IoT セキュリティチェックリスト 解説図

一般社団法人 JPCERT コーディネーションセンター

2019 年 6 月 27 日

JPCERT CC®

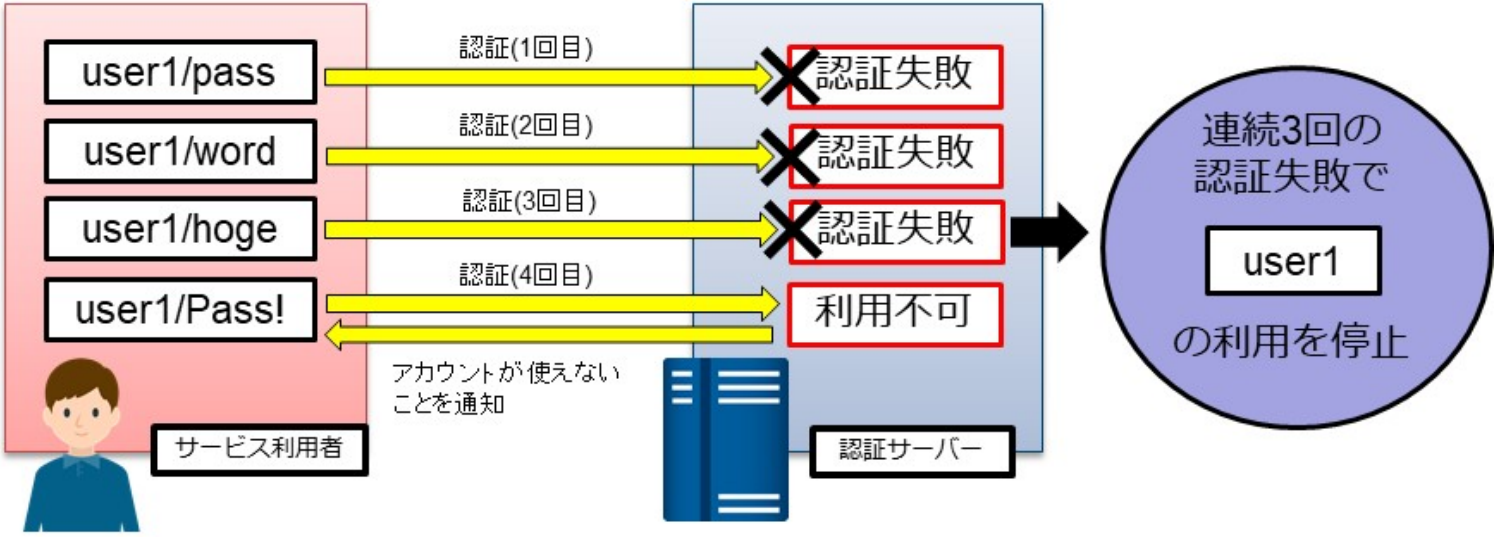
目次

JPCERT CC®

No.I-1　ユーザ管理：アカウントロックアウトメカニズム

本項目の目的：第三者が端末を不正に操作できないようにする

対　　象：Sensor、Aggregator、e-Utility、Decision Trigger



利用者：
アカウントロックに関する設定可能な内容を確認し、自身で設定したとおりにアカウントがロックされるか確認する

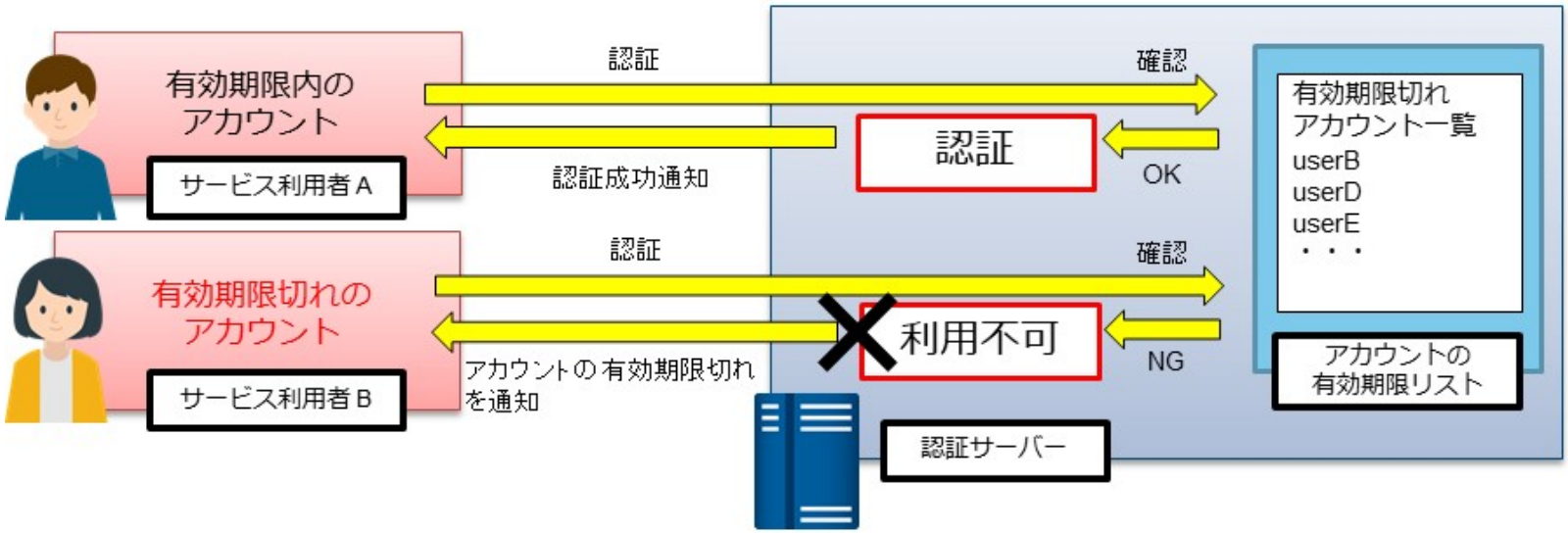
開発者：
連続した規定回数以上のログイン失敗や多重ログインなどの痕跡を確認したら、アカウントをロックし、ログインが不可になる機能を持たせる

JPCERT CC®

No.I-2　ユーザ管理：一定期間利用されていないアカウントの強制失効オプション

本項目の目的：一定期間利用されていないアカウントからのログインをできないようにする

対　　象：　Aggregator、e-Utility、Decision Trigger



利用者:
有効期限後にアカウント
が失効することを確認する

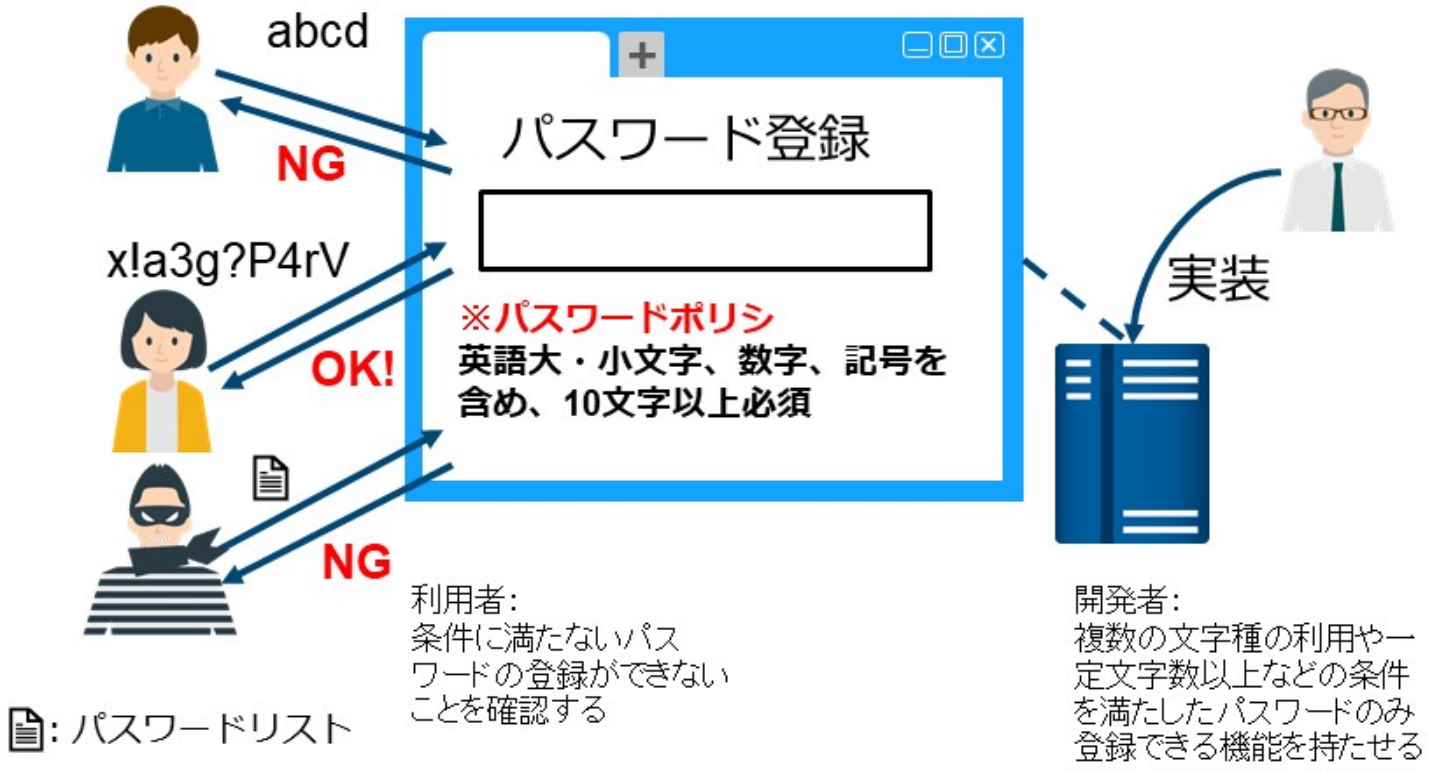
開発者:
設定した有効期限を超過した
アカウントをロックする機能を
持たせる

JPCERT CC®

No.I-3　ユーザ管理：パスワード強度の担保機能

本項目の目的：ブルートフォース、辞書攻撃などにより不正にログインされないようにする

対　　象：Aggregator、e-Utility、Decision Trigger

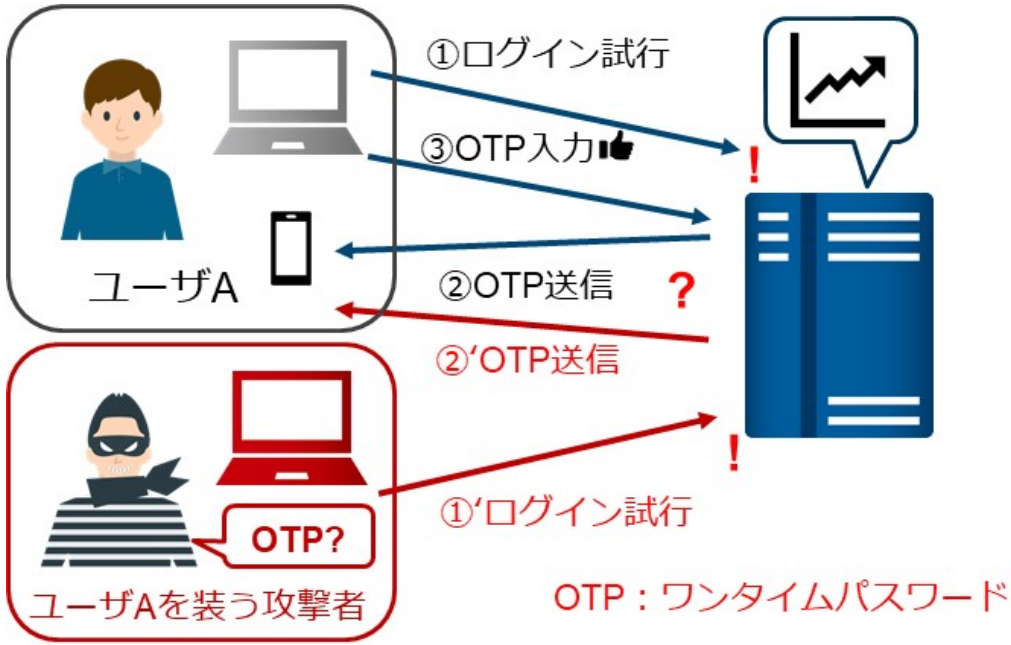


JPCERT CC®

No.I-4　ユーザ管理：パスワードセキュリティオプション（二要素認証など）

本項目の目的：第三者がシステムにログインすることを困難にする

対　　象：Aggregator、e-Utility、Decision Trigger



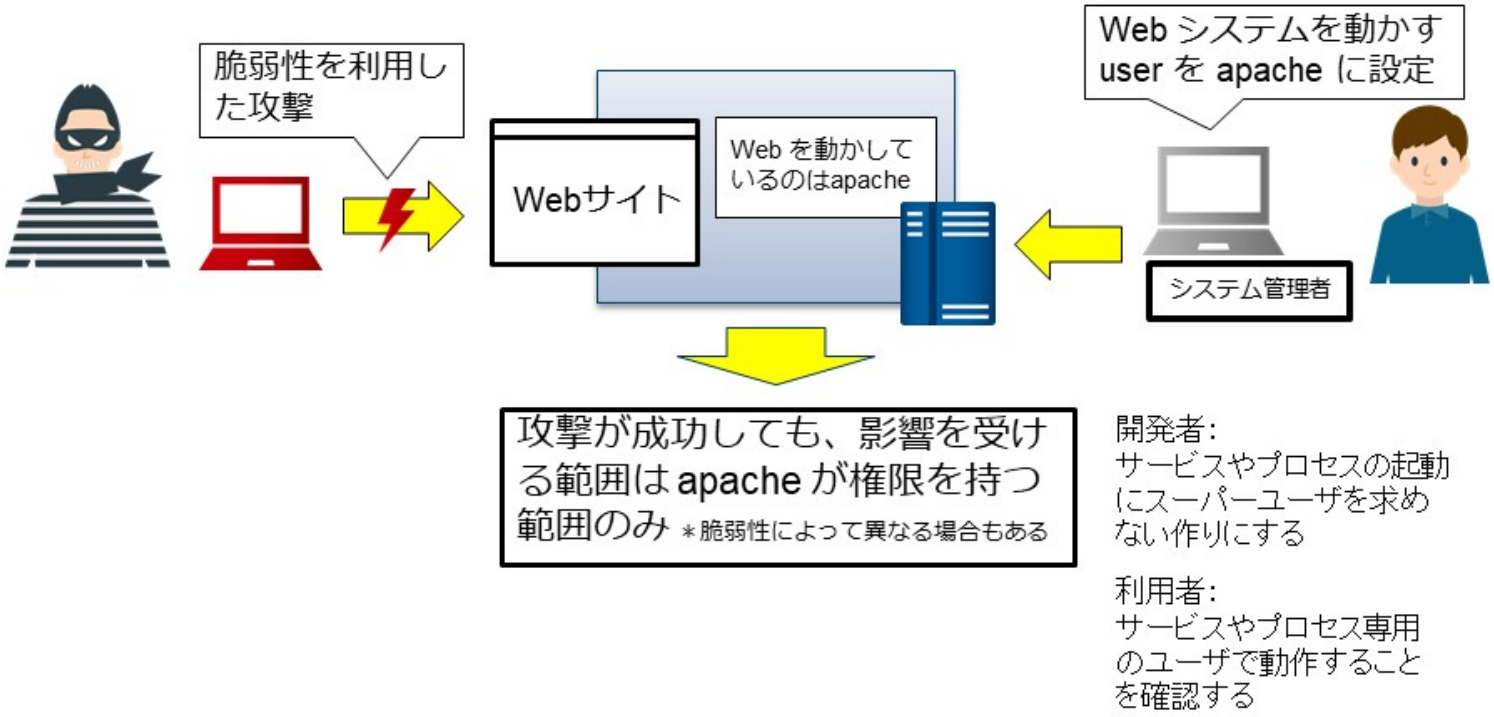
利用者:
パスワードセキュリティ
オプションが利用できる
ことを確認する

開発者:
パスワードセキュリティオプ
ションを利用できるようにす
る(例:2要素認証など)

