最前線の騎士
— The Knight on the Front Line —

イード銀行

明日の全社事業発表会は

日頃の業務を全社に向かってアピールする絶好の機会だ

パサッ

イード銀行全社事業発表会
セキュリィ統括部 発表計画

その点セキュリティ統括部の発表は

スレット（脅威）ハンティングに偏りすぎではないか？

一方で脆弱性管理にまったく時間が割かれていないのが気になるが

セキュリティ統括部　部長
速水 沙也加

侵害や脅威の能動的な調査は現在最も注目度の高い分野ですので

手前味噌ではありますが

部の存在感を示す上ではこれが最善と考えます

脆弱性管理担当としてはどうだ？

初田！

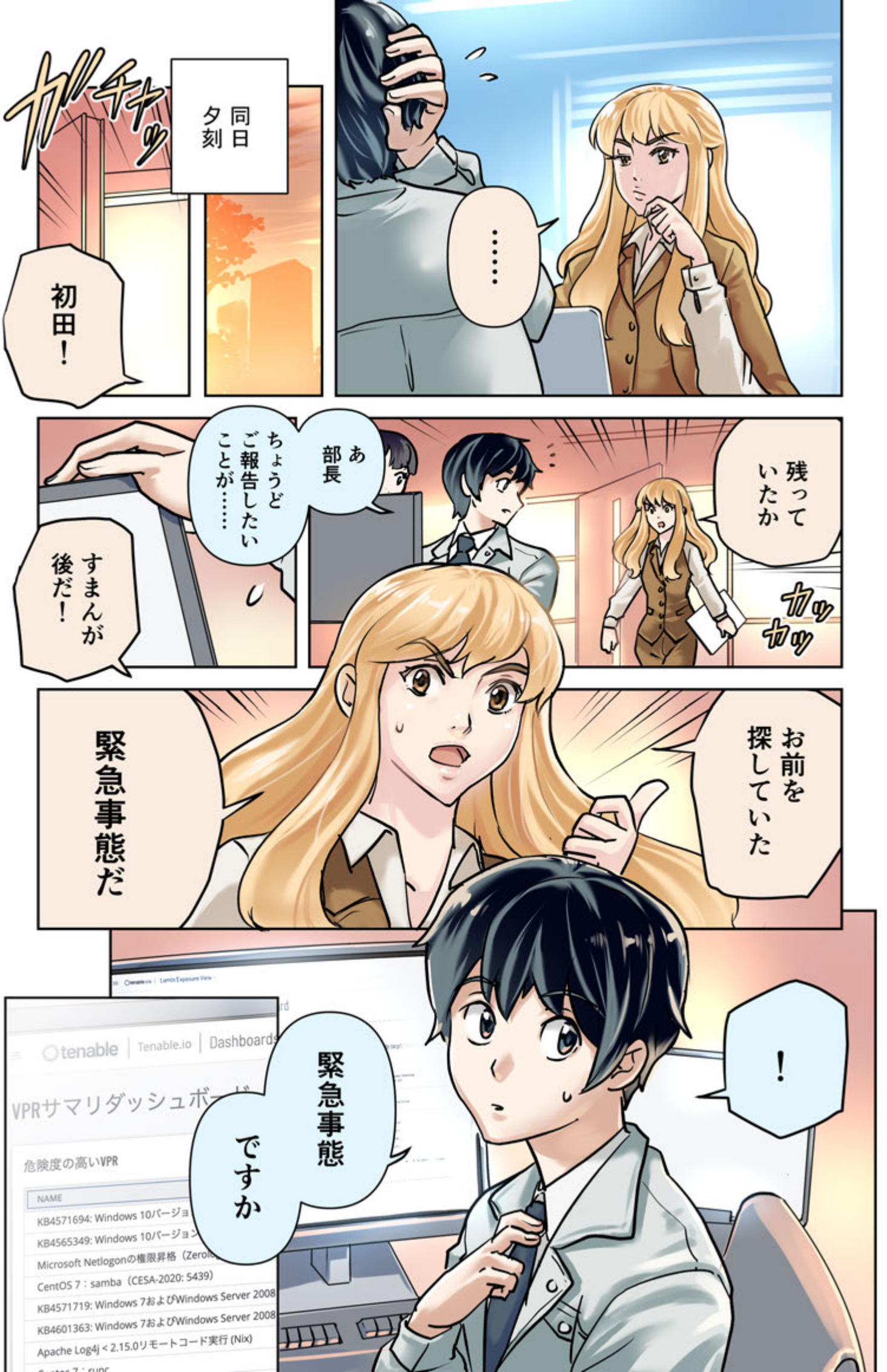
えっ

セキュリティ統括部
スレット・ハンティングチーム
山崎 真也


ボクの仕事は
公表された脆弱性に
パッチを当てる
だけですから
省いてもらって
かまわないです
セキュリティ統括部
脆弱性管理担当
初田　始
正直
発表の機会
なんか貰っても
会場全体が
寝ちゃう
というか
ビッ


脆弱性管理は
地味だからなぁ
その点
スレット
ハンティングは
華があるよ


最前線で
会社を守っている
方を主役にするのが
正解
だよなぁ


ガチャッ
同日
夕刻
初田！
……
残っていたか
カッカッ
あ
部長
ちょうどご報告したいことが……
すまんが後だ！
お前を探していた
緊急事態だ
！
緊急事態ですか
tenable
Tenable.io
Dashboards
VPRサマリダッシュボード
危険度の高いVPR
NAME
KB4571694: Windows 10バージョ
KB4565349: Windows 10バージョン
Microsoft Netlogonの権限昇格（Zerol
CentOS 7：samba（CESA-2020: 5439）
KB4571719: Windows 7およびWindows Server 2008
KB4601363: Windows 7およびWindows Server 2008
Apache Log4j < 2.15.0リモートコード実行 (Nix)

