サイバー攻撃(ランサムウェア感染)と対応について
～起きてしまったから分かること～

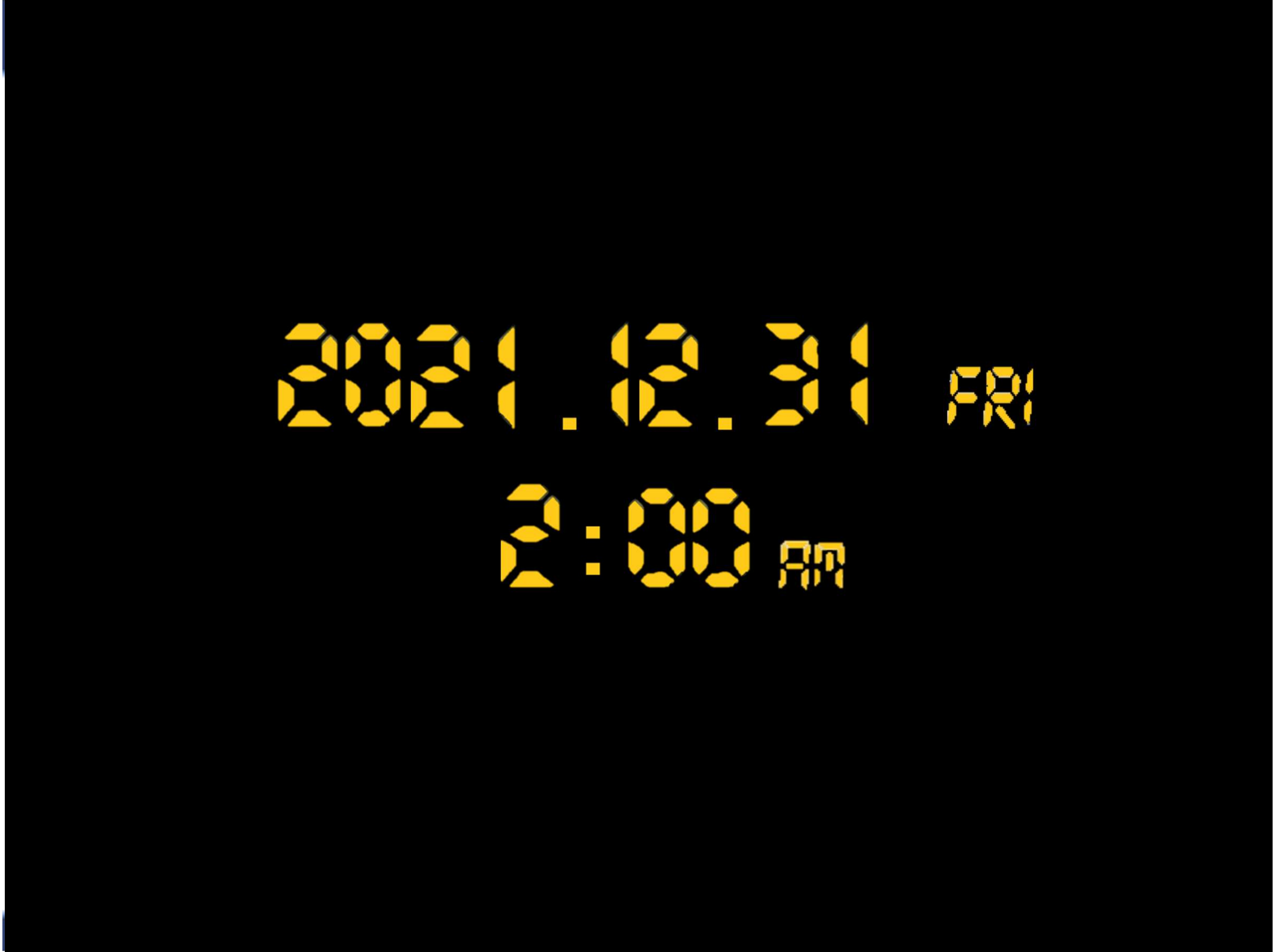
2023年10月26日

東京コンピュータサービス株式会社
サイバーセキュリティ対策本部

Agenda

1. サイバー攻撃の経緯・経過
2. ランサムウェアについて
3. 感染の直接的な原因と根本的な原因
4. 再発防止策
5. 現在までの対応と効果について
6. 更なる強化へ
7. まとめ

サイバー攻撃の経緯・経過


2021.12.31 FRI
2:00 AM

経緯・経過〈 1/4 〉

2021年12月31日 (金)

深夜2時過ぎ…	ランサムウエア 【 nightsky 】が活動開始 (セキュリティソフトのログより)
6時～10時頃	現象発生を社内で認識　～　全国全部門へ有線LAN接続機器の抜線を指示
10時頃～	初期調査開始
20～22時	所轄警察署、サイバー犯罪関係組織、及び富士通セキュリティ窓口へ通知 【通知先】・所轄警察署　・日本サイバー犯罪対策センター(JC³) ・情報処理推進機構(IPA) ・富士通(株)セキュリティ窓口

2022年 1月 1日 (土)

前日～15時頃	初期調査と情報の整理 (前日からの継続)
夕方18時	緊急社内対策会議開催 (社長以下セキュリティ関連責任者及び部門) →対策本部の設置及び初期対応方針の決定 (暗号化された機器の選別～それぞれの対応方針など)

経緯・経過〈 2/4 〉

2022年 1月 2日 (日)

- ADサーバを通じたランサムウエア配信の仕組みを特定し、該当処理を削除
- ADサーバ及び暗号化された機器の再構築開始
- ウイルス対策ソフトウエア会社より今回のランサムウエア【 nightsky 】に対するパターンファイルが公開
- 最新のパターンファイルを用いたスキャン及びウイルス除去を開始

2022年 1月 3日 (月)

- ADサーバの再構築完了
- 全PC(全社)に対し、クリーンインストール作業を着手 (1月末完了)
- 攻撃者による弊社への不正アクセスの情報が一般の人が見れないダークウェブサイト上に一部掲載された情報を確認

※ダークウェブサイト … IPアドレスを隠したウェブサイト、通称「闇サイト」

2022年 1月 4日 (火)

- 改めて所轄警察署へ状況報告を実施
- 弊社ホームページ上に「サイバー攻撃による被害と復旧状況について（第一報）」を掲載

経緯・経過〈 3/4 〉

2022年 1月 5日 (水)

- サイバーセキュリティ専門会社との連携開始
  (第三者によるデジタルフォレンジック調査の依頼など)
  ※デジタルフォレンジック … デジタル社会における司法解剖という位置付け
  デジタルデバイスにおける電磁的記録の証拠保全及び調査分析を行う行為

2022年 1月 7日 (金)

- 基本方針の変更
  (同一ネットワークで被害を受けた機器を選別　→　ネットワーク自体を凍結･分離)

2022年 1月25日 (金)

