サイバー攻撃の被害は Active Directory で最小化する！

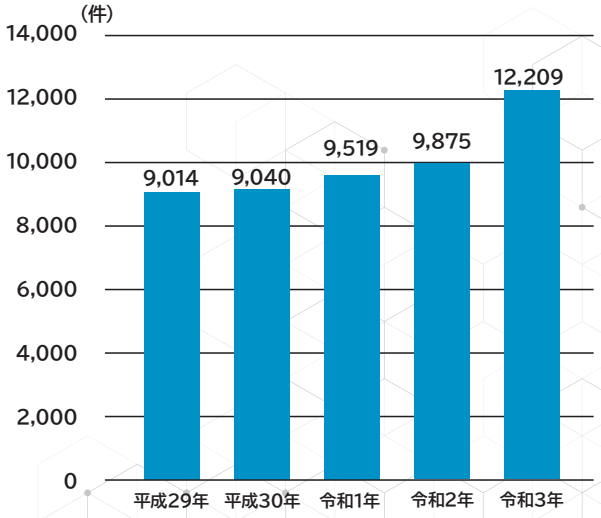
AMIYA

目次

はじめに

年々増え続けるサイバー攻撃。警視庁が発表した「令和3年におけるサイバー空間をめぐる脅威の情勢等について」では、2021年は国内のサイバー犯罪検挙数が過去最多の前年比約24%増であったことが明らかになっています。また、近年急激に進むテレワークやクラウドの導入に伴い、それらの脆弱性を狙った攻撃も増加しています。
新たなワークスタイルの下では、守るべきものは社内にあることが前提のセキュリティモデルでは限界が生じるようになりました。さらには、サイバー攻撃の手口はますます多様化・巧妙化しており、ネットワークへの侵入を防ぐ入口対策に力を入れても、侵入を防ぎきることが難しくなってきています。

サイバー犯罪の検挙件数の推移

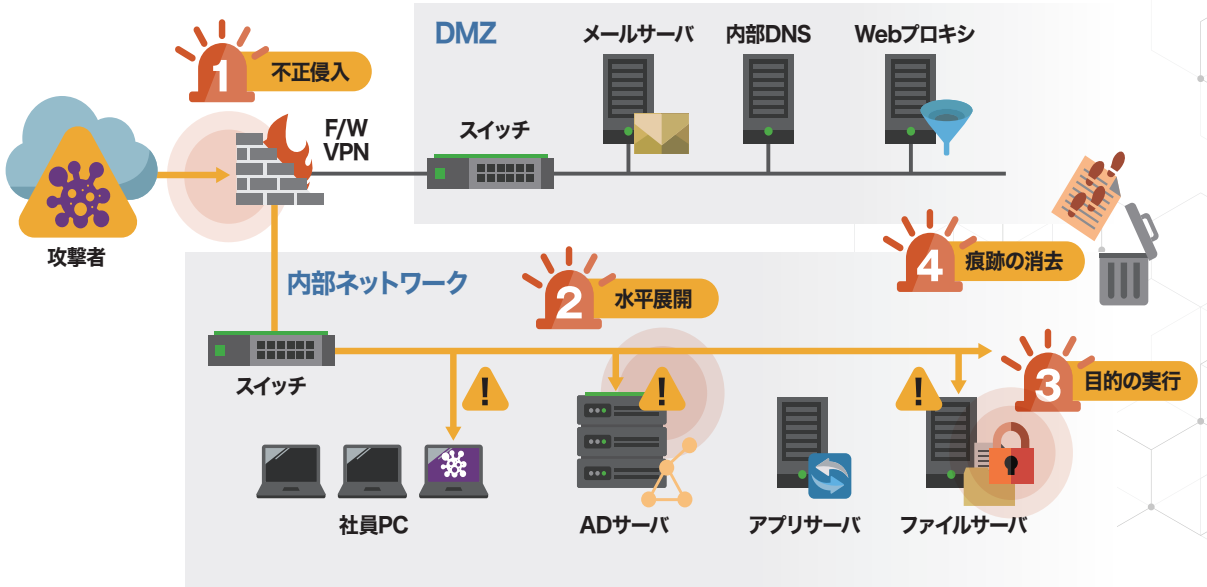


出典：令和3年上半期におけるサイバー空間をめぐる脅威の情勢等について 警察庁
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_kami_cyber_jousei.pdf

このような状況下で、「内部対策」に注目が集まっています。内部対策とは、攻撃者の侵入後の対応にフォーカスし、侵入後の被害を最小限に抑える対策のことです。侵入されてから目的達成までに至る段階で、いかに早期に検知し対処できるかどうかが重要です。
数ある内部対策の中でも特に注目したいのがActive Directoryにおける対策です。Active Directory(以下AD)とは、Windows Serverの機能の一つで、従業員のユーザアカウント管理や、各情報資源へのアクセス権限管理などを一元管理できるもので、企業のITインフラの中枢です。ADは様々な利便性の高い機能を備えているからこそ、セキュリティの観点でも非常に重要です。本書では、あらゆるサイバー攻撃がADを経由することに着目し、内部対策の中でもADをテーマに、ADにおける対策やADのログ管理などを解説していきます。皆様がセキュリティ対策を講じる際に本書が一助となれば幸いです。

サイバー攻撃の流れ

冒頭で述べたように、多様化・巧妙化するサイバー攻撃ですが、
その攻撃の流れには以下のパターンがあります。



1 不正侵入

攻撃者はまず、メールの送付やVPN・RDPの脆弱性悪用により、内部への侵入を試みます。

2 水平展開

内部へ侵入した攻撃者は次に、機密情報へのアクセス権の取得のためにADの環境を調査して、権限昇格を試みます。特権を得ることに成功した攻撃者は、権限を利用して広範囲のシステムにアクセスをして水平展開を進めます。

3 目的の実行

標的となるデータベースやファイルサーバなどに到達すると、目当てのデータを盗んだり暗号化したりして、目的を達成しようとします。

4 痕跡の消去

最後に、攻撃者は自身の攻撃の痕跡の消去を試みる場合があります。

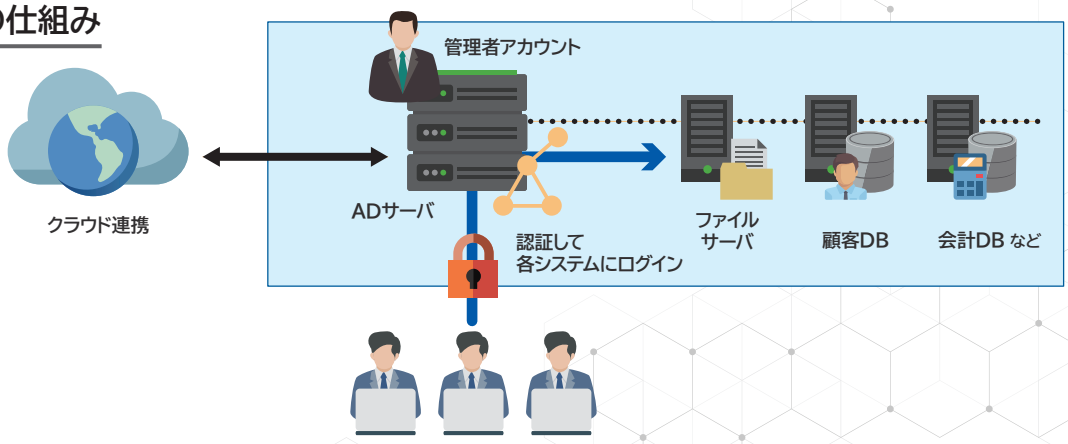
ここで注目したいのが、ADを突破されたら最後、攻撃者は自由に行動できてしまう、という点です。
そのため、攻撃者は目的達成のために必ずADを経由します。

ADが突破されれば実害を受けるのみ!!

