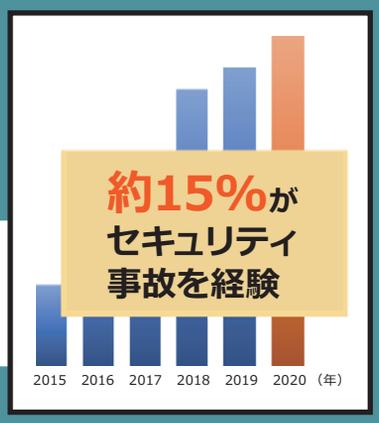
第1話

＼ サイバー攻撃対策ガイド ／

増加するリスク！ 対する対策は追いついているか？

サイバー攻撃襲来

標的型攻撃やWebサイト改ざんといったサイバー攻撃の被害に遭う企業・団体は年々増加。2015年のIPA(情報処理推進機構)が実施したアンケート調査でも、調査に協力した企業の**約15%が何らかのセキュリティ事故を経験**していると回答した。



国内企業導入率

EPP

7割弱

アンチウィルス対策に

EPP

(Endpoint Protection Platform)

KOSがオススメする ウィルス対策ソフト

ビジネスシーンでは、高い検知率と高い防御力なおかつ軽快でマネジメントの容易なものが求められます。KOSのオススメする**“Endpoint security ESET”**は、独自開発のヒューリスティック技術で**パソコンやサーバの軽快さと振る舞い検知で高い検出力を併せ持ちます。**

※EPPとは、パソコンやサーバなどのハードウェアにインストールするウィルスソフトで、代表的なものではトレンドマイクロウィルスバスター、ノートン360などがあります。

EDR

2割弱

挙動監視・検知＆対応

EDR

(Endpoint Detection and Response)

ウィルス対策ソフトと 合わせてEDRの導入がオススメ

今後のサイバー脅威に対応するために、EPPでは防げないウィルスへの対策が求められます。防御するだけでなく、被害後の対応も合わせて重要です。KOSのオススメする**“F-Secure”**は、パターンマッチングのみならず、未知のウィルスにも対応し、イベントやアクティビティをトリガーとし感染源をAIで解析し検知&対応。

標的型攻撃の増加により、通常のウイルスソフトでは防げない脅威が急増！！

従来のウイルス攻撃

不特定多数を対象に、同じウィルスがまん延するケースが多く、ウィルスサンプルを入手したソフトメーカーによって早期対応が可能であった。

標的型攻撃

”標的型攻撃“になり、対応したサンプルの入手が難しくなり、定義ファイルにない未知のウィルスに感染するケースが急増。

絶対防御は不可能！ 被害を最小限に防ぐには？

影響範囲の封じ込め

エンドポイントが感染してしまった場合を想定し端末内に侵入したマルウェアを検知し、**エンドポイント端末の隔離やシステム停止**などを行い、社内システムへの影響を防ぐ**EDR(Endpoint Detection and Response)**の導入がオススメ！！

隔離後、収集ログからマルウェアの侵入経路や被害の影響範囲を調査・分析し、対策が可能。

まずはEPPを！ よりセキュリティ強化をご検討の方はEDRをオススメします

セキュリティ対策なら…

KOSネットワーク株式会社

（TEL）**050-3538-0401**

被害を最小限に

＼ ウィルスの基礎知識を学ぶ ／

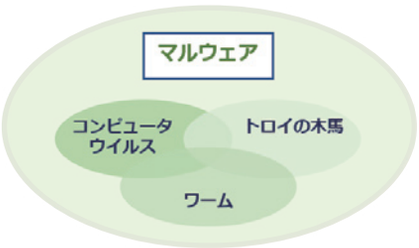
“マルウェア”知っていますか？

コンピュータウィルス、ワーム、トロイの木馬の3つの総称が“マルウェア！まずは各々の特徴を理解しよう！

① **コンピュータウィルス**は、ほかのプログラムに寄生して感染を広げるマルウェア！単独では存在できません。

② **ワーム**はネットワーク経由で感染を広げるマルウェア！自分自身をコピーし単独で増殖する

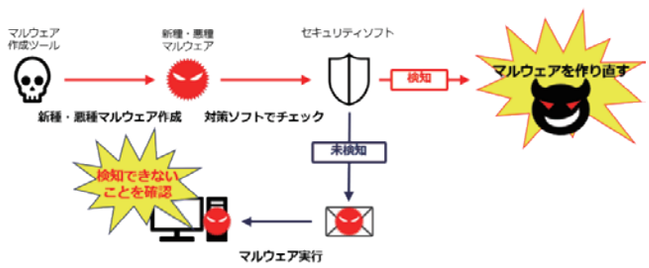
③ **トロイの木馬**は有益なソフトウェアに見せかけてユーザーに実行させるマルウェア



現在では、被害の種類や影響範囲も様々なマルウェアが出現している

なぜセキュリティソフト(EPP)で検知できない！

マルウェアを作る過程で、マルウェアをセキュリティソフトで**検知できないことを確認**してから送りつけることがあるため、EPPで検知できないマルウェアが増加しています。



セキュリティソフト(EPP)で必要なの？

EPPで防げないならウィルスソフトは必要ない！と思うかもしれませんが、それでもセキュリティソフトを導入するメリットは多数あります。セキュリティソフト(EPP)は、ウイルスをリアルタイムに“検知し駆除する機能”を備えています。

EDRやUTMと組み合わせたセキュリティ対策が効果的です

第2話につづく▶