JPCERT CC®

ログを活用した Active Directory に対する攻撃の検知と対策

JPCERT/CC 早期警戒グループ

本文書の目的

- JPCERT/CCでは、高度サイバー攻撃（標的型攻撃）において、Active Directoryを乗っ取る事例を多数確認している
- 一部の組織ではActive Directoryの脆弱性が放置されていたり、ログが十分に保存されておらず、攻撃を受けやすい、または受けても検知できない環境にある
- Active Directoryの攻撃手法とその対策を合わせて整理した日本語ドキュメントは少ない

JPCERT/CCがインシデント対応支援を通して得た知見を「ログを活用したActive Directoryに対する攻撃の検知と対策」に集約

想定している読者

- 想定読者
  - Active Directoryを運用または導入を検討しているシステム管理者
  - セキュリティ担当者
  - セキュリティインシデントの対応や調査に関わる担当者

- コンセプト
  - Active Directoryに対する攻撃手法、攻撃を検知するためのログの確認ポイント、攻撃を抑止または被害を軽減するための対策を整理
  - 実践しやすいように、手順などを具体的に記載
  - フローチャートや表で行うべき対応を分かりやすく記載
  - より詳細な情報をAppendixに掲載

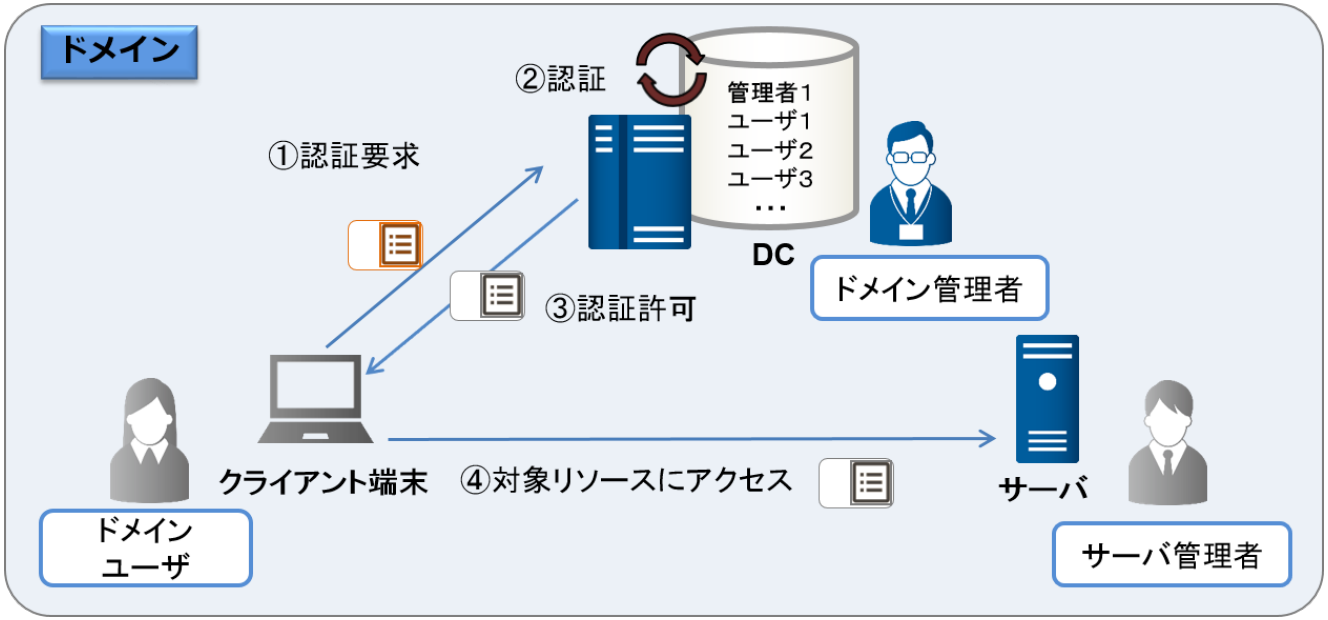
運用やインシデント対応の現場で
実践的に活用できる文書を目指して作成

本文書の活用方法

章	構成	読者のニーズ
1	はじめに	文書の全体構成を把握したい 本文書の概要(Executive Summary)を知りたい
2	高度サイバー攻撃の手法	高度サイバー攻撃の概要を理解したい
3	Active Directoryに対する攻撃手法	Active Directoryへの攻撃手法を理解したい
4	Active Directoryのイベントログを活用した高度サイバー攻撃の検知	ログを分析してActive Directoryへの攻撃を検知し、侵害されたコンピュータやアカウントを特定したい
5	Active Directoryに対する攻撃の対策	攻撃抑止のための予防的対策や、検知されたActive Directoryへの攻撃に対する緊急対処について知りたい
6	最後に	–
-	Appendix	攻撃手法や検知、対策に必要な設定についてより詳細に知りたい

