Deloitte.
デロイト トーマツ

台湾におけるサイバーインシデント対応に関する主要論点

デロイト トーマツ グループ

2020年に入ってランサムウェアを始めとするサイバー犯罪が全世界で急増しており、台湾も例外ではありません

2020年に発生したサイバー犯罪Top15

参照：ENISA Threat Landscape 2020

© 2021. For information, contact Deloitte Touche Tohmatsu LLC.

台湾に拠点を置く日系企業が標的型ランサムウェアの対象となるケースが増加しています

日系企業が標的となる主な事由

他の海外拠点よりセキュリティレベルが一段劣ると捉えられている

- 日本本社やリージョナル・ヘッド・オフィスと比較し全社的なセキュリティ関心度が低いと捉えられている。

日本本社への踏み台として利用される

- 台湾支社からID・パスワードを入手し、より重大な企業秘密、営業情報がある日本本社へアクセスを試みるケースが増えている。

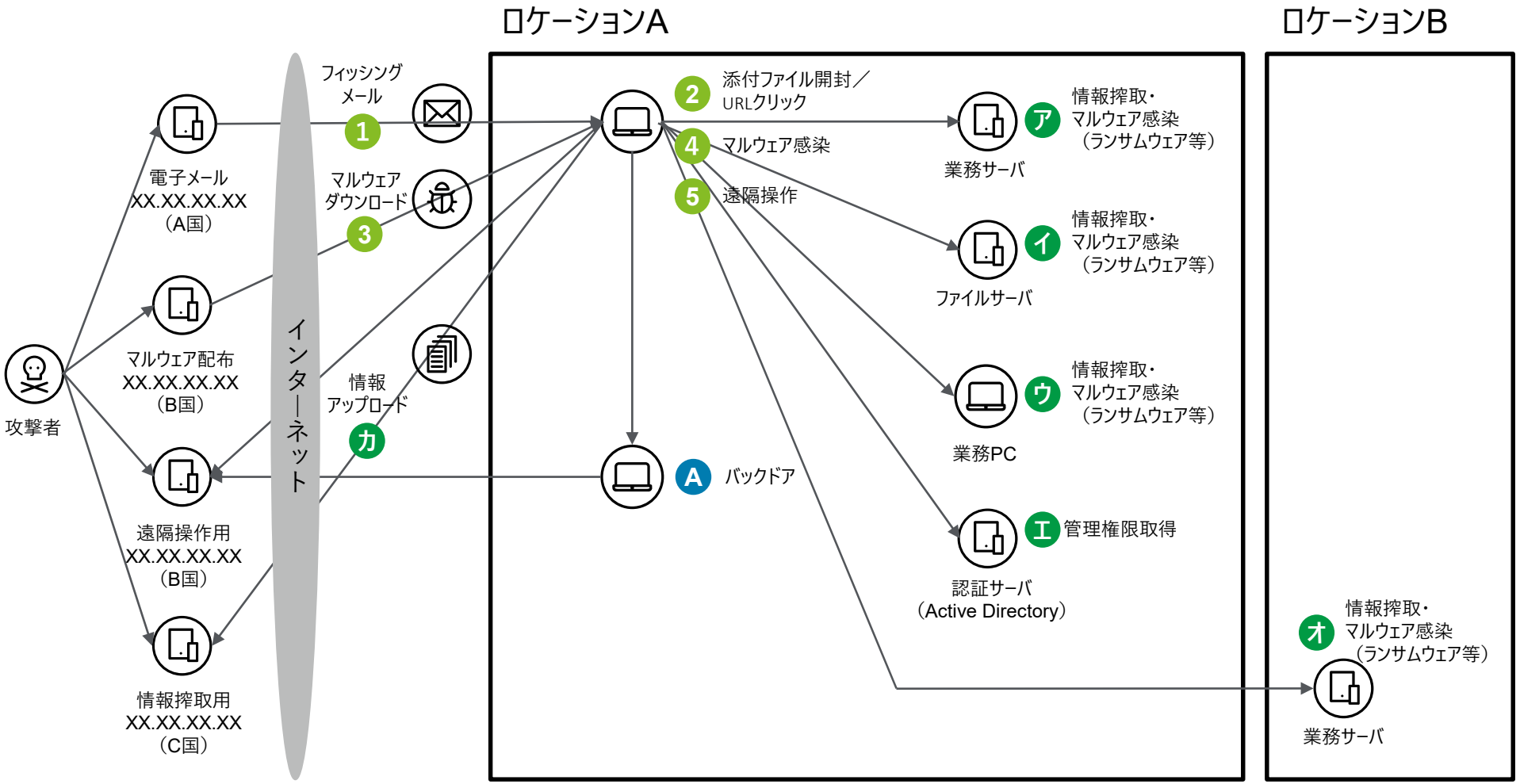
研究情報の入手が目的（特に製造業）

- 世界的に知名度のある企業が存在する台湾に、R&D部門を設置する日系企業も増加しており、最新の研究データをターゲットとした不正アクセスが増加している。

© 2021. For information, contact Deloitte Touche Tohmatsu LLC.

高度なサイバー攻撃は下図のような手口で行われます

サイバー攻撃パターン過去事例を基に作成した架空のケース



© 2021. For information, contact Deloitte Touche Tohmatsu LLC.

前述図式化したした手順上で想定される、攻撃者の侵入経路について解説します

侵入経路解説（初期侵入−マルウェア実行−ネットワーク検索）

1 2

フィッシングメール
添付ファイル開封／URLクリック

- 社内メールに対して不信なメールが送付され、ウィルスに感染
  1. 不正なマクロ入りOfficeファイル添付が送付されるケース
  2. 不正なURLが本文に添付されるケース

3 4

マルウェア
ダウンロード／感染

- 添付ファイルに記載されていたURLを通して、ウィルスのダウンロードが開始
- 会社の他の端末・サーバにもウィルスを配布を開始

5

遠隔操作

- 攻撃者が内部ネットワークの情報収集や認証情報を収集
- システム上の特権を奪取

© 2021. For information, contact Deloitte Touche Tohmatsu LLC.

前述図式化したした手順上で想定される、攻撃者の侵入経路について解説します

攻撃者の操作概要説明

ア イ ウ オ

情報搾取・マルウェア感染（ランサムウェア等）

- ランサムウェアの配置・実行によるネットワーク内機器の暗号化

エ

管理権限取得

- 内部ネットワークの支配領域を拡大するために、管理者権限を取得
- 一般的に、管理者権限奪取がひとつの目標となる

カ

情報アップロード

- 内部データを収集して攻撃者のインフラに送信
- クラウドバックアップを利用している場合、認証情報を窃取されて攻撃者のインフラにレストアされる手法もある

© 2021. For information, contact Deloitte Touche Tohmatsu LLC.

