デジタル資産セキュリティ：

原点への回帰

デジタル資産セキュリティ:
原点への回帰

世界中で激しさを増すサイバー攻撃やデータ流出は、増加の一途を辿り、防御は日増しに困難になってきています。その一方、企業においては技術分野への投資が増え、組織防御の担当者にとって毎日が闘いです。

事業を実施する環境を保護し、ブランドを防御するために企業が現在導入しているセキュリティ手法、ツール、技術の多くは、これまで一定の効果を発揮してきましたが、今や攻撃はあらゆる方面から仕掛けられるようになってきました。ハッカー、ハッキングを政治的活動に利用するハクティビスト、サイバー犯罪者、国家による攻撃、内部攻撃(従業員など)はいずれも、セキュリティ手順を激しく攻撃し、セキュリティの弱点を見つけ、内部に入り込むやり方です。

データが様々な入口から流れ込んでいることを認識し、未だ社内とペリメータ(外部との境界線)のセキュリティを区別している組織は、早急にセキュリティ手法を再検討する必要があります。日常業務を円滑に行うには、特に、ドメインやドメインネームシステム（DNS）、デジタル証明書などのデジタル資産の役割について見直すことが重要です。

従来のサイバーセキュリティ手法から、最新のリスクに備える手法に移行するにはどうすればいいのでしょうか？

自社のデジタル資産を把握、特定し、適切に管理する。

業務上の問題が発生したらその問題点を理解し、適切な計画を立てる。

ROIを最適化する。重要なもの(不可欠なドメイン)とそうでないものを知る。

様々なデジタル経路を防御する。

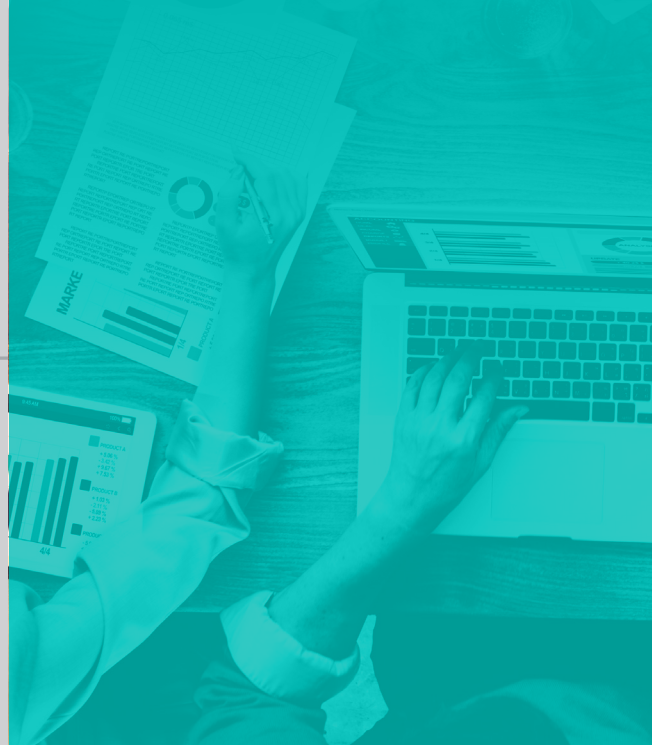
1

2

3

4

自社のデジタル資産を把握、特定し、適切に管理する。



これまで20年に渡り、組織が蓄積してきたデジタル資産は膨大な量に及びます。これらのデジタル資産は会社として、取引を行い、顧客・ベンダー・他の従業員との意思疎通ややり取りを円滑に進めてきました。つまりこれらの資産は、意思疎通から業務遂行、消費の仕方まで変えてきたのです。

現在、世界は以前とは比較にならないほどつながっています。これは世界中ですばらしいビジネスチャンスをもたらしていますが、多くの課題も投げかけています。世界のデジタル経済と同様、ドメイン名、デジタル証明書、ソーシャルメディアのユーザ名、モバイルアプリなどのオンライン資産も発展しています。そのため、企業は所有し使用しているオンライン資産を把握することが不可欠です。把握していない場合、ブランド侵害やサイバー攻撃に対して脆弱になります。

企業が所有し、実際に使用している資産の完全な情報は多くの場合、営業、法務、IT、時には人事まで、様々な部署に分散しています。そのため、監査を行うには、まず手始めにインターネット・プロバイダやレジストラに確認し、オンライン資産目録を作成するのが最もよい方法と言えます。どの企業も、この作業は総合的に行う必要があります。つまり、米国の本社だけでなく、会社が事業を展開するあらゆる場所のオンライン資産を確認しなければなりません。

