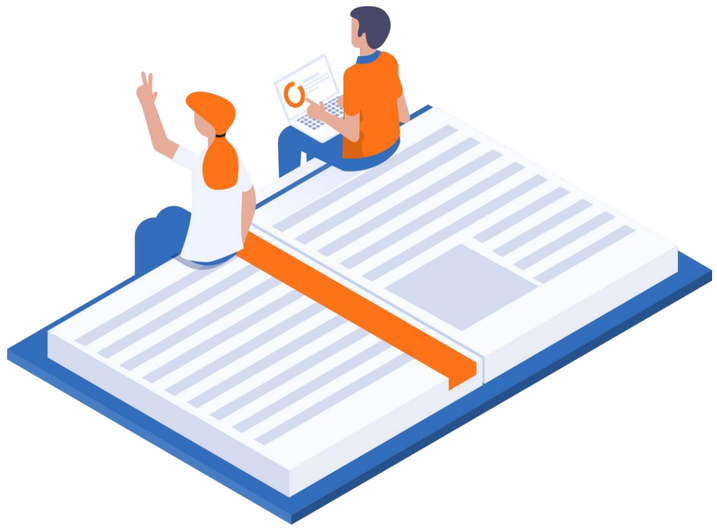
2026年版

クラウド・AI時代における情シスのための最新セキュリティ対策ガイド

～2025年のセキュリティニュースから考える、脅威と課題解決～

BCC株式会社

もくじ



はじめに

コロナ禍以降、情シスを取り巻く環境はこう変わった

昨今のIT環境は、利便性と引き換えに攻撃対象領域が拡大しています。
クラウド、SaaS、リモートアクセス、外部委託先など、
「社内ネットワークの外側」を前提としたセキュリティ設計が求められる一方で、
情報システム部門の体制は大きく変わっていない企業も少なくありません。

- **クラウド・SaaS利用が“前提”のIT環境になった**
- **テレワーク／ハイブリッドワークが定着**
- **セキュリティ対策は「導入」から「運用・継続」が重視される時代に**

このギャップこそが、2026年にセキュリティ課題が顕在化する最大の要因です。

2025年の情報セキュリティニュース

危ないのは大企業だけ？いいえ、他人事ではありません

例えばランサムウェアに感染してしまうことで、企業活動に遅れが発生し営業機会を次々と失う恐れがあります。
最悪の場合、事業の停止に追い込まれる事態も考えられます。
特にサプライチェーンを構成している中小企業は、発注元である大企業への標的型攻撃の糸口として狙われる可能性も高く、
自社のセキュリティの脆弱性を利用されたことで、ニュースになるほど大きな事態に発展する可能性も拭い切れません。

順位	ニュース
1	相次ぐ企業へのサイバー攻撃、いまや“災害級”と指摘される脅威 ～ アサヒGHD、アスクル等のランサム障害、影響は市民にも ～
2	サプライチェーンに波及するサイバー被害、賠償問題に発展するケースも ～ 被害の連鎖、賠償問題から考える委託先管理の重要性と評価制度の意義 ～
3	金融庁、証券口座乗っ取り被害急増で注意喚起、監督指針改正へ ～ デジタル時代の証券犯罪と20年越しの“認証”問題 ～
4	生成ＡＩ悪用し不正アクセスの中高生３人逮捕、12月にも ～ 圧倒的なAIパワーの光と影　攻撃もAI、防御もAI ～

出典：JNSA 2025セキュリティ十大ニュース（4位以降もこちらから）　https://www.jnsa.org/active/news10/2025.html

2025年の情報セキュリティニュース

昨今の情報セキュリティ10大脅威 の変遷

上位は毎年ほぼ変化が見られず、「システム」や「人」がリスクであることもわかります。
また、2026年以降は新たにAIによるセキュリティリスクの懸念も高まってきました。