- デジタルフォレンジック調査の中間報告 (侵入経路と侵害行為の痕跡を確認) あり

2022年 1月27日 (木)

- 「経済産業省サイバーセキュリティ課」へ本件を報告

2022年 2月2日 (水)

- 弊社ホームページに「サイバー攻撃による被害と復旧状況について（第二報）」を掲載

2022年 2月11日 (金)

- 「ダークウェブ調査サービス」による監視開始 (継続調査中)

経緯・経過〈 4/4 〉

2022年 2月15日 (火)

- 攻撃者が1月中旬から下旬にかけてダークウェブサイトに公開した「窃取された約5GBの情報」を入手
  →詳細は公開情報(第三報)に記載　https://www.to-kon.co.jp/ja/topics/topics20220411103030.html

2022年 3月18日 (金)

- 弊社ホームページに「サイバー攻撃による被害と復旧状況について（第三報）」を掲載

2022年 3月28日 (月)

- デジタルフォレンジック調査の最終報告
  →調査により、侵入経路や手法を特定。但し、攻撃者や、搾取された情報の特定には至らず…

⋮

2023年 2月 8日 (水)

- 弊社ホームページに「サイバー攻撃による被害と復旧状況について（第四報）」を掲載

⋮

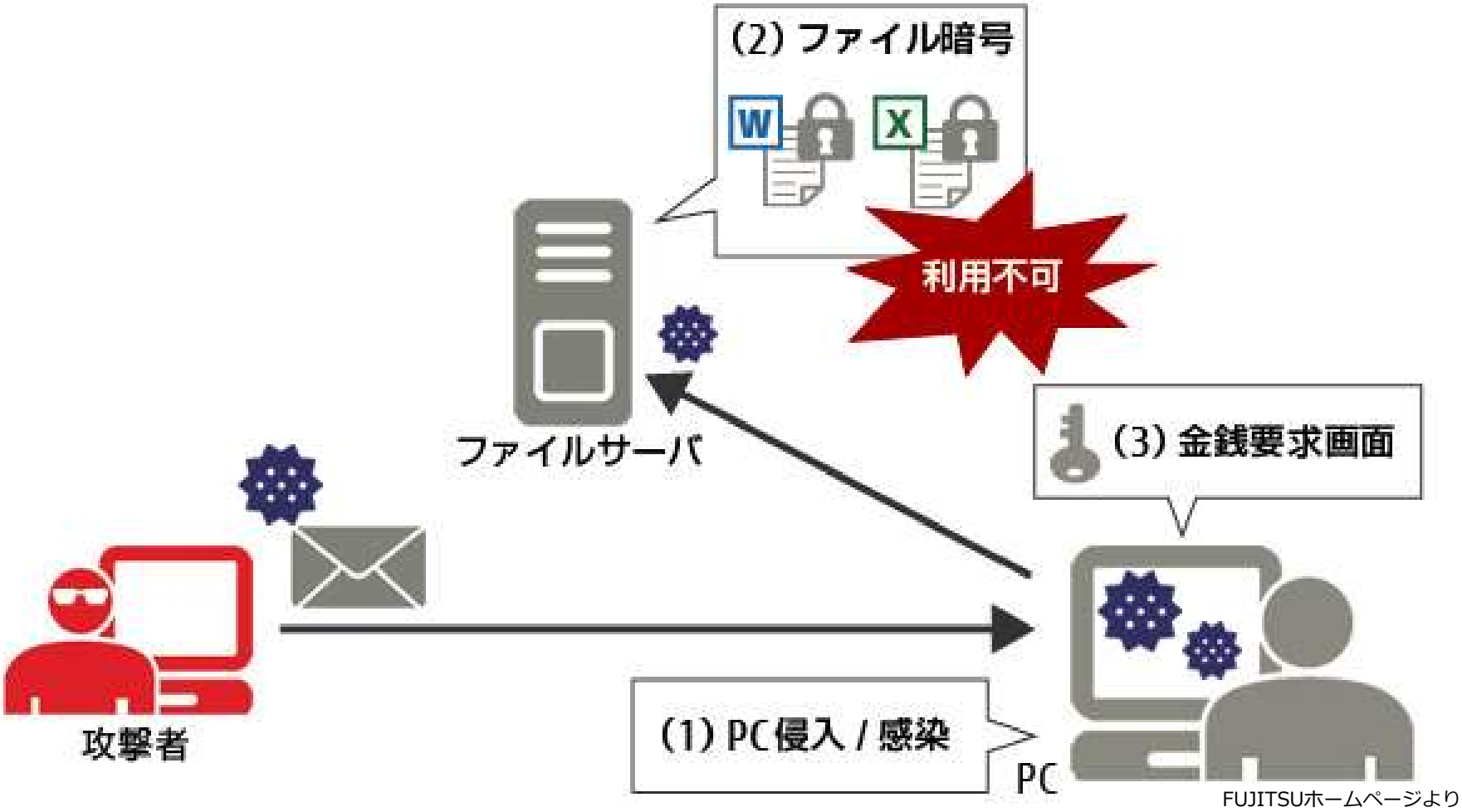
2023年10月26日 (木)

ダークウェブサイトの監視活動を継続中。

→監視活動開始～現在まで、情報が漏洩したという報告はございません。

ランサムウエアについて

ランサムウェア(Ramsomware)とは



FUJITSUホームページより

ランサムウエアとは、感染したPCをロックしたり、ファイルを暗号化したりすることによって使用不能にしたのち、元に戻すことと引き換えに「**身代金(Ransom)**」を要求する不正プログラムです。身代金要求型不正プログラムとも呼ばれます。

(トレンドマイクロより抜粋)

情報セキュリティ10大脅威 2023

前年順位	個人	順位	組織	前年順位
(1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)
(2位)	ネット上の誹謗・中傷・デマ	**2位**	サプライチェーンの弱点を悪用した攻撃	(3位)
(3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**	標的型攻撃による機密情報の窃取	(2位)
(4位)	クレジットカード情報の不正利用	**4位**	内部不正による情報漏えい	(5位)
(5位)	スマホ決済の不正利用	**5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	(4位)
(7位)	不正アプリによる スマートフォン利用者への被害	**6位**	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）	(7位)
(6位)	偽警告によるインターネット詐欺	**7位**	ビジネスメール詐欺による金銭被害	(8位)
(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	**8位**	脆弱性対策の公開に伴う悪用増加	(6位)
(10位)	インターネット上のサービスへの 不正ログイン	**9位**	不注意による情報漏えい等の被害	(10位)
(圏外)	ワンクリック請求等の 不正請求による金銭被害	**10位**	犯罪のビジネス化 （アンダーグラウンドサービス）	(圏外)

独立行政法人 情報処理推進機構(IPA)ホームページより
情報セキュリティ10大脅威 2023
https://www.ipa.go.jp/security/10threats/10threats2023.html

ランサムウェア攻撃による業務影響(弊社事例)

