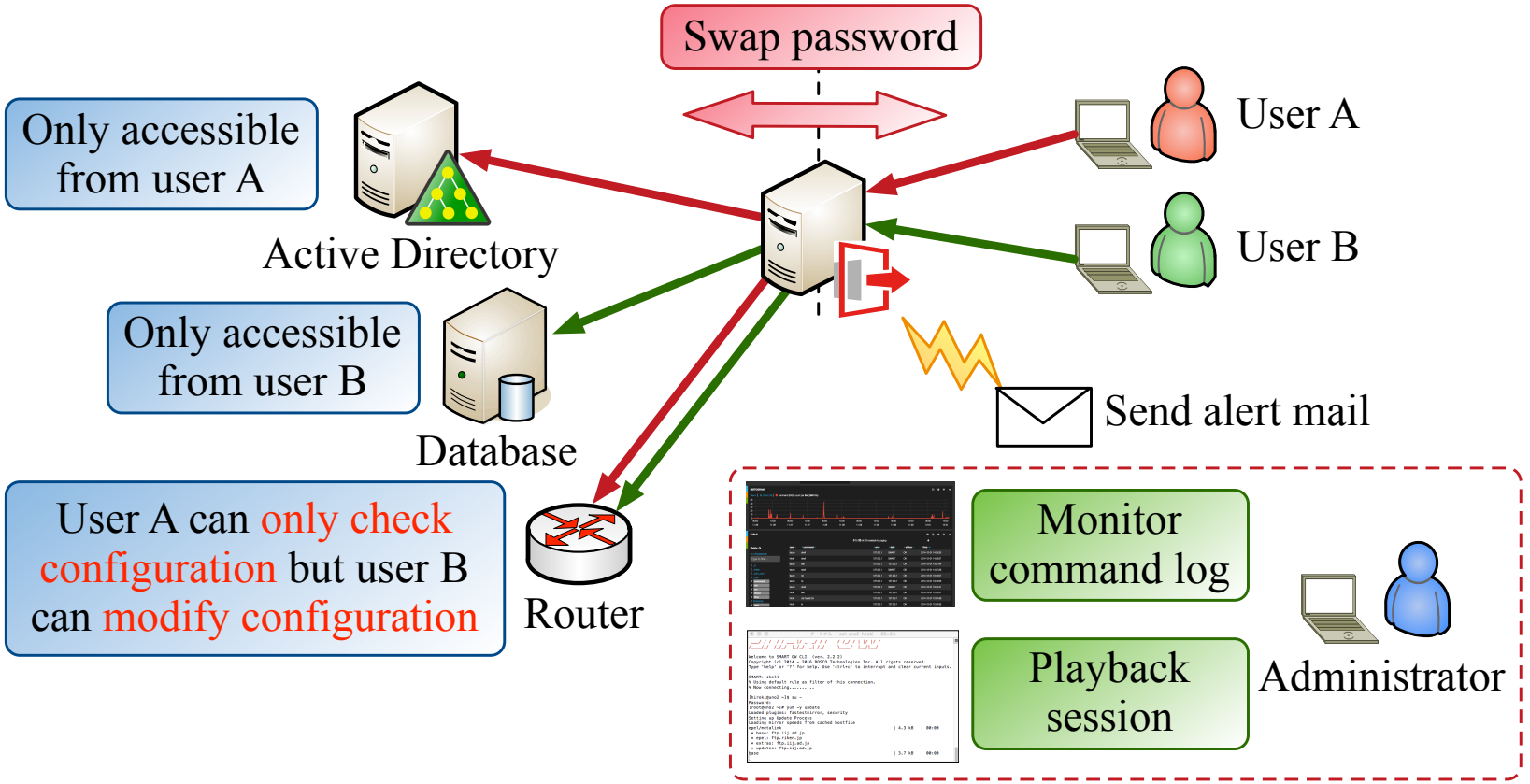
- IoTサーバ/IoTゲートウェイへのログイン操作を制限し、正確なログを記録
- ユーザ毎に各IoTサーバ/IoTゲートウェイ上のコマンド操作を制御
  - IoTサーバ/IoTゲートウェイのOSに依存せずコマンド操作出来ることが重要

ユニバーサル・アクセス制御の特徴と効用

- 特徴
  - IoTサーバ毎、情報利用ユーザ毎に利用できるコマンドを制限可能
- 効用
  - 不用意な情報閲覧、情報操作を防止
  - IoTサーバの機器の種類やOS、ファームウェアのバージョンに非依存でコマンド操作を制御可能
  - 蓄積した情報への危険な行為をリアルタイムで検知し、メール等で通知（管理）

