2016 年 7 月 14 日

ソフトバンク・テクノロジー株式会社

報道関係者　各位

サイバートラストとパスロジ、端末認証とワンタイムパスワードによる二要素認証を実現
～F5 ネットワークス「BIG-IP APM」連携でより強固なリモートアクセス環境を構築可能に～

ソフトバンク・テクノロジー株式会社の子会社であるサイバートラスト株式会社（本社:東京都港区、代表取締役社長：眞柄 泰利、以下：サイバートラスト）は、パスロジ株式会社（本社：東京都渋谷区、代表取締役社長：小川　秀治、以下、パスロジ）と、デバイス証明書管理サービスの「サイバートラスト デバイス ID、以下、デバイス ID」、パスロジック方式によるトークンレス・ワンタイムパスワードの「PassLogic（パスロジック）」と F5 ネットワークスジャパン合同会社（本社：東京都港区、代表執行役員社長：古舘正清、以下、F5）が提供するリモートアクセス・ソリューションの「BIG-IP APM（※1）」を連携させる共同検証が完了したことを発表しましたので、お知らせします。

（添付資料　全４枚）
サイバートラストとパスロジ、端末認証とワンタイムパスワードによる二要素認証を実現
～F5 ネットワークス「BIG-IP APM」連携でより強固なリモートアクセス環境を構築可能に～

以上

※本リリースに記載されている会社名、製品名、サービス名は、当社または各社、各団体の商標もしくは登録商標です。

（この報道発表は2社から同時に配信するため、重複して配信される場合があります。ご迷惑をおかけしますがご容赦ください。）

2016 年 7 月 14 日

Press Release

サイバートラスト株式会社
パスロジ株式会社

サイバートラストとパスロジ、端末認証とワンタイムパスワードによる二要素認証を実現

～F5 ネットワークス「BIG-IP APM」連携でより強固なリモートアクセス環境を構築可能に～

サイバートラスト株式会社（本社：東京都港区、代表取締役社長：眞柄 泰利、以下、サイバートラスト）とパスロジ株式会社（本社：東京都渋谷区、代表取締役社長：小川 秀治、以下、パスロジ）は、デバイス証明書管理サービスの「サイバートラスト デバイス ID、以下、デバイス ID」、パスロジック方式によるトークンレス・ワンタイムパスワードの「PassLogic（パスロジック）」と F5 ネットワークスジャパン合同会社（本社：東京都港区、代表執行役員社長：古舘正清、以下、F5）が提供するリモートアクセス・ソリューションの「BIG-IP APM（※1）」を連携させる共同検証が完了したことを発表します。この共同検証により、端末認証とワンタイムパスワードを連携させた二要素認証の利用が可能となり、より強固でセキュアなリモートアクセスが実現します。

企業における事業継続性やワークスタイルの変化に伴い、どのような環境からも安全に社内ネットワークやクラウドサービスへアクセスするためのセキュリティ対策が求められています。このようなセキュリティ対策には、多くの場合、ID/パスワードによる認証が用いられます。しかし、不正アクセスによる ID/パスワードの漏えいやパスワードリスト攻撃などによって、不正ログインによる被害が急増しており、ID/パスワードだけの認証では十分な対策とは言えません。

サイバートラストとパスロジは、「デバイス ID」と「PassLogic」を組み合わせて二要素認証を可能にすることで認証セキュリティを強化し、更に「BIG-IP APM」を連携させることで、ネットワーク統制とシングルサインオンを可能にするクラウドサービスへのセキュアなアクセスを実現します。

サイバートラストとパスロジは、今後も協力して安心安全なネットワーク社会の実現と、お客様の事業活動における業務効率化、顧客創造、リスクマネジメント等に貢献するサービスを提供して参ります。

（※1）BIG-IP APM…F5 が提供する、認証基盤の統合、リモートアクセス、ウェブアクセス、アプリケーションへのアクセスなどを統合するアクセス管理ソリューション。ユーザーID とコンテキストに基づいて、アプリケーション、データ、ネットワーク、クラウドへのアクセスが保護、区別されます。そのため、自社のネットワークやクラウドにアクセスできる

