cisco Secure

増大するサイバー犯罪と新しい働き方を支えるセキュリティ対策

Cisco SASE and Zero Trust Network

シスコシステムズ合同会社
セキュリティ事業 シニアSEマネージャー 西　豪宏
2020年11月19日

Agenda

1. 増大するサイバー犯罪
2. 新しい働き方スタイルのトレンド
3. 新しい働き方を支えるセキュリティ

増大するサイバー犯罪

➢ 脅迫型DDoS攻撃によるオンラインサービスの停止

- 対象：主に金融、証券、トラベル、Eコマース
- 影響：販売チャネル、金融取引停止によるビジネス損失
- 手法：攻撃ボリュームの増加（Bot）-短時間、不特定多数のIPからの攻撃（ランサムDDoS）

➢ 口座情報の不正入手による不正送金被害

- 対象：個人口座、電子決済サービス
- 影響：ブランド価値低下、補償や対応のコスト負担
- 手法：モバイル決済を使った不正送金、フィッシングによる口座情報取得

➢ 情報漏洩・標的型攻撃、ランサムウェア

- 対象：個人情報（口座、など）、顧客情報
- 影響：ブランド価値低下、対応
- 手法：意図的な情報流出や情報紛失、リモートワーカーを狙う

脅迫型DDoS

- DDoS（サービス妨害、停止攻撃）を利用した犯罪グループによる脅迫活動
- 金銭（仮想通貨）を要求する
- 毎年のように実施され、今年は日本もターゲットエリアに指定されている

Cisco Talos 脅威情報ニュースレター（2020/8/27, 9/3）
https://gblogs.cisco.com/jp/2020/09/talos-threat-source-newsletter-for-sept-3-2020/
https://gblogs.cisco.com/jp/2020/09/talos-threat-source-newsletter-for-aug-27-2020/

ニュージーランドの証券取引所が今週、サイバー攻撃を受けて操業を連日停止。現時点での各証拠は、分散型のサービス妨害攻撃であることを示しています。

ニュージーランド政府、国内の民間企業に対してサイバー攻撃の波に備えるよう警告。この警告に先立ち、同国の証券取引所では、最近 2 週間で 5 回目となるサイバー攻撃が発生していました。

DDoS 攻撃を示唆して仮想通貨による送金を要求する脅迫行為 (DDoS 脅迫) について

最終更新: 2020-09-07

ツイート　メール

CyberNewsFlash一覧

I. 概要

JPCERT/CC は、2020年8月以降、DDoS 攻撃を示唆して仮想通貨による送金を要求する脅迫行為に関する情報を複数確認しています。こうした脅迫行為は「DDoS 脅迫」「ransom DDoS」などとも呼ばれ、攻撃者が標的の組織宛にメールを送り、指定する期間内に仮想通貨を支払わなければ、DDoS 攻撃を実行すると脅迫します。過去には類似する攻撃として、2015年に DD4BC グループによる攻撃、2017年には Armada Collective や Phantom Squad を名乗る攻撃者からの攻撃、2019年には Fancy Bear Group を名乗る攻撃者からの攻撃等が確認されています。

JPCERT/CC は、国内の組織を標的とした攻撃に関する情報も確認しており、国内の組織においても引き続き警戒が必要な状況です。2020年8月以降に確認されている攻撃について、公開情報等から攻撃の流れ、手法や特徴を以下に整理いたしました。攻撃を検知および防御するための対策の検討や、攻撃を検知あるいは認知した場合の対応手順や体制を確認する場合の参考情報としてご活用ください。

Source:JPCERT
https://www.jpcert.or.jp/newsflash/2020090701.html

「ランサムDDoS」を国内で観測 - 支払有無で結果変わらず

JPCERTコーディネーションセンターは、8月以降にDDoS攻撃を行うと脅し、金銭を要求する攻撃が発生しているとして注意喚起を行った。攻撃と見られるパケットについても観測しているという。

攻撃対象の組織に対し、指定期間以内に仮想通貨を支払うようメールを送り付け、応じない場合は「DDoS攻撃を行う」として金銭を支払うよう脅迫する「ランサムDDoS（DDoS脅迫）」攻撃が確認されているもの。

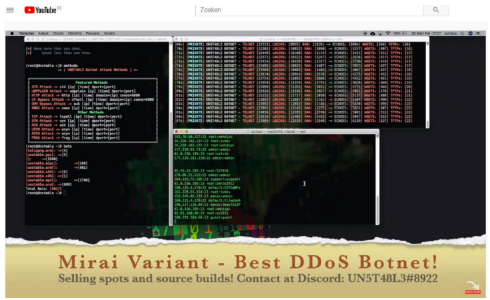
過去にも同様の攻撃が発生しており、目新しい攻撃ではないが、ふたたび8月中旬ごろよりグローバルに攻撃が展開されている。

DDoS攻撃対策を提供する複数のベンダーが観測しているほか、標的型のDDoS攻撃が展開されているとして、米国やニュージーランドなど、各国のセキュリティ機関が注意喚起を行った。

地方銀行、証券取引所、オンライン決済サービス事業者など金融関連サービスをはじめ、旅行代理店、eコマースなどが標的となっており、サービスが停止することでビジネスに大きな影響が及ぶ事業者を狙っている。

Source:Security Next https://www.security-next.com/118189

脅迫型DDoS攻撃によるオンラインサービスの停止



ボットネットの宣伝

身代金要求

Subject: About DDoS Attack

It's a weekend and you deadline is [redacted].

BTC address [redacted] is still empty.

You probably think that we were bluffing, trying to take quick money from you.

We are not.

We will just say one thing: Search news for "[redacted]" or "[redacted]".

You don't want to be like them, do you?

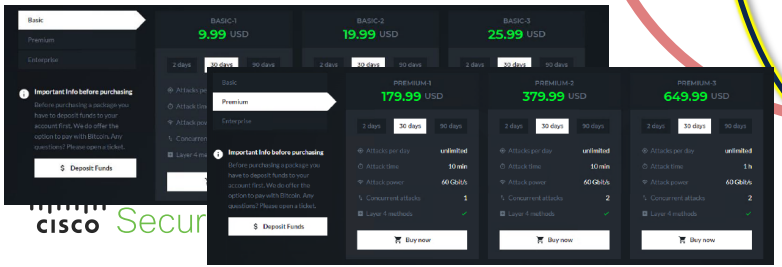
Since we prefer payment over destruction, we will give you a second chance to reconsider and buy Bitcoin if you don't have it, so we will extend the deadline for 1 day - [redacted].

But if we don't receive payment by then, your are going down for good.

