\Orchestrating a brighter world NEC

NECソリューションイノベータ

# 情報漏えい対策ソリューション

情報セキュリティコラム

# The ANGLE

## 情報漏えい対策の視角

※ 本資料は抜粋版です。完全版は第17回まで掲載しておりますが、
抜粋版は第1回・第2回のみを掲載しております。

# 目　次

情報漏えい対策強化に向けたお取り組みに役立つ情報をさまざまなアングルで切り取って発信していきます。

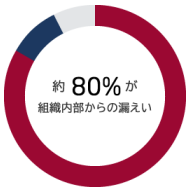
漏えいリスクから企業の資産を守る

# 情報漏えい対策ソリューション

NECソリューションイノベータの情報漏えい対策ソリューションは、
「内部からの情報漏えい」と「外部からの悪意ある攻撃」2つのリスクに着目し、
お客様の環境、ご要望に沿ったセキュリティ強化対策を、導入のご相談から運用に
至るまでワンストップでご提供。お客様の情報資産を安全かつ強固にお守りします。

## 情報漏えい対策に必要な2つの視点

情報漏えいの原因は、「管理ミス」が一番多く、「誤操作」、「紛失・置忘れ」といった人的ミスで全体の約8割を占めています。日常業務における不用意な情報の取り扱い、データを社外に持ち出して利用する内部者の不注意など、内部者の問題意識の低さが要因と言えるでしょう。一方、「不正アクセス」が、2016年の情報漏えい原因の上位3番目となっている点も、無視できません。外部攻撃は一度に大量の情報が漏えいしやすく、インシデント1件あたりの被害が大きくなる傾向があります。また、インターネット上では新しい攻撃が次々と発生しています。つまり、人的ミスによる内部情報漏えい対策に加えて、外部からの脅威に対する情報漏えい対策も必須だと言えます。さらに、情報漏えい事故は情報を流出された企業に、多大な損害と莫大な損失(損害賠償)を生じさせます。事故1件当たりの平均損害賠償額も6億2,811万円(2016年)と年々増加しています。企業にとって情報漏えい事故は、信用・イメージはもちろん、経営面にも悪影響を及ぼします。社内外リスクを洗い出し、問題点を捉え、適切な対策を早急に講じることが急務です。情報漏えい対策の最適な実施と継続的な取り組みは、企業全体のセキュリティレベル向上、さらには外部からの信頼性向上にもつながります。




| | | |
|---|---|---|
| 管理ミス | 34.0% | (159件) |
| 誤操作 | 15.6% | (73件) |
| 紛失・置忘れ | 13.0% | (61件) |
| 不正な情報持ち出し | 6.8% | (32件) |
| 盗難 | 5.3% | (25件) |
| 設定ミス | 4.7% | (25件) |
| バグ・セキュリティホール | 1.7% | (8件) |
| 内部犯罪・内部不正行為 | 0.9% | (4件) |
| 目的外使用 | 0.4% | (2件) |
| 不正アクセス | 14.5% | (68件) |
| ワーム・ウィルス | 1.1% | (5件) |
| その他 | 1.9% | (9件) |

出典:2016年情報セキュリティインシデントに関する調査報告書
【個人情報漏えい編】第1.2版2017年6月14日
NPO 日本ネットワークセキュリティ協会
セキュリティ被害調査ワーキンググループ
長崎県立大学 情報システム学部情報セキュリティ学科

## 全国に広がるソリューション提供体制でセキュリティ強化をサポート

2016年3月、NECソリューションイノベータは、スタッフ部門を含む全社全部門において、情報セキュリティマネジメントシステム(ISMS)国際規格「ISO 27001」の認証を取得しました。
情報セキュリティ全般の知識に精通し、対策構築・運用に関する豊富な実績が強みです。

刻々変わる脅威状況を踏まえ、貴社の「情報セキュリティのかかりつけ医」として、お客様に最適なソリューションを常に提供してまいります。

NECソリューションイノベータでは、多種多様な業種のお客様への数多くの導入実績のノウハウをもとに、導入前のご相談から、企画・構築・運用/保守までワンストップでお応えします。
私たちと一緒に、セキュリティ対策を見直しませんか。

情報漏えい対策ソリューション

## 組織内部からの漏えい・対策製品

社内Webシステムの情報漏えい対策、共有サーバからの情報漏えい対策、クライアントPCの盗難・紛失対策、外部デバイスの利用を制御など、組織内部からの漏えいに関する対策製品をご紹介します。

