

# アリエル・エアワン・プロジェクト A におけるセキュリティ

2004-08-31

アリエル・ネットワーク株式会社

序章 「アリエル・エアワン・プロジェクト A 」と「アリエル・フレームワーク」	2
1. アリエル・エアワン・プロジェクト A のセキュリティコンセプト	3
2. 個人を特定できる仕組み	5
2.1 ユーザー認証	5
2.2 データ署名	6
3. データを特定者にのみ明示的に開示する仕組み	6
3.1 データの暗号化	6
3.2 ユーザーとルーム単位のデータへの ACL	7
4. DoS(Denial of Service)攻撃対策	7
5. FAQ	7

## 序章 「アリエル・エアワン・プロジェクト A 」と「アリエル・フレームワーク」

アリエル・フレームワークとはアリエル・ネットワークが開発した P2P のネットワーク・アーキテクチャをベースに、さらにアプリケーション開発向けのインターフェースを強化・拡張したものです。

アリエル・エアワン・プロジェクト A はこのアリエル・フレームワークによって構築されています。

アリエル・フレームワークの主な特徴は以下になります。

### ✓ クライアントの大容量データを共有

メールや ASP 型のサービスと異なり、利用者の PC 間で直接、アプリケーション上の大容量ファイルを共有することができます。

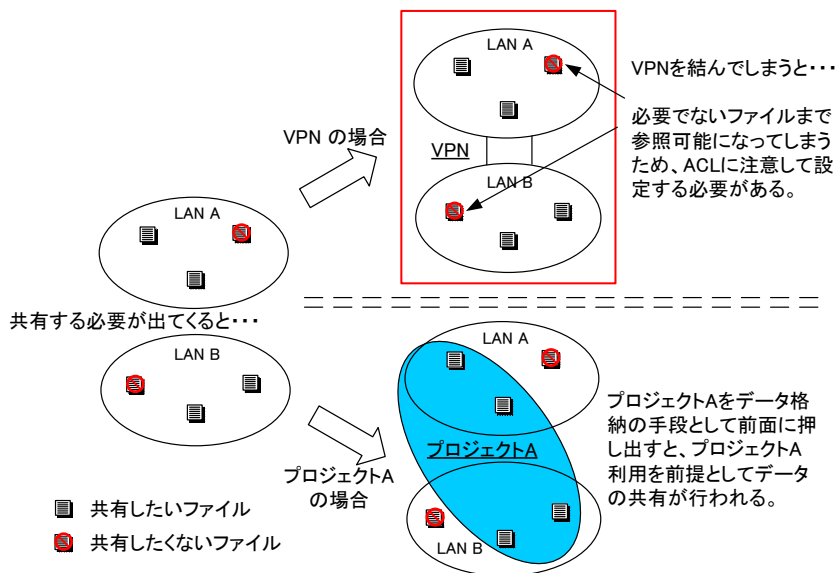
### ✓ 複数のメンバーと手軽にデータ共有

複数のメンバーとデータを共有して作業をすることができ、スタンドアロンとしての機能だけでなく、他のメンバーとのコラボレーションを図ることが可能です。

### ✓ アプリケーションレベルで高セキュリティを確保

ファイル自体を暗号化することで高いセキュリティを確保します。

アプリケーションレベルでデータを共有するため、明示的に選択したファイルのみをセキュアに共有することができます。



これらのポイントは弊社製品「アリエル・エアワン・プロジェクト A」大きな付加価値となっています。

この文書ではアリエル・エアワン・プロジェクト A の利便性を述べるにあたり必須となる、そのセキュリティのコンセプトや仕組みについて以下に記述します。

## 1. アリエル・エアワン・プロジェクト A のセキュリティコンセプト (サーバー・クライアント型システムとの比較)

アリエル・エアワン・プロジェクト A では、複数のセキュリティ手段を組み合わせることで、従来のサーバー・クライアント型のシステムでは難しかった、セキュアで柔軟な情報共有を実現します。

ここではアリエル・エアワン・プロジェクト A のセキュリティコンセプトをサーバー・クライアント型システムでのセキュリティと比較し、そのセキュリティ面での有用性を述べます。