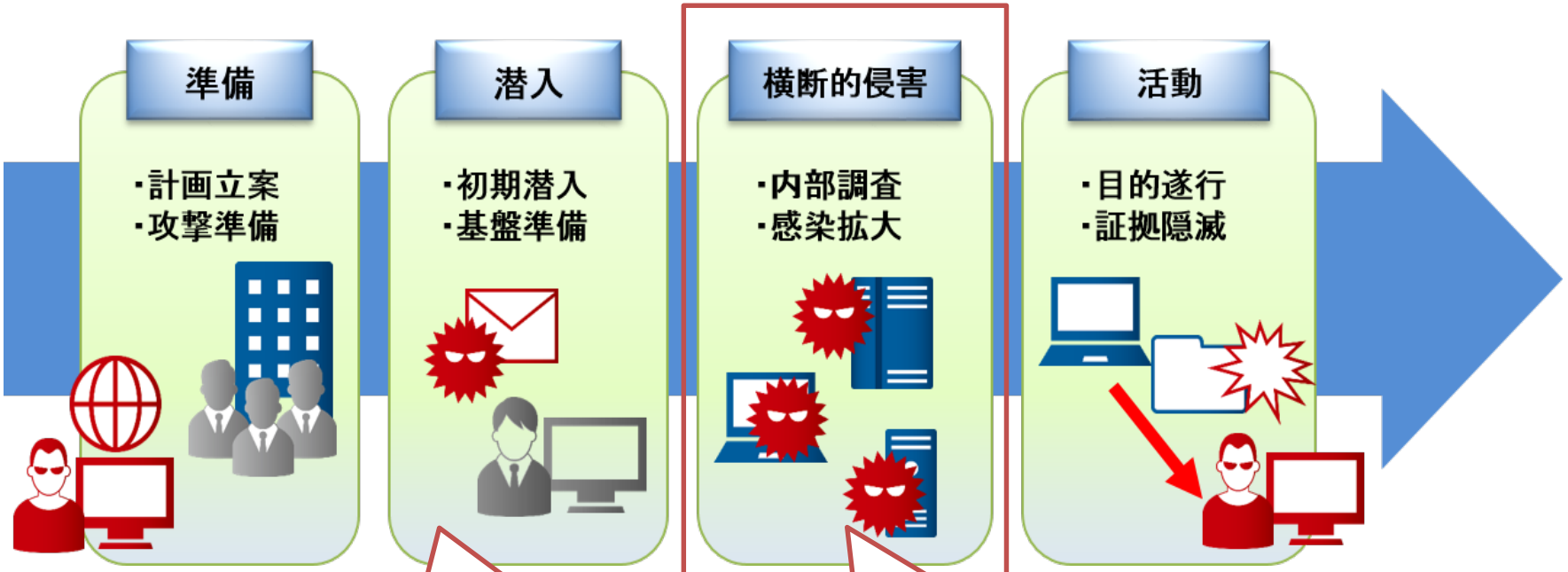
Active Directoryの概要

- Active Directoryとは
  - Microsoft社が提供している、組織内のコンピュータやユーザを集中的に管理できる仕組み
  - ドメイン：コンピュータやユーザを管理する際の管理単位
  - ドメイン管理者：ドメイン配下の全てのリソースをコントロールできる権限を持つアカウント



