シスコセキュリティウェビナーにご参加いただき、ありがとうございます！

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しております。

30分でわかる
標的型サイバー攻撃手法と対策ポイント

シスコシステムズ合同会社
セキュリティ事業
サイバーセキュリティセールススペシャリスト
森 美智雄
2020年9月

アジェンダ

1. 標的型サイバー攻撃について
2. 標的型サイバー攻撃　各フェーズの手法と対策
   - 侵入フェーズ
   - 基盤構築・諜報活動フェーズ
   - 目的遂行フェーズ
3. まとめ
   - 標的型攻撃 各フェーズの対策製品一覧

標的型サイバー攻撃について

明確な目的を持った攻撃者が特定組織を狙うサイバー攻撃の一種
IPA情報セキュリティ10大脅威（対組織）で5年連続1位！不動のセキュリティ脅威

	脅威内容
1位	**標的型攻撃による機密情報の搾取**
2位	内部不正による情報漏えい
3位	ビジネスメール詐欺による金銭被害
4位	サプライチェーンの弱点を悪用した攻撃
5位	ランサムウェアによる被害
6位	予期せぬIT基盤の障害に伴う業務停止
7位	不注意による情報漏えい（規則は遵守）
8位	インターネット上のサービスからの個人情報の窃取
9位	IoT機器の不正利用
10位	サービス妨害攻撃によるサービスの停止

IPA 情報セキュリティ10大脅威 2020 (対組織)
https://www.ipa.go.jp/security/vuln/10threats2020.html

標的型攻撃のフェーズ

●攻撃の進行フェーズに応じて、対策箇所や方法を変える必要がある。

侵入フェーズ	基盤構築・諜報活動	目的遂行
• メール経由攻撃 • ウェブ経由攻撃 • VPN機器への脆弱性攻撃 • アカウント情報の悪用	• バックドア開設 • C&Cサーバー通信 • ネットワーク諜報活動 • 端末間での感染拡大 • 端末からサーバーの侵入	• 情報搾取(情報漏えい) • データ破壊・業務妨害 • 侵入痕跡の隠蔽

参考：IPA『高度標的型攻撃』対策に向けたシステム設計ガイド
https://www.ipa.go.jp/security/vuln/newattack.html

侵入フェーズの手法と対策

標的組織の選定

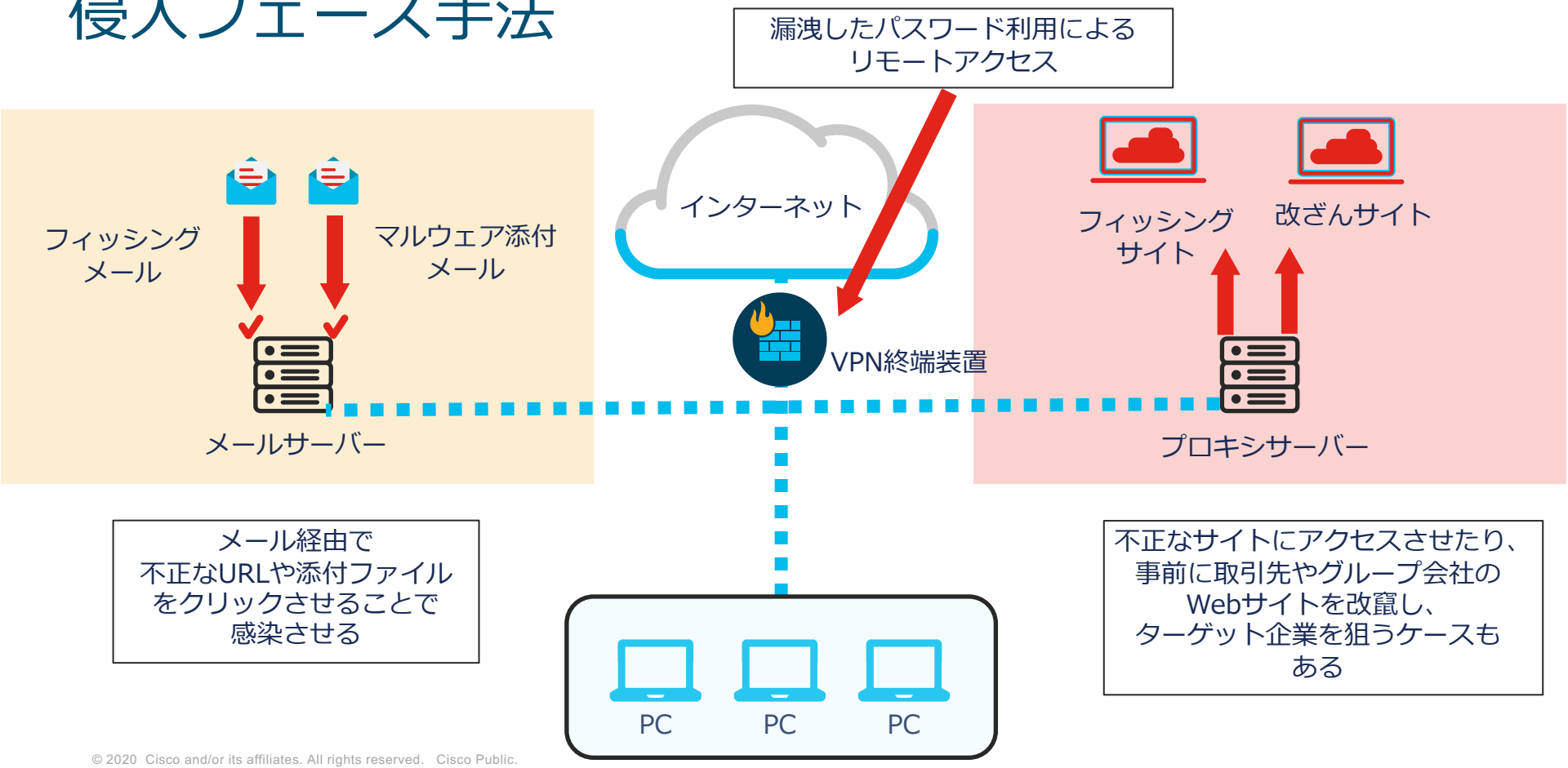
当該組織の従業員宛にフィッシングURLやマルウェアが添付されたメールを
送られることが起因することが多い。
標的組織の選定は主に下記２パターンがある。