### 組織内部からの漏えいは、情報漏えい事故原因全体の82%

PC・USBメモリなどデバイス類の紛失・置き忘れ、業務データの持ち出し、設定・管理ミス、内部犯罪、目的外使用など、情報漏えい事故原因全体の82%が内部からの情報漏えいです。

個人の心がけだけでは避けきれないミスではありますが、自社をはじめ取引先、個人などの重要情報などが容易く漏えいしてしまうことに対するダメージは信用失墜、取引中止など甚大です。組織内部ルールの周知徹底、持ち出し機器やファイルへの適切な暗号化、定期的バックアップなど日常的な情報管理が必須です。

- **Webコンテンツ保護・情報漏えい対策ソリューション**
- **NonCopy for USB**
- **Check Point Full Disk Encryption**
- **4thEye Professional**
- **情報漏えい防止ソフトウェア・NonCopy2**
- **Check Point Media Encryption**
- **Tripwire Enterprise**

情報漏えい対策ソリューション

## 外部からの脅威・対策製品

エンドポイント向け次世代マルウェア対策、セキュリティの可視化・システム全体の監視、クライアントPCの盗難・紛失対策など、外部からの脅威に関する対策製品をご紹介します。


### 外部からの脅威は、情報漏えい事故原因全体の15.6%

不正アクセス・侵入、Webサイト改ざん、システム破壊、マルウェア感染、脆弱性攻撃、標的型攻撃など、外部からの脅威は、情報漏えい事故原因全体の15.6%です。

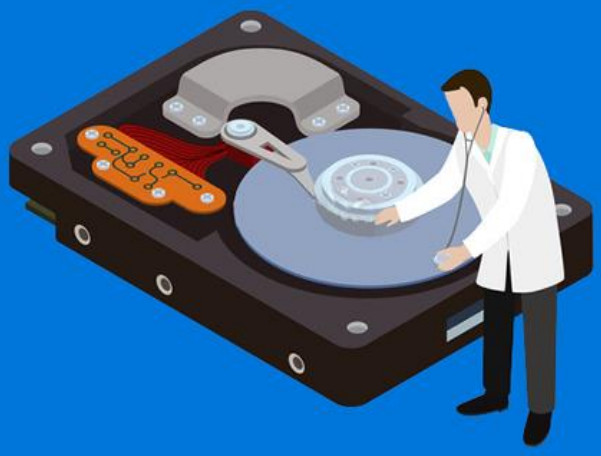
日々悪質かつ巧妙化した新種マルウェアが発生し拡散しているため、被害を受けた企業が取引先や顧客からの指摘で初めて発覚など侵入されたことに気づかないケースが増え、大量の情報流出、企業の信頼低下など被害は深刻です。複数の対策を組み合わせた多重セキュリティで「侵入させない」環境を構築することが重要です。

- **CylancePROTECT**
- **エンドポイント脅威対策サービス**
- **Tripwire Enterprise**
- **CylanceOPTICS**
- **Cylanceコンサルティングサービス**
- **Check Point Full Disk Encryption**

第1回

# Windows 10対応とハードディスク暗号化

## 「BitLocker（ビットロッカー）」で十分!?安全性・運用からの考察



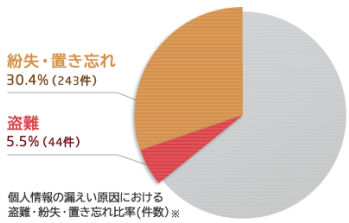
Windows XPの延長サポートの完全終了、Windows 7のメインストリームサポートの終了を受けて、企業でのWindows 10対応が急速に広がる気配を見せています。諸々の都合や事情で先延ばしにしてきた企業でもWindows 10対応に向けていよいよ本腰を入れて取り組まなければなりません。
Windows 10対応に伴い、企業として取り組むべき課題はさまざまにありますが、本コラムでは「持ち出しPCやモバイル端末は紛失や盗難のリスクから100%逃れることはできない」「データや情報が抜き取られるリスクは必ず存在する」との認識のもと、情報漏えいを可能な限り防ぐためにはどうすればよいか―。OSのバージョンアップ、PCのリプレース・増設等で必要不可欠な重要対策のひとつとして、ハードディスク暗号化にフォーカスをあてて考えていきます。

### 情報漏えい原因の約36%は、PC等の盗難・紛失・置き忘れ

ビジネスにおいてノートPCやモバイル端末を社外に持ち出し、活用するシーンが急速に拡大しています。Windows 10対応に向けて、PCのリプレース・増設を検討されている企業も多いのではないでしょうか。