順位	脅威　＜2026年 発表＞
1	ランサム攻撃による被害
2	サプライチェーンや委託先を狙った攻撃
3	AIの利用をめぐるサイバーリスク
4	システムの脆弱性を悪用した攻撃
5	機密情報を狙った標的型攻撃

順位	脅威　＜2025年 発表＞
1	ランサム攻撃による被害
2	サプライチェーンや委託先を狙った攻撃
3	システムの脆弱性を突いた攻撃
4	内部不正による情報漏えい等
5	機密情報を狙った標的型攻撃

順位	脅威　＜2024年 発表＞
1	ランサム攻撃による被害
2	サプライチェーンや委託先を狙った攻撃
3	内部不正による情報漏えい等
4	標的型攻撃による機密情報の窃取
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

出典：情報セキュリティ10大脅威 2026（5位以降もこちらから）　https://www.ipa.go.jp/security/10threats/10threats2026.html

情シスの環境変化と
セキュリティの重要さはわかったけど。。。

具体的にどんな課題が浮き彫りになったか
ご紹介していきます。

課題

①業務過多で、セキュリティ“運用”まで手が回らない

2026年のセキュリティは、「製品を導入すれば終わり」ではなく、
監視・分析・アップデートを継続する運用型対策が主流です。
しかし、情シスが日常業務に追われる中で、これらをすべて内製で回すのは
現実的ではありません。

こんなことありませんか？

- **クラウド・SaaS管理が増えた**
- **問い合わせ対応・障害対応が減らない**
- **セキュリティは「入れっぱなし」になっている**

“運用できないセキュリティ”は、対策していないのと同じです。

課題

②IT環境の複雑化で、自社の弱点が見えなくなる

これからは、「どこから攻撃されるか分からない」前提で守る必要があります。

そのため、セキュリティは入口・内部・出口の3点に加え、

ID・端末・ログまで含めた立体的な整理が欠かせません。

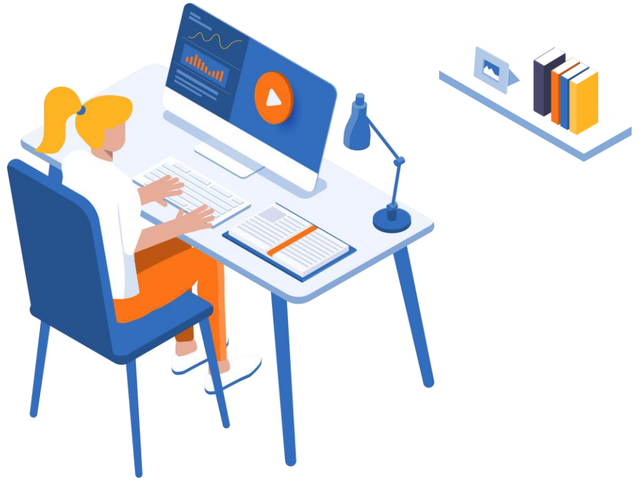
こんなことありませんか？

- **クラウド／オンプレが混在している**
- **利用しているSaaSの全体像を把握しきれていない**
- **境界防御だけでは不安**

まずは“守るべき範囲を可視化すること”が最優先です。

課題

③技術が進化するほど高まる「人」のリスク



2025年は、AIを活用したフィッシングやなりすましなど、

人の判断を狙う攻撃が増加しました。

ゼロトラストやEDRといった技術対策に加え、

「社員が迷わない設計」「教育・啓発」がこれまで以上に重要です。

こんなことありませんか？

- **メールの文面が巧妙すぎて、社員が本物かどうか迷う**
- **AI生成と思われる、見分けのつかないなりすましが増えている**
- **社員任せの判断が増えている**