翌日
全社
事業発表会


――
このように
横展開初期の
攻撃ベクトルを
発見

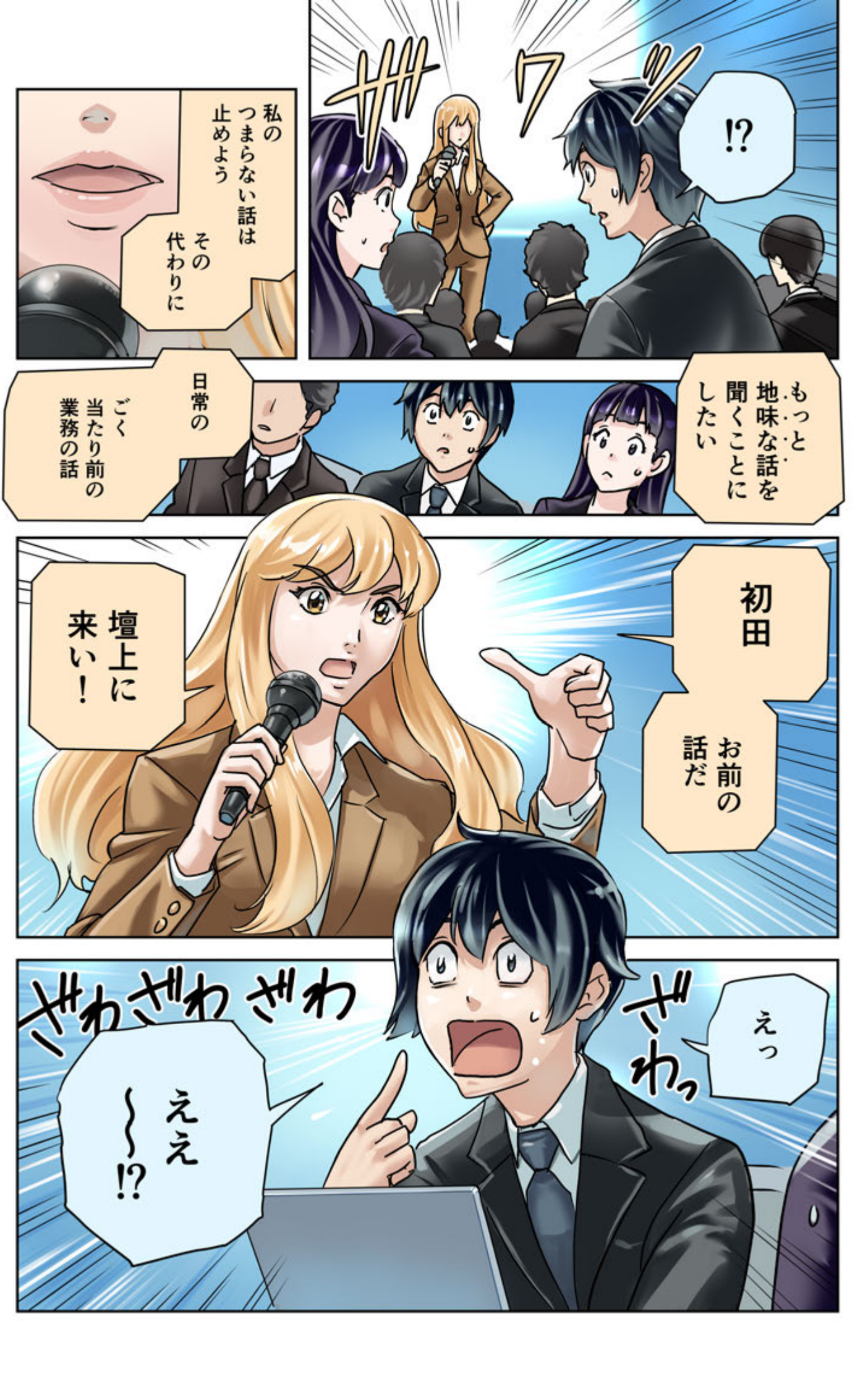

ＡＤ到達前に
封じ込めることが
できたのは
セキュリティ統括部
の大きな成果だった
と考えています


山崎さーん♥
パチパチパチパチ
パチパチ


すごい
注目度
ですね
うちの
スレット
ハンティング
チーム
というか
山崎さん
速水部長と
有名なコンビ
だからね


いくつもの
サイバー攻撃を
未然に防いでいて
当局から
名指しで賞賛
されたことも
あるんだ
人呼んで


セキュリティの
《騎士》と
その
《女王》さ
後半は
速水部長から
総括をお話し
致します
パチパチパチパチ
騎士と
女王様かあ
確かに
ふたりとも
華がありますよねぇ
イード銀行が
顧客から
預かるのは
資産だけでは
ありません
それに伴う
個人情報や
……
ホント
なら
センパイも
あそこに
立ってるはず
だったのに
似合わないよ
ボクには
地味に
業務を
こなしてる
方が
性に合って
……
やめた


!?
私の
つまらない話は
止めよう
その
代わりに
もっと
地味な話を
聞くことに
したい
日常の
ごく
当たり前の
業務の話
初田
お前の
話だ
壇上に
来い！
えっ
ざわっ
ざわざわざわ
ええ
〜〜
!?

