再考、エンドポイントセキュリティ
～インシデント発生時に慌てないための要諦～

2019年11月7日（木）

株式会社インフォメーション・ディベロプメント
サイバー・セキュリティ・ソリューション部
エバンジェリスト　内山　史一

Profile

名前：
内山　史一（うちやま　ふみかず）

所属/役職：
株式会社インフォメーション・ディベロプメント
サイバー・セキュリティ・ソリューション部 / iD-SIRT / エバンジェリスト

主な略歴：
- 大手金融機関でNWインフラ管理やNW更改プロジェクトに参画
- セキュリティ企業で不正アクセス監視業務に従事
- 大手金融機関のCSIRT支援

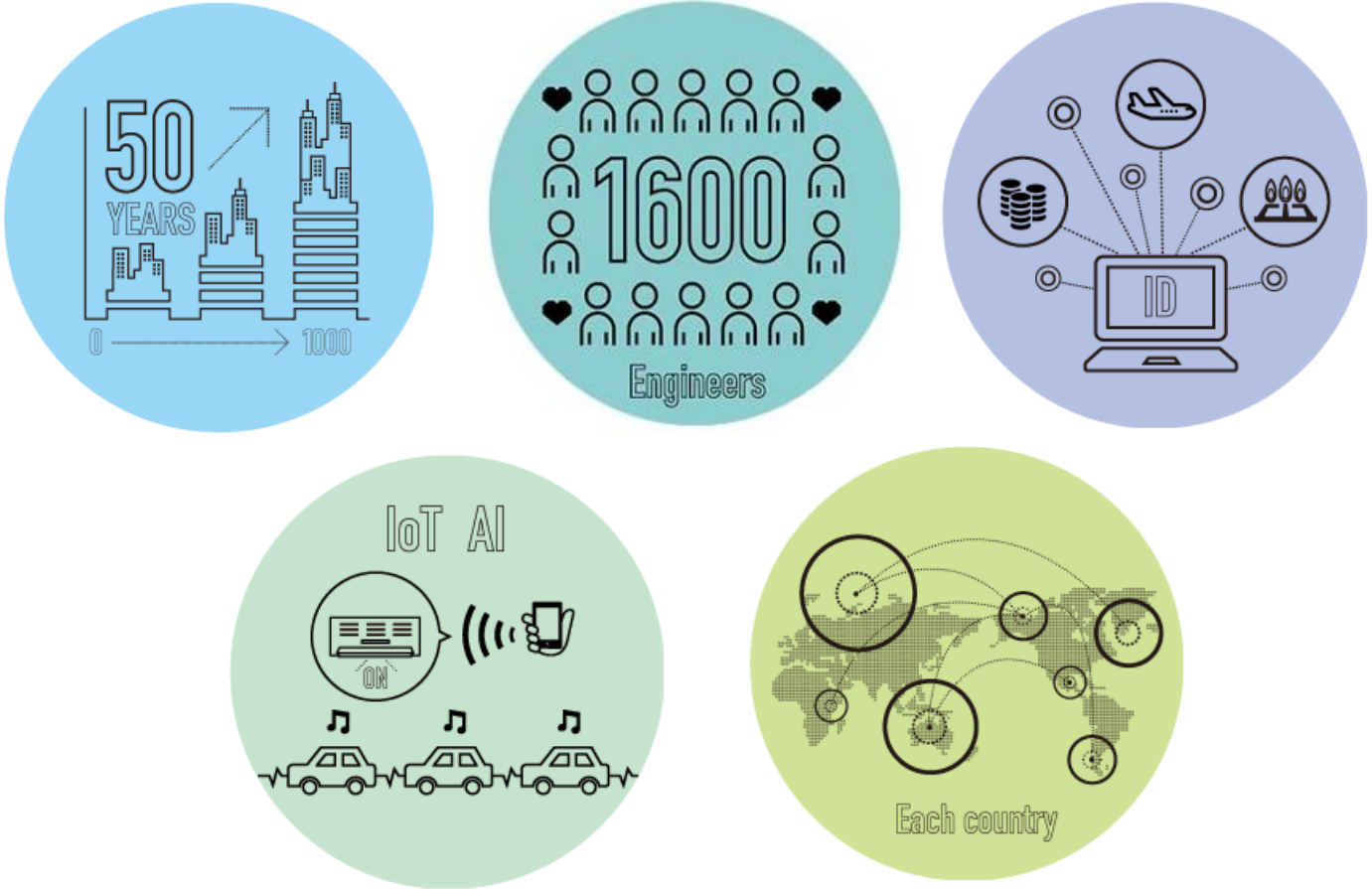
現在、当社のセキュリティサービス企画・インシデントレスポンスに従事

認定：
CISSP、PMP、情報処理技術者（ネットワーク、セキュリティ）

弊社ご紹介

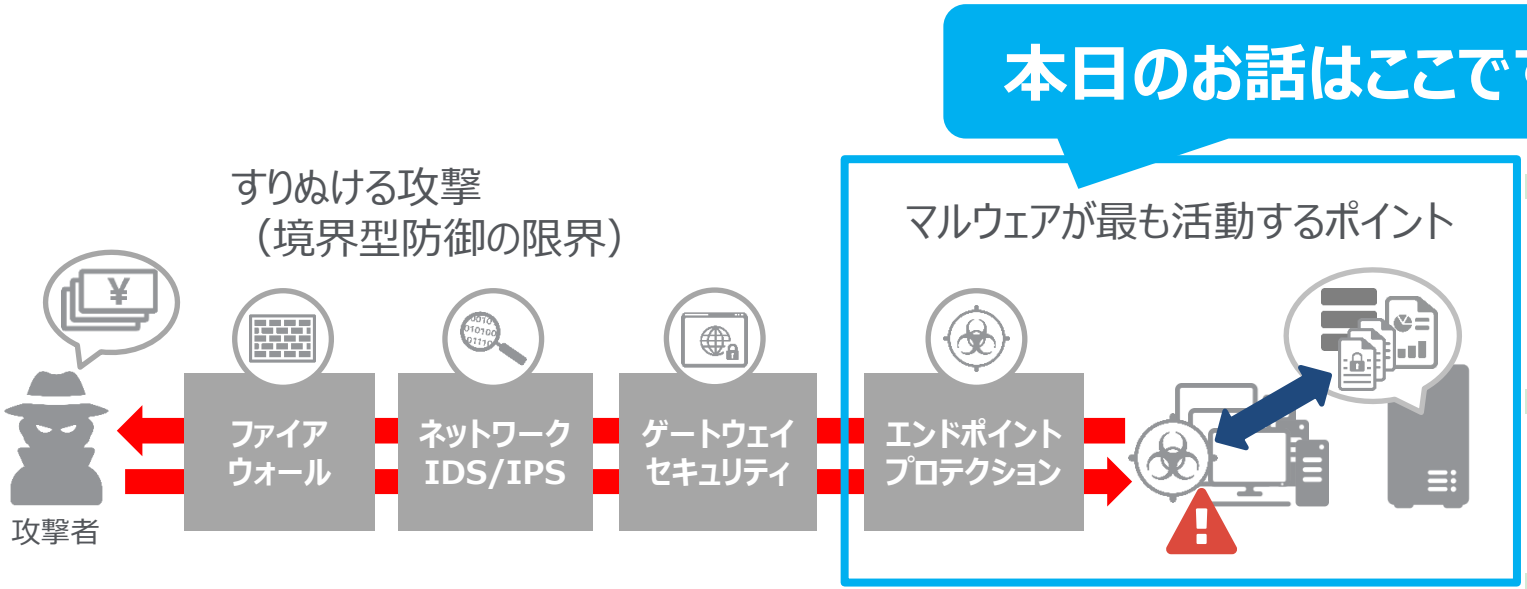
会社名	**株式会社インフォメーション・ディベロプメント**
本社所在地	東京都千代田区五番町12-1 番町会館
設立	**2019年 4月1日（IDホールディングス　1969年10月20日）**
代表者	代表取締役社長　山川 利雄
資本金	4億円（2019年4月1日現在）
従業員数	1,752名（2019年3月31日現在）
上場	株式会社IDホールディングス（持株会社） 東京証券取引所　市場第一部　証券コード：4709