攻撃の概要

2021年12月31日2時頃、ランサムウェア【nightsky】が活動を開始し主要な業務サーバおよびPCの約１割がファイルを暗号化された

主な業務影響

①社内資産が利用できず

②勤務形態の大幅な制限

③作業の大幅な手戻りやスケジュール変更

④予定外作業の発生　　等々

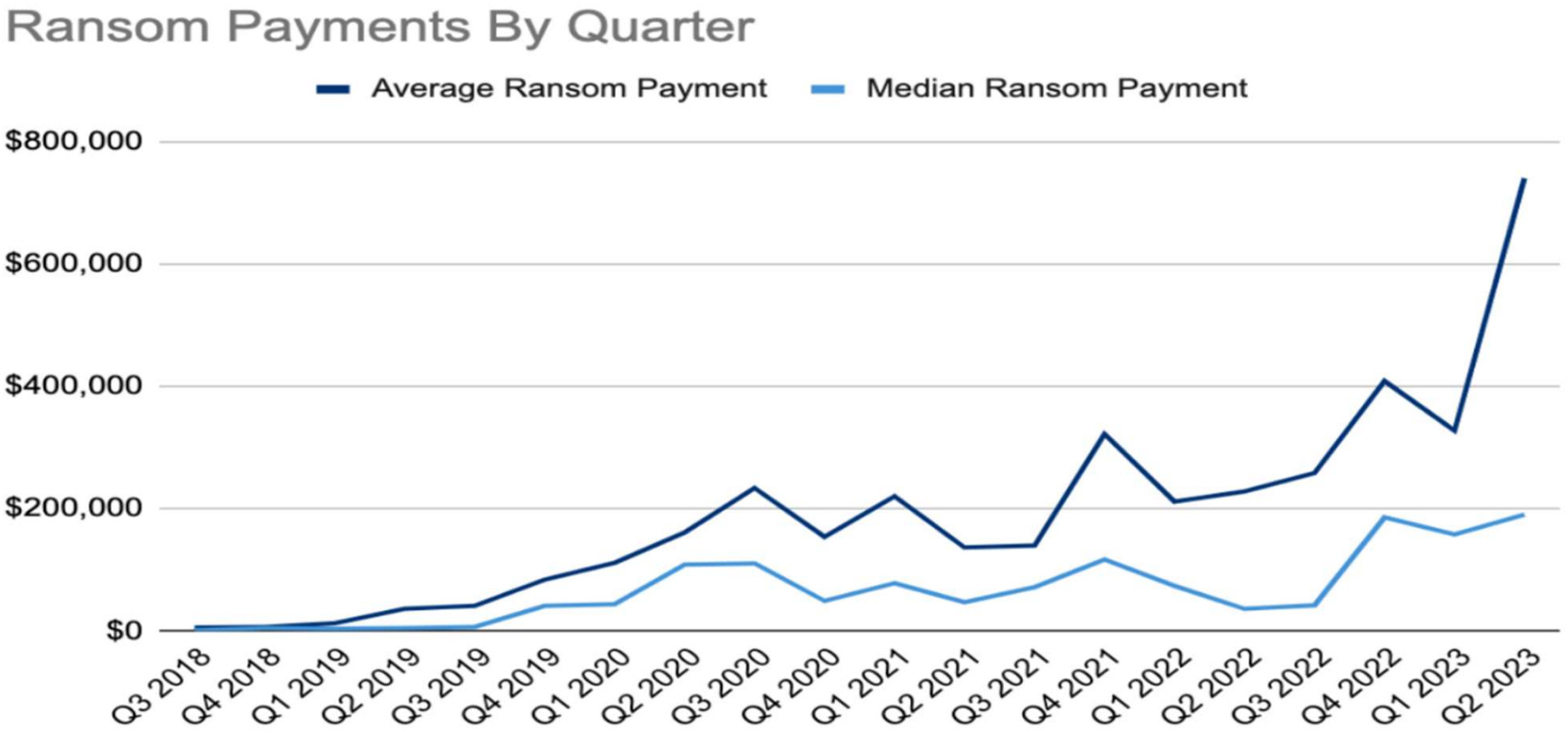
身代金の推移

支払われた身代金の総額は過去最高

2023年第2四半期

平均値は74万0144ドル（約1億5200万円）←+126% (2023年 第1四半期比較)

中央値は19万0424ドル（約2850万円）　←　+20% (2023年 第1四半期比較)



COVEWARE

米 COVEWAREより
JULY 21,2023 QUARTERLY REPORT
https://www.coveware.com/blog/2023/7/21/ransom-monetization-rates-fall-to-record-low-despite-jump-in-average-ransom-payments

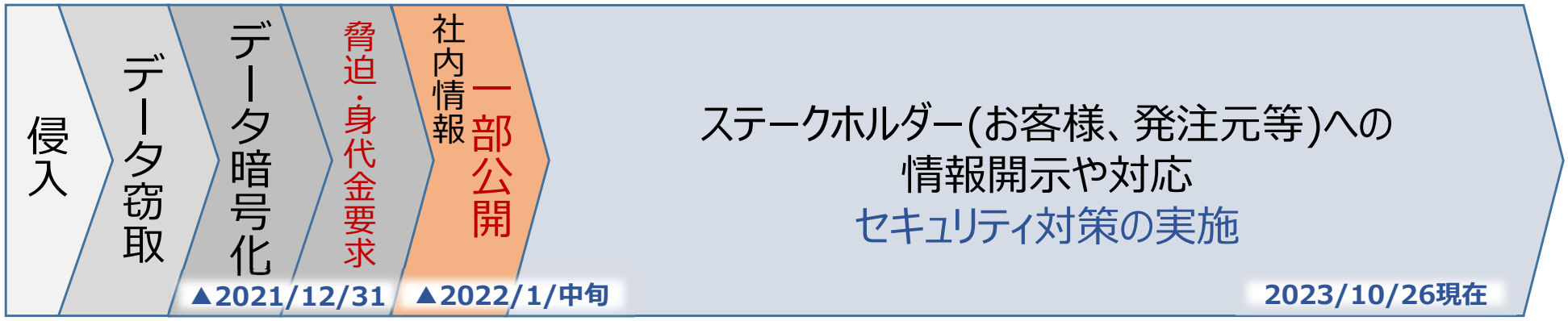
ランサムウェア攻撃による被害について〈 1/2 〉

コスト	概要	期間	規模
対策マネジメント費用	対策本部関連費用 取引先への個別説明･対応費用	2年間	数千万
各種調査費用	社外調査(第三者調査) 社内調査	2年間	数千万
システム再構築費用 (復旧費用)	機器調達費用 SE費用 業務停止に供なう損失	2年間	億越え
新システム･サービス 導入費用	導入検討費 機器調達費 SE費用	2年間	億越え
運用費用	追加費用： サービス利用費、運用費等	年間	数千万
		合計	**数億円**