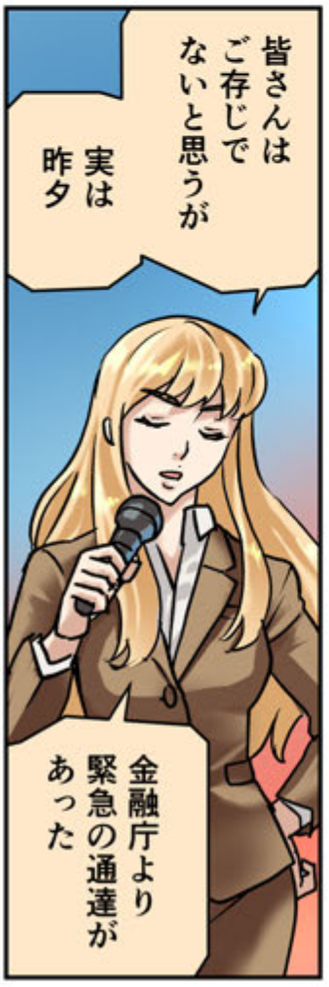

ざわ
ざわ
ざわ
ざわ
ざわ
えーと
ぜ
脆弱性
管理担当の
は
初田と
申します
ざわざわ

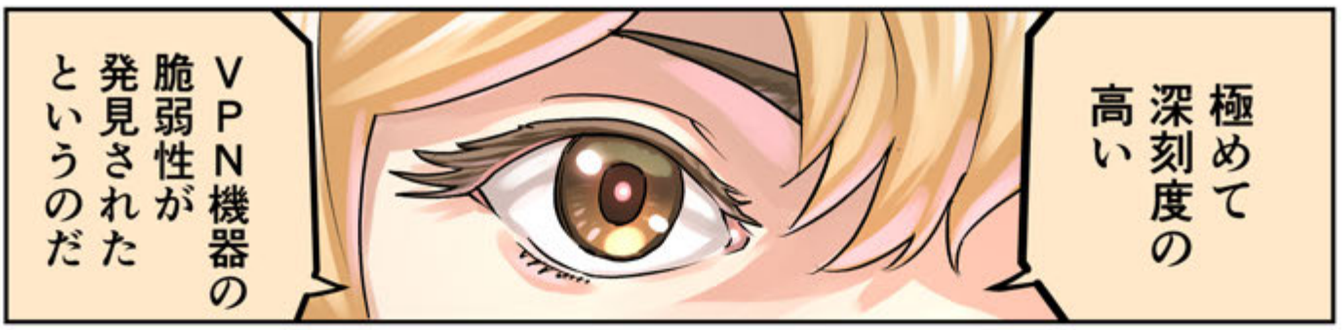

部長
話すって
なにを？
なにも
準備して
いませんよ!?