IDとは



Concept

エンドポイントセキュリティの再定義



Agenda

１．変わる、エンドポイントセキュリティの役割

２．なぜ？変化が求められるのか

３．セキュリティ担当者の心配事

４．有事に慌てないための勘所と備え

1．変わる、エンドポイントセキュリティの役割

2．なぜ？変化が求められるのか

3．セキュリティ担当者の心配事

4．有事に慌てないための勘所と備え

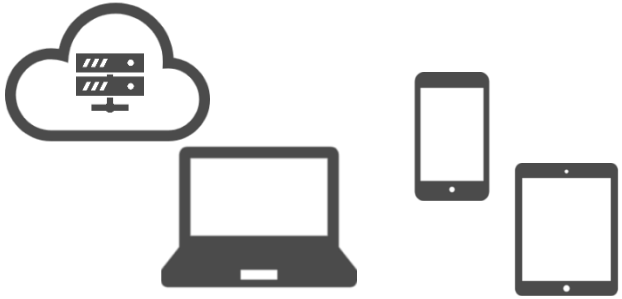
エンドポイントセキュリティのイメージ

- ✓ デバイスはPCやサーバ
- ✓ 基本的にデバイスは社内

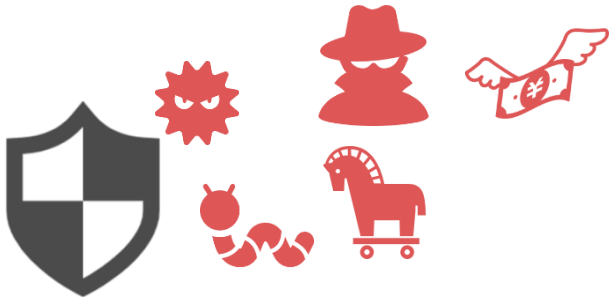
- ✓ 既知のマルウェア防御

エンドポイントセキュリティ＝ウイルス対策ソフト

変わる、エンドポイントセキュリティの役割

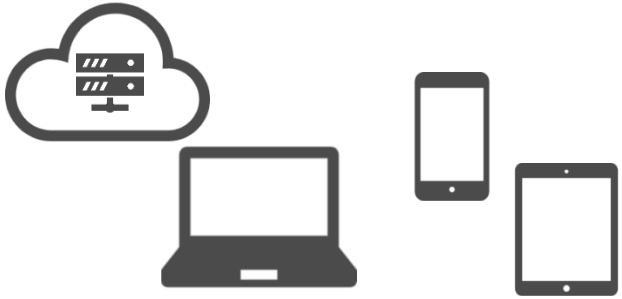


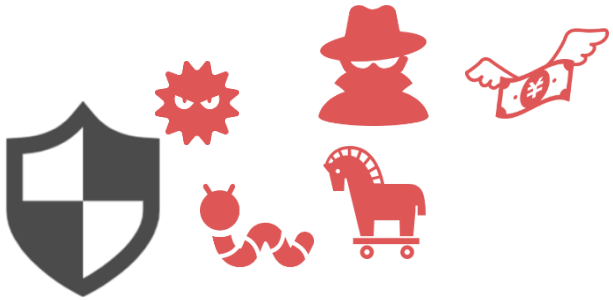
- ✓ 多様なデバイス
- ✓ 社外利用シーンの増加
- ✓ サーバは境界の外にも



- ✓ 既知のマルウェア防御
- ✓ 未知のマルウェア防御
- ✓ 不審な挙動や攻撃の防御
- ✓ 脆弱性攻撃の防御
- ✓ 資格情報の保護
- ✓ HDD暗号化の修復

変わる、エンドポイントセキュリティの役割





多様なデバイスと利用シーンをカバーする
多層化されたセキュリティ機能

- ✓ 脆弱性攻撃の防御
- ✓ 資格情報の保護
- ✓ HDD暗号化の修復

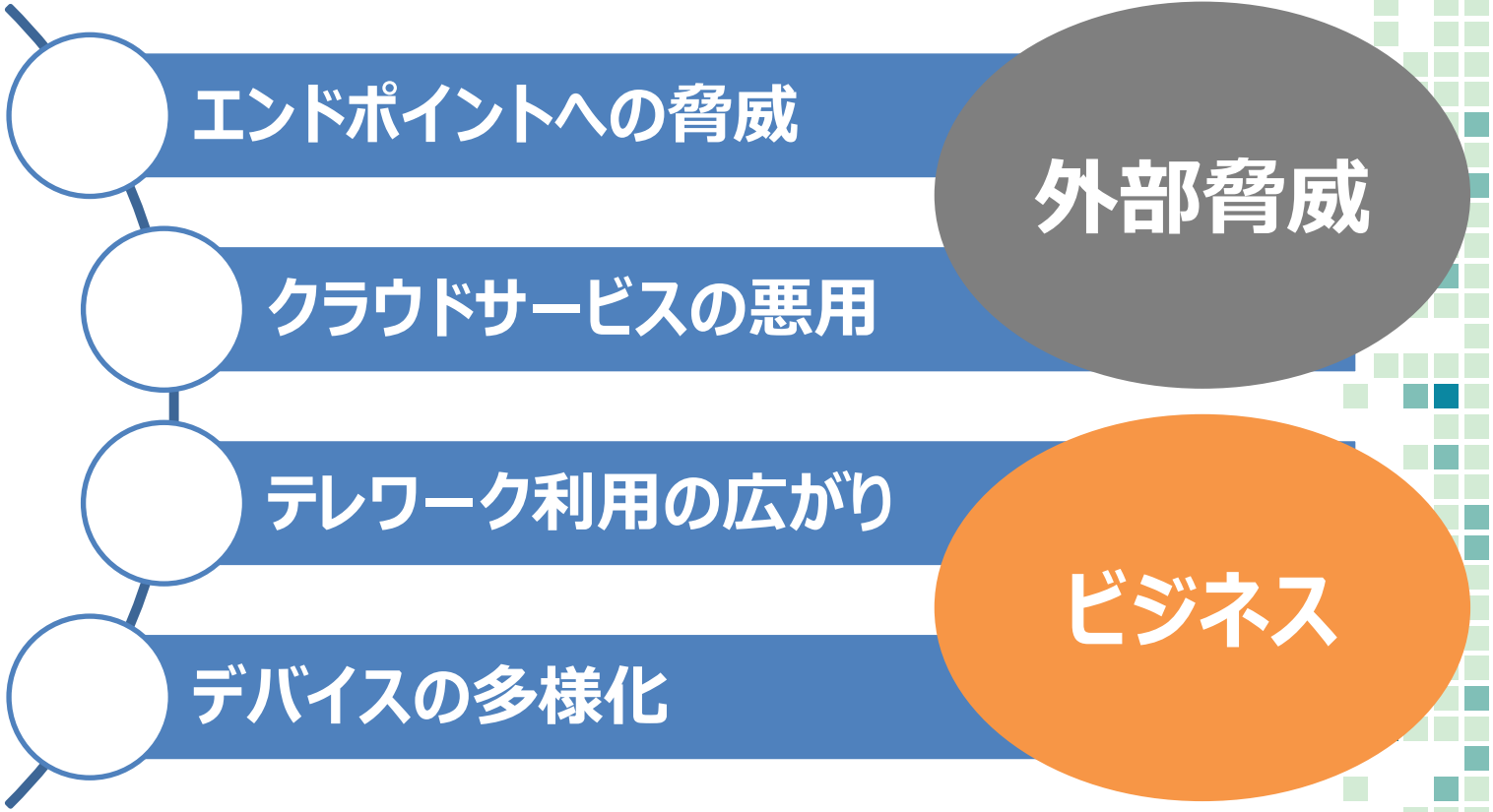
1．変わる、エンドポイントセキュリティの役割

2．なぜ？変化が求められるのか

3．セキュリティ担当者の心配事

4．有事に慌てないための勘所と備え

変化が求められる背景



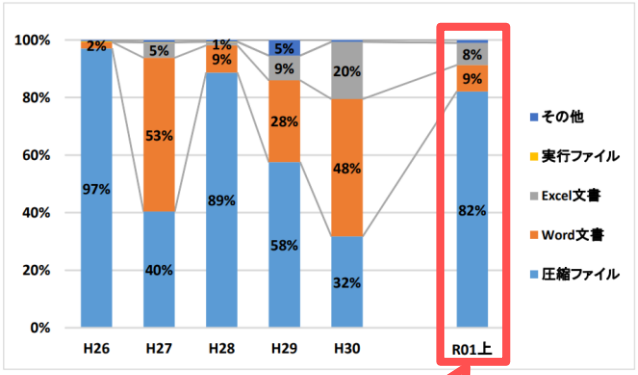
エンドポイントへの脅威 (1/3)

