E-BOOK

信頼を得るには、PKIが必要

digicert®

目次

アラスカの辺境から宇宙の果てまで

2013年夏のある雨の日、小型の水上飛行機がアラスカのピーターズバーグ近くにある山の上で低空飛行中に失速しました。乗客は6名で、LeConte（ルコンテ）氷河の観光ツアーに向かっていました。Horn Cliffs（ホーン・クリフス）に沿って上昇しようとした際に、パイロットの判断ミスから飛行機のコントロールを失い、きりもみしながら落下し、巨大な常緑樹に激突しました。

墜落事故の生存者は、負傷したまま急斜面に取り残され、自力で山を下りることは不可能に思われました。ほんの数時間で夜になります。6月とはいえ、アラスカの夜は凍えるほどの寒さで、携帯電話も通じず、道路もありません。墜落機から全員を救出し、無事に連れ帰ることができるのは、航空救助隊だけです。

上空約800Kmでは、イリジウム衛星が飛行機の緊急ビーコン信号を受信し、遭難信号と場所を救助隊に送信しました。単なるGPSまたは無線遭難信号とは異なり、イリジウム対応機器は、飛行機が離陸してから墜落する瞬間までの動きを追跡し、フライト全工程のリアルタイムのデジタルトレイルを作成します。これは、66のイリジウム衛星がそれぞれ綿密に統制された地球の周回軌道上にあり、衛星間および地上と通信を行い、常に地球全体を包括的に調査することで可能になります。イリジウム衛星ネットワークでは、南極大陸からアラスカまで、どこからでも、いつでも機能装置を見ることができます。

この特殊なトラッカーと緊急信号デバイスは、すべての航空機の標準ではありません。しかし、小型飛行機や遠隔地を横断するパイロットや所有者を中心に、これを導入する人は益々増えています。

ほとんどは安心のためですが、場合によっては、生死を分けることもあります。

飛行機が墜落した正確な場所を知ることで、米国沿岸警備隊は、数時間で事故現場に到着し、すべての生存者をヘリコプターで空から救助しました。生存者を墜落機から安全に引き上げ、病院に搬送した後、Alaska Public Media[1]が沿岸警備隊の報道官、Grant DeVuyst氏にインタビューしました。彼は、緊急信号デバイスについて次のように述べています。「それは、事故があったことを知る唯一の手段であり、実際に現場にたどり着き、救出するための唯一の手段でもあります。」

[1] https://www.alaskapublic.org/2013/06/05/one-dead-six-survive-float-plane-crash-near-petersburg/

「PKIは海底から宇宙の果てまで全てを守れると信じています」

Brian Trzupek
Digicert、製品担当上級副社長

このように希な緊急事態では、生命が危険にさらされている場合、パイロットはイリジウム衛星ネットワークがフライトを追跡し、遭難信号を傍受して、救助隊に伝えることを知っている必要があります。

信号は遮断されないように保護され、非常用装置が認証され、ネットワークが遮断されないように防御されている必要があります。イリジウム衛星のどこかに欠陥があれば、生命が失われる可能性もあります。最大の危機における信頼レベルで失敗は許されません。イリジウム衛星がPKIで保護されている理由はそこにあります。

信頼は動的なニーズ

英国人暗号学者James EllisとClifford Cocksが1970年代に初めて「公開鍵暗号（非秘密暗号）」を考案したとき、彼らはそれが世界中の何千万ものWebサイトで使用されるとは想像もしていませんでした。当時、インターネットはまだDARPAプロジェクトと呼ばれ、データや調査結果を共有しようとする大学の研究者をつなぐためにまれに使用される程度でした。

数十年間で世界は変わり、EllisとCocksの公開鍵基盤は、ハッキングや不正行為に対する盾として情報時代の中心に存在しています。今日では、Webサイトが信頼されるとしたら、その信頼はPKIによるものです。

しかし、ワールドワイドウェブ（www）の発明は、それだけで人類の発達の一時代を定義するのに十分ですが、その直後に接続機器で第二の革命が起きました。あっという間に冷蔵庫から金融アプリまですべてが、ネットワーク、デバイス、アプリケーション、およびユーザーのグローバルエコシステムの一部になり、距離を越えてつながりました。

成長のスピードは桁違いに速く、何十万人もの人々が何百万人もの人々と何十億ものモノをつなぐための新しいアイデアを開発する中で、強力なセキュリティの必要性は指数関数的な速度で上昇しています。

文化交流から医療の進歩まで、情報時代に生まれた様々な効用にもかかわらず、この巨大な通信ネットワークは、ハッカーや犯罪者がユーザーと技術を容易に信頼する気持ちにつけ込む新たな機会を提供しています。

この脅威に対するソリューションはシンプルです。接続されたすべてのモノに最高レベルの保証を組み込むことです。PKIはその基となる保証です。最も重要なデータが守られるという十分な信頼性と、最新の最も偉大な発明に取り組むために十分な柔軟性を備えたセキュリティおよびIDソリューションです。PKIによって、世界中さらには宇宙とも、ほとんど瞬時にコミュニケーションが取れる世界のメリットを享受するだけです。

PKIはその基となる保証です。

拡大を続ける脅威

ネットワーク接続を利用することで監視、効率化、および安全性をコンピュータ、アプリケーション、デバイスに組み込むための新しい独創的なアイデアを毎日目にします。しかし、新しい接続手法は、それぞれが新しい脆弱性、つまりアプリケーションやデバイスの通信相手による潜在的なエントリーポイントにもなります。

よく知られているのが金融リスクです。何年もの間、サイバー犯罪者がセキュリティギャップを利用する際に何が起きるかを見てきました。2017年、大手消費者金融が損害賠償として7億米ドルを支払うことで、大量の情報漏洩に対する訴訟を解決しました[2]。2019年に実施されたPonemon/IBMの調査では、情報漏洩時に発生するコストの平均は400万ドル弱でした[3]。さらにこの年のForgeRock社「Consumer Breach Report[4]」では、医療部門で177億6千万ドルの損失が報告されています。実際に、2019年には医療部門が最大のターゲットになっており、すべての漏洩の45%を占めています。