全てのサイバー攻撃はADに通ず

攻撃者にとってADはとても魅力的なものです。あらゆる情報資源がADによって一元管理されている環境下では、ドメイン管理者アカウントはADが管理する全ての資源をコントロールすることが可能だからです。そこで、攻撃者はADの脆弱性や端末に保存されたアカウントの認証情報を悪用したりしてAD環境に対して攻撃を仕掛け、より権限の高いアカウントの認証情報を窃取し、それらを用いてシステムを横断的に侵害しようとします。

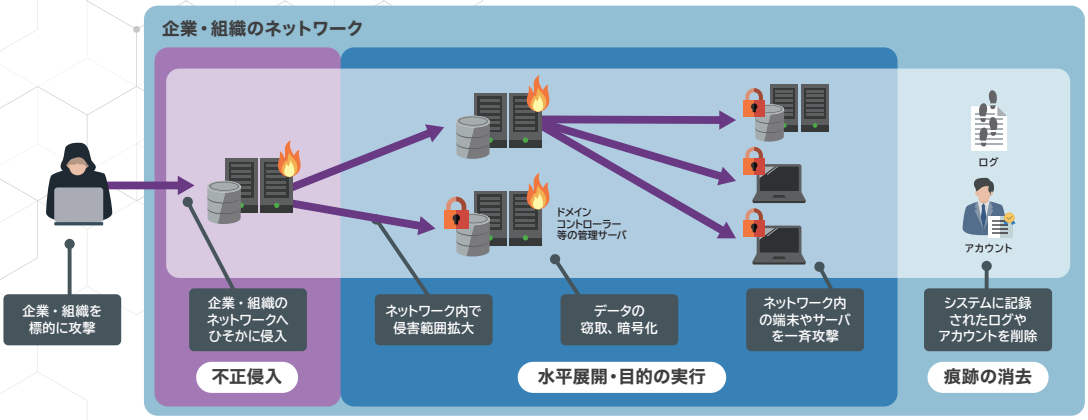
AD認証の仕組み



2021年10月に徳島県の病院がランサムウェア被害に遭ったことは記憶に新しいでしょう。LockBit 2.0と呼ばれるランサムウェアに感染し、患者の診察記録を保管する電子カルテなどのデータが暗号化され、実質的な機能停止に陥るという甚大な被害が生じました。ランサムウェアの代表格であるLockBit2.0の中には、ADを攻撃し、グループポリシーでウイルス対策ソフトを停止させた後にランサムウェアをシステム全体に拡散させる仕組みが搭載されたものもあります。その場合、ADサーバに侵入されたが最後、そこで管理されるシステム全てが被害に遭うことになります。

このインシデントでは、ADの設定に課題があったことが明らかになっています。アカウントロックアウトの設定が無効になっていたり、ドメインユーザーに管理者権限が付与されていたりと、セキュリティ上問題のある設定となっていました。これらの問題がなければ、攻撃の阻止や遅延ができたかもしれません。

LockBit 2.0の攻撃手法



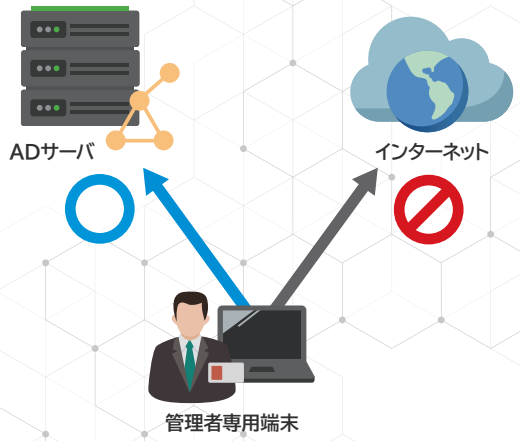
ADにおける7つの対策

では、ADにおいてどのような対策を講じればよいのでしょうか。ここでは、ADに対する攻撃を抑止するための主な対策を7つ紹介します。

一つの対策のみに頼らず、複数の対策を組織の運用状況と照らし合わせて実施すると効果的です。

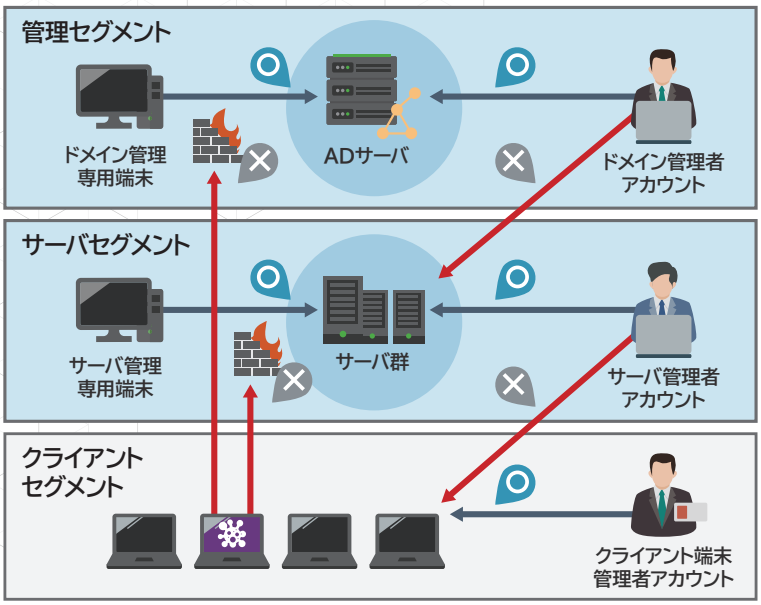
1.管理用端末の設置

ADサーバの管理に使用する端末には管理者アカウントの認証情報が保存されているので、管理者アカウントを狙った攻撃の対象になります。
これらの端末をADサーバの管理専用の端末とし、これらの端末からのインターネット接続やアプリケーションの実行を制限することで、マルウェア感染などのリスクが減ります。



2.セグメント化

コンピューターを用途に応じて別々のネットワークセグメントに配置し、セグメント間での通信の許可を必要最小限にします。さらに、認証情報が窃取された場合の被害を局所化するために、各セグメントで使用する管理者アカウントを別々に設け、各セグメント内のコンピュータとそれらの管理専用端末のみに各管理者アカウントの使用を制限します。それにより、侵害されたコンピューターからのADサーバへの横断的侵害を抑止できる可能性があります。

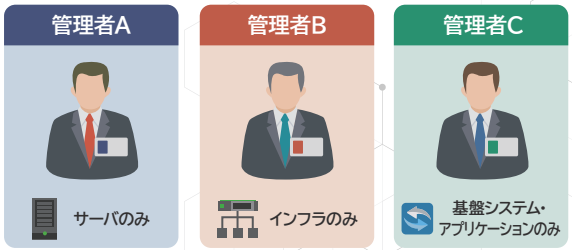


ADにおける7つの対策

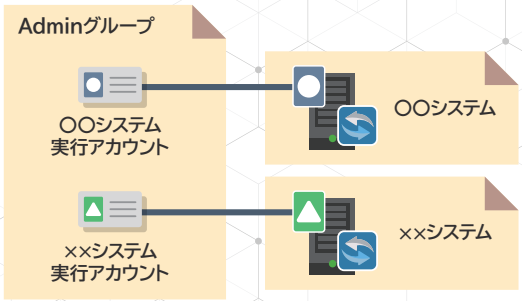
3.特権の最小化

ドメイン管理者権限やサーバの管理者権限などの特権を有するアカウントを最小限にします。業務遂行のためにアカウントに与える必要がある特権を整理し、アカウントの管理画面やグループポリシーなどを使用して最小限の特権だけ付与することで、アカウントを乗っ取られて特権を悪用されたときの被害を最小化できます。

エリアごとに職務分掌/特権の最小化

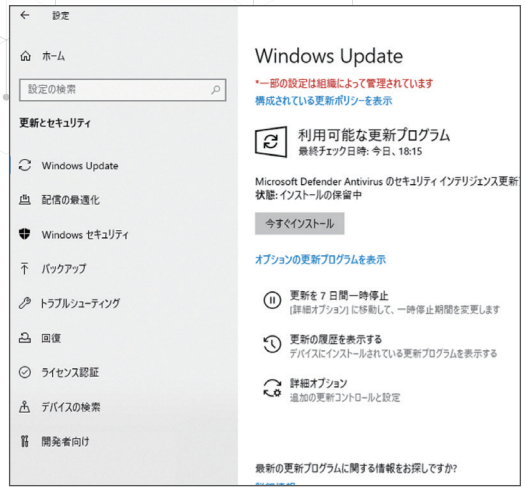


サービス実行用アカウントの分離



4.セキュリティ更新プログラムの適用

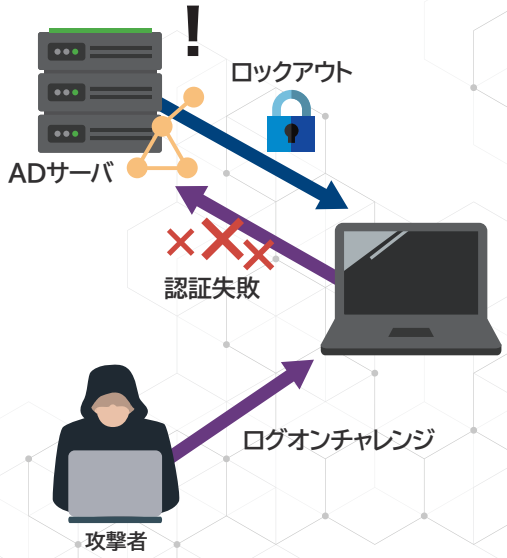
脆弱性の悪用を抑止したり、追加されたセキュリティ　機能を有効にするために、最新のセキュリティ更新プログラムを適用します。