2章
高度サイバー攻撃の手法

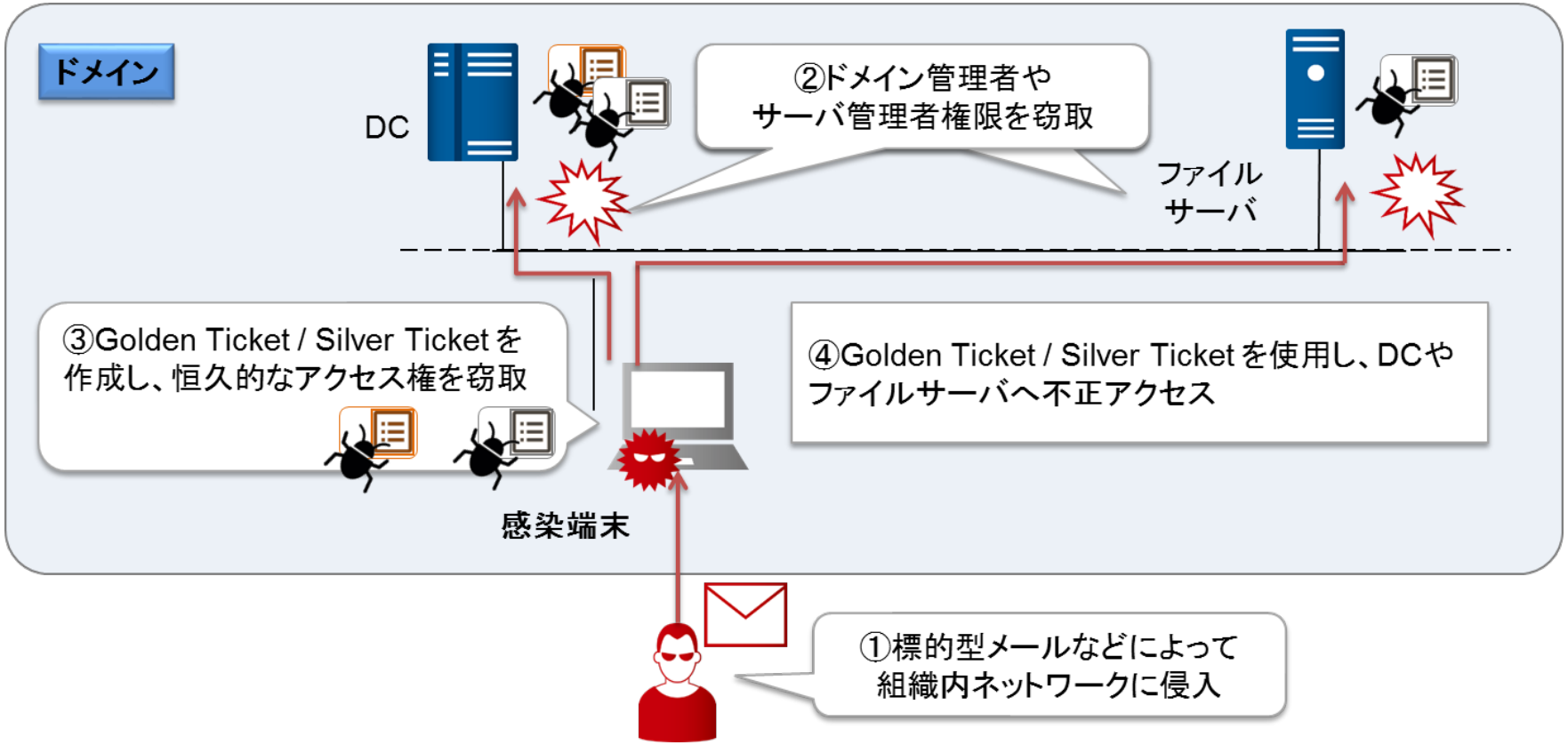
高度サイバー攻撃のプロセス



攻撃者はActive Directoryへの攻撃を行い、横断的侵害を容易にするため、認証情報やより高い権限の窃取を試みる

3章
Active Directoryに対する攻撃手法

Active Directoryに対する攻撃の例



攻撃者はドメイン管理者権限などを窃取し、正規の管理者になりすまして、長期にわたって使えるアクセス権限の獲得を試みる

Active Directoryに対する攻撃手法

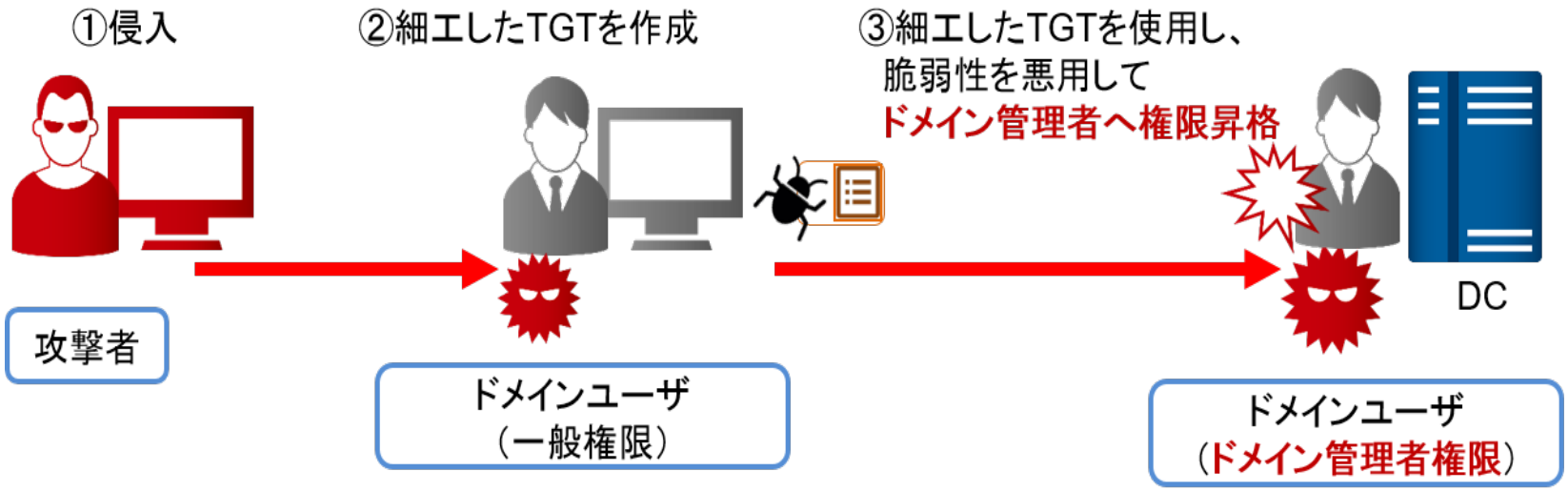
- 攻撃手法は大きく分けて2つ
  1. Active Directoryの脆弱性の悪用
  2. 端末に保存された認証情報の悪用

