Infosec
Risk Management Professionals

IPv6環境におけるセキュリティ

株式会社インフォセック
製品・サービスユニット
大和田　利郎

会社概要

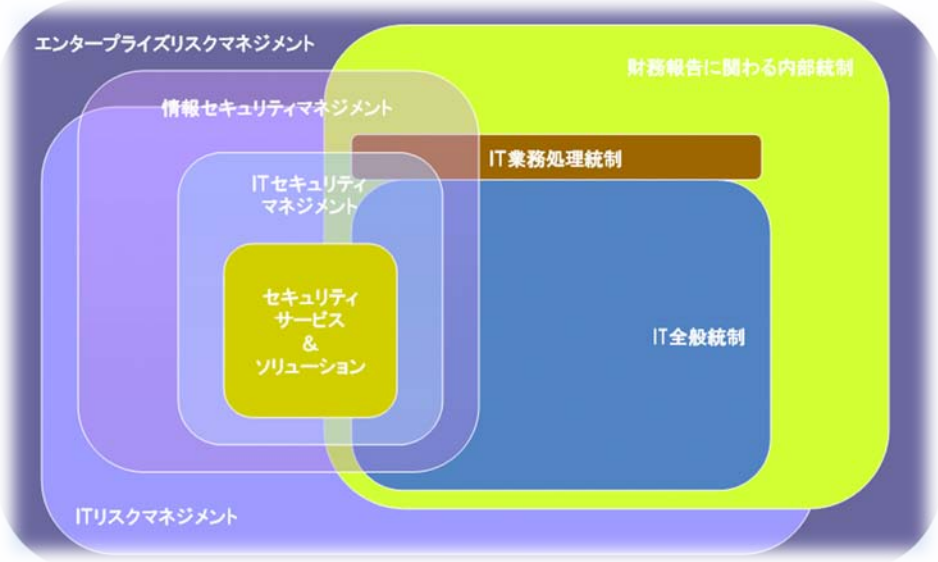
会社名　　：株式会社インフォセック

代表者　　：林　簡
設立　　：2001年
資本金　　：3億円
従業員数　　：143名（2010年4月現在）
株主　　：三菱商事株式会社
本社所在地　：東京都渋谷区恵比寿1 - 19 - 19
　　恵比寿ビジネスタワー　17階

サービス　　：情報セキュリティコンサルティング
　　内部統制コンサルティング
　　セキュアテクノロジーコンサルティング
　　セキュリティ診断（脆弱性診断）
　　セキュリティ商材の販売及びその導入支援
　　セキュリティ監視サービス

主要商材　　：ArcSight
　　Skybox View
　　Bigfix

所属団体　　：情報セキュリティ監査協会（JASA）
　　日本ネットワーク セキュリティ協会（JNSA）
　　日本セキュリティマネジメント学界（JSSM）
　　日本カード情報セキュリティ協議会（JCDSC）
　　デジタル・フォレンジック研究会（IDF）
　　日本医療情報ネットワーク協会（JAMINA）
　　日本ISMSユーザーグループ（J-ISMS-G）



ISO 27001
BUREAU VERITAS
Certification

認証範囲：全社

Infosec
Risk Management Professionals

実績紹介（抜粋）

- 官公庁
  中央省庁、政府系金融機関、地方自治体、外郭団体　等

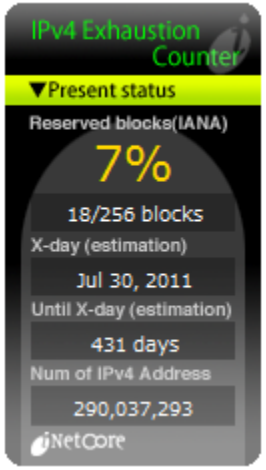
- 金融機関
  都市銀行、地方銀行、証券会社、信託銀行、生命保険会社、信販会社　等