### ➤ サーバー・クライアント型でのセキュリティ

サーバー・クライアント型のシステムでは、とにかく不正なユーザーをサーバーにつなげないことに重点を置きます。ファイアウォールや利用時の認証でセキュリティを保ち、サーバーに強固なセキュリティを集中して構築します。

逆に攻撃する側から言えば、サーバーの認証さえ突破できれば良くなり、攻撃の的が絞りがよくなってしまいます。その認証を突破されてしまうと、その後はたとえ不正ユーザーでも正当なユーザーになりすますことも可能になってしまう場合が多く、サーバーの設定を意図に反して変更されると、不正ユーザーを不正ユーザーとして認識できなくなってしまう可能性があります。

サーバーの認証を突破されると、それに順ずる各クライアントのデータも自由自在に入手できるというのもよくある話で、これを防ぐには結局各クライアントでのセキュリティも考えなくてはなりません。

これは、サーバーの認証を通ったユーザーに不正なユーザーはいないという前提の下にセキュリティを構築しているためです。そのために正当なユーザーを装って、不正にデータを入手されてしまう可能性があるのです。これは、各クライアントのデータの保管とそのセキュリティを一括集中でサーバーが負担しているために起きる現象だとも言えます。

また、外から会社のデータを利用したいときや社外の人とやり取りするためには、リモートアクセスのための裏口を設け、その裏口のセキュリティも考えなければならなくなり、クライアント側に高い自由度を与えつつセキュリティを保つためには多大な労力を必要とします。

### ➤ アリエル・エアワン・プロジェクト A でのセキュリティ

アリエル・エアワン・プロジェクト A では、クライアント側に高い自由度を与えつつセキュリティを保つために、以下の三つの仕組みを持ち合わせています。

- (1) 個人を特定できる仕組み
- (2) 情報を特定者にのみ開示する仕組み
- (3) Dos 攻撃などを防ぐ仕組み

#### ● 個人を特定できる仕組み

アリエル・エアワン・プロジェクト A では、それぞれの PC やユーザーが相手を確認するという点に重点が置かれます。

サーバーのセキュリティに左右されずに、各ユーザーが情報を交換してもいい相手かどうかを判断し、セキュリティを保ちます。情報を交換してもいい相手かどうかを判断する決め手となるのは、ユーザーを確実に本人であるかどうかを証明する仕組み、すなわち相手が持っている証明書が正しいかどうかを見極める仕組みが非常に重要なポイントになります。

この場合、内側か外側か(サーバーの認証を通っているかどうか)という環境に左右されずに相手を判断しますので、リモートからのアクセスや、ファイアウォールや企業の壁を超えた、セキュアで柔軟な情報共有を実現しやすい仕組みとなっています。

また、ユーザーがデータを作成した際には必ず作成者の署名が付加されるため、不正に改ざんされた文書を検出することができます。

また、この「個人を特定できる仕組み」が、Napstar や Winny など、いわゆるファイル交換ソフトとアリエル・エアワン・プロジェクト A の大きな違いになります。ファイル交換ソフトの違法性は、その匿名性に起因するところが大きいのですが、アリエル・エアワン・プロジェクト A では、匿名での利用はできなくなっています。またユーザーが明示的に選んだユーザーとのみデータを共有するので、違法行為を行いにくい仕組みになっています。

- データを特定者にのみ明示的に開示する仕組み

アリエル・エアワン・プロジェクト A ではデータを共有する際には自動で暗号化されますので、そのデータを不正に入手されても、解読できないようになっています。したがってインターネットを経由した環境においてもセキュリティを保つことができます。また、データへの ACL 設定によって、ルームメンバー以外のユーザーには情報を開示しない仕組みを持っています。そして、アプリケーションレベルでのデータ開示ですので、関係の無いユーザーやファイルのセキュリティレベルを変更せずに、必要なデータのみを開示することができます。

