# 他人事ではない！
# ランサムウェアの脅威と
# その対策について

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 西 豪宏

2020/12/04


CryptoLocker
Your personal files are encrypted!
Private key will be destroyed on
9/24/2013
6:21 PM
Time left
54 : 15 : 15
Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.
The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...
To obtain the private key for this computer, which will automatically decrypt files, you need to pay 100 USD / 100 EUR / similar amount in another currency.
Click <Next> to select the method of payment and the currency.
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.
MacBook Pro

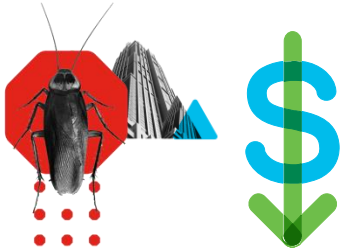
# 他人事ではない！ランサムウェアの脅威とその対策について

- ランサムウェアの脅威とは
- なぜ被害をうけてしまうのか
- どうすれば防ぐことができるか
- シスコは何をお手伝いできるか
- 付録（各対策ハイライト）

# ランサムウェアの脅威

- 事業継続の危機
- 高額な金銭の損失

身代金要求
情報暴露脅迫



ビットコイン

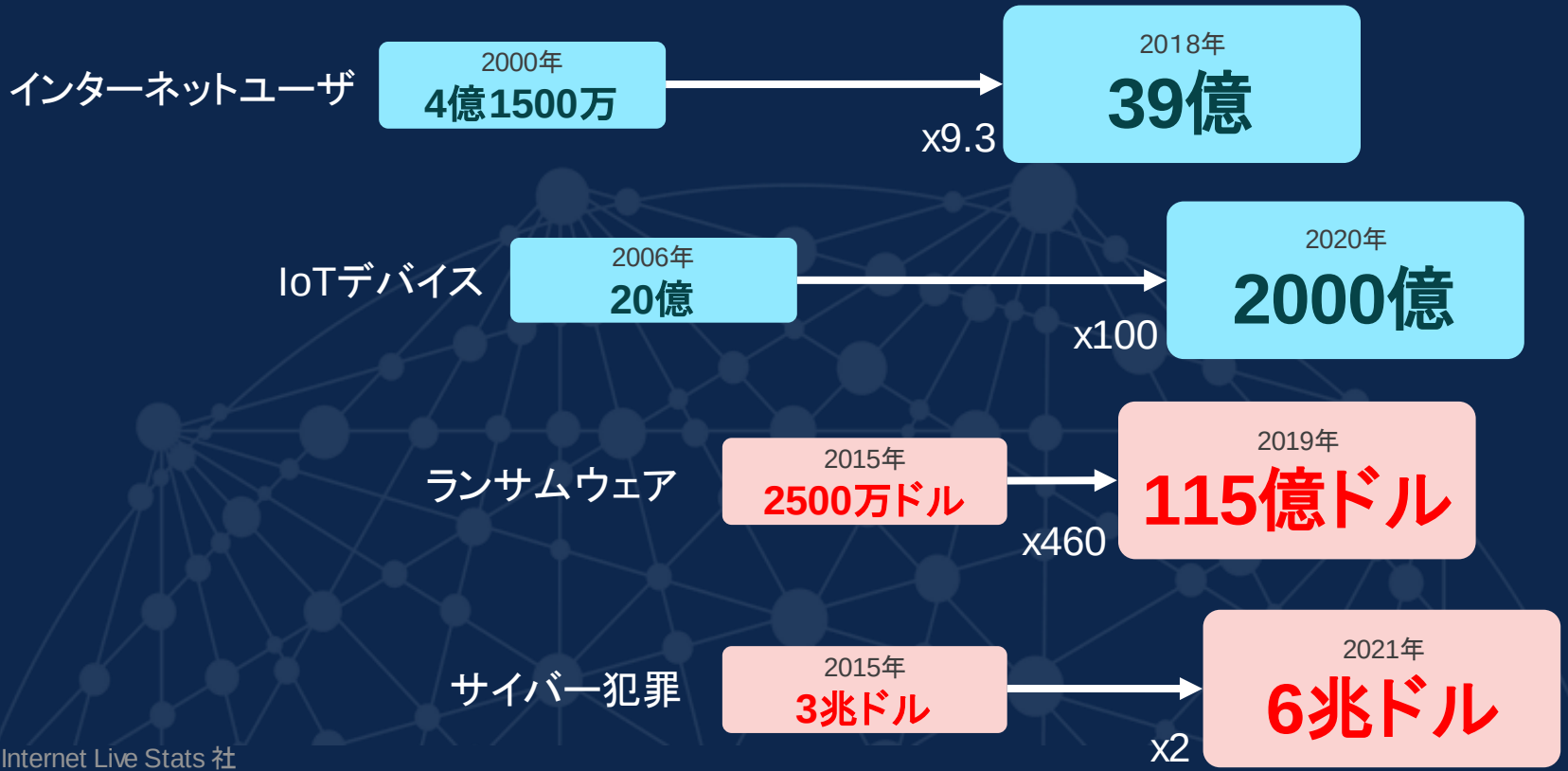
ランサムウェア

データ暗号化

業務継続不可

個人情報,認証情報
機密情報漏洩

# ユーザ・デバイス・サイバー犯罪




出典：Internet Live Stats 社
出典：Cybersecurity Ventures 社
など

# ランサムウェア
## データを利用不能・情報暴露脅迫し身代金徴収を目的とするマルウェア

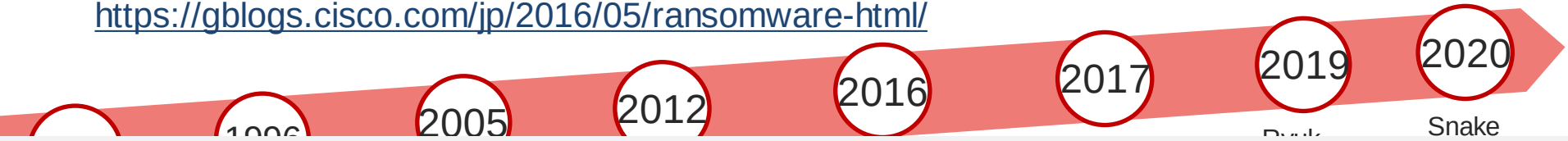
## 悪意のあるプログラムの総称：マルウェア

| | |
|---|---|
| ウィルス | プログラムの一部を改ざんして、増殖するプログラム<br>ユーザーに害を与えるプログラムの総称 |
| ワーム | 自己増殖型であり自分自身を複製して、<br>他へ感染動を行うプログラム |
| キーロガー | パソコンやキーボードの操作の<br>内容を記録するプログラム |
| スパイウェア | ユーザーの個人情報や行動を収集し<br>別の場所に送るプログラム |
| トロイの木馬 | 有用なプログラムに見せかけた悪意のあるプログラム（バックドア）で、兵士が中に入った木馬をトロイアの街に招き入れ壊滅した手口（ギリシャ神話） |
| ランサムウェア | データの利用制限（暗号化・使用不可）を行いその制限を解除するため、もしくは搾取された機密情報を公開しないために身代金（Ransom）を要求するマルウェア |
| クライムウェア | クライム（Crime：犯罪）ウェアは犯罪を目的として作られたプログラムの総称<br>技術的な知識を持たない人でも使え、クライムウェアキットも流通している |

WannaCry
ワーム型ランサムウェア

# 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/



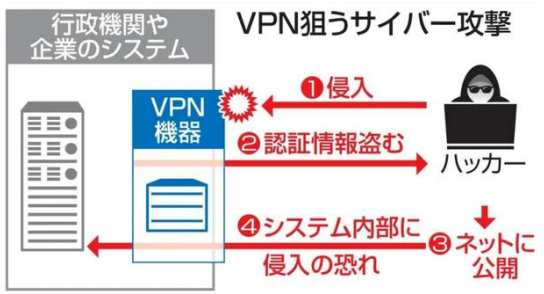

- 1989年 世界で初めてのAIDSというフロッピーディスクを介して拡散するランサムウェア
- 2012年 ランサムウェアReveton、身代金にビットコイン・高い利益を生む
- Cisco Talosが2016年初旬に発見したランサムウェアSamSamが多額を稼ぐ
- 2017年流行したWannaCry 自身を複製・拡散、大きな被害をもたらす
- 2018年 Thanatos 、暗号化プロセスに問題があり、身代金を支払った場合もデータを取り戻せない事態発生し、Cisco Talosは無料の復号化ツール「ThanatosDecryptor」を公開
- 2019年 Ryuk が猛威、盗んだデータを人質に身代金を支払わないとデータを晒すと脅す
- ランサムウェア Maze ・リモート デスクトップ 利用がコロナ禍のリモートワークで利用が拡大しており、さらに狙われる頻度が増えている
- インシデント対応の動向（2020年夏）：攻撃成功率を上げるための戦術として、特定の環境でのみ動作するランサムウェアSnakeなどの被害も報告される
- Ragnar Locker：データ漏えいの発生後、攻撃者から1,100万ドルの支払い要求があるという事例の通り、2重脅迫（暗号化と公開脅迫）にまで発展している

# 狙われるテレワーク

## 600超の組織にサイバー攻撃

テレワーク機器の欠陥悪用

2020/12/1 06:00 (JST) | 12/1 06:17 (JST) updated ©一般社団法人共同通信社




VPN狙うサイバー攻撃

テレワークや遠隔操作に使われる情報機器の欠陥が悪用され、少なくとも607の国内企業や行政機関などがサイバー攻撃を受けていたことが30日、専門家への取材で分かった。警察庁や日本政府観光局、岐阜県庁、リクルート、札幌大などで被害が判明。多くがID、パスワードなどの認証情報を盗まれていた。

この機器は外部からネットワーク内部に安全に接続するために利用され「VPN（仮想私設網）」と呼ばれる。新型コロナウイルス流行で利用が増えている。問題のVPNは米フォーティネット社製で、欠陥が放置されている機器は世界で約5万台あり、うち1割超の約5400台が日本関連だった。

Source:共同通信社
https://this.kiji.is/706248789438039137



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-newsletter-aug-22_29/

**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）

## 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

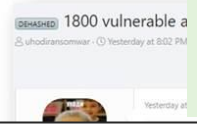
JPCERT-AT-2019-0033
JPCERT/CC
2019-09-02(新規)
2019-09-06(更新)

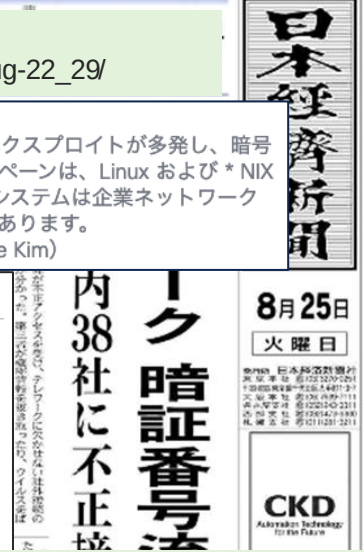
Source:JPCERT
https://www.jpcert.or.jp/at/2019/at190033.html

### I. 概要

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
います。

- Palo Alto Networks (CVE-2019-1579)
- Fortinet (CVE-2018-13379)
- Pulse Secure (CVE-2019-11510)




Source:https://www.zdnet.com/article/hacker-leaks-passwords-for-900-enterprise-vpn-servers/
900以上の企業VPNサーバのパスワードが公開
2020年6月24日～7月8日の間
Pulse Secure VPN 全体をスキャン・自動収集

## Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性 (CVE-2018-13379) の影響を受けるホストに関する情報の公開について

最終更新: 2020-11-27

Source:JPCERT
https://www.jpcert.or.jp/newsflash/2020112701.html

CyberNewsFlash一覧

(1) 概要

JPCERT/CC は、2020年11月19日以降、Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性の影響を受けるホストに関する情報が、フォーラムなどで公開されている状況を確認しています。当該情報は、FortiOS の既知の脆弱性 (CVE-2018-13379) の影響を受けるとみられるホストの一覧です。この一覧は、攻撃者が脆弱性を悪用可能であることを確認した上で作成したものとみられ、ホストの IP アドレスに加え、SSL VPN 接続を利用するユーザーアカウント名や平文のパスワードなどの情報が含まれているとのことです。

# 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/

# 特定の標的を狙う攻撃

Talos 脅威情報
https://gblogs.cisco.com/jp/author/talosjapan/

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。

**初期ベクトル**

ロギングの量が十分ではないため、ほとんどの IR 業務では初期ベクトルを明確に特定することが困難でした。ただし、初期ベクトルを特定できた事例や合理的に推測できた事例に基づく限り、最多の感染ベクトルは依然としてフィッシングです。標的組織の RDS にブルートフォース攻撃を仕掛けた事例もいくつか観測しています。これは、ランサムウェア Phobos の増加や、コロナ禍のリモートワークで攻撃対象が拡大したことと関連しているようです。通例、初期ベクトルとして利用されるのは侵害された RDS 接続です。Citrix Application Discovery Controller および Citrix Gateway（CVE-2019-19781）、さらに Pulse Secure VPN（CVE-2019-11510）に関しては、複数の侵害が継続的に観測されました。

**最近の注目すべきセキュリティ問題**

**件名：**Zerologon の脆弱性を悪用する攻撃者が増加
**説明：**Cisco Talos では、Microsoft 社の脆弱性 CVE-2020-1472 に対する攻撃が急増していることを確認しています。この脆弱性は Netlogon における権限昇格の不具合であり、8 月の Microsoft セキュリティ更新プログラムで概要が公開されました。脆弱性は Netlogon Remote Protocol で使用される暗号化認証方式の不備に起因しています。エクスプロイトされた場合、特定の Netlogon 機能の認証トークンが偽造され、コンピュータのパスワードを更新される可能性があります。脆弱性を利用すればドメイン コントローラ自体を含むあらゆるコンピュータを装えるため、ドメイン管理者のログイン情報にアクセスされる危険性があります。
**Snort SID：**55703、55704