- いずれも攻撃手法やツールも公開されており、比較的容易に攻撃できる

Active Directory環境で使用される認証方式（Kerberos/NTLM認証）の脆弱性や仕様上の弱点が狙われることが多い

攻撃手法1（ Active Directoryの脆弱性の悪用）

- Kerberos認証の脆弱性を悪用し、ドメイン管理者権限を取得する方法
  - Kerberos KDC の脆弱性（CVE-2014-6324 / MS14-068）の悪用を確認している
  - 上記脆弱性により、ドメインユーザがドメイン管理者に権限昇格することができる
  - ツールが公開されており、比較的容易に攻撃が可能



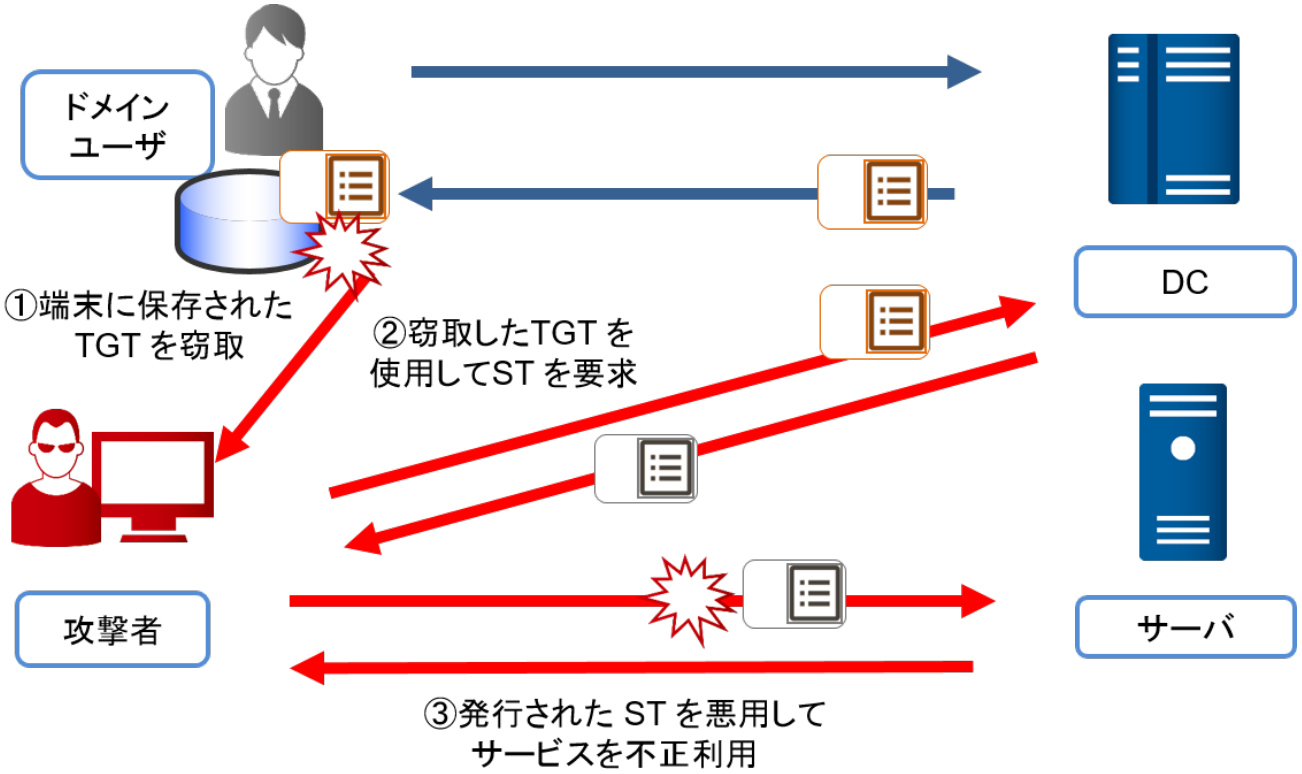
攻撃手法2（端末に保存された認証情報の悪用）

- 端末のメモリには過去にログインした認証情報が残存していることがあり、これを窃取する

攻撃手法	内容	どのように悪用するか
Pass-the-Hash	NTLM認証のパスワードハッシュでログインできる仕組みを悪用して不正にログインする	パスワードを使いまわしている（同じパスワードハッシュでアクセスできる）ことを利用し、他のコンピュータにログイン
Pass-the-Ticket	Kerberos認証で使われる認証チケットを悪用して不正にログインする	正規ユーザになりすまして検知を回避する ・Golden Ticket ・Silver Ticket を作成する

Pass-the-Ticket

- Kerberos認証で使用される認証チケットを窃取したり、不正に作成することにより、サービスを不正に利用する
  - TGT : Service Ticketを要求するためのチケット
  - Service Ticket : サービスにアクセスするために必要なチケット



Golden Ticket / Silver Ticket

- Golden Ticket （攻撃者が不正に作成したTGT）
  - ドメイン管理者権限を窃取することで作成できる
  - ドメイン管理者を含む任意のユーザになりすますことができる
  - 有効期限が10年で、任意の端末上やアカウントで使える

- Silver Ticket（攻撃者が不正に作成したST）
  - 各サーバの管理者権限を窃取することで作成できる
  - サーバの管理者や利用者になりすまして任意のサービスにアクセスできる
  - 有効期限が10年で、任意の端末上やアカウントで使える
  - DCにアクセスせずに使用できる＝DCにログが残らない