No.I-5　ユーザ管理：サービスやプロセスを起動するアカウントの権限管理

本項目の目的：アカウント毎にサービスやプロセスを動かす権限を限定してインシデント発生時の影響範囲をサービスやプロセスの範囲内におさえる

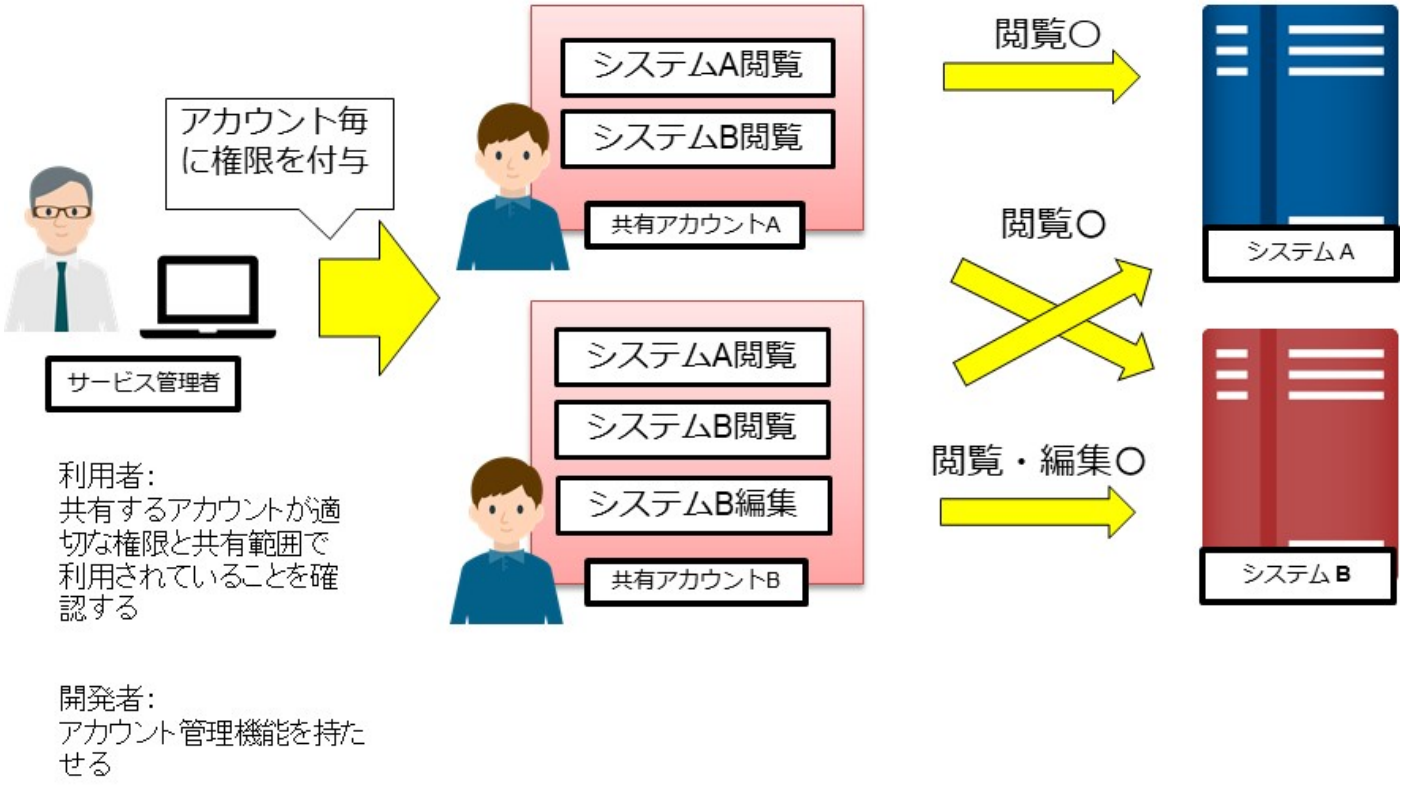
対　　象：Aggregator、e-Utility、Decision Trigger



No.I-6　ユーザ管理：共有ユーザアカウント

本項目の目的：用途に応じて適切な権限を付与できるようにする

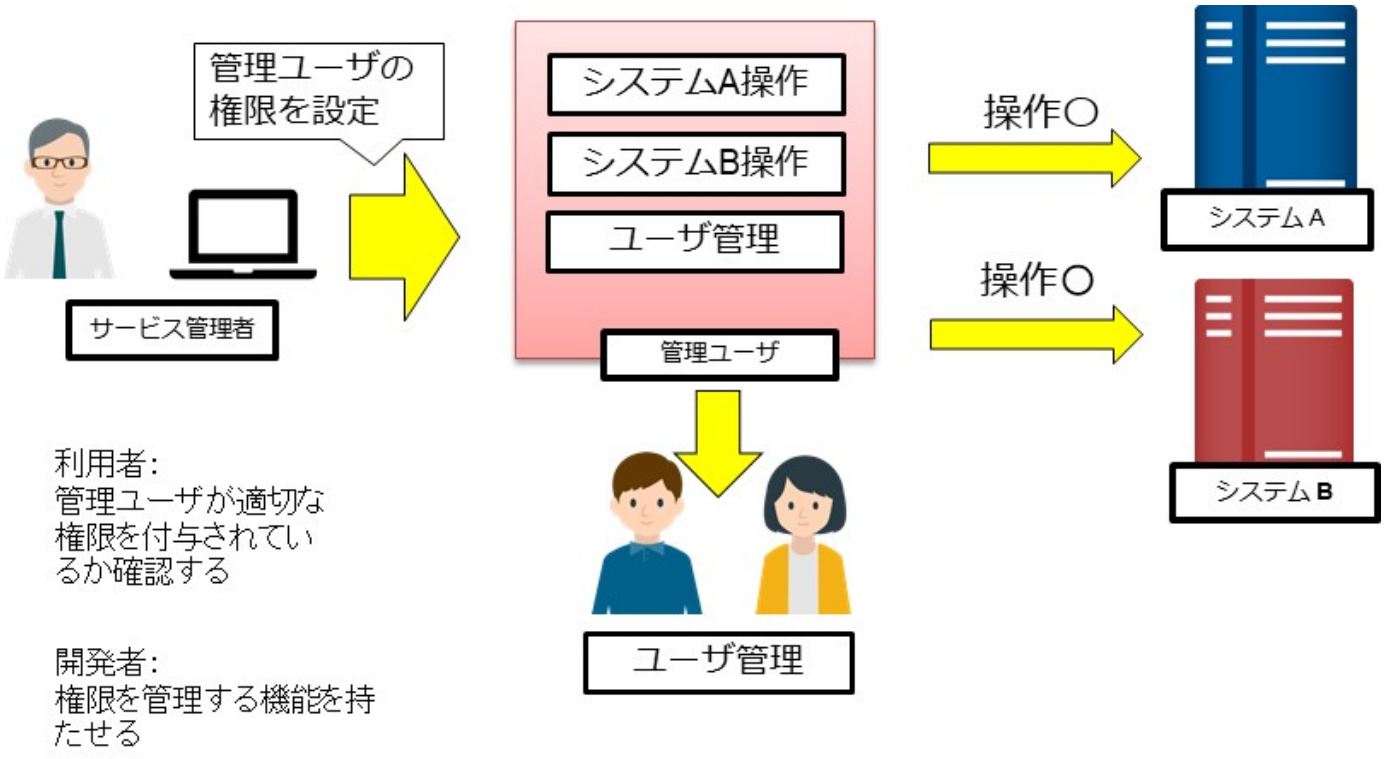
対　　象：Aggregator、e-Utility、Decision Trigger



No.I-7　ユーザ管理：管理ユーザへの適切な権限付与

本項目の目的：管理ユーザが必要な権限を使えるようにする

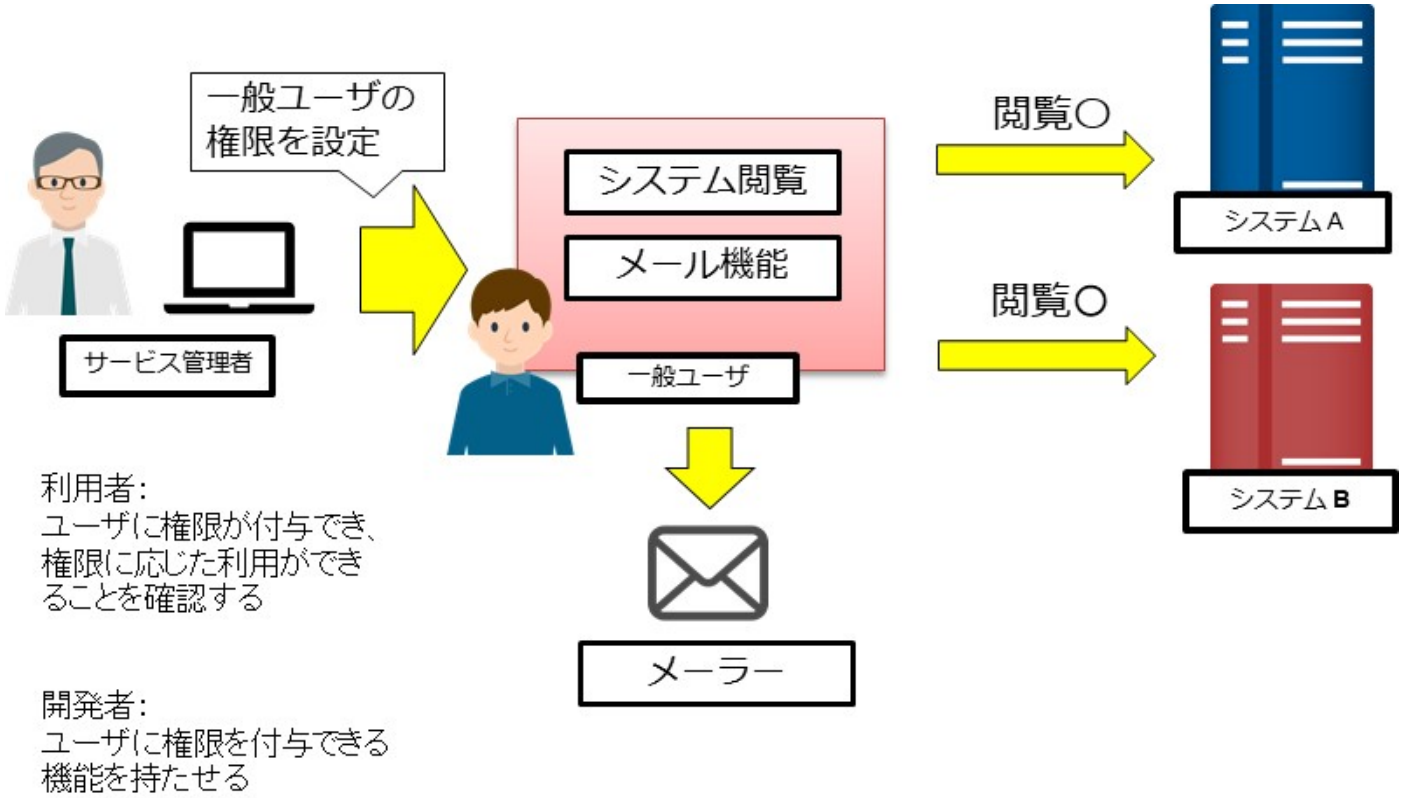
対　　象：Aggregator、e-Utility、Decision Trigger



