サイバーセキュリティの最新トピック

2018年3月5日

川口　洋, CISSP
株式会社ラック
サイバー・グリッド研究所長
チーフエバンジェリスト
hiroshi.kawaguchi @ lac.co.jp

自己紹介

川口　洋(かわぐち　ひろし),CISSP

株式会社ラック
サイバー・グリッド研究所長 兼 チーフエバンジェリスト 兼 チーフ宴会オフィサー(CEO)
内閣府本府情報化参与(非常勤)
富山県警察サイバーセキュリティ対策アドバイザー
WASForum Hardening Project テクニカルリーダー
ISOG-J 技術WG リーダ

2002年　ラック入社
2002年～2012年 社内インフラシステムの維持、運用に従事。その他、セキュアサーバの構築サービスや、サーバのセキュリティ検査業務なども行い、経験を積む。
その後、IDSやFirewall などの運用・管理業務を経て、セキュリティアナリストとして、監視サービスに従事し、日々セキュリティインシデントに対応した。

2013年4月～2016年3月末 内閣官房 内閣サイバーセキュリティセンター(NISC)にて、行政機関のセキュリティ対策支援、セキュリティインシデントの対応、一般国民向け普及啓発活動を行った。

現在はサイバー・グリッド研究所長として、ラック社内における研究開発、サイバーセキュリティに関する情報集約、情報発信を担当。情報セキュリティEXPO、Interop、各都道府県警のサイバーテロ対策協議会などで講演し、安全なITネットワークの実現を目指して日夜奮闘中。

セキュリティキャンプの講師として未来ある若者の指導にあたる。また、最高の「守る」技術を持つトップエンジニアを発掘・顕彰する技術競技会「Hardening Project」のスタッフとして、ITシステム運用に関わる全ての人の能力向上のための活動も行っている。

2017年12月10日 時点 (31)

サイバー空間の出来事

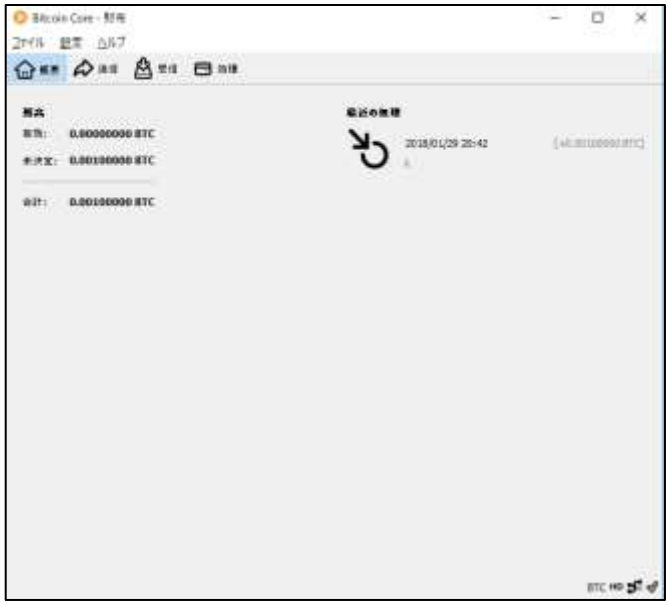
CoincheckのNEM盗難事件

- 事件概要
  - 仮想通貨取引所Coincheckから、2018年1月26日、580億円相当の仮想通貨NEMが盗みだされた
- 原因
  - 不正アクセス（内部犯行は記者会見で否定）
    - 社員、エンジニアを狙った攻撃？？（標的型攻撃、APT、など）
    - 提供ウェブアプリケーションに対する攻撃？？（SQLインジェクション、APIの不正操作、など）
- 犯人
  - 不明
- システム面の不備
  - ビットコイン以外の仮想通貨への対応が後手に回っていた
  - 顧客資産NEMと自社資産NEMを分離していなかった
  - マルチシグ(マルチシグネチャ)を使っていない
  - コールドウォレットを使っていない（すべてのNEM資産がサーバ上で扱われていた＝ホットウォレット）

仮想通貨の管理

個人のウォレット

仮想通貨取引所



ホットウォレット

オンラインのサーバで管理
操作に便利＝攻撃者にも便利

コールドウォレット

オフラインの形式で管理
操作は不便＝攻撃者も不便

犯罪者の視点から仮想通貨でお金儲け

盗む

誰かの仮想通貨を盗んでくる
・ユーザから盗む
(いわゆるバンキングマルウェア)
・取引所から盗む
(CoincheckやMtGOXの例)

だます

誰かをだましてお金を集める
・ニセコイン
・詐欺コイン
・投資詐欺

マイニング（採掘）する

他人のリソースで仮想通貨をマイニング
・コインマイナー
・コインハイブWebマイナー

レートの不正操作

レートを不正操作し、差益で儲ける
・フェイクニュースによる風説の流布
・インサイダー取引
・サイバー攻撃でシステム停止

ビットコインが不正アクセスで30万円分盗難

- 仮想通貨口座に不正ログインされ、入金していた30万円が奪われた
- 2段階認証を設定していた
- 2段階認証の方式はメール形式
- 2段階認証のメール送信先はヤフーメール
- 仮想通貨口座とヤフーメールは同じパスワードを使用

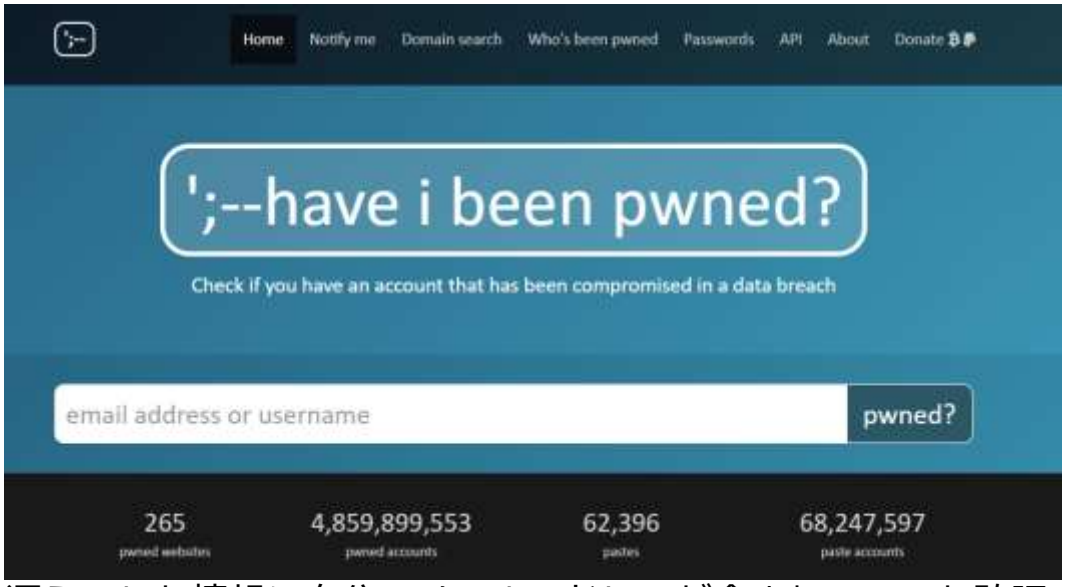
ビットコイン口座に不正ログインされ30万円を奪われた顛末 （Engadget 日本版） - Yahoo!ニュース　より
https://headlines.yahoo.co.jp/hl?a=20180127-00081580-engadgetj-sci