補足：
不正な侵入口「バックドア」を作成された場合、悪意を持ったものが遠隔操作することが可能になり、情報流出の危険性を更に高めてしまいます

バックドア解説

A

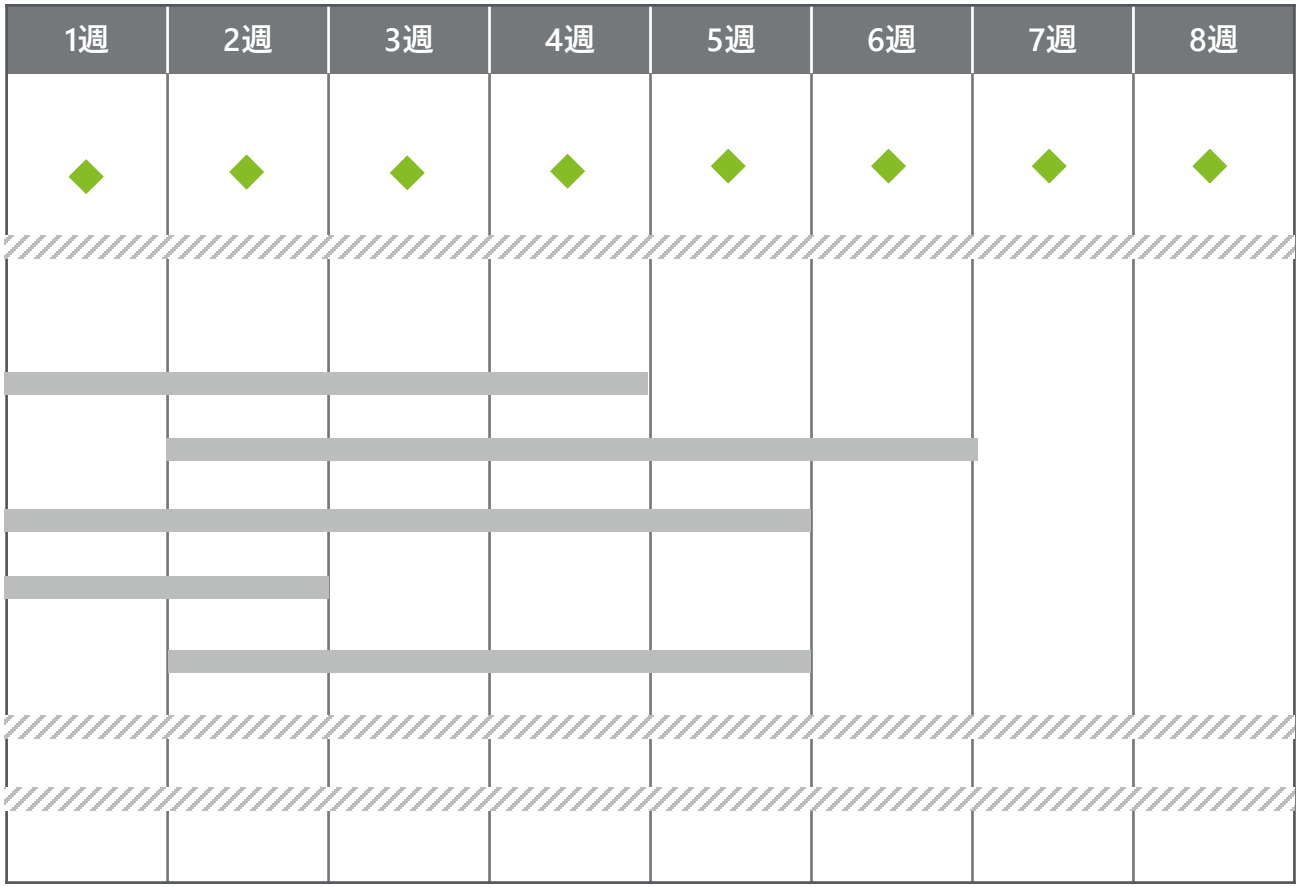
バックドア

- バックドア作成の主な手順は以下の通り
  1. 不正アクセスなどで侵入した際に、次回から進入しやすくするために抜け道を作る
  2. コンピューターウィルスなどに感染させて抜け道を作る