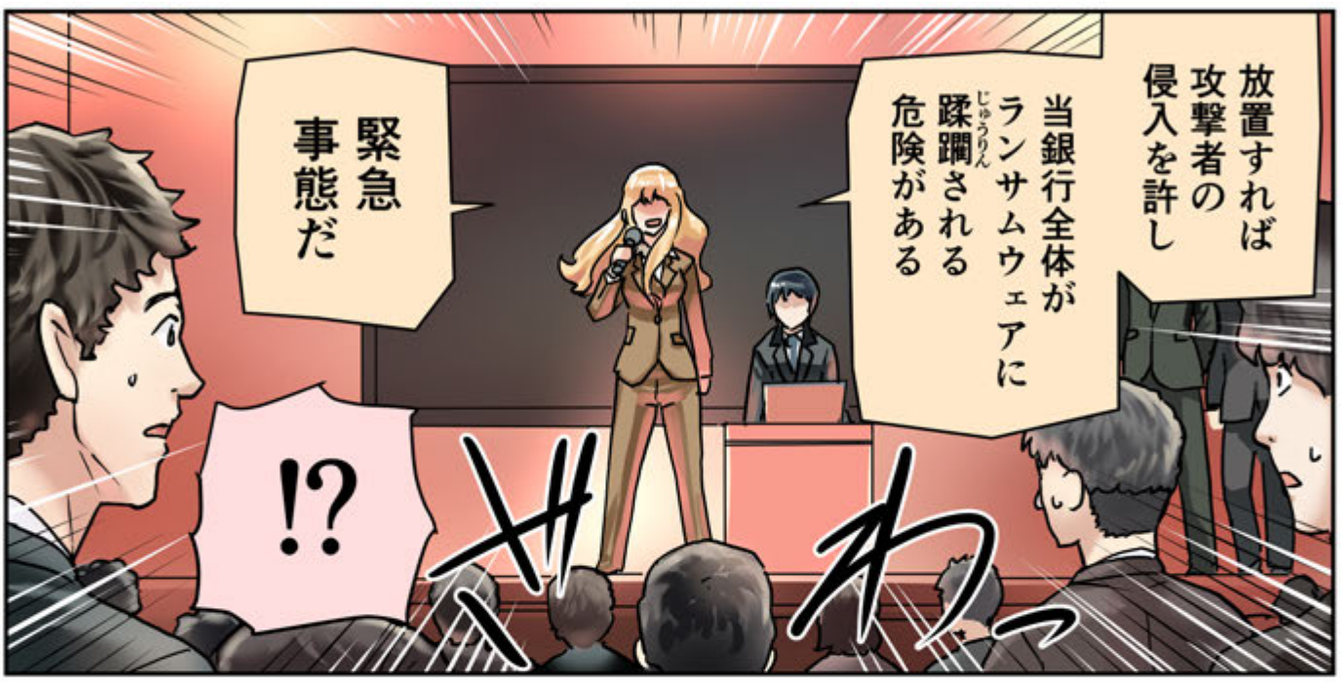

部長
酷だなぁ
地味男くんの
初田には
荷が重いよ
な？


しー


まあ
黙って
見ていま
しょうよ


皆さんは
ご存じで
ないと思うが
実は
昨夕
金融庁より
緊急の通達が
あった

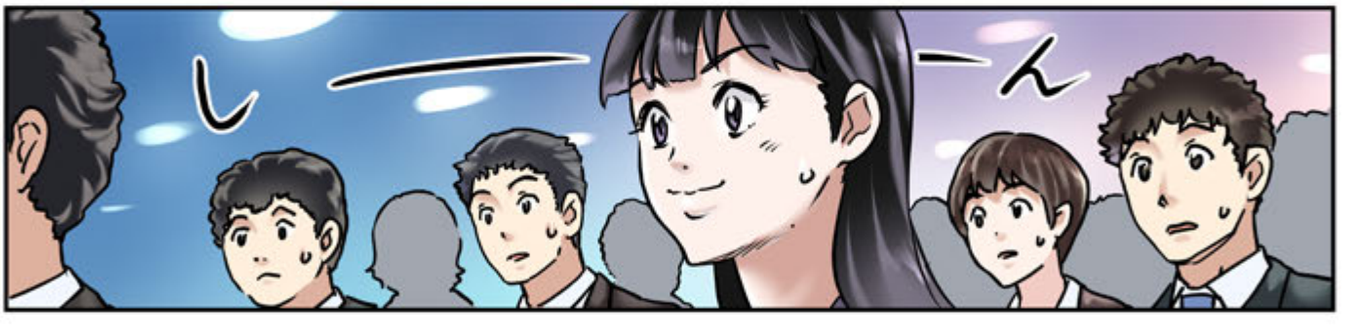

極めて
深刻度の
高い
VPN機器の
脆弱性が
発見された
というのだ


放置すれば
攻撃者の
侵入を許し
当銀行全体が
ランサムウェアに
蹂躙(じゅうりん)される
危険がある
緊急
事態だ
!?
ザワッ


各支店で
稼働している
機器を洗い出し
更新を
適用する
必要がある
膨大な
