

日本エヴィクサー株式会社

System Security

Technology White Paper – Research and Development Group

2005年7月

- 2 概要

- 4 BlastSockセキュリティ
- 4 AES及びDESの紹介
- 4 SSL

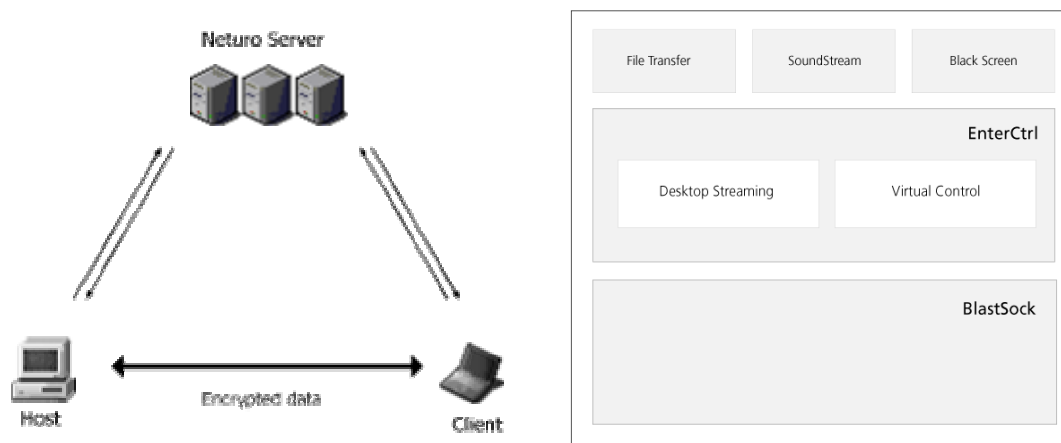
- 5 EnterCtrlセキュリティ
- 5 2つの認証

- 6 システム構成

note: Evixar Japan, Inc. is not responsible for the accuracy of the research and reports contained within this document. All figures, observations, and comments are provided for your reference only. Please use at your own discretion.

概要

弊社ではセキュリティおよびプライバシーを保障するために最先端のテクノロジーを採用しております。弊社製品であるEvixar NeturoおよびEvixar LiveSupportはホスト、クライアント、サーバの3要素を軸とする構造をしています。それぞれがEnterCtrlおよびBlastSockと呼ぶ2つの土台となるテクノロジーから構成され、BlastSockは転送中のデータを保護する役目を担い、EnterCtrlはプライバシー機能と認証機能を提供します。



弊社では、リモートコントロール（遠隔操作）中のプライバシーとセキュリティを保障するために、以下のポイントを指摘し、それに対する回答を用意しています。

1. どのようにすれば、なりすましによる不正アクセスを防ぐことができるのか。
2. どのようにすれば、転送中のデータの安全を確保出来るのか。
3. どのようにすれば、転送中のデータが改ざん、破壊されていないと保障できるのか。
4. どのようにすれば、何人もホストPC（リモートコントロールを受けるPC）を第三者が覗き見していないと保障できるのか。

BlastSockセキュリティは転送中のデータを暗号化することに特化しており、暗号化は3つの重要な役割を担っています。

- ・ **データの保護** – 認証を受けたユーザーだけが暗号化された転送データを解読でき、転送中のデータを保護します。
- ・ **データの完全性** – 転送中のデータが改ざん、破壊されていないことを保障します。
- ・ **否認防止** – 正しい方法によって送られたデータは確実に受け手に届けられ、間違って受け取りを拒否されることはありません。

EnterCtrlは以下の機能を提供します。

- ・ **二重認証** – ユーザー認証は一般的なID/パスワード認証に加え、コンピュータ毎のアクセスコードで構成されています。

弊社ではネットワーク技術とセキュリティを融合させ、全ての人が安全かつ快適に利用できる環境を実現しました。本書はセキュリティ技術の紹介であり、BlastSockおよびEnterCtrlがどのように強固なセキュリティ基準を満足するかについての報告です。