- Dos 攻撃などを防ぐ仕組み

アリエル・エアワン・プロジェクト A は Dos 攻撃などの不正なパケットを送信するユーザーを排除する仕組みを持っています。

上記の仕組みを組み合わせることによって、セキュアで柔軟な情報共有を実現します。

セキュリティの各仕組みについては次章より詳しく説明します。

## 2. 個人を特定できる仕組み

### 2.1 ユーザー認証

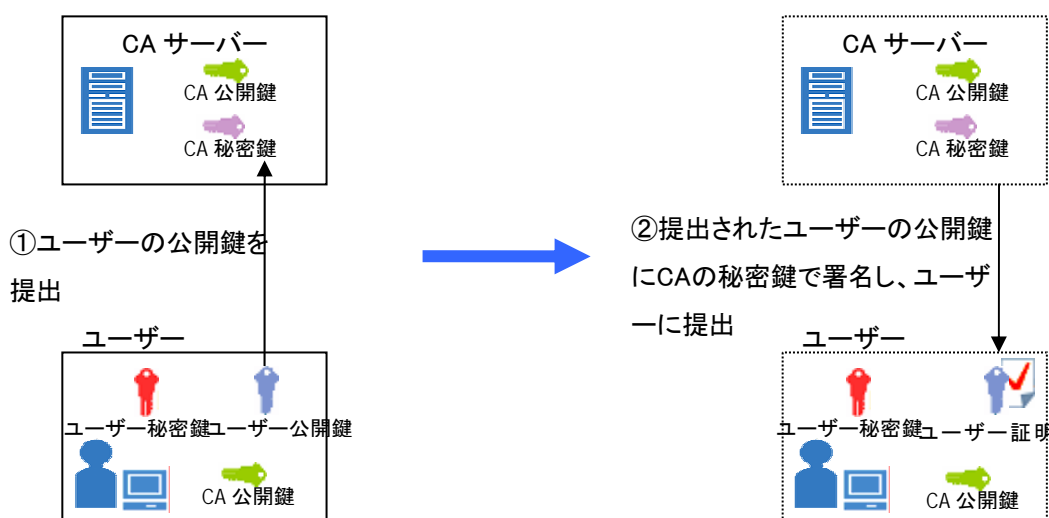
1.で述べたように、ユーザーを確実に本人であると証明する仕組みが、アリエル・エアワン・プロジェクト A でのセキュリティを維持する際の生命線になります。

そのユーザー認証方法は PKI(公開鍵暗号方式)です。

まず、各ユーザーは自分自身の秘密鍵と公開鍵(アプリケーションセットアップ時に作成)と CA の公開鍵を所持(アプリケーション内にハードコード)しています。

その後、自分の公開鍵をアリエル・ネットワークにある認証局サーバ(以下 CA)に提出します。

CA は各ユーザーから提出された公開鍵を CA の秘密鍵で署名し、それを各ユーザーに返します(CA による認証と署名、登録)。公開鍵に CA の署名をしたものがユーザーの証明書となります。CA はユーザーの成りすまし防止のために 2 重登録ができない仕組みを持っているため、そのユーザーの証明書は唯一無二の証明書になります。



セットアップ完了後には

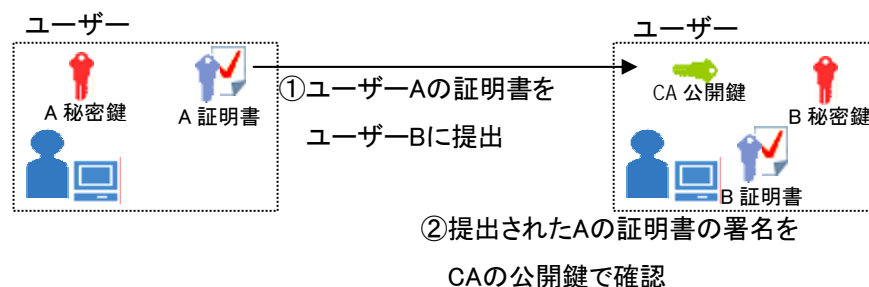
各ユーザーは自分の「秘密鍵」、「証明書」、「CA の公開鍵」を所持します。

その後、他のユーザーとデータを共有する際に、このユーザー(以下ユーザーA)は他のユーザー(以下ユーザーB)に自分の証明書を配布し、ユーザーB はそれをキャッシュします。ユーザーB は CA の公開鍵を所持しているので、提出された A の証明書の署名を確認することができます。ユーザーA から配布された証明書の署名を CA の公開鍵で確認できるということは、その証明書は CA の認証と署名を受けていることが証明され、