検討において最も重要なのは、情報漏えいリスクへの対策です。実際、盗難にあったり、紛失・置き忘れPCから不正にデータを抜き取られる情報漏えい事故が増えています。日本ネットワークセキュリティ協会の調査によると、個人情報の漏えい原因における盗難・紛失・置き忘れ比率は全体の約36%を占めています。

※参考：日本ネットワークセキュリティ協会『2015年 情報セキュリティインシデントに関する調査報告書【速報版】』




### OSログインパスワード、BIOSパスワードだけでは不十分

「PCはログインパスワードを設定しているので大丈夫」と思われるかもしれませんが、インターネット上で入手できるフリーのクラッキングツールを使えば、わずか数分でパスワードが突破される恐れがあります。

PCに詳しい人は「OS起動前に入力を求めるBIOSパスワード方式なら、安全性が高まるはず」と思われるかもしれませんが、これも誤解です。BIOSパスワードはPCのハードディスクを直接保護するものではないので、物理的なクラッキング行為に対しては効力が十分ではないと言えます。


### 「BitLocker」などを使ったハードディスク暗号化が不可欠

持ち出しPCの情報漏えい対策として欠かせないのが、ハードディスク内のデータを特殊な技術で暗号化し、第三者による不正な読み出しを困難にする暗号化ソフト(もしくは機能)です。Windows 10に標準で搭載されているドライブ暗号化機能「BitLocker(ビットロッカー)」もそのひとつです。

しかし、BitLockerで果たして十分でしょうか。市販されている他のハードディスク暗号化ソフトについてもどうでしょう。どのような仕組みや特長を持っているのか、企業のインフラ管理者視点から運用が回るのか、しっかり吟味する必要があります。

**「BitLocker」とは、**

Windows PCの上位機に搭載されるドライブ暗号化機能。システムドライブおよびデータドライブ上のファイルを保護するビジネスPCのセキュリティ強化機能のひとつです。Windows 10ではProとEnterpriseで利用可能です。

## ハードディスク暗号化ソフト選定 5つのポイント

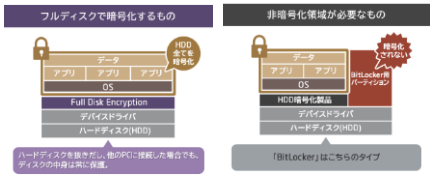
ハードディスク暗号化ソフトには、導入にあたって難しい設定が必要であったり、従業員が自分のパスワードを忘れてしまった時の手続きが面倒であったり、ハードディスクの特定領域しか暗号化できないものがあったりします。BitLockerはWindows OSでしか使えず、他のOSでは別のソフトで対策をとらなければなりません。

Windows 10対応に向けたハードディスク暗号化ソフトの検討・選定では、自社での運用状況などを踏まえたうえで、後悔しないための十分な事前検討が必要です。そこで、とりわけ重要となる5つのポイントを取り上げてみました。

### Point 1 暗号化の対象範囲

#### データ領域だけか、OSも含めたフルディスク方式か

非暗号化領域があると、ハードディスクを別のPCに付け替えることで非暗号化できる不正なプログラムがインストールされてしまうなど、セキュリティリスクが高まります。リスクを排除するには「フルディスク暗号化方式」がおすすめです。




フルディスク暗号化方式では、OSや利用者データを含めて暗号化します。クラッキングツールが使用されても、OSが起動しないため、クラッキングツールの利用自体が無効となります。ハードディスクの抜き取りによるデータの盗難被害防止にもつながります。

市場に出回っているパスワード解析ツールや、データ復旧会社でパスワード解除サービスの提供があるものは避けたほうがよいでしょう。ソフトによっては管理者権限だけで暗号化解除ができるものもありますが、特定IDを用いた内部不正が問題視されている今、情報漏えい対策としては不十分です。

**選定ポイント(暗号化の対象範囲)のまとめ**

- OSを含めたフルディスク暗号化方式のもの
- パスワード解析ツールが出回っていないもの
- 管理者権限だけでは暗号化を解除できないもの

### Point 2 導入と運用管理のしやすさ

#### 管理コンソールで一元管理ができるか、そうではないか

セキュリティポリシーなどをPC毎に手動で導入・設定する必要があるものは、対象台数が増えるほど設定作業に手間と時間がかかります。対象PCへのインストールのみで、難しい設定をせずに導入できるものが一番です。

