セッションに関するご質問

アンケートフォームにご記入ください。

担当営業やシスココンタクトセンターまでにお問い合わせください。

今後のシスコセキュリティウェビナー

https://www.cisco.com/c/ja_jp/training-events/events-webinars/webinars.html

毎週木曜日開催を予定。当面の予定は以下となります。

2020/6/4	木	14:00-14:30	30分でわかる最新の多要素認証 (Duo Security)
2020/6/4	木	15:00-15:30	30分でわかるマイクロセグメンテーション
2020/6/11	木	14:00-14:30	30分でわかるVPN（AnyConnect）
2020/6/11	木	15:00-15:30	30分でわかるクラウドセキュリティ（Umbrella）
2020/6/18	木	14:00-14:30	30分でわかるメールセキュリティ
2020/6/18	木	15:00-15:30	30分でわかるエンドポイントセキュリティ（AMP）
2020/6/25	木	14:00-14:30	30分でわかる認証基盤（ISE）
2020/6/25	木	15:00-15:30	30分でわかる可視化と脅威検出（StealthWatch）

cisco Secure

30分でわかるセキュアなリモートワーク

2020/05/29
シスコシステムズ合同会社
セキュリティ事業
SEマネージャ
西　豪宏

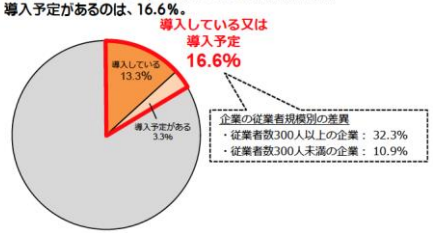
テレワークの導入状況（国内）

出典：総務省通信利用動向調査

平成28年9月末

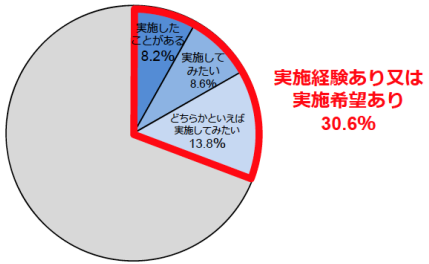
テレワークの導入状況（企業）

企業において、テレワークを導入している又は具体的な導入予定があるのは、16.6%。



テレワークの実施状況（個人）

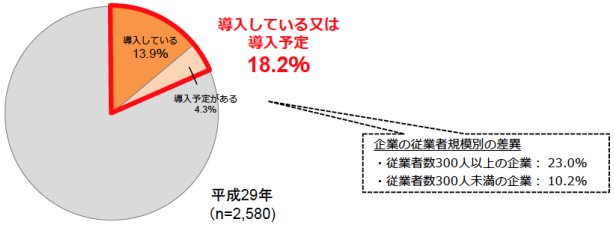
企業等に勤める15歳以上の個人のうち、過去1年間にテレワークの実施経験がある人及び実施してみたいと考えている人は、30.6%。



平成29年9月末

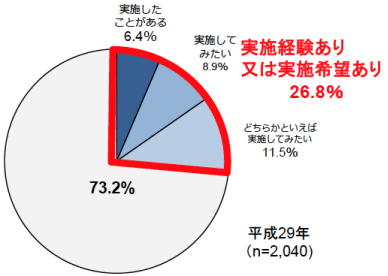
テレワークの導入状況（企業）

企業において、テレワークを導入している又は具体的な導入予定があるのは、18.2%。



テレワークの実施状況（個人）

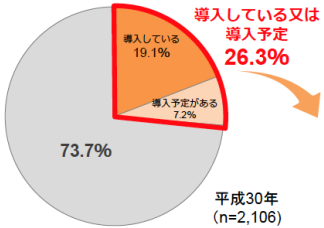
企業等に勤める15歳以上の個人のうち、過去1年間にテレワークの実施経験がある人及び実施してみたいと考えている人は、26.8%。

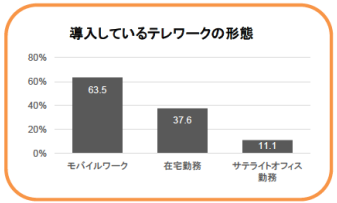


平成30年9月末

テレワークの導入状況（企業）

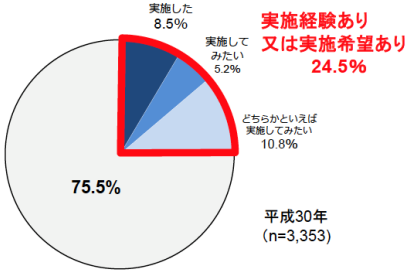
企業において、テレワークを導入している又は具体的な導入予定があるのは、26.3%。





テレワークの実施状況（個人）

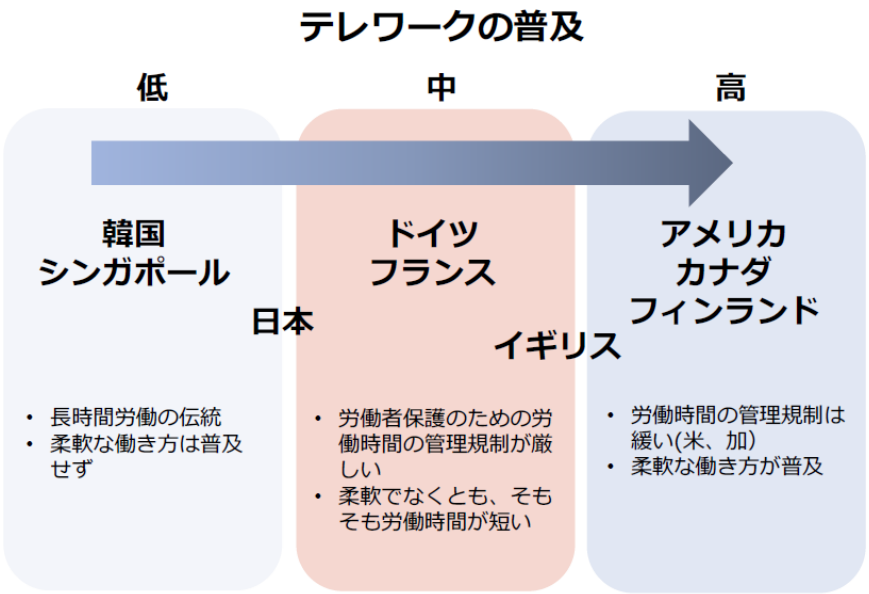
企業等に勤める15歳以上の個人のうち、過去1年間にテレワークの実施経験がある人及び実施してみたいと考えている人は、24.5%。



年々増加の傾向、最新はさらに増加基調
昨今は喫緊の課題になっている

テレワークの普及動向（海外）

（出典）総務省テレワーク情報サイト



図表 2-2　諸外国のテレワーク概要図

IPSOS社が2011年に24か国11,383名に実施したオンラインアンケート調査

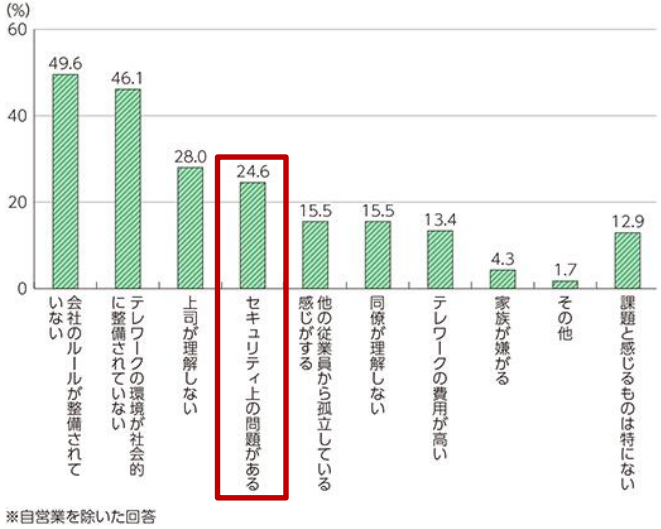
アメリカ
2010年に連邦政府がテレワーク強化法を成立、テレワークを推進
9.11以降は事業継続を目的に機能分散化を図るための導入
アメリカは個人の仕事と範囲が明確になっており、労働時間の管理規制もないのでテレワークが導入しやすい
カナダはアメリカに近い雇用制度

ヨーロッパ
ドイツやフランスなど大陸側の国は労働時間の管理規則が厳しいので、アメリカに比べると普及度は低め
労働時間の短縮化が進んでいるので、柔軟な働き方にこだわる必要がない側面も

アジア
韓国は長時間労働が根強い（2015年までにテレワークの実施30%目標も下回る）
シンガポールはフルタイム雇用かつ固定時間制度が根強く残る

テレワーク実施の課題

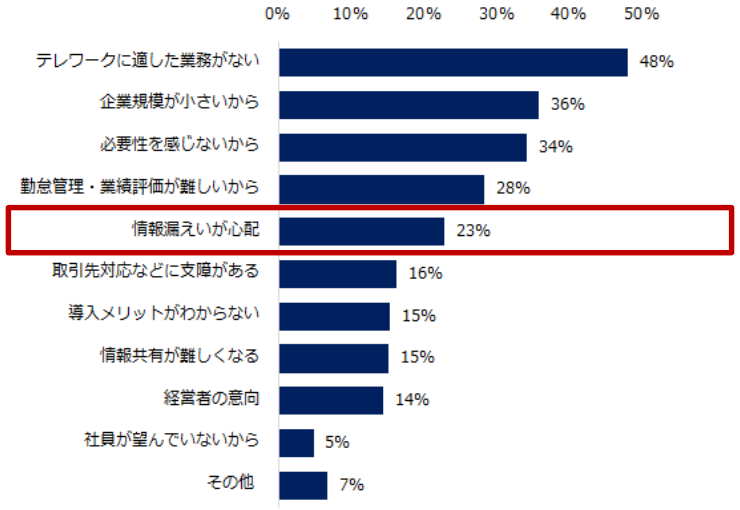
（出典）総務省「ICTによるインクルージョンの実現に関する調査研究」（2018）



