eBook

digicert®

ブランド、顧客、評判を守る10の方法

digicert®

暗号化がセキュリティの骨格だとしたら、アイデンティティはセキュリティの心臓、すなわち企業のデジタルブランドを陰で支える人としての価値です。1990年代にeコマースが始まって以来、信頼できる本人を現すアイデンティティが偽りの無いビジネスを支えてきました。

しかし昨今、悪意のあるWebサイトが暗号化を悪用しています。広く行き渡っている匿名性はビジネスアイデンティティを脅かし、企業は被害を被ったままになっています。さらに、ネットワーク上のユーザー、アプリケーションおよびデバイスのアイデンティティ検証が行われないと、ハッカーにとって侵入しやすくなり、企業が悪い意味でニュースに取り上げられる恐れがあります。

本書では、企業がビジネスアイデンティティを立証し、自社のWebサイトの正当性を証明し、ネットワークアクセスを保護して、顧客の信頼を築くためにできることについて説明します。

なぜなら、ビジネスアイデンティティを立証し、企業とその顧客双方の情報を守ることで、
自信を持ってやり取りできるようになるからです。

お客様を安心させるのは貴社です。

目次

2019年のサイバースパイの78%にフィッシングが関わっています。

2019年、Verizon Data Breach Investigations Report

* https://www.nextgov.com/cybersecurity/2019/05/cyber-espionage-targeting-public-sector-rose-168-2018/156849/

digicert®

お客様を安心させるのは貴社です

1. アイデンティティを立証するTLS/SSL証明書の使用

1.1 DV/OV/EV

ドメイン認証（DV）証明書は、暗号化は行いますが、企業のアイデンティティ立証に関してそれ以上のことはできません。実際に、多くのサイバー犯罪者はDV証明書を使用してオフィシャルWebサイトになりすましています。

偽装されたビジネスアイデンティティが最終的に被害を受けます。そのため企業は、より多くの審査が必要な高い認証水準の証明書を使用することでブランドを保護する必要があります。

企業認証（OV）とEV（Extended Validation）で貴社のアイデンティティを立証することにより、顧客の視点で正当性を証明することになります。これら高い認証水準のTLS証明書は、公開される前に企業を厳しくチェックし、さらなる保証を提供します。例えば、企業名と所在地を表示して、顧客が貴社のWebサイトが本物であると確信できるようにします。

EV証明書は、実績がある信頼済みの認証方法を使用して、OVおよびDV証明書を超える強力なアイデンティティ保証、ブランド保護、およびユーザー保護を提供します。EV要件は、証明書が認証済みの貴社の責任者によって貴社のブランドに対してのみ発行されたことを保証するだけでなく、申請した人物と企業の実在性をしっかり検証することで、詐欺行為を防止し、顧客が安心して取引できるようにします。

金融やeコマースを始めとする多くの業界で、EVはセキュリティのベストプラクティスとして、業界のトップ企業や監督機関によって推奨されています。調査によるとDVやOV証明書と比べて、EV証明書にはフィッシングの問題がほとんどないことが分かっています[1]。

高い認証水準の証明書は、包括的なWebサイトセキュリティと、アイデンティティをターゲットにした攻撃に対する強力な防御を提供するだけでなく、顧客に貴社が本物であることを保証します。

[1] Certified Phishing: Taking a Look at Public Key Certificates of Phishing Websites.（RWTH Aachen University、Computer Science部門、Vincent Drury氏およびUlrike Meyer氏）

* https://info.phishlabs.com/blog/more-than-half-of-phishing-sites-use-https

1. アイデンティティを立証するTLS/SSL証明書の使用

1.2 追加のアイデンティティ保護と金融部門に対する信頼

欧州連合（EU）のオンライン金融市場における信頼レベルのばらつきを解消するために、PSP（決済サービスプロバイダー）に対してeIDAS（Electronic Identification and Trust Services Regulation）が導入されました。

eIDASは、市場を標準化し、保護することで形式的な手続きを減らします。適格証明書には、QWAC（ウェブサイト認証の為の適格証明書）とQsealC（適格eシール証明書）の2つがあります。