攻撃者

DDoS as a Service

DDoS as a Service



オンライン上のデバイスが
攻撃元となる

ボットネット

Internet

公開されている以上は常に
攻撃の対象となる

金融、証券
トラベル、Eコマース

狙われる時事ニュース・返信メールを装う

【重要】特別定額給付金の受給について

このメッセージは '重要度 - 高' で送信されました。

[redacted]銀行 <admin@a3.yyyyyy.rest>
2020-05-26 (火) 15:01
宛先: xxxxxxxxxx@xxxxxx.co.jp

2020年5月8日
令和2年4月20日、「新型コロナウイルス感染症緊急経済対策」が閣議決定され、感染拡大防止
特別定額給付金（仮称）事業が実施されることになりました。

受給口座として、[redacted]銀行もご指定いただけますので、是非、ご活用ください。
https://zzzzzzzzz.com/

特別定額給付金の概要
　令和2年4月20日、「新型コロナウイルス感染症緊急経済対策」が閣議決定され、感染拡大防
置いたしました。

施策の目的
　「新型コロナウイルス感染症緊急経済対策」（令和2年4月20日閣議決定）において、「新型
をはじめとして全国各地のあらゆる現場で取り組んでおられる方々への敬意と感謝の気持ちを
で迅速かつ的確に家計への支援を行う。

事業費（令和2年度補正予算（第1号）計上額）
　12兆8,802億93百万円

給付事業費 12兆7,344億14百万円
事務費 1,458億79百万円
事業の実施主体と経費負担
実施主体は市区町村
実施に要する経費（給付事業費及び事務費）については、国が補助（補助率10/10）
給付対象者及び受給権者
給付対象者は、基準日（令和2年4月27日）において、住民基本台帳に記録されている者
受給権者は、その者の属する世帯の世帯主
給付額
　給付対象者1人につき10万円

特別定額給付金の受給に関連した攻撃メール

リンクをクリックさせてマルウェアに感染させる狙い

差出人 東京支店[redacted]様 <[redacted]@[redacted].ne.jp>
件名 (株)[redacted]次長様
宛先 (株)[redacted]次長様 <[redacted]@[redacted].co.jp>
返信 | 全員に返信 | 転送 | その他
2020/09/01 13:48

協力会社各位

　お世話になっております。

標記の件、2020.09.01に皆様にお送りしたご案内に修正事項がございます。
以下に要点を記載いたしますのご確認の程お願いいたします。

お心当たりがある業者様は取り急ぎご連絡いただきますようお願いいたします。
　今後の手続きについてご案内いたします。

この度は当方の不手際でご迷惑をお掛けし、大変申し訳ございません。

東京支店[redacted]様

件名：Emotet が Word 形式の新しいルアー（囮）ドキュメントを使用開始
説明：Emotet ボットネットは進化し続けており、今や Microsoft Word テンプレートを使用してマルウェアを拡散しています。「Red Dawn」と呼ばれるこの新しい感染方法では、ユーザに Word ファイルをダウンロードさせた後、ドキュメントを読み取るためにマクロを有効化するよう促します。マクロを有効にすると、Emotet が被害者のマシンにダウンロードされます。Emotet のスパムメールは、コロナ情報や財務ドキュメント、発送通知などを装ってユーザを誘導しようとします。
Snort SID：54900、54901

Talos 脅威情報ニュースレター（2020 年 9 月 3 日）
https://gblogs.cisco.com/jp/2020/09/talos-threat-source-newsletter-for-sept-3-2020/

不正送金・不正アクセス

Press Release
報道関係者各位

Source:Kyash

株式会社　Kyash
2020年9月15日

弊社に関する一部報道について

一部
以下
・金
・対
・金
・事
当口
※現

PayPayからのお知らせ

Source:PayPay

2020.09.15　セキュリティ

「PayPay」利用時の本人確認および不正利用防止に向けた対応について

PayPayと連携する金融機関について調査し、追記しました。また、ゆうちょ銀行における不正利用として公表した件数、金額を当社で再調査し、修正しました。

ドコモからのお知らせ

Source:NTT DoCoMo

一部銀行の口座情報を使用したドコモ口座の不正利用について

2020年9月8日

一部の銀行において、ドコモ口座を利用した不正利用が発生しております。

本件は、不正に取得された銀行口座番号やキャッシュカードの暗証番号等を悪用したものであり、当社システムに不正アクセスされ情報を取得されたものではございません。

当社は、これまで不正アクセスに対する二段階認証やアカウントロック等、様々なセキュリティ対策を講じておりますが、お客さまにより安心・安全にご利用頂けるよう、更なる対策強化に努めてまいります。

悪意のある第三者による不正アクセスに関するお知らせ

- ニュースリリース
- 当社
- 岡三証券
- 岡三オンライン証券
- 2020年
- 2019年
- 2018年
- その他の

Source:岡三オンライン証券

2020年9月18日
岡三オンライン証券株式会社

悪意のある第三者による不正アクセスに関するお知らせ

各　位

Source:SBI証券

株式会社SBI証券

悪意のある第三者による不正アクセスに関するお知らせ

2020年9月16日

当社のお客さま口座への悪意のある第三者による不正アクセスにより、お客さまの資産が流出したことが判明いたしました。お客さまには大変ご迷惑、ご心配をおかけいたしましたことを深くお詫び申し上げます。
被害を受けられたお客さまには個別にご連絡を行っており、捜査当局および資産流出先の銀行である株式会社ゆうちょ銀行、株式会社三菱UFJ銀行と連携して対応を進めております。なお、お客さまの被害につきましては資産保護を最優先として、当社が責任をもって速やかに補償することを予定しております。

1.　経緯

当社は、不正アクセスに対するモニタリングを常に行っており、不審なアクセスがあればお客さまに直接ご連絡を行うなどして対応を行っておりますが、直近においても不正ログインを検知し、調査・対策を行っておりました。その過程において、2020年9月7日に寄せられた身に覚えのない取引があったとのお客さまからのお申し出を端緒として、当該お客さまのログ調査等により、不審なアクセス元を特定し、そこからアクセスされたその他の口座や同様の特徴のある取引履歴等を分析いたしました。その結果、悪意のある第三者による不正アクセスが行われ、お客さまの有価証券の売却およびお客さま名義の出金先銀行口座への出金を複数件、確認いたしました。現在、出金先銀行と連携して対応を進めております。

