ログを活用した **Active Directory** に対する攻撃の検知と対策

1.2 版

一般社団法人 JPCERT コーディネーションセンター

2017 年 7 月 28 日

1. はじめに

1.1. 本文書の目的

本書は、高度サイバー攻撃への備えを強化するために運用やインシデント対応の現場で活用されることを目的として、Active Directory（以下、「AD」）に対する代表的な攻撃手法、それら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などについて具体的に記述した実践的解説書である。

JPCERT/CC は、2016 年に組織ネットワークを構成する各機器のログ分析に関する考え方をまとめたドキュメント「高度サイバー攻撃への対処におけるログの活用と分析方法」を公開し、その中で AD ログの確認観点について紹介したが、運用現場で活用するにはより具体的な記載が必要との要望をいただいた。JPCERT/CC 以外からも AD の攻撃に対する対策や検知についてさまざまなドキュメントが公開されているが、代表的な攻撃手法と検知および対策方法をセットにして整理したドキュメントは見られない。このような背景から本書をまとめた。

JPCERT/CC では、AD 環境が侵害される高度サイバー攻撃の事例を多数確認しており、JPCERT/CC が対応支援を実施した被害組織のほとんどで AD の管理者アカウントであるドメイン管理者アカウントが悪用されていた。それらの組織の一部には、AD の脆弱性が放置されていたり、AD のログが十分な期間保存されていなかったりといったケースもあった。高度サイバー攻撃の脅威が高まっているにも関わらず、AD のセキュリティ対策やログを確認することの重要性が認識されておらず、防備が立ち遅れている傾向にある。

本書をまとめる活動の一環として、 JPCERT/CC は、複数の国内組織を対象にアンケートを実施し、AD のログの保管・確認状況や、ログを確認することの有効性などを調査した。その結果、多くの組織が AD のログを取得しているものの、ログ分析のノウハウや人的リソースが不足しているなどの理由で、取得したログを確認できていないなど実態がわかった。そうした状況では、侵害されても早期に気づくことができない、あるいは気づいても侵害されたコンピュータやアカウントを特定できず、有効な対策がとれないために、被害を局所化できない可能性が高い。そうした事態を避けるためにも、AD のログ保管・確認の重要性を認識いただき、攻撃の早期検知と被害抑止のために本書を活用いただければ幸いである。

経済産業省が公開している「サイバーセキュリティ経営ガイドライン Ver 1.1 [1]」にも、攻撃の段階に応じた拡大防止及び緩和を図るために、ネットワーク全体にわたる対策や日頃から攻撃を検知・記録する仕組みが、サイバーセキュリティ経営の重要項目として必要であるとされている。本書では、状況に応じた検知、対処の選定方法や、優先度についても言及している。それを各組織の運用に合わせて、組み入れてほしい。また、JPCERT/CC が実施したアンケート結果のうち国内組織におけるログの保管状況や AD の運用状況に関する実態調査については抜粋して Appendix に掲載した。末筆ながらアンケートにご協力くださった皆様には厚く感謝申し上げる。

改訂履歴

版数	発行日	改訂内容
第 1 版	2017 年 3 月 14 日	初版発行
第 1.1 版	2017 年 3 月 22 日	P30　4.3：認証イベントに関する補足事項を追記
		P37　表 6 ：「KB2871997（資格情報保護）」「Protected Users」「Restricted Admin」について、「対策が利用できるバージョン」を修正
		P51　5.2.1：krbtgt アカウントのパスワード変更における注意事項と補足事項を追記
第 1.2 版	2017 年 7 月 28 日	P9　1.4：「Executive Summary」を「概要」に修正
		P9　1.4：2 章、3 章の概要の記載を一部修正
		P17　3.2.1：対象バージョンを追記
		P19　図 6：タイトルを修正
		P28　4.2.3：対象バージョンを追記
		P29　4.2.4：対象バージョンを追記
		P37　表 6：　Credential Guard の DC への適用を対象外に修正（DC における Credential Guard は未サポートのため）
		P48　Credential Guard の DC への適用を対象外に修正
		P63　表 10：「設定値」に関する補足を追記
		P67　「検証の流れと結果」を「検証の流れ」と「結果」に分割。「検証の流れ」との内容重複のため、「検証方法」を削除
		P67　図 18：「5.クライアント端末 2 に侵入」を追加
		P69-P70　「検証の流れと結果」を「検証の流れ」と「結果」に分割。「検証の流れ」との内容重複のため、「検証方法」を削除
		P70　図 21：「5.クライアント端末 1 に侵入」を追加
		P83-P85　「参考情報」に出典元を追記
		全般　参照情報の番号および誤字脱字を修正

1.2. 想定している読者

本文書が想定している読者は次のような方々である。

- AD を運用または AD の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

なお、上記業務を他の組織から受託している組織も対象としている。

1.3. 本文書の活用方法

本節では、読者のニーズに応じて参照すべき章を示したクイックリファレンスを記載している。通読する時間のない読者は、置かれた状況と目的に応じて、必要な章を参照いただければ幸いである。

読者のニーズ	参照すべき章	本書から得られる情報
AD への攻撃手法を理解したい	2.2. 横断的侵害と Active Directory への攻撃 3. Active Directory に対する攻撃手法	AD に対する代表的な攻撃手法（ドメイン管理者アカウントなどの高い権限を窃取する手法）
ログを分析して AD への攻撃を検知したい	4. Active Directory のイベントログを活用した横断的侵害の検知	アカウントの悪用を検知するために有効なイベントログの確認ポイント
AD への攻撃を抑止（予防）するための対策を打ちたい	5.1. 予防策	攻撃を抑止するための予防的対策、ログを確認しやすい環境に改善するための適切なアカウント管理方法など
検知された AD への攻撃について対処し、悪用されたアカウントや端末を特定したい	4.2. 不審なログの有無 5.2. 攻撃を検知した場合の緊急対処	不審なログの確認ポイント（4.2）や、攻撃の被害を軽減するための緊急対処（5.2）

また、ログ調査や AD に関する参考情報などを Appendix に収録している。

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（Kerberos / NTML）の説明
C)	メモリ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	AD 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 AD 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

1.4. 概要

【2 章 高度サイバー攻撃の攻撃手法】【3 章 Active Directory に対する攻撃手法】
攻撃者は侵入した端末を起点として、組織内ネットワークを横断的に侵害する。組織内のリソースが AD によって一元管理されている環境において、ドメイン管理者アカウントは AD が管理する全てのリソースをコントロールすることが可能である。そのため、攻撃者は AD 環境に対する攻撃を行い、ドメイン管理者アカウントなどの高い権限の窃取を試みる。攻撃者がドメイン管理者権限の窃取に成功した場合は、大きな脅威となる。

AD では認証チケットなどを使用した認証方式が使用されるが、それらを悪用した以下のような攻撃手法が用いられることが多い。

- AD の脆弱性の悪用によるドメイン管理者への権限昇格
- 端末に保存されたアカウントの認証情報を悪用したなりすまし

上記のような手法を使用してドメイン管理者権限などの窃取に成功した攻撃者は、Golden Ticket や Silver Ticket と呼ばれる長期的に使用できる認証チケットを作成し、任意のアカウントになりすました上で、横断的侵害の拡大や情報窃取などの攻撃活動を行う。

【4 章 Active Directory のイベントログを活用した横断的侵害の検知】
上述のような攻撃活動の痕跡が組織内の機器のログに記録されるため、ログを活用して攻撃を早期に検知できれば、機密情報の流出など最悪の事態を防ぐことができる。Windows では、認証のログがイベントログとして記録される。そのため、AD のイベントログを定期的に確認することでアカウントの悪用を早期に検知できる可能性がある。ただし、イベントログはデフォルト設定では保存される上限サイズが小さく、大規模な組織では 1 日分も保存されないことがあるため、イベントログが十分保存される設定になっているかを確認する必要がある。

本書では、特にドメイン管理者アカウントの悪用を検知するために有効なイベントログの確認方法について、以下 2 つの確認観点を紹介する。

- 不審なログの有無
  AD に対する攻撃を受けた際に記録される可能性があるイベントログの例を紹介しており、検索コマンドなどを使用して比較的容易に検索することが可能である。AD の脆弱性を悪用した攻撃が試行された際に記録されるエラーコードや、特定の攻撃ツールで作成された Golden Ticket / Silver Ticket が使用された場合に記録される特徴的な文字列などを紹介する。

- 認証ログの調査

認証に関するイベントを以下①～③のような観点で確認し、意図しないアカウントの利用がないかを確認することでアカウントの悪用を検知できる場合がある。しかし、攻撃を受けても一目で判断できる特異なログが記録されるケースは少ないため、平常時（運用）との比較が必要となる。

①想定していないアカウントが特権を利用していないか
②特権アカウントを使用している端末が意図したものか
③認証回数の推移に不審な挙動がないか

なお、ログからアカウントの悪用を検知するためには、適切なアカウントの運用を行い、ログを確認しやすい環境にすることも重要である。

【5 章 Active Directory に対する攻撃の対策】

AD に対する攻撃を抑止するための予防策、攻撃を検知した場合に被害を軽減するための対策について紹介する。各攻撃手法に対して効果が期待できる対策や、その適用範囲についても示しているため、自組織の状況に応じて優先度をつけて対策を実施いただきたい。

【5.1 節 予防策】

攻撃を抑止するための予防的対策について紹介する。組織や運用の状況にあわせた複数の対策をあわせて実施することで、攻撃が成功する可能性を低減できる。攻撃者はドメイン管理者権限の窃取を試みることが多いため、ドメイン管理者アカウントを守ることが重要である。以下は予防策の概要である。

予防策	説明
管理専用端末の設置	AD やサーバの管理に使用する端末を管理用途に専用化することで、マルウエア感染などの可能性を軽減する
セグメント化	ネットワークセグメントを分離し、DC やサーバに対して不要なリモートアクセスを制限することで侵害された端末からの侵害を抑止する。また、各セグメントで使用する管理者アカウントを分離し、許可されたアカウントのみ DC やサーバへアクセスできるように制限する
付与する特権の最小化	ドメイン管理者権限など特権が必要なアカウントの棚卸を行い、運用で不要な特権を削除する
セキュリティ更新プログラムの適用	脆弱性悪用の抑止や、追加のセキュリティ機能を有効にするために更新プログラムを適用する。優先的に適用してほしい更新プログラムについても紹介する
認証情報の保護	コンピュータのメモリなどに認証情報を保存しない機能や、保存される認証情報を保護する機能について紹介する
適切なパスワードの設定	特に管理者アカウントについて共通パスワードの使用を避け、アカウント毎に強固なパスワードを設定する

【5.2 節 攻撃を検知した場合の緊急対処】

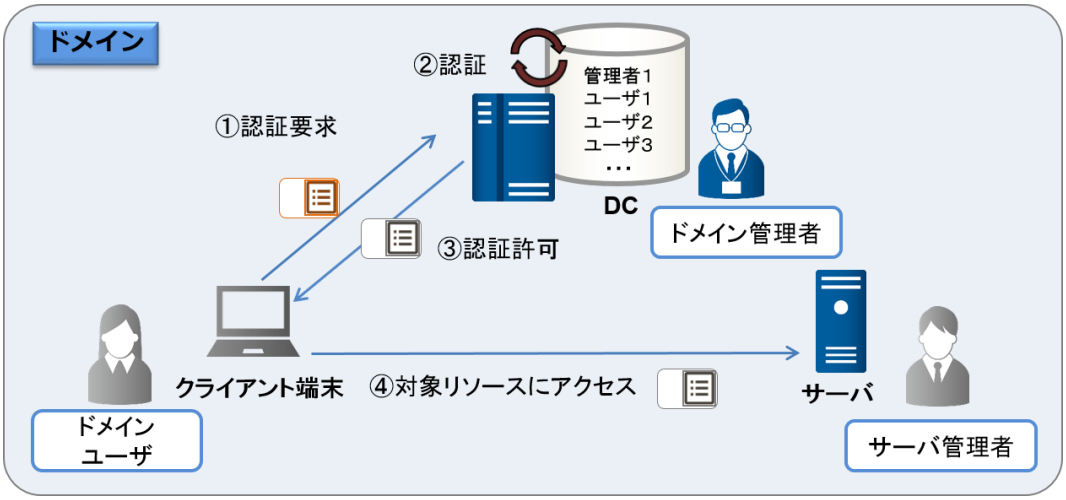
AD に対する攻撃を検知した場合、アカウント悪用による被害を軽減するために実施すべき緊急対処について紹介する。本書で紹介するのはあくまで緊急対処であり、セキュリティベンダなどの専門組織に協力を依頼することも検討いただきたい。

ドメイン管理者権限やサーバ管理者権限が窃取された場合、Golden Ticket / Silver Ticket が作成されるケースが多く、それらを使った攻撃を抑止するための対策を紹介する。以下は緊急対処の概要である。

緊急対処	説明
krbtgt アカウントのパスワード変更	Golden Ticket を使った攻撃を抑止するために、krbtgt という DC 上のビルトインサービスアカウントのパスワードを 2 回連続で変更する。ドメイン管理者アカウントのパスワード変更も合わせて実施する
サービスを実行しているアカウント（コンピュータアカウント）のパスワード変更	Silver Ticket を使った攻撃の多くは、侵害を受けたコンピュータのコンピュータアカウントのパスワードを 2 回連続で変更することで抑止できる。被害範囲の特定が難しい場合は、DC、重要なサーバ、それらの管理専用端末について優先的に実施する 当該コンピュータの管理者アカウントのパスワード変更も合わせて実施する

1.5. Active Directory の概要

AD は、組織内のコンピュータやユーザを集中的に管理するために Microsoft 社が提供しているディレクトリ管理サービスである。AD においては、コンピュータやユーザを管理する際の管理単位をドメイン、ドメインを管理するための認証サーバを Domain Controller（以下、「DC」）と呼ぶ。



［図 1. AD の概要］

リソースが AD によって一元管理されている環境（以下、「AD 環境」）では、Kerberos 認証や NTLM 認証などにより認証が行われる（詳細は「Appendix B) Active Directory で使用される認証方式」を参照のこと）。Kerberos 認証では認証チケットを使用して、DC で一元的に認証を行う。
AD の管理者アカウントであるドメイン管理者アカウントは、AD が管理しているドメイン配下の全てのリソースをコントロールする権限をもつ。

なお、Samba でも AD の機能を提供しているが[*1]、本文書では Windows OS の DC によって AD を実現している環境に関して記述している。

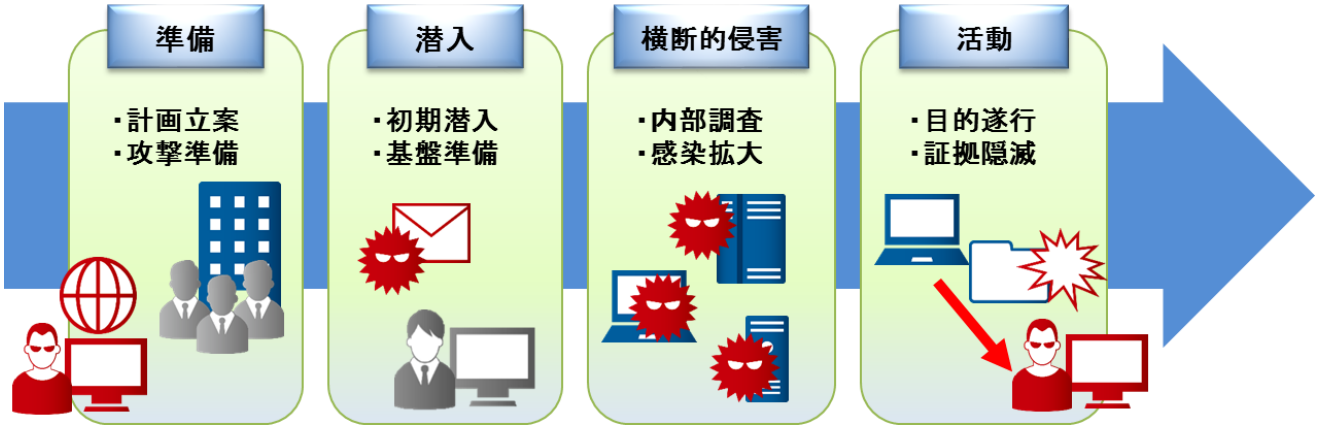
[*1] Samba 4.0 以降では、Samba を DC として動作させることが可能である。

2. 高度サイバー攻撃の手法

近年、高度サイバー攻撃による被害が国内企業においても頻発している。高度サイバー攻撃の攻撃者は明確な目的を持っており、それを達成するまで長期間に渡って組織内ネットワークに潜伏し続け、執拗に攻撃を繰り返す。本章では、典型的な高度サイバー攻撃の過程を紹介する。

2.1. 高度サイバー攻撃のプロセス

高度サイバー攻撃は、標的の選定から目的達成まで、以下のようなプロセスで行われる。



［図 2. 高度サイバー攻撃のプロセス］

(1) 準備：標的組織の情報を入念に調査し、攻撃ツールやマルウエアの作成など、攻撃の準備を整える
(2) 潜入：実行ファイルを添付した標的型メールの送付や不正な URL への誘導などにより、組織内の端末をマルウエアに感染させる
(3) 横断的侵害：感染端末を遠隔操作することで、その他の脆弱な端末の探索や感染の拡大を行い、組織内ネットワークを横断的に侵害する
(4) 目的達成：機密情報の窃取など、本来の目的を達成する

潜入には、業務メールを装った標的型メールの送付や、標的組織の利用者が日常的に閲覧している正規サイトを改ざんするなどの手段が用いられるが、その手法は日々巧妙化しており、組織内ネットワークへの侵入を完全に防ぐことはほぼ不可能である。したがって、潜入されてから目的達成に至るまでの段階で早期に検知し対処できるかどうかが、機密情報の漏洩などの被害を最小限に抑えられるか否かの分かれ目となる。

2.2. 横断的侵害と Active Directory への攻撃

侵入した端末から目的とする情報へアクセスできない場合、その情報を求めて攻撃者は組織内ネットワークを横断的に侵害し、マルウエア感染を拡大させようとする。そのために、攻撃者は C2 サーバ*2 経由で感染端末を遠隔操作し、組織ネットワークの構成や目的とする情報へのアクセス権を持つアカウント、重要なサーバの情報などを調査する。その際に、組織内のリソースが AD によって管理されている場合には、AD 環境を攻撃し、認証情報の窃取やより権限の高いアカウントの認証情報を窃取し、それを用いて横断的なシステム侵害を試みる。JPCERT/CC が対応支援した高度サイバー攻撃の事例においても、AD の侵害やドメイン管理者アカウントの悪用が確認されたことを受けて注意喚起を発行している[2]。

次節では、高度サイバー攻撃で使用されることが多い AD に対する攻撃手法について記述する。

*2 攻撃者が感染端末の遠隔操作を行うためのサーバ。マルウエアは C2 サーバと HTTP/HTTPS などを使用して定期的に通信を行い、受信した命令の実行や窃取した情報の送信などを行う。C&C （Command and Control） サーバとも呼ばれる。

3. Active Directory に対する攻撃手法

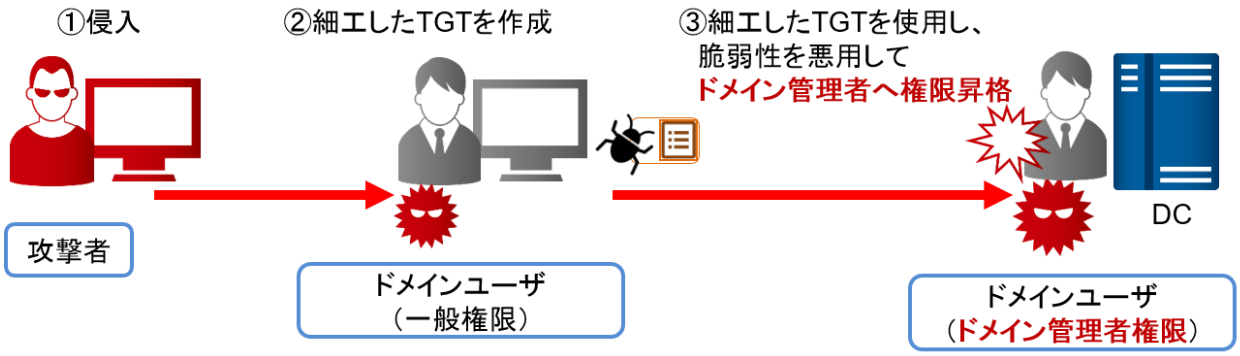
高度サイバー攻撃の横断的侵害のフェーズで、攻撃者は AD 環境からドメイン管理者やサーバの管理者権限を窃取しようとする[3]。窃取に成功すれば、正規の管理者になりすまして、長期にわたって使えるアクセス権限を獲得し、横断的侵害を試みる。

攻撃者は AD 環境からドメイン管理者やサーバの管理者権限を窃取するために、AD 環境で主に使用される Kerberos 認証や NTLM 認証の仕様上の弱点を悪用することがある。それらの攻撃手法やツールがインターネットに公開されており、こうしたツールを利用すれば、比較的容易に AD を攻撃できる。