© 2021. For information, contact Deloitte Touche Tohmatsu LLC.

上記仮想ケースに対応した弊社支援例及びスケジュール案をご紹介いたします

スケジュール草案



Mile Stone

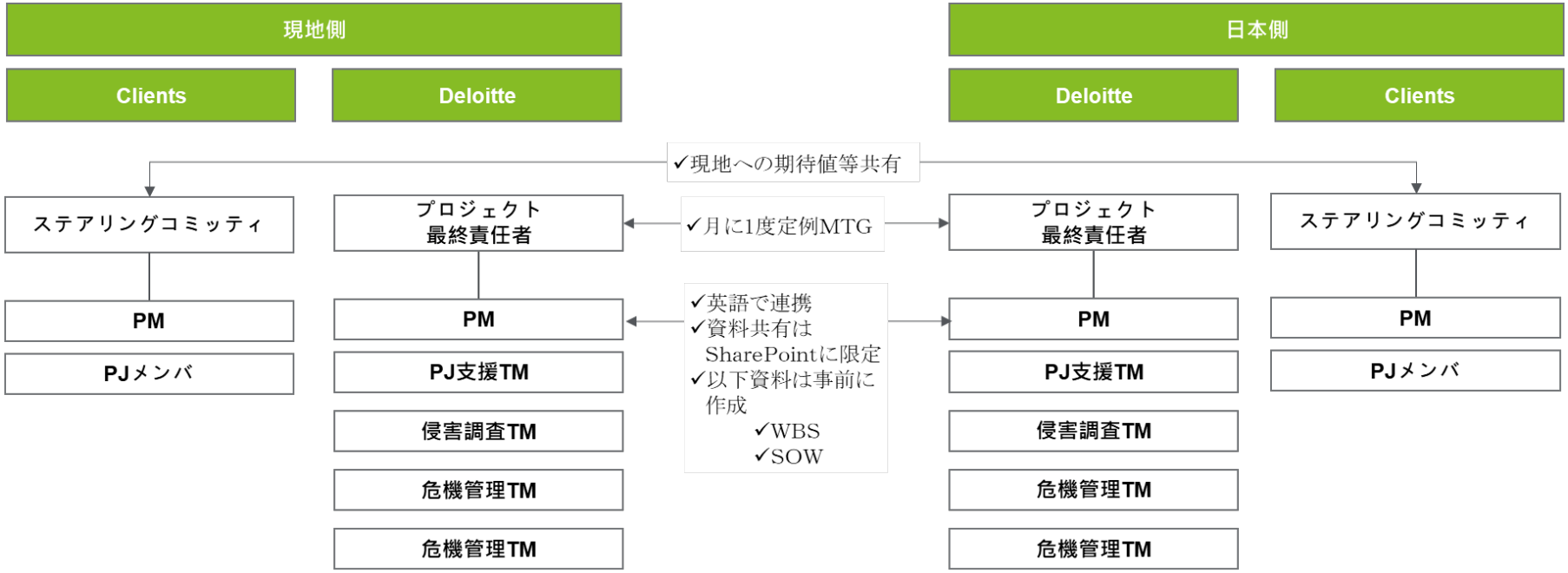
※上記スケジュールあくまで1例です。
実際の作業内容及びスケジュールは実態の被害状況に応じて変更されます。

