

NTT-ATの5つのビジョン。



# 最近のセキュリティ脅威動向と、 対抗するセキュリティソリューション

2019年11月7日

NTTアドバンステクノロジ  
セキュリティ事業本部

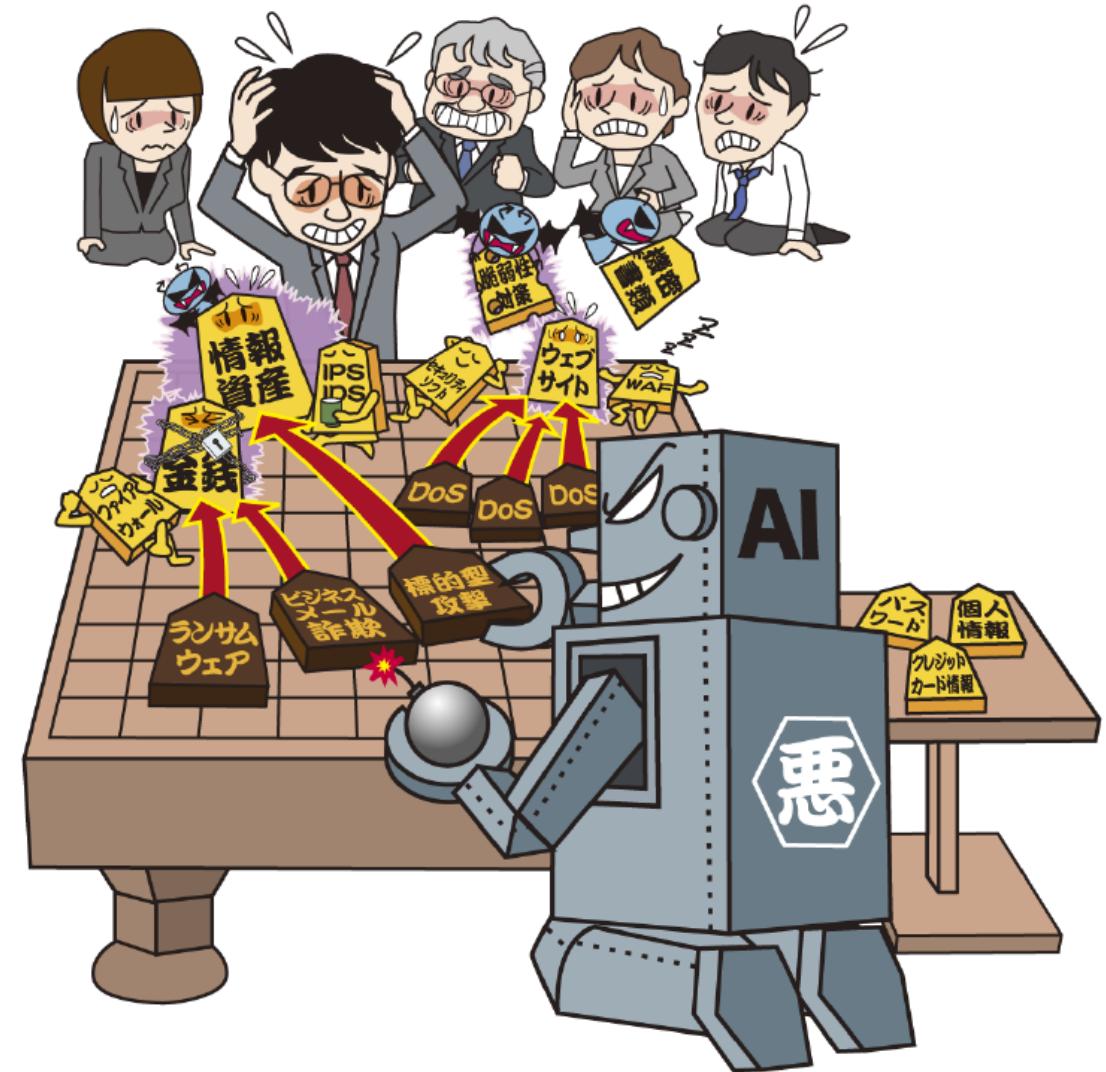
秋葉 淳哉

NTTアドバンステクノロジ株式会社



## 1-1 最近のセキュリティインシデントの状況

- 我々の身の回りに起きていること／お客様にとっての脅威にはどのようなものがあるか？
- セキュリティを考える上で知っておかなければならぬこと



IPA 情報セキュリティ10大脅威 2019より



## 1-1 最近のセキュリティインシデントの状況（その1）

2018年

- 2月 ・平昌冬季五輪を狙った攻撃
- 4月 ・米、中国大手2社の通信機器 調達禁止へ
  - ・NTTグループ<sup>®</sup> インターネット上の海賊版サイトに対するブロッキングの実施
- 5月 ・EU個人情報保護指令(GDPR)施行
- 6月 ・米カリフォルニア州で個人データの保護法成立
- 8月 ・「Struts 2」脆弱性を狙う攻撃キャンペーン「Bleeding Thunder」
- 9月 ・Facebookで5千万件の情報流出
- 10月 ・Bloomberg Supermicro社製マザーボードに不正チップ確認



## 1. 最近のセキュリティインシデントの状況（その2）

2018年

10月 **・北朝鮮ハッカー集団APT38、金融機関攻撃で1億ドル超盗む**

・キャセイパシフィック航空、顧客情報940万人流出

12月 **・Marriott傘下のホテルで5億人の情報漏えい**

・PayPay不正利用

2019年

1月 **・宅ふあいる便、480万件顧客情報流出**

・米司法省、北朝鮮ハッカーのネットワーク壊滅に大規模作戦

2月 **・Collection#1ダークウェブに出現した約27億件の巨大漏えい**

ファイル群

3月 **・ASUS自動更新機能への攻撃により100万台以上のPCマル**

ウェア感染被害



## 1. 最近のセキュリティインシデントの状況（その3）

2019年

- 5月   ・米トランプ大統領による大統領令により、**中国Huawei社の排除へ**
- 6月   ・バックドア「Triada」が仕込まれたAndroid端末が出荷
- 7月   ・セブンペイ不正アクセス・不正利用



## 2-1 特徴的な事案

2018年に発生したセキュリティインシデント事案のうち、特徴的と思われる以下の3点のトピックについて説明する。

【トピック1】 サプライチェーンリスク

【トピック2】 情報漏えい

【トピック3】 サイバー攻撃・標的型攻撃



## 【トピック1】 サプライチェーンリスク

ITサプライチェーンリスクとは (IPAより)

ITシステム・サービスの業務委託・調達の形態

- システム・サービスを構成するソフトウェア、ハードウェア、サービスのライフサイクル全般（設計・開発・流通・運用・廃棄）が対象
- ソフトウェアの調達 + モノの調達 + 運用委託



- 委託先からの納品物に  
**マルウェアが混入**
- 調達したソフトウェア  
の脆弱性による事故

- 脆弱な／悪意ある**IoTデバイス**
- **悪意ある部品**の付加されたデバイス

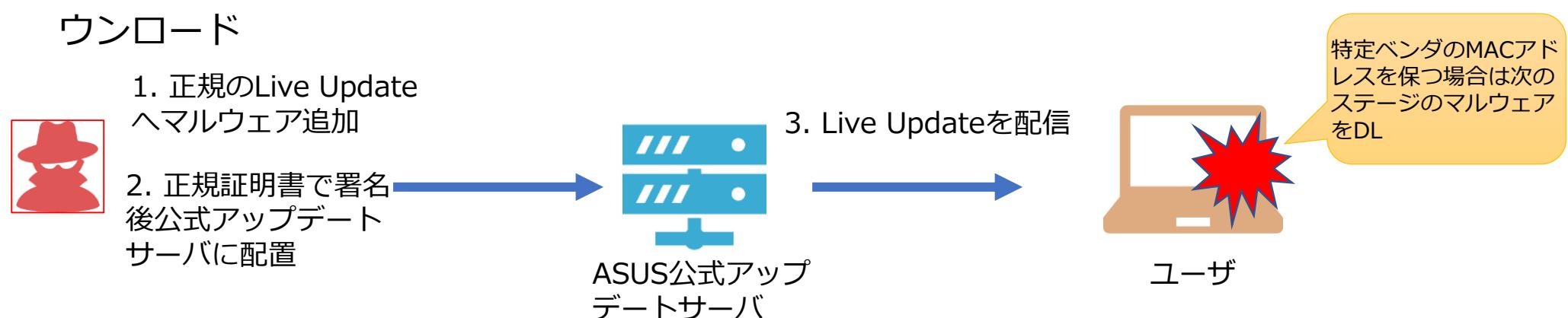
- 委託先からの**情報流出**
- 委託元／先からの**サイバー攻撃メール**



## 【トピック1】 サプライチェーンリスク ASUS社端末に仕込まればバックドアの事例

### ■ ASUS社の提供するソフトウェア「ASUS Live Update」を悪用してマルウェアを配布する攻撃 → “Operation Shadow Hammer”

- ASUS Live Updateは、最新のASUS社製PCの大部分にプリインストールされている
- マルウェア（バックドア）が追加されたユーティリティは、ASUS社の正規証明書で署名されていた（AVソフトをすり抜ける）
- ASUS公式アップデートサーバから配信され、5万7千台以上のコンピュータが感染  
(2018年6月～11月)
- 特定MACアドレスを持つデバイス上で実行されると次ステージのマルウェアを端末にダウンロード





