SuIREN

自社開発・運用
高セキュリティかつ柔軟なネットワークシステム
「SuIREN」

NIKKO 日興通信株式会社

世の中のサイバー攻撃や悪戯の状況

情報とは

コンピュータ関連分野における辞書での定義は

- 電気電子用語辞典
  ⇒ ある既知の法則によってデータに付与された意味あるいは内容のこと、データとは情報の 内容を示すための記号、文字、シンボル、符号など
- IEEE電気電子用語辞典
  ⇒ 既知の約束に基づいて、データに割り当てられた意味
- 日本工業規格
  ⇒ データに適用される約束に基づいて、そのデータに対して一般に通用している意味

  ⇒ 事実、事象、事物、過程、着想などの対象物に関して知り得たことであって概念を含み、一定の文脈の中で特定の意味をもつもの

“データ” に “意味を付与する” と “情報” となる

（例）データの集まり ： S M T W T F S

情報セキュリティ対策の基本

何を	○○で扱う重要な情報資産
何から	外部・内部の脅威
どのように	技術・ルール・扱う人の意識を総合して守る

文部科学省 「教育情報セキュリティポリシーに関するガイドライン」ハンドブック より

情報セキュリティ10大脅威 2024

順位	「組織」の脅威	前年比
1位	ランサムウェアによる被害	→
2位	サプライチェーンの弱点を悪用した攻撃	→
3位	内部不正による情報漏洩等の被害	↑
4位	標的型攻撃による機密情報の窃取	↓
5位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	↑
6位	不注意による情報漏洩等の被害	↑
7位	脆弱性対策情報の公開に伴う悪用増加	↑
8位	ビジネスメール詐欺による金銭被害	↓
9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	↓
10位	犯罪のビジネス化（アンダーグラウンドサービス）	→

IPA「情報セキュリティ10大脅威 2024」より

ランサムウェア
標的型攻撃
常に上位

テレワーク関連
内部不正・不注意
による情報漏洩
常に10位以内

「情報セキュリティ10大脅威」の振り返り

2005

「脆弱性を狙う攻撃」
- クライアントOSに潜むゼロデイ脆弱性を狙う攻撃
- WebサイトやWebアプリケーションに存在する脆弱性を狙うSQLインジェクション攻撃

「ファイル共有ソフトによる情報漏洩」

2010

「スマホを狙う不正アプリ」
- スマホ乗っ取りアプリ
- 個人情報の流出

「トロイの木馬」
- インターネットバンキングの中間者攻撃などの手法を用いて不正送金

2015

「ランサムウェア」
- 14年12月から広がる
- 仮想通貨、交換所が設置されるなど利用環境の整備でビットコインをはじめとする仮想通貨で金銭を要求する攻撃が生まれた

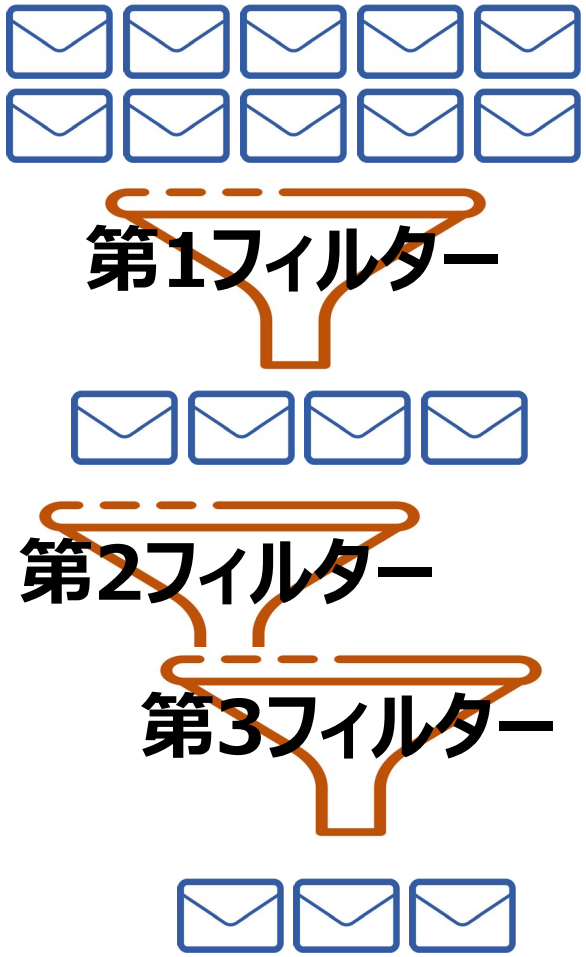
ITmedia「14年分の「情報セキュリティ10大脅威」を振り返り “変わらない”5つの対策」

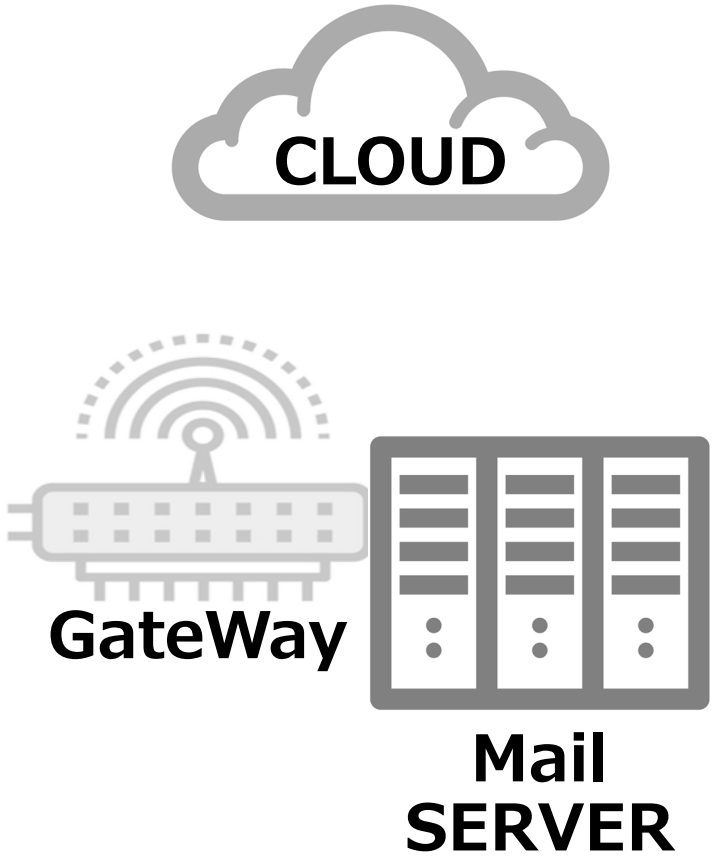
基本的な対策

- ソフトウェアの更新
- セキュリティソフトウェアの利用
- パスワードの管理・認証の強化
- 設定の見直し
- 脅威・手口を知る

当社の場合
正常なメールはどれくらい？

3つのフィルター





100

▲64.28%

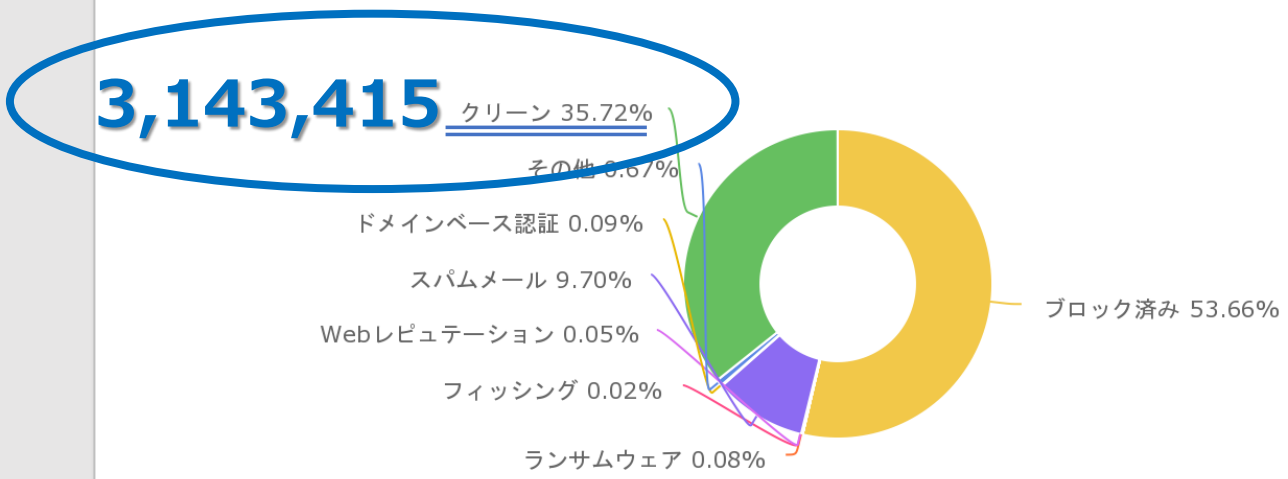
▲3.37%

32.35

Step1　総合的なマルウェア対策

当社に届く前にクラウドサービスで有害メールを削除

年間 総受信メール数　：　8,799,414通
削除されたメール数　：　5,655,999通
日興通信に届いたメール：　3,146,415通

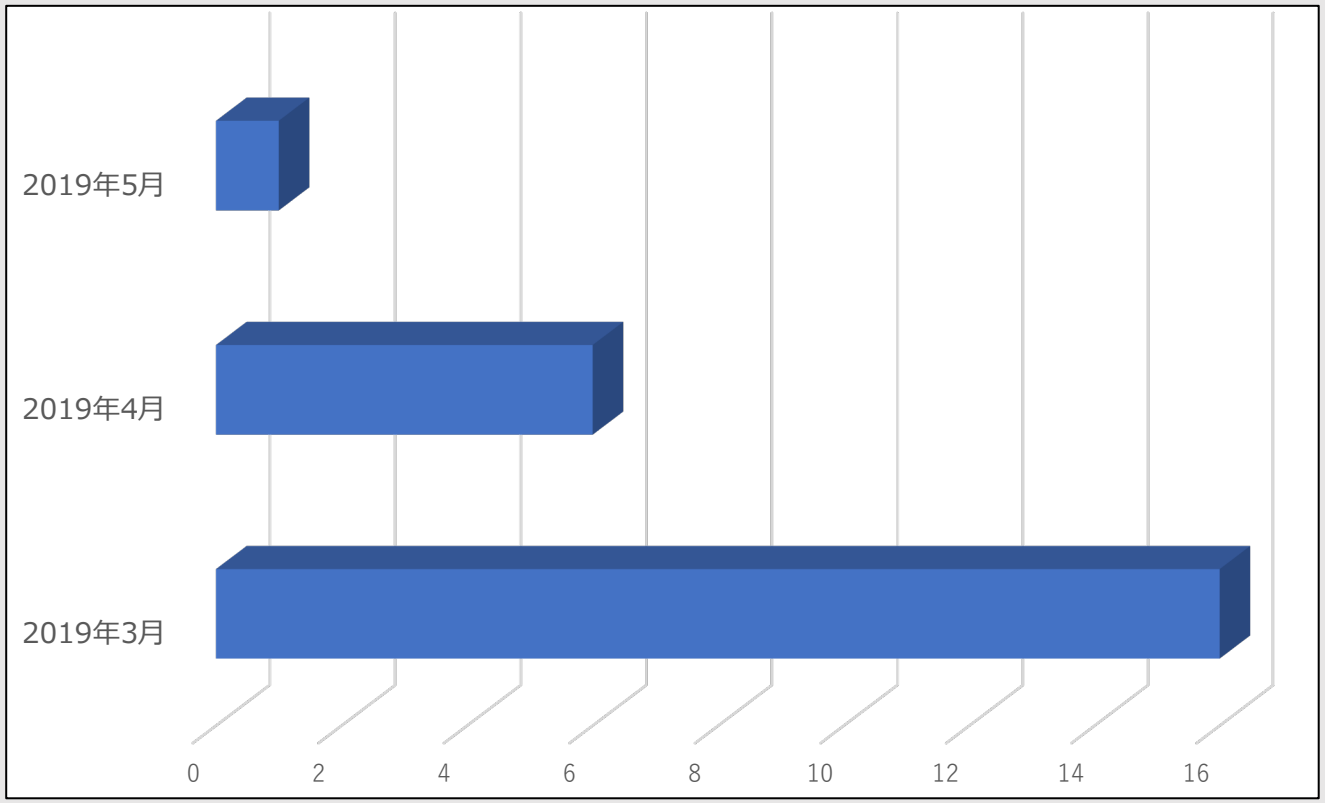


削除されたメール
64.28%

※マルウェアとは
不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称。
ウイルス、ワーム、トロイの木馬、スパイウェア、バックドア、ボットなどがそれにあたる。

Step2　ゲートウェイ機器での
マルウェア対策

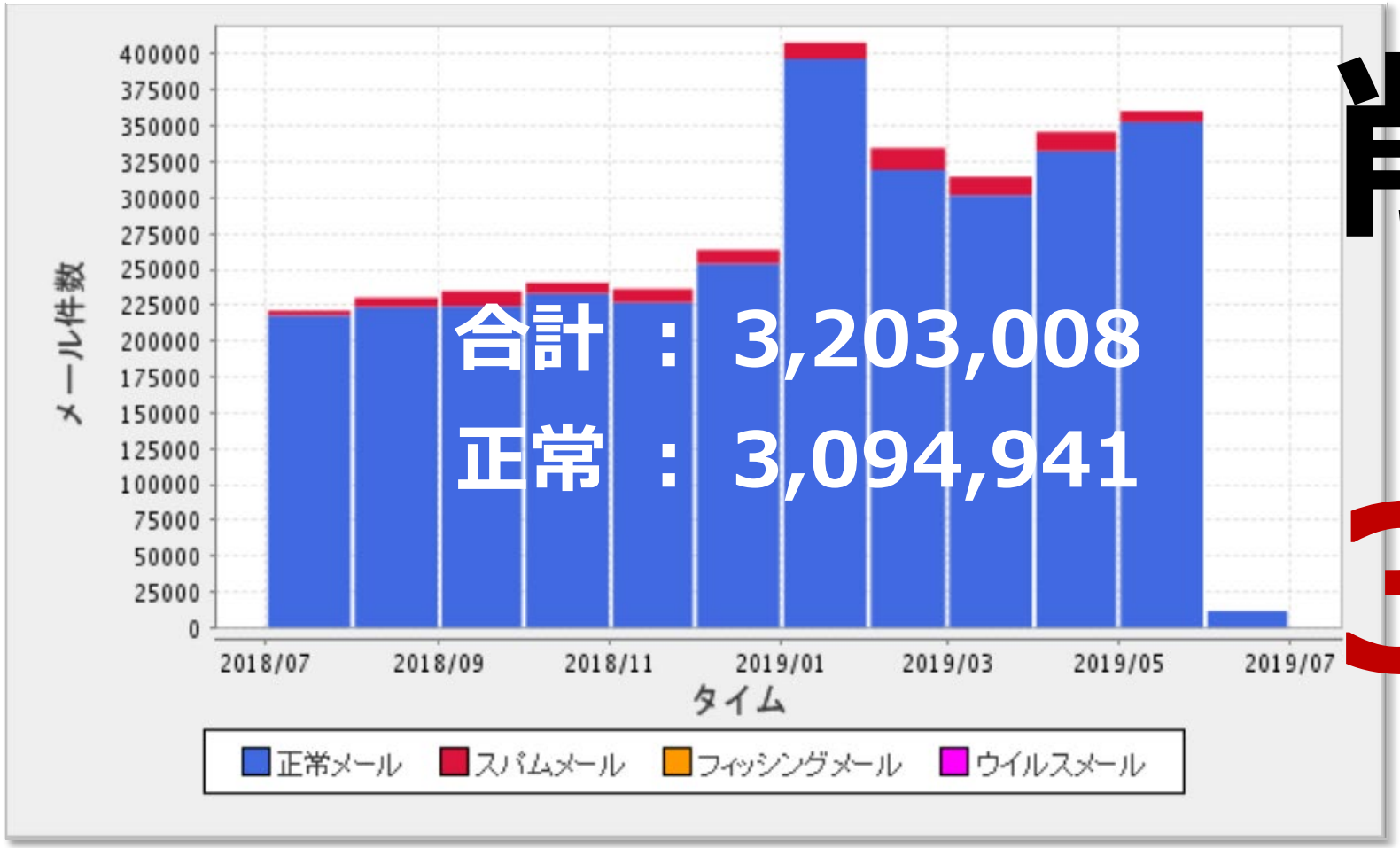
入口対策強化でゲートウェイでの対策を追加
既知の脅威対策（既に対策方法が分かっている）の2重化
Step1で殆ど有害メールは削除されている



3~5月で
23件

Step3　内部でのスパム対策

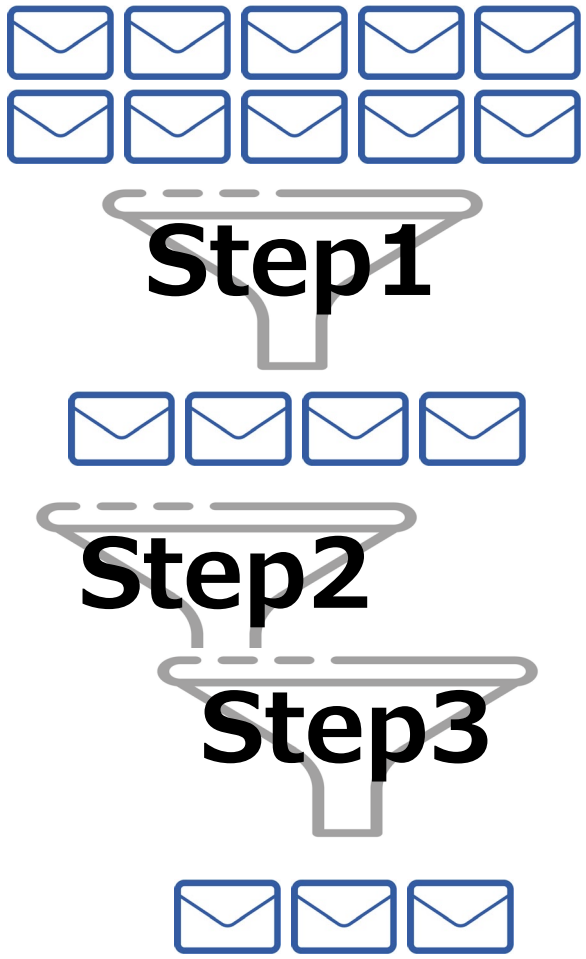
メールサーバの入口対策にスパムメール対策を追加
Step1、2を通過したメールからさらに3%強を削除



削除されたメール

3.37%

社内に届いたメール比率



Step1＋2＋3で

67.65%のメールを削除

正常と思われるメールは

わずか32.35%

そもそもセキュリティとは？

1. 一般には
   - 保安
2. 現実世界、物理的な領域では
   - 警備
   - ホームセキュリティ
   - 安全保障
3. コンピュータや仮想空間　ITのセキュリティ
   - コンピュータセキュリティ
   - 情報セキュリティ
   - ネットワーク・セキュリティ
4. 金融では
   - 証券