また、専用サーバで集中管理ができ、管理コンソールから容易に管理できるものがよいでしょう。PC毎の状況をタイムリーに把握できなければ、万が一、暗号化が解除された時に迅速な対応が難しくなります。

企業によってはWindows OSとMac OSが混在している場合がありますが、全社ガバナンスを効かせたハードディスク暗号化対策を行うには、同一ポリシーで一元管理できることが望ましいです。

**選定ポイント(導入と運用管理のしやすさ)のまとめ**

- 難しい設定をせずにインストールできるもの
- 専用サーバによる集中管理方式で各PCの暗号化状況を把握できるもの
- OSが混在しても同一ポリシーで一元管理可能なもの

### Point 3 パスワード忘れ時の対策

#### 回復キーの漏えいを想定しているか、そうではないか

ハードディスク暗号化ソフトには、パスワード忘れ時に復旧するための鍵情報を持っている製品があります。この場合、鍵情報を当該のエンドユーザに通知するのですが、万が一、鍵情報が漏えいした場合、その代償は高くつきます。アカウントロックや非常ログイン時の対応についても同様です。鍵情報のような重要な情報を使わずに、パスワード再発行やワンタイムログオンができる仕組みがあることが望ましいです。

**選定ポイント(パスワード忘れ時の対策)のまとめ**

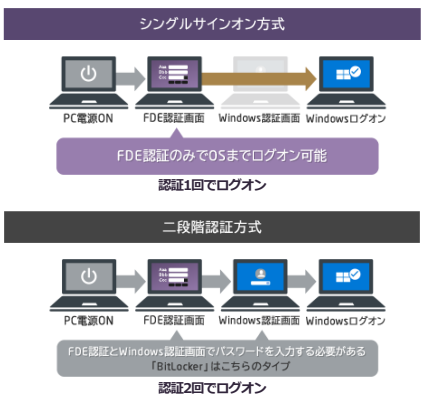
- 管理者によるリモート操作でパスワード再発行が可能なもの
- 管理者によるリモート操作でワンタイムログオンが可能なもの

### Point 4 PC起動時の認証方式

#### OS連携でログオンができるか、そうではないか

ハードディスク暗号化ソフトによっては、PC電源ON後にまず暗号化ソフトの認証画面が立ち上がり、認証後、OS認証画面が立ち上がってログオンを求める「二段階認証方式」のものがあります。この方式では複数の認証情報の管理や二度のログイン認証が必要になり、ユーザの手間が増えてしまいます。覚えられないから…とパスワードを記載した付箋をPCに貼り付けておくユーザが出てきてしまう危険性もあります。

セキュリティと業務効率のバランスは重要です。業務に使うPCは、PC起動時のログオンが一度でスピーディーに行えるものが望ましいでしょう。ハードディスク暗号化ソフトのログオンとOSのログオンを連携させたシングルサインオン方式がおすすめです。




**選定ポイント(PC起動時の認証方式)のまとめ**

- 認証1回でログオンできるシングルサインオンができるもの

### Point 5 起動トラブル時の対応

#### 面倒な手間をかけずにリカバリできるか、そうではないか

何らかの障害によって、システム領域が損傷しOSが起動できない、暗号化が解除できないといったトラブルはユーザにとって非常に深刻です。業務データを格納したPCが当日あるいは数日間にわたって使えない、最悪の場合、二度と使えなくなるようなことがあっては業務やビジネスに深刻なダメージを与えます。

ハードディスク暗号化ソフトでは、このような事態に備え、管理者による強制復号処理が可能な対応策がとられていますが、ソフトによってその手法はまちまちです。別途、ハードディスクを用意したうえでないと復号が行えないものがありますが、管理者にとっては煩わしい限りです。早急な業務復旧のためにも、特別な準備をせずに、復号処理が行える仕組みを選択されるとよいでしょう。

**選定ポイント(起動トラブル時の対応)のまとめ**

- PC起動トラブルに備えた対策がとられているもの
- トラブルPC上で復号処理が可能なもの

## NECソリューションイノベータが考えるハードディスク暗号化

Windows 10対応、PCリプレース・増設等を機に、情報漏えい防止に向けたより強固な対策を検討する動きが高まっています。

ハードディスク暗号化ソフトの導入は、盗難・紛失・置き忘れ等に備えたデータ保護の防波堤として欠かせない対策であり、その際、どのようなソフトや機能を導入するか、選定にあたっては十分な検討を重ねる必要があります。