以下、Kerberos 認証と NTLM 認証の弱点を悪用して AD を攻撃する代表的な手法を紹介する。

3.1. Active Directory の脆弱性の悪用

AD の脆弱性の一例として、2014 年に公開された MS14-068 Kerberos KDC（Key Distribution Center）の脆弱性があり、JPCERT/CC でも本脆弱性が高度サイバー攻撃で悪用されていることを確認している[4]。本脆弱性は TGT（Ticket-Granting Tickets:「Appendix B)「1. Kerberos 認証」」を参照）の検証不備に起因し、これを悪用するとドメインユーザ（Domain Users グループに所属するアカウントなど）がドメイン管理者権限に昇格できる。インターネット上に本脆弱性を悪用した攻撃ツールも公開されており、ドメインユーザが使用する端末などのローカル管理者権限やドメインユーザの認証情報が窃取できれば、比較的容易にドメイン管理者権限を獲得できる。



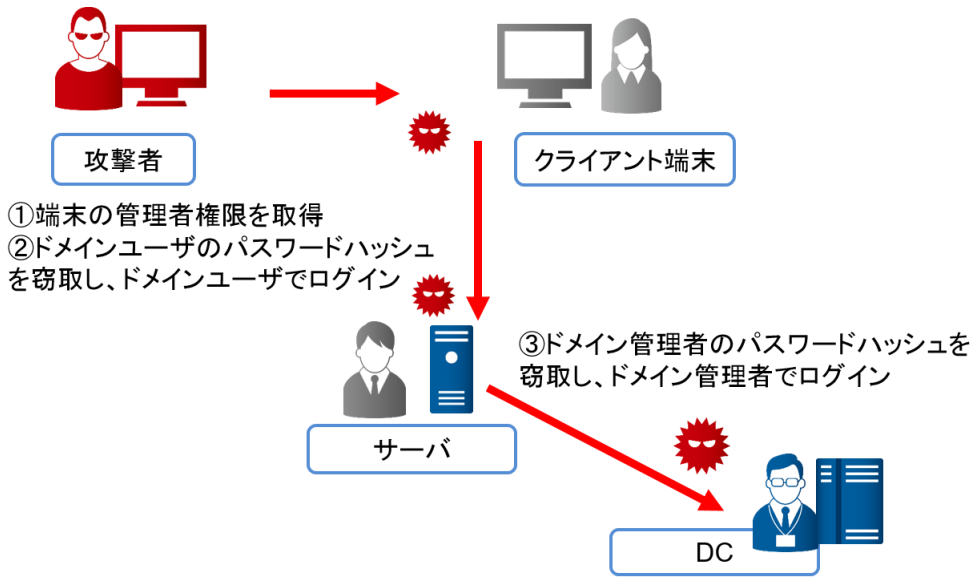
［図 3. Kerberos KDC の脆弱性を悪用した攻撃］

3.2. 端末に保存された認証情報の悪用

Windows OS のメモリ空間などには、端末上で使用したユーザの認証情報（パスワードハッシュ、認証チケットなど）が保存される。侵害した端末のローカル管理者権限を窃取した攻撃者は、攻撃ツールを使用してメモリなどに保存されている認証情報を窃取できる。
特に、Windows 8.1 / Windows Server 2012 R2 より前のバージョンの Windows では、容易に平文に復元できるパスワードハッシュや平文パスワードがメモリ上に保存されるため、パスワードを窃取される危険性が高い（詳細は「Appendix C) メモリに保存される認証情報」を参照）。
平文パスワードを獲得できなくても、窃取した認証情報を悪用して他のコンピュータに不正にアクセスする代表的な手法として、Pass-the-Hash や Pass-the-Ticket がある。

3.2.1. Pass-the-Hash

NTLM 認証で使用されるパスワードハッシュをメモリなどから窃取し、他のコンピュータに不正にアクセスする攻撃手法が Pass-the-Hash である[5]。短いパスワードや単純なパスワードを設定している場合、総当たり攻撃や辞書攻撃などによってパスワードを割り出して、他のコンピュータへアクセスできる可能性がある。しかし、Pass-the-Hash を使用すると、平文のパスワードを入手できなくてもパスワードハッシュを使用して他のコンピュータへアクセスできる。
特に、Windows 7、Windows Server 2008 よりも前のバージョンでは、デフォルトで保存される LM ハッシュや NTLM v1 ハッシュは、パスワードが同じならばハッシュも同じ値になるので、パスワードが使い回されている場合には、攻撃が成功する可能性が一層高まる。

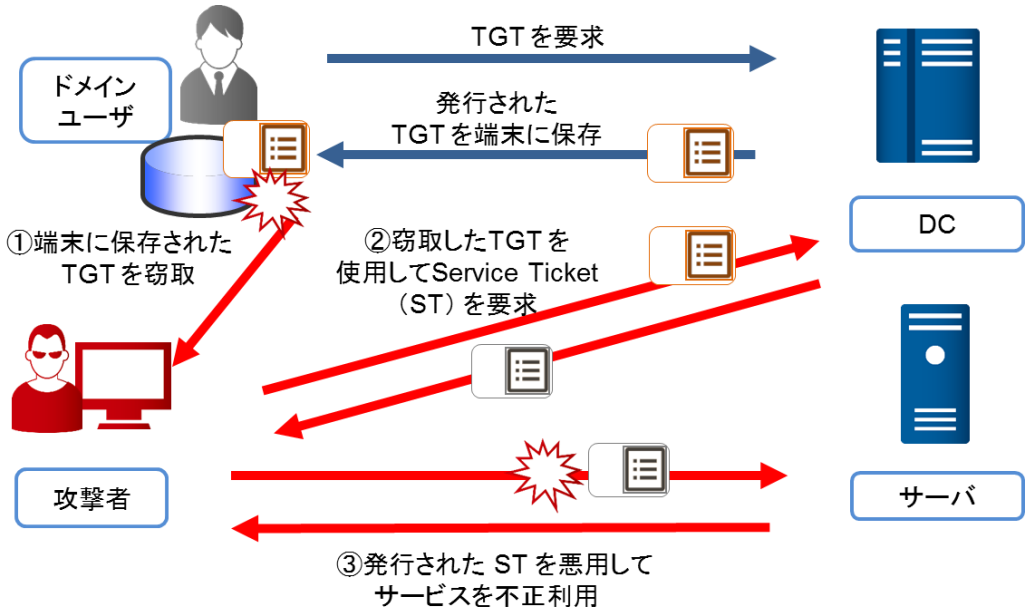


［図 4. Pass-the-Hash 攻撃の例］

3.2.2. Pass-the-Ticket

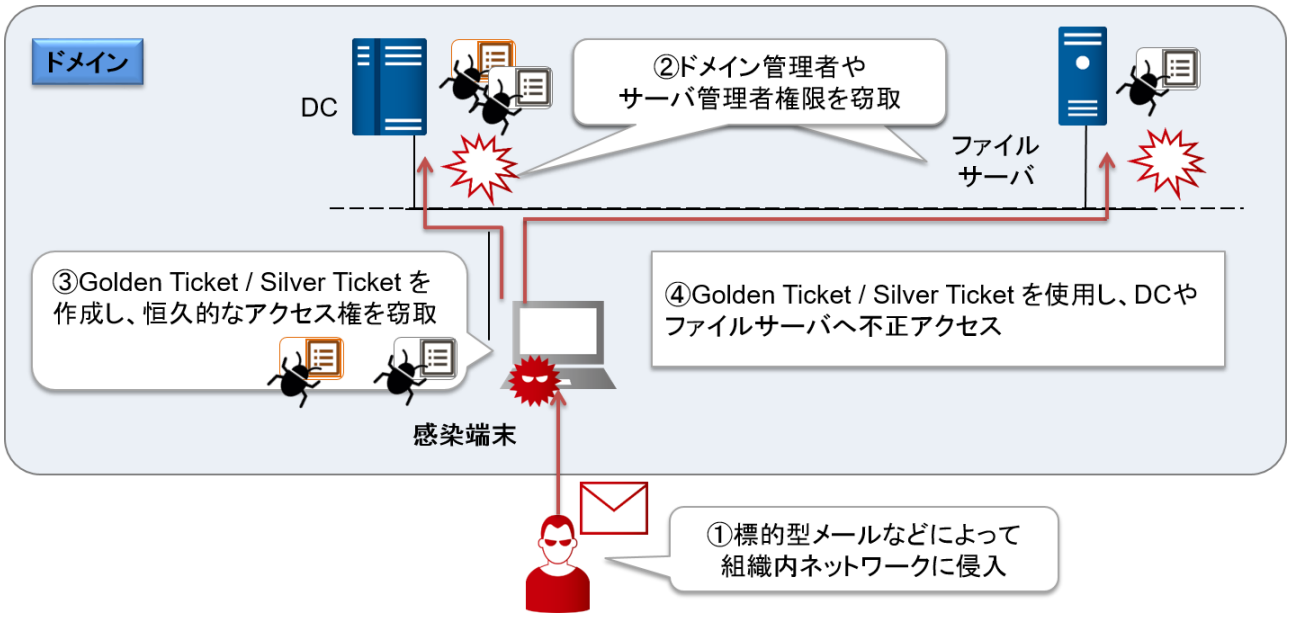
Kerberos 認証で使用される正規の認証チケットをメモリなどから窃取し、正規のユーザになりすまして

ドメインのサービスを不正に使用する攻撃手法が Pass-the-Ticket である。



［図 5. Pass-the-Ticket 攻撃の例］

攻撃者は、長期的に利用できるアクセス権限を獲得したり、攻撃の検知を回避する目的で、ドメイン管理者やコンピュータの管理者になりすませる Golden Ticket や Silver Ticket と呼ばれる Kerberos 認証チケットを作成する。これらは、攻撃者が攻撃ツールを用いて不正に作成することが可能で、有効期限が 10 年と長く、期限内であれば何度でも再利用できる（次節参照）。



［図 6. Golden Ticket および Silver Ticket を利用した攻撃の流れ］

3.2.2.1. Golden Ticket

Golden Ticket は攻撃者が不正に作成した TGT であり、Golden Ticket を使用することで、ドメイン管理者を含む任意のアカウントになりすますことが可能になる。Golden Ticket を作成するためには、krbtgt アカウント*3のパスワードハッシュが必要であり、ドメイン管理者権限を窃取していることが前提となる。krbtgt アカウントのパスワードハッシュの窃取に成功した攻撃者は任意の端末上で Golden Ticket を作成し、使用できるようになる。さらに Golden Ticket は、一旦入手できれば、なりすましたアカウントのパスワードが変更された後や MS14-068（3.1 節参照）のセキュリティ更新プログラム適用後においても、継続して使用できる。

Golden Ticket を悪用する攻撃について JPCERT/CC にて検証を行った。攻撃シナリオと検証結果については「Appendix H) 「1. Golden Ticket を悪用した攻撃の検証」」を参照のこと。

3.2.2.2. Silver Ticket

Silver Ticket は攻撃者が不正に作成した ST（Service Ticket:「Appendix B)「1. Kerberos 認証」」を参照）であり、Silver Ticket を使用することで、特定の Windows サービス（ファイル共有やタスクスケジューラなど）に対して、サーバの管理者やサービスの利用者になりすましてアクセスすることが可能になる。Silver Ticket を作成するためには、対象サービスを実行しているアカウントの NTLM ハッシュが必要である。サービスを実行しているアカウントはサービスによってさまざまであるが、ファイル共有やリモートアクセスなどの機能を提供する CIFS サービスや、タスクスケジューラなどの機能を提供する HOST サー

*3 TGT の署名などを行う DC 上のサービスアカウント。

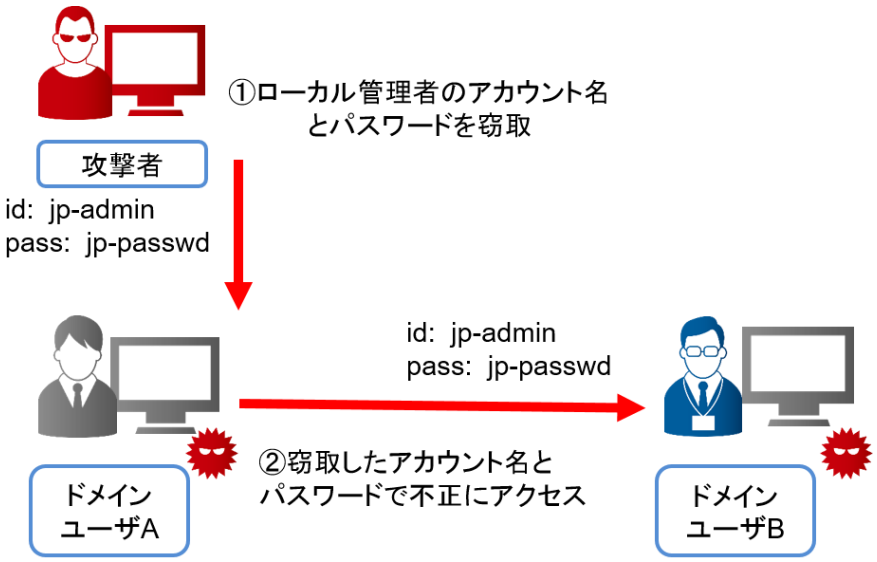
ビスはコンピュータアカウント*4 によって実行される。コンピュータのローカル管理者権限を窃取していれば、メモリ上などからコンピュータアカウントなど、サービスを実行しているアカウントの NTLM ハッシュを窃取することができる。

また、Silver Ticket を使用する際には、サービスを実行しているコンピュータに直接認証を要求するため、DC には認証を要求しない。そのため DC には認証ログが記録されず、攻撃を検知しづらい。

Silver Ticket を悪用する攻撃について JPCERT/CC にて検証を行った。攻撃シナリオと検証結果については「Appendix H)「2. Silver Ticket を悪用した攻撃の検証」」を参照のこと。

3.3. ローカル管理者アカウントの悪用

運用の効率化や端末のセットアップの都合などで、各コンピュータ上のローカル管理者アカウントに対し、共通のアカウント名、パスワードを設定している場合がある。このような環境では、1 台のコンピュータ上でローカル管理者アカウントのパスワードが窃取されると、それを使用して他のコンピュータへもログインできるようになる。その中にドメイン管理者やサーバの管理者が使用するコンピュータがあれば、特権アカウントの認証情報を窃取される可能性もある。



［図 7. ローカル管理者アカウントを悪用した攻撃の例］

*4 ドメインに参加しているコンピュータを一意に識別するためのアカウント。コンピュータアカウントは、コンピュータ名の後に"$"（ドル記号）を付けたアカウント名で作成される。
コンピューターアカウントとは
https://technet.microsoft.com/ja-jp/library/cc731641

4. Active Directory のイベントログを活用した横断的侵害の検知

横断的侵害を早期に発見することで、高度サイバー攻撃の被害を最小化することが可能である。また、攻撃の痕跡を調べることで、攻撃の状況や、悪用されたアカウントやコンピュータなどを把握することができ、適切な対策を講じることが可能となる。これら攻撃の痕跡を調べる上で非常に重要となるのが、適切なアカウント管理などの運用と、ログの保管・調査である。ログの保存期間の考え方については参考資料[6]を参照のこと。

高度サイバー攻撃対応のために保管･調査すべき主要なログの一つにAD環境のイベントログが挙げられ、DC に一元的に記録される。AD のイベントログには、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ており、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知る手掛かりとなる情報が含まれている。ただし、ST の有効期限内は DC に認証要求を行わず、接続先のサーバにのみ認証に関連するイベントが記録されるため、重要なサーバについても定期的にイベントログを確認することが望ましい。

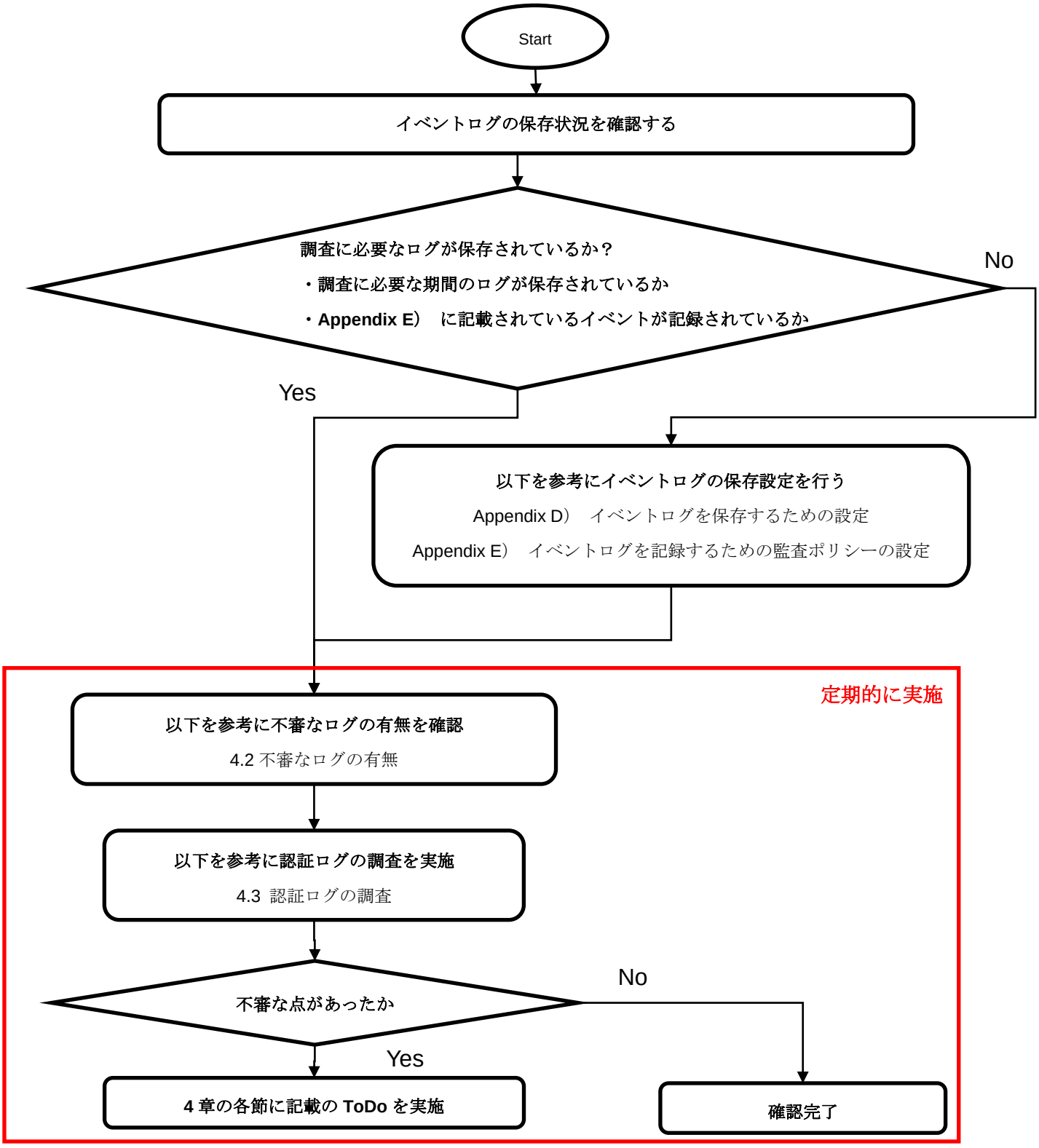
クライアント端末にも認証に関連するログが記録されるが、多数のクライアント端末のログを確認するのは時間がかかるため、まずは DC やサーバのイベントログを確認して不審な端末を絞り込んだうえで個々の端末の調査を行うことで、効率的な調査が可能になる。

本章では、AD に対する攻撃の検知、特にドメイン管理者アカウントの悪用を検知するために有効なイベントログの確認方法について紹介する。なお、本章で紹介するのは、侵害されている可能性があるアカウントやコンピュータを見つけるためのポイントであり、侵害されたコンピュータのログを詳細に調査する方法（フォレンジック）については記載していない。こちらについては、参考資料[7]を参照のこと。
また、イベントログが記録されるためには、対応する監査ポリシーが有効になっている必要がある。監査ポリシーの設定については「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」を参照のこと。

なお、ログからアカウントの悪用を検知するためには、平常時のアカウントの運用状況を把握しておくとともに、特権の使用を最小化するなど、検知しやすい運用環境に改善することも重要である。本章を参考に、平常時を含めた定期的なログ調査と、運用の見直しを実施していただきたい。

4.1. ログ確認のフロー

イベントログを確認する手順の流れを以下に示す。以下のフローに沿って、必要な章や節を参照し、ログ確認を実施いただきたい。



［図 8. イベントログ確認のフロー］

表 1 に、攻撃手法と有効なイベントログの調査方法の対応を示す。

［表 1. Active Directory に対する攻撃と有効なイベントログの調査方法］

		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

また、ログの確認対象（調査するログの発生元となるコンピュータ）および確認が有効な OS のバージョンを表 2 に示す。

［表 2. ログの確認対象］

		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、2008 R2、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

なお、Windows のイベントログはそのままのデータ形式では調査が困難である。イベントを CSV などの形式で保存する Windows 標準の機能 （「Appendix F) イベントログをエクスポートする方法」を参照）や Log Parser*5などを使用してテキスト形式に出力する、あるいはログ管理ソフトウエアや SIEM*6を用いてログを収集すると、検索しやすくなり、調査が比較的行いやすくなる。

*5 Log Parser 2.2 日本語版
クエリを使用してイベントログなどから情報を抽出することができる Microsoft 社が無償で提供しているツール
https://technet.microsoft.com/ja-jp/scriptcenter/dd919274.aspx
*6 Security Information and Event Management。さまざまなサーバや機器のログを一元的に管理するシステムのこと。