ランサムウェア攻撃による被害について〈 2/2 〉

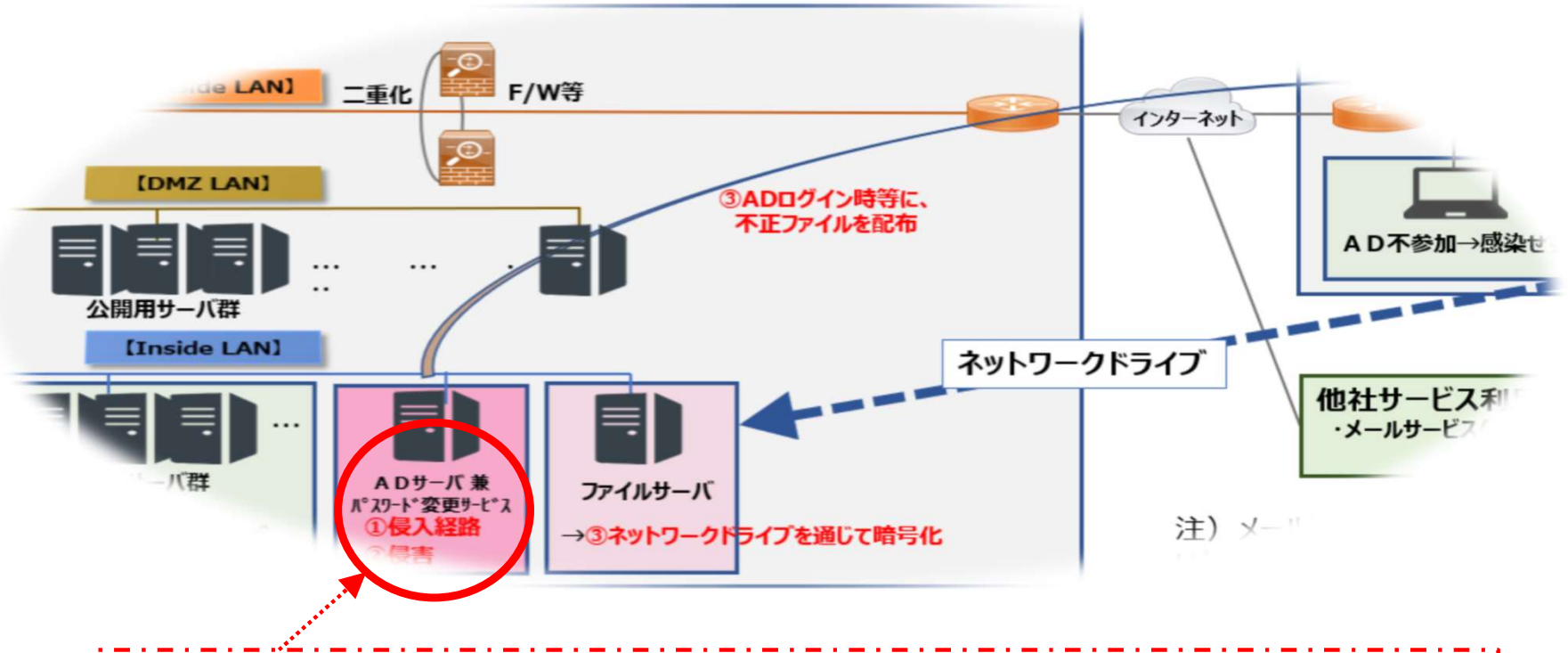
被害項目	概要
業務影響	安全性確保を優先したため、一部業務に於ける制限や遅延が発生した。（対外業務的には、ビジネスの機会損失が発生）
情報漏洩	社内情報及び一部取引データが漏洩。
信頼の損失	企業としての信頼低下が発生。
金銭的負担	第三者機関に依頼する原因調査や、情報漏洩有無の常時監視。システムの再構築や、ステークホルダー(お客様、発注元等)への補償など。
人的負担	システムの復旧や、お客様および関連機関への情報開示や対応など。

感染後の弊社がおかれている状況



感染の直接的原因と根本的原因

攻撃経路及び被害状況について



・**AD**(ActiveDirectory)**サーバ**　兼　利用者が、**パスワード変更サービス**を提供するサーバ

ADサーバに「パスワード変更サービス(※)」を追加し、社内アクセスのみ提供。

コロナ禍により、在宅勤務者およびお客様への常駐者から、パスワード失念時の対応を迅速化する目的として、インターネット経由での運用希望が増え、構成を変更（非公開）

結果、リバースプロキシを経由して、ADサーバの「パスワード変更サービス」の脆弱性を突かれ侵入を許した形になった。

※パスワード変更サービス：利用者自身がADパスワードを変更出来る、追加機能のサービス。

原因及び再発防止策について

直接的原因

公開ネットワーク上に移動したシステムの脆弱性対策漏れ

根本的原因

① 情報管理ルール（運用面）への考慮不足

② セキュリティ情報や脆弱性情報に対する管理および対応不足

③ 全社システムに対するセキュリティパッチ適用のPDCA確立不足

再発防止策

① 基本ポリシー作成（情報管理ルールに関し、運用面の詳細化）

② 脆弱性対応体制および方法の強化・整備

③ 定期的な監査による適正チェック

再発防止策

脆弱性対応の見直し

【期待効果】基準の見える化、対応手順の見える化により属人化の防止

①基本ポリシー作成（情報管理ルールに関し、運用面の詳細化）

・IPA公開ツールを使用し、**情報管理を共通化**して運用する。

◇脆弱性の影響度確認（影響範囲、重みづけ、悪用度、攻撃範囲、対策有無、ゼロデイ、ベンダ評価等）

https://www.ipa.go.jp/security/technicalwatch/20190221.html

◇脆弱性の影響度確認（影響範囲、重みづけ、悪用度、攻撃範囲、対策有無、ゼロデイ、ベンダ評価等）

脆弱性の影響	CVSS評価	脆弱性を悪用	NW越しの攻撃可否	実証コードの公開	ゼロデイ脆弱性	ベンダ評価
○:影響を受ける	4.0以上7.0未満	①攻撃情報**あり** ②攻撃情報**なし**	攻撃可能	実証コードあり	ゼロデイ脆弱性	中