## インシデント対応チームによる分析情報

医療機関を狙ったランサムウェア攻撃への複数の対応事案にも、Talos が携わっています。直近 90 日間を見ると、今四半期のインシデント対応事案のうち約 20% は医療分野で起きています。米国内のある医療センターが標的となった事案では、Ryuk に加え、レッドチーム活動ツールである Cobalt Strike が使用されていました（Cobalt Strike は Ryuk と併用されることが少なくありません。詳細については、以下をご覧ください）。ただし、米国の医療センターを狙った別のインシデント対応事案では、Ryuk 以外のランサムウェアが使用されていました。現時点では Vatet または Defray であると推定されます。どちらのインシデントに関しても、Trickbot の存在は確認されていません。

- サイバー犯罪者、裕福な都市部の学校を狙う傾向が強まる。それらの学校には大量のデータが保存されているため、身代金を支払える可能性がより高いと攻撃者が考えているようです。
- 新学期をリモート授業で迎えた教員と生徒たちは、新しい仮想クラスの利用方法とサイバー攻撃への対処方法を学ぶ必要に迫られる。フロリダ州マイアミはその代表例と言えます。市当局は域内の学校システムが 1 日で 12 回の攻撃を撃退したと発表しています。
- コネチカット州ハートフォード市、サイバー攻撃を受け新学期の開始を延期。市当局の発表によれば、学校教育に不可欠な 200 台のサーバが侵入されました。
- コロナ禍が依然として終息しない中、世界各地の教育機関がハイブリッド学習環境の維持に注力。しかし多くの教育機関は、オンライン学習を妨げるサイバー攻撃からの防御にも追われています。
- 国家の支援を受けた攻撃者、新型コロナウイルスのワクチン研究を標的とする攻撃を継続。
- チリの大手銀行、サイバー攻撃を受け今週すべての支店を閉鎖。現時点の報道では、従業員が開いた悪意のある Microsoft Office ドキュメントから攻撃が始まったようです。
- ノルウェー議会、今年初めに同国政府のネットワークに対してサイバー攻撃を仕掛けたとして、[redacted]政府の支援を受けた攻撃者集団を正式に告発。この攻撃により複数の政治家の電子メールアドレスがハッキングされています。

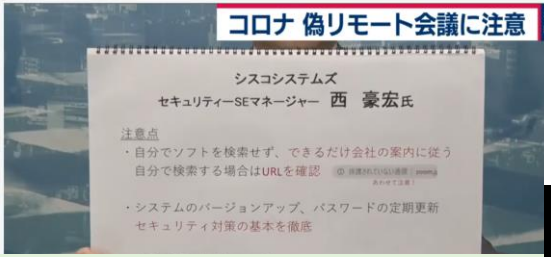
# 偽サイト・悪質広告

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。

午後


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


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。

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/

## 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）

## ほとんどマルウェア判定（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 |

# 他人事ではない！ ランサムウェアの脅威とその対策について

- ランサムウェアの脅威とは
- なぜ被害をうけてしまうのか
- どうすれば防ぐことができるか
- シスコは何をお手伝いできるか
- 付録（各対策ハイライト）

# Talosインシデント対応チーム タイムラインの典型例

0～6日目

**侵入開始・初期感染**

マルウェア配布とフィッシングに最も使われるのは電子メール
悪意のあるサイトへの誘導
リモートワークで必要なサービスへの侵入
多機能な侵入ツール・エクスプロイト（exploit）の利用
管理者アカウントが侵害

7～13日目

**偵察行動・感染拡大**

より価値のある対象を探す、より広範囲な対象を掌握する
内部状態の把握し、ログイン情報、機密情報を取得する
検出と防止を回避：仮想マシン起動、正規プログラムの利用
ファイヤウォール、ログ機能、各種セキュリティ機能を終了させる

14～21日目

**実行・被害**

暗号鍵を交換して端末のデータを一斉に暗号化される
搾取された機密情報を晒すと脅迫する

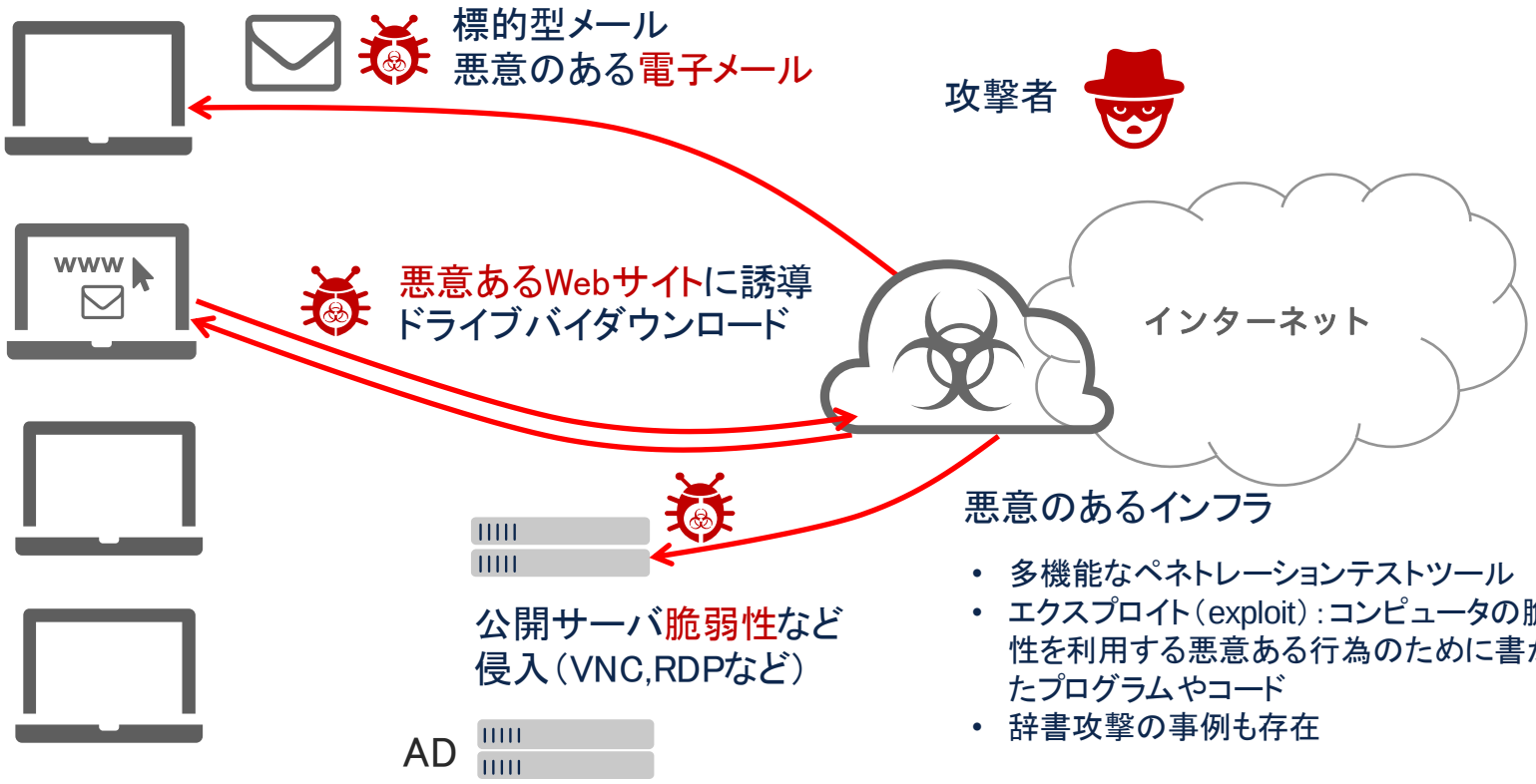
**原因特定・対応**

インシデントレスポンス(IR)対応方針を協議
フォレンジクス、封じ込め、是正措置等の対応をサポート
ソリューション活用（AMP, Stealthwatch, Umbrella等）
再発防止へ向けたプロアクティブな対策アドバイス

Talosインシデント対応チーム

- 最初の侵入から実際の攻撃までの時間は不均一
- 侵入後に攻撃を防げる時間と可能性はある

# 侵入開始・初期感染



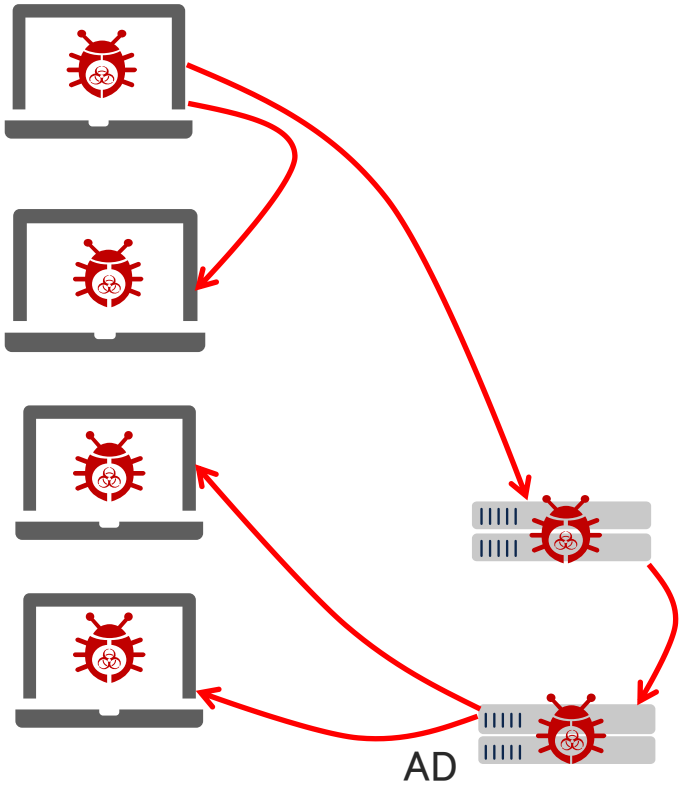

- 多機能なペネトレーションテストツール
- エクスプロイト（exploit）：コンピュータの脆弱性を利用する悪意ある行為のために書かれたプログラムやコード
- 辞書攻撃の事例も存在

特定の標的のみ動作・対象で挙動を変える場合も

侵入開始・初期感染

# 偵察行動・感染拡大

## 感染拡大し、攻撃体制を整える



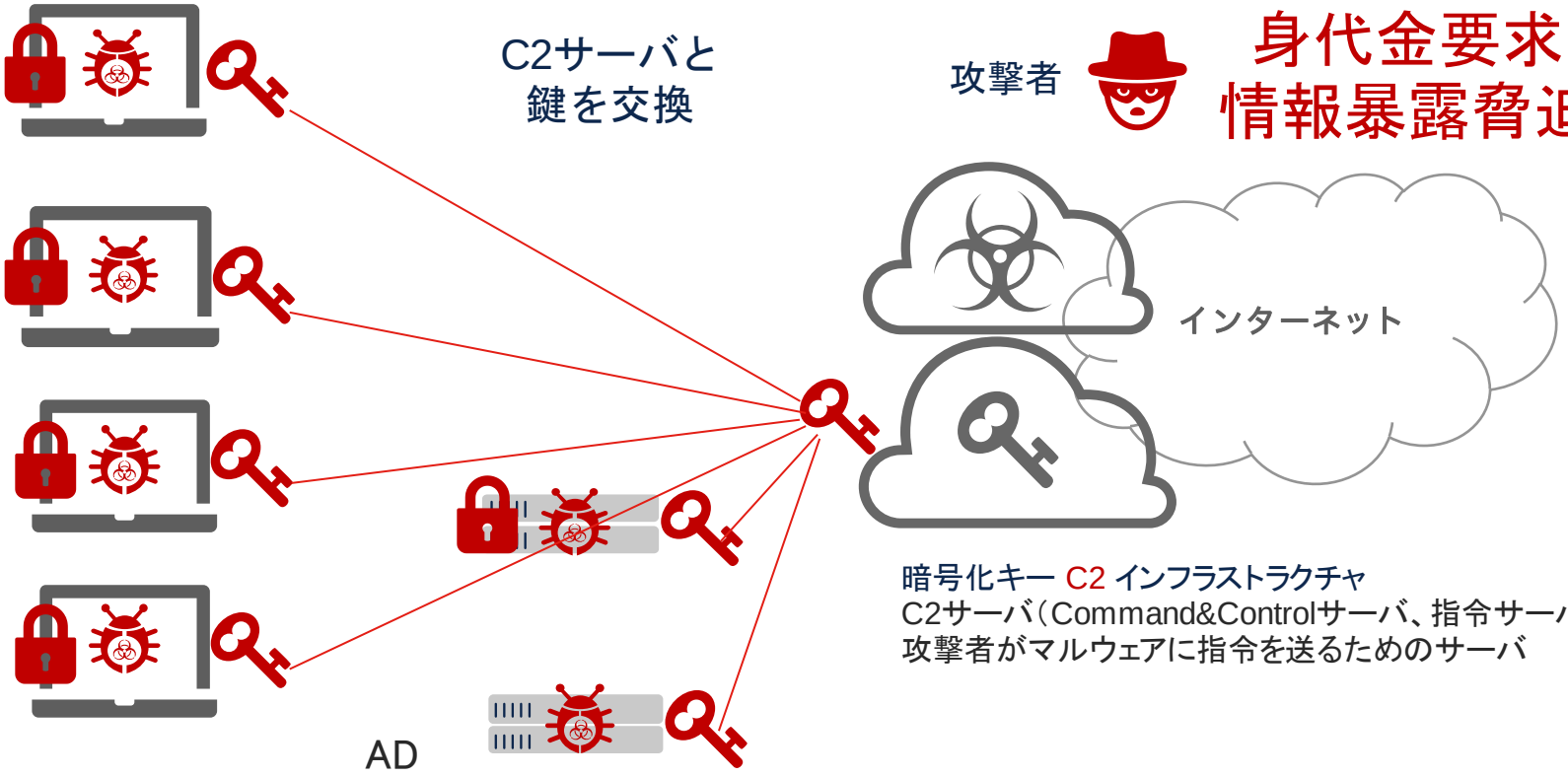


- 内部を探索する
- より価値のある対象・より広範囲な対象を掌握
- 内部状態の把握し、ログイン情報、機密情報を取得する
- 検出と防止を回避：仮想マシン起動、正規プログラムの利用
- FW、ログ機能、各種セキュリティ機能を終了させる