## 【トピック1】 サプライチェーンリスク その他の事案

- サーバ用のJavaScript環境Node.jsを管理している「Node Packaged Modules (npm)」に登録されているCookieパーサ (getcookiesパッケージ) にバックドアが仕込まれていた。 (2018年5月)
- Pythonモジュール「SSH Decorator」にSSHの認証情報を窃取するバックドアが仕込まれてた。開発者はバックドアを仕込まれたモジュールが配布サイトへ不正にアップロードされた
- Gentoo LinuxのGitHubアカウントが侵害され、ファイルを削除するマルウェアが設置された。 (2018年6月)
- RXDrioderという広告関連のSDKに悪意の機能を持つアドウェア「SimBad」が仕込まれた。当該SDKを使って開発された200以上のアプリのダウンロードは通算1億5,000万回 (2019年3月)



## 【トピック1】 サプライチェーンリスク モノの調達リスク

### ■ 米国における中国の通信機器大手2社HuaweiおよびZTE社の製品／サービス排除の動き

- 中国政府による情報収集の懸念
- AT&TがHuawei製品の販売を中止（2018年1月）
- 米商務省がZTE社を輸出規制対象組織に指名（2018年4月）
  - その後5月25日に緩和
- 2018年12月Huawei社CFO逮捕後、西側諸国でHuawei製品を重要通信インフラから排除する動きが加速（米、英、日、ドイツ、仏、チェコ、等）



## 【トピック2】 情報漏えい

### ■ ホテル予約サイトにおける個人情報流出

- 仮ファストブッキングの管理サーバが不正アクセスを受け、ホテルの予約情報やクレジットカード情報が漏洩（日本国内400以上の施設、合計約32万5千件）（2018年6月）

### ■ Facebookからの大量個人情報流出

- CambridgeAnalytica社を通じた利用者8700万人分の情報の不正使用（2018年3月）
- 情報共有を拒否しているユーザ情報を取得できるAPIを特定ベンダー（Apple, Samsung, Blackberry等）に提供（2018年6月）
- 「View As」機能の弱点を突かれ約5千万件のログイン識別情報が流出（2018年9月）

### ■ Dark Webで過去に流出したアカウントなど数十億件（うち、日本ドメイン800万件）



## 【トピック2】 情報漏えい

- キヤセイパシフィック航空顧客情報940万人漏えい（2018年10月）
  - 名前、国籍、生年月日、電話番号、電子メールアドレス、パスポート番号、IDカード番号、マイレージプログラム会員番号、顧客サービスに関する記録、旅行履歴情報
- Google社APIの不具合で最大50万件のGoogle+アカウント情報漏洩（2018年10月）
- マリオット社から最大5億人（3.8億人）の個人情報漏えい（2018年11月）
  - 奎下のスターウッド社の予約データベースへの不正アクセス
  - 暗号化されていないパスポート番号約525万人



## 【トピック3】 サイバー攻撃・標的型攻撃 参考例：平昌五輪

■ 2017年12月以降オリンピックの関連組織に対し標的型攻撃が発生。

- システム情報の窃取や遠隔操作を行なうマルウェアへの感染が試みられた
- 細工されたMicrosoft Wordのファイルが添付された標的型メール
- Wordファイルを開くと悪意あるPowerShellスクリプトが実行
  - ✓ 画像DL→ステガノグラフィ→他のPowerShell抽出
  - ✓ Gold Dragon : 感染したコンピュータのシステム関連情報窃取
  - ✓ Brave Prince : ログやレジストリの内容等を収集
  - ✓ Ghost419 : 感染したコンピュータを偵察
  - ✓ RunningRat : 遠隔操作ツール
- 被害の有無および攻撃者は不明。

■ 2018年2月9日 20時前後 公式webサイト等への攻撃

- サイト閲覧や観戦チケットの印刷が一時不可
- メインプレスセンターのテレビ視聴とインターネット通信が一時利用不可
- オリンピックスタジアムの無線LAN等が一時停止
- 大会組織委員会は「サイバー攻撃が原因」と説明、情報システムの論理的破壊に特化したマルウェア OlympicDestroyer



## 【トピック3】 サイバー攻撃・標的型攻撃 参考例：平昌五輪

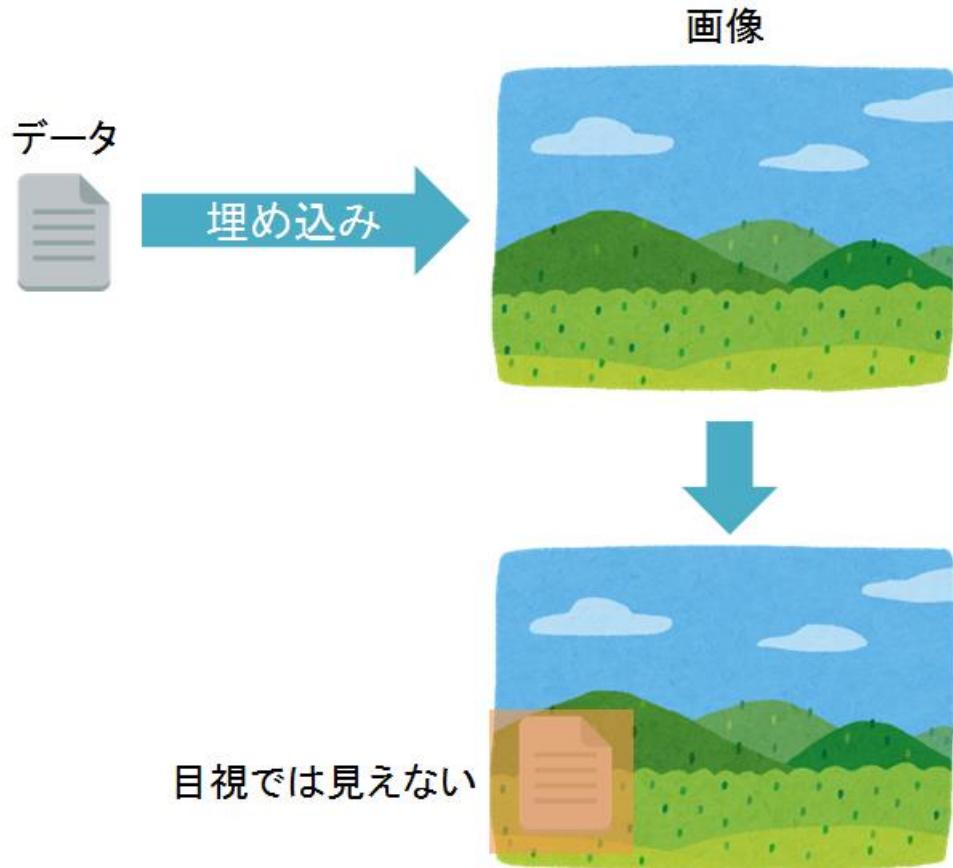
### ■ OlympicDestroyer

- 情報システムの破壊のみを行なうマルウェア
- 様々な攻撃グループの特徴がOlympic Destroyerに含まれていた。
  - ✓ Lazarus(北朝鮮)、APT28(ロシア)、APT3/APT10/APT12(中国)
- Windowsのシャドーコピーや起動時に必要な設定を消去し、コンピュータを使用できなくなる。また、ファイル共有のファイルも消去
- コンピュータに保存されているデータを窃取する機能はない。
- 初期感染の経路は不明
- 感染拡大は、WebブラウザやWindowsから認証情報を窃取し、Windows標準のツールであるPsExecとWMIを用いて他のコンピュータに不正ログインを試みる。
- 認証情報の窃取に加え、コード中に認証情報がハードコーディングされている。
  - ✓ このコード中の認証情報が異なるサンプルが存在する。窃取した認証情報を元に攻撃者がOlympic Destroyerを更新？
- 攻撃者はオリンピックの運営に関する情報システムの詳細を大量に把握している模様。(ユーザー名、パスワード、ドメイン名、サーバ名)



## (参考) ステガノグラフィ

- ステガノグラフィー (steganography)
  - データ隠蔽技術の一つであり、データを他のデータに埋め込む技術のこと、あるいはその研究を指す。クリプトグラフィー (cryptography) がメッセージの内容を読めなくする手段を提供するのに対して、ステガノグラフィーは存在自体を隠す点が異なる。 (Wikipediaより)

