基礎からわかる DNS、DHCP、IPAMな4日間

INFOBLOX DDI WEEK ONLINE

INFOBLOX DDI Week Online DAY 3 – DNSセキュリティ

Infoblox株式会社
シニア ソリューション アーキテクト

石井 勝徳

Infoblox の歴史と進化

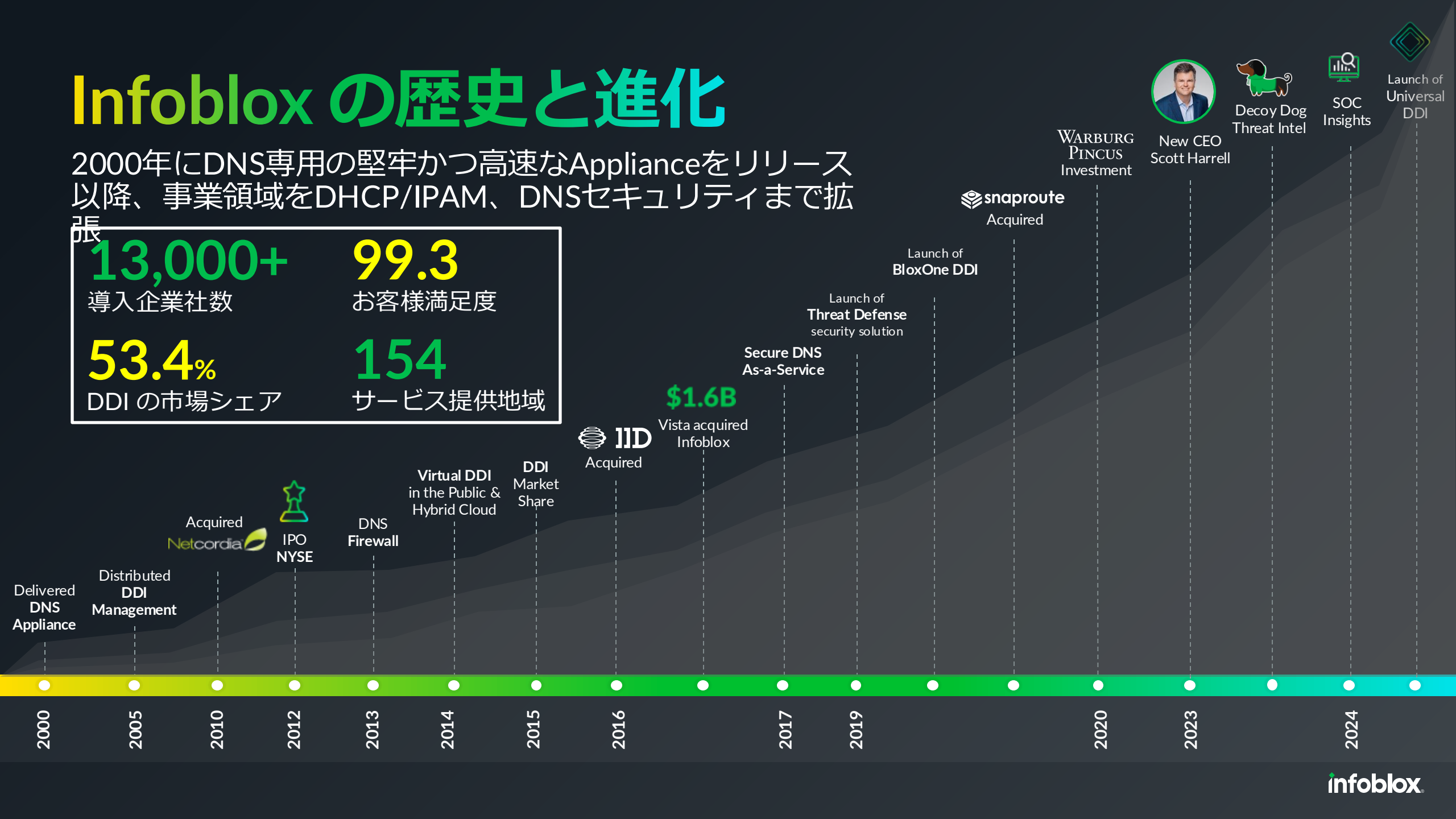
2000年にDNS専用の堅牢かつ高速なApplianceをリリース以降、事業領域をDHCP/IPAM、DNSセキュリティまで拡張