医療部門の財政的コストはそれ自体が驚異的ですが、おそらくその攻撃の数と性質はさらに注目すべきものです。

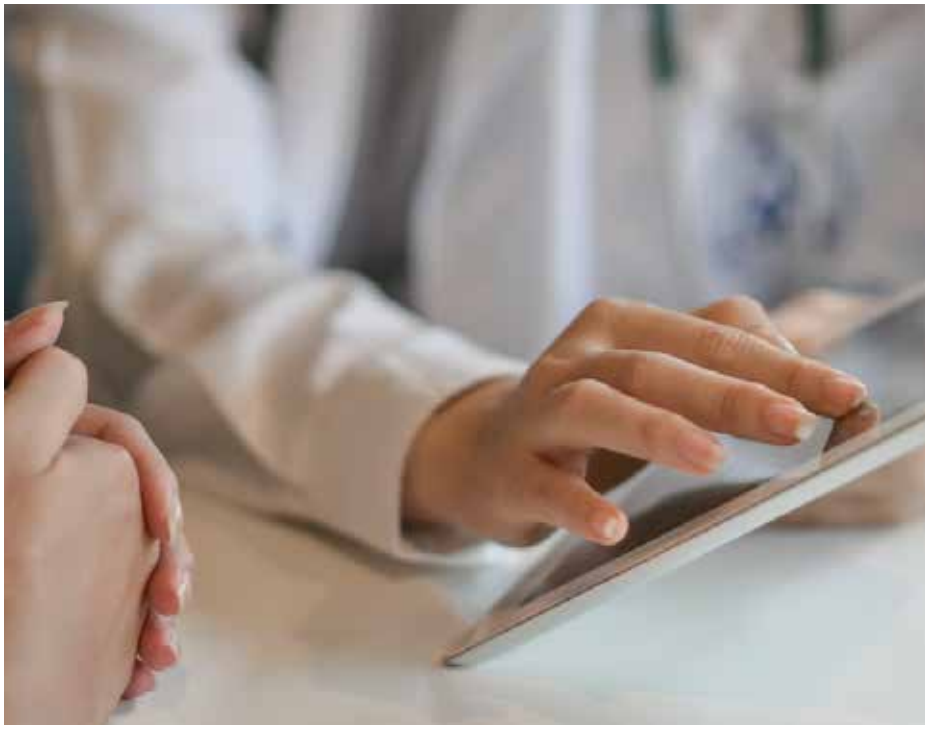
[2] https://investor.equifax.com/news-and-events/press-releases/2019/07-22-2019-125543228 [3] https://digitalguardian.com/blog/whats-cost-data-breach-2019 [4] https://healthitsecurity.com/news/health-sector-most-targeted-by-hackers-breach-costs-rise-to-17.76b

これらの損失は、様々な方法を使用して医療ネットワークを狙った382例の別々の侵害によるものです。これまでは銀行やオンライン販売を狙ったネットワーク・Webサイトのハッキングが一般的でしたが、今のサイバー犯罪者は、デバイスの脆弱性と十分な知識を持たないユーザーにつけ込んで、単純な情報から情報を引き出しています。

つまり、予算は脅威の増加に伴って増やされていないにも関わらず、企業はより大きなセキュリティ負担に対処することを余儀なくされます。電子カルテ、接続されたモニタ、高度な処置ツールは患者ケアに革命をもたらしましたが、これらの装置を使用する専門家は、セキュリティの脆弱性に関する専門家ではありません。また、IT部門には、予算の制約、新しいテクノロジー、地方や国の規制と法律がもたらす課題を乗り越えるために俊敏性が求められます。

情報社会は刺激的で前途有望な時代です。個人消費者から多国籍企業、国家に至るまで、関わっている技術的進歩の恩恵を受けられる立場にあります。しかし、舞台裏のITプロフェッショナルにとって、新しいテクノロジーに伴う新たな脅威を理解し、リスクを排除するためのソリューションを実装するのは大変な作業です。

この拡大し続ける脅威と戦うために、セキュリティのプロフェッショナルは、迅速に実装でき、管理が容易で、企業の成長と変化に合わせて拡大したり、適応したりして進化しながら、どのような攻撃にも対応できる柔軟なソリューションを必要としています。PKIはすべての要件を満たします。



この拡大し続ける脅威と戦うために、セキュリティのプロフェッショナルは、迅速に実装でき、管理が容易で、どのような攻撃にも対応できる機能を備えた柔軟なソリューションを必要としています。

ケーススタディ：アラバマ州フローレンス

井の中の蛙

2019年7月、1億人の顧客に影響する大規模な銀行情報漏洩のニュースが世界を駆け巡りました[5]。これは世界レベルでの大規模な情報詐取の1つの例です。

しかし、この漏洩の発生と同時期に、サイバー犯罪者はより小規模なターゲットに対し脆弱性をテストし、様々なサイトを調査して、セキュリティリソースが脆弱な所から何らかの利益が得られる場所を探していました。やがて、限られたリソースですべてのシステムとユーザーを保護することが困難になっている小さな政府にこの種の脆弱性を発見するに至りました。

このような犯罪者は、IT部門が大規模で設備の整った10億ドル規模の企業を相手にするのではなく、市や町のネットワークに侵入しランサムウェアをばらまくことで地方自治体を人質に取ります。

まさにこの事態が、2020年6月にアラバマ州フローレンスで発生しました。北側の州境、テネシー川のほとりにある人口4万人のこの町は、毎年行われるルネサンスフェアが有名で、ブルースの父と呼ばれるミュージシャン、W. C. Handyの出生地としても知られています。

5月末に、市の職員は侵害の可能性に関する警告を受け取っていましたが、その時点ではすでに手遅れでした。フローレンスのネットワークをハッキングした犯罪者は、1か月前から侵入し、町のシステムを掌握する作業を進めていたと思われます。6月5日にハッカーが攻撃し、身代金をビットコインで要求しました。

この犯罪の傾向に詳しいセキュリティの専門家と相談した上で、フローレンスは30万ドルを支払うことにしました。しかし、これはフローレンスだけで終わりませんでした。この侵害が成功を収めるちょうど4か月前に、ニューヨークタイムズは、2018年から2019年までにランサムウェア攻撃が41%[6]増加し、数十の市や町が攻撃されていたという調査結果を発表したのです。

はるかに大規模な情報漏洩がトップニュースになる一方で、ある犯罪グループは、より身代金を払いそうなより脆弱なターゲットを襲い、効率の良い作戦を開発しました。井の中の蛙は、防御に対するリソースがほとんどないターゲットに高度なサイバー攻撃を展開することで、コミュニティを食い物にしています。

他のセキュリティ・IDソリューションとは異なり、PKIは、ネットワークとEメールだけでなく、Webにも有効に機能する十分な柔軟性を備えています。PKIソリューションはセキュリティの実装を簡単にして、ITおよびセキュリティ担当者に、様々なシステム、デバイス、およびユーザーへ暗号化と認証用証明書の発行と管理を行う機能を提供します。