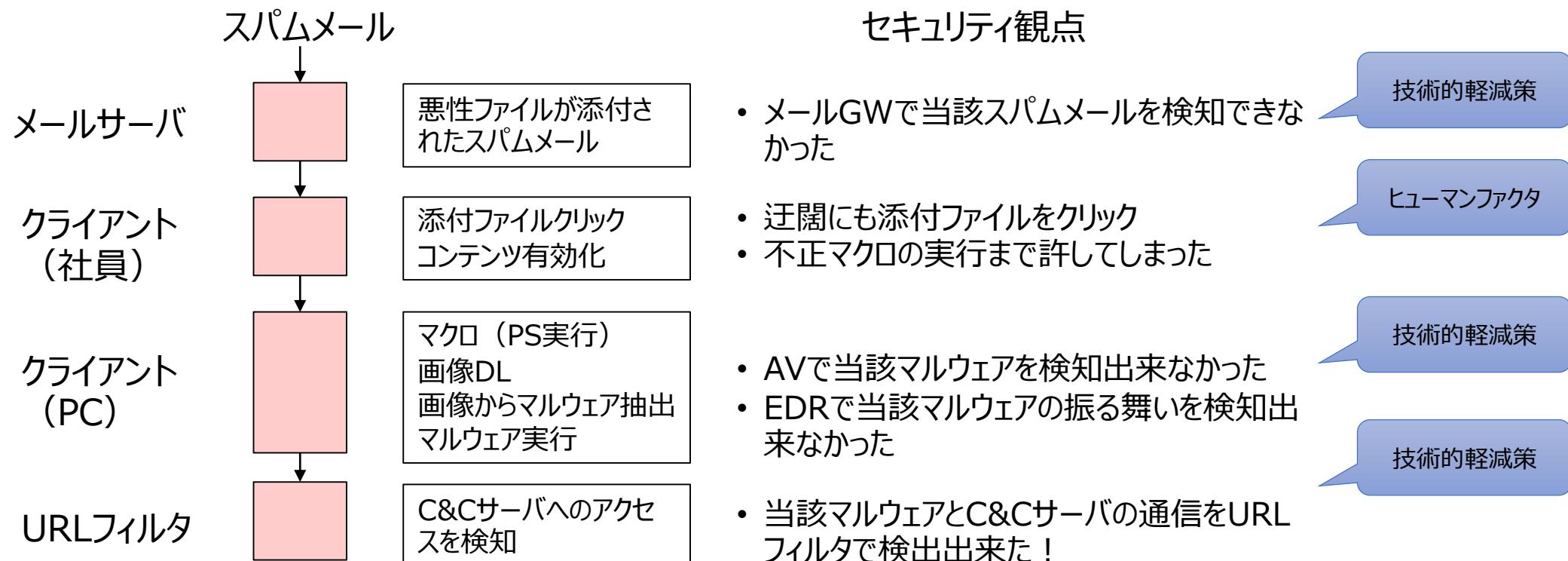


(画像 [www.cyber-attack.net](http://www.cyber-attack.net)より)



## (参考) ステガノグラフィ用いたセキュリティインシデント

- 発生場所： 某企業
- 攻撃元： 不明
- 発生日時： 2019年6月上旬
- 攻撃概要・特徴： 悪性ファイルが添付された電子メールを用いた攻撃。PowerShellを実行し、**SNSから画像をダウロード（その中にステガノグラフィを用いてマルウェアが隠されている！）**。その後URLフィルタでC&Cサーバとの通信を発見し、大事には至らず。





## 【トピック3】 サイバー攻撃・標的型攻撃

### 標的型攻撃

特定の組織内の情報を狙って行われるサイバー攻撃の一種であり、その組織の構成員宛てにコンピュータウイルスが添付された電子メールを送ることなどによって開始される。以降も持続的に潜伏して行われる標的型攻撃はAPT攻撃と呼ばれている。 (Wikipedia)

### APT攻撃 (Advanced Persistent Threat)

「発展した／高度な（Advanced）」「持続的な／執拗な（Persistent）」「脅威（Threat）」の略語で長期間にわたりターゲットを分析して攻撃する緻密なハッキング手法。 (Wikipedia)



## 【トピック3】 サイバー攻撃・標的型攻撃

### APT攻撃の攻撃プロセス

- 初期侵害 (Initial Compromise) : バックドア不正プログラム投入（通常の標的型攻撃）
- 抱点確立 (Establish Foothold) : バックドアとの通信を確立、追加機能投入
- 権限昇格 (Escalate Privileges) : パスワードクラック、パス・ザ・ハッシュ (Pass the hash) 等
- 内部偵察 (Internal Reconnaissance) : イントラネット構成調査
- (水平展開 (Move Laterally) : イントラネット内を移動) ←反復
- (存在維持 (Maintain Presence) : バックドアの追加設置等) ←反復
- 任務遂行 (Complete Mission) : 情報の窃取 (ファイル圧縮・ファイル転送等)



## 【トピック3】 サイバー攻撃・標的型攻撃

### ■ 世界のAPT一覧 (FireEyeより)

APT#	名称/別名	国名	概要
APT1	Unit 61398	中国	中国人民解放軍（PLA）の総参謀部（GSD）第三部第二局、61398部隊として知られる。英語圏のさまざまな業種の組織を主な標的にしています。インフラストラクチャの規模から判断して、少なくとも数十人、場合によっては数百人の人員を擁する大規模組織である可能性がある
APT3	UPS	中国	航空宇宙/防衛、建設/エンジニアリング、ハイテク、通信、運輸業界に関わる企業を標的とする。特に高度なグループで、ブラウザベースのゼロデイ・エクスプロイトを使用した複数の攻撃を行う
APT10	Menupass	中国	米国、ヨーロッパ、日本の建設/エンジニアリング、航空宇宙、通信業界の企業と官公庁を攻撃する中国のサイバースピオナージ・グループ
APT28	Tsar	ロシア	防衛・地政学的な問題に関する情報、すなわち政府機関のみが必要とする情報の収集に取り組む、高い技術力を持った開発者および攻撃実行者のグループ
APT30		中国	ASEANの加盟各国を対象に長期にわたり継続的に活動。ソースコードを効果的に変更、適応させて、少なくとも2005年より同じツール、戦術、インフラストラクチャを使い続けている



## 【トピック3】 サイバー攻撃・標的型攻撃

### ■ 世界のAPT一覧 (FireEyeより)

APT#	名称/別名	国名	概要
APT34		イラン	主に中東地域で長期的なサイバースピオナージ活動を展開していると見られるグループ。イランの国益につながる偵察行為を主な活動としており、遅くとも2014年から活動を続けていると考えられる。
APT37		北朝鮮	主に韓国（加えて日本、ベトナム、中東諸国）の化学、エレクトロニクス、製造、航空宇宙、自動車、医療業界の企業を対象に、ゼロデイ脆弱性やワイヤー・マルウェアを利用
APT38		北朝鮮	世界中の金融機関を対象として、少なくとも11か国、16を超える組織で攻撃活動を展開。その活動は用意周到かつ計画的で、目的を達成するためにネットワーク構成、必要な権限、システム技術を把握できるまで標的の環境へのアクセスを維持し、これまで観測されている最大規模のサイバー窃盗を行っている。
APT39		イラン	中東の通信業界、旅行業、IT企業、ハイテク業界を対象。特定の個人に対するモニタリングや追跡、調査を行い、国の優先事項に関わる戦略要件に役立つ商業目的または運営目的の専有データや顧客データを収集し、別のアクセスや経路を作成して今後のキャンペーンを進めやすくする意図があると思われる。



## 【トピック3】 サイバー攻撃・標的型攻撃

### ■ 世界のAPT一覧 (FireEyeより)

APT#	名称/別名	国名	概要
APT40		中国	一帯一路構想にとって戦略的に重要な国を標的とする、中国のサイバー エスピオナージ・グループ。グローバル組織を標的とし、特にエンジニアリングと防衛に重点を置いている。
APT41		中国	早ければ2012年から、少なくとも14か国（地域）で医療、通信、ハイテク分野を標的としてエスピオナージ活動を実施



## 【トピック3】 サイバー攻撃・標的型攻撃 APT38

### ■ 北朝鮮国家の支援を受けている脅威グループ「APT38」

- 2014年以降11カ国、16以上の金融機関を攻撃、11億ドル以上の窃盗を試み、1億ドルに成功
- チリ、メキシコ、台湾、ベトナム、バングラデシュ等を標的
  - i. 情報収集：SWIFTシステムにアクセスできる企業・団体の担当者や第三者を調査
  - ii. 初期侵入：水飲み場型攻撃や、パッチが不適用のApache Struts等を標的を攻撃
  - iii. 内部偵察：マルウェアの展開を通じて認証情報を収集し、被害者のネットワーク・トポロジのマッピング、環境内に現存するツールを悪用し、システムを精査
  - iv. SWIFTサーバーへのピボット：偵察用マルウェアと内部ネットワーク監視ツール、アクティブとパッシブ両方のバックドアをSWIFTシステムにインストール
  - v. 資金転送：マルウェアを展開・実行し、不正なSWIFT取引を挿入し、合わせて取引履歴を改ざん。別々の国にある口座へ複数の取引を通じてマネーロンダリング
  - vi. 証拠隠滅：ログをセキュアに消去しつつ、ディスクワイプ用マルウェアを実行



