安心を、ひとつ上のステージへ。

TREND MICRO

資料1－5

次世代ネットワークにおける脅威

トレンドマイクロ株式会社

Presenter Name
Presenter Title

Classification
2007/10/29

本日の内容

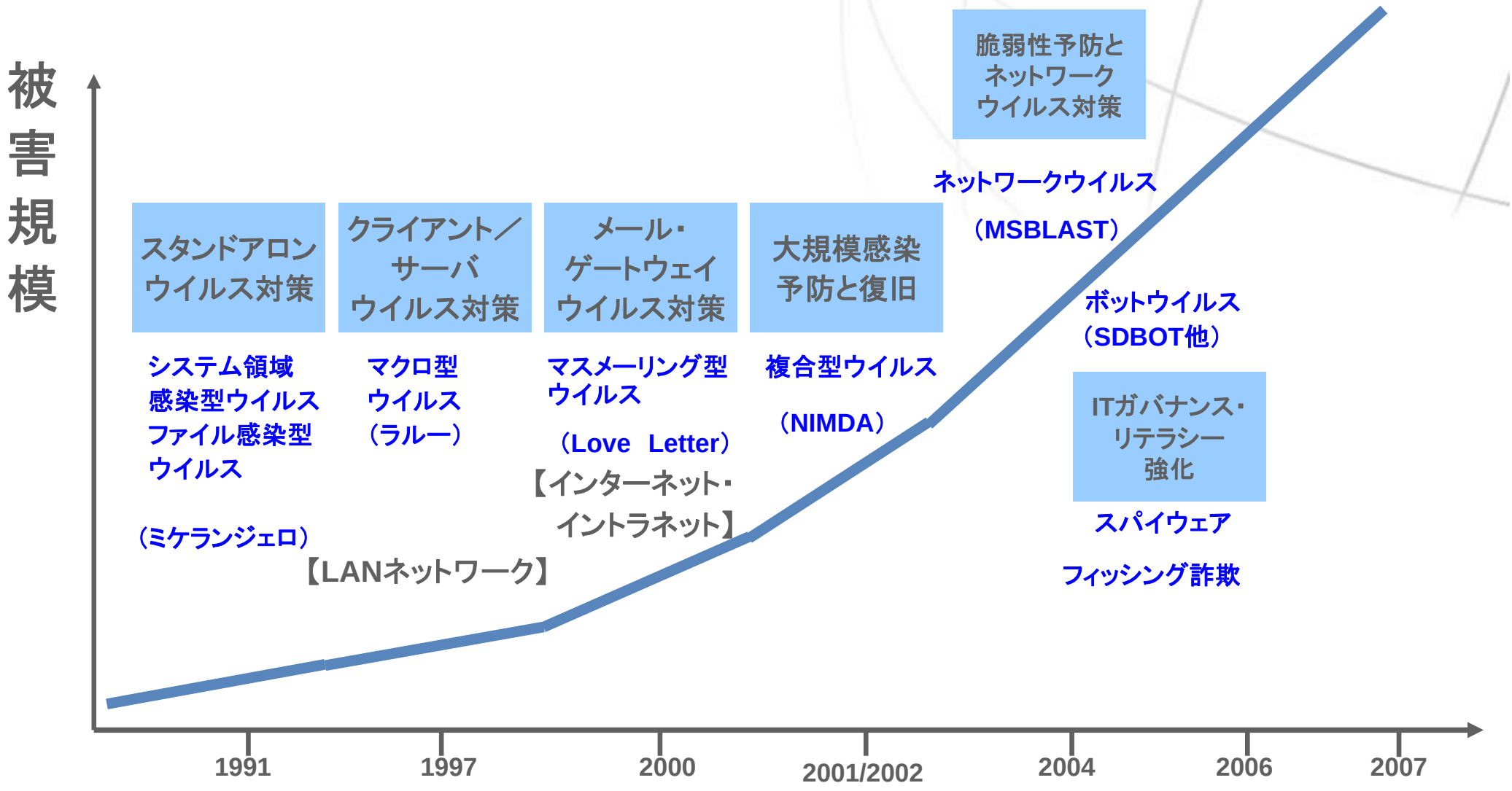
安心を、ひとつ上のステージへ。

TREND MICRO

現在までのウイルスと対策の変遷