偵察行動・感染拡大

# 実行・被害

暗号鍵を交換して端末のデータを暗号化
搾取された機密情報を晒すと脅迫する

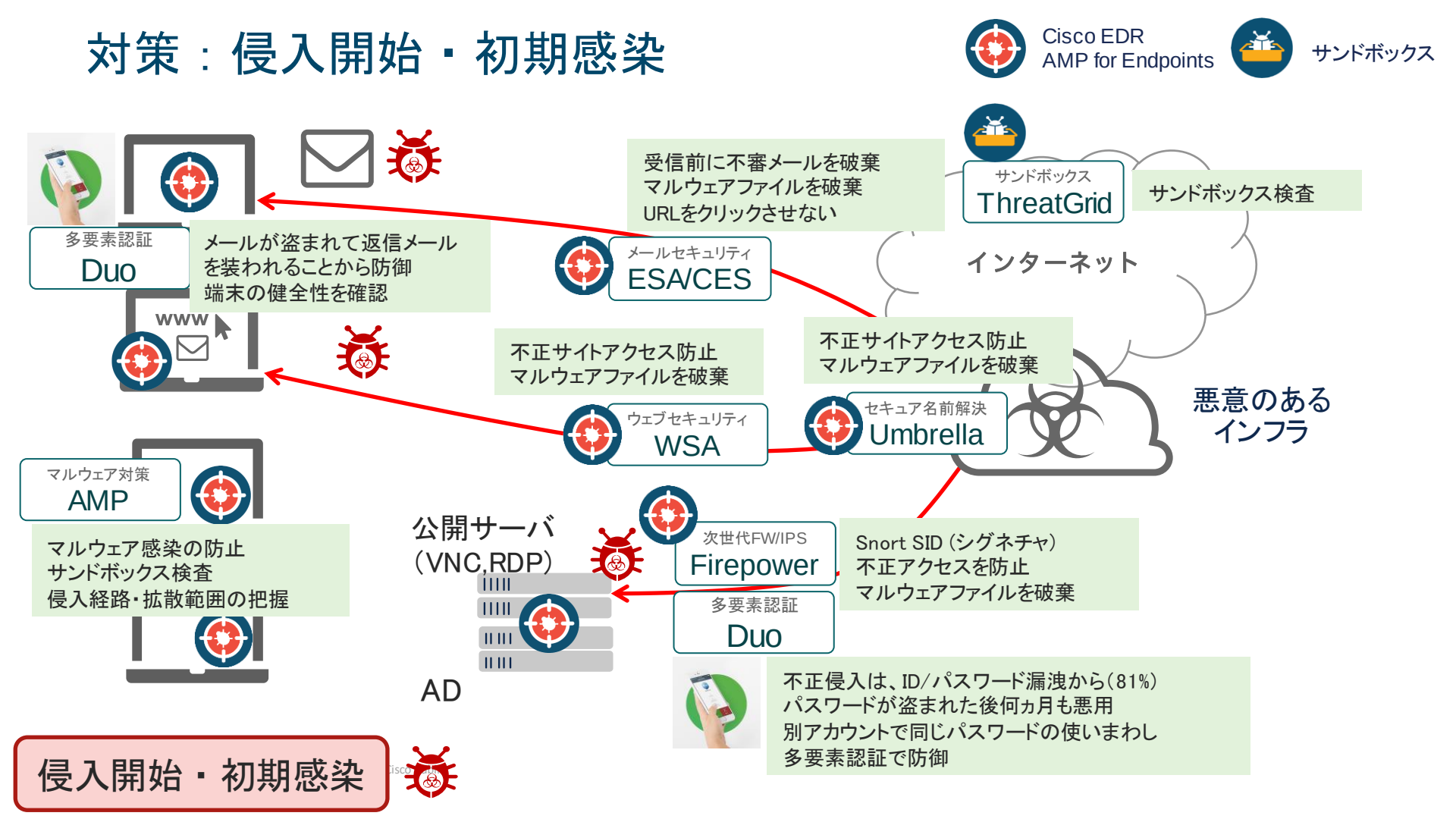



暗号化キー C2 インフラストラクチャ
C2サーバ（Command&Controlサーバ、指令サーバ）
攻撃者がマルウェアに指令を送るためのサーバ

# 他人事ではない！
# ランサムウェアの脅威とその対策について

- ランサムウェアの脅威とは
- なぜ被害をうけてしまうのか
- どうすれば防ぐことができるか
- シスコは何をお手伝いできるか
- 付録（各対策ハイライト）

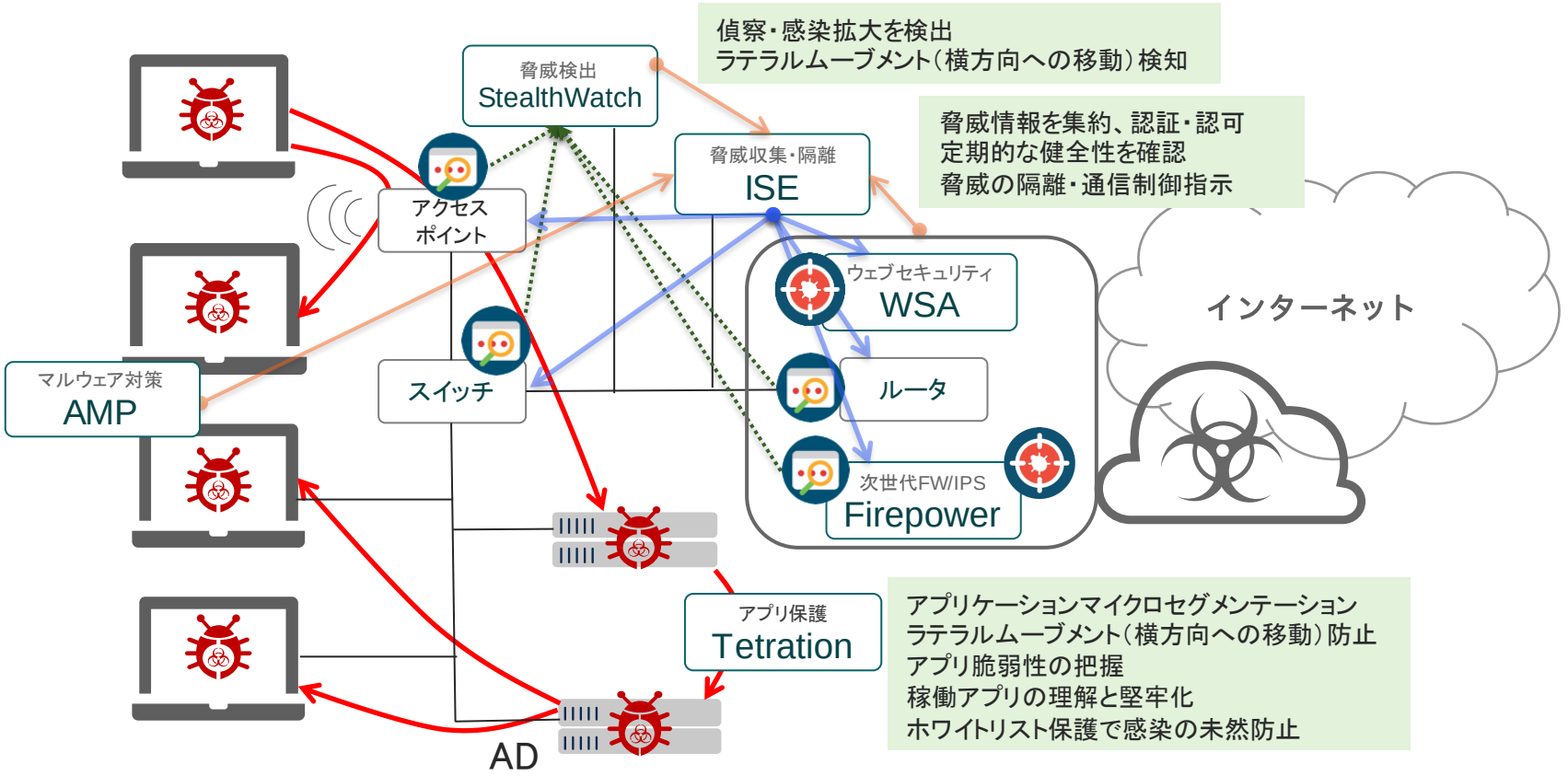
# 対策：侵入開始・初期感染


Cisco EDR
AMP for Endpoints
サンドボックス
多要素認証
Duo
メールが盗まれて返信メール
を装われることから防御
端末の健全性を確認
受信前に不審メールを破棄
マルウェアファイルを破棄
URLをクリックさせない
メールセキュリティ
ESA/CES
サンドボックス
ThreatGrid
サンドボックス検査
インターネット
不正サイトアクセス防止
マルウェアファイルを破棄
ウェブセキュリティ
WSA
不正サイトアクセス防止
マルウェアファイルを破棄
セキュア名前解決
Umbrella
悪意のある
インフラ
マルウェア対策
AMP
マルウェア感染の防止
サンドボックス検査
侵入経路・拡散範囲の把握
公開サーバ
（VNC,RDP）
AD
次世代FW/IPS
Firepower
Snort SID（シグネチャ）
不正アクセスを防止
マルウェアファイルを破棄
多要素認証
Duo
不正侵入は、ID/パスワード漏洩から（81%）
パスワードが盗まれた後何ヵ月も悪用
別アカウントで同じパスワードの使いまわし
多要素認証で防御
侵入開始・初期感染