本コラムで取り上げたポイントをクリアするハードディスク暗号化ソフトとして、NECソリューションイノベータでは「Check Point Full Disk Encryption」(旧製品名：「Pointsec」)をおすすめしています。

OSを含めたディスク全体の暗号化

### Check Point Full Disk Encryption

Check Point Full Disk Encryptionは、ハードディスク全体を自動的に暗号化(フルディスク暗号化)し、PCの盗難・紛失・置き忘れ時に悪意のある第三者によるハードディスクデータ読み出しから重要情報を保護するハードディスク暗号化ソフトで、NECソリューションイノベータでは、2000年の取り扱い開始以来、15年以上にわたりサポートを提供しています。

### 信頼と実績ある暗号化技術

ITセキュリティ評価の国際共通基準「Common Criteria」において商用利用として最高ランクのEAL4を獲得。

### 利用者に負担をかけない

直感的なユーザインターフェース、シングルサインオンなど、利用者のPC環境(業務)に負担をかけません。

### 分かりやすい管理コンソール

分かりやすいセキュリティポリシー設定画面や、端末の暗号化状態の管理などが統合的に行える。

- 国内150万ライセンス以上※
- 15年以上の取り扱い・サポート実績

※NECグループにおける累計実績　2016年5月末現在

### たとえば、このような企業様に

- PCのWindows 10対応(OSバージョンアップ、PCリプレース)を進めたい
- 商談、プレゼンテーション、フィールドワーク、出張などでPCを社外へ持ち出す機会が多い
- ビジネスの機動力アップに向けてモバイル端末の業務利用を進めたい
- 持ち出しPCの紛失、盗難で対処に追われたことがある
- 持ち出しPC内のデータをより確実に暗号化できるソフトに替えたい
- 暗号化漏れがないか管理できるソフトにしたい
- PC不具合時に暗号化したデータをすぐに救出できるものがいい
- PCのリプレースを機にフルディスク暗号化を徹底したい

### 詳しくはWebサイトをご覧ください

PC暗号化、外部記憶メディアの利用制御・暗号化

**エンドポイントセキュリティソリューション**

https://www.nec-solutioninnovators.co.jp/sl/eps/

エンドポイントセキュリティソリューション　検索

## ハードディスク暗号化ソフトの機能比較

Windows 10対応、PCリプレース・増設、暗号化ソフトリプレースをご検討中の企業様には、Windows 10のドライブ暗号化機能「BitLocker」の利用は選択肢のひとつです。ハードディスク暗号化ソフトに精通した従業員がいる企業では、BitLockerで十分に対応可能と思います。

しかし、精通した従業員がいない場合、またWindows OSとMac OSが混在している企業では、Check Point Full Disk Encryptionを是非ご検討ください。

なお、両者の違いについてお問い合わせをいただくことも多いです。そこで、機能比較を以下にまとめています。ハードディスク暗号化ソフトのご検討に、是非お役立てください。

(2016年6月22日)

### ■「Check Point Full Disk Encryption」と「BitLocker」の機能比較

| | | Check Point Full Disk Encryption | BitLocker |
|---|---|---|---|
| セキュリティ面 | 暗号レベル | **ハードディスクまるごと暗号化**<br>• OS起動前認証<br>• ITセキュリティ評価の国際共通基準において商用利用として最高ランクのEAL4を獲得 | **ドライブ単位で暗号化(※)**<br>• OSがインストールされたドライブや固定データドライブをドライブ単位で暗号化<br>• 非暗号化領域が必要<br>※AES128bit/AES256bit/XTS-AES128/XTS-AES256から選択 |
| | 暗号化の解除(無効化) | **個人の判断でアンインストール不可**<br>• システム管理者の介在が必要 | **利用者が管理者権限を持つ場合は可能**<br>• 「コントロールパネル」からBitLocker機能の無効化が可能なため、グループポリシー設定でコントロールパネルの無効化が必要 |
| 運用面 | 導入 | **インストーラ実行でセキュリティポリシーを配布**<br>• インストーラ実行でセキュリティポリシーを配布<br>• Macへ導入可能なため、一元管理が可能 | **セキュリティポリシーを一元管理するにはActive Directory環境が必要** |
| | パスワード忘れ時 | **緊急時も利用者と管理者間で解決可能**<br>• 厳重な本人確認後、チャレンジ＆レスポンスでパスワードの再発行が可能<br>• PCオフライン時でも対応可能 | **回復キー(※)をPC電源ON直後に表示される画面から入力**<br>※パスワード紛失に備え、暗号化時に保存しておく48ケタの数字 |
| | 認証方式 | **シングルサインオン対応可能**<br>• OS認証との二段階認証も選択可能 | **BitLocker認証とWindows認証の二段階認証** |
| | PC起動不可時 | **該当端末上で復号処理が可能**<br>• 初期インストール時に生成されるリカバリデータからリカバリメディアを作成し、リカバリメディアから当該端末を起動して復号処理を行う | **暗号化解除したデータの退避用に別途ハードディスクが必要**<br>• BitLockerがインストールされた別の端末へハードディスクを取り付けてログオンし、その後、ロック解除ボタンと回復キーで復号 |