ばらまき型攻撃

高度標的型攻撃

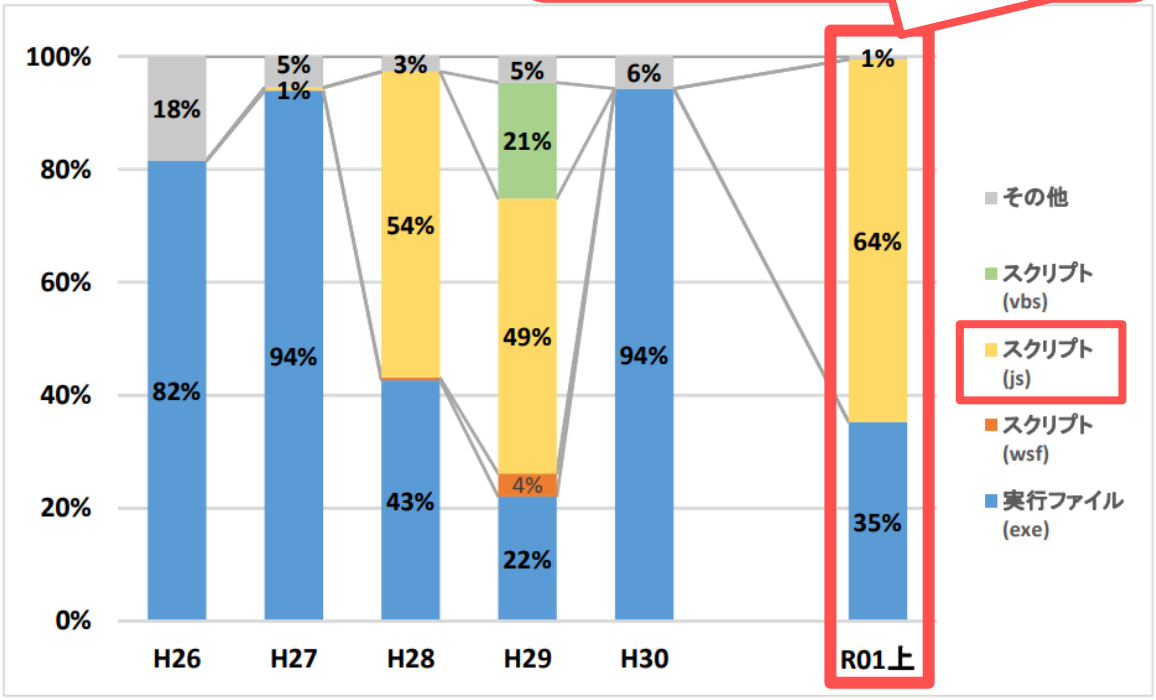
エンドポイントへの脅威 (2/3)

JavaScript を圧縮した添付ファイルが多い



添付ファイル形式は
圧縮ファイルが多数
前年32%→**82%**

添付の中身は.js
H29以来の**半数越えの64%**



出典：警察庁｜令和元年上半期におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R01_kami_cyber_jousei.pdf

エンドポイントへの脅威 (3/3)

従来型のウイルス対策では検知が難しい攻撃

July 8, 2019

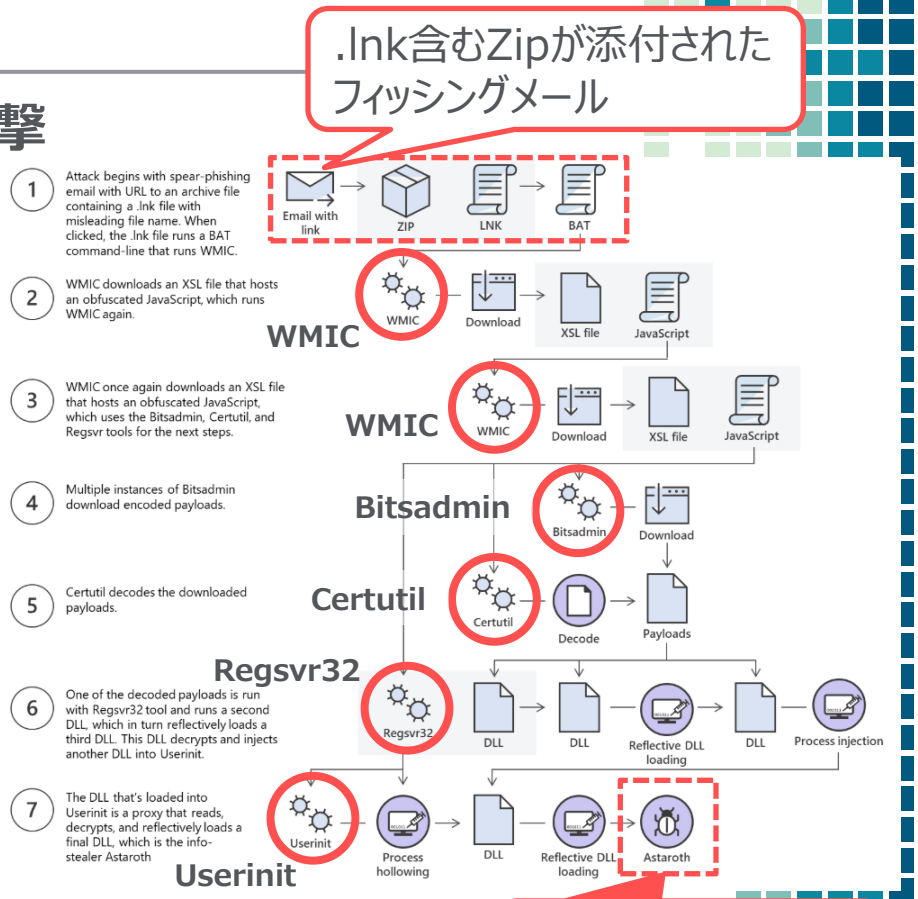
Dismantling a fileless campaign: Microsoft Defender ATP's Antivirus exposes Astaroth attack

Microsoft Defender ATP Research Team

Windowsの正規システムツールを悪用し、トロイの木馬「Astaroth」に感染させる

そこにあるもので攻撃を実行する

Living off the land（環境寄生）



出典：Microsoft | Dismantling a fileless campaign: Microsoft Defender ATP's Antivirus exposes Astaroth attack
https://www.microsoft.com/security/blog/2019/07/08/dismantling-a-fileless-campaign-microsoft-defender-atp-next-gen-protection-exposes-astaroth-attack/

クラウドサービスの悪用

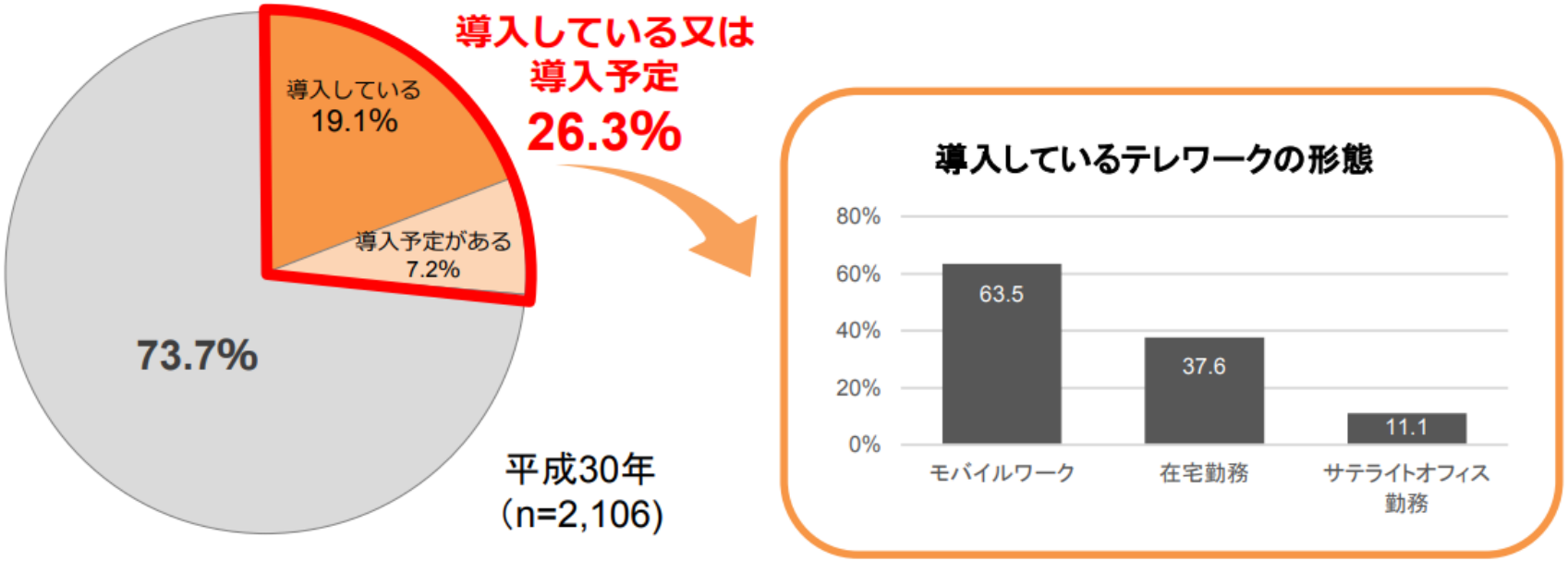
正規サービスを悪用し検知回避を狙う

出典：LAC｜DropboxをC2サーバとして悪用する、日本を狙った新たなマルウェアを確認
https://www.lac.co.jp/lacwatch/people/20180925_001704.html

AWSやGCPをC2サーバとして利用する攻撃も確認されている

テレワーク利用の広がり (1/2)