※自営業を除いた回答

（出典）エン・ジャパン株式会社 中小企業の「テレワーク」実態調査

「テレワークを導入していない」と回答した企業に伺います。
テレワークを導入していない理由は何ですか？

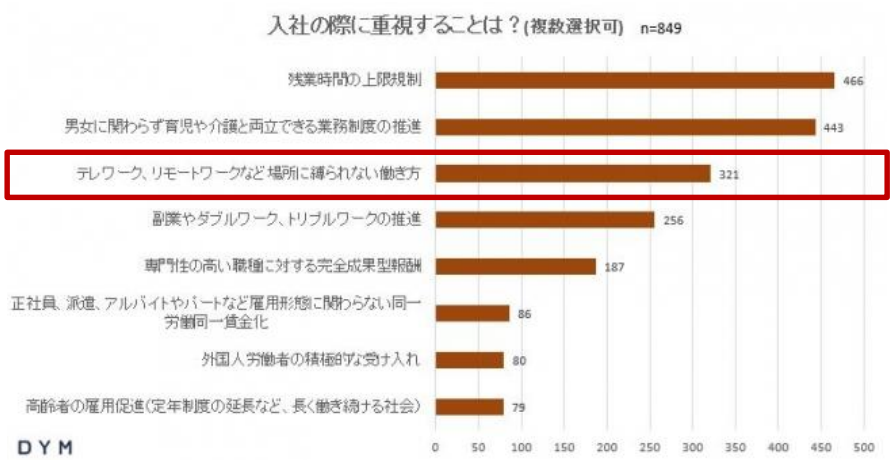


テレワークできる適した業務がない・ルール
環境の用意とセキュリティ対策が必要
コミュニケーションが希薄になる・孤立
勤務時間の把握がしにくい
仕事における評価がしづらい

業務のやり方の見直し、ルールづくり
環境の用意とセキュリティ対策は先行投資
コミュニケーションツール導入 or 出社する日
勤務時間報告システムやツールを利用
適正な評価制度のしくみ

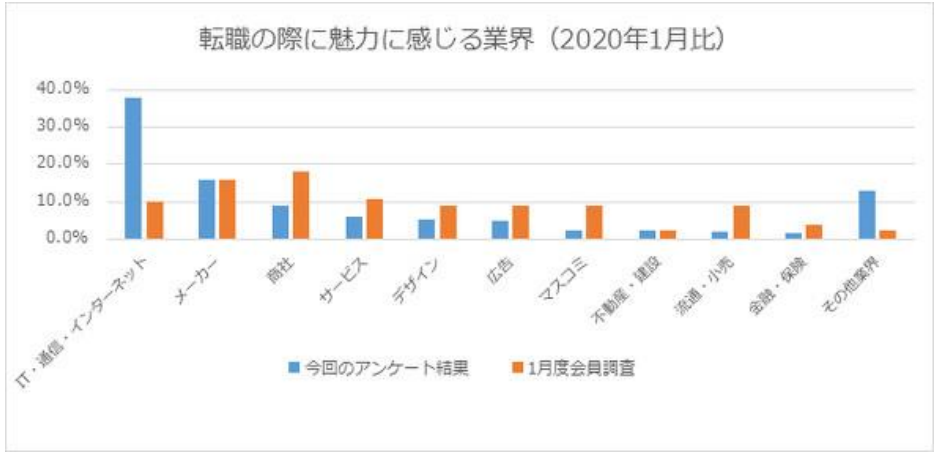
テレワーク・在宅勤務制度と人材確保

（出典）DYM 2021年卒 就職活動生アンケート



残業時間の上限規制、育児・介護と両立、
テレワーク、副業の推進など上位

（出典）ITmedia転職をする際に魅力を感じる業界



「IT・通信・インターネット」業界を希望する理由については、
「テレワークに適応している業界だから」「テレワークの環境整備が進んでいるイメージがあるから」

就活、転職サイトなどで、在宅勤務制度がある会社リストなど、
「テレワークできる」仕事というニーズに合わせた記事が増加

悪質広告「マルバタイジング」の増加

- マスクが買えるというサイト
- 偽の給付金サイト
- マルウェアに感染させる目的
- 個人情報やクレジットカード情報の搾取

2020年5月9日（土）　【第三種郵便物認可】　日本経済新

コロナに便乗 悪質広告

クリックでウイルス感染

検知、世界で50倍

防御甘い自宅ＰＣ、標的に

新型コロナウイルスの流行に乗じ、インターネット利用者を狙うサイバー犯罪が脅威を増している。米企業の調査では、閲覧するとコンピューターウイルスに感染する「悪質広告」が50倍に急増。ドイツでは偽の給付金サイトを通じ、100億円以上の詐欺被害が出た。防御の甘い自宅のパソコン利用の隙を突かれ、IT（情報技術）大手の対策も追いつかない。

各国で悪質広告の脅威が増している

セキュリティー会社アバストがブロックした累計の攻撃回数

「「マスクが買える」というSNS（交流サイト）の広告をみて注文したが怪しいのでキャンセルしたい」。3月下旬、国民生活センターに30歳代の女性から相談が舞い込んだ。SNSの広告に表示された通販サイトを訪れると、不自然な形でクレジットカードの登録を求められたという。不審に思い入力をやめたが、同センターは「新型コロナに便乗した手口」と注意を呼びかける。

こうした悪質広告は「マルバタイジング」と呼ばれる。マルウェア（悪意あるプログラム）とア

ドバタイジング（広告）を合わせた造語だ。広告を使う人も多く、悪質広告の被害を considerably 受けやすくなっている。

ネット広告はグーグルとフェイスブックの2社が世界シェアの6割を占め。両社をはじめIT大手各社は悪質広告が表示される前にブロックする対策を強化するが、防ぎ切れていない。

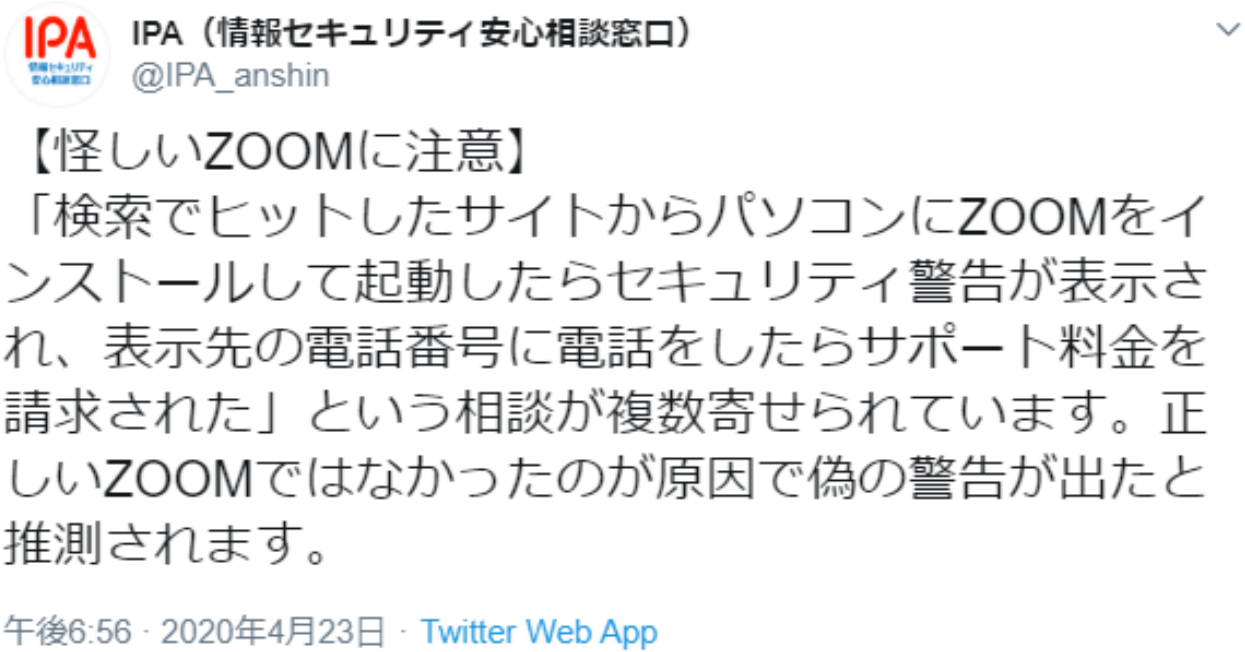
悪質広告の排除は、人の目による確認と人工知能（AI）の自動検知を併用する形が主流だ。ソフトが検知した悪質広告だけ写真共有アプリ、インスタグラムの広報担当者は「AI審査には限界があり、全てブロックするのは難しい」と明かす。

「人の目の方が厳しく審査できる」という。ところが型コロナの感染拡大を受け、チェック担当者が自宅待機に回ることが増えた。結果的に不審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、セキュリティー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。

（データエコノミー取材班　綱嶋亨）

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。

利用が拡大する遠隔会議システムが狙われる



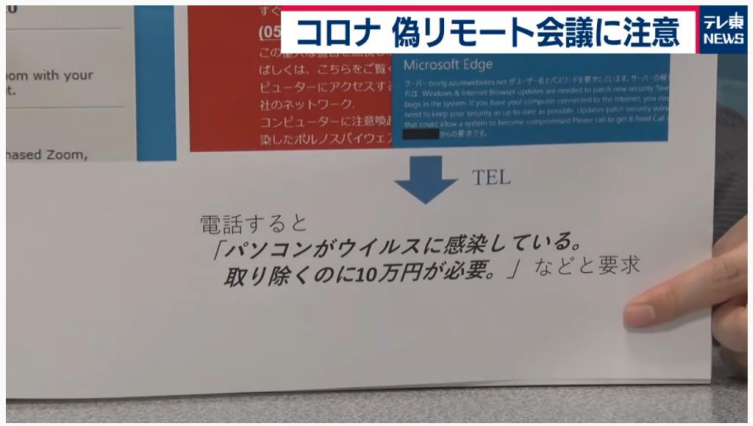
IPA（情報セキュリティ安心相談窓口）
@IPA_anshin

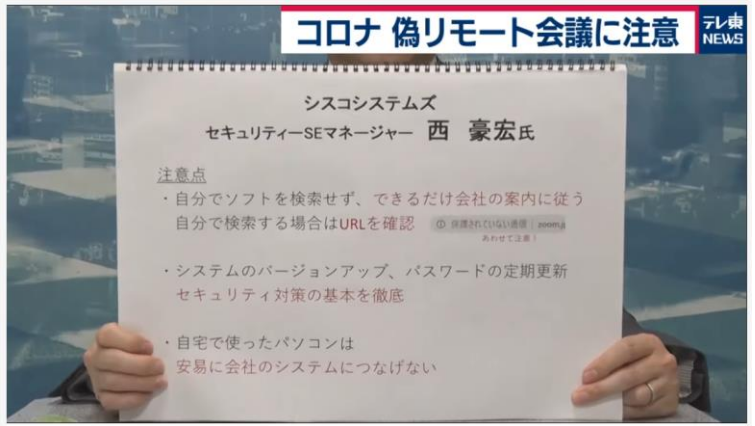
【怪しいZOOMに注意】
「検索でヒットしたサイトからパソコンにZOOMをインストールして起動したらセキュリティ警告が表示され、表示先の電話番号に電話をしたらサポート料金を請求された」という相談が複数寄せられています。正しいZOOMではなかったのが原因で偽の警告が出たと推測されます。

