サイバーセキュリティをめぐる防衛モデルの最近の動向

東京電機大学　顧問・客員教授
佐々木良一
r.sasaki@mail.dendai.ac.jp

イントロダクション

自己紹介：**佐々木良一**　（東京電機大学客員教授）

1971年―2001年　日立製作所。1984年より情報セキュリティなどの研究に従事

2001年―2018年3月　東京電機大学未来科学部教授

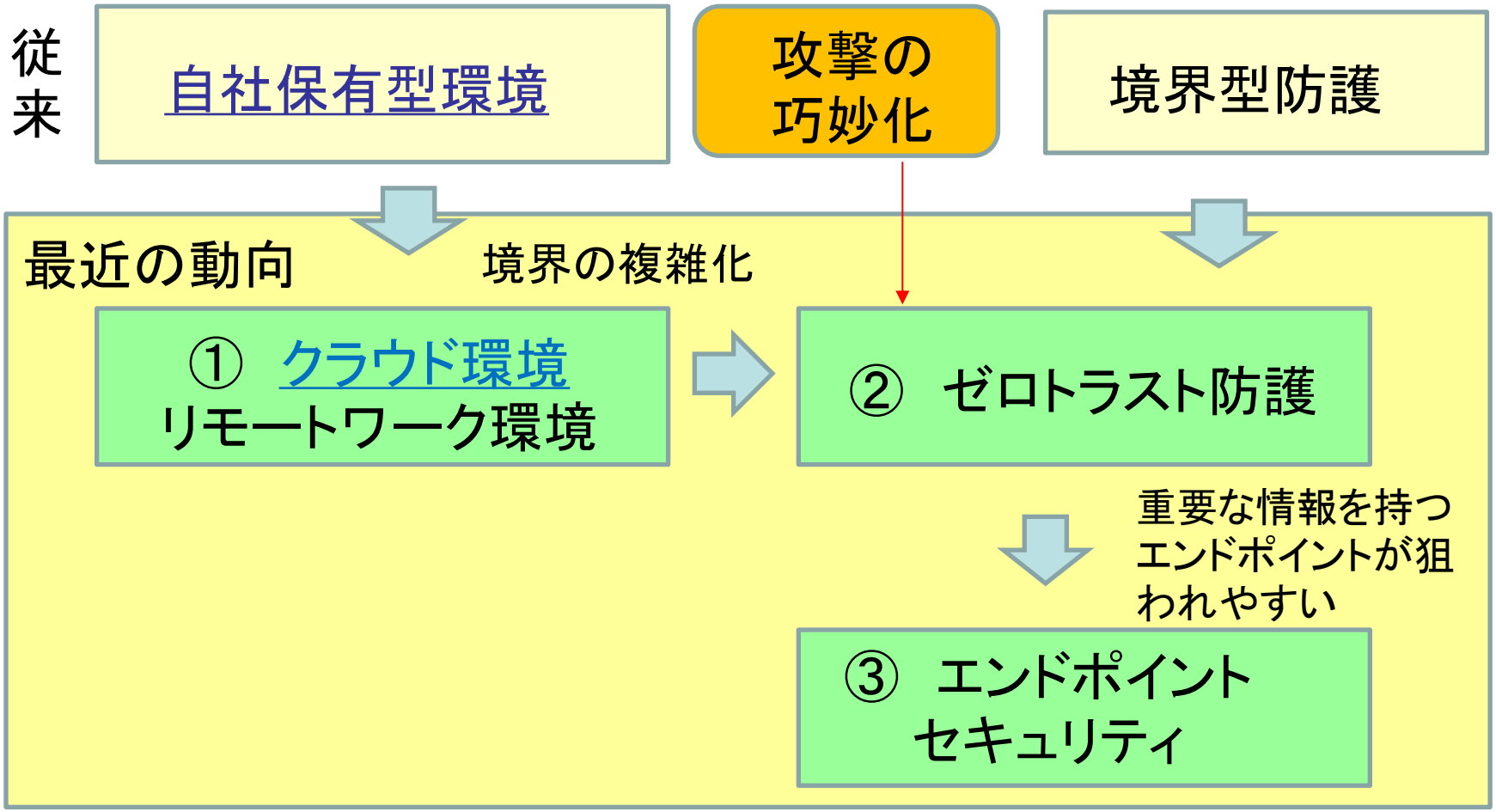
2018年―2020年3月　総合研究所　特命教授

サイバーセキュリティ研究所長

日本セキュリティマネジメント学会会長
デジタルフォレンジック研究会会長
内閣官房サイバーセキュリティ補佐官
などを歴任

目次

防護モデルの変化の相互関係

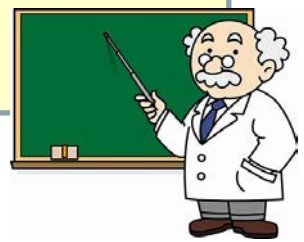


CDM: Continuous Diagnostics and Mitigation

クラウドコンピューティングとは

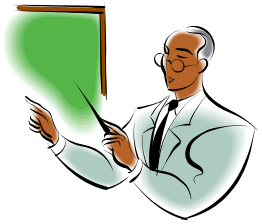
クラウドコンピューティング（英: cloud computing）は、インターネットなどのコンピュータネットワークを経由して、コンピュータ資源をサービスの形で提供する利用形態である。

