

サーバー・セキュリティサービスが築く、信頼と安心を情報発信する

NewsLetter

2025.12
vol. 54NET ASSIST
24/7 Guardian DeityNEWS
TOPICS
1

情報セキュリティ白書2025

NEWS
TOPICS
2Linuxユーザ必見!最新OS「RHEL10」登場
RHEL9との変更点やサポート期限NEWS
TOPICS
3プライバシー規制強化に対応する
新サービス「STRiGHT」

※TOPICSの各タイトルをクリックすると該当の記事へ飛びます

NEWS TOPICS 1

情報セキュリティ白書2025

今年も独立行政法人情報処理推進機構 (IPA) より9月30日に「情報セキュリティ白書2025」が公開されました。200ページ以上にもなる内容のため、簡単に抜粋してお届けいたします。

情報セキュリティ白書とは？

独立行政法人情報処理推進機構 (IPA) により毎年発行されている書籍です。2024年度の情報セキュリティに関する国内外の政策・取り組み、脅威の動向、インシデントの発生状況、被害実態などの定番トピックの他、その年ならではの注目事象などを取り上げています。

国内外の官民の各種データ、資料を数多く引用しトピックを解説しており、情報セキュリティ分野の全体把握が容易です。書籍として購入するだけでなく、PDF版でも確認が可能です。

[独立行政法人情報処理推進機構 \(IPA\)「情報セキュリティ白書2025」](#)

独立行政法人情報処理推進機構 (IPA)
「情報セキュリティ白書2025」

第1章 国内外のサイバー脅威の動向

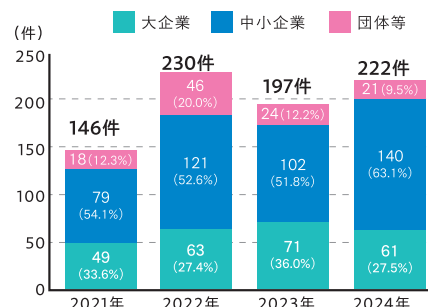
[1] サイバー空間の「戦場化」

アメリカ大統領選 (2024年11月1～6日) の期間中に60億件以上の悪意あるリクエストがブロックされるなど、世界的なイベントを標的とした、国家の関与が疑われる攻撃が確認されています。

[2] 企業に求められる視点の変化

セキュリティの強固な大企業ではなく、その取引先 (サプライチェーン) への攻撃件数が増えており、中小企業にとってもサイバーインシデントは無関係な問題ではなくなっています。

※国内のランサムウェアによる被害件数 (2021～2024年)
(出典) 警察庁「サイバー空間をめぐる脅威の情勢等」を基にネットアシストが作成
<https://www.npa.go.jp/publications/statistics/cybersecurity/index.html>



大企業にとっても、これまでの「自社を守る」だけの視点から、より広い視点が必要になっています。中小企業も含めたサプライチェーン全体の安全や、中断・停止した場合の影響、復旧プロセスも含めた体制設計に移ることが求められています。

第2章 最近のサイバー空間を巡る注目事象

AIの普及により急速な発展を遂げる一方で、そのAIを悪用した偽情報の拡散が大きな脅威になっています。

AIの悪用がもたらすリスク・脅威

AIを用いた認知機能への攻撃 (ディープフェイク)

生成AIによる本物と見分けがつかない偽の画像や動画、音声等のことを呼びます。個人を対象とした性的・心理的な虐待コンテンツや組織の評判を落とすための偽情報の拡散の他、国家を背景とした大規模な世論操作にも悪用が確認されています。

AIを利用したサイバー攻撃

2024年夏の時点では、標的型攻撃のような高度なサイバー攻撃が完全に自動化されるような水準にないと評価されていますが、手動で行うサイバー攻撃を効率化する試みが確認・摘発されています。

AIシステムへのサイバー攻撃

2025年3月時点で社会に大きく被害を及ぼす事例は確認されていませんが、開発に使われるフレームワークやサービス、データベースなどの脆弱性は確認されており、AIシステムへのサイバー攻撃が机上の空論ではないことを示しています。

