ホワイトペーパー：**2017 年 8 月**

クラウドとモバイルの世界におけるサイバーハイジーンの基本原則

vmware®

目次

はじめに

サイバーセキュリティは、世界各国の政府機関と企業にとって最高レベルの懸念事項となっています。議員、CEO、取締役をはじめとする組織のリーダーたちは、政府機関や企業における効果的なサイバーセキュリティ戦略の確立に、これまで以上に真剣に取り組んでいます。

サイバーセキュリティへの投資は加速しているにもかかわらず、情報漏えいは依然として頻繁に発生しています。一体なにが原因なのでしょうか。それをどう突き止め、どう対処したらよいのでしょうか。その対策には、新しいガバナンス フレームワークの採用から新しい製品やサービスの導入まで、さまざまな方法論があります。

VMware は、新しいフレームワークの採用や個々の製品の購入だけでは、より効果的な情報セキュリティは実現できないと確信しています。あとから付け足すのではなく、中に組み込むことが必要です。組み込みは、これまで組織にとって実現が困難なものでした。しかし、クラウドとモバイル コンピューティングによってもたらされた新しい機能によって実現可能になってきています。

より効果的なセキュリティ アプローチへと移行するためには、基本的なサイバー ハイジーンの実装と、重要な資産であるミッション クリティカルなビジネス アプリケーションの保護という、2 つのステップを実行する必要があります。

本書では、組織で実施する必要のあるもっとも重要かつ基本的な要素、サイバー ハイジーンの 5 つの基本原則について説明します。これらは新しい概念というよりも、むしろ、より効率的なセキュリティの実現に大きな影響を持つ要素であり、NIST のサイバーセキュリティ フレームワーク（CSF）などの確立されたフレームワークをベースとする、テクノロジー ニュートラルな原則です。過去数年間に、Target、Sony、米国人事局（OPM）などで発生した大規模な情報漏えいについても、これらの原則を確実に順守していれば、結果は大きく異なったと考えられます。

しかし、サイバー ハイジーンの 5 つの基本原則を確実に実装するのは容易なことではありません。多くの組織が何年かけても実現できないままでいます。そのため、VMware は、組織で特に重要と位置付けているミッション クリティカルなビジネス アプリケーションの保護に重点を置いて、セキュリティ対策に取り組むことを提案しています。こうすることで、セキュリティの有効性を大幅に向上させることができます。

本書は、政府機関や企業のリーダーたちが現在のサイバーセキュリティ戦略の問題点を理解し、より効果的なアプローチへと移行できるように支援することを目的としています。サイバーセキュリティの課題に取り組んでいるが、必ずしも技術者ではないリーダーを対象としています。より技術的な情報が必要なセキュリティ担当者向けに、実装に関する具体的な情報を含めた付録も用意しました。

サイバーセキュリティの強化は、政府機関や企業の優先事項となっています。VMware は、クラウドとモバイルのエキスパートとして、サイバーセキュリティの強化に独自の視点で貢献できると考えています。独自の立場から情報セキュリティの課題に取り組み、視点を変えて課題解決を支援できると確信しています。

「サイバー ハイジーン」の定義

サイバー ハイジーンという言葉には、さまざまな意味があります。VMware では、サイバー攻撃から身を守るために組織が備えておく必要のある基本的な要素を表す言葉として使用しています。

これは、もう 1 つの一般的な意味である、インターネット ユーザーが個人のオンライン アクティビティでウイルスに感染しないようにセキュリティを確保することとは異なります。

サイバーセキュリティの難問

セキュリティへの支出は世界的に増加を続けており、2020 年までの複合年間成長率（CAGR）は 8.7 % に達すると予測されています[1]。それにも関わらず、米国における昨年の情報漏えいの件数は史上最高値を記録し[2]、世界各国の企業や政府機関は情報漏えいによって年間約 5,000 億ドルを失っています[3]。なにか原因があることは明らかです。それをどう突き止め、どう対処したらよいのでしょうか。

豊富なガイダンス

サイバーセキュリティが完全ではないのは、情報を保護するために組織が取るべき対策についてのガイダンスが不足しているわけではありません。米国および世界各国には、NIST、ISO、SANS など、広く受け入れられている政府規格や業界標準が数多く存在しており、いずれも広く認められたベスト プラクティスを網羅しています。

圧倒的な複雑さ

現在のアプローチで企業の IT 環境全体に包括的なベスト プラクティスを実装するには、非常に複雑な作業が必要です。管理が必要なセキュリティ ツールが大量にあり、ファイアウォール、ウイルス対策、侵入防止システム、脅威検出システムなど、それぞれのツールに膨大な数のルールがあります。企業のすべてのユーザーとシステムにアクセス制御や情報保護のポリシーを適用するには、すべてのツールとそのルールを設定しなければなりません。ルールの数は数百万にもなることがあり、まさに悪夢のような作業です。

絶えず変化する状況

セキュリティ ツールは一度設定すればよいというものではありません。変化し続けるビジネス活動に対応したり、新たに見つかった脆弱性を保護したりするためには、企業全体でシステムを絶えず更新し続ける必要があります。

達成できない自動化

セキュリティ タスクを自動化するツールをいくつも導入していても、それらのツールを完全に自動で連携させることはできません。保護対象システムにラベル付けする方法がツールによって異なるため、それぞれのツールの機能を連携させることが難しくなっています。

なにか不具合が生じることを恐れて、組織がセキュリティの完全自動化に乗り気でない場合もあります。自動更新を行うと、重要なシステムがシャットダウンされる可能性がある場合などです。パッチがシステムに与える影響についての情報が十分にないこともよくあります。

厄介なアラート対応

セキュリティ アラートへの対応にかかる作業の負担も問題になっています。組織に導入されている多数のセキュリティ ツールが、それぞれ 1 日に数千件ものアラートを発信します。ときには、1 時間で数千件になることもあります。ツールごとに管理コンソールが分かれているため、セキュリティ チームは複数の画面を見なくてはなりません。アラートの優先順位付けが難しく、対応するためにはさまざまな調査が必要です。検出ツールがネットワーク内の不審なアクティビティを検出しても、それによって影響を受けるシステム、リスク レベル、対応措置などの情報が提供されないからです。

組織はセキュリティ機能の実施を人力に大きく頼っていますが、サイバーセキュリティの人材が足りておらず、十分に行われていないのが現状です。

---

[1] 『Worldwide Semiannual Security Spending Guide』、IDC、2017 年 3 月
[2] 『Identity Theft Resource Center (ITRC) Data Breach Report 2016』
[3] 『Net Losses: Estimating the Global Cost of Cybercrime』、戦略国際問題研究所、2014 年 6 月

トレーニングのプロセス

IT プロフェッショナルはシステムに組み込むセキュリティの設計を学び、開発者は最小限のコードセキュリティ スキルを身に付け、システム アーキテクトはセキュリティの成果を保証できるようになる必要があります。コンピューティング、ネットワーク、ストレージに関する知識と同様に、セキュリティに関する基礎的な知識を習得します。

エンド ユーザーは、情報保護に関するリスクと責任について学習します。Web サイトの閲覧や E メールの使用においても、セキュリティの基本事項について理解しておく必要があります。

マイクロセグメンテーション

船で使用されている水密区画のように、IT 環境を小さなコンパートメントに分割して保護します。船は、コンパートメントを使用することで万が一に備えています。船体の一部分にダメージを受けても、被害をそのエリアにとどめることができます。