Wikipediaより

コンピュータや仮想空間 ITのセキュリティ

コンピュータセキュリティ

- コンピュータシステムを災害、誤用および不正アクセスなどから守ること。
- ハードウェア、ソフトウェア、データ、ネットワークのいずれに

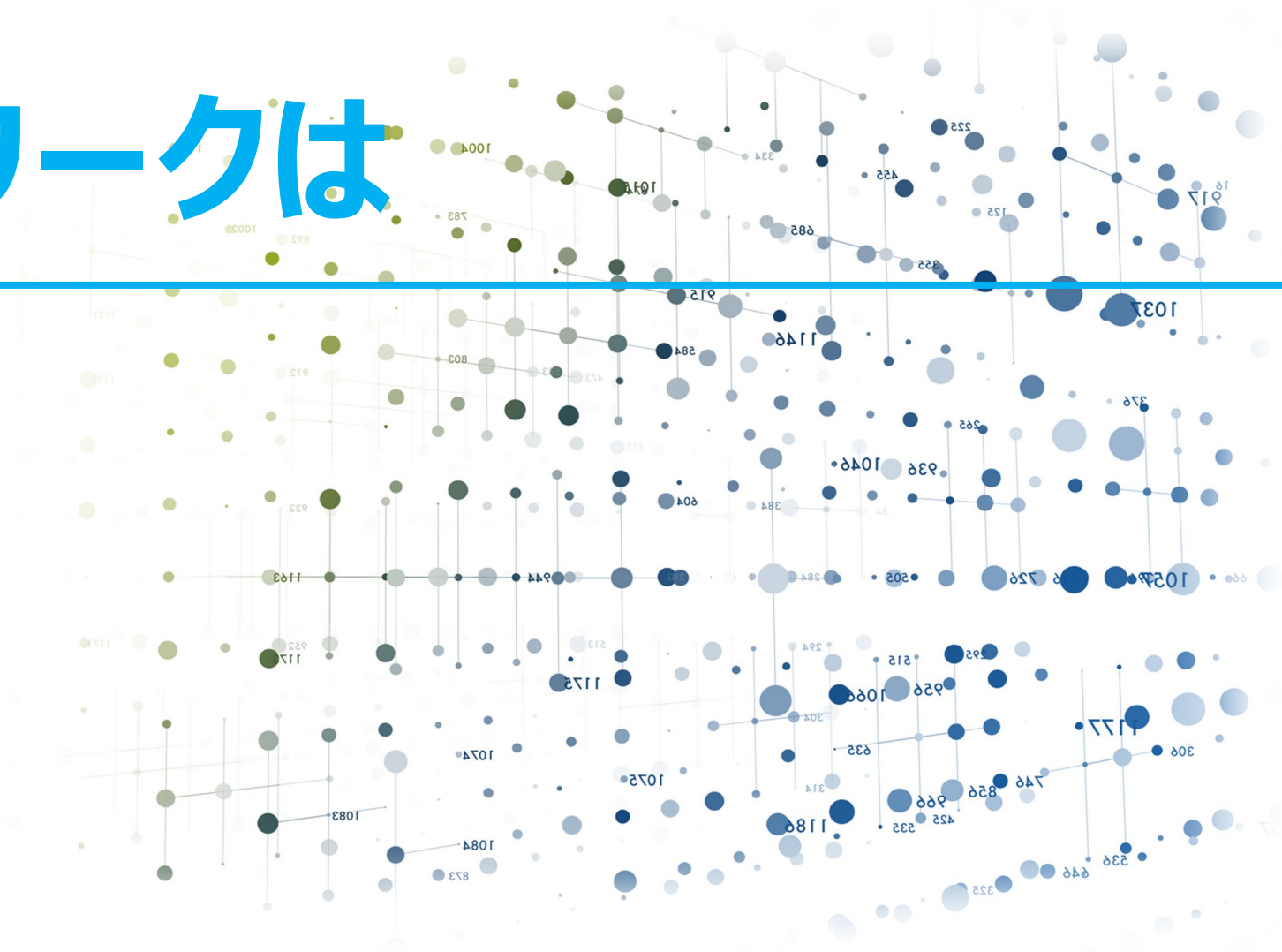
情報セキュリティ

- 情報の機密性、完全性、可用性を維持すること。

ネットワークセキュリティ

- 基礎を成すコンピュータネットワークのインフラの規定、無資格者のアクセスからネットワークとネットワークからアクセスできる資源を守るためにネットワーク管理者によって導入される方針、および一貫した継続的な監視とその効果（場合によっては欠陥）の評価までの作業から成り立つ。

