IIJセキュアアクセスサービス
メディア説明会

安全をあたりまえに
wizSafe

株式会社インターネットイニシアティブ
セキュリティ本部

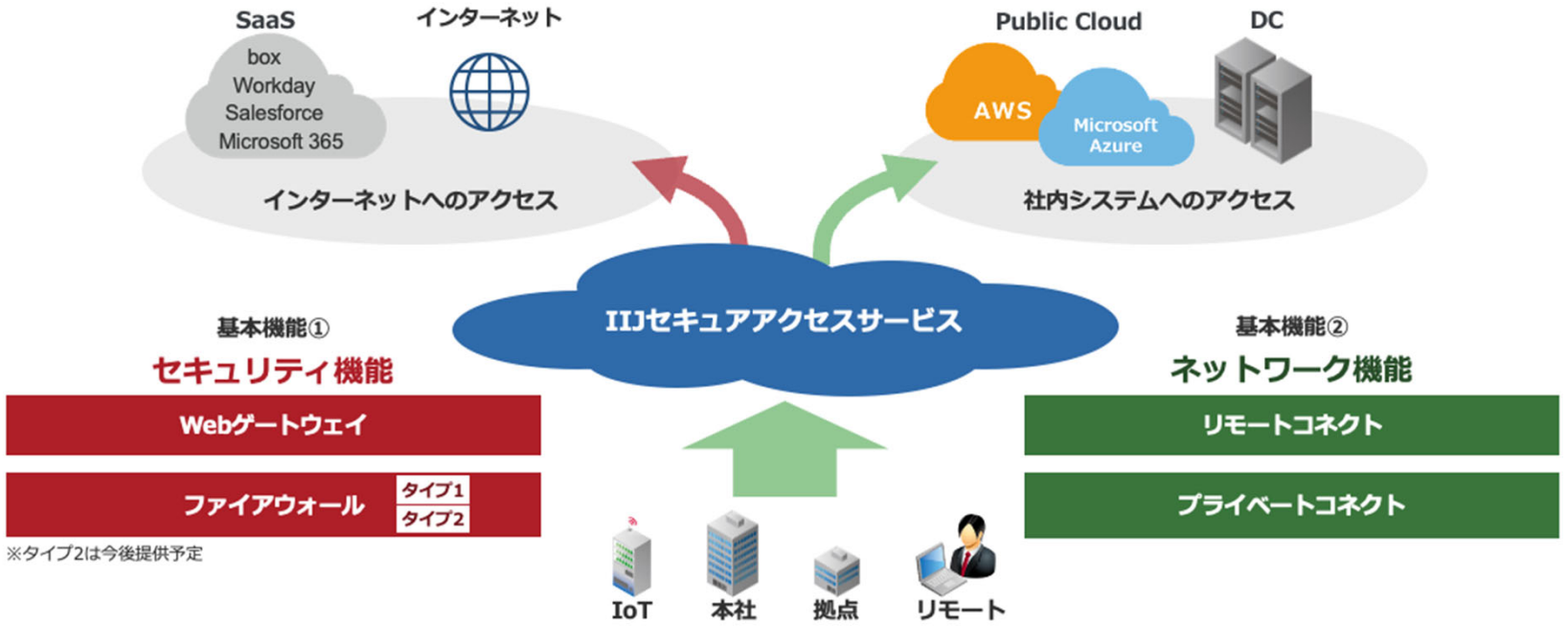
安全をあたりまえに
wizSafe

新 SASEサービス のご紹介

新SASEサービスのご紹介

「IIJセキュアアクセスサービス」を9月1日に提供開始

セキュアかつシンプル、 低価格で、安全なリモートワーク環境の実現へ



背景

環境の変化

- 業務システムの「クラウドシフト」の加速
  - クラウドに預けた情報を安全に取り扱う必要性の増大
- 働き方改革やコロナ対策としてのテレワーク普及
  - 仕事をする場所やシステムが動的に変化し、従来のセキュリティ確保のモデルでは不十分となってきた
  - エッジ側の端末を保護しつつ、通信路の安全性やセキュリティ境界を動的に設定する機能が必要

以上の課題を解決するために、ゼロトラストネットワークなどの新しいセキュリティの考え方が必要とされています

今回提供するSASEはその一部を担うものです

背景

安全をあたりまえに wizSafe

新SASEについて

IIJはこれまでの他社製品をベースにSASEの機能を提供してきましたが、下記の課題解決を目標として、内製にて新しいサービスを提供することとしました

- 日本国内のオペレーション
  - 日本企業の情報資産を、日本国内のオペレーション、国内のデータセンターで取り扱う
- IIJの提供する他のセキュリティ機能との親和性
  - 端末対策（アンチウイルス、EDR、端末管理）などを組み合わせて機能強化
  - IIJ SOC（セキュリティオペレーションセンター）によるセキュリティ運用を統合
- 小規模なお客様にも導入をご検討いただける価格帯
  - 50ユーザから低価格に利用可能
- 海外出張先や海外拠点への拡大
  - 今後、海外にも設備を展開し、海外出張時や海外拠点で利用可能

安全をあたりまえに
wizSafe

SASE・ゼロトラストとは

用語解説

安全をあたりまえに wizSafe

SASE
Secure Access Service Edge

- ガートナー社が**2019年**に提唱したコンセプト
- **“ネットワークサービスとセキュリティサービス”**が統合化・集約化され、**クラウド上で提供**されると指摘し、**サービスのあるべき姿・実装**を示したもの
- ネットワーク＋セキュリティの**ほぼすべての機能を網羅した概念**で、SD-WANやCASB、SWG、**ゼロトラスト**も含む

SSE
Secure Service Edge

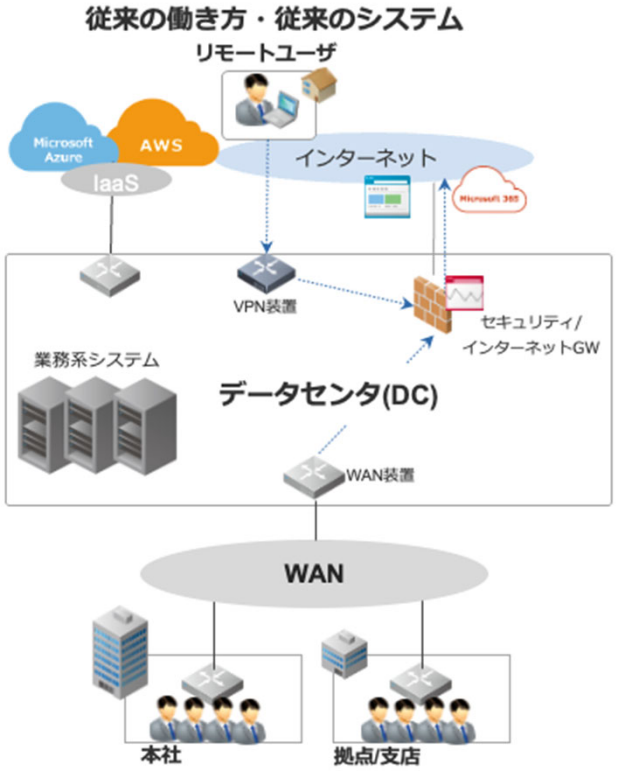
- ガートナー社が**2022年**に提唱したコンセプト
- 主に**SASEから、SD-WANの概念を取り除き**、CASB、SWG、**ゼロトラスト**の**セキュリティにより特化した概念**