より効果的なセキュリティを実現するための 2 つのステップ

クラウドとモバイル コンピューティングの進化によって、セキュリティの簡素化と完全自動化が可能になりました。より効果的なセキュリティを実現するためには、サイバー ハイジーンの実装と、ミッション クリティカルなビジネス アプリケーションの保護という、2 つの基本的なステップを実行する必要があります。

ステップ 1：サイバー ハイジーンの基本原則の実装

ここでは、組織で実施する必要のある、もっとも重要かつ基本的な要素について説明します。

基礎：トレーニング

IT プロフェッショナルやビジネス リーダーだけでなく、従業員、サードパーティの契約社員まで、すべての人員にトレーニングを実施する必要があります（サイドバーを参照）。

基本原則

トレーニングを確実に実施することに加えて、次の 5 つの原則に従うことが、より効果的なセキュリティを実現するための鍵となります。

1. 最小限の権限	ユーザーには、業務の実行に最低限必要なアクセスのみを許可し、それ以上のアクセスは許可しません。また、システム コンポーネントには目的の遂行に最低限必要な機能のみを許可して、それ以上の機能は許可しないようにします。
2. マイクロセグメンテーション	IT 環境全体を小さなパーツに分割して保護しやすくし、環境の一部が攻撃を受けても被害を食い止められるようにします（サイドバーを参照）。
3. 暗号化	重要なビジネス プロセスのデータは、すべて暗号化して保存または転送します。暗号化しておくと、情報漏えいが発生して重要なファイルが盗まれても、攻撃者は読み取り不能なデータしか入手できません。
4. 多要素認証	ユーザーやシステム コンポーネントを識別する際には、要求されたアクセスや機能のリスクに応じて、パスワードだけではなく複数の要素を使用します。
5. パッチ適用	システムは定常的に保守し、常に最新の状態にしておきます。 重要なシステムが最新の状態になっていないと、セキュリティに大きなリスクが生じます。

確立された原則

ここで取り上げる基本原則は、新しい概念ではありません。確立された原則に根ざしており、たとえば NIST CSF のさまざまな機能に対応しています（付録 1 を参照）。これらの基本原則は NIST CSF やその他のフレームワークに含まれている項目のほんの一部ですが、シンプルで自動化されたアプローチへと移行するためには不可欠な要素です。

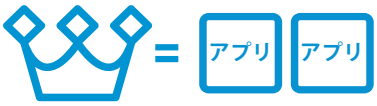
これら 5 つの原則に一貫して従うことで、サイバー攻撃を成立しづらくすることと、攻撃による被害もはるかに小さくすることができます。過去数年間に発生した大規模な情報漏えいについても、これらの原則が確実に実装されていれば、結果は大きく異なるものになったと考えられます（次の表を参照）。

基本原則が効果的に実装されていない状況で発生した重大な情報漏えい

原則	情報漏えいの例 注：情報漏えいには多くの要素が関係します。ここでは基本原則を効果的に実装していなかったために発生した情報漏えいの例を取り上げていますが、それ以外の要因も関係していた可能性があります。
1. 最小限の権限	最小限の権限を付与する仕組みが効果的に実装されておらず、ユーザーに必要以上のアクセス権が与えられていると、ユーザーの認証情報（ユーザー名とパスワード）を盗んだ攻撃者はシステムに幅広くアクセスできるようになります。 Target と Sony で発生した情報漏えいでは、攻撃者が管理者レベルの権限を入手しました。
2. マイクロセグメンテーション	マイクロセグメンテーションが効果的に実装されていないと、ネットワークの一部に侵入した攻撃者は、ほかの部分にも簡単に入り込むことができます。 Target の情報漏えいでは、HVAC システムに侵入した攻撃者は、支払いネットワーク システム内のさまざまな場所にもアクセスできました。Sony の情報漏えいでも、攻撃者はネットワーク内を次々と移動できました。OPM の情報漏えいでは、攻撃者は OPM の LAN へのアクセス権限を獲得した後、内務省のデータセンターにアクセスすることができました。
3. 暗号化	暗号化が効果的に実装されていないと、攻撃者はデータを読み取り可能な形式で盗み出すことができます。 Royal & Sun Alliance Insurance PLC で発生した情報漏えいでは、政府の調査官は同社がデータを適切に暗号化していなかったと結論付けました。
4. 多要素認証	多要素認証（MFA）が効果的に実装されていないと、パスワードを入手した攻撃者は、それを使ってシステムにアクセスできます。 OPM で発生した情報漏えいでは、契約職員のログオンに対して、リスクに見合った MFA を適用していれば、盗んだ認証情報を悪用した攻撃行動を制限できたと考えられます。また、LinkedIn で発生した情報漏えいでは、適切な保護がされていなかった約 1 億人のユーザーのパスワードがハッカーによって公開されました。複数のサイトで同じパスワードを使用するユーザーもいるため、MFA を使用していればリスクを軽減できたでしょう。
5. パッチ適用	パッチ適用が効果的に実装されていないと、攻撃者にシステムの弱点を悪用されてしまいます。 ランサムウェア WannaCry は、ソフトウェアの既知の脆弱性を攻撃しました。パッチは提供されていましたが、適用していなかった組織が被害を受けました。

基本原則を効果的に実装する難しさ

多くの組織のセキュリティ担当者は、これらの原則をよく理解しています。実際、情報漏えいを経験した組織のセキュリティ チームも、これらの実装に取り組んでいました。しかし、多くの組織で採用されている現在のセキュリティ アプローチでは、手に入れられるツールや技術を駆使しても、すべての原則を実装するのは非常に難しいことなのです。



「重要資産 =
重要なアプリケーション」

ステップ 2：重要なアプリケーションの保護に重点を置いた取り組み

次のステップでは、重要なアプリケーションを個別に保護することに重点を置きます。そうすることで、サイバー ハイジーンの基本原則をより効果的に実装できるようになります。

重要なアプリケーションに重点を置くということは、組織の重要資産を重点的に保護するということです。組織の重要資産とは、ミッション クリティカルなビジネスアプリケーションと、それらに格納されているデータです。これには、財務諸表の基になる機密データを処理する財務アプリケーション、個人情報やクレジット カード データを格納するなどの受注処理を行うアプリケーション、従業員の機密データが含まれている人事アプリケーション、企業秘密が含まれている R&D アプリケーションなどがあります。アプリケーションは、データにアクセスしてデータを操作するメカニズムです。

情報セキュリティの目的は、これらの重要資産を保護することです。しかし、現在のアプローチでは、ルータ（ネットワーク上で通信経路を制御するハードウェア）やサーバ（処理を実行するコンピューター）などの IT インフラストラクチャの保護に重点が置かれています。IT インフラストラクチャの保護は必要ですが、それだけでは十分ではありません。

リスクベースのアプローチの採用

ビジネスにとって価値があるのは、重要なアプリケーションとデータであり、これらの資産への不正アクセスは、組織にとって重大なリスクとなります。インフラストラクチャはアプリケーションが必要とするデータや機能を提供しますが、それ自体は重要資産ではありません。

より的確な保護

インフラストラクチャに重点を置いたセキュリティは、的確であるとは言えません。1 つのコミュニティを 1 つのフェンスで囲い、出入口に鍵を付けて、内側にあるすべての家を守ろうとするようなものです。それぞれの家の保護に注目すると、より効果的になります（図 1 を参照）。

