セキュリティは NTR 社のインキエロの開発の全体にわたる主要な事柄のうちの 1 つでした。私たちが組込むセキュリティ対策は、インキエロを利用中のあなたのビジネス、顧客およびスタッフを保護すると同様に無許可の人がインキエロのデータ、プログラムあるいはシステムへのアクセスするのを防ぐことを目指しています。このドキュメントでは、私たちがあなたのセキュリティを保証するために適用する手続きのうちのいくつかを概説します。

データ転送中には

全てのテキストメッセージは下記の手順でインキエロによって送信されます：

1. 送信側のユーザのパスワードによって生成された暗号化キー使ってサーバへ暗号化されたメッセージを送ります。
2. サーバは受信側のパスワードを使用して暗号化キーを生成しメッセージを解読します。そして、それを再び暗号化します。メッセージはデータベースに格納され、次に、受取人のもとへ送られます。
3. 受信側はパスワードから作成されたキーを使用して、メッセージを解読します。
4. さらに高度なセキュリティを望まれる場合はテキストチャットは 128 ビットの SSL を利用することができます。

暗号化アルゴリズムはリニア・アダプティブです。
システムにログインする場合、ユーザのパスワードそのものは送信されません。
テキストチャット会話はすべてデータ・ベース内に暗号化されて格納され、サイト管理者によっていつでもアクセスすることができます。

共同サーフィン

共同サーフィン中はお客さまのウェブブラウザーの内容をローカルの JavaScript を利用してサーバに送信されます。
共同サーフィンでオペレータが見ているウェブページはオリジナルのウェブページではありませんので、サーバに不正なリクエストなどが送信される心配がありません。

リモートコントロール

リモートコントロールは 256-bit の Advanced Encryption Standard 暗号を使用して、TCP 接続によってパケットを送り受け取ります。このプロトコルは送る前にパケットを圧縮しコード化し、認証過程を含んでいます。各 TCP パケットは、TCP データとは別に、確実性を保証するために送信側および受信側に関係のあるデータを含んでいます。
リモートコントロール・セッションが終了する場合、サーバはオペレータとクライアントの間の橋渡しの役割をするだけで、リモートコントロールのセッションの開始と終了の情報だけを記録し、リモートの内容は一切記録しません。

アクセス

オペレータのアクセスはパスワード認証を使用します。管理者アクセスはパスワード認証を使用し、128 ビットの SSL で通信が行われます。管理セッション全体も 128 ビットの SSL で通信が行われます。オペレータのログインに 3 回以上失敗すると、そのオペレータ・アカウントが利用できなくなり、更に、管理者はオペレータのアクセス制限として特定の IP を定義することができます。※特定 IP 定義の機能は近日リリース予定の Ver. 4.1 から提供されます。

スタッフのプロテクション

迷惑な顧客からあなたのカスタマ・サポート・スタッフを保護するために、インキエロは、管理者がオペレータへのアクセスからあるユーザを拒否することを可能にするブロッキング技術を具体化しました。※スタッフ保護の機能は近日リリース予定の Ver. 4.1 から提供されます。

サイト管理者

サイト管理者はログイン失敗の日時、IP アドレスなどのセキュリティイベントの情報を調査することができます。※セキュリティイベント調査の機能は近日リリース予定の Ver. 4.1 から提供されます。

ASP のホスティング環境

インキエロのサーバは JENS 株式会社のデータセンターで 24 時間・365 日オペレータに監視された環境で安全に運営されています。電源の冗長、空調設備などの二重化、耐震性の高い施設などさまざまな安全対策が取られています。

２００４年５月１３日

開発元：Net Transmit & Receive S.L.

日本総販売代理店：株式会社インターワーク

セキュリティに関してのお問い合わせ：support@inquiero.jp