2017年12月のニュース

- 14億件の平文ログインデータが漏洩、最多のパスワードは? (マイナビニュース)
  - ダークWebにおいて14億件を超えるアカウントデータを含んだファイルおよびデータベースを発見した
  - これまでダークWebで発見された流出アカウントデータとしては過去最大規模で、調査の結果、流出したアカウントデータが本物であることも確認された
- ダークウェブに14億件の個人データ流出、有名ポルノサイトも (Forbes JAPAN)
  - 4iQの12月8日のブログによると、41ギガバイトの容量を持つファイルがダークウェブで発見され、その中に14億件分のユーザーネームとパスワードのセットが含まれていたという。

漏えいしたデータの危険性

- 日本のドメイン名のデータも多く漏えいしている
- メールアドレスのユーザの管理責任ではなく、登録したサイトから漏れている可能性が高い
- 漏れたデータは5年以上前のものである可能性が高い＝最新データが漏れているわけではない
- ヤフーメールやGmailなど、認証や決済に使われるサービスは要注意
- パスワードを使いまわしているユーザに対する注意喚起



過去に漏えいした情報に自分のメールアドレスが含まれているか確認できる
https://haveibeenpwned.com/

大阪大学の情報漏えい事件 2017年

1. 教員のIDとパスワードが何らかの経路で盗まれた
2. 教育用計算機システムに教員IDで不正ログイン
3. 教育用計算システムに不正プログラムが仕込まれる
4. システム管理者のIDが盗まれる
5. システム管理者の権限を悪用され、利用者情報が漏えい

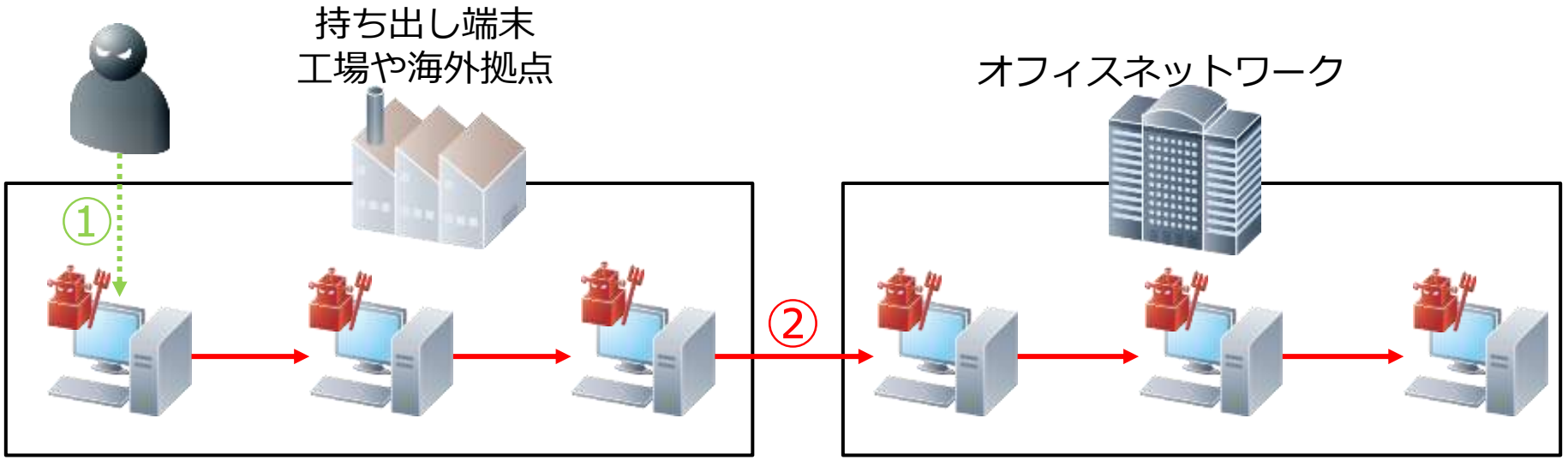
6. グループウェアに対して、教職員59人のIDで不正ログイン
7. 教職員のメールの情報が漏えい

不正アクセスによる個人情報漏えいについて ― 大阪大学
http://www.osaka-u.ac.jp/ja/news/topics/2017/12/13_01