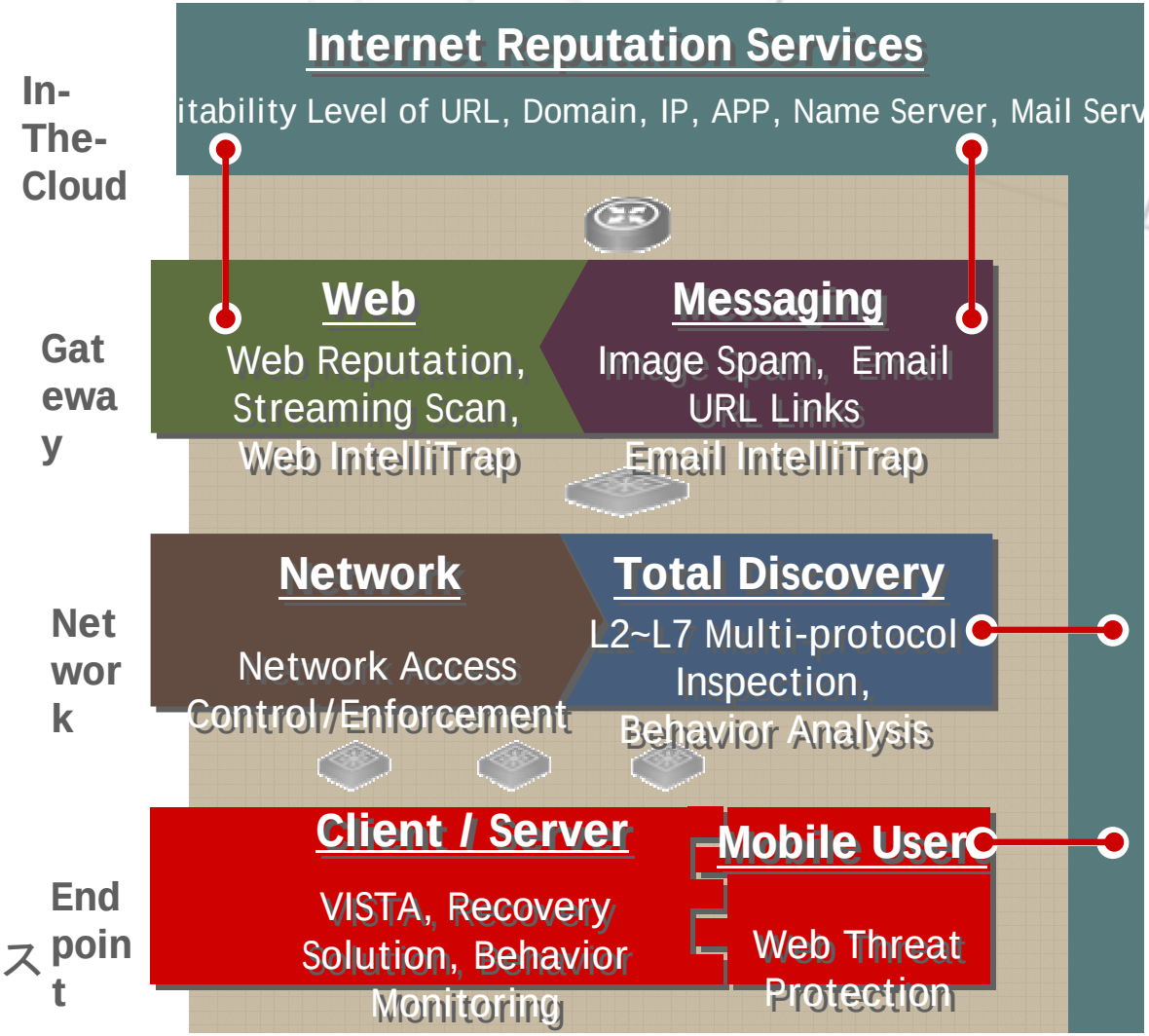
次世代ネットワークにおける脅威分析

1.1 ウイルスの変遷

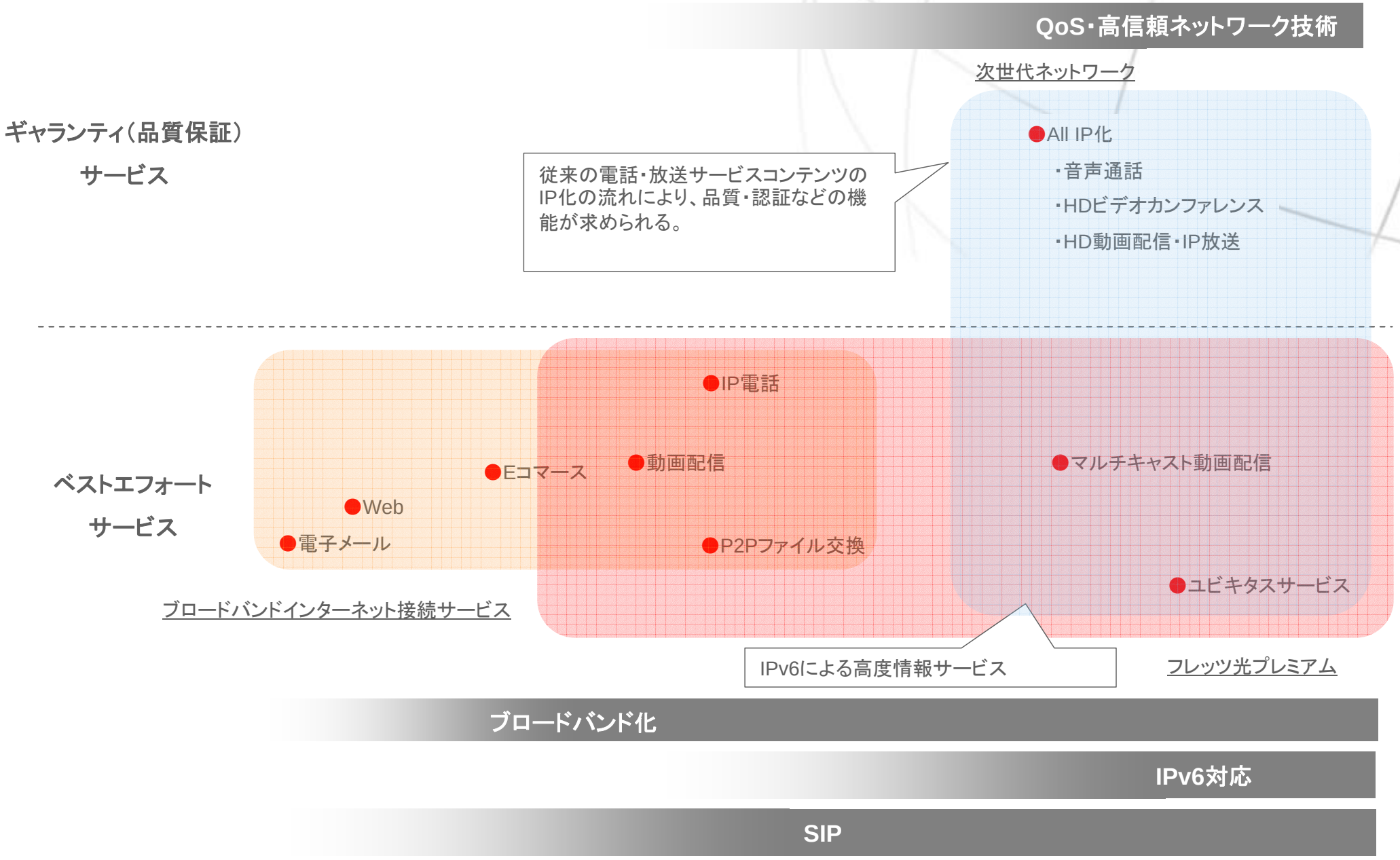


1.2 これまでの脅威に対する対策の変遷

- パターンマッチングによるウイルス対策
  - 一般的なウイルス
- 振る舞い検知
  - 新種ウイルスへの対応
- ヒューリスティック検索
  - 亜種ウイルスへの対応
  - 未知ウイルスへの対応
- Webメール検索、メール検索
  - WEB,HTMLメールウイルス
- IPSなどの進入検知テクノロジー
  - 対ネットワークウイルス
- パーソナルファイアーウォール
  - 対ネットワークウイルス
- 検疫技術
  - 対ネットワークウイルス
- URLフィルタ、レピュテーションサービス
  - フィッシングサイト
  - WEBからの脅威