13,000+
導入企業社数

99.3
お客様満足度

53.4%
DDI の市場シェア

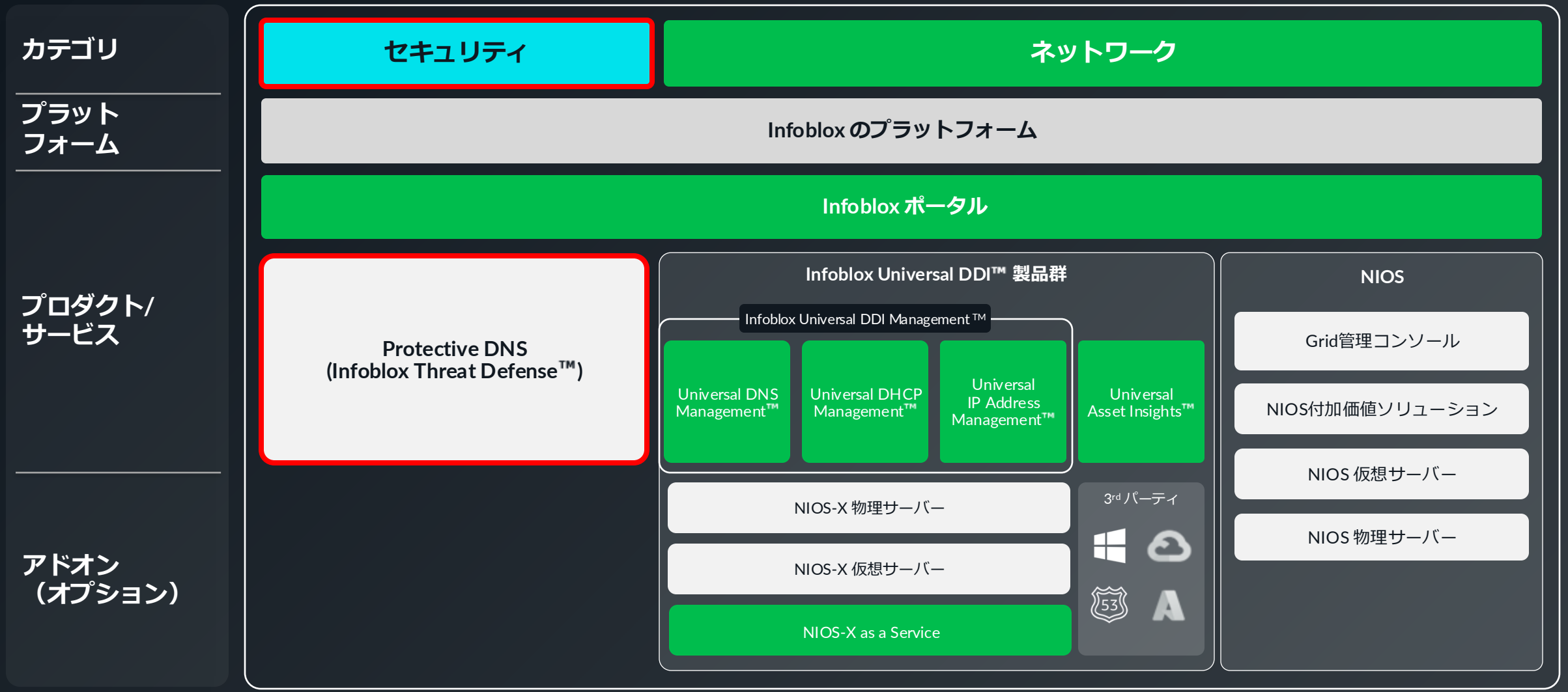
154
サービス提供地域



infoblox

ビジョン
ネットワーク&セキュリティ統合プラットフォーム

Infoblox プロダクト ポートフォリオ



AGENDA

- DNSセキュリティの必要性
- DNSを悪用した高度サイバー攻撃最新事例
- 各国政府機関での対応状況
- セキュアなDNS導入ガイドライン
- Protective DNS (Threat Defense™)の実力

infoblox

DNSセキュリティの必要性

高度サイバー攻撃とDNS

DNSはサイバー攻撃者にとっての抜け道

2022年 米国NSA（国家安全保障局）調査結果

92% のサイバー攻撃が**DNSを悪用**

- 悪意のあるサイトへリダイレクト
- C&Cサーバーとの通信
- マルウェアの送り込み
- データ漏えい

68% の企業・組織が**DNSは監視対象外**

- ログの記録なしが大半
- インシデントの特定が出来ないケース多い

46% がDNS経由での**データ漏えいを経験**

6億円 のデータ漏えい後の**追加コスト**

*平均合計コスト 4M USD (1ドル 150円換算)

Sources: National Security Agency, July 2022, Symantec Internet Security Threat Report, April 2017
SC Magazine, December 23, 2014, IBM Data Breach Report 2022

infoblox.

高度サイバー攻撃でDNSを悪用

JPCERT/CCから様々な攻撃段階/内容でDNSサーバーのログは有効であると発表

攻撃段階		ログで検知可能な攻撃内容	ログ取得対象機器
1	偵察	-	-
2	武器化	-	-
3	デリバリ	攻撃者によるマルウエア添付メールの送信	メールサーバ
		攻撃者によるマルウエア設置サイトへの誘導メールの送信と誘導	メールサーバ Webプロキシサーバ DNSサーバ
4	エクスプロイト	コールバック（Webプロキシサーバを介さない外部への通信）	Firewall DNSサーバ
		コールバック（HTTP, HTTPS等のプロトコルによる外部への通信）	Webプロキシサーバ DNSサーバ
5	インストール	-	-
		-	-
6	C&C	コールバック（Webプロキシサーバを介さない外部への通信）	Firewall DNSサーバ
		コールバック（HTTP, HTTPS等のプロトコルによる外部への通信）	Webプロキシサーバ DNSサーバ
		感染活動 （脆弱なPCや内部サーバの探索など）	Firewall
		ファイルサーバなどへのアクセスや権限の奪取	ADログ Firewall
7	目的の実行	コールバック（Webプロキシサーバを介さない外部への通信）	Firewall DNSサーバ
		コールバック（HTTP, HTTPS等のプロトコルによる外部への通信）	Webプロキシサーバ DNSサーバ
		機密情報持ち出し (メールサーバ経由)	メールサーバ DNSサーバ

92% の高度サイバー攻撃でDNSを悪用 (サイバーキルチェーンの5/7ステップ)

68% の企業・組織がDNSは監視対象外 (多くの企業ではログが記録されていない)

Source: JPCERT/CC高度サイバー攻撃への対処におけるログの活用と分析方法（最終更新: 2022-05-23）
https://www.jpcert.or.jp/research/apt-loganalysis.html

infoblox

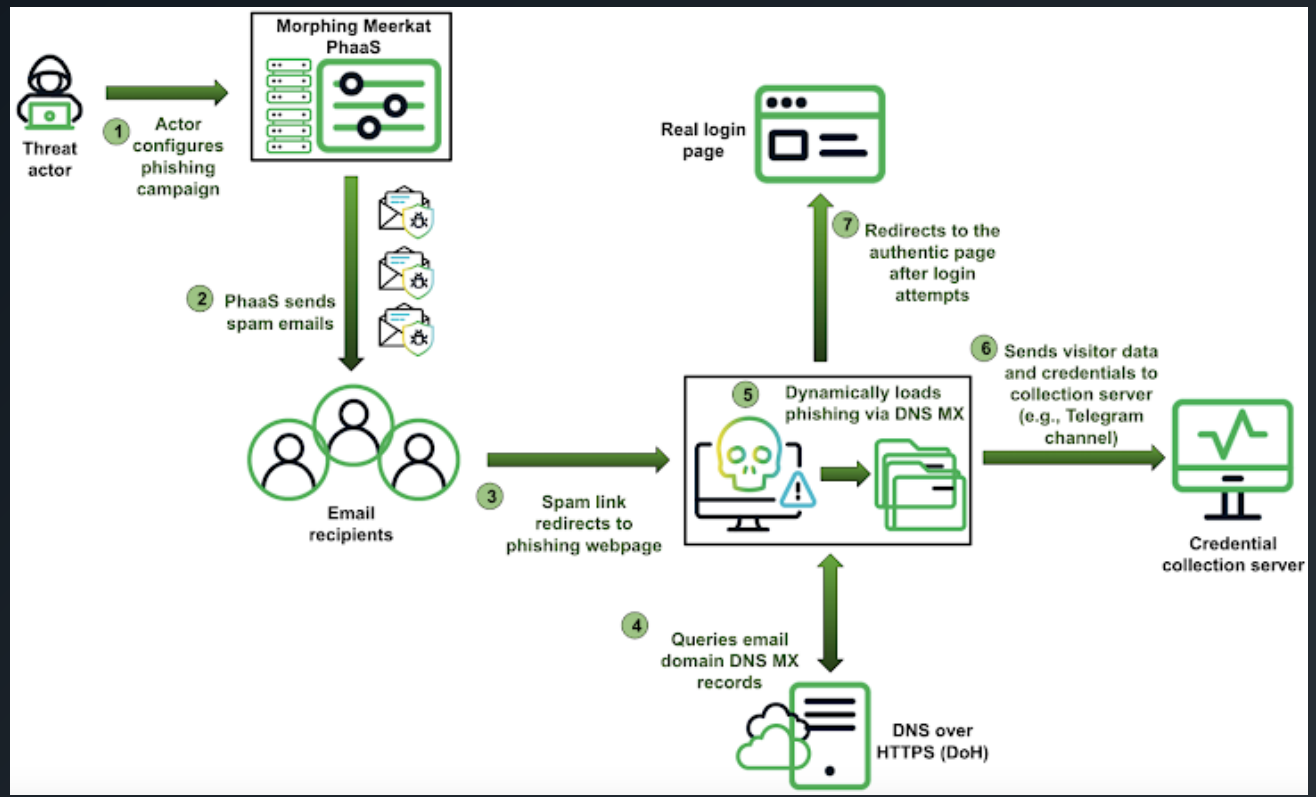
infoblox

DNSを悪用した高度サイバー攻撃の最新事例

Morphing Meerkat (モーフィング ミーアキャット)

