kaspersky

既知の悪性インフラを通信前に遮断する

NGFWと連携する脅威インテリジェンス活用



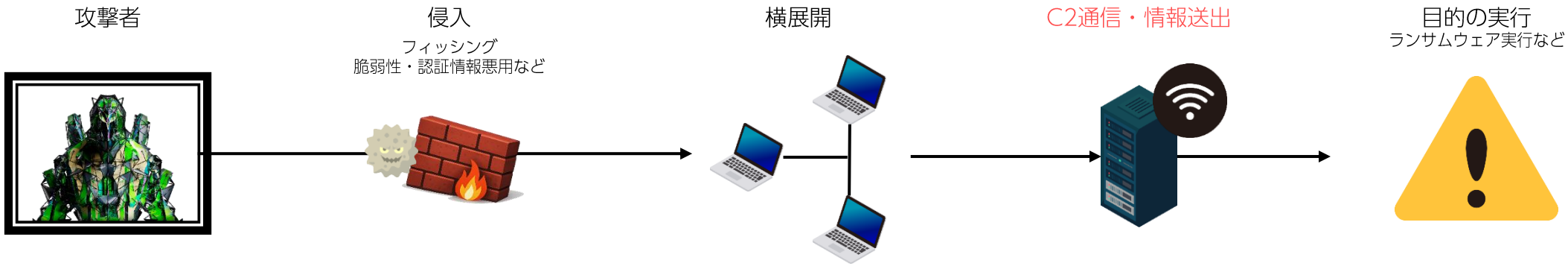
攻撃者は検知を回避するためにクラウドインフラを悪用し、短期間でドメインを大量生成するのが常套手段となり、自社で最新の脅威情報を調査し続けるのは困難です。限られたコスト（人・モノ・予算）で、必要とされるのは既存NGFWが持つ遮断機能を最新の脅威情報で継続的に強化可能な脅威インテリジェンスへの投資です。

- NGFW向けに最適化された脅威データフィード
- SIEM無しでも簡単に脅威インテリジェンスを活用
- NGFWを補完して脅威情報の網羅性を高める
- 最短10分で設定完了

01 現在のサイバー攻撃の特徴・脅威インテリジェンスの必要性

kaspersky

- 攻撃の侵入成功率が高まり、侵入後の横展開・C2通信などの活動が活発化
  さらに攻撃の無害化・ステルス化が進み、従来のシグネチャ型対策では、被害拡大前に防ぐことが難しい
- クラウドインフラ悪用による攻撃インフラの高速な変化



■ 課題

- 短期間で変化する悪性ドメインへの対策ができていない
- 脅威インテリジェンスを検討しているが、自社環境での活用方法が分からない
- 既存NGFWの活用を検討しているものの、どうやって脅威情報を調査すればいいのか分からない

追加マルウェア取得や情報窃取・遠隔操作の起点となる
C2通信を検知・遮断することが重要です。

Copyright © 2026 Kaspersky Lab. All rights reserved.

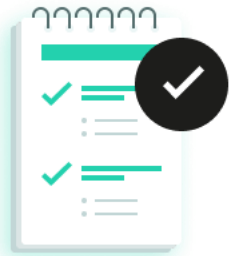
02 Kaspersky Network Security Data Feedsで解決できる4つのこと

kaspersky

- Kaspersky Network Security Data Feedsは既存NGFWの検知力を強化し、
  高確率で発生する攻撃インフラへの通信をブロックすることで、攻撃の進行を阻止

01 NGFW向けに最適された脅威データフィード

- 脅威データフィードのコンテキスト部分をあえて削除し、検知に必要な悪意のあるIPアドレス・URLのみ提供
- 本来脅威データフィード導入時に必要なチューニング、検知ロジックへの変換が不要
- 検知した脅威の詳細を確認したい場合、Kaspeskyの別サービス「Threat Lookup」で検索可能



02 脅威の最新情報を高頻度・継続的に更新

- 短期間で変化する攻撃に対抗するため、Kasperskyが発見した最新の脅威情報を高頻度で反映

■ 更新頻度

・IPアドレス：20分
・悪意のあるURL・フィッシングURL：20分
・ボットネットC2：60分



03 脅威の網羅性を高める

- 既存NGFWとKasperskyを組み合わせることで、ベンダーによるセンサー・地域性・分析対象の違いによって起こる偏りを防ぎ、セキュリティ上の死角を減らす



04 最短10分で設定完了

- 既存NGFWへの配信用URLとAPIトークン登録のみ、最短10分で設定完了
- 追加のハードウェア購入・既存NGFWへのエージェントのインストールは不要

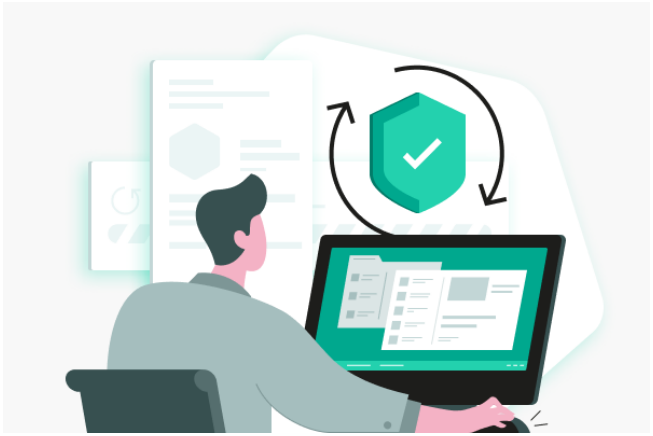


Copyright © 2026 Kaspersky Lab. All rights reserved.

Kaspersky Network Security Data Feeds：チェックリスト

以下のチェックリストで現在の状況を振り返りましょう。

チェック項目	はい	いいえ
既存NGFWを活用して防御力を高めたい	☐	☐
担当者の調査・判断不要で悪意のある通信を遮断したい	☐	☐
NGFWのブロックリストを手動で更新する運用を減らしたい	☐	☐
既存環境に追加のエージェントを入れずに防御力を高めたい	☐	☐
自社だけでは把握しにくい海外の脅威情報も活用したい	☐	☐



1つでも当てはまる場合、
脅威インテリジェンスの
自動連携が有効です。



詳しいご説明・デモ・検証のご相談はこちら

株式会社カスペルスキー　セールス営業本部　jp-sales@kaspersky.com