ケース１：当初はまだ標的となる企業を決めていない
無差別にメール送付などを行い、従業員がメール経由で感染した後の
C&Cサーバーアクセス時の送信元グローバルIPをチェックし、
めぼしい企業にあたりをつけるケース

ケース２：当初から標的となる企業を決めている
ソーシャルエンジニアリング（SNS、名刺情報など）を活用し、従業員調査を
行い、初めから攻撃対象企業を絞っているケース

※　実際の標的型メールも「ご担当者様」ではなく、「○○株式会社 xx様」など、
実在する従業員が宛名となっているケースが多い

侵入フェーズ手法



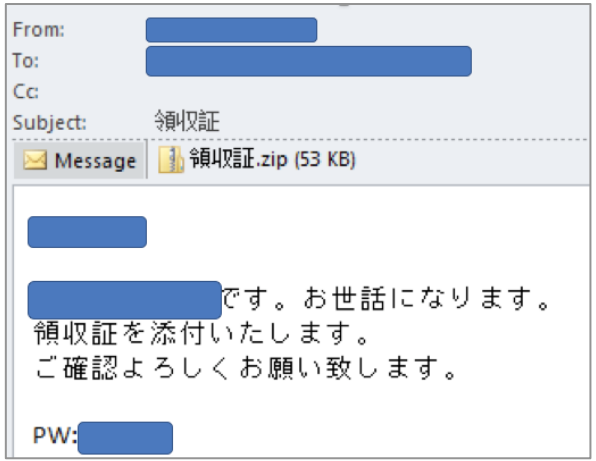
メール経由で
不正なURLや添付ファイル
をクリックさせることで
感染させる

不正なサイトにアクセスさせたり、
事前に取引先やグループ会社の
Webサイトを改竄し、
ターゲット企業を狙うケースも
ある

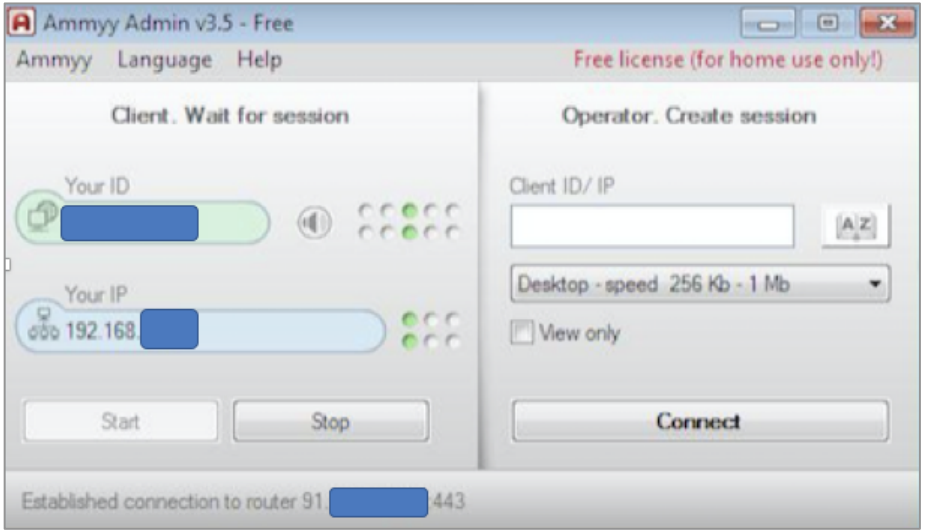
メール経由　マルウェアを利用せず、正規アプリの悪用

マルウェアを利用せず、正規のリモートコントロールソフトなどを起動させて内部侵入（例：フィッシングメールからリモートコントロールソフトのAmmyy Adminを実行）