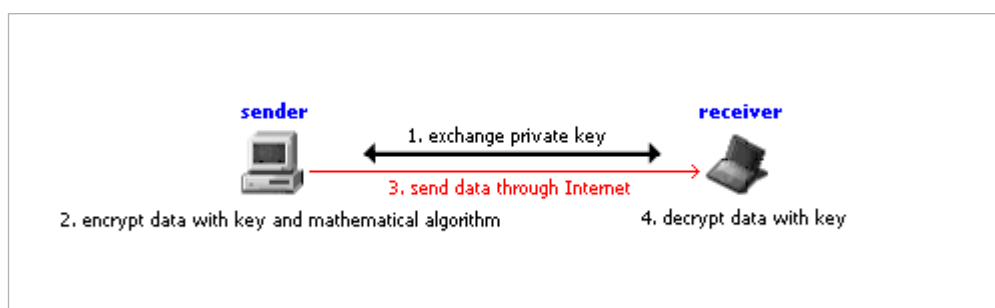
BlastSockセキュリティ

BlastSockはホストとクライアント間の転送データを保護する役割を担っています。弊社のサーバや公共のインターネット回線を利用したデータ転送も同様に保護します。BlastSockは「エンドポイント・プライベートキー・エンクリプション」と呼ばれるエンド・トゥ・エンドのデータ保護システムを提供します。

暗号化

暗号化の基本的なプロセスは2つのコンピュータ間におけるプロトコル交換から始まります。コンピュータはプライベートキーと呼ばれるものでお互いの認証を行います。お互いのコンピュータだけがキーを認識することが出来るので、キーは完全に「プライベート」なものになります。また、キーは接続毎に発行されるのでより安全です。

キーによる認証後、送り手がアルゴリズムを用いて情報を暗号化します。一度データが暗号化されるとキーを用いて暗号化を解かない限り解読することは不可能です。データはインターネットを通して送信されますが、他のコンピュータはキーが無いので、受け手だけが情報の暗号化を解くことが出来ます。このようにして受けては送り手からの情報を安全に受け取ることが可能です。基本的な構造は下図の通りです。



アルゴリズムの数理的煩雑さとキー及びデータブロックの長さが暗号化セキュリティのレベルを決定します。

AES-128¹

BlastSockはデータ転送を安全に行うためにAES（Advanced Encryption Standard）を採用しています。AESは情報を128、192、256ビットの暗号キーに変換してデータを送信します。参考として、128ビットのキーは 3.4×10^{38} 、192ビットのキーは 6.2×10^{57} 、256ビットのキーは 1.1×10^{77} 通りがあります。

1990年代の後半に「DESクラッカー」と呼ばれる機械が開発され、標準暗号化であったDESが瞬時に解読されるようになりました。そこで新たに登場したのがAESです。このDESクラッカーで128ビットのAESキーを解読しようとする149兆年を必要とすると試算されています。

¹ AES-128に関する詳細はNIST（米国商務省標準技術局）：<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>をご覧ください。

EnterCtrlセキュリティ

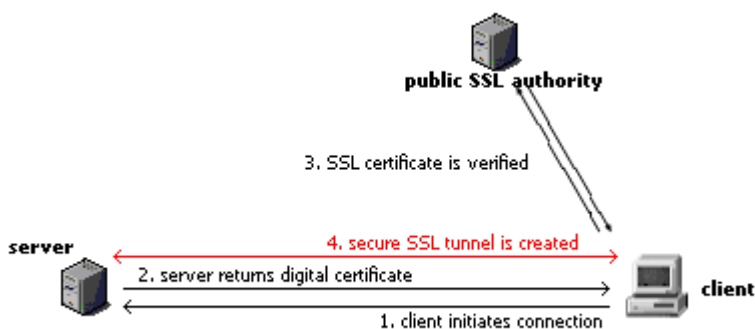
EnterCtrlはユーザーの認証機能を提供します。

認証

一般的な認証はIDとパスワードで行われ、IDとパスワードはそれぞれのユーザーが自由に作成することが出来ます。弊社製品は一般的に複数のコンピュータで作業することを想定しているため、IDとパスワード以外にそれぞれのコンピュータにアクセスコードと呼ばれるコードを設定して二重にパスワードをかけることが可能です。万が一、IDとパスワードが漏れたとしてもアクセスコードにより大切なデータを守ることができます。