開発したユニバーサル・アクセス制御のデモ

『SMART Gateway』という製品として実現



【SMART Gateway】 http://www.bosco-tech.com/smart-gw/
【動画デモ】 http://www.bosco-tech.com/file/SMART-GW_demo01.mp4

ユニバーサル・アクセス制御技術の導入実績

国土交通省

NTT Communications

NTT

Designing The Future KDDI

KDDI R&D LABS

すべては変革のために b-en-g

東洋ビジネスエンジニアリング株式会社

AZIA 株式会社エイジア

JDS Japan Digital Serve

J's Communication

JMT ジェイエムテクノロジー株式会社 JM Technology Inc.

MSC GROUP MSC Group

JAPAN SYSTEMS

本日の講演

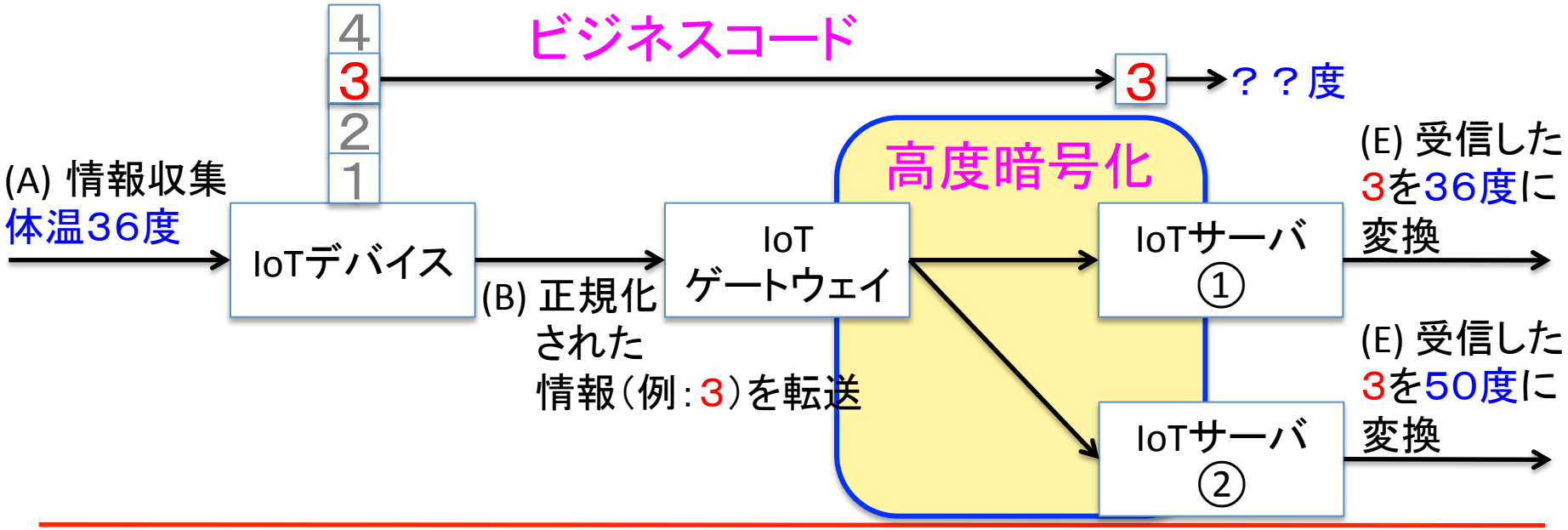
- IoTの未成熟なセキュリティ基盤
- IoT情報の収集制御の課題
- IoT情報へのアクセス制御の課題
- 上記2つの課題を解決する技術
  - ビジネスコード
  - ユニバーサル・アクセス制御

BOSCO Technologies

参考資料

よりセキュアな情報転送システム

- 低機能IoTデバイスでは、ビジネスコードを利用
- IoTゲートウェイでは、高度暗号化処理を利用
- IoTサーバでは、高度暗号化処理と、ビジネスコードを併用



ビジネスコードの本質

- 収集した情報を完全には復元できないコードに変換正規のIoTサーバでもIoTデバイスが取得した元情報には復元できず、ビジネス的に意味のある情報に変換
- 故に、不正に取得したビジネスコードから、ビジネス的に意味のある情報を取得するのは困難