ランサムウェア WannaCry

継続して発生しているランサムウェアの事件

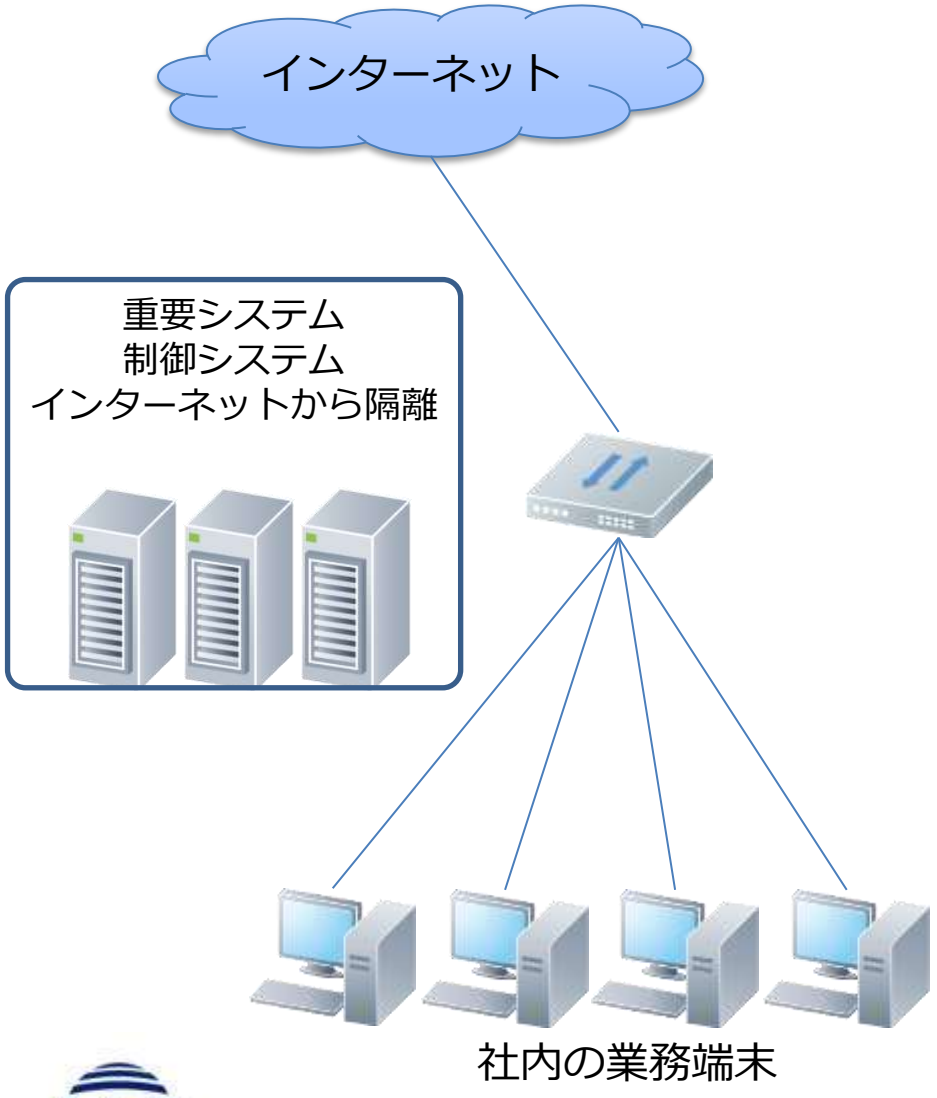
社内に入り込んだウイルスがネットワーク全体に蔓延し、業務が停止する



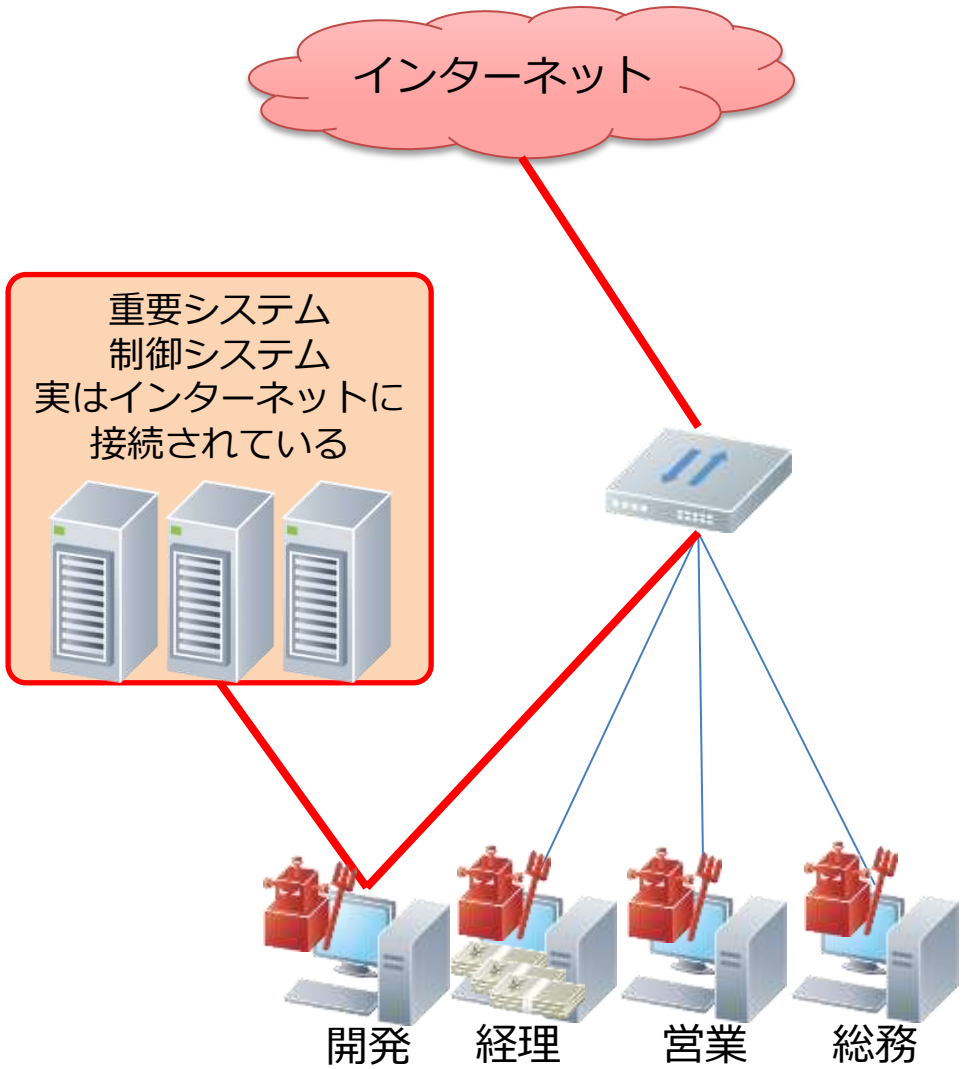
	①初期侵入	②内部展開
技術的課題	・古いOSの存在 ・パッチが未適用 ・グローバルIPアドレスのアクセス制御不備	・パッチが未適用 ・社内ネットワークのアクセス制御不備 ・検知機能がない
組織的課題	・情報資産の未把握 ・ガバナンスが効かない	・トリアージ機能がない ・IT部門とOT部門に壁がある