2.　現在判明している被害の状況

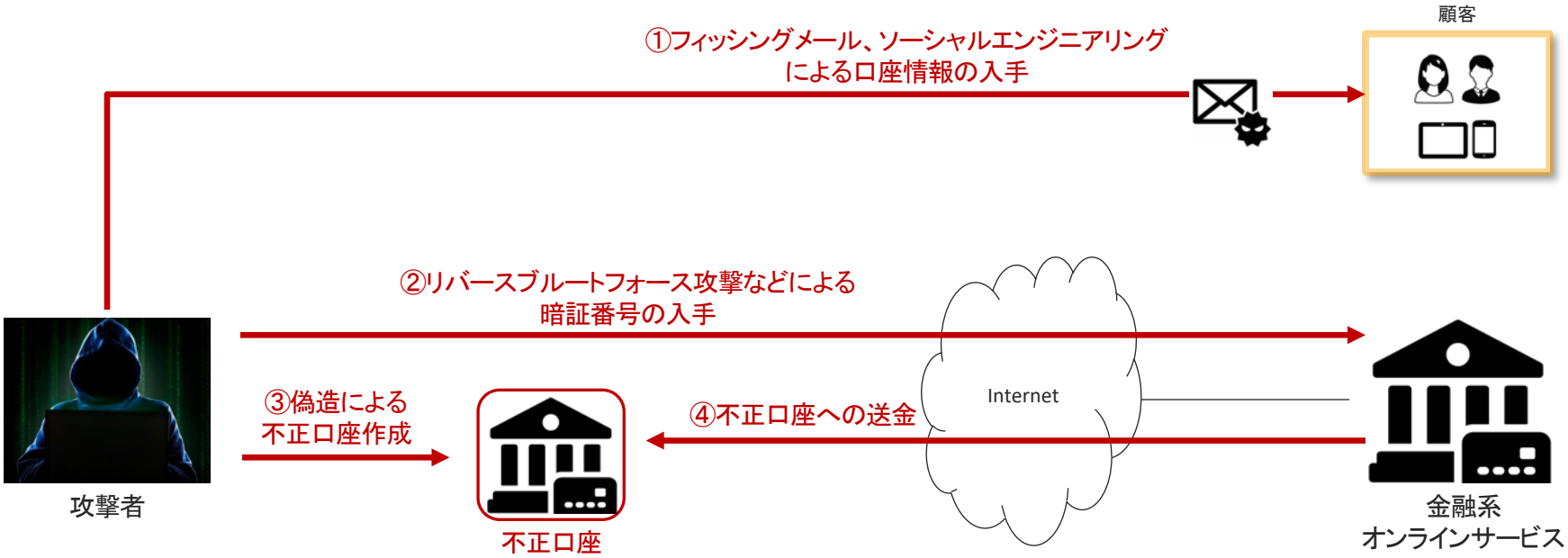
・口座数：6口座　（出金先銀行：ゆうちょ銀行5口座、三菱UFJ銀行1口座）
・被害総額：合計9,864万円（ゆうちょ銀行：9,229万円、三菱UFJ銀行：635万円）

3.　再発防止策

引き続き、本事案の個別原因の分析を継続し、より有効な施策を速やかに実施してまいります。

（1）監視
・不正アクセスに対する24時間モニタリング体制のさらなる強化
・不正アクセス検知システム（WAF）による新たな攻撃手法への対応
・不審なIPアドレスからのアクセス排除（IPレピュテーションサービスの一層の活用）

口座情報の不正入手による不正送金被害



狙われる個人情報・リモートワーク

Talos 脅威情報ニュースレター（2019 年 8 月 29 日）
https://gblogs.cisco.com/jp/2019/09/talos-threat-source-new

件名：人気の VPN サービスの脆弱性により攻撃が集中し、情報が漏えい中
説明：Fortigate および Pulse の各 VPN サービスで見つかった脆弱性で、攻撃者によるエクスプロイトが多発し、暗号化キーやパスワードなどの機密データが盗まれています。先週開始されたこれらのキャンペーンは、Linux および * NIX システムを管理するための Webmin ユーティリティを対象としています。Linux や *NIX システムは企業ネットワーク内のデバイスです。関連する脆弱性により、攻撃者がシステムを完全に乗っ取る危険性があります。
Snort SID：51240 ～ 51243（作成者：John Levy）、51288、51289（作成者：Joanne Kim）

Source:JPCERT https://www.jpcert.or.jp/at/2019/at190033.html
複数の SSL VPN 製品の脆弱性に関する注意喚起 (最終更新: 2019-09-06)
JPCERT/CC では、複数の SSL VPN 製品の脆弱性について、脆弱性に対する実証コードなどの詳細な情報が公表されていることを確認しています。
- Palo Alto Networks (CVE-2019-1579)
- Fortinet (CVE-2018-13379)
- Pulse Secure (CVE-2019-11510)

Talos 四半期レポート：インシデント対応の動向（2020 年夏）2020 年 6 月 15 日
https://gblogs.cisco.com/jp/2020/06/talos-ctir-trends-q3-2020/

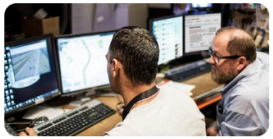
インシデント対応では、4 四半期連続で Ryuk が他を圧倒していました。前四半期のレポートで説明したとおり、Ryuk は、商用化されたトロイの木馬ではなく、環境寄生型ツールを駆使する手口へと転換が進みました。そのため、商用化されたトロイの木馬を利用する攻撃の観測は減少しています。Citrix デバイスと Pulse VPN や、リモート デスクトップ サービス（RDS）に対するセキュリティ侵害も増加していますが、最大の感染ベクトルは今でも電子メールです。今四半期で特に注目すべきが新型コロナ感染症の影響です。興味深いことに、IR 業務では感染症に便乗した事例が観測されませんでした。ただし、コロナ禍の影響で、組織のサイバーセキュリティ インシデントへの対応と封じ込めに影響が出ています。

詳細については、こちらの要約もご覧ください。

初期ベクトル

ロギングの量が十分ではないため、ほとんど
し、初期ベクトルを特定できた事例や合理的
シングです。標的組織の RDS にブルートフォ
ウェア Phobos の増加や、コロナ禍のリモー
ベクトルとして利用されるのは侵害された RI
Gateway（CVE-2019-19781）、さらに
続的に観測されました。

Cisco Japan Blog > 脅威リサーチ



脅威リサーチ

拡大する Snake と Maze ランサムウェア感染の基本情報

TALOS Japan
2020年5月25日

特定の組織のみを狙ったランサムウェア

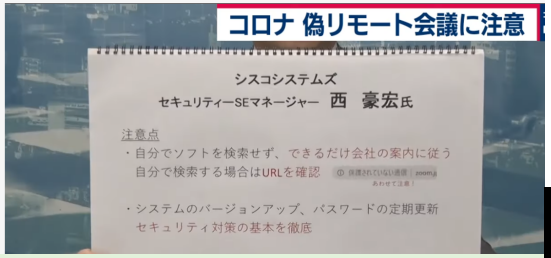
このところ、Maze や Snake を利用したランサムウェア攻撃が目立っています。重要な医薬品企業から大規模な物流企業まで、大小を問わずさまざまな企業が被害に遭っています。

偽サイト・悪質広告

IPA（情報セキュリティ安心相談窓口）
@IPA_anshin

Source:IPA

【怪しいZOOMに注意】
「検索でヒットしたサイトからパソコンにZOOMをインストールして起動したらセキュリティ警告が表示され、表示先の電話番号に電話をしたらサポート料金を請求された」という相談が複数寄せられています。正しいZOOMではなかったのが原因で偽の警告が出たと推測されます。



Source:テレ東ニュース 2020/05/15
https://www.youtube.com/watch?v=ymVQOBLbTag

Amazon アカウントの 情報を更新する必要があります https://accountupdate.amazon.hyk1.com/

マスクが買えるというサイトなど、マルウェアに感染させ、個人情報やクレジットカード情報を盗むなどの目的

シスコシステムズの西豪宏氏は「ネット利用者の自衛策が大切だ。悪質広告の存在を意識し、不審なサイトや広告を安易にクリックしないこと。ソフトやアプリ、セキュリティソフトを常に最新版に更新するなどの細かい対策を重ねるよりほかない」と話す。