MORPHING MEERKAT (モーフィング ミーアキャット)

2024年4月2日 INFOBLOXが発見した高度なフィッシング攻撃基盤



- 洗練された攻撃プラットフォーム
  フィッシング・アズ・ア・サービス（PhaaS）
- DNS MXレコードの悪用
  受信者のメールサービスプロバイダーを特定、
  それに応じた偽のログインページを動的に生成
  （Gmail、Outlook、AOL、Office 365、Yahoo）
- 100以上のブランドのなりすまし
- DNS over HTTPS（DoH）の悪用
  DNSクエリを暗号化するDoHを利用し、
  セキュリティ監視を回避
- 日本語対応
  日本企業も標的となる可能性あり

・InfobloxのDNSセキュリティサービス（Threat Defense）では、本攻撃に対応、ブロック可能
・欧州大手携帯電話会社では、高リスク（DNS脅威アクター）インテリジェンスの導入により、アラートが倍増

攻撃の詳細（弊社ブログ）
https://note.com/infoblox/n/n93b0fb5bf06e

infoblox

各国政府系機関における対応状況

Protective DNS導入を推奨

各国政府機関がDNSに対するセキュリティを推奨

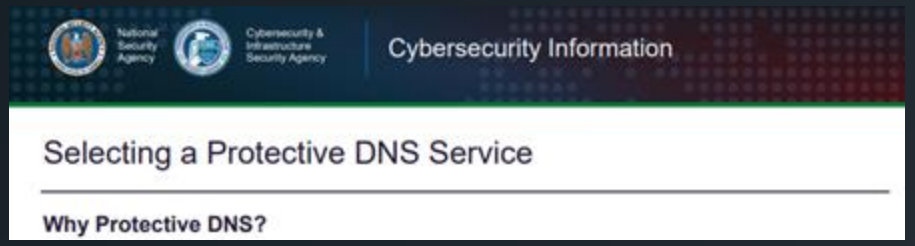
米国のサイバーセキュリティを所管するCISA が、保護ドメインネームシステム (PDNS) を連邦政府機関向けに一般提供開始（2022年 9 月 27 日）

https://www.cisa.gov/blog/2022/09/27/cisa-launches-its-protective-dns-resolver-general-availability-federal-agencies

英国でも既に保護ドメインネームシステム (PDNS) を運用しており、中央省庁、自治体などの組織で利用（2017年4月）

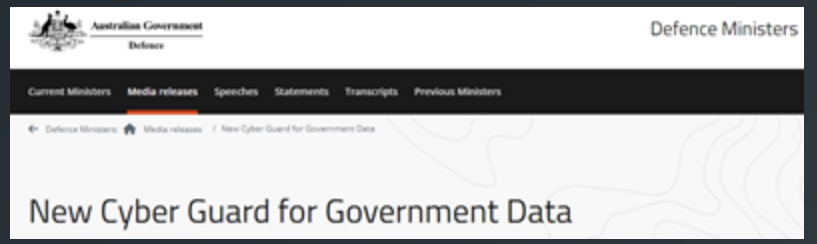
https://www.ncsc.gov.uk/news/uk-public-sector-dns-service

米国CISAと英国NCSCが共同でユーザーと管理者が保護DNS サービスを使用する利点を検討し、詳細についてまとめたシートを公表（2021年 5 月）



https://media.defense.gov/2021/Mar/03/2002593055/-1/-1/0/CSI_Selecting-Protective-DNS_UOO11765221.PDF

オーストラリアでも独自の保護DNSサービスを政府機関で利用（2021年10月）



https://www.minister.defence.gov.au/media-releases/2021-10-14/new-cyber-guard-government-data

infoblox

NISC(内閣サイバーセキュリティセンター)がDNSセキュリティサービスを提供開始

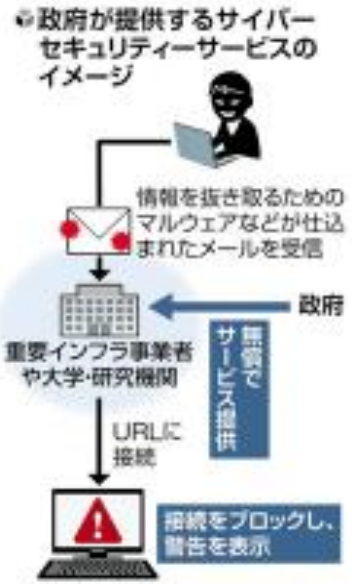
インフラ事業者や大学を国が守る、悪性サイトへの接続防ぐサービスを政府が無償提供

2024/05/15 15:00　この記事をスクラップする

政府は今夏にも、医療機関などの重要インフラ（社会基盤）事業者や大学・研究機関に対し、サイバーセキュリティーを強化するサービスの無償提供を始める。情報を抜き取るマルウェア（悪意のあるプログラム）などが仕込まれた悪性サイトへの接続を未然に防ぐ仕組みで、国民生活に直結するインフラを守る体制作りにつなげたい考えだ。

複数の政府関係者が明らかにした。内閣サイバーセキュリティセンター（ＮＩＳＣ）は今年度予算に政府機関などのサイバーセキュリティー強化関連として４９・３億円を計上しており、その具体策の一つとして実施する方針だ。

それぞれの機関はサイバー攻撃への防御策を講じているが、政府がより能力の高いサービスを提供し、脆弱（ぜいじゃく）性が指摘される国内のサイバーセキュリティーの底上げを図る。対策を通じ、先端技術の外部流出を防ぐ狙いもある。



提供するサービスは、米国や英国などで導入が進む「プロテクティブＤＮＳ（ドメイン・ネーム・システム）」だ。メールなどに届いたＵＲＬを通じ個人情報を抜き取るフィッシングサイトに誤って接続しようとすると、ブロックされたり、警告が発出されたりする。マルウェアが仕込まれた不審なファイルをダウンロードしようとすると、警告が表示される。

サービスの提供先としては、機能不全になると国民生活への影響が甚大な医療や水道といったインフラ事業者や、先端技術研究を担う大学・研究機関、独立行政法人などを想定する。今後、内閣府や文部科学省などの関係府省庁を通じて利用を呼びかける。サービス利用に伴い得られた悪性サイトの情報はＮＩＳＣで蓄積して分析し、さらなる能力の向上にも役立てる。

近年、医療機関や大学・研究機関へのサイバー攻撃は相次いでいる。３月には、鹿児島県の医療機関が攻撃を受け、診療の一部を制限する事態になった。政府は、先端技術に関する情報を盗むためのサイバー攻撃への警戒も強めており、新たな対策を講じる必要があると判断した。