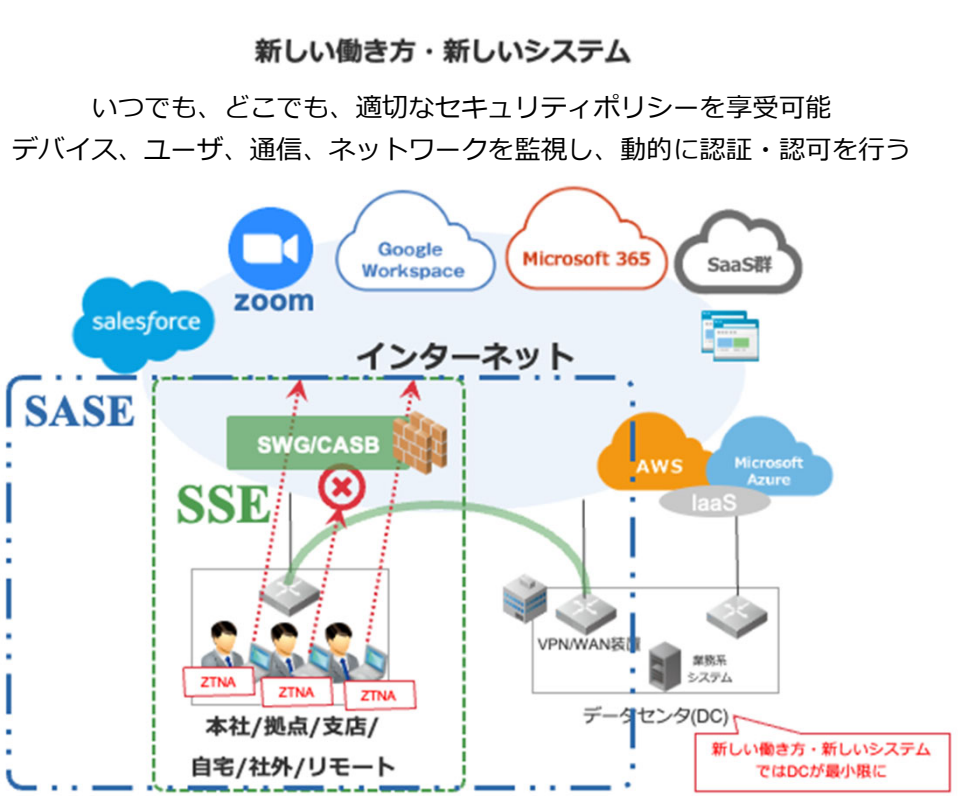
Zero Trust
Zero Trust Architecture

- **フォレスターリサーチ社**が**2010年**に提唱したコンセプトで、**NIST**でも考え方・信条が示されている
- **“守るべき企業のITリソース”**は様々なクラウド上に分散されていき、それらに**どのようにアクセスを許可していくか**という**考え方**を示したもの
- **境界型防御だけでは安全ではなく**、全てのアクセス元・ネットワークを信頼しない前提で、**ユーザからのアクセスを都度 認証・認可**する、つまり、**端末・ユーザ単位の防御**

