Blue Planet-works
Safety for the Connected World

Security Insight

～セキュリティアドバイザーから見るサイバーセキュリティの裏側～

株式会社Blue Planet-works

セキュリティアドバイザー　鴫原祐輔

© 2022 Blue Planet-works, Inc.

自己紹介

組織：株式会社Blue Planet-works

部署：プロダクト＆テクニカルサービス本部

役職：セキュリティアドバイザー

氏名：鴫原祐輔（しぎはらゆうすけ）

期間	所属	略歴
2004年04月～2011年08月	株式会社インターネットイニシアティブ（情報・通信）	公共システム事業部のコンサルタントとして主に中央省庁の業務システムやネットワーク最適化事業に従事する。
2011年08月～2019年12月	株式会社シマンテック（サイバーセキュリティ）	パートナー営業本部に所属するセキュリティアドバイザーとして販売パートナーの育成やサイバーセキュリティに関する啓蒙活動に従事する。
2019年12月～現在	株式会社Blue Planet-works（サイバーセキュリティ）	セキュリティアドバイザーとしての活動範囲を広げるためにシマンテックを離れ、引き続きサイバーセキュリティに関する啓蒙活動に従事する。

© 2021 Blue Planet-works, Inc.

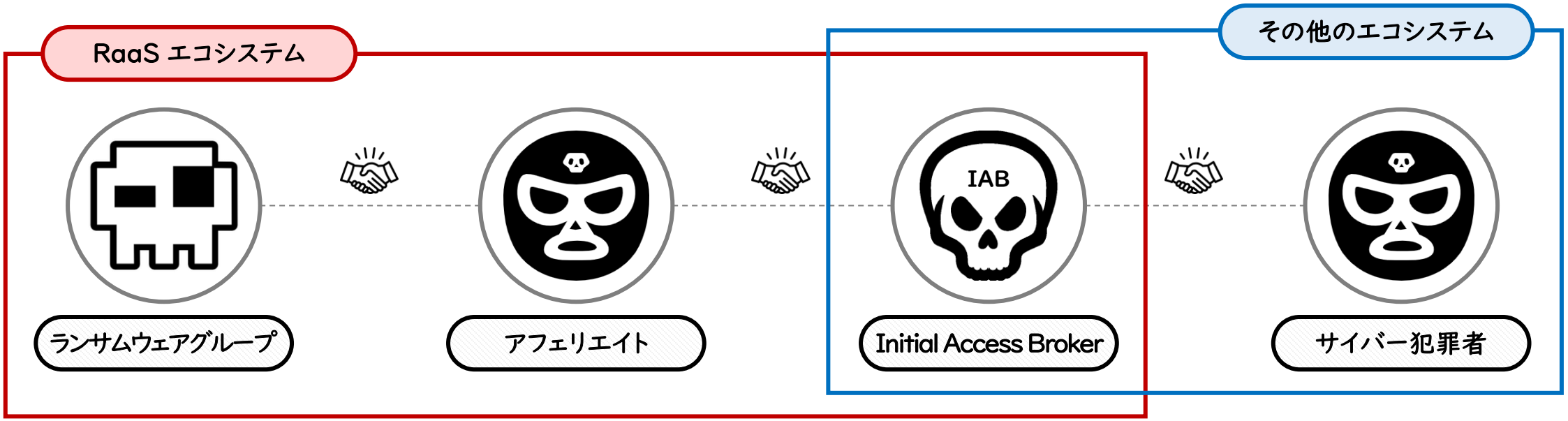
Blue Planet-works
Safety for the Connected World

2021年のサイバーセキュリティ動向を振り返る #1

- サイバー犯罪の中核を担うInitial Access Brokerの台頭 -

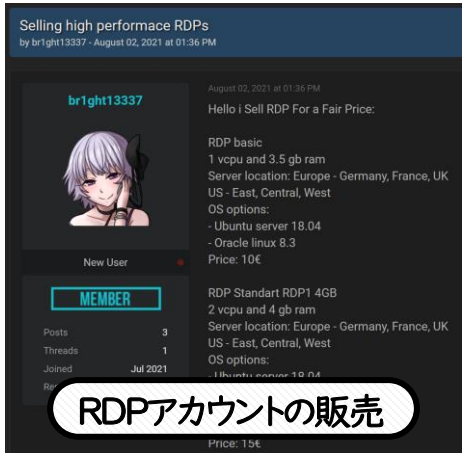
© 2022 Blue Planet-works, Inc.

ランサムウェアグループが構築したRaaSエコシステムとIAB



IAB（Initial Access Broker）とは

- サイバー攻撃において攻撃対象のネットワーク又はシステムに侵入するための経路（Initial Access）を確立して、その権利を他の攻撃者へ販売している。
- Initial Access Brokerが販売するリストを購入する最大ユーザーはランサムウェアグループであり、今やサイバー攻撃の中核的な役割を担う存在となっている。



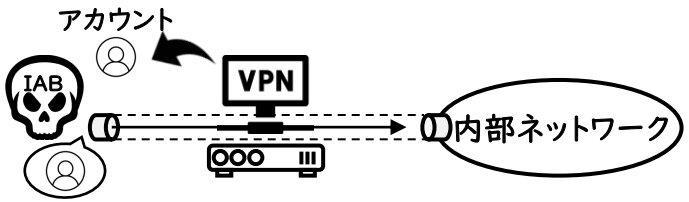
© 2022 Blue Planet-works, Inc.

IABは脆弱性ネットワークやシステムを探し出す

Blue Planet-works
Safety for the Connected World

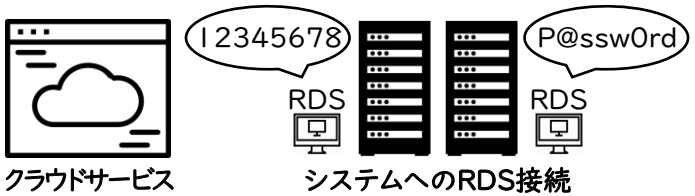
IABが狙う脆弱なシステムやネットワーク

脆弱なリモートアクセス環境



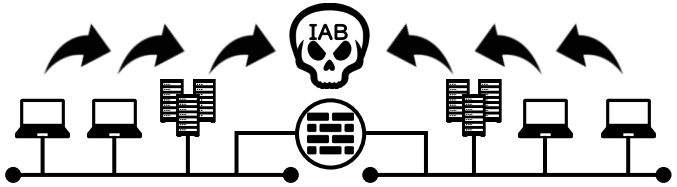
脆弱性が解消されていないリモートアクセス装置だけでなく、接続時に多要素認証を用いていない。

脆弱な認証システム



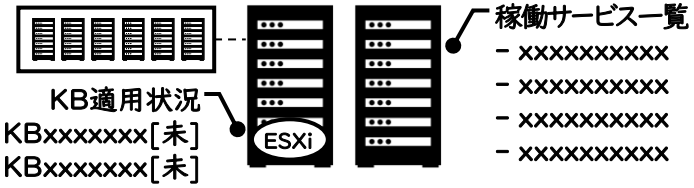
多要素認証化されておらず、推測されやすいパスワードによって認証することができるシステムが存在している。

セグメント・通信設計の不備



同一セグメント内に端末とシステムが存在していたり、セグメント間における通信制御がほとんど行われていない。

脆弱な環境のシステム



緊急性の高いセキュリティパッチが適用されておらず、不必要なサービスがシステム上で稼働している。

IABが販売するリスト（業種別割合）

業種	割合
製造	9%
教育	9%
金融サービス	9%
貿易	7%
ヘルスケア	7%
専門サービス	6%
情報技術	5%
政府	5%
運輸	5%
天然資源	5%
不動産	4%
業種不明	11%
その他	18%

万遍なく取り扱いがある

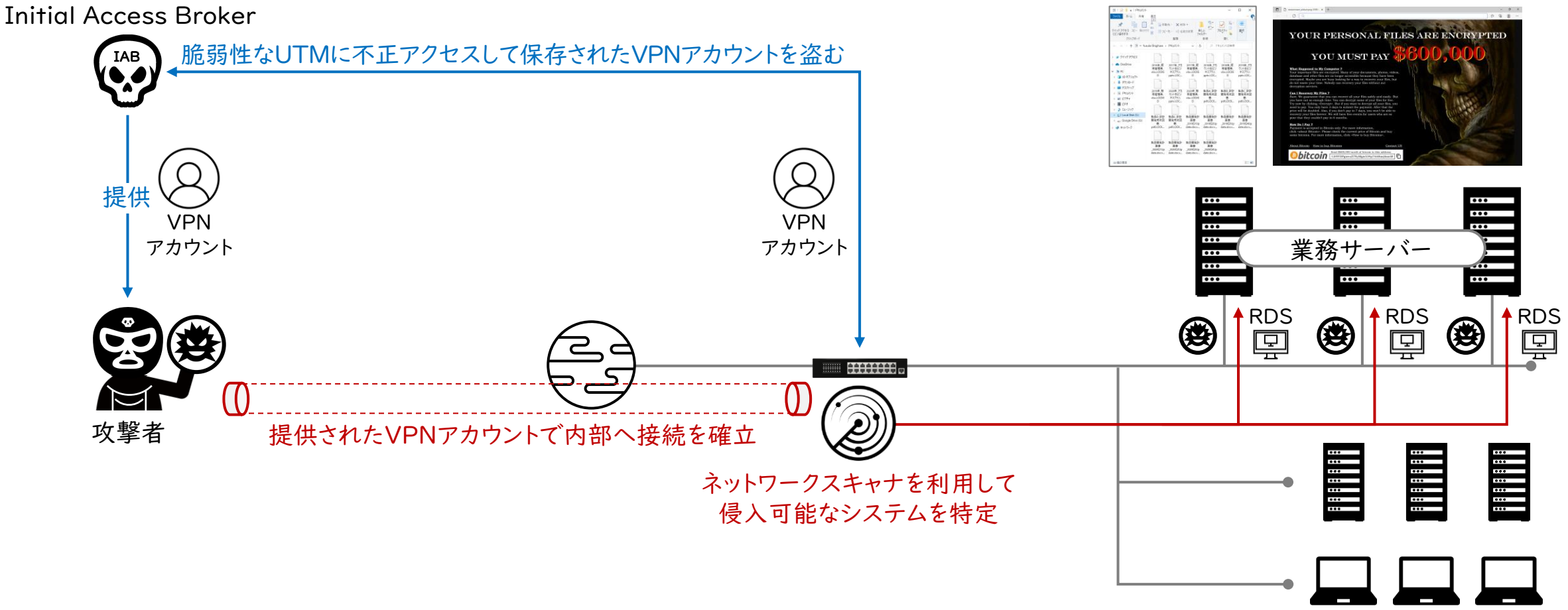
出典：Group IB：https://www.group-ib.com/media/gib-2021-2022-report/

© 2022 Blue Planet-works, Inc.