以下のチェックリストを活用しましょう。次の情報を把握します。

- ○ **所有するドメイン名。宣伝目的のバニティURLや防御目的で登録したドメインも含む。**
- ○ **各ドメイン名のプロバイダ。ドメイン名レジストリか、またはDNS専門プロバイダ、もしくは、自社インフラかなど。**
- ○ **デジタル証明書数。それぞれの認証型と管理方法を含む。**
- ○ **全プラットフォームで使用しているソーシャルメディアの数。**
- ○ **各ソーシャルメディアのユーザー名とパスワードに誰がアクセスできるのか。また、ハンドル名がどう管理されているのか。**
- ○ **モバイルアプリを作成して配布している場合は、それがどのように管理されているのか。**

このような情報を収集する際には、誰が何にアクセスできるのかも把握しておくことが極めて重要です。

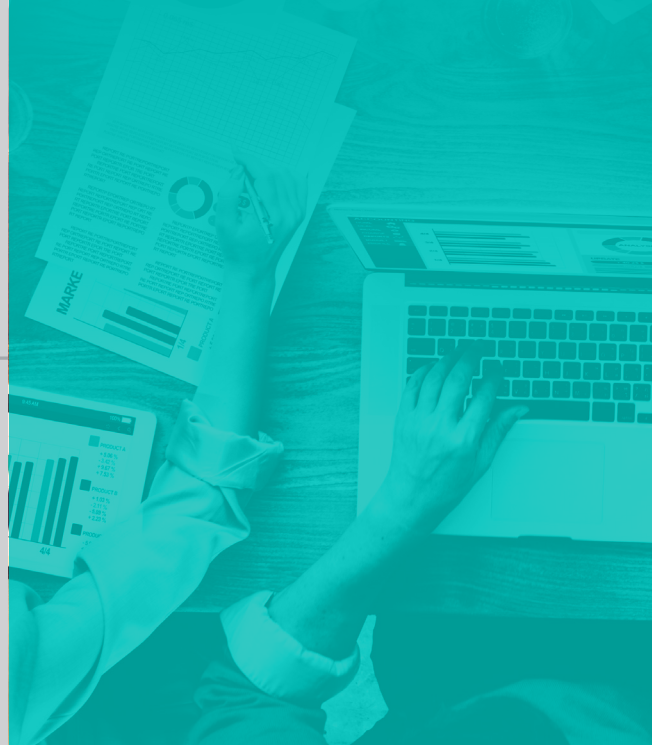
1

2

3

4

自社のデジタル資産を把握、特定し、適切に管理する。



エンタープライズクラス（企業向け）のプロバイダにオンライン資産を集中

ドメイン名やDNSデジタル証明書に関連した、国際企業として自社のニーズを把握することで、委託先の各プロバイダは、会社が求める基準に対応できるようになります。限られたサービスモデルを提供し、クレジットカードに課金する「自作型」低価格プロバイダから、「一流」サービスや、国際企業が求めるSLAや保証、請求方法を提供する大手企業向けのプロバイダまで、各分野において多様なプロバイダがサービスを提供しています。また、選定したパートナーのセキュリティに対する姿勢も重要なポイントになります。

プロバイダの質を慎重に見極めることはもちろん、円滑な管理とビジネスの継続性を確実にするため、オンライン資産を一か所に集めることも非常に効果的であり、導入すべき手法です。専門チームにより、しかもできればひとつのプラットフォームにおいて、すべてのオンライン資産を管理することで、ドメイン名登録・廃止や、ソーシャルメディアの資格情報、デジタル証明書の更新など、様々な変更にも柔軟に対応できるようになります。中でも最も重要なのは、セキュリティにおける弱点の全体像をはっきりと把握できるということです。

現在プロバイダがエンタープライズクラスのプロバイダでない場合、現在のプロバイダや今後契約を検討しているプロバイダに、会社のオンライン資産について、チェックを依頼してください。エンタープライズクラスのプロバイダは、ほとんどの場合、最適なデジタル証明書やドメイン、DNS管理サービスを提供しており、管理しているあらゆるドメインをモニターし、統合したDNSおよびデジタル証明書ポリシーの強化が可能になります。おそらくお客様は次のような疑問をお持ちでしょう。どのドメインがまだ有効で、無効になっているドメインはどれなのか？業務上重要なドメイン名で、DNSSEC（DNSセキュリティ拡張）を使用していないものはあるか？重要なドメインは「常時SSL化」されているか？