ランサムウェア：過去、現在、そして未来

https://gblogs.cisco.com/jp/2016/05/ransomware-html/

1989
AIDS
FDで拡散

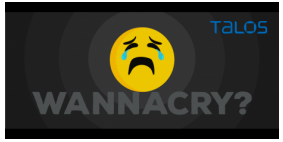
1996
Cryptovirology
RSA,TEA
暗号化

2005
Krotten
Archiveus
GPCoder

2012
Reveton
Angler/Cryptowall
Lockyなど

2016
SamSam
約6億
7000万円

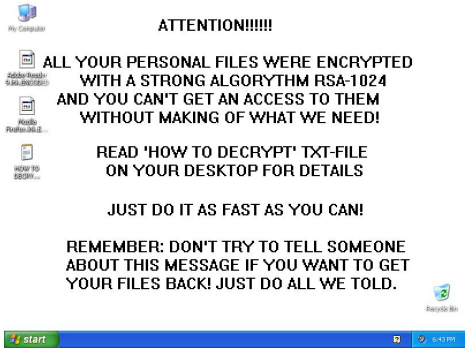
2017
WannaCry



2019
Ryuk
Emotet

2020
Snake
Maze
Ragnar Locker

標的型ランサムウェア



GPCoder
1024bit RSA暗号化

Reveton
標的所在地に応じた警察機関を名乗る
ファイルを取り戻すには「身代金」
プリペイドカードまたはビットコイン

医療業界を標的とする
ランサムウェア攻撃

WannaCry
TCP445を広範囲でスキャン
ワームと同様の仕組みで拡散
ビットコインによる身代金を要求

Agenda

1. 増大するサイバー犯罪
2. 新しい働き方スタイルのトレンド
3. 新しい働き方を支えるセキュリティ

ニューノーマル: BCPからBCEへ
事業を継続して実行する Business Continuity Execution (BCE)

旧来：オフィス中心型 vs 現在：どこでも事業継続できる環境

世界中で急速なデジタルシフトが起きている

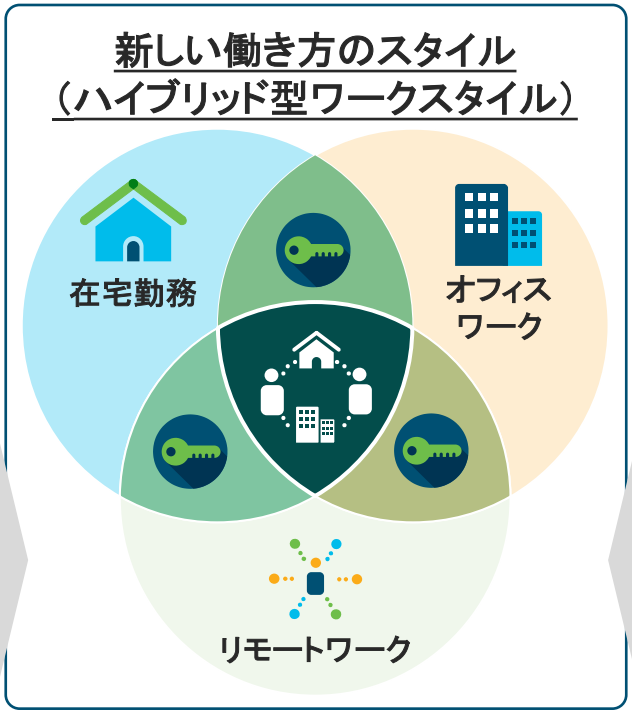
BCE の実現の為に必要なことは？

これまでの働き方

- オフィスに出社して仕事
- 会議は会議室で対面で
- 通院や子供の用事がある際は有給休暇を取得

これからの働き方

- 最も高い生産性が得られる場所で仕事
- 会議はバーチャルが中心
- 私用の際も休暇から休憩へ



これまでの
オフィスの在り方

- 仕事をする場所
- 毎日来なければならない場所

これからの
オフィスの在り方

- コラボレーションをする場所
- 会社への帰属意識を感じる為の場所

https://www.cisco.com/c/video/secure-insights/insights-live/future-of-secure-remote-work.html#~save-the-date

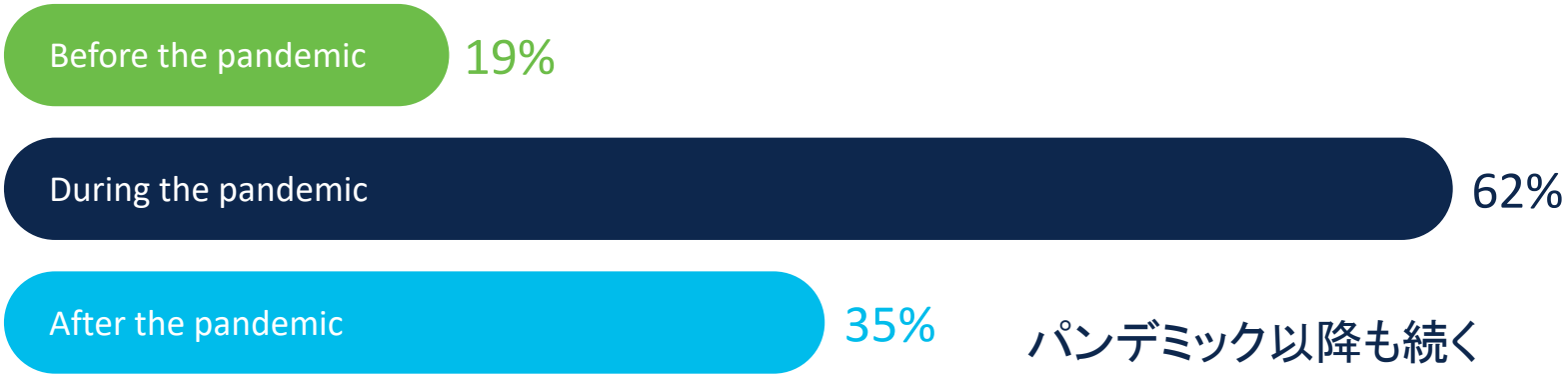
Future of Secure Remote Work report

1. パンデミックの影響で従業員を遠隔地に配置した際に、企業がグローバルにビジネスを確保するためにどのような準備をしていたかを理解する
2. Get insights into
   - サイバーセキュリティの脅威と警告の高まりから見た組織の在り処
   - この突然の移行で組織が直面した課題
   - ハイブリッドで柔軟な労働環境に備えるために、企業がサイバーセキュリティのアプローチをどのように適応させているか

