CISCO
SECURE

CISCO The bridge to possible

【緊急開催！ランサムウェア対策セミナー】

今とるべきサイバーセキュリティ対策強化、その勘所

～高まるサイバー攻撃の脅威から組織をどう守るべきか～

2022年3月17日

シスコシステムズ合同会社
豊島かおり

サイバーセキュリティ最新動向

情報セキュリティ10大脅威 2022

■「情報セキュリティ10大脅威 2022」

NEW：初めてランクインした脅威

昨年順位	個人	順位	組織	昨年順位
2位	フィッシングによる個人情報等の詐取	1位	ランサムウェアによる被害	1位
3位	ネット上の誹謗・中傷・デマ	2位	標的型攻撃による機密情報の窃取	2位
4位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	3位	サプライチェーンの弱点を悪用した攻撃	4位
5位	クレジットカード情報の不正利用	4位	テレワーク等のニューノーマルな働き方を狙った攻撃	3位
1位	スマホ決済の不正利用	5位	内部不正による情報漏えい	6位
8位	偽警告によるインターネット詐欺	6位	脆弱性対策情報の公開に伴う悪用増加	10位
9位	不正アプリによるスマートフォン利用者への被害	7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
7位	インターネット上のサービスからの個人情報の窃取	8位	ビジネスメール詐欺による金銭被害	5位
6位	インターネットバンキングの不正利用	9位	予期せぬIT基盤の障害に伴う業務停止	7位
10位	インターネット上のサービスへの不正ログイン	10位	不注意による情報漏えい等の被害	9位

出典：IPA「情報セキュリティ10大脅威 2022」
（https://www.ipa.go.jp/security/vuln/10threats2022.html）

- 組織の脅威においては、ランサムウェアによる被害および標的型攻撃による機密情報の窃取が引き続き1位と2位
- サプライチェーンの弱点を悪用した攻撃が3位に

ウクライナ情勢によるサイバー攻撃アクターの変化

セキュリティ

ウクライナ情勢の進展に関するTalosの見解

木村 滋
2022年3月7日

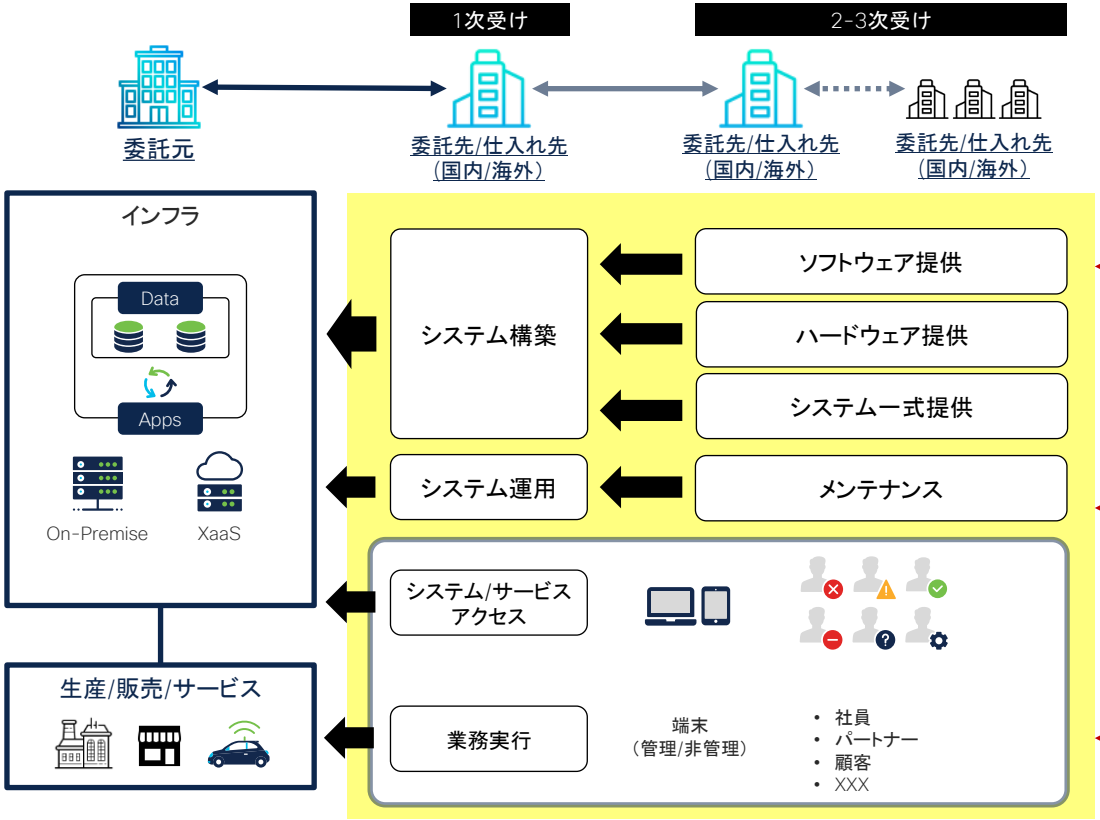
ウクライナの活動に関するコンテンツ：

- ウクライナで進行中のサイバー攻撃に関する現在のエグゼクティブガイダンス
- 脅威アドバイザリ：HermeticWiper
- 脅威アドバイザリ: Cyclops Blink
- 群衆からの攻撃による新たな危機拡大リスク
- 改ざんとワイパーによるウクライナキャンペーンの継続的な注意喚起
- Cisco stands beside its customers in Ukraine

https://gblogs.cisco.com/jp/2022/03/security-talos-on-the-developing-situation-in-ukraine/

- 政治思想によるモチベーションの高いアクターグループが結集
  - 国家による支援を受けている高度なアクターグループ
  - 従来のサイバー犯罪者アクターグループ
    - 技術と精巧さが多岐にわたっている
- ウクライナ国内への攻撃
  - フェイク情報、改ざん、ワイパーマルウェア、BGPハイジャック（銀行向けハイジャック）
  - ウクライナ外務省、国防省、内務省、国立銀行へのDDoS
- **西側支援国への攻撃**
  - 米国国防省、大手国営銀行、ウクライナ高官へのDDoS
  - 西側支援諸国に対する、対ロシア制裁に対する国民の支持を低下させる目的
  - 国内産業、国内インフラに対し、制裁に伴うペナルティを強調する目的のサイバー作戦増加の可能性

サプライチェーン攻撃概要



委託先を踏み台にした攻撃

- 取引先などのサプライチェーンの中でも、セキュリティ対策が甘い組織を攻撃の足がかりにして、大企業や政府組織など標的の組織を攻撃して不正アクセスする手法

（主なインシデント事例）
- 小島プレス、三菱パワー、など

ソフトウェアサプライチェーン攻撃

- ソフトウェアの開発元や配布元などソフトウェアのサプライチェーンを通じ て、マルウェアや攻撃コードを挿入したソフトウェアを配布して攻撃の足がかりにする手法

（主なインシデント事例）
- SolorWinds, Kesayaなど

委託先からの情報窃取

- セキュリティ対策が不十分な委託先を狙って、委託先が委託元から預かって いる個人情報や重要情報を窃取する手法

（主なインシデント事例）
- Peatix Inc., Dear Uなど

サイバーセキュリティ対策の強化に関する注意喚起

2022年3月1日に 経済産業省 / 金融庁 / 総務省 / 厚生労働省 / 国土交通省 / 警察庁 / NICT 各省庁 7組織連名で現在の情勢におけるサイバーセキュリティ注意喚起を発表
（以下 https://www.meti.go.jp/press/2021/03/20220301007/20220301007-1.pdf より抜粋）

サイバーセキュリティ対策の強化について（注意喚起）

昨今の情勢を踏まえるとサイバー攻撃事案のリスクは高まっていると考えられます。本日、国内の自動車部品メーカーから被害にあった旨の発表がなされたところです。

政府機関や重要インフラ事業者をはじめとする各企業・団体等においては、組織幹部のリーダーシップの下、サイバー攻撃の脅威に対する認識を深めるとともに、以下に掲げる対策を講じることにより、対策の強化に努めていただきますようお願いいたします。

また、中小企業、取引先等、サプライチェーン全体を俯瞰し、発生するリスクを自身でコントロールできるよう、適切なセキュリティ対策を実施するようお願いいたします。

さらに、国外拠点等についても、国内の重要システム等へのサイバー攻撃の足掛かりになることがありますので、国内のシステム等と同様に具体的な支援・指示等によりセキュリティ対策を実施するようお願いいたします。

実際に情報流出等の被害が発生していなかったとしても、不審な動きを検知した場合は、早期対処のために速やかに所管省庁、セキュリティ関係機関に対して連絡していただくとともに、警察にもご相談ください。

1．リスク低減のための措置
- ○パスワードが単純でないかの確認、アクセス権限の確認・多要素認証の利用・不要なアカウントの削除等により、本人認証を強化する。
- ○IoT 機器を含む情報資産の保有状況を把握する。特に VPN 装置やゲートウェイ等、インターネットとの接続を制御する装置の脆弱性は、攻撃に悪用されることが多いことから、セキュリティパッチ（最新のファームウェアや更新プログラム等）を迅速に適用する。
- ○メールの添付ファイルを不用意に開かない、URL を不用意にクリックしない、連絡・相談を迅速に行うこと等について、組織内に周知する。

