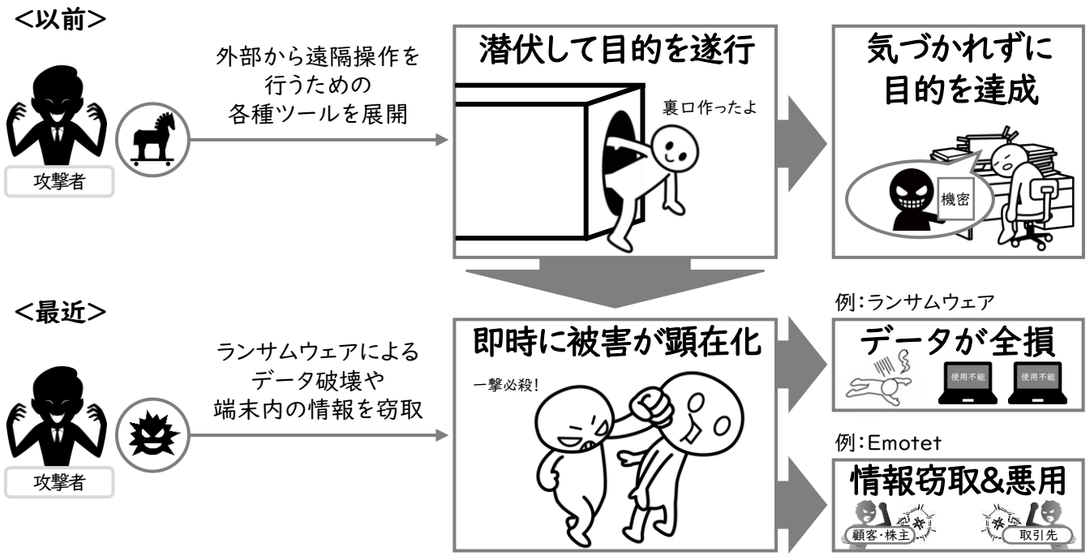
サイバー攻撃のトレンドは「Hit&Run」型の攻撃へ

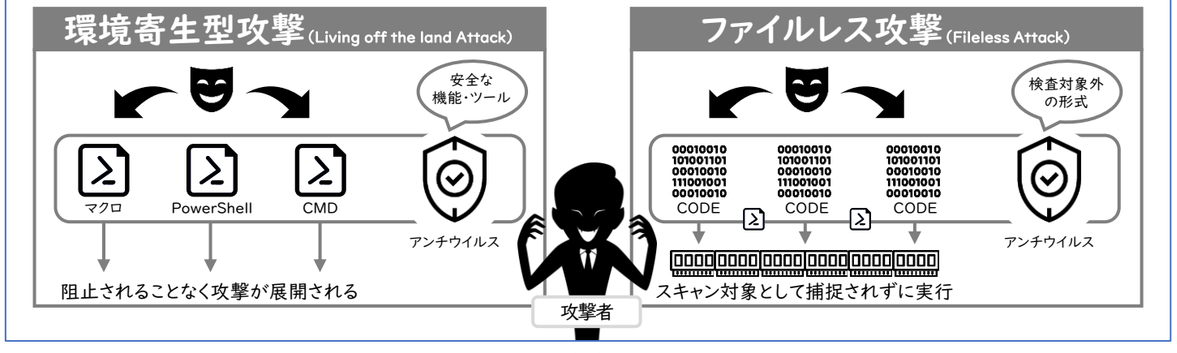
2020年に発生した国内企業におけるセキュリティインシデントの多くに共通した特徴は感染後に短時間で被害が顕在化する「Hit&Run」型の攻撃であったと言えます。



特に新型のランサムウェアは組織全体に拡散し、「情報漏洩」と「データの破壊」を同時に引き起こすことでビジネスを止め、高額な身代金を要求するようになりました。結果として身代金を支払っても支払わなくても企業にとっては甚大な損害が発生します。

