



Mass × SecurityTool

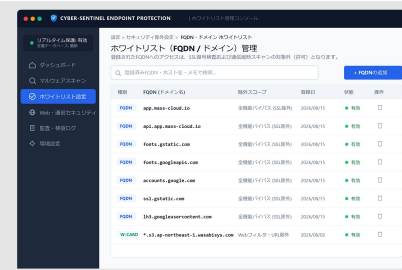
Mass
on the cloud platform

セキュリティツールでの設定ポイント

ネットワークでは、ファイアウォールやWebフィルタリング、EDRなどのセキュリティツールによって、通信が制限される場合があります。

「ブラウザではMassを開けるのに、Mass Desktopではアップロードやダウンロードができない」といった場合も含め、今回はMassが利用する通信先やアプリケーションがブロックされないための設定項目をご紹介します。

ホワイトリストにFQDNを登録



※一般的なセキュリティソフトのイメージ画像です。

【STEP1】 Massの通信先を許可する

Massが通信に利用する各FQDNに対し、HTTPS通信（TCP/443）を許可リスト（ホワイトリスト）に登録してください。

●Massアプリ

app.mass-cloud.io

api.app.mass-cloud.io

*.s3.ap-northeast-1.wasabisys.com

※プロジェクト毎にURLが異なりますので、先頭ワイルドカードの指定が推奨です。

fonts.gstatic.com

fonts.googleapis.com

accounts.google.com

ssl.gstatic.com

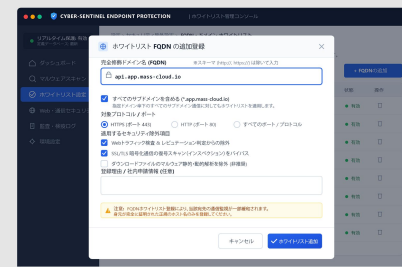
lh3.googleusercontent.com

●オンラインヘルプ

slite.com

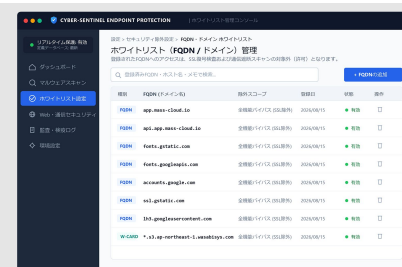
visual-graphics-inc.slite.page/p/oVSC7soOsZSAg2/Mass-cloud-io-media-assets-on-the-cloud

HTTPS（ポート443）の選択とSSLインスペクションをバイパスに設定



※一般的なセキュリティソフトのイメージ画像です。

SSLインスペクションがバイパスになっているのを確認



※一般的なセキュリティソフトのイメージ画像です。

【STEP2】 SSLインスペクションを確認する

通信先を許可していても、SSLインスペクションによってHTTPS通信が復号されることで、Mass Desktopの通信が正常に行えない場合があります。

FQDNを許可しても改善しない場合は、Mass関連の通信をSSLインスペクションの対象外（バイパス）にできないか、ネットワーク管理者へ確認してください。

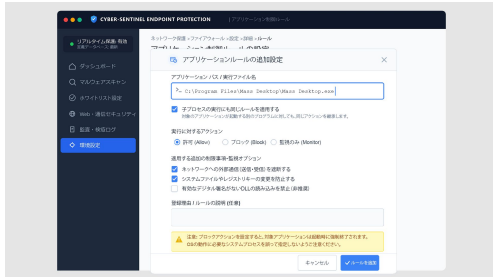


Mass × SecurityTool

Mass
on the cloud platform

セキュリティツールでの設定ポイント

アプリケーション制御の確認 「許可」



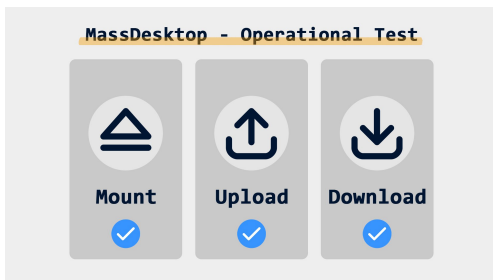
※一般的なセキュリティソフトのイメージ画像です。

【STEP3】 Mass Desktopがブロックされていないか

セキュリティツールによっては、通信先だけでなくアプリケーション単位で通信を制御しています。その場合、Mass Desktopが「未確認アプリケーションなど」として判定され、通信を遮断されることがあります。

MassBrowserは使えるが、Mass Desktopだけ使えない、という場合は、アプリケーション制御やEDRの設定も確認してみましょう。

MassDesktop の 動作テスト



【STEP4】 Mass Desktopの動作テスト

設定変更後は、Mass Desktopが起動するだけでなく、

- Massをマウントできる
- アップロードできる
- ダウンロードできる

ところまで確認します。

セキュリティツールを一時的に停止すると正常に動作する場合は、そのツールの通信制御が原因となっている可能性があります。

まとめ



Mass Desktopが正常に動作しない場合、原因がMassそのものではなく、企業ネットワーク側のセキュリティ設定にあることがあります。

FQDNの許可、HTTPS通信、SSLインスペクション、アプリケーション制御の4点を中心に確認すると、原因を切り分けやすくなります。

Mass導入時にあらかじめこれらを確認しておくことで、アップロードやダウンロード時のトラブルを減らすことができます。