導入しただけでは不完全。適切な運用が大事です。

今対策すべきUTM運用の見直し

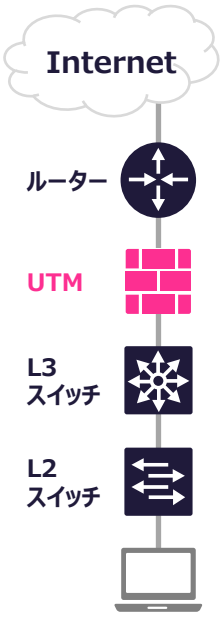
「企業のセキュリティ強化の一環として UTM (Unified Threat Management：統合脅威管理) を導入したけれど、機能を活用できていない」というお客様の声をよくお聞きします。



ファイアウォールと VPN 機能しか使えていない…。

よく分からなくて購入時のデフォルト設定のまま…。





多彩な機能を持つ UTM。
導入後、有効に活用していくにはどのようなステップが必要なのでしょうか？

① 脆弱性対応
- 定期的な脆弱性情報の収集
- 影響範囲の特定と対策
- 最新の脅威への対応

② SSL インスペクションの活用
- セキュリティ検査トラフィックの適正化
- UTM 機能の有効活用
- 暗号化通信の可視化

③ ログ分析・解析の実施
- 内部・外部における脅威の把握
- 脅威の発生傾向把握
- 検知後の動作アクションの評価
- 認証失敗等のエラーログ

④セキュリティポリシーの見直し
- 定期的なセキュリティポリシーの見直し
- 適切なアクセス制御
- 外部脅威からの防御

脆弱性対応

機器を導入後、ファームウェアのアップデートが実施されないまま放置されると、機器の脆弱性を悪用されて不正アクセスやランサムウェアによる攻撃を受ける危険性があります。

社内・社外のネットワークを分離し、境界防御を行っている UTM の脆弱性を悪用されると？
社内にある情報資産が外部に漏洩し、企業の信用問題に関わる深刻なトラブルに繋がります。
絶えず登場する脆弱性を放置せず、適切な措置を取ることが、UTM 運用の第一歩です。

参考）FortiGate 製品の脆弱性発表回数
FortiGate は世界中のファイアウォールの全出荷台数の 3 分の 1 以上を占め、世界シェア No.1 を獲得しています。利用者が多いということは攻撃者にも狙われやすいということです。実際に、報告される脆弱性の件数は増加しており、広く注意喚起されるような重大な脆弱性も多く発見されているため、早急な対策が必要です。

	2021	2022	2023	2024（想定）
Critical	0	2	3	9
High	5	6	12	9
Medium	10	13	27	15

IBC なら

IBC Care サービス を利用することで、
・脆弱性情報の公開～パッチ適用まで迅速な対応が可能！
・セキュリティインシデント発生リスクを最小限に！

▲資料DL

SSL インスペクション機能の活用

盗聴や改ざんといった被害から通信内容を守るため、SSL / TLS の暗号化技術を用いた HTTPS 通信が一般化しました。現在、全インターネットトラフィックの 90% は HTTPS 通信です。
しかし HTTPS 通信には「不正通信も暗号化して隠してしまう」という弱点があります。

UTM の SSL インスペクション機能を使用すると？

メリット： 暗号化された通信の中身を、UTM で**復号→データチェック→再暗号化**することができます。また、アンチウィルスソフトや IPS / IDS では検知できない暗号化された不正通信を発見し、ブロックすることで、第三者による改ざんやなりすましを防ぎ、企業の信頼を守ることができます。

デメリット： 機能を利用することで少なからず機器に負担が増えます。機能を有効にする前にサイジングを実施する必要がありますが、適切なサイジングを行うにはノウハウが必要です。

IBC なら

IBC-Integration のサービスを利用することで、
・各社の規模に合わせて、システム性能や容量を適切にサイジング！
→SSL インスペクション機能を利用しても、UTM 機器への負担を最小限に！

▲資料DL

ログ分析・解析の実施

UTM 機器が出力するログデータは、トラフィック傾向の把握だけでなく、サイバー攻撃や不正な通信の把握にも活用することができます。

UTM 機器のログを分析・解析を実施すると？

メリット： 自社がどんな攻撃にさらされやすいのか、脅威の検知状況を可視化でき、今後の対策を検討できます。

デメリット： 膨大な量のログを解析するために、多くの時間とスキルが必要になります。

IBC なら

IBC-SAS のログ解析サービスを利用することで、
・膨大なログの解析に必要な**時間**と**スキル**は IBC にすべてお任せ！
・IBC ならではのログ解析レポートで現状の課題を把握し、対処方法もご提案！

▲資料DL

UTM 運用を見直し、セキュリティを強化しませんか？

IBC Care
障害時の切り分け支援・脆弱性情報の提供・パッチ適用サービスをワンストップで提供

IBC-Integration
ネットワーク / サーバーインフラの新規導入の際のお悩みを一気通貫でサポート

IBC-SAS
診断から保護まで、企業のセキュリティ課題に応じたソリューションをワンストップで提供

IT 障害 119 レスキュー
IT インフラ全体を考慮した技術支援、よろず相談窓口を提供

IBC
アイビーシー株式会社

本社 〒104-0033
東京都中央区新川1-8-8 アクロス新川ビル8F
tel.03-5117-2780 fax.03-5117-2781

西日本事業所 〒532-0004
大阪府大阪市淀川区西宮原2-7-38 新大阪西浦ビル3F
tel.06-7653-1014 fax.06-7177-0542