午後6:56 · 2020年4月23日 · Twitter Web App

テレ東ニュース 2020/05/15

https://www.youtube.com/watch?v=ymVQOBLbTag





Ciscoブログでの脅威に関する情報

Zoom で確認された、ユーザアカウントを列挙される脆弱性
https://gblogs.cisco.com/jp/2020/04/talos-zoom-user-enumeration/

リモートワークでは怪しいビデオ会議サービスにご注意を
https://gblogs.cisco.com/jp/2020/04/beware-of-video-conferencing-services-that-are-suspicious-in-remote-work/

COVID-19の経済対策を題材にしたスパムの増加
https://gblogs.cisco.com/jp/2020/04/talos-covid-19-relief-package/

新型コロナウイルスの感染拡大に便乗する攻撃者
https://gblogs.cisco.com/jp/2020/02/talos-coronavirus-themed-malware/

新型コロナウイルス（COVID-19）の脅威に関する最新情報
https://gblogs.cisco.com/jp/2020/04/talos-covid-19-pandemic-threats/

脅威情報ニュースレター
https://gblogs.cisco.com/jp/2020/04/talos-threat-source-newsletter-april-9-2020/

マルバタイジング：オンライン広告の影の側面
https://gblogs.cisco.com/jp/2019/08/talos-malvertising-deepdive/

セキュリティ機能を適切に開示せず、通話が暗号化されていないことを周知していなかったとして、Zoom社が株主から訴訟を起こされる

Google社、セキュリティ上の懸念を理由に、従業員によるZoomの使用を当面禁止にすると発表・米上院や独政府も使用制限との報道

COVID-19に便乗する新種のマルウェアが標的のPCを完全に消去できることが確認される

感染拡大に伴い、悪意のあるリンクや添付ファイルをクリックさせるため攻撃者が便乗できる題材の増加（政府機関、医療機関）

便乗した配布メールが多数確認ー時事ニュースに乗じる攻撃者

景気対策法（2兆ドル・米）・特別定額給付金（10万円)ー経済対策は格好の材料

医療用マスクの販売を謳う詐欺のWebサイト

サイバー攻撃が過去 4 週間にわたって 37% 増加
大事件や珍しい出来事が起こったときは、それらに関連する最新情報やサービスを提供するとの名目で標的をおびき寄せる攻撃が多発しがち

【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。

特別定額給付金の受給に関連した攻撃メール

[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、感染拡大防止に留意しつつ、簡素な仕組みで迅速かつ的確に家計への支援を行うため、
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/

リンクをクリックさせる手口

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、感染拡大防止に留意しつつ、簡素な仕組みで迅速かつ的確に家計への支援を行うため、特別定額給付金事業が実施されることになり、総
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、「新型インフルエンザ等対策特別措置法の緊急事態宣言の下、生活の維持に必要な場合を除き、外出を自粛し、人と人との接触を最
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持ち、人々が連帯して一致団結し、見えざる敵との闘いという国難を克服しなければならない」と示され、このため、感染拡大
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

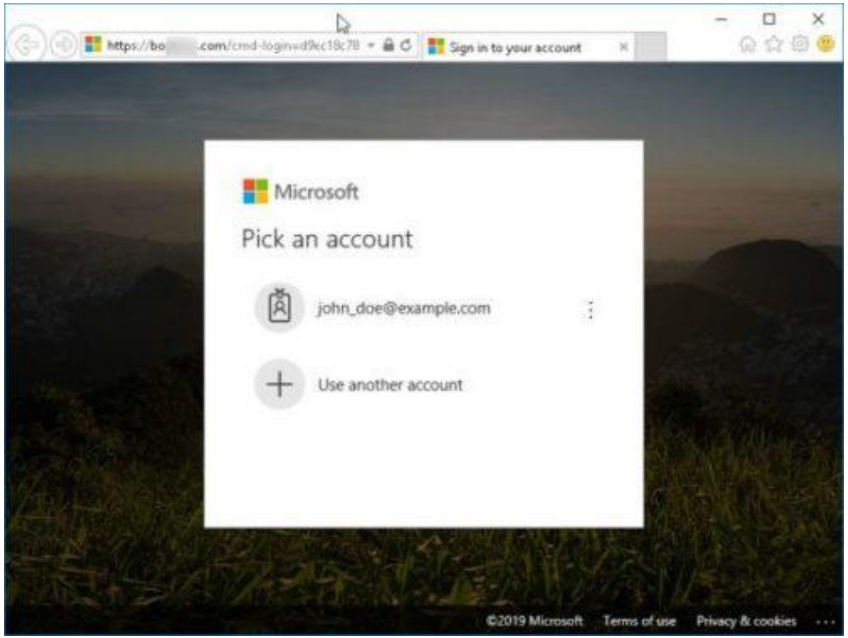
給付金の申請及び給付の方法

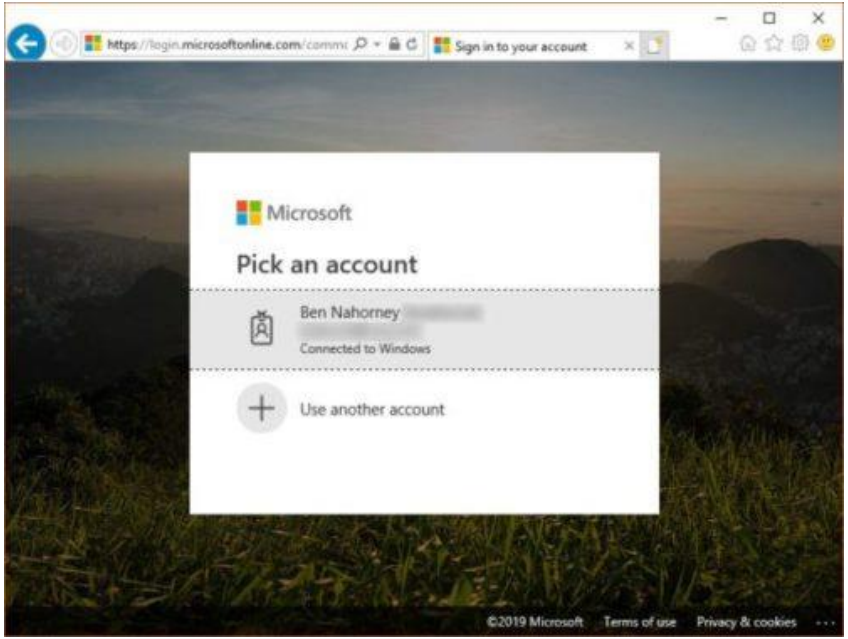
どれが正しいのか？

- singaporeair.com ?
- singaporea1r.com ?
- sıngaporeair.com ?
- singaporeạir.com ?
- singaporeair.com ?

リモートワークでは怪しいビデオ会議サービスにご注意を
https://gblogs.cisco.com/jp/2020/04/beware-of-video-conferencing-services-that-are-suspicious-in-remote-work/

どちらが正規のログイン画面？





Office 365 のフィッシング
https://gblogs.cisco.com/jp/2019/09/office-365-phishing-threat-of-the-month/

5/13 Umbrellaで調査

- Pattern Search : .*¥.corrona.*
- 500件
- April 13, 2020, 08:36pm ~ May 06, 2020, 11:46am（計30日）
- 16ドメイン / 日（過去30日間）
- 369/500 件 = Malwareサイト
- 131/500 件 = 正規サイト（悪性度が高いものも含まれるかも）

悪意のある偽サイトが急増

（フィッシング・マルウェアなど、corrona, covidをキーワードとした新規ドメイン）

ほとんどがマルウェアと判定（Umbrella）

.*\.covid.* INVESTIGATE BACK TO TOP

www.covidherocompensationfund.org	Malware	May 04, 2020, 09:43pm
www.covidapparel.ca	Malware	May 04, 2020, 09:42pm
www.covid-test.store	Malware	May 04, 2020, 09:42pm
www.covid-19news.jp	Malware	May 04, 2020, 09:42pm
www.covidactbow.org	Malware	May 04, 2020, 09:42pm
www.covid-nettoyage.com	Malware	May 04, 2020, 09:40pm
www.covidactionnetwork.org	Malware	May 04, 2020, 09:40pm
www.covid-experts.com	Malware	May 04, 2020, 09:40pm
www.covid-19-baby.xyz	Malware	May 04, 2020, 08:09pm
webdisk.covidtoday.com	Malware	May 04, 2020, 06:30pm
api.covid19zc.com	Malware	May 04, 2020, 05:33pm
www.covid19.co.com	Malware	May 04, 2020, 11:26am
www.covid19int.com	Malware	May 04, 2020, 11:24am
www.covid19-depistage.org	Malware	May 04, 2020, 07:23am
autodiscover.covidyo.com	Malware	May 04, 2020, 07:01am
www.covid-19artist.org	Malware	May 04, 2020, 06:18am
www.covidtester.de	Malware	May 04, 2020, 06:18am

.*\.corona.* INVESTIGATE BACK TO TOP

www.corona-culture-world.com	Malware	May 08, 2020, 06:59am
www.coronadivorcefaq.com	Malware	May 08, 2020, 06:05am
www.coronavirus19.tips	Malware	May 08, 2020, 05:45am
cpcontacts.coronaswimmingpoolservice.com		May 08, 2020, 04:52am
www.coronavirusbusinessinterruptionlawyers....	Malware	May 08, 2020, 04:17am
www.corona-antivirusproducts.com	Malware	May 08, 2020, 03:30am
www.coronastats123.com	Malware	May 08, 2020, 03:22am
www.coronadorentalsonline.com		May 08, 2020, 03:01am
www.coronatelegraph.com	Malware	May 08, 2020, 02:53am
www.coronavirus-online24.ru	Malware	May 08, 2020, 02:49am
www.coronavirus-gorod.ru	Malware	May 08, 2020, 02:44am
www.coronalabratory.com	Malware	May 08, 2020, 02:21am
www.coronaviruscertified.com	Malware	May 08, 2020, 02:06am
v2.corona-concerts.eu	Malware	May 08, 2020, 01:40am
la.coronavirus-face-mask.today	Malware	May 08, 2020, 01:36am
www.corona3.site	Malware	May 08, 2020, 01:24am
www.coronakilos.com	Malware	May 08, 2020, 01:19am

