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/

●記載内容は2019年11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。

2019.11



セキュリティ

NTT Communications
Go the Distance.

総合リスクマネジメントサービス

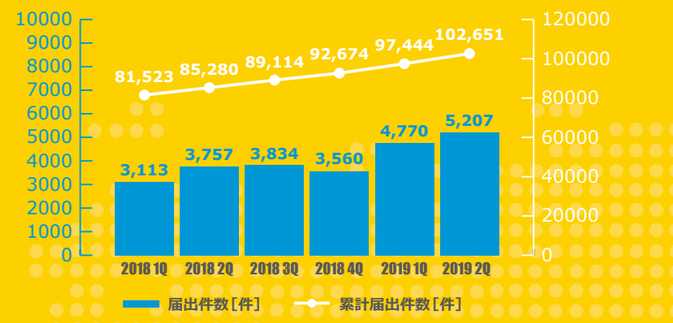
# WideAngle

サービスカタログ

WIDE ANGLE
INFORMATION SECURITY AND RISK MANAGEMENT

# Why Risk Management? ー データで見る脅威 ー

## 日本国内の脆弱性報告件数




**2019年第2四半期では、1日平均57件の脆弱性が報告されている**

出典:独立行政法人情報処理推進機構「脆弱性対策情報データベースJVN iPediaの登録状況」を集計し、作成

## 攻撃者の活動可能 期間 = 侵害発生から検知までの日数

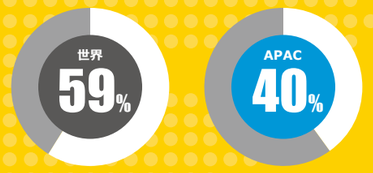
世界中央値(2018)
**78 Days**

APAC中央値(2018)
**204 Days**

**アジアでは攻撃者が長期的に活動検知が難しく被害が大きくなる**

出典:FireEye「M-TRENDS 2019」

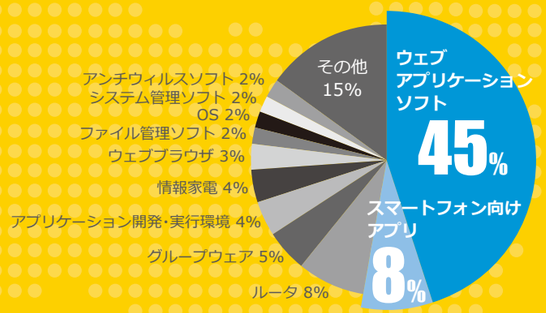
## 組織が 自社で侵害を検知した割合




**アジアに限らず世界的に見ても外部のサポートが必要**

出典:FireEye「M-TRENDS 2019」

## 日本国内で報告されている脆弱性の製品種類別割合




**ウェブサイト関連の脆弱性が約半数を占める**

出典:独立行政法人情報処理推進機構 セキュリティセンター/一般社団法人 JPCERT コーディネーションセンター「ソフトウェア等の脆弱性関連情報に関する届出状況 [2019年第2四半期(4月~6月)]」
https://www.jpcert.or.jp/report/press.html

## 複数回 の攻撃、複数攻撃者の存在

深刻な攻撃経験後1年以内に再攻撃


**継続的かつ成熟度の高い対策が必要**

出典:FireEye「M-TRENDS 2019」

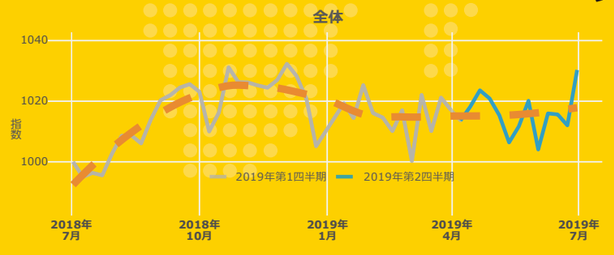
## サイバー攻撃の対 象となっている国・地域ワースト10

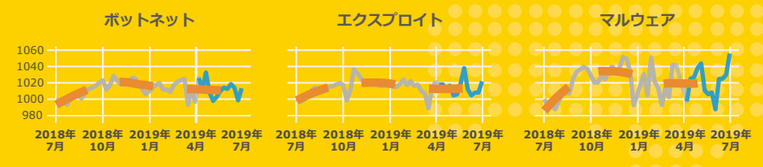
| 2019年7月 | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ワースト1 | ワースト2 | ワースト3 | ワースト4 | ワースト5 | ワースト6 | ワースト7 | ワースト8 | ワースト9 | ワースト10 |
| 米国 | 中国 | 日本 | ドイツ | 韓国 | ベトナム | 台湾 | カンボジア | タイ | 香港 |
| 検出数 819,601 | 検出数 295,492 | 検出数 166,304 | 検出数 121,283 | 検出数 120,372 | 検出数 71,550 | 検出数 66,335 | 検出数 61,022 | 検出数 56,915 | 検出数 53,457 |

**日本は世界で三番 目にサイバー攻撃の標的とされている**

出典:Palo Alto Networks「unit42 脅威インテリジェンス 月次レポート 2019年7月」

## グローバルでのサイバー攻撃動向




**サイバー攻撃を構成するエクスプロイトとマルウェアに増加傾向**

出典:Fortinet「フォーティネット脅威レポート2019年第2四半期版」

【本誌記載の短縮表記】(アルファベット順)

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AP | アプリケーション | EMM | エンタープライズモビリティ管理 | MSS | マネージドセキュリティサービス | SOC | セキュリティオペレーションセンター |
| APT | 持続的標的型攻撃 | FW | ファイアウォール | PCAP | パケットキャプチャ | UI | ユーザーインターフェース |
| CSIRT | コンピュータ セキュリティ インシデント レスポンス チーム | GW | ゲートウェイ | PCR | ポリシーチェンジリクエスト | UTM | 統合脅威管理(アプライアンス) |
| DMZ | デミリタライズドゾーン(非武装地帯) | IDS | 侵入検知システム | RTMD | リアルタイムマルウェア検知 | WAF | Web アプリケーションファイアウォール |
| EDR | エンドポイント ディテクション アンド レスポンス | IPS | 侵入防止システム | SIEM | セキュリティ情報イベント管理 | | |



## 目次

# 企業の脅威となるトレンドの攻撃

## 標的型攻撃による情報漏洩

**多くの企業・団体で被害が報告されている攻撃です。**

**【攻撃手順】**

①なりすましメールや改ざんサイトへの誘導でマルウェアを侵入させる

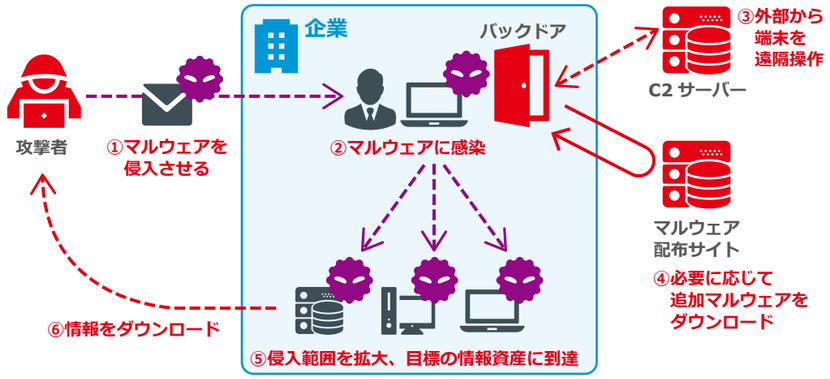
②PC がマルウェアに感染（バックドア設置）

③C2 サーバーによる遠隔操作開始

④必要に応じてマルウェア配布サイトから追加マルウェアをダウンロード

⑤侵入経路、活動領域を拡大し、目標となる情報資産を発見

⑥目的の情報をダウンロード（機密情報漏洩）




## ランサムウェアによる身代金攻撃

**最近、急激な流行を見せている直接的な金銭詐取を目的とした攻撃で、企業内部の情報を勝手に暗号化しそれを人質に身代金を要求してきます。**

**【攻撃手順】**

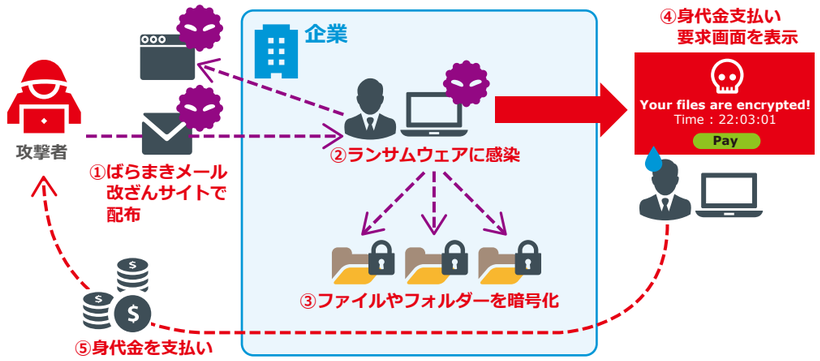
①ばらまきメールの添付ファイルや改ざん Web サイトへのアクセスでランサムウェアに感染

②PC がランサムウェアに感染

③ランサムウェアが動作開始、PC 内のフォルダーやファイルを次々に暗号化

④身代金の支払い要求画面を表示

⑤被害者による身代金の支払い




## 公開サーバーの脆弱性を突いた攻撃による情報漏洩

**公開サーバーは外部に対して解放されているため、攻撃対象になりやすく脆弱性を残しておくことは非常に危険です。**

ここでは会員制 Web サイトを例に説明しますが、サーバーを乗っ取られる事で加害者になるケースもあります。

**【攻撃手順】**

①ソフトウェアの脆弱性情報を認識し悪意を持って探索活動開始

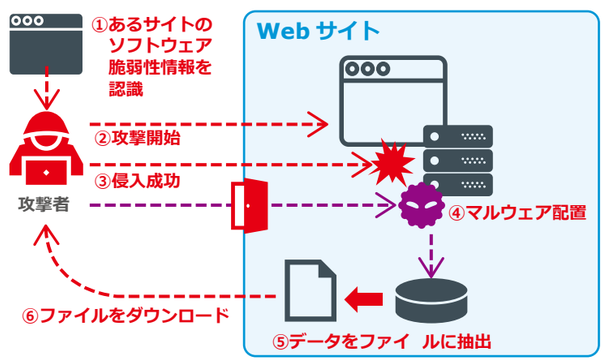
②脆弱性のある Web サイトを検索し発見

③脆弱性を突いて侵入に成功

④サーバー内にマルウェア（バックドア）を設置

⑤C2 サーバーからマルウェアを遠隔操作しサーバー内のデータをファイルに抽出

⑥ファイルを外部にダウンロード




こうした攻撃には
インターネットゲートウェイに
セキュリティ対策機器を配置し防御します。

- **IPS/IDS や UTM を設置し 不審な通信を検知・ブロック** P19
- **UTM のアンチウイルス機能で 既知のマルウェアを駆除** P19
- **サンドボックスにより未知の マルウェアを早期に発見し駆除** P21

加えて、エンドポイントセキュリティを
導入することも有効です。

- **インターネットゲートウェイを擦り抜けた マルウェアを端末側で発見し、端末を隔離** P23

こうした攻撃には公開サーバーへの
セキュリティ対策を配置し防御します。

- **IPS/IDS や UTM により サーバーやミドルウェアへの攻撃を防御** P19
- **WAF により Web アプリケーションへの 攻撃を防御** P20

さらに、脆弱性情報を管理する体制を
強化する必要もあります。

- **プラットフォームや Web アプリケーションの 定期的な脆弱性診断と改修** P13
- **ソフトウェア脆弱性の発覚時に社内状況を 確認できる総合的な脆弱性管理体制を構築** P14

# これからのビジネスとワークスタイルを拓く WideAngle

## ビジネス成長を支える サイバーネットワークのつながりを守る WideAngle

IT 技術や IT リソースの進化と多様化、さまざまな産業分野の垣根を越えたデジタルトランスフォーメーションの潮流、そして、それらをつなぐネットワークの広がりと複雑化が進む中で、グローバルに開かれた企業のビジネスは、巧妙化していく未知の脅威に常に、休みなく、晒され続けています。

もはや点でリスクを考える時代ではなく、さまざまにつながるビジネスと、ビジネスを支える ICT 環境を広い視野で捉えたマネジメントセキュリティが求められています。

WideAngle は、NTT グループの高度な技術力と経験豊富なセキュリティ人材により、お客さまのビジネスに最適なセキュリティソリューションをご提供いたします。

### 世界最大級の通信インフラを守るセキュリティ品質

・41 の国や地域の 110 都市で事業拠点を展開
・190 以上の国や地域でグローバルネットワークサービスを提供
・世界最大級のグローバル Tier1 IP バックボーン
・全世界に 140 以上のデータセンターを展開
※上記は NTT Com の事業規模です。（2018 年 3 月現在）

### ワールドワイドに展開する セキュリティオペレーションセンター

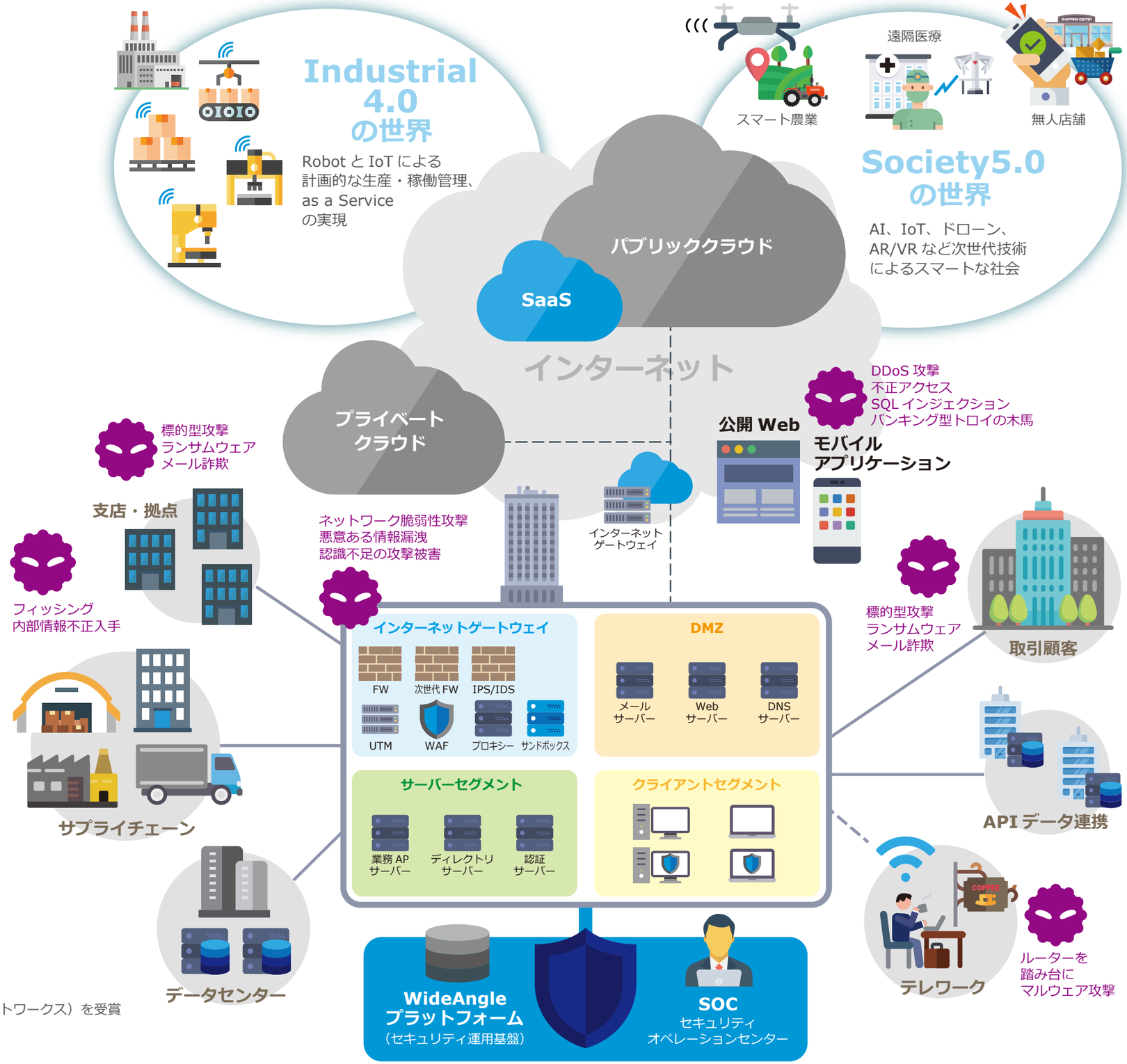
・セキュリティエキスパート：1,500 名
・SOC：10 拠点
・16 カ国に 23 オフィス
・監視対象デバイス数：165,000 台
※上記は NTT セキュリティの事業規模です。（2018 年 5 月現在）