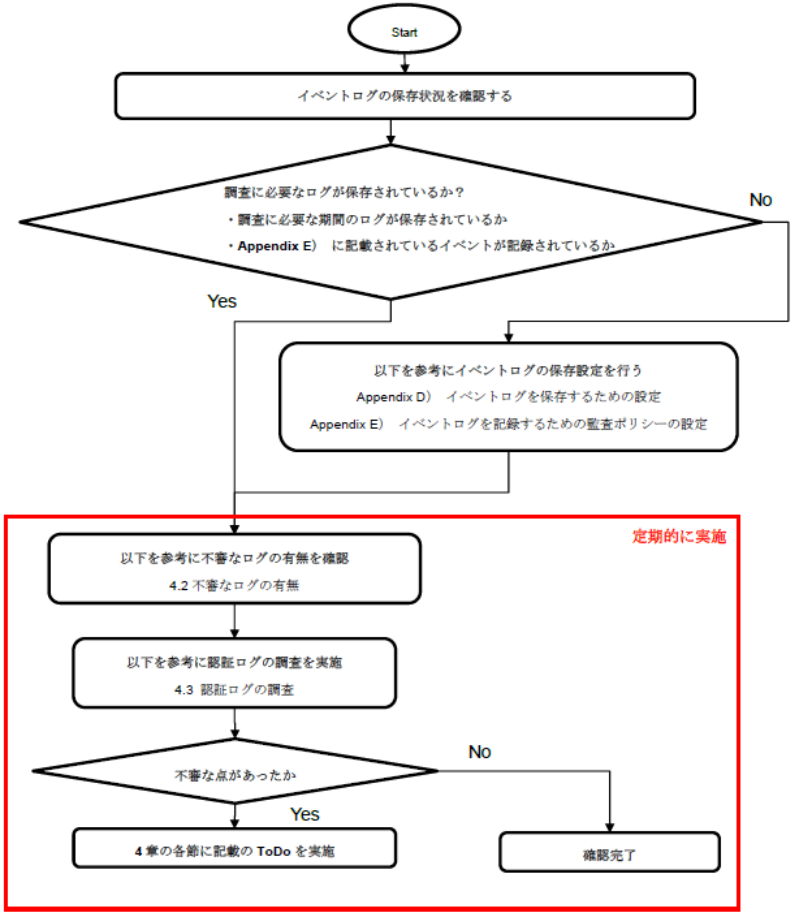
いずれも、不正に作成された正規の認証チケットであるため、検知が難しい

4章

Active Directoryのイベントログを活用した横断的侵害の検知

ログ確認のフロー

- Windows のログ（イベントログ）から攻撃の痕跡を効率的に検知する手法を紹介



フローチャートで、状況に応じて確認すべきポイントや参照すべき章を明確化

攻撃手法とログの調査方法、確認対象の対応

		攻撃手法					
		ドメイン管理者、サーバ管理者権限の窃取			管理者権限窃取後の活動		痕跡消去
		ADの脆弱性 (3.1)	保存された認証情報の悪用 (3.2)	ローカル管理者の悪用(3.3)	Golden Ticket (3.2.2.1)	Silver Ticket (3.2.2.2)	
不審なログの調査	MS14-068 (4.2.1)	○					
	Golden Ticket (4.2.2)				○		
	Silver Ticket (4.2.2)					○※	
	不審なタスクの作成 (4.2.3)				○	○※	
	イベントログの消去 (4.2.4)						○
認証ログの調査	特権割当 (4.3.1)	○					
	アカウントを利用した端末 (4.3.2)		△	△※	△	△※	
	認証回数 (4.3.3)		△	△※			

△ 運用と照らし合わせることで検知できる場合がある
※DCにはログが記録されないため、接続先コンピュータのログ確認が必要

攻撃手法と有効な検知手法の対応表を掲載

		調査範囲				調査が有効なバージョン
		DC	サーバ	DC、サーバの管理端末	その他の端末	
不審なログの調査	MS14-068 (4.2.1)	○				Windows Server 2008, 2008R2, 2012, 2012 R2
	Golden Ticket (4.2.2)	○				全バージョン※1
	Silver Ticket (4.2.2)	○	○	○		全バージョン※1
	不審なタスクの作成 (4.2.3)	○	○	○ ※2		全バージョン※1
	イベントログの消去 (4.2.4)	○	○	○ ※2		全バージョン※1
認証ログの調査	特権割当 (4.3.1)	○	○			全バージョン※1
	アカウントを利用した端末 (4.3.2)	○ ※2	○ ※2	○ ※2		全バージョン※1
	認証回数 (4.3.3)	○ ※2	○ ※2	○ ※2		全バージョン※1

※1 本レポートでは Windows Server 2008以降のイベントIDを対象に記載
※2 可能であれば調査することが望ましい

調査すべき機器と調査が有効なバージョンを明記

不審なログの調査

- 攻撃の可能性がある、特徴的で比較的容易に検知できるイベントログを紹介
- 以下は、不審なログの調査の一例として、Kerberos KDCの脆弱性「MS14-068」を悪用する攻撃を検知する方法