テレワーク・オンライン授業のセキュリティ対策

テレワークを行う際のセキュリティ上の注意事項

掲載日：2020年 4月 21日
独立行政法人情報処理推進機構
セキュリティセンター

1. はじめに

新型コロナウイルス感染症(COVID-19)の影響により、ICTを用いて自宅でも業務が行えるような環境を整えて、社員等を出社させずに事業継続を図る動きが急速に進んでいます。このような環境で働くテレワーク勤務者に向けたセキュリティ上の注意事項をご案内します。

テレワークには様々な利用環境があります。代表的なのは、自宅のパソコン等を用いてリモートデスクトップや仮想デスクトップで社内での業務用端末と同じ利用環境（テレワーク環境）を実現する方法です。

一方でそのような本格的な環境が提供されていない状況で自宅勤務を実施されている場合もあると思います。このページでは、そのような場合における注意事項も説明します。

https://www.ipa.go.jp/security/announce/telework.html

警視庁　安全な暮らし　交通安全　相談・お悩み　手続き

トップページ → 安全な暮らし → 情報セキュリティ広場 → 注目情報 → テレワーク勤務のサイバーセキュリ

テレワーク勤務のサイバーセキュリティ対策！

更新日：2020年4月16日

テレワークで勤務をされる方へ

サイバーセキュリティ対策

テレワークで使用するパソコン等（タブレット、スマートフォン）

サポートが終了しているOS（オペレーティングシステム）のパソコンを使用しない。

Windows7、WindowsVista、WindowsXPは、すでに脆弱性等に対するサポートがされていないため、マルウェア（ウイルス）に感染するリスクが高くなります。

ウイルス対策ソフトを必ず導入する。

マルウェア（ウイルス）の感染防止のために必ず導入しましょう。

https://www.keishicho.metro.tokyo.jp/kurashi/cyber/joho/telework.html

National Security Agency | Cybersecurity Information

Selecting and Safely Using Collaboration Services for Telework

Criteria to Consider When Selecting a Collaboration Service

1. Does the service implement end-to-end encryption?
2. Are strong, well-known, testable encryption standards used?
3. Is multi-factor authentication (MFA) used to validate users' identities?
4. Can users see and control who connects to collaboration sessions?

https://media.defense.gov/2020/Apr/24/2002288653/-1/-1/0/CSI-SELECTING-AND-USING-COLLABORATION-SERVICES-SECURELY-SHORT-FINAL.PDF

テレワークを実施する際にセキュリティ上留意すべき点について

3. 留意事項（要約）
(1)（Virtual PrivateNetwork）VPN：VPNで業務を実施するケースがある。VPNは完全ではないとの前提の下、迅速なパッチ適用、加えて多要素認証の採用の検討が必要。
(2) メール：各機関の「情報セキュリティポリシー」再確認
取り扱うデータの内容に応じて暗号化を推奨
(3) リモートデスクトップ(RDP)：RDPが増加しており、Windows RDP深刻な脆弱性(CVE-2019-0708、CVE-2019-1181/CVE-2019-1182)パッチ適用の注意喚起とPDP ポート開放状況の再確認
(4) 遠隔会議システム：利用が拡大しており、Zoomのセキュリティ上の問題点を指摘。潜在するリスクについて、導入前に十分調査推奨し、運用中にリスクが顕在化した際の対策をあらかじめの検討を推奨
(5) 機密情報の保護：SNSに投稿したテレワークの写真に、機密性の高い文書や業務情報が映り込む事例が発生
テレワーク実施時不用意な機密情報の漏洩に留意。
遠隔会議の実施場所や設定に配慮する必要。

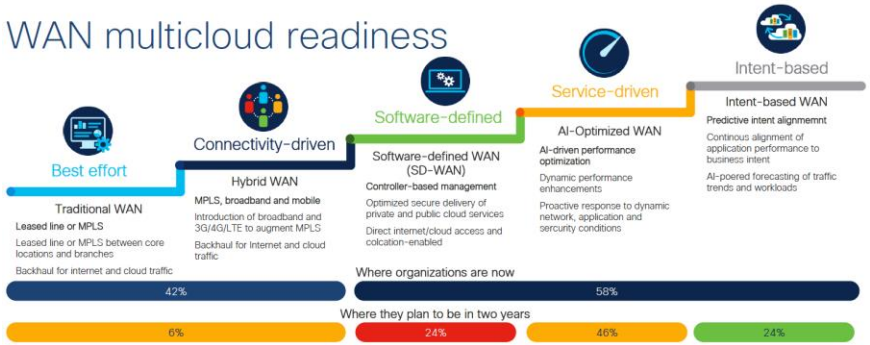
(6) その他
① 堅牢なパスワードや多要素認証の使用：システムで用いるパスワードは他者から容易に推測されない堅牢なものとし、多要素認証が使用できる場合は活用することを検討します。
② 端末や機器のアップデート：OS やソフトウェア、アプリ、機器の脆弱性を確認したうえで、必要に応じてアップデートする等、システムの状況に応じた管理策を検討します。
③ 不審なメールへの注意：業務を装ったメールや新型コロナウイルス感染症(COVID-19)をテーマにした不審なメール等に注意し、身に覚えのないメールの添付ファイルやURL はクリックしないように組織全体に注意喚起が必要です。
④ 端末の盗難や紛失への注意：ノートPC やスマートフォン、USB メモリ等は紛失のリスクもあるため、紛失を防止するための対策に加え、暗号化の実施の検討や、個人の端末を利用する場合のセキュリティ対策を考慮します。
⑤ 無線LAN のセキュリティ設定の確認
無線LAN(Wi-Fi)のセキュリティ設定に留意します。
⑥ インシデント発生時の連絡方法の確認：テレワークによるセキュリティインシデント発生に備え、あらかじめインシデント発生時の対処方法、連絡方法を確認しておきます。

出典：2020年4月14日内閣サイバーセキュリティセンター(NISC)

VPNを使わない業務への対応

- クラウド・インターネットへの直接アクセス
- 社内のセキュリティ装置を経由しない
- 通信が組織のセキュリティをバイパスする

当社の「*2019 Global Networking Trends Survey*」によると、世界の 58 % 以上の企業がすでに何らかの形で SD-WAN を導入しており、回答者の 94 % が今後 2 年以内にベーシックまたはより高度な SD-WAN を導入するだろうと回答しています。[14]



Getting a handle on VPN practices

Not surprisingly, workers are indeed on the go. Nearly 60 percent of the IT security decision-makers said their laptop-toting employees use the devices away from the corporate physical network at least 50 percent of the time. End-users' self-reporting was similar, with 45 percent saying they did just that and 20 percent indicating that they roam 100 percent of the time.

Most notably, **82 percent of the corporate laptop users admitted to sometimes bypassing their organizations' VPNs.** Much of this off-network usage was for personal activities, but nearly 30 percent of the end users said they sometimes access company data without logging into their VPNs.

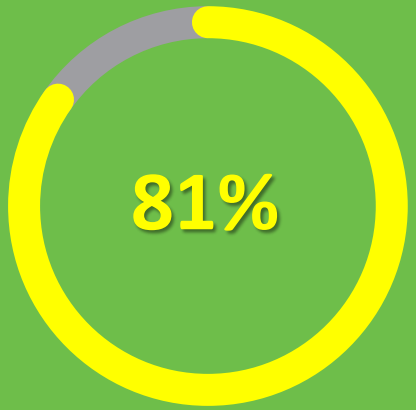
IDGの調査
企業ノートPCのユーザの82%がVPNを使わないことがある

セキュアインターネットゲートウェイ（SIG） https://gblogs.cisco.com/jp/2020/02/drop-emotet-by-umbrella/
テレワークとセキュリティ シスコの事例 https://gblogs.cisco.com/jp/2020/03/telework_and_security_casestudy_after_webinar/

不正侵入は、ID/パスワード漏洩から始まる

Targeting Identity

81%のハッキングによる侵害は、パスワード漏洩や弱いパスワードなど、クレデンシャルに関連している
*2017 Verizon Data Breach Investigations Report



遭遇した攻撃とデータ損失の割合

依然として猛威を振るうマルウェア

過去1年間に発生した攻撃のタイプ

49% マルウェア	42% 悪意のあるスパム	38% フィッシング
36% スパイウェア	33% データ漏洩	27% ランサムウェア

上位のサイバー攻撃は90%以上が電子メール

データ損失に発展した攻撃のタイプ

20% マルウェア	19% データ漏洩	14% スパイウェア
13% フィッシング	13% ランサムウェア	13% 悪意のあるスパム

出典元「2019年 CISOベンチマークレポート」

テレワークで必要なセキュリティ

1. VPNで普段の業務に安全にアクセス
2. VPNを使わない業務での安全性の確保
3. 多要素認証の利用により不正侵入を防ぐ
4. 脅威の始まりと目的であるメールとマルウェアへの対策

セキュアなテレワークの実現

VPN

VPNで普段の業務に
安全にアクセス

安全なリモートアクセスVPN

AnyConnect

外部から社内ネットワークへ安全に接続するためのクライアント ソフトウェアです。幅広い端末に対応し、DNS Web セキュリティ（Umbrella 連携）を提供します。

クラウドセキュリティ

VPNを使わない業務での
安全性の確保

セキュア インターネット ゲートウェイ

Umbrella

あらゆる場所・ユーザ・デバイスを保護できる、簡単かつ迅速に導入可能なクラウド提供型のセキュリティサービス（DNS、Web、クラウドFW、クラウドアプリ可視化・制御等）です。