No.I-8　ユーザ管理：一般ユーザへの権限付与機能

本項目の目的：ユーザに必要な権限のみを使えるようにする

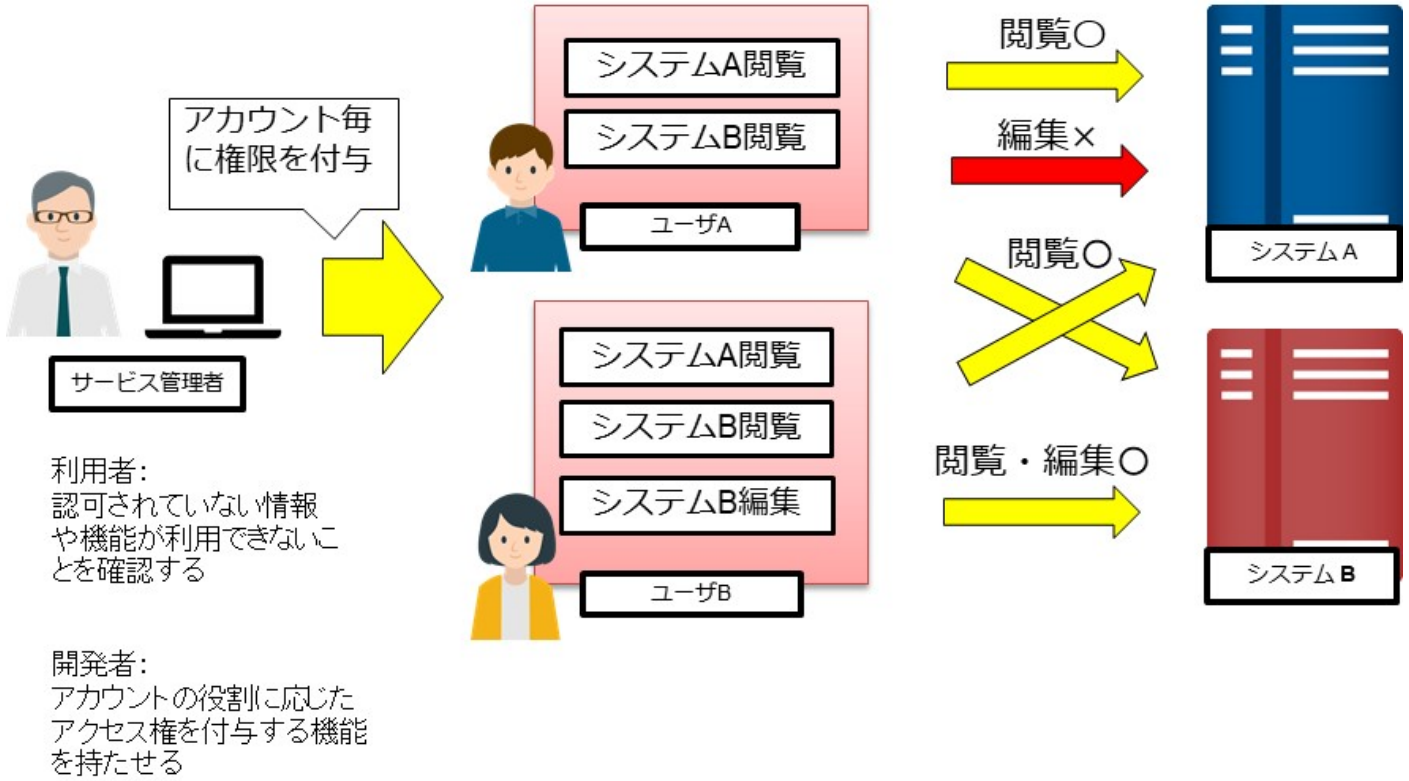
対　　象：Aggregator、e-Utility、Decision Trigger



No.I-9　ユーザ管理：認可制御機能

本項目の目的：役割に応じたアクセス権を付与できるようにする

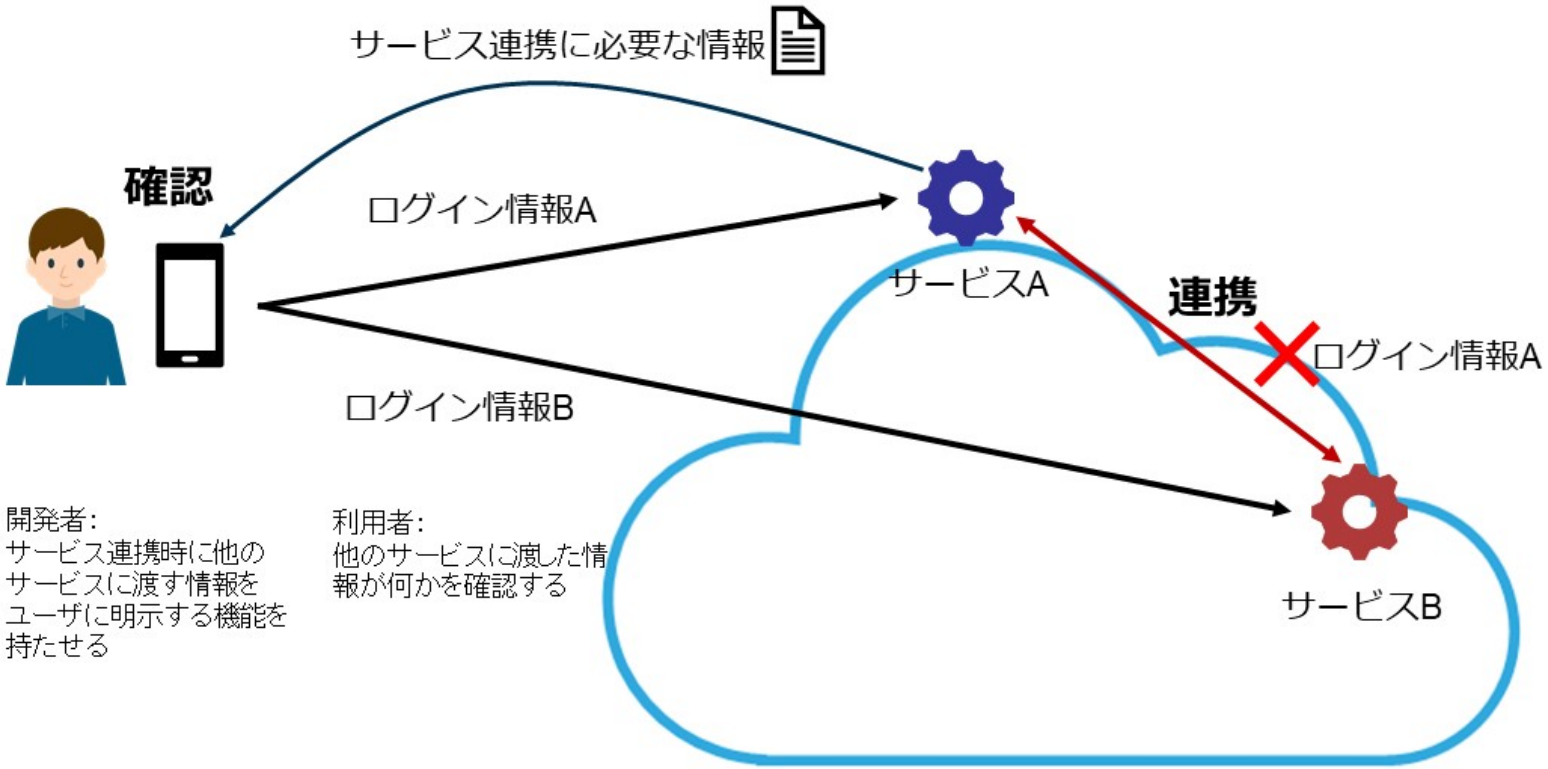
対　　象：Aggregator、e-Utility、Decision Trigger



No.I-10 ユーザ管理：サービス連携

本項目の目的：ログイン情報が必要以上に他のサービスに渡らないようにする

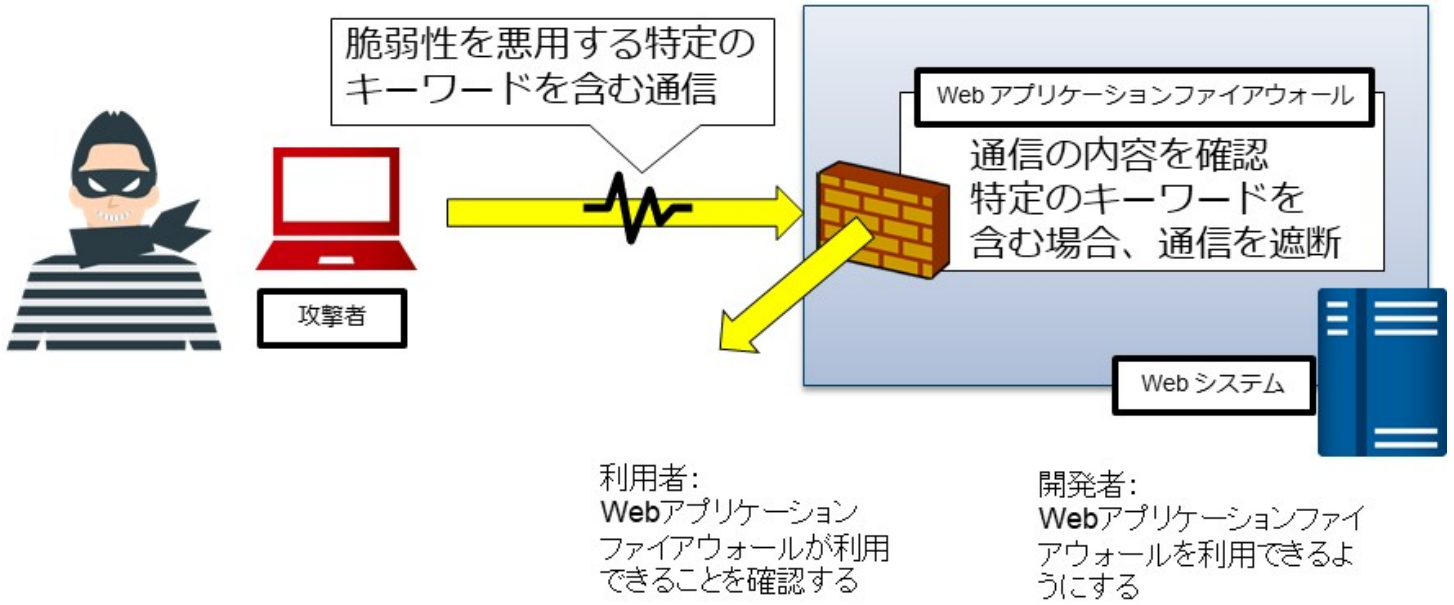
対　　象：Aggregator、e-Utility、Decision Trigger



No.II-1 ソフトウエア管理：Web アプリケーションファイアウォール

本項目の目的：Web アプリケーションファイアウォールを利用できるようにする

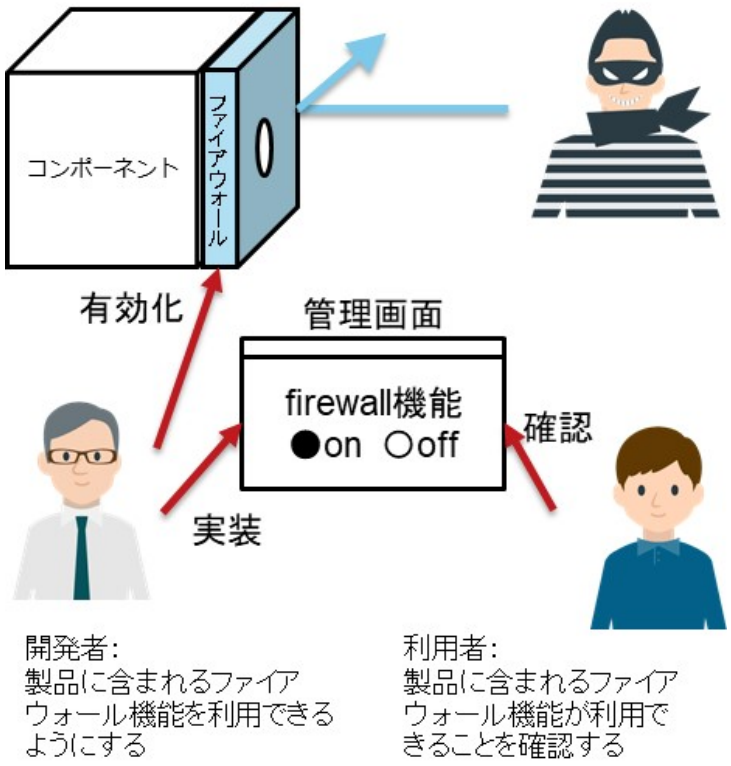
対　　象 e-Utility、Decision Trigger



No.II-2 ソフトウエア管理：製品に含まれるファイアウォール機能

本項目の目的：製品に含まれるファイアウォール機能を利用し、よりセキュアな状態にする

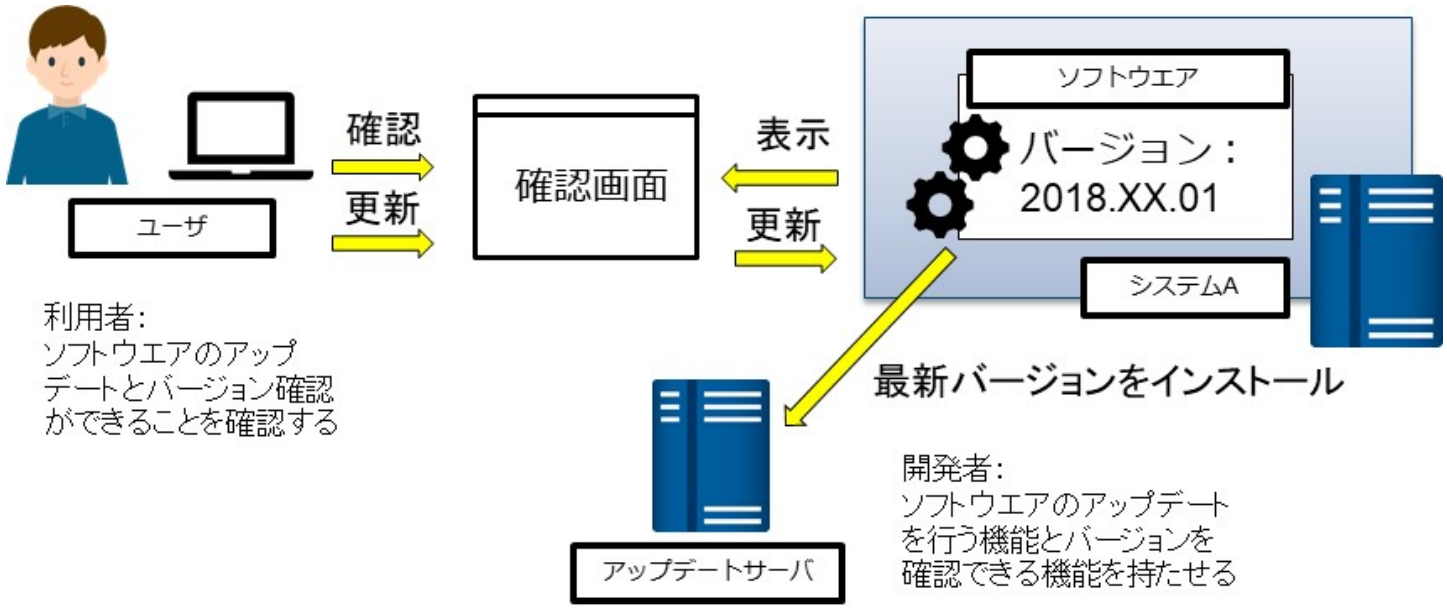
対　　象：Aggregator、e-Utility、Decision Trigger



