

— AI・脆弱性対策を含め、実際のリスクと効果を重視する —

1. はじめに

近年、AIの発達により、セキュリティホールや異常通信などを大量かつ高速に検出できるようになりました。

これはセキュリティ対策にとって大きな進歩です。

一方で、**検出できる問題が増えることと、実際のセキュリティリスクが増えることは同じではありません。**

セキュリティ対策は、技術的に考えられるすべての危険に対応するのではなく、実際の環境におけるリスクと対策効果を判断して進めることが重要です。

2. ネットワークセキュリティの基本

当社が考えるネットワークセキュリティの基本は、次の4点です。

- ① 不正侵入をさせない。
- ② 侵入されても通過させない。
- ③ 不正な通信を成立させない。
- ④ 被害を拡大させない。

外部からの不正アクセスを防止することを基本とし、万一ウイルスやマルウェア等によって端末が侵害された場合にも、外部の攻撃者との不正な通信を成立させず、被害を拡大させないことが重要です。

また、攻撃方法は変化するため、監視と必要な対策の更新は継続して行う必要があります。

3. セキュリティホールについて

セキュリティホールが存在すること自体が、不正侵入や情報漏洩・改ざんを意味するものではありません。

セキュリティホールは、**不正侵入が成立した場合などに攻撃者から利用され、その結果として情報漏洩や改ざんにつながる可能性があるもの**と考えるべきです。

したがって、セキュリティホールが発見された場合には、

- 実際に攻撃に利用できるのか
- 実際の環境で侵入につながる可能性があるのか
- 侵入された場合にどのような被害が発生するのか
- 現在の防御によって被害を抑えられるのか

などを考慮する必要があります。

セキュリティホールの検出件数だけでセキュリティの危険度を判断するべきではありません。

4. VPN・暗号化について

VPN や暗号化は、一般に「通信回線上の情報漏洩や改ざんを防ぐ技術」と説明されています。

しかし、通常のインターネット通信の仕組みを考えると、一般的な ISP 利用者の通信が第三者によって自由に読み取られたり改ざんされたりするものではありません。

そのため当社では、VPN や暗号化について、

接続元・接続先で扱われる情報の機密性を高め、通信内容を保護するための対策

という側面から考えることも重要だと考えています。

もちろん、機密性の高い情報を扱う場合など、暗号化が有効な場面はあります。

しかし、VPN や暗号化を導入することによって、不正侵入そのものを防止できるわけではありません。

VPN・暗号化は、セキュリティ対策の一つの要素として、その必要性和効果を考えて利用することが重要です。

5. AI によるセキュリティ対策

AI は、セキュリティホールの検出、ログの分析、異常な通信の発見などに利用できる有用な技術です。

しかし、

AI が危険と判断したものはすべて重大な危険である

とは限りません。

実際のリスクは、ネットワーク構成、利用しているサービス、アクセス制御、既存の防御策などによって変わります。

そのため、

AIによる検出 → 実際の環境で確認 → 人間がリスクを判断 → 必要な対策を実施

という考え方が重要です。

AIは人間の判断を置き換えるものではなく、**判断を支援するための有力な道具**として活用すべきです。

6. 過剰なセキュリティ対策を避ける

セキュリティ対策では、技術的に可能性があるというだけで、すべてのリスクに最大限の対策を行う必要はありません。

企業には、予算、人材、運用能力に限界があります。

そのため、

**実際のリスクがどの程度あるのか
対策によってどの程度リスクを低減できるのか
そのためにどの程度の費用が必要なのか**

を考える必要があります。

特に中小企業では、限られた資源を本当に効果のある対策に優先して投入することが重要です。

7. セキュリティ対策の評価

セキュリティ対策は、導入した製品や検出した脆弱性の数だけで評価するものではありません。

重要なのは、

不正侵入を防ぐことができたか。

侵入された場合に被害を抑えることができたか。

重要な情報を守ることができたか。

という実際の効果です。

「何を導入したか」ではなく、**「何を防げるようになったか」**を評価することが重要です。

8. 当社の基本的な考え方

当社は、AI や新しいセキュリティ技術を否定するものではありません。

セキュリティホール対策、VPN、暗号化、AI による検出など、それぞれに有効な利用方法があります。

しかし、それらを個別に過大評価するのではなく、

不正侵入をさせない。

侵入されても通過させない。

不正な通信を成立させない。

被害を拡大させない。

という基本を中心に、それぞれの対策を組み合わせることが重要です。

そして、セキュリティ対策の最終的な評価は、

「実際にどれだけ被害を防ぐことができたか」

で判断するべきだと当社は考えています。

技術の進歩に振り回されるのではなく、**実際のリスク、対策効果、費用対効果を見極め、必要な対策を着実に実施すること。**

それが、当社が考える現実的で持続可能なネットワークセキュリティ対策です。