## NTT-ATのご紹介

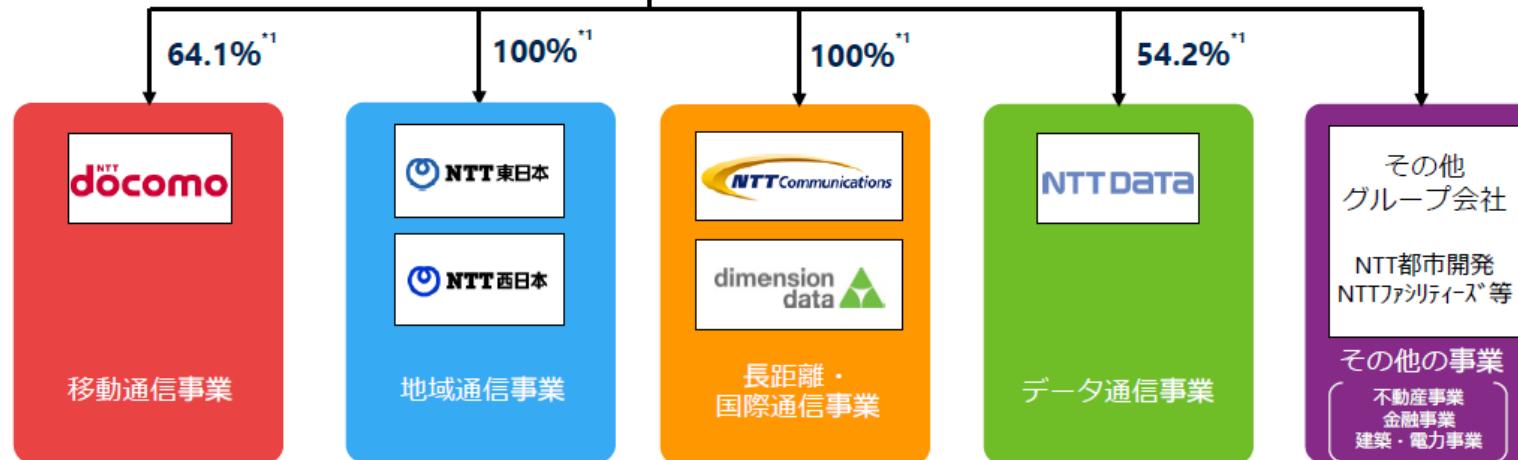
# NTTグループ概要 <体制>

NTT



- ・連結営業収益 : 118,798億円
- ・連結営業利益 : 16,938億円
- ・従業員数 : 303,350名
- ・連結子会社数 : 919社

\*1 記載の数字は主要子会社に対する議決権比率（2019年3月末現在）  
 \*2 NTTグループ全体のグローバル市場における競争力強化と収益性の向上をめざして「NTT株式会社（グローバル持株会社）」を設立し、NTTコミュニケーションズ、Dimension Data、NTTデータ、NTTセキュリティの移管を完了（2018年11月）。NTTコミュニケーションズ、Dimension Data、NTTセキュリティの3社をグローバル事業会社と国内事業会社へ再編成（2019年7月）。



営業収益	48,408億円	31,523億円	22,787億円	21,636億円	12,403億円
営業利益	10,136億円	3,607億円	1,001億円	1,477億円	856億円
従業員数	26,650名	79,550名	48,000名	123,900名	25,250名
子会社数	103社	45社	370社	306社	95社

注) 2018年度。各セグメントの営業収益および営業利益は、セグメント間取引を含む

その他の事業  
 ●不動産事業  
 ●金融事業  
 ●建築・電力事業  
 ●システム開発事業  
 ●先端技術開発事業  
 NTTアドバンステクノロジ（株）  
 ●その他



# NTT-AT 概要

正式社名	エヌ・ティ・ティ・アドバンステクノロジ株式会社
本社所在地	〒212-0014 神奈川県川崎市幸区大宮町1310 ミューザ川崎セントラルタワー
設立年月日	1976年（昭和51年）12月17日
代表者	代表取締役社長 木村 丈治
資本金	50億円
株主	日本電信電話株式会社（100%）
売上高	562億円（2019年3月期）
社員数	1,865名（2019年3月31日現在）
事業内容	<ul style="list-style-type: none"> <li>1. トータルソリューション事業           <ul style="list-style-type: none"> <li>◦ システムインテグレーション、ネットワークインテグレーション、関連ソフトウェア・サービス開発等</li> </ul> </li> <li>2. セキュリティ事業           <ul style="list-style-type: none"> <li>◦ セキュリティ関連サービス・保守、関連製品販売等</li> </ul> </li> <li>3. クラウド・IoT事業           <ul style="list-style-type: none"> <li>◦ クラウド・IoTサービス・保守、関連製品販売等</li> </ul> </li> <li>4. AI×ロボティクス事業           <ul style="list-style-type: none"> <li>◦ RPA等</li> </ul> </li> <li>5. グローバル事業           <ul style="list-style-type: none"> <li>◦ ネットワーク・メディアアプリケーション関連の海外製品販売・保守、光関連製品開発、先端材料開発・分析、環境マネジメント等</li> </ul> </li> <li>6. 知的財産事業           <ul style="list-style-type: none"> <li>◦ 特許・商標など知的財産の調査分析および管理、研修</li> </ul> </li> </ul>
グループ会社	<p>NTT-ATシステムズ株式会社            NTT-ATテクノコミュニケーションズ株式会社            NTT-ATアイピーエス株式会社            NTT-ATクリエイティブ株式会社            NTT-ATエムタック株式会社</p>



# NTT-ATが提供するセキュリティサービス

## 事前対策（特定・防御）

コンサルティング・教育

診断・監査

販売・構築

監視・運用

インシデント対応

### 情報セキュリティコンサルティング

- ・ISMS認証取得支援
- ・Pマーク認証取得支援
- ・個人情報保護法対策
- ・情報セキュリティ監査

### 情報セキュリティ教育

- ・集合研修
- ・ハンズオン
- ・教材開発

### セキュリティ診断

- ・Web/IPセキュリティ診断
- ・標的型メール耐性診断
- ・IoTセキュリティ診断



### 組織内CSIRT支援

- ・構築支援：計画立案、文書作成、組織整備 等
- ・運用支援：状況監査、改善提案、教育、訓練(サイバー演習)、  
**会員制コミュニティ (CS@T俱楽部)**

### セキュリティ情報提供

**CS@T俱楽部**

IDS/IPS: Intrusion Detection System / Intrusion Prevention System  
UTM: Unified Threat Management

### セキュアNW/AP設計構築

・DevSecOps

### インターネット環境セキュアソリューション

- ・不正侵入監視/防御：IDS/IPS
- ・次世代ファイアウォール(UTM) : SonicWall
- ・DDoS対策 : Arbor
- ・ID認証型セキュリティ : BlackRidge
- ・IDベースネットワーク : Tempered HIPスイッチ
- ・内部ネットワークセキュリティ対策 : Darktrace
- ・ロードバランサ・負荷分散等 : F5ネットワークス

SONICWALL™

DARKTRACE

f5  
 BlackRidge TECHNOLOGY  
 TEMPERED NETWORKS

allot  
See. Control. Secure.

### エンドポイントセキュアソリューション

- ・IoTデバイスセキュリティ : VDOO
- ・標的型攻撃対策 : yarai
- ・内部情報漏洩対策 : CWAT
- ・ID認証 : TRUSONA

VDOO  
 yarai  
 CWAT  
 TRUSONA

DDos: Distributed Denial of Service  
SIEM: Security Information and Event Management

SOC: Security Operation Center  
CSIRT: Computer Security Incident Response Team

### セキュリティオペレーション(ICT24-SOC)

FORTINET®

- ・FortiGate SOC
- ・FortiSandboxサポート
- ・McAfee SIEMマネージド
- ・Arbor APS SOC
- ・Paloalto SOC

McAfee™ Palo Alto Networks™



### インシデント対応支援

- ・CS@T俱楽部
- ・インシデント対応支援
- ・デジタルフォレンジック
- ・リモートフォレンジック

FIRE EYE™



## セキュリティソリューションの特徴と実績



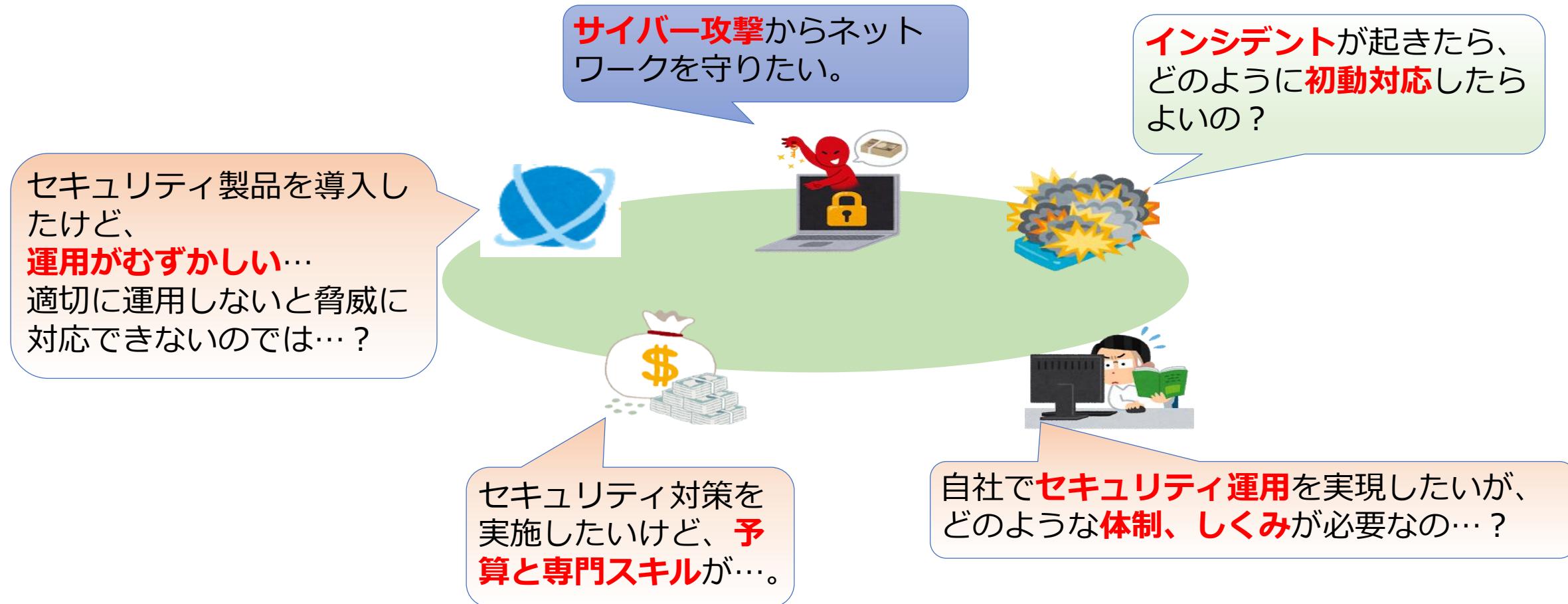
- ✓ NTTグループ企業や官公庁、重要インフラ等で長年セキュリティ業務を担ってきた確かな実績
- ✓ 標的型攻撃のような最新の攻撃にも対応できる高度な技術を持つ専門家集団
- ✓ 検討から導入およびその後の運用までお客様に合わせたトータルサポートが可能な体制