### セキュリティ脅威を分析する独自の プラットフォームとハイスキルなアナリスト

・1 年間で分析するログ数 6.1 兆
・年間に検知・防御している攻撃数 1.5 億
・100 万 IP のハニーポットをベースにした独自ブラックリスト
・クリティカルレベルの脅威のうち 7 割を検知するカスタムシグネチャー

### MSS プロバイダーのリーディングカンパニー

・APAC の MSS プロバイダーとして 3 回連続でリーダーポジションの格付け
・Japan Theater Managed Service Provider of the Year（2018 年 , パロアルトネットワークス）を受賞
・Partner of the Year（2017 年 , ファイア・アイ）を受賞
・Growth Partner of the Year（2017 年 , フォーティネット）を受賞



# WideAngle のサービス メニュー

## ●プロフェッショナルサービス

| サービスメニュー | | | 提供内容 | スポット / ランニング | Page |
|---|---|---|---|---|---|
| 総合コンサルティング | | | お客さま ICT 環境の「ガバナンス」「リスク」「コンプライアンス」に関わる各種サポートを提供<br>セキュリティポリシー作成支援　CSIRT/SOC 構築支援<br>システムリスクアセスメント　インテリジェンス導入支援<br>セキュリティプランニング支援　など | スポット | P9 |
| CSIRT 運用支援ソリューション | アドバイザリーサポート | | WideAngle で蓄積された高度な専門知識や調査分析のノウハウを活かし、サイバー情報収集 / 調査 / 分析を代行 | ランニング | P10 |
| | 脅威情報サービス | OSINT モニタリング | 公開されている情報を分析して、お客さまシステム環境に関するサイバー脅威を調査し報告 | スポット / ランニング | P10 |
| | インシデントレスポンス | 総合インシデントレスポンス | 緊急事態にエンジニアが調査・分析を実施初動対応、調査分析、改善提案まで提供 | スポット | P11 |
| | | インシデント初動対応パック | 情報の整理、事象の把握と調査、被害の拡大防止までを実施 | スポット / ランニング | |
| | | 標的型マルウェア感染端末調査 | 標的型マルウェアに感染している端末がないかを調査 | スポット | P12 |
| | | AI Analysis Powered by Cylance | AI 型検知ツールを併用することで、マルウェアの検知精度を向上 | スポット | |
| | | Endpoint Prevention Powered by Cylance | AI 型次世代アンチウイルス製品の導入と運用サポート、インシデント対応をセットで提供 | ランニング | |
| | 脆弱性診断 | プラットフォーム脆弱性診断 | OS やミドルウェアなどの脆弱性を検出、リスクを可視化 | スポット | P13 |
| | | Web アプリケーション脆弱性診断 | Web アプリケーションの脆弱性を検出、リスクを可視化 | スポット | |
| | | セルフ脆弱性診断 | 脆弱性診断をお客さま自身で行う環境を提供 | ランニング | |
| | 脆弱性見える化ソリューション | | システム情報管理、脆弱性検出 / 通知 / 診断、対策 / リスク管理機能をプラットフォームサービスとして提供 | ランニング | P14 |

## ●マネージドセキュリティサービス

| サービスメニュー | | | 提供機能 | Page |
|---|---|---|---|---|
| ネットワークセキュリティ | ファイアウォール | | ファイアウォール | P19 |
| | IPS/IDS | | IPS/IDS | |
| | ネットワークセキュリティ 基本パック | | ファイアウォール、IPS/IDS | |
| コンテンツセキュリティ | コンテンツセキュリティ 基本パック | | ファイアウォール、IPS/IDS、メール /Web アンチウイルス | |
| | コンテンツセキュリティ 拡張 A パック | | 基本パック + URL フィルタリング | |
| | コンテンツセキュリティ 拡張 B パック | | 拡張 A パック + アプリケーションフィルタリング、RTMD | |
| | WAF | | WAF（Web アプリケーションファイアウォール） | P20 |
| リアルタイムマルウェア検知 | RTMD ONSITE | RTMD Web<br>RTMD E-mail<br>RTMD マネジメント | サンドボックス（Web/E-mail/ マネジメント） | P21 |
| | Cloud base RTMD | | サンドボックス（Web/E-mail） | P26 |
| エンドポイントセキュリティ | EDR | | 感染端末の隔離 | P23 |
| | プロアクティブ レスポンス for SD-LAN | | 外部への悪性通信遮断（SD-LAN 連携） | – |
| プロキシー分析 | | | プロキシーのログ分析 | P22 |
| クラウド GW セキュリティ | WSS 基本パック | | Web Security、Mobile Security、Antivirus | P25 |
| | WSS RTMD パック | | 基本パック + Malware Analysis | |
| スレットインテリンジェンス | Active Blacklist Threat Intelligence (ABTI) | | ブラックリスト配信 | P24 |

**アドオンサービス**

| | | |
|---|---|---|
| CLA*1（非セキュリティ設備との総合ログ相関分析） | 非セキュリティデバイスとの相関分析 | P22 |

*1 CLA : Correlation Log Analysis

## ●セキュリティ対策機器の導入サービス

セキュリティ対策機器を販売またはレンタルし、同時に設定・設置などの導入サービスを提供します。



# 課題ごとの対応サービス

## お客さまの困った！を解決

- ネットワーク、システムの更改タイミングでセキュリティも見直したい
- ビジネス基盤としてのセキュリティ構築を再検討したい

→ 総合コンサルティング P9

- CSIRT の立ち上げや高度化を図りたい

→ CSIRT 構築支援 / アドバイザリーサポート / OSINT モニタリング P9 - 10

- 情報漏洩？　いざという時、自分たちで解決できるか不安

→ インシデントレスポンス P11

- 日々発信される脆弱性情報に対応できているか不安

→ 脆弱性診断、セルフ脆弱性診断 / 脆弱性見える化ソリューション P13 - 14

- 自社でのセキュリティ運用はもう限界
- 標的型対策デバイスを追加検討したい
- セキュリティ機器のアラートを確認しきれないので不安
- アラートが誤検知だらけで、ほぼ放置
- セキュリティ機器ごとに運用の委託先がバラバラでレポートもまちまち

→ マネージドセキュリティサービス P15 ～

- Web サイトへの攻撃が心配

→ WAF P20

- ウイルス対策ソフトで検知できないマルウェアが心配

→ RTMD ONSITE / 標的型マルウェア感染端末調査 P12・P21

- 出口対策を強化したい

→ プロキシー分析 / クラウド GW セキュリティ P22・P25

- エンドポイントにおけるマルウェアの検知や監視を強化したい

→ EDR P23

- 情報システム部門がいない夜間や休日にサイバー攻撃を受けても対処できない

→ MDR P24

# プロフェッショナルサービス

WideAngle のプロフェッショナルサービスは、企業のセキュリティ管理体制の整備や運用に対してセキュリティプロフェショナルの知見を提供するサービスで、**総合コンサルティング**と**CSIRT 運用支援ソリューション**で構成されています。

・セキュリティコンサルタント
・セキュリティリサーチャー
・フォレンジックエンジニア
・脆弱性診断エンジニア

**セキュリティ プロフェッショナル**

### 総合コンサルティング

・事業戦略レベルのセキュリティ対策の立ち上げ
・CSIRT や SOC など専門管理体制の構築支援
・現状のセキュリティ体制への評価、改善提案

### CSIRT 運用支援ソリューション

CSIRT の幅広い管理・運用業務に対する
専門性・高度化を備えたサポートサービス提供

## 総合コンサルティング

お客さま ICT 環境の「ガバナンス」「リスク」「コンプライアンス」に関わる各種サポートを提供します。

### セキュリティプランニング支援

情報セキュリティの戦略・組織・要員・プロセス・技術の各領域にわたり、現状のセキュリティリスクアセスメント、必要な対策の洗い出し、およびロードマップ策定を実行し、お客さまに適したセキュリティ実施計画を支援します。

| | |
|---|---|
| STEP-1　リスクアセスメント | 資料レビューと関係者ヒアリングにより現状のセキュリティリスクの有無とレベルを評価。 |
| STEP-2　対策洗い出し | アセスメント結果を踏まえ必要な対策と優先度を洗い出し、お客さまと協議のうえ決定。 |
| STEP-3　ロードマップ作成 | 洗い出した対策の実装 / 実施に向けアクション項目を検討し、ロードマップへ落とし込む。 |

対策領域と項目

**組織・人**

セキュリティポリシー、セキュリティマネジメントシステム（PDCA）、監査、インシデント対応体制（CSIRT）　等

**技術**

ネットワーク、サーバー、データベース、アプリケーション、エンドポイント、無線 LAN 対策、ログ / アラート監視、脆弱性 / パッチ管理、バックアップ / 障害復旧、暗号化　等

**物理環境**

ゾーニング、入退室管理、カード / 生体認証、盗難 / 紛失対策、耐震・防火・防水・空調・電力設備　等

### CSIRT 構築支援

セキュリティインシデントへの組織的対応に関して、抽象的な組織的概念である CSIRT を具体化し、
短期間で一定の成熟度レベルへの到達を支援します。

**セキュリティインシデントへの対応レベル** *1

成熟度レベル

- レベル 5　最適化されている
- レベル 4　管理・測定が可能
- レベル 3　定義されたプロセス
- レベル 2　再現性はあるが直感的
- レベル 1　個別対応
- レベル 0　プロセス不在

CSIRT 運用で成熟度向上を行う

**CSIRT による組織的インシデント対応実現**

**CSIRT 構築**

インシデント対応に苦悩する状態

**CSIRT 構築によるレベルアップ**

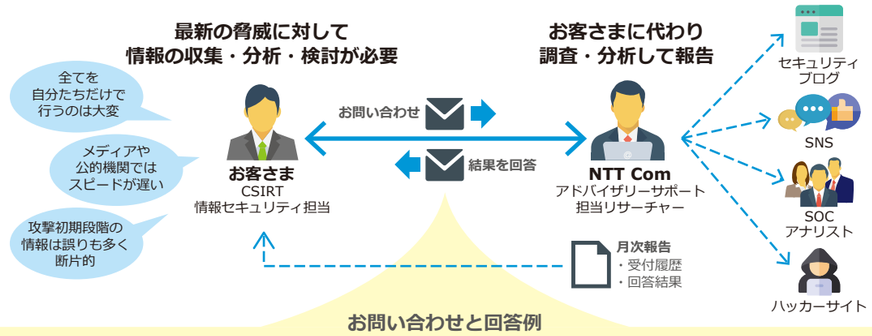
| | |
|---|---|
| STEP-4 演習実施 | STEP-3 で定義された体制・フローがインシデント発生状況下で機能するか、机上演習により検証。 |
| STEP-3 マニュアル作成 | STEP-2 で検討・定義された結論を『インシデント対応マニュアル』として文書化。 |
| STEP-2 プロセス検討 | インシデント検知～収束までの報告・指示・作業フローや、判断基準等について検討・定義。 |
| STEP-1 体制検討 | CSIRT の業務範囲や組織構成、構成要員の役割 / 権限 / 責任等について検討・定義。 |

*1　COBIT における成熟度モデルをベースに NTT Com にて作成



## アドバイザリーサポート

お客さまからの情報セキュリティに関する各種お問い合わせに対する受付窓口（リサーチャー）を設置し、助言・情報提供を行います。




**お問い合わせと回答例**

**情報提供の依頼**

Q 同業他社が標的型メール攻撃にあったと発表したが、何か関連情報はないか？

A 発表した会社のセキュリティ対策の取り組みに関して発表情報の行間を埋める付加的な情報を収集して報告

**対処 / 判断の相談依頼**

Q 「APT10」という集団の標的型攻撃キャンペーンのレポートがセキュリティ会社から出されたが自社への影響はあるか？

A セキュリティ会社等の組織が公開した APT10 に関連するレポートで、分かりにくい点や不足情報を調査し、注釈等を入れて、セキュリティの専門家でなくとも理解しやすい報告書にまとめて提出

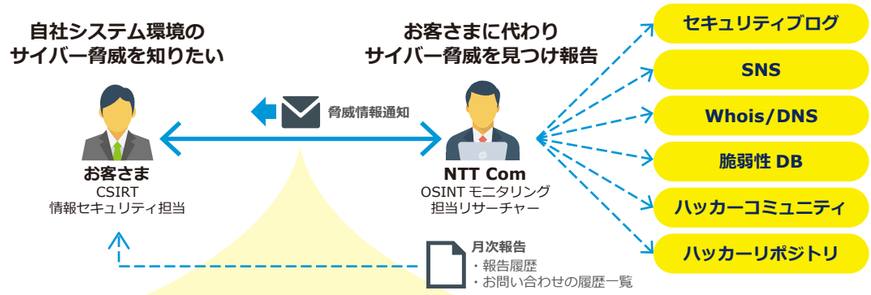
**対応 / 対策のレクチャー依頼**

Q 取引先から「そちらのメールサーバーがブラックリストに登録されているため、そちらからのメールが届かなくなった」と連絡があった。何をどのようにして確認し、解除すればよいのか？

A メールサーバーの設定に誤りがあり、第三者中継が許可されている可能性を指摘。取るべき対策をアドバイス

## OSINT モニタリング

公開されている情報を分析して、CSIRT を運用するお客さまに代わって
お客さまシステム環境に関するサイバー脅威を見つけ報告するサービスです。

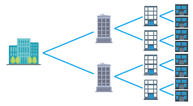



**利用例**

毎日のように新しい攻撃手法や脆弱性が見つかっている。攻撃者から見て弱点がないか心配。

OSINT 情報を活用して、攻撃者の目線でお客さまのシステムの問題点をあぶり出します。

グループ会社や関連会社がセキュリティを管理できているか、知りたい。



オープンソースの情報からグループ会社や関連会社のセキュリティ上の問題点を見つけ出します。

いろんな部署が Web サーバーを勝手に立てていて、把握できていない。


さまざまな OSINT 技術を駆使して、お客さまが把握できていないサーバーを見つけ出します。

過去に放棄したドメインが悪用されていないか心配。

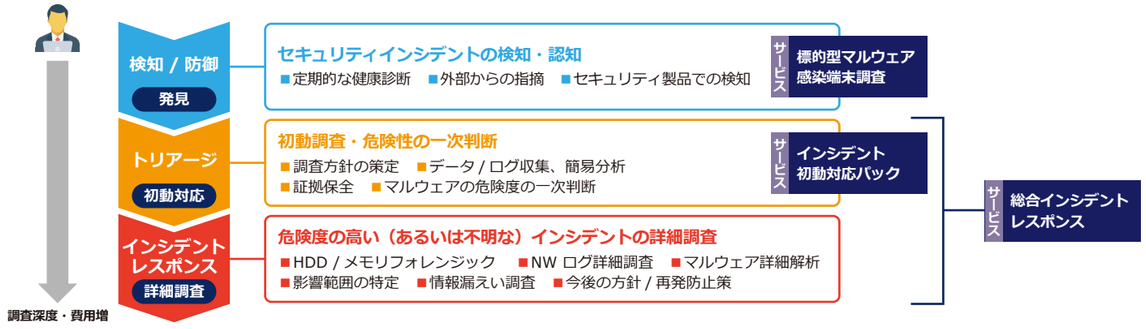

過去に放棄したドメインの利用状況を調べ、犯罪者などに悪用されていないか確認します。

# インシデントレスポンス

## セキュリティプロフェッショナルが原因究明と再発防止をサポート！

不正アクセスやマルウェア感染、情報漏えいなどインシデント対応にはスピードが求められます。セキュリティインシデント発生時にセキュリティプロフェッショナルが『初動対応（トリアージ）』『詳細解析（インシデントレスポンス）』『報告・改善提案』を実施します。