No.II-3 ソフトウエア管理：ソフトウエアバージョン

本項目の目的：脆弱性やバグ等に対応したバージョンのソフトウエアを利用し、セキュアな状態にしておく

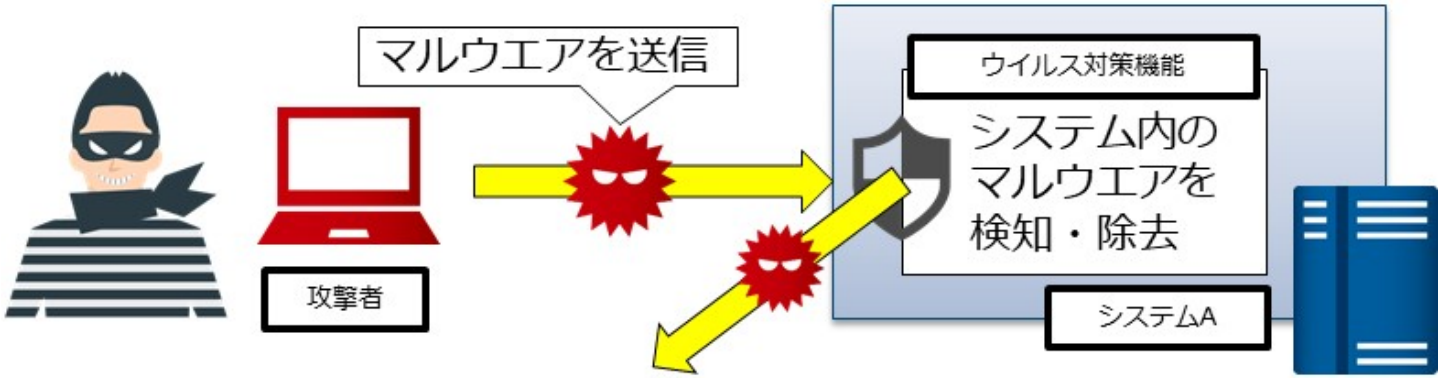
対　　象：Aggregator、e-Utility、Decision Trigger



No.II-4 ソフトウエア管理：ウイルス対策機能

本項目の目的：製品に含まれるウイルス対策機能を利用し、よりセキュアな状態にする

対　　象：Aggregator、e-Utility、Decision Trigger



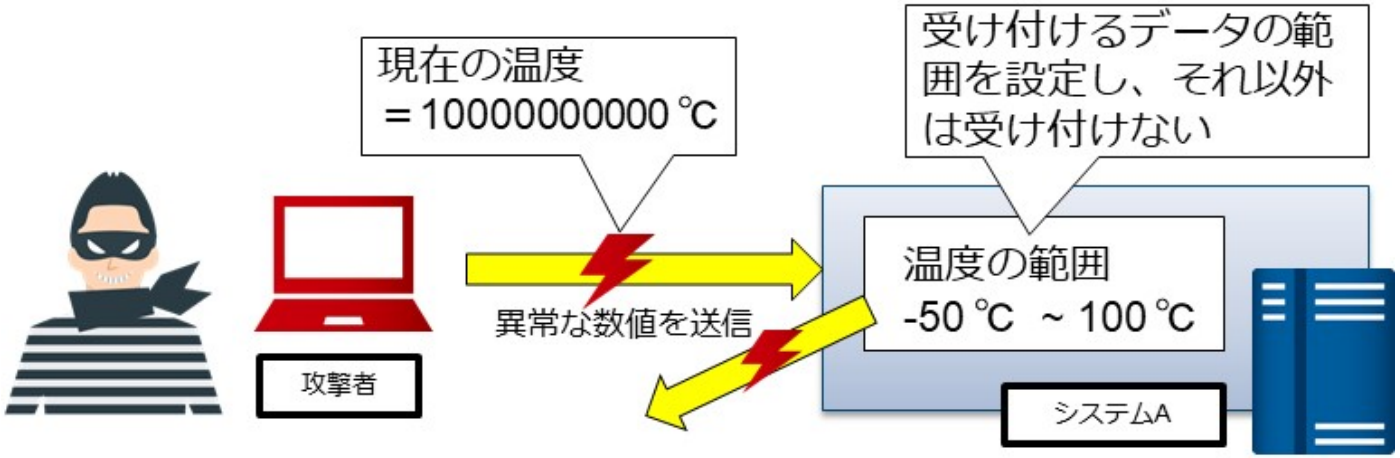
開発者:
製品に含まれるウイルス対策機能を利用できるようにする

利用者:
製品に含まれるウイルス対策機能が利用できることを確認する

No.II-5 ソフトウエア管理：不正なデータ処理

本項目の目的：システムが意図しない動作をしないようにする

対　　象：Aggregator、e-Utility、Decision Trigger

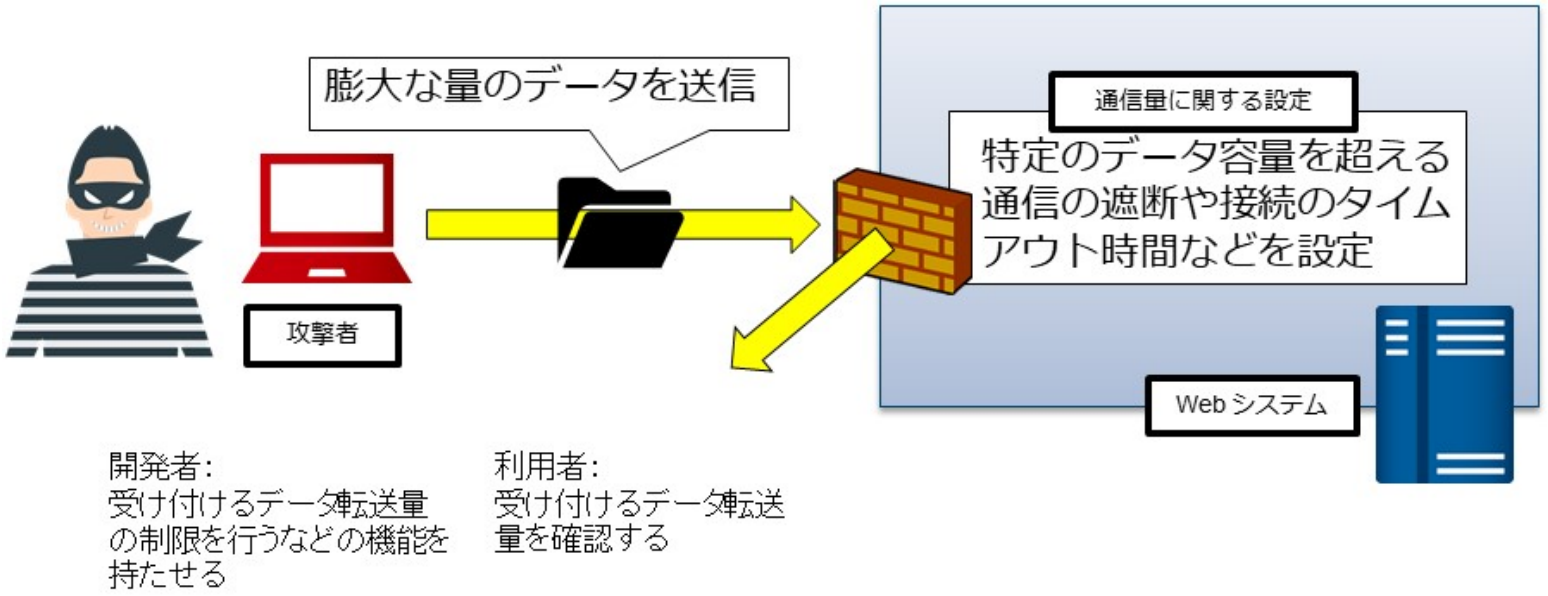


開発者：
受け付けるデータを制限する機能を持たせる

No.II-6 ソフトウエア管理：データ転送量

本項目の目的：システムのデータ転送量は DDoS 攻撃などを考慮した設計にする

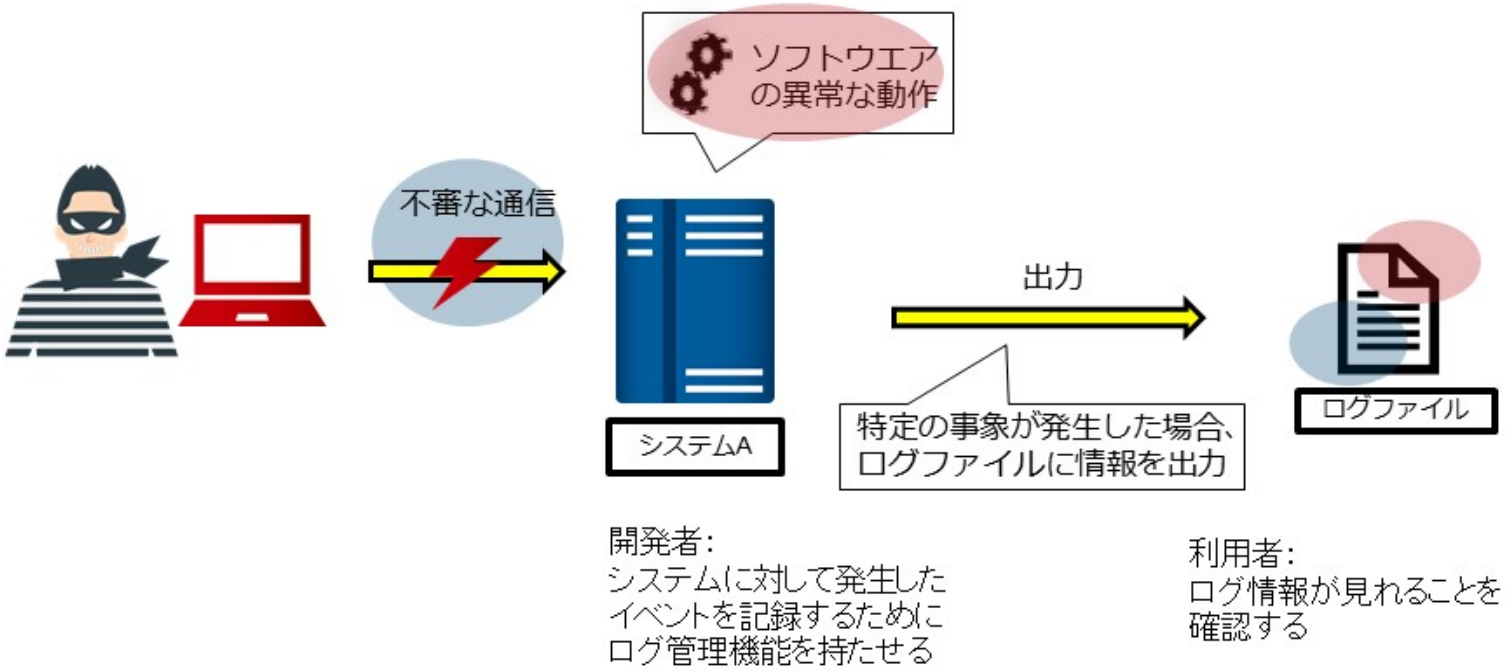
対　　象： Aggregator、Communication Channel、e-Utility、Decision Trigger



No.III-1 セキュリティ管理：ログ管理機能

本項目の目的：インシデント発生時等に事態を把握するために、ログを保存する

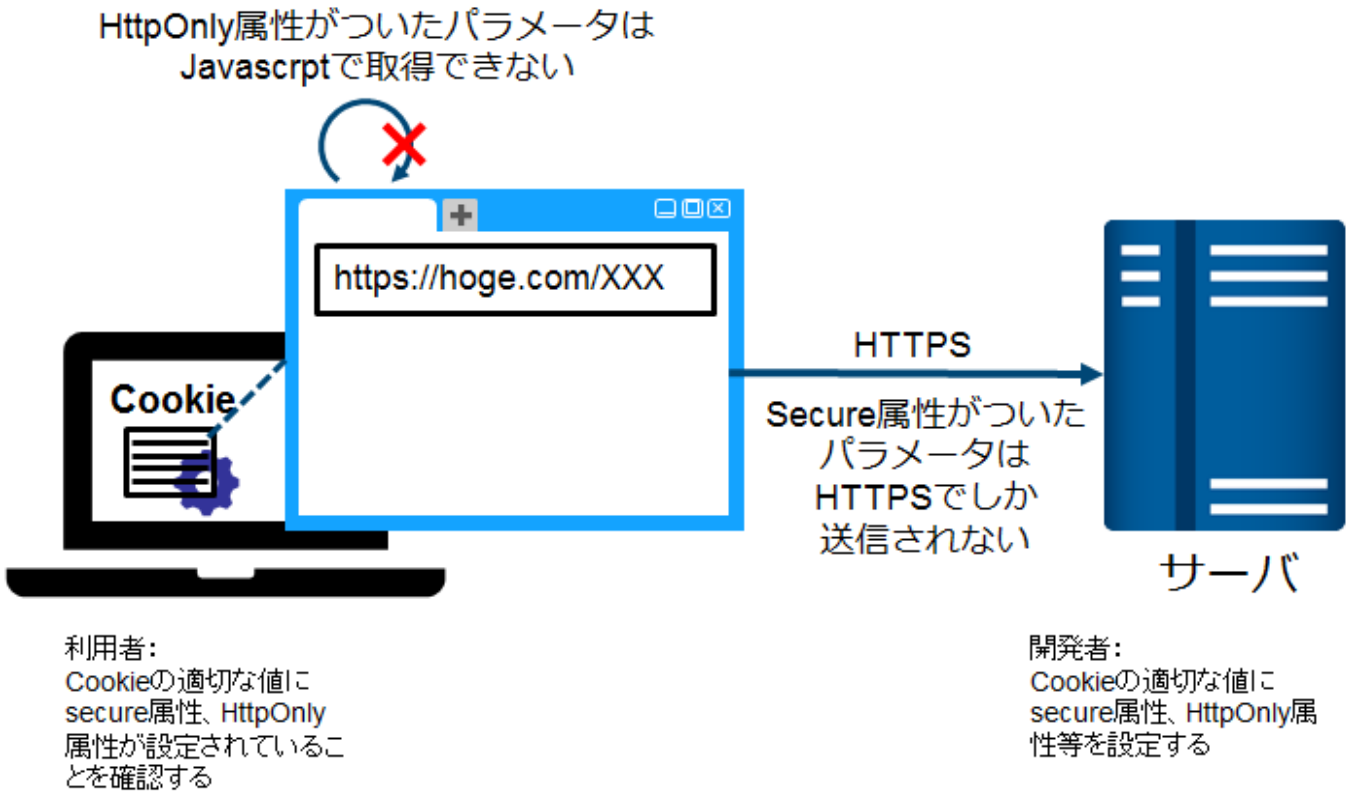
対　　象：Aggregator、e-Utility、Decision Trigger