掲載日：2016年6月22日

第２回　開発ベンダーのご担当者様へ

# 競合他社に勝つ！内部不正に強いWebシステムを目指して

新規開発システム、現行システムのいずれにも組み込みが容易な対策とは

誰から、何を、どのように保護していくか。今後提供・開発していくWebシステム、現在運用中のWebシステムにセキュリティ対策をどのように組み込めばよいか。本コラムでは、Webシステムのセキュリティレベル向上について、システム開発者の視点から「事前」「事後」の具体的な解決法にアプローチしていきます。

企業システムはWeb環境へ。ポータルサイトや文書管理システムなど、社内外の関係者と情報共有するインターフェースは今やWebが当たり前となってきています。このような中、「機密情報を扱っているが大丈夫だろうか…？」、「情報開示は業務上必要だが、共有した情報の管理は厳格に行いたい！」、「今のシステムは情報漏えい対策が取られているだろうか…？」といった、Web系の業務システム(以下、Webシステム)のセキュリティ課題に目を向ける企業ユーザが増えてきています。

Webシステム製品や受託システムの開発に取り組まれている開発ベンダーのプロジェクトマネージャー、システムエンジニア、お客様担当セールスにとっても、セキュリティ対策の強化は、製品力強化、顧客満足度向上に向けた重要テーマの一つとなっており、既に「今のシステムはそのままで内部不正対策を一層強化して欲しい」、「ユーザの利便性を損なうことなく実装できる追加対策を検討して欲しい」といったお客様からの要求対応に取り組まれているところなのではないでしょうか。

## Webシステムが直面する内部不正リスクとは

情報漏えい対策は、ともすれば外的要因に目が向けられがちですが、情報漏えい・流出の要因として無視できないのが『内部不正』です。Webシステムを使って業務情報を共有する際には、社員や派遣社員、協力会社など、内部ユーザの不正行為によるリスクに目を向けなければなりません。

一般的に、システムやファイルへのアクセス制限は、外部ユーザからの不正行為に対して有効であっても、許可されたユーザによる不正行為に対しては意外と脆いものです。またユーザのIDを不正に取得する「なりすまし行為」にも注意を払わなくてはいけません。

許可されたユーザが不正行為を行う手法として、例えば、次のようなやり方が考えられます。


画面のキャプチャ、プリントスクリーン

文書ファイルのダウンロード、印刷


図版、画像データなどの二次利用

これらの操作は、セキュリティ上は是非とも制限したい操作です。情報漏えいのリスクなく安全に情報を共有するためには、外部からの攻撃に備えるのはもちろん、内部に潜むリスクにもしっかり目を向けて、不正を許さない仕組み作りを行っていく必要があります。

## Webシステムでは何を保護するべきなのか？

Webブラウザの表示内容は、そのまま印刷したり、プリントスクリーン操作で簡単にコピーしたりすることができます。例えば、顧客情報を取り扱うコールセンターやサポート・サービス業務では、操作画面にお客様の大切な情報が表示されます。そのため、画面の印刷・コピー操作などにより、不正に情報が持ち出されかねません。

Webブラウザから直接参照できるOfficeファイルやPDFファイルなどについては言うまでもないでしょう。アクセス制御により、許可されたユーザ以外は閲覧・参照・印刷・保存などができないようにするのはもちろん、許可されたユーザの不正を防ぐ対策が必要です。具体的にはファイルの不正な流用、不正な保存・印刷による持ち出しなどを防ぐ対策が欠かせません。


意外と見落としがちなのが、図版やグラフ、写真画像の漏えいや不正な二次利用を防ぐ対策です。有料で借り出した素材写真(リースポジ)などは、許諾された条件での利用しか認められないものもあり、不正な二次利用によって高額な違約金が発生することもあります。