証明書の配布元ユーザーは間違いなく CA から認証されたユーザーA であることが証明されるのです。

※補足 CA 公開鍵の鍵長: 4k bit

各ユーザー証明書: X.509 証明書を独自拡張 鍵長 512 bit



## 2.2 データ署名

ユーザーA がデータを作成する際にはユーザーA の秘密鍵を用いた署名が付加されます。

他のユーザーB は自分が所持している A の公開鍵で署名を確認することができ、不正に改ざんされた文書を検出することができます。

## 3. データを特定者にのみ明示的に開示する仕組み

### 3.1 データの暗号化

アリエル・エアワン・プロジェクト A ではセキュアな情報共有を実現するためにデータの暗号化を行っています。暗号化はルーム単位で行います。その方法是对称鍵暗号と公開鍵暗号を組み合わせた暗号化です。まず、ユーザーA がルーム(メンバーは A と B)作成時にルームの対称鍵(以下ルーム鍵)を作成します。データ作成時にはそのルーム鍵で暗号化します。

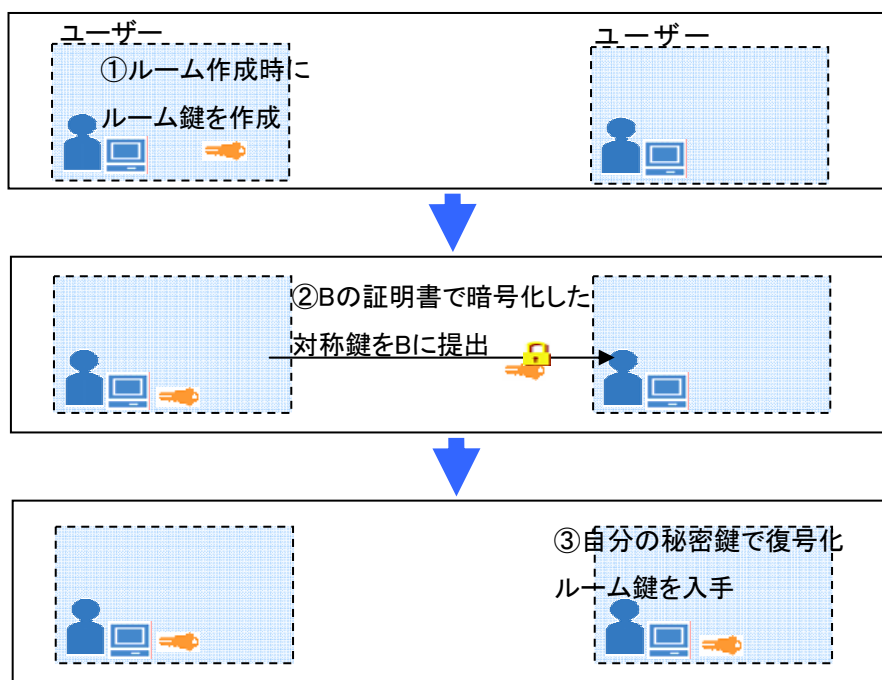
#### ➤ 対称鍵暗号と公開鍵暗号の組み合わせた暗号化(下図参照)

前述のユーザー認証にて A は B の証明書を所持していますので、ルーム鍵を B の証明書によって暗号化します。その B 宛に暗号化されたルーム鍵を B に提出します。

それを復号化できるのは B の秘密鍵を持っているユーザー、すなわち B だけになり、ルーム鍵を受け取れるのは B だけになります。したがって配布中に暗号化したルーム鍵を不正に入手されても復号化はできないので、強固なセキュリティを保ちます。

暗号化されたデータを受け取ったメンバーはルーム鍵を用いて復号化します。すなわち暗号化されたデータを復号化できるのはルームメンバーである A と B だけになります。

※補足 : ルーム鍵 対称鍵暗号: blowfish [鍵長 可変(32-448bit)]



### 3.2 ユーザーとルーム単位でのデータへの ACL

アリエル・エアワン・プロジェクト A 上でのデータは、ユーザーとルーム単位で ACL(Access Control List)を設定しています。ACL は、アクセスそのものを許可、拒否する allow フラグと、Unix ファイルシステム風の read、write、execute フラグを設定します。

