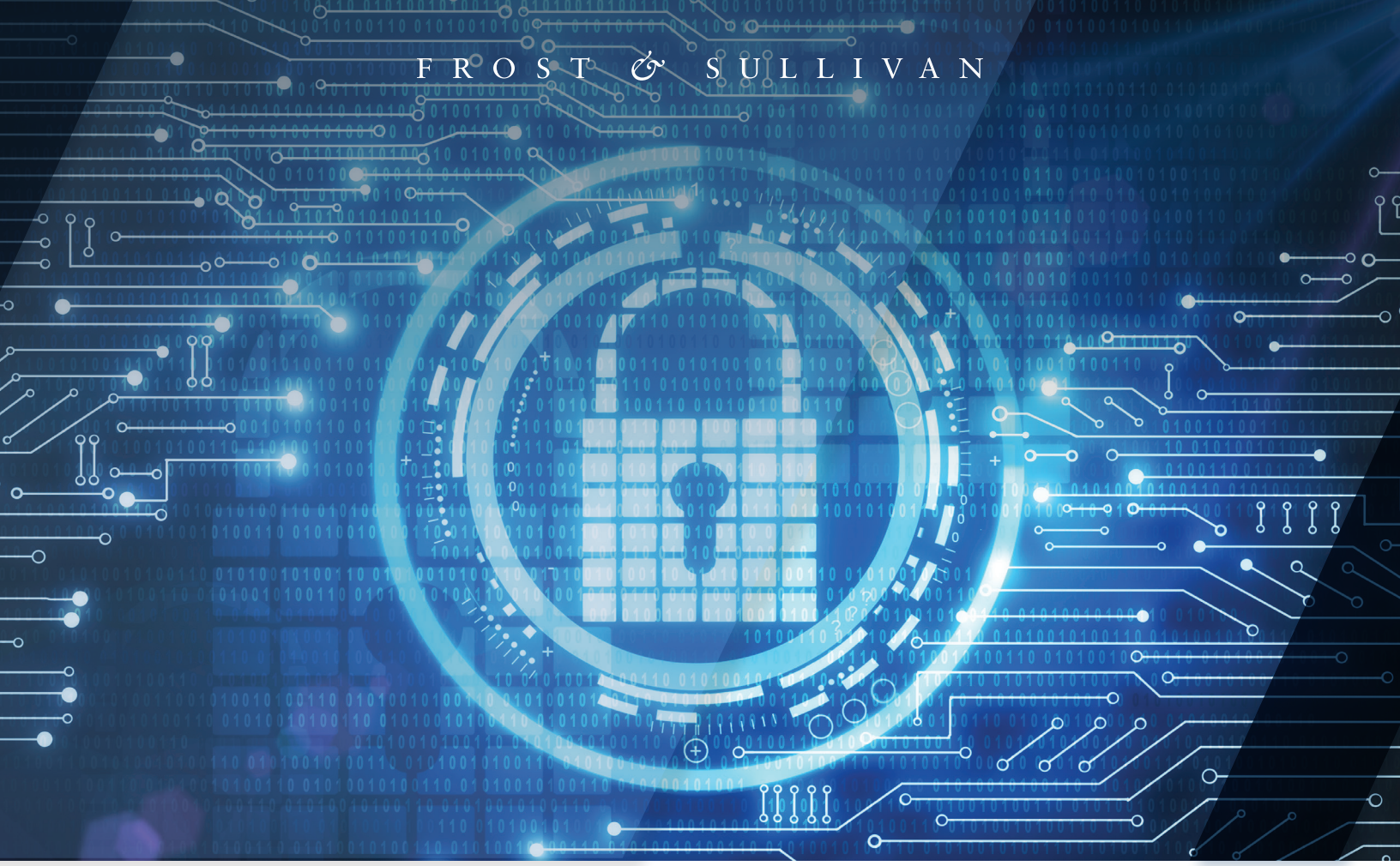
FROST & SULLIVAN



世界のTLS証明書認証局の市場

エンタープライズユーザのための主なインサイト

フロスト＆サリバン ホワイトペーパー

www.frost.com

Swetha Krishnamoorthi（サイバーセキュリティ、シニアインダストリーアナリスト）、**Jarad Carleton**（サイバーセキュリティ、プリンシパルアナリスト）

