

IIJセキュリティ事業説明会



2022年2月24日
株式会社インターネットイニシアティブ
セキュリティ本部長
齋藤 衛

この1年の脅威動向について

コロナ禍の影響

アウトソーシング先が関係する事件

クラウドサービスの安定性

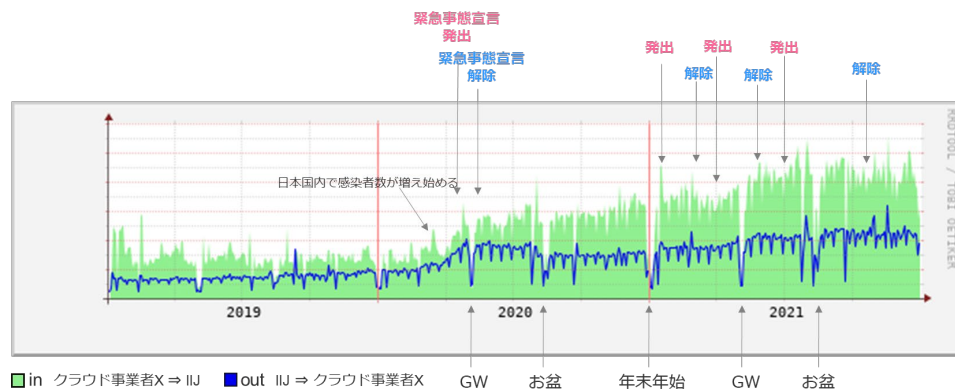
IoT装置の脆弱性

恐喝や社会情勢に関連するDDoS攻撃

ランサムウェア

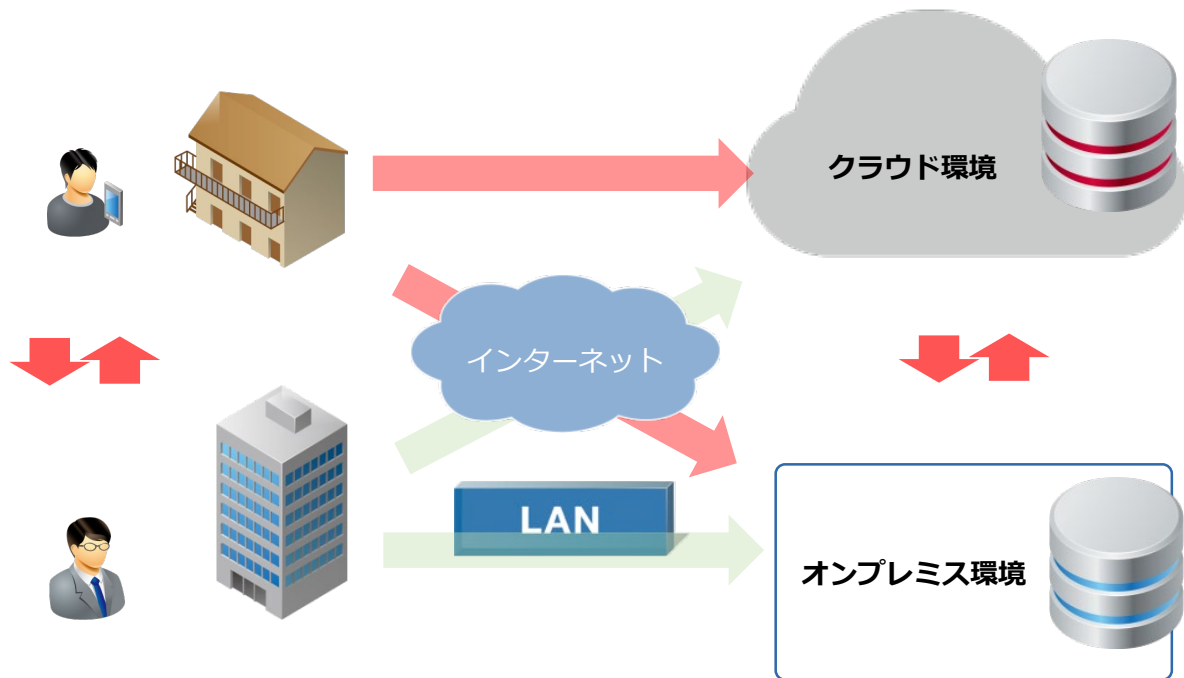
コロナ禍の影響

- ネットワーク上の様々な変化
 - テレワーク関連通信の増加
(2020年2月から6月に大幅増加)
 - 通信の方向の変化、時間の変化
 - 動画配信サービス
 - 地域差
- 仕事の仕方の変化
 - テレワーク
 - リモート会議の増加
 - リモート国際会議
 - 接待の減少
 - 仕事をする場所の多様化
(会社、自宅、サテライトオフィス)
 - リモートしか会ったことない人との関係