ADにおける7つの対策

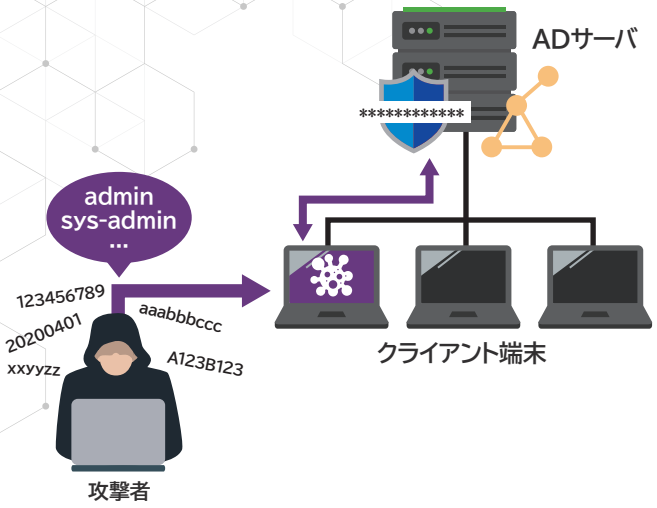
5.アカウントロックアウトの設定

ID、パスワードを連続して一定回数間違えた場合に、ログオンを禁止するアカウントロックアウトを設定します。これによって、ブルートフォース攻撃による被害を受けなくなります。また、ロックアウトの設定によって、ロックアウト自体がイベントログとして記録されるため、外部からの攻撃を検知することが可能になります。



6.適切なパスワード設定

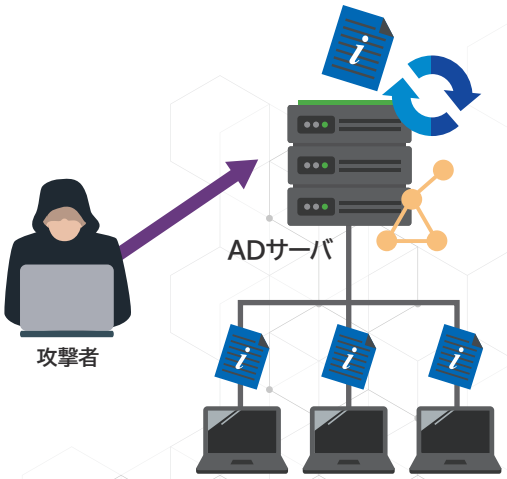
短い単純なパスワードでは、ブルートフォース攻撃などによって攻撃者にパスワードを割り出される危険性が高くなります。サーバの初期状態から存在するビルトイン Administratorは非常に強力な権限を保有するため、特に強固なパスワードを設定し、さらにパスワードを割り出された場合に備えてパスワードの使いまわしを避けます。



ADにおける7つの対策

7.グループポリシーの再読み込み

グループポリシーはサーバ側で設定・配信されるので、サーバ側での設定変更がなければコンピュータは読み込まない設定となっています。そのため、定期的にグループポリシーの再読み込みを行うことで、攻撃者によってグループポリシーが変更されても、強化された設定を取り戻すことができるので、攻撃遅延ができる可能性があります。



重要 攻撃を受けていることに気づくこと！

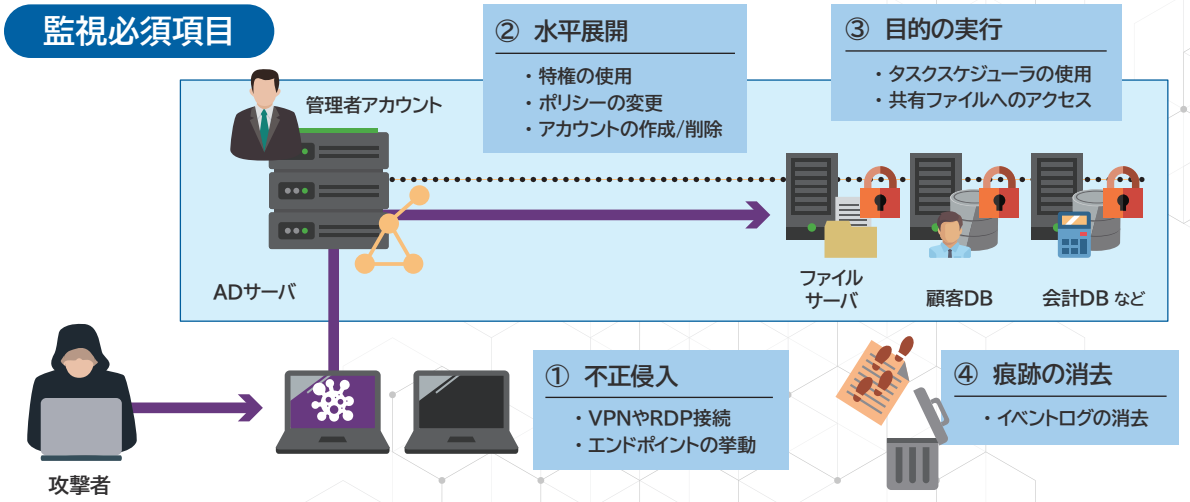
ここまで紹介してきた対策は、ADに対する攻撃を抑制する対策となります。しかし冒頭で述べたように、サイバー攻撃は高度化・巧妙化しており、攻撃者の侵入を防ぎきることが難しくなってきている昨今、このような対策をしていても、攻撃者はこの対策を回避し、目的を達成できてしまうのが実情です。
最も重要なのは、万一侵入された際に、攻撃者による不正侵入、横断的侵害にいち早く気づくことです。そこで活躍するのが**ログ管理**です。

ADのログ管理

ログを取得し、異常な操作を検知できる体制を整えることで、攻撃者による不正侵入、横断的侵害を早期に気づくことができ、その後の対応に移ることができます。一方、ログによるサイバー攻撃検知ができない状況であれば、被害が拡大するまで気づけないことになり、事業継続への多大なる影響を及ぼすことになります。つまり、ログを適切に管理できれば、サイバー攻撃の検知、早急な対応により情報流出などの最悪の事態を回避したり、サイバー攻撃の被害を最小化したりすることが可能になります。また、攻撃の痕跡を調べることもできるので、攻撃の状況や、悪用されたアカウント・コンピュータを把握することができ、適切な対応策を講じることも可能になります。

ログ自体は、Windowsの標準機能で取得可能です。ADのイベントログには、例えばログイン、特権割り当て、チケット要求などの認証に関連するログが記録されるため、悪用されたアカウントや横断的侵害を受けた端末の情報を調査する手掛かりになります。

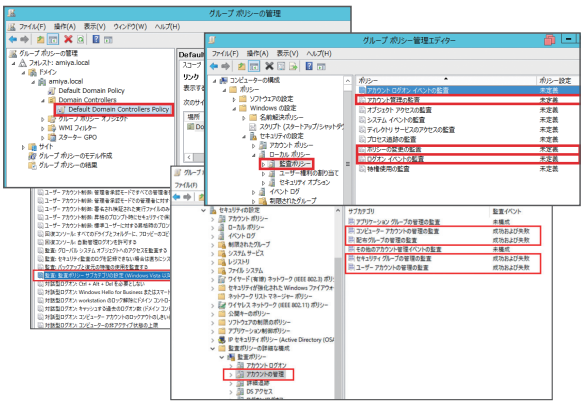
ここからは、ADに対する攻撃や管理者アカウントの悪用を検知するために最低限監視が必要なイベントログについて、サイバー攻撃の段階に分けて紹介していきます。