QWACでは、機密性の高い決済データを暗号化し、保護すると同時に、Webサイトから顧客に対して貴社のアイデンティティを立証することができます。QWAC用の認証方法は、EVよりもさらに厳格で証明書に記載された企業の正当な代表者との対面による検証が求められます。

QsealCは、データ、機密性の高いドキュメント、およびその他の通信を「密封」し、不正開封を防止すると共に、信頼できるソースから来ていることを保証して、アプリケーションとドキュメントを保護します。

PSP規制は、該当地域によって異なりますが、EUではPSD2（欧州決済サービス指令第2版）が施行された2019年9月に、これらの証明書がPSPに義務付けられました。

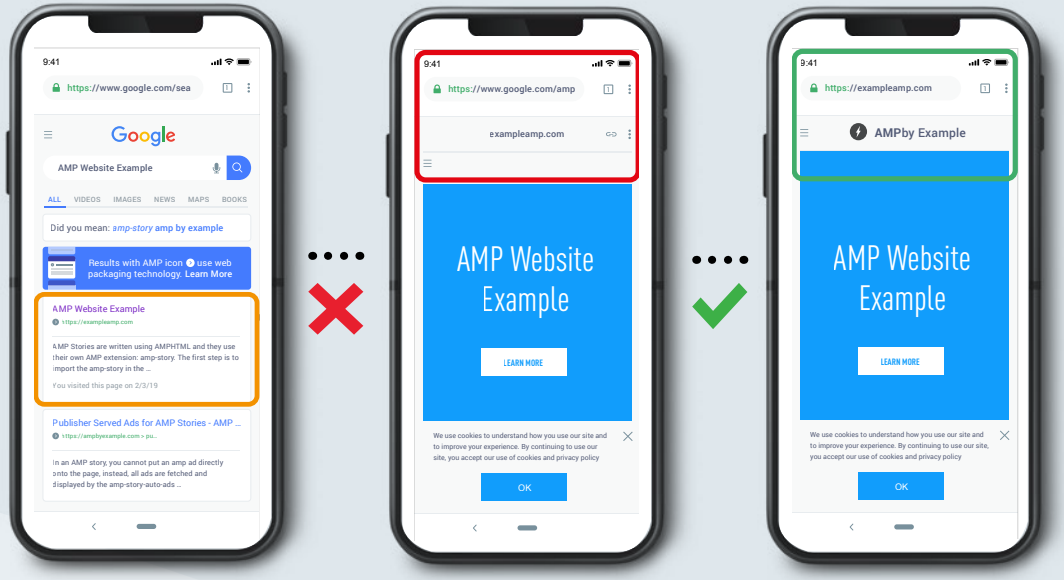
当社の高い認証水準の証明書と適格eシール証明書でこのプロセスを保護することで、顧客の情報が安全に貴社だけに届くことが明確かつ簡単に伝わります。

1. アイデンティティを立証するTLS/SSL証明書の使用

1.3 SXG（Signed HTTP Exchange）証明書

大量のWebコンテンツがモバイルデバイスで閲覧されることがビジネスにとって重要である場合、ロード時間を短縮するためにGoogle AMPを活用しているでしょう。しかし、Google AMPでは、AMPがホストするWebページがGoogleの所有サイトに見えるため、顧客が混乱し、ブランドエクスペリ認知に悪影響が及ぶ可能性があります。

DigiCert® SXG証明書は、これを是正し、URLに企業名が正しく表示されるようにすると同時に、キャッシュされたコンテンツのロード時間を短縮し、Webページに想定したセキュリティ水準を維持します。



DigiCert SXG証明書がないと、貴社のブランドとコンテンツは、Google所有サイトのように見えます。

DigiCert SXG証明書を使用すると、ドメインとコンテンツに貴社のURLとブランドが表示されます。

2. どこでもアイデンティティを明示：コードへの署名、文書への署名、安全なEメールを送信

企業は、自社が送信するEメール、ドキュメント、およびアプリケーションによって識別されます。サイバー犯罪者の多くは、この種のメッセージを傍受し、マルウェアを埋め込んで、受信者がサイバー犯罪者に代わって無意識のうちにマルウェアを拡散するようにします。貴社がターゲットになった場合、マルウェアの根源として認識され、それによって評判を損ない、経済的な損失を被る可能性があります。