# 対策：偵察行動・感染拡大

Netflow
脅威検出

Cisco EDR
AMP for Endpoints






偵察行動・感染拡大

# 対策：実行・被害

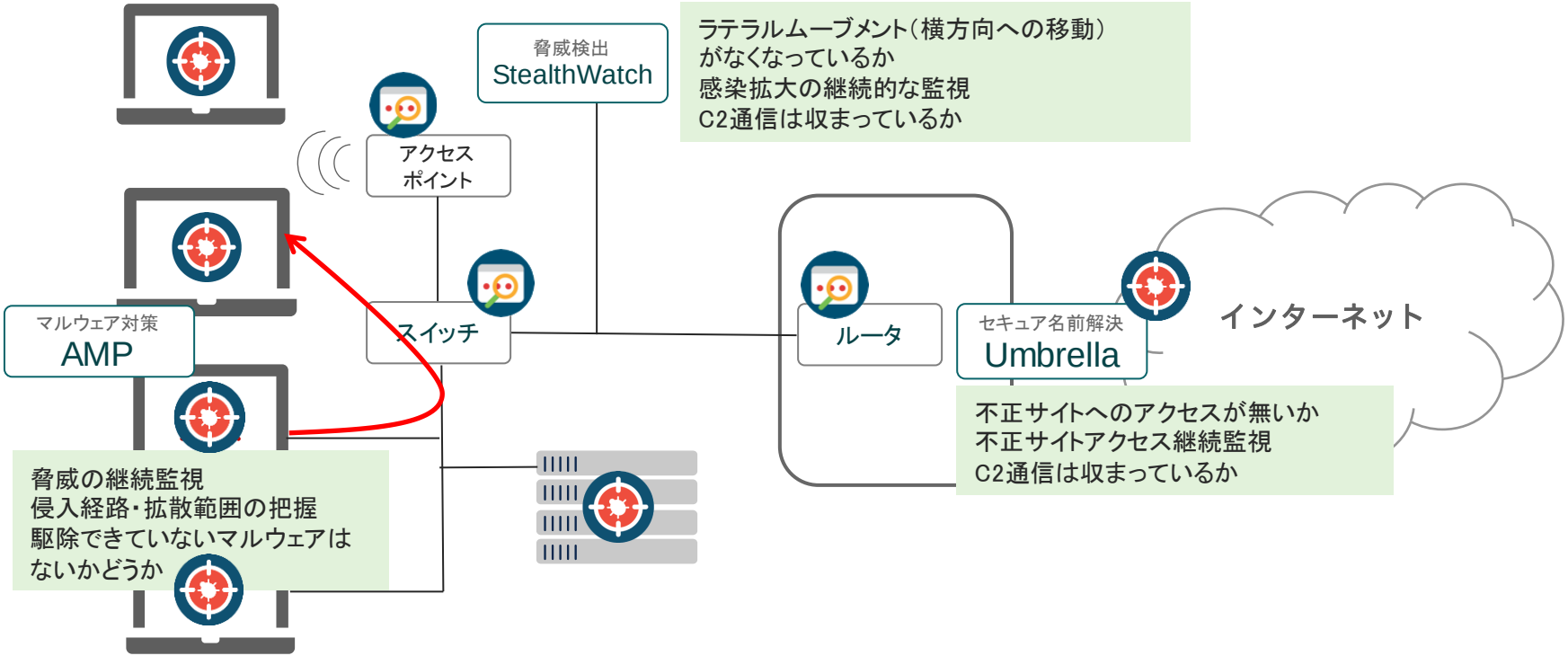
身代金要求
情報暴露脅迫






実行・被害

# 対策：原因特定・対応





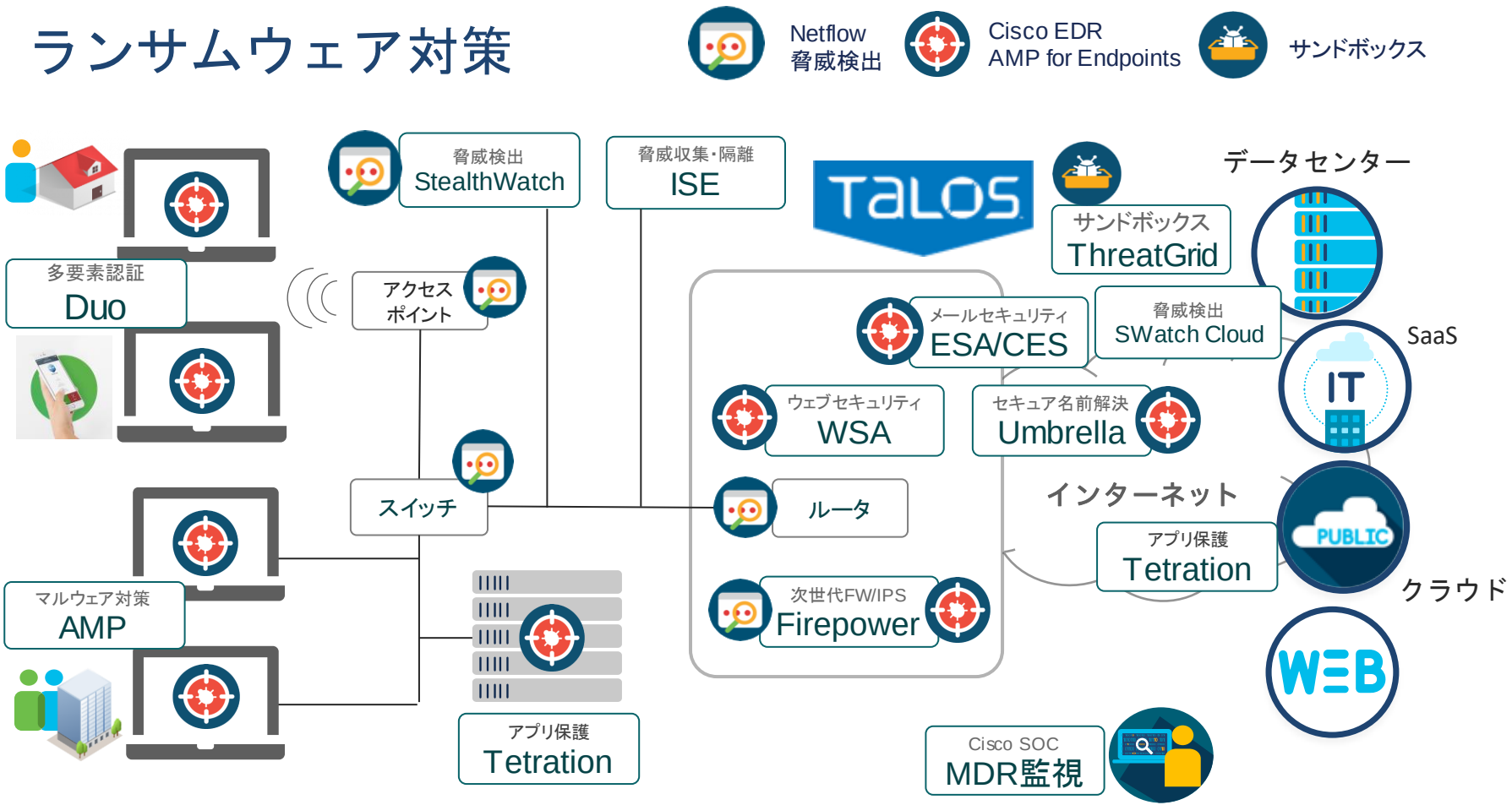

原因特定・対応（Cisco IRの例）

# ランサムウェア対策

（ Cisco IRの例）

| | 侵入・初期感染 | 偵察・感染拡大 | 実行・被害 | 原因特定・対応 |
|---|---|---|---|---|
| 多要素認証 Duo | 多要素認証で侵入を防御<br>端末の健全性を確認 | | | |
| メールセキュリティ ESA/CES | 標的型メールを破棄<br>マルウェアファイルを破棄 | | | |
| ウェブセキュリティ WSA | 不正サイトアクセス防止<br>マルウェアファイルを破棄 | | C2通信の検出と遮断 | |
| セキュア名前解決 Umbrella | 不正サイトアクセス防止<br>マルウェアファイルを破棄 | | C2通信の検出と遮断 | 不正サイトアクセス継続監視<br>C2通信収束確認 |
| 次世代FW/IPS Firepower | 不正アクセスを防止<br>マルウェアファイルを破棄 | | C2通信の検出と遮断 | |
| マルウェア対策 AMP/TG | マルウェア感染の防止・脅威の継続監視<br>侵入経路・拡散範囲の把握 | | | 脅威の継続監視<br>侵入経路・拡散範囲の把握 |
| 脅威検出 StealthWatch | | 感染拡大を検出・継続的な監視<br>ラテラルムーブメント対策 | C2通信の検出 | 脅威の継続監視<br>C2通信収束確認 |
| 脅威収集・隔離 ISE | | 脅威情報を集約、認証・認可<br>脅威の隔離・通信制御指示 | 脅威の隔離 | |
| アプリ保護 Tetration | | 感染拡大を検出・継続的な監視<br>ラテラルムーブメント対策 | C2通信の検出と遮断 | |

# ランサムウェア対策



https://gblogs.cisco.com/jp/2020/11/ransomware_defense/



セキュリティ

# 他人事ではない！ ランサムウェアの脅威とその対策について

西 豪宏
2020年11月25日

コロナ禍につけ込んだサイバー犯罪が増加の一途を辿っている中、Snake, Ragnar Locker などのランサムウェアと呼ばれる脅威と被害が拡大しています。

攻撃者は盗み出したデータを人質に取り、ビットコインなどで身代金（ransom、ランサム）を支払わないとデータを「晒す」と脅迫し、これを支払わなければ機密情報を暴露されるという被害に発展する事例が増えています。

シスコは昨今のランサムウェアの被害拡大を踏まえ、ウェビナーを緊急開催予定です。

本ブログとウェブセミナーでは、ランサムウェアの脅威は何なのかにはじまり、なぜ被害をうけてしまうのかという原因と、どうすれば防ぐことができたのかに関して Cisco Talos インシデント対応チームの対応事例なども踏まえ、対策のポイントをわかりやすく解説いたします。

## 何が起こっているのか

ランサムウェアと呼ばれる被害が急拡大し、企業や組織の事業活動への大きな脅威となっています。

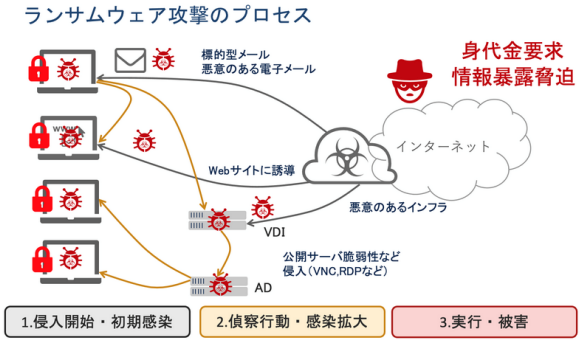
ランサムウェア(Ransomware)とは、悪意のあるプログラムであるマルウェアの一種で、これに感染するとデータが暗号化され使えない状態に至り、その復旧と引き換えに身代金（ransom、ランサム）として金銭を脅し取ろうとするサイバー攻撃のひとつです。

攻撃者は攻撃の成功率を上げるために、狙った標的を確実に攻撃し、ネットワーク内の端末やサーバーが一斉に攻撃を受け、事業の継続を脅かすような大規模な被害が生じています。（標的型ランサムウェア）

また、攻撃者は、企業・組織が金銭を支払わざるを得ないような状況を作り上げることで、より確実に、かつ高額な身代金を得るために、取得した機密情報を漏洩する被害に発展しています。（暴露型ランサムウェア）

## なぜ被害をうけてしまうのか

Cisco Talos インシデント対応チームでの典型的な対応事例でタイムラインを見てみましょう。攻撃者は通常、標的への侵入、偵察の実施、ログイン情報の窃取、ネットワーク防御の回避など、初期段階にかなりの労力を費やします。ニュースに取り上げられる攻撃の最終段階が注目されがちですが、組織へのランサムウェア攻撃は、攻撃者からすれば長いプロセスの最終段階にすぎません。




**第 1 段階（0 ～ 6 日目）：侵入開始・初期感染**

攻撃者が企業・組織のネットワークへ侵入するとことが攻撃の始まりとなります。

まず最大の侵入の理由となるのは電子メールです（攻撃の始まりはメールから）。マルウェアの配布とフィッシングに最も使われるのは電子メールで（9割を超える）、世の中の流通する85%以上が悪意のあるメールになっています。マルウェア Emotet は、盗んだ電子メールの実際のメッセージの本文を引用し、巧妙に騙す手口で知られています。また、特別定額給付金(10 万円)の受給に関連した攻撃メールなども確認されています。

つぎに悪意のあるサイトへの通信も侵入される理由となり、本物と偽のログインページの違いを見分けるのは非常に困難になっています。シスコの脅威情報においても、マスクが買えるという広告や急増するリモート会議サイトの偽サイトなど、新型コロナに関連する新たなキーワードが出る都度、関連したキーワードの悪質サイトの急増を確認しています。巣ごもり消費も狙われており、オンラインショッピングサイトの偽サイトなども増加し、マルウェア感染や、認証情報、カード情報などを取得しようとします。

そして、コロナ渦で急増するリモートワークに不可欠な VPNや、VNC、RDP、VDI 等のリモートデスクトップも標的となっており、複数の侵害が継続的に観測されています。

# ランサムウエアによるサイバー攻撃について【注意喚起】

Source:内閣サイバーセキュリティセンター
https://www.nisc.go.jp/active/infra/pdf/ransomware20201126.pdf

(1) ランサムウエアの感染を防止するための対応策(予防)
- インターネット公開の必要性を確認する
  - パッチを迅速に適用
  - 不要なポートやプロトコルを外部に開放しない
- リモートアクセス構成製品の迅速なアップデート・適切な設定が行われているか確認する。特にVPN機器の脆弱性等を利用し、組織に侵入する事例が多く確認されていることから、VPN 機器に対するセキュリティ対策の重要性を強く認識し、迅速なセキュリティパッチの適用、VPN 機器やクラウドサービスに対する多要素認証の導入の検討等について、十分留意する
- PC・サーバー等のOS、アプリケーション等が常に最新化されているか確認する。特に、ドメインコントローラーの深刻な脆弱性（CVE-2020-1472）[通称：Zerologon]を悪用し、組織内で侵害範囲を拡大する事例が多く確認されていることから、本脆弱性への対応については、特に留意する
- 必要な機器にウイルス対策ソフトが導入され、パターンファイルが最新化されているか確認する。また、定期的にスキャンが実行される設定になっているか確認する

(2) データの暗号化に備えた対応策(予防)
2重脅迫（暗号化と公開脅迫）に備え「機微データ厳格管理」
- 重要なデータに対する定期的なバックアップ
- 感染時のバックアップの保護（オフライン、アクセス制限等）
- バックアップデータで、実際に復旧できることを確認
- 公開された場合、業務に支障が生じるような機微データや個人情報等に、特別なアクセス制御や暗号化を実施
- システムの再構築を含む復旧計画の適切な策定

(3) 不正アクセスを迅速に検知するための対応策(検知)
迅速な検知を実現するために自動化を検討する必要がある。
- サーバー、ネットワーク機器、PC 等のログの監視を強化
- 振る舞い検知、EDR(Endpoint Detection and Response)、CDM(Continuous Diagnostics and Mitigation)等を活用

(4) 迅速にインシデント対応を行うための対応策(対応・復旧)
冷静で適切な対応・組織一丸となった対処態勢の構築
- データの暗号化及び公開を想定した対処態勢、対処方法、業務継続計画等を含むランサムウエアへの対応計画が適切に策定できているか確認する
- 自組織に携わる職員がランサムウエア感染の兆候を把握した場合、迅速にシステム管理者に連絡できるか確認する

# CDM(Continuous Diagnostics and Mitigation)

https://blogs.cisco.com/tag/continuous-diagnostics-and-mitigation


CDM: the new driver of cybersecurity and IT modernization

CDM: サイバーセキュリティとIT近代化の新たなドライバー

先日、私（Peter Romness）は米国の国会議事堂で、業界、省庁、および国会議員の同僚の多くと一緒に、国土安全保障省の継続的診断・緩和（CDM）プログラムについて議論する機会を得ました。CDM プログラムがフェーズ 3 に入り、連邦ネットワークを守るために協力し合う中で、これらの様々なグループが幅広い支持を得ているのを目の当たりにした


What's all the buzz about integrated, threat-driven CDM?

統合された脅威のCDMがどこが話題になっているのか？

国土安全保障省 (DHS) の継続的診断・緩和 (CDM) プログラムの展開は、政府機関にとってゲームチェンジャーとなっています。フェーズ 3 への移行を開始すると、統合された脅威主導型のセキュリティという新たな機会

CDMは単なるコンプライアンスだけではないです

統合、統合、自動化：CDMにシスコのサイバーソリューションが不可欠な理由

連邦政府のサイバーセキュリティはますます複雑になり、国の重要なサイバー弱点を修正するために、ポイント・イン・タイムの監視から、より継続的なアプローチへと移行しています。

国土安全保障省（DHS）は、継続的な監視を通じてサイバー防御を強化するために、継続的な診断と緩和（CDM）プログラムを開発しました。

継続的なモニタリングは、ポイント・イン・タイムのモニタリングとは異なり、応答時間を改善し、脅威の可視性を高め、ダウンタイムを短縮します。

CDMプログラムでは、継続的な診断能力を拡大するために、攻撃の連続体にわたってさまざまなソリューションを導入することを機関に求めています。

https://www.cisco.com/c/m/en_us/solutions/industries/government/cdm-phase-3-cybersecurity.html

# Where Cisco fits in CDM Phase 3

Primary Secondary

| Cisco Products | | How is the network protected? | What is happening on the Network? | | | Form Factor |
|---|---|---|---|---|---|---|
| | | Boundary Protection | Manage Events | Operate, Monitor, and Improve | Design and Built-in Security | |
| Network Security Products | Route/Switch (LAN) | ✓ | | | ✓ | P |
| | SD-WAN | ✓ | | | ✓ | P/V |
| | ESA/WSA | ✓ | | ✓ | ✓ | P/V |
| | FTD/NGFW/NGIPS | ✓ | ✓ | ✓ | ✓ | P/V/C |
| | ISE/TrustSec | ✓ | ✓ | ✓ | ✓ | P/V |
| | SW | ✓ | ✓ | | ✓ | P/V/C |
| | AMP/TG | ✓ | | ✓ | ✓ | P/S/C |
| | Meraki | ✓ | ✓ | ✓ | ✓ | P/C |
| | AC | ✓ | | ✓ | ✓ | S |
| | Umbrella | ✓ | ✓ | ✓ | ✓ | C |
| | Cloudlock | ✓ | ✓ | | ✓ | C |
| | ETA | ✓ | | ✓ | ✓ | C |
| Management | FMC/PI/Cisco DNA Center | ✓ | ✓ | ✓ | ✓ | P/V/S |
| | pxGrid | ✓ | ✓ | ✓ | ✓ | S |
| Threat Intelligence | CTA | ✓ | ✓ | | ✓ | C |
| | Talos | ✓ | ✓ | | ✓ | C |