◇脆弱性の対策の適用判断（**自動判断**）

脆弱性の緊急度	対応方針目安
緊急度：**高**	**①１日以内に実施** **②２～３日以内に実施**

②脆弱性対応体制および方法の強化・整備

◇体制強化、運用の見える化、情報管理の統一化　など

③定期的な監査による適正チェックを開始。

対応状況（2021/12～2023/10）

2023.10.26時点

	'21年	2022年											2023年								
	12月	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月
イベント	▼12/31 サイバー攻撃	▼01/04 第一報掲載(HP)	▼02/02 第二報掲載(HP)	▼03/18 第三報掲載(HP)											▼02/17 第四報掲載(HP)								
社外対応		お客様対応(情報共有、ご報告等)																					
		発注元対応(情報共有、ご報告等)																					
外部調査				ネットワーク診断(マルウェア検知)																			
				デジタルフォレンジング調査																			
		ダークウェブ調査																					
再発防止策		脆弱性対応（パッチ適用ルール）の見直し【完了】												直接的原因に対する対策									
		情報システム室の緊急体制強化【完了】																					
						①基本ポリシー策定【完了】								根本的原因に対する対策									
						②脆弱性対応体制及び方法の強化・整備【完了】																	
																			▼③内部監査 →問題なし				
セキュリティ強化策 ・SASE導入	セキュア＆透明性のあるネットワークの実現						SASE導入検討 ・検討 ・候補選定						SASE導入検証 ・A社 12月～01月 ・B社 02月～03月			SASE導入決定				SASE稼働		
・CAS導入	クラウドアプリケーション保護の導入				▼04/01 Trend Micro Cloud App Securityの導入																		
・統合管理	EndPointセキュリティの統合管理												ApexOneSaaSに統合										

SASE稼働
- ✓次世代型FW
- ✓URL Filtering
- ✓CASB
- ✓SOC
- ✓TLS Inspection
- ✓WAN最適化
- ✓SWG
- ✓Anti-Malware
- ✓IPS

現在までの対応と効果について

対策本部の設立（体制整備）

【効果】
対応方針の明確化：迅速な決断･正確な指示が可能→全社員の意思統一や一体感に繋がった
役割分担の明確化：情報集中と適正管理が可能→社員の負荷軽減に繋がった

【POINT】社内ケアが不足がちになりやすい。社内情報共有の徹底と、社内システム復旧チームの負荷軽減が鍵

サイバーセキュリティ 対策本部

社内外対応専門チーム
- お客様対応ST
- 発注元対応ST
- 社内情報共有ST
- FJ系エスカレーション窓口

社内システム復旧チーム
- 既存業務復旧ST
- 新システム構成検討ST
- 既存資産活用検討ST
- セキュリティ対応ST

第三機関対応チーム
- 捜査機関(警察)、IPA、他
- ダークウェブ調査
- フォレンジック調査
- ネットワーク調査

各部門

対策本部の役割分担の明確化

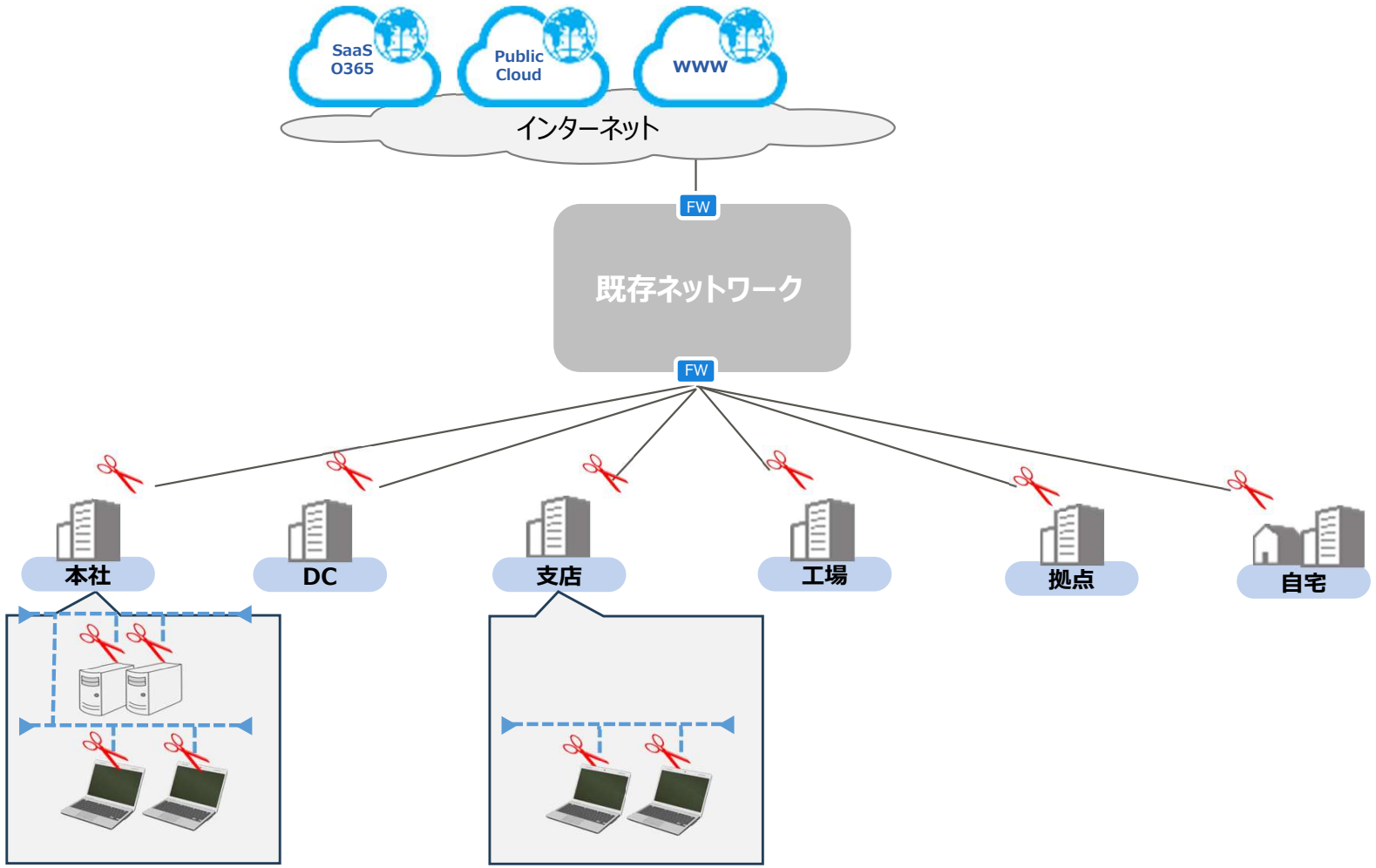
【効果】下記対応を完了しており、第三社機関からも安全との評価を頂いています　**2022.03当時**