当社のネットワークは



旧ネットワークの課題

老朽化…更新より年月が経過

- ✓ セキュリティ対策
- ✓ 停止・遅延のリスク
- ✓ 運用負荷・対応遅延

そこで・・・

新ネットワーク構築！

“ネットワークの日興通信”に恥じない

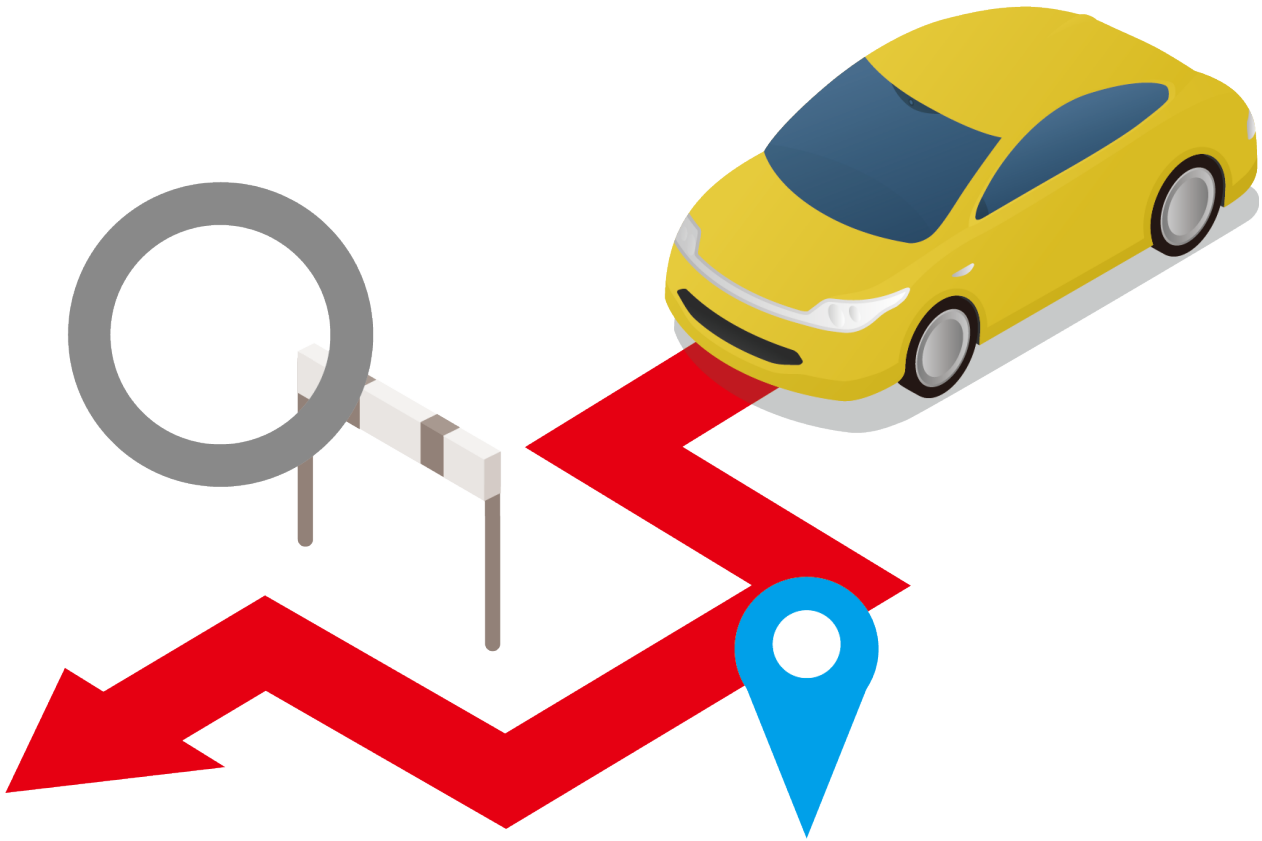
最先端かつ先進的なネットワークを再構築

SuIREN

SecUre & Innovative Redundant Network

～安全で革新的な冗長化ネットワーク～

Point 1　止まらないネットワーク



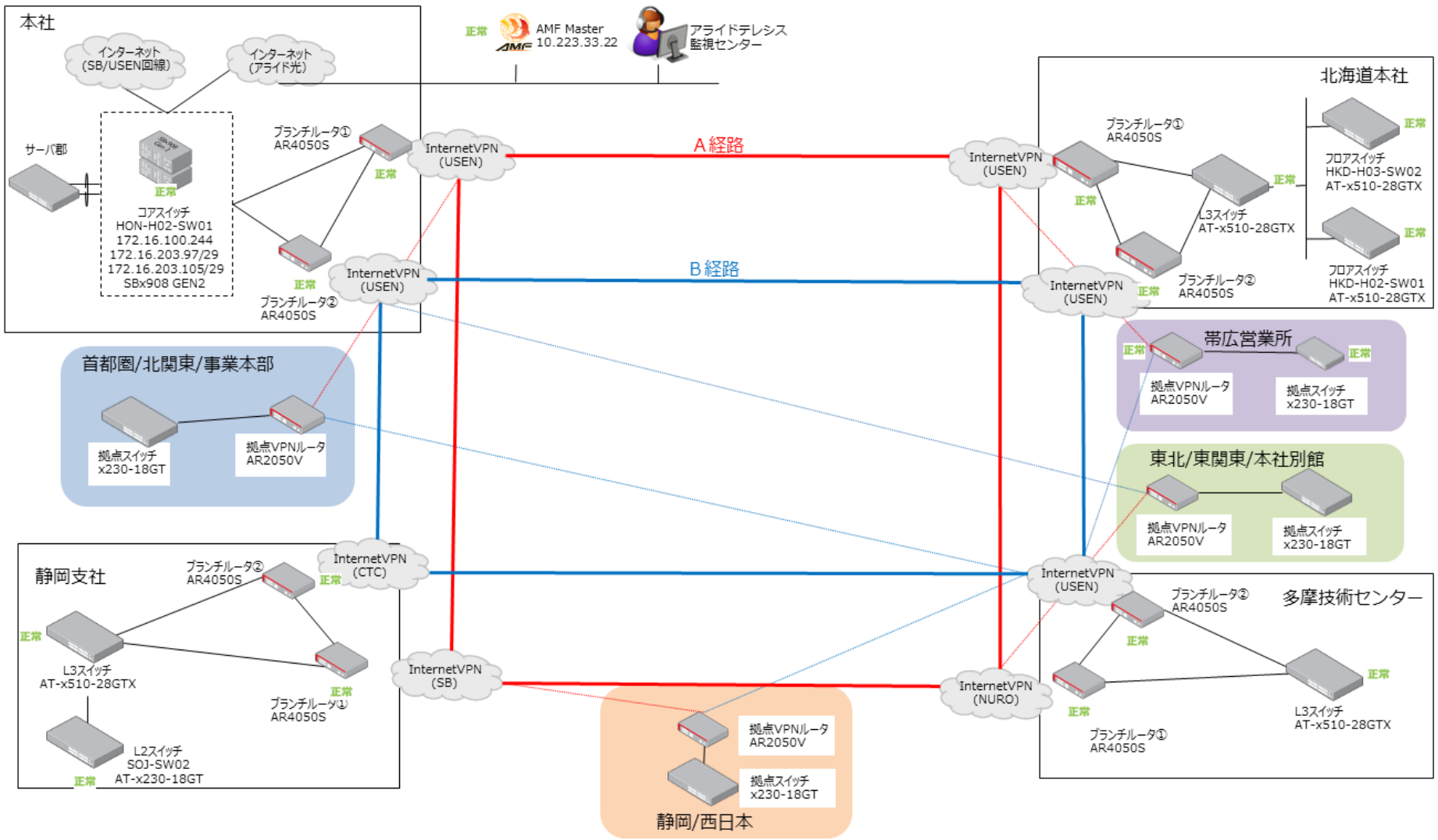
４ブランチ制で

もし障害が発生しても…

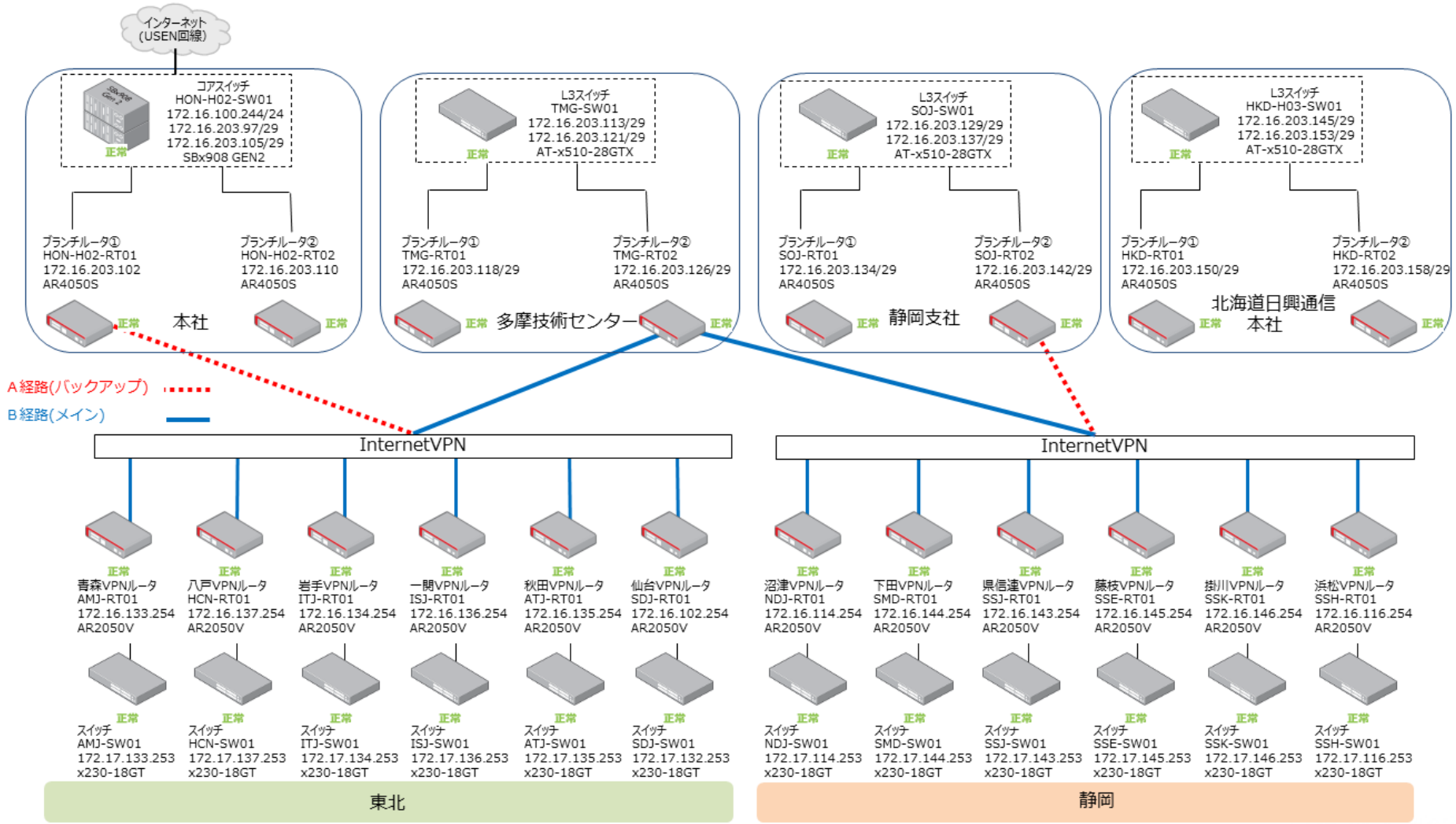
他のブランチを経由、

業務は止まらない

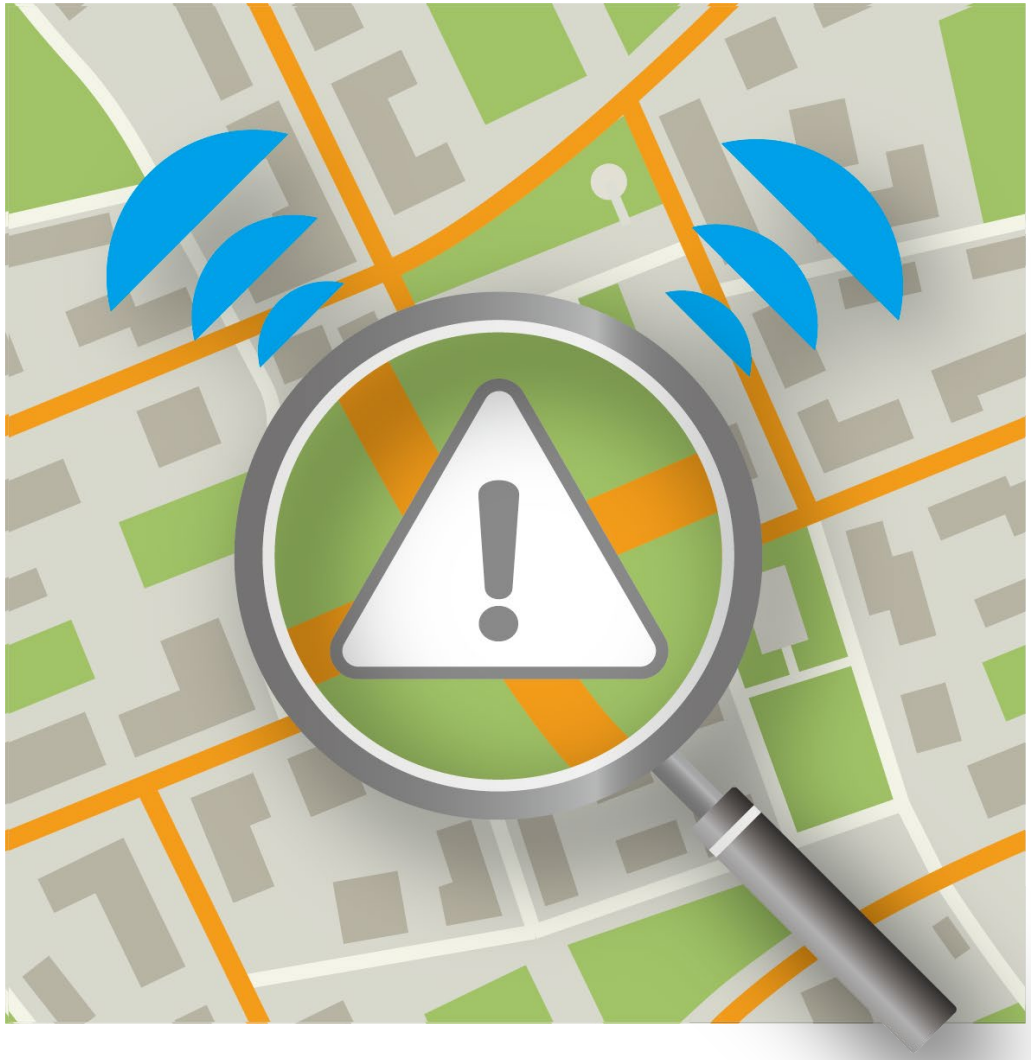
NTCS-00-全体概略図



NTCS-02-ブランチA

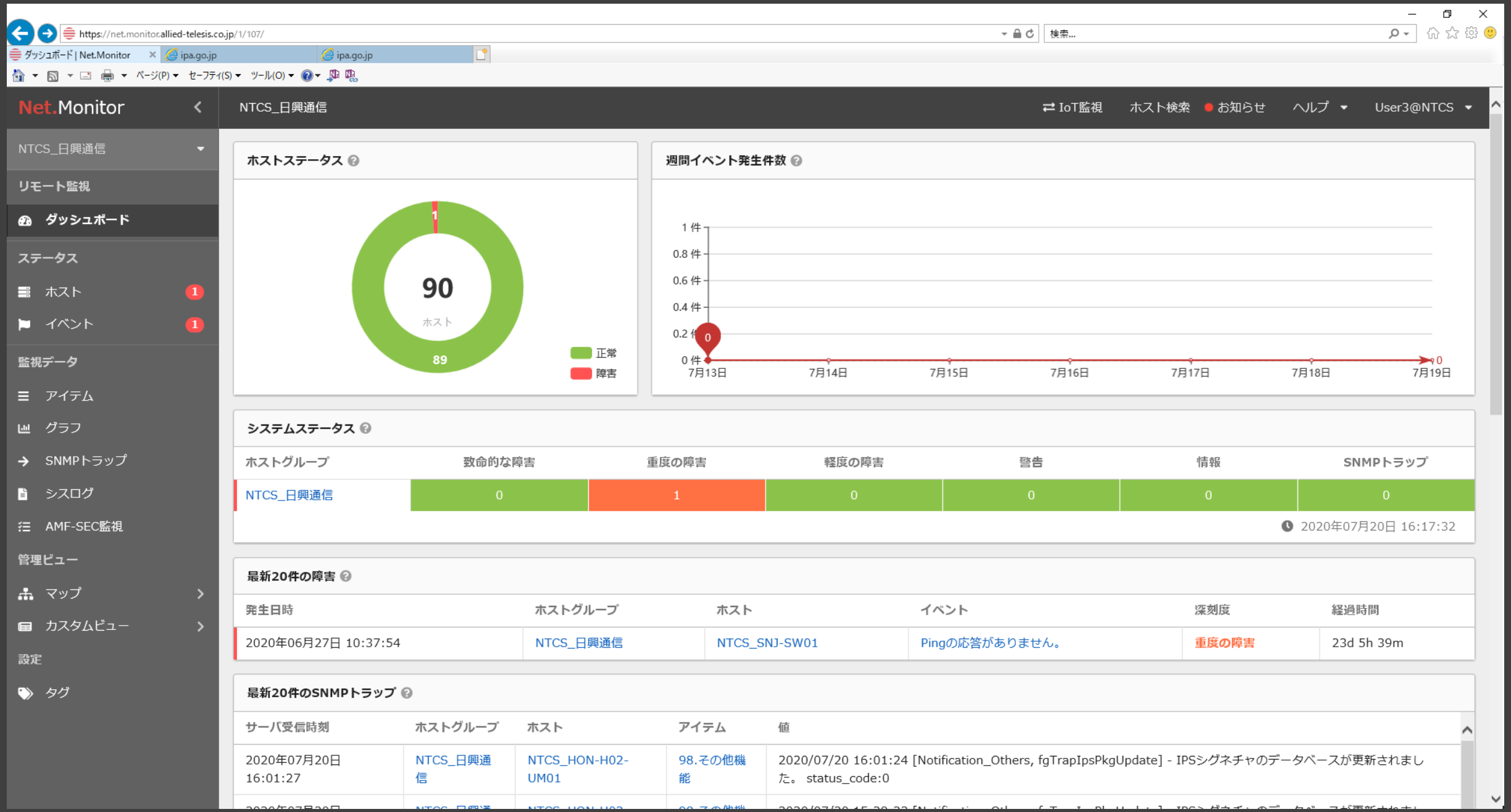


Point 2　ネットワークの見える化



SDN＋監視で全体を
見える化異常に早く気づいて

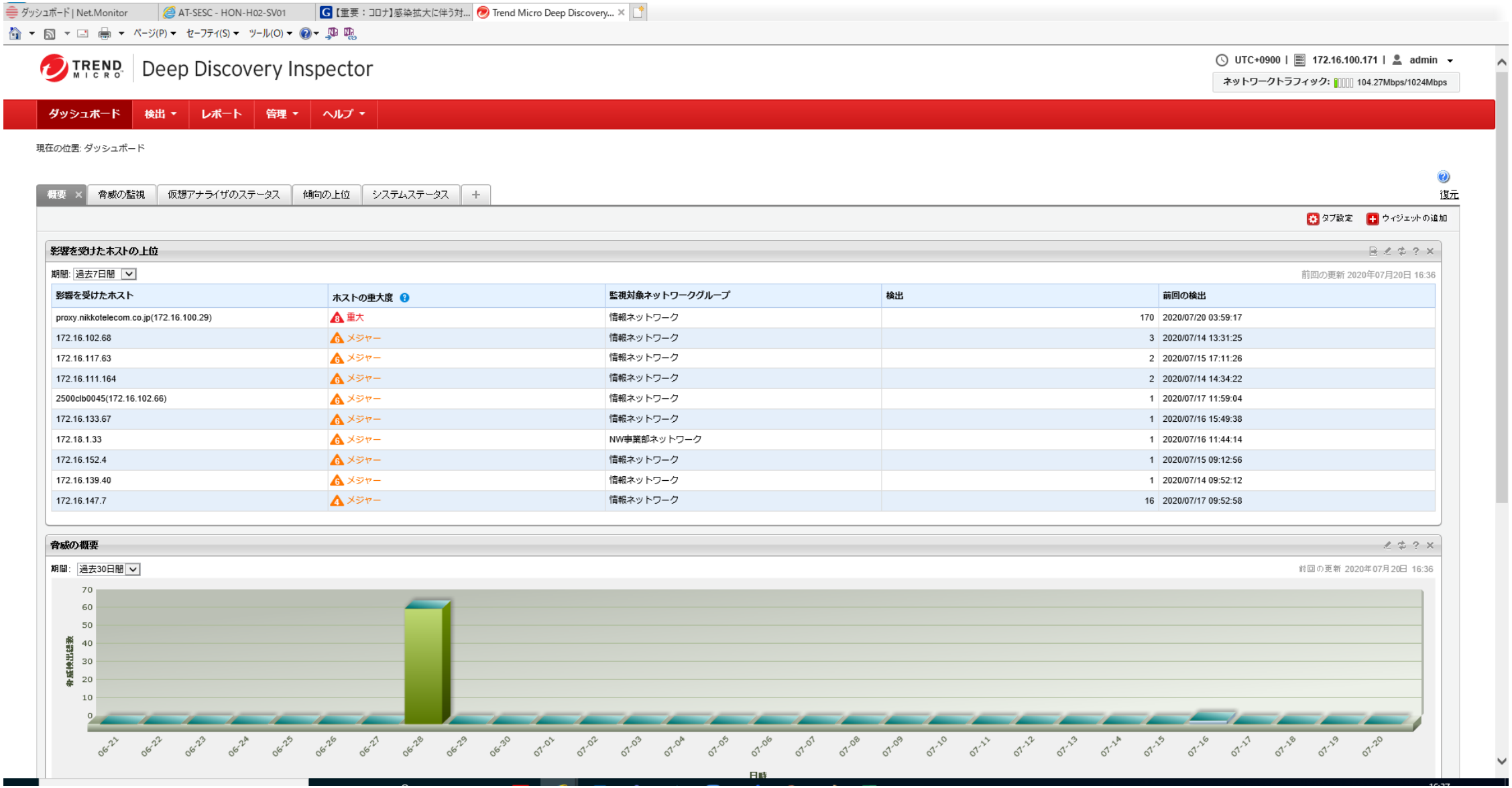
障害の原因特定から
復旧までを
スピードアップ！

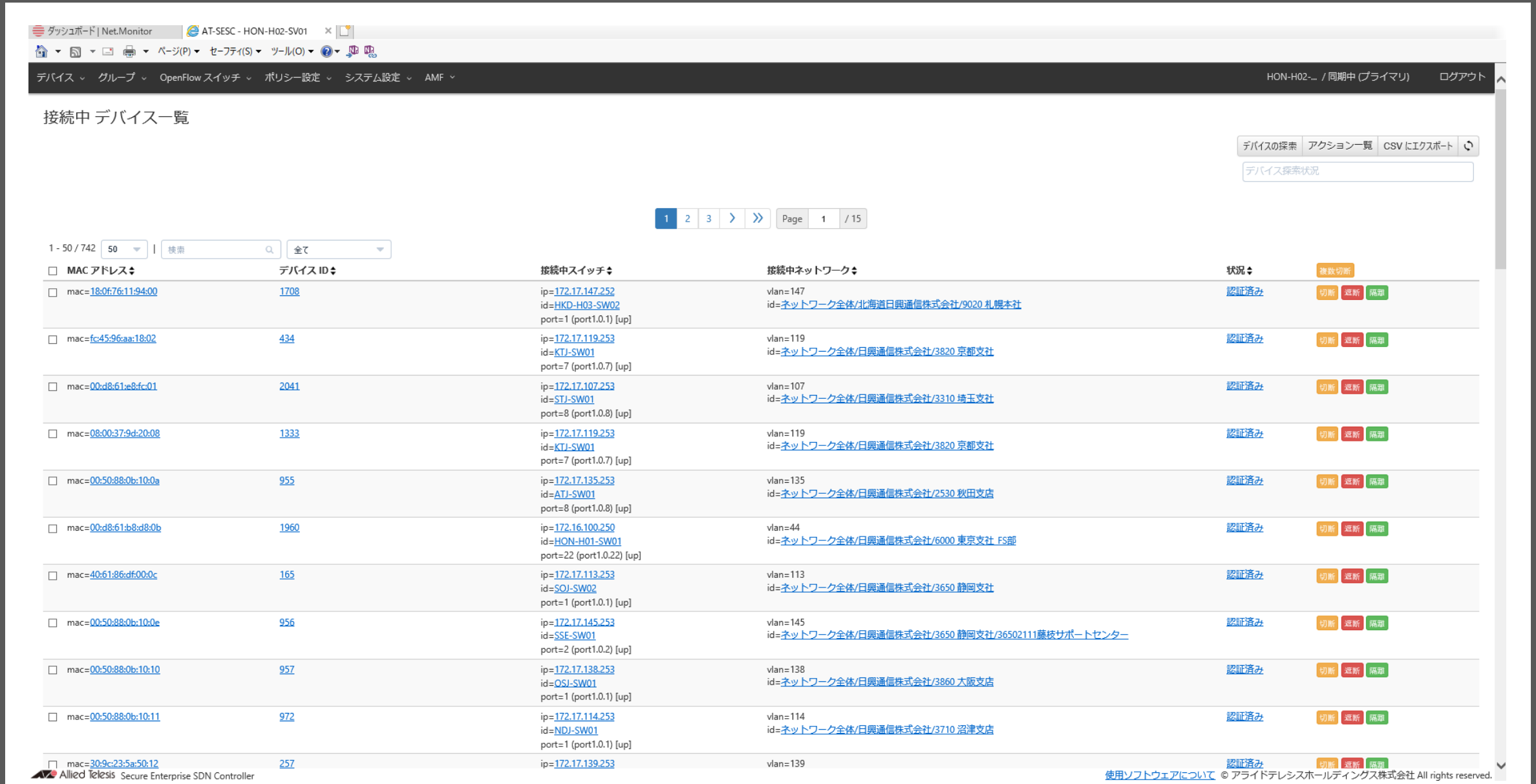

https://net.monitor.allied-telesis.co.jp/1/107/
検索...
ダッシュボード | Net.Monitor
ipa.go.jp
ipa.go.jp
ページ(P)
セーフティ(S)
ツール(O)
Net.Monitor
NTCS_日興通信
IoT監視
ホスト検索
お知らせ
ヘルプ
User3@NTCS
NTCS_日興通信
リモート監視
ダッシュボード
ステータス
ホスト 1
イベント 1
監視データ
アイテム
グラフ
SNMPトラップ
シスログ
AMF-SEC監視
管理ビュー
マップ
カスタムビュー
設定
タグ
ホストステータス
1
90
ホスト
89
正常
障害
週間イベント発生件数
1 件
0.8 件
0.6 件
0.4 件
0.2 件
0 件
0
0
7月13日
7月14日
7月15日
7月16日
7月17日
7月18日
7月19日
システムステータス
ホストグループ
致命的な障害
重度の障害
軽度の障害
警告
情報
SNMPトラップ
NTCS_日興通信
0
1
0
0
0
0
2020年07月20日 16:17:32
最新20件の障害
発生日時
ホストグループ
ホスト
イベント
深刻度
経過時間
2020年06月27日 10:37:54
NTCS_日興通信
NTCS_SNJ-SW01
Pingの応答がありません。
重度の障害
23d 5h 39m
最新20件のSNMPトラップ
サーバ受信時刻
ホストグループ
ホスト
アイテム
値
2020年07月20日 16:01:27
NTCS_日興通信
NTCS_HON-H02-UM01
98.その他機能
2020/07/20 16:01:24 [Notification_Others, fgTrapIpsPkgUpdate] - IPSシグネチャのデータベースが更新されました。 status_code:0

Point 3　強固なセキュリティ

非登録端末の接続や、
ウィルスを検知すると

自動で通信を遮断
端末を切り離す


ダッシュボード | Net.Monitor
AT-SESC - HON-H02-SV01
【重要：コロナ】感染拡大に伴う対...
Trend Micro Deep Discovery...
ページ(P)
セーフティ(S)
ツール(O)
TREND MICRO
Deep Discovery Inspector
UTC+0900 | 172.16.100.171 | admin
ネットワークトラフィック: 104.27Mbps/1024Mbps
ダッシュボード
検出
レポート
管理
ヘルプ
現在の位置: ダッシュボード
概要
脅威の監視
仮想アナライザのステータス
傾向の上位
システムステータス
復元
タブ設定
ウィジェットの追加
影響を受けたホストの上位
期間: 過去7日間
前回の更新 2020年07月20日 16:36
影響を受けたホスト
ホストの重大度
監視対象ネットワークグループ
検出
前回の検出
proxy.nikkotelecom.co.jp(172.16.100.29) 重大 情報ネットワーク 170 2020/07/20 03:59:17
172.16.102.68 メジャー 情報ネットワーク 3 2020/07/14 13:31:25
172.16.117.63 メジャー 情報ネットワーク 2 2020/07/15 17:11:26
172.16.111.164 メジャー 情報ネットワーク 2 2020/07/14 14:34:22
2500clb0045(172.16.102.66) メジャー 情報ネットワーク 1 2020/07/17 11:59:04
172.16.133.67 メジャー 情報ネットワーク 1 2020/07/16 15:49:38
172.18.1.33 メジャー NW事業部ネットワーク 1 2020/07/16 11:44:14
172.16.152.4 メジャー 情報ネットワーク 1 2020/07/15 09:12:56
172.16.139.40 メジャー 情報ネットワーク 1 2020/07/14 09:52:12
172.16.147.7 メジャー 情報ネットワーク 16 2020/07/17 09:52:58
脅威の概要
期間: 過去30日間
前回の更新 2020年07月20日 16:36
脅威検出総数
日時


ダッシュボード | Net.Monitor
AT-SESC - HON-H02-SV01
ページ(P)
セーフティ(S)
ツール(O)
デバイス
グループ
OpenFlow スイッチ
ポリシー設定
システム設定
AMF
HON-H02-... / 同期中 (プライマリ)
ログアウト
接続中 デバイス一覧
デバイスの探索
アクション一覧
CSV にエクスポート
デバイス探索状況
1 2 3
Page 1 / 15
1 - 50 / 742
50
検索
全て
MAC アドレス
デバイス ID
接続中スイッチ
接続中ネットワーク
状況
複数切断
mac=18:0f:76:11:94:00
1708
ip=172.17.147.252
id=HKD-H03-SW02
port=1 (port1.0.1) [up]
vlan=147
id=ネットワーク全体/北海道日興通信株式会社/9020 札幌本社
認証済み
切断 遮断 隔離
mac=fc:45:96:aa:18:02
434
ip=172.17.119.253
id=KTJ-SW01
port=7 (port1.0.7) [up]
vlan=119
id=ネットワーク全体/日興通信株式会社/3820 京都支社
認証済み
切断 遮断 隔離
mac=00:d8:61:e8:fc:01
2041
ip=172.17.107.253
id=STJ-SW01
port=8 (port1.0.8) [up]
vlan=107
id=ネットワーク全体/日興通信株式会社/3310 埼玉支社
認証済み
切断 遮断 隔離
mac=08:00:37:9d:20:08
1333
ip=172.17.119.253
id=KTJ-SW01
port=7 (port1.0.7) [up]
vlan=119
id=ネットワーク全体/日興通信株式会社/3820 京都支社
認証済み
切断 遮断 隔離
mac=00:50:88:0b:10:0a
955
ip=172.17.135.253
id=ATJ-SW01
port=8 (port1.0.8) [up]
vlan=135
id=ネットワーク全体/日興通信株式会社/2530 秋田支店
認証済み
切断 遮断 隔離
mac=00:d8:61:b8:d8:0b
1960
ip=172.16.100.250
id=HON-H01-SW01
port=22 (port1.0.22) [up]
vlan=44
id=ネットワーク全体/日興通信株式会社/6000 東京支社 FS部
認証済み
切断 遮断 隔離
mac=40:61:86:df:00:0c
165
ip=172.17.113.253
id=SOJ-SW02
port=1 (port1.0.1) [up]
vlan=113
id=ネットワーク全体/日興通信株式会社/3650 静岡支社
認証済み
切断 遮断 隔離
mac=00:50:88:0b:10:0e
956
ip=172.17.145.253
id=SSE-SW01
port=2 (port1.0.2) [up]
vlan=145
id=ネットワーク全体/日興通信株式会社/3650 静岡支社/36502111藤枝サポートセンター
認証済み
切断 遮断 隔離
mac=00:50:88:0b:10:10
957
ip=172.17.138.253
id=OSJ-SW01
port=1 (port1.0.1) [up]
vlan=138
id=ネットワーク全体/日興通信株式会社/3860 大阪支店
認証済み
切断 遮断 隔離
mac=00:50:88:0b:10:11
972
ip=172.17.114.253
id=NDJ-SW01
port=1 (port1.0.1) [up]
vlan=114
id=ネットワーク全体/日興通信株式会社/3710 沼津支店
認証済み
切断 遮断 隔離
mac=30:9c:23:5a:50:12
257
ip=172.17.139.253
vlan=139
認証済み
Allied Telesis Secure Enterprise SDN Controller
使用ソフトウェアについて
© アライドテレシスホールディングス株式会社 All rights reserved.

