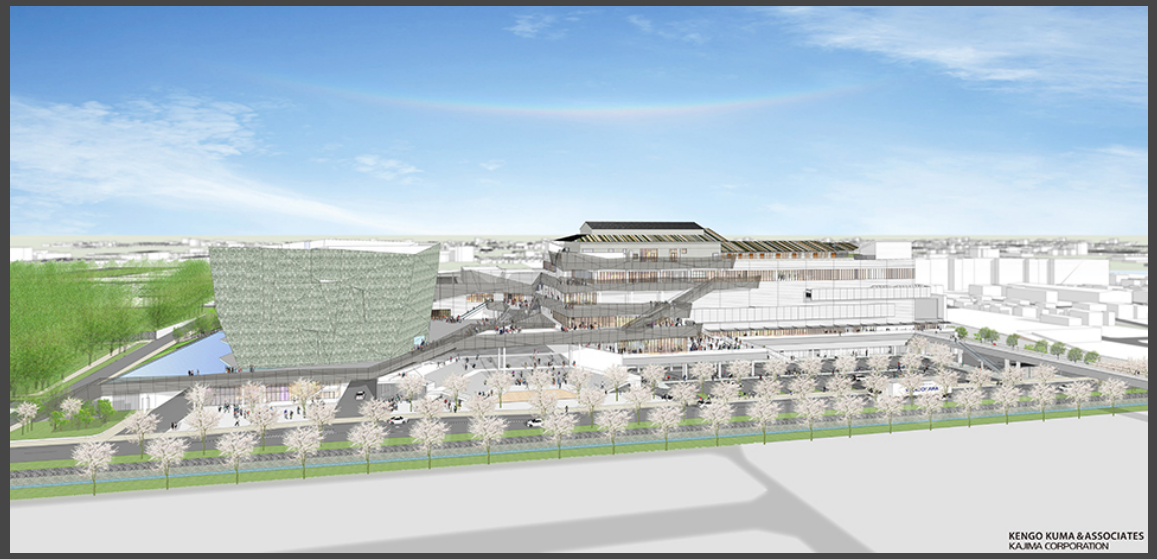
実録CSIRT24時！
その時なにが起きたか！
CSIRT活動事例その1

株式会社KADOKAWA デジタル戦略推進局 事業技術開発部
西村卓也（nishimura-t@kadokawa.jp）

簡単に自己紹介

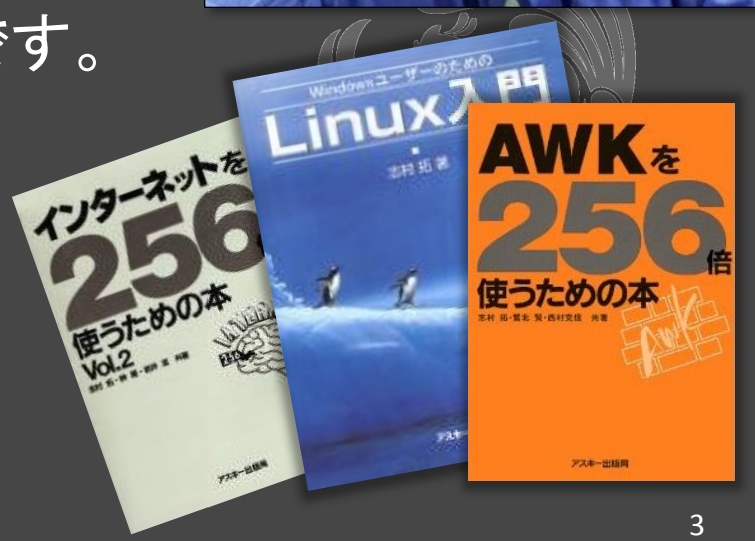
- 今は（KADOKAWAの情シス、デジ戦で）
  - システムの企画・設計・開発してます（コードも書けば、PMもします）。
  - KADOKAWA-CSIRT事務局でセキュリティ対応してます。
  - 社内重大システムのプロジェクト監理もやってます。
  - 最近はところざわサクラタウンのシステム導入、ネットワーク設計してます。



KADOKAWA

簡単に自己紹介（という割には2ページ目）

- 昔は（高校三年でapple][に出会って以来）
  - 某建築事務所でC言語でX11で動くCAD書いてました。
  - 東京藝大や武蔵野美大で非常勤講師してました。
  - コンピュータ雑誌や書籍に原稿書いてました。
    （志村拓名義で20冊強）
  - インターネット黎明期にJUNETにUUCP接続してました。
  - というわけで、ロートルのフルスタックエンジニアです。
    （いわゆるテッキー？）



