ソリューションノート

デジタルオペレーションレジリエンス法（DORA）と DNS

DNS のベストプラクティスを適用して DORA コンプライアンスを実現する方法

はじめに

デジタルオペレーションレジリエンス法（Digital Operational Resiliency Act、通称 DORA）は、金融機関のデジタルレジリエンスを強化することを目的とした欧州連合（EU）の規制です。2025年1月17日に施行され、銀行、保険会社、投資会社、その他の金融機関が、サイバー攻撃やシステム障害などの ICT（情報通信技術）の混乱に耐え、対応し、回復できることを保証します。

DORAは 9 章から構成されており、それぞれに対応する規制技術基準（RTS）が定められています。銀行やその他の従来の金融サービス組織に加え、この法律とその基準は、暗号資産サービスプロバイダーやサードパーティの ICT プロバイダーといった金融セクター企業にも適用されます。PwC によると、DORA の遵守義務は 22,000 以上の事業体に適用されます。[1]この指令は EU 域内に所在する企業だけでなく、域内で事業を運営または取引するあらゆる金融機関にも適用されます。

DORA の第 1 条は、ネットワークおよび情報システムのセキュリティに関連するさまざまな規制基準を定めています。対象となるトピックには、リスク管理、インシデント報告、レジリエンステスト、ICT サードパーティリスクの管理、サイバー脅威情報とインテリジェンスの共有が含まれます。[2]

これらの基準が進化するにつれ、これらに関連する金融機関にとっての具体的な要件がより明確になります。例えば、*脅威主導型侵入テストに関連する要素を規定する RTS 草案に関する最終報告書*[3]は、侵入テストの要件についてさらに明確にしています。報告書では、DORA の要件が、欧州中央銀行に関連する脅威インテリジェンスに基づく倫理的レッドチーム（TIBER-EU）フレームワークなど、他のセキュリティ関連の規制施策と相互運用できることが説明されています。報告書では、「[TIBER-EU フレームワーク]は、デジタルオペレーションレジリエンス法（DORA）に基づく脅威主導の侵入テストの要件を満たす上で、管轄当局と金融機関を支援することもできる」と述べられています。[4]報告書はまた、欧州中央銀行の文書『*Adopting TIBER-EU will help fulfil DORA requirements（TIBER-EU の採用は DORA 要件の達成に役立つ）*』にも言及しています。[5]

DNS は DORA コンプライアンスにどのように役立つか

Domain Name System（DNS）は、デバイス、アプリケーション、インターネットドメイン、データベース、クラウドリソース間のすべてのネットワークの相互作用において中心的な役割を果たします。DNS プロトコルを戦略的に管理および展開すると、プロアクティブなネットワークセキュリティ適用ポイント、デジタルフォレンジックの貴重なソース、迅速なインシデント対応の効果的な促進者としても機能します。そのため、DNS は、さまざまな DORA コンプライアンス活動の実行において金融機関を支援する独自の立場にあります。

- ICTリスク管理（第II章）
- ICT 関連のインシデント管理、分類、報告（第 III 章）
- デジタル運用レジリエンステスト（第 IV 章）
- ICT サードパーティリスク管理（第 V 章）
- 情報共有の取り決め（第 VI 章）

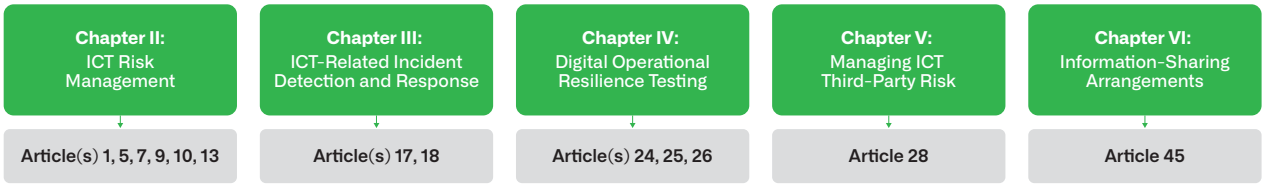

図 1. DNS が DORA コンプライアンス活動に貢献する領域

DNS の有効性は非常に高いため、特定の DORA 原則への準拠に加えて、多くの組織がほとんどの規制を満たすために DNS の機能を活用することでメリットを得られることに留意する必要があります。DNS はすでに組織のネットワークに統合されているため、まったく新しいテクノロジーと制御を導入するよりも、セキュリティと弾力性を強化するためのより実用的かつ効率的な方法を提供します。DNS が DORA の活動にどのように貢献できるかを検討する場合、事業体は規制の第 4 条に規定されている比例原則を適用する必要があります。