**インシデントレスポンス調査ステップ**




### インシデント初動対応パック　　特別価格 100 万円（税抜）

## セキュリティインシデント時に必要となる初動対応を実施！

セキュリティインシデント発生時に必要となる初動対応を３営業日以内で実施します。
NW ログを中心に事象の把握・初動調査を実施し、インシデントの危険度を判定します。

**初動対応（トリアージ）**　事象の危険度・追加調査有無を判断

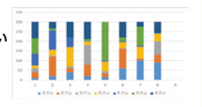
**① 状況整理・ヒアリング　～調査方針の制定～**

外部からの攻撃検知 / WEB サイトの改ざん / 情報漏えいの可能性 / 不正通信・マルウェアの検知

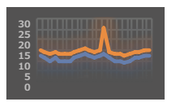
**②異常の有無や危険度を調査　～調査・分析～**

3営業日

**FW**
・通常、利用しないポートでの通信
・時間帯別の通信



**Proxy**
・不審な送信先への通信
・実行ファイルのダウンロード



**マルウェア感染**
・検体の危険度を判断し、IR の必要性判断（Open Intelligence）

1. マルウェアの可能性
2. 影響範囲・特徴
3. 危険性判定
4. 詳細解析有無

**③切分け・結果のご報告**

### 総合インシデントレスポンス

## セキュリティインシデント発生時の本格調査を実施！

初動対応に続き、セキュリティプロフェッショナルが原因・侵入手法の特定・影響範囲の明確化・情報漏えい有無の調査を実施し、改善に向けた提案を実施します。発生事象に応じて調査内容は異なります。

**詳細調査（インシデントレスポンス）**　原因・侵入手法の特定、影響範囲の明確化の調査、改善提案

- ■ ネットワークログ詳細分析 ・・・・ 多角的なログ解析による侵入経路の確認、情報流出の痕跡確認　等
- ■ HDD / メモリフォレンジック ・・ 侵入痕跡の事実確認、操作履歴、マルウェア感染有無　等
- ■ マルウェア詳細解析 ・・・・・・・ マルウェアの目的・特定・挙動の把握、情報漏えいの可能性有無　等





### 標的型マルウェア感染端末調査＋オプションサービス①（AI Analysis Powered by Cylance）　　特別価格 121 万円（税抜）※端末数 500 台の場合

## インシデントレスポンスの知見を活かした潜伏マルウェアへの感染有無を調査

お客さま環境の Windows 端末で**多くのマルウェアに共通する自動起動設定**を収集するツールを実行し、結果を分析することで潜伏マルウェアの疑いのある不審な設定・挙動を調査します。これにより、アンチウィルスでは捉えられない標的型マルウェアを検出します。

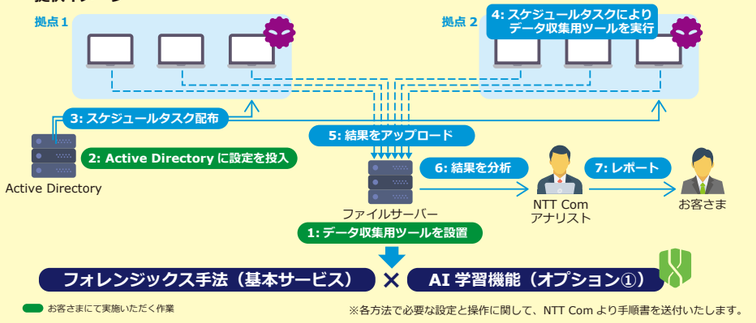
**検知**　マルウェア感染を調査する健康診断

・独自開発の情報収集ツールを実行いただき、潜伏マルウェアの有無を調査し、お客さま環境の安全性を評価する健康診断サービスです。

・多くのマルウェアに共通する特徴にフォーカスし、今のマルウェア感染有無・セキュリティ侵害の可能性を調査し、推奨事項をお伝えします。経験豊富なセキュリティアナリストのノウハウと AI 技術を併用することで、検知率を約 90%※1 まで向上させます。

※1.NTT コミュニケーションズ調査実績に基づく

**提供イメージ**




### オプションサービス②（Endpoint Prevention Powered by Cylance）

## 高い検知精度をほこる次世代 AV 製品での防御と専門エンジニアによる解析サポート

高い検知率をほこる AI 型の次世代 AV 製品 (CylancePROTECT) を導入いただき、恒久的な対策をワンストップで提供するサービスです。

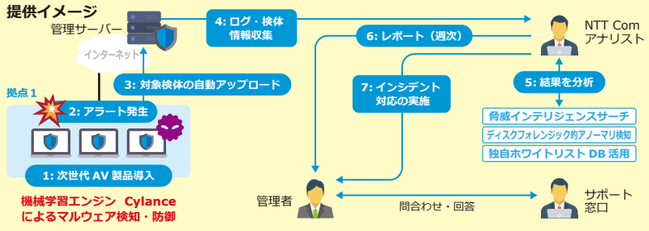
**防御**　次世代 AV 製品導入による恒久対策

・高い検知精度をほこる次世代 AV 製品を導入し、経験豊富なフォレンジックエンジニアが日々の運用をサポートします。
・万が一、インシデントが発生した場合でも、本サービスの中でインシデントレスポンスの提供が可能です。

**提供内容**

| | |
|---|---|
| 導入・設計・構築 | ライセンス提供、初期設定チューニング（お客さま環境に合わせた誤検知精査）を実施します。 |
| マルウェア解析 | マルウェア検体解析・危険度判定ならびに、結果のレポーティング（週次）を実施します。 |
| インシデントレスポンス | セキュリティインシデントが発生した場合は、インシデントレスポンスを提供します。 |
| 問合せ対応 | 製品・サービスについての問合せ対応を実施します。 |

**提供イメージ**




### サービス担当者からのおススメポイント

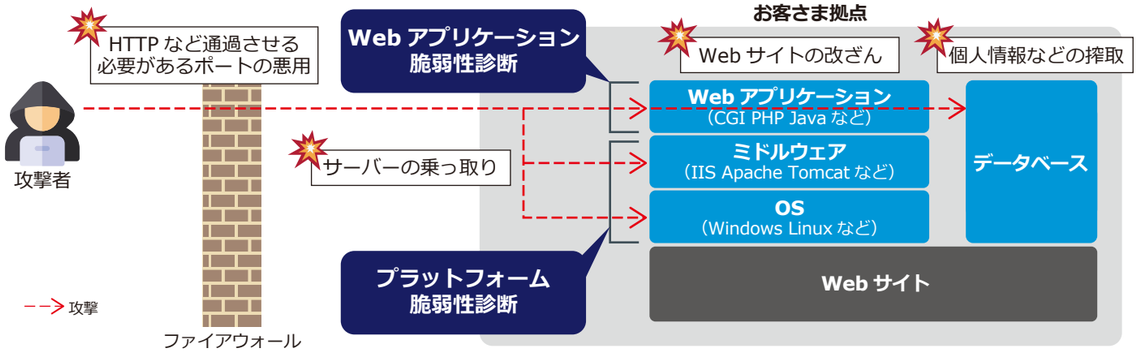
**事前にご契約いただくことで、柔軟かつ迅速な対応が可能なチケット制での提供も可能です。**

インシデントレスポンスは、実調査に入るより前に、**調査ベンダの確保・契約処理・価格調整・調査に必要なログの不足等、調査をスムーズに開始できないケースが非常に多く**存在するのが実情です。
事前に契約いただくことにより、下記のメリットを享受でき、有事の際でもスムーズな対応が可能となります。

- ■ **調査速度の向上と優先対応が可能**
- ■ **契約稼動の削減により、スムーズな調査が可能**
- ■ **インシデントが発生しなかった場合でも、定期的な健康診断や教育・訓練等で利用可能**

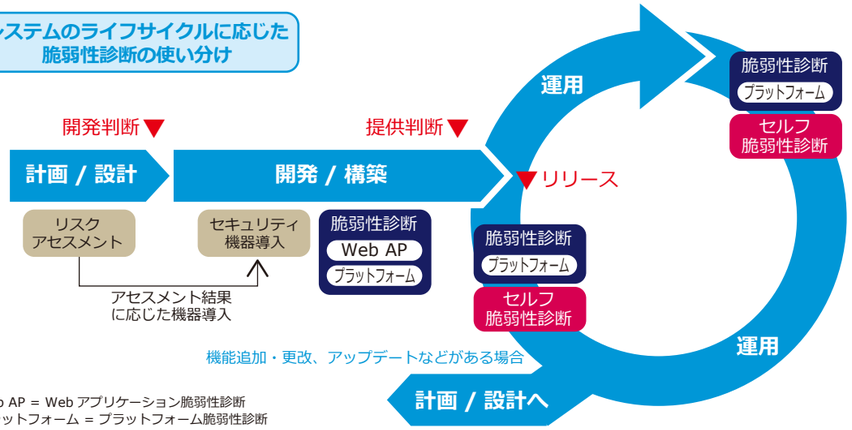
# 脆弱性診断／セルフ脆弱性診断

## サイバー攻撃で狙われる ICT 環境の欠陥（脆弱性）を補修するには、まず専門家や専用ツールによるチェック（診断）が不可欠




| | 脆弱性診断 | セルフ脆弱性診断 |
|---|---|---|
| 概要 | 専門のセキュリティエンジニアが診断し、<br>知見に基づき評価、結果を報告します。 | お客さま自身で継続的にアセットの脆弱性を把握し、<br>対策を実施するための環境を提供します。 |
| 契約単位（診断対象） | プラットフォーム／ Web アプリケーション | プラットフォーム／（オプション）Web アプリケーション |
| サービス提供形態 | 委託 | SaaS |
| 実施者 | セキュリティエンジニア | お客さま |
| 管理機能 | ー | アセット管理（OS や使用ソフト、オープンポート等）<br>／脆弱性リスク把握／チケットによる改善管理 |
| 脆弱性検出方法 | 手動／ツール（スキャン） | ツール（スキャン、エージェント） |
| 診断精度 | 高 | 中 |
| 評価 | 以下の要素を加味し、セキュリティエンジニアが評価<br>・攻撃のトレンド／難易度　・診断対象 / 環境の特徴<br>・最新のセキュリティ情勢　・IPA の推奨値　など | ツールの評価基準による評価 |
| レポート／報告書 | セキュリティエンジニアが報告書作成 | ツールの出力レポート |
| 費用 | 診断毎契約（ワンショット） | 年間定額（1 年間何度でも診断可能） |
| その他 | 診断対象／実施時期を自由に決められる<br>年間契約のチケット制あり | コンプライアンスチェック、脅威情報など<br>多数のオプションあり |

### システムのライフサイクルに応じた脆弱性診断の使い分け




Web AP = Web アプリケーション脆弱性診断
プラットフォーム = プラットフォーム脆弱性診断

**サービス担当者からの おススメポイント**

**お客さまのご要望に最適な診断サービスや診断項目、価格プランを提案します。**

**専門家にて高精度な診断を実施し、社内向け報告やシステム構築業者向けの改修サポートなどアフターフォローも充実しています。**

システムの
受入試験や提供判断時
リリース前の脆弱性診断は
エンジニアによる
手動診断がオススメ



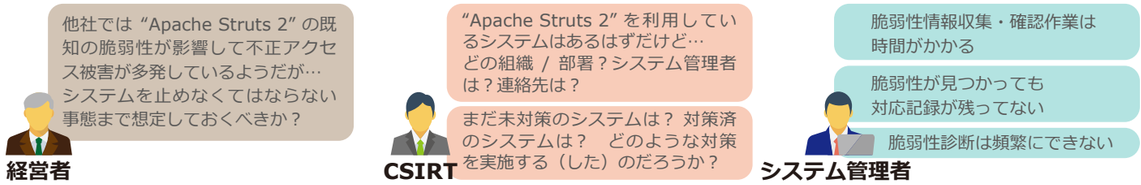


# 脆弱性見える化ソリューション

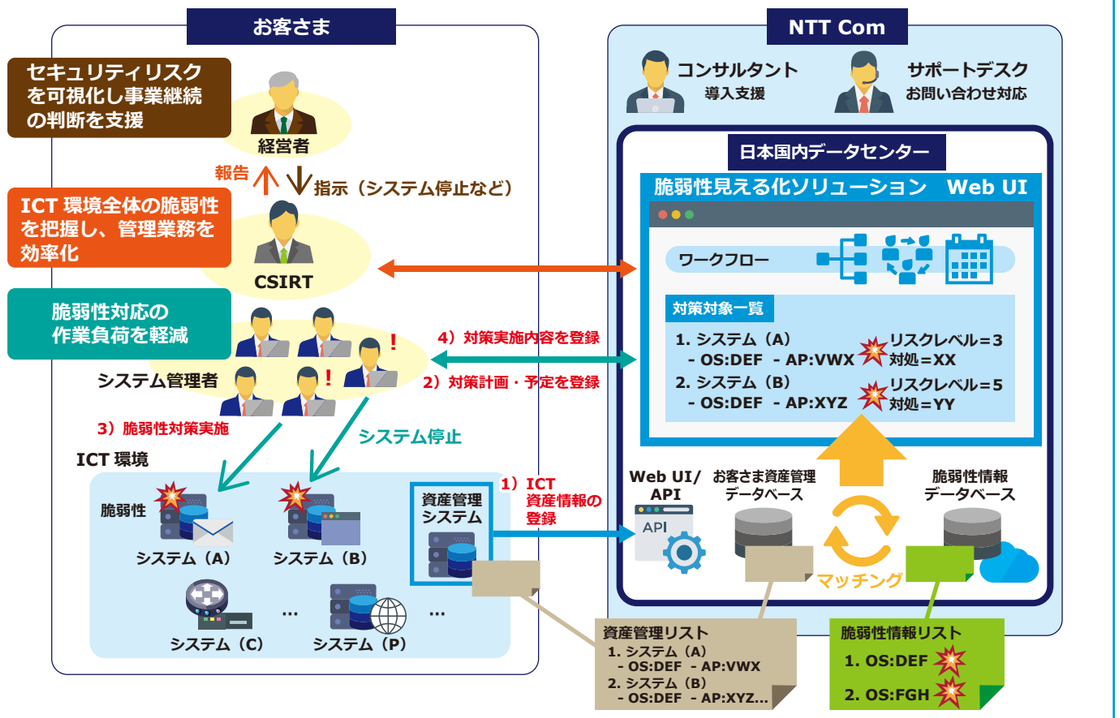
## ICT 環境の事業上の重要性が高まる中、脆弱性リスク対策は経営課題

ICT 環境のセキュリティリスクを「見える化」し、脆弱性対応の効率化や
均質的なセキュリティレベルの確保、情報セキュリティガバナンスの向上を実現します。

### お客さまのシステム脆弱性管理は大丈夫ですか？




### 脆弱性見える化ソリューション（利用イメージ）




1) ICT 資産情報（システム名、ホスト /IP アドレス 、利用ソフトウェア情報等)*1 を 脆弱性見える化ソリューションの Web UI に登録
2) ICT 資産情報と脆弱性情報の照合の結果、対策が必要なシステムが抽出・通知されるため、Web UI に対策計画・予定を登録
3) お客さまにて ICT 資産への脆弱性対策を実施
4) ICT 資産への対策実施内容（ 3. で実施された内容）を Web UI に登録