4.2. 不審なログの調査

本節では、AD に対する攻撃を受けた際に記録されるイベントログを調査する方法について説明する。本節で紹介するログは、grep などの文字列検索コマンドを使用して比較的容易に見つけ出すことができ、不審な活動を効率的に検知できる可能性がある。
それぞれの調査について、前提条件や実施すべき内容など次の各項目を表形式にまとめているので、調査のハンドブックとしても利用してほしい。

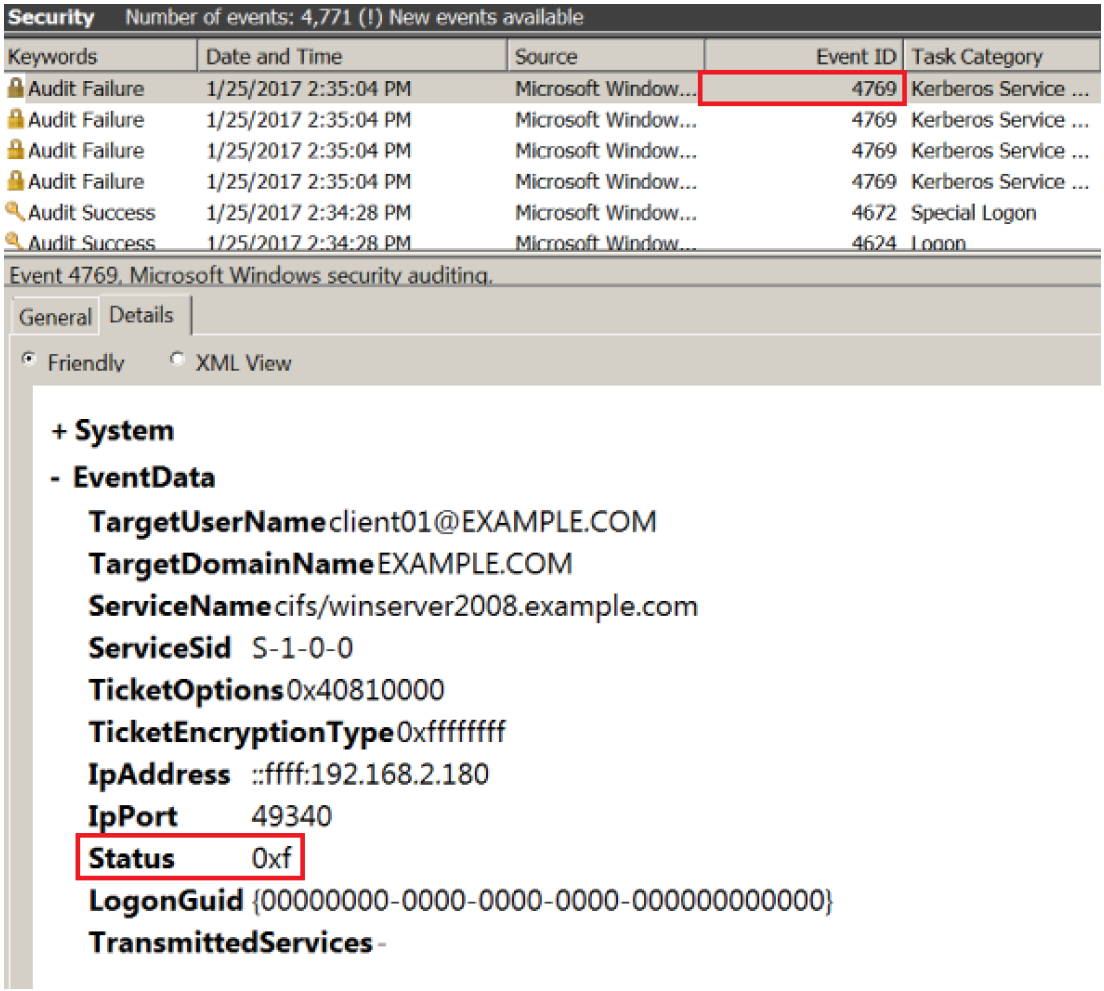
調査対象：確認の対象となるコンピュータやアカウント
前提条件：攻撃を検知するための前提条件
確認事項：確認すべき事項
ToDo：攻撃を疑わせるログが見つかった場合の対処法
注意事項：調査にあたっての注意事項
補足：補足事項

4.2.1. MS14-068 の脆弱性を悪用した攻撃の調査

MS14-068 の脆弱性を悪用した攻撃が行われた場合、対応するセキュリティ更新プログラムを適用した環境では、攻撃（権限昇格）が失敗したことがイベントログに記録される。

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, 2008 R2, 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り、かつイベント 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」*7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

*7 RFC 1510 における KDC_ERR_SUMTYPE_NOSUPP (チェックサムのタイプがサポートされていない) のエラーコードを示す。
https://technet.microsoft.com/en-us/library/bb463166.aspx



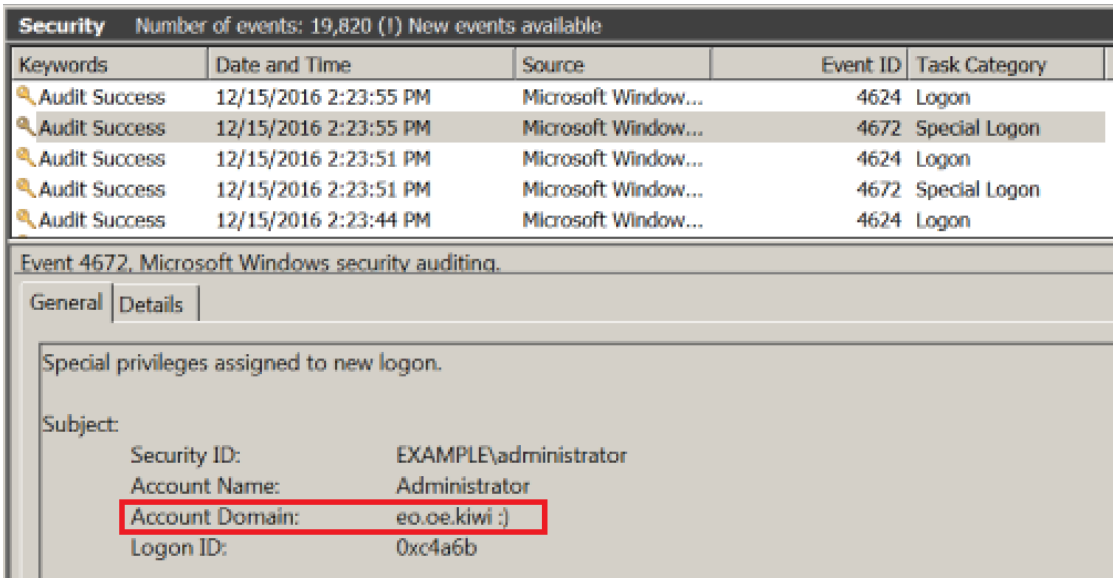
[図 9. MS14-068 の攻撃が施行された際に記録されるエラーコード]

上記の例では、「IpAddress」（クライアントアドレス）に記録されている端末上で、ドメインユーザ client01 が権限昇格を試みたが、失敗し、「Status」（エラーコード）「0xf」が記録されている。

4.2.2. Golden Ticket / Silver Ticket の使用の調査

古いバージョンの特定の攻撃ツールで作成された Golden Ticket / Silver Ticket が使用された場合、認証イベントに特徴的な文字列が記録されることがある。

Golden Ticket / Silver Ticket の使用の調査	
調査対象	DC 、サーバ、 DC・サーバの管理に使用する端末
前提条件	特になし
確認事項	イベント ID 4624, 4672 などの認証イベントの「アカウントドメイン」に次の文字列が記録されていれば、古いバージョンの特定の攻撃ツールで作成された Golden Ticket / Silver Ticket が使用されている可能性がある eo.oe.kiwi : ） <3 eo.oe ? ANSSI E>
ToDo	確認事項に該当するログがあった場合、「5.2. 攻撃を検知した場合の緊急対処」に記載の対策を実施する。イベントの認証要求元であるコンピュータも侵害されている可能性が高いため、ネットワークから隔離し、調査する
注意事項	・ 攻撃ツールやツールのバージョンによっては記録されないため、該当する文字列が見つからない場合でも、攻撃されている可能性がある ・ SilverTicket が使用された場合には、DC には認証イベントが記録されず、接続先のサーバにのみ認証イベントが記録される



［図 10. Golden Ticket / Silver Ticket が使用された際に記録される文字列］

上記の例では、DC の administrator アカウントに対する Golden Ticket が使用されて、イベント ID : 4672（特権割当）のアカウントドメインに「eo.oe.kiwi : ）」が記録されている。

4.2.3. 不審なタスク作成の調査

攻撃者は、侵害したコンピュータ上でプログラムを実行するために、タスクを作成することがある。

不審なタスク作成の調査	
調査対象	DC、サーバ DC・サーバの管理に使用する端末（可能であれば実施）
前提条件	特になし
確認事項	次の各項目を調べ、運用で使用していないタスクを探す。そのようなタスクが作成されている場合は、攻撃を受けている可能性がある – イベント ID 4698 などのタスクに関連するイベント – 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 ➢ C:¥Windows¥System32¥Tasks¥[タスク名] ➢ C:¥Windows¥Tasks¥[タスク名].job （at コマンドを使用してタスクを作成した場合、“At[数字].job” という名前でタスクが作成される）
ToDo	運用で使用していないタスクが作成されている場合には、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
注意事項	・ デフォルトではイベント ID 4698 が記録されないため、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 ・ イベント ID は Windows 7、Windows Server 2008 以降を対象としている
補足	攻撃者が Silver Ticket を使用してタスクの作成を行った場合、タスクの作成者はオリジナルのアカウント名（Silver Ticket を使ってなりすます前のアカウント名）が記録されるため、悪用されたアカウントを特定できる可能性がある

4.2.4. イベントログ消去の調査

攻撃者は、活動の痕跡を消すためにイベントログを消去する可能性がある。

イベントログ消去の調査	
調査対象	DC、サーバ DC・サーバの管理に使用する端末（可能であれば実施）
前提条件	特になし
確認事項	イベントログを消去した時に記録されるイベント ID 1102 を探す。見つかった場合には、正規の運用者による消去かどうかを確認する
ToDo	正規の運用者以外がイベントログの消去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
注意事項	イベント ID は Windows 7、Windows Server 2008 以降を対象としている

4.3. 認証ログの調査

前節（「4.2. 不審なログの調査」）では、比較的容易に調査できるイベントログについて記述した。本節では、平常時（運用）と比較することで検知できる可能のあるイベントログについて記述する。

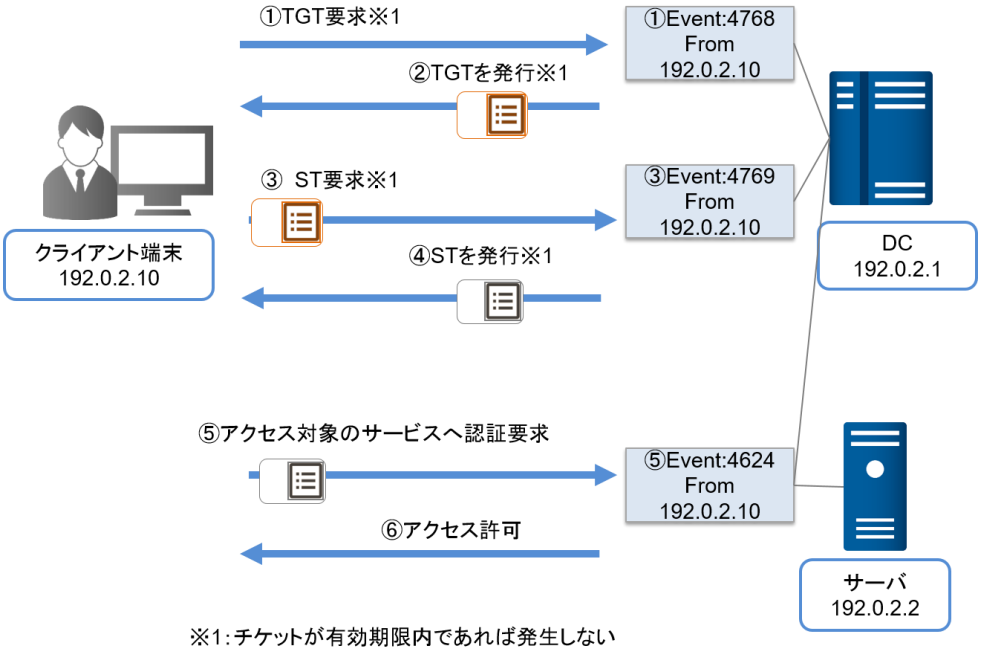
ドメインユーザを使用してコンピュータにアクセスを行った場合、DC や接続先のコンピュータに認証に関連するイベントログが記録される。認証イベントに記録される認証要求元端末やアカウント名などの情報を調査し、意図しないアカウントの利用がないかを確認することで、アカウントの悪用を検知できる場合がある。

参考までに、主要な認証イベントの例（表 3）と、Kerberos 認証を行った際に DC やサーバにどのようにログが記録されるかを示したイメージ（図 11）を以下に示す。

［表 3. 主要な認証イベントの例］

イベントID	説明	イベントログの項目名				備考
		アカウント名	認証要求元端末 (IPアドレス)	認証要求元端末 (コンピュータ名)	結果コード	
4624	ログインの成功	新しいログオン: アカウント名：	ネットワーク情報: ソース ネットワーク アドレス:	ネットワーク情報: ワークステーション名:	—	認証方式によらず、ログインの成功時に記録される
4625	ログインの失敗	ログオンを失敗したアカウント: アカウント名:	ネットワーク情報: ソース ネットワーク アドレス:	ネットワーク情報: ワークステーション名:	エラー情報: 状態:	認証方式によらず、ログインの失敗時に記録される。「エラー情報:」にはログイン失敗の原因を示すエラーコードが記録される
4768	Kerberos 認証 (TGT 要求)	アカウント情報: アカウント名：	ネットワーク情報: クライアント アドレス:	—	結果コード:	結果コード0x0:成功、それ以外:失敗
4769	Kerberos 認証 (ST 要求)	アカウント情報: アカウント名:	ネットワーク情報: クライアント アドレス:	—	エラー コード:	エラーコード0x0:成功、それ以外:失敗
4776	NTLM 認証	ログオアカウント:	—	ソースワークステーション:	エラーコード:	エラーコード0x0:成功、それ以外:失敗
4672	特権の割り当て	アカウント名:	—	—	—	ドメイン管理者やローカル管理者以外の特定の特権のみを持つアカウントを使用した際にも記録される

※上記イベント ID は Windows Server 2008 以降を対象としている。



［図 11. Kerberos 認証で記録されるログのイメージ図］

認証イベントに関する補足事項

- リモートデスクトップなどを使用して対話型ログオン*8を行った際に、接続元（図 11 の例では 192.0.2.10）／接続先（図 11 の例では 192.0.2.2）の両方からの認証要求が DC に記録されることがある
- Windows 7、Windows Server 2008、2008 R2 において、ローカルアカウントでドメインに参加するコンピュータにログインし、タスクの履歴を表示した場合、イベント ID 4625 および 4776 が DC に

*8 コンソールやターミナルサービスから、CTRL+ALT+DEL キーを押下してログオンするログオン方式
What is Interactive Logon?
https://technet.microsoft.com/en-us/library/cc780095

記録される不具合が報告されている[25]。本現象が発生した場合、イベント ID 4625 の「アカウントドメイン」がドメイン名ではなく、各コンピュータのコンピュータ名が記録される

・ 一度の認証で、複数の同じ認証イベントが重複して記録されることがある

認証に関するイベントログの調査ポイントとして、以下が挙げられる。

［表 4. 認証に関するイベントログの確認ポイント］

調査の観点	調査事項	補足
① どのアカウントが特権を得たか	想定していないアカウントが特権を得た記録がないか	grep などの検索コマンドを使用して比較的容易に検索が可能であり、アカウントの悪用を効果的に検知できる可能性があるため、優先的に実施することを推奨する
② どの端末上で特権が使われたか	特権アカウントを使用している端末が運用で意図したものか	攻撃を受けても一目で判断できる特異なログが記録されるケースは少ないため、平常時（運用）との比較が必要となる。確認に工数もかかるが、可能であれば実施いただきたい
③ 認証要求回数に急激な変化がないか	アカウント・端末ごとの認証回数の推移を確認し、不審な挙動がないか	

以下、各確認観点の詳細について記載する。

4.3.1. 特権の割り当ての妥当性の調査

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するとイベント ID 4672 が記録される。特権を得ることを想定していないアカウントに対して本イベントが記録されている場合は、MS14-068 の脆弱性悪用などにより、攻撃者が不正に権限昇格を行っている可能性がある。

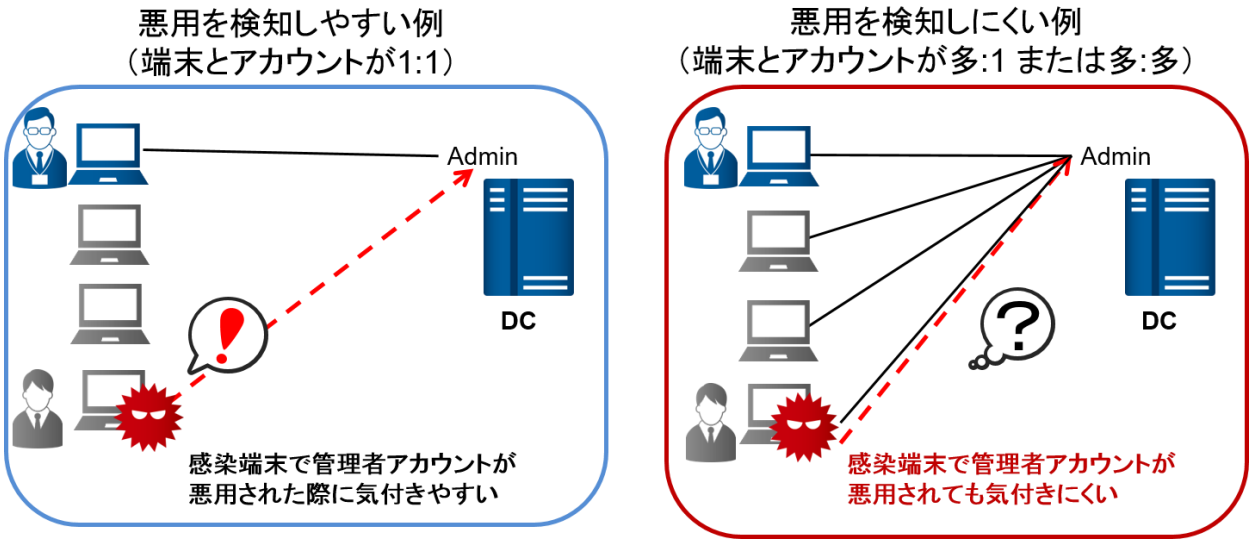
特権の割り当ての妥当性の調査	
調査対象	DC、サーバ：全てのアカウント
前提条件	特になし
確認事項	イベント ID 4672 の「アカウント名」に特権を使用することを想定していないアカウントが記録されている場合は、MS14-068 の脆弱性などを悪用し、不正に権限昇格を行っている可能性がある
ToDo	特権を使用することを想定していないアカウントについて、以下を実施する ・ 特権を割り当てていない場合は、攻撃者が不正に権限昇格を行っている可能性があると判断し、アカウントを無効化するとともにアカウントを使用している端末を調査 ・ 不要な特権が割り当てられていた場合は削除
補足	Windows 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

4.3.2. アカウントを利用した端末の妥当性の調査

特権アカウントを利用した端末が妥当か確認する。妥当でない端末上でアカウントを利用したログが記録されている場合、そのアカウントが悪用されている疑いがある。

アカウントを使用している端末の調査	
調査対象	DC：ドメイン管理者アカウント サーバ：サーバ管理者アカウント DC、サーバの管理専用端末：管理専用端末のローカル管理者アカウント（可能であれば実施）
前提条件	管理者アカウントを使用する端末を精査済みであること（次ページ参照）
確認事項	イベント ID が 4624,4625,4768,4769,4776 のイベントに記録されたアカウント名や認証要求端末を確認し、運用で意図しない利用がないかを以下の観点で確認を行う。運用で意図しない利用が確認された場合は、アカウントが侵害されている可能性がある。 ・当該端末で利用するはずがないアカウントが利用されていないか ・DC やサーバに対して、認証要求を行うはずがない端末から認証要求が行われていないか ・特定のアカウントに対して複数の端末から認証要求が行われていないか ・特定の端末から複数のアカウントに対して認証要求が行われていないか
ToDo	意図しない利用が確認されたアカウントや端末について、以下を実施する。 ・ ヒアリングなどによってアカウントの使用状況を確認。意図せずアカウントが使用されている場合は、アカウントや端末を調査 ・ 不要な管理アカウントの削除や、管理者アカウントを使用する端末の見直し
補足	認証に関するイベントはログの量が多いため、管理者アカウントに関するイベントに絞ることで効率的な調査を行うことが可能になる 例として、Windows Server 2008 R2 や 2012 R2 では、以下のグループがドメイン管理者権限を有している[5]ため、優先的に調査を行うことをおすすめする Users¥Domain Adminis Users¥Enterprise Admins Users¥Schema Admins Builtin¥Backup Operators Builtin¥Account Operators Builtin¥Administrators