以下の推奨事項は、DORA ガイドラインの関連する章ごとに整理されており、それらが準拠する規制の特定の条項の注釈も付いています。

ICTリスク管理

多くの金融機関は DNS を「ネットワークの配管の一部にすぎない」と見なしていますが、DORA が向上を目指す運用のレジリエンスにとって DNS は非常に重要です。DNS の停止は、金融機関全体のほぼすべてのアプリケーションやサービスに影響を及ぼし、壊滅的な被害をもたらします。このため、DORA を遵守する企業は、他のコアシステムと同様に DNS サービスの可用性をリスク管理計画に組み込む必要があります。[6] その取り組みの一環として、内部 DNS インフラストラクチャの実装と管理において、業界のベストプラクティスを採用することが重要です。

さらに、金融機関は定期的に外部の組織や外部ユーザーとやり取りするため、外部 DNS に関するセキュリティ対策にも同等の注意を払う必要があります。コンプライアンスのために、組織はパブリック（権威）DNSドメインの回復力と安全性を確保する必要があります。脅威アクターは、セキュリティポリシーやプロセスが緩いことを理由に誤って設定された権限のあるドメインを積極的に標的にします。外部の DNS 管理には第三者が関与する場合もあり、規制が同様に適用されるため、DORA コンプライアンスの責任者は、これらの当事者に関連する DNS サービスのリスク管理と軽減を考慮する必要があります。

推奨事項：

- サービスの継続性をサポートするように設計され、ピーク容量に合わせてサイズ設定された、レジリエントな DNS アーキテクチャを実装し、DNS インフラストラクチャとサービスの可用性とセキュリティを維持するための一貫したポリシーと手順を確立します。（第 7 条、第 9 条）
- 組織の一部が外部ドメイン名の管理を担当し、内部レジストラ/レジストリとして機能するようにします。これにより、組織の異なる部門が複数のサプライヤーを介してドメインを登録および管理することがなくなります。（第 5 条）
- プロテクティブ DNS サービスを実装して、悪意のある DNS トラフィックをブロックして記録し、DNS がデータの流出に使用されるのを防ぎ、異常なトラフィックを識別し、フォレンジックとインシデント対応のためのデータを提供します。（第 9 条、第 10 条、第 13 条）

ICT関連インシデント管理、分類、報告

セキュリティ担当者は、インシデント対応時に DNS を使用して、さらなる悪意のある通信を特定してブロックし、侵害の分類と範囲の特定に役立てます。すべてのネットワーク通信は DNS クエリから始まるため、クエリと応答データを含むログ、DHCP ログ、資産情報はインシデント管理にとって重要です。例えば、ネットワーク上のどのデバイスが悪意のあるホストと通信した可能性があるかの記録にすぐにアクセスできれば、セキュリティチームはインシデントの規模と分類を特定しやすくなります。同様に、DHCP ログは、特定の資産に関連付けられている IP アドレスを特定します。ほとんどのセキュリティログは固定 IP アドレスではなく一時的な IP アドレスに基づいてデバイスを識別するため、正確で一貫性のあるイベントと脅威の相関関係を確保したい組織は、関連するデバイスレベルのデータとコンテキストをセキュリティ運用ツールと共有できるようにする必要があります。

推奨事項：

- DNS のクエリと応答データ、DHCP リースアクティビティ、資産データを継続的に記録して、イベントの正確な相関関係を容易にし、インシデント管理の一環としてフォレンジックのコンテキストを提供します。（第17条（3）、第18条（1））
- 悪意のある DNS トラフィックをブロックする制御ポイントとして、プロテクティブ DNS サービスを実装します。この制御ポイントには、プロテクティブ DNS サービスで使用される指標に関連する脅威インテリジェンスを含める必要があります。これにより、ブロックされたトラフィックに関連するコンテキストをセキュリティエコシステムツールと共有して評価を支援できます。（第 17 条）

デジタル運用レジリエンスのテスト

DORA のデジタルレジリエンス基準を満たすためには、事業継続性と災害復旧（第 24 条）の追加テスト、および権限のある機関の枠組み内での脆弱性と侵入テスト（第 25 条および第 26 条）が必要です。リスクの考慮事項と同様に、DORA コンプライアンスを監督する担当者は、ネットワークの可用性において DNS が果たす基本的な役割を考慮する必要があります。例えば、組織はグローバルサーバーの負荷分散を通じて事業継続性を提供するために DNS を活用できます。災害復旧の面では、サイバー攻撃、誤設定、または自然災害による DNS の停止は、事業運営を停止させる可能性があります。したがって、金融機関が運用上の回復力要件を満たすためには、DNS および関連する重要なネットワークサービス（DHCP など）を強化することが不可欠です。