KADOKAWA-CSIRT

- 経緯
  - 2013年10月に9社合併、翌年1月の松の内に公式サイトが改竄される
  - この対応に、情シス内で旧アスキー系エンジニアが活動開始
  - 合併後の混乱もあり、自社で運用するWebサイトの数さえ把握不能
  - 個々のWebサイトの把握、脆弱性状態のチェックを開始
  - 2014～2015年は毎月どこかのサイトが攻撃されている状況
- 組織
  - 2014年12月にKADOKAWA-CSIRTを仮想組織として正式に設立
  - 2015年03月に日本シーサート協議会に加盟
  - 2017年03月に産業横断サイバーセキュリティ人材育成検討会に加盟

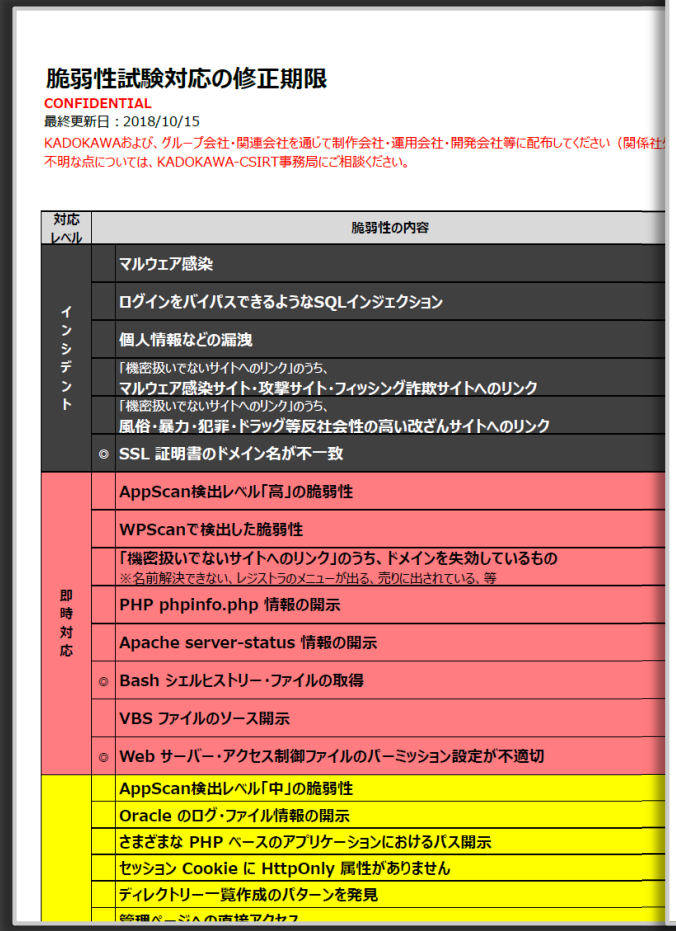
KADOKAWA

対外サービス防衛な活動

- 歴史的経緯から、活動は対外サーバ類が対象
  - 対外サービスを把握し、統制するためのルール、申請書を整備。
  - 対外サービスを守るための、組織、インフラ、運用ルールを整備。
  - 活動範囲は、KADOKAWA及び全グループ子会社。
- 作った申請書・ルール
  - Webサーバ公開・更新・削除申請書、ドメイン取得申請書、サーバ証明書取得申請書、脆弱性試験依頼書等々。
  - Webサイト構築チェックリスト、KADOKAWAパスワード基準仕様、警察署の開示請求に関するガイドライン、脆弱性トリアージシート等々。
  - KADOKAWA-CSIRT全体会議開催。（参加対象者は100名強）

KADOKAWA

申請書・ルールの例



脆弱性試験対応の修正期限

CONFIDENTIAL

最終更新日：2018/10/15

KADOKAWAおよび、グループ会社・関連会社を通じて制作会社・運用会社・開発会社等に配布してください（関係社
不明な点については、KADOKAWA-CSIRT事務局にご相談ください。

