# Google.ChromeOS-Administrator.v2024-10-07.q20

| | |
|---|---|
| 試験コード: | ChromeOS-Administrator |
| 試験名称: | Professional ChromeOS Administrator Exam |
| 認定資格: | Google |
| 無料問題数: | 20 |
| バージョン: | v2024-10-07 |
| アクセス数: | 640 |
| ページビュー数: | 200 |
| https://www.jpnpdf.com/Google.ChromeOS-Administrator.v2024-10-07.q20-mondaishu.html | |

最新問題: **1**
大手マーケティング会社が IT 部門にインターンを雇用します。インターンは ChromeOS デバイスの情報のみを閲覧でき、デバイスの管理や更新はできないようにする必要があります。
管理者はどのようにしてこの役割をインターンに割り当てるべきでしょうか?
管理者はどのようにしてこの役割をインターン生に割り当てるべきでしょうか?
**A.** カスタムサービス管理者ロールを作成し、2FA を有効にする
**B.** Chrome 管理下でカスタムロールを作成し、Telemetry API ロールを割り当てる
**C.** Chrome管理下でカスタムロールを作成し、設定のルーティンを割り当てる
**D.** Chrome 管理でカスタム ロールを作成し、ChromeOS デバイスの管理ロール K を割り当てます。
**Answer: B (**メーッセージを残す**)**
管理や更新機能なしで、インターンに ChromeOS デバイス情報への読み取り専用アクセス権を付与するには、次の操作を行う必要があります。
* カスタム ロールの作成: Google 管理コンソールで、「デバイス管理」-> 「Chrome 管理」-> 「ユーザー設定」-> 「ロール」に移動します。
* テレメトリ API ロールの割り当て: カスタム ロール内で、「テレメトリ API」ロールを割り当てます。これにより、インターンは API を通じて収集されたデバイス情報を表示できますが、変更することはできません。
* 他のロールを除外する: 管理権限または更新権限を付与する他のロールが割り当てられていないことを確認します。
オプション A は、通常、より広範な管理アクセス権を持つサービス管理者ロールに関係するため、正しくありません。
オプション C は正しくありません。「設定」ロールでは、意図したよりも多くの権限が付与される可能性があります。

オプション D は不正解です。「ChromeOS デバイスの管理」ロールでは完全な管理権限が付与されるため、インターンには適していません。
参考文献:
* Chrome ブラウザ クラウド管理 API: https://developers.google.com/chrome/policy

最新問題: **2**
Verified Boot の機能は何ですか?
**A.** ファームウェアとOSが改ざんされていないことを確認します
**B.** 匿名のゲストがデバイスを使用できないように保護します
**C.** 厳格なポリシー制御の必要性を排除します
**D.** ユーザーが許可されていないウェブサイトにアクセスするのを防ぎます
**Answer: A (**メッセージを残す**)**
検証済みブートとは、起動時にシステムの整合性をチェックする ChromeOS のセキュリティ機能です。ファームウェア (低レベルのソフトウェア) とオペレーティング システムが不正なソースによって変更または破損されていないことを確認します。改ざんが検出されると、検証済みブートは回復プロセスを開始して、システムを既知の正常な状態に復元できます。
検証済みブートはゲスト アクセスを直接管理しないため、オプション B は正しくありません。
オプション C は不正解です。検証済みブートはポリシー制御を置き換えるのではなく、補完するセキュリティ レイヤーだからです。
オプション D は不正解です。Web サイトのアクセス制御は、Web フィルタリングやコンテンツ制限などの他のメカニズムによって処理されるためです。
参考資料: https://www.chromium.org/chromium-os/chromiumos-design-docs/verified-boot/

最新問題: **3**
ネットワーク管理者が Google サービスのトラフィックをブロックしたいと考えています。結果はどうなりますか?
**A.** Google 検索は機能しません
**B.** Chromeデバイスがクラッシュします
**C.** ChromeデバイスはGoogleにアクセスできなくなります
**D.** 何も問題はありません
**Answer: A (**メッセージを残す**)**
Google サービスのトラフィックをブロックすると、Chrome デバイスは google.com を含む Google 所有のドメインにアクセスできなくなります。これは、結果を提供するために Google サーバーとの通信に依存している Google 検索に直接影響します。
Gmail、YouTube、Google ドライブなどの他の Google サービスにもアクセスできなくなります。ただし、Chrome デバイス自体はクラッシュせず、他の Web サイトやアプリケーションは引き続き機能します。