① 全端末(全社)の抜線	各部門
② サイバー犯罪対策の関係各所へ即日通報・報告	第三機関対応チーム
③ 対策本部の設立、対応方針、役割分担の明確化	サイバーセキュリティ対策本部
④ 既存ネットワーク及び感染した機器全てを凍結	社内システム復旧チーム
⑤ 攻撃者【nightsky】による犯行声明の確認（ダークウェブサイト）	サイバーセキュリティ対策本部
⑥ ウイルス対策ソフト会社からのパターンファイル取得（通報後一両日以内）	社内システム復旧チーム
⑦ ADサーバの復旧（新規サーバ構築）→後に凍結	社内システム復旧チーム
⑧ 当社ホームページにおけるサイバー被害報告（第一報）	サイバーセキュリティ対策本部
⑨ 新規ネットワークの構築	社内システム復旧チーム
⑩ 全端末のクリーンインストール	各部門
⑪ 全社員のセキュリティ再教育（e-Learningによる）	各部門
⑫ 脆弱性対応の見直し（基準の見える化、対応手順の見える化）	社内システム復旧チーム
⑬ デジタルフォレンジック調査	第三機関対応チーム
⑭ 既存ネットワーク調査(マルウェアが残存しているかの調査)	第三機関対応チーム
⑮ ダークウェブサイト調査	第三機関対応チーム
⑯ 当社ホームページにおけるサイバー被害報告（第二報）	サイバーセキュリティ対策本部
⑰ 取引先への個別説明・個別対応など	社内外対応専門チーム
⑱ 新規ネットワーク上に各種サーバの再構築(凍結中サービスの順次復旧)	社内システム復旧チーム
⑲ 当社ホームページにおけるサイバー被害報告（第三報）	サイバーセキュリティ対策本部
⑳ セキュリティを強化した新ネットワークの再構築	社内システム復旧チーム

全端末(全社)の抜線

【POINT】　**連絡体制網**や**全体構成の整備**が鍵。普段からの危機管理が有効。
証拠保全の為、電源を切らずネットワークから隔離する。

【効果】　外部からの侵入防御、被害の最小化、被害分析に有効



サイバー犯罪対策の関係各所へ即日通報・報告

【効果】通報、報告を行うことで、関係機関での情報蓄積、分析、動向把握、一般向け公開情報に役に立ちます。

即日通報 (12/31金)

所轄の警察機関

TREND MICRO
トレンドマイクロ株式会社

IPA Better Life with IT 情報処理推進機構

JC3 Japan Cybercrime Control Center
日本サイバー犯罪対策センター

後日報告 (1/27木)

経済産業省
Ministry of Economy, Trade and Industry

商務情報政策局
サイバーセキュリティ課
電話：03-3501-1253

ホーム ▶ 政策について ▶ 政策一覧 ▶ 安全・安心 ▶ サイバーセキュリティ政策

サイバーセキュリティ政策

デジタルフォレンジング調査

侵入時期や経路、攻撃手法等を早期発見。サイバー攻撃被害の早急な究明と、マルウェア感染拡大の有無、搾取された情報の推定が可能

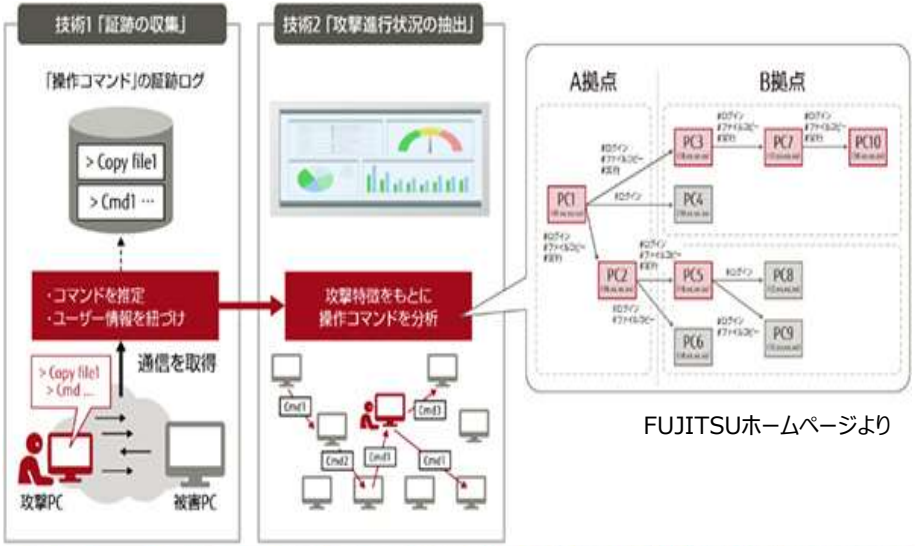
【効果】 第三社機関による専門的調査により、最新の攻撃手法を意識した対応が可能。侵入の痕跡を消し去った情報などが可能。サイバー攻撃の発見直後にデータ保全(ネットワークからの切断、現状確保)が必要

◇調査結果として、以下が判明

① 初期侵入経路の特定：

② 不審な活動の痕跡：

→情報漏洩に対する完全な調査は難しいにせよ、ある程度の推測が可能となり、お客様や発注元への説明や、その後の対応根拠に効果が有った。



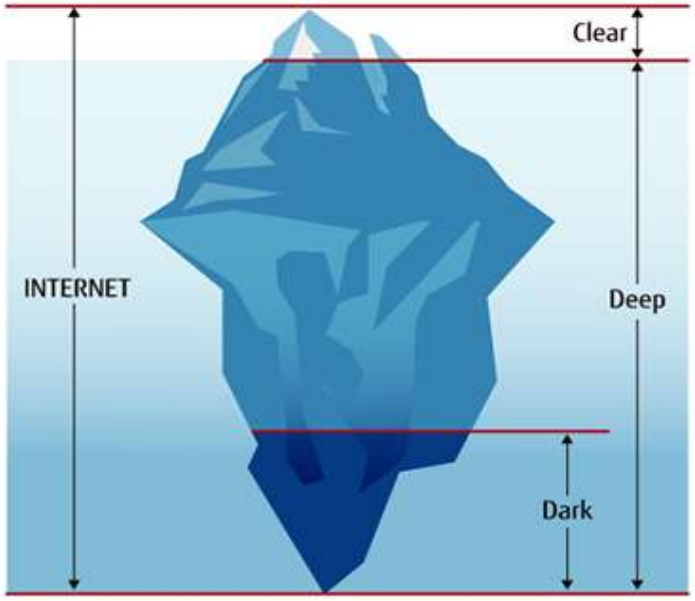
FUJITSUホームページより

「FUJITSUホームページより」

ダークサイトウェブ調査

窃取されたデータを晒す際、一般的に足が付かないダークウェブを利用するケースが殆どであり、攻撃者が窃取、又は可能性が有る弊社データをばら撒いていないか、日々監視を行います。

【効果】　第三社機関による専門的調査により、顧客情報や企業秘密の流出を早期発見。お客様の不安軽減をはかるとともに、会社をリスクから守れます



FUJITSUホームページより

幅広い情報収集

クリアウェブだけでなく、
ディープウェブやダークウェブからも収集

- クリアウェブ：SNSや個人サイト等、誰でもアクセスできるウェブサイトの総称
- ディープウェブ：検索エンジンでは見つけられないウェブサイトの総称
- ダークウェブ：専用のウェブブラウザからのみアクセスが可能な、情報交換やツールの共有な どに利用されるウェブサイトの総称

「FUJITSUホームページより」

※先ずは1年間監視を行い、自社判断で継続監視をしています

(1年間何もないこともあり、継続調査を求められることは無くなった)

→ ダークウェブサイトの監視を開始した2022年2月以降～現時点まで窃取されたデータの流出は検知されておりません。なお、万が一発見された場合には直ぐに適切な対処を行います。