コードやアプリケーションへの署名、ドキュメントやEメールに電子証明書を導入することで、顧客やパートナーが受け取るメッセージの信頼性を保証することができます。メッセージが危険にさらされた場合、受信者は警告を受け、そのメッセージは貴社のものでないことがわかります。これによりマルウェアの拡散に貴社のアイデンティティが悪用されるのを防止します。

DigiCert Enterprise PKI (Public Key Infrastructure) Manager™は、Eメール通信と文書への電子署名の両方のセキュリティを簡素化します。柔軟な証明書プロファイル構成と登録方法を使用して、ビジネスに求められる保護体制を素早く導入し、実施できるようになります。さらに、ベースがDigiCert ONE™プラットフォームであるため、クラウド、オンプレミス、ハイブリッド、さらに国内外を問わず、独自のやり方で管理できます。

2017年には、企業の76%がフィッシング攻撃の被害を受けました。*

2017年、Wombat Security社

01100011
01101111
01100100
01100101

* https://www.wombatsecurity.com/news/76-organizations-report-being-victims-phishing-attacks

3. 全IoTデバイスのアイデンティティの確立

2025年までに、推定754億4000万個のコネクテッドデバイスが登場すると予想されています[3]。企業がIoTを採用する上で、セキュリティは最大の関心事の1つです。実際に、サイバー犯罪者はすでにIoTデバイスをターゲットにしています。

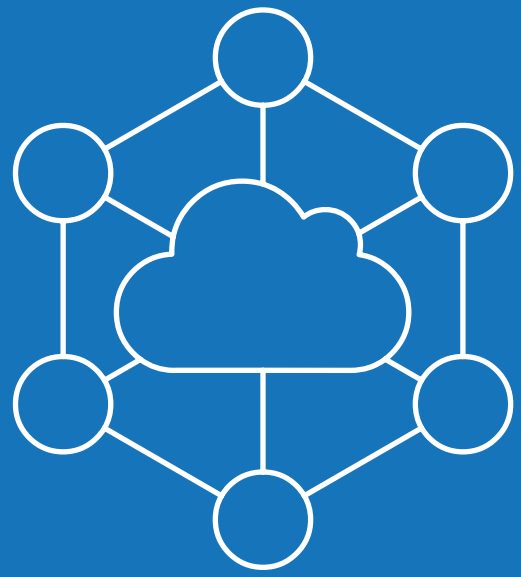
例えば、防犯カメラもその1つです[4]。

PKIと電子証明書を導入することで、メーカーはIoTデバイス用のデバイスアイデンティティを確立できます。これによって、メーカーは自社のデバイスを追跡し、必要に応じてシステムを更新して堅牢なセキュリティを維持することができます。さらに、特定の業界（自動車業界など）では、デバイス間の相互通信をメーカーが管理することもできます。未知または未承認のデバイスは接続を排除または制限され、サイバー攻撃のリスクを最小限に抑えます。

DigiCert IoT Device Manager™は、証明書ベースのアイデンティティをIoTデバイスに結びつけ、ネットワーク内の個々のデバイスに対して、暗号ベースのアイデンティティを割り当て、定義して、中央集約的に制御できるようにします。製造段階でデバイスアイデンティティを確立することで、別のセキュリティレイヤーを構築し、エンドユーザーのリスクを低減できます。

2020年のデータ漏洩の平均コストは1億5000万ドルを超えています*。

2019年、Juniper Research社



[3] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
[4] https://www.propertycasualty360.com/2019/12/19/protecting-iot-devices-from-cyberattacks/?slreturn=20191119173130
* https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion-by-2019

4. WEBサイトへトラストシールを掲載

決済のセキュリティに関する懸念は、常に顧客の頭から離れません。これは、サイバー犯罪の増加によってさらに悪化します。実際に、2017年にはすべてのショッピングカート放棄の約20%は、決済セキュリティの不安が原因でした[5]。そのため、購買フローにおいて、顧客に視覚的なアイデンティティをを示すことは極めて重要です。

