**WHITE PAPER** | 2015 年 11 月

# キル・チェーンの分断

## 特権アクセス管理によるデータ漏えいの防止

ca technologies

# まとめ

## 課題

企業機密や財務レコード、個人情報などの損失につながるデータ漏えいのニュースは、毎日のように耳に入ってきます。こうしたインシデントは、商取引、教育、政府機関などあらゆる分野に広がっています。すでに世界経済にとっても毎年ブレーキとなっており、損失は年間数千億ドルに達しています。1 今すぐ積極的な対策を取らなければ、サイバー犯罪による損害は 10 年以内に数兆ドルにも上ると推定されています。2 また、プライバシーを侵害された個人が被る被害は計り知れません。

セキュリティのエキスパートはこれまで境界ベースの防衛策を確立しようと取り組んできました。これは簡単に言えば、悪意ある人物を寄せ付けず、正当なユーザのみが入れるようにするということです。しかし次々と発生するデータ漏えいは、こうした境界がその主たる目的を果たせていないことを明白に示しています。その結果、アイデンティティの保護と管理に特に重点を置いた重要な新しいセキュリティ層が、漏えいの流れを食い止める取り組みにおいて不可欠な新しい要件であるということを、企業は認識し始めています。こうしたアイデンティティのうち、特権ユーザに属するアイデンティティほど重要なものはありません。こうしたクレデンシャルを盗み利用することは、「境界内への鍵」を手にすることになるため、次々と起きるデータ漏えいで以前にも増して主要な攻撃対象となっています。

## ビジネス・チャンス

セキュリティ・チームは、広く「特権アクセス管理」と呼ばれる、攻撃を無効にし、かつ阻止する手段を提供する成熟したテクノロジとプロセスのセットを意のままに使うことができます。社内外の悪意あるユーザは、攻撃を首尾よく成功させるために一連の論理的な手順を実行すると予測されます。これらの手順は、もともと Lockheed Martin 社のサイバーセキュリティ・チームによって特定され名づけられたもので 3、「キル・チェーン」と呼ばれています。これは、攻撃者が実行する一連の手順を遮断できれば、つまりいずれかのポイントで「キル」できれば、最終的な攻撃を防止または緩和できるという事実に基づくものです。特権アクセス管理は、攻撃のライフサイクルの複数の手順において攻撃を防止する手段を提供します。本書では、キル・チェーンの簡略化バージョンについて検討し、特権アクセス管理がどのように攻撃を阻止し、企業をデータ漏えいから保護するか具体的な例を示します。

## メリット

データ漏えいを防止することで得られる経済的なメリットは明らかです。測定は難しいですがインパクトが大きいのはブランドと評判への損害に伴う「ソフト」コスト、つまり提携先や顧客からの信頼の低下や、会社の市場評価への影響です。しかしこうしたコストは重大であるものの、詳細な個人情報の盗用が無防備で疑いを持たない個人に与える影響は、もっと破滅的なものです。特権アクセス管理は明らかにこのような広範囲の損害を軽減できるため、大きなメリットがあります。

## 課題 – データ漏えい：増大するリスクと計り知れない損害

現在次々と発生しているセキュリティ・インシデントについて考慮する際は、2013 年後半に起きた Target 社のインシデントに遡って考えるのが一般的です。この事件では 7,000 万人分の支払いカードの記録が盗まれました。このインシデントは歴史上初めて起きたものでもなければ最大規模でもなく、2013 年においてさえ最大規模だったわけではありません。しかしさまざまな要因から Target 社のデータ漏えいは、現在も起きているこのような攻撃のきわめて破壊的な性質について、多くの重要な顧客層の関心を刺激する役割を果たしました。Target 社のデータ漏えい以降、約 1 年後に起きた Home Depot と JP Morgan Chase のインシデントや、もっと最近では Experian 社への攻撃によって T-Mobile の顧客約 1,500 万人のきわめて機密性の高い個人データが流出したインシデントなど一連の大規模なインシデントに加え、あまり公にはなっていない小規模な攻撃も無数に発生しています。

> 「デジタル・ビジネスにとって、特権アイデンティティ管理はきわめて重要であり難しいものになっています。1 人の悪意ある管理者、または管理者クレデンシャルの盗難によって、顧客や収入、長期的な評判に壊滅的な損害をもたらす可能性があるため、特権アイデンティティ管理は重要です」。
>
> —Forrester Research[4]

Intel Security と Center for Strategic and International Studies のデータによると、2014 年のこうしたサイバー犯罪による損害は約 4,000 億ドルに上ったと推定されています。これほど巨額の数字は理解しにくいかもしれませんが、この 4,000 億ドルという金額を参考として全世界の麻薬密売の推定額と比べてみると、麻薬密売は年間推定 3,000 億ドルであるため、サイバー犯罪による損害の方が上回っています。サイバー犯罪の影響は多くの裕福な国の GDP を上回ることさえあります。たとえば、偶然ですがシンガポールの GDP も年間約 3,000 億ドルです。これは明らかに経済上の大きな問題であり、迅速な対策を取らなければ状況は悪化する一方で、世界における年間のサイバー犯罪よる影響は 10 年後には 3 兆ドルと、現在の被害額より桁違いに大きくなることが McKinsey によって予測されています。