zipファイルを解凍してドキュメントを開き、
マクロを実行すると、VBScriptがAmmyy Adminを
ダウンロードし、実行される。



実行されるとバックグラウンドで、Ammyy Adminが起動し、
攻撃者が端末を利用できる状態になる。



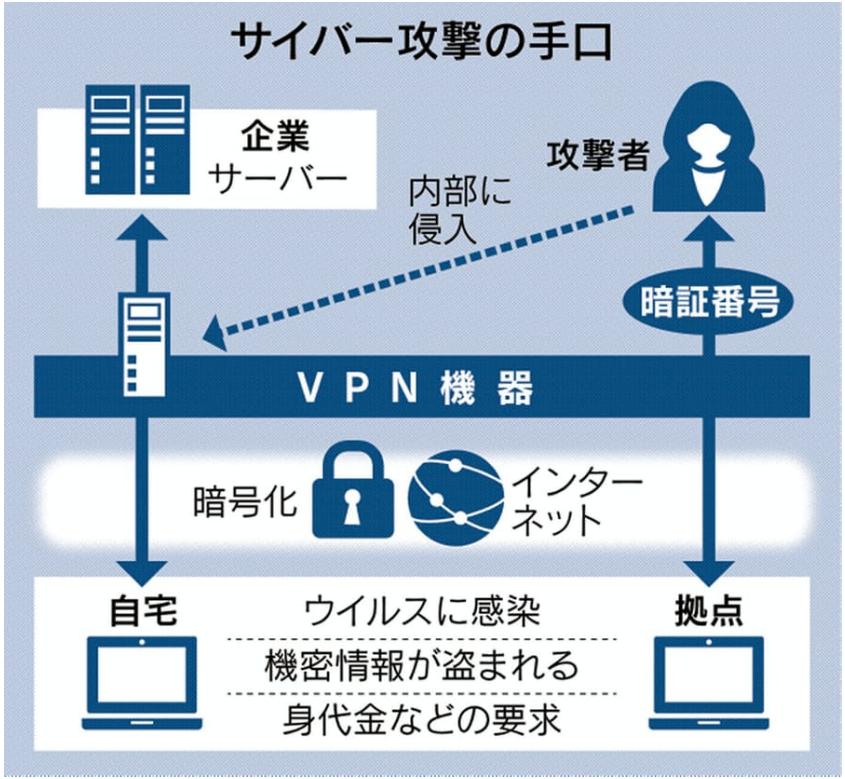
テレワークに伴い増加する攻撃者の侵入
VPN暗証番号流出　国内38社に不正接続

日本経済新聞

テレワーク、VPN暗証番号流出　国内38社に不正接続

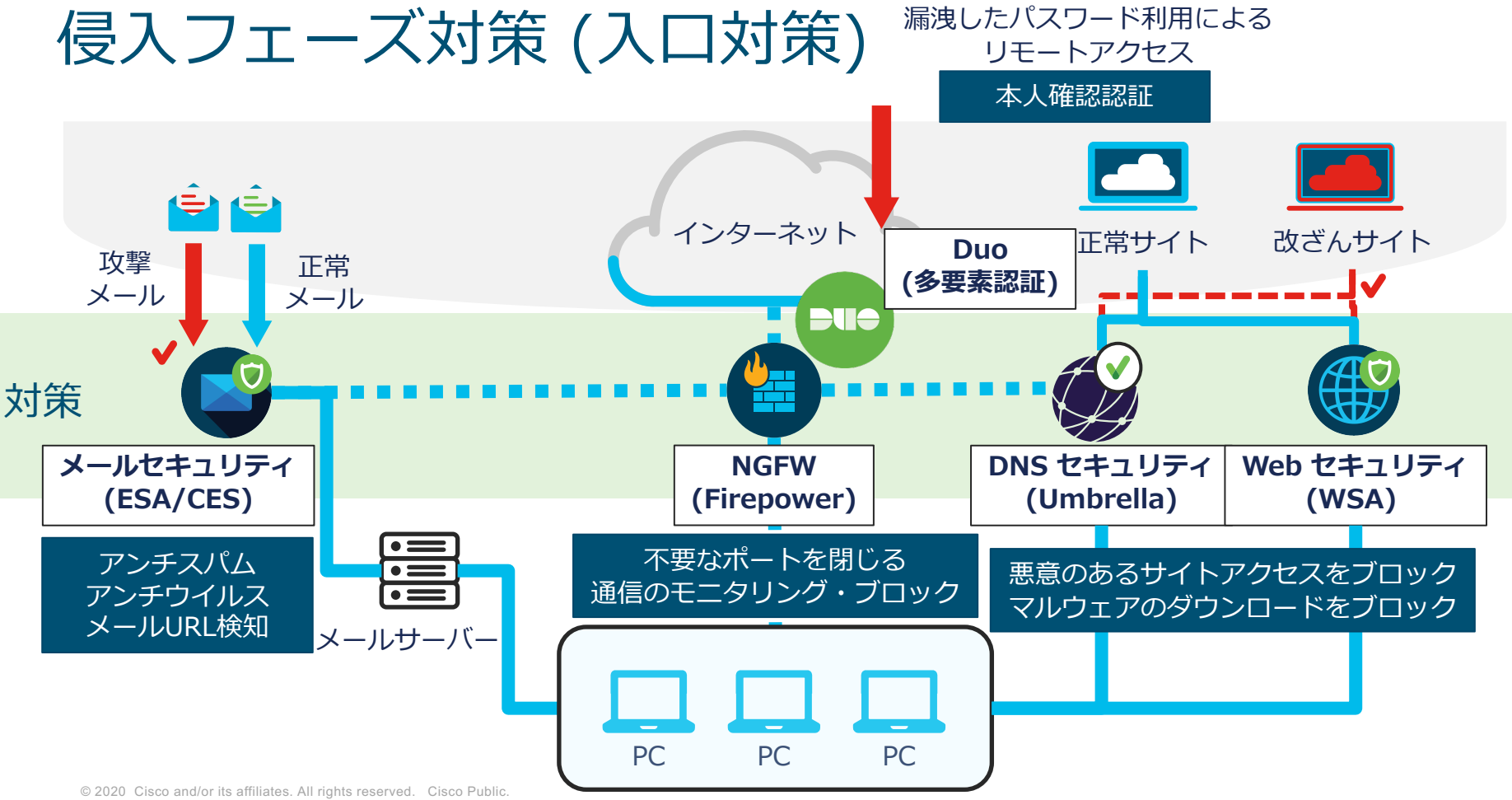
2020年8月24日 20:00 (2020年8月25日 5:33 更新) ［有料会員限定記事］