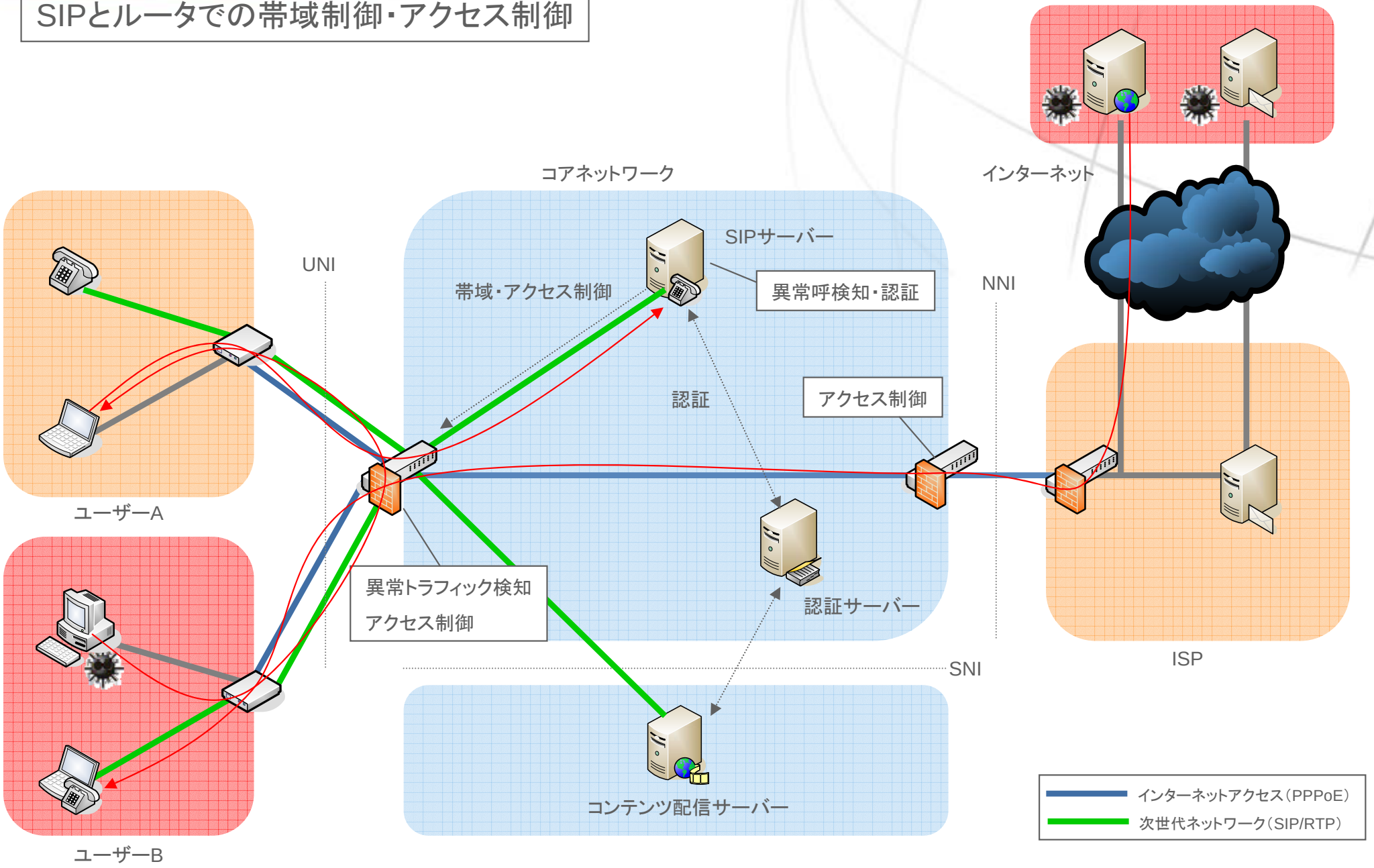
2.1 次世代ネットワークの位置づけ



2.2 次世代ネットワークに対するセキュリティ脅威（1）

安心を、ひとつ上のステージへ。
TREND MICRO

SIPとルータでの帯域制御・アクセス制御



2.3 次世代ネットワークに対するセキュリティ脅威(2)

安心を、ひとつ上のステージへ。
TREND MICRO

IPv6におけるセキュリティ脅威

Webからの脅威

- 現状では、IPv6アドレスを持つ悪性サイトは殆ど無い。
  - セキュリティベンダによる監視・フィルタリングを避けるために、IPv6アドレスへの逃避を行う可能性
  - 感染PCからの接続可容性による(特定利用者、ユーザーをターゲットとする場合にはこの限りではない)