2．インシデントの早期検知
- ○サーバ等における各種ログを確認する。
- ○通信の監視・分析やアクセスコントロールを再点検する。

3．インシデント発生時の適切な対処・回復
- ○データ消失等に備えて、データのバックアップの実施及び復旧手順を確認する。
- ○インシデント発生時に備えて、インシデントを認知した際の対処手順を確認し、対外応答や社内連絡体制等を準備する。

経産省注意喚起の解釈

【検討範囲】

- ✓ 中小企業 、取引先等、全体を俯瞰し、発生するリスクを自身でコントロールできるよう、適切なセキュリティ対策を実施
- ✓ 国外拠点についても、国内の重要システム等へのサイバー攻撃の足掛かりになることを考慮し、国内のシステム等と同様に支援・指示などによりセキュリティ対策を実施

➢ 産業、業種、業態共通
➢ 理解を深め自組織で制御
➢ ガイドから実施へ

【対応策】

（リスク低減のための措置）
- ✓ パスワード強化対策
- ✓ IoT機器を含む情報資産の保有状況を把握と脆弱性対応
- ✓ フィッシングメール対策

（インシデントの早期検知）
- ✓ サーバ等における各種ログ確認
- ✓ 通信の監視・分析やアクセスコントロールの再点検

（インシデント発生時の適切な対処・回復）
- ✓ データ損失などに備えたデータバック実施と復旧手順の確認
- ✓ インシデント発生時の対応のための体制やプロセス、対処手順の整備

システム的対応：MFA (多要素認証)

システム的対応：パッチ、脆弱性管理

システム的対応：メールセキュリティ

システム的対応：通信監視

運用管理
構成・設定管理

組織・体制

➢ 情報資産の管理強化
➢ インフラにおけるセキュリティ対策強化
➢ セキュリティ運用の強化

経産省注意喚起の解釈

【検討範囲】

- ✓ 中小企業 、取引先等、全体を俯瞰し、発生するリスクを自身でコントロールできるよう、適切なセキュリティ対策を実施
- ✓ 国外拠点についても、国内の重要システム等へのサイバー攻撃の足掛かりになることを考慮し、国内のシステム等と同様に支援・指示などによりセキュリティ対策を実施

- ➢ 産業、業種、業態共通
- ➢ 理解を深め自組織で制御
- ➢ ガイドから実施へ

【対応策】

（リスク低減のための措置）
- ✓ パスワード強化対策
- ✓ IoT機器を含む情報資産の保有状況を把握と脆弱性対応
- ✓ フィッシングメール対策

（インシデントの早期検知）
- ✓ サーバ等における各種ログ確認
- ✓ 通信の監視・分析やアクセスコントロールの再点検

（インシデント発生時の適切な対処・回復）
- ✓ データ損失などに備えたデータバック実施と復旧手順の確認
- ✓ インシデント発生時の対応のための体制やプロセス、対処手順の整備

システム的対応：MFA (多要素認証)

システム的対応：パッチ、脆弱性管理

システム的対応：メールセキュリティ

システム的対応：通信監視

運用管理
構成・設定管理

組織・体制

- ➢ 情報資産の管理強化
- ➢ インフラにおけるセキュリティ対策強化
- ➢ セキュリティ運用の強化

参考) CISA – “Shields Up”

https://www.cisa.gov/shields-up

CISA : Cybersecurity and Infrastructure Security Agency : アメリカサイバーセキュリティ庁 (https://www.cisa.gov/)
CISA Shield Up : 昨今の情勢に対する各組織のサイバー攻撃影響に備え対応するためのエグゼクティブガイドライン

サイバー攻撃からの防御
✓ **リモートアクセス、特権アクセス、管理アクセスに多要素認証を実装**
✓ ソフトウェア最新性の確認管理 : CISA 既知脆弱性カタログ参照
✓ 不必要サービス, ポートの制御
✓ クラウドサービスの制御強化 : https://www.cisa.gov/uscert/ncas/analysis-reports/ar21-013a
✓ 脆弱性スキャンによる侵入テストの実施

迅速な侵入検出への対策・運用
✓ ログの有効化
✓ **ネットワーク全体がマルウェア対策で保護されていること**

侵入発生時の組織体制
✓ テクノロジ、法務、事業継続、組織内の役割/責任分担、CSIRT、レスポンスチームの構成
✓ 机上演習の実施

システム的対応 :
MFA (多要素認証)

システム的対応 :
脆弱性管理, パッチマネージメント

システム的対応 : マルウェア対策

参考) 脅威アクターが利用する可能性のある脆弱性

Talos Blog Cisco / Kenna Top 10 Exploitable Vulnerability

Top 10 Exploitable Vulnerabilities

Talos

CVE	Kenna Score	Description
CVE-2021-40444	100	Microsoft MSHTML Remote Code Execution Vulnerability
CVE-2021-36942	100	Windows LSA Spoofing Vulnerability
CVE-2021-34527	100	Windows Print Spooler Remote Code Execution Vulnerability
CVE-2022-0609	97	Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in Animation. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system.
CVE-2021-21220	100	Insufficient validation of untrusted input in V8 in Google Chrome prior to 89.0.4389.128 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0609	97	Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in Animation. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system.
CVE-2020-1313	100	An elevation of privilege vulnerability exists when the Windows Update Orchestrator Service improperly handles file operations, aka 'Windows Update Orchestrator Service Elevation of Privilege Vulnerability'.
CVE-2020-0796	100	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Remote Code Execution Vulnerability'.
CVE-2020-0646	100	A remote code execution vulnerability exists when the Microsoft .NET Framework fails to validate input properly, aka '.NET Framework Remote Code Execution Injection Vulnerability'.
CVE-2021-1675	100	Windows Print Spooler Elevation of Privilege Vulnerability

https://gblogs.cisco.com/jp/2022/03/security-ukraine-update/

CISA KNOWN EXPLOITED VULNERABILITIES CATALOG (95)
(CISA 既知の利用可能な脆弱性カタログ 95種)

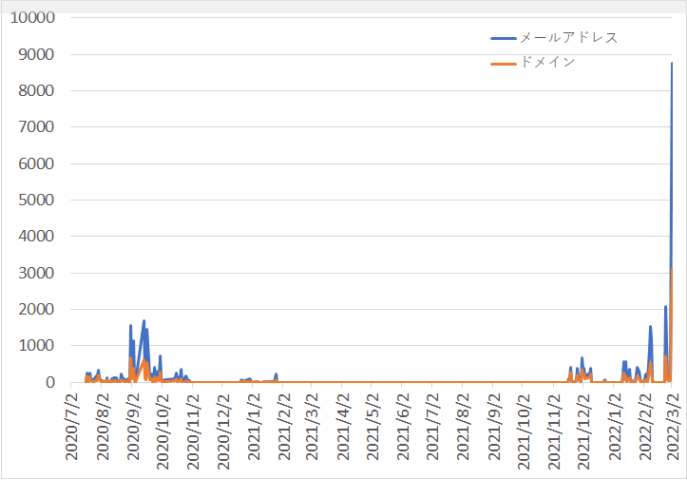
CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date	Notes
CVE-2021-27104	Accellion	FTA	Accellion FTA OS Command Injection Vulnerability	2021-11-03	Accellion FTA 9_12_370 and earlier is affected by OS command execution via a crafted POST request to various admin endpoints.	Apply updates per vendor instructions.	2021-11-17	
CVE-2021-27102	Accellion	FTA	Accellion FTA OS Command Injection Vulnerability	2021-11-03	Accellion FTA 9_12_411 and earlier is affected by OS command execution via a local web service call.	Apply updates per vendor instructions.	2021-11-17	
CVE-2021-27101	Accellion	FTA	Accellion FTA SQL Injection Vulnerability	2021-11-03	Accellion FTA 9_12_370 and earlier is affected by SQL injection via a crafted Host header in a request to document_root.html.	Apply updates per vendor instructions.	2021-11-17	
CVE-2021-27103	Accellion	FTA	Accellion FTA SSRF Vulnerability	2021-11-03	Accellion FTA 9_12_411 and earlier is affected by SSRF via a crafted POST request to wmProgressstat.html.	Apply updates per vendor instructions.	2021-11-17	
CVE-2021-21017	Adobe	Acrobat and Reader	Adobe Acrobat and Reader Heap-based Buffer Overflow Vulnerability	2021-11-03	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a heap-based buffer overflow vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	Apply updates per vendor instructions.	2021-11-17	
CVE-2021-28550	Adobe	Acrobat and Reader	Adobe Acrobat and Reader Use-After-Free Vulnerability	2021-11-03	Acrobat Reader DC versions versions 2021.001.20150 (and earlier), 2020.001.30020 (and earlier) and 2017.011.30194 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	Apply updates per vendor instructions.	2021-11-17	
CVE-2018-4939	Adobe	ColdFusion	Adobe ColdFusion Deserialization of Untrusted Data	2021-11-03	Adobe ColdFusion Update 5 and earlier versions, ColdFusion 11 Update 13 and earlier versions have an exploitable Deserialization of Untrusted Data	Apply updates per vendor	2022-05-03	