国内の38社が不正アクセスを受け、
テレワークに欠かせない社外接続の暗証番号が流出した恐れがあることが分かった。
第三者が機密情報を抜き取ったり、ウイルスをばらまいたりする2次被害が予想される。
事態を重く見た内閣サイバーセキュリティセンター（NISC）も調査に乗り出しており、
企業は対策が急務となっている。



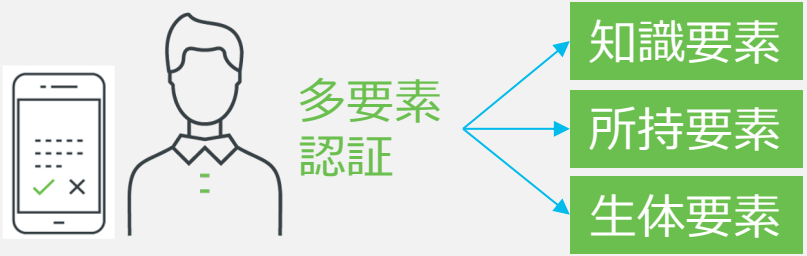
https://r.nikkei.com/article/DGXMZO62994110U0A820C2MM8000?s=5

侵入フェーズ対策 (入口対策)

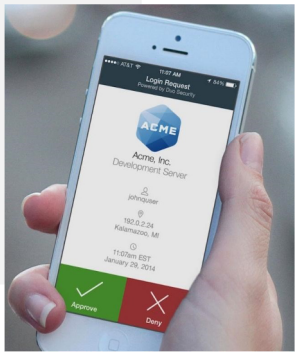


多要素認証とは？
MFA（Multi-Factor Authentication）

高度なユーザー認証



＜例＞
知識要素に所持要素を加える
パスワード入力後、デバイスプッシュを送り、
ワンタップで承認



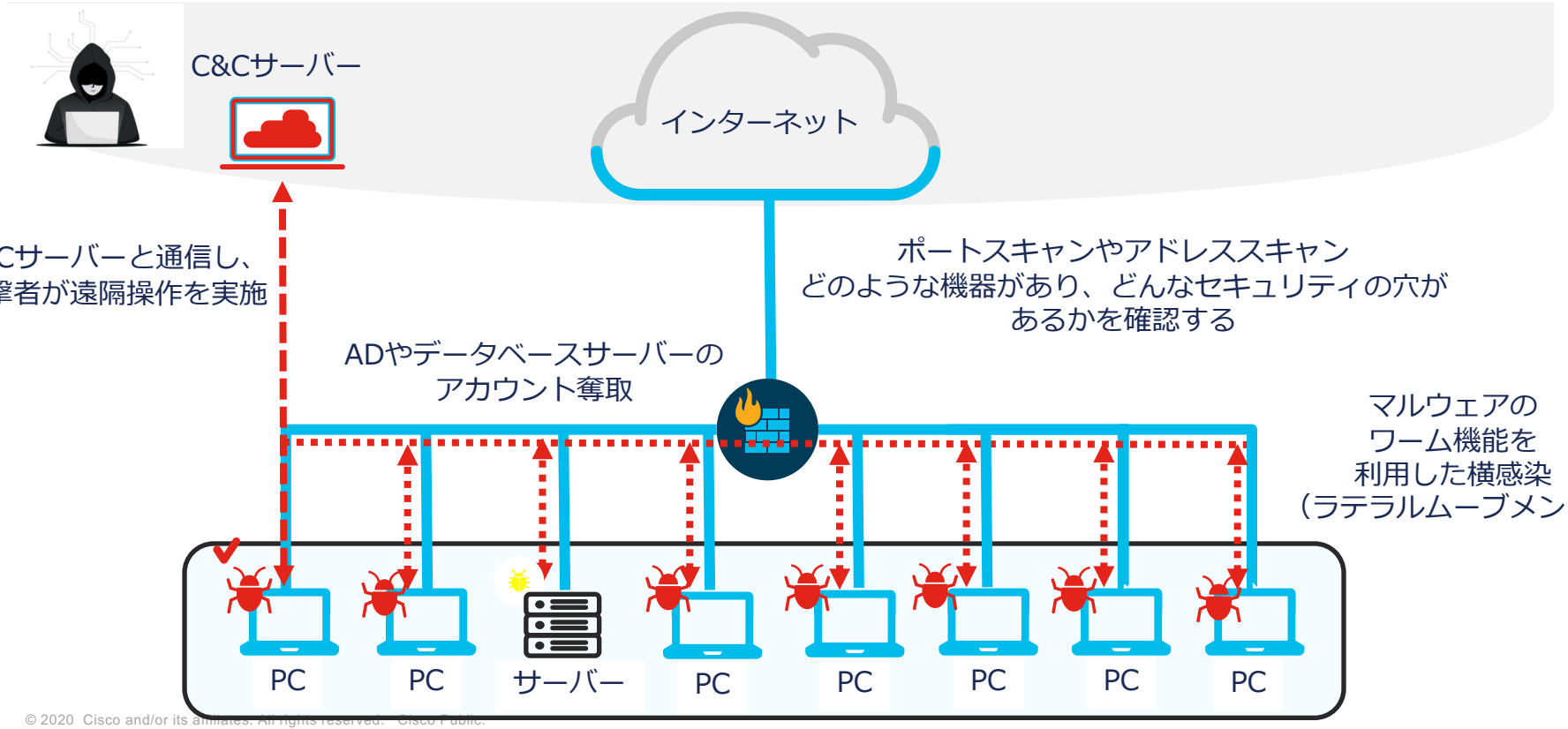
1. 知識要素
   ユーザーが知っていること
   （例：ID・パスワード、秘密の質問）