ウイルス、ワームのIPv6対応化の可能性

- ネットワークプログラミングでのIPv6対応は容易
- アドレス空間が広大なため感染パケットの送信による感染活動は非効率的(→トラヒックパターンとして検出が容易)
- アドレスが固定的なため、一度、不正プログラムが侵入した後は、Back Doorなど遠隔操作のためのチャネル作成が容易

2.4 次世代ネットワークにおけるセキュリティ脅威（3）

安心を、ひとつ上のステージへ。
TREND MICRO

コアネットワークに対する脅威

- All IP化によるインフラサービスへの攻撃可能性
- DDoS・輻輳

コアネットワークに対する脅威は限定的

- エッジルータでのポリシング（アクセス制御）によるコアネットワークへの不正トラフィックの流入の抑止
- 認証機構により信頼できるサービス提供者によるコンテンツサービス
- SIPサーバーを含むネットワークインフラに対する攻撃（異常呼など）は限定的

ユーザーネットワーク・機器に対する脅威

- インターネット接続サービスによる外部ネットワークへのアクセス、トラフィックの流入
  - SPAMメールによる悪性サイトへの誘導、フィッシング詐欺、Drive by Download

ユーザーネットワークは、従来のインターネット接続サービスと同様のセキュリティ脅威が存在する。

- 不正プログラムの侵入から、次世代ネットワークへの攻撃
- 偽装SIP-UAなどによるコアネットワークへのDDoS攻撃

2.5 次世代ネットワークに対する脅威分析 (1)

Type	No.	Description	Risk	Solution
ネットワークサーバへの攻撃	N-1	DNSサーバへのDDoS攻撃	L	エッジルータなどでの異常トラフィック検知。
	N-2	DHCPサーバへのDDoS 攻撃	L	エッジルータなどでの異常トラフィック検知。
	N-3	不正なDHCPリクエストによるIPアドレスの大量消費	M	エッジルータなどでの異常トラフィック検知。 DHCPサーバでの対策。
	N-4	SIPサーバへのDDoS攻撃	L	エッジルータなどでの異常トラフィック検知。 SIPサーバでの異常呼検知。
	N-5	偽装SIP-UAを用いたSIPサーバへのDDoS攻撃	M	エンドホストでの偽装SIP-UAの検知が必要。
コアネットワーク障害	N-6	不正なネットワーク攻撃によるネットワーク障害	L	QoSによる帯域制御とエッジルータでの異常トラフィック検知。

2.6 次世代ネットワークに対する脅威分析 (2)