企業の成長とイノベーション、リーダーシップを支えて50年

はじめに. 3

TLS証明書の重要性 4

TLS証明書の主な機能 5

市場の状況 5

市場シェア分析 6

市場の見通し 9

おわりに. 10

はじめに

イギリスでは2017年に、総人口の3分の2にあたる約4,400万人が電子決済を利用しました[1]。アメリカでも電子決済は利用されています。オンラインでの購入額は4534億6000万ドルを記録しています[2]。これはeコマース業界にとっては嬉しいニュースである一方、毎日約617万件のデータが盗難の被害に遭っているのが現状です[3]。事業部門および情報セキュリティ担当者は、デジタル世界におけるB2BやB2Cの取引では、その最初の接点はWebサイトにあり、そしてそこで自社のセキュリティに対する姿勢が最初に示されるところであるということを、知っておく必要があります。フィッシングやなりすましなどのオンライン詐欺は増大傾向にあり、自社ブランドの評判への影響を懸念する世界中の企業が、セキュリティを深刻な課題と捉えています。また、セキュリティへの懸念から電子決済の利用に慎重になる消費者も増えており、信用が落ちれば企業にとってはさらなる痛手となります。

銀行の口座情報や個人情報などのデータを盗むサイバー犯罪においては、主に以下の2つの手口が使われます：

1. 電子メールまたはSMS（ショートメール）で信頼された主体になりすまし、利用者にリンクをクリックさせて偽のWebサイトへ誘導し、ログイン情報を盗むフィッシング詐欺
2. 中間者攻撃（MITM）

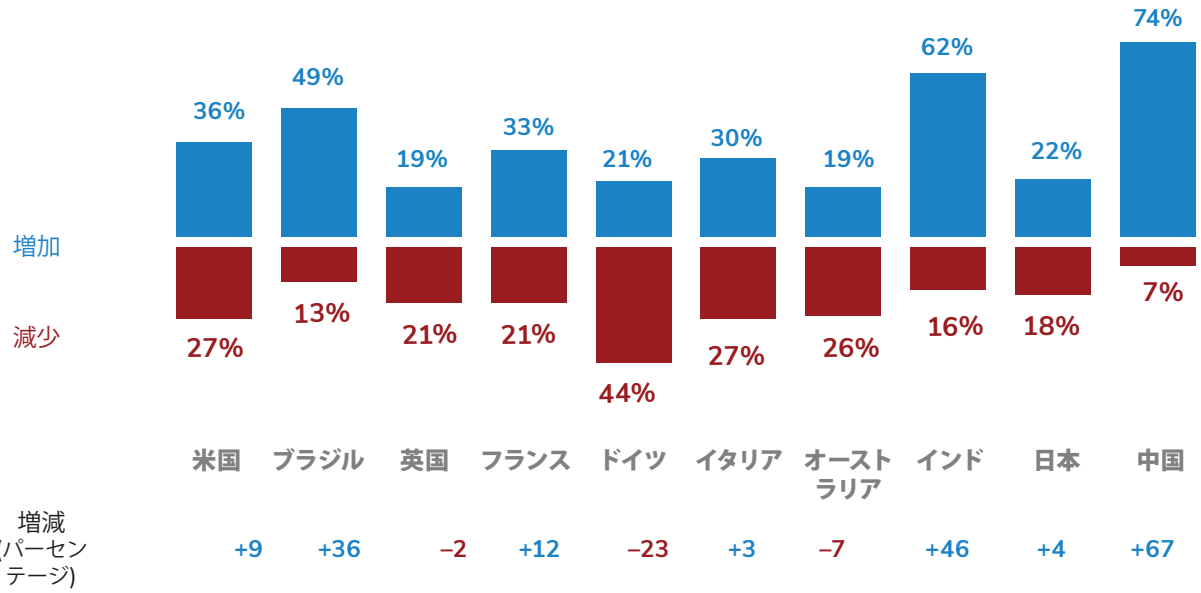
モバイル端末やWi-Fi接続環境が普及した現在、ノートパソコンやタブレット、そしてスマートフォンからWebサイトへ送信されるデータを暗号化して、安全に保護することが不可欠となっています。

フロスト＆サリバンの調査では、オンライン詐欺が増え続けると、デジタル面での企業に対する消費者の信頼（デジタルトラスト）に悪影響を及ぼしていることがわかっています。安全性の疑われる企業は、そのブランドが失墜し収益も落ち込みます。実際、フロスト＆サリバンが実施した2018年の Global State of Online Digital Trust（オンライン電子取引の信頼に関する世界的状況）調査および指標では、オンラインの信頼性と収益低下の直接的な関係性が明らかになっています。データ漏えいを理由に特定の企業のサービスの利用を止めたと回答した消費者が48%にも上っていることが、この現実を裏付けています[4]。