クラウドアプリケーション保護の導入

Trend Micro Cloud App Security

Exchangeなどのメールサービスだけでなく 、クラウドアプリケーションを不正プログラム、情報漏えいからワンストップで保護

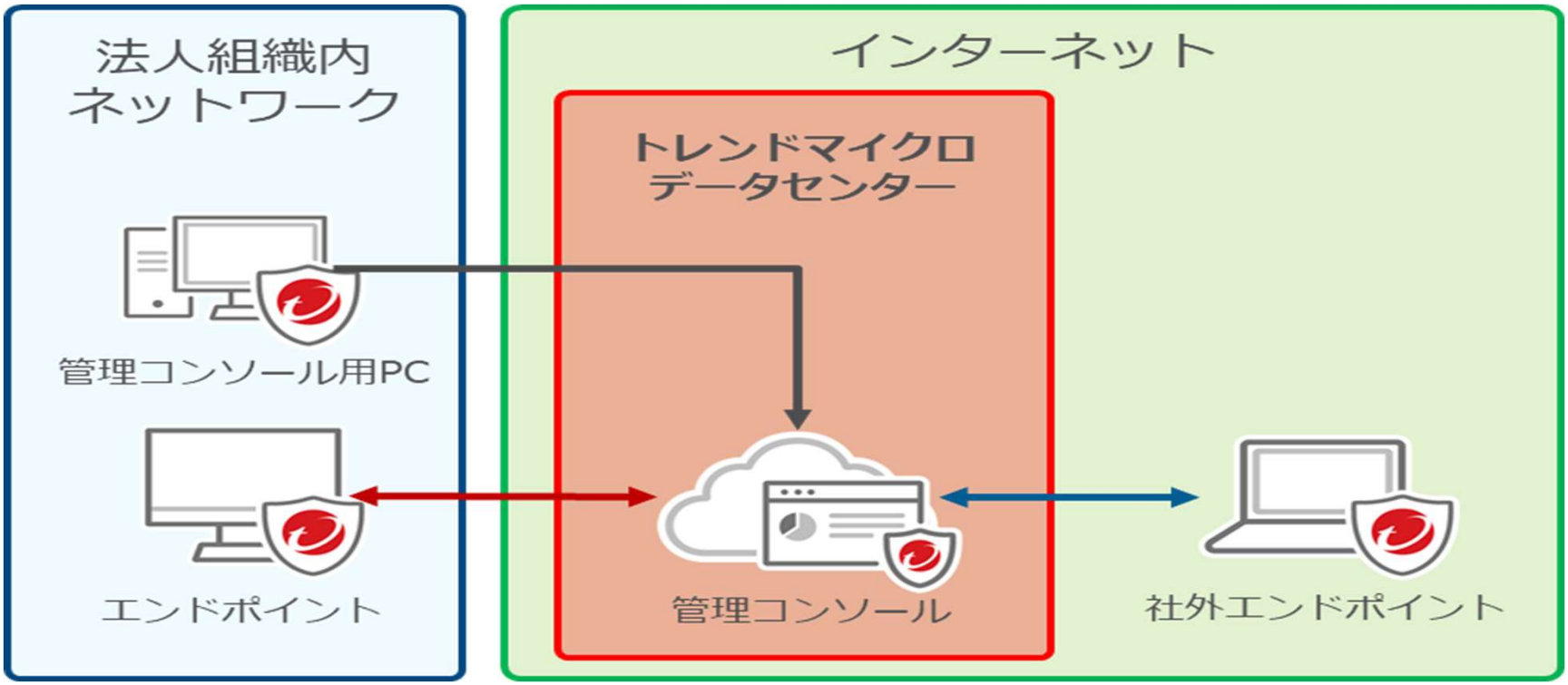
【効果】 当社で利用しているクラウドアプリケーションに関するセキュリティを強化

(他社との接続経路に対するセキュリティ強化 2022.04.01～運用開始)

エンドポイントセキュリティの統合管理

Trend Micro Apex One SaaSに統合(←ApexOne オンプレ等)

エンドポイントセキュリティを実現する為、機械学習やランサムウェア対策など多くの機能を備えたソフト。高度な脅威検出と自動対処が可能で、管理コンソールを用いて統合管理が可能。