安心を、ひとつ上のステージへ。
TREND MICRO

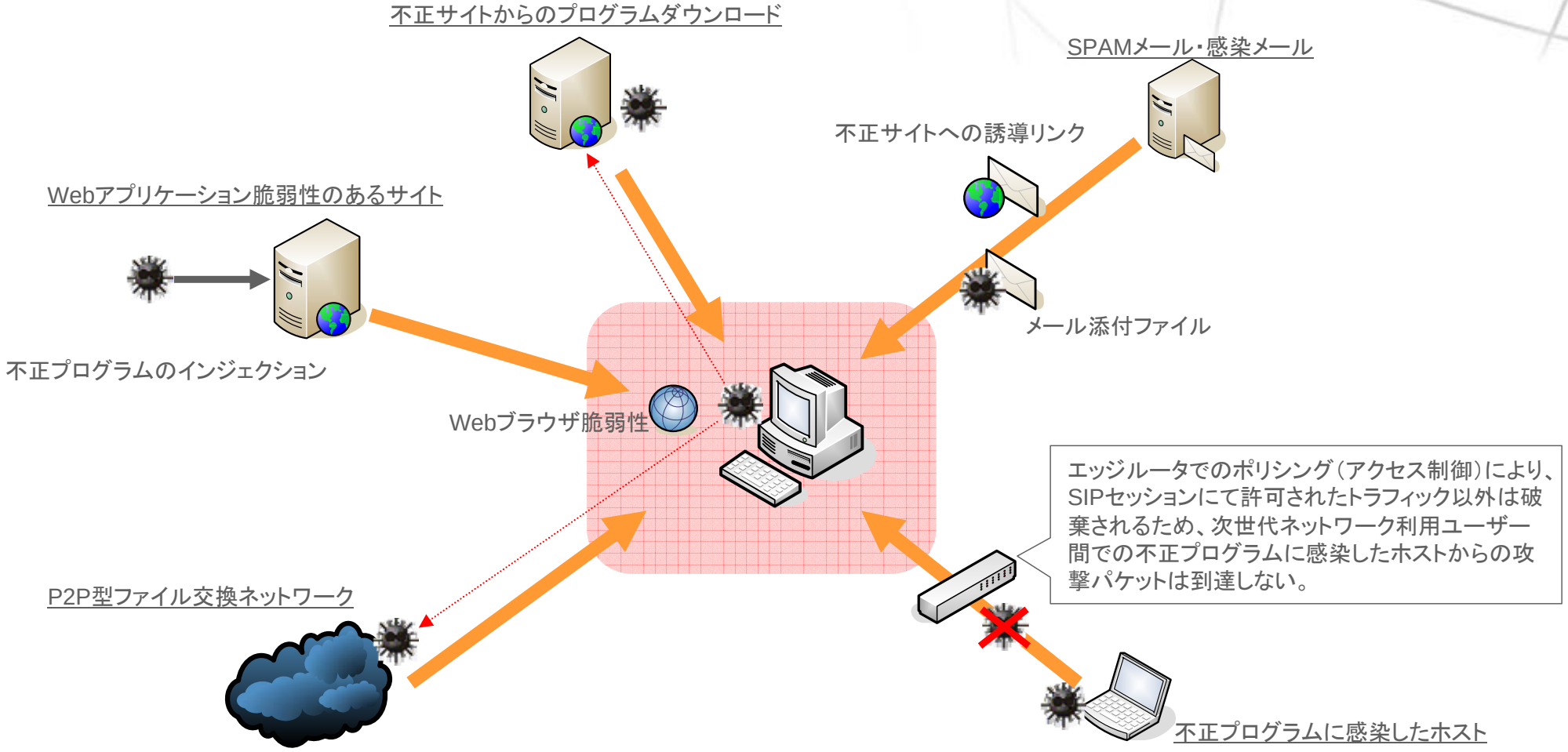
Target	No.	Description	Risk	Solution
エンドホスト	U-1	他のユーザーからの不正プログラム感染	L	エッジルータによるアクセス制御により、SIPにより確立されたセッション以外のエンドユーザー間のセッションは通過しない。
	U-2	偽装したDNS応答によるセッション誘導・詐称攻撃 エンドホスト上でのDNS設定の変更、または偽装DNSサーバの応答により、名前解決を詐称し、特定のサービス・セッションを誘導することが出来る。	M	エンドホストでの設定値などの監視。 DNSSECなどによるネームサーバ認証。
	U-3	SIPセッションの乗っ取り	L	TLSプロトコルなどを用いたSIPセッションの暗号・認証処理。
	U-4	偽装SIP-UAによる偽りのSIP INVITEメッセージ送信	M	SIP-UAの認証処理。Soft Phoneなど認証情報が不正プログラムにより入手可能な場合には、エンドホストでの対策が必要。
	U-5	確立したエンド・ツー・エンドセッションに対する、不正なパケット送信。 ホストの通信状態の監視および、SIPセッションを盗聴することによって、相手先アドレス・ポートの入手が可能な場合、メディアストリームの相手側ポートに対して不正なパケットを創始印することが出来る。	M	エンド・ツー・エンドセッションに対してIpsecやSRTPなどプロトコルレベルでの、暗号化、認証を行う。
	U-6	エンドホスト上のアプリケーションの改ざん (Soft Phone, Media Player etc.) on the PC. これらのアプリケーションの改ざん、感染により正規の認証情報の詐取および偽装セッションなどが不正プログラムによって可能となる。	H	エンドホストでのセキュリティ対策が必要