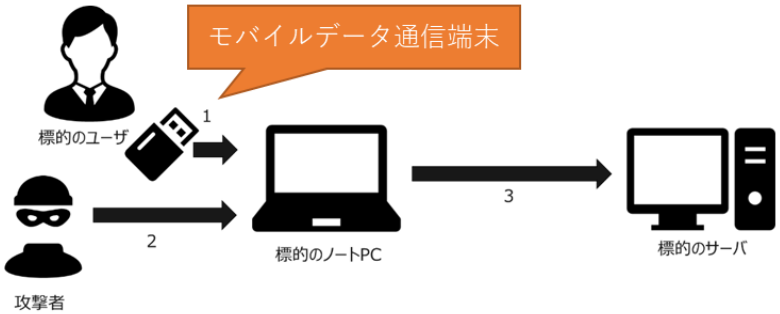
テレワークの導入状況（企業）



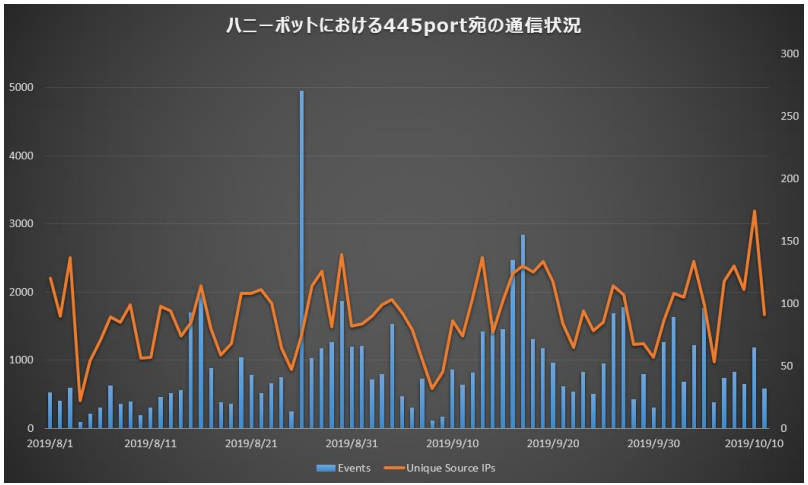
出典：総務省｜平成30年通信利用動向調査の結果
http://www.soumu.go.jp/johotsusintokei/statistics/data/190531_1.pdf

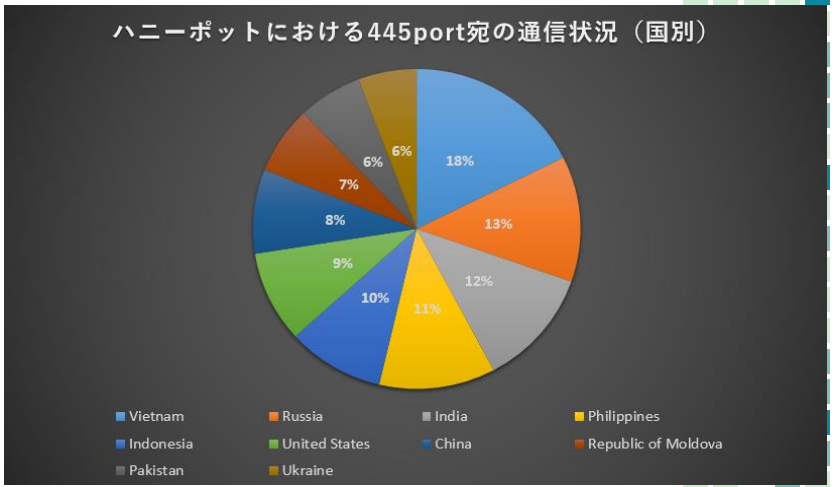
テレワーク利用の広がり (2/2)

モバイル端末のマルウェア感染



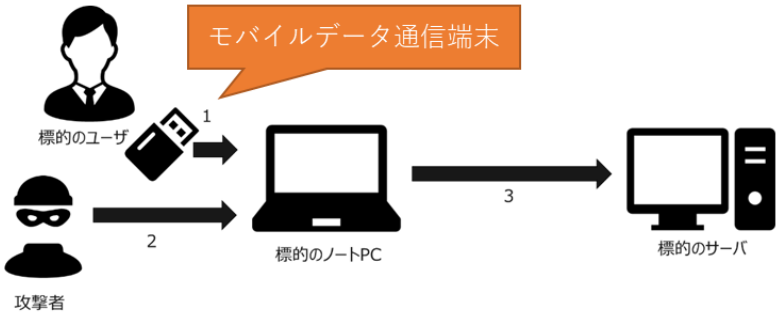
出典：Secureworks｜日本国内でモバイルデータ通信端末経由のマルウェア感染事案が増加
https://www.secureworks.jp/resources/at-portable-connection-devices-spreading-malware



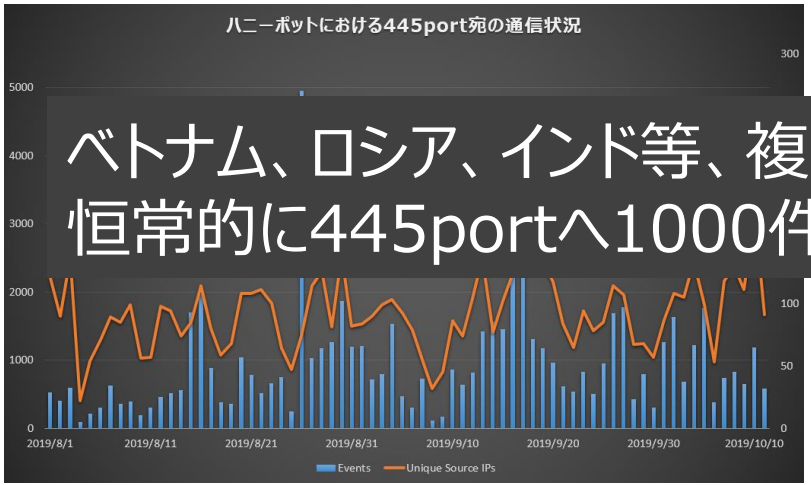


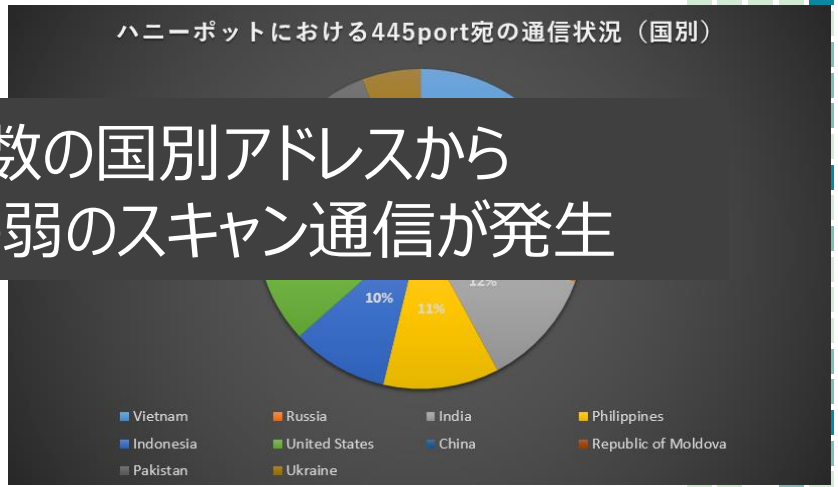
テレワーク利用の広がり (2/2)

モバイル端末のマルウェア感染



出典：Secureworks｜日本国内でモバイルデータ通信端末経由のマルウェア感染事案が増加
https://www.secureworks.jp/resources/at-portable-connection-devices-spreading-malware