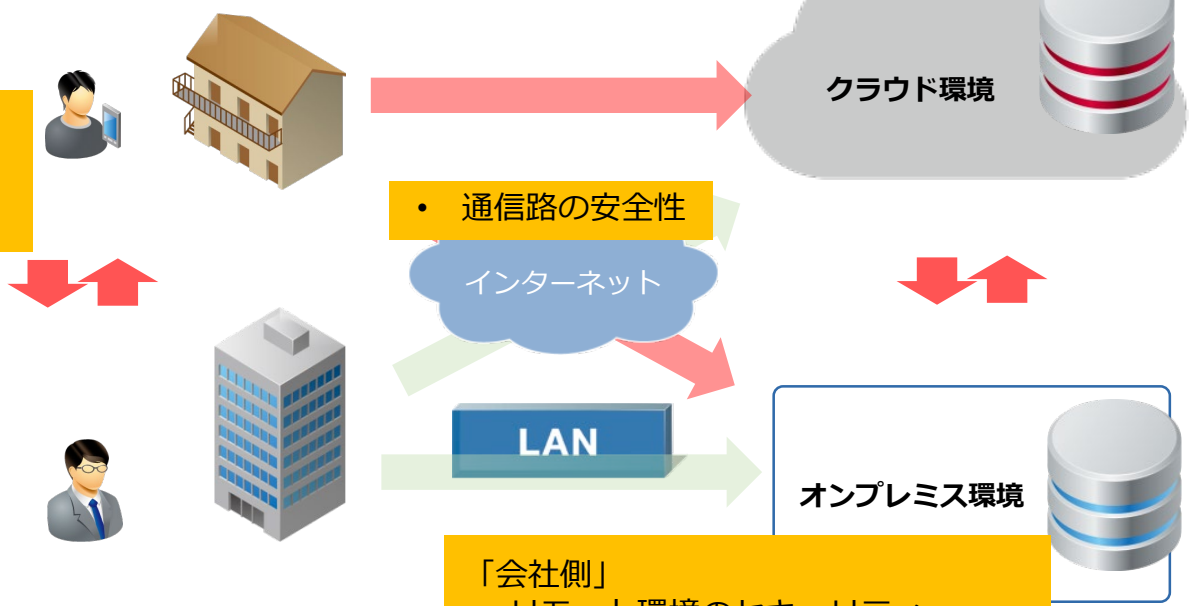
2022/01開催「新リモートアクセスサービス説明会」資料より
あるクラウド事業者とIIJの間の通信量の変化

コロナ禍の影響



コロナ禍の影響

- 「従業員」
- 家庭での働き方
 - 家庭のIT環境の安全性



- クラウドサービスの信頼性
- クラウドサービスの設定
- クラウドサービスの利用ログ取得、監視

- 通信路の安全性

- 「会社側」
- リモート環境のセキュリティ
 - 従業員の仕事の管理
 - テレワークに対応していない行事

アウトソーシング先が関係する事件

いわゆるサプライチェーン攻撃の一種で、業務で利用するソフトウェアパッケージ、システム構築や運用のアウトソース先などが関係する事件

- 米国のIT運用管理ツールの特定のバージョンにバックドアが仕込まれていた。
米国政府関係機関含む最大18,000組織が影響を受けた。
- 国内電力関連企業にシステム運用企業経由で不正アクセスが発生
 - 攻撃者は、システム運用企業が提供する ITシステム運用監視サービスを経由してアクセス。システム運用に利用するソフトウェアの脆弱性を悪用され、侵入したサーバ関連情報が流出。
- 大手SIerの利用する情報共有ツールからの情報漏洩
 - 社内外の関係者と情報を共有するために利用していたツールの一部で不正アクセスを確認。
 - 国内100組織以上の組織に関連する情報が流出した。
- 米国におけるシステム運用会社ランサムウェア大量感染被害
 - リモート監視・管理製品 脆弱性が悪用され、これを利用するシステム運用会社60社弱が攻撃を受け、これらの会社の顧客である最大1,500の組織がランサムウェアに感染。

クラウドサービスの安定性

- クラウドサービスを使い仕事をするようになってきた。
- スマートフォン、タブレットなどのように、クラウドサービスと連携して情報を処理する端末で仕事をするようになってきた。
- クラウドサービス上の設定ミスや脆弱性が深刻な問題に
 - 大手クラウドサービスのゲストユーザ関連設定不備による情報漏洩。
 - ゲストユーザに過剰な権限設定を与えている場合に、第三者に情報が漏洩する可能性。クラウドサービス側ではユーザによる設定不備との立場。
 - 大手クラウドサービスの設定ミスで3800万件の個人情報流出。
 - 大手クラウドサービスの提供するDBに脆弱性、利用者によるリスク軽減が必要に。

クラウドサービスの安定性

• 障害

- 2020/12/14 クラウドサービスの障害により連動するIoTが動作不備に、スマートキーが動作せず自宅に入れられないなどの影響
- 2021/2/20 クラウドサービスで5時間にわたる障害。複数のホームページなどに影響
- 2021/2/26 クラウドサービスの障害で、交通関連や防災関連のサービスに影響
- 2021/3/11 クラウドサービスが約1時間半の間全世界でダウン
- 2021/4/1 クラウドサービスのネット障害で複数のサイトやサービスがダウン
- 2021/5/10 クラウドサービスで緊急修正の実施により約5時間にわたり障害
- 2021/6/8 CDNサービスの障害で政府機関サイトなど一時ダウン
- 2021/6/23 クラウド連携に関する障害でスマートフォンが動作しない
- 2021/7/26 CDNのソフトウェア更新が原因で障害
- 2021/9/2 クラウドの国内設備のハードウェア故障で障害。復旧に数時間
- 2021/10/5 クラウドサービスで設定ミスにより6時間の障害
- 2021/10/6 クラウドのネットワーク障害により複数の決済サービスが利用不能に

IoT装置の脆弱性

- IoT装置の誤動作、乗っ取り、動作停止
 - 家電の誤動作から火災など。
 - プライバシーにかかわる情報が扱われている。
 - 電気ガス水道など生活インフラに対する影響。
 - 従来家電などと同じように扱われている。
 - PCやスマートフォンのようにソフトウェアの更新の仕組みがこなれていない。
 - 攻撃の踏み台として悪用される。