対応レベル		脆弱性の内容
インシデント		マルウェア感染
		ログインをバイパスできるようなSQLインジェクション
		個人情報などの漏洩
		「機密扱いでないサイトへのリンク」のうち、 マルウェア感染サイト・攻撃サイト・フィッシング詐欺サイトへのリンク
		「機密扱いでないサイトへのリンク」のうち、 風俗・暴力・犯罪・ドラッグ等反社会性の高い改ざんサイトへのリンク
	◎	SSL 証明書のドメイン名が不一致
即時対応		AppScan検出レベル「高」の脆弱性
		WPScanで検出した脆弱性
		「機密扱いでないサイトへのリンク」のうち、ドメインを失効しているもの ※名前解決できない、レジストラのメニューが出る、売りに出されている、等
		PHP phpinfo.php 情報の開示
		Apache server-status 情報の開示
	◎	Bash シェルヒストリー・ファイルの取得
		VBS ファイルのソース開示
	◎	Web サーバー・アクセス制御ファイルのパーミッション設定が不適切
		AppScan検出レベル「中」の脆弱性
		Oracle のログ・ファイル情報の開示
		さまざまな PHP ベースのアプリケーションにおけるパス開示
		セッション Cookie に HttpOnly 属性がありません
		ディレクトリー一覧作成のパターンを発見
		管理ページへの直接アクセス

Webサイト公開申請書

提出日　　年　　月　　2 日

申請者

所属

氏名　　印

Mail　　@kadokawa.jp

申請内容	プルダウンから選択			
サイト名				
サイトURL	http://			
公開開始日	年　月　日			公開
永続化	しない		サイト種類	
メールマガジン配信	有	会員登録	有	個人
脆弱性診断状況	未	脆弱性診断会社		

ステークホルダー

部署			
担当者		メール	
部署/会社			
担当者		メール	
部署/会社			

● **Webサイトの脆弱性対応指針 チェックリスト**

IPAの配布している冊子『安全なウェブサイトの作り方』をベースにチェックリストを作成しました。
項目をチェックしていくことで既知の主要な脆弱性を解消できるようになっておりますので、脆弱性試験時に重大な脆弱性が検出されにくくなり修正にかかる負担が軽減することが期待できます。
開発開始時などに開発業者などに配布していただき、参考としていただければ幸いです。 なお、こちらの書類は提出する必要はありません。

【参考】IPA『安全なウェブサイトの作り方』改訂7版
https://www.ipa.go.jp/security/vuln/websecurity.html

● **Webサイト運用におけるセキュリティ対策指針 チェックリスト**

ハッキングを受けにくく安全にWebサイトを運用するための指針をチェックリスト形式にしてまとめました。
見落としがちなポイントをまとめてありますので、参考にしてください。

【参考】 パスワード作成のガイドライン 脆弱性情報ソース

● **Webサイト構築方針 チェックリスト【NEW】**

Webサイトを構築する際にネットワークやOS、ミドルウェア等の設定で考慮してほしい事項を
チェックリストにまとめました。KADOKAWA TY3Cloud1/2でも利用している設定方針ですので
ぜひ参考にしてください。

● **CMSを利用したWebサイトの構築・運用 チェックリスト**

WebサイトでCMS（Content Management System）を安全に利用するにあたって、構築時・運用時に気を付けたい事柄をチェックリストにまとめました。
ぜひ参考にしてください。

【参考】IPA『IPAテクニカルウォッチ「CMSを用いたウェブサイトにおける情報セキュリティ対策のポイント」』
https://www.ipa.go.jp/security/technicalwatch/20160928-1.html

● **KADOKAWAのパスワード基準 チェックリスト【NEW】**

KADOKAWAのサイトで守っていただきたいパスワード認証機構の基準です。

【参考】 KADOKAWAのパスワード基準仕様

● **Apacheの設定指針 チェックリスト**

Apacheのhttp.confやssl.confで最低限設定しておいてほしい項目です。

● **WordPressの設定指針 チェックリスト**

豊富なプラグインと自由度の高さで人気のあるWordPressは非常にクラッカーに狙われやすいCMSです。
セキュリティを高める典型的な設定をまとめましたのでぜひ参考にしてください。