用語解説

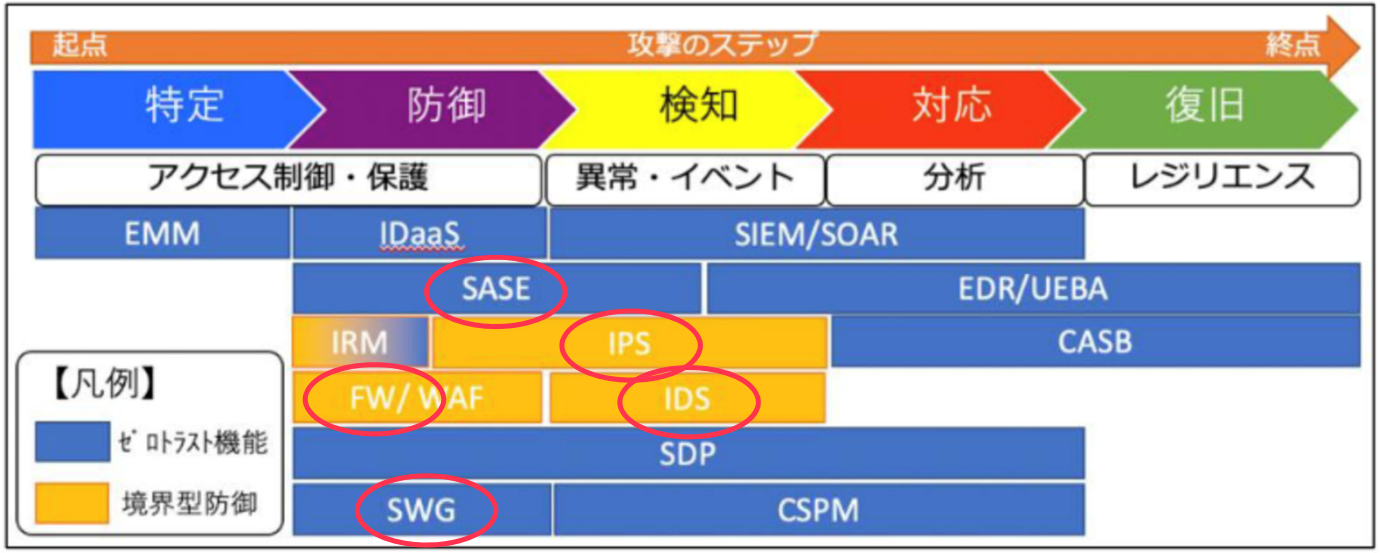
境界型防御から端末単位で防御するゼロトラストの考え方へ





ゼロトラストの考え方に求められる機能

ゼロトラストの実現には、SASEに加え様々な機能が必要



出典：IPA「ゼロトラスト導入指南書」よりサイバーセキュリティフレームワークへの防御機能の落とし込み

IIJセキュアアクセスサービス（上記SASE、SWG）に加え、IIJのセキュリティサービスやソリューションを組み合わせることで、ゼロトラスト機能の拡大が可能

安全をあたりまえに
wizSafe

IIJセキュアアクセスサービスのご紹介

安全なリモートワーク環境の実現へ
「セキュア」「シンプル」「低価格」の三拍子が揃ったネットワーク

安全をあたりまえに wizSafe

社内・社外というネットワーク境界を取り払い、ユーザとアプリケーションを保護

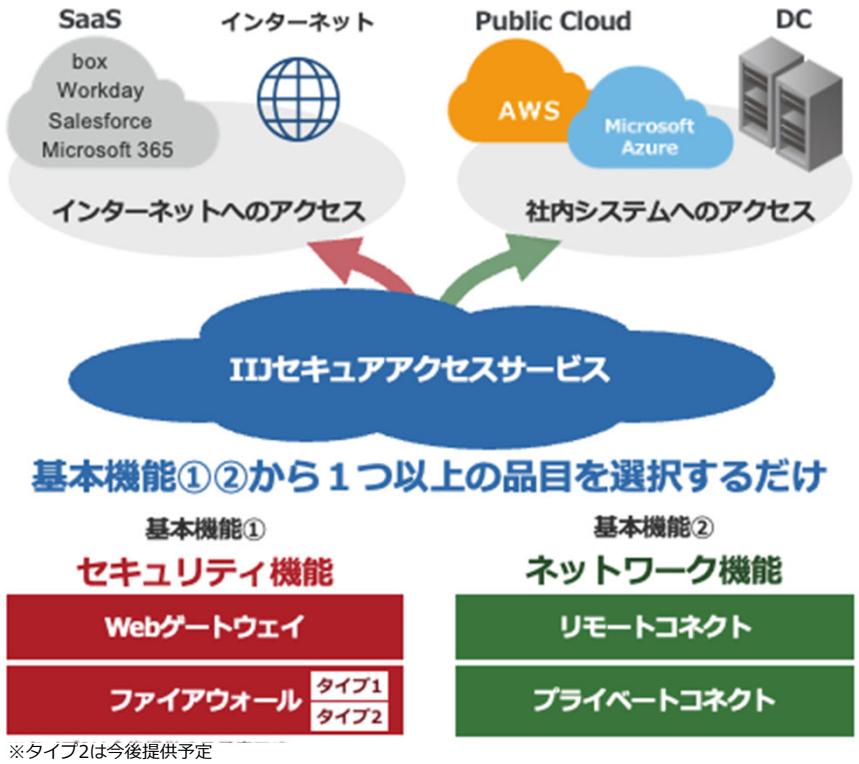
データセンター中心の従来のインターネットゲートウェイ構成ではなく、社内・社外のネットワーク境界に捉われないネットワークとセキュリティを1つにしたプラットフォームをご提供します。

機器導入が不要で利用する機能を選択するだけ

「セキュリティ機能」と「ネットワーク機能」から、それぞれ必要な機能を1つ以上選択することで利用できます。
※別途、利用端末へのエージェントインストールが必要です。

コストパフォーマンスにこだわって自社開発

最小50ユーザから利用できます。デバイス数による課金ではないため、1ユーザが複数デバイスを利用する昨今のワークスタイルでも、コスト影響を最小限に抑えられます。



※タイプ2は今後提供予定

IIJセキュアアクセスサービスのポイント

IIJがこれまで培ってきた”ネットワーク・クラウド・セキュリティ”の技術をもとに
国内企業がSASEに求める機能を１つのパッケージサービスで提供する。

1. ISPの利点を生かした**トラフィック課金がない価格体系**で提供
2. 多機能で複雑なSASEサービスを **シンプルでわかりやすい価格体系** で提供
3. 最少50ユーザから利用できる**低価格な料金体系**で提供
4. 運用効率を上げるため **すべての機能を集中管理できるIIJ独自UI** を提供
5. 高度化する脅威に対抗するため **SOC（セキュリティオペレーションセンター）の情報や専門家の知見をフル活用** する
6. 社会情勢やトレンド変化に強い**柔軟性と適応力を持ったサービス**を内製開発で提供

ユーザ数 × 品目選択のシンプルなサービスメニュー

安全をあたりまえに wizSafe

基本機能

セキュリティ機能

- Webゲートウェイ
- ファイアウォール タイプ1 / タイプ2

※タイプ2は今後提供予定

1つ以上の品目を選択してください。

ネットワーク機能

- リモートコネクト
- プライベートコネクト

1つ以上の品目を選択してください。

サービス標準提供機能


- サービスポータル


- 東西での冗長構成


- ログ・監視機能

※ログ機能は今後提供予定

＋

有償オプション

- 専用IPアドレスオプション
- 導入支援オプション

※今後提供予定

各品目の機能

セキュリティ機能

Webゲートウェイ

Web通信に対してフィルタリングやアンチウイルス処理及び各種アクセス制御を行うサービス

- プロキシ
- HTTPSデコード
- URLフィルタリング
- アプリケーション制御
- アクセス制御
- アンチウイルス
- サンドボックス
- 経路設定
- プロキシパック

ファイアウォール

タイプ1

ステートフルなアクセス制御機能を提供するサービス

- アクセス制御
- 経路設定

ファイアウォール

タイプ2

クラウド上でお客様専用のFortiGate VMを提供するサービス

- L4アクセス制御
- HTTPSデコード
- クラウドアプリケーション制御
- アンチウイルス
- 侵入防御

ネットワーク機能

リモートコネクト

インターネット上の端末がIIJセキュアアクセスサービスのWebゲートウェイ及びファイアウォール（タイプ1、タイプ2）を利用するためのサービス

- 暗号化接続
- クライアントソフトウェア
- ユーザ認証
- 固定IPアドレス
- 経路制御

プライベートコネクト

IIJセキュアアクセスサービスとIIJプライベートバックボーンサービスを接続するためのサービス

- トラフィック中継
- 経路広報

各品目の機能：Webゲートウェイ

Web通信に対してフィルタリングやアンチウイルス処理を行う機能をご提供

Webゲートウェイ

Web通信に対してフィルタリングやアンチウイルス処理及び各種アクセス制御を行うサービス

- プロキシ
- HTTPSデコード
- URLフィルタリング
- アプリケーション制御
- アクセス制御
- アンチウイルス
- サンドボックス
- 経路設定
- プロキシパック

特徴

- **IIJセキュアWebゲートウェイで培ってきた経験をWebゲートウェイ機能に集約**
- **アンチウイルス、URLフィルタリングのSWGに求められる機能に加え、サンドボックスや、アプリケーション制御を実装**
- **アプリケーション制御は、利用しようとしているクラウドアプリケーションを識別し、個別に利用の可否を制御可能**