IoT装置の脆弱性

- 2020/12/23 とあるメーカーの「TCP/IPスタック」に複数脆弱性が見つかりリモートコード実行の可能性
- 2021/5/7 IoT機器や制御機器に用いるRTOSにリモートコード実行の脆弱「BadAlloc」
- 2021/5/7 国内メーカー一部Wi-Fiルーターなどに脆弱性、「製品の使用停止」を推奨
- 2021/5/14 ほぼすべてのWi-Fi機器に影響する脆弱性「FragAttacks」
- 2021/5/25 Bluetooth CoreとMeshの仕様に脆弱性
- 2021/5/31 VPN製品脆弱性についてFBIから再度注意喚起
- 2021/7/6 国内メーカー製ルーターに脆弱性。修正はなく使用中止を勧告
- 2021/7/29 複数の国内製ルータソフトに脆弱性
- 2021/8/5 組み込みTCP/IPスタック「NicheStack」に脆弱性

恐喝や社会情勢に関連するDDoS攻撃

- DDoS攻撃とは
 - 特定の宛先に大量の通信を送付することで、攻撃先のサーバの処理能力や回線容量を無駄に浪費させることで、正常な処理を行えなくする攻撃。
- 大量の通信の作り方
 - 多人数で通信行う、専用攻撃ツール、PCのマルウェアやボット、リフレクション（反射型）攻撃、IoTボット
 - 特に、2016年オリンピックリオデジャネイロ大会あたりから、脆弱なIoTをマルウェアに感染させ、大量の装置から同時に通信を発生させるDDoS攻撃が頻発している。

恐喝や社会情勢に関連するDDoS攻撃

- 恐喝 DDoS 攻撃キャンペーン
 - 2019年10月、2020年8月に続いて世界中で発生した恐喝 DDoS 攻撃キャンペーンが再び活発に活動再開。2021年1月、10月、11月。
 - 攻撃パターンは前回同様に UDP アンプを中心とする複合攻撃で、攻撃継続時間が6～9時間程度と、前回よりも長期化する傾向であった。
 - 金融機関や通信会社ほか、多数の業種がターゲットとなる。
 - 前回のキャンペーンで被害を受けたところが再び狙われるケースがある。
- 国内外の攻撃事例
 - 1/28 国内クラウドで DDoS 攻撃による障害発生 (約 3時間)
 - 2/1 国内オンラインサービスで DDoS 攻撃による障害発生 (約 7時間)
 - 9/4 ニュージーランドの金融機関に対するDDoS攻撃

恐喝や社会情勢に関連するDDoS攻撃

- Anonymous による OpMyanmar 作戦
 - 2月にミャンマーで発生した軍事クーデターに抗議する活動として、Anonymous が OpMyanmar という攻撃作戦を開始。関連サイトへの DDoS 攻撃や Web サイト改ざんなどを実施。
 - ヤンゴンにある軍事博物館跡地への開発事業に日本が出資していることなどから、自民党、経団連、首相官邸ほか 30余りのサイトが攻撃ターゲットに指定される。
 - 4/7 に Anonymous が上記リストに含まれる日本の2サイトを DDoS 攻撃したとツイート。
- 東京オリンピック大会に係る攻撃活動
 - 大会運営に影響を与えるようなサイバー攻撃はなかった。
(サイバーセキュリティ戦略本部 第31回会合 (令和3年9月27日) 資料4より)

ランサムウェア

- ランサムウェア
 - マルウェアによりHDDなどに記録された情報を勝手に暗号化し、利用者から不当にアクセスできなくする（人質にとる）。効果を上げるためのばらまき型。
- 標的型ランサムウェア
 - 身代金を支払いそうな特定の標的に対してランサムウェアによる攻撃を仕掛ける。身代金は高額。
- 暴露型ランサムウェアと情報漏洩
 - ランサムウェアを感染させて、暗号化するまえに情報を窃取（外部に転送）。
 - その後、情報を暗号化して人質にとることで身代金を要求。
 - さらに秘密の情報をリークサイトに暴露すると恐喝して金銭を要求。
 - リークサイトはランサムウェアの種類もしくは感染活動を行っている主体ごとに設置。
 - 通常はダークウェブ上にあるが、暴露が目的なのでダークウェブにアクセスできる人は誰でも見られる状態にある。

ランサムウェア

• 事例

- 米大手石油パイプライン ランサムウェアに感染し、影響確認のために操業を停止。
- 食肉加工大手企業がランサムウェアに感染し操業を一時停止、3日後に復旧。
- 国内自治体向けコンサル企業がランサムウェア感染による情報流出、複数の地方行政、中央省庁にかかわる委託業務に影響。
- 国内建設コンサルタントにサイバー攻撃 公共事業データが盗まれた可能性。
- 徳島県の公立病院でランサムウェア感染。