- 重要インフラ企業
  電力会社、通信会社、放送会社、医療　等

- その他
  製造業、情報通信業、サービス業、小売・流通業、学校法人　等

IPv4アドレスの枯渇によって？－①

- IPv4アドレスの枯渇時期(予測)
  - 2011年秋には在庫が枯渇するかも



Source:iNetCore

IPv4(32ビット)：2^{32}=約43億(4,294,967,296)
IPv6(128ビット)：2^{128} = 約340澗
(340,282,366,920,938,463,463,374,607,431,768,211,456)

IPv4アドレス空間

事実上無限大のアドレス数

IPv6アドレス空間

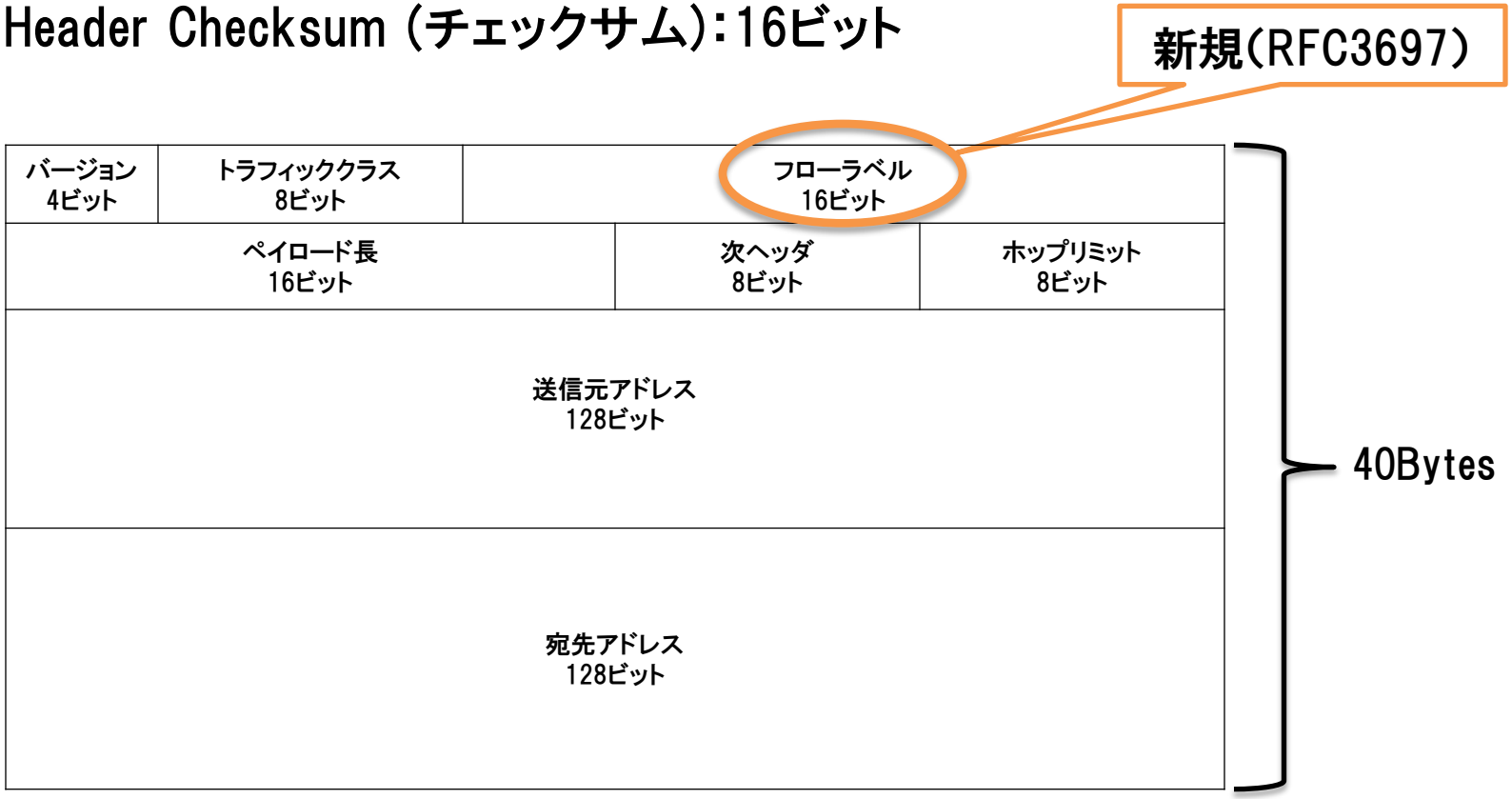
IPv4アドレスの枯渇によって？－②

- IPv4アドレス/ IPv6アドレスの共存(Dual Stack)
  - 開発業者、サービス業者などの負担が2倍？
- IPv4アドレスの延命
  - LSN
    - ✓ ポート数不足
    - ✓ P2Pなどのエンド・ツー・エンドサービスへの影響
  - 事業者間での譲渡
- セキュリティ(IPv6における主な懸念事項)
  - NAT
  - ICMPv6 (NDP)
  - Teredo

IPv6ヘッダ

IPv6より変更、廃止されたヘッダ

- IHL（ヘッダ長）：4ビット
- Identification（識別子）；16ビット
- Flags（フラグ）：3ビット
- Header Checksum（チェックサム）：16ビット