クライアントを踏み台にすることなくシステムを攻撃可能に

Blue Planet-works
Safety for the Connected World

脆弱なVPN装置からアカウントを窃取することで端末を介さずサーバーへ直接攻撃を仕掛けることが可能となる

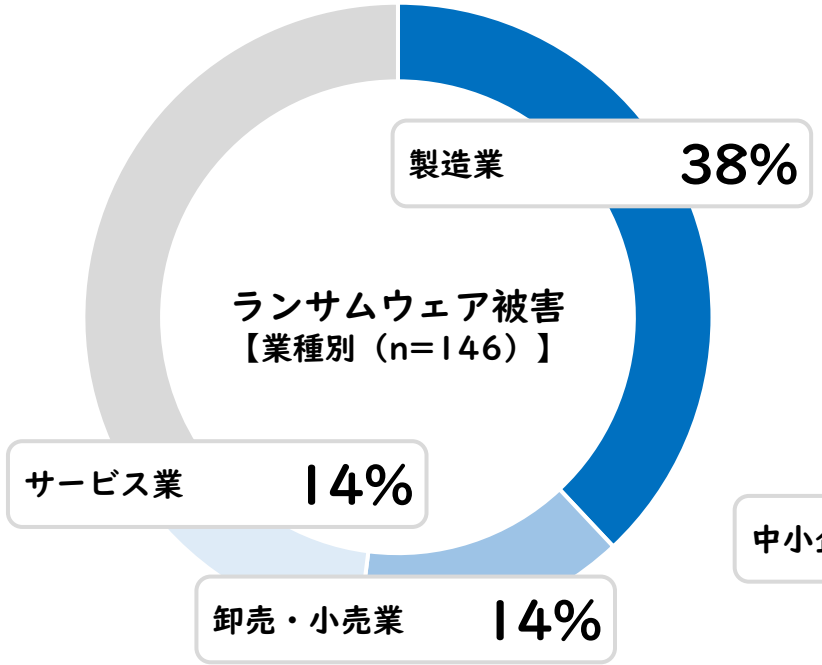


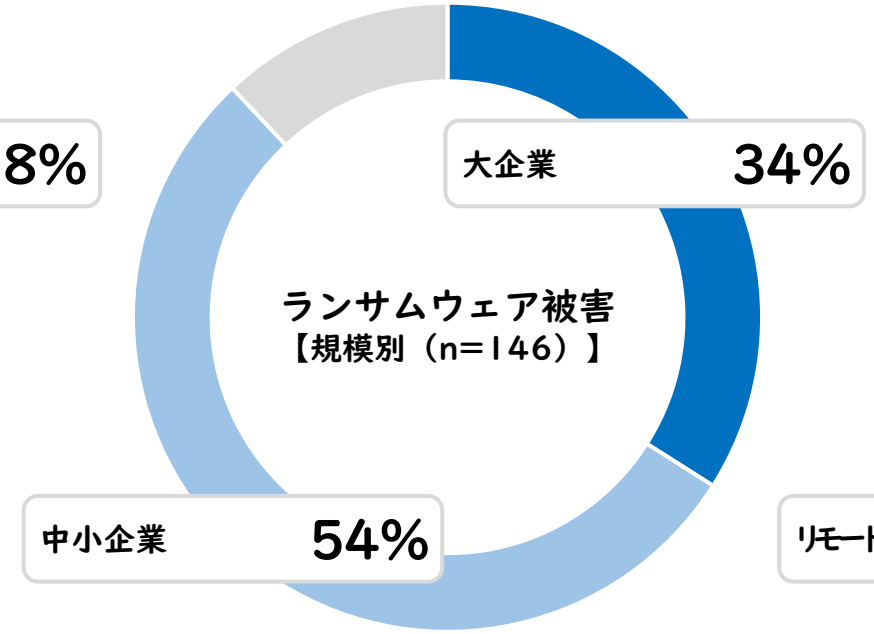
© 2022 Blue Planet-works, Inc.

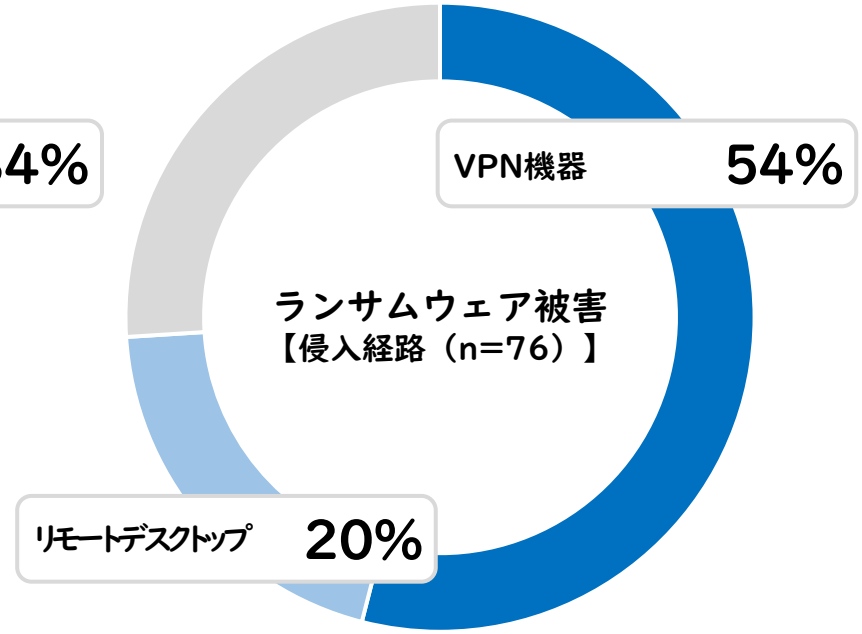
国内におけるランサムウェア被害の侵入経路にIABの影

国内におけるランサムウェア被害状況

- IBM Securityの調査においても国内におけるサイバー攻撃の対象となる業種別割合で製造業が第1位の23.2%（2021年）を占めている。※
- 狙われる理由としてはITとOTの境界が曖昧になってきたことに起因（通信経路の確立、Windows OSの利用など）すると指摘する声がある。







出典：警察庁「令和3年におけるサイバー空間をめぐる脅威の情勢等について（速報版）」
出典：IBM Security X-Force Incident Response「X-Force脅威インテリジェンス・インデックス2022」

© 2022 Blue Planet-works, Inc.

Blue Planet-works
Safety for the Connected World

被害企業に見られる共通項

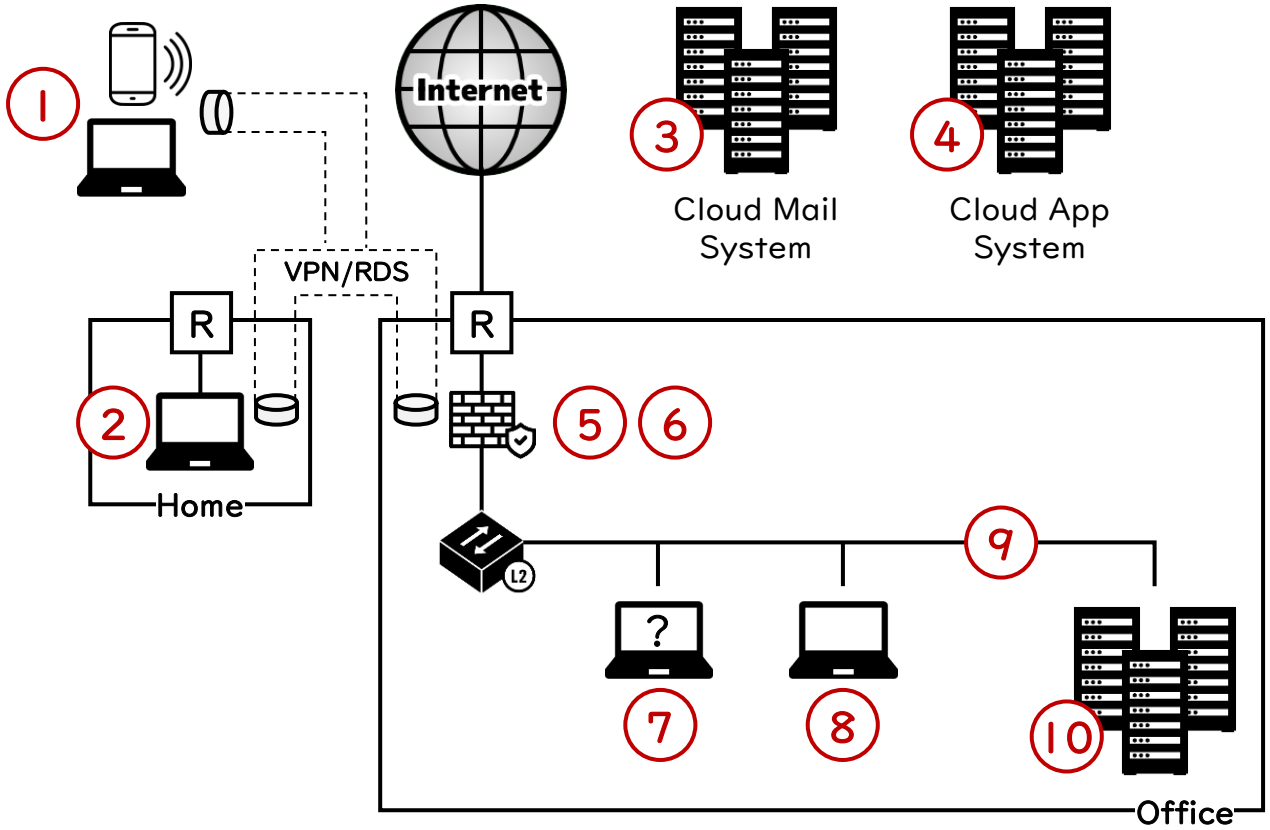
- Attack Surfaceを意識したセキュリティ設計や管理ができていない -

© 2022 Blue Planet-works, Inc.

Attack Surfaceとは何か？

Attack Surface（攻撃対象領域）

サイバー攻撃を受ける可能性がある攻撃点の総数を指します。この総数が多いということは、それだけサイバー攻撃者によって侵害されるリスク（データの破壊、窃取、エンドポイントの乗っ取られる確率）が高くなります。サイバーセキュリティ対策においては、攻撃者から見える自組織の状態を的確に把握すると共に自組織を狙う攻撃者を認識した上で適切な対策を施すことが求められます。



▼Attack Surfaceの例

①	直接インターネットに接続される端末（PC、モバイルなど）
②	脆弱なネットワーク環境下に置かれた業務端末
③	2段階認証が実装されていない脆弱性なメールシステム
④	アプリケーションに対する設定ミス、未認可のクラウドアプリケーション
⑤	外部からの不必要な通信が通過可能な設定
⑥	脆弱性が解消されていないネットワーク装置
⑦	資産としては認識されていない未認可の端末
⑧	脆弱性が解消されていない業務端末
⑨	適切なセグメント設計が施されていないネットワーク
⑩	脆弱性が解消されていないシステム

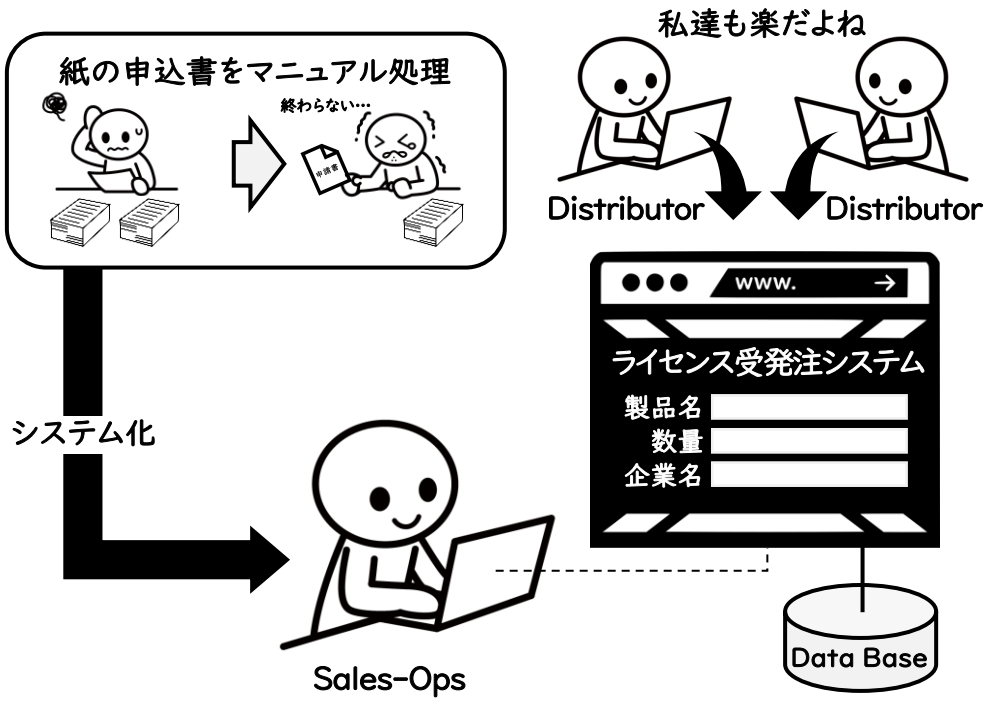
© 2022 Blue Planet-works, Inc.

