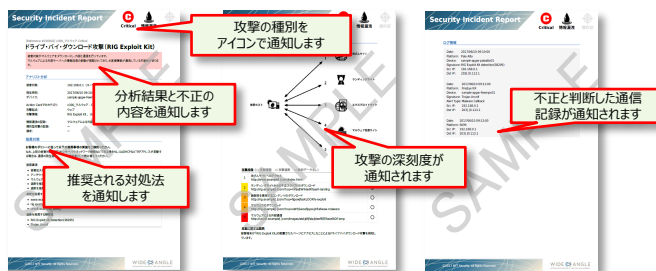


標準サービス

通信記録の監視・分析	分析対象機器の通信記録をセキュリティ分析システムに収集し、さまざまな要素をもとに相関分析を行います。通信記録の収集を行う対象は弊社サービス（Webセキュリティサービス：URLフィルタリング/Webウイルスチェック/Webセキュリティセット）になります。お客様宅内に設置されたプロキシやIPS/IDS、ファイアウォールも通信記録の収集を行うことができます。
セキュリティインシデントの判定と通知	<ul style="list-style-type: none"> 分析対象機器から収集した通信記録やNTT-Comの脅威情報をもとにセキュリティ分析システムが相関分析を行います。その結果をもとに、セキュリティ専門のアナリストがさらに詳細な分析を実施いたします。 分析の結果から発生したセキュリティインシデントは、セキュリティ専門のアナリストが、誤検知の排除を行い、危険度を「Critical」「Serious」「Medium」「Information」の4段階で判定いたします。 セキュリティインシデントが発生していると判断した場合、判断してから15分以内を目標に指定された連絡先へ通知します。 セキュリティ専門のアナリストは、セキュリティインシデントの危険度の判定やセキュリティインシデントレポート（セキュリティインシデントの内容や対応策をまとめたレポート）の作成を行い、お客様へお知らせいたします。 作成したセキュリティインシデントレポートをPDF形式にてカスタマーポータルに掲載し、お客様へメール、電話にて通知いたします。
月次レポートの提供	月間のインシデント総評、統計、セキュリティ強化策を取りまとめた様式で、月次レポートとして提供いたします。

セキュリティインシデントレポート

- 分析の結果、不正が確認された場合、速やかに不正の内容、対処法を記載したレポートを通知
- 専門家が判定することでセキュリティ事故の深刻度を認知、対処法を確認できます



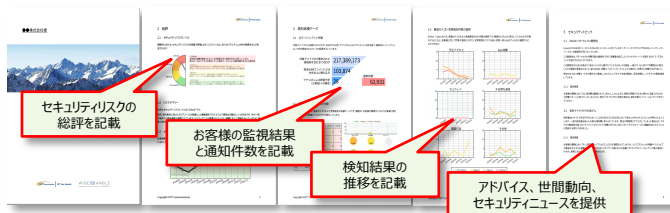
※ レポート内容はサンプルで変更となる場合があります。

参照できる情報

アナリスト分析	被害対象、発生時刻、攻撃情報 (発生したセキュリティインシデントに関連するキーワードです。マルウェアの名称など)、 情報漏洩の証跡、標的型攻撃の証跡
推奨対策	推奨事項（セキュリティインシデントに対する推奨対策）、遮断を推奨するドメイン/URL/IP アドレス、 遮断を推奨する検知名（遮断を推奨する検知されたシグネチャ名）
攻撃の詳細	攻撃の全体像、攻撃段階、攻撃に関する説明、ログ情報

セキュリティ月次レポート

- 不正通信の有無に関わらず最新のセキュリティ脅威レポートと統計レポートを毎月提供
- 検知結果の推移、アドバイスを提供しお客様のセキュリティ改善業務をサポート
- 世間動向、セキュリティニュースから最新のセキュリティ脅威に備える事が可能です



参照できる情報

総評	月次でセキュリティインシデントを総評いたします。 脅威レベルの推移を把握できるよう過去の履歴も合わせて報告いたします。
ログ・インシデント件数	分析対象機器から収集した通信記録が、セキュリティ分析システムとセキュリティ専門のアナリストによる分析を経て、最終的に何件のセキュリティインシデントとして報告されたか経過を示します。
脅威の種別・危険度別件数	セキュリティインシデントの種別と危険度別の実績データと、その推移を示します。
アドバイザー	セキュリティ専門のアナリストが、レポートしたセキュリティインシデントの傾向から導き出すセキュリティ強化案、改善提案を示します。

注意事項

- お客様監視機器を監視する場合はお客様ご自身でログ送信の設定を実施いただく必要があります。
- お客様導入の監視機器はベンダー保守に加入しメーカーサポートが提供されている機器に限ります。

記載されている会社名、製品名およびサービス名称は各会社の商標または登録商標です。記載内容は2019年1月現在のものです。記載された仕様は予告なく変更する場合があります。