さて、明らかにこれらのインシデントは損害を引き起こしています。データ漏えいの被害にあった企業は時価総額、売上、顧客からの信用度、利益などが低下しています。しかもその上に、アイデンティティの盗用などの犯罪による損害から、データ漏えいの影響を受けた個人は経済的損害と精神的損害を受けています。しかし、これはすべて厄介な問題ですが、もっと最近発生し始めた他のインシデントについて見てみると、さらに悪いニュースがあります。

まず明らかに、標的となった企業の運営に物理的なインパクトを引き起こすことを目的とした攻撃が見られはじめました。Code Spaces についてはあまり知られていないかもしれませんが、英国に拠点を置く小規模な企業で、開発者向けにクラウドベースのバージョン・コントロールおよびバックアップ・サービスを提供している企業です。2014 年 6 月、ある攻撃者が Code Space の Amazon Web Services（AWS）管理コンソールへの管理者クレデンシャルを入手することに成功しました。この攻撃者は複数のアカウントとバックドアを作成した後、Code Spaces の経営陣に身代金を要求しました。正規の管理者がシステムからこの攻撃者を追い出そうとしたときには、すでに手遅れでした。攻撃者は Code Space の管理システム全体への完全な管理アクセス権を手に入れ、Code Space の情報技術インフラストラクチャ全体（サーバ、アプリケーション、さらに重要なシステムとデータのバックアップ）を急速に破壊するという報復を始めました。この攻撃は数時間で完了しました。Code Space は数日間、運用停止に追い込まれました。5 これは劇的な例ですが、このトレンドを示すいくつかの例が他にもあります（Sony Pictures Entertainment や Saudi Aramco のインシデントなど）。

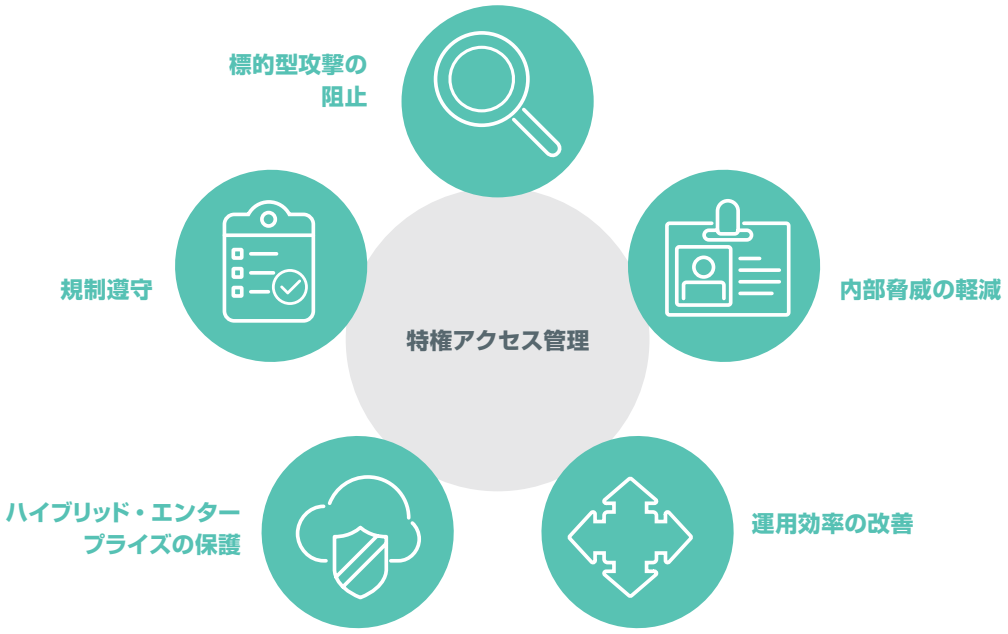
ここから、サイバー・スパイ活動と呼ばれる最新のトレンドまではあっという間でした。これらの攻撃について最初に表れた兆候は、2015 年初めの Anthem、Premera、CareFirst などの保険会社で発生したデータ漏えいでした。数百万人分の個人データ記録が盗まれたこの漏えいは国家レベルでは公式に罪に問われることはなかったものの、政府、軍事納入業者、財務および電気通信や地政学的方針の決定に関わる人物など、機密上重要な役職を担う個人についての調査書類を集めようとする大規模な活動の一部だったのではないかと広く推測されています。漏えいのタイミングは、中国のハッカーが米国の商用ネットワークや政府ネットワークにある個人情報を標的にしているという米国 FBI の機密警告の配信が行われた時期と一致していました。6 その後、米国人事局（OPM）のデータが漏えいし、アクセス権限を求める個人の詳細な経歴、金銭や雇用に関する情報、個人的な履歴などを含む個人データが盗まれるという事件がありました。