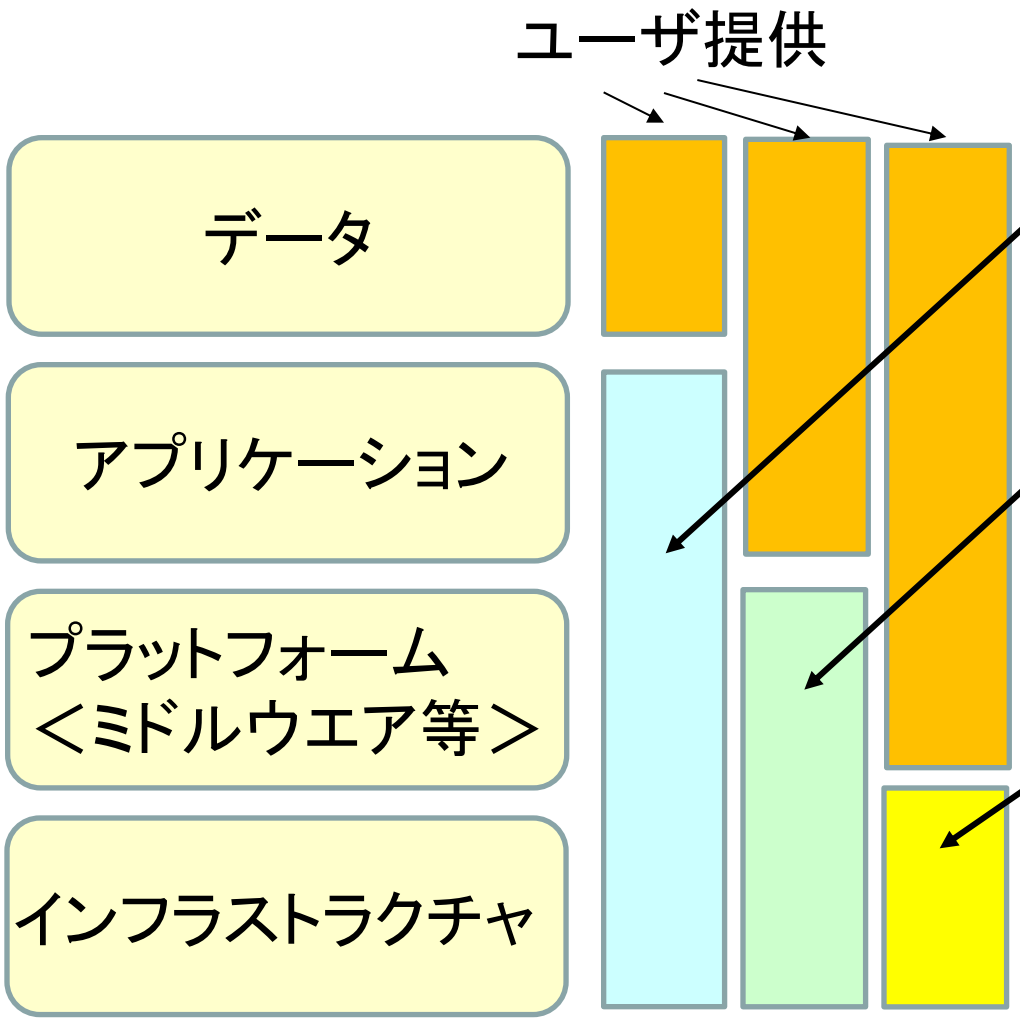
略して**クラウド**と呼ばれることも多く、cloud とは英語で「**雲**」を意味する。



https://ja.wikipedia.org/wiki/%E3%82%AF%E3%83%A9%E3%82%A6%E3%83%89%E3%82%B3%E3%83%B3%E3%83%94%E3%83%A5%E3%83%BC%E3%83%86%E3%82%A3%E3%83%B3%E3%82%B0

クラウドの種類





それぞれ、パブリッククラウドとプライベイトクラウドがある

SaaS（Software as a Service）・・・ **ソフトウェア**を提供するクラウドサービス：Office 365など

PaaS（Platform as a Service）・・・ **開発環境**を提供するクラウドサービス：Dockerなど

IaaS（Infrastructure as a Service）・・・ **サーバー（インフラ）**を提供するクラウドサービス：AWSなど

クラウド利用のセキュリティ基本原則

1. 共同責任モデル

プラットフォームを提供する事業者とソリューションを提供するパートナー、そしてユーザー企業の三者がそれぞれ協力し、セキュリティを確保していくこと。責任範囲はオンプレミスに比べ小さくなるので、今まで費やしていたリソースをほかの業務に振り分けられる。

2. 多層防御

1つの技術だけで対策するのではなく、複数のレイヤーで対策し、重要な情報に到達するまでに時間や手間がかかるようにする。つまり、攻撃しにくいシステムを作るということだ。

https://active.nikkeibp.co.jp/atcl/wp/b/19/11/28/00220/?n_cid=nbpnxta_mltg

起こっては困ることと利用者の対応

起こっては困ること
（1）機密性（Confidentiality）の喪失：情報を不当に見られる
（2）完全性(Integrity)の喪失：情報を不当に破壊、改ざんされる
（3）可用性(Availability)の喪失：不当な利用によりデータやコンピュータパワーが使えなくなる