トラストシールは常にオンラインの信頼を高める最も大きな要因の1つで、高い認証水準のTLS証明書の大きなな特長です。調査では、Webサイトにトラストシールを掲載したのちの離反率が18%減少しただけでなく、コンバージョンが19%上昇したことを示しています[6]。

すべてのデジサートの TLS証明書には、DigiCert Secured™シールが付属しています。デジサート セキュア・サーバID、グローバル・サーバIDには、DigiCert Secured™シールまたは Norton Powered by DigiCertシールが付属しています。これは、販売の最も重要な場面で、顧客にすぐに分かりやすい保証を与えます。さらに、慎重なユーザーは、サイトの信頼性をシングルクリックで確認することができます。

DigiCertのトラストシールは、最も信頼されるオンラインのマークとしてランク付けされました。*

2018年、Website Security Seal Study

[5] https://www.barilliance.com/10-reasons-shopping-cart-abandonment/

* https://www.digicert.com/site-seal-conversion-rate-benefits.htm

digicert®

意図しない発行と不正アクセスの防止

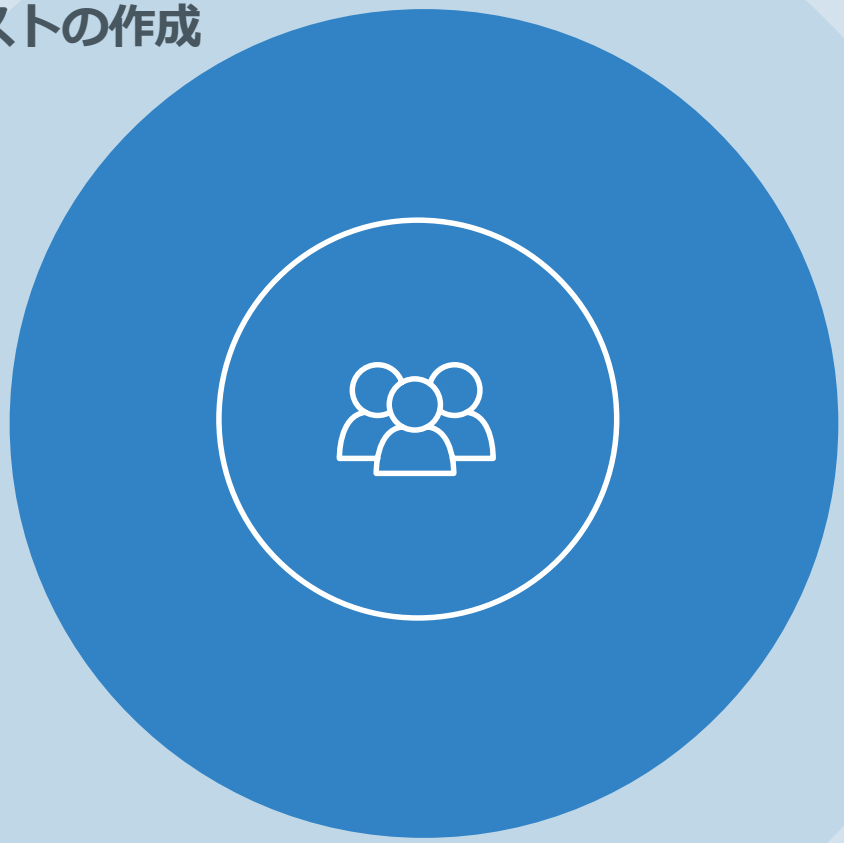
5. 意図しない証明書の発行を防止

5.1 Certificate Authority Authorization（CAA）リストの作成

企業の信頼できるアイデンティティを利用するために、内部か外部かを問わず悪意のあるハッカーは、合法ドメインの代わりにサードパーティーの認証局（CA）から信頼される証明書を獲得しようとします。この「不正な証明書」は、既知の機関によって企業の実名で発行されるため、エンドユーザーがその正当性に疑問を抱く余地はなく、攻撃者は基本的に、悪意のあるコンテンツを分かりやすいところに自由に隠すことができます。これは、特により大手の企業にとって危険です。なぜなら、誤って発行された1つの証明書が簡単に見過ごされる可能性があるからです。