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

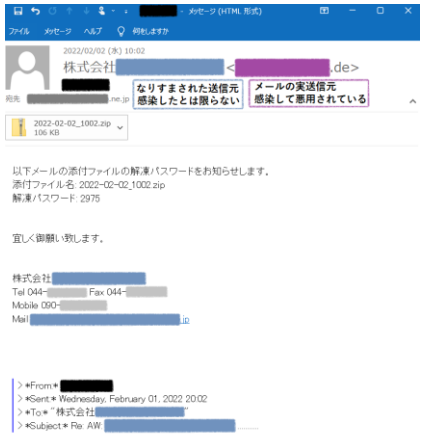
マルウェアEmotetの感染再拡大に関する注意喚起

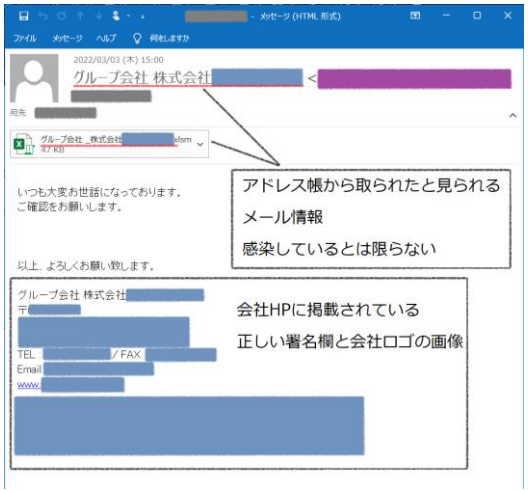
2022年2月10日にJPCERTからマルウェアEmotetの感染再拡大に関する注意喚起
（以下 https://www.jpcert.or.jp/at/2022/at220006.html から引用）

2022年3月に入り、Emotetに感染しメール送信に悪用される可能性のある.jpメールアドレス数が2020年の感染ピーク時の約5倍以上に急増しています。



［図1：Emotetに感染しメール送信に悪用される可能性のある.jpメールアドレス数の新規観測の推移 (外部からの提供観測情報)（2022年3月3日更新）］



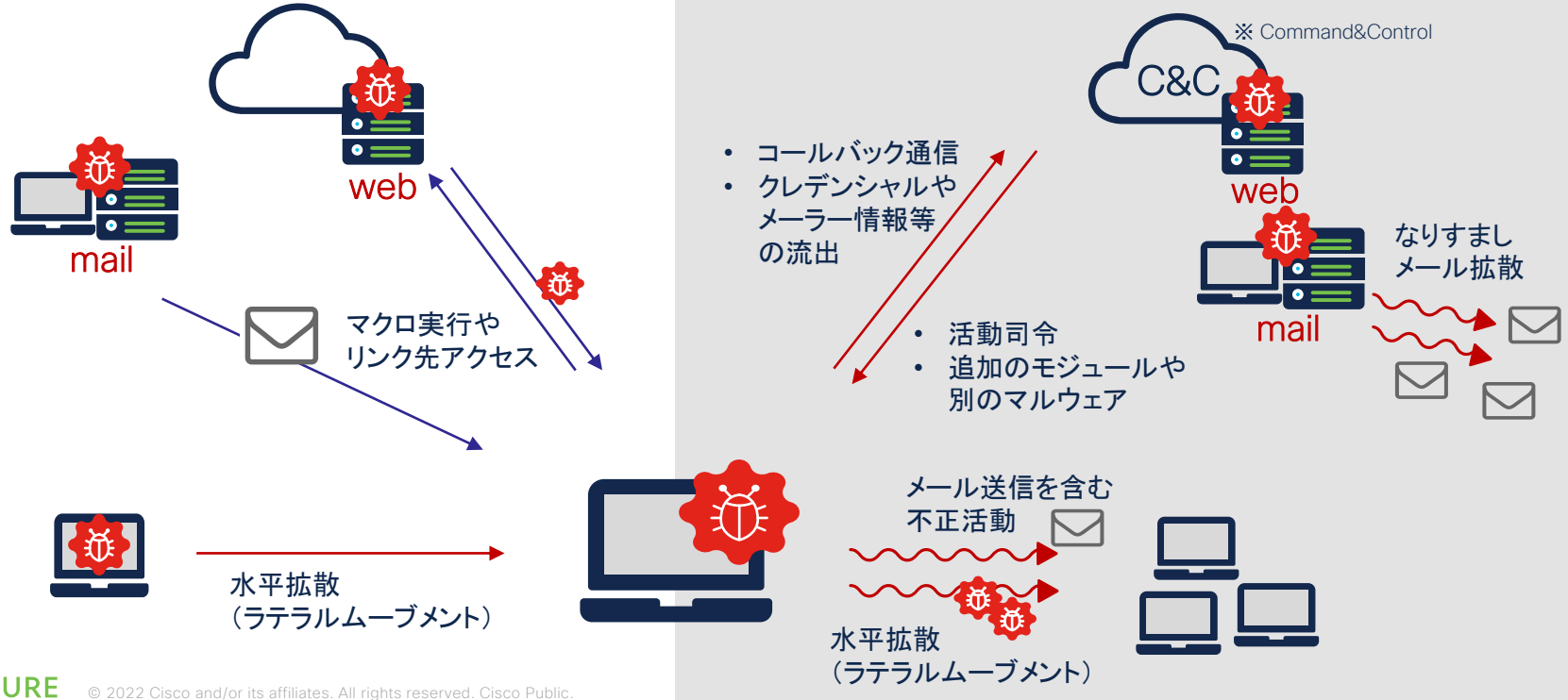


［図2, 図2-1：Emotetメールサンプル］

主にマクロ付きのExcelやWordファイル、あるいはこれらをパスワード付きZipファイルとしてメールに添付する形式で配信されており、ファイルを開封後にマクロを有効化する操作を実行することでEmotetの感染に繋がります。（中略）メール本文中のリンクをクリックすることで悪性なExcelやWordファイルがダウンロードされたり、アプリケーションのインストールを装いEmotet感染をねらうケースも観測しています。

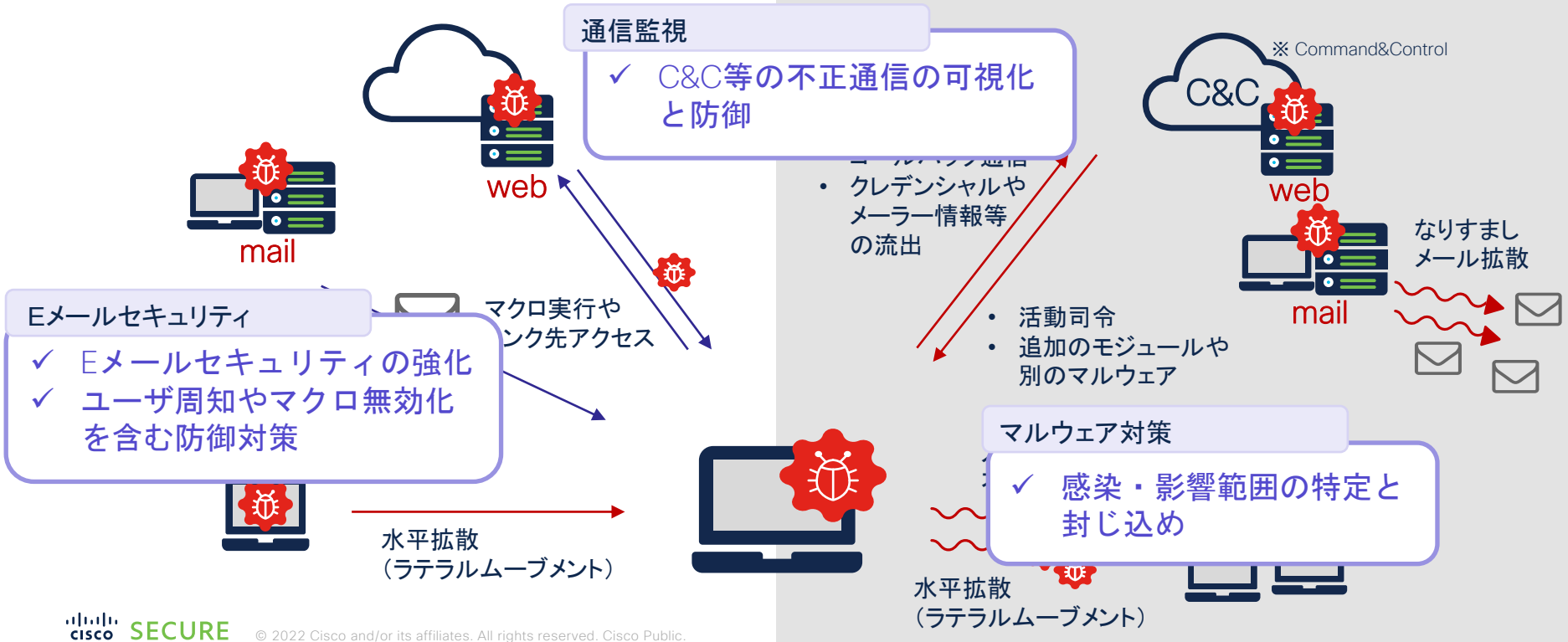
Emotet の感染拡大活動

活動は検知システムの回避技術を使いながら断続的に継続される



Emotet の感染拡大活動

活動は検知システムの回避技術を使いながら断続的に継続される



ランサムウェア (Ransomware) とは？

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 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、 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 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 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 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

最近のランサムウェア (Ransomware) の特徴

ランサム被害にあったら何が起こる？：「二重脅迫 & 標的型ランサムウェア」

1. 内部の1端末の感染を手がかりに重要システムを奪取 (ドメインコントローラ等)
2. 感染システム全体の端末からファイルを盗み出す
3. 感染端末全体のファイルを暗号化
4. 利用できないシステムの復旧に対する身代金を要求
5. 復旧のための身代金を拒んだ場合、漏洩サイトで盗んだファイルの漏洩に対する身代金を再要求

