CSC

SSL現状レポート

重要な変革を乗り切るための証明書管理における洞察

概要：SSLの状況は刻々と変化しており、断片化された管理は企業に損失をもたらす可能性があります。

近く実施される、SSL (Secure Sockets Layer) 証明書の有効期間短縮に応じて、企業は証明書管理の自動化への移行を早めるべきだと言えるでしょう。また、SSL管理が断片化されていることでドメインセキュリティが損なわれる状況も避けるべきです。

ドメインセキュリティは、これまでで最も変革的な段階に入ろうとしています。これにより、企業はオンラインブランドおよびデジタルアイデンティティの保護において大きく遅れをとる可能性があります。特に、今年初めに実施されたWHOIS情報を使用した電子メールによるドメイン検証の廃止と、2026年3月から行われる証明書の有効期間およびドメイン利用権確認 (DCV) の再利用期間の短縮は、企業の運営方法に大きな変化をもたらすでしょう。

2029年までに、SSLおよびTLS (Transport Layer Security) 証明書の有効期間が367日からわずか47日に短縮されます。つまり、約1年毎に証明書の更新を行っていた企業は、今後年間約8回の更新が必要になります。さらに、DCVの再利用期間は、2029年までに367日からわずか10日に短縮されます。

こうした変更の理由として、低コストで入手しやすいドメイン認証 (DV) 証明書が市場を独占していることが挙げられます。

サイバー犯罪者がこれらの安価または無料のドメイン認証を利用し、ブランドを偽装した詐欺サイトに同種のドメインを使用することで本物のように見せかけ、顧客に悪質なリンクを意図的にクリックさせて個人情報を侵害する事例が発生しています。

こうした中、セキュリティに重点を置いている企業もありますが、当社の年次「ドメインセキュリティレポート」では、多くの企業が依然としてドメインセキュリティにおける重大なリスクを抱えている状況が浮き彫りになっています。当社の調査によると、Forbes誌の「グローバル 2000」リストに選出された企業の3分の2以上が、推奨されるセキュリティ対策の半分未満しか実装していないことがわかりました。

本SSL現状レポートでは、240万のドメインにリンクされた802,000件以上のデジタル証明書の使用傾向およびパターンを分析し、企業によるSSL証明書の管理状況が、これらドメインの整合性保証にどのように影響するかを考察しています。当社の調査や企業リーダーとの直接的やり取りから、企業がSSL証明書の有効期間およびDCV再利用期間の短縮に対する戦略的対応の実装を無視または遅延していることがわかりました。本レポートでは、これらの問題に関する詳細に加え、回避するために必要な手順についても説明します。

簡単に取得できる認証を選択するブランドが後を絶たない

SSL証明書は、オンラインブランドの正当性と安全性を認証し、証明書の資格情報を検証し、ウェブサイトのサーバーおよびユーザーのブラウザ間の接続を暗号化します。

SSL証明書における2つの主要機能

- **セキュリティ:** 暗号化により、ログイン資格情報、クレジットカード番号、その他の機密データが確実に保護されます。
- **信頼性:** ユーザーは、証明書が設定されているサイトは正当な企業によって所有および運営されており、安全なデータ転送が可能であると信頼しています。審査のレベルに応じて、証明書の認証レベルが異なります。

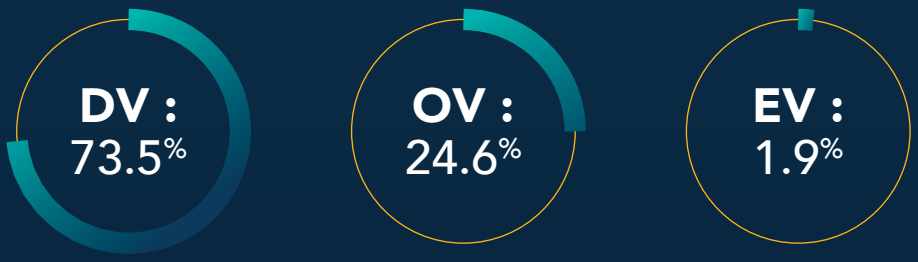
しかし、当社の調査によると、セキュリティと信頼性が理想的なバランスで実装されているケースは一般的というよりむしろ異例であり、オンラインブランドの大多数は作業負荷を軽減し効率化を図るために、取得しやすい種類の証明書を選択していることが明らかになりました。

SSL証明書における3つの認証レベル

- **ドメイン認証 (DV) :** これらは低コストかつ迅速に取得可能な証明書です。DVは、購入者がドメイン名を管理していることのみを認証するものです。ドメイン名の利用目的に関わらず、どの登録者でもSSL証明書を取得することが可能です。
- **企業認証 (OV) :** OVは、DVと同様にドメインの所有者を検証したうえで、事業登録証明書などの企業に関する特定の詳細を認証します。
- **拡張認証 (EV) :** EVは、企業が法的かつ物理的に実在し、経営活動を行っていることの徹底的な審査によって信頼性を強化した、最も綿密かつ厳格な証明書です。