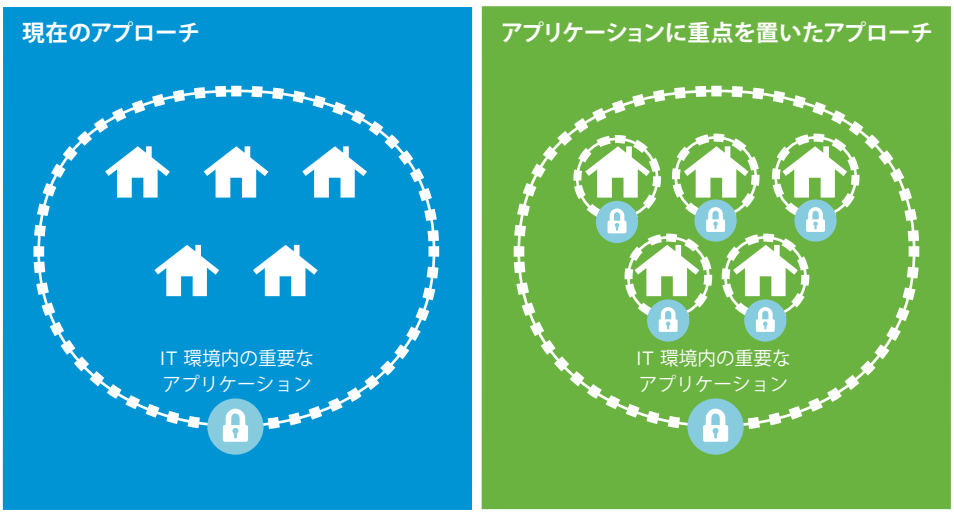


図 1：IT 環境を保護するための現在のアプローチは、1 つのコミュニティを 1 つのフェンスで囲い、出入口に鍵を付けて、内側にあるすべての家を守ろうとするようなものです。それぞれの家（重要なアプリケーション）に注目し、個別にフェンスで囲って鍵を付けると、より効果的です。

各アプリケーションへのアクセスの制御

現在のアプローチでは、最小限必要なアクセスのみを許可するなどのセキュリティ目標を効果的に達成するのは困難です。コミュニティ全体をフェンスで囲むように、企業環境全体の境界にファイアウォールを配置してアプリケーション グループへのアクセスを制御するケースが見受けられますが、対象となるアプリケーションが数千にもなることがあります。そうではなく、個々の家を保護するように、重要なアプリケーションへのアクセスを個別に制御できるようにファイアウォールを配置して、特定のアプリケーション（家）へのアクセスを必要とするユーザーやシステム コンポーネントにのみ許可するようにします。

セキュリティは効率的に運用する必要もあります。出入口にいる警備員が、コミュニティのどこかで異常なアクティビティが発生したことを告げる電話を受けたとします。これだけでは、異常なアクティビティを探してコミュニティ内を一日中見回ることになるかもしれません。どの家で発生したのか、その家は空き家なのか、それとも貴重品がたくさんあるのか、また、通報されたアクティビティがその家では普通のことなのかという情報を警備員が知っていれば、もっと効率よく行動できます（図 2 を参照）。

アプリケーションの具体的な情報を使用した監視

情報セキュリティ監視システムについても、同様のことが言えます。通常、ネットワークまたはネットワークの一部への侵入を示すアラートを送信しますが、アプリケーションに関する具体的な情報は提供しません。そのため、サイバーセキュリティ チームは時間をかけて調査しなければなりません。影響を受けたアプリケーション、影響の重大度、検出されたアクティビティがそのアプリケーションにとって正当なものかどうかがアラートに示されていれば、より効率的な対応が可能になります。

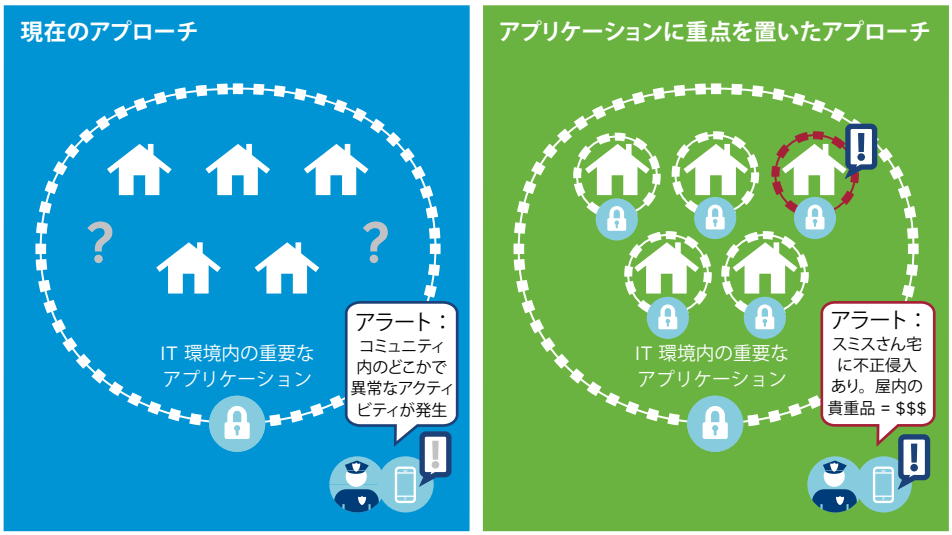


図 2：IT 環境を監視するための現在のアプローチは、コミュニティ内のどこかで異常なアクティビティが発生したことを警備員に通知するようなものです。対象となる家（重要なアプリケーション）や発生したアクティビティの内容を知ることができれば、警備員はもっと効率よく行動できます。

最新のアプリケーション：分散型の動的なシステム

- それぞれのアプリケーションが、複数のコンポーネントからなる 1 つの「システム」です。
- ソフトウェアの機能（またはサービス）は、リソース プールからネットワーク、処理能力、メモリ、ストレージを使用します。
- リソースは IT 環境全体に分散しており、組織の所有するデータセンターと複数のクラウド プロバイダーにまたがって存在する場合もあります。
- リソース プールは複数のアプリケーションで共有されます。
- リソースの使用状況は、時間とともに急速に変化します。

組織で対策が遅れている理由

重要なアプリケーションを個別に保護すればより効果的なセキュリティを実現できるのに、組織でそのような対策が取られていないのはなぜでしょうか。それは、大部分の組織で現在使われているテクノロジーや技術では、こうした対策が取れないからです。

アプリケーション個別の対応ができない現在のアプローチ

従来のアプリケーションは、すべてのコンポーネントを単一の固定マシンに置くことを前提に設計されていました。しかし、最新のアプリケーションは、分散型の動的なシステムとして設計されています。コンポーネントは複数のマシンに分散され、ソフトウェアの機能は時間の経過とともに変化する共有リソース プールを使用します（サイドバーを参照）。現在のアプローチでは、セキュリティ ツールが個々のアプリケーションを認識することはできません。

現在のアプローチでは、セキュリティ ツールに次の制約があります。

- アプリケーション A を構成するコンポーネントを特定できない
- アプリケーション A へのアクセス権が必要なユーザーを特定できない
- アプリケーション A の一部として相互通信を許可するシステム コンポーネントを識別できない
- 別のハードウェア リソースを使用するなどのアプリケーション A の変化を追跡できない

進化を続けるアプリケーション

最新のアプリケーションは小さなソフトウェア機能で構成されており、動的な性質が強くなっています。そのため、インフラストラクチャの保護に重点を置いた現在のアプローチでは、個々のアプリケーションを保護することは困難です。セキュリティを取り巻く状況が厳しくなるなかで、アプリケーションに重点を置いたアプローチへの移行は緊急の課題となっています。

クラウドとモバイル コンピューティングが可能にするセキュリティの向上

クラウド（プライベートおよびパブリック）とモバイル コンピューティングの進化によって、個々のアプリケーションの保護に重点を置いたアプローチに必要な機能が利用できるようになり、より効果的なセキュリティへの道が開かれました。

