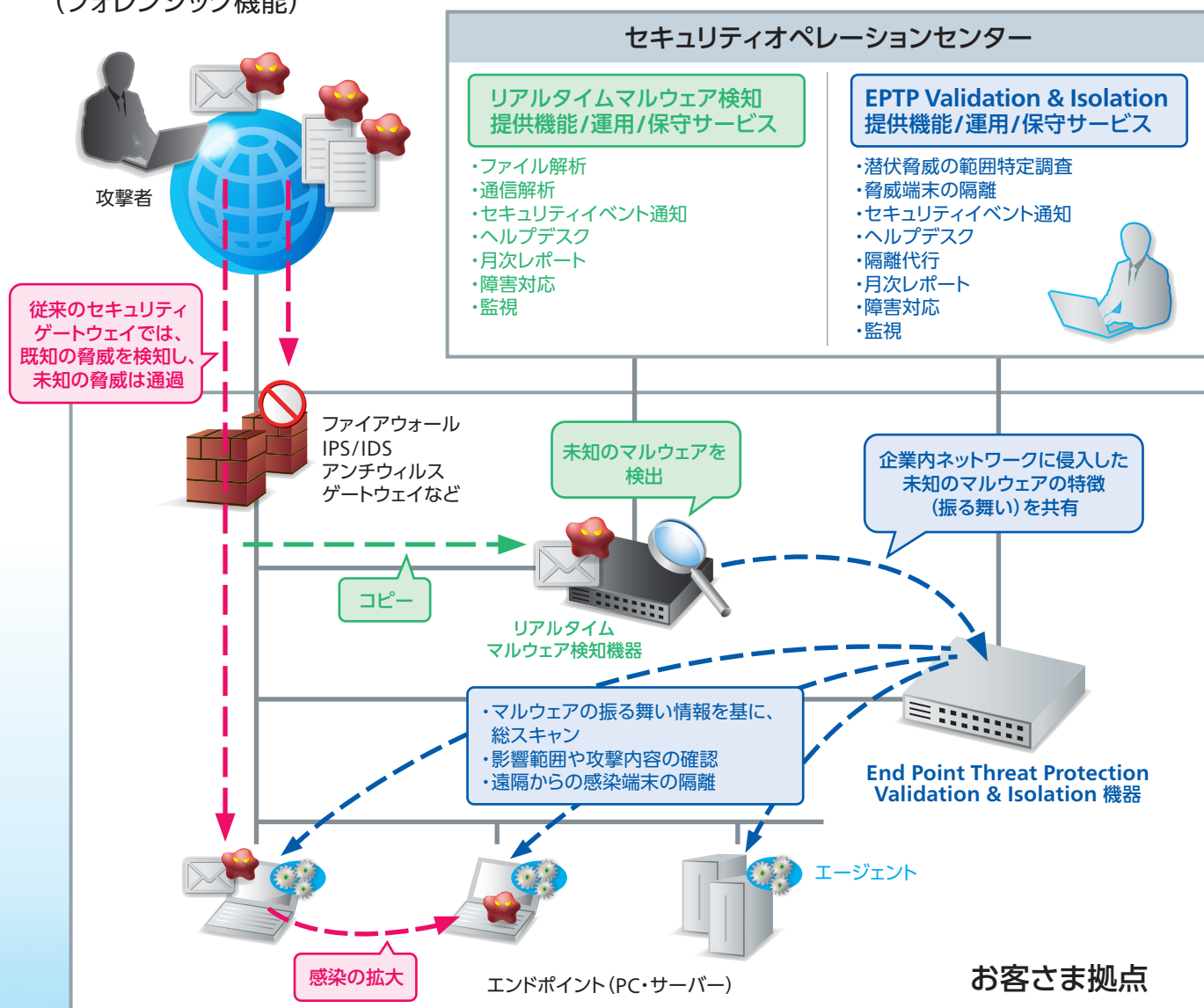


End Point Threat Protection Validation & Isolation

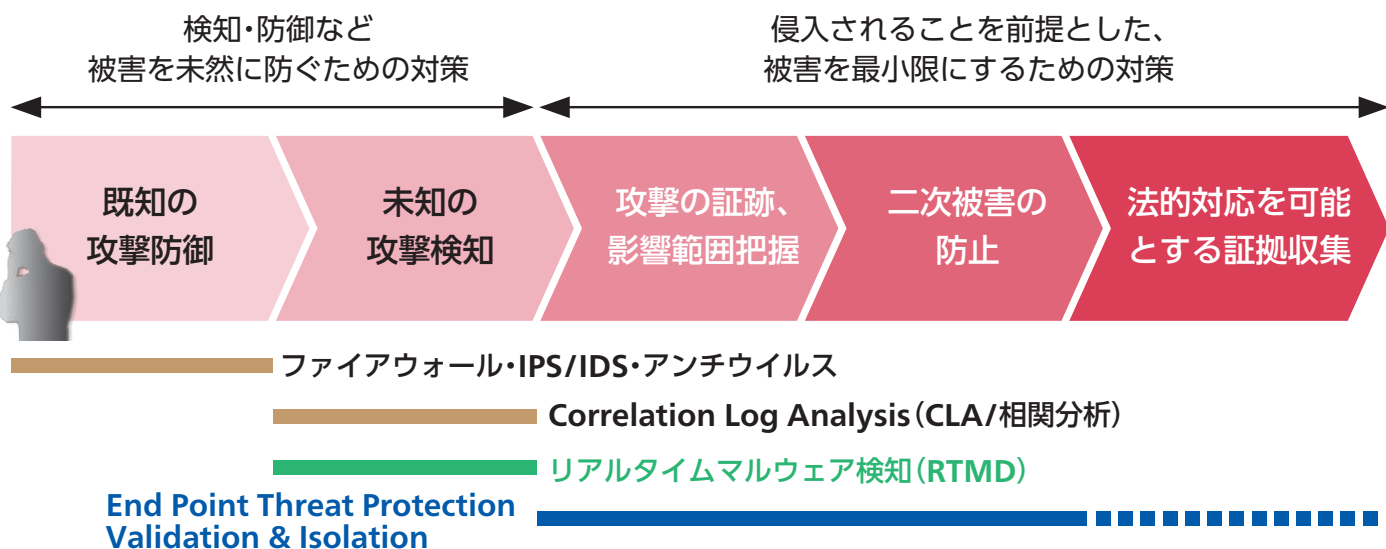
万が一マルウェア感染が発生した際、エンドポイントにおいて振る舞い情報に基づく感染範囲の特定や感染端末内のイベント情報の確認を行い、迅速なインシデントレスポンスと再発防止を実現します。

- 1 感染範囲の特定 (インシデントレスポンス機能)
- 2 迅速なリモートからの感染端末隔離、拡散防止 (インシデントレスポンス機能)
- 3 感染活動の証跡記録、ファイルの書き込み・レジストリ操作など攻撃の活動範囲・内容確認 (フォレンジック機能)



情報セキュリティ対策のステップアップ

インターネットからの未知の攻撃(新種のウイルスや新しい攻撃手法)をセキュリティゲートウェイで完全に防ぎきることは不可能です。防御策を講じながらも、侵入されることを前提とした対策を導入しておくことが重要です。



NTT Com はここが違う!

- 未知のマルウェア対策(リアルタイムマルウェア検知サービス)を日本で早期に開始し、マルウェア解析のナレッジを蓄積し、本サービスの運用ノウハウにも活かします。
- 既知の脅威への対策はもちろん、未知の脅威への防御策から侵入後の対策まで一貫したサービス提供が可能です。
- MSSP*¹ライセンスにより、お客さま自身が購入されるよりも安価に導入が可能であり、かつ高度なオペレーションサービスがご利用可能です。

*1 マネージドセキュリティサービスプロバイダ



お問い合わせ先

NTTコミュニケーションズ株式会社

ホームページ www.ntt.com/business/services/security/security-management/wideangle.html

●記載内容は2016年9月現在のものです。

●表記のサービス内容は予告なく変更することがありますので、お申し込み時にご確認ください。

●記載されている会社名や製品名は、各社の商標または登録商標です。