この ACL によって、データを閲覧できるユーザー、編集できるユーザーなどを設定することができます。

ルーム内で共有するデータは、ルームメンバーにのみアクセス権限が与えられ、他のユーザーは見ることはできません。そのため、セキュリティを維持した状態で組織の壁を越えたデータ共有を実現できます。

## 4. DoS(Denial of Service)攻撃対策

アリエル・エアワン・プロジェクト A では、各ユーザーが、『大量のパケットを送る、または不正パケット(不正な id を含むコマンドなど)を送るユーザー』との接続を自動で切断する仕組みを持っています。

全てのユーザーから接続を切断された不正ユーザーは、結果的に排除されるようになります。

## 5. FAQ

### Q1.

**Q. 通信を盗聴された場合、データは安全ですか？**

A. 安全です。

通信中を流れるデータはユーザーが設定したルームのルーム鍵によって暗号化されているので簡単には盗めません。データを復号化できるのはルーム鍵を持っているユーザー、すなわちルームメンバーだけです。

また、ルーム鍵を配布する際にはルーム鍵自体を暗号化して配布していますので、ルーム鍵を不正に入手されることはありません。

### Q2.

**Q. 鍵の強度は大丈夫ですか？**

A. 安心してください。

ユーザー認証には公開鍵暗号方式、データの暗号化には公開鍵暗号方式と対称鍵暗号方式を組み合わせた暗号方式(前述参照)を用いています。

公開鍵暗号方式はベリサインの認証局にも使用されている強度な方式です。簡単に鍵を見つけることはできません。

また、それぞれの鍵長はスーパーコンピュータを用いて解読しようとしても困難なレベルの強度を持っています。

※参考: SSL 暗号化通信の標準鍵長 = 128 bit

### Q3.

**Q. PC を盗難された場合、データは安全ですか？**

A. 安全です。

ディスク上のデータは暗号化されているのでアプリケーションにログインしないと簡単には盗めません。また、ログインにはパスワードが必要になります。そのパスワードファイルはCAの秘密鍵によって暗号化されていますので、簡単にパスワードを入手することはできません。

✚ Q4.

Q. 取得したデータがコピーされて情報漏洩しませんか？

A. 安心してください。

共有化されたデータは全て暗号化された状態で保存されていますので、データをコピーしても、暗号化されたデータがコピーされるだけです。すなわち、データだけを所持していても、中身を見ることはできません。

✚ Q5.

Q. 別ユーザーに成りすまして文書を作成する事や、匿名ユーザーの文書作成を防げますか？

A. 防げます。

ユーザーは、ユーザーID をベースにして証明書を発行されたユーザーのみに実行権限が与えられる仕組みです。このため、別ユーザーになりすますことはできなくなっています。

また、ID が無いことを匿名ユーザーの定義にするなら、匿名ユーザーで書き込むことは不可能です。万が一、表示上、別ユーザーや匿名ユーザーになることができたとしても、そのユーザーのデータは PKI ベースの署名が無いので不正な書き込みであることを判別可能です(PKI ベースの署名をつけるには秘密鍵が必要です)。

✚ Q6.

Q. 既存のネットワークのセキュリティ設定を変更する必要はありますか？

A. アリエル・エアワン・プロジェクト A では通信を行う際に複数(有限)のポートを使用しています。

セキュリティが厳しいネットワーク環境では、これらのポートはほとんど使用することはできなくなっていると思われ、設定を変更することで使用できるようになります。

しかし、アリエル・エアワン・プロジェクト A はそれらのポートが使用できない場合は 80 番と 8080 番のポートを使用して通信する仕組みを持っています。

つまりインターネットにつながる環境であれば、設定を変更せずにアリエル・エアワン・プロジェクト A を利用することが可能です。

また、アプリケーション同士だけのデータ共有ですので、関係の無い人やファイルのセキュリティレベルを下げる必要はありません。

✚ Q7.