IT化やDX化は組織のシステムへの依存度を高める

IT化やDX化の推進は攻撃対象領域を拡大させる要因であり システムへの依存度が高まればサイバー攻撃の影響も大きくなる

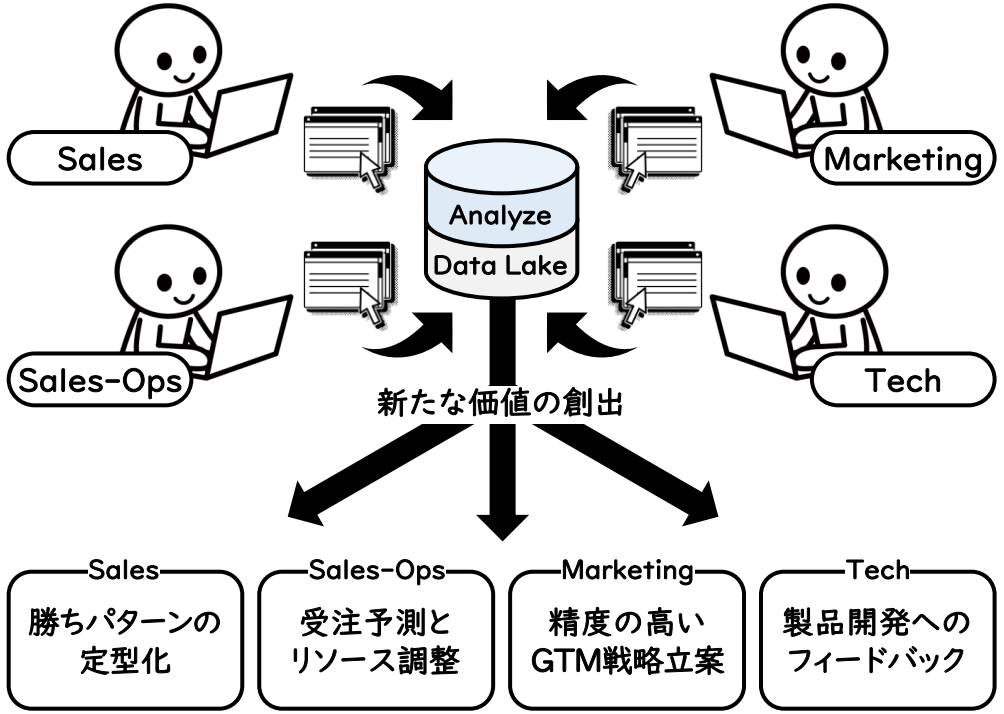
IT化の推進

アナログな仕組みを「IT」によって効率化・最適化



DX化の推進

情報を「IT」によりデータ化して新たな価値を創出



© 2022 Blue Planet-works, Inc.

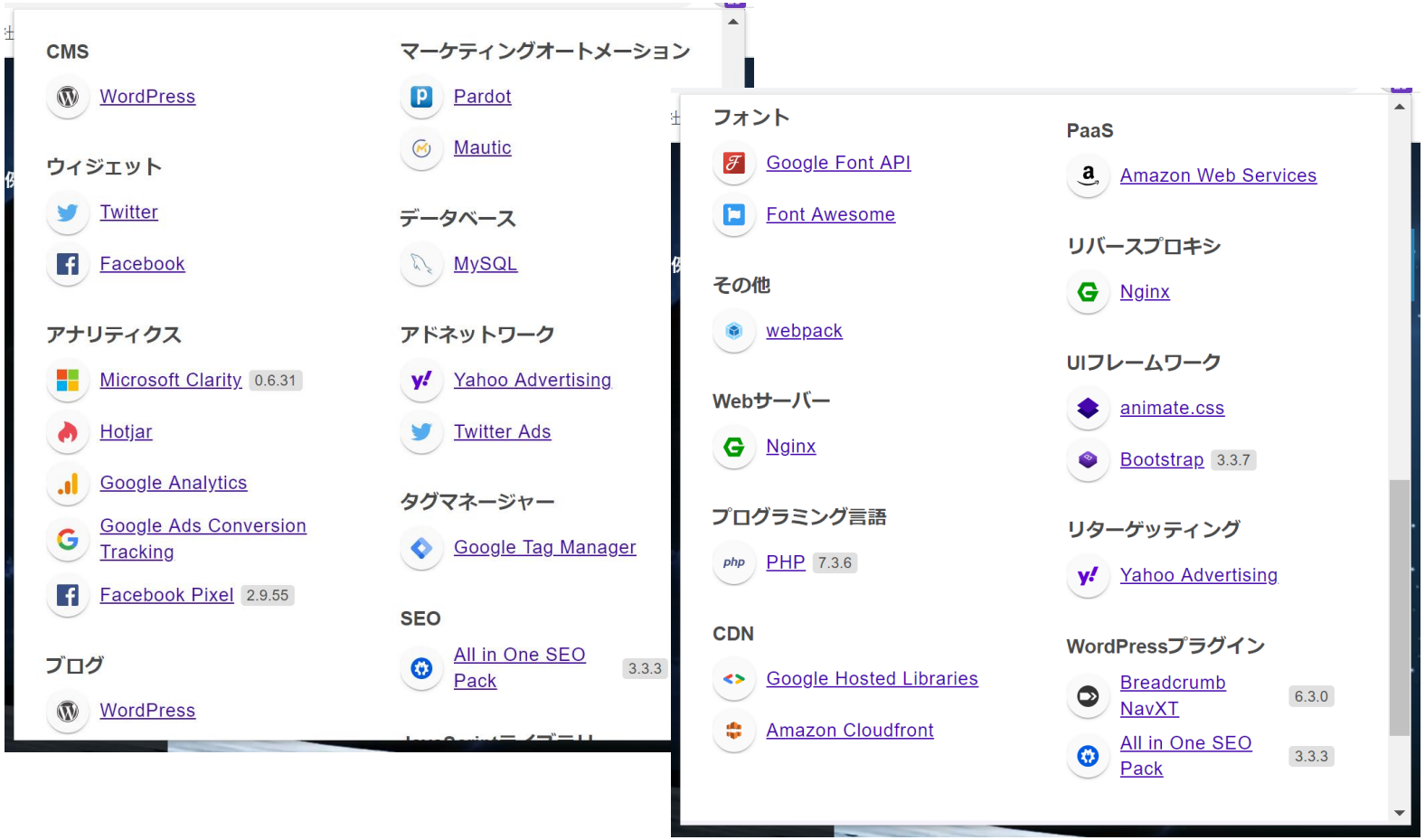
攻撃の糸口となる情報をインターネット上からどこまで探せるか #1

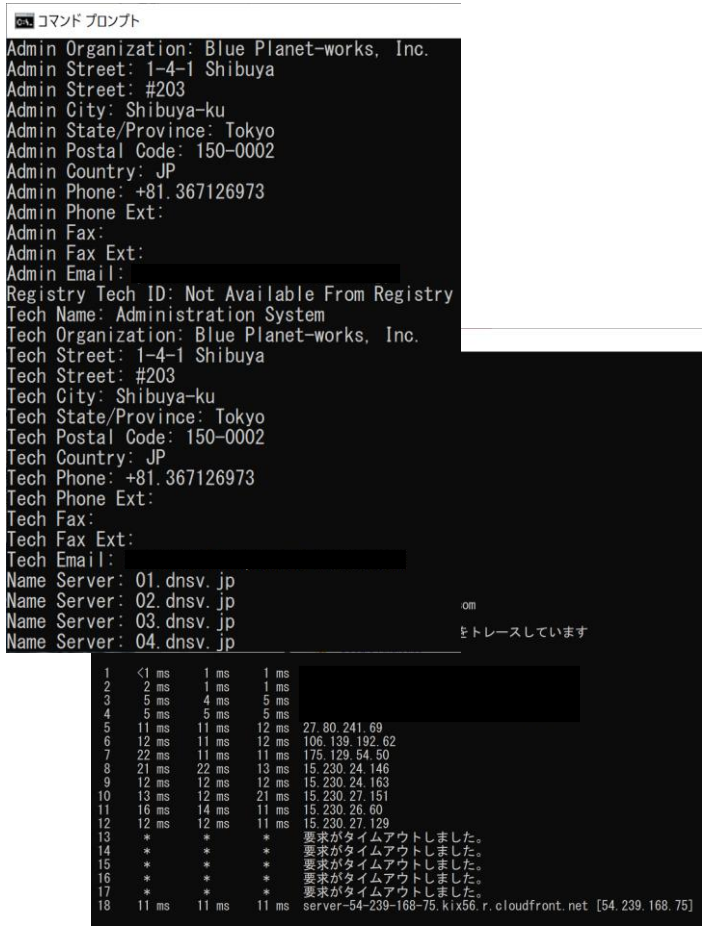
Blue Planet-works
Safety for the Connected World

▼www.blueplanet-works.com の情報を探索

GET 公開サーバーで利用しているインフラやその上で動作する各種アプリケーションの情報を取得

GET WHOISなどの公開データベース上から一部の個人情報及びメールアドレス等の情報を取得





© 2022 Blue Planet-works, Inc.

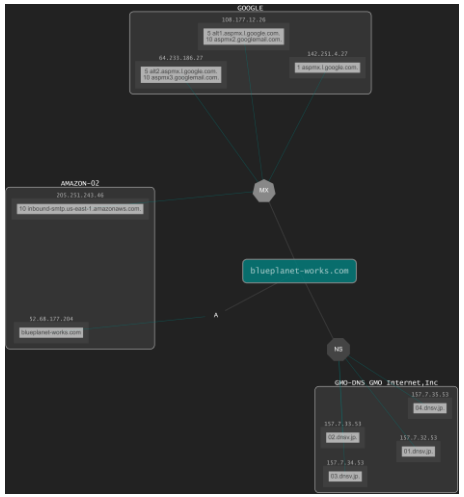
攻撃の糸口となる情報をインターネット上からどこまで探せるか #2

Blue Planet-works
Safety for the Connected World

▼Blue Planet-works のネットワークインフラ情報を探索

GET DNSサーバーのレコード情報から外部に公開されているサーバーの一覧を取得

GET MXレコードからGoogle Workspaceを利用していることを特定

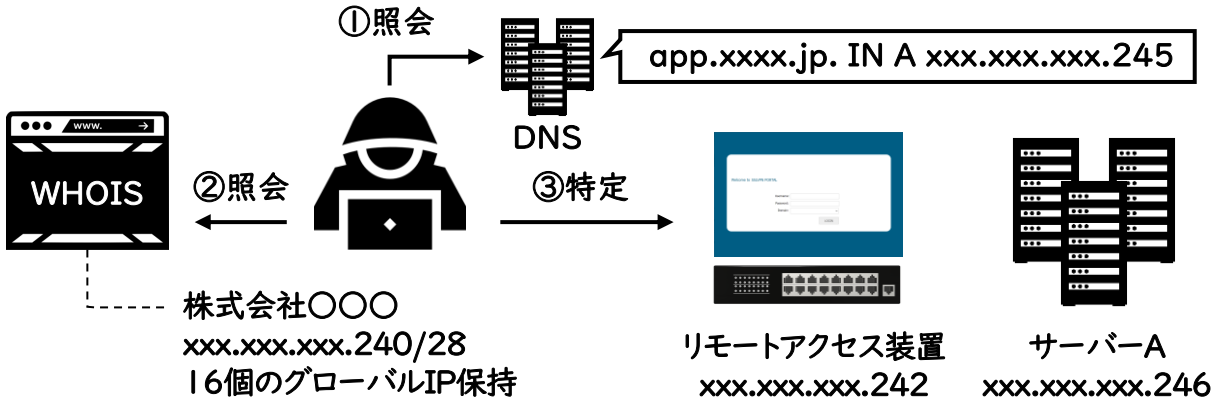


MX Records ** This is where email for the domain goes...