2.7 次世代ネットワークとサービスモデルの違い

サービスモデル	垂直統合サービス	水平統合サービス
事業会社	BT, France Telecom, etc.	NTT-E/NTT-W
基本サービス	IP電話 インターネット接続サービス（Web,email） **要確認**	IP電話 テレビ電話 動画配信 IP放送 高品位テレビ会議
コンテンツサービス	事業者に依存せず独立的なサービス？ （各、サービスごとに個別契約） **要確認**	コンテンツプロバイダへのサービスインフラ・インタフェースを提供 （課金・認証）
インターネット接続サービス	事業会社が提供	各社ISPにより提供
コアネットワークに流入するプロトコル	SIP, RTPなど認証済みセッションなど インターネットアプリケーション •Web,email •P2P, etc **要確認**	SIP, RTPなど認証済みセッションなど PPPoE
コアネットワークに対するセキュリティ対策	•ルータでの異常トラフィック検知・遮断 •SIPサーバーに対する異常呼検知・遮断 •ネットワーク輻輳監視 •Etc.	•ルータでの異常トラフィック検知・遮断 •SIPサーバーに対する異常呼検知・遮断 •ネットワーク輻輳監視 •Etc.
ユーザーネットワーク・エンドホストに対するセキュリティ機能の提供	インターネットコンテンツ、ネットワークからの脅威侵入・攻撃に対して事業者がセキュリティ機能を提供	複数の選択肢あり •サービス提供プロバイダによるセキュリティ機能の提供 •事業会社の標準機能・オプション機能 （OEMを含む）