多要素認証

多要素認証の利用により
不正侵入を防ぐ

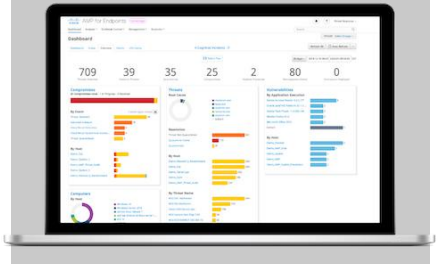
ゼロトラスト/多要素認証

DUO Security

信頼できるユーザとデバイスだけをアプリケーションに接続する適応型多要素認証（MFA）です。情報漏えいが起きるリスクを軽減します。

マルウェア対策

脅威の始まりと目的である
メール・マルウェアへの対策

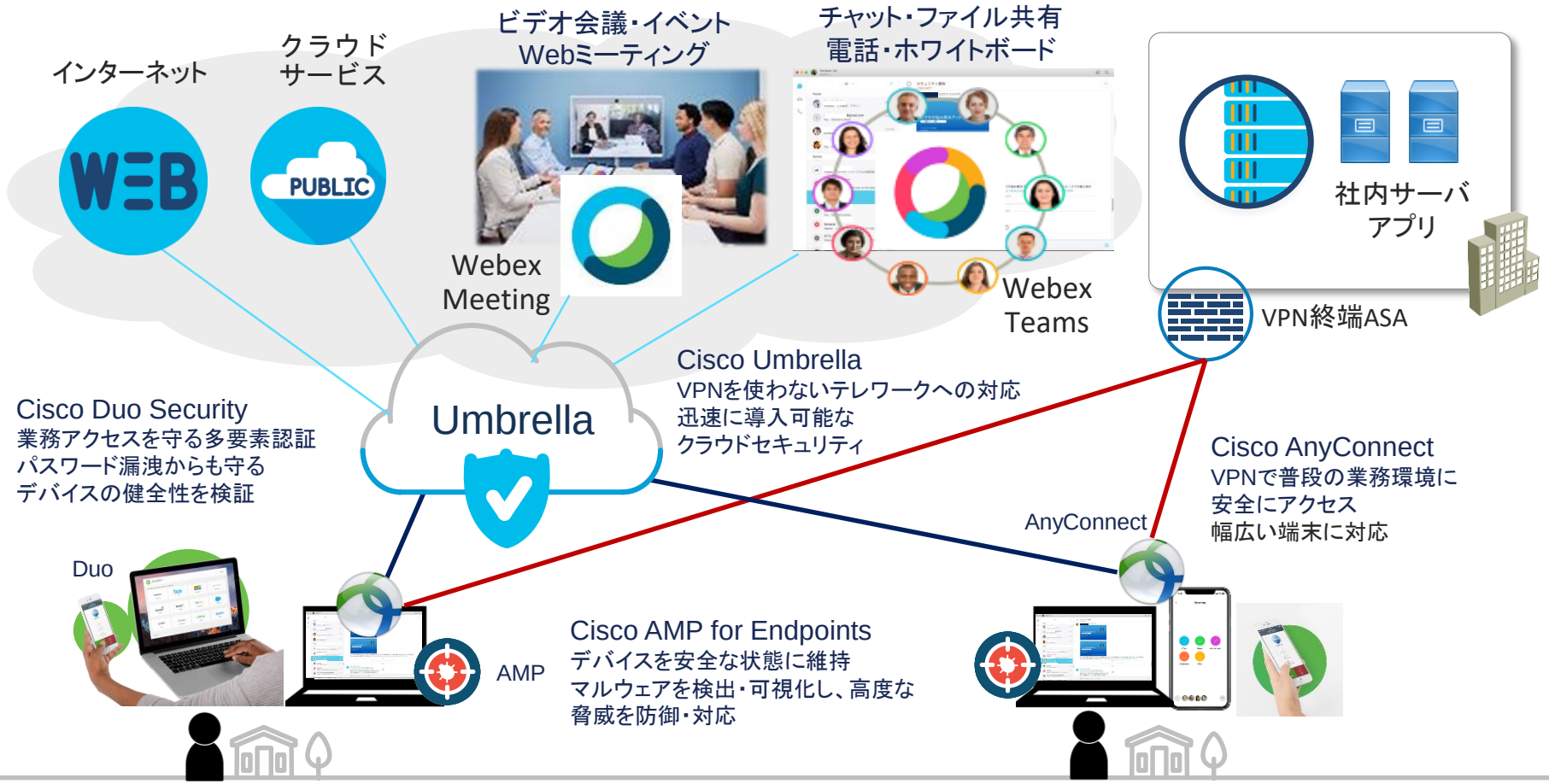


エンドポイントを保護

AMP for Endpoint

マルウェアを検出・可視化し、高度な脅威を防御・対応します。リモートワーカーのデバイスを安全な状態に維持し、生産性を向上します。

セキュアなテレワーク


インターネット
クラウド
サービス
WEB
PUBLIC
ビデオ会議・イベント
Webミーティング
Webex
Meeting
チャット・ファイル共有
電話・ホワイトボード
Webex
Teams
社内サーバ
アプリ
VPN終端ASA
Umbrella
Cisco Umbrella
VPNを使わないテレワークへの対応
迅速に導入可能な
クラウドセキュリティ
Cisco Duo Security
業務アクセスを守る多要素認証
パスワード漏洩からも守る
デバイスの健全性を検証
Duo
AMP
Cisco AMP for Endpoints
デバイスを安全な状態に維持
マルウェアを検出・可視化し、高度な
脅威を防御・対応
AnyConnect
Cisco AnyConnect
VPNで普段の業務環境に
安全にアクセス
幅広い端末に対応

https://www.cisco.com/c/m/en_us/covid19.html

Keeping You Connected During the COVID-19 Crisis

At Cisco, we're working to do our part by providing solutions, technology, tips, and resources to help our community during this challenging time.

Message from CEO Chuck Robbins >

Our Offerings | Small Business | For Partners | Ask-the-Expert | Community Support | Blogs | Resources

Helping communities, customers and partners to operate effectively in virtual environments across the globe.

Explore our offerings to help keep you securely connected.

3/10にセキュアリモートワークに関しての情報を掲載

Secure remote workers

Enable your employees to work from home and safely connect to their network and teammates.

Essential business

Solutions for essential business services to increase capacity and reliability.

Healthcare

Securely manage the surge in demand for virtual care and temporary field hospitals and clinics.

Education

Deploy virtual education solutions with simple, secure, reliable platforms for distance learning and administration.

	安全なリモートアクセス AnyConnect	セキュア インターネット ゲートウェイ Umbrella	多要素認証セキュリティ DUO Security	エンドポイント保護 AMP for Endpoint
購入済みのお客様	ユーザ数制限なしでご利用可能 2020年7月1日まで ※AnyConnect申請から90日間			ご購入の2倍までご利用可能 2020年7月1日まで
これからご利用されるお客様	ユーザ数制限なし			1,000台まで
	90日間		30日間	60日間

AnyConnect VPN
- 別途物理・仮想ASAなどVPN終端装置が必要です。
- 別途AnyConnectソフトウェアを入手頂く必要があります。

※Duo10,000ユーザ以上別途ご相談

VPN装置をお持ちでないお客様

仮想版ASAv30を特別価格（2020/7/25まで）にてご提供
（弊社営業にお問い合わせください）

ASAv30に関するオファー

モデル	ASAv5	ASAv10	ASAv30	ASAv50
Firewall性能	100 Mbps	1Gbps	2Gbps	10Gbps
VPN性能	30Mps	125Mbps	1Gbps	5Gbps
AnyConnectユーザ数	50	250	750	10,000
High availability	アクティブ/スタンバイ			
Hypervisor support	VMware ESX/ESXi 6.0, 6.5; vMotion KVM Hyper-V: Windows Server 2012 R2 (Not supported for ASAv50)			
Public Cloud Support	AWS (c3.large, c3.xlarge, c4.large, c4.xlarge, M4) Azure (d3, d3_v2) (including Azure Government Cloud)			AWS サポート
Virtual CPUs	1	1	4	8
Memory	1GB 最小 1.5 GB 最大	2 GB	8 GB	16 GB
Minimum disk storage	8 GB	8 GB	16 GB	16 GB

https://blogs.cisco.com/security/cisco-expands-free-security-offerings-to-help-with-rise-in-remote-workers

March 10, 2020 72 Comments

Security

As the Number of Remote Workers Rises, Cisco Supports Customers with Expansion of Free Security Offerings

Dr. Gee Rittenhouse

Helping employees, customers and partners in a time of need is one of Cisco's core values. Right now, COVID-19 is forcing many people around the world to work remotely. This is putting a sudden strain on both IT and security teams who are being tasked with providing support for an unprecedented number of offsite workers and their devices.

Recently, Cisco Webex expanded its free offerings to allow employees to stay connected to their teams and continue their business operations. In response to customers asking us for guidance, today, Cisco is broadening this offer to include security for remote employees by providing extended free licenses and expanded usage counts at no extra charge for three of our key security technologies that are designed to protect remote workers anywhere, anytime and on any device.

- Cisco Umbrella protects users from malicious Internet destinations whether they are on or off the network. Because it is delivered from the cloud, Umbrella makes it easy to protect users everywhere in minutes. With this offer, existing customers can exceed their user limit to support an increase in remote workers, and new customers can access a free license. To have the initial 14-day period extended to 90 days, please contact the Cisco sales team.
- Duo Security enables organizations to verify users' identities and establish device trust before granting access to applications. By employing a zero-trust model, it decreases the attack surface and reduces risk. With this offer, existing customers can exceed their user limit to support an increase in remote workers, and new customers can access a free license.
- Cisco AnyConnect Secure Mobility Client empowers employees to work from anywhere on company laptops or personal mobile devices. It also provides the visibility and control security teams need to identify who and which devices are accessing their infrastructure. Existing AnyConnect customers can exceed their user limit to support an increase in remote workers, and new customers can access a free license. To get started, existing and new customers should talk with a Cisco representative or partner to get the requested usage counts. For more information on implementation, please view the online documentation.

These offers will be available from now until July 1, 2020. Supporting our customers and partners remains a top priority, and we hope these proactive steps help companies manage the business impact and keep employees safe during this evolving situation.