※個々のユーザにランサムウェアファイルを感染させるのではなく、標的型攻撃と同様な手法で組織全体を狙う

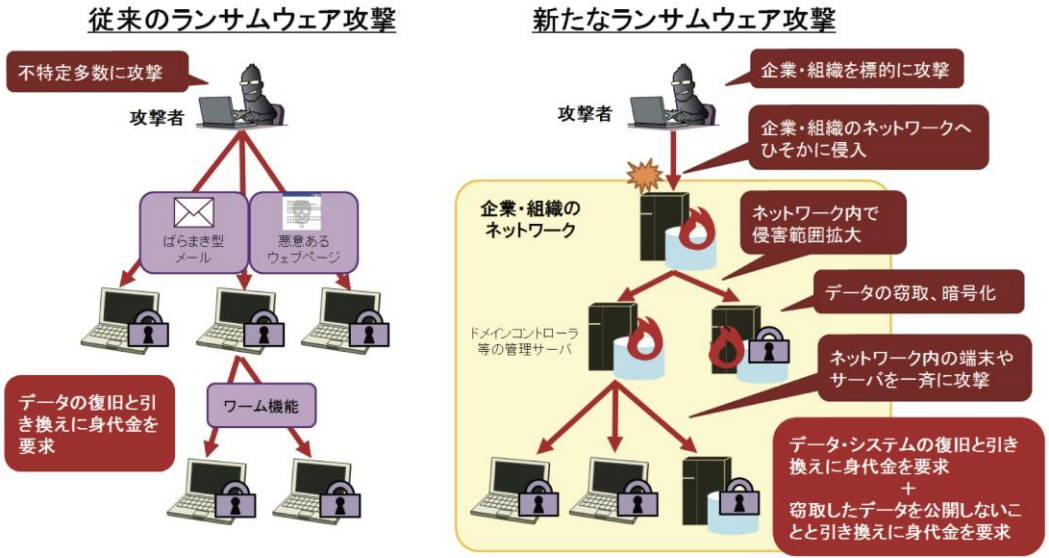


図 2-2 従来の／新たなランサムウェア攻撃の差異

出典：IPA【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について
https://www.ipa.go.jp/files/000084974.pdf

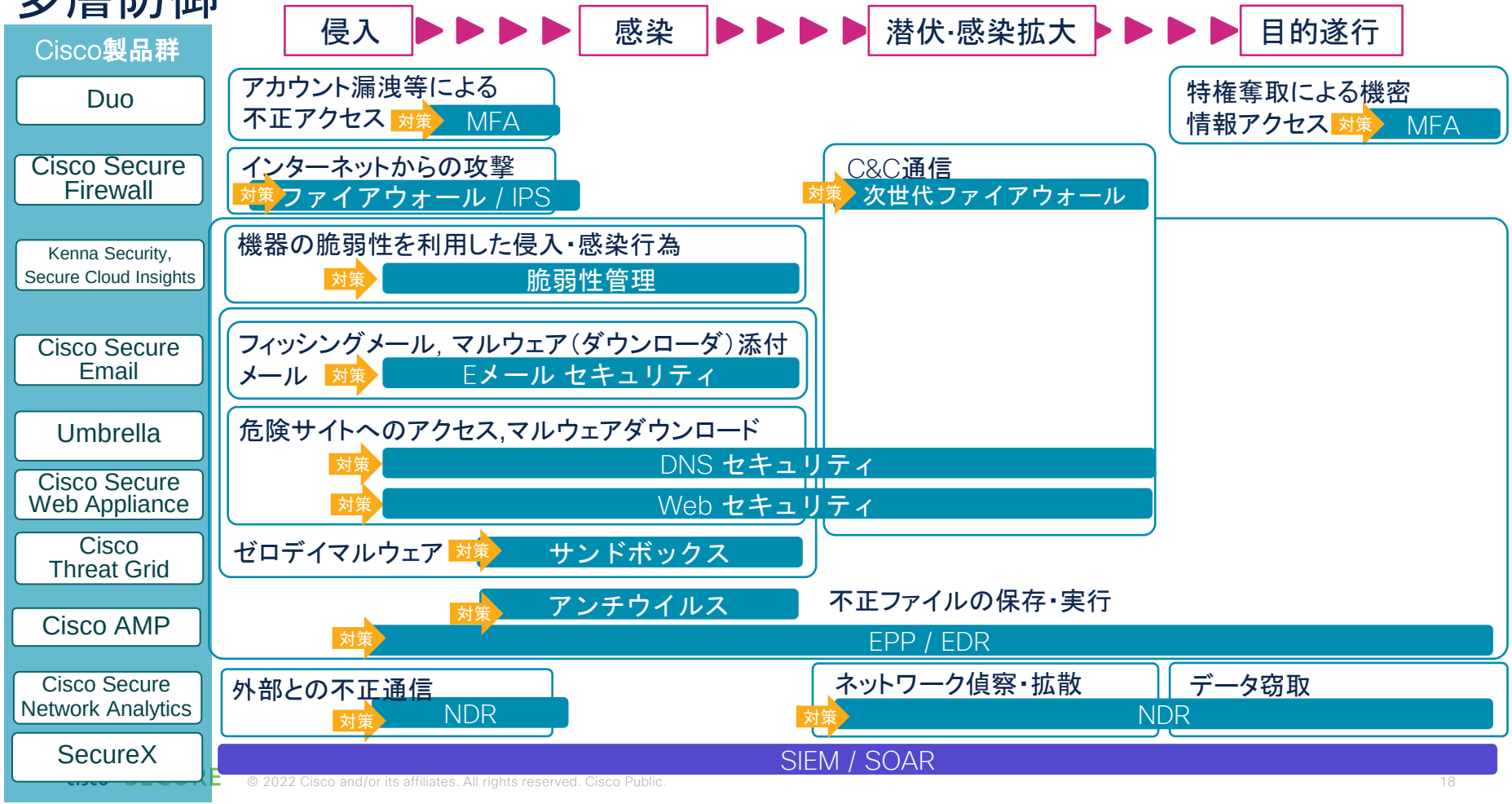
Ciscoソリューションによる対策案

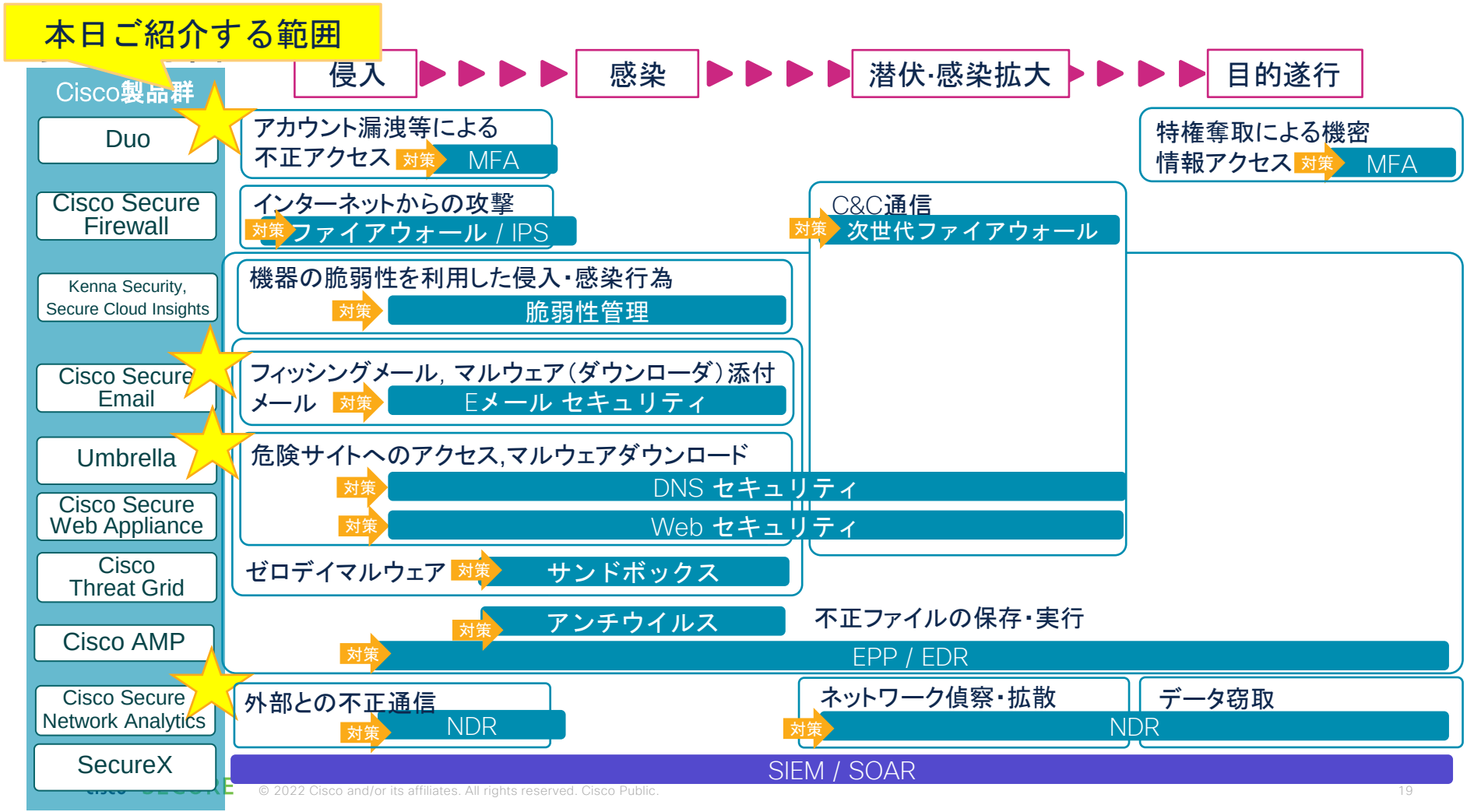
今行うべきシステムの安全対策とは

検討ポイント

- 自組織が持つリスクを整理し、現行のシステムおよび運用でのカバー範囲を再確認した上で、導入効果が高い部分を優先的に検討する
- 事故・感染が起こってしまった（または既に感染している）場合に備え、短時間かつ最小限なシステム変更で実現可能なソリューションを検討する