各品目の機能：ファイアウォール

通信を制御する機能をご提供

ファイアウォール：タイプ1

ステートフルなアクセス制御機能を提供するサービス

- アクセス制御
- 経路設定

ファイアウォール：タイプ2

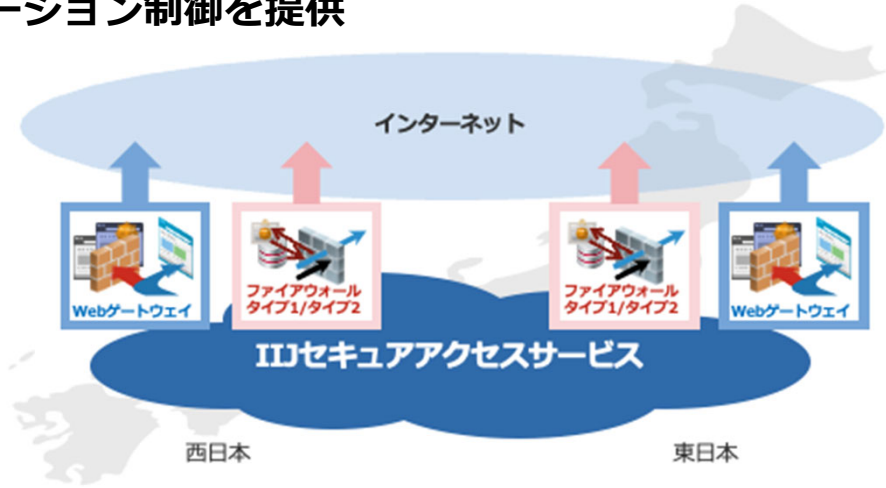
クラウド上でお客様専用のFortiGate VMを提供するサービス

- L4アクセス制御
- HTTPSデコード
- クラウドアプリケーション制御
- アンチウイルス
- 侵入防御

※ 今後提供予定

特徴

- **利用用途に合わせて、ファイルウォール機能を選択。アクセス制御を提供するシンプルなタイプ1とセキュリティ機能を強化した高機能なタイプ2の2種類のラインアップ**
- **タイプ2は、アンチウイルスや侵入防御（IPS機能）、クラウドアプリケーション制御を提供**