To learn how Cisco can help you with business continuity planning during the COVID-19 pandemic, please visit: http://cisco.com/go/covid19

https://gblogs.cisco.com/jp/2020/03/secure_teleworking_by_cisco/

zzfeatured

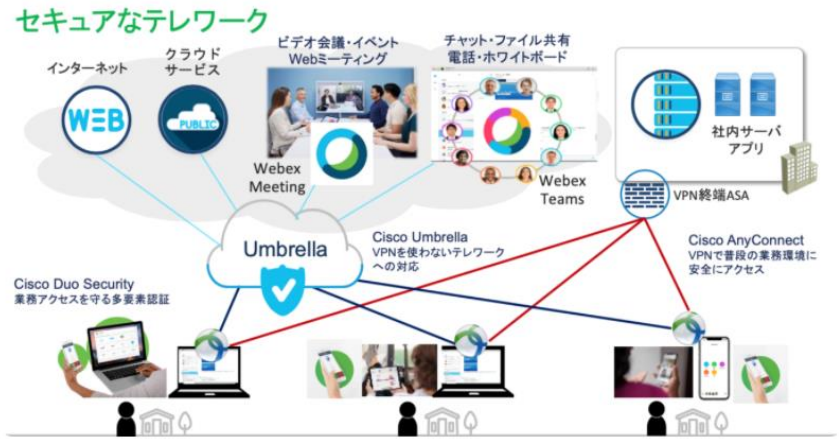
セキュアなテレワークの無料トライアル拡張

西 豪宏
2020年3月16日

現在、多くの人々にリモートワークが必要になっています。

最近Cisco Webexは無料のサービスを拡大して、業務を継続できるようなテレワーク環境を提供しています。

こちらのブログの通り、シスコはリモートワークに有効な3つのセキュリティテクノロジ（Umbrella, Duo, AnyConnect）を一定期間（2020年7月1日まで）追加料金なしで、追加ライセンスと利用ユーザの拡大を提供することで、セキュアなテレワーキングをご利用いただけるようトライアルオファーを拡大しました。



https://blogs.cisco.com/security/expanding-free-security-offers-into-customers-endpoints

April 1, 2020 Leave a Comment

Security

Expanding Free Security Offers into Customers' Endpoints

Dr. Gee Rittenhouse

During this global health crisis, normal has been redefined. We are living through a dynamic situation that has required us to reorient our personal and professional lives in ways we never have before. Companies have had to do the same. Many have taken the extraordinary step of moving the majority, if not the entirety, of their workforces to a virtual workplace. As companies adapt to their new normal, securing this sudden exponential growth of remote workers and their devices remains a challenge.

A few weeks ago, we shared that Cisco would provide extended free licenses and expanded usage counts at no extra charge for three of our key security technologies that are designed to protect remote workers: DNS-layer security from Cisco Umbrella, zero-trust security from Duo and secure network access from AnyConnect. As a result of this, there has been a huge demand for these technologies. Cisco has supported an additional 9 million-plus users during this crisis with this rollout.

Security teams generally start by securely connecting employees to the network with the VPN, and multi-factor authentication provides an additional layer of security to customers' remote access strategy. As security teams work to protect a larger remote workforce, Duo is seeing the number of daily authentications from VPNs increase by 157 percent. But we know that 85 percent of corporate users bypass the VPN when working remotely. So, customers are increasingly looking to DNS-layer security to secure users on and off the network, and we have seen the need for Umbrella licenses increase by 100 percent.

Through all of this, we have been listening to customers feedback on how else we can best support them. What we heard is that more than ever there is a need to protect both user-owned and company-owned devices. Based on that input, today we are extending our free security offers to also include Cisco Advanced Malware Protection (AMP) for Endpoints. This technology prevents breaches and blocks malware at the point of entry as well as detects, contains and remediates advanced threats if they evade the frontline of defense.

With this new addition, existing customers can exceed their device limit by two times to support an increase in remote workers. To take advantage of this offer, they simply install AMP for Endpoints Connectors on extra devices, and no other action is required. As with our AnyConnect, Umbrella and Duo offers, this will be available until July 1, 2020.

Our mission is to be our customers' most trusted partner by providing effective security solutions. This current situation demands this more than ever, and we will continue to stand with our customers and partners through this challenging time.

You can learn more about our Cisco Security Remote Worker offerings here and find additional resources on the Business Continuity site. If you have any questions, please contact your Cisco representative or email us at pandemicsupport@cisco.com.

https://gblogs.cisco.com/jp/2020/04/amp_secure_teleworking/

セキュリティ

テレワークにも有効なエンドポイント対策

西 豪宏
2020年4月30日

リモートワーク急増に伴うセキュリティ対策のご提供内容やエンドポイントへの提供の拡大に関連して、テレワークに有効なエンドポイントのセキュリティ対策についてご紹介いたします。

エンドポイントは最後の砦

テレワークの実施によりセキュリティの課題が浮上しておりCisco Talosから最新情報や対策指針が出ています。

シスコサイバーセキュリティレポートなどでもマルウェアは常に最大の脅威となっており、シスコグローバルネットワーキングトレンドレポートによると、2019年にCISOの48%が「修正までの時間」を主なKPIとして挙げており、この数字は2018年の30%から上昇しています。

エンドポイントでのマルウェア対策はあらゆる脅威の最後の砦となり、テレワークでのセキュリティ対策はもちろん、あらゆる場面で、Cisco AMP for Endpoints などのソリューションを利用してエンドポイントの可視性、保護、被害軽減を図ることが今まで以上に重要になります。

マルウェア対策に必要な要素

Why Cisco リモートワークセキュリティ

安全なリモートアクセスVPN

Cisco AnyConnect

- 長年利用されてきている実績と導入数
- パソコン、スマートフォンやタブレットなど幅広い端末に対応
- 接続前にデバイスの安全性を確認
- VPN接続を自動的に判断（Always-On機能）
- VPN通信を業務のみの通信に（Dynamic Split Tunneling）
- 業務外（ニュース・動画サイト）と業務（VPN）利用でVPN解除は不要

セキュア インターネット ゲートウェイ

Cisco Umbrella

- DNSレイヤとセキュアWebアクセスの両方をカバーするSaaS提供
- 業界トップの脅威検知率（DNS、ウェブ共（第三者調査結果））
- 攻撃者の悪用が増加している DNS セキュリティを強化迅速な展開が可能
- 柔軟な展開（DNSのみ、エージェント配布、NW連携（端末の変更無し）
- 低遅延、高パフォーマンスかつ堅牢なサービス
- マルチテナントによる管理権限移譲

ゼロトラスト/多要素認証

Cisco DUO Security

- 簡単な導入と運用・既存の認証DBの利用可能
- 多様な多要素認証の手法
- デバイス可視化・MDM連携
- 広範囲なアプリケーション連携
- 各種法規制に対応（GDPR,PCI DSS,NIST800など）

マルウェア対策・エンドポイント保護

Cisco AMP for Endpoint

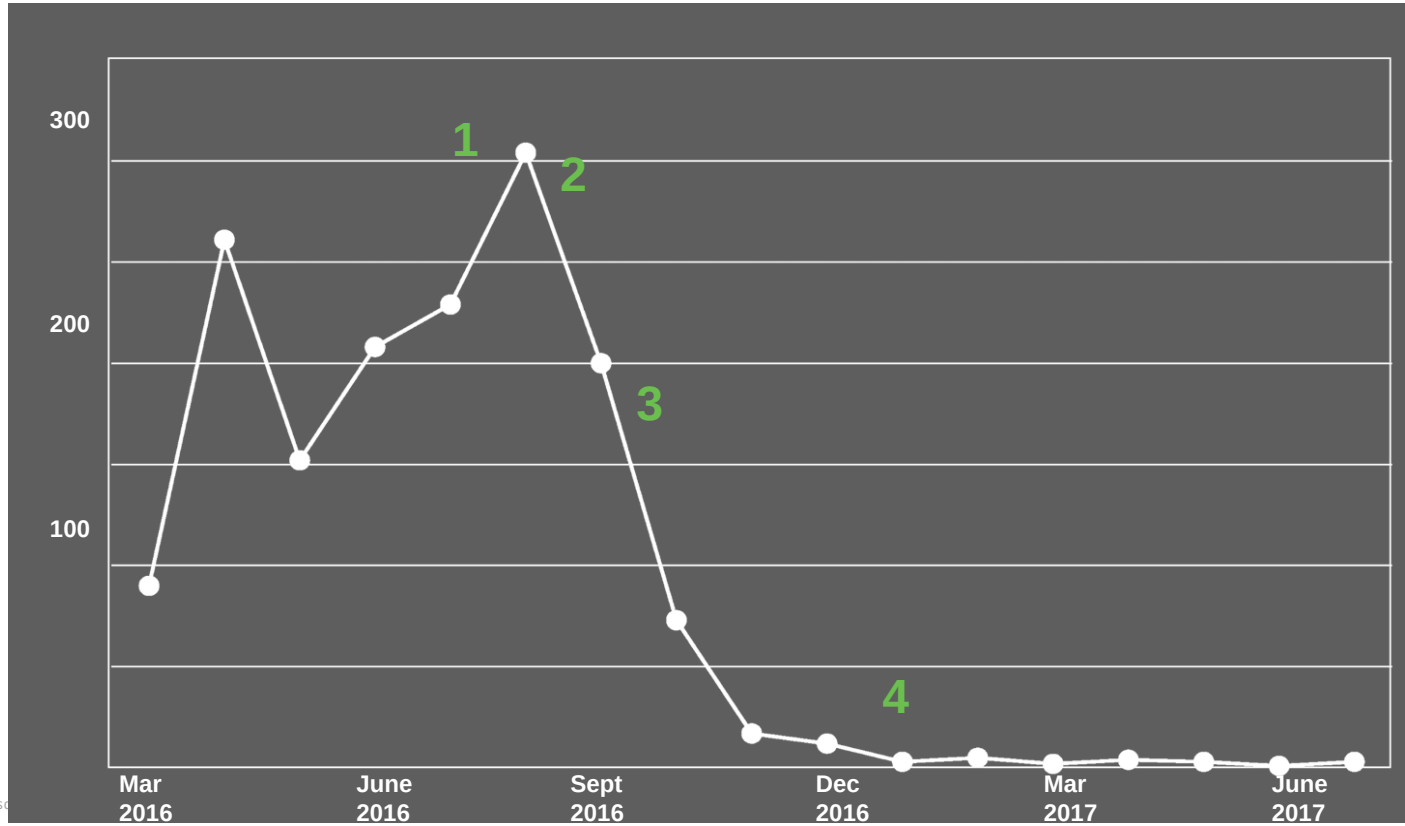
- パソコン、スマートフォンやタブレットなど幅広い端末に対応
- EPP（エンドポイント保護プラットフォーム）とEDR（エンドポイント検出と応答）の両方に対応
- マルウェア等の感染原因・範囲特定、端末隔離等全て遠隔での運用が可能
- Umbrellaやメールセキュリティなどと連携して感染の全体像を可視化可能

