ブレグジット - 特権アイデンティティへの影響

英国と他のヨーロッパの国々がブレグジット（英国の EU 離脱）の準備が進める中で、情報セキュリティの専門家は、これが過去に実装されたセキュリティおよびリスク管理プロセスにとって何を意味し、それらを今後の状況に照らしてどのように調整する必要があるのか、確たる道筋が見えません。この文書では、特権アクセス管理に対するブレグジットの影響と、情報セキュリティの専門家が考えるリスク低減に即効性のあるソリューションについて説明します。

ブレグジット - 次に起こること

英国（UK）の欧州連合（EU）離脱をテリーザ・メイ首相が公式に通告したことを受け、EU 離脱の公式プロセスが開始されました。英国と EU は、今後 24 か月間のうちに、共同作業の枠組みを策定する必要があります。そのプロセスを次の図に示します。

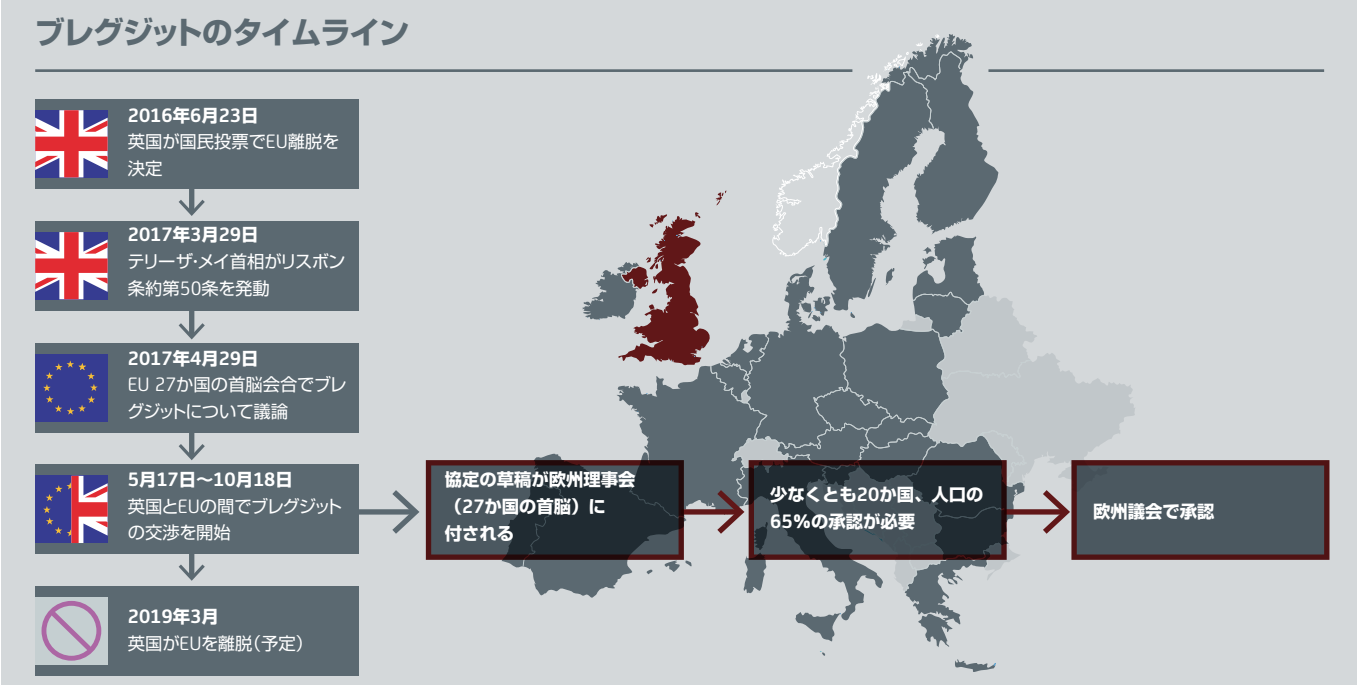

図 A：ブレグジットのタイムライン（APA および DW 提供）

EU と英国は今後 24 か月の間に、分離後の契約条項について合意する必要があります。その一方で、双方のさまざまな公的機関や民間団体が、ビジネスをスムーズに遂行するための方法を模索し始めました。このプロセスには、多くの問題とリスクがあります。結局、直接的であれ間接的であれ、このプロセスに関わる人はすべて、確証のない領域を手探りで進むことになります。したがって、熟考を重ねたリスク管理プログラムが必要になります。

潜在的な経済的影響

ブレグジットによる英国へのマクロ経済的な影響については多くのモデルがあります。その多くは以下のことを示唆しています。

- 長期的な GDP の低下
- 海外直接投資（FDI）の減少
- 移民の減速

これらはすべて、多くの組織がそれぞれの市場で競争力を保ち生き抜くための方法を考える必要があることを意味しています。各組織はビジネス遂行への影響を最小限に抑えるために、最悪のケースのシナリオを考慮に入れながら、将来への枠組みを構築しつつあります。シティグループの欧州 CEO、James Cowles 氏は、スタッフへのメモの中で「計画の策定において、英国が EU へのパスポートを失う「ハード・ブレグジット」を想定する必要があります」と述べています。他の金融機関も同様の計画を開始しています。しかし、影響を受けるのは金融機関だけではありません。離脱が EU と英国に与える影響を考慮する必要があります。たとえばボクスホール社は英国向けのサプライ・チェーン全体を英国内に築こうと考えており、BMW は Mini のためにヨーロッパ大陸内の新しい場所を探しています。ただし、雇用に影響するビジネス上の合理的な決定は、ブレグジットの被害者というレッテルを貼られるリスクをはらんでいます（他の EU 諸国のレベルや世界的需要の変化に合わせるために英国内での生産性を向上させる動きなど）。