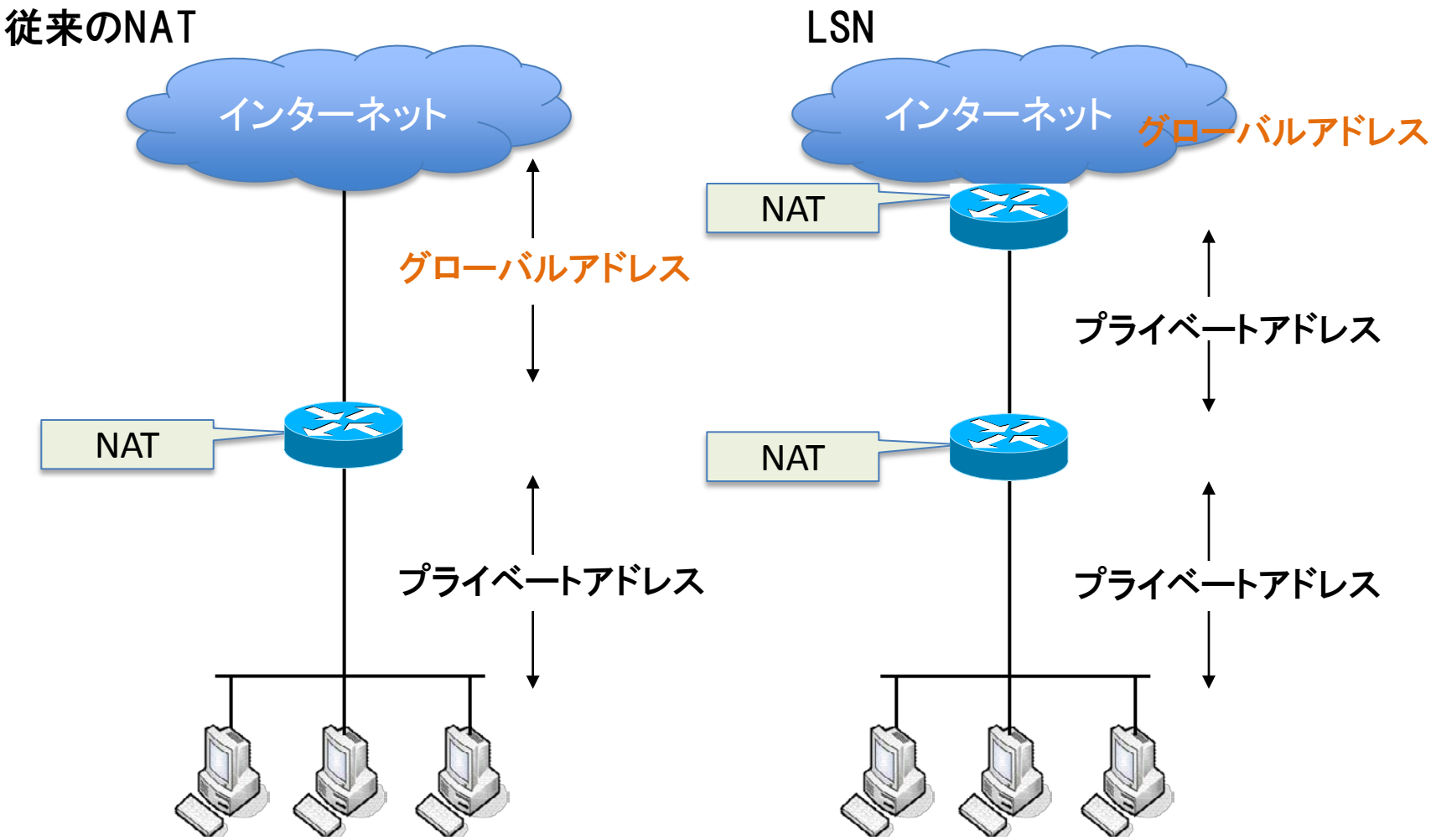


NAT

- IPv4環境におけるNAT
  - グローバルIPアドレスが足りない(IP 1/8/16…)
  - セキュリティ面　→　内部IPアドレスの隠蔽
  - プライベートアドレスの重複
  - NAT環境下で不向きなサービス
    - ✓ IPSEC
    - ✓ P2P
    - ✓ SIP

- IPv4延命によるNAT
  - LSN
    - ✓ NAT444:NATの多重
    - ✓ NAT64:企業、ユーザにはIPv6を配付、ISPでIPv4に変換

LSNとは



ICMPv6

- Path MTU Discovery
  - MTUを調べるための機能
- NDP
  - NS（近隣要請パケット）
  - NA（近隣通知パケット）
    - ✓ IPv4ではARPを使用していたが、IPv6ではNDP(近隣探索プロトコル)を使用
  - RS（ルータ要請）
  - RA（ルータ応答）
    - ✓ ネットワークアドレスプレフィクスやゲートウェイアドレスなどの情報の要求と応答
  - リダイレクトメッセージ

ICMPv6

IPv4 ICMP

タイプ	機能
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect
8	Echo Request
9	Router Advertisment
10	Router Solicitation
11	Time Exceeded
12	Paramter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request（未使用）
16	Information Reply（未使用）
17	AddressMask Request
18	AddressMask Reply