MS14-068 の脆弱性を悪用した攻撃の調査	
調査対象	以下のバージョンの DC Windows Server 2008, 2008R2, 2012, 2012 R2
前提条件	・ MS14-068 のセキュリティ更新プログラムを適用済みであること ・ イベント ID 4769（失敗）はデフォルトでは記録されないため、監査ポリシーの設定が必要 詳細は「Appendix E） イベントログを記録するための監査ポリシーの設定」を参照
確認事項	イベント ID 4769 について「エラーコード」が ”0xf” のログがあれば、攻撃を受けた可能性がある
ToDo	確認事項に該当するログがあった場合、ログの「ネットワーク情報: クライアント アドレス」に記録されているコンピュータは侵害されている可能性があるため調査を行う
注意事項	特になし
補足	MS14-068 に対するセキュリティ更新プログラムを適用していない場合は攻撃（権限昇格）に成功する。「4.3.1. 特権の割り当ての妥当性の調査」を参照し、調査すること

- 調査対象
- 不審と判断する基準
- 検知したら何をすればよいか

などについて、具体的に記載

認証ログの調査

- 平常時（運用）と比較して不審かどうかを判断する必要がある
- 以下は、認証ログの調査の一例として、意図しないアカウントに特権が割り当てられていないか調査する方法

特権の割り当ての妥当性の調査	
調査対象	DC、サーバ：全てのアカウント
前提条件	特になし
確認事項	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る場合は、MS14-068 の脆弱性などを悪用し、不正に権限昇格を行っている可能性がある
ToDo	特権を使用することを想定していないアカウントについて、以下を実施する ・ 特権を割り当てていない場合は、攻撃者が不正に権限昇格を行っている可能性があると判断し、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 ・ 不要な特権が割り当てられていた場合は削除
補足	Windows では用途に応じて複数の特権（SeSecurityPrivilege、SeBatchLogonRight など）[8]が定義されている。ドメイン管理者やローカル管理者のように全ての特権を持っていなくとも、特定の特権のみを持つアカウントを使用した際にもイベント ID 4672 が記録される