## お客様のお困りごと

セキュリティ製品を導入してサイバー攻撃への対策を実施したいが、適切に運用することが難しい等、多くの企業が様々な場面で課題を抱えています。





## ICT-24SOCサービスラインナップ

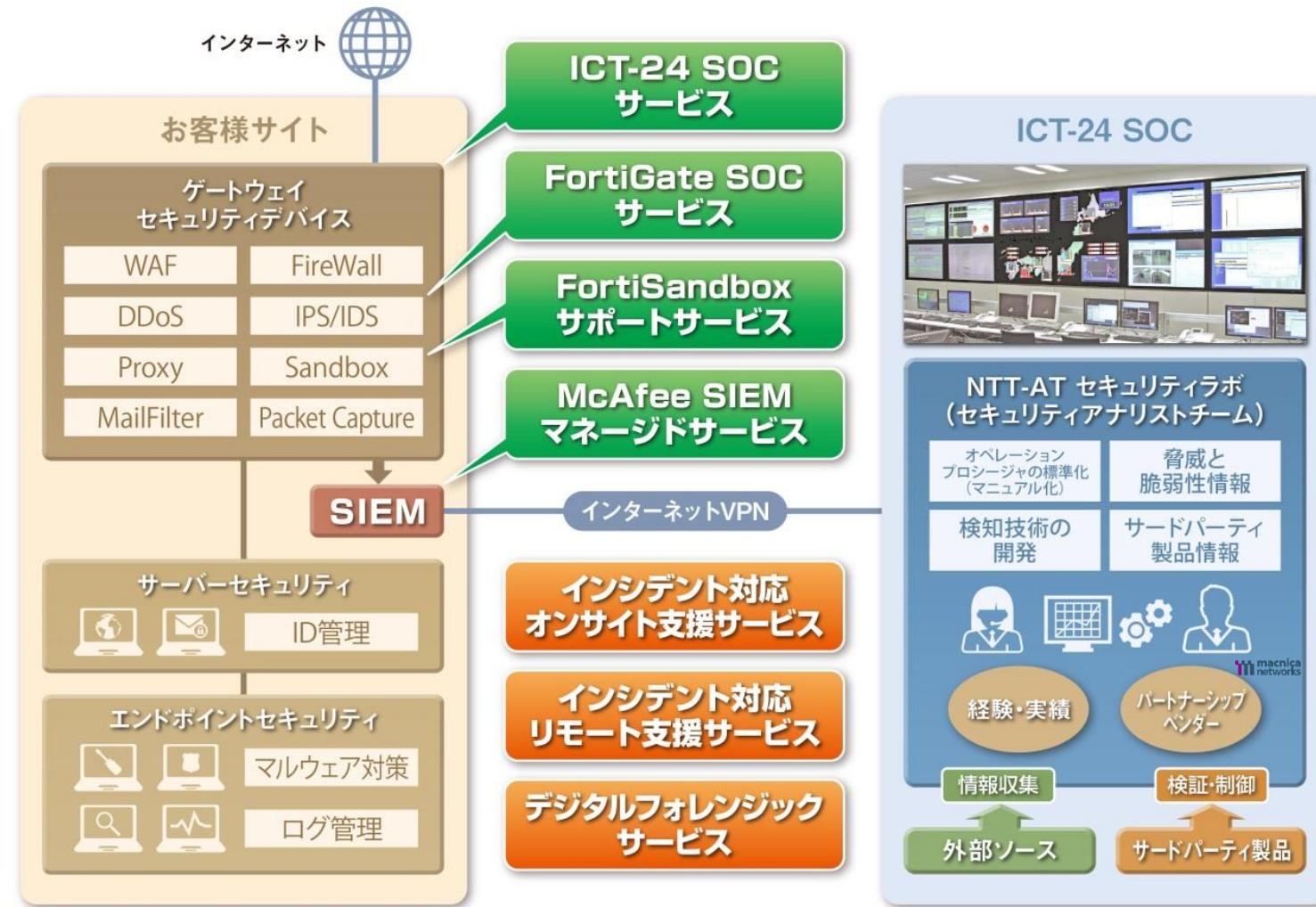
NTT-ATのICT-24SOCは、**NOC/SOC/CSIRTサービスをワンストップで**、しかもリアルタイムに高度な分析を行い、ハイクオリティなSOCサービスを提供します。

- 
1. NOC/SOC/CSIRT支援をワンストップで提供
  2. 対応可能なセキュリティデバイスの種類が豊富
  3. アナリストによる最新の脅威に対応したサービスを提供



## ICT-24SOCサービスラインナップ

お客様サイトのゲートウェイセキュリティデバイスからエンドポイントセキュリティまで遠隔監視により各種サービスをご提供します。





## ICT-24SOCサービス

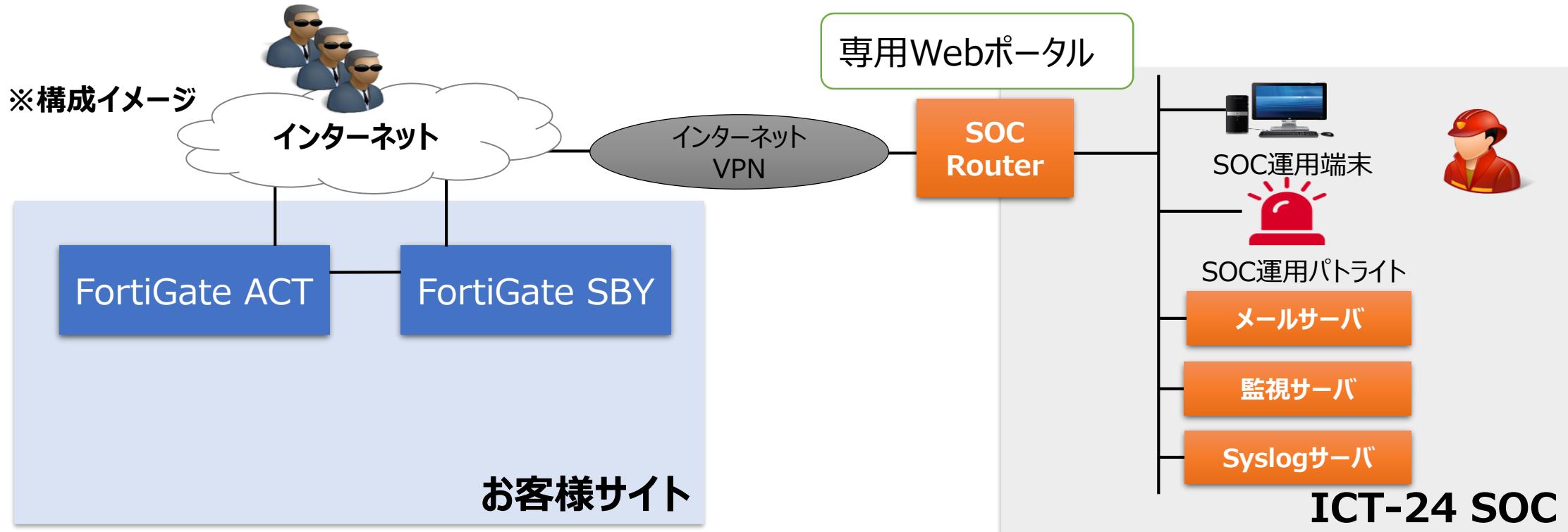
24時間365日ネットワークやデバイスのログを監視し、セキュリティアナリストによる脅威分析を行い、サイバー攻撃の検出と通知、対応策をアドバイスします。





## FortiGateSOCサービス

FortiGate/PaloAltoSOCサービスはお客様のFortiGate/PaloAltoをICT-24SOC上の設備から、**24時間365日リアルタイムで監視**し、最新のシグネチャ状態の維持、インシデントの早期発見、定期的なレポートを提供するサービスです。専用ポータルで問い合わせをしていただくことができ、レポートもダウンロードできます。