つまり、データ侵害が情報漏えいやフィッシング詐欺、なりすましサイト、またはMITMなど、それがどんな種類であっても、犠牲になるのは電子取引の信頼と企業収益であるということです。さらに同調査は、消費者の電子取引への信頼が危機に瀕していることも示しています。世界的に、信頼度指数の上昇を報告したのは38%の消費者のみで、同じレベルに留まった消費者は40%、そして低下した消費者は22%でした。アメリカやフランス、イタリア、そして日本では、信頼性指数があまりに低く、大規模なサイバー犯罪が数件でも発生すれば、それはマイナス値になる恐れすらあるため、オンラインビジネス企業にとっては警告と捉えるべきです。イギリスとドイツ、そしてオーストラリアの消費者も、2018年はオンラインでの電子取引への信頼が1年前と比べ低下したと回答しています（図1）。

1 https://www.statista.com/statistics/491938/digital-market-outlook-digital-payment-users-by-segment-uk/
2 https://www.digitalcommerce360.com/article/us-ecommerce-sales/
3 https://breachlevelindex.com/（2018年12月19日現在）
4 フロスト＆サリバンによるCA Technologies 2018 State of Online Digital Trust Survey—https://www.ca.com/us/collateral/white-papers/the-global-state-of-online-digital-trust.html

図1：過去2年間におけるエンドユーザーの企業に対する電子取引への信頼（2018年、グローバル）[5]



N = 900.

*出典：*フロスト&サリバンによる CA Technologies 2018 State of Online Digital Trust Survey

インターネットユーザーの電子取引への低下が案じられる中、企業が信用を底上げするためには、暗号化により安全で信頼性の高いデジタル環境を提供することが重要です。同様に、電子証明書などでその暗号化ツールに高い保証レベルのアイデンティティ検証プロセスを導入すれば、自社のプロセスの安全性を確保しつつ、より強固なセキュリティコントロールを確立することができます。Webサイトのデータ送受信をデフォルトでHTTPSを使用して暗号化すれば、電子取引の信頼性向上につながります。特に、大手ブラウザが暗号化されていないHTTPサイトは安全でないと警告表示するようになった今は、なおさらです。

TLS証明書の重要性

TLS[6]証明書は、証明書の発行に関する厳格な業界標準に基づき、認証局により発行されます。これにより、その証明書がインストールされたウェブサーバと、[7]それをアクセスしているエンドポイント側のブラウザ間で送受信されるデータが暗号化されます。エンドポイント側がマルウェアに侵害されていなければ、適切に実装されたTLS証明書は、通信中のデータが保護され、サイバー犯罪や国家標的型攻撃に狙われる心配がなくなります。

5 同上

6 TLSまたはTransport Layer Securityは、SSL（Secure Socket Layer）の安全性が一層強化された次世代規格であり、どちらも同様の意味で用いられます

7 デスクトップやノートパソコン、タブレット、そしてスマートフォンを総称してエンドポイントと呼びます

証明書のタイプにもよりますが、TLS証明書を実装したWebサイトでは、アクセスしたブラウザのアドレスバーには、以下が表示されます：

1. ブラウザのアドレスバーに鍵マークが表示される（ドメイン名認証、またはDV）
2. ブラウザのアドレスバーに鍵マークが表示されるのに加え、証明書の詳細にて会社情報（OV認証、またはOV）の確認が可能。あるいは
3. 会社名の表示、または緑色などの視覚による表示（EV認証、またはEV）

TLS証明書を使用すべき理由はいくつかありますが、とりわけビジネスにとって最も重要なのは通信データを不正アクセスから保護することです。TLS証明書により、ブランドを保護するだけでなく、社内でセキュリティコントロールを実装していることを顧客に示すことができます。TLS証明書により、電子取引への信頼を損なうのでなく、逆に定着させることができます。Google Chromeをはじめとする大手ブラウザでは、2018年より暗号化されていないテキストデータを使うWebサイトに対して警告を表示するようになっていることもあるため、これは重要なことです。暗号化されていないサイトにアクセスしようとすると警告が表示され、ユーザーはセキュリティの危険を承知の上でそのサイトに進むかを確認させられます。

Google Chromeは世界の約61.5%のユーザーが使用しているため[8]、この警告表示によりインターネット利用者の行動が変わりました。また、Google検索結果では、TLS証明書を導入しているサイトが優先的に表示されますが、Googleは検索エンジン市場の約64.4%を占有していることもあり[9]、企業経営者はWebサイトのデータ送受信における暗号化の重要性を無視するわけにはいかなくなっています。