想像と現実

想像



現実

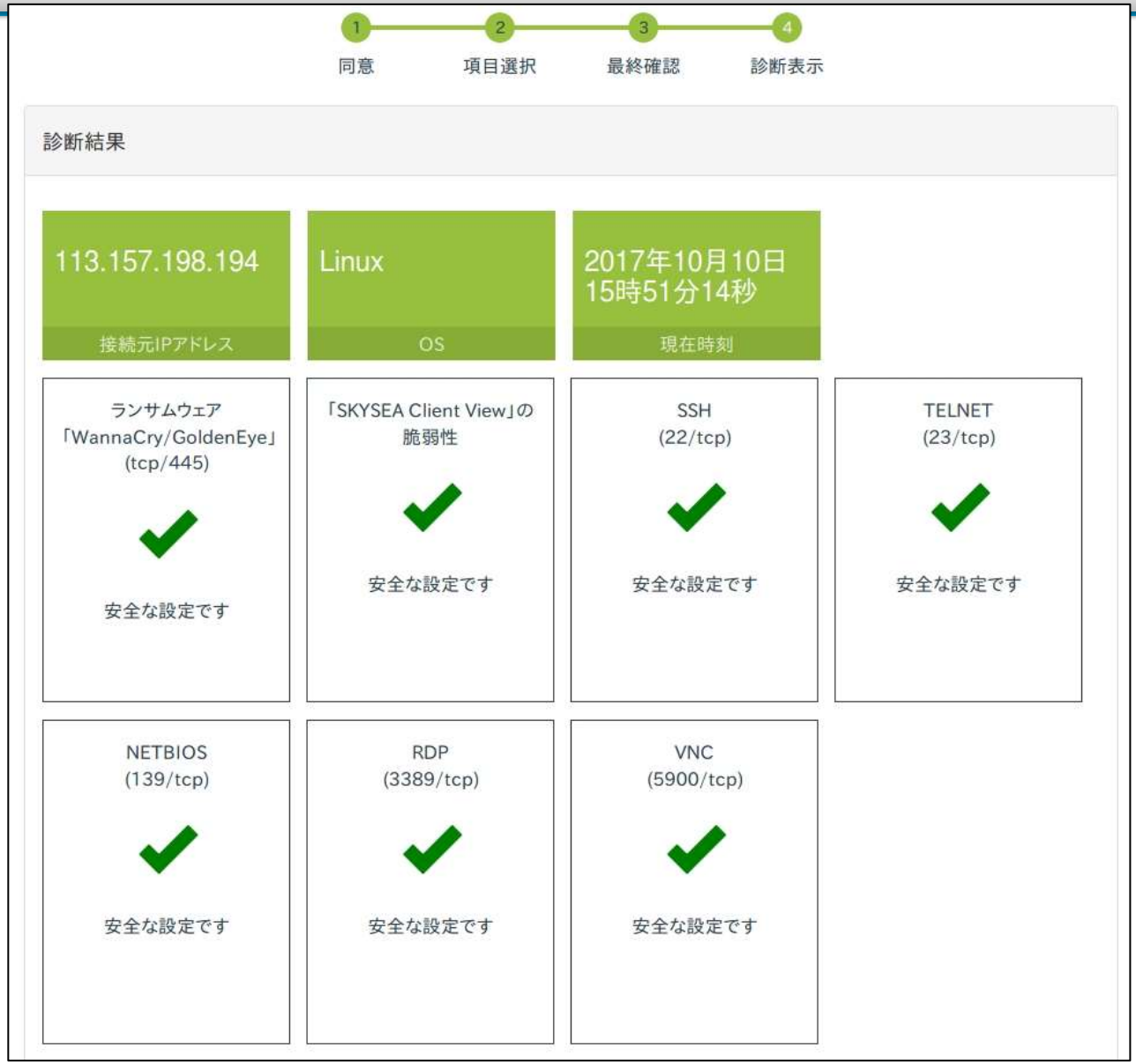


自診くんの紹介

自分のパソコンの無料診断ができるサービス

https://jisin.lac.co.jp/check.php

自診くんの紹介



2017年3月 Strutsの脆弱性

2017年
3月6日
脆弱性情報

3月7日
攻撃開始

3月10日
被害報道

2017年3月のStrutsの脆弱性

ホームページを構成するソフトウェア(Struts2)に重大な欠陥が発見され、サイバー攻撃を受けた

	G社	P社
漏洩件数	約135万件	約15万件
特別損失	2億7000万円	2億円
前期の純利益	約29億円	約12億円

取りうる選択肢

システム担当者	事業責任者
何もしない	何もしない
アップデート	アップデート
フィルタ設定	フィルタ設定
セキュリティ製品で防御	セキュリティ製品で防御
特定機能を無効化	特定機能を無効化
	サービスを(一時)停止