多要素認証（Duo Security）導入効果の事例

2016年3月から2017年7月までの月毎の侵害を受けたアカウント数

1. VPNサービス向けにDuoの登録を開始
2. 5,000 ユーザが登録され、Office365向けにユーザ登録を開始
3. 50,000 ユーザが登録される
4. 65,000 ユーザが登録される

侵害を受けたアカウントを96% 削減



Why Cisco テレワークセキュリティ

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/

- 第三者調査で1位に選出
- DNSレイヤとセキュアWebアクセスの両方をカバー

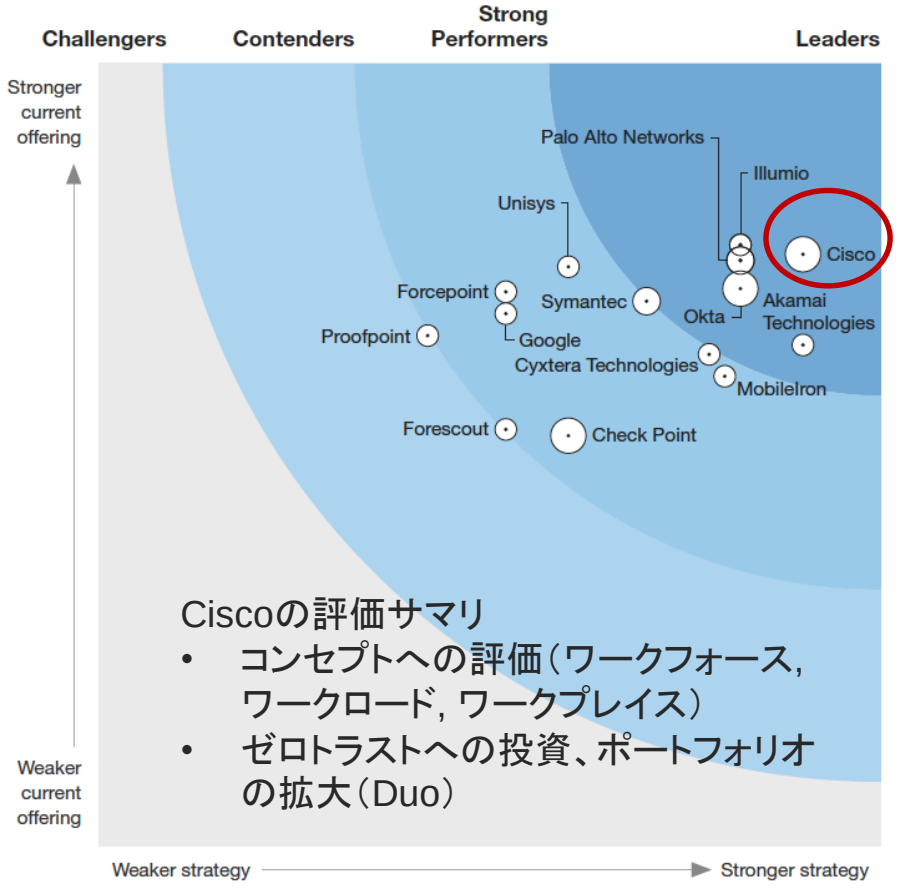
DNS レイヤー保護テスト

ベンダー	検出率 | テストケースの数 3,668
Cisco Umbrella（選択的プロキシを使用する DNS レイヤー）	72.6%
Cisco Umbrella（DNS レイヤー）	51.8%
Infoblox BloxOne	35.3%
Akamai Enterprise Threat Protector	26.5%
Palo Alto Networks Next-Generation Firewall	13.7%

セキュア Web ゲートウェイテスト

ベンダー	検出率 | テストケースの数 3,668
Cisco Umbrella Secure Web Gateway	90.5%
Symantec Web Security Service	84.7%
Zscaler Internet Access	83.7%
Palo Alto Networks Prisma Access	72.4%

Zero Trust eXtended Ecosystem Platform Providers, Q4 2019 (2019/10/29)



Ciscoの評価サマリ

- コンセプトへの評価（ワークフォース，ワークロード，ワークプレイス）
- ゼロトラストへの投資、ポートフォリオの拡大（Duo）

事例・MSP

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

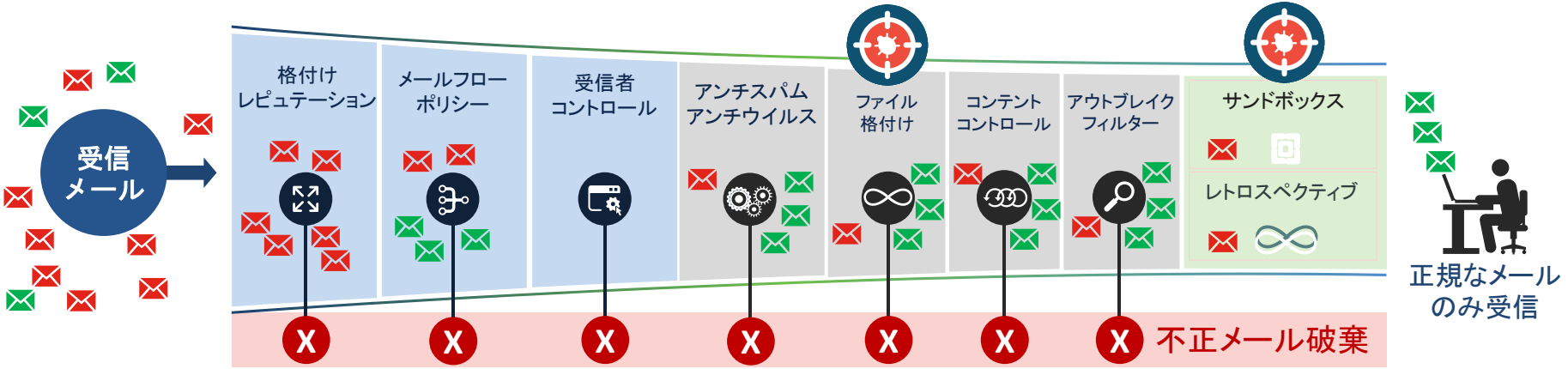
情報通信/メディア	セキュリティ	Cisco Umbrella Cisco AMP for Endpoint Cisco Threat Response Cisco ISE（Identity Services Engine）	静新 SBS グループ 多種多様な職種とデバイス、働き方の変化に対応する新たな統合セキュリティ対策を実現	2020年2月
教育	セキュリティ	Cisco クラウド E メールセキュリティ（CES）	国立大学法人 北見工業大学 クラウド E メールセキュリティにより教職員の安全と業務効率を向上	2019年11月
医療	コラボレーション,クラウド,ワイヤレス,データセンター,セキュリティ	Cisco Umbrella クラウドセキュリティ Cisco ASA 5500 シリーズ Cisco Telepresence SX, DX シリーズ Cisco IP Phone 7800, 8800 シリーズ Cisco Webex Meetings	前橋赤十字病院 iPhone を活用した多職種な職員全員が「つながる」チームコミュニケーション基盤の実現 導入編を観る（2:25 min） ユーザ編を観る（1:49 min）	2019年10月
サービス業	セキュリティ	Cisco Umbrella	SCSK 株式会社 クラウドベースのセキュア ゲートウェイを採用し社外で業務する社員とデバイスのセキュリティを強化	2019年8月
サービス業	セキュリティ	Cisco Cloudlock Cisco Umbrella	株式会社エス・エム・エス 安全な事業成長を支える SaaS での機密データ通信の可視化を実現	2019年4月
サービス業	セキュリティ	Cisco AMP for Endpoints	Destel シスコのテクノロジーで、収益性の高い健全なビジネスを実現	2018年12月

様々なお客様で
利用され
サービスとしても
活用されています

攻撃の始まりはメールから

不正なメールをブロック

忘れてはいけないメールセキュリティ



不審なメールは開かない

不正な添付ファイルを開かない

URLリンクをクリックしない

ツールに頼らない対策

シスコメールセキュリティ（アプライアンス・仮想版・クラウド）

不審なメールを受信前に破棄

不正な添付ファイルを破棄

URLなくなりクリックできない

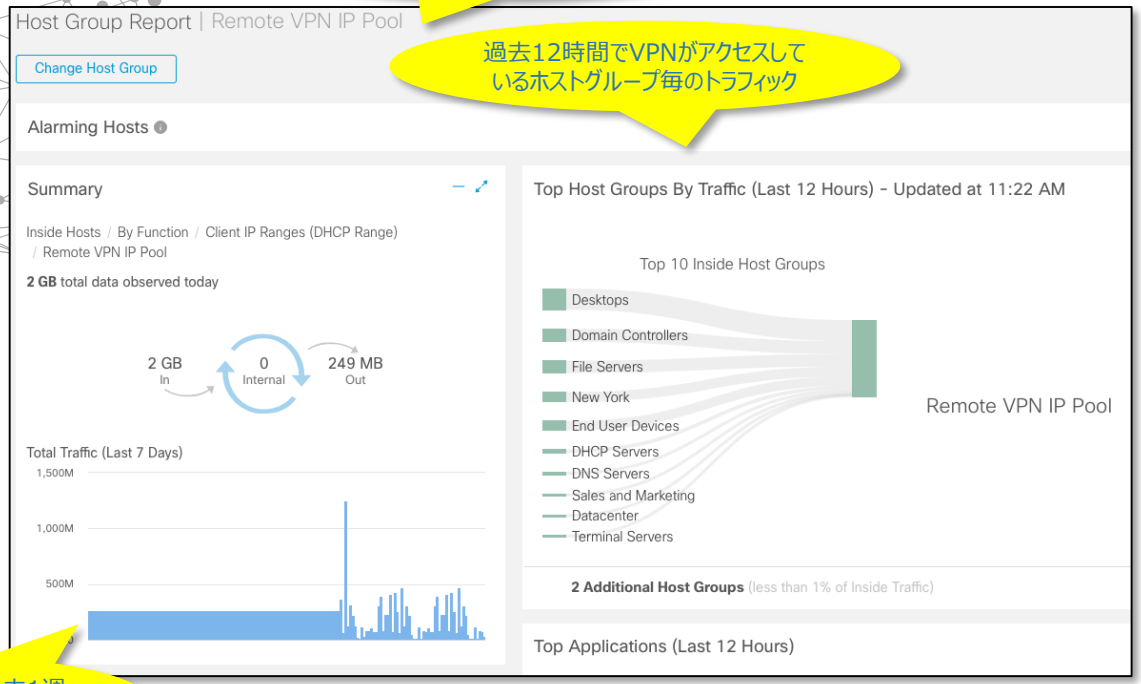
得られる効果

リモートアクセス環境におけるネットワーク可視化

リモートユーザーがネットワークとアプリケーションにいつどのようにアクセスしているか、
安全にアクセスしているかどうかをリアルタイムに監視

リモートアクセスVPN

- リモートユーザーの通信監視
  どのユーザーが何のアプリケーションをどれくらい利用しているのか
- セキュリティポリシー違反の検知
  許可されていないサーバーへのアクセスなど
- VPNの利用率
  ネットワーク遅延の調査
  キャパシティプランニングへの活用