アプリケーションに重点を置いた機能の使用

クラウドとモバイル コンピューティングによって、次のことが可能になります。

機能 I：個々のアプリケーションを認識し、ベースライン リファレンスを確立する

- アプリケーションを構成するコンポーネントを識別します。
  - アプリケーションの視認性を確保します。
- アプリケーションで想定されている動作と、実行時に実際にどのように動作するかを把握します。
  - アクセスを必要とするユーザーおよびコンポーネントと、それらの相互作用を把握できます。
- リファレンス情報を使用してアプリケーションを保護します。
  - セキュリティ ツールを設定する際にはこの情報を参照します。

機能 II：
システム コンポーネントを個々のアプリケーションに区画（コンパートメント）化する

- 1 つのアプリケーションを構成するすべてのシステム コンポーネントをグループ化します。
- グループに論理境界を設け、グループ内のすべてのシステム コンポーネントを関連付けします。
- 境界を使用して、アプリケーションに一意のラベルを付けます。

機能 III：個々のアプリケーションを保護する

- アプリケーションの周りに設けた境界の出入りを許可する要素を決定します。
- セキュリティ ツールをアプリケーション境界に合わせて調整します。
- ベースライン リファレンス情報を参照し、境界が提供するラベルを使用して、セキュリティ ツールを設定します。
- アプリケーションを個別に保護するための、アプリケーション固有のルール セットを作成します。
- アプリケーションを追跡し、アプリケーションの変化に合わせて保護を調整します。

これらの機能を使用して最新のアプリケーションを効果的に保護する例については、図 3 を参照してください。各機能の詳細と、これらの機能によって可能になる処理については、付録 2 を参照してください。

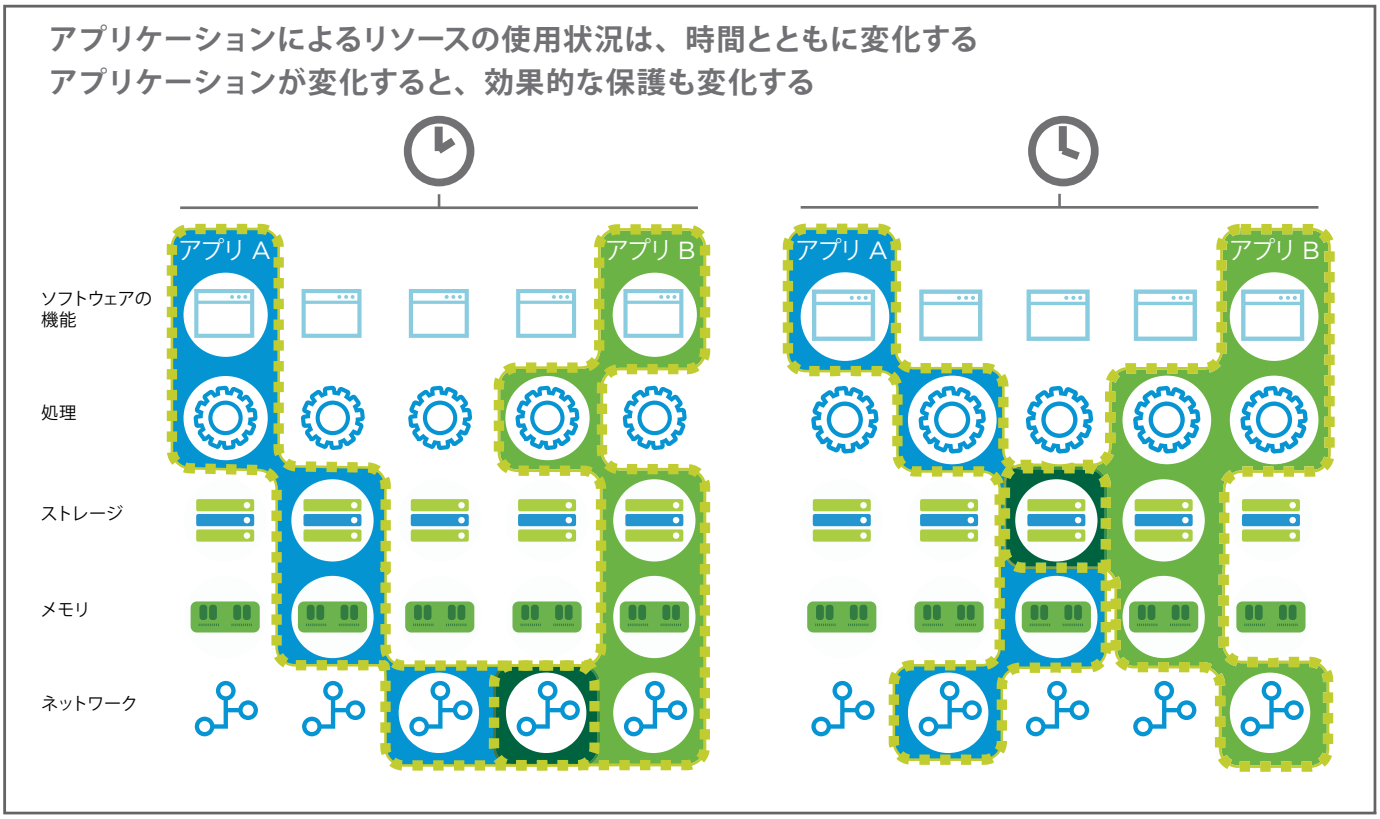


図 3：最新のアプリケーションは分散型の動的なシステムであり、共有リソース プールを使用します。リソースの使用状況は時間とともに変化します。アプリケーションを効果的に保護するには、アプリケーションを構成するすべてのソフトウェアおよびハードウェア コンポーネントを識別してグループ化し、周囲に境界を設け、「アプリケーション X」のようなラベルを付けて、境界の周りに防御を設定する必要があります。設定した境界と防御は、アプリケーションの変化に合わせて調整する必要があります。

基本原則の効果的な実装

アプリケーションに重点を置いたアプローチを採用すると、基本原則を効果的に実装できます。セキュリティがよりシンプルになり、自動化も容易になります。

原則	アプリケーションに重点を置いたアプローチ	実現する効果
基礎：トレーニング	IT プロフェッショナルやビジネス リーダーだけではなく、従業員、サードパーティの契約社員まで、すべての人員を対象に、アプリケーションに重点を置いたトレーニングを実施します。	IT プロフェッショナルやユーザーがアプリケーションを使用するうえで、より意味のあるトレーニングになります。
1. 最小限の権限	ユーザーには、アプリケーションごとに業務の実行に最低限必要なアクセスのみを許可し、それ以上のアクセスは許可しません。システム コンポーネントには、アプリケーションごとに、その目的の遂行に最低限必要な機能のみを与え、それ以上の機能は与えないようにします。	ユーザーのアクセス権とシステム コンポーネントの機能を、より厳密に制御できます。これにより、攻撃者によるアクセス権の取得、プロセスの改変、相互処理（システム間、ユーザーとシステムとの間）のハイジャックがより困難になります。
2. マイクロセグメンテーション	個々のアプリケーションの周りに境界を設けることで IT 環境全体を小さなパーツに分割して保護しやすくし、環境の一部が攻撃を受けても被害を最小限に食い止められるようにします。	IT 環境内での移動が大幅に制限されます。攻撃者が一部分への侵入に成功しても、非常に小さな部分（単一のアプリケーションなど）に限定され、別の部分に移動するのは困難です。
3. 暗号化	重要なビジネス プロセスでは、個々のアプリケーションのコンポーネントによるデータの保存や転送の際に、すべてのデータを暗号化する必要があります。暗号化しておくと、情報漏えいが発生して重要なファイルが盗まれても、攻撃者は読み取り不能なデータしか入手できません。	データのロックおよびロック解除に必要なキーの配布をアプリケーションごとに個別に管理するため、配布が簡素化されます。これにより、暗号化の包括的な実装がより実現可能になります。
4. 多要素認証	ユーザーやシステム コンポーネントの識別は、アプリケーションごとに、単純なパスワードだけでなく複数の要素を使用し、要求されたアクセスまたは機能に関するリスクに見合うものにします。	アプリケーションごとの管理になるため、すべての要求に対してリスクに対応したレベルの多要素認証（MFA）を適用しやすくなります。攻撃者は単純にパスワードを盗んだり推測したりすることができなくなるため、攻撃が難しくなります。
5. パッチ適用	個々のアプリケーションの情報に基づいて、システムを定常的に保守し、常に最新の状態に保ちます。重要なシステムが最新の状態になっていないと、セキュリティに大きなリスクが生じます。	影響を受けるアプリケーション コンポーネントやシステムに及ぶ影響を把握することで、一貫したパッチの適用が容易になり、攻撃者が脆弱なシステムを見つけづらくなります。