© 2021. For information, contact Deloitte Touche Tohmatsu LLC.

1

海外拠点のインシデント事故においては、日本本社との密なコミュニケーションが成功のカギとなります

デロイト組織体制スキームの一部



過去経験からデロイトは円滑なコミュニケーションを実現するスキームを確立しており、スムーズな初動、コミュニケーションを実現します。

© 2021. For information, contact Deloitte Touche Tohmatsu LLC.

❷ インシデント発生時にはセキュリティ専門家に加え、台湾の個人情報保護管理に詳しい専門化のアサインが不可欠です

台湾の個人資料保護法施行細則　※民國 105 年 03 月 02 日修正　國家發展委員會

Personal Data Protection Act (PDPA)
8 つのコア要素

データ主体の権利

「データ主体」の基本権利は５つ

複製、**コピー**の取得、**補足**、それらの情報の**使用**と**削除**について、基本的な権利を有する。

データの扱い方

正当な目的および同意が必要

PIIの取得、取り扱いの前に組織は必ず、本人からの**同意**の取得が必要。また必要に応じて同意を得ていることを適切に**表明**する必要がある。

外部委託先管理

サードパーティ管理

ベンダー選定の際はPIIの取り扱いについて、セキュリティ対策について**事前にチェック**する。

定期的な**モニタリング**を行う必要がある。

監査証拠エビデンス

ログの記録と保存

PIIの処理と保存に使用されるシステムは、適切にログを**記録**し、適切な期間**保存**する必要がある。

マーケティング管理

PIIを利用したマーケティング

マーケティングに個人情報を使用する場合は、当事者への通知を行う必要がある。

また当時者へマーケティング活動を**拒否する方法**を提供する必要がある。

セキュリティ

適切なサイバーセキュリティの実施義務

PIIを所持している組織は、PIIの盗難、改ざん、損傷、破壊、開示を防ぐために、**適切なサイバーセキュリティ対策**を講じる必要がある。

情報漏えい対応

報告と事後策

情報漏えいが発生した場合、

自身が所属する業界の**監督機関**へ必ず報告する必要がある。

是正および今後の予防策は**信頼できる外部機関**によって診断される必要がある。

法的要件

違反した場合

2000万NTDの罰金に科せられる可能性がある。

企業情報及び営業秘密管理代表台帳を作成していない等、十分なセキュリティ対策、ログの記録を行っていない場合、民事、刑事上の罰則に科せられる可能性がある。

© 2021. For information, contact Deloitte Touche Tohmatsu LLC.