これらを踏まえ、Webシステムでは、Webブラウザに表示される情報、 Web上で共有されるファイルに対して保護対策を講じる必要があります。

## どのような観点で保護するべきなのか？

Webシステム上の情報を守るためには、不正発生の「事前」「事後」両面から考えていく必要があります。

事前の対策
**見せつつ守る**

セキュリティを強化したいが、広く関係者に情報を共有したい。この両立が難しい要件を実現すること。

例えば

アプリケーションメニューやショートカットキー操作の制限で実現する方法があります。Webブラウザに対しては、HTML保存、ソース表示、画像保存、画面キャプチャなどをWebブラウザメニューやキーボード機能から制限します。Office、PDFなどの共有ファイルに対しては、ファイルの保存、印刷、編集、画面キャプチャなどの操作をアプリケーション側から制限します。このように情報共有に必要な機能は残した状態で、不正利用を誘引しかねない機能を制限することが必要です。

事後の対策
**流出しても守る**

不正利用が発生した際に情報が漏えいしない仕組みを用意しておくこと。

例えば

ファイルの自動暗号化で実現する方法があります。ダウンロードされた共有ファイルに対しては、ユーザが意識することなく自動的に暗号化し、流出しても閲覧できないようにすることが必要です。

### 機能設計例

**Webブラウザに表示される情報の保護**

Webサイトにアクセスするユーザが、画面上のコンテンツを流用・持ち出しできないよう、操作を制限します。

- HTMLファイル
- 画像ファイル(GIF、BMPなど)
- 動的コンテンツ(CGI、JSPなど)
- テキスト文書
- Ajax
- Flashファイル

このような操作を制限

- ソース閲覧
- キャプチャ
- 印刷
- ダウンロード
- 範囲選択
- コピー

**Web上で共有されるファイルの保護**

保護文書の印刷や流用、外部への持ち出しができないよう保護し、ユーザのファイル操作を制限します。

- Office文書
  （Word、Excel、Powerpoint）
- PDF文書


このような操作を制限

- ダウンロード
- 印刷
- 編集
- 外部への情報の持ち出し
- キャプチャ
- コピー/ペースト
- 上書き

## 開発ベンダーがセキュリティで差別化するための課題と解決法

セキュリティニーズの高まりにより、Webシステム開発時には想定していなかったセキュリティ要件が都度発生しています。セキュリティ要件に対応し続けるために開発ベンダーとしてどのように対処していくか。セキュリティ機能を自社で開発し、Webシステムに組み込むのも選択肢の一つかもしれません。しかし、競合ひしめく状況の中、開発コスト・リソースをWebシステムのコア機能の拡充に集中しなければいけません。コア機能以外の部分に関しては極力コスト・リソースを効率化する必要があります。実際、開発ベンダーからは次のような声も聞かれます。

今後提供・開発していくWebシステム、運用中のWebシステムに更に強化したセキュリティ機能が必要であることは分かっているが、現状の開発体制、費用対効果を考慮すると自社での開発対応はなかなか難しい…

そこでお勧めしたいのが、アドオン型のセキュリティ対策ソフトウェア製品の利用です。利用にあたっては、「事前」「事後」2つの対策を備え、少ない開発工数でアドオンできるものが望ましいでしょう。セキュリティ対策ソフトウェア製品の開発ベンダーと連携するスタイルが取れるのであれば、開発メンバーの負荷を減らすことが期待できます。

### アドオン型セキュリティ対策ソフトウェア製品の利用法

**新システム開発時の組み込み**

システム開発工程に影響を及ぼすことなく、セキュリティレベルの更なる向上が可能になります。お客様への提供形態は、標準機能としての組み込み、もしくはオプションとしての提供が考えられます。

**Webシステム運用中のお客様の追加要求への対応**

お客様への追加要求に対してスムーズな対応が可能になります。製品バージョンアップ時にオプションとして提供することも考えられます。

## 「Webコンテンツ保護・情報漏えい対策ソリューション」とは

当社は、開発ベンダーの課題を解決するためのアドオン型セキュリティ対策ソフトウェアとして「Webコンテンツ保護・情報漏えい対策ソリューション」を提供しています。

本ソリューションは、Webブラウザに表示される情報の保護を目的とした『Webブラウザプロテクター AE』、Web上で共有されるファイルの保護を目的とした『Webコンテンツプロテクター AE』の2つのセキュリティ対策ソフトウェア製品で構成されています。いずれもアドオン型の製品なので、今あるシステム、今後開発されるシステムに対して、少ない開発工数でセキュリティレベルをアップさせることが可能になります。いずれか一つ、あるいは両製品をセットで組み込むことも可能です。Webシステムでの安全な情報運用・共有を実現するものとして、官公庁・金融・製造など、機密性の高い情報を扱うお客様を中心に数多くの導入実績を有し、年々お問い合わせも増加しています。