最新問題: **4**
ChromeOS デバイスに追加のウイルス対策ソフトウェアが必要ない理由を尋ねられました。どのように答えるべきでしょうか?
**A.** ChromeOS が更新されるたびに、デバイス上のウイルス対策ソフトウェアが自動的に更新されます。
**B.** すべての ChromeOS デバイスには、デバイスの寿命中に自動的に更新されるウイルス対策ソフトウェアがプリインストールされています。
**C.** 多層セキュリティアプローチの一環として、ChromeOSはウイルスの影響を受けない読み取り専用のオペレーティングシステムを使用しています。
**D.** 管理コンソールは、登録された ChromeOS デバイスにウイルス対策ソフトウェアを自動的に導入します。これは Chrome Enterprise/Education Upgrade に含まれています。
**Answer: C (**メーッセージを残す**)**
ChromeOS は、マルウェアやウイルスから保護するために、複数のセキュリティ層を備えて設計されています。
* 読み取り専用ファイルシステム: オペレーティング システムの大部分は読み取り専用パーティションに保存されるため、マルウェアが重要なファイルを変更することが困難になります。
* 検証済みブート: 起動時にオペレーティング システムの整合性を保証し、不正なソフトウェアによる改ざんを防止します。
* サンドボックス: さまざまなプロセスと Web サイトを分離し、侵入したマルウェアによる潜在的な被害を制限します。
* 自動更新: 脆弱性に対処するためのセキュリティ パッチと更新を定期的に配信します。
ChromeOS には従来のウイルス対策ソフトウェアは付属していませんが、組み込みのセキュリティ機能により、ほとんどの脅威に対して強力な保護を提供します。

最新問題: **5**
顧客は ChromeOS 上でミッションクリティカルなワークロードを実行しており、ChromeOS の変更を減らすようにデバイスを構成する必要があります。管理者は、セキュリティを維持し、管理作業負荷を最小限に抑えながら、OS アップデートの予期しない変更が顧客の ChromeOS デバイス ドメイン全体に影響を及ぼすリスクを軽減するにはどうすればよいでしょうか。
**A.** 更新後に強制的に自動再起動する
**B.** バリエーションを有効にする
**C.** 長期サポート チャネルに移行する
**D.** 更新ロールアウト計画を追加する
**Answer: (**解答を表示する**)**
Google 管理コンソールのアップデート展開計画を使用すると、管理者は ChromeOS アップデートをまず一部のデバイスに段階的に展開できます。これにより、デバイス全体に展開する前に制御された環境でテストできるため、すべてのデバイスに予期しない問題が発生するリスクが軽減されます。

更新ロールアウト プランを追加する手順:
* Google 管理コンソールにアクセスします。管理者の資格情報でログインします。
* デバイス管理に移動します。[デバイス] > [Chrome] > [設定] > [アップデート] に移動します。
* ロールアウト プランの作成:  更新ロールアウト プランの追加」をクリックします。
* デバイスの選択: 初期ロールアウトに含める特定のデバイスまたは組織単位 (OU) を選択します。
* タイムラインの設定: ロールアウトの開始日と終了日を定義します。
* 保存して適用: プランを保存し、選択したデバイスに適用します。

最新問題**: 6**
オンプレミスの Active Directory 環境から Google 管理コンソールにユーザーをプロビジョニングする場合の推奨方法は何ですか?
**A.** CSV 経由でアップロード
**B.** 管理 SDK ディレクトリ API
**C.** Azure AD Google Cloud/G Suite コネクタ
**D.** Google Cloud ディレクトリ同期
**Answer: D (**メーッセージを残す**)**
「プロビジョニング解除」コマンドは、ChromeOS デバイスを管理ポリシーの更新から削除するために特別に設計されています。つまり、デバイスは Google 管理コンソールからプッシュされた更新、構成、または制限を受信しなくなります。
デバイスのプロビジョニングを解除すると、次のことが起こります。
* ポリシーの削除: すべてのエンタープライズ ポリシーと構成がデバイスから削除されます。
* 管理の削除: デバイスは Google 管理コンソールから関連付けが解除され、管理対象ではなくなります。
* データワイプ オプション）プロビジョニング解除中にデバイスのデータをワイプして、会社のデータが残らないようにすることができます。
「リセット」、 無効」、 Powerwash」などの他のオプションでは、効果が異なる場合があります。
* リセット: デバイスを工場出荷時の設定にリセットしますが、管理コンソールから実行しないと管理が削除されない可能性があります。
* 無効: ユーザーのサインインを禁止しますが、ポリシーや管理は削除されません。
* Powerwash: デバイスを工場出荷時の状態にリセットし、管理を含むすべてのユーザーデータと構成を削除します。
参考文献:
* デバイスのプロビジョニング解除: https://support.google.com/chrome/a/answer/3523633