No.III-2 セキュリティ管理：セッション管理(Cookie 設定)

本項目の目的：システムで Cookie を利用する場合、適切な属性を付与する

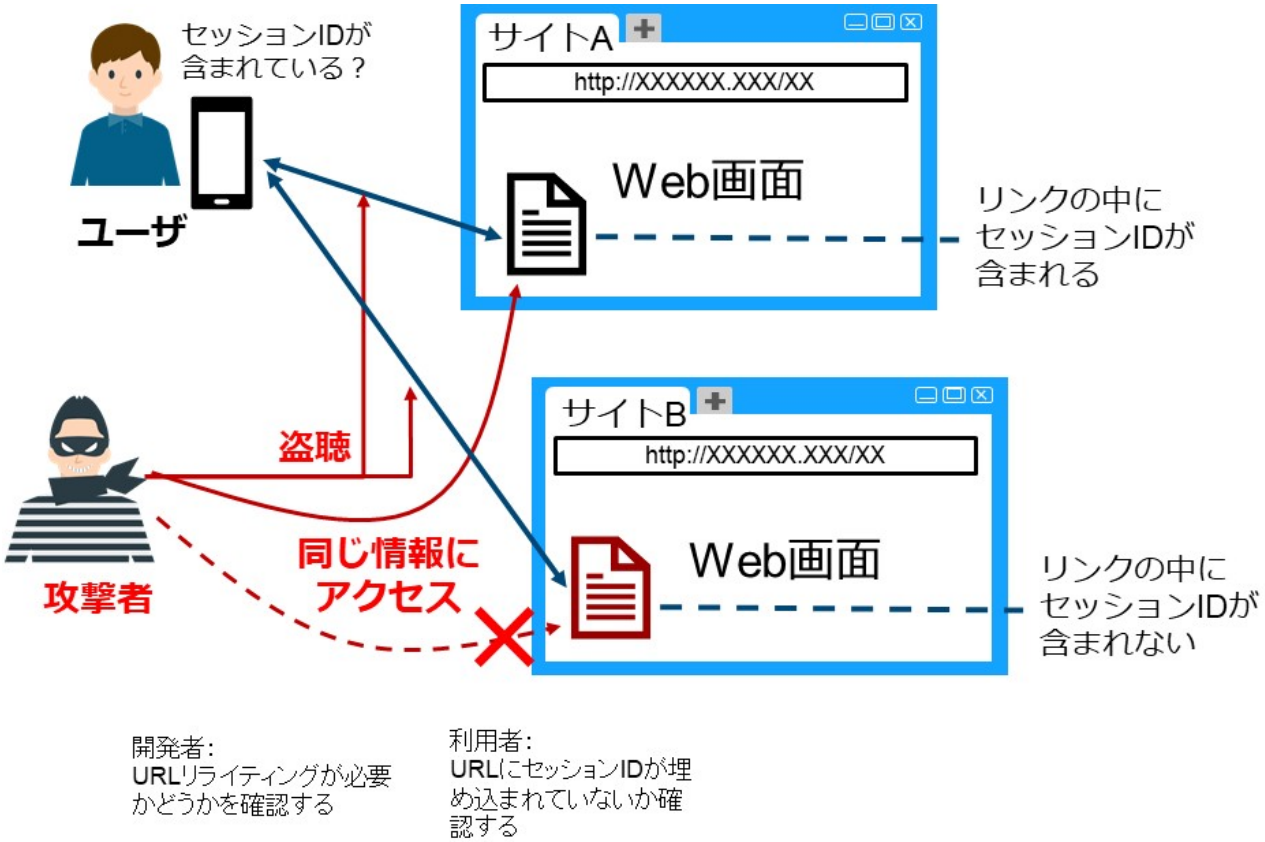
対　　象：Aggregator、e-Utility、Decision Trigger



No.III-3 セキュリティ管理：セッション管理(URL リライティング)

本項目の目的：不必要な URL リライティングによってセッション ID が漏れないようにする

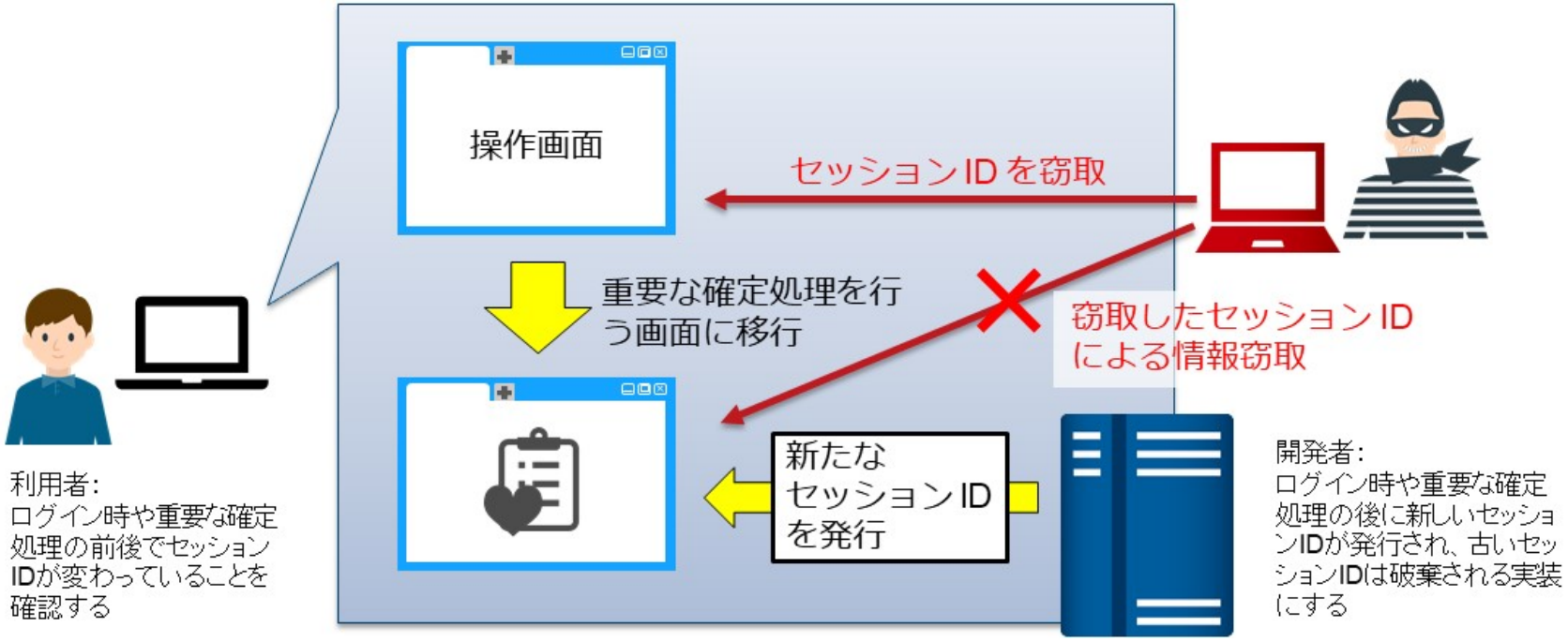
対　　象：Aggregator、e-Utility、Decision Trigger



No.III-4 セキュリティ管理：セッション管理(ログイン時や重要な確定処理の時のセッション ID の払い出し)

本項目の目的：セッション情報を盗られることによる、機密情報の窃取のリスクを低減する

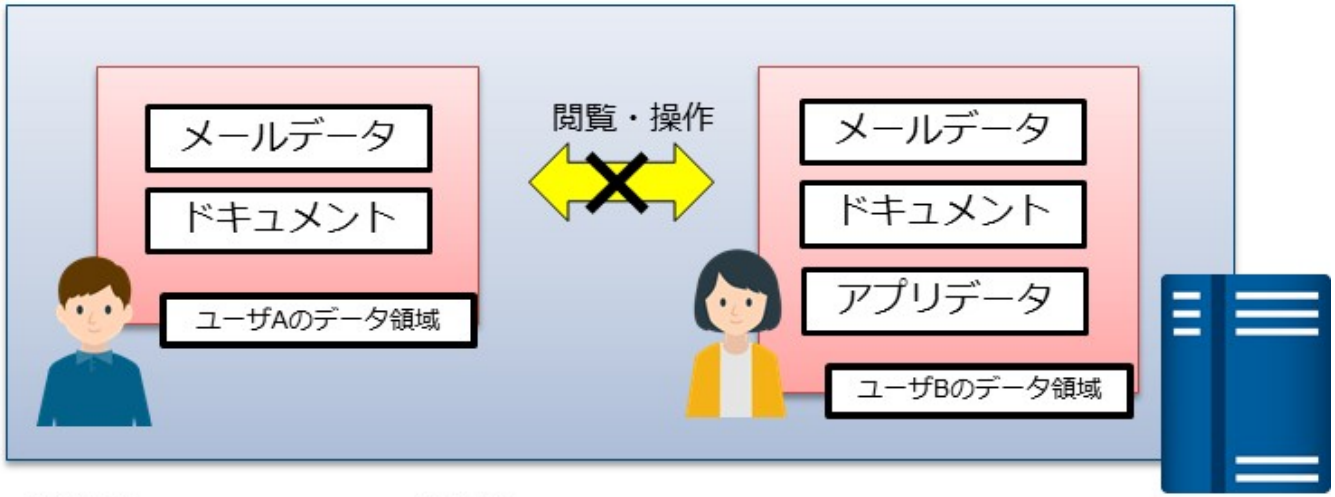
対　　象：Aggregator、e-Utility、Decision Trigger



No.III-5 セキュリティ管理：クライアントデータの操作のセキュリティ対策

本項目の目的：他のアカウントのデータを操作・閲覧できないようにする

対　　象：Aggregator、e-Utility、Decision Trigger



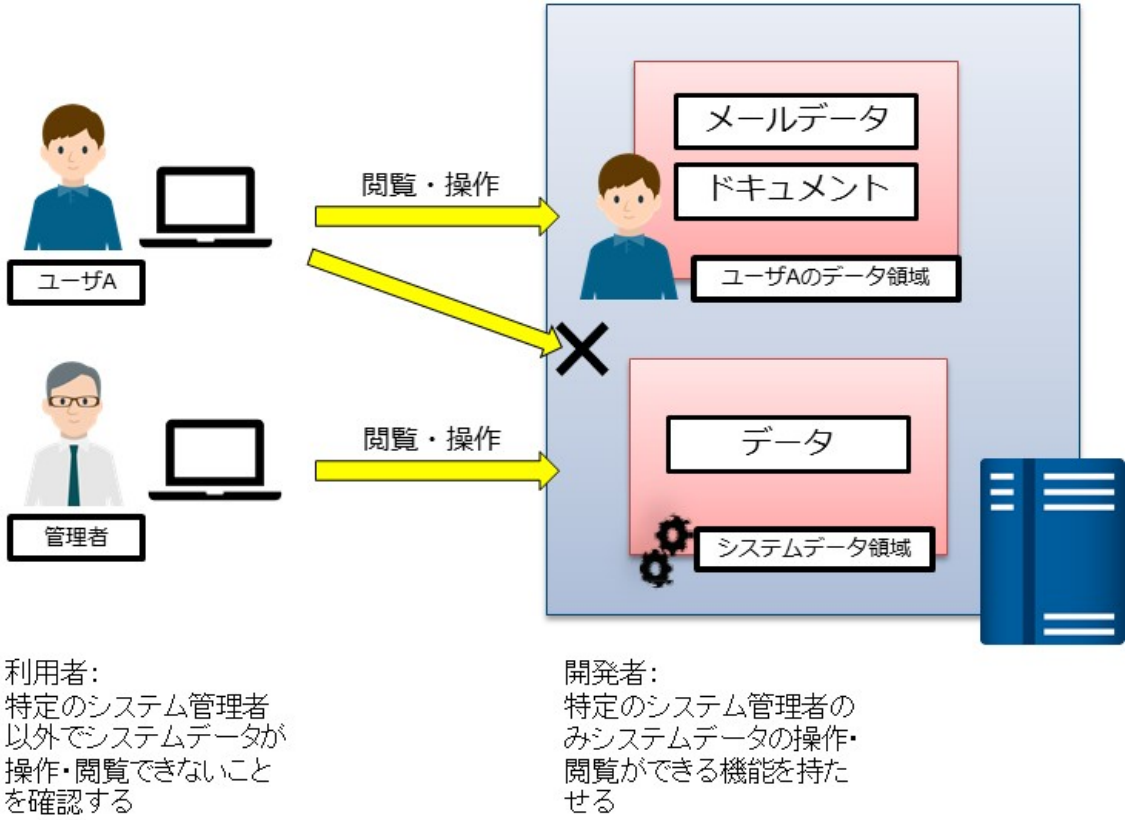
利用者:
他のアカウントのデータが操作・閲覧できないことを確認する

開発者:
アカウントごとのデータ管理機能を待たせる

No.III-6 セキュリティ管理：システムデータの操作のセキュリティ対策

本項目の目的：システムデータは制限されたユーザのみが操作・閲覧できるようにする

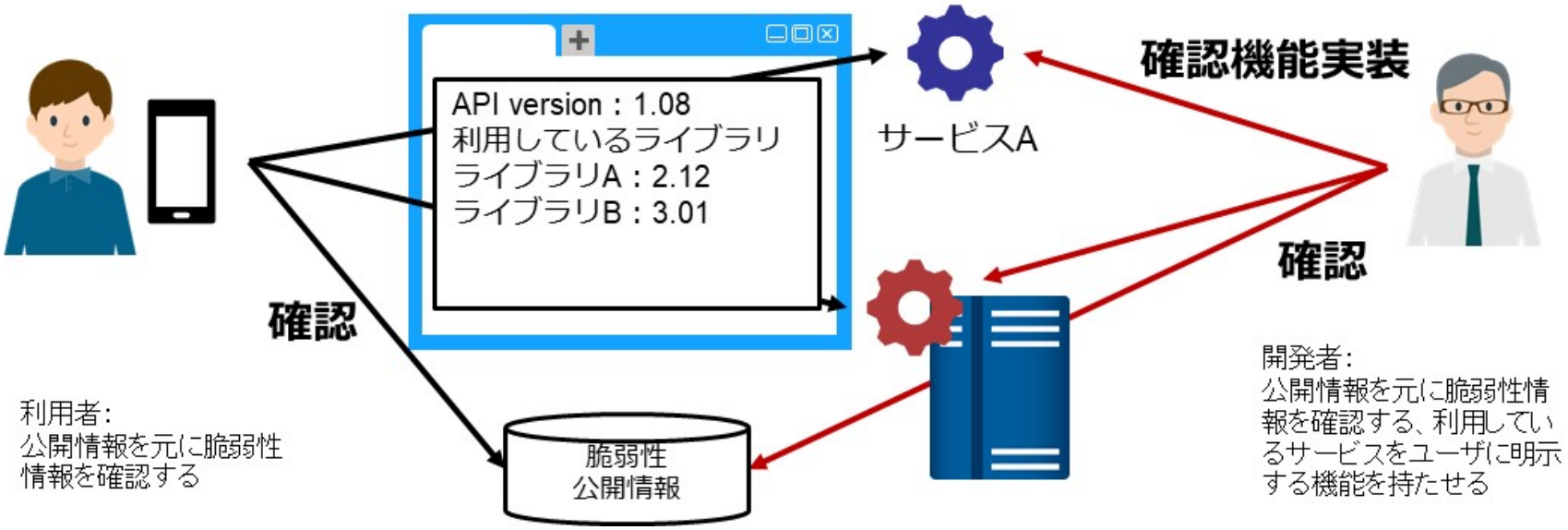
対　　象：Aggregator、e-Utility、Decision Trigger