Webサイトを保護するためにすでに機能しているソリューションも、ネットワーク、デバイス、Eメール、文書、およびユーザーを守れます。また、セキュリティエコシステムの簡素化も行いながら、ランサムウェアの攻撃を防ぎます。

[5] https://www.capitalone.com/facts2019/ [6] https://www.nytimes.com/2020/02/09/technology/ransomware-attacks.html

第2章

PKIに関して知られていないこと

今日のネットワーク化された世界の課題は複雑さです。

それがより複雑な攻撃の課題でないとしても、新旧のテクノロジーが相互に作用する複雑なエコシステムの保護の課題です。さらに、より複雑なエコシステムの課題でないとしたら、より複雑で高度な脅威に対して、ユーザーが常に最新ではないシステムを保護する際の課題です。

セキュリティのコンサルタントやアナリストは、世界中のITおよびセキュリティプロフェッショナルから同じ不安を聞きます。それは、セットアップと管理が簡単で、絶対的に信頼できるソリューションが必要だと言うことです。

そこでPKIの出番です。

インターネットセキュリティをご存知の方は、PKIのことはすでにご存知でしょう。多分かなり前から知っていたと思います。なぜなら、PKIはこの20年間、最初はSSL、現在はTLSという形式で、Webサイトのセキュリティソリューションとして信頼されてきたからです。今日も20年前と同じ信頼性を証明された仕組みで機能しています。

しかし、多くの人が、PKIはWebを保護するだけではないと知って驚きます。PKIはアプリケーションも保護します。コードも保護します。スマートウォッチ、自動車、電子契約、医療デバイス、衛星も保護します。20年間Web上で信頼性を確かめられ、信頼に裏打ちされたセキュリティソリューションは、関連する最新の最も革新的な製品においても同様に信頼できることが分かっています。

PKIは証明済みです

ネットワーク化された世界は日々進化していますが、PKIは、20年前に暗号化されたワールドワイドウェブを保護していたように、最新のIoTデバイスも保護できることが実証されています。

PKIの優れた点は、非対称暗号鍵を使用した鍵ペアの簡潔さにあります。非対称暗号では、一方がデータを保護し、共通の秘密を共有することなくもう一方に送ることができます。いずれかの鍵の暗号鍵が分かっても、他の暗号鍵を解くことはできません。データを読むには両方の暗号鍵ペアが必要です。

その結果、数十年にわたり信頼性が実証されています。

PKIはフレキシブルです

今日のエコシステムでは、専門家がWebサイトに加えてアプリケーションも保護し、電子書類に安全な署名をしながら従業員のスマートフォンを認証する必要があります。ある企業では、製造ラインの自動化ロボット用のソリューションを必要とする一方で、顧客のクレジットカード番号も保護する必要があります。１つの手段としては機能しても、他では機能しない、またはある時点には機能しても翌日は機能しないというソリューションは、セキュリティを管理するITチームの負担になるだけでなく、企業を危険にさらします。

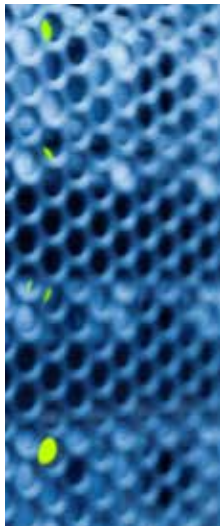
他のセキュリティソリューションとは異なり、PKIは信じられないほどフレキシブルです。PKIは、非対称鍵ペアを利用し、セキュリティプロセスで暗号化と同じくらい簡単に検証を行えるため、様々な環境に導入して、幅広い接続を保護することができます。PKIソリューションは縮小も拡大も可能で、クラウド、オンプレミス、ハイブリッドで稼働し、今日はWebとEメール、明日はBYODとIoTを保護するということも可能です。1つで複数のセキュリティニーズに対応できるソリューションです。

PKIはパブリック、プライベート両方の信頼を実現する

単なる暗号化だけでなく、PKIは署名プロセスを使用してIDと鍵を結びつけます。署名はルートより発行されるため、そのルートの公開鍵を持っていれば、誰でもPKI証明書にバインドされた署名が有効で信頼できるかが分かります。

パブリックルートの場合、ChromeやFirefoxなどのWebブラウザやMicrosoft WindowやApple MacOSなどのオペレーティングシステムによって保護された信頼できるストアより配信されます。プライベートルートの場合は、企業が内部的に使用する任意のシステムまたは小規模な企業グループ内でのみ信頼されます。暗号化はどちらのケースでも同様に行われますが、パブリックとプライベートの両方のオプションに対応できることが、PKIの汎用性を高めています。

この柔軟性により、PKIはパブリックとプライベートの信頼性のギャップを埋めます。多くの国の政府向けのプライベート暗号化およびIDソリューションとして信頼できるだけでなく、同様にIoTデバイス向けのパブリックソリューションとしても信頼できるほど十分に強力で安全です。



PKIは簡単

これまで、PKIの実装は複雑でした。専門家とそして簡単に利用ができる管理プラットフォームツールに頼らず、正しい運用に必要な専門知識も持たずに、個々のITプロフェッショナルが社内でPKIソリューションを開発するリスクを背負わなければなりませんでした。いったん稼働すると、PKIはその信頼性により理想的なソリューションになりましたが、そこに至るまでが困難で、解決するより多くの問題が発生していました。

幸いなことに、これは遠い過去のことになりました。今では、PKIは、適切に行えば、簡単にセットアップして使用することができます。PKIソリューションを配備して監視するための高度なツールが、シングルサインオンプラットフォームで実行されるようになりました。さらに、PKIは非常に汎用性があるため、1か所で多種多様なセキュリティ問題に対して簡単にソリューションを実行できます。1つの目的のためにPKIソリューションを構築する複雑さに対処するのではなく、1か所に複数のセキュリティソリューションを配備して管理できるようになったため、PKI環境を立ち上げて稼働させるために、専門知識は必要ありません。

PKIに関する4つの誤解

PKIはまだ使われていますか？

トレンドは巡ります。PKIは今も使われているだけでなく、進化しながら普及しています。PKIの価値は柔軟性と長年にわたる信頼性にあります。エンジニアはPKIが最善のソリューションを利用する必要のあるシステムを次々に見つけ出し、堅牢な保護で長年の実績があるテクノロジーであるPKIセキュリティおよびIDを実装することができます。