# 他人事ではない！
# ランサムウェアの脅威とその対策について

- ランサムウェアの脅威とは
- なぜ被害をうけてしまうのか
- どうすれば防ぐことができるか
- シスコは何をお手伝いできるか
- 付録（各対策ハイライト）

# シスコがお手伝いできること

CISCO SECURITY

セキュリティ対策

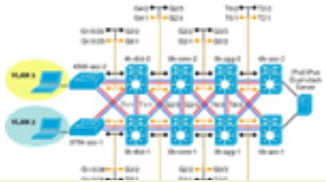

ビジネスの継続

## 世界最大級の分析能力 脅威トレンド

TALOS

先進的な脅威情報を提供する
専門家集団
圧倒的な情報量の収集/分析
による可視性
シスコ サイバーセキュリティ
レポート シリーズ

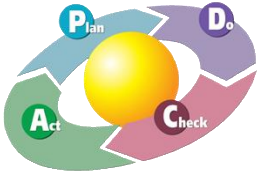
## 製品・テクノロジー



ネットワーク
次世代ファイアウォール
メール対策
未知マルウェア対策
クラウド セキュリティ
VPNクライアント

多要素認証
機械学習・人工知能
業界標準
連携による検出と封じ込め
ゼロトラスト/SASE
IoT

## サービス




SOC
IR(インシデントレスポンス)
アドバイザリ
サイバー訓練
実装支援、最適化

TALOS







TALOS Japan

Talos は、ネットワーク脅威の専門家集団です。Talos が提供する脅威インテリジェンスの情報は、既知および未知の脅威からお客様のネットワークを保護するためにシスコのセキュリティ製品によって活用されています。

2020年11月20日

Leave a Comment


セキュリティ

# シスコ、内閣サイバーセキュリティセンターとサイバーセキュリティ分野の連携を延長

Press Release

## シスコ、内閣サイバーセキュリティセンターとサイバーセキュリティ分野における連携・協力を延長

シスコシステムズ合同会社（本社: 東京都港区、代表執行役員社長: デイヴ・ウェスト、以下 シスコ）は、内閣サイバーセキュリティセンター（以下NISC）と締結済みのサイバーセキュリティ分野における連携・協力に関する基本合意書の有効期間を、2021年12月31日まで延長しました。

本合意書は、2018年12月18日に締結し、2020年12月31日までを有効期限としていました。この度の延長で、シスコがNISCにサイバーセキュリティ分野の脅威情報等を引き続き無償で提供することにより、連携・協力関係がさらに強化されることになります。

シスコは今後も、NISCの取り組みに貢献し、安心・安全なインターネット環境の実現に寄与してまいります。

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

| | | | | |
|---|---|---|---|---|
| 教育 | セキュリティ | Cisco Duo Security | デューク大学<br>米国の名門私立大学が、Cisco Duo の導入により、高い柔軟性と信頼性を備えた多要素認証を実現 | 2020年6月 |
| 情報通信/メディア | セキュリティ | Cisco Umbrella<br>Cisco AMP for Endpoint<br>Cisco Threat Response | 静新 SBS グループ<br>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<br>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<br>Cisco ASA 5500 シリーズ<br>Cisco Telepresence SX, DX シリーズ | 前橋赤十字病院<br>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 | 2019年10月 |
| サービス業 | セキュリティ | Cisco Umbrella | SCSK 株式会社<br>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<br>Cisco Umbrella | 株式会社エス・エム・エス<br>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<br>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ています

# 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

「 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。」

課題:
- スパムメール、フィッシングなどの迷惑メール対策

ソリューションと効果: **Ciscoクラウド E メールセキュリティ**
- 初期設定のレピュテーションフィルタリングの検知精度の高さ
- 管理画面のわかりやすさとユーザー登録作業不要の利便性
- 安全性とコストパフォーマンスの両立

結果～今後:
- 正確な検知で隔離通知が 1/10 程度に減少、業務効率が大きく向上
- 展開時に管理側、ユーザー側からの問い合わせもなく安心
- 学生が自身のデバイスを安全、自由に活用できる環境作り
- AI 、機械学習のためのクラウド利活用

国立大学法人 北見工業大学 様



https://www.cisco.com/c/ja_jp/about/case-studies-customer-success-stories/2114-kitami-it.html

# 教員と児童生徒の PC を未知の脅威から守るため クラウドと連携するマルウェア対策ソフトを導入

「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。」

課題:

- 教職員および児童生徒が利用する PC 端末に対する、マルウェア感染へのより強固な対策
- シグネチャを用いるウイルス対策製品では検知できない標的型攻撃やゼロデイ攻撃への対策

ソリューションと効果: **Cisco EDR AMP for End Points**

- クラウド上のセキュリティ基盤と連携して世界トップの検知率を持つ Cisco AMP を導入し、PC 端末のマルウェア対策を強化

結果～今後:

- PC を安全に利用できる環境を維持し、ICT を活用した教育を市内の小中学校で展開
- 教職員のセキュリティに対する意識を高め、児童生徒の模範となるよう努める

佐賀市教育委員会 様



https://www.cisco.com/c/ja_jp/about/case-studies-customer-success-stories/1268-sagashi.html

# 画期的なコンセプトを持つセキュア インターネット ゲートウェイ「Cisco Umbrella」の導入が低コスト、低負荷で高いセキュリティレベルを実現

「既存システム変更が少ないこと、導入負荷が少ないこと、導入後の管理負荷が軽いこと、エンドユーザに特別な教育が不要でさらには導入したことを意識する必要がないこと、そして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。」

課題:

- マルウェア、DNS トンネリングといった攻撃に対しては、既存のシステムでは対処が難しかった

ソリューションと効果: **Cisco Umbrella**

- DNS のレイヤーでセキュリティ対策ができるセキュア インターネット ゲートウェイ「Cisco Umbrella」の導入

結果～今後:

- トライアル環境のまま本番導入ができたため、簡単かつ最小限のスタッフと工数で導入を実現した


株式会社光文社 様



https://www.cisco.com/c/ja_jp/about/case-studies-customer-success-stories/1440-kobunsha.html

# 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

# 医療機関を標的とするランサムウェアへの対抗や管理されていなかった医療機器の特定に貢献

「Stealthwatch は、私のネットワーク上のトラフィックが何を、どのように、どこで行われているかのスナップショットを提供してくれるので、とても気に入っています。」

課題:

- 医療機関を標的とするランサムウェアが急増しており、患者の個人情報や医療記録が狙われ、患者受け入れや迅速な治療の脅威となっている
- ランサムウェアに対する防御に加えて、これまで管理されていなかった医療機器の特定や、侵害されたデバイスの発見などに課題があった

ソリューションと効果: **Cisco Stealthwatch**

- 侵害されたデバイスからの不正スキャンを検出
- 未知のデバイスからのスキャンを検出
- カウントされていなかった医療機器の特定
- ランサムウェアの調査に協力
- 重要かつ脆弱なものを継続的に監視に優れている


モンテフィオーレ・メディカル・センター 様



https://www.techvalidate.com/product-research/cisco-stealth-watch/case-studies/CB1-23C-570

# マルチクラウド利用におけるセキュリティ統制を実現

詳しくはこちら


マルチクラウドを使用する ADP 社

ADP 社の最高セキュリティ責任者である Roland Coultier 氏が、Tetration によるワークロード保護とマイクロ セグメンテーションの管理について話します。

## 課題

- ハイブリッドクラウド全体を統制可能なセキュリティ管理モデルを検討していた
- 従来型のFirewallでの集中制御は現実的ではない
- アプリ動作を把握し、全体にセキュリティ統制を利かすことに課題があった
- GDPR:データフローマッピング、セキュリティ機能の組み込みへの課題

## ソリューションと効果

- 14のDCとAWSに存在する70000台のサーバのサーバ間通信の可視化とマイクロセグメンテーションの実施
- **Cisco Tetration** によるアプリ毎のポリシー可視化と一元管理
- サーバでのホワイトリスト強制によるゼロトラストモデルを実践
- AWS上へのサーバへも同一管理モデルを適用

*”Tetrationのメリットはっきりしています:*

- *組織がより積極的になります*
- *市場投入までの時間を短縮*
- *セキュリティ製品と技術のマルチクラウド統合*
- *Cisco Tetration は堅牢で非常に展開しやすい技術です“*

# Cisco EDR AMP for End Points
# 優れた脅威検出技術

- エクスプロイト防止機能
- システムプロセス保護機能
- 1:1 SHA マッチングエンジン
- Tetra ウイルス対策
- Threat Grid サンドボックス
- ETHOS ファジー シグニチャ アルゴリズム
- SPERO 機械学習
- クラウド上の侵入の痕跡およびレピュテーション分析
- [illegible]
- [illegible]スクリプト/変換保護
- 脆弱性のあるソフトウェア
- Cognitive Threat Analytics（CTA）
- カスタムハッシュ検出
- ClamAV シグネチャ
- アプリケーションブロック

- AMPは競合他社と比較して検出技術の数が多い。
- その結果は第三者機関による評価にも現れている。



## 高い防御率と低い誤検知率

AV comparatives APPROVED Business Security DEC 2019

| | Protection Rate | False Alarms |
|---|---|---|
| Malware Protection Test | 100% | 0 |
| Real World Protection Test | 99.3% | 1 |

**False Alarm Test**

- “Very High” FP has as many as 100-150 false positives

| | FP rate on non-business software |
|---|---|
| Acronis, Avast, Bitdefender, Cisco, ESET, Fortinet, G Data, Kaspersky, Sophos | Very low |
| Cybereason, FireEye, SparkCognition, Microsoft | Low |
| Elastic, Vipre, VMware | Medium |
| K7, Panda | High |
| CrowdStrike | Very high |

Factsheet Business Test (March-April 2020), go to: https://www.av-comparatives.org/tests/business-security-test-march-april-2020-factsheet/

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結果

**AV-TEST によるセキュリティの有効性評価で、Cisco Umbrella が 1 位に再び選出！**
https://gblogs.cisco.com/jp/2020/11/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

# CRN Tech Innovator アワードの最優秀賞を獲得

https://gblogs.cisco.com/jp/2020/11/cisco-umbrella-named-best-cloud-security-solution-by-crn-tech-innovator/

zzfeatured

## Cisco Umbrella が CRN Tech Innovator アワードのクラウド セキュリティ ソリューション分野で最優秀賞を獲得

坂川 健太
2020年11月26日

この記事は、*Kate MacLean* によるブログ「*Cisco Umbrella named best cloud security solution by CRN Tech Innovator*」（*2020/11/12*）の抄訳です。

シスコは、クラウドセキュリティ、SASE、脅威インテリジェンス/インシデント対応などの主要な 3 つの分野で、Cisco Secure が CRN Tech Innovator アワードを受賞したことをお知らせします。真に差別化されたサービスでソリューションプロバイダーをサポートできる点が評価され、2020 年度 CRN Tech Innovator アワードで最終選考に残り、最優秀賞を受賞しました。

クラウド セキュリティ ソリューション分野で最優秀賞を獲得した Cisco Umbrella は、ネットワークのセキュリティを容易に確保できるクラウド提供型のセキュリティサービスとして、インターネットへのアクセスを保護し、ネットワーク、ブランチオフィス、ローミングユーザのすべてを対象に、クラウドアプリケーションの利用を制御しています。Umbrella は、DNS レイヤ保護、セキュア Web ゲートウェイ、ファイアウォール、クラウド アクセス セキュリティ ブローカ（CASB）機能を 1 つに統合し、リモートユーザ/ローミングユーザの保護、セキュアな SD-WAN、ダイレクト インターネット アクセスを容易に実現します。遅延が発生することはありません。復元力の高いクラウド インフラストラクチャとして、1,000 を超える世界トップクラスのインターネット サービス プロバイダー（ISP）、コンテンツ配信ネットワーク（CDN）、SaaS プラットフォームと直接連携します。

**2020 Tech Innovators Details**

« Previous | Tech Innovators 2020 Home | Next »

**Cisco**

**Cisco Umbrella**

***Winner** -- Security - Cloud*

**2020 Tech Innovators Details**

« Previous | Tech Innovators 2020 Home | Next »

**Cisco**

**Cisco SASE Solution**

***Winner** -- Networking - SD-WAN*

**2020 Tech Innovators Details**

« Previous | Tech Innovators 2020 Home | Next »

**Cisco**

**Cisco SecureX**

***Winner** -- Security - Threat Intelligence / Incident Response*

https://www.crn.com/rankings-and-lists/ti2020.htm

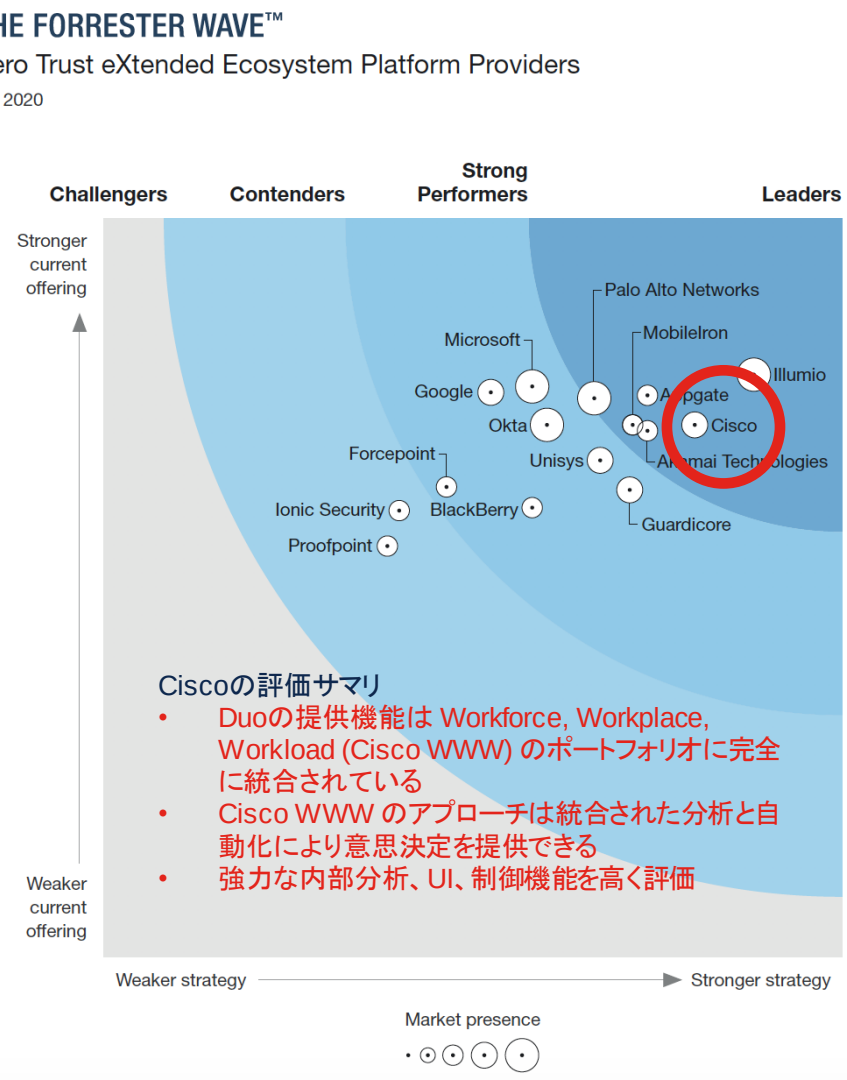
CRN Tech Innovator アワードは、IT 分野における最も画期的な製品およびサービスを称えるものです。