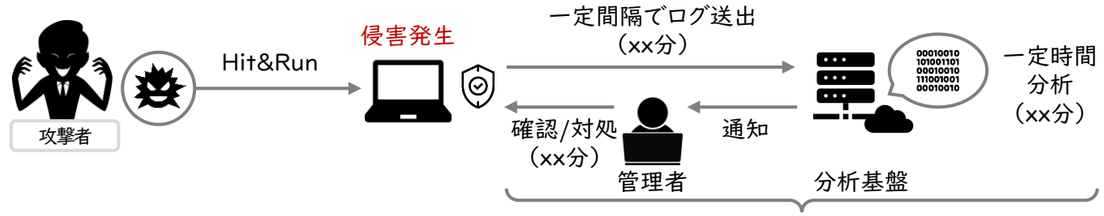
従来のセキュリティ対策を突破する手法の台頭

2019年以降、「マルウェアフリー」と呼ばれるアンチウイルスでは防御ができない攻撃手法がサイバー攻撃全体の51%を占めるに至っています。「Hit&Run」型の攻撃特性と組み合わされたことで、業務継続性のために「検知」することよりも「阻止」することを優先しなければならなくなっています。

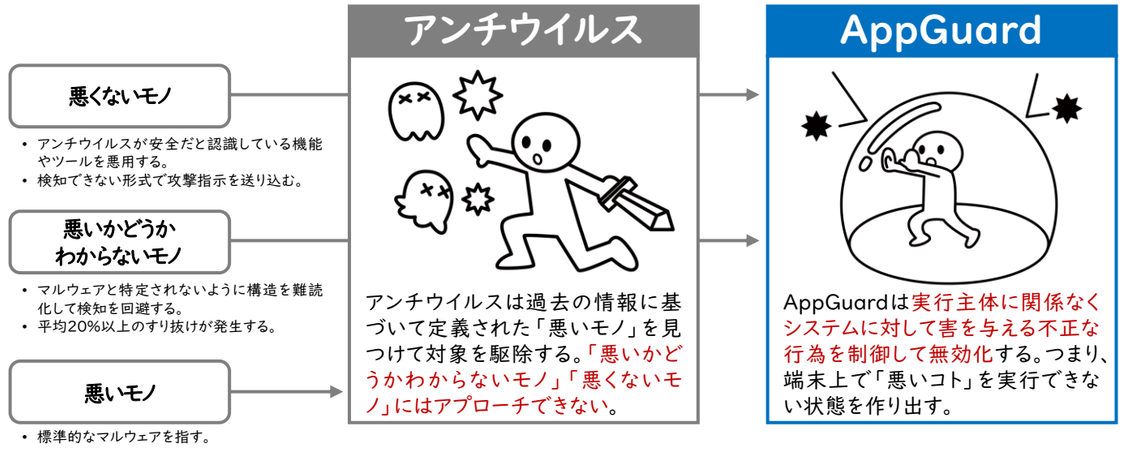


Detection(検知)よりもPrevention(防止)が重要

EDR(Endpoint Detection&Response)の様な侵害されることを前提とした検知/対処の仕組みでは「Hit&Run」型の攻撃を可視化できても「防ぐ」という観点では有効に機能するとは言えません。



AppGuardはシステムに対して「悪いコト」をさせない仕組み



AppGuardはユーザーが誤って攻撃のトリガーを引いても攻撃を成立させない

AppGuardの使いどころ

AppGuardは単体でも利用可能ですが、どのようなセキュリティソリューションとも組み合わせて使うことが可能です。特定用途に特化して課題を解決することも可能です。

Hit&Run型攻撃対策	レガシーOSの保護	閉域環境の保護	特定端末の保護
ビジネスの保護	脆弱性保護	新しい守り方	＋αの対策
Emotet / IcedID / ランサムウェア	XP SP3 / 7	工場 / 病院 / 特殊	特定社員 / 特定部署
Emotetや新型ランサムウェアに対抗するための強化策として利用	Windows7等のサポートが終了したOSをやむを得ず仕様する場合の対策	インターネットに接続できずアンチウイルスで効果的に保護できない環境へ	ビジネスを止めないために特に守らなければいけない端末へ

株式会社Blue Planet-works
〒150-0001 東京都渋谷区神宮前2-4-11 Daiwa神宮前ビル 3F
https://www.blueplanet-works.com

Blue Planet-works
Safety for the Connected World