Tips Windows標準機能で監査ログを出力

Example: 特権管理者操作ログの出力

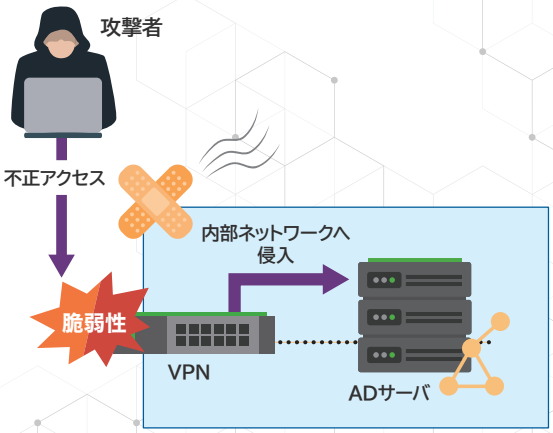
1. 対象サーバに管理者権限をもつアカウントでログオンする
2. スタートメニューから[コントロールパネル]-[管理ツール]-[グループ ポリシーの管理]を開く
3. [グループポリシーの管理]画面で[Default Domain Controller Policy]を右クリックし、[編集]を選択する
4. [グループ ポリシー管理エディター]-[コンピューターの構成]-[ポリシー]-[Windowsの設定]-[セキュリティの設定]-[ローカル ポリシー]-[監査ポリシー]の順に選択する
5. [アカウント管理の監査]-[ポリシーの変更の監査]及び[ログオンイベントの監査]をそれぞれダブルクリックし、[成功]及び[失敗]にチェックを入れて[OK]ボタンをクリックする



ADのログ管理

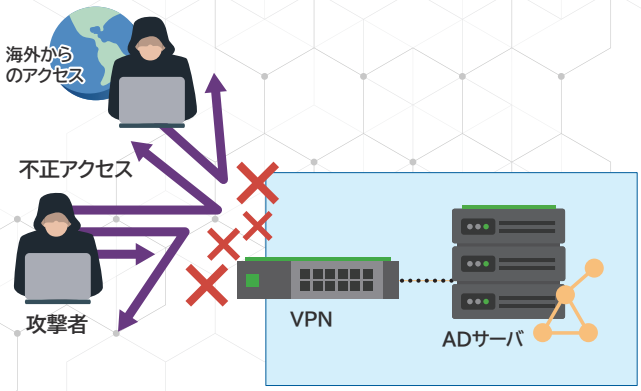
① 不正侵入

攻撃者はターゲットとなる企業のネットワークに侵入することから始まります。その経路は多々ありますが、最近はVPNやRDPが多く利用されます。その他に、フィッシングサイトや標的型メールでマルウェアに感染させ、C&Cサーバと通信させることで実質的に企業のデバイスへ不正侵入する方法もあります。



例 VPNを狙った不正アクセスをログで検知

本資料は、ADのセキュリティ対策を対象としているため、少し話題がそれますが、VPN機器を狙ったサイバー攻撃が多いため、ご紹介します。
VPN機器の特徴として、正規ユーザ、不正ユーザ問わず、インターネットを経由し誰でもVPN認証をできることにあります。そのため、ユーザーID/Passwordが漏洩すれば、不正侵入されることになります。そこで、VPNを経由した不正侵入を検知するために、ログを活用して検知する必要があります。



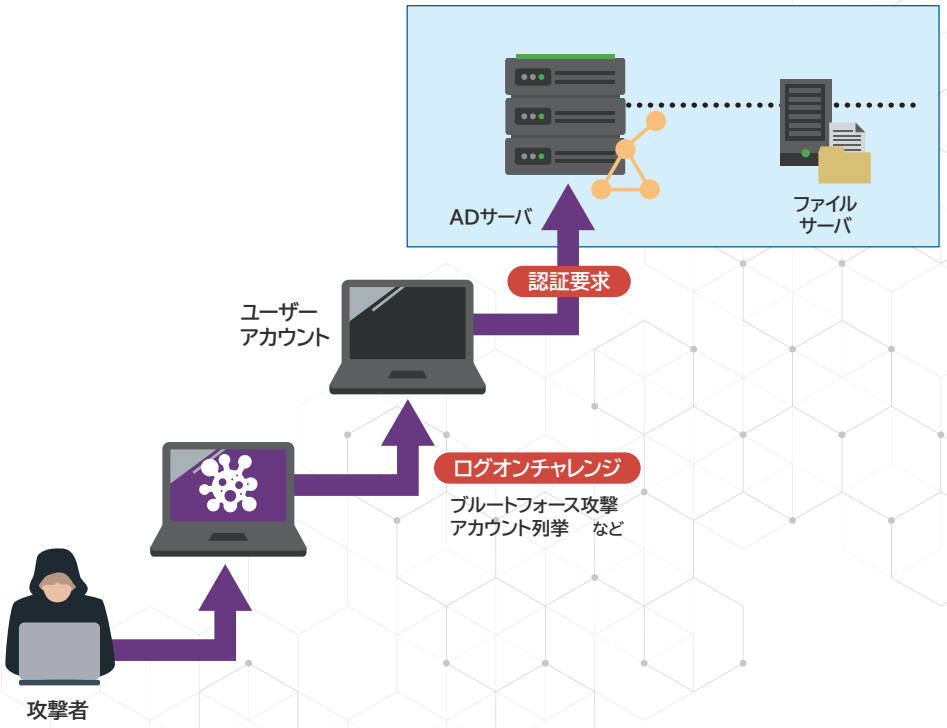
有効な監視ポイント

- 総当たり攻撃を検知
  - あるユーザのログオン失敗が1日に5回以上
  - リストにないユーザによるログオン失敗
- 海外からの不審なログオン試行を検知
  - 送信元グローバルIPアドレスが海外となっているログオン失敗

ADのログ管理

② 水平展開

ターゲットのシステム内部への侵入に成功した攻撃者は、自身が活動しやすい環境を作り出すため、権限の昇格を試みたり、行動範囲を拡大するために、他のシステムへの侵入を試みます。特にADは狙われるケースが多く、その攻撃を検知することが重要です。



例 水平展開時の総当たり攻撃をログで検知

ドメインユーザを使用してコンピュータにアクセスした場合、ADサーバに認証に関連するイベントログが記録されます。認証イベントに記録される認証要求元端末やアカウント名などの情報を調査して、意図しないアカウントの利用がないかどうか確認することで、アカウントの悪用を検知できる可能性があります。

ADのログ管理

② 水平展開

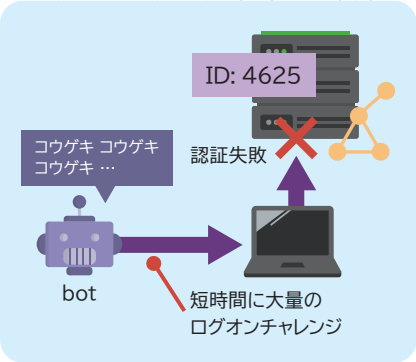
チェックすべきログ
ユーザログオンログ


```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
 <Provider Name="Microsoft-Windows-Security-Auditing"
Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />
 <EventID>4625</EventID>
 <Version>0</Version>
 <Level>0</Level>
 <Task>12546</Task>
 <Opcode>0</Opcode>
 <Keywords>0x8010000000000000</Keywords>
 <TimeCreated SystemTime="2015-09-08T22:54:54.962511700Z" />
 <EventRecordID>229977</EventRecordID>
 <Correlation />
 <Execution ProcessID="516" ThreadID="3240" />
 <Channel>Security</Channel>
 <Computer>DC01.contoso.local</Computer>
 <Security />
 </System>
- <EventData>
 <Data Name="SubjectUserSid">S-1-5-18</Data>
 <Data Name="SubjectUserName">DC01$</Data>
 <Data Name="SubjectDomainName">CONTOSO</Data>
 <Data Name="SubjectLogonId">0x3e7</Data>
 <Data Name="TargetUserSid">S-1-0-0</Data>
 <Data Name="TargetUserName">Auditor</Data>
 <Data Name="TargetDomainName">CONTOSO</Data>
 <Data Name="Status">0xc0000234</Data>
 <Data Name="FailureReason">%%2307</Data>
 <Data Name="SubStatus">0x0</Data>
 <Data Name="LogonType">2</Data>
 <Data Name="LogonProcessName">User32</Data>
 <Data Name="AuthenticationPackageName">Negotiate</Data>
 <Data Name="WorkstationName">DC01</Data>
 <Data Name="TransmittedServices">-</Data>
 <Data Name="LmPackageName">-</Data>
 <Data Name="KeyLength">0</Data>
 <Data Name="ProcessId">0x1bc</Data>
 <Data Name="ProcessName">C:¥¥Windows¥¥System32¥¥winlogon.exe</Data>
 <Data Name="IpAddress">127.0.0.1</Data>
 <Data Name="IpPort">0</Data>
 </EventData>
 </Event>
```