# Cisco is a leader in Zero Trust

**The Forrester Wave™:**
Zero Trust eXtended Ecosystem Platform Providers, Q3 2020

ForresterWaveは、
Forresterの市場へ適合性をグラフィカルに示し、スコア、重み付け、コメントが公開された詳細スプレッドシートにプロットされます。
Forrester Waveに記載されているベンダー、製品、またはサービスの情報は利用可能なリソースに基づいています。

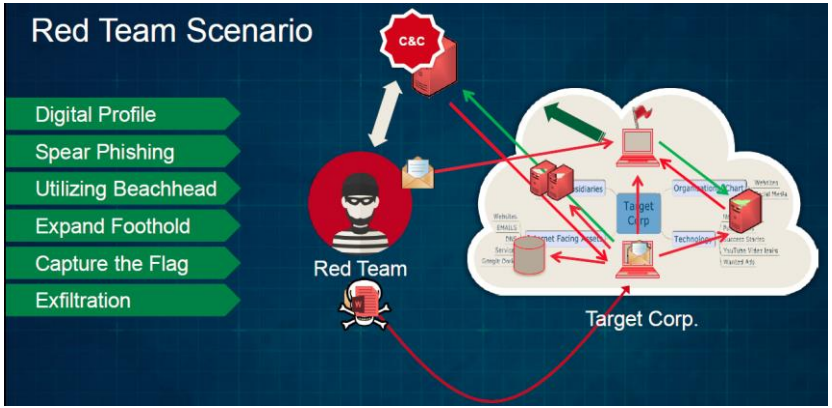




# ランサムウェア等を仕掛ける攻撃者と同様の手段で狙われたとき大丈夫かどうかを評価するサービス

- 標的型攻撃・侵入の専門家（Redチーム）が、実在するサイバー犯罪者と同様の手段の攻撃手法により、**潜在的な脅威を顕在化させる**サービス

  （注意：擬似的な攻撃ではなく、**実際に専門家が攻撃を仕掛けます**）
- Redチームは、貴社の機密データ窃取等のゴールを達成するために最先端の技術で複数の侵入・攻撃手法を試みます
- 貴社環境への不正侵入の突破口・貴社内部における不正な活動・機密データ窃取等における**攻撃手法を、サイバー犯罪者の視点に立って、識別および顕在化**させます

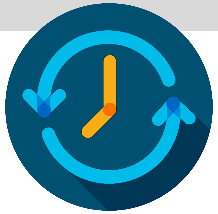


# 対応と予防：インシデントレスポンス(IR)サービス

## インシデントレスポンスリテーナー(年間契約)

### エマージェンシー インシデントレスポンス

IRへ向けて、
今サポートが必要



現在進行している
インシデントに対しての
緊急サポート対応

### プロアクティブ スレットハンティング

自社は既に
インシデントが
起こっているのか？

攻撃者が攻撃ターゲットを定めた時から開始される偵察行為など（サイバーキルチェーン初期）の段階から、兆候を察知する分析活動を行います

### IR テーブルトップ エクササイズ

有事の際、自社の
IR体制は想定通り
機能するのか？

いざ有事の際に想定通りのIR対応が可能かどうか対処訓練をサポート

### IR 態勢現状分析

IR対応にて何か不足や
課題は無いのか？

サービス・人・プロセス・テクノロジの観点から現状分析・ Gap分析・改善へ向けた施策提案を行う
ベストプラクティス等を参照し評価を行う

# まとめ

## 基本的なセキュリティ対策の徹底

- 「平易なパスワードを使わない・使いまわしをしない」「OS・アプリ・リモートアクセス環境・セキュリティソフトなど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・URLリンクをクリックしない」「不要なサービスを公開しない」「データの暗号化に備えた対応策」「迅速にインシデント対応を行うための対応策・迅速にシステム管理者に連絡する」などの基本的な対策の徹底が基本となります

## 今必要な対策の導入を検討する

- 攻撃者は目立たないように活動し、時事情報を巧妙に活用し、被害が拡大しており、目的を果たすまで執拗にあの手この手と手段を変え攻撃を継続します
- リモートワークは特に狙われており、多要素認証やクラウド・セキュリティ対策への対応が重要度が高いです。
- 不正アクセスを迅速に検知するための対応策として、振る舞い検知・EDR・継続的な監視などのセキュリティ対策手法の導入を検討することも推奨されています。

**“Never Trust” + “Always Verify” ゼロトラスト**

## シスコがお手伝いいたします

- シスコはセキュリティ研究機関Talos各種ブログ情報提供や、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、ランサムウェアも含む多様な脅威へ「事前対応」「予防」「インシデント対応」など幅広くをお手伝いさせていただきます

# ブログのご紹介

## 西 豪宏

Systems Manager
Security Sales

国内大手キャリア・SI でのプリセールス SE を経験後、2000 年にシスコに入社。
お客様担当 SE、セキュリティ SEなどを経験し、現在はセキュリティ事業の SI マネージャに従事している。

記事


セキュリティ
マシンラーニングで守るセキュリティ対策とは

西 豪宏 - 2020年9月14日 - 0 コメント

セキュリティ脅威は日々絶えることなく世界中で増加しつつ高度化しています。 情報漏えいが発生した場合、多大な被害コストが想定され、リモートワークに欠かせないVPN終端装置やVDIサーバへの攻撃の増加も発生しています。 シスコがOEMで提供するラドウェア社によるマシンラーニングを活用したユニークなアーキテクチャで守るセキュリティ対策をご説明いたします。

続きを読む>

不正送金
DDoS保護


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 - 0 コメント

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。 ご提供中であるリモートワークに有効な3つのセキュリティ（Umbrella, Duo, AnyConnect）に加えて、マルウェア（ウイルス）の感染防止のためのマルウェア対策・ウイルス対策ソフトとして、エンドポイントセキュリティの提供概要とその特徴についてご紹介いたします。

EDR


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 - 0 コメント

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。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。

テレワーク


セキュリティ
マルウェア Emotet の 脅威と対応策

西 豪宏 - 2019年12月4日 - 0 コメント

シスコのセキュリティ研究機関であるTalosブログにおいて、2019年9月16日の時点でマルウェアEmotetの活動再開を確認したことが投稿されてから、国内においてもマルウェアEmotetに関する感染被害などの報道が増えています。本ブログでは、Emotetについての情報とその対策について記載いたします。

Emotet対策

## 木村 滋

2000 年シスコシステムズ入社。テクニカルアーキテクト/エバンジェリスト。セキュリティ ソリューション専任技術担当として、大手データセンター/キャリアビジネスのプロジェクトをサポート。データセンター/VDI/デスクトップ仮想化/ネットワーク仮想化に従事、普及活動、ソリューション開発を担当
CCIE#19521
著書：「Cisco ISR ルータ教科書」、「Cisco WAN 実践ケーススタディ」、「実践Cisco IPSec VPN 教科書」等
NPO法人日本ネットワークセキュリティ協会（JNSA）幹事


セキュリティ
ゼロトラスト考察 – Forrester Zero Trust eXtended (ZTX)

木村 滋 - 2020年7月15日 - 0 コメント

「ゼロトラスト」というキーワード自体の生みの親である Forrester Research, Inc による「Forrester Zero Trust eXtended (ZTX) 」の情報、さらに先日（2020/7/8）オンラインセミナーとして開催されました、Cisco Secure Insights Summitの登壇者でありゼロトラストの提唱者である、Dr. Chase Cunningham 氏による講演内容を基に理解を広げていきたいと思います。

ゼロトラスト

cisco Secure

Cisco Secure、全世界で提供開始

木村 滋 - 2020年8月31日 - 0 コメント

発表以来大反響の新プラットフォーム、「Cisco SecureX」の提供を開始しました。「Cisco Secure」はシンプルで、本物で、新たなセキュリティの概念の出発点です。ソリューションであり、お客様が求める機能を表す製品名であり、総力をあげて効果的なセキュリティを提供していくためのビジョンでもあります。お客様のユーザエクスペリエンスをシンプルにし、成功を加速させ、現在そして未来に必要なセキュリティを実現するもの、それが Cisco Secure なのです。

SecureX

セキュリティ
Duo Security でWebex (Meetings, Teams) の “なりすまし” を防止

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

多要素認証

セキュリティ
シスコがセキュア アクセス サービスエッジへの 架け橋を築く

坂川 健太 - 2020年6月11日 - 0 コメント

マルチクラウドへの移行でワークフォースの分散化が進むことにより、アプリケーションを安全かつ最適なパフォーマンスで利用できることが求められてきています。こうした環境下、企業の間ではSD-WANの導入が急速に広まっており、キャンパスからクラウド、エッジに至るまで、アクセス

SASE

セキュリティ
多層防御を実現する Cisco Eメール セキュリティ！

國分 直晃 - 2020年9月1日 - 0 コメント

今も昔も攻撃を開始する時の入り口として一番多く利用されているのは電子メールを使った攻撃です。シスコ提供のセキュリティインテリジェンス、Talos調べでは2020年7月のスパムメール割合は約85%でした。時事ネタを使ったフィッシング攻撃も増加の一方です。そのような状況下再度

メール対策

セキュリティ
Firepower 6.6 の新機能と改良点 (その1)

小林 達哉 - 2020年7月15日 - 0 コメント

シスコの NGIPS / Anti-Malware 製品である Cisco Firepower、およびその Firepower にベーシック Firewall & VPN 終端装置である Cisco ASA の機能を包含した NGFW 製品である Firepower Threat Defense (FTD) のソフトウェアバージョン 6.6 。全4回に分けて、バージョン 6.6 の代表的な

次世代FW

セキュリティ
サプライチェーンセキュリティへの対応

浅井 達也 - 2020年9月2日 - 0 コメント

サイバー犯罪でターゲットにされるのは大企業も中小企業も同じで、連携する組織間でセキュリティ対策レベルが低いところが狙われています。業務委託先に対してもセキュリティの徹底を求め、ビジネスパートナーと連携したサプライチェーンセキュリティ対策を講じていくことが重要視されています。シスコはサプライチェーンセキュリティの向上に取り組む中小

サプライ
チェーン対策

セキュリティ
実践セキュアリモートワーク – AnyConnectトラフィックデザイン

稲澤 敏 - 2020年6月24日 - 0 コメント

パンデミックな状況の中で社員が安全に業務を継続するための一つの手段として、リモートワークの重要性はこれまで以上に高まっており、VPNを活用した既存リモートワーク環境の拡張や新規の構築などを実施・検討されている企業様は多いと思います。社員が自宅や社外から安全な環境で快

リモートアクセス


セキュリティ
暗号化されたトラフィックに潜む脅威

大野 由貴 - 2020年2月5日 - 0 コメント

パスワード認証やクレジットカード取引などのセンシティブデータが関わる場合、通信内容が漏れてしまっては問題になります。こうした背景があってトラフィックの暗号化が開発され、通信が保護される時代へと至った今、階層型アプローチを実装し、さまざまな手口に対応できる態勢を整

暗号化脅威

毎週木曜日 は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

担当営業トライアルや詳細に関して
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

**ウェビナー開催(2020/12/4) : 【緊急開催】ランサムウェアの脅威と対応について**

**ウェビナー開催(2020/12/17) : さよならパスワード次の時代のセキュリティとは？**



Cisco Japan Blog > セキュリティ

セキュリティ

他人事ではない！ ランサムウェアの脅威とその対策について

西 豪宏
2020年11月25日

コロナ禍につけ込んだサイバー犯罪が増加の一途を辿っている中、Snake, Ragnar Locker などのランサムウェアと呼ばれる脅威と被害が拡大しています。

攻撃者は盗み出したデータを人質に取り、ビットコインなどで身代金（ransom、ランサム）を支払わないとデータを「晒す」と脅迫し、これを支払わなければ機密情報を暴露されるという被害に発展する事例が増えています。