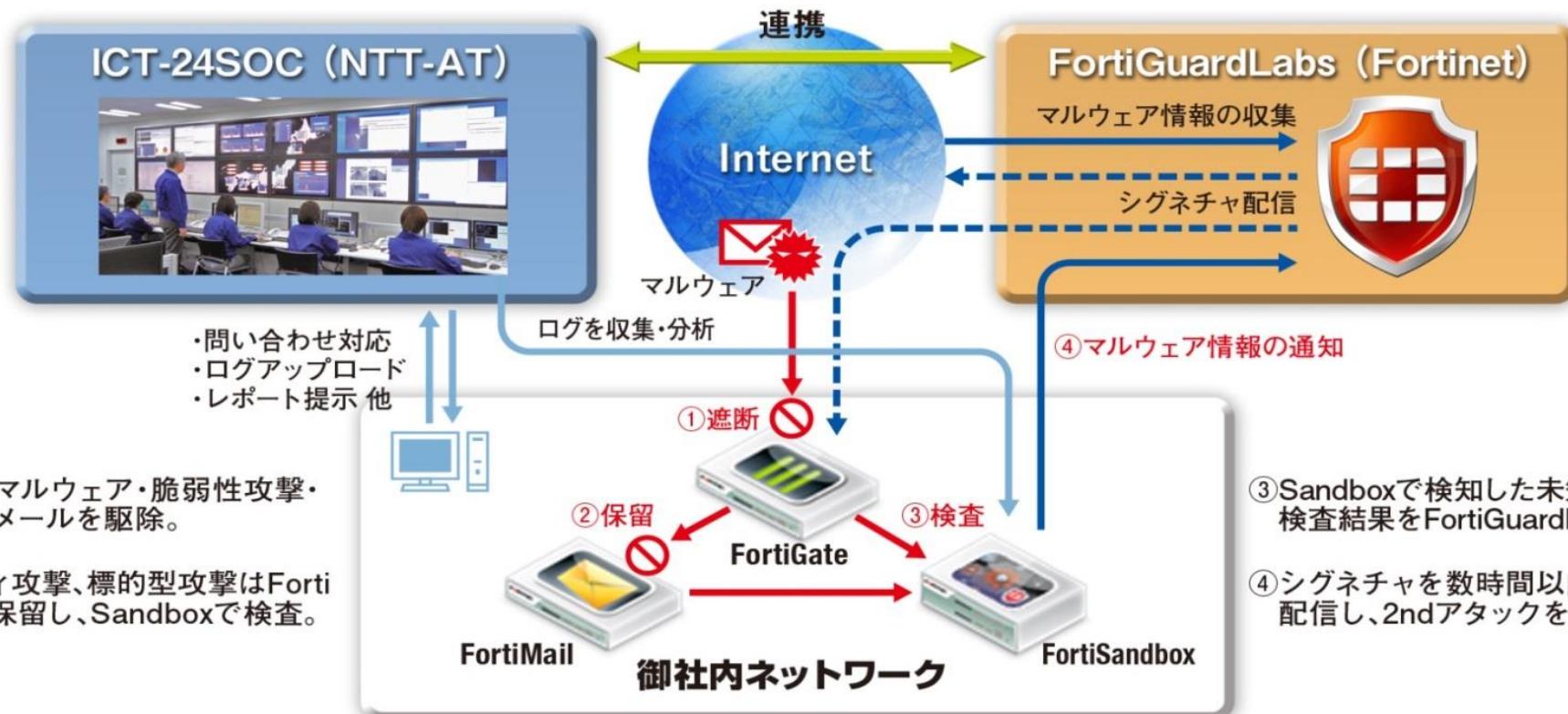




## FortiSandboxサポートサービス

Fortinetセキュリティアライアンスの組み合わせによる自動連携防御機能と、NOCで培った運用ノウハウを利用したシンプルかつ高品質なSOCサービス。

お客様内ネットワークの「FortiSandbox」のログを解析し、検知された未知の脅威の情報や最新動向による分析を盛り込んだ日本語のレポートをご提供します。ポータルサイトにてお客様からの問い合わせに日本語で回答します。





## McAfee SIEMマネージドサービス

お客様がご利用中のさまざまなセキュリティ機器のログを一元的に管理し、リアルタイムな相関分析を行うことで、不正侵入の兆候などを早期に検知し、セキュリティアナリストの分析を加えた対応策の提示を行うなどの高度なセキュリティ分析サービスです。

**POINT 1**  
マカフィーのMSP  
認定を持つICT-  
24SOCによる提供

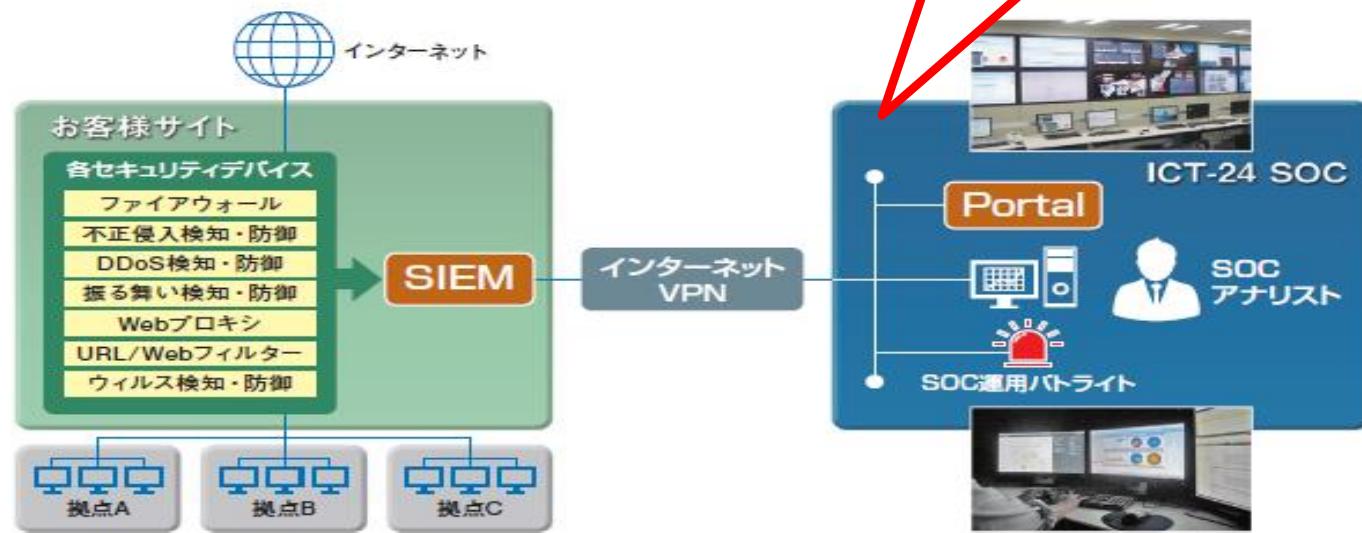


**POINT 2**  
相関分析の対象とな  
る監視対象デバイス  
の種類が豊富

**POINT 3**  
インシデント発生時  
のCSIRT支援も対  
応可能

**NTT-AT社内での運  
用を通じて、ノウハ  
ウ蓄積・技術向上を  
図っています。**

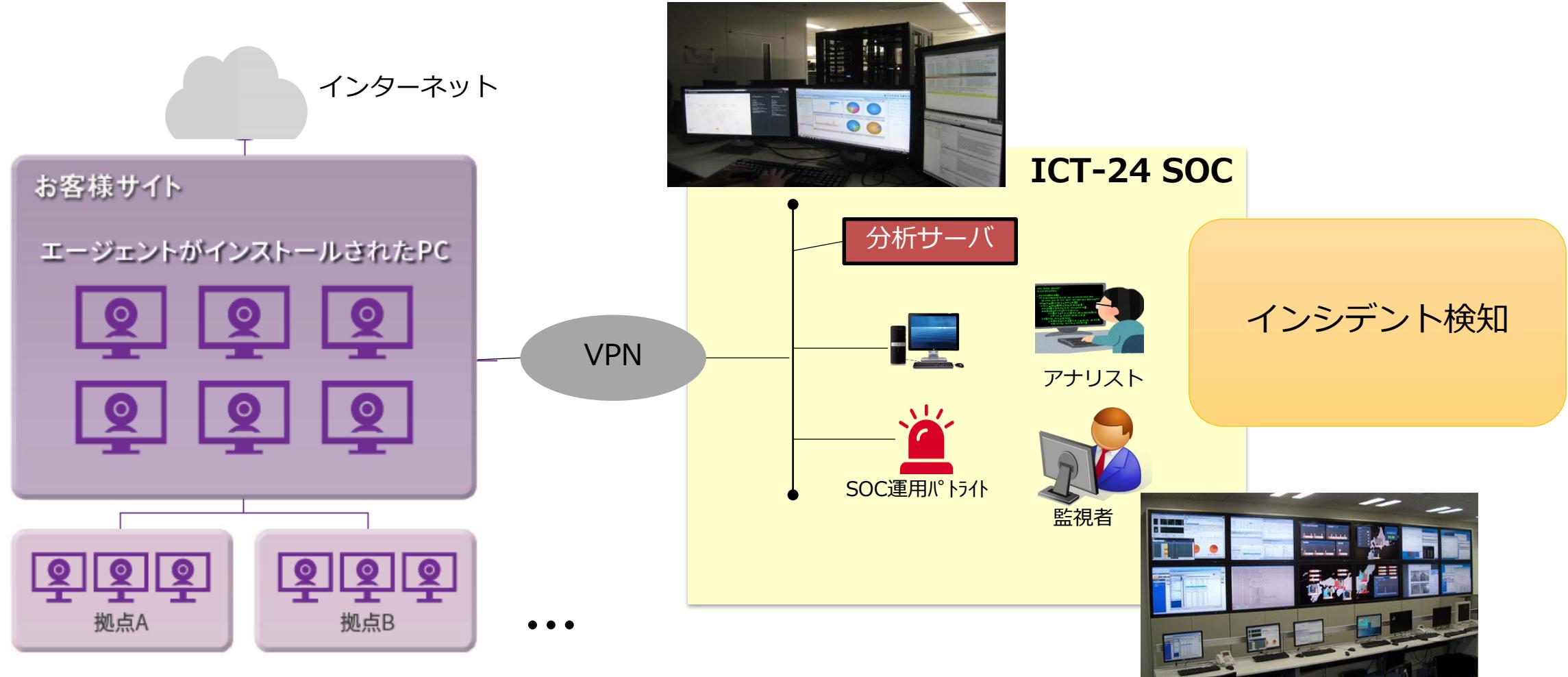
分類	メーカー	
ネットワーク セキュリティ監視	FW	Fortinet, Paloalto
	IDS/IPS	IBM Security, Cisco, McAfee
	WAF	F5, Imperva
	Proxy	BlueCoat, DigitalArts, TrendMicro
	DDoS	Radware, Arbor
	Sandbox	Fortinet, FireEye
	MailFilter	Barracuda, DigitalArts, TrendMicro
	Packet Capture	Savvius
エンドポイント セキュリティ監視	マルウェア	Yarai
	ログ管理	SML
サーバ監視	ID管理	CyberARK