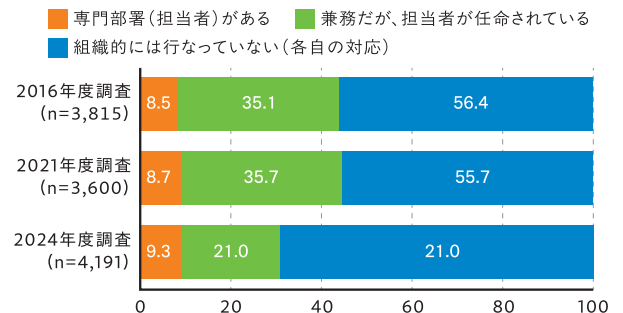
これらの対策として、安全なAI運用を実現する「AIセーフティ」という取り組み・考え方が注目されています。

第3章 国内の政策及び取り組みの動向

サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるとの目標を掲げ、国家サイバー統括室の発足や官民連携の強化など、国家レベルでのサイバー防御体制の強化が進んでいます。

組織や個人単位ではセキュリティ人材の不足が続いており、情報セキュリティ投資の必要性の認識の不足やコストの問題がうかがえます。

※情報セキュリティ白書2024 図 3-2-2 中小企業における情報セキュリティ体制（出典）
IPA「2024 年度 中小企業における情報セキュリティ対策に関する 実態調査」を基に編集
<https://www.ipa.go.jp/security/reports/sme/sme-survey2024.html>



第4章 国際的な政策及び取り組みの動向

社会サービスや企業は国境を越えて繋がりがあっているため、他国でのサイバー脅威が自国にも深刻な被害をもたらす可能性もあります。また、サイバー攻撃は国境を越えており、日本国内だけでの対策では不十分になっています。国や地域が単独で対処することは難しく、国際的な連携が重要になっております。

まとめ

AIの普及・国家間の対立により、サイバー攻撃は益々苛烈になっております。実際に飲料メーカーや配信サービス、物流サービスなど、セキュリティインシデントのニュースが続いており、企業には早急な対策が求められています。弊社では脆弱性診断やWAF、標的型メール訓練サービスなど、豊富なセキュリティツールを取り揃えています。最適なお提案をさせていただきますので、是非お気軽にご相談ください。

NEWS TOPICS
2

Linuxユーザ必見！最新OS「RHEL10」登場 RHEL9との変更点やサポート期限

5月20日にアメリカのRed Hat社より、「Red Hat Enterprise Linux 10」（以下、RHEL10）がリリースされました。これに続き、無償で利用可能な「Alma Linux 10」および「Rocky Linux10」も発表され、10系OSの普及が加速しています。

今回は、新たにメジャーバージョンアップされたRHEL10の特徴やサポート期限、各クラウドサービスでの提供状況についてご紹介いたします！



RHEL9との変更点

[1] CPUの対応範囲の変更

RHEL9では「x86-64-v2」をベースにサポートしていましたが、RHEL10からは、最低要件として「x86_64-v3」からのベースへと変更になっています。

そのため、v2以下のCPUでは動作しない可能性があるため注意が必要です。

[2] ミドルウェアのバージョンについて

RHEL10では多くの主要ミドルウェアが更新されています。代表的な変更は以下のとおりです。RHEL10より、Send mail関係のパッケージは削除され、代わりにpostfixパッケージを利用することができます。また、安全で最新機能が備えられているSMTPデーモンの使用が可能になっています。



APACHE
HTTP SERVER PROJECT

2.4→2.4.62



python™

3.9/3.11→3.12



php

8.0→8.3



OpenSSL
Cryptography and SSL/TLS Toolkit

3.0→3.2



MariaDB

10.5→10.11



PostgreSQL

15→16



サポート期限

RHEL10とAlmaLinux10のサポート期限のご紹介

RHEL10	
提供開始	2025年05月20日
フルサポートの終了日	2030年05月31日
メンテナンスサポート終了日	2035年05月31日
ELS終了予定	2038年05月31日