● **サイト閉鎖基準**

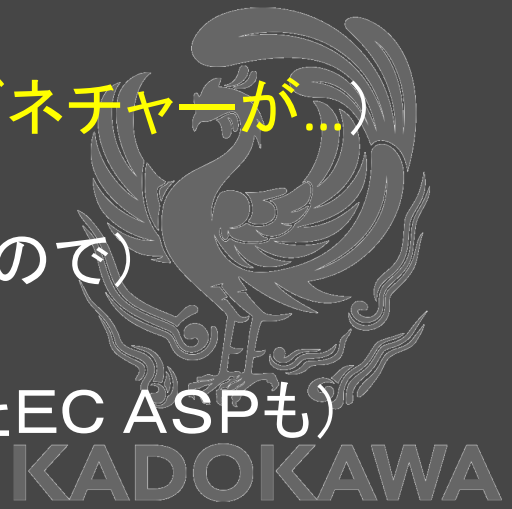
守れてきた対外サービス①

- Webサイトの管理
  - サイト公開申請書と年次棚卸でサイト把握
  - 公開時、年次棚卸時に脆弱性試験を実施し、脆弱性に対応
    （AppScan、WPscan、その他で毎年1,000サイト以上を試験）
- Webサイトの防御
  - DCの集約とIPS、WAFの導入、DDoS対策サービスの適用
    （アノニマスからの攻撃時、浜松方面の方とFBで相談した事も）
  - SOCによる上記機器・サービスの24時間監視と初動対応を委託
  - 主に役立っているのは、IPS（Proventia）とDDoS対策（PROLEXIC）
    （あまりHTTP[S]に攻撃は来ないのでWAFが遮断することは稀）

KADOKAWA

守れてきた対外サービス②

- Webサイトのインシデント対応
  - KADOKAWA-CSIRTの活動啓蒙。
    （発生インシデントや静寂性情報の社内SNSによる周知など）
  - 緊急連絡先への連絡の徹底。
- それでも残る若干の不安
  - AWSなどのクラウド環境や安価なVPSが心配
    （対応しているSOCが少なくWAF運用が自前、しかもシグネチャーが…）
  - それでもCDNが入れられれば、DDoSは防げそう
    （最近はFlood系、Refection系やUDPパケットが大半なので）
  - 更に、ASP/SaaSサービスも、セキュリティ対策に不安
    （一発のDDoS攻撃で、複数のECサイトが一斉ダウンしたEC ASPも）

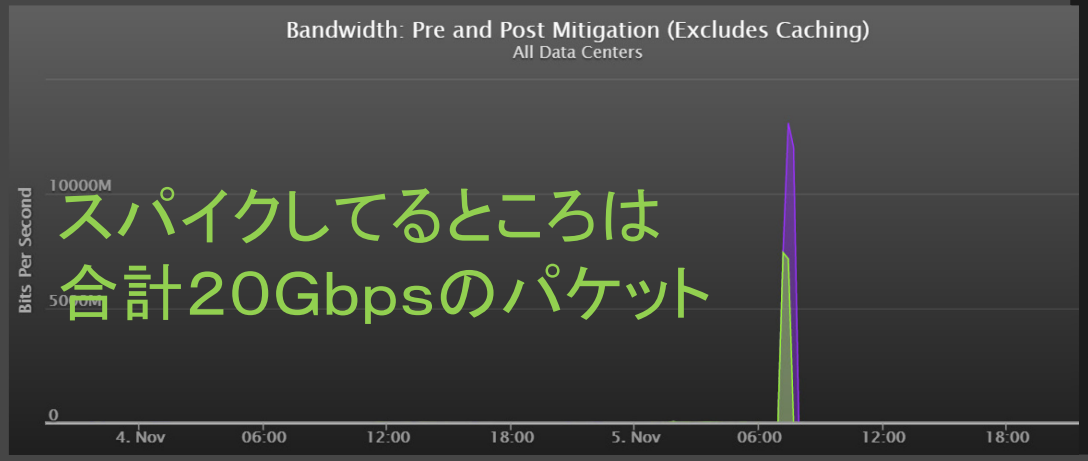


守れてきた対外サービス③

- そういえば、今月も大きなDDoSきました
  - 我が兄弟会社も含め多くのサイト・サービスがやられた
  - KADOKAWAもASCII.jpを対象に20Gbpsくらい
  - CLDAP ReflectionとDNS FloodとUDP Fragment
  - 今までにあまり無いほど、全世界からの攻撃
  - PROLEXICiさんも10分程度対応に時間を要したが、それだけで済んだ

16か所のトランジットポイントからDDoSパケットが流入している

ロケーション	帯域幅	1秒あたりのパケット数
AMS3	90[illegible] Mbps	92.4 Kpps
[illegible]A2	2.5 Gbps	253.6 Kpps
DFW3	687.7 Mbps	68.9 Kpps
FRA2	1.9 Gbps	193.4 Kpps
HKG2	746.0 Mbps	76.0 Kpps
LAX3	321.7 Mbps	31.2 Kpps
LGA3	538.6 Mbps	54.2 Kpps
LON2	1.5 Gbps	151.0 Kpps
MIA4	393.7 Mbps	39.3 Kpps
ORD3	530.4 Mbps	52.8 Kpps
PAR3	418.0 Mbps	42.1 Kpps
SIN3	667.8 Mbps	68.4 Kpps
SJC2	610.8 Mbps	63.1 Kpps
STO3	261.4 Mbps	25.2 Kpps
TYO2	1.2 Gbps	121.5 Kpps
VIE3	227.5 Mbps	23.3 Kpps