2. 所持要素
   ユーザーが持っているもの
   （例：スマホ、ハードウェアトークン）

3. 生体要素
   ユーザー自身の特徴
   （例：指紋、顔、虹彩）

基盤構築・諜報活動フェーズの手法と対策

基盤構築・諜報活動フェーズ手法



基盤構築・諜報活動フェーズ手法

- バックドア、C&C サーバー、ボットネットを利用しての端末操作
- ワーム機能を用いたマルウェアの拡散(例：SMBの脆弱性を利用したWannaCry)
- ネットワーク内端末のIPアドレススキャン、ポートスキャン
- ADなどサーバーの管理者アカウント権限取得

セキュリティ製品での不正プログラム・通信の防御が必要。
また、**通常時とは異なる通信が発生した際のアノマリー分析が重要となる。**

標的型攻撃に対してのアノマリー分析の重要性

シグネチャ = パターンファイルなど、ブラックリストで定義

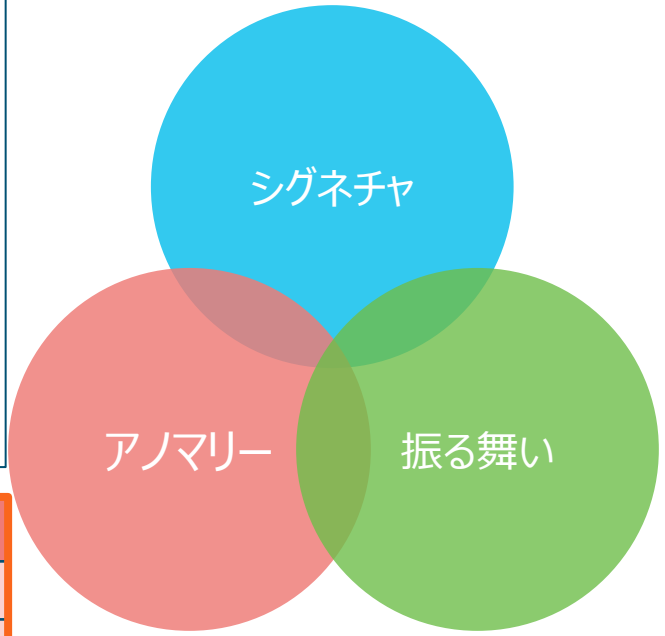
- ウイルス対策ソフト、メールフィルタリング、Webフィルタリング

振る舞い = 明らかな不正な振る舞いを検知

- サンドボックス, ホストIPS

アノマリー = 単体では正規の処理だが、限度を超えた挙動を検知

- **NBAD**（Network Based Anomaly Detection）
  → Stealthwatch



	シグネチャ	振る舞い	アノマリー
既知の脅威	**BEST**	Good	Limited
ゼロデイの脅威	LimIted	**BEST**	Good
内部犯行	Limited	Limited	**BEST**

Cisco Stealthwatch アノマリー分析が可能な製品

通常時のトラフィックをベースラインと学習し、そこから逸脱した通信を検出
ポートスキャンなどの偵察行為、ブルートフォース（辞書攻撃）など、特的アルゴリズムに該当した脅威も検知