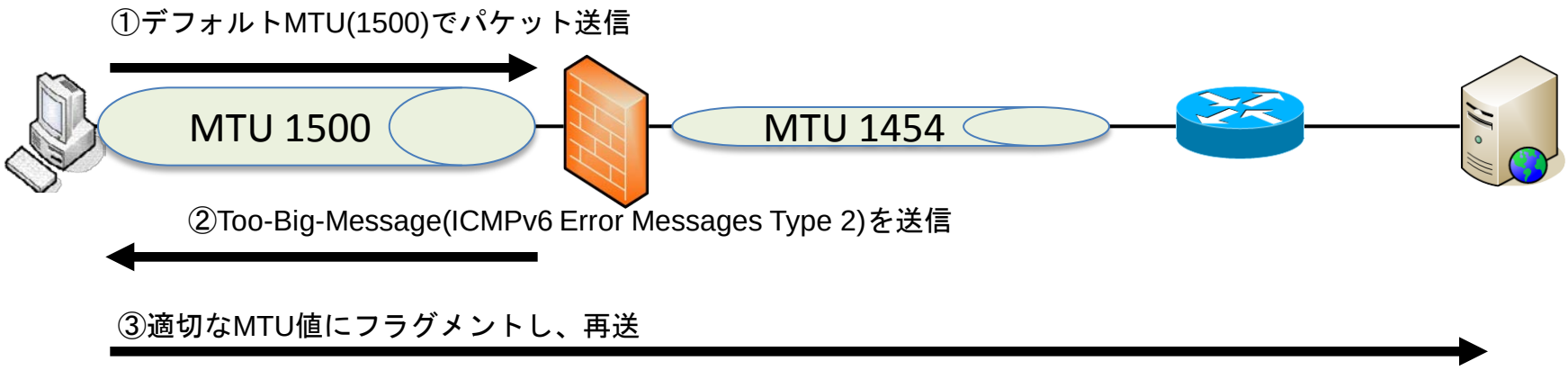
Ping

ICMPv6 情報メッセージ

タイプ	機能
128	Echo Request
129	Echo Reply
130	Multicast Listener Query
131	Multicast Listener Report
132	Multicast Listener Done
133	Router Solicitation
134	Router Advertisement
135	Neighbor Solicitation
136	Neighbor Advertisement
137	Redirect Message
138	Router Renumbering
139	ICMP Node Information Query
140	ICMP Node Information Response
143	Version 2 Multicast Listener Report
144	Home Agent Address Discovery Request
145	Home Agent Address Discovery Reply
146	Mobile Prefix Solicitation
147	Mobile Prefix Advertisement
128 - 255	Informational Messages

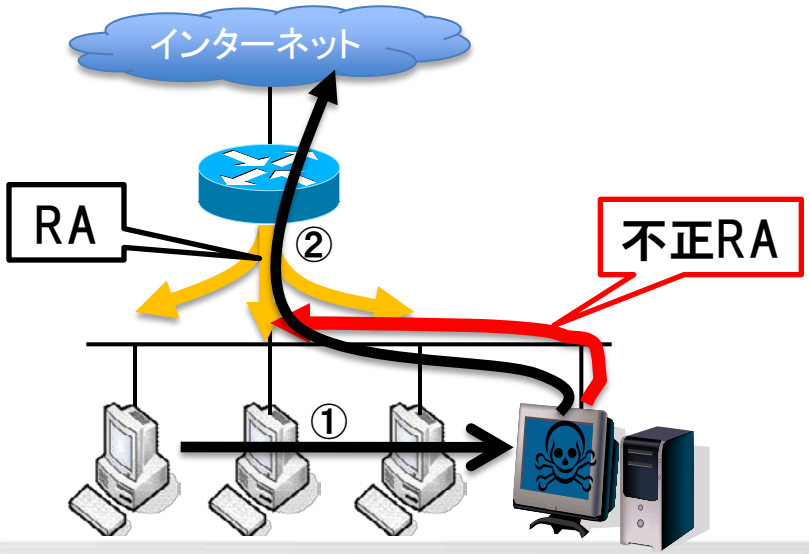
ICMPv6　Path MTU Discovery

- 送信元から宛先までの経路上において全てのリンクをフラグメントなしで通過できる最小のMTUを探索し、最小サイズでパケットを送る
  - 経路途中のルータでのフラグメントはしない
  - ルータの負荷軽減
  - FWもルータとして考えると、FWから送信されるアクセス制御の許可が必要