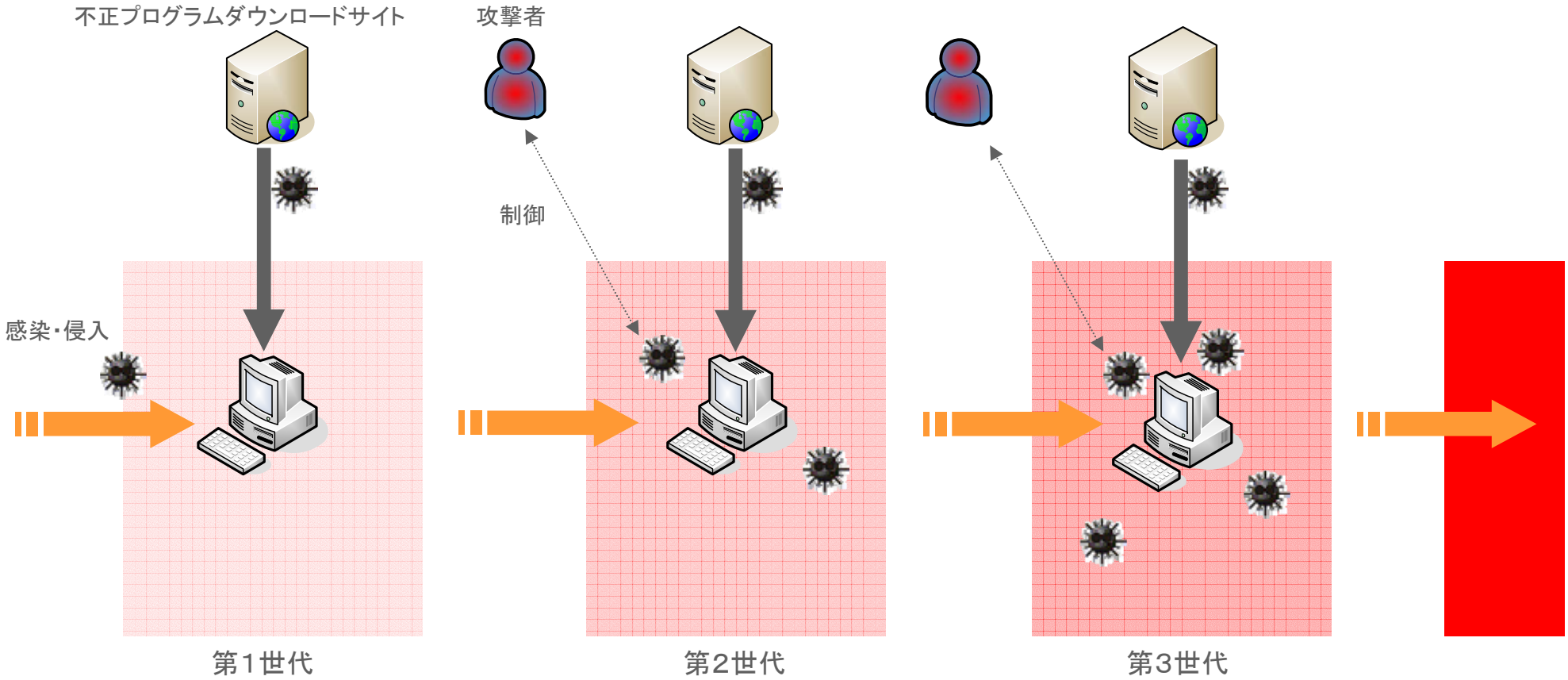
2.8 不正プログラムの感染・侵入経路

- 不正プログラムを含め、セキュリティ脅威はインターネット上の信頼置けないサイトから多様な経路で流入する
- ソフトウェア脆弱性だけではなく、ユーザーの不注意などを利用して感染を行う手法が多く用いられるようになってきた。
- 一度、不正プログラムの侵入・感染を許してしまうと、多様な手段で新たな不正プログラムの多重感染や更新など、セキュリティ被害の温床として長く脅威にさらされ続ける
- 次世代ネットワークにおいても、インターネットへの接続経路がある限りユーザーネットワーク上のホストは常にセキュリティ脅威にさらされる



2.9 不正プログラムの多重感染とWebからの脅威

- 一度感染すると、短期間で多重に不正プログラムに感染する
- ソフトウェア脆弱性を利用した感染パケット送信などによらず、Webからのダウンロードにより不正プログラムをダウンロードする
- 感染プログラムの更新・追加の頻度が速く、検知・駆除が困難
- シグネチャの提供前に新たな不正プログラムへと変質する
- 新たな機能の獲得・機能強化するなど、より巧妙化・悪質化する

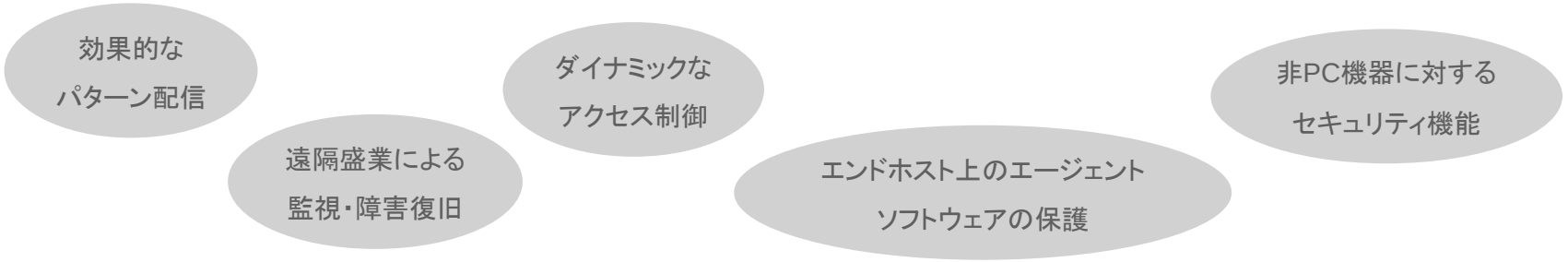


2.10 脅威分析のまとめ

1. コアネットワークに対するセキュリティ脅威は限定的
2. IPv6特有のセキュリティ脅威は少ない
3. ユーザーネットワークは、次世代ネットワークでもセキュリティ脅威にさらされ続ける
4. エンドホストに対するセキュリティ脅威により、DDoS攻撃を含めて次世代ネットワークサービスの利便性を低下させるリスクが存在する

次世代ネットワークの技術を利用することにより、従来までのエンドホスト・ユーザーネットワークへのセキュリティ対策と比べて高度なセキュリティソリューションの提供が可能

- 次世代ネットワークサービスと既存のISPサービスとの差別化
- 付加価値サービスとしてのセキュリティ機能の提供



補足：その他の脅威と必要となるべきパートナー

- 現状のトラフィックアナライザーの類では、モニタリングはできるが事故を事前予測しづらい
  - コアネットワークのモニタリング・コンサルティングチームが別に必要か？
- サーバ、IP電話の相互接続乗り入れのトラブルを事前回避するか（SIPプロトコルの方言に対するキャパビリティ）
  - フロントエンドに柔軟に対処できるジョイントサーバ的なものが必要？
- サイバーテロ・犯罪捜査時の合法的なタッピング手段
  - エッジルータ、もしくはゲートウェイ部分で対応？
- 国内のインフラが高速化することによる海外接続専用線のキャパビリティの飽和
  - 基本インフラも含めた見直しが必要？

安心を、ひとつ上のステージへ。

TREND MICRO™