推奨事項：

- 社内外の DNS アーキテクチャとサービスを見直して、「デジタル運用の回復力における弱点、欠陥、ギャップを特定し、是正措置を迅速に実施」します。この点では、NIST 800-81 などの技術標準が役立つ場合があります。（第 24 条（1））
- 包括的なデジタル運用レジリエンステストプログラムを開発する際には、DNS サービス、インフラストラクチャ、プロトコルが具体的にカバーされていることを確認します。DNS サービスの復元は、組織のアプリケーションとサービスの回復に不可欠な前提条件であり、DNS 自体がサービスの継続性と災害復旧を促進する可能性があります。（第 24 条（1））
- ネットワークが DNS に依存していることを考慮し、DNS サービスおよびインフラストラクチャに関する特定のテスト手順を全体的なレジリエンステスト計画に組み込みます。（第 24 条（2））
- 運用レジリエンスをテストし、外部の脅威主導侵入テスト（TLPT）プロバイダーと連携する場合は、可用性とセキュリティのために特定の DNS 関連テストが実行されるようにします。（第 25 条、第 26 条）
- 含める主な領域：
    - » DNS の弾力性が設計どおりに機能していること、特に名前解決用の冗長パスが複数あることを確認します。
    - » 組織のネットワークからのアウトバウンド DNS トラフィックが、制御された DNS リゾルバー（クエリと応答のデータを記録する必要があります）を経由するようにします。
    - » 現在の悪意のある活動に関連付けられているドメイン名をクエリします。
    - » DNS クエリを介してデータを盗み出し、DNS 応答を介してマルウェアを侵入させることが可能かどうかをテストします。
    - » ぶら下がったドメイン名やサブドメインの誤った委任を確実に修正するなど、DNS のセキュリティ衛生を考慮した手順と自動化ツールを導入します。

ICT サードパーティリスクの管理

外部 DNS などの DNS サービスは、サードパーティが管理する可能性があるため、DORA の範囲内にあります。さらに、特定のサービスのために委任された DNS サブドメインを管理する場合もあります。

推奨事項：

- DNS サービスやインフラストラクチャ（外部ドメインなど）を管理するサードパーティとの契約を再確認し、それらが組織の規制やポリシーに適合し、同じ運用上の弾力性とセキュリティレベルを提供していることを確認します。（第 28 条）

情報共有の取り決め

金融機関は、機密情報を保護するための適切な保護を含め、信頼できる金融サービスコミュニティと侵害指標（IoC）と戦術、技術、手順（TTP）を定期的に共有します。これらの信頼できるグループ内では、金融機関は DNS のクエリログやレスポンスログ、ブロックされた悪質なドメインの情報を、共有する情報の一部として使用できます。

推奨事項：

- DNS 関連の IoC を提供するポリシーを実装して、情報共有の準備をします。データ形式を共有グループと事前に合意しておくことは、特にセキュリティ情報イベント管理（SIEM）システムなどの運用ツールに指標を取り込む場合、運用上の面で役立ちます。特に、プロテクティブ DNS サービスを通じてキャプチャされ共有された悪意のあるアクティビティの情報は、多くの場合、他の金融機関のネットワーク防御の強化に役立ちます。（第 45 条）

INFOBLOX による DORA コンプライアンスの簡素化

DORA コンプライアンスをより簡単に達成するために、金融機関は、ICT リスクを効果的に管理するためのレジリエンスとセキュリティに重点を置いて、DNS サービスを DORA の原則に準拠させる必要があります。この整合には、フィッシングやデータ流出などの脅威に対する保護の強化、TIBER-EU や MITRE ATT&CK などのフレームワークの遵守が含まれます。Infoblox は、これらのリスクを軽減し、ICT リスク管理規制への準拠をサポートするようにカスタマイズされたソリューションを提供します。

さらに、Infoblox の堅牢な DNS インフラストラクチャとセキュリティソリューションは、金融機関が DORA の原則に準拠できるようサポートする独自の立場にあります。Infoblox は、安全で回復力のある DNS サービスに重点を置くことで、DORA の対象となる組織が、フィッシング、マルウェアのコマンドアンドコントロール、データの流出など、管理されていない DNS 通信に関連するリスクを軽減できるよう支援します。Infoblox は、MITRE ATT&CK などの業界をリードするフレームワークを活用して、ICT リスク管理要件に適合した実用的なインテリジェンスとカスタマイズされた緩和策を提供します。さらに、Infoblox は ENISA と NIST のガイドラインを統合する専門知識を有するため、金融機関は複雑な規制環境を効果的に乗り越えながら、可用性とセキュリティの義務を果たすことができます。

1. How the digital operational resilience act helps your continuity, PwC.
2. DORA 第 1 章総則、第 1 条（1）対象事項
3. Final Report on draft RTS specifying elements related to threat led penetration tests (reference JC 2024 29), European Securities and Markets Authority (ESMA), 2024年7月7日
4. What is TIBER-EU?, European Central Bank.
5. Adopting TIBER-EU will help fulfil DORA requirements, European Central Bank, 2024年9月
6. DORA 規制「（22）『不可欠または重要な機能』とは、その中断によって金融機関の財務実績、もしくはそのサービスと活動の健全性または継続性が著しく損なわれる機能、またはその機能の中止、欠陥、または不履行により、金融機関がその認可の条件と義務、または適用される金融サービス法に基づくその他の義務を継続的に遵守することが著しく損なわれる機能を指す。」

Infoblox株式会社
〒107-0062 東京都港区南青山2-26-37
VORT外苑前I
3F

03-5772-7211
www.infoblox.com/jp

バージョン：20250625v1