

情報漏えいに強い 2要素認証セキュリティ LR-AKE

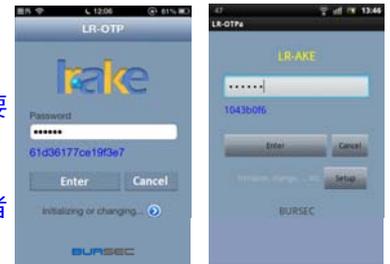
● サマリー

LR-AKE は、これまでのセキュリティ市場には無い、サーバ / クライアント双方からの情報漏えいに耐性があり、フィッシング対策も施された 2 要素認証ソフトウェアです



● Leakage Resilient-Authentication and Key Exchange (LR-AKE)

1. 利用者は、1つの短いパスワードを使用するのみ
 - 4~6文字でもセキュリティの低下なし
2. 端末や認証トークンの紛失にも耐性があり、高価なハードウェア・トークンは不要
3. 既存の VPN や様々な認証方式と連携可能
 - Active Directory、LDAP、Radius などに対応
4. 暗号鍵や認証情報などの重要なデータを分散管理
5. 利用者による認証アカウントのバックアップ、紛失アカウントの破棄など、管理者の負担を軽減



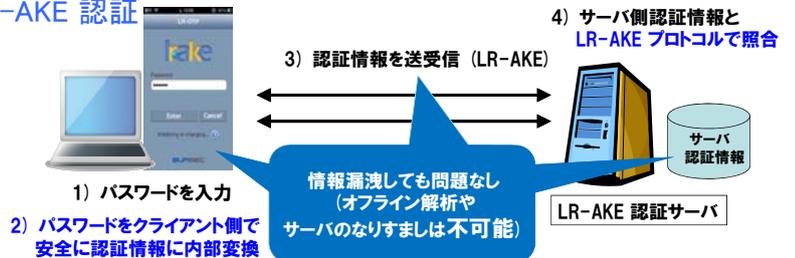
● ソフトウェア構成

- LR-AKE SDK (ソフトウェア開発キット)
 1. LR-AKE Client SDK
 - Windows, Mac, iOS, Android 対応
 2. LR-AKE Server, Satellite
 - UNIX (Linux, Mac など) 対応

● 一般的なパスワード認証



● LR-AKE 認証



● 販売体制と LR-AKE への追い風

- LR-AKE 販売代理店
 - 株式会社 SID ソリューションズ
 - <http://www.sid-sol.com/>
- Radius 製品への LR-AKE 組込み販売
 - FCS 社製 Radgate
 - <http://www.fcs-kk.co.jp/>
- 米国・中国での特許も取得済み
- 実績
 - 新潟県 燕市役所内での SSO 認証に採用
 - 愛媛大病院 小児科での VPN 認証に採用
 - 国内 クレジットカード会社の管理業務システムに導入
- PCI DSS 基準による 2 要素認証への需要

	2000 年代	現在
パスワードの全数探索	計算量が大きく、時間が掛かる	計算能力の向上 ・ノートPCでも昔のサーバ以上 ・クラウドの利用
ネットワーク接続	オフラインでの利用は必須	ネットワーク接続前提サービスの常態化
記録情報	別途記録情報を持ち歩くのは大変	モバイル端末を常に持参
クライアント端末の紛失・盗難	クライアント端末を持ち出すことは稀	モバイル端末を常に持参・ユビキタス化
サーバからの漏えい	サーバから情報が漏れることは稀	サーバからの漏えい事件多発 ・クレジットカード会社、ソニー、ロッキードなどへの不正アクセス ・パブリッククラウドの利用
パスワード	長いパスワードを利用すればよい	モバイル端末などでは長いパスワードの入力は非常に不便