③ 全端末とネットワークを対象に、感染状況及び不適切な操作情報を洗い出し、感染の原因を特定することが、事態の早期収拾と今後のセキュリティ向上のカギとなります

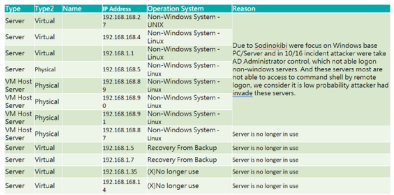
アセスメントの流れ

ステップ1
評価範囲の確認、システム情報の収集

IT資産の棚卸

- 既存情報及び、可能な場合はネットワークスキャンを実施し、IT]資産を網羅的に把握

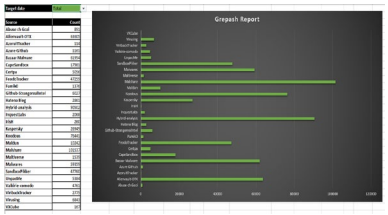
評価対象資産の特定



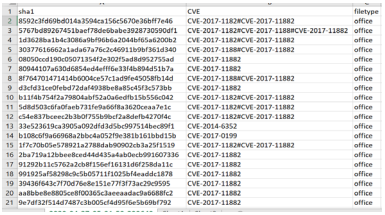
Type	Type2	Name	IP Address	Operation System	Reason
Server	Virtual		192.168.168.2 7	Non-Windows System - UNIX	
Server	Virtual		192.168.168.4	Non-Windows System - Linux	Due to Sodinokibi were focus on Windows base PC/Server and in 10/16 incident attacker were take AD Administrator control, which not able logon non-windows servers. And these servers most are not able to access to command shell by remote logon, we consider it is low probability attacker had mcade these servers.
Server	Virtual		192.168.1.1	Non-Windows System - Linux	
Server	Physical		192.168.168.5	Non-Windows System - Linux	
VM Host Server	Physical		192.168.168.8 9	Non-Windows System - Linux	
VM Host Server	Physical		192.168.168.9 0	Non-Windows System - Linux	
VM Host Server	Physical		192.168.168.9 1	Non-Windows System - Linux	
VM Host Server	Physical		192.168.168.8 7	Non-Windows System - Linux	Server is no longer in use
Server	Virtual		192.168.1.5	Recovery From Backup	Server is no longer in use
Server	Virtual		192.168.1.7	Recovery From Backup	Server is no longer in use
Server	Virtual		192.168.1.35	(X)No longer use	Server is no longer in use
Server	Virtual		192.168.168.1 4	(X)No longer use	Server is no longer in use

ステップ2
詳細安全評価

ウィルスチェック

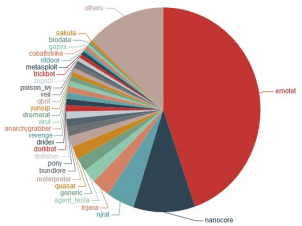


通信ログチェック

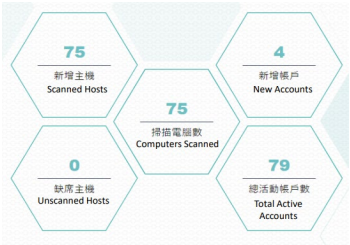


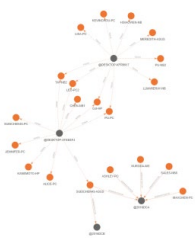
	sha1	CVE	filetype
2	8592c3fd69bd014a3594ca156e5670e36bff7e46	CVE-2017-1182#CVE-2017-11882	office
3	5767bd89267451bae778de6babe3928730590df1	CVE-2017-1182#CVE-2017-1188#CVE-2017-11882	office
4	1d3628ba1b4c3086a99bf96b6a2044bf65a6200b2	CVE-2017-1182#CVE-2017-11882	office
5	303776166f2a1ada67a76c2c469119b9bf361d340	CVE-2017-1188#CVE-2017-11882	office
6	08050ccd190c05071354f2e302f5ad8d952755ad	CVE-2017-11882	office
7	809441107a630d6854ed4eff6e33f4b894d51b7a	CVE-2017-11882	office
8	8764701474144b6004ce57c1ad9fe4505ffb1dd	CVE-2017-1188#CVE-2017-11882	office
9	d3cfd31ce0febd72daf4938be8a85c45f3c573bb	CVE-2017-11882	office
10	b11f4b754f2a79804abf52a0a6edfb15b556c042	CVE-2017-1182#CVE-2017-11882	office
11	5d8d503cdfa0faeb731fe9a66ffa3620eaa7e1c	CVE-2017-1182#CVE-2017-11882	office
12	c54e837bceec2b3b0f755b9bcf2a8defb42704c	CVE-2017-1182#CVE-2017-11882	office
13	33e523619ca3905a092dfd3d5bc997514bec89f1	CVE-2014-6352	office
14	b108c6f9a6d968a2bbc4ad52f9e381b161bbd15b	CVE-2017-0199	office
15	1f7c70b05e578921a2788dab90902cb3a25f1519	CVE-2017-1182#CVE-2017-11882	office
16	2ba719a12bbee8ced44d435a4ab0ecb991607336	CVE-2017-11882	office
17	91292b11c5762a2cb8f15ef16131d6f258fa11c	CVE-2017-11882	office
18	991925af58298c9c5b05711f1025bf4eaddd1878	CVE-2017-11882	office
19	39436f643c2f70d76e8e151e77f3f73ac29c9595	CVE-2017-11882	office
20	aa8bbe8e8805ceff00365c3aeeaadac3fa6688fc2	CVE-2017-11882	office
21	9e7df32f514d7487c3b005cf4d95f6e5b69bf792	CVE-2017-11882	office