*1　ICT 資産情報は Web UI、もしくは API でご登録いただけます。

**サービス担当者からの おススメポイント**

**ソフトウェア脆弱性情報の複数利用**
**複数の脆弱性情報ソースの利用**による情報の網羅性と
自動翻訳による日本語情報の迅速な提供を実現します。

**お客さま情報は安心の NTT Com 国内データセンターで管理**
当サービスにおけるお客さま情報は **NTT Com 国内データセンターに配置**し、
お客さま情報管理の信頼性・安全性を確保します。

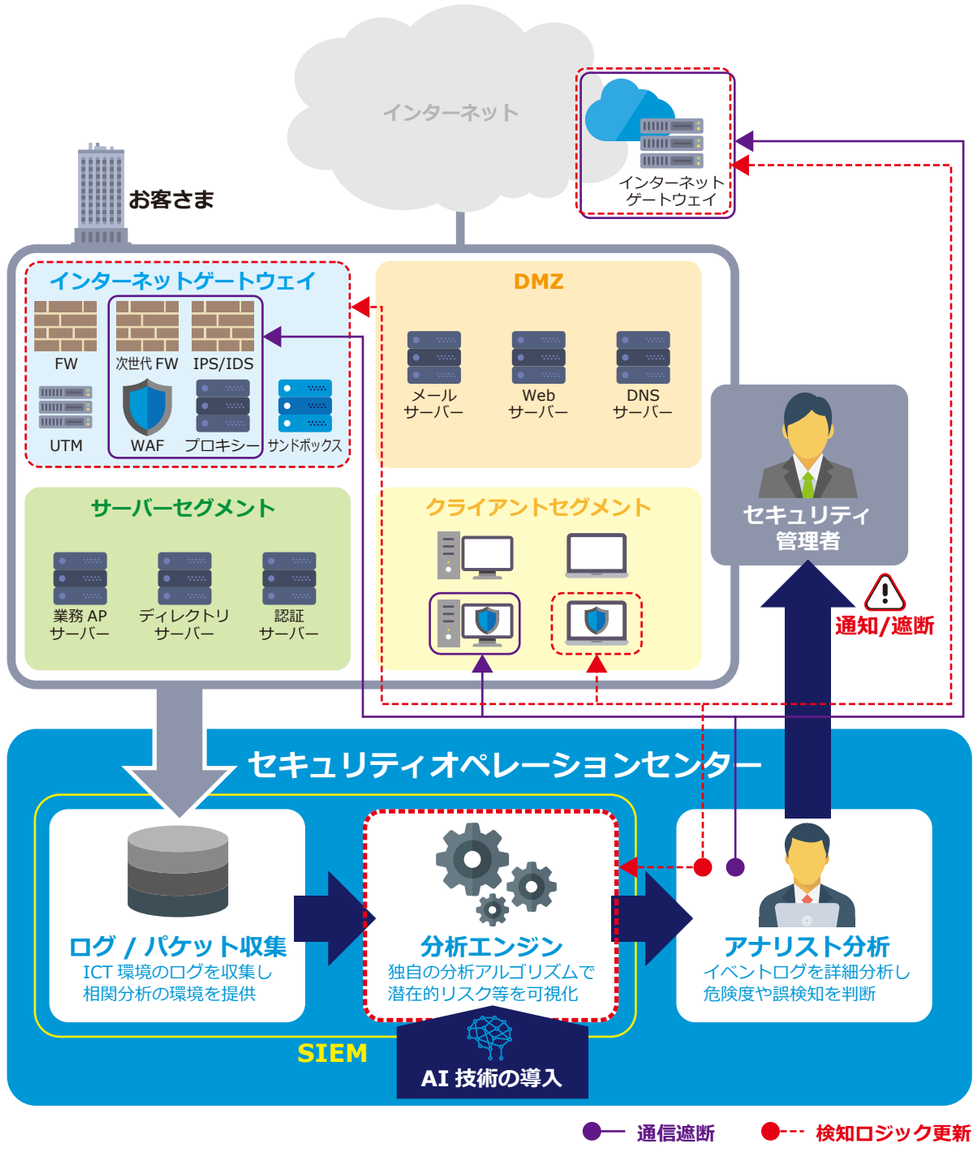
**柔軟な価格モデルの設定**
**初期費用 0 円***2(導入時オプションを除く)、**月額 8,980 円***2／**1 ホスト 1 アカウント**から対応可能
という柔軟な価格モデルの設定によりお客さまのニーズに合わせたご利用が可能です。
また複数年継続してご契約いただく場合は**ボリュームディスカウント**が適用されます。

*2　表示されている価格は税抜きです。

# マネージドセキュリティサービス

## クラウドでもオンプレミスでも お客さまの ICT 環境に応じた 24 時間 365 日のセキュリティサポート

WideAngle のマネージドセキュリティサービスは、世界 16 カ国、1,500 名のセキュリティ専門家により、国内外のオンプレミス、クラウド、ハイブリッドなど様々な ICT 環境に対して総合的なセキュリティソリューションを提供します。SOC のリスクアナリストが 24 時間 365 日の高度なセキュリティ監視を行うことでグローバルシームレスなセキュリティ対策を実現します。




## ●経験豊富なアナリストによる高度分析

SIEM エンジンによる分析に加えアナリストが潜在的なリスクを含めた高度な分析を行います。日常的に攻撃手法などを情報収集し攻撃者の心理を理解してログを注視、数百億件におよぶイベント ログから数十件の真の脅威を発見します。アナリストは独自検知ロジックやカスタム シグネチャーの作成も行い検知精度の向上に努めます。

## ●一連の事象として検知する相関分析

セキュリティ デバイス単体単位の分析だけでなく、IPS/IDS、UTM、WAF、サンドボックス、プロキシー サーバーなど複数のデバイスログを横断で分析し、精度の高い分析を行います。セキュリティデバイスでは検知できない攻撃や、暗号化されたマルウェアによる攻撃なども、プロキシーサーバーのログからイベントの前後の通信の流れを洗出し、外部へのアクセスの証跡を確認することで、実際の攻撃の成否を判断してレポートできます。

## ●独自開発の SIEM エンジン

NTT グループが独自に開発した SIEM エンジンを駆使して脅威のリアルタイム分析を行います。SIEM エンジンでは、攻撃プロセスのロジック化、時系列分析など、複数の独自検知ルールを持ち、精度の高い検知を実現します。また、開発と運用を一体で行う DevOps の体制を取り、運用で発見した新たな脅威をいち早く SIEM エンジンに反映します。

## ●独自のブラックリスト

WideAngle MSS の運用に加え、世界最大級のネットワーク サービス プロバイダーとしての運用で得られるノウハウを活用し、脅威検知のための「独自ブラックリスト」として蓄積しています。国内はもちろん、グローバルでの運用ノウハウも活用して、国内外で異なる傾向を持つ攻撃に備えることができます。

## ●カスタムシグネチャー

セキュリティ デバイスの標準シグネチャーではとらえることのできない脅威検知を可能とするため 、SOC 独自のカスタム シグネチャーを随時作成し、セキュリティ デバイスに適用します。アナリストが高度分析で培った経験、判断力、情報収集力が集積されたものであり WideAngle MSS が提供できる価値となっています。

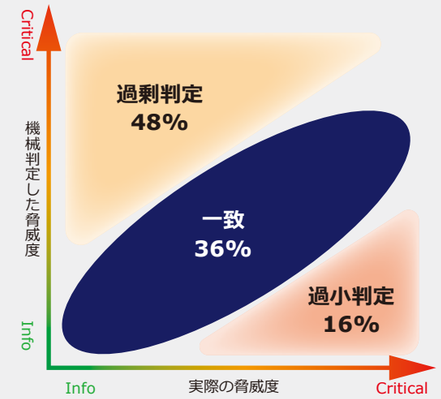
## ●サイバー攻撃の特定に欠かせないコンテンツ分析

通信内容が記録された PCAP ファイルや端末詳細情報が記録されたエンドポイントのログファイルなどを取得し、脅威の詳細を調査します。アナリストは SIEM のセキュリティ イベントを評価します。アナリストは SIEM が処理する前の Raw ログを用いて、また、セキュリティ デバイスから取得された通信内容の詳細（PCAP ファイルなど）がある場合はコンテンツ分析により false positive（誤検知・過検知）を軽減し、あるいは攻撃の成立状況や進行度など脅威の詳細を調査します。

## ●被害を抑止、最小化するレスポンス機能

SOC が収集した「今起きている攻撃」に基づく悪性通信先の URL リスト（ブラックリスト）を常時配信し、攻撃の発生を未然に防止（抑止）する機能を提供します。ブラックリストをプロキシーサーバー等に取込むことで、悪性通信の成立を回避できます。
また、SOC が強みとするアナリスト高度分析の分析結果にもとづき、悪性の通信や侵害された端末の遮断または隔離を、即時かつ能動的な遠隔オペレーションとしてセキュリティ インシデント レポートの提供と同時に自動実行し、当該脅威イベントの被害を最小化します。

### セキュリティ機器の設置だけではサイバー攻撃の検知は 3 割程度

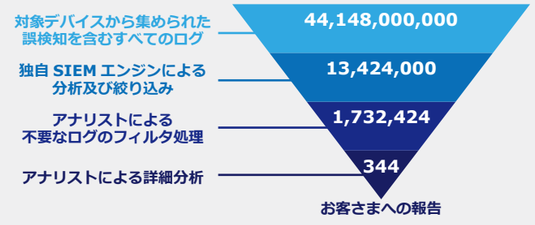



**セキュリティ機器の危険度判定は**
**48% が過剰判定、16% が過小判定**

※東京 SOC における実測に基づく

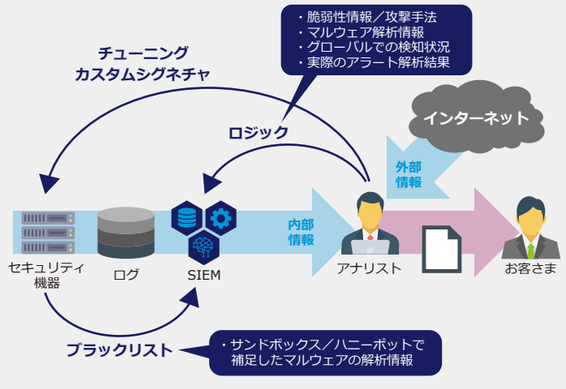
### インシデントを発見するのは億万長者になるよりも難しい

アナリスト高度分析を行っている顧客から集められる総ログ件数は、ある 1 カ月において約 440 億件。この中で実際に危険性があるのは 344 件。440 億分の 344 ーこれは宝くじに当選することよりもはるかに小さい確率です。




※東京 SOC における実測に基づく

### 日々巧妙化するサイバー攻撃を検知し続ける仕組み




**日々の検知ログや分析結果とリサーチで入手した**
**様々なインテリジェンスを活用しシステムにフィードバック**

# オペレーションメニュー

## お客さまのニーズに合わせてオペレーションを追加できる MSS

・オペレーションを選択できる「サービスメニュー」のみ、ここに記載しています。全サービスメニューは、P.7 をご覧ください。
・「サービスメニュー」および「メニュー」は、複数ご利用いただけます。「メニュー」毎に「オペレーション」を選択いただけます。
・「オペレーション」は「脅威検知」が標準提供され、「デバイス管理」と「レスポンス」を組み合わせることができます。*1 一部、例外や留　意事項がありますので、注釈を合わせてご確認ください。

●：ご利用可能なオペレーション
○：具備される機能 *2

### オペレーションメニューを選べるサービス

| サービスメニュー | |
|---|---|
| **ネットワーク セキュリティ** | ・IPS/IDS<br>・ネットワークセキュリティ 基本パック |
| **コンテンツ セキュリティ** | ・コンテンツセキュリティ 基本パック<br>・コンテンツセキュリティ 拡張 A パック<br>・コンテンツセキュリティ 拡張 B パック |
| | WAF |
| **リアルタイム マルウェア検知** | RTMD ONSITE |
| **プロキシー分析** | |
| **クラウド GW セキュリティ** | WSS 基本パック |
| | WSS RTMD パック |
| **エンドポイント セキュリティ** | EDR |

×

### オペレーションメニュー

| 標準オペレーション<br>脅威検知 *1（アナリスト高度分析） | | | | 追加できるオペレーション<br>デバイス管理 *1 *7 | | | 追加できるオペレーション<br>レスポンス | |
|---|---|---|---|---|---|---|---|---|
| | カスタム シグネチャ | 相関分析 | コンテンツ分析 *5 | 監視 | PCR（設定変更） | ライフサイクル管理 | プロアクティブ レスポンス | Active Blacklist Threat Intelligence 連携 |
| ● | ○ *3 | ○ | ○ | | ● | | — | — |
| ● | ○ *3 | ○ | ○ | | ● | | ● | ● *9 |
| ● | — | ○ | — | | ● | | — | — |
| ● | — | ○ | ○ *6 | | ● | | — | — |
| ● | — | ○ | — | | — | | — | ● |
| ● *12 | — | ○ | — | | — | | — | — |
| ● *12 | — | ○ | — | | — | | — | — |
| ● | ○ *4 | ○ | ○ | | ● *8 | | ● *10 | — |

P24

## サポート デバイス

| サービスメニュー | 製品カテゴリー | デバイスモデル |
|---|---|---|
| **ネットワークセキュリティ** | IPS/IDS | McAfee NSP シリーズ |
| | | Cisco ASA with FirePOWER Services シリーズ |
| **ネットワークセキュリティ コンテンツセキュリティ** | UTM（次世代 FW） | Palo Alto PA シリーズ |
| | | Fortinet FortiGate シリーズ |
| **コンテンツセキュリティ** | WAF | F5 BIG-IP シリーズの ASM *11 |
| | | Imperva SecureSphere |
| **リアルタイムマルウェア検知** | サンドボックス | （Web 用）FireEye Network Security |
| | | （E-mail 用）FireEye Email Security |
| **プロキシー分析** | プロキシーサーバー | Bluecoat Proxy SG |
| | | Squid |
| | | i-FILTER |
| | | McAfee Web Gateway |
| | | Forcepoint Websense |
| | クラウド型プロキシー | Zscaler Internet Access |
| **クラウド GW セキュリティ** | クラウド型プロキシー | Symantec Web Security Service |
| | クラウド型プロキシー + クラウド型サンドボックス | Symantec Web Security Service + Malware Analysis Advanced Service |
| **エンドポイントセキュリティ** | EDR | FireEye Endpoint Security |
| | | Windows Defender ATP |