有効な監視ポイント

- 総当たり攻撃を検知
  - あるユーザのログオン失敗が1日に5回以上
  - リストにないユーザによるログオン失敗
  - ロックアウトされたアカウントに対するログオン失敗

調査例

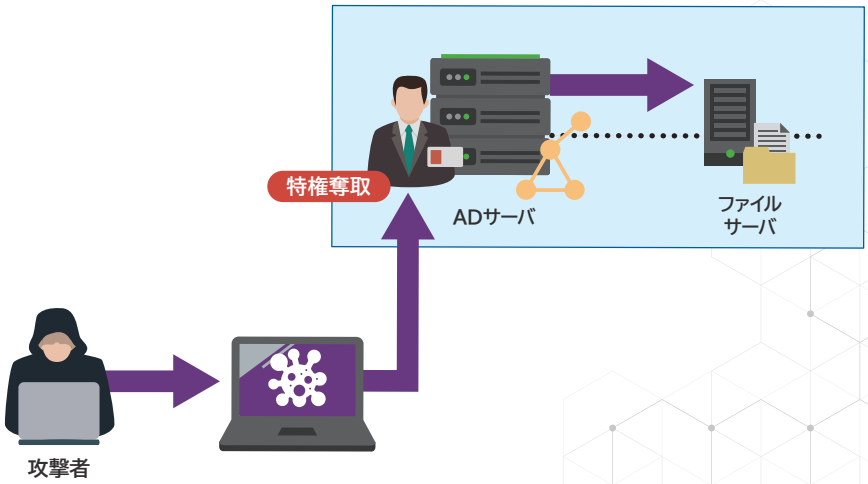


ログオン失敗の調査

確認事項	ログオン失敗の際に記録されるイベント ID 4625について、アカウント・端末ごとのログオン試行回数の推移を確認し、不審な挙動がないか調査する。
対応策	ログオン失敗が急激に多数発生している場合は、ヒアリングなどによってアカウントや端末の使用状況を確認し、意図しない使用であればアカウントが使用された端末を調査する。

ADのログ管理

② 水平展開



例 不正な特権使用をログで検知

ドメイン管理者権限などの特権が割り当てられているアカウントを使用した場合、ADサーバに特権使用に関連するイベントログが記録されます。社内で管理されているユーザ以外による特権使用や、管理者が意図しないタイミングの特権使用がないかどうか確認することで、不正な特権使用を検知できる可能性があります。

ADのログ管理

② 水平展開

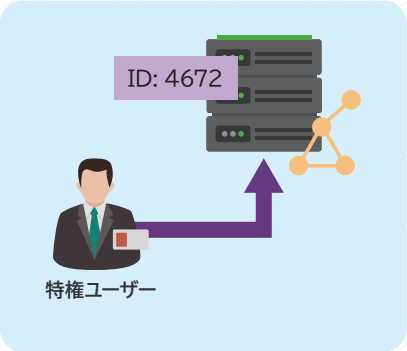
チェックすべきログ
特権ユーザのログオンログ


```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
 <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5-
BA-3E3B0328C30D}" />
 <EventID>4672</EventID>
 <Version>0</Version>
 <Level>0</Level>
 <Task>12548</Task>
 <Opcode>0</Opcode>
 <Keywords>0x8020000000000000</Keywords>
 <TimeCreated SystemTime="2015-09-11T01:10:57.091809600Z" />
 <EventRecordID>237692</EventRecordID>
 <Correlation />
 <Execution ProcessID="504" ThreadID="524" />
 <Channel>Security</Channel>
 <Computer>DC01.contoso.local</Computer>
 <Security />
 </System>
- <EventData>
 <Data Name="SubjectUser-
Sid">S-1-5-21-3457937927-2839227994-823803824-1104</Data>
 <Data Name="SubjectUserName">dadmin</Data>
 <Data Name="SubjectDomainName">CONTOSO</Data>
 <Data Name="SubjectLogonId">0x671101</Data>
 <Data Name="PrivilegeList">SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege
SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege
SeSystemEnvironmentPrivilege SeEnableDelegationPrivilege SeImpersonatePrivilege</Data>
 </EventData>
 </Event>
```


有効な監視ポイント

- 不正な特権使用を検知
  - 管理用端末以外からの特権ユーザーのログオン
  - 管理者でないユーザによるログオン

調査例



特権の割り当ての妥当性の調査

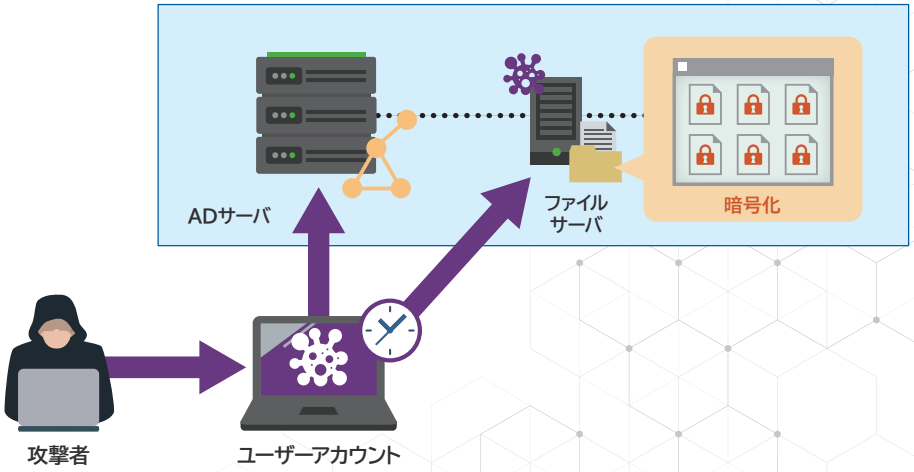
確認事項	ログオンに特権が割り当てられると記録されるイベント ID 4672 の「アカウント名」に、特権を使用することを想定していないアカウントが記録されていないかどうか確認する。
対応策	特権を使用することを想定していないアカウントを発見したら、攻撃者が不正に権限昇格を行っている可能性が あるため、アカウントを無効化するとともにアカウントを使用している端末を調査し、不要な特権が割り当てられていた場合は削除する。

ADのログ管理

③ 目的の実行

水平展開により行動範囲を広げた攻撃者は、情報の窃取、暗号化などの最終的なな目的を達成しようとします。

ADの機能を用いて目的の実行を準備する場合もあるため、そのような行動を検知して実行を阻止することが重要です。



例 タスクスケジューラによる目的実行

攻撃者は、目的実行を検知・阻止されないように、夜間や休日に遂行しようと、ADのタスクスケジューラを用いて日時を指定して悪意あるプログラムを実行することがあります。タスクスケジューラの使用はADのログに記録されるため、意図しないタイミングでのタスクスケジューラの使用がないかどうか確認することで、最終的な目的実行を阻止できる可能性があります。