サイバー攻撃の被害を受けた後

システム復旧作業

インターネット接続遮断による業務停止

メディア対応

監督官庁への報告

被害者への謝罪

事故対応担当者の過負荷

これらの事件から学ぶこと

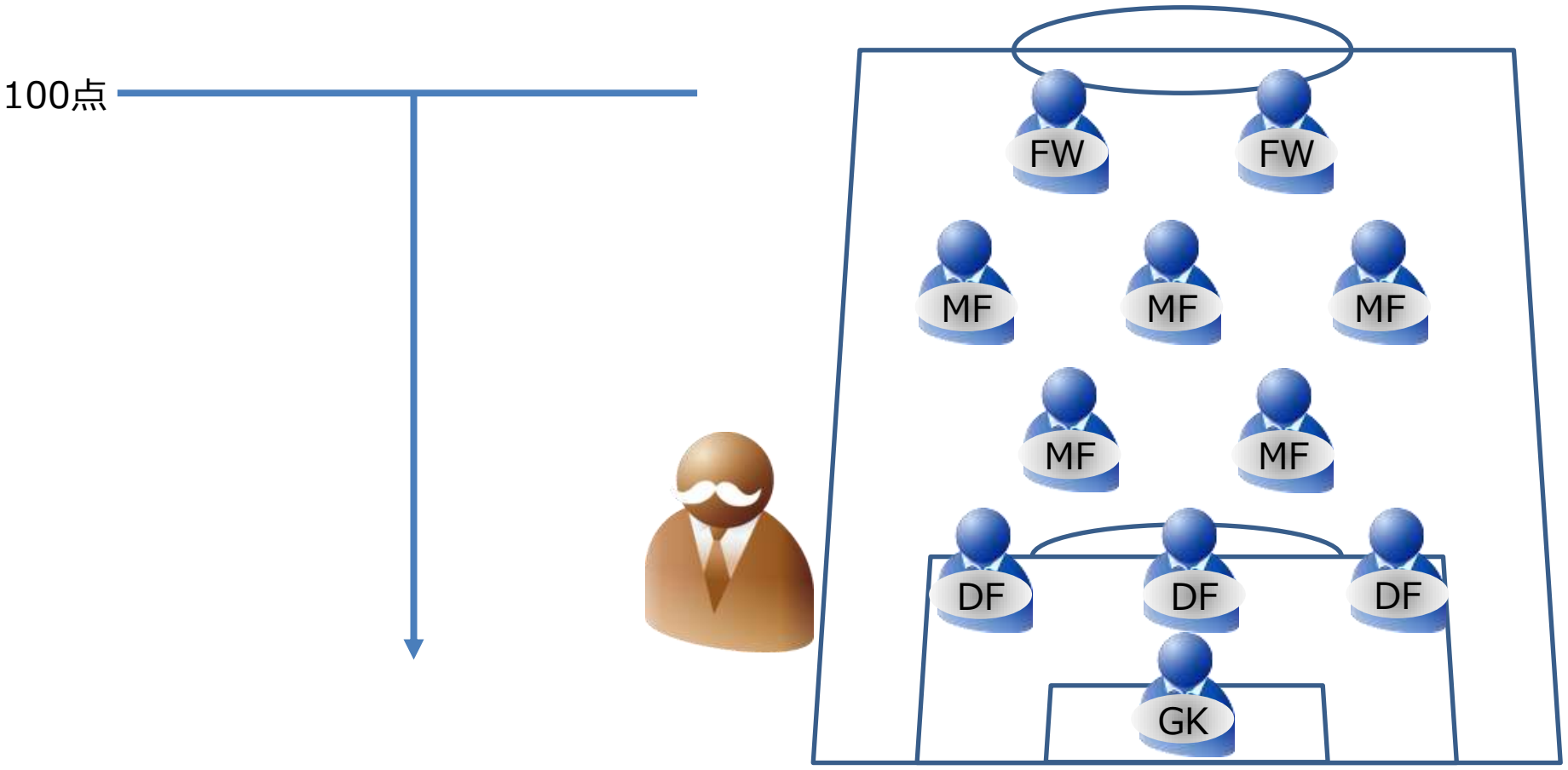
サイバー問題は役員室へ

スピードに応じた安全装置が必要

事後対応の重要性

セキュリティに100点はない？

IT部門のセキュリティ　経営者のセキュリティ



IT部門のセキュリティは100点から下がるしかない

事業継続や事業に影響を与えないセキュリティを考える必要がある＝経営者の役割

Hardening Project

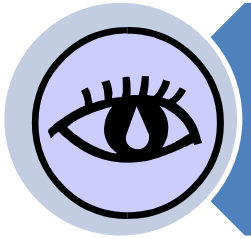
実践的な堅牢化技術の価値を最大化すること

ビジネスの視点

Focus on prevention techniques and process

守る技術の顕彰

Engineering awards and talent discovery



利用者視点の認識向上

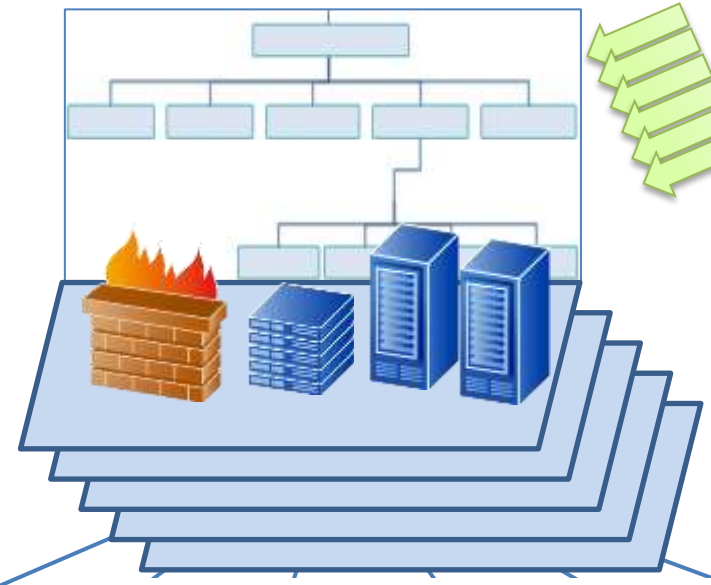
Perspective for stakeholder communication

1. 2012年 4月 Hardening Zero（東京）
2. 2012年10月 Hardening One（東京）
3. 2013年 7月 Hardening One Remix（東京）
4. 2014年 6月 Hardening 10 APAC（沖縄）
5. 2014年11月 Hardening 10 Evolutions（沖縄）
6. 2015年 6月 Hardening 10 MarketPlace（沖縄）
7. 2015年11月 Hardening 10 ValueChain（沖縄）
8. 2016年 6月 Hardening 100 Value x Value(沖縄)
9. 2016年11月 Hardening 100 Weakest Link(沖縄)
10. 2017年 6月 Hardening 1010 Cash Flow(沖縄)
11. 2017年11月 Hardening 2017 Fes(淡路島)
12. 2017年 7月 Hardening（検討中）

Hardening Project

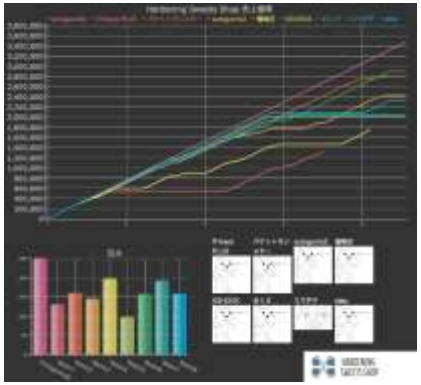
11時間の耐久競技にインターネットの縮図を実現
限られたリソースを最大限に生かし、ビジネス価値の最大化を競う

競技空間で提供される様々なサービスや製品を調達し、自チームに足りない能力を補完

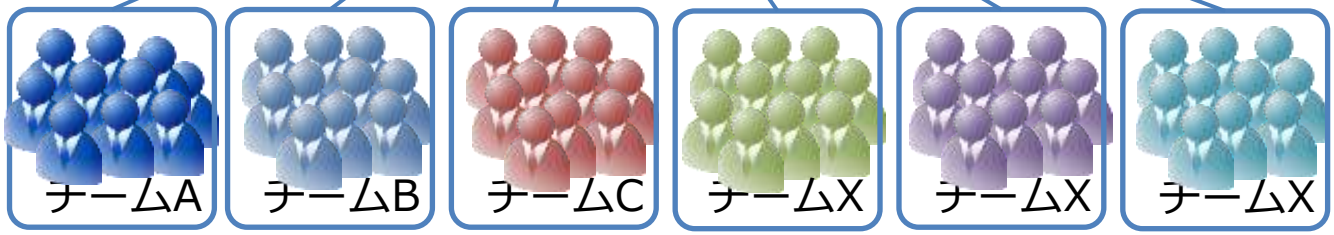


シナリオ遂行・評価
kuromame6

Eコマースサイトの”売上”と”稼働状況”をリアルタイム・スコアボードに



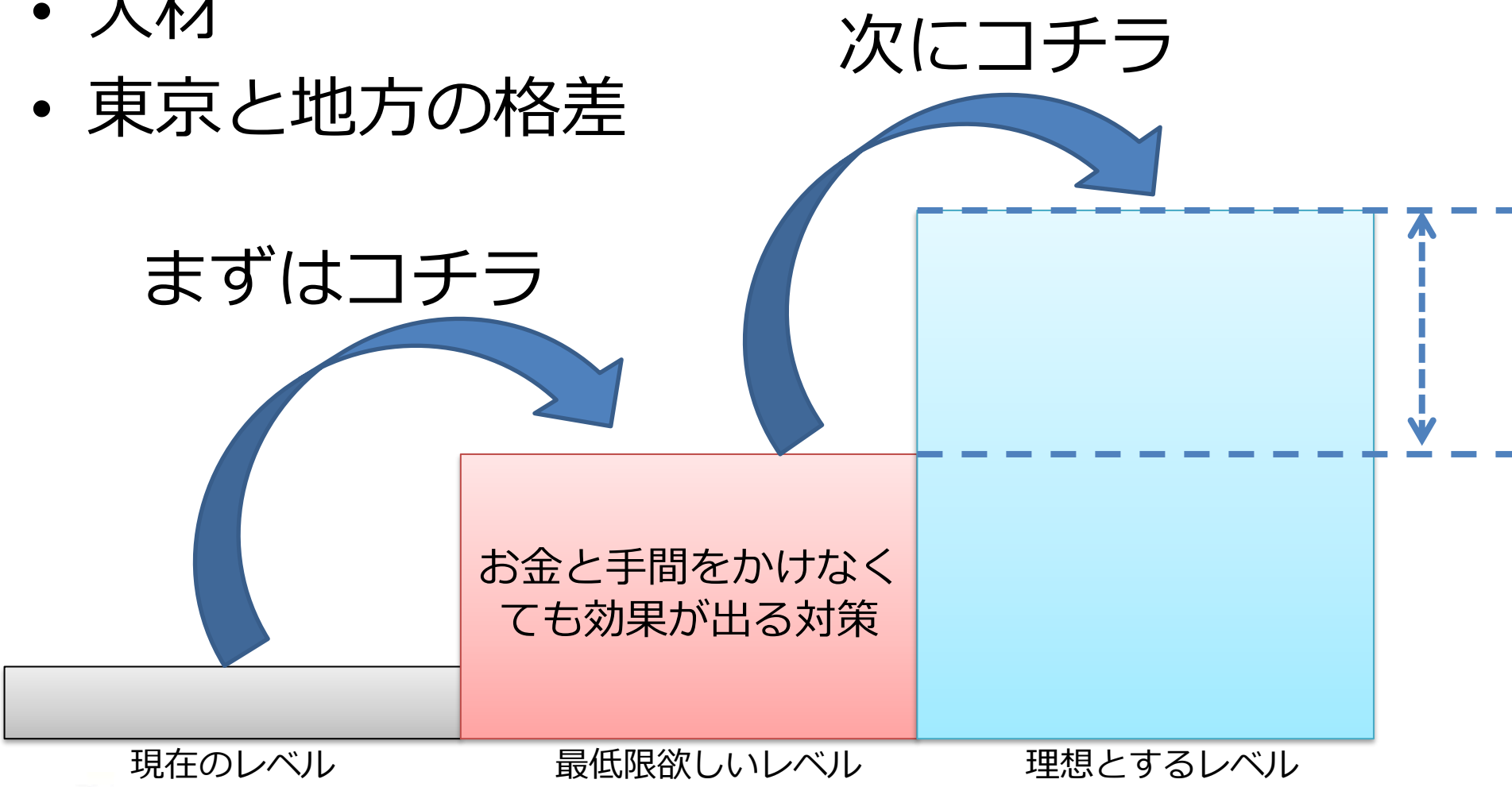
参加者（6人～10人のチームで編成）



参加者は与えられたショッピングサイトの売上を最大化するべく、チームワークを生かして行動する。
「攻撃検知」「被害の極小化」「攻撃対処」「システム復旧」「社内調整」「顧客対応」「商品調達」など様々な技能を競う。