EDRとは

侵入を前提にエンドポイントの挙動を監視し、

サイバー攻撃発生後の被害を迅速に検知・対処して

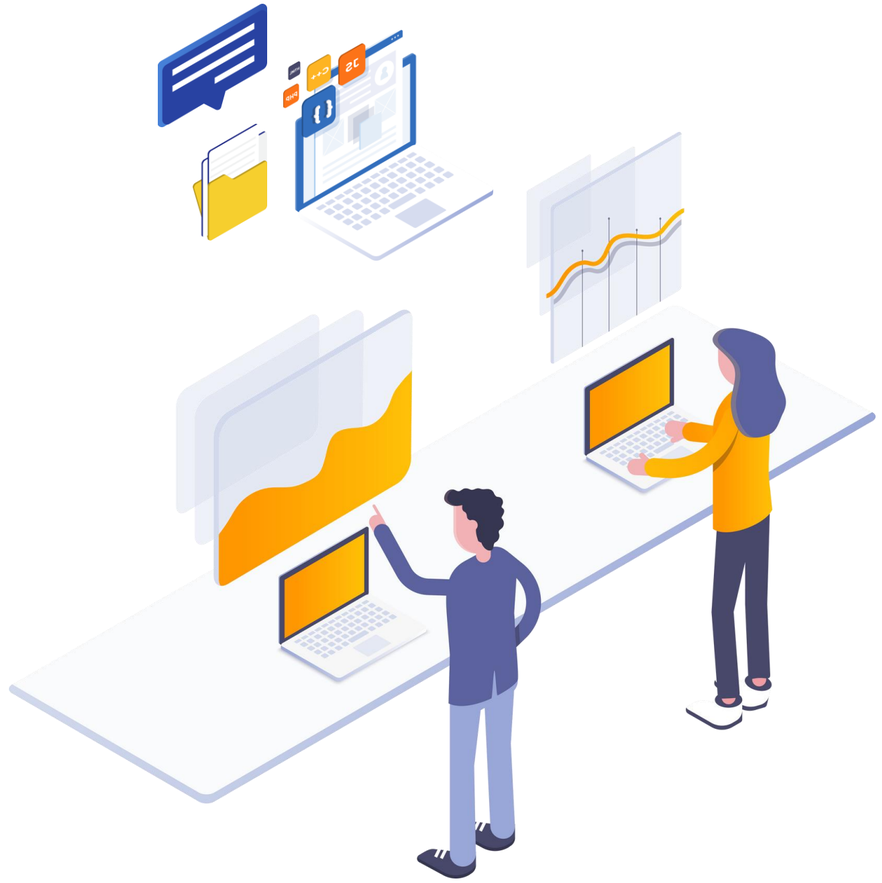
最小限に抑えるセキュリティ対策です。

セキュリティは“人を信用しない設計”と“人を育てる仕組み”の両立が鍵です。

課題

④対策の選択肢が多すぎて、優先順位を決められない

2026年の情シスに求められるのは、「最新技術をすべて入れること」ではありません。
自社の業務内容・人員体制・リスク許容度を踏まえ、
現実的に回し続けられる対策を選ぶ視点が重要です。



こんなことありませんか？

- **新しいセキュリティ製品が次々登場する**
- **何を選べば正解か分からない**
- **投資判断に自信が持てない**

優先順位を決めること自体が、最大のセキュリティ対策です。

まとめ

2026年に選ぶべき“現実解”とは

01 課題整理

自社のIT環境・体制で
どこにリスクが
集中しているのか

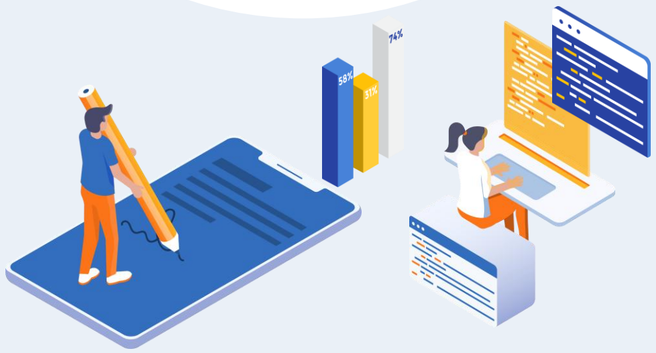
02 設計

すべてを内製で抱え込まず
外部の知見も含めた
役割分担

03 運用

導入して終わりではなく
継続的に回し続けられる
体制

人手不足が続く中、セキュリティを内製だけで完結させる時代は終わりつつあります。
マネージドサービスや外部パートナーを活用しながら、
「守れる範囲を確実に守る」体制づくりが、2026年のスタンダードです。