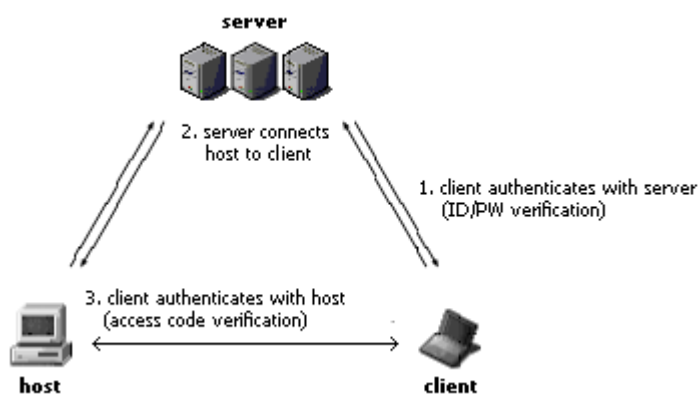
SSL証明書

ユーザー認証が安全でも認証情報自体の送信が安全でなくては意味がありません。弊社ではこの問題を解決するために認証過程にSSL通信を採用しました。SSL(Secure Sockets Layer)技術はインターネット取引で良く使われる暗号化技術です。クレジットカード決済などのeコマースでは、この技術を利用して、ウェブブラウザからサーバに送信される情報を送り手と受け手だけが解読できる暗号で通信することを実現しています。

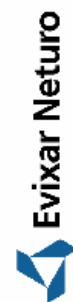
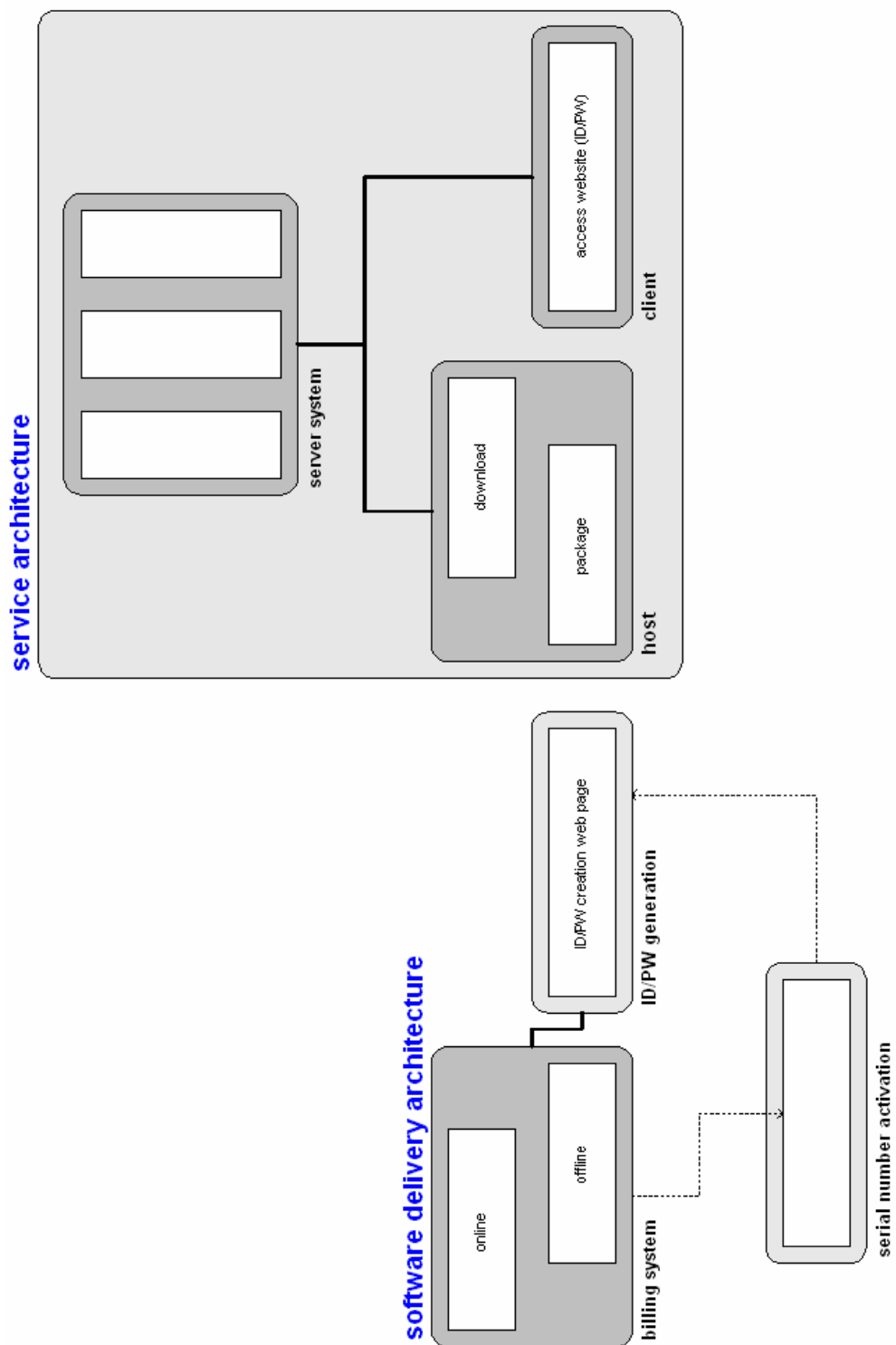