対策の前に立ちはだかる壁

- 予算獲得
- 人材
- 東京と地方の格差



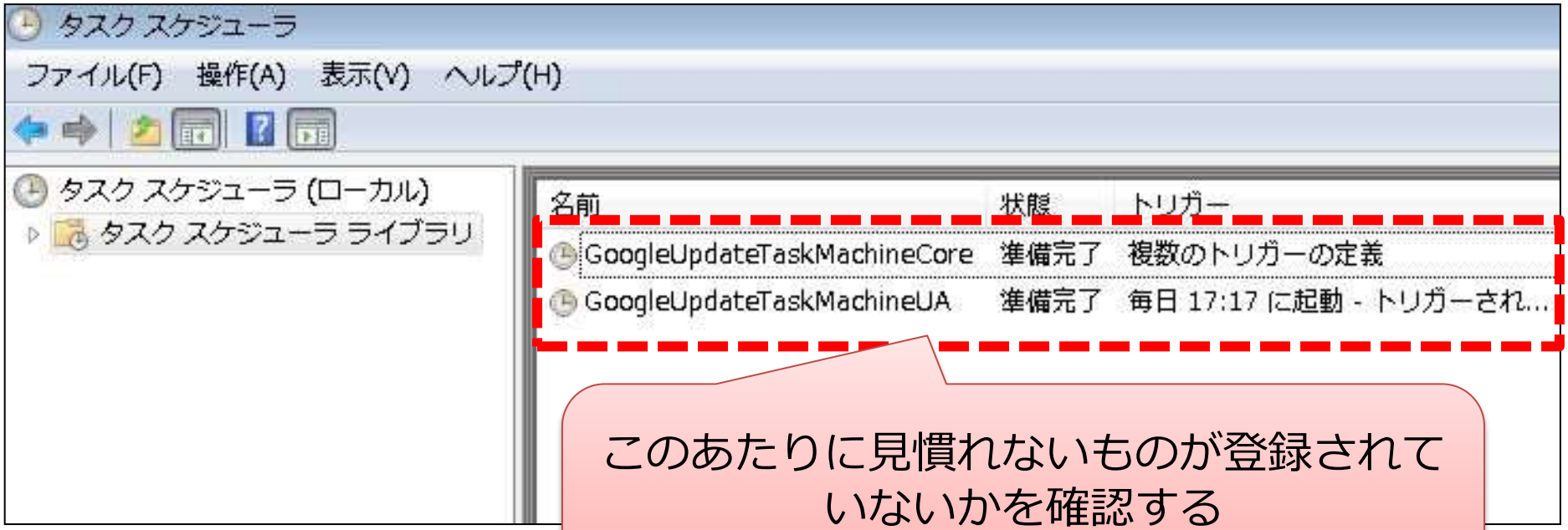
情報資産の棚卸

- パソコンの棚卸
- サーバの棚卸
- インターネット回線の棚卸
- ホームページのドメインの棚卸
- ユーザアカウント（特に管理者権限）
- 実は残っていたクレジットカード情報
  （デバッグ情報やログファイル）

すぐにやるべき対策（システム管理者向け）

対策ポイント	対策内容	チェック
システム全体	ログ保存を行う（ログイン履歴、Outboundログは必須）	
	ログ保存期間を延ばす（最低1年）	
	リモートアクセスのログイン履歴を確認する	
	時刻の同期設定を確認する	
サーバ	アプリのバージョンを確認する　（Tomcat, JBoss, Struts, Joomla!, WordPress, Movable Type, MODX など）	
	DNSのクエリログを記録する	
	cronやタスクスケジューラの中身を確認する	
	公開DNSサーバやNTPサーバがUDPアンプ攻撃に悪用されないか確認する	
クライアント	管理用端末でウェブアクセスとメール閲覧を制限する	
	Adobe Reader、Flash Player、Java、一太郎のアップデートを検討する	
	ウイルス対策ソフトの定時スキャンのログを確認する	
	UACの設定が初期値より低くなっていないか確認する	
	AutoRunの設定を確認する（特にサポート期限の切れたWindows XP）	
	ブラウザは2種類入れておく(IEの脆弱性騒ぎに対応するため)	
ネットワーク	端末間アクセスを制限する	
	FW、Proxy、URLフィルタ等のログを確認する	
	Proxy認証の認証ログを確認する	
	アクセス制御ルールに不備がないか確認する	
人・組織	CSIRTの整備、運用を行う	
	インシデント発生を想定した演習を行う	
	IPA、JPCERT、J-LIS(旧LASDEC)のコンテンツを周知する	