（1） 適切なSaaS業者の選定

（2） 利用者のPCなどの適切な管理

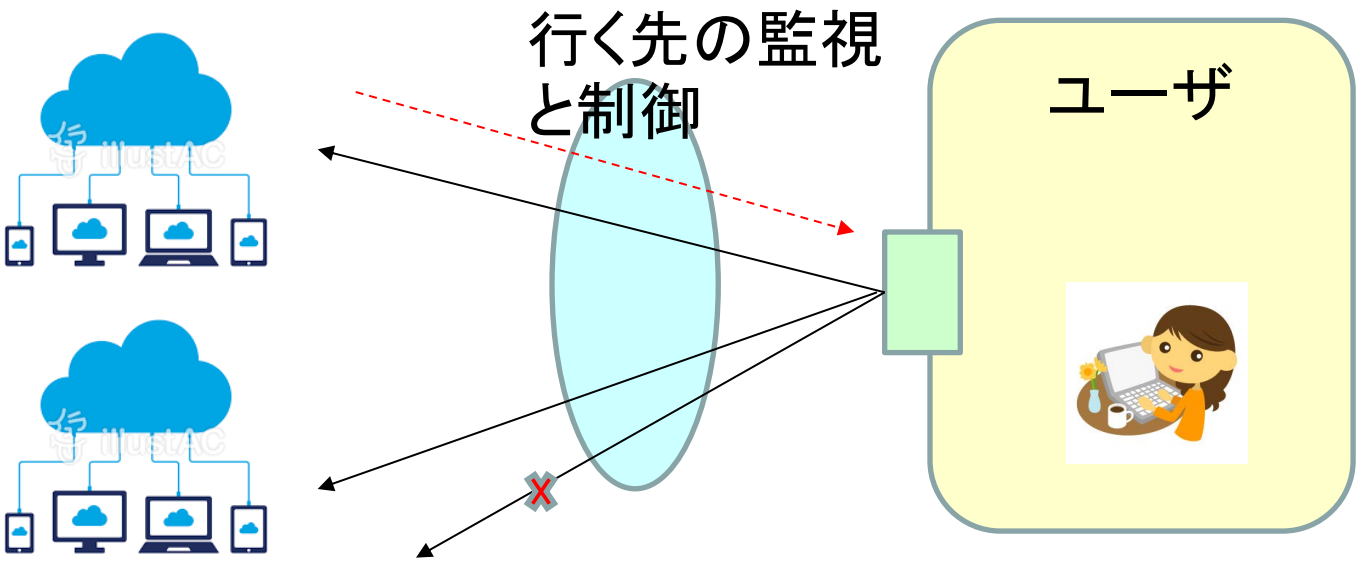
SaaS業者選択のチェックポイント

- ●OS、ソフトウェア、アプリケーションにおける脆弱性の判定と対策
- ●不正アクセスの防止
- ●アクセスログの管理
- ●通信の暗号化
- ●安全な個人認証方式の導入（2要素認証・2段階認証など）
- ●データセンターの物理的な情報セキュリティ対策（災害対策や侵入対策等）
- ●データのバックアップ
- ●セキュリティ監査の実施　他

クラウド側からの
セキュリティサービスの一例

CASB（Cloud Access Security Broker）

企業においてクラウドサービス利用が進む中で、従業員のクラウドサービス利用をコントロールするための企業向けサービスの総称。



起こっては困ることと利用者の対応

起こっては困ること
（1）機密性（Confidentiality）の喪失：情報を不当に見られる
（2）完全性(Integrity)の喪失：情報を不当に破壊、改ざんされる
（3）可用性(Availability)の喪失：不当な利用によりデータやコンピュータパワーが使えなくなる

（1） 適切なSaaS業者の選定

（2） 利用者のPCなどの適切な管理

2要素認証と2段階認証

（1）2要素認証とは

「2要素認証とは、利用者の本人確認などの認証において、二つの異なる原理の認証手段を組み合わせて用いることにより精度と安全性を高める手法。」 例：パスワードと生体認証、パスワードとICカードなど