忘れてはいけないネットワーク可視化

リモートワーカー保護のための
Cisco CX（シスコセキュリティサービス）オファー

無償の エキスパート セッション

無償のAsk the Expert セッションが
ライブ及び録画で利用できます

**セキュアリモートアクセス
テクニカルコンサルティングサービス**

コンサルタントによるサポートと
課題に対する推奨のご報告

**セキュアリモートアクセス
設計・構築支援サービス(スモール)**

新規リモートアクセス環境導入の
支援　(1 VPN クラスタ)

**セキュアリモートアクセス
設計・構築支援サービス(ミディアム)**

新規リモートアクセス環境導入の
支援　(2 VPN クラスタ)

- セキュアリモートアクセスの各サービスのお見積もりは、弊社サービス営業までお問い合わせください。

テレワークのインフラと業務アプリケーションをセキュアに DDoS・WAF無償トライアル

- リモートワークの需要が高まりVPN通信が増加しています。VPNインフラはより重要性を増し、サイバー攻撃（特にDDoS攻撃）の対象となっていますが、正規利用者のアクセスを正しく保護する必要があります。
- この重要な時期にお客様の業務を支援し、事業継続性を確保するためにCloud DDoSプロテクションサービスとCloud WAFサービスの無料トライアルをご提供します
- 2020年7月1日までのお申込み分まで
- 新規のお客様:90日間無料トライアル
- テクニカルサポート: ERT-SOC@Radware.comにて、トライアルライアル期間中のサポート(英語)

Cloud DDoS プロテクションサービスオンデマンド

- リモートワークのインフラを保護するクラウドベースのDDoSプロテクションサービス。正規通信と攻撃通信を正確に区別するためのパテントベースの独自機能と、リアルタイムシグネチャ生成機能にて最大18秒でゼロデイDDoS攻撃を防御することが可能。
- トライアルキャパシティ:Cloud DDoSオンデマンド，最大500Mbpsの正規通信量、BGPダイバージョンの場合4つの/24ネットワーク、DNSの場合は20個の防御対象IPアドレスまで

Cloud Web Application Firewall (WAF)

- マシンラーニングをベースとした自動ポリシー生成およびお客様Webサイトのセキュリティ分析を実施し、Webアプリケーションに対する不正侵入や脆弱性をつく攻撃を即座に防御します。
- トライアルキャパシティ:最大500Mbpsの正規通信量、5つの保護対象Webアプリケーションに対応

本製品はラドウェア社のDDoS・WAF製品となり、シスコはOEMでご提供しています。

❑ 詳細は弊社営業までお問い合わせください

まとめ

テレワーク・リモートワークの需要の高まり

- 普及は進みつつあるが実施に課題があるケースも存在
- テレワーク・在宅勤務制度は今後の人材確保に必要な領域
- 感染拡大に便乗する攻撃者（悪質広告の増加、遠隔会議システムが狙われる、特別定額給付金攻撃メール）

テレワークを実施する際にセキュリティ上留意すべき点

- 基本的なセキュリティ対策の徹底はテレワークでも必須
  「平易なパスワードを使わない」「パスワードの使いまわしをしない」「OS・アプリ・ソフトを常に最新の状態にする」「不審なメール添付ファイルを開かない」「メール本文中URLリンクをクリックしない」「マクロ有効・コンテンツ有効のボタンは信用できると判断できない限りクリックしない・クリックしたらすぐに管理者に相談・報告する」
- セキュリティシステムでの検討事項の例
  - VPNで普段の業務に安全にアクセス
  - VPNを使わない業務での安全性の確保
  - 多要素認証の利用により不正侵入を防ぐ
  - 脅威の始まりと目的であるメールとマルウェアへの対策

シスコがお手伝いいたします

シスコはテレワークを実施して20年になります
セキュアなリモートワークのユーザ拡大やトライアル期間延長をご提供いたします
セキュリティ研究機関であるTalosの各種ブログでの情報提供や、各種サイバーセキュリティレポートシリーズでの脅威トレンド等を提供しています。またセキュリティ製品及びサービスのご提案・ご提供を通じて、多様な脅威への対応をお手伝いさせていただきます

シスコ ブログ テレワークで検索ください　　https://gblogs.cisco.com/jp/tag/テレワーク/

生産性高く、健やかにテレワークを行うための６つのコツ

テレワーク

宮川 愛
2020年3月17日 - 0 コメント

シスコの働き方変革を推進した人事部として、生産性高く、健やかにテレワークを行うコツを 6つにまとめて、シスコ社員に共有しました。シスコ社員にとどまらず、テレワークで仕事をされている方々のお役にたてればと思い、ブログとして投稿させていただきます。

Duo Security でWebex (Meetings, Teams) の “なりすまし” を防止

セキュリティ

村上 英樹
2020年2月19日 - 0 コメント

Duo Securityを利用すれば、情報漏えいのリスクを軽減できます。今回、シリーズ第2回目としてWebexの認証にDuo Securityの多要素認証を組み合わせた“なりすまし” 防止のソリューションについて、皆様にご紹介させていただきます。

テレワークライフの楽しみ方 ～第一弾　松本ぷりっつさん～

テレワーク

石丸 美里
2020年5月14日 - 0 コメント

現在多くの皆さんがテレワークを実施されていると思いますが、2001年からテレワークを導入している私たちシスコにとっても、これほど長期間オフィスに出社せずテレワークを実施するのは、正直初めての経験です。 そこで、この長期間にわたる自粛生活、そしてテレワークライフの合間のちょっとした気分転換になれば、という思いから、特別コンテンツをご用意させていただきました。

中小事業者も ”ニューノーマル” への備えを

スモール ビジネス

中元 聡
2020年4月14日 - 1 コメント

感染症拡大の影響によって世界の状況は様変わりしています。国内においても緊急事態宣言が出され、学校の休業、テレワークの推奨、外出の自粛要請など、大きな制約に直面しています。今後の展望としても楽観的なシナリオから悲観的なシナリオまで様々な予測がされています。その中で「ニューノーマル（New Normal）」というワードが広がっています。

Cisco Webex Teams スペース / チーム運営 10のコツ

コラボレーション

田邊 靖貴 (Yasutaka Tanabe)
2020年2月6日 - 4 コメント

「 Webex Teams で部屋作っといて!」と急に言われて、お困りではありませんか? Ciscoで働き、Webex Teamsを黎明期から使い倒している筆者が、Cisco Webex Teamsの「スペース」「チーム」の作り方のコツから、ユーザー間のコミュニケーションを円滑にする小技まで、以下の通り余すところなくお伝えします。

在宅勤務のベストプラクティス

コラボレーション

粕谷 一範
2020年3月31日 - 0 コメント

自宅から生産的に働くためのヒント 在宅勤務を余儀なくされる最近の情勢により、ホームオフィスや、そこでのベストプラクティスの重要度が高まっています。長年にわたって在宅勤務で重宝されてきたのが Cisco Webex です。これまでの導入事例から学んだことは貴重なため、皆さんと共有したいと考えています。

スマートに働く：リモートチームの管理術

zzfeatured

粕谷 一範
2020年4月16日 - 0 コメント

最近、チーム運営に新たな課題が持ち上がっています。メンバーが離れた場所で働く「テレワーク」という環境のなかで、どのようにチームを連携させるべきでしょうか？リモートチームを効果的に統率するとっておきのアドバイスを以下に紹介します。

今こそテレワーカーのパワーを集結しましょう

スモール ビジネス

中川 雅之
2020年4月22日 - 0 コメント

信頼できるシンプルでセキュアなインターネットアクセスをどこからでも可能にさせるCisco Meraki。現在、世界中の従業員がテレワークに移行するという、極めてまれな状況に直面しています。私たちはみな、お互いに離れていますが、今までにないほどインターネットで互いにつながっているのも事実です。Cisco Merakiは、各組織が最も得意なことを、できるだけ中断しないように事業継続できるようお手伝いしたいと思っております。

リモートワークでは怪しいビデオ会議サービスにご注意を

セキュリティ

坂川 健太
2020年4月28日 - 0 コメント

前例のない危機的状況の中で、リモートワークを余儀なくされている状況が続いており自宅からビデオ会議サービスなどを利用してミーティングを行う事が増えてきているかと思います。残念ながら、このような状況下においてもサイバー攻撃者は常に攻撃の機会を探しています。 独立行政法人「情報処理推進機構」（IPA）は4月23日に、あるビデオ会議サービスの非正規版が流通していると注

パートナー様とお客様を支援するためのリソース

セキュアなテレワークの実現に向けた
無料トライアルのご紹介ページ

セキュアなテレワークの実現に向けた無料トライアルのご紹介

https://www.cisco.com/c/m/ja_jp/partners/support-help/telework/security.html

セッションに関するご質問

シスコ コンタクトセンター 

アンケートフォームにご記入ください。

担当営業やシスココンタクトセンターまでにお問い合わせください。

今後のシスコセキュリティウェビナー

https://www.cisco.com/c/ja_jp/training-events/events-webinars/webinars.html

毎週木曜日開催を予定。当面の予定は以下となります。

2020/6/4	木	14:00-14:30	30分でわかる最新の多要素認証 (Duo Security)
2020/6/4	木	15:00-15:30	30分でわかるマイクロセグメンテーション
2020/6/11	木	14:00-14:30	30分でわかるVPN（AnyConnect）
2020/6/11	木	15:00-15:30	30分でわかるクラウドセキュリティ（Umbrella）
2020/6/18	木	14:00-14:30	30分でわかるメールセキュリティ
2020/6/18	木	15:00-15:30	30分でわかるエンドポイントセキュリティ（AMP）
2020/6/25	木	14:00-14:30	30分でわかる認証基盤（ISE）
2020/6/25	木	15:00-15:30	30分でわかる可視化と脅威検出（StealthWatch）


cisco Secure