ドメインオーナーがこのタイプの攻撃を回避するために、証明書を発行する前に、すべてのCAがドメインのCAAレコードのチェックを行うことが、2017年に義務付けられました。

CAAレコードは、ドメインオーナーによって定義された信頼できるCAの「ホワイトリスト」です。CAAレコードを常に厳しくコントロールし、厳格な認証基準を持つCAにのみ証明書の発行を許可することで、謝って発行された証明書を使用して、攻撃者が企業のアイデンティティを損なわないようすることができます。



5. 意図しない証明書の発行を防止

5.2 CT（Certificate Transparency）ログの監視

CTログは、発行済み証明書の公開リストで、企業が誤ってまたは不正に発行された証明書を迅速に特定できるようにします。

監視機能と併せて、証明書の透明性により、ドメイン向けに発行されたすべての証明書がドメインオーナーに見えるようになり、意図せず発行された証明書や不正な証明書を簡単に識別できるようにし、エンドユーザーを保護します。

CTログを常に監視し続けることで、明確な承認なしで、またはドメインポリシーの外で発行された承認されていない証明書を数日、数週間、または数ヶ月ではなく、わずか数分で検出できます。

CTログ監視を行わない場合、企業のセキュリティポリシー外部で、承認されていない、不正なCAから発行された証明書や間違ってインストールされた証明書が存在する可能性があります。それによって、企業の最も重要なドメインを危険にさらしているかもしれません。

6. ブラックリストのチェック

セキュリティに問題のあるドメインが1つでもあれば、顧客の信用を失うだけでなく、そのドメインがブラックリストに入れられる危険性があります。ブラックリストチェッカーが組み込まれた証明書管理ソリューションがあれば、証明書管理が簡単になるだけでなく、気づかないうちにドメインがブラウザによって信頼されなくなるようなことがなくなります。

毎月100万のフィッシングサイトが登場します。*

Webroot Quarterly Threat Trends, 2017

* https://www-cdn.webroot.com/8415/0585/3084/Webroot_Quarterly_Threat_Trends_September_2017.pdf

7. ユーザーとデバイスのアイデンティティを検証

企業内で、従業員、契約社員、およびパートナーはあらゆるタイプのデバイスを使用して、企業のネットワークとアプリケーションを介して機密情報にアクセスします。適切なユーザーまたはデバイス認証がないと、セキュリティ侵害が発生し、データや評判を失いかねません。

モバイル、VPNアクセス、およびスマートカードログイン用の公開鍵基盤（PKI）を導入することで、信頼できるユーザーとデバイスが承認された情報にのみアクセスできるようにすることができます。

管理の簡素化

8. ディスカバリーと自動化

証明書を管理する上で、ほとんどの企業が直面している最大の課題が可視性の欠如です。そのため、多くの企業は、自社のすべての証明書が有効であるか不明のままで運用し、ブランドを傷つけるような証明書関連の障害を引き起こす最大の要因の1つになっています。プロセス全体の管理を合理化する機能が求められています。

DigiCert CertCentral®は、ディスカバリー機能と自動化機能で、証明書ポートフォリオ全体の問題や脆弱性を瞬時に検出し、証明書分析ツールによって推奨されたアクションに基づいて問題を修正することで、ビジネスを支援します。稼働中の証明書全体を可視化して、問題のある証明書の即時制御を可能にします。

CertCentralでは、1つの画面からサイクルのあらゆる部分が見えるようにすることで、ACMEプロトコルを使用してOVおよびEV証明書のデプロイを自動化したり、 カスタマイズした有効期間を設定することもできます。

CertCentralは、証明書の発行、インストール、検査、再発行、そして更新などの作業を統合します。そのため、面倒な手作業に掛かる時間を短縮し、より多くの時間をブランド力を向上させる作業に集中させることができ、証明書が正しく管理されているという安心感も得られます。