アカウントの悪用に気づきやすい環境を作ることも重要である。例えば、管理者アカウントを使用する端末を限定していれば、それ以外の端末上でアカウントが悪用された場合に比較的それに気づきやすい（図 12 左）。しかしながら、管理者アカウントを使用する端末を限定していないと、アカウントを悪用されても異常として判別しにくく、検知が遅れてしまう可能性が高い。また、管理者アカウントを使用した多数の端末上に管理者アカウントの認証情報が残るため、それを窃取される可能性も高まる（図 12 右）。



［図 12. 管理者アカウントと端末の関連］

管理者アカウントと管理者アカウントを使用する端末の組み合せを管理簿などで管理しておくと、調査や運用の見直しに有用である。

4.3.3. 認証回数の調査

アカウントが悪用された場合、パスワードクラックやマルウエアの定期的な活動などによって、平常時と比較して、認証回数に変化が見られることがある。

アカウントを使用している端末の調査	
調査対象	DC：ドメイン管理者アカウント サーバ：サーバ管理者アカウント DC、サーバの管理専用端末：管理専用端末のローカル管理者アカウント（可能であれば実施）
前提条件	・ 管理者アカウントを使用する端末を精査済みであること（前ページ参照） ・ サービスで使用しているアカウントは平常時においても大量の認証要求が発生することがあるため、事前にサービスアカウントについても精査を実施すること
確認事項	イベント ID 4624,4625,4768,4769,4776 の認証イベントついて、アカウント、認証要求端末ごとの認証回数の推移を、以下の観点で確認する。意図しない認証が確認された場合は、アカウントが侵害されている可能性がある ・ システム利用以外に繰り返し定常的に認証が行われていないか ・ 休日などアカウントが使用されないはずの期間に認証が行われていないか ・ 経時的に見て認証回数に急激な変化がないか ・ 認証失敗が多数発生していないか
ToDo	該当アカウント・端末について、以下を実施する ・ 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。意図せず使用されている場合は、アカウントが使用された端末を調査 ・ 認証失敗が多数発生している場合は、その原因調査
補足	・ 4.3.2 節と同様に、管理者アカウントに関するイベントだけを抽出することで調査が効率的になる ・ 運用で管理者アカウントを使用する場合は、アカウントと使用期間を管理簿などで管理しておくことで、効果的にログとの突き合わせを行うことが可能となる

5. Active Directory に対する攻撃の対策

本章では、AD に対する攻撃を抑止するための対策や、攻撃を検知した場合に被害を軽減するための対策について説明する。一つの対策だけに頼らず、複数の対策を組織の運用状況にあわせて実施することが効果的である。

表 5 に、さまざまな攻撃手法に対して効果が期待できる対策を示す。

［表 5 Active Directory に対する攻撃手法と対策］

			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

また、各対策の適用範囲（対策を実施する対象となるコンピュータ、アカウント）および対策が有効な OS のバージョンを表 6 に示す。

［表 6. 各対策の適用範囲］

		適用範囲				対策が利用できるバージョン
		DC	サーバ	DC、サーバの管理端末	その他の端末	
管理専用端末の設置 (5.1.1)				○		全バージョン
セグメント化	通信 (5.1.2)	○	○	○	○	全バージョン
	アカウント (5.1.3)	○	○	○	○	全バージョン
特権の最小化 (5.1.4)		○	○	○	○	全バージョン
セキュリティ更新プログラム適用 (5.1.5) ※2	KB3011780 (MS14-068)	○				Windows Server 2008、2008 R2、2012、2012 R2
	KB2871997 (資格保護)	○ ※1	○ ※1	○	○	Windows 7、8、8.1、Windows Server 2008 R2、2012、2012 R2
認証情報の保護 (5.1.6)	LSA Protection (5.1.6.1)	○	○	○	○ ※1	Windows 8.1、Windows Server 2012 R2 以降
	Protected Users (5.1.6.2)	○		○		Windows 8.1、Windows Server 2012 R2 以降
	Restricted Admin (5.1.6.3)	○	○	○		Windows 7、Windows Server 2008 R2 以降
	Credential Guard (5.1.6.4)		○	○	○ ※1	Windows 10 Enterprise、Windows Server 2016
適切なパスワード設定 (5.1.7)		○	○	○	○	全バージョン
krbtgt パスワード変更 (5.2.1)		○				全バージョン
ドメイン管理者アカウントパスワード変更 (5.2.2)		○				全バージョン
サービスアカウントのパスワード変更 (5.2.3)		○	○	○		全バージョン
管理者アカウントのパスワード変更 (5.2.4)			○	○		全バージョン

※1 可能であれば適用することが望ましい
※2 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

5.1. 予防策

本節では、AD に対する攻撃を予防するための対策（主にドメイン管理者権限やサーバの管理者権限の窃

取を抑止するための対策）を紹介する。各項には前提条件や実施すべき内容を表で記載しており、それぞれの項目は以下のとおりである。

適用対象：予防策を適用するために設定すべきコンピュータやアカウント
前提条件：予防策を実施するための前提条件
設定手順：予防策を実施するために必要な設定の手順

- 「・」で表記しているもの：各項目のいずれかを実施することで対策の効果が得られる
- 数字の連番で表記しているもの：設定の順序を表している

注意事項：実施にあたって注意すべき内容
補足：補足事項がある場合に記載

5.1.1. 管理専用端末の設置

DC やサーバの管理に使用する端末は、管理者アカウントの認証情報が保存されるため、管理者アカウントを狙った攻撃の対象になりやすい。これらの端末を管理専用端末とし、用途を DC やサーバの管理だけに限定する。さらに、インターネットへのアクセスやアプリケーションの実行を制限することで、マルウエア感染などのリスクが減り、高度サイバー攻撃による侵害の可能性を軽減できる。

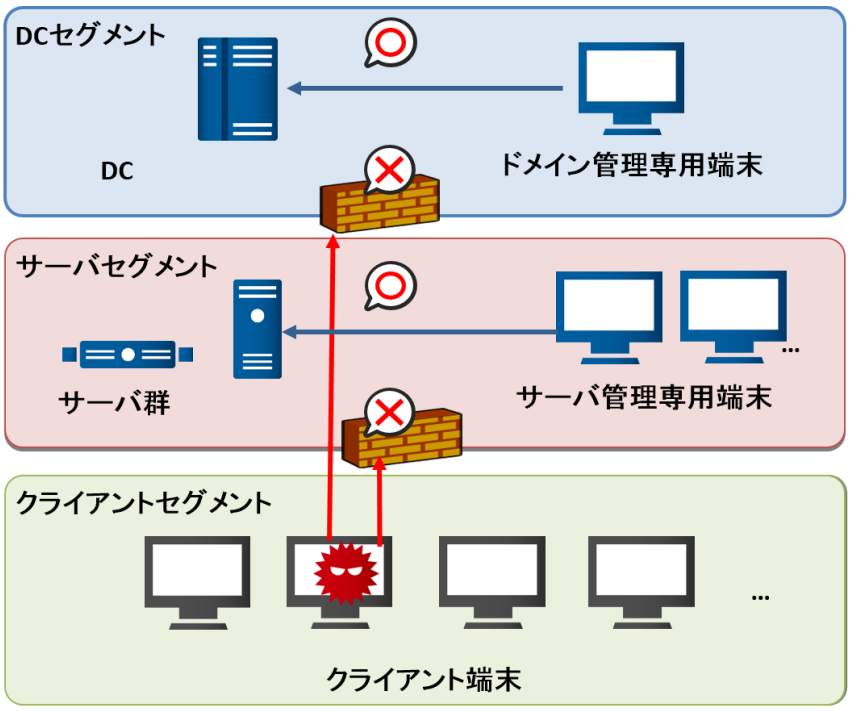
管理専用端末の設置	
適用対象	DC やサーバの管理に使用する端末 （ドメイン管理者アカウントやサーバの管理者アカウントを使用する端末）
前提条件	ファイアウォールやルータなどにより管理専用端末の通信先を制限できること または AppLocker[9] などによりプログラムの起動を制限できること
設定手順	・ ファイアウォールやルータを使用して、管理専用端末からのインターネット接続を必要最小限に制限する ・ AppLocker などを使用して、業務に不要なプログラムを起動できないように設定する
注意事項	・ 管理専用端末の OS や使用するソフトウエアの脆弱性に対処するため、セキュリティアップデートは必要である。セキュリティ更新プログラムの適用に限定したインターネット接続や、オフラインでの適用方法を検討すること ・ AppLocker は Windows Server 2008 R2 と Windows 7 以降の Windows OS で使用可能だが、一部のエディションによっては使用できないため、Microsoft 社の情報を参照し、使用できるエディションを確認すること[10]
補足	前提条件を満たすのが難しい場合は、運用ルールで制限することによって一定の効果が期待できる

5.1.2. 通信先セグメントの制限

用途に応じてコンピュータを別々のネットワークセグメントに配置し、ネットワークセグメント間で許可する通信を必要最小限にすることによって、コンピュータが侵害された場合に、そこから DC やサーバへの横断的侵害を抑止できる可能性が高まる。

以下は、Microsoft 社が推奨している[5]セグメント化の例である。

- DC セグメント：DC およびドメイン管理者権限を使用する端末（管理専用端末）だけを設置
- サーバセグメント：インターネットに公開しない重要なサーバ（組織内ファイルサーバなど）および各サーバの管理専用端末だけを設置
- クライアントセグメント：一般ユーザが使用する業務用端末を設置

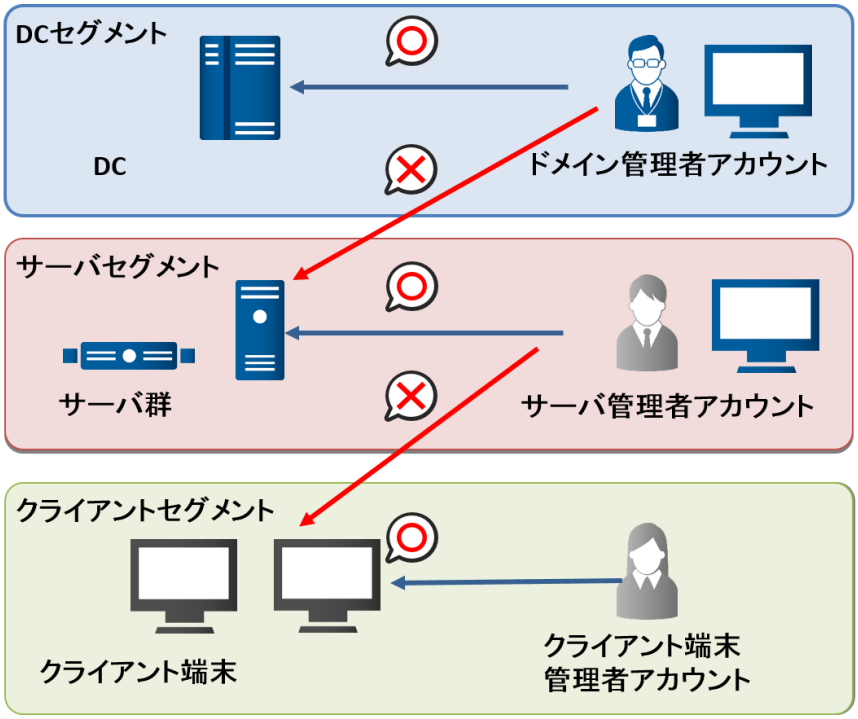


［図 13.セグメント化（通信の制限）］

通信先セグメントの制限	
適用対象	ドメインに参加している全てのコンピュータ
前提条件	ネットワークのセグメント化が可能で、アクセス制御を行えるルータやファイアウォールなどの機器や仕組みがあることが望ましいが、それが難しい場合は、パーソナルファイアウォール機能などで代替することも有効である
設定手順	1. ルータやファイアウォールなどを使用して、ネットワークセグメントを分離する 2. DC およびドメイン管理専用端末は DC セグメントに設置する 3. DC へのリモートアクセス（リモートデスクトップやファイル共有サービスなど）はドメイン管理専用端末からのみ許可する 4. クライアントセグメント、サーバセグメントの端末からは認証に必要な通信（Kerberos, SMB など[26]）のみを許可するなどのアクセス制御を行う 5. DC 以外の他の重要なサーバおよび管理専用端末はサーバセグメントに設置し、同様にアクセス制御を行う
注意事項	アクセス制御の実施にあたって、業務に必要な通信を遮断しないよう、十分に検討と検証を実施すること

5.1.3. アカウント使用を同じセグメント内に制限

認証情報が窃取された場合の影響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、対象セグメント内のコンピュータおよび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することが望ましい。前節に記載のとおり、クライアントセグメントなどのセキュリティレベルの低いセグメントで使用しているアカウントを使って、DC やサーバなどのセキュリティレベルの高いセグメントのコンピュータにログインすることは避けるべきであるが、その反対も避けるべきである。なぜなら、ドメイン管理者といった高い権限を持つアカウントを、マルウエア感染のリスクが高いクライアントセグメントに設置された端末で使用すると、仮に、その端末が感染して侵害されていた場合に、ドメイン管理者アカウントの認証情報を窃取される可能性がある。管理者アカウントによるセグメントをまたいだログインを行わないようにすることで、セグメントごとのセキュリティが維持され、セキュリティレベルの低いセグメントを陥れた攻撃者に DC やサーバの管理者アカウントの認証情報を窃取される可能性を軽減することができる。



［図 14. セグメント化（アカウント使用の制限）］

アカウント使用を同じセグメント内に制限	
適用対象	ドメインに参加している全てのコンピュータ
前提条件	特になし
設定手順	グループポリシーなどを使用して、運用で使用するユーザ以外からのリモートアクセスを制限する。例として、グループポリシーオブジェクトの「ネットワーク経由のアクセスを拒否」[27] や「リモートデスクトップサービスを使ったログオンを拒否」[28] に禁止したいアカウントを設定することにより、ネットワーク経由のアクセスを制限できる
注意事項	・業務に必要なアカウントのログインを制限しないよう、十分に検討し検証する ・グループポリシーを使用する場合は、以下の点に注意する - ネットワーク経由のアクセスを拒否：PsExec *9や管理共有*10などのアクセスを制限できるが、リモートデスクトップによるアクセスは制限できない - リモートデスクトップサービスを使ったログオンを拒否：リモートデスクトップによるアクセスを制限できるが、PsExec や管理共有などによるアクセスは制限できない
補足	本対策のみでも有効であるが、「5.1.2 通信先セグメントの制限」と組み合わせるとより効果的である。また、システム上の制限が難しい場合は、運用ルールを設け遵守するだけでも一定の効果が期待できる

*9 リモートコンピュータでコマンドを実行するためのツール
https://technet.microsoft.com/ja-jp/sysinternals/pxexec.aspx
*10 Windows に自動的に作成される管理用の共有リソース。"C$"などの管理共有を用いることで、リモートホストの C ドライブ配下をマウントすることなどが可能となる。

5.1.4. 付与する特権の最小化

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付与するアカウントを最小限にとどめる。業務遂行のためにアカウントに付与する必要がある特権を洗い出し、最小限の特権だけを与えることで、アカウントを乗っ取られて特権を悪用された時の影響を軽減できる。DC やサーバの管理端末について、認証情報窃取を防ぐために誰に対してもローカル管理者権限を与えないことも有効である。利用者が使用するアカウントに加え、サービスを実行するためのアカウントについても精査する。

付与する特権の最小化	
適用対象	全てのアカウント
前提条件	特になし
設定手順	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、アカウントが所属するグループやアカウントに割り当てる権限を変更する。Windows では用途に応じて複数の特権（SeSecurityPrivilege、SeBatchLogonRight など）[8]が定義されているため、必要最小限の権限を割り当てることが望ましい
注意事項	業務に必要な権限をはく奪しないよう、十分に検討と検証を行ってから実施する

5.1.5. セキュリティ更新プログラム適用

脆弱性悪用を抑止し、また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する。特に、影響度が大きい脆弱性の更新プログラムやセキュリティ機能向上に関する更新プログラムについては、優先して適用するのが望ましい。以下は優先的に適用すべき更新プログラムの例である。

- DC に対しては、MS14-068（Kerberos KDC の脆弱性）の更新プログラム（KB3011780）を適用することで、本脆弱性を悪用した権限昇格を抑止することが可能である[4]。特に、AD に対する攻撃を確認している場合は、早急に適用することを推奨する

- KB2871997[11]は、認証情報窃取の抑止に有効なセキュリティ機能が提供されているため、なるべく全ての端末に適用するのが望ましい

セキュリティ更新プログラム適用	
適用対象	・優先して適用すべきセキュリティ更新プログラムと適用対象コンピュータ - KB3011780：Windows Server 2008, 2008 R2, 2012, 2012 R2 の DC - KB2871997：Windows 7, 8, 8.1 Windows Server 2008 R2, 2012, 2012 R2 のコンピュータ ・その他のセキュリティ更新プログラムについては、各更新プログラムのアドバイザリを参照し、適宜適用すること
前提条件	各セキュリティ更新プログラムのアドバイザリを参照
設定手順	Microsoft Update や Windows Update、WSUS（Windows Server Update Services）[12]などを使用してセキュリティ更新プログラムを適用する。インターネットや社内ネットワークから隔離された環境においては、オフラインでの更新プログラムファイルの適用を検討する
注意事項	・ セキュリティ更新プログラムによっては、システムの挙動を変える場合や、適用にあたっての前提条件や適用後の再起動などが必要となる場合もあるため、アドバイザリを確認の上、十分に検討し検証してから実施する ・ 本項で紹介した更新プログラム以外にも、影響度が大きい脆弱性の更新プログラムが公開される可能性があるため、Microsoft 社からの情報に注意する

5.1.6. 認証情報の保護

5.1.6.1. LSA Protection

LSA（Local Security Authority）*11 Protection は、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機能である。有効化すると、攻撃ツールがメモリにアクセスし、認証情報を窃取したり不正なチケットを展開したりすることを抑止できる[13]。特に、DC や重要なサーバの管理専用端末に対して優先的に適用することで、それらの管理者アカウントの認証情報窃取を抑止できる。

LSA Protection	
適用対象	DC、サーバ、管理専用端末：優先的に適用 クライアント端末：可能であれば適用
前提条件	Windows8.1、Windows Server 2012 R2 以降であること
設定手順	本機能を有効にするために、レジストリを変更する必要がある。詳細は「参考情報[13]」を参照
注意事項	標準設定では有効化されていないため、明示的に有効にする必要がある。 また、本機能の有効化によって Microsoft によって署名されていないプラグインやドライバーは使用できなくなる

5.1.6.2. Protected Users

Protected Users [14]という名前のセキュリティグループに所属するアカウントが使用する認証方式は Kerberos 認証に限定される。NTLM 認証を使用しないため、NTLM ハッシュがメモリに保存されず、Pass-the-Hash による攻撃を防ぐことができる。特に DC やサーバの管理者アカウントを Protected Users に所属させることで、管理者アカウントの認証情報窃取を抑止できる。

Protected Users	
適用対象	ドメインユーザ
前提条件	Windows 8.1、Windows Server 2012 R2 以降であること
設定手順	Active Direcroty のユーザとグループの管理機能を使用して、アカウントを Protected Users グループに所属させる。詳細は参考情報[14]を参照のこと
注意事項	Protected Users に所属するアカウントは NTLM 認証を使用できなくなる。AD 環境では Kerberos 認証が主に使用されるが、操作やサービスによっては NTLM 認証も使用される（プリンタへのアクセスや IP アドレスによる共有フォルダへのアクセスなど）。NTLM 認証を使用する可能性がないか十分に検討、検証を行う

*11 ユーザの資格情報の管理やパスワードハッシュの保持などを行う Windows のセキュリティに関する機能。

5.1.6.3. Restricted Admin

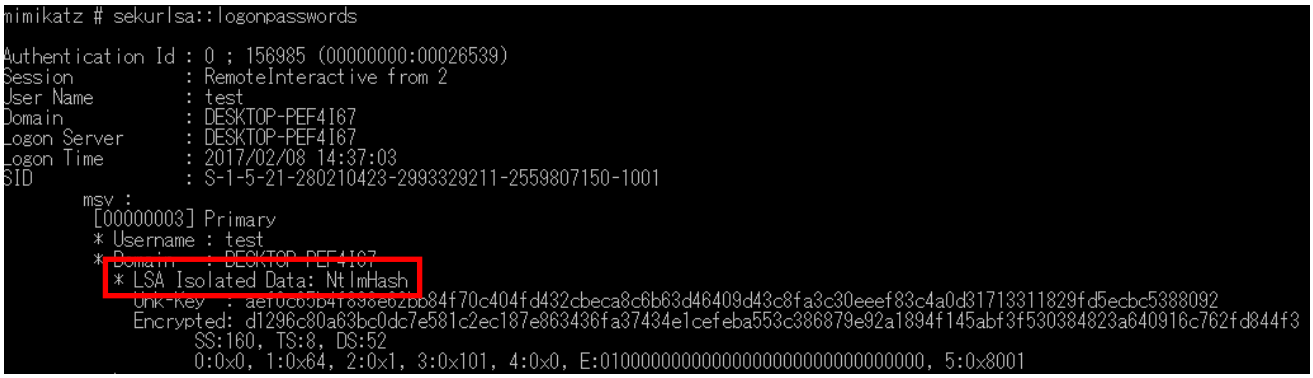
Restricted Admin[15]は、リモートデスクトップの接続先コンピュータに認証情報を残さない機能であり、Restricted Admin を使用してリモートデスクトップを行うことで、接続先コンピュータのメモリから認証情報が窃取されることを抑止できる[15]。特に、メンテナンスなどのために、侵害されたコンピュータに対して特権アカウントによるリモートデスクトップ接続する必要がある場合に、Restricted Admin を使用すれば、接続先のコンピュータから特権アカウントの認証情報が窃取される可能性を軽減できる。