3,196の回答・米州、アジア太平洋、欧州の各地域・30業種

パンデミックの影響で仕事の仕方が根本的に変化した

従業員の半数以上がリモートワークを行っている組織

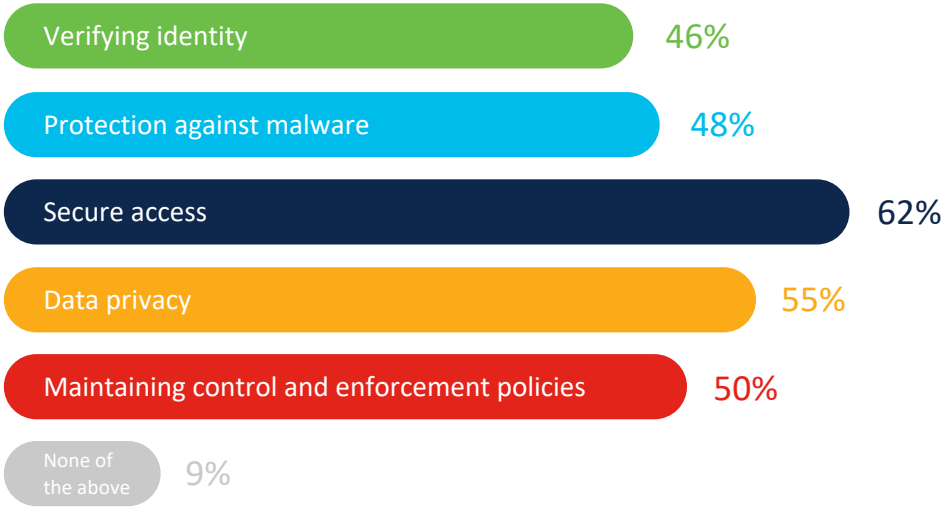


Secure accessが最優先課題

リモートワーカーを支援する際に直面するサイバーセキュリティの課題

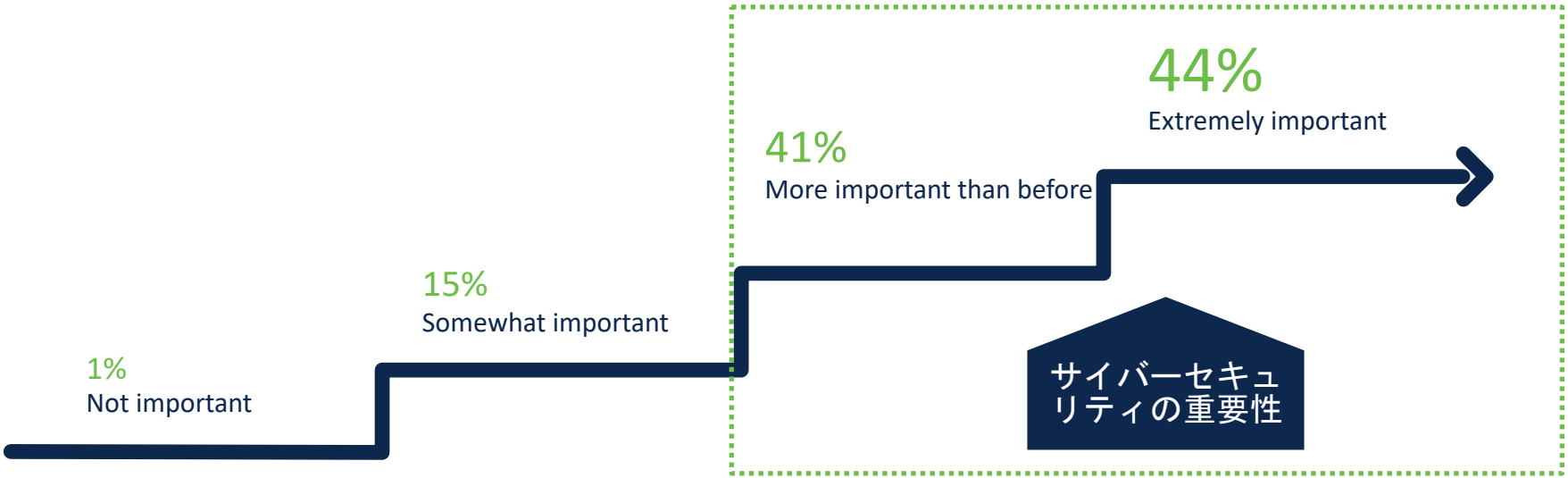
62%

respondents globally



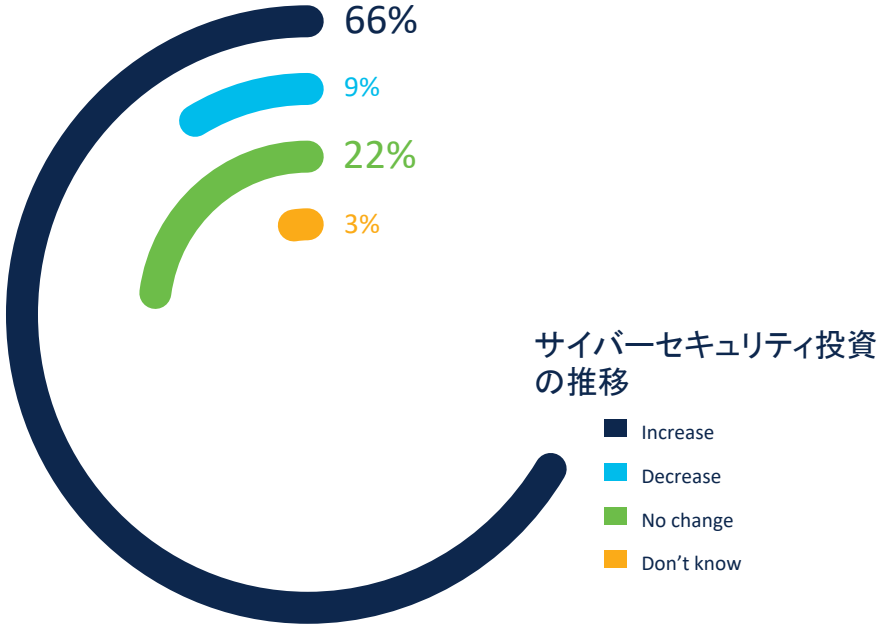
サイバーセキュリティの重要性が増す

85%の組織にとって、サイバーセキュリティは現在、非常に重要であるか、パンデミック以前よりも重要である。



サイバーセキュリティに対するアプローチを根本的に変える機会

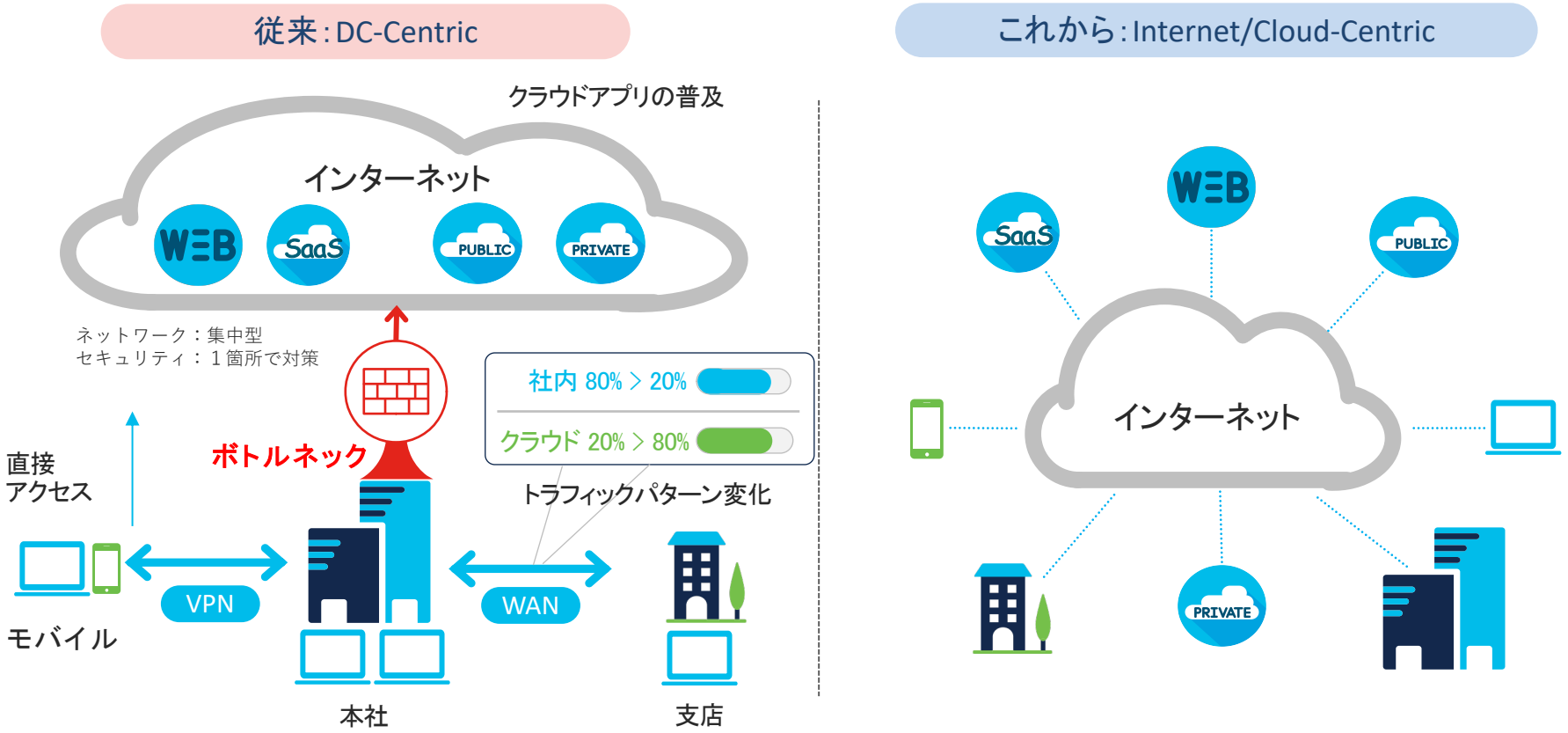
66% の組織が、パンデミックの影響でサイバーセキュリティへの投資を将来的に増やす計画を立てている



Agenda

1. 増大するサイバー犯罪
2. 新しい働き方スタイルのトレンド
3. 新しい働き方を支えるセキュリティ

新しい働き方スタイルによるネットワーク利用の変化
インターネット・クラウドがすべての中心となる

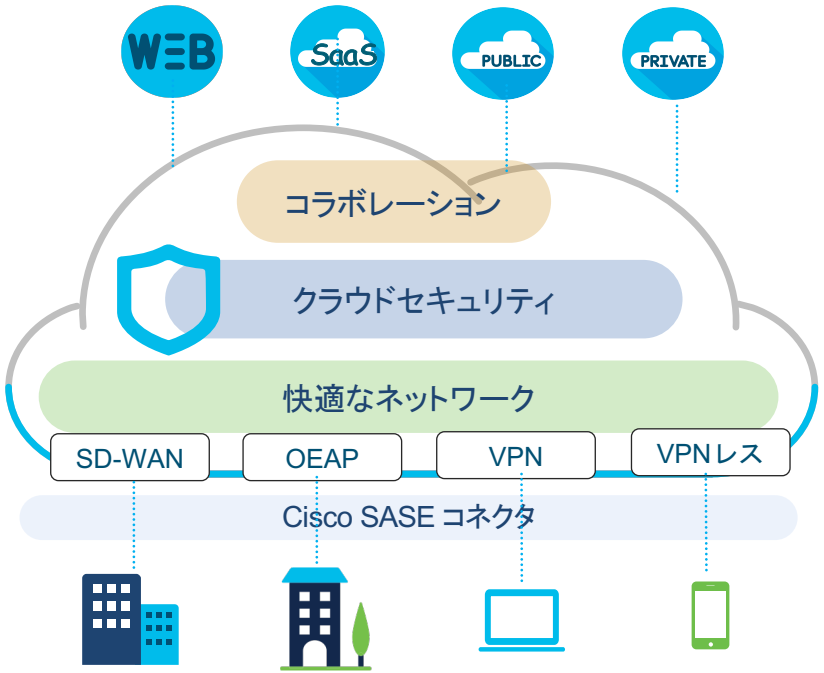


新しい働き方を支えるネットワークとセキュリティのあり方