ICMPv6　RS/RA

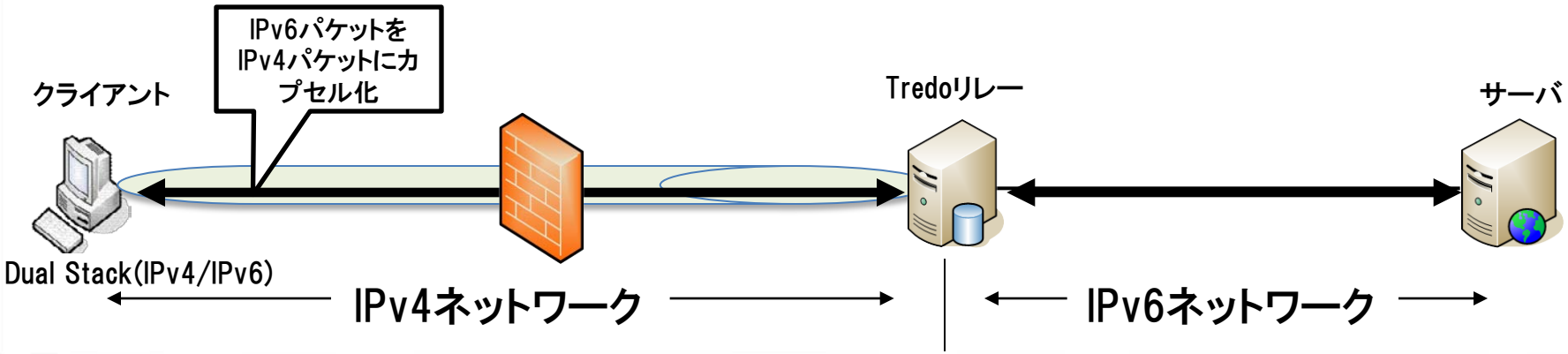
- ルータはローカルリンク内のノードにネットワークプレフィックスを通知(RA)し、ノードが自動的にIPv6アドレスを生成(ステートレスのIPv6アドレスの自動生成)
  - 不正RA
  - 不正DHCPサーバ(IPv4と同じ脅威)
  - 盗聴、改ざん、DoS



対策例)
- SWによる制限
- SeND (Secure Neighbor Discovery RFC 3971)
- 不正パケット監視
  - NDPMon　など
- パーソナルFWによる制限

Teredo

- IPv4プライベートアドレス環境下におけるNATに対応
- Windows XP SP1以降、Windows Vista/7標準実装
- Windows Vista/7　自動トンネル有効
  → 知らぬ間にFWをバイパスされる？
  → UDPポート 3544の制御
  ※6to4 → IPv4グローバルアドレスを使用
  プレフィックス2002:<aabb>:<ccdd>::/48 （RFC 3056,3068）