Chrome問題はどうなりましたか？ PKIは破綻していませんか？

PKIの実績は、セキュリティに関しては信じられないほど優秀です。ただし、実装方法は、証明書を発行する機関によって異なります。2017年、Googleは、Symantecによって発行された一連の証明書をCA/Browser Forum Baseline Requirementsに準拠しなくなったという理由で信用しないようにすることを発表しました[7]。

これは、失敗したビジネス手法の残念な例で、その影響は広範囲に及びました。世界中のセキュリティに大きなギャップが生じることを懸念して、SymantecとGoogleは、信頼レベルを保持する認証局と大量の再発行を管理するために必要なイ

[7] https://security.googleblog.com/2017/09/chromes-plan-to-distrust-symantec.html

ンフラストラクチャを探し始めました。彼らは、DigiCertを選択し、Symantecの証明書を信頼できるDigiCertのルートに移行するよう手配して、Chromeユーザーが混乱することなくPKIにより信頼されたWebサイトにアクセスできるようにしました。

20年前と同じように、PKIはChrome上においてWeb通信を保護するための信頼されたソリューションです。

PKIが機能しないデバイスが多数あります。

PKIは、プログラムが実行できるデバイスであれば、どれでも機能すると言った方が正確です。非対称鍵ペアが動作するには、十分な処理速度、メモリ、ディスクスペースが必要です。当然、PKIは20年以上も利用されてきた技術なので、90年代末のプロセッサが鍵による暗号に対応できていたことを考えれば、最近のデバイスはどれでも、PKIを実行する能力があるといえるでしょう。ただ場合によっては、マイクロプロセッサが進歩しても、IoTデバイスの性能特性は極めて原始的なため、迅速に鍵を生成したり、通信チャネルに署名したりできないこともあります。

幸いにも、PKIの専門家は、セキュリティを犠牲にしない賢い改善策を生み出しました。このソリューションは、PKI証明書のコンテンツを減らして、小さい帯域幅と多数のIoTデバイスの単純な処理にも適合するようにしました。また、低出力デバイス用に鍵を生成したり、CSR生成システムを提供するソフトウェアベンダーもあります。

今後も、いくつかのデバイスでPKIの互換性に問題が発生するかもしれません。新しい製造工程では、デバイスメーカーが鍵を半導体製造時に実装できるため、サプライチェーンの早い段階でセキュリティが組み込まれます。半導体製造時の実装は、互換性の問題を解決するだけでなく、製造を迅速化しライフサイクルを通してデバイスのセキュリティとIDを強化します。

PKIは単なるWeb向けSSLでは？

数年間で、接続されたセキュリティについて多くの経験をしてきたのであれば、PKIをSecure Sockets Layer（SSL）保護として認識しているかもしれません。SSLは、最初に機能したバージョンがNetscape向け暗号プロトコルとして利用された1995年まで遡れます。1999年に、SSLは同類の後継であるTransport Layer Security（TLS）に引き継がれました。今も、TLSは変わらずWebの信頼できる暗号プロトコルです。

TLS/SSLは、最も一般的なPKIの実装ですが、多数ある用途の1つに過ぎません。実は、PKIは様々な場所で、世界中で生まれたほとんどあらゆるタイプの顧客に信頼性をもって使用されています。実際に、今のPKIは、四半世紀前にNetscapeチームがSSLを発表したときには想像もしていなかったあらゆる種類のモノを保護しています。

あらゆる点で信頼性を証明

PKIソリューションを構築するエンジニアやセキュリティの専門家でさえ、人々がPKIを使用して、自分が発明したものを安全にする創造的な方法に驚かされることがよくあります。一見異種の技術や無関係な業界が織りなす糸のように、PKIは最も驚くべき場所で目にすることができます。しかし、どのような用途であっても、それぞれのケースの中心にあるのは、1つのこと、つまり妥協のない信頼の必要性です。

ケーススタディ1

AeroMACS

リスクが大きいときの信頼性

今日、ある民間ジェット機のパイロットは、宇宙飛行士YoungとCrippenが1981年にスペースシャトルの新しいミッション中に**Columbia**を軌道からそらすために使用したよりも多くの接続されたセンサデータにアクセスしています。

しかし、40年前のシャトルでは人的要因が重要であったように、今でも重要です。操縦桿を握っている人には、巨大な機械を地上に安全に着陸させるために、できる限り正確な情報が必要です。

飛行機旅行中の事故の大半は、離陸直後と着陸直前に発生しています。このことから、飛行機は、60トンの金属、燃料、手荷物、乗客を空に誘導する複雑な動作に影響を与える人間と自然の力に対して最も脆弱と言えます。ウィンド・シアー（風の急変）、タイミングのミス、視界の喪失などがその例です。

離陸から最終着地の間、飛行機のパイロットはセンサーから収集したコックピットの計器情報や管制官から伝えられる極めて重要な情報を使用して、安全な飛行のために必要な調整を行います。2016年以降、重要な情報は、PKIで保護された飛行機のIoTセンサーによって、世界中の管制塔と飛行機に送られています。

飛行中の事故の大半は、離陸直後と着陸直前に発生しています。このことから、飛行機は、60トンの金属、燃料、手荷物、乗客を空に誘導する複雑な動作に影響を与える人間と自然の力に対して最も脆弱と言えます。

2016年以降、重要な情報はPKIで保護された飛行機のIoTセンサーによって、世界中の管制塔と飛行機に送られています。

最少で最大を成す

上空を行き交う飛行機の数は、2025年までに倍増する見通しです。もっと多くの飛行機、もっと多くのフライトが見込まれます。事実、北京首都国際空港では、2017年から2018年までに乗客数が5%増加しました。また、米国のダラスラブフィールド空港では、2010年から2020年の間に乗客数が90%増加しています。

AeroMACSは、IoTセンサーの情報を空港から管制塔と航空機に送信するブロードバンド大容量無線データリンクです。

世界中で新しい空港が建設されていますが、過剰なフライトを処理している既存の空港にとって唯一のソリューションは、航空交通調整の効率を高め、着陸と離陸の完全性を確保することです。

AeroMACSとは？

AeroMACS（Aeronautical Mobile Aviation Communication System）は、IoTセンサーの情報を空港から管制塔と航空機に送信するブロードバンド大容量無線データリンクです。温度計や風速計からフライト情報表示システム、さらには手荷物処理（空港の一部機能である場合）まで、デバイスデータはAeroMACSを介して通信されます。