TLS証明書の主な機能

- **認証** - 認証局は、SSL証明書を発行する前に、その組織について様々な情報を確認します。例えば、ドメインの管理や、ドメイン所有者が企業であるかまたは個人であるか、所在地や法的存在などです。
- **暗号化** - TLS証明書により、ユーザーとWebサイト間で通信されるすべてのデータが暗号化されます。暗号化されないと、データはプレーンテキストとして送信されるためハッカーの標的になりやすくなります。
- **データの完全性** - TLS証明書は、メッセージ認証コード(MAC)アルゴリズムにより、通信中のデータの損失や改ざんを防ぎます。

市場の状況

ここ2年、ハイアシュアランス（高い保証：企業認証およびEV証明書）レベルの証明書の国際市場では、様々な動きがありました。市場に大きな影響を与えた主な発表は、図2に示す通りです。

8 2018年10月、http://gs.statcounter.com/

9 2018年10月、http://gs.statcounter.com/search-engine-host-market-share

図2：ハイアシュアランス証明書市場における発表とその影響（グローバル、2016–2018）

認証局への影響	発表事項	企業への影響
SHA-1は暗号上安全ではないと見なされるため、ベンダーにより発行されたTLS証明書はハッシングアルゴリズムSHA-2に移行する必要あり。	SHA–2ハッシングアルゴリズム2017年までにブラウザに必須化	サイト所有者は認証局から新しい証明書を受けないと、主要ブラウザで「安全でない」と表示される。
技術面では、認証局はセキュリティプロトコルを定期的に更新する必要がある。事業運営面では、更新・認証が頻繁になる一方、セキュリティレベルが向上する。	SSL証明書の有効期間を3年から2年に短縮	サイト所有者は、セキュリティプロトコルが定期的に更新されるため安心。これにより、エンドユーザーによるデジタルトラストも向上する。
シマンテックはTLS 証明書市場のリーダーだった。そして、その最大の競合であったデジサートに買収された。すでに技術、規格、カスタマーサポートで業界リーダー的ポジションにいたデジサートはこの買収でデータセンターを世界展開することになり、市場リーダーとなる。	シマンテックが発行した証明書がGoogleとMozillaに信頼されず、同社は認証ビジネスを撤退	シマンテックの証明書を利用していたサイト所有者は、無料でデジサート証明書に移行することができた。買収後、デジサートは世界展開のデーターセンターで、データ主権とプライバシーの問題を解決できるようになった。

シマンテックにより発行された証明書の無効化がされた結果、何百万ものWebサイトが「安全ではない」と表示されてしまうことになり、SSL市場の形勢が大きく揺れ動きました。こういったWebサイトの中には、機密性の高い個人情報や金銭取引を扱う大手金融のサイトも含まれていました。この結果、シマンテックは認証局事業から撤退することになり、そして同分野で信頼と実績のあるデジサートに買収されました。この買収により、Webサイトセキュリティ市場が部分的にも統合され、その結果デジサートは、ハイアシュアランス証明書における世界的なマーケットリーダーとなりました。

市場シェアの分析

この市場統合により、前回のフロスト＆サリバンの市場調査以降、高い保証レベルの証明書市場は大きく変化しました。2018年の認証局市場分析によると、デジサートの市場シェアが著しく増加し、企業向けハイアシュアランス証明書の市場シェアで首位になっています。

一方、SectigoやGoDaddyなどドメイン認証中心の認証局は、市場シェアを失っています。これは、エンタープライズが証明書の予算の大部分をハイアシュアランス証明書の方にかけているためです。特に金融や医療、そして小売業界の大企業と中規模企業では、ハイアシュアランス証明書が重要視されているため、ハイアシュアランスに焦点を当てているデジサートが今後も市場をリードするものと予想されています（表3）。