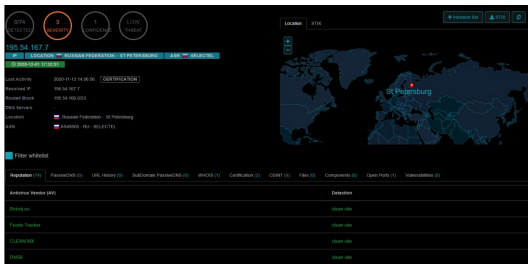
分析



ステップ3
レポート作成





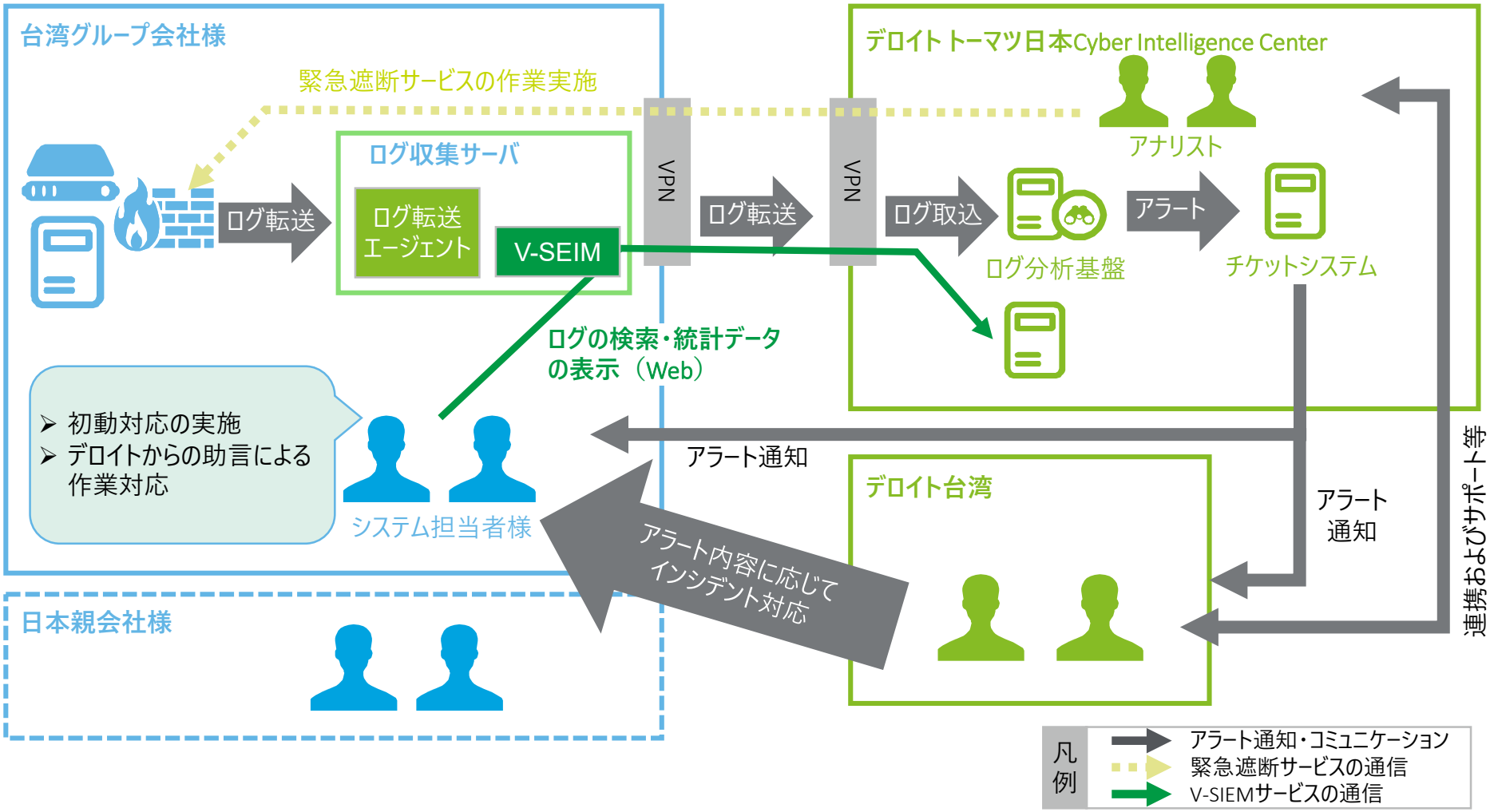


日本語、英語、中国語でレポート作成

© 2021. For information, contact Deloitte Touche Tohmatsu LLC.

4 【業務改善案】正確な原因分析結果を基に、クライアント嗜好及び業界成熟度を加味し、改善計画を立案します

改善例：24時間監視サービス



© 2021. For information, contact Deloitte Touche Tohmatsu LLC.

アジア・パシフィック地域での本サービスに関する問い合わせ先

当資料におけるサービスに関するお問い合わせは下記メールアドレスまでご連絡ください

ap_risk@tohmatsu.co.jp

当資料を含むアジアパシフィック地域における最新の経営環境やリスク情報、並びに当法人のサービスについては以下のWebサイトもご参照ください

https://www2.deloitte.com/jp/ja/pages/risk/articles/ra/risk-advisory-in-asia-pacific.html

※貴社および貴社の関係会社とデロイト トーマツ グループの関係において監査人としての独立性が要求される場合、本サービス内容がご提供できない可能性があります。詳細はお問合せください。

© 2021. For information, contact Deloitte Touche Tohmatsu LLC.

Deloitte.
デロイト トーマツ

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーであるデロイト トーマツ合同会社ならびにそのグループ法人（有限責任監査法人トーマツ、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイト トーマツ税理士法人、DT弁護士法人およびデロイト トーマツ コーポレート ソリューション合同会社を含む）の総称です。デロイト トーマツ グループは、日本で最大級のビジネスプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザリー、コンサルティング、ファイナンシャルアドバイザリー、税務、法務等を提供しています。また、国内約30都市以上に1万名を超える専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト（www.deloitte.com/jp）をご覧ください。