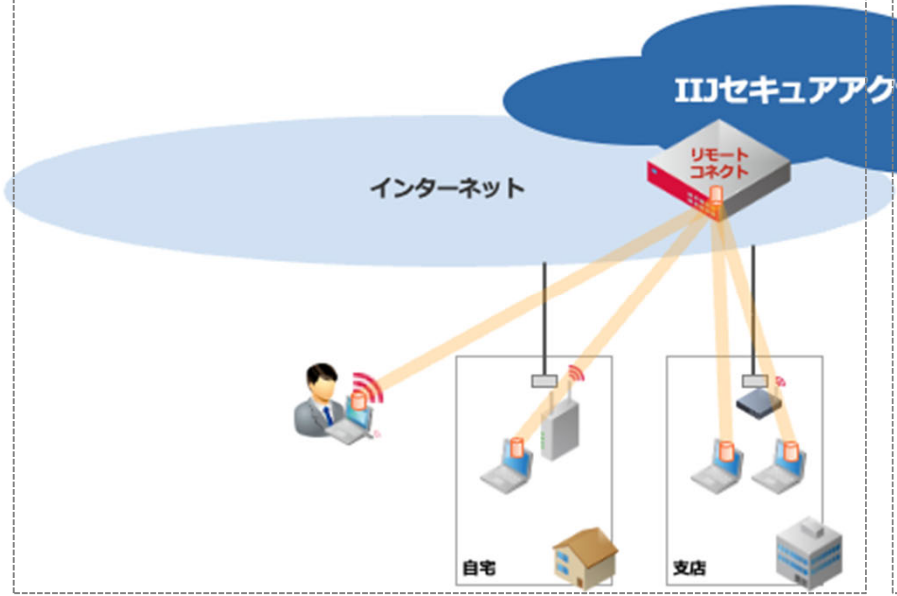


各品目の機能：リモートコネクト、プライベートコネクト

リモート接続とプライベートバックボーンを接続する機能をご提供

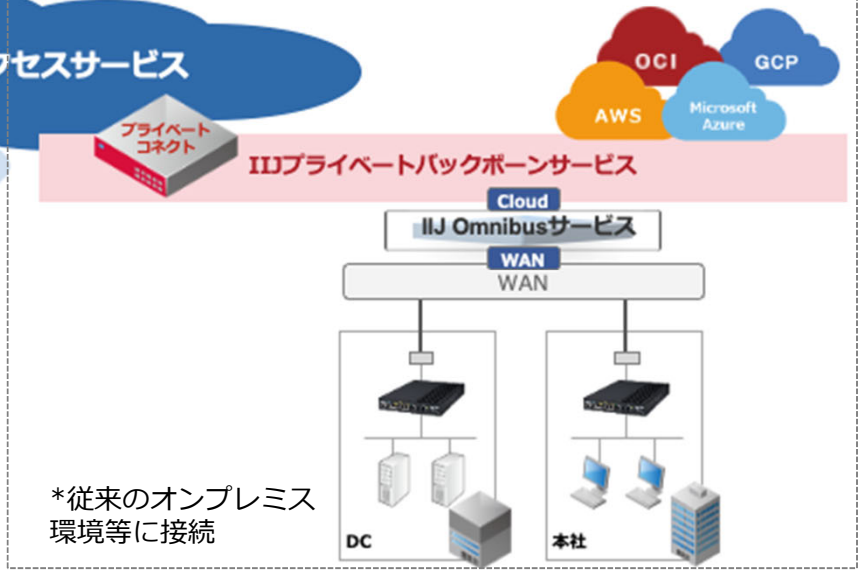
リモートコネクト

インターネット上の端末がIIJセキュアアクセスサービスに接続するための機能



プライベートコネクト

IIJセキュアアクセスサービスとIIJプライベートバックボーンサービスを接続するための機能

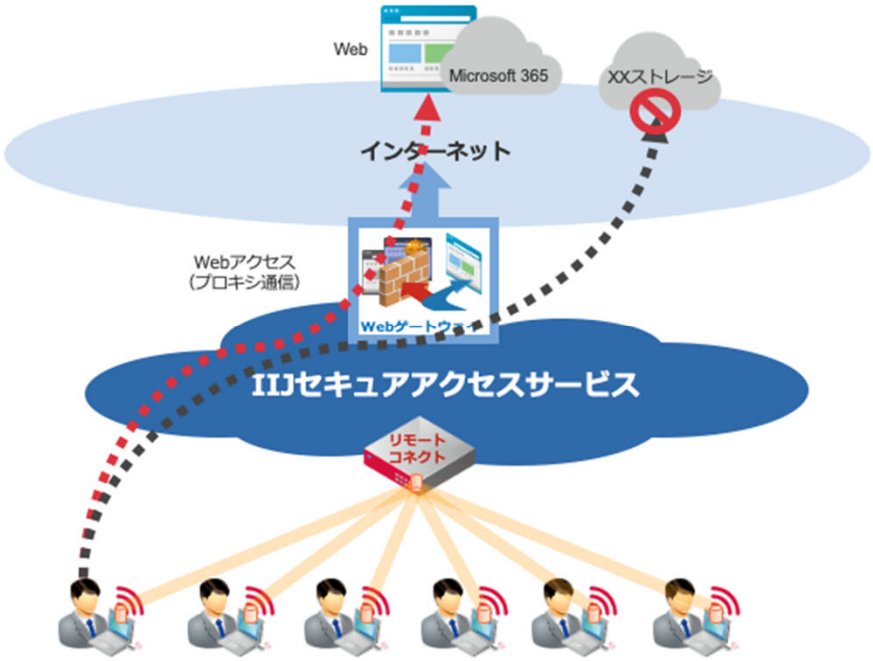


*従来のオンプレミス環境等に接続

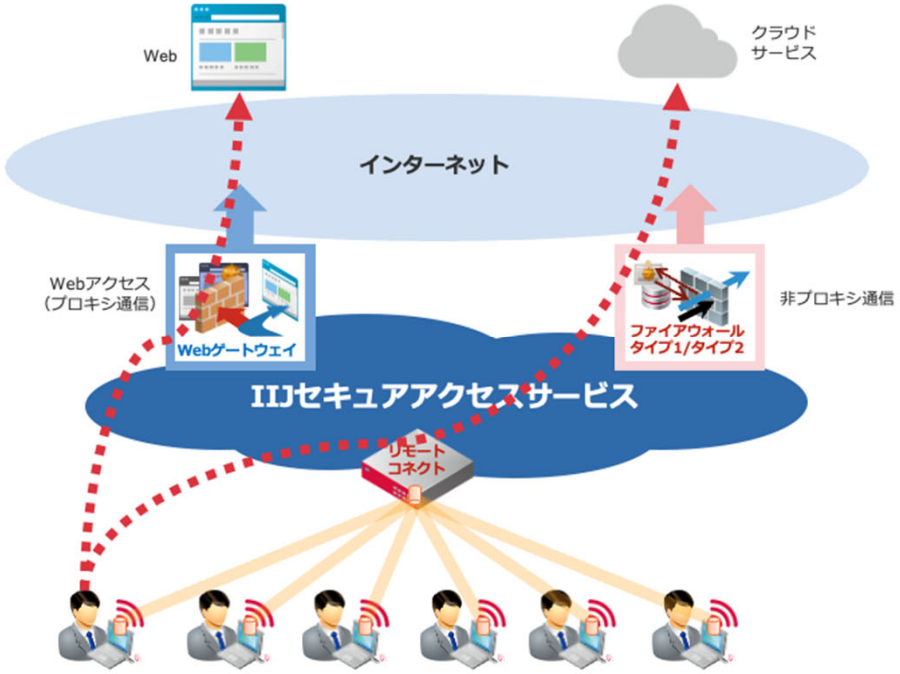
サービスイメージ

必要な構成を組み合わせて利用可能

Webアクセス（プロキシ通信）のみ利用



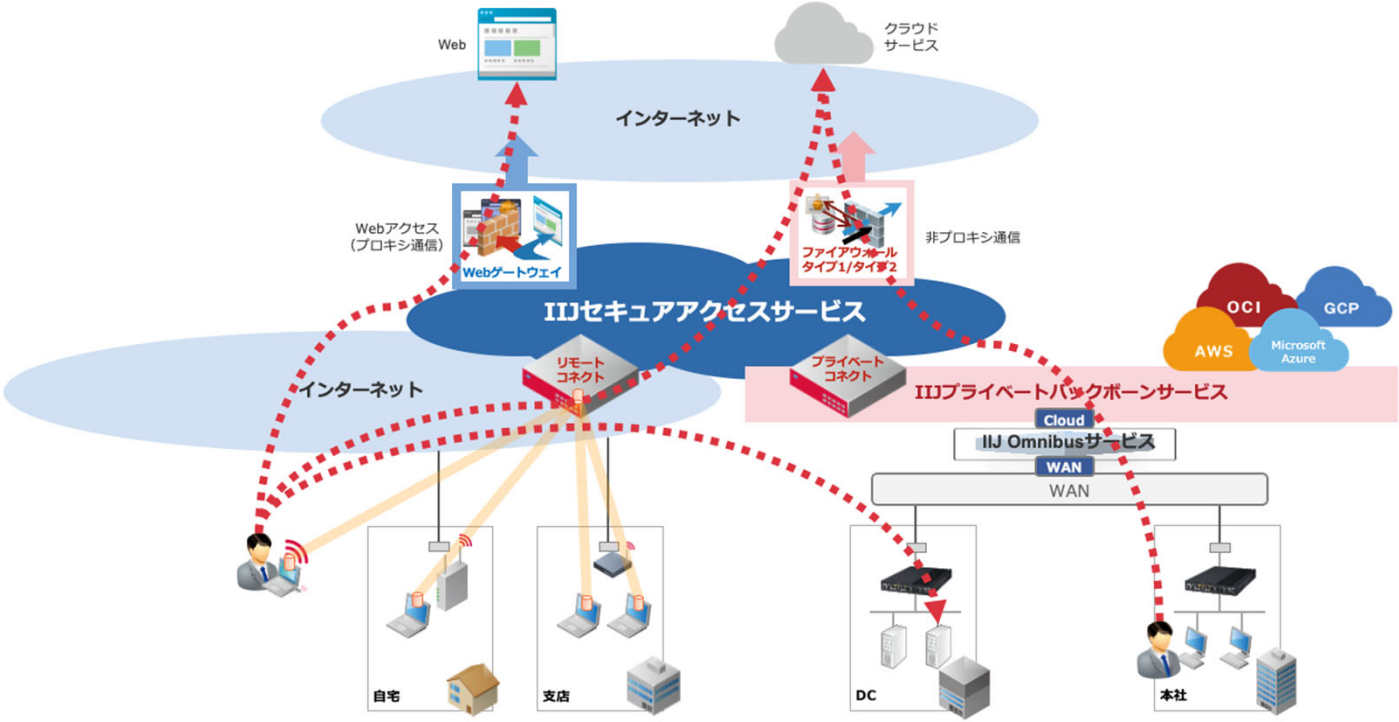
Webアクセス（プロキシ通信）と
非プロキシ通信の利用



サービスイメージ

必要な構成を組み合わせて利用可能

Webアクセス（プロキシ通信）と非プロキシ通信、プライベートコネクトの利用



安全をあたりまえに
wizSafe

C-SOCサービスとの連携

IIJ C-SOCサービスとの連携

IIJセキュアアクセスサービスで取得したログを収集、分析し、セキュリティインシデントの発見と対策を支援
日々発生するセキュリティイベントの確認や分析、対策検討などのお客様の負担を軽減します