当社の調査では、DVが証明書の4分の3 (73.5%) を占め、OVがほぼ4分の1 (24.6%) を占めていることが明らかになりました。EVは2%未満 (1.9%) となっています。

証明書種類の分布:



分布から判断すると、DV証明書は簡単かつ迅速に取得可能なため、最も人気が高いことは当然だと言えるでしょう。企業がこれらの低コストの証明書を提供するベンダーを利用する場合、サイバー犯罪者は同ベンダーから同様の証明書を入手して詐欺サイトを正当化し、HTTPS (Hypertext Transfer Protocol Secure) を追加することによってユーザーの信頼を得る可能性があります。詐欺加害者の手口は、偽装されたウェブサイトに誤字や文法の誤りが含まれていた以前のケースに比べて、ますます巧妙化しています。悪質な脅威アクターは偽装に長けており、簡単に取得可能なDV証明書は、彼らの合法的なビジネスを装う手口を手助けしていると言えるでしょう。

かつては、EV証明書を使用しているサイトではアドレスバーが緑色で表示され、閲覧者はサイトが認証済みの企業によって保護されていることを確認することができました。アドレスバーの緑色表示は主要なブラウザで使用されなくなり、それに伴いEV証明書の採用が減少しました。

このデータから、いくつかの疑問が挙げられます。まず、各種ウェブ資産に対してどの証明書を取得するかについて、IT部門には明確な戦略がありますか？ それとも、単に「簡単で早い」という理由でDV証明書を取得しているでしょうか？

複数のプロバイダーは複数のリスクポイントを生み出す

プロバイダー数	分析対象企業の割合
1	22.4%
2	18.5%
3	16.6%
4	15.8%
5	12.2%
6	7.4%
7	4.1%
8	1.9%
9	1.0%
10以上	0.3%

当社の調査によると、ほぼ**60%の企業**が3社以上の証明書プロバイダーを使用しており、なかには13社ものプロバイダーを使用する企業もありました。

当社の調査によると、ほぼ60%の企業が3社以上の証明書プロバイダーを使用しており、なかには13社ものプロバイダーを使用する企業もありました。

上記のグラフから、大多数の企業が複数の証明書プロバイダーを使用していることがわかります。

実際、約60%の企業が3社以上のプロバイダーを使用しており、管理という点において大きな懸念事項となる可能性があります。これにより、一元的なアプローチが欠如し、断片化され非生産的なプロセスが生じる可能性があります。その影響は、ライフサイクルの短縮化やDCVの再利用期間の短縮に伴い、指数関数的に増大するでしょう。

単一のプロバイダーに統合することで、証明書の更新や問題のトラブルシューティングが大幅に高速化および効率化されます。また、SSL関連の問題が発生した場合にも、セキュリティチームのメンバーが1つのソースに対処し、解決することができます。

さらに、単一のプロバイダーと連携することでリスクが軽減されます。プロバイダーによって異なる複数の有効期間に対処するのではなく、信頼できる1社のプロバイダーから適切な時期に更新通知を受け取ることができます。複数のプロバイダー管理では、単一の証明書プロバイダーに統合することで得られるコストパフォーマンスの恩恵を受けにくいと言えるでしょう。

大手プロバイダーは企業向けとは限らない

証明書プロバイダー上位3社:

Let's Encrypt、Google®、Amazon®

総計:分析対象の全証明書の66%

これら3社のプロバイダーは、分析対象企業で使用されているDV証明書の大部分 (89%) を提供しています。低コストのサービスは経費削減を目指す企業にとって魅力的ですが、同時にこれらのプロバイダーは、CSCの執行チームが閉鎖した不正ドメインの認証書の主要な供給源ともなっています。正当な企業にとって魅力的な利用しやすさは、悪質な脅威アクターにとっても同じように便利なのです。

CSCによって削除された不正ドメインの上位証明書プロバイダー:

Google　Let's Encrypt　Cloudflare®　Amazon

コスト削減とスピードを求めて、企業はこれらの消費者向けプロバイダーを選択します。しかし、プロバイダーは、企業が今後のSSL業界の変化に備えるために必要な企業向けサポートを提供していません。短絡的なアプローチは、短縮された有効期間に関しても必要以上に混乱をもたらします。

企業は、47日間の有効期間短縮への対処を無視または遅延させることはできません。直前まで手を打たない場合、圧倒的に複雑で混乱に満ちた移行プロセスに直面することになります。証明書の更新やDCVの実施頻度の増加に対応できなくなる可能性があります。更新を怠ると、経営の重要な基盤であるドメインおよびアプリケーション全体が機能停止となる可能性があります。

事前に計画を立て、企業向けSSL証明書プロバイダーのサポートを受けることで混乱を防ぎ、高い代償を払う必要もありません。確立されたパートナーは、積極的かつ効果的な証明書戦略の提案に加え、時間のかかる手動プロセスを自動化ツールに置き換え、有効期限切れによるシステム障害を未然に防ぎます。このようなツールを使用することで、エージェントは自動更新プロセスの一環として証明書の要求、取得、インストールを不備なく行うことができます。