## ビジネス・チャンス — 特権アカウント：新たに出現した前線

少し立ち止まってこれまでのことをまとめてみましょう。データ漏えいは大きな問題で、さらに大きくなっています。利害関係はますます大きくなり、攻撃者は高度化し金銭面でも潤沢になっています。ここまで読めば、非常に楽観的な方が少々悲観的に感じたとしても仕方がないでしょう。このような重大な問題を前にして、それと闘うには何をすべきでしょうか？

**図 A**

特権アクセス管理は組織が高度な目標を達成できるよう支援します。



実質的にこれらの攻撃のほとんどには共通した要素が見られるため、希望を持つことができます。その共通した要素とは特権ユーザであり、もっと具体的に言えば、こうした個人が情報技術インフラストラクチャを構成・維持・運用するために使用する特権アカウントとクレデンシャルです。このようなクレデンシャルを盗み利用すれば IT インフラストラクチャへの特権アクセスが得られるため、これはここまで説明してきたすべての漏えいにおいて重要な成功要因であり、攻撃者にとって最初の攻撃対象であることが示されています。

「2018 年までに、企業が特権アクセスに関する調査と保護を適切に行えないことは、内部関係者の誤用およびデータ盗用のインシデントの原因の最大 60% を占めるようになるでしょう（現在は 40% 以上）」。

—Gartner[7]

データ漏えいの成功に特権アクセスが果たす中心的役割について検討する前に、こうした特権ユーザがどのようなユーザであるか簡単に見てみることは有用です。なぜなら特権アクセスを持つ個人の人数も、そのアクセスのために使用される実際のアカウントとクレデンシャルの数も、一般的に認識されているよりはるかに多いからです。

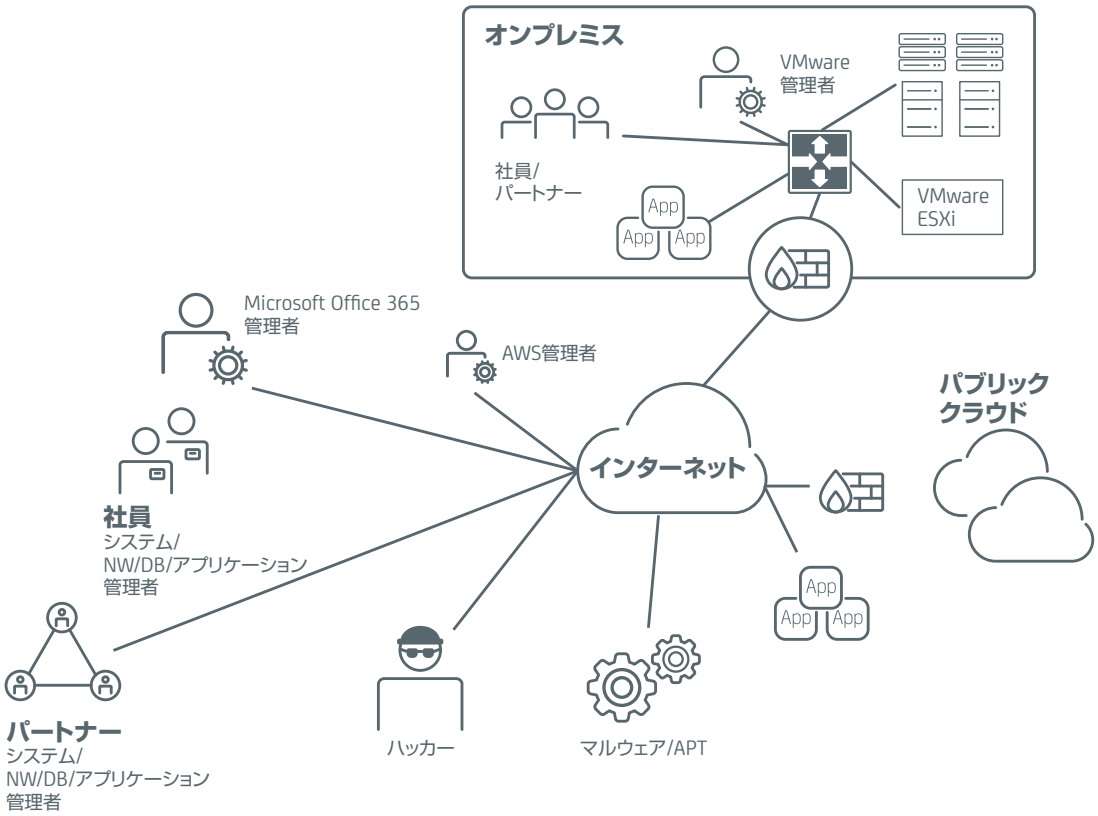



**図 B**

特権アカウント：新たに出現した前線

長年、特権ユーザについて考えるときは一般的に、システムとネットワークの管理に直接的な実地の責任を持つ組織内の人物についてのみ考慮されてきました。その結果、多くの組織ではリスクを最小化して考え、特権アクセス管理の課題をいわゆる「内部関係者による脅威」の管理の 1 つとみなすようになりました。確かに悪意ある内部関係者は大きな損害を引き起こす可能性があるものの、そうしたインシデントは比較的まれで、データ漏えいの原因としての割合は多くありません。