アプリケーションの分類

アプリケーションに重点を置いたアプローチを採用すると、セキュリティ チームは、インフラストラクチャ全体に労力を分散させるのではなく、もっとも重要な資産（ミッション クリティカル アプリケーション）に注力することができます。最初にアプリケーションを分類して重要度と優先度を確認することで、もっとも重要なアプリケーションに集中できます。ただし、すべてのアプリケーションに一定のレベルの保護が必要であることを忘れないでください。

既存のセキュリティ ツールの有効性の向上

アプリケーションに重点を置いたアプローチでは、セキュリティ ツールを最大限に活用できます。

- セキュリティ ツールの設定の誤りが少なくなります。
  - ルール セットが簡素化され、アプリケーションごとにそのアプリケーション固有のルールが適用されます。
- 各セキュリティ ツールが連携するように設定します。
  - ファイアウォール、ウイルス対策、侵入防止システム、脅威検出システムなどのすべてのセキュリティ ツールが、同じラベル（アプリケーションの境界）を使用して保護対象の資産を識別します。
- アラートの解釈と対処がより簡単かつ迅速になります。
  - セキュリティ ツールが発するアラートには、該当するアプリケーションと、優先度や可能な措置の情報が付随します。
- セキュリティ ツールをより高度に自動化して使用します。
  - セキュリティ ツールの機能（保護、監視、応答の各アクティビティ）をアプリケーションごとに連携させることができます。
- セキュリティに関するコストが削減されます。
  - 生成されるアラートの数が少なくなり、調査にかかる時間が短縮されます。

セキュリティの設計

通常、セキュリティは「追加の作業」です。アプリケーション チームがアプリケーションをビルドし、インフラストラクチャ チームがすべてのアプリケーションを処理するための一般的なインフラストラクチャを構築した後、セキュリティ チームにはすべてを保護することが求められます。セキュリティ ツールは、展開はされますが、アプリケーション ファブリックには組み込まれません。

アプリケーションに重点を置いたアプローチでは、アーキテクチャを変更する必要があります。特定のセキュリティ アプライアンスを購入したり、ソフトウェアをアップグレードしたりするだけでは、この変更は実現できません。クラウドやモバイル テクノロジーの特性を活用してセキュリティを強化することが求められます（詳細については付録 3 を参照）。

クラウドとモバイル テクノロジーによって提供されるオーバーレイ アーキテクチャを使用することで、新しいアプリケーションと既存のアプリケーションの両方を対象とするセキュリティを組み込むことができます。データセンターでの実装およびエンド ユーザー コンピューティング向けの実装に関する推奨事項については、付録 4 および 5 を参照してください。

まとめ

サイバー ハイジーンの基本原則の効果的な実装と、アプリケーションに重点を置いた保護という 2 つの基本的なステップを実行することで、情報セキュリティの有効性を高めることができます。クラウドとモバイル コンピューティングの進化によって、セキュリティの組み込みが実現可能になりました。IT 環境が進化し続けるなか、この新しいモデルを採用することで、情報セキュリティ プログラムの効果を高めるだけでなく、将来の変化への対応も可能になります。

付録 1：基本原則と NIST CSF の対応表

サイバー ハイジーンの基本原則は、確立された原則に根ざしています。たとえば、NIST のサイバーセキュリティ フレームワークの各機能に対応しています（下表を参照）。これらの基本原則は NIST CSF やその他のフレームワークでカバーされている項目のほんの一部ですが、よりシンプルで自動化されたアプローチへと移行するには不可欠なものとなっています。

基本原則	NIST CSF のサブカテゴリ
基礎：トレーニング	PR.AT：組織の社員およびパートナーは、サイバーセキュリティに対する意識向上トレーニングを受け、関連するポリシー、手順、合意内容に従って情報セキュリティ関連の職務を実行できるように適切に訓練される。
1. 最小限の権限	PR.AC-4：最小限の権限と職務分離の原則に則って、アクセス権限と承認が管理される。 PR.PT-3：最小限の機能を提供する原則に則って、基本的な機能のみを提供するようにシステムが構成される。 PR.IP-1：適切なセキュリティの原則（最小限の機能を提供する概念など）に則って、情報テクノロジー / 産業用制御システムのベースラインとなる構成が作成され、維持される。 DE.AE-1：ユーザーおよびシステムを対象とした、ネットワーク運用および予期されるデータ フローのベースラインが確立され、管理される。
2. マイクロセグメンテーション	PR.AC-5：ネットワークは整合性が担保され、必要に応じて分離される。
3. 暗号化	PR.DS-1：保存データが保護される。 PR.DS-2：送信中のデータが保護される。
4. 多要素認証	PR.AC：物理資産と論理資産、関連する設備へのアクセスは、承認されたユーザー、プロセス、デバイスのみに限定され、承認されたアクティビティおよびトランザクションに対する不正アクセスのリスク評価に従って管理される。 PR.AC-1：承認されたデバイス、ユーザー、プロセスに対して、ID および認証情報が発行、管理、検証、無効化、監査される。 PR.AC-6：ID は検証されて認証情報にバインドされ、相互処理の際に必要に応じてアサートされる。
5. パッチ適用	PR.IP-3：構成変更の管理プロセスが設けられている。 PR.IP-7：保護プロセスが継続的に改善される。 PR.IP-12：脆弱性管理計画が作成され、実装される。 ID.RA-1：資産の脆弱性が特定され、文書化される。 DE.CM-8：脆弱性スキャンが実行される。

注：以降の付録では、アプリケーションに重点を置いた新しいセキュリティ アプローチを組織内に実装する責任を負う担当者などに役立つ情報を提供します。

付録 2：アプリケーションに重点を置いた機能の詳細

以降のセクションでは、本書の 10 ページで紹介した、アプリケーションに重点を置いた機能の技術的な側面について、詳しく説明します。

機能 I：アプリケーションを特定し、ベースライン リファレンスを確立する

組織内の重要なアプリケーションをセキュリティの観点からより深く理解し、アプリケーションを構成するコンポーネントを確認できます。たとえば、どのサービス（ソフトウェアの機能など）が、どのサーバ上で実行されている必要があるか、どのリソースが使用されているか、コンポーネント同士がどのように相互作用するかなどを確認できます。

重要なのは、次に示すような、アプリケーションで意図される動作を把握することです。

- 実行されているべきコンポーネント
- 許可されている相互処理
- コンポーネント間の通信方法

アプリケーションは動的な性質を持っているため、アプリケーションが変化したり、開発者によって更新されたり、運用中に実行されたりしたときに、組織がそれを追跡できる必要があります。たとえば、実行中のインスタンスの数を把握できる必要があります。