*1 「脅威検知」と「デバイス管理」は、組み合わせにより、ご契約時の区分を「タイプ 1」「タイプ 2」としており、「タイプ 1」は両方、「タイプ 2」は「脅威検知」のみを選択した場合となります。
*2 セキュリティ機器の機種・構成等により提供できない機能がございます。
*3 「デバイス管理」をご契約いただく必要がございます。
*4 製品によりカスタム IOC と呼称される場合があります。
*5 NW セキュリティ及びコンテンツセキュリティ、RTMD では PCAP データ（パケットキャプチャーデータ）の取得、EDR では端末ログの取得による分析となります。
*6 セキュリティデバイスとして、Web 通信を監視する FireEye NX を用いる場合のみサポートします。
*7 NTT Com 経由にてデバイスを調達頂いた場合に限ります。
*8 管理装置が運用上必要な場合、同管理装置向けの監視を致します。
*9 コンテンツセキュリティ基本パックではご利用いただけません。
*10 EDR では、標準オペレーションとして提供されます。
*11「ASM」は F5 BIG-IP Application Security Manager というモジュールを指します。
*12 クラウド GW セキュリティは製品ライセンス及び製品に関するヘルプデスクが標準提供されたサービスとなります。

# ネットワークセキュリティ／コンテンツセキュリティ

## ●ネットワークセキュリティ

ファイアウォールは、送信元と送信先の IP アドレス、プロトコル、ポート番号により通信を制御します。IPS/IDS はネットワーク層やアプリケーション層の脆弱性を突くアクセスを検出してポリシーをもとに検知または遮断を適用します。WideAngle MSS ではそれぞれの機能を単体で、または両方の機能を「ネットワーク セキュリティ基本パック」としてパッケージ提供します。

**【提供サービス】**

**ファイアウォール**

**IPS/IDS**

**ネットワーク セキュリティ基本パック**
ファイアウォール　IPS/IDS

## ●コンテンツセキュリティ

メール /Web アンチウイルスは、お客さま環境のメールと Web の通信から悪意あるソフトウェアを検出しブロックします。URL フィルタリングはプロファイルを定義し、Web ブラウジング ポリシーをもとに通信を制御します。アプリケーション フィルタリングは、アプリケーションと Web コンテンツを識別して通信を制御します。WideAngle MSS では「ネットワーク セキュリティ基本パック」にそれぞれの機能を追加して「コンテンツ セキュリティ基本パック」「コンテンツ セキュリティ拡張 A パック」「コンテンツ セキュリティ拡張 B パック」としてパッケージ提供します。

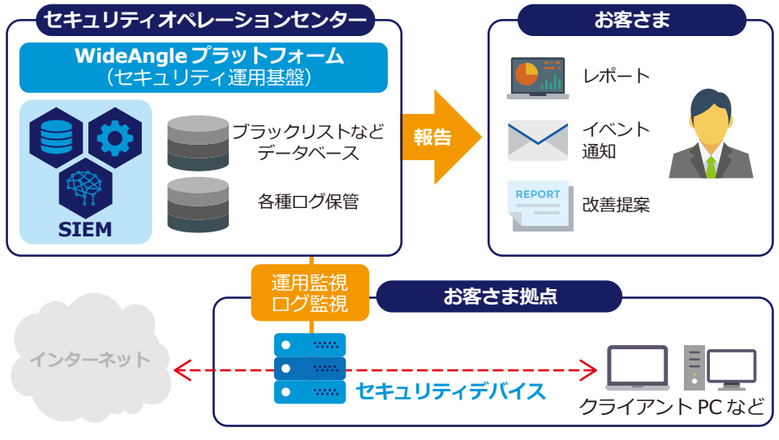
**【提供サービス】**

**コンテンツ セキュリティ 基本パック**
ファイアウォール　IPS/IDS
メール /Web アンチウイルス

**コンテンツ セキュリティ 拡張 A パック**
基本パック
＋
URL フィルタリング

**コンテンツ セキュリティ 拡張 B パック**
拡張 A パック
＋
アプリケーション フィルタリング
RTMD *1

*1 コンテンツ セキュリティの RTMD は、セキュリティ デバイスとして Palo Alto PA シリーズを利用する場合に WildFire を利用して提供可能なマルウェア検知機能です。




**ご利用イメージ**

セキュリティデバイスとセキュリティオペレーションセンターのセキュリティ運用基盤を接続。アナリストが、収集されたアラートやログを分析し、お客さまに通知します。

**サービス担当者からの おススメポイント**

**IPS の Critical アラートの 7 割以上はカスタムシグネチャによる検知！**

| 危険度 | カスタムシグネチャ検知率 |
|---|---|
| Critical | 71.4% |
| Medium | 46.2% |
| Low | 41.7% |

※東京 SOC における実測に基づく

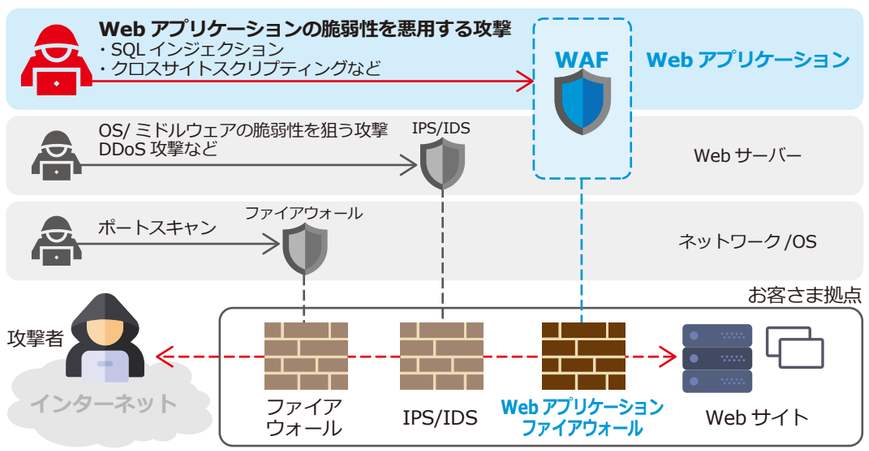
コンテンツ セキュリティの各パッケージは、お客さまの境界ゲートウェイにおける入口・出口対策に最適です！





# WAF（Web アプリケーションファイアウォール）

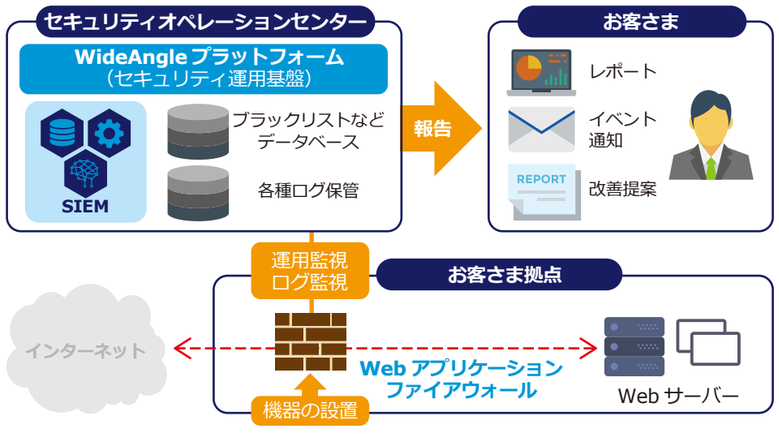
従来のファイアウォールや IPS/IDS で防げなかった Web アプリケーションの脆弱性を悪用した攻撃を検知・防御し、改ざんや情報漏えいを防御、複数の WEB サイト対策を一元的に実施します。





## WAF サービス提供内容

| | |
|---|---|
| **Web アプリケーション保護機能** | ・シグネチャなどの検知ルール（ブラックリスト）を適用し、WAF を通過する攻撃から Web アプリケーションを防御します。<br>・導入時には、お客さまサイトにおける WAF の検知状況に合わせてイニシャルチューニングレポートを提供し、お客さまのポリシー決定をサポートします。 |
| **セキュリティイベント通知とレポート機能** | ・チューニングの結果、危険であると定義したイベントが発生した際にお客さまにメールで通知します。<br>・WAF の Web GUI から、検知ログの内容や、レポート等の情報を閲覧することができます。 |
| **お客さまサポート** | ・検知ログに関するお問い合せやチューニングのご相談など、セキュリティのエキスパートによるサポートを提供いたします。 |




**ご利用イメージ**

WAF とセキュリティオペレーションセンターのセキュリティ運用基盤を接続。最適なチューニングにより Web アプリケーションを保護するとともに、セキュリティイベントの通知やお問合せへの対応を実施します。


**サービス担当者からの おススメポイント**

**多くの運用経験と実績に基づいたノウハウと WAF のエキスパートであるアナリストの分析力を活かし、最適な WAF のチューニングをサポート**

### WideAngle 独自の初期ポリシー *1 *2

お客さま環境への WAF 導入に当たり、多くの運用経験および蓄積されたノウハウに基づいて作成された WideAngle 独自の初期ポリシーを適用します。

### イニシャルチューニング

導入効果を最大化するため、ブロッキングモードを基本としています。経験豊富なアナリストが検知ログを分析し、防御力の最大化と誤検知率の最小化を実現する精度の高いポリシーチューニングを提案します。

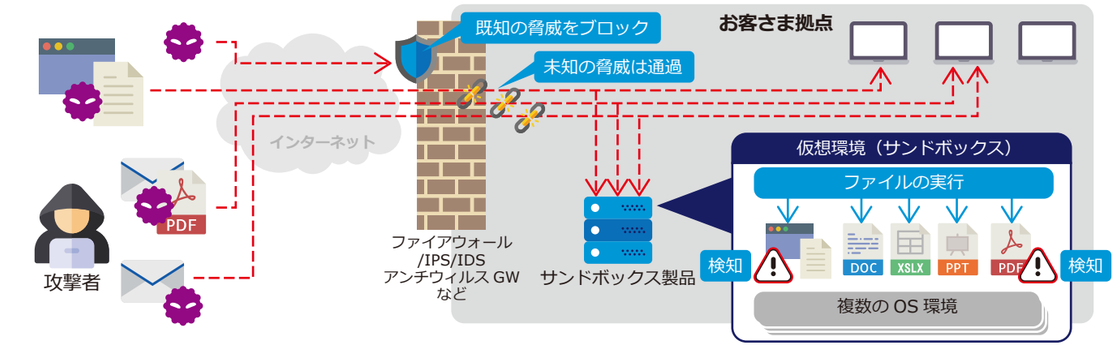
### 運用中のチューニングもエキスパートがサポート

シグネチャーの追加や Web アプリケーションの変更による誤検知を防ぐため、導入後も最適なチューニングを提案します。*3

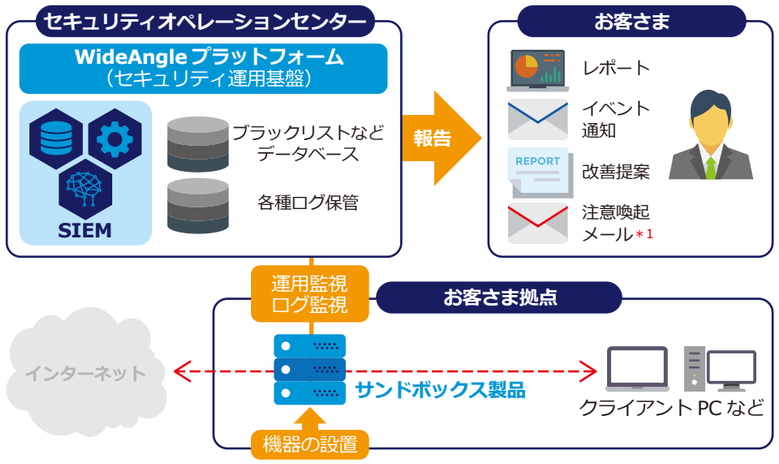
*1 ポリシー：WAF に適用されるシグネチャー、バイオレーションなどの検知ルールのセット　*2 初期ポリシー：検知精度の低い検知ルールを除外したポリシー　*3 別途、費用が必要です。

# リアルタイムマルウェア検知（RTMD ONSITE）

WideAngle MSS の RTMD ONSITE は、Web サイトやメール添付ファイルに潜む、従来のセキュリティ対策では検知できない未知の脅威を検知します。




お客さま環境で利用されている PC の OS を再現したサンドボックスと呼ばれる仮想環境で、疑わしいファイルを実行し、その挙動を監視することで、シグネチャーやパターンが未対応のマルウェアも検知します。




## ご利用イメージ

サンドボックス製品とセキュリティオペレーションセンターのセキュリティ運用基盤を接続。機器のアラートに基づき、SOC はマルウェアの疑いがあるファイルや通信を解析し、お客さまに通知します。

＊1「RTMD E-mail」のオプションサービスとなります。

お客さまの重要情報を狙う未知のマルウェアによる標的型攻撃対策に最適！プロキシとの相関分析がお勧めです！

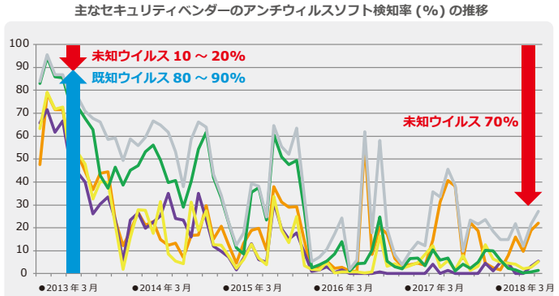
## サービス担当者からのおススメポイント

**統計情報**

**ウイルス生成技術向上によるアンチウイルス検知率の低下**

この数年で検知率が急激に低下しパターンファイルによるウイルス検知の限界に達している

主なセキュリティベンダーのアンチウィルスソフト検知率（%）の推移




※東京 SOC における実測に基づく

**WideAngle は高度なマルウェア判定能力に加えてマルウェア起因による様々な運用を豊富なオプションサービスでサポート**

**検体提供サービス**
検体提供オプションサービスでは、RTMD Web と RTMD E-mail で取得した検体をお客さまが利用する指定ファイル共有サービスへアップロード提供します。

**検体解析依頼代行**
RTMD Web で取得した検体の解析依頼を代行するためのオプションサービスです。お客さまが次の指定ベンダーのアンチウィルス製品を利用している場合に提供可能です。

**注意喚起メール**
RTMD E-mail で悪性の疑いのあるメールの受信を検知した場合、そのメールの受信者に対して注意喚起メールを送信します。また、お客さま管理者など指定の連絡先に対して注意喚起メールの送信対象者のサマリー情報をメールにて報告します。

**リセットパケット送信**
RTMD Web で、インターネット通信から悪性通信を検知した場合、FireEye NX シリーズの機能であるリセットパケット送出機能により、悪性通信を遮断するよう設定することが可能です。

**アプライアンス連携**
RTMD Web では、インターネット通信から検知された悪性通信の通信先を URL 情報リストとして機器上に作成し公開します。この URL 情報リストをお客さまが管理する連携機器が定期的に取り込むことにより、連携機器が悪性通信を遮断するように設定することができます。