5 alt1.aspmx.l.google.com.	108.177.12.26 ua-in-f26.1e100.net	GOOGLE United States
5 alt2.aspmx.l.google.com.	64.233.186.27 cb-in-f27.1e100.net	GOOGLE United States
1 aspmx.l.google.com.	142.251.4.27 gm-in-f27.1e100.net	GOOGLE United States
10 aspmx2.googlemail.com.	108.177.12.26 ua-in-f26.1e100.net	GOOGLE United States
10 aspmx3.googlemail.com.	64.233.186.27 cb-in-f27.1e100.net	GOOGLE United States
10 inbound-smtp.us-east-1.amazonaws.com.	205.251.243.46 inbound-smtp.us-east-1.amazonaws.com	AMAZON-02 United States

【補足】

自組織のDMZ上でサーバー等を公開している場合、DNSサーバーのレコード情報から自組織に割り当てられたグローバルIPアドレス及びそのアドレス範囲が特定できる。このアドレス範囲に対してポートスキャンを実行することで各ホストのポートやその状態を外部から把握することが可能である。



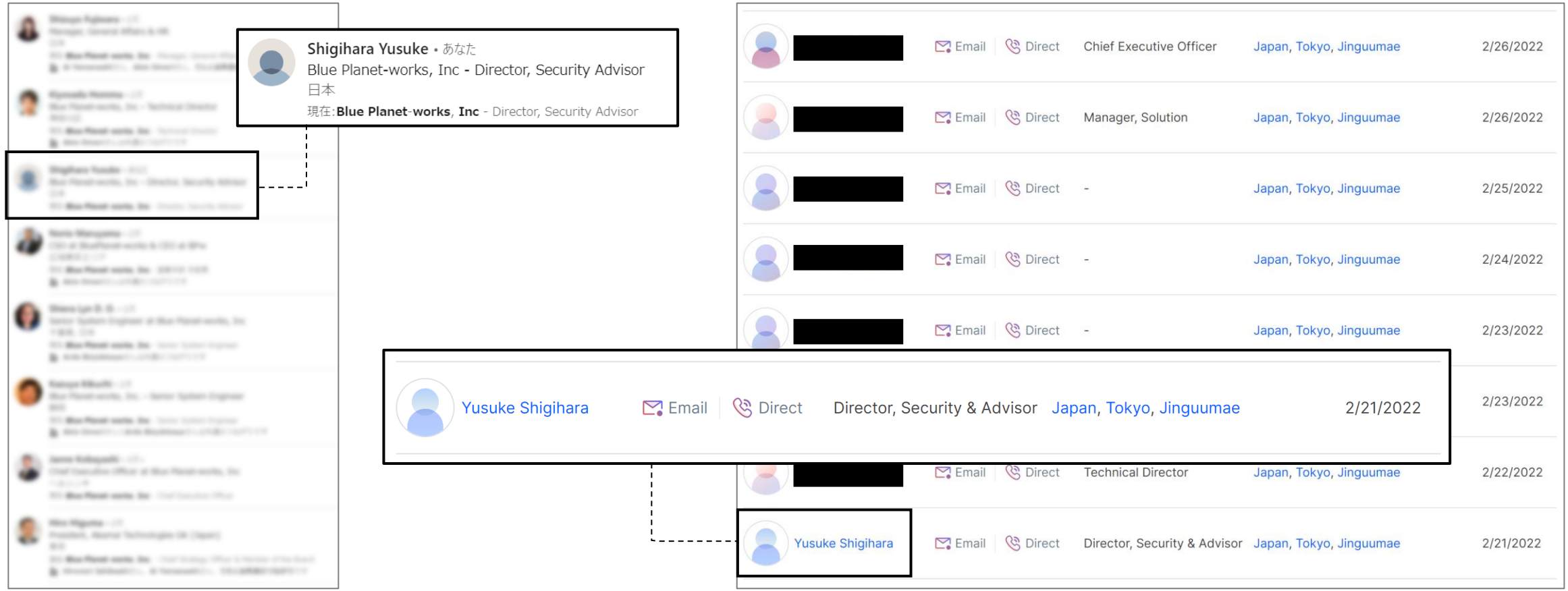
© 2022 Blue Planet-works, Inc.

攻撃の糸口となる情報をインターネット上からどこまで探せるか #3

Blue Planet-works
Safety for the Connected World

▼Blue Planet-works の従業員に関する情報を探索

- GET zoominfoを利用して従業員の氏名、所属、メールアドレス、電話番号を取得
- GET LinkedInで一部の従業員の顔写真や経歴に関する情報を取得
- GET 入手した情報からFacebook等のSNSアカウントをある程度特定することが可能



注:zoominfo及びLinkedInは違法性のない合法的なクラウドサービスです。

© 2022 Blue Planet-works, Inc.

攻撃の糸口となる情報をインターネット上からどこまで探せるか #4

Blue Planet-works
Safety for the Connected World

▼30分で集まった Blue Planet-works に関連する情報

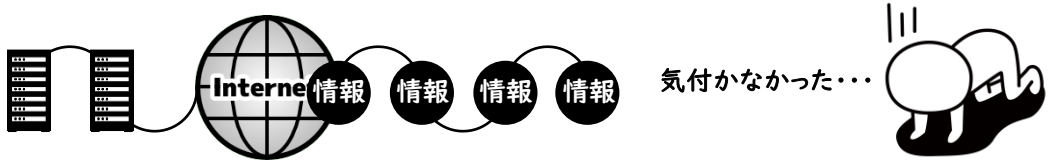
No.	対象	得られる有益な情報	攻撃への転用
1	ドメイン名	□ ドメイン登録時の責任者名 □ ドメイン登録用メールアドレス	□ ドメイン登録用メールアドレス宛にレジストラ（ドメインの登録代行事業者）を装い標的型攻撃メールを送る。
2	ウェブサイト	□ 利用しているCMS及び関連プラグイン □ 利用しているサーバーインフラ情報 □ 代表及び役員、一部従業員のフルネーム	□ 使用しているウェブアプリケーションやCMSの脆弱性を悪用した攻撃を仕掛けしてウェブサイトの改竄を試みる。 □ ウェブサーバーへDDoS攻撃を仕掛ける。
3	DNSサーバー	□ 利用しているメールサーバー（MXレコード） □ グローバルIPアドレスの割当範囲 □ グローバルIPアドレスが割り当てられたホスト一覧	□ メールサーバーのウェブメール機能に対して不正アクセスを仕掛ける。 □ 割り当てられたグローバルIPアドレスに対してポートスキャンを実行する。
4	グローバルIPアドレス	□ 利用しているプロバイダ情報 □ 公開サーバーやリモートアクセス装置等の存在 □ 開放されているポート及びその状態	□ リモートアクセス装置の設定不備を突いた不正アクセスや脆弱性を悪用してアカウント情報の窃取を試みる。 □ 公開サーバーへDDoS攻撃を仕掛ける。
5	企業DBやSNS	□ 従業員の個人情報（氏名、肩書、メールアドレス、写真など） □ 組織のメールアドレス命名規則 □ 従業員の交友関係	□ 従業員の属性情報を踏まえて標的型攻撃メール、SMS又はSNS内のDM機能を悪用して悪意あるメッセージを送信する。 □ クラウドサービスへの不正アクセスを試みる。

© 2022 Blue Planet-works, Inc.

攻撃者目線で自組織を調べてわかったこと

Blue Planet-works
Safety for the Connected World

意図せず公開されていた情報やシステム



×

見落とされた設定不備・脆弱性

非常に精度の高い攻撃が可能

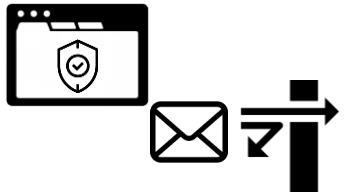
脅威を招き入れてしまうネットワークインフラやユーザー

脅威からの誘いに乗ってしまうユーザー

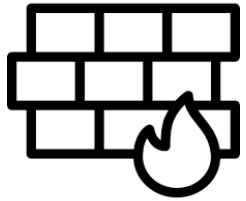
攻撃対象領域縮小への取り組み

Endpoint Security
（端末のセキュリティ）

Web/Email Security
（Web/Mailのセキュリティ）



Network Security
（ネットワークのセキュリティ）



Identity Security
（IDのセキュリティ）

Organizational/Human Security
（組織的/人的セキュリティ）

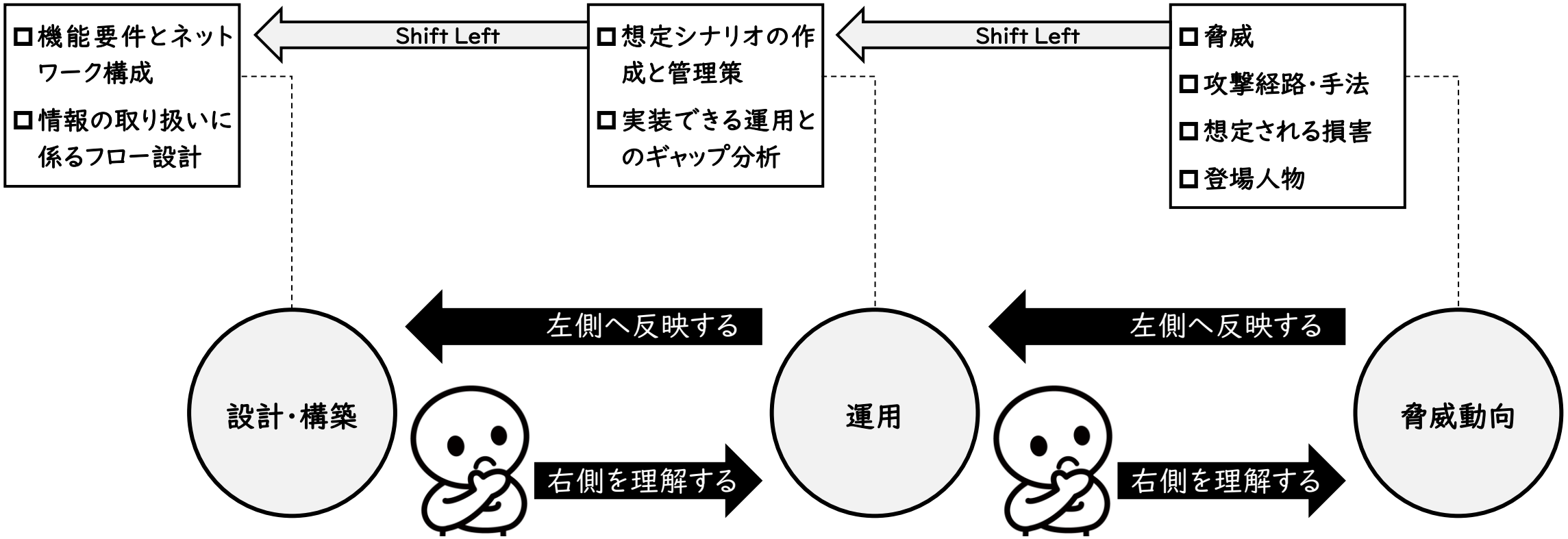
体制構築・人材配置

教育・意識向上

© 2022 Blue Planet-works, Inc.