セキュリティログ分析

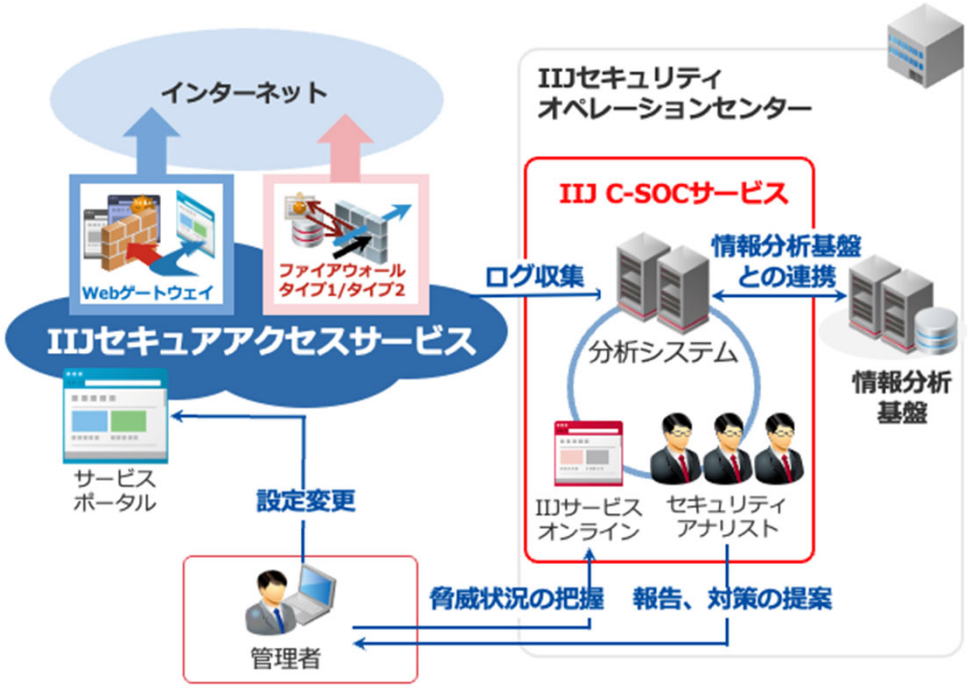
Webゲートウェイ、ファイルウォールタイプ1/タイプ2のログを分析し、情報分析基盤で生成したセキュリティインテリジェンスと連携することで、単体のセキュリティログでは検知できないセキュリティインシデントを検出します。

セキュリティインシデント通知

セキュリティインシデントを検出した場合、セキュリティアナリストが確認を行い、重大度レベルの高いインシデントについてお客様に通知します。

タイプ	特長
アドバンスト	リアルタイム監視を実施します。IIJサービス以外にもお客様運用機器を監視対象に加えることが可能です
ベーシック	平日日中帯に、1日2回のログ分析を実施します。24時間365日のリアルタイム監視までは必要とされないお客様に推奨するプランです

※利用にはC-SOC ISA連携モジュールの契約が必要です



安全をあたりまえに
wizSafe

構成例・価格

構成パターン＆料金例（IIJセキュアアクセスサービス単体）

構成パターン

500ユーザのWebセキュリティ対策を兼ね備えたインターネット接続環境

- Webゲートウェイ
- ファイアウォール タイプ1
- リモートコネクト

構成図

料金（税抜）

品 目	ユーザ単価	月額費用
IIJセキュアアクセスサービス	360円	180,000円
Webゲートウェイ	410円	205,000円
ファイアウォール：タイプ1	100円	50,000円
リモートコネクト	120円	60,000円
合計	**990円**	**495,000円**

品目	初期費用
初期費用	550,000円
専用IPアドレスオプション	200,000円

構成パターン＆料金例（ IIJセキュアアクセスサービス＋C-SOC）

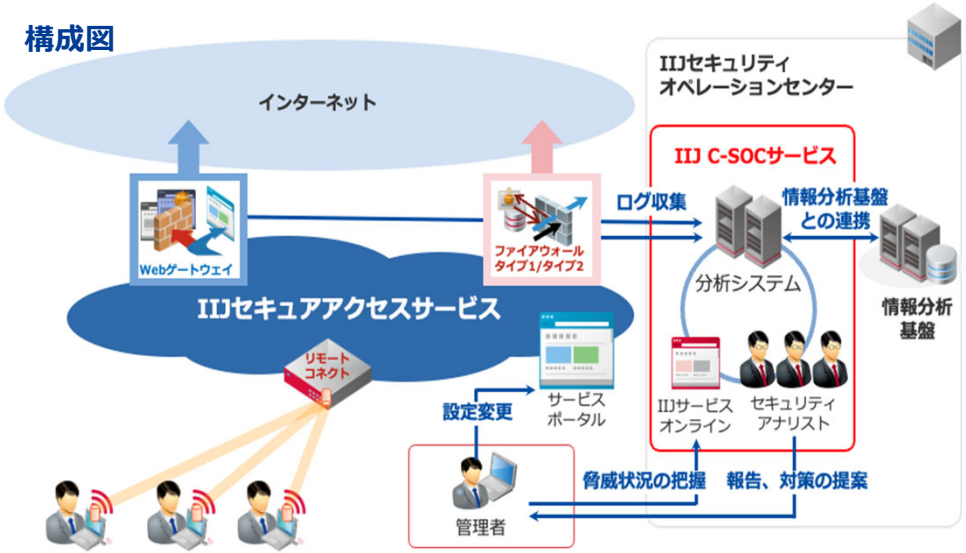
安全をあたりまえに wizSafe

構成パターン

500ユーザのWebセキュリティ対策を兼ね備えたインターネット接続環境（以下）に加え、IIJ C-SOCサービス ベーシックを契約した場合

- Webゲートウェイ
- ファイアウォール タイプ1
- リモートコネクト

構成図



料金（IIJセキュアアクセスサービス） 税抜

品 目	ユーザ単価	月額費用
IIJセキュアアクセスサービス	360円	180,000円
Webゲートウェイ	410円	205,000円
ファイアウォール：タイプ1	100円	50,000円
リモートコネクト	120円	60,000円
合計	**990円**	**495,000円**

品目	初期費用
初期費用	550,000円
専用IPアドレスオプション	200,000円

料金（IIJ C-SOCサービス　ベーシック） 税抜

品 目	ユーザ単価	月額費用
IIJ C-SOCサービス（ISA連携）	―	60,000円
Webゲートウェイ	120円	60,000円
ファイアウォール：タイプ1	120円	60,000円
合計	―	**180,000円**

品目	初期費用
初期費用	120,000円

wizSafe

安全をあたりまえに

安全をあたりまえに
wizSafe

参考：セキュリティ事業の紹介

IIJセキュリティ事業の沿革

安全をあたりまえに wizSafe

1992 **国内初**のインターネット接続事業者として創業

1993 **国内初**「インターネット接続サービス」開始

1994 **国内初**「ファイアウォールサービス」開始

1999 **国内初**フルマネージド型ファイアウォールサービス「IIJセキュリティスタンダード」開始

2001 IIJインシデントレスポンスチーム「IIJ-SECT」結成（IIJ group Security Coordination Team）

2004 **国内初**「迷惑メールフィルタ」開始

2005 技術レポート「Internet Infrastructure Review（IIR）発刊」

2006 マルウェア対策のための活動「MITF」開始（Malware Investigation Task Force）

2007 IIJセキュリティ事業の新ブランド「wizSafe（ウィズセーフ）」開始
IIJセキュリティオペレーションセンター刷新
セキュリティ情報発信サイト「wizSafe Security Signal」開設

2009 **国内初**「送信ドメイン認証技術」、「DDoS対策サービス」開始

2015 「IIJセキュアMXサービス」開始

2017 「IIJセキュアWebゲートウェイサービス」開始

2018 「サンドボックスオプション」開始

2019 「IIJ DDoSプロテクションサービス/広帯域版」
「IIJ C-SOCサービス」開始

2020 「IIJセキュアエンドポイントサービス」開始

「IIJマネージドWAFサービス」開始

「IIJマネージドファイアウォールサービス」海外展開 開始

IIJセキュリティブランド ”wizSafe（ウィズセーフ）”