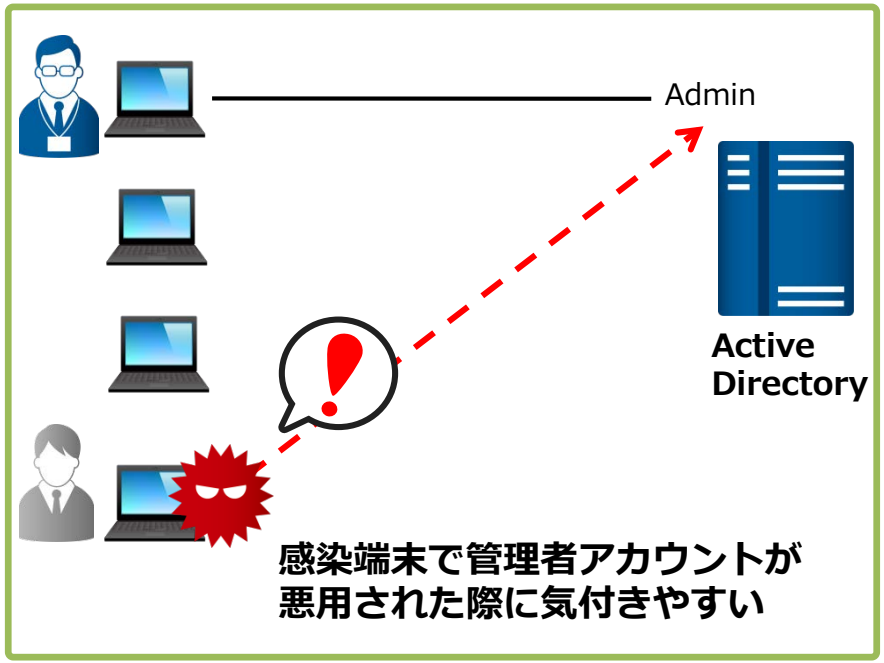
- 調査対象
- 確認観点
- 具体的なイベントIDと項目名

などについて、具体的に記載

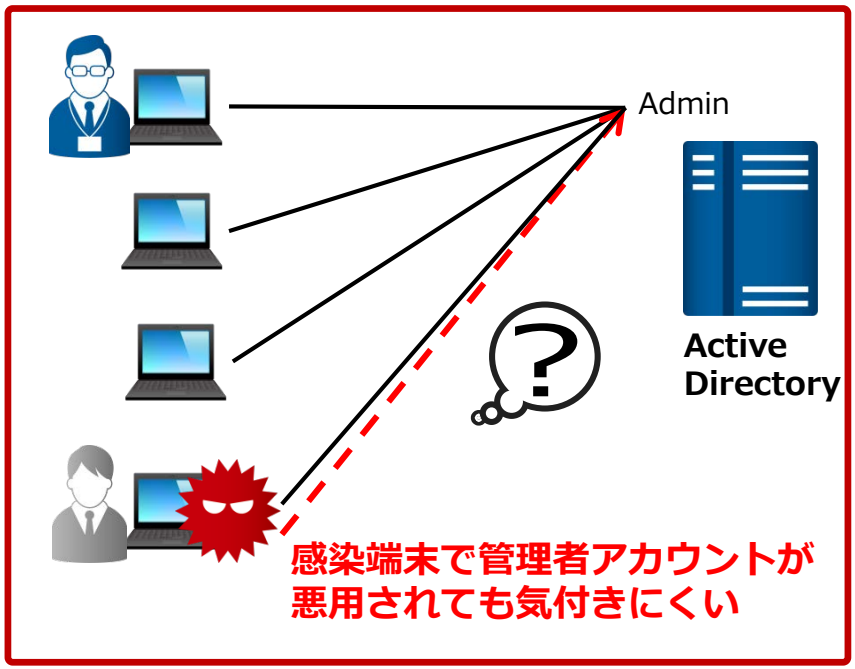
アカウントの悪用に気づきやすい環境の紹介

■管理者アカウントを使用する端末の限定

悪用を検知しやすい例
（端末とアカウントが1:1）



悪用を検知しにくい例
（端末とアカウントが多:1 または多:多）



管理者権限を窃取されるリスクも低減できる

5章
Active Directoryに対する攻撃の対策

Active Directoryに対する攻撃の対策

- 以下、2つの観点で記述
  1. 予防策：Active Directoryへの攻撃を抑止するための対策
  2. 攻撃を検知した際の緊急対処：被害を軽減するための対策

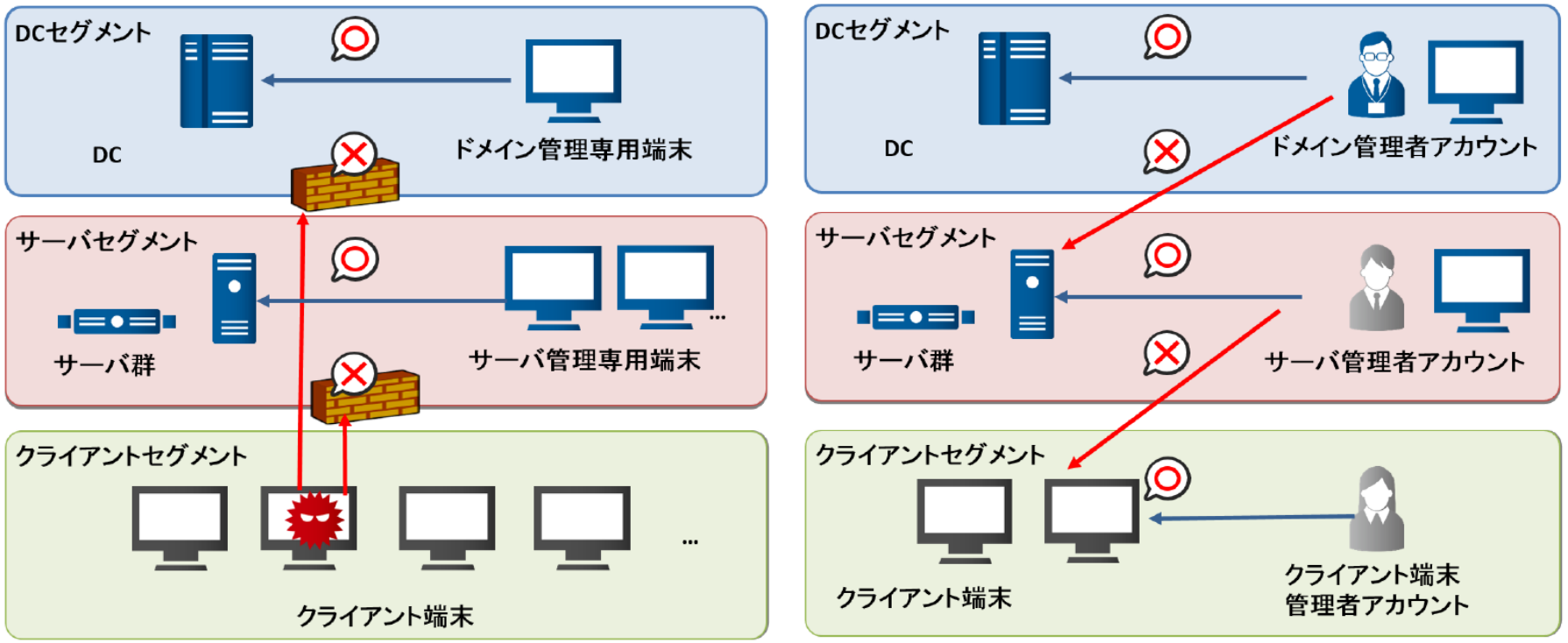
			攻撃手法				
			ドメイン管理者、サーバ管理者権限の窃取			管理者権限窃取後の活動	
			ADの脆弱性 (3.1)	保存された認証情報の悪用(3.2)	ローカル管理者の悪用(3.3)	Golden Ticket (3.2.2.1)	Silver Ticket (3.2.2.2)
予防策	管理専用端末の設置 (5.1.1)			○	○		
	セグメント化	通信 (5.1.2)		○	○		
		アカウント (5.1.3)		○	○		
	特権最小化 (5.1.4)			○	○		
	セキュリティ更新プログラム適用 (5.1.5) ※	KB3011780 (MS14-068)	○				
		KB2871997 (資格保護)		○	○		
	認証情報の保護 (5.1.6)			○	○	○	○
	適切なパスワード設定 (5.1.7)				○		
緊急対処	krbtgtのパスワード変更 (5.2.1)					○	
	ドメイン管理者アカウントのパスワード変更 (5.2.2)					○	
	サービスアカウントのパスワード変更 (5.2.3)						○
	管理者アカウントのパスワード変更 (5.2.4)						○