（2）2段階認証とは

「パスワードを入力した後、SMSを使って送られてくるコードなどを入力することにより認証の精度と安全性を高める手法」2要素認証の1つとみることもある。

クラウドユーザにとって重要なセキュリティ対策

① パスワードなどの認証手段の厳密な運用（含む2要素認証）

② 組織内PCのOSやアプリケーションを最新の状態にする

③ 組織内PCのウイルス対策の実施

②③はクラウド業者がサービスする方向も

パスワードクラック方法と対策

1. 類推攻撃　＝＞下記のようなパスワードは使わない
　自分、身内の電話番号、車のナンバープレート、guest　など

2. 辞書攻撃　＝＞　辞書に載るような単語は使わない

3. 総当たり攻撃　＝＞10文字以上、英数字特殊文字を含む

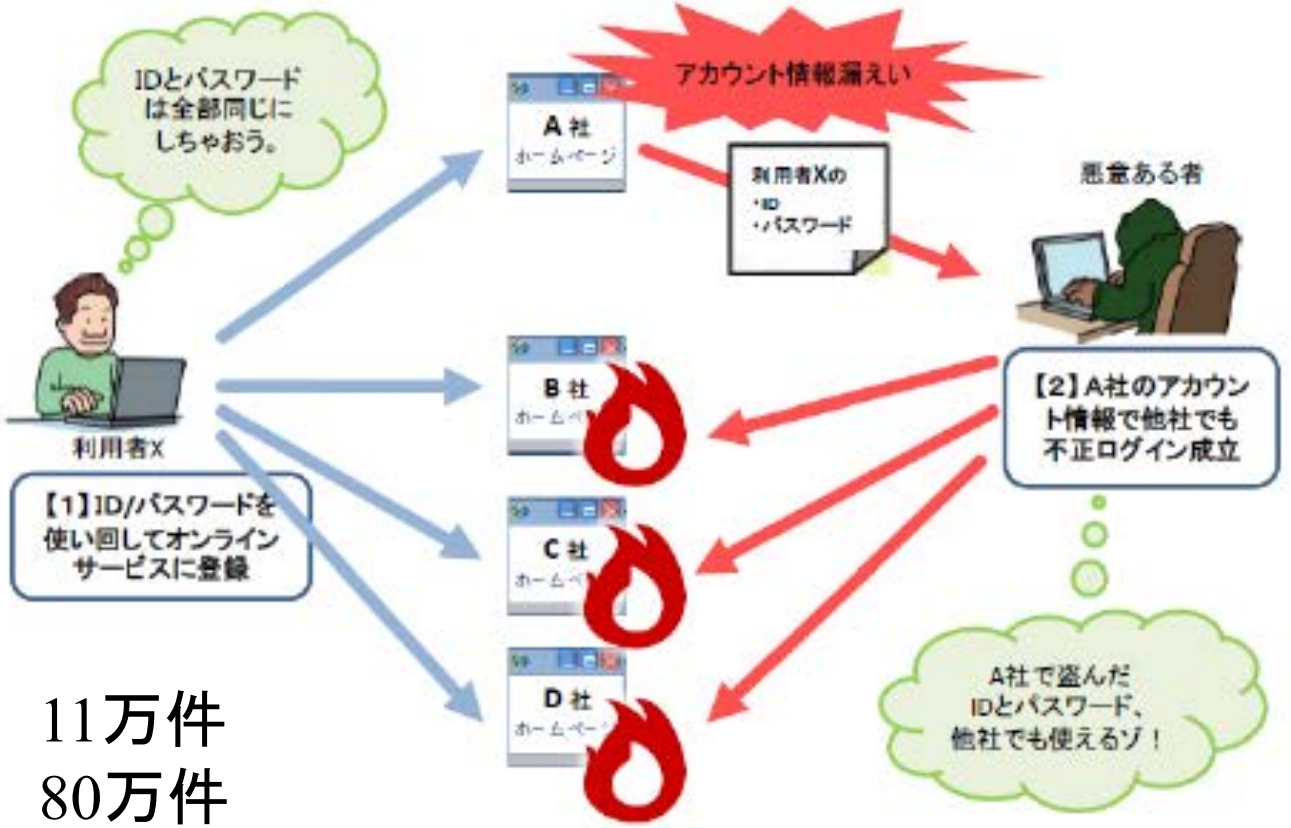
4. ソーシアルエンジニアリングによる攻撃　＝＞だまされないように

5. パスワードリスト攻撃　＝＞対象ごとにパスワードを変える

6. (a)ソフトの脆弱性を利用した攻撃(ハートブリード攻撃など)
　(b)マルウエアを利用した攻撃
　　＝＞パッチの適用など

7. 再発行システムの脆弱性を利用した攻撃
　＝＞　ページ型のサイトのサービスは利用しない

パスワードリスト攻撃



平成24年　11万件
平成25年　80万件

図 6　利用者の観点から見たパスワードリスト攻撃による被害のイメージ図
http://www.ipa.go.jp/files/000040778.pdf