作業量と
なるはずだ
ザワ ザワ
ザワ
ザワ


急いで
帰宅直前の
彼を捕まえ
緊急対応を
協議した
コトは
一刻を争う
からな
ところがだ
その
VPN
機器ですが


すでに
全支店分の
洗い出しは
完了し
現在
最新パッチの
動作確認中です
緊急対応のため
ご報告が遅れて
失礼しました
確認取れ次第
本番適用の
許可を……


しーん


自分と
いうより
新規導入した
システムの
力でして
カタカタ
ほう？


初田には
いつも
驚かされるが
今回は
格別だったよ
そんな
特別な
ことでは

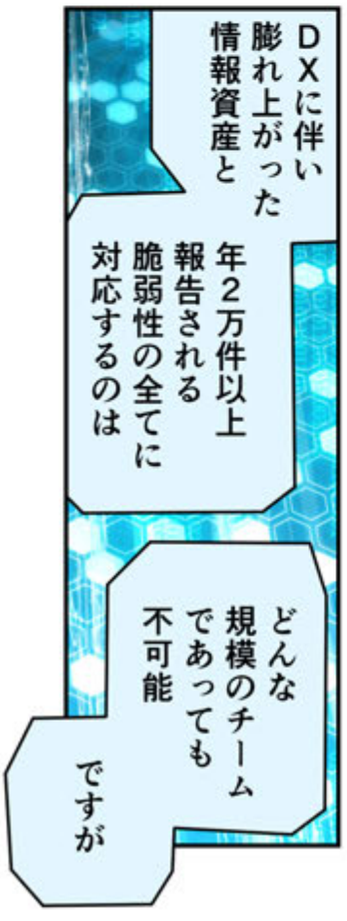

通達に先立っ
電光石火の
対応