最新問題**: 7**

SSO にサードパーティのサービスを使用しています。ユーザーは Chrome デバイスにサインインするときに、SSO プロバイダのサインイン画面にリダイレクトされる前に Google アカウントの詳細を求められるため、混乱します。管理対象デバイスがデフォルトで SSO プロバイダのログイン ページを開くようにするには、どの設定を変更する必要がありますか。
**A.** SAMLシングルサインオンログイン頻度
**B.** SAMLシングルサインオンパスワード同期フロー
**C.** シングルサインオンCookieの動作
**D.** シングルサインオンIdPリダイレクト
**Answer: D (**メーッセージを残す**)**
シングル サインオン IdP リダイレクト設定は、管理対象デバイスがサードパーティの SSO プロバイダ (ID プロバイダ) のログイン ページを直接開くか、最初に Google アカウントの認証情報を要求するかを制御します。この設定を有効にすると、ユーザーのログイン プロセスが効率化され、余分な Google アカウントのプロンプトによって生じる混乱がなくなります。
オプション A は、初期ログイン ページではなく、SAML SSO の再認証の頻度を制御するため、正しくありません。
オプション B は、ログイン ページのリダイレクトではなく、Google と IdP 間のパスワード同期に関連しているため、正しくありません。
オプション C は、ログイン ページのリダイレクトではなく、SSO の Cookie の処理方法を扱っているため、正しくありません。

最新問題**: 8**
USB スティックにリカバリ イメージを作成する必要があります。どの 2 つの手順を実行する必要がありますか?
2つの回答を選択してください
**A.** デバイス設定に移動
**B.** google com/chromebooks にアクセスしてください
**C.** Google Play ストアへ移動
**D.** Chrome デバイスで Chrome ウェブストアにアクセスする
**E.** Chrome リカバリ ユーティリティをインストールし、コーン型デバイス モデルのイメージを USB スティックにダウンロードします。
**Answer: D,E (**メーッセージを残す**)**
USB スティックにリカバリ イメージを作成するには、次の手順を実行する必要があります。
* Chrome ウェブストアにアクセス: Chrome デバイス (Chromebook または Chrome ブラウザがインストールされたパソコン) で Chrome ウェブストアを開きます。
* Chromebook リカバリ ユーティリティをインストールする: 「Chromebook リカバリ ユーティリティ」拡張機能を検索してインストールします。

* ユーティリティを起動します: インストールされた拡張機能を開きます。
* デバイスの識別: リカバリ イメージを作成する ChromeOS デバイスのモデル番号を入力します。
* USB スティックを挿入します: 十分なストレージ容量 (少なくとも 4 GB) を持つ USB スティックを挿入します。
* ダウンロードと作成: ユーティリティの画面上の指示に従って、正しいリカバリ イメージをダウンロードし、起動可能な USB スティックを作成します。
このプロセスでは、正常に機能していないデバイスで ChromeOS を回復または再インストールするために使用できる USB スティックが準備されます。
参考文献:
* Chromebook を復元する: https://support.google.com/chromebook/answer/1080595?hl=en