* https://www.bbc.co.uk/news/business-46499366

9. IT部門の証明書管理を簡素化

多くの企業は、極めて複雑な証明書管理環境に依存しています。この不確実性が、機密資産を保護するために、益々多くの企業を安全性の実証されたPKIへと駆り立てています。

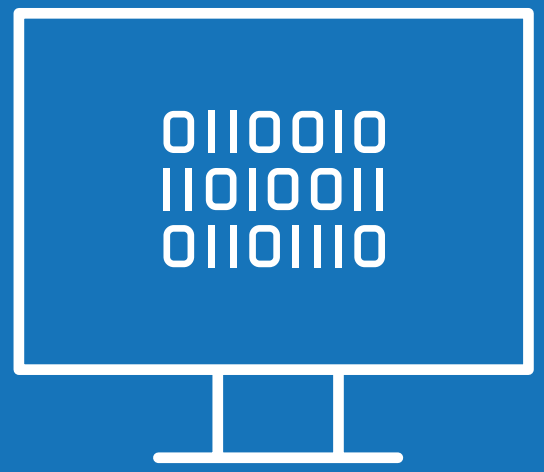
公開鍵基盤（PKI）は、企業にすべてのデジタル証明書と公開鍵を作成し、管理する機能を提供する一連のハードウェア、ソフトウェア、プロセス、およびポリシーを意味します。ところが、PKIは、設定するのも、あるいは単に導入するだけでも、困難で複雑な作業になる可能性があります。

しかし、最新のユビキタスインフラストラクチャを使用して、多くの企業が新しい統合技術を利用し始めています。PKIプラットフォームは、安全な通信で証明書のライフサイクル管理とエンドユーザーエクスペリエンスを容易にします。これは、既存のネットワークやビジネスアプリケーションとシームレスに統合され、データアクセスを大幅に向上させます。

DigiCert Enterprise PKI Managerは、DigiCert ONEに組み込まれており、中から大規模企業が堅牢な認証と暗号化を維持できるようにし、優れた性能、可用性、およびスケーラビリティでEメールとデジタル署名を保護します。

DigiCert ONEプラットフォームは、ビジネスまたは国内の要件に合わせて、オンプレミス、クラウド、またはハイブリッドの導入モデルを使用して、複雑さを低減し業界をリードする柔軟性を備えたPKIソリューションを提供します。

10. セキュリティをDevOpsとビジネスコミュニケーションにシームレスに統合



これまでの手順は、ビジネスアイデンティティを傷つけることになる脆弱性の一般的な対策となります。しかし、業界のコンプライアンス基準を満たし、強固なセキュリティ対策のベストプラクティスに取り組んでいる多くの企業は、一部のセキュリティ対策が製品の開発や全体の生産性を低下させる可能性に気づいています。

セキュリティを自動化し、DevOpsプロセスに統合することにより、ボタンを押すだけで開発中のコードまたはアプリケーションが継続的に保護されます。

DigiCert Secure App Service™（SAS）は、企業が安全で高性能なコード署名をDevOpsプロセス内に自動的に取り入れられるようにします。継続的インテグレーション/継続的デリバリー（CI/C）プラットフォームとDigiCert Cryptographic Service Provider™（CSP）の両方と簡単に統合できるため、自動化が可能になり費用効率が向上します。

鍵の管理機能、役割ベースのアクセス制御、監査ログによって、セキュリティ、制御、およびアカウンタビリティを強化します。一方で、ハッシュ署名は、大量の大容量ファイルへの署名を迅速に処理します。DigiCert Secure App Serviceにはこれらすべてが搭載されており、あらゆる規模の企業がコード署名の安全性とベストプラクティスを維持できるようにします。

お問い合わせ

TLS導入のベストプラクティスについては、当社のセキュリティ営業担当者までEメールでお問い合わせください。

websales_jp@digicert.com

企業ネットワーク全体を変えられるIoTおよびPKI管理ソリューションの詳細については、下記までお問い合わせください。

jpn-div-mpki@digicert.com