AeroMACSは単なるウィジェットではありません。地上の目となり耳となります。フライトプランとスケジュールの調整には不可欠です。まさに空港運営の要です。万が一侵害されれば、AeroMACSを使用して飛行機やパイロットに誤った情報が送られる可能性があります。多くのフライトとそれ以上に多くの乗客のことを考えると、AeroMACS情報の改ざんを防止することは、飛行機が確実に離陸し、飛行して、安全に着陸するために極めて重要です。

離陸前チェックリストにPKIを追加する

複雑なエコシステムを使用している業界では、ネットワーク化している部品が多く、デバイスの能力とデバイスタイプ間の差異に制限がある

ので、適応性と信頼性を備えたセキュリティソリューションが必要です。飛行機の場合、これらすべての要因が関与しますが、データの機密性も重要です。致命的な改ざんを回避するために、デバイス自体を保護するのと同時に、地上と飛行機の間で通信される情報も保護する必要があります。

PKIによりこれらのデバイスとそこで通信される情報を保護することで、パイロットと管制塔は安全かつ安心して様々な情報を収集し、通信し、使用することができ、飛行機や空港を問わず安全な離着陸が保証されます。AeroMACSを使用した場合、米国の小規模な空港でも、オーストラリアの大空港と同様に確実に機能します。

実装：世界的規模

PKIソリューションは、航空通信の基準であり、近いうちに世界中のすべての空港で使用されることになるAeroMACSネットワークを保護します。

主なニーズ：信頼

上空には常に数千の航空機が飛行している中で、空港、航空会社、およびパイロットは、毎日数百万人に対して安全で時間通りの旅行を保証するためにAeroMACSに頼っています。

オーストラリアのGATEKEEPER

政府の信頼を得て市民を護る

ほとんどのオーストラリア人は、彼らの情報と重要な通信の内容を保護しているセキュリティおよびIDソリューションの存在には気づいていないでしょう。最近オーストラリアで家を購入すると、Gatekeeperを使用することになります。商品を輸入する際にも、Gatekeeperが使用されます。

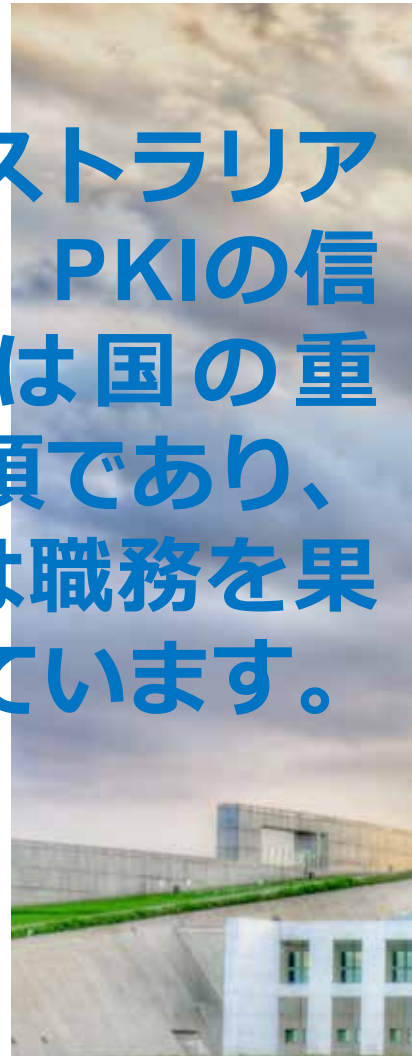
Gatekeeper PKIフレームワークは、20年以上経った今、「オーストラリア政府がデジタルキーと証明書を使用して認証サービスの加入者のIDを確認する方法を管理することに使われています。」重要な法律文書から契約書まで、国境警備から銀行業務まで、最も機密性の高い公共の信頼領域のほとんどは暗号化され、PKIソリューションで認証されます。

国全体を護る

前世紀末にオーストラリア政府は、ますます増加するデジタル文書とデジタル取引で入力される情報を保護するのに信頼できる手法を探し始めました。最初は、個々の機関が独自に開発したソリューションを実装していましたが、直ぐにセキュリティを内部で高レベルに管理することは困難で、時間も掛かりリスクが大きいと気づきました。

その結果、フレームワーク担当者は、エコシステムの管理に必要な時間とリソースを最小限に抑えながら、国全体を保護するニーズに対応できるソリューションを定義しました。現在、Gatekeeperフレームワークは、「政府機関とその顧客間の整合性、相互運用性、信頼と信用を提供しています。」

オーストラリアでは、PKIの信頼性は国の重要事項であり、PKIは職務を果たしています。



見えないときでも常にオン

私たちの生活に大きな影響を与えるにも関わらず目に見えないのがテクノロジーです。電力系統、ウォーターポンプシステム、銀行ネットワーク、このような陰のシステムでは、信頼性が重要なのは当たり前だと思っています。オーストラリア人にとって、Gatekeeperは信頼されなければならないシステムの1つです。効率性と利便性を高めるだけでなく、多くの重要な政府機能の中枢です。PKIが提供する堅牢なセキュリティがなければ、何百万人ものオーストラリア人の個人情報は盗難のリスクに晒され、重要な取引や法的手続きが遅延または中断され、税関と投資を管理する政府機関は情報漏洩にあう危険性があります。オーストラリアでは、PKIの信頼性は国の重要事項であり、PKIはその責を果たしています。

いつでも絶えず機能している必要があります。

実装：オーストラリア

複数の政府機関で実行され、最も機密性の高い公共の信頼領域のほとんどを保護する、全国規模のセキュリティおよびIDソリューションです。

主なニーズ：完全性

銀行業務から土地所有権、国境警備まで、停止や侵害は許されません。いつでも絶えず機能している必要があります。

ケーススタディ3

世界規模の輸送

世界的な信頼

海を越えて大陸間で或る港から別の港へと輸送されている数百万の輸送用コンテナの1つがどこにあるか特定するとします。今度は1つの輸送用コンテナの場所をデータベースと貨物記録を使用して特定してみます。

国際的なサプライチェーンは複雑な時計のようなもので、機械を機能させるには、個々の歯、バネ、ホイールが適切な場所にあり、意図したとおりに動く必要があります。出荷の遅延は輸送網全体を減速させます。貨物の紛失は輸送網を崩壊させ、資材と利益の両方を失うことになり、企業に損害を与えます。

毎年110億トンを越える商品が船で輸送されます。今日も、世界中に50,000隻以上のコンテナ船が存在しています。

デジタルの見通し

毎年110億トン以上の商品が船で輸送されます。今日も、世界中に50,000隻以上のコンテナ船が存在しています。海洋交易の規模は巨大であり、活動的でもあります。動きは一定で、貨物船は星空の地図のように地球上に点在しています。