この機能によって実現できること

- ベースライン リファレンスを活用して、アプリケーションを効果的に保護する
  - アプリケーションを理解し、保護方法を知ることができます。
  - アプリケーションに関する信頼できる単一の情報源を使用して、アプリケーションのすべてのセキュリティ制御を構成できます。
    - 制御を保証および監査するチームも、このリファレンスを使用して制御を評価できます。
- 厳格でありながら運用上妥当である（プロセスを壊さない）ように、権限を調整する
  - アプリケーションの構成要素に最小限必要な機能と相互処理を判断するために必要な情報を把握し、アプリケーション自体に対する最小限の権限の環境を作成できます。
  - 個々のアプリケーション内、および個々のアプリケーションに対して、システムコンポーネント間で最小限必要な通信を判断するために必要な情報を把握できます。
    - これにより、攻撃対象領域が大幅に縮小されます。
- アラートがより実用的になる
  - セキュリティ ツールからのアラートでアプリケーションを特定できるため、セキュリティ チームはリファレンス情報に基づいて、対応にどの程度の労力がかかるか、どのように優先順位を付けるか、どのような修正オプションがあるかを判断できます。

実用性

これまではアプリケーションの可視化が難しく、運用状態を把握するのは困難でしたが、新しいテクノロジーによって簡単に把握できるようになりました。

既存の多くのアプリケーションについては、ネットワーク上のトラフィックを監視して、アプリケーションを構成するコンポーネントとそれらの相互作用を理解できるようにするテクノロジーが開発されています。

新しいアプリケーション アーキテクチャについては、DevOps の手法によってビルド プロセスが自動化され、アプリケーションを構成するすべてのコンポーネントが開始時点から追跡されます。

DevOps の実現

新しいアプリケーションは、DevOps の手法とテクノロジーを使用することで、迅速かつ頻繁にビルド、テスト、展開できます。

これにより、リード タイムが長く、アジャイル アプリケーションやアジャイル開発プロセスでは機能しない、手動のセキュリティ レビュー プロセスやセキュリティ テスト プロセスから解放されます。

効果的なセグメンテーション

ネットワーク セグメンテーションの従来のモデルは、サーバのタイプ（Web サーバかデータベース サーバか）などの属性に基づくものでした。アプリケーションが単一のサーバ セグメント内ではなく複数のセグメントにまたがって動作するようになったため、これまでのモデルではアプリケーション間での水平方向への移動を効果的に抑制できず、攻撃者がセグメントを跳び越えて移動できてしまいます。アプリケーションを効果的に保護するには、アプリケーションの周りに境界を設けて、ネットワーク制御ポイントを設定する必要があります。そこからアプリケーションの各部分に出入りするすべてのトラフィックを制御および監視します。

- 信号対雑音比（SN 比）が改善される
  - 厳密に制御されたシステムでは、不正なアクセス、機能、相互処理が発生する可能性が大幅に低くなり、アラートの数も少なくなります。
  - アラート数の減少により、ノイズと誤報アラームが減って信号がより明確になります。
- 脅威を絶えず追跡する必要性がなくなる
  - 脅威は変化し続けますが、このアプローチでは、新たな脅威を事前に理解する必要はありません。
- セキュリティ チームとアプリケーション チームの緊密な連携が促進される（サイドバーを参照）
- スケーラブルに実装する：最初はいくつかの重要なアプリケーションにフォーカスする
  - 比較的少ないコンポーネントで構成され、特定のジョブを実行する重要なアプリケーションから開始します。たとえば、「この Web サーバはアプリケーション X の一部であり、このプロセスのみを Y に通信する必要がある」などを確認します。

機能 II：システム コンポーネントを個々のアプリケーションにコンパートメント化する

前述したリファレンス情報を使用して、個々のアプリケーションを構成するシステム コンポーネントを確認してコンパートメント化し、システム コンポーネントの周りに論理境界を設けます。この境界を使用すると、アプリケーションを一意に定義してラベル付けできます。また、1 つのアプリケーションがセキュリティ侵害を受けた場合でも、その単一のアプリケーションに攻撃が制限されます。

この機能によって実現できること

- アプリケーションにポリシーを効率的に適用できるように、単一のゲートウェイを設定する
- ネットワーク内部の脅威に対して、アプリケーションの保護を強化する
  - サーバのタイプなど、インフラストラクチャに基づいたセグメンテーションでは効果がありません（サイドバーを参照）。
- アプリケーションを一意に識別し、ラベルを付ける（サイドバーを参照）
- 1 つのアプリケーションに適用する 1 つのポリシーを作成する
  - アプリケーションを一意に定義し、ラベル付けして、ポリシーを適用できます。
- アプリケーション間での水平移動を抑制する
  - 攻撃者が 1 つのアプリケーションに侵入しても、そこから別のアプリケーションに移動するのは困難です。
- アプリケーション固有の制御をアプリケーションの境界で適用する
  - より重要度の高いアプリケーションに、より高いレベルの保護を適用して、より詳細に検査できます。環境内のどこかに脆弱なシステムがあり、セキュリティ侵害を受けた場合でも、攻撃者が重要なシステムに移動することはできません。

一意の識別子

従来型のセキュリティ制御では、現在もアプリケーションから OS、ハードウェアにいたるまで、スタック全体で同じ固定ラベルを使用しています。しかし、最新のアプリケーションは固定サーバに常駐しないため、この制御方法では対応できません。VLAN 識別子は複数のアプリケーションを分離しますが、アプリケーションごとに一意の識別子は提供しないので、VLAN 識別子では解決できません。より効果的なセキュリティ制御を実現するには、個々のアプリケーションにポリシーを適用する際に一意の識別子を使用する必要があります。

機能 III：個々のアプリケーションを保護する

アプリケーションの境界で提供される一意のラベルを使用して、個々のアプリケーションに適用するセキュリティ制御を構成できます。たとえば、アプリケーションの境界のラベルを使用して単一のアプリケーションを保護するファイアウォールを設定できます。また、リファレンス情報を使用してセキュリティ制御を構成できます。たとえば、リファレンス情報を使用して侵入防止システムを設定し、保護対象のアプリケーションに個別に適用するルール セットを作成できます。

この機能によって実現できること

- ポリシー適用ポイントの位置を最適化する
  - ポリシーは、アプリケーションの境界で適用されます。
- アプリケーションを保護するポリシーを簡素化する
  - たとえば 1 つのファイアウォールで数千ものアプリケーションを保護しようとする現在のアプローチでは、非常に複雑なポリシーを使用する必要がありますが、こうした手間から解放されます（図 4 を参照）。
- 暗号化キーを管理する複雑さが軽減される
  - 複数のアプリケーションではなく、個々のアプリケーションのシステム コンポーネントに暗号化/復号化キーを配布するほうが、はるかに容易です。
- ユーザーとシステム コンポーネントのアクセス対象となるアプリケーション名と、必要な要素とのシンプルなマッピングを使用して、（多要素認証などの）認証ポリシーを適用する
- セキュリティ制御の設定の誤りを回避する
  - 1 つのアプリケーションを保護するように制御が設定されます。
- 境界に制御を追加することで、個々のアプリケーションの保護が強化される
- 複数のセキュリティ制御をシステムとして連携させる
  - アプリケーションの境界を使用してアプリケーションにラベルを付けることで、1 つのアプリケーションに対するすべての制御を同期できます。
- アプリケーションの動的変化に合わせて制御を調整する
  - アプリケーションの移動にあわせて境界上で保護を適用できます。