安全をあたりまえに
wizSafe

日本のインターネットを支えてきた **熱い思い**

新たな脅威からお客様を守り続ける **技術力**

すべての人が安心できる世界を実現するのは **IIJ**

wizSafeは、”wiz＝wiz：様々な分野に熟練した職人、with：一緒に/共に、wisdom：知恵、safe = 安心/安全”を組み合わせた造語です。

〝**wizSafe**〟は、お客様の安全を実現するために行う
IIJのセキュリティの取り組みを総称する事業ブランドです。

セキュリティエンジニアの活躍

安全をあたりまえに wizSafe

マルウェア解析とフォレンジック調査能力において世界的にも評価されています。

IIJのセキュリティエンジニア、セキュリティの国際カンファレンス「Black Hat USA 2019」においてトレーニングコースを提供

「Black Hat Japan Trainings 2019」においてもトレーニングを実施

2019年7月30日

> このニュースのPDF版 [231KB]

株式会社インターネットイニシアティブ（IIJ、本社：東京都千代田区、代表取締役社長：勝 栄二郎、コード番号：3774 東証第一部）のセキュリティエンジニア3名が、世界で最も有名かつ実績があるセキュリティカンファレンスの1つである「Black Hat USA 2019」において、トレーニングプログラムの講師に選ばれました。IIJのエンジニアがBlack Hat USAのトレーニングで講師を務めるのは、日本人として初めて選ばれた昨年に引き続き2回目となります。

Black Hatは、1997年に米国ラスベガスで始まり、現在では、世界トップレベルの情報セキュリティイベントとして、米国、ヨーロッパ、アジアで年に各1回開催されています。最新の研究成果を発表するブリーフィングと、技術的な実践演習を行うトレーニングがあり、すべてのコンテンツはBlack Hatのボードメンバーによって選ばれます。IIJのエンジニアは、2019年8月3日より4日間にわたり、米国ラスベガスにて、海外のマルウェアアナリスト、インシデント対応者、CSIRTメンバー等約40名向けに、過去に発生したインシデント（事案）を再現し、デジタル・フォレンジック（調査）とマルウェア解析の総合演習を行います。

今回講師を務めるセキュリティエンジニアは、これまで「Black Hat USA/Europe 2018」、日韓台シンガポールの学生向けセキュリティキャンプ「Global Cybersecurity Camp 2018」、東京2020オリンピック・パラリンピック競技大会関係組織向けに国立研究開発法人情報通信研究機構（NICT）が主催する「サイバーコロッセオ」等において、講演やトレーニングを多数実施しています。

トレーニング概要

タイトル	A Comprehensive Guide to Digital Forensics & Malware Analysis for Practical Incident Response （実践的インシデント対応のためのデジタル・フォレンジックとマルウェア解析の総合演習）
内容	実際に起きたインシデントに基づいたシナリオに沿って、デジタル・フォレンジック手法およびマルウェア解析を用いたインシデントレスポンスの実践的なトレーニングを行います。 具体的には、マルウェアを用いて標的型攻撃を受けた仮想の企業ネットワーク環境を用意し、攻撃の過程と影響を調査する一連の流れを体験することで、攻撃者の手法や影響調査、再発防止策検討などを包括的に学びます。
期間・場所	2019年8月3日～8月6日　Mandalay Bay（米国ラスベガス）
講師	• IIJ セキュリティ本部 セキュリティ情報統括室 マルウェア＆フォレンジックアナリスト 鈴木 博志 • IIJ セキュリティ本部 セキュリティ情報統括室 スレットアナリスト 梨和 久雄 • IIJ セキュリティ本部 セキュリティビジネス推進部 セキュリティオペレーションセンター アナリスト 六田 佳祐

2018年度 JNSA表彰のご報告

2018年度

2018年12月21日
特定非営利活動法人 日本ネットワークセキュリティ協会

JNSAでは、情報セキュリティ向上のための活動を積極的に行い広く社会に貢献した、あるいはJNSAの知名度向上や活動の活性化等に寄与した個人、団体、JNSAワーキンググループを対象に「JNSA賞」と称する表彰を贈る制度を、2006年度に発足いたしました。
この賞は、情報セキュリティの向上に寄与された方々を広く紹介し、その活動を称え、更に積極的な活動をしていただけるよう、設置したものです。この賞が、広く社会に情報セキュリティが根付く発端となり、より良い社会を実現できる一助になればと考えています。

受賞者決定まで

2018年10月に、過去にJNSAの知名度向上、活動の活性化、また広く社会の情報セキュリティの 向上に貢献した個人、団体、JNSAワーキンググループの推薦（自薦、他薦は問わず）を募集し、12月に最終選考会を開催し、受賞者を決定しました。