雇用への影響

特に懸念されるのは、雇用に対するブレグジットの影響です。さまざまな組織が国境を越えた雇用の移動をほのめかしています。たとえばネスレ社は、「ブルー・リバンド」チョコレート・バーの生産を英国からポーランドに移転すると決定しましたが、これにより英国で 300 人分の雇用が失われると見られています。その原因は、移民をめぐる環境の変化（ビザに関する法律が厳しくなったり審査が厳しくなるなど）や、関税、不確実性にあると考えられます。世界最大手のある人材派遣会社によれば、ブレグジットをめぐる不確実性が原因で、英国の民間企業における雇用は 3 年間で最低レベルまで落ち込みました。このような雇用の移動は、経済全体に大きな影響を及ぼすだけでなく、情報セキュリティに対しても非常に大きな脅威を生み出します。

リスクの洗い出し

ここまで見てきたように、ブレグジットの一環として組織が管理すべき重要なリスクの存在を示す十分な証拠が揃っています。今日私たちが目の当たりにしている劇的な技術変化とあいまって、IT リスク管理の重要性が高まっています。その重要な部分の 1 つが情報セキュリティ・リスクです。情報セキュリティ資産にとって最大の経済的リスクおよびブランド・リスクが特権ユーザ・アクセスの悪用に起因することは、十分に立証されています。このリスクは、組織がビジネスの成長やデジタル・トランスフォーメーションを目的としてクラウド環境や仮想環境を採用していく中で次第に増幅します。

特権アクセス管理のリスクへの対処

組織がブレグジットに起因する課題、特に従業員の移動に対処するための選択肢を検討する場合には、内部の脅威のリスクを考慮する必要があります。雇用状態の変化や権限の委譲のなどの不確実性が、内部関係者の行動の不確実性につながる可能性があります。また、悪意のある外部の攻撃者が潜在的な脆弱性を悪用する可能性もあります。さらに、特定の事業機能のためにサードパーティのベンダを採用した場合などに起きる権限の委譲は、リスクにさらされる確率を高める可能性があり、適切な監視と可視性が必要になります。これらの問題に対処するために、効果的な特権アクセス・リスク低減戦略の実装が必要になります。実際、機密データや知的財産を保護することが非常に重要になります。

特権アクセスのリスクを低減させるための考慮事項

不確実な期間中に特権アクセスの侵害または悪用に起因するリスクを低減するには、以下の点を考慮する必要があります。

1. **規模：**リスクにさらされる対象
    a. エンドポイント / デバイス： オンプレミスで保存されているデータだけでなく仮想およびクラウドベースの資産も対象
    b. アイデンティティ： 管理者ユーザだけでなく、あらゆるアプリケーション間アカウントおよびスクリプトも対象

2. **範囲：** 将来の戦略
    a. デジタル・トランスフォーメーション：デジタル・トランスフォーメーション・プログラムが進行中の場合は、それに関わるすべての顧客、ベンダ、パートナーも考慮に入れる
    b. IoT（Internet of Things）プログラム：特権情報にアクセスできるすべてのデバイスを考慮に入れる
3. **自動化：** 機械学習とセッション記録
    a. 機械学習： リスク検出時間を低減し、危険にさらされるリスクを軽減するために、ユーザ動作分析（UBA）を使用して異常を検出する
    b. セッション記録： 否認防止とコンプライアンスのために使用
4. **リソース：** 予算と人材
    a. 予算： 地政学的な不確実性を受けて、ブレグジットの交渉中は予算が抑えられる可能性が高い
    b. 人材： 移民をめぐる状況の変化と人材の移動が切迫していることから、必要な特定のスキルがないためにデプロイが妨げられることがないようにすることが重要になる

まとめ

この地政学的変化の段階で重要な資産を確実に保護するには、CA Technologies のソリューションのような特権アクセス管理が重要になります。まずパスワード・ボールトなどの基本的な機能の導入から始めるという考えは魅力的ですが、リスクを低減するためには問題を総合的に見ることが重要です。ブレグジットの予定は決まっています。活動のペースは加速する傾向があるため、情報セキュリティの専門家が対応に割ける時間は非常に限られています。方針を決める前に、ソリューションがサポートする機能の対象範囲と規模に加えて、ソリューションの総所有コスト（TCO）もよく検討することが重要です。このプロセスの過程で遭遇する、職務の分離やデータの主権の問題などの未知の問題への対応も計画しておく必要があります。最後に、規模、対象範囲、および自動化を提供するだけでなく、安全な特権アクセス管理の土台となり、機械学習に基づく分析機能も備えたソリューションを選んでください。この変化は英国だけでなく、英国や EU 諸国と大規模な貿易を行っている国々にも影響を及ぼします。