実際には多くの特権ユーザが内部関係者以外で、ベンダや請負業者、ビジネス・パートナーなど、組織内のシステムへの特権アクセスを許可されたユーザです。多くの企業では、こうしたサードパーティ・ユーザの数が、従来の「内部」の特権ユーザの数を上回ることがあります。サードパーティが大きなリスク要因であることは、経験からも示されています。Target、Home Depot や OPM のインシデントその他、これまで述べてきたデータ漏えいは、正規のサードパーティのユーザ・クレデンシャルが侵害され、幅広いネットワークとそのリソ - スへの不正アクセスに使用された例です。

また、クラウドへの移行や、仮想化などのテクノロジの導入により、特権ユーザの数は増え続けています。特にクラウドについて見ると、こうした特権ユーザの多くは、実際には従来の IT スタッフのメンバーではない可能性もあります。たとえば、サービスベースの製品を購入している事業部門の責任者の例について考えると、最悪の場合、従来の IT およびセキュリティ組織は脅威にまったく気づいていないこともあります。

また、多くの特権ユーザは実際にはユーザではなく、人間ではないというケースも増えていることを忘れてはいけません。クラウドや仮想化環境では、スクリプトやプログラムで動く自動化された構成やプロビジョニング・ツールの出現によって、インフラストラクチャの大部分への重要なアクセスと権限を持つ「ユーザ」がさらに多く導入されています。こうした自動化システムの起こりうる帰結として、データベースあるいはその他のアプリケーションやシステムなどのリソースへの管理アクセスや機密アクセスを必要とするオペレーションによって何年にもわたり蓄積した、無数のスクリプトやプログラムが発生していることがあります。いずれの場合も、こうしたアクセスやオペレーションは認証によってかなり適切に制御できます。必要とされているクレデンシャルは残念ながら通常、アプリケーションまたは構成ファイルにハードコードされていますが、そこでは簡単に内部や外部の悪意あるユーザの標的になってしまいます。

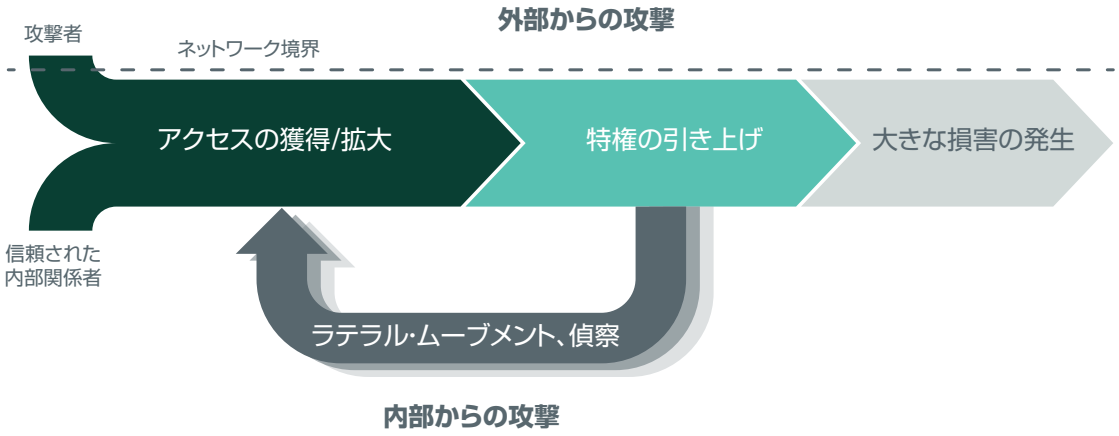
最後に、そしておそらく最も重要なことですが、私たちはここで特権ユーザについてのみ話しているのではなく、それに伴い一般的な組織に存在するすべての特権アカウントとクレデンシャルについても話しているということです。攻撃者がデータ漏えいを実行する上でクレデンシャルを利用することは重要な役割を果たしているため、クレデンシャルは最も重大な脅威をもたらしているといえます。

## キル・チェーンの導入 — それが機能する理由

データ漏えいのキル・チェーンは、攻撃者が首尾よく目標を果たすために達成しなければならない一貫した予測可能な一連の手順で構成されます。一部のキル・チェーンは複雑すぎて説明が難しいものもありますが、一般的なデータ漏えいキル・チェーンに伴う鍵となるステップについて簡単に示します。