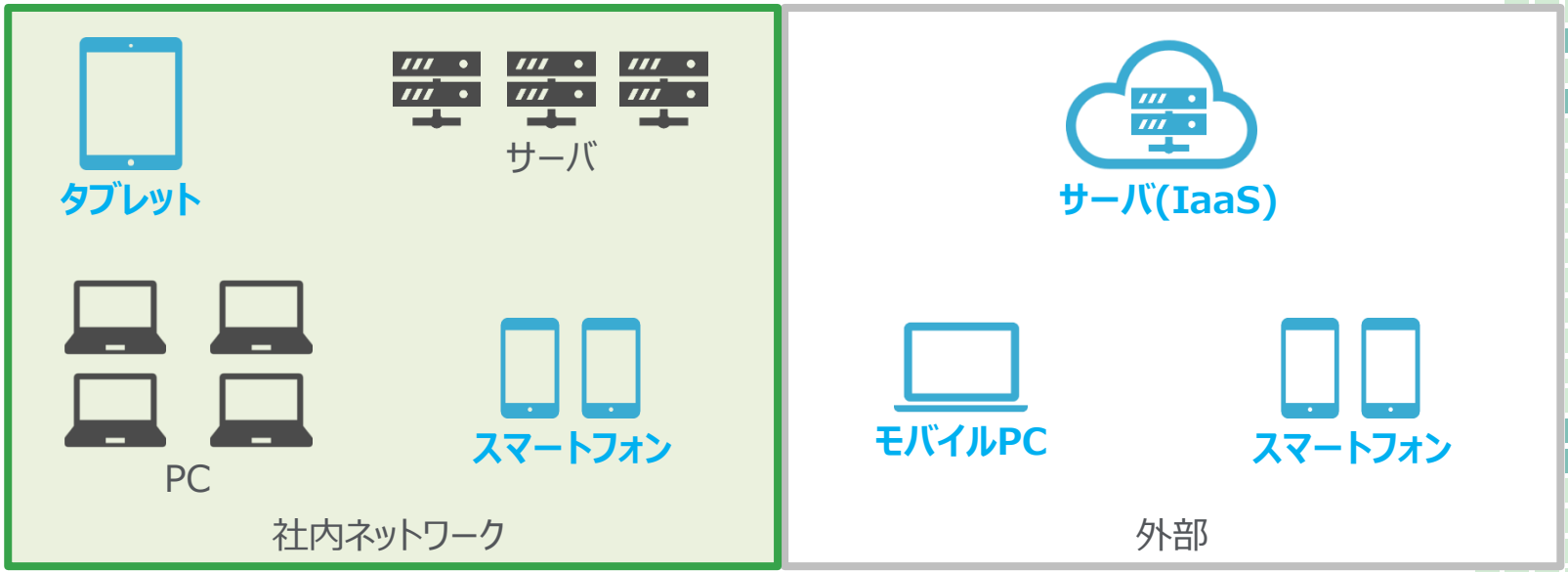




ベトナム、ロシア、インド等、複数の国別アドレスから
恒常的に445portへ1000件弱のスキャン通信が発生

デバイスの多様化

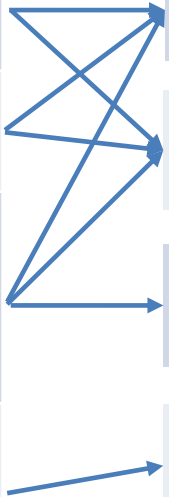
ネットワークに接続するデバイスの増加



攻撃対象可能な領域が拡大

エンドポイントセキュリティも変わらなくてはならない

背景	自組織における懸念事項
エンドポイントへの脅威	✓ Windowsの**正規管理ツールを使った**攻撃の発生
クラウドサービスの悪用	✓ **パブリッククラウドサービスを悪用**した攻撃の発生
テレワーク利用の広がり	✓ 社内NW接続時と比較して**相対的にセキュリティレベルが低い環境**での利用 ✓ **監視していないモバイル端末**がマルウェア感染
デバイスの多様化	✓ NW接続デバイスが増加し、**攻撃対象可能な領域が拡大** ✓ セキュリティ対応組織の**守る範囲が拡大**