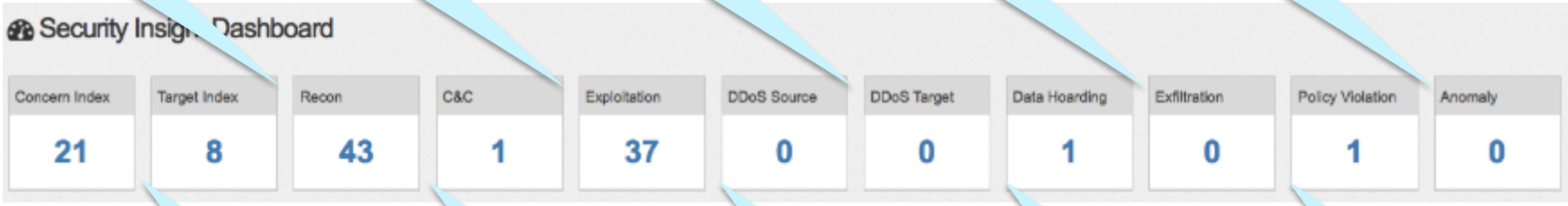
Recon
攻撃前に行われる偵察行為

Exploitation
マルウェア拡散等のホスト通信

DDoS Target
DDoS攻撃の対象ホスト

Exfiltration
外部への情報漏洩行動

Anormaly
異常行動のホスト件数



Concern Index
閾値を超えたホストの行動

Target Index
攻撃対象となっているホスト

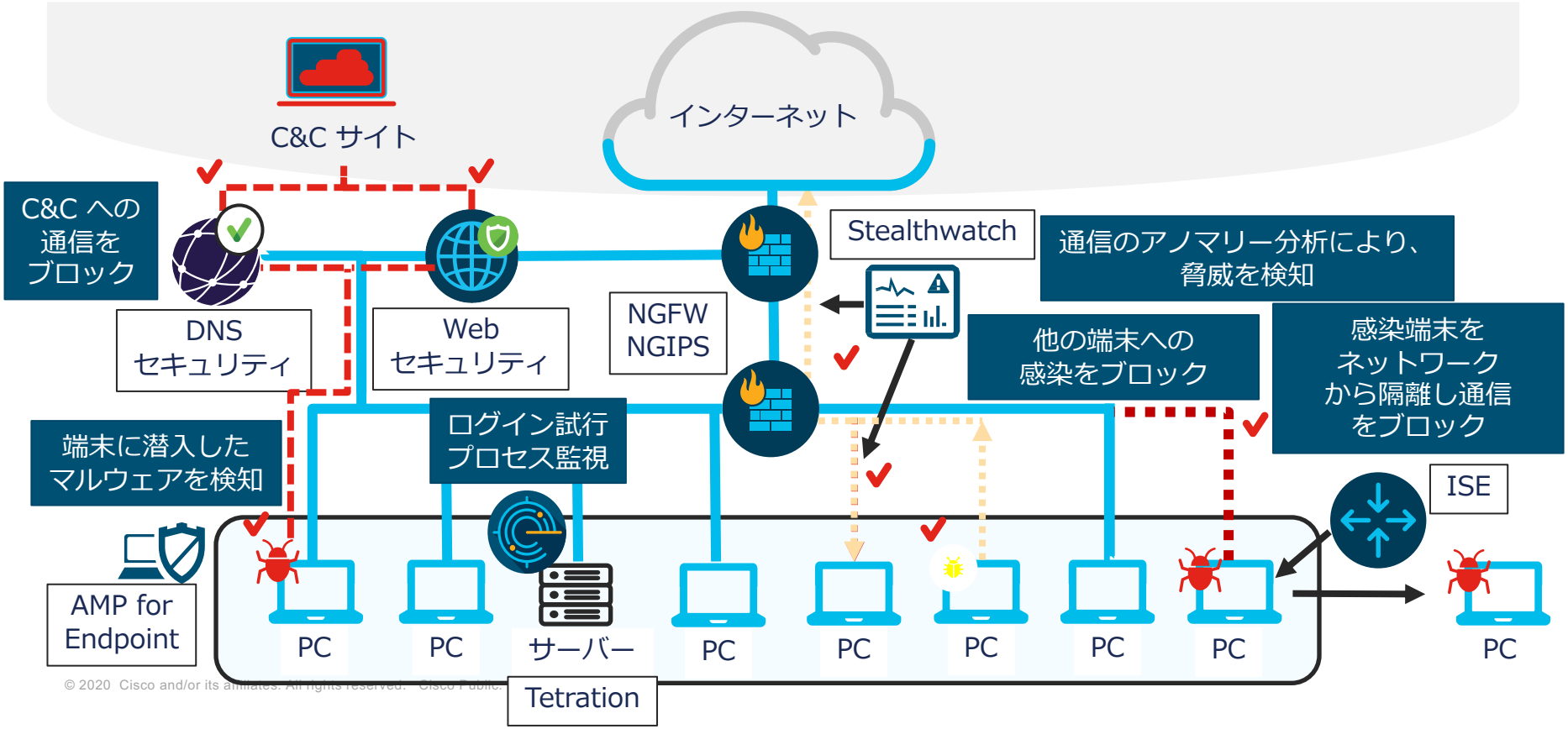
C&C
C&Cに接続しているホスト

DDoS Source
DDoS攻撃の発信元ホスト

Data Hoarding
内部での情報漏洩行動

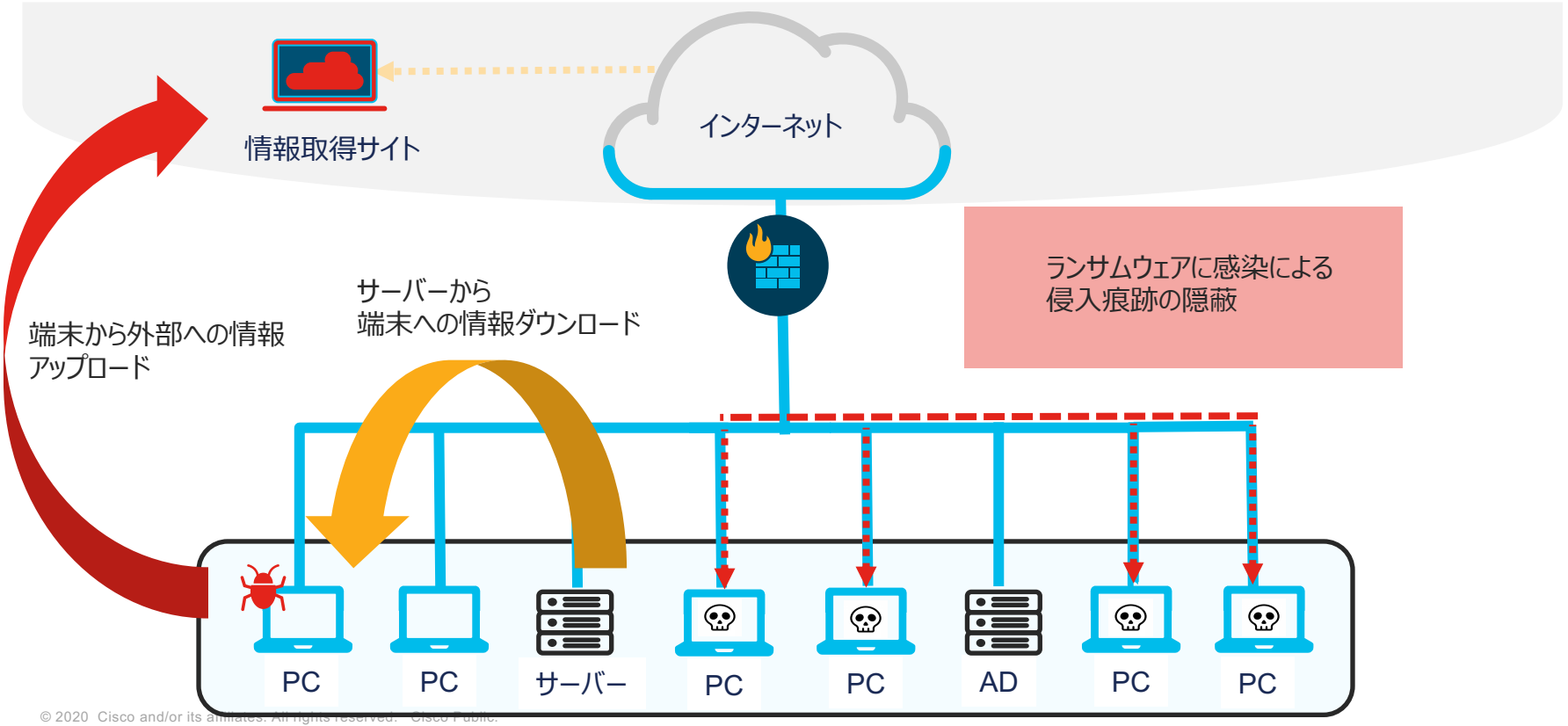
Policy Violation
通常を超えるデータ量違反

基盤構築・諜報活動フェーズの対策



目的遂行フェーズの手法と対策

目的遂行フェーズの手法