Point４　働き方改革の環境整備

残業・休出は
事前申請しないと
端末が使えない

「働き方改革」を
積極的に推進！

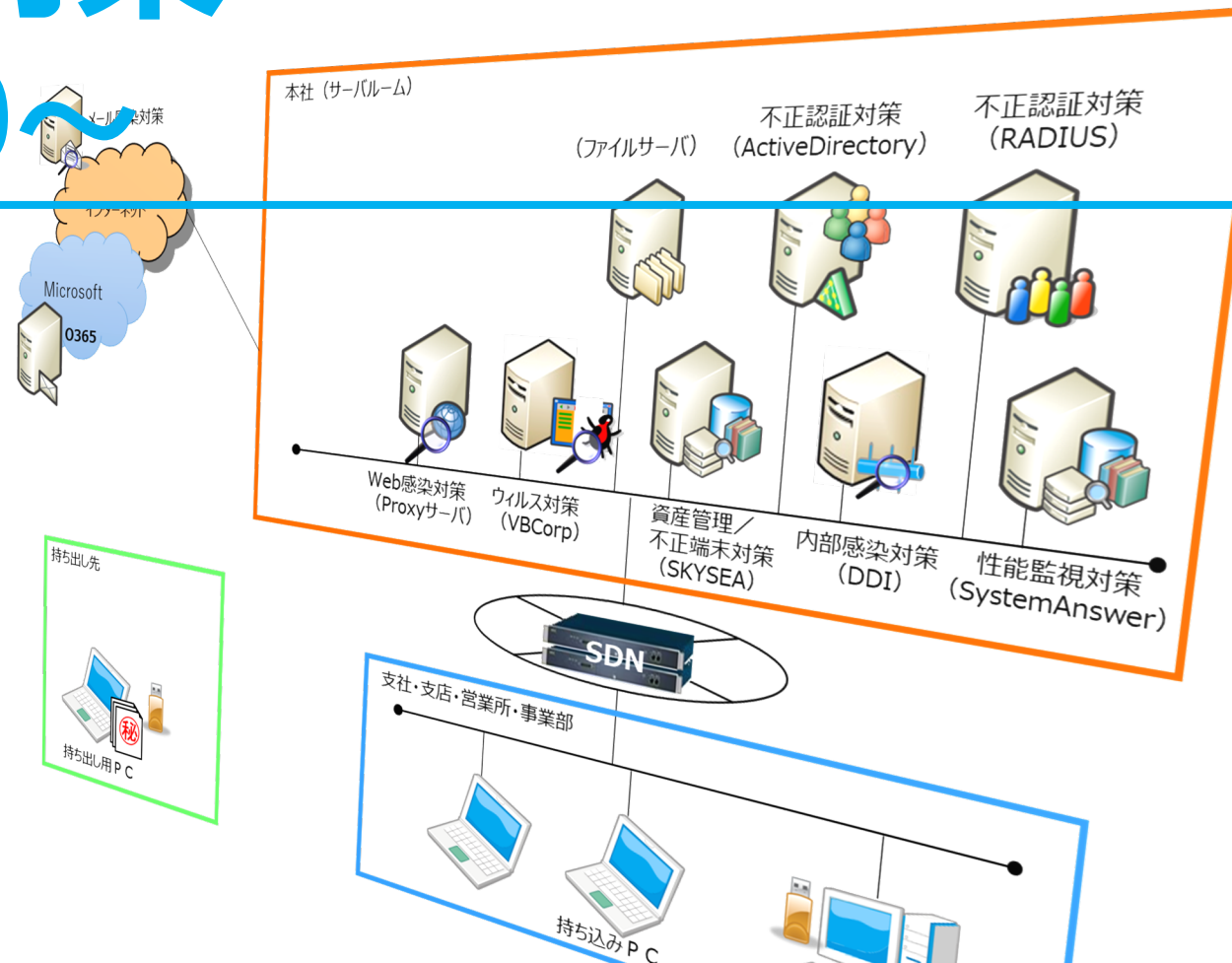
Point 5　支援体制とノウハウの蓄積

ユーザーの立場
：情報システム部

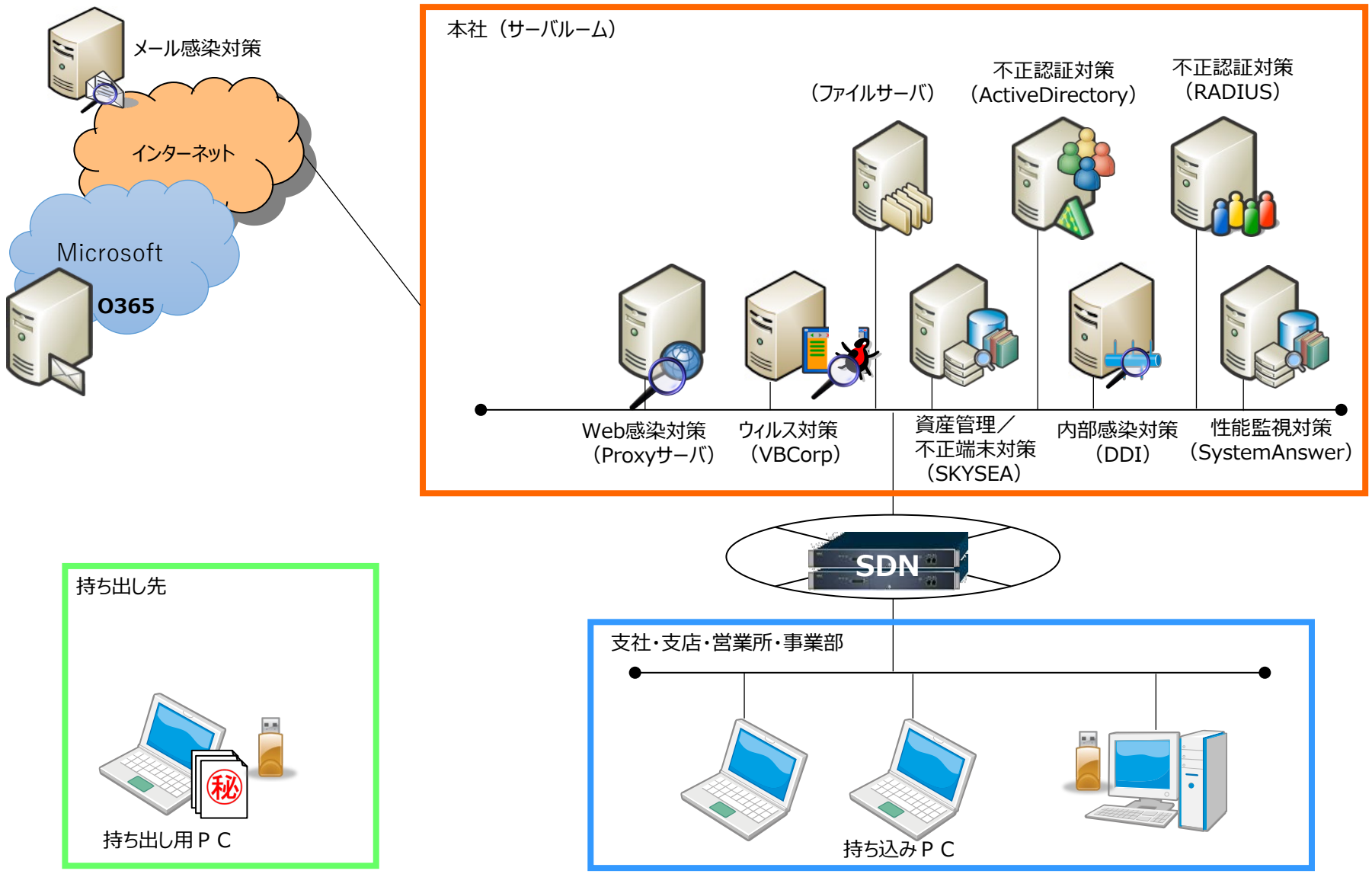
SIerの立場
：ネットワーク事業部

お客様の
提案に活かします

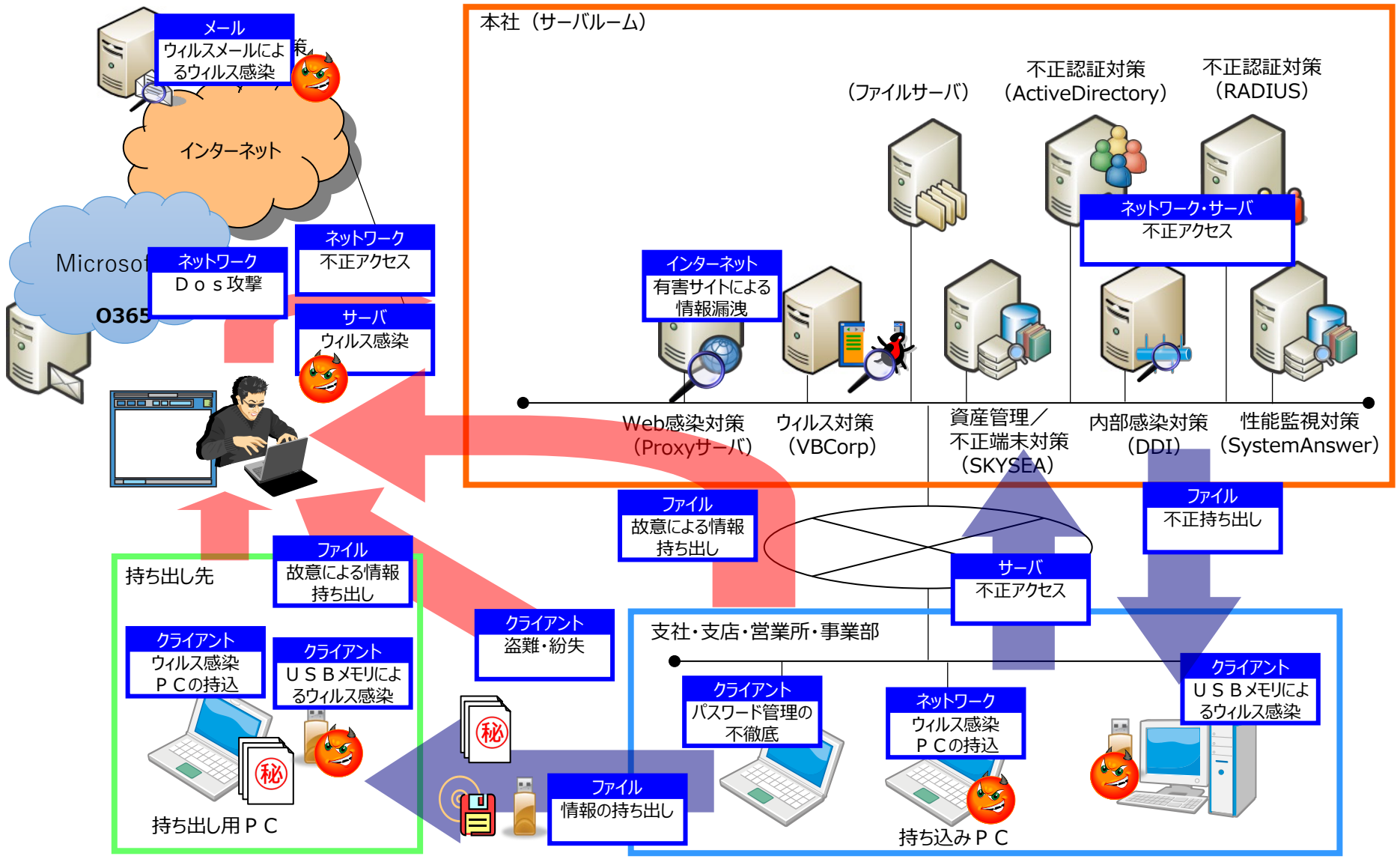
当社のセキュリティ対策
～セキュリティマップより～



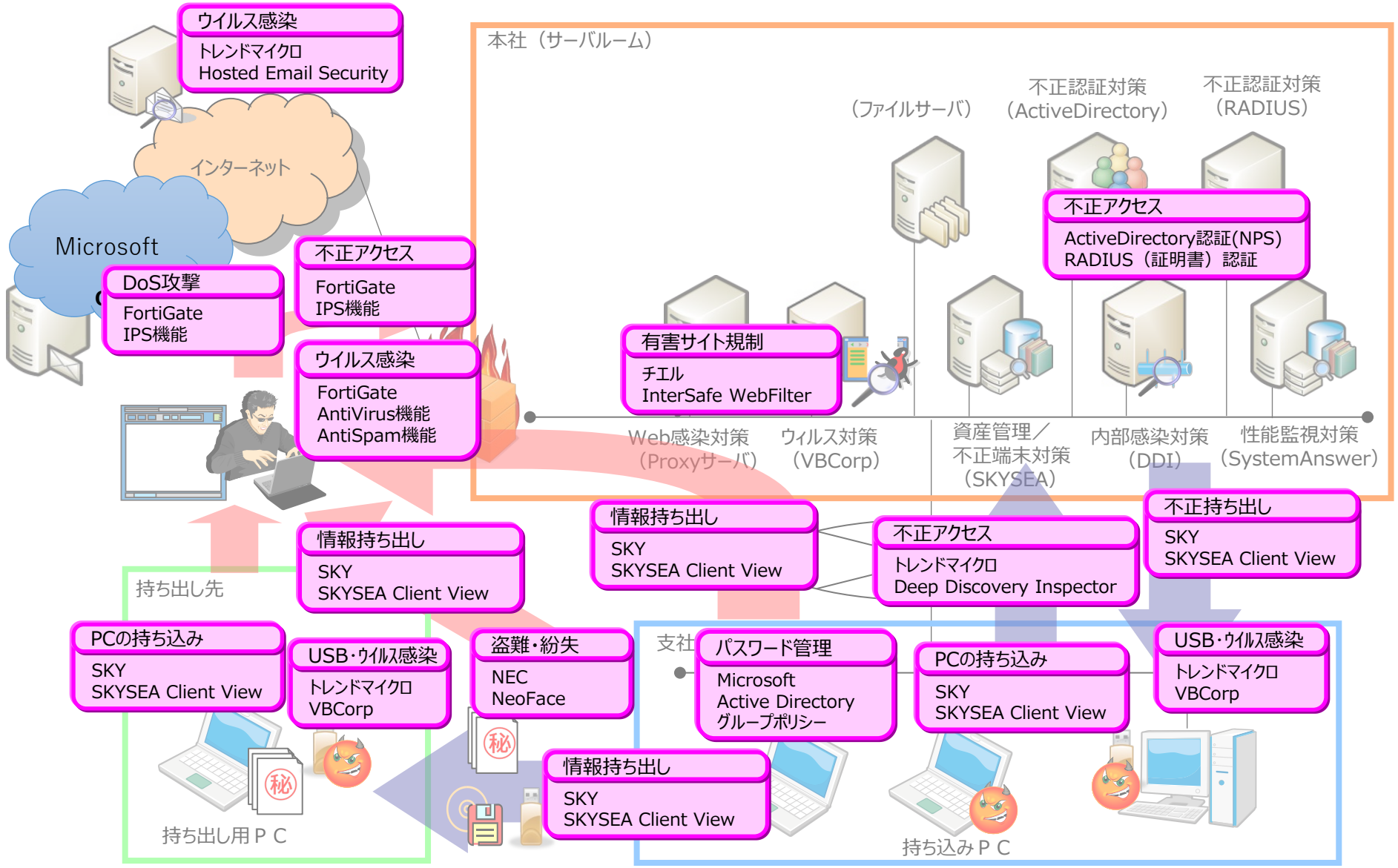
全体図（SuIRENのセキュリティ対策）



起こりうるセキュリティリスク

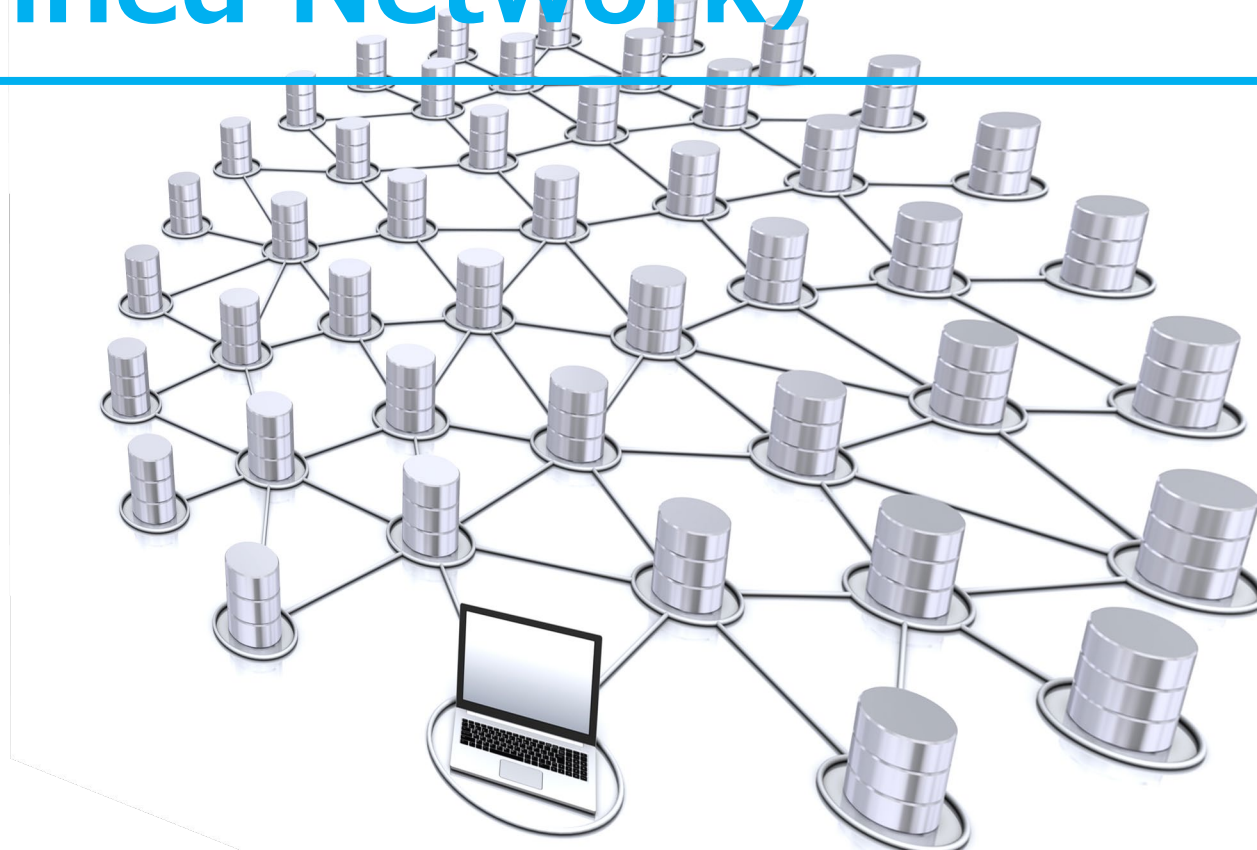


起こりうるセキュリティリスクへの対策

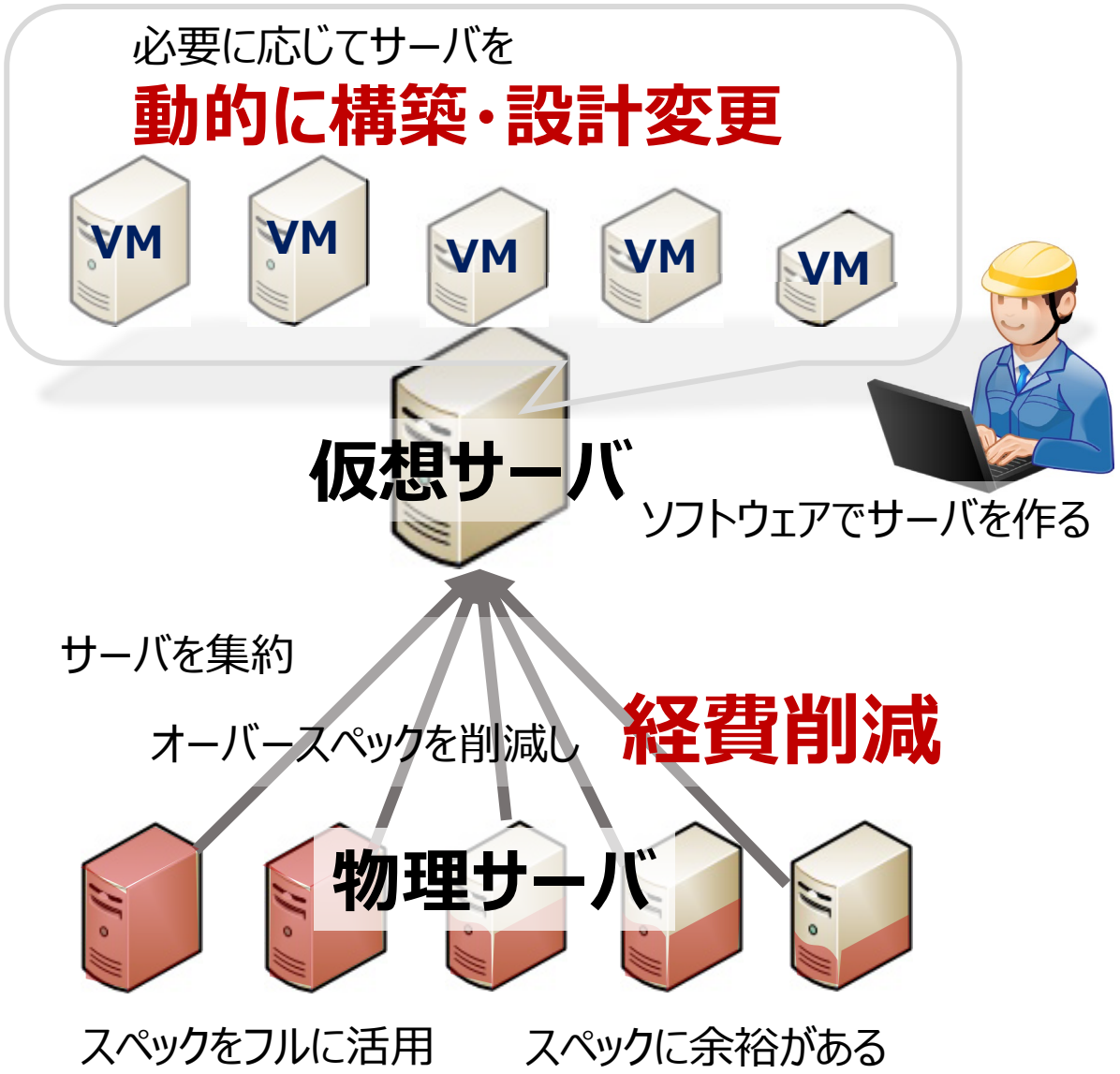


当社のセキュアネットワークを支える技術
SDN（Software-Defined Network）

SDN（Software Defined Network）とは…
単一のソフトウェアによりネットワーク機器を集中的に制御して、ネットワーク構成や設定などを柔軟に動的に変更することができる「技術の総称」のことです。
SDNでは管理ツールで設定するだけで、ネットワーク構成、性能、機能を動的に変更できます。