海上に多くの船が存在しているということは、さらに多くのコンテナが存在しています。これらのコンテナの位置を個々にリアルタイムで安全に特定して追跡することは大仕事です。

この規模の船舶輸送における課題は資産を追跡するクラウド上のデータと現場のデバイスデータを相互認証することです。万が一侵害されれば、海運会社はコンテナの位置を見失ったり、コンテナについて間違った情報が会社に送信される恐れがあります。有効な対策としては、セキュリティソリューションでデバイスだけでなく、送信される情報も保護できる必要があります。さらに、スケーラブルで、一度に数万のデバイスを確実に保護する能力も必要です。

世界中のどの航路のどこにいても

PKI認証を使用すると、輸送用コンテナは出港から仕向港までの全航路を通して確実に追跡されます。さらに、出荷側には、毎年より多くのデバイスを製造し、より多くの貨物を確保するというニーズがあるため、保証の量を増やす必要性は年々高まっています。PKIのスケーラビリティで供給は需要を満たします。

その結果、貨物の数に関わらず、データは保護され、コンテナは世界中のどこにあっても追跡されます。これにより盗難や紛失のリスクが低下し、港から港までの商品の効率的な輸送が保証されます。サプライチェーンは途切れることがなくなり、企業も消費者も低コストで商品がより安定して供給されるというメリットを享受できます。

実装：世界的規模

グローバルなサプライチェーンの本音は、関連する輸送用コンテナが地球上のどこにでも商品や資材を輸送することです。

主なニーズ：認証

単なる追跡ではなく、PKIソリューションはリアルタイムで安全な認証を実現し、企業が個々の輸送用コンテナに取り付けられたデバイスの位置を特定し確認できるようにします。

PKIを使用すると、輸送用コンテナは全航路を通して確実に追跡されます。

IBM

テクノロジーリーダーからの信頼

多くの場合、最大の課題に直面するのは最大手の企業です。事実、企業の規模が課題になることもあります。例えば、世界中の異なるオフィスで異なる役割で働いており、異なるオペレーティングシステムやアプリケーションを使用し、異なるデバイスで作業をしている個々の従業員を企業はどのように保護すればよいのでしょう？

IBMにとって、これは単なる知的訓練ではありません。現実の問題でした。そして、その問題は50万人の従業員に影響します。

すべて持ち込み可能

500,000人以上のユーザーの認証、ID、および安全。

ここでは、「フレキシブルとスケーラブル」という言葉は、単なる論理的な説明ではなく、実用的なPKIソリューションの現実的な機能である必要があります。しかし、従業員の数が課題であると同時に、それらの従業員が実行し、仕事に持ち込むデバイスやアプリケーションの種類の数も、それ以上とは言わないまでも、同様の課題を突きつけてきます。会社所有のラップトップ、個人のスマートフォン、古いiPad、従業員・ベンダー・契約業者が最も働きやすいデバイスを使用させる柔軟性を提供する一方で、ネットワークに脆弱性を持ち込みたくない場合は、適応力もあり、堅牢でもあるセキュリティソリューションが必要です。

PKIはフレキシブルなだけでなく、スケーラブルでもあります。つまり、PKIは無数のデバイスの認証を行うだけでなく、その所有者や実行している内容を問わず、数百、数千の従業員に関して、彼らがどこにいても複数のデバイスの認証を同時に行うことができます。500,000の従業員は、完全にシームレスにつながります。

信頼とは確実性

10年以上にわたり、PKI IDソリューションは、170カ国以上で途切れることなくサービスを提供しています。

信頼できるセキュリティに対するニーズがあれ

PKIはフレキシブルなだけでなく、スケーラブルでもあります。

ば、それだけ確実性に対するニーズもあります。この規模では、サービスとしてのソフトウェアの認証は、いつでもどこでも機能するほど十分に堅牢でなければなりません。1日24時間365日、世界中で数百・数千の従業員が利用デバイスを問わず、IBMネットワークへ安全にアクセスしています。安全かつシームレスなため、従業員は何も考える必要がなく企業は脆弱性について心配する必要がありません。

配備：世界的規模

世界中に存在する数千のオフィスでは、ハードウェアおよびソフトウェアの長年にわたる世界的リーダーとしてビジネスを行っています。

主なニーズ：フレキシビリティ

重要な業務をオンラインで行う際、PKIは世界中の50万人の従業員を認証、保護、特定するためのソリューションを提供します。

医療

命がかかっているときの信頼性

ほとんどの人は、ネットワーク化された機器のメリットを受けています。Bluetooth接続があれば、裏のテラスで現在の温度と湿度を確認できます。キッチンのiPadとリビングのスマートTVをWi-Fiで接続すれば、ディナーをオーブンに入れている間、続きのエピソードを視聴できます。ただネットワーク化は便利なものですが、不可欠なものとは限りません。しかし、場合によっては、接続は単にメリットや利便性を提供するだけではありません。一部の人にとって、接続は生死の問題です。

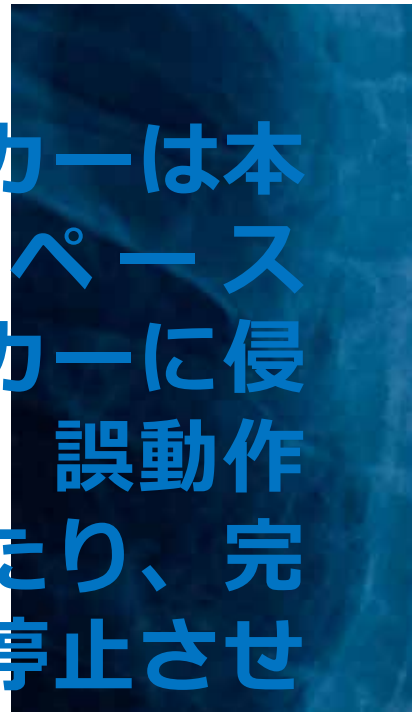
数年前、メディカルエンジニアが新しい形のペースメーカーを発表しました。この特別なモデルは「スマート」でした。ペースメーカーを外部モニタと患者の電話アプリにBluetoothで接続すると、心臓を動かしておくために必要な電気信号を送れるだけでなく、ペースメーカーがどのように機能しているかを患者と医師に伝えることができるのです。