Cisco SASE : 快適な接続性と安心なセキュリティをシンプルに実現

1 Connect（快適につながる）
あらゆるユーザー・デバイスから
すべてのアプリケーションへの
自動で最適かつ快適なネットワーク利用が可能

2 Control（安全・安心）
ユーザ・デバイスの保護と安全なアクセス
最先端の脅威からの保護
ゼロトラストのアクセス制御

3 Converge（簡単・シンプル）
シンプルかつ迅速な展開
クラウドで提供される
統合されたネットワークとセキュリティ



最も完全で統合されたエンドツーエンドのSASE
どこからスタートしても全体的なSASEを実現

接続性、セキュリティ、アイデンティティへのシンプルなアプローチを採用

Gartner®

セキュア アクセス サービス エッジ（SASE）

FORRESTER®

ゼロトラストエッジ

ESG
Enterprise Strategy Group

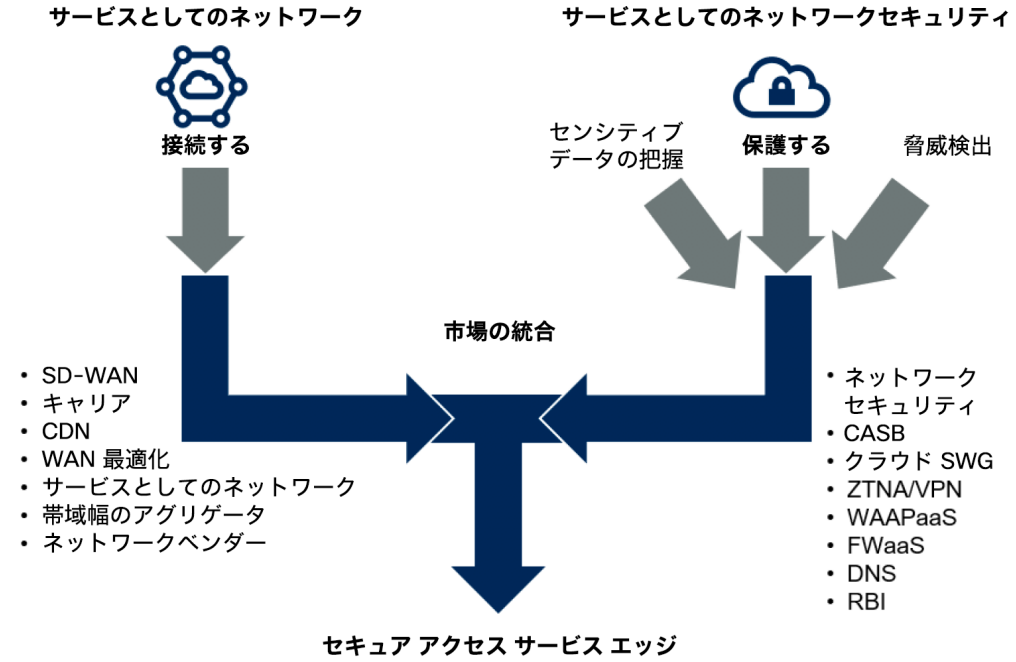
エラスティック クラウド ゲートウェイ

それぞれの名称は異なるものの、方向性は明確

クラウドネイティブへの集約については完全に一致

SASE に関する Gartner 社の見解

SASE の統合



CDN：コンテンツ配信ネットワーク、RBI：リモートブラウザ分離、WAAPaaS：サービスとしての Web アプリケーションおよび API 保護。
出典：Gartner 社
ID: 441737