**図 C**

キル・チェーンの簡単な例




4 つの鍵となるステップは以下のとおりです。

- **アクセスの確保：**まず、ネットワークへのアクセスを獲得する必要があります。正規の内部関係者または信頼されているサードパーティの場合、これは簡単です。クレデンシャルを利用してこれまでどおりにアクセスを実行するだけです。しかし、攻撃者にとっても同じことを行うのはそれほど難しくありません。LinkedIn などソーシャル・サイトの人気の高まりによって、組織内でシステムへの特権アクセスを有していると思われる特定の個人を識別し標的にすることは比較的容易になりました。スピアフィッシングがますます高度化しているため、非常に経験豊富な熟練した個人を騙してクレデンシャルを聞き出すことは、攻撃者にとってかつてないほど容易になりました。特にユーザ ID やパスワードなど、あまり高度ではないクレデンシャルの場合は簡単です。
- **特権の引き上げ：**攻撃者はアクセスを獲得すると次のステップとして通常、他の特権クレデンシャルを侵害することによって特権を引き上げます。このステップは 2 つの重要なアクティビティをサポートします。1 つには、攻撃者がマルウェアの変更、無効化、ログ、インストールなどの操作を実行できるようにすることで、これは攻撃者の存在やアクティビティの検出を防ぐために役立ちます。2 つ目はキル・チェーンや偵察、ラテラル・ムーブメントなど、次のステップへの準備を整えます。
- **ラテラル・ムーブメントと偵察の実行：**よほどラッキーな攻撃者でなければ、アクセスを獲得した最初のシステムが最終的な標的であることはあまりないでしょう。攻撃者の目標、つまり支払いカード処理システムや専有データ、個人の記録などはほとんど必ず他のシステム上のネットワークのどこかに配置されています。したがってキル･チェーンの次のステップは、ネットワークの偵察を行い、最終目標により近いシステムやサーバへと移動することです。
- **必要に応じてプロセスを繰り返す：**ここからは単純です。最終目標がどこにあろうと、そこに到達するまでプロセスを繰り返すのです。ここでも、攻撃者は非常に忍耐強く、時間をかけて調査を行い、ネットワークを移動して目的を遂行することが経験からわかっています。データ漏えいに関する公的な報告書では決まって、攻撃者が数か月、ときには数年間にわたって被害者のネットワーク内で作業を行っていたことが示されています。最終的に標的に到達すると、攻撃者はシステムを破壊したりデータを盗むなど、攻撃を遂行します。

残念ながら、そして特に基本的な特権アクセス管理のプロセスやツールさえもない場合、組織が行っているいくつかのことが、攻撃者によるキル・チェーンの実行をさらに容易にしています。以下はよくある間違いです。

- **脆弱な認証**技術をネットワークまたは特定のリソースへのアクセスに使用し、デフォルトの管理アカウントとパスワードを削除しなかったり、シンプルなユーザ ID/ パスワードの組み合わせのような容易に盗まれたり侵害されたりする単純なクレデンシャルを使用している。
- **パスワードと鍵の管理が不十分**で、クレデンシャルが十分な頻度で定期的に変更されていない。何千というリソースを有する組織では、これは大きな問題となる可能性があります。なぜならクレデンシャルを再利用したり、定期的なクレデンシャルの変更を行わないなど不十分なプラクティスに従事することによって、運用上の問題を回避しオーバーヘッドを削減することは魅力的だからです。
- **共有アカウントの使用を許可**している。特に root や admin など強力な権限を持つ特権アカウントの共有を許可している。このプラクティスではクレデンシャルを他のユーザと共有することが容易であるため多くのリスクがもたらされます。任意のクレデンシャルへのアクセス権を多数の個人が有するという事実は、特定の個人がシステム上で任意の作業を行ったことを証明する特定を実質的に不可能にしてしまい、フォレンジック調査やトラブルシューティングを複雑化します。
- **認証とアクセス制御を同じものと考える**。その結果ネットワークの大部分で区分化が不十分になり、個人は一度ネットワークに入ってしまえば、必要以上に多くのリソースを見ることができます。これは偵察やラテラル･ムーブメントを容易にし、攻撃者が最終目標に到達しやすくなります。
- **特権ユーザ･アクティビティの監視と分析の不足**は、多くの問題を引き起こす可能性があります。アクティビティの監視や定期的な分析を行っていない場合、疑わしい、あるいは疑われている動作を見逃す可能性があり、攻撃者は自由に動き回れます。また、自分の動作が検出される可能性が低いと知っていれば、規則を曲げたり破ったりするのは人間の本質でもあります。

## 推奨事項：キル・チェーンの分断

特権アクセス管理は幅広いレベルで 3 つの鍵となるステップにグループ分けされ、キル・チェーンを分断する複数の手段を提供し、攻撃者を阻止して漏えいを防止します。

### ステップ 1 — 不正アクセスの防止

リソースへの特権アクセスをネットワークベースのゲートウェイを介して行うよう強制することは、強力な認証を実施する簡単な方法です。このようなシステムを既存のアイデンティティ管理インフラストラクチャに統合すべきであるのは、当然のことです。つまりシステムは Active Directory や LDAP ディレクトリ、あるいは一部の環境では RADIUS や TACACS+ などを含め、既存のアイデンティティ・ストアへのリンクをサポートする必要があります。システムはローカル認証をサポートすることが可能であり、サポートすべきですが、通常、企業にはすでに定着したアイデンティティ・ストアがあります。これらのシステムはすでに正規のユーザ、役割、権限を定義済みであるため、企業は特権アクセスの基盤としてそのデータを活用したいと考えるのが自然です。