IIJセキュリティ事業の概要

wizSafe ～安全をあたりまえに～

セキュリティが組み込まれたサービスの提供を通して、
脅威を意識せずに、全ての人が安心してICTを利用できる未来を実現する。



wizSafe

安全をあたりまえに

社会を支える

安全であることを当然の品質と捉え、安定したIT環境を提供することで、企業の活動から人々の豊かな生活まで、社会を根幹から支えます。

安全を高める

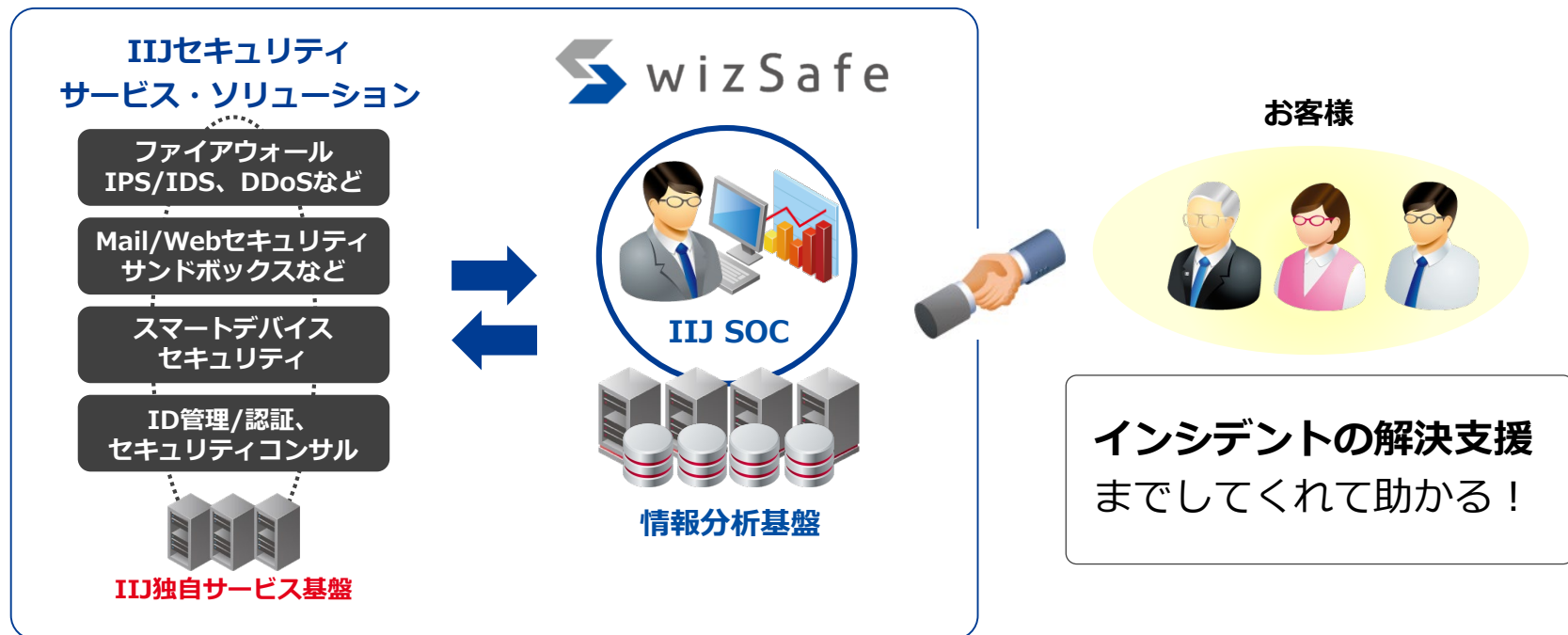
豊富な脅威情報データベースと、高度な分析技術による独自情報の積極的な提供により、社会全体のセキュリティレベルを高めます。

変革を起こす

次代を先取る先見性を持つと同時に、変化を恐れず、必要に応じて“ITセキュリティ”を根底から変革していきます

セキュリティ事業の概要

IIJ SOCを核とした各種サービス・ソリューションの提供により
インシデント発生時の対応支援まで包括的に実施。



セキュリティ本部 部門紹介

セキュリティ事業に必要な組織としての機能・役割を本部内に集約。
案件ごとの状況に応じて、関係者が柔軟に連携し対応。

セキュリティオペレーションセンター

“マルウェア、フォレンジック、ビッグデータ”
各アナリストやインシデントハンドラー

01

“SOCインフラ” 部門

IJ SOCを支えるシステム基盤を運用する
セキュリティエンジニア

02

“SI案件担当” 部門

お客様の細かな要望に応えるアカウント
エンジニア、セキュリティコンサルタント

03

“セキュリティリサーチ” 部門

マルウェア解析、暗号などの調査・研究
を行うスペシャリスト

04

“サービス運用” 部門

サービスで提供しているハードウェア・
ソフトウェアの運用エンジニア

05

“サービス開発” 部門

最新の技術動向やニーズを追いかけ、
IJ独自サービスを開発するエンジニア

06

“システム開発” 部門

サービス基盤システムの設計から開発まで
トータルで行う開発エンジニア

07

“サービスサポート” 部門

お客様からの日々の問い合わせ対応を行う
サポートエンジニア

08

セキュリティ本部

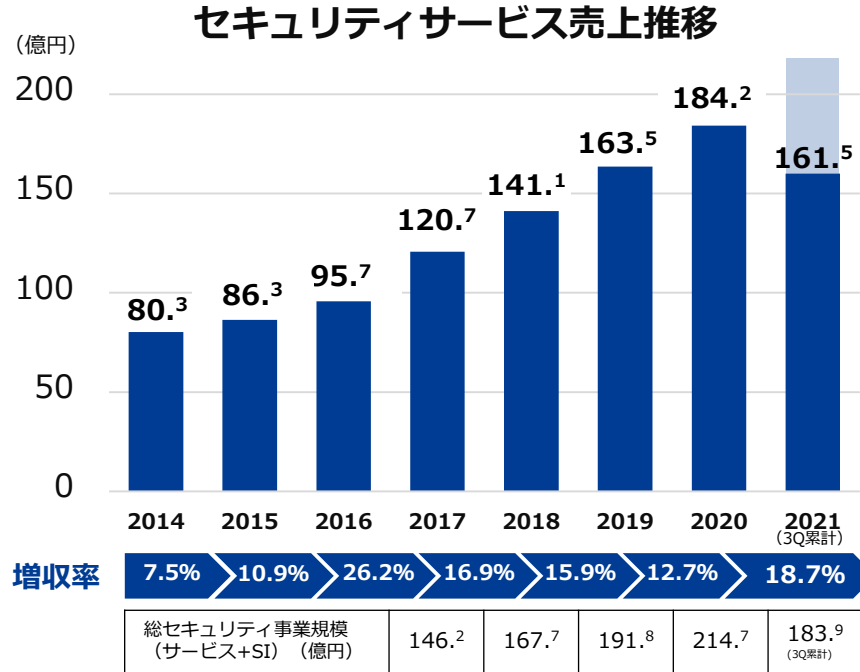
IIJセキュリティ事業の全体像 ~IIJ SOCによる統合運用~



2021年度 事業概況

セキュリティ事業概況

事業強化を開始した2016年以降、継続して二桁の増収率を維持。



月額課金サービスによる 安定したストック売上

IIJセキュアWebゲートウェイサービス、IIJセキュアMXサービス、IIJマネージドファイアウォールサービス等、長年提供しているサービスが支えるセキュリティサービスの安定した収益を維持しています。