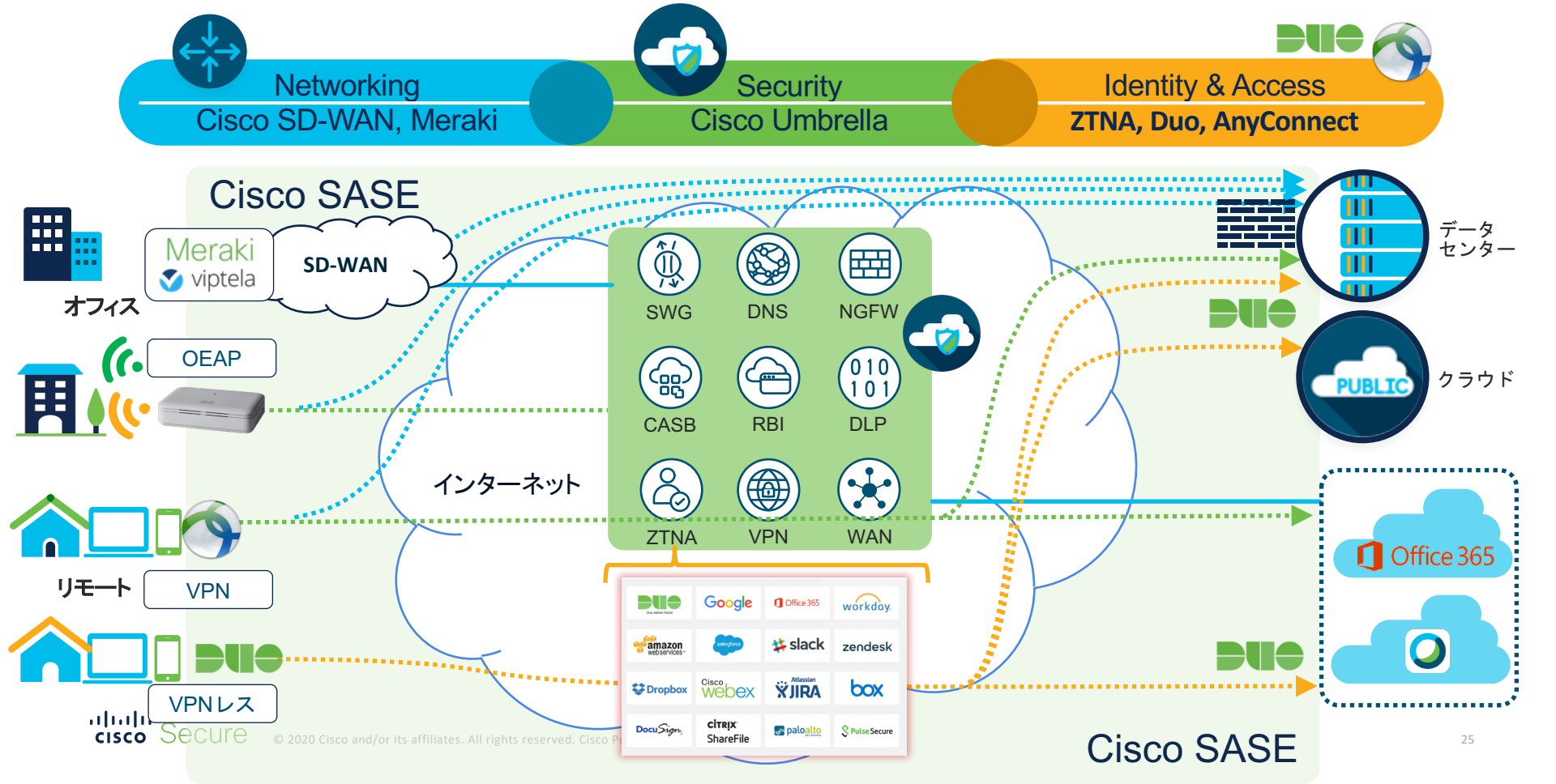
SASEとは

Secure な Web ゲートウェイ、
CASB、
Firewall、
Zero Trust Network Access
などの
クラウドネイティブなSecurity機能と
VPN および WAN 機能を
組み合わせた
ネットワークアーキテクチャ

Gartner

https://www.gartner.com/doc/reprints?id=1-1OG9EZYB&ct=190903&st=sb [英語]

快適な接続性と安心なセキュリティをシンプルに実現



セキュアなテレワーク（参考）

Cisco Duo Security
多要素認証
デバイスの健全性を検証

暗号化・社内業務・VPNレス通信

暗号化・社内業務・VPN通信

データセンター

DUO Network Gateway

社内
サーバ
アプリ

Cisco ASA
NGFW

Cisco EDR AMP for Endpoints
マルウェアを検出・可視化
高度な脅威を防御・対応

Cisco AnyConnect
ボトルネックが発生しない
セキュアリモートアクセス

Umbrella

Cisco Umbrella
クラウド・インターネットの
直接通信のセキュリティ

WEB

チャット
ファイル共有
電話

Webex
Teams

SaaS

ビデオ会議
イベント
遠隔授業

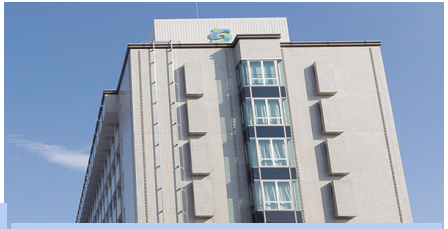
Webex
Meeting

Gartner 社から見たSASEにおけるシスコの立場

「シスコは自社開発に加え、数多くの買収により、幅広いネットワーク ソリューション（WAN エッジおよびコアスイッチング）およびセキュリティソリューション（NGFW、VPN、デバイス認証、SWG、および CASB 機能）を**長年にわたって提供**しています。さらに、**セキュア インターネット ゲートウェイ**を含むクラウドベースのネットワーク セキュリティ サービス プラットフォームでは、**SASE 関連サービスの拡充が行われています**」

出典：*How to Win as WAN Edge and Security Converge Into to the Secure Access Service Edge*、*Gartner グループ*