サーバの仮想化



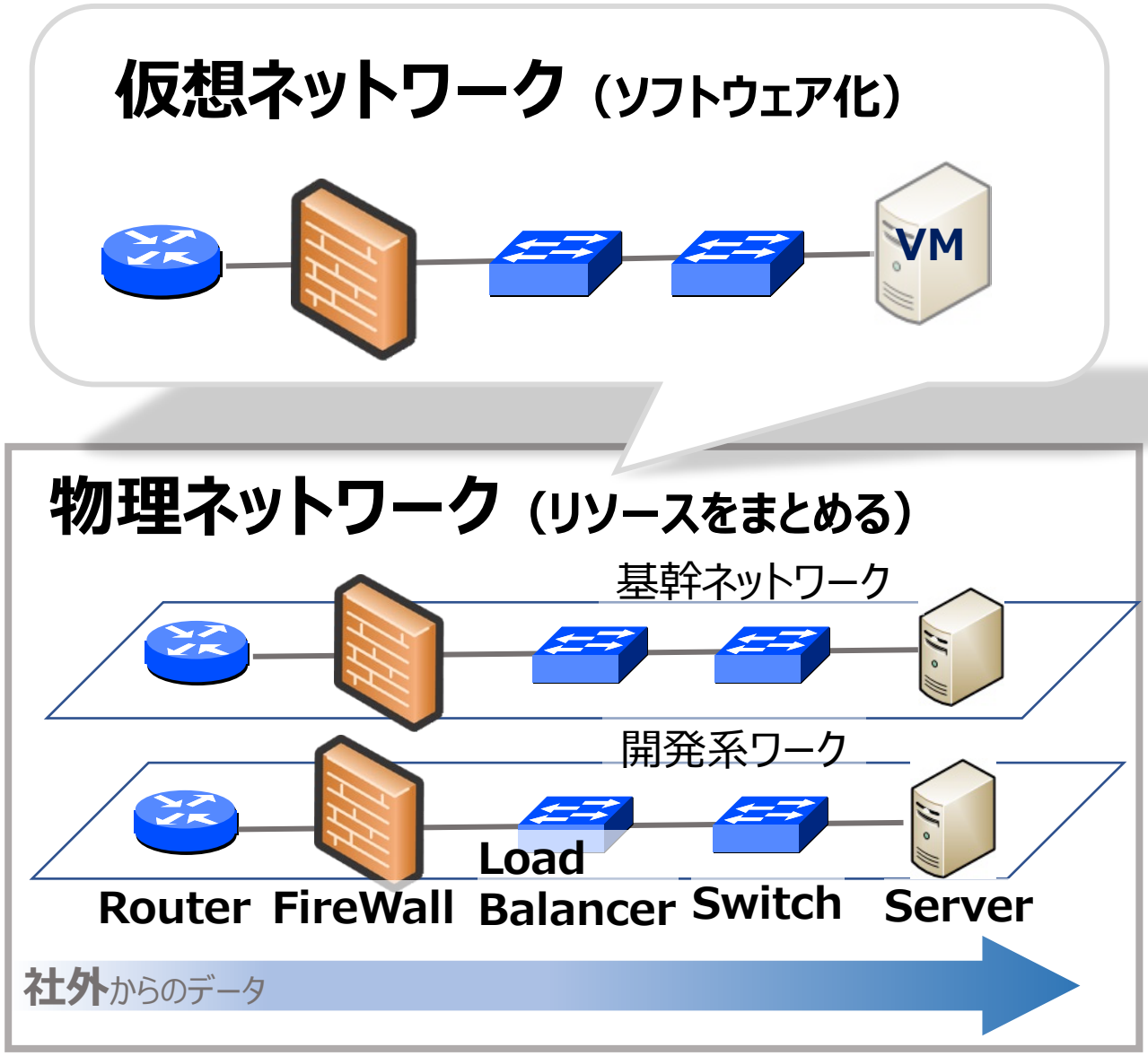
サーバの仮想化で

- **経費削減**
- **動的に構築・設定変更**

を実現

ネットワークの仮想化で
システム全体の生産性を
向上

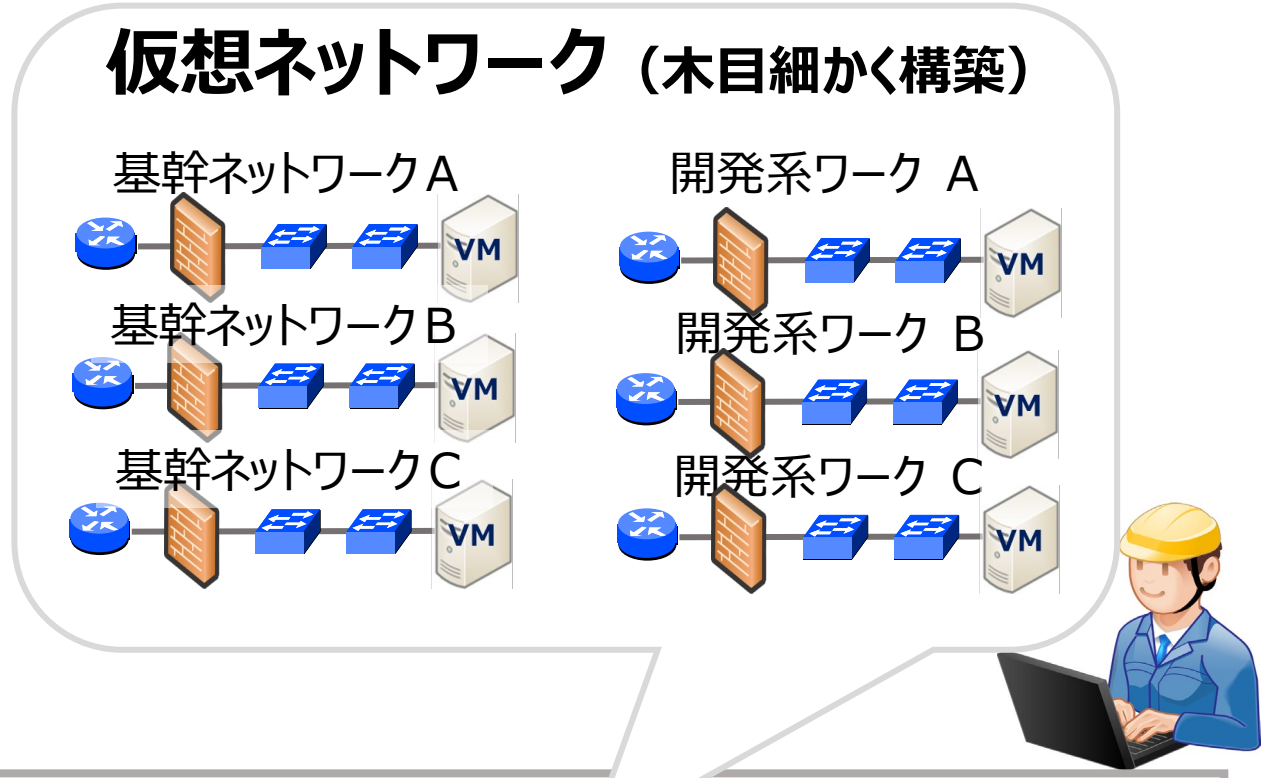
ネットワークの仮想化

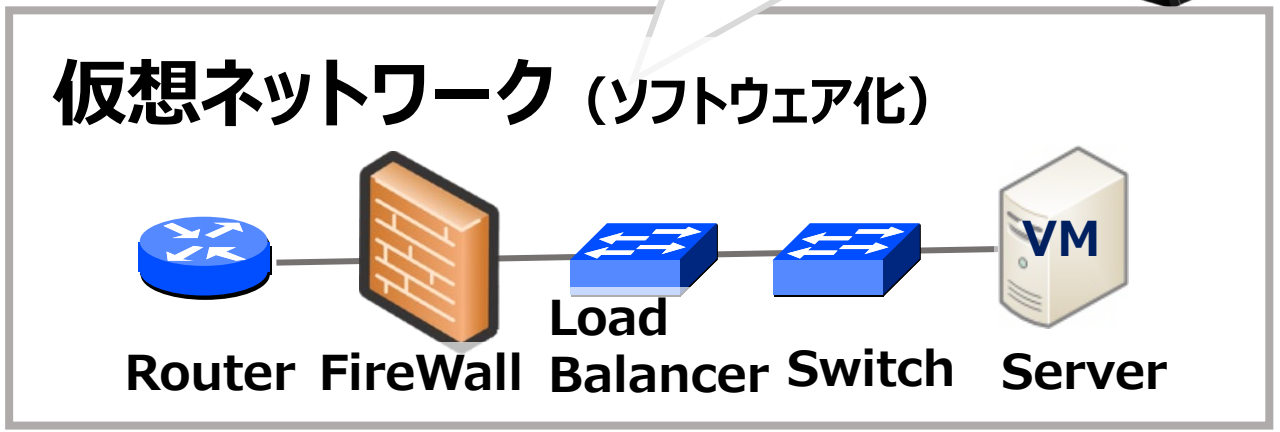


ネットワークの仮想化で

- サーバ仮想化と同様に、様々なネットワーク機器がサーバ上にソフトウェアで統合され、**経費削減**
- サーバの**動的な構築・設定変更**に対応

ネットワークの仮想化

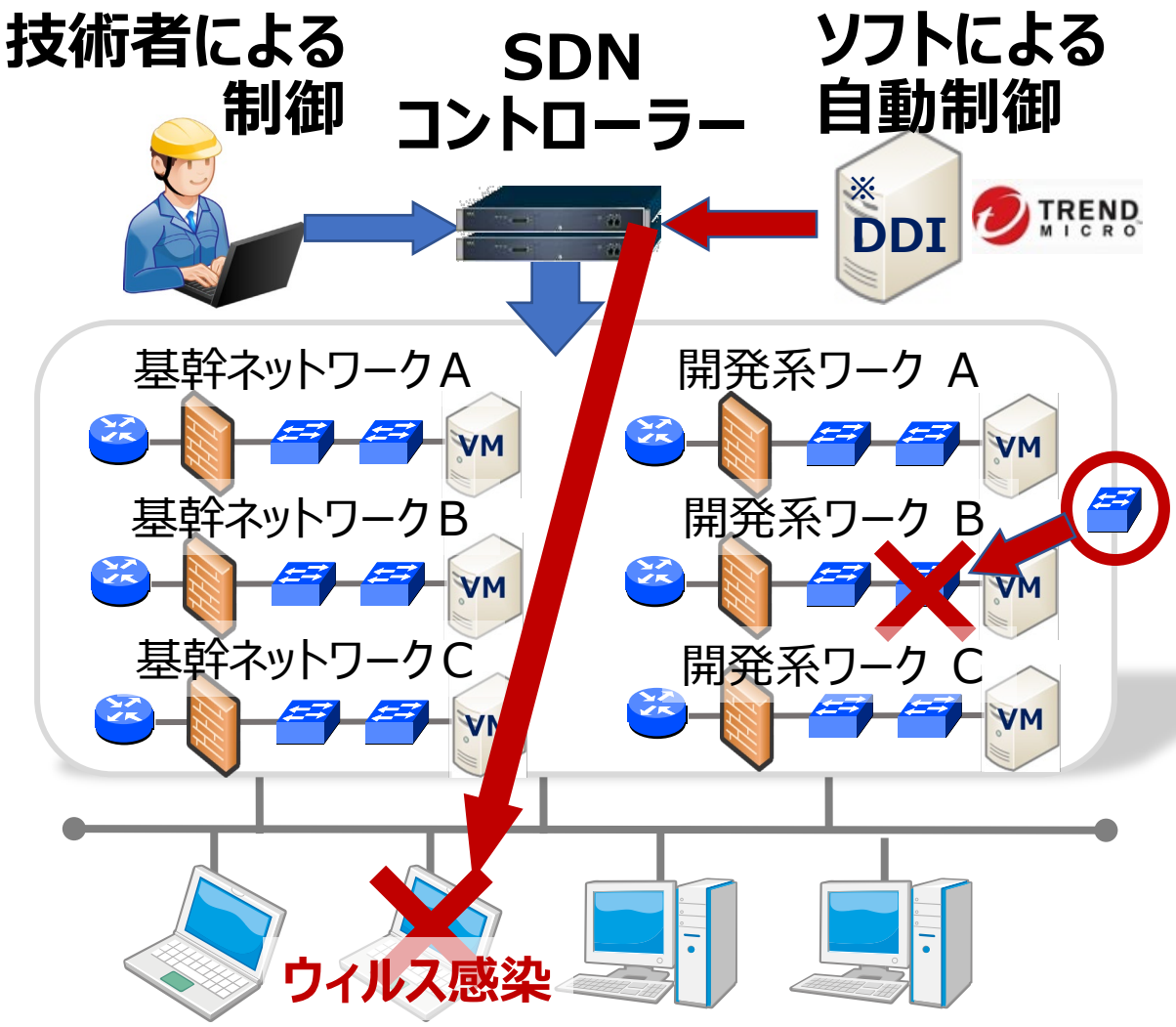




ネットワークの仮想化で

- 物理ネットワークよりも木目の細かい複雑なネットワーク構築が可能。
- ネットワークを機能別に木目細かく構築することで**セキュリティを向上**

SDNによるネットワーク制御



※DDI（Deep Discovery Inspector）とは
気付くことが難しい標的型攻撃やゼロデイ攻撃をネットワーク上の振る舞いから見つけ出し、早期に対処し被害の深刻化を防ぐためのトレンドマイクロ社製品です。

SDNの制御機能で

- 仮想ネットワークをソフトで集中管理、**障害への対応力を強化**
- セキュリティソフトと連携することで、**サイバー攻撃への対応力強化**

仮想化とSDNで何が出来る？

ネットワークリソースの有効活用
動的構築・設定変更

物理ネットワーク機器の一元管理と、無駄のない仮想ネットワーク構築で経費削減を実現します。ソフトウェアでネットワークを必要な時に動的に構築します。

SDNコントローラーによる
ネットワーク管理

ソフトウェアによるネットワーク管理が、障害を監視し早期発見をします。さらに、障害箇所を回避した新たな経路を設定し通信を継続させます。

ソフトウェア連携による
自動制御

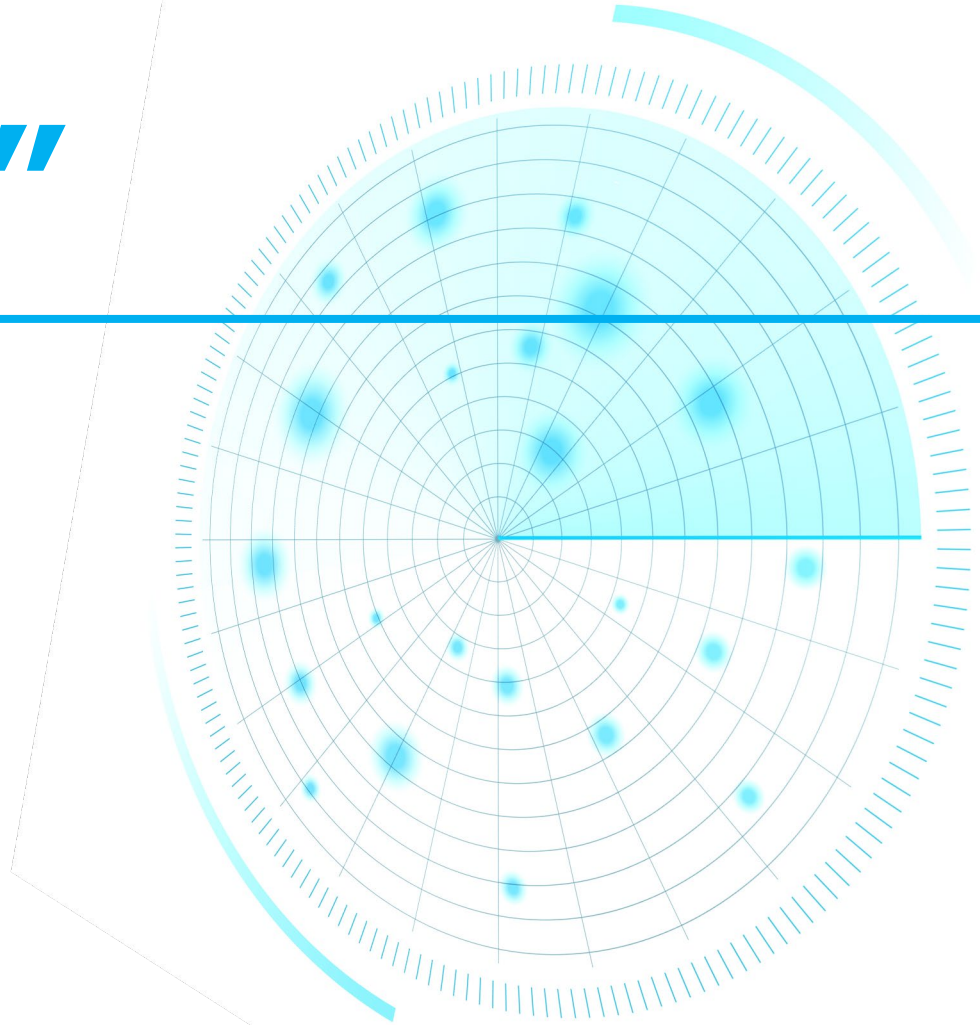
今までは人間が行っていたネットワークの監視、異常の発見と、その異常に対する対策をソフトウェアとの連携で自動化します。

セキュリティソフトや資産管理ソフトとの連携で、被疑端末を発見

↓

自動切断

“検知”そして“対策”