（読売新聞Web版 2024年5月15日）

CISA(米国サイバーセキュリティ・社会基盤安全保障庁)がInfobloxのドメイン緩和サービスを推奨

- Infobloxは、Threat DefenseプラットフォームとAPI統合を通じて充実した脅威インテリジェンスを提供し、顧客が脅威をよりよく理解し、優先順位を付け、対応できるようにします。高品質の機械可読データ（AISフィードを含む）に加えて、Infobloxはドメイン緩和サービス「テイクダウン」とフィッシング分析サービスを提供しています。

https://www.cisa.gov/sites/default/files/publications/FactSheet_SCS_Overview_9-2021_.pdf

infoblox

セキュアなDNS導入ガイドライン

Secure DNS Deployment Guide
NIST SP 800-81 Rev. 3 Initial Public Draft

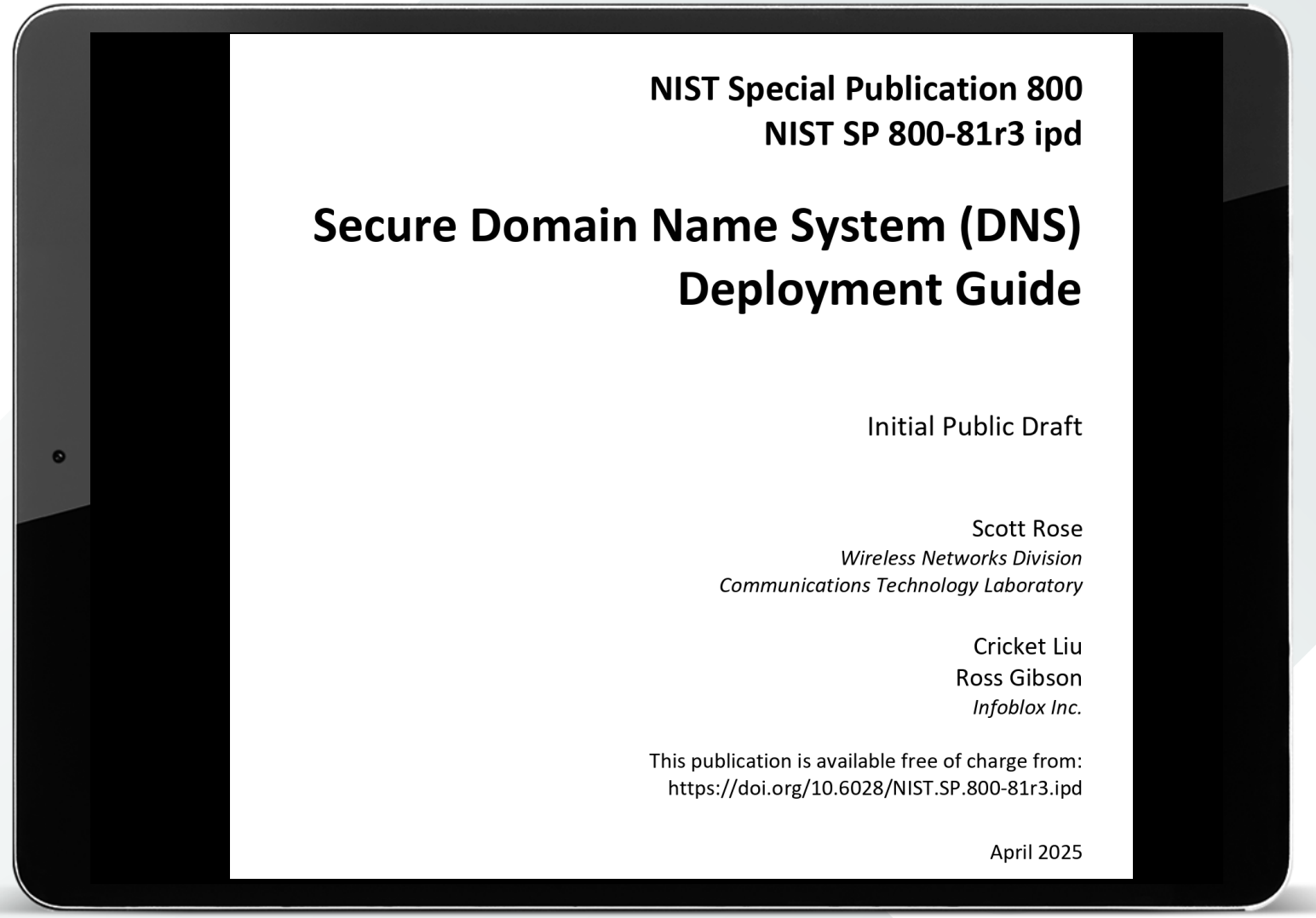
NIST SP 800-81とは何か？

DNSのベストプラクティスに関する権威ある文書

世界的な技術およびサイバーセキュリティのベストプラクティスにおける最高基準とされるNIST（米国国立標準技術研究所）発行の文書。

2013年 （約12年）ぶりにNIST SP 800-81のドラフト版が2025年4月10日に公開。

現在はコメント募集期間の開始日であり、この期間は5月26日まで続く予定。



対象者の変化

旧 800-81

当時、DNSはITインフラ部門が主な対象部門であった。

新 800-81

今や、DNSはセキュリティとレジリエンシーの問題であり、ITインフラだけでなく、CISOとCIOも対象となる。

38 **Table of Contents**

NIST SP800-81 第3版 初期公開ドラフトのサマリー

DNSはミッションクリティカルであり、かつセキュリティコントロールの基礎である

	項目	確認事項	主な理由	必要な対策
1	New **プロテクティブDNS** 及びDNSログの活用 （2.1 章）	• プロテクティブDNSが導入され、悪意あるドメインへのアクセスをブロックしているか • DNSログが記録され、SIEMシステムと統合されているか	• DNSはネットワーク通信に不可欠なものであり、DNS通信を監視、管理することで効果的なセキュリティ対策が実現できる • DNSをフォレンジックに活用することで、ユーザー活動の可視性と監査可能性を高める	• プロテクティブDNSの導入 • DNSログ記録とSIEM連携によるフォレンジック強化
2	DNSプロトコルの保護 （暗号化DNS） （2.2 章）	• **DNSトラフィックが暗号化されているか（DoT、DoH、DoQ）** New • DNSSECが有効化され、署名および検証が行われているか • Lame Delegation（ゾーン委任）、ダングリングCNAME、リソースレコード（RR）のTTL値が適切かなどドメインネームのハイジーンへの対応有無 New	• 暗号化されていないトラフィックは盗聴や改ざんのリスクがある • DNSSECはデータの真正性と完全性を保証するが、内部ゾーンの署名は推奨されない • 誤設定はサービス停止や悪用リスクを高める	• DNSトラフィックの暗号化 • DNSSECの適切な実装 • ドメインネームハイジーンの改善
3	DNSサーバー/インフラの堅牢性 （2.3 章）	• サーバが専用DNSサーバとして運用されているか • プライマリサーバが「Hidden Primary」として構成されているか • 権威サーバがネットワーク/地理的に分散されているか • 再帰サーバが内部ホストからのクエリのみを受付けるよう制限されているか	• 専用サーバでない場合、攻撃対象領域が拡大し脆弱性が悪用される可能性がある • 隠しプライマリは攻撃対象を減らす • 分散配置はDoS/DDoS攻撃に対する耐性を高める • 外部公開サーバが再帰クエリを許可している場合、キャッシュポイズニングやDoS攻撃のリスクが高まる	• DNSサーバの役割分離 • 耐障害性と可用性の向上 • スタブリゾルバの保護