安全なパスワードに関するメモ

1．重要性が高いものについては、サイトごとにパスワードを変えるべきである。

2．パスワード作成のメタルールを決めておくべきである。

3．多くのパスワードを覚えるのは困難なので安全に保管するならパスワードを手帳などにメモしてもよい。

4．3．パスワードは頻繁に変える必要はないが、やはり変えたほうが安全性は高い。＝＞両論あり

安全なパスワードの一例

基本となる核パスワード
10文字以上英数字や特殊文字を含む
（数個用意する。覚えるのが望ましいが、手帳などにメモして安全に管理してもよい）

R( ) ( )T3　　JQB　　19S

アクセスサイトを表す部分（IPAを1文字ずらしたもの）

時期の変化に合わせて変える部分

パスワードクラック方法と対策

1. 類推攻撃　＝＞下記のようなパスワードは使わない
　自分、身内の電話番号、車のナンバープレート、guest　など

2. 辞書攻撃　＝＞　辞書に載るような単語は使わない

3. 総当たり攻撃　＝＞10文字以上、英数字特殊文字を含む

4. ソーシアルエンジニアリングによる攻撃　＝＞だまされないように

5. パスワードリスト攻撃　＝＞対象ごとにパスワードを変える

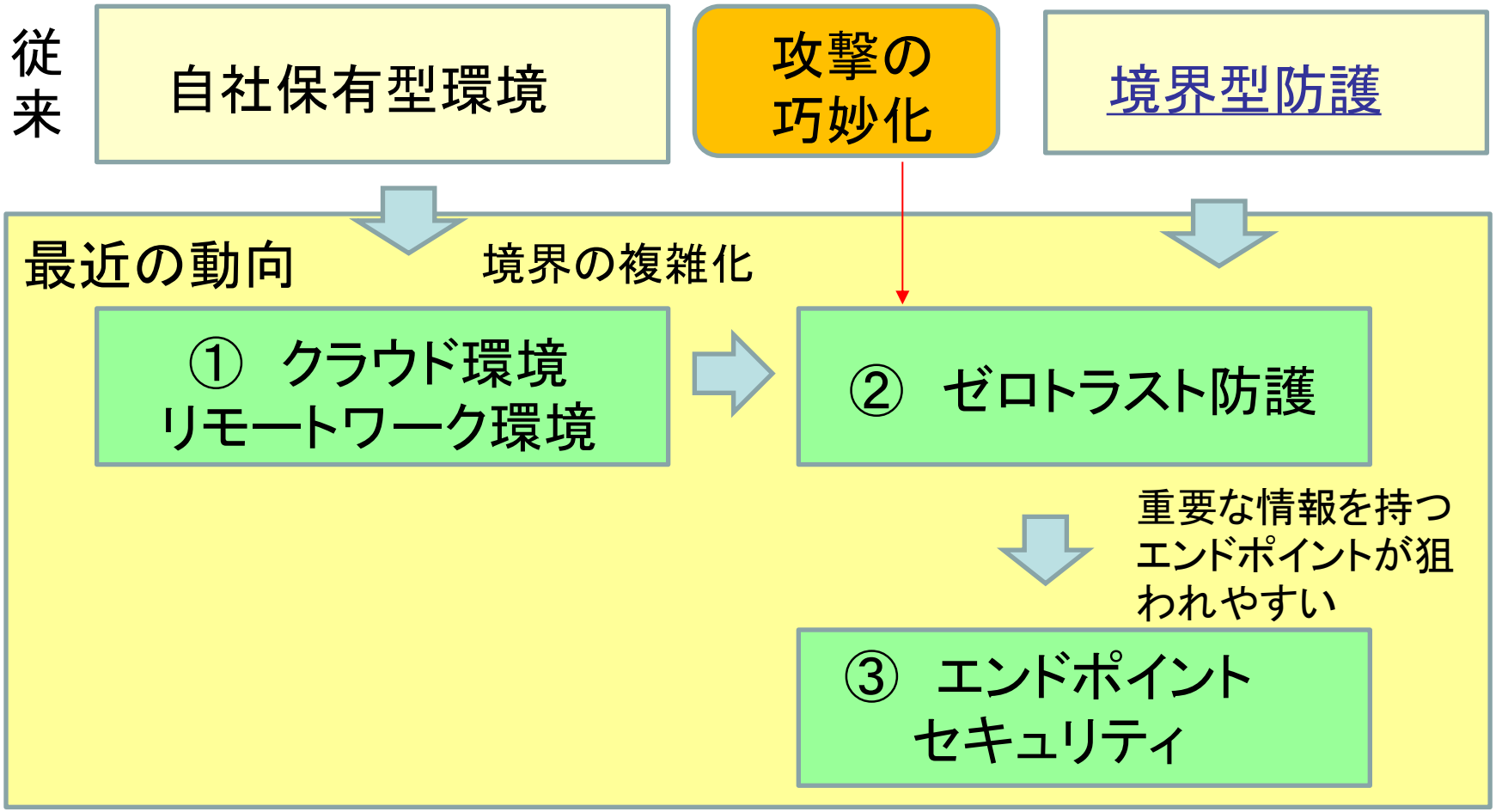
6. (a)ソフトの脆弱性を利用した攻撃(ハートブリード攻撃など)
　(b)マルウエアを利用した攻撃
　　＝＞パッチの適用など