まとめ

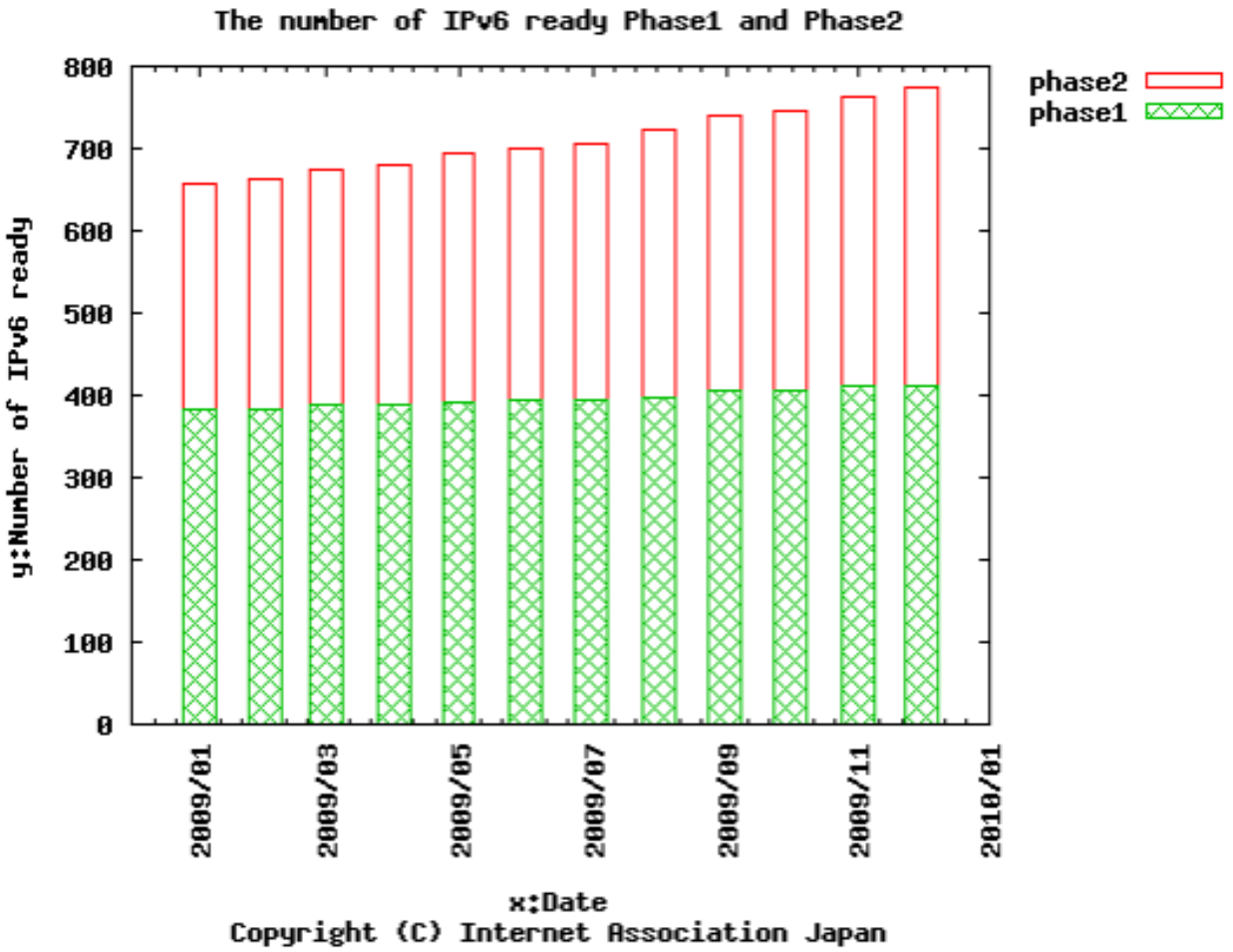
- セキュリティ対策
  - エンド・ツー・エンド通信が可能になることで、アクセス制御は厳格に
  - RHT0: Type0ルーティングヘッダ(ソースルーティング)を付加したIPv6パケットを送信することで、DoS攻撃が可能となる。RFC 5095の「Deprecation of Type 0 Routing Headers in IPv6」により、廃止。
  - フラグメントを悪用した攻撃
  - レイヤ4以上の攻撃はIPv4と同じ手法で可能なため、各セキュリティ機器(FW,IDS/IPS,WAF,UTMなど)などのIPv6対応が必要
  - マルウェア、ウイルス　など
- IPv4との仕様が異なる点を把握
  - ICMPv6(NDP)、DHCPv6、PathMTUDなど
- IPv6の挙動を把握
  - デュアルスタックにおいては、IPv6が優先されるOSもあり
- IPv4、IPv6環境における発信元の追跡(ログ管理)
  - トランスレータ環境におけるログ収集
  - 複数IPアドレスを持つノードの監視・管理

IPv6対応製品の確認

- SSAC(Survey of IPv6 Support in Commercial Firewalls)
  - http://www.icann.org/en/committees/security/
- ICSA labs IPv6 Capable Security Products
  - http://www.icsalabs.com/technology-program/ipv6/ipv6-capable-security-products
- IPv6 Ready
  - http://www.ipv6ready.org/
  - Phase-1:「最小限のIPv6サポートを証明することです。」
  - Phase-2 :「IPv6フォーラムはベンダに対してIPv6 Ready Logo Phse-2の取得を強く推奨しています。Phase-2ロゴはIETF仕様書における“MUST”と推奨される“SHOULD”の項目を全て含むテストによって最適な適合性を証明します。」