まとめ

これからのセキュリティ対策を一緒に整理しませんか？

当社では、2026年のIT環境を前提に

「現状課題の整理」「優先順位の設計」

「運用まで見据えたセキュリティ対策」をご支援しています。

2026年1月には自社マネージドサービスのオプションサービスもリリース。

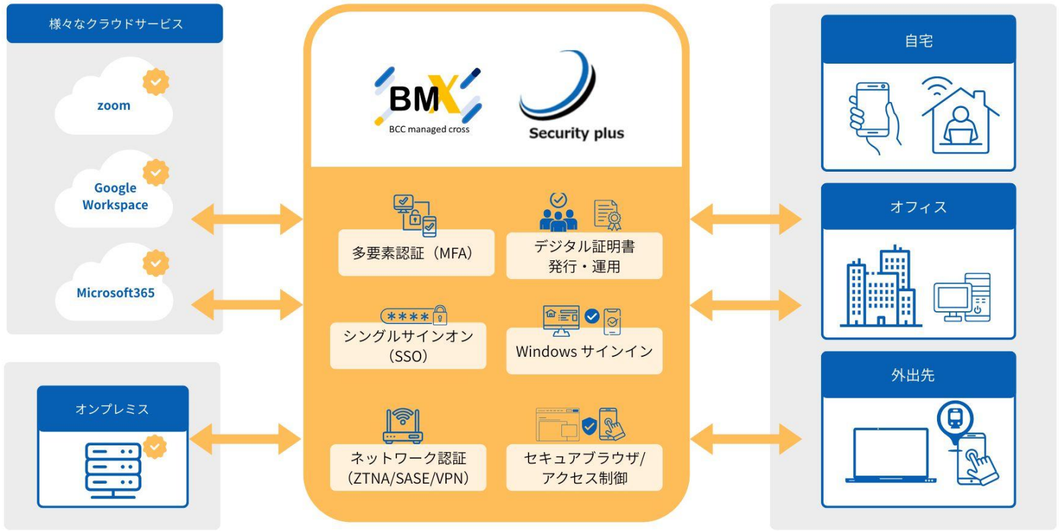
近年、**VPNの脆弱性を狙った攻撃**が増える中、

多要素認証（MFA）と**ID管理・シングルサインオン**を**標準搭載**した

本サービスは、セキュリティ対策と運用負荷の軽減を同時に実現します。

弊社セキュリティサービスの詳細は
こちらをクリック！

ネットワーク管理ソリューションにセキュリティ強化をプラス



お問い合わせ先

IT営業アウトソーシングカンパニー

マネージドサービス・セキュリティついて問い合わせる

会社概要

商号	ＢＣＣ株式会社
事業所	東京本社 ：東京都千代田区外神田６-15-９ 明治安田生命末広町ビル９Ｆ 大阪本社 ：大阪市中央区今橋2-5-8 トレードピア淀屋橋９Ｆ
創立	2002年3月
代表取締役社長	伊藤一彦
カンパニー名	IT営業アウトソーシングカンパニー
カンパニー長	松村健太
主要部門	・営業アウトソーシング ・ソリューション
許認可	一般労働者派遣事業（派27-302361） 有料職業紹介事業（27-ユ-302045） プライバシーマーク認定（第10861424(07)号） 電気通信事業（E-28-03972）
主要取引先	株式会社インターネットイニシアティブ(IIJ) 日鉄ソリューションズ株式会社 ダイワボウ情報システム株式会社 日本電気株式会社(NEC) 富士ソフト株式会社