ポリシーを規定し、ポリシーから外れたドメインを特定するため、最低限このようなチェックを定期メンテナンスで実施する必要があります。理想的なプロバイダの場合、こういった解析はほぼリアルタイムで実施され、潜在的な問題やコンプライアンス違反を警告してくれます。つまり、ポリシーを策定したらそれを遵守するよう、スタッフの教育も必要になるのです。

ポイントその4で詳細を見る。

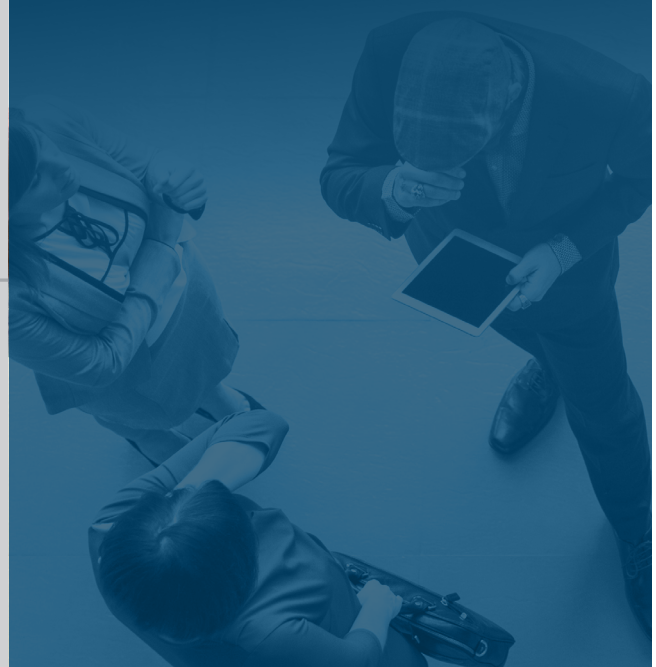
1

2

3

4

業務上の問題が発生したらその問題点を理解し、適切な計画を立てる。



そうすることで、問題が発生したら、それを確認し、重要事項として役員会議にかけ、事業継続性に反映することができます。これは非常に重要なポイントです。

事業継続研究所による『2018年版BCI Horizon Scan Report』では、76か国657名による回答から分析した、10大事業継続性リスクについて警告しています。そして驚くことに、そのうち4件はデジタル資産がリスクを高める役割をしているのです。

サイバー攻撃。DNSは、DNSキャッシュポイズニングから、DNSハイジャック、ドメインシャドウイング、マルウェア、DNSトンネリング、分散型サービス拒否（DDoS）、フィッシング攻撃、期限切れデジタル証明書悪用まで、多数のサイバー攻撃に対して脆弱です。

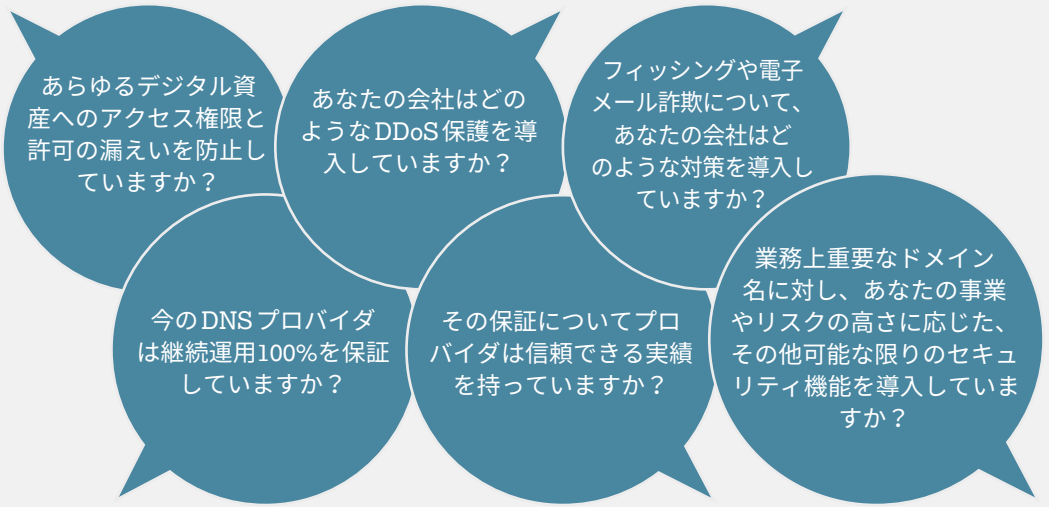
データ流出。デジタル資産に対するサイバー攻撃では、攻撃ベクトルを隠したり、セキュリティ対策や管理が甘い資産を狙って、データ盗難に使われるケースが増加しています。