のは誰で、どのアプリケーションにどのデバイスや場所からアクセスできるのかを一元管理できます。
BIG-IP APM により、ユーザーやアプリケーションの場所に関係なく、ID ベース、コンテキスト認識型、ポリシー主導の動的なアプリケーションアクセス制御を一元的に行うことができます。

F5 の代表執行役員社長である古舘正清　様は、今回の共同検証について次のように述べています。

ワンタイムパスワード認証及びクライアント証明書による端末認証を活用した非常に強固な複数要素認証の共同検証を完了したことを大変嬉しく思います。昨今、スマートデバイスの業務利用のニーズは確実に強まっている一方で、利便性を犠牲にすることなく、セキュリティをどのように担保するかが大きな課題になっています。両社のソリューションに F5 の BIG-IP APM を組み合わせることで、強固なセキュリティを実現されたいお客様への最適なソリューションがご提供できると確信しております。

■サイバートラスト　デバイス ID について
「サイバートラスト　デバイス　ID」は、会社が許可した端末を厳格に認証し、安全なネットワークアクセスを実現するマルチデバイス対応のデバイス証明書管理サービスです。マルチデバイス、マルチネットワーク環境において、不正端末からのアクセスを防止し、安全に情報資産を活用できる共通の端末認証基盤を実現します。
https://www.cybertrust.ne.jp/deviceid/

■サイバートラスト株式会社について
サイバートラストは国内で最長の運用実績を持つ認証機関であり、日本初の商用電子認証局として 20 年以上にわたり SSL サーバー証明書をはじめとした電子認証サービスを提供しているセキュリティベンダーです。マルチ OS、マルチフォームファクターに対応した端末電子認証サービス「デバイス ID」は国内導入 No.1 の実績です。今後、利用形態や用途が拡大する IoT デバイスにおいても電子認証サービスを提供することで、利用者が、安心安全にサービスを受けられる社会の実現を目指します。
https://www.cybertrust.ne.jp/

■PassLogic について
PassLogic では、トークンの要らないワンタイムパスワードを実現する認証方式として、「パスロジック方式」を採用しています。
この「パスロジック方式」は、ブラウザ上に表示される乱数表の中から、利用者ごとに設定されている“位置”および“順番”（シークレットパターン）に沿って数字を抽出し、つなげることでパスワードを生成する仕組みです。乱数表を表示するたびに表内の数字が変わるため、パスワードとなる数字も毎回変わり、ワンタイムパスワードとなります（米国特許第 6141751 号、日本国特許第 5276658 号）。第三者が乱数表を見ても数字を抽出する位置がわからなければ、パスワードを判別できません。
PassLogic ではこの認証方式を使用しているため、トークンを必要とせず、デバイスを紛失・盗難・借用された場合でも安全性を確保できます。この安全性と使用感、管理性などが評価され、リモー

トアクセスを重視される企業を中心に 100 万件を超える ID を発行し、ご利用いただいております。
http://www.passlogy.com/passlogic

■パスロジ株式会社について

パスロジ株式会社はワンタイムパスワード製品を主要ビジネスとする認証ベンダーです。マトリクス型のワンタイムパスワード「PassLogic(パスロジック)」を最初に考案した会社であり、全世界を含めて、唯一、 PassLogic の知財ライセンスを実施できる会社となっています。パスロジック方式は、パスロジのオリジナル技術であり、パスロジの製品は、日本国内だけでなく、海外からの利用・海外での利用など、ワールドワイドのシステムでも、安心してご利用いただけます。
パスロジ株式会社は急発展を遂げるネットワーク社会において、安心かつ安全なセキュリティを提供し、その発展に貢献できる企業を目指して活動しています。
http://www.passlogy.com/