Restricted Admin	
適用対象	DC、サーバ（リモートデスクトップの接続先） DC やサーバの管理専用端末（リモートデスクトップの接続元）
前提条件	接続元、接続先のコンピュータが、Windows 7、Windows 2008 R2 以降であり、参考情報[15]に記載されているセキュリティ更新プログラムが適用されていること
設定手順	1. 接続元、接続先のコンピュータで、レジストリの変更を行う 2. 接続先のコンピュータでリモートデスクトップ接続を行うアカウントをローカルの Administrators グループに所属させる 3. 接続元のコンピュータで “/restrictedadmin” オプションをつけてリモートデスクトップ接続を実行する 詳細は参考情報[15]を参照のこと
注意事項	OS のバージョンやセキュリティ更新プログラムの適用状況によっては、本機能が無効になっている可能性があり、その場合は明示的に有効にする必要がある。詳細は参考情報[15]を参照のこと

5.1.6.4. Credential Guard

Credential Guard を有効にすると、LSA の認証情報がホスト OS から分離された仮想環境上で保護される[16][17]。本機能により、攻撃ツールが不正にメモリにアクセスし、認証情報を窃取したり、不正なチケットを展開したりすることを抑止できる（図 15）。特に、重要なサーバの管理専用端末に対して優先的に適用することを推奨する。それにより管理者アカウントの認証情報窃取を抑止できる。

Credential Guard	
適用対象	サーバ、管理専用端末：優先的に適用 クライアント端末：可能であれば適用
前提条件	・Windows 10 Enterprise、Windows Server 2016 である ・「参考情報[16]」に記載しているハードウエアの要件を満たしている
設定手順	・　グループポリシー管理コンソールを使用して、「仮想化ベースのセキュリティを有効化する」から有効化する ・　仮想化に関する設定やレジストリの値を変更して有効化する 詳細は「参考情報[16]」を参照
注意事項	Credential Guard によって保護されるのはドメインアカウントのみであり、ローカルアカウントやマイクロソフトアカウントは保護対象外である。詳細は「参考情報[16]」を参照



［図 15. Credential Guard によるメモリ保護］

5.1.7. 適切なパスワードの設定

短いパスワードや単純なパスワードを設定している場合、総当たり攻撃などによって攻撃者にパスワードを割り出される可能性が高い。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、複数のアカウントに共通のパスワードを設定することを避けることが望ましい。

適切なパスワードの設定	
適用対象	全てのアカウント 特に、以下のアカウントについては横断的侵害の可能性を軽減する観点から、優先的に対応するのが望ましい ・ドメイン管理者アカウント ・各サーバの管理者アカウント ・各端末のローカル管理者アカウント ・管理者権限でサービスを実行するアカウント
前提条件	特になし
設定手順	グループポリシーやローカルセキュリティポリシーでパスワードのポリシー（満たすべき長さや複雑性の要件など）を設定する
注意事項	特になし

なお、ローカル管理者アカウントについては、Microsoft 社が提供しているツール Local Administrator Password Solution （LAPS）[18]を AD に導入することで、各コンピュータの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し、ランダムなパスワードに変更したり定期的に更新したりすることができる。LAPS の詳細については「Appendix G) LAPS によるローカル管理者のパスワード変更」を参照のこと。

5.2. 攻撃を検知した場合の緊急対処

本節では、AD に対する攻撃を検知した際に、その後の被害を軽減するために実施すべき緊急対処について説明する。

AD に対する攻撃を受けているかどうかを確認する方法や、どの端末やアカウントが侵害されたかを確認する方法については「4. Active Directory のイベントログを活用した横断的侵害の検知」を参照のこと。

なお、本節で紹介する対策はあくまで緊急対処であり、さらなる攻撃のための足掛かりを根絶するためには AD の再構築などの根本的な対処が必要になるケースもある。根本的な対処を行うにあたっては、セキュリティベンダなどの専門組織に協力を依頼することも検討してほしい。
各項には前提条件や実施すべき内容を表で記載しており、それぞれの項目は以下のとおりである。

適用対象：対処を適用する対象となるアカウント

前提条件：対処を実施するための前提条件
設定手順：対処を実施するために必要な設定の手順
注意事項：実施にあたって注意すべき内容
補足：補足事項がある場合に記載

ドメイン管理者権限の悪用が確認されている場合の対処のサマリを次に示す。

ドメイン管理者権限が侵害されている場合の緊急対処	
実施すべき対処	目的
5.2.1 krbtgt アカウントのパスワード変更	Golden Ticket の無効化
5.2.2 ドメイン管理者アカウントのパスワード変更	新たな Golden Ticket 作成の抑止
5.2.3 サービスを実行しているアカウントのパスワード変更	Silver Ticket の無効化
5.2.4 管理者アカウントのパスワード変更	新たな Silver Ticket 作成の抑止
5.1.5 セキュリティ更新プログラム適用	MS14-068（Kerberos KDC の脆弱性）のセキュリティ更新プログラム（KB3011780）適用

特定のサーバに対する攻撃を確認している場合の対処のサマリを次に示す。攻撃されたサーバの特定が難しい場合は、ファイルサーバなどの重要なサーバに対して優先的に対策を実施することをご検討いただきたい。

サーバの管理者権限が侵害されている場合の緊急対処	
実施すべき対処	目的
5.2.3 サービスを実行しているアカウントのパスワード変更	Silver Ticket の無効化
5.2.4 管理者アカウントのパスワード変更	新たな Silver Ticket 作成の抑止

5.2.1. krbtgt アカウントのパスワード変更

ドメイン管理者アカウントが侵害された場合には、Golden Ticket が作成される可能性が高い。既に作成された Golden Ticket を無効化し、新たな Golden Ticket の作成を抑止するために、krbtgt アカウントのパスワードを連続して 2 回変更する必要がある。

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 アカウント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。これに起因し、イベント ID 4769 にエラーコード「0x1f」*12 が大量に記録される可能性がある（正規ユーザを含め、該当ユーザによる認証が発生したタイミングでクライアント端末がキャッシュしている無効な TGT を DC に送信するため）。krbtgt のパスワードを 2 回変更後、Golden Ticket が使用された場合は認証エラーとなり、同エラーコードが記録されるが、正規ユーザによる認証エラーと Golden Ticket の使用による認証エラーでは、イベントの内容に違いがないので、判別することが難しい（何れの場合も、ソース IP アドレスは記録されるが、アカウント名、ドメイン名は記録されない）
補足事項	「Active Directory ユーザーとコンピュータ」で krbtgt アカウントを表示するためには、「表示」メニューの「拡張機能」を選択する必要がある

*12 RFC 1510 における KRB_AP_ERR_BAD_INTEGRITY （暗号時と復号時で異なる鍵が使用された）のエラーコードを示す。
https://technet.microsoft.com/en-us/library/bb463166.aspx

5.2.2. ドメイン管理者アカウントのパスワード変更

ドメイン管理者権限悪用による被害を軽減するために、ドメイン管理者アカウントのパスワードを変更する。

ドメイン管理者アカウントのパスワード変更	
適用対象	ドメイン管理者アカウント
前提条件	特になし
設定手順	AD のユーザとコンピュータの管理画面やアカウントを使用する端末のパスワード変更画面でパスワードを変更する
注意事項	十分な長さと複雑性を持ったパスワードを設定する

5.2.3. サービスを実行しているアカウントのパスワード変更

管理者アカウントが侵害されているコンピュータでは、そのコンピュータ上で動作するサービスに対する Silver Ticket が作成される可能性がある。Silver Ticket を無効化するために、対象サービスを実行しているアカウントのパスワードを変更する必要がある。

サービスを実行しているアカウントのパスワード変更	
適用対象	侵害されたコンピュータ上のサービスアカウント CIFS サービスや HOST サービスなどのサービスに関してはコンピュータアカウントがそれに該当するが、それ以外のサービスに関してはサービスごとに異なる （侵害されたコンピュータの特定が難しい場合は、DC、重要なサーバ、それらの管理専用端末について優先的に実施する）
前提条件	特になし
設定手順	AD のユーザとコンピュータの管理画面やアカウントを使用する端末上で、該当アカウントのパスワードを変更する コンピュータアカウントについては、対象のコンピュータ上で、管理者権限でコマンドプロンプトを起動し、以下のように NETDOM コマンド[19]を実行し、コンピュータアカウントのパスワードを 2 回変更する NETDOM RESETPWD /S:{DC の FQDN} /UD:{ドメイン名}¥{ドメインユーザのアカウント名} /PD:{ドメインユーザのパスワード}
注意事項	・ コンピュータアカウントのパスワードは必ず 2 回変更する必要がある。また、新たな Silver Ticket の作成を防止するために、パスワード変更は間隔を空けずに実施する ・ 新たな Silver Ticket の作成を防止するために、「5.2.4. 管理者アカウントのパスワード変更」を参照し、管理者アカウントのパスワードも合わせて実施すること ・ パスワード変更によって正規ユーザが使用している ST も無効化されて再発行が必要となるため、パスワード変更後にサービスを実行しているコンピュータへの認証要求が増加する可能性がある
補足	CIFS サービス、HOST サービスの Silver Ticket に関しては、コンピュータアカウントのパスワードを 2 回変更することで無効化できることを JPCERT/CC で確認しているが、その他のサービスについては未検証である

5.2.4. 管理者アカウントのパスワード変更

管理者アカウントが侵害されているコンピュータでは、メモリ上などからサービスを実行しているアカウントのパスワードハッシュを窃取し、Silver Ticket を作成される可能性があるため、当該コンピュータの管理者アカウントのパスワード変更を行う事を推奨する。

管理者アカウントのパスワード変更	
適用対象	侵害されたコンピュータの管理者アカウント（ローカル管理者アカウントを含む）（被害範囲の特定が難しい場合は、DC、重要なサーバ、それらの管理端末で使用しているアカウントについて優先的に実施する）
前提条件	特になし
設定手順	AD の「ユーザとコンピュータの管理画面」やアカウントを使用する端末上で、管理者アカウントのパスワードを変更する
注意事項	十分な長さと複雑性を持ったパスワードを設定する

対処に関する補足事項

Golden Ticket / Silver Ticket を無効にするためには、それらのチケットに対して署名・暗号化をしたアカウントのパスワードを変更する必要がある。Golden Ticket を含む TGT は krbtgt アカウントの NTLM ハッシュで署名されているので、Golden Ticket を無効化するためには krbtgt アカウントのパスワードを変更する。Silver Ticket を含むサービスチケットは対象サービスを実行しているアカウントの NTLM ハッシュで署名・暗号化されているので、Silver Ticket を無効にするためには、対象サービスを実行しているアカウントのパスワードを変更する。なお、krbtgt アカウントおよびコンピュータアカウントのパスワードは 2 世代 （現行と 1 つ前のパスワード）保持されており、現行のパスワードで認証に失敗した場合、1 つ前のパスワードで認証を行うため、パスワード変更は 2 回連続で実施する必要がある。

6. 最後に

AD は、組織ネットワーク全体の情報リソースの管理を一元的に行うことができるなど、組織ネットワークの構築と運用にとって利便性が高い反面、高度サイバー攻撃の攻撃を受けた場合に、いわばセキュリティ上のアキレス腱となりやすい。特に、攻撃者にドメイン管理者権限やサーバの管理者権限を窃取されれば、攻撃による傷口が一挙に拡大することになるため、これらの特権アカウントを守ることが非常に重要である。

管理専用端末の設置や特権の最小化など、運用を見直した上で DC やサーバのイベントログを定期的に確認することで、横断的侵害に早期に気づくことができ、被害範囲を限定することができる。対策においては、DC やサーバに対するメンテナンスが必要となるため、運用の都合で速やかな対策が難しいケースも考えられる。そのため、本文書では、状況に応じた対策の選定や、また優先度についても言及した。運用に合ったスケジュールを検討し、優先度を付けて必要な対策を適用してほしい。

本文書によって、ログの保管・確認や適切な AD の運用の重要性をご認識いただき、高度サイバー攻撃の早期発見と対策に活用していただければ幸いである。

Appendix A) ログの保管・確認にあたって

本章では、高度サイバー攻撃の備えとしてのログの保管・確認にあたって検討が必要な事項や、保管すべき主要なログの例について記載する。

ログの適切な保管・定期的な確認を実施していない場合、以下のような問題が発生する可能性がある。

- 攻撃者の活動を見逃し、侵入に気づくことができない
- 攻撃者の侵入経路が特定できず、侵入経路に対して対策を行うことができない
- 侵害された端末・ユーザアカウントを特定することができない
- アクセスされた情報資産を特定することができない
- 外部に持ち出された情報を特定することができない

適切なログの保管を行うために、以下を検討する必要がある。

- 組織のネットワーク構成を把握し、外部ネットワーク（インターネット）との通信を行う接続点（出入り口）を確認する。プロキシサーバを設置して、外部との通信は全てプロキシサーバを経由させることで、通信ログを集約して確認できる
- 組織内ネットワークを必要に応じてセグメント化し、セグメント間で発生する通信（ユーザセグメントとサーバセグメントの通信、内部セグメントと DMZ の通信など） を必要に応じて保管する。
- 認証を必要とするシステムについて、成功、失敗の認証ログを保管する
- 守るべき情報資産を特定し、それらに対するアクセスログを保管する
- 攻撃活動の痕跡消去を目的として攻撃者がログの消去などを行う場合があるため、収集したログを安全に（消去、改ざんされない状態で）保管する方法（syslog サーバ、ログ管理ソフトウエア、SIEM の活用など）を検討する

攻撃の段階と攻撃の痕跡が残る主要なログの対応を表 7 にまとめた。攻撃活動の調査においてこれらのログを活用するためには、ログを一定期間保存しておく必要がある。高度サイバー攻撃の調査においては、JPCERT/CC としては 1 年以上保存することを推奨している。全てのログをオンライン保管（OS に接続されているハードディスクなどすぐに参照できる形式で保管する方法）しておく必要はなく、オフライン保管（CD などの外部媒体に保管する方法）を併用することで、ハードディスクなどの節約、コストダウンなどが可能となる。ログの保管期間の考え方や各ログの確認ポイントについては参考資料[6]を参照のこと。

［表 7. 攻撃の段階と痕跡が残るログの対応］

攻撃段階		ログで検知可能な攻撃内容	ログ取得対象機器
1	準備	-	-
		-	-
2	侵入	攻撃者によるマルウエア添付メールの送信 （不審な送信元や、実行ファイル形式が添付されたメール）	メールサーバ
		攻撃者によるマルウエア設置サイトへの誘導メールの送信と誘導	メールサーバ プロキシサーバ DNS
		プロキシサーバを介さない外部の C2 サーバへの通信 （C2 サーバのドメインや感染端末などの情報）	ファイアウォール DNS
		HTTP, HTTPS 等のプロトコルによる外部の C2 サーバへの通信 （C2 サーバのドメインや感染端末などの情報）	プロキシサーバ DNS
3	横断的侵害	プロキシサーバを介さない外部の C2 サーバへの通信 （C2 サーバのドメインや感染端末などの情報）	ファイアウォール DNS
		HTTP, HTTPS 等のプロトコルによる外部の C2 サーバへの通信 （C2 サーバのドメインや感染端末などの情報）	プロキシサーバ DNS
		セグメント間を超えた感染活動 （脆弱な PC や内部サーバの探索など）	ファイアウォール （組織内ネットワークの内部に設置している場合）
		ファイルサーバなどへのアクセスや権限の窃取	認証サーバ (AD) ファイアウォール
4	活動	プロキシサーバを介さない外部の C2 サーバへの通信 （C2 サーバのドメインや感染端末などの情報）	ファイアウォール DNS
		HTTP, HTTPS 等のプロトコルによる外部の C2 サーバへの通信 （C2 サーバのドメインや感染端末などの情報）	プロキシサーバ DNS
		機密情報持ち出し (メールサーバ経由など)	メールサーバ DNS

Appendix B) Active Directory で使用される認証方式

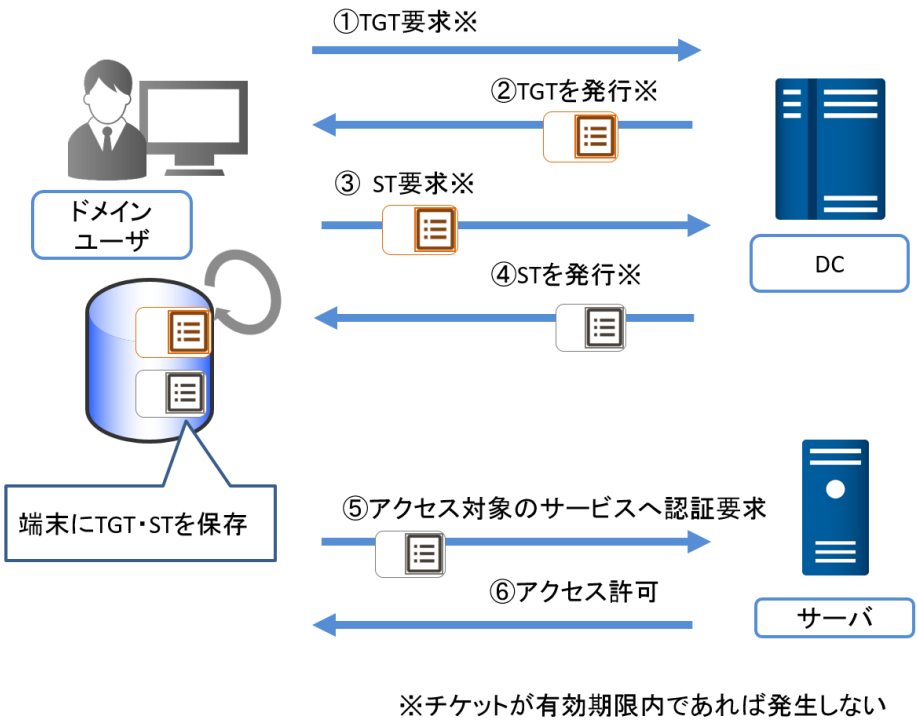
AD 環境で使用される主要な認証方式について記述する。

1. Kerberos 認証

AD 環境で主に用いられる認証方式であり、Ticket-Granting Tickets（TGT）、Service Ticket（ST）と呼ばれる認証チケットを使用する。

- TGT : ST を得るために必要なチケットである。各ユーザはドメインのサービスにアクセスするために、まず DC に対して認証要求を行い、TGT を取得する必要がある。TGT は krbtgt アカウントの認証情報を用いて署名・暗号化される。TGT は有効期限（デフォルト 10 時間）を持っており、有効期限内はクライアント端末に保存され、再利用される。

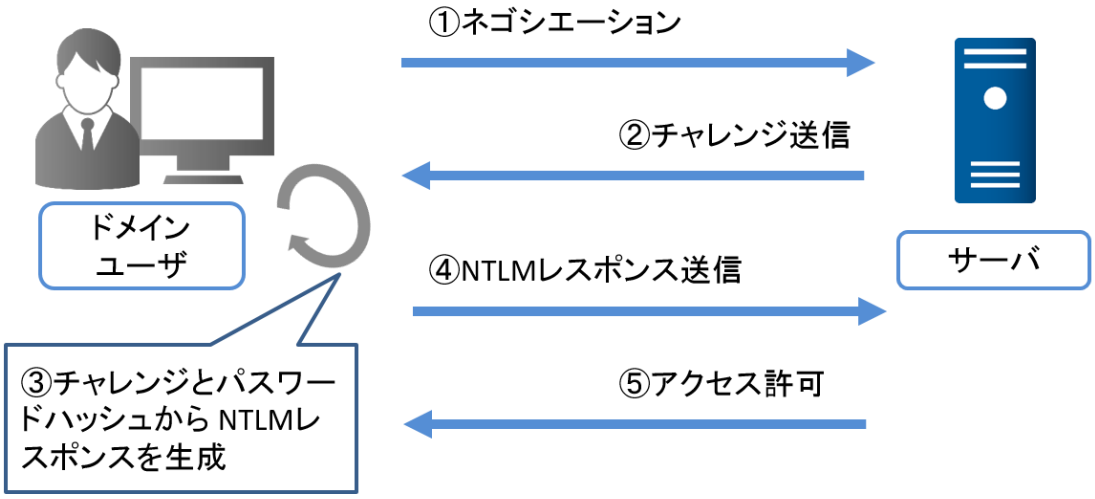
- ST : AD 環境の各サービス（ファイル共有サービスなど）にアクセスするために必要なチケットであり、各ユーザは DC から発行された TGT を元に DC にリクエストを行って ST の発行を要求する。取得した ST を元にサービスを実行しているサーバにリクエストを行う。ST は各サービスを実行しているアカウントの NTLM ハッシュで暗号化される。TGT と同様に有効期限（デフォルト 10 時間）を持っており、有効期限内はクライアント端末に保存され、再利用される。



［図 16. Kerberos 認証の概要］

2. NTLM 認証

チャレンジレスポンスを使用する認証方法であり、主にスタンドアロン（ワークグループ）の Windows システムで使用される認証方式である。AD 環境においては基本的に Kerberos 認証が用いられるが、IP アドレスベースで認証を行った場合などには NTLM 認証が使用されることがある。 NTLM 認証では、パスワードハッシュを使用して認証を行う。