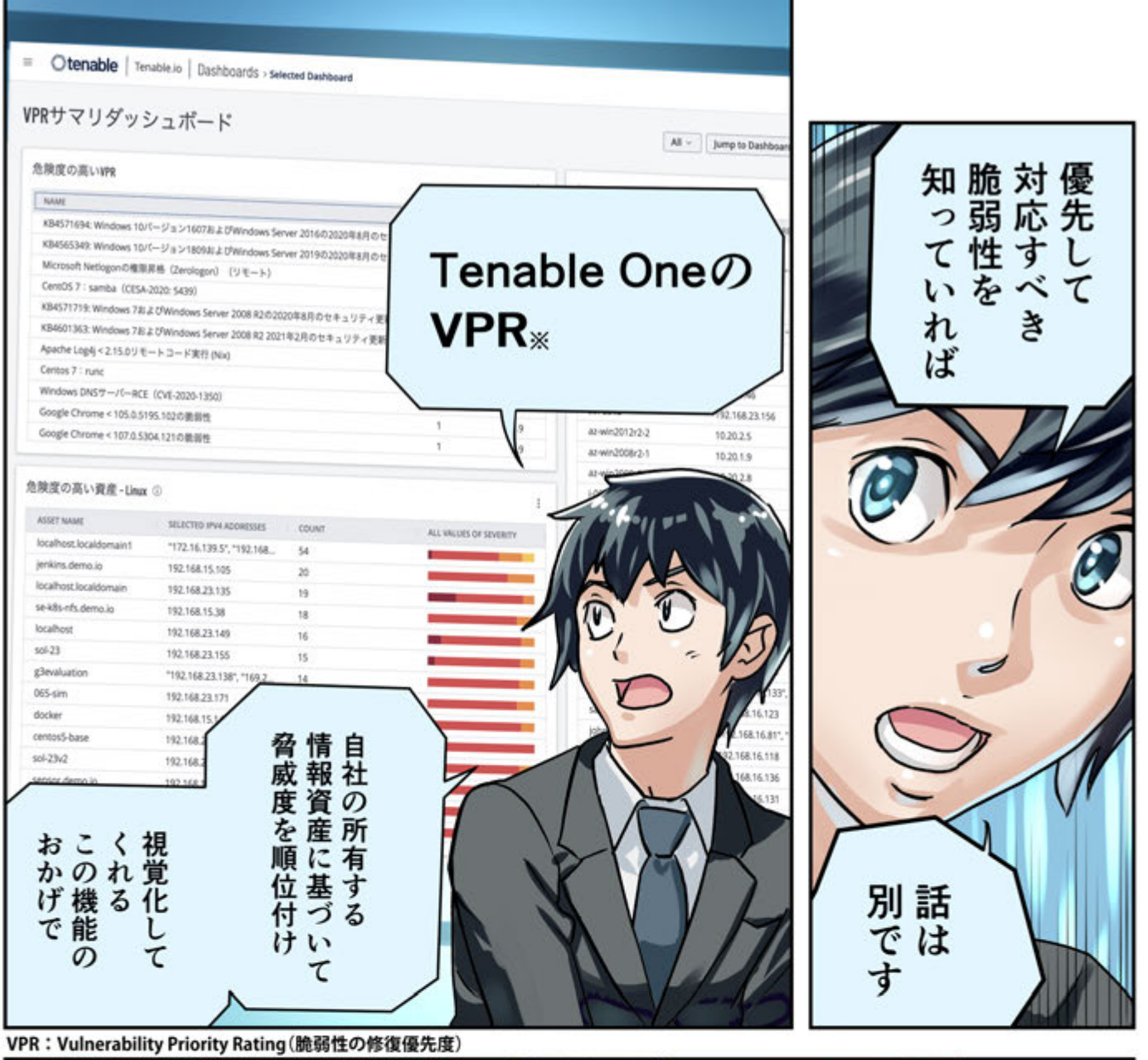
tenable


Global Exposure Card
Overall score
C
サイバーエクスポージャー管理プラットフォーム
Tenable One です

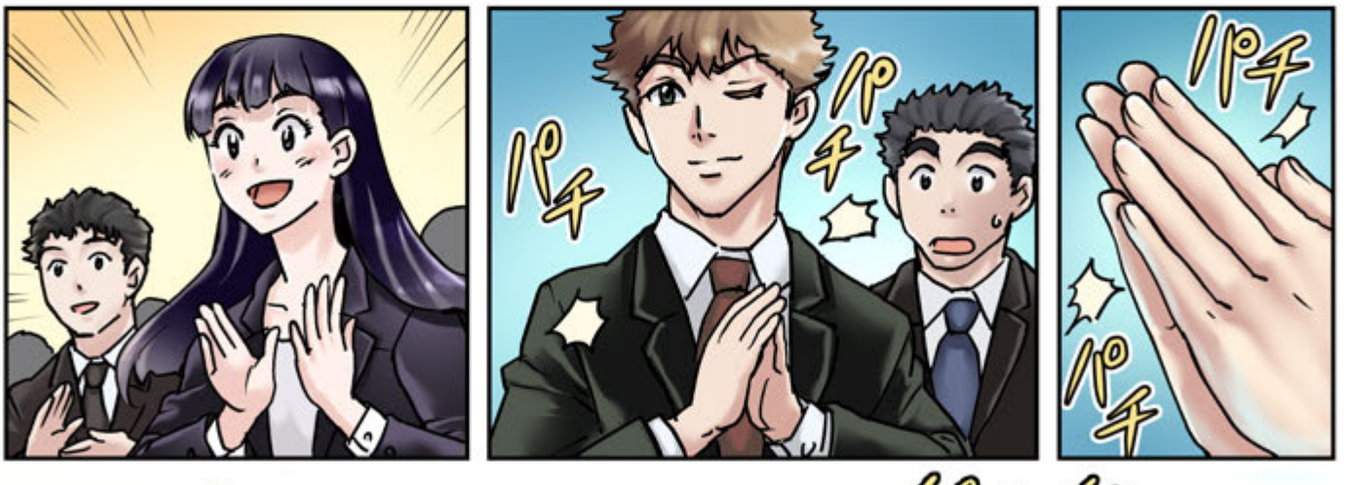

サイバー
エクスポージャー管理……？


tenable one
サイバーエクスポージャー管理プラットフォーム
EXPOSURE VIEW
サイバーリスクの集計表示と分析
ATTACK PATH ANALYSIS
侵入と攻撃の抑止対策
ASSET INVENTORY
全資産を統合した表示
エクスポージャー分析
データ集約、リスクの優先順位付けと推奨、ベンチマーキング
脆弱性管理
Web App セキュリティ
クラウド セキュリティ
認証 セキュリティ
アタック サーフェス管理
従来の脆弱性管理から広げて
クラウドからウェブアプリまであらゆる情報資産を包含する
新しいリスク管理戦略の考え方です


DXに伴い膨れ上がった情報資産と
年2万件以上報告される脆弱性の全てに対応するのは
どんな規模のチームであっても不可能
ですが



VPR：Vulnerability Priority Rating（脆弱性の修復優先度）



tenable®

パチパチパチ。。

THE END

漫画・原作：瀬尾浩史／製作：株式会社イード ScanNetSecurity 高橋潤哉