図3：ハイアシュアランス証明書市場：売り上げシェア（グローバル、2018年）

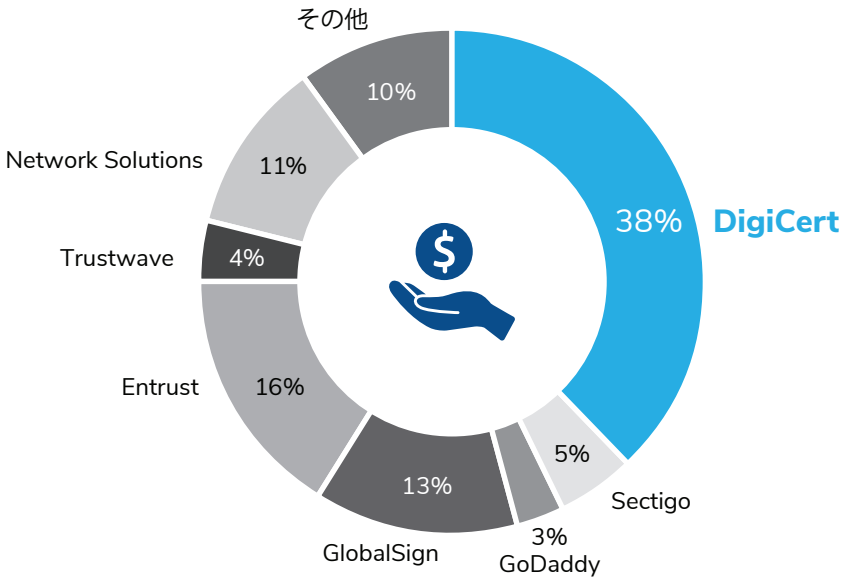
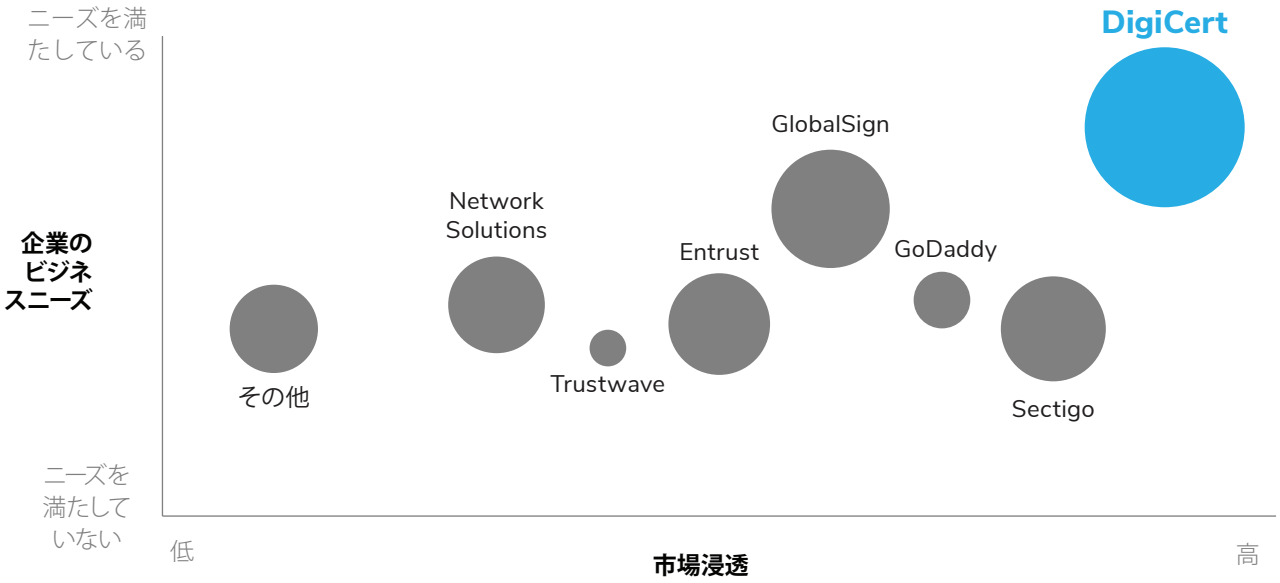


図4では、ハイアシュアランス証明書市場における各認証局の形勢を、各パラメータ別に示しています。これには、シールの認知度や信頼度、料金、顧客のロイヤリティ、インストール基盤、業種なども含まれています。それぞれの円の大きさは、各認証局の売り上げ規模を表しています。

図4：ハイアシュアランス証明書の市場勢力（グローバル、2018年）



SSL証明書のベンダーのほとんどが、ドメイン認証で競合関係にありますが、Let'sEncryptが無料でサービスを提供したことにより、安さが重視されるようになってしまっています。一方、ハイアシュアランス証明書の市場は、価値と価格が絶妙なバランスで保たれています。証明書自体で差別化することはできないため、各認証局は独自の機能やサービスを価格に含めることで差異化を図っています。TrustwaveやGoDaddy、Sectigo、そしてNetwork Solutionsは、デジサートやEntrust、GlobalSignに比べ安い料金で証明書を発行しています。ただ、価格のみで勝負している認証局は、研究開発に多くの資金をかけないため、顧客企業のビジネスニーズを満たすのが難しくなっています。この中でデジサートは例外で、研究開発に多額の資金を投資しており、たとえ業界標準が進化しても、同社発行の証明書に正当性の面で問題が生じる心配をなくすようにしています。さらに、現代的なインフラやグローバルなデータセンター、そしてスケーラビリティを持つ認証局を利用することは、証明書管理にかかる時間と労力を節約できる管理コンソールを使用するのと同じくらい、重要です。