No.III-7 セキュリティ管理：クラウドインタフェースやネットワークの脆弱性（API インタフェースやクラウドベースの Web インタフェースなど）

本項目の目的：クラウドインタフェースやネットワークの既知の脆弱性がシステムに存在しないかを確認する

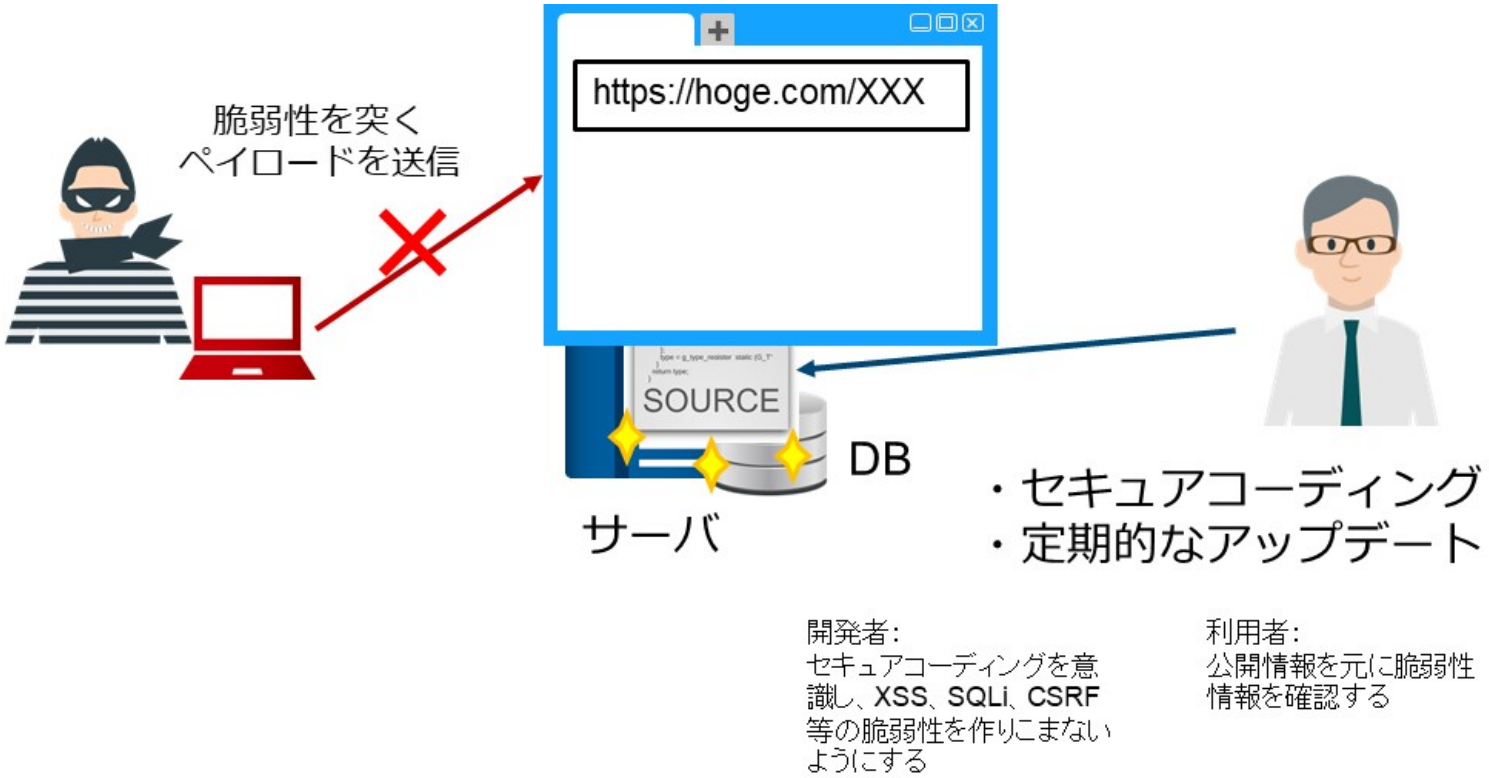
対　　象：e-Utility、Decision Trigger



No.III-8 セキュリティ管理：XSS、SQLi、および CSRF の脆弱性

本項目の目的：利用しているシステムに XSS、SQLi、CSRF 等の既知の脆弱性が存在しないかを確認する

対　　象：e-Utility、Decision Trigger



No.III-9 セキュリティ管理：Web アプリケーションの SSL 証明書

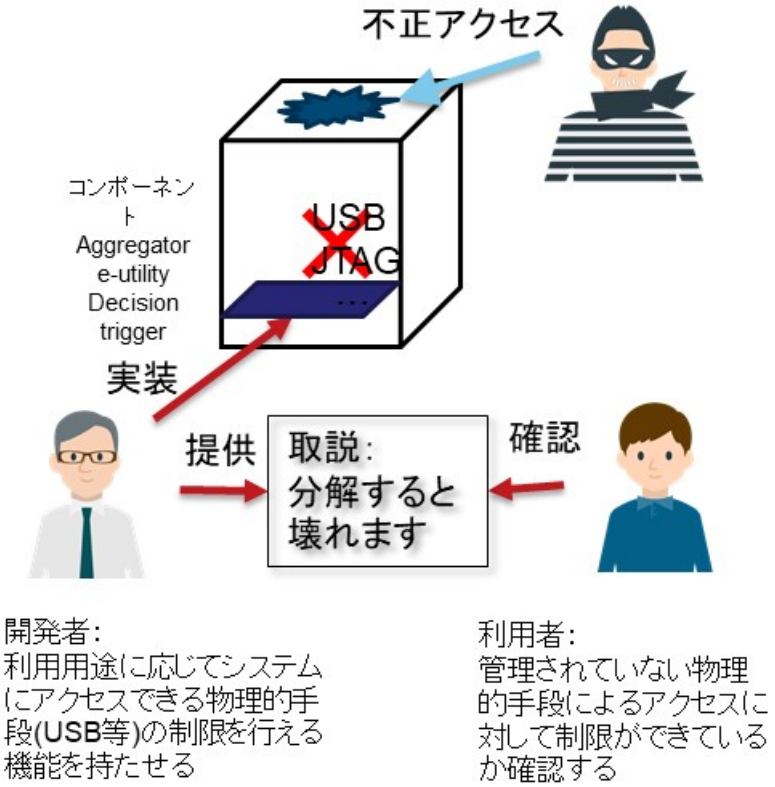
本項目の目的：SSL 実装の為の証明書を自身のシステムに適した形で実装する

対　　象：e-Utility、Decision Trigger

No.IV-1 アクセス制御：管理されていない物理手段によるアクセス

本項目の目的：管理されていない物理手段によるシステムへのアクセスを防ぐ

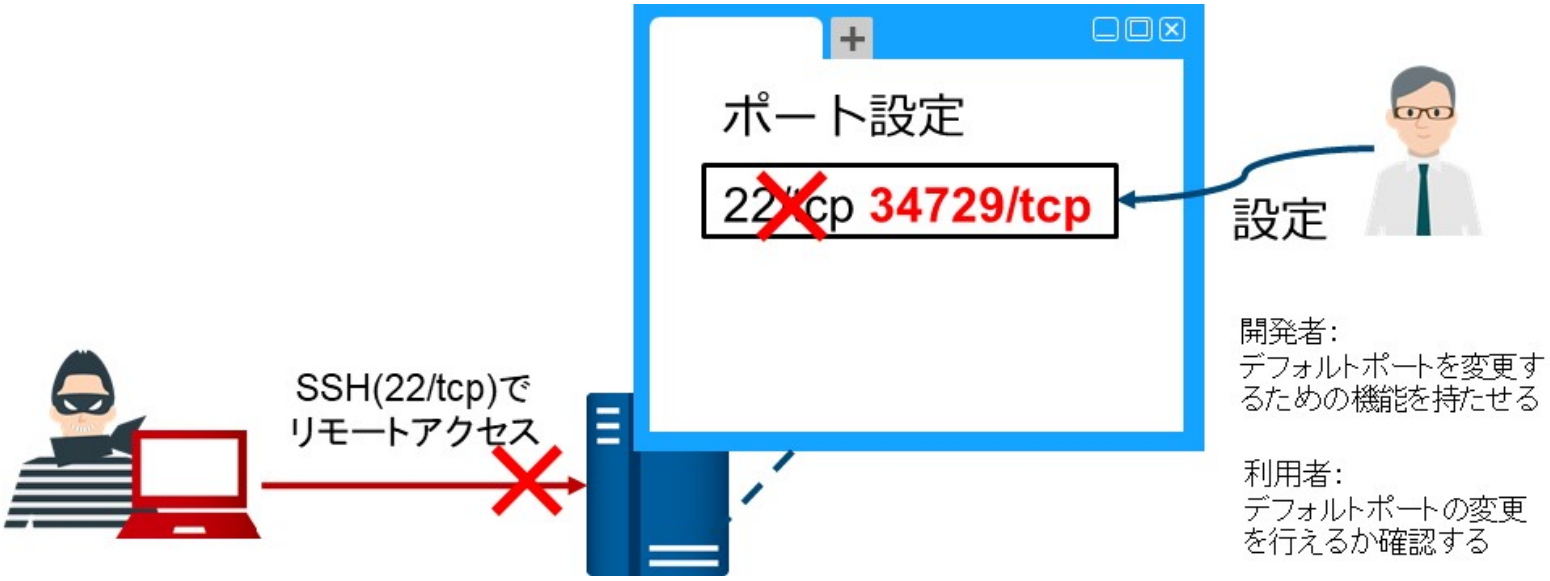
対　　象：Aggregator、e-Utility、Decision Trigger



No.IV-2 アクセス制御：リモートアクセス用ポートのデフォルトポート

本項目の目的：リモートアクセス機能のデフォルトポートを狙った攻撃を防ぐ

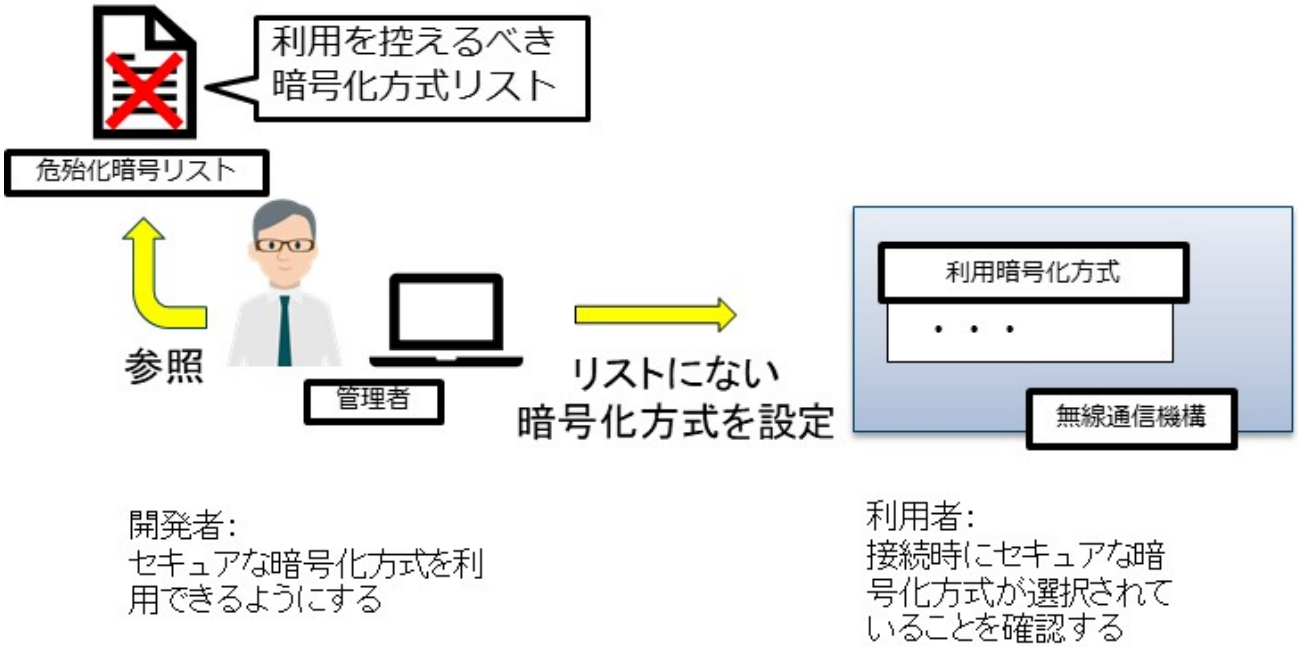
対　　象：Aggregator、e-Utility、Decision Trigger



No.IV-3 アクセス制御：無線通信におけるセキュリティ(暗号化方式)

本項目の目的：脆弱性を利用した通信内容の窃取を防ぐため、利用する暗号化方式はセキュアなものにする

対　　象：Aggregator、Communication Channel、e-Utility、Decision Trigger



No.IV-4　アクセス制御：無線通信におけるセキュリティ(WPS)