スパイクしてるところは
合計20Gbpsのパケット

気が付くと足元に火が①

- 社内のセキュリティはOAを管理する部署が奮闘していた
  - F/Wとウィルス対策ソフトで水際対策。社内LANは無菌状態が前提。
  - 昨今の標的型攻撃と多様な亜種ウィルスに対して限界が。
- 気が付けば結構危険な状況
  - メールの怪しげな添付ファイルを開いた、サーバの脆弱性を突かれた等々。
  - グループ会社ではウィルス感染のPC、社内サーバも見つかる。
- 更に、カジュアルに紛失される会社スマホ
  - 大抵、金曜日の夜か、土曜日の朝にCSIRTに連絡が。
  - 今のところ小説は事実より奇なりで済んでいるが…

KADOKAWA

気が付くと足元に火が②

- 社内でウィルスパンデミックが起ったら
  - 昨年、標的型攻撃メール耐性訓練を行った。
  - 無謀にも、前出のOA管理部署のスタッフにも知らせずに実施。
  - 各所から、「こんなメールを開いてしまった！」と連絡が大量
  - 意外と直ぐに、対応能力がパンク→これが訓練でなかったら((;゜Д゜))

- そろそろ、社内のPC、サーバを守らねば
  - と思っている矢先に、起きたインシデント
  - 次ページから紹介します…

KADOKAWA

今年の事案①

- はじまりは今年の２月
  - 関連会社の社内Windowsサーバにウィルスが検知される
  - CSIRTによるフォレンジックの結果、Office_Updaterウィルスと判明
  - PowerShellで動く、ファイルレス型
  - 発生時T社、S社のアンチウィルスともに不検知（ちなみにM社は検知）
- 被害状況は
  - 仮想通貨の採掘に勤しんでおられた
  - ADサーバをはじめとする多くのサーバに感染の痕跡

KADOKAWA

今年の事案②

- 感染経路は
  - Eternal Blue脆弱性をついて感染拡大。
  - 去年のMS17-010（2017年6月）が未だ当たっていなかった。
  - サーバ構築時の試験用アカウント“test”（パスワードも“test”）が残存。
  - 感染経路はLAN内のPC経由か、サーバでの不用意な操作？
  - 各種ログが十分に取られていないので、あまり解析できず。
- どうゆう管理・運営？
  - 大手ISV業者の担当者が1人と社内担当者1人で対応。
  - パソコンには詳しいが、セキュリティには詳しくない。
  - システムアップはできるが、安全性は担保できない状況。
  - 存外、こうした状態、少なくないかも。

KADOKAWA

今年の事案③

- ともあれ対策
  - 全サーバは、何が仕込まれたか判らないので、構築し直し。
  - 構築時試験用のアカウント“test”も削除指示。
  - Firewallをはじめ多くの機器で十分なログ取得・保持を指示。
  - 調べてみるとMS17-010が適用されていないPCが数十台。
  - 侵入経路が明確になっていないので、Windows7は全て再インストール。
  - これを契機に、全社でWSUSでのアップデート配信を無条件とする。
- インパクト
  - これから数ヵ月にわたり、上記対策を行っていく対応工数。
  - 本社側からPCを貸与するも、使えるPCの数は半減。

KADOKAWA

今年の事案④

- ６月、再びの感染
  - 関連会社のサーバが「まさかの」再び感染。
  - CSIRTがフォレンジックすると、testユーザで外部から侵入の痕跡！
  - 削除しろ！って言ったじゃん！→忘れてました→トホホ
  - ログ出して→取れてません→指示したよね→これからやるとこ…→トホホ
- プレイヤーを変えよう
  - こんどのウィルスは感染力が強そう。
  - 4ヵ月かけてPC再インストールが終わりそうな矢先。また再インストール？
  - 同じスタッフィングでは、同じ結果。
  - プレイヤーを変えることを決断。