## McAfee リモートフォレンジックサービス

お客様サイトと弊社ICT-24 SOC間をインターネットVPNで接続して遠隔でサービス提供します。必要に応じてアナリストが攻撃の分析をし、適切な対策を提案させていただきます。





## McAfee リモートフォレンジックサービス

検知した攻撃に対しては、インシデント初動対応を、リモート（電話・メール）で実施することにより専門家が迅速に対応します。

インシデント分析

不審ファイルの探索支援

手動によるウイルスの駆除、削除支援

ウイルス検体のエスカレーション方法支援



## McAfee リモートフォレンジックサービス

セキュリティ対策専門スタッフで構成されるセキュリティインシデント専門チームでは、事故発生直後の初動対応が完了した後の、事態収束、さらに改善・再発防止まで、あらゆる段階でご支援します。

- 事故発生直後の初動対応から事態収束、さらには改善・再発防止までサポート
- 社内幹部への説明から社外へのプレスリリース資料作成もご支援
- NTTグループでセキュリティ対策を担ってきた専門スタッフが迅速に対応





# IoTセキュリティ ファームウェア解析によるIoTセキュリティ診断サービス

## IoT製造ベンダ様向けサービス IoTセキュリティレベル向上を支援

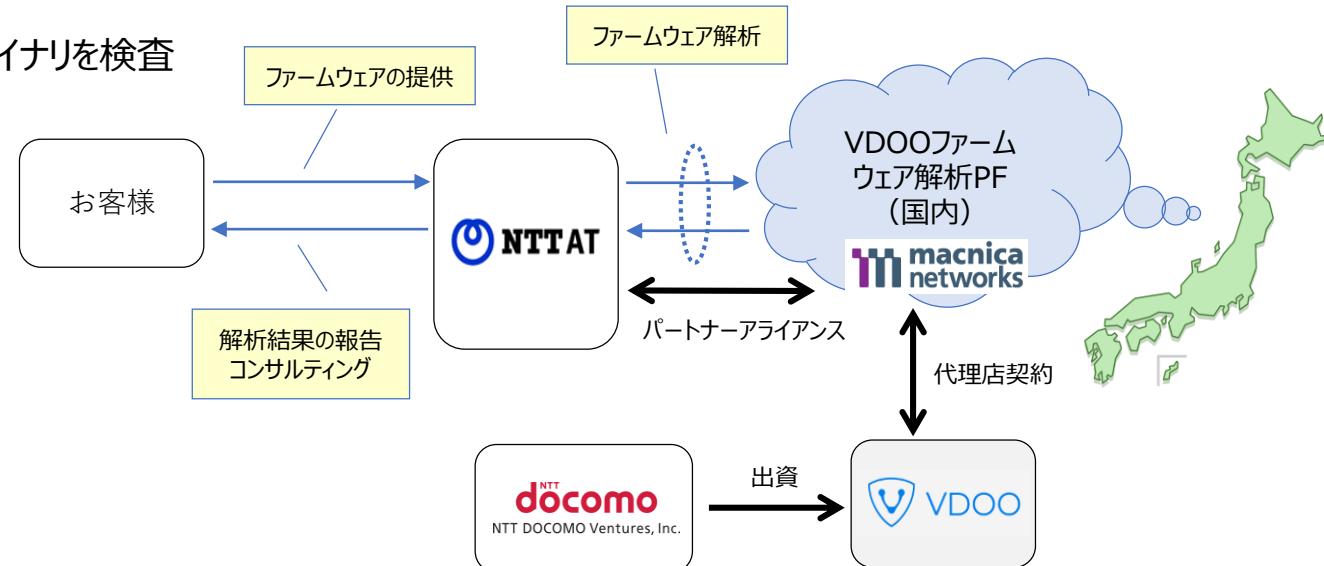
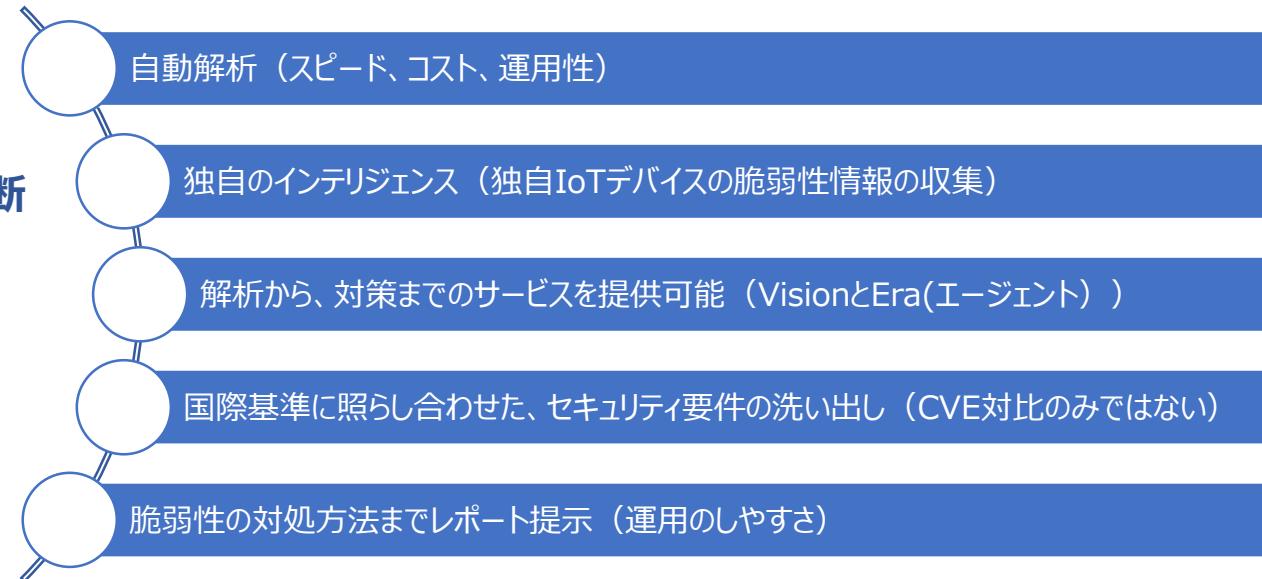
### ■ IoTデバイスのファームウェアをクラウドプラットフォームで自動診断

- IoTセキュリティ標準、特に**CCDSの適合性チェック**
- 部品表の取得 (HW/SW)
- ソースコード不要、バイナリイメージファイルのみ必要
- **高速な解析処理**によりセキュリティバイデザインを支援
- サプライチェーン問題の対処

これまで250万以上の実行ファイルからなる15,000以上のファームウェアバイナリを検査

- ・解析デバイス当たり数十のセキュリティに関する知見を獲得
- ・**120超のIoTゼロデイ脆弱性検知実績**

カテゴリー	仕様
サポートするファームウェアOS	Linux / Android
IoTデバイスのCPUアーキテクチャ	MIPS / ARM / x86
ファームウェアバイナリの最大サイズ	100GB
平均解析時間（最大）	<b>13分</b>





# DevSecOps ContrastSecurity (AP開発×セキュリティ)

アジャイル開発のスピードアップと高度なDevSecOpsの実現を両立。専用エージェントを組み込むだけで、DevOps本来のシンプルなワークフローと高いセキュリティ環境を実現。



## CONTRAST ASSESS (IAST)

- カスタムコードとライブラリの脆弱性検知  
※IAST : Interactive Application Security Testing



## CONTRAST PROTECT (RASP)

- 既知および未知の弱点に対するランタイム攻撃防御  
※RASP: Runtime Application Self-Protection



## CONTRAST OSS (SCA)

- オープンソースを安全に活用  
※SCA : Software Composition Analysis

- アプリケーションスタックにセンサー（エージェント）追加
- 組み込み式で継続的に稼働 連続的な検知と防御
- 正確な検知によりスピードアップ とコスト削減を実現
- 単一プラットフォームで統合管理
- 既存システムとの連携



### Contrast Assess

#### 脆弱性自己検証

- インタラクティブ分析 (IAST)
- 静的分析 (SAST)
- 動的分析 (DAST)
- ソフトウェア構成分析
- コンフィグレーション分析
- アプリケーション インベントリー



### Contrast Protect

#### アタックの可視化 & 防御

- 侵入防止
- F/W(WAF)
- ボットブロック
- ライブラリ遮蔽
- 仮想パッチ
- ログ保存強化

- 特徴① 従来型セキュリティ診断ツールを凌ぐ検知性能
- 特徴② シフトレフトを実現する早期診断でリスクを防止
- 特徴③ 運用時も開発時と同じエージェントで防御でき、効率的



## ◆会員制コミュニティサービス

いわゆる「CSIRT構築運用支援サービス」のような1対1のサービスではありません。担当のエキスパートや会員より提供された事例や知見を共通ナレッジとして蓄積し、会員間でシェアする、**コミュニティー型**のインタラクティブなサービスです。（会員様は匿名）

