社内プロセス記録(作成例)

セキュリティ監査 実施プロセス記録

― 通信ログ監査における確認手順のご紹介 ―

対象期間: 2026 年 6 月 1 日 〜 6 月 30 日(月次)

作成日: 2026 年 7 月 1 日

株式会社サンプル商事

この記録の目的

本記録は、月次のネットワークセキュリティ監査において、当社が実際にどのような視点・プロセスで通信データを確認しているかをご紹介する社内プロセスの記録(作成例)です。クライアントへの報告書とは別に、確認の経緯や着眼点を残すことで、監査プロセス自体の妥当性を継続的に検証できるようにしています。

※ 具体的な判定式・しきい値・集計単位等、手法の詳細部分は、監査の実効性を保つ観点から本資料では公開しておりません。

確認プロセス A:通信の出現頻度に着目した確認

宛先ごとの通信の組み合わせを集計し、出現回数が極端に少ない、いわば「珍しい」通信の有無を確認しました。低速・少量型の通信で確認をすり抜けようとするパターンは、この「珍しさ」に現れやすいと考えられています。

区分	確認件数	評価
出現頻度が低い宛先(判明分)	十数件	いずれも一般的なクラウド・配信サービス向けで異常なし
事務所内の低頻度な通信	数件	機器の標準的な自動動作の範囲内

サービス/ポート	出現回数	宛先組織(判明分)	評価
[illegible]	1	[illegible]	既知カテゴリ、異常なし
[illegible]	1	[illegible]	通常の ping 疎通確認、異常なし
[illegible]	2	[illegible]	既知カテゴリ、異常なし
[illegible]	5	[illegible]	通常の NAT 越え通信、異常なし
[illegible]	6	[illegible]	既知カテゴリ、異常なし
[illegible]	6	[illegible]	用途不明・少量データのみ。要記録
[illegible]	8	[illegible]	既知の公開サービス、異常なし
[illegible]	9	[illegible]	FortiGate 自体のシグネチャ更新関連、異常なし
[illegible]	10	[illegible]	アプリのテレメトリ送信と推定、少量。要記録
[illegible]	13	[illegible]	既知カテゴリ、異常なし
[illegible]	16	[illegible]	既知カテゴリ、異常なし
[illegible]	25	[illegible]	既知カテゴリ、異常なし
[illegible]	29	[illegible]	既知カテゴリ、異常なし

出現頻度が低い通信は、いずれも広く利用されているクラウドサービスや配信サービス向けであることを確認しており、未知の相手先への通信は見つかりませんでした。

確認プロセス B:接続間隔の規則性に着目した確認

同一の送信元・宛先の組み合わせについて、接続が発生する時間的な間隔の規則性を統計的に確認しました。人間の操作によらない、機械的に一定間隔で行われる通信は、外部からの遠隔操作を受けている兆候となり得るため、重点的に確認している観点です。

サービス/ポート	出現回数	内容
[illegible]	3	マルチキャストグループ管理(通常のネットワーク動作)
[illegible]	50	Windows 名前解決関連(通常のネットワーク動作)
[illegible]	102	同一セグメント内 [illegible] n 検出(周辺機器の自動探索)
[illegible]	303	IP アドレス自動割り当て(通常のネットワーク動作)

判定: 規則的な通信の兆候なし

定めた基準に該当する組み合わせは 1 件もありませんでした。間隔にばらつきのある上位の組み合わせも、いずれも著名なクラウドサービス向けで、通常のアプリ同期・確認動作の範囲と判断されます。

確認プロセス C:複数日にわたる継続アクセスの確認

同一の送信元・宛先の組み合わせが、対象期間中の複数日にまたがって継続的にアクセスしているケースを抽出しました。

宛先 IP	宛先組織	継続日数	セッション数
		4 日	43,287
		4 日	8,148
		4 日	3,837
		4 日	3,137
		4 日	2,382
		4 日	1,807
		4 日	各 1,700 台
		4 日	各 900 台

判定: 異常なし

継続日数が多い宛先は、いずれも契約回線の名前解決サーバーや、業務利用の裾野が広い著名なクラウド・SaaS 事業者で構成されており、常時接続の性質を持つ正当な業務通信と判断されます。特定の未知の相手先への継続アクセスは確認されませんでした。

確認プロセス D:通信タイミングの分布確認

インターネット向け通信のデータ量を時間帯別に集計し、通常想定しにくい時間帯(深夜・早朝)に発生した、まとまったデータ量の通信を個別に確認しました。

データ量は日中の業務時間帯を中心とした典型的な分布であり、深夜・早朝帯の通信量は日中のピーク時と比べて明らかに少なく、全体傾向として深夜帯の突出はありませんでした。深夜・早朝帯に発生した個別の通信についても、その大部分は一般的なコンテンツ配信サービス等向けの小規模なものであることを確認しています。

日付	時刻	宛先 IP	宛先組織	サービス	受信量(概算)
[redacted]	[redacted]	[redacted]	[redacted]	HTTPS	約 373MB
[redacted]	[redacted]	[redacted]	[redacted]	udp/443	約 4.3MB
[redacted]	[redacted]	[redacted]	[redacted]	HTTPS	約 1.3MB
[redacted]	[redacted]	[redacted]	[redacted]	HTTPS	約 1.1MB
[redacted]	[redacted]	[redacted]	[redacted]	HTTPS	約 1.1MB
[redacted]	[redacted]	[redacted]	[redacted]	HTTPS	約 1.1MB
[redacted]	[redacted]	[redacted]	[redacted]	HTTPS	約 1.1MB
[redacted]	[redacted]	[redacted]	[redacted]	HTTPS/udp443	各約 0.5? 1MB

確認プロセス E:着眼点チェックリストとの照合

外部通信の異常検知に関する一般的な着眼点をリスト化し、今回の記録範囲で確認可能な項目について照合を行いました。記録範囲の制約により、一部の着眼点(通信内容の詳細に基づくもの)は今回は評価対象外としています。評価できた項目については、いずれも重大な異常は確認されませんでした。

確認プロセス F:データ量基準による参照確認

持続的な大容量通信のしきい値監視については、別途作成している技術資料(通信データの集計表)で全期間・全通信を対象に確認済みのため、本記録では新たな集計は行わず、既存の確認結果を参照する形としています。

まとめ

今回の確認結果の総括

・接続間隔の規則性・複数日にわたる継続アクセス・出現頻度のいずれの観点においても、侵害や不正な遠隔操作を示す明確な兆候は確認されませんでした。

・着眼点チェックリストのうち、通信内容の詳細情報を要する一部の項目は、現在の記録範囲では評価対象外としました。

・名前解決先の集中度についても、記録されている範囲内では異常は確認されませんでした。

記録範囲の拡張についての検討事項

ご確認いただきたい点: 記録範囲の拡張について

今回の確認を通じて、一部の着眼点(通信内容の詳細に基づくもの)が、現在の記録設定では評価できないことが分かりました。追加の記録設定を有効化することで、より広い範囲の確認が可能になります。実施のご要否は別途ご相談のうえ判断いたします。