企業が価格だけで認証局を選ぶことは、絶対するべきではありません。次の5つの要素についてもよく検討する必要があります：

1. **管理コンソール** - よく設計された管理コンソールなら、管理にかける時間節約と適切なコンプライアンスを実現できます。時間もコンプライアンスも、企業のIT予算に大きく影響します。
2. **テクニカルサポート** - 実力あるテクニカルサポート担当者がすぐに問題解決できる体制があるかどうかによって、企業は大幅な時間の節約と収益の増加につなげることができます。
3. **オートメーション** - 労力と時間のかかる証明書取得のプロセスを自動化させることで、IT担当者に余裕が生まれ、会社の他の優先課題に焦点を当てることができます。
4. **セキュリティシールの認知度** - インターネットに詳しい人もそうでない人も、ノートンなど見おぼえのあるブランドのシールが貼られているサイトなら、安心して利用することができます。
5. **国際的な広がりと事業規模** - デジタル化された今の国際的な経済において、世界中にデータセンターを構えソリューションを大規模に展開できる認証局であれば、企業成長に伴ったニーズに対応できます。

ハイアシュアランス証明書を求める企業は、ある認証局が業界でどの程度の信頼を得ているか、またインターネットの利用者にどの程度認知されているかという点も、考慮する必要があります。それは、インターネットに詳しいエンドユーザーは、以下に影響されるためです：

1. ハイアシュアランス証明書がそのウェブサイトで使用されているか、そして
2. セキュアドシールのブランド認知度

これら2つの要素は、インターネットに詳しいエンドユーザが、既知また新規にかかわらず、そのWebサイトで商取引を行うかの決定に影響します。企業によるデジタルトラスト構築の努力が続く中、消費者による認証局発行のセキュアドシールの認知度の重要性はは無視できません。

世界の主要経済7か国を対象に、オンラインで買い物をする1,000人の消費者に行ったセキュアドシール認知度と信頼についてのアンケートでは、[10]デジサートによるノートンのシールと、デジサートブランドのシールが、86%のインターネット消費者に認知されていることがわかりました。さらに同アンケートで、デジサートは最も信頼できる世界の認証局トップ3にランクインしています。これは、デジサート採用企業のサイトでは、その顧客がが買い物かごのアイテムを取り消さず、購入を完遂することを意味し、収益増加をもたらす下支えとなることを意味しています。

10 米国、英国、フランス、ドイツ、中国、日本、そしてオーストラリア

図5は、各認証局のハイアシュアランス証明書における特徴と機能を比較したものです。

図5：主要認証局のハイアシュアランス証明書の主な機能（グローバル、2018年）

	Company								
	DigiCert	Sectigo	GoDaddy	GlobalSign	Entrust	Trustwave	Network Solutions	Certum	SwissSign
統合化された証明書管理とコンソール	✓	✓			✓	✓			✓
迅速なHA証明書発行	✓								
ウェブのスキャン	✓		✓		✓		✓		
IoTソリューション	✓	✓			✓				
電子証明書	✓	✓	✓		✓	✓		✓	✓
電子署名サービス	✓	✓	✓		✓	✓		✓	✓
24時間体制のサポート	✓	✓	✓	✓	✓	✓	✓	✓	✓
証明書の簡単な自動化	✓	✓					✓		✓
PKI管理	✓	✓		✓	✓				✓

市場の見通し

フロスト＆サリバンでは、ハイアシュアランス証明書の国際市場はその需要の高まりにより2020年まで拡張し続け、年平均成長率(CAGR)15%を達成するだろうと予測しています。この成長の背景には、インターネットを使用するエンドユーザーのセキュリティに対する認識の高まりがあり、暗号化の仕組み自体はわかっていなくとも、データ保護における暗号化の重要性を理解するユーザーが増えていることが挙げられます。そしてこの意識の高まりがまた、さらにオンラインビジネスに対する電子取引の信頼の高まりを誘発しています。市場成長に寄与している他の要素として、IoTデバイスのセキュリティの強化や、コードサイニングにおける安全性の確保などもあります。