最新問題**: 9**
ヘルプデスク管理者には、Google 管理コンソールで操作を実行するための限定された権限が必要です。
管理者は、最小権限の実践に準拠しながら、これらの権限をどのように付与すればよいでしょうか?
**A.** サービスデスクグループを作成し、サービスデスク管理者をグループに追加する
**B.** 新しいカスタム管理者ロールを作成し、割り当てる
**C.** サービスデスク管理者にサービス管理者ロールを付与する
**D.** ヘルプデスク管理者にユーザー管理のフルアクセスを許可する
**Answer: B (**メーッセージを残す**)**
* きめ細かな制御: ヘルプデスク管理者に必要な特定の権限を選択できます。これにより、悪用される可能性のある過剰なアクセス権を持たずに、ヘルプデスク管理者が職務を遂行できるようになります。
* 柔軟性: ヘルプデスクの責任が変わった場合は、後で簡単に権限を調整できます。
* 監査: Google 管理コンソールは各ロールによる変更を追跡し、不正なアクションの発生源を簡単に特定できるようにします。
* カスタム管理者ロールを作成する方法:
* Google 管理コンソールに移動します。
* 管理者ロールに移動します。
* 「新しいロールの作成」をクリックします。
* 役割にわかりやすい名前を付けます (例: 「ヘルプ デスク サポート」)。
* ヘルプ デスクに必要な権限 (パスワードのリセット、ユーザー アカウントの管理、デバイス情報の表示など) を慎重に選択します。
* ヘルプデスク管理者に役割を割り当てます。
他の選択肢が理想的でない理由:

* A. サービスデスク グループ: グループは主に組織向けであり、詳細な権限制御は提供しません。
* C. サービス管理者ロール: このロールには、ヘルプデスクに通常必要な権限よりも広範な権限があり、PoLP に違反しています。
* D. フル アクセス: 過剰な権限が付与され、偶発的または意図的な誤用のリスクが大幅に高まります。

最新問題**: 10**
組織のセキュリティプロトコルでは、無人デバイスがユーザーのログアウトを確実に行うようにすることが求められています。
24 時間。管理する ChromeOS デバイスが 1,000 台あります。管理の手間を最小限に抑えてこれを実装するにはどうすればよいでしょうか。
**A.** 「ユーザーとブラウザの設定」を有効にし、「最大ユーザーセッション時間*」を最大24時間に更新します。
**B.** 企業ポリシーを作成し、ユーザーはシフト終了後に手動でサインアウトする必要がある）
**C.** Chrome リモート デスクトップを使用して、各デバイスにリモートでアクセスし、ユーザー アカウントからログアウトできます。
**D.** 問題の各デバイスに、24時間後にデバイスからサインアウトする必要があることをユーザーに通知するカスタムアプリを強制的にインストールします。
**Answer: (**解答を表示する**)**
これは、管理コンソールで 1 回のポリシー変更を行うだけで、組織単位 (OU) 内のすべてのデバイスに設定が適用されるため、最も効率的な方法です。
他のオプションは効率が悪くなります。
* 企業ポリシー: ユーザーのコンプライアンスに依存しており、施行が困難です。
* Chrome リモート デスクトップ: デバイスごとに手動操作が必要です。
* カスタム アプリ: 複雑さが増し、セキュリティ リスクが増大します。
参考文献:
* 管理対象デバイスで Chrome ブラウザを設定します。
https://support.google.com/chrome/a/answer/3523633?hl=ja

最新問題**: 11**
管理対象のすべてのユーザー アカウントにプログレッシブ ウェブ アプリケーションを展開するにはどうすればよいでしょうか?
**A.** 「Chrome アプリと拡張機能」ページでプログレッシブ ウェブ アプリケーション URL を強制インストールします。
**B.** Chrome Imprivata 共有アプリと拡張機能を設定して、プログレッシブ ウェブ アプリケーション URL を強制的にインストールします。

**C.** 「ユーザーとブラウザの設定」に移動し、「レガシーブラウザのサポート」サイトリストにプログレッシブウェブアプリケーションのURLを追加します。
**D.** 「追加の Google サービス」を開いて、プログレッシブ ウェブ アプリケーション URL を強制的にインストールします。
**Answer: (**解答を表示する**)**
プログレッシブ ウェブ アプリケーション (PWA) をすべての管理対象ユーザー アカウントに導入するには、Google 管理コンソールで次の手順に従います。
* Google 管理コンソールにログインします。管理者の認証情報を使用してコンソールにアクセスします。
* デバイス管理に移動します。[デバイス] > [Chrome] > [設定] > [アプリと拡張機能] に移動します。
* ユーザーまたはグループの選択: PWA 展開を適用する最上位の組織単位または特定のグループを選択します。
* URL で追加: 黄色の 「+」アイコンをクリックし、「URL で追加」を選択します。
* PWA URL を入力: 展開する PWA の URL を貼り付けます。
* インストール ポリシーを構成する: 選択した範囲内のすべてのユーザーに PWA が自動的にインストールされるようにするには、「強制インストール」を選択します。
この方法により、組織全体で PWA を一元的に管理および展開できるため、ユーザーは ChromeOS デバイスで簡単にアクセスできるようになります。