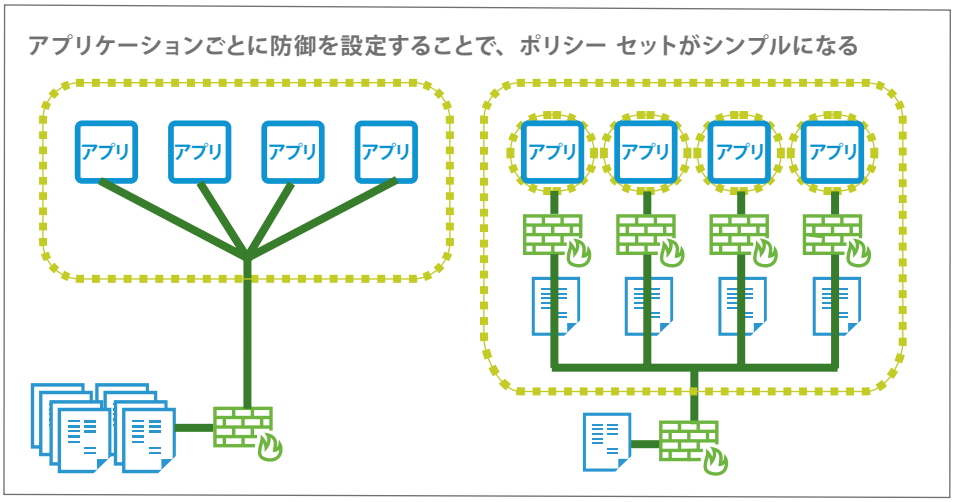


図 4：現在のアプローチでは、通常、境界にファイアウォールを設定して、その境界内のすべてのアプリケーションのあらゆるコンポーネントに出入りするトラフィックにポリシーを適用します。この場合、ファイアウォール ルールは数万にのぼることもあります。ポリシー セットは非常に大きく、複雑です。アプリケーションごとにファイアウォールを設定すると、1 つのアプリケーション内のコンポーネントに出入りするトラフィックのみが対象となるため、ポリシー セットは大幅に小さくシンプルになります。

付録 3：クラウドおよびモバイル コンピューティングの特性

クラウドおよびモバイル コンピューティングの進化によって、アプリケーションに重点を置いた機能（付録 2 を参照）を使用して、情報セキュリティにより効果的なアプローチを実装できるようになりました。

クラウド コンピューティングの特性

クラウドの基本的なファブリックは仮想化で、物理インフラストラクチャとアプリケーションの間に抽象化レイヤーを提供します。	
アプリケーション コンテキスト	仮想化レイヤーでは次のことが行われます。 • 仮想環境内で実行されているすべてのアプリケーションのコンテキスト情報を収集、保護、配布します。 – これは仮想化に本来備わっている機能で、利用可能なリソースにワークロードを移動する、ロードバランシングを実行する、必要に応じてリソースのスケール アップ / スケール ダウンを行うなど、アプリケーションの動的な変化を制御します。 – 環境内のすべてのワークロードとシステム コンポーネントのマッピング情報も格納されており、ワークロードの移動に合わせてマッピングを維持します。 • 独自の視点から以下の状況を確認します。 – 実行中のアプリケーションとそのアプリケーションを実行しているハードウェアとの接続 – アプリケーションのトポロジー • ネットワーク上でアプリケーションを構成するさまざまなシステム コンポーネントの配置 – アプリケーションのプロビジョニング方法と実行時の運用方法
分離	仮想化レイヤーでは次のことが行われます。 • 個別の信頼ドメインを提供します。 – ゲストの視認性を提供しながら、ゲストから分離します。 • アプリケーションの境界を保護するためのセキュリティ制御を配置する、分離された挿入ポイントを提供します。 – ワークロードが別の物理マシンまたはネットワーク リンクに移動されても、アプリケーションの境界を維持します。
不変性	• 仮想化レイヤーを使用することで、不変のコンポーネントをインプレースで更新するのではなく、展開ごとに置き換えることができます。 – 共通イメージを展開ごとにビルドして、テストおよび検証できます。
ソフトウェア ベース	• 仮想化すると、システム コンポーネントの動作がプログラムによって初期化、制御、変更、管理されます。 • マシンの隔離、マシン イメージの再適用、トラフィックの遮断、マシンのスナップショット作成、視認性の強化などを行うことができる、柔軟な制御ポイントです。

モバイル コンピューティングの特性

モバイル コンピューティングでは、デバイスのネイティブ機能を介して独自の機能が提供されるほか、仮想デスクトップの機能やモバイル デバイス管理テクノロジーも提供されます。	
ユーザーとデバイスのコンテキスト	• モバイル コンピューティングで提供されるユーザーやデバイスに関する豊富なデータは、リスクベースの認証およびアクセス制御に役立ちます。次のようなデータがあります。 – ユーザーやデバイスからのデータ • 生体認証データ：指紋、声、画像 • 地理的な位置 • デバイス ID：シリアル番号、証明書 • ネットワーク パラメーター（Wi-Fi、イントラネットなど）および IP アドレス • デバイス構成：ハードウェア、OS、インストールされているアプリケーション • セキュリティの状況：管理対象であるかどうか、セキュリティ ソフトウェア、ジェイルブレイクまたはルート化されているかどうか、ソフトウェア アップデートやパッチのステータス • アウトオブバンド：通話、プッシュ通知 – 条件に基づいたアクセス権 • 複数デバイス：アクセス権を付与する前に、スマートフォンやラップトップの地理的な位置が異なっているかどうかを確認します。 • ユーザー データとデバイス データの組み合わせ：アクセス権を付与する前に、信頼済みユーザーであり、かつ安全なネットワーク上にある管理対象デバイスであるかを確認します。
分離	• 仮想デスクトップは、アプリケーションへの分離接続を提供します。 – ユーザーがアクセスできる対象を、ネットワーク上のすべてのアプリケーションではなく、特定のアプリケーション セットに限定できます。 • 仮想デスクトップは、アプリケーションの使用とデバイスの使用を分離します。 – アプリケーションと、アプリケーションに関連するデータが、モバイル デバイス上に存在しないようにします。モバイル デバイスに表示されるのは、アプリケーションのリモート表示のみです。
不変性	• ノンパーシステント仮想デスクトップは、変えることができません。 – 管理されたマスター イメージから即座に作成され、使用するたびに破棄および再作成されます。この不変性により、攻撃者が永続性を維持するのは非常に困難です。
テレメトリ	• リモートからの監視、ポリシー適用、修正により、次のことが可能です。 – 継続的なアップデートとパッチ適用 – 紛失 / 盗難、チェックインの失敗、またはセキュアな Wi-Fi からのローミング アウトが発生した場合のデバイスの抹消 – 要件を満たさなかった場合のデバイスの隔離またはシャットダウン