**Q. VPN とは何が違うのですか？**

A. インターネット上をセキュアに通信するという点で言えば同じになります。

しかしアリエル・エアワン・プロジェクト A では VPN とは違い、ネットワークや拠点単位ではなく、アプリケーションレベルでセキュアな情報共有を行いますので、より精度が高いプライベートネットワークを利用することができます。

また、VPN では、A 社のネットワーク対 B 社のネットワークといった形で、1 つの VPN 毎に 2 つの拠点でルーターやファイアウォールの設定を行う必要があり、実際に情報共有を行うまでに時間と手間がかかります。アリエル・エアワン・プロジェクト A では共有相手の変更に伴う設定の変更などは必要なく、各ユーザーはネットワーク環境を意識せずに任意の共有相手を選択できるので、より柔軟にセキュアな情報共有が可能な仕組みになっています。リモートアクセスについても、リモート専用の特別な設定など必要なく、インターネット経由で利用することが可能です。

さらに、VPN はオンライン環境においてのみ利用できますが、アリエル・エアワン・プロジェクト A はクライアントアプリケーションなので、オフライン環境においても利用できることも利点のひとつです。

**Q8.****Q. アリエル・エアワン・プロジェクト A を利用した、クラッカーの侵入が心配です。**

A. 安心してください。

アリエル・エアワン・プロジェクト A は通信を行う際に複数(有限)のポートを使用しています。しかし、最悪でも 80 番と 8080 番のポートだけを空けて通信する事は可能です。

また、アリエル・エアワン・プロジェクト A では大量のパケットを送る、または不正パケット(不正な id を含むコマンドなど)を送るユーザーとの接続を自動で切断する仕組みを持っていますので、クラッカーの侵入を防ぐことができます。

**Q9.****Q. アリエル・エアワン・プロジェクト A でのウィルス感染が心配です。**

A. 安心してください。

アリエル・エアワン・プロジェクト A では匿名性を排除しており、また特定のユーザーとのみ情報共有を行います。

ウィルスメールやスパムメールのように匿名のユーザーや既知ユーザーに成りすましたユーザーからいきなりウィルスファイルを送りつけられることはありません。

ウィルスメールやスパムメールでは、大抵送信者アドレスを偽装されていますが、アリエル・エアワン・プロジェクト A 上のデータは全て作成者の署名がされ、架空のユーザーや既存のユーザーへの成りすましもできない仕組みになっていますので、ルームメンバーがアリエル・エアワン・プロジェクト A 上でウィルスファイルを共有した場合でも、感染源の特定も容易にできるようにな

っています。  
また、ローカルのウイルス対策ソフトを用いれば、ウイルスファイルを開いたときに感知することが可能です。

✚ Q10.

**Q. パスワードが盗まれたらどうなりますか？**

A. パスワードを盗まれたとしても、ユーザーの秘密鍵を所持していなければ何もできません。また、ユーザーの秘密鍵と証明書のキーペアを作成するためには CA による認証と署名が必要となりますので、秘密鍵を不正に偽造することはできません。

✚ Q11.

**Q. 秘密鍵が盗まれたらどうなりますか？**

A. 秘密鍵はユーザーが設定したパスワードで守られているので、パスワードが洩れなければ安全です。また、パスワードファイルは CA の公開鍵によって暗号化されていますので、パスワードファイルが流出しても他ユーザーが復号化することはできません。

✚ Q12.

**Q. 秘密鍵とそのパスワードの両方が盗まれたらどうなりますか？**

A. 秘密鍵を持っていることとそのパスワードを知っていることが、ユーザーの同一性の保証になっています。パスワードは 1 ヶ月に一度くらいの頻度で変更することを推奨します。また、CA 側でその ID の実行権を削除することもできますので、万が一両方が盗まれたとしても対処が可能です。

✚ Q13.

**Q. 社員が情報漏洩するのが心配です。**

A. ルームを複数作成する事で ACL を利用し、全てのデータを見せるルーム、一部のデータしか見せないルームを設定することが可能です。また、CA 側で各ユーザーの証明書の実行権限や有効期限を設定することが可能ですので、一度そのユーザーが取得した情報も、見せなくさせることができます。

✚ Q14.

**Q. 署名したユーザーをあとで無効することは可能ですか？**

A. 可能です。  
CA 側で、ユーザーの証明書の実行権限を無効にすることができます。また、証明書の期限を操作することも可能です。