ADのログ管理

③ 目的の実行

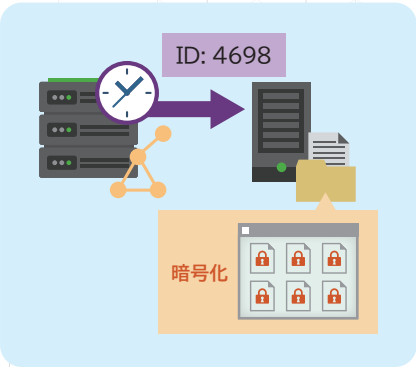
チェックすべきログ
タスクスケジューラーのログ


```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
 <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5-
BA-3E3B0328C30D}" />
 <EventID>4698</EventID>
 <Version>0</Version>
 <Level>0</Level>
 <Task>12804</Task>
 <Opcode>0</Opcode>
 <Keywords>0x8020000000000000</Keywords>
 <TimeCreated SystemTime="2015-09-23T02:03:06.944522200Z" />
 <EventRecordID>344740</EventRecordID>
 <Correlation />
 <Execution ProcessID="516" ThreadID="5048" />
 <Channel>Security</Channel>
 <Computer>DC01.contoso.local</Computer>
 <Security />
 </System>
- <EventData>
 <Data Name="SubjectUserSid">S-1-5-21-3457937927-2839227994-823803824-1104</Data>
 <Data Name="SubjectUserName">dadmin</Data>
 <Data Name="SubjectDomainName">CONTOSO</Data>
 <Data Name="SubjectLogonId">0x364eb</Data>
 <Data Name="TaskName">¥¥Microsoft¥¥StartListener</Data>
 <Data Name="TaskContent"><?xml version="1.0" encoding="UTF-16"?> <Task version="1.2"
xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo>
<Date>2015-09-22T19:03:06.9258653</Date> <Author>CONTOSO¥¥dadmin</Author>
</RegistrationInfo> <Triggers /> <Principals> <Principal id="Author"> <RunLevel>LeastPrivi-
lege</RunLevel> <UserId>CONTOSO¥¥dadmin</UserId> <LogonType>InteractiveToken</Logon-
Type> </Principal> </Principals> <Settings> <MultipleInstancesPolicy>IgnoreNew</MultipleIn-
stancesPolicy> <DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries> <StopIfGoingOnBat-
teries>true</StopIfGoingOnBatteries> <AllowHardTerminate>true</AllowHardTerminate>
<StartWhenAvailable>false</StartWhenAvailable> <RunOnlyIfNetworkAvailable>false</RunOnlyIf-
NetworkAvailable> <IdleSettings> <StopOnIdleEnd>true</StopOnIdleEnd> <RestartOnIdle>-
false</RestartOnIdle> </IdleSettings> <AllowStartOnDemand>true</AllowStartOnDemand>
<Enabled>true</Enabled> <Hidden>false</Hidden> <RunOnlyIfIdle>false</RunOnlyIfIdle>
<WakeToRun>false</WakeToRun> <ExecutionTimeLimit>P3D</ExecutionTimeLimit>
<Priority>7</Priority> </Settings> <Actions Context="Author"> <Exec> <Command>C:¥¥Docu-
ments¥¥listener.exe</Command> </Exec> </Actions> </Task></Data>
 </EventData>
 </Event>
```


有効な監視ポイント

- 不審なタスクの作成を検知
  - タスクの登録
  - スケジュールされたタスクの作成

調査例



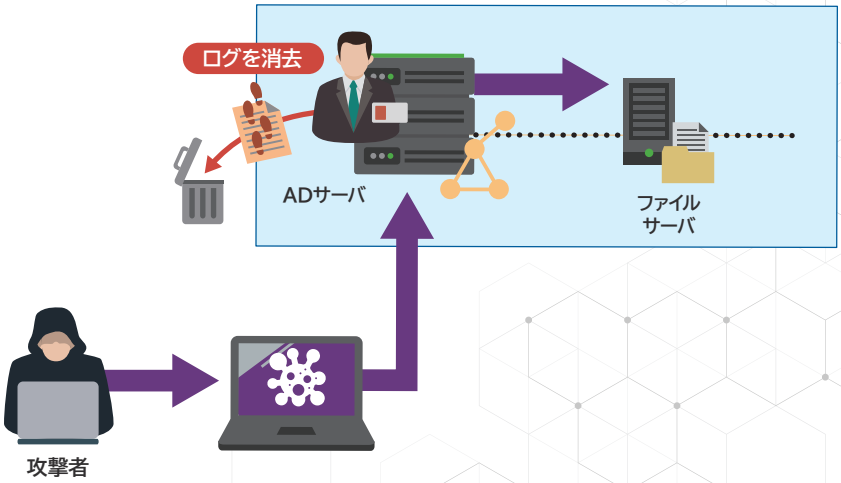
不審なタスクの作成の調査

確認事項	イベント ID 4698 などのタスクに関連するイベントや、タスクスケジューラに登録されているタスク、タスクが保存されているファイルを調べ、運用で使用するはずのないタスクを探す。
対応策	運用で使用するはずのないタスクが作成されている場合は、侵害されている可能性があるため、そのコンピュータを調査する

ADのログ管理

④ 痕跡の消去

目的を達成した攻撃者は、自身の活動の痕跡の消去を試みる場合があります。



例 イベントログの消去

イベントログの消去は、攻撃の最終フェーズで行われることが多く、システム管理者などによる意図的なログの削除でない場合は、攻撃を疑います。

ADのログ管理

④ 痕跡の消去

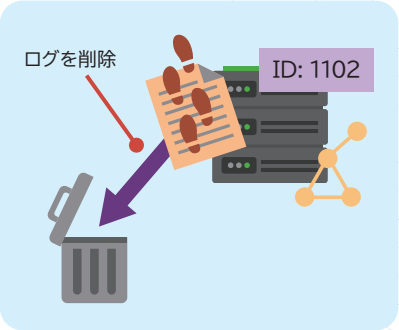
チェックすべきログ
イベントログ消去のログ


```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
 <Provider Name="Microsoft-Windows-Eventlog"
Guid="{fc65ddd8-d6ef-4962-83d5-6e5cfe9ce148}" />
 <EventID>1102</EventID>
 <Version>0</Version>
 <Level>4</Level>
 <Task>104</Task>
 <Opcode>0</Opcode>
 <Keywords>0x4020000000000000</Keywords>
 <TimeCreated SystemTime="2015-10-16T00:39:58.656871200Z" />
 <EventRecordID>1087729</EventRecordID>
 <Correlation />
 <Execution ProcessID="820" ThreadID="2644" />
 <Channel>Security</Channel>
 <Computer>DC01.contoso.local</Computer>
 <Security />
 </System>
- <UserData>
- <LogFileCleared xmlns="http://manifests.microsoft.com/win/2004/08/win-
dows/eventlog">
 <SubjectUser-
Sid>S-1-5-21-3457937927-2839227994-823803824-1104</SubjectUserSid>
 <SubjectUserName>dadmin</SubjectUserName>
 <SubjectDomainName>CONTOSO</SubjectDomainName>
 <SubjectLogonId>0x55cd1d</SubjectLogonId>
 </LogFileCleared>
 </UserData>
 </Event>
```


有効な監視ポイント

- 痕跡の消去を検知
  - イベントログの削除

調査例



イベントログ削除の調査

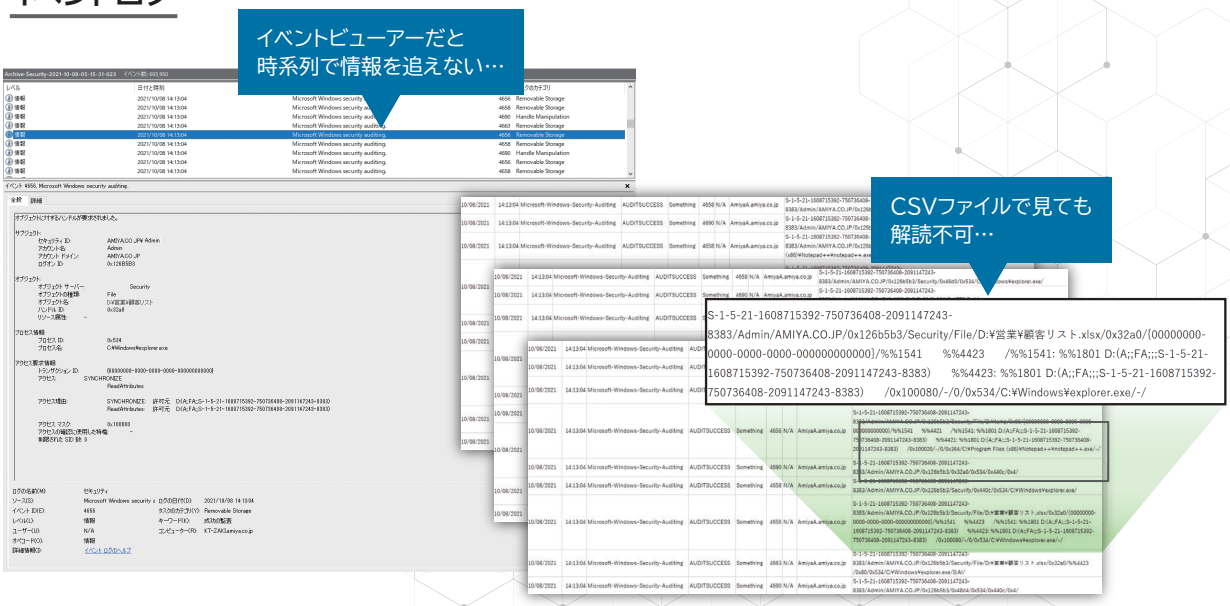
確認事項	イベントログを削除した際に記録されるイベント ID 1102 を探し、見つかった場合は、正規の運用者による消去かどうかを確認する。
対応策	正規の管理者以外がイベントログの削除を行った可能性がある場合は、該当するコンピュータを調査する。