ペースメーカーが正常に機能しているか。バッテリーの残量はどのくらいか。これまで、このような診断や治療には、来院や、ときには手術が必要でした。今では、すべて自動的に継続してモニタ、記録、通信ができるようになりました。

接続されたペースメーカーは単に便利なだけではありません。数千人が生命の維持をこのデバイスに頼っています。しかし、他の接続と同様に、障害も考えられます。他のIoTデバイスと同様に、接続されたペースメーカーには、安全なエンドツーエンドの暗号化が必要です。

文字どおりの「死活問題」

2017年8月、少なくともIoTの世界に関わっていない人にとっては異常な見出し[8]のニュースが報じられました。アメリカ食品医薬品局（FDA）がサイバーセキュリティに対する脅威から、多数のペースメーカーをリコールしたのです。インターネットハッキングのリスクに関する他の話のように、FDAは、特定のペースメーカーに「サイバーセキュリティを利用した侵入と悪用に対する脆弱性」が考えられると警告しました。



ハッカーは本当にペースメーカーに侵入し、誤動作させたり、完全に停止させたりできるのでしょうか？できるのです。

[8] https://thehealthcareblog.com/blog/2019/07/29/security-crisis-of-cardiac-pacemakers-paves-the-way-for-iot-security-evolution-in-cardiology/

それは、SF映画の筋書きのようにも思えるとんでもないものでした。ハッカーは本当にペースメーカーに侵入し、誤動作させたり、完全に停止させたりできるのでしょうか？できるのです。

医療機器メーカーが、病院用スマートベッドから持続血糖モニターまで、患者ケアツールをネットワーク化し斬新で価値のある方法を発明したことで、患者の利便性が向上しました。それと同時に、接続されたデバイスによって収集された患者データの保護に関する懸念、さらには、デバイスの故障につながる侵入に関する懸念も高まりました。

実際に、ハッカーはペースメーカーでまさにこのような侵入ポイントを見つけました。メーカーは、ペースメーカーとベッドサイドモニタ間の通信を暗号化しましたが、モニタそのものは保護されていませんでした。ハッカーは、モニタにアクセスしてペースメーカーに繰り返しコマンドを送り、バッテリーを消耗させることができました。さらに悪いことに、患者にショックを与えるようにペースメーカーに指示することができました。デバイスだけでなく、患者の安全も守るための手段を探す中で、多くのメーカーがPKIに注目しました。

医療機器におけるPKIのメリットは、強力な暗号化を担ってきた長い歴史と、組み込みIDにあります。

デバイスと患者データの整合性を守り、命がかかっているときに十分信頼できるセキュリティソリューション

医療機器はより小型化され、より高性能になりますが、患者のデータと生命を継続的に保護するセキュリティソリューションはPKIです。

PKIは、デバイスデータの保護だけでなく、暗号化IDを使用したデバイスの認証も簡単にします。つまり、デバイスは製造時に保護する機能を与えられ、そのセキュリティは病院で処置され患者に引き渡されます。デバイス自体がライフサイクルの様々なフェーズを移動していき、デバイスのセキュリティを監視する人が変わっても、セキュリティはそのまま維持され、生涯中断されることはありません。

医療機器は将来さらに高性能に

最近、より小型でより高性能なデバイスの研究開発のために新たな資金調達および認可申請が行われています。現在、リードレスペースメーカーは実際に使用されています。大腿静脈カテーテルで挿入できるほど小型で、心臓内に直接埋め込まれるため、侵襲的外科手術や何百万回、何十億回もの鼓動で心臓組織が収縮することにより摩耗する可能性がある電気リードが不要になります。

これに続くペースメーカーもリードレスで、さらに高性能になります。小型の除細動器に接続されデバイスの稼働状況だけでなく、心臓の健康状態も監視して、心不全になった場合、ショックを与えるようにBluetoothで除細動器に伝えることができます。患者の心臓専門医にデータを送信すれば、手術せずにリアルタイムで調整することができるため、自宅にいながら処置なしで患者の心臓を健全にすることができます。

今日、簡単で安全な監視システムが守ってくれていることで、ペースメーカーが継続的に機能し潜在的な問題があれば警告されることを知って、何千という人が心の平安を享受しています。近い将来、循環器検査の能力が向上すれば、より多くの患者とその医師に、より有用なデータと手術や来院が不要な緊急支援に関してより多くの選択肢が提供されます。医療機器はより小型化され、より高性能になりますが、患者のデータと生命を継続的に保護するセキュリティソリューションはPKIになるでしょう。

実装：世界中の複数の国々

何千もの病院や医療センター、数百万の人々が、異なる順守基準と実施基準を越えてプロバイダーと患者が同様に使用します。

主なニーズ：信頼性

デバイスと患者データの整合性を守り、命がかかっているときに十分信頼できるセキュリティソリューション。

第3章

知らないと傷つくことがある

確かにPKIは信頼されています。それも数十年にわたっています。しかし、その信頼は一部の専門家に頼っています。つまり、PKIソリューションが正しく実装されなければ、その脆弱性は保護されていないシステムと同じくらい大きなリスクを引き起こす可能性があります。

PKIは長い間存在しているため、エンジニアとコンピュータ科学者は、これが実際にどのように機能するかを長年にわたり研究してきました。高度で革新的な実装例もあれば、本来ならほぼ完璧なシステムになるはずが、設計ミスや間違った運用で試みが失敗した例もあります。

PKIが実装されるたびに、もう一度その動作を確認できる機会が生まれます。特に新しい環境に実装する場合や新しい技術と組み合わせた場合は良い機会です。さらに、何かがうまくいくたびにPKIエンジニアはこの技術を使用する、より高度で安全な方法を学んでいます。

セキュリティの専門家が今PKIについて知っているいくつかのこと

適切な鍵の保護

PKIの善し悪しは、証明書チェーンの署名に使用される秘密鍵によって決まります。一般的に、これはルート認証局と発行認証局（ICA）用の鍵です。これらの鍵のいずれか、または両方が安全でない方法で生成または保管されている場合、発行されるPKI証明書はあまり信用できません。企業でこのようなことが起きる例としては、IT管理者がインターネットからダウンロードしたソフトウェアを利用して管理サーバ上で読み取り可能なテキストの鍵を作成し、それらの鍵をネットワーク上で稼働している自社の認証局に転送することでバックアップが存在する場合です。この場合、保護されていなかった鍵は簡単に盗まれる可能性があるため、PKIシステムは極めて危険です。PKI階層全体の信頼性を確保できるのは、適切な保護しかありません。