プロテクティブ DNSの採用とログ活用

DNSを名前解決だけではなく、セキュリティツールとして活用する必要がある

プロテクティブDNSを展開する目標には以下が含まれます。

- ドメイン名解決の時点で、通常は悪意のある活動が開始される前に、**有害なトラフィックをリアルタイムでブロックまたはリダイレクト**する
- 組織のポリシーに準拠しないドメイン名を分類したり、既知の悪意のあるアクターのリストと照合したりすることで、トラフィックのカテゴリを**DNSでブロックする**
- デジタルフォレンジックとインシデント対応を容易にするために、リアルタイムおよび**過去のDNSクエリと応答データへの可視性を提供**する
- **多層防御の一環として、より広範なセキュリティエコシステムと統合**する（例：組織の資産（デバイス、クラウドワークロードなど）やユーザーに関するデータを、ブロックされたクエリのIPアドレスと関連付ける）
- 許可されていないサイトへのトラフィックをブロックするための規制上または契約上の要件（例：著作権侵害、法的制限）を遵守する組織の責任を促進する

暗号化DNS

暗号化DNSは、DNSにおける長年の課題であった**「ラストマイル」の脆弱性に対処**する

DNSトラフィックの暗号化（New）

- **盗聴やDNSスプーフィングを防止するため、DoT、DoH、DoQをサポート**するようDNSサーバを構成
- **プライバシーとセキュリティを向上**させるため、サーバ証明書を設定し、TLS暗号スイートがNIST SP 800-52に準拠する

DNSSECの適切な実装（R2からの継続）

- データの真正性と完全性を保証するため、外部公開ゾーンに対してDNSSEC署名を有効化
- 内部ゾーンの署名は避け、再帰サーバでDNSSEC検証を有効化
- ECDSAやEd448などの強力なアルゴリズムを使用し、鍵の寿命を1～3年に設定

ドメインネームのハイジーン（設定ミスの防止）（New）

- Lame Delegation（ゾーン委任の適切化）やダングリングCNAMEや類似ドメインを監視・修正できる仕組みの導入
- TTL値の適切な設定（例：5～30秒以上）

Microsoft がゼロトラストDNS（ZTDNS）を発表

DNSを暗黙のうちに信用している限り、本当の意味でのゼロトラストとは言えない

Announcing Public Preview of Zero Trust DNS

AditiPatange MICROSOFT
Apr 24, 2025

Deployment instructions for testing Public Preview of Zero Trust DNS (ZTDNS) on Windows 11 Insider builds.

In today's evolving cybersecurity landscape, traditional perimeter defenses are no longer sufficient . As organizations embrace the Zero Trust security model, ensuring that devices only communicate with trusted network destinations becomes paramount. We are excited to announce the public preview of Zero Trust DNS (ZTDNS), a new feature in Windows 11 Insider builds designed to enforce domain-name-based network access controls, enhancing your organization's security posture.

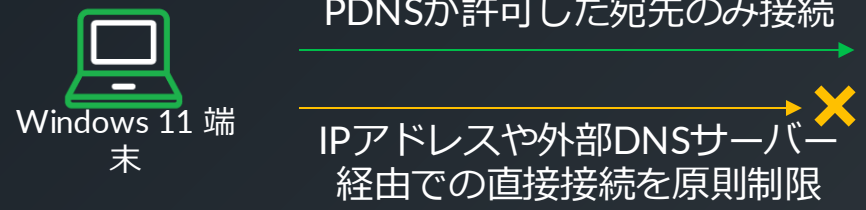
ZTDNS empowers enterprise IT administrators to natively apply outbound domain-name-based network access controls on Windows 11 endpoints. This helps prevent access to untrusted destinations, reducing the risk of a slew of network attacks from malware communication to data exfiltration.

What is Zero Trust DNS?

ZTDNS integrates the Windows DNS client with trusted Protective DNS (PDNS) servers to control outbound IP traffic based on domain names. When ZTDNS is configured on a Windows 11 device to use PDNS servers that support DNS over HTTPS (DoH) or DNS over TLS (DoT), ZTDNS ensures that:

参考：Microsoft Networking Blog「Announcing Public Preview of Zero Trust DNS」Apr 24, 2025

ゼロトラスト DNS （ZTDNS）の仕組み



- ZTDNSは、Windows DNS クライアントを信頼できるプロテクティブDNSを連携させ、不正ドメインへのアクセスを制御可能
- Widnows 11 端末が DoH もしくは DoT をサポートするPDNSサーバーを使用している場合、クライアント側に暗号化された DNS の使用を強制し、クエリは連携された PDNS サーバーにのみ送信される。
- その他全てのIPv4/v6送信トラフィックはゼロトラストの原則に従ってデフォルトでブロック
- 実行された送信接続ログはデバイス上で保持
- 上記にアプローチは、信頼できるPDNSサーバーが提供するDNS解決を通じて明示的に許可された宛先への接続のみを許可するという点で、ゼロトラストの原則にも合致している