この機会に、御社の開発製品・システムと当社「Webコンテンツ保護・情報漏えい対策ソリューション」の連携を是非ご検討ください。

(2016年8月4日)

Webシステム上で共有される重要機密情報の保護を実現

### Webコンテンツ保護・情報漏えい対策ソリューション

#### Webブラウザプロテクター AE


Webブラウザに表示される情報を流用、漏えいから守ります。

Webサイトにアクセスするユーザが、画面上のコンテンツを流用・持ち出しできないよう、操作を制限します。

- ユーザ操作制限
- 流出経路の遮断
- 操作ログの収集

#### Webコンテンツプロテクター AE


Web上で共有されるファイルの流用や持ち出しを防ぎます。

保護文書印刷や流用、外部への持ち出しができないよう保護し、ユーザのファイル操作を制限します。

- 文書の暗号化
- ユーザ操作制限
- 流出経路の遮断
- 操作ログの収集

### 適用システム例


### 利用事例

Webブラウザプロテクター AE

**官庁様　職員情報管理システム**

- Webブラウザで表示されるテキスト情報に加え、顔写真のコピー&ペースト、印刷、キャプチャなども禁止し、閲覧のみを可能にすることで安全性を向上。
- 「Webコンテンツプロテクター AE」も同時導入し、ダウンロードしたファイルを強制的に保護する仕組みを構築。

**大学様　研究情報管理システム**

- 研究員と作業者のグループで異なる閲覧制御を実施し、部門外への公開禁止情報も含めた研究情報を適切な範囲で共有。
- ユーザ属性による閲覧制御を可能にしたことで、学外での作業が可能になり、利便性・研究効率を向上。

### 利用事例

Webコンテンツプロテクター AE

**製造業様　海外委託先との情報共有**

- 企業間・部門間情報共有プラットフォームと連携し、海外委託先と重要情報を安全かつ効率的に共有する仕組みとして導入。
- 情報共有システムだけでは実現できない、委託先からの二次漏洩まで防止。
- 情報流出・悪用に怯えることなく、海外の委託先と技術情報を共有することが可能に。

**金融業様　ナレッジ保護**

- ブラウザベースのナレッジシステム上の機密文書の適正利用と外部流出防止を実現。
- 「誰が何を印刷したか」をサーバ・紙の両方で特定し、万が一の時の追跡を可能に。
- 社員のセキュリティ意識も向上。

**金融業様　社内ポータル保護**

- 契約社員やグループ会社社員も利用する社内ポータルの安全運用対策として後付で導入。
- 利便性はそのままにセキュリティを強化、ダウンロード後のデータ悪用を防止。
- 通常業務に影響しない／ユーザのリテラシーに依存しない情報漏えい対策の仕組みづくりを実現。

**プロセス業様　社内ポータルセキュリティ強化**

- 経営数値情報、中計資料、社長訓示などのファイル共有を行っていたグループ会社ポータルの安全性向上に向けて導入。
- 「Webブラウザプロテクター AE」も同時導入し、HTMLデータや画像データも合わせて保護。

利用事例について詳しい説明をご希望の方はお問い合わせください。

### 詳しくはWebサイトをご覧ください

**Webコンテンツ保護・情報漏えい対策ソリューション**

https://www.nec-solutioninnovators.co.jp/sl/wxp/

コンテンツ保護　セキュリティ対策　検索

掲載日：2016年8月4日

Orchestrating a brighter world

NEC

未来に向かい、人が生きる、豊かに生きるために欠かせないもの。
それは「安全」「安心」「効率」「公平」という価値が実現された社会です。

NECは、ネットワーク技術とコンピューティング技術をあわせ持つ
類のないインテグレーターとしてリーダーシップを発揮し、
卓越した技術とさまざまな知見やアイデアを融合することで、
世界の国々や地域の人々と協奏しながら、
明るく希望に満ちた暮らしと社会を実現し、未来につなげていきます。