KADOKAWA

今年の事案⑤

- SecureWroksに相談だ
  - IPAのJSAコンソーシアムの懇親会での挨拶がきっかけ。
  - 全PCのフォレンジックを依頼。
  - 同社のRed Cloakを全体PC、サーバにインストール。
  - 数週間のSecureWorksが不審な通信や振舞いが無いか監視・診断。
  - 台数の割に意外と安価だった。 →だいぶ素敵！
  - 幸いなことに、特に問題がないとの判断。 →だいぶ素敵！
  - PCは再インストール無しに復帰。 →だいぶ素敵！
- 関連会社のネットワークも
  - 本社の管理部門で運用管理を巻き取る。
  - これに伴いネットワーク構成も大幅に変更。

KADOKAWA

イマドキなEUCセキュリティの状況

- 瓦解していく従来のセキュリティ対策
  - 亜種が多数発生している（WannaCryはバグが原因で亜種が大量？）。
  - パターンマッチでは検知しきれない（とメーカが白旗あげてる？）。
  - 標的型の攻撃は、巧妙で機械的には防げない（利用者の気づき頼み）。
  - どこでも働く的なワークスタイル変化に対応が辛い。
  - 検疫ネットワークも作りにくい？（VPNでというのもまだるっこしいし）
  - ともするとBYODな端末も守らなければならない。
- セキュリティ確保のトポロジが変わってきている
  - どんなネットワークに接続しても、EUCを守らなければならない。
  - つまり、ネットワークでなくEUCで守らねばならない。
  - しかも、従来のセキュリティソフトだけだと心もとない。

KADOKAWA

ワークスタイル変革とセキュリティ①

- KADOKAWAの事情
  - 2020年に前出の「ところざわサクラタウン」が東所沢に完成する。
  - これに伴い、現状の飯田橋拠点と東所沢拠点の2か所の拠点ができる。
  - さらにサテライトオフィスや在宅勤務を進め「どこでも働ける」ようにする。
  - 既に本社ビルではフリーアドレスが始まっている。
  - マ・ジ・で・す・か　…
- いままでは
  - 部署ごとにVLAN、ビル毎に設定して、無用な通信を遮断。
  - ネットワークのセキュリティポシリーをLANという閉域で確保。
  - LANのインターネットトランジットのFirewallで水際防御。
  - これらが通用しなくなる。

KADOKAWA

ワークスタイル変革とセキュリティ②

- どこでも安全にPCを使うために
  - PCにデータを置かない→VDI化→結局VDIに感染する→コレジャナイ感
    （端末を守る以上に情報資源を守ることが目的なので）
  - PCにデータを置かない→アプリをSaaSで→我慢できれば→無くは無い
    （BYODへの展開も可能そう）
  - PCの所作を常に監視→SOC監視→何かあればPCをロック→これか!?
    （最も安全なのはVDIをSOC監視か？）
  - もちろん、多重防御の観点からアンチウィルスは存続。
- 総務省「テレワークセキュリティガイドライン（第4版）」（案）
  - よく整理されている。組織のコンセンサス用には大変有用！
  - セキュリティ対策の部分は、不明瞭（抽象的）な部分も多く、ちょっと…

KADOKAWA

パンデミックに対応するために

- 万一の際にもPCが使えるように
  - 各SW等に監視機器導入→LAN監視→LANだけ守ればOK？
  - 発信源のPCの所作を検知→SOC監視→該当PCを排除→やっぱこれ!?
- 社内LANを超えた防御が必要
  - SOC監視のためのセンサーを備えたEDR製品の導入が必要。
  - インターネット経由でSOC監視ができる製品でないとダメ。
  - PCは台数が多いので、効率的で安価な対応が可能なSOCが重要。
- フラットなネットワークの脅威
  - どこでも働ける、となるとネットワークはフラットになりがち。
  - これはウィルス感染がどこまでも伝搬してしまうリスク。
  - Wi-Fiは対策あるが、有線が結構面倒。（一人1VLANなら…キャリアかよ）

抜本的なEUC対策の再考

- ということで、EDR＋SOCを検討中
  - Endpoint Detection and Response
  - PCやサーバにエージェントを入れ、それをSOCが常時監視する。
  - PCやサーバのメモリやネットの利用といった振舞いから脅威を判断。
- 現在のところ
  - 現在、色々な製品を比較検討中。
  - Carbon Black、Crowd Strike、Red Cloak等々。
  - もちろん、多重防御としてアンチウィルスも必要。
  - インベントリ取得ソフトや各種社内アプリ等との相性はPOCが必要そう。
  - フラットネットワーク対策については、現在模索中。
    何か妙案があれば教えてください！（高いところからすいません）

KADOKAWA

Thank you for your attention !

KADOKAWA