infoblox

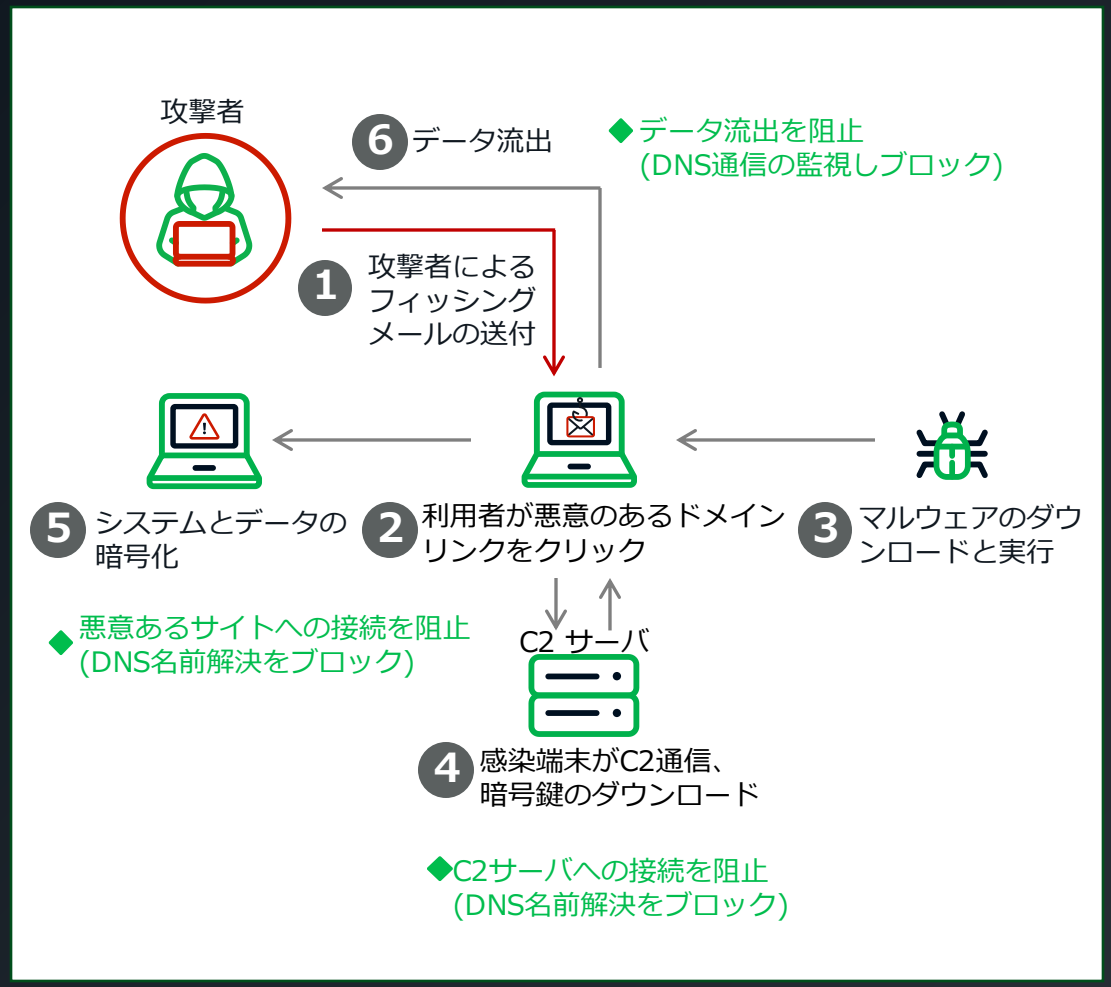
infoblox

Protective DNSの実力

Infoblox Threat Defense™

ランサムウェア攻撃におけるProtective DNS

ランサムウェアの動作を抑止、ユーザ保護を未然に提供



- ②エクスプロイト　フェーズ
  利用者が悪意のあるドメインリンクをクリック
  ー＞フィッシングリンクをクリックした際、ユーザーが悪意のあるドメインに接続しないようにブロックする。
- ④C&C通信　フェーズ
  感染端末がC2サーバへ通信し暗号鍵のダウンロード
  ー＞C2通信の接続をブロックする。
- ⑥目的の実行　フェーズ
  目的のデータをDNS通信経由で外部に送信する
  ー＞データ流出を検知すると通信を停止させる

PDNSサービスの特徴　～現代のIT環境に合致～

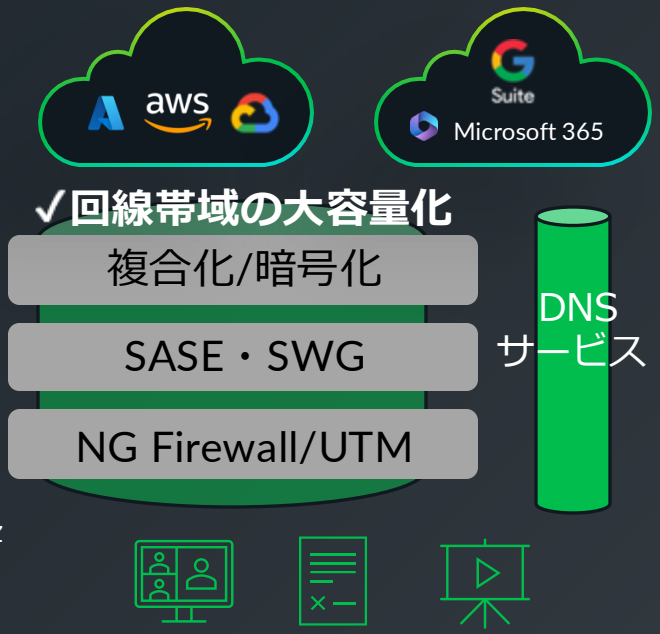
- DNSセキュリティは昨今のシステム環境に適合しやすい。
  - インターネット接続デバイスであれば、種類問わず導入できる。
    - IT(PC、スマートフォン、サーバ）、OT（カメラ、制御端末）
  - インターネット回線の大容量化、暗号化通信の高割合　により実通信の脅威解析は現実的でない。