付録 4：データセンターでの実装

アプリケーションに重点を置いた機能を組織のデータセンター内に実装する際の推奨事項を示します。

機能	実装の推奨事項
1. アプリケーションを認識し、ベースライン リファレンスを確立する	• 重要なアプリケーションの設定内容やシステム コンポーネント間で想定される相互処理を記録するシステムを作成します。 – アプリケーション チームと連携して、プロビジョニング システムを確認するか、学習 / ベースライン設定または自動化システム / ブループリントを通じて実現できます。 – 問題の特定および診断に不可欠な情報として利用できます。 • コンポーネント、プロセス、それらがネットワーク上で相互作用 / 通信する方法について、アプリケーションのホワイトリストを作成します。
2. システム コンポーネントを個々のアプリケーションにコンパートメント化する	• 仮想ファブリックを使用して、アプリケーションやサービスの周りに論理境界を設けます（マイクロセグメンテーション）。 – その境界を、分散ファイアウォールだけでなく分離された L2/L3 ネットワークも利用して適用し、不連続なアドレス空間を作成します。 – 対象となるアプリケーションのすべてのコンポーネントが、1 つの境界で制御される、分離された単一のセグメントに置かれます。 • 単一の出力ポイントを設定します。 – セグメント内の 1 つのアプリケーションのコンポーネントどうしは、自由に通信できます。 – 限られたサービスのみが境界を越えて通信できます（DHCP、DNS、Active Directory など）。 – アプリケーションの境界は、制御を調整してそれらのサービスからのトラフィックを検査できる、定義済みのポイントです。
3. 個々のアプリケーションを保護する	• 仮想化レイヤーを使用して、アプリケーションに対する制御を調整します。 – Software-Defined Networking とソフトウェアベースのセキュリティ制御により、アプリケーションに個別の保護を設定できます。

付録 5：エンド ユーザー コンピューティング向けの実装

アプリケーションに重点を置いた機能をエンド ユーザー コンピューティング向けに実装する際の推奨事項を示します。

機能	実装の推奨事項
1. アプリケーションを認識し、ベースライン リファレンスを確立する	• アプリケーションが意図した動作を維持するための対策の一環として、エンドポイント デバイス上で、パーシステント アプリケーションではなくノンパーシステント仮想デスクトップを使用します。 – ノンパーシステント デスクトップ イメージを使用すると、ログオフ時にデスクトップ イメージが破棄され、次回のログオン時に新しく作成されるため、オペレーティング システムとアプリケーションを意図した状態に維持できます。 – ノンパーシステント デスクトップ イメージがセキュリティ侵害されても、ユーザーがログオフすることで、その日のうちに攻撃が破棄されます。通常、攻撃者が最初に侵入したマシンからネットワーク経由で攻撃を広げるには数日はかかるため、ノンパーシステント デスクトップを使用することで、攻撃者が最初の攻撃場所から移動するのを阻止できます。 – 攻撃者が環境内に得た足場を維持できないようにします。APT 攻撃（Advanced Persistent Threats）の永続化を防ぐことができます。 • デバイスのセキュリティ コンプライアンスをリアルタイムでチェックし、デバイスがセキュリティ ポリシーに違反しているかどうかを素早く判断して、即座に修正するか、企業リソースへのアクセスを無効にします。
2. システム コンポーネントを個々のアプリケーションにコンパートメント化する	• ユーザーがアプリケーションに接続するプロセスを End-to-End で限定します。 – コンパートメント化されたアプリケーションをエンド ユーザー インフラストラクチャに接続します。 • 仮想デスクトップ インフラストラクチャ（VDI）テクノロジーを使用して、ユーザーが許可されたシステムのみにアクセスできるようにします。 – アプリケーション レイヤーでアクセス制御を行います。 – たとえば、契約社員に、必要なアプリケーションへのアクセスのみを許可します。 • 契約社員が仮想デスクトップにログインすると、1 つのマイクロセグメント（アプリケーション）へのアクセスのみが許可されます。 • VDI テクノロジーとマイクロセグメンテーションを併用して、攻撃者がネットワーク全体に攻撃を拡大するのを阻止します。 – 仮想デスクトップ プラットフォームでマイクロセグメンテーションを使用すると、1 人のユーザーのマシンが（スピアフィッシングなどによって）セキュリティ侵害された場合に、攻撃者がアクセスできるホストを数台のみに制限できます。 • 攻撃者は、攻撃を受けたユーザーが VDI を介してアクセス可能な、限られたアプリケーションにしかアクセスできません。 – VDI でマイクロセグメンテーションを使用すると、分離が容易になります。 • ユーザーの ID に基づくアクセスであるため、ログオンしたユーザーには、ユーザー固有のネットワーク ビューが動的に提供されます。 • あらかじめ複雑で大量なネットワーク マッピングを行う必要も、それぞれ異なる VLAN が関連付けられた複数のデスクトップ プール セットを事前に構成する必要もありません。

	• モバイル テクノロジーとマイクロセグメンテーションを組み合わせて、モバイル アプリケーションやモバイル デバイスがアクセスできるデータセンター リソースを制限します。 – デバイスがデータセンター内のリソースへのアクセスを試みると、そのデバイスの ID に基づいて、ネットワーク内のきわめて限られた部分（特定の IP やポートなど）へのアクセスのみが許可されます。 • VPN の終端をマイクロセグメントの境界にすることで、セキュアな認証によるアプリケーションへの直接接続が可能になります。 – 従来の VPN では終端がネットワークの境界に置かれるため、ユーザーがログインしていったん境界内に入ると、ネットワーク上のさまざまな場所にアクセスできます。
3. 個々のアプリケーションを保護する	• VDI テクノロジーを使用してセキュリティ制御をアプリケーションに直接適用します。 – データセンター内に置かれたアプリケーションにセキュリティ制御を適用するほうが、数千台のデバイスに制御を適用するよりも効果的です。 • BYOD のユースケースでは、OS とアプリケーションのコンテナ化テクノロジーを活用して、企業のアプリケーションやデータを個人のアプリケーションやデータから安全に分離できるため、企業のセキュリティ制御を企業アプリケーションに直接適用できます。 – アプリケーションをサンドボックス化し、暗号化して提供します。 • エンドポイント デバイスから取得したデータを利用して、ID と信頼に関する証拠レベルが、個々の重要なアプリケーションへのアクセス要求のリスク レベルに相応するものであることを確認します。 – たとえば、未知のデバイスを使用してアプリケーションにアクセスする場合は、2 要素認証が求められます。信頼された登録済みのデバイスを使用する場合は、単一要素認証に進みます。このとき、デバイスが 2 番目の要素として機能しています。また、ユーザーが信頼された（社内の）Wi-Fi ネットワークを使用する場合は、単一要素認証へと進みます。このとき、ネットワーク検証が 2 番目の要素として機能しています。 • 単一の重要なアプリケーションへのアクセスについては、位置情報を使用して、リスクに関する決定をリアルタイムで下します。 – ユーザーのラップトップやスマートフォンの位置情報を取得し、ユーザーが地理的に離れた場所にいる場合、リスク レベルに対応して追加の認証プロセスが必要になります。たとえば、スマートフォンにプッシュ通知を送信して認証に使用することができます。 • フェデレーション ID を使用して、認証をよりセキュアなものにし、ユーザーのログオンを簡素化します。 – サードパーティのディレクトリに対するフェデレーション認証では、次のようなセキュアでない処理を回避しています。 • 使用するディレクトリ間の同期 • 複数のパスワードを使用する。これは、ユーザーがパスワードを書き留めたり、同じパスワードをすべてのアプリケーションに使用したりすることにつながります。 • モバイル テクノロジーを使用して、Windows、macOS、iOS、Android、QNX など、デバイスで使用されている OS に関係なくデバイスのセキュリティを自動的に確保します。 – たとえば、デバイスをポーリングしてパッチ不適用などのセキュリティ問題を特定し、パッチを即座にプッシュ アウトして問題を修正します。

本資料は原題「CORE PRINCIPLES OF CYBER HYGIENE IN A WORLD OF CLOUD AND MOBILITY」の翻訳版です。

ヴイエムウェア株式会社 〒105-0013 東京都港区浜松町 1-30-5 浜松町スクエア 13F www.vmware.com/jp

アイテム No. : vmw-0044-wp-cyber-hygiene-A4-102
E:2017/08 J:2018/01