タスクスケジューラの中身を確認

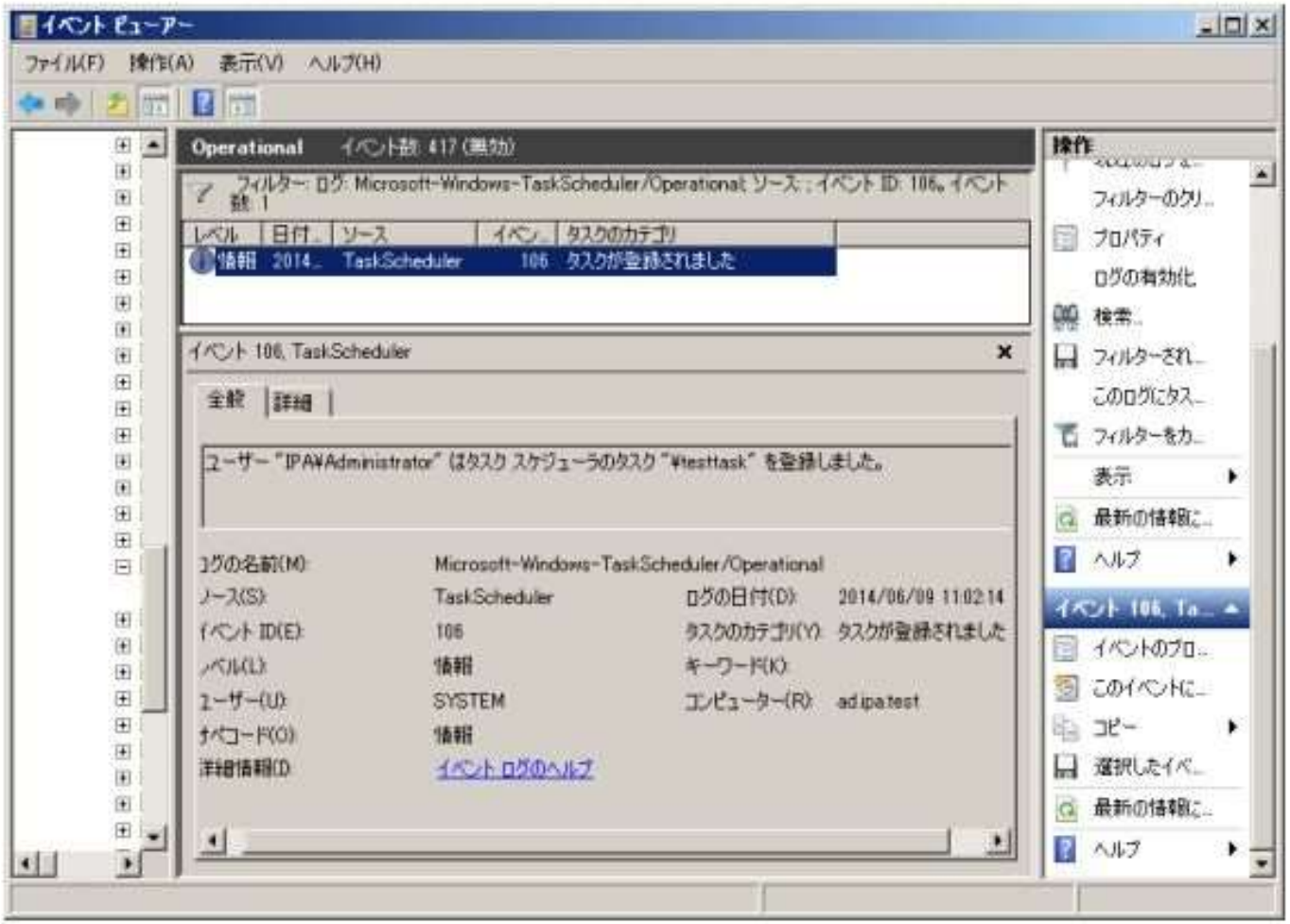


このあたりに見慣れないものが登録されていないかを確認する
（この例はGoogleのアップデートタスク）

- **攻撃者はタスクスケジューラ機能（指定時刻にプログラムを実行するWindowsの機能）を悪用して、攻撃を行う**
- **タスクスケジューラの項目で見慣れないものが存在しないかを確認する**
- **最低限、ADサーバのタスクスケジューラは確認する**