［図 17. NTLM 認証の概要］

Appendix C) メモリに保存される認証情報

以下は、Windows 8.1、Windows Server 2012 R2 の前後のバージョンにおいて端末のメモリ上に保存される認証情報について、Microsoft 社が公開している情報[5] を日本語化したものである（対象は Microsoft 社がサポートしているバージョンのみ）。

［表 8. Windows のメモリに保存される認証情報］

		kerberos TGT	ハッシュ		パスワード（平文）				
			LM	NTLM	認証方式				
					Tspkg	Wdigest	Kerberos	LiveSSP	Third Party SSP
Windows 8.1	Microsoftアカウント	○	×	×	×	×	○	×	× *1
Windows Server 2012 R2	ローカルアカウント	○	×*2	×	×*2	×*3	×*3	○	× *1
よりも前のデフォルト	ドメインアカウント	×	×*2	×	×*2	×*3	×*3	○	× *1
Windows 8.1	Microsoftアカウント	○	○	×	○	○	○	×	× *1
Windows Server 2012 R2	ローカルアカウント	○	○	×	○	○	×	○	× *1
以降のデフォルト	ドメインアカウント	×	○	×	○	○	○	○	× *1
Windows 8.1	Protected Users	×	○	○	○	○	○	○	× *1
Windows Server 2012 R2	Restricted Admin *4	○	○	○	○	○	○	○	○

○：メモリに認証情報が保存されない
×：メモリに認証情報が保存される
*1：サードパーティー製品をインストールした場合
*2：KB2871997 の適用によりメモリに認証情報が保存されない
*3：KB2871997 の適用によりメモリに認証情報が保存されないが、レジストリ設定によっては保存されることがある
*4：リモートデスクトップ接続先のメモリの情報

「*3」については、KB2871997[20] の適用によりメモリに認証情報が保存されなくなるが、レジストリ設定によっては保存されることがある。アドバイザリを参照の上、「WDigest の設定」に記載しているレジストリ設定をあわせて行う必要がある。

Windows 8.1 / Windows Server 2012 R2 より前のバージョンの Windows では、容易に復元が可能な LM ハッシュや平文パスワードがメモリ上に保存される。また、Wdigest などの一部の認証機能を有効にしている場合や Kerberos 事前認証*13に失敗した場合に平文パスワードが保存されるなどの制限事項がある。

*13 Kerberos 認証において、リプレイ攻撃を防止するために、認証チケットを使用した認証を行う前にユーザのパスワードハッシュで暗号化したタイムスタンプの情報を使って、認証を行う仕組みであり、Windows ではデフォルトで有効になっている。
https://msdn.microsoft.com/ja-jp/library/bb742516.aspx

Appendix D) イベントログを保存するための設定

以下の手順により、イベントログの最大ログサイズとアーカイブ（ローテーション）の設定を確認、変更することが可能である。

- イベントビューアーから「Windows ログ」「セキュリティ」を選択し、右クリックでプロパティを表示
- 「最大ログ サイズ （KB）」でイベントログファイルの最大サイズの値を変更する
- ログをアーカイブするためには、「イベントを上書きしないでログをアーカイブする」にチェックを入れる

  ※ 本項目を有効にすることで、最大ログサイズを超過すると
  「Archive-System-YYYY-MM-DD-HH-MM-SS-NNN.evt」という名前でアーカイブされる

詳細な手順は Microsoft 社の情報[21][22]を参照のこと。

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

4 章で紹介している調査が必要なイベントログの例は以下のとおりである。

［表 9. 調査に必要なイベントログの例］

イベント ID	説明
4698	スケジュールされたタスクの作成
1102	イベントログの消去
4624	ログインの成功
4625	ログインの失敗
4768	Kerberos 認証 （TGT 要求）
4769	Kerberos 認証 （ST 要求）
4776	NTLM 認証
4672	特権の割り当て

上記のイベントログが記録されるためには、「ローカルセキュリティポリシー」->「監査ポリシーの詳細な構成」にて、表 10 に示す項目について「成功」および「失敗」の監査を有効にする必要がある。表中に赤文字で記載しているものは、デフォルト設定から変更が必要な設定値である。ただし、監査の設定をデフォルトから変更した場合、明示的に監査を行う様に設定した項目のみ監査が有効になり、それ以外は無効（監査しない）になるため、以下の手順を実施すること。

- 変更前に、現状の監査ポリシー設定を確認する。以下のコマンドを管理者ユーザで実行することにより、監査ポリシーの一覧を取得できる[23]。
  auditpol /get /category:*
- 上記で監査が有効になっていることを確認した項目について、明示的に有効にする。

［表 10. イベントログの出力設定（Windows Server 2008 R2、Windows Server 2012 R2 の場合）］

カテゴリ	サブカテゴリ	既定値	設定値（*1）
アカウント ログオン	資格情報の確認の監査	成功	成功 および失敗
	Kerberos 認証サービスの監査	成功	成功 および失敗
	Kerberos サービスチケット操作の監査	成功	成功 および失敗
ログオン / ログオフ	ログオンの監査	成功 および失敗	成功 および失敗
	特殊なログオンの監査	成功	成功 および失敗
オブジェクト アクセス	その他のオブジェクトアクセス イベントの監査 （*2）	監査なし	成功 および失敗

*1：赤文字は追加で有効にする監査ポリシーの設定

*2：タスクに関連するイベントを記録するために必要

詳細な手順は Microsoft 社の情報[24]を参照のこと。

Appendix F) イベントログをエクスポートする方法

以下の方法で、指定した期間のイベントログを CSV などの形式でエクスポートすることができる。

1. 「イベントビューアー」->「Windows ログ」->「セキュリティ」を選択
2. 右クリックのメニューから「現在のログをフィルター」を選択
   「現在のログをフィルター」のダイアログで、「ログの日付」を選択し、採取したいログの期間を指定後、「OK」ボタンを押下し、フィルターを適用
3. 「セキュリティ」->「フィルターされたログ ファイルの名前を付けて保存」を選択
   「名前を付けて保存」ダイアログの「ファイル名」にファイル名を入力
   「ファイルの種類」から保存したい形式を選択し、「保存」ボタンを押下
   ※データ量によっては保存に時間がかかる場合がある

Appendix G) LAPS によるローカル管理者のパスワード管理

Microsoft 社が提供している無償のツール Local Administrator Password Solution（LAPS）[29]を使うことで、グループポリシーを使用して、ドメインに参加しているコンピュータのローカル管理者アカウントに対して自動でランダムなパスワードを設定し、定期的に更新することができる。

適切なパスワードの設定	
前提条件	「参考情報[18]」に記載している要件（Requirements）を満たしている
設定手順	1. 管理対象のコンピュータ、管理する側のコンピュータに LAPS をインストールする 2. LAPS に付属しているシェルを用いて、AD のスキーマを拡張する 3. LAPS のグループポリシーテンプレートを元にグループポリシーを作成し、パスワードのポリシー （満たすべきパスワードの長さや複雑性の要件など） を設定する
注意事項	AD のスキーマ拡張 （コンピュータアカウントの属性の拡張）が必要 管理が可能なアカウントは、各端末につき 1 つの管理者アカウントのみに限られる

Appendix H) Active Directory に対する攻撃の検証結果

組織内ネットワークへの侵入に成功した攻撃者は、ドメイン管理者アカウントやサービスの Golden Ticket / Silver Ticket を作成することで、恒久的なアクセス権限を得ることができる。このような Golden Ticket / Silver Ticket を作成するツールは、インターネットに公開されており、検証の結果、DC やファイルサーバに対してドメインユーザが管理者権限で不正にアクセスすることが可能になることを確認した。

1. Golden Ticket を使用した攻撃の検証

【検証内容】
攻撃者がドメイン管理者権限を窃取後、ドメイン管理者アカウントに対する Golden Ticket を作成するシナリオを想定し、検証を実施。作成した Golden Ticket をドメイン管理者権限を持たないアカウントで使用し、情報窃取が可能であるかを確認した。ドメイン管理者権限を窃取する手法として、AD の脆弱性（MS14-068）を悪用する手法を使用した。また、Golden Ticket を無効化する手順についても検証を実施した。

［表 11. 検証環境］

種別 （ ）内はホスト名	OS	運用で使用するアカウント	権限	前提条件
DC （winserver2008）	Windows Server 2008 R2	Administrator	・ドメイン管理者	AD の脆弱性（MS14-068）に対して未対処
クライアント端末 1 （client01）	Windows 7 64bit	client01	・ドメインユーザ ・クライアント端末 1 のローカル管理者	攻撃者によって侵入されている
クライアント端末 2 （client02）	Windows 7 64bit	client02	・ドメインユーザ ・クライアント端末 2 のローカル管理者	攻撃者によって侵入されている

【前提条件】
- 攻撃者がドメインユーザのクライアント端末に侵入し、マルウエア感染などによって遠隔操作が可能であること。また、クライアント端末のローカル管理者権限を窃取可能であること （メモリからの認証情報窃取などの攻撃活動を行うため）
- AD の脆弱性 （MS14-068）に対して未対処など、攻撃者がドメイン管理者権限を窃取可能であること
- 侵害したクライアント端末から DC に対するリモートログインが可能であること

【検証の流れ】

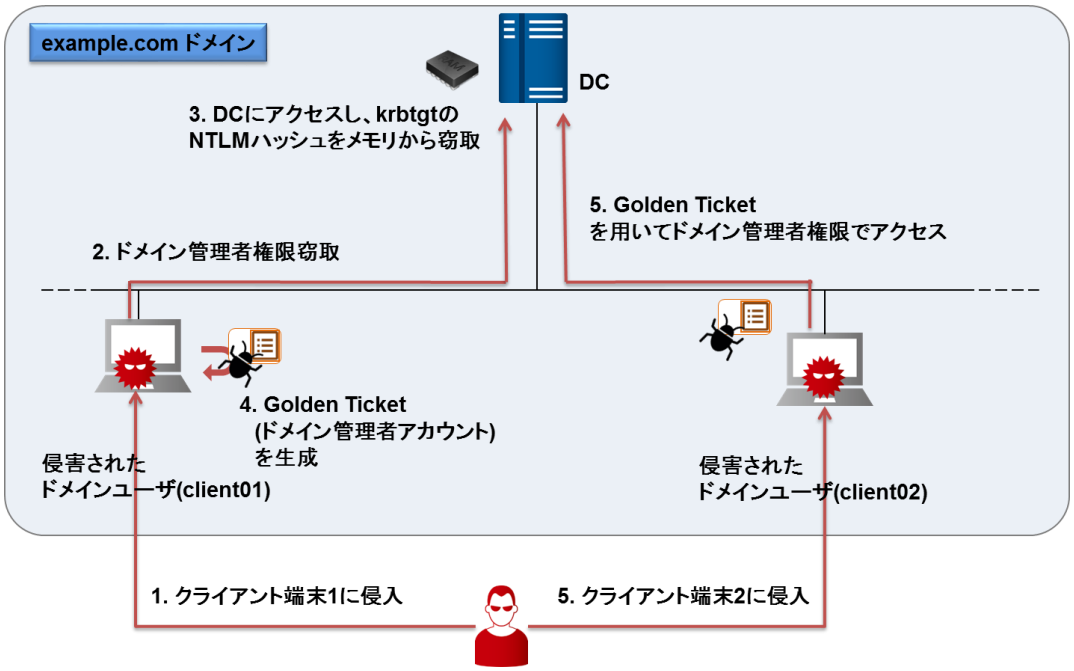
1. クライアント端末 1 にログイン
2. AD の脆弱性（MS14-068）を悪用し、ドメイン管理者へ権限昇格
3. DC へアクセスし、DC のメモリから krbtgt の NTLM ハッシュを窃取
4. クライアント端末 1 で、窃取した krbtgt の NTLM ハッシュなどを用いて Golden Ticket を作成。Golden Ticket を使用し、ドメイン管理者権限で DC へアクセス
5. クライアント端末 2 にログインし、Golden Ticket を使用して、ドメイン管理者権限で DC にアクセス
6. krbtgt アカウントのパスワードを 2 回変更

【結果】

・作成した Golden Ticket を使用し、ドメイン管理者権限で DC へアクセスできることを確認

・Golden Ticket を作成した端末やアカウント以外においても、同様にドメイン管理者権限で DC へアクセスできることを確認

・krbtgt アカウントのパスワードを 2 回変更することで、作成した Golden Ticket が無効化され、DC へのアクセスが失敗することを確認



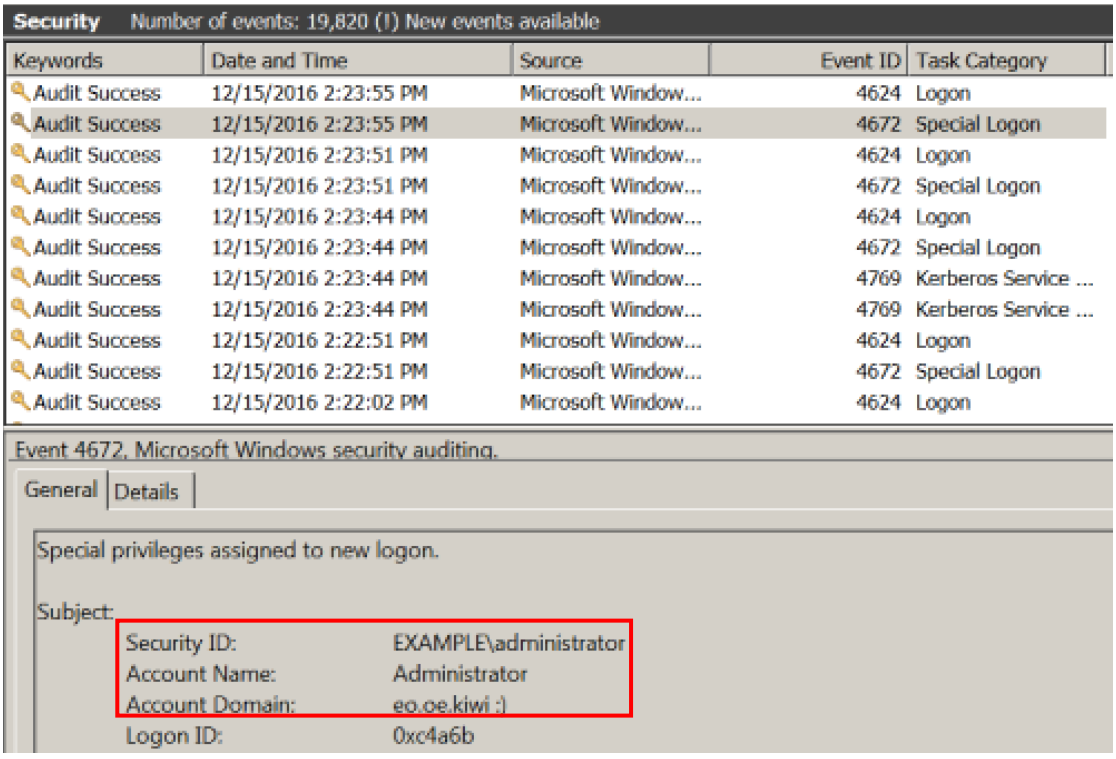
［図 18. Golden Ticket を使用した検証の流れ］

以下は、検証結果 5 にてメモリ上に展開した Golden Ticket である。ドメイン管理者アカウント（Administrator）になりすましていること、有効期限が 10 年であることなどがわかる。

```
C:\Users\client02>klist

Current LogonId is 0:0x1f0a39

Cached Tickets: (1)

#0>     Client: Administrator @ example.com
        Server: krbtgt/example.com @ example.com
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
        Start Time: 12/15/2016 14:19:15 (local)
        End Time:   12/13/2026 14:19:15 (local)
        Renew Time: 12/13/2026 14:19:15 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
```

［図 19. Golden Ticket の例］

イベントログには Kerberos 認証成功（イベント ID : 4768）や特権の割り当て（ID : 4672）が記録されたが、正規のドメイン管理者アカウント（Administrator）になりすまされているため、正規利用との判別が難しい。本検証で使用した特定ツールの古いバージョンの場合は、「Account Domain」に「eo.oe.kiwi : ） 」などの特徴的な文字列が記録される。新しいバージョンのツールではこのような特徴的な文字列は出力されない。



［図 20. DC に出力されたイベント ID:4672 の結果］

2. Silver Ticket を使用した攻撃の検証

【検証内容】

攻撃者がファイルサーバのローカル管理者権限を窃取後、ファイルサーバのファイル共有サービス（CIFS サービス）およびタスク作成などの機能を提供する HOST サービスに対する Silver Ticket を作成するシナリオを想定し、検証を実施。Silver Ticket をファイルサーバの管理者権限を持たないアカウントで使用し、タスクの作成が可能であるかを確認した。また、Silver Ticket を無効化する手順についても検証を行った。

［表 12. 検証環境］

種別 （ ）内はホスト名	OS	運用で使用するアカウント	権限	前提条件
DC （winserver2008）	Windows Server 2008 R2	Administrator	・ドメイン管理者	-
ファイルサーバ （fileserver2008）	Windows Server 2008 R2	Administrator	・ドメインユーザ ・ローカル管理者	-
ファイルサーバ管理専用端末	Windows 7 64bit	fsadmin	・ドメインユーザ ・ファイルサーバ管理専用端末のローカル管理者 ・ファイルサーバへのリモートデスクトップ接続	・攻撃者によって侵入されている ・ファイルサーバ管理者権限の認証情報が残存している
クライアント端末 1(client01)	Windows 7 64bit	client01	・ドメインユーザ ・ローカル管理者	攻撃者によって侵入されている

【前提条件】

- 攻撃者がドメインユーザのクライアント端末に侵入し、マルウエア感染などによって遠隔操作が可能であること。また、クライアント端末のローカル管理者権限を窃取可能であること （メモリからの認証情報窃取などの攻撃活動を行うため）
- 侵入した端末にファイルサーバ管理者アカウントの認証情報が残存しており、侵入した端末からファイルサーバにアクセスが可能であること
- ファイルサーバのコンピュータアカウントのパスワードを 2 回変更することで、Silver Ticket が無効化できることを確認する

【検証の流れ】

1. ファイルサーバ管理専用端末にログイン
2. メモリから fsadmin の NTLM ハッシュなどの認証情報を窃取
3. ファイルサーバ管理専用端末で、窃取した認証情報を用いて Pass-the-Hash を行い、fsadmin になり

すまし、ファイルサーバへアクセス。ファイルサーバのメモリからコンピュータアカウントの NTLM ハッシュを窃取

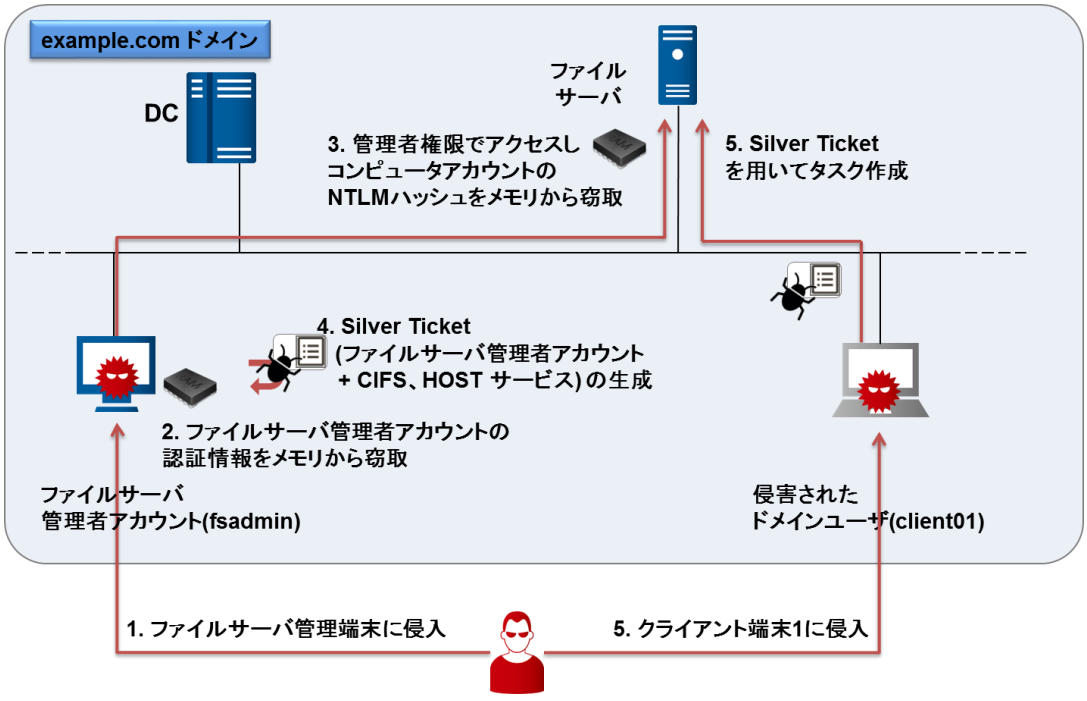
4. 窃取したコンピュータアカウントの NTLM ハッシュなどを用いて CIFS サービスと HOST サービスの Silver Ticket を作成。Silver Ticket を使用し、ファイルサーバ管理者権限でファイルサーバ上のリソースにアクセス
5. クライアント端末 1 にログインし、Silver Ticket を使用して、ファイルサーバ管理者権限でファイルサーバ上のリソースにアクセス
6. ファイルサーバのコンピュータアカウントのパスワードを 2 回変更