証明書ステータス

PKIシステムは、証明書が有効で使用可能かどうかをデバイスまたはブラウザが判断するための手段を提供する必要があります。PKIが正しく実装されていないと、階層で取り消しに必要な情報が見つからない、あるいは情報が完全に失われることがよくあります。場合によっては、情報が存在し、正しくても、システムがリクエストを適切に管理していないこともあります。原因は何であれ、結果としてシステムは信用できなくなります。

間違った構成

システムの適切なセットアップに加え、証明書または証明書チェーン内の構成には、多くの場合PKIがソフトウェアとハードウェアを保護するために特別な構成が必要になります。「自己署名証明書」実装の場合、1つのインスタンスの問題を解決する一方で、証明書をバイパス、なりすまし、悪用などの他のリスクに晒したままにするような次善策としての構成をよく見かけます。

確かにPKIは信頼されています。それも数十年にわたっています。しかし、その信頼は一部の専門家に頼っています。

PKI暗号化のセットアップ時に回避すべき4つのミス

将来の計画なしに同じことを繰り返す

セキュリティ担当者が自社用に社内で開発したPKIソリューションを準備するときに、時間の経過とともに起こる変化を見落とすことはよくあります。企業の成長、ビジネス目標の変化、新製品または新チームの出現などに際して、PKIソリューションに適応性がなかったり、新しい配備に対応できない構成であった場合、使用できなくなり最悪の場合重荷になります。

PKIエコシステムを社内で管理しようとする

PKIの信頼性の簡便さは、落とし穴になる可能性があります。確かに、フレキシブルでスケーラブル、高速で信頼できるのがPKIですが、それは適切に統合され、実装された場合に限られます。社内で構築されたソリューションは、扱いにくく、リソース消費量の多いセキュリティ対策になりがちです。専門家によって導入され、効果的に監視されていなければ、PKIが実装されている場所、PKIの状態、過失や欠落のある場所を追跡することが困難になります。管理されたPKIと集中管理されたプラットフォームがこれらの問題を解決し、監視に不要な時間を費やす必要性をなくして、セキュリティ障害、鍵の紛失、ユーザーのミスによる障害を解消します。

コンプライアンスを遵守せずにPKIを構築する

PKIの特徴の1つであり、最大のメリットでもあるのは、柔軟な実装オプションです。オンプレミスからクラウドまで、多数のモデルがあります。自社のビジネス、セキュリティ、およびユーザーのニーズに最適なオプションを判断するだけでなく、地方、地域、または国の規制を遵守した上でセキュリティを提供できるオプションを特定することも重要です。さらに、PKIソリューションが企業および業界向けのより大規模なセキュリティ戦略にどのように適合するかを理解することも重要です。

来るべきPQC革命への備えを怠っている

量子コンピューターは、サイエンスフィクションから新しい現実のテクノロジーへと急速に移行しています。量子コンピューターには、メリットと同時に危険性を含んでいます。しかし、量子コンピュータを使用して数学的に不可能なコードを解くことの限界はまだ解明されていません。セキュリティの専門家が犯す可能性のある間違いの1つは、潜在的な脅威に備えて環境を整えることなく、量子コンピューターの出現を待つことです。システムを保護するための基盤を耐量子コンピューター暗号の世界に置いているソリューションはすでに存在しており、経験豊富なセキュリティ担当者は、量子コンピューターが日常の新しい現実になった後、資産を保護するシステムについて学び、テストすることの重要性を認識しています。

分かっていることを見直す。これが最新のPKI

信頼性に定評のある数十年前のテクノロジーは、どうすればもう一度新しくなるでしょう。答えはテクノロジーの変化ではなく、世界がテクノロジーを使用する方法の変化にあります。

PKIは役に立ちます。Netscapeと33.6kのモデムの頃から、セキュリティとIDのための信頼できるソリューションであることが証明されています。コンピューティングの世界の他の部分の変更に合わせて、プロトコルの更新や若干の修正が行われてきましたが、今日のPKIは過去のPKIと基本的には変わっていません。

1996年、PKIに携わる人々はExciteでの検索結果を保護し、eBayで安全に買い物をすることを考えていました。大体において、多くの人々は、今日でもPKIについて考えるときは、同じように考えています。しかし、ほとんどの人は、最新のPKIが列車を衝突から守り、ハッカーがスマートウォッチから個人情報を盗むのを阻止して人々を保護していることに気づいていません。一方で、引き続きeBayの暗号化もしています。

PKIは、テクノロジーの進化と共に進化してきました。そして、家庭内だけでなく、世界中のあらゆるタイプの業界、企業、政府のセキュリティのニーズを満たすように拡張されています。最終的に、緊急救助ビーコンにおけるPKIの役割は、毎日何百万人もの人々がオンラインバンキング取引をし、誰もデビットカード番号を盗まれないことをPKIが保証しているという事実に勝るとも劣らないかもしれません。どちらの場合も、その信頼性の重要さは軽視できません。PKIは、実証済みのテクノロジーとソリューションの絶妙な組み合わせで、今日の発明と明日の考案にセキュリティとIDを提供します。次に何が来るとしても、PKIは実証された柔軟性のある信頼を提供し続けます。

今のPKIは、テクノロジーの進化と共に進化してきました。そして、世界中のあらゆるタイプの業界、企業、政府のセキュリティのニーズを満たすように拡張されています。

革新的な方法でPKIを使用している人をご存知ですか？ぜひ紹介してください。DigiCert PKIソリューションに興味をお持ちですか？いつでもご相談をお受けします。www.digicert.com/jp/のお問い合わせフォームよりお問い合わせください。

DigiCertについて

より良い方法は誰かがそれを見つけることで初めて一般的な習慣になります。

DigiCertでは創業以来、インターネットのセキュリティを確保するより良い方法の構築をひたむきに追求しています。これが、弊社のTLS/SSLサーバ証明書がフォーチュン500企業の89%、世界の銀行トップ100行のうち97行、世界のeコマース企業の81%により、あらゆる場所で、毎日、何百万回も信頼されている理由です。また、業界最高水準のサービスとサポートを提供する企業として、お客様から常に変わることなくDigiCertが評価されている所以でもあります。だからこそ、弊社では、企業や政府によるID、アクセス、サーバ、ネットワーク、Eメール、コード、署名、文書、IoTデバイスのセキュリティ確保に有効なDigiCert ONEプラットフォームと管理ツールを構築することで、PKIの最新化を進めています。DigiCertは、SSL、IoT、PKIなどの分野において、競合他社とは一線を画す独自性を誇っています。