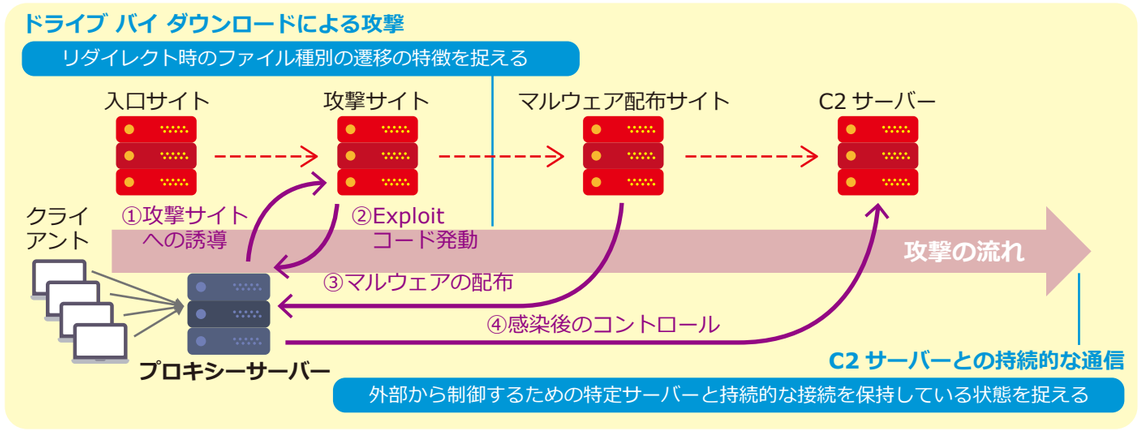


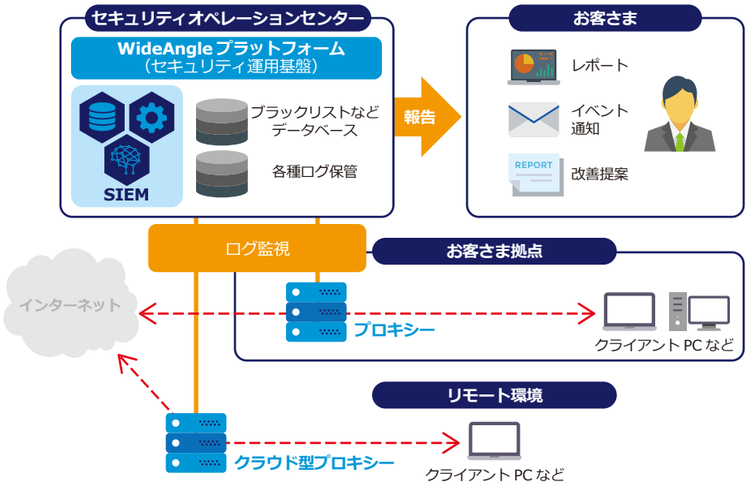


# プロキシー分析

## プロキシーログが重要となる理由

セキュリティデバイスで検知できない攻撃や暗号化されたマルウェアであっても、外部にアクセスする際は必ずプロキシーサーバーに認証が残ります。そのため、プロキシーサーバーのログで外部との通信の痕跡を調べることは、リスクのある通信を特定して、サイバー攻撃と判断するのに大変有効です。




## ご利用イメージ

プロキシーとセキュリティオペレーションセンターのセキュリティ運用基盤を接続。外部へのアクセスの証跡を解析し、攻撃の成否を判断して、お客さまに通知します。

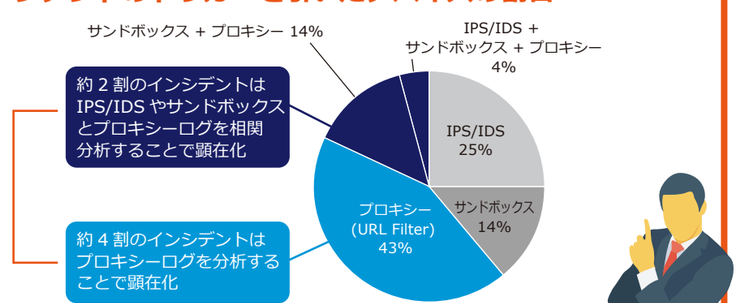
NTT Com ならではのアナリスト高度分析を活用できるプロキシー分析は他社 MSS をご利用のお客さまにもご導入いただけます！

## サービス担当者からのおススメポイント

**脅威検知において Critical インシデントのトリガーを引いたデバイスの割合**

**約6割**

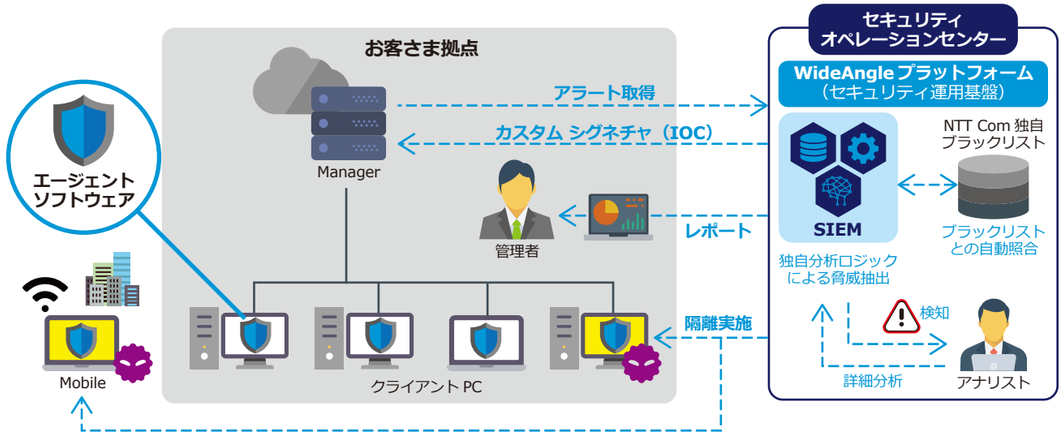
プロキシー分析だけで全体の約 4 割を占め、プロキシーを含む相関分析で全体の約 6 割の脅威を顕在化




※東京 SOC における実測に基づく

# エンドポイントセキュリティ（EDR）

EDR（Endpoint Detection and Response）は、エージェントがインストールされたエンドポイント（端末）で検知される情報を分析し、脅威と判断される場合は、SOC からの指示により端末をネットワークから即時隔離します。エンドポイントの分析にあたっては、SOC 独自の知見で作成したカスタム シグネチャーをエージェントに適用して脅威を早期に検知できることに加え、他のセキュリティメニューのログとの相関分析により、より精度の高い分析が可能です。



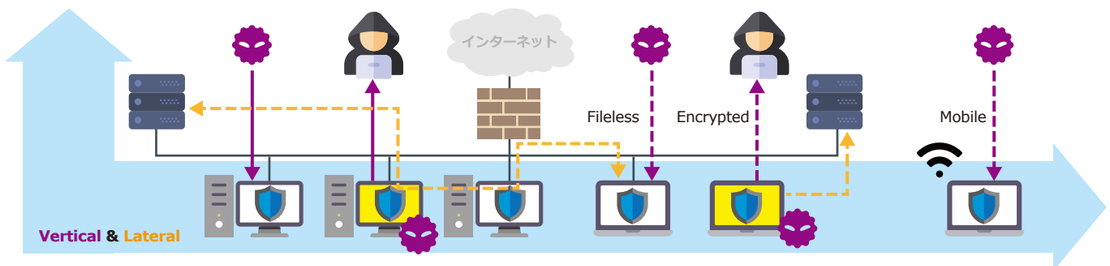

**エンドポイントセキュリティを強化**

- ランサムウェアや脆弱性を悪用した攻撃から PC 端末（エンドポイント）を保護
- 侵害された PC 端末を隔離し、被害拡大を抑制
- ICT 環境上の脅威を調査し、侵害内容を把握
- 通信経路上では難しい SSL 通信の脅威検知も可能

## サービス担当者からの おススメポイント

### エンドポイントの脅威分析と相関分析の必要性

EDR は、モバイル端末を含むエンドポイントで起きているアクティビティ（ファイルやプロセスの挙動、レジストリ変更、通信情報など）を自動的に保存することができるだけでなく、サイバーキルチェーンの一連の攻撃プロセスを関連付けて調査のスピードアップや正確性の向上、拡散範囲の特定などに極めて有効です。また、暗号化／難読化された通信やファイルレスマルウェア（- - ▶）、感染拡大（- - ▶）など、エンドポイントでしか見つからない不正なアクティビティを独自に検知することや、強制停止や遮断、無効化するコントロールも可能です。




さらに、EDR と合わせてこれまでの GW セキュリティ対策製品のログと合わせて分析を行うことにより、効果的に既知の脅威やばらまき型の攻撃を防御しつつ、標的型攻撃のように未知の脅威に対しても対策をとることができます。

### NTT Com はここが違う！

- SOC 独自のカスタム シグネチャ (IOC) にて、いち早く、より深い脅威の検知が可能
- WideAngle MSS の他のサービスと組み合わせた相関分析でより精度の高い分析が可能 *1
- 被害状況の本格的な調査（インシデントレスポンス*1）が可能

**最適な EDR 製品を選択可能**

- FireEye Endpoint Security
- Windows Defender Advanced Threat Protection (ATP) など

*1 別途契約が必要です。

エンドポイントの
脅威分析に加え、隔離
（プロアクティブ レスポンス）
により、被害拡大を抑制！
IPS やプロキシとの
相関分析がお勧め！

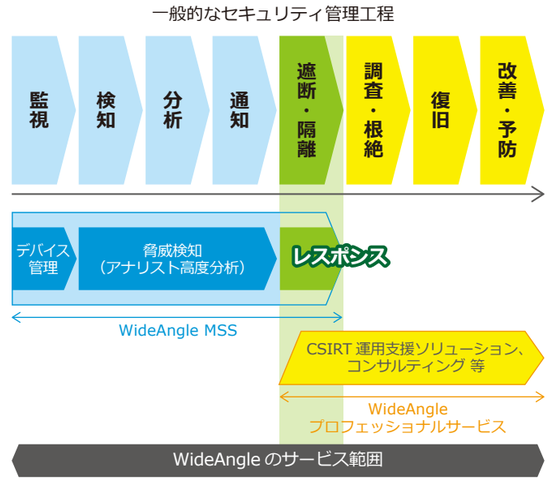


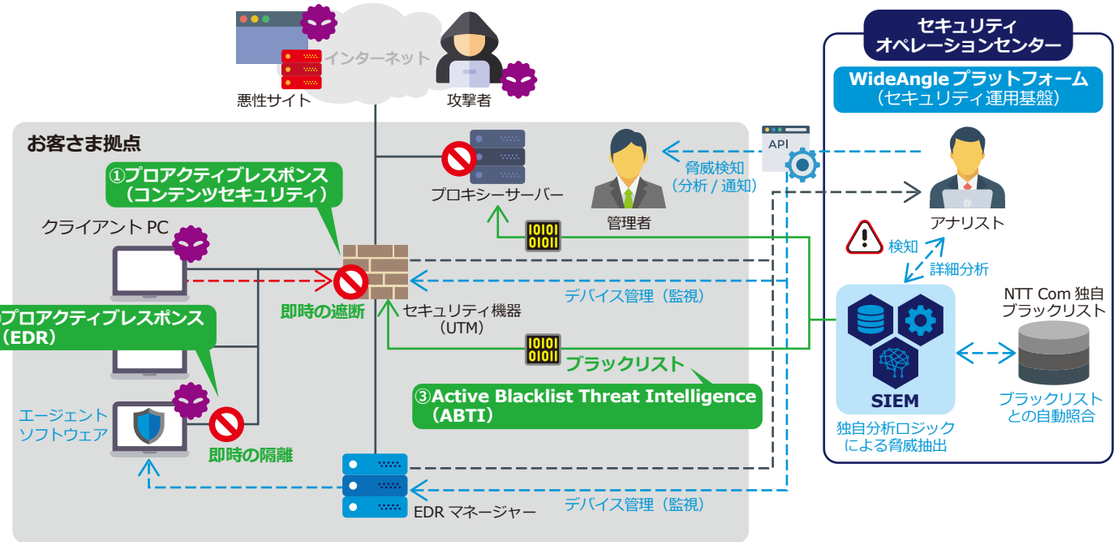


# WideAngle MSS ご利用時のお役立ち機能：レスポンス（MDR）

## 迅速・的確なレスポンス（MDR）で、サイバー攻撃の被害を抑止、最小化

近年の巧妙化するサイバー攻撃を背景に、悪性通信の遮断およびマルウェア感染端末の隔離など、従来お客さま主導の対応領域の一部までサービスの共通化範囲を広げたいというニーズに対して、WideAngle MSS は適用範囲を遮断・隔離の工程の一部まで拡大しました。
WideAngle MSS のレスポンスは、お客さまがサイバー脅威に侵害された後の被害を最小化するプロアクティブレスポンスと、SOC が収集した「今起きている攻撃」の情報をもとにお客さまの被害を未然に防止する Active Blacklist Threat Intelligence（ABTI）との 2 つのメニューをご提供します。




### プロアクティブレスポンス

**①プロアクティブレスポンス（コンテンツセキュリティ）*1**
アナリストの分析にもとづき悪性と判断された外部への通信を
ゲートウェイで即時に遮断し、被害を最小化

**②プロアクティブレスポンス（EDR）*2**
アナリストの分析にもとづきマルウェア侵害が確認された
端末をネットワークから即時に隔離し、被害を最小化

### ABTI

**③Active Blacklist Threat Intelligence（ABTI）*3**
SOC が収集した「今起きている攻撃」の悪性通信の
URL リスト（ブラックリスト）をプロキシーサーバー等に配信し
攻撃の発生を未然に防止

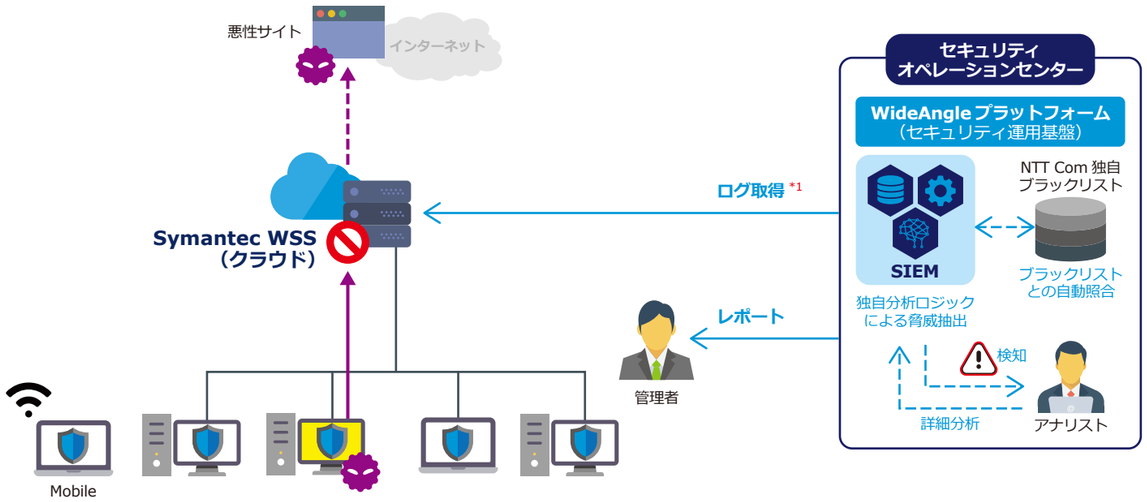
*1 コンテンツセキュリティのオプションサービスとして提供します。
*2 EDR の標準機能として提供します。
*3 コンテンツセキュリティ及びプロキシー分析のサポートデバイス向けにご契約・配信可能です。

### MDR（Managed Detection and Response）とは

MDR は近年、巧妙化しているサイバー攻撃に対し、侵入されないセキュリティだけではなく、侵入された脅威を迅速に検知しいち早く対応するためのセキュリティを実現するための対策として提供され始めた新たなマネージドセキュリティサービスです。

# クラウド GW セキュリティ

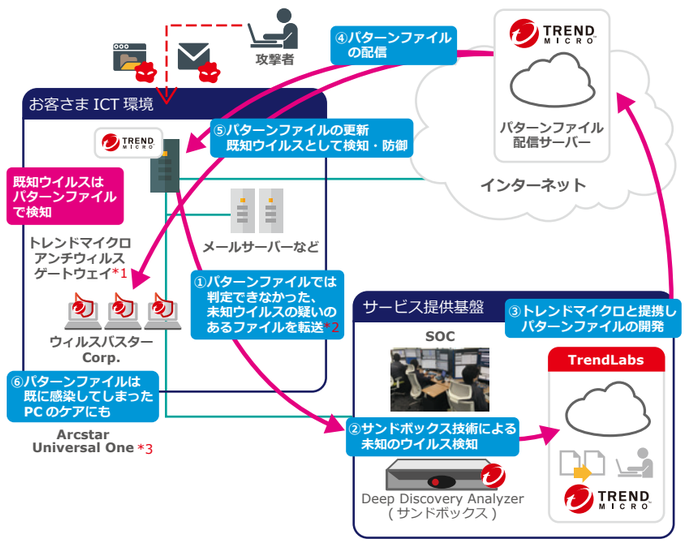
政府による働き方改革の推進、無線ネットワークの拡充など、モバイルワークスペースの充実により、企業ネットワーク外でも働くことができる機会が増える一方、これまで取り組んできた企業ネットワークのセキュリティ対策に逆行するとして、PC のモバイル利用に躊躇しているお客さまに、クラウド型プロキシーと高度分析をセットにした、「クラウド GW セキュリティ」を提供します。