予期せぬITと通信の停止。会社のドメイン名やDNSが停止すると、インターネットを使用した通信はすべて利用できなくなる可能性があります。そうなれば、お客様とのコミュニケーションや社内の連絡はどう取ればいいのでしょうか？

サプライチェーンの混乱。会社のドメイン名やDNSが停止し、通信能力が半分に低下したら、業務やサプライチェーンも機能不全に陥ります。

影響の大きさを考えれば、オンライン資産に対する基本的なセキュリティ対策が不可欠なのは言うまでもありません。世界中でサイバー攻撃の深刻さが増す中、問題は相手がハッカーかハクティビストまたはサイバー犯罪者かということではなく、実際にサイバー攻撃の対象となれば、会社に多大な損失をもたらすということです。

セルフチェックしてみてください



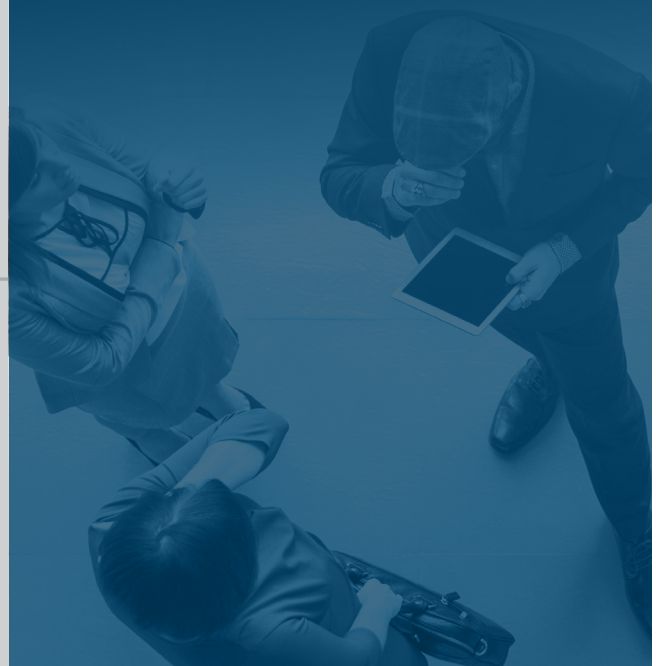
1

2

3

4

業務上の問題が発生したらその問題点を理解し、適切な計画を立てる。



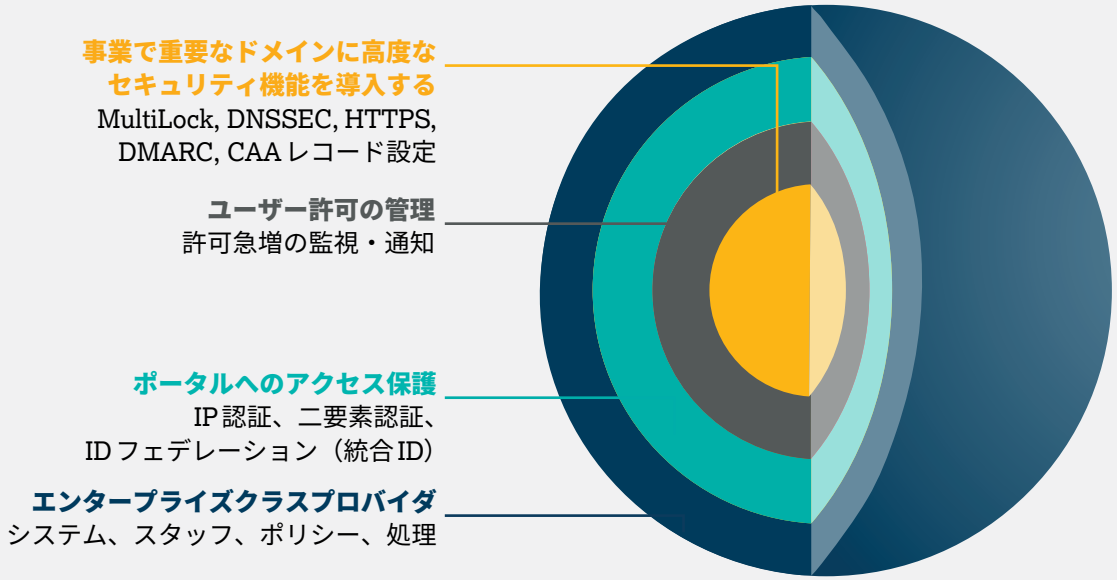
業務上重要なデジタル資産を把握する

事業において重要なデジタル資産を把握しておくことは必要不可欠です。簡単に聞こえますが、実際は社内のどの部門がどのようにドメインを使用しているのか、世界中の全部門に渡って調べる必要があるのです。