最新問題**: 12**
セキュリティ部門は、従業員の車から ChromeOS デバイスが盗まれたという報告を受けました。
デバイスの管理を維持しながらデバイスが操作不能になるようにするには、管理コンソールで何をすればよいですか?
**A.** ChromeOS デバイスを盗難品としてタグ付けする
**B.** ChromeOSデバイスを無効にする
**C.** ChromeOS デバイスを Powerwash する
**D.** ChromeOS デバイスのプロビジョニングを解除します
**Answer: B (**メーッセージを残す**)**
管理コンソールで ChromeOS デバイスを無効にすると、デバイスの起動や使用が禁止され、実質的に操作不能になります。ただし、デバイスと組織の関連付けは保持されるため、管理者はデバイスの場所を追跡し、デバイスが回復した場合にリモートで管理することができます。
他のオプションはそれほど適切ではありません。
* 盗難品としてタグ付け: デバイスの使用を阻止しません。
* Powerwash: すべてのデータと登録を削除し、管理を不可能にします。
* プロビジョニング解除: デバイスの関連付けを削除し、管理を不可能にします。

最新問題: **13**
ChromeOS 管理者として、ChromeOS ブラウザでシークレット モードをブロックする役割を担っています。ユーザーがシークレット モードを使用できないようにするにはどうすればよいでしょうか。
**A.** 「ユーザーとブラウザのセキュリティ設定」に移動し、「シークレットモードを許可しない」ポリシーを設定します
**B.** 「ユーザーとブラウザの設定」に移動して、サインインをパターンに制限し、「シークレット モードを許可しない」
**C.** 「デバイス設定」からキオスク設定を「シークレットモードを許可しない」に変更します。
**D.** In 「登録設定」で、ベンダーアクセスとシークレットモード (またはコンテンツ保護) を無効にする
**Answer: A (**メッセージを残す**)**
* Google 管理コンソールにアクセスする: ChromeOS 管理者の認証情報を使用して管理コンソールにログインします。
* ユーザー設定を見つける: 「デバイス管理」> 「Chrome 管理」> 「ユーザーとブラウザの設定」に移動します。
* シークレット モード ポリシーを見つける: 設定内で、「シークレット モード」を検索します。
* シークレット モードを無効にする: 「シークレット モードを許可しない」オプションを選択します。
* 変更を保存: 「保存」をクリックすると、指定したユーザーまたは組織単位にポリシーが適用されます。
参考文献:
* 管理対象デバイスで Chrome ブラウザを設定します。
https://support.google.com/chrome/a/answer/3523633?hl=ja

最新問題: **14**
Chrome Enterprise の試用を設定するときに、ドメインの確認を選択することの利点は何ですか?
**A.** アイデンティティ管理
**B.** アプリケーション管理
**C.** ネットワーク管理
**D.** デバイス管理
**Answer: A (**メッセージを残す**)**
Chrome Enterprise の試用設定中にドメインを確認すると、Google のシステム内でドメインの所有権と管理権を確立します。これは ID 管理における重要なステップであり、次のことが可能になります。
* ユーザー アカウントの管理: ドメイン内でユーザー アカウントを作成、編集、削除し、会社のリソースにアクセスできるユーザーを制御します。

* セキュリティ ポリシーを適用する: ドメイン内のユーザーに対して、パスワード要件、2 要素認証、アクセス制御などのセキュリティ ポリシーを適用します。
* シングル サインオン (SSO): さまざまな Google サービスやその他の統合アプリケーションで、ユーザーがシームレスかつ安全にシングル サインオンを利用できるようにします。
ドメインを検証することで、ユーザー ID とリソースへのアクセスを集中的に制御できるようになります。これは、ID 管理の中核的な側面です。