しかし、これは土台に過ぎません。正規のユーザのクレデンシャルを盗むことは比較的容易であるため、このようなゲートウェイを通り抜けることは攻撃者にとって比較的簡単な手順である可能性があります。これを防ぐには、特権アクセスへの多要素認証（MFA）の使用を義務付けることが重要です。MFA の追加は、攻撃者がネットワークへのアクセスを獲得する際の難易度を大幅に引き上げます。かつては、MFA はコストが高く、管理上も手間のかかるテクノロジでした。しかしテクノロジの進歩によって多要素認証テクノロジの実装にかかるコストは大幅に変化しており、特権アクセスに伴うリスクの高さを考えると、基本的なコスト・メリット分析でもこの実装は支持されるでしょう。

また多要素認証の使用は、コンプライアンスと監査上の問題にもなっています。米国政府はこれに早くから取り組み、システムへの管理アクセスにいわゆる PIV/CAC カードの使用を義務付ける基準を作成しました。PIV は「privileged identity verification（特権アイデンティティ確認）」（民間企業向け）、CAC は「common access card（共通アクセス・カード）」（軍隊向け）を略したものです。これらのカードは個人の PKI ベースの ID を提供し、アイデンティティ検査と組み合わせることで、ユーザ・アイデンティティの高レベルな確認を行えます。また、たとえば Payment Card Industry Data Security Standard（PCI-DSS）への最新の改訂を含め、同様の標準がさまざまなコンプライアンス要件に追加されました。

その他の、不正アクセスのリスクを軽減するために使用できる一般的な方法には、ユーザ・ログインのソース IP アドレスや時刻に基づくシステムへのアクセス制限があります。このような種類の制御は、特権アクセス管理ゲートウェイと、特定のサーバまたはリソースに対するエージェントベースの制御を介して実施できます。任意のユーザが特定の期間中に、または任意の一連の場所から定期的にログインしている場合も、無制限のアクセスを許可する理由はありません。また、アクセスが予期されない、あるいは許容できないアドレス範囲からのログインは、完全にブロックしたいと考える場合があるでしょう。

この問題の 2 番目の側面は、実際に管理対象のシステムへのアクセスに使用されるクレデンシャルを保護することです。すでに説明したように、これらのクレデンシャルは無制限に共有されたり管理が不十分だったりするなど、保護が不十分なことが非常に多く、明白なリスクをもたらしています。特権アクセス管理システムは、偵察の目や悪意あるユーザを避けてパスワードと鍵のペアを保管し暗号化できるクレデンシャルの金庫を提供する点が理想的です。クレデンシャルの金庫は実際に積極的にクレデンシャルを管理する機能をサポートする必要があり、システムとインタラクションし、組織やリソースのリスク・レベルに適した基準に基づいてパスワードを変更します。このプロセスを自動化することでセキュリティ・リスクが軽減され（数千または数十万というリソースのクレデンシャルを定期的に更新し、同時にクレデンシャルを危険から遠ざけることが可能であるため）、また、パスワードと鍵の自動更新はエラーが起こりにくいため、運用上のリスクも軽減されます。特権ユーザのシングル・サインオンと組み合わせると、関連するクレデンシャルへのアクセス権を実際に提供する必要なくシステムへのアクセス権を提供することが可能であるため、高レベルのセキュリティを実現できます。また、ユーザがクレデンシャルを保有していなければ、そのユーザがクレデンシャルを盗んだり共有したり、あるいは騙されて攻撃者にクレデンシャルを渡してしまうことは不可能になります。

## ステップ 2 — 特権のエスカレーション、偵察、ラテラル・ムーブメントの制限

これはキル・チェーン分断の次のステップです。ユーザがネットワークの偵察を行ったり動き回ったりできないよう制限します。残念ながら多くのネットワークでは、認証はアクセス制御と基本的に同じものに過ぎません。一度ネットワークにログインすれば、ネットワーク全体のリソースにアクセスできることがほとんどです。攻撃者にとってそれは明らかに好都合です。システムからシステムへと移動するための時間を得て、多くの場合手段も手に入れて、標的に近づくことができます。