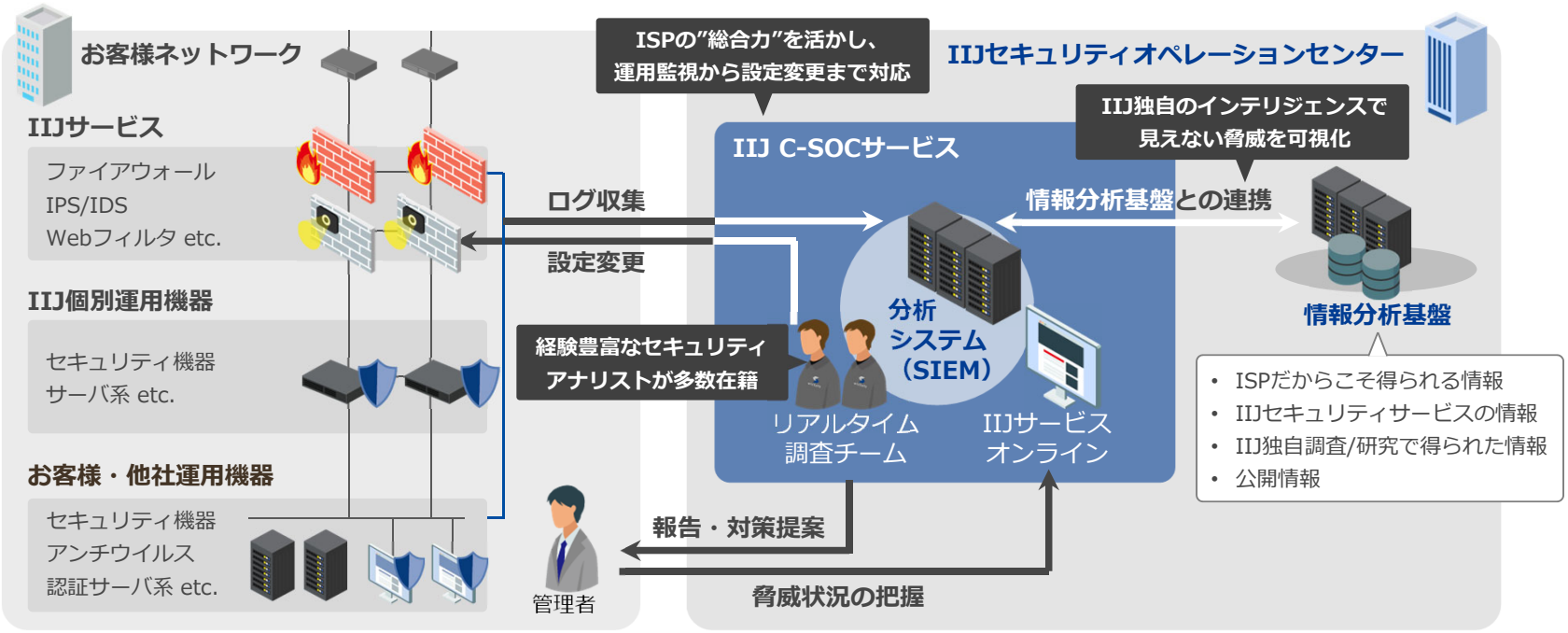
表彰式

2019年1月22日（火）にベルサール神保町で開催のJNSA新年賀詞交歓会の場にて、JNSA賞受賞者の表彰式を行いました。当日は、田中会長より各受賞者へ表彰状・表彰楯・金一封が授与されました。

2018年度　受賞者

<IIJ C-SOCサービス> サービスイメージ

セキュリティ機器やお客様運用機器のセキュリティログの分析を行い、
インシデントの発見から対策の提案、IIJ運用機器の設定変更までを実施します。



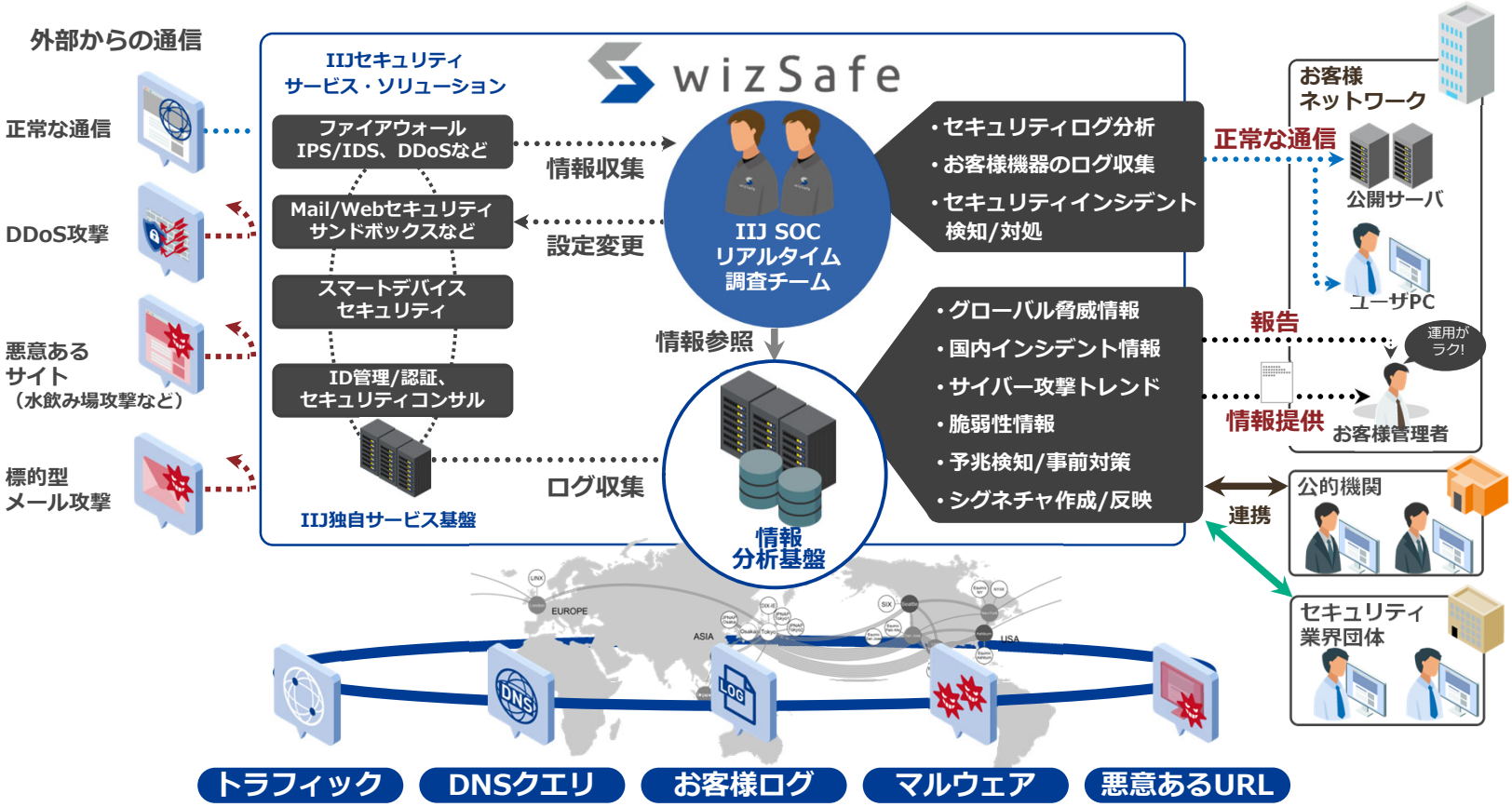
外部団体との連携

IIJは2002年にCSIRTの国際団体FIRSTに加盟し、国際間連携を深めてきました。
国内でも各団体との連携を行い、インシデントへの対応能力を向上させています。

FIRST （Forum of Incident Response and Security Teams）	一般財団法人ICT-ISAC （ICT-ISAC Japan）	日本セキュリティオペレーション事業者協議会（ISOG-J）
日本シーサート協議会 （CSIRT）	NPO法人日本ネットワークセキュリティ協会（JNSA）	特定非営利活動法人 デジタル・フォレンジック研究会

IIJセキュリティ事業強化の全体像 ～IIJ SOCによる統合運用～

安全をあたりまえに wizSafe



wizSafe

安全をあたりまえに