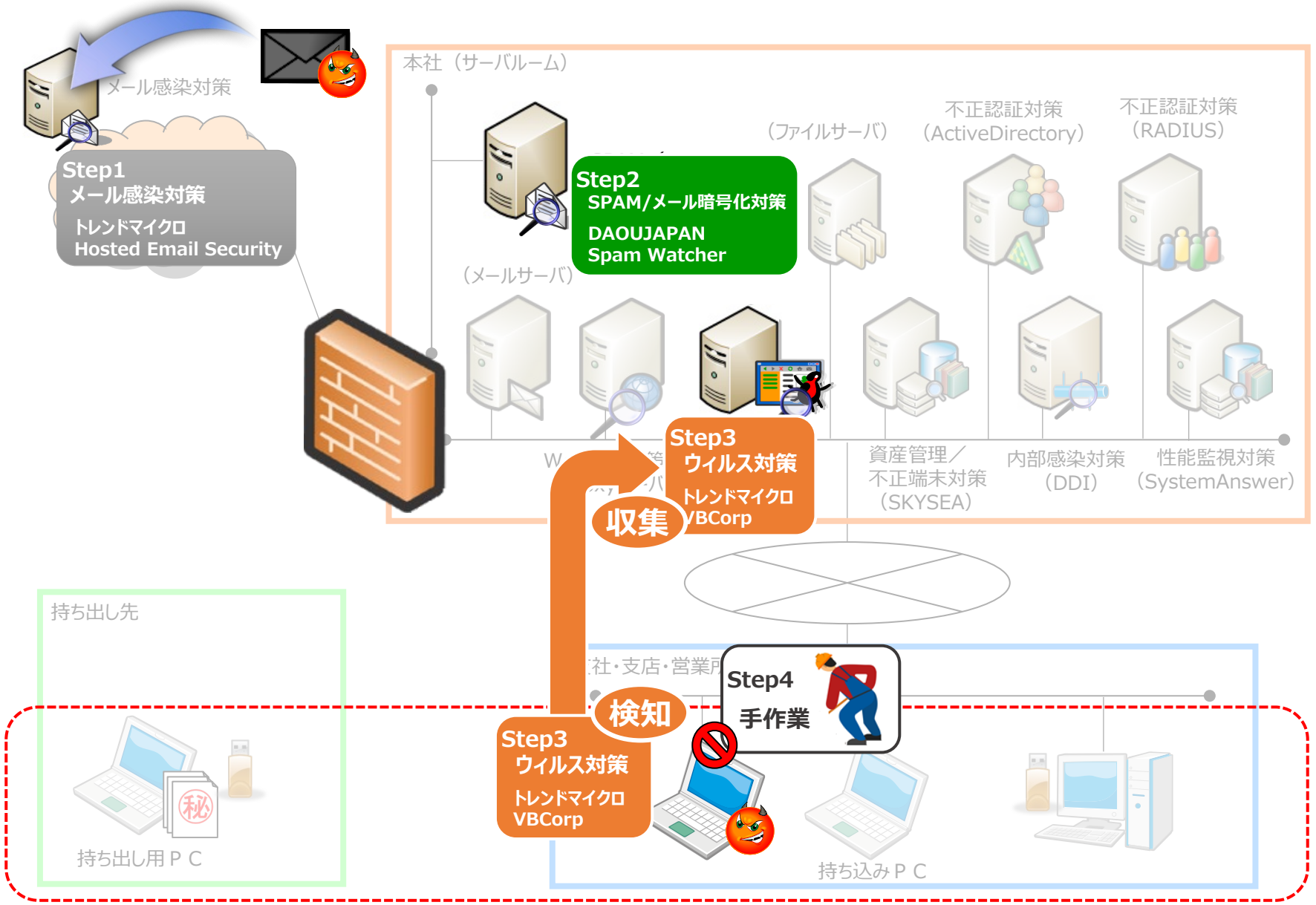
ウィルスメールを受信したら （SuIREN導入前）

Step 1
マルウェア/SPAM
入口検知・駆除

Step 2
SPAM
入口検知・駆除

Step 3
マルウェア
端末検知⇒サーバ

Step 4
ケーブルを抜いて
ネットワーク遮断



ウィルスメールを受信したら （SuIREN導入後）

Step 1
マルウェア/SPAM
入口検知・駆除

Step 2
マルウェア/SPAM
入口ブロック

Step 3
SPAM
入口検知・駆除

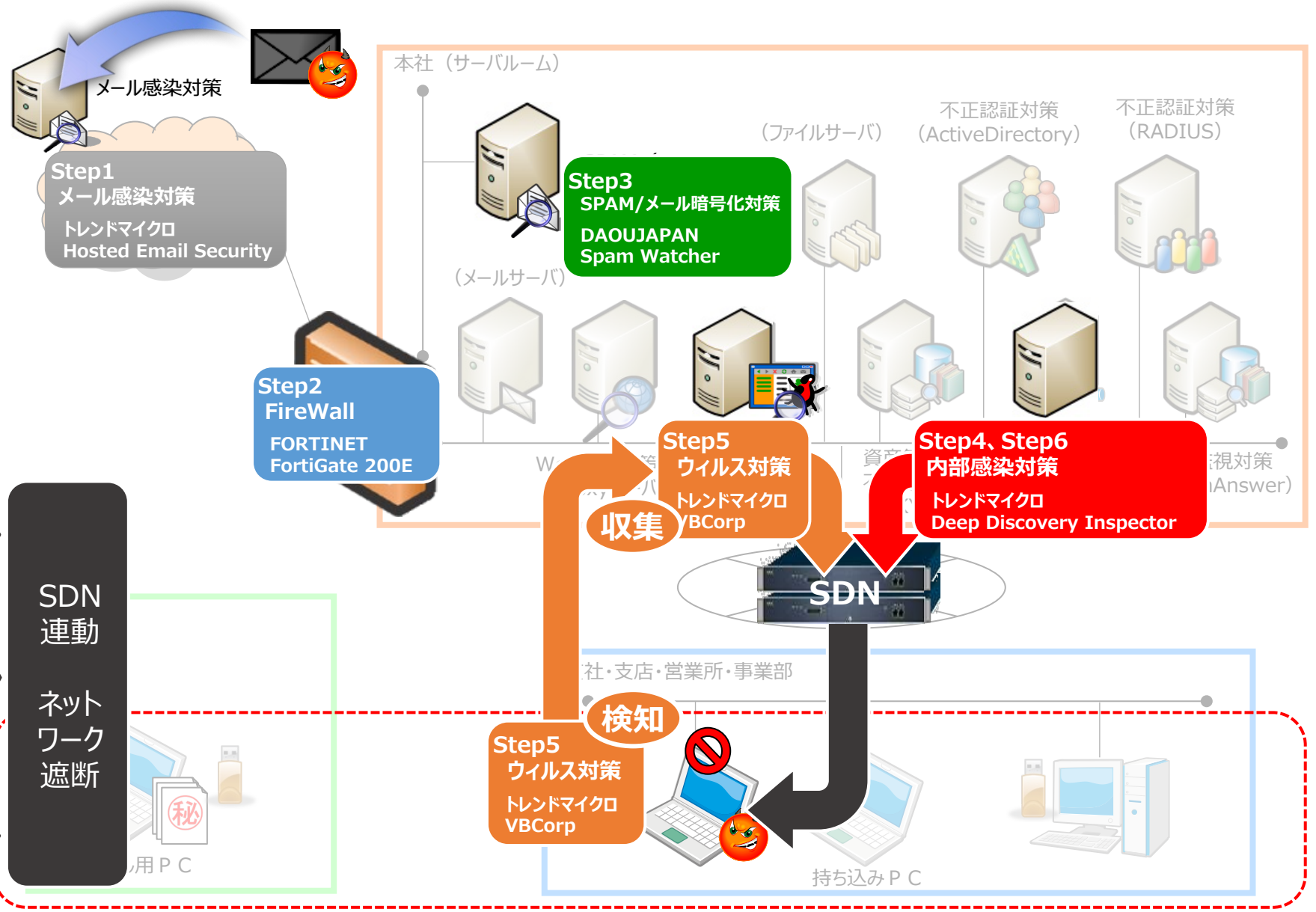
Step 4
マルウェア
内部の拡散を検知

Step 5
マルウェア
端末検知⇒サーバ

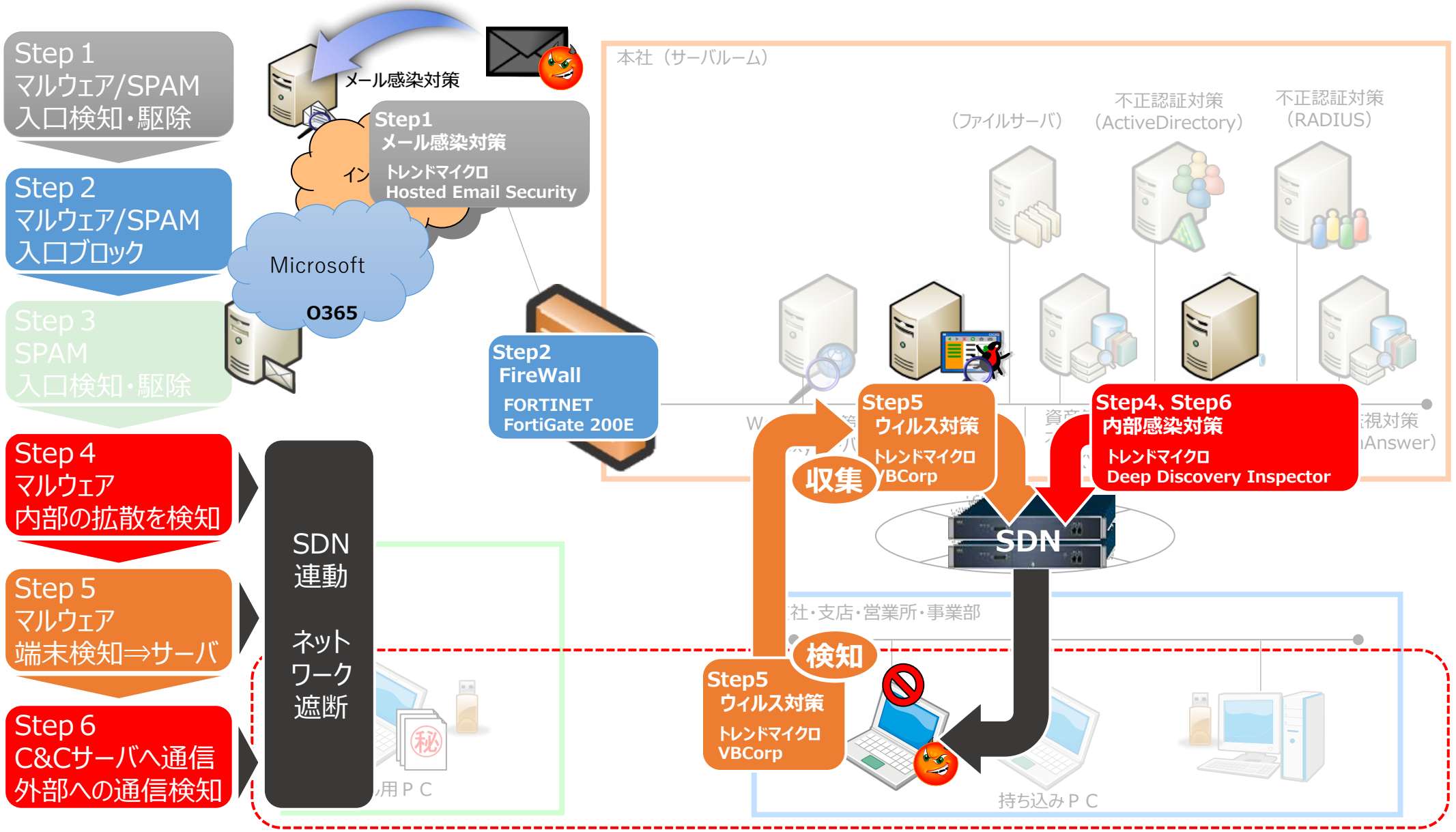
Step 6
C&Cサーバへ通信
外部への通信検知

SDN
連動

ネット
ワーク
遮断



ウィルスメールを受信したら （O365導入後）

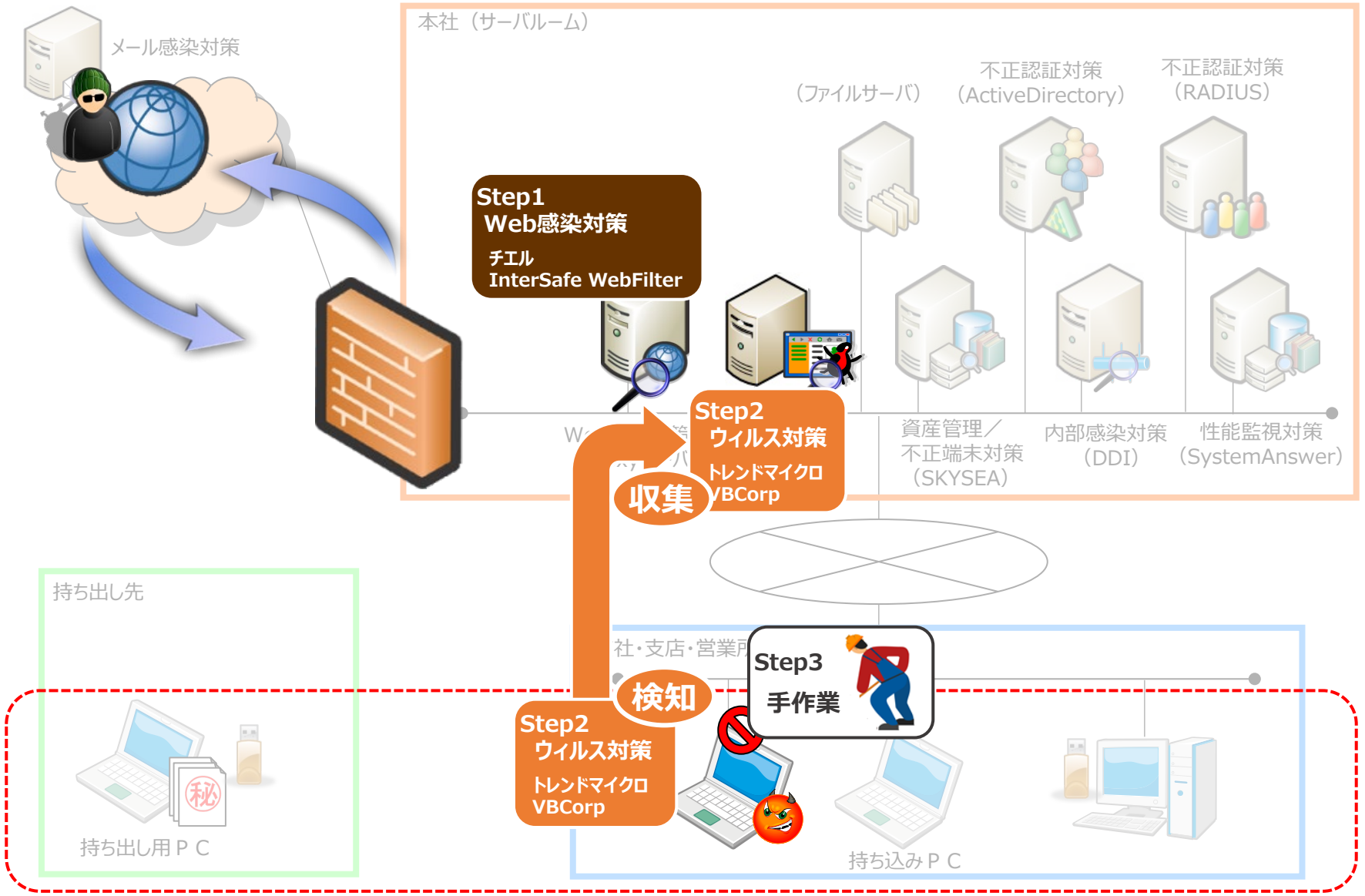


有害サイトを閲覧してしまったら （SuIREN導入前）

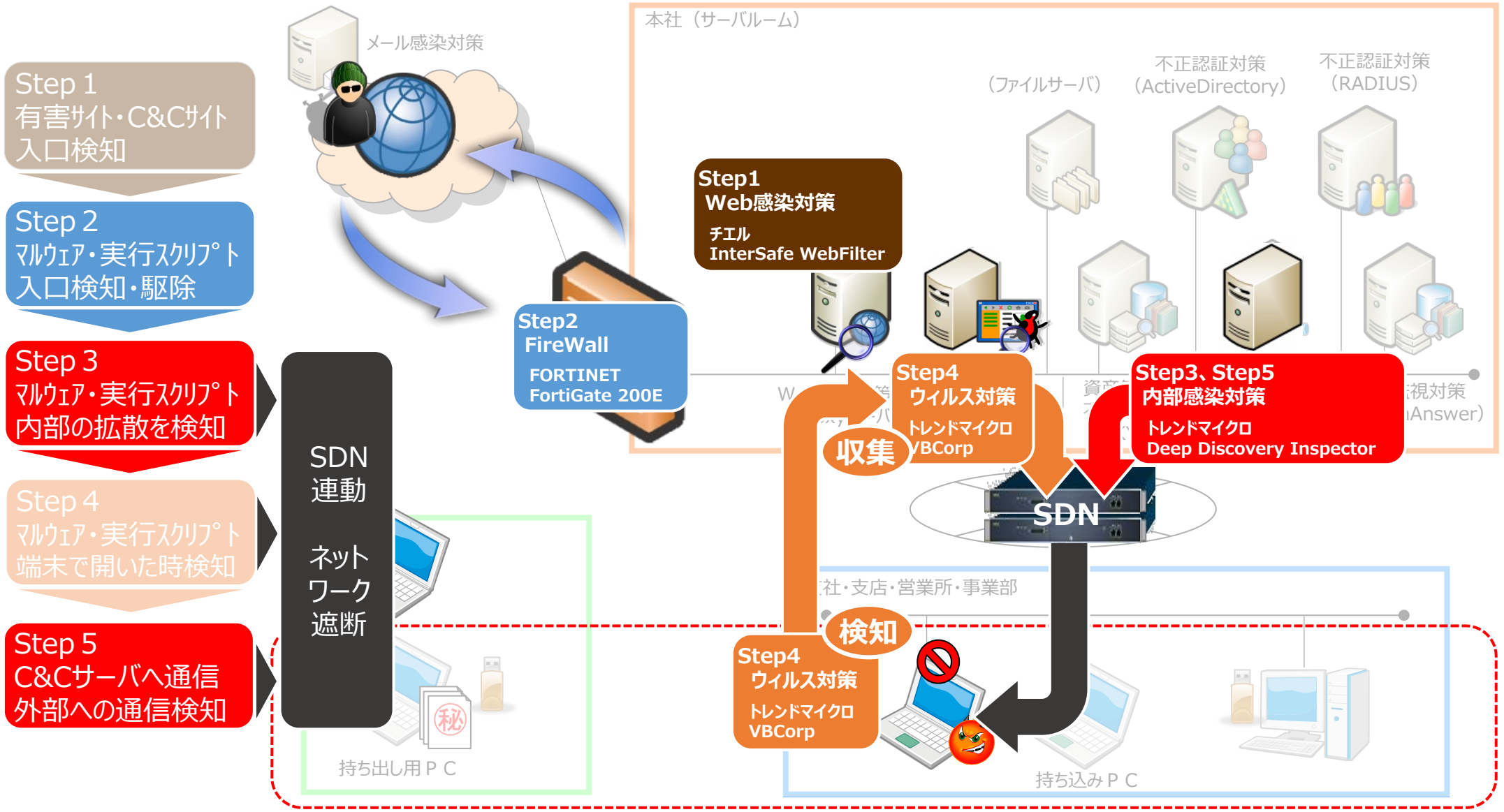