IPv6対応状況

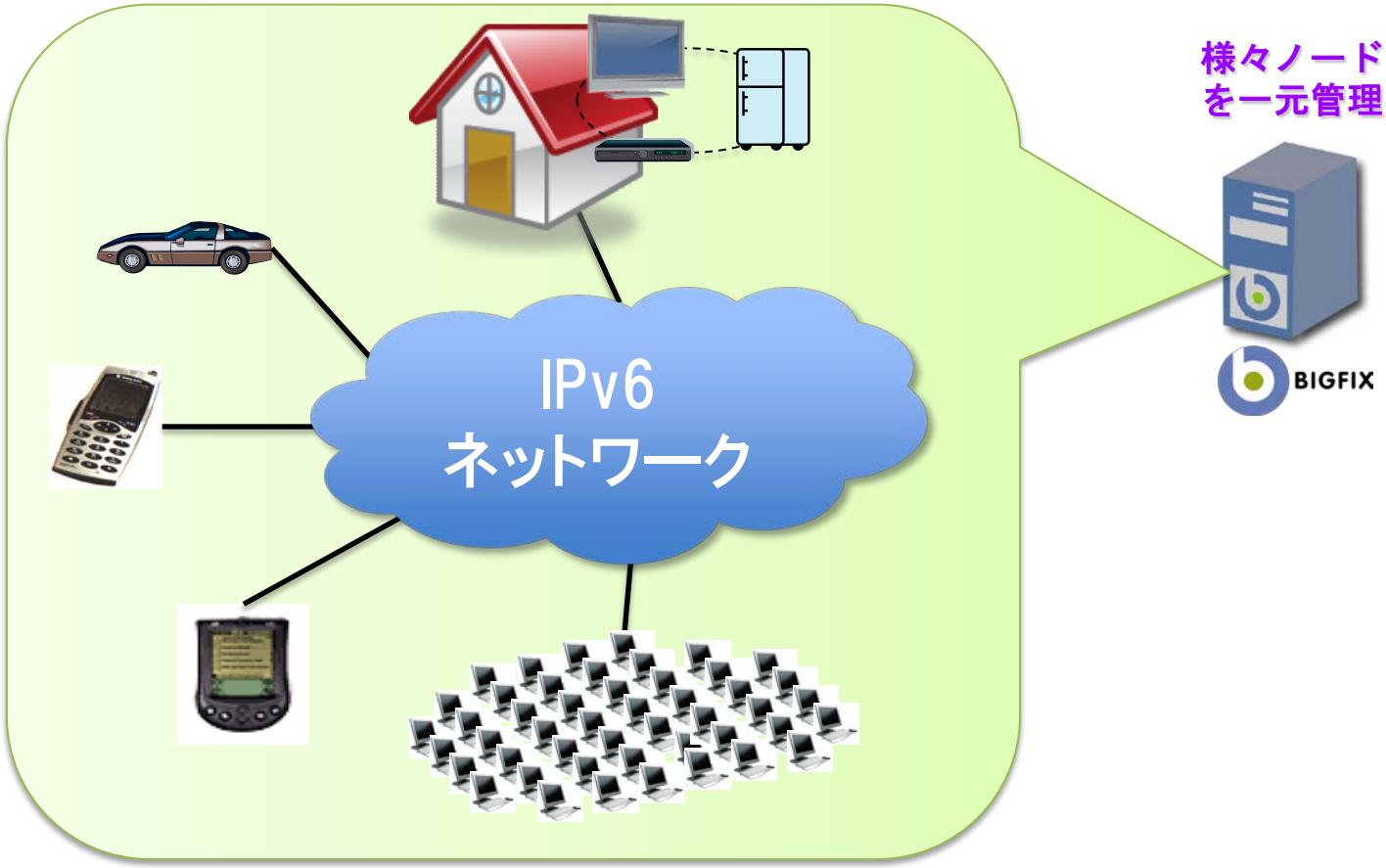
Phase1とPhase2の総登録機器数[年間]



Source：IAJAPN

IPv6エンドポイント管理ソリューション

・10万台を超えるノードの管理であっても、たった1台の専用サーバで運用できます。



全世界で7,500,000台以上のノードに導入されています。

Infosec
Risk Management Professionals