働き方の変化に伴う新たな セキュリティニーズに対応した新サービス

新型コロナウイルスの感染拡大を受け、テレワーク活用の広がり、クラウド利用へのシフト等、働き方、ICT利用の変化が見られます。それらの変化に対応した新しいサービスの投入により成長を継続させています。

2021年度 新サービス

コロナによる外部環境の変化

新型コロナウイルスの感染拡大により社会・生活が変化したことで、
各業界のデジタル化が進展、それらに合わせて脅威も変化。

新型コロナウイルス発生

社会・生活が変化

外出・移動の制限

社会的距離の確保

世界的経済危機

社会的価値観や
ビジネス規範の変化



各業界のデジタル化が進展

企業



在宅勤務/リモートワーク
業務環境のクラウド化

自治体



業務プロセスのデジタル化
窓口業務のオンライン化

小売



オンライン販売
無人店舗

教育



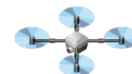
オンライン授業
映像・タブレット教材

医療



遠隔オンライン診療
電子カルテ

物流



ドローンによる無人物流
宅配ビジネス

脅威も変化

新型コロナ関連ワードを
用いた攻撃の増加

VPN製品の
脆弱性を突いた攻撃

クラウドを狙った攻撃



IIJフレックスモビリティサービス/ZTNA

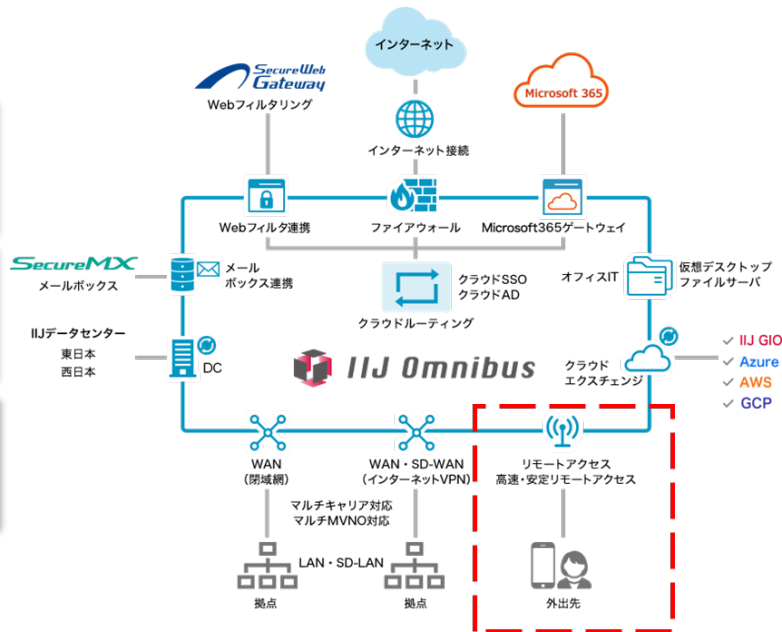
IIJ Omnibusを構成するサービスの中で
ゼロトラストネットワークの機能を追加したリモートアクセスサービス。