Step 1
有害ｻｲﾄ・C&Cｻｲﾄ
入口検知

Step 2
ﾏﾙｳｪｱ・実行ｽｸﾘﾌﾟﾄ
端末で開いた時検知

Step 3
ケーブルを抜いて
ネットワーク遮断



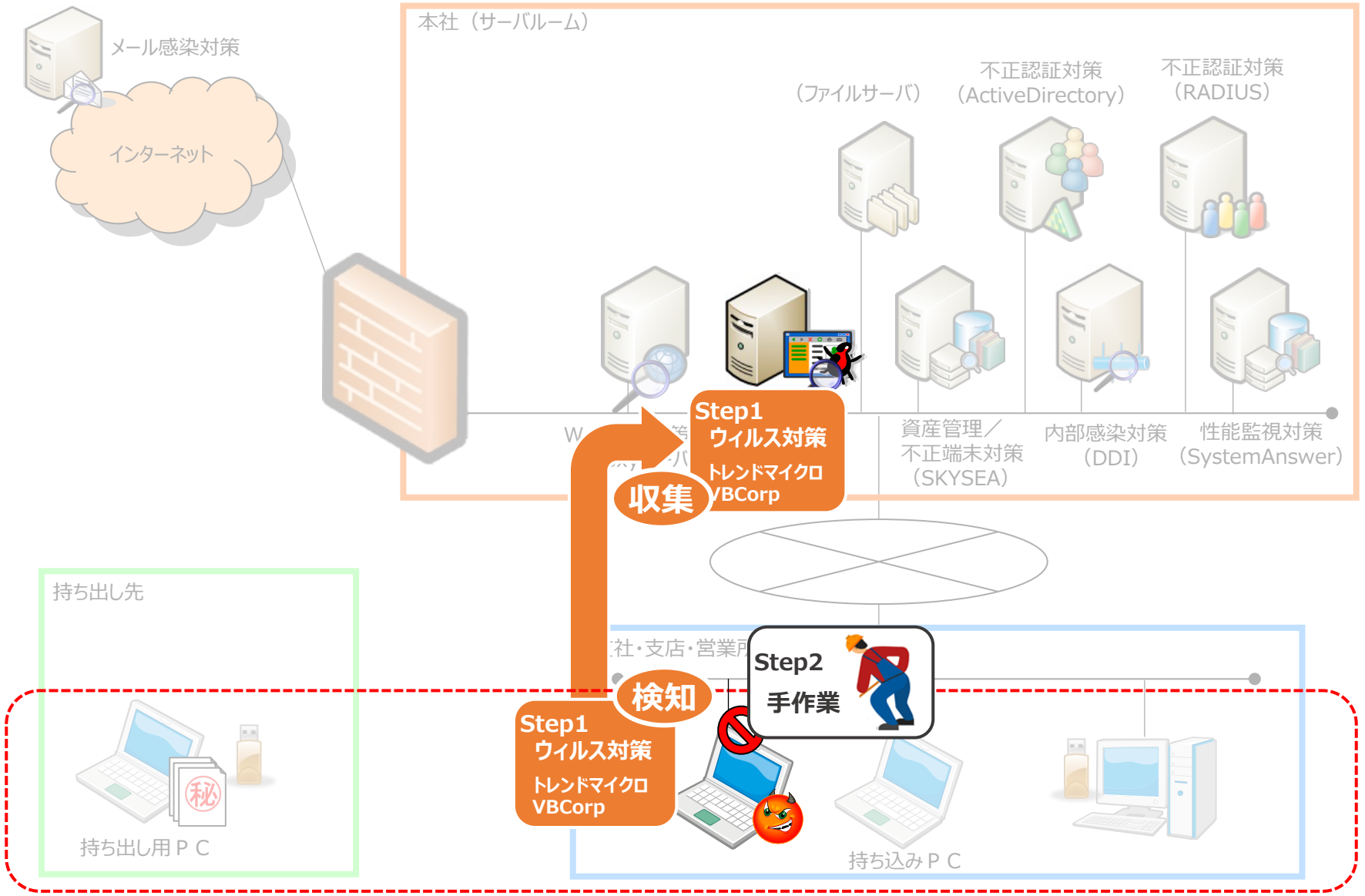
有害サイトを閲覧してしまったら （SuIREN導入後）



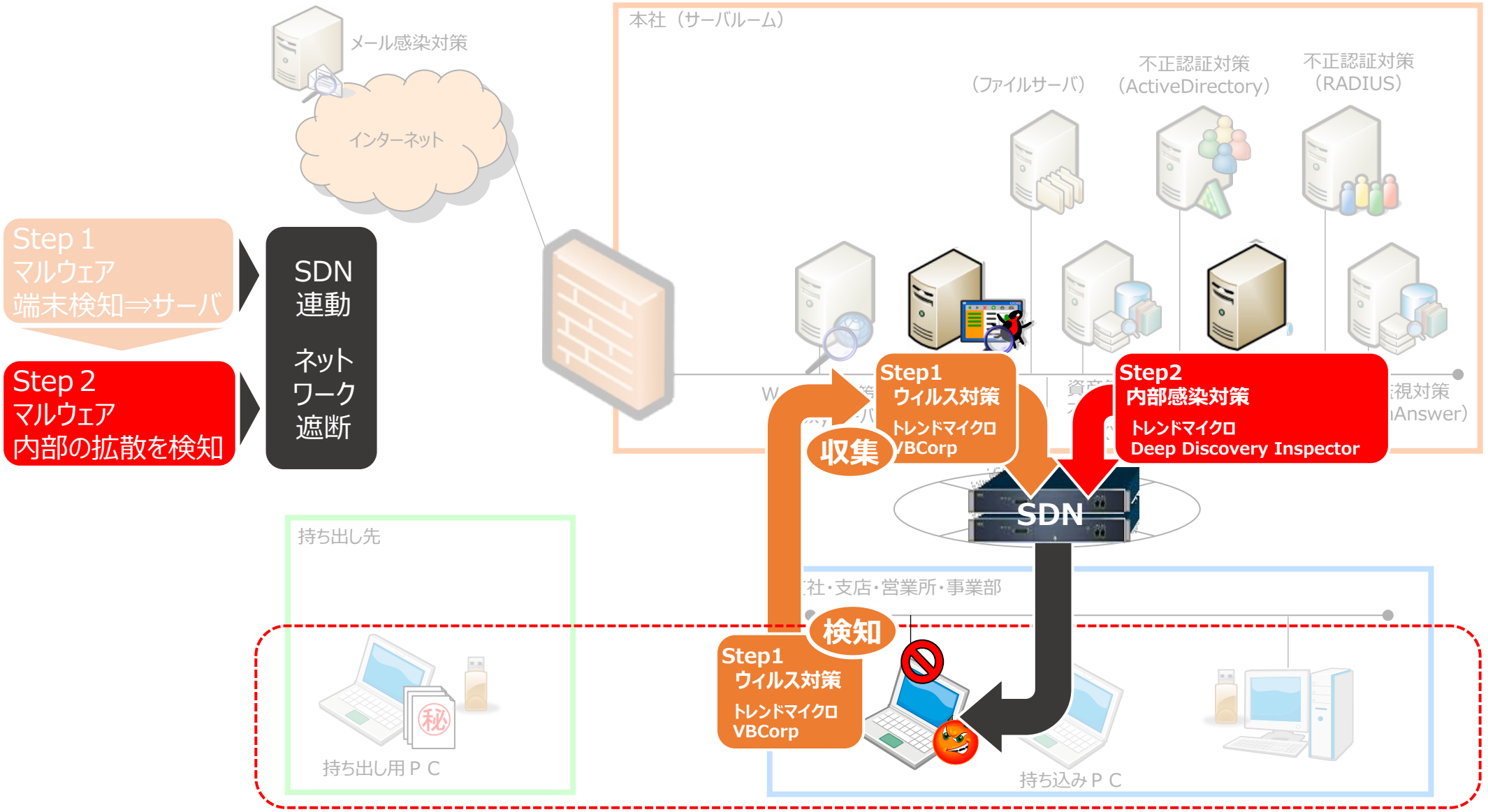
USBメモリから感染したら （SuIREN導入前）

Step 1
マルウェア
端末検知⇒サーバ

Step 2
ケーブルを抜いて
ネットワーク遮断

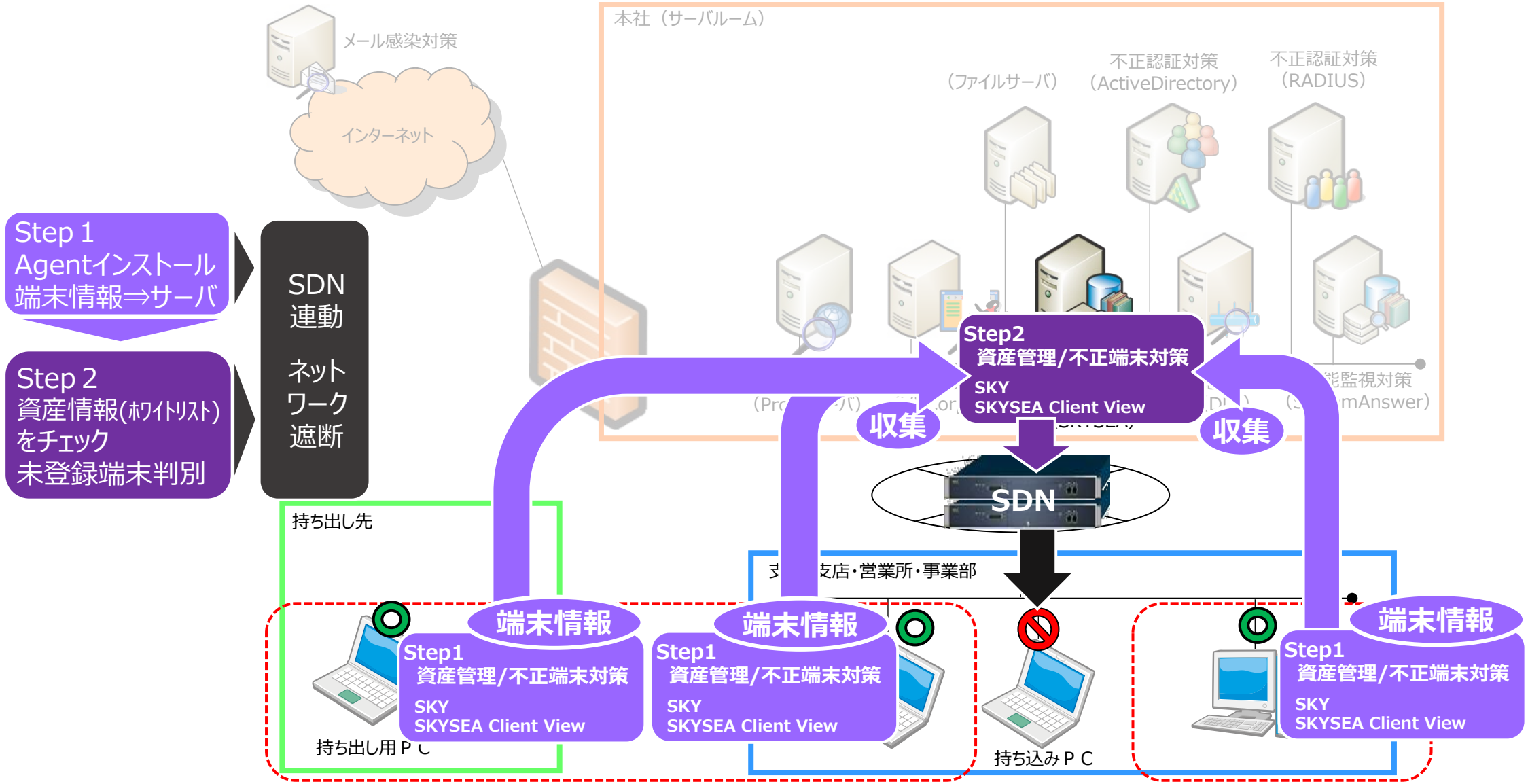


USBメモリから感染したら （SuIREN導入後）

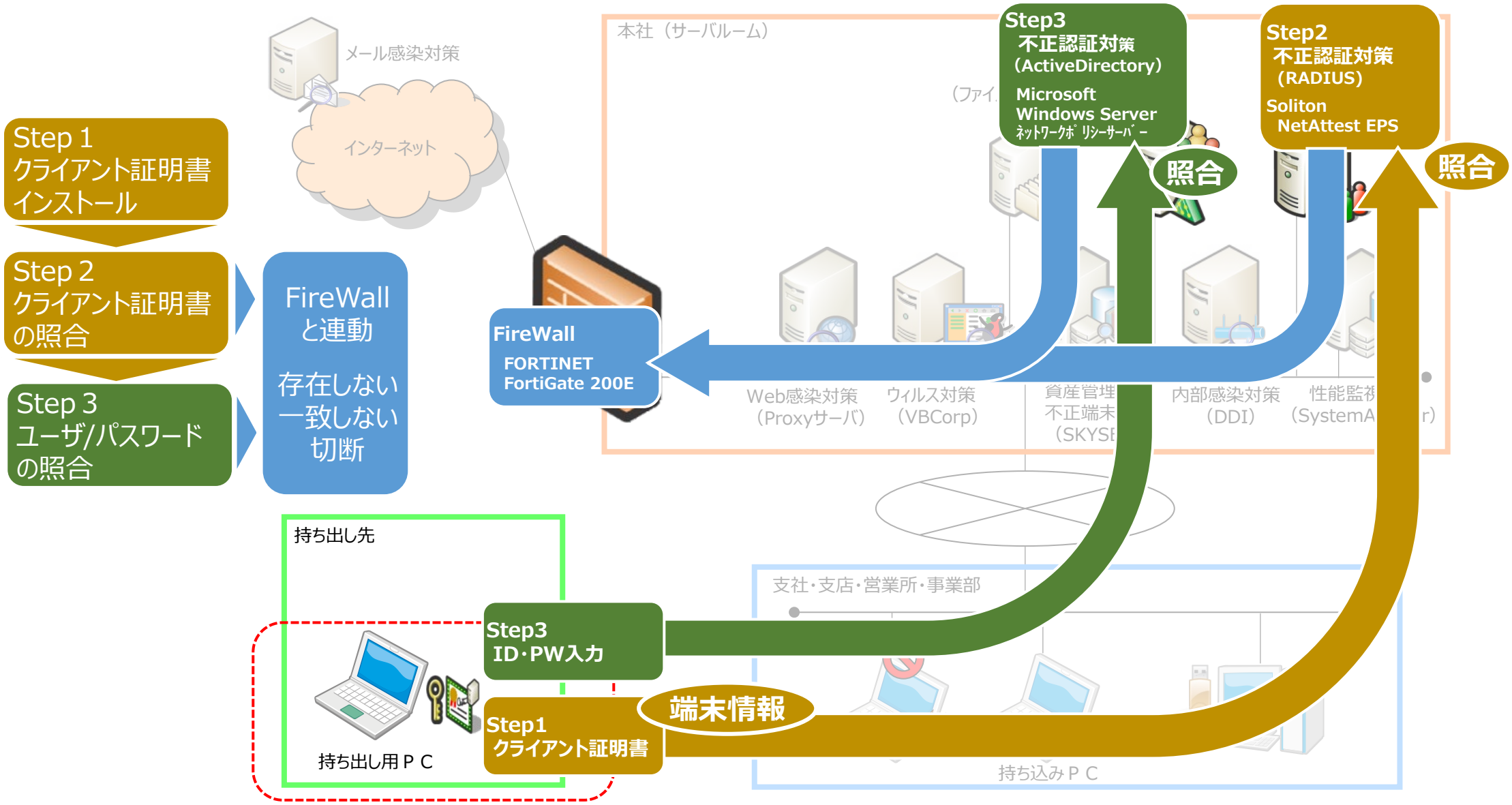


SKYSEA導入端末のみ通信を行わせる

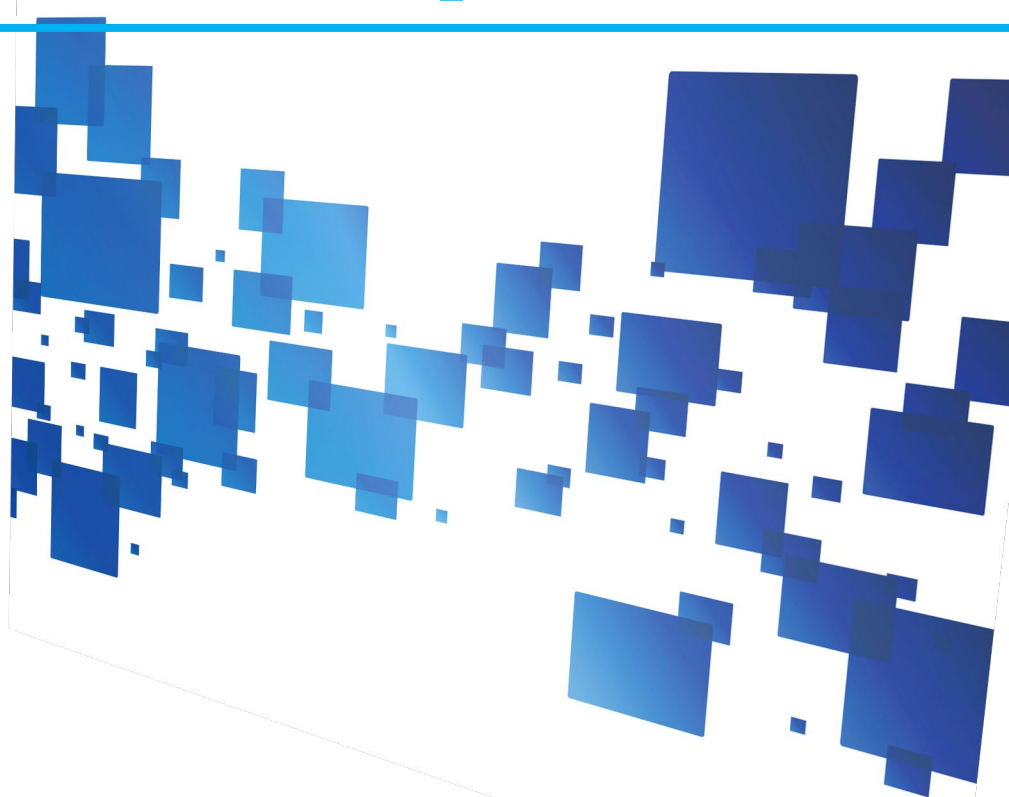
mms://live.nikkotelecom.co.jp/SuIREN事例紹介.wmv



社外からのアクセスを制御する



システムを安全に稼動するために
「可視化」による“予防”と“計画”