Blue Planet-works
Safety for the Connected World

対症療法ではなく原因療法で
発生する可能性を取り除くための方策を設計レベルに落とし込む



© 2022 Blue Planet-works, Inc.

セキュリティ対策を考える上で重要となる管理策の前提

Blue Planet-works
Safety for the Connected World

1. 自身を知ること、敵から見える自身を知ること

守るべき対象を可視化し、それらが攻撃者にどのように見えているのか攻撃対象領域を把握することが重要

2. 想定されるシナリオを顕在化させないための抑止を行うこと

可視化された攻撃対象領域に対してユーザーが絡むシナリオについては意識させて抑止効果を高めていく必要がある

3. 抑止しきれないことを想定した防止策を打つこと

意識付けによる行動の変革を促すことは非常に難しいため、システム的にリスクの顕在化を阻止する技術的な対策が必要

4. 効果は結果の如何に関わらず記録して自身で認識すること

防止できている、防止できたことを検知できている、防止した事象の原因を特定できる、その発端を特定できる、改善できるか・・・

5. 認識されたことに対して組織として即応すること

記録・認識に留めるのではなく得られた状況に基づいて即座に改善を図る瞬発力のある管理・運用体制が必要

© 2022 Blue Planet-works, Inc.

Blue Planet-works
Safety for the Connected World

2021年のサイバーセキュリティ動向を振り返る #2

- 「Emotet」is back -

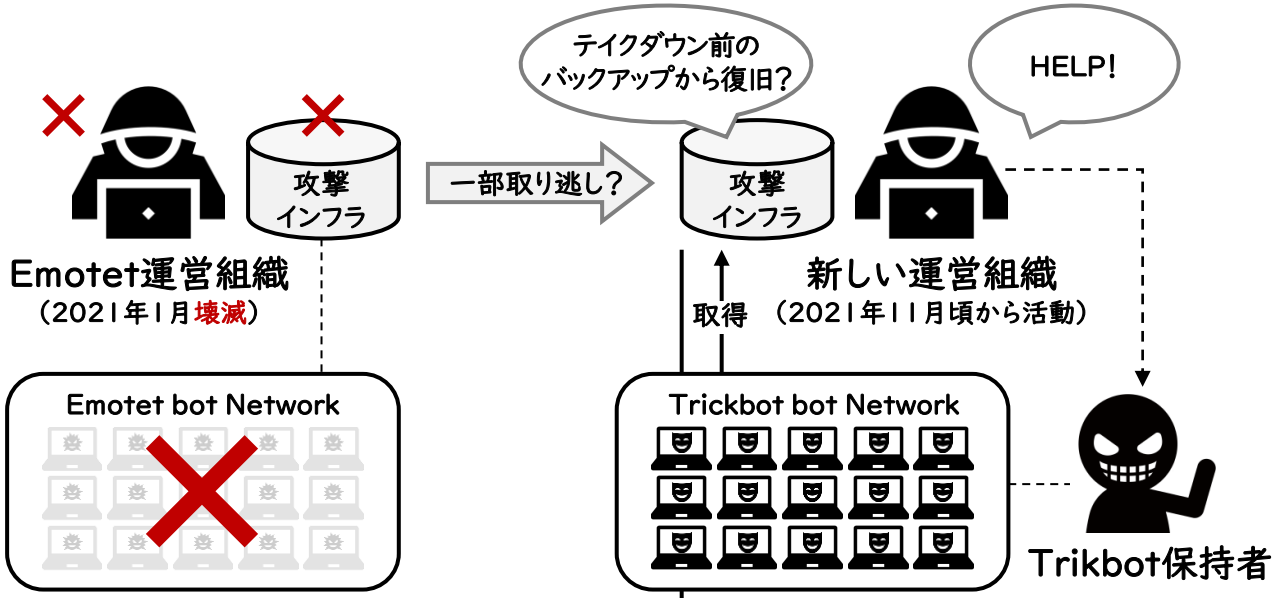
© 2022 Blue Planet-works, Inc.

テイクダウンから数ヶ月で復活した「Emotet」が拡散するまでの流れ

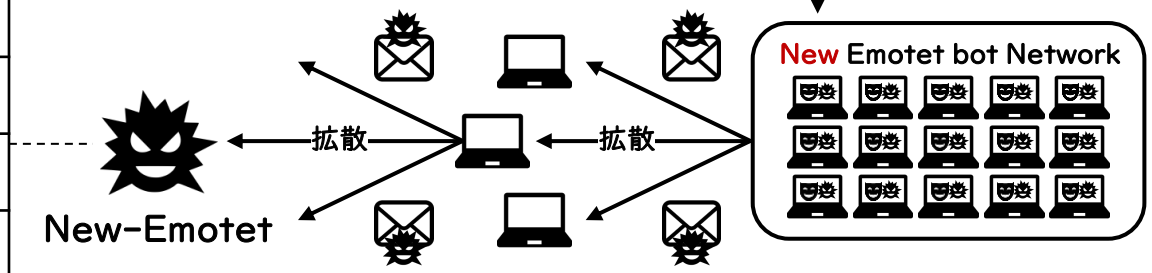
Blue Planet-works
Safety for the Connected World

Emotetが復活するまでの経緯

2021年1月27日にEUROPOL（欧州刑事警察機構）より「Emotet」テイクダウンの発表



Emotetが使う主な攻撃モジュール※	
NetPass	ログオンユーザーのシステムに保存されているネットワークパスワードを取得する。
Outlook scraper	Outlookアカウントから情報を取得して侵害アカウントから攻撃メールをばら撒く。
WebBrowsePassView	各ブラウザに保存されているパスワードを取得する。
Mail PassView	各メールソフトに保存されているアカウント情報（IDとパスワード）を取得する。
Credential enumerator	SMBを利用して書き込み可能な共有ドライブへ攻撃を拡散させる。



出典：CISA：https://www.cisa.gov/uscert/ncas/alerts/TA18-201A

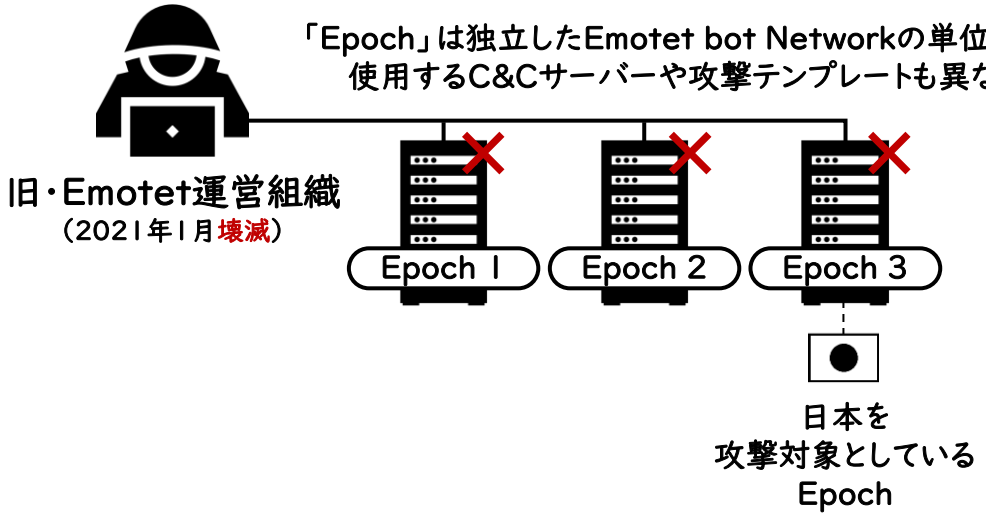
© 2022 Blue Planet-works, Inc.

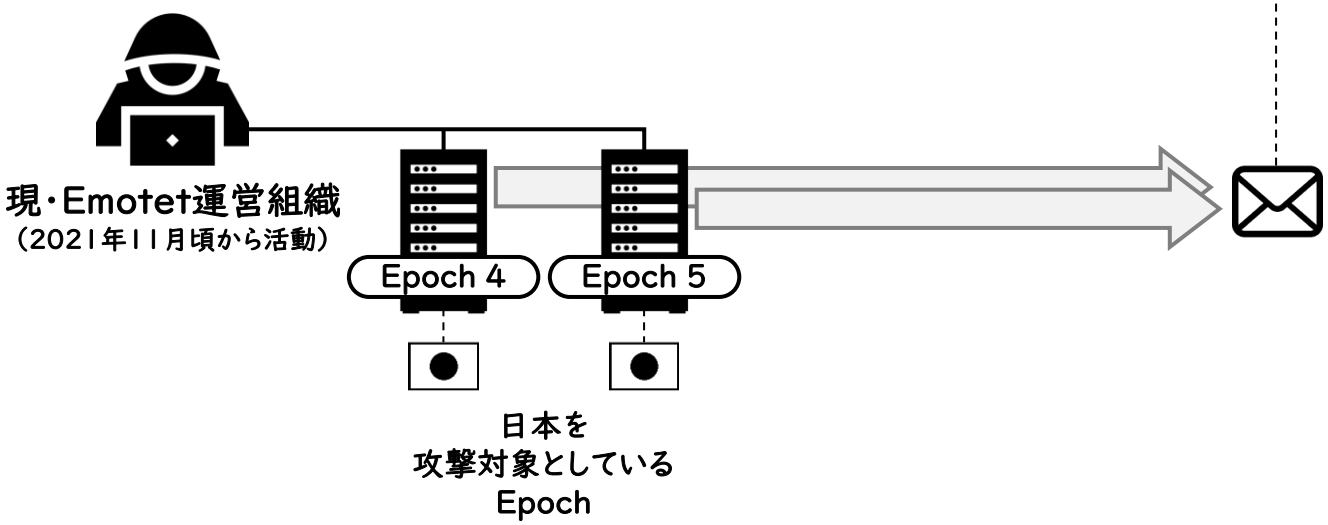
「Emotet」を配信するインフラについて

Emotetを配信するインフラと端末に着弾する理由の考察

注：本スライドの攻撃メールは例として筆者のメールアドレスを使っています。

「Epoch」は独立したEmotet bot Networkの単位であり
使用するC&Cサーバーや攻撃テンプレートも異なる

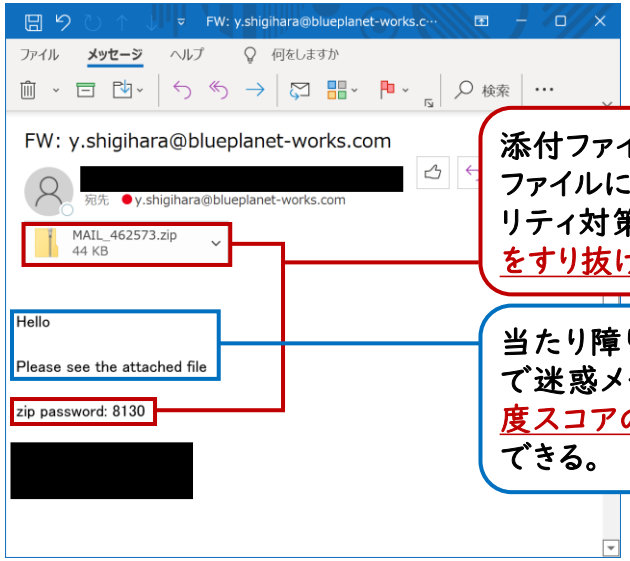




Emotetの感染誘発メールは「送信ドメイン認証」に対応（PASS）しているものが多いため、迷惑メールフィルタにおける信頼度スコアの低減が回避されている。

SPF:	PASS（IP: [redacted]）。 詳細
DKIM:	'PASS'（ドメイン: [redacted]） 詳細

SPF	差出人のメールアドレスが他のドメイン名になりすまされていないかを検証することができる。
DKIM	送信者が送信メールに電子署名を行い、受信者が署名検証することで送信元のドメインの正当性を検証することができる。



添付ファイルをパスワード付きZipファイルにすることで、メールセキュリティ対策のアンチウイルス機能をすり抜けることができる。

当たり障りのない文章を使うことで迷惑メールフィルタによる信頼度スコアの低減を回避することができる。

© 2022 Blue Planet-works, Inc.