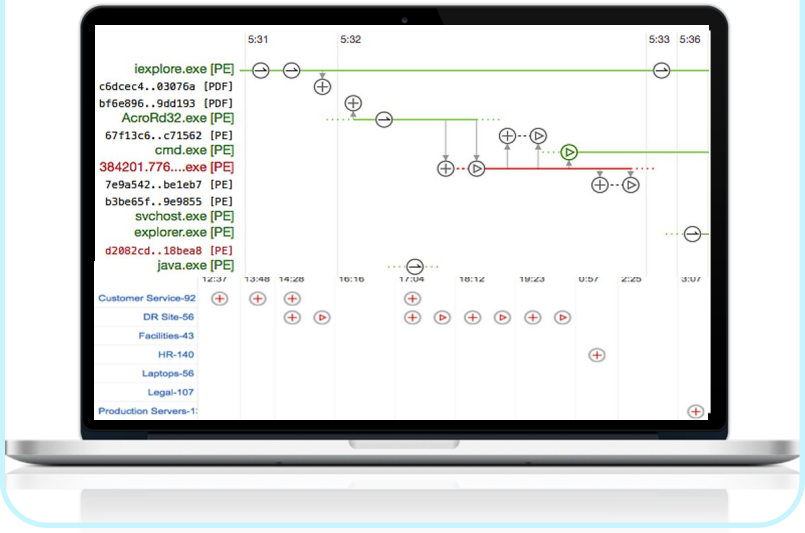


侵入痕跡の証拠隠滅
ランサムウェアをワイパーとして利用

- 標的型攻撃の最終段階
- 侵入や目的遂行までの手がかりとなるログを抹消することを目的として、ランサムウェアを利用するケースが多い。
  （データ暗号化して使えなくするランサムウェアはログ抹消に都合が良い）
- ADの管理者権限を奪取している場合は、グループポリシーのスタートアップスクリプトを利用して、イベントログ削除コマンドやランサムウェアを実行させ、端末・サーバーのログを消去（ワイプ）する。
- システム担当者はランサムウェア感染復旧に全力を注ぎ、業務復旧で安心してしまう。⇨ 標的型攻撃をカモフラージュする効果にもなる

エンドポイント対策の重要性

- クライアント　AMP for Endpoints
  既知のマルウェア対策：アンチウイルス
  未知のマルウェア対策：サンドボックス
  感染経路や被害範囲特定：EDR