多層防御

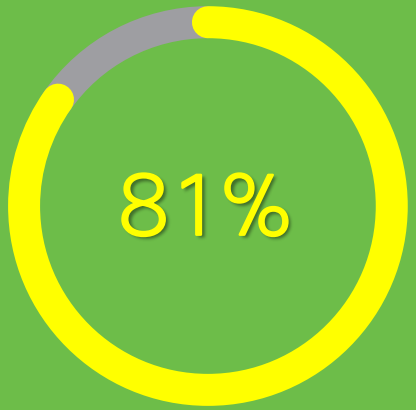




現実の脅威：不正侵入は、ID/パスワード漏洩から
セキュリティの新しいアプローチが必要とされる

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
*Verizon Data Breach Investigations Report



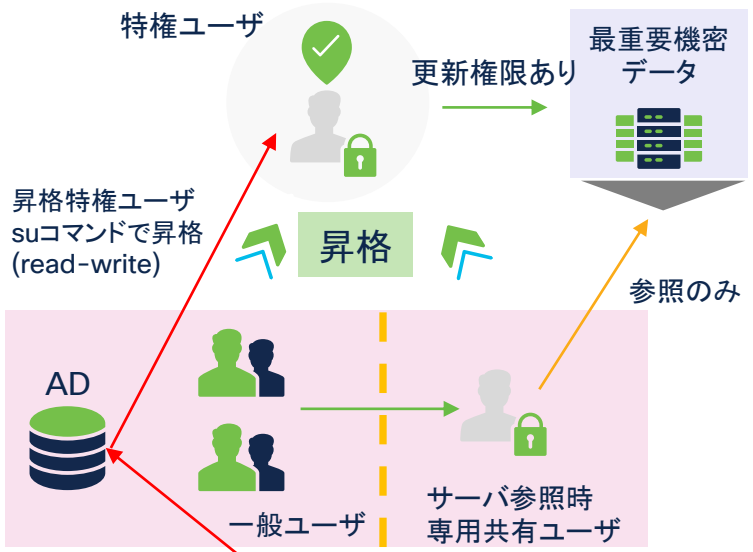
* https://gblogs.cisco.com/jp/2020/06/unpacking-2020s-verizon-dbir-human-error-and-greed-collide/