最新問題**: 15**
教育機関や企業の IT 管理者にとって ChromeOS デバイスが人気のある選択肢となっているのは、どの管理機能によるものですか?
ChromeOS デバイスをエンタープライズ向けにする管理機能はどれですか?
**A.** オンプレミスのインフラストラクチャによる安全な管理
**B.** リモート BIOS コントロールとファームウェア更新
**C.** 管理コンソールによる集中管理
**D.** デバイスのリモート制御と監視ができない
**Answer: C (**メーッセージを残す**)**
ChromeOS 管理コンソールは集中管理が可能で、IT 管理者に人気の選択肢となっています。ポリシー、アプリ、拡張機能、デバイス設定を 1 つのインターフェースから管理できるため、管理が効率化され、デバイス間の一貫性が確保されます。
ChromeOS の管理はオンプレミスではなく、主にクラウドベースであるため、オプション A は正しくありません。
オプション B は、BIOS 制御が利用できる可能性はあるものの、主要な管理機能ではないため、正しくありません。
オプション D は不正解です。ChromeOS デバイスは管理コンソールからリモートで制御および監視できます。
参考文献:
* ChromeOS デバイス管理について:
https://support.google.com/chrome/a/answer/1289314?hl=en

最新問題**: 16**
サインイン画面でアイドル状態の間にデバイスがシャットダウンしないようにするポリシーを設定する必要があります。どこに移動すればよいですか?
**A.** ユーザー設定 > アイドル設定
**B.** ユーザー設定 > ユーザーエクスペリエンス
**C.** デバイス設定 > シャットダウンを許可する
**D.** デバイス設定 > 電源管理
**Answer: (**解答を表示する**)**

ChromeOS デバイスがサインイン画面でアイドル状態になっているときにシャットダウンしないようにするには、電源管理設定を調整する必要があります。これは次の手順で実行できます。
* Google 管理コンソールに移動します。
* [デバイス管理] > [Chrome 管理] > [デバイス設定] に移動します。
* 電源管理セクションを見つけて、サインイン画面でアイドル時の動作を制御する設定を見つけます。
* アイドル期間中のシャットダウンを防止するために設定を調整します。
オプション A は不正解です。アイドル設定は主に画面の暗さやスリープ動作を制御するためです。
オプション B は正しくありません。ユーザー エクスペリエンス設定は、通常、電源管理ではなく、視覚とインタラクションの側面に重点を置いているためです。
オプション C は、ChromeOS デバイス設定に特定の 「シャットダウンを許可する」設定がないため、正しくありません。



最新問題: **17**
ユーザーが SAML シングル サインオン経由で ChromeOS デバイスにログインし、認証情報を再入力せずに同じ ID プロバイダを利用するウェブサイトやクラウド サービスにアクセスできるようにしたいと考えています。SAML をどのように構成すればよいでしょうか。
**A.** Google 認証用の SAML ID プロバイダ初期化ログインを有効にする
**B.** ChromeOS デバイスで SAML ベースのシングル サインオンを有効にし、シングル サインオン Cookie の動作を設定して、ログイン時に SAML SSO Cookie をユーザー セッションに転送できるようにします。
**C.** Chrome アプリ管理を介して各アプリケーションに対して SAML ベースのシングル サインオンを有効にする
**D.** Chrome App Builder を使用してアプリケーションの SSO を有効にし、ChromeOS ユーザー ポリシーを使用してアプリケーションを強制的にインストールします。
**Answer:** (解答を表示する)

同じ ID プロバイダを使用して ChromeOS デバイスと他のウェブ サービス間でシームレスな SSO を実現するには、Google 管理コンソールで SAML SSO を設定する必要があります。
* ChromeOS デバイスで SAML ベースの SSO を有効にします。
* SSO 設定で、シングル サインオン Cookie の動作を見つけて、「ログイン中に SAML SSO Cookie をユーザー セッションに転送できるようにする」に設定します。これにより、SAML 認証 Cookie を ChromeOS ログインと他の Web サービス間で渡すことができるようになり、再認証が不要になります。
オプション A は、後続の SSO の Cookie 転送ではなく、最初のログイン方法に関連しているため、正しくありません。
オプション C と D は、デバイスの一般的な SAML SSO 設定ではなく、アプリケーション固有の SSO 構成に関係するため、正しくありません。

