CSC

ファイアウォールを超えて:

DNS 防御を導入してオンラインの脆弱性と脅威を回避・軽減

ファイアウォールを超えて: DNS 防御を導入してオンラインの脆弱性と脅威を回避・軽減

ファイアウォールは、25 年以上に渡ってネットワークセキュリティにおける防御の最前線でした。ファイアウォールは、セキュアネットワーク、トラステッドネットワーク、および、コントロールドネットワークとインターネットなどの外側のアントラステッドネットワークの間にバリアを築きます。

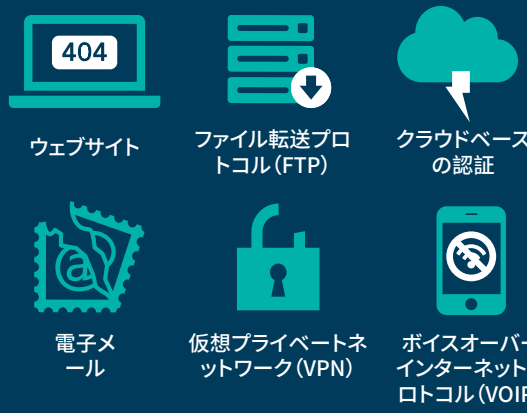
サイバー犯罪は増え続けており、いたる所で発生しているためファイアウォールが必要です。IT セキュリティ分野の多くの関係者は、ファイアウォール内のバリアを強化し、シミュレーションテストとペネトレーションテストを実行して対応しています。

しかし、サイバー犯罪が最高レベルに達した現在では、ファイアウォールだけでは不十分です。

しばしば見落とされるのは、ファイアウォールの外側にあるデジタル資産のセキュリティです。CSC では、これらを、ドメイン名、ドメインネームシステム（DNS）、デジタル証明書として定義しています。良く管理されたデジタル資産、特に、DNS は、円滑なビジネス運営にとって大変重要です。

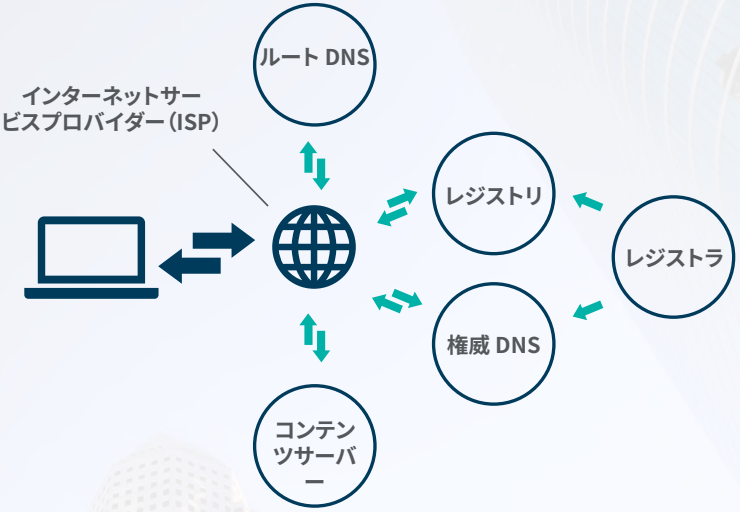
DNS は、インターネット機能の基盤となるインフラストラクチャであり、ユーザーを正しいウェブコンテンツに誘導するディレクトリとしての役割を果たします。DNS が停止すると、ウェブサイトも停止します。これが発生した場合、ビジネスを継続するための論理的な対応は、電話や電子メールを使用することです。しかし、DNS が停止すると、電子メール、電話（VoIP）、あるいは、リモート従業員ログインができません。また、大きなデータセットを移動するためのファイル転送プロトコルや多要素認証サービス（例えば、電子メール、Google®、Microsoft® など）もできなくなります。

これらのデジタル資産の不具合は、収益やデータの損失や、ブランドの評判が損なわれるなど、甚大な影響につながります。



DNS は脆弱なので取り扱いに注意が必要です!

DNS という頭文字はシンプルに見えますが、情報交換のリレイの中で活動する独立したエンティティの世界中のクモの網のような複雑な構造から構成されるシステムの複雑性が隠されています。この複雑性によって、DNS は複数の潜在的な障害点にさらされます。システム内のそれぞれのポイントは攻撃に対して脆弱なので、組織に悪い影響を及ぼします。



DNS の脆弱性に関連する 10 の脅威とリスク

1. DNS ハイジャック
2. DNS キャッシュポイズニング
3. ドメイン・シャドウイング
4. DNS 停止
5. マルウェア
6. DNS トンネリング
7. ゼロデイ攻撃
8. 分散型サービス拒否（DDoS）攻撃
9. ドメインの有効期限切れ、盗難、喪失
10. デジタル証明書の有効期限切れ、不足、不十分な設定