市場は今、特にIoTの安全確保という観点から、変革と成長の幕開けを迎えていますが、この市場をリードするには、迅速対応のサービスと柔軟性ある広範な製品ポートフォリオ、そして研究開発への継続的投資を基本にした、着実な成長戦略が必要となります。

ますます多くの消費者がオンラインで様々な商取引をおこなうようになるに従い、企業が求めるニーズも変化します。現在、TLS証明書は今やオンラインで事業を行う上での最低条件となっており、地理的・政治的な違いに関わらず、いかなる組織であっても無視できなくなっています。さらに、証明書の有効期限を2年までに制限することになったため、企業が証明書を更新する頻度は、約3割増加しました。そんな中、デジサートは企業向けの公開鍵基盤の証明書管理プラットフォームを開発しました。ここでも、証明書管理プロセスの簡易化によってIT担当者の負担削減を目指す姿勢が明らかになりました。このプラットフォームでは、企業はそのワークフローをカスタマイズし、そして証明書発行を自動化させることができます。そうすることで、スプレッドシートなどを使った手動での証明書管理にともなう人的ミスが軽減され、証明書の更新、ひいては中断のない業務の継続が実現されます。

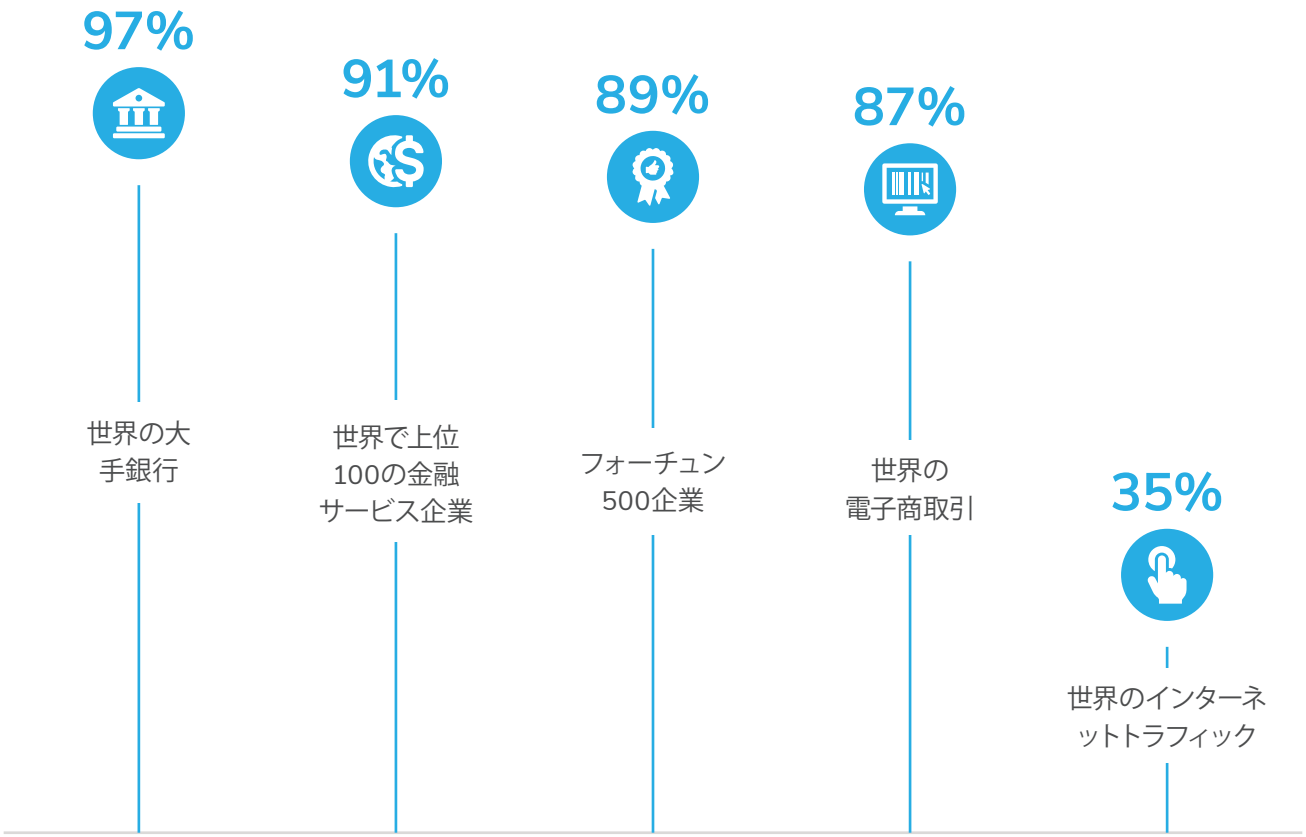
他にも未来に向けてデジサートが投資していることがわかる例として、クライアントやデバイス、そしてハイアシュアランス証明書のサポートを通した、IoTに対する早期からの取り組みが挙げられます。デジタルトランスフォーメーションへと舵を切る多くの企業がIoTソリューションの実装に着手する中、各IoTデバイスの安全確保は極めて重要です。組織の規模によっては、使用されるIoTデバイスは数百、数千、または数十万にものぼります。事業が不意に中断されることのないようにするには、それらのデバイスに送信されるデータは、適切な発信元から来ていることを認証し、機密を保ち、そして改ざんの危険から守る必要があります。デジサートは、このエンタープライズクラスのIoTデバイスに必要な高レベルのセキュリティを提供することができる立場にあります。そして、シマンテックの認証局事業撤退に際し同社のグローバルなインフラを買収したことにより、その能力を一層強化することに成功しました。