最新問題: **18**
通常のユーザーモードでは、管理者は ChromeOS デバイスで crosh シェルを開いて ping コマンドを実行するにはどうすればよいでしょうか?
**A.** Ctrl + Alt + V
**B.** Ctrl + Alt + t
**C.** Ctrl + Alt + Tab + W
**D.** Ctrl + Alt + i
**Answer: (**解答を表示する**)**
ChromeOS デバイスの通常のユーザー モードで Ctrl + Alt + t を押すと、コマンド ライン インターフェースである crosh シェル (Chrome OS 開発者シェル) が開きます。そこから、ネットワーク接続をテストするための ping など、さまざまなコマンドを実行できます。
その他のオプションは、割り当てられた機能がないか、ChromeOS で異なるアクションをトリガーするため、正しくありません。

最新問題: **19**
組織で Verified Access を使用するには、クライアント デバイスで Verified Access API を呼び出す Chrome 拡張機能が必要です。この拡張機能はどこで入手できますか?
**A.** Google Play ストア
**B.** 独立系ソフトウェアベンダー (ISV) または Google Verified Access API
**C.** 独立系ソフトウェアベンダー (ISV) リポジトリ
**D.** ソフトウェア API キー ストア
**Answer: B (**メーッセージを残す**)**
Verified Access には、Verified Access API と通信するための Chrome 拡張機能が必要です。Google はこの拡張機能を直接提供していませんが、Verified Access API を通じて詳細なドキュメントとリソースを提供しています。独立系ソフトウェア ベンダー (ISV) は、これらのリソースを使用して互換性のある拡張機能を開発し、提供できます。

オプション A は不正解です。Google Play ストアは Android アプリ用であり、Chrome 拡張機能用ではありません。
オプション C は不正解です。ISV が拡張機能を提供している可能性はありますが、それが唯一のソースではありません。Google のドキュメントが不可欠です。
オプション D は不正解です。API キーは拡張機能自体ではなく認証用です。

最新問題**: 20**
管理者は、カスタム拡張機能を使用して ChromeOS デバイスにクライアント証明書をインストールし、企業の Wi-Fi に接続できるようにしたいと考えています。
これを達成するにはどのステップが必要ですか?
**A.** ゲストモードでデバイスにインストールする
**B.** Chrome ウェブストアを通じて配布する
**C.** デバイスに強制インストール
**D.** 証明書をDERエンコード形式でエンコードします
**Answer: C (**メーッセージを残す**)**
企業の Wi-Fi 接続用に ChromeOS デバイスにクライアント証明書をインストールするには、証明書を含むカスタム拡張機能を強制的にインストールする必要があります。これにより、拡張機能がデバイスにインストールされ、アクティブ化され、認証に証明書を使用できるようになります。仕組みは次のとおりです。
* カスタム拡張機能: 管理者は、クライアント証明書を含むカスタム拡張機能を作成または取得します。
* 強制インストール: 管理者は Google 管理コンソールを使用して、組織内の ChromeOS デバイスに拡張機能を強制インストールするポリシーを設定します。
* デバイスのアクティベーション: デバイスがポリシーを受信すると、ユーザーが手動で追加しなくても、拡張機能は自動的にインストールされ、アクティベートされます。
* Wi-Fi 認証: インストールされた拡張機能により、デバイスは企業の Wi-Fi ネットワークに接続するときに認証にクライアント証明書を使用できるようになります。
オプション A は正しくありません。ゲスト モードのインストールは永続的ではなく、デバイスの Wi-Fi 設定に証明書が適用されません。
オプション B は不正解です。社内使用を目的としたカスタム拡張機能の場合、Chrome ウェブストアを通じて配布する必要はないからです。
オプション D は不正解です。証明書のエンコードは重要ですが、Wi-Fi 認証を有効にするための主な手順ではないためです。
参考文献:
* ChromeOSデバイス管理について:
https://support.google.com/chrome/a/answer/1289314?hl=en pen_spark

**Valid ChromeOS-Administrator Dumps** shared by GoShiken.com for Helping Passing ChromeOS-Administrator Exam! GoShiken.com now offer the **newest ChromeOS-Administrator exam dumps**, the GoShiken.com ChromeOS-Administrator exam **questions have been updated** and **answers have been corrected** get the **newest** GoShiken.com ChromeOS-Administrator dumps with Test Engine here: https://www.goshiken.com/Google/ChromeOS-Administrator-mondaishu.html (**118** Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)