研究テーマ等

情報セキュリティとその応用に関する研究

サーバー、OS、プロトコル、通信網などのアプリケーションを稼働するシステム基盤について、様々な脅威から情報を守るセキュリティ要素技術、セキュアなシステム構築・運用技術を研究しています。

（主な研究テーマ）
情報端末での証跡の取得・保全に関する研究
ネットワーク障害や不正アクセス、ユーザ操作、サービス利用等の証拠を確保、原因究明や訴訟対策に利用するため、PC やスマートフォンなどの情報端末上の通信をはじめとする多様な証跡を取得、保全する技術やそれを実装したシステムを開発します。

ネットワーク内部の状態推定に関する研究
安全かつ効率的にネットワーク内部の状態を把握するため、通信を行う末端の機器や通信経路上の機器においてデータの転送、複製、演算を行う（ネットワーク符号化）を応用したネットワーク状態計測技術やそれを実装したシステムを開発します。

情報システムの利用や個人情報登録の際の不安感に関する研究
情報システムの利用、個人情報の登録に際する心理的障壁を取り除く、あるいはリテラシー教育を効果的に行うための知見を得るため、クラウド型の情報システムを例に、人が抱く不安感に関して質問紙による調査、分析を行います。

（最近の業績）

1. Yoshiaki SHIRAISHI, Masami MOHRI and Youji FUKUTA, “A Server-Aided Computation Protocol Revisited for Confidentiality of Cloud Service,” Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications(JoWUA), Vol.2, No.2, pp.83-94, June 2011.
2. 白石 善明, 佐々木 啓, 福田 洋治, 毛利 公美, ”センターから端末へ動的なコードの配布・実行・検証機構,” 情報科学技術フォーラム（FIT2012）査読付き論文, RO-002, 東京, 小金井, 2012 年 9 月.
3. Taisuke YAMAMOTO, Youji FUKUTA, Masami MOHRI, Masanori HIROTOMO and Yoshiaki SHIRAISHI, “A distribution scheme of certificate revocation list by inter-vehicle communication using a random network coding,” 2012 International Symposium on Information Theory and its Applications (ISITA2012), pp.392-395, Hawaii, USA, Oct. 2012.
4. Tomoki MATSUKAWA, Taisuke YAMAMOTO, Youji FUKUTA, Masanori HIROTOMO, Masami MOHRI and Yoshiaki SHIRAISHI, ”Controlling Signature Verification of Network Coded Packet on VANET,” 2012 12th International Conference on ITS Telecommunications (ITST2012), pp.679-683, Taipei, Taiwan, Nov. 2012.
5. 福田 洋治, 白石 善明, 廣友 雅徳, 毛利 公美, ”医療クラウドサービスの間接的利用の不安要因について,” 情報科学技術フォーラム（FIT2014）査読付き論文, RO-007, 筑波, 2014 年 9 月.
6. 福田 洋治, 白石 善明, 毛利 公美, ”当事者のプライバシーを考慮したログの保管とその監査の手法,” 電子情報通信学会和文論文誌 D, Vol.J97-D, No.12, pp.1729-1732, 2014 年.

7. 福田 洋治, 白石 善明, 毛利 公美, ”イベント・アクション制御に基づくファイルシステムの提案, ” 電子情報通信学会和文論文誌 D, Vol.J97-D, No.12, pp.1701-1704, 2014 年.
8. 白石 善明, 中井 敏晴, 毛利 公美, 福田 洋治, 廣友 雅徳, 森井 昌克, ” 長期追跡研究のための複数機関にある匿名化データの共有におけるセキュリティ対策の検討, ” 情報科学技術フォーラム（FIT2015）査読付き論文, 愛媛, 2015 年 9 月.

（キーワード）
大分類
アプリケーション、ミドルウェア、OS・ネットワーク、理論・基礎、セキュリティ要素技術、システム構築・運用技術

小分類
デジタルフォレンジクス、セキュア医療情報システム、電子署名・PKI、セキュリティ管理・運用支援、セキュアモバイルアクセス、電子メールセキュリティ、セキュア通信プロトコル、ネットワークトレーサビリティ、暗号評価

---

Last modified: Dec. 21, 2015.