CERTIFICATION EUROPE

サイバーエッセンシャルズ
Cyber Essentials

サイバーエッセンシャルズとは

英国政府の調達基準であり、さまざまな組織が基本的なITセキュリティ制御の仕組みを構築するためのサイバーセキュリティ認定スキームです。既知のサイバー攻撃の約80%を防ぐのに役立つスキームとして活用されています。ITセキュリティ制御の5つの重要な領域をカバーしており、この制御を実践すると、組織の脆弱性を大幅に軽減することができます。
サイバーエッセンシャルズは、個人から企業、団体まで、あらゆる組織を対象としており、そのスキームは、それぞれの組織に適切かつ最低限必要なサイバーセキュリティの仕組みを提供します。個人情報保護や取引先の重要データの保護に役立ちます。また、ISO 27001やPマーク取得へのステップにもなります。

サイバーエッセンシャルズの5つのセキュリティ管理領域

このスキームでは、サイバー攻撃に対する脆弱性を軽減するのに役立つ、ITセキュリティ制御の5つの重要な領域において、効果的な制御を実践する必要があります。その5つについては、次の通りです。

5つのセキュリティ管理領域

1. 境界ファイアウォールとインターネットゲートウェイ

境界ファイアウォール、インターネットゲートウェイ、または同等のネットワークデバイスを使用して、インターネットからの不正アクセスおよび情報漏洩から組織を保護します。これらのデバイスが正しく構成されていない場合、外部から内部のコンピュータへ容易にアクセスされてしまい、多くのサイバー攻撃を受けやすくなります。

境界ファイアウォールは、インバウンドおよびアウトバウンドのネットワーク通信を、許可された接続のみに制限することで、コモディティ型のサイバー攻撃（インターネット上で自由に入手できるありふれた機能と技術に基づく攻撃）から保護します。このような接続制限は、ファイアウォール・ルールと呼ばれる設定を適用することによって実現されます。

2. セキュリティで保護された構成

コンピュータとネットワークデバイスは、固有の脆弱性のレベルを下げ、その役割を果たすために必要なサービスのみ利用できるように構成する必要があります。コンピュータ、ノートパソコン、タブレット、スマートフォン、ルーター(WiFiを含む)などのネットワークデバイスは、購入時の設定のままでは安全ではありません。標準装備されている「すぐに使える」構成には、多くの場合、予測しやすい管理者アカウントやパスワード、不要なユーザーアカウント(場合によっては特別なアクセス権限付き)、プリインストールされている不要なアプリケーションなどが含まれています。

コンピュータやネットワークデバイスが購入時の設定のままの場合、サイバー攻撃者による組織の機密情報への不正アクセスの可能性が高まります。コンピュータやネットワークデバイスを使用する際に、いくつかの簡単なセキュリティ制御を適用することで、組織の弱点を最小限に抑え、コモディティ(一般的な)サイバー攻撃に対する保護を強化することができます。

3. ユーザーアクセスコントロール

ユーザーアカウント、特に管理者アカウントなど特別なアクセス権限を持つアカウントは、許可された個人にのみ割り当て、アプリケーション、コンピュータ、およびネットワークへのアクセスレベルを最小限にして管理する必要があります。特別なアクセス権限(管理者アカウントなど)を持つユーザーアカウントは通常、情報、アプリケーション、およびコンピュータへの最高レベルのアクセス権を持っています。

管理者アカウントなどの特権的アカウントが侵害されると、その権限が悪用される可能性が高く、その結果、大規模な情報システムの破壊、組織の他のコンピュータへの不正アクセスが可能になり、情報漏洩がビジネスへ被害をもたらします。特別なアクセス権限が悪用されることを防ぐには、付与しているアクセス権限を適切に制限することが有効です。

4. マルウェア対策

インターネットに接続または公開されているコンピュータは、アンチマルウェアソフトを使用して、マルウェア感染から保護する必要があります。多くの場合、コンピュータは悪意のあるソフトウェアに対して脆弱であり、特にインターネットに接続しているデバイス(利用可能なデスクトップPC、ノートパソコン、スマートフォン、タブレットなど)は脆弱です。利用可能な場合、マルウェアを監視、検出、および無効化する専用のソフトウェアが必要です。

コンピュータはさまざまな理由でマルウェアに感染する可能性があります。多くの場合、感染した電子メールをユーザーが開いたり、侵害されたWebサイトを閲覧したり、リムーバブルストレージメディア上の不明なファイルを開いたりすることで感染すると言われています。ここで解説しているマルウェア保護の範囲は、インターネットにアクセスできる、またはインターネットからアクセスできるデスクトップPC、ノートパソコン、およびサーバーを対象としています。その他のコンピュータは範囲外ですが、タブレットやスマートフォンも同様に、マルウェアに対する保護が必要になる可能性があります。

5. セキュリティ更新プログラムの管理

ソフトウェアを実行するコンピュータやネットワークデバイスには、通常、技術的脆弱性と呼ばれる弱点や欠陥が含まれている可能性があります。脆弱性は多くの種類の一般的なソフトウェアで頻繁に発見されており、悪意のある個人やグループが組織のコンピュータやネットワークを日々攻撃するために、意図的に悪用する可能性があります。

通常、ソフトウェアのベンダー（提供元）は、パッチと呼ばれるソフトウェア更新プログラムを定期的に顧客にリリースし、発見された脆弱性に対する修正をできるだけ早く提供しています。ソフトウェアの脆弱性を悪用するサイバー攻撃は日々進化しており、高度化するサイバー攻撃の被害者にならないようにするために、組織はソフトウェアパッチと更新を効果的に管理する必要があります。

◆サイバーエッセンシャルズの審査及び費用について

サイバーエッセンシャルズの認証取得は、法人・組織に限定されず、個人事業主やフリーランスの方も取得可能です。審査は、すべてオンラインで行われ、下記URLよりお申し込み可能です。技術的に不安のある場合は、登録されているITコンサルタントサービスを活用することも可能です。認証取得されるとデジタル版の認証状が発効され、取引先に対して提示することができます。
審査費用は、組織の人数によって変動します。以下の料金表を参照願います。認証取得後は、毎年認証を更新するスキームであり、その都度の更新費用にも該当します。

料金表	CYBER ESSENTIALS	
Micro Organisations	従業員0*～9名 *個人事業主など	¥90,000.- （税込¥99,000.-）
Small Organisations	従業員10～49名	¥110,000.- （税込¥121,000.-）
Medium Organisations	従業員50～249名	¥130,000.- （税込¥143,000.-）
Large Organisations	従業員250名以上	¥150,000.- （税込¥165,000.-）

CERTIFICATION EUROPE™

CONFIDENCE | ASSURANCE | CERTAINTY

サーティフィケーション・ヨーロッパ・ジャパン株式会社

〒600-8815 京都市下京区中堂寺粟田町93
京都リサーチパーク6号館317号
TEL 075-323-6200 FAX 075-323-6222
Email info@certificationeurope.co.jp