「Emotet」の感染誘発メールを開かせるテクニック

Blue Planet-works
Safety for the Connected World

Emotetの感染誘発メールで使われる騙しのテクニックがレベルアップ

注：本スライドの攻撃メールは例として筆者のメールアドレスを使っています。

2021年11月頃から使われていた攻撃テンプレートの例

From: Yusuke Shigihara <y.shigihara@blueplanet-works.com>

Subject: RE:<受信者のメールアドレス>

MAIL_462574.zip

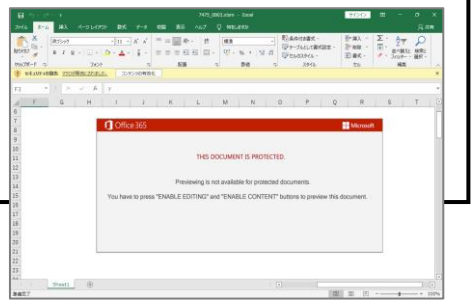
以下メールの添付ファイルの解凍パスワードをお知らせします。

添付ファイル名：MAIL_462574.zip

解凍パスワード：8130

Yusuke Shigihara

y.shigihara@blueplanet-works.com



2022年2月末頃から使われている攻撃テンプレートの例

From: Yusuke Shigihara <y.shigihara@blueplanet-works.com>

Subject: <受信者のメールアドレス>

MAIL_462574.xlsm

日頃より大変お世話になっております。

請求書を確認後、3営業日後の返金（着金）となります。

しかしながら、頂きましたご請求書ですが、3点修正が必要です。

①手数料が反映されておりませんでしたので、請求書に追記ください。（5%）

②請求書の発行日を記載してください

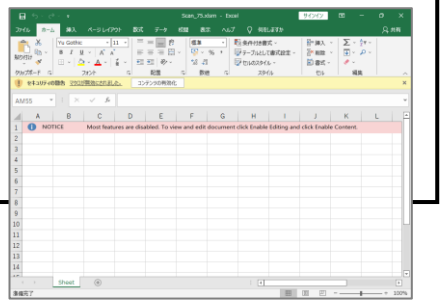
③弊社名は「{RCPT.DOMAIN-1-UP}」です、ご修正御願いします。

請求書到着日より3営業日後の着金となります。

宜しくお願いいたします。

Yusuke Shigihara

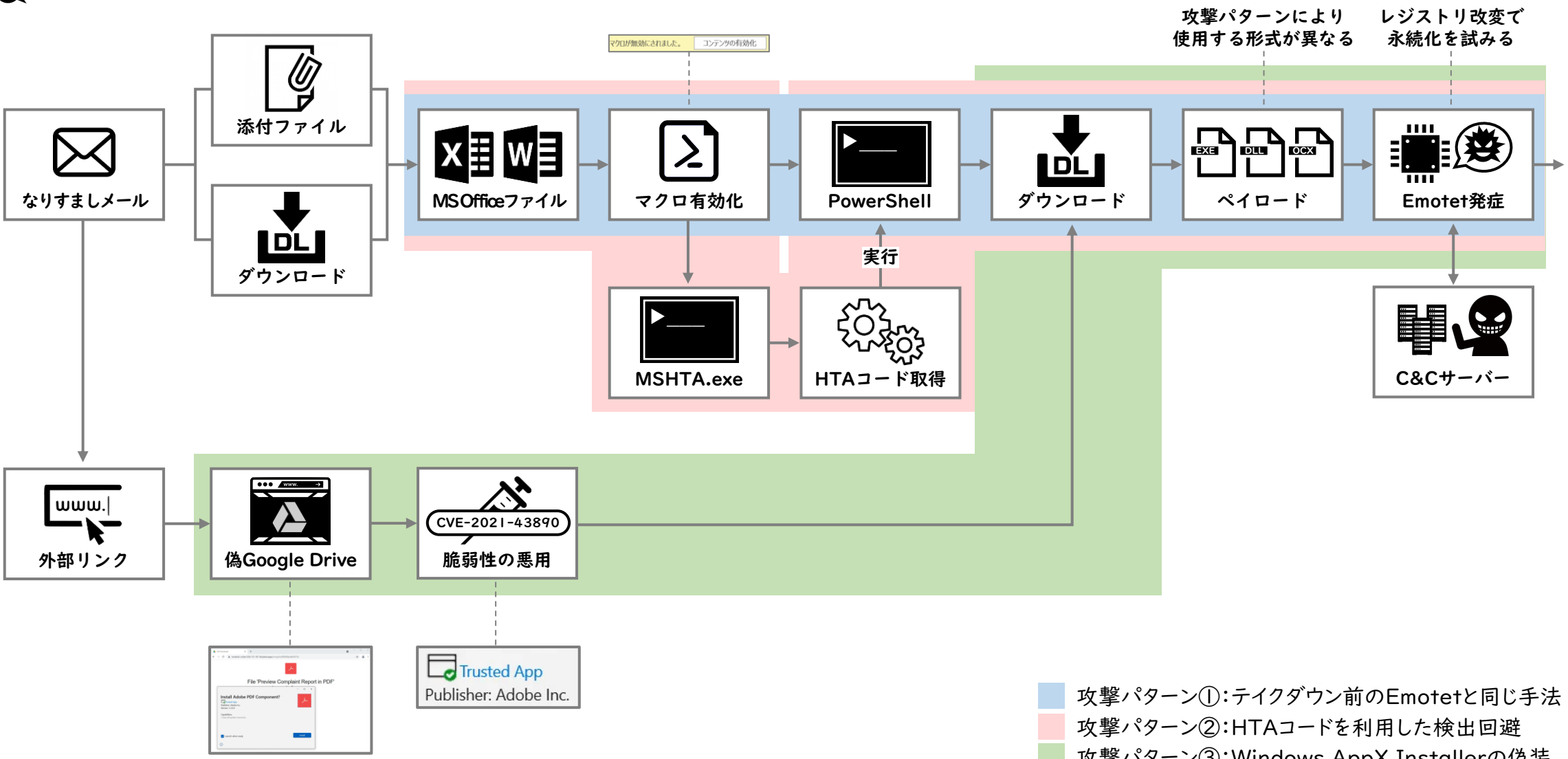
y.shigihara@blueplanet-works.com



© 2022 Blue Planet-works, Inc.

「Emotet」発症までの攻撃パターン

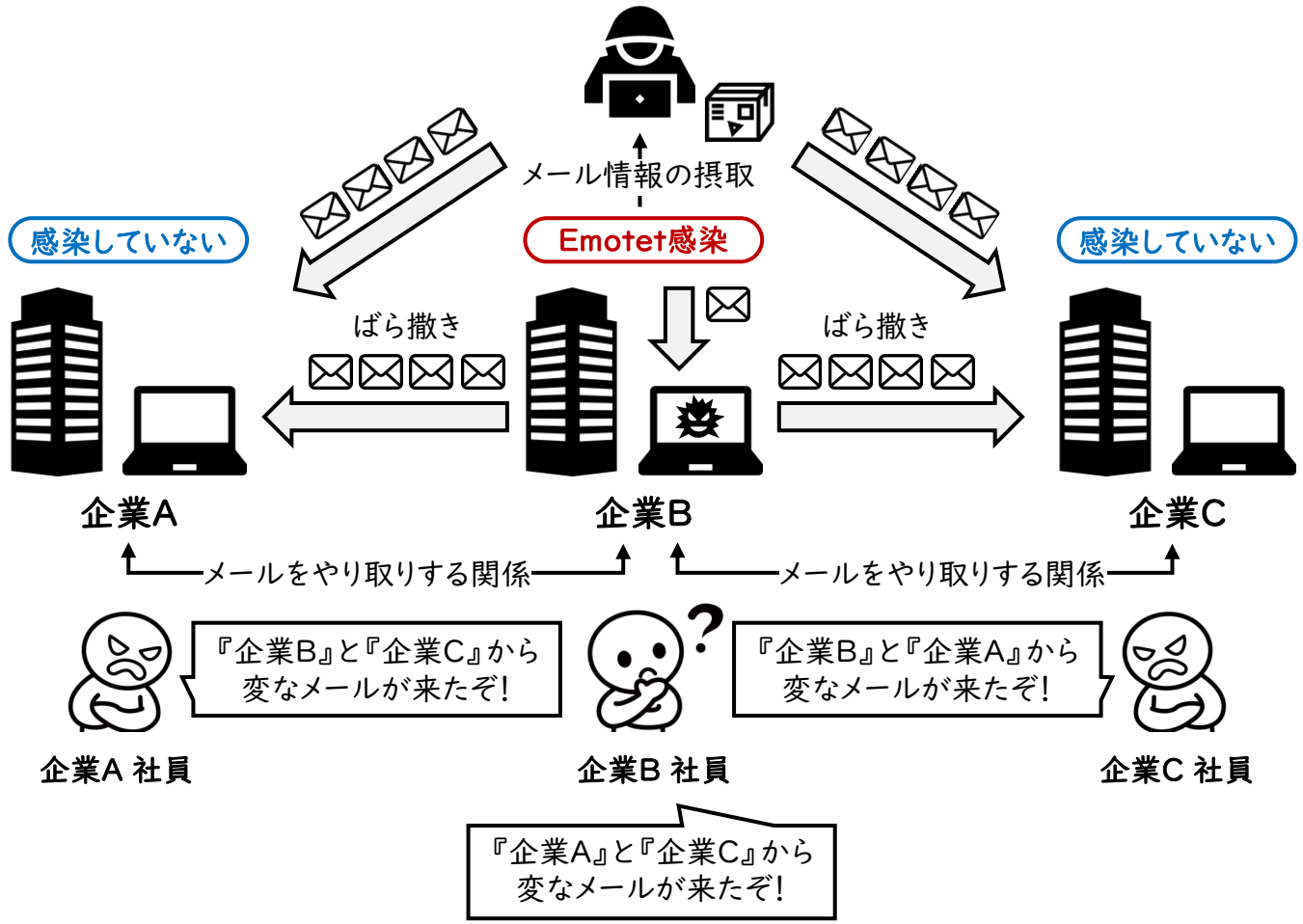
Emotet発症までの攻撃ステップ



「Emotet」の感染拡大で生じた問題

そもそも誰が「Emotet」に感染しているのかわからない

攻撃メールの着弾だけでは感染有無は特定できない。



出典:JPCERT/CC:https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

※調査を行う場合には端末を隔離してから実施する。

①	**Emocheckによる感染有無の確認** JPCERT/CCが開発・提供するEmotet感染調査ツールを端末内で実行する。検知しない=感染していないとはならないので注意する。
②	**感染を狙う固有の仕掛けに引っかかってないか確認** メール経由で受信したMS Officeファイルのマクロを有効化していないか、メール経由で誘導されたウェブサイトで何かをインストールしていないか思い出す。
③	**最新の定義ファイルでフルスキャンを実施** お使いのウイルス対策ソフトを最新の定義ファイルにアップデートした上でディスク内をフルスキャンを実施する。検知しない=感染していないとはならないので注意する。
④	**端末起動時の自動起動設定項目の確認** レジストリ内に記述された端末起動時に自動起動するアプリの中に不審なプログラムが登録されて永続化していないか確認する。対象プロセスは停止及び削除する。
⑤	**自社メールサーバーの不正利用の痕跡を確認** メールアカウントを不正利用された場合、自組織のメールサーバーから大量に攻撃メールが配信されることがあります。自社で確認、又は提供事業者に確認を依頼する。
⑥	**ファイアウォールのログ等から通信履歴を確認** 感染時に伴いC&Cサーバーとの通信が行われたか確認する。 例:https://urlhaus.abuse.ch/browse/tag/emotet/ 例:https://feodotracker.abuse.ch/browse/emotet/
⑦	**メールアカウント及びブラウザの認証情報を変更** 利用しているメールソフトに設定されているメールアカウントのパスワードを変更する。また、ブラウザに保存されているクラウドサービス等のパスワードも併せて変更する。