お客様の評価

	多要素認証 Duo	メール セキュリティ ESA/CES	セキュア名前解決 Umbrella	マルウェア対策 AMP /ThreatGrid
効果的な保護	想定を上回る従業員が一気に在宅勤務にシフトし、セキュリティ対策が急務	不正なメールを受信しない 不正な添付ファイルを破棄 リンクをクリックさせない	感染サイトに誘導されそうになってもアクセス遮断 C2通信の検出と遮断	マルウェア感染の防止 侵入経路・拡散の把握 EDR機能の充足
	ほぼ2～3日で構築完了し、ITリテラシーが高くなくてもセキュリティが向上し、チャットに加え、VDI・SSL-VPN、SaaS利用に展開を拡大予定	SMTPレベルで脅威メールをドロップ	DNSレベルで悪意あるサイトのアクセスをブロック	既知と未知に対応・マルウェア検出・隔離・可視化
	既知・未知の脅威・EDR（エンドポイント検出および応答）をカバー			
お客様の声				
	“既存の社内 IT インフラへの影響を最小限に抑えつつ、最も短期間で導入できる多要素認証の基盤と判断されたのが Cisco Duo セキュリティでした” **中西金属工業株式会社 様**	*"Cisco クラウド E メール セキュリティは、他社製品との同コスト比較で、最も多機能で検知精度も高い。費用対効果が明確なソリューションです。”* **国立大学法人 北見工業大学 様**	*“既存変更が少ない、導入負荷が少ない、導入後の管理負荷が軽い、ユーザに特別な教育が不要、導入したことを意識する必要がない、クラウドサービス利用時のパフォーマンスに影響を与えないことを条件に設定しましたが、Cisco Umbrella はこれらの要求を簡単にクリアしてくれました。”* **株式会社光文社様**	*“Cisco AMP はクラウド上に蓄積される最新の情報と常に照合して脅威を判定するという新しい仕組みで、標的型攻撃やゼロデイ攻撃への備えを万全にできる点を評価しました。”* **佐賀市教育委員会 様**

在宅勤務環境から利用するアプリケーションのセキュリティを多要素認証で強化

NKC
Nakanishi Metal Works Co., Ltd.
中西金属工業株式会社 様

「既存の社内 IT インフラへの影響を最小限に抑えつつ、最も短期間で導入できる多要素認証の基盤と判断されたのが Cisco Duo セキュリティでした。また、その背景としてグローバルで定評のあるシスコ製品ならではの安心感もありました。」

課題:
- 感染拡大という予想していなかった事態により、想定を大幅に上回る 600 名を超える従業員が一気に在宅勤務にシフト
- 従業員間の円滑なコミュニケーションを支えるべく急きょ導入したビジネスチャットツールセキュリティ対策が急務

ソリューションと効果:Cisco Duo Security
- Duoの認証方式には、最もシンプルな「アプリのプッシュ通知にワンタップ応答」を選んだ
- ITリテラシーの高くない従業員もストレスを感じることなく操作することが可能
- Duoはクラウドベースで提供されおり、既存の社内 IT インフラへの影響を最小限に抑えつつ短期間で導入できる

結果～今後:
- 構築作業はほぼ2 ～ 3日で完了し、予定どおりのスケジュールでビジネスチャットツールを多要素認証のもとで運用
- 大きなトラブルを起こすことなく安定した稼働を続けており、在宅勤務のセキュリティ強化に貢献
- VDIやSSL-VPNを経由した社内システムへのリモートアクセス、SaaS利用にいたるまで多要素認証を適用していく

https://www.cisco.com/c/ja_jp/about/case-studies-customer-success-stories/2195-nkc.html

AV-TEST、セキュリティの有効性評価で Cisco Umbrella を 1 位に選出
https://gblogs.cisco.com/jp/2020/04/av-test-places-cisco-umbrella-first-in-security-efficacy/

第三者機関AV-TEST による検証結果(2019/12)

- 2019年11～12月に AV-TEST にて準備されたデータを利用（シスコは関与せず）
- 各製品は最も高い防御となるようそれぞれ設定
- DNS レイヤにおいては、Umbrella と Akamai でセレクティブ プロキシを有効化（SWG 無し）
- ウェブレイヤにおいては、DNS セキュリティの設定無し

DNS レイヤ テスト

テストの種類	Umbrella DNS + SEL. PROXY	Umbrella DNS	Infoblox	Akamai	paloalto
Malicious PE files (Portable executables)	77.94	57.11	33.70	11.09	4.17
Malicious destinations	55.09	24.55	25.36	38.27	28.18
Phishing links	83.97	74.57	49.57	39.42	13.14
Total detection rate	**72.63**	**51.80**	**35.25**	**26.47**	**13.66**

ウェブ レイヤ テスト

Type of test	Umbrella SWG	Symantec	zscaler	paloalto
Malicious PE files (Portable executables)	92.65	88.66	77.88	65.07
Malicious destinations	93.82	89.82	88.36	77.00
Phishing links	82.80	71.69	88.25	79.70
Total detection rate	**90.49**	**84.68**	**83.67**	**72.38**

cisco Secure

Umbrella は、DNS、プロキシ共にベストの検証結果

AV-TEST places Cisco Umbrella first in security efficacy – again!
https://umbrella.cisco.com/blog/av-test-places-cisco-umbrella-first-in-security-for-secure-web-gateway-and-remote-workers

第三者機関AV-TESTによる検証結果(2020/10)

AV-TEST The Independent IT-Security Institute Magdeburg Germany

- 2020年9～10月に AV-TEST にて実施（シスコは関与せず）
- 各製品は最も高い防御となるようそれぞれ設定
- リモート エージェントへの保護を検証
- Cisco のエージェントは AnyConnect 4.9MR1

DNS レイヤ テスト

Product	製品パッケージ	検知率	誤検知率
サンプル数		3,572	2,165
Cisco Umbrella	DNS Security Advantage	70.69%	0.28%
Akamai Enterprise Threat Protector	Intelligence	53.58%	1.34%
Infoblox BloxOne	Advanced	36.28%	11.78%

ウェブ レイヤ テスト

Product	製品パッケージ	検知率	誤検知率
サンプル数		3,572	2,165
Cisco Umbrella	SIG Essentials	96.39%	0.65%
Zscaler Internet Access	Transformation	89.67%	0.69%
Palo Alto Networks Prisma Access	Prisma Access for Mobile Users	73.15%	1.29%
Netskope Secure Web Gateway	NG-SWG	61.90%	4.53%
Akamai Enterprise Threat Protector	Advanced Threat	58.43%	1.89%

Umbrella は、DNS、プロキシ共にベストの検知率と誤検知率

トライアルや詳細に関して

担当営業やシスココンタクトセンターまで

シスコ コンタクトセンター

シスコセキュリティウェビナー（今後の予定・過去開催の資料）
https://www.cisco.com/c/m/ja_jp/training-events/events-webinars/security.html

2020.10.15	悪性Botによる不正な送金やログイン、API攻撃その他様々なインシデントをRadwareで防止！	PDF	Webex 録画
2020.10.8	テレワーク時代、うちのネットワークセキュリティって大丈夫？ （録画閲覧パスワード：nWTNZd4H）		Webex 録画
2020.10.8	SASEとは？～ウイズコロナで変わりつつある IT 環境の今後～	PDF	Webex 録画
2020.9.24	事業継続のためのCisco ITの取り組みと学び～テレワークを実現するIT環境～	PDF	Webex 録画
2020.9.17	NewNormal時代のセキュリティにマシンラーニングを活用！~RadwareのDDoS/WAF/BoT対策ソリューション~	PDF	Webex 録画
2020.9.10	VPNレス 次世代リモートアクセス	PDF	Webex 録画
2020.7.9	ランサムウェア Snake の脅威とその対応策	PDF	Webex 録画


cisco
Secure