Enterprise VPN
最適化された快適な通信

ZTNA
セキュアな接続コントロール

DEM/可視化
詳細な利用状況・リスクの把握

※ZTNA : Zero Trust Network Access
※DEM : Digital Experience Monitoring



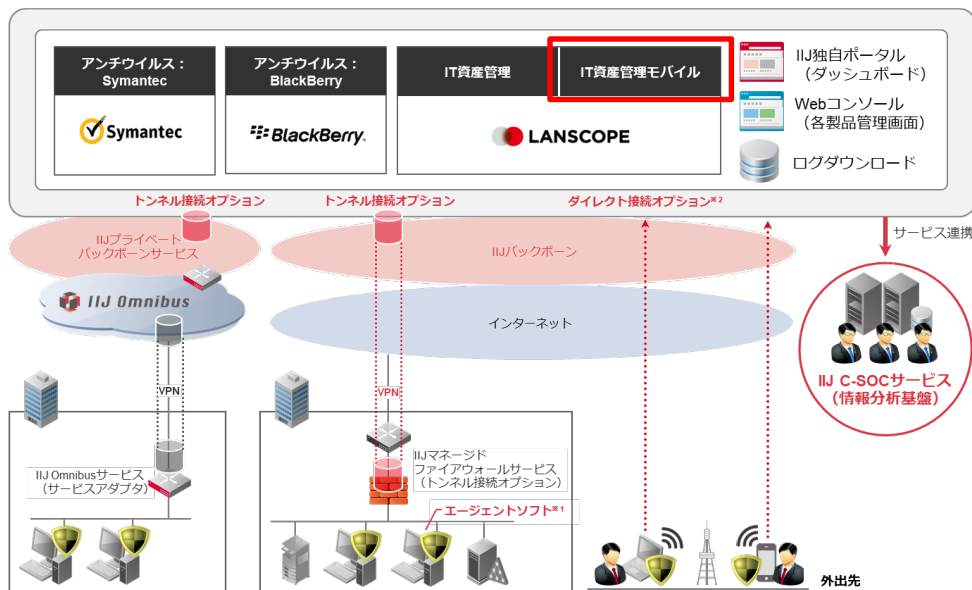
IIJ Omnibus

IIJ Omnibusは企業ネットワーク全体をカバーする、ネットワーククラウドのブランド

IIJフレックスモビリティサービス/ZTNA

「IT 資産管理機能」と「MDM機能」を一元的に提供。
PC・iOS/Androidの一元管理を実現する豊富な機能を搭載。

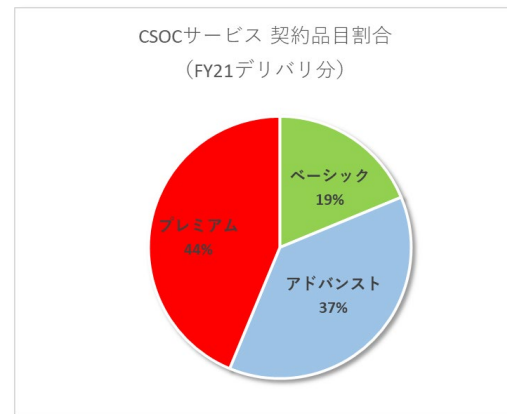
- 資産情報の自動取得やアプリ配信でPC・スマホ・タブレットのIT資産管理を効率化。
- 脆弱性の利用ルールに違反しているデバイスを把握。
- PC・iOS/Androidの操作ログを自動で取得、利用状況の把握が可能。



IIJ C-SOCサービス プレミアム

不正通信の遮断など能動的に対応。
初動の時間を短縮し、関連する事象に関してスレットハンティングの実施でお客様のセキュリティ運用の負荷と被害リスクを軽減します。

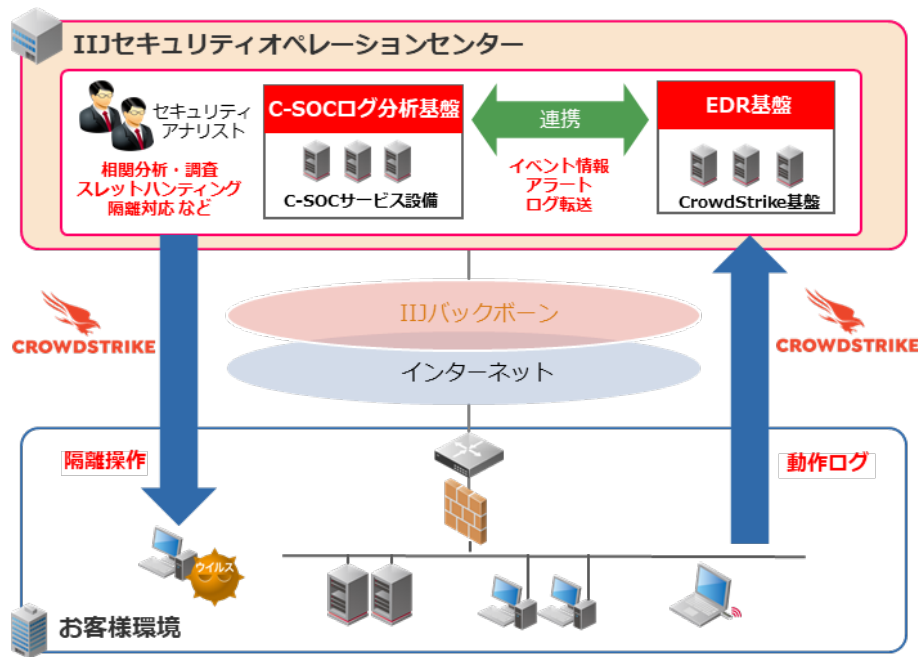
	プレミアム	アドバンスト	ベーシック
インシデント検知 (ログ分析基盤)			
インシデント分析 (セキュリティアナリスト)			
インシデントの通知 対策の提示			
IIJサービス に対する一次対応			
お客様社内対応 (端末隔離など)			
		お客様確認	お客様確認



3つのメニューでお客様のニーズに対応

お客様端末に導入したEDRツール（CrowdStrike Falcon）の運用を代行してインシデントの一次対応を行う。

- ネットワークだけでなくクライアントでも検知を実施。
- インシデントを詳細化して封じ込めなどを実施。
- クライアントに対するインシデント対応の時間が不要。お客様は再発防止策の検討などインシデントへの事後の対応に注力できる。



