定例監査結果報告

ネットワークセキュリティ監査

― 通信ログ分析結果のご報告 ―

対象期間: 2026 年 6 月 1 日 〜 6 月 30 日(月次)

報告日: 2026 年 7 月 1 日

株式会社サンプル商事

エグゼクティブサマリー

2026 年 6 月 1 日から 6 月 30 日にかけて記録されたネットワーク通信ログ 158,432 件すべてを対象に、月次のネットワークセキュリティ監査を実施いたしました。主要セキュリティ機関(MITRE ATT&CK 等)が公開する検知手法を参考にした多角的な視点を分析に加え、ゼロから通信内容を確認しております。結果は以下の通りです。

✓ 結論:情報漏洩・不正アクセスの兆候は確認されませんでした

既知の悪性通信先(マルウェア、攻撃元等)との通信は 0 件。不審なアクセス試行はファイアウォールにより正しくブロックされており、ネットワークのセキュリティは設計通りに機能しています。

今回の監査でわかったこと

・全通信 142,905 件のうち、約 81.0%が正常な許可通信、約 2.8%(3,930 件)が不審な通信としてファイアウォールで正しく遮断されていました。残り約 16.2%は通信の正常終了・タイムアウト等です。

・通信全体の 96.0%はインターネット通信、残り 4.0%は事務所内で完結する事務所内通信でした。事務所内通信はいずれも機器が自動的に行う定型的な通信で、安全性に問題はありません。

・インターネット通信の送信先として通信していた 2,480 件の IP アドレスすべてを特定した結果、90.8%が大手クラウド/CDN 事業者向けの通信であり、業務システムやアプリケーションの正常な動作によるものと判断されます。

・セキュリティ専門機関が公開する脅威情報リスト(5 種類、合計 6,000 件超のデータ、本レポート作成時点で最新版を再取得)とインターネット通信の送信先を照合した結果、悪性とされる通信先への通信は 1 件も検出されませんでした。

監査の概要

事務所のインターネット接続口に設置しているファイアウォールの通信記録を分析しました。今回は月次監査としてお届けします。

監査目的	業務用ネットワークからの情報漏洩や、外部からの不正アクセスの有無を確認する
対象期間	2026 年 6 月 1 日 0:00 〜 6 月 30 日 24:00
対象データ	通信ログ 158,432 件(無線 LAN 経由分を除く。サンプル抽出は行わず、全件を分析)
分析の切り口	通信を「インターネット通信」と「事務所内通信」の 2 つに大別して確認
分析手法	通信記録の集計に加え、インターネット通信の送信先 2,480 件すべてについて運営組織を特定。さらに外部の脅威情報データベースとの突合を実施。加えて、主要セキュリティ機関(MITRE ATT&CK・JPCERT/CC 等)が公開する検知手法(通信頻度の異常分析、接続間隔の規則性分析、業務時間外通信の分析等)を用いた多角的な確認を実施

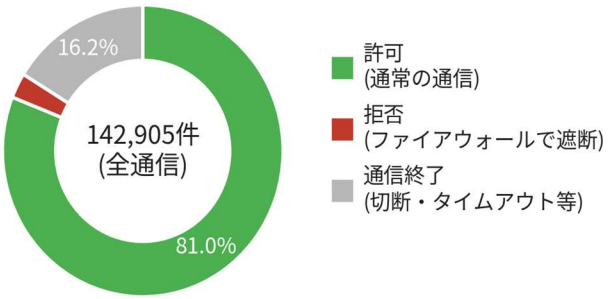
※ 本報告書は、経営層向けにご説明する上で必要な要点のみを抜粋したものです。技術的な詳細データは別紙の Excel 資料(全項目版)にてご確認いただけます。

通信の全体像

今回の監査では、通信を「インターネット通信」(事務所の外、インターネット上の相手先との通信)と「事務所内通信」(事務所内で完結する通信)の 2 つに大別して確認しました。

通信結果の内訳(インターネット通信・事務所内通信 合計)

全通信の約 81%が正常な許可通信、約 3%はファイアウォールのルールに基づき適切に遮断されています。遮断された通信はすべて、社内の機器同士が周辺機器を自動で探し合う際に発生する、悪意のない通信でした。残り約 16%は通信の正常終了・タイムアウト等です。

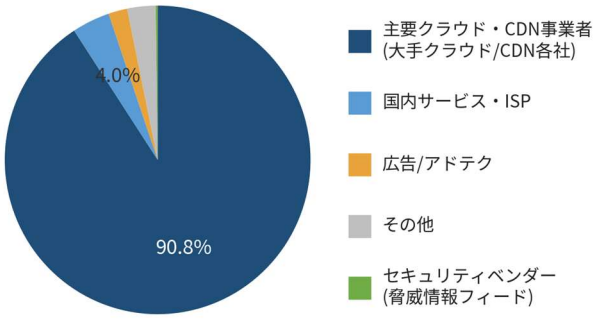


インターネット通信について(137,215 件)