- サーバー Tetration
  マイクロセグメンテーション（アプリのホワイトリスト化）
  ハッキングの兆候検知

脆弱性の検知

- CVEベースでの脆弱性表示
- 脆弱プロセスの振る舞い検知
- ハッシュ値検査

プロセスの振る舞い検知

- ログイン試行
- Shell Hack
- プロセス起動
- MITREベースの検知

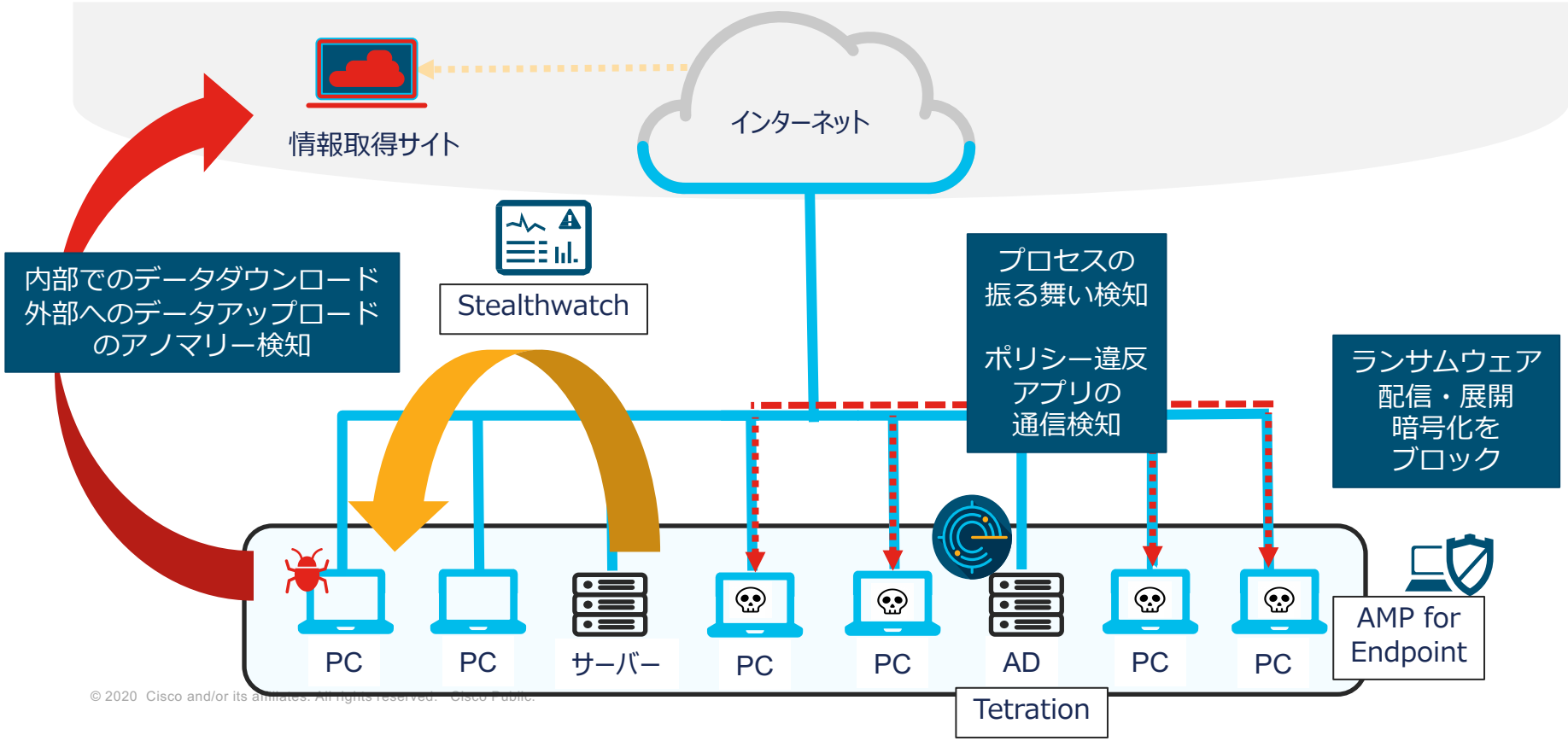
通信の制御

- アプリケーションに必要な通信のみ許可
- ポリシー違反通信の検知
- 任意のセキュリティ基準で隔離・通信制限

フォレンジック

- ログイン履歴
- 通信トラフィック履歴調査
- プロセス、コマンドの履歴調査

目的遂行フェーズの手法



まとめ　標的型サイバー攻撃 各フェーズの対策製品

対策箇所	入口・出口対策				内部対策	エンドポイント対策		認証		クラウド
製品種別	NGFW	Email	Web		Network	Client & Server	Server	User & Device	多要素	CASB
製品名	Firepower	ESA/CES	WSA	Umbrella (DNS)	Steatlhwatch	AMP4E	Tetration	ISE	Duo	Cloudlock
メール型マルウェア	○ AMP Option	◎				○				
Web型マルウェア	○ AMP Option	○ Mail URL	◎	◎		○				
認証情報の悪用								◎	◎	△ 対象SaaS
バックドア、C2接続	○		△ WEB通信の場合	○	○	○				
ネットワーク内部の諜報活動 (ポートスキャンなど)					○					
脆弱性攻撃(エクスプロイト)	○				○	○	○			
端末間での横感染					○	○	○			
端末からサーバーの侵入					○		○			
データ搾取・外部送信	△ 不正な宛先通信	△ Mail DLP Option	△ WEB通信の場合	△ 不正な宛先通信	○		○			△ 対象SaaS
データの破壊 （ランサムウェアによる暗号化など）	○				○	○	○			

◎…該当攻撃に特化した保護が可能
○…攻撃からの保護が可能
△…一部機能で対応


CISCO