*1 利用ユーザー数によっては専用設備が必要になります。

# Cloud base RTMD

メールの添付ファイルや Web サイトに潜む未知のウイルス、標的型攻撃に対し、侵入検知から分析、防御、駆除までを完全自動化し、システム管理者の負担を増やすことなく、ICT 環境のセキュリティ対策を強化できます。




**Point 1**

**高価なサンドボックスの購入不要！**
**SaaS 型サンドボックスサービスを提供**

- ネットワーク経由でサンドボックスが利用可能！
- お客さまの事業規模に応じたサービス利用可能！
- SOC による 24 時間 365 日の運用を提供！

**Point 2**

**出入口対策のゲートウェイと連携防御**

- トレンドマイクロのメール /Web ゲートウェイ製品とサンドボックスが連携することで隔離と解析が可能！
- ブラックリストによるブロック！

**Point 3**

**未知ウイルスの侵入検知から分析・防御までを迅速かつ一元的に提供**

- マルウェアやウイルスの検知→パターンファイル作成→駆除までの一連のサイクルを自動化
- システム管理者の負担を軽減

※1 C2 サーバーリストダウンロード機能
※2 トレンドマイクロのゲートウェイ製品で、未知ウイルスの可能性があると判定されたファイル
※3 本サービスには監視回線が含まれておりませんので別途契約が必要です。L3 接続、Cloud-GW 接続オプションが必要です。

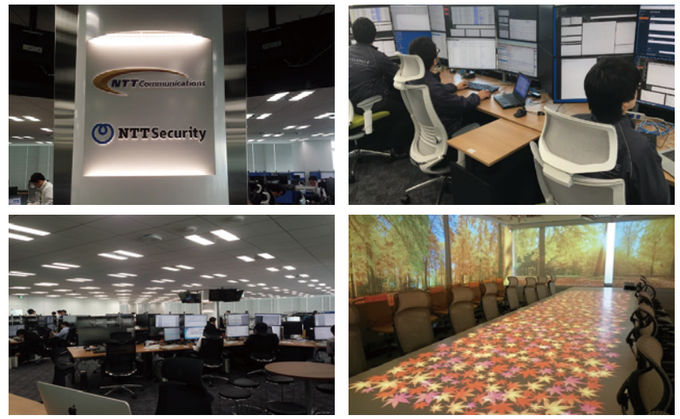
**Cloud base RTMD ゲートウェイ（トレンドマイクロ製品 / お客さま設備）対応機種についてはお問い合わせください。**





# 東京 SOC の紹介

2003 年に設立された東京セキュリティオペレーションセンター（東京 SOC）は、NTT Com および NTT セキュリティのノウハウと、NTT セキュアプラットフォーム研究所の先端技術を融合しセキュリティサービス基盤を高度化しながら、お客さまに信頼されるトータル ICT アウトソーシングサービスをグローバルシームレスに提供し、安心・安全なお客さまの ICT 環境を実現しています。




## 東京 SOC の歩み

**2003 年**
NTT コミュニケーションズ
セキュリティオペレーションセンター設立

**2009 年**
Integralis
買収

**2010 年**
Secode
買収

**2011 年**
Integralis、
Secode 会社統合

**2012 年**
運用基盤統合

**2013 年**
**NTT Com Security**
**設立**

**2016 年 8 月**
**NTT セキュリティに**
**グループのリソースを統合**

**2016 年 11 月**
東京 SOC 移転

**Integralis**
**設立：1988 年**
（事業内容）フルレイヤーセキュリティサービスの構築・運用
（実績）欧米を中心に、業種を問わない豊富な実績

**Secode**
**設立：1986 年**
（事業内容）セキュリティコンサルティングおよび、MSS の提供
（実績）官公庁および金融業を中心に豊富な実績

NTT Com Security
↕ 協力
NTT セキュア
プラットフォーム
研究所

## お客さまに安心、納得してもらえる東京 SOC 見学も随時行っています。

**来場社の業種**

製造 / 物流 / サービス / 文教 / 宗教 / 医療
官公庁 / 金融 / その他

**お客さま来場時の主な役職**

代表取締役社長 /CISO 執行役員
/CSIRT 室長 / センター長 / 博士 / 部長　他

**お客さまの主な見学目的**

・導入判断の最終確認
・最先端技術や他社同行の調査
・お客さまの上司へのセキュリティ啓蒙
・セキュリティ対策に関するお悩みのご相談

**見学時のお客さまコメント**

セキュリティの**プロに任せる必要性**を強く感じた
自分たちでは何年かかっても**この体制は作れない**
導入の**最終決断のフォローに十分な内容**だった
**リスクマネジメント体制の一助として期待**できる
次回、**上司を連れてくる**ので同じ話をしてほしい

@NTTSec_JP　**Twitter でも随時セキュリティ情報を発信中**

東京 SOC の見学については、お客さまの営業担当までお気軽にお問い合わせください。

# 多層防御における 3 つのポイント

## 入口（出口）のリスク対策
## ① インターネットゲートウェイのセキュリティ対策

標的型攻撃など未知の脅威に世界がさらされる中、インターネットゲートウェイのセキュリティ対策には、脅威の侵入を阻止するための複合的で多層的な防御が求められます。

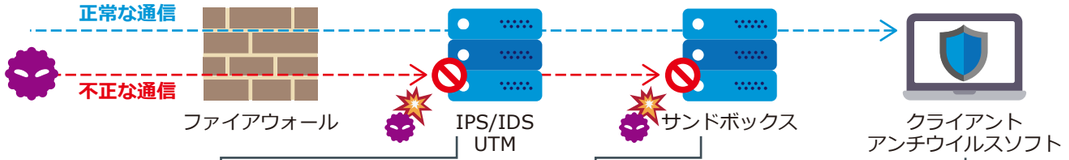
かつて、企業のセキュリティ対策の定番はファイアウォールとアンチウイルス（ウイルス対策）とされていた時期がありましたが、現在はそれだけでは不完全です。

ファイアウォールは送信元と送信先の IP アドレス、プロトコル、ポート番号により通信を制御しますが、複雑な攻撃パターン、あるいは未知の脅威への対策としては不十分ですし、エンドポイントのアンチウイルス製品は既知のマルウェアを検出しますが、エンドポイントで使用している OS やソフトウェアに脆弱性が存在する場合、ファイアウォールを適切に設定し、クライアントを要塞化しても悪意ある攻撃を防ぐことはできません。

このため IPS/IDS や UTM、サンドボックス製品を加えた多層的な対策が求められるのです。

IPS/IDS や UTM はネットワーク層やアプリケーション層のトラフィックを検出します。サンドボックスは本番環境から隔離された領域上で疑わしいファイルを実行して挙動を調べ未知のマルウェアも検出します。

《インターネットゲートウェイの多層的なセキュリティ対策》




**●主な対策対象となる攻撃**
- OS、ミドルウェアの脆弱性を突く攻撃
- 既知のマルウェア送付
- 攻撃サーバーとの通信

**●IPS/IDS、UTM の対策**
- シグネチャー情報に基づき通信可否を判断
- URL フィルタリング機能で悪性 URL の通信をブロック

P19

**●主な対策対象となる攻撃**
- **未知**のマルウェア送付

**●サンドボックスの対策**
- 仮想 PC 環境においてマルウェアを実行し挙動を監視したうえで白黒を判断

P21

**●主な対策対象となる攻撃**
- **既知**のマルウェア送付

**●クライアントアンチウイルスソフトの対策**
- パターンファイル情報に基づき白黒を判断

**WideAngle MSS でサポートする 主な IPS/IDS 製品**

McAfee Network Security Platform（McAfee NSP）シリーズ

Cisco ASA with FirePOWER Services シリーズ

**WideAngle MSS でサポートする 主な UTM・次世代 FW 製品**

Palo Alto PA シリーズ

Fortinet FortiGate シリーズ

## 外部に晒されるリスク対策
## ② 公開サーバーのセキュリティ対策

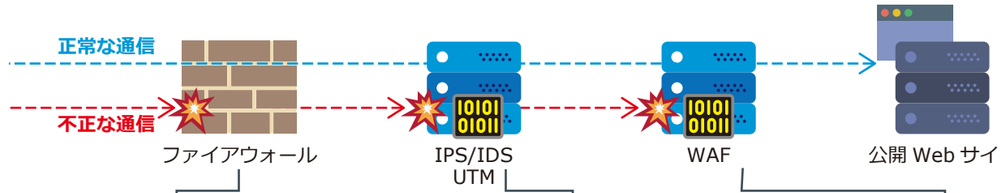
標的型攻撃など未知の脅威に世界が晒される中、公開サーバーのセキュリティ対策には正常な通信を阻害せず不正な通信を阻止するための複合的で多層的な防御が求められます。

Web サイトを公開する場合、利用しているサーバー OS、ミドルウェア、Web アプリケーションの設定不備、脆弱性を修正するパッチが適用されていないなど、サーバー側に脆弱性が内在している場合はファイアウォールを適切に設定しただけでは悪意ある攻撃を防ぐことはできません。このため公開サーバーのセキュリティ対策には、IPS/IDS（UTM 含む）、WAF を加えた多層的な対策が必要になるのです。

IPS/IDS はシグネチャー情報をもとに OS やミドルウェアの既知の脆弱性を突く攻撃を検出します。WAF はシグネチャー情報とアプライアンス製品ごとの独自の技術で、SQL インジェクションやクロスサイトスクリプティングなど Web アプリケーションへの脆弱性攻撃を検出します。

また、各セキュリティ製品を導入する前に脆弱性診断を実施して、脆弱性を発見・修正することも有効な対策です。

《公開 Web サーバーの多層的なセキュリティ対策》




**●主な対策対象となる攻撃**
- ポートスキャン攻撃

**●ファイアウォールの対策**
- 解放 / 閉塞ポート情報を踏まえ通信可否を判断

**●主な対策対象となる攻撃**
- **OS、ミドルウェア脆弱性攻撃**（市販ソフトウェアへの攻撃）

**●IPS/IDS、UTM の対策**
- シグネチャー情報にもとづき通信可否を判断

**●主な対策対象となる攻撃**
- **SQL インジェクション、クロスサイトスクリプティング攻撃など**（Web アプリケーションへの攻撃）

**●WAF の対策**
- シグネチャー情報および、IP レピュテーション情報にもとづき通信可否を判断

P20

**WideAngle MSS でサポートする 主なサンドボックス製品**

FireEye Network Security シリーズ
FireEye Email Security シリーズ

**WideAngle MSS でサポートする 主な WAF 製品**

F5 BIG-IP シリーズ ASM
(F5 BIG-IP Application Security Manager)

Imperva SecureSphere WAF シリーズ

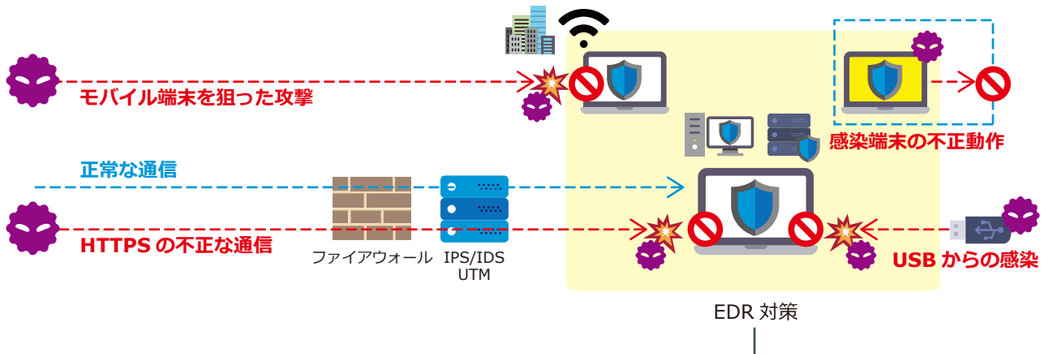
# 多層防御における 3 つのポイント

## 端末や侵入後のリスク対策
## ③ エンドポイントのセキュリティ対策

エンドポイントセキュリティ（EDR）とは、サーバーや PC など、お客さま社内ネットワークに接続された端末（エンドポイント）をサイバー攻撃から守るセキュリティ対策を指します。

インターネット経由ではない USB メモリーなどを介したマルウェア感染や、モバイル端末を狙う攻撃、あるいは HTTPS などゲートウェイで解読できない手段を用いた攻撃などに対しては、IPS/IDS や UTM などゲートウェイのセキュリティ対策だけでは対処できません。マルウェアが最終的に着弾し動作するエンドポイントでのセキュリティ対策が必要となります。

《端末（エンドポイント）の多様なセキュリティ対策》




**●主に未知の脅威への対策に限った場合の EDR の対策**

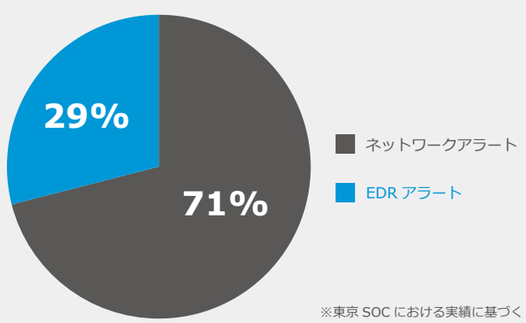
- シグネチャーマッチング型の従来型アンチウイルス機能
- ふるまい検知型の次世代アンチウイルス機能
- マルウェア感染前の状態まで復旧を行う機能
- マルウェア感染した端末をネットワークから即時隔離する機能
- マルウェア感染した端末に対する詳細フォレンジック
- マルウェア感染だけでなく、ユーザーの不審な動作まで検知・評価する機能

P23

### APT 攻撃の検知からみた EDR の有効性

プロキシー ,IPS, サンドボックス等のネットワークセキュリティ製品のアラート、EDR 製品のアラートを SOC で分析しているお客さまにおける、一年間の APT 関連の通知レポート総数に対するアラートソースの割合では、3 割が EDR 製品によるものとなっています。

つまり、**APT のような高度な攻撃のうち、3 割は EDR 製品を入れていないと気が付くことができない**ということを意味しており、EDR の有効性を示しております。