ADログ取得の課題

ここまで、チェックしておきたいADのログや、監視ポイント、調査例を紹介してきました。しかし、いざWindowsの標準機能を用いてログを取得し監視してみても、その管理は困難を極めます。

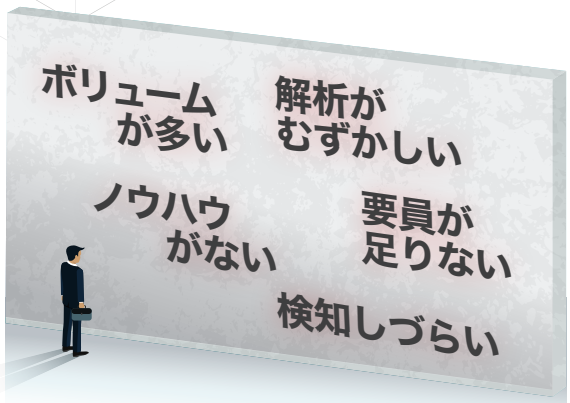
まず、Windowsのイベントログ情報は難解で、ノイズデータも含まれるので膨大なログが出力されます。

イベントログ



そのため有事の際に迅速にログを解析することが難しく、また、イベントIDは横断的な要素も持ち合わせているため、実際になんの操作が行われたかを読み解くには、専門的なノウハウが必要となります。

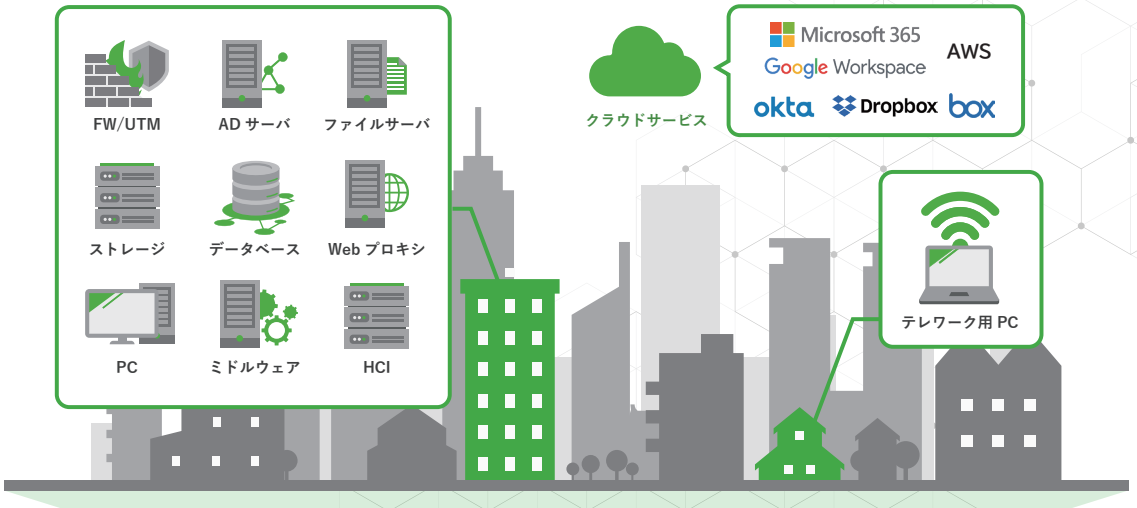
さらに、攻撃の実害を受ける前に異常を迅速に検知するには、ログを常時監視しておくことが必要となります。しかし、常時ログを監視し続けることは人的リソースを考えると現実的ではありません。



網屋のALog

セキュリティのむずかしいをカンタンに

網屋のALogシリーズなら、これらの課題を解決することができます。ALogは、ADを含め多様な情報システムのログをエージェントレスで自動集約・運用監視するデータセキュリティソリューションです。特許を取得した独自のログ翻訳変換・整形技術をはじめとした、ログ管理の「むずかしいをカンタンに」にする技術により、専門知識やノウハウがなくとも、高度なログ活用を実現でき、サイバー攻撃への迅速な対応を可能にします。

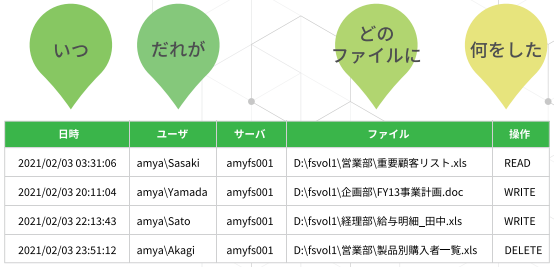


網屋のALog

むずかしいをカンタンにする3つのポイント

特許取得の翻訳変換技術

膨大なデータアクセスの記録を複雑なシステムログから
抽出し、特許取得のログの翻訳変換技術を使って、見やすい
「アクセスログ」にまとめます。

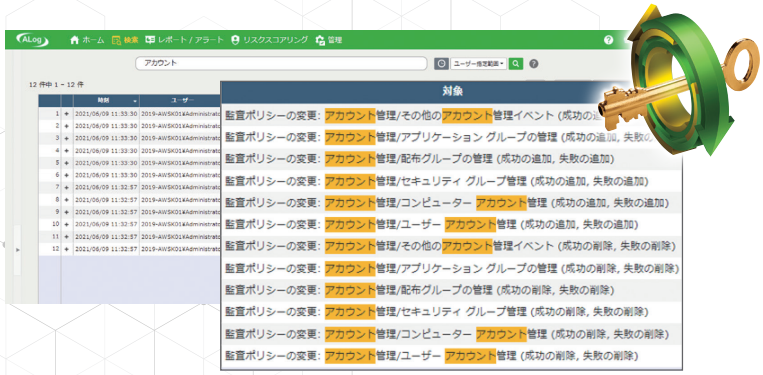


日時	ユーザ	サーバ	ファイル	操作
2021/02/03 03:31:06	amya\Sasaki	amyfs001	D:\fsvol1\営業部\重要顧客リスト.xls	READ
2021/02/03 20:11:04	amya\Yamada	amyfs001	D:\fsvol1\企画部\FY13事業計画.doc	WRITE
2021/02/03 22:13:43	amya\Sato	amyfs001	D:\fsvol1\経理部\給与明細_田中.xls	WRITE
2021/02/03 23:51:12	amya\Akagi	amyfs001	D:\fsvol1\営業部\製品別購入者一覧.xls	DELETE

