CSC Security Center
クイックガイド

今やサイバー攻撃は毎日のように行われ、その数も増え続けています。そのため、ブランドのオンラインプレンゼンスを守る責任者にとって、適切なパートナーとツールの選択は非常に重要な課題となっています。

デジタル資産は、サイバー犯罪者やハッカーに悪用されやすい弱点と見られているため、標準的な管理サービスを選んで毎年手法を確認するだけでは、もはや十分とは言えません。

サイバー犯罪者の一歩先を行き、急速に進化するビジネスモデルでブランドオーナーをサポートするため、当社はCSC Security Center℠を開発し、シンプルで管理しやすい環境を整えました。

リスクの種類とCSCセキュリティセンターの役割

各種データと、世界の大手企業で検証した複雑なアルゴリズムを用いて、CSC Security Centerは事業に不可欠なデジタル資産を識別、監視し、進行中のリスクを評価します。それにより、監視対象の資産に対するサイバー攻撃に発展しかねないリスクを即座に発見し、低減することができます。

リスク	結果	影響	CSCのソリューション
アカウント利用や管理の低下	重要なドメインやSSLデジタル証明書の有効期限切れ	Webサイトの名前解決や、電子メール、仮想プライベートネットワーク（VPN）、VoIPが利用できなくなり、消費者からの信頼を失い、マルウェアやランサムウェアの攻撃を受ける可能性がある	ドメイン、DNS、SSLの監査と統合
サードパーティープロバイダ	ソーシャルエンジニアリング、フィッシング、分散型サービス拒否攻撃（DDoS）攻撃	ウェブサイトの名前解決、電子メール、VPN、VoIPが管理できなくなり、サイバー犯罪者がサイトを複製し、メールアドレスを不正取得する恐れがある	セキュリティを最重要視し、テクノロジーと人材に重点投資
資産へのアクセス	ソーシャルエンジニアリング、フィッシング攻撃	ウェブサイトの名前解決、電子メール、VPN、VoIPが管理できなくなり、サイバー犯罪者がサイトを複製し、メールアドレスを不正取得する恐れがある	管理システムへは、IP認証、二要素認証、およびフェデレーションIDを用いて安全にアクセス
サードパーティーからの脅威	DDoSやフィッシング攻撃の低減が不可	Webサイトの名前解決や、電子メール、VPN、VoIPが利用できず、二次攻撃に繋がる	MultiLock、DDoS緩和、電子メール認証、フィッシング対策サービスを用いて、既知の脅威から資産を保護
定常的な手法	重要なドメインやリスクが特定できない	ウェブサイトの名前解決、電子メール、VPN、VoIPが管理できなくなり、サイバー犯罪者がサイトを複製し、メールアドレスを詐取される恐れがある	CSC Security Center