7. 再発行システムの脆弱性を利用した攻撃
　＝＞　ページ型のサイトのサービスは利用しない

目次

1. 防御モデルをめぐる最近の動向
2. クラウド化とセキュリティ
3. 境界型とゼロトラストモデル
4. エンドポイントセキュリティ
5. おわりに

防護モデルの変化の相互関係

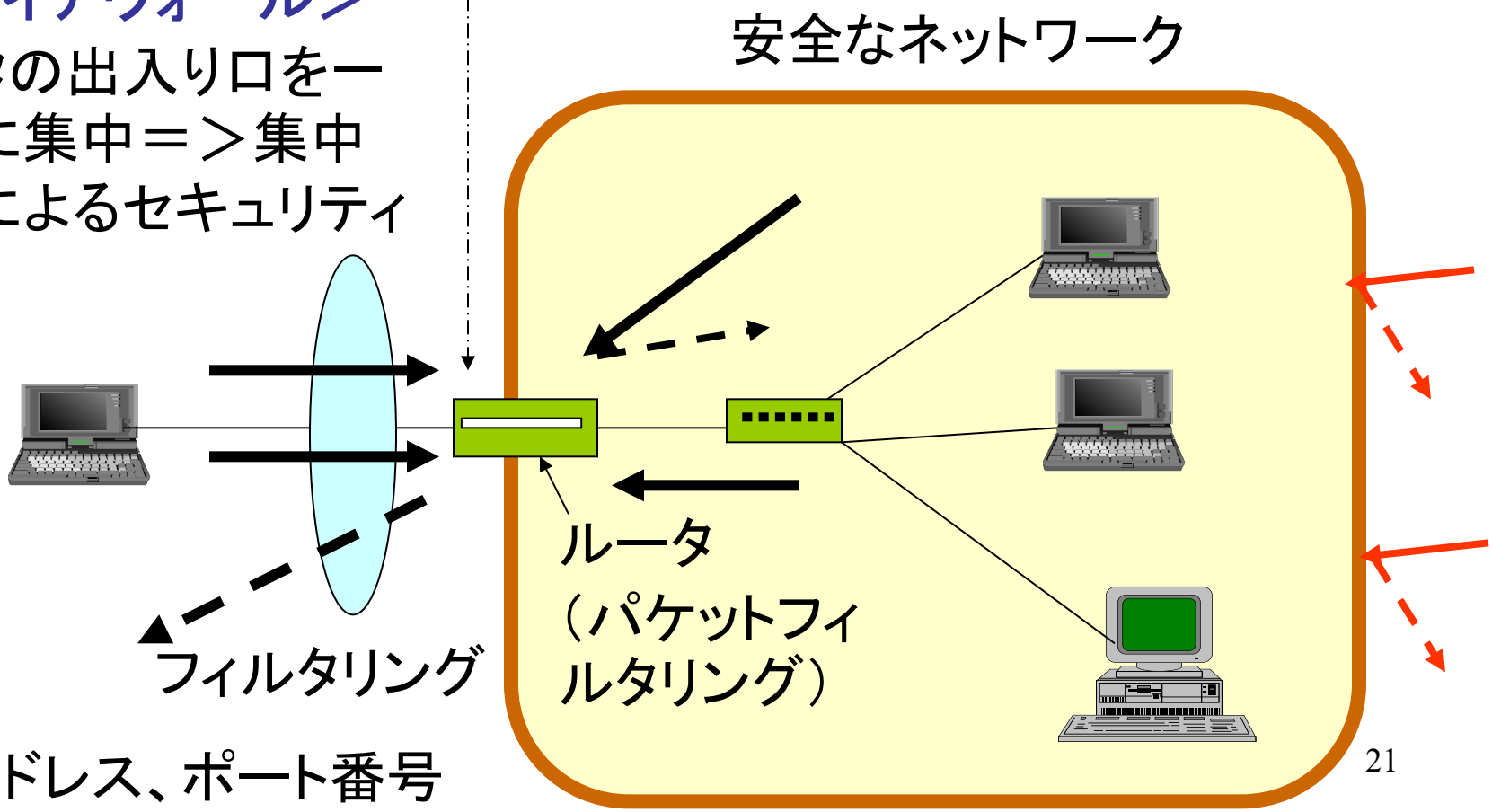


CDM: Continuous Diagnostics and Mitigation

境界防護の基本方式

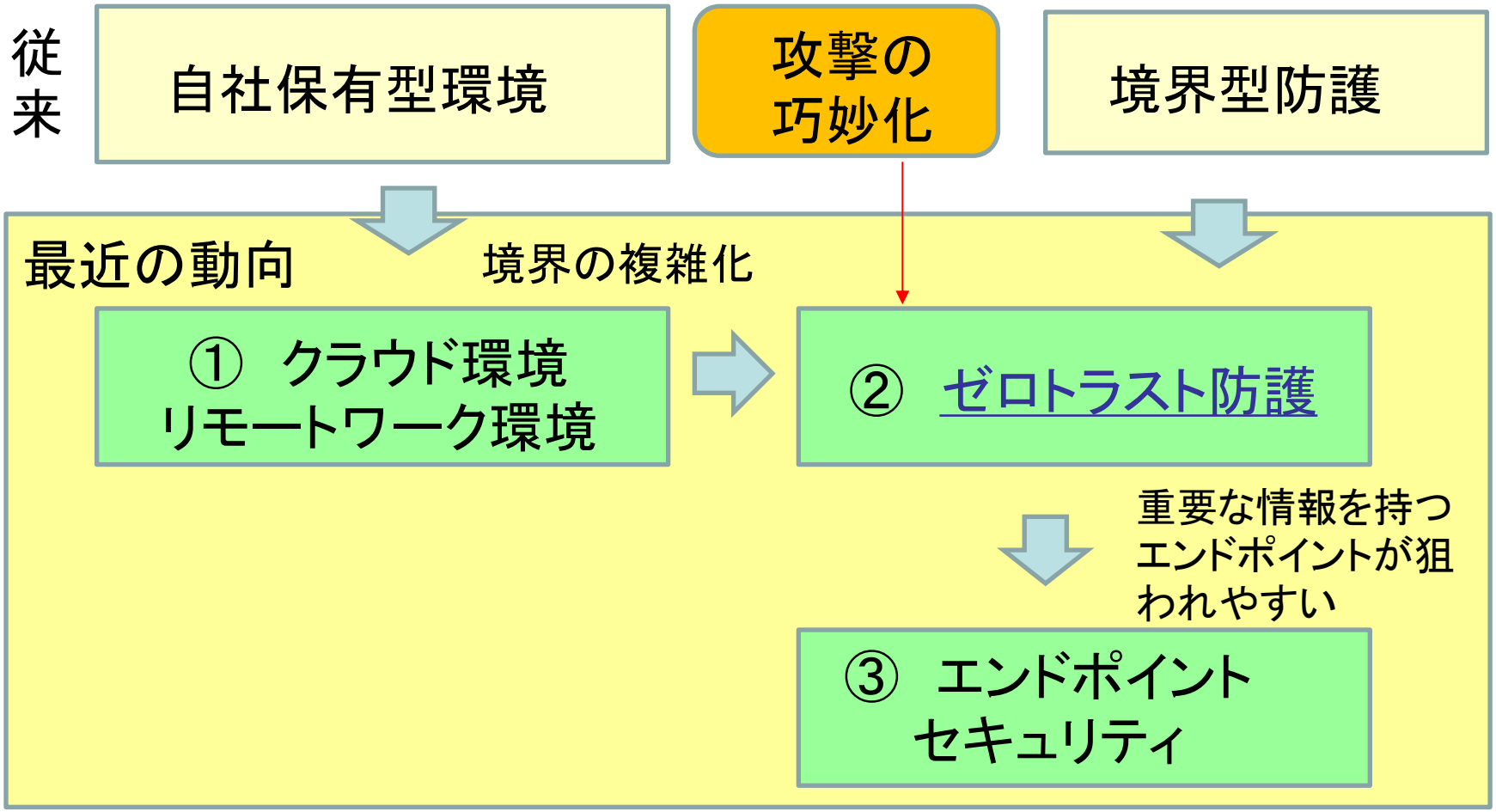
ファイアウォールの設置

＜ファイアウォール＞
データの出入り口を一箇所に集中＝＞集中管理によるセキュリティ向上



IPアドレス、ポート番号

防護モデルの変化の相互関係



CDM: Continuous Diagnostics and Mitigation

ゼロトラストアプローチが出た背景

境界が複雑になるとともに攻撃が巧妙になり、境界で防御しきるのは困難に

境界を越えた攻撃はありうるとして、通信相手のPCやサーバが信頼できないとしても、自分の安全を維持しうる防御を可能に＝＞ゼロトラストアプローチ （Forrester Research社が2010年に提唱）

