WIDE ANGLE
INFORMATION SECURITY AND RISK MANAGEMENT

NTT Communications
Transform. Transcend.

インシデントレスポンス

セキュリティインシデントは早急に対応しないと、顧客の不安は不審に変わり、
企業の信用失墜をまねきます。
情報流出が疑われる場合は、専門のエンジニアに原因究明を依頼することが肝要です。

**サイバー空間における攻撃者の脅威が増大する現在、
企業がいつマルウェア感染や不正アクセスの標的になってもおかしくありません**

いざその時、あなたは対処できますか…

エンドユーザー、取引企業、関係省庁への対応
原因や影響範囲、今後の見通し、公表の是非を早急に判断し、
公表後の対応も速やかに行わないと、不安が不審となっていく…

マルウェア感染
社内に突然ウイルス（マルウェア）が蔓延。
感染元の端末を突き止めたものの、感染経路や影響範囲の分析はこれから…

不正アクセス
不正アクセスが想定される被害に遭遇。顧客情報や
機密情報が流出した可能性があるか、早急に把握したい

インシデントレスポンス

**迅速・適切な対応が求められるセキュリティインシデントに、
プロフェッショナルエンジニアが原因究明と再発防止をサポート**

1 初動対応
セキュリティインシデントかどうか判別できない不審な事象が発生した場合、
情報の整理、事象の把握と調査を行い、セキュリティインシデントの有無を調査

2 調査・分析
インシデントの状況に応じて必要な高度な調査を行い、
原因・侵入手法の特定や影響範囲の明確化をはかります

3 改善提案
調査内容を総括し、再発防止に向けた改善提案を行います

インシデントレスポンス

数多くのインシデント対応経験と不正行為でお困りのお客さま支援を第一に必要と思われるサポートをメニュー化しています。

初動対応　インシデント初動対応パック

セキュリティインシデントの初動対応（最初の3営業日の対応）をパッケージ化し、ご依頼しやすい価格で提供します

インシデント初動対応パック　特別価格 100 万円（税別）

プロフェッショナルエンジニアをアサインし、情報の整理、事象の把握と調査を実施し、セキュリティインシデントの有無を調査します

	情報の整理	事象の把握と調査	報告
実施内容	お客さまにヒアリングを行い、発生している事象やシステム構成を把握します。必要なログやデータの確保を依頼します。	被疑端末の手がかりをつかむため、その時点で入手できているログやデータから、不正アクセスの痕跡やマルウェア感染の状況を調査します。	判明できた内容の報告と、セキュリティインシデントが判明した場合、被害の拡大防止のための打ち手を、簡易報告書としてまとめ提出します。

初動対応　インシデント対応駆付け保証オプション

インシデント調査サービスの一般的な課題

- 緊急対応サービスと書いてあるのに、1-2ヶ月待ちと言われた。。。。
- 地域限定のサービス提供で、サービス範囲対象外地域と言われた。。。。
- 調査結果がわかるまでに3週間必要と言われた。。。。

初動対応パックと駆けつけオプションを事前にご契約いただくことで

① **翌日に必ず駆けつけ**てマルウェアの簡易調査とディスク保全
② 24時間365日受付、駆けつけの**範囲は全国**
③ 自動ツールによる調査でマルウェア感染の有無を分析し、**その場で簡易レポートを提出**

調査・分析　改善提案　総合インシデントレスポンス

初動対応に続き、プロフェッショナルエンジニアが原因・侵入手法と影響範囲を調査し、改善に向けた提案を行います

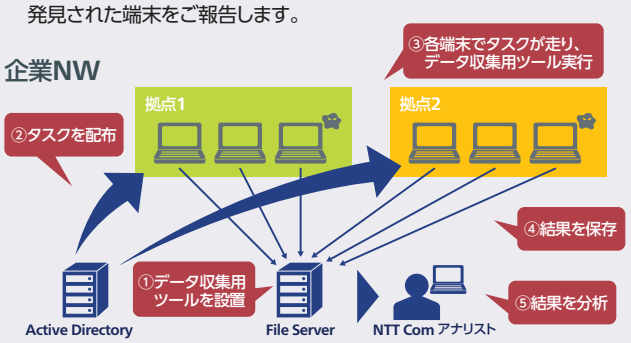
インシデントの状況に応じて高度な調査を行い、原因・侵入手法の特定や他システム等への影響範囲の明確化をはかります

	調査・分析		改善提案
項目	原因・侵入手法の特定	影響範囲の明確化	改善提案
実施内容	攻撃・感染の痕跡の詳細分析や、必要に応じより高度な調査を行い、原因・侵入手法を特定します。	攻撃・感染による影響範囲を特定します。	調査内容を総括して報告するとともに、再発防止の観点での実施事項をまとめます。
詳細	【調査手法の例】 ・デジタルフォレンジック ・ネットワークログ解析 ・マルウェア解析 ・パケット解析	【調査手法の例】 ・デジタルフォレンジック ・マルウェア解析 ・ネットワークログ解析 ・イベントログ解析	【提案例】 ・暫定的な構成変更 ・バージョンアップの推奨 ・プロファイリング ・脆弱性診断

調査・分析～改善提案の提供価格は、適宜お見積りとなります

標的型マルウェア感染端末調査

- お客様環境のすべてのWindows端末に対し、高度なマルウェアの97%が潜伏に利用する設定をチェックし、不審なプログラムの有無を調査します。
- 調査の結果判明した不審なプログラムとそのプログラムが発見された端末をご報告します。

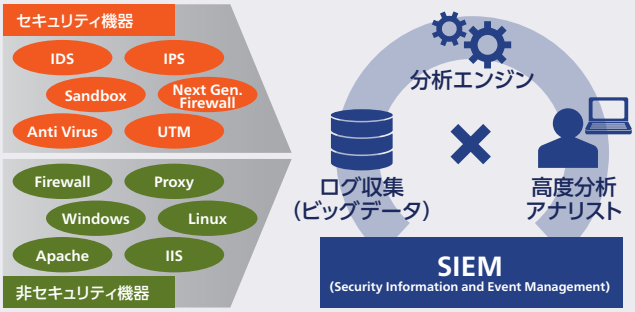


セキュリティインシデント対策関連サービス

情報流出の予防、有事の際に被害を最小化する体制整備を支援します。

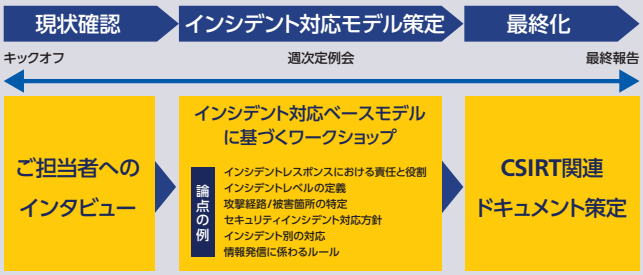
情報流出の予防　マネージドセキュリティサービス CLA (Correlation Log Analysis)

CLAサービス は、さまざまな機器のログを収集し、お客さま環境に潜在するセキュリティリスクを発見する**ログ相関分析サービス**です



有事に備える　CSIRT 構築支援コンサルティング

- 週1～2回のワークショップを通じてCSIRT構築を支援
- 弊社作成のインタビュー実施、ワークショップの実施を通し、CSIRT関連ドキュメントを策定



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

2016.09