AlmaLinux10	
提供開始	2025年05月27日
サポート期限	2030年05月31日
セキュリティサポート期限	2035年05月31日



各社クラウドサービスの対応状況

弊社のパートナーベンダーや、実績のあるクラウドを中心にご紹介

	さくらのクラウド	さくらの専用サーバー	AWS	IDCF	Azure
RHEL10	×	○	○	×	○
Alma Linux10	○	○	○	×	○

※2025年11月現在



さくらのクラウドでの提供状況

9月に公表されたさくらのクラウド「石狩第3ゾーン」においても、AlmaLinux10が利用できるようになっています！

一方で、東京第2ゾーンでは現在、RHEL8およびRHEL9のみ利用可能です。RHEL10の対応開始が待たれるところです。

ご相談受け付け中！

ネットアシストでもRHEL10/AlmaLinux10の保守やサーバー構築のご相談を受け付けておりますので、是非ネットアシストまでお問合せください！



NET ASSIST
24/7 Guardian Deity

お問い合わせはこちら



NEWS TOPICS
3プライバシー規制強化に対応する
新サービス「STRiGHT」

近年、個人情報保護法や各国のプライバシー規制が強化されており、企業サイトにおける Cookie の利用と同意取得 への対応も今まで以上に重要視されています。そのような背景を踏まえ、ネットアシストではCookie 同意管理ツール「STRiGHT (ストライト)」の提供を開始いたしました。



そもそもCookieとは何？

Cookieとは、Webサイトを閲覧した際にWebブラウザに保存される、日時・回数などを記録したデータです。

近年、世界各国でプライバシー保護に関する規制が強化されており、Cookie を収集・活用する際はCookie同意管理ツールなどでサイト利用者の同意を適切に得ることが求められています。



[1] 法規制の強化

改正個人情報保護法(日本)：
第三者提供(トラッキング含む)に対する同意取得が明確に義務化。
「Cookieが個人関連情報とみなされるケース」では、利用目的の明示・同意が必要。

※既に欧州では、GDPR(一般データ保護規則)にて 同意の取得が義務化且つ「設定」「拒否」オプションが必要と制定されている。違反に対する罰金も重い。

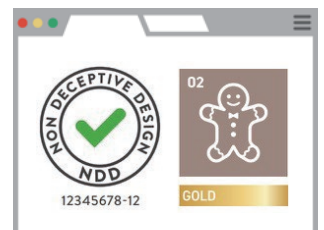
[2] Webサイト透明化の取り組み

2024年9月に「ダークパターン対策協会」が設立され、2025年10月にダークパターン被害の軽減と誠実なWebデザインの普及を目的に、「NDD(Non-Deceptive Design)認定制度」が開始。消費者庁とも連携し、Webサイトの透明化を証明する認定制度の普及促進がはじまっている。NDD認定制度では、Cookieバナーの設置と設計内容が実質必須。

NDD認定制度チェック項目一部

意思表示のUIにおける透明性	Cookieバナーや利用規約などのUIが分かりやすく表示されているか
説明の明確性・選択肢の対等性	「すべて許可」と「拒否」「設定」が平等に表示されているか
意思表示の再設定が可能	一度同意した後でも簡単に変更・撤回できる仕組みがあるか
ダークパターンに該当する誘導的デザインの排除	誘導・強制・ミスリード的な要素が存在しないか

NDD認定バッジ



STRiGHTとは？

株式会社インターネットイニシアティブ(IIJ)が開発したオールインワンのCookie 同意管理プラットフォーム(CMP)です。

世界各国の法規制(GDPR、CCPA、日本の改正個人情報保護法など)や、ダークパターンを考慮した表示方法、Google同意モードによる計測の高度化などCookie同意バナーに必要な機能を揃えています。





STRiGHTの特長

特長 1

法規制対応を一括管理



主要な国際規制に対応し、1つの管理画面で複数サイトのバナーを統一運用可能

特長 2

UXとプライバシー保護を両立



画面を覆うバナーではなく、フッターリンク型などUXに配慮した設計が可能

特長 3

高機能なのに低コスト

年間 **117,600** 円 (税抜)
(月々9,800円)

外部送信スキャン、バナーの多言語対応、カスタマイズなどの十分な機能搭載



主な機能

多層構造バナー

(第1層:同意/第2層:詳細設定)

複数テンプレート対応

(オプトイン/オプトアウト/情報提供型/CCPAなど)

法域・言語の自動切替

Google同意モード対応/外部送信スキャン機能

年齢・地域制御(Age Gate)機能にも対応

サイトデザインを損ねないボタン表示

Website下部に、プライバシー設定バナーへの呼び出しを行えるホバーボタンの設定も可能となります

カスタマイズできる項目

カスタマイズできる項目は、背景色、バナータイトル、説明文、提供元、ボタン各種のカスタマイズが可能です



Cookie対応やSTRiGHT導入のご相談は、お気軽に担当営業へお問合せください！