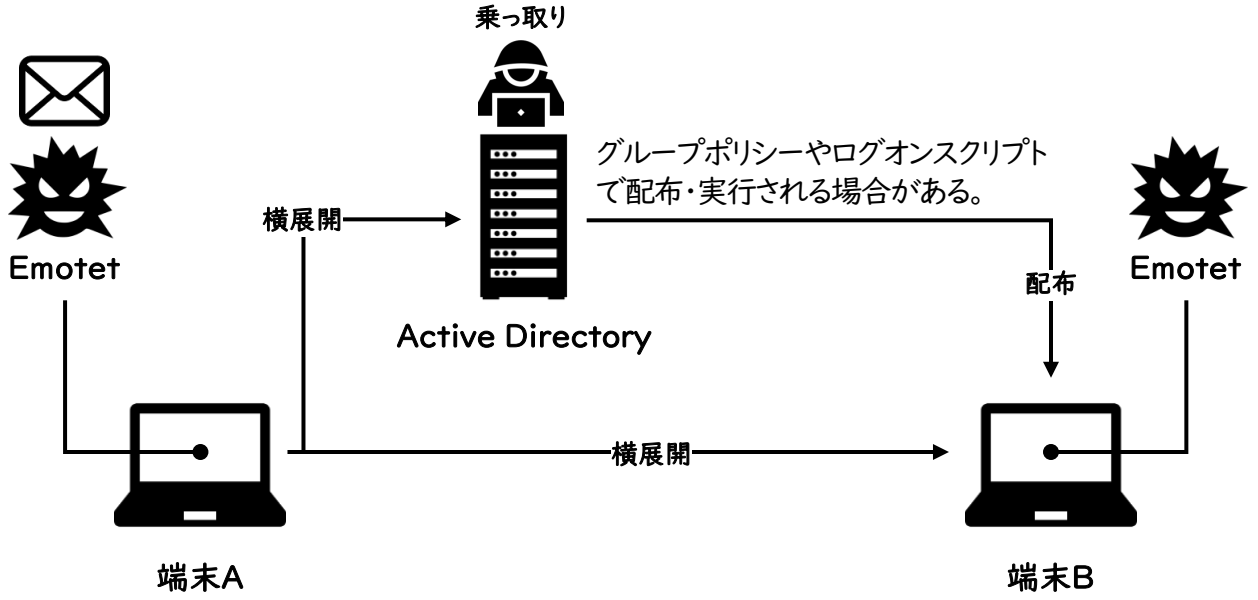
© 2022 Blue Planet-works, Inc.

「Emotet」を駆除できても油断してはならない

Emotetを削除してもEmotetが呼び込んだ別の脅威は残っている

Emotetに感染したことが確定した場合には当該端末の『初期化』を推奨します。

最初に発症するEmotetは自動起動するプロセスとしてレジストリに登録される。

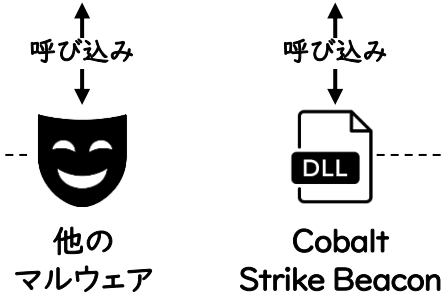


グループポリシーやログオンスクリプトで配布・実行される場合がある。

横展開された場合、Emotetは管理者権限で実行され、端末内で動作するサービスとして偽装登録される可能性がある。

Emotet呼び込む他のマルウェアの例※

国内	不正送金マルウェアなど
海外	ランサムウェアなど



Cobalt Strikeはペネトレーションツール（攻撃者の活動を再現する正規のセキュリティツール）であり、メモリ内で完結して動作する仕組みであるため、その痕跡を見つけることが極めて難しい。侵入した端末を起点として横展開する際に利用される。

出典：JPCERT/CC：https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

© 2022 Blue Planet-works, Inc.

Blue Planet-works
Safety for the Connected World

既存のサイバーセキュリティソリューションの有効性 #1

- アンチウイルスの限界 -

© 2022 Blue Planet-works, Inc.

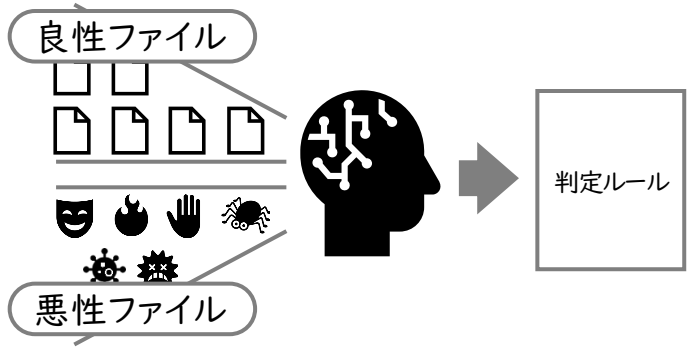
アンチウイルスで使われる中核技術の特徴と課題 #1

Blue Planet-works
Safety for the Connected World

防御技術の中核はいずれも過去の情報に依存するため過去の情報が活用できない脅威に対して無力

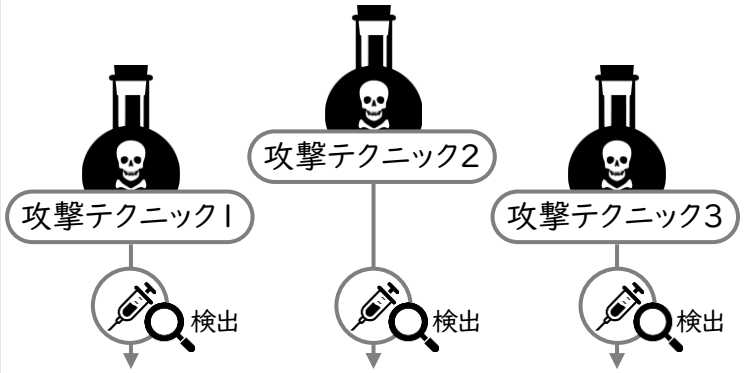
▼アンチウイルスソフトが利用する主な防御技術の特徴

機械学習に基づく高度な脅威解析



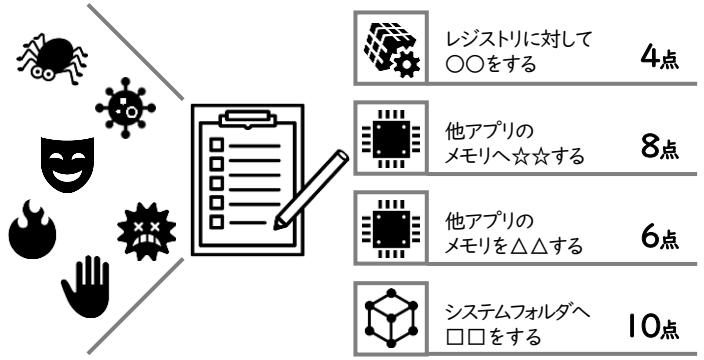
脅威から抽出した特徴点を利用

不正アクセスの阻止



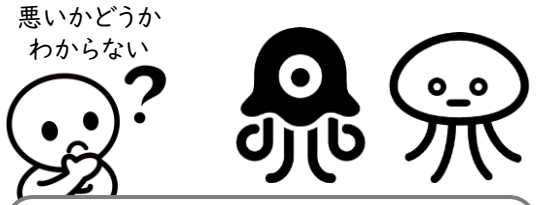
攻撃テクニックをデータベース化

システムに害を成す危険な動作の特定



悪意ある振る舞いをリスト化して採点

過去の情報が活用できない脅威は対処が困難



「未知」のマルウェア

「変容」するマルウェア

「未発見」の攻撃テクニック

「安全な」ツールや機能の悪用

© 2022 Blue Planet-works, Inc.

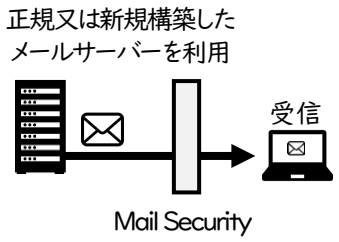
マルウェア「Emotet」はアンチウイルスの苦手な要素を持っている

Blue Planet-works
Safety for the Connected World

複数の技法を組み合わせることで ウイルス対策ソフトをすり抜ける構造を獲得している

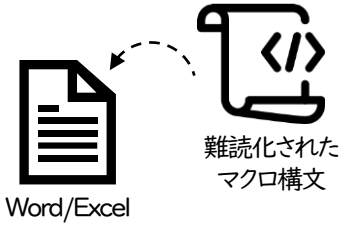
「安全な」ツールや機能の悪用 ＋ 「安全な」ツールや機能の悪用 ＋ 「安全な」ツールや機能の悪用 ＋ 「未知」のマルウェア ＋ 「変容」するマルウェア

Emotetの配信



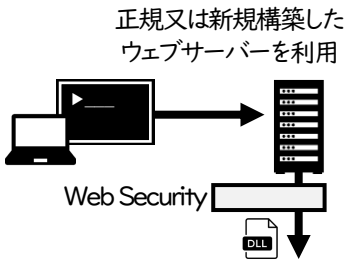
メールセキュリティ対策を回避するためにブラックリスト化されていないメールサーバーから実在する組織や個人を騙ってメールを送信する。

攻撃の発動



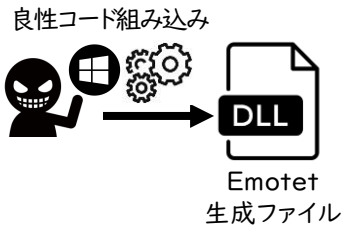
MSオフィスドキュメントに不正な構文を含むマクロを実装し、マクロを有効化することで攻撃が発動する。マクロの構文は難読化されている。

Emotetの侵入



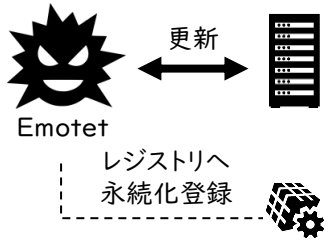
Emotetを生成するファイルをブラックリスト化されていないウェブサーバー等からダウンロードさせることでウェブセキュリティ対策を回避する。

Emotetの発症



Emotetを生成するファイルは検知を回避するためにWindowsの良性コードを含んでいる。そのため、悪性ファイルと判別することが非常に難しい。

Emotetの永続化



Emotetはメモリ上で稼働するため検知が難しい上に攻撃者のサーバーを介して定期的にアップデートして自己変容していく特性を持つ。

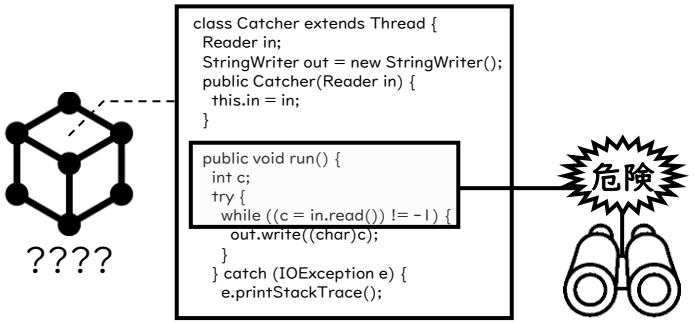
© 2022 Blue Planet-works, Inc.