おわりに

デジサートは、インフラと研究開発へ大きな投資を推進してきた結果、真にグローバルなフル-サービス認証局に変身し、そして現在市場をリードしています。その過程で、サービスのレベルの高さや信頼できるセキュリティ、機能的な管理ツール、そして柔軟性ある製品ポートフォリオを持つ認証局として知られるようになりました。デジサートのサービスとツール、そしてプロセスにより、多忙なIT部門や情報セキュリティ担当者でも、事業のデジタルトラストを向上させながら、同時に管理にかかる時間を削減することができるようになります。

テクニカルでないオンラインユーザ人口がセキュリティを懸念するようになり、電子取引の信頼が低下する中、企業が自社のセキュリティ対策で消費者に良い第一印象を持ってもらう機会は一回しかありません。デジサートは、毎年多額の研究開発費をかけ、製品ポートフォリオや管理ツールが将来にわたって活用できるようにしています。企業は、そういった信頼できる市場リーダーを選ぶことで、仮に市場の状況が変わっても、他の認証局から新しい証明書を取得しなければならない心配もありません。

図6：デジサートの実績 - ハイアシュアランス証明書の世界市場のリーダー



ハイアシュアランス証明書において確実なセキュリティを求めるには、認証局をよく検討した上で選ぶことが重要です。料金のみを重視して決めると、知らぬうちに追加料金を課される場合があるので注意が必要です。安くて得だと感じても、ここは低価格という単純な次元を超えたところで考え、デジサートのようなフルサービスのプロバイダーを使った場合の費用節約と、最終的なプラスのROIを理解する必要があります。

FROST & SULLIVAN

シリコンバレー
3211 Scott Blvd
Santa Clara, CA 95054
電話 +1 650.475.4500
ファックス +1 650.475.1571

サンアントニオ
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
電話 +1 210.348.1000
ファックス +1 210.348.1003

ロンドン
566 Chiswick High Road,
London W4 5YF
電話 +44 (0)20 8996 8500
ファックス +44 (0)20 8994 1389

+1-877-463-7678 • myfrost@frost.com
http://www.frost.com

次のステップ

- **業界ソートリーダーシップを活用し、御社のアイデアや機会そして課題を議論しませんか。弊社グローバルチームとの** ミーティングをご予約ください。
- 本ホワイトペーパーで取り上げている課題に関して詳しくお知りになりたい場合は、フロスト＆サリバン ジャパン株式会社（03-4550-2210）までお問合せください。弊社のアナリストが追ってご連絡いたします。
- 弊社の**デジタルトランスフォーメーション**のページもご覧ください。
- 弊社主催の**Growth Innovation & Leadership (GIL)**イベントにご参加ください。成長機会を見つけるチャンスです。

連携企業

digicert®

フロスト＆サリバンは、洞察のあるイノベーションを活用することで、市場参加者にとって死活問題となるグローバルな課題やそれに関連した成長機会に顧客と共に取り組んでいます。弊社には、50年以上にわたりグローバル1000企業や新興ビジネス、公共部門、そして投資コミュニティーの成長戦略開発をサポートしてきた実績があります。産業のコンバージェンスや破壊的技術、競争的緊張の高まり、メガトレンド、画期的なベストプラクティス、顧客の多様化、そして新興経済国の動向などを視野に入れ、先見的なビジネスの展開をお手伝いいたします。