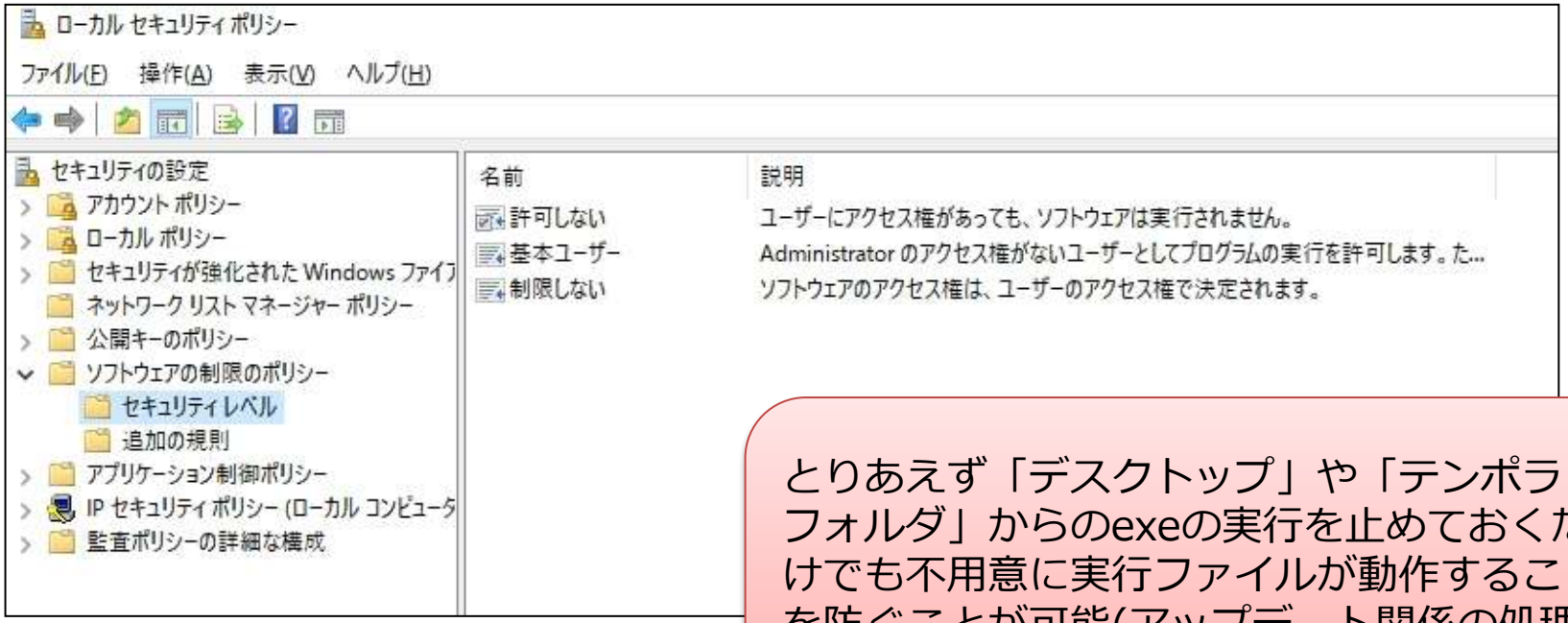
タスクスケジューラの実行ログを確認

- “現在のログをフィルター”からイベントID「106」で絞り込みを実施
- “このイベントにタスクを設定”から通知設定を実施



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

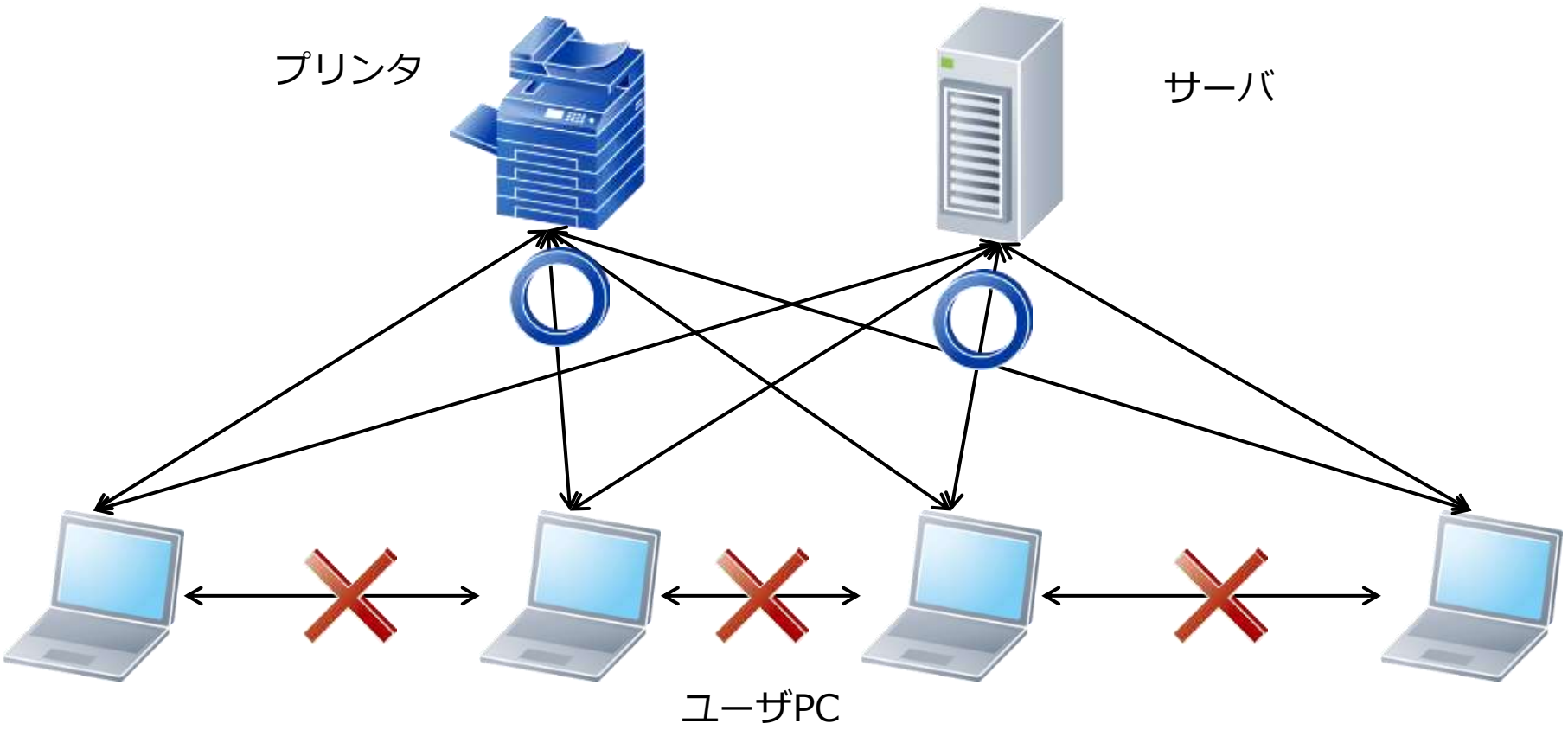
ソフトウェアの実行制御



とりあえず「デスクトップ」や「テンポラリフォルダ」からのexeの実行を止めておくだけでも不用意に実行ファイルが動作することを防ぐことが可能(アップデート関係の処理に注意)

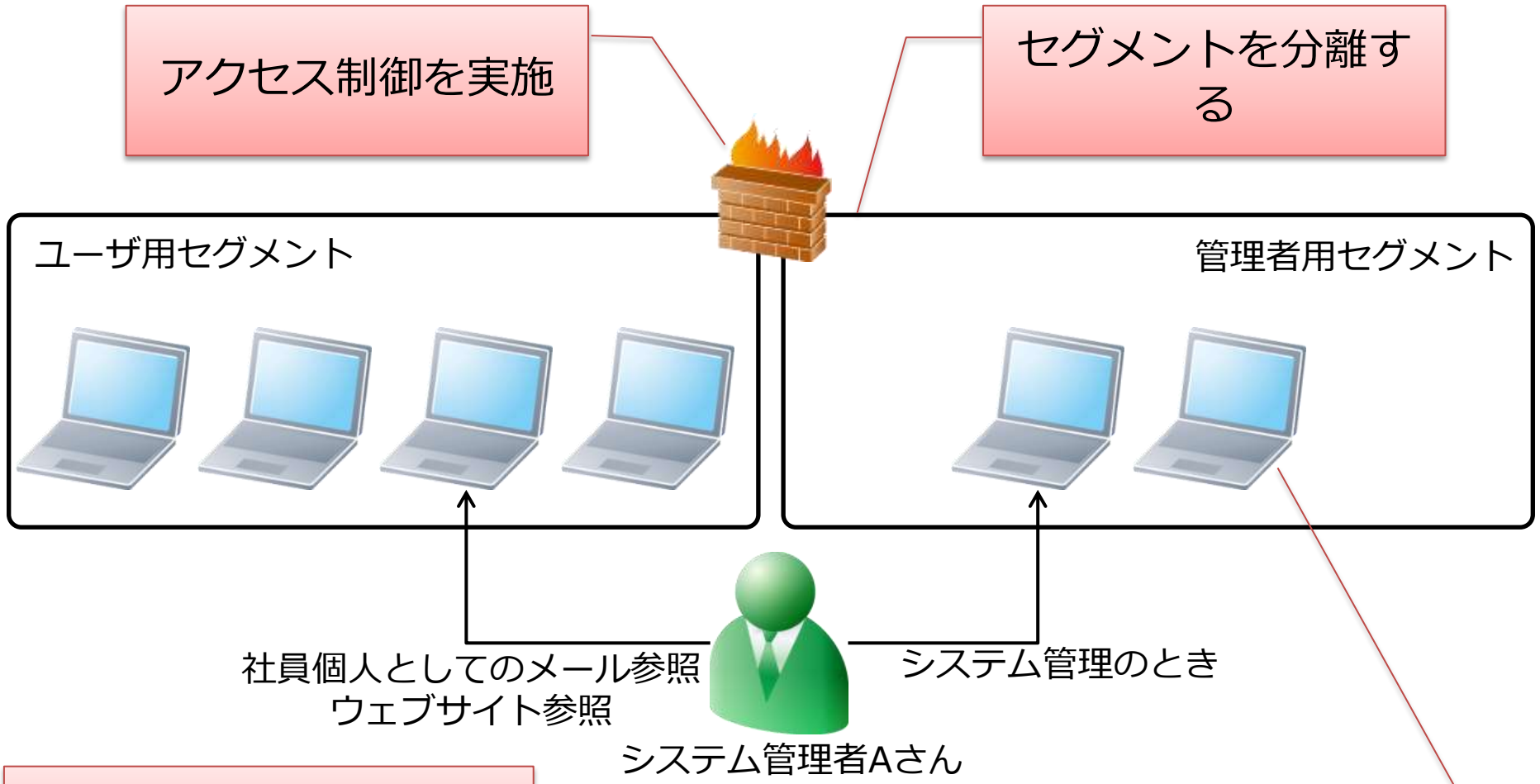
以下のディレクトリを実行許可
- C:¥Program Files
- C:¥Program Files (x86)
- C:¥ProgramData
- C:¥MSOCache
- C:¥Windows
- C:¥Users¥username¥以下の実行ツール置場

端末間アクセスの禁止



・同等構成のユーザPCの横展開を防ぐ
・ユーザPC間の通信を制限する（Windowsファイアウォール等で）
・サーバやプリンタとの間の通信のみ許可する

管理者PCの保護



家庭・個人における基本的な対策

パスワードの管理

アップデートを積極的に行う

ウイルス対策ソフトを使う

バックアップを取る

Thank you. Any Questions ?

LAC
ともに、イキル