特権ユーザのシングル・サインオンのような機能は、これらの問題をすべて防止するために役立ちます。このアプローチは基本的に、ゼロ・トラスト・アクセス制御と呼ばれる最小限の特権アクセス制御に基づいています。認証とアクセスを、特権アクセス管理システムと管理対象リソースへの実際のアクセスに分離することで、ユーザはポリシーによって定義され許可されたシステムとリソースのみの可視性を得ます。任意のユーザの職務が、単一のサーバまたは一連のリソースへのアクセスを必要とする場合、ネットワーク上で見ることができるのはそのサーバまたはリソースだけであるべきです。特権アクセス管理システムと管理対象リソースの間のセッションがプロキシやブローカーを介して行われるようにすることで、システムに対する権限を制限したり、発行できるコマンドを制御でき、さらに、特権のエスカレーションやネットワーク内のラテラル・ムーブメントを制限できます。

たとえばセッションがプロキシを介して行われると、標準的なアカウントを使用してユーザをシステムにログ・オンさせることができ、root のような強い権限を持つアカウントを使用することも可能です。システムはコマンド・フィルタを実行できるため、個人を特定のコマンドに制限したり、許可されないコマンドを禁止できます。たとえば、ユーザが一連のサーバ上のソフトウェアの更新作業を割り当てられ、その作業を行うには root としてログインする必要があるとします。コマンド・フィルタを使用すれば、ユーザをログインさせ、職務を実行するのに必要なコマンドのみを許可できます。プロセスを終了させたりシステムを再起動させるなどの他のコマンドを防止できます。

その他の制御によって、ポリシー違反の試みに対する種々の応答が可能です。たとえばユーザが許可されないコマンドを発行したときに、ポリシーによってそのアクションが悪意のないニーズまたは単なる間違いの結果だとみなすことが可能です。このような場合、防止されたユーザとコマンドに対して警告を発行できます。試行が繰り返されたり、もっと重大な違反が起きたときは、セッションを終了させることができます。あるいは、管理者がそのインシデントを詳細にレビューする機会を得るまでユーザのアカウントを無効化することも可能です。

ホストベースのエージェントの追加によっても同様の機能を得られますが、ファイルやディレクトリのアクセスを厳密に制限したり、変更対象のファイルを監視する機能など、もっと粒度の細かい制御が中心になります。ネットワーク内でのラテラル・ムーブメントを防止することも可能です。たとえば、システムへのアクセスに成功した後、攻撃者は SSH または TELNET コマンドを発行するか、ターゲット・システムへのリモート RDP セッションを開始しようとすることがあります。この場合も、特権アクセス管理システムがポリシーを確認して、そのアクティビティが許可されるかどうか判断できます。許可されないと判断した場合、コマンドは阻止され、違反の試行が記録されます。

## ステップ 3 — 監視、記録、監査アクティビティ

特権アクセス管理システムが構築し実施する多数の制御とチェックによって、データ漏えいキル・チェーンを分断するチャンスが豊富に提供され、攻撃者が最終目標に到達できるような地点まで行き着けないことが理想的です。監視、記録、監査アクティビティという最後のステップは、侵害のさらなる抑止として機能し、また、漏えいが最終的に成功した場合にも重要なメリットを提供します。

前述しましたが、自分のアクティビティが記録され分析されることを知っていることは、不正や悪意はないがリスクの可能性がある行為、システムの調査などに対する強力な抑止力となります。詳細なログ記録、警告、レコード、レポートなどの機能は、疑わしいユーザや異常な動作について他の管理者やマネージャ、監査担当者にアラートを発する「早期警告システム」を提供します。アラートとイベントはポリシー違反や漏えいの試行について即座の警告を提供するため、迅速な対応を可能にします。ログは疑わしいイベントへの詳細な手がかりを提供する他のシステム・アクティビティのコンテキストで、個別に、またはログ管理システムや SIEM システムを介して分析され、漏えいが起きる前に調査できます。

共有管理アカウントは一般的に使用されていることが多いため、このようなアカウントを使用して行われたアクションの実行者として特定の個人を割り出せることは、コンプライアンス上不可欠な要件です。

最後に、セッション・レコーディングはいくつかのメリットを提供します。管理者も間違いを犯すことはあります。セッション・レコーディングはそのような場合に役に立ちます。アクティビティをレビューでき、インタラクション中にどのようなアクションが行われたか正確に判断できるからです。これによって、システムに問題が発生した場合などのトラブルシューティングを迅速化できます。前のシフトで更新や構成の変更が行われた場合、その内容を正確に判断することは難しく時間もかかる場合があります。セッション・レコーディングを使用すれば、即座にプレイバックでき、迅速な復旧が可能です。また、ミスが起きたポイントと、望ましい一連のアクションを容易に指摘できるため、トレーニングにも役立ちます。

最悪のケースとしてデータ漏えいが成功した場合、システムに何が行われたか、どの情報が盗まれたか、リソースがどのように侵害されたかを正確に判断するために、このようなレコードとログはきわめて重要です。これらはすべてフォレンジック調査を迅速化し、損害の評価に役立ち、将来の漏えいリスクを軽減するために使用できる価値ある情報を提供します。