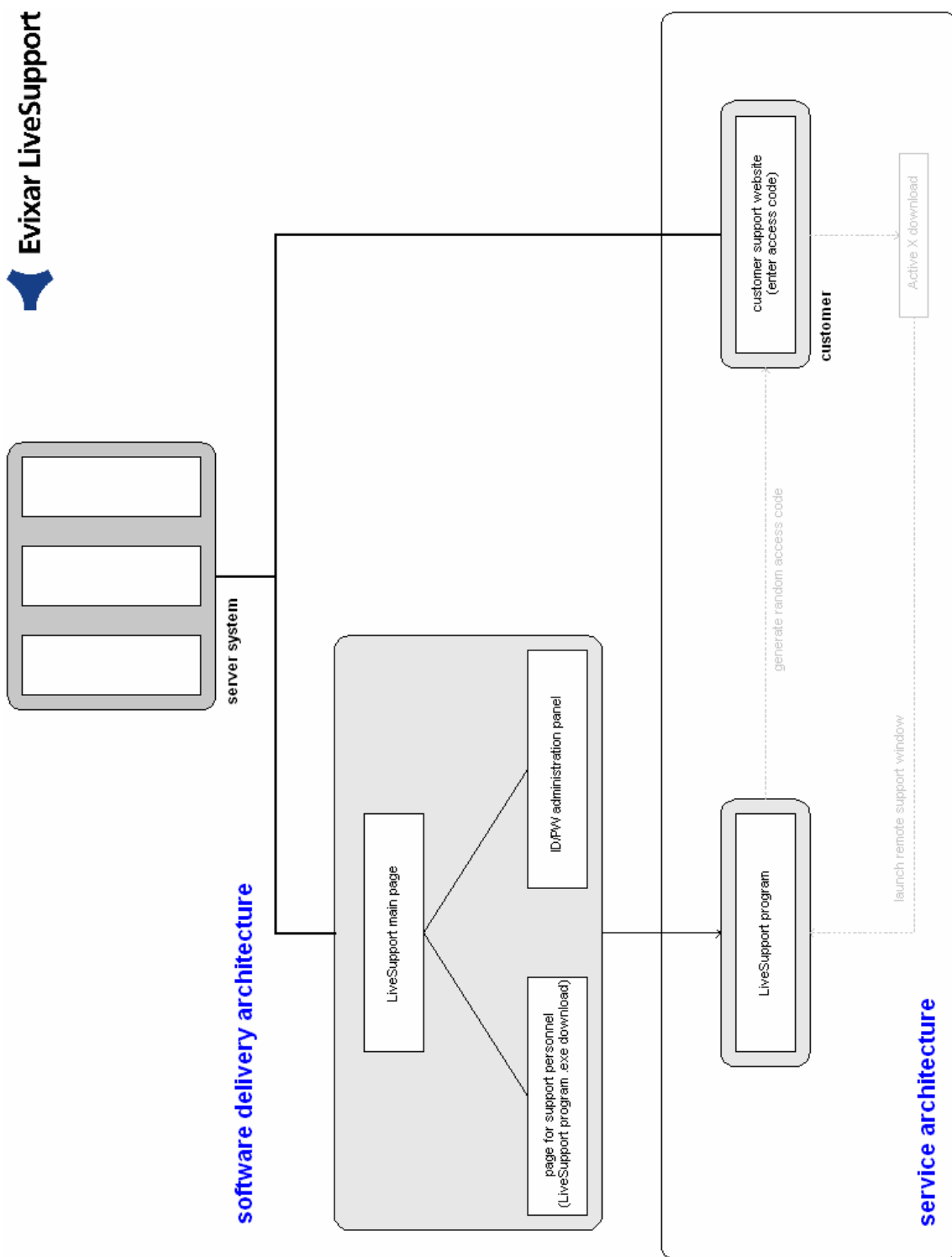
二重認証

正規ユーザーが自らのコンピュータを使用していることを保障するため、サーバだけでなくクライアントのコンピュータからも認証を要求される構成となっています。



システム構成 – Evixar Neturo





Evixar LiveSupport