Cisco Secure Access by Duo

システムとの接続の間にDuoを設置して、多要素認証を実現

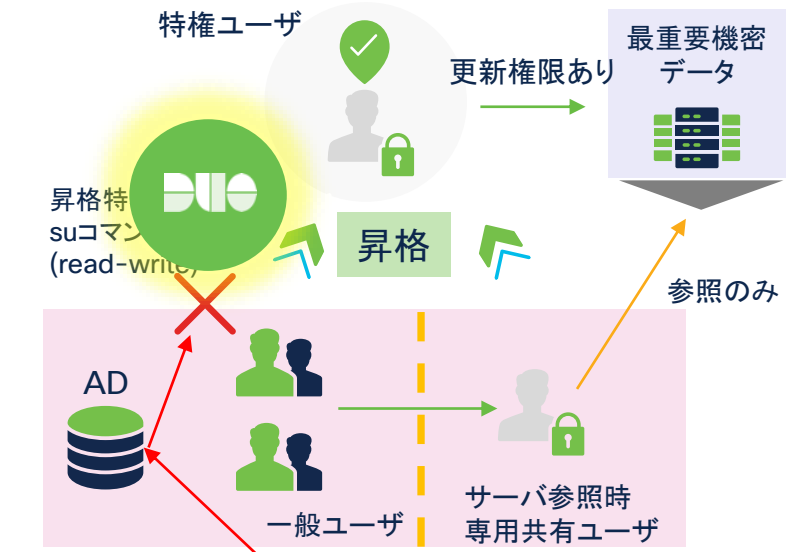
Duo 活用例：特権ユーザ管理のセキュリティ課題

従来の特権管理



【課題】特権ユーザ昇格時に、ID /パスワードのみの管理だと漏洩の可能性が高い

新特権管理

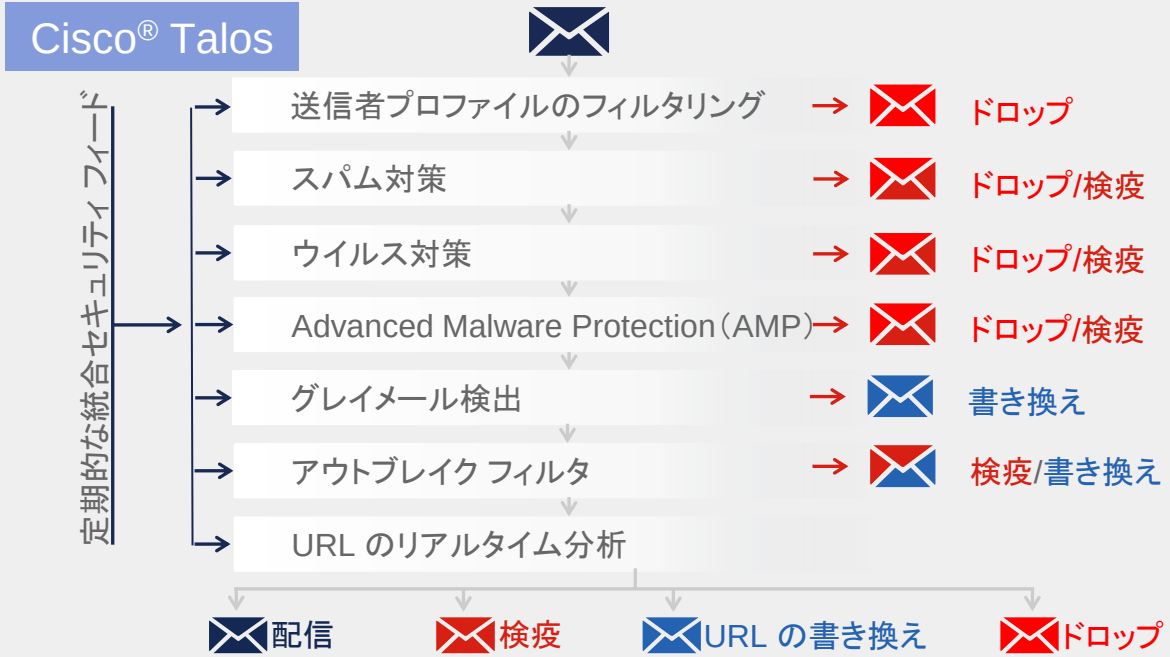


多要素認証で本人確認
ID/パスワードが漏洩しても攻撃者はアクセス不可

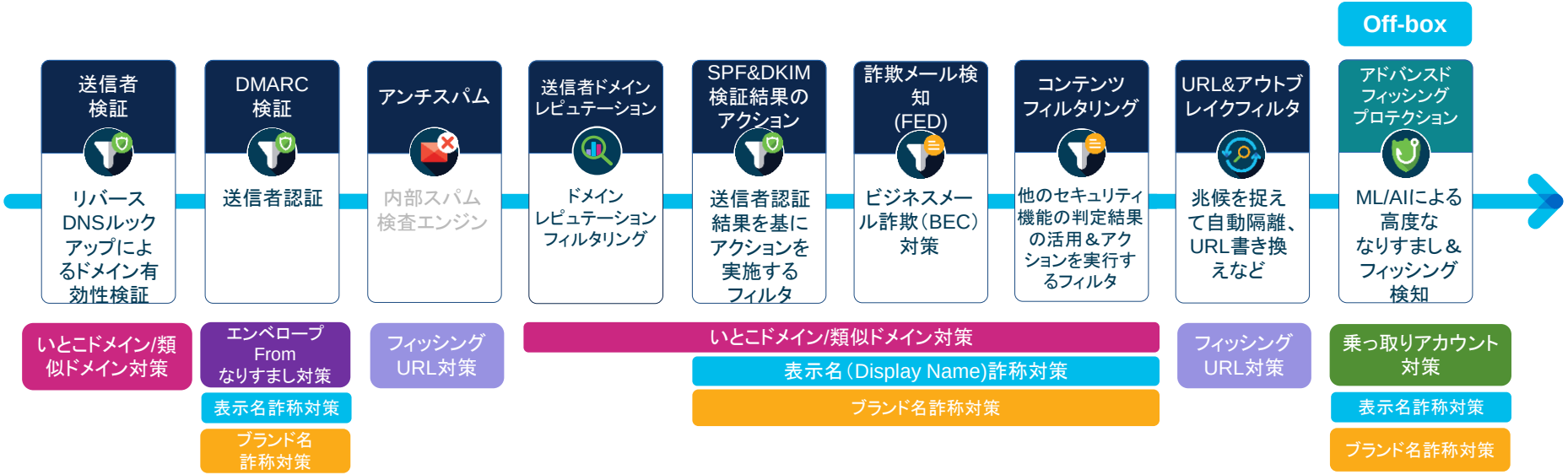
Cisco E メール セキュリティの脅威防御

あらゆるメールの脅威に対応

クラウドインテリジェンスと連動した多段のフィルタリングエンジン



なりすましメール対策



※APPはその他類似ドメインや
自社ドメインなりすまし対策にも有効

参考) Cisco Secure Email Cloud Gateway 最新拡張機能

パスワードで保護された添付ファイルのスキャン

- ファイル添付メールの本文内に記載されたパスワードを抽出
  - コンテンツスキャナの設定により、着信メッセージまたは発信メッセージ内の、パスワードで保護された添付ファイルの内容をスキャンすることができる
  - コンテンツスキャナがベストエフォートでメッセージの本文からパスワードを抽出し、添付ファイルの内容を正常にスキャンできた場合、パスワードと添付ファイルが Cisco AMP Threat Grid に送信される

注) 2022年3月現在、英語のみのサポート（日本語メール本文からのパスワード抽出は非サポート）

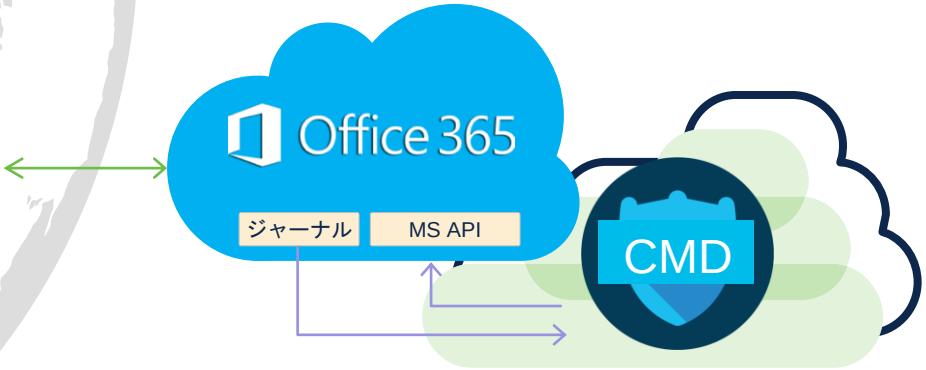
- ユーザ定義のパスフレーズ
  - ユーザ定義のパスフレーズを作成し、着信メッセージまたは発信メッセージ内のパスワードで保護された添付ファイルを開く

AsyncOS 14.0 for Cisco Secure Email Cloud Gateway ユーザガイド
https://www.cisco.com/c/ja_jp/td/docs/security/ces/user_guide/esa_user_guide_14-0/b_ESA_Admin_Guide_ces_14-0/b_ESA_Admin_Guide_12_1_chapter_01000.html#task_1256...

Secure Eメール クラウドサービス導入オプション

Cloud Email Security (CES)：ゲートウェイ

1. MX レコードが CES アドレスに変更される
2. CES がメッセージをスキャンしてアクションを実行
3. メッセージが配信される



Cloud Mailbox Defense (CMD)：CESS※

1. MX レコードは変更されない
2. 各メッセージのコピーが CMD に送信される
3. API を使用した CMD スキャンと修復

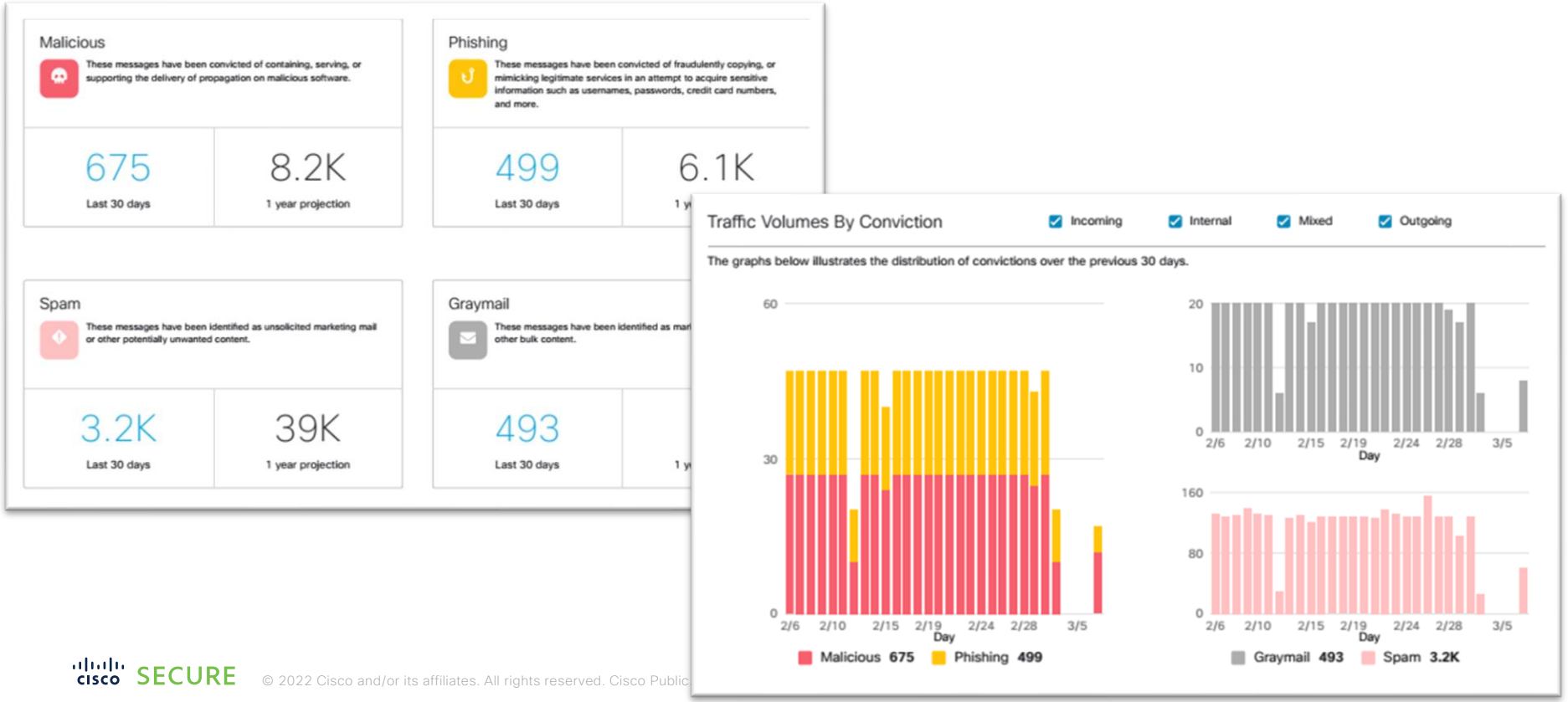
※ Cloud Email Security Supplement

参考）CESとCMDの比較 – 機能別

	Cloud Mailbox Defense (CMD)	Cloud Email Security (CES)
利用できるメールシステム	MS365のみ	特に制限なし
MXレコード変更	不要（API連携）	必要
レピュテーションフィルタリング	✓	✓
コネクションフィルタリング （送信者検証、暗号化と認証、レート制限など）		✓
スパム保護	✓	✓
ファイルレピュテーション（マルウェア対策）	✓	✓
ファイル分析（サンドボックス解析）	✓	✓
URL分析（フィッシング対策）	✓	✓
コンテンツフィルタリング （メッセージのきめ細やかな制御）		✓
Data Loss Prevention（DLP for Outbound）		✓
配信後の脅威メールの削除（自動・手動）	✓	✓
内部メールスキャン	✓	
Talos脅威インテリジェンス	✓	✓
3rd Party連携（External Threat Feed、SIEM、SSO etc.）		✓
SecureX連携	✓	✓