Deloitte（デロイト）とは、デロイト トウシュ トーマツ リミテッド（“DTTL”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人のひとつまたは複数を指します。DTTL（または“Deloitte Global”）ならびに各メンバーファームおよびそれらの関係法人はそれぞれ法的に独立した別個の組織体です。DTTLはクライアントへのサービス提供を行いません。詳細はwww.deloitte.com/jp/aboutをご覧ください。
デロイト アジア パシフィック リミテッドはDTTLのメンバーファームであり、保証有限責任会社です。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける100を超える都市（オークランド、バンコク、北京、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザリー、リスクアドバイザリー、税務およびこれらに関連するプロフェッショナルサービスの分野で世界最大級の規模を有し、150を超える国・地域にわたるメンバーファームや関係法人のグローバルネットワーク（総称して“デロイトネットワーク”）を通じFortune Global 500®の8割の企業に対してサービスを提供しています。“Making an impact that matters”を自らの使命とするデロイトの約312,000名の専門家については、（www.deloitte.com）をご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、その性質上、特定の個人や事業体に具体的に適用される個別の事情に対応するものではありません。また、本資料の作成または発行後に、関連する制度その他の適用の前提となる状況について、変動を生じる可能性もあります。個別の事案に適用するためには、当該時点で有効とされる内容により結論等を異にする可能性があることをご留意いただき、本資料の記載のみに依拠して意思決定・行動をされることなく、適用に関する具体的事案をもとに適切な専門家にご相談ください。

© 2021. For information, contact Deloitte Touche Tohmatsu LLC.

IS 669126 / ISO 27001

Member of
Deloitte Touche Tohmatsu Limited