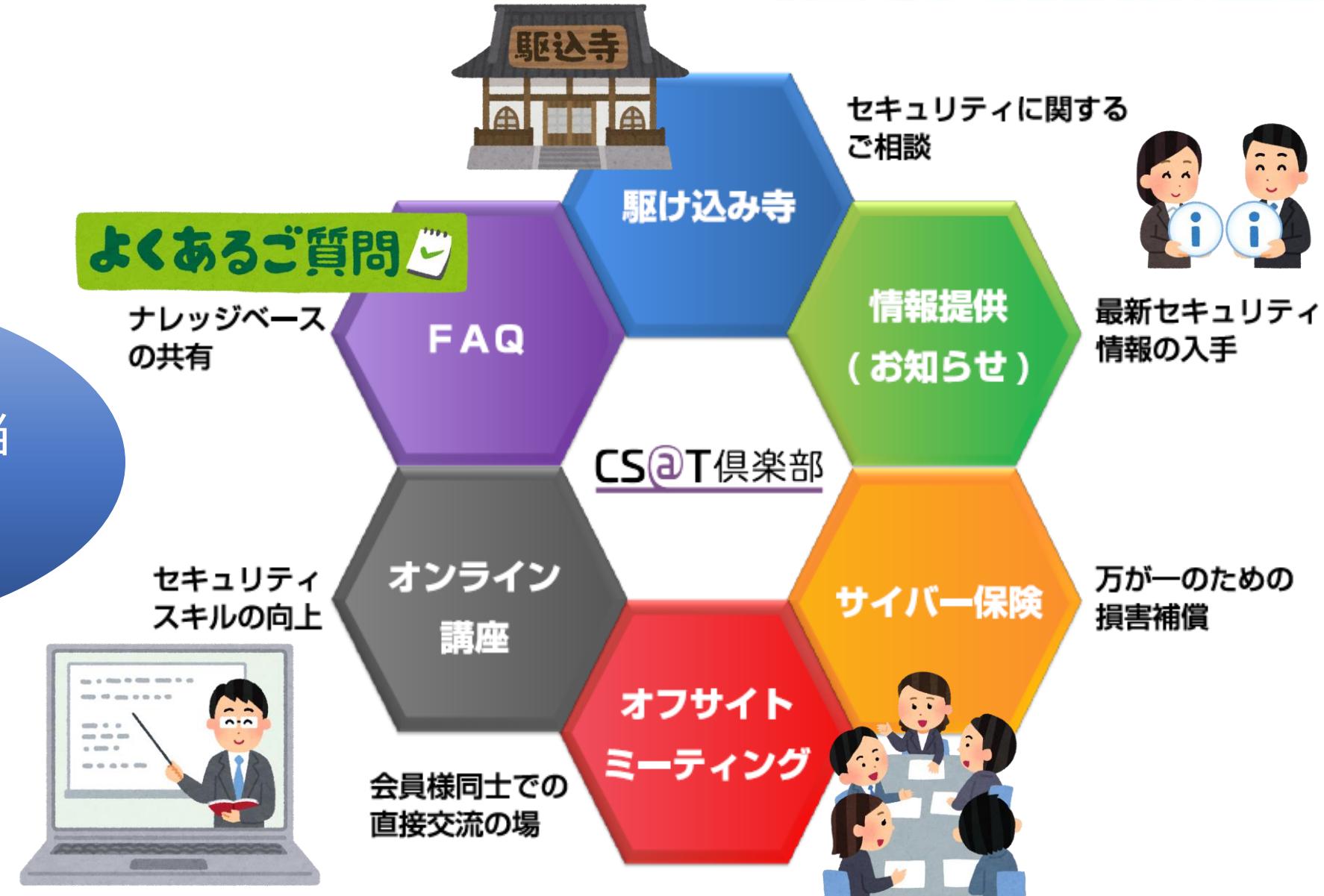
## ◆サイバー保険付帯

すべての会員には、サイバー攻撃や情報漏えい事故等による損害を補償する**サイバー保険**が必ず付帯します。（基本サービスに含みます。）





セキュリティの対応に  
不安をお持ちのご担当  
者様を様々な面から  
サポートします。





## 提供価格（基本サービス）

CS@T俱楽部 基本サービス (標準価格)	駆け込み寺サービス問い合わせ追加チケット (標準価格)
¥360,000 /年	¥15,000/チケット

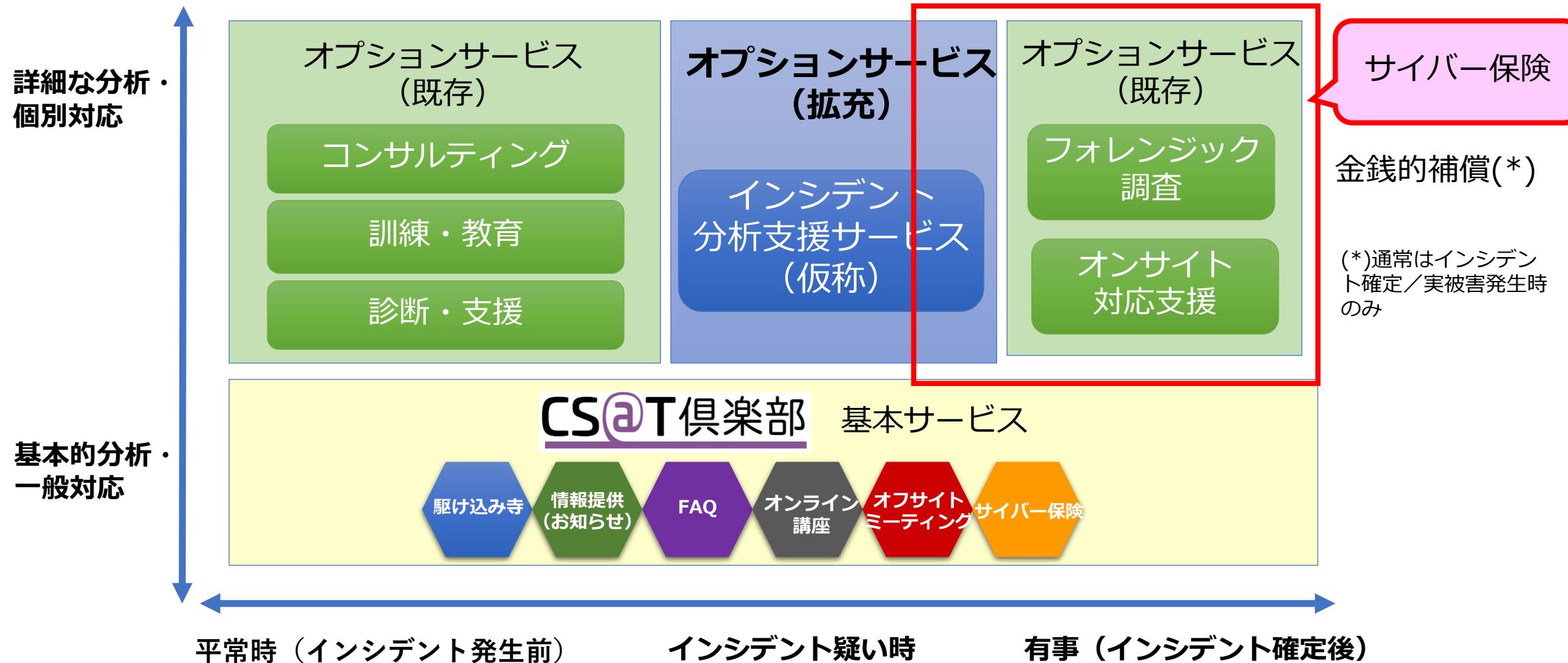
CS@T俱楽部基本サービスには、下記が含まれております。

- ◆ ログインIDの貸与（1IDを提供いたします）
- ◆ 駆け込み寺サービス
- ◆ FAQ
- ◆ 情報提供(お知らせ)サービス
- ◆ オンライン講座
- ◆ オフサイトミーティング
- ◆ サイバー保険

\* 1IDあたり、2件/月を基本サービスに含みます。  
なお、受付時をカウント対象とし、継続した質疑は月を跨いでもカウント対象にはなりません

年間 **¥ 360,000\***

\*基本サービスのみ





## CS@T俱楽部 付帯する保険内容

## CS@T俱楽部

損害の種類	対象となる事故	対象損害・対象費用	支払限度額
賠償損害	<ul style="list-style-type: none"> <li>■ 情報の漏えいまたはそのおそれ</li> <li>■ 情報システムの所有、使用または管理に起因する他人の業務阻害等</li> </ul>	<ul style="list-style-type: none"> <li>■ 法律上の損害賠償金</li> <li>■ 争訴費用</li> <li>■ 権利保全行使費用</li> <li>■ 訴訟対応費用</li> </ul>	2,000万円 (1事故・期間中)
費用損害	<ul style="list-style-type: none"> <li>■ 情報の漏えいまたはそのおそれ</li> <li>■ 情報システムの所有、使用または管理に起因する他人の業務阻害等</li> </ul>	<ul style="list-style-type: none"> <li>■ 事故対応費用</li> <li>■ 事故原因・被害範囲調査費用</li> <li>■ 広告宣伝活動費用</li> <li>■ 法律相談費用</li> <li>■ コンサルティング費用</li> <li>■ 見舞金・見舞品購入費用</li> <li>■ クレジット情報モニタリング費用</li> <li>■ 公的調査対応費用</li> <li>■ 情報システム等復旧費用</li> <li>■ 被害拡大防止費用※</li> <li>■ 再発防止費用※</li> </ul>	1,000万円 (1事故・期間中)
	上記を除き、サイバー攻撃またはそのおそれ	<ul style="list-style-type: none"> <li>■ サイバー攻撃調査費用※</li> </ul>	

※対象の費用には縮小支払割合がございます。

未 来 を 拓 く チ カ ラ と 技 術。