想定されるリスク

- 攻撃に気づきにくい
- 感染後の迅速な対応ができない
- 感染端末の社内NW接続
- セキュリティ対応組織の負荷増大

エンドポイントセキュリティも環境変化に対応しなくてはならない

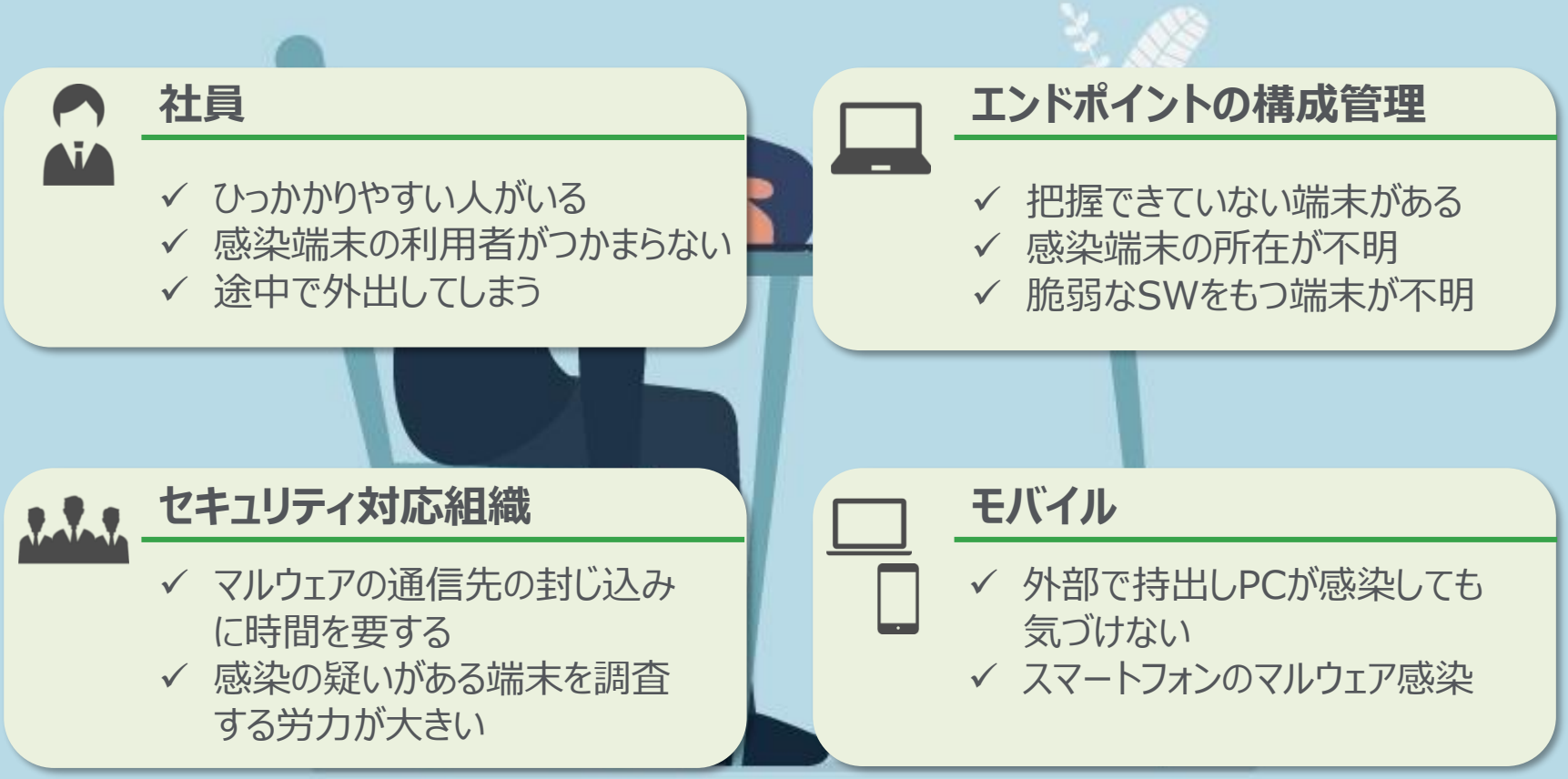
1．変わる、エンドポイントセキュリティの役割

2．なぜ？変化が求められるのか

3．セキュリティ担当者の心配事

4．有事に慌てないための勘所と備え

セキュリティ担当者の心配事



社員

- ✓ ひっかかりやすい人がいる
- ✓ 感染端末の利用者がつかまらない
- ✓ 途中で外出してしまう

エンドポイントの構成管理

- ✓ 把握できていない端末がある
- ✓ 感染端末の所在が不明
- ✓ 脆弱なSWをもつ端末が不明

セキュリティ対応組織

- ✓ マルウェアの通信先の封じ込みに時間を要する
- ✓ 感染の疑いがある端末を調査する労力が大きい

モバイル

- ✓ 外部で持出しPCが感染しても気づけない
- ✓ スマートフォンのマルウェア感染

心配事はつきないが・・・これは避けたい

✓進行中の攻撃に気づけない

✓マルウェア感染のアウトブレーク

１．変わる、エンドポイントセキュリティの役割

２．なぜ？変化が求められるのか

３．セキュリティ担当者の心配事

４．有事に慌てないための勘所と備え

基本が一番大事

✓守るものは何か

✓脅威は何か

✓どのように検知・対応するか

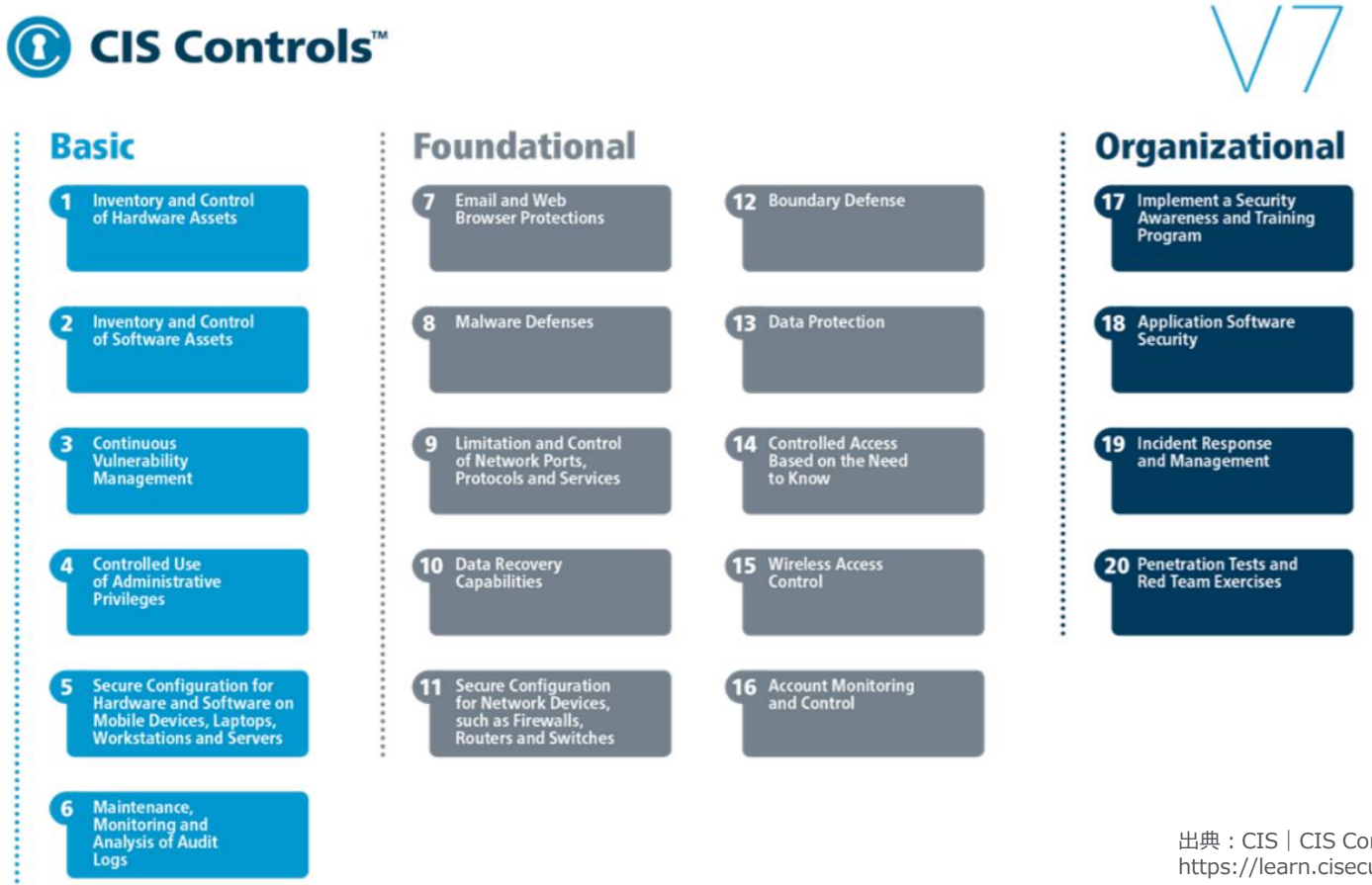
ガイドラインからのアプローチ (1/4)

- ✓ サイバーセキュリティ経営ガイドライン
- ✓ NIST Cybersecurity Framework
- ✓ ISMS（ISO/IEC27001、27002）

✓CIS Controls

- 米国の公的機関やセキュリティ企業等が共同開発した、NIST CSF やISMSに並び**グローバルで普及するフレームワーク**
- サイバー攻撃対策にフォーカスし、**具体的な技術対策**が示されている

ガイドラインからのアプローチ (2/4)



出典：CIS｜CIS Controls V7
https://learn.cisecurity.org/control-download

ガイドラインからのアプローチ (2/4)

CIS Controls™ V7

①ハードウェア資産のインベントリとコントロール

②ソフトウェア資産のインベントリとコントロール

③継続的な脆弱性管理

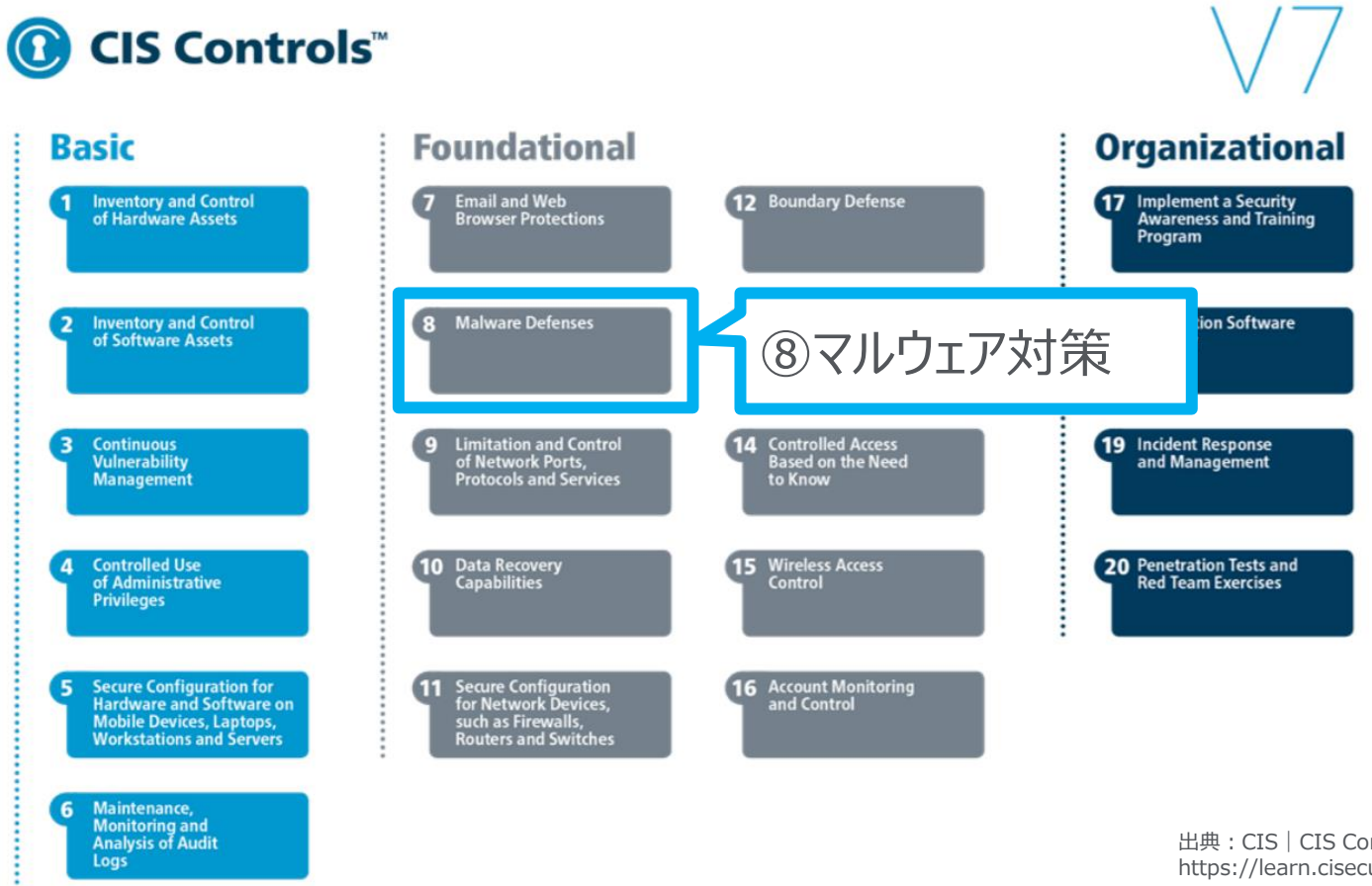
④管理権限のコントロールされた使用

⑤モバイルデバイス、ラップトップ、ワークステーションおよびサーバに関するハードウェアおよびソフトウェアのセキュアな設定

⑥監査ログの保守、監視および分析

出典：CIS｜CIS Controls V7
https://learn.cisecurity.org/control-download

ガイドラインからのアプローチ (3/4)



出典：CIS｜CIS Controls V7
https://learn.cisecurity.org/control-download

ガイドラインからのアプローチ (4/4)

CIS Control 8 : マルウェア対策

ｻﾌﾞｺﾝﾄﾛｰﾙ	ｺﾝﾄﾛｰﾙﾀｲﾌﾟ
8.1	**集中管理**されたアンチマルウェアソフトウェアを活用する
8.2	アンチマルウェアとシグネチャが**更新されている**ことを確認する
8.3	オペレーティングシステムの**悪用防止機能**を有効にする／**悪用防止技術**を適用する
8.4	取り外し可能な**メディアのアンチマルウェアスキャン**を構成する
8.5	デバイスがコンテンツを**自動実行しない**ように設定する
8.6	アンチマルウェアロギングを**集中管理**する
8.7	**DNSクエリ**のロギングを有効にする
8.8	**コマンドライン監査**ロギングを有効にする

出典：CIS｜CIS Controls V7
https://learn.cisecurity.org/control-download

ガイドラインからのアプローチ (4/4)