✓インターネット接続
のマルチデバイス化

全てのデバイスは、
名前解決から通信を開始

✓高頻度の暗号化通信
名前解決後に発生する
アプリケーション
トラフィックの95%[*1]
が暗号化されている

*1:2023年版のZscaler ThreatLabz

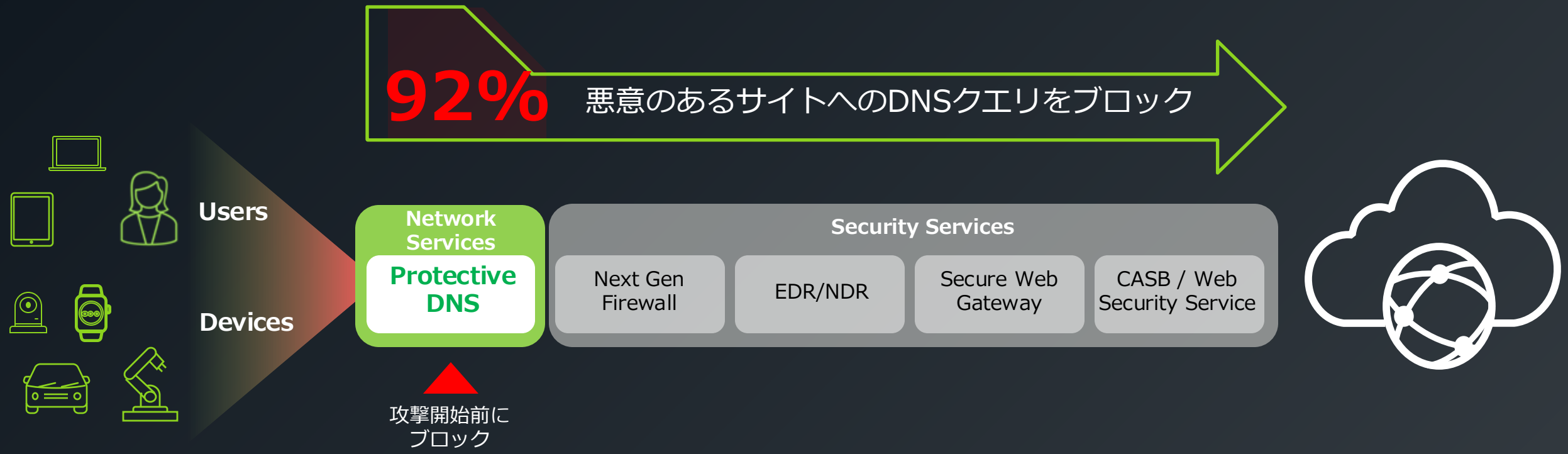


IT/OT問わず導入できる高い汎用性・現在IT環境に合致した低負荷セキュリティサービス

infoblox

PDNSサービスとは

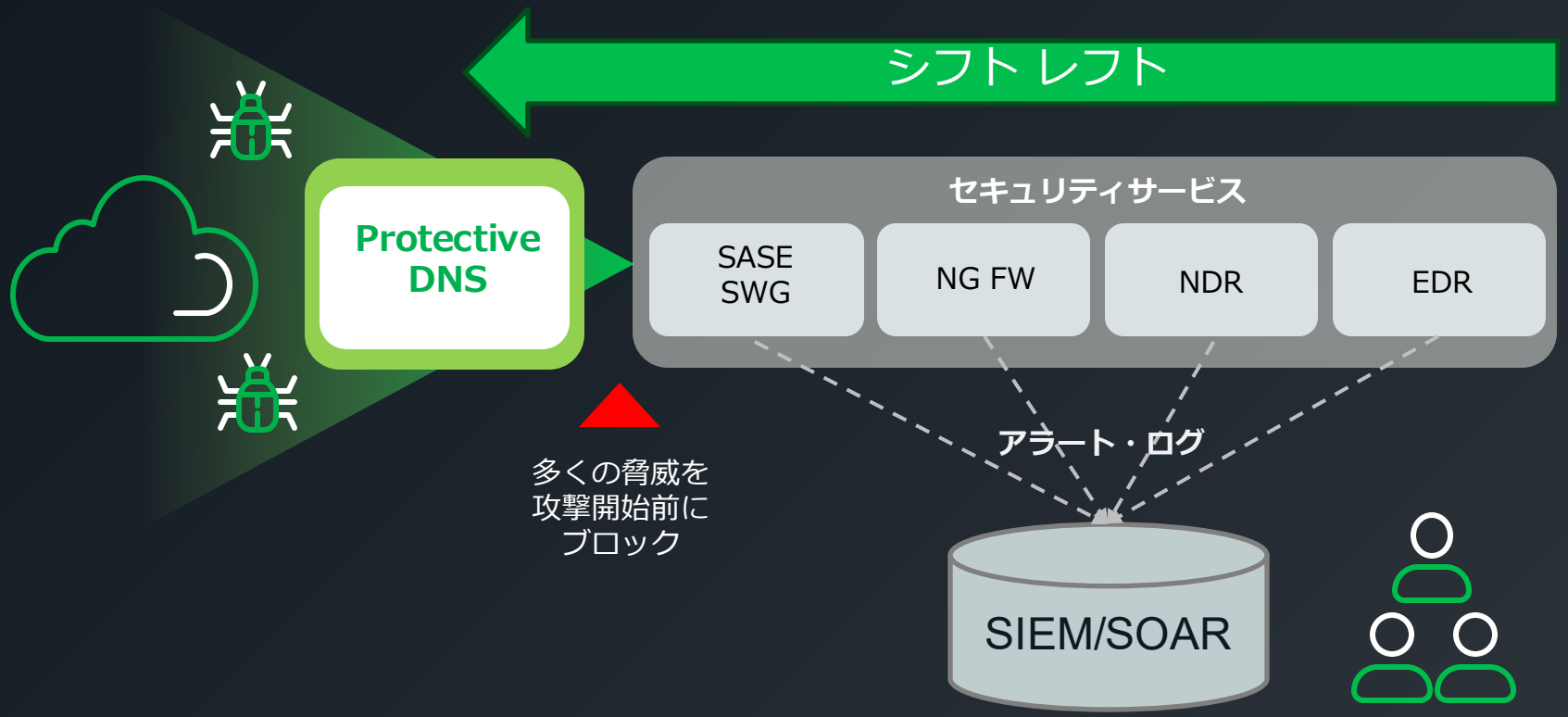
インターネットアクセスの一番最初に行われるDNSで不正通信を検知/ブロック



✓ セキュリティ製品のアラートを削減しセキュリティ運用負荷を軽減
（EDR等のセキュリティレスポンス活動にかかわる運用負荷を大幅に削減）
✓ 無駄なトラフィックを削減することで、通信・セキュリティ製品の負荷軽減

PDNSサービスの特徴　～コスト削減～

- DNSは全ての通信の起点であるため、PDNSサービスは通信の開始前に防御
- 無駄なトラフィック、アラートを削減することで、通信・セキュリティサービスの負荷軽減
- EDR等のセキュリティレスポンス活動にかかわる運用負荷を大幅に削減



