

スマート社会を支えるセキュリティ基盤構築の理論・応用

Theories and Applications for Constructing Security Infrastructure towards Smart Society

電気電子工学科・電気電子工学専攻

Department of Electrical and Electronic Engineering

情報通信研究室

Information and Communication Engineering Lab.

白石 善明

Yoshiaki SHIRAISHI

葛野 弘樹

Hiroki KUZUNO



サイバー空間とリアル空間が融合する近未来

データ活用の視点

サイバー空間でデータを共有 → 「局所的な」あるドメインでの価値の発見から
「データを相互に持ち寄り」価値を最大化
⇒ ドメインを跨るデータのガバナンスを技術的に保証

サイバーセキュリティの視点

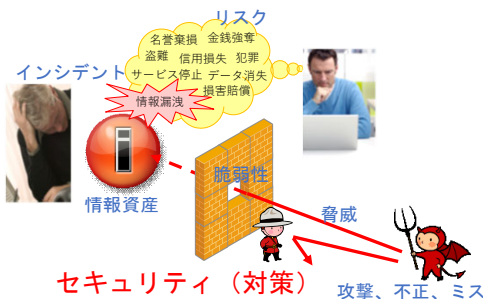
サイバー空間の脅威が拡大する → リアル空間へサイバー空間の被害・影響の最小化
現実と仮想の区別がつきづらい → 人の情報処理の混乱やさらなる歪みの是正

システム構築・運用の視点

アプリケーションのアイデアをシステムとして構築 ← セキュリティ機能の組み込み
→ セキュリティ機能 = ソフトウェア（部品）として実装
→ ソフトウェア（部品）のセキュリティ品質の維持・改善

セキュリティの考え方

情報資産（データ・情報・ソフトウェア・施設・・・）を保護するために
想定される脆弱性や脅威に対策を施す



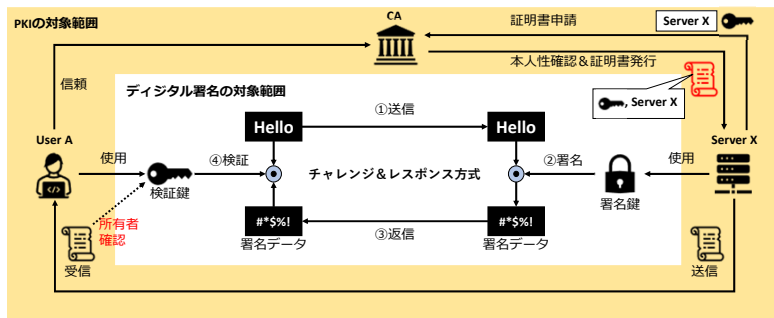
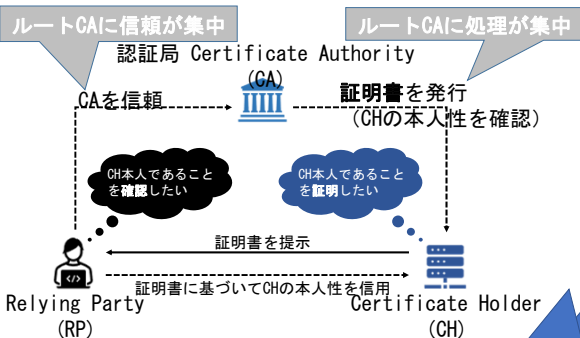
データ活用の視点 人・モノ・サービスをつなぐ堅牢で柔軟なデータ流通基盤

人/プロセス/デバイスのIDを確認する3つの方法

公開鍵基盤（Public Key Infrastructure, PKI）に基づく認証（例）



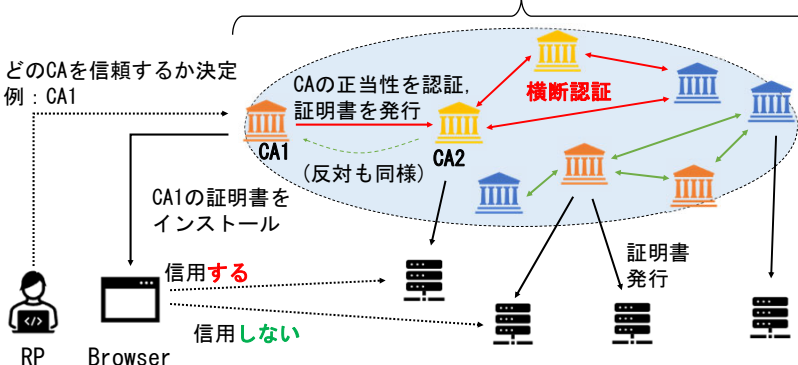
電子証明書を使った認証技術を対象



メッシュPKIの構築：個々のCAが独自の基準で別のCAを認証（横断認証）
することでPKIをメッシュ状に拡大・分散

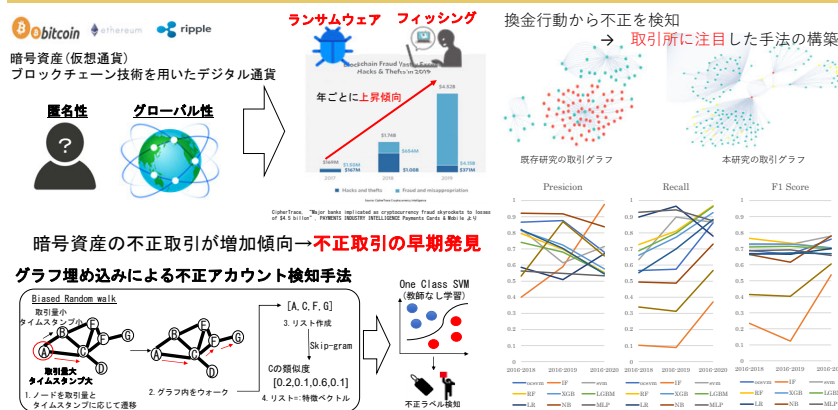
⇒ 電子証明書の発行・管理をスケールアウト = サービスの横展開を可能

分散台帳とスマートコントラクト（ブロックチェーン）で横断認証の機能を実現



サイバーセキュリティの視点

サイバー空間でのデータドリブン異常検知



システム構築・運用の視点

データドリブンセキュリティインテリジェンス