ゼロトラストモデルの3つの基本原則

①　必ず検証し、全てのリソースの完全を確保せよ

②　アクセスコントロールを限定し強制せよ

③　ログとトラフィックを全て確認せよ

https://www.atmarkit.co.jp/ait/articles/2007/14/news009.html

動的ポリシー

（１）従来のネットワークアクセスの考え方では、あらかじめ決められたポリシーによってアクセス許可が決定。

（２）ゼロトラストでは、さまざまな属性をパラメーター化し、都度ポリシーに従って計算を行い、アクセスを許可。例えば

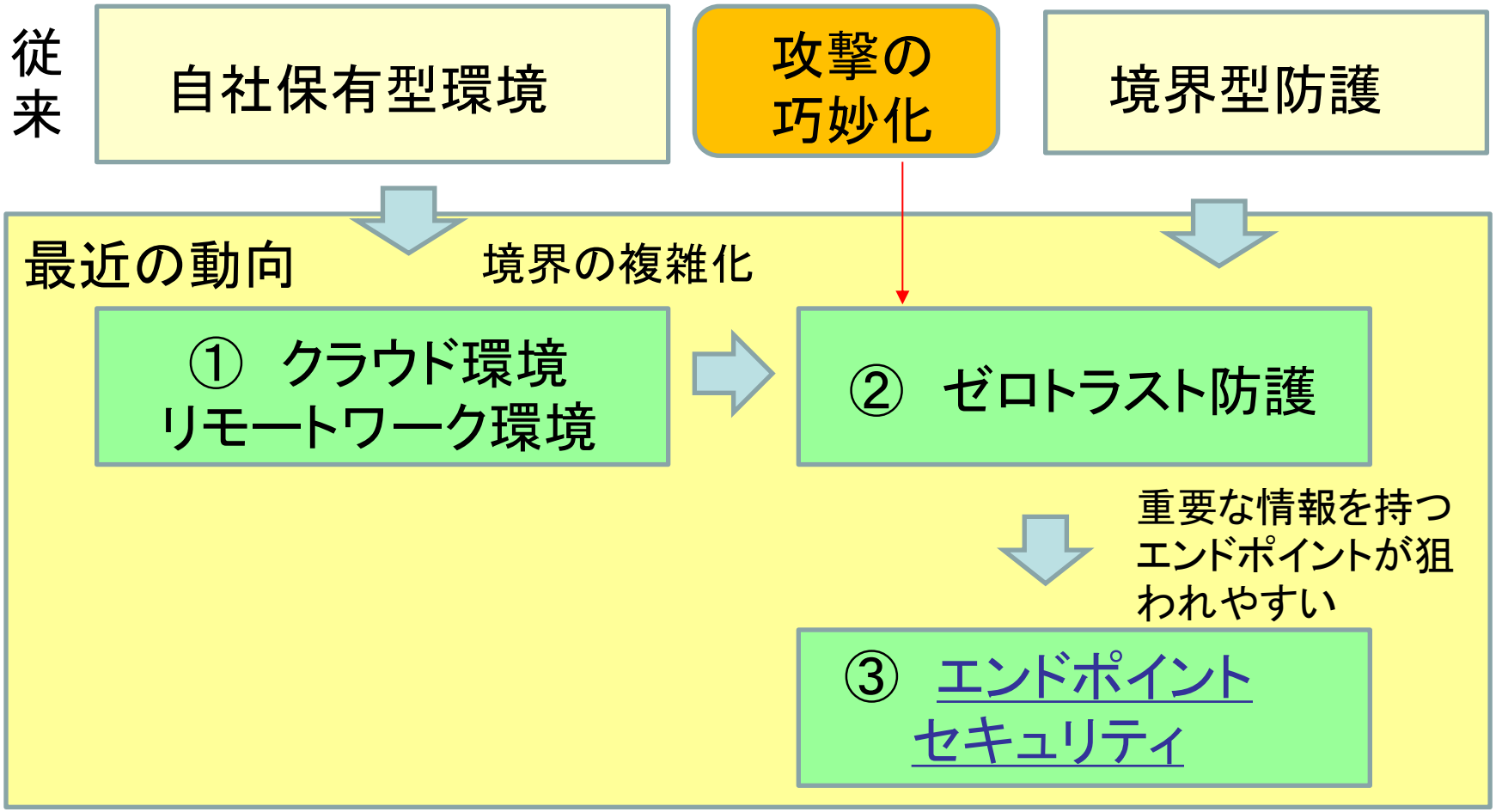
- クライアントの識別としては、ユーザーアカウントや関連属性など
- デバイスの状態では、インストールされているソフトウェアのバージョンやネットワークの場所、アクセス日時など
- 振る舞い属性として、ユーザーやデバイスの異常な振る舞いの記録の有無
- 環境属性として、ネットワークの場所や時間、報告されている攻撃など

https://www.atmarkit.co.jp/ait/articles/2009/15/news007.html#_ga=2.240946691.1082378556.1604640806-183211706.1601945296

目次

1. 防御モデルをめぐる最近の動向
2. クラウド化とセキュリティ
3. 境界型とゼロトラストモデル
4. エンドポイントセキュリティ
5. おわりに

防護モデルの変化の相互関係

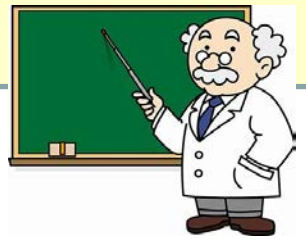


CDM: Continuous Diagnostics and Mitigation

エンドポイントセキュリティとは

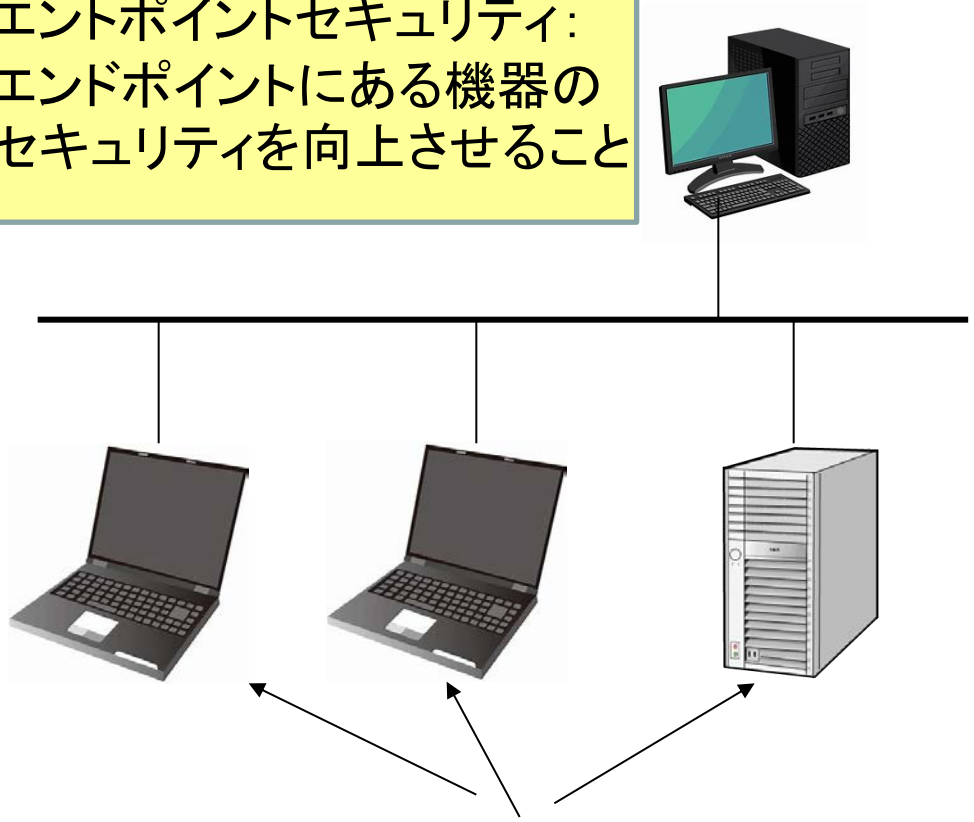
① エンドポイントセキュリティとは、サーバーやPC、スマートフォンなどを含む末端機器に対してマルウェア感染などのサイバー攻撃、あるいは内部不正を想定したセキュリティ対策を施すことを指す。