不可欠な資産として、ほぼリアルタイムで事業上重要なドメインを特定できるようなアルゴリズムを構築しているか、または機械学習を導入しているプロバイダと協力するのが最適です。

「多層防御」を導入する

多層防御とは、前述の事業継続性リスクにつながるような、デジタル資産に対する脅威から保護する、複数レイヤーを使用したセキュリティの手法です。



1

2

3

4

ROIを最適化する。重要なもの(不可欠なドメイン)とそうでないものを知る。

まずはデジタル資産、特に比較的安価で入手しやすいというドメインの特性こそが、ポートフォリオの肥大やROI（投資利益率）の低下を招いています。しかしROIの実証は可能であり、企業が不可欠なドメイン向けの高度セキュリティに費用をつぎ込む必要があると考えていることを踏まえれば、実際それは非常に重要です。コンセプトは非常にシンプルです。ブランドにあまり価値のない資産は無効にして売却することで、本当に必要なセキュリティ予算を確保することができます。

デジタルIPを関連コンテンツにしっかり紐づけるようにするには、ROIの指標である、アクセス数を確認しなければなりません。すでに使っていないか、メインのドメインにリダイレクトしているドメインも、特別なキャンペーン用に持ち続けてもよいでしょう。また、防御目的で取得したドメインも確認する必要があります。アクセス数は多くないかもしれませんが、ブランド侵害から防御することができます。必要があればそういった防御用登録は可能な範囲でキープし、不必要なドメインはポートフォリオ最適化のため売却します。それにより、ブランドを含め利用可能なドメインの空白地帯を特定し、必要に応じてドメインを取得することができます。

しかしながら使われなくなった企業ドメイン名は、攻撃ベクトルとして悪用されやすいため、合理化や売却は、エンタープライズクラスのプロバイダの協力を得て慎重に行う必要あります。価値のないドメインの合理化・売却を失敗しないためには、不可欠なドメインを特定できるツールを備えたプロバイダが必要です。

1

2

3

4

様々なデジタル経路を防御する。

自社のデジタル資産を管理できるようになったら、誰かがあなたの会社のブランドを悪用したり、なりすましていないか、社外の第三者が所有する資産を確認します。

オンライン監視サービスはほとんどの業界において非常に有益です。しかし、監視の範囲は、デジタルブランド戦略によって異なり、社内の法務部や営業部と協力して、しっかりと監視すべき対象とそれほど心配の必要がない対象に分けなくてはなりません。

担当者はセキュリティリスクの低減を求める一方で、法務部や営業部はブランド侵害を防止したいと考えています。理由は異なっていても、会社を守りたいという意図は同じです。

デジタルブランド監視が優先事項に基づいて行われていれば、コスト効率を上げ、最も大きな被害が予測される脅威に重点を置くことができます。つまり、悪人が価値ある資産に近づく前に、発見することが可能になるのです。適切な監視ソリューションを構築すれば、即刻対処すべき深刻な警告と、ブランドへさほど影響がなく無視できる問題を区別することができます。しかし、監視結果の振り分けは絶えず続く作業となることを理解しておいてください。

監視はセキュリティポリシーや管理のチェック機能にもなります。監視作業はまず、すべての従業員がドメインを、会社が選んだドメイン管理会社を通じ、一括して実施することから始まります。続いて、関連するDNSやデジタル証明書を確認し、不可欠なドメイン名を特定し、ブランドにとっての重要性に基づいて、適切なセキュリティ対策が取られているかをチェックします。

優れたブランド監視プロバイダは、絶え間ない攻撃にも対処できるばかりでなく、注意を必要とする重大な侵害だけを選択して、警告を発することさえ可能なのです。

CSC Security Center

CSC Security Center℠は、これまで手つかずだった業界のニーズ、すなわち会社の重要なドメイン名に関する、セキュリティの全体像把握に対応しています。他に類を見ないこのソリューションは、市場において最も総合的なドメインセキュリティサービスを提供するため、CSCが占有する高度なアルゴリズムを使用して構築されました。このサービスでは、不可欠なドメインを特定し、進行中の脅威を監視、異常が検知されれば通知を送信して、すぐさま脅威の低減措置を取ります。CSC Security Center を活用し、サイバーリスクを低減しながら、デジタル資産の管理方法を向上させる方法について、ぜひ詳しくご覧ください。

cscdigitalbrand.services