本項目の目的：無線の設定ミスによるセキュリティの低下を防ぐ

対　　象：Aggregator、Communication Channel、e-Utility、Decision Trigger

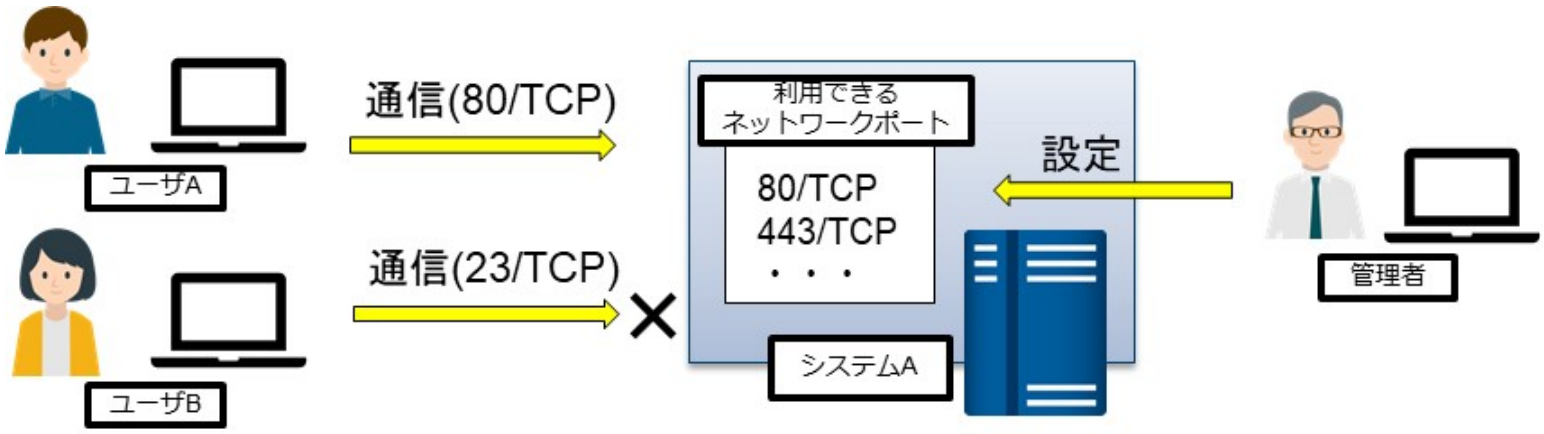
開発者:
WPS機能を持たせる場合は
セキュリティを考慮する
（例: MACアドレスフィルタリ
ングなど）

利用者:
WPSが動作するか確認
する

No.V-1　不正な接続：ネットワークポートの制限

本項目の目的：利用用途を想定して、適切なポートのみを使えるようにする

対　　象：Aggregator、e-Utility、Decision Trigger



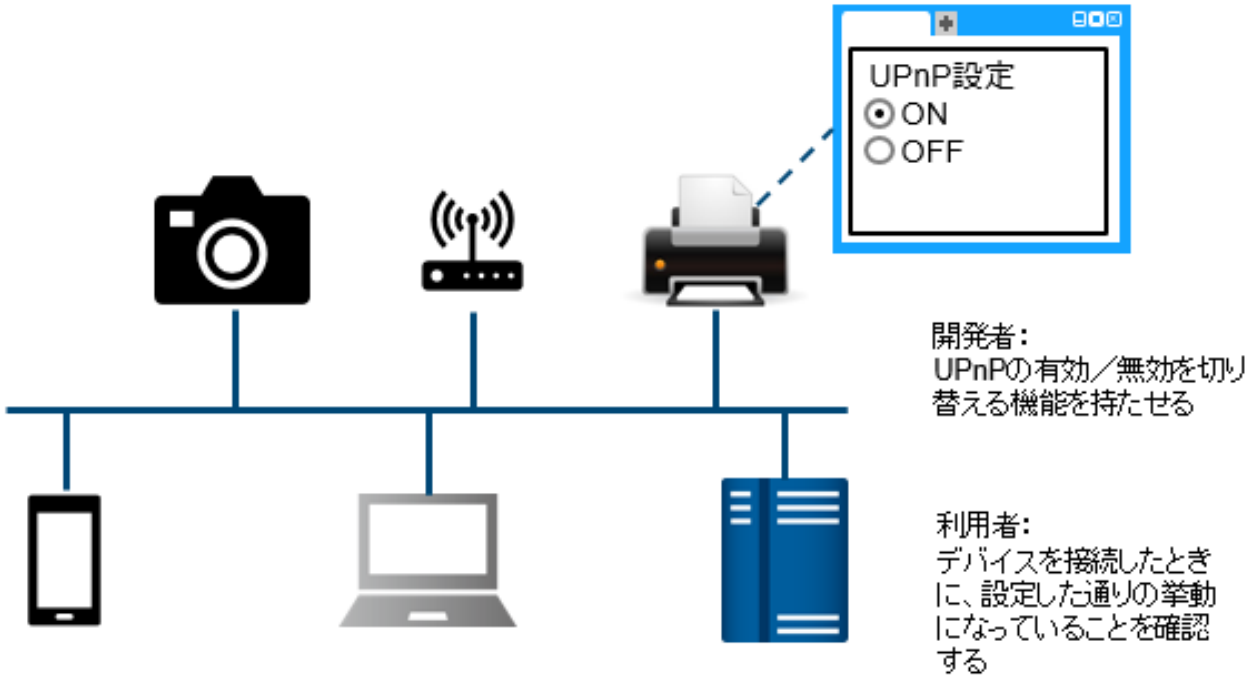
開発者：
利用用途に応じてポートの開閉を設定できる機能を持たせる

利用者：
ポートの制御が設定したとおりに開閉されていることを確認する

No.V-2　不正な接続：UPnP

本項目の目的：利用を想定しているデバイスに対して、UPnP が使えるようにする

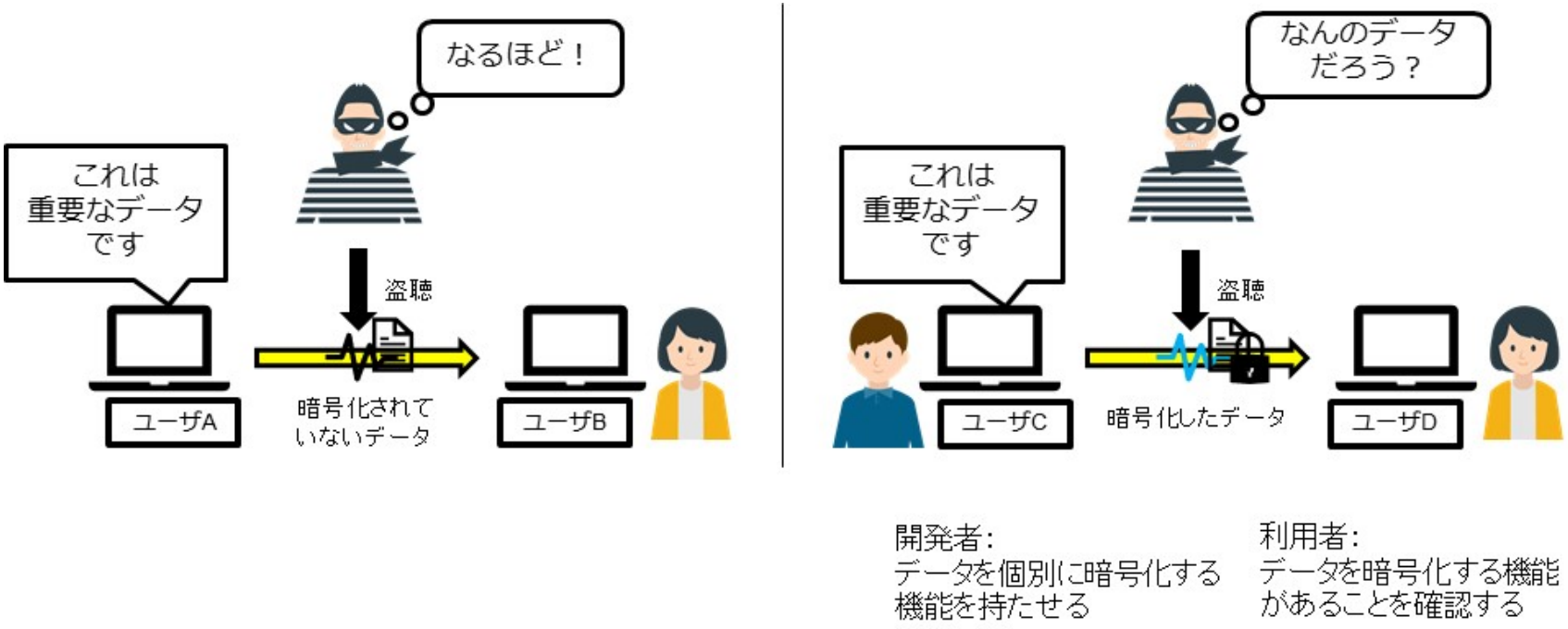
対　　象：Aggregator、e-Utility、Decision Trigger



No.VI-1　暗号化：データの暗号化機能

本項目の目的：データが平文で送られることにより、通信内容を読み取られることがないようにする

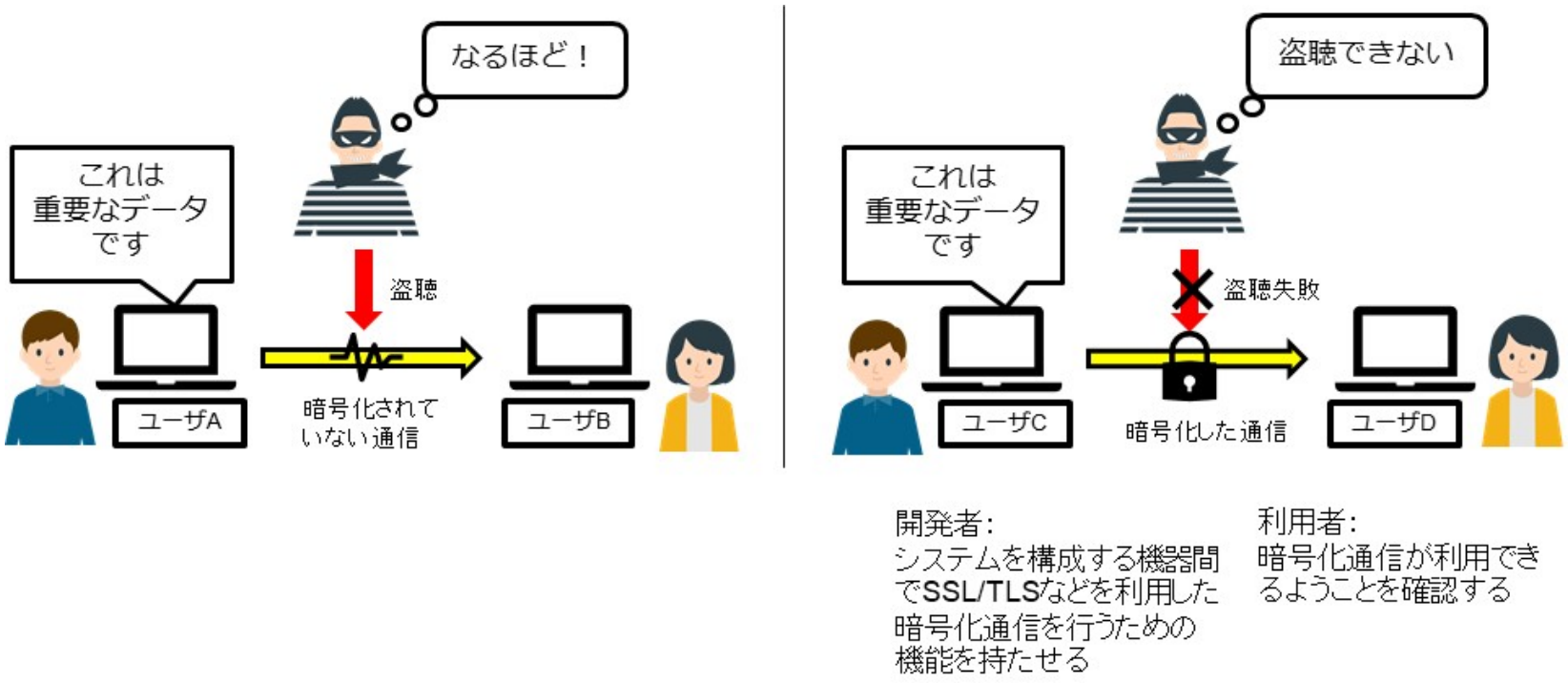
対　　象：Aggregator、Communication Channel、e-Utility、Decision Trigger



No.VI-2　暗号化：通信の暗号化機能

本項目の目的：データが平文で送られることにより、通信内容を読み取られることがないようにする

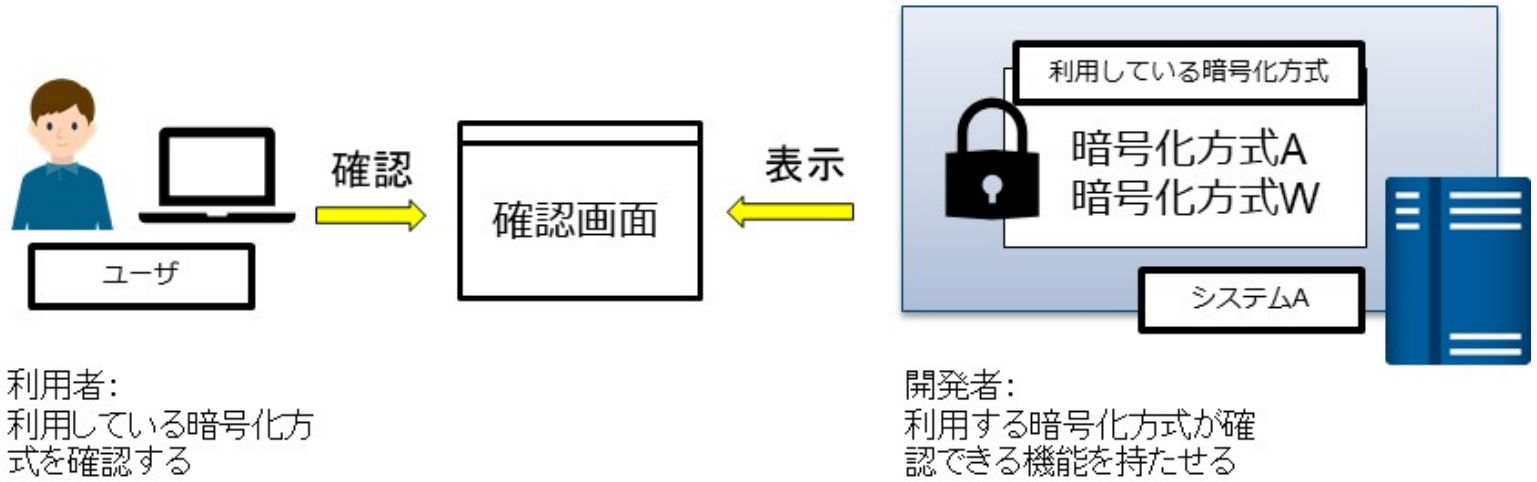
対　　象：Aggregator、Communication Channel、e-Utility、Decision Trigger