TrendMicroホームページより

【効果】
- Apex One SaaSによりタイムラグなく最新版適用が可能
- 一元管理による可視化が可能（デバイスコントロール含む）

外部調査

画面投影のみ

【効果】2022.3以降は、高度なセキュリティを保っていると評価
2023.8以降は、更にセキュリティ強化を実施。

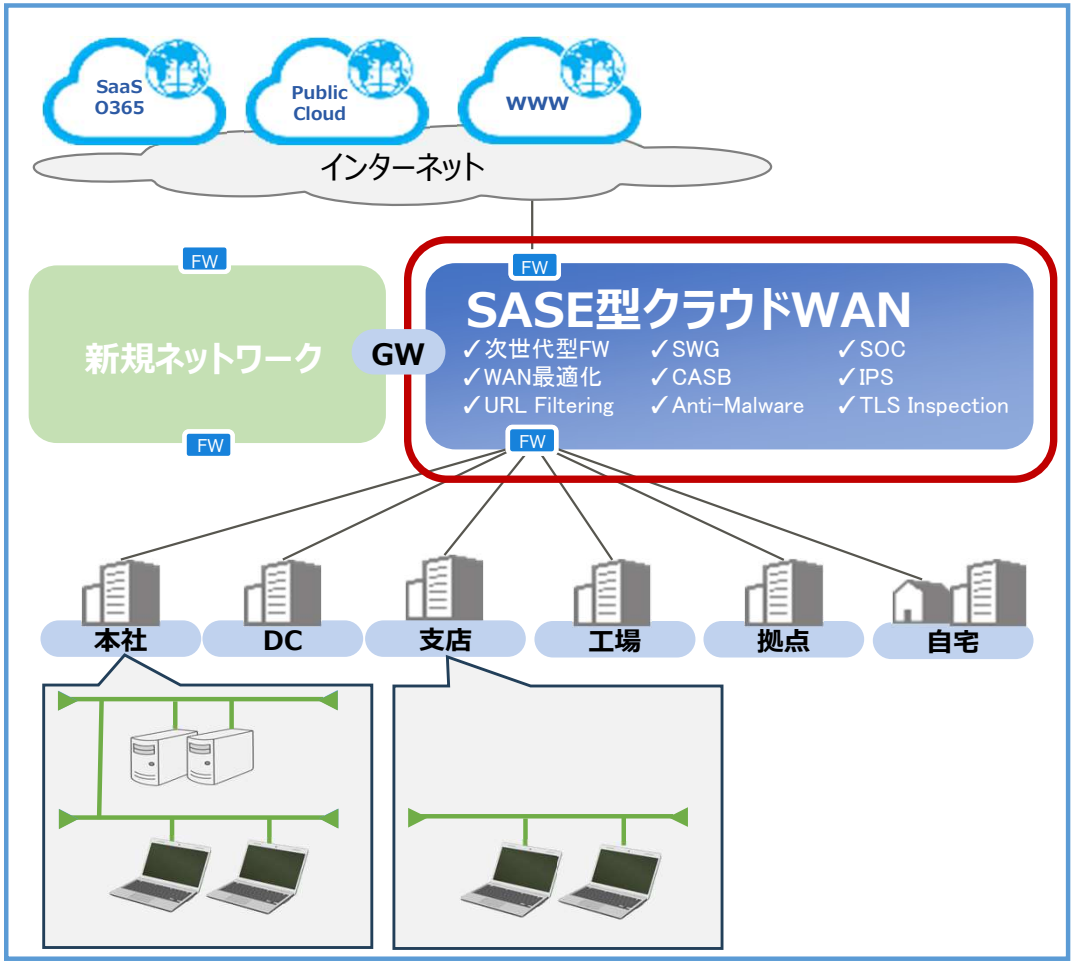
更なる強化へ

問題点と課題

	次世代型NW活用	運用強化	エンドポイント強化
問題	システム環境の変化 (クラウド利用、テレワーク浸透、等) に伴う利用環境の認識不足	新技術への変化及び管理作業増大に対する体制不足	攻撃の高度化・多様化による従来型対策の効果不足
課題	・セキュア＆透明性 ・安全活用	・自動化(省力化) ・効率化	・侵入を前提とした対策
対策	ＳＡＳＥ (ＣＡＳＢ等)	ＳＯＣ 運用の効率化	ＥＤＲ ＮＤＲ

SASE運用について

【POINT】
導入前に検証期間をしっかり確保する (動作確認の他にもパフォーマンスなど細部まで確認する)
運用面を考慮した相手(サービス)の選定が必要 (サポートレスポンスも重要)



◇各種サービスについて(一部ご紹介)

・クラウドサービスの利用状況を可視化/制御し、一貫性のあるセキュリティポリシーを適用
→ CASB (Cloud Access Security Broker)

・サイバー攻撃の検知や分析
→SOC(Security Operation Center)

・クラウド型ファイアウォール
→次世代型FWaaS (Firewall-as-a Service)

・危険なサイトやコンテンツへのアクセスを遮断
→SWG(SecureWebGateway)

→2023年8月以降 SASE運用を開始

【効果】 セキュア＆透明性のあるネットワークが実現。
自動化や効率化も推進し、社員の負荷軽減に繋がった。

SASE 比較結果<1/2>

	A社		B社	
業務に必要なInternetサービスにアクセスできる(SWG)	○	一部のhttpsのサイトについては、複合除外が必要	○	一部のhttpsのサイトについては、複合除外が必要
クラウドサービス(CASB)	○	主要なサービスで特に問題なし	△	M365系のアップデートは外部ドメイン指定が必要
社内のサービスにアクセスできる	○	PoC環境では社内サーバへはアクセス不可のため、Split Tunnelで除外し既存NW機器で直接通信	○	既存NW機器でルーティングされているため直接通信
拠点内をセキュアに通信できる	○	Off Cloud機能にて可能	△	既存NW機器のみで可能だがsigraki環境ではバグが発生しているとの情報あり
特殊な業務(通信フロー)、指定サイト通信	―	検証環境から顧客NWへのVPN接続不可(Split Tunnelで直接通信可能) →許可するかは各事業部にて判断	―	検証環境から顧客NWへのVPN接続不可(外部ドメイン指定で直接通信可能) →許可するかは各事業部にて判断
グローバルIPを固定化できる	○	3つまでは無償で利用可能 (PoCで実施済)	△	オプションで提供(PoCでは未実施)

SASE 比較結果<2/2>

	A社		B社	
社内(サーバ室や拠点内)機器へのアクセス拒否	○	Device Posture機能で可能	×	未実装
クライアント展開のしやすさ	○	Setup.exe でインストールするのみ ※PoC環境ではSSO認証としたため、初回にM365の認証が必要	△	指定ツールのインストールおよび.jsonファイルの配置が必要
管理画面の使いやすさ	△	各項目の階層が深く直感的に解りづらい UI構成(改善の兆しあり？？)	○	解りやすいメニュー体系
ログの見やすさ	△	ぱっと見の項目が多すぎる印象	○	比較的見やすい印象
テレワーク対応	○	専用VPN Clientで社内ネットワークにVPNアクセス可能	△	社内ネットワークへのアクセスを可能とするには既存NW機器側でのVPN設定および指定ツールで接続操作が必要
全社展開の容易性及び費用対効果	○	全拠点新規NW機器が必要かは要検討だが、既存NW機器が不要になるためライセンス費用が必要なくなる	△	既存NW機器利用の想定で展開は容易だが既存NW機器のライセンス費用は引き続き発生
サービスの安定性、サポート品質について	○	サービスに不安定な要素はなかったが誤検知(カテゴリ分類)が何件かあった PoC期間中のサポートは対応が早かった	△	指定ツールの接続が切れる状況が何度か発生 (Retryで自動的に復旧はする) PoC期間中のサポートはレスポンスが悪かった

まとめ

身代金を支払うのが得策か

【POINT】 身代金の支払いは、インシデント対応を遅らせ、多額の被害状況にさらにコストがかかる

Paying the ransom doubles recovery costs

Overall, 46% of organizations surveyed that had their data encrypted paid the ransom and got data back. Larger organizations were far more likely to pay with more than half of businesses with revenue of $500 million or more admitting that they paid the ransom.

However, the survey also shows that when organizations paid a ransom to get their data decrypted, they ended up doubling their non-ransom recovery costs ($750,000 in recovery costs versus $375,000 for organizations that used backups to get data back).

Moreover, paying the ransom usually meant longer recovery times, with 45% of those organizations that used backups recovering within a week, compared to 39% of those that paid the ransom.

“Incident costs rise significantly when ransoms are paid. Most victims will not be able to recover all their files by simply buying the encryption keys; they must rebuild and recover from backups as well. Paying ransoms not only enriches criminals, but it also slows incident response and adds cost to an already devastatingly expensive situation.”

Chester Wisniewski, field CTO, Sophos

SOHOS NEWSより
The State of Ransomware 2023
https://news.sophos.com/en-us/2023/05/10/the-state-of-ransomware-2023/l

今後に向けて

- 一度ランサムウエアに感染してしまうと、身代金要求額は
  数百万円～数千万円　×n回の可能性…
- ランサム(身代金支払)に応じなくても、企業規模にもよるが復旧に
  数千万円～数億円
- 被害前の運用レベルまで復旧するのには、
  数ヶ月 ～ 1年以上

やはり日頃の防御対策が重要であり、
有事の対策ルール化をお薦めします！

クラウド型FWサービス

TCG

Solution & Creation

～ICTでお客様に喜びを～