シスコは昨今のランサムウェアの被害拡大を踏まえ、ウェビナーを緊急開催予定です。

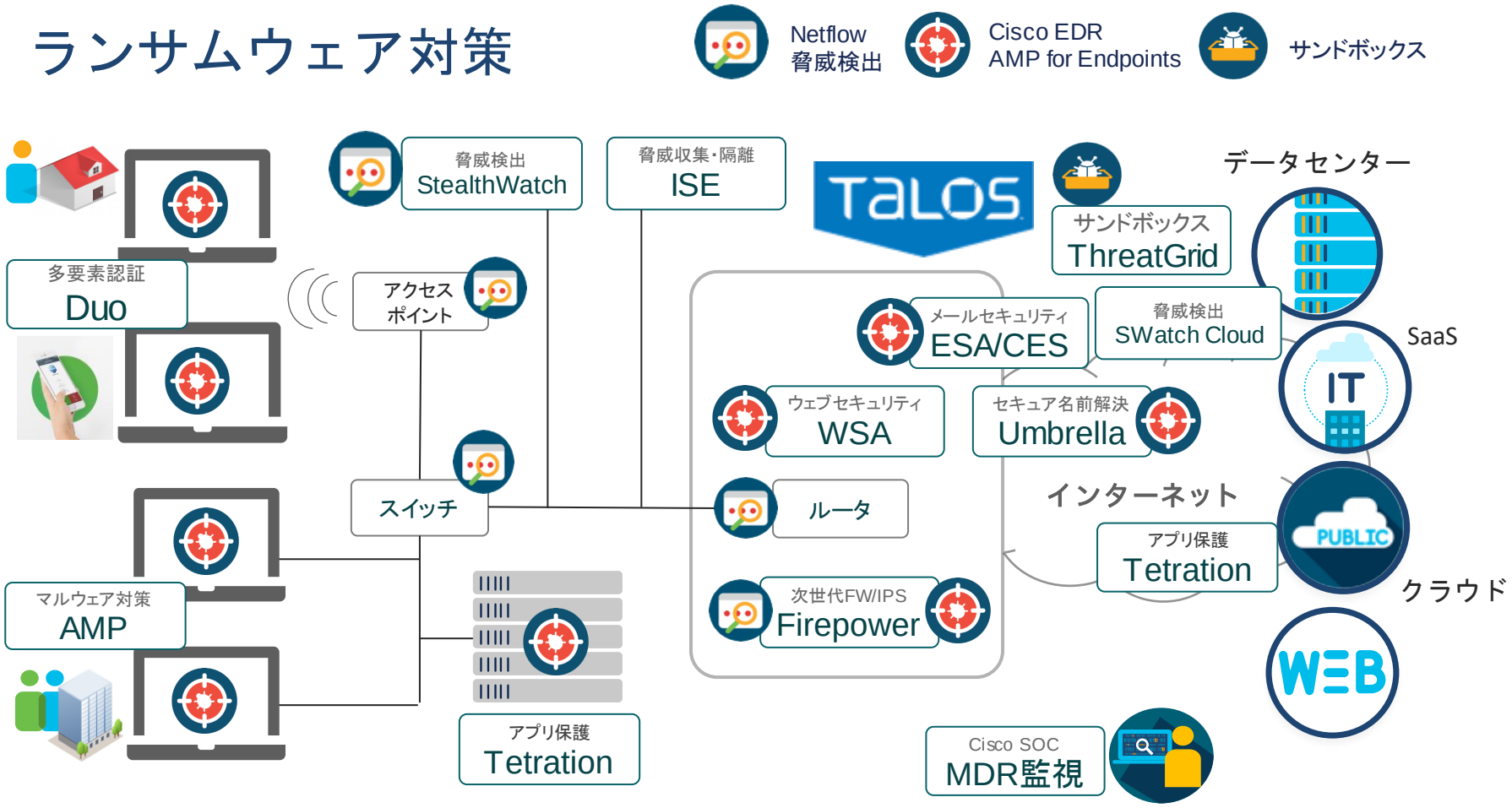
本ブログとウェブセミナーでは、ランサムウェアの脅威は何なのかにはじまり、なぜ被害をうけてしまうのかという原因と、どうすれば防ぐことができたのかに関して Cisco Talos インシデント対応チームの対応事例なども踏まえ、対策のポイントをわかりやすく解説いたします。

https://gblogs.cisco.com/jp/2020/11/ransomware_defense/

# 他人事ではない！
# ランサムウェアの脅威とその対策について

- ランサムウェアの脅威とは
- なぜ被害をうけてしまうのか
- どうすれば防ぐことができるか
- シスコは何をお手伝いできるか
- 付録（各対策ハイライト）

# ランサムウェア対策



# Why Cisco セキュリティ

安全なリモートアクセスVPN

## Cisco AnyConnect

- 長年利用されている実績と導入数
- ボトルネックが発生しないセキュア リモート アクセス
- 幅広い端末に対応・接続前にデバイスの安全性を確認
- 自動VPN接続（Always-On機能）、対象通信判定（Dynamic Split Tunneling）

クラウド セキュリティ

## 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と低い誤検知率（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
- 低遅延、高パフォーマンスかつ堅牢なサービス

ゼロトラスト/多要素認証

## Cisco Duo Security

- 学術機関なども含むで多数お客様での利用実績
- 広範囲なアプリケーション連携（Webex、Shibboleth、RDP、SSH、VPN）
- 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、デバイス可視化と継続的監視・MDM連携

マルウェア対策・EDR

## 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）
- 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
- 高い防御率と低い誤検知率を兼ね備える第三者機関の評価

メール セキュリティ

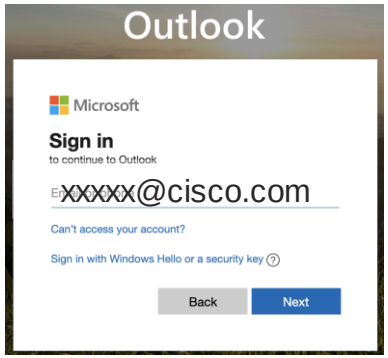
## Cisco ESA/CES

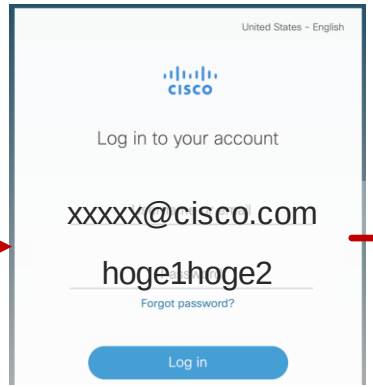
- 世界中のメールの約35%をモニターして脅威に対抗
- 長年利用されている実績と導入数、検知精度率の高さ
- アプライアンス・仮想版・クラウド環境に対応
- O365環境の脅威確認と連携

# 多要素認証で侵入を防御・端末の健全性を確認

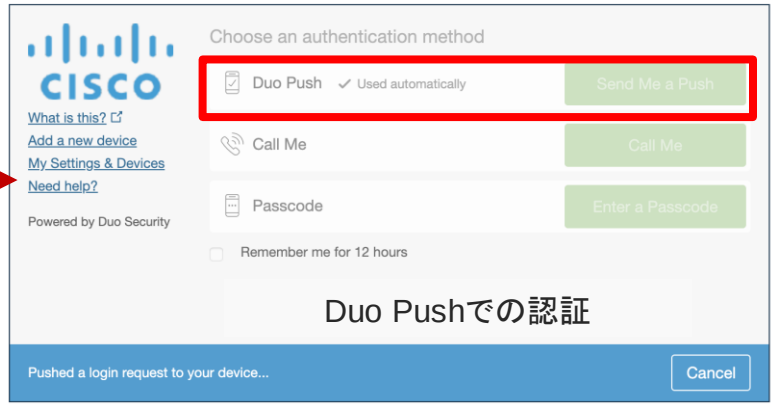
多要素認証
Duo

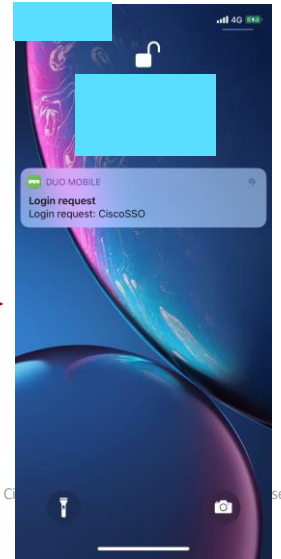
https://outlook.office.com/



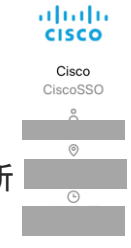



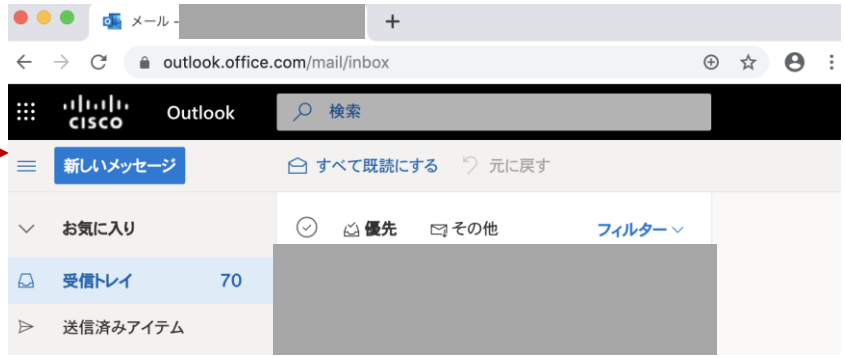

Two-Factor Authentication







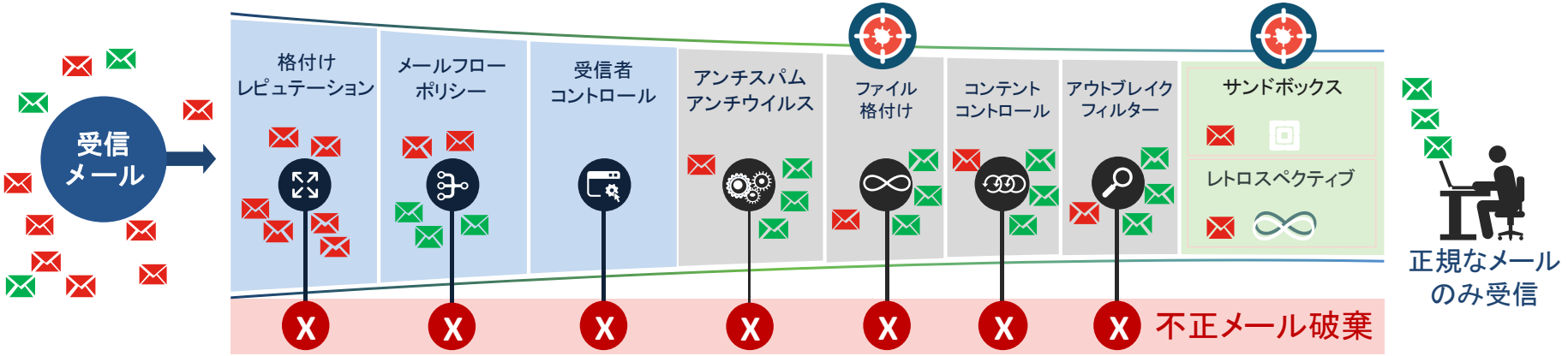




# 攻撃の始まりはメールから
# 標的型メールを破棄

Eメールセキュリティ
アプライアンス

クラウドEメール
セキュリティ

メールセキュリティ
ESA/CES




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

# マルウェア感染の防止
# 侵入経路・拡散範囲の把握

マルウェア対策 AMP

サンドボックス ThreatGrid

主にファイルレス・ランサム等正規ツール悪用型振る舞い・ヒューリスティック・マシーンラーニング・メモリプロテクション

未知

継続モニタリング(ファイル、プロセス、ネットワーク)、IOC、ダンプ、サンドボックス、ホワイト・ブラックリスト、相関分析、隔離と修正

NGAV(NGEPP)
知らないモノを止める

保護

応答

EDR
被害を最小限で食い止める

主にウイルス・ワーム・トロイの木馬等
シグネチャ、ハッシュ検査

AV(EPP)
知ってるモノを止める

すり抜けたマルウェア(ゼロデイ)
侵入経路、感染端末の動作

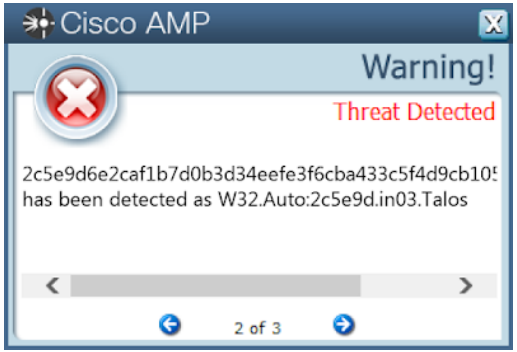
既知

EPP:エンドポイント保護プラットフォーム

EDR:エンドポイント検出および応答

AV:アンチウィルス・NGAV:次世代アンチウィルス


どこまで感染しているかを(範囲)特定
いつどうやって感染したかを(原因)特定




脅威を検出してブロック

# Cisco AMPのEDR機能における充足性

Cisco EDR
AMP for Endpoints
サンドボックス

EDRはエンドポイントシステムレベルの動作を記録・保存し、さまざまなデータ分析技術を使用して疑わしいシステムの動作を検出し、コンテキスト情報を提供し、悪意のある活動をブロックし、影響を受けたシステムを復元するための改善提案を提供するソリューションと定義されています。
EDR ソリューションは、以下の 4 つの主要な機能を提供する必要があります。

## EDRに必要な4つの機能

- セキュリティインシデントの検出
- エンドポイントでのインシデントの抑制
- セキュリティインシデントの調査
- 是正処置のガイダンスの提供
- アーキテクチャ

