这里整理工作中可能被会问到的一些安全相关的问题：

1.クライアント先のゲストLANに接続する際に、セキュリティの留意事項がありますか

Note 下記の点を確認する必要があります。 ゲストLANの暗号化方式と認証方式は？（認証なしのゲストLANは非推薦） 他社の方も同ゲストLANを利用しますか。その場合は、横展開などリスクを含めて、ゲストLANの制御方式は？

標準外の会議ツール（例えばZoom）の利用に関する注意事項を教えてください。

Note 標準外の会議ツールはIT部門のサポート対象外なので、事前に想定されるセキュリティリスクに対する対策を講じることが必要です。

- 必ず最新版のZoom（Zoom Meeting、Zoom webinarなど）を利用すること。
- 会議のURLやID/PWなどを参加者以外の方に共有しないこと。
- 会議中ファイル共有機能を利用しないこと。
- やむを得ない場合（クライアントの要求など）を除く、秘密情報を話す、画面共有することをしない。
- 必要がない場合は、常にカメラOFFしてください。
- 自分の名前のみ表示、組織名は入力しない。
- 主催者としてZoomの有料版を購入した上、ご利用ください。
- Zoomアカウントは必ず会社のメールアドレスで作成します。

From:
https://trident365.com/ - 三叉戟

Permanent link:
https://trident365.com/doku.php?id=resources:faq&rev=1731765158

Last update: **2024/11/16 22:52**