しかし、自動化ツールのシステム統合には時間がかかります。細かい点に配慮が必要なため、既製品を購入してそのまま導入というわけにはいきません。たとえば、既存のシステムコンポーネントとツール間に互換性がない場合、企業がそれらを交換する必要があります。そのため、短縮された有効期間を無視したり優先順位を下げたりすると、回避可能な、そしてコストのかかる混乱が生じることになります。

最適な自動化に向けた3つのステップ

有効期限切れによるシステム障害を回避しようとする中、企業はSSL証明書の管理に自動化が不可欠であると深く認識し始めています。従来は手作業で対応しており、スプレッドシートを用いて期限切れ間近のものを追跡し、現在の年1回の更新頻度で管理を行ってきました。しかし、状況は変わろうとしており、自動化の重要性は高まっています。

前述のとおり、自動化ツールのシステム統合は簡単なことではありません。複数の証明書プロバイダーの管理や過程で生じる不備により、システム全体の停滞や生産性の低下、そして複雑さを伴う可能性があります。効率的に移行するためにも、次の手順をお勧めします。

プロセスの標準化および文書化

チームメンバー入れ替わりへの対応。状況の変化。いずれにしても、証明書管理には、長期にわたって一貫性が保たれる標準化された方法が必要です。自動化ツールのシステム統合を進める前に、必ずこれらの手順を実行に移し文書化することで、既存および将来のチームメンバーが参照することができます。過程で生じた問題点を記載することで、チームメンバーはどのような問題が発生し、どのように解決されたかを把握できるようになります。

自分自身およびチームの育成

自動化を実行する前に理解しておくべきコンポーネントが多数あります。実績のある単一の証明書プロバイダーと提携することで、これらのコンポーネントに精通している同社がクライアントを適切に導き、学習プロセスは大幅に促進されます。

たとえば、単一のプロバイダーは、クライアントが「大規模な自動化ソリューション」を購入するか、もしくはより安価で野心的なルートを選択するかの決定をサポートすることができます。1つの大規模な自動化ソリューションの代替として登場したITツールには、オープンソースやベンダーのAPI (Application Programming Interfaces) を使用して設計されたものなどがあります。有能なプロバイダーは、クライアントが今後の進め方について情報に基づいた選択をすることを可能にします。

すべてを網羅する

チームは、自動化ツールの統合プロセスから何かを省略することがあります。これは間違いです。細切れのアプローチでは、必然的に統合の成功を妨げる大きな不備が残るため、ワークフロー全体を含める必要があります。

結論

証明書はあらゆる業務に必要であり、企業には不可欠な存在です。顧客は、「このサイトは安全ではありません」という警告表示を目にした途端に競合他社サイトへと移行します。しかし、ほとんどの企業は証明書インベントリを適切に管理できていません。業界は転機を迎えており、企業は自動化ツール導入が不可避となる状況に備える必要があります。

有効期間およびDCVの再利用期間の短縮が重なると、完全なサイバーストームが発生する可能性が高まります。更新計画を遅延させる企業は、移行段階になった際に、より多くのコストとリスクに直面することになります。実績のある単一の証明書プロバイダーと提携することで、自動化によって強化された、よりスムーズで安全な移行が可能になります。

多様なニーズを持つ企業に合わせてカスタマイズできる、CSCによる柔軟なサービス、自動証明書管理ソリューションの詳細をご覧ください。

お気軽にお問い合わせください　1 800 927 9800 | cscdbs.com/jp

CSCについて

CSCは、セキュリティ脅威の分野で信頼されているインテリジェンスプロバイダーです。ドメインのセキュリティと管理、デジタルブランド保護、詐欺防止を重点領域とし、Forbes誌の「グローバル 2000」やInterbrand®(インターブランド) が発表する「世界で最も価値のあるブランド100社」に名を連ねています。グローバル企業がセキュリティ体制に多額の投資をする中、当社の DomainSec℠ プラットフォームはサイバーセキュリティの見落としを把握し、オンラインのデジタル資産やブランドを守るのに役立っています。CSCが独自に開発したテクノロジーにより、企業はセキュリティ体制を強化して、オンライン資産やブランドの評判を狙うサイバー脅威ベクトルを防ぎ、収益の壊滅的な損失を回避することができます。CSCはまた、オンラインブランドのモニタリングとエンフォースメントアクティビティを組み合わせたオンラインブランドプロテクションを提供し、特定のドメインを標的とするファイアウォール外のさまざまな脅威を多角的に把握します。さらに、攻撃の初期段階でフィッシングに対処する不正防止サービスも提供しています。CSCは、1899 年以来、米国デラウェア州ウィルミントンに本社を置き、米国、カナダ、ヨーロッパ、およびアジア太平洋地域にオフィスを構えています。CSCは、クライアントのロケーションに関わらずビジネス展開ができるグローバル企業であり、当社がサービスを提供する各ビジネスで専門家を採用することにより、これを実現しています。cscdbs.com/jpをご覧ください。

DBS02132026