【結果】

・作成した Silver Ticket を使用し、ファイルサーバ管理者権限でファイルサーバ上のリソースへアクセスできることを確認。また、DC のログに Silver Ticket を使用したアクセスの痕跡が残らないことを確認

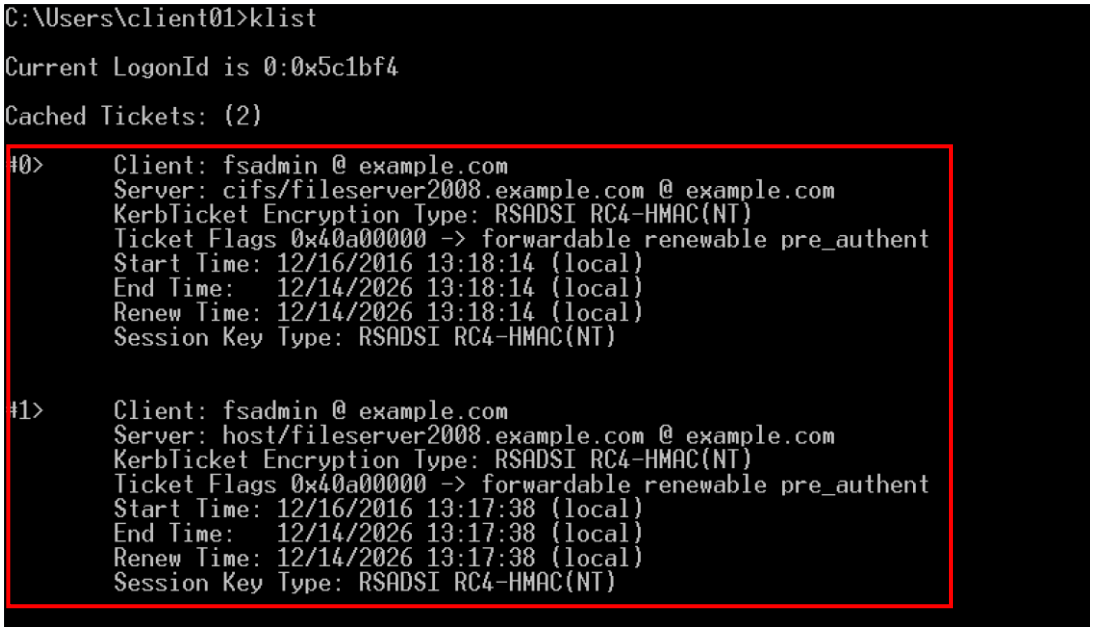
・Silver Ticket を作成した端末やアカウント以外においても、同様にファイルサーバ管理者権限でファイルサーバ上のリソースへアクセスできることを確認

・krbtgt アカウントのパスワードを 2 回変更することで、作成した Silver Ticket が無効化され、ファイルサーバ上のリソースへのアクセスが失敗することを確認



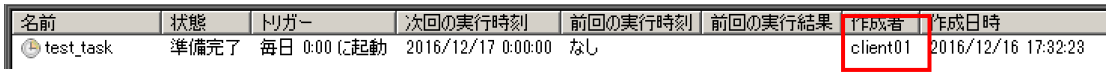
［図 21. Silver Ticket を使用した検証の流れ］

以下は、検証結果 5 にてメモリ上に展開した Silver Ticket の例である。ファイルサーバ管理者アカウント（fsadmin）になりすましていること、有効期限が 10 年であること、CIFS 、HOST サービスに対する Silver Ticket であることなどがわかる。



［図 22. Silver Ticket の例］

Silver Ticket を使用して、リモートからファイルサーバ上にタスクを作成すると、ファイルサーバのタスクスケジューラには、タスクの「作成者」として client01 （Silver Ticket を使ってなりすます前のアカウント） が記録された。



［図 23. ファイルサーバに不正に作成されたタスクスケジュール］

DC のイベントログには、Silver Ticket を使用したアクセスに関するログは記録されなかったが、接続先であるファイルサーバには イベント ID : 4624,4672 が記録された。

コンピュータアカウントのパスワード変更については、変更対象のサーバ上で、管理者権限でコマンドプロンプトを起動し、以下のように NETDOM コマンドを実行することで変更可能なことを確認した。

NETDOM RESETPWD /S:{DC の FQDN} /UD:{ドメイン名}¥{ドメインユーザのアカウント名} /PD:{ドメインユーザのパスワード}

Appendix I) ログと Active Directory の運用に関する実態調査

JPCERT/CC では、各組織においてのログの保管状況や AD の運用状況などの高度サイバー攻撃への備えに関する実態調査を目的とし、主催したセミナーなどの参加者に協力いただいてアンケートによる実態調査を実施した。
本調査で実施したアンケートの概要は次のとおりである。調査項目については以下を参照のこと。

実施日時	2016 年 7 月から 2016 年 11 月まで
実施対象	JPCERT/CC が開催したセミナーの参加者（主に組織のセキュリティ担当者やシステム管理者）
実施要綱	ログ調査状況や AD の運用に関する実態の把握、アンケート分析結果を踏まえたセキュリティ啓発への活用などの目的を説明した上で、上記のセミナーの参加者に匿名でアンケート記入を依頼し、セミナーの終了時に回収した
調査票の概要	「ログ調査に関するアンケート」と題して、各組織におけるログ調査状況や AD の運用状況などを質問した
回答組織数	52 組織

実態調査の結果より、以下のような傾向にあることが明らかになった。

- AD のログを保管している組織は 72%であり、プロキシサーバのログ（84%）やファイアウォールのログ（82%）などと比較して、若干低い傾向であった（詳細はアンケート項目 4 を参照）
- AD を含む機器のログについては、多くの組織で確認しているとの回答であった（73%）。また、ログの保管や確認に関してルールを設けている組織も一定数存在するものの、ログ分析に関する十分なノウハウがないなどの課題があることが分かった（詳細はアンケート項目 6,7,8,9 を参照）
- DC の OS としては Windows Server 2008 R2 が最も多く、次いで Windows Server 2012 R2 多かった。また、クライアント OS としては Windows 7 が多いことがわかった（詳細はアンケート項目 10-1,10-2 を参照）。また、Windows Server 2008 R2 や Windows 7 に対して有効な攻撃手法やツールが公開されていることを受けて、JPCERT/CC でこれらの OS を使用して攻撃手法や対策の有効性の検証を実施した。検証の詳細については 「Appendix H） Active Directory に対する攻撃の検証結果」を参照のこと
- 特権を使用するアカウントや端末を限定した運用を行っている組織は 26%、特権の使用に対して申請や承認を行うプロセスを設けている組織は 29%であった。多くの組織で特権が悪用されても把握しづらい環境にあることがわかった（詳細はアンケート項目 10-3 を参考）
- DC へのセキュリティ更新プログラムを適用するタイミングは組織によってばらつきがあったが、ほとんど適用していないとの回答が 26%、システムメンテナンスのタイミングで適用しているとの回

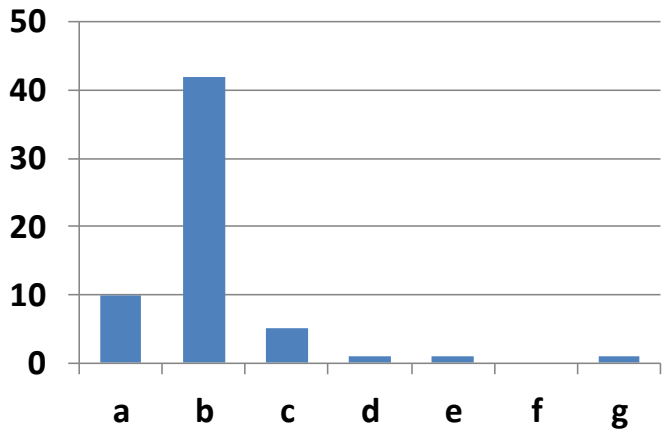
答が 21%であり、脆弱性が残存した状態で AD を運用している組織も一定数存在することがわかった（詳細はアンケート項目 10-4 を参考）

- 60%の組織で、コンピュータに共通の ID やパスワードを設定しているアカウントが存在することがわかった。多くはメンテナンスなどの目的であったが、このような環境では横断的侵害を受ける可能性が高い（詳細はアンケート項目 10-5、10-5-1 を参考）
- DC を設置しているネットワークセグメントと業務で使用する端末のネットワークセグメントを分離していない、もしくは不明と回答した組織は 44%であった（詳細はアンケート項目 10-6 を参考）。業務用端末に侵入された場合、DC への不正アクセスを受ける可能性が高い環境にあることが分かった

これらの調査結果から、AD に対するログの保管や調査、セキュリティ対策の重要性については、インターネットとの接続点となっているプロキシサーバやファイアウォールなどの機器に比べて、認知されていない傾向にあると考える。また、AD に対する攻撃を受けやすい、または攻撃を受けても検知しづらい環境になっている組織が複数存在することがわかった。

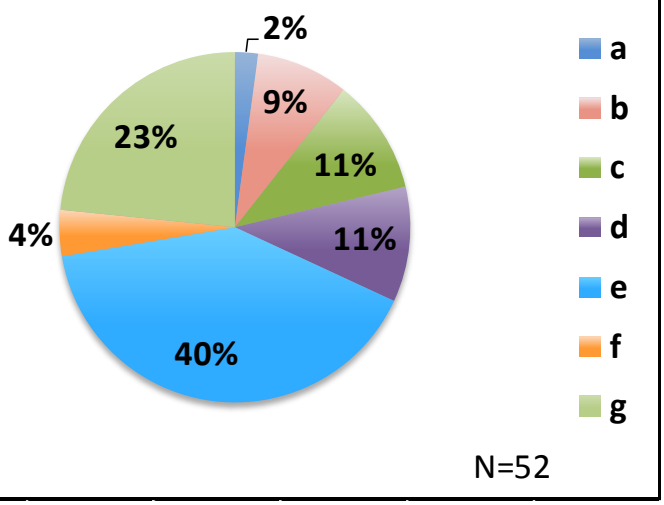
1. 回答者の担当業務について

	担当業務	回答数
a	システム管理者	10
b	セキュリティ担当者	42
c	システムエンジニア	5
d	監査担当	1
e	コンサルタント	1
f	CSO / CEO	0
g	上記以外	1
	合計	60



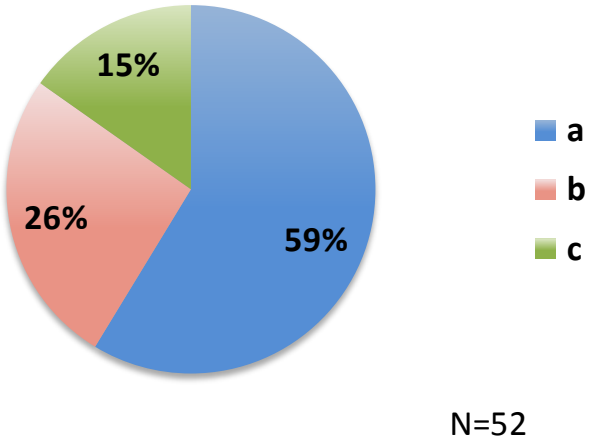
2. 組織の規模について

	組織の規模	回答数
a	50名以下	1
b	50～100名	4
c	100～500名	5
d	500～1,000名	5
e	1,000～5,000名	19
f	5,000～10,000名	2
g	10,000名以上	11
	合計	47



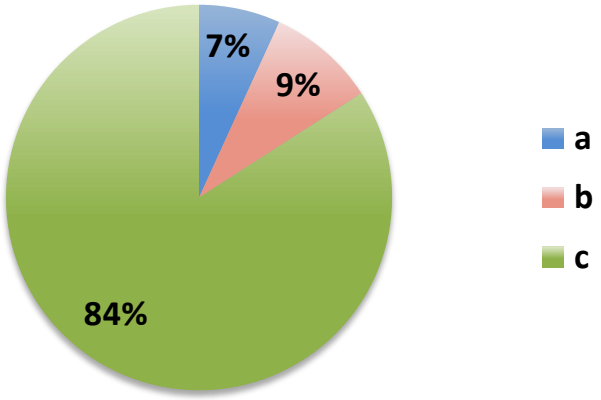
3. 標的型攻撃によるマルウエア感染の経験の有無

	感染経験の有無	回答数
a	いいえ	27
b	不明	12
c	はい	7
	合計	46



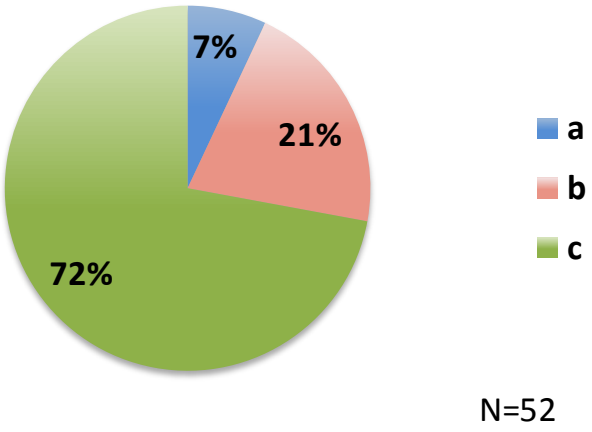
4. セキュリティ上の観点で以下の機器のログを保存しているか。
a) プロキシサーバ

	ログの保存	回答数
a	いいえ	3
b	不明	4
c	はい	37
	合計	44



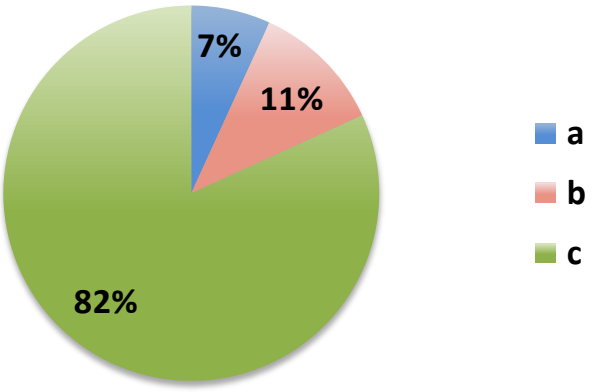
4. セキュリティ上の観点で以下の機器のログを保存しているか。
b) Active Directory

	ログの保存	回答数
a	いいえ	3
b	不明	9
c	はい	31
	合計	43



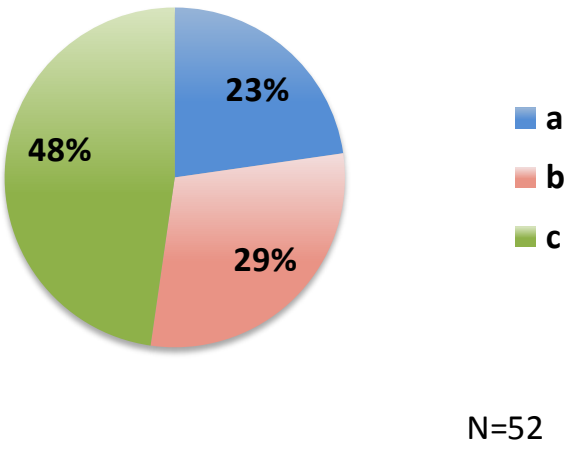
4. セキュリティ上の観点で以下の機器のログを保存しているか。
c) ファイアウォール

	ログの保存	回答数
a	いいえ	3
b	不明	5
c	はい	36
	合計	44



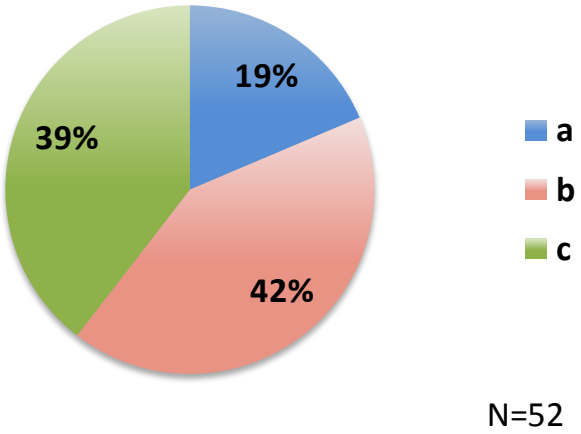
4. セキュリティ上の観点で以下の機器のログを保存しているか。
d) ファイルサーバ

	ログの保存	回答数
a	いいえ	10
b	不明	13
c	はい	21
	合計	44



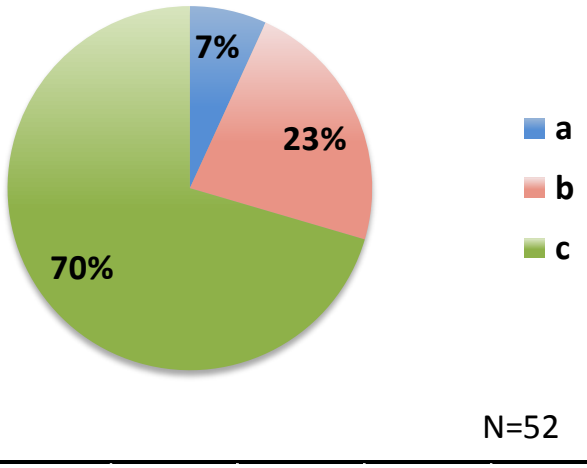
4. セキュリティ上の観点で以下の機器のログを保存しているか。
e) DNS（ｷｬｯｼｭｻｰﾊﾞ）

	ログの保存	回答数
a	いいえ	8
b	不明	18
c	はい	17
	合計	43



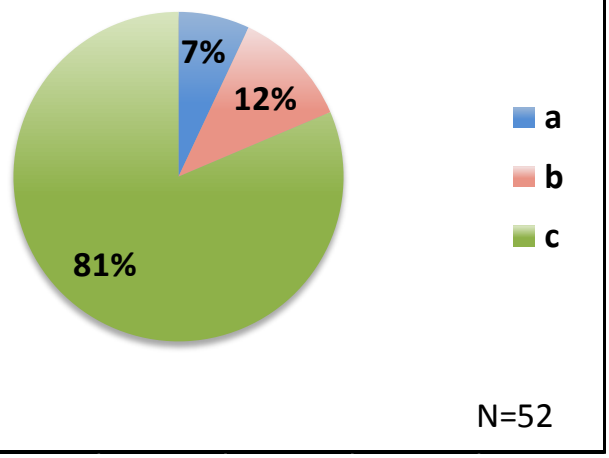
4. セキュリティ上の観点で以下の機器のログを保存しているか。
f) メールサーバ

	ログの保存	回答数
a	いいえ	3
b	不明	10
c	はい	31
	合計	44



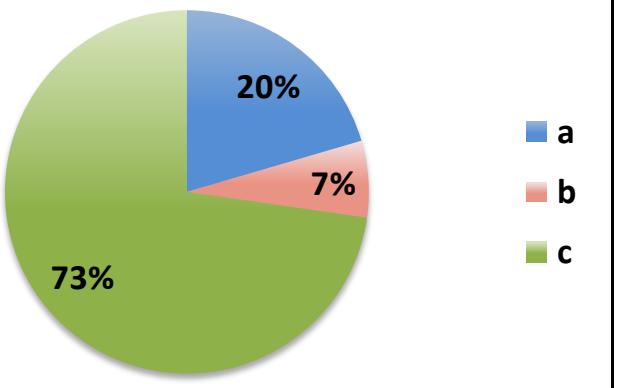
5. ログ（プロキシサーバなど）において、外部との通信先URLの情報を記録しているか

	通信先URLの記録の有無	回答数
a	いいえ	3
b	不明	5
c	はい	35
	合計	43



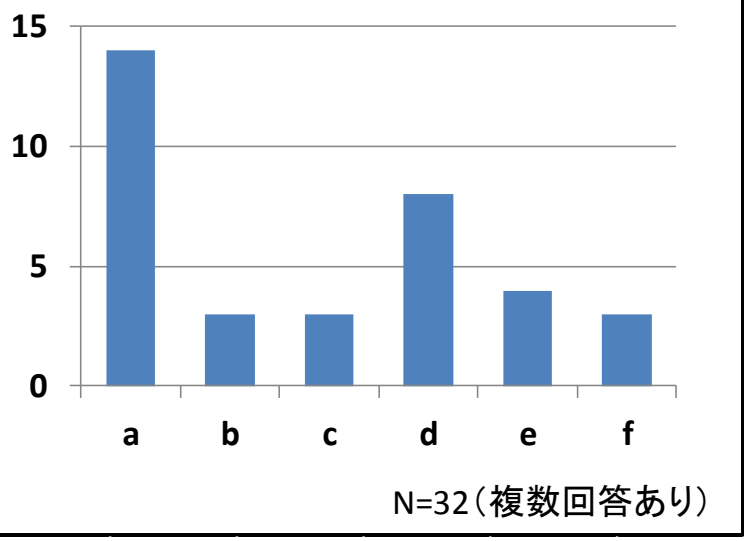
6. 保存したログをセキュリティの観点（攻撃の検知等）で確認しているか

	確認の有無	回答数
a	いいえ	9
b	不明	3
c	はい	32
	合計	44



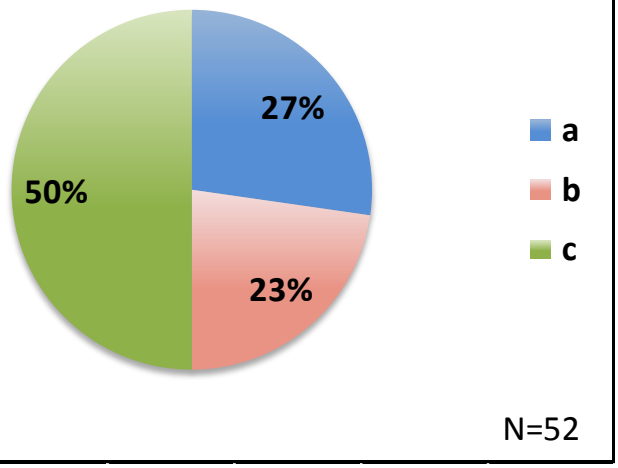
6-1. 確認している場合は、確認頻度はどれくらいか

	確認頻度	回答数
a	毎日	14
b	週に一度	3
c	月に一度	3
d	外部からの情報提供（インディケータ等）をトリガーとして	8
e	不定期	4
f	不明	3
	合計	35