No.VI-3　暗号化：暗号化方式

本項目の目的：利用する暗号化方式が確認できるようにする

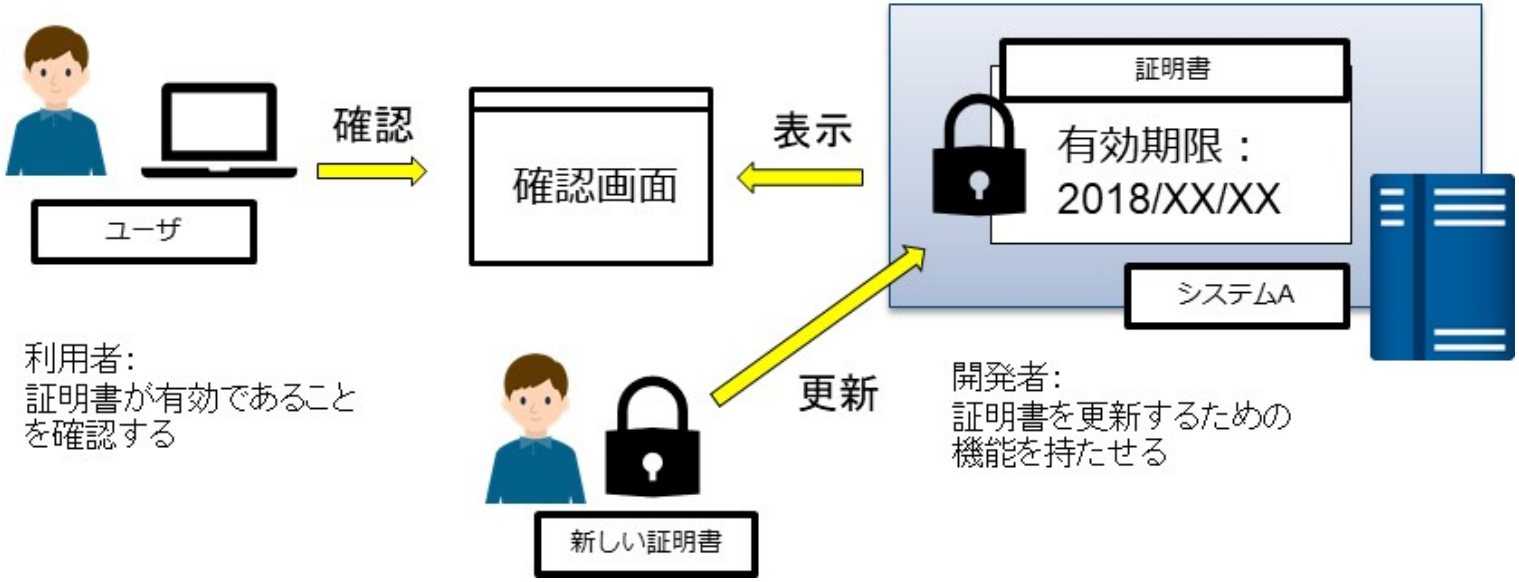
対　　象：Aggregator、Communication Channel、e-Utility、Decision Trigger



No.VI-4　暗号化：証明書更新機能

本項目の目的：証明書の期限が切れないようにする

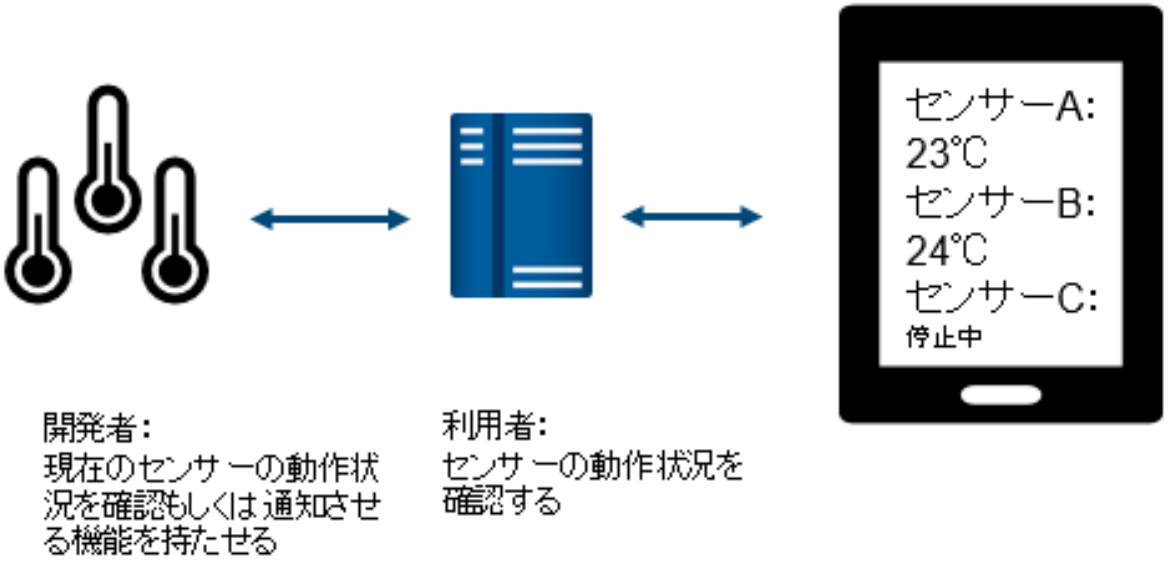
対　　象：Aggregator、Communication Channel、e-Utility、Decision Trigger



No.VII-1　システム設定：センサの動作状況確認機能

本項目の目的：動作状況を確認できるようにする

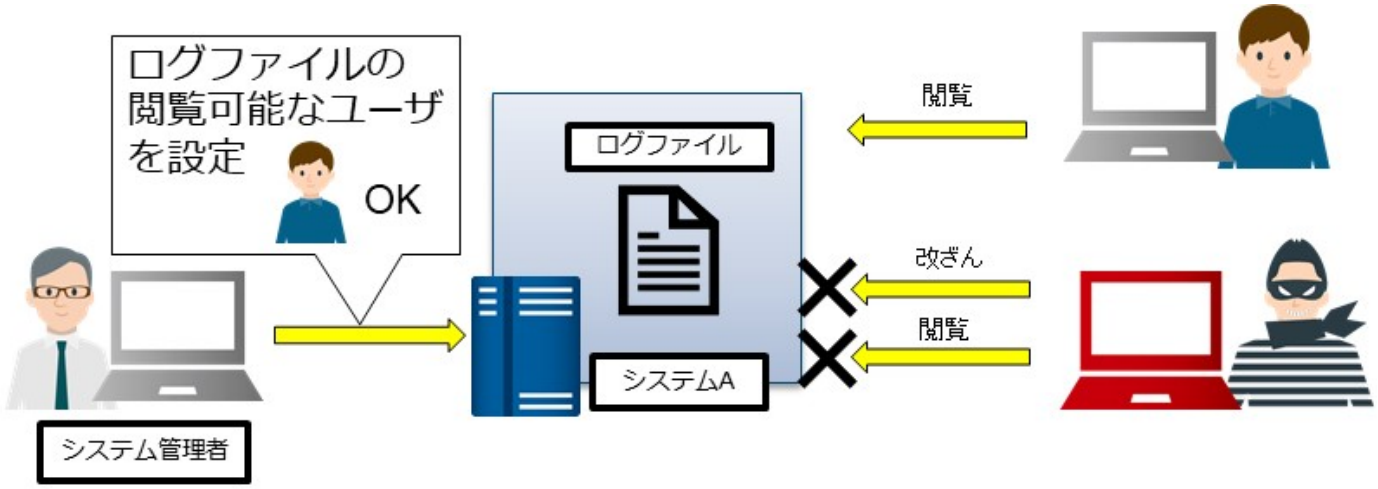
対　　象：Sensor



No. VII-2　システム設定：ログのセキュリティ管理

本項目の目的：第三者からログが閲覧されたり改ざんされたりすることを防止する

対　　象：Aggregator、e-Utility、Decision Trigger



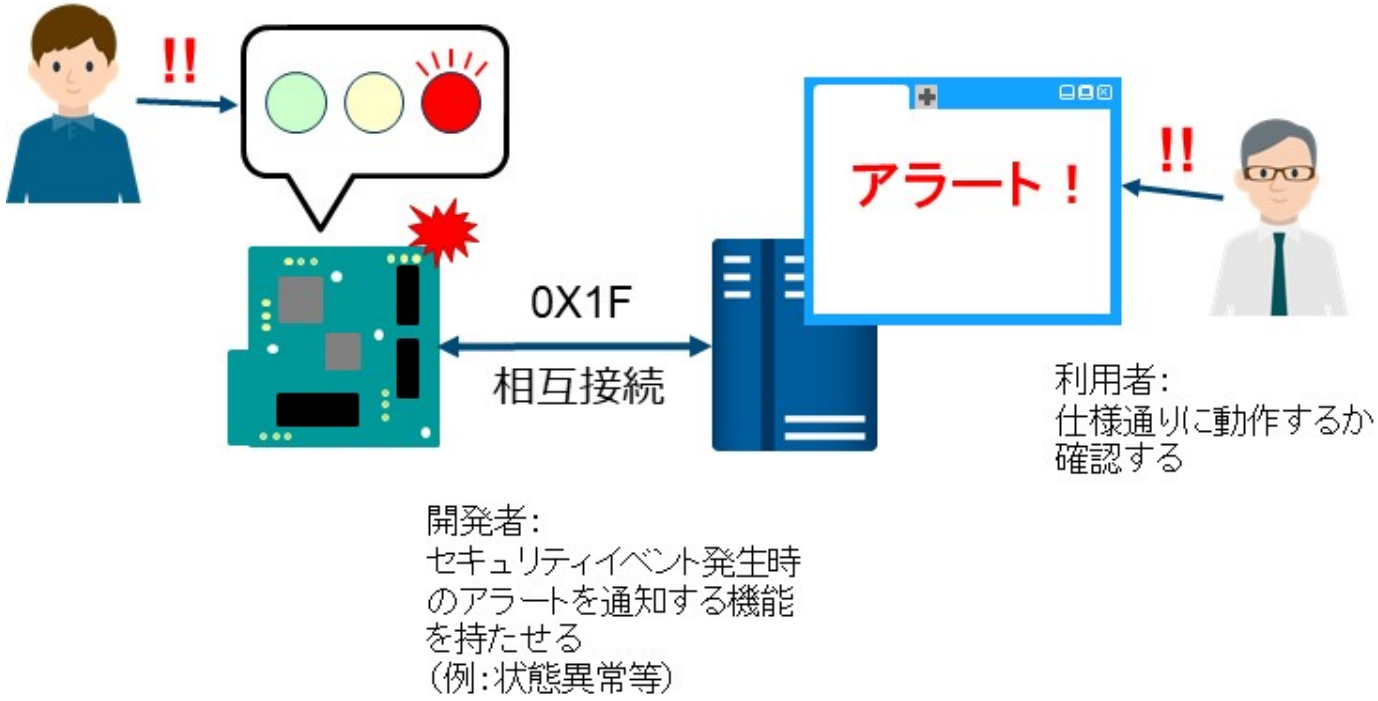
利用者：
閲覧権限のないユーザでログが見れないことを確認する、閲覧可能なユーザでログが書き換えられないことを確認する

開発者：
ログについて、閲覧可能なユーザの設定および内容の改ざんを防止する機能を持たせる

No.VIII-1　通知：セキュリティイベントのアラートと通知機能（状態異常等）

本項目の目的：セキュリティイベント発生時にアラートを通知することにより、迅速に対応できるようにする

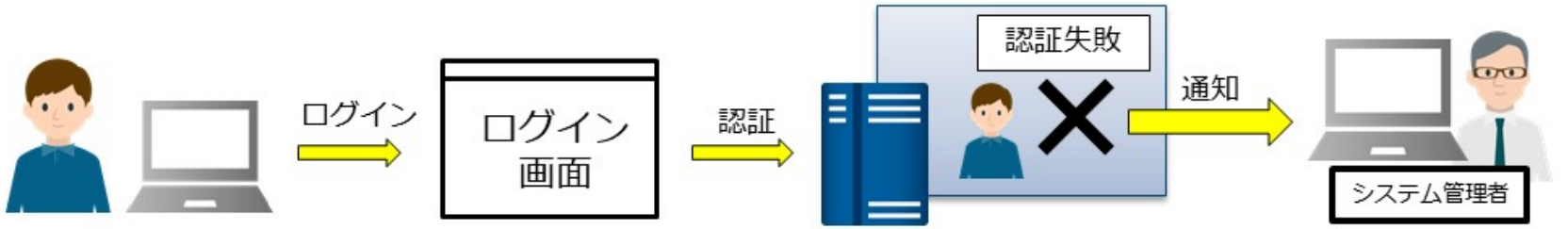
対　　象：Sensor



No.VIII-2　通知：セキュリティイベントのアラートと通知機能（認証失敗、証明書の期限切れ等）

本項目の目的：セキュリティイベント発生時にアラートを通知することにより、迅速に対応できるようにする

対　　象：Aggregator、e-Utility、Decision Trigger



開発者：
セキュリティイベント発生時のアラートを通知する機能を持たせる
（例：認証失敗、証明書の期限切れ等）

利用者：
仕様通りに動作するか確認する

Primitive（IoT システムを構成する基本単位）構成要素：

Sensor	温度、加速度、重量、音、位置などを測定する機能・機器
Aggregator	センサからのデータを集約する機能・機器
Communication Channel	データの送受信を行うための通信路・ネットワーク
e-Utility	データを閲覧したり設定したりするインタフェース
Decision Trigger	データを計算し、その結果に基づいてアクションさせるための機能