PDNS導入により

・ セキュリティサービスのサイズ減！

・SIEM/SOARへのアラート・ログ減！

・SOC運用者の業務負荷減！

コスト削減も期待できる稀有なセキュリティサービス

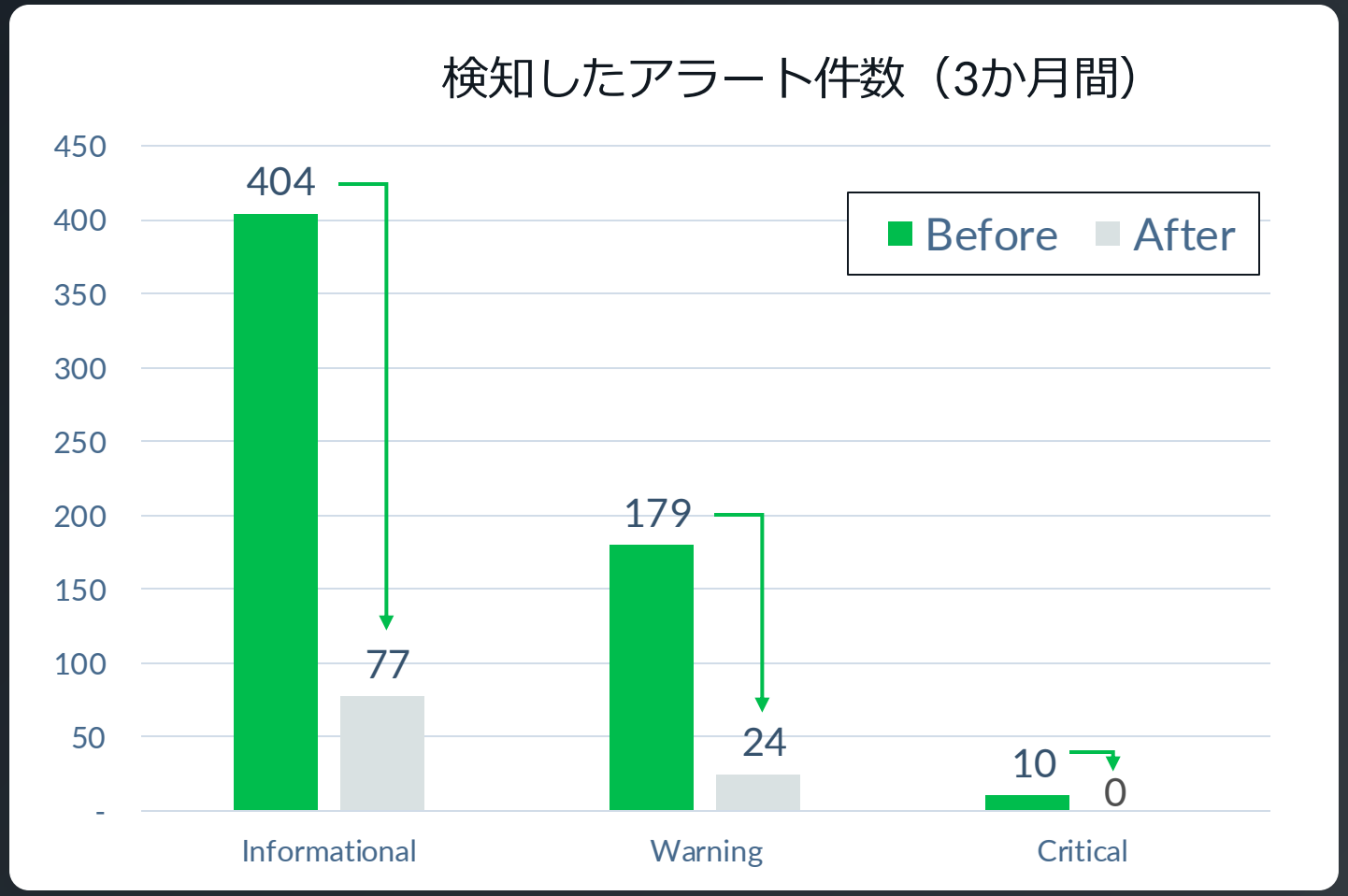
infoblox

PDNSサービスの効果　～お客様事例～

検知するアラート数が激減、SOCチームの運用負荷減

- **企業プロファイル**
  - 国　　:日本
  - 業種　　:重要インフラ
  - 従業員数　:約20,000人

- **導入済みセキュリティ製品:**
  - 次世代ファイアウォール
  - メール対策セキュリティ
  - エンドポイントセキュリティ（EDR）
  - ウェブフィルタリング など



PDNSサービス　～検知精度の高さ～

- Infoblox PDNSサービス　2023年の誤検出のエスカレーション率：**0.0002%**
  - 攻撃者が使用するツールのうち、唯一事前把握ができるDNSを利用
  - DDI(DNS,DHCP,IPアドレス管理）マーケットにおいてトップである50%のシェアを獲得。20年以上のオペレーションを通じて、DNSの専門知識、全世界のDNSトラフィックを観測できる設備等特異な能力
  - 独自の脅威解析手法：特許技術を使用した脅威のあぶり出し

Infobloxのアプローチ
・マルウェアが作成される前から脅威判定しユーザーを保護
・お客様環境で検知された75.4%の攻撃を実際の攻撃前に悪性判断

他社のアプローチ
・攻撃を受けてから脅威判定しユーザーを保護
・1日に数千の新規ドメインを作成する攻撃者に対応できない。

セキュリティサービス導入・運用負荷の原因である誤検知は、著しく低い

infoblox.

Infoblox Threat Intel: 悪性ドメインの解析例

パッシブDNS
毎日700億+
DNSイベント

ドメイン登録
時間、日付、登録者...

クエリ分布
地域、バーティカル、ボリューム...

DNSレスポンス
リゾルバ、地域、品種 ...

名前の特徴
類似性、既知のブランドの使用状況

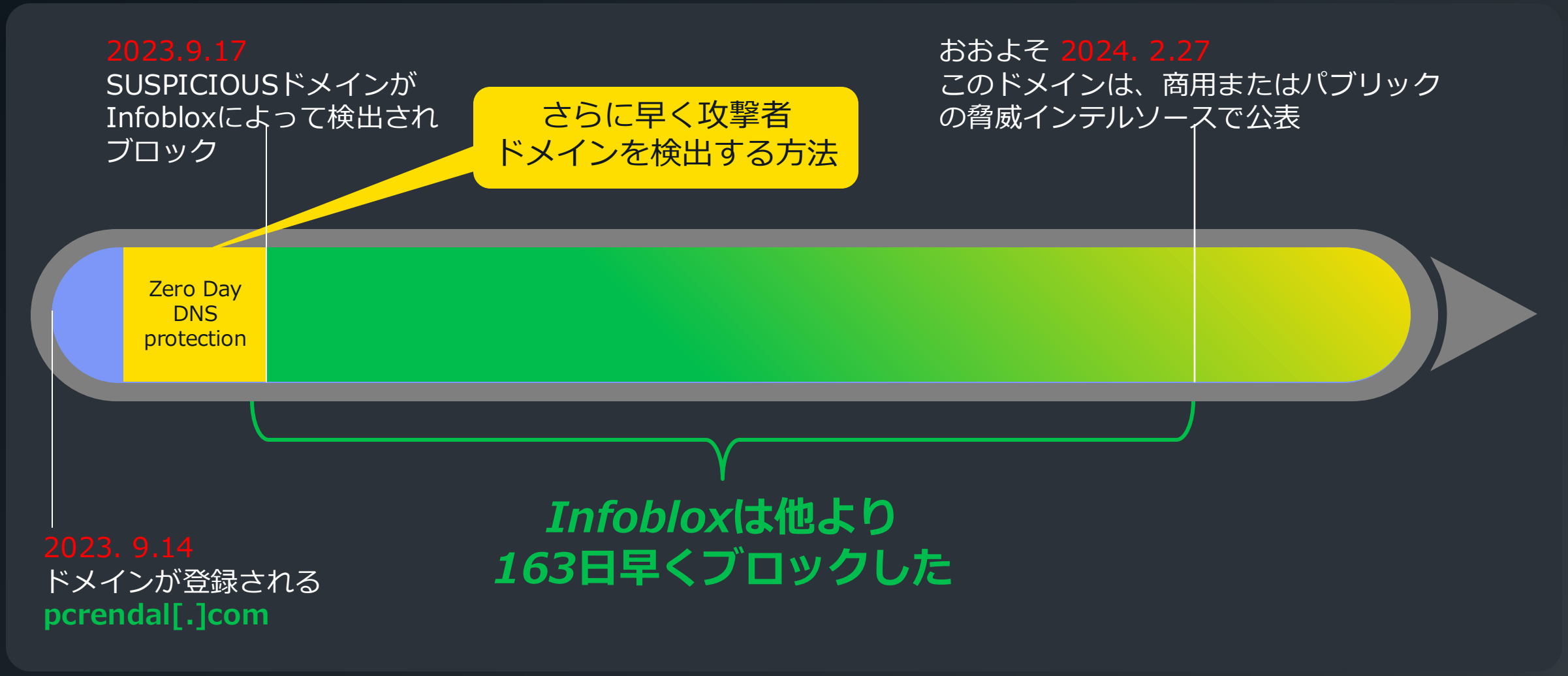
ネームサーバー
場所、評判、 ...

ホスティング
ドメインプロバイダー, 所在地, ...

ドメイン履歴
悪質なキャンペーンでの出現, ...

ドメインの普及率
ドメインの使用状況、関連システム、 ...

実際の検知例: BLACKCAT ランサムウェア



https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a

infoblox

INFOBLOX THREAT INTEL の実力

Infoblox Threat Intel Team は世界唯一のDNSエキスパート集団である

700億+
毎日分析される
DNSイベント数

400万
悪意のある不審
なドメインを
毎月発見し追加

63 days
攻撃前の平均
防御日数

75.4%
最初のDNSクエリ
前に検出された
脅威の割合

0.0002%
誤検知率