クラウドサービス利用を把握し、管理統制するためのプラットフォーム 導入から運用までフルサポート

■ シャドーITの可視化

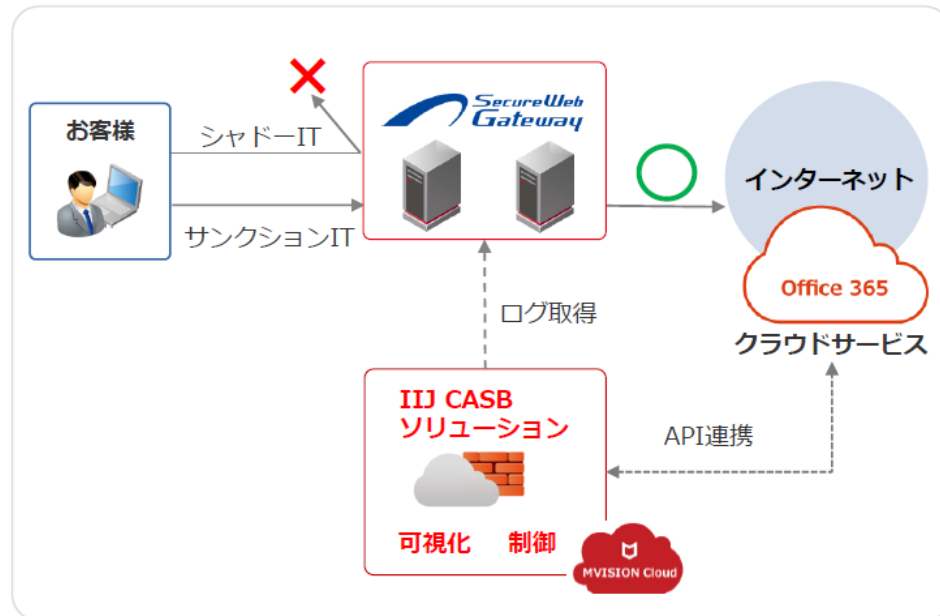
- 情報漏えい等の脅威に繋がるリスクのあるシャドーITの利用状況把握のため、“誰が、いつ、どのサービス”にアクセスしているか見える化します。

■ サンクシオンITの可視化・制御

- お客様のクラウドサービスをAPI連携することで、利用状況を可視化し、必要によりクラウド上に配置されたファイルの隔離、共有権限の削除が可能となります。

■ 導入後の運用サポート

- 導入後の運用サポートでは、ログ連携に必要なサーバをフルマネージドで運用します。また、DLP作成支援も可能です。

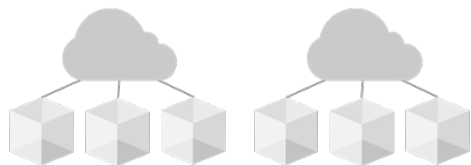


CASB (Cloud Access Security Broker) : 複数のクラウドプロバイダーの間に単一のコントロールポイントを設け、クラウド利用の可視化や制御を行う

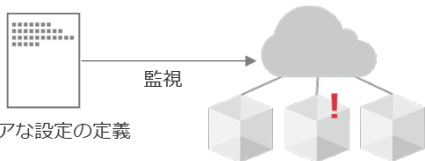
IIJ CSPMソリューション

IaaSの設定不備による脆弱性を可視化。異なるクラウドプロバイダの
一括管理でクラウド特有のセキュリティリスクを低減。

マルチクラウド・マルチアカウントを一元的に監視



ポリシー違反のリソースを検出・アラート通知



セキュアな設定の定義

Microsoft Azure・AWS・GCPに対応



アクセスしません



コンテンツ

OS & アプリケーション



インスタンス



CSPM の
監視範囲

アカウント制御

(IAM / アクセスキー)

暗号化

(データ、トラフィック)

アクセス制御

(セキュリティグループ / サービスポード)

ロギング

(FlowLogs / CloudTrail / Inspector / GuardDuty)

ネットワーク

(VPC / インターフェース / ロードバランサー)

IIJ CSPM
ソリューション



クラウドプロバイダの
責任範囲

ルータ

スイッチ

ハブ

ハイパーバイザ





データセンタ

各クラウドプロバイダの
基盤

CSPM (Cloud Security Posture Management) : 「クラウドセキュリティ動態管理」あるいは「クラウド設定に関する状態管理」

自社のセキュリティサービス運用やインシデント対応で培った知見をベースに実践的プログラムを提供。

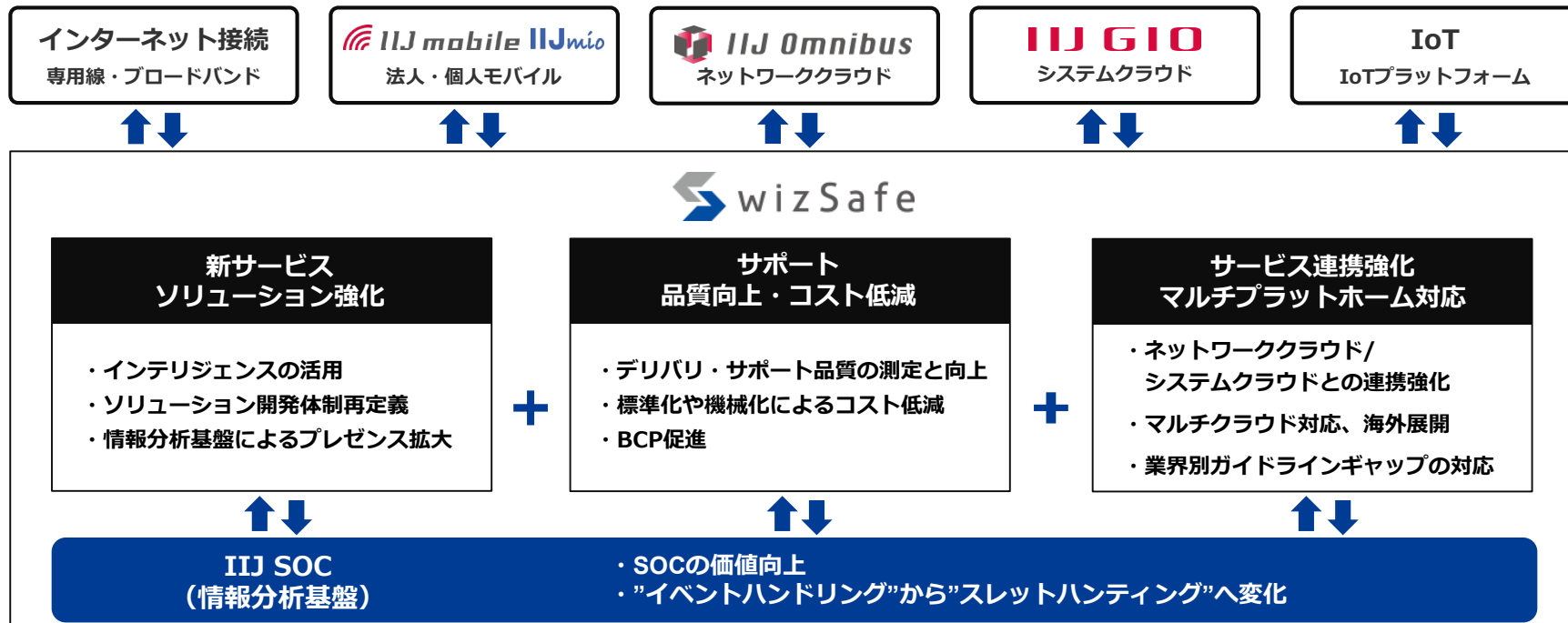
- 長年のセキュリティ運用で得られた“知見”と“ノウハウ”を伝授。
- 最新のセキュリティ脅威への対応手法や対策も学べる。
- 実践的な演習を通して必要な知識・技術を短期間で習得。