※CDMの利用ユーザ数制限は廃止済み

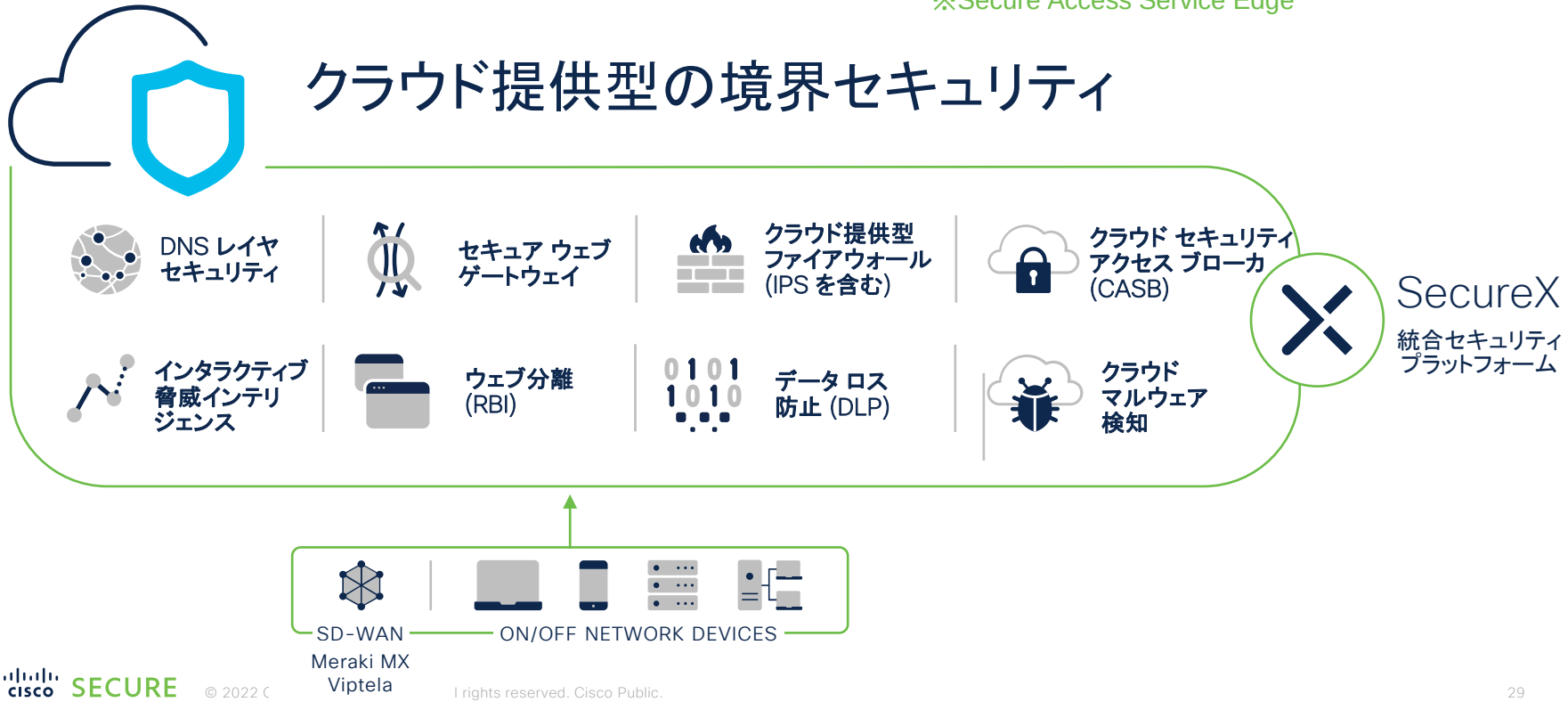
CMDメールボックス診断 レポートサンプル



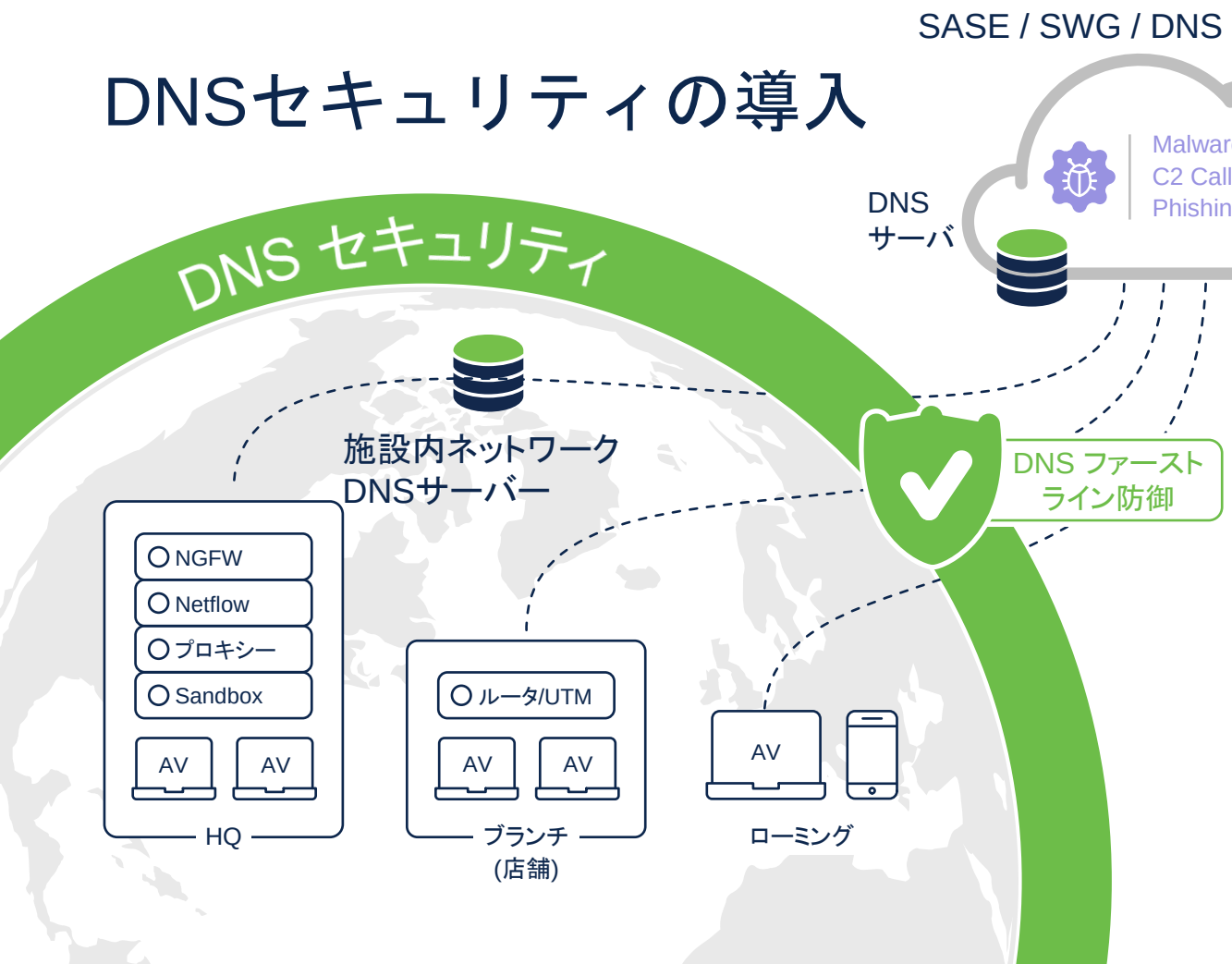
Cisco Umbrella

サブスクリプション型のクラウドサービスで提供されるSASEソリューション

※Secure Access Service Edge



DNSセキュリティの導入



導入効果

DNSをクラウドに向けるだけ

数分でグローバル展開可能

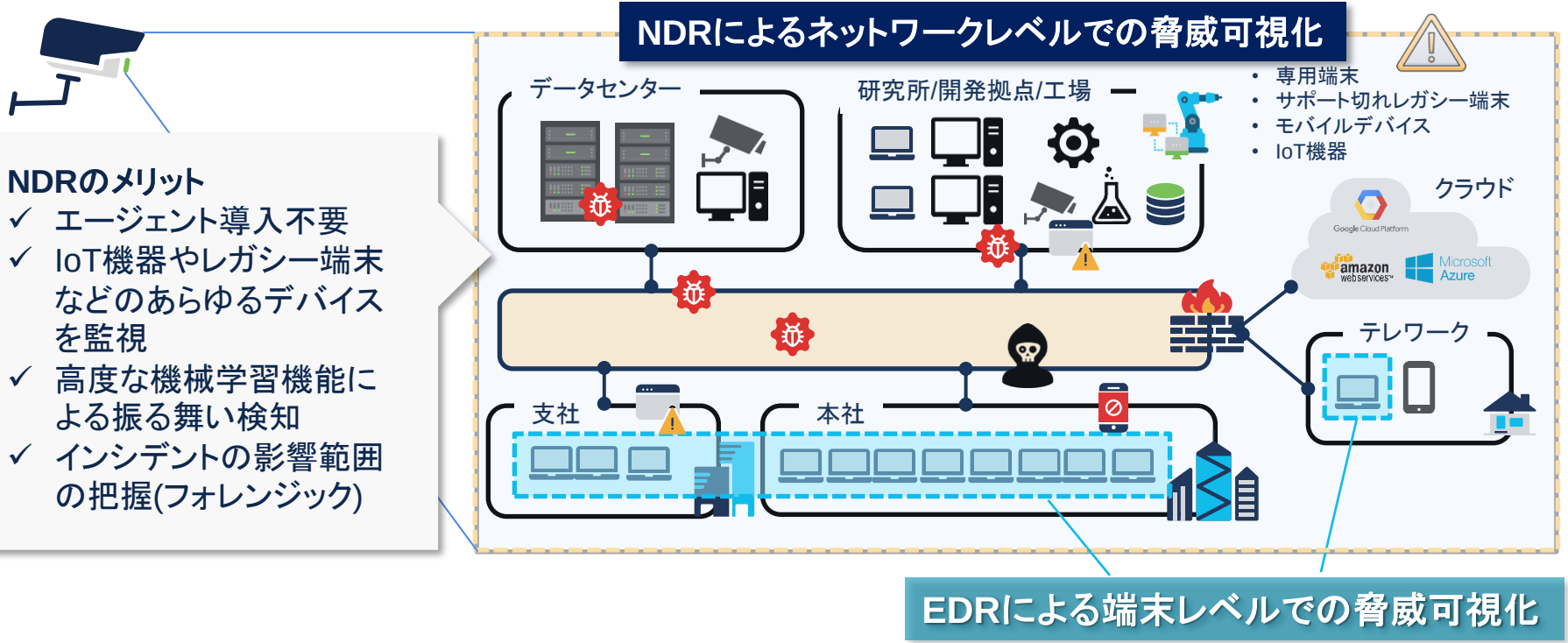
リモート拠点やローミング端末の対応

Webを含む全ポート通信の防御

組織の影響度の迅速な現状把握

感染拡大の速やかな停止

Network Detection and Response (NDR)
ネットワークの振る舞いを監視し脅威を可視化



NDRのメリット

- ✓ エージェント導入不要
- ✓ IoT機器やレガシー端末などのあらゆるデバイスを監視
- ✓ 高度な機械学習機能による振る舞い検知
- ✓ インシデントの影響範囲の把握(フォレンジック)