CIS Control 8 : マルウェア対策

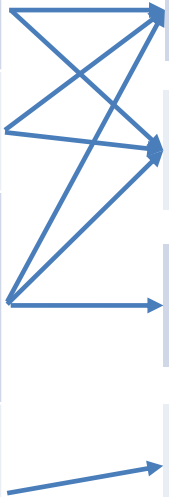
ｻﾌﾞｺﾝﾄﾛｰﾙ	ｺﾝﾄﾛｰﾙﾀｲﾌﾟ
8.1	集中管理されたアンチマルウェアソフトウェアを活用する
8.2	アンチマルウェアとシグネチャが更新されていることを確認する
8.3	オペレーティングシステムの悪用防止機能を有効にする／悪用防止技術を適用する
8.4	
8.5	
8.6	
8.7	DNSクエリの[illegible]を有効にする
8.8	コマンドライン監査ロギングを有効にする

攻撃者の「Living off the land (環境寄生)」に対し、ロギングはイベントの発生方法・内容・状況の把握を容易にする

出典：CIS｜CIS Controls V7
https://learn.cisecurity.org/control-download

エンドポイントセキュリティも変わらなくてはならない

背景	自組織における懸念事項
エンドポイントへの脅威	✓ Windowsの**正規管理ツールを使った**攻撃の発生
クラウドサービスの悪用	✓ **パブリッククラウドサービスを悪用**した攻撃の発生
テレワーク利用の広がり	✓ 社内NW接続時と比較して**相対的にセキュリティレベルが低い環境**での利用 ✓ **監視していないモバイル端末**がマルウェア感染
デバイスの多様化	✓ NW接続デバイスが増加し、**攻撃対象可能な領域が拡大** ✓ セキュリティ対応組織の**守る範囲が拡大**



想定されるリスク

- 攻撃に気づきにくい
- 感染後の迅速な対応ができない
- 感染端末の社内NW接続
- セキュリティ対応組織の負荷増大

エンドポイントセキュリティも環境変化に対応しなくてはならない

MVISION ePO

シンプルなクラウドベースの
SaaS管理サービス

MVISION Endpoint

統合された管理を備えた
Windows 10の高度な拡張防御機能

MVISION

MVISION EDR

強力な脅威の検出、調査、
および対応の簡素化

MVISION Mobile

他デバイスと同様、iOSと
Androidを集中管理し、防御

出典：McAfee

多層化された統合型セキュリティ

MVISION

MVISION Endpoint

機械学習
Fileless脅威の検知
データのロールバック
パスワード盗難防止

Endpoint Security

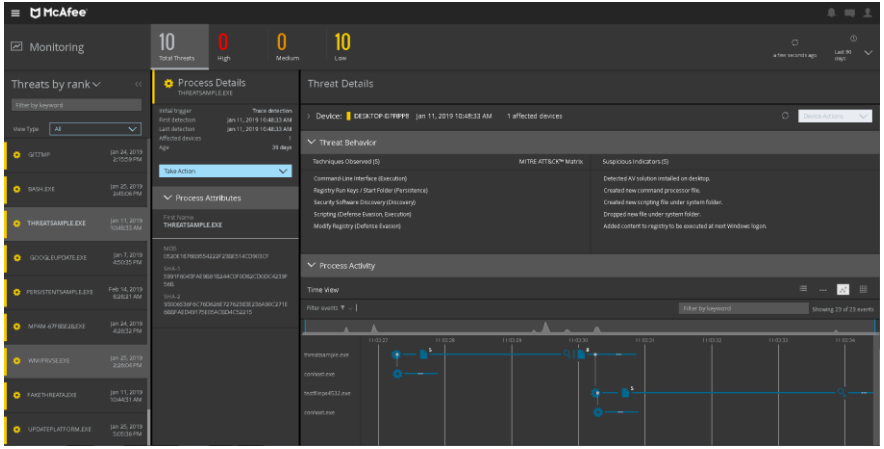
機械学習
アプリケーションの動的隔離
シグニチャベースの
マルウェア検知
ホストIPS
ファイアウォール
Webコントロール
スクリプトベースの
脅威保護(AMSI連携)

MVISION Mobile

機械学習
振る舞い分析
- Device Safety
- Network Safety
- App Safety

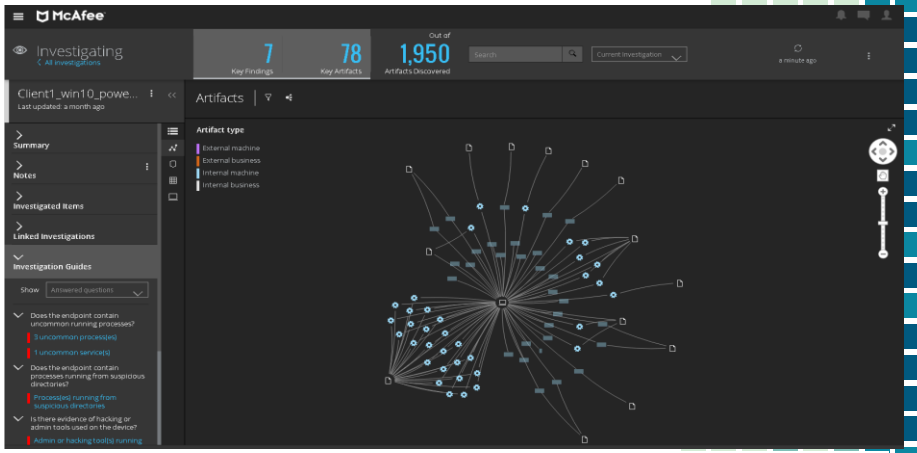
検知から恒久対応まで支援する MVISION EDR

EDR機能



- ✓ エンドポイントの動作を解析し脅威検知
- ✓ NW隔離、ファイル削除、プロセス停止等のレスポンス機能を提供
- ✓ マルウェアの挙動をタイムラインで可視化