	Information Coordinator 	Security Analyst 	Incident Handler 	System Administrator 
役割	<ul style="list-style-type: none"> ・自組織内外連絡担当 ・情報発信担当 ・リーガルアドバイザー 	<ul style="list-style-type: none"> ・リサーチャー ・セキュリティ戦略 ・脆弱性診断士 ・セルフアセスメント 	<ul style="list-style-type: none"> ・コマンダー ・インシデント管理・処理 ・フォレンジック ・マルウェア解析 	<ul style="list-style-type: none"> ・IT戦略・システム企画 ・基幹システム構築・運用・保守 ・インフラ構築・運用・保守 ・サポート・ヘルプデスク
高度			<div style="border: 1px solid black; padding: 2px; text-align: center;">マルウェア解析</div> <div style="border: 1px solid black; padding: 2px; text-align: center;">フォレンジック</div>	
応用	<div style="border: 1px solid black; padding: 5px; text-align: center;">セキュリティ マネジメント</div>		<div style="border: 1px solid black; padding: 2px; text-align: center;">パケット/ログ分析・解析</div> <div style="background-color: #0056b3; color: white; padding: 2px; text-align: center;">インシデントハンドリング実践コース</div> <div style="background-color: #0056b3; color: white; padding: 2px; text-align: center;">攻撃技術理解・防御 APT対策基礎コース（仮称、2022年3月 提供開始予定）</div>	<div style="border: 1px solid black; padding: 2px; text-align: center;">脆弱性診断・管理</div> <div style="border: 1px solid black; padding: 2px; text-align: center;">セキュアシステムデザイン</div>
基礎	<div style="border: 1px solid black; padding: 5px; text-align: center;">セキュリティ基礎</div>			

今後の展望

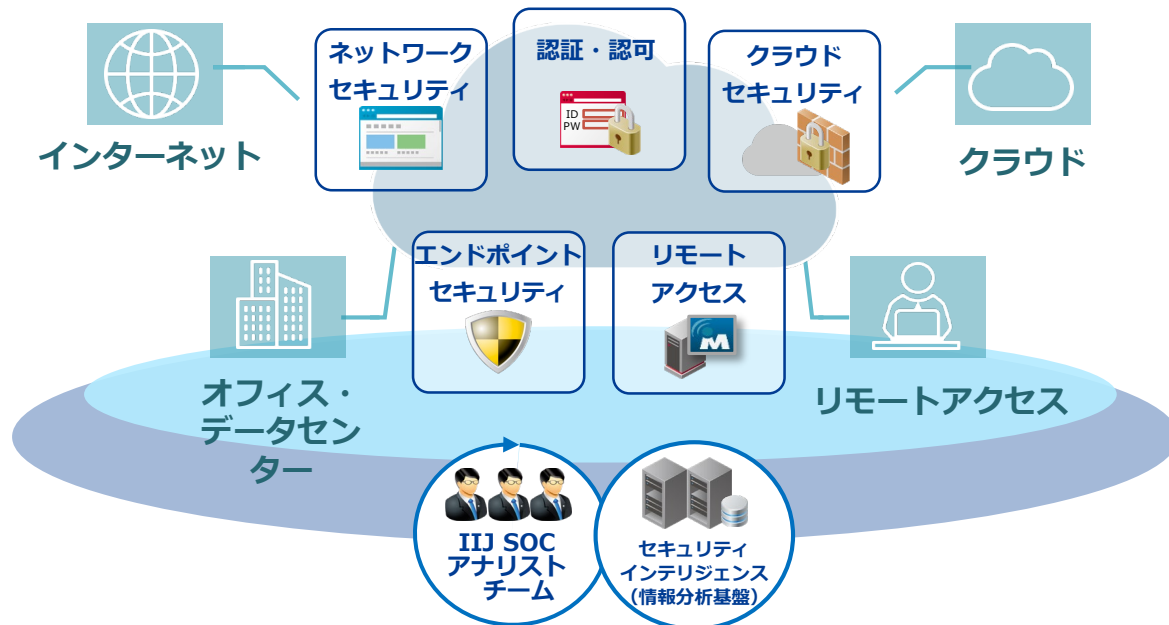
事業の方向性

“あらゆるサービスにセキュリティ要素が組み込まれている状態”を目指し、
各事業領域との連携強化および、必要機能や要素の拡充を実施。



デジタルワークスペースを支えるセキュリティ

誰もが・どこでも・どんなデバイスでも「生産性を落とさずに」かつ「セキュアに」仕事ができる。ワークスペースのセキュリティを支えていきます。





wizSafe

安全をあたりまえに