Cisco Secure Network Analytics (SNA, 旧Stealthwatch) 概要

グローバル脅威インテリジェンス
(powered by Talos)

グローバルな攻撃キャンペーンの情報をローカルのアラームとマッピングし迅速に対処

マルチレイヤ マシンラーニング

複数の機械学習（教師有り/無しを含む）の技術の組み合わせにより高度な脅威を特定

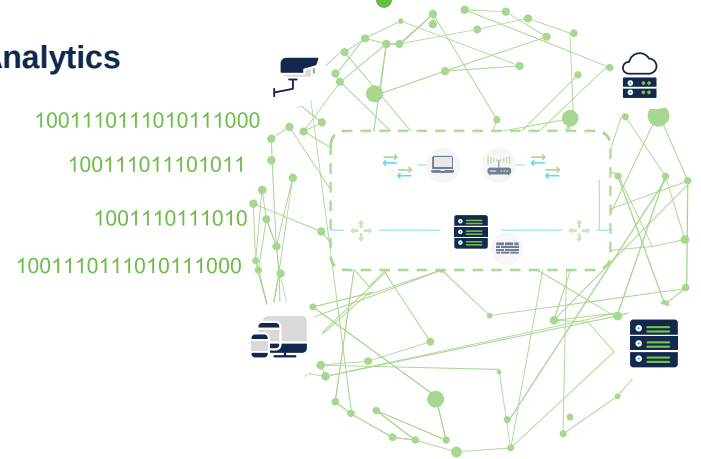
ふるまい検知モデル

ネットワーク内の全通信のふるまいを解析し不正な活動を検出

Secure Network Analytics

データ収集

既存のネットワークインフラからNetflowを利用してリッチなテレメトリ情報を取得

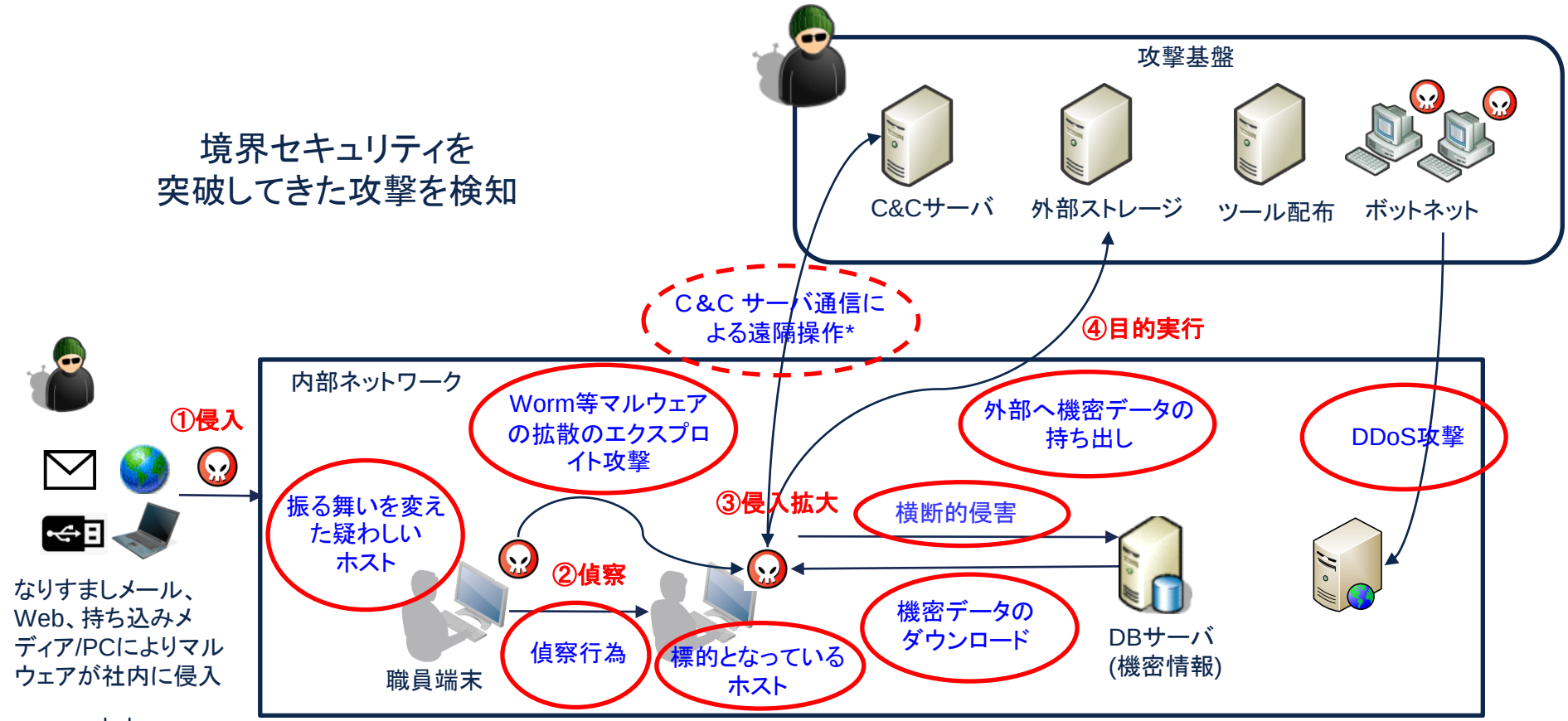


暗号化通信の解析 (ETA; Encrypted Traffic Analytics)

暗号化トラフィックの複合が不要なマルウェア検出

Secure Network Analytics が検出する不正なアクティビティ

境界セキュリティを
突破してきた攻撃を検知

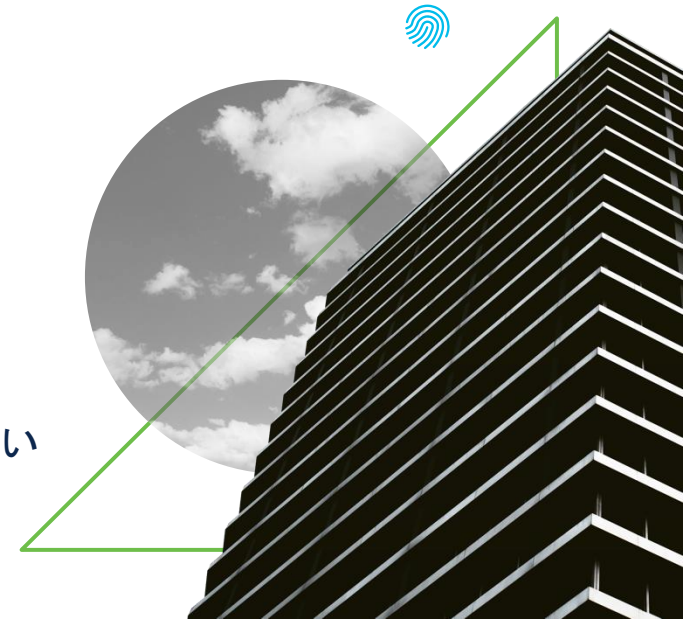


*C&Cサーバ通信を検知するためには別途有償ライセンスが必要のため点線で記載

参考情報) 無料トライアル

- 各ソリューションの無料トライアルをご提供しておりますので是非ご活用ください
  - Secure Access by Duo
    - 製品について, トライアルはこちら
  - Umbrella
    - 製品について, トライアルはこちら
  - Secure Email
    - 製品について, トライアルはこちら
  - Secure Network Analytics
    - 製品について, トライアルはこちら

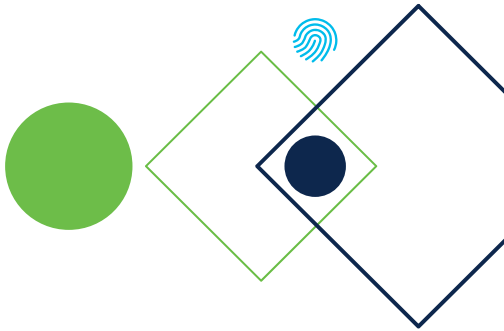
その他のご質問・ご依頼は こちら からお気軽にお問い合わせください



まとめ

- サイバー攻撃の動向
  - サプライチェーン攻撃
  - 経済産業省を含む7省庁からの注意喚起
  - ランサムウェアやマルウェアEmotet活動状況

- ソリューションのご紹介
  - 安全対策の検討ポイントと多層防御
  - 対策ソリューションの例：多要素認証、Eメールセキュリティ、DNSセキュリティ、NDR




cisco
SECURE