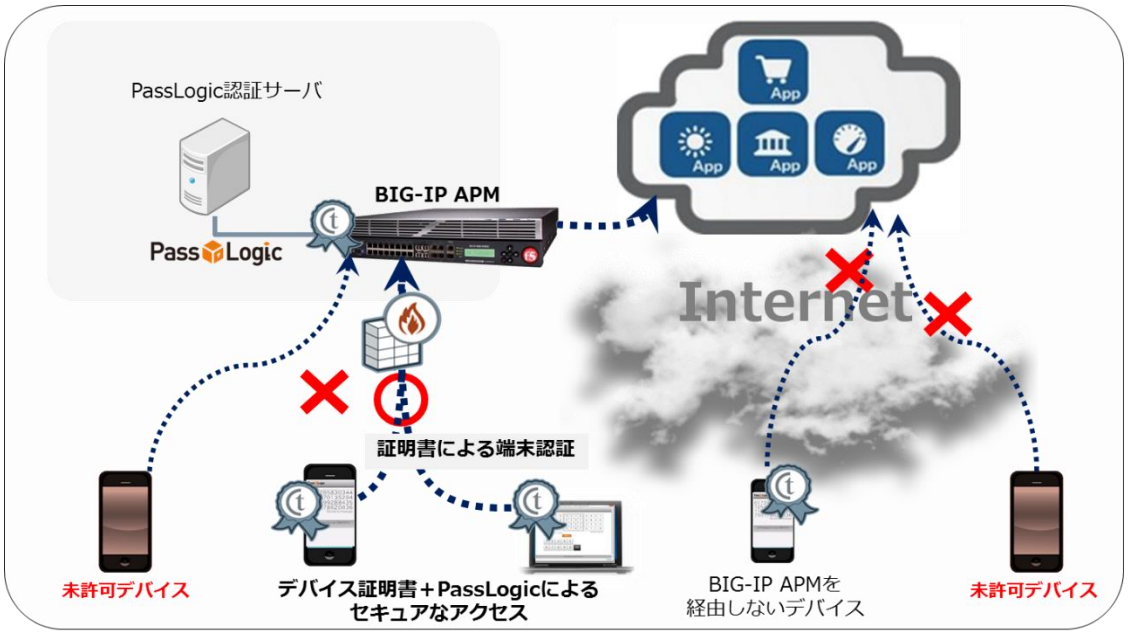
※文中記載の社名、商品名は各社の商標または登録商標です。

■報道関係者様からのお問い合わせ
サイバートラスト株式会社
広報担当:佐々木
Tel:03-6234-3800
E-mail: press@cybertrust.ne.jp

パスロジ株式会社
広報担当:黛、樫尾
Tel:03-5283-2263
E-mail:passlogic@passlogy.com

【参考資料】

各社のサービスの連携イメージ



「サイバートラスト デバイス ID」は、端末識別情報により端末を確実に特定した上でデバイス証明書を登録するため、厳格な端末認証が実現できます。不正な端末の持ち込みや不正なアクセスを防止し、クリーンなネットワーク環境を実現することによりセキュリティを強化することができます。

PassLogic は、トークンの要らないワンタイムパスワードを実現する認証方式として、「パスロジック方式」を採用しています。
この「パスロジック方式」は、ブラウザ上に表示される乱数表の中から、利用者ごとに設定されている“位置”および“順番”（シークレットパターン）に沿って数字を抽出し、つなげることでパスワードを生成する仕組みです。乱数表を表示するたびに表内の数字が変わるため、パスワードとなる数字も毎回変わり、ワンタイムパスワードとなります（米国特許第 6141751 号、日本国特許第 5276658 号）。第三者が乱数表を見ても数字を抽出する位置がわからなければ、パスワードを判別できません。

BIG-IP APM は、F5 のセキュアなリモートアクセス・ソリューションで、SAML2.0、複数のドメイン、豊富なシングルサインオン認証、およびモバイルデバイスへの対応など、さまざまな環境に対応しています。さらに、シンプルかつセキュアなアクセス環境を実現できるため、モバイルユーザー向けのアプリケーション・アクセス・コントロールを集約し、ビジネスの優先度やユーザー属性に応じて、特定のアプリケーションへの制限の無い VPN アクセスまたは制限付きアクセスを選択して許可することができます。

以上