4 段階の多層防御アプローチ

多層防御は、重層的セキュリティアプローチのコンセプトです。ファイアウォールの外側にあるデジタル資産を防御します。

ステップ 1:
最先端のセキュリティ機能を採用します。

ビジネス運営を支えるビジネス最重要ドメインには次を追加します:

- DNS ハイジャック対策のためのレジストリロック
- DNS キャッシュポイズニング対策のためのドメインネームシステムのセキュリティ拡張（DNSSEC）
- データ暗号化のためのデジタル証明書
- 電子メールを認証して、スタッフと従業員を標的にするフィッシング詐欺攻撃を低減するためのドメインベースのメッセージ認証、レポート、適合性（DMARC）
- デジタル証明書ポリシーを強化するための認証局認可（Certificate Authority Authorization、CAA）レコード

1

2

3

4

4 段階の多層防御アプローチ

多層防御は、重層的セキュリティアプローチのコンセプトです。ファイアウォールの外側にあるデジタル資産を防御します。

ステップ 2:
ユーザー権限を管理します。

誰がビジネス最重要資産にアクセスしたか、アクセスした人がどの権限を持っているかを確かに分かるようにして、それらの権限をアクティブに管理します。ボタンに触れるだけで権限にアクセスして、通知を受け取り、プラットフォーム内の変更について権限を監視したり付与できなければなりません。これは、DNS ハイジャックやドメイン・シャドウイングなどの不正な変更がある場合に役立ちます。

1

2

3

4

4 段階の多層防御アプローチ

多層防御は、重層的セキュリティアプローチのコンセプトです。ファイアウォールの外側にあるデジタル資産を防御します。

ステップ 3:
ポータルアクセスを確保します。

使用するすべてのポータルへのアクセスを確保しなければなりません。それぞれのポータルには、アクセスを付与するために、IP 検証、二要素認証、フェデレーテッド ID（または、シングルサインオン）などの多要素認証がなければなりません。これは、少数のプロバイダーを統合して、デジタル資産が不正に変更されるリスクを低減する際にも役に立ちます。

4 段階の多層防御アプローチ

多層防御は、重層的セキュリティアプローチのコンセプトです。ファイアウォールの外側にあるデジタル資産を防御します。

ステップ 4:
エンタープライズクラスのプロバイダーを使用します。

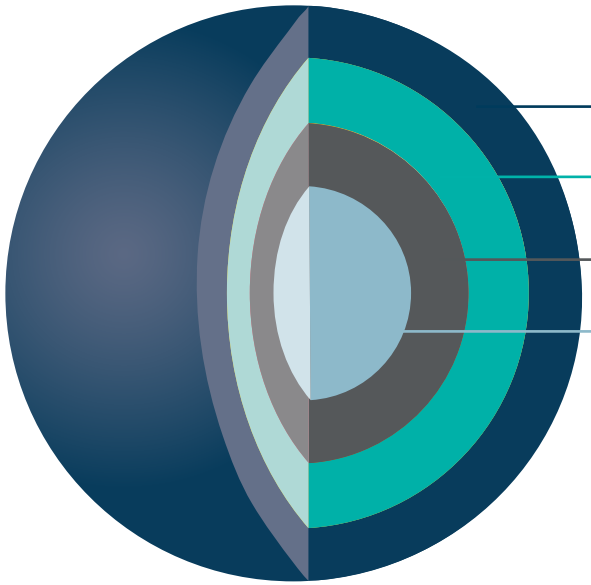
最後に、パートナーを厳選します。プロバイダーの数、および、脅威サーフェスを管理するために使用するポータルの数の制限に加え、ドメイン、DNS、または、デジタル証明書管理の品質に妥協しないことが重要です。最高のエンタープライズプロバイダーは、これらすべての資産の管理を安全なシステムおよびプロセスと統合することを可能にし、リスクと脅威を回避・軽減するお手伝いをします。エンタープライズプロバイダーは社内アナリストによる専門知識、ストラテジックアカウントマネージャーの知識とサポートを提供し、関係するリスクを理解して、正しいソリューションを選択するお手伝いをします。

ファイアウォールの外側にあるセキュリティの脅威を可視化する方法

CSC は、ビジネス、特に、情報セキュリティ管理最高責任者（CISO）が、ファイアウォールの外側にある資産に何が起こっているかを測定することを支援するものがマーケットにに何もないことに気付きました。既存のダッシュボードは社内ネットワークとファイアウォールに焦点を当てており、ファイアウォールの外側にある深刻なリスクを明らかにするツールは僅かしかありません。

CSC Security Center℠ は、IT 専門担当者が保護されていないデジタル資産のリスクを低減することを支援するため開発されました。CSC 独自のアルゴリズムを使用して、ドメインに関係する複数の特性を詳細に調べ、相互関係を理解することで、ポートフォリオ内のどのドメイン名が重要であるかを予測できます。ドメインをさらに検査することで、リスクのインスタンスを特定し、脅威を回避・軽減するための推奨事項を提案します。