情報セキュリティとは…（総務省ホームページより）

“安全性” 情報の破壊・改ざん・消去されない

当社では、セキュリティソフト＋SDNで実現

“機密性” ある情報へ認められた人だけがアクセスできる

当社では、資産管理ソフト＋SDNで実現

それだけでなく

“可用性” 情報へのアクセスを認められた人が、
必要時に中断することなくアクセスできる

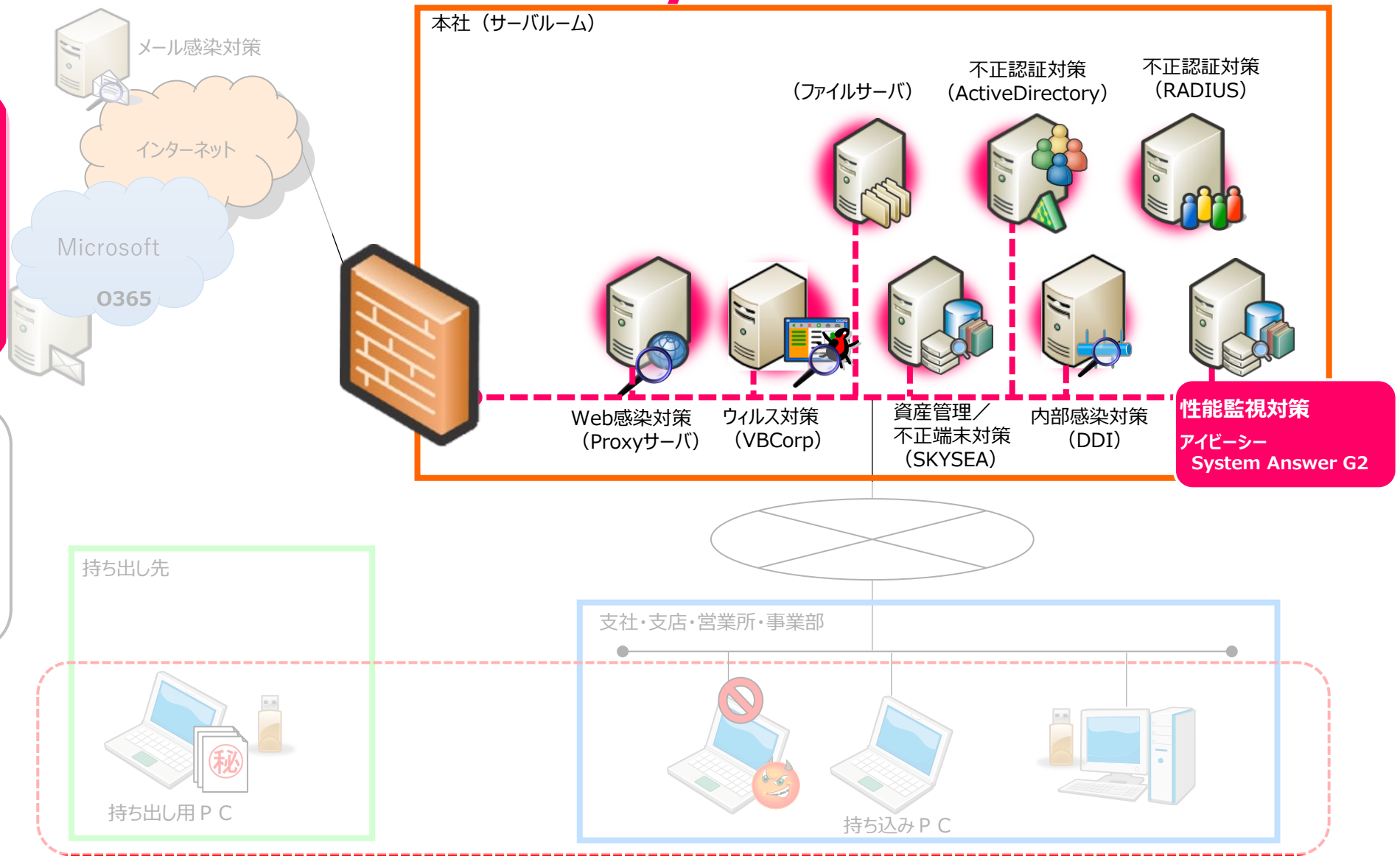
可用性を確保するための監視システム

System Answer

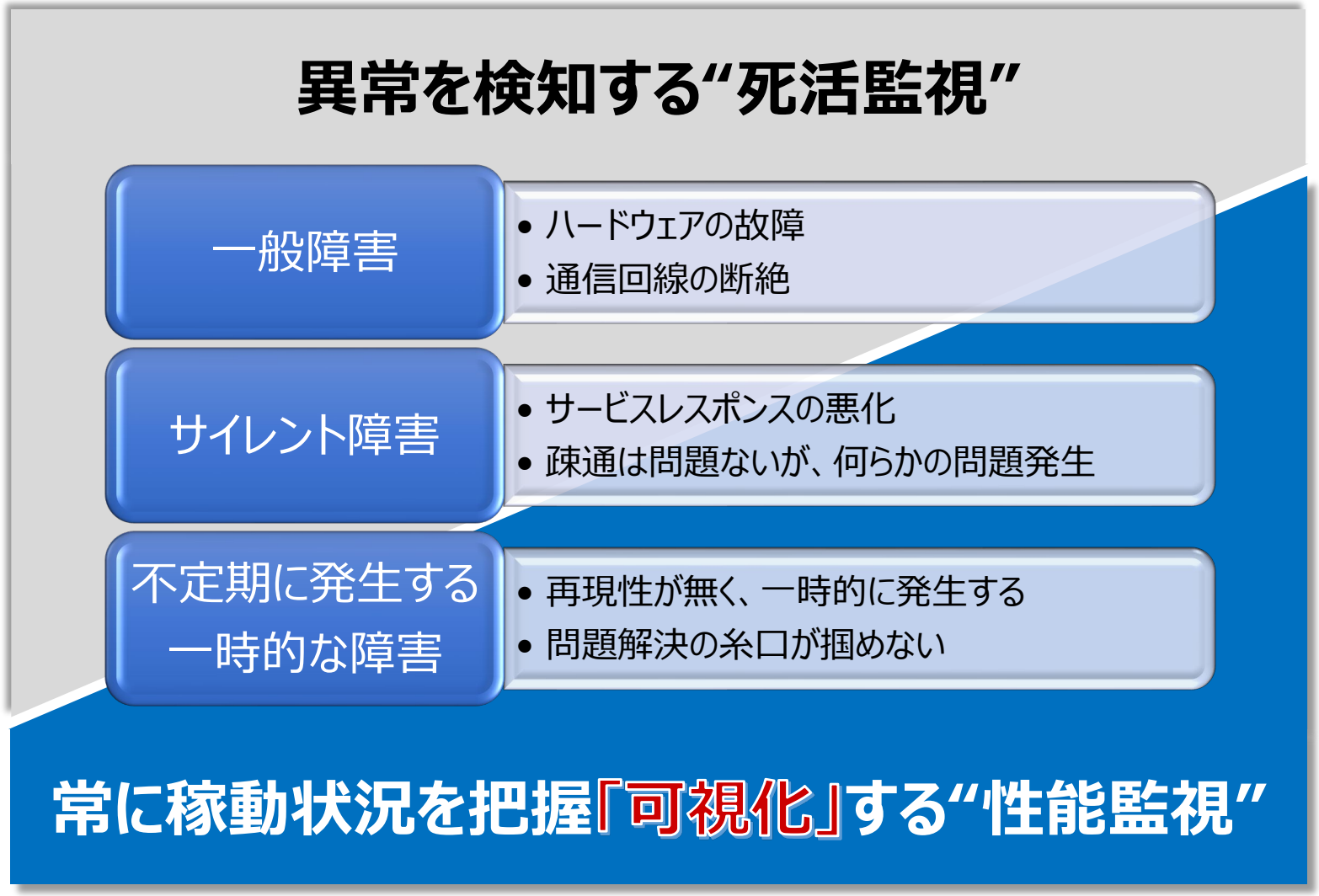
システムの
ネットワークと
サーバを監視し
閾値を越えると
ユーザ・管理者に
連絡

技術者による対応

次章
「未然に防ぐために」
～予知・予防～
で紹介



２つの監視機能



異常を検知

だけでなく

常に
稼動状態
を把握
「可視化」

「可視化」することで出来ること

予防保守　SystemAnserが正常値範囲を把握（ベースライン）

- 将来的に障害の原因となりうるウィークポイントを発見し、対策を打つこと（障害予兆の把握）
- システムダウンによる機会損失、顧客満足度低下などのリスクヘッジを実現する

守り

＋

キャパシティ計画　SystemAnserがトレンド分析

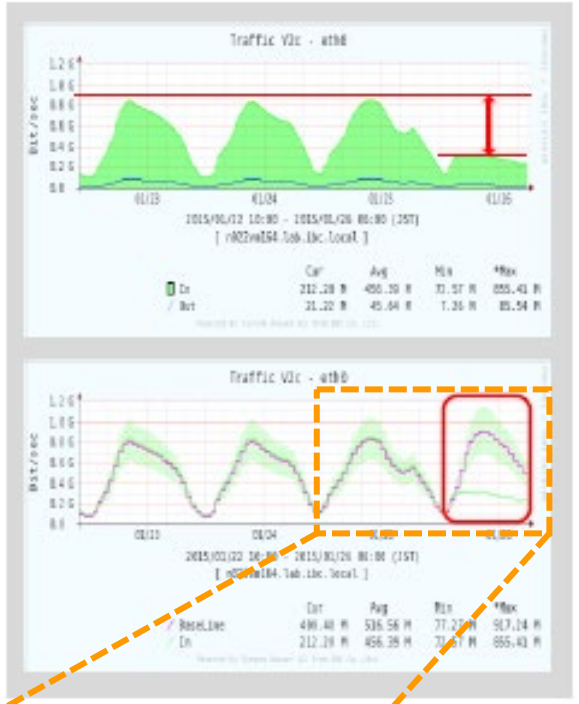
- 将来を見越したトレンド分析を定期的に実施し、システム投資の計画を策定
- 詳細情報を中・長期的に収集し、根拠となる情報を用いてキャパシティ計画を進め、最適なタイミングでの設備投資を実現する

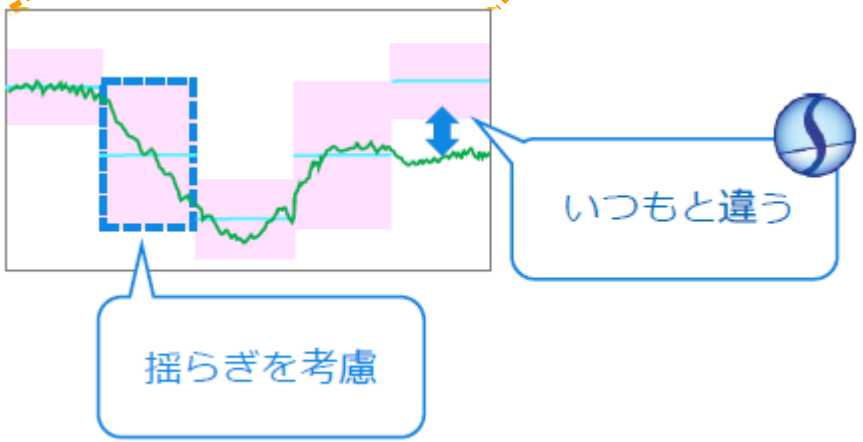
攻め

当社の予防保守

ベースライン

- 過去の稼働状況から時間別平均値、偏差値を自動学習し、稼動予測グラフを自動表示
- 予測から大きく逸脱した変化があった場合に、アラートとして通知



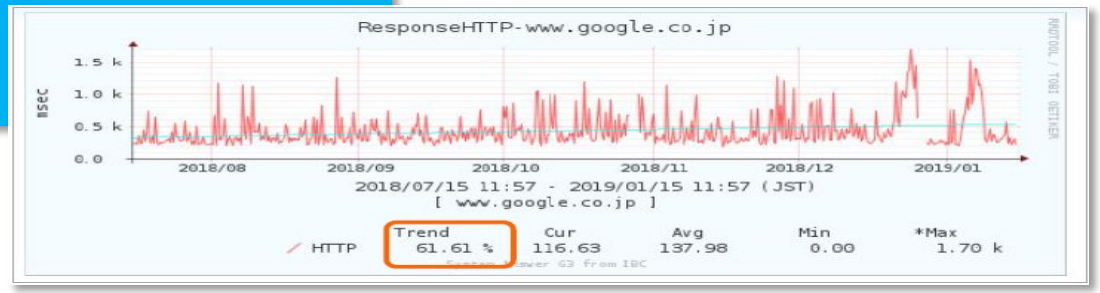


『いつもと違う』状態を検知し
障害発生前に障害対策

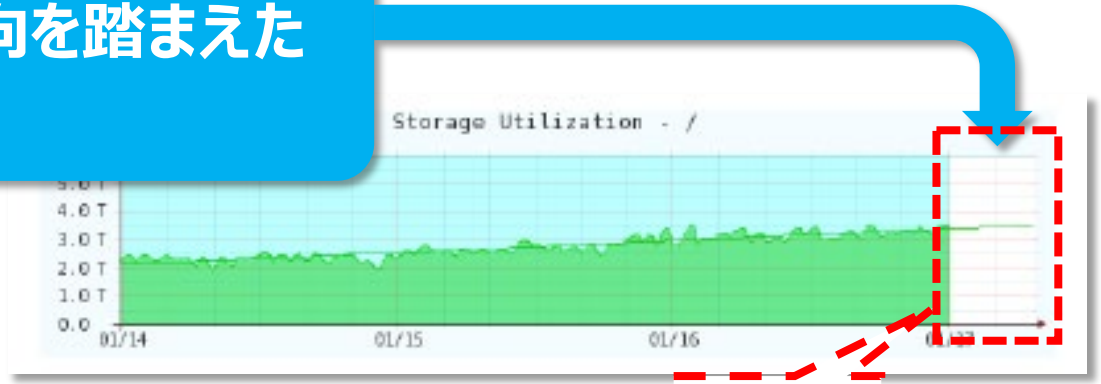
当社のキャパシティー計画

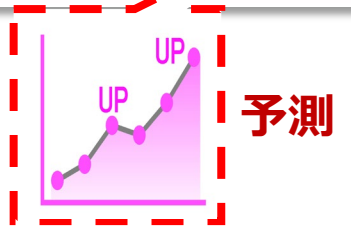
トレンドライン

- 指定期間における増加率や減少率を自動的に計算し表示
- グラフ上に傾向性を描画



- 指定期間に未来を設定することで、現在の傾向を踏まえた将来のキャパシティー予測を描画





投資計画の参考値として活用

ITセキュリティに関するご相談を承ります

安全性のご相談

●サイバー攻撃への対策

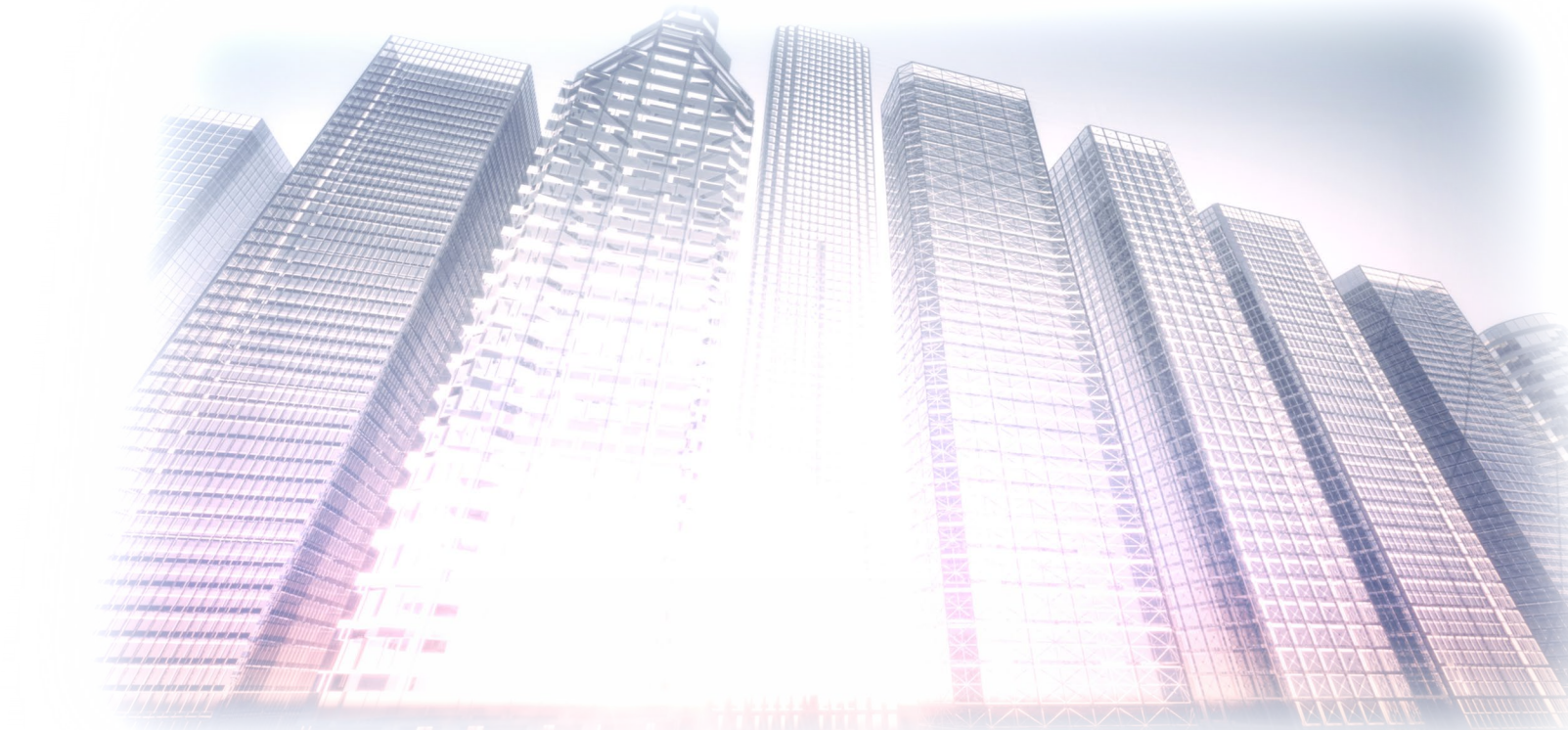
機密性のご相談

●不正アクセス・内部情報漏洩対策

可用性のご相談

●止まらないシステムの実現

“SuIREN”を支える
メーカー様からのエンドースコメント



NEC

日本電気株式会社

セキュリティ・ネットワーク事業部　事業部長

尹 秀薫様

NECが世界に先駆け製品化したSDNソリューションを、今回「SuIREN」にご採用いただきました。

日興通信様のシステム開発力・SI力と、NECのSDN技術力の連携を一層深めることで、お客様課題の解決、事業の拡大に貢献できるものと確信しています。

Allied Telesis

アライドテレシス株式会社

専務取締役　営業統括本部長　**佐藤 朝紀様**

アライドテレシスは、最先端の技術・製品・サービスと、最新のソリューションである「Net.AMF」を通じて日興通信様のネットワークを支援していくとともに、パートナーとしてお客様への提案、構築、運用などさまざまな面で積極的に協力してまいります。

トレンドマイクロ株式会社

上席執行役員 営業統括　大場 章弘様

SDN技術とトレンドマイクロのセキュリティ製品との連携ソリューションは、企業がサイバー攻撃を受けた際の迅速な初動対応と、被害拡大リスクの低減を実現します。

今回日興通信様に導入頂き、そのノウハウを今後より多くのお客様に提供されることを期待しています。

SKYSEA Client View

Ｓｋｙ株式会社

代表取締役　大浦　淳司様

多種多様なICT機器がインターネットに接続される昨今、その安全性を確保し、利用状況を適切に把握できなければ、活用を促進することはできません。

当社は日興通信様とともに、「働き方改革」に象徴される社会のニーズに対し、資産管理の観点から新たな利用シーンを提案してまいります。

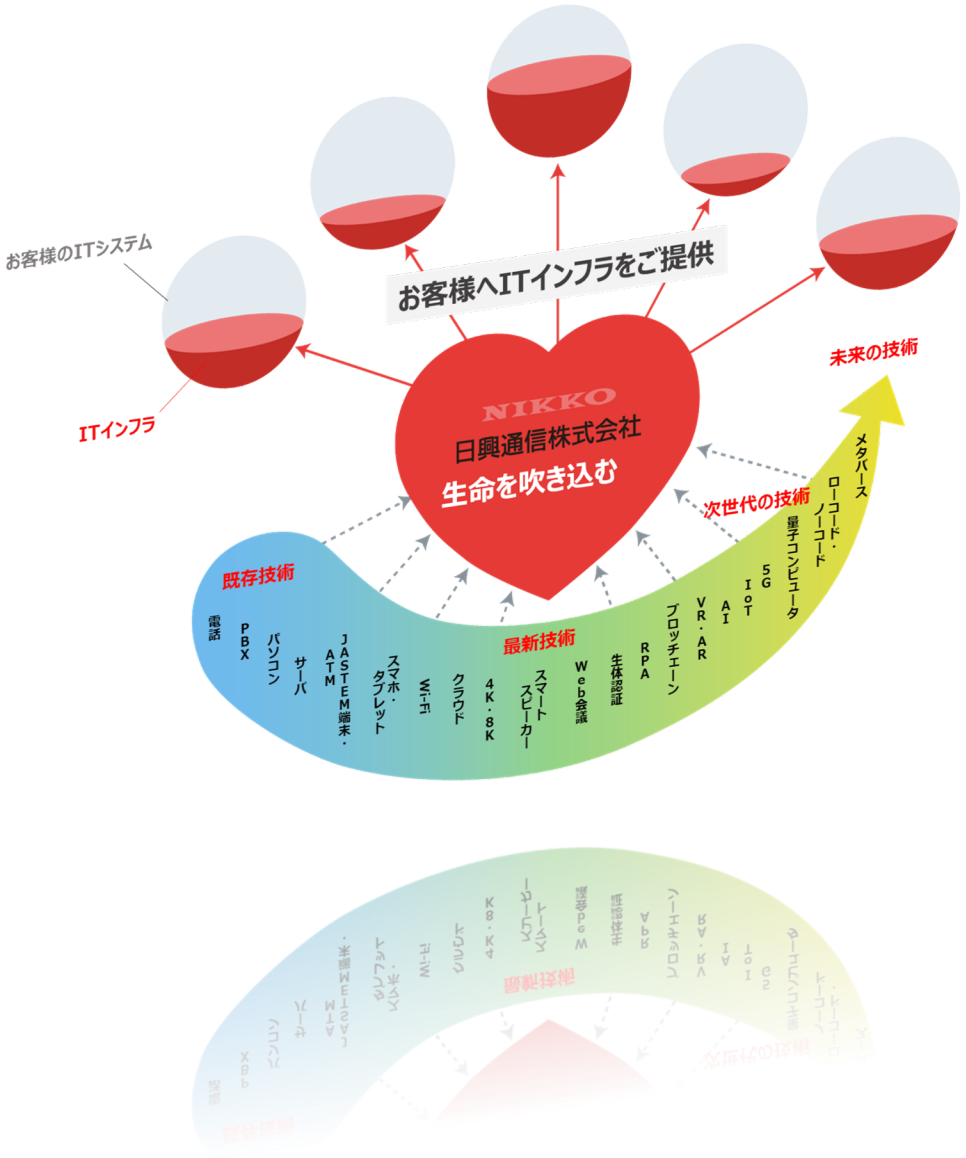
D-Link
Building Networks for People

ディーリンクジャパン株式会社

代表取締役社長　廖 晋新様

今回採用いただいたD-Linkのクラウド管理型の無線LANリューションは、お客様の導入・管理工数を大幅に削減可能なソリューションです。

NW構築経験が豊富な日興通信様をパートナーとして支援させていただき、お客様のより良いビジネス環境構築のため協力してまいります。



私たちはICT製品や技術に
利活用ノウハウで生命を吹き込み
お客様のITインフラを創造します

NIKKO 日興通信株式会社