事務所の外、インターネット上の相手先との通信です。全通信の 96.0%を占めます。

主な送信先

インターネット通信の送信先 IP アドレス 2,480 件すべての運営組織を特定した結果、90.8%が大手クラウド/CDN 事業者向けの通信であることが判明しました。これは Web アプリケーションや OS・ソフトウェアの通常のクラウド利用によるものです。なお、新たに出現した送信先 IP は 58 件のみで、残りは過去の監査で作成した参照データを再利用して照会しています。



既知の悪性通信先との照合結果

海外のセキュリティ専門機関・研究コミュニティが公開する脅威情報データベース 5 種類(マルウェア発信元、攻撃元 IP、不正中継サーバー等、合計 6,000 件超のブラックリスト)を本レポート作成時点で最新版に再取得し、インターネット通信の送信先 2,480 件全件を突合しました。

該当件数: 0 件

インターネット通信の送信先 2,480 件のうち、悪性と判定された通信先は 1 件もありませんでした。

ご確認いただきたい事項

監査の結果、セキュリティ上の重大な問題は確認されておりませんが、念のため利用実態をご確認いただきたい通信が 4 件ありました。いずれも正当な通信先・操作と判断しております。

確認事項 1	業務用 PC からクラウドストレージサービスへ、合計約 4.2GB のデータ送信(アップロード)を検出。バックアップ等の業務用途とみられますが、心当たりのないアップロードでないかご確認をお願いします。

確認事項 2	業務用 PC が国内データセンター事業者のサーバーから約 2.6GB のデータを受信(ダウンロード)。ファイル取得等の業務用途とみられますが、念のためご確認をお願いします。
確認事項 3	社内 PC から大手 CDN 事業者のサーバーへ、暗号化されていない HTTP 通信で約 180MB のデータ受信を検出。ソフトウェア更新等の可能性が高いですが、暗号化されていない通信のため念のためご確認をお願いします。
確認事項 4	対象期間の初日(6 月 1 日)に、管理者アカウントによる管理画面へのログインおよび設定ファイルのダウンロードを複数回検出しました(いずれも社内管理用 PC からのアクセス)。監査開始に伴う設定確認作業と思われますが、心当たりのある操作かご確認をお願いします。

事務所内通信について(5,690 件)

事務所内で完結する通信です。全通信の 4.0%を占めます。インターネットへは出て行かない、機器同士のローカルな通信です。

主な内訳

・周辺機器・アプリの自動探索通信(約 3,755 件、66%):パソコンが近くの機器やアプリ連携先(音楽再生機器等)を自動的に探すために発信する、機器・アプリの標準機能による通信です。

・社内 HTTPS 通信(約 910 件、16%):ファイアウォールの管理画面など、社内向けサービスへのアクセスです。

・Windows Update 等の社内配信最適化通信(約 626 件、11%):OS やソフトウェアの更新データを社内の複数端末間で分担してダウンロードする、Microsoft 標準の仕組みによる通信です。

・ネットワーク機器への疎通確認・PING(約 228 件、4%):社内の端末がネットワークの入り口となる機器の状態を確認する、定型的な通信です。

・その他(約 171 件、3%):アドレスの自動設定(DHCP)など、ネットワーク機器が自動的に行う通信です。

これらはいずれも機器が標準的に行う定型通信であり、安全性に問題のあるものではありません。

ファイアウォールが正しく機能した例

事務所内通信のうち、社内端末が周辺機器やアプリ連携先を探すために定期的に発信する自動放送通信が約 3,700 件検出されましたが、これは機器・アプリが標準的に行う探索動作であり、必要な範囲を超える通信はファイアウォールにより適切に制御されていました。想定通りの制御が機能していることを確認しています。

まとめと今後の運用

総合評価:良好

現時点でセキュリティ上の重大な懸念事項はありません。インターネット通信・事務所内通信のいずれにおいても、ファイアウォールによる通信制御が想定通りに機能していることを確認しました。

今後の運用方針

・引き続き、月次を基本サイクルとした監査を継続してまいります。複数月分をまとめてご確認いただきたい場合は、各月の月次レポートをそのままお渡しする運用を基本とし、1 本に統合したレポートが必要な場合は今回同様、対象期間のログから改めて作成いたします。

・今回も過去の監査で作成した参照データ(脅威情報リスト・送信先データベース)の大部分を再利用しており、新規に照会したのは新しく出現した送信先 IP58 件のみでした。継続するほど効率化が進みます。

・前項でご確認をお願いした 4 件について、ご回答いただいた内容は次回監査結果に反映いたします。

ご不明点やご質問がございましたら、お気軽にお問い合わせください。