可視化が実施可能な制御とポリシーにつながります



CSC Security Center の開発により、会社は、重要なドメイン、ならびに、DNS キャッシュポイズニング、ドメインおよび DNS ハイジャック、分散型サービス拒否（DDoS）攻撃などを含むセキュリティ上の盲点を特定できます。CSC はさらに一歩進んで、ポリシーを施行し、正しい枠組みを設定して、会社のセキュリティ態勢を強化することを推奨します。

エンタープライズクラスのプロバイダー

- ISO 27001 認定データセンター
- SOC 2® 準拠
- 第三者ペネトレーションテスト、脆弱性テスト、セキュリティテスト
- ICANN およびレジストリ認定
- DNS およびデジタル証明書の最高クラスのパートナーシップ
- セキュリティを最優先、フィッシング詐欺アウェアネス、および、ソーシャルエンジニアリングトレーニング
- クリアデスクポリシーの義務付け
- 書面による要求の義務付け（電話は使用しない）
- データおよび一般データ保護規則（GDPR）準拠（WHOIS（フーイズ）プラクティスなど）
- アカウント上のクレジットで対応する自動更新ポリシー
- レジストリトランスファーロックポリシー

ポータルアクセスを確保

- 二要素認証ポリシーの義務付け
- 無料 IP 検証
- 無料フェデレーテッド ID

ユーザー権限を管理

- 通知による昇格権限の可視化
- 正式なコンタクトポリシー

最先端のセキュリティ機能

- 重要なドメインの特定
- セキュリティ上の盲点の検出
- 自動ロックポリシー

DNS ハイジャック攻撃はサイバーセキュリティの最大の脅威です。毎日のヘッドラインで2019 年は転機の年になります。

- CSC Alerts Companies to Increased DNS Hijacking（CSC は企業に対して DNS ハイジャックの増加を警報）
- DNS Hijacking Abuses Trust in Core Internet Service（DNS ハイジャックが中核インターネットサービスの信頼を悪用）
- Alert Regarding Published Reports of Attacks on the Domain Name System（ドメインネームシステムへの攻撃についての公開された報告書に関するアラート）
- Emergency Directive 19-01 Mitigate DNS Infrastructure Tampering（緊急指令19-01 が DNS インフラストラクチャー改ざんを回避・軽減）

国家安全保障機関、外務省、および、大手エネルギー組織を標的とする世界的なキャンペーンは、DNS レコードを改ざんして、まず、DNS レジストラ、電気通信会社、インターネットサービスプロバイダーなどの第三者エンティティユーザーを標的とし、また、アクターが制御するサーバー上で使用するために組織の正当なデジタル証明書を盗んで、アクターが制御するサーバーに誘導することが分かりました。

「DNS 攻撃によって、犯罪者がウェブトラフィックを正当なサイトから不正なサイトに誘導し、顧客と会社が大きなリスクにさらされます。」と語るのは、CSC のセキュリティ・サービシーズの製品担当ディレクターであるマーク・フレッグ（Mark Flegg）です。「最近の攻撃は複雑で悪質であり、多くの会社が一度セットアップした後放置してきた DNS インフラストラクチャーの脆弱性を悪用します。CSC は、クライアントが利用できるツールと推奨事項を使用して、デジタルインフラストラクチャーの安全を確保することを強く推奨します。」

攻撃の重大性のために、いくつかの政府と国際組織は指令や警報で対応することになりました。これはドメインセキュリティでは前代未聞のことです。

「ドメインおよび DNS ハイジャックは新しいセキュリティ脅威ではありません。それが、CSC が CSC Security Center を開発し、世界中の何百という大手企業が CSC Security Center を使用してビジネスの運営を可能にする重要なオンラインエレメントを保護している理由です。」と語るのは、CSC デジタル・ブランド・サービシーズ（Digital Brand Services）のゼネラルマネージャーであるマーク・カランドラ（Mark Calandra）です。「最近急増する攻撃の巧妙性と影響は、ドメイン名、DNS、そして、デジタル証明書の効率的な管理が、オンラインプレゼンスのある会社のセキュリティ態勢を強化するための重要なコンポーネントであることを知らせる警鐘です。」

DNS ハイジャックのリスク、および、脅威を回避・軽減する最良の方法の詳細については、CSC のブログポスト ***Confused About Domain Locks? Understand the Intricacies and Security（ドメインロックについて不明点がありますか? 複雑性とセキュリティを理解する）*** をご覧ください

組織が重要なドメイン向けに持つべき 4 つの主要ポリシー:

デジタル資産管理はドメイン更新、変更、デジタル証明書の交換を管理するだけではありません。CSC は、革新的な技術を業界をリードするサービスと組み合わせ、クライアントがポリシーを施行および管理することをアクティブに支援します。CSC は、ファイアウォールの外側にある脅威からクライアントのビジネスを保護します。

ドメインセキュリティのファンダメンタルズに関する詳細については、**Digital Asset Security: Back to Basics!（デジタル資産セキュリティ: 基本に戻る!）** 白書をご覧ください。

cscdigitalbrand.services/jp