## メリット

残念ながら、データ漏えいが行われ、それに伴うコストと損害が発生していることは厳然たる事実です。しかしこれまで示したように、攻撃者はこうした攻撃を遂行するために明確で予測可能な一連のアクションを実行します。特権アクセス管理は、攻撃者が攻撃の鍵となる構成要素を実行するのをアクティブに防止する多数の機能や制御を提供して漏えいのキル・チェーンを分断し、また、攻撃が成功した場合のリスクの軽減、損害の最小化、復旧の迅速化に役立つ追加のサポートを提供します。包括的な特権アクセス管理ソリューソンを実装することで、以下のようなメリットを得られます。

- **リスクの低減：**不正なアクセスを防止し、ネットワークへのエントリが許可された後は、リソースへのアクセスを制限します。パスワードその他のクレデンシャルを不正な使用や侵害から保護します。ユーザがシステム上で実行できるアクションを制限し、不正なコマンドの実行を防止し、ネットワーク内でのラテラル・ムーブメントを防止します。
- **説明責任の向上：**共有アカウントが使用されている場合でも、ユーザ・アクティビティの実行者を完全に把握します。包括的なロギング、セッション・レコーディング、ユーザの警告によってアクティビティをキャプチャし、不正な動作に対する抑止力を提供します。
- **監査の改善と、コンプライアンスの促進：**新しい認証およびアクセス制御要件に対応することでコンプライアンスを簡略化し、ネットワークの論理区分を使用してコンプライアンス要件の範囲を制限します。
- **複雑性の低減と、オペレータの生産性の向上：**特権シングル・サインオンはリスクを制限するだけでなく、管理する必要があるシステムやリソースへの管理者のアクセスをより容易に迅速にすることで、個別の管理者の生産性を向上させます。一元的なポリシーの定義と適用によって、セキュリティ制御の確立と適用を簡略化します。

## まとめ

- 特権アイデンティティ、アカウント、クレデンシャルは企業にとって中核を成すきわめて重要なアセットであり、特権アクセス管理が可能にするテクノロジとプロセスの組み合わせによって高度な保護を行う必要があります。
- その保護を提供することはデータ漏えいのキル・チェーンの分断に役立ち、攻撃を防止し、攻撃が起きた場合のインパクトを軽減します。
- ゼロ・トラスト・アクセス制御モデルは、ユーザやプログラムなどあらゆるタイプの特権アクセスにとって重要です。
- セキュリティに対する境界ベースのアプローチには重大な欠点があることは明らかになりましたが、多層防御は今でもリソース保護の重要な戦略です。特権アクセス管理は、ネットワークとホスト層で特権ユーザ、アカウント、クレデンシャルの周辺に複数の防御層を追加します。
- データ漏えいが増え、攻撃者が高度化する中、漏えいの検出とそれに対する対応にのみ集中するという考えは非常に魅力的であり、またそれが奨励される場面もよくあります。しかしそれは間違いです。検出と対応は重要なアクティビティですが、特権アクセス管理があれば、そもそも企業がデータ漏えいを防止できる能力が大幅に向上することを覚えておく必要があります。

## 著者について

Dale R. Gardner はエンタープライズ・ソフトウェアの分野で 20 年以上の経験を有し、ネットワークとシステムの管理のほか、アイデンティティ管理、アプリケーション・セキュリティ、脆弱性管理、コンプライアンス、ネットワーク・セキュリティなどセキュリティの多くの分野に携わってきました。リサーチ・アナリストやライターとして、企業の情報テクノロジ・インフラストラクチャの運用を改善し、整合性と信頼性を確保するために役立つ多数の管理ソリューションやセキュリティ・ソリューションの定義、構築、マーケティングを行いました。現在は、CA Technologies 特権アクセス管理製品ポートフォリオのグローバル・マーケティングを担当しています。



1 Intel Security および Center for Strategic and International Studies、「Net Losses: Estimating the Global Loss of Cybercrime, Economic Impact of Cybercrime II」、2014 年 6 月、http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

2 World Economic Forum および McKinsey & Company、「Risk and Responsibility in a Hyper-connected World」、2014 年 1 月、http://www3.weforum.org/docs/WEF_RiskResponsibility_HyperconnectedWorld_Report_2014.pdf

3 Eric M. Hutchins、Michael J. Cloppert、Rohan M. Amin, Ph.D.、Lockheed Martin Corporation、「Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains」、http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

4 Andras Cser、Forrester Research、「Critical Questions to Ask Your Privileged Identity Management Solution Provider」、2014 年 9 月 10 日

5 Ars Technica、「AWS console breach leads to demise of service with 'proven' backup plan」、2014 年 6 月 18 日、http://arstechnica.com/security/2014/06/aws-console-breach-leads-to-demise-of-service-with-proven-backup-plan/

6 Brian Krebs、「China To Blame in Anthem Hack?」、2015 年 2 月 15 日、http://krebsonsecurity.com/2015/02/china-to-blame-in-anthem-hack/

7 Anmol Singh および Felix Gaehtgens、「Twelve Best Practices for Privileged Access Management, Gartner」、2015 年 10 月 8 日、G00277332

 CS200-162063_1115