## Cisco AMPの実装機能

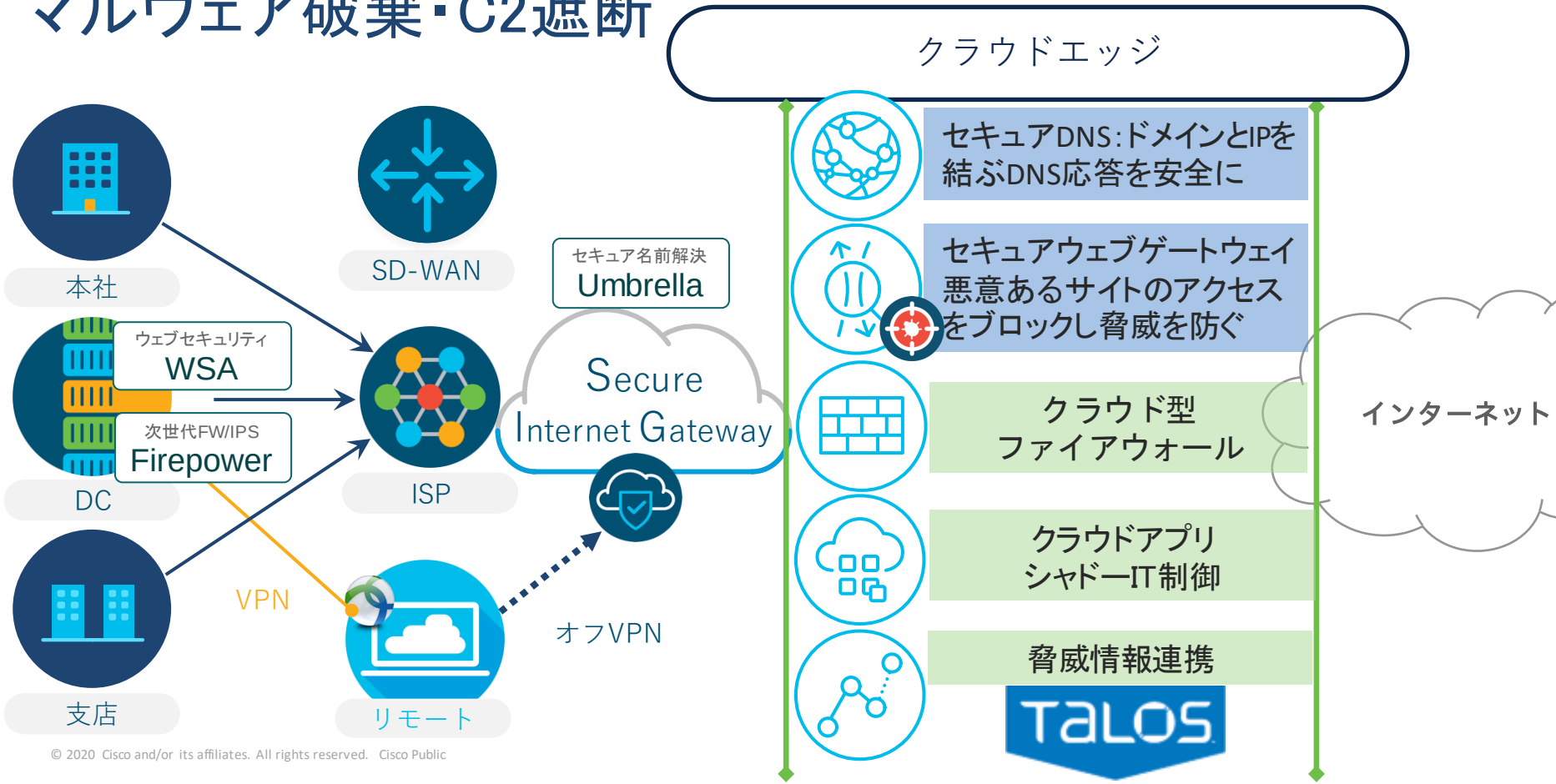
- セキュリティインシデントの検出
  - 15の検出技術
  - 継続的分析
  - レトロスペクティブ
  - サンドボックス
  - デバイストラジェクトリ
  - ファイルトラジェクトリ
- エンドポイントでのインシデントの抑制
  - ホワイトリスト
  - ブラックリスト
  - ソフトウェアの脆弱性
  - 高度な脅威からの保護
  - サンドボックス認識型マルウェアからの保護
- セキュリティインシデントの調査
  - 高度な検出(Orbital)
  - カスタム検出
  - ファイルの検索およびフェッチ
  - あらゆる脅威媒体にわたる広範な脅威情報
- 是正処置のガイダンスの提供
  - マルウェアの自動修復
  - マルウェアのゲートウェイの判定
  - 脆弱なアプリケーションの可視性
  - DNS レベルの統合型保護
- アーキテクチャ
  - オペレーティングシステムの網羅性
  - オンプレ/クラウド対応
  - AMP Everywhere
  - Cisco Threat Response
  - SecureX
  - Cisco Talos

競合他社では未実装、もしくは限定的実装

競合他社でも同等の機能を実装

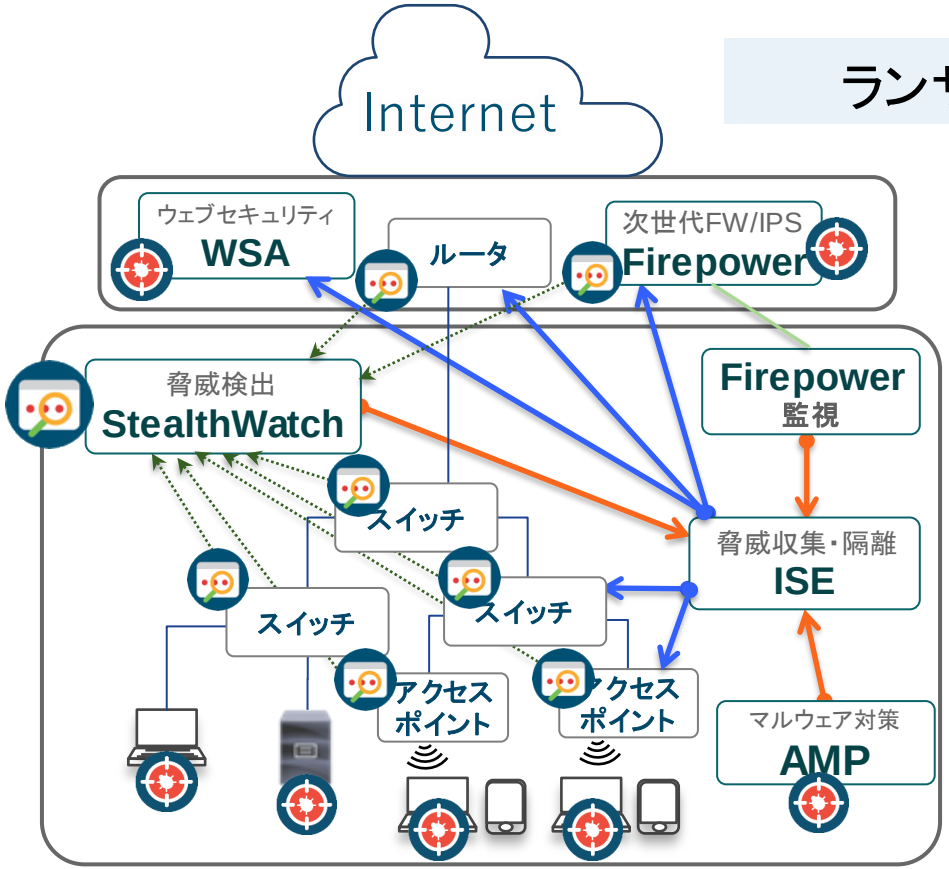
# 悪意のあるサイトのアクセス防止
# マルウェア破棄・C2遮断

ウェブセキュリティ WSA
次世代FW/IPS Firepower
セキュア名前解決 Umbrella

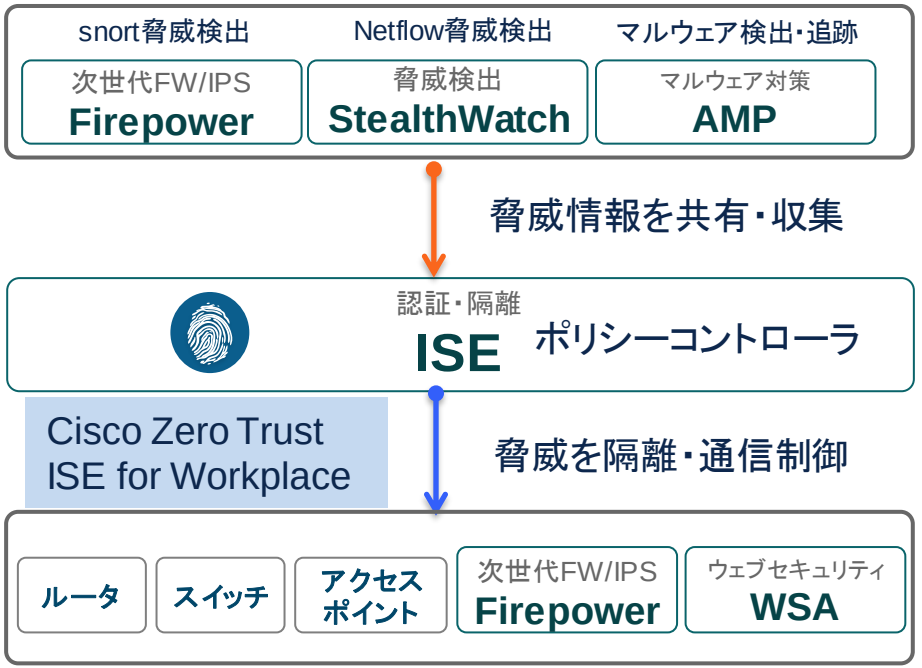


# 偵察・感染拡大・C2通信の検出と遮断

脅威検出 StealthWatch | 脅威検出 SWatch Cloud | 脅威収集・隔離 ISE




## ランサムウェア脅威をネットワークで隔離

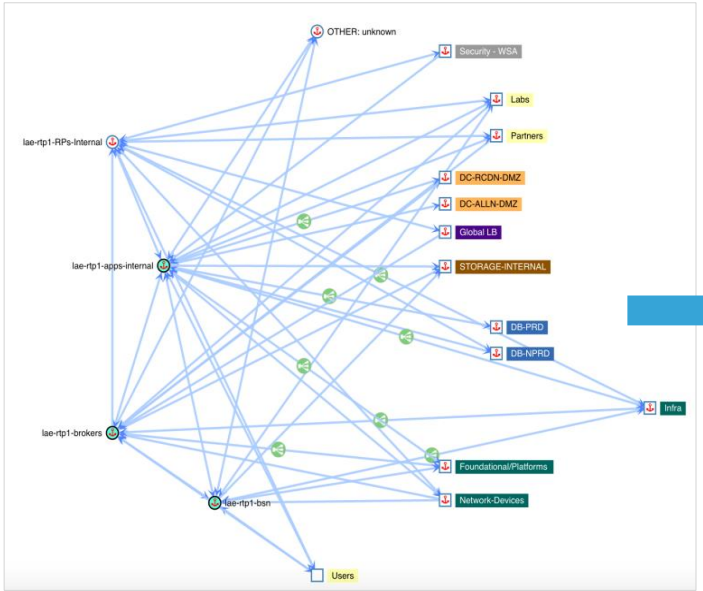


アプリ保護
Tetration

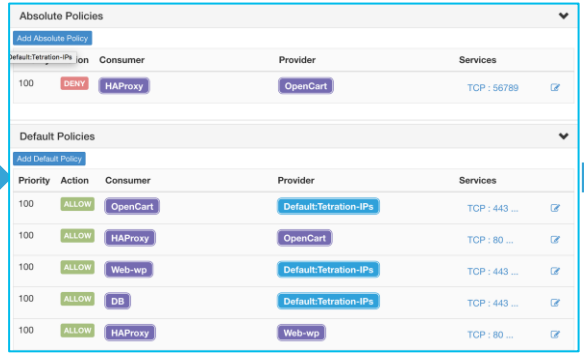
# ホワイトリスト保護で感染の未然防止

データセンター・クラウドで稼働しているものの理解と堅牢化

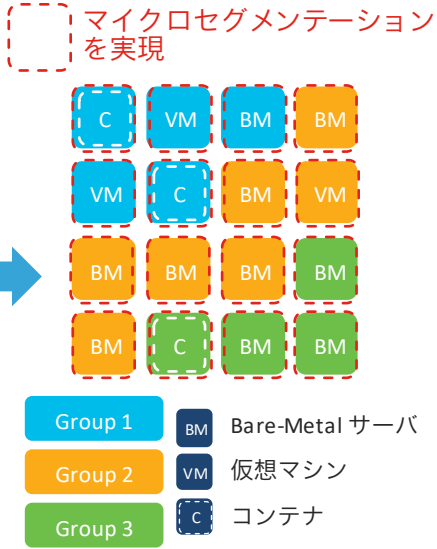
## 自動アプリ依存関係検出




## 自動ホワイトリストポリシー




## ルールセット適用




Cisco Zero Trust
Tetration for Workload

# 監視:Cisco MDR サービス

MDR

Cisco SOAR
(Security Orchestration Automation and Response)

Cisco MDR
プラットフォーム

TALOS

②各種ログを暗号化し、解析プラットフォームにリアルタイム送信

aws

Stealthwatch Cloud

AMP

Thread Grid

Umbrella

StealthWatch Cloud

①各製品のログをクラウド上で収集

ログ送信

アナリスト (一次解析)

③収集されたログを相関的に分析・調査

- File hash
- IP address
- Domain/URL
- Isolate hosts
- More...

インベスティゲータ (二次解析)

レスポンダ

拠点

AMP for Endpoints

Stealthwatch Sensor

リモートワーク

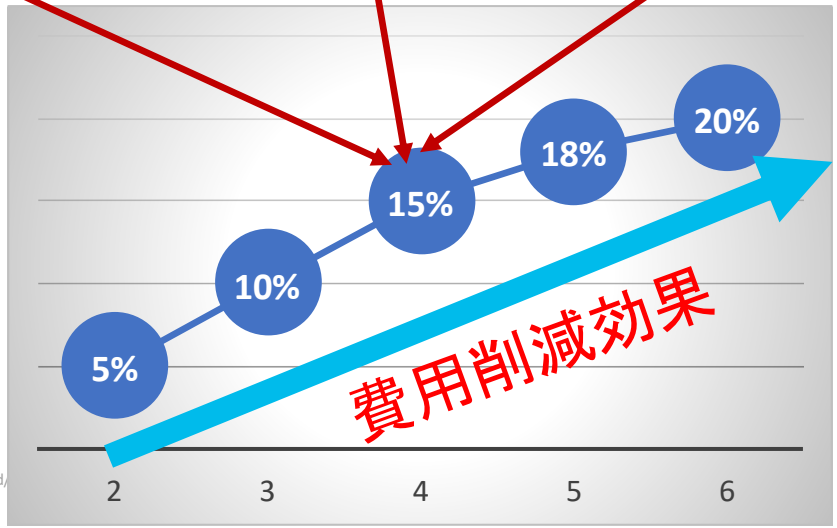
AMP for Endpoints

Cisco Security Operation Center

# まとめるとコストと数がお得なプログラム

| 不正な電子メール マルウェア防御 | 悪意のある宛先へのアクセスをブロック 感染をブロック | マルウェア感染のブロック | 業界標準Snortで マルウェア防御 | 内部拡散の検出と遮断 |
|---|---|---|---|---|
| メールセキュリティ **ESA** | ウェブセキュリティ **WSA** | マルウェア対策 **AMP** | 次世代FW・IPS **Firepower** | 脅威検出 **StealthWatch** |
| クラウドメールセキュリティ **CES** | セキュア名前解決 **Umbrella** | | | 脅威収集・隔離 **ISE** |

コスト削減




推奨例

- 2つ以上の選択
- 20%までの増加分を含む
- 3 or 5年間の利用


CISCO