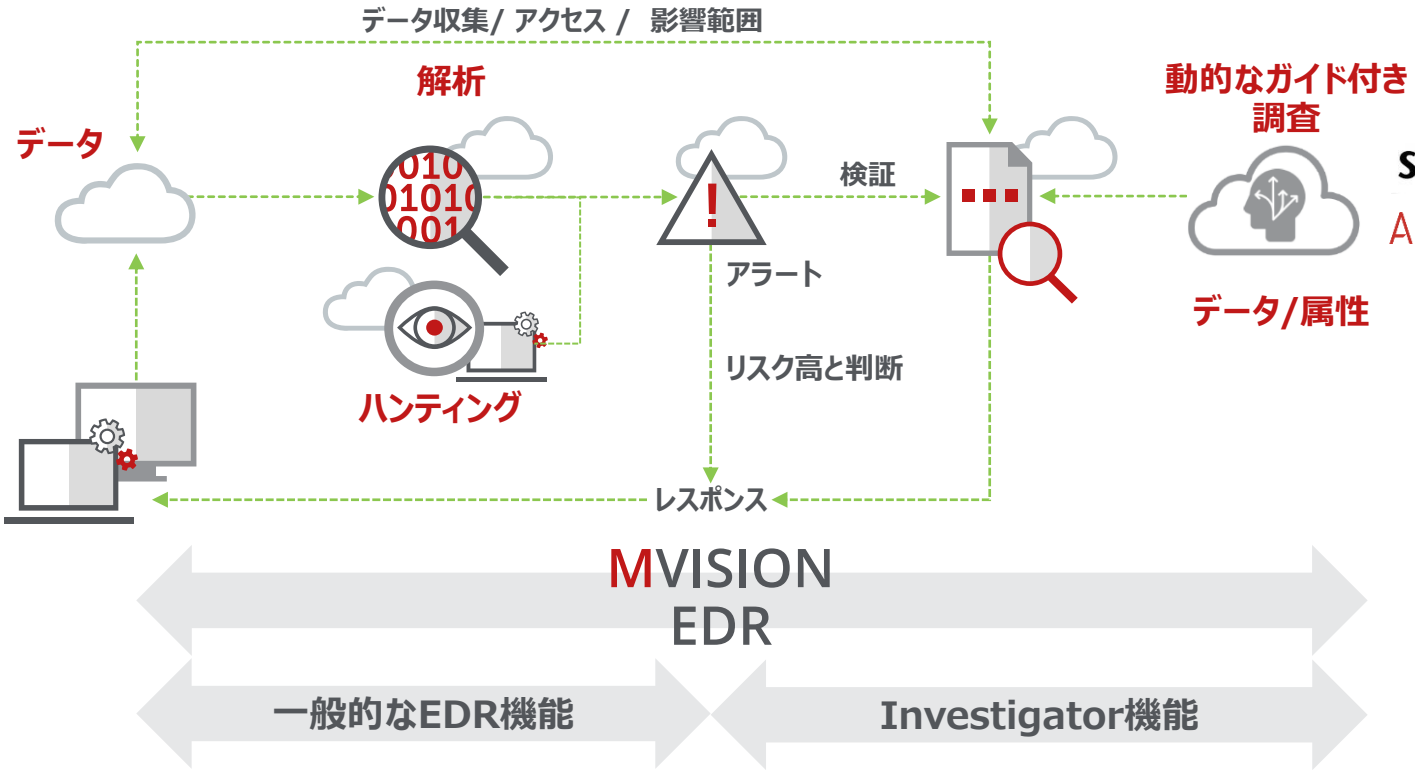
Investigator機能



- ✓ エンドポイントのスナップショットデータを基に更なる詳細な調査・解析が可能
- ✓ エキスパートガイド機能による分析作業の自動補助

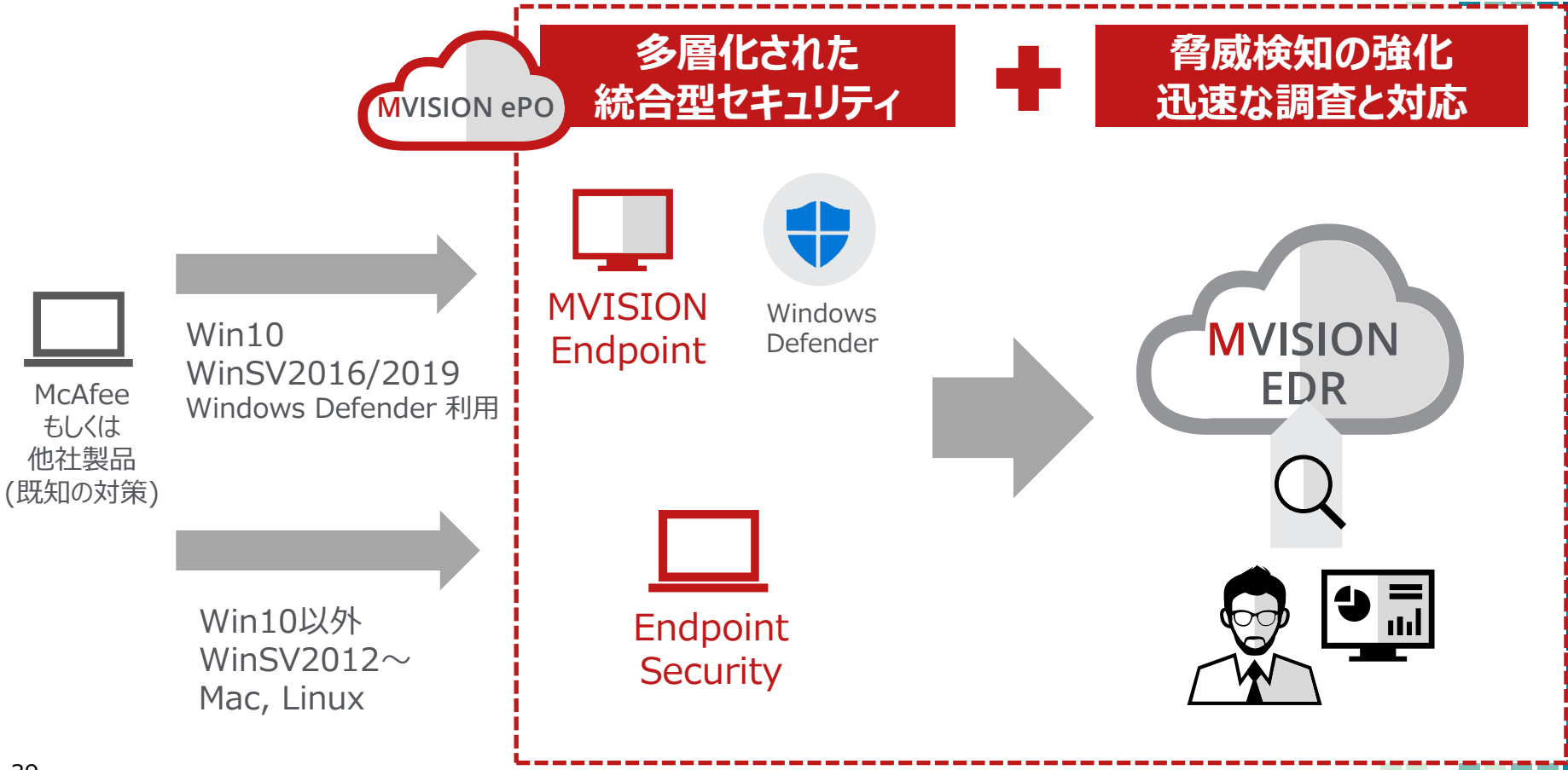
出典：McAfee

MVISION EDRにおけるレスポンスイメージ



出典：McAfee

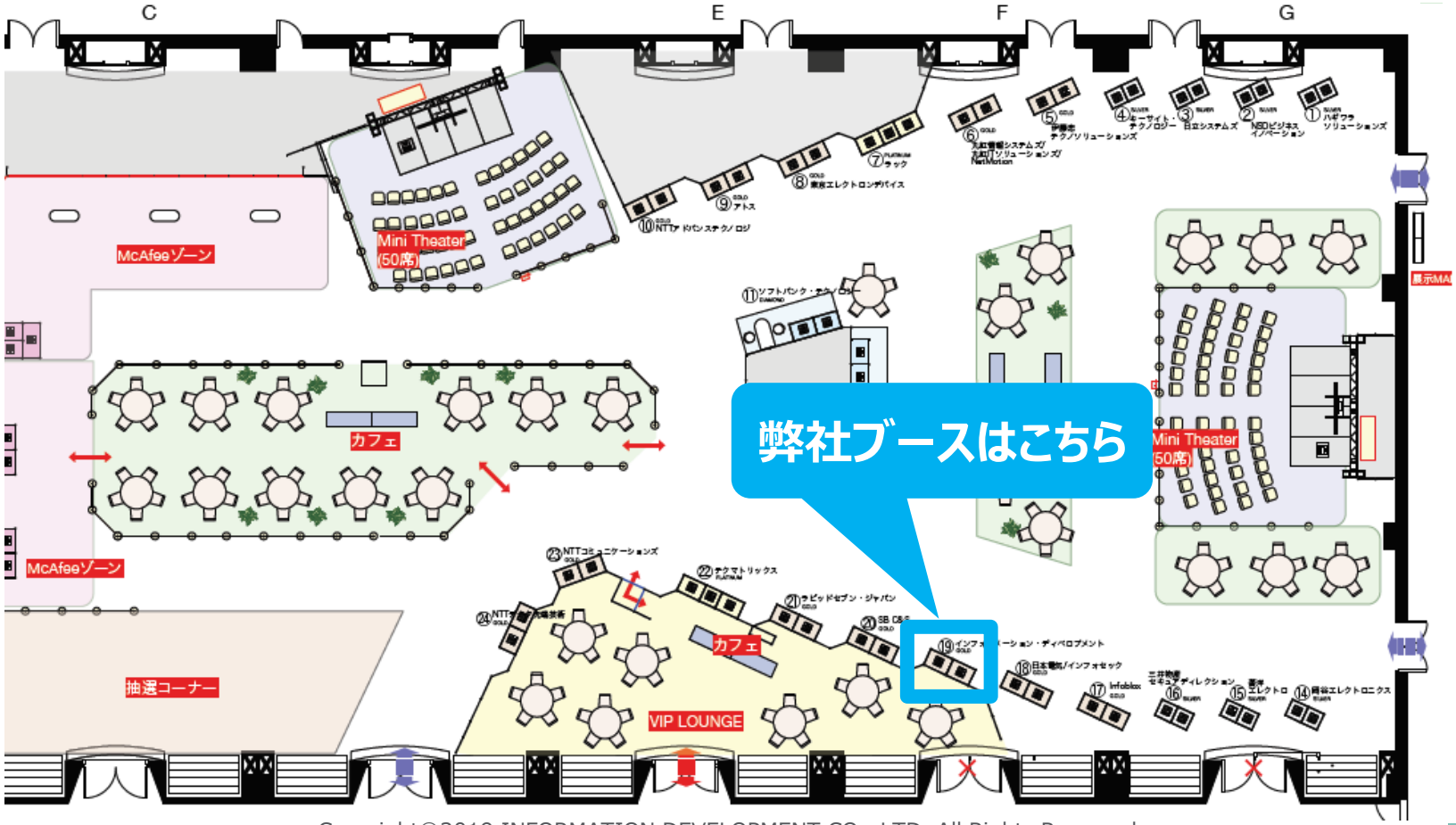
目指すべきエンドポイントセキュリティの姿



本日のまとめ

- ✓ エンドポイントセキュリティには、**多様なデバイスと利用シーン**をカバーする**多層化されたセキュリティ機能**が求められています。
- ✓ 変化が求められる背景には、**外部脅威**への対応と**ビジネス環境の変化**があります。
- ✓ 有事に備えるため、**構成管理等の基本コントロール**と**環境変化に対応したセキュリティ機能**の実装が重要です。

弊社ブースのご案内



ご清聴有難うございました