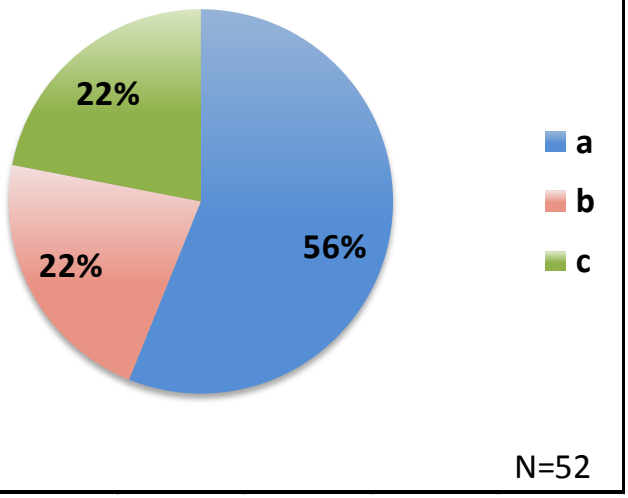
7. セキュリティ上の観点でログの保存に関するルールがあるか

	ルールの有無	回答数
a	いいえ	12
b	不明	10
c	はい	22
	合計	44



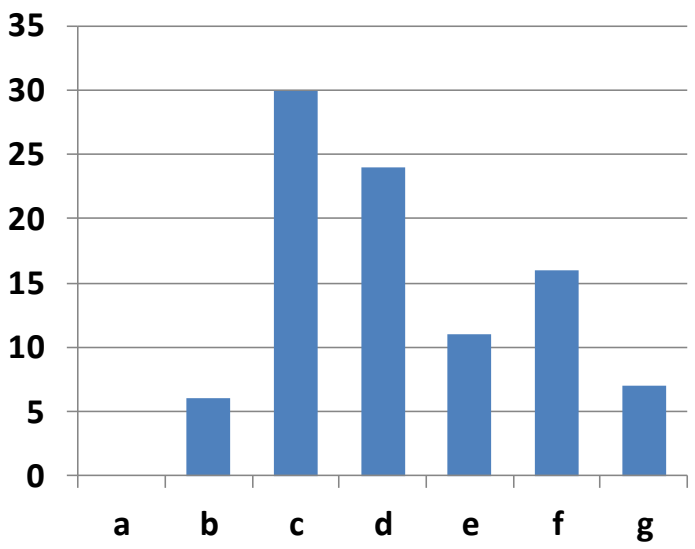
8. セキュリティ上の観点でログの監査、確認に関するルールがあるか

	ルールの有無	回答数
a	ルールはない	23
b	ルールがあり、監査ポリシーが定められている	9
c	不明	9
	合計	41



9. ログの運用や分析に関して課題と感じている点は何か

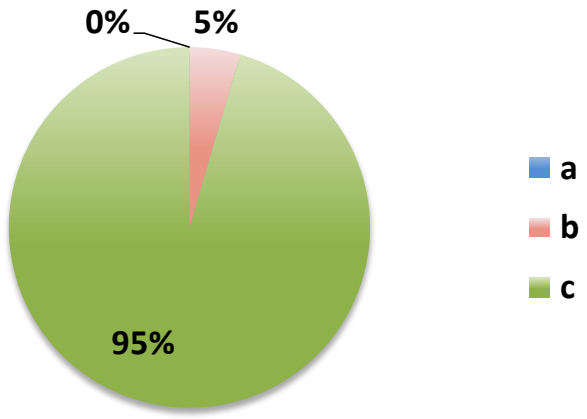
	課題	回答数
a	特に課題はない	0
b	ログを保存していない	6
c	ログ分析に関する十分なノウハウがない	30
d	ログ分析に担当者の工数をさけない	24
e	ログの運用(保存期間/容量など)を変更するための社内調整に時間がかかる	11
f	ルールや基準が存在しない	16
g	その他	7
	合計	94



N=52(複数回答あり)

10. Active Directory を利用しているか

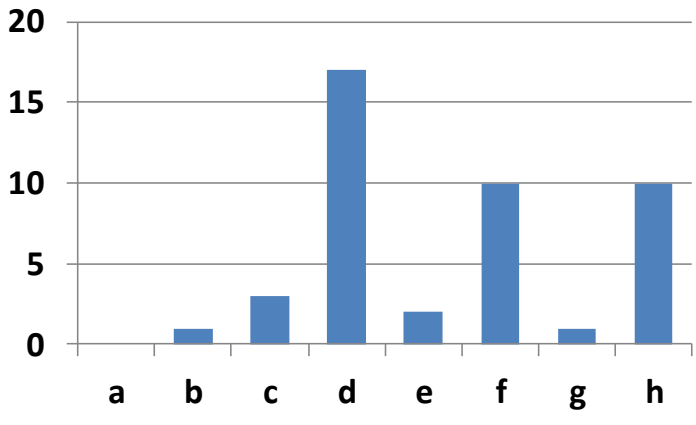
	ADの利用の有無	回答数
a	いいえ	0
b	不明	2
c	はい	42
	合計	44



N=52

10-1. ドメインコントローラの OS のバージョンは何か

	OSのバージョン	回答数
a	Windows Server 2003	0
b	Windows Server 2003 R2	1
c	Windows Server 2008	3
d	Windows Server 2008 R2	17
e	Windows Server 2012	2
f	Windows Server 2012 R2	10
g	その他	1
h	不明	10
	合計	44

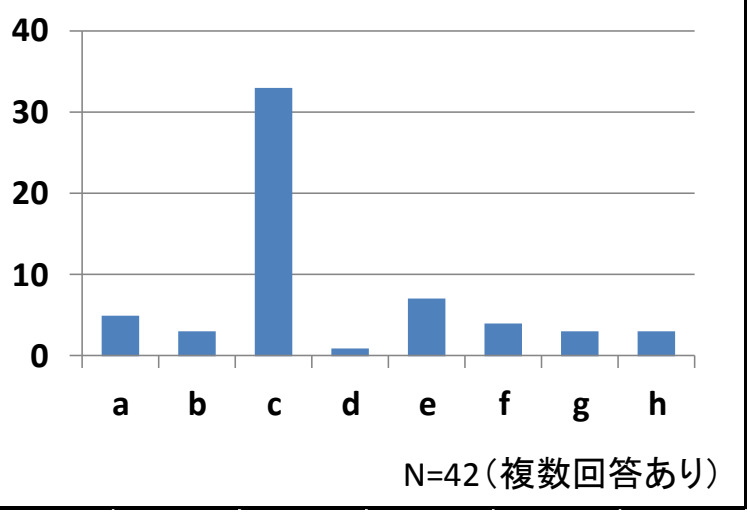


N=42(複数回答あり)

※「10. Active Directory を利用しているか」の質問に「はい」と回答いただいた 42 名のみ対象

10-2. クライアント端末の OS のバージョンは何か

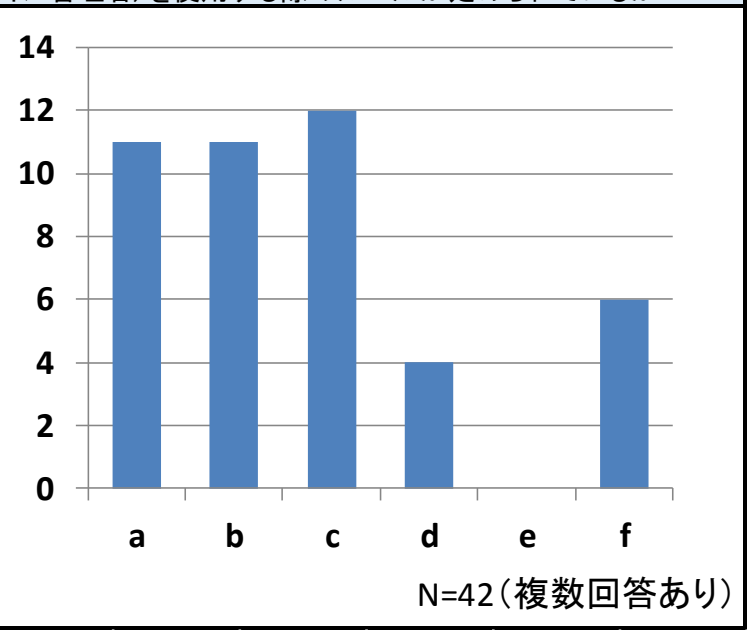
	OSのバージョン	回答数
a	Windows XP	5
b	Windows Vista	3
c	Windows 7	33
d	Windows 8	1
e	Windows 8.1	7
f	Windows 10	4
g	その他	3
h	不明	3
	合計	59



※「10. Active Directory を利用しているか」の質問に「はい」と回答いただいた 42 名のみ対象

10-3. Active Directory 環境で特権（ドメイン管理者）を使用する際のルールが定められているか

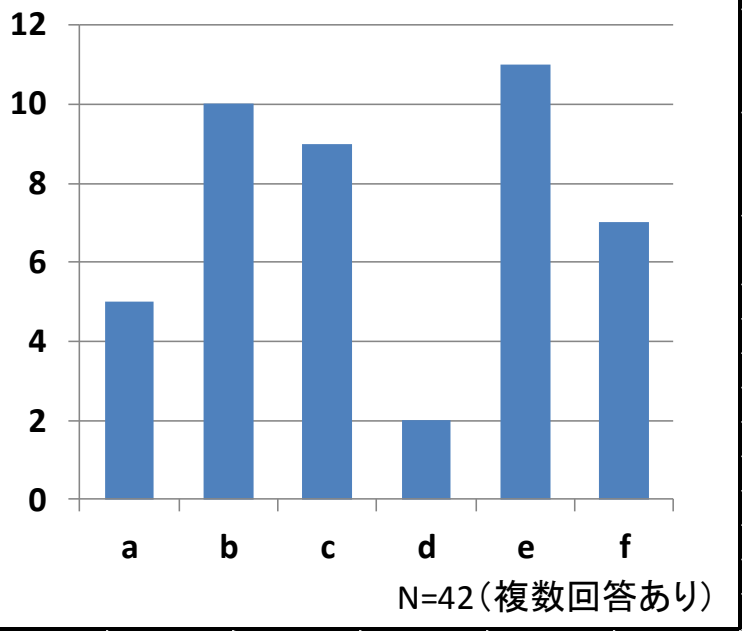
	ルールの有無	回答数
a	ルールはない	11
b	ルールがある（特権を使用するアカウントや端末が決まっている）	11
c	ルールがある（特権を使用するのに申請・承認が必要）	12
d	ルールがある（業務で必要な時に一時的に特権を割り当てる）	4
e	その他ルール	0
f	不明	6
	合計	61



※「10. Active Directory を利用しているか」の質問に「はい」と回答いただいた 42 名のみ対象

10-4. ドメインコントローラにセキュリティパッチを適用する頻度

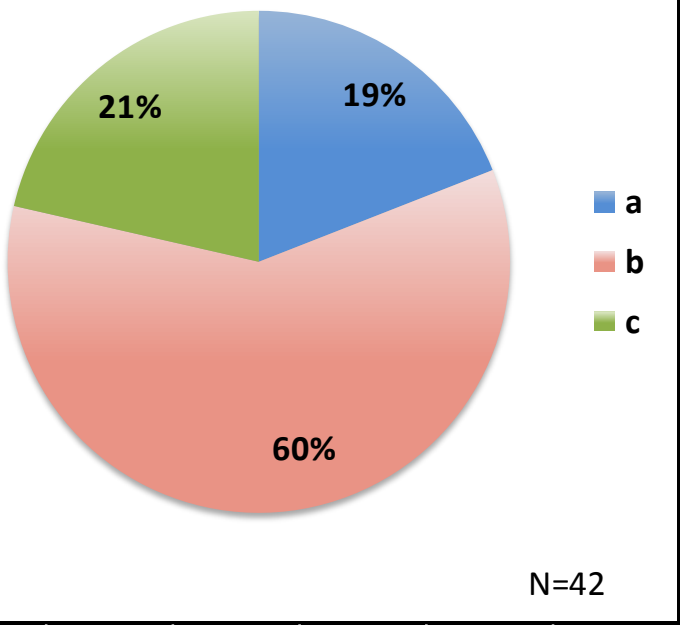
	頻度	回答数
a	セキュリティパッチがリリースされた後、速やかに適用している	5
b	脆弱性の脅威度に基づいてパッチの適用時期を検討している	10
c	システムのメンテナンスのタイミングで適用している	9
d	メンテナンス周期	2
e	ほとんど適用していない	11
f	不明	7
	合計	44



※「10. Active Directory を利用しているか」の質問に「はい」と回答いただいた 42 名のみ対象

10-5. 各端末やサーバに、共通ID/パスワードを設定しているアカウントがあるか

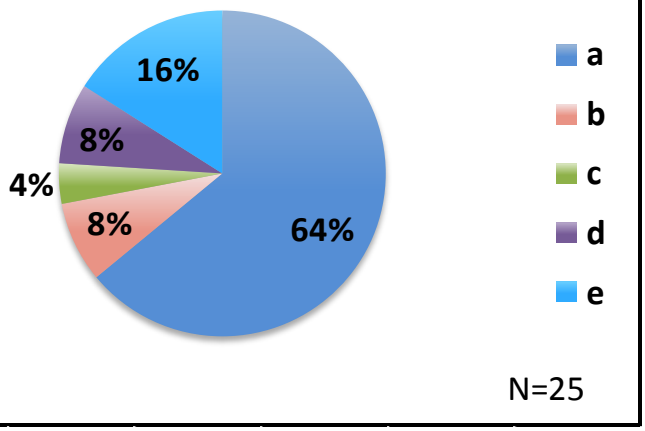
	共通ID/パスワードの有無	回答数
a	なし	8
b	あり	25
c	不明	9
	合計	42



※「10. Active Directory を利用しているか」の質問に「はい」と回答いただいた 42 名のみ対象

10-5-1. 共通ID/パスワードを設定しているアカウントの用途

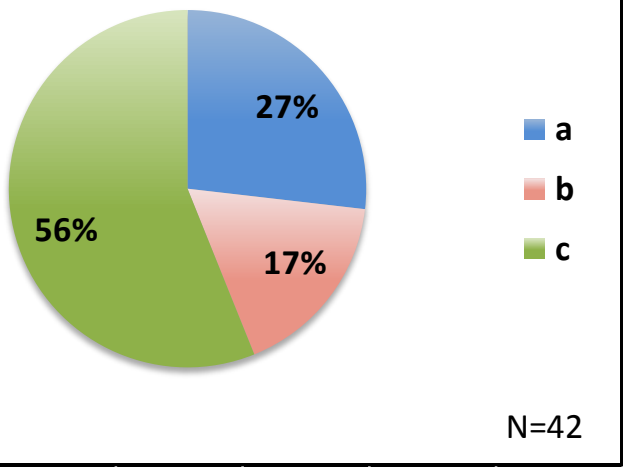
	用途	回答数
a	メンテナンス用	16
b	メンテナンス、業務用	2
c	メンテナンス用、ヘルプデスク業務用	1
d	初期設定用	2
e	業務利用	4
	合計	25



※「10-5. 各端末やサーバに、共通 ID/パスワードを設定しているアカウントがあるか」の質問に「はい」と回答いただいた 25 名のみ対象

10-6. ドメインコントローラを設置しているネットワークセグメント(サーバセグメント)とクライアント端末のネットワークセグメント(業務用セグメント)を分けているか

	共通ID/パスワードの有無	回答数
a	分けていない	11
b	不明	7
c	分けている	23
	合計	41



※「10. Active Directory を利用しているか」の質問に「はい」と回答いただいた 42 名のみ対象

参考情報

[1] 経済産業省、独立行政法人 情報推進機構
サイバーセキュリティ経営ガイドライン Ver1.1
http://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v1.1.pdf

[2] JPCERT/CC
Active Directory のドメイン管理者アカウントの不正使用に関する注意喚起
https://www.jpcert.or.jp/at/2014/at140054.html

[3] Microsoft
Securing Active Directory: An Overview of Best Practices
https://technet.microsoft.com/en-us/library/dn205220.aspx

[4] JPCERT/CC
2014 年 11 月 Kerberos KDC の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2014/at140048.html

[5] Microsoft
Mitigating Pass-the-Hash（PtH）Attacks and Other Credential Theft, Version 1 and 2
https://www.microsoft.com/en-us/download/details.aspx?id=36036

[6] JPCERT/CC
高度サイバー攻撃への対処におけるログの活用と分析方法
https://www.jpcert.or.jp/research/apt-loganalysis.html

[7] JPCERT/CC
インシデント調査のための攻撃ツールなどの実行痕跡調査に関する報告書
https://www.jpcert.or.jp/research/ir_research.html

[8] Microsoft
ユーザー権利の割り当て
https://msdn.microsoft.com/ja-jp/library/dn221963.aspx

[9] Microsoft
AppLocker の技術概要
https://technet.microsoft.com/ja-jp/library/hh831440.aspx

[10] Microsoft
AppLocker を使用するための要件

https://technet.microsoft.com/ja-jp/library/ee424382.aspx

[11] Microsoft
マイクロソフト セキュリティ アドバイザリ 2871997: 資格情報の保護と管理を強化する更新プログラム
https://technet.microsoft.com/ja-jp/library/security/2871997

[12] Microsoft
Windows Server Update Services の概要
https://technet.microsoft.com/ja-jp/library/hh852345.aspx

[13] Microsoft
追加の LSA の保護の構成
https://msdn.microsoft.com/ja-jp/library/dn408187

[14] Microsoft
Protected Users
https://msdn.microsoft.com/ja-jp/library/dn518179#BKMK_AddtoProtectedUsers

[15] Microsoft
Restricted Admin mode for RDP in Windows 7 / 2008 R2
https://blogs.technet.microsoft.com/kfalde/2015/01/10/restricted-admin-mode-for-rdp-in-windows-7-2008-r2/

[16] Microsoft
Credential Guard によるドメインの派生資格情報の保護
https://technet.microsoft.com/ja-jp/itpro/windows/keep-secure/credential-guard

[17] JPCERT/CC
Windows の新セキュリティ機能を検証する:LSA の保護モードと Credential Guard
https://www.jpcert.or.jp/magazine/acreport-lsa_protect.html

[18] Microsoft
Local Administrator Password Solution
https://technet.microsoft.com/en-us/mt227395.aspx

[19] Microsoft
Netdom resetpwd
https://technet.microsoft.com/en-us/library/cc785478

[20] Microsoft
マイクロソフト セキュリティ アドバイザリ: 資格情報の保護と管理を強化する更新プログラム: 2014 年 5 月 13 日
https://support.microsoft.com/ja-jp/help/2871997/microsoft-security-advisory-update-to-improve-credentials-protection-and-management-may-13,-2014

[21] Microsoft
最大ログ サイズを設定する
https://technet.microsoft.com/ja-jp/library/cc748849

[22] Microsoft
ログの保持ポリシーを設定する
https://technet.microsoft.com/ja-jp/library/cc721981

[23] Microsoft
Auditpol の取得
https://technet.microsoft.com/ja-jp/library/cc772576

[24] Microsoft
監査ポリシーの詳細な構成
https://technet.microsoft.com/ja-jp/library/dn452415

[25] Microsoft
Local user accounts incorrectly trigger domain account logon auditing events when they view history of scheduled tasks in Windows Vista, in Windows Server 2008, in Windows 7 or in Windows Server 2008 R2
https://support.microsoft.com/en-us/help/2549079/local-user-accounts-incorrectly-trigger-domain-account-logon-auditing-events-when-they-view-history-of-scheduled-tasks-in-windows-vista,-in-windows-server-2008,-in-windows-7-or-in-windows-server-2008-r2

[26] Microsoft
ドメイン環境で使用されるポートについて
https://blogs.technet.microsoft.com/jpntsblog/2009/03/03/563/

[27] Microsoft
ネットワーク経由のアクセスを拒否
https://technet.microsoft.com/ja-jp/library/mt629215

[28] Microsoft
リモート デスクトップ サービスを使ったログオンを拒否
https://technet.microsoft.com/ja-jp/library/mt629219

[29] Microsoft
Local Administrator Password Solution （LAPS） の提供を開始

https://blogs.technet.microsoft.com/jpsecurity/2015/05/14/local-administrator-password-solution-laps/

3 章以降に示す Windows のログ出力に関する設定例については、JPCERT/CC の調査で確認した一例であり、すべてのバージョンでの動作を保証するものではありません。

本設定に関して発生したいかなる損害も JPCERT/CC は、責任を負いかねます。実際の機器に設定を行う場合は、各機器、もしくはベンダーが提供するマニュアルを参照し、十分なテストを実施の上、設定してください。