※ 特に優先して適用すべきセキュリティ更新プログラムについて記載

攻撃手法と有効な対策、
対策の適用対象を
表に整理して掲載

予防策の例（セグメント化）

■セキュリティレベルに応じてセグメント（ネットワーク・アカウント）を分離し、侵害範囲を制限する



ドメイン管理者権限を窃取されるリスクを低減

予防策の例（セキュリティ更新プログラム適用）

- セキュリティ更新プログラムを適用することで脆弱性の改修や、セキュリティの機能向上を実現できる

セキュリティ更新プログラム	改修、機能向上の内容
KB3011780	Kerberos KDCの脆弱性「MS14-068」の改修
KB2871997	メモリに平文や、容易に平文に復元できるハッシュ（LMハッシュなど）が残存しなくなる

- 主に攻撃手法1「 Active Directoryの脆弱性」の対策
- 優先的に適用すべき更新プログラムを紹介

予防策の例（認証情報の保護）

- メモリに認証情報を保存しない、または残存する認証情報を保護する機能を活用し、認証情報の窃取を防ぐ

保護機能	保護される情報
LSA Protection	未署名または Microsoft 以外によって署名されたプロセスからメモリを保護する
Protected Users	このグループに所属するアカウントはセキュリティが強固なKerberos認証のみ使用する
Restricted Admin	リモートデスクトップの接続先コンピュータに認証情報を残さない
Credential Guard	LSA（Local Security Authority）の認証情報が仮想化によってホストOSから隔離された保護環境に保護される

主に攻撃手法2「端末に保存された認証情報の悪用」の対策

攻撃を検知した際の緊急対処の例

- Golden Ticket の無効化
  - 一度Golden Ticketを作成されてしまうと、「MS14-068」の更新プログラムを適用しても、侵害されたアカウントのパスワードを変更しても、効果がない

krbtgt アカウントのパスワード変更	
適用対象	krbtgt アカウント
前提条件	特になし
設定手順	DC にログインし、AD のユーザとコンピュータの管理画面で krbtgt アカウントのパスワードを連続して 2 回変更する
注意事項	・パスワードの変更は必ず 2 回する必要がある。また、新たな Golden Ticket の作成を防止するために、2 回のパスワード変更は間隔を空けずに実施する ・新たな Golden Ticket の作成を防止するために、「5.2.2 ドメイン管理者アカウントのパスワード変更」を参照し、ドメイン管理者アカウントのパスワードも合わせて変更する ・krbtgt のパスワード変更によって正規ユーザが使用している TGT も無効化されて再発行が必要となるため、パスワード変更後は DC への認証要求が増える可能性がある

被害拡大抑止に有効な緊急対処について、適用時の注意事項や手順なども併せて紹介

Appendix

Appendixの構成

- 攻撃手法や検知・対策のために必要な設定などについて、より詳細に知りたい方向けの参考情報（以下はAppendixの例）
  - Active Directoryの攻撃手法（Golden Ticket / Silver Ticketを使用する攻撃）の検証結果
  - ログの保管状況やActive Directoryの運用状況などの実態調査の抜粋結果

Appendixの構成

Appendix		概要
A	ログの保管・確認にあたって	高度サイバー攻撃対応のために保管すべき主要なログと保管・確認にあたっての検討事項など
B	Active Directoryで使用される認証方式	Active Directoryで使用される主要な認証方式の説明
C	Windowsに保存される認証情報	Windowsのメモリ上に保存される認証情報について、認証方式やアカウントの種類毎に紹介
D	イベントログを保存するための設定	イベントログの最大サイズやアーカイブの設定方法についての紹介
E	イベントログを記録するための監査ポリシーの設定	調査に必要なイベントログを記録するための監査ポリシーの設定方法についての紹介
F	イベントログをエクスポートする方法	イベントログをcsv形式などにエクスポートする方法についての紹介
G	LAPSによるローカル管理者のパスワード管理	ローカル管理者アカウントのパスワードを一元的に管理できるツール「LAPS」についての紹介
H	Active Directoryに対する攻撃の検証結果	Active Directory の認証方式を悪用した攻撃手法（Golden Ticket / Silver Ticket）をJPCERT/CCにて検証した内容と結果についての説明
I	ログとActive Direcrotyの運用に関する実態調査	JPCERT/CCが実施した国内組織におけるログの保管状況やActive Direcrotyの運用状況に関する実態調査の結果の一部を抜粋して掲載