② エンドポイントは多様化し、サーバー、デスクトップPC、ノートPC、仮想デスクトップを導入した端末などに加えてスマートフォンやタブレットなどが挙げられる。また、社内で使用するものだけではなく、外出先やリモートワークで使用する端末も含まれる



エンドポイントセキュリティ

エントポイントセキュリティ:
エンドポイントにある機器の
セキュリティを向上させること



エンドポイント

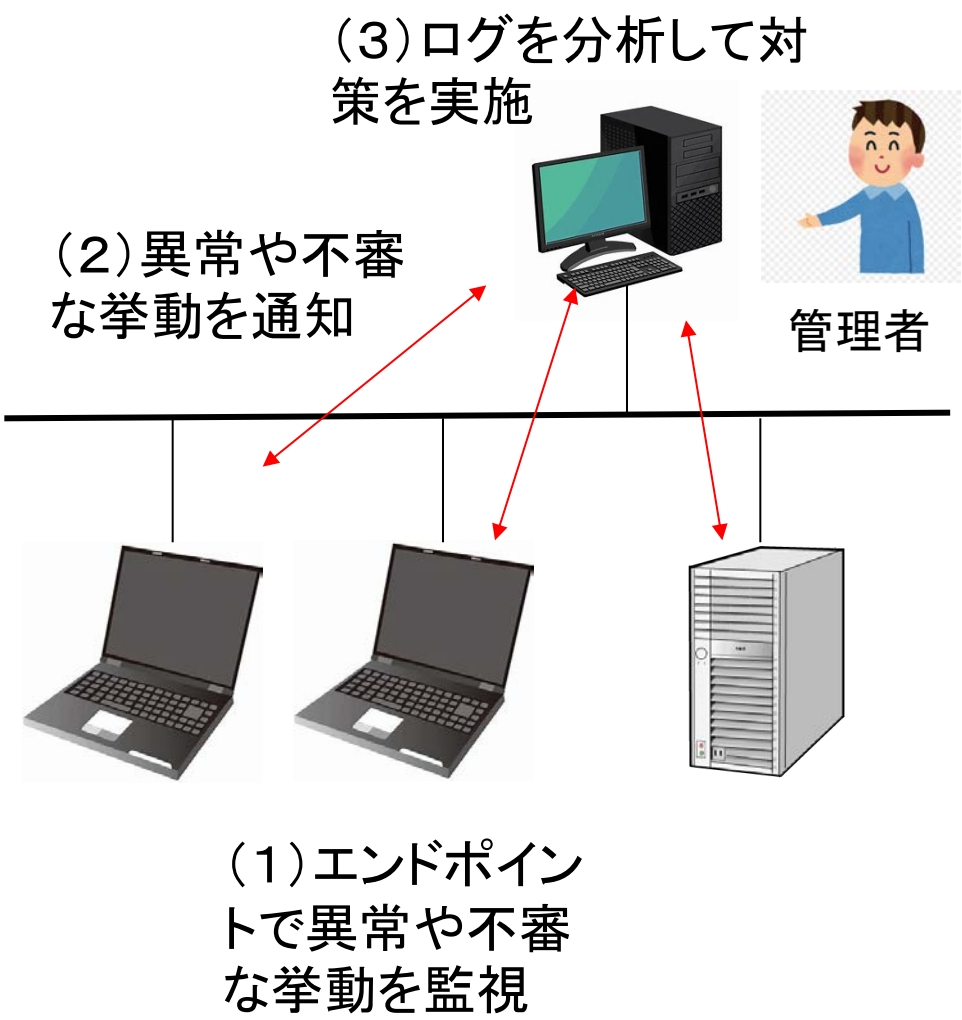
新しい対策

① EDR（Endpoint Detection and Response）
Cybereason　EDRなど

② エンドポイントにおける異常の新しい検知法
振る舞い検知　Yarai等
AI応用

従来の対策:ファイルの自動暗号化、ID・アクセス管理、アンチウイルスソフトなど

EDRとは



① EDR（Endpoint Detection and Response）とは、ユーザーが利用するパソコンやサーバー（エンドポイント）における不審な挙動を検知し、迅速な対応を支援するソリューション。

② 具体的には、パソコンやサーバーの状況および通信内容などを監視し、異常、あるいは不審な挙動があれば管理者に通知。

③ 管理者は通知を受けた後、EDRで取得されたパソコンや通信の状況を示したログを分析して対策を実施。

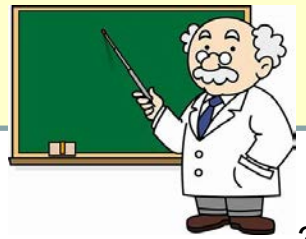
EDR製品の例

1. Cybereason EDR
   サイバーリーゾン・ジャパンKK

2. Symantec Endpoint Detection and Response
   シマンティック

3. Windows Defender Advanced Threat Protection (ATP)
   マイクロソフト

4. Sophos Intercept X Advanced with EDR
   ソフォス



https://www.itreview.jp/categories/edr?page=1

目次

おわりに

1．サイバー攻撃の最近の動向に簡単に触れたのち、防御モデルをめぐる最近の動向を整理。

2．サイバー攻撃はますます巧妙になるので、これらの防御モデルの動向を引き続き注目していく必要がある。


END