Blue Planet-works
Safety for the Connected World

アンチウイルスは歴史あるセキュリティツールが故に検出を回避するための対抗技術がすでに多数存在している

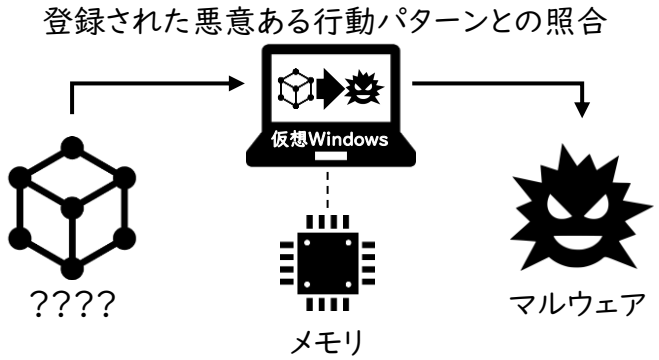
▼アンチウイルスソフトが利用する主な防御技術の特徴

対象ファイルの構造分析



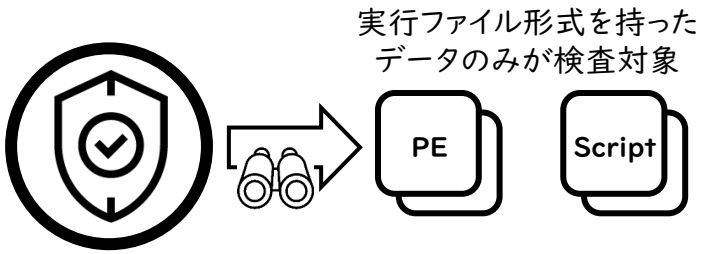
ファイルを構成するソースコードを解析

メモリ上の仮想エミュレータ



仮想Windowsによる事前起動

“ファイル”に対する多層解析



端末上にあるファイル形式のデータを解析

解析困難な構造で対抗

Go言語
D言語
Nim言語
Rust言語

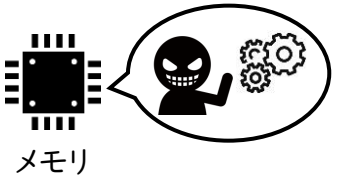
別言語利用＋難読化＋外部モジュール化

解析環境を検知して回避

- 時間差起動 …解析終了後に起動
- 実在性確認 …ユーザーの操作を確認
- ツール確認 …解析ツールの有無確認

アンチサンドボックス

ファイル形式を持たない



ディスク上に保存されないため、ファイルの有無で侵害を確認することができない。

インメモリー型の脅威コンテンツ

© 2022 Blue Planet-works, Inc.

Blue Planet-works
Safety for the Connected World

既存のサイバーセキュリティソリューションの有効性 #2

- 事後対策ソリューションの反省点 -

© 2022 Blue Planet-works, Inc.

体制づくりや運用の敷居が高い事後対策を想定したセキュリティ対策

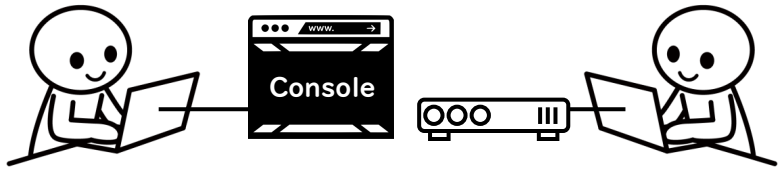
Blue Planet-works
Safety for the Connected World

▼米国・標準技術研究所（NIST）提唱のサイバーセキュリティフレームワーク

特定 Identify	防御 Protect	検知 Detect	対処 Respond	回復 Recover

事前対策（予防）

適切な設定を施して適切な状態を維持する



事後対策（治療）

事後の対処なので業務の継続性は保証されない

侵害された痕跡から脅威や攻撃を特定して対処に当たるため業務の継続性は保証されない。

24時間365日体制で監視が必要

いつ攻撃されるのかわからないため、24時間365日体制で監視している必要がある。

運用には専門人材の配備が必要

運用には「検知」する専門家、「調査・トリアージ」する専門家、現場で「復旧」させる専門家が必要になる。

© 2022 Blue Planet-works, Inc.

事後対策のベストプラクティス「1-10-60」ルールへの対応状況

Blue Planet-works
Safety for the Connected World

▼事後対策における「1-10-60」ルール

検知に「1分」、トリアージ及び調査に「10分」、修復及び封じ込めに「60分」で対応できれば、ネットワーク内へ不正侵入されたとしても実被害が生じる前に阻止することが可能であるとする実績に基づくベストプラクティス。

しかし、その運用実態は…

	検知	トリアージ	調査	修復/封じ込め
全世界平均(2019年)	120時間	5時間	6時間	31時間
日本平均(2019年)	165時間	8時間	7時間	43時間

出典:CrowdStrike:https://japan.zdnet.com/article/35145739/

© 2022 Blue Planet-works, Inc.

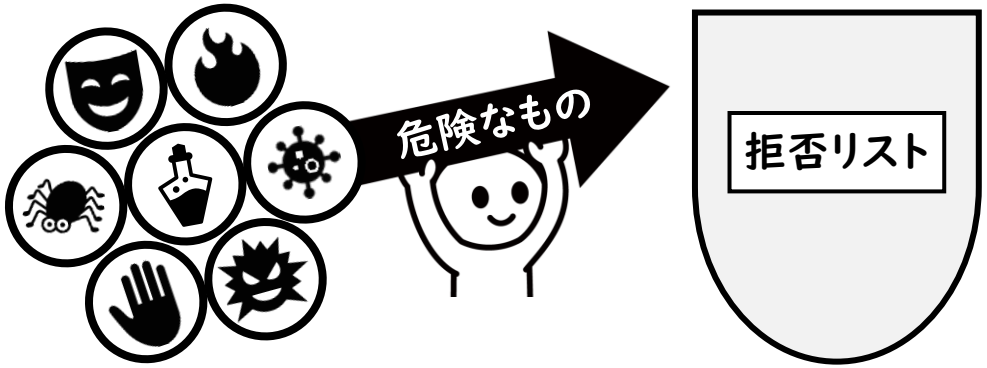
期待が寄せられている新しい守り方の概念

Blue Planet-works
Safety for the Connected World

ネットワークを守るための境界防御を突破されたとしても攻撃者に行動の自由を与えないことで攻撃を成立させない

これまでの守り方

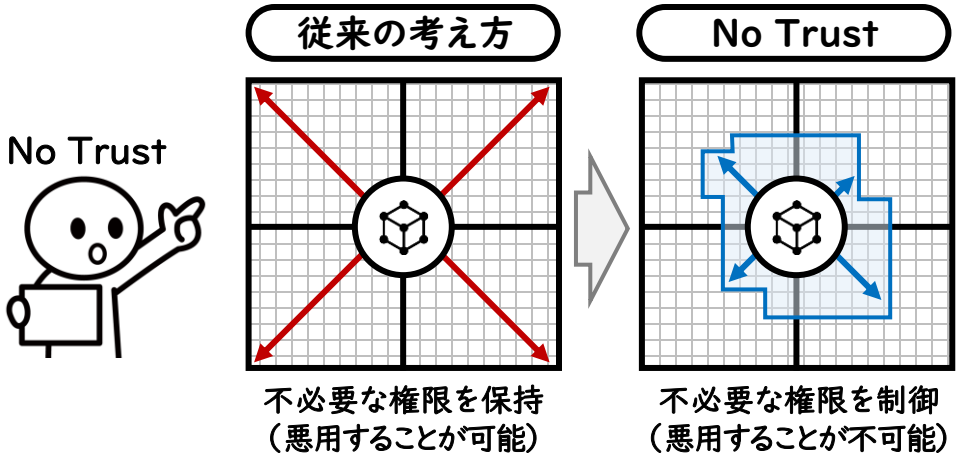
すべてを「許可」して例外で「拒否」する



過去の脅威情報から危険性の高いものを例外として拒否していく「ブラックリスト」に基づく対処方法です。

これからの守り方

すべてを「拒否」して例外で「許可」する



「No Trust（一切信用しない）」に基づき、動作を許可するものであっても不必要な権限を制限して安全かつ必要最低限の動作のみ許可します。

© 2022 Blue Planet-works, Inc.

Blue Planet-works
Safety for the Connected World

監修：全日本空輸株式会社 デジタル変革室 企画推進部

重要インフラ事業者としてのゼロトラストへの取り組み

- 事例：全日本空輸株式会社 -

© 2022 Blue Planet-works, Inc.

非公開

© 2022 Blue Planet-works, Inc.

Robert Bigman氏の教え

- 元CIA CISOが実践してきた6つのベストプラクティス -

© 2022 Blue Planet-works, Inc.

日本の情報システム担当者に贈るメッセージ

Robert Bigman

組織にとって最大の脅威はネットワークの外側よりやって来るため、外部との接点を持つ全てのエンドポイントは最もリスクが高くなる。

これらのエンドポイントに対して洗練されたハッキングツールは脆弱なファームウェア/ソフトウェア、ローカル管理者認証情報、脆弱性なセキュリティ設定などを特定することから始まる。

実にサイバーセキュリティリスクの87%はこれらで占められている。

監査当局はリスク管理に対する「バランスの取れたアプローチ」を求めるが、彼らの大半はサイバーセキュリティリスクの源泉を理解していない。

そのため、「コンプライアンス」遵守のために組織は第三者リスク、内部不正、データの暗号化、リスクの測定、脆弱性評価、セキュリティ監視、トレーニングの問題に投資を余儀なくされる。

しかし、これらの対策はハッキングを阻止するためには全く役に立たない。サイバーセキュリティにおいて「バランスの取れたアプローチ」はむしろ有害である。

© 2022 Blue Planet-works, Inc.

防御と防止に役立つ6つのベストプラクティス

私の経験から言うと98%の組織は『防御や防止』が十分ではない。

攻撃者が最も気にするのはターゲットの防御能力である。

1. ネットワーク、OS、アプリケーションをゴールドイメージで固定
   - 堅牢化されたイメージを利用してプラットフォームを作る。
2. 強固な二要素認証でログイン強化
   - 不正アクセスを防止するためにシステムに対する認証を強化する。（Bigman氏はX.509 v.3 証明書を推奨）
3. アカウント権限の分離を確実に実施
   - クレデンシャル管理を徹底する。（管理者とユーザーの明確化、不要アカウント削除、パスワードの非共通化）
4. ネットワークレベルの分離を実施
   - ネットワークをマイクロセグメント化しシステム間における通信を制御する。
5. カーネルとメモリ保護の対策
   - PCやサーバーに限らず、IoTデバイスなども含めてカーネルとメモリ保護を実施する。
6. 脆弱性検知とパッチマネージメントの自動実行
   - 脆弱性の管理を徹底して早期に解消していく取り組みを行う。

© 2022 Blue Planet-works, Inc.

Blue Planet-works
Safety for the Connected World

ありがとうございました。

© 2022 Blue Planet-works, Inc.