特許番号　特許第6501159号

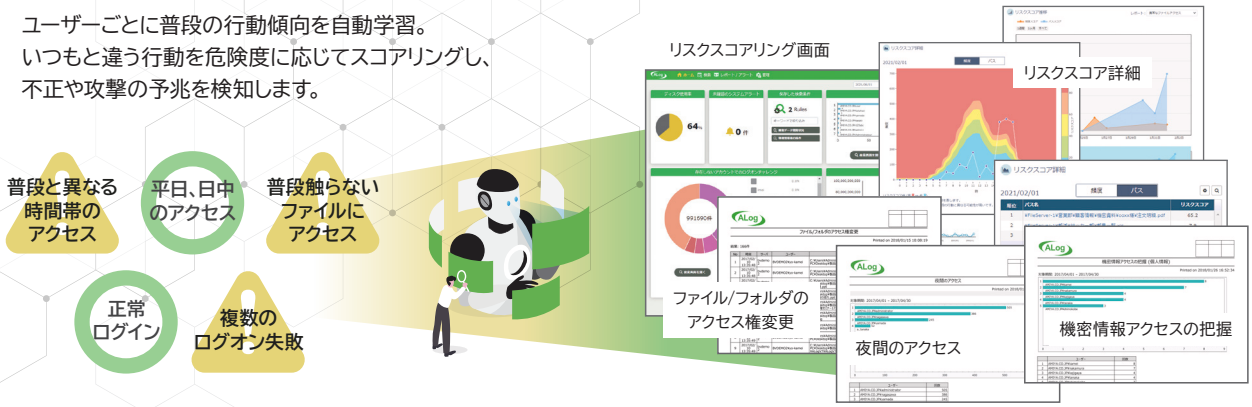
直感的に操作できるGUI

検索、レポート、管理機能全てをまとめて
直感的に運用可能。
検索項目を意識せずにフォーマットの
異なるログを横断的に検索できます。



AIが異常を自動検知

ユーザーごとに普段の行動傾向を自動学習。
いつもと違う行動を危険度に応じてスコアリングし、
不正や攻撃の予兆を検知します。



網屋のALog

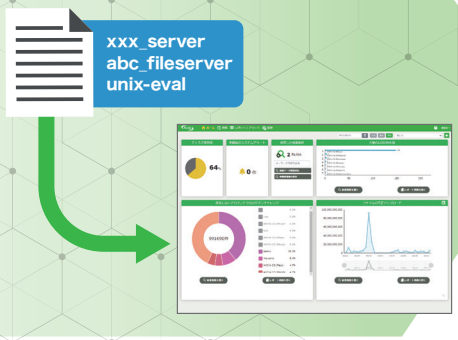
わずか3ステップでサイバー攻撃対策を自動化

サイバー攻撃自動検知パック

サイバー攻撃対策に特化したレポート内容を標準搭載。
事前にセットするだけで、IPAやJPCIRTのガイドライン
に沿った最も効果的なレポートを作成。
要件定義/設計/構築作業の必要がありません。

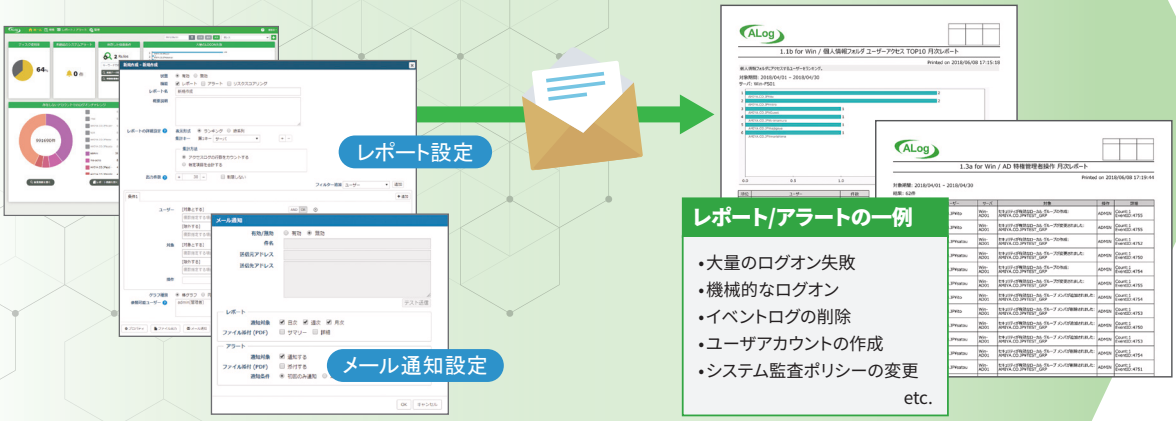
① テンプレートをインポート

② 機器名を登録



③ 事前セットでレポート/アラートを自動通知

パックの中から必要なレポートを選んで設定するだけでOK。
自動でレポートが作成され、定期的に運用者にメール送信。異常時にはアラートも。



レポート/アラートの一例

- 大量のログオン失敗
- 機械的なログオン
- イベントログの削除
- ユーザアカウントの作成
- システム監査ポリシーの変更

etc.

網屋のALog

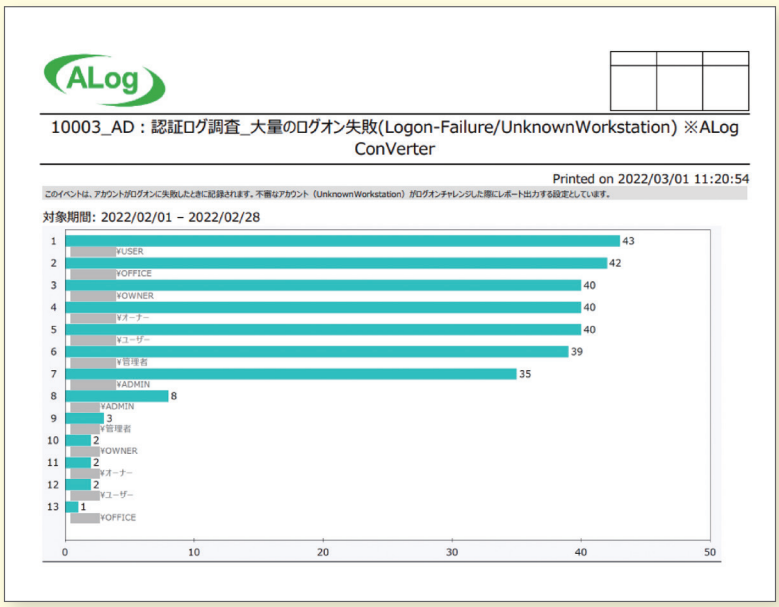
わずか3ステップでサイバー攻撃対策を自動化

レポートテンプレート例 不審なログオンの検知

Active Directory(AD)のログを監視していたところ、不審なアクセスを検知した。
ADのログから以下のことが判明。

1. 2月28日16:00ころ～19:08ころに発生
2. 不審な要素のあるアクセスである
3. 典型的なリスト攻撃のパターンに酷似

なお、同社が導入しているEDRやPC管理システムでは、通常操作によるログオン失敗と見なされ、異常は検知できていなかった。



不審な要素

1. ActiveDirectoryに登録されていないアカウント名でログインしようとしている
2. アカウント名が一般にありがちなアカウント名を使っている
3. 各アカウントのログオン失敗回数が異常に多い

順位	ユーザー	件数
1	¥USER	43
2	¥OFFICE	42
3	¥OWNER	40
4	¥オーナー	40
5	¥ユーザー	40
6	¥管理者	39
7	¥ADMIN	35
8	¥ADMIN	8
9	¥管理者	3
10	¥OWNER	2
11	¥オーナー	2
12	¥ユーザー	2
13	¥OFFICE	1
計		297

おわりに

本書では主に、ADにおけるサイバー攻撃対策とADのログ管理について紹介してきました。繰り返しになりますが、攻撃者の侵入を防ぎきることが困難となってきている中で、侵入を早期に検知し対応できる仕組みが重要であり、攻撃者が必ず経由するADにおいてその対策を重点的に施すことが、最も効果的です。

しかしながら、ADにおいて対策を施すといっても、対策のためのリソース確保やポリシー策定といった態勢の整備、予算の策定など、多くの課題が存在します。「そもそも何から手をつけてよいかわからない」と出だしからつまずいてしまう企業様も多いのではないでしょうか。

トータルセキュリティサポート「セキュサポ」

そこで紹介したいのが、包括的なセキュリティ強化を月額固定でワンストップ提供する、「セキュサポ」です。

サイバーセキュリティの専門チームが検知ツールの導入・設計から、インシデント対応までを一貫して実施。

「ポリシー決め」や「リスク分析」といった概念的なセキュリティ対策だけではなく、ADにおける対策も含め、企業様ごとの環境や業務状況に即した、実現性の高いセキュリティ対策を提案します。

SOCサービスも

- サイバー攻撃対策
- 強化レポート
- 内部不正対策
- サイバー保険
- インシデントレスポンス支援

攻撃予防も

- 脆弱性対策
- セキュリティ相談窓口

詳しい製品のご紹介、評価版のご依頼は以下にお問い合わせください。

お問い合わせ先

株式会社網屋
データセキュリティ事業部

TEL：03-6822-9996　E-mail：bv-sales@amiya.co.jp

詳しい製品概要資料はこちら ＞

開発元

AMIYA 株式会社 網屋

〒103-0007 東京都中央区日本橋浜町3-3-2 トルナーレ日本橋浜町 11F
TEL: 03-6822-9999 FAX: 03-6822-9998
https://www.amiya.co.jp/

販売元