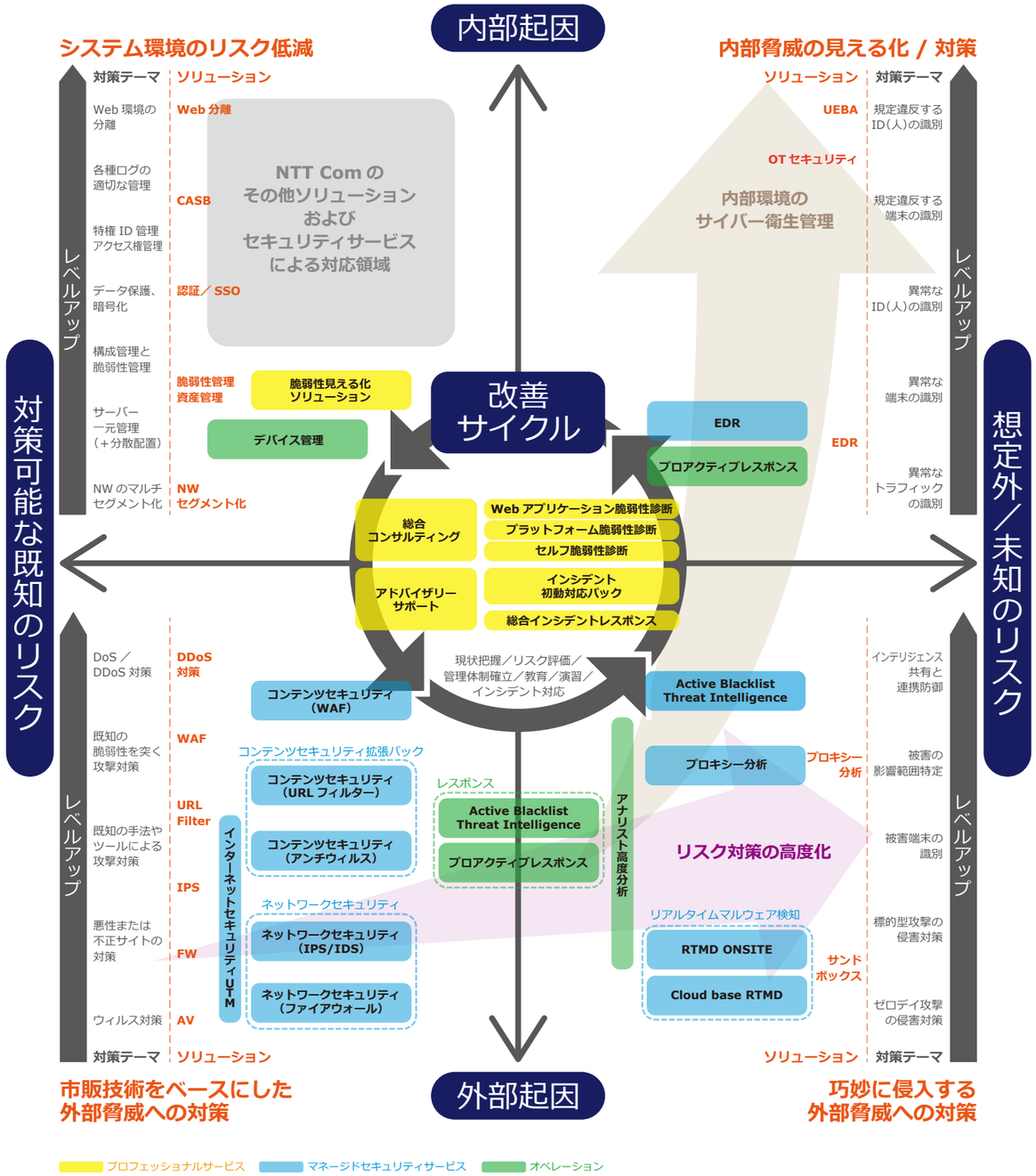

※東京 SOC における実績に基づく



# 付録① WideAngle ポートフォリオ

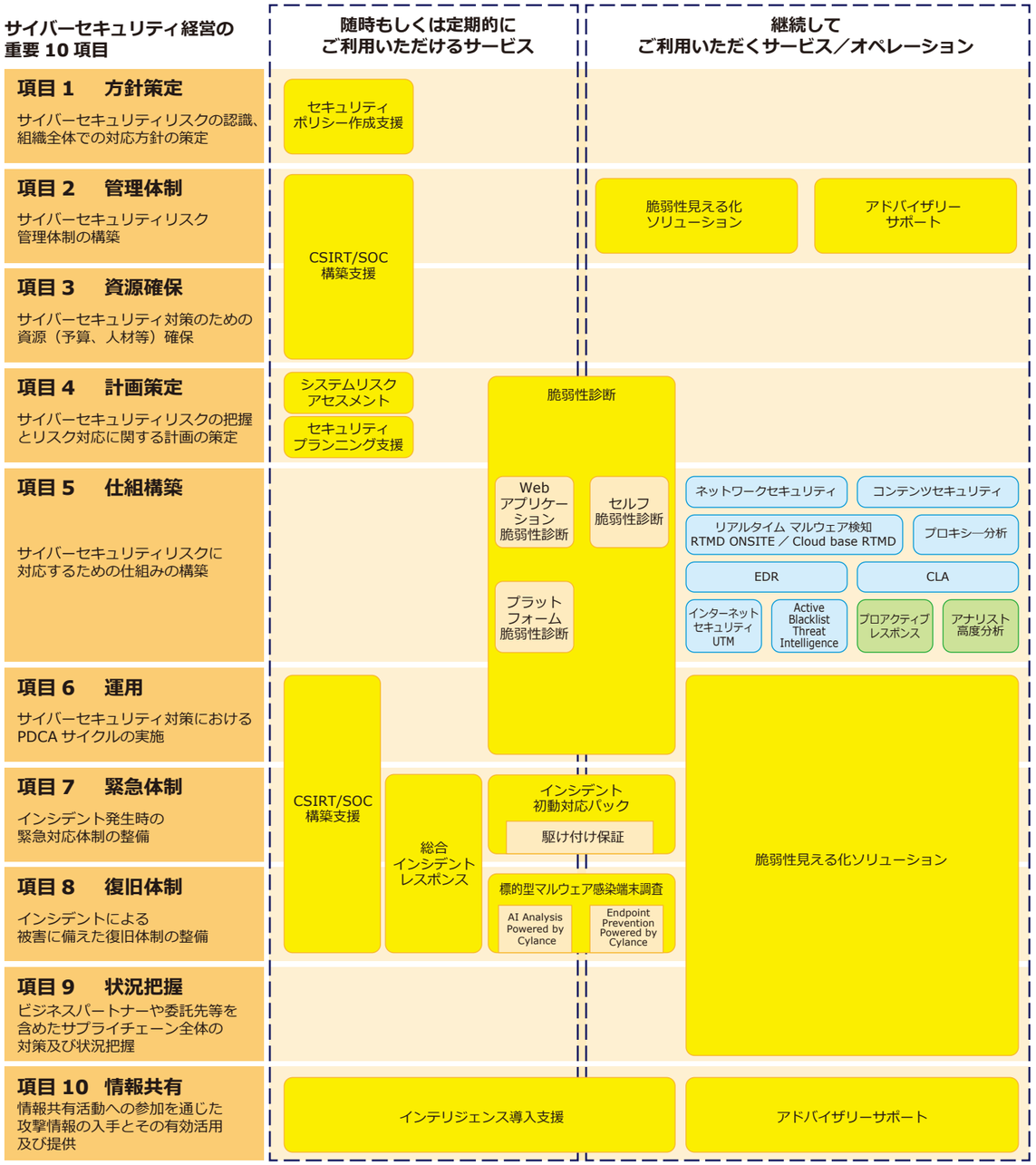
企業を狙う脅威を整理すると、その起点により「内部起因」と「外部起因」に、また脅威レベルに応じ「対策可能な既知のリスク」と「想定外 / 未知のリスク」に分類できます。そして、これらの 4 象限で作られるマトリックス領域ごとに、それぞれ「システム環境のリスク低減」「市販技術をベースにした外部脅威への対策」「巧妙に侵入する外部脅威への対策」「内部脅威の見える化 / 対策」といった具体的な対策が求められます。さらに、全ての象限に共通し、対策を束ねる存在として中核に「セキュリティ改善サイクル」があります。WideAngle は、４象限マトリックスの全領域に対して、包括的な支援ポートフォリオを形作っています。

**【企業におけるセキュリティ対策の全体像と WideAngle のサービス提供領域】**



# 付録② WideAngle を活用したセキュリティ対策

経済産業省の「サイバーセキュリティ経営ガイドライン Ver 2.0」は、IT を活用するほぼすべての企業経営が取り組むべきサイバーセキュリティの指針を実行ベースでまとめたものです。ガイドラインでは、企業のビジネスと収益性向上に不可欠な IT の利活用を脅かすサイバー攻撃のリスクと戦うために、経営者とセキュリティ対策の責任者が認識し、実行すべき 10 の項目が提示されています。WideAngle は、これらの 10 項目を企業が実践するために必要なサービス、ソリューションを網羅し、企業のサイバーセキュリティ経営への取り組みを強力に支援していきます。






# 付録③ 産業用制御システム向けサイバーセキュリティソリューション

## 産業用制御システムを防御するサイバーセキュリティソリューションを提供

### 産業用制御システムはセキュリティ対策の必要性が高まっている！

- 重要インフラを狙うサイバー攻撃の増加
- 生産ラインでのランサムウェアによる実被害発生
- 国際的な大規模イベントを狙うサイバー攻撃リスク

しかし、現状は・・・

- 現状の制御システムの構成が把握できていない
- サポート切れの OS を使用しているケースが多い
- 制御システムがインターネットと接続されている
- セキュリティパッチが適用できず脆弱性が放置されている
- 制御システムのセキュリティはほぼ実装されていない
- 設備ベンダー作業員の持ち込み PC を管理できていない

## NTT セキュリティが産業用制御システムのセキュリティ対策を支援します！

### 制御システムとセキュリティリスクの可視化

お客さまの制御システムの状況を調査し、内在するセキュリティリスクのアセスメントを行います。

### 制御システムのセキュリティ対策計画策定

リスクアセスメントの結果に基き、制御システムの実態に見合った効果的な対策計画を策定します。

### 制御システムのセキュリティ監視・遮断

お客さまに代わって制御システムを常時監視し、サイバーセキュリティ攻撃からシステムを守るお手伝いをします。

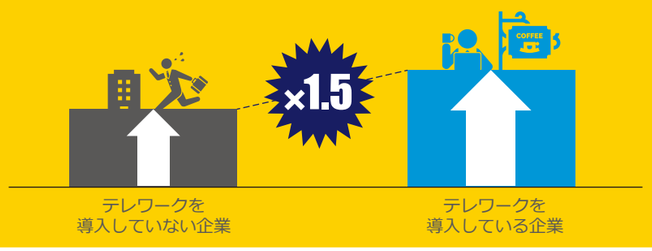
# 付録④ 自由な働き方とセキュリティの両立を ー モバイルワークスペースソリューション ー

## 「働く」を、もっと自由に快適に。まだ、ひとつの場所に縛られていませんか。

**働き方改革推進企業だからわかる長年の経験とノウハウで、お客さまに 最適な ICT の活用方法から導入後の支援まで一元的にご提供します。**

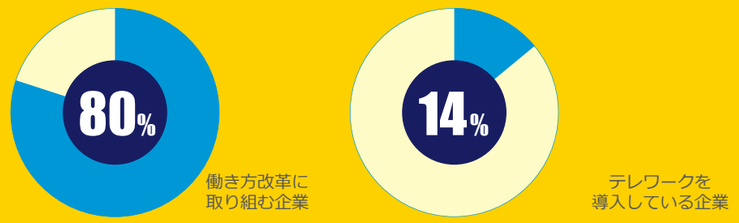
### テレワークは生産性向上につながる！

テレワーク導入済み企業の生産性は未導入企業の **約 1.5 倍**



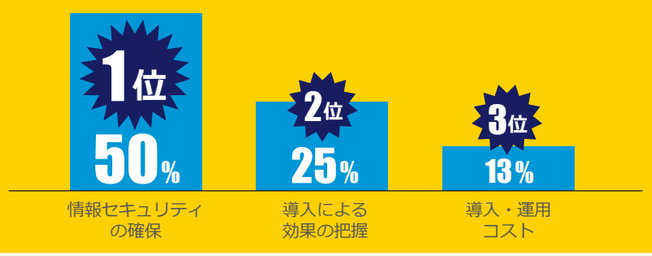

### テレワークの導入はこれから・・

テレワークを導入している企業はわずか **14%**




### 課題はセキュリティ！

テレワーク導入にあたっての課題第 1 位は **セキュリティ確保**




出典：総務省情報通信白書

“働くをもっと自由に快適に”
モバイルワークスペースソリューション の動画はこちら

**いつでもどこ でも使える**

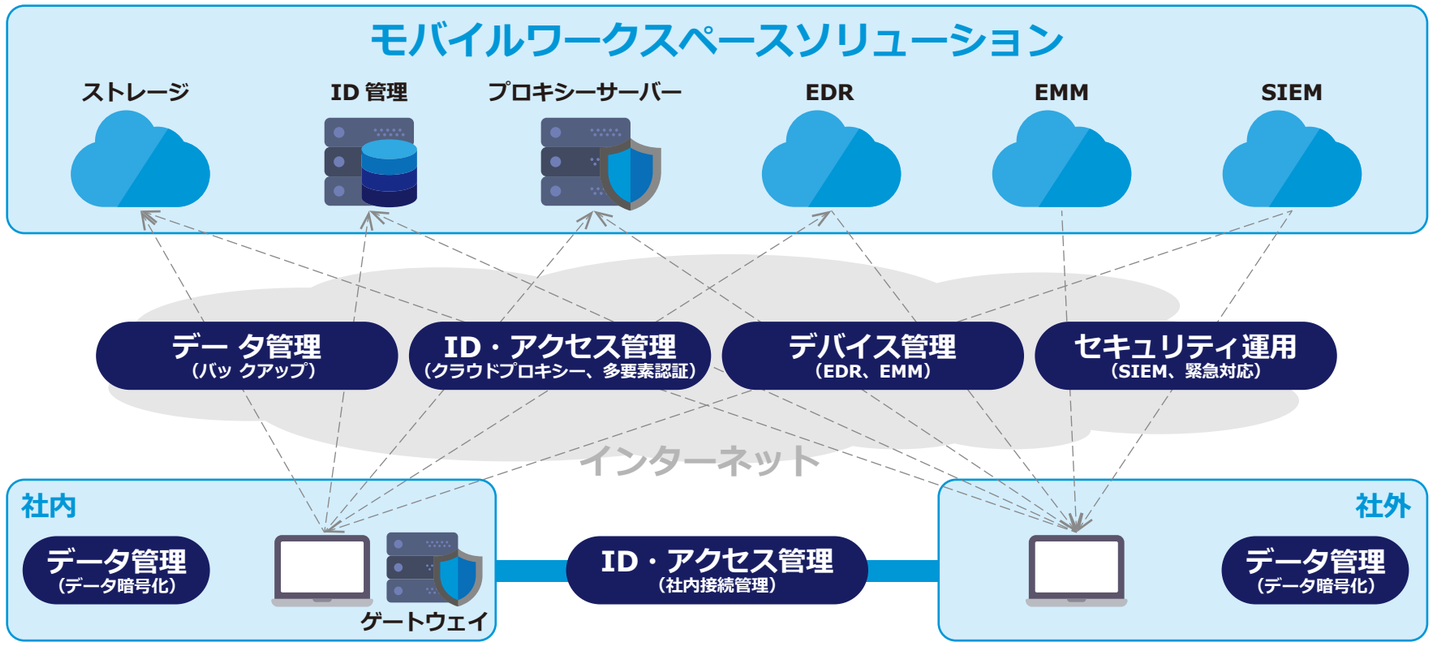
海外出張や飛行機 での移動中も
ネットワークに依 存せず作業可能
場所にとらわれな い働き方を実現

**限られた時間を効率的に**

セキュリティに守られた端末で
安全なコミュニケーションを可能に
すきま時間も有効活用

**仕事と生活の両立**

プライベートの充実が仕事の活力に
自宅がそのままオフィスになるので
業務の支障なく両立が可能




- ■データ管理　PC のデータ暗号化、バックアップ（持ち出し情報管理）
- ■ID・アクセス管理　社内接続管理、クラウドプロキシー・多要素認証
- ■デバイス管理　EDR（未知なる脅威への対応）、EMM（統合モバイル管理）
- ■セキュリティ運用　SIEM（ログ高度相関分析）、緊急対応